

SUSE Linux Enterprise Server

10 SP3

www.novell.com

2009 年8 月28 @

インストールおよび管理



インストールおよび管理

All content is copyright © Novell, Inc.

保証と著作権

このマニュアルは、Novellの知的所有権で保護されています。このマニュアルを複製、コピー、または配布するには、本使用許諾契約の各条項に明示的に同意する必要があります。

このマニュアルは、以下の条件を満たす限り、電子的または印刷物などの形式で、自由に複製、コピー、配布することができます。

複製、コピー、配布されるコピーには、この著作権表示と作成者、貢献者名が明示的かつ弁別的に表示する必要があります。このマニュアルは、特に印刷形式の場合、非商用の目的でのみ複製、配布できます。本マニュアルの全部または一部を他の目的で使用する場合は、事前にNovell, Incから明示的な許可を得る必要があります。

Novellの商標リストについては、<http://www.novell.com/company/legal/trademarks/tmlist.html>のNovell Trademark and Service Mark Listを参照してください。

Linuxは、Linus Torvaldsの登録商標です。他のすべての第三者の商標は、各所有者が所有権を有しています。商標記号(®、™など)は、Novellの商標を表しています。アスタリスク()は、サードパーティの商標を表します。

本書のすべての情報は、細心の注意を払って編集されています。しかし、このことは絶対に正確であることを保証するものではありません。Novell, Inc.、Suse Linux Products GmbH、著者、翻訳者のいずれも誤りまたはその結果に対して一切責任を負いかねます。

目次

このガイドについて	xv
パート I の導e	1
1 SUSE Linux Enterpriseのプランニング	3
1.1 SUSE Linux Enterpriseの導入にあたっての検討事項	5
1.2 SUSE Linux Enterpriseの導入	6
1.3 SUSE Linux Enterpriseの実行	6
2 導入計画	9
2.1 10台以下のワークステーションへの導入	9
2.2 100台以下のワークステーションへの導入	11
2.3 100台を超えるワークステーションへの導入	19
3 YaSTによるインストール	21
3.1 IBM POWER:ネットワークインストールのためのシステムのスタート アップ	21
3.2 IBM System z:インストールのためのシステムのスタートアップ	22
3.3 インストール時のシステム起動	22
3.4 インストールのワークフロー	25
3.5 ブート画面	25
3.6 言語	29
3.7 IBM System z:ハードディスクの設定	29
3.8 メディアチェック	32
3.9 使用許諾契約	32
3.10 インストールモード	33
3.11 時計とタイムゾーン	34

3.12	インストールの設定	34
3.13	インストールの実行	39
3.14	インストール済みシステムの環境設定	42
3.15	グラフィカルログイン	52
4	リモートインストール	53
4.1	リモートインストールのインストールシナリオ	53
4.2	インストールソースを保持するサーバのセットアップ	63
4.3	ターゲットシステムのブートの準備	74
4.4	ターゲットシステムをインストールのためにブートする	85
4.5	インストールプロセスのモニタ	91
5	自動インストール	95
5.1	単純な大規模インストール	95
5.2	ルールベースの自動インストール	108
5.3	詳細情報	113
6	カスタマイズした事前インストールの配布	115
6.1	マスタマシンの準備	116
6.2	firstbootインストールのカスタマイズ	117
6.3	マスタインストールの複製	125
6.4	インストールの個人設定	125
7	高度なディスクセットアップ	127
7.1	LVMの設定	127
7.2	ソフトウェアRAID設定	137
8	YaSTでのシステム設定	143
8.1	YaST言語	144
8.2	YaSTコントロールセンター	145
8.3	ソフトウェア	146
8.4	ハードウェア	163
8.5	システム	170
8.6	ネットワークデバイス	183
8.7	ネットワークサービス	184
8.8	AppArmor	192
8.9	セキュリティとユーザ	192
8.10	仮想化	203
8.11	その他	204
8.12	テキストモードのYaST	207

8.13	コマンドラインからのYaSTの管理	211
8.14	SaX2	214
8.15	トラブルシューティング	220
8.16	詳細情報	221
9	ZENworksを使ったソフトウェアの管理	223
9.1	コマンドラインからrugを使った更新	224
9.2	ZENツールを使ったパッケージの管理	228
9.3	詳細情報	234
10	SUSE Linux Enterpriseのアップデート	235
10.1	SUSE Linux Enterpriseのアップデート	235
10.2	サービスパックのインストール	238
10.3	バージョン9からバージョン10へのソフトウェアの変更点	250
	パート II 管理	265
11	OpenWBEM	267
11.1	OpenWBEMの設定	269
11.2	OpenWBEM CIMOM設定の変更	274
11.3	詳細情報	295
12	IPネットワークの大容量記憶デバイス—iSCSI	297
12.1	iSCSIターゲットのセットアップ	298
12.2	iSCSIイニシエータの設定	304
13	Linux向けiSNSの概要	309
13.1	iSNSのしくみ	309
13.2	Linux向けiSCSIのインストールとセットアップ	311
13.3	iSNSの設定	311
13.4	詳細情報	315
14	Oracle Cluster File System 2	317
14.1	Oracle Cluster File System 2クラスタサービス	319
14.2	ディスクハートビート	320
14.3	内部メモリファイルシステム	321
14.4	管理ユーティリティとコマンド	321
14.5	OCFS2のパッケージ	324

14.6	OCFS2ボリュームの作成	324
14.7	OCFS2ボリュームのマウント	329
14.8	追加情報	331
15	Linuxのアクセス制御リスト	333
15.1	従来のファイルパーミッション	333
15.2	ACLの利点	335
15.3	定義	336
15.4	ACLの処理	336
15.5	アプリケーションでのACLサポート	346
15.6	詳細情報	346
16	RPM—パッケージマネージャ	347
16.1	パッケージの信頼性の検証	348
16.2	パッケージの管理:インストール、アップデート、およびアンインストール	348
16.3	RPMとパッチ	350
16.4	デルタRPMパッケージ	352
16.5	RPMクエリー	353
16.6	ソースパッケージのインストールとコンパイル	356
16.7	buildによるRPMパッケージのコンパイル	358
16.8	RPMアーカイブとRPMデータベース用のツール	359
17	システムモニタリングユーティリティ	361
17.1	デバッグ	362
17.2	ファイルとファイルシステム	364
17.3	ハードウェア情報	366
17.4	ネットワーク	369
17.5	/procファイルシステム	370
17.6	プロセス	373
17.7	システム情報	377
17.8	ユーザ情報	381
17.9	日付と時刻	382
18	シェルの使用	383
18.1	Bashシェルでの作業開始	384
18.2	ユーザとアクセス権	397
18.3	Linuxの重要なコマンド	402
18.4	viエディタ	414

19 64ビットシステム環境での32ビットと64ビットのアプリケーション 421

19.1	ランタイムサポート	422
19.2	ソフトウェア開発	423
19.3	biarchプラットフォームでのソフトウェアのコンパイル	424
19.4	カーネル仕様	426

20 Linuxシステムのブートと設定 427

20.1	Linuxのブートプロセス	427
20.2	initプロセス	432
20.3	/etc/sysconfigによるシステム設定	441

21 ブートローダ 445

21.1	ブートローダの選択	446
21.2	GRUBによるブート	446
21.3	YaSTによるブートローダの設定	457
21.4	Linuxブートローダのアンインストール	461
21.5	ブートCDの作成	462
21.6	SUSEのグラフィカル画面	463
21.7	トラブルシューティング	464
21.8	詳細情報	465

22 特別なシステム機能 467

22.1	特殊ソフトウェアパッケージ	467
22.2	バーチャルコンソール	475
22.3	キーボードマッピング	475
22.4	言語および国固有の設定	476

23 プリンタの運用 481

23.1	印刷システムのワークフロー	483
23.2	プリンタに接続するための方法とプロトコル	484
23.3	ソフトウェアのインストール	484
23.4	プリンタの設定	485
23.5	ネットワークプリンタ	490
23.6	グラフィカルな印刷インタフェース	494
23.7	コマンドラインからの印刷	494
23.8	SUSE Linux Enterpriseの特殊機能	494
23.9	トラブルシューティング	499

24	udevを使用した動的カーネルデバイス管理	509
24.1	/devディレクトリ	509
24.2	カーネルのueventおよびudev	510
24.3	ドライバ、カーネルモジュールおよびデバイス	510
24.4	ブートおよび初期デバイスセットアップ	511
24.5	udevイベントのデバッグ	512
24.6	udevルールを処理するカーネルデバイスイベントへの影響	513
24.7	永続的なデバイス名の使用	513
24.8	置換されたhotplugパッケージ	514
24.9	詳細情報	515
25	Linuxのファイルシステム	517
25.1	用語	517
25.2	Linuxの主要なファイルシステム	518
25.3	サポートされている他のいくつかのファイルシステム	525
25.4	Linux環境での大規模ファイルサポート	526
25.5	詳細情報	528
26	X Windowシステム	529
26.1	X Window システムの手動設定	529
26.2	フォントのインストールと設定	536
26.3	詳細情報	543
27	PAMを使用した認証	545
27.1	PAM設定ファイルの構造	546
27.2	sshdのPAM設定	548
27.3	PAMモジュールの設定	550
27.4	詳細情報	552
28	電源管理	555
28.1	省電力機能	556
28.2	APM	557
28.3	ACPI	559
28.4	ハードディスクの休止	567
28.5	powersaveパッケージ	569
28.6	YaST電源管理モジュール	578
29	無線通信	583
29.1	無線LAN	583

パート IV サービス 595

30 ネットワークの基礎 597

30.1	IPアドレスとルーティング	601
30.2	IPv6 一次世代のインターネット	604
30.3	ネームレゾリューション	614
30.4	YaSTによるネットワーク接続の設定	616
30.5	SUSE Linux上でのVLANインタフェースの設定	636
30.6	NetworkManagerを使用したネットワーク接続の管理	638
30.7	ネットワークの手動環境設定	640
30.8	ダイアルアップアシスタントとしてのsmpppd	658

31 ネットワーク上のSLPサービス 663

31.1	SLPをアクティブ化する	663
31.2	SUSE Linux EnterpriseのSLPフロントエンド	664
31.3	SLP経由のインストール	665
31.4	SLPを使ったサービスの提供	665
31.5	詳細情報	666

32 NTPによる時刻の同期 667

32.1	YaSTでのNTPクライアントの設定	667
32.2	ネットワークでのxntp構成	671
32.3	ローカルリファレンスクロックの設定	672

33 ドメインネームシステム 673

33.1	DNS用語	673
33.2	YaSTでの設定	674
33.3	ネームサーバBINDの起動	684
33.4	設定ファイル/etc/named.conf	686
33.5	ゾーンファイル	690
33.6	ゾーンデータの動的アップデート	695
33.7	安全なトランザクション	696
33.8	DNSセキュリティ	697
33.9	詳細情報	698

34 DHCP 699

34.1	YaSTによるDHCPサーバの設定	700
34.2	DHCPソフトウェアパッケージ	709
34.3	DHCPサーバdhcpd	710
34.4	詳細情報	714

35 NISの使用	715
35.1 NISサーバの設定	715
35.2 NISクライアントの設定	722
36 LDAP—ディレクトリサービス	725
36.1 LDAPとNISの比較	726
36.2 LDAPディレクトリツリーの構造	727
36.3 slapd.confを使用したサーバの設定	731
36.4 LDAPディレクトリのデータ処理	737
36.5 YaSTによるLDAPサーバの設定	741
36.6 YaSTを使ったLDAPクライアントの設定	747
36.7 YaSTでのLDAPユーザおよびグループの設定	755
36.8 LDAPディレクトリツリーの参照	757
36.9 詳細情報	758
37 Samba	761
37.1 用語	761
37.2 Sambaの起動および停止	763
37.3 Sambaサーバの設定	763
37.4 クライアントの設定	770
37.5 ログインサーバとしてのSamba	771
37.6 Active Directoryネットワーク内のSambaサーバ	773
37.7 Windows NTサーバからSambaへの移行	775
37.8 詳細情報	777
38 NFS共有ファイルシステム	779
38.1 必要なソフトウェアのインストール	780
38.2 YaSTによるファイルシステムのインポート	780
38.3 ファイルシステムの手動インポート	781
38.4 YaSTによるファイルシステムのエクスポート	784
38.5 ファイルシステムの手動エクスポート	790
38.6 NFSでのKerberosの使用	793
38.7 詳細情報	794
39 ファイルの同期	795
39.1 使用可能なデータ同期ソフトウェア	795
39.2 プログラムを選択する場合の決定要因	797
39.3 CVSの概要	800
39.4 rsyncの概要	803

40	Apache HTTPサーバ	807
40.1	クイックスタート	807
40.2	Apacheの設定	809
40.3	Apacheの起動および停止	824
40.4	モジュールのインストール、有効化および設定	826
40.5	CGIスクリプトを実行させる	835
40.6	SSLをサポートするセキュアWebサーバのセットアップ	838
40.7	セキュリティ問題の回避	844
40.8	トラブルシューティング	846
40.9	詳細情報	847
41	Squidプロキシサーバ	851
41.1	プロキシキャッシュに関する注意事項	852
41.2	システム要件	854
41.3	Squidの起動	856
41.4	設定ファイル/etc/squid/squid.conf	858
41.5	透過型プロキシの設定	864
41.6	cachemgr.cgi	867
41.7	squidGuard	869
41.8	Calamarisを使用したキャッシュレポート生成	871
41.9	詳細情報	872
パート V	セキュリティ	873
42	X.509証明書の管理	875
42.1	デジタル証明書の原理	875
42.2	CA管理用のYaSTモジュール	880
43	マスカレードとファイアウォール	893
43.1	iptablesによるパケットフィルタリング	893
43.2	マスカレードの基礎知識	896
43.3	ファイアウォールの基礎知識	898
43.4	SuSEfirewall2	899
43.5	詳細情報	904
44	SSH:セキュアネットワークオプション	905
44.1	OpenSSHパッケージ	906
44.2	sshプログラム	906
44.3	scp—セキュアコピー	907
44.4	sftp—セキュアファイル転送	907

44.5	SSHデーモン(sshd)—サーバ側	907
44.6	SSHの認証メカニズム	909
44.7	X、認証および転送メカニズム	910
45	ネットワーク認証—Kerberos	913
45.1	Kerberosで使われる用語	913
45.2	Kerberosの仕組み	915
45.3	ユーザ側から見たKerberos	919
45.4	詳細情報	920
46	Kerberosのインストールと管理	921
46.1	Kerberosレルムの選択	921
46.2	KDCハードウェアの設定	922
46.3	時計の同期化	923
46.4	KDCの設定	924
46.5	Kerberosクライアントの手動設定	927
46.6	YaSTを使ったKerberosクライアントの設定	930
46.7	Kerberosのリモート管理	933
46.8	Kerberosホストプリンシパルの作成	935
46.9	KerberosのPAMサポートの有効化	936
46.10	Kerberos認証用のSSHの設定	937
46.11	LDAPとKerberosの使用	938
47	パーティションとファイルの暗号化	943
47.1	YaSTを使った暗号化ファイルシステムの設定	944
47.2	暗号化ホームディレクトリの使用	948
47.3	viを使用した単一ASCIIテキストファイルの暗号化	949
48	AppArmorによる権限の制限	951
48.1	Novell AppArmorのインストール	952
48.2	Novell AppArmorを有効/無効にする	953
48.3	アプリケーションのプロファイルの開始	954
49	セキュリティと機密性	963
49.1	ローカルセキュリティとネットワークセキュリティ	964
49.2	セキュリティ全般のヒントとテクニック	974
49.3	Central Security Reporting Addressの使用	977

パート VI	トラブルシューティング	979
--------	-------------	-----

50	ヘルプとドキュメント	981
----	------------	-----

50.1	SUSE Help Centerの使用方法	981
50.2	manページ	985
50.3	情報ページ	986
50.4	Linux Documentation Project	986
50.5	Wikipedia:無償のオンライン百科事典	987
50.6	ガイドブック	987
50.7	パッケージのドキュメント	988
50.8	Usenet	989
50.9	規格と仕様	990

51	最も頻繁に起こる問題およびその解決方法	993
----	---------------------	-----

51.1	情報の検索と収集	993
51.2	インストールの問題	996
51.3	ブートの問題	1006
51.4	Loginの問題	1009
51.5	ネットワークの問題	1016
51.6	データの問題	1021
51.7	IBM System z:initrdのレスキューシステムとしての使用	1035

目次	1041
----	------

このガイドについて

このガイドは、プロフェッショナルのネットワークおよびシステム管理者を対象に、SUSE Linux Enterprise®の計画、導入、設定、および操作について説明します。ここでは、SUSE Linux Enterpriseが、ネットワークで必要とされるサービスが使用可能になるように正しく設定され、最初にインストールしたとおりに適切に機能させることができるようになることを目的にしています。このガイドでは、SUSE Linux Enterpriseとお使いのアプリケーションソフトウェアに互換性があるかどうか、また、ない場合の対処方法、および主要機能がアプリケーションの要件に適合しているかどうかなどの分野については取り上げていません。すべての要件が満たされているかどうか監査済みであること、また、必要なインストール作業を実施済みであること、またはこのような監査に備えてテストインストールが求められたことを前提に、詳細を説明していきます。

このガイドでは、次の内容が取り上げられています。

導入

SUSE Linux Enterpriseをインストールする前に、お客様のニーズに合った導入方法や設定など、導入計画を策定します。システムの手動インストール、ネットワークインストールの設定、および自動インストールの実行方法などを説明します。インストールしたシステムは、YaSTを使って適切に設定します。

管理

SUSE Linux Enterpriseには、システムのさまざまな側面をカスタマイズするための幅広いツールが用意されています。この部分では、これらのツールの一部を紹介しています。

システム

このパートを参照して、OSの詳細を学習してください。SUSE Linux Enterpriseはさまざまなハードウェアアーキテクチャをサポートしています。また、これを使って独自のアプリケーションをSUSE Linux Enterprise上で実行することができます。また、Linuxシステムの仕組みを理解し、独自のカスタムスクリプトやアプリケーションに応用するために役立つ、ブートローダや、ブート手順についても説明しています。

サービス

SUSE Linux Enterpriseは、ネットワークオペレーティングシステムとして設計されています。このオペレーティングシステムは、DNS、DHCP、Web、プロキシ、および認証サービスなどの幅広いネットワークサービスを提供しています。また、MS Windowsクライアント/サーバなどとの混在環境にも、柔軟に対応することができます。

セキュリティ

このエディションのSUSE Linux Enterpriseには、さまざまなセキュリティ機能が用意されています。本製品には、アクセス権限を制限することによりアプリケーションを保護するNovell® AppArmorが同梱されています。そのほかに、安全なログイン、ファイアウォール、およびファイルシステム暗号化などの機能も用意されています。

トラブルシューティング

SUSE Linux Enterpriseには、トラブルに対処するために役立つ、さまざまなアプリケーション、ツール、およびドキュメントが用意されています。ここでは、SUSE Linux Enterpriseで発生する可能性がある問題や、その対処方法を詳細に説明します。

1 フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインドキュメントの各ページの下部にあるユーザコメント機能を使用して、コメントを入力してください。

2 マニュアルの更新

このマニュアルの最新版については、SUSE Linux Enterprise ServerWebサイト [<http://www.novell.com/documentation/sles10/index.html>]を参照してください。

3 追加のマニュアル

本製品に関連する他のマニュアルについては、<http://www.novell.com/documentation/sles10/index.html>を参照してください。

スタートアップガイド

インストールの種類やワークフローなどの基本的な情報を取り上げています。

Architecture-Specific Information

SUSE Linux Enterprise Serverターゲットのインストールを準備するために必要な、アーキテクチャ固有の情報について説明しています。

Novell AppArmor 管理ガイド

ご利用の環境のセキュリティを強化するNovell AppArmorの紹介と、実際の使用方法について詳細に説明しています。

Storage Administration Guide

SUSE Linux Enterpriseのさまざまなストレージデバイスの管理方法を紹介しています。

Heartbeat Guide

Heartbeatを使った高可用性システムの実現方法を詳細に説明しています。

Novell Virtualization Technology User Guide

SUSE Linux EnterpriseとXen*仮想化技術を使った仮想化ソリューションの概要を説明しています。

SUSE® Linux Enterprise Desktop製品で提供されているマニュアルの概要は、<http://www.novell.com/documentation/sled10/index.html>を参照してください。次のマニュアルは、SUSE Linux Enterprise Desktop専用です。

GNOME User Guide

このガイドでは、GNOMEデスクトップとその重要なアプリケーションについて、総合的に取り上げています。

KDE User Guide

このガイドでは、KDEデスクトップとその重要なアプリケーションについて、総合的に取り上げています。

Deployment Guide

SUSE Linux Enterprise Desktopの導入と管理について詳細に説明した、管理者向けのガイドです。

Novell AppArmor 管理ガイド

ご利用の環境のセキュリティを強化するNovell AppArmorの紹介と、実際の使用方法について詳細に説明しています。

このマニュアル中の多くの章に、他の資料やリソースへのリンクが記載されています。これらの資料の中には、システムから参照できるものもあれば、インターネット上に公開されているものもあります。

4 マニュアルの表記規則

本書では、次の書体を使用しています：

- `/etc/passwd`: ファイル名およびディレクトリ名
- `placeholder:placeholder`は、実際の値で置き換えられます
- `PATH`: 環境変数`PATH`
- `ls`、`--help`: コマンド、オプション、およびパラメータ
- `user`: ユーザまたはグループ
- `Alt`、`Alt + F1`: キー: 押すためのキーまたはキーの組み合わせ、キーはキーボードと同様に、大文字で表示されます
- `[ファイル]`、`[ファイル] > [名前を付けて保存]`: メニュー項目、ボタン
- ▶ **amd64 ipf**: この項は、指定されたアーキテクチャにのみ関連しています。矢印は、テキストブロックの先頭と終わりを示します。◀
 - ▶ **ipseries s390 zseries**: この項は、指定されたアーキテクチャにのみ関連しています。矢印は、テキストブロックの先頭と終わりを示します。◀
- *Dancing Penguins* (*Penguins*章、↑他のマニュアル): 他のマニュアルの章への参照です。.

パート I. の導e

SUSE Linux Enterpriseのプランニング

1

オペレーティングシステムを既存のIT環境に導入する場合でも、または完全に新しい環境として構築する場合でも、入念な準備が必要です。SUSE Linux Enterprise 10には、さまざまな新機能が追加されました。ここですべての新機能を取り上げることは不可能ですが、代表的な機能強化や新機能について説明していきます。

Xen 3.0 による仮想化

単一のサーバ上で多数の仮想マシンを実行します。各仮想マシンが、OSのインスタンスとして動作します。この技術の詳細については、<http://www.novell.com/documentation/sles10/index.html>の仮想化マニュアルを参照してください。

YaST

YaST用に、さまざまな新しい設定オプションが開発されました。これらのオプションについては、該当する章で説明しています。

OpenWBEMを使ったCIM管理

CIMOM (Common Information Model Object Manager)は、Webベースの企業管理ユーティリティです。CIMOMは、成熟した管理フレームワークを提供しています。関連項目 **第11章 *OpenWBEM*** (267 ページ)。

SPident

管理ユーティリティのSPidentは、インストールされたソフトウェアベースの概要を表示したり、システムの現在のサービスパックレベルを明確にする場合に使用します。

ディレクトリサービス

LDAPに準拠した、さまざまなディレクトリサービスを利用することができます。

- Microsoft Active Directory
- OpenLDAP

Novell AppArmor

Novell AppArmor技術により、システムを堅牢にすることができます。このサービスの詳細は、*Novell AppArmor 管理ガイド* (↑*Novell AppArmor 管理ガイド*)を参照してください。

iSCSI

iSCSIは、Linuxコンピュータを集中ストレージシステムに接続するための、簡単で手頃なソリューションです。iSCSIについての詳細は、[第12章 IPネットワークの大容量記憶デバイス—iSCSI](#) (297 ページ)を参照してください。

Network File System v4

SUSE Linux Enterpriseバージョン10からは、バージョン4のNFSをサポートするようになりました。これにより、パフォーマンス向上、セキュリティの強化、およびステートフルなプロトコルなどの利点を得られます。関連項目 [第38章 NFS共有ファイルシステム](#) (779 ページ)。

Oracle Cluster File System 2

OCFS2は、汎用のジャーナルファイルシステムで、Linux 2.6以降のカーネルと完全に統合されています。OCFS2の概要は、[第14章 Oracle Cluster File System 2](#) (317 ページ)を参照してください。

Heartbeat 2

Heartbeat 2は、クラスタメンバーシップとメッセージングのインフラストラクチャを提供しています。このようなクラスタの設定方法については、『*Heartbeat Guide*』を参照してください。

マルチパスI/O

デバイスマッピングマルチパスI/Oには、さまざまなセットアップに対応したサブシステムの自動設定機能が用意されています。詳細は、『*Storage Administration Guide*』のマルチパスI/Oに関する章を参照してください。

Linuxカーネルクラッシュダンプ

KexecとKdumpを利用することによって、カーネルに関連する問題のデバッグがより簡単に行えるようになりました。この技術は、x86、AMD64、Intel 64、およびPOWERプラットフォーム上で利用できます。

1.1 SUSE Linux Enterpriseの導入にあたっての検討事項

導入計画時に、まずプロジェクトの最終目標と、必要な機能を定義する必要があります。この作業は、プロジェクトごとに個別に行う必要がありますが、一般的には以下のような事柄を検討していきます。

- 何台のコンピュータにインストールする必要があるか? これによって、最適な導入方法も異なります。関連項目 **第2章 導入計画** (9 ページ)。
- システムを配置する環境は、攻撃を受ける可能性があるか? 詳細は、**第49章 セキュリティと機密性** (963 ページ)を参照してください。
- アップデートはどのようにして入手するか? パッチやアップデートは、登録されたユーザの方にオンラインで提供されます。登録方法、パッチ、およびサポートデータベースについては、<http://support.novell.com/patches.html>を参照してください。
- ローカルにインストールする際に手助けが必要か? Novellは、SUSE Linux Enterpriseに関する総合的なトレーニング、サポート、およびコンサルティングサービスを提供しています。詳細は、<http://www.novell.com/products/server/>を参照してください。
- サードパーティ製品が必要か? 利用するプラットフォーム上で、必要な製品やソフトウェアがサポートされているかどうかを確認してください。Novellは、異なるプラットフォームへのソフトウェアの移植支援サービスも提供しています。

1.2 SUSE Linux Enterpriseの導入

システムを完全に稼動するようにするには、できる限り認定ハードウェアを使用してください。ハードウェア認定作業は常時行われ、認定ハードウェアのデータベースは定期的に更新されています。認定ハードウェアを確認するには、<http://developer.novell.com/yessearch/Search.jsp>を参照してください。

インストール台数によっては、インストールサーバを用意したり、自動インストールを実施する方が効率的なこともあります。詳細は、[第2章 導入計画](#) (9 ページ)を参照してください。Xen仮想化技術を使用する場合は、ネットワークルータファイルシステム、またはiSCSIのようなネットワークストレージソリューションの利用を検討してください。関連項目 [第12章 IP ネットワークの大容量記憶デバイス—iSCSI](#) (297 ページ)。

SUSE Linux Enterpriseは、幅広いサービスを提供しています。マニュアルの概要については、[このガイドについて](#) (xv ページ)を参照してください。必要な環境設定の大部分は、SUSEの環境設定ユーティリティYaSTを使って行うことができます。さらに、手作業による環境設定についても、該当する各章で取り上げています。

単にソフトウェアのインストール作業を検討するだけでなく、エンドユーザのトレーニングや、ヘルプ体制なども検討しておく必要があります。

1.3 SUSE Linux Enterpriseの実行

SUSE Linux Enterpriseオペレーティングシステムは、入念にテストされた安定したシステムです。それでも、ハードウェア障害や他の理由で問題が発生し、システムダウンやデータ消失が発生する危険性を完全に回避することはできません。データ消失の危険性を避けるためにも、常に定期的なバックアップを行うようにしてください。

常にセキュリティを最良の状態に保ち、作業を安全に行うためにも、各コンピュータには定期的にアップデートを適用するようにしてください。業務上必要不可欠なサーバがある場合は、同一の構成を持つ予備コンピュータを用意して、実際のサーバに何か変更を加える必要がある場合は、まずこの予備コンピュータでテストして、何も問題がないことを確認しておくことをお勧めします。また、予備のコンピュータを用意しておくことにより、ハードウェア

障害の発生時にも、予備系のコンピュータに切り替えて、業務を続行することができます。

導入計画

SUSE® Linux Enterpriseを導入するにはさまざまな方法があります。物理メディアまたはインストール用ネットワークサーバを使ったローカルインストールから、カスタマイズ性の高い自動リモートインストール技術による大規模な導入まで、幅広いアプローチから選択できます。ご自身の要件に最も適する方法を選択してください。

2.1 10台以下のワークステーションへの導入

SUSE Linux Enterpriseを1～10台のワークステーションにインストールする場合、最も手軽で簡単な方法は、手動インストールで各ワークステーションにSUSE Linux Enterpriseを導入することです。詳細は、[第3章 YaSTによるインストール](#) (21 ページ)を参照してください。手動インストールは、要件に応じてさまざまな方法で行うことができます。

SUSE Linux Enterpriseメディアからのインストール (10 ページ)

ネットワークに接続しない1台のワークステーションにインストールする場合は、この方法を検討してください。

SLPを使ったネットワークサーバからのインストール (10 ページ)

1～数台のワークステーションにインストールする場合で、SLPでアナウンスされたネットワークインストールサーバを利用できる場合は、この方法を検討してください。

ネットワークサーバからのインストール (11 ページ)

1～数台のワークステーションにインストールする場合で、ネットワークインストールサーバを利用できる場合は、この方法を検討してください。

表 2.1 SUSE Linux Enterprise メディアからのインストール

Installation Source	SUSE Linux Enterprise メディアキット
手動操作を必要とするタスク	<ul style="list-style-type: none">・ インストールメディアの挿入・ インストールターゲットのブート・ メディアの交換・ YaSTインストール範囲の指定・ YaSTシステムを使ったシステムの設定
リモートコントロールされるタスク	なし
詳細	3.3.2項「SUSE Linux Enterprise メディアからのインストール」 (24 ページ)

表 2.2 SLPを使ったネットワークサーバからのインストール

Installation Source	SUSE Linux Enterprise インストールメディアのあるネットワークインストールサーバ
手動操作を必要とするタスク	<ul style="list-style-type: none">・ ブートディスクの挿入・ インストールターゲットのブート・ YaSTインストール範囲の指定・ YaSTシステムを使ったシステムの設定
リモートコントロールされるタスク	なし、ただし、この方法とVNCとの組み合わせ可能

詳細

3.3.3項「SLPを使ったネットワークサーバからのインストール」 (24 ページ)

表 2.3 ネットワークサーバからのインストール

Installation Source	SUSE Linux Enterpriseインストールメディアのあるネットワークインストールサーバ
手動操作を必要とするタスク	<ul style="list-style-type: none">• ブートディスクの挿入• ブートオプションの指定• インストールターゲットのブート• YaSTインストール範囲の指定• YaSTシステムを使ったシステムの設定
リモートコントロールされるタスク	なし、ただし、この方法とVNCとの組み合わせ可能
詳細	3.3.4項「SLPを使用しないネットワークソースからのインストール」 (24 ページ)

2.2 100台以下のワークステーションへの導入

ワークステーションの数が増加する場合、各ワークステーションに手動でインストールし、設定するのは、煩雑で手間がかかる作業になります。ユーザによる手動操作を最小限に抑えた、多数の自動または半自動インストールオプションが用意されています。

全自動インストールを検討する前に、設定内容やシステム構成が複雑になると、セットアップにより多くの時間かかる点を考慮してください。システムの導入に時間的な制約がある場合は、手軽で素早く完了できる、より単純な

方法を選択する方が良い場合もあります。自動インストールは、大規模な導入の場合や、リモートで実行する必要がある場合に適しています。

次のオプションから選択します。

VNC経由の単純なリモートインストール—静的なネットワーク設定 (13 ページ)

小～中規模の導入形態で、静的なネットワークセットアップを行う場合に、この方法を検討してください。この方法では、ネットワーク、ネットワークインストールサーバ、およびVNCビューアアプリケーションが必要になります。

VNC経由の単純なリモートインストール—動的なネットワーク設定 (14 ページ)

小～中規模な導入形態で、DHCPを使った動的なネットワークセットアップを行う場合に、この方法を検討してください。この方法では、ネットワーク、ネットワークインストールサーバ、およびVNCビューアアプリケーションが必要になります。

VNC経由のリモートインストール—PXEブートおよびWake on LAN (14 ページ)

小～中規模の導入形態で、インストールターゲットに対して物理的な操作を行わない、ネットワーク経由でのインストールの場合に、この方法を検討してください。この方法では、ネットワーク、ネットワークインストールサーバ、ネットワークブートイメージ、ネットワークブートが可能なターゲットハードウェア、およびVNCビューアアプリケーションが必要になります。

SSH経由の単純なリモートインストール—静的なネットワーク設定 (15 ページ)

小～中規模の導入形態で、静的なネットワークセットアップを行う場合に、この方法を検討してください。この方法では、ネットワーク、ネットワークインストールサーバ、およびSSHクライアントアプリケーションが必要になります。

SSH経由のリモートインストール—動的なネットワーク設定 (16 ページ)

小～中規模な導入形態で、DHCPを使った動的なネットワークセットアップを行う場合に、この方法を検討してください。この方法では、ネットワーク、ネットワークインストールサーバ、およびSSHクライアントアプリケーションが必要になります。

SSH経由のリモートインストール—PXEブートおよびWake on LAN (16 ページ)

小～中規模の導入形態で、インストールターゲットに対して物理的な操作を行わない、ネットワーク経由でのインストールの場合に、この方法を検討してください。この方法では、ネットワーク、ネットワークインストールサーバ、ネットワークブートイメージ、ネットワークブートが可能なターゲットハードウェア、およびSSHクライアントアプリケーションが必要になります。

単純な大規模インストール (17 ページ)

大規模な導入で、多数の同じコンピュータにインストールする場合に、この方法を検討してください。ネットワークブートを利用できる場合は、ターゲットシステムに対して物理的な操作を行う必要がなくなります。この方法では、ネットワーク、ネットワークインストールサーバ、VNCビューアやSSHクライアントなどのリモートコントロールアプリケーション、およびAutoYaST設定プロファイルが必要になります。ネットワークブートを使用する場合は、ネットワークブートイメージとネットワークブート対応ハードウェアも必要になります。

ルールベースの自動インストール (18 ページ)

さまざまな種類のハードウェアを使用する大規模な導入の場合に、この方法を検討してください。ネットワークブートを利用できる場合は、ターゲットシステムに対して物理的な操作を行う必要がなくなります。この方法では、ネットワーク、ネットワークインストールサーバ、VNCビューアやSSHクライアントなどのリモートコントロールアプリケーション、および複数のAutoYaST設定プロファイルとAutoYaST用のルール設定が必要になります。ネットワークブートを使用する場合は、ネットワークブートイメージとネットワークブート対応ハードウェアも必要になります。

表 2.4 VNC経由の単純なリモートインストール—静的なネットワーク設定

Installation Source	Network
準備作業	<ul style="list-style-type: none">インストールソースの設定インストールメディアからのブート
コントロールと監視	リモート:VNC

最適な導入形態	さまざまなハードウェアを使用する小～中規模の導入形態
短所	<ul style="list-style-type: none"> 各コンピュータを個別にセットアップする必要がある ブートするために物理的な操作が必要になる
詳細	4.1.1項「VNC経由のシンプルリモートインストール—静的なネットワーク設定」(54 ページ)

表 2.5 VNC経由の単純なリモートインストール—動的なネットワーク設定

Installation Source	Network
準備作業	<ul style="list-style-type: none"> インストールソースの設定 インストールメディアからのブート
コントロールと監視	リモート:VNC
最適な導入形態	さまざまなハードウェアを使用する小～中規模の導入形態
短所	<ul style="list-style-type: none"> 各コンピュータを個別にセットアップする必要がある ブートするために物理的な操作が必要になる
詳細	4.1.2項「VNC経由のシンプルリモートインストール—動的なネットワーク設定」(55 ページ)

表 2.6 VNC経由のリモートインストール—PXE ブートおよびWake on LAN

Installation Source	Network
---------------------	---------

準備作業	<ul style="list-style-type: none"> ・ インストールソースの設定 ・ DHCP、TFTP、PXEブート、およびWOLの設定 ・ ネットワークからのブート
コントロールと監視	リモート:VNC
最適な導入形態	<ul style="list-style-type: none"> ・ さまざまなハードウェアを使用する小～中規模の導入形態 ・ サイト間での完全なリモートインストール
短所	各コンピュータを手動でセットアップする必要がある
詳細	4.1.3項「VNC経由のリモートインストール—PXEブートとWake on LAN」(57 ページ)

表 2.7 SSH経由の単純なリモートインストール—静的なネットワーク設定

Installation Source	Network
準備作業	<ul style="list-style-type: none"> ・ インストールソースの設定 ・ インストールメディアからのブート
コントロールと監視	リモート:SSH
最適な導入形態	<ul style="list-style-type: none"> ・ さまざまなハードウェアを使用する小～中規模の導入形態 ・ ターゲットに対して低い帯域幅で接続している環境

短所	<ul style="list-style-type: none"> 各コンピュータを個別にセットアップする必要がある ブートするために物理的な操作が必要になる
詳細	4.1.4頁「SSH経由のシンプルリモートインストール—静的なネットワーク設定」(58 ページ)

表 2.8 SSH経由のリモートインストール—動的なネットワーク設定

Installation Source	Network
準備作業	<ul style="list-style-type: none"> インストールソースの設定 インストールメディアからのブート
コントロールと監視	リモート:SSH
最適な導入形態	<ul style="list-style-type: none"> さまざまなハードウェアを使用する小～中規模の導入形態 ターゲットに対して低い帯域幅で接続している環境
短所	<ul style="list-style-type: none"> 各コンピュータを個別にセットアップする必要がある ブートするために物理的な操作が必要になる
詳細	4.1.5頁「SSH経由のシンプルリモートインストール—動的なネットワーク設定」(60 ページ)

表 2.9 SSH経由のリモートインストール—PXEブートおよびWake on LAN

Installation Source	Network
---------------------	---------

準備作業	<ul style="list-style-type: none"> ・ インストールソースの設定 ・ DHCP、TFTP、PXEブート、およびWOLの設定 ・ ネットワークからのブート
コントロールと監視	リモート:SSH
最適な導入形態	<ul style="list-style-type: none"> ・ さまざまなハードウェアを使用する小～中規模の導入形態 ・ サイト間での完全なリモートインストール ・ ターゲットに対して低い帯域幅で接続している環境
短所	各コンピュータを個別にセットアップする必要がある
詳細	4.1.6項「SSH経由のリモートインストール—PXEブートとWake on LAN」(61 ページ)

表 2.10 単純な大規模インストール

Installation Source	ネットワークを推奨
準備作業	<ul style="list-style-type: none"> ・ ハードウェア情報の収集 ・ AutoYaSTプロファイルの作成 ・ インストールサーバの設定 ・ プロファイルの配布 ・ ネットワークブート(DHCP、TFTP、PXE、WOL)の設定 <p>または</p>

インストールメディアからのターゲットのブート

コントロールと監視	VNC/SSHを使ってローカルまたはリモート
最適な導入形態	<ul style="list-style-type: none">大規模な導入形態同一のハードウェアを使用している環境システムにアクセスしない場合(ネットワークブート)
短所	同一のハードウェアを使用する環境でしか利用できない
詳細	5.1項「単純な大規模インストール」 (95 ページ)

表 2.11 ルールベースの自動インストール

Installation Source	ネットワークを推奨
準備作業	<ul style="list-style-type: none">ハードウェア情報の収集AutoYaSTプロファイルの作成AutoYaSTルールの作成インストールサーバの設定プロファイルの配布ネットワークブート(DHCP、TFTP、PXE、WOL)の設定 または インストールメディアからのターゲットのブート

コントロールと監視	SSH/VNCを使ってローカルまたはリモート
最適な導入形態	<ul style="list-style-type: none"> 多様なハードウェアを使用する環境 サイト間での導入
短所	ルールのセットアップが複雑
詳細	5.2項「ルールベースの自動インストール」(108ページ)

2.3 100台を超えるワークステーションへの導入

2.1項「10台以下のワークステーションへの導入」(9ページ)で説明している中規模インストールでの検討事項の大半は、大規模な導入の場合にも当てはまります。ただし、インストールターゲット数が多くなるほど、自動インストールの短所よりも長所の方が上回るようになります。

導入サイトの要件に応じて、AutoYaSTのルールやクラスフレームワークを詳細に設定する作業にはかなりの時間がかかりますが、その価値は十分にあります。インストールプロジェクトの内容によっては、各ターゲットを個別にインストールする手間を省くことで、大幅に時間を節約できます。

YaSTによるインストール

『*Architecture-Specific Information*』マニュアルの説明に従って、SUSE Linux Enterprise®インストール用のハードウェアの準備を完了し、インストールシステムとの接続を確立したら、SUSE Linux EnterpriseのシステムアシスタントであるYaSTのインタフェースが表示されます。YaSTは、インストールおよび環境設定作業全体をお手伝いいたします。

3.1 IBM POWER: ネットワークインストールのためのシステムのスタートアップ

IBM POWERプラットフォームの場合、『*Architecture-Specific Information*』マニュアルで説明されているように、システムが初期化されます(IPL)。ネットワークインストールの場合、SUSE Linux Enterprise Serverではこれらのシステムにスプラッシュスクリーンまたはブートローダコマンドラインが表示されません。インストール中にカーネルを手動でロードしてください。VNC、X、またはSSH経由でインストールシステムとの接続が確立されると、YaSTのインストール画面が表示されます。スプラッシュスクリーンやブートローダコマンドラインがないため、カーネルまたはブートパラメータを画面に入力できませんが、これらはmkzimage_cmdlineユーティリティを使用してカーネルイメージに含める必要があります。詳細は、『*Architecture-Specific Information*』マニュアルの準備に関する章を参照してください。

ティップ: IBM POWER:次のステップ

3.6項「言語」 (29 ページ)から始まる、YaSTによるインストール手順の説明に従い、インストールを行います。

3.2 IBM System z:インストールのためのシステムのスタートアップ

IBM System zプラットフォームの場合、『*Architecture-Specific Information*』マニュアルで説明されているように、システムが初期化されます(IPL)。これらのシステムでは、SUSE Linux Enterpriseはスプラッシュスクリーンを表示しません。インストール時に、カーネル、`initrd`、および`parmfile`を手動でロードしてください。VNC、X、またはSSH経由でインストールシステムとの接続が確立されると、YaSTのインストール画面が表示されます。スプラッシュスクリーンがないため、画面上でカーネルやブートパラメータを指定することはできません。そのため、カーネルやブートパラメータは`parmfile`で指定する必要があります(詳細については`parmfile`の付録A. *Appendix (Architecture-Specific Information)*を参照してください)。

ティップ: IBM System z:次のステップ

3.6項「言語」 (29 ページ)から始まる、YaSTによるインストール手順の説明に従い、インストールを行います。

3.3 インストール時のシステム起動

SUSE Linux Enterpriseは、CDやDVDなどのローカルのインストールソース、またはFTP、HTTP、NFSサーバなどのネットワークソースからインストールできます。これらの方法を利用する場合、インストール、およびインストール中の操作を行うため、実際のシステムへの物理的なアクセスが必要です。基本的にインストール手順は、インストールソースに関係なく一緒です。

3.3.1 ブートオプション

CDまたはDVD以外からブートする方法もあり、何らかの障害でCDやDVDからブートできない場合に使用できます。これらのオプションについては、[表 3.1. 「ブートオプション」 \(23 ページ\)](#)に記載されています。

表 3.1 ブートオプション

ブートオプション	説明
DVD/CD-ROM	これが最も簡単なブートオプションです。このオプションは、LinuxでサポートされているCD/DVD-ROMが、システムのローカルにある場合に使用できます。
フロッピー (Floppy)	ブートフロッピーディスク作成用のイメージは、CD/DVD 1の/bootディレクトリにあります。READMEも同じディレクトリに格納されています。
PXEまたはBOOTP	このオプションが使用できるのは、システムのBIOSまたはファームウェアにサポートされている場合に限りです。また、ブートサーバはネットワーク内にあることが前提です。別のSUSE Linux Enterpriseシステムで、このタスクを実行させることもできます。
ハードディスク	SUSE Linux Enterpriseは、ハードディスクからブートすることもできます。ハードディスクからブートするには、CD/DVD 1の/boot/loaderディレクトリから、カーネル(linux)とインストールシステム(initrd)をハードディスクにコピーし、ブートローダに適切なエントリを追加します。

3.3.2 SUSE Linux Enterpriseメディアからのインストール

メディアからインストールするには、最初のCDまたはDVDを、適切なドライブに挿入します。メディアからシステムをブートするために、システムを再起動してブート画面を表示します。

3.3.3 SLPを使ったネットワークサーバからのインストール

ご利用のネットワークがOpenSLPをサポートしており、OpenSLPを使って自身を通知するようにネットワークインストールソースが設定されている場合は(4.2頁「インストールソースを保持するサーバのセットアップ」(63 ページ)を参照)、メディアからシステムをブートするか、または他のブートオプションを使用してください。ブート画面で、適切なインストールオプションを選択します。F4 キーを押して、[SLP] を選択します。.

インストールプログラムは、OpenSLPを使ってネットワークインストールソースの場所を取得し、DHCPを使ってネットワーク接続を設定します。DHCPを使ったネットワーク設定に失敗した場合、適切なパラメータの入力を要求するプロンプトが表示されます。以下のように、インストールが続行されます。

3.3.4 SLPを使用しないネットワークソースからのインストール

ご利用のネットワークが、ネットワークインストールソースの取得にOpenSLPをサポートしていない場合は、メディアからシステムをブートするか、他のブートオプションを使用してください。ブート画面で、適切なインストールオプションを選択します。F4キーを押して、目的のネットワークプロトコル(NFS、HTTP、FTP、またはSMB)を選択します。サーバのアドレスとインストールメディアへのパスを指定します。

インストールプログラムは、OpenSLPを使ってネットワークインストールソースの場所を取得し、DHCPを使ってネットワーク接続を設定します。DHCPを

使ったネットワーク設定に失敗した場合、適切なパラメータの入力を要求するプロンプトが表示されます。以下のように、インストールが続行されます。

3.4 インストールのワークフロー

SUSE Linux Enterpriseインストールは、準備、インストール、設定という3段階で行います。準備フェーズでは、言語、時刻、デスクトップの種類など、一部の基本パラメータを設定できます。インストールフェーズでは、インストールするソフトウェア、インストールする場所、インストールしたシステムのブート方法を指定します。インストールを終了すると、マシンがリブートされ、新しくインストールされたシステムが起動し、設定が開始されます。この段階でユーザとパスワードを設定でき、ネットワークとインターネットアクセス、およびプリンタなどのハードウェアコンポーネントを設定できます。

3.5 ブート画面

ブート画面には、インストール手順の複数のオプションが表示されます。
[ハードディスクからブート] はデフォルトの設定で、インストール済みシステムがブートされます(ドライブにCD/DVDが残っていることが多いため)。システムをインストールするには、矢印キーで移動し、インストールオプションを選択します。関連するオプションは次のとおりです。

インストール

通常のインストールモード。最新のハードウェア機能のすべてが有効になります。最新のハードウェア機能のすべてが有効になります。

インストール--ACPI無効

通常のインストールが失敗する場合、システムのハードウェアがACPI (advanced configuration and power interface)をサポートしないことが原因である可能性があります。ACPIが原因と考えられる場合は、このオプションを使用し、ACPIのサポートを省略してインストールします。

インストール--APIC無効

標準インストールに失敗する場合、システムのハードウェアがローカルAPIC(Advanced Programmable Interrupt Controllers)をサポートしていないサポートしていない可能性があります。これに該当する場合は、このオプ

ションを使用して、ローカルAPICサポートなしでインストールしてください。

わからない場合は、[インストール--ACPI無効] または [インストール--セーフ設定] オプションを試してください。

インストール--セーフ設定

システムをDMAモード(CD-ROMドライブ用)でブートし、電源管理機能は無効になります。

レスキューシステム

グラフィックユーザインタフェースのない、最小構成のLinuxを起動します。詳細については、[レスキューシステムの使用項](#) (1030 ページ)を参照してください。

メモリテスト

読み取りと書き込みサイクルを繰り返して、システムのRAMをテストします。リブートしてテストを終了します。詳細については、[51.2.5項「ブートできない」](#) (1001 ページ)を参照してください。

メニューからのインストールオプションは、問題のある機能のみを無効にします。機能を無効にしたり、他の機能を設定する必要がある場合は、[ブートオプション] プロンプトを使用します。カーネルパラメータの詳細は、<http://en.opensuse.org/Linuxrc> を参照してください。

言語、モニタの解像度、インストールソースを変更したり、ハードウェアベンダーからのドライバを追加するには、画面下部にあるバーに記載されているファンクションキーを使用します。

F1 ヘルプ

ブート画面上にあるアクティブな要素の文脈依存型ヘルプを表示します。

F2 言語

インストール時の表示言語を選択します。デフォルトの言語は、[英語] が選択されています。

F3 [ビデオモード]

インストールに使用するグラフィカルディスプレイモードを選択します。GUIで問題が発生する場合は、[テキストモード] を使用してください。

F4 ソース

通常、インストールはデバイスに挿入されたメディアから実行されます。ここでは、FTPやNFSサーバなどの、他のソースを選択します。SLPサーバを利用し、ネットワーク経由でインストールする場合、このオプションを使用してインストールに利用可能なサーバ上のソースを選択します。SLPの詳細については、[第31章 ネットワーク上のSLPサービス](#) (663 ページ) を参照してください。

F5 ドライバ

このキーを使用し、SUSE Linux Enterprise用のドライバアップデートを含むディスクがあることを、システムに通知します。[ファイル] を使って、インストール開始前にCDから直接ドライバをロードします。[はい] を選択した場合、インストールプロセス中の適切な時点で、アップデートディスクの挿入を要求するプロンプトが表示されます。デフォルトは [いいえ] で、ドライバのアップデートはロードしません。

インストールの開始後、SUSE Linux Enterpriseは最小構成のLinuxをロードして構成し、インストール手順を実行します。このプロセス中にブートメッセージと著作権表示を表示するには、Escキーを押します。このプロセスが完了すると、YaSTインストールプログラムが起動し、グラフィカルインストーラが表示されます。

ティップ: マウスを使わないインストール

インストーラがマウスを正しく検出しない場合は、Tabキーを使って項目間を移動し、矢印キーでスクロールを行い、Enterキーで項目を選択します。

3.5.1 SMTサーバのアクセスデータの提供

ネットワークにローカルアップデートソースを提供するSMTサーバがある場合、サーバのURLをクライアントに指定する必要があります。クライアントとサーバはHTTPSプロトコルのみを通じて通信するため、証明書が認証局から発行されていない場合は、サーバの証明書へのパスを入力する必要があります。この情報はブートプロンプトで入力する必要があります。

smturl

SMTサーバのURLURLは`https://FQN/center/regsvc/`という固定フォーマットで、FQNはSMTサーバの完全修飾ホスト名にします。例:

```
smturl=https://smt.example.com/center/regsvc/
```

smtcert

SMTサーバの証明書の場所。次のいずれかの場所を指定します。

URL

証明書をダウンロードできる、リモートの場所(HTTP、HTTPS、またはFTP)。例:

```
smtcert=http://smt.example.com/smt-ca.crt
```

フロッピー(Floppy)

フロッピーの場所を指定します。フロッピーはブート時に挿入する必要があります。フロッピーがなくても、挿入するよう要求されることはありません。値は、文字列floppyに証明書へのパスを連結したものにします。例:

```
smtcert=floppy/smt/smt-ca.crt
```

local path

ローカルマシン上の証明書への絶対パス。例:

```
smtcert=/data/inst/smt/smt-ca.crt
```

Interactive

askを使用してインストール中にポップアップメニューを開き、証明書へのパスを指定します。このオプションはAutoYaSTで使用しないでください。例

```
smtcert=ask
```

証明書のインストールの無効化

アドオン製品によって証明書がインストールされる場合、または公式の認証局によって発行される証明書を使用している場合は、doneを使用します。例:

```
smtcert=done
```

警告: 入力ミスに注意してください

入力した値が正しいことを確認してください。smturlが正しく指定されていないと、アップデートソースの登録が失敗します。smtcertに正しくない値が入力されると、証明書へのローカルパスの指定を求められます。

smtcertが指定されていない場合は、デフォルトで`http://FQN/smt.crt`が使用されます。ここで、FQNはSMTサーバ名です。

3.6 言語

YaSTおよびSUSE Linux Enterpriseは通常、必要に応じて、設定に多様な言語を使用できます。ここで選択された言語は、キーボード配列にも使用されます。さらに、YaSTはシステムクロックのタイムゾーンを推測するためにも、この言語設定を使用します。これらの設定は、システムにインストールする2番目の言語の選択とともに、後で変更することができます。

3.12項「インストールの設定」 (34 ページ)で示すように、インストール中に後で言語を変更できます。インストール済みシステムの言語設定の詳細は、**8.1項「YaST言語」** (144 ページ)を参照してください。

3.7 IBM System z:ハードディスクの設定

IBM System zプラットフォームへのインストールでは、言語選択ダイアログの後で、外部ハードディスクを設定するダイアログが表示されます。SUSE Linux Enterpriseのインストール時には、DASD、Fibre ChannelのAttached SCSI Disk (zFCP)、またはiSCSIを選択します。

[*Configure DASD Disks(DASDディスクの設定)*] の選択後、概要に利用可能なすべてのDASDが表示されます。使用可能なデバイスについて、より詳細な情報を取得するには、リストの上部にある入力フィールドを使用して、表示するチャンネルの範囲を指定します。指定した範囲に従ってリストをフィルタするには、[フィルタ] を選択します。**図 3.1. 「IBM System z:DASDの選択」** (30 ページ)を参照してください。

図 3.1 IBM System z:DASDの選択

設定済みの DASD ディスク
このダイアログで、システムにある DASD ディスクを管理できます。

表示したいディスクをフィルタ表示するには、「最低限のチャネル」と「最大限のチャネル」を設定して、「フィルタ」をクリックしてください。

すべてのアクションは複数のディスクで一度に行なわれます。ディスクを選択して選択または非選択をクリックし、アクションが実行されるディスクを選択してください。

選択されたディスクに対してアクションを実行するには「アクションを実行」を使用してください。アクションは即時に実行されます。

DASD ディスク管理

最低限のチャネル: 0x0000 最大限のチャネル: 0xffff

Sel.	チャネル	デバイス	タイプ	アクセスタイプ	初期化済	パーティション情報
	0.0.0150 --	--	--	--	--	
	0.0.0190 --	--	--	--	--	
	0.0.0191 --	--	--	--	--	
	0.0.0194 --	--	--	--	--	
	0.0.019e --	--	--	--	--	
	0.0.01ab --	--	--	--	--	

 ▼

次に、対応するエントリをリストから選択し、**[選択/解除]** をクリックして、インストールで使用するDASDを指定します。その後、**Perform Action (アクションの実行) > Activate (有効にする)** を選択し、DASDを有効にして、インストールに使用できるようにします。図 3.2. 「IBM System z:DASDの有効化」 (30 ページ) を参照してください。DASDをフォーマットするには、**Perform Action > Format** の順に選択してすぐに実行するか、後でYaSTパーティショナを使用して実行します(8.5.7項 「YaSTパーティション分割ツールの使用」 (172 ページ) を参照)。

図 3.2 IBM System z:DASDの有効化

設定済みの DASD ディスク
このダイアログで、システムにある DASD ディスクを管理できます。

表示したいディスクをフィルタ表示するには、「最低限のチャネル」と「最大限のチャネル」を設定して、「フィルタ」をクリックしてください。

すべてのアクションは複数のディスクで一度に行なわれます。ディスクを選択して選択または非選択をクリックし、アクションが実行されるディスクを選択してください。

選択されたディスクに対してアクションを実行するには「アクションを実行」を使用してください。アクションは即時に実行されます。

DASD ディスク管理

最低限のチャネル: 0x0000 最大限のチャネル: 0xffff

Sel.	チャネル	デバイス	タイプ	アクセスタイプ	初期化済	パーティション情報
✓	0.0.0150 /dev/dasda 3990/E9, 3390/0C RW	--	--	--	はい	--
	0.0.0190 --	--	--	--	--	--
	0.0.0191 --	--	--	--	--	--
	0.0.0194 --	--	--	--	--	--
	0.0.019e --	--	--	--	--	--
✓	0.0.01ab /dev/dasdb 3990/E9, 3390/0C RW	--	--	--	はい	--

 ▼

図 3.3 IBM System z: 使用可能なZFCPディスクの概要

設定済みの ZFCP ディスク

このダイアログで、システムにある ZFCP ディスクを管理できます。

新しい ZFCP ディスクを設定するには、「追加」をクリックしてください

設定された ZFCP ディスクを削除するには、ディスクを選択して「削除」ボタンをクリックしてください。

警告

ZFCP デバイスに READ / WRITE でアクセスする場合、このアクセスが排他アクセスになっていることを確認してください。そうでない場合は、データ損傷の危険性があります。

設定済みの ZFCP ディスク

最低限のチャネル
0x0000

最高限のチャネル
0xffff

フィルタ

チャネル番号	WWPN	zfcplun
0.0.fc00	0x5005076300caa36d	0x5611000000000000
0.0.fc00	0x5005076300caa36d	0x5611000000000000
0.0.fc00	0x5005076300caa36d	0x570a000000000000
0.0.fc00	0x5005076300caa36d	0x570b000000000000
0.0.f800	0x5005076300caa36d	0x5611000000000000
0.0.f800	0x5005076300caa36d	0x5611000000000000
0.0.f800	0x5005076300caa36d	0x570a000000000000
0.0.fc00	0x5005076300caa36d	0x5611000000000000
0.0.fc00	0x5005076300caa36d	0x5611000000000000
0.0.f800	0x5005076300caa36d	0x570b000000000000
0.0.f800	0x5005076300caa36d	0x5611000000000000
0.0.fc00	0x5005076300caa36d	0x570a000000000000
0.0.fc00	0x5005076300caa36d	0x570b000000000000
0.0.f800	0x5005076300caa36d	0x5611000000000000
0.0.f800	0x5005076300caa36d	0x570a000000000000
0.0.f800	0x5005076300caa36d	0x570b000000000000

追加

削除

キャンセル

次へ

SUSE Linux EnterpriseのインストールにZFCPディスクを使用するには、選択ダイアログで [ZFCPディスクの設定] を選択します。これによりダイアログが開き、システムで使用可能なZFCPディスクのリストが表示されます。このダイアログで [追加] を選択し、ZFCPのパラメータを入力する別のダイアログを開きます。図 3.3. 「IBM System z: 使用可能なZFCPディスクの概要」 (31 ページ)を参照してください。

SUSE Linux EnterpriseのインストールにZFCPディスクを使用できるようにするには、ドロップダウンリストから有効な [チャネル番号] を選択します。 [WWPNの取得] (World Wide Port Number)および [LUNの取得] (Logical Unit Number)は、それぞれ使用できるWWPNとFCP-LUNのリストを返し、ここから選択できます。ここまでの設定が完了したら、 [次へ] をクリックしてZFCPダイアログから、ハードディスクの一般設定ダイアログに戻ります。続いて [完了] をクリックして終了し、残りの設定を続けます。

ティップ: 後のステージでのDASDまたはzFCPディスクの追加

DASDまたはzFCPディスクの追加は、インストールワークフロー時だけでなく、インストール提案の表示時にも行えます。ステージにディスクを追加するには、 [Expert] をクリックして、下にスクロールします。 DASDおよびzFCPエントリは、下の方に表示されています。

ディスクを追加したら、パーティションテーブルを再読み込みします。インストール提案画面に戻り、[パーティション]を選択した後、[パーティションテーブルの再読み込み]を選択します。新しいパーティションテーブルが読み込まれ、以前に入力された情報がリセットされます。

3.8 メディアチェック

[メディアチェック] ダイアログは、ダウンロードしたISOから作成したメディアからインストールした場合のみ、表示されます。元のメディアセットからインストールした場合は、ダイアログはスキップされます。

メディアチェックでは、メディアの整合性を確認します。メディアチェックを開始するには、インストールメディアを含むドライブを選択し、[チェック開始]をクリックします。チェックには少し時間がかかります。

複数のメディアをテストするには、結果メッセージがダイアログに表示されるまで待機し、それからメディアを変更します。最後にチェックしたメディアがインストールを開始したメディアではない場合、YaSTからインストールを続行する前に適切なメディアを使用するよう要求されます。

警告: メディアチェックのエラー

メディアチェックが失敗した場合、メディアは破損しています。インストールを続行しないでください。インストールが失敗したり、データが損失することがあります。破損したメディアを交換し、インストール作業をやり直します。

メディアチェックの結果が良好だった場合、[次へ]をクリックしてインストールを続行します。

3.9 使用許諾契約

画面に表示されるライセンス契約全体をお読みください。この契約内容に同意できる場合には[同意します]を選択し、[次へ]をクリックして選択を確認してください。ライセンス契約に同意しない場合には、SUSE Linux Enterpriseをインストールできず、インストールは終了します。

3.10 インストールモード

YaSTがコンピュータ上の他のインストールされたシステムや、既存のSUSE Linux Enterpriseシステムの検出を完了すると、YaSTは利用可能なインストールモードを表示します。

新しいインストール

最初から新しくインストールを開始する場合に、このオプションを選択します。

既存のシステムの更新

新しいバージョンにアップデートする場合に、このオプションを選択します。システムアップデートの詳細は、[第10章 SUSE Linux Enterpriseのアップデート](#) (235 ページ)を参照してください。.

その他のオプション

このオプションは、インストールを中止して、インストールシステムをブート、修復するために用意されています。すでにインストールされているSUSE Linux Enterpriseをブートするには、[\[インストールしたシステムの起動\]](#)を選択します。すでにインストールされているSUSE Linux Enterpriseのブートに問題がある場合は、[51.3項「ブートの問題」](#) (1006 ページ)を参照してください。

ブートに失敗したインストール済みのシステム修復するには、[\[Repair Installed System\(インストール済みシステムの修復\)\]](#)を選択します。システム修復オプションの説明は、[YaSTシステム修復の使用項](#) (1025 ページ)を参照してください。

注意: インストール済みシステムの更新

アップデートは、古いSUSE Linux Enterpriseシステムからインストールされている場合にのみ行えます。SUSE Linux Enterpriseシステムがインストールされていない状態では、新規インストールのみ実行できます。

[8.3.2項「アドオン製品のインストール」](#) (154 ページ)の説明のように、初期インストール時、または後ほど任意の時点で、SUSE Linux Enterpriseシステムと一緒にアドオン製品をインストールすることができます。アドオン製品はSUSE Linux Enterpriseを拡張するために使用します。アドオン製品には、サードパーティ製製品や他の付加ソフトウェアを入れることができます。

SUSE Linux Enterpriseのインストール時にアドオン製品を入れるには、*[Include Add-On Products from Separate Media]* を選択して、*[次へ]* をクリックします。次のダイアログでは、*[追加]* をクリックして、アドオン製品をインストールするソースを選択します。CD、FTP、またはローカルディレクトリなど、さまざまなソースを指定することができます。アドオンメディアを追加したら、必要に応じてその製品の使用許諾契約に同意します。

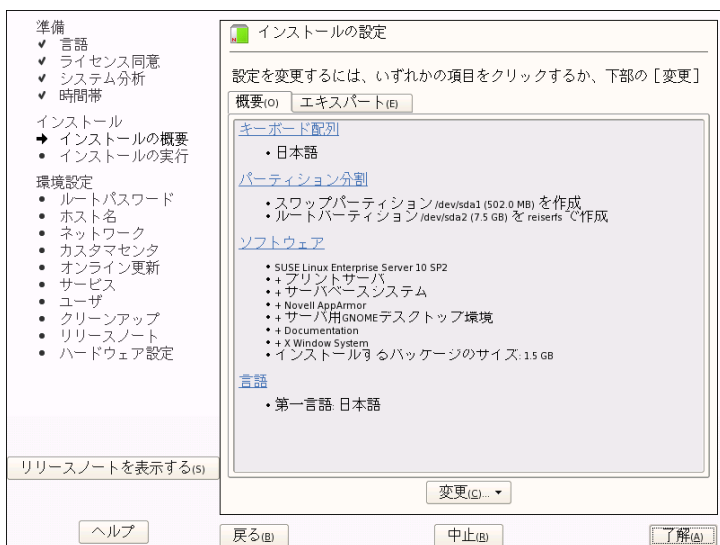
3.11 時計とタイムゾーン

このダイアログは、リストから地域とタイムゾーンを選択できます。インストール時には、これらは両方とも、選択したインストール用の言語に従い、事前に設定されています。*[ハードウェア時計の時間設定]*の下、*[ローカルタイム]*と*[世界協定時間(UTC)]*(GMT)のいずれかをオンにしてください。どちらにすべきかは、ご使用のコンピュータのBIOSハードウェアクロックの設定によって決まります。クロックがGMTに設定されている場合は、UTCに対応しており、標準時間と夏時間への切り替えはSUSE Linux Enterpriseが自動的に行います。現在の日付と時刻を変更するには、*[時刻と日付の変更]* をクリックします。作業が完了したら、*[次へ]* をクリックしてインストールを続行します。

3.12 インストールの設定

YaSTはシステムを詳しく分析した後に、すべてのインストール設定に関して、妥当と思われる提案を提示します。基本設定は*[概要]* タブで変更でき、詳細オプションは*[エキスパート]* タブで使用できます。提案を変更するには、*[変更]* をクリックして変更するカテゴリを選択するか、または見出しの1つをクリックします。これらのダイアログで提示されている項目のいずれかを変更すると、この概要ウィンドウに戻ります。この画面の内容は、設定に応じて常に更新されます。

図 3.4 インストールの設定



ティップ: 変更をデフォルト値にリセットする

すべての変更内容をデフォルト値にリセットするには、[変更] > [デフォルトにリセット] の順にクリックします。YaSTに、元の推奨値が表示されます。

3.12.1 概要

[概要] タブには、最も一般的なインストールの状況において、ユーザーによる調整が必要になる可能性のあるオプションが表示されます。パーティション分割、ソフトウェアの選択、ロケール設定を変更します。

キーボード配列

キーボードの配列を変更するには、[キーボード配列] 選択します。デフォルトでは、インストール用に選択した言語に対応する配列が選択されます。リストからキーボード配列を選択します。特殊文字などを正しく入力できるかどうかを確認するには、ダイアログの下にある [テスト] フィールドを使用します。キーボード配列の変更の詳細は、[8.4.10項「キーボード配列」](#)

(167 ページ)を参照してください。完了したら、[了解] をクリックして、インストール概要に戻ります。

► **zseries:** IBM System z の各プラットフォームでは、インストールはリモートの端末から実行されます。このような環境のホストには、ローカルに接続されたキーボード、マウスは存在しません。◀

パーティション

YaST はほとんどの場合、変更なしに受け入れることができる、適切なパーティショニングスキームを提案します。YaST は、パーティションのカスタマイズにも利用できますが、熟練したユーザ以外はパーティションを変更しないでください。

提案ウィンドウで初めて [パーティション分割] を選択した場合、YaST には、提案されるパーティション設定を示したパーティション設定ダイアログが表示されます。これらの設定を受け入れる場合は、[推奨値を使用] をクリックします。

推奨値を少し変更する場合は、[この推奨値を基にパーティションを設定] を選択して、次のダイアログでパーティションを調整します。まったく別の内容でパーティションを作成する場合は、[カスタムパーティション設定を作成] を選択します。次のダイアログで、パーティションを作成する特定のディスクを選択するか、またはすべてのディスクにアクセスするには [カスタムパーティション] を選択します。カスタムパーティションの詳細については、[8.5.7 項「YaST パーティション分割ツールの使用」](#) (172 ページ) SUSE Linux Enterprise Server のマニュアルを参照してください。YaST パーティションでは、LVM 作成ツールも装備されています。LVM 推奨値を作成するには、[Create LVM Based Proposal] を選択します。LVM の詳細については、[7.1 項「LVM の設定」](#) (127 ページ) を参照してください。

注意: z/VM でのミニディスクの使用

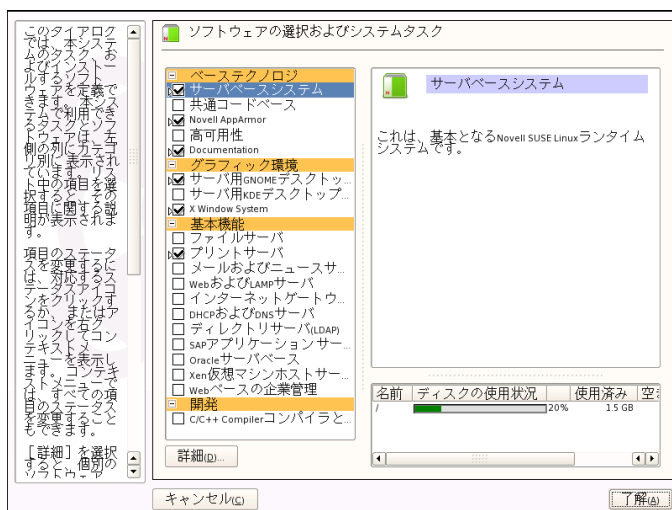
SUSE Linux Enterprise Server が同じ物理ディスク上にある z/VM のミニディスクにインストールされている場合、ミニディスクのアクセスパス (/dev/disk/by-id/) は一意ではなく、物理ディスクの ID になります。このため、同じ物理ディスク上に 2 つ以上のミニディスクがある場合、これらはすべて同じ ID を持ちます。

ミニディスクのマウント時の問題を回避するには、「パス」または「UUID」のいずれかでマウントしてください。

Software

SUSE Linux Enterpriseには、さまざまな用途に適したソフトウェアパッケージが付属しています。提案ウィンドウで [ソフトウェア] をクリックして、ソフトウェアの選択を開始し、必要に応じてインストールスコープを編集します。中央にあるリストからパターンを選択して、右側のウィンドウにある説明を参照します。各パターンには、個々の機能に必要なソフトウェアパッケージが含まれています(マルチメディアやOfficeソフトウェアなど)。インストールするソフトウェアパッケージの選択の詳細については、[詳細] を選択して、YaSTソフトウェアマネージャに切り替えます。詳細については、[図 3.5. 「YaSTソフトウェアマネージャによるソフトウェアのインストールと削除」](#) (37 ページ)を参照してください。

図 3.5 YaSTソフトウェアマネージャによるソフトウェアのインストールと削除



後で、どの時点でも追加のソフトウェアパッケージをインストールしたり、ソフトウェアパッケージをシステムから削除したりすることもできます。詳細については、[8.3.1項 「ソフトウェアのインストールと削除」](#) (146 ページ)を参照してください。

注意: デフォルトのデスクトップ

SUSE Linux Enterpriseのデフォルトのデスクトップは、GNOMEです。KDEをインストールするには、[ソフトウェア] をクリックして、[Graphical Environments(GUI)] から [KDE Desktop Environment] を選択します。

言語

システム言語を変更したり、第二言語サポートを設定するには、[言語] を選択します。リストから言語を選択します。第一言語がシステム言語として使用されます。第2言語を選択すると、追加パッケージをインストールしなくてもいつでもこれらの言語に切り替えられます。詳細については、[8.5.15項「言語の選択」](#) (182 ページ)を参照してください。

3.12.2 エキスパート

熟練したユーザの方がブート方法を設定したり、タイムゾーンやデフォルトのランレベルを変更する場合は、[エキスパート] タブを選択してください。このタブには、[概要] タブにない項目が記載されています。

システム

このダイアログには、お使いのコンピュータからYaSTが取得したすべてのハードウェア情報が表示されます。リストのいずれかの項目を選択して [詳細] をクリックすれば、選択した項目についての詳細な情報を表示できます。高度なユーザは、[システム設定] を選択してPCIID設定とカーネル設定も変更できます。

アドオン製品

概要に、追加したアドオンメディアのソースが表示されます。SUSE Linux Enterpriseのインストールを開始する前に、必要に応じてここからアドオン製品を追加、削除、変更します。

ブート

► **zseries:** IBM System zでブートローダ(zipl)の環境設定にこのモジュールを利用することはできません。 ◀

YaSTにより、システムのブート設定が提案されます。通常、設定を変更せずに、そのまま適用することができます。しかし、カスタムセットアップ

プが必要な場合、ご使用のシステムに応じ、提案された設定を変更します。詳細については、[21.3項「YaSTによるブートローダの設定」](#) (457 ページ)を参照してください。

タイムゾーン

これは、[3.11項「時計とタイムゾーン」](#) (34 ページ)の前半で表示される環境設定と同じです。

デフォルトのランレベル

SUSE Linux Enterpriseは、異なるランレベルでブートすることができます。通常は、ここでは何も変更する必要はありません。しかし、必要な場合には、このダイアログでデフォルトのランレベルを設定してください。ランレベルの設定についての詳細は、[20.2.3項「YaSTでのシステムサービス\(ランレベル\)の設定」](#) (440 ページ)を参照してください。

3.13 インストールの実行

インストール設定を完了した時点で、提案ウィンドウで[次へ]をクリックし、インストールを開始します。[インストール]で確定します。一部のソフトウェアでは、ライセンスの確認が必要になります。選択したソフトウェアの中にこのようなソフトウェアがある場合は、ライセンスの確認ダイアログが表示されます。[了解]をクリックして、ソフトウェアをインストールします。ライセンスに同意しない場合は、[同意しません]をクリックします。ソフトウェアはインストールされません。

システムのパフォーマンスと選択したソフトウェアによっても異なりますが、通常インストールには15分から30分程度かかります。この手順では、SUSE Linux Enterpriseの機能がスライドショーで紹介されます。[詳細]を選択してインストールログに切り替えます。すべてのパッケージのインストールが完了すると、YaSTは新しいLinuxシステムをブートします。ここまで完了した後、ハードウェアおよびシステムサービスの設定に移ります。

3.13.1 IBM System z: インストール済みシステムのIPL処理

多くの場合、YaSTはIBM System zプラットフォームのインストールシステムに自動的に再起動します。この件で既知の例外は、ブートローダが、LPARが

z9以前のマシン上にある環境、またはリリース5.3以前のz/VM環境でFCPデバイス上にある場合です。ブートローダは/bootディレクトリを持つデバイスに書き込まれます。/bootが個別のパーティションにない場合、ルートファイルシステム/と同じパーティションに存在します。

自動再起動を実行できない場合、YaSTはIPLを実行するデバイスについての情報を示すダイアログボックスを表示します。シャットダウンオプションを使用して、シャットダウン後にIPLを実行します。この手順はインストールのタイプによって異なります。以下に示します。

LPARインストール

IBM System z HMCでは、*[ロード]*、*[消去]*の順に選択し、次にロードアドレス(ブートローダの/bootディレクトリを持つデバイスのデバイスアドレス)を入力します。ZFCPディスクをブートデバイスとして使用している場合、*[Load from SCSI(SCSIからロード)]*を選択して、FCPアダプタのロードアドレスとブートアドレスのWWPNおよびLUNを指定します。この時点でロードプロセスが開始します。

z/VMのインストール

VMゲスト(設定は例「*Configuration of a z/VM Directory*」(*↑Architecture-Specific Information*))を参照してください)にLINUX1としてログインし、インストールしたシステムのIPL処理を続行します。

```
IPL 151 CLEAR
```

151はZFCPアダプタのアドレスの例です。この値を正しいアドレスに置き換えてください。

ZFCPディスクをブートデバイスとして使用している場合は、IPLをインストールする前に、ブートデバイスのZFCP WWPNとLUNを指定します。パラメータの長さは8文字に制限されています。8文字を越える長いパラメータを使用する場合は、以下に示すように分割します。

```
SET LOADDEV PORT 50050763 00C590A9 LUN 50010000 00000000
```

最後にIPLを初期化します。以下に示します。

```
IPL FC00
```

FC00はZFCPアダプタのアドレスの例です。この値を正しいアドレスに置き換えてください。

3.13.2 IBM System z:インストール済みシステムへの接続

インストール済みシステムのIPL処理が完了した後は、インストールを完了するためにシステムへの接続を確立します。接続を確立するためのステップは、最初に使用した接続のタイプによって異なります。

接続にVNCを使用する場合

3270端末では、VNCクライアントを使用して、Linuxシステムへ接続するように促すメッセージが表示されます。ただし、このメッセージはカーネルからのメッセージに紛れてしまったり、ユーザが気付く前にこの端末プロセスが終了していたりするため、見落とされることがよくあります。5分待機しても何も起こらないようであれば、VNCビューアを使用して、Linuxシステムへの接続を開始するようにしてください。

Java対応ブラウザを使用して接続を行う場合、インストール済みシステムの完全URLを、ポート番号付きIPアドレスの形式で入力します。以下に入力方法を示します。

```
http://<IP of installed system>:5801/
```

接続にXを使用する場合

インストール済みシステムのIPL処理を行う場合、DASDからブートする前に、インストールの最初のフェーズで利用されたXサーバが有効で、引き続き利用できることを確認してください。YaSTはこのXサーバを使ってインストールを完了します。システムが起動されてもXサーバに適切なタイミングで接続できなければ、問題が起きる可能性があります。

接続にSSHを使用する場合

重要項目: IBM System z: LinuxまたはUNIXシステムからの接続

xtermでsshを開始します。他の端末エミュレータは、YaSTに備えられているテキストベースのインタフェースを完全にサポートしていません。

3270端末では、SSHクライアントを使用して、Linuxシステムへ接続するように促すメッセージが表示されます。ただし、このメッセージはカーネルからのメッセージに紛れてしまったり、ユーザが気付く前にこの端末プロセスが終了していたりするため、見落とされることがよくあります。

メッセージが表示されたら、SSHを使ってLinuxシステムにrootとしてログインします。接続が拒否される、タイムアウトが発生するなど、ログインできない場合には、数分待ってから再度ログインするようにします。

接続が確立されたら、コマンド/usr/lib/YaST2/startup/YaST2.sshを実行します。yastは、このような場合には不十分です。

次に、YaSTは残りのパッケージのインストール作業を続行し、初期のシステム設定を作成します。

3.14 インストール済みシステムの環境設定

システムのインストールは完了しましたが、まだ環境設定が行われていません。ユーザ、ハードウェア、またはサービスは設定されていません。この段階のあるステップで設定が失敗すると、再起動して最後に成功したステップから続行されます。

まず、システム管理者アカウント(rootユーザ)のパスワードを入力します。インターネットアクセスとネットワーク接続を設定します。インターネット接続が機能する環境では、インストールの一環として、システムアップデートを実行することが可能です。さらに、ローカルネットワーク内のユーザを集中的に管理するため、認証サーバに接続することもできます。最後に、コンピュータに接続されているハードウェアデバイスの設定を行います。

3.14.1 システム管理者向けパスワード「root」

rootとは、スーパーユーザ、つまり、システム管理者の名前です。システムでの特定の作業によって、パーミッションを持っていたり、持っていない場

合のある一般ユーザと異なり、rootにはシステム設定への変更、プログラムのインストール、および新規ハードウェアのセットアップを含め、あらゆることを行うための権利が無制限で付与されています。ユーザがパスワードを忘れてしまった場合、システムに関連する他の問題がある場合、rootは支援することができます。rootアカウントは、システム管理、メンテナンス、修復のみに限って使用するのが妥当です。日常的な作業のためにrootでログインすると、ただ1度のミスが、システムファイルの回復不可能な喪失を招くことがあります、非常に危険です。

rootのパスワードは、確認の目的で示すように、2度入力しなければなりません。rootのパスワードは、決して忘れないでください。1度入力すると、このパスワードを取得することはできません。

パスワードを入力するとき、文字はドットに変換されるため、入力中の文字を見ることはできません。正しい文字列を入力したかどうか不明な場合は、テストのために *[Test Keyboard Layout]* フィールドを使用します。

SUSE Linux Enterpriseでは、パスワードにはDES、MD5、またはBlowfishの暗号化アルゴリズムを利用できます。デフォルトの暗号化タイプはBlowfishです。暗号化タイプを変更するには、*[エキスパートオプション]* > *[暗号化の種類]* の順にクリックして、目的のタイプを選択します。

rootは、インストール済みのシステムで後で変更できます。このためには、YaSTを実行し、*[セキュリティとユーザ]* > *[ユーザ管理]* を起動します。

3.14.2 ホスト名とドメイン名

ホスト名は、ネットワーク上のコンピュータ名です。ドメイン名は、ネットワークの名前です。デフォルトでは、ホスト名とドメインの推奨値が提示されます。システムがネットワークに属している場合、ホスト名はこのネットワーク内で固有である必要があります、ドメイン名はネットワーク上のすべてのホストで共通にします。

多くのネットワークでは、システムはDHCP経由で名前を受け取ります。この場合、ホスト名とドメイン名を変更する必要はありません。その代わり、*[DHCPでホスト名を変更する]* を選択します。このホスト名を使用して、ネットワークに接続してなくてもシステムにアクセスできるようにするには、*[ホスト名を/etc/hostsに書き込む]* を選択します。デスクトップ環境を再起動せずにネットワークを頻繁に変更する場合は(別のWLANに切り替える場合な

ど)、このオプションを有効にしないでください。/etc/hostsのホスト名が変更されるとデスクトップシステムが混乱するためです。

インストール後にホスト名の設定を変更する場合は、YaSTで [ネットワークデバイス] > [ネットワークカード] の順にクリックします。詳細については、[30.4.1項「YaSTでのネットワークカードの設定」](#) (617 ページ)を参照してください。

3.14.3 ネットワーク設定

ティップ: IBM System z:ネットワーク設定

IBM System zプラットフォームでは、インストール中に、ターゲットシステム、インストールソース、および、プロセスを制御する端末に接続するには、機能しているネットワーク接続が必要になります。ネットワークをセットアップするステップについては、*Architecture-Specific Information* マニュアルのネットワーク設定の章で解説されています(第2章 *Preparing for Installation* (↑*Architecture-Specific Information*))。IBM System zプラットフォームでは、そこに記載されているネットワークインタフェース(OSA Token Ring、OSA Ethernet、OSA Gigabit Ethernet、OSA Express Fast Ethernet、Escon、IUCV、OSA Express High-Speed Token Ring)のみをサポートしています。YaSTのダイアログには単純に、すでに設定されているインタフェースがそのまま表示されます。このダイアログは単に確認のみで、次に進みません。

デフォルトでは、*[NetworkManager* アプレットを使用しない従来の方法] が有効になっています。必要に応じて、NetworkManagerを使ってネットワークデバイスを管理することもできます。ただし、サーバソリューションとしては、従来の方法をお勧めします。NetworkManagerの詳細は、[30.6項「NetworkManagerを使用したネットワーク接続の管理」](#) (638 ページ)を参照してください。

また、システムのネットワークデバイスの環境設定を行ったり、ファイアウォールやプロキシなどのセキュリティを設定することもできます。後でネットワーク接続を設定する場合は、*[Skip Configuration]* を選択して、*[次へ]* をクリックします。システムのインストールが完了した後でネットワークハードウェアを設定することもできます。ネットワークデバイス設定をスキップした場合、システムはオフラインになり、アップデート情報を取得することはできません。

デバイス設定のほかに、このステップでは次のネットワーク設定を行えます。

ネットワークモード

上述したように、NetworkManagerの使用を有効または無効にします。

ファイアウォール

デフォルトで、設定されたすべてのネットワークインタフェースで SuSEfirewall2は有効になっています。このコンピュータのファイアウォールをグローバルに無効にするには、[\[無効化\]](#) をクリックします。ファイアウォールが有効になっている場合、SSHポートを開いてセキュアシェル経由でリモート接続を可能にすることができます。詳細なファイアウォール設定ダイアログを開くには、[\[ファイアウォール\]](#) をクリックします。詳細については、[43.4.1項「YaSTを使ったファイアウォールの設定」](#) (900 ページ)を参照してください。

IPv6

デフォルトでは、IPv6サポートが有効になっています。無効にするには、[\[Disable IPv6\]](#) をクリックします。IPv6の詳細は、[30.2項「IPv6 —次世代のインターネット」](#) (604 ページ)を参照してください。

VNCリモート管理

VNCを使ってコンピュータをリモートで管理する場合は、[\[変更\] > \[VNCリモート管理\]](#) の順にクリックして、リモート管理を有効にし、ファイアウォールのポートを開きます。複数のネットワークデバイスがあり、どのデバイスのポートを開くかを指定する場合は、[\[ファイアウォールの詳細\]](#) をクリックして、適切なネットワークデバイスを設定してください。より安全なSSHを使ってリモート管理を行うこともできます。

プロキシ

ネットワークでインターネットアクセスを制御するプロキシサーバがある場合は、プロキシURLと認証の詳細をこのダイアログで設定します。

ティップ: ネットワーク設定のデフォルト値へのリセット

ネットワーク設定を元の推奨値にリセットするには、[\[変更\] > \[デフォルトにリセット\]](#) の順にクリックします。この操作により、変更内容が破棄されます。

インターネット接続のテスト

ネットワーク接続を設定した後で、テストできます。YaSTはこの目的でSUSE Linux Enterpriseサーバに接続し、最新版のリリースノートダウンロードします。インストールプロセスが終了したら、これを読んでください。テストに成功しないと、オンラインの登録とアップデートを行えません。

複数のネットワークインタフェースがある場合、インターネットへの接続に適したカードを使用しているかどうかを確認してください。使用していない場合は、**[デバイスの変更]** をクリックします。

テストを開始するには、**[Yes, Test Connection to the Internet]** を選択して、**[次へ]** をクリックします。次のダイアログには、テストの進捗状況と結果が表示されます。テストプロセスの詳細は、**[ログの表示]** で参照できます。テストが失敗した場合、**[戻る]** をクリックしてネットワーク設定に戻り、入力内容を修正します。

この時点でテストを行わない場合は、**[Skip Test]** を選択し、**[次へ]** をクリックします。また、リリースノートのダウンロード、カスタマーセンターの環境設定、およびオンラインアップデートもスキップされます。これらのステップは、システムが最初に設定した後いつでも実行できます。

3.14.4 ノベルカスタマセンターの環境設定

テクニカルサポート情報や製品のアップデートを入手するには、まず製品を登録して、それをアクティブにする必要があります。製品の登録には、**[Novell Customer Center Configuration]** を利用することができます。

ネットワークに接続していない、またはこのステップをスキップしたい場合は、**[Configure Later]** を選択します。SUSE Linux Enterpriseオンラインアップデートもスキップされます。

[含める情報] で、登録時に求められていない追加情報を送信するかどうかを選択します。これにより、登録プロセスが簡単になります。**[詳細]** をクリックして、データプライバシーおよび収集したデータについての詳細情報を取得します。

製品を有効化して登録するほかに、このモジュールは公式なアップデートカタログを設定に追加します。このカタログは、既知のバグまたはセキュリティ問題の修正を含み、オンラインアップデートでインストールできます。

カタログを有効に維持するために、**[カスタマセンタで定期的に同期化]**を選択します。このオプションではカタログをチェックし、新しいカタログを追加したり、古いカタログを削除したりします。手動で追加されたソースはチェックされません。

ティップ: 技術サポート

技術サポートに関する詳細は、<http://www.novell.com/support/products/linuxenterpriseserver/>を参照してください。

3.14.5 オンラインアップデート

[ノベルカスタマセンターの環境設定]が正常に機能した場合、YaSTオンラインアップデートを実行するかどうか選択します。サーバ上に利用可能なパッチ付きパッケージがある場合、既知のバグやセキュリティ問題を修正するために、ここでそれらをダウンロードしてインストールします。インストールしたシステムでオンラインアップデートを実行する方法についての支持は、**8.3.5項「YaSTオンラインアップデート」** (156 ページ)にあります。

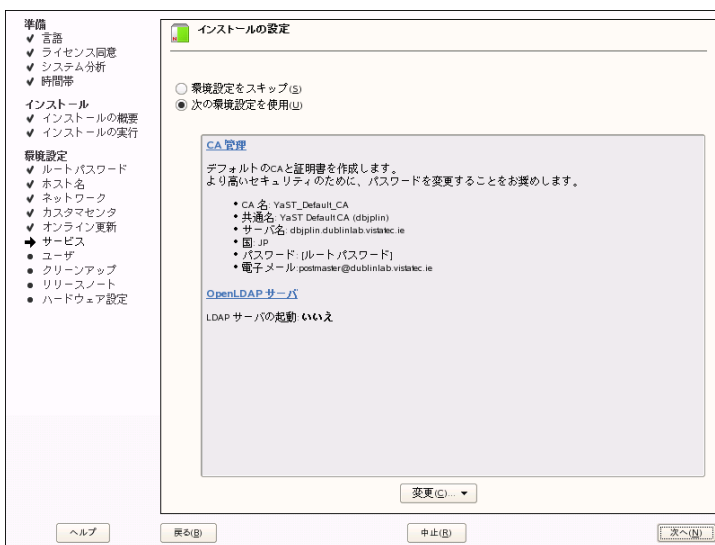
重要項目: ソフトウェアアップデートのダウンロード

アップデートのダウンロードには、インターネット接続の帯域幅とアップデートファイルのサイズによっては長時間かかります。パッチシステム自身が更新された場合、オンラインアップデートが再起動し、再起動後にその他のパッチがダウンロードされます。カーネルが更新された場合、設定の完了前にシステムが再起動します。

3.14.6 ネットワークサービス

ネットワークを設定するとダイアログが開き、認証局とOpenLDAPサーバという2つの重要なネットワークサービスを有効にして設定できます。必要に応じて、この設定推奨値をスキップすることができます。インストールの完了後は、YaSTを利用して、同じサービスを設定、開始することができます。

図 3.6 ネットワークサービスとして推奨される設定



CA管理

CA (Certificate Authority)の目的は、相互の通信に使用するすべてのネットワークサービス間で、信頼関係を保証することです。CAがない場合、各サービス個別にSSLとTLSを使ってサーバ通信を保護することができます。デフォルトでは、CAが作成され、インストール中に有効になります。YaSTを使ったCAの作成方法の詳細は、[第42章 X.509証明書の管理](#) (875 ページ)を参照してください。

OpenLDAPサーバ

一連の設定ファイルの集中管理を可能にする機能を備えるため、ご使用のホストでLDAPサービスを実行することができます。LDAPサーバは、ユーザのアカウントデータ管理に用いるのが一般的ですが、SUSE Linux Enterpriseと組み合わせることにより、電子メール、DHCP、DNS関連データに対しても使用することができます。LDAP、およびYaSTを使ったLDAPの設定については、[第36章 LDAP—ディレクトリサービス](#) (725 ページ)を参照してください。

ティップ: サーバ設定のデフォルト値へのリセット

デフォルト値にリセットするには、`[変更] > [デフォルトにリセット]`の順にクリックします。この操作により、変更内容が破棄されます。

3.14.7 Users

インストールの前のステップでネットワークアクセスが正常に設定された場合、複数のユーザ管理オプションを選択できます。ネットワーク接続が設定されていない場合は、ローカルユーザアカウントを作成します。ユーザ管理の詳細については、[8.9.1項「ユーザ管理」](#) (193 ページ)SUSE Linux Enterprise Serverのマニュアルを参照してください。

ローカル(/etc/passwd)

ユーザはインストールされたホストで、ローカルで管理されます。これはスタンドアロンのワークステーションに向いています。ユーザのデータは、ローカルファイルの/etc/passwdで管理されます。このファイルに入力されているすべてのユーザは、ネットワークが使用不能であってもシステムにログインすることができます。

YaSTが古いバージョンのSUSE Linux Enterprise、または/etc/passwdを使用する他のシステムを検出した場合、ローカルユーザをインポートすることができます。インポートする場合は、*[Read User Data from a Previous Installation]* を選択して、*[選択]* をクリックします。次のダイアログでは、インポートするユーザを選択して、*[OK]* をクリックします。

LDAP

ユーザはネットワーク上のすべてのシステムに対し、1台のLDAPサーバ上で集中的に管理されます。詳細は、[36.6項「YaSTを使ったLDAPクライアントの設定」](#) (747 ページ)にあります。

NIS

ユーザはネットワーク上のすべてのシステムに対し、1台のNISサーバ上で集中的に管理されます。詳細については、[35.2項「NISクライアントの設定」](#) (722 ページ)を参照してください。

Windowsドメイン

SMB認証は、通常、LinuxとWindowsが混在するネットワークで使用されます。詳細情報は、[37.6項「Active Directoryネットワーク内のSambaサーバ」](#) (773 ページ)から入手できます。

注意: 認証メニューの内容

カスタムパッケージ選択を使用し、認証方法がメニューに表示されない認証方法がある場合は、必要なパッケージがインストールされていない可能性があります。

選択したユーザ管理方法と一緒に、Kerberos認証を使用することができます。Active DirectoryドメインにSUSE Linux Enterpriseを統合する場合は、これが必須になります。37.6項「[Active Directoryネットワーク内のSambaサーバ](#)」(773 ページ)を参照してください。Kerberos認証を使用するには、*[Set Up Kerberos Authentication]* を選択します。

3.14.8 リリースノート

ユーザ認証のセットアップを完了した後、YaSTはリリースノートを表示します。リリースノートには、マニュアルの印刷時には利用できなかった、最新の重要情報が含まれているため確認するようにしてください。インターネット接続した場合は、SUSE Linux Enterpriseのサーバから取得した最新のリリースノートが利用できます。インストール後にリリース ノートを表示するには、*[その他]* > *[リリースノート]* の順にクリックします。

3.14.9 ハードウェア設定

インストールの最後に、システムに取り付けられているグラフィックカードや、他のハードウェアコンポーネントを設定するためのダイアログが表示されます。個別のコンポーネントをクリックすると、ハードウェア設定が開始されます。多くの場合、デバイスはYaSTにより、自動的に検出され、設定されます。

ティップ: IBM System z:ハードウェア設定

IBM System zには、XFreeがサポートしているディスプレイはありません。したがって、これらのシステムでは、*[グラフィックカード]* エントリは検出されません。

すべての周辺デバイスの設定を省略し、後で設定することもできます。**8.4項「ハードウェア」** (163 ページ)を参照してください。設定を行わない場合は、**[設定をスキップする]** を選択して **[次へ]** をクリックします。

ただし、グラフィックカードの設定は、直ちに行うのが妥当です。YaSTが自動設定したディスプレイの設定は、通常、適用して問題ありません。ただし、解像度、色深度、その他のグラフィック機能の設定については好みが変わる点でもあるため、設定はユーザごとにまったく異なることがあります。これらの設定を変更するには、それぞれの項目を選択して、値を設定してください。新しい設定をテストするには、**[Test the Configuration]** をクリックします。

ティップ: ハードウェア設定のデフォルト値へのリセット

変更内容をキャンセルするには、**[変更]** > **[デフォルトにリセット]** の順にクリックします。YaSTに、元の推奨値が表示されます。

3.14.10 インストールの完了

インストールが完了したら、**[Installation Completed]** ダイアログが表示されます。このダイアログでは、新しくインストールしたシステムを、AutoYaST用に複製するかどうかを選択します。このためには、**[このシステムをAutoYaST用に複製する]** を選択します。現在のシステムのプロファイルが、`/root/autoyast.xml` に格納されます。デフォルトでは、クローンが選択されています。

AutoYaSTは、ユーザによる介入をなくして、SUSE Linux Enterpriseシステムを自動的にインストールする場合に使用します。AutoYaSTインストールを行うには、インストールおよび環境設定データを記述した制御ファイルを使用します。詳細については、**第5章 自動インストール** (95 ページ)を参照してください。最後のダイアログで **[完了]** をクリックして、SUSE Linux Enterpriseのインストールを完了してください。

3.15 グラフィカルログイン

ティップ: IBM System z:グラフィカルログインはありません

IBM System zプラットフォームでは、使用可能なグラフィカルログインはありません。

SUSE Linux Enterpriseがインストールされ、設定されました。自動ログイン機能を有効にするか、デフォルトのランレベルを変更していない限り、グラフィカルログイン画面が表示されます。この画面から、ユーザ名とパスワードを入力してシステムにログインすることができます。自動ログインを有効にした場合は、デスクトップが自動的に起動します。

リモートインストール

SUSE Linux Enterpriseは、さまざまな方法でインストールできます。SUSE Linux Enterpriseをインストールするには、[第3章 YaSTによるインストール](#) (21 ページ)で説明されている通常のメディアによるインストールの他に、ネットワークベースのさまざまなアプローチや、完全自動のアプローチも選択できます。

それぞれの方法は、前提条件を記載したリストと、基本手順を記載したリストの2つのチェックリストを使用します。その後、これらのインストールシナリオの中で用いられているすべての方式についての詳細を説明します。

注意

次の各項では、SUSE Linux Enterpriseを新たにインストールするシステムのことを「ターゲットシステム」または「インストールターゲット」と呼びます。インストールソースという語は、インストールデータのすべてのソースを指して用います。これには、CDやDVDなどの物理メディアや、ネットワーク内でインストールデータを配布するネットワークサーバが含まれます。

4.1 リモートインストールのインストールシナリオ

このセクションでは、リモートインストールを行う場合の、最も一般的なインストールシナリオについて説明します。それぞれのシナリオについて、前

提条件のリストを注意深くチェックし、シナリオで説明されている手順に従ってください。特定のステップについての詳細な説明が必要な場合には、用意されているリンクを参照してください。

重要項目

X Window Systemの設定は、リモートインストールプロセスの一部ではありません。インストールが完了したら、ターゲットシステムにrootとしてログインして、telinit 3を入力し、SaX2を起動してグラフィックハードウェアを設定してください。

4.1.1 VNC経由のシンプルリモートインストール—静的なネットワーク設定

このタイプのインストールでは、インストール時のブートのため、ターゲットシステムにある程度物理的にアクセスすることが必要となります。インストール自体は、VNCを使用してインストールプログラムに接続することにより、リモートのワークステーションによって完全に制御されます。[第3章 YaSTによるインストール](#) (21 ページ)で説明されている手動インストールの場合と同様に、ユーザ操作も必要です。

このタイプのインストールでは、以下の必要条件を満たしていることを確認してください。

- リモートインストールソース:NFS、HTTP、FTP、またはSMBと作業用ネットワーク接続
- ターゲットシステムでネットワーク接続が動作していること
- 動作しているネットワーク接続による制御システムおよびVNCビューアソフトウェアまたはJava対応のブラウザ(Firefox、Konqueror、Internet Explorer、またはOpera)
- ターゲットシステムのブートのための物理ブートメディア(CD、またはDVD)
- インストールソースおよび制御システムに有効な静的IPアドレスがすでに割り当てられていること

- ターゲットシステムに割り当てる有効な静的IPアドレス

このタイプのインストールを実行するには、以下の手順に従います。

- 1 **4.2項「インストールソースを保持するサーバのセットアップ」** (63 ページ)で説明されている方法でインストールソースをセットアップします。NFS、HTTP、またはFTPのネットワークサーバを選択します。SMBのインストールソースの場合は、**4.2.5項「SMBインストールソースの管理」** (72 ページ)を参照してください。
- 2 SUSE Linux Enterprise メディアキットの最初のCDまたはDVDを使って、ターゲットシステムをブートします。
- 3 ターゲットシステムのブート画面が表示されたら、ブートオプションプロンプトで、適切なVNCオプションと、インストールソースのアドレスを設定します。この詳細は、**4.4項「ターゲットシステムをインストールのためにブートする」** (85 ページ)で説明しています。

ターゲットシステムはテキストベースの環境でブートします。VNCビューアアプリケーションまたはブラウザで使用するための、グラフィックインストール環境用のネットワークアドレスとディスプレイ番号が表示されます。VNCインストールのアナウンス自体はOpenSLPによって行われ、Konquerorのservice:/またはslp:/モードで表示できます。
- 4 制御用のワークステーションで、VNC表示アプリケーションまたはWebブラウザを開き、**4.5.1項「VNCによるインストール」** (91 ページ)に説明されている方法でターゲットシステムに接続します。
- 5 **第3章 YaSTによるインストール** (21 ページ)に説明されている方法でインストールを実行します。再起動後、ターゲットシステムに再接続して、インストールの最終作業を行います。
- 6 インストールを完了します。

4.1.2 VNC経由のシンプルリモートインストール—動的なネットワーク設定

このタイプのインストールでは、インストール時のブートのため、ターゲットシステムにある程度物理的にアクセスすることが必要となります。ネット

ワーク設定はDHCPによって行われます。インストール自体は、VNCを使用してインストーラに接続することにより、リモートのワークステーションによって完全に制御されます。しかし、実際の設定のためにユーザ操作も必要です。

このタイプのインストールでは、以下の必要条件を満たしていることを確認してください。

- リモートインストールソース:NFS、HTTP、FTP、またはSMBと作業用ネットワーク接続
- ターゲットシステムでネットワーク接続が動作していること
- 動作しているネットワーク接続による制御システムおよびVNCビューアソフトウェアまたはJava対応のブラウザ(Firefox、Konqueror、Internet Explorer、またはOpera)
- ターゲットシステムのブートのための物理ブートメディア(CD、DVD、またはカスタムのブートディスク)
- IPアドレスを提供するDHCPサーバが動作していること

このタイプのインストールを実行するには、以下の手順に従います。

- 1 **4.2項「インストールソースを保持するサーバのセットアップ」** (63 ページ)で説明されている方法でインストールソースをセットアップします。NFS、HTTP、またはFTPのネットワークサーバを選択します。SMBのインストールソースの場合は、**4.2.5項「SMBインストールソースの管理」** (72 ページ)を参照してください。
- 2 SUSE Linux Enterprise メディアキットの最初のCDまたはDVDを使って、ターゲットシステムをブートします。
- 3 ターゲットシステムのブート画面が表示されたら、ブートオプションプロンプトで、適切なVNCオプションと、インストールソースのアドレスを設定します。この詳細は、**4.4項「ターゲットシステムをインストールのためにブートする」** (85 ページ)で説明しています。

ターゲットシステムはテキストベースの環境でブートします。VNCビューアアプリケーションまたはブラウザで使用するための、グラフィックインストール環境用のネットワークアドレスとディスプレイ番号が表示さ

れます。VNCインストールのアナウンス自体はOpenSLPによって行われ、Konquerorのservice:/またはslp:/モードで表示できます。

- 4 制御用のワークステーションで、VNC表示アプリケーションまたはWebブラウザを開き、4.5.1項「VNCによるインストール」(91 ページ)に説明されている方法でターゲットシステムに接続します。
- 5 第3章 *YaST*によるインストール(21 ページ)に説明されている方法でインストールを実行します。再起動後、ターゲットシステムに再接続して、インストールの最終作業を行います。
- 6 インストールを完了します。

4.1.3 VNC経由のリモートインストール—PXEブートとWake on LAN

このタイプのインストールは、完全に無人で行えます。ターゲットマシンは、リモートで起動され、ブートされます。ユーザ操作は、実際のインストールで必要となるだけです。このアプローチは、遠隔サイト間での導入に適しています。

このタイプのインストールでは、以下の必要条件を満たしていることを確認してください。

- リモートインストールソース:NFS、HTTP、FTP、またはSMBと作業用ネットワーク接続
- TFTPサーバ
- ネットワークでDHCPサーバが動作していること
- ターゲットシステムにPXEブート、ネットワーク、およびWake on LANの機能があり、ネットワークに配線されて接続していること
- 動作しているネットワーク接続による制御システムおよびVNCビューアソフトウェアまたはJava対応のブラウザ(Firefox、Konqueror、Internet Explorer、またはOpera)

このタイプのインストールを実行するには、以下の手順に従います。

- 1 4.2項「インストールソースを保持するサーバのセットアップ」(63 ページ)で説明されている方法でインストールソースをセットアップします。NFS、HTTP、またはFTPのネットワークサーバを選択するか、4.2.5項「SMBインストールソースの管理」(72 ページ)で説明されている方法でSMBのインストールソースを設定します。
- 2 ターゲットシステムから取得するためのブートイメージを保持するTFTPサーバをセットアップします。これは4.3.2項「TFTPサーバのセットアップ」(76 ページ)で説明されています。
- 3 すべてのマシンにIPアドレスを提供し、ターゲットシステムにTFTPサーバの場所を知らせるためのDHCPサーバをセットアップします。これは4.3.1項「DHCPサーバのセットアップ」(74 ページ)で説明されています。
- 4 ターゲットシステムでPXEブートの準備をします。この詳細は、4.3.5項「ターゲットシステムでPXEブートの準備をする」(83 ページ)で説明しています。
- 5 Wake on LAN機能を使って、ターゲットシステムでブートプロセスを開始します。これは4.3.7項「Wake on LAN」(84 ページ)で説明されています。
- 6 制御用のワークステーションで、VNC表示アプリケーションまたはWebブラウザを開き、4.5.1項「VNCによるインストール」(91 ページ)に説明されている方法でターゲットシステムに接続します。
- 7 第3章 *YaST*によるインストール(21 ページ)に説明されている方法でインストールを実行します。再起動後、ターゲットシステムに再接続して、インストールの最終作業を行います。
- 8 インストールを完了します。

4.1.4 SSH経由のシンプルリモートインストール—静的なネットワーク設定

このタイプのインストールでは、インストール時のブートと、インストールターゲットのIPアドレスの決定のため、ターゲットシステムにある程度物理的にアクセスすることが必要となります。インストール自体は、SSHを使用

してインストーラに接続することにより、リモートのワークステーションによって完全に制御されます。[第3章 YaSTによるインストール](#) (21 ページ)で説明されている通常のインストールの場合と同様に、ユーザ操作も必要です。

このタイプのインストールでは、以下の必要条件を満たしていることを確認してください。

- リモートインストールソース:NFS、HTTP、FTP、またはSMBと作業用ネットワーク接続
- ターゲットシステムでネットワーク接続が動作していること
- ネットワーク接続が動作しており、現在使用中のSSHクライアントソフトウェアがある制御システム
- ターゲットシステムのブートのための物理ブートメディア(CD、DVD、またはカスタムのブートディスク)
- インストールソースおよび制御システムに有効な静的IPアドレスがすでに割り当てられていること
- ターゲットシステムに割り当てる有効な静的IPアドレス

このタイプのインストールを実行するには、以下の手順に従います。

- 1 [4.2項 「インストールソースを保持するサーバのセットアップ」](#) (63 ページ)で説明されている方法でインストールソースをセットアップします。NFS、HTTP、またはFTPのネットワークサーバを選択します。SMBのインストールソースの場合は、[4.2.5項 「SMBインストールソースの管理」](#) (72 ページ)を参照してください。
- 2 SUSE Linux Enterprise メディアキットの最初のCDまたはDVDを使って、ターゲットシステムをブートします。
- 3 ターゲットシステムのブート画面が表示されたら、ブートオプションプロンプトで、ネットワーク接続、インストールソースのアドレス、SSHの有効化のための適切なパラメータを設定します。この詳細は、[4.4.3項 「カスタムのブートオプションを使用する」](#) (87 ページ)で説明しています。

ターゲットシステムはテキストベースの環境でブートします。SSHクライアントで使用するための、グラフィックインストール環境用のネットワークアドレスが表示されます。

- 4 制御用のワークステーションで、ターミナルウィンドウを開いて、**インストールプログラムへの接続項**(93ページ)で説明されている方法でターゲットシステムに接続します。
- 5 **第3章 YaSTによるインストール**(21ページ)に説明されている方法でインストールを実行します。再起動後、ターゲットシステムに再接続して、インストールの最終作業を行います。
- 6 インストールを完了します。

4.1.5 SSH経由のシンプルリモートインストール—動的なネットワーク設定

このタイプのインストールでは、インストール時のブートと、インストールターゲットのIPアドレスの決定のため、ターゲットシステムにある程度物理的にアクセスすることが必要となります。インストール自体は、VNCを使用してインストーラに接続することにより、リモートのワークステーションによって完全に制御されます。しかし、実際の設定のためにユーザ操作も必要です。

このタイプのインストールでは、以下の必要条件を満たしていることを確認してください。

- リモートインストールソース:NFS、HTTP、FTP、またはSMBと作業用ネットワーク接続
- ターゲットシステムでネットワーク接続が動作していること
- ネットワーク接続が動作しており、現在使用中のSSHクライアントソフトウェアがある制御システム
- ターゲットシステムのブートのための物理ブートメディア(CD、またはDVD)
- IPアドレスを提供するDHCPサーバが動作していること

このタイプのインストールを実行するには、以下の手順に従います。

- 1 **4.2項「インストールソースを保持するサーバのセットアップ」** (63 ページ)で説明されている方法でインストールソースをセットアップします。NFS、HTTP、またはFTPのネットワークサーバを選択します。SMBのインストールソースの場合は、**4.2.5項「SMBインストールソースの管理」** (72 ページ)を参照してください。
- 2 SUSE Linux Enterprise メディアキットの最初のCDまたはDVDを使って、ターゲットシステムをブートします。
- 3 ターゲットシステムのブート画面が表示されたら、ブートオプションプロンプトで、ネットワーク接続、インストールソースの場所、SSHの有効化のための適切なパラメータを設定します。これらのパラメータの使用方法についての詳細は、**4.4.3項「カスタムのブートオプションを使用する」** (87 ページ)を参照してください。

ターゲットシステムはテキストベースの環境でブートします。SSHクライアントで使用するための、グラフィックインストール環境用のネットワークアドレスが表示されます。
- 4 制御用のワークステーションで、ターミナルウィンドウを開いて、**インストールプログラムへの接続項** (93 ページ)で説明されている方法でターゲットシステムに接続します。
- 5 **第3章 YaSTによるインストール** (21 ページ)に説明されている方法でインストールを実行します。再起動後、ターゲットシステムに再接続して、インストールの最終作業を行います。
- 6 インストールを完了します。

4.1.6 SSH経由のリモートインストール—PXEブートとWake on LAN

このタイプのインストールは、完全に無人で行えます。ターゲットマシンは、リモートで起動され、ブートされます。

このタイプのインストールでは、以下の必要条件を満たしていることを確認してください。

- リモートインストールソース:NFS、HTTP、FTP、またはSMBと作業用ネットワーク接続
- TFTPサーバ
- インストールを行うホストにIPアドレスを提供する、DHCPサーバがネットワークで動作していること
- ターゲットシステムにPXEブート、ネットワーク、およびWake on LANの機能があり、ネットワークに配線されて接続していること
- ネットワーク接続が動作しており、SSHクライアントソフトウェアがある、制御システム

このタイプのインストールを実行するには、以下の手順に従います。

- 1 **4.2項「インストールソースを保持するサーバのセットアップ」** (63 ページ)で説明されている方法でインストールソースをセットアップします。NFS、HTTP、またはFTPのネットワークサーバを選択します。SMBのインストールソースの設定は、**4.2.5項「SMBインストールソースの管理」** (72 ページ)を参照してください。
- 2 ターゲットシステムから取得するためのブートイメージを保持するTFTPサーバをセットアップします。これは**4.3.2項「TFTPサーバのセットアップ」** (76 ページ)で説明されています。
- 3 すべてのマシンにIPアドレスを提供し、ターゲットシステムにTFTPサーバの場所を知らせるためのDHCPサーバをセットアップします。これは**4.3.1項「DHCPサーバのセットアップ」** (74 ページ)で説明されています。
- 4 ターゲットシステムでPXEブートの準備をします。この詳細は、**4.3.5項「ターゲットシステムでPXEブートの準備をする」** (83 ページ)で説明しています。
- 5 Wake on LAN機能を使って、ターゲットシステムでブートプロセスを開始します。これは**4.3.7項「Wake on LAN」** (84 ページ)で説明されています。

- 6 制御用のワークステーションで、SSHクライアントを起動して、[4.5.2項「SSHによるインストール」](#) (93 ページ)で説明されている方法でターゲットシステムに接続します。
- 7 [第3章 YaSTによるインストール](#) (21 ページ)に説明されている方法でインストールを実行します。再起動後、ターゲットシステムに再接続して、インストールの最終作業を行います。
- 8 インストールを完了します。

4.2 インストールソースを保持するサーバのセットアップ

SUSE Linux Enterprise用のネットワークインストールソースとして使用するコンピュータで動作しているオペレーティングシステムに応じて、サーバ設定のためのいくつかのオプションがあります。インストールサーバをセットアップする最も簡単な方法は、SUSE Linux Enterprise Server 9、10、またはSUSE Linux 9.3以降でYaSTを使うことです。他のバージョンのSUSE Linux Enterprise ServerまたはSUSE Linux Enterpriseでは、インストールソースを手動でセットアップしてください。

ティップ

Linuxの導入のために、Microsoft Windowsマシンをインストールサーバとして用いることもできます。詳細については、[4.2.5項「SMBインストールソースの管理」](#) (72 ページ)を参照してください。

4.2.1 YaSTを使ったインストールサーバのセットアップ

YaSTは、ネットワークインストールソースを作成するためのグラフィカルなツールを提供しています。HTTP、FTP、およびNFSネットワークインストールサーバをサポートしています。

- 1 インストールサーバにするコンピュータにrootとしてログインします。

- 2 [YaST] > [その他] > [インストールサーバ] の順に選択します。
- 3 サーバのタイプを選択します(HTTP、FTP、またはNFS)選択したサーバサービスは、システムの起動時ごとに自動的に開始されます。選択したタイプのサービスがシステム上ですでに動作していて、サーバ用に手動で設定する場合には、*[Do Not Configure Any Network Services]* をオンにして、サーバサービスの自動設定を無効にします。どちらの場合でも、サーバ上のインストールデータを保管するディレクトリを設定してください。
- 4 必要なサーバタイプを設定します。このステップは、サーバサービスの自動設定と関係しています。自動設定を無効にした場合にはスキップされます。

インストールデータを置くFTPまたはHTTPサーバのルートディレクトリのエイリアスを定義してください。後ほど、インストールソースは `ftp://Server-IP/Alias/Name` (FTP)、または `http://Server-IP/Alias/Name` (HTTP) に置かれます。Nameはインストールソースの名前を表すもので、次のステップで定義します。前のステップでNFSを選択した場合には、ワイルドカードとエクスポートオプションを指定します。NFSサーバは、`nfs://Server-IP/Name` でアクセスできます。

ティップ: ファイアウォールの設定

サーバシステムのファイアウォール設定が、HTTP、NFS、およびFTPポートのトラフィックを許可していることを確認します。これらのポートのトラフィックが禁止されている場合は、YaSTファイアウォールモジュールを起動して、該当するポートを開きます。

- 5 インストールソースを設定します。インストール用メディアをコピーする前に、インストールソースの名前を定義します(容易に覚えられる、製品とバージョンの略が望ましいでしょう)。YaSTでは、インストールCDのコピーの代わりに、メディアのISOイメージを使うことができます。そうする場合には、対応するチェックボックスをオンにして、ISOファイルをローカルに保管するディレクトリのパスを指定します。このインストールサーバを使って配布する製品によっては、他のアドオンCDやサービスパックCDが必要なこともあります。このような場合は、他のインストールソースとして追加する必要があります。ネットワーク内

のインストールサーバについて知らせるためにOpenSLPを使う場合には、適切なオプションをオンにします。

ティップ

ネットワークセットアップでサポートされている場合には、OpenSLPを使ってインストールソースを知らせることを考慮してみてください。そうすれば、すべてのターゲットマシンでネットワークインストールパスを入力しなくてもよくなります。SLPブートオプションでブートされたターゲットシステムは、他の設定を行わなくても、ネットワークインストールソースを見つけます。このオプションについての詳細は、[4.4項「ターゲットシステムをインストールのためにブートする」](#) (85 ページ)を参照してください。

- 6 インストールデータをアップロードします。インストールサーバの設定で最も時間がかかるステップは、実際のインストールCDのコピーです。メディアをYaSTが要求する順序に挿入し、コピーの手順が終わるまで待ってください。ソースのコピーがすべて完了したら、既存の情報ソースの概要に戻り、[\[完了\]](#)を選択して設定を閉じます。

インストールサーバは完全に設定されて、使用する準備ができました。これはシステムが起動するたびに、自動的に開始します。それ以上の操作は必要ありません。必要なのは、YaSTの最初のステップで選択したネットワークサービスの自動設定を無効にしていた場合に、サービスを手動で正しく設定し、開始することだけです。

インストールソースを無効にするには、該当するインストールソースを選択して、[\[削除\]](#)を選択します。システムからインストールデータが削除されます。ネットワークサービスを削除する場合は、適切なYaSTモジュールを使用します。

インストールサーバから複数の製品バージョンの製品のインストールデータを提供する場合には、YaSTのインストールサーバモジュールを起動し、既存のインストールソースの概要で [\[追加\]](#) を選択して、新しいインストールソースを設定します。

4.2.2 NFSインストールソースの手動セットアップ

インストール用のNFSソースのセットアップは、基本的に2つのステップで行えます。最初のステップでは、インストールデータを保持するディレクトリ構造を作成して、インストールメディアをその構造にコピーします。2番目のステップでは、インストールデータを保持しているディレクトリをネットワークにエクスポートします。

インストールデータを保持するディレクトリを作成するには、以下の手順に従います。

- 1 rootとしてログインします。
- 2 後ほどインストールデータを保持するディレクトリを作成し、このディレクトリに移動します。たとえば、次のようにします。

```
mkdir install/product/productversion  
cd install/product/productversion
```

*product*は製品名の略語、*productversion*は製品名とバージョンを含む文字列で置き換えます。

- 3 メディアキットに含まれているCDごとに、以下のコマンドを実行します。

- 3a** インストールCDの内容全体を、インストールサーバのディレクトリにコピーします。

```
cp -a /media/path_to_your_CD-ROM_drive .
```

*path_to_your_CD-ROM_drive*は、CDまたはDVDドライブを指定するための実際のパスで置き換えてください。これは、使用しているシステムのドライブのタイプに応じて、*cdrom*、*cdrecorder*、*dvd*、または*dvdrecorder*になります。

- 3b** ディレクトリの名前をCDの番号に合わせて変更します。

```
mv path_to_your_CD-ROM_drive CDx
```

*x*は、CDの実際の番号で置き換えてください。

SUSE Linux Enterprise Serverでは、YaSTを使ってNFS経由でインストールソースをエクスポートできます。次の手順に従います。

- 1 rootとしてログインします。
- 2 `[YaST] > [ネットワークサービス] > [NFSサーバ]` の順に選択します。
- 3 `[開始]` および `[ファイアウォール内でポートを開く]` をオンにして、`[次へ]`をクリックします。
- 4 `[Add Directory]` を選択して、インストールソースのあるディレクトリ(この場合、`[productversion]`)に移動します。
- 5 `[Add Host]` をクリックして、インストールデータのエクスポート先になるコンピュータのホスト名を入力します。ここでホスト名を指定する代わりに、ワイルドカード、ネットワークアドレス、または単にネットワークのドメイン名を使用することもできます。適切なエクスポートオプションを入力するか、デフォルトのままにします。デフォルトでもほとんどのセットアップでは正しく動作します。NFS共有のエクスポートで私用される構文の詳細についてはexportsの「man」ページを参照してください。
- 6 `[完了]` をクリックします。SUSE Linux Enterpriseのインストールソースを保持しているNFSサーバは、自動的に起動し、ブートプロセスに統合されます。

YaSTのNFSサーバモジュールを使うかわりに、NFSを使用してインストールソースを手動でエクスポートする場合には、次の手順に従います。

- 1 rootとしてログインします。
- 2 `/etc/exports` ファイルを開いて、次の行を入力します。

```
/productversion *(ro,root_squash, sync)
```

これにより、ディレクトリ`/productversion`は、ネットワークに属している任意のホスト、またはこのサーバに接続している任意のホストにエクスポートされます。このサーバへのアクセスを制限するには、一般的なワイルドカード`*`の代わりにネットマスクまたはドメイン名を使用

してください。詳細は、`export`の`man`ページを参照してください。設定ファイルを保存して終了します。

- 3 NFSサービスを、システムブート時に起動するサーバのリストに追加するには、次のコマンドを実行します。

```
insserv /etc/init.d/nfsserver
insserv /etc/init.d/portmap
```

- 4 `rcnfsserver start`を実行してNFSサーバを開始します。後ほど、NFSサーバの設定を変更することが必要になった場合には、設定ファイルを修正して、`rcnfsserver restart`コマンドでNFSデーモンを再起動してください。

OpenSLPを使用してNFSサーバについてアナウンスし、ネットワーク内のすべてのクライアントにそのアドレスを知らせます。

- 1 `root`としてログインします。
- 2 `/etc/slp.reg.d/`ディレクトリに入ります。
- 3 以下の行を含む、`install.suse.nfs.reg`という名前の設定ファイルを作成します。

```
# Register the NFS Installation Server
service:install.suse:nfs://$HOSTNAME/path_to_instsource/CD1,en,65535
description=NFS Installation Source
```

`path_to_instsource`は、サーバ上のインストールソースの、実際のパスで置き換えます。

- 4 この設定ファイルを保存して、`rcslpd start`コマンドでOpenSLPデーモンを起動します。

OpenSLPについての詳細は、`/usr/share/doc/packages/openslp/`のパッケージのドキュメント、または第31章 ネットワーク上のSLPサービス(663ページ)を参照してください。

4.2.3 FTPインストールソースの手動セットアップ

FTPインストールソースの作成は、NFSインストールソースの場合と非常によく似ています。FTPインストールソースも、OpenSLPを使用してネットワーク上にアナウンスすることができます。

- 1 **4.2.2項「NFSインストールソースの手動セットアップ」** (66 ページ)で説明されているように、インストールソースを保持するディレクトリを作成します。

- 2 インストールディレクトリの内容を配布するためのFTPサーバを設定します。

2a rootとしてログインし、YaSTパッケージマネージャを使ってパッケージvsftpdをインストールします。

- 2b** FTPサーバのルートディレクトリに入ります。

```
cd /srv/ftp
```

- 2c** FTPのルートディレクトリに、インストールソースを保持するサブディレクトリを作成します。

```
mkdir instsource
```

*instsource*は製品名で置き換えてください。

- 2d** 既存のインストールリポジトリの内容を、FTPサーバのルート環境にマウントします。

```
mount --bind path_to_instsource /srv/ftp/instsource
```

*path_to_instsource*と*instsource*は、セットアップに適した値で置き換えてください。この変更を永続的にする場合には、*/etc/fstab*に追加します。

- 2e** vsftpdと入力して、vsftpdを開始します。

- 3** ネットワークのセットアップでサポートされている場合には、インストールソースをOpenSLPでアナウンスします。

- 3a** 以下の行を含むinstall.suse.ftp.regという名前の設定ファイルを、/etc/slp.reg.d/に作成します。

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/instsource/CD1,en,65535
description=FTP Installation Source
```

*instsource*は、サーバ上のインストールソースディレクトリの実際の名前で置き換えてください。service:の行は、連続した行として入力する必要があります。

- 3b** この設定ファイルを保存して、rcslpd startコマンドでOpenSLPデーモンを起動します。

4.2.4 HTTPインストールソースの手動セットアップ

HTTPインストールソースの作成は、NFSインストールソースの場合と非常によく似ています。HTTPインストールソースも、OpenSLPを使用してネットワーク上にアナウンスすることができます。

- 1** 4.2.2項「NFSインストールソースの手動セットアップ」(66 ページ)で説明されているように、インストールソースを保持するディレクトリを作成します。
- 2** インストールディレクトリの内容を配布するためのHTTPサーバを設定します。
 - 2a** 40.1.2項「インストール」(808 ページ)の説明に従って、WebサーバのApacheをインストールします。
 - 2b** HTTPサーバのルートディレクトリ(/srv/www/htdocs)に入り、インストールソースを保持するサブディレクトリを作成します。

```
mkdir instsource
```

*instsource*は製品名で置き換えてください。

- 2c** インストールソースの場所からWebサーバのルートディレクトリ(/srv/www/htdocs)への、シンボリックリンクを作成します。

```
ln -s /path_instsource /srv/www/htdocs/instsource
```

- 2d** HTTPサーバの設定ファイル(/etc/apache2/default-server.conf)を変更して、シンボリックリンクをたどるようにします。以下のように変更します。

```
Options None
```

方法

```
Options Indexes FollowSymLinks
```

- 2e** `rcapache2 reload`を使用してHTTPサーバ設定を再ロードします。

- 3** ネットワークのセットアップでサポートされている場合には、インストールソースをOpenSLPでアナウンスします。

- 3a** 以下の行を含む`install.suse.http.reg`という名前の設定ファイルを、`/etc/slp.reg.d/`に作成します。

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/instsource/CD1/,en,65535
description=HTTP Installation Source
```

*instsource*は、サーバ上のインストールソースの、実際のパスに置き換えます。`service:`の行は、連続した行として入力する必要があります。

- 3b** この設定ファイルを保存して、`rcslpd restart`コマンドでOpenSLPデーモンを起動します。

4.2.5 SMBインストールソースの管理

SMBを使用すれば、Linuxコンピュータがなくても、Microsoft Windowsサーバからインストールソースをインポートして、Linuxの導入を開始することができます。

SUSE Linux Enterpriseのインストールソースを保持する、エクスポートされたWindows Shareをセットアップするには、以下の手順に従います。

- 1 Windowsマシンにログインします。
- 2 エクスプローラを起動して、インストールツリー全体を保持する新しいフォルダを作成し、INSTALLのような名前を付けます。
- 3 この共有を、Windowsのドキュメントで説明されている方法に従ってエクスポートします。
- 4 この共有を入力し、「*product*」という名前のサブフォルダを作成します。*product*は、実際の製品名と置き換えます。
- 5 INSTALL/*product*フォルダで、各CDまたはDVDを個別のフォルダにコピーします(例:CD1およびCD2)。

SMBマウントの共有をインストールソースとして使用するには、次の手順に従います。

- 1 インストールターゲットをブートします。
- 2 [インストール] を選択します。
- 3 インストールソースの選択のために、F4キーを押します。
- 4 SMBを選択し、Windowsマシンの名前またはIPアドレス、共有名(この例ではINSTALL/*product*/CD1)、ユーザ名、パスワードを入力します。

<Enter>キーを押すと、YaSTが起動して、インストールを実行します。

4.2.6 サーバ上のインストールメディアのISOイメージの使用

サーバのディレクトリに手作業で物理メディアをコピーする代わりに、インストールサーバにインストールメディアのISOイメージをマウントして、それをインストールソースとして使用することもできます。メディアコピーの代わりに、ISOイメージを使用するHTTP、NFS、またはFTPサーバを設定するには、以下の手順に従ってください。

- 1 ISOイメージをダウンロードして、それをインストールサーバとして使用するコンピュータに保存します。
- 2 `root`としてログインします。
- 3 4.2.2項「NFSインストールソースの手動セットアップ」(66 ページ)、4.2.3項「FTPインストールソースの手動セットアップ」(69 ページ)、または4.2.4項「HTTPインストールソースの手動セットアップ」(70 ページ)の説明に従って、インストールデータの場所を選択、作成します。
- 4 各CDまたはDVD用のサブディレクトリを作成します。
- 5 各ISOイメージを最終的な場所にマウントし、パックを解除するには、次のコマンドを実行します。

```
mount -o loop path_to_iso path_to_instsource/product/mediumx
```

*path_to_iso*には、ISOイメージのローカルコピーへのパスを、*path_to_instsource*にはサーバのソースディレクトリを、*product*には製品名を、*mediumx*には使用メディアの種類(CDまたはDVD)と数を指定します。

- 6 前のステップを繰り返して、製品に必要なすべてのISOイメージをマウントします。
- 7 4.2.2項「NFSインストールソースの手動セットアップ」(66 ページ)、4.2.3項「FTPインストールソースの手動セットアップ」(69 ページ)、または4.2.4項「HTTPインストールソースの手動セットアップ」(70 ページ)の説明に従って、インストールサーバを開始します。

4.3 ターゲットシステムのブートの準備

このセクションでは、複雑なブートシナリオで必要となる設定タスクについて説明します。DHCP、PXEブート、TFTP、およびWake on LAN用の、すぐに使用できる設定例も含まれています。

4.3.1 DHCPサーバのセットアップ

DHCPサーバを設定するには、2種類の方法があります。SUSE Linux Enterprise Server 9以降のYaSTには、操作に使用するGUIが用意されています。他のSUSE Linuxベースの製品のユーザ、およびSUSE Linux以外の製品のユーザは、設定ファイルを手動で編集するか、または該当するOSのベンダーが提供するフロントエンドを使用してください。

YaSTを使ったDHCPサーバのセットアップ

TFTPサーバの場所をネットワーククライアントにアナウンスし、インストールターゲットが使用するブートイメージファイルを指定するには、DHCPサーバの設定に2つの宣言を追加します。

- 1 DHCPサーバのホストとなるマシンにrootとしてログインします。
- 2 `[YaST] > [ネットワークサービス] > [DHCPサーバ]` の順に選択します。
- 3 基本的なDHCPサーバのセットアップウィザードを完了します。
- 4 `[エキスパート設定]` を選択し、起動ダイアログ終了の警告メッセージが表示されたら、`[はい]` を選択します。
- 5 `[設定済みの宣言]` ダイアログで、新しいシステムを配置するサブネットを選択して、`[編集]` をクリックします。
- 6 `[サブネットの設定]` ダイアログで、`[追加]` を選択して、サブネットの設定に新しいオプションを追加します。

- 7 filenameを選択して、値にpxelinux.0を入力します。
- 8 他のオプション(next-server)を追加して、TFTPサーバのアドレスを値に設定します。
- 9 **[OK]** をクリックした後、 **[完了]** を選択して、DHCPサーバの設定を完了します。

特定のホストに静的IPアドレスを提供するようにDHCPを設定するには、DHCPサーバ設定モジュールの **[エキスパート設定]** **ステップ 4** (74 ページ)から、ホストタイプの新たな宣言を追加します。このホスト宣言には、hardware およびfixed-addressオプションを追加して、適切な値を指定してください。

DHCPサーバの手動セットアップ

すべてのDHCPサーバが行う必要があるのは、ネットワーククライアントへのアドレスの自動割り当てのほかに、TFTPサーバ、およびターゲットマシンがインストールルーチンで取得するファイルのIPアドレスをアナウンスすることです。

- 1 DHCPサーバのホストとなるマシンにrootとしてログインします。
- 2 /etc/dhcpd.confというDHCPサーバの設定ファイルに、以下の行を追加します。

```
group {
    # PXE related stuff
    #
    # "next server" defines the tftp server that will be used
    next server ip_tftp_server:
    #
    # "filename" specifies the pxelinux image on the tftp server
    # the server runs in chroot under /srv/tftpboot
    filename "pxelinux.0";
}
```

ip_of_the_tftp_serverは、TFTPサーバの実際のIPアドレスで置き換えてください。dhcpd.confで利用可能なオプションの詳細については、dhcpd.confのmanページを参照してください。

- 3 rcdhcpd restartを実行して、DHCPサーバをリスタートします。

PXEおよびWake on LANインストールのリモート制御にSSHを使う場合には、DHCPがインストールターゲットに提供するIPアドレスを明示的に指定してください。IPアドレスを明示的に指定するには、上記のDHCP設定を次の例に従って変更します。

```
group {
    # PXE related stuff
    #
    # "next server" defines the tftp server that will be used
    next server ip_tftp_server:
    #
    # "filename" specifies the pxelinux image on the tftp server
    # the server runs in chroot under /srv/tftpboot
    filename "pxelinux.0";
    host test { hardware ethernet mac_address;
                fixed-address some_ip_address; }
}
```

host文は、インストールターゲットのホスト名になります。ホスト名とIPアドレスを特定のホストにバインドするには、そのシステムのハードウェア(MAC)アドレスを調べ、これを指定する必要があります。この例で使用されているすべての変数を、使用する環境にマッチする実際の値で置き換えてください。

DHCPサーバをリスタートすると、サーバは指定されたホストに静的なIPを提供するので、そのシステムにSSHで接続することが可能になります。

4.3.2 TFTPサーバのセットアップ

SUSE Linux Enterprise ServerおよびSUSE Linux EnterpriseでYaSTを使用するか、またはxinetdとtftpをサポートしているLinuxオペレーティングシステム上で、手動でTFTPサーバを設定します。TFTPサーバは、ターゲットシステムがブートして要求を送ったときに、ブートイメージを提供します。

YaSTによるTFTPサーバのセットアップ

- 1 rootとしてログインします。
- 2 `[YaST] > [ネットワークサービス] > [TFTPサーバ]` の順に選択して、要求されたパッケージをインストールします。

- 3 [有効にする] をクリックして、サーバが起動し、ブートルーチンに含まれるようにします。この `xinetd` がブート時に `tftpd` を起動するようにするために必要なユーザ操作はありません。
- 4 [ファイアウォール内でポートを開く] をクリックして、マシンで動作しているファイアウォールで適切なポートを開きます。サーバでファイアウォールが動作していない場合には、このオプションは利用できません。
- 5 [参照] をクリックして、ブートイメージのディレクトリを参照します。デフォルトのディレクトリ `/tftpboot` が作成され、自動的に選択されます。
- 6 [完了] をクリックして、設定内容を適用し、サーバを起動します。

TFTPサーバの手動セットアップ

- 1 rootとしてログインして、`tftp` および `xinetd` パッケージをインストールします。
- 2 もしまだ存在していなければ、`/srv/tftpboot` および `/srv/tftpboot/pxelinux.cfg` ディレクトリを作成します。
- 3 4.3.3項「PXEブートの使用」(78 ページ)で説明されているように、ブートイメージに必要な、適切なファイルを追加します。
- 4 `/etc/xinetd.d/` にある `xinetd` の設定ファイルを変更して、ブート時に TFTPサーバが起動するようにします。
 - 4a もしまだ存在していなければ、`touch tftp` コマンドで、このディレクトリに `tftp` というファイルを作成します。それから `chmod 755 tftp` を実行します。
 - 4b `tftp` ファイルを開いて、次の行を入力します。

```
service tftp
{
    socket_type      = dgram
    protocol        = udp
    wait            = yes
    user            = root
```

```

server                = /usr/sbin/in.tftpd
server_args           = -s /srv/tftpboot
disable               = no
}

```

- 4c** このファイルを保存し、`rcxinetd restart`で`xinetd`をリスタートします。

4.3.3 PXEブートの使用

PXE (Preboot Execution Environment)の仕様書(<http://www.pix.net/software/pxeboot/archive/pxespec.pdf>)では、いくつかの技術的な背景情報と、PXEの完全な仕様について知ることができます。

- 1 インストールレポジトリのディレクトリに移動し、次のコマンドを入力して、`linux`、`initrd`、`message`、および`memtest`ファイルを`/srv/tftpboot`ディレクトリにコピーします。

```

cp -a boot/loader/linux boot/loader/initrd
    boot/loader/message boot/loader/memtest /srv/tftpboot

```

- 2 YaSTを使い、インストールCDまたはDVDから直接`syslinux`パッケージをインストールします。
- 3 次のコマンドを入力して、`/usr/share/syslinux/pxelinux.0`ファイルを`/srv/tftpboot`ディレクトリにコピーします。

```

cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot

```

- 4 インストールリポジトリにディレクトリに移動し、次のコマンドを入力して、`isolinux.cfg`ファイルを`/srv/tftpboot/pxelinux.cfg/default`にコピーします。

```

cp -a boot/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default

```

- 5 /srv/tftpboot/pxelinux.cfg/defaultファイルを編集して、
gfxboot、readinfo、およびframebufferで始まる行を削除します。
- 6 デフォルトのfailsafeおよびapicラベルのappend行に、以下のエントリを挿入します。

insmod=kernel module

このエントリを使って、PXEクライアントにネットワークインストールを行うために必要なネットワークカーネルモジュールを指定します。*kernel module*には、ネットワークデバイスの適切なモジュール名を指定してください。

netdevice=interface

このエントリは、ネットワークインストールで使用する、クライアントのネットワークインタフェースを定義します。これは、クライアントに複数のネットワークカードが装着されている場合にのみ必要です。適切に調整してください。ネットワークカードが1枚の場合には、このエントリは省略できます。

install=nfs://ip_instserver/path_instsource/CD1

このエントリは、NFSサーバとクライアントインストールのインストールソースを定義します。*ip_instserver*をインストールサーバの実際のIPアドレスと置き換えます。*path_instsource*は、インストールソースの実際のパスと置き換えます。HTTP、FTP、またはSMBソースも同様の仕方です。プロトコルのプレフィックスはhttp、ftp、またはsmbになります。

重要項目

SSHまたはVNCブートパラメータなどの、他のブートオプションをインストールルーチンに渡す必要がある場合には、それらをinstallエントリに追加します。パラメータの概要といくつかの例は、[4.4頁「ターゲットシステムをインストールのためにブートする」](#) (85 ページ)を参照してください。

/srv/tftpboot/pxelinux.cfg/defaultファイルの例は、次のようなものです。インストールソースのプロトコルプレフィックスは、ネットワークのセットアップにマッチするように調整してください。そして、使用する接続方法を指定するために、installエントリにvncと

vncpasswordまたはusesshとsshpaswordオプションを追加してください。\\で区切られている行は、改行や\\なしに、連続する1行として入力する必要があります。

```
default linux

# default
label linux
    kernel linux
        append initrd=initrd ramdisk_size=65536 insmod=e100 \
            install=nfs://ip_instserver/path_instsource/product/CD1

# failsafe
label failsafe
    kernel linux
        append initrd=initrd ramdisk_size=65536 ide=nodma apm=off acpi=off \
            insmod=e100 install=nfs://ip_instserver/path_instsource/product/CD1

# apic
label apic
    kernel linux
        append initrd=initrd ramdisk_size=65536 apic insmod=e100 \
            install=nfs://ip_instserver/path_instsource/product/CD1

# manual
label manual
    kernel linux
        append initrd=initrd ramdisk_size=65536 manual=1

# rescue
label rescue
    kernel linux
        append initrd=initrd ramdisk_size=65536 rescue=1

# memory test
label memtest
    kernel memtest

# hard disk
label hddisk
    localboot 0

implicit      0
display       message
prompt        1
timeout       100
```

*ip_instserver*と*path_instsource*は、セットアップで使った値で置き換えてください。

以下のセクションは、このセットアップで使用するPXELINUXオプションの簡単なリファレンスとなっています。使用可能なオプションの詳細については、`/usr/share/doc/packages/syslinux/`にある、`syslinux`パッケージのドキュメントを参照してください。

4.3.4 PXELINUXの設定オプション

ここに記されているのは、PXELINUX設定ファイルで利用可能なオプションの一部です。

DEFAULT *kernel options...*

デフォルトのカーネルコマンドラインを設定します。PXELINUXが自動的にブートする場合には、**DEFAULT**の後のエントリがブートプロンプトに対して入力されたときのように動作します。加えて、自動ブートであることを示す**auto**オプションも自動的に追加されます。

設定ファイルが存在しない、または設定ファイル内に**DEFAULT**エントリが存在しない場合には、オプションの付かないカーネル名「**linux**」がデフォルトとなります。

APPEND *options...*

カーネルのコマンドラインに1つまたは複数のオプションを追加します。これらは、自動ブートと手動ブートのどちらの場合でも追加されます。オプションはカーネルコマンドラインの先頭に追加されるので、通常は、明示的に入力したカーネルオプションによって上書きすることができます。

LABEL *label* KERNEL *image* APPEND *options...*

ブートするカーネルとして`label`が入力された場合、PXELINUXは代わりに`image`をブートし、ファイルのグローバルセクション(最初のLABELコマンドの前)で指定されたものの代わりに、指定されたAPPENDオプションを使用します。`image`のデフォルトは`label`と同じです。また、APPENDが指定されなかった場合には、グローバルエントリがデフォルトとして使用されます(あれば)。最大で128のLABELエントリが使用できます。

GRUBは次の構文を使用することに注意してください。

```
title mytitle
  kernel my_kernel my_kernel_options
  initrd myinitrd
```

PXELINUXは次の構文を使用します。

```
label mylabel
    kernel mykernel
    append myoptions
```

ラベルは、ファイル名の場合のように切り詰められるので、切り詰められた後も一意性が保たれるように決める必要があります。たとえば、「v2.1.30」と「v2.1.31」という2つのラベルは、PXELINUXでは区別できません。これらは切り詰められるとどちらも同じDOSファイル名になるからです。

カーネルは、Linuxのカーネルである必要はありません。ブートセクタやCOMBOOTファイルも使用できます。

APPEND -

何も追加しません。LABELセクション内で、APPENDに引数として1つのハイフンを付ければ、グローバルなAPPENDを上書きすることができます。

LOCALBOOT type

PXELINUXでは、KERNELオプションの代わりにLOCALBOOT 0を指定すると、この特定のラベルが呼び出されて、カーネルブートの代わりにローカルディスクのブートが行われます。

引数	説明
0	通常のブートを行う
4	まだメモリ上に常駐しているUNDI (Universal Network Driver Interface)ドライバを使用して、ローカルブートを行う
5	まだメモリ上に常駐しているUNDIドライバを含め、PXEスタック全体でローカルブートを行う

他の値は定義されていません。UNDIやPXEスタックについて知らない場合は、0を指定してください。

TIMEOUT *time-out*

自動的にブートする前に、ブートプロンプトをどれくらいの時間表示するかを指定します。単位は1/10秒です。タイムアウトは、ユーザがキーボードで何か入力するとキャンセルされます。この場合、ユーザがコマンドを入力するものとみなされます。タイムアウトの値を0に設定すると、タイムアウトは無効になります(これがデフォルトです)。タイムアウトの最大値は35996です(1時間よりほんの少しだけ短い時間です)。

PROMPT *flag_val*

*flag_val*を 0に設定すると、ShiftShiftAltAltCaps LockかScroll Lockキーがセットされている場合にのみ、ブートプロンプトを表示します(デフォルト)。

*flag_val*を1に設定すると、常にブートプロンプトを表示します。

F2 *filename*

F1 *filename*

..etc...

F9 *filename*

F10 *filename*

ブートプロンプトでファンクションキーを押したときに、指定されたファイルを表示します。これは、ブート前のオンラインヘルプ(おそらくはカーネルコマンドラインのオプション)を設定するために使用することができます。以前のリリースとの後方互換性のために、F10をF0として指定することもできます。現在のところ、F11とF12にファイル名を関連付けることはできないことに注意してください。

4.3.5 ターゲットシステムでPXEブートの準備をする

システムのBIOSで、PXEブートの準備をします。これには、BIOSのブート順でのPXEオプションの設定も含まれます。

警告: BIOSブートオーダー

BIOSで、PXEオプションをハードディスクブートオプションの前に指定しないでください。さもないと、システムはブートのたびに再インストールを行おうとします。

4.3.6 ターゲットシステムでWake on LANの準備をする

Wake on LAN (WOL)では、インストールの前に適切なBIOSオプションを有効にすることが必要です。また、ターゲットシステムのMACアドレスを記録しておいてください。このデータは、Wake on LANを開始するために必要です。

4.3.7 Wake on LAN

Wake on LANを使えば、コンピュータのMACアドレスを含む特別なネットワークパケットを使って、コンピュータの電源を入れることができます。世界中のすべてのコンピュータは一意のMAC識別子を持っているので、間違っても別のコンピュータの電源を入れてしまう心配はありません。

重要項目: 異なるネットワークセグメントにまたがるWake on LAN

制御用のマシンが、起動すべきインストールターゲットと同じネットワークセグメント内にはない場合には、WOL要求がマルチキャストとして送信されるように設定するか、またはそのネットワークセグメント内にあるマシンをリモートに制御して、要求の送信元として作動させてください。

SUSE Linux Enterprise Server 9以降のユーザは、WOLと呼ばれるYaSTモジュールを使って、簡単にWake on LANを設定することができます。他のバージョンのSUSE LinuxベースのOSユーザは、コマンドラインツールを使用してください。

4.3.8 YaSTを使ったWake on LAN

- 1 rootとしてログインします。
- 2 `[YaST] > [ネットワークサービス] > [WOL]` の順に選択します。
- 3 `[追加]` をクリックして、ターゲットシステムのホスト名とMACアドレスを入力します。

- 4 このコンピュータの電源を入れるには、適切な項目を選択して、**[起動]** をクリックします。

4.3.9 手動によるWake on LAN

- 1 rootとしてログインします。
- 2 **[YaST]** > **[ソフトウェアの管理]** の順に選択して、netdiagパッケージをインストールします。
- 3 ターミナルを開き、rootとして次のコマンドを入力して、ターゲットを起動します。

```
ether-wake mac_of_target
```

mac_of_targetは、ターゲットの実際のMACアドレスで置き換えてください。

4.4 ターゲットシステムをインストールのためにブートする

基本的に、[4.3.7項「Wake on LAN」](#) (84 ページ)と[4.3.3項「PXEブートの使用」](#) (78 ページ)で説明されているものを別にして、インストール用のブートプロセスをカスタマイズする方法は2とおりあります。デフォルトのブートオプションとファンクションキーを使用したり、インストールブート画面のブートオプションプロンプトを使って、特定のハードウェアでインストールカーネルが必要とするブートオプションを渡したりできます。

4.4.1 デフォルトのブートオプションを使う

ブートオプションの詳細については、[第3章 YaSTによるインストール](#) (21 ページ)を参照してください。一般に、**[インストール]** を選択すれば、インストールブートプロセスが開始します。

問題が発生した場合は、**[インストール--ACPI無効]** または **[インストール--セーフ設定]** を使用します。インストールプロセスでのトラブルシューティ

ングについての詳細は、[51.2項「インストールの問題」](#) (996 ページ)を参照してください。

4.4.2 Fキーを使う

画面の下部にあるメニューバーには、セットアップで必要になる、いくつかの高度な機能が用意されています。Fキーを使えば、これらのパラメータの構文の詳細を知らなくても、インストールルーチンに渡す付加オプションを指定できます([4.4.3項「カスタムのブートオプションを使用する」](#) (87 ページ)を参照)。

利用可能なオプションについては、次のテーブルを参照してください。

表 4.1 インストール時に使用できるFキー

Key	目的	利用可能なオプション	デフォルト値
F1	ヘルプを表示する	なし	なし
F2	インストール時の言語を選択する	サポートされているすべての言語	英語
F3	インストール時の画面解像度を変更する	<ul style="list-style-type: none">• テキストモード• VESA• 解像度#1• 解像度#2• ...	<ul style="list-style-type: none">• デフォルト値は、使用しているグラフィックハードウェアによって異なります。
F4	インストールソースを選択する	<ul style="list-style-type: none">• CD-ROMまたはDVD• SLP• FTP	CD-ROMまたはDVD

Key	目的	利用可能なオプション	デフォルト値
		<ul style="list-style-type: none"> • HTTP • NFS • SMB • ハードディスク 	
F5	ドライバアップデート ディスクを適用する	ドライバ	なし

4.4.3 カスタムのブートオプションを使用する

適切なブートオプションのセットを使えば、インストールの手順を容易にすることができます。多くのパラメータは、後ほど`linuxrc`ルーチンを使って設定することもできますが、ブートオプションを使用するほうが簡単です。いくつかの自動セットアップでは、ブートオプションを`initrd`または`info`ファイルで設定することもできます。

次のテーブルでは、この章で説明したすべてのインストールシナリオと、ブートに必要なパラメータ、および対応するブートオプションを示します。インストールルーチンに渡すブートオプション文字列を決めるには、このテーブルに表示されている順序で、それらをすべてつなげてください。たとえば次のようになります(すべてを1行で記述します)

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

この文字列の中のすべての値(...)は、セットアップに適した値で置き換えてください。

表 4.2 この章で用いられているインストール(ブート)シナリオ

インストールシナリオ	ブートに必要なパラメータ	ブートオプション
第3章 <i>YaST</i> によるインストール (21 ページ)	なし: システムは自動的にブートします	必要なし
4.1.1項「VNC経由のシンプルリモートインストール—静的なネットワーク設定」(54 ページ)	<ul style="list-style-type: none"> • インストールサーバの場所 • ネットワークデバイス • IPアドレス • ネットマスク • ゲートウェイ • VNCの有効化 • VNCのパスワード 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code> • <code>netdevice=some_netdevice</code> (複数のネットワークデバイスが利用可能な場合にのみ必要) • <code>hostip=some_ip</code> • <code>netmask=some_netmask</code> • <code>gateway=ip_gateway</code> • <code>vnc=1</code> • <code>vncpassword=some_password</code>
4.1.2項「VNC経由のシンプルリモートインストール—動的なネットワーク設定」(55 ページ)	<ul style="list-style-type: none"> • インストールサーバの場所 • VNCの有効化 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code> • <code>vnc=1</code> • <code>vncpassword=some_password</code>

インストールシ ナリオ	ブートに必 要なパラ メータ	ブートオプション
4.1.3項「VNC経 由のリモートイ ンストール—PXE ブートとWake on LAN」(57 ペー ジ)	<ul style="list-style-type: none"> • VNCの パス ワード • インス トール サーバ の場所 • TFTP サーバ の場所 • VNCの 有効化 • VNCの パス ワード 	適用されない。プロセスはPXEとDHCPによって管理される
4.1.4項「SSH経 由のシンプルリ モートインス トール—静的な ネットワーク設 定」(58 ページ)	<ul style="list-style-type: none"> • インス トール サーバ の場所 • ネット ワーク デバイ ス • IPアド レス • ネット マスク • ゲート ウェイ • SSHの 有効化 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code> • <code>netdevice=some_netdevice</code> (複数のネットワークデバイスが利用可能な場合にのみ必要) • <code>hostip=some_ip</code> • <code>netmask=some_netmask</code> • <code>gateway=ip_gateway</code> • <code>usessh=1</code> • <code>sshpassword=some_password</code>

インストールシ ナリオ	ブートに必 要なパラ メータ	ブートオプション
	<ul style="list-style-type: none"> • SSHの パス ワード 	
4.1.5項「SSH経 由のシンプルリ モートインス トール—動的な ネットワーク設 定」(60 ページ)	<ul style="list-style-type: none"> • インス トール サーバ の場所 • SSHの 有効化 • SSHの パス ワード 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code> • <code>usessh=1</code> • <code>sshpassword=some_password</code>
4.1.6項「SSH経 由のリモートイ ンストール—PXE ブートとWake on LAN」(61 ペー ジ)	<ul style="list-style-type: none"> • インス トール サーバ の場所 • TFTP サーバ の場所 • SSHの 有効化 • SSHの パス ワード 	適用されない。プロセスはPXEとDHCPによって管理される

ティップ: linuxrcブートオプションの詳細情報

Linuxシステムをブートする際に用いられるlinuxrcのブートオプションについての詳細は、`/usr/share/doc/packages/linuxrc/linuxrc.html`を参照してください。

4.5 インストールプロセスのモニタ

インストールプロセスをリモートにモニタするには、いくつかの方法があります。インストールのためのブートで、適切なブートオプションを選択すれば、VNCまたはSSHを使って、リモートのワークセッションからインストールとシステム設定を制御することができます。

4.5.1 VNCによるインストール

VNCビューアソフトウェアを使えば、事実上どのオペレーティングシステムからでも、SUSE Linux Enterpriseのインストールをリモート制御することができます。このセクションでは、VNCビューアアプリケーションまたはWebブラウザを使うセットアップについて説明します。

VNCによるインストールの準備

VNCによるインストールを準備するために、インストールターゲット上で行う必要のあることは、インストールのための初期ブートで適切なブートオプションを選択することだけです(4.4.3頁「**カスタムのブートオプションを使用する**」(87 ページ)を参照)。ターゲットシステムはテキストベースの環境にブートして、VNCクライアントがインストールプログラムに接続するのを待ちます。

インストールプログラムは、インストーラに接続するために必要なIPアドレスとディスプレイ番号をアナウンスします。ターゲットシステムに物理的にアクセスしている場合には、この情報はシステムがインストールのためにブートした直後に表示されます。VNCソフトウェアが要求してきたときにこのデータを入力し、VNCパスワードを入力してください。

インストールターゲットはOpenSLPによってアナウンスを行うので、ネットワークセットアップ、およびすべてのマシンがOpenSLPをサポートしていれば、物理的にアクセスしなくても、SLPブラウザによってインストールターゲットのアドレス情報を取得できます。

- 1 KDEのファイルおよびWebブラウザであるKonquerorを起動します。
- 2 場所バーにservice://yast.installation.suseと入力します。
ターゲットシステムは、Konquerorの画面にアイコンとして表示されま

す。このアイコンをクリックすると、KDEのVNCビューアが起動するので、その中でインストールを実行できますまたは、使用しているVNCビューアソフトウェアを、インストールの開始時に表示されたIPアドレスの後に:1を付けて実行することもできます。

インストールプログラムへの接続

基本的には、VNCサーバ(この場合はインストールターゲット)に接続するには2通りの方法があります。任意のオペレーティングシステムで独立したVNCビューアアプリケーションを起動することもできますし、Java対応のWebブラウザを使って接続することもできます。

VNCを使えば、Linuxシステムのインストールを、他のLinux、Windows、Mac OSなど、他の任意のオペレーティングシステムから制御できます。

Linuxマシンでは、`tightvnc`パッケージがインストールされていることを確認してください。Windowsマシンでは、このソフトウェアのWindows移植版をインストールしてください。これは、TightVNCのホームページから入手できます(<http://www.tightvnc.com/download.html>)。

ターゲットマシンで動作しているインストールプログラムに接続するには、以下の手順に従います。

- 1 VNCビューアを起動します。
- 2 SLPブラウザ、またはインストールプログラム自体から提供された、インストールターゲットのIPアドレスとディスプレイ番号を入力します。

```
ip_address:display_number
```

デスクトップにウインドウが開き、その中に、通常のローカルインストールの場合と同様に、YaSTの画面が表示されます。

インストールプログラムに接続するためにWebブラウザを使えば、VNCソフトウェアや、基になるオペレーティングシステムに依存しなくて済みます。ブラウザアプリケーションでJavaのサポートが有効になっているものであれば、Linuxシステムのインストールのために、どのブラウザでも使用できます(Firefox、Internet Explorer、Konqueror、Operaなど)。

VNCによるインストールを実行する場合、以下の手順に従います。

1 使用しているWebブラウザを起動します。

2 アドレスに以下のように入力します。

```
http://ip_address_of_target:5801
```

3 要求されたときにはVNCパスワードを入力します。ブラウザウィンドウに、通常のローカルインストールの場合のように、YaSTの画面が表示されます。

4.5.2 SSHによるインストール

SSHを使えば、任意のSSHクライアントソフトウェアによって、Linuxマシンのインストールを制御することができます。

SSHによるインストールの準備

ソフトウェアパッケージ(LinuxではOpenSSH、WindowsではPuTTY)のインストールの他に、SSHによるインストールのために適切なブートオプションを渡す必要があります。詳細については、[4.4.3項「カスタムのブートオプションを使用する」](#) (87 ページ)を参照してください。SUSE Linuxベースのオペレーティングシステムであれば、デフォルトでOpenSSHがインストールされています。

インストールプログラムへの接続

1 インストールターゲットのIPアドレスを取得します。ターゲットマシンに物理的にアクセスできる場合には、初期ブート後のコンソールにインストールプログラムが表示するIPアドレスを記録してください。または、DHCPサーバ設定によって特定のホストに割り当てられたIPアドレスを調べてください。

2 コマンドラインで次のコマンドを入力します。

```
ssh -X root@ip_address_of_target
```

`ip_address_of_target`は、ターゲットの実際のIPアドレスで置き換えてください。

- 3 ユーザ名を要求されたら、rootと入力します。
- 4 パスワードを求められたら、SSHのブートオプションで設定したパスワードを入力します。正しく認証されると、インストールターゲットのコマンドプロンプトが表示されます。
- 5 yastと入力して、インストールプログラムを起動します。第3章 *YaSTによるインストール* (21 ページ)で説明されているように、ウィンドウが開いて、通常のYaSTの画面が表示されます。

自動インストール

AutoYaSTを使用して、多数のコンピュータに並行してSUSE® Linux Enterpriseをインストールできます。AutoYaSTでは、異種ハードウェア環境への導入に対して柔軟に対応します。この章では、単純な自動インストールを行うための準備作業、および異種ハードウェア環境の場合の高度なインストール方法について説明します。

5.1 単純な大規模インストール

重要項目: 同一のハードウェアを使用している環境

ここでは、同一のハードウェアで構成される一連のコンピュータへのSUSE Linux Enterpriseのインストールについて説明します。

AutoYaSTの大規模インストールを準備するには、次の手順に従ってください。

- 1 導入に必要なインストールの詳細を定義したAutoYaSTプロファイルを作成します。詳細は、[5.1.1項「AutoYaSTプロファイルの作成」](#) (96 ページ)を参照してください。
- 2 AutoYaSTプロファイルのソース、およびインストールルーチンに渡すパラメータを決定します。詳細は、[5.1.2項「プロファイルの配布とAutoYaSTパラメータの決定」](#) (98 ページ)を参照してください。

- 3 SUSE Linux Enterpriseインストールデータのソースを決定します。詳細は、[5.1.3項「インストールデータの提供」](#) (101 ページ)を参照してください。
- 4 自動インストールのブートシナリオを決定および設定します。詳細は、[5.1.4項「ブートシナリオの設定」](#) (102 ページ)を参照してください。
- 5 パラメータを手動で追加、またはinfoファイルを作成して、インストールルーチンにコマンドラインを渡します。詳細は、[5.1.5項「infoファイルの作成」](#) (104 ページ)を参照してください。
- 6 自動インストールを開始します。詳細は、[5.1.6項「自動インストールの開始と監視」](#) (107 ページ)を参照してください。

5.1.1 AutoYaSTプロファイルの作成

AutoYaSTに、何をインストールするか、そしてインストール先システムをどのように設定するかを知らせるには、AutoYaSTプロファイルを使用します。このプロファイルは、さまざまな方法で作成できます。

- インストールした直後のコンピュータから同一構成の他のコンピュータに複製する
- AutoYaST GUIを使って、要件に合うようにプロファイルを作成および変更する
- XMLエディタを使って最初からプロファイルを作成する

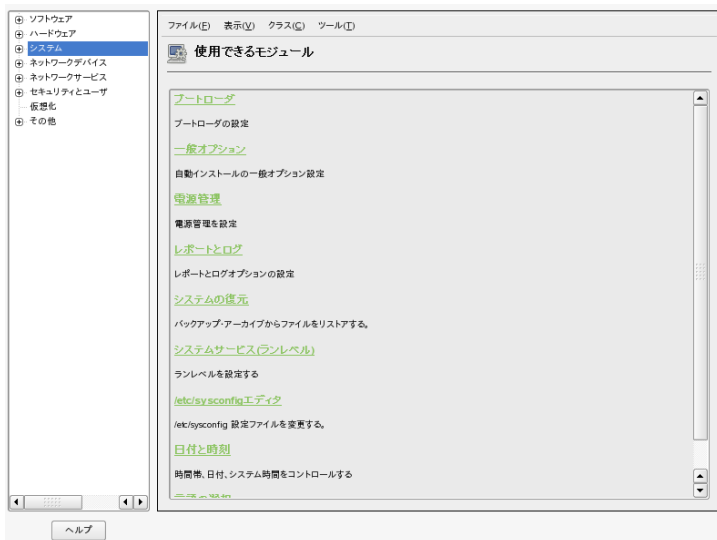
インストール直後のコンピュータから複製するには、次の手順に従ってください。

- 1 通常のインストールを行います。
- 2 ハードウェア設定を完了して、リリースノートを読んだら、*[Clone This Installation for AutoYaST]* (AutoYaST用にこのインストールを複製する) を選択します。デフォルトでは、このチェックボックスは選択されていません。プロファイル/root/autoinst.xmlが作成されます。このプロファイルを使って、このインストールの複製を作成することができます。

AutoYaST GUIを使って既存のシステム設定からプロファイルを必要に応じて作成および変更するには、次の手順に従ってください。

- 1 rootとして、YaSTを開始します。
- 2 [その他] > [Autoinstallation] の順に選択して、AutoYaST GUIを起動します。
- 3 現在のシステム設定がミラーされているAutoYaSTプロファイルを作成するには、[Tools] > [Create Reference Control File] の順に選択します。
- 4 ブートローダ、パーティション、およびソフトウェアの選択内容などのデフォルトのリソースに加えて、システム中の他の要素に関する情報も追加する場合は、[Create a Reference Control File] リスト中の該当する項目を選択します。
- 5 [作成] をクリックすると、YaSTによりすべてのシステム情報が収集され、新しいプロファイルが作成されます。
- 6 次に、以下のいずれかの作業を行います。
 - 作成されたプロファイルが完全に要件と一致している場合は、[ファイル] > [名前を付けて保存] の順に選択して、autoinst.xmlのようにプロファイル名を入力します。
 - 左側のツリービューから適切な設定項目(ハードウェア、プリンタなど)を選択し、「[設定]」をクリックして参照プロファイルを変更します。各YaSTモジュールが開きますが、変更内容はシステムに適用されるのではなく、AutoYaSTプロファイルに書き込まれます。作業が完了したら、[ファイル] > [名前を付けて保存] の順に選択して、適切なプロファイル名を入力します。
- 7 ファイル > 終了の順に選択して、AutoYaSTモジュールを終了します。

図 5.1 AutoYaSTフロントエンドを使ったAutoYaSTプロファイルの編集



5.1.2 プロファイルの配布とAutoYaSTパラメータの決定

AutoYaSTプロファイルは、さまざまな方法で配布できます。プロファイルデータを配布するために使用するプロトコルによって、プロファイルの場所を知らせるために使用するAutoYaSTパラメータが異なります。プロファイルの場所は、ブートプロンプト、またはブート時にロードされるinfoファイルを使って、インストールルーチンに渡されます。次のオプションを指定できます。

プロファイルの場所	パラメータ	説明
ファイル	<code>autoyast=file:// /path</code>	インストールルーチンに、指定したパス(ソースルートディレクトリの相対パス—CD ROMの最上位ディレクトリにある場合はfile:///

プロファイルの場所	パラメータ	説明
		autoinst.xml)内にある制御ファイルを参照させます。
Device	autoyast=device:// /path	インストールルーチンに、ストレージデバイス上の制御ファイルを参照させます。デバイス名以外は必要ありません。たとえば、/dev/sda1ではなく、sda1と指定する必要があります。
フロッピー (Floppy)	autoyast=floppy:// /path	インストールルーチンに、フロッピードライブにあるフロッピーディスク上の制御ファイルを参照させます。このオプションは、CD-ROMからブートする場合などに役立ちます。 フロッピーディスクから制御ファイルを取得できなかった場合、AutoYaSTはコンピュータに接続されているUSBデバイスを自動的に検索します。
USB(フラッシュ)ディスク	autoyast=usb:// /path	このオプションを指定すると、接続されている任意のUSBデバイスの制御ファイルが検索されます。
NFS	autoyast=nfs:// /server/path	インストールルーチンに、NFSサーバから制御ファイルを取得させます。
HTTP	autoyast=http:// /server/path	インストールルーチンに、HTTPサーバから制御ファイルを取得させます。

プロファイルの場所	パラメータ	説明
HTTPS	<code>autoyast=https:// /server/path</code>	インストーलルーチンに、 HTTPS サーバから制御ファイルを取得させます。
TFTP	<code>autoyast=tftp:// /server/path</code>	インストーलルーチンに、 TFTP サーバから制御ファイルを取得させます。
FTP	<code>autoyast=ftp:// /server/path</code>	インストーलルーチンに、 FTP サーバから制御ファイルを取得させます。

`server`および`path`の部分には、それぞれ実際のサーバ名またはパス名を指定してください。

AutoYaSTには、特定のプロファイルをクライアントのMACアドレスにバインドできるようにする機能があります。この機能を利用することにより、`autoyast=`パラメータを変更せずに、異なるプロファイルを使用して、同じセットアップで別のインスタンスのインストールを行うことができます。

この機能を使用するには、次の手順に従ってください。

- 1 クライアントのMACアドレスをファイル名にして、個別のプロファイルを作成します。作成したプロファイルは、自分のAutoYaSTプロファイルがあるHTTPサーバに保管します。
- 2 `autoyast=`パラメータの作成時には、パスとファイル名を省略します。以下に例を示します。

```
autoyast=http://192.0.2.91/
```

- 3 自動インストールを開始します。

YaSTは、次の手順でプロファイルの場所を判断します。

1. YaSTは、自分のIPアドレスの大文字16進数表記を使ってプロファイルを検索します。たとえば、IPアドレスの}}192.0.2.91は、16進数表記でC000025Bとなります。
2. このファイルが見つからなかった場合、16進数表記の桁を1つ削除して、もう一度検索を行います。適切な名前を持つファイルが見つかるまで、この手順を8回繰り返します。
3. これでもファイルが見つからない場合は、ファイル名がクライアントのMACアドレスであるファイルを検索します。たとえば、クライアントのMACアドレスが0080C8F6484Cである場合、この名前を持つファイルが検索されます。
4. ファイル名がMACアドレスであるファイルが見つからなかった場合は、ファイル名がdefault(小文字)のファイルを探します。YaSTがAutoYaSTプロファイルを検索する順序の例を以下に示します。

```
C000025B
C000025
C00002
C0000
C000
C00
C00
C0
C
0080C8F6484C
default
```

5.1.3 インストールデータの提供

インストールデータは、製品CD、DVD、またはネットワークインストールソースを介して提供できます。製品CDをインストールソースとして使用する場合は、ブートプロセスを手動で開始したり、CDを交換したりするため、インストール対象クライアントに物理的にアクセスする必要があります。

ネットワーク経由でインストールソースを提供する場合は、**4.2.1項「YaSTを使ったインストールサーバのセットアップ」** (63 ページ)の説明に従ってネットワークインストールサーバ(HTTP、NFS、FTP)を設定します。インストールルーチンにサーバの場所を渡すには、infoファイルを使用します。

5.1.4 ブートシナリオの設定

クライアントは、さまざまな方法でブートできます。

ネットワークブート

通常のリモートインストールでは、Wake on LANやPXEを使って自動インストールを開始することができます。また、ブートイメージと制御ファイルはTFTP経由で取得し、インストールソースはネットワークインストールサーバを利用します。

ブート可能CD-ROM

自動インストールするシステムのブートにオリジナルのSUSE Linux Enterpriseメディアを使い、制御ファイルをネットワークやフロッピーディスクから取得します。または、インストールソースとAutoYaSTプロファイルの両方を格納した独自のCD-ROMを作成することもできます。

以降の項では、ネットワークブートまたはCD-ROMからのブート手順の基本的な概略を説明します。

ネットワークブートの準備

Wake on LAN、PXE、およびTFTPを使ったネットワークブートについては、[4.1.3項「VNC経由のリモートインストール—PXEブートとWake on LAN」](#) (57 ページ)を参照してください。自動インストールの準備を行うには、PXE Linux設定ファイル(/srv/tftp/pxelinux.cfg/default)に、AutoYaSTプロファイルの場所を指定したautoyastパラメータを追加します。標準インストールを行う場合のエントリの例を以下に示します。

```
default linux

# default label linux
kernel linux append initrd=initrd ramdisk_size=65536 insmod=e100 \
install=http://192.168.0.22/install/suse-enterprise/
```

自動インストール時の例を以下に示します。

```
default linux

# default label linux
```

```
kernel linux append initrd=initrd ramdisk_size=65536 insmod=e100 \  
install=http://192.168.0.22/install/suse-enterprise/ \  
autoyast=nfs://192.168.0.23/profiles/autoinst.xml
```

これらの例のIPアドレスとパスは、実際の環境に合わせて変更する必要があります。

CD-ROM からのブートの準備

AutoYaSTインストールでCD-ROMからブートするには、さまざまな方法があります。次の中から、適切な方法を選択してください。

SUSE Linux Enterpriseメディアからブートし、プロファイルをネットワーク経由で取得する

ネットワークベースのインストールでは完全にインストールできない場合（ハードウェアがPXEをサポートしていない場合など）で、プロセス中にシステムに物理的にアクセスできる場合は、この方法を使用します。

この方法では、次のものが必要になります。

- SUSE Linux Enterpriseメディア
- プロファイルデータを提供するネットワークサーバ(詳細は[5.1.2項「プロファイルの配布とAutoYaSTパラメータの決定」](#) (98 ページ)を参照)
- プロファイルの場所をインストールルーチンに知らせるinfoファイルを含んだフロッピーディスク

または

autoyast=パラメータを手動で入力するため、システムのブートプロンプトへのアクセス

SUSE Linux Enterpriseメディアからブートおよびインストールを行い、プロファイルはフロッピーから取得する

ネットワークベースのインストールでは完全にインストールできない場合に、この方法を使用します。この方法では、ターゲットコンピュータを起動したり、ブートプロンプトにプロファイルの場所を入力するため、システムに物理的にアクセスする必要があります。また、いずれの場合

でも、インストールの内容によってはメディアを交換しなければならないこともあります。

この方法では、次のものが必要になります。

- SUSE Linux Enterprise メディア
- プロファイルとinfoファイルの両方を格納したフロッピーディスク

または

autoyast=パラメータを入力するため、ターゲットのブートプロンプトへのアクセス

カスタムメディアからブートおよびインストールを行い、プロファイルもそのメディアから取得する

特定のソフトウェアパッケージだけをインストールすればよく、ターゲット数が比較的少ない場合は、インストールデータとプロファイルの両方を格納した独自のCDを作成することも考慮してください。この方法は、ネットワークが利用できない場合などに役立ちます。

5.1.5 infoファイルの作成

ターゲットのインストールルーチンには、AutoYaSTフレームワークのすべてのコンポーネントを認識させる必要があります。認識させるには、インストールプロセスを制御するために必要なAutoYaSTコンポーネント、インストールソース、およびパラメータを探すのに必要なすべてのパラメータを含んだコマンドラインを作成します。

このためには、インストール時にブートプロンプトから手動でこれらのパラメータを指定するか、またはインストールルーチン(`linuxrc`)に参照させるinfoファイルを作成します。ブートプロンプトから手動で指定する方法は、インストール対象クライアントに物理的にアクセスする必要があるため、大規模な導入には向いていません。ファイルを作成する方法は、infoファイルをいくつかのメディアに格納し、それを自動インストールの前にクライアントのドライブに挿入して準備しておくことができます。かわりに、`pxelinux.cfg/default`ファイルに`linuxrc`パラメータを指定して、PXEブートを使用することもできます。詳細は、[ネットワークブートの準備項](#) (102 ページ)を参照してください。

linuxrcで一般的に使用されるパラメータを以下に示します。詳細は、/usr/share/doc/packages/autoyastにある、AutoYaSTパッケージのドキュメントを参照してください。

重要項目: パラメータと値の区切り方

ブートプロンプトからlinuxrcに渡すパラメータを入力する場合、パラメータと値の間は「=」で区切ります。infoファイルを使用する場合は、パラメータと値の間を「:」で区切ります。

キーワード	値
netdevice	ネットワークセットアップに使用するネットワークデバイス(BOOTP/DHCPリクエスト用) 複数のネットワークデバイスを利用できる場合にのみ指定する必要があります。
hostip	指定しない場合、クライアントはBOOTPリクエストを送信します。値を指定した場合は、指定したデータに基づいてクライアントが設定されます。
netmask	ネットマスク。
gateway	ゲートウェイ
nameserver	ネームサーバ。
autoyast	自動インストールに使用するコントロールファイルの場所で、 「autoyast=http://192.168.2.1/profiles/」 のように指定します
install	インストールソースの場所で、 「install=nfs://192.168.2.1/CDs/」のように 指定します。
vnc	「1」を設定すると、VNCリモート制御によるインストールが有効になります。

キーワード	値
vncpassword	VNCのパスワードを指定します。
usessh	「1」を設定すると、SSHリモート制御によるインストールが有効になります。

自動インストール時にDHCP経由でクライアントを設定し、ネットワークインストールソースを使い、インストールプロセスをVNCを使って監視する場合、infoファイルは次のようになります。

```
autoyast:profile_source install:install_source vnc:1 vncpassword:some_password
```

インストール時に静的なネットワーク設定を使う場合、infoファイルは次のようになります。

```
autoyast:profile_source \  
install:install_source \  
hostip:some_ip \  
netmask:some_netmask \  
gateway:some_gateway
```

改行を示す「\
」は、読みやすくするためだけに挿入されています。すべてのオプションは、連続した文字列として入力する必要があります。

infoファイル中のデータをlinuxrcに利用させるには、さまざまな方法があります。

- ・ インストール時に、クライアントのフロッピードライブ内にあるフロッピーディスクのルートディレクトリにファイルを格納する。
- ・ カスタムインストールメディアまたはPXEブートから提供されるシステムのブート用初期RAMディスクのルートディレクトリにファイルを格納する。
- ・ AutoYaSTプロファイルの一部としてファイルデータを保管する。この場合、linuxrcに認識させるために、AutoYaSTファイルのファイル名は、infoでなければなりません。この場合の例を以下に示します。

linuxrcは、プロファイル内でファイルの先頭を表す文字列(`start_linuxrc_conf`)を探します。文字列が見つかったら、そこから内容の解析を開始し、終端を表す文字列(`end_linuxrc_conf`)が見つかった時点で解析を終了します。プロファイル内で、オプションを次のように指定します。

```
....
<install>
....
  <init>
    <info_file>
<![CDATA[
#
# Don't remove the following line:
# start_linuxrc_conf
#
install: nfs:server/path
vnc: 1
vncpassword: test
autoyast: file:///info

# end_linuxrc_conf
# Do not remove the above comment
#
]]>

    </info_file>
  </init>
.....
</install>
....
```

この場合、**linuxrc**は従来の`info`ファイルのかわりに、ブートパラメータを含んだプロファイルをロードします。`install:`パラメータは、インストールソースの場所を示しています。`vnc`と`vncpassword`は、インストールの監視にVNCを使うことを表しています。`autoyast`パラメータは、`info`をAutoYaSTプロファイルとして扱うように指示します。

5.1.6 自動インストールの開始と監視

前述の準備が完了したら(プロファイル、インストールソース、および`info`ファイル)、自動インストールを開始できます。ブート方法やプロセスの監視方法によっては、クライアントでの物理的な操作が必要なこともあります。

- ・ クライアントシステムを物理メディア(製品CDやカスタムCDなど)からブートする場合は、それらのメディアをクライアントのドライブに挿入する必要があります。
- ・ Wake on LANを使ってクライアントの電源を入れる場合以外は、クライアントの電源を手動で入れる必要があります。
- ・ リモートによる自動インストールを行わない場合は、AutoYaSTからのメッセージはクライアントのモニタに表示されます。モニタが接続されていない場合は、シリアルコンソールに送られます。

リモートによる自動インストールを行うには、5.1.5項「**infoファイルの作成**」(104 ページ)の説明に従ってVNCまたはSSHパラメータを指定し、4.5項「**インストールプロセスのモニタ**」(91 ページ)の説明に従って、他のコンピュータからクライアントに接続します。

5.2 ルールベースの自動インストール

以降の項では、AutoYaSTを使用したルールベースのインストールの基本的な概念、およびカスタム自動インストール設定の作成例について説明します。

5.2.1 ルールベースの自動インストールとは

ルールベースのAutoYaSTインストールを利用すれば、異種ハードウェアが存在する環境で自動インストールを実施できます。

- ・ サイトに異なるベンダからのハードウェアが混在していますか?
- ・ サイトにあるコンピュータのハードウェア構成がそれぞれ異なっていますか(違うデバイスを使っていたり、メモリ量やディスクサイズが異なる場合など)?
- ・ 複数のドメイン間でインストールを実施する場合に、これらのドメインを区別する必要がありますか?

基本的に、ルールベースの自動インストールでは、異種ハードウェア環境に合わせて複数のプロファイルをマージした、独自のカスタムプロファイルを作成します。各ルールにはセットアップの特徴(ディスクサイズなど)が記述

されており、ルールに一致した場合にどのプロファイルを使用するかをAutoYaSTに指示します。それぞれの特徴が記述された複数のルールは、AutoYaSTのrules.xmlファイルに保管されます。AutoYaSTはこれらのルールを処理して、AutoYaSTルールに一致する複数のプロファイルをマージした最終プロファイルを生成します。この手順の概略図は、[5.2.2項「ルールベースの自動インストールの例」](#) (110 ページ)を参照してください。

ルールベースのAutoYaST自動インストールを利用すれば、柔軟にSUSE Linux Enterpriseの導入を計画し、それを実施することができます。以下の操作を行います。

- AutoYaSTで事前定義されているシステム属性に一致するかどうかを判断するルールを作成する。
- 論理演算子を使って複数のシステム属性(ディスクサイズとカーネルのアーキテクチャなど)を1つのルールにまとめる
- シェルスクリプトを実行して、その出力をAutoYaSTフレームワークに渡すことによって独自のカスタムルールを作成する 作成可能なカスタムルールの数は5つです。

注意

AutoYaSTを使ったルールの作成と使用については、`/usr/share/doc/packages/autoyast2/html/index.html`にあるパッケージドキュメントの「*Rules and Classes*」の章を参照してください。

ルールベースのAutoYaSTの大規模インストールを準備するには、次の手順に従ってください。

- 1 異種ハードウェア環境のセットアップに必要なインストールの詳細を定義した、複数のAutoYaSTプロファイルを作成します。詳細は、[5.1.1項「AutoYaSTプロファイルの作成」](#) (96 ページ)を参照してください。
- 2 ハードウェアセットアップのシステム属性と一致するルールを定義します。詳細は、[5.2.2項「ルールベースの自動インストールの例」](#) (110 ページ)を参照してください。

- 3 AutoYaSTプロファイルのソース、およびインストールルーチンに渡すパラメータを決定します。詳細は、[5.1.2項「プロファイルの配布とAutoYaSTパラメータの決定」](#) (98 ページ)を参照してください。
- 4 [5.1.3項「インストールデータの提供」](#) (101 ページ)の説明に従って、SUSE Linux Enterpriseインストールデータのソースを決定します
- 5 パラメータを手動で追加、またはinfoファイルを作成して、インストールルーチンにコマンドラインを渡します。詳細は、[5.1.5項「infoファイルの作成」](#) (104 ページ)を参照してください。
- 6 自動インストールのブートシナリオを決定および設定します。詳細は、[5.1.4項「ブートシナリオの設定」](#) (102 ページ)を参照してください。
- 7 自動インストールを開始します。詳細は、[5.1.6項「自動インストールの開始と監視」](#) (107 ページ)を参照してください。

5.2.2 ルールベースの自動インストールの例

ルールをどのように作成するかを理解するため、ここでは次の例を使って説明します。概略図は、[図 5.2. 「AutoYaSTルール」](#) (111 ページ)を参照してください。AutoYaSTインストールを1回実行すると、次のセットアップが行われます。

プリントサーバ

このコンピュータには、最低限の項目しかインストールされません。デスクトップ環境は必要なく、一部のソフトウェアパッケージのみが必要とされます。

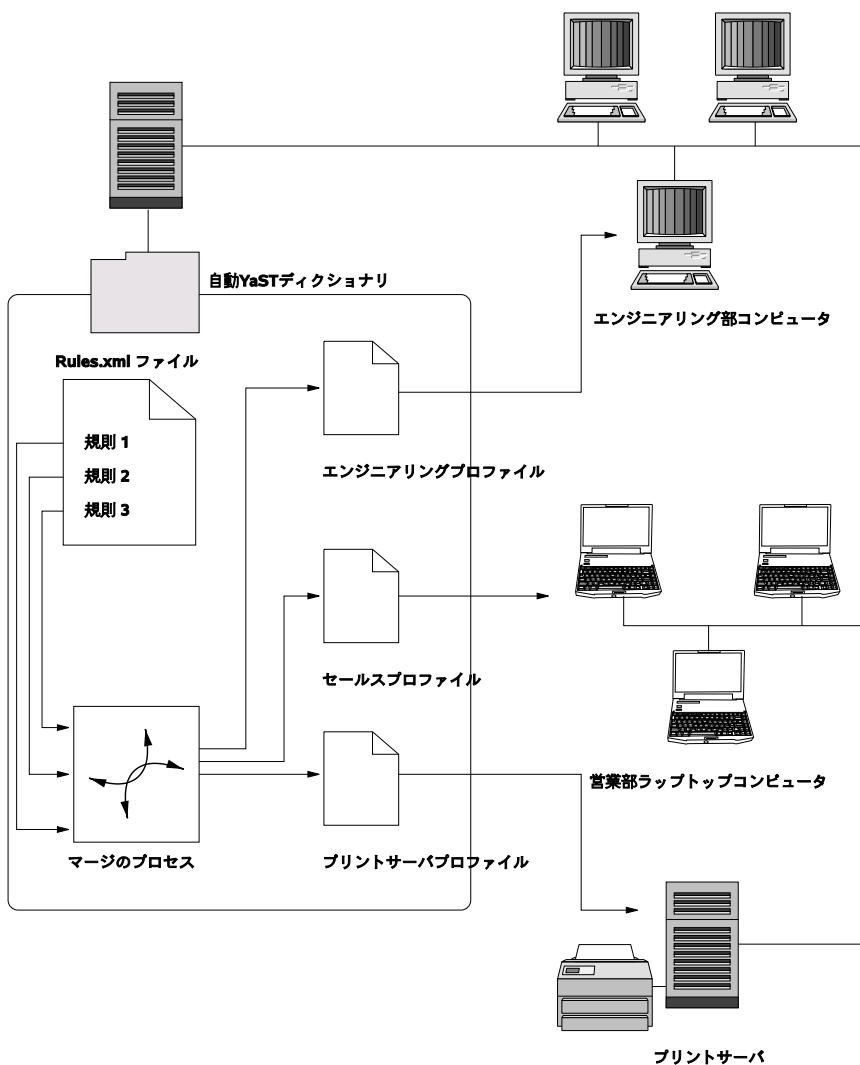
技術部門のワークステーション

これらのコンピュータにはデスクトップ環境と、さまざまな開発ソフトウェアが必要です。

営業部門のラップトップ

これらのコンピュータには、デスクトップ環境と特定のアプリケーション(オフィス、カレンダーソフトウェアなど)が必要です。

図 5.2 AutoYaSTルール



まず最初に、5.1.1項「AutoYaSTプロファイルの作成」(96 ページ)に説明されているいずれかの方法を使って、それぞれのケースに対応するプロファイルを作成します。この例では、それぞれprint.xml、engineering.xml、およびsales.xmlを作成します。

次に、AutoYaSTに使用するプロファイルを指示するために、3種類のハードウェアタイプを識別するルールを作成します。次のようなアルゴリズムに基づいて、ルールをセットアップします。

1. コンピュータのIPアドレスが192.168.27.11かどうか? そうならば、プリントサーバとして設定する。
2. コンピュータにPCMCIAハードウェアが搭載されており、Intel製のチップセットが使用されているか? そうならば、Intel製ラップトップであると判断し、営業部門に適したソフトウェアをインストールする。
3. 前述の条件に当てはまらない場合は、開発部門のワークステーションと判断し、適切なソフトウェアやパッケージをインストールする。

このような条件を定義したrules.xmlファイルの例を以下に示します。

```
<?xml version="1.0"?>
<!DOCTYPE autoinstall SYSTEM "/usr/share/autoinstall/dtd/rules.dtd">
<autoinstall xmlns="http://www.suse.com/1.0/yast2ns"
xmlns:config="http://www.suse.com/1.0/configs">
  <rules config:type="list">
    <rule>
      <hostaddress>
        <match>192.168.27.11</match>
        <match_type>exact</match_type>
      </hostaddress>
      <result>
        <profile>print.xml</profile>
        <continue config:type="boolean">false</continue>
      </result>
    </rule>
    <rule>
      <haspcmcia>
        <match>1</match>
        <match_type>exact</match_type>
      </haspcmcia>
      <custom1>
        <script>
if grep -i intel /proc/cpuinfo > /dev/null; then
echo -n "intel"
else
echo -n "non_intel"
fi;
        </script>
        <match>*</match>
        <match_type>exact</match_type>
      </custom1>
      <result>
```

```

        <profile>sales.xml</profile>
        <continue config:type="boolean">false</continue>
    </result>
    <operator>and</operator>
</rule>
<rule>
    <haspcmcia>
        <match>0</match>
        <match_type>exact</match_type>
    </haspcmcia>
</result>
    <profile>engineering.xml</profile>
    <continue config:type="boolean">false</continue>
</result>
</rule>
</rules>
</autoinstall>

```

このルールファイルを配布する場合、`autoyast=protocol:serverip/profiles/URL`で指定されているprofilesディレクトリ内にrulesディレクトリが常駐することを確認してください。AutoYaSTは、rulesサブディレクトリのrules.xmlを探し、ファイルに指定されているプロファイルを読み込みおよびマージします。

以降の自動インストール作業は、通常と同じように実施します。

5.3 詳細情報

AutoYaST技術の詳細は、ソフトウェアと一緒にインストールされているドキュメントを参照してください。このドキュメントは、`/usr/share/doc/packages/autoyast2`ディレクトリにあります。このドキュメントの最新版については、http://www.suse.de/~ug/autoyast_doc/index.htmlを参照してください。

カスタマイズした事前インストールの配布

カスタマイズしたSUSE Linux Enterpriseの事前インストールを多数の同じ形式のコンピュータに配布することにより、各コンピュータ個別にインストール作業を行う手間を省けます。また、エンドユーザは、標準のインストール手順を使って、インストール作業を行うことができます。YaST firstbootを利用すれば、カスタマイズした事前インストールイメージを作成し、エンドユーザが各自の要件に応じて環境設定を行うための最終作業用ワークフローを決定することができます。これは、完全な自動インストールを行うAutoYaSTとは異なります。詳細は、[第5章 自動インストール](#) (95 ページ)を参照してください。

カスタムインストールを作成し、それを展開して各自の要件に合わせた環境設定を行わせるには、次のような作業を行います。

- 1 クライアントコンピュータに複製するディスクを持つマスタコンピュータを準備します。詳細については、[6.1項 「マスタマシンの準備」](#) (116 ページ)を参照してください。
- 2 ワークフローをカスタマイズします。詳細については、[6.2項 「firstboot インストールのカスタマイズ」](#) (117 ページ)を参照してください。
- 3 マスタコンピュータのディスクを複製し、そのイメージをクライアントのディスクに展開します。詳細については、[6.3項 「マスタインストールの複製」](#) (125 ページ)を参照してください。
- 4 エンドユーザに対して、各自の要件に合わせてSUSE Linux Enterpriseの環境設定を行わせます。詳細については、[6.4項 「インストールの個人設定」](#) (125 ページ)を参照してください。

6.1 マスタマシンの準備

firstbootワークフロー用のマスタマシンを準備するには、以下の手順に従ってください。

- 1 インストールメディアをマスタコンピュータに挿入します。
- 2 コンピュータを起動します。
- 3 標準のインストールと必要なすべての設定作業を行い、そのコンピュータのブートが完了するまで待ちます。yast2-firstboot パッケージもインストールします。
- 4 エンドユーザ用のYaST環境設定ワークフローの定義したり、このワークフローに独自のYaSTモジュールを追加する場合は、[6.2項「firstbootインストールのカスタマイズ」](#) (117 ページ)に進んでください。それ以外の場合は、[ステップ 5](#) (116 ページ)に進んでください。
- 5 rootとしてfirstbootを有効にします。
 - 5a firstboot実行の契機となる空のファイル/etc/reconfig_systemを作成します。firstbootの環境設定が正しく完了すると、このファイルは削除されます。このファイルを作成するには、次のコマンドを使用します。

```
touch /etc/reconfig_system
```
 - 5b YaSTのランレベルエディタを使って、firstbootサービスを有効にします。
- 6 [6.3項「マスタインストールの複製」](#) (125 ページ)に進みます。

6.2 firstbootインストールのカスタマイズ

firstbootインストールのカスタマイズには、さまざまなコンポーネントが含まれます。それらのカスタマイズは省略することもできます。何も変更を行わなかった場合、firstbootはデフォルトの設定を使ってインストールを行います。次のオプションを指定できます。

- ユーザへのメッセージのカスタマイズについては、[6.2.1項「YaSTメッセージのカスタマイズ」](#) (118 ページ)を参照してください。
- ライセンス、およびライセンス動作のカスタマイズについては、[6.2.2項「ライセンス動作のカスタマイズ」](#) (119 ページ)を参照してください。
- 表示するリリースノートのカスタマイズについては、[6.2.3項「リリースノートのカスタマイズ」](#) (119 ページ)を参照してください。
- インストールに入れるコンポーネント、およびその順序をカスタマイズする場合は、[6.2.4項「ワークフローのカスタマイズ」](#) (120 ページ)を参照してください。
- オプションスクリプトの設定については、[6.2.5項「追加スクリプトの設定」](#) (125 ページ)を参照してください。

これらのコンポーネントをカスタマイズするには、次の環境設定ファイルを編集します。

```
/etc/sysconfig/firstboot
```

リリースノート、スクリプト、およびライセンス動作など、firstbootの環境設定を行います。

```
/etc/YaST2/firstboot.xml
```

コンポーネントを有効/無効にしたり、カスタムコンポーネントを追加して、インストールワークフローの環境設定を行います。

6.2.1 YaSTメッセージのカスタマイズ

デフォルトでは、SUSE Linux Enterpriseのインストールにはさまざまなデフォルトメッセージが含まれています。これらのメッセージは、インストールの進み具合に応じて適宜表示されます。たとえば、歓迎のメッセージ、ライセンスメッセージ、およびインストールの完了を知らせるメッセージなどが含まれます。これらのメッセージを独自のメッセージに変更したり、翻訳したメッセージを入れることができます。独自の歓迎メッセージを入れるには、以下の手順に従ってください。

- 1 rootとしてログインします。
- 2 環境設定ファイル/etc/sysconfig/firstbootを開いて、次の変更を行います。
 - 2a FIRSTBOOT_WELCOME_DIRに、歓迎メッセージとローカライズ版を含むファイルを保存するディレクトリパスを設定します。次に例を示します。

```
FIRSTBOOT_WELCOME_DIR="/usr/share/firstboot/"
```

- 2b 歓迎メッセージのファイル名がwelcome.txtおよびwelcome_locale.txt (localeは「cs」や「de」などのISO 639言語コードに一致する)以外の場合、ファイル名のパターンをFIRSTBOOT_WELCOME_PATTERNSで指定してください。たとえば、次のようにします。

```
FIRSTBOOT_WELCOME_PATTERNS="mywelcome.txt"
```

このパラメータを設定しない場合、デフォルトのwelcome.txtが使用されます。

- 3 歓迎メッセージファイルとそのローカライズ版を作成し、それを環境設定ファイル/etc/sysconfig/firstbootに指定されているディレクトリに保管します。

ライセンスメッセージやインストール完了メッセージも、同じような方法でカスタマイズすることができます。これらの変数は、それぞれ

FIRSTBOOT_LICENSE_DIR(ライセンス)およびFIRSTBOOT_FINISH_FILE(完了)になります。

6.2.2 ライセンス動作のカスタマイズ

ユーザが使用許諾契約に同意しない場合のインストールシステムの動作をカスタマイズすることができます。使用許諾契約に同意しないユーザに対するシステムの動作は、3種類用意されています。

halt

firstbootインストールを中止し、システムをシャットダウンします。デフォルトの設定です。

continue

firstbootインストールを続行します。

abort

firstbootインストールを中止しますが、ブートを試みます。

動作を決めたら、LICENSE_REFUSAL_ACTIONに適切な値を設定します。

6.2.3 リリースノートのカスタマイズ

firstbootを使って展開するSUSE Linux Enterpriseのインスタンスの変更内容に応じて、エンドユーザに適切な情報や重要な情報を知らせる必要があります。標準インストールでは、ユーザに重要な情報を知らせるために、リリースノートを使用します。リリースノートは、インストール完了時に表示されます。firstbootのインストール完了時に、独自のリリースノートを表示するには、以下の手順に従ってください。

- 1 独自のリリースノートファイルを作成します。 /usr/share/doc/release-notesにあるサンプルファイルのようなRTF形式を使用して、結果をRELEASE-NOTES.en.rtfファイルに保存してください。
- 2 オプションのローカライズ版をオリジナル版の次に保存し、ファイル名のenの部分を該当するISO 639言語コードに置き換えます。たとえば、日本語版の場合はjaになります。

- 3 `/etc/sysconfig/firstboot`にある**firstboot**環境設定ファイルを開いて、`FIRSTBOOT_RELEASE_NOTES_PATH`にリリースノートを保存したディレクトリを指定します。

6.2.4 ワークフローのカスタマイズ

デフォルトでは、標準の**firstboot**ワークフローには、次のコンポーネントが含まれています。

- 言語の選択
- ようこそ
- 使用許諾契約
- ホスト名
- Network
- 日付と時刻
- Desktop
- rootのパスワード
- ユーザ認証方法
- ユーザ管理
- ハードウェア設定
- セットアップの完了

この**firstboot**インストールワークフローの標準レイアウトは、必須ではありません。特定のコンポーネントを有効/無効にしたり、独自のモジュールをワークフローにフックすることができます。 **firstboot**ワークフローを変更するには、**firstboot**環境設定ファイル`/etc/YaST2/firstboot.xml`を編集します。このXMLファイルは、YaSTがインストールワークフローを制御するために使用する標準の`control.xml`ファイルのサブセットになります。

firstbootインストールワークフローの変更の概要を次に示します。ここには、firstboot環境設定ファイルの基本的な文法、および主要要素の設定内容なども含まれています。

例 6.1 提案画面の設定

```
...
<proposals config:type="list">❶
  <proposal>❷
    <name>firstboot_hardware</name>❸
    <mode>installation</mode>❹
    <stage>firstboot</stage>❺
    <label>Hardware Configuration</label>❻
    <proposal_modules config:type="list">❼
      <proposal_module>printer</proposal_module>❽
    </proposal_modules>
  </proposal>
</proposal>
...
</proposals>
```

- ❶ firstbootワークフローの一部となるすべての提案用のコンテナです。
- ❷ 個人提案用のコンテナです。
- ❸ 提案の内部名です。
- ❹ この提案のモードです。ここは変更しないでください。firstbootインストールを行う場合、installationと設定する必要があります。
- ❺ この提案を行う、インストールプロセスのステージです。ここは変更しないでください。firstbootインストールを行う場合、firstbootと設定する必要があります。
- ❻ 提案に表示するラベルです。
- ❼ 提案画面の一部となるすべてのモジュール用コンテナです。
- ❽ 提案画面の一部となる、1つまたは複数のモジュールです。

firstboot環境設定ファイルの次のセクションは、ワークフロー定義から成り立っています。ここには、firstbootインストールワークフローの一部とするすべてのモジュールを記載する必要があります。

例 6.2 Workflow(ワークフロー)セクションの設定

```
<workflows config:type="list">
  <workflow>
    <defaults>
      <enable_back>yes</enable_back>
      <enable_next>yes</enable_next>
      <archs>all</archs>
    </defaults>
    <stage>firstboot</stage>
    <label>Configuration</label>
    <mode>installation</mode>
    ... <!-- list of modules -->
    </modules>
  </workflow>
</workflows>
...
```

workflowセクションの全体的な構造は、proposalセクションと似ています。コンテナには、ワークフロー要素が保持されます。ワークフロー要素には、例 6.1.「提案画面の設定」(121 ページ)で説明している提案と同様に、ステージ、ラベル、およびモード情報などが含まれます。一番大きな違いは、defaultsセクションです。このセクションには、ワークフローコンポーネントの基本的なデザイン情報が含まれています。

enable_back

すべてのダイアログに、[Back(戻る)] ボタンを入れます。

enable_next

すべてのダイアログに、[Next(次へ)] ボタンを入れます。

archs

このワークフローを使用するハードウェアアーキテクチャを指定します。

例 6.3 ワークフローコンポーネントリストの設定

```
<modules config:type="list">❶
  <module>❷
    <label>Language</label>❸
    <enabled config:type="boolean">false</enabled>❹
    <name>firstboot_language</name>❺
  </module>
</modules>
```


- ❶ ワークフローの全コンポーネントのコンテナです。
- ❷ モジュール定義です。
- ❸ モジュールと一緒に表示するラベルです。
- ❹ ワークフローでこのコンポーネントを有効/無効にするためのスイッチです。
- ❺ モジュール名です。モジュールは、`/usr/share/YaST2/clients`にファイル拡張子`.ycp`で保管する必要があります。

firstbootインストール時の提案画面数または表示順序を変更するには、以下の手順に従ってください。

- ❶ `/etc/YaST2/firstboot.xml`にある**firstboot**環境設定ファイルを開きます。
- ❷ 提案画面を追加、削除したり、既存の画面の順序を変更します。
 - 提案全体を削除するには、`proposal`セクションから`proposals`要素とそのサブ要素を削除して、ワークフローから対応する`module`要素とサブ要素を削除します。
 - 新しく提案を追加するには、新たに`proposal`要素を作成し、必要なサブ要素を指定します。提案が`/usr/share/YaST2/clients`の**YaST**モジュールとして存在するようにしてください。
 - 提案の順序を変更するには、ワークフロー内で該当する提案を含む`module`要素を移動します。特定の順序で提案やワークフローコンポーネントを実施しなければならないような、他のインストールステップとの依存関係がある場合もあることに注意してください。

- ❸ 変更内容を反映し、環境設定ファイルを閉じます。

デフォルト設定がニーズに合わない場合は、環境設定ステップのワークフローを随時変更することができます。ワークフロー内の適切なモジュールを有効/無効にしたり、独自のカスタムモジュールを追加してください。

firstbootワークフローのモジュールのステータスを切り替えるには、以下の手順に従ってください。

- 1 `/etc/YaST2/firstboot.xml`環境設定ファイルを開きます。
- 2 モジュールを無効にする場合は、`enabled`要素の値を、`true`から`false`に変更します。有効にする場合は、`false`から`true`に変更します。

```
<module>
  <label>Time and Date</label>
  <enabled config:type="boolean">true</enabled>
  <name>firstboot_timezone</name>
</module>
```

- 3 変更内容を反映し、環境設定ファイルを閉じます。

独自のカスタムモジュールをワークフローに追加するには、以下の手順に従ってください。

- 1 独自のYaSTモジュールを作成し、ファイル名`module_name.ycp`で`/usr/share/YaST2/clients`に保存します。
- 2 `/etc/YaST2/firstboot.xml`環境設定ファイルを開きます。
- 3 このモジュールを実行するワークフロー内のポイントを決定します。そのためには、ワークフロー内の他のステップとの依存関係を検討し、必要に応じてそれを解消する必要があります。
- 4 `modules`コンテナ内に新たな`module`要素を作成し、適切なサブ要素を追加します。

```
<modules config:type="list">
  ...
  <module>
    <label>my_module</label>
    <enabled config:type="boolean">true</enabled>
    <name>filename_my_module</name>
  </module>
</modules>
```

- 4a `label`要素に、モジュールで表示するラベルを入力します。
- 4b ワークフロー内にモジュールを入れるために、`enabled`に`true`が設定されていることを確認します。

- 4c** name要素に、モジュールのファイル名を入力します。このときに、フルパスと拡張子.ycpは省略してください。

- 5** 設定内容を反映し、環境設定ファイルを閉じます。

ティップ: 詳細情報

YaST開発の詳細は、<http://developer.novell.com/wiki/index.php/YaST>を参照してください。

6.2.5 追加スクリプトの設定

firstbootワークフローの実行完了後に、他のスクリプトを実行するように設定できます。firstbootシーケンスに他のスクリプトを追加するには、以下の手順に従ってください。

- 1** /etc/sysconfig/firstboot環境設定ファイルを開いて、SCRIPT_DIRに指定されているパスが正しいことを確認します。デフォルトは/usr/share/firstboot/scriptsです。
- 2** シェルスクリプトを作成し、指定したディレクトリに保存します。次に、そのファイルに適切なファイルパーミッションを設定します。

6.3 マスタインストールの複製

利用できる任意のイメージング機能を使って、マスタコンピュータのディスクを複製し、そのイメージをターゲットコンピュータに展開/配布します。

6.4 インストールの個人設定

複製されたディスクイメージがブートされると、firstbootが開始され、**6.2.4項「ワークフローのカスタマイズ」** (120 ページ)で設計したようにインストールが開始されます。firstbootワークフロー設定に含まれているコンポーネントだけが開始されます。他のインストールステップはスキップされます。エンド

ユーザは、言語、キーボード、ネットワーク、およびパスワードを各自の要件に応じて設定し、ワークステーションの個人設定を行います。作業が完了すると、システムは他のSUSE Linux Enterpriseインスタンスと同様に動作します。

高度なディスクセットアップ

高性能のシステム設定を行うには、特定のディスクセットアップが必要となります。すべての一般的なパーティション関連作業は、YaSTを使って行えます。ブロックデバイスで固定的なデバイス名を取得するには、`/dev/disk/by-id/`下のブロックデバイス名を使用します。LVM (Logical Volume Management)は、ディスクパーティショニング用のスキーマで、標準的なセットアップで使用する物理パーティショニングよりもずっと柔軟性が高くなるように設計されています。そのスナップショット機能を利用すれば、簡単にデータバックアップを作成できます。RAID(Redundant Array of Independent Disks)を使用すれば、データの整合性、パフォーマンス、および耐障害性が向上します。SUSE® Linux Enterprise Serverは、マルチパスI/Oもサポートしています。詳細は、『Storage Administration Guide』のマルチパスI/Oに関する章を参照してください。SUSE Linux Enterprise 10からは、iSCSIをネットワークディスクとして使用するためのオプションも用意されています。iSCSIの詳細については、[第12章 IP ネットワークの大容量記憶デバイス—iSCSI](#) (297 ページ)を参照してください。

7.1 LVMの設定

このセクションでは、LVMの基本原則と様々な状況で役立つ基本的な機能を簡単に説明します。[7.1.2項 「YaSTによるLVMの設定」](#) (130 ページ)では、YaSTを使用したLVMのセットアップ方法を学びます。

警告

LVMを使用することでデータ損失などの危険性が増加する恐れがあります。この危険性にはアプリケーションのクラッシュ、電源障害、誤ったコマンドなども含まれます。LVMまたはボリュームの再設定を実施する前にデータを保存してください。バックアップなしでは作業を実行しないでください。

7.1.1 論理ボリュームマネージャ(LVM)

論理ボリュームマネージャ(LVM)は、複数のファイルシステム上でハードディスクスペースを柔軟に割り振ることができます。これは、インストール中の初期パーティショニングを終了した後になってハードディスクスペースの区分を変更する必要がある場合として発生するために開発されました。稼働中のシステムでパーティションを変更することは困難なため、LVMは必要に応じて論理ボリューム(LV)を作成できるメモリスペースの仮想プール(ボリュームグループ(VG))を提供します。オペレーティングシステムは物理パーティションの代わりにこれらのLVにアクセスします。ボリュームグループは2つ以上のディスクを使用することができます。また、複数のディスクまたはその一部が連続した1つのVGを形成することも可能です。この方法でLVMは物理ディスクスペースから一種の抽象層を提供します。この抽象層により、物理的にパーティショニングを再度行うよりもより簡単かつ安全な方法で区分に変更を加えられるようになります。物理パーティショニングに関連する背景情報についてはパーティションのタイプ項 (174 ページ)および8.5.7項「YaSTパーティション分割ツールの使用」 (172 ページ)を参照してください。

図 7.1 物理パーティショニング対LVM

ディスク			ディスク 1		ディスク 2		
PART	PART	PART	PART	PART	PART	PART	PART
			VG 1		VG 2		
			LV 1	LV 2	LV 3	LV 4	
MP	MP	MP	MP	MP	MP	MP	

図7.1.「物理パーティショニング対LVM」(128 ページ)では物理パーティショニング(左)とLVM区分(右)を比較しています。左側は、1つのディスクが割り当てられたマウントポイント(MP)をもつ3つの物理パーティション(PART)に分かれています。これによりオペレーティングシステムはそれぞれのパーティションにアクセスできます。右側では2つのディスクがそれぞれ3つの物理パーティションに分かれています。2つのLVMボリュームグループ(VG1およびVG2)が定義されています。VG1にはDISK1とDISK2の2つのパーティションが含まれます。VG2はDISK2の2つのパーティションを除いた残り部分になります。LVMではボリュームグループに組み込まれた物理ディスクパーティションは物理ボリューム(PV)と呼ばれます。ボリュームグループ内に4つの論理ボリューム(LV1からLV4)が定義されています。これらのボリュームは、それぞれに関連づけられたマウントポイントを介してオペレーティングシステムに使用されます。別の論理ボリュームとの境界とパーティションの境界を並べることはできません。この例ではLV1およびLV2の間に境界があります。

LVMの機能:

- 複数のハードディスクまたはパーティションを大きな論理ボリュームにまとめることができます。
- 提供された設定が適切であれば、LV(/usrなど)は空きスペースがなくなったときに拡張することができます。
- LVMを使用することで、実行中のシステムにハードディスクまたはLVを追加できます。ただし、こうしたディスクやLVを追加するには、ホットスワップ可能なハードウェアが必要になります。
- 複数の物理ボリューム上に論理ボリュームのデータストリームを割り当てる「ストライピングモード」を有効にすることもできます。これらの物理ボリュームが別のディスクに存在する場合、RAID0と同様に読み込みおよび書き込みのパフォーマンスを向上できます。
- スナップショット機能は稼働中のシステムで一貫性のある(特にサーバ)バックアップを取得できます。

これらの機能とともにLVMを使用することは、頻繁に使用されるホームPCや小規模サーバではそれだけでも意義があります。データベース、音楽アーカイブ、ユーザディレクトリなどの増え続けるデータストックがある場合は、LVMが最適と言えます。LVMは物理ハードディスクより大きなファイルシステムを利用できます。LVMのもう1つの利点は最大256個のLVを追加できることです。ただし、LVMでの作業は従来のパーティションでの作業とは異なる

ことに留意してください。LVMの設定についての指示および詳しい情報は <http://tldp.org/HOWTO/LVM-HOWTO/> の公式LVM HOWTOからご利用いただけます。

カーネルバージョン2.6から開始して、LVMバージョン2を利用することができます。これはLVMの前バージョンとの下方互換になり、これまでのボリュームグループを管理できるようにします。新しいボリュームグループを作成する場合は、新しいフォーマットまたは下方互換バージョンのどちらを使用するか決定します。LVM 2にはいずれのカーネルパッチも必要ありません。これは、カーネル2.6に統合されているデバイスマッパーを活用しています。このカーネルはLVMバージョン2のみをサポートしています。そのため、このセクションでLVMと書かれている場合、それはLVMバージョン2を指しています。

LVM 2のかわりにEVMS (Enterprise Volume Management System)を使用できます。EVMSは論理ボリュームとRAIDボリュームに一般的なインタフェースを提供します。LVM 2と同様、EVMSはカーネル2.6でデバイスマッパーを使用できるようにします。

7.1.2 YaSTによるLVMの設定

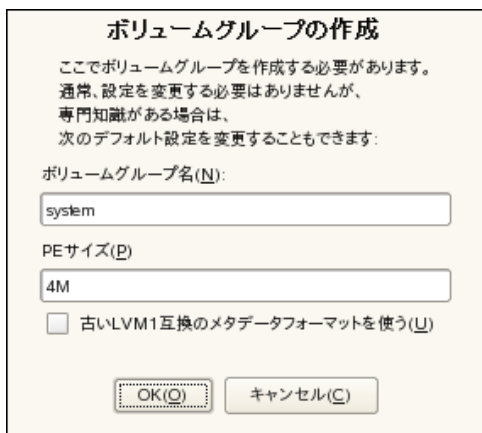
YaSTのLVM設定には、YaSTのパーティションモジュールのエキスパートページ(8.5.7項「**YaSTパーティション分割ツールの使用**」(172 ページ)を参照)からアクセスできます。このパーティショニングツールにより、既存のパーティションを編集、および削除できます。また、LVMで使用する新規パーティションを作成することもできます。次に [作成] >、[Do not format(フォーマットしない)] を最初にクリックし、続いて [0x8E Linux LVM] をパーティションIDとして選択します。LVMで使用するすべてのパーティションを作成した後、[LVM] をクリックして、LVMの設定を開始します。

ボリュームグループの作成

システムにまだボリュームグループが存在しない場合、ボリュームグループを追加するようにプロンプトされます(図 7.2. 「**ボリュームグループの作成**」(131 ページ)を参照)。[グループの追加] で追加グループを作成できますが、通常はボリュームグループは1つで十分です。systemは、SUSE Linux Enterprise®システムファイルが配置されるボリュームグループの名前として提案されています。物理エクステンツサイズではボリュームグループの物理

ブロックサイズを定義します。ボリュームグループにある全ディスクスペースはこの物理ブロックサイズ内で使用されます。この値は通常4MBに設定され、物理ボリュームおよび論理ボリュームには最大サイズとして256GB使用できます。物理エクステントは論理ボリュームとして256GB以上必要な場合のみ、8、16、32MBのように増やしてください。

図 7.2 ボリュームグループの作成



ボリュームグループの作成

ここでボリュームグループを作成する必要があります。
通常、設定を変更する必要はありませんが、
専門知識がある場合は、
次のデフォルト設定を変更することもできます:

ボリュームグループ名(N):
system

PEサイズ(P):
4M

☐ 古いLVM1互換のメタデータフォーマットを使う(U)

OK(O) キャンセル(C)

物理ボリュームの設定

いったんボリュームグループが作成されると、続くダイアログで「Linux LVM」または「Linux Native」のすべてのパーティションがリストされます。スワップパーティションまたはDOSパーティションは表示されません。パーティションがボリュームグループにすでに割り振られている場合、ボリュームグループの名前がリストに表示されます。割り当てられていないパーティションは、「--」で示されます。

複数のボリュームグループが存在する場合は、選択ボックスで現在のボリュームグループを左上に設定します。右上にあるボタンは追加ボリュームグループの作成および既存ボリュームグループの削除を実行します。ボリュームグループのパーティションが未割り当ての場合のみ、そのボリュームグループを削除できます。ボリュームグループに割り当てられたすべてのパーティションも、同様に物理ボリューム(PV)として参照されます。

図 7.3 物理ボリュームの設定

物理ボリュームと呼ばれるパーティションをボリュームグループに追加します。

ボリュームグループは、仮想パーティションのような、論理パーティションから割り当てられる「ストレージプール」を形成します。

通常は、ボリュームグループを複数作成する必要はありません。特別な理由で複数作成する必要がある場合は、ここで作成します。各ボリュームグループには、そのボリュームグループに属するパーティションが1つ以上必要です。

1つの物理ボリュームは、1つのボリュームグループに属します。すべてのパーティションをLinux LVMを使用してボリュームグループに割り当てます。

さらに、ボリュームグループに論理ボリュームが含まれていなければ、ボリュームグループを削除することもできます。

論理ボリュームマネージャ: 物理ボリューム設定

ボリュームグループ(G)
system

サイズ: 9.9 GB

グループの削除(G)

グループの追加(D)

デバイス	サイズ	タイプ	ボリュームグループ
/dev/hdb	10.0 GB	—	system

ボリュームの追加(A)

ボリュームの削除(R)

戻る(B)

中止(E)

次へ(N)

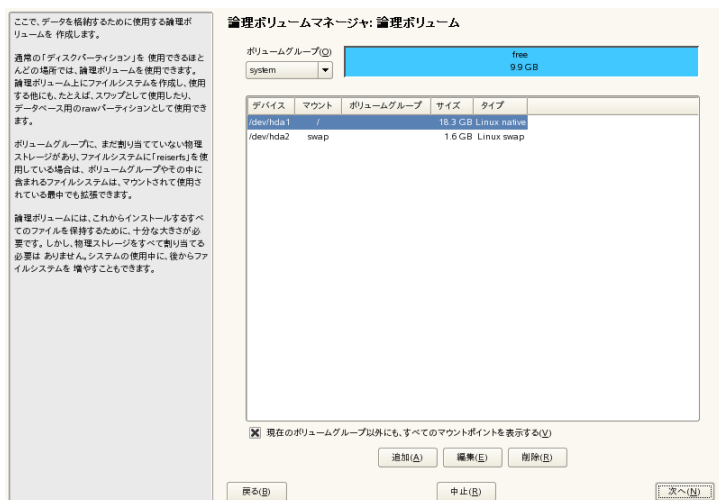
これまで未割り当てだったパーティションを選択したボリュームグループに追加するには、そのパーティションをクリックしてから [ボリュームの追加] をクリックします。この時点で、そのボリュームグループの名前が選択したパーティションの隣に入力されます。LVM用に予約されているパーティションをすべて1つのボリュームグループに割り当ててください。すべてのパーティションを割り当てないと、パーティションのスペースが未使用のまま残ります。ダイアログを終了する前に、すべてのボリュームグループを少なくとも1つの物理ボリュームに割り当ててする必要があります。すべての物理ボリュームを割り当て終えた後、[次へ] をクリックして論理ボリュームの設定に進みます。

物理ボリュームの設定

物理ボリュームにボリュームグループを設定し終えた後、次のダイアログでオペレーティングシステムが使用する論理ボリュームを定義します。現在のボリュームグループを選択ボックスで左上に設定します。設定したボリュームグループの隣に現在の空き領域が表示されます。下のリストにはボリュームグループの全論理ボリュームが表示されます。マウントポイントが割り当てられている通常の全Linuxパーティション、全スワップパーティション、既存の全論理ボリュームがここにリストされています。ボリュームグループのすべての領域がなくなるまで、必要に応じて論理ボリュームの [追加]、[編

集]、[削除]を実行します。各ボリュームグループに少なくとも1つの論理ボリュームを割り当ててください。

図 7.4 論理ボリューム管理



新しい論理ボリュームを作成するには[追加]をクリックし、開いたポップアップの内容を埋めます。パーティショニングの場合、サイズ、ファイルシステム、およびマウントポイントを入力します。通常、**ReiserFS**または**Ext2**などのファイルシステムは論理ボリューム上に作成され、マウントポイントを指定します。この論理ボリューム上に格納されたファイルは、インストールしたシステム上の該当するマウントポイントで検出することができます。さらに、複数の物理ボリューム上(ストライピング)に存在する論理ボリュームにデータストリームを分配することも可能です。これらの物理ボリュームが別のハードディスクに存在する場合、この性質により、読み込みおよび書き込みのパフォーマンスが向上します(**RAID 0**など)。ただし、**n**ストライプで**LV**をストライピングする場合、**LV**が必要とするハードディスクスペースが物理ボリューム**n**個に等しく配分されている場合にのみ、ストライプが正しく作成されます。たとえば、使用可能な物理ボリュームが2個だけの場合、3個の論理ボリュームを持つことはできません。

警告: ストライピング

YaSTには、現時点でストライピングの観点からエントリの正確性を確認する機会はありません。何か間違いがあった場合、それが明らかになるのはLVMがディスクに実装された後です。

図 7.5 論理ボリュームの作成

論理ボリュームの作成

フォーマット

☐ フォーマットしない(N)

☒ フォーマット(E)

ファイルシステム(S)

Reiser

オプション(P)

☐ 暗号ファイルシステム(E)

論理ボリューム名(N)

(例: var, opt)

サイズ(S): (例: 4.0 GB 210.0 MB)

2.4 GB

最大 = 9.9 GB

最大(Σ)

ストライプ(P)

1

ストライプサイズ(S)

64

Fstabオプション(I)

マウントポイント(M)

/home

OK(Q) キャンセル(C)

すでにシステム上にLVMを設定した場合、ここで既存の論理ボリュームを指定することができます。続行する前に、これらの論理ボリュームを適切なマウントポイントに割り当てます。[次へ]でYaSTのパーティションモジュールのエクスパートページに戻り、ここでの設定作業を完了します。

LVMの直接管理

LVMをすでに設定し、一部に変更を加えるのみの場合は、別の方法でLVMにアクセスすることができます。YaSTコントロールセンターで [システム]、> [LVM] の順に選択します。このダイアログでは基本的に、先に説明したアクションと同じことを実行できます。ただし物理パーティショニングは除きます。2つのリストに既存の物理ボリュームと論理ボリュームが表示されま

す。これにより、先に説明した方法を使用して、LVMシステムを管理できます。

7.1.3 EVMSを使ったストレージ管理

EVMS2(Enterprise Volume Management System 2)は、豊富な機能を備えた拡張性の高いボリュームマネージャで、クラスタにも対応しています。EVMSでは、プラグインを使って機能を追加したり、任意のパーティションタイプに対応させることができます。クラスタに対応しているEVMS2では、クラスタ中の各ノードにあるデバイスに同一の名前を付けて、管理を容易にすることができます。

EVMS2には、以下のストレージリソースを管理するために、一体化されたインタフェース(evmsguiとコマンドライン)が用意されています。

- iSCSIなど、ローカルメディア/SANベースのメディア上の物理ディスクと論理デバイス
- 高可用性を保つソフトウェアRAID0、1、4、および5
- 障害対策用クラスタ対応マルチパスI/O
- クラスタストレージオブジェクトとCSM(Cluster Segment Manager)プラグイン
- EVMS2用ファイルシステムインタフェースモジュール(FSIM)を含んだ全ファイルシステム用のボリューム
- ボリュームのスナップショット

SUSE Linux Enterprise Server 10での新機能には、次のようなものがあります。

- EVMS2とCLVM2(Cluster Linux Volume Manager 2)は、カーネル内で同じマルチディスク(MD)ドライバ、およびデバイスマAPPER(DM)ドライバを使用します。
- Heartbeat 2 Cluster ManagerとOracle Cluster File System 2では、ファイルシステムプラグインを使用できます。

EVMSデバイス

EVMS管理ユーティリティは、5種類の異なるレベルのデバイスを識別します。

Disks

最下位レベルのデバイスです。物理ディスクとしてアクセスされる可能性があるデバイスは、すべてディスクとして取り扱われます。

セグメント

セグメントは、ディスク上のパーティション、およびMBR (Master Boot Record)などの他のメモリ領域で構成されます。

コンテナ

LVM中のボリュームグループに相当します。

領域

利用可能なデバイスは、ここでLVM2とRAIDにグループ化されます。

Volumes

すべてのデバイスです。それが実パーティション、論理ボリューム、またはRAIDデバイスであるかどうかに関わらず、適切なマウントポイントからデバイスを利用することができます。

EVMSを使用する場合、デバイス名をEVMSデバイス名に変更する必要があります。単純なパーティションは/dev/evms/に、論理ボリュームは/dev/evms/lvm/に、RAIDデバイスは/dev/evms/mdにあります。ブート時にEVMSを有効にするには、YaSTランレベルエディタを使って、ブートスクリプトにboot.evmsを追加します。関連項目 [20.2.3項「YaSTでのシステムサービス\(ランレベル\)の設定」](#) (440 ページ)。

詳細情報

EVMSを使ったストレージリソースの管理方法は、『*Storage Administration Guide*』を参照してください。このガイドは、パッケージsles-stor_evms_enをインストールした後、/usr/share/doc/manual/sles-stor_evms_enから参照できます。また、SourceForge*が主催するEVMS project [<http://evms.sourceforge.net/>]にある『EVMS User Guide [http://evms.sourceforge.net/users_guide/』にも、EVMSに関する一般的な情報が記載されています。

7.2 ソフトウェアRAID設定

RAID (Redundant Array of Independent Disks)の目的は、複数のハードディスクパーティションを1つの大きい**仮想**ハードディスクに結合し、パフォーマンスとデータのセキュリティを最適化することです。ほとんどのRAIDコントローラはSCSIプロトコルを使用します。これは、IDEプロトコルも効率的な方法で多数のハードディスクのアドレスを指定でき、コマンドの平行処理に適しているからです。一方、IDEまたはSATAハードディスクをサポートしているRAIDコントローラもあります。ソフトウェアRAIDは、ハードウェアRAIDコントローラの追加購入することなく、RAIDシステムの利点を提供します。ただし、これにはいくらかのCPU時間を要し、高性能なコンピュータには適さないメモリ要件があります。

7.2.1 RAIDレベル

SUSE® Linux Enterpriseでは、YaSTを使用することにより、複数のハードディスクを1つのソフトウェアRAIDシステムに結合するオプションを提供します。これは、非常にリーズナブルな、ハードウェアRAIDの代替機能です。RAIDには、それぞれが異なる目標、利点、および属性を持ついくつかのハードディスクを1つのRAIDシステムに結合するためのいくつかの戦略が含まれています。これらは通常、**RAID**レベルと呼ばれます。

一般的なRAIDレベルは次のとおりです。

RAID 0

このレベルでは、各ファイルのブロックが複数のディスクドライブに分散されるので、データアクセスのパフォーマンスが向上します。このレベルはデータのバックアップを提供しないため、実際にはRAIDではありませんが、この種のシステムでは**RAID 0**という名前が一般的です。RAID 0では、2つ以上のハードディスクが互いにブールします。高いパフォーマンスが得られます。ただし、1つのハードディスクに障害が発生しただけで、RAIDシステムが破壊され、データは失われます。

RAID 1

このレベルでは、データが他のハードディスクに一対一でコピーされるため、データに対する適切なセキュリティが提供されます。これは、ハードディスクミラーリングとして知られています。一方のディスクが破壊された場合、そのディスク内容のコピーが他方のディスク上で利用できま

す。一方のディスクが破壊されても、データが危険にさらされることはありません。ただし、破壊が検出されない場合、破損したデータが適切なディスクにミラーされ、そのようにデータ破損が発生することもあります。単一ディスクアクセスを使用した場合を比較すると、コピー処理において書き込みのパフォーマンスが若干、低下しますが(10～20%遅くなる)、読み取りアクセスは通常の物理ハードディスクに比べ、大幅に速くなります。これは、データが複製されており、並列にスキャンできるためです。一般的に、レベル1は、単一ディスクのほぼ2倍の読み取りトランザクション速度と、単一ディスクとほぼ同じ書き込みトランザクション速度を提供します。

RAID 2およびRAID 3

これらは、一般的なRAID実装ではありません。レベル2では、データは、ブロックレベルではなく、ビットレベルでストライプ化されます。レベル3は、専用パリティディスクによってバイトレベルのストライプ化を提供しますが、複数の要求を同時にサービスすることはできません。両方のレベルとも、使用されることはまれです。

RAID 4

レベル4は、専用パリティディスクと結合されたレベル0と同様に、ブロックレベルのストライプ化を提供します。データディスク障害の場合、交換用ディスクを作成するために、パリティデータが使用されます。ただし、パリティディスクは、書き込みアクセスの場合に障害となる可能性があります。にもかかわらず、レベル4は時々使用されます。

RAID 5

RAID5は、レベル0とレベル1の間をパフォーマンスおよび冗長性の面で調整して、最適化したものです。ハードディスクスペースは、使用されるディスク数から1を引いたものに等しくなります。データは、RAID0の場合のようにハードディスク間で分散されます。パーティションの1つで作成されたパリティブロックがあるのは、セキュリティ上の理由からです。各パーティションはXORによって互いにリンクされているので、システム障害の場合に、内容が対応するパリティブロックによって再構築されます。RAID5の場合、同時に複数のハードディスクが障害を起こすことはありません。1つのハードディスクに障害がある場合は、そのハードディスクをできるだけ早く交換して、データ消失の危険性をなくす必要があります。

その他のRAIDレベル

他のRAIDレベル(RAIDn、RAID 10、RAID 0+1、RAID 30、RAID 50など)が開発されていますが、そのうちのいくつかはハードウェアベンダによって独自規格で作成される実装となります。これらのレベルは、広く使用されてはいないため、ここでの説明は省略します。

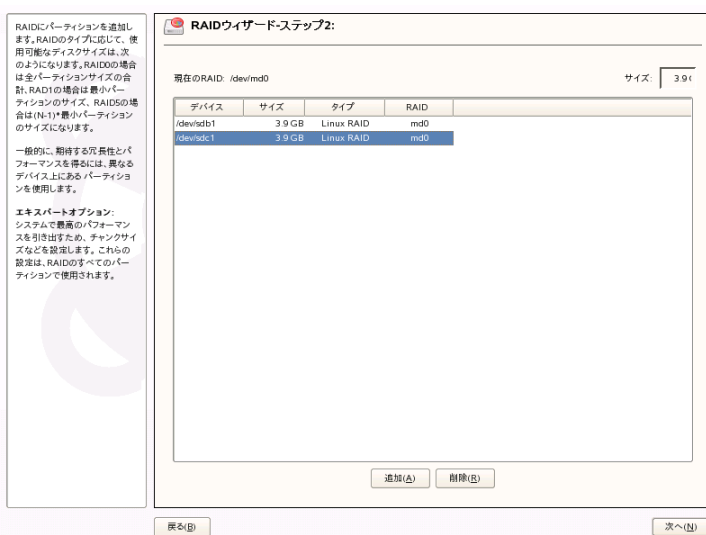
7.2.2 YaSTによるソフトウェアRAID設定

YaSTソフトウェアRAID設定には、YaST Expert Partitioner (8.5.7頁「[YaSTパーティション分割ツールの使用](#)」(172ページ)を参照)からアクセスできます。このパーティション設定ツールを使用すると、既存のパーティションを編集および削除したり、ソフトウェアRAIDで使用する新規パーティションを作成できます。ここでは、RAIDパーティションを作成します。最初に [作成] >

[Do not format (フォーマットしない)] の順にクリックし、次にパーティション識別子として [0xFD Linux RAID] を選択します。RAID 0およびRAID 1の場合、少なくとも2つのパーティションが必要です。RAID 1の場合、パーティションは2つだけです。RAID 5を使用する場合、少なくとも3つのパーティションが必要です。同じサイズのパーティションだけを使用するようにお勧めします。RAIDパーティションを異なるハードディスクに保存すると、1つが損傷した場合のデータ消失のリスクが削減され(RAID 1と5)、またRAID 0のパフォーマンスを最適化できます。RAIDで使用するすべてのパーティションを作成したら、[RAID] > [Create RAID (RAIDの作成)] の順にクリックして、RAID設定を開始します。

次のダイアログでは、RAIDレベル0、1、および5の間で選択します。詳細については、「[7.2.1 項「RAIDレベル」](#)」(137ページ)を参照してください。[次へ] をクリックすると、次のダイアログにタイプが「Linux RAID」または「Linux Native」であるすべてのパーティションのリストが表示されます([図7.6.「RAIDパーティション」](#) (140ページ)を参照)。スワップパーティションまたはDOSパーティションは表示されません。パーティションがRAIDボリュームにすでに割り当てられている場合は、RAIDデバイスの名前(たとえば/dev/md0)がリストに表示されます。割り当てられていないパーティションは、「-」で示されます。

図 7.6 RAIDパーティション



前に割り当てを解除したパーティションを、選択したRAIDボリュームに追加するには、そのパーティションをクリックしてから、**［ボリュームの追加］**をクリックします。この時点で、そのRAIDデバイスの名前が選択したパーティションの隣に入力されます。すべてのパーティションをRAID用の予約パーティションとして割り当てます。すべてのパーティションを割り当てないと、パーティションのスペースが未使用のまま残ります。すべてのパーティションを割り当てたら、**［次へ］**をクリックして、設定ダイアログに進みます。このダイアログではパフォーマンスを微調整できます(図 7.7. 「ファイルシステム設定」 (141 ページ)を参照)。

図 7.7 ファイルシステム設定

チャンクサイズ:
デバイスに書き込み可能な、データの最小単位。RAID 5の相応なチャンクサイズは128KBです。RAID 0では、32KBが指定しやすい値になります。RAID 1の場合、チャンクサイズはアレイに対して、それほど影響を与えません。

パリティアルゴリズム:
RAID5で使用されるパリティアルゴリズムです。プラッタを回転させるタイプの一般的なディスクであれば、「Leftasymmetric」が最大のパフォーマンスを実現します。

RAIDウィザード:ステップ3:

フォーマット

☐ フォーマットしない(N)

☒ フォーマット(F)

ファイルシステム(S)

Reiser

オプション(O)

☐ 暗号ファイルシステム(E)

RAIDタイプ(T)

raid1

チャンクサイズ(KB)(U)

4

パリティアルゴリズム(G)(RAID 5のみ)

leftasymmetric

Finalオプション(F)

マウントポイント(M)

/home

戻る(B)

完了(F)

従来のパーティションの場合と同様の設定以外だけでなく、暗号化とRAIDボリュームのマウントポイントを使用するように、ファイルシステムを設定します。[完了]をクリックして設定を完了した後、エキスパートパーティション内のRAIDとマークされた/dev/md0デバイスと他のデバイスを観察してください。

7.2.3 トラブルシューティング

/proc/mdstatsファイルを調べて、RAIDパーティションが破壊されているかどうかを調べます。システム障害が発生した場合は、Linuxシステムをシャットダウンして、問題のあるハードディスクを、同じ方法でパーティション分割されている新しいハードディスクで置き換えます。次に、システムを再起動して、mdadm /dev/mdX --add /dev/sdXコマンドを入力します。「X」を使用しているデバイス識別子に置き換えてください。これにより、ハードディスクがRAIDシステムに自動的に統合され、そのRAIDシステムが完全に再構築されます。

7.2.4 詳細情報

ソフトウェアRAIDの設定方法と詳細情報が、次のHOWTOにあります。

- http://www.novell.com/documentation/sles10/stor_evms/data/bookinfo.html
- `/usr/share/doc/packages/mdadm/Software-RAID.HOWTO.html`
- <http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html>

Linux RAIDメーリングリストも使用できます。たとえば、<http://marc.theaimsgroup.com/?l=linux-raid&r=1&w=2>などがあります。

YaSTでのシステム設定

SUSE Linux Enterpriseでは、YaSTはインストールとシステムの設定の両方を処理します。この章ではシステムコンポーネント(ハードウェア)の設定、ネットワークアクセス、セキュリティ設定、およびユーザ管理について説明します。テキストベースのYaSTインターフェースの概要は、[8.12項「テキストモードのYaST」](#) (207 ページ)を参照してください。手動によるシステム設定の説明については、[20.3項「/etc/sysconfigによるシステム設定」](#) (441 ページ)を参照してください。

さまざまなYaSTモジュールを使って、YaSTでシステムを設定します。ハードウェアプラットフォームおよびインストール済みのソフトウェアに応じて、YaSTがインストールされたシステムへのアクセス方法は異なります。

KDEまたはGNOME内で、メインメニューからYaSTコントロールセンターを起動します。YaSTがシステムファイルを変更するには、システム管理者の権限が必要なので、YaSTの開始前に、rootのパスワードを入力するように要求されます。

コマンドラインからYaSTを起動するには、コマンド「su」(rootユーザに変更するため)と入力してから、「yast2」と入力します。テキストバージョンを起動するには、「yast2」ではなく、「yast」と入力します。また、「yast」コマンドを使用すると、仮想コンソールの1つからプログラムを起動することもできます。

独自のディスプレイデバイスをサポートしないハードウェアプラットフォームの場合、または他のホストをリモート管理する場合は、YaSTをリモートで実行します。最初に、YaSTを表示するホスト上のコンソールを開き、「ssh

-X root@<system-to-configure>」コマンドを入力してrootを設定するためにシステムにログインし、Xサーバ出力を自分の端末にリダイレクトします。SSHログインが成功したら「yast2」と入力して、グラフィカルモードでYaSTを起動します。

他のシステム上で、YaSTをテキストモードで起動するには、ssh root@<system-to-configure>コマンドを使用して接続を開きます。その後、yastを使用してYaSTを起動します。

時間節約のため、個別のYaSTモジュールを直接起動できます。モジュールを起動するには、「yast2 module_name」と入力します。「yast2 -l」または「yast2 --list」と入力して、システムで使用可能になっているすべてのモジュールのリストを表示します。たとえば、「yast2 lan」と入力して、ネットワークモジュールを起動します。

8.1 YaST言語

YaSTが使用する言語を変更するには、YaSTコントロールセンターの中で、[システム] > [言語の選択] の順に選択します。言語を選択した後、YaSTコントロールセンターを終了し、システムからログアウトしてから再度ログインします。次回YaSTを起動したときから、新しい言語設定が使用されます。これにより、システム全体の言語も変更されます。

別の言語で作業したいけれども、このシステムの言語設定を変更したくない場合は、YaSTを実行してLANG変数に使用する言語を設定してください。langcode_statecodeの形式で、長い言語コードを指定します。たとえば、米語の場合はLANG="en_US" yast2と入力します。

このコマンドを実行すると、指定された言語でYaSTが起動します。指定した言語は、そのYaSTセッション中のみ有効です。ターミナル、他のユーザ、および他のセッションで使用する言語には、何の影響もありません。

SSHでYaSTをリモートで実行する場合は、YaSTはローカルシステムの言語設定を使用します。

8.2 YaSTコントロールセンター

グラフィカルモードでYaSTを起動する場合、「[図 8.1. 「YaSTコントロールセンター」](#) (145 ページ)」に示すように、YaSTコントロールセンターが開きます。左のフレームには利用可能なカテゴリが含まれます。カテゴリの1つをクリックすると、右側のフレームにその内容がリストされます。そこから、目的のモジュールを選択します。たとえば、[ハードウェア]を選択し、右側のフレームの[サウンド]をクリックすると、サウンドカード用の設定ダイアログが開きます。各項目を設定するには、通常複数の処理を実行する必要があります。[次へ]をクリックして、次の処理手順に進みます。

ほとんどのモジュールで、左側のフレームにはヘルプテキストが表示され、そのヘルプには設定に関する提案および必要なエントリの説明が含まれます。ヘルプのフレームなしでモジュールのヘルプを表示するには、F1キーを押すか、[ヘルプ]を選択します。必要な設定を選択したあとに、設定ダイアログの最後で[承認]をクリックして処理を完了します。この時点で設定が保存されます。

図 8.1 YaSTコントロールセンター



注意: YaSTソフトウェア管理GtkおよびQtフロントエンド

システムにインストールされているデスクトップに応じて、YaSTには2つのフロントエンドが用意されています。デフォルトで、YaST gtkフロントエン

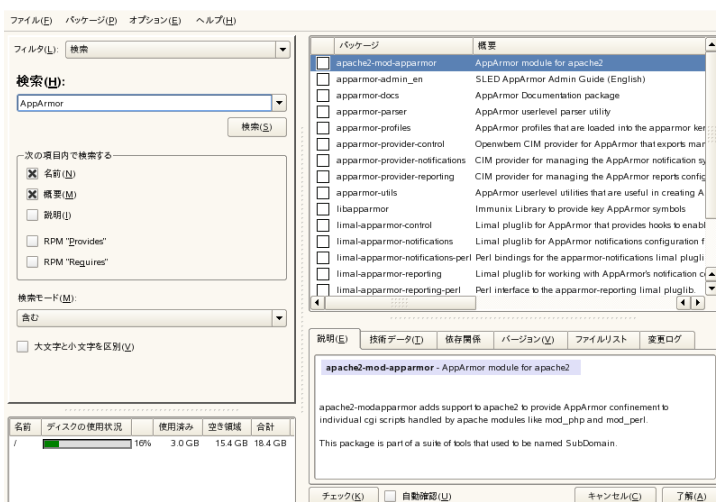
ドがGNOMEデスクトップで実行され、YaST qtフロントエンドがもう1つのデスクトップで実行されます。これは/sbin/yast2スクリプトのWANT_UI変数で定義されます。gtkフロントエンドの機能はマニュアルで説明されているqtフロントエンドと非常によく似ています。例外はgtkソフトウェア管理モジュールで、これはqtポートと大きく異なります。

8.3 ソフトウェア

8.3.1 ソフトウェアのインストールと削除

マシン上へのソフトウェアのインストール、アンインストール、および更新を行うには、[ソフトウェア] > [ソフトウェアの管理] を使用します。これにより、「[図 8.2. 「YaSTパッケージマネージャ」 \(146 ページ\)](#)」に表示されているように、パッケージマネージャダイアログが開きます。

図 8.2 YaSTパッケージマネージャ



SUSE® Linux Enterpriseでは、ソフトウェアはパッケージの形で用意されています。通常、パッケージコンテナには、プログラム、環境設定ファイル、および関連ドキュメントなど、そのプログラムに必要なすべてのものが含まれています。個々のパッケージのリストが、個々のパッケージウィンドウの右

側に表示されます。このリストの内容は現在選択されているフィルタにより決定されます。たとえば、[Patterns] フィルタが選択されている場合、個々のパッケージウィンドウは現在選択されているすべてのパッケージを表示します。

パッケージマネージャでは、各パッケージは、パッケージで実行する事柄を決定するステータスを持ちます。ステータスには、「インストール」や「削除」などがあります。」このステータスは行の先頭にあるステータスボックス内に記号で表示されます。項目を右クリックしたときに表示されるメニューから、該当のステータスをクリックまたは選択することにより、ステータスを変更できます。状況によっては、いくつかの潜在的なステータスフラグを選択できません。たとえば、まだインストールしていないパッケージに、「削除」フラグを設定することはできません。」使用可能なステータスフラグを表示するには、[ヘルプ] > [シンボル] の順に選択します。

個々のパッケージウィンドウのさまざまなパッケージに使用されるフォントカラーは、追加の情報を提供します。インストールメディア上にあるより新しいバージョンが使用できるインストール済みのパッケージは、青で表示されます。インストールメディア上にあるパッケージのバージョン番号がインストール済みのパッケージよりも新しい場合、赤で表示されます。ただし、パッケージのバージョン番号は、新しいバージョン番号が大きくなるとは限らないため、バージョン情報は正しくない可能性があります。問題を引き起こすパッケージを示すには十分なはずですが、必要ならば、バージョン番号をチェックします。

インストールするパッケージ

パッケージをインストールするには、インストールするパッケージを選択し、[承認] をクリックします。選択されたパッケージには、[インストール] ステータスアイコンが表示されるはずです。パッケージマネージャは自動的に依存関係をチェックし、他に必要なパッケージがあれば選択します(依存関係の解決)。[承認] をクリックする前にインストールに必要な他のパッケージを表示するには、メインメニューから [エクストラ] > [自動パッケージ変更を表示する] の順に選択します。パッケージをインストールした後は、[Install More (さらにインストールする)] をクリックしてパッケージマネージャの使用を続行するか、[完了] をクリックしてそれを終了します。

パッケージマネージャはインストール用にあらかじめ選択されたグループを提供します。個々のパッケージの代わりにグループ全体を選択することもで

きます。これらのグループを表示するには、左のフレームの [フィルタ] を使用します。

ティップ: すべての利用可能なパッケージのリスト

インストールメディア上のすべてのパッケージを表示するには、フィルタ [Package Groups] (パッケージグループ)を使って、ツリーの下部にある [zzz All] (すべて)を選択します。SUSE Linux Enterpriseには、さまざまなパッケージが含まれているため、すべてのパッケージを表示するために少し時間がかかることがあります。

パターンのインストールと削除

[Patterns] フィルタは、ファイルやプリントサーバなどのアプリケーションの目的に従って、プログラムパッケージをグループ化します。[Patterns] フィルタのさまざまなグループがインストールされたパッケージとともにリストされています。

この選択をインストールまたはアンインストールするには、行の先頭にあるステータスボックスをクリックします。パターンを右クリックして直接ステータスを選択すると、コンテキストメニューを使用できます。現在のパターンに含まれるパッケージが表示している右側の個々のパッケージ概要から、個々のパッケージを選択または選択解除します。

言語サポートのインストールと削除

プログラムのユーザインターフェース用に翻訳されたテキスト、ドキュメント、フォントなど、言語固有のパッケージを見つけるには、[言語] フィルタを使用します。このフィルタでは、SUSE Linux Enterpriseによりサポートされるすべての言語のリストが表示されます。これらのうちの1つを選択すると、右側のフレームに、選択した言語で使用可能なすべてのパッケージが表示されます。これらの中で、現在のソフトウェア選択にあてはまるすべてのパッケージに、自動的にインストール用のタグが付けられます。

システムから言語をアンインストールするには、言語リストから目的の言語を選択して、行の先頭にあるステータスボックスの選択を解除してください。

注意

言語が指定されたパッケージは他のパッケージに依存するため、パッケージマネージャはインストールに追加のパッケージを選択する場合があります。

パッケージとインストールソース

特定のリソースからパッケージだけを検出したい場合、`[インストールソース]` フィルタを使用します。デフォルト設定では、このフィルタは選択されたソースからすべてのパッケージのリストを表示します。リストを絞り込むには、2番目のフィルタを使用します。

選択されたインストールソースからすべてのインストール済みパッケージのリストを表示するには、`[インストールソース]` フィルタを選択し、`[Secondary Filters]` から `[インストール概要]` を選択し、チェックボックスから `[Keep]` 以外のすべてのチェックをはずします。

通常、個々のパッケージウィンドウのパッケージステータスは変更できます。ただし、変更したパッケージは検索条件に当てはまらなくなる可能性があります。そのようなパッケージをリストから削除するには、`[リストの更新]` を使用してリストを更新します。

ソースパッケージのインストール

プログラム用のソースファイルを含むパッケージが通常利用可能です。ソースファイルはプログラムを実行するためには必要ありませんが、プログラムのカスタムバージョンをコンパイルするには、ソースをインストールします。

選択されたプログラム用にソースをインストールするには、`[Source (ソース)]` 列にあるチェックボックスを有効にします。チェックボックスが表示されない場合は、インストールソースにパッケージのソースが含まれていません。

パッケージ選択の保存

複数のコンピュータ上に同じパッケージをインストールしたい場合は、設定をファイルに保存し、他のシステムに使用できます。パッケージ選択を保存

するには、メニューから [ファイル] > [エクスポート] の順に選択します。準備した選択をインポートするには、[ファイル] > [インポート] を使用します。

重要項目: ハードウェアの互換性

この機能は、パッケージリスト自体を保存するため、ソースシステムとターゲットシステムのハードウェアが同一でなければなりません。より複雑な環境下では、「[第5章 自動インストール \(95 ページ\)](#)」に説明されている AutoYaST の方が適切かもしれません。

パッケージの削除

パッケージを削除するには、削除するパッケージに正しいステータスを割り当て、[承認] をクリックします。選択されたパッケージには、[削除] ステータスが表示されるはずです。他のインストール済みのパッケージで必要とされるパッケージが削除としてマーク付けされた場合、パッケージマネージャは警告メッセージと、詳細な情報および代替の解決策を表示します。

パッケージの再インストール

パッケージ内に破損したファイルを見つけた場合、またはインストールメディアからオリジナルバージョンのパッケージを再インストールしたい場合は、パッケージを再インストールします。パッケージを再インストールするには、再インストールするパッケージを選択し、[承認] をクリックします。選択されたパッケージには、[更新] ステータスが表示されるはずです。他のインストール済みのパッケージとの依存関係の問題が発生した場合、パッケージマネージャは警告メッセージと、詳細な情報および代替の解決策を表示します。

パッケージ、アプリケーション、およびファイルの検索

特定のパッケージを検索するには、[検索] フィルタを使用します。検索文字列を入力し、[検索] をクリックします。さまざまな検索条件を指定することで、少数、さらには1つのパッケージのみ表示させるように検索を絞るこ

とができます。 *[Search Mode (検索モード)]* でワイルドカードおよび正規表現を使用することで、特別な検索パターンを定義することができます。

ティップ: クイック検索

[検索] フィルタに加えて、パッケージマネージャのリストすべてにクイックサーチ機能があります。1文字入力すると、入力した文字で始まる、リスト内の最初のパッケージにカーソルが移動します。カーソルはリスト内になければなりません(リストをクリックする)。

パッケージを名前で検索するには、 *[名前]* を選択し、検索フィールドに検索するパッケージの名前を入力し、 *[検索]* をクリックします。パッケージを説明内テキストで検索するには、 *[Summary (概要)]* および *[Descriptions (説明)]* を選択し、検索文字列を入力して、 *[検索]* をクリックします。

特定のファイルを含むパッケージを検索するには、ファイル名を入力し、 *[RPM "Provides"]* を選択し、 *[検索]* をクリックします。特定のパッケージに依存するすべてのパッケージを検索するには、 *[RPM "Requires"]* を選択し、パッケージ名を入力し、 *[検索]* をクリックします。

SUSE Linux Enterpriseのパッケージ構成について詳しい場合は、 *[パッケージグループ]* フィルタを使用して題名でパッケージを検索できます。このフィルタはプログラムパッケージを対象ごとにソートします。対象には、左側のツリー構造にある、アプリケーション、開発、およびハードウェアなどがあります。ブランチを展開するほど選択項目は特定化されます。これにより、個々のパッケージウィンドウに表示されるパッケージが少なくなります。

[Installation Summary]

インストール、更新、または削除するパッケージを選択した後に、 *[インストール概要]* を使用してインストール概要を表示します。これにより、 *[了解]* をクリックした場合にパッケージが受ける影響が表示されます。左側のチェックボックスを使用してパッケージをフィルタし、個々のパッケージウィンドウを表示します。たとえば、どのパッケージが既にインストールされているかを確認するには、 *[保持]* を除くすべてのチェックボックスを無効にします。

通常、個々のパッケージウィンドウのパッケージステータスは変更できます。ただし、変更したパッケージは検索条件に当てはまらなくなる可能性があります。

ます。そのようなパッケージをリストから削除するには、[\[リストの更新\]](#)を使用してリストを更新します。

パッケージに関する情報

右下のフレーム内にあるタブを使用して、選択されたパッケージについての情報を取得します。パッケージの他のバージョンが利用可能な場合は、両方のバージョンの情報が取得可能です。

選択されたパッケージの説明を表示する [\[説明\]](#) タブが自動的にアクティブになります。パッケージサイズ、インストールメディア、および他の技術的な詳細に関する情報を表示するには、[\[Technical Data \(技術的なデータ\)\]](#) を選択します。提供および要求されたファイルに関する情報は、[\[Dependencies \(依存関係\)\]](#) の中にあります。利用可能なバージョンとそのインストールソースを表示するには、[\[バージョン\]](#) をクリックします。

ディスク使用

ソフトウェアの選択中、モジュールの左下のリソースウィンドウには、すべてのマウントされたファイルシステムの仮想ディスク使用量を表示されます。配色されたバークラフが選択ごとに上昇します。緑の状態は、十分な容量があることを示します。ディスク容量の限界に近づくと、バーの色が次第に赤くなります。インストールするパッケージを選択しすぎると、警告が表示されます。

依存関係のチェック

一部のパッケージは他のパッケージに依存しています。つまり、パッケージの一部のソフトウェアは、他のパッケージもインストールされている場合にのみ適切に動作します。一部のパッケージは、同一または類似する機能を持っています。これらのパッケージが同じシステムリソースを使用する場合は、同時にインストールしないでください(パッケージの競合)

パッケージマネージャが起動すると、システムを検査し、インストール済みのパッケージを表示します。インストールまたは削除を行うパッケージを選択する際、パッケージマネージャに自動的に依存関係を確認させて、必要な他のパッケージを選択することができます(依存関係の解決)。競合するパッ

パッケージを選択または選択解除した場合、パッケージマネージャは競合を示し、問題を解決するための提案を行います(競合の解決)

依存関係の自動確認機能を有効にするには、情報ウィンドウの下部にある **[Autocheck]** (自動確認)を選択してください。 **[Autocheck]** を選択すると、パッケージステータスの変更が行われると、自動確認が実施されます。これは便利な機能です。パッケージ選択の整合性が永続的に監視されるためです。ただし、このプロセスはリソースを消費し、パッケージマネージャの動作が遅くなります。この理由により、デフォルトでは自動依存チェックは有効ではありません。 **[Autocheck]** のステータスに関係なく、 **[了解]** を選択した場合は整合性チェックが実施されます。

情報ウィンドウの下にある **[依存チェック]** をクリックすると、パッケージマネージャは、現在のパッケージ選択により解決していないパッケージの依存関係または競合が発生していないかどうかをチェックします。解決していない依存関係がある場合、必要となる追加のパッケージが自動的に選択されます。パッケージの競合の場合、パッケージマネージャは競合を示すダイアログを開き、問題を解決するためのさまざまなオプションを提供します。

たとえば、sendmailおよびpostfixは同時にはインストールされません。**図 8.3. 「パッケージマネージャの競合管理」** (154 ページ)に、どちらをインストールするのかの決定を要求する、競合メッセージが表示されます。postfixはすでにインストールされています。選択肢としては、sendmailのインストールを無効にする、postfixを削除する、危険を承知で競合メッセージを無視する、があります。

警告: パッケージの競合の処理

パッケージの競合を処理する場合、経験豊富な場合以外はYaSTの提案に従うようにお勧めします。提案を受け入れなかった場合、システムの安定性と機能が存在する競合により失われる可能性があります。

図 8.3 パッケージマネージャの競合管理



-develパッケージのインストール

パッケージマネージャは、`devel`および`debug`パッケージを素早く簡単にインストールするための機能を提供します。インストールされたシステム用にすべての`devel`パッケージをインストールするには、`[エクストラ] > [Install All Matching — -devel Packages]`の順に選択します。インストールされたシステム用にすべての`debug`パッケージをインストールするには、`[エクストラ] > [Install All Matching — -debuginfo Packages]`の順に選択します。

8.3.2 アドオン製品のインストール

アドオン製品はシステムを拡張するために使用します。SDKアドオンやバイナリドライバで使用するCDなど、サードパーティのアドオン製品またはお使いのSUSE Linux Enterpriseの特殊拡張機能をインストールできます。新規のアドオンをインストールするには、`[ソフトウェア] > [アドオン製品の追加]`を使用します。CD、FTP、またはローカルディレクトリなど、さまざまな種

類の製品メディアを選択できます。また、ISOファイルで直接作業することもできます。アドオンをISOファイルメディアとして追加するには、*[Local Directory]* を選択して、次に *[ISO Images]* を選択します。

アドオンメディアを問題なく追加した後、*[パッケージマネージャ]* ウィンドウが表示されます。アドオンが新しいパターンを提供すると、*[Patterns]* フィルタに新しい項目が表示されます。選択されたインストールソースからすべてのパッケージリストを表示するには、フィルタ *[インストールソース]* を選択して、表示するインストールソースを選択します。選択されたアドオンからパッケージグループごとにパッケージを表示するには、セカンダリフィルタの *[パッケージグループ]* を選択します。

ティップ: カスタムアドオン製品の作成

YaST Add-On Creatorを使って、独自のアドオン製品を作成することができます。YaST Add-On Creatorの詳細は、http://developer.novell.com/wiki/index.php/Creating_Add-On_Media_with_YaSTを参照してください。技術情報は、http://developer.novell.com/wiki/index.php/Creating_Add-Onsを参照してください。

8.3.3 インストールソースの選択

いくつかのタイプの複数のインストールソースを使用できます。*[ソフトウェア]* > *[インストールソース]* を使用してソースを選択し、インストールまたは更新用に使用可能にします。たとえば、SUSE Software Development Kitをインストールソースとして指定できます。起動すると、以前に登録したソースすべてのリストが表示されます。CDからの通常のインストールが終了すると、インストールCDのみがリストされます。*[追加]* をクリックして、このリストにある追加のソースを含めます。ソースは、CD、DVD、またはNFSおよびFTPサーバなどのネットワークソースのいずれかの可能性があります。ローカルハードディスク上のディレクトリもインストールメディアとして選択できます。詳細については、YaSTのヘルプテキストを参照してください。

登録されたソースはすべて、リストの最初の列に有効状態が表示されます。*[Activate or Deactivate (有効化または無効化)]* をクリックして、個々のインストールソースを有効化または無効化します。ソフトウェアパッケージのインストールまたはアップデート中に、YaSTは有効化されたインストールソースのリストから適切なエントリを選択します。*[閉じる]* をクリックしてモ

ジュールを終了した時点で、現在の設定が保存され、設定モジュールの「ソフトウェアの管理」および「*System Update*(システム更新)」に適用されます。

8.3.4 SUSE Linux Enterpriseの登録

テクニカルサポートを受けたり、製品アップデートを入手するには、システムを登録する必要があります。インストール時に登録作業をスキップした場合は、「ソフトウェア」の「*Novell*カスタマセンタへの登録」モジュールを使って登録してください。このダイアログは、「**3.14.4項「ノベルカスタマセンタの環境設定」** (46 ページ)」と同じものです。

8.3.5 YaSTオンラインアップデート

YaSTオンラインアップデートを使用して、重要なアップデートと改善をインストールします。お使いのSUSE Linux Enterpriseに対する現在のアップデートは、パッチを含む製品固有のアップデートカタログから利用できます。カタログを追加または削除するには、で説明している通り、> 「ソフトウェア」、**8.3.3項「インストールソースの選択」** (155 ページ) 「インストールソース」モジュールを使用します。

注意: アップデートカタログのアクセス時のエラー

アップデートカタログにアクセスできない場合、登録の期限が切れている場合があります。通常、SUSE Linux Enterpriseには1年または3年の登録期間があり、この期間内にアップデートカタログにアクセスできます。このアクセスは登録期間が切れると拒否されます。

アップデートカタログへのアクセスが拒否される場合は、ノベルカスタマセンタにアクセスして登録を確認することを推奨する警告メッセージが表示されます。ノベルカスタマセンタには、<http://www.novell.com/center/>でアクセスできます。

YaSTを使ってアップデートやパッチをインストールするには、「ソフトウェア」>「オンラインアップデート」の順にクリックします。お使いのシステムに適用できるすべてのパッチが、インストールする項目として最初から選択されています(任意項目を除く)。「了解」をクリックすると、これらのパッチが自動的にインストールされます。インストールが完了したら、「完了」をクリックします。これで、システムが最新の状態になりました。

用語の定義

パッケージ

パッケージはrpmフォーマットの圧縮ファイルで、特定のプログラム向けのファイルを含んでいます。

パッチ

パッチは、フルパッケージでもpatchrpmまたはdeltarpmパッケージでも、1つ以上のパッケージで構成されています。また、まだインストールされていないパッケージとの依存関係もあります。

patchrpm

patchrpmはSUSE Linux Enterprise 10が最初にリリースされてから更新されたファイルのみで構成されています。ダウンロードサイズは通常、パッケージサイズよりも非常に小さくなっています。

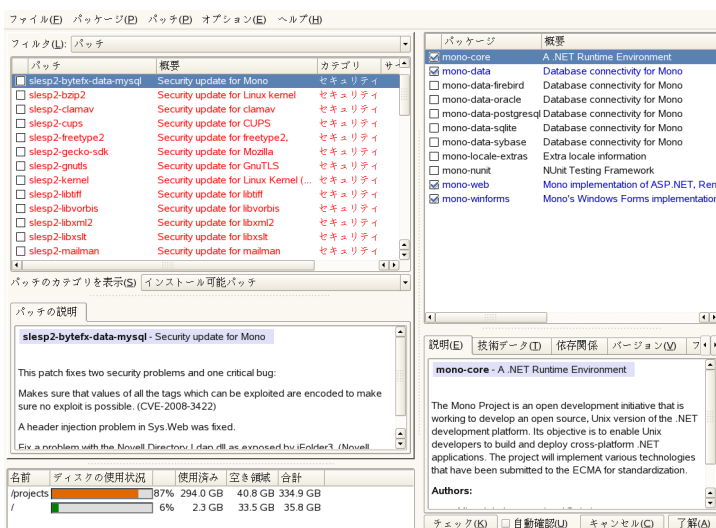
deltarpm

deltarpmは2つの定義されたパッケージバージョンのバイナリ差分のみで構成されているため、ダウンロードサイズは最小です。インストールする前に、rpmパッケージをローカルマシン上で再構築する必要があります。

パッチの手動インストール

[オンラインアップデート] ウィンドウは、5つのセクションから成り立っています。利用できるパッチは、左側のリストに表示されています。パッチを選択すると、パッチリストの下部にその情報が表示されます。左側の列の下部には、ディスク使用状況が表示されます。右側の列には、選択したパッチに含まれているパッケージが表示されます(パッチが複数のパッケージから構成されることもあります)。その下には、選択したパッケージの詳細が表示されます。

図 8.4 YaSTオンラインアップデート



パッチディスプレイは、SUSE Linux Enterpriseに利用できるパッチを表示します。パッチはセキュリティ重要度順にソートされています。パッチ名の色とマウスカーソルを置いたときのポップアップウィンドウは、パッチのセキュリティ状態を示します。状態は、セキュリティ(赤)、推奨(青)、オプション(黒)です。パッチには異なる3つのビューがあります。[パッチのカテゴリを表示]を使用して、ビューを切り替えます。

インストール可能パッチ(デフォルトビュー)

システムにインストールされたパッケージに適用される、まだインストールされていないパッチ。

インストール可能およびインストール済みパッチ

システムにインストールされたパッケージに適用される、すべてのパッチ。

すべてのパッチ

SUSE Linux Enterpriseに使用できるすべてのパッチ。

リストの各項目は、記号とパッチ名から成り立っています。リストに表示される記号については、**Shift + F1**キーを押してください。セキュリティおよび推奨パッチで要求されるアクションは、自動的に設定されます。アクション

は、[自動インストール]、[自動更新]、[自動削除]です。オプションパッチのアクションは事前設定されません。パッチを右クリックして、リストからアクションを選択します。

アップデートカタログ以外のカatalogから最新のパッケージをインストールする場合、このパッケージのパッチ要件はこのインストールで満たせます。この場合、パッチ概要の前にチェックマークが表示されます。パッチは、インストール用にマークするまでリストに表示されます。これによってパッチは実際にはインストールされませんが(パッチはすでに最新であるため)、インストール済みとしてパッチをマークします。

大部分のパッチには、複数のパッケージのアップデートが含まれています。あるパッケージに対するアクションを変更する場合は、パッケージウィンドウからパッケージを右クリックしてアクションを選択してください。適用するパッチとパッケージをすべて選択したら、[了解]を選択します。

ティップ: deltarpmの無効化

rpmパッケージのdeltarpmからの再構築はリソースとCPU時間を消費するタスクなので、セットアップまたはハードウェア構成によっては、パフォーマンス上の理由でdeltarpmの使用を無効にする必要があります。deltarpmの使用を無効にするには、ファイル/etc/zypp/zypp.confを編集してdownload.use_deltarpmをfalseに設定します。

ソフトウェア更新のための他の手段は、KDEおよびGNOME用のZENworks updaterアプレットを用いる方法です。ZENworks updaterは新しいパッチをモニタするのに役立ちます。また、手軽なアップデート機能も用意されています。詳細については、[9.2項「ZENツールを使ったパッケージの管理」](#) (228ページ)を参照してください。

8.3.6 自動オンラインアップデート

YaSTでは、自動アップデートを設定することもできます。[ソフトウェア] > [自動オンラインアップデート]の順に選択します。アップデート間隔を、[Daily] (毎日)または[Weekly] (1週間ごと)から選択します。カーネルアップデートなど、ユーザによる作業が必要なパッチもあります。このような場合は、自動アップデート処理が中止されます。この場合に、アップデート処理を自動的に継続するには、[Skip Interactive Patches] (対話型パッチをスキップ)を選択してください。このオプションを選択した場合、ユーザが作業を行

う必要があるパッチをインストールするには、手動で [オンラインアップデート] を実行してください。

[*Only Download Patches*] (パッチのダウンロードのみ)を選択している場合、指定した時間にパッチがダウンロードされますが、インストールは行われません。手動でインストールを行う必要があります。デフォルトでは、パッチはragキャッシュディレクトリの/var/cache/zmd/webにダウンロードされます。現在のrugキャッシュディレクトリを表示するには、`rug get-prefs cache-directory`コマンドを使用します。rugの詳細は、[9.1項「コマンドラインからrugを使った更新」](#) (224 ページ)を参照してください。

8.3.7 パッチCDを使用した更新

注意

s390システムで、パッチCDによるアップデートオプションが可能になりました。

[ソフトウェア] セクションからの [PatchCD Update] は、FTPサーバからではなく、CDからパッチをインストールします。CDを使用するほうがより速くアップデートできることが利点です。パッチCDを挿入すると、CDに保存されているすべてのパッチがダイアログに表示されます。パッチのリストから希望するパッケージを、インストール対象として選択します。モジュールは、パッチCDが存在しない場合にエラーメッセージを表示します。パッチCDを挿入してモジュールを再起動します。

8.3.8 システムのアップデート

システムにインストールされているSUSE Linux Enterpriseのバージョンを更新するには、[ソフトウェア] > [System Update] を使用します。操作中には、ベースシステムではなく、アプリケーションソフトウェアのみをアップデートできます。ベースシステムをアップデートするには、CDなどのインストールメディアからコンピュータをブートします。YaSTのインストールモードを選択する場合は、[更新] を選択します。

システムをアップデートする処理手順は、新規のインストールと類似しています。最初に、YaSTはシステムを検査し、適切なアップデートの方針を決定

し、推奨ダイアログに結果を表示します。詳細を変更するには、[変更] または個々の項目をクリックします。

アップデートオプション

システムに対するアップデート方法を設定します。2つのオプションが使用可能です。

選択項目に応じた新しいソフトウェアと機能のインストールによる更新
システム全体を最新のソフトウェアバージョンにアップデートするには、定義済みの選択グループの1つを選択します。これにより以前に存在しなかったパッケージもインストールされることが確認されます。

インストール済みパッケージのみアップデート
このオプションはシステムに既に存在するパッケージだけをアップデートします。新しい機能はインストールされません。

さらに、[Delete Outdated Packages(廃止されたパッケージの削除)] を使用して、新しいバージョンが存在しないパッケージを削除します。このオプションは、廃止されたパッケージが不必要にハードディスクの容量を使用しないように、デフォルトで事前に選択されています。

[Packages]

[パッケージ] をクリックして、パッケージマネージャを起動し、アップデートする個々のパッケージを選択または選択解除します。整合性チェックを実行すると、すべてのパッケージの競合が解決されます。パッケージマネージャの詳細な使用方法については、[8.3.1項「ソフトウェアのインストールと削除」](#) (146 ページ)を参照してください。

バックアップ

アップデート中に、いくつかのパッケージの設定ファイルは、新しいバージョンの設定ファイルにより置き換えられます。現在のシステムでいくつかのファイルを変更した場合、通常、パッケージマネージャは、置き換えるファイルのバックアップコピーを作成します。このダイアログを使用して、これらのバックアップの範囲を決定します。

重要項目: バックアップの範囲

このバックアップにはソフトウェアは含まれません。設定ファイルだけが含まれます。

言語

システムに現在インストールされている第一言語および他の言語がここにリストされます。表示された設定の中で **[言語]** をクリックするか、**[変更]** > **[言語]** を使用して言語を変更します。必要に応じて、第一言語が話されている地域に、キーボードレイアウトおよびタイムゾーンを合わせるよう選択できます。言語の選択の詳細については、**8.5.15項「言語の選択」** (182 ページ) を参照してください。

アップデートに関する重要な情報

システムのアップデートはとても複雑な処理です。各プログラムパッケージごとに、YaSTは最初にコンピュータにインストールされているバージョンを確認し、旧バージョンを新バージョンと正常に置き換えるのに必要な事柄を判断します。YaSTはまた、インストール済みパッケージ独自の設定をすべて使用するように試みます。

ほとんどの場合、YaSTは問題なく旧バージョンを新バージョンに置き換えます。既存のシステムのバックアップをアップデート前にとっておく必要があります。既存の設定がアップデート中に失われる可能性があるためです。アップデートが完了した後に、競合を手動で解決します。

8.3.9 ディレクトリへのインストール

YaSTモジュールを使用すると、指定したディレクトリにパッケージをインストールすることができます。rootディレクトリの配置場所、ディレクトリの命名、およびインストールしたいシステムとソフトウェアの種類を決めます。このモジュール選択後、YaSTがシステム設定を判別し、デフォルトディレクトリ、インストール手順、およびインストールするソフトウェアをリストします。**[変更]** をクリックして、これらの設定を編集します。すべての変更は、**[承認]** をクリックして確定する必要があります。変更がすべて終わっ

たら、インストールが完了したという表示が出るまで [次へ] をクリックします。 [完了] をクリックしてダイアログを終了します。

8.3.10 メディアの確認

SUSE Linux Enterpriseインストールメディアの使用中に問題が発生した場合、[ソフトウェア] > [メディアチェック] を使用してCDまたはDVDをチェックできます。メディアの問題は、独自に作成したメディアを使用する場合により発生します。SUSE Linux Enterprise CDまたはDVDにエラーがないことをチェックするには、メディアをドライブに挿入してこのモジュールを実行します。[開始] をクリックすると、YaSTはメディアのMD5チェックサムをチェックします。これには少し時間がかかります。問題が検出された場合、インストール用にこのメディアを使用しないでください。

8.4 ハードウェア

新しいハードウェアは、最初にインストールされているか、ベンダが指定する方法で接続されている必要があります。外部デバイスの電源を入れ、適切なYaSTモジュールを起動します。ほとんどのデバイスは自動的にYaSTにより検出され、技術的なデータが表示されます。自動検出が失敗した場合、YaSTはデバイスのリスト(モデル、ベンダなど)を表示するので、その中から適切なデバイスを選択します。詳細については、ハードウェアに付属しているマニュアルを参照してください。

重要項目: モデルの指定

使用中のモデルがデバイスリストに含まれていない場合、類似するモデルを指定します。ただし、モデルは正確に適合しなければならない場合があります。類似するモデルは互換性があるとは限らないためです。

8.4.1 赤外線デバイス

[ハードウェア] > [赤外線デバイス] を使用して、赤外線デバイスを設定します。[IrDaの開始] をクリックして、設定を開始します。[ポート] と [Limit Baud Rate] をここで設定できます。

8.4.2 グラフィックカードとモニタ

[ハードウェア] > [Graphics Card and Monitor] を使用して、グラフィックカードとモニタを設定します。これにはSaX2インタフェースが使用されます。インタフェースについては、「[8.14項「SaX2」](#) (214 ページ)」を参照してください。

8.4.3 プリンタ

[ハードウェア] > [プリンタ] を使用して、プリンタを設定します。システムにプリンタが正しく接続されると、そのプリンタは自動的に検出および設定されます。YaSTにおけるプリンタの設定の詳細については、[23.4項「プリンタの設定」](#) (485 ページ)を参照してください。

8.4.4 ハードディスクコントローラ

通常、インストール中にシステムのハードディスクコントローラが設定されます。コントローラを追加すると、[ハードウェア] > [ディスクコントローラ] の順に使用してシステムにコントローラを統合します。既存の設定も変更できますが、通常は必要ありません。

検出されたハードディスクコントローラのリストがダイアログに表示され、特定のパラメータを使用して適切なカーネルモジュールを割り当てることができます。[モジュールのロードをテストする] を使用して現在の設定が動作することを確認してから、システムに設定を恒久的に保存します。

警告: ハードディスクコントローラの設定

設定をテストしてから、システムに恒久的な設定をするようにお勧めします。適切でない設定をするとシステムがブートしなくなります。

8.4.5 ハードウェア情報

[ハードウェア] > [ハードウェア情報] を使用して、検出されたハードウェアおよび技術データを表示します。デバイスの詳細については、任意のツリー

ノードをクリックします。たとえば、サポートを依頼するときに、ハードウェアに関する情報が必要な場合などに、このモジュールが特に役立ちます。

[Save to File (ファイルに保存)] をクリックして、表示されたハードウェア情報をファイルに保存します。希望するディレクトリとファイル名を選択し、[保存] をクリックしてファイルを作成します。

8.4.6 IDE DMAモード

[ハードウェア] > [IDE DMAモード] を使用して、インストール済みシステムのIDEハードディスク、IDE CDおよびDVDドライブ用に、DMAモードを有効化および無効化します。このモジュールは、SCSIデバイスには影響を与えません。DMAモードは、パフォーマンスとシステム内でのデータ転送スピードを大幅に向上します。

インストール中に、現在のSUSE Linux Enterpriseカーネルは自動的にハードディスク用のDMAを有効化しますが、CDドライブ用のDMAは有効化しません。すべてのドライブに対してDMAを有効化すると、CDドライブに問題が発生する場合があります。DMAモジュールを使用して、ドライブに対してDMAを有効化します。ドライブが問題なくDMAモードをサポートする場合、ドライブのデータ転送率はDMAを有効化することにより向上します。

注意

DMA(ダイレクトメモリアクセス)は、プロセッサの制御を回避して、データがRAMに直接転送されることを意味します。

8.4.7 IBM System z:DASDデバイス

DASDをインストールシステムに追加するには、2つの方法があります。

YaST

DASDをインストール済みのシステムに追加するには、YaSTDASDモジュールを使用します([ハードウェア] > [DASD] の順に選択)。最初の画面で、Linuxインストールを行うディスクを選択し、[Perform Action(アクションの実行)] をクリックします。[アクティベート] を選択し、[次へ] をクリックしてダイアログを終了します。

コマンドライン

次のコマンドを実行します。

```
dasd_configure 0.0.0150 1 0
```

}0.0.0150をDASDが添付されている実際のチャンネル番号と置き換えます。
DASDがDIAGモードでアクセスしなければならない場合、最後がゼロ(0)
のコマンドラインは、1です。

注意

いずれの場合でも、コマンドを実行して

```
mkinitrd  
zipl
```

この変更を永続的にします。

8.4.8 IBM System z:ZFCP

さらにFCPが添付されたSCSIデバイスをインストール済みシステムに追加する場合は、YaST ZFCPモジュール([ハードウェア] > [ZFCP] の順に選択)を使用します。 [追加] を選択して、追加のデバイスを追加します。リストから [Channel Number(チャンネル番号)] (アダプタ)を選択して、 [WWPN] と [FCP-LUN] を両方指定します。 [次へ] と [閉じる] を選択してセットアップを完了します。 デバイスが追加されたことを確認するために、 cat /proc/scsi/scsi の出力を確認します。

注意

リブートして変更を恒久的にするには、次のコマンドを実行します。

```
mkinitrd  
zipl
```

8.4.9 ジョイスティック

[ハードウェア] > [ジョイスティック] を使用して、サウンドカードに接続されているジョイスティックを設定します。表示されるリストからジョイスティックタイプを選択します。お使いのジョイスティックがリストにない場合、[一般的なアナログジョイスティック] を選択します。ジョイスティックを選択したあとは、それが接続されていることを確認し、[テスト] をクリックして、機能をテストします。[続行] をクリックすると、YaSTは必要なファイルをインストールします。[ジョイスティックのテスト] ウィンドウが表示されたあと、ジョイスティックをすべての方向に動かし、すべてのボタンを押してテストします。すべての動きがウィンドウに表示されるはずです。設定が満足できるものであれば、[OK] をクリックしてモジュールに戻り、[完了] をクリックして設定を終了します。

USBデバイスをお持ちの場合は、この設定は必要ではありません。ジョイスティックをつなぐだけで、使用可能です。

8.4.10 キーボード配列

コンソール用にキーボードを設定するには、YaSTをテキストモードで実行し、[ハードウェア] > [キーボード配列] を使用します。モジュールをクリックすると、現在のレイアウトが表示されます。他のキーボードレイアウトを選択するには、表示されたリストから、任意のレイアウトを選択します。キーボード上のキーを押すことで、[テスト] 内でレイアウトをテストします。

[エキスパート設定] をクリックして、設定の微調整ができます。ここでは、[起動状態] の中で、任意の設定を選択することで、キーリピート率および遅延を調節し、起動時の状態を設定できます。[ロックするデバイス] には、スペースで区切られたデバイスのリストを入力します。これは、<Scroll Lock>キー、<Num Lock>キー、および<Caps Lock>キーの設定が適用されるデバイスです。[OK] をクリックして、微調整を終了します。最後に、すべての選択が終了したら、[承認] をクリックして、変更を有効にします。

グラフィック環境にキーボードを設定するには、グラフィカルYaSTを実行し、[キーボード配列] を選択します。グラフィカル設定については、「[8.14.3 項「キーボードのプロパティ」](#) (219 ページ)」を参照してください。

8.4.11 マウスモデル

グラフィック環境でマウスを設定するには、[マウスモデル] をクリックしてSaX2マウス設定にアクセスします。詳細については、[8.14.2項「マウスのプロパティ」](#) (218 ページ)を参照してください。

テキスト環境でマウスを設定するには、YaSTをテキストモードで使用します。テキストモードに入って、[ハードウェア] > [マウスモデル] を選択したあと、キーボードの矢印キーを使用して表示されたリストからお使いのマウスを選択します。その後、[承認] をクリックして、設定を保存しモジュールを終了します。

8.4.12 サウンド

ほとんどのカードは初期インストール時に自動的に検出され、適切な値で環境設定が行われます。新しく追加したカードをインストールしたり、既存の設定を変更する場合は、[ハードウェア] > [サウンド] を使用します。また、カードの順番を変更することもできます。

図 8.5 サウンドの設定



YaSTがご使用のサウンドカードを自動検出できない場合は、次の処理を実行します。

- 1 [追加] をクリックして、サウンドカードのベンダおよびモデルを選択するダイアログを開きます。必要な情報については、使用中のサウンドカードのマニュアルを参照してください。ALSAによってサポートされるサウンドカードおよびその対応するサウンドモジュールの参照リストについては、`/usr/share/doc/packages/alsa/cards.txt`および「<http://www.alsa-project.org/alsa-doc/>」を参照してください。選択が終了したら、[次へ] をクリックします。
- 2 [サウンドカードの構成] 内では、最初のセットアップ画面で設定レベルを選択します。

[簡易自動設定]

さらに設定処理を続行する必要はありません。またサウンドテストも実行されません。サウンドカードは自動的に設定されます。

[標準の設定]

出力ボリュームを調整したり、テスト用サウンドを再生することができます。

[詳細設定]

手動ですべての設定をカスタマイズすることができます。

このダイアログでは、ジョイスティックの設定へのショートカットも用意されています。[ジョイスティックの設定] をクリックして表示されるダイアログで、適切なジョイスティックタイプを選択し、ジョイスティックの設定を行ってください。[次へ] をクリックします。

- 3 [サウンドカードのボリューム] 内で、サウンド設定をテストし、音量の調整を行います。ボリュームを10%程度にして、スピーカーにダメージを与えたり、耳を損傷することがないようにしてください。テストサウンドは、[テスト] をクリックすると聞くことができます。何も聞こえない場合、ボリュームを上げます。[次へ] > [完了] の順に選択して、サウンドの設定を終了します。

サウンドカードの設定を変更する場合は、[サウンド設定] ダイアログで表示されている[カードモデル]を選択し、[編集] をクリックします。サウンドカードを完全に削除するには、[削除] を使用します。

次のいずれかのオプションを手動でカスタマイズする場合は、[その他] をクリックします。

Volume

このダイアログを使ってボリュームの設定を行います。

[*Start Sequencer*] (シーケンサの開始)

MIDIファイルを再生する場合、このオプションを選択してください。

[*Set as Primary Card*] (プライマリカードに設定)

サウンドカードの順番を変更する場合は、 [*Set as Primary Card*] をクリックします。 インデックス0のサウンドデバイスが、システムやアプリケーションが使用するデフォルトのデバイスになります。

インストールされたすべてのサウンドカードのボリュームと設定は、YaSTサウンドモジュールで [完了] をクリックしたときに保存されます。 ミキサー設定は/etc/asound.confファイルに保存され、ALSA設定データは、/etc/modprobe.d/soundおよび/etc/sysconfig/hardwareファイルの最後に追加されます。

8.5 システム

このモジュールグループはお使いのシステム管理に役立つように設計されています。このグループに含まれるすべてのモジュールは、システムに関連し、システムがきちんと動作し、データが効率良く管理されていることを確実にするための貴重なツールとして使用されます。

ティップ: IBM System z: 継続

IBM System zの場合、「[8.5.3項「ブートローダの設定」](#) (171 ページ)」に進んでください。

8.5.1 バックアップ

[システム] > [*System Backup* (システムバックアップ)] を使用して、システムとデータのバックアップを作成します。ただし、モジュールによって作成されるバックアップには、システム全体は含まれません。システムのバックアップは、ハードディスク上の重要な記憶領域を保存することで実行されます。その記憶領域はパーティションテーブルまたはマスタブートレコード (MBR) など、システムを復元するときに不可欠なものです。このシステムの

バックアップには、AutoYaSTに使用されるシステムのインストールから、XML設定を含めることができます。データのバックアップは、インストールメディア上のアクセス可能なパッケージの変更されたファイル、アクセス不可能なパッケージ全体(例えば、オンラインアップデート)、および、/etcまたは/homeのディレクトリの下にある、たくさんの設定ファイルのような、パッケージに属しないファイルを保存することで実行されます。

8.5.2 復元

[システム] > [システムの復元] を使用して、[システムのバックアップ] で作成したバックアップアーカイブから、ご使用のシステムを復元します。最初に、アーカイブが格納されている場所(リムーバブルメディア、ローカルハードディスク、ネットワークファイルシステム)を指定します。[次へ] をクリックして、個別のアーカイブの説明および内容を表示し、アーカイブから復元するものを選択します。

最後にバックアップしたときから追加されたパッケージをアンインストールしたり、最後にバックアップしたときから削除されたパッケージを再インストールしたりすることもできます。これらの2つの処理により最後にバックアップしたときと完全に同じシステムを復元できます。

警告: システムの復元

このモジュールは、通常多くのパッケージとファイルをインストール、置換、アンインストールするため、必ず事前にバックアップ処理を実行してから使用してください。バックアップ処理を実行しなかった場合、データを失う可能性があります。

8.5.3 ブートローダの設定

コンピュータにインストール済みのシステムのブートを設定するには、[システム] > [Boot Loader] モジュールを使用します。YaSTを使用するブートローダの設定方法の詳細については、[21.3項「YaSTによるブートローダの設定」](#) (457 ページ)を参照してください。

8.5.4 クラスタリング

YaSTを使ったHeartbeatと高可用性の設定に関する詳細は、『*Heartbeat Guide*』を参照してください。

8.5.5 LVM

論理ボリュームマネージャ(LVM)は、論理ドライブを使用するハードディスクのカスタムパーティション用ツールです。LVMについては、「**7.1項「LVMの設定」** (127 ページ)」を参照してください。

8.5.6 EVMS

enterprise volume management system (EVMS)は、LVM同様に、カスタムパーティショニングのためのツール、またハードディスクをバーチャルボリュームにグループ化するためのツールです。柔軟性や拡張性があり、プラグインモデルを使用して、さまざまなボリューム管理システムの個々の必要に適合するように調整できます。

EVMSは、既存のメモリおよびボリューム管理システムとの互換性があります。ボリューム管理システムには、DOS、Linux LVM、GPT (GUIDパーティションテーブル)、IBM System z、Macintosh、およびBSDパーティションなどがあります。詳細については、<http://evms.sourceforge.net/>を参照してください。

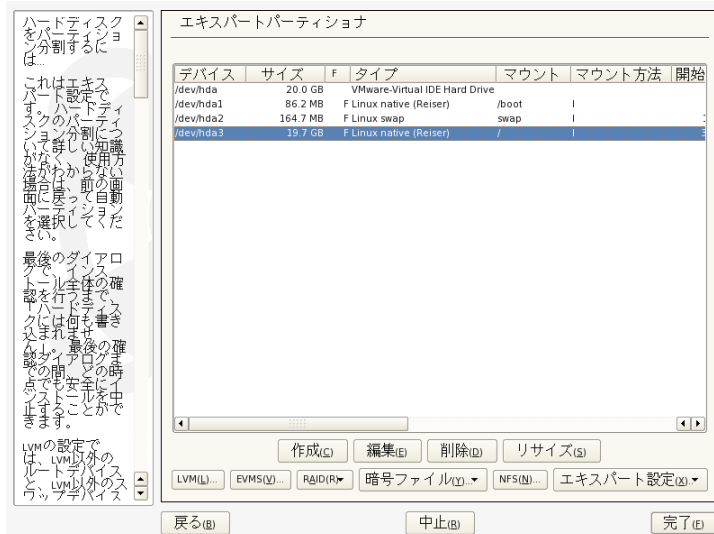
8.5.7 YaSTパーティション分割ツールの使用

図8.6. 「YaSTパーティション分割ツール」 (173 ページ)に示す「上級者向けのパーティション設定」ダイアログを使って、1つまたは複数のハードディスクのパーティションを手動で設定します。パーティションは追加、削除、および編集することができます。このYaSTモジュールからソフトウェアRAID設定、EVMS設定、およびVM設定にもアクセスできます。

警告: 稼働中システムのパーティション再設定

実行中にシステムのパーティションを再設定できますが、誤操作によるデータ損失のリスクが非常に高くなります。インストールしたシステムのパーティション再設定は避けて、常に再設定の前にデータを完全にバックアップしてください。

図 8.6 YaSTパーティション分割ツール



ティップ: IBM System z: デバイス名

IBM System zは、DASDとSCSIハードディスクしか認識できません。IDEハードディスクはサポートされていません。これが理由で、これらのデバイスは、パーティションテーブル内でdasdaまたはsdaという名前が表示され、最初に認識されるデバイスになります。

接続されているすべてのハードディスクの既存パーティションまたは提案パーティションのリストが、YaST [パーティションのエキスパート設定] ダイアログに表示されます。このリストでは、ハードディスク全体は、/dev/hdaや/dev/sda(または/dev/dasda)など、番号のないデバイスとして表されます。パーティションは、/dev/hda1や/dev/sda1(または/dev/dasda1)など、それらのデバイスの一部として表されます。ハードディスクのサイズ、

形式(タイプ)、ファイルシステム、マウントポイントと、ハードディスクのパーティションも表示されます。マウントポイントには、Linuxファイルシステムツリー内のどこにパーティションが表示されるかが指定されています。

インストール中、エキスパートダイアログで作業中の場合は、未使用のハードディスクスペースも表示され、自動的に選択されます。追加のディスクスペースをSUSE Linux Enterprise®用に用意するには、リストの下から上に、必要なスペースが確保できるまで、領域を解放します(ハードディスクの最後のパーティションから始めて、最初のパーティションの方に向かいます)。たとえば、パーティションが3つある場合、2番目のパーティションをSUSE Linux Enterprise専用で使用し、1番目と3番目のパーティションを別のオペレーティングシステム用に保持しておくことはできません。

パーティションのタイプ

ティップ: IBM System z:ハードディスク

IBM System zプラットフォームの場合、SUSE Linux Enterprise ServerはSCSIハードディスクとDASD (Direct Access Storage Devices)の両方をサポートしています。SCSIディスクは以下の方法でパーティション設定することが可能ですが、DASDではパーティションテーブルに指定できるパーティションエントリが3つに限られます。

どのハードディスクにも、パーティションテーブルがあり、4つのエントリ領域が設けられています。パーティションテーブルのエントリは、基本パーティションまたは拡張パーティションのいずれかに使用されます。ただし、拡張パーティションとして指定できるエントリは、1つだけです。

基本パーティションは、単純にシリンダの連続した領域(物理ディスク領域)で構成され、これらのシリンダは、特定のオペレーティングシステムに割り当てられています。パーティションテーブルの制限に伴い、基本パーティションの場合、1台のハードディスクで作成できるパーティションの数が4つに限られます。このような理由から、拡張パーティションが使用されます。拡張パーティションもディスクの連続シリンダから構成されますが、拡張パーティションの場合は、パーティション自体を分割して、論理パーティションを作成できます。論理パーティションは、必ずしもパーティションテーブルに存在している必要はありません。つまり、拡張パーティションは論理パーティションのコンテナということになります。

パーティションが4つ以上必要な場合は、4つ目(またはそれ以前)に拡張パーティションを1つ作成します。この拡張パーティションには、残りの空きシリンダ領域全体を使用するのが妥当です。さらに、この拡張パーティションを複数の論理パーティションに区切ります。SCSI、SATA、Firewireなどのディスクで作成可能な論理パーティションは、最大で15個、(E)IDEディスクの場合は、最大63個です。どのタイプのパーティションを使用しても、Linuxへの影響はありません。基本パーティション、論理パーティションのいずれも、正常に動作します。

ティップ: GPTディスクラベル付きのハードディスク

GPTディスクラベルを使用しているアーキテクチャの場合、基本パーティションの数に制限がありません。そのため、論理パーティションはありません。

パーティションの作成

パーティションを最初から作成するには、以下の手順に従ってください。

- 1 [作成] を選択します。複数のハードディスクが接続されている場合、新規パーティションの作成先ハードディスクの選択ダイアログが表示されます。
- 2 パーティションの形式(基本か拡張)を指定します。最大4つの基本パーティションを作成するか、最大3つの基本パーティションと1つの拡張パーティションを作成します。拡張パーティション内に、いくつかの論理パーティションを作成します(詳細については、[パーティションのタイプ項](#) (174 ページ)を参照してください)。
- 3 使用するファイルシステムと、マウントポイントを選択します。YaSTによって、作成する各パーティション用のマウントポイントが提案されます。各種ファイルシステムの詳細については、[第25章 Linuxのファイルシステム](#) (517 ページ)を参照してください。
- 4 セットアップで必要な場合は、追加のファイルシステムオプションを指定します。たとえば、永続的デバイス名が必要な場合に必要になります。使用できるオプションの詳細については、[パーティションの編集項](#) (176 ページ)を参照してください。

- 5 **[OK]** > **[OK]** の順にクリックして、パーティション設定を適用し、パーティション設定モジュールを終了します。

インストール時にパーティションを作成した場合は、インストール概要画面に戻ります。

パーティションの編集

新規パーティションの作成、または既存パーティションの変更の際には、多数のパラメータを設定します。新規パーティションの場合、適切なパラメータがYaSTによって設定されるので、通常は変更の必要はありません。パーティション設定を手動で編集するには、以下の手順に従ってください。

- 1 パーティションを選択します。
- 2 **[編集]** をクリックして、パーティションの編集およびパラメータ設定を実行します。

ファイルシステムID

この段階でパーティションをフォーマットしたくない場合であっても、パーティションにファイルシステムIDを割り当て、パーティションが正しく登録されるようにします。可能な値は、**[Linux]**、**[Linux swap]**、**[Linux LVM]**、**[Linux EVMS]** または **[Linux RAID]** です。LVMとRAIDの詳細については、**7.1項「LVMの設定」** (127 ページ) および **7.2項「ソフトウェアRAID設定」** (137 ページ) を参照してください。

ファイルシステム

ここでは、ファイルシステムを変更したり、パーティションをフォーマットします。ファイルシステムの変更またはパーティションの再フォーマットによって、パーティションからすべてのデータが完全に削除されます。さまざまなファイルシステムの詳細は、**第25章 Linuxのファイルシステム** (517 ページ) を参照してください。

ファイルシステムのオプション

[ファイルシステムのオプション] 画面では、選択したファイルシステムのパラメータを指定します。たいていの場合は、デフォルト値をそのまま利用できます。

暗号化ファイルシステム

暗号化を有効にした場合、すべてのデータは暗号化された状態で、ハードディスクに書き込まれます。これにより、機密データのセキュリティが向上しますが、暗号化に時間がかかるので、システムの処理速度はわずかに低下します。ファイルシステムの暗号化の詳細については、[第47章 パーティションとファイルの暗号化](#)(943ページ)を参照してください。

fstabのオプション

グローバルファイルシステム管理ファイル(/etc/fstab)にあるさまざまなパラメータを指定します。ほとんどの設定では、デフォルト設定で動作します。たとえば、ファイルシステムIDをデバイス名からボリュームラベルに変更できます。ボリュームラベルには、/ およびスペース以外のすべての文字を使用することができます。

マウントポイント

パーティションのファイルシステムツリー内でのマウント先ディレクトリを指定します。YaSTで表示されるさまざまなディレクトリから選択するか、または他のディレクトリ名を入力します。

- 3 [OK] > [適用] の順にクリックして、パーティションをアクティブにします。

エキスパート用オプション

[エキスパート設定] は、次のコマンドを含むメニューを開きます。

パーティションテーブルの再読み込み

ディスクからパーティション設定を再読み込みします。たとえば、テキストコンソールで手動パーティション設定を行った後で、これが必要になります。

パーティションテーブルとディスクラベルの削除

この処理では、古いパーティションテーブルが完全に上書きされます。たとえば、独自のディスクラベルに問題がある場合に役立ちます。この方法を用いると、ハードディスク上のすべてのデータが失われます。

パーティション設定に関するヒント

以降のセクションでは、システムの設定時に正しく判断するための、パーティション設定のヒントを説明します。

ティップ: シリンダ番号

パーティション設定ツールによっては、パーティションのシリンダの番号を0または1で開始します。シリンダ数を計算するには、最後と最初のシリンダ番号の差に1を加えます。

YaSTによってパーティション設定が実行され、システム内に他のパーティションが検出された場合、検出されたパーティションも/etc/fstabファイルに追加され、この設定データへのアクセスが簡単になります。このファイルには、システム内のすべてのパーティションとそのプロパティ（ファイルシステム、マウントポイント、ユーザのパーミッションなど）が記載されています。

例 8.1 /etc/fstab: パーティションデータ

```
/dev/sda1    /data1    auto      noauto,user 0 0
/dev/sda5    /data2    auto      noauto,user 0 0
/dev/sda6    /data3    auto      noauto,user 0 0
```

LinuxパーティションかFATパーティションに関係なく、パーティションは、noautoオプションとuserオプションを使って指定されます。これにより、すべてのユーザがこれらのパーティションを、必要に応じてマウントまたはアンマウントすることができます。セキュリティ上の理由で、YaSTでは、プログラムを関連位置で実行するのに必要なexecオプションは、ここに自動的に入力されません。ただし、そこからプログラムを実行するために、このオプションを手動で入力できます。「不正インタプリタ」や「パーミッションの拒否」などのシステムメッセージが出されたら、この方法が必要になります。

パーティション設定とLVM

Expert Partitionerから[LVM]を選択してLVM設定にアクセスします(7.1項「**LVMの設定**」(127 ページ)を参照)。ただし、作業するLVM設定がシステムにすでに存在している場合は、セッションで初めてLVM設定を入力した時点

でただちに、自動的にその設定がアクティブになれます。この場合、アクティブになったボリュームグループに属するパーティションを含むすべてのディスクは、パーティションを再設定できません。Linuxカーネルは、ハードディスクの変更されたパーティションテーブルを、このディスク上のいずれかのパーティションが使用中になった時点では、再読みすることができないからです。ただし、機能しているLVM設定がシステム上にがすでにある場合は、物理的なパーティション再設定は必要になりません。代わりに、論理ボリュームの設定を変更します。

物理ボリューム(PV)の先頭では、そのボリュームに関する情報がパーティションに書き込まれます。こうしたパーティションをLVM以外の目的で再使用するには、このボリュームの先頭を削除しておくようにお勧めします。たとえば、VG systemおよびPV /dev/sda2では、これは、コマンド`ddif=/dev/zero of=/dev/sda2 bs=512 count=1`で行うことができます。

警告: ブート用ファイルシステム

ブートに使用するファイルシステム(rootファイルシステムまたは/boot)をLVM論理ボリュームに格納しないでください。通常の物理パーティションに格納してください。

8.5.8 PCIデバイスドライバ

ティップ: IBM System z:継続

IBM System zの場合、「[8.5.12項「システムサービス\(ランレベル\)」](#) (181 ページ)」に進んでください。

各カーネルドライバには、サポートしているすべてのデバイスのデバイスIDリストが含まれています。新しいデバイスがどのドライバのデータベースにも含まれていない場合、既存のドライバで利用できる場合でも、そのデバイスはサポートされていないものとして処理されます。YaSTの [システム] セクションから、PCI IDを追加できます。このYaSTモジュールは、専門知識を持つユーザ以外は使用しないでください。

図 8.7 PCI IDの追加



IDを追加するには、**[追加]** をクリックして、割り当て方法を選択します。割り当て方法には、リストからPCIデバイスを選択する方法と、手動でPCIの値を入力する方法があります。最初のオプションの場合、提供されたリストからPCIデバイスを選択し、ドライバ名またはディレクトリ名を入力します。ディレクトリが空のままの場合は、ドライバ名はディレクトリ名として使用されます。PCI ID値を手動で指定する場合、適切なデータを入力してPCI IDをセットアップします。**[OK]** をクリックして、変更を保存します。

PCIIDを編集するには、リストから編集するデバイスドライバを選択し、**[編集]** をクリックします。情報を編集して **[OK]** をクリックすると、変更が保存されます。IDを削除するには、そのドライバを選択し、**[削除]** をクリックします。IDはすぐにリストに表示されなくなります。終了したら、**[OK]** をクリックします。

8.5.9 電源管理

[システム] > **[電源管理]** モジュールを使用すると、省エネ技術を利用して作業することができます。ラップトップの操作時間を拡張することは、ラップトップでは特に重要です。このモジュールの使用法に関する詳細は、[28.6 項「YaST電源管理モジュール」](#) (578 ページ)に記載しています。

8.5.10 Powertweakの設定

Powertweakは、カーネルおよびハードウェア設定をチューニングすることで、システムのパフォーマンスを最高にするためのSUSE Linuxのシステム微調整用ユーティリティです。これは、上級のユーザにのみ使用されるべきユーティリティです [システム] > [Powertweak] を選択してこのユーティリティを起動すると、ユーティリティがシステム設定を検出し、モジュールの左側のフレームにツリー形式でリストします。[検索] ボタンを使って設定用の変数を探すこともできます。微調整したいオプションを選択すると、画面にそのオプションがディレクトリおよび設定とともに表示されます。設定を保存するには、[完了] をクリックし、[OK] をクリックして確認します。

8.5.11 プロファイルマネージャ

[システム] > [プロファイル管理] を開き、YaSTシステム設計プロファイル管理(SCPM)モジュールを使用して、システム設定を作成、管理、切り替えます。これは、さまざまな場所(さまざまなネットワーク)でさまざまなユーザが使用するモバイルコンピュータには特に便利です。それだけでなく、この機能は、さまざまなハードウェアコンポーネントやテスト設定の使用が可能ですので、固定マシンにも便利です。

8.5.12 システムサービス(ランレベル)

[システム] > [システムサービス (ランレベル)] を使用して、ランレベルおよびその中で開始するサービスを設定します。SUSE Linux Enterpriseでのランレベルの詳細について、およびYaSTランレベルエディタについての説明は、[20.2.3項「YaSTでのシステムサービス\(ランレベル\)の設定」](#) (440 ページ)を参照してください。

8.5.13 /etc/sysconfigエディタ

/etc/sysconfigディレクトリには、SUSE Linux Enterpriseにとって最も重要な設定ファイルが含まれています。[システム] > [/etc/sysconfigエディタ] を選択して、値を変更し、個別の設定ファイルに保存します。一般的に、ファイルを手動で編集する必要はありません。パッケージがインストールされたとき、またはサービスが設定されたときにファイルは自動的に変更され

るためです。/etc/sysconfigとYaST sysconfigエディタの詳細については、[20.3.1項「YaSTのsysconfigエディターを使ってシステム設定を変更する」](#) (442 ページ)を参照してください。

8.5.14 日付と時刻の設定

タイムゾーンは初めのインストール時に設定されますが、`[システム] > [Date and Time]` を使用して変更できます。現在の日付と時刻を変更する場合にも、これを使用します。

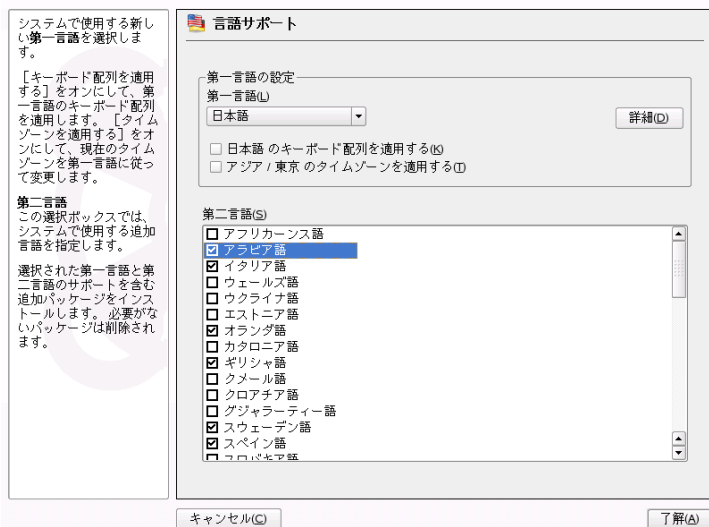
タイムゾーンを変更するには、左の列で地域を選択し、右の列で場所またはタイムゾーンを選択します。`[ハードウェア時計の時間設定]` を使用して、システムクロックが`[ローカルタイム]` または `[UTC]` (*世界協定時刻、以前のグリニッジ標準時*)のどちらを使用するか設定します。`[UTC]` はLinuxシステムではよく使用されるタイムゾーンです。他方、Microsoft Windowsなどの追加のオペレーティングシステムを使用しているコンピュータは、ほとんどローカルタイムを使用します。

`[変更]` を使用して、現在のシステム時刻および日付を設定します。開いたダイアログの中で、新しい値を入力するか<矢印>ボタンで調節して、時刻および日付を変更します。`[適用]` を押して、変更内容を保存します。

8.5.15 言語の選択

システムの第一および第二言語は、インストール時に設定されます。ただし、`[システム] > [言語]` を使用すれば、いつでもそれらを変更できます。YaSTに設定された第一言語は、YaSTおよびデスクトップ環境を含んだ、システム全体に適用されます。この言語がほとんどの場合使用されます。第二言語は、デスクトップ言語や文書作成などのさまざまな目的のために、ユーザが必要とすることがある言語です。

図 8.8 言語の設定



「第一言語」内で、システム用に使用するメイン言語を選択します。キーボードやタイムゾーンをこの設定用に調整するには、`[Adapt Keyboard Layout]` または `[Adapt Time Zone]` を有効化します。

`[Details]` を使用して、rootユーザ用のロケール変数の設定方法を設定します。また、`[詳細]` を使用して、メインリストでは利用不可能な方言に対して、第一言語を設定します。これらの設定は、`/etc/sysconfig/language` ファイルに書き込まれます。

8.6 ネットワークデバイス

システムに接続されたネットワークデバイスはすべて、サービスにより使用される前に初期化する必要があります。これらのデバイスの検出および設定は、`[ネットワークデバイス]` モジュールグループで行われます。

8.6.1 DSL、ISDN、モデム、またはネットワークカード

DSL、ISDN、ネットワークインタフェースまたはモデムを設定するには、[\[ネットワークデバイス\]](#) セクションから適切なモジュールを選択します。自動検出されるデバイスについては、リストからそのデバイスを選択し、[\[編集\]](#) をクリックします。使用中のデバイスが検出されない場合、[\[追加\]](#) をクリックし、デバイスを手動選択します。既存のデバイスを編集するには、そのデバイスを選択し、[\[編集\]](#) をクリックします。詳細については、[30.4 項「YaSTによるネットワーク接続の設定」](#) (616 ページ)を参照してください。ワイヤレスネットワークインタフェースに関しては、「[第29章 無線通信](#) (583 ページ)」を参照してください。

ティップ: CDMAおよびGPRSモデム

サポートされているCDMAおよびGPRSモデムを通常のモデムとしてYaSTモデムモジュール内で設定できます。

8.7 ネットワークサービス

このグループには、ネットワークにあるすべての種類のサービスを設定するツールが含まれています。これには名前解決、ユーザー認証、およびファイルサービスが含まれます。

8.7.1 メール転送エージェント

使用中のプロバイダのsendmail、postfix、またはSMTPサーバを使用して電子メールを送信する場合、[\[ネットワークサービス\]](#) > [\[Mail Transfer Agent\]](#) 内でメール設定を行えます。fetchmailプログラムを介してメールを受け取ることもできます。このプログラムには、お使いのプロバイダのPOP3またはIMAPサーバの詳細を入力することもできます。または、KMailまたはEvolutionなど、任意のメールプログラムを使用してアクセスデータを設定します。この場合、このモジュールは必要ありません。

YaSTを使用してメールを設定するには、最初のダイアログで、インターネットへの任意の接続タイプを指定します。次のオプションのいずれかを選択します。

常にネットワークと接続している

インターネット接続専用回線がある場合に、このオプションを選択します。マシンは永続的にオンラインであり、ダイヤルアップ接続は必要ありません。システムが、一元的な電子メールサーバを使用するローカルネットワークの一部であれば、電子メールメッセージに永続的にアクセスするためにこのオプションを選択します。

ダイヤルアップ

この項目は、ネットワーク上ではなく自宅にコンピュータがあり、時々インターネットに接続するユーザが対象です。

接続なし

インターネットへアクセスする方法がなく、ネットワークにも接続していない場合は、電子メールを送受信できません。

そのオプションを選択することにより、AMaViSを使用して着信および発信する電子メールに対してウィルススキャンを有効化することができます。メールフィルタリング機能を有効化すると、即座にまた自動的にこのパッケージがインストールされます。次のダイアログでは、発信メールサーバ(通常は使用中のプロバイダのSMTPサーバ)、および着信メールに対するパラメータを指定します。さまざまなユーザからのメール受信に対応するために、さまざまなPOPまたはIMAPサーバを設定します。このダイアログを使用して、エイリアス、マスカレードの使用、バーチャルドメインの設定も可能です。[完了]をクリックして、メール設定を終了します。

8.7.2 メールサーバ

重要項目: LDAPベースのメールサーバ設定

SUSE Linux Enterpriseのメールサーバモジュールはユーザ、グループ、DNSおよびDHCPサービスが、LDAPを使用して管理されている場合にのみ動作します。

このメールサーバモジュールを使用すると、SUSE Linux Enterpriseをメールサーバとして設定できます。YaSTでは次の設定プロセスの手順を使用できます。

グローバル設定

ローカルメールサーバの識別、着信および発信メッセージの最大サイズ、およびメール転送のタイプを設定します。

ローカル配信

ローカルメール配信のタイプを設定します。

メール転送

宛先アドレスに基づいて特別なメール転送ルートを設定します。

スパム防止

メールサーバのスパム防止の設定を行います。これでAMaViSツールを有効にします。SPAMチェックの種類と厳密度を設定します。

メールサーバ中継

メールサーバがローカルではないメールを送信するために使用できないネットワークを指定します。

メールの取得

さまざまなプロトコル介して外部のメールアカウントがメールを取得できる設定をします。

メールサーバドメイン

これは、メールサーバが役割を果たすドメインを指定します。メールを全く受信しないで送信専用としてマルチクライアントからサーバが実行されないようにするには、最低1つのマスタドメインを設定する必要があります。

次の3つの異なるドメインタイプを識別します。

メイン

ローカルメールサーバのメインまたはマスタドメイン

ローカル

マスタドメイン内でメールを受信できるすべてのユーザはローカルドメイン内のメールも受信できます。ローカルドメイン内のメッセージの場合は、@より前の部分だけで判断されます。

virtual

バーチャルドメイン内で明示的なアドレスを使用するユーザだけがメールを受信します。バーチャルメールアドレスは、YaSTのユーザ管理モジュールでセットアップします。

8.7.3 他の使用可能なサービス

YaSTの [ネットワークサービス] では、他の多くのネットワークモジュールを使用できます。

DHCPサーバ

これを使用すると、簡単な処理でカスタムDHCPサーバをセットアップできます。「[第34章 DHCP](#) (699 ページ)」には、この処理に関する基本的な情報と、設定プロセスに関する処理手順の段階的な説明が記載されています。

DNSサーバ

大規模なネットワークの場合、名前解決の役割を果たすDNSサーバを設定するようにお勧めします。これには、「[33.2項 「YaSTでの設定」](#) (674 ページ)」で説明しているように、[DNSサーバ] を使用できます。「[第33章 ドメインネームシステム](#) (673 ページ)」には、DNSの背景情報が記述されています。

DNSとホスト名

このモジュールを使用して、ネットワークデバイス設定中に設定されなかった場合の、ホスト名とDNSを設定します。ホスト名とドメイン名を変更する場合も、このモジュールを使用します。使用中のプロバイダがDSL、モデム、またはISDNアクセスを正常に設定した場合、ネームサーバのリストにはプロバイダのデータから自動的に抽出されたエントリが含まれています。ローカルネットワークに配置されている場合、ホスト名をDHCP経由で入手する場合があります、その場合は名前を変更しません。

HTTPサーバ

独自のWebサーバを稼動するには、[HTTPサーバ] でApacheを設定します。詳細情報については、[第40章 Apache HTTPサーバ](#) (807 ページ)を参照してください。

ホスト名

ブートの際、および小規模なネットワーク環境の場合は、DNSではなく [ホスト名] をホスト名解決に使用できます。このモジュールのエントリは、`/etc/hosts` ファイルのデータに反映されます。詳細については、[/etc/hosts 項 \(647 ページ\)](#)を参照してください。

Kerberosクライアント

ネットワーク認証でKerberosサーバがネットワークにない場合、[\[Kerberosクライアント\]](#)を使用します。YaSTを使用したクライアント設定に関する詳細は、[46.6項「YaSTを使ったKerberosクライアントの設定」 \(930 ページ\)](#)に説明しています。

LDAPクライアント

ネットワーク内で、ユーザ認証にLDAPを使用する場合は、[\[LDAPクライアント\]](#)内でクライアントを設定します。LDAPに関連する情報、およびYaSTを使用するクライアント設定の詳細については、[36.6項「YaSTを使ったLDAPクライアントの設定」 \(747 ページ\)](#)を参照してください。

LDAPサーバ

LDAPサーバは中心となるディレクトリにさまざまなデータを保存し、ネットワーク内のすべてのクライアントにそのデータを配信します。ほとんどの場合、共有された連絡先情報を保存するために使用されますが、その機能はそれ以外にも利用できます。LDAPサーバは認証にも使用できます。LDAPに関連する情報、およびYaSTを使用するサーバ設定の詳細については、[第36章LDAP—ディレクトリサービス \(725 ページ\)](#)を参照してください。

NFSクライアント

NFSクライアントでは、NFSサーバにより提供されたディレクトリを自分が所有するファイルツリーにマウントします。[\[NFSクライアント\]](#)を使用して、ご使用のシステムをネットワーク内のNFSサーバにアクセスするように設定します。

NFSサーバ

NFSを使用すると、ネットワークのすべてのメンバーがアクセス可能なファイルサーバを移動できます。ファイルサーバは、特定のアプリケーション、ファイル、および記憶域の容量を、ユーザに対して使用可能にするために使用されます。[\[NFSサーバ\]](#)内で、使用中のホストをNFSサーバとして設定し、ネットワークユーザにより一般的に使用されるエクスポートディレクトリを決定します。適切なアクセス権限を持つすべての

ユーザは、それらのディレクトリを、自分のファイルツリーにマウントできます。YaSTモジュールについての説明と、NFSについての背景情報は、「[第38章 NFS共有ファイルシステム](#) (779 ページ)」を参照してください。

NISクライアント

NISサーバを実行して中央でユーザデータを管理し、クライアントに配布する場合、クライアントツリーを設定します。NISクライアントについての詳細な情報、およびYaSTを使用する設定については、[35.2項「NISクライアントの設定」](#) (722 ページ)を参照してください。

NISサーバ

複数のシステムを運用している場合、ローカルユーザ管理(/etc/passwdと/etc/shadowファイルの使用)は現実的ではなく、管理に手間がかかります。この場合、ユーザデータは一元的なサーバによって管理され、そこからデータをクライアントに配布する必要があります。NISはこれに対するオプションの1つです。NISについての詳細な情報、およびYaSTを使用する設定については、[35.1.1項「NISマスタサーバの設定」](#) (716 ページ)を参照してください。

NTPクライアント

NTP(network time protocol)は、ネットワーク経由でハードウェアクロックを同期するためのプロトコルです。NTPについての詳細な情報、およびYaSTを使用する設定の説明については、[第32章 NTPによる時刻の同期](#) (667 ページ)を参照してください。

ネットワークサービス(xinetd)

[ネットワークサービス] を使用して、SUSE Linux Enterpriseのブート時に、ネットワークサービス(finger、talk、ftpなど)が開始するように設定します。これらのサービスは外部ホストを有効にして、コンピュータに接続します。さまざまなパラメータが、すべてのサービスに対して設定できます。デフォルトでは、個々のサービス(inetdまたはxinetd)を管理するマスタサービスは起動しません。

このモジュールが起動すると、inetdまたはxinetdを起動するかどうかを選択します。選択されたデーモンは一般的なサービスを選択して起動します。または、[追加]、[削除]、[編集] を使用して起動するサービスを独自に選択および構成します。

警告: ネットワークサービス(xinetd)の設定

システムのネットワークサービスの構成と調整は、処理が複雑で、Linux サービスの概念を包括的に理解する必要があります。通常は、デフォルトの設定のままで十分です。

プロキシ

[プロキシ] 内で、インターネットプロキシのクライアント設定を行います。[プロキシの有効化] をクリックして、任意のプロキシ設定を入力します。[プロキシ設定のテスト] をクリックして、これらの設定をテストできます。小さなウィンドウには、編集したプロキシ設定が正しく機能するかどうかが表示されます。設定を入力しテストし終わったら、[承認] をクリックして設定を保存します。

リモート管理

あるマシンを他のマシンからリモートで管理するには、[リモート管理] を使用します。システムのメンテナンスをリモートで実行できるようにするには、krdcまたはJava対応ブラウザなどのVNCクライアントを使用します。VNCを使用したリモート管理は簡単かつ迅速なのですが、SSHを使用するよりも安全ではないので、VNCサーバを使う場合は常にこのことに注意する必要があります。VNCクライアントのインストール方法の詳細については、[4.1.1項「VNC経由のシンプルリモートインストール—静的なネットワーク設定」](#) (54 ページ)を参照してください。

[リモート管理設定] 中の [リモート管理の許可] を選択して、リモート管理を許可します。[リモート管理の不許可] を選択すると、この機能が無効になります。[ファイアウォールで開いているポート] をクリックして、コンピュータへのアクセスを可能にします。[ファイアウォールの詳細] をクリックすると、ファイアウォールで開いているポートとともにネットワークインタフェースが表示されます。任意のインタフェースを選択し、[OK] をクリックして、メインダイアログに戻ります。[了解] をクリックして設定を完了します。

コンピュータ上でVNCを設定するには、YaSTの [リモート管理] モジュールの使用を推奨します。SaX2インタフェースを使用しても、リモートアクセスのプロパティを設定できますが、YaSTには適していません。SaX2は、お使いのXサーバをVNCセッションのホストとして設定できるようにするだけです。

ルーティング

「ルーティング」を使用して、データがネットワーク上を通るパスを設定します。ほとんどの場合、「デフォルトゲートウェイ」のすべてのデータを送信するのに使用するシステムのIPアドレスのみ入力します。より複雑な設定を作成するには、「エキスパート設定」を使用します。

Sambaサーバ

LinuxとWindowsホストにより構成される異種ネットワークでは、Sambaが2つの環境間の通信を制御します。Sambaに関して、およびクライアントとサーバの設定情報については、[第37章 Samba](#) (761 ページ)を参照してください。

SLPサーバ

service location protocol (SLP)を使用すると、るサーバ名と、これらのサーバが提供するサービスの知識がなくてもネットワークでクライアントを設定できます。SLPサーバについての詳細な情報、およびYaSTを使用する設定については、[第31章 ネットワーク上のSLPサービス](#) (663 ページ)を参照してください。

TFTPサーバ

TFTPサーバはFTPサーバではありません。FTPサーバはファイル転送プロトコル(FTP)を使用しますが、TFTPサーバはセキュリティ機能がない、非常に簡略化されたTrivial File Transfer Protocol(TFTP)を使用します。TFTPサーバは、サーバがディスクレスのワークステーション、Xターミナル、およびルータを起動する際によく使用されます。TFTPサーバについての詳細な情報、およびYaSTを使用する設定については、[4.3.2項 「TFTPサーバのセットアップ」](#) (76 ページ)を参照してください。

WOL

WOL (wake on LAN)とは、特殊なパッケージを使用して、ネットワーク上でコンピュータをスタンバイモードからウェイクアップする機能をさします。WOLは、BIOSでの機能をサポートするマザーボードでのみ使用できます。YaSTを使用してWOLを設定する方法は、「[4.3.7項 「Wake on LAN」](#) (84 ページ)」で説明しています。

Windows Domain Membership

LinuxとWindowsホストにより構成される異種ネットワークでは、Sambaが2つの環境間の通信を制御します。「Sambaクライアント」モジュールを使用すると、Windowsドメインのメンバとしてコンピュータを設定できま

す。Sambaに関する情報とクライアントの設定に関しては、[第37章 Samba](#) (761 ページ)を参照してください。

iSCSIターゲット

iSCSI技術はLinuxコンピュータを中央保存システムに接続するための簡単で合理的な安価なソリューションです。サーバサイドを設定するには、[\[その他\] > \[iSCSI Target\]](#) を使用します。YaSTを使用したiSCSIの設定に関する詳細は、[第12章 IPネットワークの大容量記憶デバイス—iSCSI](#) (297 ページ)を参照してください。

iSCSIイニシエータ

中央保存システムへの接続を設定するには、[\[その他\] > \[iSCSI Initiator\]](#) を使用します。YaSTを使用したiSCSIの設定に関する詳細は、[第12章 IPネットワークの大容量記憶デバイス—iSCSI](#) (297 ページ)を参照してください。

8.8 AppArmor

Novell AppArmorは、サーバとワークステーションの両方に対応する使いやすいアプリケーションセキュリティを提供するように設計されています。Novell AppArmorを使用するとプログラムごとに、ファイルを読み取り、書き込み、および実行する権限を設定することができます。システム上のNovell AppArmorを有効化または無効化するには、[\[AppArmorコントロールパネル\]](#) を使用します。Novell AppArmorに関連する情報、およびYaSTを使用するクライアント設定の詳細については、[Novell AppArmor 管理ガイド](#) ([↑Novell AppArmor 管理ガイド](#))を参照してください。

8.9 セキュリティとユーザ

Linuxの基本的な特徴の1つは、マルチユーザ機能です。つまり、複数のユーザが同じLinuxシステム上で個別に作業することができます。各ユーザは、システムにログインするためのログイン名と個人パスワードにより識別されるユーザアカウントを持ちます。すべてのユーザは独自のホームディレクトリを持ち、そこに個人的なファイルと設定を保存します。

8.9.1 ユーザ管理

[セキュリティとユーザ] > [ユーザ管理] を使用して、ユーザの作成および編集を行います。これは、必要があればNIS、LDAP、Samba、およびKerberos ユーザを含む、システム内のユーザの概要を提供します。ネットワークの一部の場合、すべてのユーザカテゴリを表示するには、[フィルタを設定] をクリックします。[Customize Filter] をクリックして、フィルタ設定をカスタマイズすることもできます。

ティップ: モジュールを終了しないで設定の変更を適用する

複数の設定を変更する必要があるけれども、そのたびにユーザ/グループモジュールを再起動する手間をかけたくない場合は、[変更を今すぐ書き込む] を使用します。このオプションを使用すると、設定モジュールを終了せずに、変更内容を保存することができます。

ユーザの追加

新しいユーザを追加するには、以下の手順に従ってください。

- 1 [Add] をクリックします。
- 2 [ユーザデータ] に必要な情報を入力します。このユーザに関する詳細設定を変更する必要がない場合は、**ステップ 5**(193 ページ)を参照してください。
- 3 ユーザのID、ホームディレクトリ名、デフォルトホーム、グループ、グループメンバーシップ、ディレクトリのパーミッション、またはログインシェルを変更する場合は、[詳細] タブを開いてデフォルト値を変更してください。
- 4 ユーザのパスワード有効期限、長さ、および期限切れ警告を設定するには、[パスワード設定] タブを使用します。
- 5 ユーザアカウントの設定内容を保存するには、[了解] をクリックします。

新しいユーザは新規作成されたログイン名とパスワードを使用してただちにログインできます。

ユーザの削除

ユーザを削除するには、以下の手順に従ってください。

- 1 リストからユーザを選択します。
- 2 [削除] をクリックします。
- 3 削除するユーザのホームディレクトリを保持するか、それとも一緒に削除するかを選択します。
- 4 設定内容を適用するには、[はい] をクリックします。

ログイン設定の変更

ログイン設定を変更するには、以下の手順に従ってください。

- 1 リストからユーザを選択します。
- 2 [Edit] をクリックします。
- 3 [ユーザデータ]、[詳細]、および [パスワード設定] の設定を変更します。
- 4 ユーザアカウントの設定内容を保存するには、[了解] をクリックします。

暗号化ホームディレクトリの管理

ユーザアカウント作成の一環として、暗号化ホームディレクトリを作成することができます。暗号化ホームディレクトリを作成するには、以下の手順に従ってください。

- 1 [Add] をクリックします。
- 2 [ユーザデータ] に必要な情報を入力します。
- 3 [詳細] タブで、[暗号化ホームディレクトリを使用] を選択します。

- 4 [了解] をクリックして、設定内容を反映します。

既存のユーザ用の暗号化ホームディレクトリを作成するには、以下の手順に従ってください。

- 1 リストからユーザを選択して、[編集] をクリックします。
- 2 [詳細] タブで、[暗号化ホームディレクトリを使用] を選択します。
- 3 選択したユーザのパスワードを入力してください。
- 4 [了解] をクリックして、設定内容を反映します。

ホームディレクトリの暗号化を無効にするには、以下の手順に従ってください。

- 1 リストからユーザを選択して、[編集] をクリックします。
- 2 [詳細] タブで、[暗号化ホームディレクトリを使用] の選択を解除します。
- 3 選択したユーザのパスワードを入力してください。
- 4 [了解] をクリックして、設定内容を反映します。

暗号化ホームの詳細は、[47.2項「暗号化ホームディレクトリの使用」](#) (948 ページ)を参照してください。

自動ログイン

警告: 自動ログインの使用

複数のユーザがアクセスできるような環境にあるシステムで自動ログイン機能を使用することには、セキュリティ上の危険性があります。そのようなシステムにアクセスできる任意のユーザが、システム内のデータを操作することができます。システムに機密情報などの重要なデータを保管している場合は、自動ログイン機能は使用しないでください。

自分のみが利用できるシステムの場合は、自動ログインを設定することができます。自動ログイン機能を使用すると、起動後に自動的にユーザのログインが行われます。選択した1人のユーザのみが自動ログイン機能を利用できます。自動ログイン機能は、KDMまたはGDMでしか使用できません。

自動ログインを有効にするには、目的のユーザをリストから選択して、次に [エキスパートオプション] > [ログイン設定] の順にクリックします。次に、[自動ログイン] を選択し、[OK] をクリックします。

この機能を無効にするには、ユーザを選択して [エキスパートオプション] > [ログイン設定] の順にクリックします。次に、[自動ログイン] の選択を解除して、[OK] をクリックします。

パスワードなしのログイン

警告: パスワードなしのログインの許可

複数のユーザがアクセスできるような環境にあるシステムでパスワードなしのログイン機能を使用することは、セキュリティ上の危険性があります。そのようなシステムにアクセスできる任意のユーザが、システム内のデータを操作することができます。システムに機密情報などの重要なデータを保管している場合は、この機能は使用しないでください。

パスワードなしのログイン機能を使用すると、ユーザがユーザ名を入力すれば、そのシステムにログインできます。この機能は、複数のユーザに適用することができます。また、KDMとGDMでしか利用できません。

この機能を有効にするには、目的のユーザをリストから選択して、次に [エキスパートオプション] > [ログイン設定] の順にクリックします。次に、[パスワードレスログイン] を選択し、[OK] をクリックします。

この機能を無効にするには、この機能を無効にするユーザをリストから選択し、[エキスパートオプション] > [ログイン設定] の順にクリックします。次に、[パスワードレスログイン] の選択を解除して、[OK] をクリックします。

ユーザログインを無効にする

システムにログインさせないけれども、そのユーザIDを使ってさまざまなシステム関連の作業を管理する必要があるようなユーザを作成するには、そのユーザアカウントの作成時にユーザログインを無効にします。次の手順に従います。

- 1 [Add] をクリックします。
- 2 [ユーザデータ] に必要な情報を入力します。
- 3 [ユーザログインを禁止] を選択します。
- 4 [了解] をクリックして、設定内容を反映します。

既存のユーザのログインを無効にするには、以下の手順に従ってください。

- 1 リストからユーザを選択して、[編集] をクリックします。
- 2 [ユーザデータ] の [ユーザログインを禁止] を選択します。
- 3 [了解] をクリックして、設定内容を反映します。

パスワードポリシーの強制

複数のユーザが使用するシステムでは、最低限のパスワードセキュリティポリシーを強制することをお勧めします。ユーザに定期的にパスワードを変更させたり、推測しにくいような複雑なパスワードを使用させることができます。厳格なパスワードルールの強制方法については、[8.9.3項「ローカルセキュリティ」](#) (200 ページ) を参照してください。パスワードを定期的に変更させる場合は、パスワードの有効期限に関するポリシーを作成します。

新規ユーザのパスワード有効期限ポリシーを作成するには、以下の手順に従ってください。

- 1 [Add] をクリックします。
- 2 [ユーザデータ] に必要な情報を入力します。

3 [パスワード設定] 内の値を調整します。

4 [了解] をクリックして、設定内容を反映します。

既存のユーザのパスワード有効期限ポリシーを作成するには、以下の手順に従ってください。

1 リストからユーザを選択して、[編集] をクリックします。

2 [パスワード設定] 内の値を調整します。

3 [了解] をクリックして、設定内容を反映します。

任意のユーザアカウントに対して、そのアカウントの有効期限を指定することができます。設定するには、[有効期限] に有効期限をYYYY-MM-DD(年月日)の形式で指定します。[有効期限] に値を指定しない場合、そのユーザアカウントに有効期限はありません。

新規ユーザのデフォルト設定の変更

新しくローカルユーザを作成する場合、YaSTはさまざまなデフォルトの設定値を使用します。これらのデフォルト設定値は、必要に応じて変更することができます。

1 [エキスパートオプション] > [Defaults for New Users] (新規ユーザのデフォルト)の順に選択します。

2 次の項目を、必要に応じて変更します。

- [Default Group] (デフォルトのグループ)
- [Secondary Groups] (セカンダリグループ)
- [Default Login Shell] (デフォルトのログインシェル)
- [Path Prefix for Home Directory] (ホームディレクトリのパスのプリフィックス)
- [Skeleton for Home Directory] (ホームディレクトリのスケルトン)

- *[Umask for Home Directory]* (ホームディレクトリのumask)
- *[Default Expiration Date]* (デフォルトの有効期限)
- *[Days after Password Expiration Login is Usable]* (パスワードの有効期限切れログインを使用できる日数)

3 変更内容を反映するには、*[了解]* をクリックします。

[ローカルセキュリティ] モジュールを使えば、他のさまざまなセキュリティ関連のデフォルト設定値を変更することができます。詳細については、[8.9.3 項「ローカルセキュリティ」](#) (200 ページ)を参照してください。

パスワード暗号化の変更

注意

パスワード暗号化の変更内容は、ローカルユーザにのみ適用されます。

SUSE Linux Enterpriseでは、パスワードの暗号化にDES、MD5、またはBlowfishを使用できます。パスワード暗号化手法のデフォルトは、Blowfishです。暗号化方法は、システムのインストール時に設定されます。詳細は、[3.14.1項「システム管理者向けパスワード「root」」](#) (42 ページ)を参照してください。インストール済みシステムのパスワード暗号化手法を変更するには、*[エキスパートオプション]* > *[パスワード暗号化]* の順にクリックします。

認証とユーザソースの変更

ユーザ認証手法(NIS、LDAP、Kerberos、Sambaなど)は、インストール時に設定されます。詳細は、[3.14.7項「Users」](#) (49 ページ)を参照してください。インストール済みシステムのユーザ認証手法を変更するには、*[エキスパートオプション]* > *[Authentication and User Sources]* (認証とユーザソース)の順にクリックします。このモジュールには、環境設定の概要と、クライアントを設定するためのオプションが表示されます。高度なクライアント設定も、このモジュールを使用して実行できます。

8.9.2 グループ管理

グループを作成および編集するには、[セキュリティとユーザ] > [グループ管理] を選択するか、ユーザ管理モジュールの [グループ] をクリックします。どちらのダイアログも、グループの作成、編集、削除という同じ機能を提供します。

モジュールでは、すべてのグループの概要が表示されます。ユーザ管理ダイアログのように、[フィルタを設定する] をクリックしてフィルタ設定を変更できます。

グループを追加するには、[追加] をクリックし、適切なデータを入力します。リストから対応するボックスにチェックを入れてグループメンバを選択します。[承認] をクリックすると、グループが作成されます。グループを編集するには、リストから編集するグループを選択し、[編集] をクリックします。必要な変更を加え、[承認] を使用して変更を保存します。グループを削除するには、リストからグループを選択し、[削除] をクリックします。

[エキスパート用オプション] をクリックすると、高度なグループ管理ができます。これらのオプションの詳細については、[8.9.1項「ユーザ管理」](#) (193 ページ)を参照してください。

8.9.3 ローカルセキュリティ

システム全体にセキュリティ設定セットを適用したい場合は、[セキュリティとユーザ] > [ローカルセキュリティ] を使用します。設定には、ブート、ログイン、パスワード、ユーザ作成、および権限用のセキュリティが含まれています。SUSE Linux Enterpriseには、[ホームワークステーション]、[ネットワークワークステーション]、および[ネットワークサーバ]の、事前設定された3種類のセキュリティセットが用意されています。[詳細]を使用して、デフォルトを修正します。自分のスキーマを作成するには、[カスタム設定] を使用します。

詳細またはカスタム設定には次のものが含まれます。

パスワードの設定

承認される前に、システムによってセキュリティのために新規パスワードの確認を行うには、[新規パスワードの確認] および [複雑なパスワード

のテスト] をクリックします。新規作成されたユーザ用に、最短のパスワードを設定します。パスワードを有効とする期限、またユーザがテキストコンソールにログインしたときに発行する期限切れの警告を、期限切れの何日前に表示するかを定義します。

ブート設定

キーの組み合わせ **Ctrl + Alt + Del** キーを使用して、どのようなアクションを実行するかを設定します。通常、この組み合わせが、テキストコンソールに入力されると、システムは再起動されます。使用中のマシンまたはサーバが、誰でも触ることができる場所にあり、誰かが承認なしにこのアクションを行う恐れがない限り、この変更を行わないでください。[中止] を選択すると、このキーの組み合わせを押すとシステムがシャットダウンします。[無視する] を選択すると、このキーの組み合わせは無視されます。

KDEログインマネージャ(KDM)を使用する場合は、[KDMのシャットダウン] でシステムをシャットダウンする権限を設定します。[ルートのみ] (システム管理者)、[全てのユーザ]、[該当者なし]、または[ローカルユーザ] に権限を与えます。[該当者なしが選択された場合、システムはテキストコンソール経由からのみシャットダウンできます。

ログイン設定

一般的に、ログイン試行が失敗した後、数秒待ってから、再度ログインが可能になります。これによりパスワードスニファのログインはさらに難しくなります。必要に応じて、[成功したログインを記録する] を有効化します。誰かがパスワードを見破ろうとしている可能性がある場合、/var/logにあるシステムログファイルのエントリを確認します。ユーザのグラフィカルログイン画面に、ネットワーク経由で別のユーザがアクセスできるようにするには、[リモートグラフィカルログインを許可する] を有効化します。このアクセス手段には潜在的なセキュリティリスクがあるため、デフォルトでは無効になっています。

ユーザの追加

各ユーザに数値とアルファベットで構成されたユーザIDが割り当てられます。これらの相関関係は、/etc/passwdファイルを介して確立され、可能な限り一意的である必要があります。この画面のデータを使用して、新しいユーザを追加するときに、ユーザIDの数値部分に割り当てる数字の範囲を定義します。ユーザには最低500が適切です。自動生成されるシステムユーザは1000から始まります。グループID設定も同じ方法で設定します。

その他の設定

事前定義されたファイルのパーミッション設定を使用するには、**[簡易]**、**[安全]**、または**[被害妄想]**を選択します。ほとんどのユーザには、**[簡易]**で十分です。**[被害妄想]**設定は非常に制約が強く、カスタム設定用には操作の基本レベルしか設定できません。**[被害妄想]**を選択する場合、一部のプログラムは適切に動作しないか、まったく動作しない可能性があります。これは、ユーザが特定のファイルへのアクセス権を失うためです。

インストールされている場合は、どのユーザがupdatedbプログラムを起動するかも設定します。このプログラムは、毎日またはブート後に自動的に実行され、コンピュータ上の各ファイルの場所が保存されるデータベース(locatedb)を生成します。**[該当者なし]**を選択する場合、すべてのユーザは、他の(アクセス権のない)ユーザが参照可能なデータベースへのパスのみを参照できます。**root**が選択された場合、すべてのローカルファイルにインデックスが付けられます。これは、スーパーユーザである**root**ユーザがすべてのディレクトリにアクセスするためです。**[カレントディレクトリをrootユーザのパスに追加する]**および**[カレントディレクトリを通常ユーザのパスに追加する]**のオプションが、無効化されていることを確認します。これらの設定は、正しく使用されないとセキュリティ上に深刻なリスクを生じる恐れがあるので、上級ユーザのみこれらのボックスにチェックを入れるようにします。システムがクラッシュしても、ある程度システムを制御できるようにするには、**[マジックSysRqキーの有効化]**をクリックします。

[完了] をクリックして、セキュリティ設定を完了します。

8.9.4 証明書管理

証明書は通信用に使用されます。また、たとえば、会社のIDカードにも使用されます。共通のサーバ証明書を管理またはインポートするには、**[セキュリティとユーザ] > [CA管理]**を使用します。YaSTを使用した証明書、その技術、および管理に関する詳細については、**第42章 X.509 証明書の管理**(875ページ)を参照してください。

8.9.5 ファイアウォール

SuSEfirewall2は、インターネットからの攻撃に対してマシンを保護します。
[セキュリティとユーザ] > [ファイアウォール] を使用して設定します。
SuSEfirewall2の詳細については、[第43章 マスカレードとファイアウォール](#) (893 ページ)を参照してください。

ティップ: ファイアウォールの自動有効化

YaSTは、すべての設定済みネットワークインターフェース上で、適切な設定を使用してファイアウォールを自動的に起動します。カスタム設定を使用してファイアウォールを再設定するか、無効にする場合にのみ、このモジュールを起動します。

8.10 仮想化

仮想化機能を使用すると、1台の物理的なコンピュータ上でLinuxシステムを複数起動できます。異なるシステム用のハードウェアは仮想的に提供されます。YaSTの仮想化モジュールでは、Xen仮想化システムの環境設定を行えます。この技術の詳細については、<http://www.novell.com/documentation/sles10/index.html>の仮想化マニュアルを参照してください。

[仮想化] セクションでは、次のモジュールを利用できます。

ハイパーバイザとツールのインストール

Xenの使用を開始する前に、Xenをサポートするカーネルと関連ツールをインストールしてください。これらをインストールするには、[仮想化] > [ハイパーバイザとツールのインストール] の順に選択します。インストール後は、システムを再起動してXenカーネルを使用してください。

仮想マシンの作成

Xenハイパーバイザとツールをインストールしたら、仮想サーバ上に仮想マシンをインストールすることができます。仮想マシンをインストールするには、[仮想化] > [仮想マシンの作成] の順に選択します。

8.11 その他

YaSTコントロールセンターには、最初の6つのモジュールグループには単純に分類できないモジュールがいくつかあります。それらのモジュールは、ログファイルの表示およびベンダCDからのドライバのインストールなどのような機能に使用できます。

8.11.1 カスタムインストールCDの作成

[その他] > [CD Creator] の順に選択して、オリジナルのインストールセットからカスタマイズしたインストールCDを作成することができます。作成を開始するには、[追加] をクリックします。パッケージマネージャを使用してパッケージを選択するか、AutoYaSTコントロールファイルを選択して仮設定されたAutoYaSTプロファイルを使用し、CDを作成します。

8.11.2 インストールサーバの設定

ネットワークインストールには、インストールサーバが必要です。そのサーバを設定するには、[その他] > [インストールサーバ] を使用します。YaSTを使用したインストールサーバの設定に関する詳細は、[4.2.1項「YaSTを使ったインストールサーバのセットアップ」](#) (63 ページ)を参照してください。

8.11.3 自動インストール

AutoYaSTツールは、自動インストールを目的にしています。[その他] > [Autoinstallation]で、このツール用のプロファイルを作成します。AutoYaSTを使用した自動インストールに関する詳細は、[第5章 自動インストール](#) (95 ページ)を参照してください。[Autoinstallation] モジュールの使用法に関する情報は、「[5.1.1項「AutoYaSTプロファイルの作成」](#) (96 ページ)」にあります。

8.11.4 サポートに関するクエリ

[その他] > [Support Query] は、問題を検出するためにサポートチームが必要とするすべてのシステム情報を収集することができ、できる限りその問題を解決するための支援を受けることができます。クエリに関して、次のウィ

ンドウで問題のカテゴリを選択してください。すべての情報が収集されたら、それをサポートリクエストに添付します。

8.11.5 リリースノート

リリースノートはインストール、更新、設定、および技術的問題についての重要な情報源です。リリースノートは継続的に更新され、オンラインアップデートで公開されます。[その他] > [リリースノート] を使用して、リリースノートを表示します。

8.11.6 起動ログ

[その他] > [起動ログの表示] 内では、コンピュータの起動時に関わる情報を表示します。これは、システム上で問題が発生したり、トラブルシューティングを行う際に、真っ先に確認したいモジュールです。このモジュールは、ブートログ/var/log/boot.msgを表示します。これには、コンピュータが起動するときに表示される画面メッセージが含まれています。このログは、コンピュータが正常に起動したか、すべての機能とサービスが正常に起動したか、を判別するのに使用されます。

8.11.7 システムログ

[その他] > [システムログ] を使用して、var/log/messages内にコンピュータの稼働状況を追跡して保存するシステムログを表示します。日時順のカーネルメッセージもここで記録されます。最上部にあるボックスを使用して、特定のシステムコンポーネントの状態を表示します。以下のオプションが、システムログおよびブートログモジュールから利用可能です。

/var/log/messages

一般的なシステムログファイルです。このログには、カーネルメッセージ、rootでログインしたユーザ、およびその他の役立つ情報が表示されます。

/proc/cpuinfo

プロセッサのタイプ、製造元、モデル、およびパフォーマンスなどを含む情報を表示します。

/proc/dma

どのDMAチャネルが現在使用されているかを表示します。

/proc/interrupts

どの割り込みが使用されているか、各割り込みの使用回数を表示します。

/proc/iomem

入力/出力メモリの状態を表示します。

/proc/ioports

その時点でどのI/Oポートが使用されているかを表示します。

/proc/meminfo

メモリの状態を表示します。

/proc/modules

個々のモジュールを表示します。

/proc/mounts

現在マウントされているデバイスを表示します。

/proc/partitions

すべてのハードディスクのパーティション設定を表示します。

/proc/version

現在のLinuxバージョンを表示します。

+/var/log/YaST2/y2log

すべてのYaSTログメッセージが表示されます。

/var/log/boot.msg

システム起動関連の情報を表示します。

/var/log/faillog

ログイン失敗に関する情報を表示します。

/var/log/warn

すべてのシステム警告を表示します。

8.11.8 ベンダのドライバCD

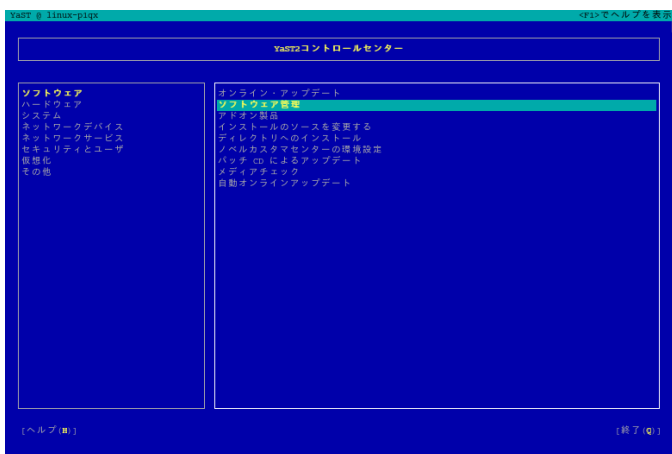
[その他] > [Vendor Driver CD] を使用して、SUSE Linux Enterprise用のドライバが含まれているLinuxドライバCDから、デバイスドライバをインストールします。SUSE Linux Enterpriseを最初からインストールした場合、このYaSTモジュールを使用して、インストール後にベンダが提供するCDから必要なドライバをロードします。

8.12 テキストモードのYaST

このセクションは、システムでXサーバを実行せずに、テキストベースのインストールツールを使用しているシステム管理者や専門家の方を対象にしています。ここでは、YaSTをテキストモードで開始、操作するための、基本的な情報を説明しています。

YaSTをテキストモードで起動すると、YaSTコントロールセンターが最初に表示されます。参照先 [図 8.9. 「テキストモードのYaSTのメインウィンドウ」](#) (208 ページ). このメインウィンドウは、以下の3つの主要領域で構成されています。太い白枠で囲まれた左側のフレームには、各種モジュールが属するカテゴリが示されます。アクティブカテゴリは、背景色付きで示されています。細い白枠で囲まれた右側のフレームには、アクティブカテゴリで使用可能なモジュールの概要が示されています。下方のフレームには、[ヘルプ] および [終了] 用のボタンがあります。

図 8.9 テキストモードのYaSTのメインウィンドウ



YaSTコントロールセンターが起動されると、カテゴリ [ソフトウェア] が自動的に選択されます。カテゴリを変更するには、↓と↑を使用します。選択したカテゴリからモジュールを起動するには、→を押します。選択したモジュールがここで太い枠付きで表示されます。必要なモジュールを選択するには、↓と↑を使用します。矢印キーを押したままにして、使用可能なモジュールのリストをスクロールします。モジュールを選択すると、モジュールのタイトルが背景色付きで表示され、簡単な説明が下方のフレームが表示されます。

<Enter>キーを押して、必要なモジュールを起動します。モジュール内のさまざまなボタンまたは選択フィールドには、別の色(デフォルトでは黄色)の文字が含まれます。そのまま<Tab + Alt+yellow_letter>キーでナビゲートする代わりとなるボタンを選択するには、を使用します。Alt + Qを押すか、または [終了] を選択してEnterを押して、YaSTコントロールセンターを終了します。

8.12.1 モジュールでのナビゲーション

以降では、YaSTモジュール内のコントロール要素について、ファンクションキーとAltキーの組み合わせがすべて機能し、別のグローバル機能を割り当てられていないことを前提として説明します。可能性のある例外事項については、[8.12.2項「キーの組み合わせの制約」](#) (210 ページ)を参照してください。

ボタンおよび選択リスト間のナビゲーター

ボタン間および選択リストを含むフレーム間でナビゲートするには、**Tab**キーと**Alt + Tab**キーまたは**Shift + Tab**キーを使用します。

選択リストでのナビゲーター

選択リストを含むアクティブフレーム内の個々の要素間でナビゲーターするには、矢印キー(↑と↓)を使用します。フレーム内の個別エントリがその幅を超える場合は、**Shift + →**または**Shift + ←**を使用して、右または左にスクロールします。代わりに**Ctrl + E**または**Ctrl + A**を使用することもできます。この組み合わせは、コントロールセンターの場合のように、**→**または**←**を使用したのでは、アクティブフレームまたは現在の選択リストが変更されてしまう場合に使用できます。

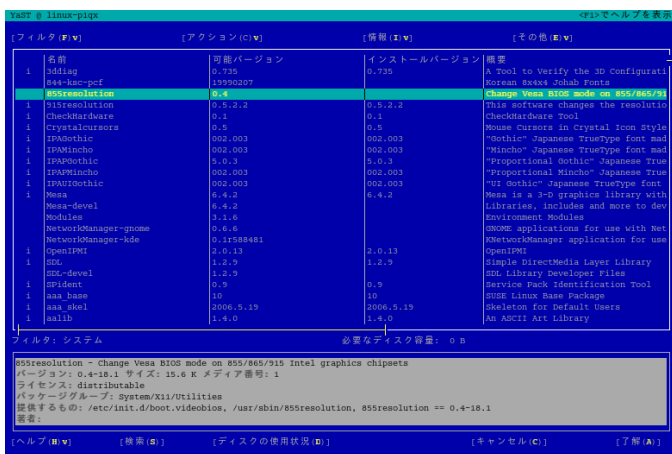
ボタン、ラジオボタン、およびチェックボックス

☐ が付いているボタン(チェックボックス)または☐が付いているボタン(ラジオボタン)を選択するには、**<Space>**キーまたは**<Enter>**キーを押します。代わりに、**Alt + yellow_letter**でラジオボタンおよびチェックボックスを直接選択することもできます。この場合、**<Enter>**キーによる確認は不要です。**<Tab>**キーでアイテムにナビゲートする場合は、**<Enter>**キーを押して、選択したアクションを実行するか、対応するメニューアイテムをアクティブにします。

ファンクションキー

Fキーの(**F1**から**F12**を使用すると、さまざまなボタンの機能を素早く利用できます。どのファンクションキーが実際にどのボタンにマップされているかは、アクティブになっているYaSTモジュールによります。提供されるボタン([詳細] 、 [情報] 、 [追加] 、 [削除] など)は、モジュールごとに異なるからです。**F10**は、 [OK] 、 [次へ] 、 および [完了] の代用として使用します。**F1**キーを押すと、YaSTのヘルプが表示され、個々の**F**キーにマップされた機能がそのヘルプに表示されます。

☒ 8.10 ソフトウェアインストールモジュール



8.12.2 キーの組み合わせの制約

ウィンドウマネージャがグローバルなAltキーの組み合わせを使用していると、YaSTでのAltキーの組み合わせが機能しない場合があります。AltやShiftなどのキーは、端末の設定に専有されている場合もあります。

<Alt>キーを<Esc>キーの代用とする

Altショートカットは、<Alt>キーの代わりに<Esc>キーでも実行できます。たとえば、Esc-Hは、Alt+Hの代わりとなります。(まずEscを押して、次にHを押します)。

Ctrl+FとCtrl+Bによる前後のナビゲーション

AltとShiftの組み合わせがウィンドウマネージャまたは端末に専有されている場合は、Ctrl+F(進む)とCtrl+B(戻る)を代わりに使用できます。

ファンクションキーの制約

Fキーは、各種機能にも使用されます。一部のファンクションキーは、端末に専有され、YaSTで使用できない場合があります。ただし、<Alt>キーのキーの組み合わせとファンクションキーは、ピュアテキストコンソールでは常に完全に使用できます。

8.13 コマンドラインからのYaSTの管理

一般的に、作業を1回だけ行うような場合は、グラフィカルインタフェースまたはncursesインタフェースの利用が最適です。ただし、その作業を繰り返す必要があるような場合は、YaSTのコマンドラインインタフェースを利用した方が便利なこともあります。このインタフェースでは、カスタムスクリプトを使って作業を自動化することもできます。

システムで利用できるモジュールのリストを表示するには、「yast -l」または「yast --list」と入力します。モジュールで利用できるオプションを表示するには、「yast モジュール名 help」と入力します。モジュールにコマンドラインモードがない場合は、その旨を知らせるメッセージが表示されます。

モジュールのコマンドオプションのヘルプを表示するには、「yast モジュール名 コマンド help」と入力します。オプション値を設定する場合は、「yast モジュール名 コマンド オプション=値」と入力します。

一部のモジュールは、同じ機能を持つコマンドラインツールがすでに存在しているため、コマンドラインモードをサポートしていません。このようなモジュールと、関連するコマンドラインツールを以下に示します。

sw_single

sw_singleは、パッケージ管理、システムアップデート機能を提供しています。スクリプトでは、YaSTの代わりにrugを使用してください。[9.1 項「コマンドラインからrugを使った更新」](#) (224 ページ)を参照してください。

online_update_setup

online_update_setupは、システムの自動アップデートを設定します。cronコマンドも、同じ機能を提供しています。

inst_suse_register

inst_suse_registerを使って、SUSE Linux Enterpriseを登録することができます。登録の詳細は、[8.3.4 項「SUSE Linux Enterpriseの登録」](#) (156 ページ)を参照してください。

hwinfo

hwinfoは、システムハードウェアに関する情報を提供します。hwinfoコマンドも、同じ機能を提供しています。

GenProf、LogProf、SD_AddProfile、SD_DeleteProfile、SD_EditProfile、SD_Report、およびsubdomain

これらのモジュールは、AppArmorを制御、設定します。AppArmorには、独自のコマンドラインツールがあります。

8.13.1 ユーザの管理

従来のコマンドとは異なり、ユーザ管理用のYaSTコマンドは、ユーザの作成、変更、削除時に、システムに設定されている認証方法とデフォルトのユーザ管理設定を考慮します。たとえば、ユーザの追加時、または追加後にホームディレクトリを作成したり、skelファイルをコピーする必要はありません。ユーザ名とパスワードを入力すれば、デフォルトの設定に基づいて自動的に他の設定が行われます。コマンドラインが提供する機能は、グラフィカルインタフェースが提供する機能と同じです。

YaSTモジュールusersは、ユーザ管理に用いられます。コマンドのオプションを表示するには、`yast users help`と入力してください。

複数のユーザを追加する場合は、`/tmp/users.txt`ファイルを作成して、追加するユーザを指定してください。1行あたり1つのユーザ名を入力してから、次のスクリプトを使用します。

例 8.2 複数ユーザの追加

```
#!/bin/bash
#
# adds new user, the password is same as username
#

for i in `cat /tmp/users.txt`;
do
    yast users add username=$i password=$i
done
```

追加の場合と同様に、`/tmp/users.txt`に定義されているユーザを削除することもできます。

例 8.3 複数ユーザの削除

```
#!/bin/bash
#
# the home will be not deleted
# to delete homes, use option delete_home
#

for i in `cat /tmp/users.txt`;
do
yast users delete username=$i
done
```

8.13.2 ネットワークとファイアウォールの設定

ネットワークおよびファイアウォール設定コマンドは、しばしばスクリプト内で用いられます。ネットワーク設定には `yast lan` を、ファイアウォール設定には `yast firewall` を使用します。

YaST ネットワークカード設定オプションを表示するには、`yast lan help` と入力します。YaST ファイアウォール設定オプションを表示するには、`yast firewall help` と入力します。YaST を使ったネットワークおよびファイアウォールの設定は、一時的なものではなく永続的に保持されます。再起動後にもう一度スクリプトを実行する必要はありません。

ネットワークの環境設定の概要を表示するには、`yast lan list` を使用します。例 8.4. 「`yast lan list` コマンドの出力例」(213 ページ)を実行すると、最初にデバイスIDが表示されます。デバイスの詳細な設定情報を表示する場合は、`yast lan show id=<number>` を使用します。たとえば、この例では、`yast lan show id=0` と入力します。

例 8.4 `yast lan list` コマンドの出力例

```
0          Digital DECchip 21142/43, DHCP
```

YaST ファイアウォール設定用コマンドラインインタフェースを使用すれば、サービス、ポート、またはプロトコルを簡単に有効/無効にすることができま

す。許可されているサービス、ポート、およびプロトコルを表示するには、`yast firewall services show`を使用します。サービスやポートを有効にする方法の例を表示するには、`yast firewall services help`を使用します。IPマスカレードを有効にするには、`yast firewall masquerade enable`と入力します。

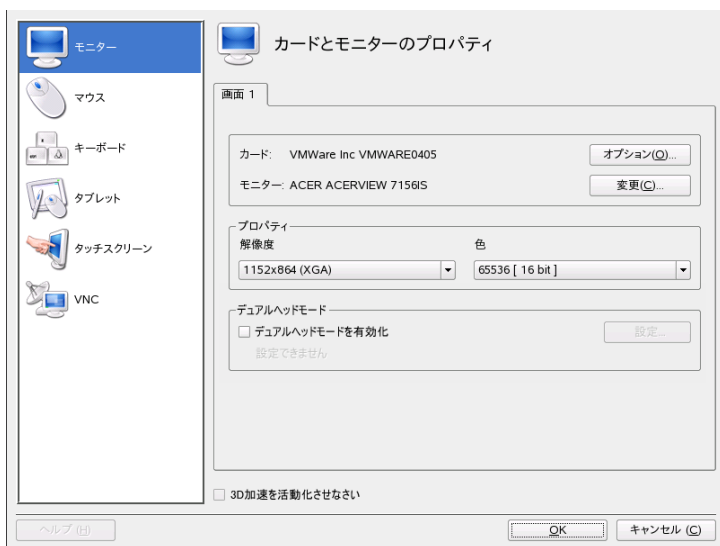
8.14 SaX2

[ハードウェア] > [グラフィックカードとモニタ] を使用して、システムのグラフィック環境を設定します。そうすると、マウス、キーボード、またはディスプレイデバイスのようなデバイスの設定ができるSUSE詳細設定インタフェース(SaX2)が開きます。このインタフェースは、GNOMEメインメニューから [コンピュータ] > [その他のアプリケーション] > [システム] > [Sax2] の順に選択して、またはKDEのメインメニューから [システム] > [設定] > [Sax2] の順に選択して表示することもできます。

8.14.1 カードおよびモニタのプロパティ

[Card and Monitor Properties] グラフィックカードの設定およびディスプレイデバイスを調整します。複数のグラフィックカードがインストールされている場合は、各デバイスは別のタブ付きダイアログに表示されます。ダイアログの上部には、選択したグラフィックカードおよび接続されているモニタの現在の設定が表示されます。複数の画面がカードに接続されている場合は(デュアルヘッド)、主出力のモニタが表示されます。通常、カードおよびディスプレイデバイスはインストール中にシステムで自動検出されます。ただし、多くのパラメータを手動で調整したり、ディスプレイデバイスを完全に変更したりすることもできます。

図 8.11 カードおよびモニタのプロパティ



ティップ: 新しいディスプレイハードウェアの自動検出

インストール後にディスプレイハードウェアを変更する場合は、コマンドラインで `sax2 -r` を入力します。これにより、**SaX2** がハードウェアを検出します。コマンドラインで **SaX2** を実行するには、`root` である必要があります。

グラフィックカード

グラフィックカードを変更することはできません。その理由は、既知のモデルのみサポートされており、それらは自動検出されるからです。ただし、カードの動作に影響を与えるような多くのオプションがあり、これらを変更することはできます。通常は、インストール時にシステムが適切にカードの設定を行っているので、オプションの変更は必要ではありません。上級者で、一部のオプションを変更する場合は、グラフィックカードの隣の **[オプション]** をクリックし、変更するオプションを選択します。特定のオプションに必要な値を指定するには、このオプションの選択後に表示されるダイアログで値を入力します。 **[OK]** をクリックして、このダイアログを閉じます。

Monitor

モニタの現在の設定を変更するには、モニタの隣の [変更] をクリックします。モニタ特有のさまざまな設定を調整できる新しいダイアログが開きます。このダイアログには、さまざまなモニタの動作向けに、複数のタブがあります。ベンダーおよびディスプレイデバイスのモデルをリストから手動で選択するには、最初のタブを選択します。モニタがリストに含まれていないとき、ベンダーのドライバディスクかCDを持っている場合は、ニーズに合わせていずれかのVESAまたはLCDモデルを選択します。 [Utility Disk] をクリックし、画面の指示に従ってこれを使用します。電源管理信号を使用するには、 [Activate DPMS] をオンにします。 [Display Size] (モニタの寸法プロパティ) と [Sync Frequencies] (モニタの水平および垂直同期周波数) は、システムで正しくセットアップされますが、これらの値を手動で変更することもできます。すべての調整を行った後、 [OK] をクリックしてこのダイアログを閉じます。

警告: モニタの周波数の変更

安全機構が付いていますが、モニタの周波数を手動で変更する場合は特に注意する必要があります。不正な値を設定した結果、モニタが壊れることがあります。周波数を変更する際は、必ずモニタの付属マニュアルを参照してください。

解像度およびカラー設定

解像度および色深度は、ダイアログの^ん中にある2つのリストから直接選択できます。ここで選択する解像度は、使用可能な最高の解像度になります。640x480に至るまでの一般的な解像度は、すべて設定に自動的追加されます。使用するデスクトップによっては、後で再設定することなくこれらの設定のいずれかに切り替えることができます。

デュアルヘッド

2つの出力のあるグラフィックカードがコンピュータにインストールされている場合、システムに2つの画面を接続できます。同じグラフィックカードに接続されている2つの画面は、デュアルヘッドと呼ばれます。SaX2は、システム上の複数のディスプレイデバイスを自動的に検出し、それに応じて設定の準備を行います。グラフィックカードのデュアルヘッドモードを使用するには、

ダイアログ下部の *[Activate Dual Head Mode]* をオンにし、*[設定]* をクリックして、デュアルヘッドダイアログでデュアルヘッドオプションおよび画面の配置を設定します。

ダイアログの上端の列内にある各タブは、ご使用のシステムのグラフィックカードに対応します。下のダイアログで設定するカードを選択し、マルチヘッドオプションを設定します。マルチヘッドダイアログの上部で、*[変更]* をクリックして、他の画面を設定します。設定可能なオプションは、最初の画面と同じです。リストから、この画面用に使用する解像度を選択します。3つのマルチヘッドモードからいずれかを選択します。

複製されたマルチヘッド

このモードでは、すべてのモニタに同じ内容が表示されます。マウスは、メイン画面でのみ表示されます。

Xineramaマルチヘッド

すべての画面を組み合わせて1つの大きな画面を形成します。すべての画面でプログラムウィンドウを自由に配置したり、複数のモニタのサイズに合わせたりできます。

注意

現在、Linuxでは、Xineramaマルチヘッド環境用3Dサポートはありません。この場合、SaX2で3Dサポートは無効にされます。

デュアルヘッドの環境の配置は、個々の画面の順序を説明しています。デフォルトでは、グラフィックカードの検出順に従って標準レイアウトがSaX2によって設定され、すべての画面が左から右に1列に並べられます。ダイアログの *[Arrangement]* でいずれかのシーケンスボタンを選択し、モニタの配置方法を決定します。 *[OK]* をクリックして、このダイアログを閉じます。

ティップ: ラップトップコンピュータでのプロジェクタの使用

ラップトップコンピュータにプロジェクタを接続するには、デュアルヘッドモードを有効化します。この場合、SaX2は外部出力を1024x768の解像度および60Hzのリフレッシュレートに設定します。これらの値は、プロジェクタに最も適しています。

マルチヘッド

コンピュータに複数のグラフィックカードがインストールされている場合、システムに複数の画面を接続できます。複数の画面が異なるグラフィックカードに接続されている場合は、マルチヘッドと呼ばれます。SaX2は、システム内の複数のグラフィックカードを自動検出し、適切に設定準備を行います。デフォルトでは、SaX2は、検出されたグラフィックカードのシーケンスに従って、すべての画面を左から右に配置する標準レイアウトを設定します。他の *[Arrangement]* タブを使用して、このレイアウトを手動で変更できます。グリッド内で各画面を表すアイコンをドラッグし、*[OK]* をクリックしてダイアログを閉じます。

設定のテスト

モニタおよびグラフィックカードの設定を完了した後は、メインウィンドウで *[OK]* をクリックして設定をテストします。これにより、設定がデバイスに適しているかどうかを確認できます。画像が安定しない場合は、**Ctrl+Alt+Backspace** キーを押して、テストをすぐに終了し、リフレッシュレートまたは解像度およびカラー設定の値を下げます。

注意

テストを実行する、しないにかかわらず、すべての変更はXサーバを再起動した場合にのみ有効になります。

8.14.2 マウスのプロパティ

マウスの設定は、*[Mouse Properties]* で調整します。ドライバが異なる複数のマウスをインストールしている場合、各ドライバは別のタブに表示されます。同じドライバによって操作される複数のデバイスは、1つのマウスとして表示されます。ダイアログの上部のチェックボックスを使用して、現在選択されているマウスを有効または無効にします。チェックボックスの下には、このマウスの現在の設定が表示されます。通常、マウスは自動検出されますが、自動検出が失敗した場合にのみ手動で変更できます。お使いのマウスモデルに関する説明は、マウスのドキュメントを参照してください。 *[変更]* をクリックして、2つのリストからベンダーおよびモデルを選択し、*[OK]* をクリックして選択内容を確定します。ダイアログのオプション部分で、マウス操作の各オプションを設定します。

Activate 3-Button Emulation

お使いのマウスに2つのボタンしかない場合、2つのボタンを同時にクリックすると3つ目のボタンがエミュレーションされます。

Activate Mouse Wheel

スクロールホイールを使用するには、このボックスをオンにします。

[*X軸を反転させます*] と [*Y軸を反転させます*]

いずれかのオプションを選択すると、マウスポインタが反対方向に移動します。この機能は、タッチパッドを使用する場合などに役立ちます。

Emulate Wheel with Mouse Button

マウスにスクロールホイールがないが、同様の機能を使用したい場合、このオプションで追加ボタンを指定できます。使用するボタンを選択します。このボタンを押している間、マウスの動きはスクロールホイールのコマンドに変換されます。この機能は、トラックボールの場合に特に便利です。

設定が完了したら、 [*OK*] をクリックして、変更を確定します。

注意

ここで行った変更内容は、Xサーバを再起動した後でのみ適用されます。

8.14.3 キーボードのプロパティ

このダイアログを使用して、グラフィカル環境でのキーボードの操作用設定を調整します。ダイアログの上部で、種類、言語レイアウト、およびバリエーションを選択します。ダイアログの下部のテストフィールドを使用して、特殊文字が正しく表示されるかどうかを確認します。真ん中のリストから、使用したい追加のレイアウトおよびバリエーションを選択します。お使いのデスクトップのタイプによって、これらは稼働中のシステムで再設定する必要なく切り替えられます。 [*OK*] をクリックすると、変更がすぐに適用されます。

8.14.4 タブレットのプロパティ

このダイアログを使用して、お使いのシステムに接続されたグラフィックタブレットの設定を行います。 [*グラフィックタブレット*] タブをクリックし

て、リストからベンダとモデルを選択します。現在の所、一部のグラフィックタブレットのみがサポートされています。タブレットを有効化するには、ダイアログの上端にある [このタブレットの有効化] にチェックを入れます。

Port and Mode ダイアログ内で、タブレットへの接続を設定します。SaX2では、USBポートかシリアルポートに接続されているタブレットの設定が可能です。タブレットがシリアルポートに接続されている場合、ポートを確認します。/dev/ttyS0は、最初のシリアルポートを示します。/dev/ttyS1は、2番目のシリアルポートを示します。追加のポートも同様の命名規則が適用されます。適切な [オプション] をリストから選択し、お客さまのニーズに合った [primary tablet mode] を選択します。

お使いのグラフィックタブレットが電子ペンをサポートしている場合、[電子ペン] の中で設定します。[プロパティ] をクリックしたあと、消しゴムとペンを追加し、それらのプロパティを設定します。

設定が満足行くものであれば、[OK] をクリックして変更を確定します。

8.14.5 タッチスクリーンのプロパティ

このダイアログを使用して、システムに接続されているタッチスクリーンを設定します。複数のタッチスクリーンが取り付けられている場合は、各デバイスは別のタブ付きダイアログに表示されます。現在選択しているタッチスクリーンを有効にするには、ダイアログ上部の [Assign a Touchscreen to Display] をオンにします。下のリストからベンダーおよびモデルを選択し、下部で適切な [Connection Port] を設定します。USBポートまたはシリアルポートに接続されているタッチスクリーンを設定できます。タッチスクリーンがシリアルポートに接続されている場合、ポートを確認します。/dev/ttyS0は、最初のシリアルポートを示します。/dev/ttyS1は、2番目のシリアルポートを示します。追加のポートも同様の命名規則が適用されます。設定が完了したら、[OK] をクリックして、変更を確定します。

8.15 トラブルシューティング

すべてのエラーメッセージおよびアラートは、/var/log/YaST2ディレクトリにログが記録されます。YaSTに関する問題を発見するための最も重要なファイルは、y2logです。

8.16 詳細情報

YaSTの詳細については、以下のWebサイトおよびディレクトリから入手可能です。

- `/usr/share/doc/packages/yast2`—ローカルのYaST開発文書
- http://www.opensuse.org/YaST_Development—openSUSE wikiのYaSTプロジェクトページ
- <http://forge.novell.com/modules/xfmod/project/?yast>—他のYaSTプロジェクトページ

ZENworksを使ったソフトウェアの管理

SUSE Linux Enterpriseを、Novell ZENworks Linux Managementが管理する環境に統合することができます。これには、オープンソースのZENworks管理エージェント、バックエンドデーモン、およびユーザスペースソフトウェア管理ツールが含まれています。Novell ZENworksパッケージ管理ツールは、ZENworks Linux Managementサーバを使って、パッケージやアップデートのダウンロードを行います。ローカルネットワーク内でZENworks Linux Managementサーバを利用できる場合、Novell Customer Centerからアップデートを入手することができます。Novell Customer Centerについては、[3.14.4項「ノベルカスタマセンターの環境設定」](#) (46 ページ)を参照してください。

Novell ZENworks Linux管理エージェント用のバックエンドデーモンは、ZENworks管理デーモン(ZMD)です。ZMDは、ソフトウェア管理機能进行处理します。このデーモンは、ブート時に自動的に開始されます。

このデーモンのステータスをチェックするには、`rczmd status`を使用します。デーモンを実行するには、`rczmd start`と入力してください。再開する場合、`rczmd restart`と入力します。無効にする場合は、`rczmd stop`と入力します。

ZMDは、その動作を制御するオプションを指定して実行することができます。常にオプションを指定してZMDを起動する場合は、`/etc/sysconfig/zmd`にZMD_OPTIONSを設定してから、`SuSEconfig`を実行します。使用できるオプションは次のとおりです。

`-n, --no-daemon`

このデーモンをバックグラウンドでは実行しません。

-m, --no-modules

モジュールをロードしません。

-s, --no-services

初期サービスをロードしません。

-r, --no-remote

リモートサービスを開始しません。

ZMDの環境設定情報は、`/etc/zmd/zmd.conf`に保管されます。この情報は手動で変更することも、`rug`を使って変更することもできます。初期スタートアップ時に`zmd`が使用するZENworksサービスのURL、および登録キーは、`/var/lib/zmd`に保管されます。アップデートは、`/var/cache/zmd`にあるZMDキャッシュにダウンロードされます。

ZMDはバックエンド専用です。ソフトウェア管理タスクは、コマンドラインツール`rug`またはグラフィカルなSoftware Updaterアプレットを使って開始されます。

9.1 コマンドラインからrugを使った更新

`rug`は`zmd`デーモンを使用し、与えられたコマンドに従って、ソフトウェアのインストール、更新、および削除を行います。ローカルファイルまたはサーバからソフトウェアをインストールできます。「サービス」と呼ばれる、リモートサーバを1つ以上使用することができます。サポートされたサービスはローカルファイル用の`mount`、サーバ用の`yum`またはZENworksです。

`rug`によりソフトウェアはチャンネル(カタログとも呼ばれる)という、同種のソフトウェアのグループにソートされます。たとえば、1つのカタログには更新サーバからのソフトウェアが含まれ、別のカタログには、サードパーティのソフトウェアベンタからのソフトウェアが含まれます。個別のカタログに加入することで、利用可能なパッケージの表示を管理し、希望しないソフトウェアがインストールされるのを防ぐことができます。操作は通常、加入したカタログに含まれるソフトウェアに対してのみ実行されます。

9.1.1 rugからの情報の取得

rugは、幅広い有益な情報を提供しています。zmdの状態の確認、登録されたサービスとカタログの参照、使用できるパッチについての情報の参照を行います。

zmdデーモンが一定期間使われなかった場合、スリープモードに切り替えることができます。zmdのステータスを確認し、デーモンを再びアクティブにするには、`rug ping`を使用します。このコマンドでzmdが起動し、ステータス情報がログに記録されます。

登録されたサービスを参照するには、`rug sl`を使用し、システムでサポートされているサービスを確認するには、`rug st`を使用します。

新しいパッチを確認するには、`rug pch`を使用します。パッチに関する情報を取得するには、`rug patch-info patch`と入力します。

9.1.2 rugサービスへの登録

デフォルトでは、新しくインストールされたシステムはさまざまなサービスに登録されます。新しいサービスを追加するには、`rug sa URI service_name`を実行します。ここで、`service_name`には、新しいサービスを識別するための、わかりやすく一意の文字列を指定してください。

注意: アップデートカタログのアクセス時のエラー

アップデートカタログにアクセスできない場合、登録の期限が切れている場合があります。通常、SUSE Linux Enterpriseには1年または3年の登録期間があり、この期間内にアップデートカタログにアクセスできます。このアクセスは登録期間が切れると拒否されます。

アップデートカタログへのアクセスが拒否される場合は、ノベルカスタマセンターにアクセスして登録を確認することを推奨する警告メッセージが表示されます。ノベルカスタマセンターには、<http://www.novell.com/center/>でアクセスできます。

9.1.3 rugを使ったソフトウェアのインストールと削除

登録したカタログからパッケージをインストールするには、`rug in package_name`を使用します。選択したカタログからのみインストールするには、`-c` カタログ名を使用します。パッケージに関する情報を表示するには、`rug if package_name`を使用します。

パッケージを削除するには、`rug rm package_name`を使用します。このパッケージに依存するパッケージがある場合は、その名前、バージョン、およびタイプが表示されます。確認して、パッケージを削除します。

9.1.4 rugユーザ管理

`rug`の主な利点の1つは、ユーザ管理です。通常、`root`のみ新規パッケージを更新したりインストールしたりできます。`rug`を使用して、システムを更新できる権利を他のユーザに割り当てたり、たとえば、ソフトウェアは更新だけ可能で削除はできないなど、権利を制限できます。付与できる権限は、次のとおりです。

インストール

ユーザは新規ソフトウェアをインストールできる。

ロック

ユーザはパッケージロックを設定できる。

削除

ユーザはソフトウェアを削除できる。

subscribe (登録)

ユーザはチャンネル加入を変更できる。

信頼済み

ユーザは信頼されているため、パッケージ署名がなくてもパッケージをインストールできる。

upgrade

ユーザはソフトウェアパッケージをアップデートできる。

表示

これにより、ユーザはどのソフトウェアがマシンにインストールされて使用可能なチャンネルであるかを確認できます。オプションはリモートユーザのみ対象としており、ローカルユーザは通常、インストール済みで使用可能なパッケージの表示が許可されています。

スーパーユーザ

ローカルで実行されなければならないユーザ管理と設定を除く、すべてのrugコマンドを許可します。

システムを更新するためのユーザパーミッションを付与するには、`rugua username upgrade`コマンドを使用します。`username`はユーザ名と置き換えてください。ユーザの権限を無効にするには、`rugudusername`コマンドを使用します。ユーザをそれぞれの権限をリストするには、`rug ul`を使用します。

ユーザの現在の権限を変更するには、`rugueusername`を使用し、`username`を該当するユーザ名と置き換えます。選択したユーザの権限のリストが取得されます。`edit`コマンドは対話型です。プラス(+)またはマイナス(-)を使用してユーザの権限を追加または削除し、**Enter**キーを押します。たとえば、ユーザにソフトウェアを削除する権限を付与するには、「`+remove`」と入力します。この権限を保存して終了するには、空のプロンプトで**Enter**キーを押します。

9.1.5 更新のスケジューリング

rugを使用することにより、スクリプトなどを使用して、システムを自動的にアップデートすることができます。最も単純な例は、完全な自動更新です。これを行うには、rootユーザで`rug up -y`を実行するcronジョブを設定します。`up -y`オプションは、ご使用のカタログから確認を求めることなくパッチのダウンロードおよびインストールを行います。

ただし、パッチを自動的にインストールしたくないが、後でパッチを取得してインストールするパッチを選択したいということがあります。パッチのダウンロードのみを行う場合、`rug up -dy` コマンドを使用します。`up -dy` オプションは、使用しているカタログから確認を求めることなくパッチをダウンロードし、それをrugキャッシュに保存します。rugキャッシュのデフォルトの場所は`/var/cache/zmd`です。

9.1.6 rugの設定

rugでは、初期設定のセットでセットアップをカスタマイズできます。一部の設定は、インストール時に設定されます。rug getコマンドを使用して、使用できる初期設定のリストを取得します。初期設定を編集するには、rug set *preference*と入力してください。たとえば、プロキシ経由でシステムをアップデートする必要がある場合に、設定内容を調整します。更新をダウンロードする前に、プロキシサーバにユーザ名とパスワードを送信します。そのように設定するには、次のコマンドを使用します。

```
rug set proxy-url url_path
rug set proxy-username name
rug set proxy-password password
```

*url_path*をプロキシサーバの名前と置き換えます。*name*をユーザ名に置き換えます。*password*をパスワードに置き換えます。

9.1.7 詳細情報

コマンドラインからの更新の詳細については、「rug --help」と入力するか、rug(1)のマニュアルページを参照してください。--helpオプションは、すべてのrugコマンドにおいても利用可能です。たとえば、rugupdateに関するヘルプを読みたい場合、「rug update --help」と入力します。

9.2 ZENツールを使ったパッケージの管理

ZENツールは、ZENworks Management Daemon (zmd)のグラフィカルなフロントエンドとしての役割を果たし、ソフトウェアのインストール/削除、セキュリティアップデートの適用、サービス/カタログの管理などの作業を簡単に行えます。

9.2.1 パーミッションの取得

Linuxシステムでパッケージを管理するには、root権限が必要です。ZENツールとrugには、ユーザがソフトウェアアップデートをインストールするための独自のユーザ管理システムが用意されています。ZENツールで特別な権限を必要とする操作を実行しようとする、最初はrootパスワードの入力が要求されます。パスワードが検証されたら、ユーザ管理システムにユーザのアカウントが、更新パーミッションで自動的に追加されます。これらの設定を確認、変更するには、ユーザ管理コマンドrugを使用します(9.1.4頁「rugユーザ管理」(226 ページ)を参照)。

9.2.2 ソフトウェアアップデートの取得とインストール

Software Updaterは、パネルの通知領域(GNOME)またはシステムトレイ(KDE)に、地球の形をしたアイコンとして表示されています。このアイコンは、ネットワークリンクや新規アップデートの状況に応じて、色や形状が変化します。Software Updaterは1日に1回、システムのアップデートがあるかどうかを自動的にチェックします(手動チェックを行う場合は、アイコンを右クリックして[更新]を選択します)。新しいアップデートがある場合は、パネルのSoftware Updaterアプレットが、地球の形から、オレンジの背景に感嘆符が付けられた形に変化します。

注意: アップデートカタログのアクセス時のエラー

アップデートカタログにアクセスできない場合、登録の期限が切れている場合があります。通常、SUSE Linux Enterpriseには1年または3年の登録期間があり、この期間内にアップデートカタログにアクセスできます。このアクセスは登録期間が切れると拒否されます。

アップデートカタログへのアクセスが拒否される場合は、ノベルカスタマセンターにアクセスして登録を確認することを推奨する警告メッセージが表示されます。ノベルカスタマセンターには、<http://www.novell.com/center/>でアクセスできます。

パネルアイコンを左クリックすると、アップデートウィンドウが表示されます。このウィンドウには、利用できるパッチと新規パッケージが表示されて

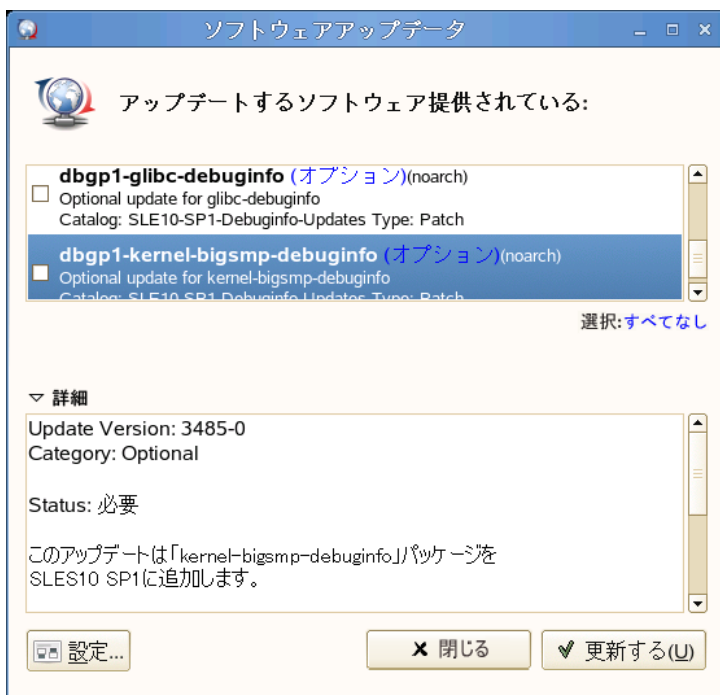
います。各項目には簡単な説明と、カテゴリアイコン(ある場合)が表示されます。セキュリティパッチには、黄色の盾の形をしたマークが付けられます。オプションのパッチには、明るい青色の円が付けられています。推奨するパッチには、何もマークが付けられていません。最初にセキュリティパッチが表示され、次に推奨するパッチ、オプションのパッチの順に表示されています。最後に、新しいバージョンのパッケージが表示されます。表示するパッケージを限定する場合は、`[すべて]`、`[パッケージ]`、および`[パッチ]`を使用します。

注意: パッケージとパッチ

Novellから公式にリリースされたアップデートは、`[パッチ]`として表示されます。他のソースからの新しいバージョンのパッケージは、`[パッケージ]`として表示されます。

特定の項目に関する詳細を表示するには、マウスで項目を選択してからリストウィンドウの下にある`[詳細]`リンクをクリックします。インストールする項目を選択するには、該当する項目のチェックボックスを選択します。すべてのパッチを洗濯、または選択解除する場合は、`[すべて]`および`[なし]`を使用します。`[更新]`を選択すると、選択したプログラムがインストールされます。

図 9.1 ソフトウェアアップデートの選択



9.2.3 ソフトウェアのインストール

ソフトウェアパッケージをインストールするには、メニューから [ソフトウェアのインストール] を選択するか、またはzen-installerを実行してください。インターフェースは、Software Updaterとほとんど同じです(9.2.2項「ソフトウェアアップデートの取得とインストール」(229ページ)を参照)。ただし、パッケージの検索やリストのフィルタリングに使用する検索パネルが異なっています。インストールするパッケージのチェックボックスを選択したら、[インストール] をクリックするとパッケージのインストールが開始されます。他のパッケージとの依存関係は、インストーラが自動的に解決します。

9.2.4 ソフトウェアの削除

ソフトウェアパッケージをアンインストールするには、メニューから **[ソフトウェアの削除]** を選択するか、または `zen-remover` を実行します。パッケージのリストに表示する項目を限定するには、**[製品]** (製品全体をアンインストール)、**[パターン]** (パターンの詳細は **パターンのインストールと削除項** (148 ページ) を参照)、**[パッケージ]**、**[パッチ]** リンクを使用します。リストから削除する項目のチェックボックスを選択し、**[削除]** を選択すると、パッケージのアンインストールが開始されます。選択されたパッケージに依存する他のパッケージがあった場合は、それらのパッケージも削除されます。この場合、それらのパッケージの削除を確認するメッセージが表示されます。このメッセージに対して **[キャンセル]** をクリックすると、どのパッケージもアンインストールされません。

9.2.5 Software Updaterの設定

ZENツールを設定するには、アプリケーションウィンドウから **[設定]** をクリックします。ウィンドウに **[サービス]**、**[カタログ]**、および **[設定]** の3種類のタブが表示されます。

サービスとカタログ

基本的にサービスは、ソフトウェアパッケージとその情報を提供するソースです。各サービスは、1つまたは複数のカタログを提供することができます。

[サービス] タブには、利用できるすべてのサービスと、そのタイプ、ステータス情報が表示されます(後の2つの情報が見えない場合は、ウィンドウサイズを調整してください)。サービスを追加、削除するには、**[サービスの削除]** または **[サービスの追加]** を使用します。次のサービスタイプを利用できます。

YUM

パッケージデータにRPM-MD形式を使用するHTTP、HTTPS、またはFTPサーバ。

ZYPP

ZYPPサービスは、YaSTで **[ソフトウェア] > [インストールソース]** の順に選択して追加された、YaSTインストールソースです。インストール

ソースを追加するには、**Software Updater**または**YaST**を使用します。最初にインストールしたソース(**DVD**または**CD-ROM**)が、事前設定されています。このソースを削除、または変更した場合は、それを他の有効なインストールソース(**ZYPP**サービス)と置換してください。そうしないと、新しいソフトウェアをインストールできません。

注意: 用語

YaSTインストールソース、**YaST**パッケージリポジトリ、および**ZYPP**サービスは、どれもソフトウェアをインストールできるソースのことを表しています。

マウント

[マウント] を使って、コンピュータにマウントされているディレクトリを組み込むことができます。この機能は、たとえば定期的に**Novell YUM**サーバのミラーリングを行い、その内容をローカルネットワークにエクスポートするようなネットワーク環境で役立ちます。ディレクトリを追加するには、[サービス**URI**] にディレクトリへのフルパスを指定してください。

NU

NUは、**Novell**アップデート(**Novell Update**)の省略形です。**Novell**は、**SUSE Linux Enterprise**のアップデートを、**NU**サービスとして提供しています。インストール時にアップデートの設定を行った場合、リストに公式の**Novell NU**サーバが表示されます。

インストール時にアップデート設定をスキップした場合は、コマンドラインから**suse_register**を実行するか、または**root**ユーザとして**YaST**から [ソフトウェア] > [製品登録] の順にクリックしてください。**Software Updater**に**Novell**アップデートサーバが追加されます。

RCEとZENworks

Opencarpet、**Red Carpet Enterprise**、または**ZENworks**サービスは、内部ネットワークでこれらのサービスが設定されている場合にのみ利用できます。たとえば、所属組織が単一のサーバからアップデートを配布するサードパーティ製のソフトウェアを利用している場合、これらのサービスは利用できません。

SUSE Linux Enterpriseをインストールすると、**ZYPP**サービスとしてのインストールソースと、**NU**サービスとしての**SUSE Linux Enterprise**アップデートサー

バ(製品登録時に追加)の、2種類のサービスが事前設定されています。通常は、これらの設定を変更する必要はありません。NUYUMサービスが表示されない場合は、rootシェルを開いてsuse_registerコマンドを実行してください。サービスは自動的に追加されます。

カタログ

サービスでは、異なる複数のソフトウェアのパッケージを提供したり、異なるバージョンのソフトウェアのパッケージ(RCEやZENworksサービスはそうしている)を提供することができます。これらは、カタログと呼ばれるカテゴリにより分類されています。カタログを登録または登録解除するには、該当するカタログのチェックボックスを選択、または選択解除します。

現時点では、SUSE Linuxサービス(YUMとZYPP)は、別のカタログは提供していません。各サービスには、1つしかカタログがありません。インストール時にsuse_registerを使ってSoftware Updaterを設定した場合は、YUMおよびZYPPカタログが自動的に登録されます。手動でサービスを追加した場合は、これらのカタログを登録する必要があります。

初期設定

[設定] タブで、起動時にSoftware Updaterを開始するかどうかを設定します。rootユーザは、Software Updater設定を変更することもできます。権限のないユーザは、設定を参照することしかできません。設定の詳細については、rugのマニュアルページを参照してください。

9.3 詳細情報

ZENworks Linux ManagementおよびZMDの詳細は、<http://www.novell.com/products/zenworks/linuxmanagement/index.html>を参照してください。

SUSE Linux Enterpriseのアップ デート

10

SUSE® Linux Enterpriseには、完全な再インストールを実行せずに既存のシステムを新しいバージョンに更新できるオプションがあります。新たにインストールする必要はありません。ホームディレクトリ、システム設定などの古いデータは、そのまま保持されます。製品のライフサイクル中は、サービスパックを適用してシステムのセキュリティを強化し、ソフトウェアの不具合を修正できます。CD/DVDドライブから、またはネットワーク上のインストールソースからインストールします。

10.1 SUSE Linux Enterpriseのアップ デート

たとえばSUSE Linux Enterprise 9からSUSE Linux Enterprise 10にアップデートする場合は、このセクションで概説するステップに従ってください。また、SUSE Linux Enterprise 10 SP1からSUSE Linux Enterprise 10 SP2にアップデートする場合もこのステップに従ってください。

ソフトウェアは、バージョンが上がるたびに「増加する」傾向があります。そのため、更新する前に、はじめにdfコマンドで、利用できるパーティションの容量を調べてください。ディスク容量が不足していると思われる場合は、システムの更新とパーティション設定を行う前に、データをバックアップしておきます。各パーティションに必要な容量を決定する一般的な規則はありません。必要な容量は、特定のパーティションプロファイルおよび選択したソフトウェアによって異なります。

10.1.1 準備作業

更新を開始する前に、データを確保するために、古い設定ファイルを別のメディア(テープデバイス、取り外し可能なハードディスク、**USBスティック**、または**ZIPドライブ**など)にコピーしておきます。主に、`/etc`の下に格納されているファイル、また、`/var`と`/opt`の下にあるディレクトリとファイルの一部に当てはまります。さらに、`/home` (HOMEディレクトリ)下のユーザデータをバックアップメディアに書き込むようにします。このデータは、`root`ユーザでバックアップします。`root`だけがすべてのローカルファイルを読み取るパーミッションを持っています。

更新を開始する前に、ルートパーティションの記録をとります。`df /`コマンドは、ルートパーティションのデバイス名リストを表示します。に示すように、書き留めておくルートパーティションは、`/dev/hda3`です(/としてマウントされています)。**例 10.1. 「df -hの出力例」** (236 ページ)

例 10.1 df-hの出力例

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/hda3	74G	22G	53G	29%	/
tmpfs	506M	0	506M	0%	/dev/shm
/dev/hda5	116G	5.8G	111G	5%	/home
/dev/hda1	44G	4G	40G	9%	/data

10.1.2 起こり得る問題

デフォルトのシステムを以前のバージョンからこのバージョンに更新する場合、**YaST**が必要な変更を分析し、それを実行します。カスタマイズに依存して、中には失敗する手順があったり、すべての更新手続きが失敗する可能性もありますので、その場合はバックアップデータをコピーして元に戻してください。システムの更新を開始する前に、次の点を確認してください。

`/etc`内の`passwd`と`group`の確認

システムを更新する前に、`/etc/passwd`と`/etc/group`に、構文エラーがまったく存在していないことを確認してください。この目的で、`root`になって検証ユーティリティ`pwck`と`grpck`を起動し、報告されたエラーを取り除きます。

PostgreSQL

PostgreSQL(postgres)を更新する前に、データベースをダンプします。詳細については、pg_dumpのマニュアルページを参照してください。この作業が必要になるのは、更新の前にPostgreSQLを実際に使用している場合だけです。

10.1.3 YaSTによる更新

に概要を示した準備手順を実行しましたから、ここでシステムを更新できるようになります。10.1.1項「準備作業」(236 ページ)

- 1 オプションで、インストールサーバを準備します。背景情報については、4.2.1項「YaSTを使ったインストールサーバのセットアップ」(63 ページ)を参照してください。
- 2 インストールの目的でシステムをブートします(3.3項「インストール時のシステム起動」(22 ページ)を参照)。YaSTで、言語を選択し [インストールモード] ダイアログ内で [更新] を選択します。[新規インストール] を選択しないようにします。
- 3 YaSTは、複数のルートパーティションが存在するかどうか判定します。1つだけであれば、次のステップに進みます。複数あれば、正しいパーティションを選択し、[次へ] で確認します(の例では、/dev/hda310.1.1項「準備作業」(236 ページ)が選択されています)。YaSTはそのパーティション上にある以前のfstabを読み込み、そこにリストされているファイルシステムを解析してマウントします。
- 4 [インストール設定] ダイアログで、必要に応じて設定を調整します。一般的には、デフォルト設定は変更なしで問題ありませんが、システムを拡張しようとする場合は、[ソフトウェア選択] サブメニューの中にあるパッケージを確認するか、追加の言語向けのサポートを追加します。
 - 4a すでにインストールされているソフトウェアのみを更新する場合 ([Only Update Installed Packages] (インストールされているパッケージのみを更新))、または選択内容に応じてシステムに新しいソフトウェアを追加する場合は、[Update Options] (更新オプション)をクリックします。推奨されている設定を使用することをお勧めします。この設定は、後でYaSTを使って調整することができます。

- 4b** 各種システムコンポーネントのバックアップを作成する([バックアップ])可能性もあります。バックアップを選択すると、更新処理を低速化します。このオプションは、最近バックアップを作成していない場合に使用します。

- 5** [了解] をクリックして、[アップデート開始] を確認してソフトウェアのインストールプロセスを開始します。

インストールが終了したらリリースノートを読み、[完了] をクリックしてコンピュータを再起動し、ログインします。

10.2 サービスパックのインストール

サービスパックを使用して、SUSE Linux Enterpriseのインストールを更新します。サービスパックは複数の方法で適用できます。サービスパックメディアを使用して新規のインストールを開始することも、既存のインストールを更新することもできます。システムの更新、および一元的なネットワークインストールソースのセットアップとして考えられるシナリオについて、本章で説明しています。

ティップ: インストールの変更

今後の変更については、サービスパックメディアのインストール手順をお読みください。

10.2.1 サービスパックメディア用にネットワークインストールソースをセットアップする

SUSE Linux Enterpriseを最初にインストールする場合と同様、物理メディアを使用して個別にクライアントをインストールするよりも、ネットワークに一元的インストールソースを配置してすべてのクライアントで利用できるようにする方がはるかに効率的です。

YaSTを使用してSUSE Linux Enterpriseにネットワークインストールソースを設定する

基本的に、[4.2項「インストールソースを保持するサーバのセットアップ」](#) (63 ページ)で説明されている手順に従います。SLE-10-SP-*x-arch*、SLES-10-SP-*x-arch*、またはSLED-10-SP-*x-arch*(*x*は、サービスパックの番号、*arch*はハードウェアアーキテクチャ名)という名前のインストールソースを追加し、NFS、HTTP、またはFTPを介して使用できるようにするだけです。

10.2.2 サービスパックのインストール

注意

既存のSUSE Linux Enterprise 10システムをSUSE Linux Enterprise 10 サービスパックに更新する場合は、[10.2.3項「サービスパックへの更新」](#) (242 ページ)を参照してください。

SUSE Linux Enterpriseサービスパックのインストール手順は、元のSUSE Linux Enterpriseメディアの手順とよく似ています。元のインストールと同じように、ローカルのCDまたはDVDドライブ、またはネットワーク上のインストールソースからインストールする方法を選択できます。

ローカルのCDまたはDVDドライブからインストールする

SUSE Linux Enterprise SPの新規インストールを開始する前に、すべてのサービスパック用インストールメディア(CDまたはDVD)が用意されていることをご確認ください。

手順 10.1 サービスパックメディアからブートする

- 1 1枚目のSUSE Linux Enterpriseサービスパックメディアメディア(CDまたはDVD 1)を挿入し、コンピュータをブートします。元のSUSE Linux Enterprise 10のインストール時と同様のブート画面が表示されます。
- 2 `[インストール]` を選択し、[第3章 YaSTによるインストール](#) (21 ページ)のYaSTインストールに関する説明に従って作業を続行してください。

ネットワークインストール

SUSE Linux Enterpriseサービスパックメディアのネットワークインストールを開始する前に、次の要件が満たされていることを確認します。

- ネットワークインストールソースが**10.2.1項「サービスパックメディア用にネットワークインストールソースをセットアップする」** (238 ページ)の記述どおりにセットアップされていること。
- インストールサーバと、ネームサービス、DHCP (オプション設定だが、PXEブートには必要)、およびOpenSLP (オプション)が含まれているターゲットコンピュータの両方でネットワーク接続が機能していること。
- このターゲットシステムをブートするSUSE Linux EnterpriseサービスパックCDかDVDの1枚目が用意されていること、またはPXEブートを実行するためのターゲットシステムがセットアップされていること(**4.3.5項「ターゲットシステムでPXEブートの準備をする」** (83 ページ)の説明を参照)。

ネットワークインストール—CDまたはDVDからのブート

ブートメディアとしてSP CDまたはDVDを使ってネットワークインストールを実行するには、次の手順に従います。

- 1 1枚目のSUSE Linux Enterpriseサービスパックメディア(CD 1またはDVD 1)を挿入し、コンピュータをブートします。元のSUSE Linux Enterprise 10のインストール時と同様のブート画面が表示されます。
- 2 `[インストール]` を選択してサービスパックカーネルをブートし、F3 キーを押してネットワークインストールソースの種類(FTP、HTTP、NFS またはSMB)を選択します。
- 3 適切なパス情報を入力するか、`[SLP]` をインストールソースとして選択します。
- 4 表示されるものから適切なインストールサーバを選択するか、**3.3.4項「SLPを使用しないネットワークソースからのインストール」** (24 ページ)に説明しているとおり、ブートオプションプロンプトを使用してインストールソースの種類とその実際の場所を指定します。YaSTが起動します。

第3章 *YaST*によるインストール(21 ページ)の説明に従って、インストールを完了します。

ネットワークインストール—PXEブート

ネットワークからSUSE Linux Enterpriseサービスパックのネットワークインストールを実行するには、次の手順に従います。

- 1 4.3.5項「ターゲットシステムでPXEブートの準備をする」(83 ページ)に従って、DHCPサーバのセットアップを調整してPXEブートに必要なアドレス情報を取得します。

- 2 PXEブートに必要なブートイメージが保管されるTFTPサーバをセットアップします。

このセットアップを実行するには、SUSE Linux EnterpriseサービスパックのCDまたはDVDの1枚目を使用するか、4.3.2項「TFTPサーバのセットアップ」(76 ページ)の手順に従います。

- 3 ターゲットコンピュータにPXEブートとWake-on-LANを準備します。
- 4 ターゲットシステムのブートを開始し、VNCを使用してこのコンピュータで実行中のインストールルーチンにリモートで接続します。詳細については、4.5.1項「VNCによるインストール」(91 ページ)を参照してください。
- 5 ライセンス契約に同意して、言語、デフォルトのデスクトップ、その他のインストール設定を選択します。
- 6 [インストールする] をクリックして、インストールを開始します。
- 7 通常のインストール操作を続行します (rootのパスワードの入力、ネットワーク設定の完了、インターネット接続のテスト、オンラインアップデートサービスの有効化、ユーザー認証方法の選択、およびユーザー名とパスワードの入力)。

SUSE Linux Enterpriseのインストール手順の詳細については、第3章 *YaST*によるインストール(21 ページ)を参照してください。

10.2.3 サービスパックへの更新

システムをサービスパック(SP)機能レベルでアップデートするには、2種類の推奨する方法があります。まず、SPメディアからブートする方法があります。もう1つは、YaSTオンラインアップデートまたはzen-updaterを実行して、*[Update to Service Pack X]* パッチを選択します。新機能レベルにアップデートすることにより、新しいドライバやソフトウェアの拡張機能などの、新たな機能を利用できるようになります。

警告: *[Update to Service Pack]* パックを見逃さないようにします。

[Update to Service Pack] パッチを選択しないと、システムは以前の機能レベルのままになり、バグフィックスおよびセキュリティアップデートを期間限定でしか受け取れません(SUSE Linux Enterprise 10 SP2では、この期間は6ヶ月間に延長されています)。このため、常にシステムの整合性を維持するため、できるだけ早期に新しい機能レベルに切り替えることを推奨します。

その他のアップデート方法は、パッチCD(8.3.7項「**パッチCDを使用した更新**」(160 ページ)を参照)を使用するか、またはローカルにインストールしたSMTシステムを使用して、rugコマンドを手動で実行することです。

注意

s390システムで、パッチCDによるアップデートオプションが可能になりました。

SPメディアからのブートによるアップデート

SPメディアからブートして、YaSTのインストールモードで、*[更新]* を選択します。詳細な情報とアップデート手順については、10.1.3項「**YaSTによる更新**」(237 ページ)を参照してください。

YaSTオンラインアップデートの開始

YaSTオンラインアップデートを開始してSP機能レベルでのアップデートを行う前に、次の前提条件を満たしていることを確認してください。

- アップデート作業中は、ノベルカスタマセンターにアクセスする必要があります。そのため、システムは常時オンラインでなければなりません。
- セットアップ時にサードパーティ製のソフトウェアやアドオンソフトウェアもインストールする場合は、別のコンピュータでこの手順を試して、アップデートにより依存関係がおかしくならないことを確認してください。
- すべてのプロセスが正常に完了することを確認してください。そうしないと、システムに不整合が発生してしまいます。

あらかじめサービスパック1が完全にインストールされている場合は、サービスパック2のみにアップデートできます。そうでない場合は、**SUSE Linux Enterprise GAからSP1およびSP2項(248 ページ)**の説明のとおりにもずサービスパック1にアップデートします。

図 10.1 サービスパック1パッケージ管理のアップデート

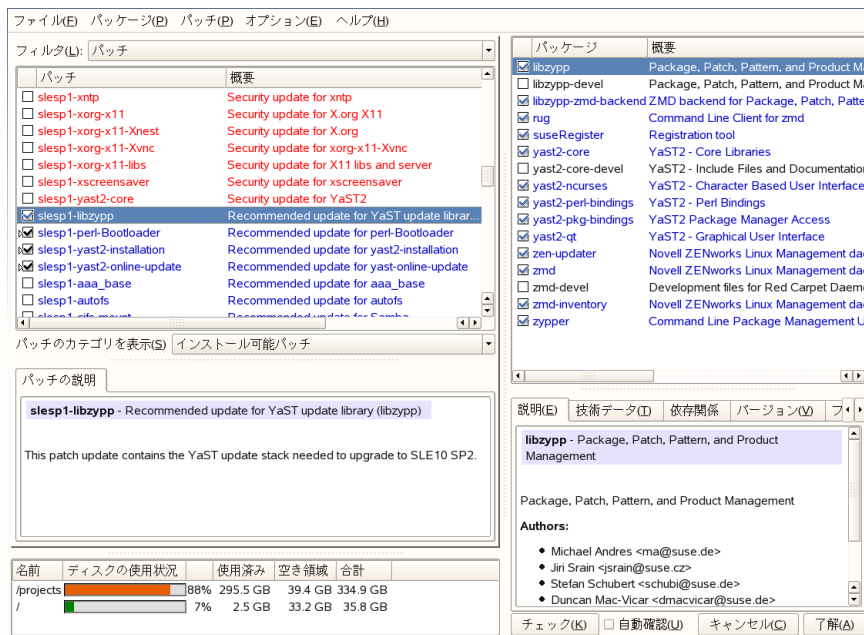
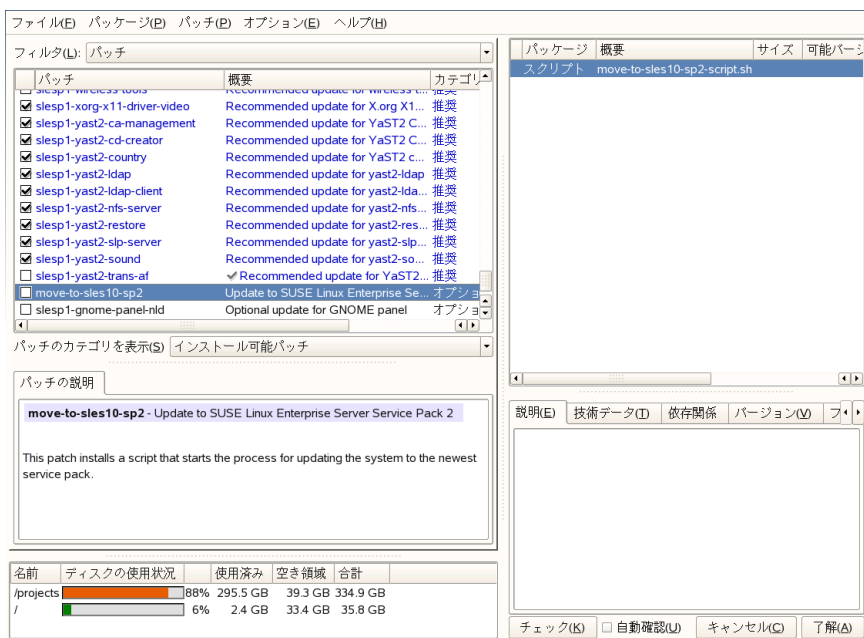


図 10.2 サービスパック2へのアップデート



注意

YaSTオンラインアップデートを使用したアップデート移行中に、ZMDスタックはアップデートされ、ZMDデーモンも再起動されます。このため、rug、zen-updater、zen-installerおよびzen-removerなどのその他のソフトウェア管理ツールを使用しないことを推奨します。移行中は、zen-updaterを終了しておくことを推奨します。

- 稼働中のSUSE Linux Enterpriseシステムで、[コンピュータ] > [YaST] > [ソフトウェア] > [オンラインアップデート] の順にクリックします。

rootとしてログインしない場合、プロンプトが表示されたら、rootパスワードを入力します。

- [オンラインアップデート] ダイアログが表示されます。いくつかのパッチがあらかじめ選択されています。パッチリストを下にスクロールして、パッケージ管理に関連したパッチとSUSE Linux Enterprise 10 SP2

メンテナンススタックアップデート(slesplu-libzypp)が実際に選択済みであることを確認します。 [了解] をクリックして、選択したアップデートを適用します。

- 3 [パッチのダウンロードとインストール] ダイアログで、進行状況のログを追跡します。 [全体の進行状況] が [100%] になったら、 [閉じる] をクリックします。 [オンラインアップデート] が自動的に再起動されます。
- 4 再起動したら、 [了解] をクリックして、新しいカーネルですべての使用できるアップデートを適用します。 インストールされたら、システムを再起動する必要があります。

- 5 再起動したオンラインアップデートで、パッチリストを下にスクロールし、 **図 10.2. 「サービスパック2へのアップデート」** (244 ページ)に示すように、 [Update to Service Pack 2] (move-to-sles10-sp2)を選択します。 ポップアップウィンドウで、サービスパックのアップデート作業を開始することを確認したら、 [了解] をクリックします。

move-to-sles10-sp2パッチはオプションとしてマークされています。 これを選択しないと、システムはSP1機能レベルのままになり、バグフィックスとセキュリティアップデートを期間限定でしか受け取れません(SP2を入手してから6ヶ月間)。

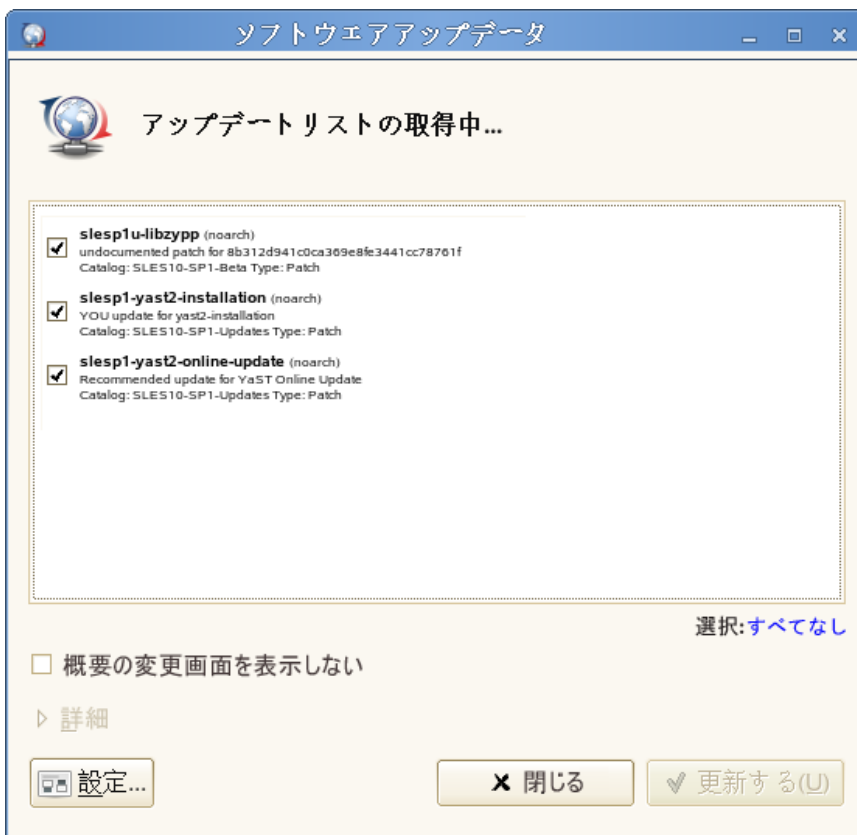
- 6 [Patch Download and Installation] ダイアログには、移行パッチインストールの進捗状況ログが表示されます。 [Total Progress] が [100%] になったら、 [完了] をクリックします。
- 7 YaSTオンラインアップデートを再度起動します。 product-sles10-sp2 と slesp2o-sp2_onlineパッチを適用して、システムをSP2レベルにします。 これらのパッチは両方ともあらかじめ選択されています。 以前のステップでmove-to-sles10-sp2をインストールした場合、これは必須だからです。
- 8 [閉じる] をクリックして、SUSE Linux Enterprise 10 SP2へのアップデートを完了し、再起動します。

zen-updaterで開始する

ZENworksの背景情報については、[第9章 ZENworksを使ったソフトウェアの管理](#) (223 ページ)を参照してください。

zen-updaterを使用してオンラインアップデートを開始してSP機能レベルに進む前に、[YaSTオンラインアップデートの開始項](#) (242 ページ)に挙げる要件を満たしていることを確認します。

図 10.3 SLE10 SP2メンテナンススタックアップデートの適用



- 1 実行しているSUSE Linux Enterpriseシステムで、下部のupdaterアイコンをクリックしてzen-updaterを起動します。

ティップ: ZMDの有効化

「ZMDが実行していません」というメッセージが表示される場合、rootとしてrczmd statusを使用して端末を確認し、ZMDが実行されているかどうか確認します。問題がある場合は、rug restart --cleanと入力して強制的に再起動し、ZMDとそのデータベースをクリーンアップします。

rootとしてログインしない場合、プロンプトが表示されたら、rootパスワードを入力します。

- 2 システムに利用できるすべてのメンテナンスアップデートを適用します。
- 3 SLE10 SP2メンテナンススタックアップデートを適用します (slesplu-libzypp)。アイテムが選択済みで、[アップデート] をクリックするとこのステップが開始されます。すべての依存関係を解決したら、[適用] をクリックします。完了したら [閉じる] をクリックして、ポップアップメッセージを確認します。
- 4 再起動したソフトウェアアップデートで、ページの下に進んでオプションのmove-to-sles10-sp2パッチを選択して適用します。これを選択しないと、システムはSP1機能レベルのままになり、バグフィックスとセキュリティアップデートを期間限定でしか受け取れません(SP2を入手してから6ヶ月間)。
- 5 ソフトウェアアップデートで、product-sles10-sp2とslesp2o-sp2_onlineパッチを適用して、システムをSP2レベルにします。以前のステップでmove-to-sles10-sp2をインストールした場合はこの両方のパッチは必須であるため、事前に選択されています。
- 6 [閉じる] をクリックして、SUSE Linux Enterprise 10 SP2へのアップデートを完了し、再起動します。

rugの使用

rugコマンドラインツールの背景情報については、[9.1項「コマンドラインからrugを使った更新」](#) (224 ページ)を参照してください。アップデートにスクリプトによるソリューションが必要な場合は、rugを使用します。

rugを使用したオンラインアップデートを開始してSP機能レベルに進む前に、**YaSTオンラインアップデートの開始項**(242 ページ)に挙げる要件を満たしていることを確認します。

これはシステムをSP2パッチレベルに移行するために必要な最小のコマンドシーケンスです。

```
rug in -t patch slesplu-libzypp && rug ping -a
rug in -t patch move-to-sles10-sp2 && rug ping -a
rug refresh && rug ping -a
rug up -t patch -g recommended && rug ping -a
reboot
```

注意

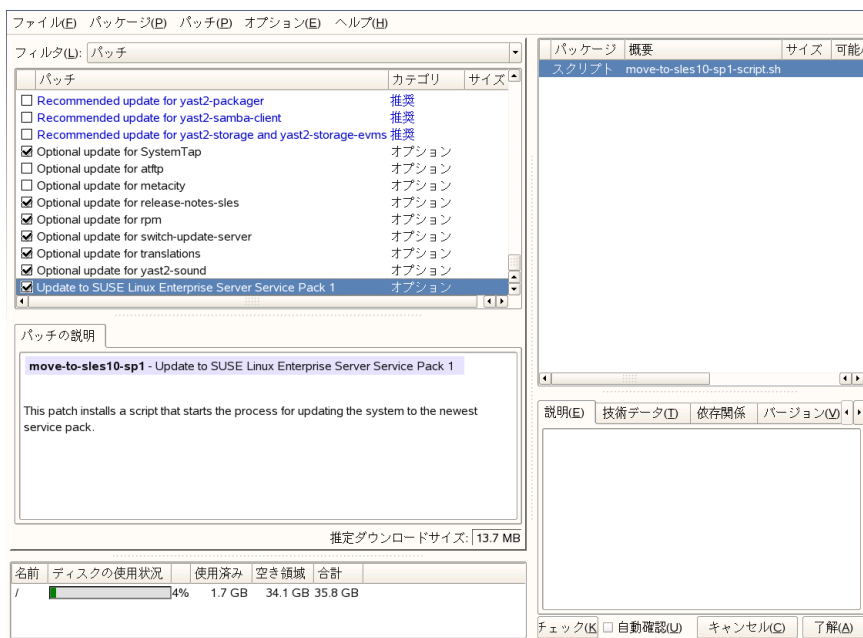
rug ping -aは、以前のrugコマンドの後にZMD初期化が完了させます。

SUSE Linux Enterprise GAからSP1およびSP2

注意

次のステップは、GAパッチレベルでシステムを実行している場合にのみ関連します。

図 10.4 サービスパック1へのアップデート



- 稼働中のSUSE Linux Enterpriseシステム(GA)で、`[コンピュータ] > [YaST] > [ソフトウェア] > [オンラインアップデート]` の順にクリックします。

rootとしてログインしない場合、プロンプトが表示されたら、rootパスワードを入力します。

- `[オンラインアップデート]` ダイアログが表示されます。パッチリストをスクロールして、のように `[Update to Service Pack 1]` 図 10.4. 「サービスパック1へのアップデート」 (249 ページ) を選択します。ポップアップウィンドウで、サービスパックのアップデート作業を開始することを確認したら、`[了解]` をクリックします。
- `[Patch Download and Installation]` ダイアログには、移行パッチインストールの進捗状況ログが表示されます。`[Total Progress]` が `[100%]` になったら、`[完了]` をクリックします。

- 4 もう一度オンラインアップデートを実行します。作業が完了したら、*[Patch Download and Installation]* で *[閉じる]* をクリックします。YaSTの2回目の実行時には、カーネルと他のすべてのソフトウェアがインストールされます。
- 5 処理ログが終わりに近づき、*[インストール完了]* のメッセージが表示されたら、*[完了]* をクリックします。
- 6 アップデートを完了するには、システムを手動で再起動して、新しいカーネルを有効にしてください。

これでSUSE Linux EnterpriseがSP1パッチレベルで実行されます。**YaSTオンラインアップデートの開始項** (242 ページ)を続行し、システムをSP2パッチレベルに進めます。

10.3 バージョン9からバージョン10へのソフトウェアの変更点

バージョン9から10への個別の変更は、以降で要約されています。この要約には、基本設定が完全に変更されているかどうか、設定ファイルが他の場所に移されているかどうか、共通アプリケーションが大幅に変更されているかどうかなどの情報が示されています。ユーザレベルまたは管理者レベルで日々のシステムの使用に影響を与える重要な変更が、ここに記載されています。

注意: SLES 10からSLES 10 SP 1でのソフトウェアの変更

SUSE Linux Enterprise Server 10からSUSE Linux Enterprise Server 10 SP1になって変更されたソフトウェアや環境設定情報の詳細は、サービスパックのリリースノートを参照してください。リリースノートは、インストール済みシステムでYaSTのリリースノートモジュールを使って参照できます。

10.3.1 複数カーネル

複数のカーネルを並べてインストールできます。この機能の目的は、管理者が新規カーネルをインストールし、新規カーネルが期待通りに機能することを確認したのち、古いカーネルをアンインストールすることによって、カー

ネルをアップグレードできるようにすることです。YaSTはまだこの機能をサポートしていませんが、`rpm -i package.rpm`を使用すれば、カーネルのインストールとアンインストールはシェルを使用して簡単に行うことができます。

デフォルトのブートローダメニューには、1つのカーネルエントリがあります。複数のカーネルをインストールする場合、追加するカーネルごとに1つのエントリを追加し、それらを簡単に選択できるようにしておくと便利です。新規カーネルのインストール前にアクティブであったカーネルは、`vmlinux.previous`および`initrd.previous`としてアクセスできます。デフォルトエントリに似たブートローダエントリを作成し、このエントリが`vmlinux`および`initrd`ではなく、`vmlinux.previous`および`initrd.previous`を参照するようにすると、前にアクティブであったカーネルにアクセスできます。またGRUBおよびLILOも、ワイルドカードのブートローダエントリをサポートします。詳細については、GRUBのinfoページ(`info grub`)および`lilo.conf` (5)のマニュアルページを参照してください。

10.3.2 カーネルモジュールに関する変更

以下のカーネルモジュールは、利用できなくなりました。

- `km_fcdsl`—AVM Fritz!Card DSL
- `km_fritzcapi`—AVM FRITZ! ISDN Adapters

以下のカーネルモジュールパッケージは、内部に変更が加えられました。

- `km_wlan`—さまざまな無線LANカード用のドライバが追加されました。
`km_wlan`から、Atheros WLANカード用の`madwifi`ドライバが削除されました。

技術上の理由から、Ralink WLANカードのサポートが中止されました。今回の配布には、以下のモジュールは含まれていません。また、今後追加される予定也没有ありません。

- `ati-fglrx`—ATI FireGLグラフィックカード
- `nvidia-gfx`—NVIDIA gfxドライバ

- `km_smartlink-softmodem`—Smart Link Softモデム

10.3.3 コンソール番号の変更とシリアルデバイス

2.6.10では、ia64のシリアルデバイスは、ACPIおよびPCIリストの順番に名前が付けられます。たとえば、ACPIネームスペースの最初のデバイスは`/dev/ttyS0`、次のデバイスは`/dev/ttyS1`のようになります。また、PCIデバイスはACPIデバイスの後に、順番に名前が付けられていきます。

HPシステムの場合は、EFIコンソールを再設定しないと、カーネルブートコマンドからコンソールパラメータを破棄できません。対処方法としては、`console=ttyS0...`の代わりに`console=ttyS1...`をブートパラメータとして試してください。

詳細は、`kernel-source`ソフトウェアパッケージの`/usr/src/linux/Documentation/ia64/serial.txt`を参照してください。

10.3.4 LD_ASSUME_KERNEL環境変数

`LD_ASSUME_KERNEL`環境変数は設定しないでください。従来は、この環境変数を使ってLinuxThreadsサポートを利用することができましたが、この機能はなくなりました。SUSE Linux Enterprise 10で`LD_ASSUME_KERNEL=2.4.x`を設定すると、`ld.so`は存在しないパスを使ってglibcと関連ツールを探そうとするため、正常に動作しません。

10.3.5 より厳密になったtar構文

`tar`の使用構文がさらに厳密になりました。`tar`のオプションは、ファイルまたはディレクトリの前に指定する必要があります。ファイルまたはディレクトリの後に`--atime-preserve`、`--numeric-owner`などのオプションを指定すると、`tar`は失敗します。バックアップスクリプトを確認してください。次のようなコマンドは動作しません。

```
tar czf etc.tar.gz /etc --atime-preserve
```

詳細については、tarの情報ページを参照してください。

10.3.6 Apache 2からApache 2.2への置き換え

Apache Webサーバ (バージョン2)のバージョンが、2.2になりました。Apache バージョン2.2では、**第40章 Apache HTTPサーバ**(807 ページ)が完全に作り直されました。一般的なアップグレード情報については、<http://httpd.apache.org/docs/2.2/upgrading.html>、新機能については、http://httpd.apache.org/docs/2.2/new_features_2_2.htmlを参照してください。

10.3.7 ネットワーク認証用Kerberos

Kerberosがネットワーク認証のデフォルトです。heimdalではありません。既存のheimdal設定の自動変換は行えません。システム更新の間に、設定ファイルのバックアップコピーが**表 10.1. 「バックアップファイル」** (253 ページ)に示すように作成されます。

表 10.1 バックアップファイル

古いファイル	バックアップファイル
/etc/krb5.conf	/etc/krb5.conf.heimdal
/etc/krb5.keytab	/etc/krb5.keytab.heimdal

クライアント設定(/etc/krb5.conf)は、heimdaの1つによく似ています。特に何も設定することがなかった場合は、パラメータkpasswd_serverをadmin_serverへ置き換えることで十分です。

サーバ(kdc/kadmind)関連データをコピーすることはできません。システムのアップデート後、古いheimdalデータベースは、/var/heimdalでまだ使用できます。MIT kerberosは、/var/lib/kerberos/krb5kdc内のデータベースを管理します。詳細については、**第45章 ネットワーク認証—Kerberos**(913 ページ)および**第46章 Kerberosのインストールと管理**(921 ページ)を参照してください。

10.3.8 udevデーモンによって処理される Hotplugイベント

Hotplugイベントは、完全にudevデーモン(udev)によって処理されるようになりました。/etc/hotplug.dおよび/etc/dev.d中のイベントマルチプレクサシステムは、すでに使われていません。かわりに、udevが、規則に応じてすべてのhotplugヘルパーツールを直接呼び出します。udevルールとヘルパーツールは、udevおよび他の各種パッケージによって提供されます。

10.3.9 インストール時のファイアウォールの有効化

セキュリティレベルを上げるために、提案ダイアログでインストールを終了すると、同梱のファイアウォールソリューションSuSEFirewall2が有効になります。これは、最初はすべてのポートがクローズされており、必要に応じて提案ダイアログでオープンできることを意味します。デフォルトでは、リモートシステムからログインできません。SLP、Samba(「ネットワークコンピュータ」)、ある種のゲームなど、ネットワーク参照アプリケーションおよびマルチキャストアプリケーションとのインタフェースにもなります。YaSTを使用してファイアウォールを微調整できます。

サービスのインストールまたは設定中にネットワークへのアクセスを必要とする場合は、関連YaSTモジュールにより、すべての内部インタフェースと外部インタフェースの必須TCPポートおよびUDPポートがオープンされます。これが不要な場合は、YaSTモジュールでポートを閉じるか、他の詳しいファイアウォール設定を指定できます。

10.3.10 KDEとGNOMEのサポート

デフォルトでは、KDEにはIPv6サポートは有効ではありません。YaSTの/etc/sysconfigエディタを使用して有効にすることができます。この機能を無効にする理由は、一部のインターネットサービスプロバイダではIPv6アドレスが正しくサポートされないからです。結果として、Webの検索中にエラーメッセージが表示され、Webページの表示で遅れが生じます。

10.3.11 オンラインアップデートとデルタパッケージ

オンラインアップデートは、基本パッケージからの差分のみを格納する特殊なRPMパッケージをサポートするようになっています。この方法の場合、最終的なパッケージの再構成のためCPUの負荷が高くなるという欠点がありますが、パッケージのサイズとダウンロード時間の面では大幅な削減が見られます。技術的な詳細については、`/usr/share/doc/packages/deltarpm/README`を参照してください。

10.3.12 印刷システムの設定

インストールの終了時に(提案ダイアログ)、印刷システムに必要なポートをファイアウォール設定でオープンする必要があります。ポート631/TCPとポート631/UDPはCUPSに必須であり、通常の動作ではクローズしないでください。LPDまたはSMBを介して印刷を行うには、ポート515/TCP (古いLPDプロトコル用)とSambaで使用されるポートもオープンする必要があります。

10.3.13 X.Orgへの移行

互換リンクを使用すると、XFree86からX.Orgに容易に移行できます。このリンクにより、重要なファイルとコマンドに古い名前でアクセスできます。

表 10.2 [コ\83\7dンド]

XFree86	X.Org
XFree86	Xorg
xf86config	xorgconfig
xf86cfg	xorgcfg

表 10.3 /var/log内のログファイル

XFree86	X.Org
XFree86.0.log	Xorg.0.log
XFree86.0.log.old	Xorg.0.log.old

X.Orgに移行する過程で、パッケージ名がXFree86*からxorg-x11*に変更されました。

10.3.14 X.Org設定ファイル

設定ツールSaX2は、X.Org設定を/etc/X11/xorg.confに書き込みます。最初からのインストール時には、XF86Configからxorg.confへの互換性のないリンクが作成されます。

10.3.15 XViewとOpenLookのサポートを中止

パッケージxview、xview-devel、xview-devel-examples、olvwm、およびxtoolplは削除されました。これまでのリリースでは、XView(OpenLook)のベースシステムだけが提供されていました。システムのアップデート後は、XViewライブラリは提供されなくなります。それよりも大きな変更は、OLVWM(OpenLook Virtual Window Manager)が使用できなくなったことです。

10.3.16 X11用のターミナルエミュレータ

多くのターミナルエミュレータが削除されました。それらのターミナルエミュレータはデフォルト環境ではメンテナンスされず、また機能しません。特にUTF-8をサポートしていません。SUSE Linux Enterprise Serverは、xterm、KDE、GNOMEといった端末やmlterm(Multilingual Terminal Emulator for X)などの標準端末を提供しています。これらは、atermおよびetermに置き換わるものです。

10.3.17 OpenOffice.org (OOo)

ディレクトリ

OOoは、`/opt/OpenOffice.org`の代わりに `/usr/lib/ooo-2.0`にインストールされます。ユーザ設定用のデフォルトディレクトリは、`~/OpenOffice.org2.0`ではなく `~/.ooo-1.1`です。

Wrapper

OOoコンポーネントの起動用に、いくつか新規ラッパーが用意されています。新しい名前については、表 10.4. 「Wrapper」 (257 ページ)を参照してください。

表 10.4 *Wrapper*

旧	新規
<code>/usr/X11R6/bin/OOo-calc</code>	<code>/usr/bin/oocalc</code>
<code>/usr/X11R6/bin/OOo-draw</code>	<code>/usr/bin/oodraw</code>
<code>/usr/X11R6/bin/OOo-impress</code>	<code>/usr/bin/ooimpress</code>
<code>/usr/X11R6/bin/OOo-math</code>	<code>/usr/bin/oomath</code>
<code>/usr/X11R6/bin/OOo-padmin</code>	<code>/usr/sbin/oopadmin</code>
<code>/usr/X11R6/bin/OOo-setup</code>	—
<code>/usr/X11R6/bin/OOo-template</code>	<code>/usr/bin/oofromtemplate</code>
<code>/usr/X11R6/bin/OOo-web</code>	<code>/usr/bin/ooweb</code>
<code>/usr/X11R6/bin/OOo-writer</code>	<code>/usr/bin/oowriter</code>
<code>/usr/X11R6/bin/OOo</code>	<code>/usr/bin/ooffice</code>
<code>/usr/X11R6/bin/OOo-wrapper</code>	<code>/usr/bin/ooo-wrapper</code>

ラッパーは、KDEアイコンとGNOMEアイコンの間で切り替えるためのオプション`--icons-set`をサポートするようになりました。オプション、`--default-configuration`、`--gui`、`--java-path`、`--skip-check`、`--lang`(言語はロケール(locale)で指定)、`--messages-in-window`、および`--quiet`のサポートが中止され、サポートされなくなりました。

KDEとGNOMEのサポート

`OpenOffice_org-kde`および`OpenOffice_org-gnome`パッケージ内でKDEおよびGNOME拡張を使用できます。

10.3.18 サウンドミキサー**kmix**

サウンドミキサー**kmix**がデフォルトとして事前設定されています。ハイエンドのハードウェア向けには、**QAMix**、**KAMix**、**envy24control**(ICE1712専用)、または**hdspmixer**(RME Hammerfall専用)などの、他のミキサーも用意されています。

10.3.19 DVD作成

従来、DVD作成をサポートするために、パッチを**cdrecord**パッケージから**cdrecord**バイナリに適用しました。現在、このパッチ付きの新規バイナリ**cdrecord-dvd**がインストールされています。

dvd+rw-toolsパッケージの**growisofs**プログラムは、現在ではすべてのDVDメディア(DVD+R、DVD-R、DVD+RW、DVD-RW、DVD+RL)を作成できるようになりました。パッチされた**cdrecord-dvd**の代わりに、これを使用するようにお勧めします。

10.3.20 カーネルプロンプトでの手動インストールの開始

[手動インストール] モードは、ブートローダの画面からなくなっています。それでも、ブートプロンプトで`manual=1`を使用すれば、**inuxrc**を手動モードにすることはできます。通常ではこれは必要ありません。`textmode=1`のよ

うに インストールオプションをカーネルプロンプトで直接設定するか、インストールソースとしてURLを設定できるからです。

10.3.21 JFS:以降サポートされません

JFSは、技術的な問題があるため、サポートされなくなりました。カーネルのファイルシステムドライバはまだ存在しますが、YaSTではJFSのパーティションを作成できません。

10.3.22 Tripwireの代替としてのAIDE

侵入検出システムとして、AIDE(パッケージ名はaide)を使用します。これはGPLに基づいて提供されます。SUSE Linuxでは、以降Tripwireは利用できません。

10.3.23 PAM設定

新規設定ファイル(詳細に関するコメントを含む)

`common-auth`

認証セッション用のデフォルトPAM設定

`common-account`

アカウントセッション用のデフォルトPAM設定

`common-password`

パスワード変更用デフォルトPAM設定

`common-session`

セッション管理用デフォルトPAM設定

アプリケーション固有設定ファイル内から、これらのデフォルト設定ファイルを含める必要があります。システム上に存在する、およそ40ファイルの代わりに、1つの設定ファイルを変更して維持するほうが簡単だからです。後でアプリケーションをインストールすると、そのアプリケーションはすでに適用済みの変更を継承するので、管理者は、設定を調整するために覚えておく必要がありません。

変更は次のように簡単です。次の設定ファイルがあるとします(このファイルは、ほとんどのアプリケーションのデフォルトです)。

```
#%PAM-1.0
auth      required      pam_unix2.so
account   required      pam_unix2.so
password  required      pam_pwcheck.so
password  required      pam_unix2.so      use_first_pass use_authtok
#password required      pam_make.so      /var/yp
session   required      pam_unix2.so
```

次のものに変更できます。

```
#%PAM-1.0
auth      include      common-auth
account   include      common-account
password  include      common-password
session   include      common-session
```

10.3.24 suしてスーパーユーザになる方法

デフォルトでは、suを実行してrootになると、PATHがroot用のものに設定されません。su -を使用して、root用の完全な環境を備えたログインシェルを開始するか、デフォルトのsuコマンドの動きを変更したい場合は、/etc/default/su内のALWAYS_SET_PATHにyesを設定します。

10.3.25 powersaveパッケージの変更

/etc/sysconfig/powersave内の設定ファイルが変更されています。

表 10.5 /etc/sysconfig/powersave内の設定ファイルの分割

旧	分割後
/etc/sysconfig/powersave/ common	common
	cpufreq
	イベント

旧	分割後
	battery
	sleep
	thermal

/etc/powersave.confは、廃止されました。既存の変数は表 10.5. 「[/etc/sysconfig/powersave内の設定ファイルの分割](#)」 (260 ページ)に示すファイルに移動されています。/etc/powersave.conf内で「event」の変数を変更している場合は、これらの変数を/etc/sysconfig/powersave/events内で調整する必要があります。

スリープ状態の名前が次のように変更されました。変更前の名前は次のとおりです。

- suspend (ACPI S4、APMサスペンド)
- standby (ACPI S3、APMスタンバイ)

宛先:

- suspend to disk (ACPI S4、APMサスペンド)
- suspend to ram (ACPI S3、APM サスペンド)
- standby (ACPI S1、APMスタンバイ)

10.3.26 Powersave設定変数

powersave設定変数の名前は、一貫性を保つために変更されますが、sysconfig ファイルは同じままです。詳細情報については、[28.5.1項「powersaveパッケージの設定」](#) (569 ページ)を参照してください。

10.3.27 PCMCIA

cardmgrは、PCカードを管理しなくなりました。代わりに、カーネルモジュールが、Cardbusカードおよび他のサブシステムと同様にPCカードを管理します。すべての必要な操作は、hotplugによって実行されます。pcmcia起動スクリプトは削除され、cardctlはpccardctlによって置き換えられました。詳細については、『/usr/share/doc/packages/pcmciautils/README.SUSE』を参照してください。

10.3.28 .xinitrcでのプロセス間通信のためのD-BUSのセットアップ

現在、多くのアプリケーションで、IPC(プロセス間通信)にD-BUSが使用されています。dbus-launchを呼び出すと、dbus-daemonが起動します。システム全体の/etc/X11/xinit/xinitrcは、dbus-launchを使用してウィンドウマネージャを起動します。

ローカルの~/.xinitrcファイルがある場合は、それを変更する必要があります。変更しない場合、f-spot、banshee、tomboyまたはNetwork Manager bansheeが失敗する可能性があります。以前の~/.xinitrcを保存します。次のコマンドを使用して、新規テンプレートファイルをホームディレクトリにコピーします。

```
cp /etc/skel/.xinitrc.template ~/.xinitrc
```

最後に、保存された.xinitrcからのカスタマイズを追加します。

10.3.29 NTP関連ファイルの名前変更

LSB (Linux Standard Base)との互換性の理由から、多くの設定ファイルとinitスクリプトはxntpからntpに名前が変更されました。新規のファイル名は次のとおりです。

- /etc/slp.reg.d/ntp.reg
- /etc/init.d/ntp

- /etc/logrotate.d/ntp
- /usr/sbin/rcntp
- /etc/sysconfig/ntp

10.3.30 GNOMEアプリケーション用ファイルシステム変更通知

適切に機能するため、GNOMEアプリケーションは、ファイルシステム変更通知サポートに依存しています。ローカルのためのファイルシステムでは、**gamin** パッケージをインストールするか(優先)、または**FAM**デーモンを実行します。リモートのファイルシステムでは、**FAM**をサーバとクライアントの両方で実行し、**FAM**によって**RPC**コール用のファイアウォールを開きます。

GNOME (**gnome-vfs2**および**libgda**)には、ファイルシステム変更通知を提供するための**gamin**または**fam**を取得するラッパーが含まれています。

- **FAM**デーモンが動作していない場合、**gamin**が優先されます(理由:**Inotify**は**gamin**だけがサポートしており、この方がローカルファイルシステムにとって効率的だから)。
- **FAM**デーモンが動作している場合は、**FAM**が優先されます(理由:**FAM**が動作している場合、ユーザによるリモート通知の利用が予想され、この機能は**FAM**だけがサポートしているから)。

10.3.31 FTPサーバ(vsftpd)の起動

デフォルトで、**xinetd**は**vsftpd** FTPサーバを起動しなくなりました。これは、スタンドアロンのデーモンになり、**YaST**ランタイムエディタを使用して設定する必要があります。

10.3.32 Firefox 1.5:URL openコマンド

Firefox 1.5では、**Firefox**インスタンスまたはウィンドウを開くためのアプリケーション用メソッドは変更されました。この新規メソッドは、一部、以前

のバージョンに含まれており、その動作はラッパースクリプトに実装されています。

アプリケーションでmozilla-xremote-clientまたはfirefox -remoteを使用していない場合、変更の必要はありません。使用している場合は、URLを開くために使用する新規コマンドは、`firefox url`で、Firefoxがすでに動作しているかどうかによります。すでに実行している場合は、*[Open links from other applications in]* で設定されている環境設定に従います。

コマンドラインで、`firefox -new-window url` または `firefox -new-tab url` を使用して、その動作に影響を与えることができます。

パートⅡ. 管理

OpenWBEM

Novell®は、DMTF (Distributed Management Task Force) [<http://www.dmtf.org/home>]により提案されたオープンスタンダード規格である、WBEM (Web-Based Enterprise Management)に賛同しています。これらの規格を実装することにより、ネットワーク上の多様なシステムを管理する手間を大幅に削減することができます。

ここでは、DMTFによって提案されたコンポーネントについて説明します。これらの情報および情報間の関連性を理解することにより、ネットワークでのOpenWBEMおよびOpenWBEM活用方法を理解できます。

- **Web-Based Enterprise Management (WBEM)**とは、企業のコンピューティング環境の一元管理のために開発された、一連の管理およびインターネット標準テクノロジーです。WBEMは、新しいWebテクノロジーを活用した標準ベースの統一管理ツールを作成する機能を業界に提供するものです。DMTFでは、次に挙げるようなWBEMを構成する標準の中で中心的なものを開発しました。
- データモデル:CIM(Common Information Model)標準
- 符号化規格:CIM-XML符号化規格
- 伝送メカニズム:CIM operations over HTTP
- **Common Information Model (CIM)**は、管理について記述した概念情報モデルで、特定の実装を対象にはしていません。CIMにより、管理システムとアプリケーション間で管理情報をやり取りすることができます。これは、分散システム管理を提供する、エージェント-マネージャまたはマネージャ

-エージェント通信になります。CIMには、CIM仕様とCIMスキーマの2つのパートがあります。

CIM仕様は、言語、ネーミング、およびメタスキーマを記述しています。メタスキーマは、モデルの公式な定義です。メタスキーマは、モデルの内容、使用方法、および意味の説明に使う用語を定義します。メタスキーマの要素には、クラス、プロパティ、およびメソッドがあります。メタスキーマは、クラスのタイプとしてインジケーションとアソシエーション(関連)をサポートしています。また、プロパティのタイプとして参照をサポートしています。

CIMスキーマは、実際のモデルを記述しています。CIMスキーマは、管理対象環境で利用できる情報を編成できる汎用の概念的なフレームを提供する、プロパティと関連を持つ一連の名前が付けられたクラスです。

- **Common Information Model Object Manager (CIMOM)**は、CIM標準に基づいてオブジェクトを管理するアプリケーションです(CIM Object Manager)。
- **CIMOMプロバイダ**は、クライアントアプリケーションから要求された特定のタスクを実行するソフトウェアです。各プロバイダは、CIMOMのスキーマの1つまたは複数の機能や役割を果たします。

SUSE® Linux Enterprise Serverには、OpenWBEMプロジェクト [<http://openwbem.org>]が提供するオープンソースのCIMOMが含まれています。

WBEMソフトウェアには、サンプルのプロバイダも含む基本的なNovellプロバイダ、およびNovellスキーマのベースセットを含む一連のパッケージが用意されています。

NovellはOpenWBEMに賛同して特定のプロバイダを開発し、以下のような重要な機能を持つツールを提供しています。

- ネットワークシステムの効率的な管理
- 既存の管理環境設定内の変更を記録
- ハードウェアのインベントリ/資産管理

OpenWBEM CIMOMがどのようにセットアップされ、どのように環境を設定するかを理解しておけば、多彩なネットワーク環境をより確実かつ容易に監視および管理することができます。

11.1 OpenWBEMの設定

OpenWBEMを設定するには、SUSE Linux Enterprise Serverのインストール時にWeb-Based Enterprise Managementソフトウェアを選択するか、またはすでにSUSE Linux Enterprise Serverが稼働しているサーバ上にコンポーネントとしてこのソフトウェアをインストールします。このソフトウェアには、以下のパッケージが含まれています。

cim-schema、CIM (Common Information Model)スキーマ:

このパッケージには、Common Information Model (CIM)が含まれます。CIMは、ネットワーク/企業環境内の総合的な管理情報を記述するモデルです。CIMは仕様とスキーマで構成されます。仕様は、他の管理モデルとの統合に関する詳細を定義しています。スキーマは、実際のモデルを記述しています。

openwbem、WBEM (Web Based Enterprise Management)の実装版:

このパッケージには、OpenWBEMの実装版が含まれています。OpenWBEMは、DMTFのCIMおよびWBEM技術を簡単に導入、展開するために役立つ一連のソフトウェアコンポーネントです。DMTF、およびその技術に関する詳細は、DMTF Webサイト [<http://www.dmtf.org>]を参照してください。

openwbem-base-providers:

このパッケージには、OpenWBEM CIMOM用のコンピュータ、システム、オペレーティングシステム、およびプロセスなどのベースオペレーティングシステムコンポーネントのNovell Linux一式が含まれています。

openwbem-smash-providers:

このパッケージには、Novell Linux版のOpenWBEM CIMOM用SMASH (Systems Management Architecture for Server Hardware)が含まれています。

yast2-cim、YaST2 - CIMのバインド:

このパッケージは、YaST2(SUSEシステムツールマネージャのグラフィカルユーザインタフェース)へのCIMバインディングを追加します。これらのバインディングにより、Common Information Model Object Manager (CIMOM)へのクライアントインタフェースが提供されます。

この節では、次の情報を紹介します。

- [11.1.1項「owcimomdの起動、終了、またはステータスの確認」](#) (270 ページ)
- [11.1.2項「セキュアアクセスの確保」](#) (270 ページ)
- [11.1.3項「ログのセットアップ」](#) (274 ページ)

11.1.1 owcimomdの起動、終了、またはステータスの確認

デフォルトでは、WBEM(Web-Based Enterprise Management)ソフトウェアをインストールすると、owcimomdデーモンが起動します。次の表で、owcimomdの起動、停止、および確認ステータスを説明します。

表 11.1 owcimomdの管理用コマンド

タスク	Linuxコマンド
owcimomdの開始	コンソールシェルのルートでrcowcimomd startを入力します。
owcimomdの終了	コンソールシェルのルートでrcowcimomd stopを入力します。
owcimomdステータスの確認	コンソールシェルのルートでrcowcimomd statusを入力します。

11.1.2 セキュアアクセスの確保

OpenWBEMのデフォルトのセットアップは、比較的安全(セキュア)です。ただし、組織の要望に応じてOpenWBEMコンポーネントに対し、できる限りセキュアなアクセスを確保するため、次の項目を検討してください。

- [証明書項](#) (271 ページ)
- [ポート項](#) (271 ページ)

- [認証項 \(273 ページ\)](#)

証明書

安全にSSL (Secure Socket Layers)通信を行うには、証明書が必要になります。OESをインストールすると、OpenWBEMはインストールされたOES用に自己署名済み証明書を生成します。

必要に応じて、デフォルトの証明書へのパスを、購入した商用証明書、または/etc/openwbem/openwbem.confファイルのhttp_server.SSL_cert = *path_filename*設定で生成した別の証明書へのパスと置き換えることができます。

デフォルトで生成された証明書は、次の場所に置かれています。

```
/etc/openwbem/servercert.pem
```

新しい証明書を生成する場合は、以下のコマンドを使用します。このコマンドを起動すると、現在の証明書が置き換えられるため、新しい証明書を生成する前に、古い証明書のコピーを作成することをお勧めします。

コンソールシェルのルートで次を入力します。

```
sh/etc/openwbem/owgencert
```

OpenWBEMが使用する証明書を変更する場合は、[11.2.2項「証明書設定の変更」](#) (282 ページ)を参照してください。

ポート

OpenWBEMは、セキュアなポートである5989を使用するすべての通信をデフォルトで受け入れるように設定されています。次の表で、ポート通信のセットアップと推奨設定について説明します。

表 11.2 ポート通信セットアップおよび推奨設定

ポート	タイプ	推奨設定と注意事項
5989	セキュア	<p>OpenWBEM通信がHTTPSサービスを介して使用するセキュアなポート。</p> <p>これはのデフォルトの設定です。</p> <p>この設定で、CIMOMとクライアントアプリケーション間のすべての通信は、サーバとワークステーション間でインターネットを通じて送信されるときに暗号化されます。この情報を表示するには、クライアントアプリケーションを通じてユーザ認証を行う必要があります。</p> <p>この設定を設定ファイル内に保管することをお勧めします。</p> <p>ルータやファイアウォールがクライアントアプリケーションとモニタリングされるノードとの間に存在する場合、OpenWBEM CIMOMが必要なアプリケーションと通信できるようにするには、このポートを開いておく必要があります。</p>
5988	保護なし	<p>OpenWBEM通信がHTTPSサービスを介して使用するセキュアでないポート。</p> <p>デフォルトでは、この設定は無効にされています。</p> <p>この設定では、CIMOMとクライアントアプリケーション間のすべての通信は、サーバとワークステーション間でインターネットを通じて送信されるときに、誰でも認証なしで開き、レビューできます。</p> <p>この設定は、CIMOMの問題をデバッグするときのみに使用することをお勧めします。問題が解決されたら、すぐにセキュアでないポートオプションを無効に戻してください。</p> <p>ルータやファイアウォールが、クライアントアプリケーションとモニタリングされるノードとの間に存在する場合、</p>

OpenWBEM CIMOMがセキュアでないアクセスを要求する必要なアプリケーションと通信できるようにするには、このポートを開いておく必要があります。

デフォルトのポートの割り当てを変更する場合は、[11.2.3項「ポート設定の変更」](#) (283 ページ)を参照してください。

認証

次の認証設定は、SUSE Linux Enterprise ServerのOpenWBEMに対するデフォルトとして設定および有効化されています。

このデフォルト設定はいずれも変更が可能です。詳細については、[11.2.1項「認証設定の変更」](#) (275 ページ)を参照してください。

- `http_server.allow_local_authentication = true`
- `http_server.ssl_client_verification = disabled`
- `http_server.use_digest = false`
- `owcimomd.allow_anonymous = false`
- `owcimomd.allowed_users = root`
- `owcimomd.authentication_module =`
`/usr/lib/openwbem/authentication/libpamauthentication.so`

OpenWBEM CIMOMは、デフォルトでPAMが有効になっているため、ローカルのルートユーザは、ローカルのルートユーザ証明書を使用してOpenWBEM CIMOMの認証を行うことができます。

11.1.3 ログのセットアップ

このデフォルト設定はいずれも変更が可能です。詳細については、[11.2.4項「デフォルトのログ設定の変更」](#) (284 ページ)を参照してください。

デフォルトでは、OpenWBEMのログは以下のように設定されています。

- `log.main.components = *`
- `log.main.level = ERROR`
- `log.main.type = syslog`

この設定の場合、owcimomdのログはsyslogdの設定に応じて、`/var/log/messages`ファイル、または他のファイルに書き込まれます。これは、すべてのコンポーネント(owcimomd)のすべてのエラーを記録します。

11.2 OpenWBEM CIMOM設定の変更

OpenWBEM CIMOM(owcimomd)を起動すると、`openwbem.conf`ファイルからランタイム設定が読み込まれます。`openwbem.conf`ファイルは、`/etc/openwbem`ディレクトリにあります。

オプションがセミコロン(;), またはシャープ記号(#)でコメントアウトされている設定では、デフォルト設定が使用されます。

このファイルに変更を加える場合は、使用するプラットフォームにネイティブな形式でファイルを保存するテキストエディタを使用できます。

`openwbem.conf`ファイル中の任意の設定を変更することができます。ここでは、次の環境設定について説明していきます。

- [11.2.1項「認証設定の変更」](#) (275 ページ)
- [11.2.2項「証明書設定の変更」](#) (282 ページ)
- [11.2.3項「ポート設定の変更」](#) (283 ページ)
- [11.2.4項「デフォルトのログ設定の変更」](#) (284 ページ)

- [11.2.5項 「デバッグログの設定」 \(293 ページ\)](#)
- [11.2.6項 「他のログの設定」 \(294 ページ\)](#)

11.2.1 認証設定の変更

認証設定を変更する場合、制御可能な項目がいくつかあります。

- CIMOMにアクセスできるユーザ
- 使用する認証モジュール

以下の設定を参照してください。

- [http_server.allow_local_authentication 項 \(275 ページ\)](#)
- [http_server.digest_password_file 項 \(276 ページ\)](#)
- [http_server.ssl_client_verification 項 \(277 ページ\)](#)
- [http_server.ssl_trust_store 項 \(278 ページ\)](#)
- [http_server.use_digest 項 \(278 ページ\)](#)
- [owcimomd.ACL_superuser 項 \(279 ページ\)](#)
- [owcimomd.allow_anonymous 項 \(279 ページ\)](#)
- [owcimomd.allowed_users 項 \(280 ページ\)](#)
- [owcimomd.authentication_module 項 \(281 ページ\)](#)
- [simple_auth.password_file 項 \(282 ページ\)](#)

http_server.allow_local_authentication

目的

ローカルシステムのファイルのパーミッションによって、パスワードなしでローカル認証を許可するよう、http_serverに指示します。

この設定と、[Basic] または [Digest] の設定を併用することができます。

構文

```
http_server.allow_local_authentication = option
```

オプション	説明
true	ローカル認証を有効にします。 デフォルトの設定です。
false	ローカル認証を無効にします。

例

```
http_server.allow_local_authentication = true
```

http_server.digest_password_file

目的

パスワードファイルの場所を指定します。http_server.use_digestを有効にしている場合、この設定が必要になります。

構文

```
http_server.digest_password_file = path_filename
```

ダイジェストパスワードファイルの、デフォルトのパスとファイル名を以下に示します。

```
/etc/openwbem/digest_auth.passwd
```

例

```
http_server.digest_password_file =  
/etc/openwbem/digest_auth.passwd
```

http_server.ssl_client_verification

目的

SSLクライアント証明書を使って、サーバにクライアントの認証を行わせるかどうかを指定します。

デフォルトでは、この設定は無効にされています。

構文:

```
http_server.ssl_client_verification = option
```

オプション	説明
autoupdate	[Optional] オプションと同じ機能を指定します。ただし、これまでに未知のクライアント証明書でもHTTP認証に成功したものはトラストストアに追加されるため、同じ証明書を使用する後続のクライアント接続ではHTTP認証は要求されません。
disabled (無効)	クライアント証明書の確認を無効にします。 デフォルトの設定です。
optional	信頼された証明書の認証を許可します(HTTP認証は必要なし)。 クライアントがHTTP認証に成功した場合は、信頼のない証明書もSSLハンドシェイクに成功します。
required	SSLハンドシェイクに成功するには、信頼された証明書が必要とされます。

例

```
http_server.ssl_client_verification = disabled
```

http_server.ssl_trust_store

目的

OpenSSLトラストストアのあるディレクトリを指定します。

構文

```
http_server.ssl_trust_store = path
```

トラストストアファイルのデフォルトパスを以下に示します。

```
/etc/openwbem/truststore
```

例

```
http_server.ssl_trust_store = /etc/openwbem/truststore
```

http_server.use_digest

目的

HTTPサーバに、ダイジェスト認証の使用を指示します。基本(Basic)認証機構はバイパスされます。ダイジェスト認証を使用するには、owdigestgenpassを使ってダイジェストパスワードファイルを設定する必要があります。

ダイジェスト認証の場合、owcimomd.authentication_moduleに指定された認証モジュールは使われません。

構文

```
http_server.use_digest = option
```

オプション	説明
false	基本(Basic)認証機構を有効にします。 デフォルトの設定です。

オプション	説明
true	基本(Basic)認証機構を無効にします。

例

```
http_server.use_digest = false
```

owcimomd.ACL_superuser

目的

owcimomdによって維持されるすべてのネームスペース内のすべてのCommon Information Model (CIM) データにアクセスするユーザのユーザ名を指定します。このユーザ名は、すべてのACLユーザ権限が保管される/root/securityネームスペースの管理に使用します。

ACL処理は、OpenWBEM_Acl1.0.mofファイルがインポートされない限り、有効になりません。

構文

```
owcimomd.ACL_superuser = username
```

例

```
owcimomd.ACL_superuser = root
```

owcimomd.allow_anonymous

目的

owcimomdへの匿名(Anonymous)ログインを有効、または無効にします。

構文

```
owcimomd.allow_anonymous = option
```

オプション	説明
false	owcimomdデータへのアクセスにユーザ名とパスワードを使用したログインが必要とされます。 デフォルトでは、このオプションが選択されています。また、この設定を使用することをお勧めします。
true	owcimomdへの匿名ログインを許可します。 この設定を使用する場合、認証が無効になります。owcimomdデータにアクセスするために、ユーザ名やパスワードは必要ありません。

例

```
owcimomd.allowed_anonymous = false
```

owcimomd.allowed_users

目的

owcimomdデータへのアクセスを許可する一連のユーザを指定します。

構文

```
owcimomd.allowed_users = option
```

オプション	説明
ユーザ名	owcimomdデータへのアクセスを許可する、1人または複数のユーザを指定します。 複数のユーザ名を指定する場合、各ユーザはスペースで区切ります。 ルートユーザがデフォルト設定です。

オプション	説明
*	すべてのユーザに認証を許可します(ACLでのアクセス制御を代わりに選択した場合など)。 owcimomd.allow_anonymousにtrueを設定しない限り、すべての認証方法にこのオプションが適用されます。

例

```
owcimomd.allowed_users = bcwhitely jkcarey jlanderson
```

owcimomd.authentication_module

目的

owcimomdが使用する認証モジュールを指定します。この設定は、認証モジュールを含む共有ライブラリへの絶対パスです。

構文

```
owcimomd.authentication_module = path_filename
```

認証モジュールの、デフォルトのパスとファイル名を以下に示します。

```
/usr/lib/openwbem/authentication/libpamauthentication.so
```

例

```
owcimomd.authentication_module =  
/usr/lib/openwbem/authentication/libpamauthentication.so
```

simple_auth.password_file

目的

シンプル(simple)認証モジュールを使用する場合に、パスワードのパスを指定します。

デフォルトでは、この設定は無効にされています。

構文

```
simple_auth.password_file = path_filename
```

例

```
simple_auth.password_file =  
/etc/openwbem/simple_auth.passwd
```

11.2.2 証明書設定の変更

http_server.SSL&lowbarcertおよびhttp_server.SSL&lowbarkey設定には、ホストの秘密鍵と証明書を含むファイルの場所を指定します。この秘密鍵と証明書は、OpenSSLがHTTPS通信を行う場合に使用されます。

デフォルトでは、.pemファイルは以下の場所に格納されています。

```
/etc/openwbem/servercert.pem
```

```
/etc/openwbem/serverkey.pem
```

構文

```
http_server.SSL_cert = path_filename
```

または

```
http_server.SSL_key = path_filename
```

注意

鍵と証明書の両方を同じファイルに保管することができます。この場合、`http_server.SSL_cert`と`http_server.SSL_key`の値は同じになります。

例

```
http_server.SSL_cert = /etc/openwbem/servercert.pem
```

```
http_server.SSL_key = /etc/openwbem/servercert.pem
```

```
http_server.SSL_key = /etc/openwbem/serverkey.pem
```

11.2.3 ポート設定の変更

`http_server.http&lowbarport`および`server.https_port`設定には、`owcimomd`がすべてのHTTP/HTTPS通信のために待機するポート番号を指定します。

構文

```
http_server.http_port = option
```

または

```
http_server.https_port = option
```

オプション	説明
<i>Specific_port_number</i>	HTTPまたはHTTPS通信を行うための特定のポートを指定します。 HTTPの場合、デフォルトのポートは5988です。 HTTPSの場合、デフォルトのポートは5989です。

オプション	説明
-1	HTTP接続、またはHTTPS接続を無効にします (HTTPS接続のみをサポートする場合など)。
0	実行時に動的にポート番号を割り当てます。

例

HTTPポートを無効にして、HTTPS通信用のポート5989を有効にする設定を以下に示します。

```
http_server.http_port = -1
```

```
http_server.https_port = 5989
```

11.2.4 デフォルトのログ設定の変更

owcimomd.confファイルの次のログ設定で、ログを記録する場所、頻度、およびエラータイプ、ログのサイズ、ファイル名および形式を指定できます。

- [log.main.categories項](#) (285 ページ)
- [log.main.components項](#) (286 ページ)
- [log.main.format項](#) (287 ページ)
- [log.main.level項](#) (289 ページ)
- [log.main.location項](#) (290 ページ)
- [log.main.max_backup_index項](#) (291 ページ)
- [log.main.max_file_size項](#) (291 ページ)
- [log.main.type項](#) (292 ページ)

デバッグログの記録を設定する場合は、[11.2.5項「デバッグログの設定」](#) (293 ページ)を参照してください。

他のログを設定する場合は、[11.2.6項「他のログの設定」](#) (294 ページ)を参照してください。

log.main.categories

目的

ログ出力のカテゴリを指定します。

構文

```
log.main.categories = option
```

オプション	説明
<code>category_name</code>	<p>記録するカテゴリを、スペースで区切って指定します。</p> <p>owcimomdで利用できるカテゴリを以下に示します。</p> <ul style="list-style-type: none">• DEBUG• エラー• FATAL• INFO <p>これらのオプションの詳細については、log.main.level項 (289 ページ)を参照してください。</p> <p>このオプションに指定した場合、あらかじめ定義されているカテゴリはレベルとして扱われずに、それぞれ独立したカテゴリとして処理されます。デフォルト値はありません。カテゴリが設定されていない場合、いずれのカテゴリも記録されず、<code>log.main.level</code>の設定が使用されます。</p> <p>* すべてのカテゴリを記録します。</p>

オプション	説明
	デフォルトの設定です。

例

```
log.main.categories = FATAL ERROR INFO
```

log.main.components

目的

ログが出力するコンポーネントを指定します。

構文

```
log.main.components = option
```

オプション	説明
<i>component_name</i>	記録するコンポーネント(owcimomdなど)を指定します。複数を指定する場合は、スペースで各コンポーネントを区切ります。 プロバイダは、独自のコンポーネントを使用できます。
*	すべてのコンポーネントを記録することを指定します。 デフォルトの設定です。

例

```
log.main.components = owcimomd nssd
```

log.main.format

目的

ログメッセージの形式(`printf()`スタイル変換指定子が混在するテキスト)を指定します。

構文

```
log.main.format = conversion_specifier
```

オプション	指定内容
%%	%
%c	コンポーネント(owcimomdなど)
%d	<より前(日付) 中カッコで囲まれた日付形式指定子を後ろに付けることができます。たとえば、 <code>%d{%H:%M:%S}</code> or <code>%d{%d %b %Y %H:%M:%S}</code> のようになります。日付形式指定子がない場合は、ISO 8601形式であると見なされます。 唯一追加される変数は、ミリ秒の数値を示す%Qです。 日付形式指定子の詳細については、<ctime>ヘッダの <code>strftime()</code> 関数に関する説明を参照してください。
%e	XML CDATAとしてのメッセージ。これには、“<![CDATA[“ and ending “]]>”も含まれます。
%F	ファイル名
%l	ファイル名と行番号。例:file.cpp(100)
%L	行番号

オプション	指定内容
%M	ログ要求が発行されたメソッド名 (<code>__PRETTY_FUNCTION__</code> またはC99's <code>__func__</code> をサポートするC++コンパイラとのみ動作可能)。
%m	メッセージ
%n	プラットフォーム依存の行区切り文字(<code>\n</code>)または(<code>\r\n</code>)。
%p	カテゴリ(レベルまたは優先度)。
%r	アプリケーションの起動からログに記録されるイベントの発生までの経過時間を表すミリ秒の数値。
%t	スレッドID
\n	復帰改行
\t	<Tab>
\r	改行
\\	\
\x<hexDigits>	16進数で表した文字

フィールドの最小幅、最大幅、および位置揃えを調整することができます。書式変更子(オプション)は、パーセント記号(%)と変換文字の間に指定します。最初の書式変更子マイナス記号(-)は、左揃えを指示します。その次に、フィールドの最小幅を指定する場合は、出力する最小文字数を表す整数を書式変更子として指定します。表示するデータの文字数がこれより少ない場合は、位置揃えの指定に応じてフィールドの左または右が、スペースで埋められます。表示するデータの文字数がフィールドの最小幅よりも多い場合は、そのデータ全体を表示できるように、フィールドが拡張されます。

フィールドの最大幅を指定するには、ピリオドに続けて(.)10進定数を指定します。データの文字数がフィールドの最大幅よりも大きい場合、超過する文

字数分の文字がデータの先頭から(デフォルト)、またはデータの最後から(左揃えが指定されている場合)切り捨てられます。

例

Log4j TTCCレイアウト:

```
"%r [%t] %-5p %c - %m"
```

固定サイズがある以外はTTCCに類似しているフィールド:

```
"%-6r [%15.15t] %-5p %30.30c - %m"
```

log4j.dtd 1.2に準拠し、Chainsawで処理可能なXML出力(実際に使用する場合は1行でなければなりません、ここでは見やすくするために行を分けています)。

```
"<log4j:event logger=\"%c\" timestamp=\"%d{%s%Q}\" level=\"%p\"  
thread=\"%t\"> <log4j:message>%e</log4j:message>  
<log4j:locationInfo class=\"\" method=\"\" file=\"%F\"  
line=\"%L\"/></log4j:event>"
```

デフォルトを以下に示します。

```
log.main.format = [%t]%m
```

log.main.level

目的

ログ出力のレベルを指定します。レベルを設定した場合、指定したレベル以上にある、あらかじめ定義されているすべてのカテゴリが、ログに出力されます。

構文

```
log.main.level = option
```

オプション	説明
DEBUG	すべてのDebug(デバッグ)、Info(情報)、Error(エラー)およびFatal(致命的)エラーメッセージをログに記録します。
エラー	すべてのError(エラー)およびFatal(致命的)エラーメッセージをログに記録します。 デフォルトの設定です。
FATAL	致命的(Fatal)エラーメッセージのみをログに記録します。
INFO	すべての情報(Info)、Error(エラー)およびFatal(致命的)エラーメッセージをログに記録します。

例

```
log.main.level = ERROR
```

log.main.location

目的

log.main.type設定オプションで、ログをファイルに送信するように指定されている場合、owcimomdログファイルが使用する場所を指定します。

構文

```
log.main.location = path_filename
```

例

```
log.main.location = /system/cimom/var/owcimomd.log
```


log.main.max_backup_index

目的

記録を保持するバックアップログの量を指定します。この量を超えた場合は、最も古いバックアップログが消去されます。

構文

```
log.main.backup_index = option
```

オプション	説明
<i>unsigned_integer_above_0</i>	保持するバックアップログ数を指定します。 デフォルトは1です。
0	バックアップログは作成されず、最大ファイルサイズに達したログは切り捨てられます。

例

```
log.main.max_backup_index = 1
```

log.main.max_file_size

目的

owcimomdログの最大サイズ(KB)を指定します。

構文

```
log.main.max_file_size = option
```

オプション	説明
<code>unsigned _integer_in_KB</code>	ログを一定のサイズ(KB)に制限します。
0	ログのサイズを制限しません(無制限)。 デフォルトの設定です。

例

```
log.main.max_file_size = 0
```

log.main.type

目的

owcimomdが使用するメインログの種類を指定します。

構文

```
log.main.type = option
```

オプション	説明
file	log.main.location設定で識別されるファイルにすべてのメッセージを送信します。
null	ログを無効にします。
syslog	すべてのログメッセージをsyslogインタフェースに送信します。 デフォルトの設定です。

例

```
log.main.type = syslog
```

11.2.5 デバッグログの設定

owcimomdがデバッグモードで起動している場合、次の設定でデバッグログがアクティブになります。

- `log.debug.categories = *`
- `log.debug.components = *`
- `log.debug.format = [%t] %m`
- `log.debug.level = *`
- `log.debug.type = stderr`

デバッグログの色設定

デバッグログで色を使用する場合は、以下のASCIIエスケープコードを使用します。

```
log.debug.format =  
\x1b[1;37;40m[\x1b[1;31;40m%- .6t\x1b[1;37;40m]\x1b[1;32;40m  
%m\x1b[0;37;40m
```

追加の色を使用する場合は、`log.debug.format`コマンドで次のコードを使用します。

表 11.3 *log.debug.format* コマンド用の追加カラーコード

色	コード
赤	<code>\x1b[1;31;40m</code>
えんじ色	<code>\x1b[0;31;40m</code>

色	コード
緑	\x1b[1;32;40m
深緑	\x1b[0;32;40m
黄色	\x1b[1;33;40m
濃い黄色	F\x1b[0;33;40m
青	\x1b[1;34;40m
濃い青	\x1b[0;34;40m
紫	\x1b[1;35;40m
濃い紫	\x1b[0;35;40m
シアン	\x1b[1;36;40m
暗いシアン	\x1b[0;36;40m
白	\x1b[1;37;40m
暗い白	\x1b[0;37;40m
灰色	\x1b[0;37;40m
色のリセット	\x1b[0;37;40m

11.2.6 他のログの設定

追加ログを作成するには、次の設定でログ名のリストを作成します。

```
owcimomd.additional_logs = logname
```

複数のログ名を指定する場合は、間をスペースで区切ります。

構文

```
owcimomd.additional_logs = logname
```

各ログに対して、以下の設定が適用されます。

- ログ.*log_name*.categories
- ログ.*log_name*.components
- ログ.*log_name*.format
- ログ.*log_name*.level
- ログ.*log_name*.location
- ログ.*log_name*.max_backup_index
- ログ.*log_name*.max_file_size

例

```
owcimomd.additional_logs = errorlog1 errorlog2 errorlog3
```

11.3 詳細情報

OpenWBEMの詳細は、以下の情報を参照してください。

- ローカルサーバファイルシステムのusr/share/doc/packages/openwbem中にあるドキュメント。
- Readme
- openwbem-faq.html
- Novell Cool Solutionsの記事:An Introduction to WBEM and OpenWBEM in SUSE Linux [<http://www.novell.com/cool solutions/feature/14625.html>]

- OpenWBEM Webサイト [<http://www.openwbem.org>]
- DMTF Webサイト [<http://www.dmtf.org>]

IPネットワークの大容量記憶デバイス—iSCSI

12

サーバの運用、またはコンピュータセンターの重要なタスクの1つには、サーバシステムに対してハードディスクスペースを提供することがあります。メインフレームセクターでは、ディスクスペースを提供するためにしばしばファイバチャネルが使われます。今まで、UNIXコンピュータや、他の主要サーバでは、このような集中ストレージソリューションは利用されていませんでした。

Linux-iSCSIは、Linuxコンピュータを集中ストレージシステムに接続するための、簡単で費用もあまりかからない手頃なソリューションです。基本的にiSCSIは、SCSIコマンドをIPレベルで転送することを表しています。プログラムがデバイスへの照会を開始すると、オペレーティングシステムが必要なSCSIコマンドを作成します。作成されたコマンドは、一般的にiSCSIイニシエータと呼ばれるソフトウェアにより、IPパッケージに組み込まれ、必要に応じて暗号化されます。次に、目的のiSCSIリモートステーションにパッケージが転送されます。リモートステーションは、iSCSIターゲットと呼ばれることもあります。

多くのストレージソリューションが、iSCSIによるアクセス手段を提供しています。また、LinuxサーバにiSCSIターゲットの役割をさせることもできます。この場合、ファイルシステムサービスが最適化されるようにLinuxサーバを設定する必要があります。iSCSIターゲットは、Linux中のブロックデバイスにのみアクセスします。そのため、RAIDソリューションを使ってディスクスペースを増やしたり、メモリを大量に搭載してデータキャッシュの性能を向上することができます。RAIDの詳細については、7.2項「ソフトウェアRAID設定」(137 ページ)も参照してください。

12.1 iSCSIターゲットのセットアップ

SUSE® Linux Enterprise Serverには、Ardis iSCSIターゲットから発展したオープンソースのiSCSIソリューションが用意されています。基本的な設定はYaSTを使って行えますが、iSCSIの機能をフル活用するには、手動で設定を行う必要があります。

12.1.1 YaSTを使ったiSCSIターゲットの作成

iSCSIターゲットの設定では、既存のブロックデバイスまたはファイルシステムのイメージが、iSCSIイニシエータにエクスポートされます。まず、YaSTを使って必要なブロックデバイスを作成するか、ファイルシステムイメージを作成していただきパーティションの作成については、[8.5.7項「YaSTパーティション分割ツールの使用」](#) (172ページ)を参照してください。ファイルシステムイメージは、手動で作成する必要があります。たとえば、サイズが4GBの/var/lib/xen/images/xen-0イメージを作成する場合、まずこのディレクトリを作成してから、イメージを作成します。

```
mkdir -p /var/lib/xen/images
dd if=/dev/zero of=/var/lib/xen/images/xen-0 seek=1M bs=4096 count=1
```

iSCSIターゲットを設定するには、YaSTの *[iSCSIターゲット]* モジュールを起動します。設定項目は、3つのタブに分かれています。[Service] タブでは、実行モードとファイアウォールの設定を行います。リモートコンピュータからiSCSIターゲットにアクセスする場合は、*[ファイアウォールでポートを開く]* を選択します。iSNSサーバでディスカバリとアクセス制御を管理する場合は、*[iSNSアクセス管理]* を有効にして、iSNSサーバのIPアドレスを入力します。ホスト名は有効なものでも使用できず、IPアドレスを使用する必要がありますことに注意してください。iSNSの詳細は、[第13章 Linux向けのiSNSの概要](#) (309 ページ)を参照してください。

[Global] タブでは、iSCSIサーバの設定を行います。ここで設定する認証方法は、サービスの検出に使用します。ターゲットにアクセスする場合のものではありません。ディスカバリへのアクセスを制限しない場合は、*[No Authentication]* を選択します。

認証が必要な場合、2つの検討事項があります。まず、イニシエータは、iSCSIターゲットでディスカバリを実行するためのパーミッションがあることを証明できなければなりません。この設定は、*[Incoming Authentication]* で行い

ます。もう1つは、iSCSIターゲットはイニシエータに、自分が正しいターゲットであることを証明しなければなりません。そのため、iSCSIターゲットもユーザ名とパスワードを使用できます。この設定は、*[Outgoing Authentication]*で行います。認証の詳細は、RFC3720を参照してください(<http://www.ietf.org/rfc/rfc3720.txt>を参照)。

ターゲットは、*[Targets]* タブで定義します。新しいiSCSIターゲットを作成するには、*[追加]* をクリックします。最初のダイアログでは、エクスポートするデバイスに関する情報を指定します。

ターゲット

[Target] 行には、以下のような固定形式の構文を指定します。

```
iqn.yyyy-mm.<reversed domain name>
```

この行は常に「iqn」から始まります。「yyyy-mm」の部分には、このターゲットをアクティブにする日付を指定します。命名規則の詳細については、RFC3722を参照してください(<http://www.ietf.org/rfc/rfc3722.txt>を参照)。

Identifier

[Identifier] は、自由に指定することができます。ただし、システムを体系的に管理するためにも、一定のスキーマを使用するようにしてください。

LUN

ターゲットに複数のLUNを割り当てることができます。そのためには、*[ターゲット]* タブのターゲットを選択し、*[編集]* をクリックします。そこから、既存のターゲットに新しいLUNを追加します。

パス

エクスポートするブロックデバイス、またはファイルシステムイメージのパスを追加します。

次のメニューでは、ターゲットへのアクセス制限を設定します。この設定は、ディスクバリの認証設定とほとんど変わりありません。この場合、少なくとも着信認証を設定する必要があります。

新しいターゲットの設定を完了するには、*[次へ]* をクリックします。

[Target] タブの概要ページが表示されます。変更内容を適用するには、*[完了]* をクリックします。

12.1.2 iSCSIターゲットの手動設定

iSCSIターゲットを設定するには、`/etc/ietd.conf`を編集します。このファイル中の、最初の*Target*宣言より前にあるすべてのパラメータは、ファイルのグローバルパラメータになります。この部分にある認証情報は、グローバルパラメータではありません。iSCSIターゲットの検出に用いられます。

iSNSサーバにアクセスできる場合、最初の設定内容はこのサーバをターゲットに通知することです。iSNSサーバのアドレスは常にIPアドレスで指定する必要がありますことに注意してください。通常のドメイン名では不十分です。この機能の設定は、次のようになります。

```
iSNSServer 192.168.1.111
iSNSAccessControl no
```

この設定では、iSCSIターゲットがiSNSサーバでそれ自体を登録し、ディスクバリのイニシエータとなります。iSNSの詳細は、[第13章 Linux向けiSNSの概要](#)(309ページ)を参照してください。iSNSディスクバリのアクセス制御はサポートされていないことに注意してください。[iSNSアクセス管理]を[いいえ]のままにします。

すべての直接iSCSI認証は、双方向で行われます。iSCSIターゲットがiSCSIイニシエータに認証を要求するには、IncomingUserを使用します。このオプションは、複数回追加できます。一方、iSCSIイニシエータも、iSCSIターゲットに認証を要求することができます。この場合は、OutgoingUserを使用します。どちらの場合も、構文は同じです。

```
IncomingUser <username> <password>
OutgoingUser <username> <password>
```

認証の後には、1つまたは複数のターゲット定義を指定します。定義する各ターゲットについて、Targetセクションを追加します。このセクションは、常にTarget識別子から始まり、その後に論理ユニット番号(LUN)を定義します。

```
Target iqn.yyyy-mm.<reversed domain name>[:identifier]
    Lun 0 Path=/dev/mapper/system-v3
    Lun 1 Path=/dev/hda4
    Lun 2 Path=/var/lib/xen/images/xen-1,Type=fileio
```

Target行の「yyyy-mm」の部分は、ターゲットを有効にする日付を定義します。また、identifier (識別子)には、任意の値を指定できます。命名規

則の詳細については、RFC3722を参照してください(<http://www.ietf.org/rfc/rfc3722.txt>を参照)。この例では、3つの異なるブロックデバイスをエクスポートしています。最初のブロックデバイスは論理ボリューム(7.1項「LVMの設定」(127 ページ)も参照)、2番目はIDEパーティション、3番目はローカルファイルシステムで利用できるイメージです。これらはすべてiSCSIイニシエータへのブロックデバイスのようになります。

iSCSIターゲットを有効にする前に、Lun定義の後に、最低1つのIncomingUserを追加してください。このパラメータは、このターゲットの使用に対する認証を指定します。

変更内容を有効にするには、`rcopen-iscsi restart`コマンドを実行して、`iscsitaraget`デーモンを再起動します。`/proc`ファイルシステムで、設定内容を確認してください。

```
cat /proc/net/iet/volume
tid:1 name:iqn.2006-02.com.example.iserv:systems
    lun:0 state:0 iotype:fileio path:/dev/mapper/system-v3
    lun:1 state:0 iotype:fileio path:/dev/hda4
    lun:2 state:0 iotype:fileio path:/var/lib/xen/images/xen-1
```

ここで説明しているほかにも、iSCSIターゲットの動作を制御するさまざまなオプションがあります。詳細については、`ietd.conf`のマニュアルページを参照してください。

`/proc`ファイルシステムには、アクティブなセッションも表示されます。接続されている各イニシエータに対応するエントリが、`/proc/net/iet/session`に追加されます。

```
cat /proc/net/iet/session
tid:1 name:iqn.2006-02.com.example.iserv:system-v3
    sid:562949957419520
initiator:iqn.2005-11.de.suse:cn=rome.example.com,01.9ff842f5645
    cid:0 ip:192.168.178.42 state:active hd:none dd:none
    sid:281474980708864 initiator:iqn.2006-02.de.suse:01.6f7259c88b70
    cid:0 ip:192.168.178.72 state:active hd:none dd:none
```

12.1.3 ietadmを使ったオンラインターゲットの設定

iSCSIターゲットの設定を変更する必要がある場合、設定ファイルの変更内容を有効にするには、変更後にターゲットを再起動する必要があります。ただ

し、この作業を行うと、アクティブなセッションがすべて中断されます。この問題を回避するには、環境設定ファイルの/etc/ietd.confを変更すると同時に、ietadm管理ユーティリティを使って現在の設定も変更してください。

LUNを指定した新しいiSCSIターゲットを作成するには、まず設定ファイルを更新します。追加するエントリの例を以下に示します。

```
Target iqn.2006-02.com.example.iserv:system2
    Lun 0 Path=/dev/mapper/system-swap2
    IncomingUser joe secret
```

この設定を手動で行うには、次の手順に従ってください。

- 1 `ietadm --op new --tid=2 --params Name=iqn.2006-02.com.example.iserv:system2` コマンドを実行して、新しいターゲットを作成します。
- 2 `ietadm --op new --tid=2 --lun=0 --params Path=/dev/mapper/system-swap2` コマンドを実行して、LUNを追加します。
- 3 `ietadm --op new --tid=2 --user --params=IncomingUser=joe,Password=secret` コマンドを実行して、このターゲットにユーザ名とパスワードを設定します。
- 4 `cat /proc/net/iet/volume` コマンドを実行して、設定内容を確認します。

アクティブな接続を削除することもできます。まず、`cat /proc/net/iet/session` コマンドを実行して、アクティブな接続を表示します。次のような情報が表示されます。

```
cat /proc/net/iet/session
tid:1 name:iqn.2006-03.com.example.iserv:system
    sid:281474980708864 initiator:iqn.1996-04.com.example:01.82725735af5
    cid:0 ip:192.168.178.72 state:active hd:none dd:none
```

セッションIDが 281474980708864 のセッションを削除する場合は、`ietadm --op delete --tid=1 --sid=281474980708864 --cid=0` コマンドを実行します。このコマンドを実行すると、クライアントシステムからデバイスにアクセスできなくなるため、このデバイスにアクセスしているデバイスがハングアップする可能性があることに注意してください。

ietadmを使って、さまざまな環境設定パラメータを変更することもできます。グローバル変数を一覧表示する場合は、`ietadm --op show --tid=1 --sid=0`コマンドを実行します。次のような実行結果が表示されます。

```
InitialR2T=Yes
ImmediateData=Yes
MaxConnections=1
MaxRecvDataSegmentLength=8192
MaxXmitDataSegmentLength=8192
MaxBurstLength=262144
FirstBurstLength=65536
DefaultTime2Wait=2
DefaultTime2Retain=20
MaxOutstandingR2T=1
DataPDUInOrder=Yes
DataSequenceInOrder=Yes
ErrorRecoveryLevel=0
HeaderDigest=None
DataDigest=None
OFMarker=No
IFMarker=No
OFMarkInt=Reject
IFMarkInt=Reject
```

これらのパラメータは、すべて簡単に変更することができます。たとえば、最大接続数を2に変更する場合は、`ietadm --op update --tid=1 --params=MaxConnections=2`を実行します。`/etc/ietd.conf`ファイルでは、このパラメータに対応する行が`MaxConnections 2`のように指定されています。

警告: ietadmによる変更に応じたietd.confファイルの更新

ietadmコマンドで行った設定の変更は、一時的なものです。`/etc/ietd.conf`設定ファイルに変更内容を追加しない限り、システムを再起動すると設定内容は失われます。ネットワーク上でのiSCSIの利用方法によっては、設定内容が失われることにより、問題が発生する可能性もあります。

ietadmコマンドでは、ほかにもさまざまなオプションを利用できます。オプションの概要を表示するには、`ietadm -h`コマンドを実行してください。また、省略形も利用できます。省略形には、ターゲットID (tid)、セッションID (sid)、および接続ID (cid)などがあります。これらの情報は、`/proc/net/iet/session`にもあります。

12.2 iSCSIイニシエータの設定

iSCSIイニシエータ(クライアント)を使って、任意のiSCSIターゲットに接続することができます。前述したiSCSIターゲットソリューション以外への接続にも使用できます。iSCSIイニシエータの設定には、大別すると利用可能なiSCSIターゲットの検出と、iSCSIセッションのセットアップの2つのステップがあります。どちらの設定も、YaSTを使って行うことができます。

12.2.1 YaSTを使ったiSCSIイニシエータの設定

設定項目は、3つのタブに分かれています。[*Service*] タブは、ブート時にiSCSIイニシエータを有効にする場合などに使用します。固有のイニシエータ名とディスクバリエーションに使用するiSNSサーバも設定できます。iSNSのデフォルトポートは3205です。[*Connected Targets*] タブには、現在接続しているiSCSIターゲットの概要が表示されます。このタブは[*Discovered Targets*] タブのように、システムに新しいターゲットを追加するオプションが用意されています。[*Discovered Targets*] タブから設定を行います。このタブ、ネットワーク内のiSCSIターゲットを検出する場合に使用します。

- 1 [*Discovery*] は、ディスクバリエーションダイアログを表示する場合に使用します。
- 2 IPアドレスを入力し、必要に応じてポートを変更します。
- 3 必要に応じて、[*Incoming*] または [*Outgoing*] 認証を追加します。
- 4 [*次へ*] をクリックして、検出を開始します。

検出に成功したら、[*ログイン*] を使ってターゲットを有効にします。指定したiSCSIターゲットを使用するための、認証情報を要求するメッセージが表示されます。設定を完了するには、[*次へ*] をクリックします。作業が正常に完了すると、[*Connected Targets*] にターゲットが表示されます。

これで、仮想iSCSIデバイスを利用できるようになりました。実際のデバイスを探すには、`lsscsi`コマンドを使用します。

```
lsscsi
[1:0:0:0]    disk      IET          VIRTUAL-DISK    0          /dev/sda
```

12.2.2 手動によるiSCSIイニシエータの設定

iSCSI接続の検出や設定を行うには、iscsidが稼働していなければなりません。初めて検出(ディスカバリ)を実行する場合、iSCSIイニシエータの内部データベースが、/var/lib/open-iscsiディレクトリに作成されます。

ディスカバリがパスワードにより保護されている場合は、iscsidに認証情報を渡します。最初にディスカバリを実行する時には内部データベースが存在していないため、現時点でこれは使用できません。かわりに、/etc/iscsid.conf設定ファイルを編集して、情報を指定する必要があります。パスワード情報をiscsidに渡すには、/etc/iscsid.confファイルの最後に、次の行を追加します。

```
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = <username>
discovery.sendtargets.auth.password = <password>
```

ディスカバリは、受け取ったすべての値を内部データベースに保存します。また、検出したターゲットをすべて表示します。ディスカバリを実行するには、iscsiadm -m discovery --type=st --portal=<targetip>コマンドを使用します。次のような実行結果が表示されます。

```
149.44.171.99:3260,1 iqn.2006-02.com.example.iserv:systems
```

iSNSサーバで利用できるターゲットを検出するには、コマンドiscsiadm --mode discovery --type isns --portal <targetip>を使用します。

iSCSIターゲットに定義されている各ターゲットが、それぞれ1行に表示されます。保管されているデータの詳細は、[12.2.4項「iSCSIクライアントデータベース」](#) (307 ページ)を参照してください。

iscsiadmコマンドの--loginオプションを使用すると、必要なすべてのデバイスが作成されます。

```
iscsiadm -m node -n iqn.2006-02.com.example.iserv:systems --login
```

lsscsiコマンドを実行すると、新しく生成されたデバイスが表示されます。これらのデバイスをマウントして、アクセスできるようになりました。

12.2.3 iSCSIデバイスでのLVMオートアセンブリの設定

LVMスタートアップはudevでサポートされているため、必要なすべての物理ボリュームが検出されると、LVMボリュームグループはudevによって自動的に有効になります。

udevのLVMオートアセンブリはudevヘルパープログラムcollectを使用します。このプログラムは、最初の引数としてチェック対象の抽象IDを取り、コンポーネントIDのリストがこれに続きます。このプログラムがコンポーネントIDを最初の引数として呼び出されると、0を返します。

オートアセンブリに対して、指定されたボリュームグループの物理ボリュームUUIDは引数リストとしてcollectに登録されます。udev(またはvol_id)はデバイス上の物理ボリュームUUIDを検出できるため、最初の引数としてcollectに渡すことができます。

collectがすべての物理ボリュームUUIDで呼び出されたとき(udevがすべてのコンポーネントデバイスのイベントを受信したとき)、次のルールがトリガされ、vgchange -a y <vgname>を呼び出し、ボリュームグループは有効になります。

設定方法

スクリプト/usr/share/doc/packages/lvm2/lvm-vg-to-udev-rules.shを使用します。引数として、自動的に起動したいボリュームグループを指定します。このスクリプトは必要なudevルールを生成します。iSCSIを再起動して、ボリュームグループを有効にします。ブート時にアレイを自動的に起動する場合は、iSCSIコンポーネントデバイスを自動的に切り替え、イニシエータがターゲットをブート時に自動的にログに記録するようにします。

12.2.4 iSCSIクライアントデータベース

iSCSIイニシエータが検出した情報は、`/var/lib/open-iscsi`に格納されている2つのデータベースファイルに保管されます。1つは、ディスクバリが検出したターゲット用のデータベースで、もう1つは検出したノード用のデータベースです。データベースにアクセスする場合、まずデータをディスクバリ用データベースから取得するのか、またはノードデータベースから取得するのかを指定する必要があります。指定するには、`iscsiadm`コマンドの`-m discovery`または`-m node`パラメータを使用します。`iscsiadm`コマンドに、どちらかのパラメータを指定して実行すると、そのデータベースに保管されているレコードの概要が表示されます。

```
iscsiadm -m discovery
149.44.171.99:3260,1 iqn.2006-02.com.example.iserv:systems
```

この例のターゲット名は`iqn.2006-02.com.example.iserv:systems`です。このデータセットに関連する操作を行う場合に、この名前が必要になります。ID `iqn.2006-02.com.example.iserv:systems`のデータレコードのコンテンツを調べるには、次のコマンドを使用します。

```
iscsiadm -m node --targetname iqn.2006-02.com.example.iserv:systems
node.name = iqn.2006-02.com.example.iserv:systems
node.transport_name = tcp
node.tpgt = 1
node.active_conn = 1
node.startup = manual
node.session.initial_cmds_n = 0
node.session.reopen_max = 32
node.session.auth.authmethod = CHAP
node.session.auth.username = joe
node.session.auth.password = *****
node.session.auth.username_in = <empty>
node.session.auth.password_in = <empty>
node.session.timeo.replacement_timeout = 0
node.session.err_timeo.abort_timeout = 10
node.session.err_timeo.reset_timeout = 30
node.session.iscsi.InitialR2T = No
node.session.iscsi.ImmediateData = Yes
....
```

これらの変数の値を変更する場合は、`iscsiadm`コマンドで`update`オプションを使用します。たとえば、初期化時に`iscid`をiSCSIターゲットにログインさせる場合は、値に`automatic`と`node.startup`を設定します。

```
iscsiadm -m node -n iqn.2006-02.com.example.iserv:systems --op=update
--name=node.startup --value=automatic
```

不要になったデータセットを削除する場合は、`delete`を使用します。ターゲット`iqn.2006-02.com.example.iserv:systems`が有効なレコードでなくなった場合は、このレコードをコマンド`iscsiadm -m node -n iqn.2006-02.com.example.iserv:systems --op=delete`で削除します。このオプションでは、確認のメッセージを表示せずにレコードを削除するため、使用する際には細心の注意を払うようにしてください。

検出されたすべてのターゲットのリストを取得するには、コマンド`iscsiadm -m node`を実行します。

12.2.5 詳細情報

iSCSIプロトコルは、数年に渡って利用されています。そのため、iSCSIとSANソリューションの比較、ベンチマークテスト、ハードウェアソリューションの解説など、さまざまなレビューや参考資料が発表または公開されています。`open-iscsi`の詳細に関する代表的なサイトを以下に示します。

- <http://www.open-iscsi.org/>
- <http://www.open-iscsi.org/cgi-bin/wiki.pl>
- <http://www.novell.com/coolsolutions/appnote/15394.html>

このほか、オンラインマニュアルも利用できます。`iscsiadm`、`iscsid`、`ietd.conf`、および`ietd`のマニュアルページ、およびサンプルの環境設定ファイルの`/etc/iscsid.conf`などを参照してください。

Linux向けiSNSの概要

ストレージエリアネットワーク(SAN)には、複数のネットワークにまたがる多数のディスクドライブを使用できます。これによって、デバイス検出とデバイスの所有権の判定が難しくなります。iSCSIイニシエータはSANのストレージリソースを識別し、どれにアクセスできるか判定する必要があります。

インターネットストレージ名サービス(iSNS)は標準ベースのサービスで、SUSE Linux Enterprise Server (SLES) 10サポートパック2で利用できます。iSNSでは、TCP/IPネットワーク上のiSCSIデバイスのディスカバリ、管理、設定を自動化します。iSNSでは、ファイバチャネルネットワークと同等の知的なストレージディスカバリと管理サービスを提供します。

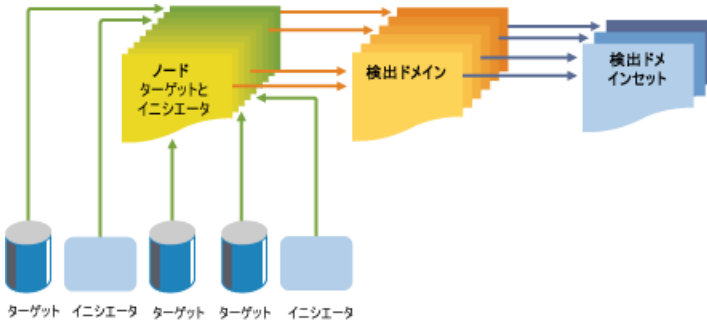
13.1 iSNSのしくみ

iSCSIイニシエータがiSCSIターゲットを検出するには、ネットワークのどのデバイスがストレージリソースで、アクセスするにはどのIPアドレスが必要かを特定する必要があります。iSNSサーバへクエリすると、iSCSIターゲットとイニシエータがアクセス許可を持つIPアドレスのリストが返されます。

iSNSを使用してiSNS検出ドメインと検出ドメインセットを作成します。次に、iSCSIターゲットとイニシエータを検出ドメインにグループ化またはまとめて、検出ドメインを検出ドメインセットにグループ化します。多くのストレージノードを複数のドメインに振り分けることで、各ホストの検出プロセスをiSNSで登録された最適なターゲットのサブセットに限定でき、これによって、不要な検出を削減し、各ホストが検出関係の確立に費やす時間を制限することで、ストレージネットワークの規模を調整できるようになります。このよ

うにして、ディスクバリ対象のターゲットとイニシエータの数を制御し、簡略化できます。

図 13.1 iSNS検出ドメインと検出ドメインセット



iSCSIターゲットとiSCSIイニシエータは、ともにiSNSクライアントを使用して、iSNSプロトコルによるiSNSサーバとのトランザクションを開始します。iSCSIターゲットとiSCSIイニシエータは、次にデバイス属性情報を共通検出ドメインに登録し、その他の登録されたクライアント情報をダウンロードし、検出ドメインで発生したイベントの非同期通知を受け取ります。

iSNSサーバは、iSNSプロトコルクエリとiSNSクライアントがiSNSプロトコルを使用して作成した要求に応答します。iSNSサーバはiSNSプロトコル状態変更通知を開始し、登録要求から送られてきた適切に認証された情報をiSNSデータベースに保存します。

Linux向けiSNSには、次のようなメリットがあります。

- ネットワーク接続させたストレージ資産の登録、検出、管理に役立つ情報を提供する。
- DNSインフラストラクチャと統合する。
- iSCSIストレージの登録、検出、管理を統合する。
- ストレージ管理の実装が簡素化される。
- その他のディスクバリ方法よりもスケーラビリティが向上する。

次のシナリオは、iSNSのメリットについて具体的に説明したものです。

100個のiSCSIイニシエータと100個のiSCSIターゲットが会社にあるとします。設定によっては、すべてのiSCSIイニシエータが100個のiSCSIターゲットを検出して接続しようとする可能性があります。これによって、検出と接続が大きな負荷になります。イニシエータとターゲットをいくつかの検出ドメインにグループ化することで、ある部門のiSCSIイニシエータが別の部門のiSCSIターゲットを検出しないようにできます。その結果、各部門のiSCSIイニシエータはその部門の検出ドメインに属すiSCSIターゲットのみを検出します。

13.2 Linux向けiSCSIのインストールとセットアップ

Linux向けiSCSIはSLES 10 SP2に付属していますが、デフォルトではインストールも設定もされていません。使用するには、iSNSパッケージモジュール(isnsおよびyast2-isnsモジュール)をインストールして、iSNSを設定する必要があります。

注意

iSNSはiSCSIターゲットまたはイニシエータと同じサーバにインストールできます。iSCSIターゲットとイニシエータを同じマシン上で使用することはサポートされていません。

Linux向けiSNSをインストールするには、次の手順に従います。

- 1 YaSTを起動して、`[ソフトウェア管理]` を選択します。
- 2 `[検索]` フィールドに「isns」と入力します。
- 3 isnsとyast2-isnsパッケージの両方を選択して、`[了解]` をクリックします。

13.3 iSNSの設定

iSNSはサーバで起動する必要があります。インストールしたときにサーバコンソールで`rcisns start`または`/etc/init.d/isns start`と入力すると実行できます。iSNSでは、`stop`、`status`、`restart`オプションも使用できます。

iSNSはサーバの再起動時に自動的に起動するように設定することもできます。
操作

- 1 YaSTを起動して、[ネットワークサービス] で [iSNSサーバ] を選択します。
- 2 [サービス] タブを選択して、iSNSサーバのIPアドレスを指定して、[SaveAddress] を選択します。
- 3 画面の [サービスの開始] セクションで、[ブート時] を選択します。

iSNSサーバを手動で起動することもできます。この場合、`rcisns start`コマンドを使用して、サーバを再起動するときにサービスを毎回起動する必要があります。

13.3.1 iSNS検出ドメインの作成

iSCSIイニシエータおよびターゲットでiSNSサービスを使用するには、これらが検出ドメインに属している必要があります。iSNSサービスをインストールすると、デフォルト*DD*というデフォルトの検出ドメインが自動的に作成されます。iSNSを使用するように設定されている既存のiSCSIターゲットとイニシエータは、デフォルト検出ドメインに自動的に追加されます。

新しい検出ドメインを作成するには、次の手順に従います。

- 1 YaSTを起動して、[ネットワークサービス] で [iSNSサーバ] を選択します。
- 2 [検出ドメイン] タブをクリックして、[Create Discovery Domain] ボタンをクリックします。

既存の検出ドメインを選択して [削除] ボタンをクリックして、その検出ドメインを削除できます。

- 3 作成している検出ドメインの名前を指定して、[OK] をクリックします。

13.3.2 iSNS検出ドメインセットの作成

検出ドメインは検出ドメインセットに属している必要があります。検出ドメインを作成してこの検出ドメインにノードを追加できますが、これはアクティブではないため、iSNSサービスは検出ドメインを検出ドメインセットに追加するまで機能しません。iSNSをインストールすると、デフォルト*DDS*というデフォルトの検出ドメインセットが自動的に作成され、デフォルトの検出ドメインは自動的にこのドメインセットに追加されます。

検出ドメインセットを作成するには、次の手順に従います。

- 1 YaSTを起動して、[ネットワークサービス] で [*iSNS*サーバ] を選択します。
- 2 [検出ドメインセット] タブをクリックして、[*Create Discovery Domain Set*] ボタンをクリックします。

既存の検出ドメインセットを選択して [削除] ボタンをクリックして、その検出ドメインセットを削除できます。

- 3 作成している検出ドメインセットの名前を指定して、[OK] をクリックします。

13.3.3 iSCSIノードの検出ドメインへの追加

- 1 YaSTを起動して、[ネットワークサービス] で [*iSNS*サーバ] を選択します。
- 2 [*iSCSI*ノード] タブをクリックして、iSNSサービスを使用するiSCSIターゲットとイニシエータが表示されていることを確認します。

iSCSIターゲットまたはイニシエータが一覧にない場合、ノード上のiSCSIサービスを再起動する必要があります。これは、`rcopen-iscsi restart`コマンドを実行してイニシエータを再起動するか、または `rciscsitarget restart`コマンドでターゲットを再起動して実行します。

iSCSIノードを選択して [削除] ボタンをクリックして、そのノードをiSNSデータベースから削除できます。iSCSIノードをもう使用しない場合や名前を変更した場合に有効です。

iSCSIノードは、iSCSIサービスを再起動したとき、またはサーバを再起動したときに、iSCSI環境設定ファイルのiSNSの部分削除したりコメント化していない限り、リスト(iSNSデータベース)に再度追加されます。

- 3 [検出ドメイン] タブをクリックして該当する検出ドメインを選択し、[メンバーの表示] ボタンをクリックします。
- 4 [Add existing iSCSI Node] をクリックしてドメインに追加するノードを選択し、[ノードの追加] をクリックします。
- 5 検出ドメインに追加するノードについて最後のステップを繰り返し、ノードの追加が終了したら [完了] をクリックします。

iSCSIノードは複数の検出ドメインに属することができます。

13.3.4 検出ドメインの検出ドメインセットへの追加

- 1 YaSTを起動して、[ネットワークサービス] で [iSNSサーバ] を選択します。
- 2 [検出ドメインセット] タブをクリックします。
- 3 [Create Discovery Domain Set] を選択して、新しいセットを検出ドメインセットのリストに追加します。
- 4 変更する検出ドメインを選択します。
- 5 [検出ドメインの追加] をクリックして検出ドメインセットに追加する検出ドメインを選択し、[検出ドメインの追加] をクリックします。
- 6 検出ドメインセットに追加する検出ドメインについて最後のステップを繰り返して、[完了] をクリックします。

検出ドメインは複数の検出ドメインセットに属することができます。

13.4 詳細情報

linuxisnsプロジェクトは<http://sourceforge.net/projects/linuxisns/>でホストされています。このプロジェクトのメーリングリストはhttp://sourceforge.net/mailarchive/forum.php?forum_name=linuxisns-discussionで参照できます。iSNSについての一般情報は、rfc4171に記載されています。<http://www.ietf.org/rfc/rfc4171>も参照してください。

Oracle Cluster File System 2

Oracle Cluster File System 2は、Linux 2.6以降のカーネルと完全に統合された、汎用のジャーナルファイルシステムです。Oracle Cluster File System 2を利用すれば、アプリケーションバイナリファイル、データファイル、およびデータベースを、SAN中のデバイスに保管することができます。このファイルシステムには、クラスタ中のすべてのノードが同時に読み書きすることができます。また、分散ロックマネージャにより、アクセスの競合を回避することができます。Oracle Cluster File System 2は、最高32,000個までのサブディレクトリ、および数百万個のファイルをサポートしています。各ノード上ではO2CBクラスタサービス(ドライバ)が動作して、クラスタを管理しています。

Oracle Real Application Cluster(RAC)データベースとそのアプリケーションファイルをサポートするため、OCFS2がSUSE Linux Enterprise Server 9に追加されました。SUSE Linux Enterprise Server 10以降では、以下のストレージソリューションでOracle Cluster File System 2を使用することができます。

- Oracle RACおよび他のデータベース
- 一般アプリケーションと負荷
- クラスタ中のXENイメージ

サーバ間でXEN仮想マシンの素早く簡単な移植性を活用するために、XEN仮想マシンおよび仮想サーバを、クラスタサーバによりマウントされたOracle Cluster File System 2ボリュームに保管することができます。

- LAMP(Linux、Apache、MySQL、およびPHP | PERL | Python)スタック

また、Heartbeat 2と完全に統合されています。

Oracle Cluster File System 2は、高性能なパラレルクラスタファイルシステムで、次の機能をサポートしています。

- クラスタ中のすべてのノードが、アプリケーションのファイルを利用することができます。ユーザは、クラスタ中のOracle Cluster File System 2ボリュームに1回インストールするだけで構いません。
- 標準のファイルシステムインタフェースを通じて、すべてのノードが並行してストレージに読み書きできるため、クラスタにまたがって稼働するアプリケーションの管理が容易になります。
- ファイルアクセスは、分散ロックマネージャ(DLM:Distributed Lock Manager)により、管理、調整されます。

ほとんどの場合、DLMによる制御は適切に機能しますが、DLMとファイルアクセスを競合するようなアプリケーションなど、アプリケーションの設計によっては、スケーラビリティが制限される可能性もあります。

- すべてのバックエンドストレージで、ストレージのバックアップ機能を利用することができます。共有アプリケーションファイルのイメージを簡単に作成することができるため、災害発生時でも素早くデータを復元することができます。

Oracle Cluster File System 2には、次の機能も用意されています。

- メタデータのキャッシュ処理
- メタデータのジャーナル処理
- ノード間にまたがるファイルデータの整合性
- ocfs2consoleユーティリティを介したGTK GUIベースの管理機能
- 共有ルートファイルシステムとしての運用
- 最大16TBまでのボリュームで、最高4KBまでの複数ブロックサイズをサポート(各ボリュームで異なるブロックサイズを使用可能)
- 255台までのクラスタノードをサポート

- ・ ノード固有のローカルファイルに対するCDSL(Context-dependent symbolic link)のサポート
- ・ データベースのパフォーマンスを向上する非同期、直接I/Oのサポート

14.1 Oracle Cluster File System 2 クラスタサービス

Oracle Cluster File System 2 クラスタサービスは、OCFS2サービス/ボリュームを管理するために必要な、一連のモジュールとメモリ内ファイルシステムです。これらのモジュールは、システムブート時にロード、マウントすることができます。方法については、[14.6.2項「OCFS2サービスの設定」](#) (325 ページ)を参照してください。

表 14.1 Oracle Cluster File System 2 クラスタサービススタック

サービス	説明
Node Manager (NM)	/etc/ocfs2/cluster.confファイル中のすべてのノードを追跡します。
Heartbeat (HB)	ノードがクラスタに参加/退席した時に稼働/非稼働を通知する信号を送信します。
TCP	ノード間のTCPプロトコルを使った通信を処理します。
分散ロックマネージャ (DLM:Distributed Lock Manager)	すべてのロック、およびその所有者とステータスを追跡します。
CONFIGFS	ユーザスペース設定ファイルシステム。詳細については、 14.3項「内部メモリファイルシステム」 (321 ページ)を参照してください。
DLMFS	カーネルスペースDLMへのユーザスペースインタフェース。詳細については、 14.3項「内部メモ

[リファイルシステム」](#) (321 ページ)を参照してください。

14.2 ディスクハートビート

Oracle Cluster File System 2を利用するには、ネットワーク上のノードが稼働していなければなりません。O2CBクラスタサービスは、正常に稼働していることを確認するために、定期的にキープアライブパケットを送信します。ネットワーク遅延が発生すると、ノードがダウンしたと判断される可能性があるため、パケットの送信にはLANの代わりにノード間のプライベートな接続を使用しています。

OC2Bクラスタサービスは、ディスクハートビートを介してノードステータスをやり取りします。ハートビートシステムファイルは、クラスタ中のすべてのノードが利用できるSAN(ストレージエリアネットワーク)上に常駐しています。このファイル中のブロック割り当ては、各ノードのスロット割り当てに順番に対応しています。

各ノードは2秒間隔でファイルを読み込み、それをファイル中の割り当てられたブロックに書き込みます。ノードのタイムスタンプの変更により、そのノードが稼働していることが分かります。一定時間ハートビートファイルに書き込みがない場合、そのノードは停止しているとみなされます。この時間は、書き込み間隔数で表されるハートビートしきい値として設定します。単一のノードだけが動作している場合でも、他のノードが動的に追加される可能性があるため、O2CBクラスタサービスはこのチェックを行います。

ディスクハートビートのしきい値を変更するには、`/etc/sysconfig/o2cb` ファイルのO2CB_HEARTBEAT_THRESHOLDパラメータを使用します。このしきい値の時間は以下のように算出されます。

```
(O2CB_HEARTBEAT_THRESHOLD value - 1) * 2 = threshold in seconds
```

たとえば、O2CB_HEARTBEAT_THRESHOLDにデフォルト値の7が設定されている場合、時間は12秒になります $((7 - 1) * 2 = 12)$ 。

14.3 内部メモリファイルシステム

Oracle Cluster File System 2は、通信用に2つのメモリ内ファイルシステムを使用しています。

表 14.2 Oracle Cluster File System 2が使用するメモリ内ファイルシステム

内部メモリ ファイルシ ステム	説明	マウントポイ ント
configfs	クラスタ中のノードリストをカーネル内ノードマネージャに、そしてハートビートで使われるリソースをカーネル内ハートビートスレッドに通知します。	/config
ocfs2_dlmfs	クラスタ内のリソースに対するロック/ロック解除ステータスを、ロックの所有者とステータスを追跡するカーネル内分散ロックマネージャに通知します。	/dlm

14.4 管理ユーティリティとコマンド

OCFS2はノード固有のパラメータファイルをノードに保存します。このクラスタ設定ファイル(/etc/ocfs2/cluster.conf)は、クラスタに割り当てられた各ノード上にあります。

ocfs2consoleユーティリティは、クラスタ中のOracle Cluster File System 2の環境設定を管理するための、GTK GUIベースのインタフェースです。クラスタ中の各メンバノードの/etc/ocfs2/cluster.confファイルの設定と保存には、このユーティリティを使用します。また、このユーティリティを使ってOCFS2ボリュームの、フォーマット、チューニング、マウント、およびアンマウントなどの作業を行うこともできます。

重要項目

ocfs2consoleユーティリティのファイルブラウザ列は、非常に遅く、クラスター間で整合性がありません。ファイルを表示する場合は、代わりに**ls(1)**コマンドを使用することをお勧めします。

他のOCFS2ユーティリティを以下の表に示します。これらのコマンドの指定形式については、マニュアルページを参照してください。

表 14.3 OCFS2ユーティリティ

OCFS2ユーティリティ	説明
debugfs.ocfs2	デバッグの目的で、Oracle Cluster File System 2のファイルシステムの状態を調査します。
fsck.ocfs2	ファイルシステムにエラーがないかをチェックし、必要に応じてエラーを修復します。
mkfs.ocfs2	デバイス上にOCFS2ファイルシステムを作成します。通常は、共有物理/論理ディスク上のパーティションに作成します。このツールを利用するには、O2CBクラスタサービスが稼働していなければなりません。
mounted.ocfs2	クラスタシステム上のすべてのOCFS2ボリュームを検出、表示します。OCFS2デバイスをマウントしているシステム上のすべてのノードを検出、表示するか、またはすべてのOCFS2デバイスを表示します。
ocfs2cdsl	ノードに対して、特定のファイル名(ファイルまたはディレクトリ)のCDSLを作成します。CDSLファイル名は特定のノードに対する独自のイメージを持っていますが、一般名はOCFS2中に保管されます。
tune.ocfs2	ボリュームラベル、ノードスロット数、すべてのノードスロットのジャーナルサイズ、およびボリュームサイズなど、OCFS2ファイルのシステムパラメータを変更します。

O2CBサービスを管理するには、以下のコマンドを使用します。o2cbコマンドの詳細や指定形式については、該当するマニュアルページを参照してください。

表 14.4 O2CBのコマンド

コマンド	説明
/etc/init.d/o2cb status	O2CBサービスがロードされ、マウントされているかどうかをレポートします。
/etc/init.d/o2cb load	O2CBモジュールとメモリ内ファイルシステムをロードします。
/etc/init.d/o2cb online ocfs2	ocfs2という名前のクラスタがオンラインになります。 クラスタをオンラインにするには、クラスタ中の1つ以上のノードをアクティブにしていなければなりません。
/etc/init.d/o2cb offline ocfs2	ocfs2という名前のクラスタがオフラインになります
/etc/init.d/o2cb unload	O2CBモジュールとメモリ内ファイルシステムをアンロードします。
/etc/init.d/o2cb start ocfs2	ブート時にロードするようにクラスタが設定されている場合、o2cbをロードして、「ocfs2」の部分に指定された名前を持つクラスタをオンラインにし、クラスタを起動します。 クラスタをオンラインにするには、クラスタ中の1つ以上のノードをアクティブにしていなければなりません。
/etc/init.d/o2cb stop ocfs2	ブート時にロードするようにクラスタが設定されている場合に、「ocfs2」の部分に指定された名前を持

コマンド	説明
	つクラスタをオフラインにして、O2CBモジュールとメモリ内ファイルシステムをアンロードします。

14.5 OCFS2のパッケージ

SUSE Linux Enterprise Server 10以降では、OCFS2カーネルモジュール(`ocfs2`)は自動的にインストールされます。OCFS2を使用するには、YaST(またはコマンドライン)を使って`ocfs2-tools`と`ocfs2console`パッケージを、クラスタ中の各ノードにインストールします。

- 1 `root`としてログインし、YaSTコントロールセンタを起動します。
- 2 [ソフトウェア] > [ソフトウェア管理] の順に選択します。
- 3 [検索] フィールドに、以下の文字列を入力します。 `ocfs2`。

右側のパネルに、`ocfs2-tools`と`ocfs2console`のソフトウェアパッケージが表示されます。これらのパッケージが選択されている場合、すでにこれらのパッケージはインストールされています。

- 4 パッケージをインストールするには、該当するパッケージを選択した後 [インストール] をクリックして、以降画面に表示される指示に従って作業を行います。

14.6 OCFS2ボリュームの作成

ここでは、OCFS2ボリュームの作成方法、およびOCFS2を使用するためのシステムの設定方法について説明していきます。

14.6.1 前提条件

まず、次の作業を行ってください。

- 必要に応じてSANディスク上のRAID(Redundant Array of Independent Disks)を初期化、設定し、OCFS2ボリュームで使用するデバイスを準備します。デバイスには、空き領域を残してください。

アプリケーションファイルとデータファイルは、異なるOCFS2ボリュームに保管することをお勧めします。アプリケーション用ボリュームとデータ用ボリュームでマウントの要件が異なる場合は、必ずそうしてください。たとえば、Oracle RACデータベースボリュームには、マウントオプション `datavolume` と `nointr` が必要になりますが、Oracle Home ボリュームではこれらのオプションは使われません。

- `ocfs2console` および `ocfs2-tools` パッケージがインストールされていることを確認してください。これらのパッケージがインストールされていない場合は、YaST または コマンドライン を使ってインストールします。YaST を使ったインストール方法については、[14.5 項 「OCFS2 のパッケージ」](#) (324 ページ) を参照してください。

14.6.2 OCFS2 サービスの設定

OCFS2 ボリュームを作成する前に、OCFS2 サービスを設定する必要があります。ここでは、`/etc/ocfs2/cluster.conf` ファイルを生成し、すべてのノード上に `cluster.conf` ファイルを保存し、O2CB クラスタ サービス(`o2cb`)を作成、開始する手順を説明していきます。

クラスタ中の1台のノードに対して、以下の作業を行います。

- 1 ターミナルウィンドウを開いて、`root` ユーザとしてログインします。
- 2 `o2cb` クラスタ サービスがまだ有効になっていない場合は、`chkconfig -- add o2cb` を入力します。

新しくサービスを追加する場合、`chkconfig` でランレベルを表示、設定、変更することができます。

- 3 `ocfs2` サービスがまだ有効になっていない場合は、`chkconfig --add o2cfs2` を入力します。
- 4 `o2cb` クラスタ サービスドライバを、ブート時にロードするように設定します。

4a `/etc/init.d/o2cb configure`と入力します。

4b `[Load O2CB driver on boot (y/n) [n]]` プロンプトで、「y (はい)」と入力してブート時のロードを有効にします。

4c `[Cluster to start on boot (Enter "none" to clear) [ocfs2]]` というメッセージが表示されたら、「none」と入力します。この場合、**OCFS2**を初めて設定しているか、サービスをリセットしていると仮定されます。次のステップで`/etc/ocfs2/cluster.conf`ファイルを設定する際に、クラスタ名を指定します。

- 5** `ocfs2console`ユーティリティを使用して、`/etc/ocfs2/cluster.conf`ファイルをクラスタ内の各メンバノードに設定して保存します。

クラスタ中のすべてのノードで、このファイルの内容は同じでなければなりません。最初のノードにファイルを設定するには、以下の手順に従ってください。後で、`ocfs2console`を使って新しいノードをクラスタに動的に追加して、変更した`cluster.conf`ファイルをすべてのノードに反映することができます。

ただし、クラスタ名やIPアドレスなどの他の設定を変更した場合は、変更内容を有効にするために、**ステップ 6** (327 ページ)の説明に従ってクラスタを再起動する必要があります。

5a `ocfs2console GUI`を`ocfs2console`と入力して起動します。

5b `ocfs2console`で、`[Cluster] > [Cluster Nodes]` の順に選択します。

`cluster.conf`が存在していない場合は、デフォルトのクラスタ名 `ocfs2` を使ってファイルが作成されます。必要に応じてクラスタ名を変更してください。

5c `[Node Configuration]` ダイアログボックスで、`[Add]` をクリックして、`[Add Node]` ダイアログボックスを表示します。

- 5d** **[AddNode]** ダイアログボックスで、プライマリノード用の一意の名前、一意のIPアドレス(例:192.168.1.1)、およびポート番号(オプション、デフォルトは7777)を入力し、**[OK]** をクリックします。

ocfs2consoleコンソールは、0～254の順番にノードスロット番号を割り当てます。

- 5e** **[Node Configuration]** ダイアログボックスで、**[Apply]** をクリックした後、**[Close]** をクリックして、**[AddNode]** ダイアログボックスを閉じます。

- 5f** **[Cluster]** > **[Propagate Configuration]** の順にクリックして、cluster.confファイルをすべてのノードに保存します。

- 6** 変更内容を有効にするために、OCFS2クラスタを再起動する場合、以下の行を入力して、プロセスのステータスが **[OK]** に戻るまで待ってください。

```
/etc/init.d/o2cb stop  
/etc/init.d/o2cb start
```

14.6.3 OCFS2ボリュームの作成

OCFS2ファイルシステムを作成してクラスタに新しいノードを追加する作業は、クラスタ中の1台のノードに対してのみ行います。

- 1** ターミナルウィンドウを開いて、rootユーザとしてログインします。
- 2** O2CBクラスタサービスがオフラインの場合、以下のコマンドを入力し、プロセスのステータスが **[OK]** に戻るまで待ちます。

```
/etc/init.d/o2cb online ocfs2
```

ここで、ocfs2には、実際のOCFS2クラスタ名を入力してください。

フォーマット操作を行う場合、まずクラスタ中のいずれのノードにもボリュームがマウントされていないことを確認する必要があるため、OCFS2クラスタはオンラインになっていなければなりません。

3 次のいずれかの方法を使って、ボリュームを作成、フォーマットします。

- EVMSGUIで [Volumes] ページに移動して、 [Make a file system] > [OCFS2] の順に選択し、適切な情報を設定します。
- mkfs.ocfs2ユーティリティを使用します。このコマンドの指定形式については、mkfs.ocfs2マニュアルページを参照してください。
- ocfs2consoleコンソールで [Tasks] > [Format] の順にクリックして、 [Available Devices] リストからOCFS2ボリュームで使用するデバイスを選択します。次に、ボリュームに関する情報を設定して、 [OK] をクリックすると、ボリュームがフォーマットされます。

推奨する設定については、次の表を参照してください。

OCFS2パラメータ	説明と推奨設定
Volume label	<p>異なるノードへのマウント時に、正しく識別できるように、一意のわかりやすいボリューム名を指定します。</p> <p>ラベルを変更するには、tunefs.ocfs2ユーティリティを使用します。</p>
Cluster size	<p>クラスタサイズは、ファイルに割り当てられる、データ保管領域の最小単位です。</p> <p>4、8、16、32、64、128、256、512、および1024KBを指定することができます。ボリュームのフォーマット後にクラスタサイズを変更することはできません。</p> <p>Oracleでは、データベースボリュームのクラスタサイズに128KB以上を指定することを推奨しています。また、Oracle Homeの場合は32KBまたは64KBを指定することも推奨しています。</p>
Number of node slots	<p>同時にボリュームをマウントできる最大ノード数を指定します。マウント時に、OCFS2は各ノードに対して、個別のシステムファイル(ジャーナルなど)を作成します。</p>

ボリュームにアクセスするノードに、リトルエンディアン形式のノード(x86、x86-64、およびia64など)とビッグエンディアン形式のノード(ppc64やs390xなど)が混在しても構いません。

ノード固有のファイルは、ローカルファイルとして参照されます。ローカルファイルには、ノードスロット番号が付加されます。たとえば、「journal:0000」は、スロット番号0が割り当てられているノードに所属します。

各ボリュームの作成時に、ボリュームと同時にマウントする予定のノード数に応じて、そのボリュームの最大ノードスロット数を指定します。必要に応じて、`tuneefs.ocfs2`ユーティリティを使って、ノードスロット数を増やすことができます。ただし、ノードスロット数を減らすことはできません。

Block size ファイルシステムがアドレス可能な領域の最小単位を指定します。ブロックサイズは、ボリュームの作成時に指定します。

512Byte(推奨されません)、1KB、2KB、または4KB(ほぼすべてのボリュームに最適)を選択することができます。ブロックサイズは、ボリュームのフォーマット後に変更することはできません。

14.7 OCFS2ボリュームのマウント

- 1 ターミナルウィンドウを開いて、rootユーザとしてログインします。
- 2 O2CBクラスタサービスがオフラインの場合、以下のコマンドを入力し、プロセスのステータスが **[OK]** に戻るまで待ちます。

```
/etc/init.d/o2cb online ocfs2
```

ここで、`ocfs2`には、実際のOCFS2クラスタ名を入力してください。

フォーマット操作を行う場合、クラスタ中のいずれのノードにもボリュームがマウントされていないことを確認する必要があるため、OCFS2クラスタはオンラインになっていなければなりません。

3 次のいずれかの方法を使って、ボリュームをマウントします。

- `ocfs2console`で、使用できるデバイスのリストからデバイスを選択し、[マウント] をクリックします。オプションでディレクトリのマウントポイントとマウントオプションを指定して、[OK] をクリックします。
- コマンドラインから、`mount`コマンドを使ってボリュームをマウントします。
- `/etc/fstab`ファイルを使って、システムブート時にボリュームをマウントします。

OCFS2ボリュームのマウントには、5秒ほどの時間がかかります。この時間は、ハートビートスレッドが安定するまでの時間によって異なります。マウントが正常に完了すると、`ocfs2console`のデバイスリストに、そのマウントポイントとデバイスが表示されます。

ティップ: 新しいノードの追加

新しいノードがクラスタに接続しようとしても、ノードは接続リストに追加されていないため、接続できません。この問題を解決するには、各ノードに手動で移動して次のコマンドを発行し、それぞれの接続リストを更新します。

```
o2cb_ctl -H -n ocfs2 -t cluster -a online=yes
```

これらの方法を使ったOCFS2ボリュームのマウントに関する詳細情報は、*OCFS2 project at Oracle* [<http://oss.oracle.com/projects/ocfs2/documentation/>]にある『OCFS2 User Guide [<http://oss.oracle.com/projects/ocfs2/>)]』を参照してください。

Oracle RACを実行する場合、CRS (Voting Diskファイル)、OCR (クラスタレジストリ)、データファイル、Redoログ、アーカイブログ、および

コントロールファイルを含むOCFS2ボリュームに対しては、`datavolume` および `nointr` マウントオプションを使用してください。Oracle Home ボリュームのマウント時には、これらのオプションを使用しないでください。

オプション	説明
<code>datavolume</code>	Oracle プロセスが、 <code>o_direct</code> フラグでファイルを開きます。
<code>nointr</code>	割り込みなし。I/O が信号により割り込まれないようにします。

14.8 追加情報

OCFS2 の使用の詳細については、*OCFS2 project at Oracle* [<http://oss.oracle.com/projects/ocfs2/documentation/>] にある『OCFS2 User Guide [<http://oss.oracle.com/projects/ocfs2/>)]』を参照してください。

Linuxのアクセス制御リスト

POSIX ACL(アクセスコントロールリスト)は、ファイルシステムオブジェクトに対する従来のパーミッション概念の拡張として使用できます。ACLを使用すれば、従来のパーミッション概念で許されていた以上のパーミッションを柔軟に定義できます。

POSIX ACLという用語は、このACLが真のPOSIX(Portable Operating System Interface)規格であることを示唆しています。ドラフト規格のPOSIX 1003.1eとPOSIX 1003.2cは、いくつかの理由で白紙に戻されました。それにもかかわらず、UNIXファミリに属している多くのシステムに見られるACLは、これらのドラフト規格に基づいており、この章で説明するファイルシステムACLの実装も同様にこの2つの規格に従っています。これらの規格については、<http://wt.xpilot.org/publications/posix.1e/>を参照してください。

15.1 従来のファイルパーミッション

従来のLinuxファイルパーミッションの基本については、**18.2項「ユーザとアクセス権」** (397 ページ)を参照してください。より高度な機能としては、setuid、setgid、およびsticky bitがあります。

15.1.1 setuidビット

特定の状況では、アクセス権の制約が強すぎる場合があります。したがって、Linuxは、特定のアクションが実行できるように、現在のユーザとグループのID(身分とその権限)を一時的に変更できるようにする追加の設定項目を用意し

ています。たとえば、passwdプログラムでは、一般に/etc/passwdにアクセスする際にrootユーザのパーミッションが必要です。このファイルには、ユーザのホームディレクトリ、ユーザとグループのIDなどの重要情報が含まれます。したがって、このファイルへのアクセスをすべてのユーザに許可することは危険が大きいのので、一般ユーザはpasswdを変更できません。setuidを使用すれば、この問題を解決することができます。setuid (ユーザIDの設定) は、特定のユーザIDでマークされたプログラムの実行をシステムに指示するための特殊なファイル属性です。次のpasswdコマンドを参照してください。

```
-rwsr-xr-x  1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

sという文字が表示されていて、ユーザパーミッションでsetuidビットがセットされていることを示しています。setuidビットによって、passwdコマンドを実行するすべてのユーザは、rootで実行できます。

15.1.2 setgidビット

setuidビットはユーザに適用されます。ただし、グループにもsetgidビットという同等のプロパティがあります。この属性がセットされているプログラムは、どのユーザがそのプログラムを起動したかにかかわらず、そのプログラムと共に保存されているグループIDを使用して動作します。したがって、setgidビットがオンになっているディレクトリ内では、新しく作成されるすべてのファイルとサブディレクトリは、そのディレクトリが所属しているグループに対して割り当てられます。次のサンプルディレクトリについて考えてみます。

```
drwxrws---  2 tux archive 48 Nov 19 17:12  backup
```

sという文字が表示されていて、グループパーミッションでsetgidビットがセットされていることを示しています。ディレクトリの所有者とarchiveグループのメンバは、このディレクトリにアクセスできます。このグループのメンバでないユーザは、それぞれ適切なグループに「マップ」されます。すべての書き込みファイルの有効なグループIDは、archiveになります。たとえば、グループIDarchiveで実行されるバックアッププログラムは、ルート権限なしにこのディレクトリにアクセスできます。

15.1.3 sticky(スティッキー)ビット

sticky(スティッキー)ビットもあります。このビットは、実行可能プログラムとディレクトリのどちらに所属しているかにより意味が異なります。このビットがプログラムに所属している場合、このようにマークが付けられたファイルは、使用するたびにハードディスクにアクセスする必要がないようにRAMにロードされます。現在のハードディスクは十分高速なので、この属性はほとんど使用されなくなっています。このビットをディレクトリに割り当てた場合、各ユーザが他のユーザのファイルを削除することが防止されます。一般的な使用例として、/tmpと/var/tmpの各ディレクトリを挙げることができます。

```
drwxrwxrwt 2 root root 1160 2002-11-19 17:15 /tmp
```

15.2 ACLの利点

従来どおり、Linuxシステムのファイルオブジェクトごとに3セットのパーミッションが定義されます。この3セットには、読み取り(r)、書き込み(w)、実行(x)の各パーミッションがあり、それぞれが3種類のユーザ(ファイル所有者、グループ、その他のユーザ)ごとに設定されます。そのほかに、ユーザID設定ビット、グループID設定ビット、スティッキービットを設定できます。この無駄のない概念は、ほとんどの実際的なケースに十分適しています。ただし、複雑なシナリオまたは高度なアプリケーションの場合、以前は、システム管理者が従来のパーミッション概念の制限を回避するために多くの仕掛けを施す必要がありました。

ACLは、従来のファイルパーミッション概念の拡張として使用できます。ACLを使用すれば、パーミッションが元の所有者や所有者の所属グループに対応していない場合でも個々のユーザまたはグループにそうしたパーミッションを割り当てることができます。アクセス制御リストは、Linuxカーネルの機能であり、現在ReiserFS、Ext2、Ext3、JFS、およびXFSでサポートされています。ACLを使用すると、アプリケーションレベルで複雑なパーミッションモデルを実装しなくても複雑なシナリオを実現できます。

ACLの利点は、WindowsサーバをLinuxサーバに置き換える場合にはっきりします。接続した一部のワークステーションは、移行後も引き続きWindowsの下で動作できます。Linuxシステムは、Sambaを搭載したWindowsクライアントにファイルサービスと印刷サービスを提供します。Sambaがアクセス制御

リストをサポートしている場合は、LinuxサーバおよびWindows(Windows NT以降のみ)のどちらでもグラフィカルユーザインタフェースでユーザパーミッションを設定できます。Sambaスイートの一部であるwinbinddを使用すれば、Linuxサーバ上にアカウントのない、Windowsドメインにしか存在していないユーザにパーミッションを割り当てることができます。

15.3 定義

ユーザクラス

従来のPOSIXパーミッションの概念では、ファイルシステムのパーミッションをユーザに割り当てるために、所有者、所有者の所属グループ、および他のユーザの、3種類のクラスを使用しています。読み取り(r)、書き込み(w)、および実行(x)を可能にする3つのパーミッションビットは、ユーザクラスごとに設定できます。

アクセスACL

あらゆる種類のファイルシステムオブジェクト(ファイルやディレクトリ)のユーザアクセスパーミッションとグループアクセスパーミッションは、アクセスACLによって決定されます。

デフォルトACL

デフォルトACLは、ディレクトリにしか適用できません。このACLでは、ファイルシステムオブジェクトが作成されたときにその親ディレクトリから継承するパーミッションが決定されます。

ACLエントリ

各ACLは、ACLエントリセットから成ります。ACLエントリには、タイプ、エントリが参照するユーザまたはグループのクォリファイア、およびパーミッションセットが含まれます。一部のエントリタイプの場合、グループまたはユーザのクォリファイアは定義されていません。

15.4 ACLの処理

表15.1. 「ACLエントリタイプ」(337ページ)に、考えられる6つのACLエントリタイプをまとめています。各エントリで、ユーザまたはユーザグループのパーミッションが定義されます。所有者エントリでは、ファイルまたはディレクトリを所有しているユーザのパーミッションが定義されます。所有者の

所属グループエントリでは、ファイルの所有者の所属グループのパーミッションが定義されます。スーパーユーザは、chownまたはchgrpを使用して所有者または所有者の所属グループを変更できます。その場合、所有者と所有者の所属グループエントリは、新しい所有者と所有者の所属グループを参照します。各名前付きユーザエントリでは、エントリのクォリファイアフィールドで指定されたユーザのパーミッションが定義されます。各名前付きグループエントリでは、エントリのクォリファイアフィールドで指定されたグループのパーミッションが定義されます。名前付きユーザと名前付きグループのエントリのクォリファイアフィールドだけが指定されます。その他のエントリでは、他のすべてのユーザのパーミッションが定義されます。

マスクエントリでは、名前付きユーザ、名前付きグループ、および所有者の所属グループのエントリで与えられたパーミッションをさらに制限するために、それらのエントリのパーミッションのどれが有効で、どれをマスクするかが定義されます。パーミッションは、マスク内と同様にこのいずれかのエントリ内にも存在する場合に有効です。マスクだけまたは実際のエントリだけに指定されているパーミッションは有効ではありません。つまり、パーミッションは与えられません。所有者と所有者の所属グループのエントリで定義されているすべてのパーミッションは常に有効です。表 15.2. 「アクセスパーミッションのマスキング」 (338 ページ) の例に、このメカニズムを示しています。

ACLには、2つの基本クラスがあります。最小ACLには、所有者、所有者の所属グループ、およびその他というタイプのエントリだけが含まれます。これらのエントリは、ファイルやディレクトリの従来のパーミッションビットに対応しています。拡張ACLは、このACLを越えるものです。このACLには、マスクエントリが必ず含まれ、名前付きユーザと名前付きグループのタイプのエントリがいくつか含まれている場合があります。

表 15.1 ACL エントリタイプ

タイプ	テキスト書式
owner	user::rwx
名前付きユーザ	user:name:rwx
所有者の所属グループ	group::rwx

タイプ	テキスト書式
名前付きグループ	group:name:rwX
マスク	mask::rwX
その他	other::rwX

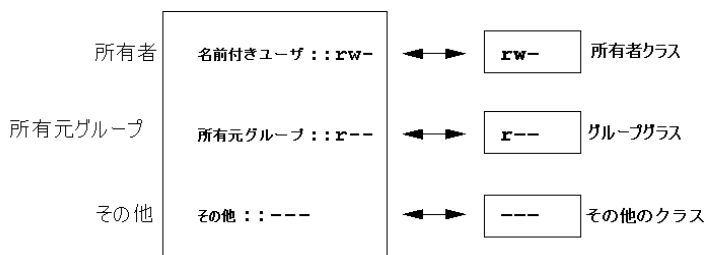
表 15.2 アクセスパーミッションのマスキング

エントリタイプ	テキスト書式	パーミッション
名前付きユーザ	user:geeko:r-x	r-x
マスク	mask::rw-	rw-
	有効なパーミッション:	r--

15.4.1 ACLエントリとファイルモードのパーミッションビット

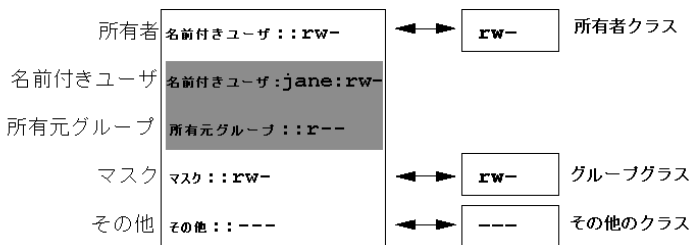
図 15.1. 「最小ACL:ACLエントリとパーミッションビットの比較」 (339 ページ)と図 15.2. 「拡張ACL:ACLエントリとパーミッションビットの比較」 (339 ページ)に、最小ACLと拡張ACLの2つのケースを示します。図は、3つのブロックから成ります。左側のブロックはACLエントリのタイプを示し、中央のブロックはACLの例を示しています。右側のブロックは、従来のパーミッション概念に基くそれぞれのパーミッションビット(1s-1などで表示される)を示します。どちらのケースも、所有者クラスのパーミッションは、ACLエントリ所有者に割り当てられます。その他のクラスのパーミッションは、それぞれのACLエントリに割り当てられます。しかし、グループクラスのパーミッションの割り当ては、2つのケースで異なります。

図 15.1 最小ACL:ACLエントリとパーミッションビットの比較



最小ACL(マスクなし)の場合、グループクラスのパーミッションがACLエントリ所有者の所属グループにマッピングされます。これを図15.1.「最小ACL:ACLエントリとパーミッションビットの比較」(339ページ)に示します。拡張ACL(マスクあり)の場合、グループクラスのパーミッションがマスクエントリにマップされます。これを図15.2.「拡張ACL:ACLエントリとパーミッションビットの比較」(339ページ)に示します。

図 15.2 拡張ACL:ACLエントリとパーミッションビットの比較



この割り当て方法により、アプリケーションがACLをサポートしているかどうかにかかわらず、アプリケーションとのスムーズなインタラクションができます。パーミッションビットによって割り当てられたアクセスパーミッションは、ACLで他のすべてのパーミッションを「微調整」する場合の上限を表します。パーミッションビットの変更は、ACLに反映されます。その逆も同様です。

15.4.2 アクセスACLが設定されたディレクトリ

コマンドラインに`getfacl`および`setfacl`を指定すると、ACLにアクセスできます。これらのコマンドの使用法については次の例に示します。

ディレクトリを作成する前に、`umask`コマンドを使用して、ファイルオブジェクトを作成するたびにどのアクセスパーミッションをマスクする必要があるかを定義します。`umask027`コマンドでは、デフォルトパーミッションを設定するために、所有者にすべてのパーミッションを与え(0)、グループ書き込みアクセスを拒否して(2)、その他のユーザにはパーミッションを与えません(7)。実際に、`umask`は対応するパーミッションビットをマスクするか、またはそのビットをオフにします。詳細については、対応する `umaskman` ページを参照してください。

`mkdir mydir`は、`umask`で設定されたデフォルトパーミッションで`mydir`ディレクトリを作成します。`ls -dl mydir`を使用して、すべてのパーミッションが正しく割り当てられたかどうかをチェックします。このコマンドの出力例は、次のとおりです。

```
drwxr-x--- ... tux project3 ... mydir
```

`getfacl mydir`では、ACLの初期状態をチェックします。このコマンドでは、次のような情報が得られます。

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

最初の3つの出力行には、名前、所有者、およびディレクトリの所有者の所属グループが表示されています。次の3行には、所有者、所有者の所属グループ、およびその他という3つのACLエントリが表示されています。実際には、この最小ACLの場合、`getfacl`コマンドでは`ls`で取得できなかった情報は生成されません。

読み取り、書き込み、実行の各パーミッションをさらにユーザ`geeko`とグループ`mascoats`に割り当てるには、次のようにします。

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

オプション-mを指定すると、setfaclに対して既存のACLの変更が求められます。このオプションの後の引き数は、変更するACLエントリを示します(複数のエントリはカンマで区切られます)。最後の部分には、こうした変更を適用するディレクトリの名前を指定します。設定されたACLを確認するには、getfaclコマンドを使用します。

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

ユーザgeekoとグループmascots向けのエントリのほかに、マスクエントリが生成されました。このマスクエントリは、すべてのパーミッションを有効にするように、自動的に設定されます。setfaclは、既存のマスクエントリを変更された設定に応じて自動的に適合させます(-nでこの機能が無効にしている場合を除く)。マスクは、グループクラス中のすべてのエントリに対して有効なアクセスパーミッションの最大数を定義します。こうしたエントリには、名前付きユーザ、名前付きグループ、および所有者の所属グループがあります。ls-dl mydirで表示されたグループクラスのパーミッションビットは、maskエントリに対応しています。

```
drwxrwx---+ ... tux project3 ... mydir
```

出力の最初のカラムには、この項目に拡張ACLがあることを示すためにさらに+が表示されます。

lsコマンドの出力に従って、マスクエントリのパーミッションには書き込みアクセスが追加されています。従来どおり、そのようなパーミッションビットは、所有者の所属グループ(ここではproject3)もディレクトリmydirに書き込みアクセスできることを表します。ただし、所有者の所属グループの有効なアクセスパーミッションは、所有者の所属グループ向けおよびマスク用に定義されたパーミッションの重複部分に相当します。この部分は、この例ではr-xです(表 15.2. 「アクセスパーミッションのマスキング」 (338 ページ)を参照)。この例の所有者の所属グループの有効なパーミッションに関する限り、ACLエントリを追加した後も何も変わりませんでした。

マスクエントリを編集するには、`setfacl`または`chmod`を使用します。たとえば、`chmod g-w mydir`を使用すると、`ls -dl mydir`では、次のように表示されます。

```
drwxr-x---+ ... tux project3 ... mydir
```

`getfacl mydir`では、次の出力が得られます。

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascots:rwx       # effective: r-x
mask::r-x
other::---
```

`chmod`コマンドを実行してグループクラスビットから書き込みパーミッションを削除した後に、`ls`コマンドの出力を見れば、マスクビットが相応に変更されている、つまり、書き込みパーミッションが再び`mydir`の所有者に制限されていることを十分に確認できます。`getfacl`の出力でこの確認を行います。この出力に、有効なパーミッションビットが元のパーミッションと一致しないすべてのエントリのコメントが含まれる理由は、それらのビットがマスクエントリに基いてフィルタ処理されるためです。`chmod g+w mydir`を使用すれば、いつでも元のパーミッションに戻すことができます。

15.4.3 デフォルトACLが設定されたディレクトリ

ディレクトリには、デフォルトACLを設定できます。デフォルトACLとは、ディレクトリのオブジェクトを作成するときにそうしたオブジェクトが継承するアクセスパーミッションを定義する特別な種類のACLのことです。デフォルトACLは、サブディレクトリとファイルに作用します。

デフォルトACLの作用

ディレクトリのデフォルトACLのパーミッションをそのディレクトリ内のファイルやサブディレクトリに渡す方法は、次の2種類があります。

- サブディレクトリは、そのデフォルトACLおよびアクセスACLとして親ディレクトリのデフォルトACLを継承します。
- ファイルは、そのアクセスACLとしてデフォルトACLを継承します。

ファイルシステムオブジェクトを作成するすべてのシステムコールは、新たに作成したファイルシステムオブジェクトのアクセスパーミッションを定義するmodeパラメータを使用します。親ディレクトリにデフォルトACLが設定されていない場合、umaskで定義されたパーミッションビットは、modeパラメータで渡されるパーミッションから取り去られ、その結果が新しいオブジェクトに割り当てられます。親ディレクトリのデフォルトACLが存在する場合、新しいオブジェクトに割り当てられるパーミッションビットは、modeパラメータのパーミッションとデフォルトACLで定義されているパーミッションの重複部分に相当します。この場合、umaskは無視されます。

デフォルトACLのアプリケーション

次の3つの例は、ディレクトリとデフォルトACLの主要な操作を示しています。

1. 次のコマンドで、既存のディレクトリmydirにデフォルトACLを追加します。

```
setfacl -d -m group:mascots:r-x mydir
```

setfaclコマンドのオプション-dを指定することによって、setfaclは、後続の変更(オプション-m)をデフォルトACLに加えるように求められます。

このコマンドの結果を詳しく見てみます。

```
getfacl mydir
```

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
```

```
default:group:mascots:r-x
default:mask::r-x
default:other:---
```

getfaclは、アクセスACLとデフォルトACLを返します。デフォルトACLは、defaultで始まるすべての行によって生成されます。デフォルトACLのmascotsグループのエントリでsetfaclコマンドを実行しただけですが、setfaclで他のすべてのエントリが自動的にアクセスACLからコピーされ、有効なデフォルトACLが作成されました。デフォルトACLが、アクセスパーミッションに即時に作用することはありません。デフォルトACLは、ファイルシステムオブジェクトが作成された場合にのみ作用し始めます。こうした新しいオブジェクトは、それぞれの親ディレクトリのデフォルトACLからのみパーミッションを継承します。

2. 次の例では、mkdirでmydirにサブディレクトリを作成しています。このサブディレクトリは、デフォルトACLを継承します。

```
mkdir mydir/mysubdir

getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: project3
user::rw-
group::r-x
group:mascots:r-x
mask::r-x
other:---
default:user::rw-
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other:---
```

予想どおり、新たに作成されたサブディレクトリmysubdirには、親ディレクトリのデフォルトACLからのパーミッションが設定されています。mysubdirのアクセスACLは、mydirのデフォルトACLを正確に反映しています。このディレクトリからその下位オブジェクトにも同じデフォルトACLが継承されます。

3. touchコマンド(touch mydir/myfileなど)でmydirディレクトリにファイルを作成します。次に、ls -l mydir/myfileを実行すると、次のように表示されます。

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

getfacl mydir/myfileの出力は、次のようになります。

```
# file: mydir/myfile
# owner: tux
# group: project3
user::rw-
group::r-x      # effective:r--
group:mascots:r-x  # effective:r--
mask::r--
other::---
```

touchコマンドは、新しいファイルの作成時に値0666を指定してmodeを使用します。この値は、umaskおよびデフォルトACLにほかに制限がなければ、すべてのユーザクラスのファイルが読み取りと書き込みのパーミッションで作成されることを表します(デフォルトACLの作用項(342ページ)を参照)。つまり、mode値に含まれていないアクセスパーミッションはすべて、それぞれのACLエントリから削除されます。パーミッションは、グループクラスのACLエントリから削除されていませんが、マスクエントリは、modeで設定されていないパーミッションをマスクするように変更されています。

この方法により、ACLが設定されたアプリケーション（コンパイラなど）とのスムーズなインタラクションができます。制限付きアクセスパーミッションでファイルを作成し、作成したファイルを後で実行可能ファイルとしてマークすることができます。maskメカニズムでは、正当なユーザやグループが必要に応じて実行可能ファイルを実行できることが保証されます。

15.4.4 ACLチェックアルゴリズム

任意のプロセスまたはアプリケーションがACL保護されたファイルシステムオブジェクトにアクセスできるようになる前に、チェックアルゴリズムが適用されます。基本的には、所有者、名前付きユーザ、所有者の所属グループまたは名前付きグループ、およびその他の順番で、ACLエントリが検証されます。アクセスは、プロセスに最も適したエントリに従って処理されます。パーミッションへ累積しません。

プロセスが複数のグループに属し、複数のグループエントリに適する可能性がある場合は、さらに複雑になります。エントリは、必要なパーミッションを備えた適切なエントリから無作為に選択されます。どのエントリによって最終結果「アクセス許可」が実行されるかには関係ありません。同様に、適

切なグループエントリのどれにも必要なパーミッションが設定されていない場合は、無作為に選択されたエントリによって最終結果「アクセス拒否」が実行されます。

15.5 アプリケーションでのACLサポート

ACLを使用すれば、最新のアプリケーションの要件を満たす非常に複雑なパーミッションシナリオを実現できます。従来のパーミッション概念とACLは、洗練された方法で組み合わせることができます。基本的なファイルコマンド(cp、mv、lsなど)では、ACLがサポートされます。SambaやKonquerorでも同様です。

残念ながら、多くのエディタやファイルマネージャでは、依然としてACLをサポートしていません。たとえば、Emacsでファイルをコピーすると、ファイルのACLは失われます。エディタでファイルを変更すると、使用するエディタのバックアップモードによっては、ファイルのACLが維持されるときもあれば、維持されないときもあります。エディタが元のファイルに変更を書き込む場合、アクセスACLは維持されます。エディタで更新内容を新しいファイルに保存し、そのファイルの名前を後で古いファイル名に変更しても、ACLは失われるおそれがあります。ただし、エディタがACLをサポートしている場合は除きます。starアーカイバ以外に、ACLを維持するバックアップアプリケーションは現在ありません。

15.6 詳細情報

ACLの詳細については、<http://acl.bestbits.at/>を参照してください。getfacl(1)、acl(5)、およびsetfacl(1)については、manページも参照してください。

RPM—パッケージマネージャ

RPM (RPM Package Manager)がソフトウェアパッケージを管理するのに使用されます。RPMの主要コマンドは、rpmとrpmbuildです。ユーザ、システム管理者、およびパッケージの作成者は、強力なRPMデータベースでクエリーを行って、インストールされているソフトウェアに関する情報を取得できます。

基本的にrpmには、ソフトウェアパッケージのインストール、アンインストール、アップデート、RPMデータベースの再構築、RPMベースまたは個別のRPMアーカイブの照会、パッケージの整合性チェック、およびパッケージへの署名の5種類のモードがあります。rpmbuildは、元のソースからインストール可能なパッケージを作成する場合に使用します。.

インストール可能なRPMアーカイブは、特殊なバイナリ形式でパックされています。それらのアーカイブは、インストールするプログラムファイルとある種のメタ情報で構成されます。メタ情報は、ソフトウェアパッケージを設定するためにrpmによってインストール時に使用されるか、または文書化の目的でRPMデータベースに格納されています。通常、RPMアーカイブには拡張子.rpmが付けられます。

ティップ: ソフトウェア開発パッケージ

多くのパッケージにおいて、ソフトウェア開発に必要なコンポーネント(ライブラリ、ヘッダ、インクルードファイルなど)は、別々のパッケージに入れています。それらの開発パッケージは、最新のGNOMEパッケージのように、ソフトウェアを自分自身でコンパイルする場合にのみ、必要になります。それらのパッケージは、パッケージalsa-devel、gimp-devel、kdelibs3-develなどのように、名前の拡張子-develで識別できます。

16.1 パッケージの信頼性の検証

RPMパッケージにはGnuPG署名があります。フィンガープリントを含む鍵は、次のとおりです。

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>  
Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
```

`rpm --checksig package-1.2.3.rpm`コマンドを使用して、RPMパッケージの署名を検証し、パッケージが本当にSUSEから提供されたものか、他の信頼できる機関から提供されたものか判定できます。これは、インターネットからアップデートパッケージを入手する場合には、特に推奨されます。SUSEのパブリックパッケージ用の署名キーは通常、`/root/.gnupg/`にあります。バージョン8.1以降、キーは、ディレクトリ`/usr/lib/rpm/gnupg/`も格納されており、一般ユーザがRPMパッケージの署名を検証できるようになっています。

16.2 パッケージの管理:インストール、アップデート、およびアンインストール

通常RPMアーカイブのインストールはとても簡単です。`rpm -i package.rpm`の用に入力します。このコマンドで、パッケージをインストールできます。ただし、依存関係が満たされており、他のパッケージとの競合がない場合に限られます。`rpm`では、依存関係の要件を満たすためにインストールしなければならないパッケージがエラーメッセージで要求されます。バックグラウンドで、RPMデータベースは競合が起きないようにします。ある特定のファイルは、1つのパッケージだけにしか属せません。別のオプションを選択すると、`rpm`にこれらのデフォルト値を無視させることができますが、この処置を行うのは専門知識のある人に限られます。それ以外の人が行うと、システムの整合性を危うくするリスクが発生し、システムアップデート機能が損なわれる可能性があります。

`-U`または`--upgrade`と`-F`または`--freshen`の各オプションは、パッケージをアップデートするのに使用できます。たとえば、`rpm -F package.rpm`です。このコ

マンドは、古いバージョンのファイルを削除し、新しいファイルをただちにインストールします。2つのバージョン間の違いは、`-U`がシステムに存在していなかったパッケージをインストールするのに対して、`-F`がインストールされていたパッケージを単にアップデートする点にあります。アップデートする際、rpmは、以下のストラテジーに基づいて設定ファイルを注意深くアップデートします。

- 設定ファイルがシステム管理者によって変更されていない場合、rpmは新しいバージョンの適切なファイルをインストールします。システム管理者は、何も行う必要はありません。
- アップデートの前に設定ファイルがシステム管理者によって変更されている場合、rpmは変更されたファイルに拡張子`.rpmorig`または`.rpmsave` (バックアップファイル)を付けて保存し、新しいパッケージからファイルをインストールします。ただしこれは、元々インストールされていたファイルと新しいファイルのバージョンが異なる場合に限りです。異なる場合は、バックアップファイル(`.rpmorig`または`.rpmsave`)と新たにインストールされたファイルを比較して、新しいファイルに再度、変更を加えます。後ですべての`.rpmorig`と`.rpmsave`ファイルを必ず削除して、今後のアップデートで問題が起きないようにします。
- 設定ファイルがすでに存在しており、また`noreplace`ラベルが`.spec`ファイルで指定されている場合、`.rpmnew`ファイルが作成されます。

アップデートが終了したら、`.rpmsave`ファイルと`.rpmnew`ファイルは、比較した後、将来のアップデートの妨げにならないように削除する必要があります。ファイルがRPMデータベースで認識されなかった場合、ファイルには拡張子`.rpmorig`が付けられます。

認識された場合には、`.rpmsave`が付けられます。言い換えれば、`.rpmorig`は、RPM以外の形式からRPMにアップデートした結果として付けられます。`.rpmsave`は、古いRPMから新しいRPMにアップデートした結果として付けられます。`.rpmnew`は、システム管理者が設定ファイルに変更を加えたかどうかについて、何の情報も提供しません。それらのファイルのリストは、`/var/adm/rpmconfigcheck`にあります。設定ファイルの中には(`/etc/httpd/httpd.conf`など)、操作が継続できるように上書きされないものがあります。

-Uスイッチは、単に-eオプションでアンインストールして、-iオプションでインストールする操作と同じではありません。可能なときは必ず-Uを使用します。

パッケージを削除するには、`rpm -e package`を入力します。rpmは、解決されない依存関係がない場合にのみパッケージを削除します。他のアプリケーションがTcl/Tkを必要とする限り、Tcl/Tkを削除することは理論的に不可能です。その場合でも、RPMはデータベースに援助を要求します。他の依存関係がない場合でも、また、どのような理由、特殊な環境であってもそのような削除が不可能であれば、--rebuilddbオプションを使用してRPMデータベースを再構築するのが良いでしょう。

16.3 RPMとパッチ

システムの運用上のセキュリティを保証するには、ときどきアップデートパッケージをシステムにインストールする必要があります。以前は、パッケージ内のバグは、パッケージ全体を交換しなければ取り除けませんでした。大きいパッケージの場合、その中の小さなファイルにバグがあると、膨大な量のデータになってしまうことがありました。しかし、SUSE RPMを使用すると、パッケージ内にパッチをインストールできます。

最も重要な考慮事項について、pineを例として説明します。

パッチRPMはシステムに適したものか。

これを検査するには、はじめにインストールされたパッケージでクエリーを行います。pineでは、以下のコマンドを実行します。

```
rpm -q pine
pine-4.44-188
```

パッチRPMがこのバージョンのpineに適しているかどうかを検査します。

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

このパッチは、3種類のバージョンのpineに適しています。例でインストールされたバージョンもリストされています。パッチはインストールできます。

どのファイルがパッチで置き換えられるか。

パッチの影響を受けるファイルは、パッチRPMで見つけられます。
rpmの-Pパラメータを使用すると、特殊なパッチ機能を選択できます。次のコマンドでファイルをリストします。

```
rpm -qpPl pine-4.44-224.i586.patch.rpm  
/etc/pine.conf  
/etc/pine.conf.fixed  
/usr/bin/pine
```

パッチがすでにインストールされていれば、次のコマンドを使用します。

```
rpm -qPl pine  
/etc/pine.conf  
/etc/pine.conf.fixed  
/usr/bin/pine
```

パッチRPMをどのようにシステムにインストールするか。

パッチRPMは、通常のRPMと同様に使用されます。唯一の違いは、適切なRPMがすでにインストールされていなければならない点です。

どのパッチがシステムにインストールされており、それらはどのパッケージバージョンのものか。

システムにインストールされているすべてのパッチのリストは、コマンドrpm -qPaで表示できます。(この例のように)新しいシステムに1つのパッチだけがインストールされている場合、リストは次のようになります。

```
rpm -qPa  
pine-4.44-224
```

後日、オリジナルとしてインストールされていたパッケージのバージョンを知りたい場合、その情報はRPMデータベースから得られます。pineの場合、その情報は次のコマンドで表示できます。

```
rpm -q --basedon pine  
pine = 4.44-188
```

RPMのパッチ機能に関する情報を含む詳細な情報は、man rpmコマンドとrpmbuildコマンドのマニュアルページで収集できます。

16.4 デルタRPMパッケージ

デルタRPMパッケージには、RPMパッケージの新旧バージョン間の違いが含まれています。デルタRPMパッケージを古いRPMに適用すると、まったく新しいRPMになります。デルタRPMパッケージは、インストールされたRPMとも互換性があるので、古いRPMのコピーを保管する必要はありません。デルタRPMパッケージは、パッチRPMよりもさらに小さく、パッケージをインターネット上で転送するのに便利です。欠点は、デルタRPMが組み込まれたアップデート操作の場合、そのままのRPMまたはパッチRPMに比べて、CPUサイクルの消費が目立って多くなることです。

`prepdeltarpm`、`writedeltarpm`、および`applydeltarpm`バイナリは、デルタRPMスイート(`deltarpm`パッケージ)の一部であり、デルタRPMパッケージの作成と適用に際して役立ちます。次のコマンドを使用して、`new.delta.rpm`というデルタRPMを作成します。次のコマンドでは、`old.rpm`および`new.rpm`が存在することが前提となります。

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

最後に、一時作業ファイル`old.cpio`、`new.cpio`、および`delta`を削除します。

古いパッケージがすでにインストールされていれば、`applydeltarpm`を使用して、ファイルシステムから新たにRPMを構築できます。

```
applydeltarpm new.delta.rpm new.rpm
```

ファイルシステムにアクセスすることなく、古いRPMから構築するには、`-r`オプションを使用します。

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

技術的な詳細については、『`/usr/share/doc/packages/deltarpm/README`』を参照してください。

16.5 RPMクエリー

-qオプションを使用すると、rpmはクエリーを開始し、(-pオプションを追加することにより) RPMアーカイブを検査できるようにして、インストールされたパッケージのRPMデータベースでクエリーを行えるようにします。必要な情報の種類を指定する複数のスイッチを使用できます。詳細については、[表 16.1. 「最も重要なRPMクエリーのオプション」](#) (353 ページ)を参照してください。

表 16.1 最も重要なRPMクエリーのオプション

-i	パッケージ情報
-l	ファイルリスト
-f FILE	ファイルFILEを含むパッケージでクエリーを行います(FILEにはフルパスを指定する必要があります)。
-s	ステータス情報を含むファイルリスト(-lを暗示指定)
-d	ドキュメントファイルだけをリストします (-lを暗示指定)。
-c	設定ファイルだけをリストします(-lを暗示指定)。
--dump	詳細情報を含むファイルリスト(-l、-c、または-dと共に使用します)
--provides	他のパッケージが--requiresで要求できるパッケージの機能をリストします。
--requires, -R	パッケージが要求する機能
--スクリプト	インストールスクリプト(preinstall、postinstall、uninstall)

たとえば、コマンド `rpm -q -i wget` は、例 16.1. 「`rpm -q -i wget`」 (354 ページ) に示された情報を表示します。

例 16.1 `rpm -q -i wget`

```
Name           : wget                               Relocations: (not relocatable)
Version        : 1.9.1                             Vendor: SUSE LINUX AG,
Nuernberg, Germany
Release        : 50                                 Build Date: Sat 02 Oct 2004
03:49:13 AM CEST
Install date: Mon 11 Oct 2004 10:24:56 AM CEST      Build Host: f53.suse.de
Group          : Productivity/Networking/Web/Utilities Source RPM:
wget-1.9.1-50.src.rpm
Size           : 1637514                             License: GPL
Signature      : DSA/SHA1, Sat 02 Oct 2004 03:59:56 AM CEST, Key ID
a84edae89c800aca
Packager       : http://www.suse.de/feedback
URL            : http://wget.sunsite.dk/
Summary        : A tool for mirroring FTP and HTTP servers
Description    :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

オプション `-f` が機能するのは、フルパスで完全なファイル名を指定した場合だけです。必要な数のファイル名を指定します。たとえば、次のコマンドを実行します。

```
rpm -q -f /bin/rpm /usr/bin/wget
```

出力は次のとおりです。

```
rpm-4.1.1-191
wget-1.9.1-50
```

ファイル名の一部分しかわからない場合は、例 16.2. 「パッケージを検索するスクリプト」 (354 ページ) に示すようなシェルスクリプトを使用します。実行するときに、ファイル名の一部を、パラメータとして示されるスクリプトに渡します。

例 16.2 パッケージを検索するスクリプト

```
#!/bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```


`rpm -q --changelog rpm` コマンドは、特定のパッケージに関する詳細な変更情報を日付順に表示します。この例は、`rpm` パッケージに関する情報を示します。

インストールされたRPMデータベースを使うと、確認検査を行うことができます。それらの検査は、`-V`、`-y`、または`--verify` オプションを使用して開始します。このオプションを使うと、`rpm` は、パッケージ内にあり、インストール以降変更されたことがあるすべてのファイルを表示します。`rpm` は、次の変更に関するヒントを表示するのに、8文字の記号を使用します。

表 16.2 RPM 確認オプション

5	MD5 チェックサム
S	ファイルサイズ
L	シンボリックリンク
T	変更時間
D	メジャーデバイス番号とマイナーデバイス番号
U	所有者
G	グループ
M	モード (許可とファイルタイプ)

設定ファイルの場合は、文字 `c` が表示されます。`/etc/wgetrc(wget)` に対する変更例を以下に示します。

```
rpm -V wget
S.5....T c /etc/wgetrc
```

RPM データベースのファイルは、`/var/lib/rpm` に格納されています。パーティション `/usr` のサイズが **1 GB** であれば、このデータベースは、完全なアップデート後、およそ **30 MB** 占有します。データベースが予期していたよりもはるかに大きい場合は、オプション `--rebuilddb` でデータベースを再構築するようにします。再構築する前に、古いデータベースのバックアップを作成しておきます。`cron` スクリプトの `cron.daily` は、データベースのコピー (`gzip`

でバックされる)を毎日作成し、`/var/adm/backup/rpmdb`に格納します。コピー数は`/etc/sysconfig/backup`にある変数`MAX_RPMDDB_BACKUPS`で制御します(デフォルト:5)。1つのバックアップのサイズは、1GBの`/usr`に対しておよそ1MBです。

16.6 ソースパッケージのインストールとコンパイル

すべてのソースパッケージには、拡張子`.src.rpm`(ソース RPM)が付けられています。

ティップ

ソースパッケージは、インストールメディアからハードディスクにコピーされ、YaSTを使用して展開できます。ただし、ソースパッケージは、パッケージマネージャでインストール済み([i])というマークは付きません。これは、ソースパッケージがRPMデータベースに入れられないためです。インストールされたオペレーティングシステムソフトウェアだけがRPMデータベースにリストされます。ソースパッケージを「インストールする」場合、ソースコードだけがシステムに追加されます。

(`/etc/rpmrc`などのファイルでカスタム設定を指定していない限り)以下のディレクトリが、`/usr/src/packages`の下で`rpm`と`rpmbuild`から使用可能でなければなりません。

SOURCES

オリジナルのソース(`.tar.gz`ファイルや`.tar.gz`ファイルなど)とディストリビューション固有の調整ファイル(ほとんどの場合`.dif`ファイルや`.patch`ファイル)用です。

SPECS

ビルド処理を制御する、メタ`Makefile`に類似した`.spec`ファイル用です。

BUILD

すべてのソースは、このディレクトリでアンパック、パッチ、コンパイルされます。

RPMS

完成したバイナリパッケージが格納されます。

SRPMS

ソースRPMが格納されます。

YaSTを使ってソースパッケージをインストールすると、必要なすべてのコンポーネントが/usr/src/packagesにインストールされます。ソースと調整はSOURCES、関連する.specファイルはSPECSに格納されます。

警告

システムコンポーネント(glibc、rpm、sysvinitなど)で実験してはいけません。システムが正しく動作しなくなります。

次の例は、wget.src.rpmパッケージを使用します。YaSTでパッケージをインストールすると、次のファイルが作成されるはずです。

```
/usr/src/packages/SOURCES/nops_doc.diff
/usr/src/packages/SOURCES/toplev_destdir.diff
/usr/src/packages/SOURCES/wget-1.9.1+ipvmisc.patch
/usr/src/packages/SOURCES/wget-1.9.1-brokentime.patch
/usr/src/packages/SOURCES/wget-1.9.1-passive_ftp.diff
/usr/src/packages/SOURCES/wget-LFS-20040909.tar.bz2
/usr/src/packages/SOURCES/wget-wrong_charset.patch
/usr/src/packages/SPECS/wget.spec
```

rpmbuild -b X /usr/src/packages/SPECS/wget.spec コマンドは、コンパイルを開始します。Xは、ビルド処理のさまざまな段階に対して使用されるワイルドカードです(詳細については、--helpの出力またはRPMのドキュメントを参照してください)。以下に簡単な説明を示します。

-bp

/usr/src/packages/BUILD内のソースを用意します。アンパック、パッチしてください。

-bc

-bpと同じですが、コンパイルを実行します。

-bi

-bpと同じですが、ビルドしたソフトウェアをインストールします。警告: パッケージがBuildRoot機能をサポートしていない場合は、設定ファイルが上書きされることがあります。

-bb

-biと同じですが、バイナリパッケージを作成します。コンパイルに成功すると、バイナリパッケージは、/usr/src/packages/RPMSに作成されるはずです。

-ba

-bbと同じですが、ソース RPMを作成します。コンパイルに成功すると、バイナリは/usr/src/packages/SRPMSに作成されるはずです。

--short-circuit

一部のステップをスキップします。

作成されたバイナリRPMは、rpm -iコマンドまたはrpm -Uコマンドでインストールできます。rpmを使用したインストールは、RPMデータベースに登場します。

16.7 buildによるRPMパッケージのコンパイル

多くのパッケージにつきものの不都合は、ビルド処理中に不要なファイルが稼働中のシステムに追加されてしまうことです。これを回避するには、パッケージのビルド先の定義済みの環境を作成するbuildを使用します。このchroot環境を確立するには、build スクリプトが完全なパッケージツリーと共に提供されなければなりません。パッケージツリーは、NFS経由で、またはDVDからハードディスク上で利用できるようにすることができます。build --rpms *directory*で、位置を指定します。rpmとは異なり、buildコマンドはソースディレクトリでSPECファイルを探します。(上記の例と同様に)システムで/media/dvdの下にマウントされているDVDでwgetをビルドするには、rootユーザーで次のコマンドを使用します。

```
cd /usr/src/packages/SOURCES/  
mv ../SPECS/wget.spec .  
build --rpms /media/dvd/suse/ wget.spec
```

これで、最小限の環境が/var/tmp/build-rootに確立されます。パッケージは、この環境でビルドされます。処理が完了すると、ビルドされたパッケージは/var/tmp/build-root/usr/src/packages/RPMSに格納されます。

buildスクリプトでは、他のオプションも多数使用できます。たとえば、スクリプトがユーザ独自のRPMを処理するようにするには、ビルド環境の初期化を省略するか、rpmコマンドの実行を上記のビルド段階のいずれかに制限します。build --helpコマンドとman buildコマンドで、詳細な情報が得られます。

16.8 RPMアーカイブとRPMデータベース用のツール

Midnight Commander (mc)は、RPMアーカイブの内容を表示し、それらの一部をコピーできます。アーカイブを仮想ファイルシステムとして表し、Midnight Commanderの通常のメニューオプションを使用できます。<F3>キーを使用してHEADERを表示します。カーソルキーと<Enter>キーを使ってアーカイブ構造を表示します。<F5>キーを使用してアーカイブコンポーネントをコピーします。

KDEは、rpmのフロントエンドとしてkpackageツールを提供します。完全装備のパッケージマネージャが、YaSTモジュールとして使用可能です(「[8.3.1項「ソフトウェアのインストールと削除」](#) (146 ページ)」を参照してください)。

システムモニタリングユーティリティ

17

システムのステータスは、多数のプログラムやメカニズムを使用して検査できます。ここではその一部について説明します。また、日常作業に役立つ一部のユーティリティとその最も重要なパラメータについても説明します。

ここでは、コマンドごとに関連出力の例を示してあります。これらの例の1行目はコマンド自体です(ドル記号(>)または#記号プロンプトの後)。省略は、大カッコ [...] で示されており、長い行は必要に応じて折り返されています。長い行の改行はバックスラッシュ(\)で示されています。

```
# command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

できるだけ多数のユーティリティを紹介できるように、簡潔に説明しています。すべてのコマンドの詳細は、マニュアルページで確認できます。また、ほとんどのコマンドではパラメータ--helpが認識されます。このパラメータを指定すると、使用可能なパラメータの簡略リストが表示されます。

17.1 デバッグ

17.1.1 必須ライブラリの指定:ldd

lddコマンドを使用すると、引数として指定した動的実行可能ファイルをロードするライブラリを確認できます。

```
tux@mercury:~> ldd /bin/ls
linux-gate.so.1 => (0xfffffe000)
librt.so.1 => /lib/librt.so.1 (0xb7f97000)
libacl.so.1 => /lib/libacl.so.1 (0xb7f91000)
libc.so.6 => /lib/libc.so.6 (0xb7e79000)
libpthread.so.0 => /lib/libpthread.so.0 (0xb7e67000)
/lib/ld-linux.so.2 (0xb7fb6000)
libattr.so.1 => /lib/libattr.so.1 (0xb7e63000)
```

静的バイナリファイルには、動的ライブラリは不要です。

```
tux@mercury:~> ldd /bin/sash
not a dynamic executable
tux@mercury:~> file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for
GNU/Linux 2.6.4, statically linked, for GNU/Linux 2.6.4, stripped
```

17.1.2 実行されたプログラムによるライブラリ呼び出し:ltrace

コマンドltraceを使用すると、プロセスによるライブラリ呼び出しをトレースできます。このコマンドの使用方法は、straceと同様です。パラメータ-cを指定すると、発生したライブラリ呼び出しの回数と持続期間が出力されます。

```
tux@mercury:~> ltrace -c find ~
% time      seconds  usecs/call   calls      function
-----
34.37      6.758937      245      27554  __errno_location
33.53      6.593562      788      8358   __fprintf_chk
12.67      2.490392      144     17212  strlen
11.97      2.353302      239     9845   readdir64
 2.37      0.466754       27     16716  __ctype_get_mb_cur_max
 1.17      0.230765       27     8358   memcpy
[...]
 0.00      0.000036       36        1  textdomain
```


17.1.3 実行中のプログラムのシステム呼び出し: strace

ユーティリティ `strace` を使用すると、現在実行中のプロセスのシステム呼び出しをすべてトレースできます。行頭の `strace` に続けてコマンドを通常どおり入力します。

```
tux@mercury:~> strace ls
execve("/bin/ls", ["ls"], [/ 61 vars *]) = 0
uname({sys="Linux", node="mercury", ...}) = 0
brk(0) = 0x805c000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or \
    directory)
open("/etc/ld.so.cache", O_RDONLY) = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=89696, ...}) = 0
mmap2(NULL, 89696, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb7ef2000
close(3) = 0
open("/lib/librt.so.1", O_RDONLY) = 3
read(3, "\177ELF\1\1\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0000\36\0"... , 512) \
    = 512
fstat64(3, {st_mode=S_IFREG|0755, st_size=36659, ...}) = 0
[... ]
stat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
    = 0xb7ca7000
write(1, "bin Desktop Documents music\tM"... , 55bin Desktop Documents \
    \ music Music public_html tmp
) = 55
close(1) = 0
munmap(0xb7ca7000, 4096) = 0
exit_group(0) = ?
```

たとえば、特定のファイルを開く試みをすべてトレースするには、以下を入力します。

```
tux@mercury:~> strace -e open ls .bashrc
open("/etc/ld.so.cache", O_RDONLY) = 3
open("/lib/librt.so.1", O_RDONLY) = 3
open("/lib/libacl.so.1", O_RDONLY) = 3
open("/lib/libc.so.6", O_RDONLY) = 3
open("/lib/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY) = 3
[... ]
```

すべての子プロセスをトレースするには、パラメータ-fを使用します。straceの動作と出力形式は厳密に制御できます。詳細については、man straceを参照してください。

17.2 ファイルとファイルシステム

17.2.1 ファイルタイプの判断:file

fileコマンドは、/etc/magicを確認して、1つまたは複数のファイルのファイルタイプを判断します。

```
tux@mercury:~> file /usr/bin/file
/usr/bin/file: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, dynamically linked (uses shared libs), stripped
```

パラメータ-f listは、複数のファイルを調べる場合に使用します。fileコマンドで圧縮ファイル内を調べる場合は、-zオプションを指定します。

```
tux@mercury:~> file /usr/share/man/man1/file.1.gz
usr/share/man/man1/file.1.gz: gzip compressed data, from Unix, max compression
tux@mercury:~> file -z /usr/share/man/man1/file.1.gz
/usr/share/man/man1/file.1.gz: ASCII troff or preprocessor input text \
(gzip compressed data, from Unix, max compression)
```

17.2.2 ファイルシステムとその使用 法:mount、df、およびdu

コマンドmountは、どのファイルシステム(デバイスとタイプ)がどのマウントポイントにマウントされているかを出力します。

```
tux@mercury:~> mount
/dev/sda3 on / type reiserfs (rw,acl,user_xattr)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/sda1 on /boot type ext2 (rw,acl,user_xattr)
/dev/sda4 on /local type reiserfs (rw,acl,user_xattr)
/dev/fd0 on /media/floppy type subfs (rw,nosuid,nodev,noatime,fs=floppyfs,p
```

コマンドdfを使用して、ファイルシステムの使用状況に関する合計情報を入力してください。パラメータ-h(または--human-readable)を指定すると、出力は通常のユーザが理解できる形式に変換されます。

```
tux@mercury:~> df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        11G   3.2G   6.9G  32% /
udev            252M   104K   252M   1% /dev
/dev/sda1        16M    6.6M    7.8M  46% /boot
/dev/sda4        27G    34M    27G   1% /local
```

指定したディレクトリとそのサブディレクトリの全ファイルの合計サイズを表示するには、コマンドduを使用します。-sパラメータを指定すると、詳細情報は出力されません。-hは、再びデータを通常のユーザが理解できる形式に変換します。

```
tux@mercury:~> du -sh /local
1.7M    /local
```

17.2.3 ELF バイナリに関する補足情報

バイナリの内容を読み込むには、readelfユーティリティを使用します。このユーティリティは、他のハードウェアアーキテクチャ用に作成されたELFファイルにも使用できます。

```
tux@mercury:~> readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                               ELF32
  Data:                                 2's complement, little endian
  Version:                             1 (current)
  OS/ABI:                               UNIX - System V
  ABI Version:                         0
  Type:                                 EXEC (Executable file)
  Machine:                              Intel 80386
  Version:                              0x1
  Entry point address:                  0x8049b60
  Start of program headers:             52 (bytes into file)
  Start of section headers:            81112 (bytes into file)
  Flags:                                0x0
  Size of this header:                  52 (bytes)
  Size of program headers:              32 (bytes)
  Number of program headers:            9
  Size of section headers:              40 (bytes)
  Number of section headers:            30
  Section header string table index:    29
```

17.2.4 ファイルのプロパティ:stat

コマンドstatは、ファイルのプロパティを表示します。

```
tux@mercury:~> stat /etc/profile
  File: `/etc/profile'
  Size: 8080          Blocks: 16          IO Block: 4096   regular file
Device: 806h/2054d   Inode: 64942        Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/   root)   Gid: (    0/   root)
Access: 2007-07-16 23:28:18.000000000 +0200
Modify: 2006-09-19 14:45:01.000000000 +0200
Change: 2006-12-05 14:54:55.000000000 +0100
```

パラメータ--filesystemを指定すると、指定したファイルが置かれているファイルシステムのプロパティの詳細が出力されます。

```
tux@mercury:~> stat /etc/profile --filesystem
  File: "/etc/profile"
   ID: 0      Namelen: 255      Type: reiserfs
Block size: 4096      Fundamental block size: 4096
Blocks: Total: 2622526   Free: 1809771   Available: 1809771
Inodes: Total: 0         Free: 0
```

17.3 ハードウェア情報

17.3.1 PCIリソース:lspci

コマンドlspciはPCIリソースをリストします。

```
mercury:~ # lspci
00:00.0 Host bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
  DRAM Controller/Host-Hub Interface (rev 01)
00:01.0 PCI bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
  Host-to-AGP Bridge (rev 01)
00:1d.0 USB Controller: Intel Corporation 82801DB/DBL/DBM \
  (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #1 (rev 01)
00:1d.1 USB Controller: Intel Corporation 82801DB/DBL/DBM \
  (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #2 (rev 01)
00:1d.2 USB Controller: Intel Corporation 82801DB/DBL/DBM \
  (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #3 (rev 01)
00:1d.7 USB Controller: Intel Corporation 82801DB/DBM \
  (ICH4/ICH4-M) USB2 EHCI Controller (rev 01)
00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev 81)
00:1f.0 ISA bridge: Intel Corporation 82801DB/DBL (ICH4/ICH4-L) \
  LPC Interface Bridge (rev 01)
00:1f.1 IDE interface: Intel Corporation 82801DB (ICH4) IDE \
```

```

    Controller (rev 01)
00:1f.3 SMBus: Intel Corporation 82801DB/DBL/DBM (ICH4/ICH4-L/ICH4-M) \
    SMBus Controller (rev 01)
00:1f.5 Multimedia audio controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) AC'97 Audio Controller (rev 01)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. G400/G450 (rev 85)
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM) \
    Ethernet Controller (rev 81)

```

-vを使用すると、さらに詳細なリストが出力されます。

```

mercury:~ # lspci
[...]
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM)\
    Ethernet Controller (rev 81)
    Subsystem: Fujitsu Siemens Computer GmbH: Unknown device 1001
    Flags: bus master, medium devsel, latency 66, IRQ 11
    Memory at d1000000 (32-bit, non-prefetchable) [size=4K]
    I/O ports at 3000 [size=64]
    Capabilities: [dc] Power Management version 2

```

デバイス名の解決に関する情報は、ファイル/usr/share/pci.idsから取得されます。このファイルにないPCI IDは、「Unknown device」で示されます。

パラメータ-vvを指定すると、プログラムが問い合わせ可能な情報がすべて出力されます。数値のみを表示するには、パラメータ-nを使用します。

17.3.2 USBデバイス:lsusb

コマンドlsusbは、すべてのUSBデバイスのリストを表示します。オプション-vを使用すると、詳細なリストが印刷されます。この詳細は、ディレクトリ/proc/bus/usb/から読み込まれます。ハブ、メモリスティック、ハードディスク、およびマウスなどのUSBデバイスが接続された状態での、lsusbコマンドの出力例を以下に示します。

```

mercury:/ # lsusb
Bus 004 Device 007: ID 0ea0:2168 Ours Technology, Inc. Transcend JetFlash \
    2.0 / Astone USB Drive
Bus 004 Device 006: ID 04b4:6830 Cypress Semiconductor Corp. USB-2.0 IDE \
    Adapter
Bus 004 Device 005: ID 05e3:0605 Genesys Logic, Inc.
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000

```

```
Bus 001 Device 005: ID 046d:c012 Logitech, Inc. Optical Mouse
Bus 001 Device 001: ID 0000:0000
```

17.3.3 SCSIデバイスに関する情報:scsiinfo

コマンド`scsiinfo`は、SCSIデバイスに関する情報のリストを表示します。オプション`-l`を使用すると、システムに登録されているすべてのSCSIデバイスのリストが表示されます(同様の情報は、コマンド`lsscsi`でも入手できます)。次に示すものは、`scsiinfo -i /dev/sda`の出力です。この場合、ハードディスクに関する情報が表示されます。オプション`-a`で、詳細が表示されます。

```
mercury:/ # scsiinfo -i /dev/sda
Inquiry command
-----
Relative Address                0
Wide bus 32                     0
Wide bus 16                     1
Synchronous neg.               1
Linked Commands                 1
Command Queueing                1
SftRe                           0
Device Type                     0
Peripheral Qualifier            0
Removable?                      0
Device Type Modifier            0
ISO Version                     0
ECMA Version                    0
ANSI Version                    3
AENC                            0
TrmIOP                          0
Response Data Format            2
Vendor:                         FUJITSU
Product:                        MAS3367NP
Revision level:                 0104A0K7P43002BE
```

オプション`-d`を指定すると、ハードディスクの不良ブロックを2つのテーブルに出力します。1つは、メーカーが提供するテーブル(製造業者テーブル)で、もう1つは処理中に発見された不良ブロックのリスト(grownテーブル)です。成長テーブル内のエントリ数が増えた場合、ハードディスクを交換するほうが良いでしょう。

17.4 ネットワーキング

17.4.1 ネットワークステータスの表示:netstat

netstatコマンドを利用すれば、ネットワーク接続、ルーティングテーブル(-r)、インタフェース(-i)、マスカレード接続(-M)、マルチキャストメンバーシップ(-g)、および統計情報(-s)を表示することができます。

```
tux@mercury:~> netstat -r
Kernel IP routing table
Destination      Gateway           Genmask           Flags   MSS Window  irtt Iface
192.168.2.0      *                 255.255.254.0     U        0 0        0 eth0
link-local       *                 255.255.0.0       U        0 0        0 eth0
loopback         *                 255.0.0.0         U        0 0        0 lo
default          192.168.2.254    0.0.0.0           UG       0 0        0 eth0
```

```
tux@mercury:~> netstat -i
Kernel Interface table
Iface   MTU Met  RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0    1500  0 1624507 129056      0      0  7055      0      0      0 BMNRRU
lo      16436  0   23728      0      0      0 23728      0      0      0 LRU
```

ネットワーク接続または統計情報を表示する場合、表示するソケットタイプを指定することができます:TCP(-t)、UDP(-u)、またはraw(-r)。-pオプションを指定すると、各ソケットが属するプログラムのPIDとプログラム名が表示されます。

以下の例では、これらの接続を使用するすべてのTCP接続とプログラムが表示されています。

```
mercury:~ # netstat -t -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address   State       PID/Pro
tcp      0      0 mercury:33513   www.novell.com:www-http ESTABLISHED 6862/fi
tcp      0      0 mercury:ssh     mercury2.:trc-netpoll ESTABLISHED
19422/s
tcp      0      0 localhost:ssh   localhost:17828    ESTABLISHED -
```

以下の例では、TCPプロトコルに関する統計情報が表示されています。

```
tux@mercury:~> netstat -s -t
Tcp:
  2427 active connections openings
  2374 passive connection openings
  0 failed connection attempts
```

```

0 connection resets received
1 connections established
27476 segments received
26786 segments send out
54 segments retransmitted
0 bad segments received.
6 resets sent
[...]
TCPAbortOnLinger: 0
TCPAbortFailed: 0
TCPMemoryPressures: 0

```

17.5 /procファイルシステム

/procファイルシステムは、カーネルにより重要な情報が仮想ファイルの形式で保持される疑似ファイルシステムです。たとえば、次のコマンドを使用すると、CPUのタイプを確認できます。

```

tux@mercury:~> cat /proc/cpuinfo
processor       : 0
vendor_id      : AuthenticAMD
cpu family     : 6
model          : 8
model name     : AMD Athlon(tm) XP 2400+
stepping       : 1
cpu MHz        : 2009.343
cache size     : 256 KB
fdiv_bug       : no
[...]

```

割り当てと割り込み回数を照会するには、以下のコマンドを使用します。

```

tux@mercury:~> cat /proc/interrupts
CPU0
 0:   3577519      XT-PIC  timer
 1:     130       XT-PIC  i8042
 2:         0      XT-PIC  cascade
 5:   564535      XT-PIC  Intel 82801DB-ICH4
 7:         1      XT-PIC  parport0
 8:         2      XT-PIC  rtc
 9:         1      XT-PIC  acpi, uhci_hcd:usb1, ehci_hcd:usb4
10:         0      XT-PIC  uhci_hcd:usb3
11:    71772      XT-PIC  uhci_hcd:usb2, eth0
12:   101150      XT-PIC  i8042
14:    33146      XT-PIC  ide0
15:   149202      XT-PIC  ide1
NMI:         0
LOC:         0

```



```
ERR:      0
MIS:      0
```

重要なファイルとその内容の一部は次のとおりです。

```
/proc/devices
  使用可能なデバイス
```

```
/proc/modules
  ロードされたカーネルモジュール
```

```
/proc/cmdline
  カーネルコマンドライン
```

```
/proc/meminfo
  メモリ使用状況に関する詳細情報
```

```
/proc/config.gz
  gzip-現在実行中のカーネルの圧縮設定ファイル
```

詳細は、テキストファイル/usr/src/linux/Documentation/filesystems/proc.txtにあります。現在実行中のプロセスについては、/proc/NNNディレクトリで確認できます。この場合、NNNは関連プロセスのプロセスID(PID)です。/proc/self/を指定すると、プロセスとその特有の特性を確認できます。

```
tux@mercury:~> ls -l /proc/self
lrwxrwxrwx 1 root root 64 2007-07-16 13:03 /proc/self -> 5356
tux@mercury:~> ls -l /proc/self/
total 0
dr-xr-xr-x 2 tux users 0 2007-07-16 17:04 attr
-r----- 1 tux users 0 2007-07-16 17:04 auxv
-r--r--r-- 1 tux users 0 2007-07-16 17:04 cmdline
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 cwd -> /home/tux
-r----- 1 tux users 0 2007-07-16 17:04 environ
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 exe -> /bin/ls
dr-x----- 2 tux users 0 2007-07-16 17:04 fd
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 loginuid
-r--r--r-- 1 tux users 0 2007-07-16 17:04 maps
-rw----- 1 tux users 0 2007-07-16 17:04 mem
-r--r--r-- 1 tux users 0 2007-07-16 17:04 mounts
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 oom_adj
-r--r--r-- 1 tux users 0 2007-07-16 17:04 oom_score
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 root -> /
-rw----- 1 tux users 0 2007-07-16 17:04 seccomp
-r--r--r-- 1 tux users 0 2007-07-16 17:04 smaps
```

```
-r--r--r-- 1 tux users 0 2007-07-16 17:04 stat
[...]
dr-xr-xr-x 3 tux users 0 2007-07-16 17:04 task
-r--r--r-- 1 tux users 0 2007-07-16 17:04 wchan
```

実行可能ファイルとライブラリのアドレス割り当ては、mapsファイルに含まれています。

```
tux@mercury:~> cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:03 17753      /bin/cat
0804c000-0804d000 rw-p 00004000 03:03 17753      /bin/cat
0804d000-0806e000 rw-p 0804d000 00:00 0        [heap]
b7d27000-b7d5a000 r--p 00000000 03:03 11867      /usr/lib/locale/en_GB.utf8/
b7d5a000-b7e32000 r--p 00000000 03:03 11868      /usr/lib/locale/en_GB.utf8/
b7e32000-b7e33000 rw-p b7e32000 00:00 0
b7e33000-b7f45000 r-xp 00000000 03:03 8837       /lib/libc-2.3.6.so
b7f45000-b7f46000 r--p 00112000 03:03 8837       /lib/libc-2.3.6.so
b7f46000-b7f48000 rw-p 00113000 03:03 8837       /lib/libc-2.3.6.so
b7f48000-b7f4c000 rw-p b7f48000 00:00 0
b7f52000-b7f53000 r--p 00000000 03:03 11842      /usr/lib/locale/en_GB.utf8/
[...]
b7f5b000-b7f61000 r--s 00000000 03:03 9109       /usr/lib/gconv/gconv-module
b7f61000-b7f62000 r--p 00000000 03:03 9720       /usr/lib/locale/en_GB.utf8/
b7f62000-b7f76000 r-xp 00000000 03:03 8828       /lib/ld-2.3.6.so
b7f76000-b7f78000 rw-p 00013000 03:03 8828       /lib/ld-2.3.6.so
bfd61000-bfd76000 rw-p bfd61000 00:00 0        [stack]
ffffe000-fffff000 ---p 00000000 00:00 0        [vdso]
```

17.5.1 procinfo

/procファイルシステムからの重要情報のサマリを確認するには、コマンドprocinfoを使用します。

```
tux@mercury:~> procinfo
Linux 2.6.18.8-0.5-default (geeko@buildhost) (gcc 4.1.2 20061115) #1 2CPU

Memory:      Total      Used      Free      Shared      Buffers
Mem:         2060604    2011264    49340     0           200664
Swap:        2104472      112      2104360

Bootup: Tue Jul 10 10:29:15 2007      Load average: 0.86 1.10 1.11 3/118 21547

user   :      2:43:13.78    0.8%  page in :    71099181  disk 1:  2827023r 968
nice   :    1d 22:21:27.87  14.7%  page out:   690734737
system:    13:39:57.57    4.3%  page act:  138388345
IOwait:    18:02:18.59    5.7%  page dea:   29639529
hw irq:      0:03:39.44    0.0%  page flt:  9539791626
sw irq:      1:15:35.25    0.4%  swap in :           69
idle    :    9d 16:07:56.79  73.8%  swap out:           209
```

```

uptime:    6d 13:07:11.14          context :   542720687

irq 0: 141399308 timer             irq 14:   5074312 ide0
irq 1:    73784 i8042              irq 50:   1938076 uhci_hcd:usb1, ehci_
irq 4:      2                      irq 58:      0 uhci_hcd:usb2
irq 6:      5 floppy [2]          irq 66:   872711 uhci_hcd:usb3, HDA I
irq 7:      2                      irq 74:     15 uhci_hcd:usb4
irq 8:      0 rtc                  irq 82: 178717720 0          PCI-MSI  e
irq 9:      0 acpi                irq169: 44352794 nvidia
irq 12:     3                     irq233: 8209068 0          PCI-MSI  1

```

すべての情報を表示するには、パラメータ-aを使用します。**-nN**パラメータを指定すると、情報が**N秒間隔**で更新されます。この場合、プログラムを終了するには<Q>キーを押します。

デフォルトでは、累積値が表示されます。パラメータ-dを入力すると、別の値が作成されます。procinfo -dn5を入力すると、過去5秒間に变化した値が表示されます。

17.6 プロセス

17.6.1 プロセス間通信:ipcs

コマンドipcsは、現在使用中のIPCリソースのリストを出力します。

```

----- Shared Memory Segments -----
key          shmid      owner      perms      bytes      nattch     status
0x00000000   58261504    tux        600         393216      2          dest
0x00000000   58294273    tux        600         196608      2          dest
0x00000000   83886083    tux        666         43264       2
0x00000000   83951622    tux        666         192000      2
0x00000000   83984391    tux        666         282464      2
0x00000000   84738056    root       644         151552      2          dest

----- Semaphore Arrays -----
key          semid      owner      perms      nsems
0x4d038abf   0          tux        600         8

----- Message Queues -----
key          msqid      owner      perms      used-bytes   messages

```

17.6.2 プロセスリスト:ps

コマンドpsは、プロセスのリストを作成します。多くのパラメータは、マイナス記号なしで指定する必要があります。簡単なヘルプはps --helpを使用し、詳細なヘルプはマニュアルページを参照します。

すべてのプロセスをユーザとコマンドライン情報とともに表示するには、ps axuを使用します。

```
tux@mercury:~> ps axu
USER      PID  %CPU  %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1   0.0   0.0    696   272 ?        S    12:59    0:01 init [5]
root         2   0.0   0.0      0      0 ?        SN   12:59    0:00 [ksoftirqd
root         3   0.0   0.0      0      0 ?        S<   12:59    0:00 [events
[...]
tux      4047   0.0   6.0 158548 31400 ?        Ssl   13:02    0:06 mono-best
tux      4057   0.0   0.7   9036  3684 ?        Sl    13:02    0:00 /opt/gnome
tux      4067   0.0   0.1   2204   636 ?        S    13:02    0:00 /opt/gnome
tux      4072   0.0   1.0  15996  5160 ?        Ss    13:02    0:00 gnome-scre
tux      4114   0.0   3.7 130988 19172 ?        SLl   13:06    0:04 sound-juic
tux      4818   0.0   0.3   4192  1812 pts/0    Ss    15:59    0:00 -bash
tux      4959   0.0   0.1   2324   816 pts/0    R+    16:17    0:00 ps axu
```

実行中のsshdプロセスの数を確認するには、pidofコマンドとともに-pオプションを使用します。これにより、指定したプロセスのプロセスIDが表示されます。

```
tux@mercury:~> ps -p `pidof sshd`
  PID TTY          STAT       TIME COMMAND
 3524 ?           Ss          0:00 /usr/sbin/sshd -o PidFile=/var/run/sshd.init.pid
 4813 ?           Ss          0:00 sshd: tux [priv]
 4817 ?           R           0:00 sshd: tux@pts/0
```

プロセスリストは、必要に応じてフォーマットできます。-Lオプションを指定すると、すべてのキーワードのリストが返されます。次のコマンドを入力すると、メモリ使用量順の全プロセスのリストが発行されます。

```
tux@mercury:~> ps ax --format pid,rss,cmd --sort rss
  PID  RSS  CMD
    2     0 [ksoftirqd/0]
    3     0 [events/0]
    4     0 [khelper]
    5     0 [kthread]
   11     0 [kblockd/0]
   12     0 [kacpid]
  472     0 [pdflush]
  473     0 [pdflush]
[...]

```

```

4028 17556 nautilus --no-default-window --sm-client-id default2
4118 17800 ksnapshot
4114 19172 sound-juicer
4023 25144 gnome-panel --sm-client-id default1
4047 31400 mono-best --debug /usr/lib/beagle/Best.exe --autostarted
3973 31520 mono-beagled --debug /usr/lib/beagle/BeagleDaemon.exe --bg --aut

```

17.6.3 プロセスツリー:pstree

pstreeコマンドは、プロセスリストをツリー形式で出力します。

```

tux@mercury:~> pstree
init--NetworkManagerD
    |-acpid
    |-3*[automount]
    |-cron
    |-cupsd
    |-2*[dbus-daemon]
    |-dbus-launch
    |-dcopserver
    |-dhcpcd
    |-events/0
    |-gpg-agent
    |-hald--hald-addon-acpi
    |   `--hald-addon-stor
    |-kded
    |-kdeinit--kdesu---su---kdesu_stub---yast2---y2controlcenter
    |   |   |-kio_file
    |   |   |-klauncher
    |   |   |-konqueror
    |   |   |-konsole--bash---su---bash
    |   |   |   `--bash
    |   |   `--kwin
    |-kdesktop---kdesktop_lock---xmatrix
    |-kdesud
    |-kdm--X
    |   `--kdm---startkde---kwrapper
[...]
```

パラメータ-pを指定すると、プロセス名にプロセスIDが追加されます。コマンドラインも表示させるには、-aパラメータを使用します。

17.6.4 プロセス:top

コマンド**top** ("table of processes"=プロセステーブルを意味します)は、2秒間隔で更新されるプロセスリストを表示します。プログラムを終了するには、

<Q>キーを押します。**-n 1**パラメータを指定すると、プロセスリストが1回表示された後にプログラムが終了します。次に示すものは、コマンド**top -n 1**の出力例です。

```
tux@mercury:~> top -n 1
top - 17:06:28 up 2:10, 5 users, load average: 0.00, 0.00, 0.00
Tasks: 85 total, 1 running, 83 sleeping, 1 stopped, 0 zombie
Cpu(s): 5.5% us, 0.8% sy, 0.8% ni, 91.9% id, 1.0% wa, 0.0% hi, 0.0% si
Mem: 515584k total, 506468k used, 9116k free, 66324k buffers
Swap: 658656k total, 0k used, 658656k free, 353328k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1	root	16	0	700	272	236	S	0.0	0.1	0:01.33	init
2	root	34	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
3	root	10	-5	0	0	0	S	0.0	0.0	0:00.27	events/0
4	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	khelper
5	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	kthread
11	root	10	-5	0	0	0	S	0.0	0.0	0:00.05	kblockd/0
12	root	20	-5	0	0	0	S	0.0	0.0	0:00.00	kacpid
472	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pdflush
473	root	15	0	0	0	0	S	0.0	0.0	0:00.06	pdflush
475	root	11	-5	0	0	0	S	0.0	0.0	0:00.00	aio/0
474	root	15	0	0	0	0	S	0.0	0.0	0:00.07	kswapd0
681	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	kseriod
839	root	10	-5	0	0	0	S	0.0	0.0	0:00.02	reiserfs/0
923	root	13	-4	1712	552	344	S	0.0	0.1	0:00.67	udevd
1343	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	khubd
1587	root	20	0	0	0	0	S	0.0	0.0	0:00.00	shpchpd_event
1746	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_control
1752	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_bus_master1
2151	root	16	0	1464	496	416	S	0.0	0.1	0:00.00	acpid
2165	messageb	16	0	3340	1048	792	S	0.0	0.2	0:00.64	dbus-daemon
2166	root	15	0	1840	752	556	S	0.0	0.1	0:00.01	syslog-ng
2171	root	16	0	1600	516	320	S	0.0	0.1	0:00.00	klogd
2235	root	15	0	1736	800	652	S	0.0	0.2	0:00.10	resmgrd
2289	root	16	0	4192	2852	1444	S	0.0	0.6	0:02.05	hald
2403	root	23	0	1756	600	524	S	0.0	0.1	0:00.00	hald-addon-acpi
2709	root	19	0	2668	1076	944	S	0.0	0.2	0:00.00	NetworkManagerD
2714	root	16	0	1756	648	564	S	0.0	0.1	0:00.56	hald-addon-stor

topの実行中に<F>キーを押すと、メニューが開き、出力形式を大幅に変更できます。

-U *UID*パラメータを指定すると、特定のユーザに関連したプロセスのみがモニタされます。*UID*は、ユーザのユーザIDに置き換えます。top -U `id -u` は、ユーザ名に基づいてユーザのUIDを返し、そのプロセスを表示します。

17.7 システム情報

17.7.1 システムアクティビティ情報:sar

sarを使用するには、sadc(システムアクティビティデータコレクタ)が動作していなければなりません。これを起動したり、ステータスを確認するには、`rccsysstat {start|status}`を使用します。

sarを利用すれば、CPU、メモリ、IRQ使用状況、I/O、またはネットワークなど、重要な大部分のシステムアクティビティに関するレポートを生成することができます。このコマンドのオプションは、多い上に複雑なためここでは説明しきれません。詳細、およびコマンドの使用例については、該当するマニュアルページを参照してください。

17.7.2 メモリ使用率:free

ユーティリティfreeはRAMの使用状況を検査します。以下の例では、空きメモリと使用済みメモリ(およびスワップ領域)の両方について詳細が示されています。

```
tux@mercury:~> free
```

	total	used	free	shared	buffers	cached
Mem:	515584	501704	13880	0	73040	334592
-/+ buffers/cache:		94072	421512			
Swap:	658656	0	658656			

-b、-k、-m、-gの各オプションは、それぞれバイト、KB、MBまたはGBの出力を表示します。-d delayパラメータを指定すると、表示がdelay秒間隔で確実に更新されます。たとえば、`free -d 1.5`と入力すると1.5秒ごとに更新されます。

17.7.3 ユーザアクセス中ファイル:fuser

現在一定のファイルにアクセスしているプロセスまたはユーザを判別しておくことは有効です。たとえば、/mntにマウントされているファイルシステムをアンマウントするとします。umountでは、「デバイスがビジー」状態が返

されます。ここで次のようにコマンドfuserを使用すると、デバイスにアクセスしているプロセスを判断することができます。

```
tux@mercury:~> fuser -v /mnt/*
```

	USER	PID	ACCESS	COMMAND
/mnt/notes.txt	tux	26597	f....	less

別の端末で実行中であったlessプロセスの終了後は、ファイルシステムを正常にアンマウントできます。

17.7.4 カーネルリングバッファ:dmesg

Linuxカーネルは、リングバッファに一定のメッセージを保持します。これらのメッセージを表示するには、コマンドdmesgを入力します。

```
$ dmesg
[...]
```

end_request: I/O error, dev fd0, sector 0
subfs: unsuccessful attempt to mount media (256)
e100: eth0: e100_watchdog: link up, 100Mbps, half-duplex
NET: Registered protocol family 17
IA-32 Microcode Update Driver: v1.14 <tigran@veritas.com>
microcode: CPU0 updated from revision 0xe to 0x2e, date = 08112004
IA-32 Microcode Update Driver v1.14 unregistered
bootsplash: status on console 0 changed to on
NET: Registered protocol family 10
Disabled Privacy Extensions on device c0326ea0(lo)
IPv6 over IPv4 tunneling driver
powernow: This module only works with AMD K7 CPUs
bootsplash: status on console 0 changed to on

古いイベントは、ファイル/var/log/messagesおよび/var/log/warnに記録されています。

17.7.5 開いているファイルのリスト:lsdf

プロセスIDがPIDのプロセスについて開いている全ファイルのリストを表示するには、-pを使用します。たとえば、現行のシェルで使用されている全ファイルを表示するには、次のように入力します。

```
tux@mercury:~> lsdf -p $$
```

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE	NODE	NAME
bash	5552	tux	cwd	DIR	3,3	1512	117619	/home/tux
bash	5552	tux	rtd	DIR	3,3	584	2 /	


```

bash    5552 tux  txt    REG    3,3  498816  13047 /bin/bash
bash    5552 tux  mem    REG    0,0          0 [heap] (stat: No such
bash    5552 tux  mem    REG    3,3  217016  115687 /var/run/nscd/passwd
bash    5552 tux  mem    REG    3,3  208464  11867  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3  882134  11868  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3  1386997  8837  /lib/libc-2.3.6.so
bash    5552 tux  mem    REG    3,3    13836   8843  /lib/libdl-2.3.6.so
bash    5552 tux  mem    REG    3,3  290856  12204  /lib/libncurses.so.5.5
bash    5552 tux  mem    REG    3,3    26936  13004  /lib/libhistory.so.5.1
bash    5552 tux  mem    REG    3,3  190200  13006  /lib/libreadline.so.5.
bash    5552 tux  mem    REG    3,3     54  11842  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3    2375  11663  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3     290  11736  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3     52  11831  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3     34  11862  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3     62  11839  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3    127  11664  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3     56  11735  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3     23  11866  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3  21544   9109  /usr/lib/gconv/gconv-m
bash    5552 tux  mem    REG    3,3    366   9720  /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3  97165   8828  /lib/ld-2.3.6.so
bash    5552 tux   0u    CHR   136,5          7 /dev/pts/5
bash    5552 tux   1u    CHR   136,5          7 /dev/pts/5
bash    5552 tux   2u    CHR   136,5          7 /dev/pts/5
bash    5552 tux  255u   CHR   136,5          7 /dev/pts/5

```

この例では、値としてシェルのプロセスIDをとる特殊なシェル変数\$\$が使用されています。

パラメータを指定せずにコマンドlsdfを入力すると、現在開いている全ファイルがリストされます。開いているファイルの数が何千にも達することがあるので、そのすべてをリストすることはほとんど無意味です。ただし、開いているすべてのファイルのリストを検索機能と組み合わせて使用すると、役立つリストが生成されます。たとえば、次のように使用されているすべてのキャラクタデバイスのリストを表示します。

```

tux@mercury:~> lsdf | grep CHR
bash    3838    tux    0u    CHR   136,0          2 /dev/pts/0
bash    3838    tux    1u    CHR   136,0          2 /dev/pts/0
bash    3838    tux    2u    CHR   136,0          2 /dev/pts/0
bash    3838    tux   255u   CHR   136,0          2 /dev/pts/0
bash    5552    tux    0u    CHR   136,5          7 /dev/pts/5
bash    5552    tux    1u    CHR   136,5          7 /dev/pts/5
bash    5552    tux    2u    CHR   136,5          7 /dev/pts/5
bash    5552    tux   255u   CHR   136,5          7 /dev/pts/5
X        5646    root  mem    CHR    1,1        1006 /dev/mem
lsdf    5673    tux    0u    CHR   136,5          7 /dev/pts/5
lsdf    5673    tux    2u    CHR   136,5          7 /dev/pts/5

```

```
grep          5674      tux      1u        CHR 136,5          7 /dev/pts/5
grep          5674      tux      2u        CHR 136,5          7 /dev/pts/5
```

17.7.6 カーネルとudevイベントシーケンス ビューア:udevmonitor

udevmonitorは、udevルールから送られてくるカーネルのueventやeventをリスンし、イベントのデバイスパス(DEVPATH)をコンソールに表示します。これはUSBメモリスティックに接続時に発生する一連のイベントです。

```
UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806687] add@/class/scsi_host/host4
UEVENT[1138806687] add@/class/usb_device/usbdev4.10
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806687] add@/class/scsi_host/host4
UDEV [1138806687] add@/class/usb_device/usbdev4.10
UEVENT[1138806692] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806692] add@/block/sdb
UEVENT[1138806692] add@/class/scsi_generic/sg1
UEVENT[1138806692] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806693] add@/class/scsi_generic/sg1
UDEV [1138806693] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/block/sdb
UEVENT[1138806694] add@/block/sdb/sdb1
UDEV [1138806694] add@/block/sdb/sdb1
UEVENT[1138806694] mount@/block/sdb/sdb1
UEVENT[1138806697] umount@/block/sdb/sdb1
```

17.7.7 X11クライアントが使用するサーバリ ソース:xrestop

xrestopは、接続されている各X11クライアントの、サーバ側リソースの統計情報を表示する場合に使用します。出力内容は、17.6.4項「プロセス:top」(375 ページ)とよく似ています。

```
xrestop - Display: localhost:0
Monitoring 40 clients. XErrors: 0
Pixmaps: 42013K total, Other: 206K total, All: 42219K total

res-base Wins GCs Fnts Pxms Misc Pxm mem Other Total PID Identifier
3e00000 385 36 1 751 107 18161K 13K 18175K ? NOVELL: SU
4600000 391 122 1 1182 889 4566K 33K 4600K ? amaroK - S
```

1600000	35	11	0	76	142	3811K	4K	3816K	?	KDE Deskto
3400000	52	31	1	69	74	2816K	4K	2820K	?	Linux Shel
2c00000	50	25	1	43	50	2374K	3K	2378K	?	Linux Shel
2e00000	50	10	1	36	42	2341K	3K	2344K	?	Linux Shel
2600000	37	24	1	34	50	1772K	3K	1775K	?	Root - Kon
4800000	37	24	1	34	49	1772K	3K	1775K	?	Root - Kon
2a00000	209	33	1	323	238	1111K	12K	1123K	?	Trekstor25
1800000	182	32	1	302	285	1039K	12K	1052K	?	kicker
1400000	157	121	1	231	477	777K	18K	796K	?	kwin
3c00000	175	36	1	248	168	510K	9K	520K	?	de.comp.la
3a00000	326	42	1	579	444	486K	20K	506K	?	[opensuse-
0a00000	85	38	1	317	224	102K	9K	111K	?	Kopete
4e00000	25	17	1	60	66	63K	3K	66K	?	YaST Contr
2400000	11	10	0	56	51	53K	1K	55K	22061	suseplugge
0e00000	20	12	1	50	92	50K	3K	54K	22016	kded
3200000	6	41	5	72	84	40K	8K	48K	?	EMACS
2200000	54	9	1	30	31	42K	3K	45K	?	SUSEWatche
4400000	2	11	1	30	34	34K	2K	36K	16489	kdesu
1a00000	255	7	0	42	11	19K	6K	26K	?	KMix
3800000	2	14	1	34	37	21K	2K	24K	22242	knotify
1e00000	10	7	0	42	9	15K	624B	15K	?	KPowersave
3600000	106	6	1	30	9	7K	3K	11K	22236	konqueror
2000000	10	5	0	21	34	9K	1K	10K	?	klipper
3000000	21	7	0	11	9	7K	888B	8K	?	KDE Wallet

17.8 ユーザ情報

17.8.1 実行者と実行内容:w

コマンドwを使用すると、システムにログオンしているユーザと、そのユーザが実行している操作を確認できます。たとえば、次のようにします。

```
tux@mercury:~> w
 16:33:03 up  3:33,  2 users,  load average: 0.14, 0.06, 0.02
USER      TTY      LOGIN@  IDLE   JCPU   PCPU WHAT
tux      :0        16:33   ?xdm?  9.42s  0.15s /bin/sh /opt/kde3/bin/startk
tux      pts/0     15:59    0.00s  0.19s  0.00s w
```

他のシステムのユーザがリモートログインしている場合は、パラメータ-fを指定すると、そのユーザがどのコンピュータから接続を確立したかが出力されます。

17.9 日付と時刻

17.9.1 timeを使用した時間測定

コマンドによる消費時間を判断するには、timeユーティリティを使用します。このユーティリティは、シェルビルトインバージョンとプログラムバージョン(/usr/bin/time)の2種類が用意されています。

```
tux@mercury:~> time find . > /dev/null
```

```
real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

シェルの使用

Linuxシステムを起動すると、通常はグラフィカルユーザインタフェースが使用可能になり、ログイン処理やその後のシステムとのやり取りもこのインタフェースを通じて行われます。グラフィカルユーザインタフェースの重要性は高まり、ユーザにとっても使い易くなりましたが、このインタフェースの使用が、システムとやり取りを行う唯一の方法というわけではありません。通常はシェルと呼ばれる、コマンドを入力できるコマンドラインインタプリタなどのテキストベースのやり取りも可能です。Linuxでは、グラフィカルユーザインタフェースからシェルウィンドウを起動するオプションが提供されているので、両方の方法を簡単に使用できます。

管理面では、シェルベースのアプリケーションは、遅いネットワークリンク上でコンピュータを制御する場合、またはコマンドラインでrootとしてタスクを実行する場合に、特に重要です。Linux「初心者」の方にとっては、シェル内でコマンドを入力することは多少例外的に感じるかもしれませんが、シェルは管理者のみが使用するものではないことがすぐに実感されるはずです。実際の日常業務の中には、シェルを使用することで最も簡単に素早く行えるものがあります。

UNIXまたはLinuxには複数のシェルが用意されています。SUSE® Linux EnterpriseのデフォルトのシェルはBash(GNU Bourne-Again Shell)です。

この章では、シェルを使用する際に知っておく必要のあるいくつかの基本事項を説明します。これには次のトピックが含まれます。コマンドの入力方法、Linuxのディレクトリ構造、ファイルおよびディレクトリ使用方法、および基本機能の使用方法、Linuxにおけるユーザおよび権限の概念、重要なシェルコマンドの概要、およびUnixとLinuxシステムで常に利用可能なデフォルトエディタであるviエディタの簡単な概要などです。

18.1 Bashシェルでの作業開始

Linuxでは、コマンドラインをグラフィカルユーザインタフェースと併用して、簡単にそれらを切り替えることができます。KDEのグラフィカルユーザインタフェースからターミナルウィンドウを起動するには、パネル内の [Konsole] アイコンをクリックします。GNOMEでは、パネル内の [GNOME Terminal] アイコンをクリックします。

KonsoleまたはGNOMEのターミナルウィンドウが表示され、[図18.1. 「Bashのターミナルウィンドウの例」](#) (384 ページ)のように、先頭行にプロンプトが表示されます。通常、プロンプトにはログイン名(この例ではtux)、コンピュータのホスト名(この例ではknox)、および現在のパス(この例ではホームディレクトリ。チルダ記号~)で示されます。リモートコンピュータにログインすると、この情報により、自分が現在作業中のシステムが常に示されます。カーソルがこのプロンプトの右端にあるときは、使用中のコンピュータシステムに対してコマンドを直接入力できます。

図18.1 Bashのターミナルウィンドウの例



18.1.1 コマンドの入力

1つのコマンドは複数の要素によって構成されています。最初の要素は必ず、実際のコマンド自体であり、その後にパラメータまたはオプションが続きます。コマンドを入力し、←、→、<←、Del、およびSpaceキーを使って編集できます。オプションを追加したり、入力ミスを訂正することもできます。コマンドは、<Enter>キーを押すと実行されます。

重要項目: 問題がなければメッセージは表示されません

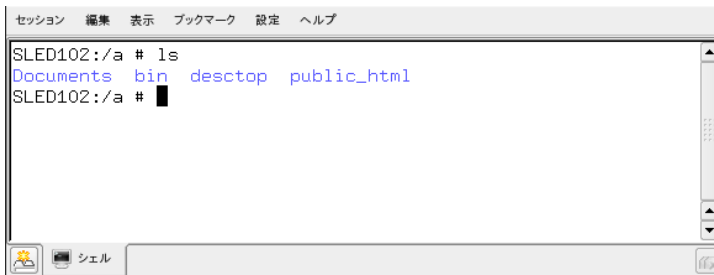
このシェルは詳細ではありません。一部のグラフィカルユーザインタフェースと比較すると、シェルでは通常、コマンドの実行時に確認メッセージが表示されません。メッセージは問題またはエラーが発生した場合にのみ表示されます。

また、オブジェクトを削除するコマンドを実行する際には注意が必要です。rmといったコマンドを入力してファイルを削除する前に、本当にそのオブジェクトを削除するかどうか確認してください。

コマンドの使用(オプションなし)

簡単なコマンド例に基づいて、コマンドの構造を説明します。lsコマンドは、ディレクトリの内容を表示する場合に使用します。コマンドは、オプションと共に使用することも、オプションなしで使用することもできます。引数なしでlsコマンドを入力すると、カレントディレクトリの内容が表示されます。

図 18.2 lsコマンド

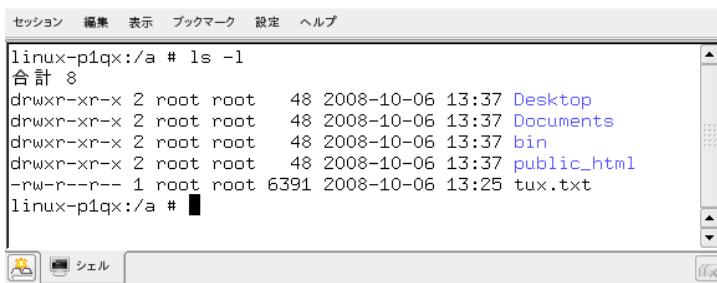


他のOSとは異なり、Linuxでは、ファイルに.txtなどのファイル拡張子を付けることはできますが、必須ではありません。このため、lsのこの出力では、ファイルとフォルダを区別するのが困難です。デフォルトでは、表示項目が色分けされます。通常、ディレクトリは青で、ファイルは黒で表示されます。

コマンドの使用(オプションあり)

ディレクトリの内容に関するより詳細な情報を得るには、`ls`コマンドをオプションの文字列と共に使用するのが適しています。オプションによりコマンドの動作を変更できるので、特定のタスクを実行できます。オプションは空白でコマンドと区切られ、先頭にハイフンが付きます。`ls -l`コマンドは、同じディレクトリの内容を詳しい情報付きで表示します(長いリスト形式)。

図 18.3 `ls -l`コマンド



```
linux-p1qx:/a # ls -l
合計 8
drwxr-xr-x 2 root root  48 2008-10-06 13:37 Desktop
drwxr-xr-x 2 root root  48 2008-10-06 13:37 Documents
drwxr-xr-x 2 root root  48 2008-10-06 13:37 bin
drwxr-xr-x 2 root root  48 2008-10-06 13:37 public_html
-rw-r--r-- 1 root root 6391 2008-10-06 13:25 tux.txt
linux-p1qx:/a #
```

各オブジェクト名の左側に、オブジェクトに関する情報が複数の列で表示されます。大切なのは、1列目には、オブジェクトのファイルタイプが表示されることです(この例では、`d`はディレクトリ、`-`は通常のファイルです)。次の9列には、オブジェクトに対するユーザパーミッションが表示されます。列11および12には、ファイル所有者およびグループの名前が表示されます(この例では、`tux`および`users`)。ユーザパーミッションおよびLinuxのユーザの概念については、「[18.2項「ユーザとアクセス権」](#) (397ページ)」を参照してください。次の列には、ファイルサイズがバイト単位で表示されます。次に、最終変更日時が表示されます。最後の列には、オブジェクト名が表示されます。

さらに詳細な情報を表示する場合は、`ls`コマンドの2つのオプションを組み合わせ、`ls -la`と入力します。こうすると、シェルでディレクトリ内の隠しファイルも表示され、先頭にドットを付けて示されます(`.hiddenfile`など)。

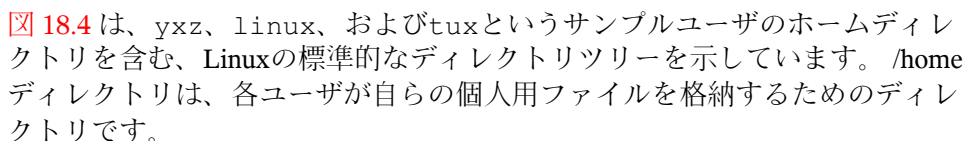
ヘルプの表示

すべてのコマンドのすべてのオプションを暗記する必要はありません。コマンド名は思い出せるのに、オプションがはっきり思い出せないという場合は、

コマンドを入力し、空白を空けて「--help」と入力します。この--helpオプションは、多くのコマンドに存在します。「ls --help」と入力すると、lsコマンドのすべてのオプションが表示されます。

18.1.2 Linuxのディレクトリ構造

シェルでは、ファイルマネージャのツリービューのような、ディレクトリおよびファイルのグラフィカルな概要表示を提供していないので、Linuxシステムのデフォルトのディレクトリ構造の基本を理解しておくと便利です。ディレクトリは、ファイル、プログラム、およびサブディレクトリが保存されている電氣的なフォルダと考えることができます。階層の最上位にあるディレクトリはルートディレクトリであり、/で表されます。ここから、他のすべてのディレクトリにアクセスできます。

 **図 18.4** は、xyz、linux、およびtuxというサンプルユーザのホームディレクトリを含む、Linuxの標準的なディレクトリツリーを示しています。/homeディレクトリは、各ユーザが自らの個人用ファイルを格納するためのディレクトリです。

注意: ネットワーク環境でのホームディレクトリ

ネットワーク環境で作業している場合、ホームディレクトリは/homeと呼ばれない可能性があります。ファイルシステム内の任意のディレクトリに割り当てられている場合があります。

次に、Linux環境内にある標準的なディレクトリに関してリスト形式で簡単に説明します。

図 18.4 標準的なディレクトリツリーの例

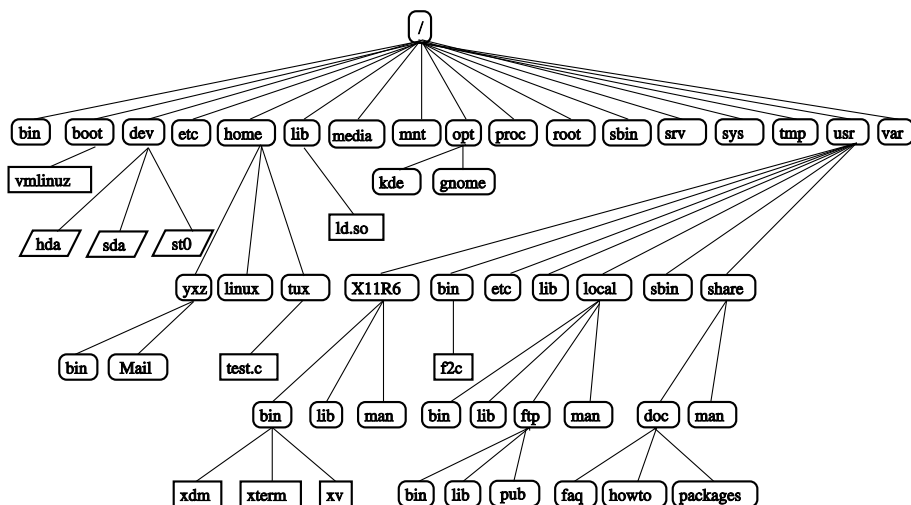


表 18.1 標準的なディレクトリツリーの概要

/	ルートディレクトリ(ディレクトリツリーの開始場所)
/home	ユーザの個人的なディレクトリ
/dev	ハードウェアコンポーネントを表すデバイスファイルを格納するディレクトリ
/etc	システム設定に関する重要なファイルを格納するディレクトリ
/etc/init.d	ブートスクリプトを格納するディレクトリ
/bin、/sbin	ブートプロセス初期に必要なプログラムを格納するディレクトリ(/bin)、および管理者用プログラムを格納するディレクトリ(/sbin)
/usr、/usr/local	すべてのアプリケーションプログラム、およびローカルで配布に依存しない拡張ファイルを格納するディレクトリ(/usr/local)

<code>/usr/bin</code> 、 <code>/usr/sbin</code>	一般的にアクセス可能なプログラムを格納するディレクトリ(<code>/usr/bin</code>)、およびシステム管理者用に予約されているディレクトリ(<code>/usr/sbin</code>)
<code>/usr/share/doc</code>	さまざまなドキュメントファイルを格納するディレクトリ
<code>/tmp</code> 、 <code>/var/tmp</code>	一時ファイルを格納するディレクトリ(不要なファイル以外はこのディレクトリに保存しないでください)
<code>/opt</code>	オプションのソフトウェア、たとえば大規模なアドオンプログラムパッケージ(KDE、GNOME、Netscapeなど)を格納するディレクトリ
<code>/proc</code>	プロセスファイルシステムを格納するディレクトリ
<code>/sys</code>	カーネルに関するすべてのデバイス情報が集められる「system」ファイルシステムを格納するディレクトリ
<code>/var/log</code>	システムログファイルを格納するディレクトリ

18.1.3 ディレクトリおよびファイルの使用

特定のファイルまたはディレクトリを指定するには、そのディレクトリまたはファイルへのパスを指定する必要があります。パスを指定するには、次の2つの方法があります。

- ルートディレクトリから該当するファイルへの完全(絶対)パス
- カレントディレクトリから始まるパス(相対パス)

絶対パスの先頭には必ずスラッシュが付きます。相対パスの先頭にはスラッシュは付きません。

注意: Linuxでは大文字と小文字が区別されます

Linuxでは、ファイルシステム内で大文字と小文字が区別されます。たとえば、「test.txt」または「Test.txt」と入力すると、Linuxでは区別さ

れます。ファイル名またはパスを入力する場合は、この点に注意してください。

ディレクトリ変更するには、`cd`コマンドを使用します。

- ホームディレクトリに切り替えるには、`cd`を入力します。
- カレントディレクトリは、ドット(`.`)で表します。).これは、他のコマンド(`cp`、`mv`、...など)を利用する場合に役立ちます。
- ツリー内で、それよりすぐ上にあるレベルは、2つのドット(`..`)で表します。).たとえば、カレントディレクトリの親ディレクトリに切り替えるには、`cd ..`を入力します。

ファイル指定の例

の`cd`コマンドでは、相対パスを使用しています。**18.1.3項「ディレクトリおよびファイルの使用」**(389ページ)絶対パスも使用できます。たとえば、ホームディレクトリから`/tmp`のサブディレクトリにファイルをコピーするとします。

- 1 まず、ホームディレクトリから、`/tmp`内にサブディレクトリを作成します。
 - 1a カレントディレクトリがホームディレクトリではない場合は、「`cd ~`」と入力してホームディレクトリに切り替えます。「`cd ~`」と入力すると、ファイルシステム内の任意の場所からホームディレクトリに戻ることができます。
 - 1b ホームディレクトリで、「`mkdir /tmp/test`」と入力します。`mkdir`は「**make directory** (ディレクトリ作成)」の略です。このコマンドでは、`test`という名前の新しいディレクトリが`/tmp`ディレクトリ内に作成されます。この場合は、絶対パスを使用してディレクトリが作成されます。
 - 1c 何が行われたのかを確認するために、「`ls -l /tmp`」と入力します。新しいディレクトリ`test`が、`/tmp`ディレクトリの内容の一覧に表示されます。

2 次に、ホームディレクトリ内に新しいファイルを作成し、そのファイルを相対パスを使用して/tmp/testディレクトリにコピーします。

2a 「touch myfile.txt」と入力します。touchコマンドとmyfile.txtオプションを使用すると、myfile.txtという名前の新しい空のファイルがカレントディレクトリ内に作成されます。

2b 「ls -l」と入力して、このことを確認します。新しいファイルが内容の一覧に表示されます。

2c 「cp myfile.txt ../tmp/test」と入力します。こうすると、myfile.txtがファイル名を変更せずに、ディレクトリ/tmp/testにコピーされます。

2d 「ls -l /tmp/test」と入力して、このことを確認します。ファイルmyfile.txtが、/tmp/testの内容の一覧に表示されます。

他のユーザのホームディレクトリの内容をリストするには、「ls ~username」と入力します。で例となっているディレクトリツリーでは、サンプルユーザの1人が図 18.4. 「標準的なディレクトリツリーの例」 (388 ページ)tuxという名前です。この場合、ls ~tuxと入力すると、tuxのホームディレクトリの内容をリストできます。

注意: ファイル名またはディレクトリ名での空白の扱い

ファイル名にスペースが含まれている場合には、空白の前にバックスラッシュ(\)を使用してスペースをエスケープするか、ファイル名を一重または二重引用符で囲ってください。そうしないと、バッシュは、My Documentsのようなファイル名を、2つのファイルまたはディレクトリ名と解釈します。一重および二重引用符の違いは、二重引用符の場合には変数の展開が行われるという点にあります。一重引用符を使えば、シェルは、囲まれた文字列をそのまま用います。

18.1.4 シェルの便利な機能

Bashでコマンドを入力する場合は、入力に手間がかかります。次に、作業をより簡略化して入力の手間を省くことができるBashの機能をいくつか紹介します。

履歴および補完

デフォルトでは、入力したコマンドはBashに「記憶」されています。この機能は履歴と呼ばれます。以前に入力したコマンドを再実行する場合は、そのコマンドがプロンプト上に表示されるまで、↑キーを押します。キーを押すと、以前に使用したコマンドが逆方向に順番に表示されます。↓次のキーCtrl + Rを使用すると、履歴を検索することができます。

選択したコマンドはいつでも編集できます。たとえば、ファイルの名前を変更してから、Enterキーを押してコマンドを実行します。コマンドラインを編集するには、矢印キーを使用して希望の場所までカーソルを移動し、編集を行います。

ファイル名またはディレクトリ名の最初の数文字を入力した後で、その名前全体を補完できるのが、Bashのもう1つの便利な機能です。これを行うには、最初の数文字を入力してから<<Tab>>キーを押します。ファイル名またはパスが一意に識別された場合は、一度で補完され、カーソルはファイル名の末尾に移動します。次に、必要に応じて、コマンドの次のオプションを入力します。ファイル名またはパスが一意に識別されない場合は(同じ数文字で始まるファイル名はいくつもあります)、ファイル名またはパスは可能な部分まで補完され、そこから複数のオプションから選択します。もう一度<<Tab>>キーを押すと、それらのリストが表示されます。この後、ファイルまたはパスの次の数文字を入力し、<<Tab>>キーを押して再び補完を試みます。を使用してファイル名およびパスを補完したら、入力したいファイルまたはパスが実際に存在するかどうかを同時に確認できます(スペルが正しいかどうかも確認できます)。<Tab>

ワイルドカード

このシェルは、パス名を展開するためのワイルドカードという、もう1つの規則も用意しています。ワイルドカードは、他の文字を表す文字です。バッシュでは、次のような3種類のワイルドカードを利用できます。

?

任意の1文字に対応します。

*

任意の数文字に対応します。

[set]

角かっこの中で指定されたグループのうち、どれか1つの文字に対応します。ここでは、`set`という文字列で代替しています。`set`の一部として、`[:class:]`という構文で、文字のクラスを指定することができます。ここで`class`は、`alnum` (英数字)、`alpha` (英字)、`ascii` (ASCII文字)などのいずれかです。

使用`!`または`^`をグループの先頭で使用した場合(`!set`)、`set`で識別されるもの以外の1文字にマッチします。

たとえば、`test`ディレクトリの中に、`Testfile`、`Testfile1`、`Testfile2`、および`datafile`ファイルがある場合を考えてみましょう。

- 「`ls Testfile?`」と入力すると、`Testfile1`と`Testfile2`が表示されます。
- 「`ls Testfile?`」と入力すると、`Testfile1`と`Testfile2`が表示されます。
- 「`ls Test*`」と入力すると、`Testfile`も表示されます。
- 「`ls *fil*`」と入力すると、すべてのサンプルファイルが表示されます。
- 最後の文字が数字のすべてのサンプルファイルに対処するには、`set`ワイルドカードを使用します。たとえば、「`ls Testfile[1-9]`」またはクラスを使って「`ls Testfile[:digit:]`」のように指定します。

これら4種類のワイルドカードのうち、最も包括性が高いのは、アスタリスク(*)です。1つのコマンドを実行するだけで、あるディレクトリ内に含まれているすべてのファイルを他のディレクトリへコピー、またはすべてのファイルを削除することができます。たとえば、`rm *fil*`コマンドは、カレントディレクトリ内で、`fil`という文字列をファイル名の一部として使用しているすべてのファイルを削除します。

lessおよびmoreによるファイルの表示

Linuxには、テキストファイルをシェル内で直接表示するlessとmoreの2つの小さなプログラムが付属しています。エディタを起動してReadme.txtのようなファイルを読み取る代わりに、less Readme.txtコマンドを入力して、テキストをコンソールウィンドウ内で表示します。<Space>キーを押すと、1ページ下へスクロールします。Page UpとPage Downを使用すると、テキスト内を前方または後方へ移動できます。lessを終了するには、Qを押します。

lessの代わりに、それより古いプログラムであるmoreを使用することもできます。しかし、後方(上)へのスクロールができないので、利便性は劣ります。

lessプログラムは、*less is more*(少ない方が豊か)ということわざに由来する名前であり、他のコマンドの出力を便利な方法で表示する目的で使用することもできます。このコマンドの機能について理解するには、「[リダイレクトとパイプ項 \(394 ページ\)](#)」を参照してください。

リダイレクトとパイプ

通常、シェル内の標準出力は画面またはコンソールウィンドウであり、標準入力キーボードです。ただし、シェルには、入力または出力をファイルまたは別のコマンドとして別のオブジェクトにリダイレクトする機能が用意されています。たとえば、>および<の記号を使用すると、コマンドの出力をファイルに転送したり(出力リダイレクト)、ファイルをコマンドの入力として使用したりできます(入力リダイレクト)。たとえば、lsなどのコマンドの出力をファイルに書き込む場合は、「ls -l > file.txt」と入力します。こうすると、file.txtという名前のファイルが作成され、このファイルにはlsコマンドによって生成されたカレントディレクトリの内容の一覧が含まれます。ただし、file.txtという名前のファイルが既に存在する場合は、このコマンドを実行すると既存のファイルが上書きされます。それを避けるには、>>を使用します。「ls -l >> file.txt」と入力すると、lsコマンドの出力が、file.txtという名前の既存のファイルに単に追加されます。ファイルが存在しない場合は作成されます。

ファイルをコマンドの出力として使用すると便利な場合もあります。たとえば、trコマンドを使用すると、ファイルからリダイレクトされた文字を置換して、その結果を標準の出力である画面上に書き込むことができます。たと

えば、上記の例で、`file.txt`の文字`t`をすべて`x`に置換して、これを画面に出力するとします。それには、「`tr t x < file.txt`」と入力します。

標準出力と同様、標準エラー出力も画面へ送信されます。標準エラー出力を `errors` というファイルへリダイレクトするには、該当のコマンドに対して `2> errors` を指定します。 `>&alloutput` を追加した場合は、標準出力と標準エラー出力の両方が、`alloutput` という 1 つのファイルに保存されます。

パイプラインまたはパイプもリダイレクトの一種ですが、パイプの使用はファイルに限りません。パイプ(`|`)を使用すると、1つのコマンドの出力を次のコマンドの入力として使用して、複数のコマンドを組み合わせることができます。たとえば、`less`でカレントディレクトリの内容を表示するには、「`ls | less`」と入力します。これらの組み合わせに意味があるのは、`ls` コマンドによる通常の出力が非常に長い場合だけです。たとえば、`ls /dev` コマンドを使用して `dev` ディレクトリの内容を表示する場合、参照できるのは、ウィンドウ内に表示されているわずかな部分だけです。`ls /dev | less` コマンドを使用すると、リスト全体を参照できます。

18.1.5 アーカイブとデータ圧縮

ここまでで、多くのファイルとディレクトリを作成しました。次に、アーカイブとデータ圧縮について説明します。ここでは、`test` ディレクトリ全体をパックして1つのファイルに記録し、そのファイルのバックアップコピーをフロッピーディスクに保存するか、電子メールで送信できるようにしたいと思います。この作業を行うには、`tar` (*tape archiver*の略称)コマンドを使用します。`tar --help` コマンドを使用すると、`tar` コマンドのすべてのオプションを表示できます。これらのオプションのうち、重要度の高いものを以下で説明します。

`-c`

(createの略)新しいアーカイブを作成します。

`-t`

(tableの略)新しいアーカイブの目次(table of contents)を作成します。

`-x`

(extractの略)アーカイブをアンパック(展開)します。

-v

(verboseの略)アーカイブの作成中に、すべてのファイルを画面に表示します。

-f

(fileの略)アーカイブファイルに割り当てるファイル名を指定します。アーカイブを作成する場合、このオプションを最後に指定する必要があります。

testディレクトリ、およびその中のすべてのファイルとサブディレクトリをアーカイブtestarchive.tarに保存するには、次の手順に従ってください。

- 1 シェルを開きます。
- 2 cdコマンドで、ホームディレクトリに移動します。ここに、testディレクトリがあります。
- 3 tar -cvf testarchive.tar testを入力します。-cオプションは、アーカイブを作成する場合に使用します。アーカイブは、-fオプションに指定されたファイル名で作成されます。-vオプションを指定すると、処理中にそのファイル名が表示されます。
- 4 tar -tf testarchive.tarコマンドを使用して、このアーカイブファイルの内容を表示できます。

testディレクトリ、およびその配下のすべてのファイルとディレクトリは、そのままハードディスク上に残ります。このアーカイブをアンパック(展開)するには、tar -xvf testarchive.tarコマンドを入力します。しかし、今の時点では、このコマンドを実行しないでください。

ファイル圧縮の場合、よく使われるのはgzipです。bzip2を使えば、さらに圧縮率が良くなります。「gzip testarchive.tar」と入力します(または「bzip2 testarchive.tar」と入力することもできますが、この例ではgzipを使用します)。lsコマンドを使用すると、testarchive.tarが存在しなくなっていること、代わりにtestarchive.tar.gzが作成されたことがわかります。このファイルはかなり小さいので、電子メールによる転送やUSBメモリへの保存に適しています。

次に、以前に作成したtest2ディレクトリ内で、このファイルをアンパック(圧縮解除)してみます。この作業を行うには、`cp testarchive.tar.gz test2`と入力し、このファイルを上記のディレクトリへコピーします。`cd test2`コマンドを使用して、そのディレクトリへ移動します。拡張子が.tar.gzの圧縮済みアーカイブをunzipするには、gunzipコマンドを使用します。`gunzip testarchive.tar.gz`と入力します。その結果、testarchive.tarを取り出すことができます。このファイルは、`tar -xvf testarchive.tar`コマンドを使用して展開、または圧縮解除(*tar解除*)する必要があります。unzipと圧縮アーカイブの展開は、`tar -xvf testarchive.tar.gz`で一度に行うこともできます(-zオプションの追加は、必要なくなりました)。lsコマンドを使用すると、新しいtestディレクトリが作成されたことを確認できます。その内容は、自分のホームディレクトリ内にあるtestディレクトリとまったく同じものです。

18.1.6 クリーンアップ

この入門コースで、Linuxのシェル、言い換えるとコマンドラインの基本について理解できたはずです。rmとrmdirコマンドを使用して、テスト用のさまざまなファイルとディレクトリを削除することにより、自分のホームディレクトリをクリーンアップすることもできます。には、最も重要なコマンドと、それらの機能についての簡単な説明が記されています。[18.3項「Linuxの重要なコマンド」](#) (402 ページ)

18.2 ユーザとアクセス権

1990年代初期の開始以来、Linuxはマルチユーザシステムとして開発が進められてきました。任意の数のユーザがLinux上で同時に作業することができます。ユーザは各自のワークステーションでセッションを開始する前に、システムにログインする必要があります。各ユーザは、各自のユーザ名およびそれに対応するパスワードを持っています。このようにユーザが区別されているので、権限のないユーザが、アクセス権のないファイルを表示できないことが保証されています。新しいプログラムをインストールするなど、より大きな変更をシステムに加える作業は、一般のユーザは通常は実行できないか、制約を加えられています。rootユーザ、またはスーパーユーザだけが、システムに変更を加える制限なしの権限と、すべてのファイルに対する制限なしのアクセス権を持っています。この概念を理解した上で、必要な場合にのみroot

ユーザでログインし、完全なアクセス権を使用することが求められます。その結果、意図せずにデータを失うリスクを軽減することができます。一般的な状況では、システムファイルの削除やハードディスクのフォーマットを実行できるのはrootユーザだけです。そのため、一般ユーザとしてログインしていれば、トロイの木馬や、破壊的なコマンドを誤って入力することに起因する脅威を大幅に軽減できます。

18.2.1 ファイルシステムのパーミッション

基本的に、Linuxファイルシステム内にある各ファイルは、1人のユーザと1つのグループに所属しています。この所有グループと他のすべてのユーザに対して、これらのファイルへの書き込み、読み取り、または実行を許可することができます。

この状況では、グループとは、特定のいくつかの権利を共通に持つ、互いに関連付けられた一連のユーザと定義することができます。たとえば、あるプロジェクトに携わっているグループをproject3と呼ぶことにします。Linuxシステム内のあらゆるユーザは、少なくとも1つの所有グループ、通常はusersグループのメンバに所属します。1つのシステム内に、必要に応じてグループをいくつか作成してもかまいませんが、グループを追加できるのはrootユーザだけです。どのユーザも、groupsコマンドを使用して、自分が所属しているグループを確認することができます。

ファイルアクセス

ファイルシステム内でのパーミッション(アクセス権)の編成は、ファイルごと、ディレクトリごとに異なります。ファイルのパーミッション情報は、ls -lコマンドを使用して表示できます。出力例については、[例18.1. 「ファイルパーミッションを示すサンプル出力」](#) (398 ページ)を参照してください。

例 18.1 ファイルパーミッションを示すサンプル出力

```
-rw-r----- 1 tux project3 14197 Jun 21 15:03 Roadmap
```

3番目の列が示しているように、このファイルはユーザtuxに所属しています。また、このファイルはグループproject3に対して割り当てられています。Roadmapファイルのユーザパーミッションを調べるには、最初の列を詳細に検討する必要があります。

-	rw-	r--	---
タイプ	ユーザパーミッ ション	グループパーミッ ション	他のユーザのパー ミッション

この列は、先頭に1つの文字があり、その後に3文字ずつ3つのブロック、つまり9つの文字が続く構成です。10文字のうち最初の1文字は、ファイルシステムコンポーネントのタイプを表す略称です。ダッシュ(-)は、これがファイルであることを意味します。ディレクトリ(d)、リンク(l)、ブロックデバイス(b)、またはキャラクタデバイスが代わりに表示されることもあります。

続く3つのブロックは、標準的なパターンに従っています。各ブロックの最初の文字は、ファイルが読み取り可能(r)またはそうでないこと(-)を意味します。中間の位置にあるwは、対応するオブジェクトが編集可能であることを示し、ダッシュ(-)であれば、ファイルへの書き込みが不可能であることを意味します。3番目の位置にあるxは、そのオブジェクトが実行可能であることを意味します。この例のファイルはテキストファイルなので、実行可能ではありません。したがって、この特定のファイルに対する実行可能アクセス権は必要ありません。

この例では、tuxはRoadmapファイルの所有者として、読み取りアクセス権(r)および書き込みアクセス権(w)を持っていますが、このファイルを実行する(x)ことはできません。project3グループのメンバは、このファイルを読み取ることはできますが、変更や実行はできません。他のユーザは、このファイルに対するアクセス権が何もありません。他のパーミッションは、アクセス制御リスト(ACL)を使用して割り当てることができます。

ディレクトリ

ディレクトリに対応するアクセス権は、タイプがdと表示されています。ディレクトリの場合、個別のパーミッションは、やや異なる意味を持ちます。

例 18.2 ディレクトリパーミッションを示すサンプル出力

```
drwxrwxr-x 1 tux project3 35 Jun 21 15:15 ProjectData
```

では、ディレクトリ例 18.2. 「ディレクトリパーミッションを示きサンプル出力」 (399 ページ)ProjectDataの所有者 (tux) と所有グループ (project3) を簡単に識別できます。ファイルアクセス (398 ページ)で説明したファイルのアクセス権(パーミッション)とは異なり、読み取りアクセス権(r)を持つことは、ディレクトリの内容を表示できることを意味します。書き込みアクセス権(w)の場合は、新しいファイルを作成できることを意味します。実行可能アクセス権(x)の場合は、ユーザがこのディレクトリに変更を加えられることを意味します。上記の例では、ユーザtuxとproject3グループのメンバがProjectDataディレクトリに変更を加え(x)、内容を表示し(r)、このディレクトリにファイルを追加する(w)ことができることを表します。一方、他のユーザに対して与えられているのは、それより少ないアクセス権です。このディレクトリにアクセスし(x)、内容を閲覧する(r)ことはできますが、新しいファイルを作成する(w)ことはできません。

18.2.2 ファイルパーミッションの変更

アクセス権の変更

ファイルまたはディレクトリに対するアクセス権を変更できるのは、所有者とrootユーザです。chmodコマンドで、パーミッションを変更するパラメータと1つ以上のファイル名を指定することにより変更します。パラメータは、次のカテゴリに分けられます。

1. 対象ユーザ

- u (ユーザ)-ファイルの所有者
- g (グループ)-ファイルの所有者が所属するグループ
- o (その他)-その他のユーザ(パラメータが何も指定されていない場合、変更はすべてのカテゴリに対して適用されます)

2. 削除(-)、設定(=)、または挿入(+)を表す文字

3. 略称

- r—読み込み
- w—書き込み

- x—実行

4. 空白によって区切られた1つ以上のファイル名

たとえば、例 18.2. 「ディレクトリパーミッションを示すサンプル出力」(399 ページ)で、tuxユーザが、その他のユーザに対してProjectDataディレクトリへの書き込み(w)アクセス権を許可する場合、`chmod o+w ProjectData`コマンドを使用します。

また、自分以外のユーザに対する書き込みパーミッションを拒否する場合は、`chmod go-w ProjectData`コマンドを入力します。すべてのユーザに対して、ProjectDataディレクトリに新しいファイルを追加することを禁止するには、`chmod -w ProjectData`と入力します。また、たとえ所有者でも、書き込みパーミッションを再確立しない限り、ディレクトリ中に新たなファイルを作成できなくなりました。

所有に関するパーミッションの変更

ファイルシステムコンポーネントの所有に関するパーミッションを制御する他の重要なコマンドは、`chown(change owner)`コマンドと`chgrp(change group)`コマンドです。`chown`コマンドを使用すると、ファイルの所有権を他のユーザに移すことができます。しかし、このような変更を行うことができるのは、rootユーザだけです。

今度は、例 18.2. 「ディレクトリパーミッションを示すサンプル出力」(399 ページ)のRoadmapのファイル所有権を、tuxではなく、ユーザのgeekoに与える場合を考えてみましょう。この場合、rootは「`chown geeko Roadmap`」と入力する必要があります。

`chgrp`コマンドは、ファイル所有者の所属グループを変更します。ただし、そのファイルの所有者は、新しいグループのメンバでなければなりません。この方法により、例 18.1. 「ファイルパーミッションを示すサンプル出力」(398 ページ)のtuxユーザは、`chgrp project4 ProjectData`コマンドを使用して、ProjectDataファイル所有者の所属グループをproject4に切り替えることができます。ただし、このユーザが、この新しいグループのメンバであることが条件です。

18.3 Linuxの重要なコマンド

このセクションでは、重要なコマンドについて説明していきます。この章に掲載した以外にも、多くのコマンドがあります。個別のコマンドとそのパラメータを掲載し、必要な場合は一般的なサンプルアプリケーションを紹介します。さまざまなコマンドの詳細については、マニュアルページ(manページ)を参照してください。manの後にコマンド名、たとえば、`man ls`と入力すると、そのコマンドのマニュアルページを表示できます。

manページでは、<PgUp>キーと<PgDn>キーを使用して上下に移動できます。<Home>キーと<End>キーを使用すると、それぞれドキュメントの最初と最後に移動できます。<Q>キーを押すと、この表示モードが終了します。manコマンド自体の詳細については、`man man`と入力します。

以下の概要では、各コマンド要素を本文とは異なる書体で表記しています。実際のコマンド名とその必須オプションは、`command option`の形式で表記します。必須ではない詳細指定やパラメータは、`[]`(角かっこ)内で表記します。

設定値は、実際の状況に合わせて変更してください。`ls file`という入力は、`file`というファイルが実際に存在している場合以外は、意味がありません。ほかに、通常は、複数のパラメータを組み合わせることができます。たとえば、`ls -l -a`の代わりに、`ls -la`と入力することができます。

18.3.1 ファイル関連コマンド

以降のセクションでは、ファイル管理に使用する非常に重要なコマンドについて説明します。一般的なファイル管理からファイルシステムのACL操作まであらゆる事柄を説明します。

ファイル管理

`ls[options][files]`

パラメータなしでlsコマンドを実行した場合、このプログラムはカレントディレクトリの内容を短い形式でリストします。

-l
詳しいリストを表示します。

-a
隠しファイルを表示します。

cp [options] source target
sourceをtargetにコピーします。

-i
必要な場合、つまりtargetfileが既に存在し、そのファイルへ上書きする場合は、確認を求めます。

-r
再帰コピーを行います(サブディレクトリもコピーします)。

mv [options] source target
sourceをtargetへコピーし、元のsourceを削除します。

-b
移動する前に、sourceのバックアップコピーを作成します。

-i
必要な場合、つまりtargetfileが既に存在し、そのファイルへ上書きする場合は、確認を求めます。

rm [options] files
指定されたファイルをファイルシステムから削除します。-rオプションを指定しない限り、rmコマンドを使用してディレクトリを削除することはできません。

-r
既存のサブディレクトリをすべて削除します。

-i
各ファイルを削除する前に、確認を求めます。

ln [options] source target
sourceからtargetへの内部リンクを作成します。通常、このリンクは、同じファイルシステム上のsourceを直接指しています。しかし、-sオブ

ションを指定してlnコマンドを実行した場合、このコマンドは、sourceが存在しているディレクトリを指すだけのシンボリックリンクを作成します。その結果、ファイルシステム間でのリンクが可能になります。

-s

シンボリックリンクを作成します。

cd [options] [directory]

カレントディレクトリを変更します。cdコマンドにパラメータを指定しない場合、そのユーザのホームディレクトリへ移動します。

mkdir [options] directory

新しいディレクトリを作成します。

rmdir [options] directory

指定されたディレクトリがすでに空である場合、そのディレクトリを削除します。

chown [options] username[:[group]] files

ファイルの所有権を、指定されたユーザ名を持つユーザへ移動します。

-R

すべてのサブディレクトリ内にあるファイルとディレクトリを変更します。

chgrp [options] groupname files

特定のfileに対するグループ所有権を、指定されたグループ名を持つグループへ移動します。ファイル所有者は、現在のグループと新しいグループ両方のメンバーである場合に限り、グループ所有権を変更できます。

chmod [options] mode files

アクセス権を変更します。

modeパラメータは、「group」、「access」、および「access type」の3つの部分に分けられます。groupには、次の文字を指定できます:

u

ユーザ

g
グループ

o
その他

access(アクセス)は、+でアクセスを許可し、-でアクセスを拒否します。

accesstype (アクセスタイプ)を制御するには、次のオプションを使用します。

r
読み込み

w
書き込み

x
実行—ファイルを実行したり、ディレクトリを変更します

s
uidビットの設定—あたかもファイルの所有者が起動したかのように、アプリケーションまたはプログラムを起動します。

代わりに、数値コードを使用することもできます。このコードを構成する4桁の各数字は、4、2、および1の中から状況に応じて選択された値を合算したものですつまり、2進(バイナリ)マスクの合計を10進表記したものです。最初の桁で、設定するユーザID(set user ID、SUID)(4)、設定するグループID(2)、およびスティッキー(sticky)(1)の各フラグを設定します。2番目の桁で、ファイルの所有者に割り当てるアクセス権を定義します。3番目の桁で、グループメンバーに割り当てるアクセス権を定義します。最後の桁では、他のすべてのユーザに割り当てるアクセス権を設定します。読み取りアクセス権を設定するには4、書き込みアクセス権を設定するには2、およびファイルの実行アクセス権を設定するには1を使用します。ファイルの所有者の場合、通常は6または7が実行可能ファイルに指定されます。

gzip [parameters] files

このプログラムは、複雑な算術アルゴリズムを使用して、ファイルの内容を圧縮します。この方法で圧縮されたファイルは.gz拡張子を割り当てら

れ、使用する前に圧縮解除する必要があります。複数のファイルまたはディレクトリ全体を圧縮するには、tarコマンドを使用します。

-d

パックされたgzipファイルを圧縮解除して元のサイズに戻し、通常の方法で処理できるようにします(gunzipコマンドに似ています)。

tar options archive files

tarコマンドは、1つ以上のファイルを1つのアーカイブ内に格納します。圧縮はオプションです。tarコマンドは、多くのオプションを持つ、かなり複雑なコマンドです。使用頻度の高いオプションは、以下のとおりです。

-f

出力を画面ではなくファイルに書き込みます。これは一般的な使用方法です。

-c

新しいtarアーカイブを作成します。

-r

既存のアーカイブにファイルを追加します。

-t

アーカイブの内容を出力します。

-u

ファイルを追加する際に、対応するファイルが既にアーカイブ内に存在している場合、追加するファイルがアーカイブ内のファイルより新しければ追加します。

-x

アーカイブ内のファイルをアンパック(展開)します。

-z

生成されたアーカイブを、gzipコマンドを使用してパックします。

-j

生成されたアーカイブを、bzip2コマンドを使用して圧縮します。

-v

処理されたファイルをリストします。

tarコマンドが作成したアーカイブファイルの最後には、.tarが付きます。gzipコマンドを使用してtarアーカイブを圧縮した場合、ファイル名の最後は.tgzまたは.tar.gzになります。bzip2コマンドを使用して圧縮した場合、ファイル名の最後は.tar.bz2になります。

locate patterns

このコマンドはfindutils-locateパッケージをインストールした場合にのみ、利用できます。locateコマンドは、指定されたファイルが存在するディレクトリを検索できます。必要に応じて、ワイルドカードを使用して、ファイル名を指定することができます。このプログラムは(ファイルシステム全体を検索する代わりに)専用に作成したデータベースを使用するので、非常に高速です。この事実は、欠点にもつながります。データベースの最後の更新後に作成されたファイルをlocateで見つけることはできません。このデータベースを生成するには、rootユーザでupdatedbコマンドを使用します。

updatedb [options]

このコマンドは、locateコマンドが使用するデータベースを更新します。既存のすべてのディレクトリ内にあるファイルをこのデータベースに登録するには、rootユーザでこのプログラムを実行します。アンパサンド(&)を追加してこのプログラムをバックグラウンドで実行することには、意味があります。その場合、同じコマンドライン(updatedb &)上で、直ちに作業を続けることができるからです。このコマンドは通常、毎日cronジョブとして実行します(cron.dailyを参照してください)。

find [options]

findコマンドを使用すると、特定のディレクトリ内でファイルを検索することができます。最初の引数は、検索を開始するディレクトリを指定します。-nameオプションの後には、検索文字列を指定する必要があります。その中でワイルドカードを使用することもできます。データベースを使用するlocateとは異なり、findコマンドは実際のディレクトリを検索します。

ファイルの内容にアクセスするコマンド

`file [options] [files]`

`file`は、指定されたファイル内の内容を検出します。

`-Z`

圧縮されたファイル内を検索しようとします。

`cat [options] files`

`cat`コマンドは、ファイルの内容を表示します。特に、ファイルの内容全体を、一時停止なしで画面に出力します。

`-n`

出力の左マージンに、行番号を表示します。

`less [options] files`

このコマンドは、指定されたファイルの内容を閲覧する目的で使用できます。<PgUp>キーと<PgDn>キーを使用して画面を半ページだけ上または下にスクロールすることや、<Space>キーを使用して画面1ページ分を下に移動することができます。<Home>キーと<End>キーを使用すると、ファイルの最初または最後に移動できます。<Q>キーを押すと、このプログラムが終了します。

`grep [options] searchstring files`

`grep`コマンドは、指定された1つ以上のファイルの中で、特定の検索文字列を見つけます。検索文字列が見つかった場合、`searchstring`を含む行と該当のファイル名が表示されます。

`-i`

大文字と小文字を区別しません。

`-H`

該当するファイルの名前だけを表示し、テキスト行を表示しません。

`-n`

文字列が見つかった行の行番号も追加で表示します。

`-l`

`searchstring`を含んでいないファイルの名前だけを出力します。

`diff [options] file1 file2`

diffコマンドは、指定された2つのファイルの内容を比較します。このプログラムの出力は、一致していないすべての行をリストします。プログラマがソースコード全体ではなく、プログラムの変更箇所だけを送信する必要が生じた場合に、このコマンドがよく使用されます。

`-q`

2つのファイルに違いがあるかどうかだけを報告します。

`-u`

統合された「diffを出力します。出力がより読みやすくなります。」

ファイルシステム

`mount [options] [device] mountpoint`

このコマンドを使用すると、ハードディスク、**CD-ROM**ドライブ、および他のドライブなど、あらゆるデータメディアを、**Linux**ファイルシステムのディレクトリにマウントすることができます。

`-r`

読み取り専用でマウントします。

`-t filesystem`

ファイルシステムを指定します。最も一般的なのは、**Linux**ハードディスクを表す**ext2**、**MS-DOS**メディアを表す**msdos**、**Windows**ファイルシステムを表す**vfat**、および**CD**を表す**iso9660**です。

`/etc/fstab`ファイル内で定義されていないハードディスクについては、デバイスタイプも指定する必要があります。この場合、マウントを実行できるのはrootユーザだけです。他のユーザがファイルシステムをマウントする必要がある場合、`/etc/fstab`ファイル内の該当行にuserオプションを入力し、その変更結果を保存します。複数のユーザを指定する場合はカンマ(,)で区切ります。詳細については、`mount (1)`のmanページを参照してください。

`umount [options] mountpoint`

このコマンドは、マウント済みドライブをファイルシステムからマウント解除(アンマウント)します。データの損失を防止するために、リムーバブルデータメディアをドライブから取り出す前に、このコマンドを実行して

ください。通常、mountコマンドとumountコマンドを実行できるのはrootユーザだけです。他のユーザもこれらのコマンドを実行できるようにするには、/etc/fstabファイルを編集し、該当するドライブに対してuserオプションを指定します。

18.3.2 システム関連コマンド

以降の項では、システム情報を検索し、プロセスとネットワークの制御のために必要な最も重要なコマンドのいくつかについて説明します。

システム情報

df [options] [directory]

df (disk free) コマンドをオプションなしで使用した場合、マウント済みのすべてのドライブに関する全ディスク容量、現在使用中のディスク容量、および空き容量を表示します。ディレクトリを指定した場合、そのディレクトリの配置先ドライブに関する情報だけが表示されます。

-h

使用中のブロック数を、ギガバイト(GB)、メガバイト(MB)、またはキロバイト(KB)単位で表示します。一般的に読みやすい形式です。

-T

ファイルシステムのタイプ(ext2、nfsなど)を表示します。

du [options] [path]

このコマンドをパラメータなしで実行した場合、カレントディレクトリ内にある各ファイルとサブディレクトリが使用している全ディスク容量を表示します。

-a

個別のファイルのサイズを表示します。

-h

一般的に読みやすい形式で出力します。

-s

計算後の合計サイズだけを表示します。

`free [options]`

free コマンドは、RAMとスワップ領域の使用状況、および両方のカテゴリでの全容量と使用中容量に関する情報を表示します。詳細については、[22.1.6項「free コマンド」](#) (472 ページ)を参照してください。

`-b`

バイト単位で出力します。

`-k`

キロバイト(**KB**)単位で出力します。

`-m`

メガバイト(**MB**)単位で出力します。

`date [options]`

この簡単なプログラムは、現在のシステム時刻を表示します。**root**ユーザでこのコマンドを実行した場合、システム時刻を変更することもできます。このプログラムの詳細については、**date(1)**の**man**ページを参照してください。

プロセス

`top [options]`

top コマンドは、現在動作しているプロセスの概要を表示します。**H**を押すと、このプログラムをカスタマイズするための主要なオプションについて簡単に説明しているページにアクセスできます。

`ps [options] [process ID]`

オプションなしで実行した場合、このコマンドは現在のユーザ独自のプログラムまたはプロセスすべてからなる表を表示します。それらは、現在のユーザが起動したものを意味します。このコマンドでオプションを指定する場合、ハイフンは付けません。

aux

所有者に関係なく、すべてのプロセスからなる詳しいリストを表示します。

`kill [options] process ID`

作業中、プログラムが通常の方法で終了できなくなることがあります。ほとんどの場合、該当するプロセスID(`top`コマンドと`ps`コマンドを参照)を指定し、`kill`コマンドを実行することにより、そのような暴走したプログラムを終了させることができます。`kill`コマンドは、**TERM**シグナルを送信します。このシグナルは、そのようなプログラムに対して、自らを終了するよう指示します。これだけでは解決しない場合、次のパラメータを使用できます。

-9

TERMシグナルの代わりに**KILL**シグナルを送信します。これで、ほとんどすべての場合、指定されたプロセスが終了します。

`killall [options] processname`

このコマンドは`kill`コマンドに似ていますが、引数として(プロセスIDではなく)プロセス名を使用し、その名前を持つすべてのプロセスを終了させます。

Network

`ping [options] ホスト名またはIPアドレス`

`ping`コマンドは、TCP/IPネットワークの基本的な機能をテストする標準的なツールです。小さいデータパケットを送信先ホストへ送信し、即座の応答を要求します。この作業が成功した場合、`ping`コマンドは、その結果を知らせるメッセージを表示します。これは、ネットワークリンクが基本的に機能していることを意味します。

-c 数字

送信するパケットの総数を決定し、それらをディスパッチし終わった後で処理を終了します(デフォルトでは、上限は設定されていません)。

-f

*flood ping*できるだけ多くのデータパケットを送信します。一般的には、`root`がネットワークをテストする目的で使用します。

-i value

2つのデータパケットの間隔を秒単位で指定します(デフォルトは、1秒)。

nslookup

ドメインネームシステム(DNS)は、ドメイン名からIPアドレスへの変換を行います。このツールは、ネームサーバ(DNSサーバ)に問い合わせを送信します。

telnet [options] ホスト名またはIPアドレス [port]

Telnetは、実際のところ、ネットワーク経由でリモートホスト上での操作を可能にするインターネットプロトコルの1つです。telnetは、このプロトコルを使用してリモートコンピュータ上での操作を可能にするLinuxプログラムの名前でもあります。

警告

第三者が「傍受」可能なネットワークを経由する場合、telnetを使用しないでください。」特にインターネットを経由する場合、パスワードが悪用されるリスクを回避するために、sshコマンドのような暗号化された伝送方法を使用してください(sshコマンドのmanページを参照してください)。

その他

passwd [options] [username]

ユーザはこのコマンドを使用することにより、自分のパスワードをいつでも変更できます。管理者rootはこのコマンドを使用して、システム上に存在するあらゆるユーザのパスワードを変更できます。

su [options] [username]

suコマンドは、実行中のセッションから、他のユーザ名を使用してログインできるようにします。ユーザ名と、対応するパスワードを指定してください。rootユーザはあらゆるユーザのID (身元)を使用することが承認されているので、rootがこのコマンドを使用する場合、パスワードの入力を要求されません。ユーザの名前を指定しないでこのコマンドを使用する場合、rootのパスワードの入力を求めるプロンプトが表示され、スーパーユーザ(root)に変更されます。

-

別なユーザとしてログインシェルを起動するには、su -を使用します。

`halt [options]`

データの損失を防止するために、システムをシャットダウンする場合、必ずこのコマンドを使用することをお勧めします。

`reboot [options]`

システムが直ちにリブートすることを除き、このコマンドは、`halt`コマンドと同じ処理を実行します。

`clear`

このコマンドは、コンソールの表示領域すべてをクリアします。オプションはありません。

18.3.3 詳細情報

この章に掲載した以外にも、多くのコマンドがあります。他のコマンドの概要、またはより詳しい情報については、オライリー刊の*Linux in a Nutshell*(邦訳『Linux クイックリファレンス』)をお勧めします。

18.4 viエディタ

プログラミングのみでなく、多くのシステム管理タスクにも、相変わらずテキストエディタが使用されています。Unixでは、viは使いやすい編集機能を提供し、マウスサポート機能を持つ多数のエディタに比べて人間工学の面から優れたエディタとなっています。

18.4.1 動作モード

注意: キーの表示

次では、viでキーを押すだけで入力できるいくつかのコマンドについて確認してください。これらは、キーボードと同様、大文字で表示されます。キーを大文字で入力する必要がある場合は、**<Shift>**キーを含む、キーの組み合わせを示すことによって、このことが明示的に示されています。

基本的にviは、挿入モード、コマンドモード、および拡張モードの3種類のモードを活用します。キーの機能は動作モードに応じて異なります。起動時には、

通常、**vi**はコマンドモードに設定されます。はじめに、モード間で切り替える方法について説明します。

コマンドモードから挿入モードへ

さまざまな方法があり、追加の場合は**a**、挿入の場合は**i**、現在行の下に新規行を挿入する場合は**o**を使用します。

挿入モードからコマンドモードへ

挿入モードを終了するには、**<Esc>**キーを押します。**vi**は、挿入モードになっていると、終了できません。**<Esc>**キーを押す習慣を付けることが大切です。

コマンドモードから拡張モードへ

viの拡張モードを有効にするには、コロン(:)を入力します。拡張(**ex**)モードは、単純なものから複雑なものまで各種タスクに使用できる行単位のエディタです。

拡張モードからコマンドモードへ

拡張モードでコマンドを実行した後、エディタは自動的にコマンドモードに戻ります。拡張モードでコマンドを実行しないことにした場合は、でコロンを削除します。**<—**エディタはコマンドモードに戻ります。

挿入モードから拡張モードに直接切り替えることはできません。はじめに、コマンドモードに切り替える必要があります。

他のエディタと同様に、**vi**にも独自の終了手順があります。挿入モードでは**vi**を終了できません。最初に、**<Esc>**キーを押して挿入モードを終了します。その後は、次の2つの選択肢があります。

1. *Exit without saving*(保存しないで終了):変更内容を保存しないでエディタを終了する場合はコマンドモードで、**:—Q—!**と入力します。感嘆符(!)を付けると、**vi**では変更内容が無視されます。
2. *Save and exit*(保存して終了):変更内容を保存してエディタを終了するには、複数の方法があります。コマンドモードで、**Shift+Z Shift+Z**を使用します。拡張モードで変更内容をすべて保存してエディタを終了するには、**:—W—Q**と入力します。拡張モードでは、**w**は「書き込み」、**q**は「終了」を表します。

18.4.2 操作中のvi

viを標準エディタとして使用できます。挿入モードで、テキストの入力と削除に<—とDelキーを使用します。カーソル移動には矢印キーを使用します。

ただし、これらのコントロールキーを使用するとしばしば問題が発生します。これは、特殊なキーコードを使用する端末タイプが多数存在するからです。これは、コマンドモードに影響します。<Esc>キーを押して挿入モードからコマンドモードに切り替えます。コマンドモードでは、<H>キー、<J>キー、<K>キー、および<L>キーを使用してカーソルを移動します。各キーの機能は、以下のとおりです。

H
左に1文字分移動します。

J
下に1行分移動します。

K
上に1行分移動します。

L
右に1文字分移動します。

コマンドモードでは、コマンドを使用してさまざまな操作を行うことができます。コマンドを2度以上実行するには、単に反復回数を入力してから実際のコマンドを入力します。たとえば、<5>キー<L>キーと入力すると、カーソルは右に5文字分移動します。

一部の重要なコマンドについては、表 18.2. 「viエディタの簡単なコマンド」 (416 ページ)で説明しています。ただし、ここで説明されているコマンドはほんの一部でしかありません。詳細なリストは、18.4.3頁「詳細情報」 (417 ページ)のドキュメント内で利用できます。

表 18.2 viエディタの簡単なコマンド

Esc	コマンドモードに変更します。
I	挿入モードに変更します(文字は現在のカーソル位置に表示されます)。

A	挿入モードに変更します(文字は現在のカーソル位置の後に挿入されます)。
Shift + A	挿入モードに変更します(文字は行末に追加されます)。
Shift + R	置換モードに変更します(古いテキストを上書きします)。
R	カーソルの下の文字を置き換えます。
O	挿入モードに変更します(現在の行の後に新しい行が挿入されます)。
Shift + O	挿入モードに変更します(現在の行の前に新しい行が挿入されます)。
X	現在の文字を削除します。
D - D	現在の行を削除します。
D - W	現在の語の終わりまで削除します。
C - W	挿入モードに変更します(現在の語の残りの文字が次に入力するエントリに上書きされます)。
U	最後のコマンドを取り消します。
Ctrl + R	取り消された変更を再実行します。
Shift + J	次の行を現在の行と連結します。
.	最後のコマンドを繰り返します。

18.4.3 詳細情報

viは多様なコマンドをサポートしています。マクロ、ショートカット、名前付きバッファ、および他の多数の便利な機能を使用できます。さまざまなオプションの詳細な説明は、このマニュアルの対象範囲外です。SUSE Linux

Enterpriseには、viの改良版のvimが用意されています。このアプリケーションについては、さまざまな情報源があります。

- vimtutorは、vimの対話形式のチュートリアルです。
- vimで :help コマンドを入力すると、さまざまなヘルプトピックが表示されます。
- vimに関するマニュアルは、<http://www.truth.sk/vim/vimbook-OPL.pdf>からオンラインで入手できます。
- にあるvimプロジェクトのWebページでは、あらゆる種類のニュース、メーリングリスト、およびその他のドキュメントが提供されます。<http://www.vim.org>
- インターネットでは、<http://www.selflinux.org/selflinux/html/vim.html>、<http://www.linuxgazette.com/node/view/9039>、およびhttp://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.htmlなどの、多数のvimソースが提供されています。チュートリアルへのリンクについては、「<http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html>」を参照してください。

重要項目: VIMライセンス

vimは、「無償ソフトウェア」です。つまり、作者からはソフトウェアの代金を請求されませんが、資金援助による非営利プロジェクトの支援が奨励されます。このプロジェクトは、ウガンダの貧しい子供たちに対する援助を求めています。詳細については、<http://iccf-holland.org/index.html>、<http://www.vim.org/iccf/>、および<http://www.iccf.nl/>でオンライン情報を参照してください。

パート III. システム

64ビットシステム環境での32ビットと64ビットのアプリケーション

19

SUSE Linux Enterprise®は、複数の 64ビットプラットフォームで利用できます。ただし、付属のすべてのアプリケーションが64ビットプラットフォームに移植されている訳ではありません。SUSE Linux Enterpriseは、32ビットアプリケーションの64ビットシステム環境での使用をサポートしています。この章では、64ビットSUSE Linux Enterpriseプラットフォームでこのサポートがどのように行われているかについて簡潔に説明します。また、32ビットアプリケーションの実行方法(ランタイムサポート)、および32ビットと64ビットのシステム環境の両方で実行できるように32ビットアプリケーションをコンパイルする方法について説明します。さらに、カーネルAPIに関する情報、および32ビットアプリケーションを64ビットカーネルで実行する方法についても説明します。

注意: IBM System zの31ビットアプリケーション:

IBM System zでのs390は31ビット環境を使用します。次に示す32ビットアプリケーションへの参照は、31ビットアプリケーションにも適用されます。

64ビットプラットフォーム ia64、ppc64、s390x、x86_64に対応したSUSE Linux Enterpriseは、既存の32ビットアプリケーションが64ビット環境で「出荷してすぐに」動作するように設計されています。」対応する 32ビットプラットフォームには、ia64のx86、ppc64のppc、s390xのs390、およびx86_64のx86があります。このサポートにより、対応する 64ビット移植版が使用可能になるのを待たなくても、使用したい 32ビットアプリケーションを引き続き使用できます。現在のppc64システムは、大部分のアプリケーションを 32ビットモードで実行しますが、64ビットアプリケーションを実行することもできます。

19.1 ランタイムサポート

重要項目: アプリケーションバージョン間の競合

アプリケーションが32ビットと64ビットの両方の環境で使用可能な場合に、両方のバージョンを同時にインストールすると問題が生じます。そのような場合は、2つのバージョンのどちらかだけをインストールして使用してください。

正しく実行するために、すべてのアプリケーションにはライブラリが必要です。しかし残念ながら、32ビットバージョンと64ビットバージョンのライブラリの名前は同じです。そのため、ライブラリを別の方法で区別する必要があります。

64ビットプラットフォームppc64、s390x、およびx86_64でも、同じ手法が使用されます。32ビット版との互換性を維持するために、32ビット環境と同じ場所にライブラリが保存されます。libc.so..6の32ビットバージョンは、32ビットと64ビットのどちらの環境でも/lib/libc.so..6の下にあります。

64ビットのすべてのライブラリとオブジェクトファイルは、lib64というディレクトリにあります。通常、/lib、/usr/lib、および/usr/X11R6/libの下にあると想定されている64ビットのオブジェクトファイル

は、/lib64、/usr/lib64、および/usr/X11R6/lib64の下にあります。つまり、両方のバージョンのファイル名を変更しなくても済むように、32ビットライブラリ用の領域は/lib、/usr/lib、および/usr/X11R6/libの下になっています。

データの内容がワードサイズに依存しない、32ビットの/libディレクトリ中のサブディレクトリは移動されません。たとえば、X11フォントは、これまでどおり/usr/X11R6/lib/X11/fontsの下の通常の下にあります。このスキームは、LSB (Linux Standards Base)とFHS (File System Hierarchy Standard)に準拠しています。

► **ipf:** ia64用の64ビットライブラリは、標準のlibディレクトリにあります。この場合、lib64ディレクトリやlib32ディレクトリは存在しません。ia64は、32ビットのX86コードをエミュレーションで実行します。基本的なライブラリセットは、/emul/ia32-linux/libおよび/emul/ia32-linux/usr/X11R6/libにインストールされます。 ◀

19.2 ソフトウェア開発

すべての64ビットアーキテクチャで、64ビットオブジェクトの開発がサポートされています。32ビットコンパイル機能のサポートレベルは、アーキテクチャによって異なります。32ビットコンパイル機能は、GCC (GNU Compiler Collection)やbinutilsによるツールチェーンの各種実装オプションになっています。Binutilsには、アセンブラasとリンカーldが含まれています。

biarchコンパイラ

32ビットと64ビットのオブジェクトはどちらもbiarch開発ツールチェーンで生成できます。ほぼすべてのプラットフォームにおいて、デフォルトでは64ビットオブジェクトのコンパイルが実行されます。32ビットオブジェクトは、特殊なフラグを使用すれば生成できます。この特殊なフラグは、gccでは-m32 (s390バイナリの生成では-m31)です。binutilsのフラグはアーキテクチャによって異なりますが、GCCは正しいフラグをリンカーやアセンブラに転送します。現在では、amd64 (x86とamd64の開発をサポート)、s390x、およびppc64用のbiarch開発ツールチェーンが存在します。通常、32ビットオブジェクトはppc64プラットフォームで作成されます。-m64フラグは、64ビットオブジェクトの生成に使用する必要があります。

未サポート

SUSE Linux Enterpriseでは、すべてのプラットフォームで32ビットソフトウェアを直接開発できるとは限りません。ia64でx86用のアプリケーションを開発するには、対応する32ビットバージョンのSUSE Linux Enterpriseを使用します。

すべてのヘッダファイルは、アーキテクチャに依存しない形式で作成する必要があります。インストール済みの32ビットと64ビットのライブラリには、インストール済みのヘッダファイルに対応するAPI (アプリケーションプログラミングインタフェース)が必要です。標準のSUSE Linux Enterprise環境は、この原則に従って設計されています。ライブラリを手動で更新した場合は、各自でAPIの問題を解決してください。

19.3 biarchプラットフォームでのソフトウェアのコンパイル

biarchアーキテクチャで他のアーキテクチャ向けのバイナリを開発するには、対象のアーキテクチャのそれぞれのライブラリをさらにインストールする必要があります。こうしたパッケージは、対象のアーキテクチャが32ビットアーキテクチャである場合はrpmname-32bitまたはrpmname-x86(ia64の場合)と呼ばれ、対象のアーキテクチャが64ビットアーキテクチャである場合はrpmname-64bitと呼ばれます。さらに、rpmname-develパッケージからそれぞれのヘッダとライブラリ、また、rpmname-devel-32bitまたはrpmname-devel-64bitから対象のアーキテクチャ向けの開発ライブラリも必要です。

たとえば、対象のアーキテクチャが32ビットアーキテクチャ(x86_64またはs390x)であるシステムでlibaioを使用するプログラムをコンパイルするには、次のRPMが必要です。

libaio-32bit

32ビットランタイムパッケージ

libaio-devel-32bit

32ビット開発用のヘッダとライブラリ

libaio

64ビットランタイムパッケージ

libaio-devel

64ビット開発用のヘッダとライブラリ

ほとんどのオープンソースプログラムでは、autoconfベースのプログラム設定が使用されています。対象のアーキテクチャ向けプログラムの設定にautoconfを使用するには、autoconfの標準のコンパイラとリンカーの設定に上書きするために、さらに環境変数を指定してconfigureスクリプトを実行します。

次の例は、対象のアーキテクチャとしてx86を採用しているx86_64システムを示しています。対象のアーキテクチャとしてs390を採用しているs390x、ま

またはppcを採用しているppc64の場合も同様です。この例は、32ビットパッケージをビルドしないia64には適用されません。

ティップ

二次アーキテクチャとしてs390を使用する場合、これは31ビットシステムなので-m32の代わりに-m31を使用する必要があります。

- 1 32ビットコンパイラを使用します。

```
CC="gcc -m32"
```

- 2 リンカーに32ビットオブジェクトの処理を指示します(リンカーのフロントエンドには常にgccを使用)。

```
LD="gcc -m32"
```

- 3 32ビットオブジェクトを生成するためにアセンブラを設定します。

```
AS="gcc -c -m32"
```

- 4 libtoolなどのライブラリが/usr/libから得られたか確認します。

```
LDFLAGS="-L/usr/lib"
```

- 5 ライブラリがlibサブディレクトリに格納されているか確認します。

```
--libdir=/usr/lib
```

- 6 32ビットXライブラリが使用されているか確認します。

```
--x-libraries=/usr/X11R6/lib/
```

こうした変数のすべてがどのプログラムにも必要なわけではありません。それぞれのプログラムに合わせて使用してください。

x86_64、ppc64、またはs390xでネイティブの32ビットアプリケーションをコンパイルする場合の、configureコールの例を次に示します。

```
CC="gcc -m32" \
LDFLAGS="-L/usr/lib;" \
    .configure \
    --prefix=/usr \
```

```
--libdir=/usr/lib  
make  
make install
```

19.4 カーネル仕様

X86_64、ppc_64およびs390x向けの64ビットカーネルには、64ビットと32ビットのカーネルABI(アプリケーションバイナリインタフェース)が用意されています。32ビットのカーネルABIは、該当する32ビットカーネルのABIと同じものです。つまり、32ビットアプリケーションが、32ビットカーネルの場合と同様に64ビットカーネルと通信できるということです。

64ビットカーネルのシステムコールの32ビットエミュレーションでは、システムプログラムで使用するすべてのAPIをサポートしていません。ただし、このサポートの有無はプラットフォームによって異なります。このため、lspciなどの少数のアプリケーションは、正しく機能するように64ビットプログラムとして非ppc64プラットフォームでコンパイルする必要があります。IBM System zでは、32ビットカーネルABIで利用できないioctlがあります。

64ビットカーネルでは、このカーネル用に特別にコンパイルされた64ビットカーネルモジュールしかロードできません。したがって、32ビットカーネルモジュールを使用することはできません。

ティップ

一部のアプリケーションには、カーネルでロード可能な個々のモジュールが必要です。64ビットシステム環境でそのような32ビットアプリケーションを使用する予定がある場合は、このアプリケーションのプロバイダやNovellに問い合わせ、このモジュール向けのカーネルでロード可能な64ビットバージョンのモジュールと32ビットコンパイルバージョンのカーネルAPIを入手できるかを確認してください。

Linuxシステムのブートと設定

Linuxシステムのブートには、さまざまなコンポーネントが関係しています。ハードウェアはBIOSにより初期化され、BIOSはブートローダを介してカーネルを起動します。それ以後は、オペレーティングシステムがinitとランレベルを含むブートプロセスを完全にコントロールします。ランレベルのコンセプトにより、日常使用のセットアップを保持できるほか、システム上でタスクを保守することもできます。

20.1 Linuxのブートプロセス

Linuxのブートプロセスは、いくつかの段階から成り、それぞれを別のコンポーネントが代表しています。次のリストに、主要なすべてのコンポーネントが関与するブートプロセスと機能を簡潔にまとめています。

1. **BIOS** コンピュータに電源を投入すると、BIOSで画面とキーボードの初期化およびメインメモリのテストが行われます。この段階まで、コンピュータは大容量ストレージメディアにアクセスしません。続いて、現在の日付、時刻、および最も重要な周辺機器に関する情報が、CMOS値からロードされます。最初のハードディスクとそのジオメトリが認識されると、システム制御がBIOSからブートローダに移ります。BIOSがネットワークブートをサポートしている場合は、ブートローダを提供するブートサーバを設定することもできます。x86システムの場合、PXEブートを利用する必要があります。他のアーキテクチャの場合は、通常BOOTPプロトコルを使ってブートローダを取得します。

2. **ブートローダ** 最初のハードディスクの先頭の 512 バイト物理データセクタがメインメモリにロードされ、このセクタの先頭に常駐するブートローダが起動します。ブートローダによって実行されたコマンドがブートプロセスの残りの部分を確定します。したがって、最初のハードディスクの先頭 512 バイトのことをマスタブートレコード(MBR)といいます。次に、ブートローダは実際のオペレーティングシステム(この場合はLinuxカーネル)に制御を渡します。GRUB(Linuxのブートローダ)の詳細については、[第21章 ブートローダ](#)(445 ページ)を参照してください。ネットワークブートを行う場合、BIOSがブートローダとしての役割を果たします。BIOSは、ブートサーバから起動するためのイメージを取得し、それを使ってシステムを起動します。この作業にローカルのハードディスクからは完全に独立した処理として行われます。
3. **カーネルとinitramfs** システムに制御を渡すために、ブートローダは、カーネルとRAMベースの初期ファイルシステム(initramfs)をメモリにロードします。カーネルは、initramfsの内容を直接使用できます。initramfsには、実際のルートファイルシステムのマウント処理を担当するinitと言う名前の小さな実行可能ファイルが含まれています。大容量ストレージにアクセスするために特別なハードウェアドライバが必要な場合、それらはinitramfs内になければなりません。initramfsについての詳細は、[20.1.1 項「initramfs」](#) (429 ページ)を参照してください。システムにローカルハードディスクがない場合、initramfsがルートファイルシステムをカーネルに提供する必要があります。そのためには、iSCSIやSANなどのネットワークブロックデバイスを利用しますが、NFSをルートデバイスとして使うことも可能です。
4. **initramfs上のinit** このプログラムは、適切なルートファイルシステムをマウントするために必要なすべてのアクションを実行します。たとえば、udevに必要なファイルシステム用のカーネル機能や、大容量ストレージコントローラ用のデバイスドライバを提供します。ルートファイルシステムが見つかり、エラーをチェックしてからマウントします。これが正常に実行されれば、initramfsはクリアされ、ルートファイルシステムのinitが実行されます。initについての詳細は、[20.1.2 項「initramfs上のinit」](#) (430 ページ)を参照してください。udevについての詳細は、[第24章 udevを使用した動的カーネルデバイス管理](#) (509 ページ)を参照してください。
5. **init** initは、さまざまなレベルでシステムの実際のブートを処理し、各種の機能を提供します。initについては、[20.2 項「initプロセス」](#) (432 ページ)で説明しています。

20.1.1 initramfs

initramfsは、カーネルがRAMディスクにロードできる、小さなcpioアーカイブです。また、実際のルートファイルシステムがマウントされる前にプログラムを実行できるようにする最低限のLinux環境を提供します。この最低限のLinux環境は、BIOSルーチンでメモリにロードされます。十分な容量のメモリがあること以外には具体的なハードウェア要件はありません。initramfsには必ず、initという名前の実行可能ファイルがあります。これは、ブートプロセスが進行するにつれて、ルートファイルシステム上の本当のinitプログラムを実行することになります。

ルートファイルシステムをマウントして実際のオペレーティングシステムを起動する前に、カーネルには、ルートファイルシステムが配置されているデバイスにアクセスするための対応ドライバが必要です。こうしたドライバには、特定のハードディスク用の特殊なドライバや、ネットワークファイルシステムにアクセスするためのネットワークドライバが含まれる場合もあります。ルートファイルシステムで必要となるモジュールは、initramfs上のinitによってロードされます。モジュールをロードしたら、udevによって必要なデバイスがinitramfsに提供されます。ブートプロセス後半で、ルートファイルシステムが変更された後、デバイスを再生成する必要があります。これには、udevtriggerコマンドでboot.udevを実行します。

インストール済みのシステムのハードウェア(ハードディスクなど)を変更する必要が生じ、このハードウェアがブート時にカーネル内に存在する別のドライバを必要とする場合には、initramfsファイルを更新する必要があります。これは、initramfsの前身であるinitrdの場合と同様に、mkinitrdを呼び出すことによって行えます。引数を付けずにmkinitrdを呼び出すと、initramfsが作成されます。mkinitrd -Rを呼び出すと、initrdが作成されます。SUSE Linux Enterprise®では、ロードするモジュールは/etc/sysconfig/kernel内のINITRD_MODULESで指定されます。インストール後、この変数は自動的に正しい値に設定されます。モジュールは、INITRD_MODULESに指定されている順序で正確にロードされます。このことは、デバイスファイルの/dev/sd?の設定の正確性に依存している場合にも重要になります。..ただし、現在のシステムで/dev/disk/ディレクトリ下にあるデバイスファイルを使用することもできます。これらのファイルは、by-id、by-path、およびby-uuidなどのサブディレクトリに分類されており、常に同じディスクを表します。これは、該当するマウントオプションの指定により、インストール時にも可能です。

重要項目: **initramfs**または**initrd**の更新

ブートローダは、カーネルと同じように**initramfs**または**initrd**をロードします。**GRUB**はブート時にディレクトリ内の正しいファイルを検索するので、**initramfs**または**initrd**の更新後に**GRUB**を再インストールする必要はありません。

20.1.2 **initramfs**上の**init**

initramfs上の**init**の主な目的は、実際のルートファイルシステムのマウントとそのファイルシステムへのアクセスの準備です。システム設定に応じて、**init**は次のタスクを実行します。

カーネルモジュールのロード

ハードウェア設定によっては、使用するコンピュータのハードウェアコンポーネント(特にハードディスク)にアクセスするために特殊なドライバが必要になる場合があります。最終的なルートファイルシステムにアクセスするには、カーネルが適切なファイルシステムドライバをロードする必要があります。

ブロック特殊ファイルの提供

ロードされるモジュールごとに、カーネルはデバイスイベントを生成します。**udev**は、これらのイベントを処理し、**RAM**ファイルシステム上で必要なブロック特殊ファイルを**/dev**内に生成します。これらの特殊ファイルがないと、ファイルシステムや他のデバイスにアクセスできません。

RAIDと**LVM**のセットアップの管理

RAIDまたは**LVM**の下でルートファイルシステムを保持するようにシステムを設定した場合、**init**は**LVM**または**RAID**をセットアップして、後でルートファイルシステムにアクセスできるようにします。**RAID**については、**7.2項「ソフトウェアRAID設定」** (137 ページ)を参照してください。**LVM**については、「**7.1項「LVMの設定」** (127 ページ)」を参照してください。**EVMS**および特殊ストレージ設定については、『*Storage Administration Guide*』を参照してください。

ネットワーク設定の管理

ネットワークマウントしたルートファイルシステム(**NFS**を介したマウント)を使用するようにシステムを設定した場合、**linuxrc**は適切なネットワー

クドライバがロードされ、ドライバがルートファイルシステムにアクセスできるように設定されていることを確認する必要があります。

ファイルシステムがiSCSIやSANなどのネットワークブロックデバイスに常駐している場合は、ストレージサーバへの接続もinitramfsによって設定されます。

初期ブート時にlinuxrcがインストールプロセスの一環として呼び出される場合、そのタスクは前に説明したタスクと異なります。

インストールメディアの検出

インストールプロセスを開始すると、使用するコンピュータでは、YaSTインストーラでインストールカーネルと特殊なinitrdがインストールメディアからロードされます。RAMファイルシステムで実行されるYaSTインストーラには、インストールメディアにアクセスしてオペレーティングシステムをインストールするために、そのメディアの場所に関する情報が必要になります。

ハードウェア認識の開始および適切なカーネルモジュールのロード

で説明しているように、ブートプロセスは、ほとんどのハードウェア設定で利用できる最小限のドライバセットで開始されます。initは、ハードウェア設定に適したドライバセットを確定する、初期ハードウェアスキャンプロセスを開始します。20.1.1項「initramfs」(429 ページ)ブートプロセスに必要なモジュール名は、/etc/sysconfig/kernelディレクトリ中のINITRD_MODULESに書き込まれます。これらのモジュール名は、システムをブートするために必要なカスタムinitramfsを生成するために使用されます。ブートではなくcoldplugに必要なモジュールは、/etc/sysconfig/hardware/hwconfig-*ディレクトリに書き込まれます。ブートプロセス時には、このディレクトリ中の設定ファイルに記述されているすべてのデバイスが初期化されます。

インストールシステムまたはレスキューシステムのロード

ハードウェアが正しく認識され、適切なドライバがロードされ、udevがデバイス特定ファイルを作成するとすぐに、linuxrcはインストールシステムを起動します。このシステムには、実際のYaSTインストーラまたはレスキューシステムが含まれています。

YaSTの開始

最後に、initはYaSTを起動します。これはパッケージのインストールとシステム設定を開始します。

20.2 initプロセス

initプログラムは、プロセスIDが1のプロセスです。このプロセスは、システムの初期化を担当しています。initは直接カーネルから起動し、プロセスを強制終了するsignal9で終了することはできません。他のすべてのプログラムは、initまたは子プロセスのいずれかによって直接起動されます。

initの中心的な設定は、`/etc/inittab`ファイルで行われています。このファイルはランレベルを定義しています(20.2.1項「ランレベル」(432ページ)を参照)。このファイルはまた、各レベルで利用可能なサービスとデーモンを指定しています。`/etc/inittab`のエントリに応じて、initが複数のスクリプトを実行します。わかりやすくするために、これらのinitスクリプトと呼ばれるスクリプトはすべて、ディレクトリ`/etc/init.d`にあります(20.2.2項「initスクリプト」(435ページ)を参照)。

システムを起動し、シャットダウンするプロセス全体は、initによって管理されます。この点から見ると、カーネルは、他のプログラムからの要求に従って、他のすべてのプロセスとCPU時間やハードウェアアクセスを管理するバックグラウンドプロセスと考えることができます。

20.2.1 ランレベル

Linuxでは、ランレベルはシステムの起動方法および稼働中のシステムで使用可能なサービスを定義します。ブート後、システムは`/etc/inittab`の`initdefault`行での定義に従って起動します。通常のランレベルは3または5です。参照先表 20.1. 「ランレベルの種類」(432ページ)。別の方法として、ランレベルをブート時に(たとえばブートプロンプトにランレベル番号を追加する)指定することもできます。パラメータは、カーネル自体が直接評価するもの以外、initに渡されます。ランレベル3にブートするには、ブートプロンプトに単一の番号3を追加します。

表 20.1 ランレベルの種類

ランレベル	説明
0	システム停止

ランレベル	説明
Sまたは1	シングルユーザモード
2	リモートネットワーク(NFSなど)なしのローカルマルチユーザモード
3	ネットワークを使用するフルマルチユーザモード
4	未使用
5	ネットワークとXディスプレイマネージャのKDM、GDM、またはXDMを使用するフルマルチユーザモード
6	システム再起動

重要項目: パーティションがNFSマウントされている場合にはランレベル2は避ける

システムでNFSを介して/usrなどのパーティションをマウントする場合は、ランレベル 2を使用しないでください。NFSサービスは、ランレベル2(リモートネットワークのないローカルマルチユーザモード)では使用できないため、プログラムファイルまたはライブラリがない場合、システムは予想しない動作をする可能性があります。

システムの移動中にランレベルを変更するには、telinitの後に、ランレベルに対応する番号を引数として入力します。これができるのは、システム管理者だけです。次のリストは、ランレベルに関連した最も重要なコマンドの概要です。

telinit 1またはshutdown now

システムはシングルユーザモードに入ります。このモードは、システムメンテナンスや管理タスクで使います。

telinit 3

(ネットワークを含む)すべての重要なプログラムとサービスが起動します。グラフィック環境はありませんが、一般ユーザは、システムにログインして作業することができます。

telinit 5

グラフィック環境は有効になります。通常、XDM、GDMまたはKDMなどのディスプレイマネージャが起動します。自動ログインが有効な場合、ローカルユーザは事前に選択されているウィンドウマネージャ(GNOME、KDEまたはその他のウィンドウマネージャ)にログインします。

telinit 0またはshutdown -h now
システムは停止します。

telinit 6またはshutdown -r now
システムは停止した後、再起動します。

ランレベル5は、すべてのSUSE Linux Enterprise標準インストールにおけるデフォルトのランレベルです。ユーザは、グラフィカルインタフェースでログインするように求められます。デフォルトユーザの場合は自動的にログインされます。デフォルトのランレベルは3で、ランレベルを5に切り替えるには、**第26章 X Windowシステム** (529 ページ)で説明するようにX Window Systemを正しく設定している必要があります。その後、telinit5を入力して、システムが意図したとおりに動作するかを確認します。すべてが意図したとおりに動作した場合は、YaSTを使用してデフォルトのランレベルを5に設定します。

警告: /etc/inittab内のエラーのためシステムブートが失敗することがある

/etc/inittabが破損した場合、システムが正しく起動しないことがあります。そのため、/etc/inittabを編集する場合は細心の注意を払ってください。また、コンピュータを再起動する前には、常にtelinitqコマンドを使って、initに/etc/inittabを再読み込みさせるようにしてください。

ランレベルを変更するときには、一般に2つの操作が行われます。1つは、現在のランレベルの停止スクリプトが起動し、現在のランレベルに必要なプログラムを終了します。次に、新しいランレベルの起動スクリプトが起動します。ここで、ほとんどの場合、プログラムがいくつか起動します。たとえば、ランレベルを3から5に変更する場合、次の操作が行われます。

1. 管理者(root)がtelinit 5を入力して、initにランレベルを変更することを伝えます。

2. `init`は現在のランレベル(`runlevel`)を調べ、新しいランレベルをパラメータとして`/etc/init.d/rc`を起動する必要があるかどうか判断します。
3. ここで`rc`は、現在のランレベルの停止スクリプトであって、新しいランレベルの起動スクリプトがないものを呼び出します。この例では、元のランレベルが3なので、`/etc/init.d/rc 3.d`の中のKで始まるすべてのスクリプトが対象となります。Kの次の番号は、`stop`パラメータを使ってスクリプトを実行する順番を示します(検討する必要がある依存関係が存在するため)。
4. 最後に、新しいランレベルの起動スクリプトを起動します。この例では`/etc/init.d/rc5.d`の中のSで始まるスクリプトがそれにあたります。この場合も、sの次の番号が、スクリプトの実行順序を表します。

現在のランレベルと同じランレベルに変更する場合、`init`は`/etc/inittab`の変更部分だけをチェックし、適切な手順を開始します。たとえば、別のインタフェースで`getty`を起動します。`telinit q`コマンドを使用しても同じ操作を実行できます。

20.2.2 `init`スクリプト

`/etc/init.d`内に、2種類のスクリプトがあります。

`init`によって直接実行されるスクリプト

これは、ブートプロセスの実行中、または即座のシステムシャットダウンを行ったとき(電源障害またはユーザが`Ctrl+Alt+Del`キーを押した場合)にのみ適用されます。IBM System zシステムの場合、ブートプロセスの実行中または即座のシステムシャットダウンを行ったとき(電源障害または「シグナルによる停止」)にのみ適用されます。こうしたスクリプトの実行は、`/etc/inittab`で定義されます。

`init`によって間接的に実行されるスクリプト

これらは、ランレベルの変更時に実行され、関連スクリプトの正しい順序を保証するマスタスクリプト`/etc/init.d/rc`を常に呼び出します。

すべてのスクリプトは、`/etc/init.d`にあります。ブート時に実行されるスクリプトは、`/etc/init.d/boot.d`からのシンボリックリンク経由で呼び出されます。ランレベルを変更するスクリプトもサブディレクトリの1つから

のシンボリックリンク(/etc/init.d/rc0.dから/etc/init.d/rc6.dへ)経由で呼び出されます。これは単にわかりやすくして、複数のランレベルで使用されている場合にスクリプトが重複するのを防ぐためです。すべてのスクリプトは、起動スクリプトとしても停止スクリプトとしても実行できるので、これらのスクリプトはパラメータのstartとstopを認識する必要があります。また、これらのスクリプトはrestart、reload、force-reload、およびstatusのオプションも認識します。これらのオプションについては、[表 20.2. 「initスクリプトのオプション」](#) (436 ページ)で説明します。initによって直接実行されるスクリプトには、このようなリンクはありません。こうしたスクリプトは、必要なときにランレベルとは無関係に実行されます。

表 20.2 *init*スクリプトのオプション

オプション	説明
起動	サービスを起動します。
中止	サービスを停止します。
restart	サービスが実行中の場合は、停止して再起動します。実行中でない場合は、起動します。
reload	サービスの停止や再起動をせずに、設定を再ロードします。
force-reload	サービスが設定の再ロードをサポートする場合は、それを実行します。サポートしない場合は、restartが指定された場合と同じ操作を行います。
ステータス	サービスの現在のステータスを表示します。

ランレベル固有のサブディレクトリにあるリンクによって、スクリプトを複数のランレベルに関連付けることができます。パッケージのインストールまたはアンインストール時に、プログラムinsservを使用して(またはこのプログラムを呼び出す/usr/lib/lsb/install_initdスクリプトを使用して)、このようなリンクを追加または削除することができます。詳細は、insserv(8)のmanページを参照してください。

これらの設定は、YaSTモジュールにより変更されることもあります。コマンドラインからステータスを確認するには、**chkconfig**ツールを使います。このツールの詳細は、**chkconfig(8)**マニュアルページを参照してください。

次に、最初または最後に起動するブートスクリプトおよび停止スクリプトの概略を示すとともに、保守スクリプトについて説明します。

boot

initを直接使用してシステムを起動するときに実行されます。選択したランレベルから独立で、一度だけ実行されます。これによって **/proc** ファイルシステムと **/dev/pts** ファイルシステムがマウントされ、**blogd**(ブートログ出力デーモン)が有効化されます。システムがアップデートまたはインストール後初めてブートされる場合、初期システム設定が起動します。

blogdデーモンは、**boot**および**rc**によって最初に起動されるサービスです。また、これらのスクリプトにより開始されたアクション(サブスクリプトの実行、たとえばブロック特殊ファイルを利用可能にする)が完了すると停止します。**blogd**は、**/var**が読み書き可能でマウントされている場合のみ、画面出力をログファイル**/var/log/boot.msg**に出力します。そうでない場合は、**/var**が利用できるようになるまで、**blogd**がすべての画面データをバッファします。**blogd**についての詳細は、**blogd(8)**の**man**ページを参照してください。

スクリプト**boot**はまた、**/etc/init.d/boot.d**の中の**S**で始まる名前のスクリプトをすべて起動します。そこで、ファイルシステムがチェックされ、必要に応じてループデバイスが設定されます。加えて、システム時間が設定されます。ファイルシステムの自動チェックや修復中にエラーが発生した場合、システム管理者はルートパスワードを入力して介入することができます。最後に、スクリプト**boot.local**が実行されます。

boot.local

ブート時、ランレベルへの移行前に実行する追加のコマンドを入力します。これは、**DOS**システムの**AUTOEXEC.BAT**に相当します。

boot.setup

このスクリプトは、シングルユーザモードから他のランレベルへの移行時に実行され、キーボードレイアウトや仮想コンソールの初期化に関する基本的な設定を行います。

halt

このスクリプトは、ランレベル 0 または 6 への移行時のみ実行され、halt または reboot として機能します。システムがシャットダウンするかリブートするかは、halt の呼び出され方に依存します。

rc

このスクリプトは、現在のランレベルの適切な停止スクリプトと、新しく選択したランレベルの起動スクリプトを呼び出します。

独自のスクリプトを作成して、先に説明したスキーマに容易に組み込むことができます。カスタムスクリプトの形式、名前付け、および構成方法は、LSB の仕様と、init、init.d、chkconfig、および insserv のマニュアルページを参照してください。加えて、startproc および killproc のマニュアルページも参照してください。

警告: init スクリプトのエラーはシステムの停止につながる

init スクリプトに問題があると、コンピュータがハングアップします。このようなスクリプトは最大限の注意を払って編集し、可能であれば、マルチユーザ環境で徹底的にテストします。init スクリプトに関する他の情報は、**20.2.1 項 「ランレベル」 (432 ページ)**を参照してください。

特定のプログラムまたはサービス用にカスタムの init スクリプトを作成する場合は、テンプレートとしてファイル /etc/init.d/skeleton を使用します。このファイルのコピーを別名で保存し、関連のプログラムやファイル名、パス、その他の詳細を必要に応じて編集します。また場合によっては、init プロシージャで正しいアクションが実行されるように、独自の改良をスクリプトに加える必要があります。

最初に記載されている INIT INFO ブロックはスクリプトの必須部分で、次のように編集する必要があります。詳細については、**例 20.1. 「最低限の INIT INFO ブロック」 (439 ページ)**を参照してください。

例 20.1 最低限のINIT INFOブロック

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

INFOブロックの最初の行では、**Provides:**の後に、このinitスクリプトで制御するプログラムまたはサービスの名前を指定します。「Required-Start:」および「Required-Stop:」行には、このサービスを開始/停止する前に開始/停止する必要があるすべてのサービスを指定します。この情報は後で、ランレベルディレクトリに表示するスクリプト名に対し、番号を生成するために使用します。Default-Start:およびDefault-Stop:の後に、サービスが自動的に起動または停止する際のランレベルを指定します。最後に、Description:の下に、対象のサービスについての簡単な説明を記載します。

ランレベルディレクトリ(/etc/init.d/rc?.d/)から/etc/init.d/内の対応するスクリプトへのリンクを作成するには、コマンドinsserv <新しいスクリプト名>を入力します。insservプログラムは、INIT INFOヘッダを評価して、ランレベルディレクトリ(/etc/init.d/rc?.d/)のスクリプトを起動、停止するために必要なリンクを作成します。このプログラムはまた、必要な番号をこれらのリンクの名前に取り込むことによって、ランレベルごとに正しい起動、停止の順序を管理します。グラフィックツールを使用してリンクを作成する場合は、**20.2.3項「YaSTでのシステムサービス(ランレベル)の設定」** (440 ページ)の説明に従って、YaSTのランレベルエディタを使用します。

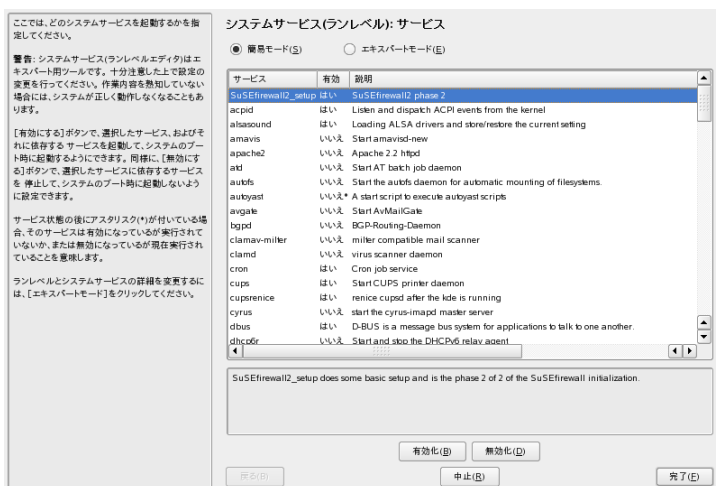
/etc/init.d/にすでに存在するスクリプトを既存のランレベルスキーマに統合する場合は、はじめにinsservを使用するか、YaSTのランレベルエディタで対応するサービスを有効にすることにより、ランレベルディレクトリにリンクを作成します。変更内容は、次のブート時に適用され、新しいサービスが自動的に起動します。

作成したリンクは手動で設定しないでください。INFOブロック内に誤りがある場合は、後で他のサービスに対してinsservを実行すると問題が生じます。手動で追加されたサービスは、このスクリプトに対するinsservの次回実行時に削除されます。

20.2.3 YaSTでのシステムサービス(ランレベル)の設定

[YaST] > [システム] > [システムサービス(ランレベル)] の順に選択して、このYaST moduleを起動すると、利用可能なすべてのサービスの概要と、各サービスの現在のステータス(有効か無効か)が表示されます。モジュールを[単純モード]と[エキスパートモード]のどちらで使用するかを決定します。ほとんどの場合、デフォルトの[単純モード]で十分です。左の列にはサービスの名前が、中央の列にはその現在のステータスが、右の列には簡単な説明が表示されます。ウィンドウの下部には、選択したサービスについての詳細な説明が表示されます。サービスを有効にするには、表でそれを選択し、[有効にする]を選択します。同じ手順で、サービスを無効にできます。

図 20.1 システムサービス(ランレベル)



サービスの起動または停止時のランレベルを詳細に制御する場合、またはデフォルトのランレベルを変更する場合は、はじめに[エキスパートモード]を選択します。上部には、現在のデフォルトのランレベル、つまり「initdefault」(システムのブート時にデフォルトで入るランレベル)が表示されます。通常、SUSE Linux Enterpriseシステムのデフォルトのランレベルは5(ネットワークありフルマルチユーザモードおよびX)です。適切な代替の設定は、ランレベル3(ネットワークありフルマルチユーザモード)です。

YaSTのダイアログボックスでは、ランレベルのいずれか1つを新しいデフォルトとして選択できます(表 20.1. 「ランレベルの種類」 (432 ページ)を参照)。また、このウィンドウのテーブルを使用して、個々のサービスやデーモンを有効、無効にできます。テーブルには、利用可能なサービスとデーモンが一覧表示され、現在システム上で有効かどうかと、有効な場合はそのランレベルが表示されます。マウスで行を選択し、ランレベルを表すチェックボックス(*[B]*、*[0]*、*[1]*、*[2]*、*[3]*、*[5]*、*[6]*、*[S]*)をクリックして、選択しているサービスまたはデーモンが実行されるランレベルを定義します。ランレベル4は、カスタムランレベルを作成できるように未定義になっています。最後に現在選択しているサービスまたはデーモンの簡単な説明が、テーブルの概要の下に表示されます。

[スタート／中止／更新] をクリックして、サービスを有効化するかどうかを決定します。現在の状態が自動的に確認されなかった場合は、[状態を更新] を使用して確認することができます。[設定／リセット] をクリックすると、変更をシステムに適用するか、ランレベルエディタの起動前に存在していた設定を復元するかを選択できます。[完了] を選択すると、設定の変更がディスクに保存されます。

警告: ランレベルの設定を誤るとシステムに害が及ぶことがある

ランレベルの設定が誤っていると、システムが使用できなくなることがあります。変更を実際に適用する前に、どういう結果が出るかをよく確認してください。

20.3 /etc/sysconfigによるシステム設定

SUSE Linux Enterpriseの主な設定は、/etc/sysconfigディレクトリに格納されている設定ファイルで指定できます。/etc/sysconfigディレクトリの個々のファイルは、それらが関係するスクリプトによってのみ読み込まれます。これにより、たとえば、ネットワークはネットワーク関連のスクリプトでのみ解析されるようになります。

システム設定を編集するには、2通りの方法があります。YaSTのsysconfigエディターを使う方法と、設定ファイルを手動で編集する方法です。

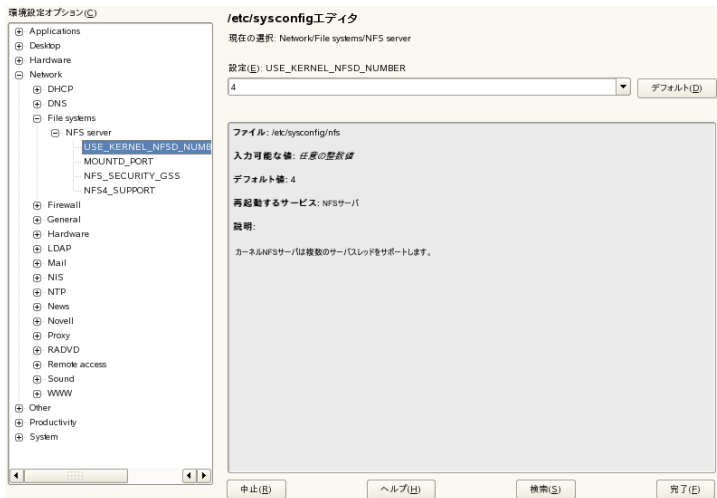
20.3.1 YaSTのsysconfigエディターを使ってシステム設定を変更する

YaSTのsysconfigエディタは、使いやすいシステム設定のフロントエンドです。変更する必要がある設定用変数の実際の場所が分からなくても、このモジュールに内蔵された検索機能を使うだけで、必要に応じて設定用変数の値を変更できますし、これらの変更の適用、sysconfigで設定されている値に基づく設定の更新、サービスのリスタートは、YaSTが行います。

警告: `/etc/sysconfig/*`ファイルの変更はインストールに害を及ぼすことがある

知識や経験が豊富でない限り、`/etc/sysconfig`ファイルは変更しないでください。場合によっては、システムに相当なダメージを与えることがあります。`/etc/sysconfig`のファイルには、各変数が持つ実際の効果を説明する簡単なコメントが付いています。

 **20.2** sysconfigエディタを使用したシステム設定



YaSTのsysconfigダイアログは、3つの部分に分かれています。ダイアログの左側には、すべての設定変数がツリー表示されます。変数を選択した段階で、右側に現在選択されている変数と、この変数の現在の設定が表示されます。

その下の3番目のウィンドウには、変数の目的、有効な値、デフォルト値、およびこの変数が設定されている実際の設定ファイルについての簡単な説明が表示されます。このダイアログボックスには、変数の変更後に実行された設定スクリプトや、変更の結果起動された新しいサービスについての情報も表示されます。YaSTにより変更の確認が求められ、[完了]を選択してダイアログを終了した後にはどのスクリプトが実行されるかが通知されます。現在は実行しないサービスやスクリプトを選択すると、それらが後で実行されます。YaSTはすべての変更を自動的に適用し、変更と関係のあるすべてのサービスをリスタートします。

20.3.2 システム設定を手動で変更する

システム設定を手動で変更するには、以下の手順に従います。

- 1 rootになります。
- 2 `init 1`コマンドで、システムをシングルユーザモード(ランレベル1)にします。
- 3 必要に応じて、設定ファイルを、自分が使っているエディタで変更します。

/etc/sysconfigの設定ファイルの変更にYaSTを使用しない場合、空の変数値は2つの引用符(KEYTABLE="")によって表し、空白を含む値へ引用符で囲むことに注意してください。語の値は、引用符で囲む必要はありません。

- 4 SuSEconfigを実行して、変更が有効になっていることを確認します。
- 5 `init default_runlevel`のようなコマンドで、システムを以前のランレベルに戻します。`default_runlevel`の部分は、システムのデフォルトのランレベルで置き換えてください。ネットワークとXのあるフルマルチユーザモードに戻るには5を、ネットワークのあるフルマルチユーザa[ドに戻るには3を選択します。

この手順は主に、ネットワーク設定など、システム全体の設定を変更する場合に必要です。小さな変更であれば、シングルユーザモードに移行する必要はありませんが、関与するすべてのプログラムが正しく再起動することを絶対的に保証する必要がある場合は、移行しても差し支えありません。

ティップ: 自動システム設定機能の設定

SuSEconfigの自動システム設定機能を無効にするに

は、`/etc/sysconfig/suseconfig`の`ENABLE_SUSECONFIG`を`no`に設定します。**SUSE**のインストールサポートを使用する場合は、**SuSEconfig**を無効にしないでください。無効にすると、自動設定も部分的に無効になる可能性があります。

ブートローダ

この章では、SUSE Linux Enterpriseで現在使用されているブートローダGRUBの設定方法について説明します。すべての設定操作には、特殊なYaSTモジュールを使用できます。Linuxでのブートに不慣れな場合は、以降の各セクションを読んで背景情報を理解してください。また、この章では、GRUBでのブート時に頻繁に発生する問題とその解決策についても説明します。

この章は、ブート管理とGRUBブートローダの設定に重点を置いています。ブート手順は、総じて第20章 *Linuxシステムのブートと設定* (427 ページ) で説明しています。ブートローダは、マシン(BIOS)とオペレーティングシステム(SUSE Linux Enterprise)の間のインタフェースになります。ブートローダの設定は、オペレーティングシステムの起動に直接影響を及ぼします。

次の用語は、この章で頻繁に使用されており、少し説明を加えた方がよいと思われるものです。

マスターブートレコード

MBRの構造は、オペレーティングシステムに依存しない規則に従って定義されます。最初の446バイトは、プログラムコード用に予約されています。通常、ここにはブートローダプログラムやオペレーティングシステムセクタの一部が保管されています。次の64バイトは、最大4つのエントリからなるパーティションテーブル用のスペースです(*パーティションのタイプ項* (174 ページ) を参照)。パーティションテーブルには、ハードディスクのパーティション分割とファイルシステムのタイプに関する情報が含まれています。オペレーティングシステムでハードディスクを処理するには、このテーブルが必要です。MBRの従来の汎用コードでは、1つのパーティションにだけアクティブのマークを付ける必要があります。MBRの最後の2バイトは、静的な「マジックナンバー」(AA55)を含む必要があ

ります。一部のBIOSでは、異なる値を持つMBRは無効とみなされ、ブートの対象とはみなされません。

ブートセクタ

ブートセクタは、拡張パーティションを除くハードディスクパーティションの最初のセクタであり、その他のパーティションの「コンテナ」として機能するだけです。これらのブートセクタのうち512バイトのスペースは、関連パーティションにインストールされているオペレーティングシステムをブートするためのコードが占有します。これは、フォーマット済みのDOS、Windows、およびOS/2パーティションのブートセクタに該当し、ファイルシステムの重要な基本データも一部含まれています。これに対して、Linuxパーティションのブートセクタは、XFS以外のファイルシステムの設定直後は当初空になっています。そのため、Linuxパーティションは、カーネルと有効なルートファイルシステムが含まれている場合にも、単独ではブートできません。システムブート用の有効なコードを含むブートセクタの場合、最後の2バイトにはMBRと同じマジックナンバー(AA55)があります。

21.1 ブートローダの選択

SUSE Linux Enterpriseでは、デフォルトでブートローダGRUBが使用されます。ただし、特殊なハードウェアやソフトウェアなど、状況によっては、LILOの方が必要な場合があります。LILOを使用していた古いバージョンのSUSE Linux Enterpriseからアップデートする場合、LILOがインストールされます。

LILOのインストールと設定についての詳細は、サポートデータベースのキーワードLILOの下、または「/usr/share/doc/packages/lilo」を参照してください。

21.2 GRUBによるブート

GRUB(Grand Unified Bootloader)は、2つのステージから成り立っています。stage1は512バイトで構成され、そのタスクは、ブートローダのstage2をロードすることだけです。その後、stage2が読み込まれます。このステージには、ブートローダの主要部分が含まれています。

一部の設定では、適切なファイルシステムからステージ2を検出し、ロードする中間ステージの1.5を使用できます。可能であれば、デフォルトでインストール時、またはYaSTを使用したGRUBの初回セットアップ時に、こ

stage2は、多くのファイルシステムにアクセスできます。現在、Windowsで使用されているExt2、Ext3、ReiserFS、Minix、およびDOS FATファイルシステムがサポートされます。BSDシステムで使用されているXFS、UFS、およびFFSも、特定の範囲までサポートされます。バージョン0.95以降のGRUBには、「El Torito」仕様に準拠するISO 9660標準ファイルシステムを含むCDまたはDVDからブートする機能も用意されています。システムをブートする前にも、GRUBはサポートされているBIOSディスクデバイス(BIOSにより検出されるフロッピーディスクまたはハードディスク、CDドライブ、およびDVDドライブ)のファイルシステムにアクセスできます。したがって、GRUBの設定ファイル(menu.lst)を変更しても、ブートマネージャを再インストールする必要はありません。システムをブートすると、GRUBはメニューファイルと共にカーネルまたは初期RAMディスク(initrd)の有効なパスとパーティションデータを再読み込みし、これらのファイルを検索します。

GRUBの実際の設定は、以下の3つのファイルに基づきます。

/boot/grub/menu.lst

このファイルには、GRUBでブートできるパーティションまたはオペレーティングシステムに関する情報がすべて含まれています。この情報が無い場合、GRUBコマンドラインは、どのように処理を続行するかユーザの指示を求めます(詳細については、[ブート手順実行中のメニューエントリの編集項](#) (453 ページ)を参照してください)。

/boot/grub/device.map

このファイルは、デバイス名をGRUBとBIOSの表記法からLinuxデバイス名に変換するために使います。

/etc/grub.conf

このファイルには、GRUBシェルでブートローダを正常にインストールするために必要なコマンド、パラメータおよびオプションが含まれています。

GRUBは、さまざまな方法で制御できます。グラフィカルメニュー(スプラッシュ画面)を使用して、既存の設定からブートエントリを選択できます。設定は、ファイルmenu.lstから読み込まれます。

GRUBでは、すべてのブートパラメータをブート前に変更できます。たとえば、メニューファイルを間違えて編集した場合は、この方法で訂正できます。また、一種の入力プロンプトからブートコマンドを対話形式で入力することもできます(「[ブート手順実行中のメニューエントリの編集項 \(453 ページ\)](#)」を参照してください)。GRUBには、ブート前にカーネルとinitrdの位置を判別する機能が用意されています。この機能を使用すると、ブートローダ設定にエントリが存在しないインストール済みオペレーティングシステムでもブートできます。

GRUBは、2種類のバージョンで存在します。ブートローダとして、または/usr/sbin/grub中のLinuxプログラムとしてです。このプログラムをGRUBシェルと呼びます。GRUBシェルは、インストールされたシステムにGRUBのエミュレーションを提供し、GRUBのインストールまたは新規設定の適用前のテストに使用できます。ハードディスクやフロッピーディスクにGRUBをブートローダとしてインストールする機能は、installコマンドとsetupコマンドの形でGRUBに組み込まれています。この機能は、Linuxの読み込み時にGRUBシェル内で使用できます。

21.2.1 GRUBのブートメニュー

ブートメニューを含むグラフィカルスプラッシュ画面は、GRUBの設定ファイル/boot/grub/menu.lstに基づいており、このファイルにはメニューを使用してブートできるパーティションまたはオペレーティングシステムに関する情報がすべて含まれています。

システムをブートするたびに、ファイルシステムからメニューファイルを読み込みます。このため、ファイルを変更するたびにGRUBを再インストールする必要があります。[21.3項「YaSTによるブートローダの設定」 \(457 ページ\)](#)で説明しているように、YaSTのブートローダを使用してGRUBの設定を変更します。

メニューファイルにはコマンドが含まれています。構文はきわめて単純です。各行には、コマンド1つとオプションのパラメータがシェルと同様にスペースで区切って指定されています。これまでの経緯が理由で、一部のコマンドでは最初の引数の前に等号(=)を使用することができます。コメントを記述するには、行頭にシャープ記号(#)を入力します。

メニュー概要の中にあるメニュー項目を識別できるように、各エントリに対してtitle(タイトル)を設定します。キーワードtitleの後に続くテキスト

(半角スペースも使用できます)は、メニューの中で、選択可能なオプションとして表示されます。そのメニュー項目が表示された場合、次のtitleまでに記述されているすべてのコマンドが実行されます。

最も簡単な例は、他のオペレーティングシステムのブートローダにリダイレクトすることです。該当するコマンドはchainloaderであり、引数は通常、他のパーティション内にあるブートブロックをGRUBのブロック表記に従って記述したものです。たとえば、次のようにします。

```
chainloader (hd0,3)+1
```

GRUBでのデバイス名については、**ハードディスクとパーティションに関する命名規則項(450ページ)**を参照してください。この例では、1台目のハードディスクの4番目のパーティションの最初のブロックを指定しています。

カーネルイメージを指定するには、kernelコマンドを使用します。最初の引数は、パーティションにあるカーネルイメージを表すパスです。他の引数は、そのコマンドラインでカーネルに渡されます。

ルートパーティションへのアクセスに必要なビルトインドライバがカーネルに用意されていない場合、または高度なhotplug機能のある新しいLinuxシステムが使用されていない場合は、initrdファイルへのパスを示す引数だけを指定して、別のGRUBコマンドでinitrdを指定する必要があります。initrdのロードアドレスは、ロードされるカーネルイメージに書き込まれるので、initrdコマンドは、kernelコマンドの後に記述する必要があります。

rootコマンドは、kernelとinitrdの各ファイルの指定を簡略化します。rootの引数は、デバイスまたはパーティションだけです。このデバイスは、すべてのカーネル、initrd、または次のrootコマンドまでデバイスが明示的に指定されて「ない他のファイルのパスに使用されます。

bootコマンドは各メニューエントリの最後に必ず含まれています。そのため、メニューファイルにこのコマンドを記述する必要はありません。ただし、GRUBをブート時に対話形式で使用する場合は、bootコマンドを最後に入力する必要があります。このコマンド自体は、引数を使用しません。単純に、読み込み済みのカーネルイメージ、または指定のチェーンローダをブートします。

すべてのメニューエントリを記述した後、その1つをdefaultエントリとして定義します。デフォルトエントリを指定しなかった場合、最初のエントリ(エ

ントリ0)が使用されます。デフォルトエントリがブートされるまでのタイムアウトを秒単位で指定することもできます。通常、`timeout` および `default` は、メニューエントリより先に記述します。サンプルファイルについては、[メニューファイルの例項](#) (451 ページ)を参照してください。

ハードディスクとパーティションに関する命名規則

GRUBでのハードディスクとパーティションの命名規則は、通常のLinuxデバイスの命名規則と異なっています。どちらかという、BIOSが使用する単純なディスクエミュレーションに似ており、構文は一部のBSDデリバティブで使用されているものに類似しています。GRUBでは、パーティション番号は0から始まります。これは、(hd0,0)は最初のハードディスクの最初のパーティションになります。ハードディスクがプライマリマスタとして接続されている一般的なデスクトップマシンでは、対応するLinuxデバイス名は/dev/hda1になります。

可能な4つの基本パーティションに、パーティション番号}0～3が割り当てられます。論理パーティション番号は4から始まります。

```
(hd0,0)  first primary partition of the first hard disk
(hd0,1)  second primary partition
(hd0,2)  third primary partition
(hd0,3)  fourth primary partition (usually an extended partition)
(hd0,4)  first logical partition
(hd0,5)  second logical partition
```

GRUBは、BIOSデバイスに依存するため、IDE、SATA、SCSIおよびハードウェアRAIDデバイス間を区別しません。BIOSまたは他のディスクコントローラで認識されるすべてのハードディスクには、BIOSの中で事前に設定されたブートシーケンスに従って番号が割り当てられます。

一般に、GRUBには、Linuxデバイス名をBIOSデバイス名に正確にマップする機能がありません。このマッピングはアルゴリズムを使用して生成され、`device.map`ファイルに保存されるため、必要に応じて編集できます。ファイル`device.map`については、[21.2.2項「device.mapファイル」](#) (454 ページ)を参照してください。

GRUBのフルパスは、カッコ内のデバイス名と、指定のパーティションにあるファイルシステム内のファイルへのパスで構成されます。このパスはスラッシュで始まります。たとえば、単一IDEハードディスクの最初のパーティショ

ンにLinuxを含んでいるシステムでは、ブート可能カーネルを次のように指定できます。

```
(hd0,0)/boot/vmlinuz
```

メニューファイルの例

次の例は、GRUBのメニューファイルの構造を示しています。このインストール例では、Linuxのブートパーティションが/dev/hda5、ルートパーティションが/dev/hda7、およびWindowsのインストールファイルが/dev/hda1にあります。

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
    kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
    initrd (hd0,4)/initrd

title windows
    chainloader (hd0,0)+1

title floppy
    chainloader (fd0)+1

title failsafe
    kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
    apm=off acpi=off vga=normal nosmp maxcpus=0 3
    initrd (hd0,4)/initrd.shipped
```

最初のブロックは、スプラッシュ画面の設定を定義します。

gfxmenu (hd0,4)/message

背景画像messageは、/dev/hda5パーティションの最上位ディレクトリにあります。

color white/blue black/light-gray

カラースキーマ:白(前景色)、青(背景色)、黒(選択項目)、明るい灰色(選択項目の背景色)です。配色はスプラッシュ画面には影響しません。影響を受けるのは、Escキーを押してスプラッシュ画面を終了するとアクセスできるカスタマイズ可能なGRUBメニューだけです。

default 0

最初のメニューエントリ `title linux` は、デフォルトでのブート対象です。

timeout 8

ユーザ入力がないまま8秒が経過した場合、**GRUB**は自動的にデフォルトエントリをブートします。自動ブートを無効にするには、`timeout`の行を削除します。`timeout 0`と設定すると、**GRUB**は待ち時間なしでデフォルトのエントリをブートします。

2番目の(最大)ブロックは、ブート可能な各種オペレーティングシステムを示します。個々のオペレーティングシステムに関するセクションは `title` で始まります。

- 最初のエントリ(`title linux`)は、**SUSE Linux Enterprise**をブートする役割を果たします。カーネル(`vmlinuz`)は、1台目のハードディスクの最初の論理パーティション(ブートパーティション)内に配置されています。ルートパーティションや**VGA**モードなどのカーネルパーティションは、ここに追加されます。ルートパーティションは、**Linux**の命名規則に従って指定されたものです(`/dev/hda7`)。この情報を読み込むのは**Linux**カーネルであり、**GRUB**は関係しないからです。`initrd`も、1台目のハードディスクの最初の論理パーティション内に配置されています。
- 第2のエントリは、**Windows**を読み込む役割を果たします。**Windows**は、1台目のハードディスク(`hd0,,0`)の最初のパーティションからブートされます。`chainloader +1` コマンドは、指定されたパーティションの最初のセクタを読み取って実行するよう**GRUB**に指示します。
- 次のエントリは、**BIOS**設定を変更することなく、フロッピーディスクからブートすることを可能にします。
- ブートオプション `failsafe` は、問題のあるシステム上でも**Linux**のブートを可能にするカーネルパラメータを選択して**Linux**を起動します。

メニューファイルは必要に応じて変更できます。その場合、**GRUB**は変更後の設定を次のブート時に使用します。このファイルを永続的に編集するには、**YaST**または好みのエディタを使用します。また、対話形式で一時的に変更するには、**GRUB**の編集機能を使用します。詳細については、**ブート手順実行中のメニューエントリの編集項** (453 ページ)を参照してください。

ブート手順実行中のメニューエントリの編集

グラフィカルブートメニューでは、ブートするオペレーティングシステムを矢印キーで選択します。Linuxシステムを選択した場合は、ブートプロンプトからブートパラメータを追加入力できます。個々のメニューエントリを直接編集するには、<Esc>キーを押してスプラッシュ画面を終了し、GRUBテキストベースメニューを表示してから<E>キーを押します。この方法で加えた変更は、現在のブートだけに適用され、永続的に採用されることはありません。

重要項目: ブート手順実行中のキーボードレイアウト

ブート時は、USキーボードレイアウトだけが使用可能です。図 51.1. 「US キーボードレイアウト」 (1001 ページ)の図を参照してください。

メニューエントリの編集により、障害が発生してブートできなくなったシステムを容易に修復できます。これは、ブートローダの設定ファイルの誤りをパラメータの手動入力により回避できるからです。ブート手順の中でパラメータを手動で入力する方法は、ネイティブシステムを損傷せずに新規設定をテストする際にも役立ちます。

編集モードを有効にした後、矢印キーを使用して、設定を編集するメニューエントリを選択します。設定を編集可能にするには、もう一度<E>キーを押します。このようにして、不正なパーティションまたはパス指定を、ブートプロセスに悪影響を及ぼす前に編集します。<Enter>キーを押して編集モードを終了し、メニューに戻ります。次に、キーを押してこのエントリをブートします。下部のヘルプテキストに、さらに可能なアクションが表示されます。

変更後のブートオプションを永続的に入力してカーネルに渡すには、ユーザのrootでファイルmenu.lstを開き、関連カーネルパラメータをスペースで区切って既存の行に追加します。

```
title linux
    kernel (hd0,0)/vmlinuz root=/dev/hda3 additional parameter
    initrd (hd0,0)/initrd
```

GRUBは、次のシステムブート時に新規パラメータを自動的に使用します。または、この変更をYaSTのブートローダモジュールで行うこともできます。新規パラメータをスペースで区切って既存の行に追加します。

21.2.2 device.mapファイル

device.mapファイルは、GRUBおよびBIOSのデバイス名をLinuxのデバイス名にマップします。IDEとSCSIの各ハードディスクが混在するシステムでは、GRUBは特殊プロシージャを使用してブートシーケンスの判定を試みる必要があります。これは、GRUBはBIOSのブートシーケンス情報にアクセスできない場合があるためです。GRUBはこの分析の結果をファイル/boot/grub/device.mapに保存します。BIOS内でブートシーケンスがIDE、SCSIの順に設定されているシステムの場合、ファイルdevice.mapは次のようになります。

```
(fd0)  /dev/fd0
(hd0)  /dev/hda
(hd1)  /dev/sda
```

IDE、SCSI、および他のハードディスクのシーケンス(順序)は、さまざまな要因によって異なり、Linuxではマッピングを識別できないため、device.mapファイル内のシーケンスは手動で設定できます。ブート時に問題に直面した場合、このファイル内のシーケンスが、BIOS内のシーケンスに対応しているかどうかチェックします。さらに、必要に応じてGRUBは、前者を一時的に変更するように指示します。Linuxシステムのブート後に、YaSTブートロードモジュールまたは好みのエディタを使用して、device.mapファイルを永続的に変更できます。

重要項目: SATAディスク

コントローラによっては、SATAディスクはIDE (/dev/hd x)か、SCSI (/dev/sd x)のいずれのデバイスとして認識されます。

device.mapを手動で編集した後、次のコマンドを実行してGRUBを再インストールします。このコマンドにより、device.mapファイルが再読み込みされ、grub.confに指定されているコマンドが実行されます。

```
grub --batch < /etc/grub.conf
```

21.2.3 /etc/grub.confファイル

menu.lstおよびdevice.mapの次に重要な第3のGRUB設定ファイルは、/etc/grub.confです。このファイルには、GRUBシェルでブートローダを正常にインストールするために必要なコマンド、パラメータおよびオプションが含まれています。

```
root (hd0,4)
  install /grub/stage1 (hd0,3) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
quit
```

各エントリの意味:

root (hd0,4)

このコマンドは、GRUBに対して後続のコマンドを1台目のハードディスクの最初の論理パーティション(ブートファイルの位置)に適用するように指示します。

installパラメータ

grubコマンドには、installパラメータを指定して実行しなければなりません。ブートローダのstage1は、拡張パーティションコンテナ (/grub/stage1 (hd0,3)) にインストールする必要があります。この設定は多少複雑ですが、多くの事例で動作することが確認されています。stage2は、メモリアドレス 0x8000 (/grub/stage2 0x8000) にロードする必要があります。最後のエントリ ((hd0,4)/grub/menu.lst) は、メニューファイルを探す場所をGRUBに伝えます。

21.2.4 ブートパスワードの設定

オペレーティングシステムのブート前でも、GRUBはファイルシステムへのアクセスを可能にします。rootパーミッションを持たないユーザは、システムのブート後、アクセス権のないLinuxシステム上のファイルにアクセスできます。この種のアクセスを阻止したり、ユーザによる特定のオペレーティングシステムのブートを防止するために、ブートパスワードを設定できます。

重要項目: ブートパスワードとスプラッシュ画面

GRUBにブートパスワードを使用する場合、通常のスプラッシュ画面は表示されません。

ユーザrootとして、次の手順に従ってブートパスワードを設定します。

- 1 rootプロンプトで、grub-md5-cryptを使ってパスワードを暗号化します。

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

- 2 暗号化後の文字列を、menu.lstファイルのグローバルセクションに貼り付けます。

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

これで、ブートプロンプトからGRUBコマンドを実行するには、先にPキーを押してパスワードを入力する操作が必要になります。しかし、ユーザはブートメニューから引き続き任意のオペレーティングシステムをブートすることができます。

- 3 ブートメニューから1つまたは複数のオペレーティングシステムをブートする操作を禁止するには、menu.lst内で、パスワードを入力しなければブートできないようにする必要のある各セクションにエントリlockを追加します。たとえば、次のようにします。

```
title linux
    kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
    initrd (hd0,4)/initrd
    lock
```

システムをリブートしてブートメニューからLinuxエントリを選択すると、次のエラーメッセージが表示されます。

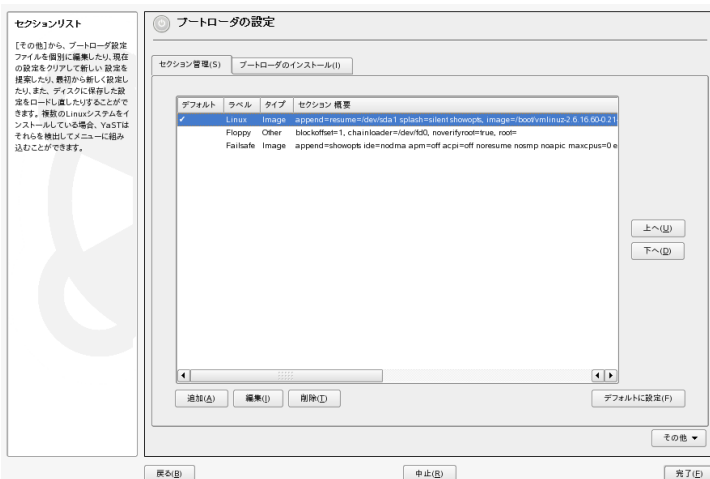
Error 32: Must be authenticated

<Enter>キーを押してメニューを表示します。次に、<P>キーを押してパスワードプロンプトを表示します。パスワードを入力して<Enter>キーを押すと、選択したオペレーティングシステム(この場合はLinux)がブートします。

21.3 YaSTによるブートローダの設定

SUSE Linux Enterpriseシステムでブートローダを設定する最も簡単な方法は、YaSTモジュールを使用することです。YaSTコントロールセンタで、[システム]、> [ブートローダ] の順に選択します。図 21.1. 「ブートローダの設定」(457 ページ)で説明しているように、システムの現在のブートローダ設定が表示され、設定を変更できます。

図 21.1 ブートローダの設定



[セクション管理] タブでは、各オペレーティングシステムのブートローダセクションの編集、変更、削除を行うことができます。オプションを追加するには、[追加] をクリックします。既存のオプションの値を変更するには、マウスで選択してから [編集] をクリックします。既存のエントリを削除するには、エントリを選択して [削除] をクリックします。ブートローダのオ

プシオンをよくご存知でない場合には、はじめに**21.2項「GRUBによるブート」** (446 ページ)を参照してください。

[ブートローダのインストール] タブで、タイプ、場所、高度なローダ設定に関する設定を表示および変更できます。

[その他] をクリックすると開くドロップダウンメニューから、高度な設定オプションにアクセスします。組み込みエディタでGRUB設定ファイルを変更できます(詳細は**21.2項「GRUBによるブート」** (446 ページ)を参照してください)。既存の設定を削除して新しい設定を作成したり、YaSTで新しい設定を提案できます。設定をディスクに書き込んだり、ディスクから設定を読み直すこともできます。インストール中に保存された元のマスタブートレコードを復元するには、[ハードディスクのMBRの復元] を選択します。

21.3.1 ブートローダのタイプ

[ブートローダのインストール] でブートローダのタイプを設定します。SUSE Linux EnterpriseのデフォルトのブートローダはGRUBです。LILOを使用するには、以下の手順に従います。

手順 21.1 ブートローダのタイプの変更

- 1 [ブートローダのインストール] タブを選択します。
- 2 [ブートローダ] で、[LILO] を選択します。
- 3 表示されるダイアログボックスで、次のオプションのうち、いずれかを選択します。

新しい設定を提案する

YaSTは新しい設定を提案します。

Convert Current Configuration (現在の設定を変換する)

YaSTは現在の設定を変換します。設定を変換すると、いくつかの設定内容が失われることがあります。

Start New Configuration from Scratch (新しい設定を新規に作成する)

カスタム設定を書き込みます。この動作は、SUSE Linux Enterpriseのインストール時には利用できません。

Read Configuration Saved on Disk (ディスクに保存されている設定を読み込む)

独自の/etc/lilo.confをロードします。この動作は、SUSE Linux Enterpriseのインストール時には利用できません。

4 [OK] をクリックして、変更内容を保存します。

5 メインのダイアログで [完了] をクリックして、変更を適用します。

変換中に、古いGRUB設定はディスクに保存されます。これを使用するには、ブートローダのタイプをGRUBに戻し、[Restore Configuration Saved before Conversion] を選択します。この操作は、インストール済みのシステムでのみ実行可能です。

注意: カスタムのブートローダ

GRUBやLILO以外のブートローダを使用する場合は、[ブートローダはインストールしないでください] を選択します。このオプションを選択する場合には、あらかじめ、ブートローダのドキュメントをよくお読みください。

21.3.2 ブートローダの場所

ブートローダの場所を変更するには、次の手順に従います。

手順 21.2 ブートローダの場所の変更

1 [ブートローダのインストール] タブを選択し、[ブートローダの場所] について次のオプションのうち、いずれかを選択します。

ブートパーティションからブート

/bootパーティションのブートセクタです。

拡張パーティションからブート

拡張パーティションコンテナにブートローダがインストールされます。

マスタブートレコードからブート

最初のディスクのMBRにブートローダをインストールします(BIOS中のブートシーケンスプリセットによる)。

ルートパーティションからブート

/パーティションのブートセクタにブートローダがインストールされます。

カスタムブートパーティション

このオプションを選択すると、手動でブートローダの場所を指定できます。

- 2 [完了] をクリックして、変更を適用します。

21.3.3 標準のシステム

デフォルトでブートされるシステムを変更するには、次の手順に従います。

手順 21.3 標準のシステムの設定

- 1 [セクション管理] タブを開きます。
- 2 リストから目的の項目を選択します。
- 3 [デフォルトにする] をクリックします。
- 4 [完了] をクリックして、変更を有効にします。

21.3.4 ブートローダのタイムアウト

ブートローダは、標準のシステムを直ちにブートするわけではありません。タイムアウト中、ブートまたはカーネルパラメータを書き込むシステムを選択できます。ブートローダのタイムアウトを設定するには、次の手順に従います。

手順 21.4 ブートローダのタイムアウトの変更

- 1 [ブートローダのインストール] タブを開きます。
- 2 [ブートローダのオプション] をクリックします。

- 3 新しい値を入力するか、マウスで矢印キーをクリックするか、またはキーボードの矢印キーを使って、[タイムアウト(秒)] の値を変更します。
- 4 [OK] をクリックします。
- 5 [完了] をクリックして、変更を保存します。

21.3.5 セキュリティの設定

このYaSTモジュールでは、ブートを保護するためのパスワードを設定することもできます。そうすれば、セキュリティに付加的なレベルを追加できます。

手順 21.5 ブートローダパスワードの設定

- 1 [ブートローダのインストール] タブを開きます。
- 2 [ブートローダのオプション] をクリックします。
- 3 [メニューインタフェースのパスワード] でパスワードを設定します。
- 4 [OK] をクリックします。
- 5 [完了] をクリックして、変更を保存します。

21.4 Linuxブートローダのアンインストール

YaSTを使用してLinuxブートローダをアンインストールし、MBRをLinuxインストール前の状態に戻すことができます。インストール中に、YaSTは自動的にオリジナルMBRのバックアップコピーを作成しており、要求があるとMBRを復元します。

GRUBをアンインストールするには、YaSTブートローダモジュールを起動します(システム> ブートローダの設定)。その他> ハードディスクのMBRの復元を選択し、はい、上書きしますで確認します。

21.5 ブートCDの作成

ブートマネージャを使用してシステムをブートできない場合、またはハードディスクやフロッピーディスクのMBRにブートマネージャをインストールできない場合は、Linuxに必要なすべての起動ファイルを使用してブート可能CDを作成することもできます。そのためには、システムにCDライターがインストールされている必要があります。

GRUBでは、*stage2_eltorito*という特殊形式のstage2とカスタマイズされたmenu.lst(オプション)を使用するだけで、ブート可能CDROMを作成することができます。従来のファイルstage1およびstage2は不要です。

手順 21.6 ブートCDの作成

- 1 以下のように、ISOイメージの作成先ディレクトリに移動します。cd /tmp

- 2 GRUB用のサブディレクトリを作成します。

```
mkdir -p iso/boot/grub
```

- 3 カーネル、stage2_eltorito、initrd、menu.lstおよびmessage ファイルをiso/boot/にコピーします。

```
cp /boot/vmlinuz iso/boot/  
cp /boot/initrd iso/boot/  
cp /boot/message iso/boot/  
cp /usr/lib/grub/stage2_eltorito iso/boot/grub  
cp /boot/grub/menu.lst iso/boot/grub
```

- 4 CD-ROMデバイスを指すようにiso/boot/grub/menu.lstのパスエントリを調整します。そのためには、パス名に(sd*)形式で表示されるハードディスクのデバイス名を、CD-ROMドライブのデバイス名(cd)で置き換えます。

```
timeout 8  
default 0  
gfxmenu (cd)/boot/message  
  
title Linux  
root (cd)  
kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
```

```
splash=verbose showopts  
initrd /boot/initrd
```

ブート処理時にブートメッセージの表示を防止するには、
「splash=verbose」の代わりに「splash=silent」を使用します。

5 次のコマンドでISOイメージを作成します。

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \  
-boot-load-size 4 -boot-info-table -o grub.iso /tmp/iso
```

6 好みのユーティリティを使用して、生成されたファイルgrub.isoをCD に書き込みます。ISOイメージをデータファイルとして書き込まず、お 使いのCD書き込みユーティリティのCDイメージ作成オプションを使用 します。

21.6 SUSEのグラフィカル画面

SUSE Linux 7.2以降は、オプション `vga=value` がカーネルパラメータとして
使用されている場合、SUSEのグラフィカル画面が1番目のコンソール上に表
示されます。YaSTを使用してインストールする場合、このオプションは、選
択した解像度とグラフィックカードに基づいて自動的に使用されます。必要
な場合にSUSEの画面を無効にするには、3つの方法があります。

必要に応じてSUSE画面を無効にする。

コマンドラインでコマンド `echo 0 >/proc/splash` を入力し、グラフィ
カル画面を無効にします。画面を再度有効にするには、`echo 1
>/proc/splash` コマンドを入力します。

デフォルトでSUSE画面を無効にする。

カーネルパラメータ `splash=0` をブートローダの設定に追加します。これ
については、[第21章 ブートローダ](#) (445 ページ) を参照してください。ただ
し、前のバージョンでデフォルトとなっていたテキストモードを選択する
場合は、`vga=normal` を設定します。

SUSE画面を完全に無効にする。

新しいカーネルをコンパイルし、*framebuffer support* でオプション *Use splash
screen instead of boot logo* を無効にします。

ティップ

カーネルでフレームバッファのサポートを無効にすると、スプラッシュ画面も自動的に無効になります。システムをカスタムカーネルで実行した場合、SUSE はサポートを何も提供することができません。

21.7 トラブルシューティング

ここでは、GRUBを使用してブートする際に頻繁に発生する一部の問題と、考えられる解決策の概略について説明します。一部の問題については、<http://support.novell.com/>のKnowledgebase(ナレッジベース)に記事が提供されています。「GRUB」、「ブート」、および「ブートローダ」などのキーワードを使って検索を行うには、検索ダイアログを使用します。

GRUBとXFS

XFSの場合、パーティションブートブロックにはstage1のための余地がありません。そのため、ブートローダの位置としてXFSパーティションを指定しないでください。この問題は、XFSでフォーマットされていない別のブートパーティションを作成することで解決できます。

GRUBがGRUB Geomエラーを報告した

GRUBは、システムのブート時に、接続されているハードディスクのジオメトリを検査します。ときには、BIOSから一貫性のない情報が戻され、GRUBがGRUB Geom Errorをレポートする場合があります。このような場合は、LILOを使用するか、BIOSを更新します。LILOのインストール、設定、および保守の詳細については、Support Database (サポートデータベース)でキーワード「LILO」を使用すると検索できます。

また、LinuxがBIOSに登録されていない追加ハードディスクにインストールされている場合にも、GRUBはこのエラーメッセージを戻します。ブートローダのstage1は正常に検出されロードされますが、stage2は検出されません。この問題は、新規ハードディスクをBIOSに登録することで解消できます。

IDEハードディスクとSCSIハードディスクを搭載したシステムがブートしないインストール中、YaSTは、ハードディスクのブートシーケンスを誤って判断する場合があります。たとえば、GRUBが/dev/hdaをhd0、/dev/

sdaをhd1と見なしても、BIOS内ではブートシーケンスが逆(IDEの前にSCSI)になっている場合があります。

この場合は、ブートプロセス中にGRUBコマンドラインを使用してハードディスクを訂正します。システムのブート後に、device.mapファイルを編集して新規マッピングを永続的に適用します。次に、/boot/grub/menu.lstファイルと/boot/grub/device.mapファイルでGRUBデバイス名を検査し、次のコマンドでブートローダを再インストールします。

```
grub --batch < /etc/grub.conf
```

2台目のハードディスクからのWindowsのブート

Windowsのような一部のオペレーティングシステムは、1台目のハードディスクからのみブートできます。この種のオペレーティングシステムが2台目以降のハードディスクにインストールされている場合は、関連メニューエントリに対して論理的な変更を加えることができます。

```
...
title windows
    map (hd0) (hd1)
    map (hd1) (hd0)
    chainloader (hd1,0)+1
...
```

この例では、Windowsは2台目のハードディスクから起動されます。この目的で、mapを使用して、ハードディスクの論理的な順序を変更します。この変更は、GRUBのメニューファイル内のロジックには影響を及ぼしません。したがって、2台目のハードディスクはchainloaderに対して指定する必要があります。

21.8 詳細情報

GRUBの詳細情報は、<http://www.gnu.org/software/grub/>で入手できます。また、grub情報ページも参照してください。<http://www.novell.com/support>にあるTechnical Information Search(技術情報検索)で、キーワード「GRUB」を検索して、特別な事項に関する情報を入手することもできます。

特別なシステム機能

この章では、はじめに、さまざまなソフトウェアパッケージAバーチャルコンソール、およびキーボードレイアウトについて説明します。bash、cron、およびlogrotateといったソフトウェアコンポーネントについても説明します。これらは、前回のリリースサイクルで変更または強化されたからです。これらのコンポーネントはそれほど重要ではないと思われるかもしれませんが、システムと密接に結びついているものなので、デフォルトの動作を変更したい場合もあることでしょう。この章の最後では、言語および国固有設定(I18NおよびL10N)について説明します。

22.1 特殊ソフトウェアパッケージ

bash、cron、logrotate、locate、ulimit、およびfreeといったプログラム、およびresolv.confファイルは、システム管理者および多くのユーザにとって非常に重要です。manのページとinfoのページは、コマンドについての2つの役立つ情報源ですが、その両方が常に利用できるとは限りません。GNU Emacsは、人気のある、自由度に設定できるテキストエディタです。

22.1.1 bashパッケージと/etc/profile

Bashはデフォルトのシステムシェルです。ログインシェルとして使用する場合には、いくつかの初期化ファイルを読み込みます。Bashは、各ファイルを次の順序で処理します:

1. /etc/profile
2. ~/.profile
3. /etc/bash.bashrc
4. ~/.bashrc

~/.profileまたは~/.bashrcに、カスタム設定を行います。これらのファイルを正しく処理するには、基本設定ファイル/etc/skel/.profileまたは/etc/skel/.bashrcを、ユーザのホームディレクトリにコピーする必要があります。更新後、/etc/skelから設定ファイルをコピーすることをお勧めします。次のシェルコマンドを実行して、既存の個人別設定が失われるのを防止します。

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

それから、個人的な調整点を、*.oldファイルから書き戻します。

22.1.2 cronパッケージ

コマンドを、前もって決めた時間に、定期的かつ自動的にバックグラウンドで実行したい場合、**cron**を用います。**cron**は特別な形式のタイムテーブルに従って起動します。その一部はシステムに付属しています。ユーザは必要に応じ、自分自身のテーブルを書くことができます。

cronテーブルは、/var/cron/tabsにあります。/etc/crontabはシステム全体の**cron**テーブルとして機能します。ユーザ名を入力して、タイムテーブルの後、コマンドの前に直接コマンドを実行するようにします。では、**例 22.1. 「/etc/crontab内のエントリ」** (468 ページ)rootが入力されています。/etc/cron.dにあるパッケージ固有のテーブルも同じ形式です。**cron**のマニュアルページを参照してください(man cron使用)。

例 22.1 /etc/crontab内のエントリ

```
1-59/5 * * * * root    test -x /usr/sbin/atrun && /usr/sbin/atrun
```

/etc/crontabを、`crontab -e`コマンドで編集することはできません。これは、エディタに直接ロードして、変更し、保存する必要があります。

複数のパッケージによりシェルスクリプトが/etc/cron.hourly、/etc/cron.daily、/etc/cron.weekly、および/etc/cron.monthlyの各ディレクトリにインストールされます。これらの実行は、/usr/lib/cron/run-cronsによって制御されます。/usr/lib/cron/run-cronsは、15分おきにメインテーブル(/etc/crontab)から実行されます。これにより、無視されていたプロセスが、適切な時刻に実行されることが保証されます。

管理用のスクリプトを1時間ごと、毎日、または他の特定の周期で実行するには、/etc/crontabのエントリで、定期的に、使用するタイムスタンプファイルを削除します(「[例 22.2. 「/etc/crontab:タイムスタンプファイルの削除」](#) (469 ページ)」を参照してください。そこでは、hourlyという名前の付いているファイルが毎時59分に、dailyという名前の付いているファイルが毎日午前 2::14に削除されるようになっていきます)。

例 22.2 /etc/crontab:タイムスタンプファイルの削除

```
59 * * * * root rm -f /var/spool/cron/lastrun/cron.hourly
14 2 * * * root rm -f /var/spool/cron/lastrun/cron.daily
29 2 * * 6 root rm -f /var/spool/cron/lastrun/cron.weekly
44 2 1 * * root rm -f /var/spool/cron/lastrun/cron.monthly
```

または、/etc/sysconfig/cronのDAILY_TIMEをcron.dailyを起動する時刻に設定します。MAX_NOT_RUNの設定では、ユーザが長期にわたってコンピュータを指定したDAILY_TIMEに起動しなくても、毎日のジョブの実行がトリガされるようにします。MAX_NOT_RUNの最大値は14日です。

日常のシステムメンテナンスジョブは、わかりやすいようにさまざまなスクリプトに分散されています。これらはパッケージaaa_baseに含まれています。たとえば、/etc/cron.dailyディレクトリには、コンポーネントsuse.de-backup-rpmdb、suse.de-clean-tmp、またはsuse.de-cron-localがあります。

22.1.3 ログファイル:パッケージlogrotate

カーネル自体に加え、定期的にシステムステータスおよび特定のイベントをログファイルに記録する多数のシステムサービス(デーモン)があります。これ

により、管理者は、ある特定時期のシステムステータスを定期的を確認し、エラーまたは問題のある機能を認識し、正確にトラブルシューティングできます。通常、これらのログファイルは、FHSで指定されるように/var/log内に格納され、毎日記録が追加されるためにサイズが増大します。logrotateパッケージを使用して、これらのファイルが増大するのを制御できます。

/etc/logrotate.confファイルを使用して、logrotateを設定します。特に、includeには、最初に読み込む追加ファイルを設定します。ログファイルを生成しないプログラムは、個別の環境設定ファイルを/etc/logrotate.dにインストールします。たとえば、そのようなファイルは、apache2 (/etc/logrotate.d/apache2)およびsyslogd (/etc/logrotate.d/syslog) パッケージに含まれています。

例 22.3 /etc/logrotate.confの例

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#     monthly
#     create 0664 root utmp
#     rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotateは、cronによって制御され、/etc/cron.daily/logrotateにより毎日呼び出されます。

重要項目

createオプションは、管理者によって/etc/permissions*内に作成されるすべての設定を読み取ります。個人的な変更によっていずれの競合も発生することがないようにしてください。

22.1.4 locateコマンド

ファイルをすばやく検索するためのlocateコマンドは、標準のインストール済みソフトウェアには含まれていません。必要であれば、パッケージfind-locateをインストールしてください。updatedbプロセスは、毎晩、またはシステムをブートしてから約15分で自動的に起動します。

22.1.5 ulimitコマンド

ulimit (使用制限)コマンドを使用すると、システムリソースの使用量に制限を設けたり、これらの制限を表示したりすることができます。ulimitは、アプリケーションでの使用可能メモリを制限する場合に特に便利です。1つのアプリケーションが大量のメモリを独占するとシステムが停止してしまいますが、これを使用することで、それが避けられます。

ulimitコマンドには、さまざまなオプションがあります。メモリの使用量を制限するには、表22.1.「ulimit:ユーザのためのリソースの設定」(471 ページ)に示すオプションを使用します。

表 22.1 ulimit: ユーザのためのリソースの設定

-m	物理メモリの最大サイズ
-v	仮想メモリの最大サイズ
-s	スタックの最大サイズ
-c	コアファイルの最大サイズ
-a	制限セットの表示

システム全体のエントリは、`/etc/profile`で設定できます。コアファイルの作成を有効にします。これはプログラマがデバッグを行うために必要です。通常のユーザは、`/etc/profile`ファイルでシステム管理者が指定した値を大きくすることはできませんが、`~/.bashrc`に特別なエントリを作成することは可能です。

例 22.4 `ulimit:~/.bashrc`中の設定

```
# Limits of physical memory:
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

メモリの量は、**KB**単位で指定する必要があります。詳細については、`man bash`コマンドで**man**ページを参照してください。

重要項目

すべてのシェルがPAM(たとえば、`pam_limits`)を使用すれば、包括的な調整が可能になります。

22.1.6 freeコマンド

現在使用されている**RAM**の容量を確認することが目的ならば、`free`コマンドは、少々誤解を招くかもしれません。そのような情報は、`/proc/meminfo`で表示できます。今日では、**Linux**のような最新のオペレーティングシステムにアクセスする場合、ユーザはメモリについてそれほど深刻に考える必要はありません。利用可能な**RAM**という概念は、統一的なメモリ管理が生まれる以前の遺物です。空きメモリは悪いメモリというスローガンは、**Linux**にぴったりで。結果として、**Linux**では、空きメモリや未使用メモリを実質的に発生させず、キャッシュの量を調整するよう努力が重ねられてきました。

基本的に、カーネルは、アプリケーションやユーザデータについての直接的な知識はありません。その代わりにカーネルは、ページキャッシュのアプリケーションとユーザデータを管理します。メモリが不足すると、その一部はスワップパーティションかファイルに書き込まれ、そこから**mmap**コマンドで読み込まれます(`man mmap`コマンドで**man**ページを参照)。

カーネルには、たとえば、ネットワークアクセスに使用されたキャッシュが格納されている`slab`キャッシュなどの別のキャッシュがあります。これが`/proc/meminfo`のカウント間の違いになります。全部ではありませんが、これらのキャッシュのほとんどは、`/proc/slabinfo`でアクセスできます。

22.1.7 /etc/resolv.confファイル

ドメイン名は、`/etc/resolv.conf`ファイルを使用して管理されます。参照先 **第33章 ドメインネームシステム** (673 ページ)。

このファイルを更新できるのは、スクリプト`/sbin/modify_resolvconf`のみで、他のプログラムには`/etc/resolv.conf`ファイルを直接変更するパーミッションがありません。このルールを強制することによってのみ、システムのネットワークの環境設定と関連のファイルが一貫性のある状態に維持されます。

22.1.8 manページとinfoページ

一部のGNUアプリケーション(`tar`など)では、`man`ページが提供されなくなりました。`man`ページが用意されていたコマンドについては、`--help`オプションを使用して簡単な概要を表示するか、詳細な手順を説明する`info`ページを使用します。`info`は、GNUのハイパーテキストシステムです。このシステムについての説明は、`info info`と入力してください。`Info` ページは、`emacs -f info`コマンドを入力してEmacsを起動するか、コンソールで直接`info`と入力します。あるいは、`tkinfo`、`xinfo`、またはヘルプシステムを使用して、`info`ページを表示します。

22.1.9 GNU Emacs用の設定

GNU Emacsは、複合作業環境です。ここでは、GNU Emacsを起動する際に処理される設定ファイルについて説明します。詳細については、<http://www.gnu.org/software/emacs/>を参照してください。

Emacsは起動時に、ユーザ、システム管理者、およびカスタマイズまたは事前設定のディストリビュータに関する設定が含まれているいくつかのファイルを読み取ります。`~/.emacs`初期化ファイルは、`/etc/skel`から各ユーザのホーム

ディレクトリにインストールされます。その後、`.emacs`は、`/etc/skel/.gnu-emacs`ファイルを読み取ります。プログラムをカスタマイズするには、`.gnu-emacs`をホームディレクトリにコピーし(`cp /etc/skel/.gnu-emacs ~/.gnu-emacs`を使用)、このディレクトリで希望どおりに設定します。

`.gnu-emacs`は、`~/.gnu-emacs-custom`ファイルを`custom-file`として定義します。**Emacs**で`customize`を使用して設定を行う場合、この設定は、`~/.gnu-emacs-custom`に保存されます。

SUSE® Linux Enterpriseにより、`emacs`パッケージは、`site-start.el`ファイルを`/usr/share/emacs/site-lisp`ディレクトリ内にインストールします。`site-start.el`ファイルは、`~/.emacs`初期化ファイルの前にロードされます。`site-start.el`は、`psgml`などの**Emacs**アドオンパッケージと共に配布される特殊な設定ファイルが自動的にロードされるようにします。この種類の設定ファイルも`/usr/share/emacs/site-lisp`に置かれ、ファイル名は常に`suse-start-`で始まります。ローカルのシステム管理者は、`default.el`でシステム全体の設定を指定できます。

これらのファイルに関する詳しい説明は、*InitFile*: info:/emacs/InitFile。これらのファイルを無効にする(必要な場合)方法についても記載されています。

Emacsのコンポーネントは、いくつかのパッケージに分かれています。

- 基本パッケージの`emacs`。
- `emacs-x11`(通常インストールされている): **X11**をサポートしているプログラム。
- `emacs-nox`: **X11**をサポートしていないプログラム。
- `emacs-info:info`形式のオンラインマニュアル。
- `emacs-el`: **Emacs Lisp**内のコンパイルされていないライブラリファイル。これらは、実行時には必要ありません。
- 必要に応じて`emacs-auctex`(**LaTeX**用)、`psgml`(**SGML**および**XML**用)、`gnuserv`(クライアント/サーバ操作)など、さまざまなアドオンパッケージをインストールできます。

22.2 バーチャルコンソール

Linuxは、マルチユーザ、マルチタスクのシステムです。これらの機能は、スタンドアロンのPCシステム上でも利用できます。テキストモードでは、6つのバーチャルコンソールが使用できます。これらの切り替えには、**Alt + F1** から **Alt + F6** を使用します。7番目のコンソールはX用に予約されており、10番目のコンソールにはカーネルメッセージが表示されます。コンソールの割り当て数は、`/etc/inittab` ファイルを修正すれば変更できます。

Xを終了せずにXからコンソールに切り替えるには、**Ctrl + Alt + F1** から **Ctrl + Alt + F6** を使用します。Xに戻るには、**Alt + F7** を押します。

22.3 キーボードマッピング

プログラムのキーボードマッピングを標準化するために、次のファイルに変更が行われました。

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

これらの変更は、`terminfo` エントリを使用するか、その設定ファイルが直接変更されるアプリケーション(`vi`、`less`など)にのみ影響します。.. システムに付随しないアプリケーションは、これらのデフォルト値に合わせる必要があります。

Xでは、**Compose**キー(マルチキー)は、**<Ctrl + Shift**キー(右)を使用してアクセスできます。対応するエントリも`/etc/X11/Xmodmap`に示されます。

詳しい設定は、**X**キーボード拡張(**XKB**)を使って行うことができます。この拡張機能は、デスクトップ環境GNOME(`gswitchit`)およびKDE (`kxkb`)によっても使用されます。

ティップ: 詳細情報

XKBに関する説明は、`/etc/X11/xkb/README`とそこにリストされた文書にあります。

中国語、日本語、および韓国語(CJK)に関する詳しい説明は、<http://www.suse.de/~mfabian/suse-cjk/input.html>のMike Fabianのページにあります。

22.4 言語および国固有の設定

本システムは、非常に広い範囲で国際化されており、現地の状況に合わせて柔軟に変更できます。言い換えれば、国際化(I18N)によって具体的なローカライズ(L10N)が可能になっています。I18NとL10Nという略語は、語の最初と最後の文字の間に、省略されている文字数を挟み込んだ表記です。

設定は、ファイル`/etc/sysconfig/language`の変数`LC_`で定義します。これは、単なる現地語サポートだけでなく、*Messages* (メッセージ)(言語)、*Character Set* (文字セット)、*Sort Order* (ソート順)、*Time and Date* (時刻と日付)、*Numbers* (数字)および*Money* (通貨)の各カテゴリも指します。これらのカテゴリはそれぞれ、独自の変数を使用して直接定義することも、ファイル`language`にあるマスタ変数を使用して間接的に定義することも可能です(`man locale`コマンドで`man`ページを参照)。

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`,
`RC_LC_NUMERIC`, `RC_LC_MONETARY`

これらの変数は、プレフィクス`RC_`を付けずにシェルに渡され、前述のカテゴリを表します。関連するシェルスクリプトファイルについては後で説明します。現在の設定は、コマンド`locale`を使用して表示できます。

`RC_LC_ALL`

この変数は、すでに参照された変数の値を上書きします。

`RC_LANG`

前述の変数がまったく設定されていない場合、これがフォールバックとなります。デフォルトでは、`RC_LANG`だけが設定されます。これにより、ユーザが独自の変数を入力しやすくなります。

ROOT_USES_LANG

yesまたはno変数。noに設定すると、rootが常にPOSIX環境で動作します。

変数は、YaSTのsysconfigエディタで設定できます(20.3.1項「YaSTのsysconfigエディターを使ってシステム設定を変更する」(442ページ)を参照してください)。このような変数の値には、言語コード、国コード、エンコーディング、および修飾子が入っています。個々のコンポーネントは特殊文字で接続されます。

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

22.4.1 例

言語コードと国コードは必ず一緒に設定する必要があります。言語の設定は、<http://www.evertype.com/standards/iso639/iso639-en.html>および<http://www.loc.gov/standards/iso639-2/>で入手できる、ISO 639規格に従います。国コードは、http://www.din.de/gremien/nas/nabd/iso3166ma/codlstpl/en_listpl.htmlで入手できる、ISO 3166にリストされています。

使用可能な説明ファイルが/usr/lib/localeに存在する場合のみ、値を設定する意味があります。追加の記述ファイルは、/usr/share/i18nのファイルを使用し、コマンドlocaledefを実行して作成できます。記述ファイルは、glibc-i18ndataパッケージに含まれています。en_US.UTF-8の説明ファイル(英語および米国)は以下のように作成します。

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

```
LANG=en_US.UTF-8
```

インストール時にAmerican Englishを選択すると、これがデフォルトの設定になります。他の言語を選択した場合、その言語が有効になりますが、文字コードはUTF-8が使用されます。

```
LANG=en_US.ISO-8859-1
```

これにより、言語が英語、国が米国、文字セットがISO-8859-1に設定されます。この文字セットは、ユーロ記号をサポートしませんが、UTF-8がサポートされていない、更新前のプログラムを使用する方が便利なことも

あります。文字セット(この状況ではISO-8859-1)を定義する文字列は、Emacsのようなプログラムによって評価されます。

```
LANG=en_IE@euro
```

上記の例では、ユーロ記号が言語設定に明示的に組み込まれています。厳密に言うと、この設定は今では古くなっています。UTF-8もユーロ記号を扱うからです。この設定が役立つのは、アプリケーションがUTF-8ではなく、ISO-8859-15しかサポートしない場合だけです。

SuSEconfigは、/etc/sysconfig/languageにある変数を読み込み、必要な変更を/etc/SuSEconfig/profileと/etc/SuSEconfig/csh.cshrcに書き込みます。/etc/SuSEconfig/profileは/etc/profileによって読み込まれます。つまり、ソースとして使用されます。/etc/SuSEconfig/csh.cshrcは/etc/csh.cshrcのソースとして使用されます。これにより、設定はシステム全体に渡って使用できるようになります。

ユーザは、同様に~/.bashrcファイルを編集して、システムのデフォルトを上書きすることができます。たとえば、システム設定のen_USをプログラムメッセージに使用しない場合は、LC_MESSAGES=es_ESを指定してメッセージが英語の代わりにスペイン語で表示されるようにします。

22.4.2 ~/.i18nでのロケール設定

ロケールシステムのデフォルトが不十分な場合、Bashスクリプトの構文に従って~/.i18nの設定を変更してください。~/.i18n内のエントリは、/etc/sysconfig/languageのシステムデフォルトを上書きします。同じ変数名をRC_ネームスペースプレフィクスなしで使用します。たとえば、RC_LANGではなく、LANGを使用します。

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

22.4.3 言語サポートの設定

カテゴリMessagesのファイルは、フォールバックを確保するため、対応する言語ディレクトリ(たとえば、en)にのみ格納されることになっています。たとえばLANGをen_USに設定したが、messageファイルが/usr/share/locale/

en_US/LC_MESSAGESに存在しない場合は、/usr/share/locale/en/LC_MESSAGESにフォールバックされます。

フォールバックチェーンも定義できます。たとえば、ブルターニュ語、次いでフランス語、またはガリシア語、次いでスペイン語、次いでポルトガル語の順にフォールバックするには、次のように設定します。

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

必要に応じて、次のようにノルウェー語の方言であるニーノシクやブークモールをノルウェー語の代わりに使用できます(noへのフォールバックを追加します)。

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

または

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

ノルウェー語では、LC_TIMEの扱いも違うので注意してください。

生じる可能性のある1つの問題は、数字の桁を区切るための文字が正しく認識されないことです。このことは、LANGがdeのような2文字の言語コードにのみ設定されているのに、glibcが使用している定義ファイル/usr/share/lib/de_DE/LC_NUMERICに存在している場合に生じます。それで、区切り文字の定義がシステムに認識されるようにするには、LC_NUMERICをde_DEに設定する必要があります。

22.4.4 詳細情報

- 『*The GNU C Library Reference Manual*』の「Locales and Internationalization」の章。glibc-infoパッケージに格納されています。

- 『UTF-8 and Unicode FAQ for Unix/Linux』、*Markus Kuhn* 著。Web ページ <http://www.cl.cam.ac.uk/~mgk25/unicode.html> (現在のアドレス)を参照してください。
- *Unicode-Howto*(Bruno Haible著):/usr/share/doc/howto/en/html/Unicode-HOWTO.html。

プリンタの運用

SUSE Linux Enterprise®は、リモートネットワークプリンタも含め、さまざまな種類のプリンタを使った印刷をサポートしています。プリンタはYaSTを使って、または手動で設定することができます。プリントジョブの開始、管理には、グラフィカルインタフェースまたはコマンドラインユーティリティの両方を利用できます。プリンタが正常に動作しない場合は、[23.9項「トラブルシューティング」](#) (499 ページ)を参照してください。

CUPSは、SUSE Linux Enterpriseでの標準的な印刷システムです。CUPSは、特にユーザ中心の構造(ユーザ志向の設計)です。多くの状況ではLPRngとの互換性があるか、比較的少ない作業で適応させることができます。LPRngは、互換性を維持する理由でのみ、SUSE Linux Enterpriseに付属しています。

プリンタは、インタフェース(USB、ネットワークなど)と、プリンタ言語によって区別できます。プリンタの購入時には、プリンタにご利用のハードウェアで利用できるインタフェース(USBやパラレルポートなど)が搭載されていること、およびプリンタの対応言語が正しいことをご確認ください。プリンタは、次の3つのプリンタ言語クラスに基づいて分類できます。

PostScriptプリンタ

PostScriptは、LinuxとUnix環境のほとんどの印刷ジョブを生成する際に使用されるプリンタ言語であり、内部の印刷システムもこの言語を使用して処理を行います。この言語はかなり古いのですが、かなり効率的です。使用中のプリンタがPostScriptドキュメントを直接処理でき、印刷システム側で追加のステージを使用して変換を行う必要がない場合、潜在的なエラーの原因の数が減少します。PostScriptプリンタは多額のライセンスコストの対象になるので、通常、これらのプリンタは、PostScriptインタプリタを内蔵しないプリンタよりコストが高くなります。

標準的なプリンタ(PCLおよびESC/Pなどの言語)

これらのプリンタ言語はかなり古いのですが、プリンタで新機能を実現するために、引き続き拡張が行われています。既知のプリンタ言語の場合、印刷システムはGhostscriptの支援により、PostScriptのジョブを該当のプリンタ言語へ変換できます。この処理ステージを「解釈」(interpreting)と呼びます。非常によく知られている言語は、ほとんどのHPのプリンタおよび互換モデルが採用しているPCLと、Epsonのプリンタが採用しているESC/Pです。これらのプリンタ言語は、通常はLinuxによってサポートされていて、まずまずの印刷結果をもたらします。最新のプリンタや特殊なプリンタの機能は、Linuxがサポートしていないことがあります。オープンソースの開発者は、それらの機能に関してまだ作業をしている可能性もあります。HPが開発したhpijsドライバを除き、現時点では、Linuxドライバを開発してオープンソース条項に基づきそれらをLinuxのディストリビュータに提供しているプリンタメーカーは存在しません。これらのプリンタのほとんどは、中間の価格帯にあります。

独自規格のプリンタ(GDIプリンタ)

これらのプリンタは、共通のプリンタ言語をサポートしていません。これらのプリンタは独自のプリンタ言語を使用しており、新しいエディション/モデルがリリースされると、プリンタ言語も変更される可能性があります。一般的にこのようなプリンタでは、Windowsドライバしか利用できません。詳細については、[23.9.1項「標準的なプリンタ言語をサポートしないプリンタ」](#) (499 ページ)を参照してください。

新しいプリンタを購入する前に、次の各ソース(情報源)を参照し、購入を予定しているプリンタがどの程度までサポートされているかを確認してください。

<http://www.linuxprinting.org/>

LinuxPrinting.orgのプリンタデータベース。

<http://www.cs.wisc.edu/~ghost/>

GhostscriptのWebページ。

`/usr/share/doc/packages/ghostscript/catalog.devices`

付属するドライバのリスト。

オンラインデータベースはいつでも、Linuxによるサポートの最新のステータスを示しています。しかし、Linuxのディストリビューションが統合できるのは、製造の時点で使用可能だったドライバだけです。したがって、現時点で「perfectly supported」(完全にサポート済み)と評価されているプリンタであっ

ても、最新バージョンのSUSE Linux Enterpriseがリリースされた時点では、そのステータスに達していなかった可能性があります。そのため、これらのデータベースは必ずしも正しいステータスを表しているとは限らず、おおよその状況を提示するだけにとどまっています。

23.1 印刷システムのワークフロー

ユーザが印刷ジョブを作成します。印刷ジョブは、印刷するデータとスプーラに対する情報から構成されますが、その情報には、プリンタの名前またはプリンタキューの名前だけでなく、必要に応じて、プリンタ固有のオプションなど、フィルタに関する情報も含まれます。

各プリンタには、1つ以上の専用プリンタキューが存在しています。指定のプリンタがデータを受け取れるようになるまで、スプーラは印刷ジョブをキュー内に留めています。プリンタの準備が整うと、スプーラはフィルタおよびバックエンドを経由して、プリンタにデータを送信します。

このフィルタは、印刷中のアプリケーションが生成したデータ(通常的是PostScriptやPDFですが、ASCII、JPEGなどの場合もあります)を、プリンタ固有のデータ(PostScript、PCL、ESC/Pなど)に変換します。プリンタの機能については、PPDファイルに記述されています。PPDファイルには、プリンタ固有のオプションが記述されています。各オプションに対しては、プリンタでそのオプションを有効にするために必要なパラメータが指定されています。フィルタシステムは、ユーザが有効として選択したオプションを確認します。

PostScriptプリンタを選択すると、フィルタシステムがデータをプリンタ固有のPostScriptに変換します。この変換にプリンタドライバは必要ありません。PostScript非対応プリンタを使用すると、フィルタシステムがGhostscriptを使用して、データをプリンタ固有データに変換します。この変換には、使用しているプリンタに適応したGhostscriptプリンタドライバが必要です。バックエンドは、プリンタ固有データをフィルタから受信し、そのデータをプリンタに送信します。

23.2 プリンタに接続するための方法とプロトコル

プリンタをシステムに接続するには、さまざまな方法があります。CUPS印刷システムの設定は、ローカルプリンタと、ネットワーク経由でシステムに接続されているプリンタを区別しません。Linux環境では、ローカルプリンタは、プリンタメーカーのマニュアルに記載されているとおりに接続する必要があります。CUPSは、シリアル、USB、パラレル、およびSCSI接続をサポートしています。プリンタ接続の詳細については、http://en.opensuse.org/SDB:CUPS_in_a_NutshellにアクセスしてSupport Database (サポートデータベース)で「*CUPS in a Nutshell*」という記事を参照してください。

► **zseries:** IBM System zの各メインフレームにローカル接続できる、z/VMによって提供されているプリンタおよびその類似デバイスは、CUPSまたはLPRngのどちらにおいてもサポートされていません。これらのプラットフォーム上では、ネットワーク経由の印刷だけを利用できます。ネットワークプリンタのケーブリング(ケーブル接続)は、プリンタメーカーの指示にしたがって設置する必要があります。 ◀

警告: 稼働中システムのケーブル接続の変更

プリンタをコンピュータに接続する場合、コンピュータの動作中に接続と取り外しを行って良いのはUSBデバイスだけであることに注意してください。システムやプリンタの損傷を回避するために、USB以外の接続を変更する場合は、あらかじめシステムをシャットダウンしてください。

23.3 ソフトウェアのインストール

PPD (PostScript printer description、PostScriptプリンタ記述)は、PostScriptプリンタの特性(解像度など)やオプション(両面印刷ユニットなど)を記述するコンピュータ言語です。これらの記述は、CUPS側でさまざまなプリンタオプションを使用するために必須です。PPDファイルがない場合、印刷データは「raw」(ロー、未加工)状態でプリンタへ送信されますが、そのことは通常は望ましくありません。SUSE Linux Enterpriseのインストール時には、PostScriptサポート機能のないプリンタでも使用できるように、多数のPPDファイルが事前インストールされます。

PostScriptプリンタを設定する場合、最善のアプローチは、適切なPPDファイルを手に入れることです。この種の多数のPPDファイルは、標準インストールの範囲内で自動的にインストールされるパッケージmanufacturer-PPDsに用意されています。および、**23.9.2項「特定のPostScriptプリンタに適したPPDファイルが入手できない」** (500 ページ)。を参照してください。**23.8.3項「各種パッケージ内のPPDファイル」** (496 ページ)

新しいPPDファイルは、`/usr/share/cups/model/`ディレクトリ内に保存するか、YaSTで印刷システムに追加できます(**YaSTを使ったPPDファイルの追加項**(489 ページ)を参照)。その結果、インストールの際にPPDファイルを選択できるようになります。

ユーザが設定ファイルを変更するのみでなくソフトウェアパッケージ全体をインストールすることを、プリンタメーカーが望んでいるかどうかに注意してください。第一に、このようなタイプのインストールを行うと、SUSE Linux Enterpriseによって提供されているサポートが失われる結果になります。第二に、印刷コマンドが異なる方法で機能する可能性があり、システムは他のメーカーのデバイスに対応できなくなる可能性もあります。この理由で、メーカーのソフトウェアをインストールすることをお勧めしません。

23.4 プリンタの設定

YaSTを使って、コンピュータに直接接続されているプリンタ(通常はUSBやパラレルポート)を設定したり、ネットワーク経由の印刷を設定することができます。また、プリンタにPPDファイル(PostScript Printer Description)を追加することもできます。

23.4.1 ローカルプリンタの設定

未設定のローカルプリンタが検出された場合、それを設定するためにYaSTが自動的に開始されます。パラレルまたはUSBポートを自動的に設定し、接続されたプリンタを検出できる場合、YaSTはプリンタを自動的に設定できます。このプリンタモデルは、ハードウェアの自動検出時に使用されるデータベースにも登録する必要があります。

プリンタモデルがわからない場合、または自動検出できない場合は、手動設定を行ってください。プリンタが自動検出されない原因としては、次の2種類の理由が考えられます。

- プリンタが自己を正しく識別していない。これは、非常に古いデバイスなどにみられます。**手動による設定項 (486 ページ)**の説明に従って、プリンタを設定してください。
- 手動設定でも正常に動作しない場合は、プリンタとコンピュータ間の通信ができない可能性があります。ケーブルやプラグをチェックして、プリンタが正しく接続されていることを確認してください。この場合は、問題はプリンタ関連ではなく、USBポートやパラレルポート関連の問題である可能性が高いです。

手動による設定

プリンタを手動設定するには、YaSTコントロールセンタで **[ハードウェア]** > **[プリンタ]** の順に選択します。これでプリンタ設定のメインウィンドウが開きます。このウィンドウでは、検出されたデバイスのリストが上部に表示されます。下部には、現在までに設定されているキューが表示されます(プリントキューの詳細は、**23.1項「印刷システムのワークフロー」 (483 ページ)**を参照してください)。プリンタが検出されなかった場合は、どちらの部分も空になります。表示されているプリンタの設定を変更するには **[編集]** を、自動検出されなかったプリンタを設定する場合は **[追加]** を使用します。既存の設定を編集する場合は、**ローカルプリンタの手作業による追加 (487 ページ)**と同じダイアログを使用します。

[プリンタ設定] では、既存の項目を **[削除]** することもできます。**[その他]** をクリックすると、詳細設定オプションが表示されます。**[検出の再開]** を選択して、プリンタの自動検出を手動で開始します。コンピュータに複数のプリンタが接続されている場合、またはプリンタに複数のキューが設定されている場合は、アクティブな項目をデフォルトとして設定することができます。**[CUPSエキスパート設定]** と **[IPPリッスンの変更]** は詳細設定オプションです。詳細は、**第23章 プリンタの運用 (481 ページ)**を参照してください。

ティップ: YaST印刷テスト

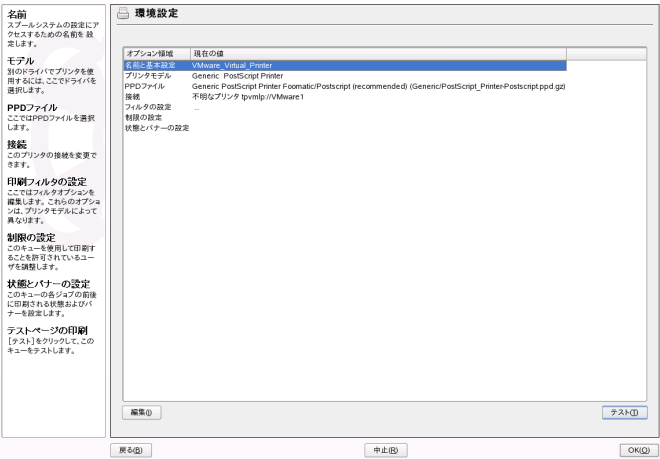
すべてが正しく機能していることを確認するために、各設定をYaSTの印刷テスト機能で確認してください。テストページには、テストする設定についての重要な情報もあります。たとえば、数ページがほとんど何も印刷されない状態になるなど、出力が文字化けした場合は、最初にすべての用紙を取り出し、YaSTがテストを実行できないようにすると、プリンタを停止できます。

- 1 YaSTを起動して、[ハードウェア] > [プリンタ] の順にクリックして、[プリンタ環境設定] ダイアログを表示します。
- 2 [プリンタ] をクリックして、[プリンタタイプ] ウィンドウを表示します。
- 3 [直接接続されているプリンタ] を選択します。
- 4 プリンタが接続されているポートを選択し(通常はUSBかパラレル)、次の設定画面でデバイスを選択します。この時点で[プリンタ接続のテスト]を実施することをお勧めします。問題が発生する場合は、正しいデバイスを選択するか、または[戻る]を選択して前のダイアログに戻ります。
- 5 [キュー名] で、プリントキューを設定します。[印刷用の名前] は必須項目です。わかりやすい名前を指定することをお勧めします。アプリケーションの印刷ダイアログでは、この名前を使ってプリンタを指定します。[プリンタの説明] と [プリンタの場所] に、プリンタの詳細を指定します。この項目の指定は省略できますが、コンピュータに複数のプリンタを接続している場合や、プリントサーバを設定する場合に役立ちます。[ローカルフィルタリングを行う] は選択する必要があります。ローカルプリンタの場合は必須です。
- 6 [プリンタモデル] で、プリンタの[製造元] と [モデル] を指定します。ご利用のプリンタが表示されない場合は、製造元のリストから[不明なメーカー] を選択し、モデルリストから適切な標準言語(プリンタの制御言語)を選択してみてください(ご利用のプリンタで使われている言語については、プリンタのマニュアルを参照してください)。これで

うまくいかない場合は、**YaSTを使ったPPDファイルの追加項** (489 ページ)を参照して他の解決方法を試してください。

7 [設定] 画面に、プリンタ設定の概要が表示されます。このYaSTモジュールの開始画面から、既存のプリンタ設定を変更する場合も、このダイアログが表示されます。

図 23.1 プリンタ設定の概要



この概要には、次の項目が表示されます。項目は、[編集] で編集することができます。

- [Name and basic settings] (名前と基本設定)、[プリンタモデル]、[接続] を使って、この手順中に作成された項目を変更することができます。
- [PPDファイル] の詳細は、**YaSTを使った代替PPDファイルの選択項** (489 ページ)を参照してください。
- [フィルタ設定] を使って、プリンタ設定をきめ細かく調整することができます。ここでは、[ページサイズ]、[カラーモード]、[解像度] などのオプションを設定します。
- デフォルトでは、すべてのユーザがこのプリンタを使用できます。
[制限の設定] では、プリンタの使用を禁止するユーザや、使用を許可するユーザを表示できます。

- ・ [状態とバナーの設定] では、状態を変更してプリンタを無効にしたり、各ジョブの前後に [開始バナー] や [終了バナー] を印刷するかどうかを指定できます(デフォルトでは印刷しない)。

YaSTを使ったPPDファイルの追加

プリンタの [プリンタモデル] ダイアログが表示されない場合、そのモデルのPPD (PostScript Printer Description) ファイルがありません(PPDファイルの詳細は23.3頁「ソフトウェアのインストール」(484 ページ)を参照)。*[Add PPD File to Database]* (PPDファイルのデータベースへの追加)では、ローカルファイルシステム、またはFTP/HTTPサーバから、PPDファイルを追加することができます。

プリンタメーカーまたはプリンタのドライバCDからPPDファイル入手してください(詳細は23.9.2頁「特定のPostScriptプリンタに適したPPDファイルが入手できない」(500 ページ)を参照)。PPDファイルの代替ソースとして「Linux Printing Database(Linux印刷データベース)」の<http://www.linuxprinting.org/>があります。linuxprinting.orgからPPDファイルをダウンロードする場合、ここには最新のLinuxサポートステータスが記載されていることに注意してください。この情報が、SUSE Linux Enterpriseと一致していなくても構いません。

YaSTを使った代替PPDファイルの選択

多くのプリンタモデルでは、さまざまなPPDファイルを利用できます。プリンタを設定する場合、YaSTでは一般的な規則として1つにrecommendedのマークを付けます。プリンタで利用できるPPDファイルのリストを入手するには、[環境設定] の [PPDファイル] を選択して、[編集] をクリックします。詳細については、図 23.1. 「プリンタ設定の概要」(488 ページ)を参照してください。

通常は、PPDファイルを変更する必要はありません。YaSTが選択したPPDファイルで、最良の結果が得られます。ただし、たとえばカラープリンタで白黒印刷だけを行いたいような場合は、カラー印刷をサポートしないPPDファイルを利用するのが便利で簡単です。画像印刷時にPostScriptプリンタのパフォーマンスに関する問題が発生する場合、PostScript PPDファイルからPCL PPDファイルに変更すると問題が改善されることがあります(ご利用のプリンタがPCL言語を理解できる場合)。

23.4.2 YaSTを使ったネットワークプリンタの設定

ネットワークプリンタは、自動的に検出されません。ネットワークプリンタは、YaSTプリンタモジュールを使って手動設定する必要があります。ネットワークの設定内容に応じて、プリントサーバ(CUPS、LPD、SMB、またはIPX)に印刷したり、ネットワークプリンタに直接印刷(TCP経由を推奨)することができます。ご利用の環境でのネットワークプリンタの設定については、ネットワーク管理者にお問い合わせください。

手順 23.2 YaSTを使ったネットワークプリンタの設定

- 1 YaSTを起動して、[ハードウェア] > [プリンタ] の順にクリックして、[プリンタ環境設定] ダイアログを表示します。
- 2 [プリンタ] をクリックして、[プリンタタイプ] ウィンドウを表示します。
- 3 [ネットワークプリンタ] を選択して、表示されたダイアログにネットワーク管理者から指示された詳細情報を設定します。

23.5 ネットワークプリンタ

ネットワークプリンタは、さまざまなプロトコルをサポートできますし、その複数を同時にサポートすることも可能です。サポートされているプロトコルのほとんどは標準化されたものですが、いくつかのメーカーはその標準に拡張(変更)を加えました。それらのメーカーは標準を正しく実装していないシステムのテストや、標準では使用できない特定の機能を提供することを望んでいます。そのような場合、メーカーは少数のオペレーティングシステム用ののみドライバを提供し、自社のシステムにつきまとう課題を排除します。残念なことに、Linuxドライバはめったに提供されません。現在の状況では、あらゆるプロトコルがLinux環境で円滑に動作するという仮定に基づいて行動することはできません。したがって、機能する設定を実現するために、さまざまなオプションを実験する必要があります。

重要項目: リモートアクセス設定

デフォルトで、**cupsd**は内部ネットワークインタフェース(**localhost**)のみで待機します。**CUPS**ネットワークサーバを設定する際、**/etc/cups/cupsd.conf**の**Listen**ディレクティブを調整して外部ネットワークを待機する必要があります。

CUPSは**socket**、**LPD**、**IPP**、および**smb**の各プロトコルをサポートしています。

socket

socketは、データのハンドシェイクを最初に行うことなく、データをインターネットソケットへ送信する接続を意味します。一般的に使用される**socket**のポート番号のいくつかは、9100または35です。デバイスURI (**uniform resource identifier**)の構文は、**socket://プリンタのIP:ポート**です。たとえば、**socket://192.168.2.202:9100/**のようになります。

LPD (line printer daemon、ラインプリンタデーモン)

実証されてきた**LPD**プロトコルは、**RFC1179**で説明されています。このプロトコルを使用する場合、プリンタキューのIDのようなジョブ関連データの一部は、実際の印刷データより先に送信されます。したがって、データを送信するために、**LPD**プロトコルを設定する際にプリンタキューを指定する必要があります。さまざまなプリンタメーカーによる実装は、プリンタキューとして任意の名前を受け入れる柔軟性を備えています。必要に応じて、使用可能な名前がプリンタのマニュアルに提示されています。多くの場合、**LPT**、**LPT1**、**LP1**、または他の類似した名前が使用されています。**CUPS**システムを採用している他の**Linux**ホストまたは**Unix**ホスト上で、**LPD**キューを設定することもできます。**LPD**サービスが使用するポート番号は515です。デバイスURIの例は、**lpd://192.168.2.202/LPT1**です。

IPP (Internet Printing Protocol、インターネット印刷プロトコル)

IPPは比較的新しい(1999年)プロトコルであり、**HTTP**プロトコルに基づいています。**IPP**を使用する場合、他のプロトコルより、ジョブとの関連性が高いデータが送信されます。**CUPS**は、**IPP**を使用して内部のデータ送信を行います。これは、2台の**CUPS**サーバ間でキューを転送する上で優先されるプロトコルです。**IPP**を正しく設定するには、印刷キューの名前は必須です。**IPP**のポート番号は631です。デバイスURIの例は、

ipp://192.168.2.202/psおよび
ipp://192.168.2.202/printers/psです。

SMB (Windows共有)

CUPSは、Windows共有に接続されたプリンタへの印刷もサポートしています。この目的で使用されるプロトコルは、SMBです。SMBは、ポート番号137、138、および139を使用します。デバイスURIの例は、

smb://user:password@workgroup/smb.example.com/printer、
smb://user:password@smb.example.com/printer、および
smb://smb.example.com/printerです。

設定を行う前に、プリンタがサポートしているプロトコルを決定する必要があります。必要な情報をメーカーが提供していない場合、nmapコマンド(nmapパッケージ)を使用して、プロトコルを推定します。nmapは、ホストでオープンしているポートを確認します。たとえば、次のようにします。

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

23.5.1 コマンドラインツールによるCUPS設定

YaSTでのCUPSオプションとは別に、ネットワークプリンタの設定時にlpadminやlpoptionsなどのコマンドラインツールを使ってCUPSを設定することができます。バックエンド(USBなど)とパラメータ(/dev/usb/lpなど)で構成されるデバイスURIが必要です。たとえば、完全URIはparallel:/dev/lp0 (パラレルポート1に接続されているプリンタ)またはusb:/dev/usb/lp0 (USBポートに接続されている最初に検出されたプリンタ)などとなります。

lpadminで、CUPSサーバ管理者の追加、削除、またはクラスおよび印刷キューの管理ができます。プリントキューを追加するには、次の構文を使用します。

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

このデバイス(-v)は、指定したPPDファイル(-P)を使用して、queue(-p)として使用できます。プリンタを手動で設定する場合は、このPPDファイルとデバイスの名前を把握しておく必要があります。

-Eは、最初のオプションとして使用しないでください。どのCUPSコマンドでも、-Eを最初の引数として使用した場合、暗号化接続を使用することを暗示的に意味します。プリンタを使用可能にするには、次の例に示す方法で-Eを使用する必要があります。

```
lpadmin -p ps -v parallel:/dev/lp0 -P \  
/usr/share/cups/model/Postscript.ppd.gz -E
```

ネットワークプリンタの設定例:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \  
/usr/share/cups/model/Postscript-levell.ppd.gz -E
```

lpadminのオプションの詳細は、lpadmin(1)のマニュアルページを参照してください。

プリンタのセットアップ時には、一部のオプションがデフォルトとして設定されています。これらのオプションは、各印刷ジョブ用に変更できます(使用される印刷ツールに依存)。YaSTを使用して、これらのデフォルトオプションを変更することもできます。コマンドラインツールを使用して、デフォルトオプションを次のように設定します。

1 最初に、すべてのオプションを列挙します。

```
lpoptions -p queue -l
```

例:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

アクティブになったデフォルトオプションは、先頭にアスタリスク(*)が付いています。

2 次のようにlpadminを使用してオプションを変更します。

```
lpadmin -p queue -o Resolution=600dpi
```

3 新しい設定値の確認:

```
lpoptions -p queue -l
```

```
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

標準ユーザがlpoptionsを実行すると、設定が~/.lpoptionsに書き込まれます。ただし、root設定は/etc/cups/lpoptionsに書き込まれます。

23.6 グラフィカルな印刷インタフェース

xppやKDEプログラムKprinterなどのツールは、キューを選択したり、CUPS標準オプションとPPDファイルを介して使用可能になるプリンタ固有オプションの両方を設定するための、グラフィカルなインタフェースを提供します。Kprinterを、KDE以外のアプリケーションの標準印刷インタフェースとして使用することもできます。これらのアプリケーションの印刷ダイアログで、プリンタコマンドとしてkprinterまたはkprinter --stdinを指定してください。使用するコマンドは、アプリケーションのデータ転送方法によって異なります。両方のコマンドを試して、KPrinterが開始された方を使用してください。設定が適切であれば、アプリケーションから印刷ジョブが発行されると、アプリケーションはKprinterのダイアログを表示します。このダイアログを使用してキューを選択し、他の印刷オプションを設定できます。この場合、アプリケーション自身の印刷設定がkprinterの印刷設定と競合が発生せず、Kprinterが使用可能になった後で、印刷オプションの変更がKprinterによってのみ行われる必要があります。

23.7 コマンドラインからの印刷

コマンドラインから印刷するには、コマンド `lp -d queuefilename filename` を入力し、*queuefilename* および *filename* を対応する名前で置き換えます。

一部のアプリケーションでは、印刷処理をlpコマンドに依存しています。この場合、アプリケーションの印刷ダイアログで正しいコマンドを入力します。ただし、通常は*filename*を指定しません。たとえば、`lp -d queuefilename` と入力します。

23.8 SUSE Linux Enterpriseの特殊機能

CUPSの多くの機能は、SUSE Linux Enterpriseでできるように調整されています。ここでは、最も重要な変更点について説明します。

23.8.1 CUPSとファイアウォール

デフォルトのSUSE Linux Enterpriseインストールを実行した後、SuSEfirewall2はアクティブになり、外部ネットワークデバイスは着信トラフィックをブロックする外部ゾーンに設定されます。これらのデフォルト設定は、CUPSを使用するときに調整します。SUSEfirewall2設定の詳細については、[43.4項「SuSEfirewall2」](#) (899 ページ)を参照してください。

CUPSクライアント

通常、CUPSクライアントはファイアウォール内部のネットワーク上の通常のワークステーションで実行されます。この場合、外部ネットワークデバイスを内部ゾーンに設定し、ワークステーションにネットワーク内部から到達できるようにすることを推奨します。

CUPSサーバ

CUPSサーバがファイアウォールで保護されたネットワークの一部の場合、外部ネットワークデバイスはファイアウォールの内部ゾーンに設定します。外部ゾーンの一部になると、TCPおよびUDPポート631を開いて、CUPSサーバをネットワークで使えるようにする必要があります。

23.8.2 CUPS印刷サービスの変更点

BrowseAllowとBrowseDenyの一般化された機能

BrowseAllowとBrowseDenyに対して設定されたアクセスパーミッションは、cupsdに対して送信されたすべてのタイプのパッケージに適用されます。/etc/cups/cupsd.conf内にあるデフォルトの設定値は、次のとおりです。

```
BrowseAllow @LOCAL
BrowseDeny All
```

および

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
```

```
Allow From 127.0.0.2
Allow From @LOCAL
</Location>
```

この方法では、LOCALホストだけが、CUPSサーバ上のcupsdにアクセスできます。LOCALホストとは、PPPインタフェース以外(より正確に表現すると、IFF_POINTOPOINTフラグがセットされていないインタフェース)に所属するIPアドレスを使用し、そのIPアドレスがCUPSサーバと同じネットワークに所属しているホストのことです。他のすべてのホストから着信したパケットは、即座に拒否されます。

cupsdがデフォルトで有効化

標準的なインストールでは、cupsdは自動的に有効になり、追加で手動の操作を行うことなく、CUPSネットワークサーバのキューに対して適切にアクセスすることができます。この機能を使用するには、**BrowseAllowとBrowseDenyの一般化された機能項**(495 ページ)内の項目が必須の前提条件になります。それらが満たされていない場合、cupsdを自動的に有効にする状態で、セキュリティが不十分になります。

23.8.3 各種パッケージ内のPPDファイル

YaSTのプリンタ設定機能は、`/usr/share/cups/model/`内に記述されたPPDファイルのみを使用して、CUPS用のキューをセットアップします。プリンタモデルに適したPPDファイルを決定するために、YaSTはハードウェア検出の際に判断されたベンダおよびモデルを、システムの`/usr/share/cups/model/`内で使用可能なすべてのPPDファイル内にあるベンダおよびモデルと比較します。この目的で、YaSTのプリンタ設定機能は、PPDファイルから抽出したベンダおよびモデルの情報に基づいて、データベースを生成します。ベンダおよびモデルのリストから特定のプリンタを選択した場合、そのベンダおよびモデルに対応するPPDファイルを受け取ることになります。

PPDファイルのみを使用し、他の情報ソースを使用しない設定には、`/usr/share/cups/model/`内のPPDファイルを自由に変更できるという利点があります。YaSTのプリンタ設定機能は、変更結果を認識し、ベンダおよびモデルからなるデータベースを再生成します。たとえば、PostScriptプリンタのみを使用している場合、通常はcups-driversパッケージ内にあるFoomatic PPDファイルや、cups-drivers-stpパッケージ内にあるGimp-Print PPDファイ

ルを必要としません。代わりに、使用中のPostScriptプリンタ用のPPDファイルを/usr/share/cups/model/へ直接コピーし(それらがまだmanufacturer-PPDsパッケージ内に存在していない場合)、使用中のプリンタに合わせて最適な設定を行うこともできます。

cupsパッケージ内のCUPS PPD ファイル

cupsパッケージ内にある基本PPDファイルは、PostScript Level 1およびLevel 2プリンタに適応したFoomatic PPDファイルによって補足されます。

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

cups-driversパッケージ内のPPD ファイル

通常、Foomaticプリンタフィルタのfoomatic-ripは、PostScript非対応プリンタ用のGhostscriptと組み合わせて使用されます。適切なFoomatic PPDファイルには、`*NickName: ... Foomatic/Ghostscript driver`および`*cupsFilter: ... foomatic-rip`のエントリがあります。これらのPPDファイルは、cups-driversパッケージ内にあります。

「`*NickName: ... Foomatic ... (recommended)`」のエントリがあるFoomatic PPDファイルがプリンタモデルに一致していて、manufacturer-PPDsパッケージに、より適したPPDファイルが含まれていない場合は、Foomatic PPDファイルをYaSTに使用することをお勧めします。

cups-drivers-stpパッケージ内のGimp-Print PPD ファイル

多くのPostScript非対応プリンタでは、foomatic-ripの代わりに、Gimp-Printから取得したCUPSフィルタrastertoprinterを使用できます。このフィルタと、適切なGimp-Print PPDファイルは、cups-drivers-stpパッケージ内に用意されています。Gimp-Print PPD ファイルは/usr/share/cups/model/stp/内に配置されていて、そのファイル内にエントリ`*NickName: ...`

CUPS+Gimp-Printおよび*cupsFilter: ... rastertoprinterがあります。

manufacturer-PPDsパッケージ内にあるプリンタメーカーからのPPDファイル

manufacturer-PPDsパッケージには、十分自由なライセンスに基づいてプリンタメーカーから提供されたPPDファイルが含まれています。PostScriptプリンタは、プリンタメーカーの適切なPPDファイルを使用して設定するのが妥当です。このファイルを使用すると、そのPostScriptプリンタの機能すべてを活用できるためからです。YaSTは、次の各条件が満たされている場合、manufacturer-PPDsパッケージから得られたPPDファイルを優先します。

- ハードウェア検出の際に決定されたベンダおよびモデルが、manufacturer-PPDsパッケージから得られたPPDファイル内にあるベンダおよびモデルと一致しています。
- manufacturer-PPDsパッケージからのPPDファイルは、このプリンタモデルに対して、またはプリンタモデルに一致する*NickName: ... Foomatic/Postscript (recommended) エントリがあるFoomatic PPDファイルがある場合に適している唯一のPPDファイルになります。

したがって、YaSTは次のような状況では、manufacturer-PPDsパッケージから得られたどのPPDファイルも使用しません。

- manufacturer-PPDsパッケージから得られたPPDファイルが、プリンタのベンダおよびモデルに一致していません。これは、manufacturer-PPDsパッケージに同様のモデル用にPPDファイルが1つしかない場合、たとえば、一連のモデルの個々のモデルに別々のPPDファイルがないが、PPDファイル内にFunprinter 1000 seriesのような形式でモデル名が指定されている場合に発生します。
- Foomatic PostScript PPDファイルは、推奨されていません。プリンタモデルは、PostScriptモードでは十分効率よく動作しないことがあるからです(たとえば、メモリが少なすぎるためにこのモードではプリンタの信頼性が低い、またはプリンタ内蔵プロセッサの能力が低いために動作が遅すぎる、などです)。デフォルトでは、プリンタがPostScriptをサポートしてい

ないこともあります。たとえば、PostScriptサポートがオプションのモジュールという形でしか使用できない場合などです。

manufacturer-PPDsパッケージから得られたPPDファイルが特定のPostScriptプリンタに適しているが、上記で説明された理由によってYaSTがそのファイルを設定できない場合、YaST内で該当のプリンタモデルを手動で選択してください。

23.9 トラブルシューティング

ここでは、プリンタハードウェアおよびソフトウェアに最も一般的に発生する問題と、それを解決または回避する方法について説明します。GDIプリンタ、PPDファイル、およびポート設定などのトピックをカバーしています。一般的なネットワークプリンタに関する問題、印刷に問題がある場合、およびキュー処理についても対処しています。

23.9.1 標準的なプリンタ言語をサポートしないプリンタ

これらのプリンタは、共通のプリンタ言語をサポートしておらず、独自のコントロールシーケンスを使用しないと対処できません。そのため、これらのプリンタは、メーカーがドライバを添付した特定のバージョンのオペレーティングシステムでのみ動作します。GDIは、Microsoft*がグラフィックデバイス用に開発したプログラミングインタフェースです。通常、メーカーはWindows用のドライバだけを提供しています。また、WindowsドライバはGDIインタフェースを使用しているため、これらのプリンタは「**GDIプリンタ**」と呼ばれることもあります。実質的な問題は、このプログラミングインタフェースではなく、これらのプリンタを制御できるのは、各プリンタモデルが採用している独自のプリンタ言語のみという事実にあります。

いくつかのGDIプリンタは、GDIモードと標準的なプリンタ言語のいずれかの間で切り替えることができます。マニュアルがある場合は、プリンタのマニュアルを参照してください。モデルによっては、切り替えを行うために特別なWindowsソフトウェアが必要なこともあります(Windowsから印刷する場合、Windowsプリンタドライバは常にプリンタをGDIモードに切り替える場合があることに注意してください)。他のGDIプリンタでは、標準のプリンタ言語を利用するための拡張モジュールが用意されています。

一部のメーカーは、プリンタに独自規格のドライバを提供しています。独自規格のプリンタドライバの欠点は、インストール済みの印刷システムとそのドライバを組み合わせたときに動作するという保証も、さまざまなハードウェアプラットフォームに適しているという保証もないことです。一方、標準的なプリンタ言語をサポートするプリンタは、特殊なバージョンの印刷システムや特殊なハードウェアプラットフォームに依存しません。

独自規格に対応するLinuxドライバを正常に機能させるために時間を費やすより、サポートされているプリンタを購入する方がコスト効率が良いこともあります。この方法により、ドライバの問題を一度だけで、そしてあらゆる状況で解決できます。特殊なドライバソフトウェアのインストールと設定を行う必要はなく、新しい印刷システムの開発に伴ってドライバのアップデートを入手する必要もありません。

23.9.2 特定のPostScriptプリンタに適したPPDファイルが入手できない

manufacturer-PPDsパッケージの中に、特定のPostScriptプリンタに適したPPDファイルが含まれていない場合、プリンタメーカー製のドライバCDに収録されているPPDファイルを使用すること、またはプリンタメーカーのWebページから適切なPPDファイルをダウンロードすることができるはずです。

PPDファイルがzipアーカイブ(.zip)または自己展開zipアーカイブ(.exe)の形で提供されている場合、unzipを使用してそのファイルを展開します。最初に、PPDファイルのライセンス(許諾契約)条項を読みます。次にcupstestppdユーティリティを使って、PPDファイルが「Adobe PostScript Printer Description File Format Specification, version 4.3」に準拠しているかどうかを確認します。

「FAIL」ユーティリティから失敗が返された場合は、PPDファイル中のエラーは深刻なもので、問題を引き起こす可能性があります。cupstestppdによって報告された問題点は、取り除く必要があります。必要に応じて、適切なPPDファイルが入手できるかどうかをプリンタメーカーに問い合わせることも考えられます。

23.9.3 パラレルポート

最も安全なアプローチは、プリンタを最初のパラレルポートに直接接続し、BIOS内で次のパラレルポート設定値を選択することです。

- I/Oアドレス:378 (16進)
- 割り込み:無関係
- モード:Normal (通常)、SPP、またはOutput Only (出力専用)
- DMA:無効

これらの設定値を使用した場合でも、パラレルポートに接続したプリンタを使用できない場合、BIOS内での設定値に合わせて、I/Oアドレスを0x378という形で/etc/modprobe.conf内に明示的に入力します。2つのパラレルポートが存在し、それぞれのI/Oアドレスが378と278 (16進)に設定されている場合、それらを0x378, 0x278という形で入力します。

割り込み(IRQ) 7が空いている場合、例 23.1. 「/etc/modprobe.conf:最初のパラレルポートの割り込みモード」 (501 ページ)に示すエントリを使用して、その割り込みを有効にすることもできます。割り込みモードを有効にする前に、/proc/interruptsファイルを参照して、すでに使用中の割り込みを調べます。現時点で使用中の割り込みだけが表示されます。どのハードウェアコンポーネントがアクティブになっているかに応じて、この表示は変化することがあります。パラレルポート用の割り込みは、他のどのデバイスも使用してはなりません。自信がない場合、irq=noneを指定してポーリングモードを使用します。

例 23.1 /etc/modprobe.conf:最初のパラレルポートの割り込みモード

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

23.9.4 ネットワークプリンタ接続

ネットワークの問題の識別

プリンタをコンピュータに直接接続します。テストの目的で、そのプリンタをローカルプリンタとして設定します。この方法で動作する場合、問題はネットワークに関連しています。

TCP/IPネットワークの確認

TCP/IPネットワークと名前解決が正しく機能していることが必要です。

リモートアクセスの確認

デフォルトで、**cupsd**は内部ネットワークインタフェース(**localhost**)のみで待機します。**/etc/cups/cupsd.conf**の**Listen**ディレクティブで外部ネットワークからのアクセスが許可されていることを確認してください。

```
Listen 192.168.2,*:631
```

ファイアウォール設定の確認

CUPSサーバは、内部ファイアウォールゾーン内に存在するか、または外部ゾーンの場合は**UDP**および**TCP**ポート**631**のデータを送受信できる必要があります。

リモートlpdの確認

次のコマンドを使用して、*host*上の**lpd**(ポート**515**)に対する**TCP**接続を確立できるかどうかをテストします。

```
netcat -z host 515 && echo ok || echo failed
```

lpdへの接続を確立できない場合、**lpd**がアクティブになっていないか、ネットワークの基本的な問題があります。

rootユーザで次のコマンドを使用し、リモート*host*上の**queue**に関するステータスレポート(おそらく、非常に長い)を照会することもできます。これは、該当の**lpd**がアクティブで、そのホストが照会を受け付けることを前提にしています。

```
echo -e "\004queue" \  
| netcat -w 2 -p 722 host 515
```

lpdが応答しない場合、それがアクティブになっていないか、ネットワークの基本的な問題が発生している可能性があります。**lpd**が応答する場合、その応答は、*host*上にある**queue**を介して印刷ができない理由を示すはずです。例23.2.「**lpdからのエラーメッセージ**」(502ページ)でこうした応答を受け取った場合、問題はリモートの**lpd**にあります。

例 23.2 lpdからのエラーメッセージ

```
lpd: your host does not have line printer access  
lpd: queue does not exist  
printer: spooling disabled  
printer: printing disabled
```

リモート cupsd の確認

デフォルトでは、CUPS ネットワークサーバはUDPポート631を使用して、自らのキューを30秒ごとにブロードキャストします。したがって、次のコマンドを使用して、ネットワーク内にCUPS ネットワークサーバが存在しているかどうかをテストすることができます。

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

ブロードキャストを行っているCUPS ネットワークサーバが存在している場合、出力は例23.3、「CUPS ネットワークサーバからのブロードキャスト」(503 ページ)に示すようになります。

例 23.3 CUPS ネットワークサーバからのブロードキャスト

```
ipp://192.168.2.202:631/printers/queue
```

► **zseries:** IBM System z のイーサネットデバイスが、デフォルトではブロードキャストを受信しないことを考慮してください。◀

次のコマンドを使用して、host 上の cupsd (ポート631) に対するTCP接続を確立できるかどうかをテストすることができます。

```
netcat -z host 631 && echo ok || echo failed
```

cupsd への接続を確立できない場合は、cupsd が有効になっていないか、基本的なネットワークの問題が発生している可能性があります。lpstat -h host -l -t は、host 上のすべてのキューに関するステータスレポート(非常に長い場合がある)を返しますが、それぞれの cupsd が有効になっていて、ホストがクエリを受け入れることが前提になります。

次のコマンドを使用して、host 上の queue が、1つのキャリッジリターン(CR、改行)文字からなる印刷ジョブを受け付けるかどうかをテストできます。何も印刷されないのが妥当です。おそらく、空白のページが排出されるはずです。

```
echo -en "\r" \  
| lp -d queue -h host
```

ネットワークプリンタまたは印刷サーバボックスのトラブルシューティング
印刷サーバボックス上のスプーラは時々、大量の印刷ジョブを処理する必要が生じた場合、問題を引き起こすことがあります。これは印刷サーバボックス内のスプーラに起因しているので、ほとんどの場合、管理者が実行できる対策はありません。回避策として、印刷サーバボックス内のス

プーラを使用することを避け、TCPソケットを使用して、印刷サーバボックスに接続されているプリンタに直接送信できます。詳細については、**23.5項「ネットワークプリンタ」** (490 ページ)を参照してください。

この方法により、印刷サーバボックスは異なる形式のデータ転送(TCP/IP ネットワークとローカルプリンタ接続)間の単純なコンバータになります。この方法を使用するには、印刷サーバボックス内にある、該当するTCPポートについて把握する必要があります。プリンタが印刷サーバボックスに接続されていて、電源がオンになっている場合、印刷サーバボックスの電源をオンにした後、しばらく経過した時点で、nmapパッケージのnmapユーティリティを使用することにより、このTCPポートを特定できます。たとえば、nmap *IP-address*は、印刷サーバボックスに関して次のような出力をすることがあります。

Port	State	Service
23/tcp	open	telnet
80/tcp	open	http
515/tcp	open	printer
631/tcp	open	cups
9100/tcp	open	jetdirect

この出力は、印刷サーバボックスに接続されているプリンタが、ポート9100上のTCPソケットを介して使用できることを示します。nmapはデフォルトでは、`/usr/share/nmap/nmap-services`内でリストされている多数の一般的な既知のポートだけを確認します。可能性のあるすべてのポートをチェックするには、nmap

`-p from_port-to_portIP-address`コマンドを使用します。これは、ある程度の時間を要することがあります。詳細な情報については、nmapのマニュアルページを参照してください。

次のようなコマンドを入力します。

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

これは、このポートを通してプリンタを使用できるかどうかをテストするために、該当のポートへ文字列またはファイルを直接送信します。

23.9.5 エラーメッセージを生成しない異常なプリントアウト

印刷システムの観点では、CUPSバックエンドが受信側(プリンタ)へのデータ転送を完了した段階で、印刷ジョブは完了します。受信側でそれ以降の処理が失敗した場合(たとえば、プリンタがそのプリンタ固有のデータを印刷できない)、印刷システムはそのことを検出しません。プリンタがそのプリンタ固有のデータを印刷できない場合、そのプリンタにより適していると考えられる他のPPDファイルを選択します。

23.9.6 無効にされたキュー

受信側へのデータ転送が数回の試行後に完全に失敗した場合、usbやsocketなどのCUPSバックエンドは印刷システム(より正確にはcupsd)にエラーを報告します。データ転送が不可能であると報告する前に、バックエンドは、試行に意味があるかどうか、また何回の試行に意味があるかを判断します。それ以上の試行は無駄に終わる可能性があるため、cupsdは該当のキューへの印刷を無効にします。問題の原因を取り除いた後、システム管理者は/usr/bin/enableコマンドを使用して、印刷を再度有効にする必要があります。

23.9.7 CUPS参照:印刷ジョブの削除

CUPSネットワークサーバが参照機能を使用して自らのキューをクライアントホストへブロードキャストし、クライアントホスト側で適切なローカルcupsdがアクティブになっている場合、クライアント側のcupsdはアプリケーションから印刷ジョブを受け付け、サーバ側のcupsdへそれらを転送します。cupsdが印刷ジョブを受け付けた段階で、そのジョブに新しいジョブ番号が割り当てられます。したがって、クライアントホスト上のジョブ番号は、サーバ上のジョブ番号とは異なっています。印刷ジョブは通常、即座に転送されるので、クライアントホスト上でジョブ番号を使用してそのジョブを削除することはできません。クライアント側のcupsdは、サーバ側のcupsdへの転送が完了した段階で、その印刷ジョブは完了したと考えるからです。

サーバ上にある印刷ジョブを削除するには、`lpstat -h cups.example.com -o`などのコマンドを使用してサーバ上でのジョブ番号を判断します。サーバがまだその印刷ジョブを完了していない(つまり、プリンタへ完全に送信していない)ことが前提条件です。このジョブ番号を使用して、サーバ上にある印刷ジョブを削除できます。

```
cancel -h cups.example.com queue-jobnumber
```

23.9.8 異常な印刷ジョブとデータ転送エラー

印刷プロセスの実行中に、管理者がプリンタの電源をオフにして再度オンにした場合、またはコンピュータをシャットダウンしてリポートした場合、印刷ジョブはキュー内にとどまっていて、印刷が再開されます。異常な印刷ジョブは、`cancel`を使用してキューから削除する必要があります。

印刷ジョブが異常な場合、またはホストとプリンタの間で通信エラーが発生した場合、プリンタはデータを正しく処理できなくなるので、文字化けのような大量のページを印刷することがあります。この状態を処理するには、次の処理を実行します。

- 1 プリンタの動作を停止するために、インクジェットプリンタの場合、すべての用紙を取り除きます。レーザープリンタの場合、用紙トレイを開けます。上位機種のプリンタでは、現在のプリントアウトをキャンセルするボタンを用意していることもあります。
- 2 この時点で、印刷ジョブはキューに残っている可能性があります。ジョブがキューから削除されるのは、ジョブ全体をプリンタへ送信した後に限られるからです。`lpstat -o`(または`lpstat -h cups.example.com -o`)を使用して、どのキューが現在印刷に使用されているかを確認します。`cancel queue-jobnumber`(または`cancel -h cups.example.com queue-jobnumber`)を使用して、該当の印刷ジョブを削除します。
- 3 印刷ジョブがすでにキューから削除されたにもかかわらず、一部のデータが依然として、プリンタへ送信され続けることもあります。**CUPS**バックエンドプロセスが、引き続き該当のキューを対象として動作しているかどうかをチェックし、その処理を終了します。たとえば、プリンタがパラレルポートに接続されている場合、`fuser -k /dev/lp0`コマンドを使用して、引き続きそのプリンタ(より正確に表現すると、パラレル

ポート)にアクセスしているすべてのプロセスを終了することができます。

- 4 ある程度の時間にわたって電源をオフにして、プリンタを完全にリセットします。その後、紙を元に戻し、プリンタの電源をオンにします。

23.9.9 CUPS印刷システムのデバッグ

CUPS印刷システムの問題を特定するために、次の一般的な処理を実行してください。

- 1 `/etc/cups/cupsd.conf`内に、`LogLevel debug`を設定します。
- 2 `cupsd`コマンドを停止します。
- 3 `/var/log/cups/error_log*`を削除して、大規模なログファイルから検索を行うことを避けます。
- 4 `cupsd`を起動します。
- 5 問題の原因となったアクションをもう一度実行します。
- 6 `/var/log/cups/error_log*`内のメッセージを確認し、問題の原因を識別します。

udevを使用した動的カーネル デバイス管理

24

バージョン2.6以降、カーネルは、実行中のシステム上のほぼすべてのデバイスを追加または削除できるようになりました。デバイス状態の変更(デバイスが接続されているか、または取り外されたか)をユーザスペースに反映させる必要があります。デバイスは、接続後、検出されるとすぐに設定されなければなりません。また、特定のデバイスのユーザは、このデバイスの状態に関する変更について通知を受ける必要があります。udevは、/devディレクトリ内にデバイスノードファイルおよびシンボリックリンクを動的に管理することにより、必要なインフラストラクチャを提供します。udevルールによって、外部ツールをカーネルデバイスイベント処理に含めることができます。これにより、カーネルデバイス処理の一部として実行する特定のスクリプトを追加するなど、udevデバイス処理をカスタマイズしたり、デバイス処理中に評価する他のデータを要求およびインポートしたりできます。

24.1 /devディレクトリ

/devディレクトリ内のデバイスノードを使用して、対応するカーネルデバイスにアクセスできます。udevにより、/devディレクトリは、カーネルの現在の状態を反映します。カーネルデバイスは、それぞれ1つの対応するデバイスファイルを持ちます。デバイスがシステムから取り外されると、そのデバイスノードは削除されます。

/devディレクトリのコンテンツは一時的なファイルシステム内で管理され、すべてのファイルはシステムの起動時に新規に作成されます。意図的に、手動で作成または変更されたファイルは再起動時に復元されません。対応するカー

ネルデバイスの状態にかかわらず、`/dev`ディレクトリ内に常駐する静的ファイルおよびディレクトリは、`/lib/udev/devices`ディレクトリ内に保管できます。システムの起動時、そのディレクトリのコンテンツは、`/lib/udev/devices`内のファイルと同じ所有者およびパーミッションの`/dev`ディレクトリ内にコピーされます。

24.2 カーネルのueventおよびudev

必要なデバイス情報は、システムファイルシステムによってエクスポートされます。カーネルが検出および初期化するすべてのデバイスについて、そのデバイス名を含んだディレクトリが作成されます。このディレクトリには、デバイス固有のプロパティのある属性ファイルが含まれます。デバイスが追加または削除されるたびに、カーネルはueventを送信して、udevに変更を通知します。

udevデーモンは、起動時に`/etc/udev/rules.d/*.rules`から提示されたすべての規則を読み、解析し、メモリ内に保管します。規則ファイルが変更、追加または削除されると、デーモンはイベントを受信し、メモリ内の規則を更新します。

着信したイベントは、すべて一連のプロバイダルールと一致します。規則によって、イベント環境キーを追加または変更したり、作成するデバイスノードに特定の名前を要求したり、ノードを指すシンボリックリンクを追加したり、またはデバイスノードの作成後に実行するプログラムを追加したりできます。ドライバのコアueventは、カーネルのネットリンクソケットから受信されます。

24.3 ドライバ、カーネルモジュールおよびデバイス

カーネルバスドライバは、デバイスを検出します。検出されたデバイスごとに、カーネルは内部デバイス構造を作成し、ドライバコアは、ueventをudevデーモンを送信します。バスデバイスは、デバイスの種類を示す特別な形式のIDを識別します。通常、これらのIDは、ベンダー、製品IDおよびサブシステム固有の値で構成されています。各バスには、これらのIDに対してMODALIAS

という独自のスキームを持ちます。カーネルは、デバイス情報を読み取り、この情報からMODALIASID文字列を作成し、イベントとともに文字列を送信します。USBマウスの場合、次のようになります。

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

各デバイスドライバは、既知の処理可能デバイスのエイリアスのリストを持ちます。このリストは、カーネルモジュールファイル自体にも含まれています。depmodプログラムは、IDリストを読み取り、現在使用可能なすべてのモジュールについて、カーネルの/lib/modulesディレクトリ内にmodules.aliasを作成します。このインフラストラクチャにより、MODALIASキーを持つイベントごとにmodprobeを呼び出すだけで簡単にモジュールをロードできます。modprobe \$MODALIASが呼び出されると、そのデバイスに付けられたデバイスエイリアスとモジュールによって提示されるエイリアスとが一致します。一致したエントリが見つかり、そのモジュールがロードされます。これらの処理はすべて、udevによってトリガされ、自動的に行われます。

24.4 ブートおよび初期デバイスセットアップ

udevデーモンが実行する前にブートプロセス中に発生するすべてのデバイスイベントは、rootファイルシステムに常駐し、ブート時にはアクセスできないため、これらのイベントは消失します。この消失を補うため、カーネルは、sysfsファイルシステム内のデバイスごとにueventファイルを提供します。そのファイルにaddと書き込むことにより、カーネルは、ブート時に消失したものと同一イベントを再送信します。/sys内のすべてのueventファイル間で簡単にループすることにより、すべてのイベントが再びデバイスノードを作成し、デバイスセットアップを実行します。

たとえば、ブート中に存在するUSBマウスは、ドライバはそのときに存在しないため、先のブート論理では初期化されない場合があります。デバイス検出イベントは、消失し、そのデバイスのカーネルモジュールは検出されません。接続されている可能性があるデバイスを手動で検索する代わりに、udevは、rootファイルシステムが使用可能になった後でカーネルからすべてのデバイスイベントを要求するだけです。これにより、このUSBマウスデバイスのイベントが再び実行します。これで、マウントされたrootファイルシステム上のカーネルモジュールが検出され、USBマウスが初期化されます。

ユーザスペースでは、実行時のデバイスのcoldplugシーケンスとデバイス検出との間に明らかな違いはありません。両方の場合も、同じ規則を使用して一致検出が行われ、同じ設定されたプログラムが実行されます。

24.5 udevイベントのデバッグ

udevmonitorプログラムを使用して、ドライバコアイベントおよびudevイベントプロセスのタイミングをビジュアル化できます。

```
UEVENT[1132632714.285362] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UEVENT[1132632714.288166] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UEVENT[1132632714.309485] add@/class/input/input6
UEVENT[1132632714.309511] add@/class/input/input6/mouse2
UEVENT[1132632714.309524] add@/class/usb_device/usbdev2.12
UDEV [1132632714.348966] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UDEV [1132632714.420947] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UDEV [1132632714.427298] add@/class/input/input6
UDEV [1132632714.434223] add@/class/usb_device/usbdev2.12
UDEV [1132632714.439934] add@/class/input/input6/mouse2
```

UEVENT行は、カーネルがnetlinkで送信したイベントを示します。UDEV行は、完了したudevイベントハンドラを示します。タイミングは、マイクロ秒で出力されます。UEVENTおよびUDEV間の時間は、udevがこのイベントの処理に要した時間、またはudevデーモンがこのイベントと関連する実行中のイベントとの同期の実行に遅れた時間です。たとえば、ハードディスクパーティションのイベントは常に、メインディスクイベントがハードウェアに問い合わせたデータに依存する可能性があるため、メインデバイスイベントが完了するのを待ちます。

udevmonitor --envは、完全なイベント環境を示します。

```
UDEV [1132633002.937243] add@/class/input/input7
udevmon LOG=3
ACTION=add
DEVPATH=/class/input/input7
SUBSYSTEM=input
SEQNUM=1043
PHYSDEVPATH=/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
PHYSDEVBUS=usb
PHYSDEVDRIVER=usbhid
PRODUCT=3/46d/c03e/2000
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.1-2/input0"
```

```
UNIQ=""  
EV=7  
KEY=70000 0 0 0 0 0 0 0  
REL=103
```

udevは、syslogにもメッセージを送信します。いずれのメッセージがsyslogに送信されるかを制御するデフォルトのsyslogの優先度は、udev設定ファイルの/etc/udev/udev.conf内で指定されています。実行中のデーモンのログ優先度は、udevcontrol log_priority=level/numberで変更できます。

24.6 udevルールを処理するカーネルデバイスイベントへの影響

udevルールは、カーネルがイベント自体に追加するすべてのプロパティ、またはカーネルがsysfsにエクスポートするすべての情報と一致します。また、この規則で、外部プログラムからの追加情報を要求することもできます。各イベントは、指定されたすべての規則と一致します。すべての規則は、/etc/udev/rules.dディレクトリにあります。

規則ファイル内の各行には、少なくとも1つのキー値ペアが含まれています。これらは、一致と割り当てキーという2種類のキーです。すべての一致キーが各値と一致する場合、その規則が適用され、割り当てキーに指定された値が割り当てられます。一致する規則がある場合、デバイスノードの名前を指定、ノードを指すシンボリックリンクを追加、またはイベント処理の一部として指定されたプログラムを実行できます。一致する規則がない場合、デフォルトのデバイスノード名を使用して、デバイスノードが作成されます。規則の構文、および一致またはデータをインポートするために指定されたキーについては、udevのマニュアルページで説明します。

24.7 永続的なデバイス名の使用

動的デバイスディレクトリおよびudevルールインフラストラクチャによって、認識順序やデバイスの接続手段にかかわらず、すべてのディスクデバイスに一定の名前を指定できるようになりました。カーネルが作成する適切なブロックデバイスはすべて、特定のバス、ドライブタイプまたはファイルシステムに関する特別な知識を備えたツールによって診断されます。動的カーネルに

よって指定されるデバイスノード名とともに、udevは、デバイスを指す永続的なシンボリックリンクのクラスを維持します。

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   |-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   |-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    |-- 4210-8F8C -> ../../sdd1
```

24.8 置換されたhotplugパッケージ

以前に使用されていたhotplugパッケージは、udevとudev関連カーネルインフラストラクチャに完全に置き換えられました。以前のhotplugインフラストラクチャの次の部分は不要になったか、または、udevに機能が移行しました。

```
/etc/hotplug/*.agent
```

不要になったか、または/lib/udevに移動しました。

```
/etc/hotplug/*.rc
```

/sys/*/ueventトリガに置き換えられました。

```
/etc/hotplug/blacklist
```

blacklist option in modprobe.confに置き換えられました。

/etc/dev.d/*

RUNキーに置き換えられました。

/etc/hotplug.d/*

RUNキーに置き換えられました。

/sbin/hotplug

netlinkをリスンする**udev**dによって置き換えられました。**root**ファイルシステムがマウントされるまで最初の**RAM**ファイルでのみ使用され、その後は無効になります。

/dev/*

/lib/udev/devices/*内の動的**udev**および静的コンテンツによって置き換えられました。

次のファイルおよびディレクトリには、**udev**インフラストラクチャの重要な要素が含まれています。

/etc/udev/udev.conf

メインの**udev**設定ファイル

/etc/udev/rules.d/*

規則と一致する**udev**イベント

/lib/udev/devices/*

静的/devコンテンツ

/lib/udev/*

udevルールから呼び出されるヘルパープログラム

24.9 詳細情報

udevインフラストラクチャの詳細については、次のマニュアルページを参照してください。

udev

udev、キー、規則およびその他の重要な設定問題に関する一般情報。

udevinfo

udevinfoは、**udev**データベースからデバイス情報を取得するのに使用されます。

udev

udevイベント管理デーモンに関する情報。

udevmonitor

udevmonitorは、コンソールにカーネルおよび**udev**イベントシーケンスを出力します。このツールは、主にデバッグの目的で使用されます。

Linuxのファイルシステム

SUSE Linux Enterprise®には、ReiserFS、Ext2、Ext3、およびXFSなどの、さまざまなファイルシステムが用意されています。これらのファイルシステムは、インストール時に選択することができます。各ファイルシステムには、それぞれの長所と欠点があります。利用環境に応じて最適のファイルシステムをご利用ください。高性能のクラスタリングが必要な場合に備えて、SUSE Linux Enterprise ServerにはOCFS2 (Oracle Cluster File System 2)が付属しています。

25.1 用語

メタデータ(metadata)

ファイルシステムの内部にあるデータ構造で、ディスク上にあるすべてのデータが適切に編成され、アクセス可能であることを保証します。本質的には、「データに関するデータ」です。」ほぼすべてのファイルシステムが、メタデータからなる独自の構造を採用していますが、各ファイルシステムが互いに異なるパフォーマンス特性を示すのは、それが1つの理由になっています。メタデータが破損しないよう維持するのは、非常に重要なことです。もし破損した場合、ファイルシステム内にあるすべてのデータがアクセス不能になる可能性があるからです。

inode

inodeには、サイズ、リンクの数、ファイルの内容を実際に格納しているディスクブロックへのポインタ、作成された日時、変更された日時、およびアクセスされた日時など、ファイルに関するさまざまな情報が記録されています。

ジャーナル(journal)

ファイルシステムの用語では、ジャーナルとはディスク上に存在する構造であり、ファイルシステムのメタデータに対して加えられた変更を記録するためにファイルシステムが格納するさまざまなログを保持しています。ジャーナル機能は、Linuxシステムの回復時間を大幅に短縮します。システム起動時に、ファイルシステム全体をチェックする冗長な検索プロセスを不要にするからです。ただし、それはジャーナルが再現できる場合に限定されます。

25.2 Linuxの主要なファイルシステム

2、3年前とは異なり、Linuxシステムで使用するファイルシステムを選択するのは、数秒で済む問題(Ext2とReiserFSのどちらにするか)ではありません。カーネル2.4およびそれ以降では、さまざまなファイルシステムが選択できるようになりました。この後で、各ファイルシステムの基本的な動作原理、およびそれらが提供する利点の概要について説明します。

あらゆる用途で最適な単一のファイルシステムなど存在しない、ということ を考慮しておくことが重要です。各ファイルシステムには特定の利点と欠点があり、それらを考慮する必要があります。最も洗練されたファイルシステムであっても、妥当なバックアップの方針を別の機能で置き換えることはできません。

この章で「データの完全性」および「データの一貫性」という用語が登場した場合、それらはユーザスペースのデータ(アプリケーションが自らのファイルに書き込むデータ)の一貫性を指していません(メタデータの一貫性を指します)。ユーザスペースのデータが一貫しているかどうかは、アプリケーション自体が管理する必要があります。

重要項目: ファイルシステムのセットアップ

この章では特に注記がない限り、パーティションやファイルシステムのセットアップまたは変更するために必要なステップは、すべてYaSTを使用して実行できます。

25.2.1 ReiserFS

2.4カーネルの主要機能の1つとして、バージョン6.4から2.2.x SUSEカーネルに対して、ReiserFSをカーネルパッチとして利用できるようになりました。

ReiserFSは、Hans ReiserとNamesys開発チームにより設計されました。ReiserFSは、Ext2に代わる強力な選択肢であることを実証してきました。その主要な利点は、より良いディスクスペース使用効率、より良いディスクアクセスパフォーマンス、およびより高速なクラッシュ回復機能です。

ReiserFSの利点をより詳細に記述すると、以下のようになります。

より良いディスクスペース使用効率

ReiserFSでは、すべてのデータは、**B^{*}-Tree**(バランストツリー)と呼ばれる構造内で編成されています。このツリー構造は、より良いディスクスペース使用効率に貢献しています。小さなファイルは、**B^{*}-Tree**のリーフノードに直接格納されるからです。そのようなファイルをどこか他の場所に格納して、ディスク上の実際の場所を指すポインタを維持するより優れています。それに加えて、ストレージ(記憶領域)は1KBまたは4KBのチャンク単位で割り当てられるのではなく、実際に必要なサイズの構成部分(エクステント)を割り当てられます。もう1つの利点は、inodeの動的割り当てに関係しています。これは、ファイルシステムの作成時にinodeの密度を指定する必要のある、Ext2のような従来のファイルシステムに比べて、ファイルシステムの柔軟性を高めます。

より良いディスクアクセスパフォーマンス

小規模なファイルでは、多くの場合、ファイルのデータと「stat_data」(inode)情報が互いに隣り合って保存されます。これらは1回のディスクI/O操作で読み取れるので、ただ1回のディスクアクセスで、必要な情報すべてを取得できることを意味します。

高速なクラッシュ回復機能

ジャーナルを使用して、メタデータに加えられた最新の変更結果を記録しているので、ファイルシステムが大規模な場合を含め、ファイルシステムを数秒でチェックできます。

データジャーナリングによる信頼性

ReiserFSは、Ext3のセクション25.2.3項「Ext3」(521 ページ)で説明した概念に類似したデータジャーナリングおよび順序データモードをサポートしています。デフォルトのモードは、data=orderedです。このモードで

は、データとメタデータの完全性は保証されますが、メタデータのジャーナリングだけが行われます。

25.2.2 Ext2

Ext2の起源は、Linuxの歴史の初期にさかのぼります。その前身であったExtended File Systemは、1992年4月に実装され、Linux 0.96cに統合されました。Extended File Systemは多くの変更を加えられ、Ext2として数年にわたって、最も人気のあるLinuxファイルシステムになりました。その後、他のジャーナルファイルシステムが作成され、非常に短い回復時間を達成したため、Ext2の重要性は低下しました。

Ext2の利点に関する短い要約を読むと、かつて幅広く好まれ、そして今でも一部の分野で多くのLinuxユーザから好まれるLinuxファイルシステムである理由を理解するのに役立ちます。

堅牢性

「古くからある標準」として、Ext2は過去に多くの改良を受け、集中的にテストされてきました。このような理由で、多くの人はExt2を岩のように堅牢(rock-solid)と呼びます。ファイルシステムが正常にアンマウントできず、システムが機能停止した場合、e2fsckはファイルシステムのデータの分析を開始します。メタデータは一貫した状態に戻り、保留されていたファイルとデータブロックは、指定のディレクトリ(lost+found)に書き込まれます。ジャーナルファイルシステムとは対照的に、e2fsckは、最近変更されたわずかなメタデータだけではなく、ファイルシステム全体を分析します。この結果、ジャーナルファイルシステムがログデータだけをチェックするのに比べて、かなり長い時間を要します。ファイルシステムのサイズにもよりますが、この手順は30分またはそれ以上を要することがあります。したがって、高可用性を必要とするどのようなサーバでも、Ext2を選択することは望ましくありません。ただし、Ext2はジャーナルを維持せず、非常にわずかなメモリを使用するだけなので、時には他のファイルシステムより高速なことがあります。

容易なアップグレード性

Ext2のコードは、Ext3が次世代ファイルシステムであることを明確に主張するための強力な土台になりました。Ext2の信頼性および堅牢性が、ジャーナルファイルシステムの利点と見事に融合されました。

25.2.3 Ext3

Ext3は、Stephen Tweedieによって設計されました。他のすべての次世代ファイルシステムとは異なり、Ext3は完全に新しい設計理念に基づいているわけではありません。Ext3は、Ext2をベースとしています。これら2つのファイルシステムは、互いに非常に似通っています。Ext3ファイルシステムを、Ext2ファイルシステムの上に構築することも容易です。Ext2とExt3の間にある最も重要な違いは、Ext3がジャーナルをサポートしていることです。要約すると、Ext3には、次の3つの主要な利点があります。

Ext2からの容易で信頼性の高いアップグレード

Ext3はExt2のコードをベースとし、ディスクフォーマットとメタデータフォーマットが共通しているので、Ext2からExt3へのアップグレードは非常に容易です。ReiserFSまたはXFSのような他のファイルシステムへの移行はかなり手間がかかります(ファイルシステム全体のバックアップを作成し、移行先ファイルシステムを新規に作成する必要があります)が、それとは異なり、Ext3への移行は数分で完了します。ファイルシステム全体を新規に作成する作業は障害なしで完了するとは限りませんが、Ext3への移行にはそのような作業が伴わないので、非常に安全でもあります。ジャーナルファイルシステムへのアップグレードを待つ既存のExt2システムの数を考慮すると、多くのシステム管理者にとってExt3が重要な選択肢になっていることが容易に想像できるはずです。Ext3からExt2へのダウングレードも、アップグレードと同じほど容易です。Ext3ファイルシステムのアンマウントを正常に行い、Ext2ファイルシステムとして再マウントするだけです。

信頼性とパフォーマンス

他のジャーナルファイルシステムは、「メタデータのみ」のジャーナルアプローチに従っています。これは、使用中のメタデータは常に一貫した状態を維持されていますが、ファイルシステムのデータ自体に関しては同じことが自動的に保証されるわけではない、という意味です。Ext3は、メタデータとデータの両方に注意するよう設計されています。「注意」の度合いはカスタマイズできます。Ext3のdata=journalモードを有効にした場合、最大の保護(データの完全性)を実現しますが、メタデータとデータの両方がジャーナル化されるので、システムの動作が遅くなります。比較的新しいアプローチは、data=orderedモードを使用することです。これは、データとメタデータ両方の完全性を保証しますが、ジャーナルを適用するのはメタデータのみです。ファイルシステムドライバは、1つのメタデータの更新に対応するすべてのデータブロックを収集します。

これらのブロックは、メタデータの更新前にディスクに書き込まれます。その結果、パフォーマンスを犠牲にすることなく、メタデータとデータの両方に関する一貫性を達成できます。3番目のオプションは、`data=writeback`を使用することです。これは、対応するメタデータをジャーナルにコミットした後で、データをメインファイルシステムに書き込むことを可能にします。多くの場合、このオプションは、パフォーマンスの点で最善と考えられています。しかし、内部のファイルシステムの完全性が維持される一方で、クラッシュと回復を実施した後では、古いデータがファイル内に再登場することを許してしまう可能性があります。管理者が他のオプションを指定しない限り、Ext3はデフォルトで`data=ordered`を使用して動作します。

25.2.4 Ext2ファイルシステムからExt3への変換

Ext2ファイルシステムをExt3に変換するには、次の手順に従います。

- 1 `root`として`tune2fs -j`を実行して、Ext3ジャーナルを作成します。この結果、デフォルトのパラメータを使用してExt3ジャーナルが作成されます。

ジャーナルの大きさや、どのデバイスにジャーナルを配置するかを自分で決定するには、代わりに`tune2fs -J`を実行し、希望のジャーナルオプションである`size=`および`device=`を指定します。`tune2fs`プログラムの詳細については、「`tune2fs`マニュアル」ページを参照してください。

- 2 Ext3ファイルシステムがExt3として正しく認識されることを保証するために、`root`として`/etc/fstab`ファイルを編集し、対応するパーティションに対して指定されているファイルシステムタイプを`ext2`から`ext3`へ変更します。この変更結果は、次の再起動後に有効になります。
- 3 Ext3パーティションとしてセットアップされたファイルシステムからブートするには、`ext3`と`jbd`の各モジュールを`initrd`内に含めます。この作業を行うには、`root`として、`ext3`および`jbd`を`INITRD_MODULES`変数に追加して`/etc/sysconfig/kernel`を編集します。変更を保存した後、`mkinitrd`コマンドを変更します。これにより新規の`initrd`がビルドされ、すぐに使用できます。

25.2.5 XFS

本来は、IRIX OS用のファイルシステムを意図してSGIがXFSの開発を開始したのは、1990年代初期です。XFSの背後にある考えは、ハイパフォーマンスの64ビットジャーナルファイルシステムを作成し、非常に要求の多い今日のコンピューティングの課題を満たすことです。XFSは大規模なファイル进行操作する点で非常に優れていて、ハイエンドのハードウェアを適切に活用します。しかし、XFSには1つの欠点があります。ReiserFSと同様、XFSはメタデータの完全性には最大の注意を払いますが、データの完全性にはそれほど注意を払いません。

XFSの主要な機能を簡単に観察することにより、ハイエンドのコンピューティング分野で、XFSが他のジャーナルファイルシステムの強力な競合相手という立場を実証している理由を説明できます。

アロケーショングループの採用による高いスケーラビリティ

XFSファイルシステムの作成時に、ファイルシステムの基にあるブロックデバイスは、等しいサイズを持つ8つ以上の線形の領域に分割されます。これらをアロケーショングループと呼びます。各アロケーショングループは、独自のinodeと空きディスクスペースを管理します。実用的には、アロケーショングループを、1つのファイルシステムの中にある複数のファイルシステムと見なすこともできます。アロケーショングループは互いに独立しているのではなく、カーネルから複数を同時にアドレス指定できる、という特徴があります。この特徴は、XFSの高いスケーラビリティの鍵です。独立性の高いアロケーショングループは、性質上、マルチプロセッサシステムのニーズに適しています。

ディスクスペースの効率的な管理によるハイパフォーマンス

空きスペースとinodeは、各アロケーショングループ内の B^+ -Treeによって処理されます。 B^+ -Treeの採用は、XFSのパフォーマンスとスケーラビリティに大きく貢献しています。XFSでは、遅延アロケーションを採用しています。XFSはアロケーション(割り当て)を2つのパートに分割して、この操作を処理します。保留されているトランザクションはRAMの中に保存され、適切な量のスペースが確保されます。XFSはこの時点では、データの格納場所(言い換えると、ファイルシステムのどのブロックか)を決定しません。決定可能な最後の瞬間まで、この決定は遅延(先送り)されます。短時間だけ存続する一部の一時データは、ディスクに書き込まれません。XFSがデータの実際の保存場所を決定する時点で、それらのデータは不要になっているからです。したがって、XFSは書き込みのパフォー

マンスを向上させ、ファイルシステムの断片化(フラグメンテーション)を減らします。遅延アロケーションは、他のファイルシステムより書き込みイベントの頻度を下げる結果をもたらすので、書き込み中にクラッシュが発生した場合、データ損失が深刻になる可能性が高くなります。

事前割り当てによるファイルシステムの断片化の回避

データをファイルシステムに書き込む前に、XFSはファイルが必要とする空きスペースを予約(プリアラケート、事前割り当て)します。したがって、ファイルシステムの断片化は大幅に減少します。ファイルの内容がファイルシステム全体に分散することがないので、パフォーマンスが向上します。

25.2.6 Oracle Cluster File System 2

OCFS2は、クラスタリング設定用に作成されたジャーナルファイルシステムです。Ext3などの標準の単一ノードファイルシステムとは対称的に、OCFS2では複数ノードを管理することができます。OCFS2では、SANやマルチパスセットアップなどの共有ストレージにまたがって、ファイルシステムを拡散することができます。

OCFS2セットアップの各ノードは、すべてのデータに対して同時に読み込み/書き込みアクセスを行うことができます。そのためには、OCFS2がクラスタに対応していなければなりません。つまり、OCFS2には、クラスタを構成するノード、およびノードが実際に動作して利用できるかどうかを判断できる手段がなければなりません。クラスタのメンバーシップを算出するために、OCFS2にはノードマネージャ(NM)が用意されています。クラスタ内のノードの可用性を監視するために、OCFS2には簡単なハートビート機能が実装されています。多数のノードからのファイルシステムへの直接アクセスによる混乱を回避するために、OCFS2にはロックマネージャのDLM(distributed lock manager)も用意されています。ノード間の通信は、TCPベースのメッセージングシステムにより処理されます。

OCFS2の主要機能と利点を次に示します。

- メタデータのキャッシングとジャーナリング
- データベースのパフォーマンスを向上する非同期、直接I/Oのサポート
- 最大16TBまでのボリュームで、最高4KBまでの複数ブロックサイズをサポート(各ボリュームで異なるブロックサイズを使用可能)

- ・ ノード間にまたがるファイルデータの整合性
- ・ 255台までのクラスタノードをサポート

OCFS2の詳細は、[第14章 Oracle Cluster File System 2](#) (317 ページ)を参照してください。

25.3 サポートされている他のいくつかのファイルシステム

表 25.1. 「Linux環境でのファイルシステムのタイプ」 (525 ページ)は、Linuxがサポートしている他のいくつかのファイルシステムを要約したものです。これらは主に、他の種類のメディアや外部オペレーティングシステムとの互換性およびデータの相互交換を保証することを目的としてサポートされています。

表 25.1 Linux環境でのファイルシステムのタイプ

cramfs	<i>Compressed ROM file system</i> (圧縮ROMファイルシステム):ROM用の圧縮された読み込み専用ファイルシステムです。
hpfs	<i>High Performance File System</i> (ハイパフォーマンスファイルシステム):IBM OS/2の標準ファイルシステムです。読み取り専用モードでサポートされています。
iso9660	CD-ROMの標準ファイルシステム。
minix	このファイルシステムは、オペレーティングシステムに関する学術的なプロジェクトを起源とするもので、Linuxで最初に使用されたファイルシステムです。現在では、フロッピーディスク用のファイルシステムとして使用されています。
msdos	<i>fat</i> 、つまり当初はDOSで使用されていたファイルシステムであり、現在はさまざまなオペレーティングシステムで使用されています。

ncpfs	Novellのボリュームをネットワーク経由でマウントするためのファイルシステム。
nfs	<i>Network File System</i> (ネットワークファイルシステム): この場合、ネットワーク内にある任意のコンピュータにデータを格納でき、ネットワーク経由でアクセスを許可できるファイルシステムを指します。
smbfs	<i>Server Message Block</i> (サーバメッセージブロック): Windowsのような製品が、ネットワーク経由でのファイルアクセスを可能にする目的で採用しています。
sysv	SCO UNIX、Xenix、およびCoherent (PC用の商用UNIXシステム)が採用。
ufs	BSD、SunOS、およびNeXTstepが採用しています。読み取り専用モードでサポートされています。
umsdos	<i>UNIX on MSDOS</i> : 通常のfatファイルシステムに対して適用されるもので、特別なファイルを作成することにより、UNIXの機能(パーミッション、リンク、長いファイル名)を実現します。
vfat	<i>Virtual FAT</i> : fatファイルシステムを拡張したものです(長いファイル名をサポートします)。
ntfs	<i>Windows NT file system</i> (Windows NTファイルシステム)、読み取り専用です。

25.4 Linux環境での大規模ファイルサポート

当初、Linuxは最大2GBのファイルサイズをサポートしていました。マルチメディアが爆発的に普及する前、およびLinux環境で大規模データベースを運用することを誰も試みていないうちは、これで十分でした。サーバコンピューティングの重要性がますます高くなるにつれて、カーネルとCライブラリが変

更され、2GBを超えるファイルサイズをサポートするようになりました。現在、ほぼすべての主要ファイルシステムで、LFSがサポートされており、高度なコンピューティングを行うことができます。現在のLinuxファイルやファイルシステムの制約の概要については、表25.2、「ファイルシステムの最大サイズ(ディスクフォーマット時)」(527 ページ)を参照してください。

表 25.2 ファイルシステムの最大サイズ(ディスクフォーマット時)

ファイルシステム	ファイルサイズ(バイト)	ファイルシステムのサイズ(バイト)
Ext2またはExt3(ブロックサイズ 1KB)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2またはExt3(ブロックサイズ 2KB)	2^{38} (256 GB)	2^{43} (8 TB)
Ext2またはExt3(ブロックサイズ 4KB)	2^{41} (2 TB)	2^{44} -4096 (-16 TB-4096 バイト)
Ext2またはExt3(ブロックサイズ 8KB)(Alphaなどの、8KBページ採用のシステム)	2^{46} (64 TB)	2^{45} (32 TB)
ReiserFS v3	2^{46} (64 TB)	2^{45} (32 TB)
XFS	2^{63} (8 EB)	2^{63} (8 EB)
NFSv2 (クライアント側)	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3 (クライアント側)	2^{63} (8 EB)	2^{63} (8 EB)

重要項目: Linuxカーネルの制限

表 25.2. 「ファイルシステムの最大サイズ(ディスクフォーマット時)」(527 ページ)は、ディスクフォーマット時の制限について説明しています。カーネル2.6は、自らが取り扱うファイルとファイルシステムのサイズについて、独自の制限を課しています。これらを次に示します。

File Size

32ビットシステムでは、ファイルは2TB (2^{41} バイト)のサイズを上回ることができません。

ファイルシステムのサイズ

ファイルシステムは最大 2^{73} バイトのサイズまでサポートします。しかし、この制限は、現在使用可能なハードウェアが到達可能な範囲を上回っています。

25.5 詳細情報

ここまでに説明した各ファイルシステムのプロジェクトには、独自のWebページがあります。そこで詳しいドキュメントとFAQ、さらにメーリングリストを参照することができます。

- <http://e2fsprogs.sourceforge.net/>
- <http://www.zipworld.com.au/~akpm/linux/ext3/>
- http://chichkin_i.zelnet.ru/namesys/
- <http://oss.sgi.com/projects/xfs/>
- <http://oss.oracle.com/projects/ocfs2/>

Linuxのファイルシステムに関する包括的で複数のパートからなるチュートリアルは、*IBM developerWorks*のWebページ<http://www-106.ibm.com/developerworks/library/l-fs.html>から入手できます。Wikipediaプロジェクトhttp://en.wikipedia.org/wiki/Comparison_of_file_systems#Comparisonから、ファイルシステム(Linuxファイルシステム以外も含む)の詳細な比較情報を入手することができます。

X Windowシステム

X Window System (X11)は、UNIX系のグラフィカルユーザインタフェースで、事実上の標準となっています。Xはネットワークベースであり、あるホスト上で起動されたアプリケーションを、任意のネットワーク(LANやインターネット)を介して接続されている他のホスト上で表示できるようにします。この章ではX Window System環境のセットアップと最適化について説明し、SUSE Linux Enterprise®でのフォントの使用の背景情報を記載しています。

ティップ: IBM System z:グラフィカルユーザインタフェースの設定

IBM System zには、X.Orgがサポートする入出力デバイスはありません。そのため、このセクションで説明している環境設定手順は適用されません。IBM zSeriesの関連情報は、**8.6項 「ネットワークデバイス」** (183 ページ)を参照してください。

26.1 X Window システムの手動設定

デフォルトでは、X Windowシステムは**8.14項 「SaX2」** (214 ページ)に説明されているSaX2インタフェースを使って設定されます。代わりに環境設定ファイルを編集して、手動設定することもできます。

警告: X環境設定ファイルに不適切な設定を行うとハードウェアが損傷する可能性があります

X Window Systemの設定は慎重に行う必要があります。設定が完了するまでは、X Window Systemを起動しないでください。システムが正しく設定されていないと、ハードウェアが復元不能な損傷を受ける可能性があります(特に固定周波数モニタの場合)。本書およびSUSE Linux Enterpriseの作成者は、このような原因による損傷や損害に対していかなる責任も負いません。この情報は慎重に調査されたものですが、ここで説明する方法がすべて正しく、ハードウェアが損傷を受けないという保証はありません。

コマンドsax2で/etc/X11/xorg.confファイルが作成されます。これはX Window Systemの基本設定ファイルです。このファイルには、グラフィックカード、マウス、およびモニタに関する設定がすべて含まれています。

重要項目: X -configureの使用

SUSE Linux EnterpriseのSaX2で失敗した場合は、X -configureを使ってX セットアップの設定を行ってください。 セットアップ 専有(ソフトウェア)

ここでは、設定ファイル/etc/X11/xorg.confの構造について説明します。xorg.confは複数のセクションで構成され、各セクションは設定の特定の側面を取り扱います。各セクションは、キーワードSection <designation>で始まってキーワードEndSectionで終わります。すべてのセクションで、以下の表記規則を使用します。

```
Section "designation"
    entry 1
    entry 2
    entry n
EndSection
```

使用可能なセクションのタイプのリストは表 26.1. 「/etc/X11/xorg.confのセクション」 (531 ページ)にあります。

表 26.1 /etc/X11/xorg.confのセクション

タイプ	意味
ファイル	フォントとRGBカラーテーブルで使用するパス。
ServerFlags	サーバ動作の汎用スイッチ。
モジュール	サーバがロードする必要があるモジュールリスト。
InputDevice	キーボードや特殊入力デバイス(タッチパッド、ジョイスティックなど)といった入力デバイスを設定します。このセクションで重要なパラメータはDriverと、ProtocolおよびDeviceを定義するオプションです。通常、コンピュータに接続した1つのデバイスごとに1つのInputDeviceがあります。
Monitor	使用するモニタ。このセクションの重要な要素は、後でScreenの定義で参照するID、リフレッシュレートのVertRefresh、および同期周波数の制限(HorizSyncおよびVertRefresh)です。設定値はMHz、kHz、およびHz単位です。通常、サーバはモニタ仕様に対応しないmodelineを拒否します。このため、意図せずに高すぎる周波数がモニタに送信されるのを防止できます。
Modes	特定の画面解像度のmodelineパラメータ。これらのパラメータは、ユーザ指定の値に基づいてSaX2で計算でき、通常は変更不要です。固定周波数モニタに接続する場合などは、この時点で手動で介入します。個々の数値の意味の詳細については、HOWTOファイル/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTOを参照してください(howtoenhパッケージ内)。
Device	特定のグラフィックカード。グラフィックカードは記述名で参照されます。

タイプ	意味
画面	MonitorとDeviceを組み合わせ、 X.Org に必要な設定を形成します。Displayサブセクションでは、仮想画面のサイズ(Virtual)、ViewPort、およびこの画面で使用するModesを指定します。
ServerLayout	シングルまたはマルチヘッド設定のレイアウト。このセクションにより、入力デバイスInputDeviceと表示デバイスScreenがバインドされます。
DRI	DRI(Direct Rendering Infrastructure)の情報を提供します。

ここでは、Monitor、Device、およびScreenについて詳しく説明します。他のセクションの詳細については、X.Orgおよびxorg.confのマニュアルページを参照してください。

xorg.confには、複数の異なるMonitorおよびDeviceセクションを記述できます。複数のScreenセクションを記述することも可能です。ServerLayoutセクションでは、このセクションのうち使用するものを判定します。

26.1.1 Screenセクション

Screenセクションでは、MonitorセクションとDeviceセクションを組み合わせ、どの解像度とカラー設定を使用するかを決定します。Screenセクションは例 26.1. 「ファイル/etc/X11/xorg.confのScreenセクション」 (533 ページ) のようになります。

例 26.1 ファイル/etc/X11/xorg.confのScreenセクション

```
Section "Screen"❶
    DefaultDepth 16❷
    SubSection "Display"❸
        Depth 16❹
        Modes "1152x864" "1024x768" "800x600"❺
        Virtual 1152x864❻
    EndSubSection
    SubSection "Display"
        Depth 24
        Modes "1280x1024"
    EndSubSection
    SubSection "Display"
        Depth 32
        Modes "640x480"
    EndSubSection
    SubSection "Display"
        Depth 8
        Modes "1280x1024"
    EndSubSection
    Device "Device[0]"
    Identifier "Screen[0]"❼
    Monitor "Monitor[0]"
EndSection
```

- ❶ Sectionはセクションタイプを判定し、この場合はScreenになります。
- ❷ DefaultDepthは、色深度が明示的に指定されていない場合にデフォルトで使用する色深度を示します。
- ❸ 各色深度に対して、異なるDisplayサブセクションが指定されます。
- ❹ Depthは、このセットのDisplay設定とともに使用する色深度を示します。8、15、16、24、および32を指定できますが、すべてのXサーバモジュールまたは解像度がこれらの値をすべてサポートしている訳ではありません。
- ❺ Modesセクションは、可能な画面解像度のリストから成り立っています。Xサーバは、このリストを左から右に検査します。解像度ごとに、XサーバはModesセクション内で適切なModelineを検索します。Modelineは、モニタとグラフィックカード両方の機能に応じて異なります。Monitor設定により、Modelineが決まります。

最初に検出される解像度はDefault modeです。Ctrl + Alt + +(数字パッド上のキー)を使用すると、リスト内で右隣の解像度に切り替えることが

できます。以前の値に切り替えるには、**Ctrl+Alt+-**(数字パッド上のキー)を使用します。これにより、**X**の実行中に解像度を変更できます。

- ⑥ Depth 16が指定されているDisplayサブセクションの最終行は、仮想画面のサイズを指します。仮想画面の最大許容サイズは、モニタの最大解像度ではなく、グラフィックカードにインストールされているメモリの容量と必要なカラー設定に応じて異なります。この行を省略すると、仮想解像度は物理解像度と同じになります。最近のグラフィックカードはビデオメモリ容量が大きくなってきているため、きわめて大型の仮想デスクトップを作成できます。ただし、ビデオメモリのほとんどが仮想デスクトップを占めると、3D機能を使用できなくなる場合があります。たとえば、カードのビデオRAMが16MBであれば、仮想画面には8ビットカラー深度で最大4096x4096ピクセルのサイズを設定できます。ただし、特にアクセラレータカードの場合は、仮想画面にメモリすべてを使用しないことをお勧めします。この種のカードのメモリは、複数のフォントやグラフィックキャッシュにも使用されるからです。
- ⑦ Identifier行(ここではScreen[0])では、このセクションに以降のServerLayoutセクションで一意に参照できる定義済みの名前を割り当てています。Device行とMonitor行では、この定義に属しているグラフィックカードとモニタを指定しています。これらは、対応する名前または識別子を持つDeviceおよびMonitorセクションにリンクされます。これらのセクションの詳細については、以下を参照してください。

26.1.2 Deviceセクション

Deviceセクションでは、特定のグラフィックカードを記述します。名前が異なっていれば、キーワードIdentifierを使用してxorg.conf内で必要な数だけデバイスエントリを指定できます。複数のグラフィックカードをインストールしている場合、セクションには順番に番号が付けられます。最初のセクションはDevice[0]、2番目のセクションはDevice[[1]]となります。次のファイルは、Matrox Millennium PCIグラフィックカードが搭載されているコンピュータのDeviceセクションから抜粋したものです(SaX2が設定)。

```

Section "Device"
    BoardName      "MGA2064W"
    BusID          "0:19:0"❶
    Driver         "mga"❷
    Identifier     "Device[0]"
    VendorName     "Matrox"
    Option         "sw_cursor"
EndSection

```

- ❶ BusIDは、グラフィックカードがインストールされているPCIスロットまたはAGPスロットの定義です。これは、`lspci`コマンドで表示されるIDと一致します。Xサーバは10進形式による詳細を必要としますが、`lspci`ではこれらが16進形式で表示されます。BusIDの値は、**SaX2**が自動検出します。
- ❷ Driverの値は**SaX2**が自動的に検出し、グラフィックカードで使用するドライバを指定します。カードが**Matrox Millennium**である場合は、ドライバモジュールはmgaと呼ばれます。Xサーバは、driversサブディレクトリのFilesセクションで定義されているModulePathを検索します。標準のインストールでは、`/usr/X11R6/lib/modules/drivers`または`/usr/X11R6/lib64/modules/drivers`ディレクトリになります。名前には`_drv.o`が追加されるので、mgaドライバの場合は、ドライバファイル`mga_drv.o`がロードされます。

Xサーバやドライバの動作は、その他のオプションを使用して変更することもできます。その一例がDeviceセクションで設定するオプション`sw_cursor`です。このオプションは、ハードウェアのマウスカーソルを無効にし、ソフトウェアを使用してマウスカーソルを示します。ドライバモジュールによっては、さまざまなオプションを使用できます。各オプションは、ディレクトリ`/usr/share/doc/package_name`内のドライバモジュール記述ファイル内にあります。通常、有効なオプションについてはマニュアルページ(`man xorg.conf`、`man X.Org`、および`man 4chips`)でも確認できます。

グラフィックカードに複数のビデオコネクタがある場合、この1枚のカードの異なるデバイスを単一ビューとして設定できます。**SaX2**を使用してグラフィックインタフェースをこのように設定します。

26.1.3 MonitorセクションとModesセクション

Deviceセクションと同様に、MonitorセクションとModesセクションでもモニタを1つずつ記述します。設定ファイル/etc/X11/xorg.confでは、Monitorセクションを必要な数だけ指定できます。Monitorセクションはそれぞれ、UseModes行があるModesセクションを参照します。MonitorセクションにModesセクションがない場合、Xサーバは該当する値を一般的な同期の値から計算します。サーバレイアウトセクションでは、どのMonitorセクションが関係するかを指定します。

熟練者以外は、モニタ定義を設定しないでください。**modeline**は、Monitorセクションで重要な役割を果たします。**modeline**では、関連解像度の水平と垂直のタイミングを設定します。モニタ特性、特に許容周波数は、Monitorセクションに格納されます。

警告

モニタおよびグラフィックカード機能の詳細な知識がない場合は、**modeline**を変更しないでください。モニタに重大な損傷が生じることがあります。

モニタ記述を開発する方は、/usr/X11R6/lib/X11/doc/(パッケージ xorg-x11-docをインストールする必要があります)を完全に理解していなければなりません。

modelineの手動指定が必要になることはほとんどありません。最新のマルチシンクモニタを使用している場合、許容周波数と最適解像度は、**SaX2**設定セクションで説明したように、原則としてXサーバがDDCを介してモニタから直接読み込みます。何らかの原因で直接読み込めない場合は、Xサーバに付属するVESAモードの1つを使用してください。このモードは、実際にはグラフィックカードとモニタのすべての組み合わせに機能します。

26.2 フォントのインストールと設定

SUSE Linux Enterpriseで追加のフォントをインストールするのは簡単です。フォントを、X 11フォントパスにある任意のディレクトリにコピーするだけ

です(26.2.1項「**X11コアフォント**」(538ページ)を参照)。インストールディレクトリは/etc/fonts/fonts.confに設定されているディレクトリのサブディレクトリでなければなりません(26.2.2項「**Xft**」(539ページ)を参照)。または、このファイルを/etc/fonts/suse-font-dirs.confに入れなければなりません。

以下は、/etc/fonts/suse-font-dirs.confから抜粋したものです。このファイルは/etc/fonts/fonts.confに含まれる/etc/fonts/conf.dディレクトリにリンクされているため、設定に含まれます。このディレクトリには、すべてのファイルまたは2桁の数字で始まるシンボリックリンクがfontconfigによりロードされます。この機能の詳細な説明は、/etc/fonts/conf.d/READMEを参照してください。

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/.fonts</dir>
<dir>~/.fonts/kde-override</dir>
<include ignore_missing="yes">suse-font-dirs.conf</include>
```

/etc/fonts/suse-font-dirs.confは、OpenOffice.org、Java、またはAdobe Acrobat Readerなどのアプリケーション(多くはサードパーティ製)に付属のフォントを取り込むために、自動的に生成されます。/etc/fonts/suse-font-dirs.confの一般的なエントリは次のようになります:

```
<dir>/usr/lib/ooo-2.0/share/fonts</dir>
<dir>/usr/lib/ooo-2.0/share/fonts/truetype</dir>
<dir>/usr/lib/jvm/java-1.5.0-sun-1.5.0_update10/jre/lib/fonts</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font/PPM</dir>
```

システム全体に追加フォントをインストールするには、フォントファイルを/usr/share/fonts/truetypeなどの適切なディレクトリに手動コピーしてください(rootとして)。また、この作業は、KDEコントロールセンターでKDEフォントインストーラを使用して行うこともできます。結果は同じです。

フォントを実際にコピーする代わりに、シンボリックリンクを作成することもできます。たとえば、マウントされているWindowsパーティション上にライセンスを取得しているフォントがあり、それらのフォントを使用したい場

合は、シンボリックリンクを作成します。次に、`SuSEconfig--module fonts`コマンドを実行します。

`SuSEconfig--module fonts`コマンドは、フォントを設定するスクリプト、`/usr/sbin/fonts-config`を実行します。このスクリプトの詳細については、マニュアルページ(`man fonts-config`)を参照してください。

手順は、ビットマップフォント、TrueTypeフォントとOpenTypeフォント、およびType1 (PostScript)フォントの場合と同様です。これらのタイプのフォントはすべて、任意のディレクトリにインストールできます。

X.Orgには、従来のX11 コアフォントシステムと、新たに設計されたXftおよびfontconfigシステムの2種類のまったく異なるフォントシステムが含まれています。以降のセクションでは、これらの2つのシステムについて簡単に説明します。

26.2.1 X11コアフォント

今日、X11コアフォントシステムは、ビットマップフォントだけでなく、Type1フォント、TrueTypeとOpenTypeフォントなどのスケーラブルフォントもサポートしています。スケーラブルフォントは、アンチエイリアスとサブピクセルレンダリングなしでサポートされており、多数の言語用のグリフを持つ大きいスケーラブルフォントのロードには時間がかかります。Unicodeフォントもサポートされていますが、使用すると時間がかかり、より多くのメモリが必要になります。

X11コアフォントシステムには、その他にも固有の弱点がいくつかあります。時代遅れになっており、これ以上拡張することはできません。下位互換性のために保持されていますが、可能なときはいつでも、新しいXftおよびfontconfigシステムを使用してください。

Xサーバは、操作のためにどのようなフォントが使用可能で、そのフォントがシステム内のどこにあるかを認識する必要があります。この情報は、有効なすべてのシステムフォントディレクトリへのパスを含むFontPath変数で処理されます。これらの各ディレクトリでは、ファイル`fonts.dir`にそのディレクトリ内で使用可能なフォントのリストがあります。FontPathは、起動時にXサーバにより生成されます。設定ファイル`/etc/X11/xorg.conf`の各FontPathエントリ内で、有効なファイル`fonts.dir`が検索されます。これ

らのエントリは、Filesセクションにあります。実際のFontPathを表示するには、xsetqを使用します。このパスは、xsetを使用して実行時に変更することもできます。パスを追加するには、xset+fp <path>を使用します。不要なパスを削除するには、xset-fp <path>を使用します。

Xサーバがすでにアクティブである場合、マウントされたディレクトリに新たにインストールされたフォントは、コマンドxsetfp rehashで使用可能にできます。このコマンドは、SuSEconfig--module fontsによって実行されます。コマンドxsetが実行中のXサーバにアクセスする必要がある場合、これは、SuSEconfig--module fontsが実行中のXサーバにアクセスできるシェルから起動されている場合にのみ可能です。これを実行する簡単な方法は、suとrootパスワードを入力して、ルートパーミッションを取得することです。suによってXサーバを起動したユーザのアクセス許可がrootシェルに転送されます。フォントが正しくインストールされ、X11コアフォントシステムを介して使用可能かどうか検査するには、コマンドxlsfontsを使用して、すべての使用可能なフォントのリストを表示します。

デフォルトでは、SUSE Linux EnterpriseはUTF-8ロケールを使用します。そのため、Unicodeフォントを使用するようにします(xlsfontsの出力中で iso10646-1で終了するフォント名)。使用可能なすべてのUnicodeフォントは、xlsfonts| grep iso10646-1コマンドでリストを表示できます。SUSE Linux Enterpriseで使用可能なほとんどすべてのUnicodeフォントには、少なくともヨーロッパ言語に必要なグリフが含まれています(以前はiso-8859-*としてエンコードされていました)。

26.2.2 Xft

最初から、Xftのプログラマは、アンチエイリアスを含むスケーラブルフォントが適切にサポートされるようにしています。Xftが使用された場合、フォントは、X11コアフォントシステムにおけるXサーバではなく、そのフォントを使用するアプリケーションによってレンダリングされます。このようにすると、それぞれのアプリケーションは実際のフォントファイルにアクセスでき、グリフのレンダリング方法を完全に制御できます。これが、多数の言語においてテキストを正しく表示するための基本となっています。フォントファイルに直接アクセスできることは、印刷のためにフォントを組み込んで、画面出力と同じ印刷出力を得るのに役立ちます。

SUSE Linux Enterpriseでは、2種類のデスクトップ環境KDEとGNOME、Mozilla、および他の多くのアプリケーションが、すでにXftをデフォルトで使用しています。そのため、Xftはすでに、古いX11コアフォントシステムよりも多くのアプリケーションで使用されています。

Xftは、fontconfigライブラリを使ってフォントを検索し、フォントのレンダリング方法を制御します。fontconfigのプロパティは、グローバルな設定ファイル/etc/fonts/fonts.confとユーザ固有の設定ファイル~/.fonts.confによって制御されます。これらのfontconfig設定ファイルはどちらも、以下の行で始まっていなければなりません。

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

さらに、以下の行で終わっていなければなりません。

```
</fontconfig>
```

フォントを検索するためのディレクトリを追加するには、以下のような行を付加します。

```
<dir>/usr/local/share/fonts/</dir>
```

ただし、これは通常、必要ありません。デフォルトで、ユーザ固有のディレクトリ~/.fontsは、すでに/etc/fonts/fonts.confに入っています。その結果、追加のフォントをインストールするには、それらのフォントを~/.fontsにコピーするだけです。

また、フォントの見栄えを制御する規則を導入することもできます。例えば、次のように入力して、すべてのフォントについてアンチエイリアスを無効にします。

```
<match target="font">
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>
```

あるいは次のように入力します。

```
<match target="font">
  <test name="family">
    <string>Luxi Mono</string>
    <string>Luxi Sans</string>
  </test>
```

```
<edit name="antialias" mode="assign">
<bool>false</bool>
</edit>
</match>
```

この場合、特定のフォントのアンチエイリアスが無効になります。

デフォルトで、ほとんどのアプリケーションは、フォント名のsans-serif (または等価のsans)、serif、あるいはmonospaceを使用します。これらは、実際のフォントではなく、言語設定に応じて適切なフォントに解決されるエイリアスにすぎません。

ユーザは、規則を~/.fonts.confファイルに追加して、それらのエイリアスを簡単に好みのフォントに変換できます。

```
<alias>
  <family>sans-serif</family>
  <prefer>
    <family>FreeSans</family>
  </prefer>
</alias>
<alias>
  <family>serif</family>
  <prefer>
    <family>FreeSerif</family>
  </prefer>
</alias>
<alias>
  <family>monospace</family>
  <prefer>
    <family>FreeMono</family>
  </prefer>
</alias>
```

ほとんどすべてのアプリケーションで、これらのエイリアスがデフォルトで使用されるので、システム全体が影響を受けます。そのため、個々のアプリケーションでフォント設定を変更しなくても、ほとんどどこでも好みのフォントを簡単に使用できます。

fc-listを使用して、どのフォントがインストールされており、使用可能になっているか調べます。たとえば、fc-listコマンドを実行すると、すべてのフォントのリストが表示されます。使用可能なスケーラブルフォント (:scalable=true)の内、どのフォントがHebrew (:lang=he)に必要なすべてのグリフ、それらのフォント名(family)、それらのスタイル(style)、それらの幅(weight)、およびフォントを含むファイルの名前を含んでいるか調べるには、次のコマンドを入力します。

```
fc-list ":lang=he:scalable=true" family style weight
```

上記のコマンドの出力は、以下ようになります。

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
FreeSans.ttf: FreeSans:style=Medium:weight=80
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

fc-listで調べることができる重要なパラメータ:

表 26.2 *fc-list*のパラメータ

パラメータ	意味と有効な値
family	フォントファミリの名前。たとえば、FreeSans。
foundry	フォントメーカー。たとえば、urw。
style (スタイル)	フォントスタイル。たとえば、Medium、Regular、Bold、Italic、Heavy。
lang	フォントがサポートする言語。例えば、ドイツ語にはde、日本語にはja、繁体字中国語にはzh-TW、簡体字中国語にはzh-CN。
weight	フォント幅。たとえば、通常では80、ボールドでは200。
slant	スラント。通常、なしでは0、イタリックでは100。
file	フォントを含むファイルの名前。

パラメータ	意味と有効な値
outline	アウトラインフォントではtrue、他のフォントではfalse。
scalable	スケーラブルフォントではtrue、他のフォントではfalse。
bitmap	ビットマップフォントではtrue、他のフォントではfalse。
pixelsize	ピクセル単位でのフォントサイズ。fc-listとの関連で、このオプションはビットマップフォントでのみ有効。

26.3 詳細情報

X11に関する詳細情報を入手するには、xorg-x11-docおよびhowtoenhパッケージをインストールしてください。X11開発の詳細情報は、プロジェクトのホームページ<http://www.x.org>で参照できます。

PAMを使用した認証

Linuxは、ユーザとアプリケーションを仲介するレイヤとしての認証プロセスでPAM (Pluggable Authentication Modules)を使用します。PAMモジュールはシステム単位で利用できるため、どのアプリケーションからもリクエストできます。この章では、モジュラー認証メカニズムの機能とその設定方法について説明します。

通常、システム管理者とプログラマは、システムの一部分へのアクセスを制限することや、アプリケーションの一定の機能の使用を制限することを望みます。PAMを使用しなければ、新規の認証メカニズム(LDAPやSamba、Kerberosなど)が導入されるたびにアプリケーションを調整する必要があります。ただし、このプロセスには時間がかかり、ミスが発生する可能性があります。このような難点を回避する方法の1つは、アプリケーションを認証メカニズムから分離し、認証は集中管理されるモジュールに任せることです。新しい認証方式が必要になった場合は、問題のプログラムでできるように適切なPAMモジュールを調整または記述するだけで済みます。

PAMメカニズムに依存するすべてのプログラムについて、ディレクトリ/etc/pam.d/*programname*に専用の設定ファイルがあります。これらのファイルでは、認証に使用するPAMモジュールが定義されます。また/etc/securityにはPAMモジュール用のグローバル設定ファイルがあり、これらのモジュール(pam_env.conf、pam_pwcheck.conf、pam_unix2.conf、time.confなど)の正確な動作が定義されます。PAMモジュールを使用する各アプリケーションは、実際には一連のPAM関数を呼び出し、各PAM関数は各種設定ファイルの情報を処理して、その結果を呼び出し元のアプリケーションに戻します。

27.1 PAM設定ファイルの構造

PAM設定ファイルの各行は、次のように最大4列で構成されています。

```
<Type of module> <Control flag> <Module path> <Options>
```

PAMモジュールはスタックとして処理されます。モジュールの用途はタイプごとに異なり、パスワードをチェックするモジュール、システムのアクセス元ロケーションを検証するモジュール、ユーザ固有の設定を読み込むモジュールなどがあります。PAMは、次の4タイプのモジュールを認識します。

auth

このタイプのモジュールの目的は、ユーザの信憑性をチェックすることです。従来、この確認のためにパスワードの問い合わせが行われていましたが、チップカードやバイオメトリクス(指紋や虹彩のスキャン)の助けを借りて行うこともできます。

account

このタイプのモジュールは、ユーザがリクエストしたサービスを使用するための一般許可を付与されているかどうかをチェックします。たとえば、失効したアカウントのユーザ名では誰もログインできないようにするには、この種の確認を実行する必要があります。

password

このタイプのモジュールの目的は、認証トークンを変更可能にすることです。ほとんどの場合、このトークンはパスワードです。

session

このタイプのモジュールは、ユーザセッションの管理と設定を受け持ちます。認証の前後に起動され、ログイン試行をシステムログに記録し、ユーザ固有の環境(メールアカウント、ホームディレクトリ、システム制限など)を設定します。

2列目には、起動されたモジュールの動作に影響する制御フラグが含まれています。

required

このフラグが付いているモジュールは、認証を進める前に正常に処理される必要があります。requiredフラグが付いたモジュールが失敗した後、

同じフラグが付いた他のモジュールがすべて処理されてから、ユーザが認証試行の失敗メッセージを受け取ります。

requisite

このフラグが付いているモジュールも、**required**フラグが付いている場合とほぼ同様に、正常に処理される必要があります。ただし、このフラグが付いたモジュールが失敗した場合は、ユーザに即座にフィードバックが送られ、他のモジュールは処理されません。成功すると、**required**フラグが付いているモジュールの場合とほぼ同様に、続いて他のモジュールが処理されます。**requisite**フラグは、正しい認証に不可欠な一定条件の有無を確認するための基本フィルタとして使用できます。

sufficient

このフラグが付いたモジュールが正常に処理されると、呼び出し元アプリケーションは即時に成功メッセージを受け取り、前に**required**フラグが付いたモジュールが失敗していなければ、他のモジュールは処理されません。**sufficient**フラグが付いたモジュールが失敗しても、直接的な結果は発生せず、以降のモジュールはそれぞれの順序で処理されます。

optional

このフラグが付いたモジュールが成功しても失敗しても、直接的な影響はありません。このフラグは、それ以上はアクションを実行しない、メッセージ表示(ユーザへのメール着信通知など)専用のモジュールに便利です。

include

このフラグが設定された場合、引数として指定されたファイルがこの場所に挿入されます。

モジュールがデフォルトディレクトリ `/lib/security` にあれば、そのパスを明示的に指定する必要はありません(**SUSE Linux Enterprise®**でサポートされるすべての64ビットプラットフォームの場合、このディレクトリは `/lib64/security` です)。4列目には、**debug**(デバッグの有効化)や**nullok**(空のパスワードの使用を許可)など、対応するモジュール用のオプションが表示される場合があります。

27.2 sshdのPAM設定

PAMの裏付けとなっている理論の機能を示すために、実務的な例としてsshdのPAM設定を考えてみましょう。

例 27.1 sshdのPAM設定

```
##PAM-1.0
auth      include      common-auth
auth      required      pam_nologin.so
account   include      common-account
password  include      common-password
session   include      common-session
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
#session optional      pam_resmgr.so fake_ttyname
```

アプリケーション(この場合sshd)の一般的なPAM設定には、4種類のモジュールタイプの環境設定ファイルを参照する4つのincludeステートメント common-auth、common-account、common-password、および common-sessionが含まれています。これら4つのファイルにはそれぞれのモジュールタイプ用のデフォルト設定があります。各PAMアプリケーションごとにそれぞれのモジュールを個別に呼び出す代わりとしてこれらを組み込むことで、管理者がデフォルトを変更した場合、更新されたPAM設定を自動的に取得します。これまでPAMへの変更があった場合、または新規アプリケーションをインストールした場合には、すべてのアプリケーションの全設定ファイルを手動で調整しなければなりませんでした。現在では、PAMの設定は中心となる設定ファイルで行われ、すべての変更は、各サービスのPAM設定に自動的に継承されます。

最初のincludeファイル(common-auth)はauthタイプの2つのモジュール、pam_envおよびpam_unix2を呼び出します。詳細については、[例 27.2. 「auth セクションのデフォルト設定」](#) (548 ページ)を参照してください。

例 27.2 authセクションのデフォルト設定

```
auth      required      pam_env.so
auth      required      pam_unix2.so
```

1つ目はpam_envで、ファイル/etc/security/pam_env.confをロードし、このファイルに指定されている環境変数を設定します。pam_envモジュールはログイン元を認識するため、このファイルを使用するとDISPLAY変数を

適切な値に設定できます。2つ目のpam_unix2は、ユーザのログインとパスワードを/etc/passwdおよび/etc/shadowと比較対照して確認します。

common-authで指定されたモジュールが正常に呼び出された後、pam_nologinという3番目のモジュールがファイル/etc/nologinの存在する場所を確認します。このファイルが存在する場合、root以外のユーザはログインできません。authモジュールのスタック全体が処理された後に、sshdがログインの成否に関するフィードバックを取得します。スタックの全モジュールにrequired制御フラグが付いている場合は、すべてが正常に処理されなければ、sshdには成功メッセージが送られません。モジュールが1つでも失敗すると、モジュールスタック全体が処理され、その後のみsshdに失敗が通知されます。

authタイプのすべてのモジュールが正常に処理された時点で、別のinclude文が処理されます。この例ではになります。例 27.3. 「accountセクションのデフォルト設定」 (549 ページ)common-accountには、pam_unix2モジュールだけが含まれています。pam_unix2からユーザが存在するという結果が戻されると、sshdは成功したことを通知するメッセージを受信し、モジュールの次のスタック(password)が処理されます。この処理を例 27.4. 「passwordセクションのデフォルト設定」 (549 ページ)に示します。

例 27.3 accountセクションのデフォルト設定

```
account required      pam_unix2.so
```

例 27.4 passwordセクションのデフォルト設定

```
password required    pam_pwcheck.so  nullok
password required    pam_unix2.so    nullok use_first_pass use_authtok
#password required   pam_make.so     /var/yp
```

繰り返しになりますが、sshdのPAM設定はcommon-passwordにあるpasswordモジュールのデフォルト設定を参照する1つのinclude文にのみ関係します。アプリケーションが認証トークンの変更をリクエストするたびに、これらのモジュールを正常に完了する必要があります。(制御フラグrequired)。パスワード変更や別の認証トークンについてはセキュリティチェックが必要です。これはpam_pwcheckモジュールで実現可能です。その後使用されたpam_unix2モジュールがpam_pwcheckから新旧のパスワードを引き継ぐため、ユーザが再認証する必要はありません。また、これでpam_pwcheckによるチェックを回避することもできなくなります。accountまたはauthタイプのモジュールが期限切れパスワードに関するメッセージを送るように設定されている場合は、passwordタイプのモジュールを使用する必要があります。

例 27.5 sessionセクションのデフォルト設定

```
session required      pam_limits.so
session required      pam_unix2.so
session optional      pam_umask.so
```

最終ステップとして、common-sessionに組み込まれたsessionタイプのモジュールが呼び出され、問題のユーザ用の設定に従ってセッションが設定されます。pam_unix2が再び処理されますが、このモジュール、pam_unix2.confが関連する設定ファイルにnoneオプションが指定されているため、実際の結果はありません。pam_limitsモジュールは/etc/security/limits.confファイルをロードします。このファイルでは、特定のシステムリソースの使用制限が定義されている場合があります。sessionモジュールはユーザのログアウト時に再び呼び出されます。

27.3 PAMモジュールの設定

PAMモジュールの一部は設定可能です。対応する設定ファイルは/etc/securityにあります。この項では、sshdの例(pam_unix2.conf、pam_env.conf、pam_pwcheck.confおよびlimits.conf)について簡単に説明します。

27.3.1 pam_unix2.conf

従来のパスワードベースの認証方式は、PAMモジュールpam_unix2によって制御されます。このモジュールは、必要なデータを/etc/passwd、/etc/shadow、NISマップ、NIS+テーブル、またはLDAPデータベースから読み込むことができます。このモジュールの動作は、アプリケーション自体のPAMオプションを設定して個別に変更するか、/etc/security/pam_unix2.confを編集してグローバルに変更できます。例 27.6. 「pam_unix2.conf」(550 ページ)に、このモジュールの最も基本的な設定ファイルを示します。

例 27.6 pam_unix2.conf

```
auth:    nullok
account:
password:    nullok
session:    none
```

authおよびpasswordモジュールタイプのnullokオプションは、対応するタイプのアカウントに空のパスワードを許可するように指定します。また、ユーザは自分のアカウントのパスワード変更を許可されます。sessionモジュールタイプのnoneオプションは、代わりにメッセージが記録されないように指定します(デフォルト)。その他の設定オプションの詳細については、ファイル自体のコメントまたはpam_unix2のマニュアルページを参照してください。

27.3.2 pam_env.conf

このファイルを使用すると、pam_envモジュールが呼び出されるたびに設定される、ユーザ用に標準化された環境を定義できます。それにより、次の構文を使用して環境変数を事前設定できます。

```
VARIABLE [DEFAULT=[value]] [OVERRIDE=[value]]
```

VARIABLE

設定する環境変数の名前です。

[DEFAULT=[value]]

管理者が設定するデフォルト値です。

[OVERRIDE=[value]]

問い合わせ可能でpam_envによって設定される値です。この値でデフォルト値が上書きされます。

pam_envの典型的な使用例は、DISPLAY変数の取得です。これは、リモートログインが行われるたびに変更されます。これを例 27.7. 「pam_env.conf」(551 ページ)に示します。

例 27.7 pam_env.conf

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY          DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

1行目では、REMOTEHOST変数の値がlocalhostに設定されており、pam_envが他の値を判別できない場合にこの値が使用されます。DISPLAY変数には、REMOTEHOSTの値が含まれています。ファイル/etc/security/pam_env.confでより詳細な情報を参照してください。

27.3.3 pam_pwcheck.conf

この設定ファイルから、pam_pwcheckモジュールがpasswordタイプの全モジュールのオプションを読み込みます。このファイルに格納されている設定は、個々のアプリケーションのPAM設定よりも優先されます。アプリケーション固有の設定が定義されていない場合、アプリケーションではグローバル設定が使用されます。例 27.8. 「pam_pwcheck.conf」 (552 ページ) はpam_pwcheckに対して空のパスワードとパスワード変更を許可するように指示しています。このモジュールの他のオプションについては、ファイル/etc/security/pam_pwcheck.confを参照してください。

例 27.8 pam_pwcheck.conf

```
password: nullok
```

27.3.4 limits.conf

ファイルlimits.confでは、ユーザ別またはグループ別のシステム制限を設定できます。このファイルは、pam_limitsモジュールに読み込まれます。このファイルを使用すると、絶対に超過できない厳密な制限と、一時的な超過が許される緩やかな制限を設定できます。構文および使用可能なオプションの詳細については、ファイルに含まれているコメントを参照してください。

27.4 詳細情報

インストール済みシステムのディレクトリ/usr/share/doc/packages/pamには、次のドキュメントが用意されています。

READMEs

このディレクトリの最上位レベルには、一般的なREADMEファイルがいくつか入っています。サブディレクトリmodulesには、使用可能なPAMモジュールのREADMEファイルがあります。

『Linux-PAM System Administrators' Guide』

このマニュアルには、システム管理者を対象としたPAMに関する必須情報がすべて含まれています。設定ファイルの構文からPAMのセキュリティ

面に至るまで、広範囲な項目を説明しています。このマニュアルは、PDFファイル、HTML形式およびプレーンテキストで提供されます。

『Linux-PAM Module Writers' Manual』

このマニュアルには、開発者を対象として標準準拠のPAMモジュールを記述する方法の概要が記載されています。このマニュアルは、PDFファイル、HTML形式およびプレーンテキストで提供されます。

『The Linux-PAM Application Developers' Guide』

このマニュアルには、PAMライブラリを使用するアプリケーション開発者に必要な情報がすべて含まれています。このマニュアルは、PDFファイル、HTML形式およびプレーンテキストで提供されます。

Thorsten KukukはPAMモジュールを多数開発しており、その一部の情報は<http://www.suse.de/~kukuk/pam/>で公開されています。

電源管理

電源管理はラップトップコンピュータで特に重要ですが、他のシステムでも役に立ちます。APM (Advanced Power Management) と ACPI (Advanced Configuration and Power Interface) という、2つのテクノロジーが利用可能です。これらに加えて、電源の節約や騒音の低減のために、CPU周波数を制御することもできます。これらのオプションは手動で、または専用のYaSTモジュールを使って設定することができます。

► **zseries:** この章で説明する機能とハードウェアは、IBM System zには存在しないため、この章はこれらのプラットフォームには無関係です。 ◀

電源管理はラップトップコンピュータで特に重要ですが、他のシステムでも役に立ちます。ACPI(Advanced Configuration and Power Interface)は現在のすべてのコンピュータ(ラップトップ、デスクトップ、サーバ)で使用できます。電源管理テクノロジーでは、適切なハードウェアとBIOSルーチンを必要とします。ほとんどのラップトップと多くの新型デスクトップおよびサーバは、これらの必要条件を満たしています。電源の節約や騒音の低減のために、CPU周波数を制御することもできます。

APMは、従来型のコンピュータで多く使われてきました。APMは、ほとんどがBIOSに実装された関数セットからなるため、APMサポートのレベルはハードウェアによって異なります。より複雑なACPIでは、この傾向がさらに強まります。このため、どちらか片方を推奨することは無理です。さまざまな手順をハードウェア上でテストし、最も適切なサポートが実現できるテクノロジーを選択してください。

28.1 省電力機能

省電力機能はラップトップをモバイル使用する場合に限らず、デスクトップシステムでも重要です。APMおよびACPI電源管理システムの主要な機能と、その使用目的は、以下のとおりです。

スタンバイ

この動作モードは、ディスプレイの電源をオフにします。プロセッサのパフォーマンスを低下させるコンピュータも一部あります。この機能は、ACPI状態S1またはS2に対応します。

サスペンド(メモリに保存)

このモードでは、システム状態をすべてRAMに書き込みます。その後、RAMを除くシステム全体がスリープします。この状態では、コンピュータの消費電力が非常に小さくなります。この状態の利点は、ブートやアプリケーションの再起動をせずに、数秒でスリープ前の作業をスリープの時点から再開できることです。この機能はACPI状態S3に対応します。この状態のサポートはまだ開発中なので、ハードウェアに大幅に依存します。

ハイバーネーション(ディスクに保存)

この動作モードでは、システム状態がすべてハードディスクに書き込まれ、システムの電源がオフになります。すべてのアクティブデータを書き込むには、少なくともRAMの大きさのスワップパーティションが必要です。この状態から再開するには、30～90秒かかります。サスペンド前の状態が復元されます。メーカーの中には、このモードを便利なハイブリッド仕様にして提供するものもあります(たとえば、IBM ThinkpadのRediSafe)。対応するACPI状態は、S4です。Linux環境では、suspend to diskはAPMおよびACPIから独立したカーネルルーチンにより実行されます。

バッテリーモニタ

ACPIとAPMは、バッテリーをチェックして、充電ステータスに関する情報を提供します。また、どちらのシステムも、重要な充電ステータスに達した時点で実行するようにアクションを調整します。

自動電源オフ

シャットダウンの後、コンピュータの電源が切れます。これは、バッテリーが空になる直前に自動シャットダウンが行われる場合に特に重要です。

システムコンポーネントのシャットダウン

システム全体を考えた場合、電力消費量を抑えるという点では、ハードディスクをオフにすることが最も重要です。システム全体の信頼性に応じて、しばらくハードディスクをスリープ状態にすることは可能です。ただし、スリープ時間が長くなれば、データ損失のリスクも高くなります。特別な省電力モードになるPCIデバイスなど、他のコンポーネントは、ACPIにより無効にしたり(少なくとも理論的には)、BIOSセットアップで永久的に無効に設定したりできます。

プロセッサ速度の制御

CPUに関して、エネルギーを節約するには3種類の方法があります。周波数と電圧のスケーリング(PowerNow!またはSpeedstepとしても知られています)、スロットル、およびプロセッサのスリープ状態(Cステート)への移行の3種類です。コンピュータの動作モードによっては、この3つの方法を併用することもできます。

28.2 APM

省電力機能の中には、APM BIOS自体によって実行される機能もあります。多くのラップトップにおいて、スタンバイ状態とサスペンド状態は、特別なオペレーティングシステムの機能を使用するのではなく、キーの組み合わせによって、またはふたを閉じることによって有効になります。しかし、コマンドを使用してこれらのモードを有効にするには、システムがサスペンドする前に、特定のアクションがトリガされなければなりません。さらに、バッテリーの充電レベルを表示するには、特殊なプログラムパッケージと適切なカーネルが必要になります。

SUSE Linux Enterpriseのカーネルでは、ビルトインのAPMをサポートしています。しかし、APMが有効になるのは、ACPIがBIOSに実装されておらず、APM BIOSが検出された場合に限られます。APMサポートを有効にするには、ブートプロンプトで`acpi=off`を実行してACPIを無効にする必要があります。APMが有効かどうかを確認するには、`cat /proc/apm`を入力します。ここでさまざまな値が出力されれば、すべて正常であることを意味します。ここで、コマンド`shutdown -h`を実行して、コンピュータをシャットダウンします。

BIOS実装が規格に完全に準拠していないと、APMに問題が発生することがあります。一部の問題は、特殊なブートパラメータで回避できます。すべての

パラメータは、ブートプロンプトで、`apm=parameter`の形式で入力します。
`parameter`は、以下のいずれかの値になります。

`on`または`off`

APMサポートの有効化または無効化。

`(no-)allow-ints`

BIOS機能の実行中の中断を許可します。

`(no-)broken-psr`

BIOSの「GetPowerStatus」機能が正しく動作しません。

`(no-)realmode-power-off`

シャットダウンの前にプロセッサをリアルモードにリセットします。

`(no-)debug`

APMイベントをシステムログに記録します。

`(no-)realmode-power-off`

シャットダウンの後、システムの電源を切断します。

`bounce-interval=n`

サスペンドイベントの後、別のサスペンドイベントが無視される確率を
1/100秒単位で表した数値です。

`idle-threshold=n`

システムのアイドル状態がこの値に達するとBIOSのidle関数が実行されます(0=常時、100=実行しない)。

`idle-period=n`

システムアクティビティを測定した後の時間を1/100秒単位で表した数値。

APMデーモン(`apmd`)は廃止になりました。代わりに、新しい`powersaved`で処理されるようになりました。`powersaved`は、ACPIをサポートし、他の多くの機能を提供します。

28.3 ACPI

ACPI (advanced configuration and power interface)は、オペレーティングシステムが個々のハードウェアコンポーネントをセットアップ、および制御できるように設計されています。ACPIは、PnPとAPMの両方の後継となります。また、ACPIはバッテリー、ACアダプタ、温度、ファン、および「close lid」や「battery low」などのシステムイベントに関する情報も提供します。

BIOSには個々のコンポーネントとハードウェアアクセス方法についての情報が入ったテーブルがあります。オペレーティングシステムは、この情報を使用して、割り込みまたはコンポーネントの有効化と無効化などのタスクを実行します。BIOSに格納されているコマンドを、オペレーティングシステムが実行するとき、機能はBIOSの実装方法に依存します。ACPIが検出可能で、ロードできるテーブルは、`/var/log/boot.msg`にレポートされます。ACPIに生じた問題のトラブルシューティングについては、[28.3.4頁「トラブルシューティング」](#) (565 ページ)を参照してください。

28.3.1 動作中のACPI

システムのブート時に、カーネルがACPI BIOSを検出する場合、ACPIが自動的に有効になります。旧式のコンピュータでは、ブートパラメータ`acpi=on`を指定しなければならない場合があります。コンピュータは、ACPI 2.0以降をサポートする必要があります。`/var/log/boot.msg`のカーネルブートメッセージで、ACPIが有効にされていることを確認します。

続いて、複数のモジュールがロードされます。これは、`acpid`の起動スクリプトによって行われます。これらのモジュールのいずれかが問題になる場合、`/etc/sysconfig/powersave/common`から、該当するモジュールをロード/アンロードの対象から除外することができます。システムログ(`/var/log/messages`)には、モジュールに関するメッセージが記録されています。このログから、どのコンポーネントが検出されたかを確認することができます。

`/proc/acpi`には、システム状態に関する情報を提供するファイルや、状態を変更するために使用できるファイルが多数含まれています。一部の機能はまだ開発中であるため動作しません。また、一部の機能はメーカーの実装状況に大きく依存するためサポートされていない場合もあります。

すべてのファイル(dsdtおよびfadt)は、コマンドcatで読み取ることができます。一部のファイルでは、echoを使って設定を変更することができます。たとえば、Xに適切な値を指定するには、「echo X > file」と指定します。これらの値に簡単にアクセスする手段としては、powersaveコマンドがあります。このコマンドは、Powersaveデーモンのフロントエンドとして機能します。以下で最も重要なファイルについて説明します。

/proc/acpi/info

ACPIに関する一般的な情報。

/proc/acpi/alarm

システムがいつスリープ状態から回復するかを指定します。現在、この機能は完全にはサポートされていません。

/proc/acpi/sleep

さまざまなスリープ状態に関する情報を提供します。

/proc/acpi/event

すべてのイベントがここにレポートされ、Powersaveデーモン(powersaved)で処理されます。Powerボタンの押下げ、またはふたを閉じるなど、いずれのデーモンもこのファイルにアクセスしないイベントは、cat /proc/acpi/eventによって読み取ることができます(Ctrl+Cキーで終了します)。

/proc/acpi/dsdtおよび/proc/acpi/fadt

これらのファイルにはACPIテーブルのDSDT (differentiated system description table)とFADT (fixed ACPI description table)が含まれています。これらは、acpidmp、acpidisasm、およびdmdecodeで読み取ることができます。これらのプログラムとマニュアルは、pmtoolsパッケージにあります。たとえば、acpidmp DSDT | acpidisasmなどです。

/proc/acpi/ac_adapter/AC/state

ACアダプタが接続されているかを示します。

/proc/acpi/battery/BAT*/{alarm,info,state}

バッテリー状態についての詳細情報です。充電レベルを読み取るには、infoのlast full capacityとstateのremaining capacityを比較します。これをもっと円滑に行うには、[28.3.3項「ACPIツール」](#) (565 ページ)で説明する特別なプログラムの1つを使用します。バッテリーイベント

(warning、low、criticalなど)がトリガされる充電レベルは、alarmで指定できます。

/proc/acpi/info

このディレクトリには、ラップトップの蓋およびボタンなどのスイッチに関する情報が含まれています。

/proc/acpi/fan/FAN/state

ファンが現在、作動しているかを示します。ファンは、このファイルに0(オン)か3(オフ)かを書き込むことによって、オンまたはオフにできます。ただし、システムが異常に熱くなった場合は、カーネルとハードウェア(またはBIOS)の両方のACPIコードによってこの設定が上書きされます。

/proc/acpi/processor/*

システムに搭載されているCPUごとに、個別のサブディレクトリが保持されます。

/proc/acpi/processor/*/info

プロセッサの省エネオプションに関する情報。

/proc/acpi/processor/*/power

現在のプロセッサ状態に関する情報。C2の横にアスタリスクが付いている場合、プロセッサがアイドル状態です。usageに示すように、これが最もよくある状態です。

/proc/acpi/processor/*/throttling

プロセッサクロックの減速の設定に使用できます。通常、スロットリングは8つのレベルで使用できます。これは、CPUの周波数制御とは独立しています。

/proc/acpi/processor/*/limit

パフォーマンス(廃止)とスロットリングがデーモンによって自動的に制御される場合、上限をここで指定できます。制限事項の一部は、システムによって決まります。中には、ユーザによって調整できるものもあります。

/proc/acpi/thermal_zone/

すべてのサーマルゾーンに対し、個別の下位ゾーンが存在します。サーマルゾーンとは、よく似たサーマルプロパティを持ち、ハードウェアメカによって番号と名前が指定された領域です。しかし、ACPIが持つ可能性の多くは、ほとんど実装されていません。そして、温度制御は相変わらず

BIOSによって管理されています。オペレーティングシステムが介入すると、ハードウェアの寿命が短くなるので、オペレーティングシステムが介入する機会はあまりありません。したがって、一部のファイルの内容は、単なる理論上の値です。

```
/proc/acpi/thermal_zone/*/temperature
```

サーマルゾーンの現在の温度です。

```
/proc/acpi/thermal_zone/*/state
```

この状態は、すべてがokなのか、またはACPIがアクティブまたはパッシブ冷却を適用しているかを示します。ACPI独立のファン制御の場合、この状態は常にokです。

```
/proc/acpi/thermal_zone/*/cooling_mode
```

ACPIで制御される冷却化方式を選択します。パッシブ(パフォーマンスは低いが経済的)またはアクティブ(フルパフォーマンス、ファンノイズ)のどちらかを選択できます。

```
/proc/acpi/thermal_zone/*/trip_points
```

パッシブ/アクティブ冷却、サスペンション(hot)、またはシャットダウン(critical)など、特定のアクションをトリガする温度を設定します。可能なアクションは、**DSDT**(デバイス依存)内で定義されます。ACPI仕様で定義されているトリップポイントは、critical、hot、passive、active1、およびactive2です。実装されていないトリップポイントがあっても、このファイルにはすべてを常にこの順序で入力する必要があります。たとえば、エントリecho90:0:70:0:0>trip_pointsは、criticalの温度を90、passiveの温度を70に設定します(温度はすべて摂氏)。

```
/proc/acpi/thermal_zone/*/polling_frequency
```

温度が変化してもtemperatureの値が自動的に更新されない場合は、ポーリングモードをここでオンにします。コマンドechoX > /proc/acpi/thermal_zone/*/polling_frequencyを使用すると、X 秒ごとに温度の問い合わせが行われます。ポーリングを無効にするには、X=0に設定します。

これらの設定、情報、イベントは、いずれも手動で編集する必要はありません。編集はPowersaveデーモン(powersaved)および各種フロントエンド

(powersave、kpowersave、wmpowersaveなど)で実行できます。詳細については、[28.3.3項「ACPIツール」](#) (565 ページ)を参照してください。

28.3.2 CPUパフォーマンスの制御

CPUには、3つの省電力方法があります。コンピュータの動作モードによっては、この3つの方法を併用することもできます。また、省電力とは、システムの温度上昇が少なく、ファンが頻繁にアクティブにならないことを意味します。

周波数と電圧の調節

PowerNow!とSpeedstepは、AMD社とIntel社が使用するこのテクノロジーの名称です。ただし、このテクノロジーは他のメーカーのプロセッサにも適用されます。CPUのクロック周波数とそのコア電圧が同時に低下し、段階的な省エネよりも大きな効果が得られます。つまり、周波数が半分になると(半分のパフォーマンス)、消費電力も半分以下になります。このテクノロジーは、APMまたはACPIには依存していません。CPU周波数制御には、カーネル自体か、またはユーザスペースアプリケーションを使用した2つのアプローチがあります。従って、`/sys/devices/system/cpu/cpu*/cpufreq/`で設定できる各種カーネルガバナがあります。

ユーザスペースガバナ

ユーザスペースガバナが設定されている場合、カーネルは、通常、デーモンなどのユーザスペースアプリケーションにCPU周波数制御を譲渡します。SUSE Linux Enterpriseでは、このデーモンはpowersavedパッケージにあります。この実装が使用されるとき、CPU周波数は現在のシステム負荷に応じて調整されます。デフォルトでは、カーネル実装の1つが使用されます。ただし、一部のハードウェア、特定のプロセッサまたはドライバによっては、ユーザスペースの実装が唯一の対策となっています。

オンデマンドガバナ

これは、動的CPU周波数ポリシーのカーネル実装で、ほとんどのシステムで使用できます。システムの負荷が高くなるとすぐに、CPU周波数が直ちに上がります。システム負荷が低い場合は、周波数が下がります。

保守的ガバナ

このガバナは、より保守的なポリシーが使用される以外は、オンデマンド実装と類似しています。CPU周波数が上がる前に、一定の時間、システムの負荷が高くなっている必要があります。

省電力ガバナ

CPU周波数を一定にできるだけ低く設定します。

パフォーマンスガバナ

CPU周波数を一定にできるだけ高く設定します。

クロック周波数のスロットリング(速度を抑える)

このテクノロジーでは、CPUのクロック信号インパルスが一定割合だけ省略されます。25%のスロットリングでは、4回に1回の割合でインパルスが省略されます。87.5%では、プロセッサにインパルスが届くのは8回に1回だけになります。ただし、省エネ度が減速の割合に比例して増えることはありません。通常、スロットリングが使用されるのは、周波数調節を使用できない場合、または省電力を最大限に使用する場合だけです。このテクノロジーも、特殊なプロセスで制御する必要があります。システムインタフェースは、`/proc/acpi/processor/*/throttling`です。

プロセッサのスリープ状態への切り替え

オペレーティングシステムは、何も実行することがない場合にプロセッサをスリープ状態にします。この場合、オペレーティングシステムはCPUにhaltコマンドを送ります。C1、C2、およびC3の、3つのオプションがあります。最も経済的な状態C3では、プロセッサキャッシュとメインメモリとの同期も停止します。そのため、この状態を適用できるのは、バスマスタアクティビティを介してメインメモリの内容を変更している他のデバイスが存在しない場合だけです。一部のドライバでは、C3を使用できません。現在の状態は、`/proc/acpi/processor/*/power`に表示されます。

周波数調節とスロットリングが関係するのは、プロセッサがビジー状態の場合だけです。これは、プロセッサがアイドル状態のときには、最も経済的なC状態が常に適用されるためです。CPUがビジー状態の場合、省電力方式として周波数調節を使用することをお勧めします。通常、プロセッサは部分的な負荷でのみ動作します。この場合は、低周波数で実行できます。一般に、カーネルのオンデマンドガバナまたはpowersavedのようなデーモンで制御される動的な周波数調節が最善の方法といえます。低周波数をスタティックに設定す

る方法は、バッテリー使用時やコンピュータを冷却または静止させたい場合に役立ちます。

スロットリングは、システムが高負荷であるにもかかわらずバッテリー使用時間を延長する場合など、最後の手段として使用する必要があります。ただし、スロットリングの割合が高すぎると、スムーズに動作しないシステムがあります。さらに、CPUの負荷が小さければ、CPUスロットリングは無意味です。

SUSE Linux Enterpriseでは、これらのテクノロジーはpowersaveデーモンで制御されます。この設定については、[28.5項「powersaveパッケージ」](#) (569 ページ)を参照してください。

28.3.3 ACPIツール

総合的に呼べるACPIユーティリティには、バッテリー充電レベルや温度などの情報を表示するだけのツール(acpi、klaptopdaemon、wmacpimonなど)、/proc/acpi内の構造へのアクセスを容易にするツール、変化の監視を補助するツール(akpi、acpiw、gtkacpiw)、BIOS内のACPIテーブルを編集するためのツール(パッケージ pmtools)などが含まれています。

28.3.4 トラブルシューティング

問題を2つに大別できます。1つはカーネルのACPIコードに、未検出のバグが存在する可能性があることです。この場合は、いずれ修正プログラムがダウンロードできるようになります。ただし、問題の多くはBIOSが原因になっています。また、場合によっては、他の広く普及しているオペレーティングシステムにACPIを実装した場合にエラーが起きないように、BIOSにおけるACPIの指定を故意に変えていることがあります。ACPIに実装すると重大なエラーを生じるハードウェアコンポーネントは、ブラックリストに記録され、これらのコンポーネントに対してLinuxカーネルがACPIを使用しないようにします。

問題に遭遇したときに最初に実行することは、BIOSの更新です。コンピュータがまったくブートしない場合、次のブートパラメータは有用です。

```
pci=noacpi
```

PCIデバイスの設定にACPIを使用しません。

`acpi=ht`

単純なリソース設定のみを実行します。ACPIを他の目的には使用しません。

`acpi=off`

ACPIを無効にします。

警告: ACPIなしに起動できない場合

一部の新型のコンピュータは(特に、SMPシステムとAMD64システム)、ハードウェアを正しく設定するためにACPIが必要です。これらのコンピュータでACPIを無効にすると、問題が生じます。

システムのブートメッセージを調べてみましょう。そのためには、ブート後にコマンド `dmesg | grep -2i acpi` を使用します(または、問題の原因がACPIだとは限らないので、すべてのメッセージを調べます)。ACPIテーブルの解析時にエラーが発生した場合、重要なDSDTテーブルを改善版と置換することができます。この場合、BIOSで障害のあるDSDTが無視されます。具体的な手順については28.5.4項「トラブルシューティング」(576 ページ)を参照してください。

カーネルの設定には、ACPIデバッグメッセージを有効にするスイッチがあります。ACPIデバッグを有効にした状態でカーネルをコンパイルし、インストールすると、詳細な情報を表示するエラーのエクスポート検索がサポートできるようになります。

BIOSまたはハードウェアに問題がある場合は、常にメーカーに連絡することをお勧めします。特に、Linuxに関するサポートを常に提供していないメーカーには、問題を通知する必要があります。なぜなら、メーカーは、自社の顧客の無視できない数がLinuxを使用しているとわかってやっと、問題を真剣に受け止めるからです。

詳細情報

ACPIに関する補足資料とヘルプ

- <http://www.cpqlinux.com/acpi-howto.html> (詳細なACPIHOWTO、DSDTパッチが含まれています)
- <http://www.intel.com/technology/iapc/acpi/faq.htm> (IntelのACPIに関するFAQ)
- <http://acpi.sourceforge.net/> (SourceforgeによるACPI4Linuxプロジェクト)
- <http://www.poupinou.org/acpi/> (Bruno DucrotによるDSDTパッチ)

28.4 ハードディスクの休止

Linux環境では、不要な場合にハードディスクを完全にスリープ状態にしたり、より経済的な静止モードで動作させることができます。最近のラップトップの場合、ハードディスクを手動でオフに切り替える必要はありません。不要な場合は自動的に経済的な動作モードになります。ただし、省電力レベルを最大限にする場合は、次の方法をいくつかテストしてください。機能のほとんどは、**powersaved**および**YaST電源管理モジュール**でコントロールできます。その詳細については、**28.6項「YaST電源管理モジュール」** (578 ページ)を参照してください。

hdparmアプリケーションを使用して、各種のハードディスク設定を変更できます。**-y**オプションは、簡単にハードディスクをスタンバイモードに切り替えます。**-y**を指定すると、スリープ状態になります。**hdparm -S x**を使用すると、一定時間アクティビティがなければハードディスクが回転を停止します。**x**は、次のように置換します:**0**を指定するとこの機構が無効になり、ハードディスクは常時稼働します。**1**から**240**までの値を指定すると、指定した値**x** 5秒が設定値になります。**241**から**251**は、**30分**の**1倍**から**11倍**(**30分**から**5.5時間**)に相当します。

ハードディスクの内部省電力オプションは、オプション**-B**で制御できます。**0** (最大限の省電力)～**255** (最大限のスループット)の値を選択します。結果は使用するハードディスクに応じて異なり、査定するのは困難です。ハードディ

スクを静止状態に近づけるにはオプション-Mを使用します。128(静止)~254(高速)の値を選択します。

ハードディスクをスリープにするのは、多くの場合簡単ではありません。Linuxでは、多数のプロセスがハードディスクに書き込むので、ウェイクアップが常に繰り返されています。したがって、ハードディスクに書き込むデータを、Linuxがどのように処理するかを理解することは重要です。はじめに、すべてのデータがRAMにバッファされます。このバッファは、カーネル更新デーモン(kupdated)によって監視されます。データが一定の寿命に達するか、バッファがある程度一杯になると、バッファの内容がハードディスクにフラッシュされます。バッファサイズはダイナミックであり、メモリサイズとシステム負荷に対応して変化します。デフォルトでは、kupdatedの間隔が短く設定されて、完全性を最大まで高めます。バッファが5秒毎にチェックされ、データが30秒以上経過していたり、バッファの使用レベルが30%に達すると、bdflushデーモンに通知されます。bdflushデーモンが、データをハードディスクに書き込みます。このデーモンはまた、たとえば、バッファが一杯のときに、kupdatedと無関係に書き込みます。

警告: データの完全性に関する障害

カーネル更新デーモンの設定を変更すると、データの完全性が損なわれる可能性があります。

これらのプロセスとは別に、ReiserFSやExt3などのジャーナリングファイルシステムは、それらが持つメタデータをbdflushとは無関係に書き込むので、ハードディスクが回転を停止しなくなります。モバイル機器では、これを避けるために特別なカーネル拡張が開発されています。詳細については、`/usr/src/linux/Documentation/laptop-mode.txt`を参照してください。

もう1つの重要な要因は、アクティブプログラムが動作する方法です。たとえば、優れたエディタは、変更中のファイルを定期的にハードディスクに自動バックアップし、これによってディスクがウェイクアップされます。データの完全性を犠牲にすれば、このような機能を無効にできます。

この接続では、メールデーモンpostfixが変数POSTFIX_LAPTOPを使用します。この変数をyesに設定すると、postfixがハードディスクにアクセスする頻度は大幅に減少します。しかしながら、kupdatedの間隔が広くなると、このことは重要でなくなります。

28.5 powersaveパッケージ

powersaveパッケージには、省電力機能がすべて含まれています。一般に省電力に関する要望が高まっているため、サスペンド、スタンバイまたはCPU周波数調節など、いくつかの機能がワークステーションとサーバで重要です。

このパッケージにはご使用のコンピュータの電源管理機能がすべて含まれます。電源管理機能はACPI、APM、IDEハードディスク、PowerNow!またはSpeedStepテクノロジーを使用してハードウェアをサポートします。apmd、acpid、ospm、cpufreqd(現在はcpuspeed)などの各パッケージの機能がpowersaveパッケージに統合されています。acpiイベントとして機能するacpid以外、これらのパッケージのデーモンは省電力デーモンと同時に実行しないでください。

ご使用のシステムに前述のハードウェア要素の一部が含まれていないとしても、省電力機能の制御にはpowersaveデーモンを使用してください。ACPIおよびAPMは相互排他的であるため、ご使用のシステムではこれらのシステムのどちらか一方しか使用できません。このデーモンはハードウェア構成に変更があった場合、これを自動的に検出します。

28.5.1 powersaveパッケージの設定

powersaveの設定は複数のファイルに分散されています。ファイル内の設定オプションにはすべて、機能に関するドキュメントが含まれています。

```
/etc/sysconfig/powersave/common
```

このファイルにはpowersaveデーモンの一般的な設定が含まれます。たとえば、エラーメッセージの量(/var/log/messages内の)は、変数POWERSAVE_DEBUGの値を増加させることで増やせます。

```
/etc/sysconfig/powersave/events
```

powersaveデーモンはシステムイベントを処理するためにこのファイルが必要とします。1つのイベントには外部アクションまたはデーモン自体が実行したアクションを割り当てることができます。外部アクションの場合、デーモンは/usr/lib/powersave/scripts/にある外部ファイル(通常、Bashスクリプト)を実行しようとします。事前定義された内部アクションは次のとおりです。

- ignore
- throttle
- dethrottle
- suspend_to_disk
- suspend_to_ram
- standby
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby
- 通知
- screen_saver
- reread_cpu_capabilities

throttleは、MAX_THROTTLINGで指定された値に従ってプロセッサの速度を遅くします。この値は、現在のスキーマによって異なります。dethrottleは、プロセッサに最高のパフォーマンスを発揮させます。suspend_to_disk、suspend_to_ram、およびstandbyは、スリープモードの契機となるシステムイベントです。これら3つのアクションは一般的にスリープモードのトリガとなりますが、常に、これらを特定のシステムイベントと関連付けるようにしてください。

ディレクトリ/usr/lib/powersave/scriptsにはイベントを処理するための各種スクリプトが含まれます。

switch_vt

サスペンドやスタンバイの後に画面が戻らない場合に有用です。

wm_logout

設定を保存し、GNOME、KDE、または他のウィンドウマネージャからログアウトします。

wm_shutdown

GNOMEまたはKDEの設定を保存し、システムをシャットダウンします。

set_disk_settings

/etc/sysconfig/powersave/diskで作成されたディスク設定を実行します。

たとえば、変数

EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk"が設定されている場合、ユーザがスリープモード用のコマンドであるsuspend to diskをpowersavedに対して発行するとすぐに、2つのスクリプトまたはアクションが指定された順番で処理されます。デーモンは外部スクリプトである/usr/lib/powersave/scripts/prepare_suspend_to_diskを実行します。このスクリプトが正常に実行されると、重要なモジュールがスクリプトによりアンロードされ、各種サービスが停止された後、デーモンが内部アクションであるdo_suspend_to_diskを実行し、コンピュータをスリープモードにします。

sleepボタンのイベントを処理するアクションは

EVENT_BUTTON_SLEEP="notify suspend_to_disk"のように変更することができます。この場合、コンソールに表示されるメッセージまたはX内のポップアップウィンドウで、サスペンドについて通知されます。その結果、イベントEVENT_GLOBAL_SUSPEND2DISKが生成され、前述のアクションが実行されて、システムはサスペンドモードに入ります。内部アクションであるnotifyは/etc/sysconfig/powersave/commonにある変数NOTIFY_METHODを使用してカスタマイズできます。

/etc/sysconfig/powersave/cpufreq

動的CPU周波数設定の最適化、およびユーザスペースか、カーネル実装のいずれを使用するかを設定する変数が含まれます。

/etc/sysconfig/powersave/battery

バッテリーの制限とその他のバッテリー固有設定が含まれます。

/etc/sysconfig/powersave/sleep

このファイルでは、スリープモードを有効にし、サスペンドイベントまたはスタンバイイベントの前にアンロードすべき重要なモジュールと、停止

すべき各種サービスを指定します。システムが再開されるとこれらのモジュールは再ロードされ、各種サービスも再開されます。また、ファイルを保存するなどのために、トリガされたスリープモードを遅らせることも可能です。デフォルト設定は主にUSBおよびPCMCIAモジュールに関係しています。サスペンドまたはスタンバイの障害は通常、ある一定のモジュールによって発生します。エラーの特定の詳細については[28.5.4項「トラブルシューティング」](#) (576 ページ)を参照してください。

```
/etc/sysconfig/powersave/thermal
```

冷却コントロールおよびサーマルコントロールを有効にします。このテーマの詳細については、ファイル/usr/share/doc/packages/powersave/README.thermalを参照してください。

```
/etc/sysconfig/powersave/disk
```

この設定ファイルは、ハードディスクに関して作成されたアクションおよび設定を制御します。

```
/etc/sysconfig/powersave/scheme_*
```

これらは特定の導入シナリオに応じて消費電力を最適化するさまざまなスキーマです。多くのスキーマが事前に設定され、そのまま使用できます。また、カスタムスクリプトをここに保存することもできます。

28.5.2 APMおよびACPIの設定

サスペンドおよびスタンバイ

次に示すように、3種類の基本ACPIスリープモードおよび2種類のAPMスリープモードがあります。

サスペンド(ディスク)(ACPI S4、APMサスペンド)

メモリの内容全部をハードディスクに保存します。コンピュータは完全に電源オフの状態になり、電力は消費されません。このスリープモードは、デフォルトで有効に設定されており、すべてのシステムで機能します。

サスペンド(RAM)(ACPI S3、APMサスペンド)

デバイス全体の状態をメインメモリに保存します。メインメモリ以外からの電力消費はありません。通常SUSE Linux Enterpriseはこのスリープモー

ドをサポートしていませんが、多くのコンピュータでこれを使用することができます。

このスリープモードはデフォルトで有効になっています。ただし、現在のコンピュータがこのモードをサポート可能とデータベース中に記録されている場合にのみ実行されます。このデータベースは、/usr/sbin/s2ram バイナリにあり、suspendパッケージが提供しています。

デフォルトのパラメータを変更する場合は(たとえば、通常はsuspend to ramスリープモードを無効にしたり、データベースに記載されていないコンピュータにもモードを強制するなど)、/etc/sysconfig/powersave/sleep環境設定ファイル中の利用可能なオプションに関する情報を参照してください。

s2ramバイナリの詳細は、/usr/share/doc/packages/suspendにあるREADMEファイルを参照してください。

スタンバイ(ACPI S1、APMスタンバイ)

一部のデバイスの電源をオフにします(メーカーにより異なる)。

サスペンド、スタンバイ、再開を正しく処理するため、ファイル/etc/sysconfig/powersave/eventsで次のデフォルトオプションが設定されていることを確認してください(SUSE Linux Enterprise のインストール時のデフォルト設定)。

```
EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk screen_saver do_suspend_to_disk"
EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram screen_saver do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
    "prepare_standby screen_saver do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

バッテリー状態のカスタマイズ

ファイル/etc/sysconfig/powersave/batteryで3通りのバッテリー充電レベル(パーセント指定)を定義します。バッテリーの充電量がこれらのレベルに達

すると、システムアラートが生成されたり、特定のアクションが実行されたりします。

```
BATTERY_WARNING=12
BATTERY_LOW=7
BATTERY_CRITICAL=2
```

充電レベルが指定された制限値を下回った場合に実行されるアクションまたはスクリプトは、設定ファイル/etc/sysconfig/powersave/eventsに定義されています。各種ボタンの標準アクションは[28.5.1項「powersaveパッケージの設定」](#) (569 ページ)に示されているように変更できます。

```
EVENT_BATTERY_NORMAL="ignore"
EVENT_BATTERY_WARNING="notify"
EVENT_BATTERY_LOW="notify"
EVENT_BATTERY_CRITICAL="wm_shutdown"
```

さまざまな条件に応じた電力消費の最適化

システムの動作は電源のタイプによって調整することができます。システムがAC電源を使用せずバッテリーで稼働している場合は、システムの電力消費を抑えねばなりません。また、システムがAC電源に接続された場合はすぐ、自動的にパフォーマンスを上げる必要があります。このように、CPUの周波数、IDEの省電力機能、他のさまざまなパラメータを変更することができます。

コンピュータがAC電源に接続されている場合、またはされていない場合に実行される各種アクションは、/etc/sysconfig/powersave/eventsで定義されています。以下で/etc/sysconfig/powersave/commonで使用するスキーマを選択します。

```
AC_SCHEME="performance"
BATTERY_SCHEME="powersave"
```

各スキーマは/etc/sysconfig/powersaveにあるファイルに保存されています。ファイル名はscheme_name-of-the-schemeという形式になっています。この例は2つのスキーマscheme_performanceとscheme_powersaveを表しています。performance、powersave、presentation、およびacousticは事前設定されています。 [28.6項「YaST電源管理モジュール」](#) (578 ページ)で説明されている、YaSTの電源管理モジュールを使用して、既存

のスキーマの編集、作成、削除、別の電源状態との関連付けを行うことができます。

28.5.3 その他のACPI機能

ACPIを使用している場合、ACPIボタン(電源、スリープ、ラップトップを開く、ラップトップを閉じる)に対するシステム応答を制御することができます。/etc/sysconfig/powersave/eventsでアクションの実行を設定します。個別のオプションについての説明はこの設定ファイルを参照してください。

EVENT_BUTTON_POWER="wm_shutdown"

電源ボタンが押されると、システムは応答して該当するウィンドウマネージャ(KDE、GNOME、fvwmなど)を閉じます。

EVENT_BUTTON_SLEEP="suspend_to_disk"

スリープボタンが押されると、システムはsuspend-to-diskモードに設定されます。

EVENT_BUTTON_LID_OPEN="ignore"

ラップトップのふたが開いている状態でアクションは発生しません。

EVENT_BUTTON_LID_CLOSED="screen_saver"

ラップトップが閉じられると、スクリーンセーバが有効になります。

EVENT_OTHER="ignore"

このイベントは、デーモンで不明なイベントが起こった場合に発生します。不明なイベントには、一部のマシンにあるACPIホットキーなどがあります。

指定した時間内に、CPUの負荷が指定した制限を越えない場合、さらにCPUのパフォーマンスを低下させることも可能です。負荷制限値を

PROCESSOR_IDLE_LIMITに、タイムアウトをCPU_IDLE_TIMEOUTに指定します。CPU負荷が制限値を越えない状態が、タイムアウトで指定した時間よりも長く続いた場合には、EVENT_PROCESSOR_IDLEで設定されたイベントが有効になります。CPUが再びビジーになると、EVENT_PROCESSOR_BUSYが実行されます。

28.5.4 トラブルシューティング

すべてのエラーメッセージおよびアラートはファイル`/var/log/messages`に記録されます。必要な情報が得られない場合、ファイル`/etc/sysconfig/powersave/common`にある、`DEBUG`を使用して`powersave`に関連するメッセージの冗長度を上げます。変数の値を7または15まで増やし、デーモンを再起動します。`/var/log/messages`で利用可能なより詳しいエラーメッセージは、エラーの発見に役立ちます。以下のセクションでは`powersave`で最も頻繁に起こる問題について解説します。

ACPIはハードウェアサポートで有効になっていますが、各機能を使用できません。

ACPIで問題が発生した場合は、コマンド`dmesg | grep -i acpi`を使用し、`dmesg`の出力からACPI固有のメッセージを検索します。問題を解決するためにBIOSのアップデートが必要になる場合があります。ラップトップメーカーのホームページにアクセスし、BIOSの更新バージョンを検索してインストールします。メーカーに最新のACPI仕様に準拠していることを確認してください。BIOSの更新後もエラーが継続する場合は、以下の手順に従い、BIOS内で問題が発生しているDSDTテーブルを更新されたDSDTに置き換えます。

- 1 <http://acpi.sourceforge.net/dsdt/index.php>からシステムに適したDSDTをダウンロードします。以下に示すようにファイルを解凍し、コンパイル後ファイル拡張子が`.aml` (ACPI machine language)になっていることを確認します。拡張子が`.aml`の場合はステップ3に進みます。
- 2 ダウンロードしたテーブルのファイル拡張子が`.asl` (ACPI source language)である場合は、`iasl` (`pmtools`パッケージ)でコンパイルします。コマンド`iasl -sa file.asl`を入力してください。`iasl` (Intel ACPIコンパイラ)の最新バージョンは、<http://developer.intel.com/technology/iapc/acpi/downloads.htm>で入手できます。
- 3 ファイル`DSDT.aml`をいずれかのロケーション(`/etc/DSDT.aml`が推奨されています)にコピーします。`/etc/sysconfig/kernel`を編集し、DSDTファイルに応じてパスを変更します。`mkinitrd` (`mkinitrd`パッケージ)を開始します。カーネルをアンインストールし、`mkinitrd`を使用して`initrd`

を作成する場合は常に、変更されたDSDTが組み込まれ、システムブート時にロードされます。

CPU周波数調節が機能しません。

カーネルソース(kernel-source)を参照して、ご使用のプロセッサがサポートされているか確認してください。CPU周波数制御を有効にするには特別なカーネルモジュールまたはモジュールオプションが必要になる場合があります。この情報については/usr/src/linux/Documentation/cpu-freq/*を参照してください。特別なモジュールまたはモジュールオプションが必要な場合その設定は、ファイル/etc/sysconfig/powersave/cpufreqにある変数CPUFREQD_MODULEおよびCPUFREQD_MODULE_OPTSで行います。

サスペンドとスタンバイが機能しません。

ACPIシステムでは問題のあるDSDTを実装していることにより(BIOS)、サスペンドとスタンバイに関する問題が発生する可能性があります。そのような場合は、BIOSをアップデートしてください。

ACPIおよびAPMシステムでは、システムが不具合のあるモジュールをアンロードしようとする、システムは停止するか、またはサスペンドイベントがトリガされません。また、サスペンドに入らない原因となるモジュールをアンロードしない、またはそうしたサービスを停止しない場合、同様の状態に陥る可能性があります。どちらの場合でも、スリープモードに入らない原因となっている障害モジュールを識別してください。このモジュールの判別には/var/log/suspend2ram.logおよび/var/log/suspend2disk.logにあるpowersaveによって生成されたログファイルが非常に便利です。コンピュータがスリープモードにならない場合、その原因は最後にアンロードされたモジュールに関係しています。/etc/sysconfig/powersave/sleepにある以下の設定を変更し、サスペンドまたはスタンバイがトリガされる前に問題のあるモジュールをアンロードします。

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES=""
```

SambaやNISといったネットワーク環境の変更時、またはリモートでマウントされたファイルシステムとの接続時にサスペンドまたはスタンバイを使用する場合、オートマウンタを使用してそれらをマウントするか、それぞれのサービスを追加するようにします。たとえば、前述の変数では、`smbfs`または`nfs`などが該当します。サスペンドまたはスタンバイの前に、アプリケーションがリモートでマウントされたファイルシステムにアクセスすると、このサービスは正常に停止されません。このためファイルシステムを正常にアンマウントすることができなくなります。このようなことが原因で、システムを再開した後、ファイルシステムに障害が発生したり、再マウントが必要になったりする場合があります。

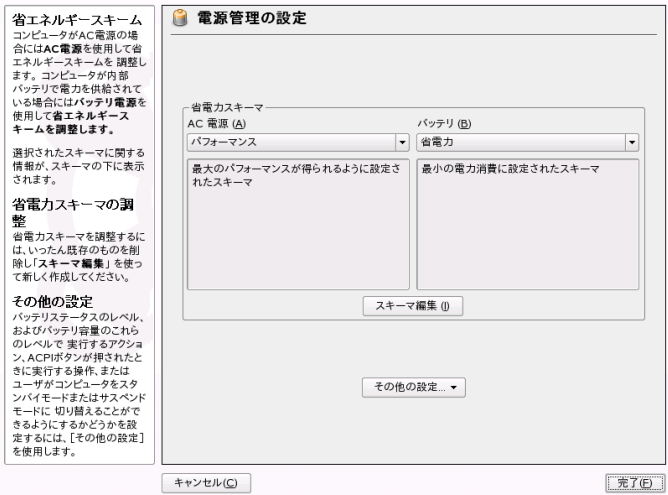
28.5.5 詳細情報

- `/usr/share/doc/packages/powersave`—ローカルのPowersaveデーモンに関するドキュメント
- <http://powersave.sourceforge.net>—最新のPowersaveデーモンに関するドキュメント
- http://www.opensuse.org/Projects_Powersave—openSUSE wiki内のプロジェクトページ

28.6 YaST電源管理モジュール

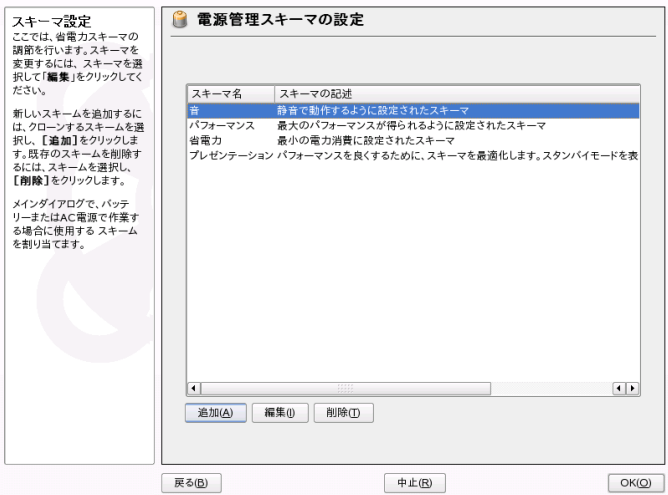
YaST電源管理モジュールではこれまで解説してきたすべての電源管理を設定できます。YaSTコントロールセンターから `[システム]` > `[電源管理]` の順に選択して、モジュールを開始すると、モジュールの最初のダイアログが開きます(「[図 28.1. 「スキーマの選択」](#) (579 ページ)」を参照してください)。

図 28.1 スキーマの選択



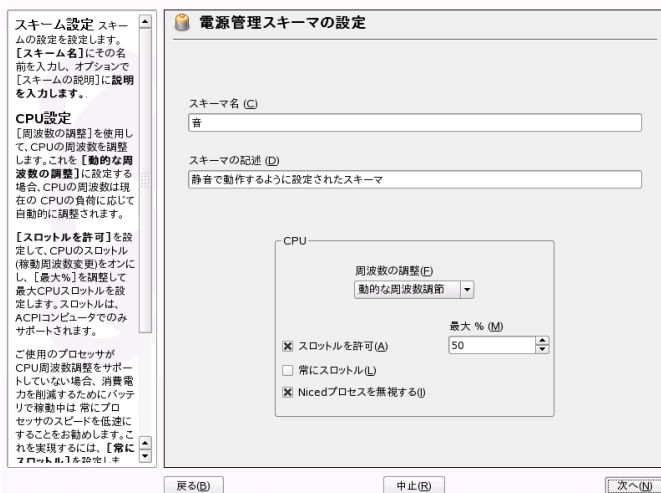
このダイアログでバッテリー使用時およびAC電源使用時に適用するスキーマを選択します。スキーマを追加、または変更するには「スキーマ編集」をクリックします。これにより、既存のスキーマの概要が表示されます。図 28.2. 「既存のスキーマの概要」 (579 ページ)を参照してください。

図 28.2 既存のスキーマの概要



スキーマの概要で変更するスキーマを選択し、[編集]をクリックします。新しいスキーマを追加するには、[追加]をクリックします。どちらを使用した場合でも、**図 28.3. 「スキーマの設定」** (580 ページ)に示す同じダイアログが表示されます。

図 28.3 スキーマの設定



はじめに、新規または編集するスキーマに適切な名前と説明を指定します。このスキーマを使用した場合、CPUパフォーマンスを制御するか、さらにどのように制御するかを決定します。また、周波数の調整およびスロットル(減速)の使用の有無、およびその使用範囲を指定します。また、CPU周波数の調整時に、優先度の低いプロセス(nicedプロセス)を無視するかどうかも指定します。続くダイアログはハードディスクの設定です。ここでは最大パフォーマンス使用時または省電力時の[スタンバイポリシー]を定義します。[音のポリシー]ではハードディスクのノイズレベルを制御します(ハードディスクによってはサポートされていません)。**[冷却ポリシー]**は使用する冷却メソッドを決定します。残念ながら、このタイプの温度制御をサポートしているBIOSはほとんどありません。

ん。/usr/share/doc/packages/powersave/powersave_manual.html#Thermalで、ファンおよびパッシブ冷却メソッドの使用方法を参照してください。

また、最初のダイアログの**[バッテリー警告]**、**[ACPIの設定]**、または**[Suspend Permissions]**を使用して、全体的な電源管理設定を行うこともできます。これらのコントロールにアクセスするには、**[Other Settings]**をクリック

クして、メニューから適切な項目を選択します。[バッテリー警告] をクリックし、**図 28.4. 「バッテリー充電レベル」** (581 ページ) に示す、バッテリー充電レベルのダイアログを開きます。

図 28.4 バッテリー充電レベル

バッテリー容量通知
3つのバッテリー容量レベルを設定し、各容量レベルにアクションを割り当てます。

[警告容量]、[低容量]、および[致命的容量]を使用して、全容量に対する割合でバッテリーレベルを設定します。

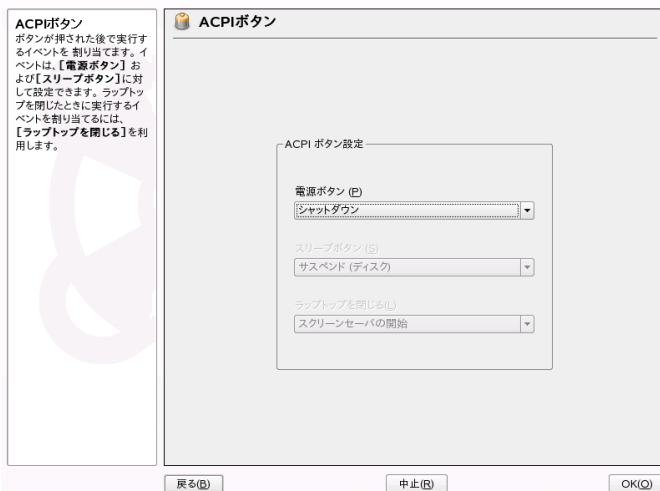
警告レベルアクション、低レベルアクション、致命的レベルアクションにおいて、それぞれのレベルに達したときに実行するアクションを設定できます。

バッテリー容量通知	
警告容量 (W)	警告レベルアクション (W)
12	通知
低容量 (L)	低レベルアクション (A)
7	通知
致命的容量 (C)	致命的レベルアクション (I)
2	シャットダウン

戻る(B) 中止(R) OK(O)

充電レベルが一定の基準値を下回った段階で、システムのBIOSはオペレーティングシステムに通知します。このダイアログでは、*[Warning Capacity]*、*[Low Capacity]*、および *[Critical Capacity]* を定義します。充電レベルがこれらの基準値を下回ると特定のアクションがトリガされます。通常、初めの2つの状態ではユーザーへの通知がトリガされるのみです。3つめの致命的なレベルではシャットダウンをトリガします。これは残りの電力ではシステムのオペレーションを維持することが困難であるためです。適切な充電レベルとそれに応じて実行するアクションを選択し、*[了解]* をクリックして開始ダイアログに戻ります。

図 28.5 ACPIの設定



「**ACPIの設定**」を使用してACPIボタンを設定するダイアログを開きます。このツールを「**図 28.5. 「ACPIの設定**」 (582 ページ)」に示します。ACPIボタンの設定は特定のスイッチに対するシステムの応答を決定します。電源ボタンが押された場合、スリープボタンが押された場合、ラップトップが閉じられた場合のそれぞれに応じて、システムがどのように応答するかを設定します。

「**了解**」をクリックして設定を終了し、開始ダイアログに戻ります。

「**サスペンドを有効化**」ダイアログを開きます。このダイアログではこのシステムのユーザがサスペンドまたはスタンバイ機能を使用できるか、さらにそれらをどのように使用するかを決定します。「**了解**」をクリックしてメインダイアログに戻ります。「**了解**」を再度クリックしてモジュールを終了し、電源管理設定を確認してください。

無線通信

無線LANを使用して、SUSE Linux Enterprise®コンピュータ間の接続を確立できます。この章では、無線ネットワークの原理と、無線ネットワークの基本的な設定方法について説明します。

29.1 無線LAN

無線LANは、モバイルコンピューティングに不可欠な側面となってきています。現在、ほとんどのラップトップにはWLANカードが内蔵されています。WLANカードによる無線通信に関する802.11規格がIEEEにより策定されました。当初、この規格は最大伝送速度2MBit/sについて提供されましたが、その後、データ伝送速度を高めるために複数の補足事項が追加されています。これらの補足事項では、モジュレーション、伝送出力、および伝送速度などの詳細が定義されています。

表 29.1 各種WLAN規格の概要

名前	帯域(GHz)	最大伝送速度 (MBit/s)	メモ
802.11	2.4	2	廃止、実質上、使用可能な エンドデバイスはなし
802.11b	2.4	11	普及
802.11a	5	54	あまり普及せず
28.29oz	2.4	54	11bとの下位互換性あり

また、最大伝送速度 22MBit/s の Texas Instruments の 802.11b バージョン (802.11b+) のような独自規格もあります。ただし、この規格を使用するカードは一般的ではありません。

29.1.1 ハードウェア

802.11 カードは、SUSE Linux Enterprise® ではサポートされていません。802.11a、802.11b、および 802.11g を使用するカードのほとんどは、サポートされています。通常、新しいカードは 802.11g 規格に準拠していますが、802.11b を使用するカードも使用可能です。一般に、次のチップを内蔵したカードがサポートされています。

- Aironet 4500, 4800
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Intel PRO/Wireless 2100, 2200BG, 2915ABG, 3945ABG
- Intersil Prism2/2.5/3
- Intersil PrismGT
- Lucent/Agere Hermes

- Texas Instruments ACX100、ACX111
- ZyDAS zd1201

普及していたが廃止になった古いカードも、多数サポートされています。WLAN カードと使用チップについての詳細なリストは、にあるAbsoluteValue Systemshttp://www.linux-wlan.org/docs/wlan_adapters.html.gzのWebサイトを参照してください。さまざまなWLANチップの概要は、<http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz>を参照してください。

一部のカードの場合は、ドライバの初期化時にファームウェアイメージをカードにロードする必要があります。Intersil PrismGT、Atmel、TI ACX100およびACX111がその例です。ファームウェアは、YaSTオンラインアップデートを使用して簡単にインストールできます。Intel PRO/Wirelessカード用のファームウェアSUSE Linux Enterpriseに内蔵されており、この種のカードが検出されるとただちに、YaSTによって自動的にインストールされます。このトピックに関する詳細は、インストール済みシステムの/usr/share/doc/packages/wireless-tools/README.firmwareを参照してください。

29.1.2 機能

無線ネットワークでは、高速で高品質、そして安全な接続を確保するために、さまざまなテクニックや設定が使用されています。動作のタイプが違えば、それに適したセットアップ方式も異なります。適切な認証方式を選択するのは難しいことがあります。利用可能な暗号化方式には、それぞれ異なる利点と欠点があります。

動作モード

基本的に、無線ネットワークは管理ネットワークとAd-hocネットワークに分類できます。管理ネットワークには、管理要素のアクセスポイントがあります。このモード(インフラストラクチャモードとも呼ばれます)では、ネットワーク内のWLAN局の接続はすべてアクセスポイント経由で行われ、イーサネットへの接続としても機能できます。Ad-hocネットワークには、アクセスポイントはありません。局は相互に直接通信します。Ad-hocネットワークの場合は、伝送範囲と参加局の数が大幅に制限されます。そのため、通常はアクセスポイントを使用の方が効率的です。また、WLANカードをアクセス

ポイントとして使用することも可能です。ほとんどのカードは、この機能をサポートしています。

有線ネットワークよりも無線ネットワークの方がはるかに盗聴や侵入が容易なので、各種の規格には認証方式と暗号化方式が含まれています。IEEE 802.11規格のオリジナルバージョンでは、これらがWEPという用語で説明されています。ただし、WEPは安全でないことが判明したので(セキュリティ項(592ページ))、WLAN業界(Wi-Fi Allianceという団体名で協力)はWPAという新規の拡張機能を定義しており、これによりWEPの弱点がなくなるものと思われます。その後のIEEE 802.11i規格には、WPAと他の認証方式および暗号化方式が含まれています(WPAはドラフトバージョンの802.11iに基づいているので、この規格はWPA2と呼ばれることもあります)。

認証

認可された局だけが接続できるように、管理ネットワークでは各種の認証メカニズムが使用されます。

オープン

オープンシステムとは、認証を必要としないシステムです。任意の局がネットワークに参加できます。ただし、WEP暗号化(暗号化項(587ページ)を参照)は使用できます。

共有キー(IEEE 802.11に準拠)

この方式では、認証にWEPキーが使用されます。ただし、WEPキーが攻撃にさらされやすくなるので、この方式はお勧めしません。攻撃者は、局とアクセスポイント間の通信を長時間リスニングするだけで、WEPキーを奪取できます。認証処理中には、通信の両側が1度は暗号化形式、1度は暗号化されていない形式で同じ情報を交換します。そのため、適当なツールを使えば、キーを再構成することが可能です。この方式では認証と暗号化にWEPキーを使用するので、ネットワークのセキュリティは強化されません。適切なWEPキーを持っている局は、認証、暗号化および復号化を行うことができます。キーを持たない局は、受信したパケットを復号化できません。したがって、自己認証を行ったかどうかに関係なく、通信を行うことができません。

WPA-PSK (IEEE 802.1xに準拠)

WPA-PSK (PSKはpreshared keyの略)の機能は、共有キー方式と同様です。すべての参加局とアクセスポイントは、同じキーを必要とします。キーの長さは256ビットで、通常はパスフレーズとして入力されます。この方式

では、WPA-EAPのような複雑なキー管理を必要とせず、個人で使用するのに適しています。したがって、WPA-PSKはWPA「Home」とも呼ばれます。

WPA-EAP (IEEE 802.1xに準拠)

実際には、WPA-EAPは認証システムではなく、認証情報を転送するためのプロトコルです。WPA-EAPは、企業内の無線ネットワークを保護するために使用されます。プライベートネットワークでは、ほとんど使用されていません。このため、WPA-EAPはWPA「Enterprise」とも呼ばれます。

WPA-EAPは、ユーザを認証するのにRadiusサーバを必要とします。EAPには、サーバへの接続と認証手段として、TLS(Transport Layer Security)、TTLS(Tunneled Transport Layer Security)、およびPEAP(Protected Extensible Authentication Protocol)の、3種類の方法が用意されています。簡単に説明すると、これらのオプションは以下のように働きます。

EAP-TLS

TLSの認証は、サーバとクライアント両方の、証明書の相互交換に依存しています。はじめに、サーバがクライアントに対して証明書を提示し、それが評価されます。証明書が有効であるとみなされた場合には、今度がクライアントがサーバに対して証明書を提示します。TLSはセキュアですが、ネットワーク内で証明書管理のインフラストラクチャを運用することが必要になります。このインフラストラクチャは、プライベートネットワークでは通常存在しません。

EAP-TTLSとPEAP

TTLSとPEAPは両方とも、2段階からなるプロトコルです。最初の段階ではセキュリティが確立され、2番目の段階ではクライアントの認証データが交換されます。これらの証明書管理のオーバーヘッドは、もしあるとしても、TLSよりずっと小さいものです。

暗号化

権限のないユーザが無線ネットワークで交換されるデータパケットを読み込んだりネットワークにアクセスしたりできないように、さまざまな暗号化方式が存在しています。

WEP (IEEE 802.11で定義)

この規格では、RC4暗号化アルゴリズムを使用します。当初のキー長は40ビットでしたが、その後104ビットも使用されています。通常、初期化ベ

クタの24ビットを含めるものとして、長さは64ビットまたは128ビットとして宣言されます。ただし、この規格には一部弱点があります。このシステムで生成されたキーに対する攻撃が成功する場合があります。それでも、ネットワークをまったく暗号化しないよりはWEPを使用する方が適切です。

TKIP (WPA/IEEE 802.11iで定義)

このキー管理プロトコルはWPA規格で定義されており、WEPと同じ暗号化アルゴリズムを使用しますが、弱点は排除されています。データパケットごとに新しいキーが生成されるので、これらのキーに対する攻撃は無駄になります。TKIPはWPA-PSKと併用されます。

CCMP (IEEE 802.11iで定義)

CCMPは、キー管理を記述したものです。通常は、WPA-EAPに関連して使用されますが、WPA-PSKとも併用できます。暗号化はAESに従って行われ、WEP規格のRC4暗号化よりも厳密です。

29.1.3 YaSTでの設定

無線ネットワークカードを設定するには、YaSTの「ネットワークカード」モジュールを起動します。ここで、ネットワークカードの管理にYaSTまたはNetworkManagerのいずれを使用するかを選択できます。YaSTを選択した場合は、「ネットワークアドレス設定」のデバイスタイプに「無線」を選択し、「次へ」をクリックします。「無線ネットワークカードの設定」で(図 29.1. 「YaST:無線ネットワークカードの設定」 (589 ページ)を参照)、WLAN操作の基本設定を行います。

図 29.1 YaST: 無線ネットワークカードの設定



動作モード

WLANでは、局を3つのモードで統合できます。最適なモードは、アドホック(アクセスポイントのないピアツーピアネットワーク)、管理(アクセスポイントにより管理されるネットワーク)、またはマスタ(アクセスポイントとしてネットワークカードを使用)など、通信するネットワークによって異なります。WPA-PSKまたはWPA-EAPモードを使用するには、動作モードを「*Managed*」に設定する必要があります。

ネットワーク名(ESSID)

無線ネットワークのすべての局が相互に通信するには、同じESSIDが必要です。何も指定しなければ、カードは自動的にアクセスポイントを選択しますが、それが意図したアクセスポイントとは異なる場合があります。

認証モード

ネットワークに適した認証方法を選択します: [オープン]、[共有キー]、
[WPA-PSK]、または [WPA-EAP]。WPA認証を選択した場合は、ネット
ワーク名を設定する必要があります。

エキスパート設定

このボタンをクリックすると、**WLAN**接続の詳細設定用ダイアログが開きます。このダイアログの詳細については後述します。

基本設定を完了すると、自局がWLANで運用可能になります。

重要項目: 無線ネットワークでのセキュリティ

ネットワークトラフィックを保護するために、サポートされている認証方式と暗号化方式の1つを必ず使用してください。暗号化されていないWLAN接続では、第三者がすべてのネットワークデータを盗聴することができます。弱い暗号化(WEP)でも、まったく暗号化しないよりはましです。詳細については、[暗号化項 \(587 ページ\)](#)と[セキュリティ項 \(592 ページ\)](#)を参照してください。

選択した認証方式によっては、YaSTの別のダイアログで設定を微調整するように要求されます。[オープン]を選択した場合、何も設定項目はありません。この設定では、認証なしの暗号化されない動作が実装されるからです。

共有キー

キーの入力タイプを設定します。[パスフレーズ]、[ASCII]、[16進]のいずれかを選択します。最大4つの異なるキーを使用して伝送データを暗号化できます。[WEPキー]をクリックしてキー設定ダイアログを開きます。キー長を設定します:128ビットまたは64ビット。デフォルト設定は、[128ビット]ビットです。ダイアログ下部にあるリスト領域では、局で暗号化に使用するキーを最大4つまで指定できます。[デフォルト設定とする]を押して、4つのうち1つをデフォルトキーとして定義します。この方法で変更しない限り、YaSTでは最初に入力したキーがデフォルトキーとして使用されます。標準キーが削除された場合は、残りのキーの1つを手動でデフォルトキーに設定する必要があります。[編集]をクリックし、既存のリストエントリを変更するか、新規のキーを作成します。新規作成の場合、ポップアップウィンドウが表示され、キーの入力タイプ([パスフレーズ]、[ASCII]、または[16進])を選択する必要があります。[パスフレーズ]を選択した場合は、前に指定した長さに従ってキーの生成に使用するワードまたは文字列を入力します。[ASCII]を選択した場合は、64ビットキーであれば5文字、128ビットキーであれば13文字を入力する必要があります。[Hexadecimal]を選択した場合は、64ビットキーであれば10文字、128ビットキーであれば26文字を16進表記で入力します。

WPA-PSK

WPA-PSK用のキーを入力するには、入力方法として[パスフレーズ]または[16進]を選択します。[Passphrase]モードでは、8から63文字を入力する必要があります。[16進]モードでは、64文字を入力します。

WPA-EAP

ネットワーク管理者から受け取った証明書を設定します。TLSの場合は、**[Identity]**、**[Client Certificate]**、**[Client Key]**、および**[Server Certificate]**に適切な値を入力します。TTLSとPEAPでは、**[Identity]**と**[Password]**が必要です。**[Server Certificate]**と**[Anonymous Identity]**は、必要に応じて指定してください。YaSTは、`/etc/cert`で証明書を探すので、受け取った証明書はこの場所に保存し、これらのファイルに対するアクセス権は0600(所有者の読み取りと書き込み)に制限してください。

[詳細] をクリックして、WPA-EAPセットアップ用の高度認証ダイアログを入力します。EAP-TTLSまたはEAP-PEAP通信の第2ステージ用の認証方法を選択します。前のダイアログでTTLSを選択した場合は、any、MD5、GTC、CHAP、PAP、MSCHAPv1またはMSCHAPv2を選択します。PEAPを選択した場合は、any、MD5、GTCまたはMSCHAPv2を選択します。自動的に決定された設定を変更する必要がある場合は、**[PEAP version]** を使用して特定のPEAP実装を使用するように強制できます。

[エキスパート設定] をクリックしてWLAN接続の基本設定ダイアログを終了し、上級者用の設定に入ります。このダイアログでは、次のオプションを使用できます。

チャンネル

WLAN局が使用するチャンネルの指定を必要とするのは、**[Ad-hoc]** モードと**[マスタ]** モードだけです。**[管理]** モードでは、カードはアクセスポイントに使用可能なチャンネルを自動的に検索します。**[Ad-hoc]** モードでは、自局と他局との通信用に提供されている12のチャンネルから1つを選択します。**[マスタ]** モードでは、使用するカードがアクセスポイント機能を提供する必要があるチャンネルを指定します。このオプションのデフォルト設定は**[自動]** です。

転送ビットレート

ネットワークのパフォーマンスに応じて、あるポイントから別のポイントへの伝送について特定のビットレートを設定できます。デフォルト設定の**[自動]** では、システムは最大許容データ伝送速度を使用しようとします。ビットレートの設定をサポートしていないWLANカードもあります。

Access Point

複数のアクセスポイントがある環境では、MACアドレスを指定することで、その1つを事前に選択できます。

29.1.4 ユーティリティ

WLANカードをアクセスポイントとして使用するには、**hostap** (hostapパッケージ)を使用します。このパッケージの詳細については、プロジェクトのホームページ(<http://hostap.epitest.fi/>)を参照してください。

kismet (kismetパッケージ)は、WLANパケットトラフィックのリスニングに使用するネットワーク診断ツールです。このツールを使用すると、ネットワーク内の侵入試行も検出できます。詳細については、<http://www.kismetwireless.net/>とマニュアルページを参照してください。

29.1.5 WLANのセットアップに関するヒントとテクニック

これらのヒントでは、速度と安定性を微調整する方法や、WLANのセキュリティの側面について説明します。

安定性と速度

無線ネットワークのパフォーマンスと信頼性は、主として参加局が他局からクリーンな信号を受信するかどうかに依存します。壁などの障害物があると、信号が大幅に弱くなります。信号強度が低下するほど、伝送速度も低下します。操作中には、コマンドライン(Link Qualityフィールド)で*iwconfig*ユーティリティを使用するか、またはNetworkManagerかKNetworkManagerを使用して、信号強度を確認します。信号品質に問題がある場合は、他の場所でデバイスをセットアップするか、またはアクセスポイントのアンテナ位置を調整してください。多くのPCMCIA WLANカードの場合、受信品質を実質的に向上させる補助アンテナを利用できます。メーカー指定のレート(54MBit/sなどは、理論上の上限を表す公称値です。実際の最大データスループットは、この値の半分以下です。

セキュリティ

無線ネットワークをセットアップする際には、セキュリティ対策を導入しなければ、伝送範囲内の誰もが簡単にアクセスできることを忘れないでください。したがって、必ず暗号化方式をアクティブにする必要があります。すべ

てのWLANカードとアクセスポイントが、WEP暗号化をサポートしています。それでも完全に安全とは言えませんが、潜在的な攻撃者に対する障害物は存在することになります。通常、プライベート用であればWEPで十分です。WPA-PSKも適していますが、WLAN機能を持つ古いアクセスポイントやルータには実装されていません。デバイスによっては、ファームウェア更新を使用してWPAを実装できます。さらに、Linuxは、すべてのハードウェアコンポーネントでWPAをサポートしているわけではありません。このマニュアルの制作時点では、WPAが機能するのは、Atheros、Intel PRO/Wireless、またはPrism2/2.5/3チップを使用するカードの場合だけです。Prism2/2.5/3の場合、WPAが機能するのはhostapドライバを使用している場合だけです(を参照)。**Prism2カードの問題項**(593 ページ)WPAが使用できない場合、暗号化しないよりはWEPを使用することをお勧めします。高度なセキュリティ要件を持つ企業では、無線ネットワークの運用にWPAを使用する必要があります。

29.1.6 トラブルシューティング

WLANカードが応答しない場合は、必須ファームウェアをダウンロードしたかどうかを確認します。参照先 **29.1.1項「ハードウェア」** (584 ページ). ここでは、判明している一部の問題について説明します。

複数のネットワークデバイス

通常、最近のラップトップにはネットワークカードとWLANカードが搭載されています。DHCP(自動アドレス割り当て)を使用して両方のデバイスを構成すると、名前解決とデフォルトゲートウェイに問題が発生することがあります。これは、ルータはpingできるがインターネット上でナビゲーションできないことを示しています。詳細については、http://en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_ClientsにあるSupport Databas (サポートデータベース)を参照してください。

Prism2カードの問題

Prism2チップ搭載のデバイスには、複数のドライバが用意されています。各種カードがスムーズに動作するかどうかは、ドライバに応じて異なります。この種のカードの場合、WPAに使用できるのはhostapドライバだけです。この種のカードが正常に動作しない場合、まったく動作しない場合、またはWPA

を使用する必要がある場合は、`/usr/share/doc/packages/wireless-tools/README.prism2`を参照してください。

WPA

WPAのサポートは、SUSE Linux Enterpriseでも新しく、まだ発展途上にあります。そのため、YaSTはすべてのWPA認証方式の設定をサポートしているわけではありません。また、すべての無線LANカードやドライバがWPAをサポートしているわけでもありません。カードの中には、WPAを有効にするためにファームウェアのアップデートを必要とするものがあります。WPAを使用する場合は、`/usr/share/doc/packages/wireless-tools/README.wpa`を参照してください。

29.1.7 詳細情報

Linux用の無線ツールを開発したJean Tourrilhesのインターネットページには、無線ネットワークに関して役立つ情報が多数提供されています。詳細については、http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.htmlを参照してください。

パート IV. サービス

ネットワークの基礎

Linuxには、あらゆるタイプのネットワークストラクチャに統合するために必要なネットワークツールと機能が用意されています。ここでは、一般に使用されるLinuxプロトコルであるTCP/IPについて説明します。このプロトコルが持つさまざまなサービスや特別な機能について述べます。ネットワークカード、モデム、その他のデバイスを使用したネットワークアクセスは、YaSTによって設定できます。手動による環境設定も可能です。この章では、基本的なメカニズムと関連のネットワークの環境設定ファイルのみを扱います。

Linuxおよび他のUnix系オペレーティングシステムは、TCP/IPプロトコルを使用します。これは1つのネットワークプロトコルではなく、さまざまなサービスを提供する複数のネットワークプロトコルのファミリーです。TCP/IPを使用して2台のコンピュータ間でデータをやり取りするために、表 30.1、「TCP/IP プロトコルファミリーを構成する主要なプロトコル」(598ページ)に示した各プロトコルが提供されています。TCP/IPによって結合された世界規模のネットワーク全体のことを「インターネット」と呼びます。

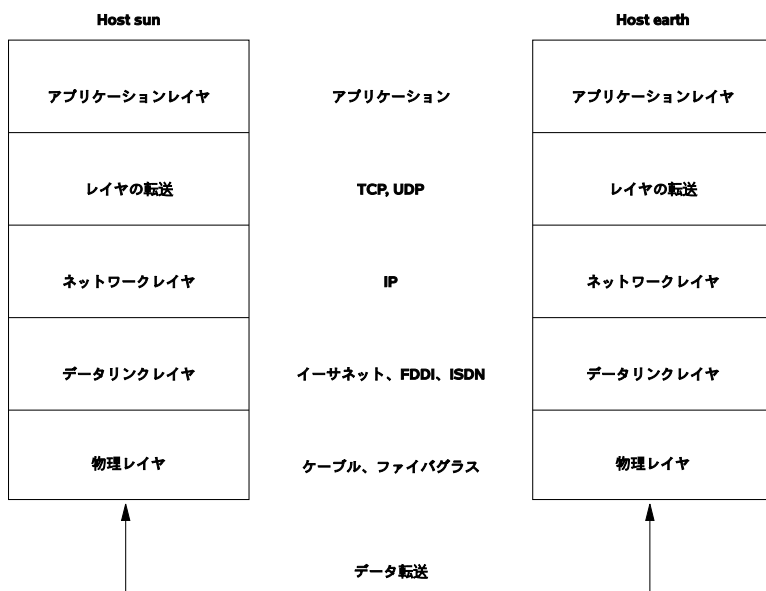
RFCは、*Request for Comments*の略です。RFCは、さまざまなインターネットプロトコルとそれをオペレーティングシステムとそのアプリケーションに実装する手順を定めています。RFC文書ではインターネットプロトコルのセットアップについて説明しています。プロトコルについての知識を広めるには、その種類にかかわらず、適切なRFC文書を参照してください。RFC文書は、<http://www.ietf.org/rfc.html>で参照してください。

表 30.1 TCP/IP プロトコルファミリーを構成する主要なプロトコル

プロトコル	説明
TCP	TCP (Transmission Control Protocol): 接続指向型の安全なプロトコルです。転送されるデータはまずアプリケーションによってデータのストリームとして送信され、次にオペレーティングシステムによって適切な形式に変換されます。データは、それが送信されたときの元のデータ形式で、宛先ホストのそれぞれのアプリケーションに到着します。TCPは、伝送中にデータに損失がなかったか、データの混同がないかどうかを確認します。データの順序が意味を持つ場合は常にTCP/IPが実装されます。
UDP	UDP (User Datagram Protocol): コネクションレスのプロトコルで安全ではありません。転送されるデータは、アプリケーションで生成されたパケットの形で送信されます。データが受信側に到着する順序は保証されず、データの損失の可能性もあります。UDPはレコード指向のアプリケーションに適しています。TCPよりも遅延時間が小さいことが特徴です。
ICMP	ICMP (Internet Control Message Protocol): 基本的にはエンドユーザ向けのプロトコルではありませんが、エラーレポートを発行し、TCP/IPデータ転送にかかわるマシンの動作を制御できる特別な制御プロトコルです。またICMPには特別なエコーモードがあります。エコーモードは、pingで使用されています。
IGMP	IGMP (Internet Group Management Protocol): このプロトコルは、IPマルチキャストを実装した場合のコンピュータの動作を制御します。

に示したように、データのやり取りはさまざまなレイヤで実行されます。
図 30.1. 「TCP/IPの簡易レイヤモデル」 (599 ページ) 実際のネットワークレイヤは、IP (インターネットプロトコル) によって実現される確実性のないデータ転送です。IPの上で動作するTCP(転送制御プロトコル)によって、ある程度の確実性のあるデータ転送が保証されます。IPレイヤの下層には、イーサネットなどのハードウェア依存プロトコルがあります。

図 30.1 TCP/IPの簡易レイヤモデル



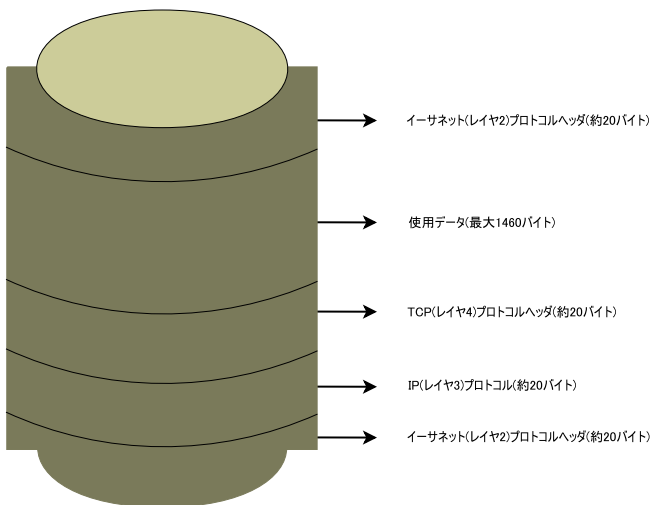
図では、各レイヤに対応する例を1つまたは2つ示しています。レイヤは抽象化レベルに従って並べられています。最下位レイヤは最もハードウェアに近い部分です。一方、最上位レイヤは、ハードウェアがまったく見えないほぼ完全な抽象化になります。各レイヤにはそれぞれの固有の機能があります。各レイヤ固有の機能は、上記の主要プロトコルの説明を読めば大体わかります。データリンクレイヤと物理レイヤは、使用される物理ネットワーク（たとえばイーサネット）を表します。

ほとんどすべてのハードウェアプロトコルは、パケット単位で動作します。転送されるデータは、一度にすべて送信できないので、パケットに分割されます。TCP/IPパケットの最大サイズは約64KBです。しかし、パケットサイズは通常、64KBよりもかなり小さな値になります。これは、ネットワークハードウェアでサポートされているパケットサイズに制限があるからです。イーサネットの最大パケットサイズは、約1500バイトです。イーサネット上に送出されるTCP/IPパケットは、このサイズに制限されます。転送するデータ量が大きくなると、それだけ多くのパケットがオペレーティングシステムによって送信されます。

すべてのレイヤがそれぞれの機能を果たすためには、各レイヤに対応する情報を各データパケットに追加する必要があります。この情報はパケットのヘッ

ダとして追加されます。各レイヤでは、プロトコルヘッダと呼ばれる小さなデータブロックが、作成されたパケットに付加されます。図 30.2. 「TCP/IP イーサネットパケット」 (600 ページ) に、イーサネットケーブル上に送出される TCP/IP データパケットの例を示します。誤り検出のためのチェックサムは、パケットの先頭ではなく最後に付加されます。これによりネットワークハードウェアの処理が簡素化されます。

図 30.2 TCP/IP イーサネットパケット



アプリケーションがデータをネットワーク経由で送信すると、データは各レイヤを通過します。これらのレイヤは、物理レイヤを除き、すべてLinuxカーネルに実装されています。各レイヤは、隣接する下位レイヤに渡せるようにデータを処理します。最下位レイヤは、最終的にデータを送信する責任を負います。データを受信したときには、この手順全体が逆の順序で実行されます。重なり合ったたまねぎの皮のように、各レイヤで伝送データからプロトコルヘッダが除去されていきます。最後に、トランスポートレイヤが、着信側のアプリケーションがデータを利用できるように処理します。この方法では、1つのレイヤが直接やり取りを行うのは隣接する上下のレイヤのみです。データが伝送される物理的なネットワークは、100MBit/sのFDDIかもしれませんし、56Kbit/sのモデム回線かもしれませんが、アプリケーションがその違いを意識することはありません。同様に、物理ネットワークは、パケットの

形式さえ正しければよく、伝送されるデータの種類を意識することはありません。

30.1 IPアドレスとルーティング

ここでは、IPv4ネットワークについてのみ説明しています。IPv4の後継バージョンであるIPv6については、[30.2項「IPv6 ―次世代のインターネット」](#) (604 ページ)を参照してください。

30.1.1 IPアドレス

インターネット上のすべてのコンピュータは、一意の32ビットアドレスを持っています。この32ビット(4バイト)は、通常、[例 30.1. 「IPアドレスの表記」](#) (601 ページ)の2行目に示すような形式で表記されます。

例 30.1 IPアドレスの表記

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.      168.      0.      20
```

10進表記では、4つの各バイトが10進数で表記され、ピリオドで区切られます。IPアドレスは、ホストまたはネットワークインタフェースに割り当てられます。各アドレスは世界で唯一のアドレスであり、重複して使用されることはありません。このルールには例外もありますが、以下の説明には直接関係していません。

IPアドレスにあるピリオドは、階層構造を表しています。1990年代まで、IPアドレスは、各クラスに固定的に分類されていました。しかし、このシステムがあまりに柔軟性に乏しいことがわかったので、今日、そのような分類は行われていません。現在採用されているのは、クラスレスルーティング(CIDR: classless inter domain routing)です。

30.1.2 ネットマスクとルーティング

ネットマスクは、サブネットワークのアドレス範囲を定義するために用いられます。2台のホストが同一のサブネットワークに属している場合には、それらは相互に直接連絡できますが、そうでない場合には、サブネットワークとそれ以外の場所との間のトラフィックを処理するゲートウェイのアドレスを

必要とします。2つのIPアドレスが同じサブネットワークに属しているかどうかを確認するには、両方のアドレスとネットマスクの「AND」を求めます。結果が同一であれば、両方のIPアドレスは同じローカルネットワークに属しています。相違があれば、それらのIPアドレス、そしてそれらに対応するインタフェースが連絡するには、ゲートウェイを通過する必要があります。

ネットマスクの役割を理解するには、例 30.2. 「IPアドレスとネットマスクの論理積(AND)」 (602 ページ)を参照してください。ネットマスクは、そのネットワークにいくつのIPアドレスが属しているかを示す、32ビットの値から成っています。1になっているビットは、IPアドレスのうち、特定のネットワークに属することを示すビットに対応します。0になっているビットは、サブネットワーク内での識別に使われるビットに対応します。これは、1になっているビット数が多いほど、サブネットワークが小さいことを意味します。ネットマスクは常に連続する1のビットから構成されているので、その数だけでネットマスクを指定することができます。例 30.2. 「IPアドレスとネットマスクの論理積(AND)」 (602 ページ)の、24ビットからなる第1のネットワークは、192.168.0.0/24と書くこともできます。

例 30.2 IPアドレスとネットマスクの論理積(AND)

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
-----
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:      192.      168.      0.      0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
-----
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:      213.      95.      15.      0
```

また、たとえば同じイーサネットケーブルに接続しているすべてのマシンは、普通同じサブネットワークに属し、直接アクセスできます。サブネットワークがスイッチまたはブリッジで物理的に分割されていても、これらのホストは直接アクセス可能です。

ローカルサブネットワークの外部のIPアドレスには、ターゲットネットワーク用のゲートウェイが設定されている場合にのみ、連絡できます。最も一般的には、外部からのすべてのトラフィックを扱うゲートウェイを1台だけ設置します。ただし、異なるサブネットワーク用に、複数のゲートウェイを設定することも可能です。

ゲートウェイを設定すると、外部からのすべてのIPパケットは適切なゲートウェイに送信されます。このゲートウェイは、パケットを複数のホストを経由して転送し、それは最終的に宛先ホストに到着します。ただし、途中でTTL (time to live)に達した場合は破棄されます。

表 30.2 特殊なアドレス

アドレスのタイプ	説明
基本ネットワークアドレス	ネットマスクとネットワーク内の任意のアドレスの論理積をとったもの。例 30.2. 「IPアドレスとネットマスクの論理積(AND)」 (602 ページ)のANDをとった結果を参照。このアドレスは、どのホストにも割り当てることができません。
ブロードキャストアドレス	ブロードキャストアドレスは、基本的には「サブネットワーク内のすべてのホストにアクセスする」ためのアドレスです。」このアドレスを生成するには、2進数形式のネットマスクを反転させ、基本ネットワークアドレスと論理和をとります。そのため上記の例では、192.168.0.255になります。このアドレスをホストに割り当てることはできません。
ローカルホスト	アドレス127.0.0.1は、各ホストの「ループバックデバイス」に割り当てられます。このアドレスを使用すると、自分のマシンに対して接続を確立できます。

IPアドレスは、世界中で一意でなければならぬので、自分勝手にアドレスを選択して使うことはできません。IPベースのプライベートネットワークをセットアップする場合のために、3つのアドレスドメインが用意されています。これらは、外部のインターネットに直接接続することはできません。インターネット上で転送されることがないからです。このようなアドレスドメインは、RFC 1597で、表 30.3. 「プライベートIPアドレスドメイン」 (604 ページ)に示すとおりに定められています。

表 30.3 プライベートIPアドレスドメイン

ネットワーク/ネットマスク	ドメイン
10.0.0.0/255.0.0.0	10.x.x.x
172.16.0.0/255.240.0.0	172.16.x.x – 172.31.x.x
192.168.0.0/255.255.0.0	192.168.x.x

30.2 IPv6 一次世代のインターネット

重要項目: IBM System z: IPv6サポート

IPv6は、IBM System zハードウェアのCTCおよびIUCVネットワーク接続ではサポートされていません。

WWW(ワールドワイドウェブ)の出現により、ここ10年間でTCP/IP経由で通信を行うコンピュータの数が増大し、インターネットは爆発的に拡大しました。CERN (<http://public.web.cern.ch>)のTim Berners-Leeが1990年にWWWを発明して以来、インターネットホストは、数千から約1億まで増加しました。

前述のように、IPv4のアドレスはわずか32ビットで構成されています。しかも、多くのIPアドレスが失われています。というのは、ネットワークの編成方法のせいで、使われないIPアドレスが無駄に割り当てられてしまうからです。サブネットで見られるアドレスの数は、 $(2^{\text{ビット数}} - 2)$ で与えられます。たとえば、1つのサブネットワークでは、2、6、または14個のアドレスが使用可能です。たとえば128台のホストをインターネットに接続するには、256個のIPアドレスを持つサブネットワークが必要ですが、そのうち2つのIPアドレスは、サブネットワーク自体を構成するのに必要なブロードキャストアドレスと基本ネットワークアドレスになるので、実際に使用できるのは254個だけです。

現在のIPv4プロトコルでは、アドレスの不足を避けるために、DHCPとNAT(ネットワークアドレス変換)の2つのメカニズムが使用されています。これらの方法をパブリックアドレスとプライベートアドレスを分離するという慣習

と組み合わせて使用することで、確かにアドレス不足の問題を緩和することができます。問題は、セットアップが面倒で保守しにくいその環境設定方法にあります。IPv4ネットワークでホストをセットアップするには、ホスト自体のIPアドレス、サブネットマスク、ゲートウェイアドレス、そして場合によってはネームサーバアドレスなど、相当数のアドレス項目が必要になります。管理者は、これらをすべて自分で設定しなければなりません。これらのアドレスをどこから取得することはできません。

IPv6では、アドレス不足と複雑な環境設定方法はもはや過去のもので。ここでは、IPv6がもたらした進歩と恩恵について説明し、古いプロトコルから新しいプロトコルへの移行について述べます。

30.2.1 長所

この新しいプロトコルがもたらした最大かつ最もわかりやすい進歩は、利用可能なアドレス空間の飛躍的な増加です。IPv6アドレスは、従来の32ビットではなく、128ビットで構成されています。これにより、2の128乗、つまり、約 3.4×10^{38} 個のIPアドレスが得られます。

しかしながら、IPv6アドレスがその先行プロトコルと異なるのはアドレス長だけではありません。IPv6アドレスは内部構造も異なっており、それが属するシステムやネットワークに関してより具体的な情報を有しています。詳細については、[30.2.2項「アドレスのタイプと構造」](#) (607 ページ)を参照してください。

以下に、この新しいプロトコルの利点をいくつか紹介します。

自動環境設定機能

IPv6を使用すると、ネットワークが「プラグアンドプレイ」対応になります。つまり、新しくシステムをセットアップすると、手動で環境設定しなくても、(ローカル)ネットワークに統合されます。新しいホストは自動環境設定メカニズムを使用して、ネイバーディスカバリ (ND) と呼ばれるプロトコルにより、近隣のルータから得られる情報を元に自身のアドレスを生成します。この方法は、管理者の介入が不要だけでなく、サアドレス割り当てを1台のサーバで一元的に管理する必要もありません。これもIPv4より優れている点の1つです。IPv4では、自動アドレス割り当てを行うために、DHCPサーバを実行する必要があります。

モバイル性

IPv6を使用すると、複数のアドレスを1つのネットワークインタフェースに同時に割り当てることができます。これにより、ユーザは複数ネットワークに簡単にアクセスできます。このことは、携帯電話会社が提供する国際ローミングサービスにたとえられます。携帯電話を海外に持って行った場合、現地会社のサービス提供エリアに入ると自動的に携帯電話はそのサービスにログインし、同じ番号で普段と同じように電話をかけることができます。

安全な通信

IPv4では、ネットワークセキュリティは追加機能です。IPv6にはIPSecが中核的機能の1つとして含まれているので、システムが安全なトンネル経由で通信でき、インターネット上での部外者による通信傍受を防止します。

後方互換性

現実的に考えて、インターネット全体を一気にIPv4からIPv6に切り替えるのは不可能です。したがって、両方のプロトコルが、インターネット上だけでなく1つのシステム上でも共存できることが不可欠です。これは、一方ではアドレスの互換性によって(IPv4アドレスは容易にIPv6アドレスに変換できます)、他方ではトンネルの使用によって保証されています。参照先 [30.2.3項「IPv4とIPv6の共存」](#) (612 ページ)。また、システムはデュアルスタックIPテクニックによって、両方のプロトコルを同時にサポートできるので、2つのプロトコルバージョン間に相互干渉のない、完全に分離された2つのネットワークスタックが作成されます。

マルチキャストによるサービスの詳細なカスタマイズ

IPv4では、いくつかのサービス(SMBなど)が、ローカルネットワークのすべてのホストにパケットをブロードキャストする必要があります。IPv6では、これよりはるかにきめ細かいアプローチが取られ、サーバがマルチキャストという、複数のホストをグループの一部として扱う技術によって、ホストにデータを送信します(これは、すべてのホストにデータを送信するブロードキャストとも、各ホストに個別に送信するユニキャストとも異なります)。どのホストを対象グループに含めるかは、個々のアプリケーションによって異なります。事前定義のグループには、たとえば、すべてのネームサーバを対象とするグループ(全ネームサーバマルチキャストグループ)やすべてのルータを対象とするグループ(全ルータマルチキャストグループ)があります。

30.2.2 アドレスのタイプと構造

これまでに述べたように、現在のIPプロトコルには、IPアドレス数が急激に不足し始めているということと、ネットワーク設定とルーティングテーブルの管理がより複雑で煩雑な作業になっているという、2つの重要な問題があります。IPv6では、1つ目の問題を、アドレス空間を拡張することによって解決しています。2番目の問題には、階層的なアドレス構造を導入し、ネットワークアドレスを割り当てる高度なテクニックとマルチホーミング(1つのデバイスに複数のアドレスを割り当てることによって、複数のネットワークへのアクセスを可能にします)を組み合わせて対応しています。

IPv6を扱う場合は、次の3種類のアドレスについて知っておくと役に立ちます。

ユニキャスト

このタイプのアドレスは、1つのネットワークインタフェースだけに関連付けられます。このようなアドレスを持つパケットは、1つの宛先にのみ配信されます。したがって、ユニキャストアドレスは、パケットをローカルネットワークまたはインターネット上の個々のホストに転送する場合に使用します。

マルチキャスト

このタイプのアドレスは、ネットワークインタフェースのグループに関連します。このようなアドレスを持つパケットは、そのグループに属するすべての宛先に配信されます。マルチキャストアドレスは、主に、特定のネットワークサービスが、相手を特定のグループに属するホストに絞って通信を行う場合に使用されます。

エニーキャスト

このタイプのアドレスは、インタフェースのグループに関連します。このようなアドレスを持つパケットは、基盤となるルーティングプロトコルの原則に従い、送信側に最も近いグループのメンバに配信されます。エニーキャストアドレスは、特定のネットワーク領域で特定のサービスを提供するサーバについて、ホストが情報を得られるようにするために使用します。同じタイプのすべてのサーバは、エニーキャストアドレスが同じになります。ホストがサービスを要求すると、ルーティングプロトコルによって最も近い場所にあるサーバが判断され、そのサーバが応答します。何らかの理由でこのサーバが応答できない場合、プロトコルが自動的に2番目のサーバを選択し、それが失敗した場合は3番目、4番目が選択されます。

IPv6アドレスは、4桁の英数字が入った8つのフィールドで構成され、それぞれのフィールドが16進数表記の16ビットを表します。各フィールドは、コロン(:)で区切られます。各フィールドで先頭の0は省略できますが、数字の間にある0や末尾の0は省略できません。もう1つの規則として、0のバイトが5つ以上連続する場合は、まとめて2つのコロン(::)で表すことができます。ただし、アドレスごとに::は1回しか使用できません。この省略表記の例については、[例 30.3. 「IPv6アドレスの例」](#) (608 ページ)を参照してください。この3行はすべて同じアドレスを表します。

例 30.3 IPv6アドレスの例

```
fe80 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                                : 10 : 1000 : 1a4
```

IPv6アドレスの各部の機能は個別に定められています。最初の4バイトはプレフィクスを形成し、アドレスのタイプを指定します。中間部分はアドレスのネットワーク部分ですが、使用しなくてもかまいません。アドレスの最後の4桁はホスト部分です。IPv6でのネットマスクは、アドレスの末尾のスラッシュの後にプレフィクスの長さを指定して定義します。に示すアドレスには、最初の64ビットがアドレスのネットワーク部分を構成する情報、最後の64ビットにホスト部分を構成する情報が入っています。[例 30.4. 「プレフィクスの長さを指定したIPv6アドレス」](#) (608 ページ)言い換えると、64は、ネットマスクに64個の1ビット値が左から埋められていることを意味します。IPv4と同様、IPアドレスとネットマスクのANDをとることにより、ホストが同じサブネットワークにあるかそうでないかを判定します。

例 30.4 プレフィクスの長さを指定したIPv6アドレス

```
fe80::10:1000:1a4/64
```

IPv6は、事前に定義された複数タイプのプレフィクスを認識します。に、一部のプレフィクスタイプを示します。[表 30.4. 「IPv6のプレフィクス」](#) (608 ページ)

表 30.4 IPv6のプレフィクス

プレフィクス (16進)	定義
00	IPv4アドレスおよびIPv4 over IPv6互換性アドレス。これらは、IPv4との互換性を保つために使用します。これらを使

プレフィクス 定義 (16進)

	用した場合でも、IPv6パケットをIPv4パケットに変換するルータが必要です。いくつかの特殊なアドレス(たとえばループバックデバイスのアドレス)もこのプレフィクスを持ちます。
先頭桁が2または3	集約可能なグローバルユニキャストアドレス。IPv4と同様、インタフェースを割り当てて特定のサブネットワークの一部を構成することができます。現在、2001::/16(実稼動品質のアドレス空間)と2002::/16(6to4アドレス空間)の2つのアドレス空間があります。
fe80::/10	リンクローカルアドレス。このプレフィクスを持つアドレスは、ルーティングしてはなりません。したがって、同じサブネットワーク内からのみ到達可能です。
fec0::/10	サイトローカルアドレス。ルーティングはできますが、それが属する組織のネットワーク内に限られます。要するに、IPv6版のプライベートネットワークアドレス空間です(たとえば、10.x.x.x)。
ff	マルチキャストアドレス。

ユニキャストアドレスは、以下の3つの基本構成要素からなります。

パブリックトポロジ

最初の部分(前述のいずれかのプレフィクスが含まれる部分)は、パブリックインターネット内でパケットをルーティングするために使用します。ここには、インターネットアクセスを提供する企業または団体に関する情報が入っています。

サイトトポロジ

2番目の部分には、パケットの配信先のサブネットワークに関するルーティング情報が入っています。

インタフェースID

3番目の部分は、パケットの配信先のインタフェースを示します。これを使用して、MACをアドレスの一部に含めることができます。MACは、世界中で重複がない固定の識別子であり、ハードウェアメカによってデバイスにコーディングされるので、環境設定手順が大幅に簡素化されます。実際には、最初の64アドレスビットが統合されてEUI-64トークンを構成します。このうち、最後の48ビットにはMACアドレス、残りの24ビットにはトークンタイプに関する特別な情報が入ります。これにより、PPPやISDNのインタフェースのようにMACを持たないインタフェースにEUI-64トークンを割り当てられるようになります。

IPv6は、この基本構造の上で、以下の5種類のユニキャストアドレスを区別します。

:: (未指定)

このアドレスは、インタフェースが初めて初期化される時、すなわち、アドレスが他の方法で判定できないときに、ホストがそのソースアドレスとして使用します。

:::1 (ループバック)

ループバックデバイスのアドレス。

IPv4互換アドレス

IPv6アドレスが、IPv4アドレスおよび96個の0ビットからなるプレフィクスで作成されます。このタイプの互換アドレスは、IPv4とIPv6のホストが、純粋なIPv4環境で動作している他のホストと通信するためのトンネリング(30.2.3項「IPv4とIPv6の共存」(612 ページ)を参照)として使用されます。

IPv6にマッピングされたIPv4アドレス

このタイプのアドレスは、IPv6表記で純粋なIPv4アドレスを指定します。

ローカルアドレス

ローカルで使用するアドレスのタイプには、以下の2種類があります。

リンクローカル

リンクローカルこのタイプのアドレスは、ローカルのサブネットワークでのみ使用できます。このタイプの送信元または宛先アドレスを持つパケットをインターネットまたは他のサブネットワークにルーティングしてはなりません。これらのアドレスは、特別なプレフィクス

(fe80::/10)とネットワークカードのインタフェースID、およびヌルバイトからなる中間部分からなります。このタイプのアドレスは、自動環境設定のとき、同じサブネットワークに属する他のホストと通信するために使用されます。

サイトローカル

このタイプのアドレスを持つパケットは、他のサブネットワークにはルーティングできますが、それより広いインターネットにはルーティングしてはなりません。つまり、組織自体のネットワークの内側だけで使用するよう制限する必要があります。このようなアドレスはイントラネット用に使用され、IPv4によって定義されているプライベートアドレス空間に相当します。これらのアドレスは、特殊なプレフィクス(fec0::/10)とインタフェースID、およびサブネットワークIDを指定する16ビットのフィールドからなります。

IPv6では、各ネットワークインタフェースが複数のIPアドレスを持つことができるというまったく新しい機能が導入されました。これにより、同じインタフェースで複数のネットワークにアクセスできます。これらのネットワークは、MACと既知のプレフィクスを使用して完全に自動設定できるので、IPv6を有効にするとすぐに、(リンクローカルアドレスを使用して)ローカルネットワーク上のすべてのホストに接続できるようになります。IPアドレスにMACが組み込まれているので、使用されるIPアドレスは世界中で唯一のアドレスになります。アドレスの唯一の可変部分は、ホストが現在動作している実際のネットワークによって、サイトトポロジとパブリックトポロジを指定する部分になります。

複数のネットワークに接続するホストの場合、少なくとも2つのアドレスが必要です。1つはホームアドレスです。ホームアドレスには、インタフェースIDだけでなく、それが通常属するホームネットワークの識別子(および対応するプレフィクス)も含まれています。ホームアドレスは静的アドレスなので、通常は変更されません。しかし、モバイルホスト宛てのパケットは、それがホームネットワーク内にあるかどうかにかかわらず、すべてそのホストに配信できます。これは、IPv6で導入されたステートレス自動環境設定やネイバーディスカバリのようまったく新しい機能によって実現されました。モバイルホストは、ホームアドレスに加え、ローミング先の外部ネットワークに属するアドレスも取得します。これらはケアオブアドレスと呼ばれます。ホームネットワークには、ホストが対象エリア外をローミングしている間、そのホスト宛てのすべてのパケットを転送する機能があります。IPv6環境において、このタスクは、ホームエージェントによって実行されます。ホームエージェントは、ホームアドレスに届くすべてのパケットを取得してトンネルにリレー

します。一方、ケアオブアドレスに届いたパケットは、特別迂回することなく、直接モバイルホストに転送されます。

30.2.3 IPv4とIPv6の共存

インターネットに接続されている全ホストをIPv4からIPv6に移行する作業は、段階的に行われます。両方のプロトコルは今後しばらく共存することになります。両方のプロトコルをデュアルスタックで実装すれば、同じシステム上に共存することが保証されます。しかし、それでもなお、IPv6対応のホストがどのようにしてIPv4ホストと通信するか、また多くがIPv4ベースの現行ネットワークでIPv6パケットをどのように伝送するかなど、解決すべき問題が残ります。最善のソリューションは、トンネリングと互換アドレスです(30.2.2項「アドレスのタイプと構造」(607 ページ)を参照)。

ワールドワイドなIPv4ネットワークと隔離されているIPv6ホストは、トンネルを使って通信を行うことができます。IPv6パケットをIPv4パケットにカプセル化すれば、それをIPv4ネットワークに送ることができます。2つのIPv4ホスト間のこのような接続をトンネルと呼びます。これを行うには、パケットにIPv6の宛先アドレス(または対応するプレフィクス)とともに、トンネルの受信側にあるリモートホストのIPv4アドレスも含める必要があります。基本的なトンネルは、ホストの管理者間が合意すれば、手動で設定が可能です。これは、静的トンネリングとも呼ばれます。

ただし、静的トンネルの環境設定とメンテナンスは、あまりに手間がかかるので、多くの場合、日常の通信には向きません。そこで、IPv6は、動的トンネリングを実現する3つの異なる方法を提供しています。

6over4

IPv6パケットが自動的にIPv4パケットとしてカプセル化され、マルチキャスト対応のIPv4ネットワークによって送信されます。IPv6は、ネットワーク全体(インターネット)を巨大なLAN(local area network)だと思い込んで動作することになります。これにより、IPv4トンネルの着信側の端を自動的に判定できます。ただし、この方法は拡張性に欠けているだけではなく、IPマルチキャストがインターネット上で広く普及しているとはいえないという事実も障害となります。したがってこの解決方法を採用できるのは、マルチキャストが利用できる小規模な企業内ネットワークだけです。この方式の仕様は、RFC 2529に規定されています。

6to4

この方式では、IPv6アドレスからIPv4アドレスを自動的に生成することで、隔離されたIPv6ホストがIPv4ネットワーク経由で通信できるようにします。しかし、隔離されたIPv6ホストとインターネットの間の通信に関して、多くの問題が報告されています。この方式は、RFC 3056で規定されています。

IPv6トンネルブローカ

この方式は、IPv6ホスト専用のトンネルを提供する特殊なサーバに依存します。この方式は、RFC 3053で規定されています。

30.2.4 IPv6の設定

通常、IPv6を設定するために、個々のワークステーションの設定を変更する必要はありません。IPv6は、デフォルトで有効になっています。インストール時にネットワーク設定ステップで、これを無効にすることができます。3.14.3項「**ネットワーク設定**」(44 ページ)を参照してください。インストール済みシステムでIPv6を有効または無効にするには、YaSTの「ネットワークカード」を使用します。メソッドを変更せずに、「次へ」をクリックしてください。次にカードを選択して、「アドレス」タブで「詳細設定」>「IPv6」の順にクリックします。IPv6を手作業で有効にするには、rootとして`modprobe ipv6`と入力します。

IPv6の自動環境設定の概念があるため、ネットワークカードには、リンクローカルネットワーク内のアドレスが割り当てられます。通常、ワークステーション上ではルーティングテーブルの管理を実行しません。ワークステーションは、ルータアダプタイズプロトコルを使用して、実装する必要のあるプレフィクスとゲートウェイをネットワークルータに問い合わせます。IPv6ルータは、`radvd`プログラムを使用して設定できます。このプログラムは、IPv6アドレスに使用するプレフィクスとルータをワークステーションに通知します。または、`zebra`を使用してアドレスとルーティングを自動環境設定することもできます。

詳細については、`ifup(8)`のmanマニュアルページを参照してください。`/etc/sysconfig/network`ファイルを使用してさまざまなタイプのトンネルを設定する方法が説明されています。

30.2.5 詳細情報

ここでの概要は、IPv6に関する情報を網羅しているわけではありません。IPv6の詳細については、次のオンラインドキュメントや書籍を参照してください。

<http://www.ipv6.org/>

IPv6のあらゆる情報にここからリンクできます。

<http://www.ipv6day.org>

独自のIPv6ネットワークを開始するには、すべての情報が必要です。

<http://www.ipv6-to-standard.org/>

IPv6対応製品のリスト。

<http://www.bieringer.de/linux/IPv6/>

Linux IPv6-HOWTOと多くの関連トピックへのリンクが用意されています。

RFC 2640

IPv6に関する基本的なRFCです。

IPv6 Essentials

Silvia Hagenによる*IPv6 Essentials* (ISBN 0-596-00125-8)は、このトピックに関するあらゆる重要な面を扱っている本です。

30.3 ネームレゾリューション

DNSはIPアドレスに1つまたは複数のホスト名を割り当てるとともに、ホスト名をIPアドレスに割り当てます。Linuxでは、この変換は通常、bindという特別な種類のソフトウェアによって行われます。また、この変換を行うマシンをネームサーバと呼びます。ホスト名は、その名前構成要素がピリオド(.)で区切られた階層システムを構成しています。しかしながら名前の階層構造は、先に述べたIPアドレスの階層構造とは無関係です。

hostname.domainという形式で書かれた完全な名前、たとえば、earth.example.comを考えてみましょう。完全修飾ドメイン名(FQDN: *fully qualified domain name*)と呼ばれるフルネームは、ホスト名とドメイン名

(example.com)で構成されます。ドメイン名には最上位ドメイン(TLD) (de)が含まれます。

TLDの割り当ては、これまでの経緯もあって、非常に複雑になっています。従来から、米国では、3文字のドメイン名が使用されています。他の国では、ISOで制定された2文字の国コードが標準です。これに加えて、2000年には、特定の活動領域を表す、より長いTLDが導入されました(たとえば、.info、.name、.museum)。

インターネットの初期(1990年より前)には、ファイル/etc/hostsに、インターネットで利用されるすべてのマシン名を記述していました。しかし、インターネットに接続されるコンピュータ数の急激な増加により、この方法はすぐに現実的でなくなりました。このため、ホスト名を広く分散して保存するための分散データベースが開発されました。このデータベースは、ネームサーバと同様、インターネット上のすべてのホストに関するデータがいつでも用意されているわけではなく、他のネームサーバに問い合わせを行います。

この階層の最上位には、複数のルートネームサーバがあります。ルートネームサーバは、Network Information Center (NIC)によって運用されており、最上位レベルドメインを管理します。各ルートネームサーバは、特定の最上位ドメインを管理するネームサーバについての情報を持っています。最上位ドメインNICの詳細については、<http://www.internic.net>を参照してください。

DNSには、ホスト名の解決以外の機能もあります。ネームサーバには、特定のドメイン宛の電子メールをどのホストに転送するかも管理しています(メールエクスチェンジャ(MX))。

マシンがIPアドレスを解決するには、少なくとも1台のネームサーバとそのIPアドレスを知っている必要があります。YaSTを使用すれば、このようなネームサーバを簡単に指定できます。モデムを使ったダイヤルアップ接続の場合は、ネームサーバを手動で設定する必要はありません。接続が設定されるときに、ダイヤルアッププロトコルによってネームサーバのアドレスが提供されるからです。SUSE Linux Enterprise®でのネームサーバアクセスの環境設定については、**第33章 ドメインネームシステム** (673 ページ)を参照してください。

whoisプロトコルは、DNSと密接な関係があります。このプログラムを使用すると、特定のドメインの登録者名をすぐに検索できます。

注意: MDNSおよび.localドメイン名

.localトップレベルドメインは、リゾルバではリンクローカルドメインとして処理されます。DNS要求は通常のDNS要求ではなく、マルチキャスト要求として送信されます。ネームサーバ構成で.localドメインをすでに使用している場合は、このオプションを/etc/host.confでオフに変更する必要があります。host.confマニュアルページも参照してください。

インストール中にMDNSをオフにするには、nomdns=1をブートパラメータとして使用してください。

マルチキャストDNSの詳細は、<http://www.multicastdns.org>を参照してください。

30.4 YaSTによるネットワーク接続の設定

Linuxでは多くのタイプのネットワーク接続がサポートされています。その多くは、異なるデバイス名と、ファイルシステム内の複数の場所に分散した設定ファイルを使用しています。手動によるネットワーク設定のさまざまな面についての詳細は、[30.7項「ネットワークの手動環境設定」](#) (640ページ)を参照してください。

インストール中に、YaSTは検出したすべてのインタフェースを自動的に設定します。インストール済みのシステムの付加的なハードウェアは、インストール後に設定することができます。以下のセクションでは、SUSE Linux Enterpriseがサポートするすべてのタイプのネットワーク接続について、その設定方法を説明します。

ティップ: IBM System z: ホットプラグ対応ネットワークカード

IBM System zプラットフォームでは、ホットプラグ可能なネットワークカードがサポートされていますが、DHCPを介したネットワークの自動統合は(PCの場合とは異なり)サポートされていません。検出後はインタフェースを手動で設定してください。

30.4.1 YaSTでのネットワークカードの設定

YaSTで無線/有線ネットワークカードを設定するには、[\[ネットワークデバイス\]](#) > [\[ネットワークカード\]](#) の順に選択します。モジュールを起動すると、YaSTの汎用のネットワーク設定ダイアログが表示されます。すべてのネットワークデバイスを管理するのにYaSTか、NetworkManagerのいずれを使用するかを選択します。YaSTを使用して従来の方法でネットワークを設定する場合は、[\[ifupを使用した従来の方法\]](#) を選択して、[\[次へ\]](#) をクリックします。NetworkManagerを使用するには、[\[NetworkManagerでユーザを制御\]](#) を選択して、[\[次へ\]](#) をクリックします。NetworkManagerの詳細は、[30.6項「NetworkManagerを使用したネットワーク接続の管理」](#) (638 ページ)を参照してください。

注意: ネットワーク設定方法とXen

NetworkManagerは、Xenと一緒に利用できません。Xenでは、[\[ifupを使用した従来の方法\]](#) のみを利用できます。

ダイアログの上部に、設定に使用可能なすべてのネットワークカードのリストが表示されます。正しく検出されたカードであれば、その名前が表示されます。選択したデバイスの設定を変更するには、[\[編集\]](#) をクリックします。[検出されないネットワークカードの設定項](#) (623 ページ)で説明されているように、検出できなかったデバイスも、[\[追加\]](#) を選択して設定できます。

図 30.3 ネットワークカードの設定

IPアドレスが不要な場合は、[IPアドレスなし]を選択します。

ローカルネットワークでDHCPサーバが作動中の場合は、[自動アドレス設定]を選択できます。

ケーブルまたはDSLのプロバイダからスタティックダイナミックでないIPアドレスを取得できない場合にも、これを選択してください。

そうすることで、ネットワークアドレスは自動的にサーバから与えられます。

ダイナミック割り当てを使用しない場合は、ネットワークのアドレスを手動で設定しなければなりません。

コンピュータのIPアドレス(たとえば192.168.1.100.99)、ネットワークマスク(通常は255.255.255.0)、デフォルトゲートウェイのIPアドレス(オプション)を入力してください。

[次へ]をクリックすると、環境設定が完了します。

ネットワークの環境設定の詳細については、ネットワーク管理者に問い合わせてください。

ネットワークアドレスの設定

一般(G) アドレス(A)

デバイスの型(D) 選択設定名(C)

イーサネット 00:0c:29:85:1e:c8

☐ IPアドレスなし(ボンDEDデバイス)

☒ 自動アドレス設定(DHCPを介して)(U)

☐ スタティックなアドレスの設定(I)

IPアドレス(I)

サブネットマスク(M)

詳細設定

ホスト名とドメイン名(H)

ルーティング(Q)

詳細設定(A)...

戻る(B) 中止(E) 次へ(N)

ネットワークカードの設定の変更

ネットワークカードの設定を変更するには、YaSTネットワークカード設定モジュールの検出されたカードのリストから目的のカードを選択して、**[編集]**をクリックします。**[ネットワークアドレス設定]**ダイアログが表示されます。このダイアログの**[アドレス]**および**[一般]**タブを使って、カードの設定を変更します。無線カードの設定については、[29.1.3項「YaSTでの設定」](#)(588 ページ)を参照してください。

IPアドレスの設定

DHCPを利用できる場合、インストール時に、有線ネットワークカードは自動的にDHCPを使うように設定されます。

注意: IBM System zとDHCP

IBM System zプラットフォームでは、DHCPベースのアドレス設定はMACアドレスを持つネットワークカードの場合にのみサポートされます。これに該当するのは、OSAカードおよびOSA Expressカードだけです。

ISPからスタティックIPが割り当てられていないDSL回線を使用している場合も、DHCPを使用する必要があります。DHCPを使用する場合は、*[DHCPクライアントオプション]* を選択して詳細を設定します。このダイアログを表示するには、*[アドレス]* タブで *[詳細]* > *[DHCP Options]* の順に選択します。DHCPサーバが常にブロードキャストリクエストを受け付けるかどうか、および使用するIDを指定します。さまざまなホストが同じインタフェースを介して通信するようにバーチャルホストがセットアップされている場合は、各ホストの識別にIDが必要になります。

DHCPは、クライアント設定には適していますが、サーバ設定には適していません。静的なIPアドレスを設定するには、以下の手順に従ってください。

- 1 YaSTネットワークカード設定モジュールの検出されたカード一覧から目的のカードを選択し、*[編集]* をクリックします。
- 2 *[アドレス]* タブで、*[スタティックなアドレスの設定]* を選択します。
- 3 *[IPアドレス]* と *[サブネットマスク]* に適切な値を入力します。
- 4 *[Next]* をクリックします。
- 5 環境設定を有効にするには、*[完了]* をクリックします。

静的アドレスを使用する場合、ネームサーバとデフォルトゲートウェイは、自動的に設定されません。ゲートウェイを設定するには、*[ルーティング]* をクリックしてデフォルトのゲートウェイを追加してください。ネームサーバを設定するには、*[ホスト名とネームサーバ]* をクリックしてネームサーバのアドレスとドメインを追加してください。

エイリアスの設定

1台のネットワークデバイスに、複数のIPアドレスを割り当てることをできます。追加するIPアドレスは、エイリアスと呼ばれます。ネットワークカードにエイリアスを設定するには、以下の手順に従ってください。

- 1 YaSTネットワークカード設定モジュールの検出されたカード一覧から目的のカードを選択し、*[編集]* をクリックします。
- 2 *[アドレス]* タブで、*[詳細]* > *[Additional Addresses(他のアドレス)]* の順に選択します。

- 3 *[Add]* をクリックします。
- 4 *[Alias Name(エイリアス名)]*、*[IPアドレス]*、および *[ネットマスク]* に適切な値を入力します。
- 5 *[OK]* をクリックします。
- 6 もう一度*[OK]*をクリックします。
- 7 *[Next]*をクリックします。
- 8 環境設定を有効にするには、*[完了]* をクリックします。

ホスト名とDNSの設定

有線ネットワークカードが利用できる状態で、インストール時にネットワーク設定を変更しなかった場合、コンピュータのホスト名が自動的に生成され、DHCPが有効になります。また、ホストがネットワークに参加するために必要なネームサービス情報も自動的に生成されます。ネットワークアドレス設定にDHCPを使用している場合は、ドメインネームサーバのリストは自動的に記入されます。静的設定を利用する場合は、これらの項目を手動で設定してください。

コンピュータ名を変更し、ネームサーバの検索リストを修正するには、以下の手順に従ってください。

- 1 YaSTネットワークカード設定モジュールの検出されたカード一覧から目的のカードを選択し、*[編集]* をクリックします。
- 2 *[アドレス]* タブで、*[Hostname and Name Server]* をクリックします。
- 3 DHCPを使ったホスト名の設定を無効にするには、*[DHCP経由でのホスト名の変更]* の選択を解除します。
- 4 *[ホスト名]* にホスト名を入力し、必要に応じて *[ドメイン名]* にドメイン名を入力します。
- 5 DHCPを使ったネームサーバリストの更新を無効にする場合は、*[DHCP経由でのネームサービスおよび検索リストの更新]* の選択を解除します。

- 6 ネームサーバ名とドメイン検索リストを設定します。
- 7 **[OK]** をクリックします。
- 8 **[Next]** をクリックします。
- 9 環境設定を有効にするには、**[完了]** をクリックします。

ルーティングの設定

コンピュータを他のコンピュータやネットワークと通信させるには、ネットワークトラフィックが正しい経路を通過するように、ルーティング情報を設定する必要があります。DHCPを使用している場合、この情報は自動的に設定されます。静的アドレスを使用する場合は、このデータを手作業で追加する必要があります。

- 1 YaSTネットワークカード設定モジュールの検出されたカード一覧から目的のカードを選択し、**[編集]** をクリックします。
- 2 **[アドレス]** タブで、**[ルーティング]** をクリックします。
- 3 **[デフォルトゲートウェイ]** のIPアドレスを指定します。
- 4 **[OK]** をクリックします。
- 5 **[Next]** をクリックします。
- 6 環境設定を有効にするには、**[完了]** をクリックします。

特殊なハードウェアオプションの追加

ネットワークカードによっては、正常に利用するために特別なパラメータを指定しなければならないこともあります。YaSTを使って特別なパラメータを設定するには、次の手順に従います。

- 1 YaSTネットワークカード設定モジュールの検出されたカード一覧から目的のカードを選択し、**[編集]** をクリックします。
- 2 **[アドレス]** タブで、**[詳細]** > **[Hardware Details]** の順にクリックします。

- 3 [オプション] に、ネットワークカードに必要なパラメータを入力します。同じモジュールを使うカードが2つ設定されている場合、ここに入力したパラメータは両方のカードで使われます。
- 4 [OK] をクリックします。
- 5 [Next] をクリックします。
- 6 環境設定を有効にするには、[完了] をクリックします。

デバイスの起動

ifupを使った従来の方法を使用している場合、デバイスをブート時、ケーブル接続時、カード検出時、または手動で起動するように設定したり、起動しないように設定することができます。デバイスの起動方法を変更するには、以下の手順に従ってください。

- 1 YaSTネットワークカード設定モジュールの検出されたカード一覧から目的のカードを選択し、[編集] をクリックします。
- 2 [一般] タブの [デバイスの起動] から、適切な項目を選択します。
- 3 [Next] をクリックします。
- 4 環境設定を有効にするには、[完了] をクリックします。

ファイアウォールの設定

43.4.1項「YaSTを使ったファイアウォールの設定」(900ページ)で説明しているような詳細なファイアウォール設定を行わずに、デバイスに基本的なファイアウォールを設定することができます。次の手順に従います。

- 1 YaSTネットワークカード設定モジュールの検出されたカード一覧から目的のカードを選択し、[編集] をクリックします。
- 2 ネットワーク設定ダイアログの [一般] タブを表示します。
- 3 インタフェースを割り当てるファイアウォールゾーンを指定します。次のオプションを指定できます。

ゾーンなし、すべてのトラフィックをブロックする
このインタフェースのすべてのトラフィックがブロックされます。

内部ゾーン(未保護)

ファイアウォールを実行しますが、このインタフェースを保護するルールは使いません。コンピュータが、外部ファイアウォールにより保護されているネットワークに接続している場合にのみ、このオプションを使用してください。

非武装地帯(DMZ)

非武装地帯ゾーンは、内部ネットワークと(悪意のある)インターネットとの中間にあたるゾーンです。このゾーンに割り当てられたホストは、内部ネットワークおよびインターネットからアクセスされますが、ホストから内部ネットワークにアクセスすることはできません。

外部ゾーン

このインタフェースでファイアウォールを実行し、(危険な可能性のある)他のネットワークトラフィックからインタフェースを保護します。これはデフォルトの設定です。

4 [Next]をクリックします。

5 環境設定を有効にするには、[完了]をクリックします。

検出されないネットワークカードの設定

ネットワークカードが正しく検出されないこともあります。このような場合、検出されたカードのリストに、そのカードは表示されません。システムにそのカード用のドライバが間違いなく含まれている場合は、そのようなカードを手動で設定することができます。検出されなかったネットワークカードを設定するには、以下の手順に従ってください。

1 [Add] をクリックします。

2 インタフェースの [デバイスの型]、[Configuration Name]、および [Module Name] に、それぞれ適切な値を設定します。ネットワークカードが、PCMCIAデバイスかUSBデバイスの場合、[ネットワークカードの手動設定] ダイアログで、[PCMCIA] または [USB] チェックボックスを選択して、[次へ] をクリックしてダイアログを終了します。そ

れ以外の場合には、[*Select from List*]でネットワークカードの型式を選択します。YaSTは自動的に、そのカードに適したカーネルモジュールを選択します。

[*Hardware Configuration Name*] では、ネットワークカードのハードウェア設定を記述する `/etc/sysconfig/hardware/hwcfg-*` ファイルの名前を指定します。この名前には、カーネルモジュールの名前や、ハードウェアを初期化するために必要なオプションがあります。

3 [Next]をクリックします。

4 [アドレス] タブで、インタフェースのデバイスタイプ、設定名、およびIPアドレスを設定します。静的なアドレスを使用する場合は、[ステティックなアドレスの設定] を選択して、[IP アドレス] と [サブネットマスク] を入力します。ここでは、ホスト名、ネームサーバ、およびルーティングの詳細を設定することもできます(**ホスト名とDNSの設定項** (620 ページ)と**ルーティングの設定項** (621 ページ)を参照)。

インタフェースのデバイスタイプとして、[無線] を選択した場合は、次のダイアログで無線接続の設定を行います。無線デバイスの設定方法の詳細は、**29.1項 「無線LAN」** (583 ページ)を参照してください。

5 [一般] タブで、[ファイアウォールゾーン] と [デバイスの起動] を設定します。[ユーザコントロール] では、一般ユーザへの接続コントロールを許可します。

6 [Next]をクリックします。

7 ネットワーク設定を有効にするには、もう一度 [完了] をクリックします。

設定名の命名規則については、`getcfg(8)` のマニュアルページを参照してください。

30.4.2 Modem

ティップ: IBM System z:モデム

このタイプのハードウェアの設定は、IBM System zプラットフォームではサポートされていません。

YaSTコントロールセンターで、[ネットワークデバイス] > [モデム] の順に選択して、モデム設定にアクセスします。モデムが自動的に検出されない場合は、[追加] をクリックして手動設定用のダイアログを開きます。開いたダイアログの [モデムデバイス] に、モデムの接続先インタフェースを入力します。

ティップ: CDMAおよびGPRSモデム

YaSTのモデムモジュールを使って、通常のモデムの設定と同様に、サポートするCDMAおよびGPRSモデムを設定します。

図 30.4 モデム設定

すべてのモデム環境設定値を入力してください。

[モデムデバイス]には、モデムが接続されているポートを入力します。DOS/Windows上では、ttyS0、ttyS1などはシリアルポートで、通常はCOM1、COM2などに対応し、ttyACM0、ttyACM1はUSBポートです。

PBXを使用する場合は、[ダイヤルプレフィックス]に番号を入力する必要があります。多くの場合、この番号は9または0になります。

電話回線に接続して「ダイヤルモード」を選択してください。ほとんどの電話会社は、ダイヤルモードとしてトーンダイヤル方式を使用しています。モデムのスピーカーをオンにする場合（[モデムのスピーカーを動作させる]）や発信音を検出する場合（[電話の発信音を検出する]）は、それぞれのチェックボックスをオンにしてください。

[詳細]をクリックすると、ポートとモデム初期化文字列を環境設定できます。

モデムのパラメータ

モデムデバイス (D)

/dev/modem

ダイヤルプレフィックス (必要時のみ) (X)

ダイヤルモード

☒ トーンダイヤル方式 (D)

☐ パルスダイヤル方式 (D)

特別の設定

☒ モデムのスピーカーを動作させる (S)

☒ 電話の発信音を検出する (E)

詳細 (D)

戻る (B) 中止 (E) 次へ (N)

構内交換機(PBX)経由で接続している場合は、ダイヤルプレフィックスの入力が必要な場合があります。通常、このプレフィックスは0(ゼロ)です。PBX付

属の指示書で確認してください。また、トーンダイヤル方式とパルスダイヤル方式のどちらを使用するか、スピーカをオンにするかどうか、およびモデムをダイヤルトーンの検出まで待機させるかどうかを選択します。モデムが交換機に接続されている場合、後者のオプションは無効です。

[詳細] で、ボーレートとモデムの初期化文字列を設定します。これらの設定は、モデムが自動検出されなかった場合、またはデータ転送を動作させるために特殊な設定が必要な場合にのみ変更してください。これは、主にISDN端末アダプタを使用する場合です。[OK] をクリックしてこのダイアログを閉じます。モデムの制御権をroot権限のない通常のユーザに委任するには、[ユーザコントロール] を有効にします。このようにすると、管理者権限のないユーザがインタフェースを有効化または無効化できるようになります。[Dial Prefix Regular Expression] には、正規表現を指定します。この正規表現とKInternetで設定する[ダイヤルプレフィックス] が一致する必要があります。このフィールドを空のままにした場合、管理者権限のないユーザは[ダイヤルプレフィックス] を変更できません。

次のダイアログで、ISP(インターネットサービスプロバイダ)を選択します。事前定義済みの国内ISPリストから選択するには、[国] を選択します。または、[新規] をクリックしてダイアログを開き、独自ISPのデータを入力します。これには、ダイヤルアップ接続名、ISP名、ISPから提供されるログインとパスワードが含まれます。接続するたびにパスワードを要求させるには、[常にパスワードを要求する] を選択します。

最後のダイアログでは、次のようにその他の接続オプションを指定できます。

[必要に応じてダイヤルする]

ダイヤルオンデマンドを有効にする場合は、ネームサーバを少なくとも1つ指定します。

[接続時にDNSを変更する]

このオプションはデフォルトでオンになっていて、インターネットに接続するたびにネームサーバアドレスが更新されます。

[自動でDNS情報を取得]

接続後にプロバイダからドメインネームサーバの情報が送信されない場合は、このオプションをオフにしてDNSの情報を手動で入力します。

[スチューピッドモード]

デフォルトでは、このオプションは有効になっています。その場合、接続プロセスを妨げないように、ISPのサーバから送信される入力プロンプトは無視されます。

External Firewall Interface(外部ファイアウォールインタフェース)

このオプションを選択すると、SUSEfirewall2が有効になり、インタフェースが外部として設定されます。このようにして、システムはインターネット接続時に外部からの攻撃から保護されます。

[アイドルタイムアウト(秒)]

このオプションでは、ネットワークがアイドル状態になってからモデムが自動的に切断されるまでの時間を指定します。

[IP Details(IP詳細設定)]

このオプションを選択すると、アドレス設定ダイアログが開きます。ISPからホストにダイナミックIPアドレスが割り当てられていない場合は、[ダイナミックIPアドレス]を無効にして、ホストのローカルIPアドレスとリモートIPアドレスを入力します。この情報については、ISPにお問い合わせください。[デフォルトルート]は有効なままにし、[OK]を選択してダイアログを閉じます。

[次へ]を選択すると、元のダイアログに戻り、モデム設定の概要が表示されます。[完了]を選択し、このダイアログを閉じます。

30.4.3 ISDN

ティップ: IBM System z: ISDN

このタイプのハードウェアの設定は、IBM System zプラットフォームではサポートされていません。

このモジュールは、システムの1つ以上のISDNカードを設定します。YaSTによってISDNカードが検出されなかった場合は、[\[追加\]](#) をクリックして手動で選択してください。複数のインタフェースを設定することも可能ですが、1つのインタフェースに複数のISPを設定することも可能です。以降のダイアログでは、カードが正しく機能するために必要なISDNオプションを設定します。

図 30.5 ISDNの設定

実行モード: [起動中] を選択すると、ドライバはシステムブート時にロードされます。[手動] を選択した場合は、ルートユーザが「iscnstart」コマンドを使用してドライバを起動する必要があります。[オプション] は、PCMCIAおよびUSBデバイスを使用する場合の特別なオプションです。

ISDNプロトコル: 多くの場合、Euro-SDNを使用します。

局番: ISDNの局番を入力してください。最初の02の局番等は必要ありません。

ダイヤルプレフィックス: 外線へ接続するためにダイヤルプレフィックスが必要な場合は、ここで入力してください。これは内部の50xバスでのみ使用され、通常は「0」です。

ISDNトラフィックを記録しない場合は、[ISDN記録を開始する]を選択解除してください。

[デバイスの起動]では、ネットワークインタフェースをいつ起動するかを選択してください。[ブート時]を選択すると、インタフェースはシステムブート中に起動されます。[起動しない]を選択すると、

control に関するISDNの低レベルの環境設定

ISDNカードの情報

ベンダ Abocom/Magitek

ISDNカード 2BD1

ドライバ(D) HISax driver

ISDNプロトコル

☒ Euro-SDN (EDSS1) (E)

☐ ITR6 (R)

☐ 専用回線 (L)

☐ NI1 (I)

国 (C) ドイツ

コード (D) 49

市外局番 (A)

ダイヤルプレフィックス (D)

☒ ISDN記録を開始する (I)

デバイスの起動 (D) ブート時

戻る(B) 中止(B) OK(O)

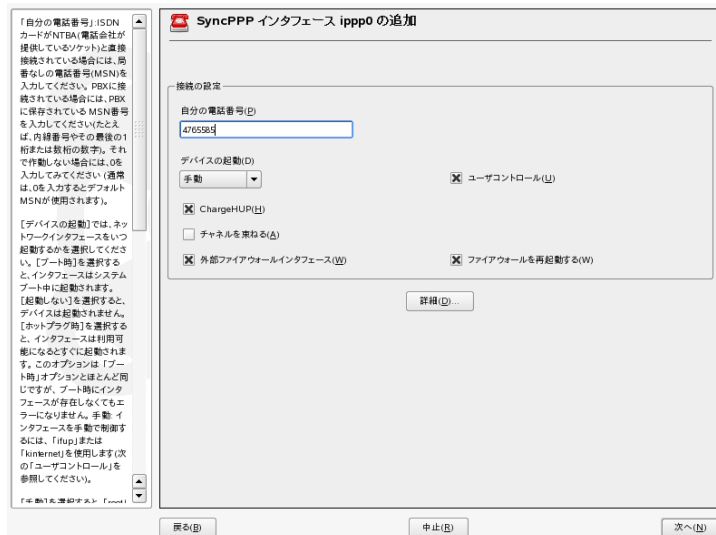
図 30.5. 「ISDNの設定」 (628 ページ)に示すダイアログでは、使用するプロトコルを選択します。デフォルトは、[\[Euro-SDN \(EDSS1\)\]](#) ですが、旧式または大型の交換機の場合は、[\[ITR6\]](#) を選択します。米国では、[\[NI1\]](#) を選択します。関連するフィールドで国を選択してください。隣接するフィールドに対応する国コードが表示されます。最後に、必要に応じて [\[Area Code \(市外局番\)\]](#) と [Dial Prefix \(ダイヤルプレフィックス\)](#) を入力します。

[*デバイスの起動*] は、ISDNインタフェースの起動方法を定義します。 [*At Boot Time*] (ブート時)を選択すると、システムブート時にISDNドライバが毎回初期化されます。 [*Manually*] を選択した場合は、rootとしてrcisdn startコマンドを実行して、ISDNドライバをロードする必要があります。

[*On Hotplug*] は、PCMCIAやUSBデバイスに使用します。デバイスを装着したときにドライバがロードされます。これらの設定が完了したら、 [*OK*] を選択します。

次のダイアログでは、ISDNカードのインタフェースタイプを指定し、既存のインタフェースにISPを追加します。インタフェースタイプには、SyncPPPまたはRawIPのどちらかを指定できますが、たいていのISPは、SyncPPPモードで運用しています。このモードについては後述します。

図 30.6 ISDNインタフェースの設定



[*自分の電話番号*] に入力する番号は、次の設定によって異なります。

電話線引出口に直接接続されたISDNカード

標準のISDN回線では、3つの電話番号を使用できます(MSN(multiple subscriber number)と呼ばれる)。加入者によっては、最大10個まである場合もあります。これらの電話番号の1つをここに入力します。ただし、市外局番は入力しないでください。間違った番号を入力すると、お使いの

ISDN回線に付与された最初のMSNが、電話交換手によって自動的に使用されます。

PBX (Private Branch Exchange)に接続されたISDNカード

この場合も、設定方法は設置された装置によって異なります。

1. 小型のPBX (private branch exchanges)ではたいてい、内線通話にEuro-ISDN (EDSS1)プロトコルを使用します。これらの交換機にはS0バスが内蔵されており、交換機に接続された装置に内線番号を付与します。

内線番号の1つをMSNとして使用してください。外線用に付与されたMSNの少なくとも1つは外線用に使用できるはずですが、もし使用できない場合は、1つのゼロを試してください。詳細については、交換機付属のマニュアルを参照してください。

2. ビジネス向けに設計された大型の交換機では通常、内線通話に1TR6プロトコルを使用します。このタイプの交換機に付与されるMSNはEAAZと呼ばれ、通常直通番号に対応しています。Linuxでの設定では、EAAZの最後の数字を入力するだけで十分なはずですが、どうしてもうまくいかない場合は、1から9までの数字をすべて試してみてください。

次の課金単位の直前に接続を切断するようにする場合は、[ChargeHUP(課金HUP)]を有効にします。ただし、このオプションはすべてのISPで使用できるわけではないため注意してください。チャネルバンドル(マルチリンクPPP)を有効にするオプションも用意されています。最後に、使用している回線でSuSEfirewall2を有効にするには、[External Firewall Interface]と[Restart Firewall]を選択します。管理者権限のない通常のユーザがインタフェースの有効化と無効化を行えるようにするには、[ユーザコントロール]を選択します。

[詳細]でダイアログが開き、コールバックモード、このインタフェースへのリモート接続、追加のippdオプションを設定できます。[OK]をクリックして[Details]ダイアログを閉じます。

次のダイアログでは、IPアドレスを設定します。プロバイダからスタティックなIPアドレスを与えられていない場合は、[ダイナミックIPアドレス]を選択します。スタティックなIPアドレスを与えられている場合は、ISPの指示に従って、ホストのローカルIPアドレスとリモートIPアドレスを該当するフィールドに入力します。このインタフェースをインターネットへのデフォルトルートにする必要がある場合は、[デフォルトルート]を選択します。各ホスト

は、デフォルトルートとして設定されたインタフェースを1つだけ持つことができます。[次へ] をクリックして次のダイアログに進みます。

次のダイアログでは、国を設定し、ISPを選択できます。リストに登録されているISPは、call-by-callプロバイダだけです。契約しているISPがリストに登録されていない場合は、[新規] を選択します。[プロバイダパラメータ] ダイアログが開き、契約しているISPの詳細な情報を入力できます。電話番号を入力するときは、各数字の間に空白やカンマを挿入しないように注意してください。最後に、ISPから提供されたログインIDとパスワードを入力します。入力したら、[次へ] をクリックします。

スタンドアロンワークステーションで[必要に応じてダイヤルする] を使用するには、ネームサーバ(DNSサーバ)も指定します。ほとんどのISPはダイナミックDNSをサポートしており、接続するたびにISPからネームサーバのIPアドレスが送信されます。ただし、単一ワークステーションの場合は、192.168.22.99のようなブレースホルダアドレスを入力してください。ISPがダイナミックDNSをサポートしていない場合は、ISPから提供されたネームサーバIPアドレスを入力します。必要に応じて、接続タイムアウト、すなわち、ネットワークがアイドル状態になってから接続を自動的に切断するまでの時間(秒)を指定します。[次へ] をクリックすると設定が確定し、YaSTは、設定されたインタフェースの概要を表示します。すべての設定を有効にするには、[完了] を選択します。

30.4.4 ケーブルモデム

ティップ: IBM System z:ケーブルモデム

このタイプのハードウェアの設定は、IBM System zプラットフォームではサポートされていません。

オーストリアや米国など、一部の国では、ケーブルテレビネットワークを介したインターネット接続が広く普及しています。ケーブルテレビ加入者は通常、モデムを貸与されます。このモデムは、ケーブルテレビの引出線とネットワークカード(10Base-TGより対線を使用)に接続して使用します。ケーブルモデムを接続すると、固定IPアドレスが付与されたインターネット専用接続が提供されます。

契約しているISPから、ネットワークカードを設定する際に、[自動アドレス設定(DHCPを介して)] または[スタティックなアドレスの設定] のどちらか

を選択するように指示があります。最近では、大半のプロバイダがDHCPを使用しています。スタティックなIPアドレスは、多くの場合、特殊なビジネス用アカウントの一部として提供されます。

ケーブルモデムの設定に関する詳細については、http://en.opensuse.org/SDB:Setting_Up_an_Internet_Connection_via_Cable_Modem_with_SuSE_Linux_8.0_or_Higherにある、サポートデータベースの記事を参照してください。

30.4.5 DSL

ティップ: IBM System z: DSL

このタイプのハードウェアの設定は、IBM System zプラットフォームではサポートされていません。

DSLデバイスを設定するには、YaSTの [ネットワークデバイス] セクションから [DSL] モジュールを選択します。このモジュールは、次のいずれかのプロトコルに基づいてDSLリンクのパラメータを設定する複数のダイアログで構成されます。

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoATM)
- CAPI for ADSL (Fritz Cards)
- ポイントツーポイントトンネリングプロトコル(PPTP)—オーストリア

PPPoEまたはPPTPに基づくDSL接続を設定するには、対応するネットワークカードが正しく設定されている必要があります。ネットワークカードをまだ設定していない場合は、はじめに、[ネットワークカードの設定] を選択してカードを設定してください(30.4.1項「YaSTでのネットワークカードの設定」(617 ページ)参照)。DSLリンクの場合は、IPアドレスが自動的に割り当てられる場合もありますが、その場合でもDHCPは使用されません。そのため、[自動アドレス設定(DHCPを介して)] オプションを有効にしないでください。その代わりに、スタティックなダミーアドレス(192.168.22.1など)をインタフェースに入力します。[サブネットマスク] には、「255.255.255.0」

ミックDNSをサポートしており、接続するたびにISPからネームサーバのIPアドレスが送信されます。ただし、単一ワークステーションの場合は、192.168.22.99のようなプレースホルダアドレスも入力する必要があります。ISPがダイナミックDNSをサポートしていない場合は、ISPのネームサーバIPアドレスを指定してください。

[切断するまでのアイドル時間(秒数)] には、ネットワークがアイドル状態になってからモデムを自動的に切断するまでの時間を指定します。タイムアウト値としては、60秒～300秒が妥当です。[必要に応じてダイヤルする] を無効にしている場合は、このタイムアウト値をゼロに設定して自動的に接続が切断されないようにしておきます。

T-DSLの設定はDSLの設定とほぼ同じです。T-DSLの設定はDSLの設定とほぼ同じです。プロバイダとして [T-Online] を選択すると、T-DSL設定ダイアログが開きます。このダイアログで、T-DSLに必要な追加情報(ラインID、T-Online番号、ユーザコード、パスワードなど)を指定します。T-DSLに加入すると、プロバイダからこれらの情報がすべて提供されるはずです。

30.4.6 IBM System z: ネットワークデバイスの設定

IBM System z用のSUSE Linux Enterpriseは、さまざまな種類のネットワークインタフェースをサポートしています。これらのインタフェースは、YaSTを使って設定することができます。

qeth-hsiデバイス

[qeth-hsi] (Hipersocket)インタフェースをインストール済みのシステムに追加するには、YaSTネットワークカードモジュールを起動します([ネットワークデバイス] > [ネットワークカード] の順に選択)。READデバイスアドレスとして使用する [IBM Hipersocket] というマークの付いたデバイスの1つを選択して、[設定] をクリックします。[ネットワークアドレスの設定] ダイアログで、新しいインタフェースのIPアドレスとネットマスクを指定し、[次へ] および [完了] をクリックしてネットワークの設定を終了します。

qeth-ethernetデバイス

[qeth-ethernet] (IBM OSA Expressイーサネットカード)インタフェースをインストール済みのシステムに追加するには、YaSTネットワークカードモジュールを起動します([ネットワークデバイス] > [ネットワークカード]の順に選択)。READデバイスアドレスとして使用する[IBM OSA Expressイーサネットカード]というマークの付いたデバイスの1つを選択して、[設定]をクリックします。ポート名や他のオプション(http://www.ibm.com/developerworks/linux/linux390/documentation_novell_suse.htmlの『Linux for IBM System z: Device Drivers, Features, and Commands』マニュアルを参照)、IPアドレス、およびネットマスクを入力します。[次へ]、続いて[完了]をクリックして、ネットワークの設定を終了します。

ctcデバイス

[ctc] (IBMパラレルCTCアダプタ)インタフェースをインストール済みのシステムに追加するには、YaSTネットワークカードモジュールを起動します([ネットワークデバイス] > [ネットワークカード]の順に選択)。READデバイスアドレスとして使用する[IBMパラレルCTCアダプタ]というマークの付いたデバイスの1つを選択して、[設定]をクリックします。お使いのデバイスに合わせて[S/390デバイス設定]を選択します(通常は、[互換モード])。自IPアドレスとリモートのIPアドレスを指定します。必要に応じて、[詳細] > [詳細設定]の順に選択してMTUサイズを調整します。[次へ]、続いて[完了]をクリックして、ネットワークの設定を終了します。

警告

このインタフェースを使用することはお勧めしません。今後のSUSE Linux Enterpriseのリリースでは、このインタフェースはサポートされません。

lcsデバイス

[lcs] (IBMOSA-2アダプタ)インタフェースをインストール済みのシステムに追加するには、YaSTネットワークカードモジュールを起動します([ネットワークデバイス] > [ネットワークカード]の順に選択)。[IBM OSA-2アダプタ]というマークの付いたデバイスの1つを選択して、[設定]をクリックします。ポート番号や他のオプション(<http://www.ibm.com/>

developerworks/linux/linux390/documentation_novell_suse.htmlの『*Linux for IBM System z: Device Drivers, Features, and Commands*』マニュアルを参照)、IPアドレス、およびネットマスクを入力します。[次へ]、続いて[完了]をクリックして、ネットワークの設定を終了します。

IUCVデバイス

[lcs] (IBMOSA-2アダプタ)インタフェースをインストール済みのシステムに追加するには、YaSTネットワークカードモジュールを起動します([ネットワークデバイス] > [ネットワークカード] の順に選択)。[IUCV] というマークの付いたデバイスを選択し、[設定] をクリックします。IUCVパートナーの名前を入力するように要求されます。パートナー名(大文字小文字も区別する)を入力して、[次へ] をクリックします。自IPアドレスとリモートのIPアドレスを指定します。必要に応じて、[詳細] > [詳細設定] の順に選択してMTUサイズを調整します。[次へ]、続いて[完了] をクリックして、ネットワークの設定を終了します。

警告

このインタフェースを使用することはお勧めしません。今後のSUSE Linux Enterpriseのリリースでは、このインタフェースはサポートされません。

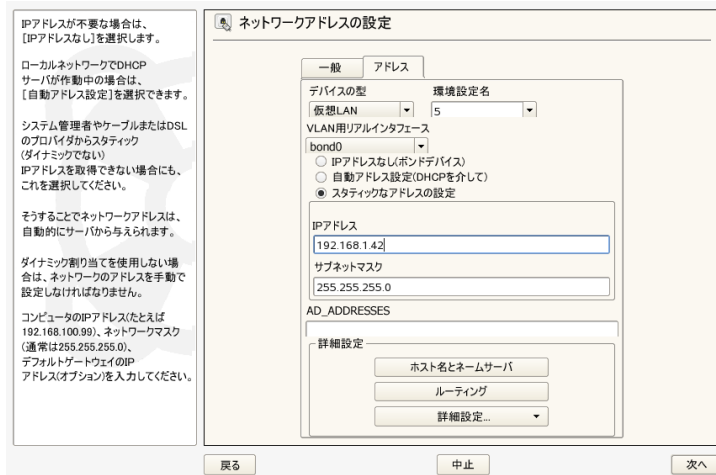
30.5 SUSE Linux上でのVLANインタフェースの設定

VLANは*Virtual Local Area Network*(仮想ローカルエリアネットワーク)の略です。複数の論理(仮想)Ethernetを1つの物理Ethernet上で実行できます。ネットワークを論理的に複数のブロードキャストドメインに分割し、パケットが同じVLANに指定されたポート間でのみ切り替えられるようにします。VLANをネットワークセットアップで使用する予定の場合、パッケージvlanをインストールしてください。

Linuxのネットワーク接続が特定の論理LAN専用ではない場合、これらの1つ以上の論理LANへアクセスを設定できます。VLANインタフェース設定は、その他すべてのネットワークインタフェースと同様、標準のifupとifdownスクリプト

リプトでサポートされています。VLANデバイスのセットアップはYaSTでサポートされています。

30.8 YaST VLANの設定



IPアドレスが不要な場合は、
[IPアドレスなし]を選択します。

ローカルネットワークでDHCP
サーバが作動中の場合は、
[自動アドレス設定]を選択できます。

システム管理者やケーブルまたはDSL
のプロバイダからスタティック
(ダイナミックでない)
IPアドレスを取得できない場合にも、
これを選択してください。

そうすることでネットワークアドレスは、
自動的にサーバから与えられます。

ダイナミック割り当てを使用しない場
合は、ネットワークのアドレスを手動で
設定しなければなりません。

コンピュータのIPアドレス(たとえば
192.168.100.99)、ネットワークマスク
(通常は255.255.255.0)、
デフォルトゲートウェイのIP
アドレス(オプション)を入力してください。

YaST モジュールで [ネットワークデバイス] > [ネットワークカード] を実行し、 [ifupを使用した従来の方法] を選択して [次へ] を選択します。次の手順に従って、実際にVLANデバイスをセットアップします。

手順 30.1 YaSTによるVLANインタフェースのセットアップ

- 1 [追加] をクリックして、新規ネットワークインタフェースを作成します。
- 2 [ネットワーク設定] で、 [デバイスの型] [仮想LAN] を選択します。
- 3 [環境設定名] の値をVLANのIDに変更します。VLAN IDの1は、通常は管理目的で使用されることに注意してください。
- 4 [次へ] をクリックします。
- 5 VLANが接続するインタフェースを [VLAN用リアルインタフェース] で選択します。

6 IPアドレスをVLANデバイスに割り当てるために使用する方法を選択します。

7 [次へ] をクリックして、設定を完了します。

VLANの詳細は、<http://www.candelatech.com/~greear/vlan.html> および `/usr/share/doc/packages/vlan/`にあるパッケージドキュメントを参照してください。

30.6 NetworkManagerを使用したネットワーク接続の管理

NetworkManagerは、モバイルワークステーションに理想的なソリューションです。NetworkManagerを利用すれば、場所を変更してもいちいちネットワークインタフェースを再設定して、ネットワークを切り替える手間を省くことができます。NetworkManagerは、自動的に既知のWLANネットワークに接続できます。2つ以上の接続がある場合は、速い方に接続します。

NetworkManagerは、以下の場合には適していません。

- 1つのインタフェースに対し、複数のダイアルアッププロバイダを使用する場合。
- コンピュータがネットワークのルータである場合。
- コンピュータが、DHCPまたはDNSサーバなど、ネットワーク内で他のコンピュータにネットワークサービスを提供している場合。
- コンピュータがXenサーバの場合、またはシステムがXen内の仮想システムの場合。
- ネットワーク設定管理にSCPMを使用する場合。SCPMとNetworkManagerを同時に使用する場合、SCPMはネットワークリソースを制御できません。.
- 1つ以上のアクティブなネットワーク接続を同時に使用する場合。

インストール時にNetworkManagerを有効または無効にするには、[ネットワーク設定] の [ネットワークモード] で、[NetworkManagerの有効化] または [NetworkManagerの無効化] をクリックします。インストール済みのシステムでNetworkManagerを有効化または無効化するには、次の手順に従います。

- 1 YaSTを開きます。
- 2 [ネットワークデバイス] > [Network Card] の順に選択します。
- 3 最初の画面で、[ネットワークのセットアップ方法] オプションを [NetworkManagerでユーザを制御] に設定して、NetworkManagerを使用するようにします。NetworkManagerを無効化するには、[ネットワークのセットアップ方法] を [ifupを使用した従来の方法] に設定します。

方法を選択したら、DHCP経由の自動設定または静的IPアドレスを使ってネットワークカードを設定するか、またはモデムを設定します。YaSTを使用したネットワーク接続の詳細については、[30.4項「YaSTによるネットワーク接続の設定」](#) (616 ページ)および[29.1項「無線LAN」](#) (583 ページ)を参照してください。NetworkManager内で直接、サポートされているワイヤレスカードを設定します。

NetworkManagerを設定するには、NetworkManagerアプレットを使用します。KDEとGNOMEには、それぞれNetworkManager用の独自のアプレットが用意されています。適切なアプレットが、デスクトップ環境で自動的に起動します。その後、このアプレットはシステムトレイ内にアイコンで表示されます。両アプレットの機能は類似していますが、インターフェースは多少異なります。また、標準のシステムトレイサポートのある他のグラフィカル環境でも使用できます。

30.6.1 ifupとNetworkManagerとの相違点

ネットワークセットアップにNetworkManagerを使用する場合、アプレットを使用するデスクトップ環境内からいつでも簡単にネットワーク接続を切り替え、停止または開始できます。NetworkManagerでは、必要なroot権限なしに、ワイヤレスカード接続の変更および設定もできます。この理由から、NetworkManagerは、モバイルワークステーションに理想的なソリューションと言えます。

ifupを使用する従来の設定では、ユーザ管理デバイスのようなユーザの介入があってもなくても、接続を切り替え、停止または開始する方法がいくつか用意されていますが、ネットワークデバイスを変更または設定するのにroot権限が常に必要とされます。このことは、多くの場合、考えられるすべての接続を事前に設定することができないモバイルコンピューティングでは問題になります。

従来の設定およびNetworkManagerの両方とも、DHCPと静的設定の両方を使用する有線ネットワーク、ダイヤルアップ、ワイヤレスネットワーク(WEP、WPA-PSK、WPA-Enterpriseアクセス)によるネットワーク接続を処理できます。また、VPNを介した接続もサポートしています。

NetworkManagerは、コンピュータが常に最適な接続を使用して接続されるようにします。最も高速の有線接続がある場合は、それを使用します。ネットワークケーブルの接続が誤って切断された場合は、再接続しようとします。また、ワイヤレス接続のリストから信号強度が最高のネットワークを検出し、自動的にそれを使用して接続します。ifupと同じ機能を得るため、多くの設定作業が必要です。

30.6.2 詳細情報

NetworkManagerの詳細は、次のWebサイトやディレクトリを参照してください:

- <http://www.gnome.org/projects/NetworkManager/>—NetworkManagerプロジェクトページ
- <http://en.opensuse.org/Projects/KNetworkManager>—NetworkManager KNetworkManagerプロジェクトページ

30.7 ネットワークの手動環境設定

ネットワークソフトウェアの手動環境設定は、常に最後の手段です。設定には可能な限りYaSTを使用してください。しかし、ネットワークの環境設定に関する背景知識がYaSTでの設定作業に役立つことがあります。

すべての内蔵式のネットワークカードおよびホットプラグのネットワークカード(PCMCIA、USB、一部のPCIカード)は、**hotplug**によって検出され、設定されます。システムは、ネットワークカードを物理デバイスとインタフェースの2種類の方法で参照します。デバイスが挿入または検出されると、ホットプラグイベントが生成されます。このホットプラグイベントによって、hwupスクリプトが実行され、デバイスが初期化されます。ネットワークカードが新しいネットワークインタフェースとして初期化されると、カーネルによって別のホットプラグイベントが生成され、それにより/sbin/ifupが実行されてインタフェースがセットアップされます。

カーネルは、登録順に従ってインタフェース名に番号を付けます。割り当てられる名前は、初期化の順序によって決まります。あるネットワークカードの初期化に失敗した場合、その後に初期化されるカードの番号は1つずつずらされます。実際のホットプラグ対応カードでは、デバイスを接続する順序が重要になります。

柔軟な環境設定を可能にするために、デバイス(ハードウェア)の環境設定とインタフェースの環境設定は切り分けられ、デバイスの環境設定とインタフェースの環境設定のマッピングをインタフェース名で管理する方式は廃止されました。デバイスの環境設定は、/etc/sysconfig/hardware/hwcfg-*に格納されます。インタフェースの環境設定は、/etc/sysconfig/network/ifcfg-*に格納されます。これらの環境設定ファイルには、そのファイルに関連付けられるデバイスまたはインタフェースを表す名前が付けられます。ドライバをインタフェース名にマッピングする従来の方式では静的なインタフェース名が必要なため、このマッピングを/etc/modprobe.confで行うことはできなくなりました。この新しい方式では、このファイルにエイリアスエントリが設定されていると、好ましくない副作用が発生することがあります。

環境設定名、すなわち、hwcfg-またはifcfg-の後の部分では、スロット、デバイス固有のID、インタフェース名などでデバイスを表します。たとえば、PCIカードの環境設定名は、bus-pci-0000:02:01.0 (PCIスロット)、vpid-0x8086-0x1014-0x0549 (メーカー名と製品ID)などになります。対応するインタフェース名は、bus-pci-0000:02:01.0、wlan-id-00:05:4e:42:31:7a (MACアドレス)などになります。

特定のカードではなく特定のタイプのカードにネットワークの環境設定を割り当てる場合は(ただし、同じタイプのカードを同時に2枚以上は装着しない)、もう少し汎用的な設定名を選択します。たとえば、すべてのPCMCIAカード

に対してbus-pcmciaという設定名を使用できます。一方、先頭にインタフェースタイプが付いた限定的な設定名も使用できます。たとえば、USBポートに接続するWLANカードにはwlan-bus-usbという設定名を付けることができます。

システムは常に、インタフェースまたはそのインタフェースを提供するデバイスに最適な環境設定を使用します。最適な環境設定の検索は、getcfgによって行われます。getcfgの出力には、デバイスを記述するために使用できるすべての情報が含まれています。環境設定名の指定の詳細については、getcfgのマニュアルページを参照してください。

この方法により、ネットワークデバイスは常に同じ順序で初期化されるとは限りませんが、ネットワークインタフェースは適切に設定されます。ただし、インタフェース名は、やはり初期化の順序によって決まります。特定のネットワークカードのインタフェースに確実にアクセスするには、次の2とおりの方法があります。

- getcfg-interfaceconfiguration nameを実行すると、対応するネットワークインタフェース名が返されます。したがって、一部の環境設定ファイルでは、ファイアウォール、dhcpcd、ルーティング、各種仮想ネットワークインタフェース(トンネル)などの設定名を、固定的でないインタフェース名の代わりに指定できます。
- 固定的なインタフェース名が各インタフェースに自動的に割り当てられます。必要に応じて名前を変更します。インタフェースが作成されたら、/etc/udev/rules.d/30-net_persistent_names.rulesの指示に従います。ただし、固定名pnameは、カーネルによって自動的に割り当てられる名前とは異なっていなければなりません。したがって、eth*、tr*、wlan*、qeth*、iucv*などの名前は使用できません。このような名前ではなく、net*またはexternal、internal、dmzなどの説明的な名前を使用します。同じインタフェース名が2回使用されないことを確認してください。インタフェース名に使用できる文字は、[a-zA-Z0-9]に制限されています。固定名は、登録直後にのみインタフェースに割り当てることができます。つまり、ネットワークカードのドライバを再ロードするか、hwupデバイス記述を実行する必要があります。rcnetwork restartコマンドを実行するだけでは不十分です。

重要項目: 固定的なインタフェース名の使用について

固定的なインタフェース名の使用は、一部の領域ではテストされていません。したがって、アプリケーションによっては、自由に選択したインタフェース名を使用できないことがあります。

ifupはハードウェアを初期化しないため、すでに存在しているインタフェースを必要とします。ハードウェアの初期化は、hwupコマンドによって行われます(このコマンドはhotplugまたはcoldplugによって実行されます)。デバイスが初期化されると、hotplugによってifupが新しいインタフェースに対して自動的に実行され、実行モードがonboot、hotplug、またはautoでありnetworkサービスが既に起動していれば、インタフェースがセットアップされます。従来は、ifup インタフェース名コマンドによってハードウェアの初期化が行われていましたが、新しいバージョンでは処理順序が逆になりました。はじめに、ハードウェアコンポーネントを初期化してから、その他の処理が行われます。この方法により、可変数のデバイスを、既存の環境設定を用いてできる限り最適な方法で設定できます。

表 30.5. 「手動ネットワーク環境設定用スクリプト」 (643 ページ)に、ネットワークの環境設定関連の最も重要なスクリプトをまとめます。各スクリプトはハードウェアとインタフェースに分類してあります。

表 30.5 手動ネットワーク環境設定用スクリプト

環境設定 段階	コマンド	機能
ハード ウェア	hw{up,down,status}	hw*スクリプトは、ホットプラグサブシステムによって実行され、デバイスの初期化、初期化の取り消し、デバイスのステータスの問い合わせを行います。詳細は、hwupのマニュアルページを参照してください。
インタ フェース	getcfg	getcfgは、環境設定名またはハードウェア記述に対応するインタフェース名の問い合わせに使用しま

環境設定 段階	コマンド	機能
		す。詳細は、getcfgのマニュアルページを参照してください。
インタ フェース	<code>if{up,down,status}</code>	if*スクリプトは、既存のネットワークインタフェースを起動したり、指定のインタフェースのステータスを表示したりします。詳細は、ifupのマニュアルページを参照してください。

ホットプラグおよび固定的なデバイス名の詳細については、[第24章 *udev*を使用した動的カーネルデバイス管理](#) (509 ページ)を参照してください。

30.7.1 環境設定ファイル

ここでは、ネットワークの環境設定ファイルの概要を紹介し、その目的と使用される形式について説明します。

/etc/syconfig/hardware/hwcfg-*

これらのファイルには、ネットワークカードおよびその他のデバイスのハードウェアの環境設定が記述されています。これには、カーネルモジュール、実行モード、スクリプトの関連付けなどの必要なパラメータが含まれます。詳細については、hwupのマニュアルページを参照してください。存在しているハードウェアとは無関係に、coldplugの起動時にはhwcfg-static-*が適用されます。

/etc/sysconfig/network/ifcfg-*

これらのファイルには、ネットワークインタフェースの環境設定が記述されています。これには、実行モード、IPアドレスなどが含まれます。指定可能なパラメータについては、ifupのマニュアルページを参照してください。また、一般的設定を1つのインタフェースだけに使用する場合は、dhcp、

wireless、およびconfigの各ファイルにあるすべての変数が、ifcfg-*ファイルで使用されます。

► **zseries:** IBM System zは、USBをサポートしていません。インタフェースファイル名とネットワークエイリアスには、qethのようにSystem z固有の要素が含まれます。 ◀

/etc/sysconfig/network/{config,dhcp,wireless}

configファイルには、ifup、ifdown、およびifstatusの動作に関する汎用的な設定が記述されています。また、dhcpにはDHCPの設定が、wirelessには無線LANカードの設定が記述されています。これら3つの環境設定ファイルの変数にはコメントが付けられており、優先度の高い変数としてifcfg-*ファイルでも使用できます。

/etc/sysconfig/network/{routes,ifroute-*}

TCP/IPパケットの静的ルーティングが設定されています。ホストへのルート、ゲートウェイ経由のホストへのルート、およびネットワークへのルートなど、さまざまなシステムタスクが必要とするすべての静的ルートは、/etc/sysconfig/network/routesファイルに指定できます。個別のルーティングが必要な各インタフェースにタイして、付加環境設定ファイル/etc/sysconfig/network/ifroute-*を定義します。*はイン^フェース名で読み替えてください。経路の環境設定ファイルのエントリは次のようになります。

# Destination	Dummy/Gateway	Netmask	Device
#			
127.0.0.0	0.0.0.0	255.255.255.0	lo
204.127.235.0	0.0.0.0	255.255.255.0	eth0
default	204.127.235.41	0.0.0.0	eth0
207.68.156.51	207.68.145.45	255.255.255.255	eth1
192.168.0.0	207.68.156.51	255.255.0.0	eth1

第1列は、経路の宛先です。この列には、ネットワークまたはホストのIPアドレスが入ります。到達可能なネームサーバの場合は、完全に修飾されたネットワークまたはホスト名が入ります。

第2列は、デフォルトゲートウェイ、すなわちホストまたはネットワークにアクセスする際に経由するゲートウェイです。第3列は、ゲートウェイの背後に

あるネットワークまたはホストのネットマスクです。たとえば、ゲートウェイの背後にあるホストのネットマスクは、255.255.255.255になります。

最後の列は、ローカルホスト(ループバック、イーサネット、ISDN、PPP、モデムデバイスなど)に接続されたネットワークのみに関連します。ここには、デバイス名を指定する必要があります。

(オプションの)5番目のコラムには、経路のタイプを指定することができます。必要ではないコラムには、マイナス記号-を記入してください。これは、パーサがコマンドを正しく解釈できるようにするためです。詳細は、`routes(5)` マニュアルページを参照してください。

/etc/resolv.conf

このファイルには、ホストが属するドメインが指定されています(キーワード `search`)。また、アクセスするネームサーバアドレスのステータスのリストも記述されています(キーワード `nameserver`)。ドメイン名は複数指定することができます。完全修飾でない名前を解決する場合は、`search`の各エントリを付加して完全修飾名の生成が試みられます。複数のネームサーバを使用するには、`nameserver`で始まる行を複数行入力します。#記号の後に記入します。**例 30.5**、**「/etc/resolv.conf」** (646 ページ)に/etc/resolv.confの例を示します。

例 30.5 /etc/resolv.conf

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

`pppd(wvdial)`、`ipppd(isdn)`、`dhcpcp(dhccpd, dhclient)`、`pcmcia`、`hotplug`などの一部のサービスは、スクリプト`modify_resolvconf`を使用してファイル/etc/resolv.confに変更を加えます。ファイル/etc/resolv.confがこのスクリプトによって一時的に変更された場合、変更を加えたサービス、元のファイルがバックアップされている場所、および自動変更メカニズムを無効にする方法を示す事前定義のコメントが付されます。/etc/resolv.confが複数回変更された場合、ファイルには変更内容がネスト形式で保存

されます。変更が行われた順序と異なる順序で復元を行った場合も、問題なく元通りに復元できます。このような柔軟性を必要とするサービスには、`isdn`、`pcmcia`、および`hotplug`があります。

サービスが通常のクリーンな状態で停止しなかった場合、`modify _resolvconf`を使用して元のファイルを復元することができます。また、システムブート時に、クリーンアップされていない変更された`resolv.conf`が存在しないかが確認され(たとえば、システムクラッシュがあった場合)、存在する場合は、元の(変更されていない)`resolv.conf`が復元されます。

YaSTは、`modify _resolvconfcheck`コマンドを使用して、`resolv.conf`が変更されているかどうかを確認し、ユーザに対してファイルの復元後は変更内容が失われることを警告します。**YaST**はこれ以外の作業で`modify _resolvconf`に依存しないため、**YaST**を使用して`resolv.conf`を変更した場合の影響は、手動で変更した場合と同じです。どちらの場合も、変更は永久に有効です。一方、前述のサービスによって要求された変更は、一時的に有効なだけです。

/etc/hosts

このファイル(例 30.6. 「`/etc/hosts`」 (647 ページ)を参照)では、**IP**アドレスがホスト名に割り当てられています。ネームサーバが実装されていない場合は、**IP**接続をセットアップするすべてのホストをここにリストする必要があります。ファイルには、各ホストについて1行を入力し、**IP**アドレス、完全修飾ホスト名、およびホスト名を指定します。**IP**アドレスは、行頭に指定し、各エントリはブランクとタブで区切ります。コメントは常に#記号の後に記入します。

例 30.6 /etc/hosts

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.1 earth.example.com earth
```

/etc/networks

このファイルには、ネットワーク名とネットワークアドレスの対応が記述されています。形式は、ネットワーク名をアドレスの前に指定すること以外は、`hosts`ファイルと同様です。詳細については、[例 30.7. 「/etc/networks」 \(648 ページ\)](#)を参照してください。

例 30.7 /etc/networks

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

名前解決(リゾルバライブラリを介したホストおよびネットワーク名の解釈)は、このファイルにより制御されます。このファイルは、`libc4`または`libc5`にリンクされているプログラムについてのみ使用されます。最新の`glibc`プログラムについては、`/etc/nsswitch.conf`の設定を参照してください。パラメータは、その行内で常に独立しています。コメントは`#`記号の後に記入します。[表 30.6. 「/etc/host.conf」ファイルのパラメータ \(648 ページ\)](#)に、利用可能なパラメータを示します。`/etc/host.conf`の例については、[例 30.8. 「/etc/host.conf」 \(649 ページ\)](#)を参照してください。

表 30.6 /etc/host.confファイルのパラメータ

<code>order hosts,bind</code>	名前の解決の際、サービスがアクセスされる順序を指定します。有効な引数は次のとおりです(空白またはカンマで区切ります)。 <code>hosts</code> : <code>/etc/hosts</code> ファイルを検索します。 <code>bind</code> : ネームサーバにアクセスします。 <code>nis</code> : NISを使用します。
<code>multi on/off</code>	<code>/etc/hosts</code> に指定されているホストが、複数のIPアドレスを持てるかどうかを定義します。

<code>nospoof on</code> <code>spoofalert on/off</code>	これらのパラメータは、ネームサーバ <i>spoofing</i> に影響を与えますが、それ以外のネットワークの環境設定に対してまったく影響を与えません。
<code>trim domainname</code>	ホスト名が解決された後、指定したドメイン名をホスト名から切り離します(ホスト名にドメイン名が含まれている場合)。このオプションは、ローカルドメインにある名前だけが/etc/hostsファイルに指定されているが、付加されるドメイン名でも認識する必要がある場合に便利です。

例 30.8 /etc/host.conf

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

/etc/nsswitch.conf

GNU C Library 2.0を導入すると、*Name Service Switch* (NSS)も合わせて導入されます。詳細については、`nsswitch.conf(5)` manページおよび『*The GNU C Library Reference Manual*』を参照してください。

クエリの順序は、ファイル/etc/nsswitch.confで定義します。`nsswitch.conf`の例については、を参照してください。例 30.9. 「/etc/nsswitch.conf」(650 ページ)コメントは#記号の後に記入します。この例では、`hosts`データベースの下のエントリは、要求がDNSを介して、/etc/hosts(files)に送信されることを意味しています(第33章 ドメインネームシステム (673 ページ)参照)。

例 30.9 /etc/nsswitch.conf

```
passwd:      compat
group:       compat

hosts:       files dns
networks:    files dns

services:    db files
protocols:   db files

netgroup:    files
automount:   files nis
```

NSSで利用できる「データベース」については、表 30.7. 「[/etc/nsswitch.confで利用できるデータベース](#)」 (650 ページ)を参照してください。それらに加えて、automount、bootparams、netmasks、およびpublickeyが近い将来導入される予定です。NSSデータベースの環境設定オプションについては、表 30.8. 「[NSS 「データベース」 の環境設定オプション](#)」 (651 ページ)を参照してください。

表 30.7 /etc/nsswitch.confで利用できるデータベース

aliases	sendmailによって実行されたメールエイリアス。man 5 aliasesコマンドで、マニュアルページを参照してください。
ethers	イーサネットアドレス。
group (グループ)	getgrentがユーザグループを調べるとき使用します。groupのマニュアルページも参照してください。
hosts	gethostbynameおよび同類の関数によって使用されるホスト名とIPアドレス。
netgroup	アクセス許可を制御するための、ネットワーク内にあ る有効なホストとユーザのリスト。netgroup(5) man ページを参照してください。

networks	ネットワーク名とアドレス。getnetentによって使用されます。
passwd	ユーザパスワード。getpwentによって使用されます。 passwd(5) manページを参照してください。
protocols	ネットワークプロトコル。getprotoentによって使用されます。 protocols(5) manページを参照してください。
rpc	リモートプロシージャコール名とアドレス。 getrpcbynameおよび同様の関数によって使用されます。
services	ネットワークサービス。getserventによって使用されます。
shadow	ユーザのシャドウパスワード。getspnamによって使用されます。 shadow(5) manページを参照してください。

表 30.8 NSS 「データベース」 の環境設定オプション

ファイル	たとえば/etc/aliasesのような直接アクセスファイル。
db	データベース経由のアクセス。
nis、nisplus	NIS。第35章 <i>NISの使用</i> (715 ページ)を参照。
dns	hostsおよびnetworksの拡張としてのみ使用できます。
compat	passwd、shadow、およびgroupの拡張としてのみ使用できます。

/etc/nscd.conf

このファイルは、`nscd` (name service cache daemon)の環境設定に使用します。`nscd(8)` および `nscd.conf(5)` `man` ページを参照してください。デフォルトでは、`nscd`によって`passwd`と`groups`のシステムエントリがキャッシュされます。キャッシュが行われないと名前やグループにアクセスするたびにネットワーク接続が必要になるため、このキャッシュ処理は `NIS` や `LDAP` といったディレクトリサービスのパフォーマンスに関して重要な意味を持ちます。`hosts`はデフォルトではキャッシュされません。これは、`nscd` でホストをキャッシュすると、ローカルシステムで正引き参照と逆引き参照のルックアップチェックを信頼できなくなるからです。したがって、`nscd`を使用して名前をキャッシュするのではなく、キャッシュDNSサーバをセットアップします。

`passwd`オプションのキャッシュを有効にすると、新しく追加したローカルユーザが認識されるまで、通常、約15秒かかります。この待ち時間を短縮するには、コマンド `rcnscdrestart` を使用して `nscd` を再起動します。

/etc/HOSTNAME

このファイルには、ドメイン名の付いていないホスト名が記述されています。このファイルは、マシンの起動時に複数のスクリプトによって読み込まれます。指定できるのは、ホスト名が設定されている1行のみです。

30.7.2 設定のテスト

設定内容を設定ファイルに書き込む前に、それをテストすることができます。テスト環境を設定するには、`ip` コマンドを使用します。接続をテストするには、`ping` コマンドを使用します。また、以前の設定ツールの `ifconfig` や `route` も使用することができます。

`ip`、`ifconfig`、および `route` コマンドは、ネットワーク設定を直接変更します。ただし、設定ファイルに変更内容は保存されません。正しい設定ファイルに変更内容を保存しない限り、変更したネットワーク設定は再起動時に失われてしまいます。

ipコマンドを使ったネットワークインタフェースの設定

ipは、ルーティング、ネットワークデバイス、ルーティングポリシー、およびトンネルに関する設定を行ったり、設定内容を表示したりするコマンドです。ipは、以前のifconfigコマンド、およびrouteコマンドに代わるコマンドとして設計されました。

ipは非常に複雑なツールです。一般的には、`ip options object command`の形式で指定します。objectの部分には、次のオブジェクトを指定することができます。

リンク

ネットワークデバイスを表します。

アドレス

デバイスのIPアドレスを表します。

neighbour

ARPまたはNDISCキャッシュエントリを表します。

route

ルーティングテーブルエントリを表します。

ルール

ルーティングポリシーデータベース中のルールを表します。

maddress

マルチキャストアドレスを表します。

mroute

マルチキャストルーティングキャッシュエントリを表します。

tunnel

IPトンネルを表します。

commandの部分に何も指定しないと、デフォルトのコマンド(通常はlist)が使用されます。

デバイスの状態を変更するには、`ip link set device_name command` コマンドを使用します。たとえば、デバイス `eth0` を無効にするには、`ip link set eth0 down` を実行します。このデバイスを有効にする場合は、`ip link set eth0 up` を実行します。

デバイスを有効にしたら、そのデバイスを設定することができます。デバイスのIPアドレスを使用する場合は、`ip addr add ip_address + dev device_name` を使用します。たとえば、インタフェース `eth0` にアドレス「`192.168.12.154/30`」を設定し、標準のブロードキャスト(`brd` オプション)を使用する場合は、`ip addr add 192.168.12.154/30 brd + dev eth0` と入力します。

実際に利用できる接続を作成するには、デフォルトのゲートウェイも設定する必要があります。ゲートウェイを設定するには、`ip route get gateway_ip_address` と入力します。あるIPアドレスを別のIPアドレスに変換するには、`nat: ip route add nat ip_address via other_ip_address` を使用します。

すべてのデバイスを表示する場合は、`ip link ls` を使用します。動作しているインタフェースだけを表示する場合は、`ip link ls up` を使用します。デバイスのインタフェース統計情報を印刷する場合は、`ip -s link ls device_name` と入力します。デバイスのアドレスを表示する場合は、`ip addr` と入力します。`ip addr` の出力には、デバイスのMACアドレスに関する情報も表示されます。すべてのルートを表示する場合は、`ip route show` を使用します。

`ip` の使用方法の詳細は、`iphelp` を入力するか、または `ip(8)` マニュアルページを参照してください。`help` オプションは、すべての `ip` オブジェクトで利用することができます。たとえば、`ipaddr` に関するヘルプを表示する場合は、「`ipaddr help`」と入力します。`ip` のマニュアルは、`/usr/share/doc/packages/iproute2/ip-cref.pdf` に用意されています。

pingを使った接続のテスト

`ping` コマンドは、TCP/IP 接続が正常に動作しているかどうかを調べるための、標準ツールです。`ping` コマンドはICMPプロトコルを使って、小さなデータパケット `ECHO_REQUEST` データグラムを、宛先ホストに送信し、即時応答

を要求します。この作業が成功した場合、pingコマンドは、その結果を知らせるメッセージを表示します。これは、ネットワークリンクが基本的に機能していることを意味します。

pingは、2台のコンピュータ間の接続をテストするだけでなく、接続品質に関する基本的な情報も提供します。**ping例 30.10. 「pingコマンドの出力」**(655ページ)コマンドの実行結果例は、を参照してください。2番目の行から最後の行には、転送パケット数、失われたパケット数、およびpingの実行時間の合計が記載されています。

pingの宛先には、ホスト名またはIPアドレスを指定することができます。たとえば、pingexample.comやping130.57.5.75のように指定します。pingコマンドを実行すると、Ctrl + Cキーを押すまでの間、継続的にパケットが送信されます。

接続されているかどうかを確認するだけで良い場合は、-cオプションを使って送信するパケット数を指定することができます。たとえば、パケットを3つだけ送信する場合は、ping-c 3 192.168.0を入力します。

例 30.10 pingコマンドの出力

```
ping -c 3 example.com
PING example.com (130.57.5.75) 56(84) bytes of data.
64 bytes from example.com (130.57.5.75): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (130.57.5.75): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (130.57.5.75): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

デフォルトでは、pingは1秒ごとにパケットを送信します。送信間隔を変更するには、-iオプションを指定します。たとえば、10秒ごとにパケットを送信する場合は、ping-i 10 192.168.0を入力します。

複数のネットワークデバイスを持つシステムの場合、特定のインタフェースアドレスを指定してpingを実行することができます。インタフェースを指定するには、-Iオプションにデバイス名を指定します。たとえば、ping-I wlan1 192.168.0のように指定します。

pingのオプションと使用方法の詳細は、ping-hを入力するか、またはping(8)マニュアルページを参照してください。

ifconfigを使ったネットワークの設定

ifconfigは、従来のネットワーク設定ツールです。ipと違い、このコマンドはインタフェースを設定する場合にのみ使用します。ルーティングを設定する場合は、routeを使用します。

注意: ifconfigとip

ifconfigプログラムは廃止されました。かわりにipを使用します。

ifconfigに引数を指定しないと、現在アクティブなインタフェースのステータスが表示されます。例 30.11. 「ifconfigコマンドの出力」 (656 ページ)のように、ifconfigでは、詳細な情報がわかりやすく表示されています。この出力では、デバイスのMACアドレス(HWaddrの値)も1行目に表示されています。

例 30.11 ifconfigコマンドの出力

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 Mb)
```

ifconfigのオプションと使用方法の詳細については、ifconfig-hを入力するか、またはifconfig(8)マニュアルページを参照してください。

routeを使ったルーティングの設定

routeは、IPルーティングテーブルを操作するプログラムです。このコマンドを使って、ルーティングの設定内容を表示したり、ルートを追加または削除することができます。

注意: routeとip

routeプログラムは廃止されました。かわりにipを使用します。

routeは、総合的なルーティング情報を素早く参照して、ルーティングに関する問題を探す場合などに役立ちます。現在のルーティング設定を表示するには、rootとしてroute-nを入力します。

例 30.12 route -n コマンドの実行結果

```
route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags   MSS Window  irtt Iface
10.20.0.0        *               255.255.248.0   U        0 0        0 eth0
link-local       *               255.255.0.0     U        0 0        0 eth0
loopback         *               255.0.0.0       U        0 0        0 lo
default          styx.exam.com   0.0.0.0         UG       0 0        0 eth0
```

routeのオプションと使用方法の詳細については、route-hを入力するか、またはroute (8) マニュアルページを参照してください。

30.7.3 スタートアップスクリプト

前述の環境設定ファイルに加え、マシンのブート時にネットワークプログラムをロードするさまざまなスクリプトも用意されています。これらは、システムがマルチユーザランレベルのいずれかに切り替わったときに起動します。これらのスクリプトの一部は、**表 30.9. 「ネットワークプログラム用スタートアップスクリプト」** (657 ページ) で説明されています。

表 30.9 ネットワークプログラム用スタートアップスクリプト

/etc/init.d/ network	このスクリプトは、ネットワークインタフェースの環境設定を処理します。ハードウェアが事前に
-------------------------	--

(hotplug経由で) /etc/init.d/coldplugによって初期化されている必要があります。networkサービスが起動していないと、ネットワークインタフェースは、ホットプラグ経由で挿入されたときに初期化されません。

/etc/init.d/inetd	xinetdを開始します。xinetdを使用すると、サーバサービスがシステム上で利用できるようになります。たとえば、FTP接続の開始時に必ずvsftpdを起動するといったことができます。
/etc/init.d/portmap	NFSサーバなどのRPCサーバに必要なポートマップを起動します。
/etc/init.d/nfsserver	NFSサーバを起動します。
/etc/init.d/postfix	postfixプロセスを制御します。
/etc/init.d/ypserv	NISサーバを起動します。
/etc/init.d/ypbind	NISクライアントを起動します。

30.8 ダイアルアップアシスタントとしてのsmpppd

一部のホームユーザは、インターネット接続専用の回線を持っていません。代わりにダイアルアップ接続を使用しています。接続は、ダイアルアップ方法(ISDNまたはDSL)に応じてipppdまたはpppdで制御されます。基本的には、これらのプログラムを正常に起動するだけでオンラインで接続できます。

ダイアルアップ接続時に追加費用が発生しない定額接続を使用している場合は、単に該当するデーモンを起動します。ダイアルアップ接続の管理には、KDEアプレットまたはコマンドラインインタフェースを使用します。インター

ネットゲートウェイ以外のホストを使用している場合は、ネットワークホスト経由でダイヤルアップ接続を管理できます。

smpppdが関係するのはこの部分です。このプログラムは補助プログラム用に一般的なインタフェースを提供し、双方向に動作します。第1に、必要なpppdまたはipppdをプログラミングし、そのダイヤルアッププロパティを制御します。第2に、各種プロバイダをユーザプログラムで使えるようにして、現在の接続ステータスに関する情報を送信します。smpppdはネットワーク経由で制御することもできるため、プライベートサブネットワーク内のワークステーションからインターネットへのダイヤルアップ接続の制御に適しています。

30.8.1 smpppdの設定

smpppdによる接続は、YaSTにより自動的に設定されます。実際のダイヤルアッププログラムであるkinternetとcinternetも事前に設定済みです。手動設定が必要となるのは、リモート制御など、smpppdの付加的機能を設定する場合のみです。

smpppdの設定ファイルは/etc/smpppd.confです。デフォルトでは、このファイルによるリモート制御はできません。この設定ファイルの最も重要なオプションを次に示します。

`open-inet-socket = yes/no`

smpppdをネットワーク経由で制御するには、このオプションをyesに設定する必要があります。smpppdがリッスンするポートは3185です。このパラメータをyesに設定した場合は、パラメータbind-address、host-rangeおよびpasswordもそれに応じて設定する必要があります。

`bind-address = ip address`

ホストに複数のIPアドレスがある場合は、このパラメータを使用してsmpppdで接続の受け入れに使用するIPアドレスを指定します。デフォルトでは、すべてのアドレスでリッスンします。

`host-range = min ip max ip`

パラメータhost-rangeを使用して、ネットワーク範囲を定義します。この範囲内のIPアドレスを持つホストには、smpppdへのアクセス権が付与されます。この範囲外のホストはすべてアクセスを拒否されます。

`password = password`

パスワードを割り当てることで、クライアントを認可されたホストに限定できます。これはプレーンテキストによるパスワードのため、このパスワードによるセキュリティを過大評価しないでください。パスワードを割り当てないと、すべてのクライアントがsmpppdへのアクセスを許可されます。

`slp-register = yes / no`

このパラメータにより、smpppdサービスがSLPによってネットワーク上にアナウンスされます。

smpppdについての詳細は、smpppd(8)およびsmpppd.conf(5) manページを参照してください。

30.8.2 リモートで使用するためのkinternet、cinternet、およびqinternetの設定

KInternet、cinternet、およびqinternetを使って、ローカル/リモートsmpppdを制御することができます。cinternetは、グラフィカルなKInternetのコマンドライン版です。基本的にqinternetはKInternetと同じです。ただし、KDEなしでも利用できるように、KDEライブラリは使用しません。また、個別にインストールする必要があります。これらのユーティリティをリモートsmpppdに使用するには、設定ファイル/etc/smpppd-c.confを手動で、またはkinternetを使用して編集します。このファイルでは、以下の3つのオプションのみを使用します。

`sites = list of sites`

このオプションでは、フロントエンドがsmpppdを検索する場所を指定します。フロントエンドは、ここに記述されている順序でオプションをテストします。localは、ローカルsmpppdへの接続の確立を指定します。

gatewayは、ゲートウェイ上のsmpppdをポイントします。接続は、config-fileのserverの指定に従って確立する必要があります。slpは、フロントエンドに対してSLPによって検出されたsmpppdに接続するよう指示します。

`server = server`

このオプションでは、smpppdを実行するホストを指定します。

```
password = password
```

このオプションでは、**smpppd**用に選択したパスワードを挿入します。

smpppdがアクティブな場合は、これでコマンド**cinternet--verbose**
--interface-listなどのコマンドを使用してアクセスを試行できます。この時点でアクセスできない場合は、**smpppd-c.conf**(5)および**cinternet**(8)
manページを参照してください。

ネットワーク上のSLPサービス

サービスロケーションプロトコル(*SLP*)は、ローカルネットワークに接続されているクライアントの構成を簡略化するために開発されました。ネットワーククライアントを設定するには、すべての必要なサービスを含め、管理者はネットワークで利用できるサーバに関する詳しい知識が必要とされました。*SLP*は、ローカルネットワーク上にあるすべてのクライアントに対して特定のサービスを利用できることを通知します。このような通知情報を利用して*SLP*をサポートする各種アプリケーションを自動的に設定することができます。

SUSE Linux Enterprise®は、*SLP*によって提供されるインストールソースを使用するインストールをサポートしています。また、多くのシステムサービスは、統合*SLP*をサポートしています。*YaST*と*Konqueror*は、どちらも*SLP*用の適切なフロントエンドを持っています。ご利用のシステムでインストールサーバ、ファイルサーバ、印刷サーバなどの*SLP*を使用することにより、ネットワークに接続されたクライアントに一元的な管理機能を提供します。

重要項目: SUSE Linux EnterpriseでのSLPサポート

*SLP*サポートを提供するサービスには*cupsd*、*rsyncd*、*ypserv*、*openldap2*、*openwbem* (CIM)、*ksysguardd*、*saned*、*kdm vnc login*、*smpppd*、*rpasswd*、*postfix*、および*sshd* (fish経由)があります。

31.1 SLPをアクティブ化する

*SLP*サービスを提供するには、システム上で*slpd*を実行する必要があります。サービスの照会を作成するだけの場合は、このデーモンを開始する必要はあ

りません。SUSE Linux Enterprise中のほとんどのシステムサービスと同様、slpdデーモンは別のinitスクリプトを使用して制御されます。このデーモンはデフォルトで非アクティブになっています。セッション中にこのデーモンを有効化するには、rcslpd startをrootで実行してデーモンを開始し、rcslpd stopで停止します。restartで再始動、またはstatusで状態チェックを実行します。デフォルトでslpdをアクティブにする必要がある場合は、YaSTで [システム] > [システムサービス(ランレベル)] の順に選択してslpdを有効にするか、またはrootとしてを1回実行します。insservslpdシステムのブート時に開始するサービスセットとしてslpdが自動的に追加されます。

31.2 SUSE Linux EnterpriseのSLPフロントエンド

ネットワーク内でSLPが提供するサービスを検索するには、SLPフロントエンドを使用します。SUSE Linux Enterpriseには、さまざまなフロントエンドが用意されています。

slptool

slptoolはネットワーク上のSLP照会を通知するため、または適切なサービスを通知するために使用される単純なコマンドラインプログラムです。slptool --helpはすべての利用可能なオプションと機能をリストします。slptoolはSLP情報を処理するスクリプトから呼び出すことができます。

YaSTのSLPブラウザ

YaSTには別のSLPブラウザが含まれています。SLPブラウザには、SLPによって通知されたローカルネットワークのすべてのサービスがツリー形式で表示されます。このブラウザを表示するには、[ネットワークサービス] > [SLPブラウザ] の順にクリックします。

Konqueror

ネットワークブラウザとして使用される場合、Konquerorはslp:/のローカルネットワークで使用可能なすべてのSLPサービスを表示できます。メインウィンドウにあるアイコンをクリックして、関連サービスについての詳細情報を参照してください。Konquerorをservice:/で使用する場合、ブラウザウィンドウで関連するアイコンをクリックして、選択したサービスとの接続をセットアップします。

31.3 SLP経由のインストール

ネットワークでSUSE Linux Enterpriseインストールメディアを使用したインストールサーバを利用できるようにする場合、SLPに登録することができます。詳細については、[4.2.1項「YaSTを使ったインストールサーバのセットアップ」](#) (63 ページ)を参照してください。SLPインストールが選択されると、選択したブートメディアからシステムがブートして検出されたソースを表示した後、linuxrcがSLP照会を開始します。

31.4 SLPを使ったサービスの提供

SUSE Linux Enterpriseのアプリケーションの多くはlibslpライブラリを使用することで、最初から統合SLPをサポートしています。サービスがSLPサポートでコンパイルされていない場合は、SLPを利用できるように次の方法のいずれかを使用してください。

/etc/slp.reg.dによる静的登録

新規サービスに個別の登録ファイルを作成します。次はスキャナサービスを登録するためのファイルの例です。

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

このファイルで最も重要な行は`service:`から開始するサービスURLです。このURLにはサービスタイプ(`scanner.sane`)および、サーバ上でサービスが使用可能になるアドレスが含まれます。`$HOSTNAME`は自動的に完全ホスト名で置き換えられます。その後ろにはサービスごとのTCPポートの名前がコロンで区切られる形で続きます。さらにサービスを表示する場合に使用される言語、登録の期間を秒単位で入力します。これらはコンマを使用してサービスURLと分けるようにします。0から65535で登録期間の値を設定します。0の場合は登録する必要がありません。65535はすべての制限を削除します。

登録ファイルには、2つの変数`watch-tcp-port`と`description`もあります。`watch-tcp-port`はSLPサービスアナウンスとリンクして、`slpd`にサービスのステータスをチェックさせることにより、関連サービスがアクティブかどうか確認します。`description`には、正しいブラウザを使用している場合に表示される、さらに詳細なシステム名が含まれています。

ティップ: YaSTとSLP

インストールサーバ、YOUサーバなどのようにYaSTが処理を行うサービスの一部では、モジュールダイアログでSLPがアクティブになった時点で自動的にこの登録が実行されます。続いてYaSTはこれらのサービスの登録ファイルを作成します。

`/etc/slp.reg`による静的登録

`/etc/slp.reg.d`を使用した場合の手順との唯一の違いは、すべてのサービスを1つの特定ファイル内にグループ化する点です。

`slptool`による動的登録

専用のスクリプトからサービスをSLPに登録するには、`slptool`コマンドラインフロントエンドを使用します。

31.5 詳細情報

次のソースではSLPについての詳しい情報が提供されています。

RFC 2608、2609、2610

一般的にRFC 2608はSLPの定義を取り扱います。RFC 2609は、使用されるサービスURLの構文を詳細に扱います。またRFC 2610ではSLPを使用したDHCPについて説明しています。

<http://www.openslp.org/>

OpenSLPプロジェクトのホームページです。

`/usr/share/doc/packages/openslp`

このディレクトリには、SUSE Linux Enterpriseの詳細、RFC、および2つの入門用HTMLマニュアルが記載されている`README.SuSE`を含め、SLPに関する利用可能なマニュアルがすべて用意されています。SLPを使用するプログラマは`openslp-devel`パッケージをインストールし、その中で提供される『*Programmers Guide*』を確認してください。

NTPによる時刻の同期

NTP (network time protocol)メカニズムは、システムの時刻をネットワーク上で同期させるためのプロトコルです。最初に、マシンは信頼できる時刻を持つサーバに時刻を照会できます。次に、ネットワーク上の他のコンピュータがこのマシン自体に対し、時刻を照会できます。目的は2つあり、絶対的な時間を維持することと、ネットワーク内のすべてのマシンのシステム時刻を同期させることです。

正確なシステムタイムを維持することはさまざまな場で重要です。ハードウェア組み込み型(BIOS)クロックがデータベースなどのアプリケーション要件に合致しないことがよくあります。システムタイムを手動で修正することは時に問題を発生させる可能性があります。たとえば、時間を逆廻りに戻すことで重要なアプリケーションの誤動作を誘発することもあります。ネットワーク内では、すべてのマシンのシステムタイムを同期させることが通常必要とされますが、手動での時刻調整はよい方法ではありません。xntpには、この問題を解決するメカニズムがあります。このメカニズムは常にネットワーク上の信頼できるタイムサーバに照会することで、システムタイムを調整します。さらに、電波時計のようなローカルリファレンスクロックを管理する機能があります。

32.1 YaSTでのNTPクライアントの設定

xntpは、ローカルのコンピュータクロックを時刻の標準として参照するように事前に設定されています。ただし、BIOSクロックの使用は、それ以上に正確な時刻ソースが利用できない場合の代替として以外は避けるようにしてください。YaSTを利用すれば、NTPクライアントを簡単に設定することができます。

す。ファイアウォールを利用していないシステムの場合は、クイック設定または詳細設定のいずれかを使用してください。ファイアウォールで保護されているシステムの場合は、詳細設定を使ってSuSEfirewall2の適切なポートを開きます。

32.1.1 NTPクライアントの簡易設定

NTPクライアントのクイック設定([ネットワークサービス]、> [NTPの環境設定] の順に選択)には、2つのダイアログがあります。最初のダイアログでは、`xntpd`の実行モードおよびクエリ先のNTPサーバを設定します。システムのブート時に`xntpd`を自動起動させるには、[When Booting System]をクリックします。次に、[NTPサーバの設定]を指定します。ローカルタイムサーバを使用できない場合は[Use Random Servers from pool.ntp.org]をクリックするか、または、[Select]をクリックして2番目のダイアログにアクセスし、ネットワークに適切なタイムサーバを選択します。

図 32.1 YaST:NTPクライアントの設定

NTPデーモンの自動起動
システムブート時にNTPデーモンを起動するかどうかを選択してください。NTPデーモンは、初期化中にホスト名を解決します。NTPデーモンを起動する前に、ネットワークが起動している必要があります。

NTPサーバのアドレス
NTPサーバのアドレスを設定するには、[アドレス]エントリを使用します。NTPサーバを見つけたら、ネットワーク管理者またはインターネットプロバイダにお問い合わせください。

サーバの選択
ローカルネットワークで検出されたNTPサーバまたは既知のNTPサーバの一覧から、NTPサーバを選択するには、[選択]をクリックし、[ローカルNTPサーバ]および[公開NTPサーバ]から選択します。

サーバの動作確認
選択したサーバが起動し正しく応答するかどうかを確認するには、[テスト]をクリックしてください。

ランダムサーバの使用
このサービスはpool.ntp.orgによって提供されます。このオプションを選択すると、設定に3つの異なるサーバが追加されます。このサーバの利点は、永続的ですが、DNSレコードの更新は毎時間ごとに変わります。つまり、ユーザのNTPクライアントは毎時間ごとに異なるサーバと同期することを意味します。

高度な設定
このホストを設定して複数のリモートホストまたはローカルに接続されたクロックの同期を取るには、**高度な設定**を使用します。

NTP環境設定

NTPデーモンの自動機能:
☐ 起動しない(E)
☒ 起動時の動作(B)

NTPサーバの設定
☐ pool.ntp.orgからランダムサーバを使用する(L)
アドレス(A):

選択(S): ▼
テスト(T)

詳細な環境設定(V)

キャンセル(C) 完了(F)

Tサーバ選択用の詳細ダイアログでは、ローカルネットワーク上のタイムサーバ([Local Network])とインターネット上のタイムサーバ([Public NTP Server])のどちらを使用して時刻の同期を行うかを指定します。ローカルタイムサーバを使用する場合は、[検索]をクリックして、ネットワーク上の利用可能なタイムサーバを問い合わせるSLPクエリを実行します。検索結果のリストから最

適なタイムサーバを選択し、[了解]をクリックしてダイアログを閉じます。インターネット上の公開タイムサーバを使用する場合は、国(タイムゾーン)および適切なタイムサーバを[公開NTPサーバ]のリストから選択し、[了解]をクリックしてダイアログを閉じます。メインダイアログで、[テスト]をクリックして選択したサーバが利用可能かどうかをテストし、[完了]をクリックしてダイアログを閉じます。

32.1.2 NTPクライアントの詳細設定

NTPクライアントの詳細設定は、簡易設定の項目で説明した実行モードを選択した後、[NTP Configuration]モジュールのメインダイアログの[詳細設定]([図 32.1. 「YaST:NTPクライアントの設定」 \(668 ページ\)](#))をクリックすると表示されます。

図 32.2 YaST:NTPの詳細設定

[高度なNTP設定]で、xntpdをchroot jailで実行するかどうかを指定します。デフォルトでは、[Run NTP Daemon in Chroot Jail]が選択されています。このオプションは、xntpd上の攻撃に対するセキュリティを強化し、不正ユーザーによってシステム全体が危険な状態に陥ることを防ぎます。[DHCPからNTPデーモンを設定]は、ローカルネットワーク上のNTPサーバのリストをDHCP経由で取得するようにNTPクライアントを設定します。

SuSEfirewallがアクティブな場合、[ファイアウォール内でポートを開く]を有効にします(デフォルト)。ポートを閉じたままにすると、タイムサーバと接続を確立することはできません。

ダイアログ下部には、クライアントに対するサーバおよび時刻情報のその他の情報源が表示されます。必要に応じて、[追加]、[削除]、および[編集]を使用してこのリストを変更します。[Display Log]では、クライアントのログファイルを表示できます。

時刻情報の情報源を追加するには、[追加]をクリックします。表示されるダイアログで、時刻同期に使用する情報源のタイプを選択します。次のオプションを指定できます。

サーバ

[同期相手のタイプの選択]ダイアログで、(32.1.1項「NTPクライアントの簡易設定」(668ページ)で説明したように)NTPサーバを選択できます。システムのブート時にサーバとクライアント間で時刻情報の同期を実行するには、[初期同期に用いる]を有効にします。[オプション]では、xntpdの追加オプションを指定できます。詳細は、/usr/share/doc/packages/xntp-doc (xntp-docパッケージの一部)を参照してください。

ピア

ピアは、対称的な関係が確立されたコンピュータで、タイムサーバとクライアントの両方の役割を果たします。サーバの代わりに、同じネットワーク内のピアを使用するには、そのピアシステムのアドレスを入力します。ダイアログのそれ以外の内容は[サーバ]ダイアログと同じです。

ラジオクロック

時刻同期にシステムのラジオクロックを使用するには、クロックタイプ、ユニット番号、デバイス名、およびその他のオプションをこのダイアログで指定します。ドライバを微調整するには、[ドライバの調整]をクリックします。ローカルのラジオクロックに関する詳細な情報は/usr/share/doc/packages/xntp-doc/html/refclock.htmを参照してください。

ブロードキャストの発信

時刻情報とクエリは、ネットワーク上にブロードキャストすることができます。このダイアログでは、このブロードキャストの送信先を指定します。電波時計のような信頼できる時刻ソースがない限りブロードキャストをアクティブにしないでください。

ブロードキャストの着信

クライアントで情報をブロードキャスト経由で受け取る場合は、どのアドレスからのパケットを受け入れるかをこのフィールドに指定します。

32.2 ネットワークでのxntp構成

ネットワーク内のタイムサーバを使用するには、`server`パラメータを設定するのが最も簡単です。たとえば、タイムサーバ`ntp.example.com`がネットワークから接続可能な場合、その名前をファイル`/etc/ntp.conf`に行として追加します。

```
server ntp.example.com
```

別のタイムサーバを追加するには、別の行にキーワードの「`server`」を挿入します。`rcntpd start`コマンドで`xntpd`を初期化すると、アプリケーションは時計が安定するまで1時間待機し、ドリフトファイルを作成してローカルコンピュータのクロックを修正します。ドリフトファイルを用いることで、ハードウェアクロックの定誤差はコンピュータの電源が入った時点で、すぐに算出されます。修正はすぐに反映されるため、システム時刻がより安定します。

NTP機構をクライアントとして使用するには、2種類の方法があります。まず、クライアントは既知のサーバに定期的に時間を照会することができます。クライアント数が多い場合、この方法はサーバの過負荷を引き起こす可能性があります。2つ目は、ネットワークでブロードキャストを行う時刻サーバから送信されるNTPブロードキャストを、クライアントが待機する方法です。この方法には不利な面があります。サーバの精度が不明なこと、そしてサーバから送信される情報が誤っていた場合、深刻な問題が発生する可能性があります。

ブロードキャスト経由で時刻を取得する場合、サーバ名は必要ではありません。この場合は、設定ファイル`/etc/ntp.conf`に行`broadcastclient`を記述します。1つ以上の信頼された時刻サーバのみを使用するには、`servers`で始まる行にサーバの名前を記述します。

32.3 ローカルリファレンスクロックの設定

ソフトウェアパッケージxntpには、ローカルリファレンスクロックに接続するためのドライバが含まれています。サポートされているクロックのリストは、xntp-docパッケージの/usr/share/doc/packages/xntp-doc/refclock.htmファイルに記載されています。各ドライバには、番号が関連付けられています。xntpの実際の設定は、疑似IPアドレスを使用して行われます。クロックは、ネットワークに存在しているものとして/etc/ntp.confファイルに入力されます。このため、これらのクロックには127.127.t.uという形式の特別なIPアドレスが割り当てられます。ここで、tはクロックのタイプを示し、使用されているドライバを決定します。uはユニットのタイプを示し、使用されているインタフェースを決定します。

通常、各ドライバは設定をより詳細に記述する特別なパラメータを持っています。ファイル/usr/share/doc/packages/xntp-doc/driverNN.html(ここでNNはドライバの番号)は特定のクロックタイプに関する情報を提供します。たとえば、「タイプ8」クロック(シリアルインタフェース経由のラジオクロック)はクロックをさらに細かく指定する追加モードを必要とします。また、Conrad DCF77レシーバモジュールはモード5です。このクロックを優先参照として使用するには、キーワードpreferを指定します。Conrad DCF77レシーバモジュールの完全なserver行は次のようになります。

```
server 127.127.8.0 mode 5 prefer
```

他のクロックも同じパターンで記述されます。xntp-docパッケージのインストール後に、ディレクトリ/usr/share/doc/packages/xntp-docにあるxntpのマニュアルを参照してください。ドライバパラメータについて説明するドライバページへのリンクがファイル/usr/share/doc/packages/xntp-doc/refclock.htmに記載されています。

ドメインネームシステム

DNS (ドメインネームシステム)は、ドメイン名とホスト名をIPアドレスに解決するために必要です。これにより、たとえばIPアドレス192.168.0.1がホスト名earthに割り当てられます。独自のネームサーバをセットアップする前に、[30.3項「ネームレゾリューション」](#) (614 ページ)で DNS に関する一般的な説明を参照してください。以降に示す設定例はBINDの場合のものです。

33.1 DNS用語

ゾーン

ドメインのネームスペースは、ゾーンと呼ばれる領域に分割されます。たとえば、example.orgの場合、orgドメインのexampleセクション(ゾーン)を表します。

DNSサーバ

DNSサーバは、ドメインの名前とIP情報を管理するサーバです。マスタゾーン用にプライマリDNSサーバ、スレーブゾーン用にセカンダリサーバ、またはキャッシュ用にいずれのゾーンも持たないスレーブサーバを持つことができます。

マスタゾーンのDNSサーバ

マスタゾーンにはネットワークからのすべてのホストが含まれ、DNSサーバのマスタゾーンにはドメイン内のすべてのホストに関する最新のレコードが格納されます。

スレーブゾーンのDNSサーバ

スレーブゾーンはマスタゾーンのコピーです。スレーブゾーンのDNSサーバは、ゾーン転送操作によりマスタサーバからゾーンデータを取得します。スレーブゾーンのDNSサーバは、有効なゾーンデータである(期限切れでない)限り、ゾーンに適切に応答します。スレーブがゾーンデータの新規コピーを取得できない場合、ゾーンへの応答を停止します。

フォワーダ

フォワーダは、DNSサーバがクエリに回答できない場合に、そのクエリの転送先になるDNSサーバです。

レコード

レコードは、名前とIPアドレスに関する情報です。サポートされているレコードおよびその構文は、BINDのドキュメントで説明されています。次は、特別なレコードの一部です。

NSレコード

NSレコードは、指定のドメインゾーンの担当マシンをネームサーバに指定します。

MXレコード

MX(メール交換)レコードは、インターネット上でメールを転送する際に通知するマシンを説明します。

SOAレコード

SOA (Start of Authority)レコードは、ゾーンファイル内で最初のレコードです。SOAレコードは、DNSを使用して複数のコンピュータ間でデータを同期化する際に使用されます。

33.2 YaSTでの設定

YaSTのDNSモジュールを使用すると、ローカルネットワーク用のDNSサーバを設定できます。Sambaサーバを設定するには、YaSTを起動して、[ネットワークサービス] > [DNSサーバ] の順に選択します。このモジュールを初めて起動すると、サーバ管理に関して少数の基本的な事項を決定するように要求されます。この初期セットアップを完了すると、必要最低限の機能が設定された基本的なサーバ設定が生成されます。エキスパートモードを使用す

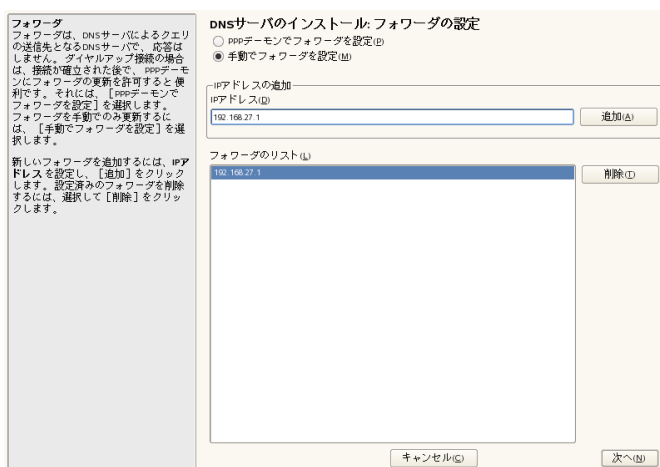
ると、ACL、ログ、TSIGキーおよび他のオプションなど、より詳細な設定タスクを行うことができます。

33.2.1 ウィザードによる設定

ウィザードは3つのステップ(ダイアログ)で構成されています。各ダイアログの適切な箇所ではエキスパート用の設定モードに入ることができます。

- 1 モジュールを初めて起動すると、のような「フォワーダの設定」[図33.1](#)、「DNSサーバのインストール:フォワーダの設定」(675 ページ)ダイアログが表示されます。このダイアログでは、PPPデーモンがDSLまたはISDNを介してダイヤルアップ時にフォワーダのリストを提供するか(「PPPデーモンがフォワーダを設定する」)、または独自のリストを指定するか(「手動でフォワーダを設定する」)を指定できます。

図 33.1 DNSサーバのインストール:フォワーダの設定



- 2 「DNSゾーン」ダイアログは、複数の部分で構成されており、[33.5項「ゾーンファイル」](#)(690 ページ)で説明するゾーンファイルの管理に関する項目を設定します。新しいゾーンを作成する場合は、「ゾーン名」にその名前を入力します。逆引きゾーンを追加する場合は、.in-addr.arpaで終わる名前を入力しなければなりません。最後に、「ゾーンタイプ」(マスタまたはスレーブ)を選択します。参照先

図 33.2. 「DNSサーバのインストール:DNSゾーン」 (676 ページ). 既存のゾーンのその他の項目を設定するには、[Edit Zone] をクリックします。ゾーンを削除するには、[Delete Zone] をクリックします。

図 33.2 DNSサーバのインストール:DNSゾーン

DNSゾーン
このダイアログでDNSゾーンを管理します。

新規ゾーンを追加するには、ゾーン名を入力し、ゾーンタイプを選択して追加をクリックします。新規の逆ゾーンを追加するには、`lin+addr.arpa`を後ろに付けて、逆IPアドレスの一部をゾーン名として入力したたとえば、ネットワーク192.168.0.0/24用ゾーン名0.168.192.lin+addr.arpa、ゾーンタイプを選択し、追加をクリックします。

ゾーン転送や、ゾーン名、メールサーバなど、ゾーン用の設定を変更するには、変更するものを選択し、[ゾーン編集]をクリックします。設定されたゾーンを削除するには、ゾーンを選択し、[ゾーンの削除]をクリックします。

DNSサーバのインストール: DNSゾーン
新しいゾーンの追加(D)

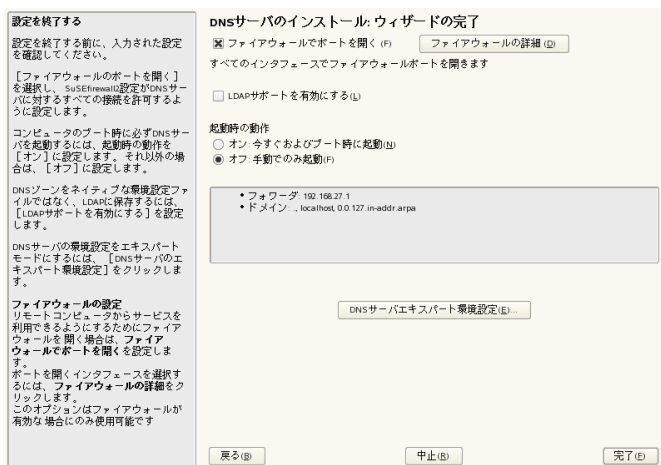
名前: タイプ:

設定済みDNSゾーン

ゾーン	タイプ
example.com	マスタ

- 最後のダイアログでは、[ファイアウォールで開いているポート] をクリックして、ファイアウォールのDNSポートを開くことができます。次に、DNSサーバを起動するかどうかを指定します([オン] または [オフ])。LDAPサポートを有効にすることもできます。詳細については、図 33.3. 「DNSサーバのインストール:完了ウィザード」 (677 ページ)を参照してください。

図 33.3 DNSサーバのインストール:完了ウィザード



33.2.2 エキスパート設定

YaSTのモジュールを起動するとウィンドウが開き、複数の設定オプションが表示されます。設定を完了すると、基本的な機能が組み込まれたDNSサーバ設定が作成されます。

DNSサーバの起動

〔サービスの開始〕では、DNSサーバをシステムのブート時(システムのブート中)に起動するか、それとも手動で起動するかを指定します。DNSサーバをすぐに起動するには、〔*Start DNS Server Now*〕を選択します。DNSサーバを停止するには、〔*DNSサーバの停止*〕を選択します。現在の設定を保存するには、〔*Save Settings and Restart DNS Server Now*〕を選択します。ファイアウォールのDNSポートを開くには〔*ファイアウォール内でポートを開く*〕を、ファイアウォールの設定を変更するには〔*Firewall Details*〕をクリックします。

〔*LDAPサポートを有効にする*〕を選択すると、ゾーンファイルがLDAPデータベースによって管理されるようになります。ゾーンデータを変更してそれがLDAPデータベースに書き込まれると、設定を再ロードするように要求されます。DNSサーバを再起動すると、変更がすぐに反映されます。

DNSサーバ:基本オプション

このセクションでは、基本的なサーバオプションを設定します。[オプション]メニューから設定する項目を選択して、対応する入力フィールドに値を指定します。新しいエントリを追加するには、[追加]を選択してください。

ログ

DNSサーバがログに記録する内容とログの方法を設定するには、[ログ記録]を選択します。[Log Type]に、DNSサーバがログデータを書き込む場所を指定します。システム全体のログファイル [/var/log/messages] を使用する場合は[システムログ]を、別のファイルを指定する場合は[ファイル]を選択します。別のファイルを指定する場合は、ファイル名、ログファイルの最大サイズ(メガバイト(MB))と保管するログファイル数(バージョン)も指定します。

[追加のログ]には、さらに詳細なオプションが用意されています。[すべてのDNSクエリをログに記録]を有効にすると、すべてのクエリがログに記録されるため、ログファイルが非常に大きくなる可能性があります。ですから、このオプションを有効にするのはデバッグ時だけにすることをお勧めします。DHCPサーバとDNSサーバ間でのゾーン更新時のデータトラフィックをログに記録するには、[ゾーン更新をログに記録]を有効にします。マスタからスレーブへのゾーン転送時のデータトラフィックをログに記録するには、[ゾーン転送をログに記録]を有効にします。詳細については、[図33.4.「DNSサーバ:ログの記録」](#) (679 ページ)を参照してください。

図 33.4 DNSサーバ: ログの記録

ACLの使用

このウィンドウでは、アクセス制限を実施するACL(アクセス制御リスト)を定義します。[名前]に個別名を入力したら、次の形式で、[値]にIPアドレス(ネットマスクは省略可)を指定します。

```
{ 10.10/16; }
```

設定ファイルの構文に従って、アドレスの末尾にはセミコロンを付け、中カッコで囲む必要があります。

TSIGキー

TSIG(トランザクションシグネチャ)の主な目的は、DHCPおよびDNSサーバ間で安全な通信を行うことです。33.7項「安全なトランザクション」(696 ページ)を参照してください。

TSIGキーを生成するには、[キーID] フィールドに個別名を入力し、キーを格納するファイルを[ファイル名] フィールドに入力します。[追加] をクリックすると、入力内容が確定されます。

以前に作成したキーを使用するには、[キーID] フィールドを空白にして、そのキーが格納されているファイルを[ファイル名]で選択します。その後、[追加]をクリックすると、入力内容が確定されます。

スレーブゾーンの追加

スレーブゾーンを追加するには、[DNSゾーン]を選択し、ゾーンタイプに[Slave]を選択し、[追加]をクリックします。

[マスタDNSサーバIP]の[ゾーンエディタ]で、データの転送元としてスレーブが使用するマスタを指定します。サーバへのアクセスを制限するために、リストから定義済みのACLを1つ選択します。詳細については、[図 33.5](#)、「DNSサーバ:スレーブゾーンエディタ」(680 ページ)を参照してください。

図 33.5 DNSサーバ:スレーブゾーンエディタ

DNSサーバ:スレーブゾーンエディタ
このダイアログでは、ゾーンのダイナミックDNSの設定変更 およびゾーンへのアクセスの制御を行うことができます。

ゾーンを動的に更新できるようにするには、[動的更新の許可]を設定し、[Tsigキー]を選択します。ゾーンの動的な更新を許可する前に、少なくともTsigキーを1つ定義しておく必要があります。

ゾーンの転送を許可するには、[ゾーン転送を有効にする]を選択し、リモートホストでゾーンを転送するときに有効にされる[ACL]を選択してください。ゾーンの転送を許可する前に、少なくとも1つACLを定義しておく必要があります。

ゾーンエディタ
ゾーンの設定

基本(B) NSレコード(D) MXレコード(X) SOA(S) レコード(E)

☐ 動的更新の許可(L)

Tsigキー(G)

☒ ゾーン転送を有効にする(Z)

ACL

☒ any
☐ localhost
☐ localnet
☐ none

キャンセル(C) 中止(B) OK(O)

マスタゾーンの追加

マスタゾーンを追加するには、[DNSゾーン]を選択し、ゾーンタイプに[マスタ]を選択し、新規ゾーンの名前を書き込み、[追加]をクリックします。

マスタゾーンの編集

マスタゾーンを編集するには、[DNSゾーン] を選択し、ゾーンタイプに [Master] を選択し、テーブルからマスタゾーンを選択し、[編集] をクリックします。このダイアログには、[基本] (最初に表示される)、[NSレコード]、[MXレコード]、[SOA]、および [レコード] などのページがあります。

に示す基本ダイアログを使用すると、ダイナミックDNSの設定と、クライアントおよびスレーブネームサーバへのゾーン転送に関するアクセスオプションを定義できます。図33.6、「DNSサーバ:ゾーンエディタ(基本)」(681 ページ) ゾーンの動的更新を許可するには、[動的更新の許可] および対応するTSIGキーを選択します。このキーは、更新アクションの開始前に定義しておく必要があります。ゾーン転送を有効にするには、対応するACLを選択します。ACLは事前に定義しておく必要があります。

図 33.6 DNSサーバ: ゾーンエディタ(基本)

DNSゾーンエディタ
このダイアログでは、ゾーンのダイナミックDNSの設定変更 およびゾーンへのアクセスの制御を行うことができます。

ゾーンを動的に更新できるようにするには、[動的更新の許可]を設定し、[TSIGキー]を選択します。ゾーンの動的な更新を許可する前に、少なくともTSIGキーを1つ定義しておく必要があります。

ゾーンの転送を許可するには、[ゾーン転送を有効にする]を選択し、リモートホストでゾーンを転送するときに有効にされる[ACL]を選択してください。ゾーンの転送を許可する前に、少なくとも1つACLを定義しておく必要があります。

ゾーンエディタ
ゾーンの設定:

基本(B) NSレコード(D) MXレコード(X) SOA(S) レコード(E)

☒ 動的更新の許可(L)
TSIGキー(K)

☒ ゾーン転送を有効にする(Z)
ACL
☐ any
☐ localhost
☐ localnets
☒ none

キャンセル(C) 中止(B) OK(O)

ゾーンエディタ(NSレコード)

このダイアログでは、指定したゾーンの代替ネームサーバを定義できます。リストに自分が使用しているネームサーバが含まれていることを確認してください。レコードを追加するには、[追加するネームサーバ] にレコード名を入力し、[追加] をクリックして確定します。詳細について

は、[図 33.7. 「DNSサーバ:ゾーンエディタ\(NSレコード\)」](#) (682 ページ)を参照してください。

図 33.7 DNSサーバ:ゾーンエディタ(NSレコード)

NSレコード
新しいネームサーバを追加するには、ネームサーバのアドレスを入力し、[追加]をクリックしてください。示されたネームサーバのいずれかを削除するには、リストから選択して[削除]をクリックしてください。

ゾーンエディタ
ゾーンの設定

基本(B) NSレコード(D) MXレコード(X) SOA(S) レコード(E)

追加するネームサーバ(N)

ネームサーバのリスト(L)

ゾーンエディタ(MXレコード)

現行ゾーンのメールサーバを既存のリストに追加するには、対応するアドレスと優先順位の値を入力します。その後、[\[追加\]](#)を選択して確定します。詳細については、[図 33.8. 「DNSサーバ:ゾーンエディタ\(MXレコード\)」](#) (683 ページ)を参照してください。

33.8 DNSサーバ: ゾーンエディタ(MXレコード)

MXレコード
新しいメールサーバを追加するには、メールサーバの[アドレス]と[優先度]を入力し、[追加]をクリックしてください。示されたメールサーバのいずれかを削除するには、リストから選択して[削除]をクリックしてください。

ゾーンエディタ

ゾーンの設定example.com

基本(B)NSレコード(D)MXレコード(X)SOA(S)レコード(E)

追加するメールサーバ

アドレス(A)優先度(P)追加(A)

メールリレーリスト

メールサーバ優先度削除(D)

キャンセル(C)中止(B)OK(O)

ゾーンエディタ(SOA)

このページでは、SOA (start of authority)レコードを作成できます。個々のオプションについては、[例 33.6. 「/var/lib/named/world.zoneファイル」 \(691 ページ\)](#)を参照してください。LDAPを介して管理される動的ゾーンの場合、SOAレコードの変更がサポートされないので注意してください。

33.9 DNSサーバ: ゾーンエディタ(SOA)

SOAレコードの編集設定
SOAレコードに関する情報を設定します。

[シリアル番号]は、マスターサーバでゾーンの変更があったかどうかの判断に 使用される番号です。スレーブサーバは、必ずしもゾーン全体と同期を取る必要があるとは 限りません。

[TTL]は、明示的なTTLを持たないゾーンのすべてのレコードの 残存時間を指定します。

[更新間隔]では、マスターサーバからスレーブサーバに対して ゾーンの同期を取る頻度を指定します。

[リトライ間隔]では、同期が失敗した場合にスレーブサーバが マスターサーバのゾーンと同期を取る頻度を指定します。

[有効期限]は、スレーブサーバでゾーンが期限切れになり、ゾーンが 同期化されるまでスレーブサーバが応答を停止する期間を表します。

【最小値】では、スレーブサーバが否定応答(名前解決の失敗)をキャッシュ する期間を設定します。

ゾーンエディタ

ゾーンの設定example.com

基本(B)NSレコード(D)MXレコード(X)SOA(S)レコード(E)

シリアル番号(A)更新間隔(E)単位(U)

20081007003時間

TTL(L)リトライ間隔(U)単位(U)

2日1時間

有効期限(E)単位(M)

1週

最小限(M)単位(D)

1日

キャンセル(C)中止(B)OK(O)

ゾーンエディタ(レコード)

このダイアログでは、名前解決を管理します。[レコードキー]では、ホスト名を入力してレコードタイプを選択します。Aレコード]はメインエントリを表します。この値はIPアドレスでなければなりません。

[CNAME]はエイリアスです。[NS]および[MX]の各タイプを指定すると、[NSレコード]および[MXレコード]の各タブで提供される情報に基づいて、詳細レコードまたは部分レコードが展開されます。この3つのタイプのは、既存のAレコードに解決されます。[PTR]は逆引きゾーン用レコードです。これは、Aレコードとは反対にIPアドレスに対するホスト名を定義します。

33.3 ネームサーバBINDの起動

SUSE Linux Enterprise®システムでは、BIND (*Berkeley Internet name domain*)が事前に設定された状態で提供されているので、インストールが正常に完了すればすぐにネームサーバが起動されます。既にインターネットに接続

し、/etc/resolv.confのlocalhostにネームサーバアドレス127.0.0.1が入力されている場合、通常、プロバイダのDNSを知らなくても、既に機能する名前解決メカニズムが存在します。この場合、BINDは、ルートネームサーバを介して名前の解決を行うため、処理が非常に遅くなります。通常、効率的で安全な名前解決を実現するには、forwardersの下の設定ファイル/etc/named.confにプロバイダのDNSとそのIPアドレスを入力する必要があります。いままでこれが機能している場合、ネームサーバは、純粋なキャッシュ専用ネームサーバとして動作しています。ネームサーバは、自身のゾーンを設定してはじめて、本当のDNSになります。これの簡単な例については、/usr/share/doc/packages/bind/configのドキュメントを参照してください。

ティップ: ネームサーバ情報の自動取得

インターネット接続やネットワーク接続のタイプによっては、ネームサーバ情報を自動的に現在の状態に適合させることができます。これを行うには、/etc/sysconfig/network/configファイル内でMODIFY_NAMED_CONF_DYNAMICALY変数にyesを設定します。

ただし、公式ドメインは、管理団体から割り当てられるまでセットアップしないでください。独自のドメインを持っていて、プロバイダがそれを管理し

ている場合でも、**BIND**はそのドメインに対する要求を転送しないので、そのドメインを使用しないほうが賢明です。たとえば、プロバイダの**Web**サーバは、このドメインからはアクセスできません。

ネームサーバを起動するには、rootユーザとして、コマンド**rcnamedstart**を入力します。右側に緑色で「done」と表示されたら、**named** (ネームサーバプロセス名)が正常に起動しています。サーバが正常に起動したらずぐに、**host**または**dig**プログラムを用いてローカルシステム上でネームサーバをテストしてください。デフォルトサーバ**localhost**とそのアドレス**127.0.0.1**が返されるはずです。これが返されない場合は、**/etc/resolv.conf**に含まれているネームサーバエントリが誤っているか、同ファイルが存在しないかのいずれかです。最初のテストとして、**host127.0.0.1**を入力します。これは常に機能するはずです。エラーメッセージが表示された場合は、**rcnamed status**を使用して、サーバが実際に起動されていることを確認します。ネームサーバが起動しない場合、または予想しない動作をしている場合、多くはログファイル**/var/log/messages**でその原因が明らかになります。

プロバイダのネームサーバまたはフォワーダとして既にネットワーク上で動作しているネームサーバを使用する場合は、**forwarders**の下**options**セクションに、対応する**IP**アドレスまたはアドレスを入力します。に含まれているアドレスは、単なる例です。例 33.1. 「**named.conf**ファイルの転送オプション」 (685 ページ)各自サイトの設定に合わせて変更してください。

例 33.1 **named.conf**ファイルの転送オプション

```
options {  
    directory "/var/lib/named";  
    forwarders { 10.11.12.13; 10.11.12.14; };  
    listen-on { 127.0.0.1; 192.168.0.99; };  
    allow-query { 127/8; 192.168.0/24; };  
    notify no;  
};
```

optionsエントリの後には、ゾーン用のエントリ、**localhost**と**0.0.127.in-addr.arpa**が続きます。「**.**」の下**type hint** (タイプヒント) は必ず存在しなければなりません。対応するファイルは、変更する必要がなく、そのまま機能します。また、各エントリの末尾が「**;**」で閉じられ、中カッコが適切な位置にあることを確認してください。設定ファイル**/etc/named.conf**またはゾーンファイルを変更したら、**rcnamedreload**を使用して、**BIND**にそれらを再読み込みさせます。または、**rcnamedrestart**を使用してネームサーバを停

止、再起動しても同じ結果が得られます。サーバは`rcnamedstop`を入力していつでも停止することができます。

33.4 設定ファイル/etc/named.conf

BINDネームサーバ自体の設定はすべて、ファイル`/etc/named.conf`に格納されます。ただし、ホスト名、IPアドレスなどで構成され、ドメインが処理するゾーンデータは、`/var/lib/named`ディレクトリ内の個別のファイルに格納されます。この詳細については、後述します。

`/etc/named.conf`ファイルは、大きく2つのエリアに分けられます。1つは一般的な設定用の`options`セクション、もう1つは個々のドメインの`zone`エントリで構成されるセクションです。ログセクションと`acl` (アクセス制御リスト)エントリは省略可能です。コメント行は、行頭に`#`記号または`//`を指定します。最も基本的な`/etc/named.conf`ファイルの例を、[例 33.2. 「基本的な/etc/named.confファイル」 \(686 ページ\)](#)に示します。

例 33.2 基本的な/etc/named.confファイル

```
options {
    directory "/var/lib/named";
    forwarders { 10.0.0.1; };
    notify no;
};

zone "localhost" in {
    type master;
    file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};

zone "." in {
    type hint;
    file "root.hint";
};
```

33.4.1 重要な設定オプション

`directory "filename";`

BINDが検索する、ゾーンファイルが格納されているディレクトリを指定します。通常は/var/lib/namedです。

`forwarders { ip-address; };`

DNS要求が直接解決できない場合、それらが転送されるネームサーバ(ほとんどの場合、プロバイダのネームサーバ)を指定します。*ip-address*には、IPアドレスを10.0.0.1のように指定します。

`forward first;`

ルートネームサーバでDNS要求の解決を試みる前に、それらを転送するようにします。`forward first`の代わりに`forward only`を指定すると、要求が転送されたままになり、ルートネームサーバには送り返されません。このオプションは、ファイアウォール構成で使います。

`listen-on port 53 { 127.0.0.1; ip-address; };`

BINDがクライアントからのクエリを受け取るネットワークインタフェースとポートを指定します。`port 53`はデフォルトポートであるため、明示的に指定する必要はありません。ローカルホストからの要求を許可するには、127.0.0.1と記述します。このエントリ全体を省略した場合は、すべてのインタフェースがデフォルトで使われます。

`listen-on-v6 port 53 { any; };`

BINDがIPv6クライアント要求をリッスンするポートを指定します。*any*以外で指定できるのは*none*だけです。IPv6に関して、サーバはワイルドカードアドレスのみ受け付けます。

`query-source address * port 53;`

ファイアウォールが発信DNS要求をブロックする場合、このエントリが必要です。BINDに対し、外部への要求をポート53から発信し、1024を超える上位ポートからは発信しないように指示します。

`query-source address * port 53;`

BINDがIPv6のクエリに使用するポートを指定します。

`allow-query { 127.0.0.1; net; };`

クライアントがDNS要求を発信できるネットワークを定義します。`net`には、アドレス情報を192.168.1/24のように指定します。末尾の/24は、ネットマスクの短縮表記で、この場合255.255.255.0を表します。

`allow-transfer ! *;;`

ゾーン転送を要求できるホストを制御します。この例では、`!`が使用されているので、ゾーン転送要求は完全に拒否されます。`*`。このエントリがなければ、ゾーン転送をどこからでも制約なしに要求できます。

`statistics-interval 0;`

このエントリがなければ、BINDは1時間ごとに数行の統計情報を生成して/var/log/messagesに保存します。`0`を指定すると、統計情報をまったく生成しないか、時間間隔を分単位で指定します。

`cleaning-interval 720;`

このオプションは、BINDがキャッシュをクリアする時間間隔を定義します。キャッシュがクリアされるたびに、/var/log/messagesにエントリが追加されます。時間の指定は分単位です。デフォルトは60分です。

`statistics-interval 0;`

BINDは定期的にインタフェースを検索して、新しいインタフェースや存在しなくなったインタフェースがないか確認します。この値を0に設定すると、この検索が行われなくなり、BINDは起動時に検出されたインタフェースのみをリッスンします。0以外の値を指定する場合は分単位で指定します。デフォルトは60分です。

`notify no;`

`no`に設定すると、ゾーンデータを変更したとき、またはネームサーバが再起動されたときに、他のネームサーバに通知されなくなります。

33.4.2 ロギング

BINDでは、何を、どのように、どこにログ出力するかを詳細に設定できます。通常は、デフォルト設定のままで十分です。**例 33.3. 「ログを無効にするエントリ」** (689 ページ)に、このエントリの最も簡単な形式、すなわちログをまったく出力しない例を示します。

例 33.3 ログを無効にするエントリ

```
logging {  
    category default { null; };  
};
```

33.4.3 ゾーンエントリ

例 33.4 *my-domain.de*のゾーンエントリ

```
zone "my-domain.de" in {  
    type master;  
    file "my-domain.zone";  
    notify no;  
};
```

zoneの後、管理対象のドメイン名my-domain.deを指定し、次にinと関連のオプションを中カッコで囲んで指定します(参照)。例 33.4. 「my-domain.deのゾーンエントリ」(689 ページ)スレーブゾーンを定義するには、typeをslaveに変更し、このゾーンをmasterとして管理することをネームサーバに指定します(例 33.5. 「other-domain.deのゾーンエントリ」(689 ページ)参照)。これが他のマスタのスレーブとなることもあります。

例 33.5 *other-domain.de*のゾーンエントリ

```
zone "other-domain.de" in {  
    type slave;  
    file "slave/other-domain.zone";  
    masters { 10.0.0.1; };  
};
```

ゾーンオプション

type master;

masterを指定して、BINDに対し、ゾーンがローカルネームサーバによって処理されるように指示します。これは、ゾーンファイルが正しい形式で作成されていることが前提となります。

type slave;

このゾーンは別のネームサーバから転送されたものです。必ずmastersとともに使用します。

`type hint;`

ルートネームサーバの設定には、ゾーン.(hintタイプ)を使用します。このゾーン定義はそのまま使用できます。

`file my-domain.zone`またはfile 「slave/other-domain.zone」;

このエントリは、ドメインのゾーンデータが格納されているファイルを指定します。スレーブの場合、このデータを他のネームサーバから取得するので、このファイルは不要です。マスタとスレーブのファイルを区別するには、スレーブファイルにディレクトリslaveを使用します。

`masters { server-ip-address; };`

このエントリは、スレーブゾーンにのみ必要です。ゾーンファイルの転送元となるネームサーバを指定します。

`allow-update {! *; };`

このオプションは、外部書き込みアクセスを制御し、クライアントにDNSエントリへの書き込み権を付与することができます。ただし、これは通常、セキュリティ上の理由で好ましくありません。このエントリがなければ、ゾーンの更新は完全に拒否されます。!*によってそのような操作が禁止されるため、前述のエントリは同じものをアーカイブします。

33.5 ゾーンファイル

ゾーンファイルは2種類必要です。一方はIPアドレスをホスト名に割り当て、もう一方は逆にIPアドレスのホスト名を提供します。

ティップ: ゾーンファイルでのピリオドの使用

.はゾーンファイル内で重要な意味を持ちます。末尾に.のホスト名を指定すると、ゾーンが追加されます。完全なホスト名を完全なドメイン名とともに指定する場合は、末尾に.を付けて、ドメインが追加されないようにします。ピリオドの打ち忘れや位置の間違いは、ネームサーバ設定エラーの原因としておそらく最も頻繁に見られるものです。

最初に、ドメインworld.cosmosに責任を負うゾーンファイルworld.zoneについて示します(例 33.6. 「/var/lib/named/world.zone ファイル」 (691 ページ)参照)。

例 33.6 /var/lib/named/world.zone ファイル

```
$TTL 2D
world.cosmos. IN SOA      gateway root.world.cosmos. (
                        2003072441 ; serial
                        1D          ; refresh
                        2H          ; retry
                        1W          ; expiry
                        2D )        ; minimum

                        IN NS      gateway
                        IN MX      10 sun

gateway  IN A      192.168.0.1
         IN A      192.168.1.1
sun      IN A      192.168.0.2
moon     IN A      192.168.0.3
earth    IN A      192.168.1.2
mars     IN A      192.168.1.3
www      IN CNAME   moon
```

1行目:

\$TTLは、このファイルのすべてのエントリに適用されるデフォルトの寿命(time to live)です。この例では、エントリは2日間(2 D)有効です。

2行目:

ここから、SOA (start of authority)制御レコードが始まります。

- 管理対象のドメイン名は、先頭にあるworld.cosmosです。これは、末尾に. (ピリオド)が付いています。ピリオドを付けないと、ゾーンが再度末尾に追加されてしまいます。あるいはピリオドを@で置き換えるこ

ともできます。その場合は、ゾーンが/etc/named.confの対応するエントリから抽出されます。

- INSOAの後には、このゾーンのマスタであるネームサーバの名前を指定します。これらの名前は末尾に.(ピリオド)が付いていないので、gatewayからgateway.world.cosmosに拡張されます。
- この後には、このネームサーバの責任者の電子メールアドレスが続きます。@記号は既に特別な意味を持つので、ここでは代わりに.(ピリオド)を使用します。root@world.cosmosの場合、エントリはroot.world.cosmosとなります。.ここでもゾーンが追加されないよう、.を末尾につける必要があります。
- (は、)までの行をすべてSOAレコードに含める場合に使用します。

3行目:

シリアル番号は任意の番号で、このファイルを変更するたびに増加します。変更があった場合、セカンダリネームサーバ(スレーブサーバ)に通知する必要があります。これには、日付と実行番号をYYYYMMDDNNという形式で表記した10桁の数値が、慣習的に使用されています。

4行目:

リフレッシュレートは、セカンダリネームサーバがゾーンserial numberを確認する時間間隔を指定します。この例では1日です。

5行目:

再試行間隔は、エラーが生じた場合に、セカンダリネームサーバがプライマリサーバに再度通知を試みる時間間隔を指定します。この例では2時間です。

6行目:

有効期限は、セカンダリネームサーバがプライマリサーバに再通知できなかった場合に、キャッシュしたデータを廃棄するまでの時間枠を指定します。この例では1週間です。

7行目:

SOAレコードの最後のエントリは、ネガティブキャッシュTTLです。これは、DNSクエリが解決できないという他のサーバからの結果をキャッシュしておく時間です。

9行目:

IN NSでは、このドメインを担当するネームサーバを指定します。
gatewayは、gateway.world.cosmosに拡張されます。これは、末尾に.が付いていないためです。このように、プライマリネームサーバと各セカンダリネームサーバに1つずつ指定する行がいくつかあります。/etc/named.confでnotifyをnoに設定しない限り、ゾーンデータが変更されると、ここにリストされているすべてのネームサーバにそれが通知されます。

10行目:

MXレコードは、ドメインworld.cosmos宛ての電子メールを受領、処理、および転送するメールサーバを指定します。この例では、ホストsun.world.cosmosが指定されています。ホスト名の前の数字は、プリファレンス値です。複数のMXエントリが存在する場合、値が最も小さいメールサーバが最初に選択され、このサーバへのメール配信ができなければ、次に小さい値のメールサーバが試みられます。

行12-17:

これらは、ホスト名に1つ以上のIPアドレスが割り当てられている実際のアドレスレコードです。ここでは、名前が.なしでリストされています。これは、これらの名前にはドメインが含まれていないためです。したがって、これらの名前にはすべて、world.cosmosが追加されます。ホストgatewayは、ネットワークカードが2枚搭載されているので、2つのIPアドレスが割り当てられます。ホストアドレスが従来型のアドレス(IPv4)の場合、レコードにAAAAが付きます。アドレスがIPv6アドレスの場合、エントリにAAAA 0が付きます。以前は、IPv6アドレスはAAAAで示されていましたが、現在では廃止されました。

注意: IPv6の構文

IPv6の構文は、IPv4と少し異なっています。断片化の可能性があるため、アドレスの前に消失したビットに関する情報を入力する必要があります。完全に断片化されないアドレスを使用する場合でも、この情報を入力する必要があります。構文のあるIPv4レコード

```
pluto IN          AAAA 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto IN          AAAA 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

消失したビットに関する情報はIPv6形式で追加する必要があります。上記の例は完全なので(いずれのビットも消失していない)、このレコードのIPv6形式は次のようになります。

```
pluto IN AAAA 0 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto IN AAAA 0 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

IPv6マッピングでは、IPv4アドレスを使用しないでください。

18行目:
エイリアスwwwをmondの別名として使用できます(CNAMEは*canonical name*(キャノニカル名)という意味です)。

擬似ドメインin-addr.arpaは、IPアドレスからホスト名への逆引き参照に使用されます。このドメインの前に、IPアドレスのネットワーク部分が逆順に指定されます。たとえば、192.168.1は、1.168.192.in-addr.arpaに解決されます。参照先 [例 33.7. 「逆引き」 \(694 ページ\)](#)。

例 33.7 逆引き

```
$TTL 2D
1.168.192.in-addr.arpa. IN SOA gateway.world.cosmos. root.world.cosmos. (
                                2003072441      ; serial
                                1D                ; refresh
                                2H                ; retry
                                1W                ; expiry
                                2D )              ; minimum

                                IN NS              gateway.world.cosmos.

1                               IN PTR            gateway.world.cosmos.
2                               IN PTR            earth.world.cosmos.
3                               IN PTR            mars.world.cosmos.
```

1行目:
\$TTLは、このファイルのすべてのエントリに適用される標準のTTLです。

2行目:
この設定ファイルは、ネットワーク192.168.1.0の逆引きを有効にします。ゾーン名は1.168.192.in-addr.arpaであり、これはホスト名に追加しません。そのため、すべてのホスト名はドメインの最後に.を付け

た完全形式で入力します。残りのエントリは、前のworld.cosmosの例の記述と同じです。

行3-7:

前の例のworld.cosmosを参照してください。

9行目:

正引きの場合と同様、この行は、このゾーンを担当するネームサーバを指定します。ただし、ホスト名はドメインと末尾の.(ピリオド)が付いた完全な形で指定されます。

行 11-13:

これらはそれぞれのホスト上でのIPアドレスを示すポインタレコードです。IPアドレスの最後のオクテットのみが、行の最初に入力され、末尾に.(ピリオド)は付きません。ゾーンをこれに追加すると(.in-addr.arpaを付けずに)、完全なIPアドレスが逆順で生成されます。

通常、異なるバージョンのBIND間のゾーン転送は、問題なく行えるはずです。

33.6 ゾーンデータの動的アップデート

動的アップデートという用語は、マスタサーバのゾーンファイル内のエントリが追加、変更、削除される操作を指します。この仕組みは、RFC 2136に記述されています。動的アップデートをゾーンごとに個別に構成するには、オプションのallow-updateルールまたはupdate-policyルールを追加します。動的に更新されるゾーンを手動で編集してはなりません。

サーバに更新エントリを転送するには、nsupdateコマンドを使用します。このコマンドの詳細な構文については、nsupdateのマニュアルページ(man8 nsupdate)を参照してください。セキュリティ上の理由から、こうした更新はTSIGキーを使用して実行するようにしてください(33.7項「安全なトランザクション」(696 ページ)参照)。

33.7 安全なトランザクション

安全なトランザクションは、共有秘密キー(TSIGキーとも呼ばれる)に基づくトランザクション署名(TSIG)を使用して実現できます。ここでは、このキーの生成方法と使用方法について説明します。

安全なトランザクションは、異なるサーバ間の通信、およびゾーンデータの動的アップデートに必要です。アクセス制御をキーに依存する方が、単にIPアドレスに依存するよりもはるかに安全です。

TSIGキーの生成には、次のコマンドを使用します(詳細については、`mandnssec-keygen`を参照)。

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

これにより、次のような形式の名前を持つファイルが2つ作成されます。

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

キー自体(`ejIkuCyyGJwwuN3xAteKgg==`のような文字列)は、両方のファイルにあります。キーをトランザクションで使用するには、2番目のファイル(`Khost1-host2.+157+34265.key`)を、できれば安全な方法で(たとえば`scp`を使用して)、リモートホストに転送する必要があります。`host1`と`host2`の間で安全な通信ができるようにするには、リモートサーバでキーをファイル`/etc/named.conf`に含める必要があります。

```
key host1-host2. {  
    algorithm hmac-md5;  
    secret "ejIkuCyyGJwwuN3xAteKgg==";  
};
```

警告: `/etc/named.conf`のファイルパーミッション

`/etc/named.conf`のファイルパーミッションが適切に制限されていることを確認してください。このファイルのデフォルトのパーミッションは0640で、オーナーが`root`、グループが`named`です。この代わりに、パーミッションが制限された別ファイルにキーを移動して、そのファイルを`/etc/`

named.conf内にインクルードすることもできます。外部ファイルをインクルードするには、次のようにします。

```
include "filename"
```

ここで、filenameには、キーを持つファイルへの絶対パスを指定します。

サーバhost1がhost2(この例では、アドレス192.168.2.3)のキーを使用できるようにするには、host1の/etc/named.confに次の規則が含まれている必要があります。

```
server 192.168.2.3 {  
    keys { host1-host2. ;};  
};
```

同様のエントリがhost2の設定ファイルにも含まれている必要があります。

IPアドレスとアドレス範囲に対して定義されているすべてのACL(アクセス制御リスト—ACLファイルシステムと混同しないこと)にTSIGキーを追加してトランザクションセキュリティを有効にします。対応するエントリは、次のようになります。

```
allow-update { key host1-host2. ;};
```

このトピックについての詳細は、update-policyの下、『*BIND Administrator Reference Manual*』を参照してください。

33.8 DNSセキュリティ

DNSSEC、すなわちDNSセキュリティは、RFC2535に記述されています。DNSSECに利用できるツールについては、BINDのマニュアルを参照してください。

ゾーンが安全だといえるためには、1つ以上のゾーンキーが関連付けられている必要があります。キーはホストキーと同様、dnssec-keygenによって生成されます。現在、これらのキーの生成には、DSA暗号化アルゴリズムが使用されています。生成されたパブリックキーは、\$INCLUDEルールによって、対応するゾーンファイルにインクルードします。

生成したすべてのキーは、dnssec-makekeysetコマンドによって1つのセットにパッケージングし、安全な方法で親ゾーンに転送する必要があります。

親ゾーンでは、`dnssec-signkey`によってセットに署名が付されます。このコマンドによって複数のファイルが生成され、これらのファイルを使用して`dnssec-signzone`が実行され、ゾーンに署名が付されます。このときにファイルが生成されて、各ゾーンの`/etc/named.conf`にインクルードされます。

33.9 詳細情報

ここで扱ったトピックの詳細については、`/usr/share/doc/packages/bind/ディレクトリ`にインストールされる`bind-doc`パッケージ内の『`BIND Administrator Reference Manual`』を参照してください。`BIND`に付属のマニュアルやマニュアルページで紹介されているRFCも、必要に応じて参照してください。`/usr/share/doc/packages/bind/README.SuSE`には、`SUSE Linux Enterprise`の`BIND`に関する最新情報が含まれています。

DHCP

dynamic host configuration protocol (DHCP)の目的は、ネットワーク環境設定を各ワークステーションでローカルに行うのではなく、サーバから一元的に割り当てることです。DHCPを使用するように設定されたクライアントは、自身の静的アドレスを制御できません。サーバからの指示に従って、すべてが自動的に設定されるからです。クライアント側でNetworkManagerを使用する場合は、クライアントを設定する必要はありません。これは、環境を変更し、一度に1つのインタフェースしかない場合に便利です。DHCPサーバが実行しているマシン上ではNetworkManagerを使用しないでください。

ティップ: IBM System z:DHCPサポート

IBM System zプラットフォーム上では、OSAおよびOSA Expressネットワークカードを使用しているインタフェースに対してのみDHCPを使用できます。DHCPの自動環境設定機能に必要なMACアドレスを持つのは、これらのカードだけです。

DHCPサーバの設定方法の1つとして、ネットワークカードのハードウェアアドレス(ほとんどの場合、固定)を使用して各クライアントを識別し、そのクライアントがサーバに接続するたびに同じ設定を提供する方法があります。DHCPはまた、サーバが用意したアドレスプールから、アドレスを各クライアントに動的に割り当てるように設定することもできます。後者の場合、DHCPサーバは要求を受信するたびに、接続が長期にわたる場合でも、クライアントに同じアドレスを割り当てようと試みます。これは、ネットワークにアドレス以上のクライアントが存在しない場合にのみ機能します。

DHCPは、システム管理者の負担を軽減します。サーバの環境設定ファイルを編集して、アドレスに関するあらゆる変更(大きな変更であっても)と一般的なネットワークの環境設定を一元的に実装できます。これは、多数のワークステーションをいちいち再設定するのに比べるとはるかに簡単です。また、特に新しいマシンをネットワークに統合する場合、IPアドレスをプールから割り当てられるので、作業が楽になります。適切なネットワークの環境設定をDHCPサーバから取得する方法は、日常的に、ラップトップをさまざまなネットワークで使用する場合に特に便利です。

DHCPサーバは、クライアントが使用するIPアドレスとネットマスクを供給するだけでなく、ホスト名、ドメイン名、ゲートウェイ、およびネームサーバアドレスも供給します。この他にも、DHCPを使用して一元的に設定できるパラメータがあり、たとえば、クライアントが現在時刻をポーリングするタイムサーバやプリントサーバも設定可能です。

34.1 YaSTによるDHCPサーバの設定

重要項目: LDAPのサポート

このバージョンのSUSE Linux Enterpriseでは、サーバの環境設定をローカルに(DHCPサーバを実行するホスト上に)格納するか、または環境設定データをLDAPサーバで管理させるように、YaSTのDHCPモジュールをセットアップできます。LDAPを使用するには、LDAP環境を設定してからDHCPサーバを設定してください。

YaSTのDHCPモジュールを使用すると、ローカルネットワーク用に独自のDHCPサーバをセットアップできます。このモジュールは、[簡易モード] または [エキスパートモード] で実行できます。

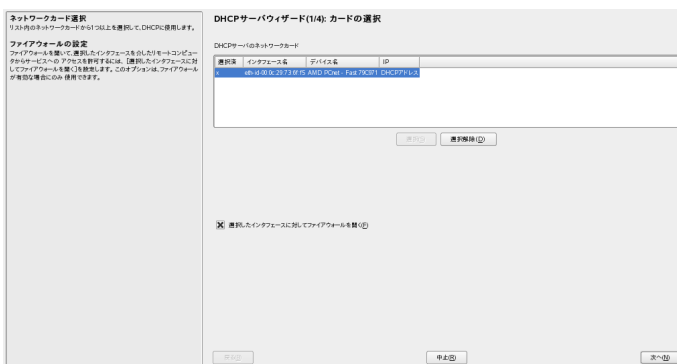
34.1.1 初期設定(ウィザード)

このモジュールを初めて起動すると、サーバ管理に関して少数の基本的な事項を決定するように要求されます。この初期セットアップを完了すると、必要最低限の機能が設定された基本的なサーバ設定が生成されます。エキスパートモードは、さらに高度な設定タスクを行う場合に使用できます。

カードの選択

最初のステップでは、YaSTによりシステムで使用可能なネットワークインタフェースが検査され、リスト形式で表示されます。リストから、DHCPサーバがリスンするインタフェースを選択し、**[追加]**をクリックします。この後、**[Open Firewall for Selected Interfaces]**を選択して、このインタフェース用のファイアウォールを開きます。詳細については、[図 34.1. 「DHCPサーバ:カードの選択」](#) (701 ページ)を参照してください。

図 34.1 DHCPサーバ:カードの選択



グローバル設定

チェックボックスを使って、LDAPサーバがDHCP設定を自動的に格納する必要があるかどうかを指定します。エントリフィールドに、DHCPサーバで管理する全クライアントのネットワークを指定します。この指定には、ドメイン名、タイムサーバのアドレス、プライマリネームサーバとセカンダリネームサーバのアドレス、印刷サーバとWINSサーバのアドレス (WindowsクライアントとLinuxクライアントの両方が混在するネットワークを使用する場合)、ゲートウェイアドレスおよびリース期間が含まれます。詳細については、[図 34.2. 「DHCPサーバ:グローバル設定」](#) (702 ページ)を参照してください。

☒ 34.2 DHCPサーバ:グローバル設定

[illegible]

動的DHCP

このステップでは、クライアントに対する動的IPアドレスの割り当て方法を設定します。そのためには、サーバがDHCPクライアントに割り当て可能なIPアドレスの範囲を指定します。これらのアドレスは、すべて同じネットマスクを使用する必要があります。また、クライアントがリースの延長を要求せずにIPアドレスを維持できるリース期間も指定します。必要に応じて、最大リース期間、つまりサーバが特定のクライアントのIPアドレスを保持する期間を指定します。詳細については、[図 34.3. 「DHCPサーバ: ダイナミックDHCP」](#) (702 ページ)を参照してください。

☒ 34.3 DHCPサーバ: ダイナミックDHCP

[illegible]

環境設定の完了と実行モードの設定

環境設定ウィザードの3つ目の手順を終了すると、最後にDHCPサーバの起動方法を定義するダイアログが表示されます。ここでは、システムの

ブート時にDHCPサーバを自動的に起動するか、テスト時など必要に応じて手動で起動するかを指定します。[完了] をクリックして、サーバの環境設定を完了します。参照先 [図 34.4. 「DHCPサーバ:起動」](#) (703 ページ)。基本環境設定に加え、特別なホスト管理機能を設定する場合は、左側のツリービューから [ホスト管理] を選択します([図 34.5. 「DHCPサーバ:ホスト管理」](#) (704 ページ)を参照)。

図 34.4 DHCPサーバ:起動

サービス開始
コンピュータを起動するたびにサービスを再起動するには、ブート時 を指定します。または、手動 を指定します。

エキストラブート環境設定
DHCPサーバの再起動と環境設定を入力するには、[DHCPサーバにホスト管理機能を有効にする]をクリックします。

DHCPサーバウィザード(4/4): 起動

サービスの種別

☐ ブート時

☒ 手動

DHCPサーバにホスト管理機能を有効にする

戻る 中止 完了

ホスト管理

前のセクションで説明した方法で動的DHCPを使用するかわりに、アドレスを疑似静的方式で割り当てるようにサーバを設定することもできます。そのためには、下部のエントリフィールドを使用して、この方法で管理するホストのリストを指定します。具体的には、[名前] と [IPアドレス] に、この種のクライアントに与える名前とIPアドレスを指定し、さらに [ハードウェアアドレス] と [ネットワークタイプ] (トークンリングまたはイーサネット)を指定します。上部に表示されるクライアントリストを修正するには、[追加]、[編集]、および[削除] を使用します。詳細については、[図 34.5. 「DHCPサーバ:ホスト管理」](#) (704 ページ)を参照してください。

図 34.5 DHCPサーバ:ホスト管理

34.1.2 エキスパート設定

前述の環境設定方法に加えて、DHCPサーバのセットアップを詳細に調整できるようにエキスパート設定モードが用意されています。エキスパート設定を開始するには、[エキスパート設定...]を選択します。

chroot環境と宣言

この最初のダイアログで[DHCPサーバの起動]を選択し、既存の環境設定を編集可能にします。DHCPサーバの動作のうち、重要なのはchroot環境またはchroot jailで動作してサーバホストを保護する機能です。DHCPサーバが外部からの攻撃にさらされるとしても、攻撃者はchroot jailの中にとどまるためシステムの残りの部分には進入できません。ダイアログの下部には、定義済みの宣言を示すツリービューが表示されます。これらの修正には、[追加]、[削除]、および[編集]を使用します。[詳細]を選択すると、上級者用のダイアログが追加表示されます。参照先 図 34.6. 「DHCPサーバ:Chroot Jailと宣言」(705 ページ)。[追加]を選択後、追加する宣言の種類を定義します。[詳細]から、サーバのログファイルの表示、TSIGキー管理の設定、およびDHCPサーバのセットアップに応じたファイアウォール設定の調整を行うことができます。

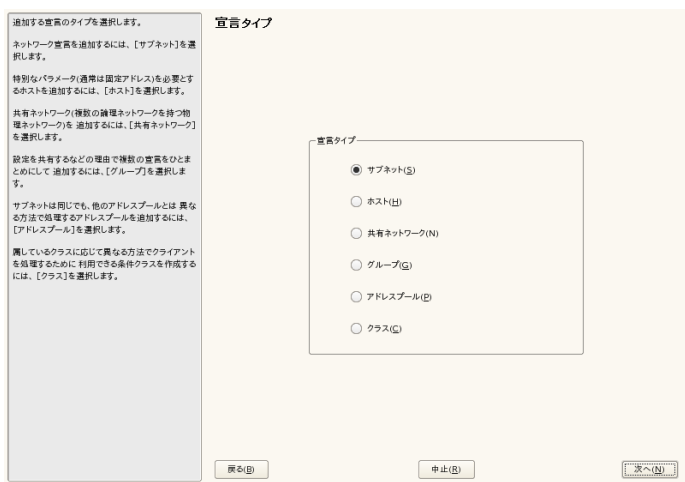
図 34.6 DHCPサーバ:Chroot Jailと宣言



宣言タイプの選択

DHCPサーバの「グローバルオプション」は、多数の宣言で構成されています。このダイアログでは、宣言タイプ「サブネット」、「ホスト」、「共有ネットワーク」、「グループ」、「アドレスプール」、および「クラス」を設定できます。この例は、新しいサブネットワークの選択を示しています(図 34.7.「DHCPサーバ:宣言タイプの選択」(705 ページ)を参照)。

図 34.7 DHCPサーバ:宣言タイプの選択



サブネットの設定

このダイアログでは、IPアドレスとネットマスクを使用して新しいサブネットを指定できます。ダイアログの中央部分で **[追加]**、**[編集]**、および **[削除]** を使用して、選択したサブネットのDHCPサーバ起動オプションを変更します。サブネットのダイナミックDNSを設定するには、**[ダイナミックDNS]** を選択します。

図 34.8 DHCPサーバ:サブネットの設定

サブネットの環境設定

サブネットの [ネットワークアドレス] および [ネットワークマスク] を指定します。

DHCPオプションを継承するには、テーブルの適切なエントリを 選択し、**[編集]** をクリックします。新しいオプションを追加するには、**[追加]** を使用します。オプションを 削除するには、オプションを選択し、**[削除]** をクリックします。

このサブネットのホストのダイナミックDNSを調整するには、**[ダイナミックDNS]** を使用します。

サブネットの環境設定

ネットワークアドレス(N) ネットワークマスク(M)

192.168.27.0 255.255.255.0

オプション	値
Default lease time	14400

[追加(A)] **[編集(E)]** **[削除(D)]** **[ダイナミックDNS(D)]**

[戻る(B)] **[中止(C)]** **[OK(O)]**

TSIGキー管理

前のダイアログでダイナミックDNSを設定するように選択した場合は、セキュアゾーン転送用のキー管理を設定できます。**[OK]** を選択すると別のダイアログが表示され、ダイナミックDNSのインタフェースを設定できます(図 34.10. 「**DHCPサーバ:ダイナミックDNS用のインタフェースの設定**」 (708 ページ)を参照)。

図 34.9 DHCPサーバ:TSIGの設定

TSIGキー管理
このダイアログでTSIGキーを管理します。

既存のTSIGキーの追加
すでに作成されているTSIGキーを追加するには、キーが含まれているファイルのファイル名を選択し、[追加]をクリックします。

新しいTSIGキーの作成
新しいTSIGキーを作成するには、キーを作成するファイルのファイル名およびキーを識別するキーIDを設定し、[生成]をクリックします。

TSIGキーの削除
設定済みのTSIGキーを削除するには、キーを選択して[削除]をクリックします。同じファイル内のすべてのキーが削除されます。サーバの環境設定でTSIGにキーが使用中の場合は削除できません。また、環境設定におけるそのキーの使用を中止する必要があります。

TSIGキー管理

既存のTSIGキーの追加

ファイル名(F)

新しいTSIGキーの作成

キーID(K) ファイル名(F)

現在のTSIGキー

キーID	ファイル名	<input type="button" value="削除(D)"/>

ダイナミックDNS:インタフェースの設定

ここでは、[このサブネットにダイナミックDNSを有効にする]を選択して、サブネットのダイナミックDNSを有効化できます。その後、ドロップダウンリストを使用して正引きゾーンと逆引きゾーン両方のTSIGキーを選択し、そのキーがDNSとDHCPサーバに共通であることを確認します。

[グローバルダイナミックDNS設定の更新]を使用すると、ダイナミックDNS環境に従ってグローバルDHCPサーバ設定を自動的に更新および調整できます。最後に、ダイナミックDNSに従って更新する正引きゾーンと逆引きゾーンについて、プライマリネームサーバの名前を個別に指定し、この2つのゾーンを定義します。ネームサーバがDHCPサーバと同じホスト上で動作する場合、これらのフィールドは空白のままでもかまいません。[OK]を選択すると、サブネットの設定ダイアログに戻ります(図 34.8. 「DHCPサーバ:サブネットの設定」(706 ページ)を参照)。[OK]を選択すると、エキスパート設定ダイアログに戻ります。

図 34.10 DHCPサーバ: ダイナミックDNS用のインタフェースの設定

ダイナミックDNSの有効化
このサブネットでのダイナミックDNSを有効にするには、[このサブネットでのダイナミックDNSを有効にする]を設定します。

TSIGキー
ダイナミックDNSを更新するには、認証キーを設定する必要があります。[TSIGキー]から認証に使用するキーを選択できます。このキーはDHCPサーバとDNSサーバ両方で同じでなければなりません。正引き、逆引き両方のゾーンのキーを指定してください。

DHCPサーバのグローバル設定
ダイナミックDNSが正しく動作するためには、DHCPサーバのグローバル設定を更新する必要があります。これを自動で行うには、[グローバルダイナミックDNS設定の更新]を設定します。

更新するゾーン
更新する正引きおよび逆引きのゾーンを指定します。その両方で、プライマリ/ネームサーバも指定します。ネームサーバがDHCPサーバと同じホストで稼働している場合は、ここを空欄にできます。

インタフェース環境設定

☒ このサブネットのダイナミックDNSを有効にする(E)

正引きゾーンのTSIGキー(K)
example

逆引きゾーンのTSIGキー(K)
example

☐ グローバルダイナミックDNS設定の更新(U)

ゾーン(Z) プライマリDNSサーバ(P)

逆引きゾーン(N) プライマリDNSサーバ(I)

戻る(B) 中止(R) OK(O)

ネットワークインタフェースの環境設定

DHCPサーバがリッスンするインタフェースを定義し、ファイアウォールの環境設定を調整するには、エキスパート設定ダイアログで [詳細] > [インタフェースの設定] の順に選択します。表示されるインタフェースリストから、DHCPサーバがリッスンするインタフェースを1つ以上選択します。すべてのサブネット内のクライアントとサーバとの通信を可能にする必要があり、サーバホストでもファイアウォールを実行する場合は、それに応じてファイアウォールを調整してください。調整するには、[Adapt Firewall Settings(ファイアウォール設定の調整)] を選択します。設定を完了した後、[OK] をクリックして元のダイアログに戻ると、YaST がSuSEfirewall2のルールを、新しい条件に調整します(図 34.11. 「DHCPサーバ: ネットワークインタフェースとファイアウォール」 (709 ページ) を参照)。

☒ 34.11 DHCPサーバ: ネットワークインタフェースとファイアウォール



設定ステップをすべて完了した後、**[OK]** を選択してダイアログを閉じます。これでサーバは新規環境設定に従って起動します。

34.2 DHCPソフトウェアパッケージ

SUSE Linux Enterpriseでは、DHCPサーバとDHCPクライアントのどちらも利用可能です。用意されているDHCPサーバは、`dhcpd` (Internet Software Consortium製)です。クライアント側で、`dhcp-client` (ISCから)または`dhcpcd`パッケージにあるDHCPクライアントデーモンの、いずれかのDHCPクライアントプログラムを選択します。

SUSE Linux Enterpriseは、デフォルトで`dhcpcd`をインストールします。このプログラムは非常に扱いやすく、システムブート時に自動的に起動して、DHCPサーバを監視します。環境設定ファイルは必要ありません。標準的な設定であればほとんどの場合、そのまま使用できます。複雑な状況で使用する場合は、環境設定ファイル`/etc/dhclient.conf`によって制御されるISC `dhcpcd`を使用します。

34.3 DHCPサーバdhcpcd

DHCPシステムの中核には、動的ホスト環境設定プロトコルデーモンがあります。このサーバは、環境設定ファイル`/etc/dhcpd.conf`に定義された設定に従ってアドレスを「リース」し、その使用状況を監視します。システム管理者は、このファイルのパラメータと値を変更して、プログラムの動作をさまざまな方法で調整できます。例 34.1. 「環境設定ファイル`/etc/dhcpd.conf`」 (710 ページ)で、`/etc/dhcpd.conf`ファイルの基本的な例を見てみましょう。

例 34.1 環境設定ファイル`/etc/dhcpd.conf`

```
default-lease-time 600;           # 10 minutes
max-lease-time 7200;              # 2  hours

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.10 192.168.1.20;
    range 192.168.1.100 192.168.1.200;
}
```

DHCPサーバを用いてネットワーク内でIPアドレスを割り当てるには、このサンプルのような環境設定ファイルを用意すれば十分です。各行の末尾にセミコロンが付いていることに注意してください。これがなければ、`dhcpcd`は起動しません。

サンプルファイルは、3つのセクションに分けられます。最初のセクションは、要求側クライアントにIPアドレスがリースされた場合に、デフォルトで最大何秒間経過すればリースの更新が必要になるか(デフォルトリース時間)が定義されます。このセクションには、DHCPサーバがマシンにIPアドレスを割り当てた場合に、マシンが更新を求めずにそのIPアドレスを保持できる最大時間(`max-lease-time`)も指定されています。

2つ目のセクションでは、基本的なネットワークパラメータがグローバルレベルで定義されています。

- `option domain-name`の行は、ネットワークのデフォルトドメインを定義しています。
- `option domain-name-servers`エントリには、IPアドレスをホスト名(また逆方向に)に解決するためのDNSサーバを最高3つを指定します。ネームサーバは、DHCPをセットアップする前に、使用しているマシン上またはネットワーク上のどこか他の場所で設定するのが理想的です。ネームサーバではまた、各ダイナミックアドレスに対してホスト名を定義し、またその逆も定義する必要があります。独自のネームサーバを設定する方法については、[第33章 ドメインネームシステム \(673 ページ\)](#)を参照してください。
- `option broadcast-address`の行は、要求しているクライアントで使用されるブロードキャストアドレスを定義します。
- `option routers`の行では、ローカルネットワークでホストに配信できないデータパケットの送信先を(指定されたソース/ターゲットホストアドレスおよびサブネットに応じて)が指定されます。ほとんどの場合、特に小規模ネットワークでは、このルータはインターネットゲートウェイと同一です。
- `option subnet-mask`では、クライアントに割り当てるネットマスクを指定します。

ファイルの最後のセクションでは、サブネットマスクを含め、ネットワークを定義します。最後に、DHCPが対象のクライアントにIPアドレスを割り当てるために使用するアドレス範囲を指定します。では、クライアントは192.168.1.10～192.168.1.20および192.168.1.100～192.168.1.200の範囲にある任意のアドレスを与えられます。[例 34.1. 「環境設定ファイル/etc/dhcpd.conf」 \(710 ページ\)](#)。

これら数行を編集すると、`rcdhcpdstart`コマンドを使用してDHCPデーモンを有効にできるようになります。DHCPデーモンはすぐに使用できます。`rcdhcpdcheck-syntax`コマンドを使用すると、簡単な構文チェックを実行できます。サーバでエラーが発生して中断する、起動時にdoneが返されないなど、環境設定に関して予期しない問題が発生した場合は、メインシステムログ/var/log/messagesまたはコンソール 10 (Ctrl+Alt+F10)で情報を探せば、原因が突き止められます。

SUSE Linux Enterpriseシステムで、セキュリティを確保するためにchroot環境からDHCPデーモンを起動します。デーモンが見つけられるように、環境設定ファイルは、chroot環境にコピーします。このファイルは、`rcdhcpd start` コマンドによって自動的にこのファイルがコピーされるので、通常は、手動でコピーする必要はありません。

34.3.1 固定IPアドレスを持つホスト

DHCPは、事前定義の静的アドレスを特定のクライアントに割り当てる場合にも使用できます。明示的に割り当てられるアドレスは、プールから割り当てられる動的アドレスに常に優先します。たとえばアドレスが不足していて、サーバがクライアント間でアドレスを再配布する必要がある場合でも、静的アドレスは動的アドレスと違って期限切れになりません。

静的アドレスを割り当てられたホストを識別するために、`dhcpd`は、ハードウェアアドレスを使用します。ハードウェアアドレスは、6つのオクテットペアで構成される世界で唯一の固定数値コードで、すべてのネットワークデバイスの識別に使用されます(たとえば、`00::00:45:12:EE:F4`)。たとえば、**例 34.2. 「環境設定ファイルへの追加」** (712 ページ)のような数行を**例 34.1. 「環境設定ファイル/etc/dhcpd.conf」** (710 ページ)に示す環境設定ファイルに追加すると、DHCPデーモンはあらゆる状況で、対応するホストに同じデータのセットを割り当てます。

例 34.2 環境設定ファイルへの追加

```
host earth {  
    hardware ethernet 00:00:45:12:EE:F4;  
    fixed-address 192.168.1.21;  
}
```

対応するクライアントの名前(hostクライアント名、ここではearth)を1行目に、MACアドレスを2行目に入力します。LinuxホストでMACアドレスを確認するには、`ip link show`コマンドの後にネットワークデバイス(たとえば、`eth0`)を指定して実行します。出力例を次に示します。

```
link/ether 00:00:45:12:EE:F4
```

上の例では、MACアドレス`00:00:45:12:EE:F4`を持つネットワークカードが装着されたクライアントに、IPアドレス`192.168.1.21`とホスト名earthが自動的に割り当てられます。指定するハードウェアの種類は、ほとんどの場

合ethernetですが、IBMシステムでよく使用されるtoken-ringもサポートされています。

34.3.2 SUSE Linux Enterpriseのバージョン

セキュリティ向上のため、SUSE Linux EnterpriseバージョンのISC製DHCPサーバには、Ari Edelkind氏開発の非root/chrootパッチが付属しています。これにより、`dhcpd`をユーザID `nobody`で実行したり、`chroot`環境で実行したりできます(`/var/lib/dhcp`)。この機能を使用するには、環境設定ファイル`dhcpd.conf`が`/var/lib/dhcp/etc`に存在する必要があります。`init`スクリプトは、起動時に環境設定ファイルをこのディレクトリに自動的にコピーします。

この機能に関するサーバの動作は、環境設定ファイル`/etc/sysconfig/dhcpd`のエントリを使用して制御できます。非`chroot`環境で`dhcpd`を実行するには、`/etc/sysconfig/dhcpd`内の変数`DHCPD_RUN_CHROOTED`を「`no`」に設定します。

`chroot`環境内であっても、`dhcpd`を有効にしてホスト名を解決するには、次のような他の環境設定ファイルをコピーする必要があります。

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

これらのファイルは、`init`スクリプトの起動時に、`/var/lib/dhcp/etc`にコピーされます。コピーされたファイルが`/etc/ppp/ip-up`のようなスクリプトによって動的に変更されている場合は、必要な変更箇所がないか注意する必要があります。ただし、環境設定ファイルに(ホスト名でなく)IPアドレスだけを指定している場合は、これについて考える必要はありません。

環境設定の中に、`chroot`環境にコピーすべき追加ファイルが存在する場合は、`etc/sysconfig/dhcpd`ファイルの`DHCPD_CONF_INCLUDE_FILES`変数で、これらのファイルを設定します。`syslog-ng`デーモンの再起動後もDHCPログイン

グ機能が継続して動作するようにするには、`/etc/sysconfig/syslog`ファイル内の`SYSLOGD_ADDITIONAL_SOCKET_DHCP`エントリを指定します。

34.4 詳細情報

DHCPの詳細については、*Internet Software Consortium*のWebサイト(<http://www.isc.org/products/DHCP/>)を参照してください。また、`dhcpcd`、`dhcpcd.conf`、`dhcpcd.leases`、および`dhcpcd-options`のmanページにも詳細が記載されています。

NISの使用

ネットワーク上の複数UNIXシステムが共通のリソースにアクセスするようになると、すべてのユーザおよびグループ識別情報がネットワーク上のすべてのコンピュータで一致していることが重要になります。ネットワークはユーザに対して透過的でなければなりません。使用マシンに関わらず、ユーザは常に同じ環境でなければなりません。これはNISおよびNFSサービスを使用して実行できます。NFSはファイルシステムをネットワーク上に分散します。

NIS (Network Information Service)は、`/etc/passwd`、`/etc/shadow`、`/etc/group`の各ファイルにネットワーク越しにアクセスできるようにするデータベースサービスと考えることができます。NISの用途はこれ以外にもありますが(`/etc/hosts`や`/etc/services`といったファイルにアクセスできるようにするなど)、ここでは触れません。NISはよくYPと呼ばれますが、これは、NISがちょうどネットワークの「イエローページ」のような役割を果たすためです。

35.1 NISサーバの設定

NIS情報をネットワーク上で配信するには、すべてのクライアントと通信する単一のサーバ(マスタ)を使用するか、またはNISスレーブサーバにマスタからこの情報を要求させ、各クライアントに転送させることができます。

- ・ ネットワーク上で1つのNISサーバのみを設定するには、[35.1.1項「NISマスタサーバの設定」](#) (716 ページ)に進みます。

- NISマスタサーバがデータをスレーブサーバにエクスポートする場合は、[35.1.1項「NISマスタサーバの設定」](#) (716 ページ)で説明しているようにマスタサーバをセットアップし、[35.1.2項「NISスレーブサーバの設定」](#) (721 ページ)で説明しているようにサブネット内にスレーブサーバをセットアップします。

35.1.1 NISマスタサーバの設定

ネットワーク上にNISマスタサーバを設定するには、次の手順に従います。

- 1 `[YaST]` > `[ネットワークサービス]` > `[NISサーバ]` の順に選択します。
- 2 ネットワーク上に1つのNISサーバのみ必要な場合、またはこのサーバが
続くNISスレーブサーバのマスタとして機能する場合は、`[Install and
set up NIS Master Server]` を選択します。YaSTは必要なパッケージをイ
ンストールします。

ティップ

NISサーバソフトウェアがマシン上にすでにインストールされている場合は、`[Install and set up NIS Master Server]` をクリックしてNISマスタサーバの作成を開始します。

図 35.1 NISサーバの設定

NISサーバを[マスターまたはスレーブ]として設定する
ため、NISサーバの環境設定を行わないか選択し
てください。

NISサーバを環境設定する場合は、まずNISサーバ
のパッケージをインストールします。

Network Information Service (NIS)サーバのセットアップ

現在の状況: NISソフトウェアがインストールされていません。
設定されたNISサーバがありません。

ご希望の項目を選んでください

- ☐ NISマスターサーバをインストールおよびセットアップする(M)
- ☐ NISスレーブサーバをインストールおよびセットアップする(S)
- ☒ 何もしないでセットアップを中止する(D)

戻る(B) 中止(E) 完了(F)

3 基本NISセットアップオプションを決定します。

3a NISドメイン名を入力します。

- 3b** `[This host is also a NIS client]` を選択して、ホストがNISクライアントとしても機能するかどうかを定義します。これにより、ユーザはログインおよびNISサーバからのデータにアクセスできるようになります。

`[Changing of passwords]` を選択して、ネットワーク上のユーザ(ローカルユーザとNISサーバで管理されているユーザの両方)が`yppasswd` コマンドを用いてNISサーバ上のパスワードを変更できるようにします。

これにより、`[Allow Changes to GECOS Field]` および `[Allow Changes to Login Shell]` オプションが選択可能になります。「前者」を選択すると、ユーザが`ypchfn`コマンドを使用して自分の名前とアドレスの設定を変更できるようになります。「SHELL」により、ユーザは`ypchsh`コマンドを使って、デフォルトのシェルを変更することができます。たとえば、`bash`から`sh`に切り替えることができます。使用するシェルは、`/etc/shells`中にあらかじめ定義されていなければなりません。

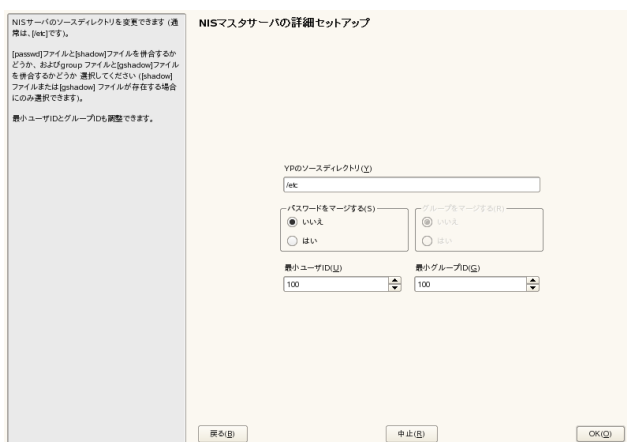
3c NISサーバがサブネット内のNISスレーブサーバへのマスターサーバとして機能するようにする場合は、`[Active Slave NIS Server exists]` を選択します。

3d YaSTでNISサーバのファイアウォール設定が適用されるようにするには、`[Open Ports in Firewall]` を選択します。

図 35.2 マスターサーバの設定

3e `[次へ]` をクリックしてこのダイアログを終了するか、または、`[Other global settings]` をクリックして他の設定を行います。`[Other global settings]` には、NISサーバのソースディレクトリ(デフォルトでは`/etc`)の変更などが含まれます。また、パスワードを結合することもできます。ここで `[はい]` を選択して、ユーザデータベースのビルドに`/etc/passwd`、`/etc/shadow`、および`/etc/group`の各ファイルが使用されるようにします。また、NISで提示される最小のユーザおよびグループIDも決定します。設定を確認して前の画面に戻るには、`[OK]` を選択します。

図 35.3 ディレクトリの変更とNISサーバ用の各ファイルの同期化



The image shows a dialog box titled "NIS マスタサーバの詳細セットアップ" (NIS Master Server Detailed Setup). On the left, there is a text area with instructions in Japanese about file synchronization. The main area contains several input fields and radio buttons. At the bottom, there are three buttons: "戻る (B)" (Back), "中止 (B)" (Cancel), and "OK (O)" (OK).

NISサーバのソースディレクトリを変更できます (通常は、/etc) です。

[passwd]ファイルと[shadow]ファイルを併存するかどうかが、および[group]ファイルと[shadow]ファイルを併存するかどうかを選択してください。[shadow]ファイルまたは[shadow]ファイルが存在する場合にのみ選択できます。

選択ユーザIDとグループIDも調整できます。

NIS マスタサーバの詳細セットアップ

YRPのソースディレクトリ (Q)

/etc

パスワードをマージする (S)

☒ いいえ ☐ はい

グループをマージする (R)

☒ いいえ ☐ はい

選択ユーザID (U)

100

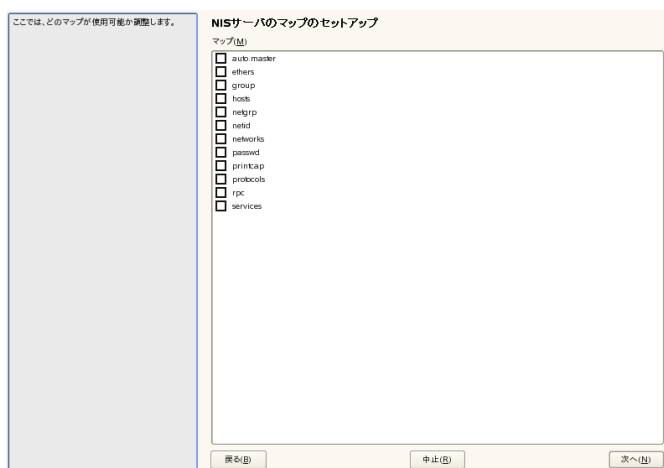
選択グループID (G)

100

戻る (B) 中止 (B) OK (O)

- 4 前の画面で「NIS スレーブサーバが存在する」を選択した場合は、スレーブとして使用するホスト名を入力して「次へ」をクリックします。
- 5 スレーブサーバを使用しない場合は、スレーブ設定を省略して、データベース設定のダイアログに進んでください。ここでは、マップを指定します。マップとは、NISサーバからNISクライアントに転送される部分データベースのことです。通常は、デフォルトの設定のままで十分です。「次へ」をクリックして、このダイアログを終了します。
- 6 いずれのマップが使用できるかを確認し、続行する場合は、「次へ」をクリックします。

図 35.4 NISサーバマップの設定

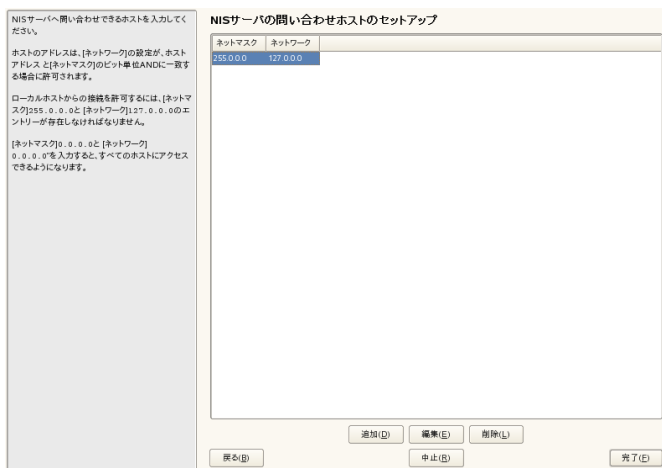


- 7** NISサーバへのクエリが許可されているホストを入力します。ホストは、適切なボタンをクリックして追加、削除、編集できます。ここでは、NISサーバにリクエストを送信できるネットワークを指定します。通常は、内部ネットワークを指定します。その場合は、次の2つのエントリが必要です。

```
255.0.0.0      127.0.0.0
0.0.0.0        0.0.0.0
```

最初のエントリによって、自分自身、つまりNISサーバからの接続が許可されます。2番目は、すべてのホストがサーバに要求を送信できるようにします。

図 35.5 NISサーバに対するリクエスト送信許可の設定



- 8 [完了] をクリックして変更を保存し、セットアップを終了します。

35.1.2 NISスレーブサーバの設定

ネットワーク上に適切なNISスレーブサーバを設定するには、次の手順に従います。

- 1 [YaST] > [ネットワークサービス] > [NISサーバ] の順に選択します。
- 2 [Install and set up NIS Slave Server] を選択し、[次へ] をクリックします。

ティップ

NISサーバソフトウェアがマシン上にすでにインストールされている場合は、[Create NIS Slave Server] をクリックしてNISスレーブサーバの作成を開始します。

- 3 NISスレーブサーバの基本セットアップを完了します。

3a NISドメインを入力します。

3b マスタサーバのホスト名またはIPアドレスを入力します。

3c ユーザがこのサーバにログインできるようにする場合は、`[This host is also a NIS client]` を設定します。

3d `[Open Ports in Firewall]` を選択して、ファイアウォール設定を適用します。

3e `[Next]` をクリックします。

4 NISサーバへのクエリが許可されているホストを入力します。ホストは、適切なボタンをクリックして追加、削除、編集できます。ここでは、NISサーバにリクエストを送信できるネットワークを指定します。通常、これはすべてのホストです。その場合は、次の2つのエントリが必要です。

255.0.0.0	127.0.0.0
0.0.0.0	0.0.0.0

最初のエントリによって、自分自身、つまりNISサーバからの接続が許可されます。2つ目のエントリによって、同一ネットワークにアクセス可能なすべてのホストがNISサーバにリクエストを送信することを許可されます。

5 `[完了]` をクリックして変更を保存し、セットアップを終了します。

35.2 NISクライアントの設定

`[NISClient]` YaSTモジュールを使用して、NISを使用するようにワークステーションを設定します。ホストに静的IPアドレスを割り当ててるのか、DHCPから提供されたIPアドレスを使用するのを選択してください。DHCPからは、NISドメインとNISサーバも提供されます。DHCPについては、[第34章 DHCP](#) (699 ページ)を参照してください。固定IPアドレスを使用する場合は、NISドメインとNISサーバを手動で指定します。参照先 [図 35.6. 「NISサーバのドメインとアドレスの設定」](#) (723 ページ). `[Find]` をクリックすると、YaSTはネットワーク全体でアクティブなNISサーバを検索します。ローカルネットワーク

のサイズにもよりますが、時間がかかる場合があります。[ブロードキャスト] は、指定したサーバが応答しなかったときに、ローカルネットワーク内でNISサーバを検索します。

[*Addresses of NIS servers*] にアドレスをスペースで区切って入力することにより、複数のサーバを指定することもできます。

ローカルインストールにもよりますが、オートマウンタも有効化することをお勧めします。このオプションは、必要に応じて他のソフトウェアもインストールします。

クライアントが使用しているサーバを他のホストに知られたくない場合は、エキスパート設定で、[*Answer Remote Hosts*] をオフにします。[ブローケンサーバ] を有効にすると、クライアントが、特権のないポートを介して通信するサーバからの応答を受信できるようになります。詳細については、`manypbind`を参照してください。

設定を終えたら、[完了] をクリックして変更を保存し、YaSTコントロールセンタに戻ります。

図 35.6 NISサーバのドメインとアドレスの設定

NISドメイン(たとえば example.com)とNISサーバのアドレス(たとえば nis.example.com または 10.20.1.1)を入力してください。

複数のサーバを指定する場合は、アドレスをスペースで区切ってください。

[ブロードキャスト]オプションを使用すると、指定されたサーバからの応答がない場合にすべてのローカルネットワーク上のサーバを検索できます。ただし、セキュリティ上の問題が生じる可能性があります。

DHCPを使用して、そのサーバがNISドメイン名またはサーバを提供する場合は、それを使用するように設定できます。DHCP自体は、ネットワークモジュールでセットアップできます。

オートマウンタは自動的にディレクトリをマウントするデモンで、ユーザのホームディレクトリなどに使用されます。オートマウンタの環境設定ファイル(auto.*は、ローカルコンピュータまたはNIS上に存在する必要があります)。

NISクライアントの環境設定

☐ NISを使用しない(N)

☒ NISを使用する(U)

NISクライアント

☐ 自動設定(DHCPを介して)(T)

☒ スタティックなセットアップ(S)

NISドメイン(I)

example.com

NISサーバのアドレス(A)

192.168.27.4

☐ ブロードキャスト(Q)

検索(D)

追加のNISドメイン

localdomain

編集(E)

☐ オートマウンタを起動(M)

エキスパート(E)

戻る(B)

中止(B)

完了(F)

LDAP—ディレクトリサービス

LDAP (Lightweight Directory Access Protocol)は、情報ディレクトリへのアクセスと管理を行うために設計されたプロトコルセットです。LDAPは、ユーザおよびグループ管理、システム構成の管理、アドレス管理など、さまざまな目的に使用できます。この章では、OpenLDAPの動作原理とYaSTを使用したLDAPデータの管理方法の基本事項について説明します。LDAPプロトコルには複数の実装方法がありますが、この章ではもっぱらOpenLDAPの実装を中心に説明します。

ネットワーク環境では、重要な情報をすぐに利用できるように整理しておくことは不可欠です。そのため、一般的に使用されているイエローページのようなディレクトリサービスを使用して、情報を整理し、すぐに検索できる形式にしておくことができます。

理想的なケースは、一元的なサーバでデータをディレクトリに保持し、特定のプロトコルを使用してそれをすべてのクライアントに配布するという形態です。データはさまざまなアプリケーションがアクセスできる方法で整理されます。この方法では、個々のカレンダーツールや電子メールクライアントが独自のデータベースを持つ必要はありません。一元的なリポジトリにアクセスすればよいからです。これにより、情報管理のための負荷も大幅に軽減されます。LDAP (lightweight directory access protocol)のようなオープンで標準化されたプロトコルを使用すれば、可能な限り多くの異なるクライアントアプリケーションが、このような情報にアクセスできるようになります。

この文脈でのディレクトリとは、高速かつ効果的に読み込みと検索ができるように最適化された一種のデータベースです。

- 膨大な同時読み込みアクセスを可能にするため、書き込みアクセスは、管理者による少量の更新作業に限られます。従来のデータベースは、できる限り大量のデータを短時間に受け付けられるように最適化されます。
- 書き込みアクセスは制約された形でのみ可能なため、ディレクトリサービスは、ほとんどが変更のない静的情報の管理に使用されます。一般に、非常に頻繁に変更されるデータ(動的データ)は、従来のデータベースに保存されます。たとえば、企業ディレクトリにある電話番号は、経理で管理する数字ほど頻繁に変更されません。
- 静的データを管理する場合、既存のデータセットの更新は非常にまれです。動的データ、特に銀行口座や経理のデータセットが関与する場合、データの一貫性が最重要課題となります。たとえばある項目から差し引かれた金額を他の項目に加算する場合、データストックで残高を正しく維持するためには、1回のトランザクション内で両方の操作が同時に行われる必要があります。データベースはこのようなトランザクションをサポートしますが、ディレクトリではサポートされません。ディレクトリでは、短期的にデータの一貫性が崩れても大きな問題にはなりません。

LDAPなどのディレクトリサービスの設計には、複雑な更新やクエリメカニズムのサポートは含まれません。このサービスにアクセスするすべてのアプリケーションが、すばやく簡単にアクセスできることが主な課題です。

36.1 LDAPとNISの比較

Unix系システムの管理者は、従来から、ネットワーク内の名前の解決やデータ配信にNISサービスを使用しています。設定データは/etc内のファイルに保存され、group、hosts、mail、netgroup、networks、passwd、printcap、protocols、rpc、およびservicesの各ディレクトリは、ネットワーク内の複数のクライアントに分散されています。これらのファイルはシンプルテキストファイルのため、保守にそれほどの手間はかかりません。しかし、構造化されていないため、大量のデータを処理することがますます困難になっています。NISはUnix系プラットフォーム専用設計されています。このため、異種ネットワークでの一元的データ管理には採用できません。

LDAPサービスはNISと異なり、純粋なUnix系ネットワークに制限されていません。Windowsサーバ(2000以降)は、LDAPをディレクトリサービスとしてサ

ポートします。前述のアプリケーションタスクは、Unix系以外のシステムでもサポートされます。

LDAPの原則は、一元管理が必要なあらゆるデータ構造に適用可能です。いくつかの例を次に示します。

- NISサービスの代替としての採用
- メールルーティング(postfix、sendmail)
- Mozilla、Evolution、およびOutlookなどのメールクライアント用アドレス帳
- BIND9ネームサーバのゾーン記述の管理
- 異種ネットワークでのSambaのユーザ認証

LDAPはNISと異なり拡張できるため、これら以外にも広範な用途が考えられます。データが明確に定義された階層構造になっているため、検索が容易であり、大量データの管理が簡単になります。

36.2 LDAPディレクトリツリーの構造

LDAPサーバの機能とデータの保存方法について詳細な背景知識を得るには、サーバでデータがどのように編成され、この構造によってどのようにLDAPが必要なデータに高速にアクセスするかを理解することが重要です。LDAPセットアップを正常に実行するには、一部の基本的なLDAP用語を理解しておく必要があります。このセクションでは、LDAPディレクトリツリーの基本レイアウトを紹介し、LDAPコンテキストで使用される基本用語を説明します。すでにLDAPの背景知識があり、LDAP環境をSUSE Linux Enterpriseに設定する方法を知りたいだけの場合は、この説明セクションはスキップしてください。36.5項「YaSTによるLDAPサーバの設定」(741 ページ)または36.3項「slapd.confを使用したサーバの設定」(731 ページ)を参照してください。

LDAPディレクトリは、ツリー構造です。ディレクトリのすべてのエントリ(オブジェクトと呼びます)には、この階層内に定義された位置があります。この階層はディレクトリ情報ツリー(DIT)と呼ばれます。対象のエントリへの完全パスは、識別名(DN)と呼ばれ、確実にエントリを識別します。このエントリ

へのパス上にある個々のノードを**相対識別名(RDN)**と呼びます。オブジェクトは、一般的に、2つのタイプのいずれかに割り当てられます。

コンテナ

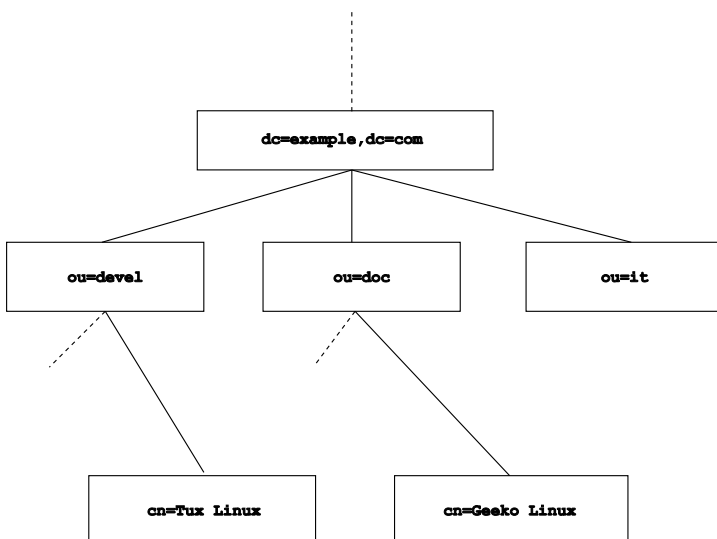
これらのオブジェクトは、それ自体に他のオブジェクトを持っています。オブジェクトクラスにはroot(ディレクトリツリーのルート要素。実際には存在しません)、c(国)、ou(組織単位)、dc(ドメインコンポーネント)があります。このモデルは、ファイルシステムのディレクトリ(フォルダ)にあたります。

リーフ

これらのオブジェクトは、ブランチの端にあり、下位のオブジェクトを持ちません。たとえば、person、InetOrgPerson、またはgroupofNamesがあります。

ディレクトリ階層の最上位には、ルート要素rootがあります。これには、下位要素として、c(国)、dc(ドメインコンポーネント)、またはo(組織)が含まれます。LDAPディレクトリ内ツリーの関係については、**図 36.1. 「LDAPディレクトリの構造」** (728 ページ)に示す次の例で詳細に説明します。

図 36.1 LDAPディレクトリの構造



この図は、架空のディレクトリ情報ツリーです。3レベルのエントリが示されています。各エントリは、図内の1つの箱に対応します。最後に、このケースにおける架空のSUSE社員Geeko Linuxの識別名をcn=Geeko Linux,ou=doc,dc=example,dc=comとします。この識別名は、RDN cn=Geeko Linuxを前のエントリのDN ou=doc,dc=example,dc=comに追加して構成されます。

DITに格納するオブジェクトの種類は、スキーマによりグローバルに決定されます。オブジェクトタイプは、オブジェクトクラスによって決定されます。オブジェクトクラスは、オブジェクトに割り当てる、または割り当てられる属性を決定します。したがって、スキーマには、すべてのオブジェクトクラスと、想定したアプリケーションシナリオで使用される属性の定義を含む必要があります。RFC 2252と2256では、一般的なスキーマがいくつか用意されています。しかし、LDAPサーバの操作環境で必要になる場合は、カスタムスキーマを作成したり、複数のスキーマを相互補完的に使用することもできます。

表 36.1. 「一般的に使用されるオブジェクトクラスと属性」 (729 ページ)では、前述の例で使用されているcore.schemaとinetorgperson.schemaのオブジェクトクラスについて、必要な属性や有効な属性値などの簡単な概要を示します。

表 36.1 一般的に使用されるオブジェクトクラスと属性

Object Class	意味	例で使用されているエントリ	必須属性
dcObject	<i>domainComponent</i> (ドメインのコンポーネントの名前を指定します)	例	dc
organizationalUnit	<i>organizationalUnit</i> (組織単位)	doc	ou
inetOrgPerson	<i>inetOrgPerson</i> (イントラネットまたはイントラネット用の個人関連情報)	Geeko Linux	snとcn

例 36.1. 「**schema.coreからの抜粋**」(730 ページ)は、説明の付いたスキーマディレクティブからの抜粋です(行番号は説明のために付けられています)。

例 36.1 *schema.core*からの抜粋

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2         DESC 'RFC2256: organizational unit this object belongs to'
#3         SUP name )

...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5         DESC 'RFC2256: an organizational unit'
#6         SUP top STRUCTURAL
#7         MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory
    $ x121Address $ registeredAddress $ destinationIndicator
    $ preferredDeliveryMethod $ telexNumber
    $ teletexTerminalIdentifier $ telephoneNumber
    $ internationalISDNNumber $ facsimileTelephoneNumber
    $ street $ postOfficeBox $ postalCode $ postalAddress
    $ physicalDeliveryOfficeName
    $ st $ l $ description) )

...
```

属性タイプ`organizationalUnitName`とそれに対応するオブジェクトクラス`organizationalUnit`がここで例として使用されています。1行目では、属性名、一意のOID(オブジェクト識別子)(数値)、および属性値の省略名が指定されています。

2行目には、DESCを使用して、属性の簡単な説明が記入されています。この定義がどのRFCに基づいているかもここに記載されます。3行目のSUPは、この属性が属する上位属性を示します。

オブジェクトクラス`organizationalUnit`の定義は、4行目から始まり、属性の定義と同様、OEDとオブジェクトクラスが最初に定義されます。行目はオブジェクトクラスの簡単な説明です。SUP topで始まる6行目は、このオブジェクトクラスが他のオブジェクトクラスの上位でないことを示します。MUSTで始まる7行目は、`organizationalUnit`タイプのオブジェクトで使用する必要がある属性値をすべてリストします。MAYで始まる8行目は、このオブジェクトクラスで利用できる属性値をすべてリストします。

スキーマの用途については、OpenLDAPのマニュアルにわかりやすく説明されています。これはインストール後に、`/usr/share/doc/packages/openldap2/admin-guide/index.html`で参照してください。

36.3 slapd.confを使用したサーバの設定

インストールされたシステムでは、`/etc/openldap/slapd.conf`にLDAPサーバの完全な設定ファイルが用意されています。ここでは1つのエントリについて簡単に説明し、必要な調整について説明します。ハッシュ(#)で始まるエントリは無効です。エントリを有効にするには、このコメント文字を削除します。

36.3.1 slapd.conf内のグローバルエントリ

例 36.2 *slapd.conf*: スキーム用ディレクティブの取り込み

```
include      /etc/openldap/schema/core.schema
include      /etc/openldap/schema/cosine.schema
include      /etc/openldap/schema/inetorgperson.schema
include      /etc/openldap/schema/rfc2307bis.schema
include      /etc/openldap/schema/yast.schema
```

に示すように、`slapd.conf`にある最初のディレクティブは、LDAPディレクトリを編成するスキーマを指定します。**例 36.2. 「slapd.conf: スキーム用ディレクティブの取り込み」** (731 ページ) `core.schema` エントリは必須です。付加的に必要とされるスキーマは、このディレクティブの後に追加します。詳細は、付属のOpenLDAPマニュアルを参照してください。

例 36.3 *slapd.conf*: *pidfile* と *argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

この2つのファイルには、PID (プロセスID) と `slapd` プロセスの起動時に使用される引数が含まれています。これらを変更する必要はありません。

例 36.4 *slapd.conf*: アクセス制御

```
# Sample Access Control
#       Allow read access of root DSE
# Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
#       access to * by self write
#               by users read
#               by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

例 36.4. 「*slapd.conf*: アクセス制御」 (732 ページ)は、サーバ上のLDAPディレクトリへのアクセス許可を制御する*slapd.conf*の一部です。*slapd.conf*のグローバルセクションで行われている設定は、データベース固有のセクションで、カスタムのアクセス規則が宣言されていない限り有効です。これらはグローバル宣言を上書きするためです。ここで示すように、すべてのユーザはディレクトリの読み込みアクセスができますが、ディレクトリに書き込めるのは管理者(*rootdn*)のみです。LDAPのアクセス制御の管理は、非常に複雑なプロセスです。次のヒントが役立ちます。

- すべてのアクセス規則は、次の構造に従います。

```
access to <what> by <who> <access>
```

- *what*には、アクセスを付与するオブジェクトまたは属性を指定します。個々のディレクトリブランチを、別の規則で明示的に保護することもできます。正規表現を使って、ディレクトリツリー中の特定の領域を1つの規則で処理することもできます。*slapd*は、設定ファイル中に記述されている順番で、すべての規則を評価します。一般的な規則は、特定の規則の後に指定する必要があります。*slapd*が有効だと考える最初の規則が評価され、それ以降のエントリは無視されます。
- *who*には、*what*で指定された領域へのアクセスを付与されるユーザを指定します。ここでも*slapd*は、最初に一致する*who*を見つけた後、評価を行わないため、特定の規則は、一般的な規則より前に指定する必要があります。**表 36.2. 「ユーザグループと付与されるアクセス許可」** (733 ページ) に有効なエントリを示します。

表 36.2 ユーザグループと付与されるアクセス許可

タグ	スコープ
*	例外なくすべてのユーザ
anonymous	認証されていない(「匿名」)ユーザ
ユーザ	認証済みユーザ
self	ターゲットオブジェクトに接続されているユーザ
dn.regex=<regex>	正規表現に一致するすべてのユーザ

- *access*は、アクセスタイプを指定します。に示すオプションを使用してください。**表 36.3. 「アクセスのタイプ」** (733 ページ)

表 36.3 アクセスのタイプ

タグ	アクセスのスコープ
none	アクセス不可

タグ	アクセスのスコープ
auth	サーバへの連絡用
compare	比較アクセス用のオブジェクト
検索	検索フィルタ設定用
読む	読み込みアクセス
write	書き込みアクセス

slapdはクライアントが要求するアクセス権をslapd.confで付与されたアクセス権と比較します。要求された権限と比較して、同等または上位の権限が規則によって与えられている場合は、クライアントに対して、アクセスが許可されます。規則に宣言された権限を越える権限をクライアントが要求した場合、アクセスが拒否されます。

例 36.5. 「slapd.conf:アクセス制御の例」 (734 ページ)に、簡単なアクセス制御の例を示します。このように正規表現を用いて自由にアクセス制御できます。

例 36.5 slapd.conf: アクセス制御の例

```
access to dn.regex="ou=([^,]+),dc=example,dc=com"
by dn.regex="cn=Administrator,ou=$1,dc=example,dc=com" write
by user read
by * none
```

この規則は、担当の管理者のみが個別のouエントリに書き込みアクセスできることを宣言します。他のすべての認証済みユーザは読み込みアクセスができ、その他のユーザはアクセスできません。

ティップ: アクセス規則の設定

access to規則または一致する**by**ディレクティブが存在しない場合、アクセスが拒否されます。付与されるのは、明示的に宣言されたアクセス権だけです。規則がまったく宣言されていない場合、デフォルトの原則として、管理者は書き込みアクセスができ、残りのユーザ全員は読み込みアクセスができます。

詳細な説明およびLDAPのアクセス権の設定例については、インストールした `openldap2` パッケージのオンラインマニュアルを参照してください。

アクセス許可を一元的なサーバ設定ファイル(`slapd.conf`)で管理する方法以外に、**ACI**(アクセス制御情報)を使用する方法があります。**ACI**は、個々のオブジェクトのアクセス情報をLDAPツリーに格納します。アクセス制御のタイプには共通のものがなく、開発者の間では未だ実験的だと考えられています。詳細については、<http://www.openldap.org/faq/data/cache/758.html>を参照してください。

36.3.2 slapd.conf内のデータベース固有のディレクティブ

例 36.6 `slapd.conf`: データベース固有のディレクティブ

```
database bdb❶
suffix "dc=example,dc=com"❷
checkpoint 1024 5❸
cachesize 10000❹
rootdn "cn=Administrator,dc=example,dc=com"❺
# Cleartext passwords, especially for the rootdn, should
# be avoided. See slapasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret❻
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap❼
# Indices to maintain
index objectClass eq❽
overlay ppolicy❾
ppolicy_default "cn=Default Password Policy,dc=example,dc=com"
ppolicy_hash_cleartext
ppolicy_use_lockout
```

- ❶ この種類のデータベース(この場合Berkeleyデータベース)は、このセクションの先頭行に設定されます(例 36.6. 「**slapd.conf: データベース固有のディレクティブ**」 (735 ページ)を参照)。
- ❷ `suffix`には、このサーバが担当するLDAPツリー中の部分を指定します。

- ③ checkpointには、実際にデータベースに書き込むまでトランザクションに保持するデータ量(KB)と、2つの書き込み処理間の時間(分)を指定します。
- ④ cachesizeには、データベースキャッシュ中に保持するオブジェクト数を設定します。
- ⑤ rootdnには、このサーバに対して、管理者権限を持つユーザを指定します。ここで宣言されるユーザは、LDAPエントリが必要ではなく、通常ユーザとして存在する必要ありません。
- ⑥ rootpwには、管理者パスワードを設定します。ここでsecretを使用する代わりに、slappasswdによって作成した管理者パスワードのハッシュを入力することもできます。
- ⑦ directoryディレクティブは、サーバ上でデータベースディレクトリが格納されているファイルシステム内のディレクトリを示します。
- ⑧ 最後のディレクティブindex objectClass eqは、すべてのオブジェクトクラスのインデックスを管理します。経験的に、ユーザが最も頻繁に検索しそうな属性をここに追加できます。
- ⑨ overlay ppolicyは、パスワード制御機構のレイヤを追加します。ppolicy_defaultには、ユーザのエントリにポリシーが設定されていない場合に使用する、pwdPolicy objectのDNを指定します。エントリに対するポリシーがなく、デフォルト値も設定されていない場合は、ポリシーは利用されません。ppolicy_hash_cleartextは、平文パスワードが存在し、データベースに格納される前に変更要求がハッシュされることを示します。このオプションを使用する場合、ppolicy_hash_cleartextはX.500/LDAP情報モデルに違反しているため、すべてのディレクトリユーザに対してuserPassword属性への比較、検索、および読み込みアクセスを禁止することをお勧めします。クライアントからロックされたアカウントへの接続が試みられた場合、ppolicy_use_lockoutは特定のエラーコードを送信します。サイトのセキュリティを強化するには、このオプションを無効にしてください。エラーコードは、不正侵入者に対して有益な情報を与えてしまいます。

データベースに対してここで定義されたカスタムのAccess規則は、グローバルAccess規則に代わって使用されます。

36.3.3 サーバの起動と停止

LDAPサーバが完全に設定され、[36.4項「LDAPディレクトリのデータ処理」](#) (737 ページ)で説明するパターンに従ってすべてのエントリが作成されたら、rootユーザで「`rcldap start`」を入力し、LDAPサーバを起動します。実行されているかどうかわからない場合は、`rcldap stop`コマンドを実行します。実行しているLDAPサーバのステータスは、`rcldapstatus`コマンドを実行して要求します。

YaSTランレベルエディタ([20.2.3項「YaSTでのシステムサービス\(ランレベル\)の設定」](#) (440 ページ)を参照)を使用して、システムのブートまたは停止時に、サーバを自動的に起動および停止することができます。またコマンドプロンプトで`insserv`コマンドを実行して、起動および停止スクリプトそれぞれへのリンクを作成することもできます。詳細については、[20.2.2項「initスクリプト」](#) (435 ページ)を参照してください。

36.4 LDAPディレクトリのデータ処理

OpenLDAPは、LDAPのデータを管理するためのツールを提供しています。ここでは、中でも重要な4つのツール、データストックの追加、削除、検索、および変更について説明します。

36.4.1 LDAPディレクトリへのデータの挿入

`/etc/openldap/slapd.conf`でLDAPサーバを正しく設定し、使用する準備ができたら (suffix、directory、rootdn、rootpw、およびindexについて適切なエントリが表示されることを確認)、レコード入力に進みます。OpenLDAPでは、`ldapadd`コマンドを使用してこのタスクを実行します。可能であれば、実践的な見地から、バンドルされたデータベースにオブジェクトを追加してください。

LDAPは、LDIF形式(LDAP data interchange format)を処理してデータを入力します。LDIFは、任意の数の属性と値が指定されたシンプルテキストファイルです。指定できるオブジェクトクラスと属性については、`slapd.conf`で宣言したスキーマファイルを参照してください。[図 36.1.「LDAPディレクトリの構造」](#) (728 ページ)の例のような簡単なフレームワークを作成するには、[例 36.7.「LDIFファイルの例」](#) (738 ページ)のLDIFを使用します。

例 36.7 LDIF ファイルの例

```
# The Organization
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organization
o: Example dc: example

# The organizational unit development (devel)
dn: ou=devel,dc=example,dc=com
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=example,dc=com
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=example,dc=com
objectClass: organizationalUnit
ou: it
```

重要項目: LDIF ファイルのエンコーディング

LDAPでは、**UTF-8 (Unicode)**を使用します。ウムラウトは正しくエンコードする必要があります。**UTF-8**をサポートするエディタ(たとえばKateまたは最近のバージョンのEmacs)を使用してください。それ以外のエディタを使用する場合は、ウムラウトや他の特殊文字の使用を避けるか、`recode`を使用して**UTF-8**をコード変換します。

ファイルには、`.ldif`というサフィックスを付けて保存し、次のコマンドでサーバに渡します。

```
ldapadd -x -D <dn of the administrator> -W -f <file>.ldif
```

`-x`は、認証(この例ではSASL)をオフにします。`-D`は、操作を呼び出すユーザを宣言します。`slapd.conf`での設定と同様、管理者の有効なDNをここに入力します。この例では、`cn=Administrator,dc=example,dc=com`です。`-w`を指定すると、コマンドライン(クリアテキスト)でのパスワード入力が必要になり、別のパスワードプロンプトがアクティブ化されます。このパスワードは、`slapd.conf`の`rootpw`で事前に指定されています。`-f`はファイル名を渡します。`ldapadd`の実行方法の詳細については、[例 36.8. 「example.ldif」のldapaddの使用](#) (739 ページ)を参照してください。

例 36.8 *example.ldif*での*ldapadd*の使用

```
ldapadd -x -D cn=Administrator,dc=example,dc=com -W -f example.ldif
```

```
Enter LDAP password:
adding new entry "dc=example,dc=com"
adding new entry "ou=devel,dc=example,dc=com"
adding new entry "ou=doc,dc=example,dc=com"
adding new entry "ou=it,dc=example,dc=com"
```

個人のユーザデータを、個別のLDIFファイルに用意することができます。

例 36.9. 「**TuxのLDIFデータ**」(739 ページ)は、新しいLDAPディレクトリにTuxを追加します。

例 36.9 *TuxのLDIFデータ*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@example.com
uid: tux
telephoneNumber: +49 1234 567-8
```

LDIFファイルには、任意の数のオブジェクトを指定できます。サーバのディレクトリブランチ全体を一度に渡すことも、個別のオブジェクトの例で示すように、その一部だけを渡すことも可能です。一部のデータを比較的頻繁に変更する必要がある場合は、1つのオブジェクトごとに細かく分割することをお勧めします。

36.4.2 LDAPディレクトリのデータの変更

データストックの変更に用いるには、ツール*ldapmodify*が用意されています。最も簡単な方法は、対応するLDIFファイルを変更してから、変更したファイルをLDAPサーバに渡すことです。Tux社員の電話番号を+49 1234 567-8から+49 1234 567-10に変更するには、例 36.10. 「**LDIFファイル*tux.ldif*の変更**」(740 ページ)のようにLDIFファイルを編集する必要があります。

例 36.10 LDIF ファイル *tux.ldif* の変更

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

次のコマンドを使用して、変更したファイルをLDAPディレクトリにインポートします。

```
ldapmodify -x -D cn=Administrator,dc=example,dc=com -W -f tux.ldif
```

代替りの方法として、変更する属性を直接`ldapmodify`に渡すこともできます。この処理手順を次に示します。

- 1 `ldapmodify` を起動し、パスワードを入力します。

```
ldapmodify -x -D cn=Administrator,dc=example,dc=com -W
Enter LDAP password:
```

- 2 次に示す順序に従って、慎重に変更を入力します。

```
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

`ldapmodify` についての詳細とその構文は、`ldapmodify` のマニュアルページを参照してください。

36.4.3 LDAPディレクトリでのデータの検索と読み込み

OpenLDAPには、`ldapssearch` を使用して、LDAPディレクトリでデータを検索して読み込むコマンドラインツールが用意されています。簡単なクエリの構文は次のとおりです。

```
ldapssearch -x -b dc=example,dc=com "(objectClass=*)"
```

-bオプションは検索ベース、つまり、検索を実行するツリーのセクションを指定します。この例では、dc=example,dc=comです。セクション内の特定の部分(たとえば、devel部門内のみ)で精度の高い検索を実行するには、-bを使用してこのセクションをldapsearchに渡します。-xは、簡単な認証を起動するよう要求します。(objectClass=*)は、対象のディレクトリにあるすべてのオブジェクトを読むように宣言します。このコマンドオプションは、新しいディレクトリツリーを作成した後に、すべてのエントリが正しく記録され、サーバが意図したとおりに応答することを確認するために使用されます。ldapsearchの使用の詳細については、対応するマニュアルページ(ldapsearch(1))を参照してください。

36.4.4 LDAPディレクトリでのデータの削除

不要なエントリを削除するには、ldapdeleteを使用します。構文は、他のコマンドとほぼ同じです。たとえば、Tux Linuxに関するエントリをすべて削除するには、次のコマンドを実行します。

```
ldapdelete -x -D cn=Administrator,dc=example,dc=com -W cn=Tux \
Linux,ou=devel,dc=example,dc=com
```

36.5 YaSTによるLDAPサーバの設定

LDAPサーバを設定するには、YaSTを使用します。一般的にLDAPサーバは、ユーザアカウントデータ、メール設定、DNS設定、およびDHCPサーバ設定を管理するために用いられます。

図 36.2 YaST LDAPサーバの設定

LDAPサーバのユーザアカウントデータを設定するには、以下の手順に従ってください。

- 1 rootとしてログインします。
- 2 YaSTを起動して、`[ネットワークサービス] > [LDAPサーバ]` の順に選択します。
- 3 システムブート時にLDAPを開始するように設定します。
- 4 LDAPサーバに、自己のサービスをSLP経由でアナウンスさせる場合は、`[Register at an SLP Daemon]` を選択します。
- 5 `[General Setting]` と `[データベース]` を設定するには、`[設定]` を選択します。

LDAPサーバの `[グローバル設定]` を設定するには、以下の手順に従ってください。

- 1 ダイアログの左側にある `[Schema Files]` を選択して、サーバの環境設定に含めるスキーマファイルを変更するか、またはそのまま使用しま

す。スキーマファイルのデフォルトは、YaSTユーザアカウントデータのソースを提供するサーバに適用されます。

- 2 *[Log Level Settings]* を選択すると、LDAPサーバの記録動作(冗長度)を設定できます。事前定義済みのリストから、必要に応じて記録オプションを選択するか、選択を解除します。ログファイルは、多数のオプションを選択するほど大きくなります。
- 3 LDAPサーバが許可する接続の種類を選択します。以下の項目を選択することができます。

`bind_v2`

このオプションを選択すると、旧バージョンのプロトコル(LDAPv2)を使用してクライアントから接続要求(バインド要求)を出すことができます。

`bind_anon_cred`

通常、LDAPサーバは空の資格情報(DNまたはパスワード)を使用した認証試行を拒否します。ただし、このオプションを使用すると、DNを使用せずにパスワードのみを使用して接続し、匿名接続を確立できます。

`bind_anon_dn`

このオプションを有効にすると、DNだけでパスワードは使用せずに認証なしで(匿名で)接続できます。

`update_anon`

このオプションを有効にすると、非認証(匿名)更新操作が許可されます。アクセスはACLとその他の規則に従って制限されます(36.3.1項「[slapd.conf内のグローバルエントリ](#)」(731 ページ)を参照)。

- 4 クライアントとサーバ間の安全な通信を設定するには、*[TLS Settings]* を使用します。
 - 4a クライアント/サーバの通信にTLSおよびSSL暗号化を使用するには、*[TLSActive]* に *[Yes]* を設定します。
 - 4b *[Select Certificate]* をクリックして、有効な証明書の入手方法を設定します。*[Import Certificate]* (外部ソースから証明書をインポートする場合)または *[Use Common Server Certificate]* (インストール時に作成された証明書を使用する場合)を選択します。

- 証明書をインポートすることを選択した場合、証明書へのパスの入力を要求するメッセージが表示されます。
- 共通のサーバ証明書を使用するが、インストール時に証明書が作成されていない場合は、証明書が作成されます。

LDAPサーバが管理するデータベースを設定するには、以下の手順に従ってください。

- 1 ダイアログの左側にある、*[Databases]* を選択します。
- 2 新しいデータベースを追加するには、*[Add Database]* をクリックします。
- 3 必要なデータを入力します。

Base DN

LDAPサーバのベースDNを入力します。

Root DN

サーバ管理者のDNを入力します。*[Append Base DN(ベースDNの追加)]* を選択した場合は、管理者のcnのみを入力すると、残りはシステムにより自動的に入力されます。

LDAP Password

データベース管理者のパスワードを入力します。

暗号化

ルートDNのパスワードを保護するために使用する暗号化アルゴリズムを指定します。*[crypt]*、*[smd5]*、*[sha]*、または*[sha]*を選択します。このダイアログには*[plain]* オプションも用意されています。このオプションを選択すると、プレーンテキストパスワードが使用可能になりますが、セキュリティ上の理由から選択することはお薦めしません。設定を確認して前のダイアログに戻るには、*[OK]* を選択します。

- 4 LDAPサーバのセキュリティを強化するには、パスワードポリシーの強制を有効にしてください。

- 4a パスワードポリシーを指定するには、[パスワードポリシーの設定] を選択します。
- 4b 追加、変更時に、平文テキストパスワードをデータベースに書き込む前にハッシュするには、[平文パスワードをハッシュする] を選択します。
- 4c [アカウントロック状態を知らせる] は、ロックされたアカウントへのバインド要求時に、詳細なエラーメッセージを返します。

警告: セキュリティが重要な環境におけるロックされたアカウント

セキュリティが大切な環境では、[アカウントロック状態を知らせる] は使用しないでください。ロックされたアカウントに関するエラーメッセージには、セキュリティに関する情報も含まれているため、不正侵入者に悪用される可能性があります。

- 4d デフォルトのポリシーオブジェクトのDNを入力してください。YaST が推奨するDN以外のDNを使用するには、選択項目を入力してください。それ以外の場合は、デフォルト設定を使用してください。

- 5 データベース設定を終了するには、[完了] をクリックします。

パスワードポリシーを選択していない場合は、この時点でサーバを実行することができます。パスワードポリシーを有効にしている場合は、パスワードポリシーの設定作業を行います。存在していないパスワードポリシーオブジェクトを選択した場合、YaSTがそれを作成します。

- 1 LDAP サーバパスワードを入力します。

- 2 パスワード変更ポリシーの設定:

- 2a パスワード履歴に保管するパスワード数を指定します。保存されているパスワードは、ユーザが再利用することはできません。
- 2b ユーザが各自のパスワードを変更できるかどうか、また管理者がリセットした場合にユーザにパスワードの変更を強制するかどうかを指定します。必要に応じて、パスワード変更時に古いパスワードの入力を要求するかどうかを指定します。

- 2c** パスワード品質の検査を行うかどうか、またどの程度まで検査するかを指定します。有効なパスワードとみなす最小パスワード長を設定します。[確認できないパスワードを受け付ける]を選択した場合、品質検査を実行できない場合でも、ユーザは暗号化パスワードを使用することができます。[確認済みパスワードのみを受け付ける]を選択した場合、パスワード検査に合格したパスワードだけが有効とみなされます。

3 パスワードエージングポリシーの設定:

- 3a** 最小パスワード有効日数(有効なパスワードを変更できるようになるまでの時間)と最大パスワード有効日数を指定します。
- 3b** パスワード有効期限の警告を出してから、実際にパスワードの有効期限が切れるまでの時間を指定します。
- 3c** パスワードが完全に失効するまでの、有効期限切れパスワードの使用を許可する猶予回数を指定します。

4 ロックアウトポリシーの設定:

- 4a** パスワードロックを有効にします。
- 4b** パスワードをロックするまでのバインド失敗回数を指定します。
- 4c** パスワードのロック期間を指定します。
- 4d** パスワード失敗をキャッシュに保持する期間を指定します。

5 [了解] を選択して、パスワードポリシー設定を適用します。

以前に作成したデータベースを編集するには、そのベースDNを左側のツリーで選択します。ウィンドウの右側に、新規データベースの作成に使用する際と同様にダイアログが表示されます。ただし、この場合、ベースDNはグレー表示され、変更することはできません。

[終了] を選択してLDAPサーバの設定を終了すると、LDAPサーバの基本的な動作設定に進む準備ができたことになります。この設定を微調整するには、

ファイル/etc/openldap/slapd.confを適切に編集してからサーバを再起動します。

36.6 YaSTを使ったLDAPクライアントの設定

YaSTには、LDAPベースのユーザ管理をセットアップするためのモジュールが組み込まれています。インストール時にこの機能を有効にしなかった場合は、[ネットワークサービス] > [LDAPクライアント] の順に選択してモジュールを起動します。LDAPに必要なPAMおよびNSS関連の変更が自動的に有効になり、必要なファイルがインストールされます。

36.6.1 標準的な処理手順

クライアントマシンのバックグラウンドで動作しているプロセスについての背景となる知識があれば、YaST LDAPクライアントモジュールの動きを理解するうえで助けになります。ネットワーク認証でLDAPが有効になっている場合、またはYaSTモジュールが呼び出された場合、pam_ldapおよびnss_ldapパッケージがインストールされ、該当する2つの環境設定ファイルが設定されます。pam_ldapは、ログインプロセスと認証データのソースとなるLDAPディレクトリ間のネゴシエーションを担当します。専用モジュールのpam_ldap.soがインストールされ、PAM設定が調整されます(例 36.11. 「LDAPに合わせて調整されたpam_unix2.conf」 (747 ページ)を参照)。

例 36.11 LDAPに合わせて調整されたpam_unix2.conf

```
auth:      use_ldap
account:   use_ldap
password:  use_ldap
session:   none
```

LDAPを使用するようにサービスを手動で追加設定する場合は、/etc/pam.d内のサービスに対応するPAM設定ファイルにPAM LDAPモジュールを組み込みます。/usr/share/doc/packages/pam_ldap/pam.d/には、個々のサービスに合わせて調整済みの設定ファイルが用意されています。適切なファイルを/etc/pam.dにコピーしてください。

nsswitchメカニズムを介したglibcの名前解決は、LDAPと共にnss_ldapを使用するように調整されています。新しく調整されたファイルnsswitch.confが、このパッケージのインストールと共に/etcに作成されます。nsswitch.confの詳細は、を参照してください。30.7.1項「環境設定ファイル」(644 ページ)LDAPを使用してユーザ管理および認証を行うために、nsswitch.confに次の行が存在する必要があります。参照先 例 36.12. 「nsswitch.confの調整」 (748 ページ)。

例 36.12 nsswitch.confの調整

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

この行は、glibcのリゾルバライブラリに対して、最初に/etc内で対応するファイルの評価し、次に認証およびユーザデータのソースとしてLDAPサーバにアクセスするように指示しています。このメカニズムをテストするために、たとえばgetent passwdコマンドを使用してユーザデータベースの内容を読み込みます。返されたセットには、システムのローカルユーザに関する情報と、LDAPサーバに格納されている全ユーザに関する情報が含まれているはずです。

LDAPで管理されている一般ユーザが、sshまたはloginを使ってサーバにログインするのを禁止するには、/etc/passwdおよび/etc/groupファイルを編集します。それぞれのファイルに行を追加する必要があります。この行は、/etc/passwdの場合は+:::/:sbin/nologin、/etc/groupの場合は+:::です。

36.6.2 LDAPクライアントの設定

最初にnss_ldapを調整すれば、pam_ldap、/etc/passwd、/etc/groupの設定はYaSTによって行われるので、単にクライアントをサーバに接続すれば、YaSTにLDAPによるユーザ管理を行わせることができます。この基本的なセットアップは**基本的な設定項** (749 ページ)で説明されています。

YaSTのグループおよびユーザ設定モジュールをさらに設定するには、YaST LDAPクライアントを使います。これには、新規ユーザおよびグループのデフォルト設定、そしてユーザまたはグループに割り当てられる属性の数と性

質を操作することが含まれます。LDAPのユーザ管理を使えば、従来のユーザまたはグループ管理ソリューションより、ユーザやグループにずっと多くの異なった属性を割り当てることができます。これは**YaSTのグループおよびユーザ管理のモジュールを設定する項** (752 ページ)で説明されています。

基本的な設定

インストール時にLDAPユーザ管理を選択するか、インストール後のシステムのYaSTコントロールセンタで [ネットワークサービス] > [LDAPクライアント] の順に選択すると、基本的なLDAPクライアント設定ダイアログ(図 36.3. 「YaST:LDAPクライアントの設定」 (749 ページ))が表示されます。

図 36.3 YaST:LDAPクライアントの設定



マシンのユーザをOpenLDAPサーバに対して認証し、OpenLDAPによるユーザ管理を有効にするには、以下の手順に従います。

- 1 [UseLDAP] をクリックして、LDAPの使用を有効にします。認証のためにLDAPを使うものの、他のユーザがこのクライアントにログインしないようにする場合には、[Use LDAP but Disable Logins] を選択します。
- 2 使用するLDAPサーバのIPアドレスを入力します。

- 3 [LDAP base DN] に入力して、LDAPサーバ上の検索ベースを選択します。ベースDNを自動的に取得する場合は、[Fetch DN] をクリックします。その後、YaSTは、上記で指定したサーバアドレス上でLDAPデータベースをチェックします。YaSTによって出力された検索結果から適切なベースDNを選択します。
- 4 サーバとの間でTLSまたはSSLによって保護された通信が必要な場合には [LDAP TLS/SSL] を選択します。
- 5 LDAPサーバがまたLDAPv2を使用している場合には、[LDAP Version 2] を選択して、このプロトコルのバージョンの使用を明示的に有効にします。
- 6 リモートに管理された/homeなど、クライアントにリモートディレクトリをマウントする場合には、[Start Automounter] をオンにします。
- 7 最初にユーザがログインした時に、ユーザのホームを自動的に作成する場合は、[ログイン時にホームディレクトリを作成します] を選択します。
- 8 [Finish] をクリックして、設定を適用します。

図 36.4 YaST: 詳細設定

The screenshot shows the 'YaST: Detailed Environment Configuration' window. The left sidebar contains the 'LDAP Client Configuration' section, which includes instructions on how to configure LDAP client settings, such as using the 'ldap.conf' file or the 'ldap.conf' file in the '/etc/ldap' directory. The main window displays the 'LDAP Client Configuration' tab, which is divided into two sub-tabs: 'Client Configuration' and 'Group Mapping'. The 'Client Configuration' sub-tab is active, showing fields for 'User Mapping', 'Password Mapping', and 'Group Mapping'. The 'User Mapping' field is set to 'dc=example,dc=com', the 'Password Mapping' field is set to 'dc=example,dc=com', and the 'Group Mapping' field is set to 'member'. There are buttons for 'Browse', 'Reference', and 'Cancel' next to each field. At the bottom of the window, there are buttons for 'Cancel' and 'Apply'.

サーバ上のデータを管理者として修正するには、[詳細な設定] をクリックします。次のダイアログは2つのタブに分かれています。詳細については、**図 36.4. 「YaST:詳細設定」** (750 ページ)を参照してください。

- 1** [Client Settings] タブで、必要に合わせて以下の設定を調整します。
 - 1a** ユーザ、パスワード、グループの検索ベースが [LDAP base DN] で指定したグローバルな検索ベースとは異なる場合には、[User Map]、[Password Map]、および [Group Map] でそれらの異なる名前付けコンテキストを入力します。
 - 1b** パスワード変更プロトコルを指定します。パスワードが変更されたときに使用する標準的な方法はcryptで、cryptによって生成されたパスワードハッシュが使用されることを意味しています。この点や他のオプションの詳細については、pam_ldap manページを参照してください。
 - 1c** [Group Member Attribute] で、使用するLDAPグループを指定します。このデフォルトの値はmemberです。
- 2** [Administration Settings] で、以下の設定を調整します。
 - 2a** [Configuration Base DN] で、ユーザ管理データを保管するベースを設定します。
 - 2b** [Administrator DN] に適切な値を入力します。この特定のユーザがLDAPサーバに保管されたデータを操作できるようにするためには、このDNは、/etc/openldap/slapd.confで指定されたrootdn値と同一である必要があります。フルDN。
(cn=Administrator,dc=example,dc=comなど)を入力するか、または [Append Base DN] を有効化して、cn=Administratorを入力するときに自動的にベースDNが追加されるようにします。
 - 2c** サーバ上に基本設定オブジェクトを作成して、LDAPによるユーザ管理を有効にするには、[Create Default Configuration Objects] をオンにします。
 - 2d** お使いのクライアントマシンを、ネットワーク上のホームディレクトリ用のファイルサーバとして動作させる場合には、[Home Directories on This Machine] をオンにします。

2e 使用するパスワードポリシー設定を選択、追加、削除、または変更するには、`[パスワードポリシー]` セクションを使用します。YaSTを使ったパスワードポリシーの設定は、LDAPサーバ設定の一部です。

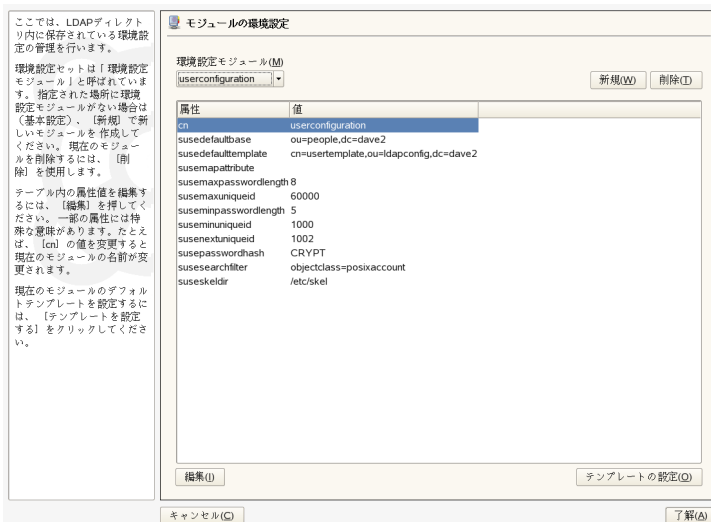
2f `[Accept]` をクリックして `[Advanced Configuration]` を終え、`[Finish]` をクリックして設定を適用します。

`[ユーザ管理の設定]` をクリックし、LDAPサーバ上のエントリを編集します。これにより、サーバに格納されているACLとACIに従って、サーバ上の設定モジュールへのアクセス権が付与されます。**YaSTのグループおよびユーザ管理のモジュールを設定する項**(752 ページ)で概略が説明されている手順に従います。

YaSTのグループおよびユーザ管理のモジュールを設定する

YaSTのLDAPクライアントを使用して、YaSTモジュールをユーザとグループの管理用に調整し、それを必要に応じて拡張します。データの登録を単純化するために、個々の属性のデフォルトの値のテンプレートを定義します。ここで作成した事前設定は、LDAPディレクトリにLDAPオブジェクトとして格納されます。ユーザデータの登録には、通常のYaSTのユーザおよびグループ管理用モジュールが使用されます。登録されたデータはサーバ上にLDAPオブジェクトとして保管されます。

図 36.5 YaST: モジュール設定



モジュール設定ダイアログ(図 36.5. 「YaST:モジュール設定」 (753 ページ))を使用すると、新規モジュールの作成、既存の設定モジュールの選択と変更、およびそれらのモジュールのテンプレートの設計と変更ができます。

新しい設定モジュールを作成するには、以下の手順に従います。

- 1 [New] をクリックして、作成するモジュールのタイプを選択します。ユーザ設定モジュールの場合にはsuseuserconfigurationを選択し、グループ設定の場合にはsusegroupconfigurationを選択します。
- 2 新しいテンプレートの名前を選択します。これにより、コンテンツビューに、このモジュールで許可されている全属性と、それぞれに割り当てられている値がテーブル形式のリストとして表示されます。このリストには、設定されているすべての属性に加えて、現行スキーマで許可されているが現在は使用されていない他の属性もすべて含まれています。
- 3 プリセットされている値を受け入れるか、それぞれの属性を選択して [Edit] を押し、新しい値を入力して、グループおよびユーザ構成で使用するデフォルトを調整します。モジュールの名前を変更するには、モジュールのcn属性を変更します。現在選択しているモジュールを削除するには [削除] をクリックします。

- 4 [了解] をクリックすると、選択メニューに新しいモジュールが追加されます。

YaSTのグループおよびユーザ管理用モジュールには、重要な標準値が設定されたテンプレートが埋め込まれています。設定モジュールに関連したテンプレートを編集するには、以下の手順に従います。

- 1 [Module Configuration] ダイアログで、[Configure Template] をクリックします。
- 2 必要に応じて、このテンプレートに割り当てられている一般的な属性の値を決めます。空にしておくこともできます。空の属性は、LDAPサーバ上で削除されます。
- 3 新しいオブジェクト(LDAPツリー内のユーザまたはグループ設定オブジェクト)のデフォルトの値を修正、削除、または追加します

図 36.6 YaST: オブジェクトテンプレートの設定

ここでは、新しいオブジェクト(ユーザやグループなど)を作成するためのテンプレートを指定します。

テンプレートの属性値を編集するには、「編集」を選択します。「cn」の値を変更すると、テンプレートの名前が変更されます。

2番目のテーブルには、新しいオブジェクトで使われる「デフォルト値」の一覧が表示されます。この一覧で、新しい値を追加したり、既存の値を編集/削除したりできます。

オブジェクトテンプレートの環境設定

属性	値
cn	usertemplate
susenamingattribute	uid
suseplugin	UsersPluginLDAPAllUsersPluginMail
susessecondarygroup	

編集(E)

新規オブジェクトのデフォルト値

オブジェクトの属性	デフォルト値
homedirectory	/home/%uid
loginshell	/bin/bash

追加(D) 編集(E) 削除(D)

キャンセル(C)

了解(A)

モジュールのsusedefaulttemplate属性値を調整済みテンプレートのDNに設定し、テンプレートを対応するモジュールに接続します。

ティップ

絶対値の代わりに変数を使用すると、属性のデフォルト値を他の属性から作成できます。たとえば、新規ユーザの作成時には、`sn`と`givenName`の属性値から`cn=%sn %givenName`が自動的に作成されます。

すべてのモジュールとテンプレートを適切に設定し、実行する準備が完了したら、新しいグループとユーザを通常の方法でYaSTに登録できます。

36.7 YaSTでのLDAPユーザおよびグループの設定

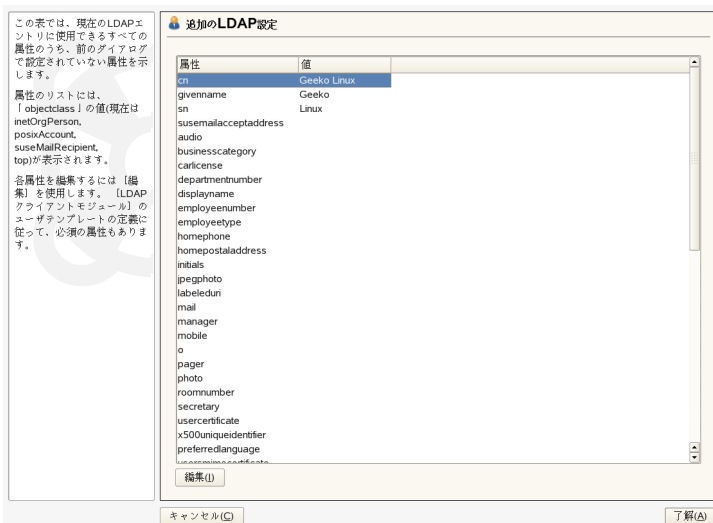
ユーザおよびグループデータの実際の登録手順は、LDAPを使用しない場合とほぼ同様です。次に、ユーザ管理に関連する手順の概略を示します。グループの管理手順も同様です。

- 1 [セキュリティとユーザ] > [ユーザを作成あるいは編集する] の順に選択し、YaSTのユーザ管理にアクセスします。
- 2 [Set Filter] を使って、ユーザの表示をLDAPユーザに制限し、Root DNのパスワードを入力します。
- 3 [Add] をクリックして、新しいユーザの設定を入力します。4つのタブのある[描画色を変更] ダイアログが開きます。
 - 3a [User Data] タブでユーザ名、ログイン名、およびパスワードを指定します。
 - 3b [Details] タブをクリックして、新しいユーザの所属するグループ、ログインシェル、およびホームディレクトリを設定します。必要であれば、デフォルトの値を、必要に適した値に変更します。デフォルトの値、およびパスワードの設定は、**YaSTのグループおよびユーザ管理のモジュールを設定する項**(752 ページ)で説明されている手順で設定できます。
 - 3c デフォルトの [Password Settings] の設定を修正するか、受け入れます。

3d [Plug-Ins] タブで、LDAPプラグインを選択し、[Launch] をクリックして、新規ユーザに割り当てる付加的なLDAP属性を設定します(図 36.7. 「YaST:他のLDAP設定」 (756 ページ)を参照)。

4 [Accept] をクリックして設定を適用し、ユーザ設定を終了します。

図 36.7 YaST:他のLDAP設定



ユーザ管理の初期入力フォームには、[LDAPオプション] が用意されています。ここでは、使用可能なユーザのセットにLDAP検索フィルタを適用するか、[LDAP User and Group Configuration(LDAPユーザとグループの設定)] を選択してLDAPユーザおよびグループの設定モジュールにアクセスできます。

36.8 LDAPディレクトリツリーの参照

LDAPディレクトリツリーとそのすべてのエントリを手軽に参照するには、YaST LDAPブラウザを使用します。

- 1 rootとしてログインします。
- 2 `[YaST]` > `[ネットワークサービス]` > `[LDAPブラウザ]` の順にクリックします。
- 3 LDAPサーバのアドレスと管理者DNを入力し、サーバに保管されているデータに対して読み込みアクセスと書き込みアクセスの両方を行う場合は、このサーバのRootDNのパスワードも入力します。

代わりに `[Anonymous Access]` (匿名アクセス)を選択して、パスワードを指定しないでディレクトリに読み込みアクセスすることもできます。

`[]` タブには、お使いのコンピュータが接続しているLDAPディレクトリの内容が表示されます。項目をクリックすると、その下位の項目が表示されます。

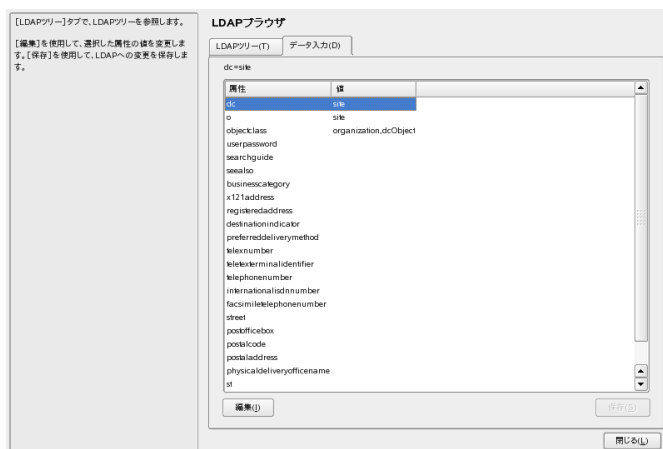
☒ 36.8 LDAPディレクトリツリーの参照



- 4 項目の詳細を表示するには、`[LDAPツリー]` ビューで該当する項目を選択し、`[データ入力]` タブを開きます。

項目に関連するすべての属性と値が表示されます。

図 36.9 項目データの参照



5 これらの属性の値を変更するには、該当する属性を選択して **[編集]** をクリックします。次に、新しい値を入力して **[保存]** をクリックします。RootDNのパスワードの入力を要求するプロンプトが表示されたら、パスワードを入力してください。

6 LDAPブラウザを終了する場合は、 **[閉じる]** を選択します。

36.9 詳細情報

SASL設定や、複数のスレーブ間で作業不可を分散するためのLDAPサーバのレプリケートの設定などの複雑なトピックについては、ここではあえて触れませんでした。この2つの項目の詳細については、『*OpenLDAP 2.2 Administrator's Guide*』を参照してください。

OpenLDAPプロジェクトのWebサイトには、LDAPの初心者向けや熟練者向けのあらゆるマニュアルが用意されています。

『OpenLDAP Faq-O-Matic』

OpenLDAPのインストール、設定、および運用に関する豊富なQAがまとめられています。「OpenLDAP Faq-O-Matic」は、<http://www.openldap.org/faq/data/cache/1.html>にあります。

Quick Start Guide

LDAPサーバのインストール方法を手順を追って簡単に説明しています。、またはインストール済みのシステムで/usr/share/doc/packages/openldap2/admin-guide/quickstart.htmlを参照してください。
<http://www.openldap.org/doc/admin22/quickstart.html>

『OpenLDAP 2.2 Administrator's Guide』

アクセス制御や暗号化など、LDAP設定の重要な側面を詳細に説明しています。、またはインストール済みのシステムで/usr/share/doc/packages/openldap2/admin-guide/quickstart.htmlを参照してください。
<http://www.openldap.org/doc/admin22/>

『Understanding LDAP』

LDAPの基本原則一般について、詳細に説明しています:<http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf>。

LDAPに関する書籍

- *LDAP System Administration* by Gerald Carter (ISBN 1-56592-491-6)
- *Understanding and Deploying LDAP Directory Services* by Howes, Smith, and Good (ISBN 0-672-32316-8)

LDAPに関する究極的な参考資料は、RFC 2251～2256です。

Samba

Sambaを使用すると、DOS、Windows、OS/2マシンに対するファイルサーバおよびプリントサーバをUnixマシン上に構築できます。Sambaは、今や成熟の域に達したかなり複雑な製品です。Sambaは、YaST、SWAT (Webインタフェース)または設定ファイルを使用して設定します。

37.1 用語

ここでは、SambaのマニュアルやYaSTモジュールで使用する用語について説明します。

SMBプロトコル

SambaはSMB(サーバメッセージブロック)プロトコルを使用します。SMBはNetBIOSサービスを基にしています。IBMからの圧力によって、Microsoftがこのプロトコルをリリースしたので、他のソフトウェアメーカーはMicrosoftドメインネットワークに接続できるようになりました。Sambaでは、SMBプロトコルがTCP/IPプロトコルの上で動作するので、すべてのクライアントにTCP/IPプロトコルをインストールする必要があります。

ティップ: IBM System z:NetBIOSサポート

IBM System zではSMB over TCP/IPのみがサポートされています。これら2つのシステムではNetBIOSをサポートしていません。

CIFSプロトコル

CIFS (common Internet file system)プロトコルは、Sambaがサポートしているプロトコルです。CIFSは、ネットワーク上で使用する標準のリモートファイルシステムで、ユーザグループによる共同作業およびネットワーク間でのドキュメントの共有ができるようにします。

NetBIOS

は、マシン間通信用に設計されたソフトウェアインタフェース(API)です。ここではネームサービスが提供されています。これにより、ネットワークに接続されたマシンが、それ自体の名前を維持できます。予約を行えば、これらのマシンを名前によって指定できます。名前を確認する一元的なプロセスはありません。ネットワーク上のマシンでは、すでに使用済みの名前でない限り、名前をいくつでも予約できます。現在、NetBIOSインタフェースは、異なるネットワークアーキテクチャ用に実装できるようになっています。ネットワークハードウェアと比較的密接に機能する実装はNetBEUIと呼ばれますが、これはよくNetBIOSとも呼ばれます。NetBIOSとともに実装されるネットワークプロトコルは、Novell IPX (TCP/IP経由のNetBIOS)とTCP/IPです。

TCP/IP経由で送信されたNetBIOS名は、`/etc/hosts`で使用されている名前、またはDNSで定義された名前とまったく共通点がありません。NetBIOSは独自の、完全に独立した名前付け規則を使用しています。しかし、管理を容易にするために、DNSホスト名に対応する名前を使用することゝ勧めします。これはSambaが使用するデフォルトでもあります。

Sambaサーバ

Sambaサーバは、IPネーミングサービスを介してクライアントにSMB/CIFSサービスおよびNetBIOSを提供するサーバです。Linuxの場合、SMB/CIFSサービス用の`smnd`と、ネーミングサービス用の`nmbd`の2種類のSambaサーバデーモンが用意されています。

Sambaクライアント

Sambaクライアントは、SMBプロトコルを介してSambaサーバからSambaサービスを使用するシステムです。Mac OS X、Windows、OS/2などの一般的なオペレーティングシステムは、すべてSMBプロトコルをサポートしています。TCP/IPプロトコルは、すべてのコンピュータにインストールする必要があります。Sambaは、異なるUNIXフレーバーに対してクライアントを提供します。Linuxでは、SMB用のカーネルモジュールがあり、LinuxシステムレベルでのSMBリソースの統合が可能です。Sambaクライアントに対していずれのデーモンも実行する必要はありません。

共有

SMBサーバは、そのクライアントに対し、共有によってハードウェア空間を提供します。共有は、サーバ上のサブディレクトリのあるディレクトリおよびプリンタです。これは名前によってエクスポートされ、名前によってアクセスされます。共有名にはどのような名前も設定できます。エクスポートディレクトリの名前である必要はありません。プリンタにも名前が割り当てられます。クライアントはプリンタに名前でアクセスできます。

37.2 Sambaの起動および停止

Sambaサーバは、ブート中に自動か手動で起動または停止できます。ポリシーの開始および停止は、[37.3.1項「YaSTによるSambaサーバの設定」](#) (763 ページ)で説明しているように、YaST Sambaサーバ設定の一部です。

YaSTを使用して実行中のSambaサービスを停止または起動するには、`[システム] > [システムサービス (Runlevel)]` の順に選択します。コマンドラインで、`rcsmb stop && rcnmb stop`を入力して、Sambaに必要なサービスを停止し、`rcnmb start && rcsmb start`を入力して起動します。

37.3 Sambaサーバの設定

SUSE Linux Enterprise®のSambaサーバは、YaSTを使って、または手動で設定することができます。手動で設定を行えば細かい点まで調整できますが、YaSTのGUIほど便利ではありません。

37.3.1 YaSTによるSambaサーバの設定

Sambaサーバを設定するには、YaSTを起動して、`[ネットワークサービス] > [Sambaサーバ]` の順に選択します。モジュールを初めて起動すると、`[Samba Server Installation]` ダイアログが表示され、サーバの管理に関するいくつかの基本設定を行うように指示された後、最後にSambaのrootのパスワードを入力するように指示されます。次回起動時には、`[Samba Server Configuration]` ダイアログが表示されます。

〔*Samba Server Installation*〕 ダイアログは、次の2つのステップで構成されています。

ワークグループまたはドメイン名

〔*Workgroup or Domain Name*〕 から既存の名前を選択するか、新しい名前を入力し、〔次へ〕を入力します。

Sambaサーバのタイプ

次のステップで、PDCとして機能するサーバを指定し、〔次へ〕を入力します。

〔*Samba Server Installation*〕 の設定はすべて、後で 〔*Samba Server Configuration*〕 ダイアログの 〔個人情報〕 タブで変更できます。

YaSTを使ったSambaの詳細設定

Sambaサーバモジュールの初回起動中、〔*Samba Server Installation*〕 ダイアログの直後に 〔*Samba Server Configuration*〕 ダイアログが表示されます。ここでは、Sambaサーバの設定を編集することができます。

編集し終わったら、〔*Finish*〕 をクリックして、設定ダイアログを閉じます。

サーバを起動する

〔*Start Up*〕 タブで、Sambaサーバの起動に関する設定を行います。システムのブート時に毎回サービスが起動されるようにするには、〔*During Boot*〕 を選択します。手動起動を有効化するには、〔*Manually*〕 を選択します。Sambaサーバの起動の詳細については、[37.2項「Sambaの起動および停止」](#) (763 ページ)を参照してください。

このタブで、ファイアウォールのポートを開くこともできます。そのためには、〔*Open Port in Firewall*〕 を選択します。複数のネットワークインタフェースがある場合は、〔*Firewall Details*〕 をクリックし、インタフェースを選択した後、〔*OK*〕 をクリックして、Sambaサービス用のネットワークインタフェースを選択します。

共有

〔共有〕 タブで、有効にするSambaの共有を指定します。homesおよびプリンタなど、事前定義済みの共有がいくつかあります。〔状態の変更〕を使用し

て、[有効]と[無効]の間で切り替えます。新規の共有を追加するには [追加]、共有を削除するには [削除]をクリックします。

ID

[個人情報] タブで、ホストが関連付けられているドメイン([Base Settings])と、ネットワークで代替ホスト名を使用するかどうか([NetBIOS Host Name])を指定します。エキスパートグローバル設定、またはLDAPなどのユーザ認証を設定するには、 [詳細な設定] をクリックします。

他のドメインからのユーザ

他のドメインのユーザを、自分のドメインにアクセスさせるには、 [Trusted Domains] タブで適切な設定を行います。新しいドメインを追加するには、 [追加] をクリックします。選択したドメインを削除するには、 [削除] をクリックします。

LDAPを使用する場合

[LDAP Settings] タブでは、認証に使用するLDAPサーバを設定することができます。LDAPサーバへの接続をテストするには、 [Test Connection] をクリックします。エキスパートLDAP設定を設定するか、デフォルト値を使用する場合、 [詳細な設定] をクリックします。

LDAP設定の詳細は、[第36章 LDAP—ディレクトリサービス](#) (725 ページ)を参照してください。

37.3.2 SWATを使用したWeb管理

Sambaサーバ管理の代替ツールは、SWAT(Samba Web管理ツール)です。このプログラムには、Sambaサーバを設定するための簡単なWebインタフェースがあります。SWATを使用するには、Webブラウザで、<http://localhost:901>を開き、rootユーザでログインします。特別なSamba rootアカウントがない場合、システムのrootアカウントを使用します。

注意: **SWAT**の有効化

Sambaサーバのインストール後、**SWAT**は有効化されていません。**SWAT**を有効化するには、**YaST**で [ネットワークサービス] > [ネットワークサービス(*xinetd*)] の順に開き、ネットワークサービス設定を有効にし、テーブルから [*swat*] を選択し、[状態の変更(オンまたはオフ)] をクリックします。

37.3.3 サーバの手動設定

Sambaをサーバとして使用する場合は、sambaをインストールします。Sambaの主となる設定ファイルは、`/etc/samba/smb.conf`です。このファイルは2つの論理部分に分けられます。[*global*]セクションには、中心的なグローバル設定が含まれます。[*share*]セクションには、個別のファイルとプリンタ共有が入っています。このアプローチにより、共有に関する詳細は[*global*]セクションで個別に、またはグローバルに設定することができ、設定ファイルの構造的透過性が高まっています。

グローバルセクション

[*global*]の次のパラメータは、ネットワークの設定に応じた必要条件を満たし、**Windows**環境で他のマシンが**SMB**を経由してこの**Samba**サーバにアクセスできるようにするために多少の調整が必要です。

workgroup = TUX-NET

この行は、**Samba**サーバをワークグループに割り当てます。**TUX-NET**を実際のネットワーク環境にある適切なワークグループに置き換えてください。**DNS**名がネットワーク内の他のマシンに割り当てられていなければ、**Samba**サーバが**DNS**名の下に表示されます。**DNS**名が使用できない場合は、`netbiosname=MYNAME`を使用してサーバ名を設定します。このパラメータについての詳細は`mansmb.conf`を参照してください。

os level = 2

このパラメータは、**Samba**サーバがワークグループの**LMB**(ローカルマスターブラウザ)になるかどうかのきっかけとなります。**Samba**サーバの設定が誤っていた場合に、既存の**Windows**ネットワークに支障が出ないように、小さな値を選択します。この重要なトピックについての詳細は、パッケージ

マニュアルのtextdocsサブディレクトリにあるBROWSING.txtとBROWSING-Config.txtを参照してください。

ネットワーク内に他のSMBサーバ(たとえば、Windows NTまたは2000サーバ)が存在せず、ローカル環境に存在するすべてのシステムのリストをSambaサーバに保存する場合は、os_levelの値を大きくします(たとえば、65)。これでSambaサーバが、ローカルネットワークのLMBとして選択されました。

この設定を変更するときは、それが既存のWindowsネットワーク環境にどう影響するかを慎重に検討する必要があります。はじめに、隔離されたネットワークで、または影響の少ない時間帯に、変更をテストしてください。

wins supportとwins server

アクティブなWINSサーバをもつ既存のWindowsネットワークにSambaサーバを参加させる場合は、wins_serverオプションを有効にし、その値をWINSサーバのIPアドレスに設定します。

各Windowsマシンの接続先サブネットが異なり、互いを認識させなければならない場合は、WINSサーバをセットアップする必要があります。SambaサーバをWINSサーバなどにするには、wins_support = Yesオプションを設定します。ネットワーク内でこの設定が有効なSambaサーバは1台だけであることを確認します。smb.confファイル内で、オプションwins_serverとwins_supportは同時に有効にしないでください。

共有

次の例では、SMBクライアントがCD-ROMドライブとユーザディレクトリ(homes)を利用できるようにする方法を示します。

[cdrom]

CD-ROMドライブが誤って利用可能になるのを避けるため、これらの行はコメントマーク(この場合はセミコロン)で無効にします。最初の列のセミコロンを削除し、CD-ROMドライブをSambaと共有します。

例 37.1 CD-ROMの共有

```
;  
[cdrom]  
;  
comment = Linux CD-ROM  
path = /media/cdrom  
locking = No
```

[cdrom]およびコメント

[cdrom]エントリは、ネットワーク上のすべてのSMBクライアントが認識できる共有の名前です。さらにcommentを追加して、共有を説明することができます。

```
path = /media/cdrom
```

pathオプションで、/media/cdromディレクトリをエクスポートします。

デフォルトを非常に制約的に設定することによって、このシステム上に存在するユーザのみがこの種の共有を利用できるようになります。この共有をあらゆるユーザに開放する場合は、設定にguest ok = yesという行を追加します。この設定は、ネットワーク上の全ユーザに読み込み許可を与えます。このパラメータを使用する場合には、相当な注意を払うことをお勧めします。またこのパラメータを[global]セクションで使用する場合には、さらに注意が必要です。

[homes]

[home]共有は、ここでは特に重要です。ユーザがLinuxファイルサーバの有効なアカウントとパスワードを持ち、独自のホームディレクトリを持っていればそれに接続することができます。

例 37.2 homes共有

```
[homes]  
comment = Home Directories  
valid users = %S  
browseable = No  
read only = No  
create mask = 0640  
directory mask = 0750
```

[homes]

SMBサーバに接続しているユーザの共有名を他の共有が使用していない限り、[homes]共有ディレクティブを使用して共有が動的に生成されます。生成される共有の名前は、ユーザ名になります。

`valid users = %S`

%S は、接続が正常に確立されるとすぐに、具体的な共有名に置き換えられます。[homes]共有の場合、これは常にユーザ名です。したがって、ユーザの共有に対するアクセス権は、そのユーザだけに付与されます。

`browseable = No`

この設定を行うと、共有がネットワーク環境で認識されなくなります。

`read only = No`

デフォルトでは、Sambaは`read only = Yes`パラメータによって、エクスポートされた共有への書き込みアクセスを禁止します。共有に書き込めるように設定するには、`read only = No`値を設定します。これは`writable = Yes`と同値です。

`create mask = 0640`

MS Windows NTベース以外のシステムは、UNIXのパーミッションの概念を理解しないので、ファイルの作成時にアクセス権を割り当てることができません。`create mask`パラメータは、新しく作成されたファイルに割り当てられるアクセス権を定義します。これは書き込み可能な共有にのみ適用されます。実際、この設定はオーナーが読み書き権を持ち、オーナーの一次グループのメンバが読み込み権を持つことを意味します。`valid users = %S`を設定すると、グループに読み込み権が与えられても、読み込みアクセスができなくなります。グループに読み書き権を付与する場合は、`valid users = %S`という行を無効にしてください。

セキュリティ レベル

セキュリティを向上させるため、各共有へのアクセスは、パスワードによって保護されています。SMBには、パーミッションを確認する方法が3つあります。

共有レベルのセキュリティ(セキュリティ=共有)

パスワードが共有に対し確実に割り当てられています。このパスワードを持っているユーザ全員が、その共有にアクセスできます。

ユーザレベルのセキュリティ(セキュリティ=ユーザ)

このセキュリティレベルは、ユーザという概念をSMBに取り入れています。各ユーザは、サーバにパスワードを登録する必要があります。登録後、エクスポートされた個々の共有へのアクセスは、ユーザ名に応じてサーバが許可します。

サーバレベルのセキュリティ(セキュリティ=サーバ):

クライアントに対しては、Sambaがユーザレベルモードで動作しているように見えます。しかし、Sambaはすべてのパスワードクエリを別のユーザレベルモードサーバに渡し、ユーザレベルモードサーバが認証されます。

設定には追加のパラメータが必要です(password server)。

共有、ユーザ、またはサーバレベルのセキュリティの設定は、サーバ全体に適用されます。個別の共有ごとに、ある共有には共有レベルのセキュリティ、別の共有にはユーザレベルセキュリティを設定するといったことはできません。しかし、システム上に設定したIPアドレスごとに、別のSambaサーバを実行することは可能です。

この詳細については、『Samba HOWTO Collection』を参照してください。つのシステムに複数のサーバをセットアップする場合は、オプション `interfaces` および `bind interfaces only` に注意してください。

37.4 クライアントの設定

クライアントは、TCP/IP経由でのみSambaサーバにアクセスできます。IPX経由のNetBEUIおよびNetBIOSは、Sambaで使用できません。

37.4.1 YaSTによるSambaクライアントの設定

Sambaサーバ上の共有リソース(ファイルまたはプリンタ)にアクセスするSambaクライアントを設定します。[ネットワークサービス] > [Windows Domain Membership]を選択して表示されるダイアログに、ドメインまたはワークグループを入力します。[検索]をクリックすると、使用可能なすべてのグループとドメインが表示され、マウスで選択することができます。[Linuxの認証

にもSMBの情報をを用いる]を有効にした場合、ユーザ認証はSambaサーバによって行われます。設定が終わったら、[完了]をクリックします。

37.4.2 Windows 9xおよびME

Windows 9xおよびMEには、あらかじめTCP/IPのサポートが組み込まれています。しかし、デフォルトでインストールされるわけではありません。TCP/IPを追加するには、[コントロールパネル] > [システム] の順に移動し、[追加] > [プロトコル] > [TCP/IP] の順に選択します。Windowsマシンをリブートし、デスクトップでネットワーク環境のアイコンをダブルクリックしてSambaサーバを見つけます。

ティップ

Sambaサーバ上でプリンタを使用するには、対応するWindowsバージョンから、標準のプリンタドライバまたはApple-PostScriptプリンタドライバをインストールします。これをLinuxプリンタキュー(Postscriptを入力形式として許可)にリンクするのが最適な方法です。

37.5 ログインサーバとしてのSamba

Windowsクライアントが大部分を占めるネットワークでは、ユーザが有効なアカウントとパスワードを持つ場合のみ登録できることが求められるのが普通です。Windowsベースのネットワークでは、このタスクはPDC (プライマリドメインコントローラ)によって処理されます。Windows NTサーバをPDCとして使用することもできますが、Sambaサーバを使用しても処理できます。

例 37.3. 「smb.confファイルのグローバルセクション」 (771 ページ)に示すように、smb.confの[global]セクションにエントリを追加する必要があります。

例 37.3 smb.confファイルのグローバルセクション

```
[global]
workgroup = TUX-NET
domain logons = Yes
domain master = Yes
```

暗号化されたパスワードが検証に使用されている場合は(強固に保守された**MS Windows 9x**インストール、**MS Windows NT 4.0**(サービスパック 3以降)、およびそれ以降にリリースされた製品でのデフォルト設定)、**Samba**サーバでこれ进行处理する必要があります。これには、[global]セクションでエントリ `encrypt passwords = yes`を指定します(**Samba**バージョン3ではデフォルト)。また、ユーザアカウントとパスワードを**Windows**に準拠した暗号化形式で作成する必要があります。そのためにはコマンド `smbpasswd -a name`を実行します。さらに次のコマンドを使用して、**Windows NT**ドメイン概念で必要になるコンピュータのドメインアカウントを作成します。

例 37.4 マシンアカウントのセットアップ

```
useradd hostname\$\n\nsmbpasswd -a -m hostname
```

`useradd`コマンドを使用すると、ドル記号が追加されます。コマンド `smbpasswd`を指定すると、パラメータ `-m`を使用したときにドル記号が自動的に挿入されます。コメント付きの設定例(`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`)には、この作業を自動化するための設定が含まれています。

例 37.5 マシンアカウントの自動セットアップ

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \n\n-s /bin/false %m$
```

Sambaがこのスクリプトを確実に正しく実行できるようにするため、必要な管理者許可を持つ**Samba**ユーザを選択します。これには、1人のユーザを選択して `ntadmin`グループに追加します。これにより、この**Linux**グループに属するすべてのユーザに対し、次のコマンドによって `Domain Admin`ステータスを割り当てることができます。

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

この詳細については、`/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`の『**Samba HOWTO Collection**』の第12章を参照してください。

37.6 Active Directoryネットワーク内のSambaサーバ

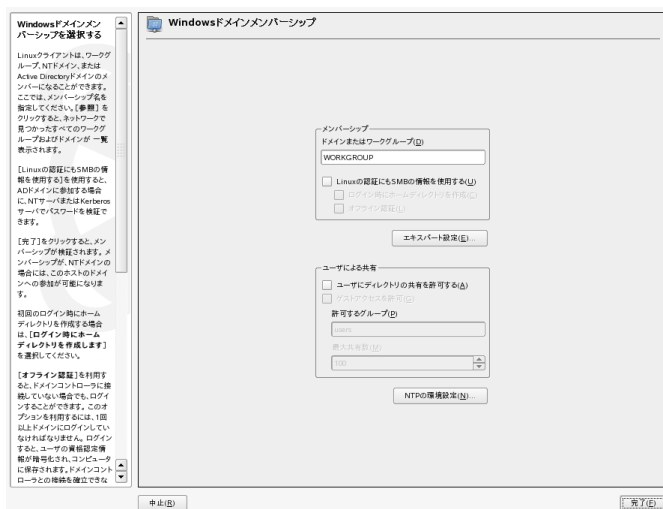
LinuxサーバとWindowsサーバの両方を利用する場合、2つの独立した認証システムまたはネットワークを作成するか、または単一の中央認証システムを持つ単一のネットワークに両方のサーバを接続します。SambaはActive Directoryドメインと連携できるため、お使いのSUSE Linux Enterprise ServerをActive Directory (AD)に参加できます。

既存のActive Directoryドメインに参加するには、インストール時に設定を行うか、または後でYaSTを使って、SMBユーザ認証を有効にします。インストール時にドメインへの参加を設定する方法については、[3.14.7項「Users」](#) (49 ページ)を参照してください。

稼働中のシステムをActive Directoryドメインに参加させるには、以下の手順に従ってください。

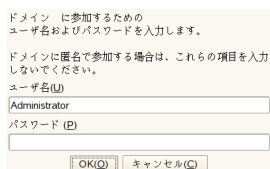
- 1 rootとしてログインし、YaSTを起動します。
- 2 [ネットワークサービス] > [Windows Domain Membership] の順に選択します。
- 3 [Windows Domain Membership] 画面の [Domain or Workgroup] に、参加するドメインを入力します。または、[Browse] を使って、利用できるドメインのリストを表示し、そこから適切なドメインを選択します。

図 37.1 Windows ドメインメンバーシップの決定



- 4 SUSE Linux Enterprise ServerでLinux認証にSMBソースを使用する場合は、*[Linuxの認証にもSMBの情報を提供する]* を選択します。
- 5 *[完了]* をクリックし、ドメインへの参加を確認するメッセージが表示されたら、*[OK]* をクリックします。
- 6 Active DirectoryサーバのWindows管理者用パスワードを入力し、*[OK]* をクリックします。

図 37.2 管理者資格情報の提供



Active Directoryドメインコントローラから、すべての認証データを取得できるようになりました。

37.7 Windows NTサーバからSambaへの移行

SambaとLDAPの設定とは異なり、Windows NTサーバからSUSE Linux Enterprise Server Sambaサーバへの移行手順は、基本的な2つのステップに分かれています。まず、プロファイルを移行して、次にアカウントを移行します。

37.7.1 LDAPサーバの準備

移行の最初のステップとして、まずLDAPサーバを設定します。ソフトウェアクライアントのアカウントに関するベースDN情報とエントリ、およびパスワードを追加する必要があります。LDAP設定の詳細は、[第36章 LDAP—ディレクトリサービス](#) (725 ページ)を参照してください。

すべての項目を手動で設定する必要はありません。smbldap-toolsから、スクリプトを使用することができます。これらのスクリプトは、samba-docパッケージに含まれています。このパッケージがインストールされると、スクリプトは/usr/share/doc/packages/samba/examples/LDAPに格納されます。

注意: LDAPとセキュリティ

LDAPの管理DNは、ルートDN以外アカウントでなければなりません。ネットワークのセキュリティを強化するために、TSLを使った安全な接続を使用することもできます。

37.7.2 Sambaサーバの準備

移行を開始する前に、Sambaサーバを設定します。YaSTのSamba Serverモジュールの[共有]タブで、profile、netlogon、およびhomeシェアを探します。デフォルト値を編集するには、適切なシェアを選択してから、[編集]をクリックします。

SambaサーバにLDAP設定とLDAP管理者の資格情報を追加するには、YaSTのSamba Serverモジュールの[LDAP Settings]タブを使用します。LDAPディレ

クトリにアカウントを追加したり、アカウントを変更するには、LDAP管理DN(ラベル*Administration DN*)とパスワードが必要になります。

37.7.3 Windowsプロファイルの移行

移行する各プロファイルに対して、以下の作業を行います。

手順 37.1 プロファイルの移行

- 1 NT4ドメインコントローラで、[マイコンピュータ] を右クリックして [プロパティ] を選択します。[ユーザー プロファイル] タブを選択します。
- 2 移行するユーザプロファイルを選択します。
- 3 [コピー先] をクリックします。
- 4 [プロファイルのコピー] にパスを指定します(例:c:\temp\profiles)。
- 5 [許可] の [変更] をクリックします。
- 6 [すべてのユーザー] をクリックします。[OK] をクリックして、ボックスを閉じます。
- 7 プロファイルの保存を完了するには、[OK] をクリックします。
- 8 保存したプロファイルを、Sambaサーバの適切なプロファイルディレクトリにコピーします。

37.7.4 Windowsアカウントの移行

手順 37.2 アカウントの移行プロセス

- 1 NTサーバーマネージャを使って、古いNT4ドメイン中にSambaサーバ用のBDCアカウントを作成します。この時、Sambaを動作させてはいけません。

```
net rpc join -S NT4PDC -w DOMNAME -U Administrator%passwd net rpc  
vampire  
-S NT4PDC -U administrator%passwd pdbedit -L
```

2 各UNIXグループをNTグループに割り当てます。

例 37.6 *initGroups.sh* スクリプトの例

```
#!/bin/bash ##### Keep this as a shell script for future re-use #  
Known domain global groups net groupmap modify ntgroup="Domain  
Admins"  
unixgroup=root net groupmap modify ntgroup="Domain Users"  
unixgroup=users net groupmap modify ntgroup="Domain Guests"  
unixgroup=nobody # Our domain global groups net groupmap add  
ntgroup="Operation" unixgroup=operation type=d net groupmap add  
ntgroup="Shipping" unixgroup=shipping type=d
```

3 すべてのグループが認識されていることを確認します。

```
net groupmap list
```

37.8 詳細情報

Sambaについての詳細な情報は、デジタルドキュメントの形で入手できます。コマンドラインから`apropossamba`と入力するとマニュアルページを参照できます。または、**Samba**マニュアルがインストールされている場合は、`/usr/share/doc/packages/samba`ディレクトリに格納されているオンラインマニュアルと例を参照できます。また、コメント付きの設定例(`smb.conf.SuSE`)が`examples`サブディレクトリに用意されています。

Sambaチームが作成した『**Samba HOWTO Collection**』にはトラブルシューティングについても説明されています。またマニュアルの**Part V**では、手順を追って設定を確認するためのガイドが用意されています。`samba-doc`パッケージのインストール後、`/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`で、『**Samba HOWTO Collection**』を参照できます。

/usr/share/doc/packages/samba/examples/LDAP/smbldap-tools-*/docには、LDAPの詳細、およびWindows NT/2000からの移行に関する詳細情報が格納されています。ここで、「*」は、お使いのsmbldap-toolsのバージョンに置き換えてください。

NFS共有ファイルシステム

ネットワーク上でファイルシステムを分散して共有することは、企業環境では一般的なタスクです。NFSは実績のあるシステムで、イエローページプロトコルNISとも連携します。LDAPと連携する暗号化されたより安全なプロトコルについては、NFSv4を確認してください。

NFSをNISと連携して使用すると、ユーザに対してネットワークを透過的にすることができます。NFSでは、ネットワーク経由で任意のファイルシステムを分散できます。適切なセットアップで、ユーザは現在使用している端末と独立した同じ環境を利用できます。

NIS同様、ANFSはクライアント/サーバシステムです。ただし、ファイルシステムをネットワーク経由で提供し(エクスポート)、同時に他のホストからファイルシステムをマウントする(インポート)ことができます。

重要項目: DNSの必要性

原則として、すべてのエクスポートはIPアドレスのみを使用して実行できます。タイムアウトを回避するために、実際に動作するDNSシステムを用意しておく必要があります。mountdデーモンは逆引きを行うため、少なくともログ目的にはDNSが必要です。

38.1 必要なソフトウェアのインストール

ホストをNFSクライアントとして設定する場合、他のソフトウェアをインストールする必要はありません。デフォルトで、NFSクライアントを設定するために必要なすべてのパッケージがインストールされています。

NFSサーバソフトウェアは、デフォルトではインストールされません。NFSサーバソフトウェアをインストールするには、YaSTを起動してから、[ソフトウェア] > [ソフトウェア管理] の順に選択してください。次に [フィルタ] > [パターン] を選択して、[Misc. Server] を選択するか、または [検索] オプションを使って、NFS Serverを検索します。パッケージのインストールを確認して、インストールプロセスを完了します。

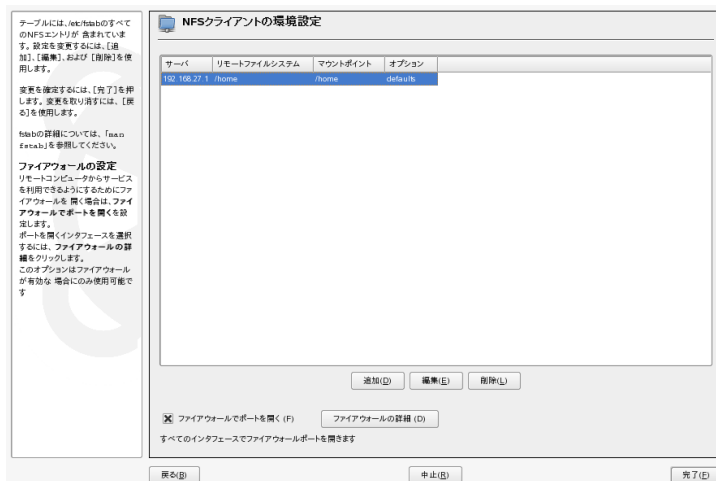
38.2 YaSTによるファイルシステムのインポート

適切な権限があれば、NFSディレクトリをNFSサーバから自分のファイルツリーにマウントできます。これには、YaSTの [NFSクライアント] モジュールを使用します。NFSサーバのホスト名、インポートするディレクトリ、およびこのディレクトリをマウントするマウントポイントを入力するだけです。最初のダイアログで [追加] をクリックすると、変更が反映されます。[Open Port in Firewall] をクリックしてファイアウォールを開き、リモートコンピュータからサービスにアクセスすることを許可します。チェックボックスの下には、ファイアウォールのステータスが表示されます。変更内容を保存するには、[完了] をクリックします。詳細については、[図 38.1. 「YaSTによるNFSクライアント設定」](#) (781 ページ)を参照してください。

設定は/etc/fstabに書かれ、指定されたファイルシステムがマウントされます。後でYaST設定クライアントを起動した時には、このファイルから既存の設定情報が取得されます。

現在の所、NFSv4ファイルシステムは手動でのみインポートできます。これについては、[38.3項 「ファイルシステムの手動インポート」](#) (781 ページ)で説明します。

☒ 38.1 YaSTによるNFSクライアント設定



38.3 ファイルシステムの手動インポート

ファイルシステムは、NFSサーバから手動でもインポートできます。唯一の前提条件はRPCを実行していることです。RPCを起動するにはrootユーザとして「rpcportmap start」と入力します。この前提条件を満たせば、エクスポートされたリモートファイルシステムを、ローカルのハードディスクと同じようにマウントすることができます。マウントするには、次のようにmountコマンドを使用します。

```
mount host:remote-path local-path
```

たとえば、sunコンピュータからユーザディレクトリをインポートする場合は、次のコマンドを使用します。

```
mount sun:/home /home
```

38.3.1 NFSv4ファイルシステムのインポート

NFSv4インポートを実行するには、クライアント上でidmapdサービスが動作していなければなりません。コマンドプロンプトからrcidmapd startと入力し、idmapdサービスを起動してください。idmapdのステータスを確認するには、rcidmapd statusを使用します。

idmapdサービスのパラメータは、/etc/idmapd.confファイルに格納されます。Domainパラメータの値は、localdomainのままにしてください。NFSクライアントとNFSクライアントの両方で、指定されている値が同じことを確認してください。

NFSv4インポートを実行するには、シェルプロンプトからコマンドを実行します。NFSv4ファイルシステムをインポートするには、次のコマンドを使用します。

```
mount -t nfs4 host:/ local-path
```

ここで、hostには1つまたは複数のNFSv4エクスポートを提供するNFSサーバ名を、local-pathにはこれをマウントするクライアントコンピュータ上のディレクトリを指定します。たとえば、sun上のNFSv4でエクスポートされた/homeを/local/homeにインポートするには、次のコマンドを使用します。

```
mount -t nfs4 sun:/ /local/home
```

サーバ名とコロンの続くリモートファイルシステムパススラッシュ(/)です。これは、リモートファイルシステムの正確なパスが必要だった、v3インポートとは異なります。この概念は、疑似ファイルシステムと呼ばれます。詳細は、[38.4.1項「NFSv4クライアント用のエクスポート」](#) (786 ページ)を参照してください。

38.3.2 自動マウントサービスの使用

通常のローカルデバイスをマウントする場合と同様に、autofsデーモンを使ってリモートファイルシステムを自動的にマウントすることもできます。そのためには、/etc/auto.masterファイルに次のエントリを追加してください。

```
/nfsmounts /etc/auto.nfs
```

これで、`/nfsmounts`ディレクトリがクライアント上のすべてのNFSマウントのルートディレクトリの役割を果たすようになります(`auto.nfs`ファイルが正しく設定されている場合)。ここでは、`auto.nfs`と言う名前を使用しましたが、任意の名前を選択することができます。選択したファイルに(存在しない場合はファイルを作成してください)、次の例のようにすべてのNFSマウントのエントリを追加します。

```
localdata -fstype=nfs server1:/data
nfs4mount -fstype=nfs4 server2:/
```

`rcautoofs start`を実行して、設定をアクティブにします。この例で、`server1`の`/data`ディレクトリの`/nfsmounts/localdata`は、NFSでマウントされ、`server2`の`/nfsmounts/nfs4mount`はNFSv4でマウントされます。

`autoofs`サービスの動作中に`/etc/auto.master`ファイルを編集した場合、変更内容を反映するには自動マウント機能を再起動する必要があります。再起動するには、`rcautoofs restart`を実行します。

38.3.3 /etc/fstabの手動編集

`/etc/fstab`中で、一般的なNFSマウントに関するエントリは次のようになっています。

```
host:/data /local/path nfs rw,noauto 0 0
```

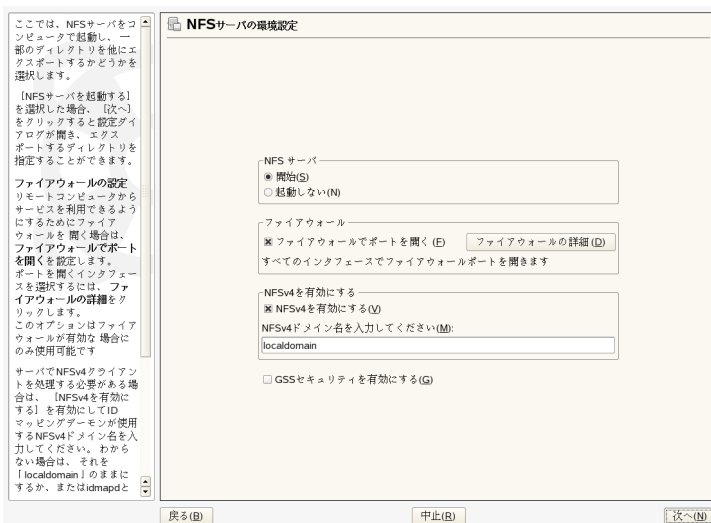
`/etc/fstab`ファイルにNFSv4マウントを手動で追加することもできます。この場合、3列目に`nfs`の代わりに`nfs4`を指定します。また、1列目の`host:`の後にリモートファイルシステムを/`として指定してください。この情報を``/etc/fstab`に保存すると、マウントするためのコマンドにローカルマウントポイントを指定するだけで済むという利点があります。次に例を示します。

```
mount /local/path
```

38.4 YaSTによるファイルシステムのエクスポート

YaSTを使用して、ネットワーク上のホストをNFSサーバに変更し、そのホストへのアクセスを許可されたすべてのホストに、ディレクトリやファイルをエクスポートすることができます。これにより、グループに属する全社員がそれぞれのホストにアプリケーションをローカルにインストールしなくても、全員にアプリケーションを提供できるようになります。NFSサーバをインストールするには、YaSTを起動して、[ネットワークサービス] > [NFSサーバ] の順に選択します。図 38.2. 「NFSサーバ設定ツール」 (784 ページ) に示すダイアログが開きます。

図 38.2 NFSサーバ設定ツール



次に [Start NFS Server] を実行して、[NFSv4 domain name] (NFSv4ドメイン名)を入力します。

サーバに安全にアクセスするには、[GSSセキュリティを有効にする] をクリックします。この機能を有効にする前提条件として、ドメインにKerberosがインストールされており、サーバとクライアントの両方でKerberosが有効になっていなければなりません。[Next]をクリックします。

上部のテキストフィールドに、エクスポートするディレクトリを入力します。下部に、それらのディレクトリへのアクセスを許可するホストを入力します。
図 38.3. 「YaSTを使ったNFSサーバの設定」 (785 ページ)に示すダイアログボックスが表示されます。この図は、前のダイアログでNFSv4を有効にしたシナリオを示しています。右側のペインには、Bindmountターゲットが表示されています。詳細は、左側のペインに表示されるヘルプを参照してください。ダイアログの下部には、各ホストに対して設定できる4種類のオプション single host、netgroups、wildcards、およびIP networksがあります。これらのオプションの詳細は、exportsマニュアルページを参照してください。 [完了] をクリックして設定を完了します。

図 38.3 YaSTを使ったNFSサーバの設定

上のボックスには、エクスポートするすべてのディレクトリが含まれます。ディレクトリを選択すると、このディレクトリをマウントできるホストが下のボックスに表示されます。

[ホストのワイルドカード] では、選択したディレクトリにアクセスできるホストを設定します。単一のホスト、グループワイルドカード、またはIPネットワークを指定できます。

アスタリクスを入力して、(*)すべてのホストを指定します。

前のページでNFSv4オプションが有効にされています。特定のクライアントに対しては、1つのエクスポートされたファイルシステムだけが「fsid=0」オプションでマークされていることを確認してください。

NFSv4クライアントへの複数エクスポートに備えて、エクスポート読み込みパス（fsid=0）でないパスを「fsid=0」のパスにバインドする必要があります。そのためには、エクスポートオプション「bind=/target/path」を追加します。ここで、/target/pathはfsid=0のエクスポート読み取り下にある既存のいくつかのディレクトリを参照します。

詳細については、「man exports」を参照してください。

エクスポートするディレクトリ

ディレクトリ	ターゲットをバインドマウント
/home	

ディレクトリの追加(A)編集(E)削除(L)

/home

ホストのワイルドカード (H)	オプション
*	fsid=0,ro,sync,root_squash

ホストの追加(H)編集(E)削除(L)

戻る(B)中止(S)完了(F)

重要項目: 自動ファイアウォール設定

システムでファイアウォール(SuSEfirewall2)が有効になっている場合に、
[ファイアウォールで開いているポート] を選択すると、YaSTは、nfsサービスを有効にすることでNFSサーバ用にファイアウォール設定を変更します。

38.4.1 NFSv4クライアント用のエクスポート

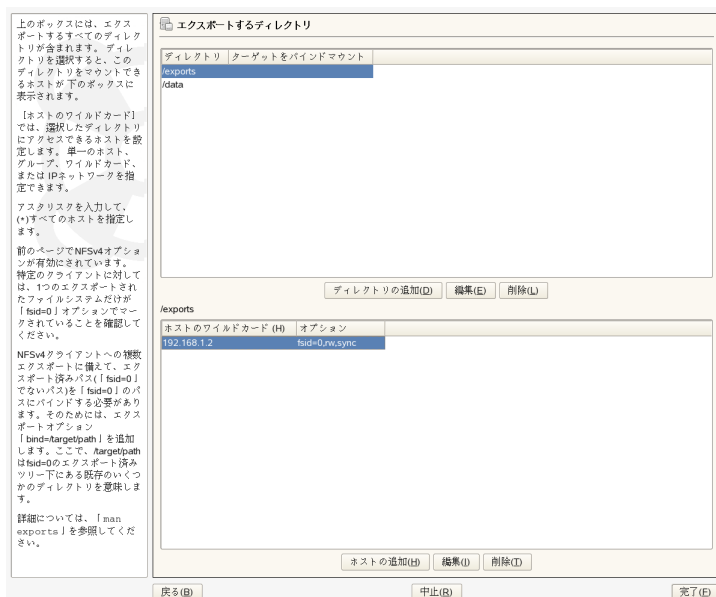
NFSv4クライアントをサポートするには、*[NFSv4を有効にする]* を有効にします。NFSv3クライアントも、引き続きサーバからエクスポートされています(適切にエクスポートされている場合)。この機能については、[38.4.3項「NFSv3エクスポートとNFSv4エクスポートの共存」](#) (789 ページ)で詳細に説明しています。

NFSv4を有効にしたら、適切なドメイン名を入力します。ここに入力する名前は、このサーバにアクセスするNFSv4クライアントの/etc/idmapd.confファイルに指定されている名前であればなりません。このパラメータは、NFSv4サポートに必要なidmapdサービスが使用します(サーバとクライアントの両方で)。特に必要のない限り、そのままlocaldomain(デフォルト)を使用してください。詳細については、[38.7項「詳細情報」](#) (794 ページ)を参照してください。

[次へ] をクリックします。次のダイアログには、2つのセクションがあります。上部のセクションには、*[Directories]* と *[Bind mount targets]* の2つの列があります。*[Directories]* には、エクスポートするディレクトリが表示されています。この列は、直接変更することができます。

クライアントに対してエクスポートできるディレクトリには、疑似rootファイルシステムの役割を果たすディレクトリと、疑似ファイルシステムのサブディレクトリにバインドされるディレクトリの2種類があります。疑似ファイルシステムは、同じクライアントに対してエクスポートされたすべてのファイルシステムをまとめる、ルートディレクトリの役割を果たします。クライアントに対しては、サーバ上の1つのディレクトリのみを、エクスポート用の疑似rootディレクトリとして設定できます。同じクライアントに対して複数のディレクトリをエクスポートするには、疑似root中の既存のサブディレクトリにこれらのディレクトリをバインドします。

図 38.4 NFSv4を使ったディレクトリのエクスポート



このダイアログの下部には、クライアントを入力し(ワイルドカード)、ディレクトリに対するエクスポートオプションを指定します。上部のセクションでディレクトリを追加すると、クライアントとオプションを入力するダイアログが自動的に表示されます。新しいクライアント(クライアントセット)を追加するには、[ホストの追加]をクリックします。

表示される小さなダイアログに、ホストを示すワイルドカードを入力してください。4種類の方法でホストを指定することができます。1台のホスト(名前またはIPアドレス)(single host)、ネットグループ(netgroups)、ワイルドカード(すべてのコンピュータがサーバにアクセスできることを示す*など)(wild cards)、およびIPネットワーク(IP networks)です。 [オプション] に、疑似rootにするディレクトリを設定する場合は、カンマ区切り形式のオプションリストにfsid=0を指定します。このディレクトリを、すでに疑似rootとして設定されているディレクトリ下のディレクトリにバインドする場合は、オプションリストにターゲットのバインドパスをbind=/target/pathの形式で指定します。

たとえば、サーバにアクセスするすべてのクライアントの疑似ディレクトリとして、/exportsを使用する場合を考えてみましょう。この場合、上部セ

クションでこのディレクトリを追加して、このディレクトリのオプションに `fsid=0` を指定します。別に `/data` ディレクトリも NFSv4 を使ってエクスポートする必要がある場合は、このディレクトリも上部のセクションに追加します。このディレクトリに関するオプションを設定する際には、リストに `bind=/exports/data` を指定します。また、`/exports/data` がすでに `/exports` の既存のサブディレクトリとなっていることを確認してください。オプション `bind=/target/path` に対する変更は(追加、削除、値の変更など)、`[Bindmount targets]` に反映されます。ディレクトリとその性質の概要を表示しているこの列は、直接編集することはできません。情報の入力が完了したら、`[完了]` をクリックして設定を終了します。サービスを再起動する場合は、`[開始]` をクリックしてください。

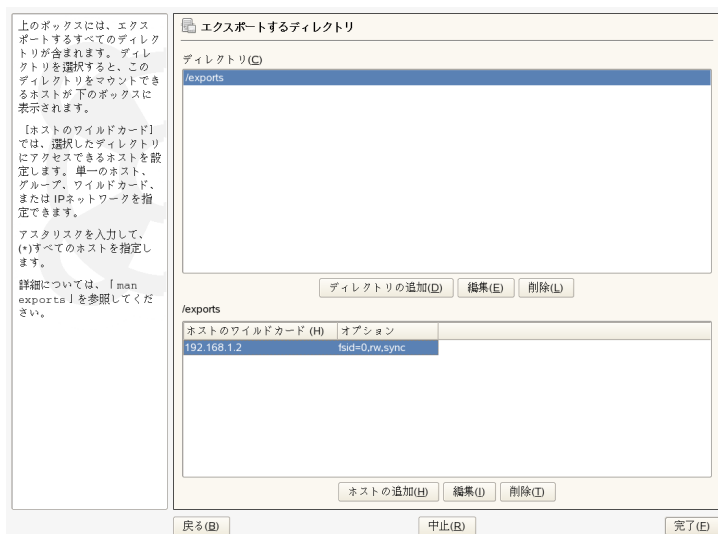
38.4.2 NFSv3およびNFSv2エクスポート

初期ダイアログで `[NFSv4を有効にする]` の選択が解除されていることを確認してから、`[次へ]` をクリックします。

次のダイアログは、2つの部分に分かれています。上部のテキストフィールドに、エクスポートするディレクトリを入力します。下部に、それらのディレクトリへのアクセスを許可するホストを入力します。4種類の方法でホストを指定することができます。1台のホスト(名前またはIPアドレス)(single host)、ネットグループ(netgroups)、ワイルドカード(すべてのコンピュータがサーバにアクセスできることを示す*など)(wild cards)、およびIPネットワーク(IP networks)です。

に示すダイアログボックスが表示されます。図 38.4. 「NFSv4を使ったディレクトリのエクスポート」 (787 ページ)これらのオプションの詳細は、`man exports` を実行して表示される、マニュアルページを参照してください。 `[完了]` をクリックして設定を完了します。

図 38.5 NFSv2およびNFSv3を使ったディレクトリのエクスポート



38.4.3 NFSv3エクスポートとNFSv4エクスポートの共存

1台のサーバ上に、NFSv3エクスポートとNFSv4エクスポートの両方を共存させることができます。初期設定ダイアログでNFSv4サポートを有効にすると、オプションリストに`fsid=0`と`bind=/target/path`が指定されていないエクスポートは、NFSv3エクスポートとみなされます。図 38.4. 「NFSv4を使ったディレクトリのエクスポート」 (787 ページ)の例を参考に説明します。[ディレクトリの追加] を使って、`/data2`ディレクトリを追加したけれども、そのオプションに`fsid=0`や`bind=/target/path`を指定しなかった場合、このエクスポートはNFSv3エクスポートとして処理されます。

重要項目

自動ファイアウォール設定

システムでSuSEfirewall2が有効になっている場合に、[ファイアウォールで開いているポート]を選択すると、YaSTは、サービスを有効にすることでNFSサーバ用にファイアウォール設定を変更します。2

38.5 ファイルシステムの手動エクスポート

NFSエクスポートサービスの環境設定ファイルは、`/etc/exports`と`/etc/sysconfig/nfs`です。NFSv4サーバ環境設定には、これらのファイルに加えて`/etc/idmapd.conf`も必要です。サービスを起動または再起動するには、コマンド`rcnfsserver restart`と`rcidmapd restart`を実行します。NFSサーバは、RPCポートマッパーに依存しています。そのため、`rcportmap restart`コマンドを実行して、ポートマッパーサービスも起動/再起動してください。

38.5.1 NFSv4を使ったファイルシステムのエクスポート

NFSv4は、SUSE Linux Enterprise 10で利用できる最新版のNFSプロトコルです。NFSv4でエクスポートするディレクトリの設定方法は、前のバージョンと多少異なっています。

`/etc/exports`ファイル

このファイルには、一連のエントリが含まれています。各エントリはそれぞれ共有するディレクトリと共有方法を示します。`/etc/exports`中の一般的なエントリは、次の項目から成り立っています。

```
/shared/directory host(option_list)
```

たとえば、次のような指定内容です。

```
/export 192.168.1.2(rw,fsid=0,sync)
/data 192.168.1.2(rw,bind=/export/data,sync)
```

オプションリストで`fsid=0`が指定されているディレクトリは、疑似rootファイルシステムと呼ばれます。ここでは、IPアドレス192.168.1.2が使われています。ホスト名、ホスト名を表すワイルドカード、または`(*.abc.comや*など)` ネットグループを使用できます。

クライアントに対してNFSv4エクスポートできるディレクトリには、次の2種類しかありません。

- 疑似rootディレクトリとして指定するディレクトリ(1つ)。この例では、/exportsが疑似rootディレクトリになります。疑似rootディレクトリのオプションリストには、fsid=0が指定されています。
- 疑似ファイルシステム中の既存のサブディレクトリにバインドするディレクトリ。上記の例では、/dataがこれにあたります。このディレクトリは、疑似ファイルシステム/export中の既存のサブディレクトリ(/export/data)にバインドされています。.

疑似ファイルシステムは最上位のディレクトリで、このディレクトリ下にNFSv4エクスポートするすべてのファイルシステムがハイチされます。クライアントに対しては、サーバ上の1つのディレクトリだけが、エクスポート用の疑似rootディレクトリとして設定できます。この同じクライアントまたはクライアントセットに対して、他の複数のディレクトリをエクスポートするには、疑似root下にある既存のサブディレクトリにバインドします。

/etc/sysconfig/nfs

このファイルには、NFSv4サーバデーモンの動作を示すパラメータが含まれています。NFSv4_SUPPORTパラメータは、yesに設定する必要があります。このパラメータは、NFSサーバがNFSv4エクスポートとクライアントをサポートするかどうかを決定します。

/etc/ldapd.conf

Linuxコンピュータ上の各ユーザには、ユーザ名とIDがあります。ldapdは、サーバへのNFSv4リクエストやクライアントへのNFSv4応答用に、名前とID間のマッピングサービスを提供しています。NFSv4は通信中で名前のみを使用するため、NFSv4のサーバとクライアントの両方でldapdが動作していなければなりません。

NFSを使ってファイルシステムを共有するコンピュータ間では、ユーザへのユーザ名とID(uid)の割り当てには同じ方法を使用してください。そのためには、NIS、LDAP、または他の同一ドメイン認証機構を利用することができます。

正常に機能するために、このファイル中のDomainパラメータには、クライアント側とサーバ側の両方で同じ値を設定する必要があります。よくわからない場合には、クライアントとサーバの両方のファイルでそのままlocaldomainを使用してください。環境設定ファイルの例を次に示します。

```
[General]

Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]

Nobody-User = nobody
Nobody-Group = nobody
```

パラメータの意味を理解していない場合は、これらのパラメータを変更しないでください。詳細は、idmapdとidmapd.confのマニュアルページを参照してください。参照するには、man idmapd、man idmapd.confを実行します。

Servicesの起動と停止

/etc/exportsまたは/etc/sysconfig/nfsを変更したら、rcnfsserver restartコマンドを実行して、NFSサーバサービスを起動/再起動します。
/etc/idmapd.confを変更したら、rcidmapd restartコマンドを実行して、idmapdサービスを起動/再起動します。両方のサービスが動作していることを確認してください。

38.5.2 NFSv2とNFSv3を使ったファイルシステムのエクスポート

ここでは、NFSv2エクスポートとNFSv3エクスポート固有の話題を取り上げます。NFSv4エクスポートについては、「[38.5.1項「NFSv4を使ったファイルシステムのエクスポート」](#) (790 ページ)」を参照してください。

NFSを使ってファイルシステムをエクスポートする場合、/etc/exportsと/etc/sysconfig/nfsの2つの環境設定ファイルが関わってきます。一般的な/etc/exportsファイルには、各エントリが次のような形式で指定されています。

```
/shared/directory host(list_of_options)
```

たとえば、次のような指定内容です。

```
/export 192.168.1.2(rw, sync)
```

ここで、/exportディレクトリはホスト 192.168.1.2と共有されています。オプションリストには、rw, syncが設定されています。このIPアドレスは、特定のクライアント名、ワイルドカードを使った複数のクライアント(*.abc.com など)、またはネットグループに置換することができます。

各オプションの詳細とその意味については、exportsのマニュアルページ(man exports)を参照してください。

/etc/exportsまたは/etc/sysconfig/nfsを変更したら、rcnfsserver restartコマンドを実行して、NFSサーバを起動/再起動します。

38.6 NFSでのKerberosの使用

NFSでKerberos認証を使用するには、GSSセキュリティを有効にする必要があります。有効にするには、YaSTの初期ダイアログで *[GSSセキュリティを有効にする]* を選択します。また、以下の作業を行ってください。

- サーバとクライアントの両方が、同じKerberosドメインにあることを確認します。つまり、クライアントとサーバが同じKDC(Key Distribution Center)サーバにアクセスし、krb5.keytabファイル(the default location on any machine is /etc/krb5.keytab)を共有していなければなりません。
- クライアントでrcgssd startコマンドを実行して、gssdサービスを開始します。
- サーバでrcsvcgssd startコマンドを実行して、svcgssdサービスを開始します。

NFSでのKerberosの設定の詳細は、[38.7頁「詳細情報」](#) (794 ページ)を参照してください。

38.7 詳細情報

NFSサーバ/クライアントの環境設定の詳細は、`exports`、`nfs`、および`mount`のマニュアルページや、`/usr/share/doc/packages/nfs-tls/README`、およびこれらのWebドキュメントを参照してください。

また、SourceForge [<http://nfs.sourceforge.net/>]にも技術ドキュメントが用意されています。

NFSでのKerberosの設定方法は、「NFS Version 4 Open Source Reference Implementation [<http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html>]

」には、NFSv4に関するFAQが用意されています。

ファイルの同期

今日、多くの人々が複数のコンピュータを使用しています。自宅に1台、職場に1台またはそれ以上、外出時にラップトップやPDAを携帯することも珍しくありません。これらすべてのコンピュータには、多くのファイルが必要です。どのコンピュータでも作業して、ファイルを変更した後は、すべてのコンピュータで最新バージョンを使用したいと考えるでしょう。

39.1 使用可能なデータ同期ソフトウェア

データの同期は、高速ネットワークで固定接続されているコンピュータ間ではまったく問題なく実現できます。この場合、NFSなどのネットワークファイルシステムを使用し、ファイルをサーバに保存して、すべてのホストがネットワーク経由で同じデータにアクセスすればよいわけです。ところがこの方法は、ネットワーク接続が低速な場合、または固定でない場合には不可能です。ラップトップをもって外出しているとき、必要なファイルをローカルハードディスクにコピーする必要があります。しかし、そうすると今度は、変更したファイルを同期させる必要があります。1台のコンピュータでファイルを変更したときは、必ず他のすべてのコンピュータでファイルを更新しなければなりません。たまにコピーする程度なら、手動で`scp`または`rsync`を使用してコピーすればよいでしょう。しかし、ファイルが多い場合、手順が複雑になるだけでなく、新しいファイルを古いファイルで上書きしてしまうといった間違いを防ぐために細心の注意が必要になります。

警告: データ損失の危険

データを同期システムで管理する前に、使用するプログラムをよく理解し、機能をテストしておく必要があります。重要なファイルのバックアップは不可欠です。

このように手動によるデータの同期は、時間がかかる上に間違いが起こりやすい作業ですが、この作業を自動化するためのさまざまな方法を採用したプログラムを使用することで手動による作業は行わずに済みます。ここでの説明は、このようなプログラムの仕組みと使用法について、一般的な理解を図ることを目的としています。実際に使用する場合は、プログラムのマニュアルを参照してください。

39.1.1 CVS

CVSは、多くの場合プログラムソースのバージョン管理に使用されるプログラムで、複数のコンピュータでファイルのコピーを保存する機能を持っています。したがって、データ同期にも適しています。CVSはサーバ上に一元的なリポジトリを設定し、ファイルおよびファイルの変更内容を保存します。ローカルに実行された変更はリポジトリにコミットされ、更新によって他のコンピュータに取得されます。両方の処理はユーザによって実行される必要があります。

CVSは、複数のコンピュータで変更が行われた場合、非常に優れたエラー回復力を発揮します。変更内容がマージされ、同じ行が変更された場合は、競合がレポートされます。競合が生じてでも、データベースは一貫した状態のままです。競合はクライアントホストで解決するためにのみ表示されます。

39.1.2 rsync

バージョン管理は不要であっても、低速ネットワーク接続を使用して大きなディレクトリ構造を同期させる必要がある場合は、ツールrsyncの適切に開発されたメカニズムを使用して、ファイル内の変更箇所のみを送信できます。この処理では、テキストファイルのみでなくバイナリファイルも対象となります。ファイル間の差分を検出するために、rsyncはファイルをブロック単位で分割してチェックサムを計算します。

変更内容の検出処理は高コストを伴います。`rsync`の使用量に合わせて、同期対象となるシステムの規模を調整する必要があります。特に、RAMが重要です。

39.2 プログラムを選択する場合の決定要因

使用するプログラムを決定する際に重要な要因がいくつかあります。

39.2.1 クライアントサーバか、ピアツーピアか

一般に、データの配信には2種類のモデルが使用されます。1つは、すべてのクライアントが、そのファイルを一元的なサーバによって同期させるモデルです。サーバはすべてのクライアントから、少なくともいずれかの時点でアクセスする必要があります。このモデルは、CVSが使用します。

もう1つは、すべてのネットワークホストがそれぞれのデータをピアとして相互に同期させるモデルです。`rsync`は、実際にクライアントモードで動作しますが、任意のクライアントがサーバとして動作できます。

39.2.2 移植性

CVS、および`rsync`は、各種のUNIXおよびWindowsシステムなど、他の多くのオペレーティングシステムでも使用できます。

39.2.3 インタラクティブと自動制御

CVSでは、ユーザが手動によってデータの同期を開始します。これにより、データの同期を詳細に制御でき、競合の処理も容易です。ただし、同期の間隔が長すぎると、競合が起こりやすくなります。

39.2.4 競合:問題と解決策

複数のユーザが大きなプログラミングプロジェクトにかかわっている場合も、CVSでは、競合はまれにしか発生しません。これはドキュメントが個別の行単位でマージされるためです。競合が起これば、影響を受けるのは1台のクライアントだけです。CVSでは、通常、競合が容易に解決できます。

rsyncには、競合処理の機能はありません。ユーザは、意図せずにファイルを上書きしないように注意し、考えられる競合はすべて手動で解決する必要があります。安全のために、RCSなどのバージョンングシステムを追加採用できます。

39.2.5 ファイルの選択と追加

CVSでは、新しいディレクトリやファイルは、コマンド`cvs add`を使って明示的に追加する必要があります。これにより、同期の対象となるファイルについて、ユーザがより詳細に制御できます。しかし他方で、新しいファイルが見過ごされることが多く、特に`cvs update`の出力に表示される疑問符は、ファイルの数が多いためにたびたび無視されます。

39.2.6 履歴

CVSは追加機能として、古いバージョンのファイルが再構成できます。変更を行うたびに簡単な編集コメントを挿入しておくことで、内容とコメントからファイルの作成状況を後で簡単に追跡できます。これは論文やプログラムテキストを作成する際、貴重な支援となります。

39.2.7 データ量と必要なハードディスク容量

同期の対象となるすべてのホストには、分散されたデータを処理できるだけの十分なハードディスクの空き容量が必要です。CVSでは、サーバ上のリポジトリデータベースに余分な容量が必要となります。ファイルの履歴もサーバに保存されるため、このための容量も別に必要です。テキスト形式のファイルが変更されたときには、変更された行だけを保存すれば足ります。バイナリファイルは、ファイルが変更されるたびに、ファイルのサイズと同じだけの容量が必要なため、テキストより必要な容量が多くなります。

39.2.8 GUI

CVSを使い慣れたユーザは、通常、コマンドラインでプログラムを制御します。しかし、*cervisia*のようなLinux用のグラフィカルユーザインタフェースがあり、また他のオペレーティングシステム用に*wincvs*なども用意されています。*kdevelop*などの開発ツールや*Emacs*などのテキストエディタの多くが、CVSをサポートしています。競合の解決は、これらのフロントエンドの方が、はるかに容易です。

39.2.9 使いやすさ

*rsync*は、より使いやすく初心者向けです。CVSは、より操作が難しくなっています。ユーザはレポジトリとローカルデータの間のインタラクションを理解する必要があります。データを変更すると、最初にローカルでレポジトリとマージする必要があります。これはコマンド*cvcs*または*update*で実行します。次にコマンド*cvcs*または*commit*でデータをレポジトリに送信する必要があります。この手順をいったん理解すれば、初心者の方でもCVSを簡単に利用できるようになります。

39.2.10 攻撃に備えるセキュリティ

伝送中、データは妨害や改ざんから保護される必要があります。CVSや*rsync*はいずれも*ssh*(セキュアシェル)経由で容易に使用できるため、この種の攻撃からセキュリティ保護されます。CVSを*rsh*(リモートシェル)経由で実行するのは避けるべきです。また、安全でないネットワークで*pserver*メカニズムを使用してCVSにアクセスすることもお勧めできません。

39.2.11 データ損失からの保護

CVSは、プログラミングプロジェクト管理のため長期間にわたって開発者に使用されてきたため、きわめて安定しています。CVSでは開発履歴が保存されるため、誤ってファイルを削除するといったユーザの誤操作にも対応できます。

表 39.1 ファイル同期化ツールの機能: -- = とても悪い、- = 悪い、または利用不可、o = 普通、+ = 良好、++ = とても良好、x = 利用可能

	CVS	rsync
クライアント/サーバ	C-S	C-S
移植性	Lin、Un*x、Win	Lin、Un*x、Win
対話処理	x	x
Speed	o	+
競合	++	o
ファイル選択	Sel./file, dir.	ディレクトリ
履歴	x	-
ハードディスクスペース	--	o
GUI	o	-
難度	o	+
攻撃	+(ssh)	+(ssh)
データ損失	++	+

39.3 CVSの概要

CVSは、個々のファイルが頻繁に編集され、ASCIIテキストやプログラムソーステキストのようなファイル形式で保存される場合の同期に適しています。CVSを使用して他の形式、たとえばJPEGファイルのデータを同期させることは可能ですが、データ量が膨大になるとともに、生成される数多くのファイルをCVSサーバに恒久的に保存する必要があります。このような場合、CVSの機能のほとんどが利用できません。CVSを使用したファイルの同期は、すべてのワークステーションが同じサーバにアクセスできる場合のみ可能です。

39.3.1 CVSサーバの設定

サーバとは、すべてのファイルの最新バージョンを含め、有効なファイルが配置されるホストです。固定のワークステーションであれば、どれでもサーバとして使用できます。可能であれば、CVSレポジトリのデータを定期バックアップに含めます。

CVSサーバを設定するとき、できればユーザアクセスをSSH経由で許可します。ユーザがサーバにtuxとして認識され、CVSソフトウェアがサーバとクライアントにインストールされている場合、次の環境変数をクライアント側に設定する必要があります。

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

コマンドcvsinitを使用して、クライアント側からCVSサーバを初期化します。これは一度だけ実行すれば、後は必要ありません。

最後に、同期に名前を付ける必要があります。クライアント上で、CVSで管理するファイル専用のディレクトリ(空のディレクトリ)を選択するか作成します。ディレクトリには、同期用の名前を付けます。この例で、ディレクトリ名はsynchomeです。このディレクトリに移動し、次のコマンドを入力して、同期名をsynchomeと設定します。

```
cvs import synchome tux wilber
```

CVSの多くはコメントが必要です。このため、CVSはエディタを起動します(環境変数\$EDITORで定義されたエディタか、エディタが定義されていない場合はvi)。事前に次の例のようなコマンドラインにコメントを入力しておけば、エディタ呼び出しが避けられます。

```
cvs import -m 'this is a test' synchome tux wilber
```

39.3.2 CVSの使用

これで、すべてのホストが`cvsco synchome`を使用して同期レポジトリからチェックアウトできます。これにより、クライアントに新しいサブディレクトリ`synchome`が作成されます。変更内容をサーバにコミットするには、ディレクトリ`synchome`(またはそのサブディレクトリ)に移動し、「`cvs commit`」と入力します。

デフォルトでは、すべてのファイル(サブディレクトリを含め)がサーバにコミットされます。個別のファイルまたはディレクトリだけをコミットするには、`cvs commit file1 directory1`のように指定します。新しいファイルとディレクトリは、サーバにコミットする前に、`cvs add file1 directory1`のようなコマンドを使用してレポジトリに追加する必要があります。この後、`cvs commit file1 directory1`を実行して、新しく追加したファイルとディレクトリをコミットします。

他のワークステーションに移動する場合、同じワークステーションの以前のセッションで同期レポジトリからチェックアウトしていない場合は、ここでチェックアウトします。

サーバとの同期は、`cvs update`を使用して起動します。`cvs update file1 directory1`を使用すると、ファイルやディレクトリを個別に更新できます。現行のファイルとサーバに格納されているバージョンとの違いを確認するには、コマンド`cvs diff`または`cvs diff file1 directory1`を使用します。更新によって変更されたファイルを確認する場合は、`cvs -nq update`を使用します。

更新時に表示されるステータス記号の例を次に示します。

U

ローカルバージョンが更新されました。この更新はサーバが提供しているすべてのファイル、およびローカルにシステムに存在しないすべてのファイルに影響します。

M

ローカルバージョンが変更されました。サーバ上で変更があれば、その差分がローカルコピーに取り込まれていることがあります。

P

ローカルバージョンに対し、サーバ上のバージョンからパッチが適用されました。

C

ローカルファイルが、レポジトリの現在のバージョンと競合しています。

?

このファイルがCVSに存在しません。

ステータスMは、ローカルで変更されたファイルを示します。ローカルコピーをサーバにコミットするか、ローカルファイルを削除して更新を再実行します。この場合、不足しているファイルは、サーバから取得されます。ローカルに変更したファイルをコミットしたが、そのファイルで同じ行に変更があり以前にコミットされている場合は、競合がCで示されて表示されることがあります。

この場合、ファイルの競合マーク(>と<)を確認し、2つのバージョンのどちらを採用するかを決定します。これは厄介な作業のため、変更を破棄し、ローカルファイルを削除して「cvs up」と入力し、現在のバージョンをサーバから取得することもできます。

39.3.3 詳細情報

ここでは、CVSが持つ多くの機能から、その概要だけを紹介しました。詳細については、多数のマニュアルが次のURLに用意されています。

- CVS: <http://www.cvshome.org>
- rsync: <http://www.gnu.org/manual>

39.4 rsyncの概要

rsyncは、大量のデータを定期的に変送する必要があるが、変更量はあまり多くない場合に便利だ。たとえば、バックアップの作成時などが該当します。もう1つのアプリケーションはステージングサーバに関係します。この種のサーバには、DMZでWebサーバに定期的にミラー化されるWebサーバの完全なディレクトリツリーが格納されます。

39.4.1 設定と操作

`rsync`には2つの操作モードがあります。このプログラムを使用してデータをアーカイブまたはコピーできます。そのためには、ターゲットシステム上に `ssh`などのリモートシェルがあれば十分です。ただし、`rsync`を `daemon`として使用し、ネットワークにディレクトリを提供することもできます。

`rsync` の基本操作モードの場合、特別な設定は不要です。 `rsync` では、ディレクトリ全体を別のシステムに直接ミラー化できます。たとえば、次のコマンドでは、`tux`のホームディレクトリのバックアップがバックアップサーバ `sun`上に作成されます。

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

次のコマンドは、ディレクトリを復元する場合に使用します。

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

ここまでの操作は、`scp`のような通常のコピーツールの場合とほぼ同じです。

「`rsync`」のすべての機能を完全に使用可能にするには、「`rsync`」モードで操作する必要があります。そのためには、いずれかのシステムで `rsyncd`デーモンを起動します。設定はファイル `/etc/rsyncd.conf`内で行います。たとえば、`rsync`でディレクトリ `/srv/ftp`を使用可能にするには、次の設定を使用します。

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log
```

```
[FTP]
    path = /srv/ftp
    comment = An Example
```

次に、`rcrsyncdstart`を使用して `rsyncd`を起動します。また、ブート処理中に `rsyncd`を自動的に起動する方法もあります。このようにセットアップするに

は、このサービスをYaSTのランラベルエディタで有効にするか、またはコマンド`insservrsyncd`を入力します。かわりに、`xinetd`から`rsyncd`を起動することもできます。ただし、この方法は`rsyncd`の使用頻度が低いサーバの場合にのみ使用してください。

この例では、すべての接続を示すログファイルも作成されます。このファイルは`/var/log/rsyncd.log`に格納されます。

これで、クライアントシステムからの転送をテストできます。そのためには次のコマンドを使用します。

```
rsync -avz sun::FTP
```

このコマンドを入力すると、サーバのディレクトリ`/srv/ftp`にあるファイルがすべてリストされます。このリクエストはログファイル`/var/log/rsyncd.log`にも記録されます。実際の転送を開始するには、ターゲットディレクトリを指定します。現在のディレクトリには`..`を使用してください。たとえば、次のようにします。

```
rsync -avz sun::FTP .
```

デフォルトでは、`rsync`での同期中にファイルは削除されません。ファイルを削除する必要がある場合は、オプション`--delete`を追加してください。新しい方のファイルが削除されないように、代わりにオプション`--update`を使用することもできます。競合が発生した場合は、手動で解決する必要があります。

39.4.2 詳細情報

`rsync`に関する重要な情報は、マニュアルページ`manrsync`および`manrsyncd.conf`を参照してください。`rsync`の基本原則に関する技術情報については、`/usr/share/doc/packages/rsync/tech_report.ps`を参照してください。`rsync`の最新ニュースについては、このプロジェクトのWebサイト<http://rsync.samba.org/>を参照してください。

Subversionまたは他のツールが必要な場合は、SDKをダウンロードしてください。「OpenLDAP Faq-O-Matic」は、http://developer.novell.com/wiki/index.php/SUSE_LINUX_SDKにあります。

Apache HTTPサーバ

Apache HTTPサーバ(Apache)は、世界で70%を超える市場シェアを持つ、最も広く利用されているWebサーバです(<http://www.netcraft.com/>の調査)。Apacheは、Apache Software Foundation (<http://www.apache.org/>)により開発され、ほとんどのオペレーティングシステムに対応しています。SUSE® Linux Enterprise Serverには、Apache version 2.2が付属しています。この章では、Webサーバのインストール、設定、セットアップ方法、SSL、CGI、その他のモジュールの使用方法、およびApacheのトラブルシューティング方法について説明します。

40.1 クイックスタート

このセクションでは、Apacheを迅速に設定し、起動します。タイム. Apacheは、rootとしてインストールし、設定する必要があります。

40.1.1 要件

Apache Webサーバをセットアップする前に、次の必要条件を満たしていることを確認してください。

1. マシンのネットワークが適切に設定されているか。この項目の詳細については、[第30章 ネットワークの基礎](#)(597 ページ)を参照してください。

2. マシンの正確なシステム時間は、タイムサーバとの同期により維持されます。これは、HTTPプロトコルの一部が正確な時間に依存するために必要です。この項目の詳細については、[第32章NTPによる時刻の同期](#)(667 ページ)を参照してください。
3. 最新のセキュリティアップデートがインストールされています。不明な場合は、YaSTオンラインアップデートを実行します。
4. ファイアウォールで、デフォルトのWebサーバポート(ポート80)が開いています。ポートを開くには、SUSEFirewall2を設定して外部ゾーンでHTTPサーバサービスを実行できるようにします。これは、YaSTを使用して行います。詳細については、[43.4.1項「YaSTを使ったファイアウォールの設定」](#) (900 ページ)を参照してください。

40.1.2 インストール

SUSE Linux Enterprise ServerのApacheは、デフォルトではインストールされません。このアプリケーションをインストールするには、YaSTを起動し、[ソフトウェア] > [ソフトウェアの管理] の順に選択します。次に、[フィルタ] > [パターン] の順に選択し、[基本機能] の下にある [WebおよびLAMPサーバ] を選択します。依存関係のあるパッケージのインストールを確認して、インストールプロセスを完了します。

Apacheは、「そのまま」実行できるように事前定義された標準設定でインストールされます。このインストールには、マルチプロセッシングモジュールのapache2-preforkおよびPHP5モジュールが含まれています。モジュールの詳細については、[40.4項「モジュールのインストール、有効化および設定」](#) (826 ページ)を参照してください。

40.1.3 開始

システムのブート時に自動的にapacheが起動されるようにするには、YaSTを起動し、[システム] > [システムサービス(ランレベル)] の順に選択します。サービスの [apache2] および [有効] を検索します。Webサーバがすぐに起動します。[完了] を選択して変更を保存することにより、システムのブート時にランレベル 3と 5でApacheが自動的に起動するように設定されます。SUSE Linux Enterprise Serverでのランレベルの詳細について、およびYaST

ランレベルエディタについての説明は、[20.2.3項「YaSTでのシステムサービス\(ランレベル\)の設定」](#) (440 ページ)を参照してください。

シェルを使用してApacheを起動するには、`rcapache2 start`を実行します。システムのブート時にランレベル3と5でApacheが自動的に起動されるようにするには、`chkconfig -a apache2`を使用します。

Apacheの起動時にエラーメッセージが表示されない場合、Webサーバは現在動作しています。ブラウザを起動し、<http://localhost/>を開きます。Apacheテストページに「If you can see this, it means that the installation of the Apache Web server software on this system was successful.というメッセージが表示されます。」このページが表示されない場合は、[40.8項「トラブルシューティング」](#) (846 ページ)を参照してください。

Webサーバの起動後は、ドキュメントを追加、必要に応じて設定を調整、およびモジュールをインストールして機能を追加することができます。

40.2 Apacheの設定

SUSE Linux Enterprise ServerのApacheは、YaSTを使って、または手動で環境設定を行うことができます。手動で設定を行えば細かい点まで調整できますが、YaSTのGUIほど便利ではありません。

重要項目: 設定の変更

Apacheの大部分の設定を変更した場合、Apacheを再起動または再ロードしないと変更が有効になりません。これは、YaSTで設定を完了し、`[HTTP Service]`で`[有効にする]`をオンにすると、自動的に行われます。手動での再起動については、[40.3項「Apacheの起動および停止」](#) (824 ページ)を参照してください。ほとんどの設定の変更は、`rcapache2 reload`を実行して再ロードすれば有効になります。

40.2.1 Apacheを手動で設定する

Apacheを手動で設定するには、rootユーザとしてブレンテキストの設定ファイルを編集する必要があります。

環境設定ファイル

Apache設定ファイルは、次の2つの場所にあります。

- /etc/sysconfig/apache2
- /etc/apache2/

/etc/sysconfig/apache2

/etc/sysconfig/apache2は、ロードするモジュール、インクルードする付加的な設定ファイル、サーバを起動するときのフラグ、コマンドラインに追加すべきフラグなど、Apacheのいくつかのグローバル設定を制御します。このファイルの各設定オプションについては、詳細なドキュメントが存在するので、ここでは説明しません。一般的な目的のWebサーバの場合には、/etc/sysconfig/apache2の内容を設定するだけで十分でしょう。

/etc/apache2/

/etc/apache2/には、Apacheのすべての設定ファイルが含まれます。ここでは、各ファイルの目的について説明します。各ファイルには、複数の設定オプション(ディレクティブ)が含まれています。これらのファイルの各設定オプションについては、詳細なドキュメントがあるので、ここでは説明しません。

Apache設定ファイルは、次のように編成されます。

```
/etc/apache2/  
|  
|- charset.conv  
|- conf.d/  
|   |  
|   |- *.conf  
|  
|- default-server.conf  
|- errors.conf  
|- httpd.conf  
|- listen.conf  
|- magic  
|- mime.types  
|- mod_*.conf  
|- server-tuning.conf  
|- ssl.*  
|- ssl-global.conf
```



```
| - sysconfig.d
|   |
|   | - global.conf
|   | - include.conf
|   | - loadmodule.conf . .
|
| - uid.conf
| - vhosts.d
|   | - *.conf
```

「etc/apache2」内のApache設定ファイル

charset.conf

各言語に使用する文字セットを指定します。編集しません。

conf.d/*.conf

他のモジュールによって追加される設定ファイル。これらの設定ファイルは、必要に応じて仮想ホスト設定に含めることができます。その例として、vhosts.d/vhost.templateを参照してください。設定ファイルを仮想ホスト設定に含めることにより、仮想ホストごとに別のモジュールセットを指定できます。

default-server.conf

すべての仮想ホストに対応するグローバル設定で、それぞれ適切なデフォルト値が指定されています。デフォルト値を変更する代わりに、仮想ホスト設定で上書きします。

errors.conf

Apacheによるエラーの対処方法を定義します。すべての仮想ホストに対してこれらのメッセージをカスタマイズするには、このファイルを編集します。カスタマイズしない場合は、仮想ホスト設定内のこれらのディレクトィブを上書きします。

httpd.conf

メインのApacheサーバ設定ファイル。このファイルは変更しません。この設定ファイルは、インクルード文およびグローバル設定が含まれています。ここに記載されている各設定ファイルのグローバル設定を上書きします。仮想ホスト設定内のホスト固有の設定(ドキュメントルートなど)を変更します。

`listen.conf`

Apacheを特定のIPアドレスおよびポートにバインドします。名前ベースの仮想ホスト([名前ベースの仮想ホスト項 \(814 ページ\)](#))を参照してください)もこのファイルで設定されます。

`magic`

Apacheが自動的に不明なファイルのMIMEタイプを判別できるようにする `mime_magic` モジュール用のデータ。変更しません。

`mime.types`

システムで認識されるMIMEタイプ(実際には `/etc/mime.types` へのリンク)。編集しません。このリスト以外にMIMEタイプを追加する必要がある場合は、`mod_mime-defaults.conf` に追加します。

`mod_*.conf`

デフォルトでインストールされるモジュール用の設定ファイル。詳細については、[40.4 項「モジュールのインストール、有効化および設定」 \(826 ページ\)](#)を参照してください。オプションのモジュール用の設定ファイルは、`conf.d` ディレクトリ内にあります。

`server-tuning.conf`

各MPMの設定ディレクティブ([40.4.4 項「マルチプロセッシングモジュール」 \(831 ページ\)](#))を参照)、およびApacheのパフォーマンスを制御する一般的な設定オプションが含まれています。このファイルを変更する場合は、Webサーバを適切にテストしてください。

`ssl-global.conf` and `ssl.*`

グローバルSSL設定およびSSL証明書データ。詳細については、[40.6 項「SSLをサポートするセキュアWebサーバのセットアップ」 \(838 ページ\)](#)を参照してください。

`sysconfig.d/*.conf`

`/etc/sysconfig/apache2` から自動的に生成される設定ファイル。これらのファイルは、いずれも変更しません。その代わりに、`/etc/sysconfig/apache2` を編集します。このディレクトリには、他の設定ファイルを配置しません。

uid.conf

Apacheを実行する際に使用するユーザおよびグループIDを指定します。
変更しません。

vhosts.d/*.conf

仮想ホスト設定は、ここに含めます。このディレクトリには、SSLを持つ、持たないに関係なく、仮想ホストのテンプレートファイルが含まれます。このディレクトリ内の.confで終わるファイルは、すべて自動的にApache設定に含まれます。詳細については、[仮想ホスト設定項](#) (813 ページ)を参照してください。

仮想ホスト設定

仮想ホストという用語は、同じ物理マシンで複数のURI (universal resource identifiers)のサービスを行えるApacheの機能を指しています。これは、たとえばwww.example.comやwww.example.netのような複数のドメインが、1台の物理コンピュータ上で動作する単一のWebサーバで処理されていることを表します。

管理の手間(1つのWebサーバを維持すればよい)とハードウェアの費用(ドメインごとの専用のサーバを必要としない)を省くために仮想ホストを使うことは、よく行われています。仮想ホストは名前ベース、IPベース、またはポートベースのいずれかになります。

仮想ホストは、YaSTを使用するか([仮想ホスト項](#) (821 ページ)を参照)、または設定ファイルを手動で編集して設定できます。SUSE Linux Enterprise ServerのApacheは、デフォルトでは、/etc/apache2/vhosts.d/の仮想ホストごとに1つの設定ファイルを使用するようになっています。このディレクトリ内で、拡張子が.confのファイルは、すべて自動的に設定に含まれます。仮想ホストの基本的なテンプレートはこのディレクトリ内に用意されています(vhost.template、またはSSLサポートのある仮想ホストの場合はvhost-ssl.template)。

ティップ: 常に仮想ホスト設定を作成する

Webサーバに1つのドメインしか存在しない場合でも、常に仮想ホスト設定ファイルを作成することをお勧めします。仮想ホスト設定ファイルを作成することで、1つのファイルにドメイン固有の設定を含めるのみでなく、仮想ホスト用の設定ファイルを移動、削除または名前変更することにより、

常に使用中の基本設定にフォールバックできます。同じ理由で、仮想ホストごとに個別の設定ファイルも作成します。

<VirtualHost></VirtualHost>ブロックには、特定のドメインに適用される情報を記述します。Apacheは、クライアントから定義済みの仮想ホストへの要求を受け取ると、このセクションに記述されているディレクティブを使用します。仮想ホストでは、ほぼすべてのディレクティブを使用できます。Apacheの設定ディレクティブの詳細については、<http://httpd.apache.org/docs/2.2/mod/quickreference.html>を参照してください。

名前ベースの仮想ホスト

名前ベースの仮想ホストでは、1つのIPアドレスで複数のWebサイトを運用することができます。Apacheは、クライアントから送られたHTTPヘッダのホストフィールドを使用して、要求を、仮想ホスト宣言の1つの、一致するServerNameエントリに結び付けます。一致するServerNameが見つからない場合には、指定されている最初の仮想ホストがデフォルトとして用いられます。

NameVirtualHost仮想ディレクティブが、Apacheに、どのIPアドレス、そしてオプションとしてどのポートをリスンして、HTTPヘッダ内にドメイン名を含むクライアントからのリクエストを受け付けるかを指定します。このオプションは、/etc/apache2/listen.conf設定ファイルで設定されます。

最初の引数には完全修飾ドメイン名を指定することができますが、IPアドレスを使用することをお勧めします。2番目の引数はポートで、オプションです。デフォルトでは、ポート80が使用され、Listenディレクティブで設定されます。

ワイルドカード*は、IPアドレスとポート番号の両方で使用することができます。その場合、すべてのインタフェースでの要求を受け取ります。IPv6のアドレスは、角カッコの中に記述する必要があります。

例 40.1 名前ベースのVirtualHostエントリの応用例

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.3.100:80
NameVirtualHost 192.168.3.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:364::]:80
```

VirtualHost開始タグには、名前ベースの仮想ホスト設定でNameVirtualHostを引数として使用して以前に宣言されたIPアドレス(または完全修飾ドメイン名)が採用されます。NameVirtualHostディレクティブで以前に宣言されたポート番号はオプションです。

ワイルドカード*をIPアドレスの代わりに使うこともできます。この構文は、ワイルドカードをNameVirtualHost *として組み合わせて使用する場合にのみ有効です。IPv6アドレスを使用する場合には、アドレスを角カッコの中に記述することが必要です。

例 40.2 名前ベースのVirtualHostディレクティブ

```
<VirtualHost 192.168.3.100:80>
...
</VirtualHost>

<VirtualHost 192.168.3.100>
...
</VirtualHost>

<VirtualHost *:80>
...
</VirtualHost>

<VirtualHost *>
...
</VirtualHost>

<VirtualHost [2002:c0a8:364::]>
...
</VirtualHost>
```

IPベースの仮想ホスト

この仮想ホスト設定では、1つのコンピュータに対して複数のIPアドレスを設定する必要があります。Apacheの1つのインスタンスが、複数のドメインにホストとしてサービスを提供し、各ドメインに別のIPアドレスが割り当てられることになります。

物理サーバは、IPベースの仮想ホストごとに、1つのIPアドレスを持つ必要があります。マシンに複数のネットワークカードがない場合には、仮想ネットワークインタフェース(IPエイリアス)を使用することもできます。

次の例では、IP 192.168.3.100のマシンでApacheが実行されており、付加的なIP 192.168.3.101および192.168.3.102をホストしています。すべての仮想サーバについて、VirtualHostブロックが個別に必要です。

例 40.3 IPベースのVirtualHostディレクティブ

```
<VirtualHost 192.168.3.101>
...
</VirtualHost>

<VirtualHost 192.168.3.102>
...
</VirtualHost>
```

ここでは、VirtualHostディレクティブは、192.168.3.100以外のインタフェースに対してのみ指定されています。Listenディレクティブが192.168.3.100に対しても設定される場合、このインタフェースへのHTTP要求に応答するために別のIPベースの仮想ホストを作成する必要があります。作成しない場合、デフォルトのサーバ設定(/etc/apache2/default-server.conf)内のディレクティブが適用されます。

基本的な仮想ホスト設定

仮想ホストをセットアップするには、少なくとも次のディレクティブが各仮想ホスト設定に含まれている必要があります。オプションについては、「/etc/apache2/vhosts.d/vhost.template」を参照してください。

ServerName

ホストに割り当てられている完全修飾ドメイン名。

DocumentRoot

Apacheがこのホストにファイルをサービスする際に使用されるディレクトリパス。セキュリティ上の理由から、ファイルシステム全体へのアクセスはデフォルトで禁じられているため、Directoryコンテナ内でこのディレクトリを明示的にロック解除する必要があります。

ServerAdmin

サーバ管理者の電子メールアドレス。このアドレスは、Apacheが作成するエラーページなどに表示されます。

ErrorLog

この仮想ホストに関するエラーログファイル。仮想ホストごとに個別のエラーログファイルを作成する必要はありませんが、エラーのデバッグが簡単にできるため、よく行われています。/var/log/apache2/は、Apacheのログファイルの保管先となるデフォルトディレクトリです。

CustomLog

この仮想ホストに関するアクセスログファイル。仮想ホストごとに個別のアクセスログファイルを作成する必要はありませんが、ホストごとのアクセス統計を個別に分析できるため、よく行われています。/var/log/apache2/は、Apacheのログファイルの保管先となるデフォルトディレクトリです。

セキュリティ上の理由から、ファイルシステム全体へのアクセスはデフォルトで禁じられています。したがって、DocumentRootなど、Apacheによりサービスされるファイルを保管したディレクトリを明示的にロック解除する必要があります。

```
<Directory "/srv/www/www.example.com/htdocs">
    Order allow,deny
    Allow from all
</Directory>
```

完全な設定ファイルは次のようになります。

例 40.4 基本的な仮想ホスト設定

```
<VirtualHost 192.168.3.100>
    ServerName www.example.com;
    DocumentRoot /srv/www/www.example.com/htdocs
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com_log
    CustomLog /var/log/apache2/www.example.com-access_log common
    <Directory "/srv/www/www.example.com/htdocs">
        Order allow,deny
        Allow from all
    </Directory>
</VirtualHost>
```

40.2.2 ApacheをYaSTで設定する

YaSTを使用してWebサーバを設定するには、YaSTを起動して、[ネットワークサービス] > [HTTPサーバ] の順に選択します。このモジュールを初めて

起動すると、HTTP Server Wizardが起動して、サーバ管理に関していくつかの基本的な事項を決定するように要求されます。このウィザードの完了後、[HTTPサーバ] モジュールを呼び出すたびにHTTPサーバの設定項(822ページ)のダイアログが起動します。

HTTP Server Wizard

HTTP Server Wizardには、5つのステップがあります。ダイアログの最後のステップでは、上級者用の設定モードに入って、さらに詳細な設定を行うかどうか選択できます。

Network Device Selection (ネットワークデバイスの選択)

ここでは、Apacheが着信リクエストをリスンするために使用する、ネットワークインタフェースとポートを指定します。既存のネットワークインタフェースとそれらに対応するIPアドレスから、任意のものを組み合わせて選択できます。他のサービスによって予約されていないものであれば、3つの範囲(ウェルknownポート、レジスタードポート、ダイナミックまたはプライベートポート)のうちのどのポートでも使用できます。デフォルトの設定では、すべてのネットワークインタフェース(IPアドレス)のポート80をリスンします。

ファイアウォールで、Webサーバがリスンするポートを開くには、[*Open Firewall for Selected Ports*] をオンにします。これは、LAN、WAN、または公共のインターネットなど、ネットワーク上でWebサーバを利用可能にする場合には必須です。外部からWebサーバにアクセスすることが不要なテスト段階でのみ、ポートを閉じておくのが有用です。

[Next] をクリックして設定を続けます。

モジュール

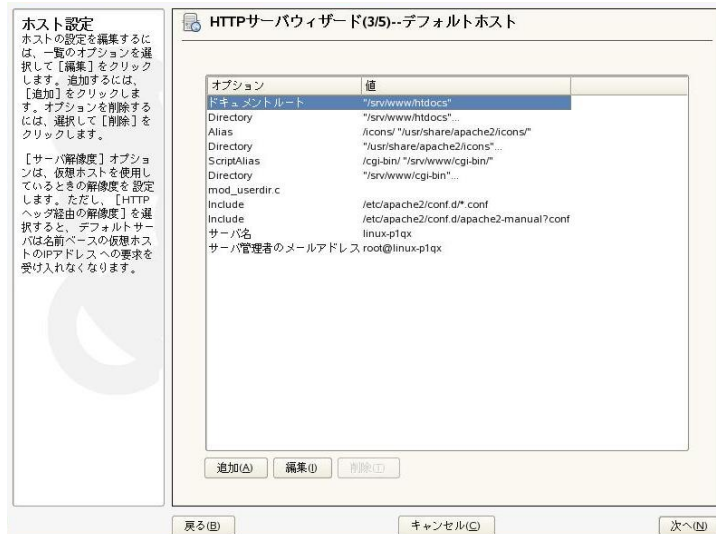
[モジュール] 設定オプションによって、Webサーバでサポートされるスクリプト言語の有効化または無効化を設定できます。他のモジュールの有効化または無効化の詳細については、サーバモジュール項(824ページ)を参照してください。[次へ] をクリックして次のダイアログに進みます。

Default Host (デフォルトのホスト)

このオプションは、デフォルトのWebサーバに関連しています。**仮想ホスト設定項** (813 ページ)で説明されているように、Apacheは、1つの物理的マシンで複数の仮想ホストに使用することができます。設定ファイルで最初に宣言された仮想ホストは通常、デフォルトのホストと呼ばれます。各仮想ホストは、デフォルトホストの設定を継承します。

ホストの設定(ディレクティブ)を編集するには、テーブル内の適切なエントリを選択して、**[編集]** をクリックします。新しいディレクティブを追加するには、**[追加]** をクリックします。ディレクティブを削除するには、そのアカウントを選択し、**[削除]** をクリックします。

図 40.1 HTTP Server Wizard: デフォルトホスト



これはサーバのデフォルト設定のリストです。

ドキュメントルート

Apacheがこのホストにファイルを送るときに使用されるディレクトリパス。/srv/www/htdocsはデフォルトの場所です。

別名

Aliasディレクティブを使えば、URLを物理的なファイルシステムの場所にマップすることができます。このことは、パスのURLエイリアスを行えば、ファイルシステムのDocument Rootの外にあるパスでもアクセスできることを意味しています。

デフォルトのSUSE Linux Enterpriseでは、Alias/iconsが/usr/share/apache2/iconsを指しています。ここには、ディレクトリのインデックス表示で使用するApacheのアイコンがあります。

ScriptAlias

Aliasディレクティブと同様に、ScriptAliasディレクティブはURLをシステム内の場所にマップします。相違点は、ScriptAliasはターゲットディレクトリをCGIの場所として指定するということです。つまり、その場所にあるCGIスクリプトが実行されます。

ディレクトリ

ディレクトリ設定を使用して、指定したディレクトリにのみ適用される設定オプションのグループを含めることができます。

/usr/share/apache2/iconsと/srv/www/cgi-binディレクトリのアクセスおよび表示オプションをここで設定します。デフォルトを変更する必要はありません。

対象項目

インクルードにより、他の設定ファイルを指定できます。2つのインクルードディレクティブが設定済みです。/etc/apache2/conf.d/は外部モジュールに付属する設定ファイルを保持するディレクトリです。このディレクティブにより、このディレクトリ内の.confで終わるすべてのファイルが対象となります。もう1つのディレクティブでは、/etc/apache2/conf.d/apache2-manual.confというapache2-manual設定ファイルが対象となります。

サーバ名

クライアントがWebサーバとコンタクトするために使うデフォルトのURLを指定します。http://FQDN/にあるWebサーバへの接続用FQDN(完全修飾ドメイン名)か、またはそのIPアドレスを使用します。ここでは任意の名前は選択できません。サーバはこの名前です「認識」されなければなりません。

Server Administrator E-Mail

サーバ管理者の電子メールアドレス。このアドレスは、Apacheが作成するエラーページなどに表示されます。

[デフォルトホスト] のステップを完了したら、[次へ] をクリックして、設定を続けます。

仮想ホスト

このステップでは、ウィザードはすでに設定されている仮想ホストのリストを表示します(**仮想ホスト設定項** (813 ページ)を参照)。YaST HTTPウィザードを起動する前に手動で変更を行っていないければ、仮想ホストは表示されません。

ホストを追加するには、[追加] をクリックしてダイアログを表示し、ホストについての基本的な情報を入力します。[サーバID] には、サーバ名、サーバのコンテンツのroot(DocumentRoot)、管理者の電子メールアドレスが含まれます。[サーバ解像度] は、ホストの識別方法を決めるために使用されます(名前ベースまたはIPベース)。[仮想ホストIDの変更] で名前またはIPアドレスを指定します。

[次へ] をクリックして、仮想ホスト設定ダイアログの2番目の部分に進みます。

仮想ホスト設定のパート2では、CGIスクリプトを有効にするかどうか、およびこれらのスクリプトを使用するディレクトリを指定できます。また、SSLも有効にできます。SSLを有効化する場合は、証明書のパスも指定する必要があります。SSLおよび証明書の詳細については、**40.6.2項「SSLサポートのあるApacheの設定」** (843 ページ)を参照してください。[ディレクトリインデックス] オプションを使用して、クライアントがディレクトリを要求するときに表示するファイルを指定できます(デフォルトではindex.html)。ファイルを変更する場合は、1つ以上のファイル名(スペースで区切る)を追加します。[公開HTMLを有効にする] で、ユーザのパブリックディレクトリ(~user/public_html/)のコンテンツが、サーバのhttp://www.example.com/~userからアクセスできるようにします。

重要項目: 仮想ホストの作成

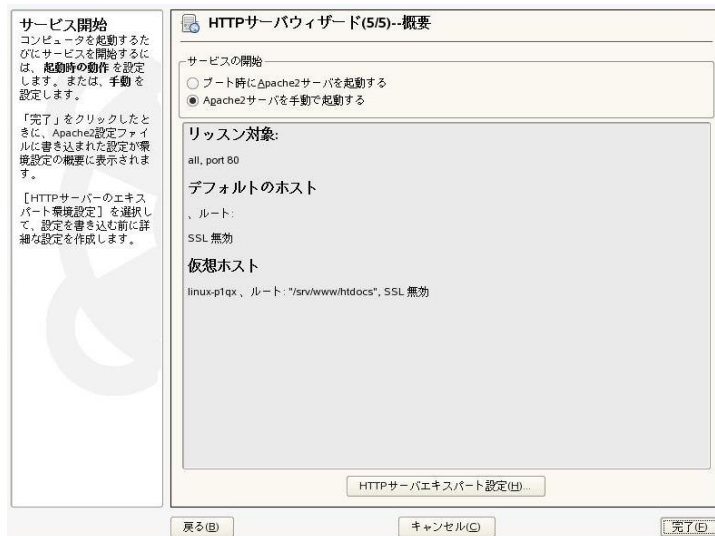
仮想ホストを自由に追加することはできません。名前ベースの仮想ホストを使用する場合は、各ホスト名がネットワーク内で解決されている必要が

あります。IPベースの仮想ホストを使用する場合は、使用可能な各IPアドレスに対し1つのホストのみを割り当てることができます。

概要

これはウィザードの最後のステップです。ここでは、Apacheサーバをいつ、どのようにして起動するか(ブート時に起動するか、手動で起動するか)を指定します。また、ここまで行った設定の簡単な要約を確認します。この設定でよければ、[完了] をクリックして、設定を完了します。変更する場合は、希望のダイアログまで[戻る] をクリックして戻ります。[HTTPサーバのエキスパート環境設定] をクリックして、**HTTPサーバの設定項** (822 ページ)で説明しているダイアログを開きます。

図 40.2 HTTP Server Wizard: 概要



HTTPサーバの設定

[HTTPサーバの設定] ダイアログでは、ウィザード(Webサーバを最初に設定する場合にのみ実行)よりも詳細に設定を調整できます。このダイアログは、次で説明する4つのタブで構成されています。ここで変更する設定オプションは、すぐには適用されません。変更を適用するには、常に[完了] をクリッ

クして変更を確認する必要があります。[キャンセル] をクリックすると、設定モジュールを終了し、変更が破棄されます。

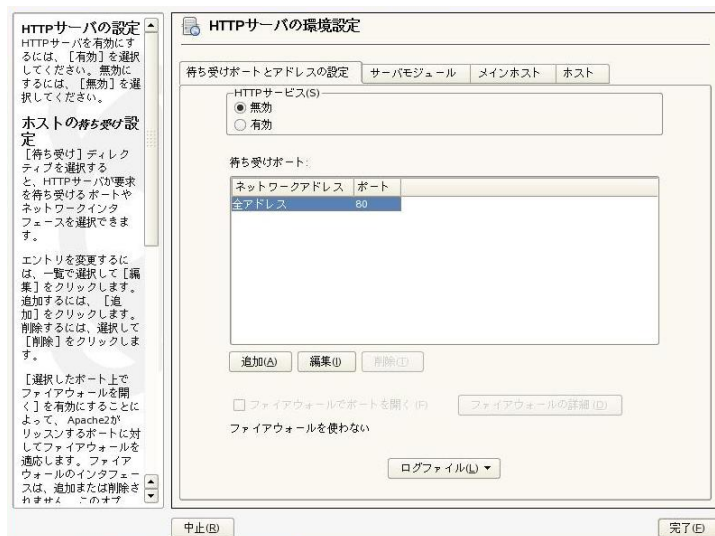
待ち受けポートおよびアドレス

[HTTPサービス] で、Apacheを実行するか([有効にする])、または停止するか([無効])を選択します。[Listen on Ports] で、サーバが使用可能なアドレスおよびポートについて [追加]、[編集]、または [削除] を選択します。デフォルトでは、すべてのインタフェースがポート80をリッスンします。

[Open Firewall on Selected Ports] は常に選択します。このオプションを選択しない場合、外部からWebサーバに到達できなくなります。外部からWebサーバにアクセスすることが不要なテスト段階でのみ、ポートを閉じておくのが有用です。

[ログファイル] で、アクセスログまたはエラーログのいずれかを確認します。これは、設定をテストする場合に便利です。ログファイルが別のウィンドウ内に表示され、ここからWebサーバを再起動または再ロードすることもできます(詳細については40.3頁「[Apacheの起動および停止](#)」(824 ページ)を参照してください)。これらのコマンドは、すぐに適用されます。

図 40.3 HTTP Server Configuration: 設定: リッスンポートとアドレス



サーバモジュール

[状態の変更] をクリックして、Apache2モジュールのステータス(有効または無効)を変更できます。すでにインストールされているがリストに含まれていない新規モジュールを追加するには、[Add Module] をクリックします。モジュールの詳細については、[40.4頁「モジュールのインストール、有効化および設定」](#) (826 ページ)を参照してください。

図 40.4 HTTP Server Configuration: サーバモジュール



メインホストまたはホスト

これらのダイアログは、すでに説明したものと同じです。詳細については、[Default Host \(デフォルトのホスト\) 頁](#) (819 ページ)および[仮想ホスト 頁](#) (821 ページ)を参照してください。

40.3 Apacheの起動および停止

YaSTを使って環境設定した場合([40.2.2頁「ApacheをYaSTで設定する」](#) (817 ページ)を参照)、Apacheはブート時にランレベル3および5で開始され、ランレベル

1、2、および6で停止されます。YaSTのランレベルエディタまたはコマンドラインツールのchkconfigを使って、この動作を変更することができます。

実行中のシステムでApacheを起動、停止または操作するには、initスクリプトの/usr/sbin/rcapache2を使用します(initスクリプトの一般的な情報については20.2.2頁「initスクリプト」(435 ページ)を参照してください)。rcapache2コマンドでは、次のパラメータが使用されます。

起動

Apacheが実行中でない場合に起動します。

startssl

SSLサポートのあるApacheが実行中でない場合に起動します。SSLサポートについての詳細は、40.6頁「SSLをサポートするセキュアWebサーバのセットアップ」(838 ページ)を参照してください。

中止

親プロセスを終了して、Apacheを終了します。

restart

Apacheを停止し、再起動します。Apacheが実行中でなかった場合は、新規に起動します。

try-restart

Apacheが実行中の場合にのみ、停止し、再起動します。

reload or graceful

フォークしたすべてのApacheプロセスに、シャットダウンする前に要求を完了させて、それからWebサーバを停止します。1つのプロセスが終了するたびに、新たに開始したもので置き換えられるので、最終的にはApacheが完全に「再起動」したことになります。

ティップ

rcapache2 reloadは、設定の変更を有効化するときなど、実働環境でApacheを再起動する場合に推奨されている方法です。接続の切断を行わずに、すべてのクライアントにサービスを提供し続けることができるからです。

`configtest`

実行中のWebサーバに影響することなく、設定ファイルの構文をチェックします。このチェックは、サーバが起動、再ロードまたは再起動するた
びに行われるため、通常は明示的にテストを実行する必要はありません
(設定エラーが検出された場合、Webサーバは起動、再ロードまたは再起
動されません)。

`probe`

再ロードの必要性を検出し(設定が変更されたかどうかを確認)、`rcapache2`
コマンドに必要な引数を提示します。

`server-status` and `full-server-status`

それぞれ、簡単または完全ステータス画面を表示します。`lynx`または`w3m`
のいずれかがインストールされており、`module mod_status`が有効になって
いる必要があります。これに加え、`status`を`/etc/sysconfig/apache2`
ファイルの`APACHE_SERVER_FLAGS`に追加する必要があります。

ティップ: その他のフラグ

`rcapache2`にその他のフラグを指定すると、これらのフラグはWebサーバを
通過します。

40.4 モジュールのインストール、有効 化および設定

Apacheソフトウェアは、モジュール構成で用意されており、一部の主要タ
スクを除いてはモジュールにより処理されます。この方法で、HTTPさえもモ
ジュールによって処理されています(`http_core`)。

Apacheのモジュールは、ビルド時にApacheのバイナリに組み込むことも、実
行時に動的にロードすることもできます。動的なモジュールのロード方法の
詳細については、[40.4.2項「有効化と無効化」](#) (827 ページ)を参照してくださ
い。

Apacheモジュールは、次の4つのカテゴリに分類されます。

基本モジュール

基本モジュールは、デフォルトでApacheにコンパイルされています。SUSE LinuxのApacheは、`mod_so`(他のモジュールのロードに必要)および`http_core`のみがコンパイルされています。他のモジュールは、サーバのバイナリに入れる代わりに、ランタイム時に入れるように共有オブジェクトとして利用できます。

拡張モジュール

一般に、拡張とされているモジュールは、Apache ソフトウェアパッケージに含まれてはいますが、通常、サーバに静的にはコンパイルされていません。SUSE Linux Enterprise Serverでは、これらはApacheに実行時にロードすることができる共有オブジェクトとして利用可能になっています。

外部モジュール

外部とラベルされているモジュールは、公式のApacheのディストリビューションには含まれていません。しかし、SUSE Linux Enterprise Serverでは、それらのいくつかをすぐに使えるように用意しています。

マルチプロセッシングモジュール

MPMは、Webサーバへのリクエストを受け取って処理する役割を果たすもので、Webサーバソフトウェアの中核となっています。

40.4.1 モジュールのインストール

デフォルトの方法でApacheをインストールした場合(40.1.2項「インストール」(808 ページ)を参照してください)、すべての基本と拡張モジュール、マルチプロセッシングモジュールのプリフォークMPM、および外部モジュールの`mod_php5` および`mod_python`もインストールされます。

YaSTを起動し、`[ソフトウェア]` > `[ソフトウェアの管理]` の順に選択して、その他の外部モジュールをインストールできます。`[フィルタ]` > `[検索]` の順に選択し、`[apache]` を検索します。他のパッケージの中で、すべての使用可能な外部Apacheモジュールが検索結果のリストに表示されます。

40.4.2 有効化と無効化

YaSTを使用して、**HTTP Server Wizard**項 (818 ページ)で説明しているモジュール設定によってスクリプト言語モジュール(PHP5、Perl、およびPython)を有効

化または無効化できます。その他のすべてのモジュールは、**サーバモジュール項** (824 ページ)で説明しているように有効化または無効化できます。

手動でモジュールを有効化または無効化する場合は、`a2enmod mod_foo`または`a2dismodmod_foo`コマンドをそれぞれ使用します。`a2enmod -l`は、すべての現在アクティブなモジュールのリストを出力します。

重要項目: 外部モジュール用の設定ファイルを含める

手動で外部モジュールを有効化した場合は、各設定ファイルがすべての仮想ホスト設定にロードされていることを確認します。外部モジュール用の設定ファイルは、`/etc/apache2/conf.d/`内に位置し、デフォルトではロードされません。各仮想ホスト上に同じモジュールが必要な場合は、このディレクトリ内の`*.conf`を含めることができます。必要でない場合は、個々のファイルを含めます。その例として、「`/etc/apache2/vhost.d/vhost.template`」を参照してください。

40.4.3 基本および拡張モジュール

すべての基本および拡張モジュールは、Apacheのマニュアルに詳しく説明されています。ここでは、主要なモジュールについて簡単に説明します。各モジュールの詳細については、<http://httpd.apache.org/docs/2.2/mod/>を参照してください。

`mod_actions`

特定のMIMEタイプ(application/pdfなど)、特定の拡張子を持つファイル(.rpmなど)、または特定の要求方法(GETなど)が要求された場合に、常にスクリプトを実行する方法を提供します。このモジュールは、デフォルトで有効です。

`mod_alias`

AliasおよびRedirectディレクティブを提供します。これにより、特定のディレクトリにURIをマップ(Alias)、または要求されたURLを別の場所にリダイレクトできます。このモジュールは、デフォルトで有効です。

mod_auth*

認証モジュールは、`mod_auth_basic`や`mod_auth_digest`を使ったダイジェスト認証などの認証方法を提供しています。Apache 2.2のダイジェスト認証は実験的なものであると考えなくてはなりません。

`mod_auth_basic`および`mod_auth_digest`は、認証プロバイダモジュールの`mod_authn_*`(テキストファイルベースの認証用の`mod_authn_file`など)および認証モジュールの`mod_authz_*`(ユーザ認証用の`mod_authz_user`)と組み合わせる必要があります。

この項目の詳細は、<http://httpd.apache.org/docs/2.2/howto/auth.html>の「Authentication howto」で説明されています。

mod_autoindex

Autoindexは、インデックスファイル(`index.html`など)が存在しない場合にディレクトリリストを生成します。これらのインデックスのルックアンドフィールは設定可能です。このモジュールは、デフォルトで有効です。ただし、ディレクトリリストは、デフォルトでOptionsディレクティブを経由して無効化されています。仮想ホスト設定でこの設定を上書きします。このモジュール用のデフォルト設定は、`/etc/apache2/mod_autoindex-defaults.conf`に存在します。

mod_cgi

`mod_cgi`は、CGIスクリプトを実行するのに必要です。このモジュールは、デフォルトで有効です。

mod_deflate

このモジュールを使用して、配信前にファイルタイプを圧縮するようにApacheを設定できます。

mod_dir

`mod_dir`は、DirectoryIndexディレクティブを提供します。これを使用して、ディレクトリが要求されたときに(デフォルトでは`index.html`)自動的に配信されるファイルを設定できます。ディレクトリ要求に末尾のスラッシュが含まれていない場合にURIを修正するための自動リダイレクトも提供します。このモジュールは、デフォルトで有効です。

`mod_env`

CGIスクリプトやSSIページに渡す環境を制御します。環境変数を設定、設定解除したり、`httpd`プロセスを起動したシェルから渡すことができます。このモジュールは、デフォルトで有効です。

`mod_expires`

`mod_expires`を使用して、Expiresヘッダを送信することにより、プロキシとブラウザキャッシュがドキュメントを更新する頻度を制御できます。このモジュールは、デフォルトで有効です。

`mod_include`

`mod_include`は、動的にHTMLページを生成するための基本機能を提供するSSI (Server-Side Includes)を使用できるようにします。このモジュールは、デフォルトで有効です。

`mod_info`

`http://localhost/server-info/`にサーバ設定の包括的な概要を表示します。セキュリティ上の理由から、このURLへのアクセスは常に制限されます。デフォルトでは、localhostのみ、このURLへのアクセスが許可されます。`mod_info`は、`/etc/apache2/mod_info.conf`で設定されます。

`mod_log_config`

このモジュールを使用して、Apacheログファイルの書式を設定できます。このモジュールは、デフォルトで有効です。

`mod_mime`

`mime`モジュールは、ファイル名の拡張子(HTMLドキュメント用の`text/html`など)に基づき、適切なMIMEヘッダを使用してファイルが配信されるようにします。このモジュールは、デフォルトで有効です。

`mod_negotiation`

コンテンツネゴシエーションに必要です。詳細については、<http://httpd.apache.org/docs/2.2/content-negotiation.html>を参照してください。このモジュールは、デフォルトで有効です。

`mod_rewrite`

`mod_alias`の機能を提供しますが、それ以外の機能も提供し、柔軟性を与えます。`mod_rewrite`を使用して、複数の規則、要求ヘッダなどに基づいてURLをリダイレクトできます。

`mod_setenvif`

クライアントから送信されたブラウザ文字列やIPアドレスなどの、クライアントからのリクエスト詳細に基づいて環境変数を設定します。このモジュールは、デフォルトで有効です。

`mod_speling`

`mod_speling`は、大文字小文字の違いなど、URLの表記エラーの訂正を自動的に試みます。

`mod_ssl`

Webサーバとクライアント間の暗号化接続を有効化します。詳細については、[40.6頁「SSLをサポートするセキュアWebサーバのセットアップ」](#) (838 ページ)を参照してください。このモジュールは、デフォルトで有効です。

`mod_status`

サーバの動作およびパフォーマンスに関する情報を<http://localhost/server-status/>に表示します。セキュリティ上の理由から、このURLへのアクセスは常に制限する必要があります。デフォルトでは、localhostのみ、このURLへのアクセスが許可されます。`mod_status`は、`/etc/apache2/mod_status.conf`で設定されます。

`mod_suexec`

`mod_suexec`は、CGIスクリプトを別のユーザとグループで実行できるようにします。このモジュールは、デフォルトで有効です。

`mod_userdir`

`~user/`の下に、ユーザ固有のディレクトリを用意します。UserDirディレクティブを設定で指定する必要があります。このモジュールは、デフォルトで有効です。

40.4.4 マルチプロセシングモジュール

SUSE Linux Enterprise Serverには、Apacheで使用するための2つのマルチプロセシングモジュール(MPM)が用意されています。

プリフォークMPM

プリフォークMPMは、スレッド対応でない、プリフォークWebサーバを実装します。Webサーバは、それぞれのリクエストを分離し、個別の子プロセスを分岐することによって処理する、Apacheバージョン1.xと同様の動作を行います。これにより、問題のあるリクエストが他のものに影響することがなくなるので、Webサーバのロックアップを避けられます。

プロセスベースのアプローチによって安定性がもたらされますが、プリフォークMPMは、もう一方のワーカーMPMよりも多くのシステムリソースを消費します。プリフォークMPMは、UnixベースのオペレーティングシステムでのデフォルトのMPMとみなされています。

重要項目: このドキュメントでのMPM

このドキュメントでは、ApacheがプリフォークMPMで使用されていることを假定しています。

ワーカーMPM

ワーカーMPMは、マルチスレッド対応のWebサーバを提供します。スレッドとは、「軽い」形態のプロセスです。プロセスよりもスレッドが優れている点は、リソースの消費が少ないことです。ワーカーMPMは、子プロセスを分岐する代わりに、サーバプロセスでスレッドを使用することによってリクエストを処理します。プリフォークした子プロセスは複数のスレッドになります。このアプローチでは、プリフォークMPMの場合よりもシステムリソースの消費が少なくなるので、Apacheの性能が良くなります。

主な欠点としては、ワーカーMPMの安定性の問題が挙げられます。スレッドが壊れた場合、プロセスのすべてのスレッドに影響してしまいます。最悪の場合には、サーバがクラッシュすることがあります。特に、ApacheでCGI (Common Gateway Interface)を使用している場合、負荷が大きくなると、スレッドがシステムリソースと通信できなくなって、内部サーバエラーが生じることがあります。ワーカーMPMを使用すべきでないという意見の別の根拠は、利用できるApacheのモジュールのすべてがスレッドセーフになっているわけではなく、そのためワーカーMPMと組み合わせて使用することはできないという点です。

警告: MPMと組み合わせてPHPモジュールを使用する

利用可能なPHPモジュールのすべてがスレッドセーフになっているわけではありません。ワーカーMPMとmod_phpを組み合わせてください。

40.4.5 外部モジュール

ここでは、SUSE Linux Enterprise Serverに付属しているすべての外部モジュールについて記載しています。モジュールのドキュメントは、記載のディレクトリ内に存在します。

mod-apparmor

mod_php5やmod_perlなどのモジュールが処理する各CGIスクリプトに対して、Novell AppArmor制限を提供するために、Apacheにサポートを追加します。

パッケージ名: apache2-mod_apparmor

詳細: *Novell AppArmor 管理ガイド* (↑*Novell AppArmor 管理ガイド*)

mod_perl

mod_perlは、埋め込まれているインタプリタでPerlスクリプトを実行できるようにします。サーバに埋め込まれている永続的なインタプリタにより、外部インタプリタの起動のオーバーヘッド、およびPerlの起動時間のペナルティを回避できます。

パッケージ名: apache2-mod_perl

環境設定ファイル: /etc/apache2/conf.d/mod_perl.conf

詳細: /usr/share/doc/packages/apache2-mod_perl

mod_php5

PHPは、サーバ側クロスプラットフォームのHTML埋込みスクリプト言語です。

パッケージ名: apache2-mod_php5

環境設定ファイル: /etc/apache2/conf.d/php5.conf

詳細: /usr/share/doc/packages/apache2-mod_php5

mod_python

mod_pythonは、Apache HTTPサーバへのPythonの埋込みができるようにし、Webベースのアプリケーションの設計で、さらに柔軟性を持たせ、パフォーマンスを向上させます。

パッケージ名:apache2-mod_python

詳細:/usr/share/doc/packages/apache2-mod_python

40.4.6 コンパイル

上級ユーザは、カスタムのモジュールを記述してApacheを拡張することができます。Apache用のモジュールを開発したり、サードパーティのモジュールをコンパイルしたりするには、apache2-develパッケージ、および対応する開発ツールが必要です。apache2-develには、Apache用の追加モジュールのコンパイルに必要なapxs2ツールも含まれています。

apxs2は、ソースコードからモジュールをコンパイルし、インストールすることを可能にします(設定ファイルへの必要な変更も含みます)。これは、実行時にApacheにロードされる、ダイナミック共有オブジェクト(DSO)を作成します。

apxs2バイナリは、/usr/sbinの下層にあります

- /usr/sbin/apxs2—MPMと共に動作する拡張モジュールを構築するのに適しています。インストール場所は/usr/lib/apache2です。
- /usr/sbin/apxs2-prefork—プリフォークMPMモジュールに適しています。インストール場所は/usr/lib/apache2-preforkです。
- /usr/sbin/apxs2-worker—ワーカーMPMモジュールに適しています。

apxs2は、どのMPMに対しても使用できるようにモジュールをインストールします。他の2つのプログラムは、それぞれのMPMに対してのみ使用できるようにモジュールをインストールします。apxs2は、/usr/lib/apache2にモジュールをインストールし、apxs2-preforkおよびapxs2-workerは、/usr/lib/apache2-preforkまたは/usr/lib/apache2-workerにモジュールをインストールします。

`cd /path/to/module/source; apxs2 -cia mod_foo.c`コマンド(-cはモジュールをコンパイル、-iはモジュールをインストール、-aはモジュールを有効化する)を使用して、ソースコードからモジュールをインストールし、有効化します。apxs2のその他のオプションについては、`apxs2(1) man`ページを参照してください。

40.5 CGIスクリプトを実行させる

ApacheのCGI(Common Gateway Interface)により、通常CGIスクリプトと呼ばれるスクリプトまたはプログラムを含んだ動的コンテンツを作成できます。CGIスクリプトは、どのプログラム言語でも作成できます。通常、PerlまたはPHPなどのスクリプト言語が使用されます。

ApacheがCGIスクリプトによって作成されたコンテンツを配信できるようにするには、`mod_cgi`を有効化する必要があります。また、`mod_alias`も必要です。デフォルトでは、両モジュールとも有効化されています。モジュールの有効化の詳細については、[40.4.2項「有効化と無効化」](#) (827 ページ)を参照してください。

警告: CGIセキュリティ

サーバがCGIスクリプトを実行できるようになると、潜在的なセキュリティホールが発生します。詳細については、[40.7項「セキュリティ問題の回避」](#) (844 ページ)を参照してください。

40.5.1 Apacheの設定

SUSE Linux Enterprise Serverでは、CGIスクリプトの実行は、`/srv/www/cgi-bin/`ディレクトリ内でのみ許可されています。この場所は、すでにCGIスクリプトを実行するように設定されています。仮想ホスト設定を作成しておらず([仮想ホスト設定項](#) (813 ページ)を参照してください)、ホスト固有のディレクトリにスクリプトを配置する場合は、このディレクトリのロックを解除し、設定する必要があります。

例 40.5 VirtualHost CGIの設定

```
ScriptAlias /cgi-bin/ "/srv/www/www.example.com/cgi-bin/"❶
```

```
<Directory "/srv/www/www.example.com/cgi-bin/">  
Options +ExecCGI❷  
AddHandler cgi-script .cgi .pl❸  
Order allow,deny❹  
Allow from all  
</Directory>
```

- ❶ このディレクトリ内のすべてのファイルをCGIスクリプトとして処理するようにApacheに指示します。
- ❷ CGIスクリプトの実行を有効化します。
- ❸ .plおよび.cgiの拡張子が付いたファイルをCGIスクリプトとして処理するようにサーバに指示します。必要に応じて調整します。
- ❹ OrderとAllowディレクティブは、デフォルトのアクセス状態、およびこれらのディレクティブが評価される順序を制御します。この場合、「allow」文およびすべての場所からのアクセスが有効化される前に、「deny」文が評価されます。

40.5.2 テストスクリプトの実行

CGIプログラミングは通常のプログラミングとは異なり、CGIプログラムとスクリプトの前にContent-type: text/htmlなどのMIMEタイプヘッダを記述する必要があります。このヘッダはクライアントに送信されるので、クライアントは、受信したコンテンツによってコンテンツの種類を識別します。次に、このスクリプトの出力は、通常、Webブラウザなどのクライアントが認識できる形式(たいていの場合はHTML、プレーンテキスト、画像など)でなければなりません。

Apacheパッケージの一部として、/usr/share/doc/packages/apache2/test-cgi内に簡単なテストスクリプトが含まれています。このスクリプトは、いくつかの環境変数の内容をプレーンテキストとして出力します。このスクリプトを/srv/www/cgi-bin/か、仮想ホストのスクリプトディレクトリ/srv/www/example.com_cgi-bin/のいずれかにコピーし、「test.cgi」という名前を付けます。

Webサーバによってアクセス可能なファイルは、rootユーザが所有する必要があります(詳細については、[40.7項「セキュリティ問題の回避」](#) (844 ページ)を参照してください)。Webサーバは別のユーザ名で実行しているので、CGI スクリプトはworld-executableおよびworld-readableである必要があります。CGI ディレクトリに移動し、`chmod 755 test.cgi` コマンドを使用して適切なパーミッションを適用します。

次に、`http://localhost/cgi-bin/test.cgi` または `http://www.example.com/cgi-bin/test.cgi` を呼び出します。「CGI/1.0 test script report」を参照してください。

40.5.3 トラブルシューティング

テストプログラムの出力の代わりにエラーメッセージが表示される場合は、次を確認します。

CGIトラブルシューティング

- 設定を変更した後、サーバを再ロードしましたか?`rcapache2 probe`を使用して確認します。
- カスタムCGIディレクトリを設定した場合、適切に設定されていますか? 不明な場合は、デフォルトのCGIディレクトリの`/srv/www/cgi-bin/`内にあるスクリプトを実行し、`http://localhost/cgi-bin/test.cgi` を呼び出します。
- ファイルのパーミッションは正しいですか?CGIディレクトリに移動し、`ls -l test.cgi`を実行します。その出力が次で始まっているかどうかを確認します。

```
-rwxr-xr-x  1 root root
```
- そのスクリプトにプログラミングエラーがないかどうか確認します。`test.cgi` を変更しなかった場合は該当しませんが、独自のプログラムを使用する場合は、常にプログラミングエラーがないかどうか確認してください。

40.6 SSLをサポートするセキュアWebサーバのセットアップ

クレジットカード情報などの機密データがWebサーバとクライアント間で転送される場合は常に、接続が安全で、認証により暗号化されていることが必要です。`mod_ssl`は、クライアントとWebサーバ間のHTTP通信に、SSL (secure sockets layer) およびTLS (transport layer security) プロトコルを使用する、強力な暗号化を提供します。SSL/TLSを使用することにより、Webサーバとクライアント間でプライベートな接続が確立されます。データの整合性が保証され、クライアントとサーバ間で相互認証ができるようになります。

この目的で、サーバは、URLに対するリクエストに応答する前に、サーバの有効な識別情報を含むSSL証明書を送ります。これにより、サーバが唯一の正当な通信相手であることが保証されます。加えて、この証明書は、クライアントとサーバの間の暗号化された通信が、重要な内容がプレーンテキストとして見られる危険なしに、情報を転送できることを保証します。

`mod_ssl`は、SSL/TLSプロトコル自体は実装しませんが、ApacheとSSLライブラリ間のインタフェースとして機能します。SUSE Linux Enterprise Serverでは、OpenSSLライブラリが使用されます。OpenSSLは、Apacheとともに自動的にインストールされます。

Apacheで`mod_ssl`を使用する場合の最もはっきりした影響は、URLのプレフィックスが`http://`ではなく`https://`となることです。

40.6.1 SSL証明書の作成

SSL/TLSをWebサーバで使用するには、SSL証明書を作成する必要があります。この証明書は、両者が互いに相手を識別できるように、Webサーバとクライアント間の認証に必要です。証明書の整合性を確認するには、すべてのユーザが信用する者によって署名される必要があります。

3種類の証明書を作成することができます。テストの目的のみの「ダミー証明書」、あらかじめ定義されている信用する一部のユーザグループ用の自己署名付き証明書、および公的な独立団体のCA (Certificate Authority) によって署名される証明書です。

証明書の作成には、基本的に2つのステップで行うことができます。はじめに、CAの秘密鍵が生成され、次に、この鍵を使用してサーバ証明書が署名されます。

ティップ: 詳細情報

SSL/TSLの概念および定義の詳細については、http://httpd.apache.org/docs/2.2/ssl/ssl_intro.htmlを参照してください。

ダミー「証明書の作成」

ダミー証明書の生成は簡単です。/usr/bin/gensslcertスクリプトを呼び出すだけです。このスクリプトは次のファイルを作成または上書きします。

- /etc/apache2/ssl.crt/ca.crt
- /etc/apache2/ssl.crt/server.crt
- /etc/apache2/ssl.key/server.key
- /etc/apache2/ssl.csr/server.csr

ca.crtのコピーは、ダウンロード用に/srv/www/htdocs/CA.crtにも配置されます。

重要項目

ダミー証明書は、実動システム上では使用しないでください。テストの目的のみで使用してください。

自己署名付き証明書の作成

イントラネットまたは定義されている一部のユーザグループ用にセキュアWebサーバをセットアップするとき、独自のCA (Certificate Authority)を通じて証明書に署名するので十分な場合があります。

自己署名付き証明書の作成手順は、対話形式の9つのステップで構成されています。/usr/share/doc/packages/apache2ディレクトリに移動し、次の

コマンドを実行します。/mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/ custom。このディレクトリ以外からこのコマンドを実行しないでください。プログラムは、一連のプロンプトを表示します。この一部には、ユーザ入力が必要なものもあります。

手順 40.1 mkcert.shを使用した自己署名付き証明書の作成

1 証明書を使用してシグネチャアルゴリズムを決定します

一部の古いブラウザでDSAを使用すると問題があるため、RSA (デフォルトのR)を選択します。

2 CA用RSA秘密鍵を生成(1024ビット)

操作の必要はありません。

3 CAへのX.509証明書署名要求を生成

ここで、CAの識別名を作成します。このとき、国名または組織名など、いくつかの質問に答える必要があります。ここで入力した内容が証明書に含まれるため、有効なデータを入力します。すべての質問に答える必要はありません。該当しない、または空白のままにする場合は、「.」を使用します。」一般名は、CA自体の名前です。My company CAなど、意味のある名前を選択します。

4 CAによる署名用のX.509証明書を生成

証明書バージョン3を選択します(デフォルト)。

5 SERVER用のRSA秘密鍵を生成(1024ビット)

操作の必要はありません。

6 SERVERへのX.509証明書署名要求を生成

ここで、サーバの鍵の識別名を作成します。質問は、CAの識別名で答えたものとほぼ同じです。ここで入力するデータがWebサーバに適用されますが、CAのデータと同一である必要はありません(サーバが別の場所に位置する場合など)。

重要項目: 一般名の選択

ここで入力する一般名は、セキュアサーバの完全修飾ホスト名 (`www.example.com` など) である必要があります。完全修飾ホスト名でない場合、Webサーバへのアクセス時、証明書がサーバと一致していないという警告がブラウザに表示されます。

7 独自のCAによる署名付きX.509証明書を生成

証明書バージョン3を選択します(デフォルト)。

8 セキュリティ用のパスフレーズのあるCAのRSA秘密鍵の暗号化

CAの秘密鍵をパスワードで暗号化することをお勧めします。そのため、Yを選択し、パスワードを入力します。

9 セキュリティ用のパスフレーズのあるSERVERのRSA秘密鍵の暗号化

秘密鍵をパスワードで暗号化すると、Webサーバを起動するたびにこのパスワードを入力するよう求められます。このため、Webサーバのブートおよび再起動時にサーバを自動的に起動するのが難しくなります。したがって、一般的に、この質問にはNと答えます。パスワードで暗号化しないと鍵は保護されないため、この鍵へのアクセスは許可されたユーザのみに限定する必要があることに注意してください。

重要項目: サーバ鍵の暗号化

サーバ鍵をパスワードで暗号化する場合

は、`/etc/sysconfig/apache2`の`APACHE_TIMEOUT`の値を増やします。値を増やさないと、サーバを起動しようとする試みが停止する前に、パスフレーズを入力するのに十分な時間がなくなります。

スクリプトの結果ページに、生成された鍵と証明書の一覧が表示されます。スクリプトの出力とは異なり、ファイルはローカルディレクトリの`conf`内ではなく、適切な場所である、`/etc/apache2/`内に生成されます。

最後のステップとして、Webブラウザ内の認識および信用されたCAの一覧に含まれるように、ユーザがアクセスできる場所に`/etc/apache2/ssl.crt/ca.crt`からCA証明書ファイルをコピーします。コピーしない場合、ブラウ

ずは、この証明書が不明な認証局から発行されたものであると見なします。証明書は1年間有効です。

重要項目: 自己署名付き証明書

自己署名付き証明書は、CA (Certificate Authority)として認識および信用するユーザによってアクセスされるWebサーバ上でのみ使用します。自己署名付き証明書をオンラインショップなどで使用することはお勧めしません。

公式に署名された証明書の取得

証明書に署名する公式なCA (Certificate Authority)は、多数存在します。証明書は、信用のあるサードパーティによって署名されるため、完全に信用できます。通常、一般に運営されているセキュアWebサーバでは、証明書が公式に署名されます。

最も良く知られている公式なCAには、Thawte (<http://www.thawte.com/>) またはVerisign (<http://www.verisign.com>)があります。これらや、その他のCAは、すべてのブラウザにすでにコンパイルされているため、これらのCAによって署名された証明書は、ブラウザによって自動的に許可されます。

公式に署名された証明書を要求するとき、CAに証明書を送信しません。代わりに、CSR (Certificate Signing Request)を発行します。CSRを作成するには、`/usr/share/ssl/misc/CA.sh -newreq`スクリプトを呼び出します。

はじめに、スクリプトは、CSRの暗号化に使用されているパスワードを問い合わせてきます。その後、識別名を入力するよう求められます。このとき、国名または組織名など、いくつかの質問に答える必要があります。ここで入力した内容が証明書に含まれ、確認されるため、有効なデータを入力します。すべての質問に答える必要はありません。該当しない、または空白のままにする場合は、「.」を使用します。」一般名は、CA自体の名前です。My company CAなど、意味のある名前を選択します。最後に、チャレンジパスワードおよび代替の企業名を入力する必要があります。

スクリプトを呼び出したディレクトリでCSRを検索します。ファイルには、`newreq.pem`という名前が付きます。

40.6.2 SSLサポートのあるApacheの設定

Webサーバ側のSSLとTLS要求用のデフォルトのポートは443です。ポート80をリスンする「通常」のApacheと、ポート443をリスンするSSL/TLS対応のApacheとの間に競合は生じません。通常、ポート80とポート443への要求はそれぞれ別の仮想ホストが処理し、別の仮想サーバに送られます。

重要項目: ファイアウォール設定

ポート443でSSL対応のApache用のファイアウォールを開くことを忘れないでください。ファイアウォールは、[43.4.1項「YaSTを使ったファイアウォールの設定」](#) (900 ページ)で説明されているように、YaSTを使用して設定できます。

SSLを使用するには、グローバルサーバ設定でSSLが有効化されている必要があります。`/etc/sysconfig/apache2`をエディタで開き、`APACHE_MODULES`を検索します。「`ssl`」がモジュールのリストに存在しない場合は、追加します(デフォルトでは`mod_ssl`が有効化されている)。次に、`APACHE_SERVER_FLAGS`を検索し、「`SSL`」を追加します。サーバ証明書をパスワードで暗号化している場合は、`APACHE_TIMEOUT`の値を増やし、Apacheの起動時にパスワードを入力するのに十分な時間が与えられるようにします。これらの変更を適用するため、サーバを再起動します。再ロードでは不十分です。

仮想ホスト設定ディレクトリには、SSL固有ディレクティブが詳細に記述されている`/etc/apache2/vhosts.d/vhost-ssl.template`テンプレートが含まれています。一般的な仮想ホスト設定については、[仮想ホスト設定項](#) (813 ページ)を参照してください。

始めるには、テンプレートを`/etc/apache2/vhosts.d/mySSL-host.conf`にコピーして編集します。次のディレクティブの値を調整するだけです。

- `DocumentRoot`
- `ServerName`
- `ServerAdmin`
- `ErrorLog`

- TransferLog

重要項目: 名前ベースの仮想ホストとSSL

IPアドレスが1つだけの1台のサーバで、複数のSSL対応の仮想ホストを実行することはできません。そのような構成のサーバに接続するユーザは、URLを訪問するたびに、証明書がサーバ名と一致しないという警告メッセージを受け取ることになります。有効なSSL証明書に基づいて通信を行うには、SSL対応のドメインごとに、個別のIPアドレスまたはポートが必要です。

40.7 セキュリティ問題の回避

公共のインターネットに公開しているWebサーバについては、管理面での不断の努力が求められます。ソフトウェアと、偶然の設定ミスの両方に関連したセキュリティの問題が発生することは避けられません。それらに対処するためのいくつかのヒントを紹介します。

40.7.1 最新版のソフトウェア

Apacheソフトウェアに脆弱性が見つかると、SUSEからセキュリティ上の勧告が出されます。これには、脆弱性を修正するための指示が含まれているので、できる限り早く適用すべきです。SUSEセキュリティ通知は、次の場所から入手できます。

- **Webページ** <http://www.novell.com/linux/security/securitysupport.html>
- **メーリングリスト** <http://en.opensuse.org/Communicate#Mailinglists>
- **RSSフィード** http://www.novell.com/linux/security/suse_security.xml

40.7.2 DocumentRootのパーミッション

SUSE Linux Enterprise Serverのデフォルトでは、DocumentRootディレクトリの/srv/www/htdocsおよびCGIディレクトリの/srv/www/cgi-binの所有者はユーザおよびグループのrootになっています。これらのパーミッションは変更しないでください。これらのディレクトリにすべてのユーザが書き込めるようにすると、どのユーザでもそこにファイルを配置できるようになります。その後これらのファイルは、Apacheによりwwwrunのパーミッションで実行されます。その結果、意図しない仕方で、ユーザがファイルシステムのリソースにアクセスできるようになる可能性があります。/srv/wwwのサブディレクトリを使用して仮想ホストのDocumentRootおよびCGIディレクトリを配置し、このユーザおよびグループのrootがディレクトリとファイルの所有者であることを確認します。

40.7.3 ファイルシステムアクセス

デフォルトでは、ファイルシステム全体へのアクセスは、/etc/apache2/httpd.confで定義されています。これらのディレクティブは決して上書きしないでください。ただし、特に、Apacheが読み取ることができるすべてのディレクトリへのアクセスは有効にしてください(詳細は、[基本的な仮想ホスト設定項](#) (816 ページ)を参照してください)。このためには、パスワードまたはシステム設定ファイルなど重要なファイルは外部から読み取ることができないことを確認します。

40.7.4 CGIスクリプト

Perl、PHP、SSIまたは他のプログラミング言語によるインタラクティブなスクリプトは、事実上、任意のコマンドを実行できるため、一般的なセキュリティの問題が存在します。サーバから実行されるスクリプトは、サーバの管理者が信用するソースからのみインストールされる必要があります。一般的には、ユーザが独自のスクリプトを実行できる環境は適切ではありません。また、すべてのスクリプトに対してセキュリティ監査を行うこともお勧めします。

スクリプトの管理をできるだけ簡単にするため、CGIスクリプトの実行をグローバルに許可するのではなく、通常、特定のディレクトリに制限されてい

ます。設定には、ディレクティブのScriptAliasおよびOption ExecCGIが使用されます。SUSE Linux Enterprise Serverのデフォルト設定では、任意の場所からのCGIスクリプトの実行は許可されていません。

すべてのCGIスクリプトは同一のユーザとして実行するため、異なるスクリプトが互いに競合する可能性があります。suEXECモジュールは、CGIスクリプトを別のユーザとグループで実行できるようにします。

40.7.5 ユーザディレクトリ

ユーザディレクトリを有効化するとき(mod_userdirまたはmod_rewriteを使用)は、.htaccessファイルを許可しないことをお勧めします。このファイルは、ユーザによるセキュリティ設定の上書きを許可します。AllowOverrideディレクティブを使用して、少なくとも、ユーザの操作を制限する必要があります。SUSE Linux Enterprise Serverでは、.htaccessファイルはデフォルトで有効化されていますが、ユーザはmod_userdirを使用するときいずれのOptionディレクティブも上書きすることは許可されていません(/etc/apache2/mod_userdir.conf設定ファイルを参照してください)。

40.8 トラブルシューティング

Apacheが起動しないと、Webページにアクセスすることはできず、ユーザがWebサーバに接続することもできないので、問題の原因を見つけ出すことは重要です。ここでは、どこを見てエラーの理由を探したらよいかということと、チェックすべき重要な点について説明します。

はじめに、rcapache2(40.3項「**Apacheの起動および停止**」(824 ページ)を参照)はエラーについて詳しく報告するので、Apacheの運用で実際に使用すればとても役立ちます。ときには、Webサーバの起動と停止に/usr/sbin/httpd2バイナリを使用している場合もあります。その代わりにrcapache2スクリプトを使用します。rcapache2は、設定エラーを解決するためのヒントも提供します。

第2に、ログファイルの重要性を十分に認識してください。致命的なエラーとそうでないエラーのどちらの場合でも、Apacheのログファイル、主にエラーログファイルを見て、原因を探してください。さらに、ログファイルにさらに詳細な情報を記録することが必要な場合には、LogLevelディレクティブ

で、記録されるメッセージの詳細を制御することができます。デフォルトでは、エラーログファイルは、`/var/log/apache2/error_log`にあります。

ティップ: 簡単なテスト

`tail -F /var/log/apache2/my_error_log`コマンドで、Apacheのログメッセージを確認します。それから、`rcapache2 restart`を実行します。そして、ブラウザでの接続をもう一度試みて、出力を確認してください。

よくある間違いは、サーバのファイアウォール設定で、Apache用のポートを開けていないことです。YaSTでApacheを設定する場合には、この点を扱うための別のオプションが存在します(40.2.2項「[ApacheをYaSTで設定する](#)」(817 ページ)を参照してください)。Apacheを手動で設定する場合は、YaSTのファイアウォールモジュールを使用してHTTPとHTTPS用のファイアウォールポートを開きます。

このようにしても、エラーを特定できない場合には、http://httpd.apache.org/bug_report.htmlの、オンラインのApacheバグデータベースをチェックしてください。加えて、<http://httpd.apache.org/userslist.html>のメーリングリストで、Apacheのユーザコミュニティに参加することができます。お勧めできるニュースグループは、<comp.infosystems.www.servers.unix>です。

40.9 詳細情報

apache2-docパッケージには、ローカルインストールおよび参照用にそれぞれローカライズされている完全なApacheマニュアルが含まれています。このマニュアルはデフォルトではインストールされません。このマニュアルの最も簡単なインストール方法としては、`yast -i apache2-doc`コマンドを使用します。Apacheマニュアルは、インストールされると、<http://localhost/manual/>から表示できるようになります。また、Webの<http://httpd.apache.org/docs-2.2/>からもアクセスできます。SUSE固有の設定に関するヒントについては、`/usr/share/doc/packages/apache2/README.*`を参照してください。

40.9.1 Apache 2.2

Apache 2.2の新機能のリストは、http://httpd.apache.org/docs/2.2/new_features_2_2.htmlを参照してください。バージョン2.0から2.2へのアップグレード情報も<http://httpd.apache.org/docs-2.2/upgrading.html>で参照できます。

40.9.2 Apacheモジュール

の外部Apacheモジュールの詳細については、以下を参照してください。[40.4.5 項「外部モジュール」](#) (833 ページ)。

mod-apparmor

<http://en.opensuse.org/AppArmor>

mod_perl

<http://perl.apache.org/>

mod_php5

<http://www.php.net/manual/en/install.unix.apache2.php>

mod_python

<http://www.modpython.org/>

40.9.3 開発

Apacheモジュールの開発、またはApache Webサーバプロジェクトへの参加に関する情報については、次を参照してください。

Apache開発情報

<http://httpd.apache.org/dev/>

Apache開発者ドキュメント

<http://httpd.apache.org/docs/2.2/developer/>

PerlおよびCを使用したApacheモジュールの作成

<http://www.modperl.com/>

40.9.4 その他の情報源

SUSE Linux Enterprise ServerのApacheに固有な問題が発生したときは、Technical Information Search(技術情報検索)(<http://www.novell.com/support>)を参照してください。Apacheの沿革は、http://httpd.apache.org/ABOUT_APACHE.htmlで参照できます。このページでは、Apacheというサーバ名の由来についても説明しています。

Squidプロキシサーバ

Squidは、LinuxおよびUNIXプラットフォームで普及しているプロキシキャッシュです。これは、WebまたはFTPサーバなど、要求されたインターネットオブジェクトを、サーバよりも要求しているワークステーションに近いマシン上に格納することを意味します。Squidは、応答時間や低帯域幅の使用を最適化するために複数の階層上でセットアップされます。エンドユーザにとって透過的なモードである場合さえあります。squidGuardを利用すれば、Webコンテンツをフィルタリングすることができます。

Squidはプロキシキャッシュとして機能します。クライアント(この場合はWebブラウザ)からのオブジェクト要求をサーバにリダイレクトします。要求されたオブジェクトがサーバから到着すると、クライアントに配信され、そのコピーがディスクキャッシュに格納されます。キャッシングの利点の1つは、様々なクライアントが同じオブジェクトを要求した場合に、これらのオブジェクトをハードディスクのキャッシュから提供できることです。これにより、クライアントはインターネットから取得する場合に比べてはるかに高速にデータを受信できます。また、ネットワークトラフィックも減少します。

Squidは、実際のキャッシングとともに、プロキシサーバの通信階層にまたがる負荷の分散、プロキシにアクセスする全クライアントの厳密なアクセス制御リストの定義、他のアプリケーションを使用した特定のWebページへのアクセスの許可または拒否、ユーザのアクセスパターンの調査を目的としたアクセス回数の多いWebサイトに関する統計の生成など、多様な機能を備えています。Squidは汎用プロキシではありません。通常は、HTTP接続のみのプロキシを行います。また、FTP、Gopher、SSLおよびWAISの各プロトコルをサポートしていますが、Real Audio、newsまたはビデオ会議など、他のインターネットプロトコルはサポートしていません。Squidは様々なキャッシュ間

に通信を提供するUDPプロトコルのみをサポートしているため、他の多くのマルチメディアプログラムはサポートされません。

41.1 プロキシキャッシュに関する注意事項

プロキシキャッシュとして、Squidは複数の方法で使用されます。ファイアウォールと組み合わせると、セキュリティに役立ちます。複数のプロキシを一緒に使用できます。また、キャッシュされるオブジェクトのタイプ、およびその期間も決定できます。

41.1.1 Squidとセキュリティ

Squidをファイアウォールと併用し、プロキシキャッシュを使用して社内ネットワークを外部から保護することもできます。ファイアウォールは、Squidを除く外部サービスに対する全クライアントのアクセスを拒否します。すべてのWeb接続は、プロキシを使用して確立する必要があります。この設定では、SquidはWebアクセスを完全に制御します。

ファイアウォール設定にDMZが含まれている場合、プロキシはこのゾーン内で動作しなければなりません。「[透過的な](#)」プロキシの実装方法については、[41.5項「透過型プロキシの設定」](#) (864 ページ)を参照してください。この場合、プロキシに関する情報が必要とされないため、クライアントの設定が簡略化されます。

41.1.2 複数のキャッシュ

複数のSquidインスタンスを設定して、これらの間でオブジェクトを交換できます。これにより、システム全体の負荷を削減し、ローカルネットワーク内の既存のオブジェクトの検出率を高めることができます。また、キャッシュから兄弟キャッシュまたは親キャッシュにオブジェクト要求を転送できるように、キャッシュ階層を設定することも可能です。これにより、ローカルネットワーク内の他のキャッシュから、またはソースから直接、オブジェクトを取得できるようになります。

ネットワークトラフィック全体が増大することは望ましくないため、キャッシュ階層に適切なトポロジを選択することがきわめて重要です。大規模ネットワークの場合は、サブネットワークごとにプロキシサーバを設定して親プロキシに接続し、親プロキシはISPのプロキシキャッシュに接続すると有効です。

この通信はすべて、UDPプロトコルの最上位で実行されるICP (Internet cache protocol)により処理されます。キャッシュ間のデータ転送は、TCPベースのHTTP (hyper text transmission protocol)により処理されます。

どのサーバからオブジェクトを取得するのが最も適切であるかを検出するために、あるキャッシュからすべての兄弟プロキシにICPリクエストが送信されます。各兄弟プロキシは、オブジェクトが検出された場合はHITコード、検出されなかった場合はMISSを使用し、ICPレスポンスを介してリクエストに応答します。複数のHITレスポンスが検出された場合、プロキシサーバは、最も短時間で応答したキャッシュまたは最も近接するキャッシュなどのファクタに従ってダウンロード元のサーバを決定します。リクエストを満たすレスポンスが受信されなければ、リクエストは親キャッシュに送信されます。

ティップ

ネットワーク上の様々なキャッシュ内でオブジェクトの重複を回避するために、CARP (Cache Array Routing Protocol)やHTCP (Hypertext Cache Protocol)など、他のICPプロトコルが使用されます。ネットワーク上で維持されるオブジェクトが多くなるほど、必要なオブジェクトを検出できる可能性が高くなります。

41.1.3 インターネットオブジェクトのキャッシュ

ネットワーク上で使用可能なオブジェクトがすべてスタティックであるとは限りません。動的に生成されるCGIページ、アクセス件数カウンタ、暗号化されたSSLコンテンツドキュメントが多数存在します。この種のオブジェクトは、アクセスされるたびに变化するためキャッシュされません。

その他のオブジェクトについても、キャッシュにどのくらいの期間残しておくかという問題があります。これを決定するために、オブジェクトが取り得るさまざまな状態を定義し、キャッシュ内のすべてのオブジェクトに1つの状

態を割り当てます。Webサーバとプロキシサーバは、これらのオブジェクトに「Last modified」や「Expires」などのヘッダおよび対応する日付を追加することで、オブジェクトの状態を検出します。その他、オブジェクトをキャッシュしないように指定するヘッダも使用されます。

ハードディスクの空き容量不足が原因で、通常、キャッシュ内のオブジェクトはLRU (Least Recently Used)などのアルゴリズムを使用して置換されます。これは、基本的には、長期間要求されていないオブジェクトがプロキシにより消去されることを意味します。

41.2 システム要件

最も重要なのは、システムにかかる最大ネットワーク負荷を判断することです。したがって、負荷のピークに注意する必要があります。ピーク時の負荷が1日の平均負荷の4倍を超えることもあるためです。疑わしい場合は、システム要件を多めに見積もることをお勧めします。これは、Squidの動作状態が処理能力の限界に近づくと、サービス品質が著しく低下する可能性があるためです。次の各項では、システム要件を重要度に従って説明します。

41.2.1 ハードディスク

速度はキャッシュ処理に重要な役割を果たすため、この要件には特に注意する必要があります。ハードディスクの場合、このパラメータはランダムシーク時間と呼ばれ、ミリ秒単位で計測されます。Squidがハードディスクとの間で読み書きするデータブロックは比較的少数である傾向があるため、データのスループットよりもハードディスクのシーク時間の方が重要です。プロキシに使用する場合は、回転速度の高い(つまり読取り/書込みヘッドが必要な位置に迅速に移動する)ハードディスクを選択するのが適切です。システムを高速化するには、同時に多数のディスクを使用する方法や、ストライピングRAIDアレイを使用する方法があります。

41.2.2 ディスクキャッシュのサイズ

キャッシュ容量が小さいと、簡単にいっぱいになってしまい、要求頻度の低いオブジェクトが新規オブジェクトで置換されるため、HIT (要求された既存のオブジェクトの検出)の可能性は低くなります。逆に、キャッシュに1GBが

使用可能で、ユーザが1日に10MB分しかアクセスしなければ、キャッシュがいっぱいになるまでに100日以上かかることになります。

必要なキャッシュサイズを判断する場合に最も簡単なのは、接続の最大転送速度を考慮することです。1MBit/sの接続の場合、最大転送速度は125KB/sになります。このトラフィックがすべてキャッシュに入ると、1時間で合計450MBとなり、このトラフィックがすべて8時間の営業時間帯にのみ発生すると仮定すれば、1日に3.6GBに達します。通常、接続が上限まで使用されることはないため、キャッシュで処理される合計データ量は約2GBと想定できます。このため、Squidで1日にブラウズされたデータをキャッシュに保持する例では、2GBのディスク容量が必要となります。

41.2.3 RAM

Squidに必要なメモリ容量(RAM)は、キャッシュ内のオブジェクト数に比例します。また、Squidでは、キャッシュオブジェクト参照と要求頻度の高いオブジェクトの検索を高速化するために、これらのデータがメインメモリに格納されます。ランダムアクセスメモリの方が、ハードディスクよりも高速です。

その他、Squidでは、処理された全IPアドレスの表、正確なドメインネームキャッシュ、最もアクセス頻度の高いオブジェクト、アクセス制御リスト、バッファなどのデータもメモリに保持する必要があります。

ディスクにスワップする必要があるとシステムパフォーマンスが大幅に低下するため、Squidプロセス用に十分なメモリを用意する必要があります。キャッシュメモリの管理には、`cachemgr.cgi`ツールを使用できます。このツールの詳細については、[41.6項「cachemgr.cgi」](#) (867ページ)を参照してください。大量のネットワークトラフィックのあるサイトでは、4GB以上のメモリを持つAMD64またはIntel 64システムを使用することを考慮してください。

41.2.4 CPU

Squidは、CPU集約型のプログラムではありません。プロセッサの負荷が増大するのは、キャッシュの内容がロードまたはチェックされる間のみです。マルチプロセッサマシンを使用しても、システムパフォーマンスは向上しません。効率を高めるには、高速ディスクまたは増設メモリを購入することをお勧めします。

41.3 Squidの起動

SquidはSUSE® Linux Enterprise Serverで事前に設定されているため、インストール直後に起動できます。スムーズに起動するように、インターネットおよび少なくとも1つのネームサーバにアクセスできるようにネットワークを設定してください。ダイナミックDNS設定でダイヤルアップ接続を使用すると、問題が発生する可能性があります。このような場合は、少なくともネームサーバを明確に入力してください。というのは、`/etc/resolv.conf`内でDNSサーバが検出されないとSquidが起動しないためです。

41.3.1 Squidの起動コマンドと停止コマンド

Squidを起動するには、root権限でコマンドラインに「`rcsquid start`」と入力します。初期起動時には、最初に `/var/cache/squid`内でキャッシュのディレクトリ構造を定義する必要があります。この操作は、`/etc/init.d/squid`起動スクリプトにより自動的に実行され、完了までに数秒ないし数分かかります。右側に緑で完了と表示されたら、Squidは正常にロードされています。ローカルシステム上でSquidの機能をテストするには、ブラウザでプロキシとして「localhost」、ポートとして「3128」を入力します。

ユーザ全員にSquidおよびインターネットへのアクセスを許可するには、設定ファイル`/etc/squid/squid.conf`内のエントリを`http_access deny all`から`http_access allow all`に変更します。ただし、その場合は、この操作によりSquidが完全に誰でもアクセス可能になることに注意してください。したがって、プロキシへのアクセスを制御するACLを定義します。この詳細については、[41.4.2項「アクセス制御オプション」](#) (862 ページ)ファイルを参照してください。

設定ファイル`/etc/squid/squid.conf`を変更した後、Squidで変更後の設定ファイルを再ロードする必要があります。それには、`rcsquidreload`コマンドを使用します。または、「`rcsquid restart`」と入力してSquidを完全に再起動します。

プロキシが稼働しているかどうかを確認するには、`rcsquidstatus`コマンドを使用します。Squidをシャットダウンするには、`rcsquidstop`コマンドを使用します。Squidは、クライアントへの接続が切断されてデータがディスクに書き込まれるまで最大30秒(`/etc/squid/squid.conf`の

shutdown_lifetimeオプション) 待機するため、終了までに少し時間がかかることがあります。

警告: Squidの終了

killまたはkillallを使ってSquidを終了すると、キャッシュが破損してしまう可能性があります。Squidを再起動できるようにするには、破損したキャッシュを完全に削除する必要があります。

Squidが正常に起動しても短時間で停止する場合は、ネームサーバエントリに誤りがないかどうかと、/etc/resolv.confファイルが欠落していないかどうかを確認してください。起動エラーの原因は、Squidにより/var/log/squid/cache.logファイルに記録されます。システムのブート時にSquidを自動的にロードする必要がある場合は、YaSTランレベルエディタを使用してSquidを必要なランレベルで有効にしてください。詳細については、[8.5.12項「システムサービス\(ランレベル\)」](#) (181 ページ)を参照してください。

Squidをアンインストールしても、キャッシュ階層やログファイルは削除されません。これらを削除するには、/var/cache/squidディレクトリを手動で削除します。

41.3.2 ローカルDNSサーバ

サーバで独自ドメインを管理しない場合も、ローカルDNSサーバをセットアップすると有効です。ローカルDNSサーバは単にキャッシュ専用ネームサーバとして機能し、特に設定しなくてもルートネームサーバを介してDNSリクエストを解決できます([33.3項「ネームサーバBINDの起動」](#) (684 ページ)を参照)。ローカルDNSサーバを有効にする方法は、インターネット接続の設定時にダイナミックDNSを選択したかどうかによって異なります。

ダイナミックDNS

通常、ダイナミックDNSを使用すると、インターネット接続が確立されるときプロバイダによってDNSサーバが設定され、ローカルの/etc/resolv.confファイルが自動的に変更されます。この動作は、/etc/sysconfig/network/configファイル内でsysconfig変数の

MODIFY_RESOLV_CONF_DYNAMICALYを「yes」に設定することで制御されます。この変数をYaST sysconfigエディタを使用して「no」に設定します([20.3.1項「YaSTのsysconfigエディターを使ってシステム設定を変](#)

更する」(442 ページ)」を参照してください)。そして、`/etc/resolv.conf`ファイルに、ローカルのDNSサーバとして「localhost」、そのIPアドレスとして「127.0.0.1」を入力します。このようにすれば、Squidは常に、起動時にローカルのネームサーバを検出できます。

プロバイダのネームサーバにアクセスするには、`/etc/named.conf`設定ファイル内の`forwarders`にサーバ名とそのIPアドレスを入力します。ダイナミックDNSを使用すると、この動作を接続の確立時に自動的に実行できます。それには、`sysconfig`変数の`MODIFY_NAMED_CONF_DYNAMICALLY`を「YES」に設定します。

スタティックDNS

スタティックDNSを使用する場合は、接続の確立時にいずれの自動DNS調整も行われないため、`sysconfig`変数を変更する必要はありません。ただし、`/etc/resolv.conf`ファイルにローカルのDNSサーバを入力する必要があります。また、プロバイダのスタティックなネームサーバにアクセスするには、`/etc/named.conf`設定ファイルに、サーバ名`forwarders`とそのIPアドレスを手動で入力する必要があります。

ティップ: DNSとファイアウォール

ただし、ファイアウォールを実行している場合は、DNSリクエストがファイアウォールを通過できることを確認してください。

41.4 設定ファイル `/etc/squid/squid.conf`

Squidのプロキシサーバ設定は、すべて`/etc/squid/squid.conf`ファイル内で行います。Squidを初めて起動する場合、このファイル内で設定を変更する必要はありませんが、外部クライアントは最初はアクセスを拒否されます。プロキシはlocalhostに使用できます。デフォルトポートは3128です。プリインストール済みの`/etc/squid/squid.conf`設定ファイルには、オプションの詳細と多数の例が用意されています。ほぼすべてのエントリは(コメント行を示す) `#`記号で始まり、関連する指定が行末にあります。示されている値は、ほぼ常にデフォルト値に関係しているため、パラメータを実際に変更せずにコメント記号を削除しても、ほとんどの場合に影響はありません。

サンプルはそのまま残し、変更したパラメータと共にオプションを次の行に挿入することをお勧めします。この方法では、簡単にデフォルト値に戻し、変更と比較することができます。

ティップ: 更新後の設定ファイルの変更について

Squidを旧バージョンから更新した場合は、新規の/etc/squid/squid.confを編集し、旧バージョンのファイルで行った変更のみを適用することをお勧めします。旧バージョンのsquid.confファイルを使用すると、オプションが変更されたり新たな変更が加えられているために、設定が機能しなくなる危険性があります。

41.4.1 一般設定オプション(選択)

http_port 3128

これは、Squidがクライアントリクエストをリスンするポートです。デフォルトポートは3128ですが、8080も一般的です。必要な場合は、複数のポート番号を空白で区切って指定します。

cache_peer hostname type proxy-port icp-port

ここでは、たとえばISPのプロキシを使用する場合に、親プロキシを入力します。hostnameには、使用するプロキシの名前とIPアドレスを入力し、typeには親プロキシを入力します。proxy-portには、ブラウザで使用する親の演算子でも指定されているポート番号(通常は8080)を入力します。icp-portは、7に設定するか、親のICPポートが不明で、その使用がプロバイダに無関係な場合は0に設定します。また、ICPプロトコルの使用を禁止するため、ポート番号に続けてdefaultおよびno-queryを指定することもできます。このように指定すると、Squidはプロバイダのプロキシに関する限り通常のブラウザのように動作します。

cache_mem 8 MB

このエントリは、Squidで頻繁に求められる応答に対して使用できるメモリ容量を定義します。デフォルトは8MBです。これは、Squidのメモリ使用量を指定せず、メモリ使用量を超えても構いません。

cache_dir ufs /var/cache/squid/ 100 16 256

cache_dirエントリは、すべてのオブジェクトが格納されるディスク上のディレクトリを定義します。末尾の数値は、使用される最大ディスク領域

(単位MB)と第1レベルと第2レベルのディレクトリ数を示します。ufsパラメータは残しておく必要があります。デフォルトでは、/var/cache/squidディレクトリに100MBのディスク領域を使用して16個のサブディレクトリが作成され、各サブディレクトリにそれぞれ256個以上のサブディレクトリが含まれます。使用するディスク領域を指定するときには、予備のディスク領域を十分に残しておきます。ここでは、使用可能ディスク領域の50～80%が最も有効です。ディレクトリが多すぎるとパフォーマンスが低下する可能性があるため、ディレクトリに関する最後の2つの数値を増やす場合は注意してください。複数のディスクでキャッシュを共有する場合は、複数のcache_dir行を入力します。

```
cache_access_log /var/log/squid/access.log , cache_log /var/log/squid/cache.log ,  
cache_store_log /var/log/squid/store.log
```

これらの3つのエントリは、Squid!によるすべてのアクションの記録先のパスを指定します。通常、ここでは何も変更しません。Squidの使用負荷が大きい場合は、キャッシュとログファイルを複数のディスクに分散すると有効な場合があります。

```
emulate_httpd_log off
```

このエントリをonに設定すると、読み込み可能なログファイルが生成されます。ただし、一部の評価プログラムではこの形式のログファイルを解釈できません。

```
client_netmask 255.255.255.255
```

このエントリを使用して、ログファイルでクライアントのIPアドレスをマスクします。ここで「255.255.255.0」と入力すると、IPアドレスの最終桁はゼロに設定されます。このようにして、クライアントのプライバシーを保護できます。

```
ftp_user Squid@
```

このエントリでは、Squidで匿名FTPログインに使用する必要のあるパスワードを設定します。一部のFTPサーバには電子メールアドレスの妥当性が確認されるため、ここでは有効な電子メールアドレスを指定できます。

```
cache_mgr webmaster
```

Squidが予期せずにクラッシュした場合のメッセージ送信先となる電子メールアドレスを指定します。デフォルトはwebmasterです。

logfile_rotate 0

squid-k rotateを実行すると、Squidは保護されたログファイルを循環利用することができます。このプロセス中にファイルに番号が割り当てられ、指定した値に達すると最も古いファイルが上書きされます。SUSE Linux Enterprise Serverではログファイルのアーカイブと削除が設定ファイル/etc/logrotate/squid内で検出された自動実行ジョブにより実行されるため、デフォルト値は0です。

append_domain <domain>

append_domainには、未指定の場合に自動的に追加されるドメインを指定します。通常、ブラウザに「www」と入力して独自Webサーバにアクセスできるように、このエントリには独自ドメインを入力します。

forwarded_for on

このエントリをoffに設定すると、SquidではHTTPリクエストからクライアントのIPアドレスとシステム名が削除されます。設定しない場合は、次のような行がヘッダに追加されます。

```
X-Forwarded-For: 192.168.0.1
```

negative_ttl 5 minutes; negative_dns_ttl 5 minutes

通常、これらの1を変更する必要はありません。ただし、ダイヤルアップ接続を使用する場合は、インターネットが一時的にアクセス不能になる場合があります。Squidは、失敗したリクエストを記録してから新規リクエストの発行を拒絶しますが、インターネット接続は再確立されています。このような場合は、minutesをsecondsに変更し、ブラウザの更新機能を使用すると、数秒後にダイヤルアッププロセスが再開されます。

never_direct allow acl_name

Squidがインターネットからリクエストを直接取り込むのを防ぐには、上記のコマンドを使用して他のプロキシに強制的に接続します。このプロキシは、あらかじめcache_peerに入力しておく必要があります。acl_nameとしてallを指定すると、すべてのリクエストは「親」に直接転送されます。たとえば、プロキシの使用を奨励しているプロバイダや、ファイアウォールによるインターネットへのダイレクトアクセスを拒否しているプロバイダを使用している場合は、この設定が必要な場合があります。

41.4.2 アクセス制御オプション

Squidには、プロキシへのアクセスを制御する詳細システムが用意されています。ACLを実装することで、このシステムを簡単かつ包括的に設定できます。そのためには、順次処理されるルールを持ったリストが必要です。ACLは定義しなければ使用できません。*all*や*localhost*などのデフォルトACLがいくつか用意されています。ただし、ACLを定義しただけで、実際に適用されるわけではありません。実際に適用するには、*http_access*ルールも共に定義する必要があります。

`acl <acl_name> <type> <data>`

ACLの定義には、3つ以上の指定が必要です。名前<*acl_name*>は任意に選択できます。<*type*>は、`/etc/squid/squid.conf`ファイルのACCESS CONTROLSセクションにある多数のオプションから選択できます。<*data*>の指定は個々のACLタイプに応じて異なり、ホスト名、IPアドレスまたはURLを使用するなど、ファイルから読み込むこともできます。次に単純な例を示します。

```
acl mysurfers srcdomain .my-domain.com
acl teachers src 192.168.1.0/255.255.255.0
acl students src 192.168.7.0-192.168.9.0/255.255.255.0
acl lunch time MTWHF 12:00-15:00
```

`http_access allow <acl_name>`

*http_access*では、プロキシの使用を許可されるユーザと、インターネット上でどのユーザが何にアクセスできるかを定義します。この場合、ACLを設定する必要があります。*localhost*および*all*の定義はすでに前述しており、この2つのACLでは*deny*または*allow*を介してアクセスを拒否または許可できます。多数の*http_access*エントリを含むリストを作成できます。各エントリは上から下へと処理され、発生順に従って個々のURLへのアクセスが許可または拒否されます。最後のエントリは、常に*http_access deny all*にする必要があります。次の例では、*localhost*はすべてに自由にアクセスできますが、他のホストはいずれもアクセスを完全に拒否されます。

```
http_access allow localhost
http_access deny all
```

また、このルールの使用を示す次の例では、グループ*teachers*は常にインターネットへのアクセス権を持ちます。グループ*students*は月曜日から金曜日のランチタイム中にのみアクセス権を取得します。

```
http_access deny localhost
http_access allow teachers
http_access allow students lunch time
http_access deny all
```

http_access エントリを含むリストは、読みやすいように `/etc/squid/squid.conf` ファイルの指定の位置にのみ入力してください。つまり、次の2つの間に入力します。

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

および最後の

```
http_access deny all
```

`redirect_program /usr/bin/squidGuard`

このオプションでは、`squidGuard` など、望ましくない URL をブロックできるリダイレクタを指定します。プロキシ認証と適切な ACL を利用すれば、さまざまなユーザグループ個別にインターネットアクセスを制御することができます。`squidGuard` を使用する場合は、個別にインストール、設定する必要があります。

`auth_param basic program /usr/sbin/pam_auth`

ユーザのプロキシ認証が必要な場合は、`pam_auth` などの対応するプログラムを設定します。ユーザが `pam_auth` に初めてアクセスすると、ログインウィンドウが表示され、ユーザ名とパスワードを入力することになります。また、有効なログインを持つクライアント以外はインターネットを使用できないように、ACL も必要です。

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

proxy_auth の後の **REQUIRED** は、許可されるユーザ名のリストまたはそのリストへのパスで置き換えることができます。

`ident_lookup_access allow <acl_name>`

ここでは、ACL で定義されたクライアントすべてについて `ident` リクエストを実行させ、各ユーザの識別情報を検索させます。`<acl_name>` に *all* を適用すると、すべてのクライアントに対して有効になります。また、すべて

のクライアントでidentデーモンを実行する必要があります。Linuxの場合、そのためにはpidentdパッケージをインストールします。Microsoft Windowsの場合は、インターネットからダウンロードできるフリーソフトウェアが提供されています。identが正常に検索されたクライアントのみが許可されるように、対応するACLをここで定義します。

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

この場合も、*REQUIRED*を許可されるユーザ名のリストで置き換えることができます。*ident*を使用すると、その検索がリクエストごとに繰り返されるため、アクセス速度が少し低下する場合があります。

41.5 透過型プロキシの設定

一般的なプロキシサーバの作業では、Webブラウザがプロキシサーバの特定のポートに要求を送信し、プロキシが要求に応じて必要なオブジェクトを提供します。ネットワークで操作する場合には、次のような状況が発生することがあります。

- セキュリティ上の理由から、すべてのクライアントがインターネットでのナビゲーションにはプロキシを使用することを推奨される場合。
- すべてのクライアントが、認識するかどうかに関係なくプロキシを使用する必要がある場合。
- ネットワーク上でプロキシが移動しても、既存のクライアントは古い設定を保持する必要がある場合。

いずれの場合も、透過型プロキシを使用できます。原則はきわめて簡単で、プロキシはWebブラウザのリクエストを捕捉して応答するため、Webブラウザは要求したページを出所を認識せずに受信します。透過型プロキシと呼ばれるのは、このプロセス全体が透過的に実行されるためです。

41.5.1 /etc/squid/squid.conf内の設定オプション

/etc/squid/squid.confファイル内で透過型プロキシの起動と実行に使用できるオプションは、次のとおりです。

- `httpd_accel_host virtual`
- `httpd_accel_port 80`
実HTTPサーバが動作するポート番号
- `httpd_accel_with_proxy on`
- `httpd_accel_uses_host_header on`

41.5.2 SuSEfirewall2を使用したファイアウォール設定

ファイアウォールを介して受信するリクエストをすべて、Squidポートへのポート転送ルールに従ってリダイレクトします。そのためには、[43.4.1項「YaSTを使ったファイアウォールの設定」](#) (900 ページ)で説明しているように、同梱のツールであるSuSEfirewall2を使用します。このツールの設定ファイルは/etc/sysconfig/SuSEfirewall2にあります。この設定ファイルは、適切なエントリで構成されています。透過型プロキシを設定するには、次に示すようにいくつかのファイアウォールオプションを設定する必要があります。

- インターネットを指すデバイス:FW_DEV_EXT="eth1"
- インターネットを指すデバイス:FW_DEV_INT="eth0"

インターネットなど、信頼されない(外部)ネットワークからアクセスが許可される、ファイアウォール上のポートとサービスを定義します(/etc/servicesを参照)。この例では、外部に対してWebサービスのみが提供されます。

```
FW_SERVICES_EXT_TCP="www"
```

安全な(内部)ネットワークからのアクセスが許可される、ファイアウォール上のポートとサービス(TCPサービスとUDPサービスの両方)を定義します(/etc/servicesを参照)。

```
FW_SERVICES_INT_TCP="domain www 3128"  
FW_SERVICES_INT_UDP="domain"
```

この例では、WebサービスとSquid(デフォルトポートは3128)へのアクセスが許可されます。domain「サービスはDNS(ドメインネームサービス)を意味します。」このサービスは一般に使用されます。一般に公開しない場合は、単に上記のエントリから削除して次のオプションをnoに設定します。

```
FW_SERVICE_DNS="yes"
```

最も重要なのは15番目のオプションです。

例 41.1 ファイアウォールの設定:オプション15

```
# 15.)  
# Which accesses to services should be redirected to a local port  
# on the firewall machine?  
#  
# This can be used to force all internal users to surf via your  
# Squid proxy, or transparently redirect incoming Web traffic to  
# a secure Web server.  
#  
# Choice: leave empty or use the following explained syntax of  
# redirecting rules, separated with spaces.  
# A redirecting rule consists of 1) source IP/net,  
# 2) destination IP/net, 3) original destination port and  
# 4) local port to redirect the traffic to, separated by a colon,  
# e.g. "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
```

上記のコメントは、次の構文を示しています。最初に、プロキシファイアウォールにアクセスする内部ネットワークのIPアドレスとネットマスクを入力します。次に、これらのクライアントからのリクエストの送信先となるIPアドレスとネットマスクを入力します。Webブラウザの場合は、ネットワーク0/0を指定します。これは、「あらゆる場所」を意味するワイルドカードです。」その後、これらのリクエストの送信先となるオリジナルポートを入力し、最後に全リクエストのリダイレクト先となるポートを入力します。SquidはHTTP以外のプロトコルをサポートしているため、要求は他のポートからFTP(ポート21)、HTTPSまたはSSL(ポート443)などのプロキシにリダイレクトされます。この例では、Webサービス(ポート80)がプロキシポート(ポート

3128)にリダイレクトされます。他にも追加するネットワークやサービスがある場合は、対応するエントリに空白1個で区切って指定する必要があります。

```
FW_REDIRECT="192.168.0.0/16,0/0,tcp,80,3128 192.168.0.0/16,0/0,tcp,21,3128"  
FW_REDIRECT="192.168.0.0/16,0/0,udp,80,3128 192.168.0.0/16,0/0,udp,21,3128"
```

ファイアウォールとそれを使用した新規設定を開始するには、`/etc/sysconfig/SuSEfirewall12`ファイル内のエントリを変更します。エントリ`START_FW`を`"yes"`に設定する必要があります。

41.3項「Squidの起動」 (856 ページ)のように、Squidを起動します。正常に動作しているかどうかを確認するには、`/var/log/squid/access.log`にあるSquidログを参照してください。すべてのポートが正しく設定されているかどうかを確認するには、ネットワーク外にあるコンピュータから、該当するコンピュータのポートスキャンを行います。Webサービス(ポート80)のみがオープンしている必要があります。nmapコマンドを使用してポートを検索する場合の構文は、`nmap -O IP_address`です。

41.6 cachemgr.cgi

キャッシュマネージャ(`cachemgr.cgi`)は、実行中のSquidプロセスによるメモリ使用状況に関する統計を表示するCGIユーティリティです。また、キャッシュを管理し、サーバのログギンなしで統計を表示できる便利な手段でもあります。

41.6.1 設定

最初に、システムでWebサーバを稼働させる必要があります。で説明しているように、Apacheを設定します。**第40章Apache HTTPサーバ**(807 ページ)Apacheがすでに稼働しているかどうかを確認するには、「rootとして`rcapachestatus`」コマンドを入力します。次のようなメッセージが表示される場合は、マシンでApacheが実行されています。

```
Checking for service httpd: OK  
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

Apacheはそのマシンで実行されています。実行していない場合は、「`rcapachestart`」を入力して、SUSE Linux Enterprise Serverのデフォルト設定でApacheを起動します。最後に、`cachemgr.cgi`ファイルをApacheのディレクトリ`cgi-bin`にコピーします。

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi /srv/www/cgi-bin/
```

41.6.2 /etc/squid/squid.conf内のキャッシュマネージャACL

キャッシュマネージャの場合は、オリジナルファイル内で次のようなデフォルト設定が必要です。最初に、2つのACLを定義し、`http_access`オプションがこれらのACLを使用して、CGIスクリプトからSquidへのアクセスを付与するようにします。キャッシュマネージャは`cache_object`プロトコルを用いてSquidと通信するため、最初のACLが最も重要です。

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

次の規則によって、ApacheにSquidへのアクセス権が付与されます。

```
http_access allow manager localhost
http_access deny manager
```

これらの規則は、WebサーバとSquidが同じマシンで実行されている場合を想定しています。キャッシュマネージャとSquidとの通信が他のコンピュータ上のWebサーバで開始される場合は、[例 41.2. 「アクセスルール」](#) (868 ページ)に示すACLを追加します。

例 41.2 アクセスルール

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # webserver IP
```

次に、[例 41.3. 「アクセスルール」](#) (869 ページ)に規則を追加して、Webサーバからのアクセスを許可します。

例 41.3 アクセスルール

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

キャッシュのリモートクローズやキャッシュ詳細情報の表示など、より多数のオプションにアクセスする場合は、マネージャのパスワードを設定します。そのためには、マネージャ用のパスワードと表示するオプションのリストを指定してエントリ `cachemgr_passwd` を設定します。このリストは、`/etc/squid/squid.conf` にエントリのコメントの一部として表示されます。

設定ファイルを変更するたびに Squid を再起動してください。それには、`rcsquid reload` コマンドを使用します。

41.6.3 統計情報の表示

対応する Web サイトの <http://webserver.example.org/cgi-bin/cachemgr.cgi> に移動します。[続行] をクリックして様々な統計情報をブラウズします。キャッシュマネージャに表示される各エントリの詳細は、<http://www.squid-cache.org/Doc/FAQ/FAQ-9.html> にある Squid の FAQ を参照してください。

41.7 squidGuard

このセクションでは、squidGuard の詳細な設定については説明しません。ごく基本的な設定のみを紹介し、squidGuard の用法についていくつか助言するに留めます。詳細な設定については、squidGuard の Web サイト <http://www.squidguard.org> を参照してください。

squidGuard は、Squid 用の無償 (GPL) で柔軟で高速なフィルタ、リダイレクタおよびアクセスコントローラプラグインです。squidGuard を利用すれば、Squid キャッシュ上にある異なるユーザグループに対して、異なる制限を持つ複数のアクセスルールを定義することができます。squidGuard は、Squid の標準リダイレクタインタフェースを使用しています。squidGuard の機能を以下に示します。

- 一部のユーザによるWebアクセスを、許可されているか既知のWebサーバまたはURLのリストに限定します。
- リストまたはブラックリストに含まれたWebサーバまたはURLへの、一部のユーザによるアクセスをブロックします。
- 正規表現または語のリストと一致するURLへの、一部のユーザによるアクセスをブロックします。
- ブロックしたURLを「インテリジェント」CGIベースの情報ページにリダイレクトします。
- 未登録ユーザを登録フォームにリダイレクトします。
- バナーを空のGIFにリダイレクトします。
- 時刻、曜日、日付などに基づいて異なるアクセスルールを使用します。
- ユーザグループごとに異なるルールを使用します。

squidGuardとSquidは、以下の用途には使用できません。

- ドキュメント内のテキストの編集、フィルタ処理または検閲。
- JavaScriptやVBScriptなど、HTML埋込みスクリプト言語の編集、フィルタ処理または検閲。

squidGuardを使用するにははじめに、インストールします。最小限の設定ファイルとして/etc/squidguard.confを設定します。に設定例が用意されています。<http://www.squidguard.org/config/>最小限の設定で正常に動作したら、より複雑な設定を試してみてください。

次に、クライアントがブラックリストに含まれるWebサイトを要求した場合にSquidをリダイレクトするために、ダミーの「アクセス拒否」ページまたは複雑度の異なるCGIページを作成します。Apacheを使用することをお薦めします。

ここで、squidGuardを使用するようにSquidを設定します。/etc/squid.confファイル内の次のエントリを使用してください。

```
redirect_program /usr/bin/squidGuard
```

他の`redirect_children`と呼ばれるオプションには、コンピュータ上で動作するリダイレクト(この場合は`squidGuard`)プロセス数を設定します。`squidGuard`は高速で多数のリクエストを処理できます。たとえば、500MHz Pentiumを利用した場合5,900のドメインと7,880のURLを管理して(合計13,780)、100,000件のリクエストを10秒以内に処理できます。したがって、プロセスを5つ以上設定しないように推奨します。これは、5つ以上設定すると、それらのプロセスの割り当てに大量のメモリが消費されるためです。

```
redirect_children 4
```

最後に、`rcsquidreload`を実行し、`Squid`に新規設定をロードさせます。ここで、ブラウザで設定をテストします。

41.8 Calamarisを使用したキャッシュレポート生成

`Calamaris`は、ASCIIまたはHTML形式でキャッシュアクティビティレポートを生成するためのPerlスクリプトです。このスクリプトはネイティブの`Squid`アクセスログファイルを処理します。`Calamaris`のホームページは<http://Calamaris.Cord.de/>にあります。このプログラムの使用方法はきわめて簡単です。

`root`としてログインし、「`cat access.log.files | calamaris options > reportfile`」と入力します。複数のログファイルをパイプする場合は、各ログファイルを古いものから時系列順に指定する必要があります。このプログラムには、次のようなオプションがあります。

- a
使用可能な全レポートを出力
- w
HTMLレポートとして出力
- l
レポートヘッダにメッセージまたはロゴを挿入

各種オプションの詳細については、「mancalamaris」と入力してプログラムのマニュアルページで参照できます。

典型的な例を次に示します。

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \  
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

このコマンドでは、レポートがWebサーバのディレクトリに生成されます。レポートを表示するにはApacheが必要です。

ほかにも、SARG (Squid Analysis Report Generator)と呼ばれる強力なキャッシュレポート生成ツールがあります。詳細については、<http://sarg.sourceforge.net/>を参照してください。

41.9 詳細情報

にあるSquidのホームページにアクセスしてください。<http://www.squid-cache.org/>ここにはS「quid User Guide」が置かれており、Squidに関する広範囲なFAQ集もあります。

透過型プロキシの使用方法に関する簡潔な情報

は、`/usr/share/doc/howto/en/txt/TransparentProxy.gz`にhowtoenhとして含まれています。また、squid-users@squid-cache.orgで、Squidに関するメーリングリストに登録できます。このアーカイブは<http://www.squid-cache.org/mail-archive/squid-users/>にあります。

パート V. セキュリティ

X.509証明書の管理

多くの認証メカニズムで、暗号化処理が利用されています。この方法では、所有者に暗号鍵を割り当てるデジタル証明書が重要な役割を果たします。これらの証明書は通信に使用され、また企業IDカードなどにも利用されています。一般的に証明書の生成と管理は、証明書を商用サービスとして提供する公式機関によって行われています。ただし、たとえば会社の個人データを第三者機関に渡したくないような場合などには、社内で証明書の生成と管理が行われることもあります。

YaSTには、証明書用の2種類のモジュールが用意されています。これらのモジュールは、デジタルX.509証明書に関する基本的な管理機能を提供しています。以降の各項で、デジタル証明書の基礎と、この種類の証明書のYaSTを使った作成、管理方法について説明します。詳細については、<http://www.ietf.org/html.charters/pkix-charter.html>を参照してください。

42.1 デジタル証明書の原理

デジタル証明書は、不正なユーザによるデータへのアクセスを防止するために、暗号化処理を使ってデータを暗号化します。ユーザデータは鍵またはキーと呼ばれる、第2のデータレコードを使って暗号化されます。この鍵を使ってユーザデータに数学的な処理が行われ、元の内容を確認できない暗号化されたデータが生成されます。現在では、非対称暗号方式(公開鍵方式)が一般的に使用されています。鍵は、常に対で使用されます。

Private Key (秘密鍵)

秘密鍵は、その所有者が安全に保管する必要があります。何らかの理由で秘密鍵が公開されてしまうと、その鍵を使った暗号の機密性は保証されず、暗号化に費やす労力が無駄になってしまいます。

Public Key (公開鍵)

公開鍵は、鍵の所有者が第三者に使わせる目的で公開します。

42.1.1 鍵の正当性

公開鍵は幅広く使われるため、さまざまな公開鍵が出回っています。この暗号方式を正しく使用するには、使用する公開鍵が、実際に目的の鍵所有者によって公開されたものかどうかを確認する必要があります。ユーザへの公開鍵の割り当ては、信頼できる組織または機関からの公開鍵証明書により確認されます。このような証明書には、鍵の所有者名、対応する公開鍵、および証明書を発行した人物または組織の電子署名が含まれています。

一般的に、公開鍵証明書を発行、署名する信頼できる機関は、証明書の発行、取り消し、および更新など、さまざまな面で証明書管理作業を担当する、認証基盤の一部となっています。このような認証基盤は、通常「*PKI*」または「*公開鍵基盤*」と呼ばれています。代表的なPKIとしては、*OpenPGP*標準規格があります。この規格では、特定の機関ではなく、ユーザ自身が証明書を発行します。これらの証明書は、「信頼の連鎖」中の他のユーザまたは組織により署名されることにより、信頼できるものとなります。

X.509公開鍵基盤(*PKIX*)は、*IETF(Internet Engineering Task Force)*により定義された代替モデルで、現在一般的に利用されている大半のPKIのモデルとなっています。このモデルでは、階層ツリー構造中の認証局(CA)によって認証が行われます。ツリーのルートには、ルートCAがあります。このCAは、下位のすべてのCAを認証します。そして、最下位レベルのCAが、ユーザ証明書を発行します。ユーザ証明書は、ルートCAに至るまでの証明により信頼できるものとなります。

このようなPKIのセキュリティは、CA証明書の信頼度によって異なります。証明書の利用目的/方針をPKI顧客に明示するために、PKIオペレータはCPS(Certification Practice Statement: 認証局運用規定)を定義します。CPSには、証明書の管理手続きや認証局の運用方法などが定義されています。これにより、PKIだけが信頼できる証明書を発行できることが保証されます。

42.1.2 X.509証明書

X.509証明書は、さまざまな固定フィールドと、必要に応じて追加されたエクステンションから成り立っているデータ構造です。固定フィールドには、おもに鍵所有者名、公開鍵、および証明書を発行したCAに関する情報(名前や署名など)が含まれます。セキュリティ上の理由から、証明書には一定の有効期限があります。そのため、フィールドにはこの有効期限も記載されています。CAは、この有効期限内における証明書の妥当性を保証します。通常、有効期限が切れる前に新しい証明書を作成して配布するには、PKI(発行元CA)が必要になります。

エクステンションには、その他の情報が含まれています。エクステンションに「critical(重要)」が指定されている場合、アプリケーションはそのエクステンションを評価する必要があります。アプリケーションがこのエクステンションを認識できない場合は、その証明書を拒否する必要があります。signature(署名)やencryption(暗号化)などのエクステンションは、特定のアプリケーションに対してのみ利用されます。

基本的なX.509証明書バージョン 3のフィールドを、表 42.1 に示します。

表 42.1 X.509v3証明書

フィールド	内容
バージョン	証明書のバージョン(例:v3)
Serial Number	一意の証明書ID (整数)
署名	証明書に署名するために使われるアルゴリズムのID
[発行者]	発行元認証局(CA)の一意の名前(DN)
Validity	有効期間
件名	所有者の一意の名前(DN)
Subject Public Key Info	所有者の公開鍵およびアルゴリズムのID

フィールド	内容
Issuer Unique ID	発行元認証局の一意のID (オプション)
Subject Unique ID	所有者の一意のID(オプション)
Extensions	KeyUsage 「(鍵の使用目的)や『BasicConstraints』(基本的な制約)などの任意の付加情報」

42.1.3 X.509証明書のブロック

証明書の有効期限が切れる前に、その証明書の信頼性が失われた場合は、それをすぐにブロックする必要があります。たとえば、秘密鍵が何らかの理由により公開されてしまった場合などに、証明書をブロックします。特に、ユーザ証明書ではなく、CAに秘密鍵が所属しているような場合は、証明書をブロックすることが非常に重要になります。このような場合、該当するCAから発行されたすべてのユーザ証明書をすぐにブロックする必要があります。証明書がブロックされると、PKI(責任のあるCA)はCRL(証明書取り消しリスト)を使って、この情報をすべての関連するユーザに知らせる必要があります。

これらのリストはCAからCDP(CRL Distribution Points:CRL配布ポイント)に、定期的に提供されます。必要に応じて証明書のエクステンションに、CDP名を指定することができます。このようにすれば、アプリケーションは最新のCRLを使って妥当性を検証することができます。これを実現する手段の1つとして、OSCP(Online Certificate Status Protocol)を使用する方法があります。CRLの正当性は、発行元認証局の署名により保証されます。X.509CRLの基本的な部分を表42.2.「X.509証明書取り消しリスト(CRL)」(878ページ)に示します。

表 42.2 X.509証明書取り消しリスト(CRL)

フィールド	内容
バージョン	CRLのバージョン(例:2)
署名	CRLに署名するために使われるアルゴリズムのID
[発行者]	CRL発行者(通常は発行元CA)の一意の名前(DN)

フィールド	内容
This Update	このCRLの公開日時(日付、時刻)
[次の更新]	次のCRL公開日時(日付、時刻)
取り消された証明書のリスト	各エントリには、証明書のシリアル番号、取り消し日時、およびオプションでエクステンション(CRLエントリエクステンション)が含まれています。
Extensions	任意のCRLエクステンション

42.1.4 証明書とCRLのリポジトリ

CAの証明書とCRLは、リポジトリを使って、一般からアクセスできるようにする必要があります。証明書やCRLの偽造は署名により防止できるため、リポジトリ自体には特にセキュリティを適用する必要はありません。それよりも、できる限り簡単かつ素早くアクセスできなければなりません。このような理由から、証明書はしばしばLDAPまたはHTTPサーバにより提供されます。LDAPの詳細は、[第36章 LDAP—ディレクトリサービス](#) (725 ページ)を参照してください。HTTPサーバについては、[第40章 Apache HTTPサーバ](#) (807 ページ)を参照してください。

42.1.5 独自のPKI

YaSTには、X.509証明書を管理するための、基本的なモジュールが用意されています。基本的な管理作業には、おもにCAやサブCA、およびその証明書の作成作業が含まれます。単純に証明書やCRLを作成、配布するのは違い、PKIのサービスは非常に複雑です。PKIを運用するには、証明書やCRLを連続して更新していくための、入念に検討された管理基盤が必要になります。この基盤は、商用のPKI製品により提供されています。また、一部の作業が自動化されているものもあります。YaSTには、CAと証明書を作成、配布するツールが用意されています。ただし現時点では、そのバックグラウンドとなる基盤は提供されていません。小規模なPKIをセットアップする場合は、現行のYaSTモジュールを利用することができます。ただし、公式の、または商用のPKIをセットアップする場合は、商用製品を使用する必要があります。

42.2 CA管理用のYaSTモジュール

YaSTには、基本的なCA管理作業を行うために、2つのモジュールが用意されています。ここでは、これらのモジュールを使った、主な管理作業について説明していきます。

42.2.1 ルートCAの作成

PKIをセットアップするには、まずルートCAを作成します。以下を実行します。

- 1 YaSTを起動して、`[セキュリティとユーザ] > [CA Management(CAの管理)]`の順に選択します。
- 2 `[Create Root CA]` をクリックします。
- 3 最初のダイアログでは、CAに関する基本的な情報を入力します。このダイアログの例を図42.1、「YaST CAモジュール—ルートCAの基本データ」(880 ページ)に示します。このダイアログ中の、各テキストフィールドの意味を以下に示します。

図42.1 YaST CAモジュール—ルートCAの基本データ

新しいCAを生成するには、いくつかのエントリが必要です。
設定ファイルで定義されたポリシーに依存します。

「CA 名」は CA の証明書の名前です。ASCII、`[_]`、`[.]` のみが使用できます。

「共通名」は CA の名前です。

「メールアドレス」はユーザまたはサーバの管理者の正式なメールアドレスです。

「組織」、「郵便」、「市区町村」、および「郵便番号」は、通常はオプションです。

新規作成Root CA (ステップ 1/3)

CA 名 (C):
example-cert

共通名 (CN):
example-ca

メールアドレス: デフォルト
root@example.com

削除(D)

デフォルト(F)

通知(A)

組織 (O):
example organization

組織単位 (OU):
example

市区町村 (L):

郵便番号 (Z):

国 (Q):
アイスランド

戻る(B) 中止(S) 次へ(N)

CA Name

CAの名前を入力します。この名前から、ディレクトリ名や他の情報が作成されます。そのため、使用できる文字は制限されています。使用できる文字については、ヘルプを参照してください。ここに指定した名前は、モジュール開始時の概要にも表示されます。

Common Name

CAを参照する場合に使用する名前を入力します。

E-Mail Addresses

複数の電子メールアドレスを入力することができます。CAのユーザには、この電子メールアドレスが表示されます。電子メールアドレスは、問い合わせ先などを知らせる場合に役立ちます。

Country

CAを運用する国を選択します。

Organisation, Organisational Unit, Locality, State

オプション項目です

4 [Next]をクリックします。

5 2番目のダイアログでは、パスワードを入力します。サブCAを作成したり、証明書を作成するなど、CAを使用する場合は常にパスワードが必要になります。このダイアログ中の、各テキストフィールドの意味を以下に示します。

Key Length

[Key Length] には、妥当なデフォルト値が含まれているため、アプリケーションがここに指定されているキー長を処理できない場合を除いて、変更する必要はありません。

Valid Period(日数)

CAの場合、[Valid Period] のデフォルト値は3560日になります(約10年)。削除されたCAを交換する場合、膨大な管理作業の手間がかかるため、このような長期間の値がデフォルト値になっています。

[詳細オプション] をクリックすると、X.509エクステンション()からの他の属性を設定するダイアログが表示されます。図 42.4. 「YaST CAモジュール—拡張設定」 (886 ページ)これらの値には、それぞれ妥当なデ

フォルト値が設定されています。そのため、本当に変更する必要がある場合以外は、これらの値を変更してはなりません。

- 6 確認のため、現在の設定が表示されます。[作成] をクリックします。ルートCAが作成され、概要に表示されます。

ティップ

一般的に、ルートCAによるユーザ証明書の発行は禁止することをお勧めします。最低でも1つのサブCAを作成し、そこからユーザ証明書を発行するようにしてください。こうすることによって、ルートCAを安全な場所に隔離することができます(たとえば、隔離されているコンピュータや安全な部屋など)。こうすることにより、ルートCAへの攻撃を防ぐことができます。

42.2.2 サブCAの作成と取り消し

サブCAは、ルートCAと同一の手順で作成することができます。以下を実行します。

- 1 YaSTを起動して、CAモジュールを開きます。
- 2 目的のCAを選択して、[Enter CA] をクリックします。

注意

サブCAの有効期間は、「親」CAの有効期間内でなければなりません。サブCAは「親」CAの後に作成されるため、デフォルト値を利用するとエラーメッセージが表示されてしまいます。そのため、適切な有効期間を入力してください。

- 3 このCAが初めての場合は、パスワードを入力します。[説明] タブに、CA鍵の情報が表示されます(図 42.2 を参照)。

図 42.2 YaST CA モジュール—CA の使用



- 4 [詳細] をクリックして、[Create SubCA] を選択します。ルートCAの作成時と同じダイアログが表示されます。
- 5 42.2.1項「ルートCAの作成」(880 ページ)の説明に従って、作業を行ってください。
- 6 [証明書] タブを選択します。セキュリティ上の危険があるサブCAや、不要になったサブCAを取り消すには、[Revoke] を使用します。ここで、サブCAを取り消すだけでは、サブCAが完全に無効にはなりません。CRLを使って、サブCAの取り消しを公開する必要があります。CRLの作成については、42.2.5項「CRLの作成」(887 ページ)を参照してください。
- 7 [OK] をクリックして、作業を完了します。

42.2.3 ユーザ証明書の作成と取り消し

クライアント/サーバ証明書の作成は、42.2.1項「ルートCAの作成」(880 ページ)で説明されているCAの作成とよく似ています。同じ原理がこの場合にも当てはまります。電子メール用の証明書では、電子メールプログラムが正しい証明書を割り当てることができるように、電子メール署名と送信者(秘密鍵所有者)の電子メールアドレスが含まれていなければなりません。暗号化中の証

明書割り当てでは、証明書に受信者(公開鍵所有者)の電子メールアドレスを含める必要があります。サーバ/クライアント証明書の場合、*[CommonName]* フィールドにサーバのホスト名を入力する必要があります。証明書のデフォルトの有効期間は365日です。

クライアント/サーバ証明書を作成するには、以下の手順に従ってください。

- 1 YaSTを起動して、CAモジュールを開きます。
- 2 目的のCAを選択して、*[Enter CA]* をクリックします。
- 3 このCAが初めての場合は、パスワードを入力します。*[説明]* タブに、CA鍵の情報が表示されます。
- 4 *[証明書]* をクリックします(図 42.3. 「CAの証明書」 (884 ページ)を参照)。

図 42.3 CAの証明書

まず、この CA で利用可能なすべての証明書が一覧表示されます。カラムにはメールアドレスを含む証明書の DN や「有効」「失効」といった証明書の状態があります。

証明書をひとつ選択し、アクションを実行してください。

「表示」をクリックすると、完全な証明書がテキスト状態で表示されます。

さらに、証明書の「失効」、「削除」、「エクスポート」ができます。

「追加」により、新しいサーバまたはクライアント証明書を生成します。

ここでは、選択された証明書の最も重要な値を表示しています。

証明書局(CA)
CA 名: YaST_Default_CA

説明(D) 証明書(E) CRL(L) 要求(R)

状態 共通名 電子メールアドレス 組織 部署 市区町村 状態 国

追加(A) 表示(V) 取り消し(B) 削除(D) エクスポート

戻る(B) 中止(R) OK(O)

- 5 *[追加]* > *[Add Server Certificate]* の順にクリックして、サーバ証明書を作成します。
- 6 *[追加]* > *[Add Client Certificate]* の順にクリックして、クライアント証明書を作成します。電子メールアドレスを忘れずに入力してください。

7 [OK] をクリックして、作業を完了します。

セキュリティ上の危険がある証明書や、不要になった証明書を取り消すには、以下の手順に従ってください。

- 1 YaSTを起動して、CAモジュールを開きます。
- 2 目的のCAを選択して、[Enter CA] をクリックします。
- 3 このCAが初めての場合は、パスワードを入力します。[説明] タブに、CA鍵の情報が表示されます。
- 4 [証明書] をクリックします(42.2.2項「サブCAの作成と取り消し」(882 ページ)を参照)。
- 5 取り消す証明書を選択して、[Revoke] をクリックします。
- 6 証明書を取消す理由を選択します。
- 7 [OK] をクリックして、作業を完了します。

注意

証明書を取消すだけでは、証明書が無効にはなりません。同様に、CRLを使って証明書の取消しを公開する必要があります。CRLの作成方法については、42.2.5項「CRLの作成」(887 ページ)を参照してください。[削除]を使ってCRLを公開すると、取消された証明書が完全に削除されます。

42.2.4 デフォルト値の変更

前の項では、サブCA、クライアント証明書、およびサーバ証明書の作成方法について説明しました。X.509証明書のエクステンションでは、特別な設定が使われています。これらの設定項目には、それぞれ妥当なデフォルト値が設定されているため、通常これらの値を変更する必要はありません。ただし、状況によってはこれらのエクステンションに特定の値を設定しなければならないこともあります。このような場合は、必要に応じてデフォルト値を適切な値に調整してください。それ以外の場合は、毎回最初から証明書を作成してください。

- 1 YaSTを起動して、CAモジュールを開きます。
- 2 42.2.2項「サブCAの作成と取り消し」(882 ページ)の説明に従って、目的のCAを開きます。
- 3 [詳細] > [Edit Defaults] の順にクリックします。
- 4 変更する設定項目の種類を選択します。図 42.4. 「YaST CAモジュール—拡張設定」(886 ページ)のような、デフォルト値を変更するためのダイアログが表示されます。

図 42.4 YaST CAモジュール—拡張設定



- 5 右側にある適切な値を変更して、重要な設定に [critical] を設定するか、または不要な設定を解除してください。
- 6 [次へ] をクリックすると、簡単な概要が表示されます。
- 7 [保存] をクリックして変更内容を保存します。

ティップ

デフォルト値の変更内容は、この時点より後に作成されるオブジェクトにのみ適用されます。すでに存在しているCAや証明書は変更されません。

42.2.5 CRLの作成

セキュリティ上の危険がある証明書や、不要になった証明書を、今後利用できないようにするには、まずその証明書を取り消す必要があります。証明書を取り消す方法は、[42.2.2項「サブCAの作成と取り消し」](#) (882 ページ)(サブCAの場合)および[42.2.3項「ユーザ証明書の作成と取り消し」](#) (883 ページ)(ユーザ証明書の場合)で説明しています。証明書を取り消したら、CRLを作成して証明書の取り消し情報を公開する必要があります。

システムは、各CAを1つのCRLで管理しています。このCRLを作成、更新するには、以下の手順に従ってください。

- 1 YaSTを起動して、CAモジュールを開きます。
- 2 [42.2.2項「サブCAの作成と取り消し」](#) (882 ページ)の説明に従って、目的のCAを開きます。
- 3 `[CRL]` をクリックします。ダイアログに、このCAの最後のCRLの概要が表示されます。
- 4 作成後にサブCAや証明書を取り消した場合は、`[Generate CRL]` を使って新たなCRLを作成します。
- 5 CRLの有効期間を入力します(デフォルトは30日)。
- 6 `[OK]` をクリックすると、CRLが作成、表示されます。CRLを作成したら、それを公開する必要があります。

ティップ

CRLが利用できない、またはCRLの有効期限を過ぎている場合、アプリケーションはそのCRLを評価して、CRLを拒否します。PKIプロバイダは、現在のCRLの有効期間(妥当性の期限)が切れる前に、新しいCRLを作成して公開する義務があります。YaSTには、この作業を自動化する機能は用意されていません。

42.2.6 CAオブジェクトのLDAPへのエクスポート

この作業を実行するコンピュータには、LDAPエクスポート用のYaST LDAPクライアントを設定する必要があります。こうすることにより、ダイアログの各フィールドを入力する際に利用できる、LDAPサーバ情報が実行時に提供されます。LDAPエクスポート用のYaST LDAPクライアントを設定しない場合、エクスポートすることはできますが、すべてのLDAPデータを手動で入力しなければなりません。特定のパスワードは、常に入力する必要があります(表 42.3. 「LDAPエクスポート中に必要なパスワード」 (888 ページ)を参照)。

表 42.3 LDAPエクスポート中に必要なパスワード

パスワード	意味
LDAP Password	LDAPツリー中にエントリを作成することを許可します。
Certificate Password (証明書パスワード)	証明書をエクスポートすることを許可します。
New Certificate Password (新規証明書パスワード)	LDAPのエクスポート中は、PKCS12形式が使われます。この形式では、エクスポートされた証明書に対して、新しいパスワードを割り当てる必要があります。

LDAPには、証明書、CA、およびCRLをエクスポートできます。

LDAPへのCAのエクスポート

CAをエクスポートするには、**42.2.2項「サブCAの作成と取り消し」** (882 ページ)の説明に従ってCAを開きます。表示されるダイアログから、**[Extended]** > **[Export to LDAP]** の順に選択して、LDAPデータを入力するためにダイアログを表示します。すでにシステムが、YaST LDAPクライアントを使って設定されている場合、一部のフィールドはすでに記入されています。そうでない場合は、すべてのデータを手動で入力してください。エントリはLDAP中の個別のツリーに、属性「caCertificate」で保存されます。

LDAPへの証明書のエクスポート

エクスポートする証明書のあるCAを開き、*[Certificates]*を選択します。ダイアログの上部にある証明書リストから目的の証明書を選択し、*[Export]* > *[Export to LDAP]* の順に選択します。ここでは、CAの場合と同様に、LDAPデータを入力していきます。証明書は、「userCertificate」(PEM形式)および「userPKCS12」(PKCS12形式)の各属性のあるLDAPツリー中の対応するユーザオブジェクトとともに保存されます。

LDAPへのCRLのエクスポート

エクスポートするCRLのあるCAを開き、*[CRL]*を選択します。必要に応じて新しいCRLを作成して、*[エクスポート]* をクリックします。ダイアログが開き、エクスポートパラメータが表示されます。このCAのCRLを1回のみ、または定期的にエクスポートできます。*[LDAPにエクスポート]* を選択してエクスポートを有効にして、該当するLDAPデータを入力します。定期的に実行するには、*[再作成とエクスポートの繰り返し]* ラジオボタンを選択して、必要に応じて間隔を変更します。

42.2.7 CAオブジェクトのファイルへのエクスポート

コンピュータ上にCAを管理するリポジトリを設定している場合、このオプションを使ってCAオブジェクトを適切な場所に、直接ファイルとして作成することができます。CAオブジェクトは、PEM、DER、およびPKCS12など、さまざまな形式で出力することができます。PEMを利用する場合は、証明書と一緒に鍵をエクスポートするかどうか、および鍵を暗号化するかどうかを指定することもできます。PKCS12を利用する場合は、証明書のパスをエクスポートすることもできます。

証明書およびCAも、**42.2.6項「CAオブジェクトのLDAPへのエクスポート」** (888 ページ)で説明されているLDAPと同じ方法でエクスポートできます。ただし、*[LDAPにエクスポート]* の代わりに *[Export as File]* を選択します。この項目を選択すると、出力形式を選択し、パスワードとファイル名を入力するためのダイアログが表示されます。*[OK]* をクリックすると、証明書が必要な場所に保存されます。

CRLの場合は *[エクスポート]* をクリックして *[ファイルにエクスポート]* を選択し、エクスポートフォーマット(PEMまたはDER)を選択してパスを入力します。*[OK]* をクリックして続行し、該当する場所に保存します。

ティップ

保存先としては、ファイルシステム中の任意の場所を選択することができます。このオプションは、**CA**オブジェクトを**USB**スティックなどのリムーバブルメディアに保存する場合にも利用できます。`/media`ディレクトリには、一般にシステムのハードディスク以外のあらゆるタイプのドライブが保持されます。

42.2.8 共通サーバ証明書のインポート

CA管理コンピュータとは別のメディアに、**YaST**を使ってサーバ証明書をエクスポートしたら、その証明書を**共通サーバ証明書**として他のサーバにインポートすることができます。インポートは、インストール時に行うことも、後で**YaST**を使って行うこともできます。

注意

証明書を正常にインポートするには、いずれかの**PKCS12**形式が必要になります。

共通サーバ証明書は`/etc/ssl/servercerts`に保管され、**CA**をサポートする任意のサービスで利用することができます。この証明書の有効期限が切れた場合、同じ方法で簡単に証明書を置換することができます。置換した証明書を正常に機能させるには、関連するサービスを再開してください。

ティップ

ここで **[インポート]** を選択すれば、ファイルシステム中のソースを選択することができます。このオプションは、**USB**スティックなどのリムーバブルメディアから証明書をインポートする場合にも利用できます。

共通サーバ証明書をインポートするには、以下の手順に従ってください。

- 1 **YaST**を起動して、**[セキュリティとユーザ]** の下にある **[Common Server Certificate]** を開きます。
- 2 **YaST**が起動したら、説明フィールドに記載されている現在の証明書のデータを確認します。

- 3 [インポート] を選択して、証明書ファイルを選択します。
- 4 パスワードを入力して、[次へ] をクリックします。証明書がインポートされ、それが説明フィールドに表示されます。
- 5 [完了] をクリックして、YaSTを終了します。

マスカレードとファイアウォール

43

ネットワーク環境でLinuxを使用する場合は常に、ネットワークパケットを操作するカーネル機能を使用して内部ネットワークと外部ネットワークを隔離できます。Linuxのnetfilterフレームワークは、複数のネットワークを隔離する効果的なファイアウォールを構築する手段を提供します。ルールセットを定義する汎用的なテーブル構造体であるiptablesを使用すれば、ネットワークインタフェースを通すパケットを詳細に制御することが可能です。このようなパケットフィルタは、SuSEfirewall2および対応するYaSTモジュールを使用して簡単にセットアップできます。

43.1 iptablesによるパケットフィルタリング

netfilterコンポーネントおよびiptablesコンポーネントは、ネットワークアドレス変換(NAT)に加え、ネットワークパケットのフィルタリングと操作の機能を備えています。フィルタ条件およびそれに関連付けられたアクションはルールセットとして格納され、受信したネットワークパケットに対して1つずつ個別に照合されます。使用されるフィルタ条件とアクションはテーブルに格納されます。これらのテーブルおよびルールセットに変更を加えるには、iptablesコマンドを使用します。

Linuxカーネルは、以下の3つのテーブルを管理します。各テーブルは、パケットフィルタの特定の機能カテゴリに対応しています。

フィルタ

このテーブルは、狭い意味での「パケットフィルタリング」メカニズムを実装するもので、フィルタルールの大半を含んでいます。たとえば、パケットを通すか(Accept)破棄するか(Drop)を判定します。

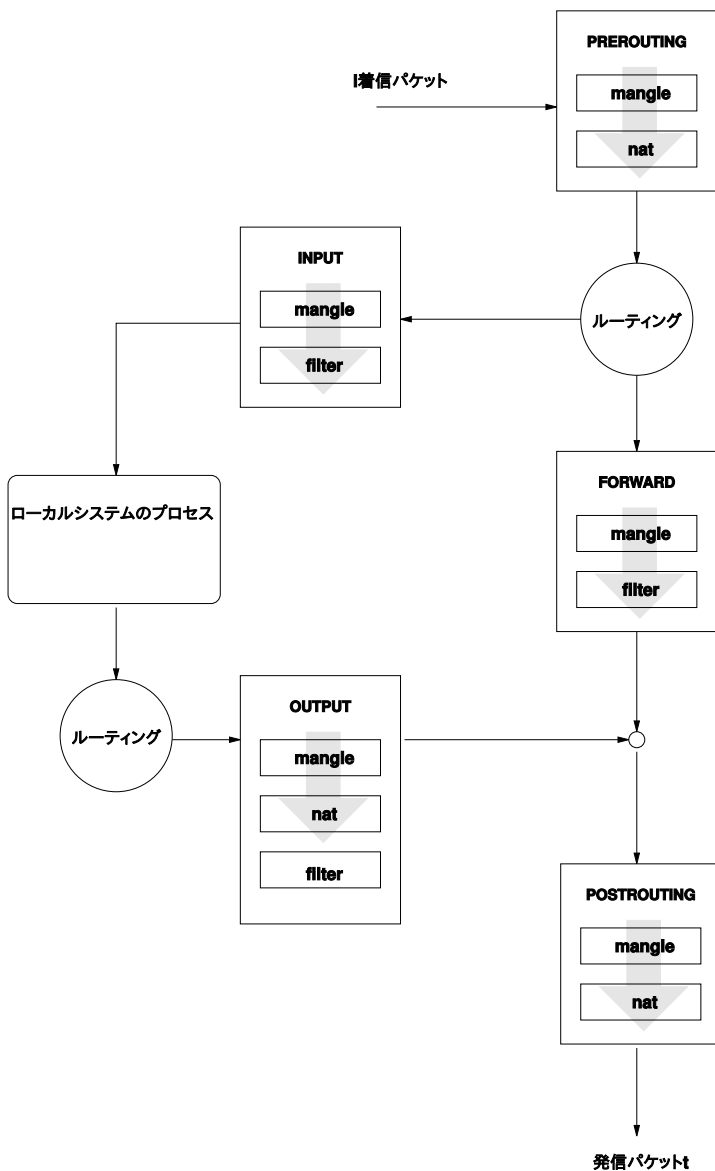
nat

このテーブルは、パケットの送信元アドレスと宛先アドレスに対する変更内容を定義します。これらの機能を使用して、「マスカレード」を実装できます。マスカレードは、プライベートネットワークとインターネットをリンクするNATの一種です。

mangle

このテーブルのルールを使用して、IPヘッダ内の値(サービスタイプなど)を操作できます。

図 43.1 iptables: パケットの可能な経路



これらのテーブルには、パケットと照合される次のような複数の事前定義ルールセットが含まれています。

PREROUTING

このルールセットは、着信パケットに適用されます。

INPUT

このルールセットは、システムの内部プロセス宛てのパケットに適用されます。

FORWARD

このルールセットは、システムを通過するだけのパケットに適用されます。

OUTPUT

このルールセットは、このシステム自身が送信元であるパケットに適用されます。

POSTROUTING

このルールセットは、すべての発信パケットに適用されます。

あるシステムにおけるネットワークパケットの伝送経路を図 43.1. 「**iptables: パケットの可能な経路**」(895 ページ)に示します。簡略化するために、この図ではテーブルをルールセットの一部として示してありますが、実際にはこれらのルールセットはテーブル自体に格納されています。

最も単純なケースとして、システム宛の着信パケットがeth0インタフェースに届いた場合を考えてみます。このパケットははじめにmangleテーブルのPREROUTINGルールセットと照合され、次にnatテーブルのPREROUTINGルールセットと照合されます。パケットのルーティングに関する次のステップでは、パケットの実際の宛先がシステム自身のプロセスであることが確認されます。mangleテーブルおよびfilterテーブルのINPUTルールセットを経た後、このパケットは、filterテーブルのルールに実際に適合していれば、最終的に宛先に届きます。

43.2 マスカレードの基礎知識

マスカレードは、Linux固有のNAT(ネットワークアドレス変換)です。マスカレードを使用すると、小規模LAN(ホストがプライベート範囲のIPアドレスを使用するネットワーク—30.1.2項「**ネットマスクとルーティング**」(601 ページ)を参照)をインターネット(パブリックIPアドレスを使用するネットワーク)に接続することができます。このLANのホストをインターネットに接続する

ためには、プライベートアドレスをパブリックアドレスに変換する必要があります。この変換処理は、LANとインターネット間のゲートウェイとして動作するルータで行います。その原理は単純です。ルータには複数のネットワークインタフェースがあります。一般的には、ネットワークカードと、インターネットに接続する個別のインタフェースです。インターネット接続用インタフェースは外部に接続し、その他のインタフェースはLAN上のホストに接続します。ルータのネットワークカード(eth0など)に接続されているローカルネットワーク内のホストは、ローカルネットワーク以外の宛先を持つすべてのパケットをデフォルトゲートウェイ、つまりルータに送信します。

重要項目: 正しいネットワークマスクの使用

ネットワークを設定する際は、すべてのローカルホストに同じブロードキャストアドレスとネットワークマスクを設定する必要があります。そうしないと、パケットが正しく転送されません。

前述のように、LAN上のホストがインターネット上のアドレス宛にパケットを送信すると、そのパケットは常にデフォルトルータに送信されます。しかし、そのためには、これらのパケットを転送できるようにルータを設定しておく必要があります。セキュリティ上の理由から、デフォルトのインストールではこれは無効になっています。有効にするには、`/etc/sysconfig/sysctl`ファイルの`IP_FORWARD`変数を`IP_FORWARD=yes`に設定します。

宛先ホストからは、ルータは参照できますが、内部ネットワーク内の送信元ホストに関する情報は一切分かりません。この技術がマスカレード(masquerading: 「変装」の意)と呼ばれているのは、このためです。アドレス変換が行われているため、あらゆる応答パケットははじめにルータに届きます。ルータはこれらの着信パケットを識別し、宛先アドレスを変換して、ローカルネットワーク内の正しいホストにパケットを転送します。

着信トラフィックのルーティングはマスカレードテーブルによって決まるため、外部から内部ホストへの接続を開く方法はありません。テーブルには、そのような接続に関するエントリがありません。また、確立済みの接続に対してはテーブルでステータスエントリが割り当てられるため、そのエントリは他の接続では使用されません。

このため、マスカレードを使用すると、ICQ、cucme、IRC (DCC、CTCP)、FTP (PORTモード)などいくつかのアプリケーションプロトコルで問題が発生する可能性があります。Web ラウザ、標準のFTPプログラム、および他の多くのプログラムがPASVモードを使用します。PASVモードを使用すれば、パ

ケットフィルタとマスカレードに関する問題が発生する可能性はかなり低くなります。

43.3 ファイアウォールの基礎知識

「ファイアウォール」は、ネットワーク間のリンクを提供、管理し、ネットワーク間のデータフローを制御するメカニズムを表す用語として、おそらくもっとも広く知られています。ただし、厳密にいうと、このセクションで説明するメカニズムは「パケットフィルタ」と呼ばれるものです。パケットフィルタは、プロトコル、ポート、IPアドレスなどに関する一定の条件に従ってデータフローを規制します。これにより、アドレスに応じて内部ネットワークに到達しないように定められているパケットが、ブロックされます。たとえば、社内のWebサーバを外部に公開するには、対応するポートを明示的に開きます。ただし、パケットフィルタは、社内のWebサーバ宛てのパケットなど、正当なアドレスを持つパケットの内容はスキャンしません。たとえば、着信パケットがWebサーバ上のCGIプログラムの破壊を目的としたものである場合でも、パケットフィルタはそれをそのまま通してしまいます。

より効果的な、しかしより複雑なメカニズムとして、いくつかのタイプのシステムを組み合わせる方法があります。たとえば、パケットフィルタと、プロキシと呼ばれるアプリケーションゲートウェイを連携動作させます。この場合、パケットフィルタは、無効にされたポート宛のパケットをすべて拒否します。アプリケーションゲートウェイ宛にパケットだけが受け付けられます。このゲートウェイ、つまりプロキシは、サーバの実際のクライアントであるかのように振る舞います。ある意味で、このようなプロキシは、アプリケーションによって使用されるプロトコルレベルのマスカレードホストと見なすことができます。プロキシの例としては、HTTPプロキシサーバのSquidがあります。Squidを使用するには、プロキシ経由で通信するようにブラウザを設定する必要があります。要求したHTTPページははじめにプロキシのキャッシュ内で検索され、キャッシュに見つからなかったページのみがプロキシによってインターネットから取得されます。別の例としては、FTPプロトコルのプロキシサーバであるSUSE proxy suite (proxy-suite)があります。

次のセクションでは、SUSE Linux Enterpriseに付属のパケットフィルタについて説明します。パケットフィルタとファイアウォールに関するより詳細な説明については、howtoパッケージに含まれている『Firewall HOWTO』を参照してください。このパッケージがインストールされている場合、HOWTOを参照してください。

43.4 SuSEfirewall2

SuSEfirewall2は、`/etc/sysconfig/SuSEfirewall2`から変数を読み取って一連のiptablesルールを生成するスクリプトです。このスクリプトは、次に示す3つのセキュリティゾーンを定義します(ただし、以降のサンプル設定では1番目と2番目のセキュリティゾーンについてのみ考察します)。

外部ゾーン

外部ネットワークで何が発生しているかを制御できないことを考えれば、ホストを外部ネットワークから保護する必要があることがわかります。外部ネットワークはほとんどの場合インターネットですが、WLANなどそれ以外の安全でないネットワークであることもあります。

内部ゾーン

これはプライベートネットワークを表します。ほとんどの場合はLANになります。内部ネットワーク内のホストがプライベート範囲のIPアドレス(30.1.2項「ネットマスクとルーティング」(601 ページ)を参照)を使用している場合、ネットワークアドレス変換(NAT)を有効にして内部ネットワークのホストが外部ネットワークにアクセスできるようにします。

非武装地帯(DMZ)

このゾーンのホストには外部ネットワークと内部ネットワークの両方からアクセスできますが、このゾーンのホストは自身では内部ネットワークにアクセスできません。DMZ内のシステムは内部ネットワークから隔離されるため、内部ネットワークの周りに追加の防衛線を設けたい場合にこのゾーンを設定します。

フィルタリングルールセットで明示的に許可されていないあらゆる種類のネットワークトラフィックは、iptablesによって抑止されます。したがって、着信トラフィックを持つそれぞれのインタフェースは、3つのゾーンのいずれかに配置する必要があります。各ゾーンに対して、許可するサービスやプロトコルを定義します。ルールセットは、外部ホストから送信されたパケットにのみ適用されます。ローカルに生成されたパケットは、ファイアウォールによって捕捉されません。

設定はYaSTで行うことができます(43.4.1項「YaSTを使ったファイアウォールの設定」(900 ページ)を参照)。または、ファイル`/etc/sysconfig/`

SuSEfirewall2に手動で設定することもできます。このファイルには、詳しい注釈が付けられています。また、さまざまな設定例が/usr/share/doc/SuSEfirewall2/EXAMPLESに格納されています。

43.4.1 YaSTを使ったファイアウォールの設定

重要項目: 自動ファイアウォール設定

インストール後に、YaSTは、すべての設定済みインタフェース上で自動的にファイアウォールを起動します。システム上でサーバが設定されており有効になっていれば、YaSTは、サーバ設定モジュールの「ファイアウォールで開いているポート」オプションまたは「*Open Ports on Selected Interface in Firewall*(選択したインタフェースでファイアウォールを開く)」オプションを使用して、生成されたファイアウォール設定に自動的に変更を加えます。サーバモジュールの一部のダイアログでは、「ファイアウォールの詳細」ボタンをクリックすると、追加のサービスとポートを有効にできます。YaSTのファイアウォール設定モジュールは、ファイアウォールを有効または無効にする作業、あるいは再設定する作業に使用できます。

グラフィカル設定用のYaSTダイアログには、YaSTコントロールセンターからアクセスできます。「セキュリティとユーザ」>「ファイアウォール」の順に選択します。設定は7つのセクションに分かれており、画面左側のツリー構造で各セクションに直接ジャンプすることができます。

起動

このダイアログでは起動動作を設定します。デフォルトのインストールでは、SuSEfirewall2は自動的に起動します。このダイアログで、ファイアウォールを起動または停止することもできます。動作中のファイアウォールに新しい設定を適用するには、「*Save Settings and Restart Firewall Now*」をクリックします。

Interfaces

ここには、認識されているすべてのネットワークインタフェースがリストされます。ゾーンからインタフェースを削除するには、削除するインタフェースを選択して、「*Change*」をクリックし、「*No Zone Assigned*」を選択します。ゾーンにインタフェースを追加するには、追加するインタフェースを選択して、「*変更*」をクリックし、使用可能ないずれかのゾー

ンを選択します。[Custom] を使用して、ユーザ固有の設定で特殊なインタフェースを作成することもできます。

[許可されるサービス]

このオプションは、システムに対するアクセスが禁止されているゾーンに対してシステムサービスを提供するために使用します。デフォルトでは、システムには、外部ゾーンからの保護だけが設定されています。外部のホストで利用可能にするサービスだけを、明示的に許可してください。[選択したゾーンで許可されるサービス] から該当するゾーンを選択して、リストからサービスを有効にします。

[マスカレード]

マスカレードは、インターネットのような外部のネットワークから内部のネットワークを隠します。その一方で、内部のネットワークのホストからは外部のネットワークに透過的にアクセスできるようにします。外部ネットワークから内部ネットワークへの要求はブロックされますが、内部ネットワークからの要求は、外部から見ると、マスカレードサーバから発信されたように見えます。内部ホストの特殊なサービスを外部ネットワークから利用可能にする必要がある場合は、そうしたサービス用の特殊なリダイレクトルールを追加します。

[ブロードキャスト]

このダイアログでは、ブロードキャストが可能なUDPポートを設定します。各ゾーンに必要なポート番号またはサービス名を、スペースで区切って指定してください。/etc/servicesも参照してください。

ここでは、受け付けられなかったブロードキャストについてのログを有効にすることもできます。ただし、Windowsホストは、互いを認識するためにブロードキャストを使用するため、大量のパケットが禁止されることになります。このため、ログを有効にすると大量のパケットがすべてログに記録されてしまいます。

[IPsecサポート]

このダイアログでは、外部ネットワークに対するIPsecサービスを利用できるようにするかどうかを設定します。どのパケットを信頼するかは、[Details] で設定します。

ログレベル

ログには、受け付けられたパケットと、受け付けられなかったパケットの2つのルールがあります。受け付けられなかったパケットは、捨てられる

か拒否されます。その両方について、[すべてログに記録する]、[重要なパケットのみログに記録する]、[ログに何も記録しない]のいずれかを選択します。

機能設定が終わったら、[次へ]をクリックしてダイアログを閉じます。ゾーンごとのファイアウォール設定の概要が表示されます。設定がすべて正しいかどうかチェックしてください。このサマリーには、許可されたすべてのサービス、ポート、プロトコルがリストされます。設定を修正するには、[Back]をクリックします。設定内容を保存するには、[Accept]をクリックします。

43.4.2 手動による設定

以降では、適切に設定するための手順を順を追って説明します。各設定項目には、ファイアウォールとマスカレードのどちらに関連するかを示してあります。必要に応じて、ポート範囲(500:510など)使用します。設定ファイルで述べられているDMZ(非武装地帯)関連の設定については、ここでは取り上げません。DMZは、大規模な組織に見られる複雑なネットワークインフラストラクチャ(企業ネットワークなど)でのみ使用されるものであり、広範な設定とこの分野に関する深い知識を必要とします。

はじめに、YaSTのシステムサービスモジュール(ランレベル)を使用して、使用中のランレベル(通常(3または5)でSuSEfirewall2を有効にします。これにより、/etc/init.d/rc?.d/ディレクトリ内のSuSEfirewall2_*スクリプトへのシンボリックリンクが設定されます。

FW_DEV_EXT (ファイアウォール、マスカレード)

インターネットへの接続デバイス。モデム接続の場合は、ppp0を指定します。ISDNリンクの場合は、ippp0を指定します。DSL接続には、dsl0を指定します。デフォルトルートに対応するインタフェースを使用する場合は、autoを指定します。

FW_DEV_INT (ファイアウォール、マスカレード)

内部プライベートネットワークへの接続デバイス(eth0など)。内部ネットワークがなく、ファイアウォールが動作するホストのみを保護する場合は、空にします。

FW_ROUTE (ファイアウォール、マスカレード)

マスカレード機能が必要な場合は、yesに設定します。内部ホストのネットワークアドレス(例:192.168.x.x)がインターネットルータで無視されるようになるため、内部ホストは外部から見えなくなります。

マスカレード機能なしのファイアウォールで、内部ネットワークへのアクセスを許可する場合は、これをyesに設定します。この場合、内部ホストでは公式のIPアドレスを使用する必要があります。ただし、外部ネットワークから内部ネットワークへのアクセスは許可しないのが普通です。

FW_MASQUERADE (マスカレード)

マスカレード機能が必要な場合は、yesに設定します。これにより、内部ホストからインターネットへの仮想的な直接接続が実現されます。内部ネットワークのホストとインターネット間にプロキシを設定すると、セキュリティが強化されます。プロキシサーバが提供するサービスにはマスカレードは必要ありません。

FW_MASQ_NETS (マスカレード)

マスカレードを行うホストやネットワークを指定します。各エントリはスペースで区切ります。たとえば、次のようにします。

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (ファイアウォール)

内部ネットワークからの攻撃に対してファイアウォールホストを保護するには、yesに設定します。サービスは、明示的に有効にした場合にのみ、内部ネットワークに対して提供されます。FW_SERVICES_INT_TCPおよびFW_SERVICES_INT_UDPも参照してください。

FW_SERVICES_EXT_TCP (ファイアウォール)

使用可能にするTCPポートを指定します。一般的な自宅用のワークステーションでは、通常サービスは提供していないため、空にします。

FW_SERVICES_EXT_UDP (ファイアウォール)

UDPサービスを実行しており、それを外部から使用できるようにする場合を除き、空にします。UDPを使用したサービスとしては、DNSサーバ、IPSec、TFTP、DHCPなどがあります。これらのサービスを使用可能にする場合は、使用するUDPポートを指定します。

FW_SERVICES_INT_TCP (ファイアウォール)

この変数には、内部ネットワークに対して使用可能にするサービスを指定します。記述形式はFW_SERVICES_EXT_TCPと同じですが、この設定は内部ネットワークに適用されます。この変数は、FW_PROTECT_FROM_INTをyesに設定した場合のみ設定します。

FW_SERVICES_INT_UDP (ファイアウォール)

FW_SERVICES_INT_TCPの項を参照してください。

ファイアウォールの設定が完了したら、設定をテストします。ファイアウォールのルールセットは、root権限でSuSEfirewall2 startを実行すると作成されます。次に、telnetを使用して、たとえば外部ホストから接続が実際に拒否されるかどうかを確認します。その後、/var/log/messagesを参照します。次のようなログが記録されているはずです。

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGF=0
OPT (020405B40402080A061AFEBBC0000000001030300)
```

他にも、nmapやnessusといったパッケージを使用して、ファイアウォールの設定をテストできます。パッケージをインストールすると、nmapのドキュメントは/usr/share/doc/packages/nmapに、nessusのドキュメントは/usr/share/doc/packages/nessus-coreに置かれます。

43.5 詳細情報

SuSEfirewall2の最新情報およびその他のドキュメント

は、/usr/share/doc/packages/SuSEfirewall2で参照できます。また、netfilter/iptablesプロジェクトのホームページ<http://www.netfilter.org>では、さまざまな文書を多くの言語で参照できます。

SSH:セキュアネットワークオプション

44

ネットワーク環境に多数のコンピュータがインストールされるほど、遠隔地からホストへのアクセスが必要となります。通常、これはユーザが認証のためにログイン文字列とパスワード文字列を送信することを意味します。これらの文字列が平文で転送され、パケットが盗聴されて、転送元ユーザのアカウントにアクセスするために、そのアカウントを知る権限ユーザを使用せずに不正使用される恐れがあります。これはユーザのファイルがすべて攻撃者に公開されてしまうだけでなく、不正なアカウントを使用して管理者やrootユーザのアクセス権を取得したり、他のシステムに侵入することにもなります。従来、リモート接続の確立にはtelnetが使用されていましたが、telnetには暗号化形式や他のセキュリティメカニズムのパケット盗聴に対する防護機能が用意されていません。その他にも、従来のFTPプロトコルや一部のリモートコピープログラムのように、保護機能のない通信チャネルが存在します。

SSHスイートは、認証文字列(通常はログイン名とパスワード)およびホスト間でやりとりされる他のすべてのデータを暗号化することで、必要な保護を提供します。SSHを使用した場合も、データフローを第三者に記録される可能性は残りますが、内容は暗号化されており、暗号鍵を知らない限り平文に戻すことはできません。そのため、SSHを使用すると、インターネットのように安全でないネットワーク上でも安全な通信が可能になります。SUSE Linux Enterprise付属のSSH機能はOpenSSHです。

44.1 OpenSSHパッケージ

SUSE Linux Enterpriseでは、デフォルトでパッケージOpenSSHがインストールされます。これによりtelnet、rlogin、rsh、rcp、およびftpの代わりにプログラムssh、scp、およびsftpが使用可能になります。デフォルト設定では、SUSE Linux EnterpriseシステムのシステムアクセスはOpenSSHユーティリティを使用し、ファイアウォールがアクセスを許可した場合にのみ可能になります。

44.2 sshプログラム

sshプログラムを使用すると、リモートシステムにログインして対話形式で作業できます。このプログラムは、telnetおよびrloginに代わるものです。sloginプログラムは、sshを指す単なるシンボリックリンクです。たとえば、コマンドssh sunを使用してホストsunにログインするとします。ホストはsunのパスワードを求めるプロンプトを表示します。

認証に成功すると、リモートのコマンドラインで作業したり、YaSTなどの対話型アプリケーションを使用できます。ローカルユーザ名がリモートユーザ名と異なる場合は、ssh -l augustine sunまたはsshaugustine@sunを使用して、異なるログイン名でログインできます。

さらに、sshでは、rshから既知されるリモートシステム上でコマンドを実行できます。次の例では、ホストsun上でコマンドuptimeを実行し、tmpというディレクトリを作成します。プログラムの出力は、ホストsunのローカル端末に表示されます。

```
ssh otherplanet "uptime; mkdir tmp"
Password:
1:21pm up 2:17, 9 users, load average: 0.15, 0.04, 0.02
```

この例では、両方のコマンドを1つのコマンドで送信するために、引用符が必要です。2つ目のコマンドもsun上で実行するには、このように引用符で囲む必要があります。

44.3 scp—セキュアコピー

scpは、ファイルをリモートマシンにコピーします。これは、rcpに対する安全で暗号化機能を持つ代替策です。たとえば、`scp MyLetter.tex sun:`を実行すると、`MyLetter.tex`がホスト `earth` からホスト `sun` にコピーされます。`earth` 上でのユーザ名が `sun` 上でのユーザ名と異なる場合は、後者を `username@host` 形式で指定します。このコマンドには `-l` オプションがありません。

正しいパスワードを入力すると、scpによりデータ転送が開始され、進行状況バーをシミュレートする一連のアスタリスクが表示されます。また、進行状況バーの右端への到達予想時間も表示されます。すべての出力を抑制するには、オプション `-q` を指定します。

scpには、ディレクトリ全体の再帰コピー機能も用意されています。コマンド `scp -r src/ sun:backup/` を入力すると、ディレクトリ `src` の内容全体がすべてのサブディレクトリを含めてホスト `sun` 上の `backup` ディレクトリにコピーされます。このサブディレクトリが存在しない場合は、自動的に作成されます。

オプション `-p` は scp に対して、変更のないファイルのタイムスタンプを残すように指示します。`-c` を指定するとデータ転送が圧縮されます。この場合、データ転送量は最小限ですみますが、プロセッサにかかる負荷が大きくなります。

44.4 sftp—セキュアファイル転送

安全なファイル転送のために、scpの代わりにsftpプログラムを使用できます。sftpセッション中は、ftpで認識される多数のコマンドを使用できます。特にファイル名がわからないデータを転送する場合に、sftpプログラムはscpよりも優れた選択肢です。

44.5 SSHデーモン(sshd)—サーバ側

SSHのクライアントプログラムであるsshおよびscpを操作する場合は、サーバであるSSHデーモンをバックグラウンドで実行し、TCP/IP port 22で接続

をリスンする必要があります。このデーモンは、初回起動時に鍵のペアを3組生成します。鍵のペアはそれぞれ、秘密鍵と公開鍵で構成されます。そのため、このプロシージャは公開鍵ベースと呼ばれます。SSHを介した通信のセキュリティを保証するために、秘密鍵ファイルへのアクセスはシステム管理者に限定する必要があります。ファイルアクセス権は、デフォルトインストールにより適切に設定されます。秘密鍵はSSHデーモンでローカルにのみ必要であり、他人には付与しないでください。公開鍵コンポーネント(拡張子.pubで識別)は、接続を要求しているクライアントに送信されます。これは、ユーザ全員が読み込み可能です。

接続はSSHクライアントにより開始されます。待機中のSSHデーモンと要求側のSSHクライアントは、プロトコルとソフトウェアのバージョンを比較して不正なポートを介した接続を防止するために、識別データを交換します。オリジナルのSSHデーモンの子プロセスが要求に応答するため、同時に複数のSSH接続を確立できます。

SSHサーバとSSHクライアントとの通信の場合、OpenSSHはバージョン1および、2のSSHプロトコルをサポートします。デフォルトではバージョン2のSSHプロトコルが使用されます。バージョン1のプロトコルを使用するには、`-1`スイッチを指定してこの設定を上書きします。システムのアップデート後もバージョン1を使用するには、`/usr/share/doc/packages/openssh/README.SuSE`に記載されている説明に従って作業を行ってください。このドキュメントには、SSH 1環境を数ステップでSSH 2作業環境に変換する方法も含まれています。

バージョン1のSSHを使用する場合、サーバはホスト公開鍵とSSHデーモンにより1時間ごとに再生成されるサーバ鍵を送信します。この両方を使用すると、SSHクライアントは自由に選択したセッション鍵を暗号化でき、この鍵がSSHサーバに送られます。また、SSHクライアントはサーバに対して、どの暗号化方式(暗号)を使用するかも指示します。

バージョン2のSSHプロトコルはサーバ鍵を必要としません。クライアント側とサーバ側は、Diffie-Helmanのアルゴリズムを使用して鍵を交換します。

セッション鍵を復号化するにはホストとサーバの秘密鍵が不可欠であり、公開部分からは導出できません (`man /usr/share/doc/packages/openssh/RFC.nroff`)。この初期接続フェーズは、SSHクライアントの詳細デバッグオプション`-v`をオンにすると緊密に監視できます。

クライアントでは、すべてのホスト公開鍵がリモートホストとの初期接続後に`~/.ssh/known_hosts`に格納されます。このため、中間者攻撃、つまり、外部SSHサーバが他の名前とIPアドレスを偽装して使用しようとする攻撃が防止されます。この種の攻撃は、`~/.ssh/known_hosts`に含まれていないホスト鍵が使用されたことで検出されるか、適切な秘密鍵がないためにサーバがセッション鍵を復号化できないことで検出されます。

`/etc/ssh/`に格納された秘密鍵と公開鍵のバックアップを、外部の安全な場所に保管することをお勧めします。これにより、鍵の変更を検出でき、再インストール後は古い鍵を再び使用できます。また、ユーザの動揺を招くような警告を出す必要もなくなります。警告にも関わらず実際には正しいSSHサーバであることが確認された場合は、このシステムに関する既存のエントリを`~/.ssh/known_hosts`から削除する必要があります。

44.6 SSHの認証メカニズム

この時点で実際の認証が発生します。最も単純な形式の認証は、前述のようにパスワードを入力することからなっています。SSHの目標は、使いやすく安全なソフトウェアを提供することでした。これは、`rsh`および`rlogin`にとって代わるという側面もあるため、SSHは日常的な使用に適した認証方式も提供できるようにする必要があります。そのために、SSHはもう1つ、ユーザが生成する鍵のペアを使用します。SSHパッケージには、そのためのヘルパープログラム「`ssh-keygen`」が用意されています。`ssh-keygen -t rsa`または`ssh-keygen -t dsa`を入力すると鍵のペアが生成され、鍵を格納するペースファイルの名前を求めるプロンプトが表示されます。

デフォルト設定を確認し、パスフレーズ要求に応答します。ソフトウェアから空のパスフレーズが提示された場合も、ここで説明する手順には10~30文字のテキストを使用することをお勧めします。短くて単純な語句は使用しないでください。また、パスフレーズを再入力して確認してください。その後、秘密鍵と公開鍵の格納場所(この例ではファイル`id_rsa`および`id_rsa.pub`)が表示されます。

古いパスフレーズを変更するには、`ssh-keygen -p -t rsa`または`ssh-keygen -p -t dsa`を使用します。公開鍵コンポーネント(この例では`id_rsa.pub`ファイル)をリモートマシンにコピーし、`~/.ssh/authorized_keys`ファイルに保存します。次の接続確立時には、パスフレーズで自己

認証するように要求されます。このプロンプトが表示されない場合は、これらのファイルの位置と内容を確認してください。

長時間実行する場合、この手順はその都度パスワードを入力するよりも煩雑です。そのため、SSHパッケージには`ssh-agent`というツールが用意されており、Xセッションの存続期間中は秘密鍵が保持されます。Xセッション全体は`ssh-agent`の子プロセスとして開始されます。この場合に最も簡単な方法は、`.xsession`ファイルの先頭にある変数`usessh`を`yes`に設定し、KDMやXDMなどのディスプレイマネージャを介してログインすることです。また、`ssh-agent startx`と入力する方法もあります。

これで、`ssh`または`scp`を通常どおり使用できます。前述のように公開鍵を配布している場合、パスワードを求めるプロンプトは表示されなくなります。Xセッションを終了するか、`xlock`などのパスワード保護アプリケーションでロックすることに注意してください。

バージョン2のSSHプロトコル導入に関連する変更は、すべてファイル`/usr/share/doc/packages/openssh/README.SuSE`にも記載されています。

44.7 X、認証および転送メカニズム

前述したセキュリティ関連の改善に加えて、SSHを使用するとリモートXアプリケーションの使用も簡略化されます。オプション`-X`を指定して`ssh`を実行すると、リモートマシン上で`DISPLAY`変数が自動的に設定され、すべてのX出力が既存のSSH接続を介してリモートマシンにエクスポートされます。それと同時に、権限のないユーザは、この方法でリモートで起動してローカルに表示していたXアプリケーションのパケットを盗聴できなくなります。

オプション`-A`を追加すると、`ssh-agent`の認証メカニズムが次のマシンに繰り越されます。これにより、事前に接続先ホストに公開鍵を配布してそこで適切に保存している場合にのみ、パスワードを入力しなくても様々なマシンから作業できます。

デフォルト設定では両方のメカニズムが無効になっていますが、システム単位の設定ファイル`/etc/ssh/sshd_config`またはユーザの`~/.ssh/config`ファイル内でいつでも永続的に有効にすることができます。

sshを使用してTCP/IP接続をリダイレクトすることもできます。次の例では、SSHに対してそれぞれSMTPポートとPOP3ポートをリダイレクトするように指定しています。

```
ssh -L 25:sun:25 earth
```

このコマンドを使用すると、earthのポート25(SMTP)に送られた接続は、すべて暗号化チャンネルを介してsunのSMTPポートにリダイレクトされます。これが特に役立つのは、SMTP-AUTHまたはPOP-before-SMTP機能のないSMTPサーバを使用する場合です。ネットワークに接続している任意の場所から「ホーム」メールサーバに電子メールを転送して配信できます。同様に、次のコマンドを使用すると、earth上のすべてのPOP3要求(ポート 110)をsunのPOP3ポートに転送できます。

```
ssh -L 110:sun:110 earth
```

どちらのコマンドも、権限付きのローカルポートに接続するためrootユーザで実行する必要があります。電子メールは、既存のSSH接続で標準ユーザにより送受信されます。これを機能させるには、SMTPとPOP3のホストをlocalhostに設定する必要があります。追加情報は、前述の各プログラムのマニュアルページおよび/usr/share/doc/packages/opensshにある該当ファイルを参照してください。

ネットワーク認証—Kerberos

オープンネットワークでは、従来から使われているパスワードメカニズムを利用する以外、ワークステーションのユーザを正しく認識、識別する手段はありませんでした。通常のインストールでは、ネットワーク内のサービスにアクセスする場合、ユーザは毎回パスワードを入力する必要があります。

Kerberosを利用すれば、ユーザは1回登録するだけで、以降のセッションでネットワーク全体へのアクセスに認証情報を入力する必要がなくなります。ネットワークを安全な状態に保つためには、次の要件を満たしていなければなりません。

- すべてのユーザに、各自が利用するサービスに対するIDを証明させ、他のユーザのIDを利用できないようにすること。
- それぞれのネットワークサーバも、各自のIDを証明すること。これがない場合、攻撃者がサーバになりすまし、そのサーバに送信される重要な情報が盗まれる危険性があります。この方法は、クライアントがサーバを、サーバがクライアントを相互に認証するため、**相互認証**と呼ばれます。

これらの要件を満たすには、Kerberosの強力な暗号認証機能を利用します。ここでは、この目的を達成するための、Kerberosの使用方法について説明します。ただし、ここではKerberosの基本的な機能についてのみ取り上げます。技術的な詳細については、Kerberosのマニュアルを参照してください。

45.1 Kerberosで使われる用語

ここでは、Kerberosで使われる用語の定義を説明します。

資格情報

ユーザやクライアントは、サービスを要求する資格があることを証明する、一種の資格情報を提示する必要があります。**Kerberos**は、チケットとオーセンティケータの2種類の資格情報を知っています。

チケット

チケットは、サービスを要求するサーバに対して、クライアントが認証に使用するサーバ単位の資格情報です。チケットには、サーバ名、クライアント名、クライアントのインターネットアドレス、タイムスタンプ、利用期間、およびランダムなセッションキー情報が保管されています。このデータはすべて、サーバのキーを使って暗号化されます。

オーセンティケータ

オーセンティケータはチケットとともに、クライアントが提示したチケットが正しいかどうかを証明するために使われます。オーセンティケータは、クライアント名、ワークステーションのIPアドレス、および現在のワークステーションの時刻などの情報を、サービスを要求するクライアントとサーバだけが知っているセッションキーで暗号化したデータから作成されます。オーセンティケータは、チケットと違い、1回しか使用できません。クライアントは、オーセンティケータ自身を作成することができます。

プリンシパル

Kerberosのプリンシパルは、チケットを割り当てることができる一意のエンティティ(ユーザやサービス)です。プリンシパルは次のコンポーネントで構成されます。

- **プライマリ**—プリンシパルの最初の部分で、ユーザの場合はユーザ名になります。
- **インスタンス**—プライマリの特徴を説明するオプション情報。プライマリとこの文字列は、/で区切られます。
- **レルム**—**Kerberos**のレルムを指定します。通常、レルムはドメイン名を大文字で表したものになります。

相互認証

Kerberosでは、クライアントとサーバの両方が、互いのIDを確認することができます。クライアントとサーバはセッションキーを共有し、それを使って安全に通信することができます。

セッションキー

セッションキーは、Kerberosが生成する一時的な秘密鍵です。クライアントはセッションキーを使って、チケットを要求したり受け取る場合の、クライアント-サーバ間の通信を暗号化します。

再生

ネットワークに送信されるメッセージは、盗聴、傍受、または改ざんされる危険性があります。Kerberosの場合、攻撃者によりユーザのチケットやオーセンティケータを含むサービス要求が傍受された場合、重大な危険性があります。攻撃者は入手したサービス要求を再送信(再生)して、そのユーザになりすますことができます。ただし、Kerberosにはこのような問題に対処するための、さまざまな機能が実装されています。

サーバ/サービス

サービスは、実行する特定のアクションを表す場合に用いられます。このアクションの背後にあるプロセスのことを、サーバと呼んでいます。

45.2 Kerberosの仕組み

Kerberosは、サードパーティによる信頼された認証サービスに呼び出されます。クライアントはすべて、Kerberosによる他のクライアントが正当かどうかの判断を信頼します。Kerberosは、ユーザとその秘密鍵をすべてデータベースに保管しています。

すべての信用情報を安全に管理するために、認証サーバとチケット保証サーバは、専用のコンピュータ上で稼働させます。また、このコンピュータには、管理者だけが物理的、またはネットワーク経由でアクセスできるようにします。危険性を減らすためにも、このコンピュータ上では必要最低限のネットワークサービスだけが実行するようにしてください。sshdも稼働させてはいけません。

45.2.1 初めて使用する

Kerberosを初めて利用する場合の操作は、通常のネットワークシステムへのログイン手順とほとんど変わりありません。ユーザ名を入力します。この情報と、チケット保証サービス(TGS)名が、認証サーバ(Kerberos)に送られます。認証サーバがユーザの存在を確認したら、ランダムなセッションキーが生成されます。このキーを使って、クライアントとチケット保証サーバ間の通信

が行われます。次に、認証サーバがチケット保証サーバ用のチケットを用意します。チケットには以下の情報が含まれています。これらの情報はすべて、認証サーバとチケット保証サーバしか知らないセッションキーで暗号化されます。

- クライアントとチケット保証サーバの両方の名前
- 現在の時刻
- このチケットの有効期限
- クライアントのIPアドレス
- 新しく生成されたセッションキー

このチケットはセッションキーと一緒に、暗号化されてクライアントに送られます。ただし、今回は暗号化に、クライアントの秘密鍵が用いられます。秘密鍵は、ユーザパスワードから取得されるため、Kerberosとクライアントしか知りません。クライアントがチケットを受け取ると、パスワードの入力を要求するプロンプトが表示されます。このパスワードが、認証サーバから送られてきたパッケージを復号化する鍵に変換されます。パッケージの暗号化が「解除」され、ワークステーションのメモリからはパスワードと鍵が消去されます。チケットの有効期限が切れるまでの間、ワークステーションは自己のIDを証明することができます。

45.2.2 サービスの要求

ネットワーク上の任意のサーバにサービスを要求する場合、クライアントアプリケーションは自己のIDをサーバに証明する必要があります。そのため、アプリケーションはオーセンティケータを生成します。オーセンティケータは以下のコンポーネントから成り立っています。

- クライアントのプリンシパル
- クライアントのIPアドレス
- 現在の時刻
- チェックサム(クライアントが選択)

これらの情報はすべて、クライアントがサーバから受け取ったセッションキーを使って暗号化されます。オーセンティケーターとチケットがサーバに送信されます。サーバはセッションキーのコピーを使って、オーセンティケーターを復号化します。オーセンティケーターには、サービスを要求したクライアントを、チケット内の情報と比較するための情報が含まれています。サーバは、オーセンティケーターとチケットが、同じクライアントから送られてきたかどうかを確認します。

サーバ側にセキュリティ手段が実装されていない場合、この段階は再生攻撃の絶好の目標となります。攻撃者は、ネットから傍受した要求メッセージを再送信しようとします。この問題を防止するために、サーバが以前に受け取ったタイムスタンプを持つ要求やチケットは、受け付けられません。また、要求を受け取った時刻と、要求自体のタイムスタンプが大幅に違う要求は無視されます。

45.2.3 相互認証

Kerberos認証は、双方向に利用することができます。クライアントだけが認証を受ける訳ではありません。サーバ自身も、サービスを要求するクライアントに対して、認証を受けるようにすることができます。この場合、サーバに関する一種のオーセンティケーターが送信されます。サーバは、受け取ったクライアントのオーセンティケーター中のチェックサムに情報を追加し、それをクライアントと共有しているセッションキーで暗号化します。クライアントは、受け取ったデータからサーバの認証情報を確認し、その後データのやり取りを行います。

45.2.4 チケット保証—すべてのサーバとの通信

チケットは、1回に1つのサーバと通信することを前提に設計されています。つまり、他のサービスを要求する場合、そのたびに新しいチケットを入手する必要があります。Kerberosでは、個別のサーバのチケットを取得する仕組みが実装されています。このサービスは、「**ticket-granting** (チケット保証) サービス」と呼ばれています。**ticket-granting**サービスは、前述のサービスと同様のサービスで、チケットの入手手順も同じように行われます。チケットを必要とするアプリケーションは、**ticket-granting**サーバに問い合わせます。このチケット要求は、以下のコンポーネントから成り立っています。

- 要求したプリンシパル
- ticket-grantingチケット
- オーセンティケータ

他のサーバと同様に、ticket-grantingサーバはticket-grantingチケットとオーセンティケータを確認します。これらが有効な場合、ticket-grantingサーバは新しいセッションキーを作成します。このセッションキーは、元のクライアントと新しいサーバ間で利用されます。次に、新規サーバ用のチケットが作成されます。このチケットには、次の情報が含まれています。

- クライアントのプリンシパル
- サーバのプリンシパル
- 現在の時刻
- クライアントのIPアドレス
- 新しく生成されたセッションキー

新しいチケットにはライフタイムが割り当てられます。この時間は、ticket-grantingチケットの残りのライフタイムやサービスのデフォルト値よりも短くなります。クライアントは、ticket-grantingサービスから送られてきたチケットとセッションキーを受け取ります。ただし、これらのデータは、元のticket-grantingチケットと一緒に送られたセッションキーで暗号化されています。新サービスへの接続時に、これを使ってサービスからの応答を復号化できるため、ユーザがパスワードを入力する必要はありません。Kerberosは、このような方法でチケットを入手するため、ユーザが毎ログイン情報を入力する必要はありません。

45.2.5 Windows 2000との互換性

Windows 2000には、Microsoft版のKerberos 5が含まれています。SUSE Linux Enterprise®はMIT版のKerberos 5を利用しているため、詳細情報などはMITのドキュメントを参照してください。詳細については、[45.4項「詳細情報」](#) (920 ページ)を参照してください。

45.3 ユーザ側から見たKerberos

ユーザは、ワークステーションへのログイン時に1回だけ、Kerberosと情報のやり取りを行うのが理想です。ログイン処理には、`ticket-granting`チケットの取得処理も含まれています。ログアウト時に、ユーザのKerberosチケットは自動的に破棄されます。そのため、他人がそのユーザになりすますことは困難です。チケットには有効期限があるため、ユーザのログインセッションが`ticket-granting`チケットのライフタイム(一般的に10時間)より長くなった場合は、それが問題になることがあります。ただし、`kinit`を実行すれば、新しく`ticket-granting`チケットを入手することができます。この場合、パスワードをもう一度入力すれば、Kerberosにより目的のサービスへのアクセスチケットを入手できます。サービスに対して認証を行う必要はありません。Kerberosにより入手されたチケットのリストを表示するには、`klist`を実行してください。

ここには、Kerberos認証を利用するアプリケーションの一例を記載しています。これらのアプリケーションは、`/usr/lib/mit/bin`または`/usr/lib/mit/sbin`ディレクトリにあります。これらのアプリケーションには、通常のUNIX/Linuxが提供する機能に加えて、Kerberosが管理する透過的な認証手段を利用できるという利点があります。

- `telnet`, `telnetd`
- `rlogin`
- `rsh`, `rcp`, `rshd`
- `ftp`, `ftpd`
- `ksu`

これらのアプリケーションを利用する場合、KerberosによりIDが証明されているため、いちいちパスワードを入力する必要はありません。`ssh`の場合、Kerberosサポートによりコンパイルされていれば、取得したすべてのチケットをあるワークステーションから別のワークステーションに転送することもできます。`ssh`を使って他のワークステーションにログインした場合、暗号化されたチケットの内容を、その環境に合わせて`ssh`が調整します。チケットにはワークステーション固有の情報(IPアドレス)が含まれているため、単にワークステーション間でチケットをコピーしても、それを利用することはできません。XDM、GDM、およびKDMも、Kerberosをサポートしています。Kerberosネットワー

クアプリケーションの詳細は、<http://web.mit.edu/kerberos>にある『*Kerberos V5 UNIX User's Guide*』を参照してください。

45.4 詳細情報

MIT Kerberosの公式サイトは<http://web.mit.edu/kerberos>です。このサイトには、Kerberosのインストールガイド、ユーザガイド、管理ガイドなど、Kerberosに関連する資料/情報や、他のリソースへのリンクが記載されています。

<ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS>には、Kerberosの基本原理が説明されています。また、Kerberosに関するさまざまな考察や、関連資料なども記載されています。

Kerberosの公式なFAQは、<http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>を参照してください。また、Brian Tung著の書籍『*Kerberos—A Network Authentication System*』(ISBN 0-201-37924-4)にも、さまざまな情報が記載されています。

Kerberosのインストールと管理

46

ここでは、MIT版のKerberosのインストール方法、および一部の管理作業について取り上げています。この項は、Kerberosの基本概念を理解しているユーザを対象にしています(第45章 ネットワーク認証—Kerberos (913 ページ)も参照)。

46.1 Kerberosレルムの選択

Kerberosのドメインはレルムと呼ばれ、「FOOBAR.COM」や「ACCOUNTING」のような名前で識別されます。Kerberosでは、大文字と小文字が区別されるため、「foobar.com」と「FOOBAR.COM」は異なるドメインとみなされます。好きな方をお使いください。ただし、一般的にレルム名には大文字が用いられています。

また、DNSドメイン名を使用することもできます(または、ACCOUNTING.FOOBAR.COMのようなサブドメイン名)。後述するように、DNSを使ってKDCや他のKerberosサービスを検索するようにKerberosクライアントを設定すれば、管理作業が大幅に楽になります。DNSドメインのサブドメイン名をレルム名にしておけば、このような場合に便利です。

DNSネームスペースと違い、Kerberosは階層構造ではありません。たとえば、レルムFOOBAR.COMの直下に、サブレルム「DEVELOPMENT」とACCOUNTINGを配置して、これらのサブレルムにFOOBAR.COMから属性を継承させるようなことはできません。このような場合は、3つの独立したレルムを作成し、それらのレルム間の認証情報を設定します(あるレルムのユーザから他のレルムのサーバーになど)。

ここでは問題を簡単にするために、ある組織全体に対して1つのレルムを作成する場合を例に説明していきます。以降の項では、レルム名に「EXAMPLE.COM」を使って例を説明していきます。

46.2 KDCハードウェアの設定

Kerberosを使用するにはまず、キー配布センタの役割を果たすコンピュータを設定します。このコンピュータは、**KDC (Key Distribution Center)**と呼ばれます。このコンピュータの**Kerberos**ユーザデータベースには、パスワードや他のすべての関連情報が保管されます。

KDCは、セキュリティインフラストラクチャの最重要部分になります。何者かがこのコンピュータに侵入した場合、**Kerberos**により保護されているすべてのユーザアカウントとインフラストラクチャが危険にさらされてしまいます。**Kerberos**データベースにアクセスできた場合、その攻撃者はデータベース中の任意のプリンシパルになりますことができます。このマシンには、利用できる最強のセキュリティ手段を適用してください。

- 1 また、このサーバコンピュータは、特定の者だけが入室できる鍵のかかったサーバ専用ルームなど、物理的に安全な場所に設置してください。
- 2 また、このコンピュータ上では、**KDC**以外のネットワークアプリケーションは実行しないでください。ここで、ネットワークアプリケーションには、サーバとクライアントも含まれます。たとえば、**KDC**で**NFS**を使ってファイルシステムをインポートしたり、**DHCP**を使ってネットワーク設定を取得しないでください。
- 3 まず、最低限のシステムをインストールしてから、インストールされたパッケージのリストを確認し、不要なパッケージを削除してください。また、**inetd**、**portmap**、および**cups**などのサーバや、**X**系のプログラムも削除してください。**SSH**サーバも潜在的なセキュリティリスクがあるので、インストールしないようにしてください。
- 4 このマシンに**GUI**は必要ありません。**X**サーバも潜在的な危険になります。**Kerberos**には、独自の管理インタフェースが用意されています。

- 5 ユーザ/グループのルックアップにローカルファイルだけを使用するように、`/etc/nsswitch.conf`を設定します。たとえば、`passwd`および`group`の行を、次のように変更します。

```
passwd:      files
group:       files
```

`/etc`中のファイル`passwd`、`group`、`shadow`、および`gshadow`を編集し、先頭が「+」で始まる行(NISルックアップ用の行)を削除します。

- 6 `root`以外のすべてのユーザアカウントを無効にします。`/etc/shadow`を編集して、ハッシュパスワードを「*」や「!」などの文字に置換してください。

46.3 時計の同期化

Kerberosを適切に利用するには、組織内のすべてのシステムの時計(クロック)を一定範囲内に同期化する必要があります。このことは、Kerberosで再生攻撃からシステムを保護する場合に重要になります。攻撃者は、ネットワーク上のKerberos資格情報を傍受し、それを使ってサーバを攻撃する可能性があります。Kerberosは、このような攻撃から防御するために、さまざまな手段を採用しています。そのような保護手段の1つとして、チケットにタイムスタンプが記入されます。サーバが現在の時刻と異なるタイムスタンプを持つチケットを受け取った場合、そのチケットは拒否されます。

Kerberosでは、タイムスタンプの比較時に多少の誤差は許容されます。ただし、コンピュータの時計の時刻が実際とずれてしまうこともよくあります。一週間で30分ほど進んだり、遅れたりすることも珍しくはありません。このような理由から、ネットワーク上のすべてのホストの時刻を、単一の時刻ソースと同期化するように設定する必要があります。

時刻を同期化するもっとも簡単な方法は、あるコンピュータ上にNTP時間サーバをインストールして、他のすべてのクライアントをこのサーバの時刻と同期化するように設定することです。そのためには、すべてのクライアント上でNTPデーモンをクライアントモードで稼働させるか、または毎日1回各クライアント上で`ntpddate`コマンドを実行します(この方法は、クライアント数が多い場合、現実的ではない)。KDC自身も、共通の時間ソースと時刻を同期化する必要があります。ただし、KDCコンピュータ上でNTPデーモンを稼働さ

せることにはセキュリティリスクがあるため、`cron`を使って`ntpd`を毎日実行することをお勧めします。お使いのコンピュータをNTPクライアントとして設定するには、[32.1項「YaSTでのNTPクライアントの設定」](#) (667 ページ)の説明に従ってください。

Kerberosがタイムスタンプを比較する際に許容する、時間の最大許容誤差を変更することもできます。この値(クロックスキュー(`clock skew`))を設定するには、[46.5.3項「クロックスキューの調整」](#) (930 ページ)の説明に従って、`krb5.conf`ファイルを編集してください。

46.4 KDCの設定

この項では、KDCのインストールと初期設定、および管理プリンシパルの作成について説明します。この作業は、いくつかのステップに分けられます。

- 1 RPMのインストール** KDCとして使用するコンピュータに、特別なソフトウェアパッケージをインストールします。詳細については、[46.4.1項「RPMのインストール」](#) (925 ページ)を参照してください。
- 2 設定ファイルの変更** 利用目的に応じて、`/etc/krb5.conf`および`/var/lib/kerberos/krb5kdc/kdc.conf`ファイルを変更する必要があります。これらのファイルには、KDCに関するすべての情報が保管されています。
- 3 Kerberosデータベースの作成** Kerberosでは、すべてのプリンシパルID、および認証する必要があるすべてのプリンシパルの秘密鍵が、データベースに保管および管理されています。
- 4 ACLファイルの調整:管理者の追加** KDC上のKerberosデータベースは、リモート管理することができます。不正なプリンシパルによるデータベースの改ざんを防止するために、KerberosはACL(アクセス制御リスト)を使用します。管理者プリンシパルにデータベースを管理させるためには、管理者プリンシパルに明示的にリモートアクセスを許可する必要があります。
- 5 Kerberosデータベースの調整:管理者の追加** Kerberosを管理するには、最低1つの管理者プリンシパルを実行する必要があります。このプリンシパルは、KDCを開始する前に追加する必要があります。

- 6 Kerberosデーモンの開始 KDCソフトウェアをインストールして、適切な設定を行ったら、Kerberosデーモンを開始して、レルムにKerberosサービスを提供します。

7 自分用のプリンシパルの作成

46.4.1 RPMのインストール

作業を開始する前に、Kerberosソフトウェアをインストールしてください。KDCで、パッケージkrb5、krb5-server、およびkrb5-clientをインストールします。

46.4.2 データベースの設定

次に、Kerberosがプリンシパルに関するすべての情報を保管するデータベースを初期化します。テープへのバックアップ時など、データベースを間違えて公開することを防ぐために使用する、データベースのマスタキーを設定します。マスタキーはパスフレーズから取得され、stashファイルに格納されます。こうすることによって、KDCの再起動時に毎回パスワードを入力する手間を省くことができます。パスフレーズには、適当に本を開いたページにある語句など、類推しにくいフレーズを使用してください。

テープにKerberosデータベース(/var/lib/kerberos/krb5kdc/principal)をバックアップする場合、stashファイル(/var/lib/kerberos/krb5kdc/.k5.EXAMPLE.COM)をバックアップしてはいけません。そうしないと、テープを読み取れるユーザは誰でもデータベースを参照できてしまいます。また、データベースのクラッシュ後にテープからデータベースを復元する場合、元のパスフレーズを指定する必要があります。そのため、パスフレーズをどこか安全な場所に保管しておくことをお勧めします。

stashファイルとデータベースを作成するには、次のコマンドを実行してください。

```
$> kdb5_util create -r EXAMPLE.COM -s
Initializing database '/var/lib/kerberos/krb5kdc/principal' for realm
'EXAMPLE.COM',
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
```

```
Enter KDC database master key: <= Type the master password.  
Re-enter KDC database master key to verify: <= Type it again.  
$>
```

実行結果を確認するには、次のコマンドを使用します。

```
$>kadmin.local  
kadmin> listprincs  
K/M@EXAMPLE.COM  
kadmin/admin@EXAMPLE.COM  
kadmin/changepw@EXAMPLE.COM  
krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

表示された内容から、データベース中にいくつかのプリンシパルがあることが分かります。これらのプリンシパルは、**Kerberos**内部で使われます。

46.4.3 プリンシパルの作成

次に、日常作業用と**Kerberos**関連の管理作業用の2つの**Kerberos**プリンシパルを自分用に作成します。ここでは、ログイン名としてnewbieを使用し、次の操作を行います。

```
kadmin.local  
  
kadmin> ank newbie  
newbie@EXAMPLE.COM's Password: <type password here>  
Verifying password: <re-type password here>
```

次に、kadminプロンプトから「anknewbie/admin」と入力し、newbie/adminと言う名前のプリンシパルを作成します。ユーザ名の後に付けられているadminは、ロールを表しています。以降、このロールを使って**Kerberos**データベースを管理します。目的に応じて異なるロールを使用することができます。基本的にロールは、同じ名前を持つけれども、まったく異なるアカウントです。

46.4.4 KDCの開始

KDCデーモンとkadminデーモンを開始します。これらのデーモンを手動で開始するには、`rckrb5kdc start` および `rckadmind start` を入力します。また、`insserv krb5kdc` および `insserv kadmind` コマンドを使って

サーバコンピュータをリブートした場合、デフォルトではKDCとkadmindが開始されます。

46.5 Kerberosクライアントの手動設定

Kerberosを設定する場合、基本的には/etc/krb5.confファイルに静的に設定する方法と、DNSを使って動的に設定する方法があります。DNSによる設定を使用する場合、KerberosアプリケーションはDNSレコードを使ってKDCサービスを探します。静的な設定を使用する場合は、KDCサーバのホスト名をkrb5.confファイルに追加してください(この場合、KDCを移動したりレルムの設定を他の方法で変更したら、ファイルを修正する必要があります)。

一般的にはDNSを使用する方が、柔軟に対応できるだけでなく、コンピュータに関する設定作業の手間を減らせます。ただし、この場合レルム名をDNSドメイン名、またはサブドメイン名と同じにする必要があります。また、Kerberosの設定にDNSを使用する方法では、多少セキュリティ上の問題があり、攻撃者がDNSを通じて、インフラストラクチャに重大なダメージを与える可能性があります(ネームサーバをダウンさせたり、偽のDNSレコードを作成するなど)。ただし、この影響は、最悪の場合でサービスの拒否程度です。静的な設定の場合でも、krb5.confファイルにホスト名ではなくIPアドレスを指定しない限り、同じような危険性があります。

46.5.1 スタティック設定

Kerberosを設定する方法の1つとして、`/etc/krb5.conf`設定ファイルを編集する方法があります。デフォルトでは、このファイルにはさまざまなサンプル項目が記載されています。作業を開始する前に、これらのサンプル項目はすべて削除してください。`krb5.conf`はさまざまなセクションから成り立っています。各セクションは「`[this]`」のように、角かっこに囲まれたセクション名から始まります。

Kerberosクライアントを設定するには、`krb5.conf`に次の節を追加してください(ここで、`kdc.example.com`はKDCのホスト名を表します)。

```
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
    EXAMPLE.COM = {
        kdc = kdc.example.com
        admin_server = kdc.example.com
    }
```

`default_realm`行には、Kerberosアプリケーションのデフォルトのレルムを設定します。複数のレルムがある場合は、`[realms]`セクションに残りのレルムを定義してください。

また、このファイルには、ホスト名のレルムへのマップ方法も定義します。たとえば、リモートホストに接続する場合、Kerberosはそのホストがどのレルムにあるかを知る必要があります。この設定は、`[domain_realms]`セクションに追加する必要があります。

```
[domain_realm]
    .example.com = EXAMPLE.COM
    www.foobar.com = EXAMPLE.COM
```

この例では、DNSドメイン`example.com`中のすべてのホストが、Kerberosのレルム`EXAMPLE.COM`に所属することになります。また、外部ホストである`www.foobar.com`も、`EXAMPLE.COM`レルムのメンバとみなされます。

46.5.2 DNSを使った設定

DNSを使ったKerberos設定では、SRVレコードが頻繁に使用されます。詳細は、にある『(RFC2052) A DNS RR for specifying the location of services <http://www.ietf.org>』を参照してください。これらのレコードは、古いバージョンのBINDネームサーバではサポートされていません。最低でもBINDバージョン8が必要になります。

Kerberosが利用するSRVレコードの形式は、常に`_service._proto.realm`になります。ここで、「realm」の部分には、Kerberosのレルム名が入ります。DNS中のドメイン名では大文字と小文字は区別されません。Kerberosレルムでは大文字と小文字が区別されるため、この設定方法を使用する場合、重複が発生する可能性があります。`_service`はサービス名を表します(たとえば、KDCと通信する場合やパスワードサービスを利用する場合は異なる名前が使われます)。`_proto`は、`_udp`(UDP)または`_tcp`(TCP)になります。ただし、一部のプロトコルをサポートしていないサービスもあります。

SRVリソースレコードのデータ部は、優先値、重み、ポート番号、およびホスト名で構成されます。優先値は、ホストを利用する順序を定義しています(値が小さいほど優先度が高くなる)。重みは、同じ優先度を持つサーバ間の負荷分散に用いられます。通常は、これらの値を指定する必要がないため、値に0を設定しても構いません。

現在、MIT Kerberosはサービスの検索時に、次の名前を使用しています。

`_kerberos`

KDCデーモン(認証サーバとTGS(チケット保証サーバ))の場所を定義しています。一般的なレコードの例を以下に示します。

```
_kerberos._udp.EXAMPLE.COM.  IN  SRV      0 0 88 kdc.example.com.
_kerberos._tcp.EXAMPLE.COM.  IN  SRV      0 0 88 kdc.example.com.
```

`_kerberos-adm`

リモート管理サービスの場所を記述しています。一般的なレコードの例を以下に示します。

```
_kerberos-adm._tcp.EXAMPLE.COM. IN  SRV      0 0 749 kdc.example.com.
```

`kadmind`はUDPをサポートしていないため、`_udp`が付けられたレコードはありません。

静的な設定ファイルの場合と同様に、example.com DNSドメインに所属していないホストでも、そのホストがEXAMPLE.COMレルムに所属していることをクライアントに知らせる方法があります。クライアントに知らせるには、次の例のようにTXTレコードを_keberos.hostnameに追加します。

```
_keberos.www.foobar.com. IN TXT "EXAMPLE.COM"
```

46.5.3 クロックスキューの調整

クロックスキューは、ホストのシステム時刻とチケットのタイムスタンプが異なる場合に、どの程度の誤差まで許容するかを示します。通常、クロックスキューは300秒(5分)に設定されています。つまり、サーバの時刻の5分前～5分後までのタイムスタンプを持つチケットが受け付けられます。

NTPを使ってすべてのホストを同期化する場合、この値を1分に減らすことができます。クロックスキューは、/etc/krb5.confファイルに次のように指定します。

```
[libdefaults]
    clockskew = 120
```

46.6 YaSTを使ったKerberosクライアントの設定

前述した手動設定のほかに、YaSTを使ってKerberosクライアントを設定することもできます。次の手順に従います。

- 1 rootとしてログインしたら、[ネットワークサービス] > [Kerberosクライアント] の順に選択します。
- 2 [Use Kerberos] を選択します。
- 3 DNSを使用するKerberosクライアントを設定するには、次の手順に従ってください。
 - 3a [Basic Kerberos Settings] の表示内容を確認します。

3b チケット関連の設定、OpenSSHサポート、および時刻同期などの詳細を設定する場合は、[\[詳細な設定\]](#) をクリックします。

4 静的な設定ファイルを使用するKerberosクライアントを設定するには、次の手順に従ってください。

4a [\[Default Domain\]](#)、[\[Default Realm\]](#)、および [\[KDC Server Address\]](#) に、適切な値を入力します。

4b チケット関連の設定、OpenSSHサポート、および時刻同期などの詳細を設定する場合は、[\[詳細な設定\]](#) をクリックします。

図 46.1 YaST : Kerberosクライアントの基本設定

Kerberosによる認証
Kerberosクライアントの環境設定によって、PAMの設定がアップデットされ、Kerberos認証が有効になります。これを動作させるには、システムにネットワーク内のKerberosサーバへのアクセスが必要です。

基本クライアント設定: [デフォルトドメイン]、[デフォルトレルム]、およびKey Distribution Centerのホスト名またはアドレス([KDCサーバのアドレス])を入力してください。

通常、ドメイン名が大文字のものをデフォルトのレルム名として使用しますが、別の名前も使用できます。サーバでレルムを使用できない場合は、ログインできません。詳細な情報が必要な場合は、サーバ管理者にお問い合わせください。

詳細な環境設定のためには、[\[詳細な設定\]](#) をクリックしてください。

Kerberosクライアントの環境設定

☐ Kerberosをしない(I)
☒ Kerberosを使用する(U)

基本的なKerberosの設定

デフォルトドメイン(D) デフォルトレルム(M)
example.com EXAMPLE.COM

KDCサーバのアドレス(S)
kdc.example.com

[詳細な設定\(V\)...](#)

[戻る\(B\)](#) [中止\(B\)](#) [完了\(E\)](#)

[\[詳細な設定\]](#) ダイアログでチケット関連オプションを設定するには、次のオプションから選択してください。

- [\[Default Ticket Lifetime\]](#) および [\[Default Renewable Lifetime\]](#) には、それぞれ日数、時間数、分数を指定します(単位には d 、 h 、および m を使用し、値とこれらの単位の間にスペースを入れないでください)。
- チケットを使用するための自分のID情報を他のホストに転送する場合は、[\[Forwardable\]](#) を選択します。

- 特定のチケットの転送を有効にするには、 *[Proxiable]* を選択します。
- セッションの終了後もチケットをPAMモジュールで利用できるようにするには、 *[Retained]* を選択します。
- OpenSSHクライアントに対してKerberos認証サポートを有効にするには、該当するチェックボックスを選択します。選択すると、クライアントはSSHサーバの認証に、Kerberosチケットを使用します。
- 一定範囲のユーザアカウントを、Kerberos認証の使用から除外する場合は、その内容を *[Minimum UID]* に設定します。たとえば、システム管理者(root)を除外することができます。
- *[Clock Skew]* には、ホストのシステム時刻とチケットのタイムスタンプの時刻の許容誤差を設定します。
- システムの時刻をNTPサーバと同期化するには、ホストをNTPクライアントとして設定します。設定するには、 *[NTP Configuration]* を選択します。選択すると、YaST NTPクライアントダイアログが表示されます。このダイアログについては、[32.1項「YaSTでのNTPクライアントの設定」](#) (667 ページ)を参照してください。設定を完了して、YaSTを終了すると、Kerberosクライアントの使用準備が完了します。

46.2 YaST : Kerberosクライアントの詳細設定

【デフォルトのライフタイム】、【デフォルトの更新可能なライフタイム】、および【クロックスキュー】の値は、デフォルトで秒単位です。または、時間の単位を指定して (分はm、時間はh、日数はd)、値のサフィックスとして使用します。たとえば、1日は1dまたは24hと表します。

【転送可能】では、完全な識別情報(TGT)を別のマシンに転送できます。【プロキシ可能】では、特定のチケットのみを転送できます。

【保持】を有効にすると、PAMモジュールはセッションを閉じた後もチケットを保持します。

OpenSSHクライアント用のKerberosのサポートを有効にするには、【OpenSSHクライアント用のKerberosのサポート】を選択します。そのような場合、SSHサーバでのユーザ認証にKerberosチケットが使用されます。

【最小ユーザID】がより大きい場合は、指定された値より小さいユーザIDを持つユーザの認証は無視されます。これによって、システム管理者(ルート)のKerberos認証を無効にできます。

【クロックスキュー】は、ホストのシステムクロックとの間に生じるタイムスタンプのずれの許容値で、値は秒単位です。

時刻をNTPサーバと同期するには、使用しているコンピュータをNTPクライアントとして設定する必要があります。【NTPの設定】で、設定してください。

ユーザアカウントのソースを設定するには、【ユーザデータの設定】で適切な設定モジュールを選択します。

Kerberosクライアントの詳細な環境設定

チケットの属性

デフォルトのライフタイム(D)

デフォルトの更新可能なライフタイム(E)

☒ 転送可能(Y)
 ☐ プロキシ可能(P)
 ☐ 保持(E)

☐ OpenSSHクライアント用のKerberosサポート(S)

最小ユーザID(U)

クロックスキュー(L)

46.7 Kerberosのリモート管理

KDCコンソールを利用せずに、Kerberosデータベースからプリンシパルを追加、削除するには、Kerberos管理サーバにどのプリンシパルにどのような操作を許可するかを指示します。このような設定を行うには、`/var/lib/kerberos/krb5kdc/kadm5.acl`ファイルを編集します。このACL(アクセス制御リスト)ファイルには、何にどのような操作を許可するかを細かく設定することができます。詳細については、`man 8 kadmind`を実行して、表示されるマニュアルページを参照してください。

ここでは、データベースに対してすべての操作を行える権限を自分に与えるために、ファイルに次の行を追加します。

```
newbie/admin *
```

ここで、ユーザ名newbieは、自分のユーザ名と置き換えてください。変更内容を有効にするには、`kadmind`を再起動してください。

46.7.1 kadminを使ったリモート管理

これで、`kadmin`ツールを使ってKerberosの管理作業をリモートで行えるようになりました。まず、管理者ロールのチケットを入手し、それを使って`kadmin`サーバに接続します。

```
kadmin -p newbie/admin
Authenticating as principal newbie/admin@EXAMPLE.COM with password.
Password for newbie/admin@EXAMPLE.COM:
kadmin: getprivs
current privileges: GET ADD MODIFY DELETE
kadmin:
```

`getprivs`コマンドを使って、自分が持っているアクセス権限を確認します。前述の例では、すべてのアクセス権限を保有しています。

ここでは、例としてプリンシパルnewbieを変更します。

```
kadmin -p newbie/admin
Authenticating as principal newbie/admin@EXAMPLE.COM with password.
Password for newbie/admin@EXAMPLE.COM:
```

```

kadmin: getprinc newbie
Principal: newbie@EXAMPLE.COM
Expiration date: [never]
Last password change: Wed Jan 12 17:28:46 CET 2005
Password expiration date: [none]
Maximum ticket life: 0 days 10:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Wed Jan 12 17:47:17 CET 2005 (admin/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, Triple DES cbc mode with HMAC/shal, no salt
Key: vno 1, DES cbc mode with CRC-32, no salt
Attributes:
Policy: [none]

kadmin: modify_principal -maxlife "8 hours" newbie
Principal "newbie@EXAMPLE.COM" modified.
kadmin: getprinc joe
Principal: newbie@EXAMPLE.COM
Expiration date: [never]
Last password change: Wed Jan 12 17:28:46 CET 2005
Password expiration date: [none]
Maximum ticket life: 0 days 08:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Wed Jan 12 17:59:49 CET 2005 (newbie/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, Triple DES cbc mode with HMAC/shal, no salt
Key: vno 1, DES cbc mode with CRC-32, no salt
Attributes:
Policy: [none]
kadmin:

```

この例では、チケットのライフタイムを最大8時間に変更しています。kadmin コマンドの詳細、および利用できるオプションについては、<http://web.mit.edu/kerberos/www/krb5-1.4/krb5-1.4/doc/krb5-admin.html#Kadmin%20Options> または `man 8 kadmin` で表示されるマニュアルページを参照してください。

46.8 Kerberosホストプリンシパルの作成

ネットワーク上の各コンピュータがそれぞれのKerberosレルムに所属しているか、またどのKDCと通信するかを設定するほかに、そのホストプリンシパルを作成します。ここまでは、ユーザ資格情報について説明してきました。しかし、一般的にKerberos互換のサービスは、自分自身もクライアントから認証を受ける必要があります。そのため、レルム中の各ホストのKerberosデータベース中に、特別なホストプリンシパルを作成する必要があります。

ホストプリンシパルの命名規則は、`host/<hostname>@<REALM>`です。ここで、`hostname`には、ホストの完全修飾ホスト名を指定します。ホストプリンシパルはユーザプリンシパルと似ていますが、大きな違いがあります。ユーザプリンシパルのキーは、パスワードにより保護されています。ユーザがKDCからticket-grantingチケットを入手する場合、そのチケットを復号化するにはパスワードを入力する必要があります。システム管理者にとっては、SSHデーモン用のチケットを8時間ごとに入手し直さなければならないのは不便です。

そこで、ホストプリンシパル用の初期チケットを復号化するために必要なキーは、KDCから1回入手したら、それを`keytab`と呼ばれるローカルファイルに格納します。SSHデーモンなどのサービスは、必要な時にこのキーを読み込んで、新しいチケットを自動的に入手します。デフォルトでは、`keytab`ファイルは`/etc/krb5.keytab`に格納されています。

`test.example.com`用のホストプリンシパルを作成するには、`kadmin`セッション中に次のコマンドを入力します。

```
kadmin -p newbie/admin
Authenticating as principal newbie/admin@EXAMPLE.COM with password.
Password for newbie/admin@EXAMPLE.COM:
kadmin: addprinc -randkey host/test.example.com
WARNING: no policy specified for host/test.example.com@EXAMPLE.COM;
defaulting
to no policy
Principal "host/test.example.com@EXAMPLE.COM" created.
```

新しいプリンシパル用のパスワードを設定するかわりに、`-randkey`を指定して、`kadmin`にランダムキーの生成を指示します。このプリンシパルの場

合、ユーザが処理に介入することは想定されていないため、このオプションを使用します。このプリンシパルは、このコンピュータ用のサーバアカウントです。

最後に、キーを入手して。それをローカルのkeytabファイルである/etc/krb5.keytabに保管します。このファイルはスーパーユーザが所有者になります。そのため、**kadmin**シェルで次のコマンドを実行するには、rootでなければなりません。

```
kadmin: ktadd host/test.example.com
Entry for principal host/test.example.com with kvno 3, encryption type Triple
DES cbc mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/test.example.com with kvno 3, encryption type DES
cbc mode with CRC-32 added to keytab WRFILE:/etc/krb5.keytab.
kadmin:
```

作業が完了したら、前述の**kinit**で入手した管理チケットを**kdestroy**コマンドで破棄してください。

46.9 KerberosのPAMサポートの有効化

SUSE Linux Enterprise®には、PAMモジュールpam_krb5が同梱されています。このモジュールは、Kerberosログインとパスワード更新をサポートしています。このモジュールは、コンソールログイン、su、およびKDMのようなGUIログインアプリケーションなどで、ユーザの代わりにそのアプリケーションに初期Kerberosチケットを入手させるような場合に使用します。

pam_unix2モジュールは、Kerberos認証とパスワードのアップデートもサポートしています。pam_unix2でKerberosサポートを有効にするには、/etc/security/pam_unix2.confファイルに次の行を追加します。

```
auth:      use_krb5 nullok
account:   use_krb5
password:  use_krb5 nullok
session:   none
```

以降、このファイル中のエントリを評価するすべてのプログラムで、ユーザ認証にKerberosが使用されます。Kerberosプリンシパルのないユーザの場合、pam_unix2が標準のパスワード認証メカニズムになります。プリンシパルの

あるユーザの場合は、passwdコマンドを使って、簡単にKerberosパスワードを変更できるようになります。

pam_krb5の利用方法を変更するには、/etc/krb5.confを編集して、pamにデフォルトのアプリケーションを追加します。詳細については、man5 pam_krb5を実行して、表示されるマニュアルページを参照してください。

pam_krb5モジュールは、ユーザ認証の一部として、Kerberosチケットを受け付けるネットワークサービス用には設計されていません。ここでは、まったく別のことについて取り上げます。

46.10 Kerberos認証用のSSHの設定

OpenSSHは、プロトコルバージョン1と2の両方でKerberos認証をサポートしています。バージョン1には、Kerberosチケットを送信する特別なプロトコルメッセージがありました。バージョン2ではKerberosを直接利用せずに、GSSAPI(General Security Services API)を使用しています。これは、Kerberos、SPKMなどの公開鍵認証システム、または他の認証システムなどの、認証システム固有の特性を隠すために設計されたプログラミングインタフェースで、Kerberos専用ではありません。ただし、GSSAPIライブラリは、Kerberosだけをサポートしています。

Kerberos認証でsshdを使用するには、/etc/ssh/sshd_configに次のオプションを設定します。

```
# These are for protocol version 1
#
# KerberosAuthentication yes
# KerberosTicketCleanup yes

# These are for version 2 - better to use this
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

次に、rcsshdrestartコマンドを実行して、SSHデーモンを再開始します。

プロトコルバージョン2でKerberos認証を使用するには、クライアント側でもそれを有効にする必要があります。有効にするには、システム全体用の設定ファイル/etc/ssh/ssh_config、またはユーザレベルの設定ファイル~/

.ssh/configを編集します。どちらのファイルを利用する場合でも、ファイルにGSSAPIAuthentication yesオプションを追加してください。

これで、Kerberos認証を使って接続できるようになりました。klistを使って有効なチケットがあるかどうかを確認し、SSHサーバに接続します。SSHプロトコルバージョン1を使用する場合は、コマンドラインに-1を指定します。

ティップ: 補足情報

/usr/share/doc/packages/openssh/README.kerberosファイルには、OpenSSHとKerberosの利用に関する詳細が記述されています。

46.11 LDAPとKerberosの使用

Kerberosを使用する場合、ローカルネットワークにユーザ情報(ユーザID、グループ、ホームディレクトリなど)を配布するために、LDAPを使用することができます。LDAPを使用する場合、偽のチケットによる攻撃や他の攻撃を防止するために、強力な認証メカニズムが必要になります。対処方法の1つとして、LDAP通信にKerberosを使用することが挙げられます。

OpenLDAPは、SASL (Aimble Authentication Session Layer)を通じて、多くの認証フレーバーを実装しています。基本的にSASLは、認証用に設計されたネットワークプロトコルです。実装版のSASLはcyrus-saslで、さまざまな認証フレーバーをサポートしています。Kerberos認証は、GSSAPI (General Security Services API)を介して実行されます。デフォルトでは、GSSAPI用SASLプラグインはインストールされていません。このプラグインをインストールするには、rpm -ivh cyrus-sasl-gssapi-*.rpmを実行します。

KerberosにOpenLDAPをバインドさせるには、プリンシパル ldap/earth.example.comを作成して、それをkeytabに追加します。

デフォルトでは、LDAPサーバslapdが、ユーザおよびグループldapとして動作し、keytabファイルはrootしか参照できません。そのため、LDAPの設定を変更して、サーバをrootとして動作させるか、またはグループldapがkeytabファイルを参照できるようにしてください。/etc/sysconfig/openldapファイル中の変数OPENLDAP_KRB5_KEYTABにkeytabファイルが指定され、変数OPENLDAP_CHOWN_DIRSにyesが設定されている場合(デフォルト)、グルー

pldapがkeytabファイルを参照できるようにする設定作業は、OpenLDAP起動スクリプト (/etc/init.d/ldap) により自動的に行われます。

OPENLDAP_KRB5_KEYTABに何も指定されていない場合は、/etc/krb5.keytabにあるデフォルトのkeytabが使用されます。この場合は、以降の説明に従って、自分のアクセス権限を設定する必要があります。

slapdをrootとして実行する場合は、/etc/sysconfig/openldapを編集します。変数OPENLDAP_USERとOPENLDAP_GROUPの直前に注釈文字を指定して、これらの変数を無効にしてください。

グループLDAPがkeytabファイルを参照できるようにするには、次のコマンドを実行します。

```
chgrp ldap /etc/krb5.keytab
```

```
chmod 640 /etc/krb5.keytab
```

それ以外に、OpenLDAPに特殊なkeytabファイルを使用させる方法もあります。この方法が最良かもしれません。この場合、kadminを起動してldap/earth.example.comを追加した後に、次のコマンドを入力します。

```
ktadd -k /etc/openldap/ldap.keytab ldap/earth.example.com@EXAMPLE.COM
```

シェルから次のコマンドを実行します。

```
chown ldap.ldap /etc/openldap/ldap.keytab
```

```
chmod 600 /etc/openldap/ldap.keytab
```

OpenLDAPに別のkeytabファイルを使わせるには、/etc/sysconfig/openldap中の次の変数を変更します。

```
OPENLDAP_KRB5_KEYTAB="/etc/openldap/ldap.keytab"
```

最後に、rcldaprestartコマンドで、LDAPサーバを再起動します。

46.11.1 LDAPでのKerberos認証の使用

ここまでの作業で、`ldapsearch`などのツールをKerberos認証で利用できるようになりました。

```
ldapsearch -b ou=people,dc=example,dc=com '(uid=newbie)'

SASL/GSSAPI authentication started
SASL SSF: 56
SASL installing layers
[...]

# newbie, people, example.com
dn: uid=newbie,ou=people,dc=example,dc=com
uid: newbie
cn: Olaf Kirch
[...]
```

ご覧のように、GSSAPI認証を開始したことを伝えるメッセージが、`ldapsearch`から表示されます。次のメッセージは難解ですが、*SSF*(Security Strength Factor)が56であることを表しています(ここで、56は任意の値になります。ここには、DES暗号キーのビット数が表示されます)。このメッセージは、GSSAPI認証が正常に開始され、LDAP接続を保護するために暗号が使われていることを表しています。

Kerberosでは、認証は常に相互に行われます。つまり、LDAPサーバの認証を受けるだけでなく、こちら側でもLDAPサーバを認証します。つまり、攻撃者が設定した偽のサーバではなく、正しいLDAPサーバと通信していることを確認することができます。

46.11.2 Kerberos認証とLDAPのアクセス制御

ここでは、ユーザに各自のLDAPユーザレコードのログインシェル属性の変更を許可する作業を行います。この例では、ユーザjoeのLDAPエントリが`uid=joe,ou=people,dc=example,dc=com`にあり、`/etc/openldap/slapd.conf`ファイルに次のアクセス制御が設定されていると仮定しています。

```
# This is required for things to work _at all_
access to dn.base="" by * read
# Let each user change their login shell
access to dn="*,ou=people,dc=example,dc=com" attrs=loginShell
```

```
        by self write
# Every user can read everything
access to *
        by users read
```

2番目のステートメントでは、認証されたユーザに対して、自己のLDAPエントリのloginShell属性への書き込みアクセス権を与えています。3番目のステートメントでは、認証されたユーザに対して、LDAPディレクトリ全体に対する読み込みアクセス権を与えています。

ここまでで、1つ分からないことがあります。LDAPサーバはどのようにして、Kerberosユーザであるjoe@EXAMPLE.COMが、LDAP識別名のuid=joe,ou=people,dc=example,dc=comと対応していることを判断するのでしょうか。このためには、saslExprディレクティブを使って、手動でマッピングを設定する必要があります。この例の場合は、次の項目をslapd.confに追加してください。

```
authz-regexp
    uid=(.*),cn=GSSAPI,cn=auth
    uid=$1,ou=people,dc=example,dc=com
```

この仕組みを理解するには、いつSASLがユーザを認証するか、OpenLDAPがSASLから与えられた名前(joeなど)を使って識別名を作成するか、およびSASLフレーバーの名前(GSSAPI)を知る必要があります。その結果が、uid=joe,cn=GSSAPI,cn=authになります。

authz-regexpが指定されている場合、最初の引数を正規表現として使い、SASL情報から作成されたDNがチェックされます。この正規表現が一致した場合、名前がauthz-regexpステートメントの2番目の引数に置換されます。プレースホルダの\$1は、(.*?)式に一致するサブストリングで置き換えられます。

より複雑な式を作成することもできます。ユーザ名がDNの一部にはならない複雑なディレクトリ構造またはスキーマがある場合でも、検索式を使ってSASL DNをユーザDNにマップすることができます。

パーティションとファイルの暗号化

47

どのユーザも、第三者がアクセスできないようにするべき機密データを持っています。モバイルコンピューティングや異なる環境およびネットワーク上での作業が増えるにつれ、データ処理への注意がより一層必要となります。システムに他者がネットワーク経由または物理的にアクセスできる場合は、ファイルまたはパーティション全体の暗号化を推奨します。ラップトップ、または外部ハードディスクやUSBスティックなどのリムーバブルメディアは、紛失したり、盗まれたりしやすいものです。このため、ファイルの機密データが含まれる部分を暗号化することを推奨します。

暗号化によりデータを保護するには、さまざまな方法があります。

ハードディスクパーティションの暗号化

インストール中に、またはインストールが終了したシステムに、YaSTを使って暗号化パーティションを作成することができます。詳細については、[47.1.1項「インストール時の暗号化パーティションの作成」](#) (945 ページ)と[47.1.2項「稼働中のシステムでの暗号化パーティションの作成」](#) (946 ページ)を参照してください。このオプションは、外部ハードディスクなどのリムーバブルメディアに対して使用することもできます。詳細は、[47.1.4項「リムーバブルメディアの内容の暗号化」](#) (947 ページ)を参照してください。

暗号化ファイルをコンテナとして作成

YaSTを使用して、ハードディスクまたはリムーバブルメディアにいつでも暗号化ファイルを作成できます。作成した暗号化ファイルは、他のファイルやフォルダを格納する目的で利用できます。詳細については、[47.1.3項「暗号化ファイルをコンテナとして作成する」](#) (947 ページ)を参照してください。

ホームディレクトリの暗号化

SUSE Linux Enterpriseを使って、ユーザ用の暗号化ホームディレクトリを作成することもできます。ユーザがシステムにログインすると、暗号化ホームディレクトリがマウントされ、その内容を利用できるようになります。詳細については、[47.2項「暗号化ホームディレクトリの使用」](#) (948 ページ)を参照してください。

単一ASCIIテキストファイルの暗号化

重要なデータや機密データを含むASCIIテキストファイルがわずかしかなければ、それらのファイルを個別に暗号化したり、viエディタを使ってパスワードで保護することができます。詳細については、[47.3項「viを使用した単一ASCIIテキストファイルの暗号化」](#) (949 ページ)を参照してください。

警告: メディアの暗号化による保護には限界がある

この章で説明する方法では、限定的な保護のみ行います。実行しているシステムを侵害から保護することはできません。暗号化されたメディアが正常にマウントされると、適切なパーミッションを持つ人なら誰でもそれにアクセスできます。ただし、メディアの暗号化は、コンピュータの紛失や盗難に備える場合や、権限のないユーザによる機密データの参照を防止するような場合に役立ちます。

47.1 YaSTを使った暗号化ファイルシステムの設定

インストール中、またはすでにインストールされているシステムのパーティション、またはファイルシステムの一部を暗号化するには、YaSTを使用します。ただし、すでにインストールされているシステムのパーティションを暗号化するには、既存のパーティションのサイズ変更や区切り直しなどの複雑な作業が必要となります。このような場合は、一定サイズの暗号化ファイルを作成し、そのファイルに他のファイルやファイルシステムの一部を保管する方が簡単なこともあります。パーティション全体を暗号化するには、パーティションレイアウト内に暗号化用の専用パーティションが必要になります。ただし、YaSTによって提示されるデフォルトの標準パーティション設定には、暗号化パーティションは含まれていません。暗号化パーティションは、パーティション設定用のダイアログで手動で設定します。

47.1.1 インストール時の暗号化パーティションの作成

警告: パスワード入力

暗号化パーティションのパスワードを記録しておいてください。パスワードがなければ、暗号化データにアクセスしたり復元したりできません。

YaSTの [Expert Partitioner] ダイアログ(を参照)には、暗号化パーティションの作成に必要なオプションが用意されています。新しい暗号化パーティションを作成するには、以下の手順に従います。

- 1 [システム] > [パーティショナ] でYaSTコントロールセンターからYaSTパーティショナを実行します。
- 2 [作成] をクリックして、プライマリまたは論理パーティションを選択します。
- 3 目的のファイルシステム、サイズ、このパーティションのマウントポイントを選択します。
- 4 必要な場合にのみ暗号化ファイルシステムをマウントするには、 [Fstabのオプション] ダイアログの [システムスタート時にマウントしない] をオンにします。
- 5 [暗号ファイルシステム] チェックボックスを選択します。
- 6 [OK] をクリックします。このパーティションの暗号化に使用するパスワードの入力を求められます。このパスワードは表示されません。入力ミスを防止するため、パスワードを2回入力します。
- 7 [OK] をクリックして、処理を完了します。新しい暗号化パーティションが作成されます。

[システムスタート時にマウントしない] を選択しない場合は、オペレーティングシステムの起動時に、パーティションをマウントする前にパスワードの入力を要求されます。パーティションは、いったんマウントされるとすべてのユーザが使用できるようになります。

起動時に暗号化パーティションのマウントをスキップするには、パスワードの要求時に**Enter**キーを押します。その後、再度パスワードの入力が求められたらそれを拒否します。この場合、暗号化されたファイルシステムはマウントされません。オペレーティングシステムはブートを続けますが、データへのアクセスは遮断します。

ブート時にマウントしない暗号化パーティションにアクセスするには、`mount name_of_partition mount_point`と入力して該当するパーティションをマウントします。要求された場合はパスワードを入力します。そのパーティションでの作業を終えたら、`umount name_of_partition`を実行してアンマウントし、他のユーザからアクセスされないようにします。

すでに複数のパーティションが作成されているコンピュータにシステムをインストールする場合、インストール時に既存のパーティションを暗号化することもできます。詳細については、[47.1.2項「稼動中のシステムでの暗号化パーティションの作成」](#) (946 ページ)を参照してください。また、この操作を行うと、暗号化する既存のパーティション中のすべてのデータが破棄されてしまうことに注意してください。

47.1.2 稼動中のシステムでの暗号化パーティションの作成

警告: 稼動中のシステムでの暗号化のアクティブ化

稼動中のシステムに暗号化パーティションを作成することもできます。ただし、既存のパーティションを暗号化すると、パーティション中のすべてのデータが破壊されてしまい、既存のパーティションのサイズ変更と再構築が必要となります。

稼動しているシステムのYaSTコントロールセンターで、[\[システム\]](#)、[> \[ディスクの分割\]](#)の順に選択します。[\[はい\]](#)をクリックして続行します。[\[Expert Partitioner\]](#)で、暗号化するパーティションを選択して、[\[編集\]](#)をクリックします。以降の手順は[47.1.1項「インストール時の暗号化パーティションの作成」](#) (945 ページ)と同じです。

47.1.3 暗号化ファイルをコンテナとして作成する

パーティションを使うかわりに、一定サイズの暗号化ファイルを作成して、そのファイルに機密データを含んだ他のファイルやフォルダを保管することができます。このようなコンテナファイルは、YaST エキスパートパーティショナダイアログで作成します。[暗号化ファイル]を選択して、ファイルのフルパスとファイルのサイズを入力します。フォーマット設定およびファイルシステム種別については、提示される設定をそのまま使用するか、または変更します。マウントポイントを指定して、システムブート時に暗号化ファイルシステムをマウントするかどうかを指定します。

暗号化コンテナファイルが暗号化パーティションよりも優れている点は、ハードディスクのパーティション設定を再度行わなくても追加できるという点です。暗号化ファイルは、ループデバイスを活用してマウントされ、通常のパーティションのように動作します。

47.1.4 リムーバブルメディアの内容の暗号化

YaSTは、外部ハードディスクのようなリムーバブルメディアまたはUSBフラッシュドライブを他のハードディスクと同様に扱います。これらのメディアのコンテナファイルやパーティションは、前述の方法で暗号化できます。ただし、通常リムーバブルメディアはシステム動作中にのみ接続されるため、[Fstab Options] ダイアログで [Do Not Mount During Booting] を有効にしてください。

リムーバブルデバイスをYaSTで暗号化した場合、KDEおよびGNOMEデスクトップは暗号化パーティションを自動的に認識し、デバイスが認識されたときにパスワードを要求します。KDEまたはGNOMEを実行中にFATでフォーマットしたリムーバブルデバイスを接続した場合、パスワードを入力したデスクトップユーザが自動的にデバイスの所有者になり、ファイルを読み書きできます。FAT以外のファイルシステムを使用するデバイスの場合、root以外のユーザがそのデバイス上のファイルを読み書きするには、明示的に所有権を変更する必要があります。

47.2 暗号化ホームディレクトリの使用

ホームディレクトリ内のデータを、盗難およびハードディスクの取り外しから保護するには、YaSTユーザ管理モジュールを使用してホームディレクトリの暗号化を有効にします。新しいユーザまたは既存のユーザに対する暗号化ホームディレクトリを作成できます。既存ユーザのホームディレクトリを暗号化または復号化するには、そのユーザのログインパスワードを知っておく必要があります。手順を参照してください。

暗号化されたホームパーティションが、[47.1.3項「暗号化ファイルをコンテナとして作成する」](#) (947 ページ)で説明したようにファイルコンテナ内に作成されます。暗号化ホームディレクトリそれぞれの/homeの下に、2つのファイルが作成されます。

`LOGIN.img`

イメージを保持するディレクトリ

`LOGIN.key`

ユーザのログインパスワードで保護されたイメージキー。

ログインすると、ホームディレクトリが自動的に復号化されます。内部的には、`pam`モジュール`pam_mount`が使用されます。暗号化ホームディレクトリを作成する別のログイン方法を付加する必要がある場合は、このモジュールを`/etc/pam.d/`の該当する設定ファイルに追加する必要があります。詳細は、[第27章 PAMを使用した認証](#) (545 ページ)および`pam_mount`のマニュアルページを参照してください。

警告: セキュリティ制限

ユーザのホームディレクトリを暗号化しても、他のユーザに対しては強力なセキュリティ手段にはなりません。強力なセキュリティが必要な場合は、システムを物理的には共有しないでください。

セキュリティを強化するには、`swap`パーティション、`/tmp`および`/var/tmp`ディレクトリも暗号化してください。これらのディレクトリには、重要なデータの一時イメージが保管される可能性があります。`swap`、`/tmp`、および`/var/tmp`は、YaSTパーティションを使って暗号化することができます。詳細は、[47.1.1項「インストール時の暗号化パーティションの作成」](#)

(945 ページ)と47.1.3項「暗号化ファイルをコンテナとして作成する」
(947 ページ)を参照してください。

47.3 viを使用した単一ASCIIテキスト ファイルの暗号化

暗号化パーティションの短所は、パーティションをマウントしている間、少なくともrootはデータにアクセスできるという点です。このことを防ぐため、viを暗号化モードで 사용할 ことができます。

vi -xfilenameを使用して新しいファイルを編集します。viは、ファイルのコンテンツを暗号化し、パスワードの入力を求めます。このファイルにアクセスするたびに、viは正しいパスワードを要求します。

さらにセキュリティを向上させるため、暗号化されたファイルを暗号化されたパーティションに置くことができます。viによる暗号化はそれほど強力ではないので、このことが勧められます。

AppArmorによる権限の制限

セキュリティの脆弱性の多くは、信頼されたプログラムから発生します。信頼されたプログラムは攻撃者が好む権限を使用して実行されます。プログラムに攻撃者にそのような権限を許可してしまうバグがあると、そのプログラムは信頼性を維持できなくなります。

Novell® AppArmorは、疑わしいプログラムに対して、最低限の特権制限を提供することを目的に設計されたアプリケーションセキュリティソリューションです。AppArmorでは、プログラムが実行できる動作を指定できます。動作を指定するには、プログラムがアクセスするファイル、またはプログラムが実行する処理を定義するアプリケーションのセキュリティプロファイルを作成します。

効果的にコンピュータシステムを強固にするには、権限を仲介するプログラムの数を最小限に抑え、できるだけプログラムを安全にすることが必要です。Novell AppArmorを使用することで、必要な作業は、環境内で攻撃の危険にさらされる可能性のあるプログラムに対してのみプロファイルを作成することになります。このため、コンピュータを保護するための作業を大幅に減らすことができます。AppArmorプロファイルは、プログラムが予定通りの動作を実行するが、それ以外の動作は実行しないというポリシーを強制します。

管理者に必要なことは攻撃されやすいアプリケーションに注意を払い、それらのアプリケーションへのプロファイルを生成することだけです。システムを強固にするためには、AppArmorプロファイルを適切に作成、管理し、AppArmorのレポート機能を使ってポリシー違反や例外を監視する必要があります。

アプリケーションの動作を制限するためのAppArmorプロファイルの作成は、簡単に直感的に行うことができます。AppArmorには、プロファイル作成に役立つさまざまなツールが用意されています。プログラムやスクリプトを使う必要はありません。管理者に必要なのは、アクセス制限ポリシー、およびセキュリティを強化する必要がある各アプリケーションの実行パーミッションを決定する作業のみです。

ソフトウェア構成が変わった場合や、意図する動作範囲を変更する場合を除いて、アプリケーションプロファイルを更新または変更する必要はありません。AppArmorには、プロファイルを更新、変更するために役立つ、直感的なツールが用意されています。

ユーザがAppArmorに気付くことはありません。画面の背後で実行され、ユーザの操作を必要としません。AppArmorを利用しても、パフォーマンスに目立った影響はありません。アプリケーションの一部の処理がAppArmorプロファイルでカバーされていない場合、またはAppArmorがアプリケーションの一部の処理を妨害している場合、管理者は該当するアプリケーションのプロファイルを適切に修正する必要があります。

このガイドでは、AppArmorを使用して処理すべき基本的な作業の概要を述べ、効果的にシステムを強固にします。詳細については、『*Novell AppArmor 管理ガイド*』を参照してください。

48.1 Novell AppArmorのインストール

Novell AppArmorは、どのパターンをインストールした場合でも、SUSE Linux Enterprise®のインストール時にデフォルトでインストールされ、稼働します。AppArmorを完全に機能させるには、次のパッケージが必要です。

- apparmor-parser
- libapparmor
- apparmor-docs
- yast2-apparmor
- apparmor-profiles
- apparmor-utils
- Audit

48.2 Novell AppArmorを有効/無効にする

Novell AppArmorはSUSE Linux Enterpriseのインストール時にデフォルトで実行されるように設定されています。AppArmorのステータスを切り替えるには、次の2種類の方法があります。

YaSTシステムサービス(ランレベル)の使用

AppArmorを無効や有効にするには、システムブート時に実行される一連のスクリプトシーケンスから、ブートスクリプトを削除または追加します。変更内容は、次のシステムブート時に適用されます。

Novell AppArmorコントロールパネルの使用

稼働中のシステムでNovell AppArmorのステータスをオフまたはオンに切り替えるには、YaST Novell AppArmorコントロールパネルを使用します。ここで行った変更は、すぐに適用されます。コントロールパネルでは、AppArmorの停止や開始イベントをトリガしたり、システムのブートシーケンスにブートスクリプトを追加または削除できます。

システムブート時に実行される一連のスクリプトからAppArmorブートスクリプトを削除して、AppArmorを永続的に無効にするには、次の手順に従ってください。

- 1 rootとしてログインし、YaSTを起動します。
- 2 [システム]、> [システムサービス (ランレベル)] の順に選択します。
- 3 [エキスパートモード] を選択します。
- 4 [boot.apparmor] を選択し、[設定/リセット]、> [Disable the service] の順にクリックします。
- 5 [完了] をクリックして、YaSTランレベルツールを終了します。

次のシステムブート時から、AppArmorは実行されません。再びブート時に起動するには、サービスを有効にする必要があります。YaSTランレベルツールを使用してサービスを再度有効にする方法、無効にする手順と同様です。

稼働中のシステムでAppArmorのステータスを切り替えるには、AppArmorコントロールパネルを使用します。コントロールパネルからの変更内容はすぐに適用され、システムを再起動しても設定は引き継がれます。AppArmorのステータスを切り替えるには、以下の手順に従ってください。

- 1 rootとしてログインし、YaSTを起動します。
- 2 `[Novell AppArmor]`、> `[AppArmorコントロールパネル]` の順に選択します。
- 3 `[AppArmorを有効にする]` を選択します。AppArmorを無効にする場合は、このオプションの選択を解除してください。
- 4 `[終了]` をクリックして、AppArmorコントロールパネルを終了します。

48.3 アプリケーションのプロファイルの開始

以下の項目を慎重に考慮し、Novell AppArmorをうまくシステムへ導入する準備をします。

- 1 プロファイルするアプリケーションを判別します。詳細は[48.3.1項「プロファイルするアプリケーションの選択」](#) (955 ページ)を参照してください。
- 2 [48.3.2項「プロファイルの作成と変更」](#) (956 ページ)に概略が説明されているように、必要なプロファイルを作成します。結果を確認し、必要な場合プロファイルを調整します。
- 3 AppArmorレポートを実行し、セキュリティイベントを処理して、システムの経過を追跡してください。 [48.3.3項「Novell AppArmorイベントの通知およびレポートの設定」](#) (959 ページ)を参照してください。
- 4 使用する環境が変わるとき、またはAppArmorのレポートツールによりログに記録されたセキュリティイベントに対応する必要があるときは常に、プロファイルを更新します。 [48.3.4項「プロファイルの更新」](#) (961 ページ)を参照してください。

48.3.1 プロファイルするアプリケーションの選択

特定の設定のもとで攻撃にさらされるプログラムのみ保護する必要があるため、実際に実行するこれらのアプリケーションにのみプロファイルを使用します。最も候補となりそうなアプリケーションを判別するには、以下の一覧を使用してください。

ネットワークエージェント

オープンネットワークポートがあるプログラム（サーバおよびクライアント）メールクライアントおよびWebブラウザなどのユーザクライアントは、権限を仲介します。これらのプログラムは、ユーザのホームディレクトリへの書き込み権限を使用して実行され、敵意のあるWebサイトおよび電子メールによる悪意のあるコードなど、潜在的に敵意のあるリモートのソースからの入力进行处理します。

Webアプリケーション

Webブラウザを使用して呼び出されるプログラムです。CGI Perlスクリプト、PHPページ、およびさらに複雑なWebアプリケーションを含みます。

1 cronジョブ

cronデーモンが定期的に行うプログラムは、さまざまなソースからの入力を読み取ります。

オープンネットワークポートで現在実行しているプロセス、および制限するプロファイルが必要とするプロセスを確認するには、rootとしてaa-unconfinedを実行します。

例 48.1 aa-unconfinedの出力

```
19848 /usr/sbin/cupsd not confined
19887 /usr/sbin/sshd not confined
19947 /usr/lib/postfix/master not confined
29205 /usr/sbin/sshd confined by '/usr/sbin/sshd (enforce)'
```

上記の例の制限なしのプロセスは、制限するカスタムプロファイルを必要とする場合があります。confined byというラベル付きのものは、すでにAppArmorにより保護されています。

プロファイルを作成するアプリケーションを正しく選択するための方法については、項「**Determining Programs to Immunize**」(第1章 *Immunizing Programs*, ↑*Novell AppArmor 管理ガイド*)を参照してください。

48.3.2 プロファイルの作成と変更

SUSE Linux Enterprise上のNovell AppArmorは、最も重要なアプリケーション向けに、事前に設定されたプロファイルセットを備えています。さらに、AppArmorを使って任意のアプリケーションに対する独自のプロファイルを作成することもできます。

プロファイルの管理には2つの方法があります。一つはYaST Novell AppArmorモジュールにあるグラフィカルフロントエンドを使用すること、もう一つはAppArmorスイートにあるコマンドラインツールを使用することです。いずれの方法も同様に機能します。

48.3.1項「**プロファイルするアプリケーションの選択**」(955 ページ)で示されているように、`aa-unconfined`を実行すると、プロファイルを安全モードで実行する必要があるアプリケーションの一覧を識別できます。

各アプリケーションでプロファイルを作成するには、以下のステップを行ってください。

- 1 rootとしてログインし、`aa-genprof programname`を実行してAppArmorにアプリケーションのプロファイルの概要を作成させます。

または

基本的なプロファイルの概要を作成するには、`[YaST] > [Novell AppArmor] > [プロファイルの追加ウィザード]`の順に選択してウィザードを実行し、プロファイルを作成するアプリケーションの完全パスを指定します。

基本的なプロファイルの概要が表示され、AppArmorはラーニングモードに設定されます。実行中のプログラムの任意の処理がログに記録されますが、処理は制御されません。

- 2 AppArmorがアプリケーションの動作の非常に具体的な像を得られるよう、アプリケーションの動作の全範囲を実行します。
- 3 **ステップ 2** (957 ページ)で生成されたログファイルをAppArmorに分析させるには、aa-genprofでSキーを押します。

または

[プロファイルの追加ウィザード] で [AppArmorイベントのシステムログのスキャン] をクリックして、ウィザードの指示に従いプロファイルを完成させて、ログを分析します。

AppArmorはアプリケーションの実行中に記録したログをスキャンし、記録された各イベントへのアクセス権を設定するよう求めます。各ファイルへのアクセス権を設定するか、またはグロッピングを使用します。

- 4 アプリケーションの複雑さによっては、**ステップ 2** (957 ページ)と**ステップ 3** (957 ページ)を繰り返す必要があります。アプリケーションを制限し、制限された状況下で試してみて、新しいログイベントを生成します。幅広いアプリケーションを適切に制限するために、この手順を何回か繰り返さなければならないこともあります。
- 5 一度アクセス権が設定されると、プロファイルは強制モードに設定されます。プロファイルが適用され、作成されたプロファイルに従ってAppArmorはアプリケーションを制御します。

既存のプロファイルがコンプレインモードであったアプリケーションに対しaa-genprofを起動すると、このプロファイルでは、このラーニングサイクルを終了する際にラーニングモードを保持します。プロファイルのモード変更の詳細は、aa-complain—Entering Complain or Learning Mode項 (第4章 *Building Profiles from the Command Line*, ↑Novell AppArmor 管理ガイド)とaa-enforce—Entering Enforce Mode項 (第4章 *Building Profiles from the Command Line*, ↑Novell AppArmor 管理ガイド)を参照してください。

制限したアプリケーションを使用し、必要なすべての処理を行って、プロファイルの設定をテストしてください。通常、制限されたプログラムは円滑に実行し、ユーザがAppArmorの動作に気付くことはありません。しかし、アプリケーションのある種の間違いに気付いた場合、システムログを確認して、AppArmorが必要以上にアプリケーションを抑制していないかを確認します。

システムで使われているログのメカニズムに応じて、AppArmorのログエントリを参照できる場所も変わります。

`/var/log/audit/audit.log`

auditパッケージがインストールされ、auditdが動作している場合、AppArmorイベントは次のように記録されます。

```
type=APPARMOR msg=audit(1140325305.502:1407): REJECTING w access to
/usr/lib/firefox/update.test (firefox-bin(9469) profile
/usr/lib/firefox/firefox-bin active /usr/lib/firefox/firefox-bin)
```

`/var/log/messages`

auditdが使われていない場合、AppArmorイベントは/var/log/messagesの標準システムログに記録されます。ログエントリの例を以下に示します。

```
Feb 22 18:29:14 dhcp-81 klogd: audit(1140661749.146:3): REJECTING w access
to /dev/console (mdnsd(3239) profile /usr/sbin/mdnsd active
/usr/sbin/mdnsd)
```

`dmesg`

auditdが動作していない場合、dmesgコマンドを使ってAppArmorイベントを確認することもできます。

```
audit(1140661749.146:3): REJECTING w access to /dev/console (mdnsd(3239)
profile /usr/sbin/mdnsd active /usr/sbin/mdnsd)
```

プロファイルを調整するには、**ステップ 3** (957 ページ)の説明に従って、このアプリケーションに関連するログメッセージを分析します。プロンプトが表示されたら、アクセス権またはアクセス制限を指定します。

ティップ: 詳細情報

プロファイルの作成と変更の詳細は、第2章 *Profile Components and Syntax* (↑Novell AppArmor 管理ガイド)、第3章 *Building and Managing Profiles with YaST* (↑Novell AppArmor 管理ガイド)、および第4章 *Building Profiles from the Command Line* (↑Novell AppArmor 管理ガイド)を参照してください。

48.3.3 Novell AppArmorイベントの通知およびレポートの設定

セキュリティイベントの確認を行えるよう、Novell AppArmorでイベントの通知を設定します。イベントの通知は、選択した重要度レベルのもとで全体に及ぶNovell AppArmor動作が発生したときに、特定の電この機能は現在、YaSTインタフェースから入手できます。

YaSTでイベントの通知を設定するには、以下のように進めます。

- 1 イベントの通知を配信するには、システムでメールサーバが実行していることを確認します。
- 2 rootとしてログインし、YaSTを起動します。次に、*[Novell AppArmor]*、> *[AppArmorコントロールパネル]* の順に選択します。
- 3 *[セキュリティイベント通知を有効にする]* で *[環境設定]* を選択します。
- 4 各レコードの種類（*[簡潔]*、*[概要]* および *[詳細]*）に対し、レポートの頻度を設定し、レポートを受け取る電子メールアドレスを入力し、記録するイベントの重要度を判定します。イベントレポートに未知のイベントを含める場合は、*[未知の重要度イベントを含める]* をオンにします。

注意: ログするイベントの選択

AppArmorのイベント分類に精通している場合意外は、すべてのセキュリティレベルのイベントについて通知を受けることを選択します。

- 5 *[OK]* > *[完了]* の順にクリックして設定を適用し、このダイアログを終了します。

Novell AppArmorレポートを使用すると、aa-logprofツールだけに役立つ扱いにくいメッセージを手動で取捨選択することなく、ログファイルにレポートされた重要なNovell AppArmorセキュリティイベントを参照できます。レポートのサイズは、日付またはプログラム名の範囲でフィルタリングをして絞り込むことができます。

AppArmorのレポートを設定するには、以下の手順に従います。

- 1 rootとしてログインし、YaSTを起動します。 [Novell AppArmor] > [AppArmor レポート] の順に選択します。
- 2 調べたいレポートの種類を選択するか、または [エグゼクティブセキュリティサマリ]、[アプリケーション監査]、および [セキュリティ問題レポート] から設定します。
- 3 [編集] を選択して要求されたデータを表示し、レポート生成の頻度、電子メールアドレス、エクスポート形式、およびレポートの場所を編集します。
- 4 選択した種類のレポートを実行するには、[今すぐ実行] をクリックします。
- 5 [アーカイブの参照] を選択し、レポートの種類を指定して、各種類のアーカイブされたレポートをブラウズします。

または

必要ないレポートを削除するか、新しいレポートを追加します。

ティップ: 詳細情報

Novell AppArmorのイベント通知の設定に関する詳細は、項「Configuring Security Event Notification」(第6章 *Managing Profiled Applications*, ↑Novell AppArmor 管理ガイド)を参照してください。 レポート設定の詳細は、項「Configuring Reports」(第6章 *Managing Profiled Applications*, ↑Novell AppArmor 管理ガイド)を参照してください。

48.3.4 プロファイルの更新

ソフトウェアおよびシステムの設定は、時間とともに変化します。そのため、状況に応じてAppArmorのプロファイル設定を微調整する必要があります。AppArmorでは、システムログや他のAppArmorイベントをチェックして、ポリシーに違反するイベントが発生していないかどうかを確認し、必要に応じてプロファイルを調整できます。また、プロファイルの定義外であるアプリケーションの動作はすべて、[プロファイルウィザードの更新] を使用して処理できます。

プロファイルセットを更新するには、以下のように進めます。

- 1 rootとしてログインし、YaSTを起動します。
- 2 [Novell AppArmor] > [プロファイルウィザードの更新] を選択します。
- 3 指示が出たら、リソースまたはログされた実行ファイルに対してアクセスを調整するか権限を実行します。
- 4 すべての質問に答えたら、YaSTを閉じます。変更は各プロファイルに適用されます。

ティップ: 詳細情報

システムログからプロファイルを更新する方法の詳細については、項「Updating Profiles from Log Entries」(第3章 *Building and Managing Profiles with YaST*, ↑Novell AppArmor 管理ガイド)を参照してください。

セキュリティと機密性

LinuxまたはUNIXシステムの主な特性は、同時に複数のユーザを処理できること(マルチユーザ)と、これらのユーザが同じコンピュータ上で同時に複数のタスクを実行できること(マルチタスキング)です。さらに、オペレーティングシステムはネットワークを意識させません。通常、ユーザは自分が使用しているデータやアプリケーションが各自のマシンからローカルに提供されているのか、ネットワークを介して使用可能になっているかを意識することはありません。

マルチユーザ機能を使用する場合、様々なユーザのデータを別々に格納する必要があります。また、セキュリティとプライバシーを保証する必要があります。データのセキュリティは、コンピュータをネットワーク経由でリンクできるようになる以前から、すでに重要な問題になっていました。現在と同様に、最重要課題は、データメディア(ほとんどの場合はハードディスク)が消失したり他の方法で破損した場合にも、データを使用可能な状態で維持する機能でした。

この章では、主として機密性の問題とユーザのプライバシーを保護する手段について重点的に説明します。ただし、定期的に更新されて作業可能なテスト済みバックアップを常に備えておくための手順を確立することが包括的なセキュリティの概念には不可欠であるという点については、詳しく説明しません。この手順がなければ、何らかのハードウェア障害が発生した場合のみでなく、誰かが不正にアクセスしてファイルを改ざんしたという疑いが生じた場合にも、データの復旧作業に手間と時間がかかることになります。

49.1 ローカルセキュリティとネットワークセキュリティ

データにアクセスするには、次のような複数の方法があります。

- 必要な情報を持っているユーザとの個人的な通信、またはコンピュータ上のデータへのアクセス
- コンピュータのコンソールからの直接アクセス(物理アクセス)
- シリアル回線を介したアクセス
- ネットワークリンクを使用したアクセス

いずれの場合も、ユーザが問題のリソースやデータにアクセスするには、認証を受ける必要があります。この点ではWebサーバはあまり限定的ではありませんが、すべての個人データを第三者に公開しないようにする必要はあります。

上記のリストのうち、最初の項目では、銀行の担当者に連絡したときに自分が口座名義人であるという証明を要求される場合のように、多くの対話を必要とします。この場合は、署名、PINまたはパスワードなど、自分の身元を証明する情報を提供するように要求されます。場合によっては、単に知っている情報を断片的に述べ、言葉巧みに信頼させて相手から情報を引き出す可能性もあります。その結果、情報が少しずつ明らかになり、そのことに気づかないことさえあります。ハッカーの間では、この行為を「ソーシャルエンジニアリング」と呼んでいます。この行為を防止するには、人々を教育し、言語や情報を自覚して取り扱うしかありません。通常、攻撃者はコンピュータシステムに侵入する前に、受付係、会社のサービススタッフ、家族などをターゲットにしようとします。多くの場合、このようなソーシャルエンジニアリングに基づく攻撃は、はるか後になるまで発見されません。

他人のデータに不正にアクセスしようとする第三者は、従来の方法を使用して他人のハードウェアに直接接続を試みることもあります。そのため、マシンは他人にコンポーネントを削除、交換または無効化されないように、あらゆる改ざんから保護する必要があります。これは、バックアップ、ネットワークケーブル、電源コードにも当てはまります。また、一部のキーの組合せは異常動作を引き起こす場合があるため、ブート手順も保護してください。自

己防衛のためには、BIOSとブートローダーのパスワードを設定する必要があります。

シリアルポートに接続されたシリアル端末は、従来から多くの場所で使用されています。ネットワークインタフェースとは異なり、ホストとの通信をネットワークプロトコルに依存しません。デバイス間での単なる文字のやりとりには、単純なケーブルまたは赤外線ポートが使用されます。このようなシステムでは、ケーブル自体が一番の弱点になります。古いプリンタを接続すれば、ケーブルを通じて伝送されるすべてのデータを記録できてしまいます。攻撃対象によっては、プリンタで実行できることであれば他の方法でも実行できます。

ホスト上でファイルをローカルに読み込むには、他のホスト上でサーバとのネットワーク接続をオープンする以外のアクセスルールが必要です。ローカルセキュリティとネットワークセキュリティには、違いがあります。つまり、データをどこかにパケット単位で送信する必要がある場合には、回線が使用されます。

49.1.1 ローカルセキュリティ

ローカルセキュリティは、コンピュータが稼働している場所の物理環境から始まります。マシンは、セキュリティ上の要件やニーズに沿った場所に設置してください。ローカルセキュリティの主な目標は、誰も他人の権限や識別情報を偽れないように、常にユーザを相互に分離しておくことです。これは遵守すべき原則ですが、ユーザ`root`の場合はシステム上で最高の権限を持つため、このことが特に重要になります。`root`ユーザは、パスワードを求めるプロンプトなしで、他のすべてのローカルユーザの識別情報を使用して、ローカルに格納されているファイルをすべて読み込むことができます。

49.1.2 パスワード

Linuxシステムでは、パスワードが平文として格納されることはなく、入力されたテキスト文字列が保存されているパターンと単に照合されるのでもありません。平文として格納され、保存されているパターンと照合されるのみであれば、対応するファイルに誰かがアクセスした直後、システム上のすべてのアカウントが危険にさらされることになります。代わりに、格納されているパスワードは暗号化されており、入力されるパスワードもそのたびに再び暗号化され、暗号化された2つの文字列が比較されます。この方法でセキュリ

ティレベルが向上するのは、暗号化されたパスワードを逆算して元のテキスト文字列に戻せない場合のみです。

実際には、この処理は特殊なアルゴリズムによって達成されます。このアルゴリズムは、一方向にしか機能しないため、「トラップドアアルゴリズム」とも呼ばれます。暗号化された文字列を攻撃者が入手しても、単に同じアルゴリズムを再適用するだけでは他人のパスワードを取得できません。代わりに、暗号化すると他人のパスワードになる組合せが見つかるまで、考えられる文字の組合せをすべてテストする必要があります。パスワードが長さ8文字であれば、計算が必要な組合せの候補は膨大な数になります。

1970年代には、使用されていたアルゴリズムが比較的低速で、1つのパスワードを暗号化するだけで数秒かかっていたため、この方法が他の方法よりも安全であると言われていました。ただし、その後はPCのパフォーマンスが向上し、毎秒数10万～数100万回の暗号化を実行できるようになっています。このため、暗号化されたパスワードは通常のユーザが参照できないようにする必要があります(通常のユーザは/etc/shadowファイルを読み込めません)。さらに重要なのは、何らかのエラーが原因でパスワードファイルが参照可能になった場合に備えて、簡単に推測できないパスワードを使用することです。したがって、「tantalise」のようなパスワードを「t@nt@1ls3」に「変換」したとしても、実際には役に立ちません。

語句の一部の文字を数字に同じパターンで置き換えただけでは、安全とは言えません。辞書を使用して語句を推測するパスワードクラックプログラムも、これと同様の置換を行います。そこで、「The Name of the Rose」 by Umberto Eco(ウンベルトエーコ著『薔薇の名前』)のように、文や書名に含まれる語句の頭文字など、一般的な意味はなく、自分にしか意味のない語句を作成するのが適切な方法です。こうして作成される「TNotRbUE9」のようなパスワードは安全と言えます。これに対して、「beerbuddy」や「jasmine76」のようなパスワードは、ユーザに関してわずかしき知識のない他人でさえ簡単に推測できます。

49.1.3 ブート手順

システムは、ドライブ全体を取り外すか、BIOSパスワードを設定してハードディスクからでなければブートできないようにBIOSを設定し、フロッピーやCDからはブートできないように設定してください。通常、Linuxシステムはブートローダーから起動するため、ブートしたカーネルに追加のオプションを渡すことができます。/boot/grub/menu.lst内でパスワードを追加設定し、他

のユーザがこの種のパラメータをブート時に使用できないようにしてください(を参照)。**第21章 ブートローダ**(445 ページ)これはシステムのセキュリティに不可欠です。カーネル自体がroot権限で実行されるのみでなく、システム起動時にroot権限を付与する最初の認可でもあります。

49.1.4 ファイルのパーミッション

通常は、特定のタスクに可能な最も限定的な権限で作業します。たとえば、電子メールを読み書きするには、rootユーザである必要はありません。メールプログラムにバグがあると、このバグが攻撃にさらされ、起動時にプログラムのパーミッションが正確に処理されてしまう可能性があります。限定的な権限のルールに従って、考えられる損害を最小限に抑えてください。

SUSE Linux Enterpriseのディストリビューションパッケージに付属するすべてのファイルについては、パーミッションが慎重に選択されています。ソフトウェアや他のファイルを追加インストールするシステム管理者は、特にパーミッションビットの設定時には細心の注意を払う必要があります。経験豊富でセキュリティ意識の高いシステム管理者は、常にコマンドlsで-lオプションを使用して広範なファイルリストを取得します。これにより、不正なファイルパーミッションを即時に検出できます。不正なファイル属性は、そのファイルが変更または削除された可能性を意味するだけではありません。このように変更されたファイルがrootユーザにより実行される可能性や、設定ファイルの場合はこの種のファイルがプログラムでrootユーザの権限で使用される可能性があります。このため、攻撃者が侵入する可能性が大幅に増大します。このような攻撃は、カッコウが他の鳥をだまして自分の卵を孵化させるのと同様に、プログラム(卵)が他のユーザ(鳥)によって実行(孵化)されるため、カッコウの卵と呼ばれます。

SUSE Linux Enterpriseシステムでは、ファイルpermissions、permissions.easy、permissions.secure、およびpermissions.paranoidがすべてディレクトリ/etcにあります。これらのファイルの目的は、world-writableなディレクトリなどの特殊な権限や、ファイルに対するsetuser IDビットを定義することです(setuser IDビットが設定されているプログラムは、それを起動したユーザの権限ではなく、ファイル所有者、ほとんどの場合はrootユーザの権限で実行されます)。管理者は、ファイル/etc/permissions.localを使用して自分専用の設定を追加できます。

SUSE Linux Enterpriseの環境設定プログラムが上記のどのファイルを使ってパーミッションを設定するかを定義するには、YaSTの「ローカルセキュリティ」セクションで、「*Security and Users*」を選択します。このトピックの詳細は、`/etc/permissions`内のコメントまたは`chmod`のマニュアルページを(`man chmod`コマンドを実行して)参照してください。

49.1.5 バッファオーバーフローと書式文字列のバグ

プログラムがユーザによる変更が可能なデータを処理すると思われる場合は、特に注意する必要がありますが、これは通常のユーザよりもアプリケーションプログラマにとって問題です。プログラマは、小さすぎてデータを保持できないメモリ領域に書き込むことなく、自分のアプリケーションでデータが適切に解析されることを確認する必要があります。また、プログラムでは、専用に定義されたインタフェースを使用して、データを一貫した方法で受け渡す必要があります。

実際のメモリバッファのサイズを考慮しないと、そのバッファの書き込み時に「バッファオーバーフロー」が発生する可能性があります。また、このデータ(ユーザが生成)に使用される領域が、バッファ内で使用可能な領域を超える場合があります。その結果、データはそのバッファ領域の終わりを越えて書き込まれ、状況によってはプログラムで単にユーザデータが処理されるのではなく、ユーザ(プログラマではなく)が変更したプログラムシーケンスが実行される可能性があります。この種のバグは、特にプログラムが特殊な権限で実行されている場合には、重大な結果を招きます(49.1.4項「ファイルのパーミッション」(967 ページ)を参照)。

書式文字列のバグの場合、動作は少し異なりますが、プログラムの異常動作を引き起こす可能性のあるユーザ入力です。ほとんどの場合、この種のプログラミングエラーは、`setuid`プログラムや`setgid`プログラムなど、特殊な権限で実行されるプログラムに見られます。これも、対応する実行権限をプログラムから削除することで、データとシステムをこの種のバグから保護できることを意味します。また、最善の方法は、考えられる最小権限を使用するというポリシーを適用することです(49.1.4項「ファイルのパーミッション」(967 ページ)を参照)。

バッファオーバーフローと書式文字列のバグがユーザデータの処理に関連するバグであるとすれば、アクセス権がローカルアカウントに付与されている

場合にのみ発生するわけではありません。レポートされているバグの多くは、ネットワークリンク上でも利用される可能性があります。したがって、バッファオーバーフローと書式文字列のバグは、ローカルセキュリティとネットワークセキュリティの両方に関連する問題として分類する必要があります。

49.1.6 ウィルス

通説とは異なり、Linux上で動作するウィルスは存在します。ただし、判明しているウィルスは、テクニックが意図したとおりに動作することを証明するために、作成者が自分のアイデアの証明としてリリースしたものです。この種のウィルスは、これまでのところいずれも一般には検出されていません。

ウィルスは、活動するホストがなければ存続も拡散もできません。たとえば、ホストがプログラムやシステムの重要な記憶領域(マスターブートレコードなど)であり、そこにウィルスのプログラムコードを書き込む必要があるとします。Linuxにはマルチユーザ機能があるため、特定のファイルへの書き込みアクセスを制限でき、これは特にシステムファイルの場合に重要です。したがって、root権限で通常の作業を実行すると、システムがウィルスに感染する可能性が増大します。これに対して、考えられる最小権限を使用するという原則に従えば、ウィルスに感染する可能性は低下します。

それとは別に、実際には知らないインターネットサイトからはプログラムを実行しないようにする必要があります。SUSE Linux EnterpriseのRPMパッケージは、その作成に必要な措置が講じられたデジタルラベルとして暗号署名を使用します。ウィルスは、管理者やユーザにセキュリティに関して必要な自覚が欠けており、設計によって高度に保護されているシステムであっても危険にさらす可能性があることを示す典型的な兆候です。

ウィルスをワームと混同しないようにする必要があります。ワームの対象はネットワーク全体です。ワームの拡散にはホストを必要としません。

49.1.7 ネットワークセキュリティ

ネットワークセキュリティは、外部で開始される攻撃から保護する場合に重要です。ユーザ認証にユーザ名とパスワードを必要とする典型的なログイン手順は、ローカルセキュリティの課題です。ネットワーク経由の特殊なログインの場合は、2つのセキュリティの課題を区別してください。実際の認証ま

でに発生する処理はネットワークセキュリティに関連し、その後に発生する処理はローカルセキュリティに関連します。

49.1.8 X Window SystemとX認証

冒頭に述べたように、ネットワーク透過性は、UNIXシステムの中核的な特性の1つです。UNIXオペレーティングシステムのウィンドウシステムであるXは、この機能を優れた方法で実現します。Xを使用すると、リモートホストでログインしてグラフィカルプログラムを起動しても基本的には問題はなく、グラフィカルプログラムはネットワーク経由で送信されてコンピュータに表示されます。

Xサーバを使用してXクライアントをリモートで表示する必要がある場合、Xサーバは管理対象のリソース(ディスプレイ)を不正アクセスから保護する必要があります。より厳密には、クライアントプログラムに特定の権限を付与する必要があります。X Window Systemでは、この権限付与をホストベースのアクセスコントロールおよびCookieベースのアクセスコントロールと呼ばれる2通りの方法で実行できます。前者は、クライアントが実行されるホストのIPアドレスに依存します。これを制御するプログラムがxhostです。xhostは正当なクライアントのIPアドレスをXサーバに属する小型データベースに入力します。ただし、認証はIPアドレスに依存するため、安全度は高くありません。たとえば、クライアントプログラムを送信中のホストで第2のユーザが作業している場合、そのユーザはXサーバにもアクセスできます。IPアドレスを盗む第三者はこれと同じことをしているに過ぎません。このような欠点があるため、ここではこの認証方式について詳述しません。詳細は、manxhostを参照してください。

Cookieベースのアクセスコントロールの場合は、ある種のIDカードと同様に、Xサーバと正当なユーザにのみ認識される文字列が生成されます。このCookie(通常のクッキーを意味するのではなく、エピソードが入っている中国のフォーチュンクッキー)は、ログイン時にユーザのホームディレクトリのファイル.Xauthorityに格納され、Xサーバを使用してウィンドウを表示しようとするすべてのXクライアントで使用できます。ファイル.Xauthorityは、ツールxauthを使用して検査できます。.Xauthorityの名前を変更したり、意図せずにホームディレクトリから削除すると、新規のウィンドウやXクライアントをオープンできなくなります。X Window Systemのセキュリティメカニズムの詳細は、Xsecurityのmanページを参照してください(manXsecurity)。

SSH(セキュアシェル)を使用すると、ユーザには暗号化メカニズムを意識させることなく、ネットワーク接続を完全に暗号化してXサーバに透過的に転送(フォワード)することができます。この処理は「X転送」とも呼ばれます。X転送は、サーバ側でXサーバをシミュレートし、リモートホスト上でシェルのDISPLAY変数を設定することで行われます。SSHについての詳細な情報は第44章 **SSH: セキュアネットワークオプション** (905 ページ)を参照してください。

警告

ログイン先のホストに対して、ホストの保護を考慮していない場合は、X転送を使用しないでください。X転送を有効にすると、攻撃者がユーザのSSH接続を介して認証し、Xサーバに侵入し、ユーザになりすましてキーボード入力などを行う可能性があります。

49.1.9 バッファオーバーフローと書式文字列のバグ

49.1.5項「**バッファオーバーフローと書式文字列のバグ**」(968 ページ)で説明したように、バッファオーバーフローと書式文字列のバグは、ローカルセキュリティとネットワークセキュリティの両方に関係する課題として分類する必要があります。この種のバグのローカルバリエーションと同様に、ネットワークプログラムでのバッファオーバーフローは、首尾よく利用されてしまうと、ほとんどの場合はroot権限の取得に使用されます。それ以外の場合にも、攻撃者がバグを利用して権限のないローカルアカウントにアクセスし、システムに存在する他の脆弱部分を利用する可能性があります。

ネットワークリンク経由で利用される恐れのあるバッファオーバーフローと書式文字列のバグは、リモート攻撃全体で最も頻度の高い形式であることは確実です。このような、新しく見つかったセキュリティホールを悪用するプログラムは、しばしばセキュリティメーリングリストに投稿されます。この情報を使用すると、コードの詳細を知らなくても脆弱部分を絞り込むことができます。多年の経験では、オペレーティングシステムメーカーは自社ソフトウェアの問題を修正せざるを得ないため、悪用可能なコードを知ることがオペレーティングシステムのセキュリティレベル向上に役立つことが判明しています。フリーソフトウェアを使用すれば、誰でもソースコードにアクセスでき(SUSE Linux Enterpriseの場合は、ソースコードがすべて使用可能です)、

脆弱部分とその悪用可能なコードを見つけたユーザは誰でも、対応するバグ修正のためのパッチを発行できます。

49.1.10 サービス拒否

DoS攻撃は、サーバプログラムまたはシステム全体をブロックすることを目的にしています。そのために、サーバを過負荷状態にして、常時無駄なパケットを送信してビジー状態にしたり、リモートバッファオーバーフローを引き起こすなど、さまざまな手段が用いられます。通常、DoS攻撃はサービスの消失のみを目的として実行されます。ただし、特定のサービスが使用不能になると、*man-in-the-middle*攻撃(パケット盗聴、TCP接続のハイジャック、偽装攻撃)やDNSポイズニングなどに対して脆弱になる可能性があります。

49.1.11 中間者攻撃:盗聴、ハイジャック、なりすまし

一般に、通信中のホスト間に割り込む攻撃者が実行するリモート攻撃は、「*man-in-the-middle*攻撃」と呼ばれます。ほぼすべてのタイプの*man-in-the-middle*攻撃に共通するのは、通常、ユーザは何が起きているのかに気づかないことです。攻撃者が接続要求をターゲットマシン宛てに転送するなど、様々なバリエーションが考えられます。その場合、相手のマシンは有効な接続先マシンであるかのように偽装されているので、知らないうちに不正なホストとの接続が確立されることになります。

最も単純なタイプの中間者攻撃は盗聴(傍受)と呼ばれ、攻撃者はネットワークトラフィックを傍受します。より複雑な「*man in the middle*」攻撃は、すでに確立された接続を乗っ取ろうとします(ハイジャック)。これを実現するため、攻撃者は一定時間だけパケットを分析し、接続に属するTCPシーケンス番号を予測する必要があります。攻撃者が最終的にターゲットホストのローンを停止すると、エラーのため接続が終了したことを示すエラーメッセージが「95V5c」示されるため、このことがわかります。暗号化を介してハイジャックから保護されるプロトコルはなく、接続の確立時には単純認証手順しか実行されないことが、攻撃を容易にしています。

偽装攻撃は、パケットが偽のソースデータ(通常はIPアドレス)を含むように変更される攻撃です。攻撃に利用させる手段の多くは偽のパケット(Linuxマシン

ではスーパーユーザであるrootのみしか実行できないようなパケット)を送りつける方法です。

前述の攻撃の多くは、DoSと組み合わせて実行されます。特定のホストを短時間でも突然停止できることが攻撃者にわかれば、ホストは攻撃で一定時間は干渉できなくなるため、攻撃者は容易にアクティブ攻撃をかけられるようになります。

49.1.12 DNSポイズニング

DNSポイズニングとは、攻撃者が偽装したDNSリプライパケットで応答し、サーバの情報を要求しているユーザに対して、そのサーバから特定のデータを送信するよう試みることにより、DNSサーバのキャッシュを破壊す⁷とを意味します。多くのサーバは、IPアドレスまたはホスト名に基づいて他のホストとの信頼関係を維持しています。攻撃者は、ホスト間の信頼関係の実際の構造を詳細に理解した上で、自分を信頼のおけるホストの1つとして偽装する必要があります。通常、攻撃者はサーバから受信した一部のパケットを分析し、必要な情報を取得します。また、しばしば攻撃者はネームサーバも適切なタイミングによるDoS攻撃のターゲットとする必要があります。接続先ホストの識別情報を確認できる、暗号化された接続を使用することで、自分自身を保護してください。

49.1.13 ワーム

ワームはしばしばウィルスと混同されますが、両者には明らかな違いがあります。ウィルスとは異なり、ワームはホストプログラムに感染しなくても活動できます。代わりに、ネットワーク構造上でできるだけ迅速に拡散するように特化されています。Ramen、Lion、Adoreなど、これまでに出現したワームは、bind8やlprNGなどのサーバプログラムの周知のセキュリティホールを使用しています。ワームからの保護は、比較的容易です。代わりに、ネットワーク構造上でできるだけ迅速に拡散するように特化されています。これが役立つのは、管理者が問題のシステムにセキュリティ更新を実際にインストールする場合のみです。

49.2 セキュリティ全般のヒントとテクニック

セキュリティの問題に適切に対処するには、新規の開発に遅れをとらず、常に最新のセキュリティ問題に関する情報を入手することが重要です。システムをあらゆる種類の問題から保護するために、セキュリティ通知で推奨されているパッケージ更新版をできるだけ迅速に入手してインストールすることをお薦めします。SUSEのセキュリティ通知はメーリングリストで公開されており、リンク<http://en.opensuse.org/Communicate/Mailinglists>から参加できます。リストopensuse-security-announce@opensuse.orgは、パッケージ更新版に関する最初の情報源であり、アクティブな貢献者の中でもSUSEのセキュリティチームのメンバーが含まれています。

メーリングリストopensuse-security@opensuse.orgは、必要なセキュリティ問題の説明の参照先として活用できます。同じWebページから参加してください。

bugtraq@securityfocus.comは、世界中で最もよく知られているセキュリティメーリングリストです。このリストは1日15～20件を受け付けているため、このリストを参照することをお勧めします。詳細は、<http://www.securityfocus.com>を参照してください。

ここでは、基本的なセキュリティ問題に対処する上で役立つルールについて説明します。

- ジョブごとに考えられる最も限定的な権限セットを使用するというルールに従い、日常的なジョブはroot ユーザで実行しないようにします。これにより、カッコウの卵やウィルスに感染する危険性が減少し、自分自身のミスも防止できます。
- セキュリティホールが検出されてからワームがサーバに侵入するまでにある程度の時間があれば、影響を受けるプログラムの更新バージョンが間に合う可能性が大きくなります。telnet、ftp、rshおよびrloginの代わりにssh(セキュアシェル)を使用することを、習慣づけてください。
- IPアドレスのみに基づく認証方式は使用しないでください。

- 最も重要なネットワーク関連パッケージは常に更新し、対応するメーリングリストにサブスクライブして、この種のプログラム(bind、sendmail、ssh など)の新バージョンに関する通知を受け取ります。これは、ローカルセキュリティに関連するソフトウェアの場合も同じです。
- /etc/permissionsファイルを変更し、システムのセキュリティに不可欠なファイルのパーミッションを最適化します。プログラムからsetuidビットを削除すると、そのジョブは意図した方法で実行できなくなる場合があります。一方、ほとんどの場合、プログラムの潜在的なセキュリティリスクもなくなることを考慮してください。同様のアプローチは、world-writableなディレクトリおよびファイルにも適用できます。
- サーバの正常動作に不可欠でないネットワークサービスを停止します。これにより、システムの安全性が向上します。ソケットがLISTEN状態のオープンポートは、プログラムnetstatで検出できます。オプションとしてnetstat -apまたはnetstat -anpを使用することをお勧めします。-pオプションを使用すると、指定した名前のポートを使用しているプロセスを確認できます。

netstatの結果を、ホスト外部から実行したポートスキャンの結果と比較します。このジョブに適したプログラムはnmapで、マシンのポートが確認されるのみでなく、その背後で待機中のサービスについてもある程度の情報が得られます。ただし、ポートスキャンは攻撃的な行為と解釈される場合があるため、管理者から明示的な承認を受けない限りホスト上では実行しないでください。最後に、TCPポートのみでなくUDPポートも検出することが重要であることを忘れないでください(オプション-sSおよび-sUを使用します)。

- システムのファイルの整合性を信頼できる方法で監視するには、SUSE Linux Enterpriseで利用可能なプログラムAIDE (Advanced Intrusion Detection Environment)を使用します。他人に改ざんされないように、AIDEで作成されたデータベースは暗号化します。さらに、マシン外部から使用可能なこのデータベースのバックアップは、ネットワークリンクで接続されていない外部データメディアに格納します。
- サードパーティソフトウェアのインストール時には、適切な措置を講じます。幸いにして迅速に発見されたものの、ハッカーがセキュリティソフトウェアパッケージのtarアーカイブにトロイの木馬を組み込んでいた事例が

あります。バイナリパッケージをインストールする場合は、それをダウンロードしたサイトを信頼します。

SUSEのRPMパッケージは、GPGにより署名されています。SUSEが署名に使用している鍵は、次のとおりです。

```
ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
```

コマンド`rpm--checksig package.rpm`を実行すると、アンインストールされたパッケージのチェックサムと署名が正しいかどうかを確認できます。この鍵は、配布パッケージCDの1枚目と、世界中のほとんどのキーサーバにあります。

- ユーザファイルとシステムファイルのバックアップを定期的にチェックします。バックアップが動作するかどうかをテストしなければ、実際には役に立たない可能性があることを考慮してください。
- ログファイルを確認します。可能な場合は、小型スクリプトを記述して疑わしいエントリを検索します。実際、これは些細な作業ではありません。結局のところ、どのエントリが例外的でどのエントリがそうでないかわかるのは自分だけです。
- `tcp_wrapper`を使用して、サービスに接続できるIPアドレスを明示的に制御できるように、マシンで実行中の個々のサービスへのアクセスを制限します。`tcp_wrapper`の詳細は、`tcpd`および`hosts_access`の`man`ページを参照してください(`man 8 tcpd`, `man hosts_access`)。
- `SuSEfirewall`を使用して、`tcpd` (`tcp_wrapper`)が提供するセキュリティを強化します。
- セキュリティ手段は冗長性を確保するように設計してください。何もメッセージが表示されないよりは、メッセージが複数回表示される方がセキュリティ上はお勧めできます。

49.3 Central Security Reporting Addressの使用

セキュリティ関連の問題を発見した場合は(はじめに使用可能な更新パッケージを確認してから)、security@suse.deに電子メールでお送りください。その際に、問題の詳しい説明と、関係するパッケージのバージョン番号をお知らせください。SUSEは、できる限り迅速に応答するように努めています。電子メールメッセージはpgpで暗号化することをお薦めします。SUSEのPGP鍵は:

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>  
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```


この鍵は<http://www.novell.com/linux/security/securitysupport.html>からもダウンロードできます。

パート VI. トラブルシューティング

ヘルプとドキュメント

SUSE Linux Enterprise®には、さまざまな情報と文書が付属しています。Help Center は、使用中のシステムに関する最も重要な文書にアクセスするための集中的な手段であり、それらのドキュメントは検索可能な形式で提供されています。これらのリソースの中には、インストール済みのアプリケーションに関するオンラインヘルプ、マニュアルページ、情報ページ、ハードウェアに関するデータベース、および製品に付属しているすべてのマニュアル含まれます。

50.1 SUSE Help Centerの使用方法

メインメニューから([SUSE Help Center] を選択)またはシェルでコマンド `susehelp` を実行することで、初めてSUSE Help Centerを起動すると、 **50.1. 「SUSE Help Centerのメインウィンドウ」** (982 ページ)に示すウィンドウが表示されます。このダイアログウィンドウは、以下の3つの主要領域で構成されています。

メニューバーとツールバー

メニューバーには、編集、移動、および環境設定に関する主要なオプションがあります。[ファイル] メニューには現在表示されているコンテンツを印刷するためのオプションもあります。検索機能にアクセスするには、[編集] メニューを使用します。[移動] には、[目次] (Help Center のホームページ)、[戻る]、[進む]、および [最後の検索結果] など、すべてのナビゲーション機能が含まれています。[設定] > [Build Search Index] を選択すると、選択されているすべての情報ソースに関する検索インデックスを生成することができます。ツールバーには、3つの移動ア

アイコン([進む] 、 [戻る] 、 [ホーム])と、現在のコンテンツを印刷するためのプリンタアイコンもあります。

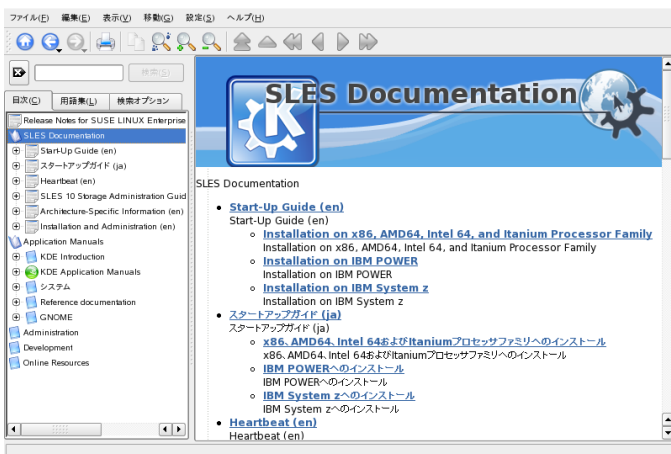
タブ付きの移動エリア

ウィンドウの左側にある移動(ナビゲーション)エリアには、選択された情報ソース内で、すぐに検索をするための入力フィールドがあります。[検索] タブ内での検索と検索機能の設定の詳細については、[50.1.2項「検索機能」](#)(983 ページ)を参照してください。[コンテンツ] タブには、現時点でインストール済みで、使用可能な情報ソースすべてがツリー形式で表示されます。ブックアイコンをクリックすると、個別のカテゴリが開いて、参照可能になります。

ビューウィンドウ

ビューウィンドウには常に、現在選択されているコンテンツが表示されます。オンラインマニュアル、検索結果、またはWebページなどがこれに該当します。

50.1 SUSEHelp Centerのメインウィンドウ



注意: 言語選択ビュー

SUSE Help Centerで利用可能なマニュアルは現在の言語によって異なります。言語を変更するとツリービューが変わります。

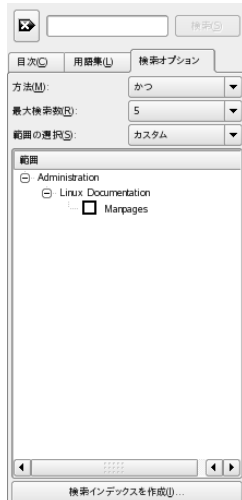
50.1.1 目次

SUSE Help Centerでは、さまざまなソースから得られた役立つ情報を提供しています。SUSE Linux Enterprise用のドキュメント(*Start-Up*、*KDE User Guide*、*GNOME User Guide*、および*Reference*)、使用中のワークステーション環境で使用可能な情報ソースすべて、インストール済みのプログラムに関するオンラインヘルプ、および他のアプリケーション用のヘルプテキストです。さらに、SUSE Help Centerを使用してSUSE Linux Enterpriseに関連するハードウェアとソフトウェアのトピックを網羅している、SUSEのオンラインデータベースにアクセスすることもできます。検索インデックスを一度生成すると、これらのソースすべてを快適に検索できます。

50.1.2 検索機能

SUSE Linux Enterpriseのインストール済み全情報ソースを検索するには、検索インデックスを生成し、いくつかの検索パラメータを設定します。この作業を行うには、[図 50.2. 「検索機能の設定」](#) (983 ページ)に示されている[検索]タブを使用します。

図 50.2 検索機能の設定



以前に検索インデックスが生成されていない場合は、ユーザが[検索]タブをクリックした時点、または検索文字列を入力して[検索]ボタンをクリックした時点で、システムは自動的に検索インデックスを生成するかどうかを確認するメッセージを表示します。図 50.3. 「検索インデックスの生成」(984 ページ)の検索インデックスを生成するウィンドウで、チェックボックスを使ってインデックスを作成する情報ソースを選択します。[インデックス作成]をクリックしてこのダイアログを終了すると、インデックスの生成が開始されます。

図 50.3 検索インデックスの生成



検索対象を限定し、できるだけ関連性の高いヒットリストを得るには、3つのドロップダウンメニューを使用して、表示されるヒット数(検索数)、および検索対象ソースの選択エリア(スコープ)を決定します。選択エリアを決定する際は、次の各オプションを使用できます。

デフォルト

定義済みのソース選択領域を検索します。

すべて

すべてのソースを検索します。

なし

検索する際に、どのソースも選択しません。

カスタム

概要リストの中で、該当するチェックボックスをオンにすることにより、検索対象のスコープを決定します。

検索条件の設定を完了したら、[検索] ボタンをクリックします。該当する項目がビューウィンドウ内で表示され、マウスをクリックするだけでそれらの項目間を移動できるようになります。

50.2 manページ

マニュアルページは、どのLinuxシステムにおいても重要な役割を担っています。マニュアルページでは、コマンドと利用可能なオプションおよびパラメータについての使用法が説明されています。マニュアルページは、表 50.1. 「マニュアルページ—カテゴリと説明」 (985 ページ)(マニュアルページ自身から抽出)に示すように、カテゴリ別にソートされています。

表 50.1 マニュアルページ—カテゴリと説明

[数値]	説明
1	実行可能プログラムまたはシェルコマンド
2	システムコール(カーネルによって提供される機能)
3	ライブラリコール(プログラムライブラリ内での機能)
4	特別なファイル(通常は/dev内にある)
5	ファイル形式と命名規則(/etc/fstab)
6	ゲーム
7	その他(マクロパッケージおよび規則)、例：man(7)、groff(7)
8	システム管理コマンド(通常はrootに関するもののみ)
9	カーネルルーチン(非標準)

一般に、マニュアルページはコマンドに関連付けて配布されています。マニュアルページは、**Help Center**で参照するか、シェル内で直接参照することができます。マニュアルページをシェル内で表示するには、`man`コマンドを使用します。たとえば、`ls`のマニュアルページを表示するには、「`man ls`」と入力します。各マニュアルページは、*NAME*、*SYNOPSIS*、*DESCRIPTION*、*SEE ALSO*、*LICENSING*および*AUTHOR*といういくつかのパートで構成されています。コマンドのタイプによっては、他のセクションが追加されている場合があります。マニュアルページを終了するには、`<Q>`キーを使用します。

マニュアルページを表示するもう1つの方法としては、**Konqueror**の使用があります。**Konqueror**を起動し、たとえば、「`man:/ls`」と入力します。1つのコマンドに対して異なるカテゴリがある場合、**Konqueror**はそれらのカテゴリをリンクで表示します。

50.3 情報ページ

情報ページは、システム上にあるもう1つの重要な情報ソースです。通常、情報ページの内容はマニュアルページよりも詳細です。情報ページは情報ビューアを使用して参照でき、「ノード」と呼ばれる異なるセクションを表示することができます。」このタスクを実行するには、`info`コマンドを使用します。たとえば、`info`自体の情報ページを表示するには、シェルで「`info info`」と入力します。

さらに簡単に操作する場合は、**Help Center**または**Konqueror**を使用します。**Konqueror**を起動し、「`info:/`」と入力すると、最上位レベルの情報が表示されます。`grep`の情報ページを表示するには、「`info:/grep`」と入力します。

50.4 Linux Documentation Project

Linux Documentation Project(TLDP)は、LinuxおよびLinux関連のマニュアルを制作するボランティアチームによって運営されています(<http://www.tldp.org>を参照)。マニュアルのセットには初心者向けのチュートリアルも含まれますが、主にシステム管理者などの経験者向けの内容になっています。TLDPは、HOWTO(操作方法)、FAQ(よくある質問)、ガイド(ハンドブック)を無償で提供しています。

50.4.1 HOWTO(操作方法)

HOWTOは通常、特定のタスクの実行について、処理を順番に簡略に示したものです。これは、上級者によって書かれた初心者向けの記述であり、順を追った説明がなされています。たとえば、DHCPサーバの設定方法などがあります。HOWTOは、howtoパッケージ内にあり、`/usr/share/doc/howto`にインストールされます。

50.4.2 よくある質問とその回答

FAQ(よくある質問)は、一連の質問と回答をまとめたものです。FAQはもともと、初歩的な同じ質問が繰り返し投稿されるのを減らすため、Usenetニュースグループが始めたものです。

50.5 Wikipedia:無償のオンライン百科事典

ウィキペディアは「多言語で提供される百科事典であり、誰でも読み込みと編集が行えるように設計されています」(を参照)。<http://en.wikipedia.org> ウィキペディアの内容はウィキペディアのユーザによって作成され、無償で公開されます(GDFL)。ウィキペディアへの訪問者は誰でも記事を編集することができるため、破壊行為の危険性を伴いますが、このことが原因でサイトへの訪問を拒否されることはありません。ウィキペディアには4,000,000件以上の記事が登録されており、ほとんどのトピックに対し、答えを見つけることができます。

50.6 ガイドブック

Linuxのトピックに関連した、広範囲のガイドブックが入手可能です。

50.6.1 SUSEのガイドブック

SUSEでは、詳細で有益なガイドブックを用意しています。これらのガイドブックは、HTMLおよびPDFの各バージョンを複数の言語で提供しています。PDFファイルは、DVDのdocuディレクトリにあります。HTML版は、`opensuse-manual_LANG`パッケージをインストールしてください(`LANG`は、利用したい言語で置き換えてください)。インストールすると、それらをSUSE Help Centerで表示できるようになります。

50.6.2 他のマニュアル

SUSE Help Centerでは、さまざまなトピックやプログラムについてのマニュアルとガイドブックを提供しています。詳細については<http://www.tldp.org/guides.html>を参照してください。「*Bash Guide for Beginners* (初心者のためのBashガイド)」から「*Linux Filesystem Hierarchy*」、*Linux Administrator's Security Guide* (Linux 管理者のセキュリティガイド) などがあります。一般に、ガイドブックの内容はHOWTOやFAQよりも、詳細な情報を網羅しています。これらのガイドブックは通常、上級者によって執筆されており、内容も上級者向けです。中には古いガイドブックもありますが、内容はまだ十分通用するものです。これらのガイドブックはYaSTを使用してインストールします。

50.7 パッケージのドキュメント

パッケージをシステムにインストールすると`/usr/share/doc/packages/package_name`というディレクトリが作成されます。そこには、パッケージのメンテナが記したファイルや、SUSEからの付加的な情報が置かれます。また、例となるファイル、設定ファイル、付加的なスクリプトなどが含まれていることもあります。通常は、以下のようなファイルが含まれています。しかし、これらは標準的なものでないため、すべてのファイルが用意されているわけではありません。

AUTHORS

パッケージの主な開発者のリストが記されています。通常はそれぞれの役割も書かれています。

BUGS

パッケージの既知のバグや不具合などが記されています。通常、**Bugzilla Web**ページへのリンクもあり、そこでバグを検索することができます。

CHANGES , ChangeLog

バージョン間の変更点の概要です。非常に詳細なものなので、通常は、開発者にとって興味あるものです。

COPYING , LICENSE

ライセンス情報。

FAQ

メーリングリストやニュースグループから集められた質問と答えが含まれています。

INSTALL

パッケージをシステムにインストールするための手順が含まれています。通常はパッケージをすでにインストールしているはずなので、必要はありません。

README , README.*

使用方法についての一般的な情報、そのパッケージで行える事柄などが記されています。

今後の課題

まだ実装されていないものの、今後実装される予定の機能についての説明です。

MANIFEST

ファイルのリストと、それぞれの簡単な概要です。

NEWS

このバージョンでの新しい点が記されています。

50.8 Usenet

1979年、インターネットがまだ普及する以前に創設されたUsenetは、最大級のコンピュータネットワークであり、現在もその活動を継続しています。Usenet

の記事のフォーマットと伝送方式は、電子メールと非常に似ていますが、多数対多数のコミュニケーションを目的として開発された点が異なります。

Usenetでは、記事は7つのカテゴリに分けられています:comp.*は、コンピュータ関連のディスカッションが行われています。misc.*は、雑多な話題を取り扱っています。news.*は、ニュースグループ関連の話題を取り扱っています。rec.*は、レクリエーションとエンターテインメントについて取り扱っています。sci.*は、サイエンス関連の話題を取り扱っています。soc.*は、ソーシャル関連の話題を取り扱っています。talk.*は、さまざまな議論を取り扱っています。これらの最上位のレベルは、さらにサブグループに分けられています。たとえば、comp.os.linux.hardwareでは、Linuxに関連したハードウェアの話題を扱っています。

記事の投稿を行うには、クライアントをニュースサーバに接続して、目的のニュースグループに加入する必要があります。ニュースクライアントにはKnodeやEvolutionがあります。各ニュースサーバは、互いに通信することによって記事を交換し合います。加入を行ったニュースサーバですべてのニュースグループが利用できない場合があります。

Linuxユーザ向けのニュースグループとしては、comp.os.linux.apps、comp.os.linux.questions、およびcomp.os.linux.hardwareがあります。特定のニュースグループを見つけられない場合は<http://www.linux.org/docs/usenetlinux.html>を参照してください。ご利用の際は、<http://www.faqs.org/faqs/usenet/posting-rules/part1/>で閲覧可能なUsenetの一般規則に従ってください。

50.9 規格と仕様

規格と仕様に関する情報は、さまざまな情報源から提供されます。

<http://www.linuxbase.org>

Free Standards Groupは、無償ソフトウェアとオープンソースソフトウェアの配布を促進する独立した非営利団体です。この団体は、ディストリビューションに依存しない規格を定義することで、この目標達成に努めています。また、重要なLSB (Linux Standard Base、Linux標準ベース)など、複数の規格の維持管理を監督しています。

<http://www.w3.org>

World Wide Web Consortium (W3C)は、最もよく知られた標準化団体です。1994年10月にTim Berners-Leeによって設立され、Webテクノロジーの標準化に専念しています。W3Cは、HTML、XHTML、XMLなど、メーカーに依存しないオープン仕様の無償による普及を促進しています。これらのWeb規格はワーキンググループにおいて4段階のプロセスを経て開発され、W3C勧告(REC)として一般に公表されます。

<http://www.oasis-open.org>

OASIS (構造化情報標準促進協会: Organization for the Advancement of Structured Information Standards)は、Webセキュリティ、Eビジネス、商取引、ロジスティクス、各種市場間の相互運用性に関する標準の開発を専門とする国際団体です。

<http://www.ietf.org>

Internet Engineering Task Force (IETF)は、研究者、ネットワーク設計者、サプライヤ、ユーザが参加する国際的な団体です。インターネットアーキテクチャの開発とプロトコルを使用したインターネット運用の円滑化を目的としています。

IETFによる標準はすべてRFC (Request for Comments)として公開され、無償で入手できます。RFCには、提案、ドラフト、インターネット標準、実験プロトコル、情報ドキュメント、および記録の6種類のRFCがあります。より狭義では、最初の3タイプ(提案、ドラフト、完成版)のみがIETFの標準といえます(<http://www.ietf.org/rfc/rfc1796.txt>を参照)。

<http://www.ieee.org>

電気電子学会(Institute of Electrical and Electronics Engineers: IEEE)は、情報技術、通信、医薬、輸送などの分野における標準を策定する組織です。IEEEの標準は有償です。

<http://www.iso.org>

国際標準化機構委員会(ISO Committee: International Organization for Standards)は、世界最大の標準開発機関であり、世界140カ国の標準化機関からなるネットワークを維持しています。ISOの標準は有償です。

<http://www.din.de> , <http://www.din.com>

ドイツ工業規格(Deutsches Institut für Normung, DIN)は、登録された技術および科学関連の協会です。DINは1917年に設立されました。DINによれば、この組織は「ドイツにおける標準を取り扱い、各国およびヨーロッパ

の標準化団体に対してドイツの考えを提示することを目的とした組織」です。

この組織にはメーカー、消費者、貿易業者、サービス業者、科学者、標準の設立に関心を持つその他の人々が参加しています。標準は有償であり、DINのホームページから発注できます。

最も頻繁に起こる問題およびその解決方法

51

この章では、できるだけ多くの起こり得る問題のタイプについて説明することを意図して、最も頻繁に起こる可能性のある一連の問題について述べます。そうすることで、実際に遭遇した状況がここにリストされていない場合でも、解決のヒントを与えるのに十分類似したものがあり得ます。

51.1 情報の検索と収集

Linuxでは、詳細なログが取得されます。システムの使用中に問題が発生した場合、調べる必要のあるところは何箇所かあります。それらのほとんどは、Linuxシステム一般で標準とされるもので、あとの残りはSUSE Linux Enterpriseシステムに特有のものです。大半のログファイルはYaSTを使って表示することができます([その他] > [ログの起動])。

YaSTでは、サポートチームが必要な情報の大半を収集することができます。 [その他] > [クエリーのサポート] .を使用してください。問題のカテゴリを選択します。すべての情報が収集されたら、それをサポートリクエストに添付します。

以下に、最も一般的に確認されるログファイルおよびそのファイルが通常含んでいるもののリストを示します。

表 51.1 ログファイル

ログファイル	説明
/var/log/boot.msg	ブート時にカーネルから受け取るメッセージです。
/var/log/mail.*	メールシステムから受け取るメッセージです。
/var/log/messages	起動中に、カーネルおよびシステムのログデーモンから継続的に受け取るメッセージです。
/var/log/ NetworkManager	NetworkManagerからのログファイルで、ネットワーク接続についての問題を収集します。
/var/log/SaX.log	SaXディスプレイとKVMシステムから受け取るハードウェアメッセージです。
/home/user/ .xsession-errors	現在実行中のデスクトップアプリケーションからのメッセージです。userは、実際の値で置き換えられます。
/var/log/warn	カーネルおよびシステムのログデーモンから受け取る、警告レベル以上が割り当てられたすべてのメッセージです。
/var/log/wtmp	現在のコンピュータセッションのユーザのログインレコードを含むバイナリファイルです。lastコマンドを使用して表示させます。
/var/log/Xorg.*.log	Windowシステムから受け取る、起動時および実行時のさまざまなログです。Xの失敗した起動をデバッグするのに役に立ちます。
/var/log/YaST2/	YaSTのアクションとその結果を保管するディレクトリ。
/var/log/samba/	Sambaサーバおよびクライアントのログメッセージを含んでいるディレクトリです。

ログファイルとは別に、稼働中のシステムの情報も提供されます。詳細については、[表 51.2: システム情報](#)を参照してください。

表 51.2 システム情報

ファイル	説明
/proc/cpuinfo	プロセッサのタイプ、製造元、モデル、およびパフォーマンスなどを含む情報を表示します。
/proc/dma	どのDMAチャネルが現在使用されているかを表示します。
/proc/interrupts	どの割り込みが使用されているか、各割り込みの使用回数を表示します。
/proc/iomem	I/Oメモリの状態を表示します。
/proc/ioports	その時点でどのI/Oポートが使用されているかを表示します。
/proc/meminfo	メモリの状態を表示します。
/proc/modules	個々のモジュールを表示します。
/proc/mounts	現在マウントされているデバイスを表示します。
/proc/partitions	すべてのハードディスクのパーティション設定を表示します。
/proc/version	現在のLinuxバージョンを表示します。

Linuxには、システム解析とモニタリング用のさまざまなツールが含まれています。システム診断で使用する最も重要なツールの選択については、[第17章 システムモニタリングユーティリティ](#) (361 ページ)を参照してください。

以下に含まれる各シナリオは、問題を説明するヘッダに続いて、推奨される解決方法、詳細な解決方法への利用可能な参照、および関連する他のシナリオへの相互参照が書かれた、1つまたは2つの段落から構成されています。

51.2 インストールの問題

インストールの問題とは、コンピュータがインストールに失敗した状態のことを指します。インストールが全体において失敗する、またはグラフィカルインストーラが起動できないという可能性があります。ここでは、通常経験するような問題のいくつかに集中して説明し、そのような場合に考えられる解決方法または回避方法を示します。

51.2.1 メディアの確認

SUSE Linux Enterpriseの使用時に問題が発生した場合は、`[ソフトウェア] > [メディアチェック]`を選択してインストールメディアの整合性をチェックすることができます。メディアの問題は、独自に作成したメディアを使用する場合により発生します。SUSE Linux EnterpriseのCDまたはDVDをチェックするには、メディアをドライブに挿入してYaSTの場合は`[開始]`をクリックして、メディアのMD5のチェックサムを確認してください。これには少し時間がかかります。問題が検出された場合、インストール用にこのメディアを使用しないでください。

51.2.2 ハードウェア情報

`[ハードウェア] > [ハードウェア情報]`を使用して、検出されたハードウェアおよび技術データを表示します。デバイスの詳細については、任意のツリーノードをクリックします。たとえば、サポートを依頼するときに、ハードウェアに関する情報が必要な場合などに、このモジュールが特に役立ちます。

`[Save to File (ファイルに保存)]`をクリックして、表示されたハードウェア情報をファイルに保存します。希望するディレクトリとファイル名を選択し、`[保存]`をクリックしてファイルを作成します。

51.2.3 ブート可能なCD-ROMドライブが利用不可能

お使いのコンピュータにブート可能なCDまたはDVD-ROMドライブがない場合、または使用しているドライブがLinuxでサポートされていない場合、内蔵CDまたはDVD-ROMドライブを使用しないでコンピュータをインストールするオプションがいくつかあります。

フロッピーディスクからのブート

ブートフロッピーを作成し、CDまたはDVDの代わりにフロッピーディスクからブートします。

外付けブートデバイスの使用

コンピュータのBIOSおよびインストールカーネルでサポートされている場合は、インストール時に外部CDまたはDVDドライブからブートします。

PXE経由のネットワークブート

コンピュータにCDまたはDVDドライブがない場合でも、使用可能なイーサネット接続がある場合は、完全にネットワークベースのインストールを実行します。詳細については、[4.1.3項「VNC経由のリモートインストール—PXEブートとWake on LAN」](#) (57 ページ)と[4.1.6項「SSH経由のリモートインストール—PXEブートとWake on LAN」](#) (61 ページ)を参照してください。

フロッピーディスク(SYSLINUX)からのブート

旧式のコンピュータには、ブート可能なCD-ROMドライブはなく、フロッピーディスクドライブしかないものがあります。そのようなシステムにインストールするには、ブートディスクを作成し、それを使ってシステムを起動します。

ブートディスクには、ローダSYSLINUXとプログラムlinuxrcも含まれています。SYSLINUXを使用すると、ブート時にカーネルを選択し、使用するハードウェアに必要なパラメータを指定できます。プログラムlinuxrcは、使用するハードウェア用のカーネルモジュールのローディングをサポートし、その後インストールを開始します。

ブートディスクからブートする際は、ブート処理は、ブートローダーSYSLINUX(パッケージsyslinux)によって開始されます。システムが起動す

ると、SYSLINUXは、以下のステップで構成される、最小限のハードウェア検出検査を実行します。

1. ブートローダは、BIOSがVESA 2.0準拠のフレームバッファサポートを提供しているかどうかを調べ、適宜、カーネルを起動します。
2. モニタデータ(DDC info)が読み込まれます。
3. 1番目のハードディスクの最初のブロック(MBR)が読み込まれ、BIOS IDとLinuxのデバイス名がブートローダの設定時に対応付けられます。ブートローダは、BIOSのlba32関数を使用して当該ブロックを読み込み、BIOSがそれらの関数をサポートしているかどうかを判別します。

SYSLINUXの開始時に、<Shift>キーを押したままにすると、上記のステップはすべてスキップされます。トラブルシューティングの目的で、

```
verbose 1
```

syslinux.cfgに次の行を挿入した場合、ブートローダは、現在実行中のアクションを表示します。

マシンがフロッピーディスクからブートしない場合は、BIOS内のブートシーケンスをA,C,CDROMに変更しなければならないことがあります。

外付けブートデバイス

ほとんどのCD-ROMドライブがサポートされています。CD-ROMドライブからブートできない場合は、CD-SetのCD 2からブートを試みてください。

システムにCD-ROMもフロッピーディスクもない場合でも、USB、FireWire、またはSCSIを使用して外部接続したCD-ROMを使用してシステムをブートできます。これは、BIOSおよびご利用のハードウェアのインタラクションに大きく依存します。問題が発生した場合、BIOSアップデートにより解決する場合があります。

51.2.4 インストールメディアからのブートに失敗する

コンピュータがインストール時に起動しない理由には2つのものが考えられます。

CDまたはDVD-ROMドライブのブートイメージを読み込み不可能
ご使用のCD-ROMドライブがCD 1 上のブートイメージを読み込めない場合、CD 2を使用してシステムをブートしてください。CD2には従来の2.88MBブートイメージが格納されており、サポートされていないドライブでも読み込むことができます。それにより、**第4章 リモートインストール** (53 ページ)で説明されているように、ネットワークを介してのインストールができます。

BIOS内での不正なブートシーケンス

BIOSブートシーケンスでは、ブート用の最初のエントリとしてCD-ROMがセットされている必要があります。そうでない場合、コンピュータは他のメディア(通常ハードディスク)からブートを試みます。BIOSのブートシーケンスを変更するための説明が、マザーボードに付属するマニュアルまたは以下の段落で提供されます。

BIOSとはコンピュータの非常に基本的な機能を有効にするソフトウェアです。マザーボードを供給するベンダが、独自のハードウェア用のBIOSを供給します。通常、BIOSセットアップは特別な時(マシンのブート時)にだけアクセスされます。この初期化段階の間に、マシンは数多くのハードウェア診断テストを実行します。そのうちの1つとして、メモ리카ウンタにより示されるメモリチェックがあります。メモ리카ウンタが表示されたとき、通常カウンタの下または画面の下部の辺りに、BIOSセットアップにアクセスするために押すキーについて表示されています。通常押すキーは、キー、<F1>キー、または<Esc>キーです。BIOSセットアップ画面が表示されるまでこのキーを押します。

手順 51.1 BIOSのブートシーケンスの変更

- 1 ブートルーチンによって宣言されたように、適切なキーを使用してBIOSを入力します。その後、BIOS画面が表示されるのを待ちます。
- 2 AWARD BIOSでブートシーケンスを変更するには、[BIOS FEATURES SETUP]エントリを探してください。他のメーカーでは、[ADVANCED

CMOSSETUP] といった違う名前が使用されています。エントリが見つかったなら、そのエントリを選択して、<Enter>キーを押して確定します。

- 3 開いた画面で、[*BOOTSEQUENCE*] というサブエントリを探します。ブートシーケンスは、通常C, AまたはA, Cのように設定されています。C, Aの場合、マシンは最初にハードディスク(C)を検索し、次にフロッピーディスクドライブ(A)を検索して、ブート可能なメディアを検出します。ブートシーケンスがA, CDROM, Cになるまで<PgUp>キーまたは<PgDown>キーを押して、設定を変更します。
- 4 <Esc>キーを押してBIOS設定画面を終了します。設定を保存するには、[*SAVE & EXIT SETUP*] を選択し、<F10>キーを押します。設定が保存されていることを確認するには、<Y>キーを押します。

手順 51.2 SCSI BIOS (Adaptec ホストアダプタ) 内でのブートシーケンスの変更

- 1 Ctrl + Aを押してセットアップを開きます。
- 2 [*Disk Utilities*] を選択します。接続されているハードウェアコンポーネントが表示されます。

ご使用のCD-ROMドライブに割り当てられているSCSI IDの記録をとります。
- 3 <Esc>キーを押して、メニューを閉じます。
- 4 [アダプタセッティングの設定] を開きます。[追加オプション] で、[*Boot Device Options*(ブートデバイスオプション)] を選択し、<Enter>キーを押します。
- 5 CD-ROMドライブのIDを入力して、再度<Enter>キーを押します。
- 6 <Esc>キーを2回押して、SCSI BIOSの起動画面に戻ります。
- 7 [はい] を押して、この画面を終了しコンピュータを起動します。

最終的なインストールが使用する言語やキーボードレイアウトに関係なく、BIOS設定では、通常以下の図に示されているようなUSキーボードレイアウトが使用されます。

☒ 51.1 USキーボードレイアウト



51.2.5 ブートできない

ハードウェアのタイプ(主にかかなり旧式かごく最近のタイプ)では、インストールが失敗するものもあります。多くの場合、インストールカーネル内でこのタイプのハードウェアのサポートが欠けているか、または、ある種のハードウェアに問題を引き起こすACPIのような、カーネルに含まれている特定の機能が原因の可能性があります。

最初のインストールブート画面から、標準の [インストール] モードを使用してインストールするのに失敗した場合、以下のことを試してみてください。

- 1 最初のCDまたはDVDがCD-ROMドライブにまだ入った状態であれば、**Ctrl+Alt+Del**キーを押すか、ハードウェアリセットボタンを使用して、コンピュータを再起動します。
- 2 ブート画面が表示されたら、キーボードの<矢印>キーを使用して、[インストール--ACPIは無効] を探して、**Enter**このオプションはACPIの電源管理技術が無効にします。
- 3 第3章 *YaSTによるインストール* (21 ページ)の中での説明に従って、インストールを進めます。

これが失敗する場合、以上で述べた手順の代わりに [インストール--セーフ設定] を選択してインストール処理を続行します。このオプションはACPIおよびDMAサポートを無効化します。このオプションを使うと、ほとんどのハードウェアが起動するはずです。

両方のオプションともに失敗する場合、ブートオプションプロンプトを使用して、ハードウェアタイプをサポートするのに必要な追加のパラメータをインストールカーネルに渡します。ブートオプションとして使用可能なパラメータの詳細については、`/usr/src/linux/Documentation/kernel-parameters.txt`にあるカーネルマニュアルを参照してください。

ティップ: カーネルマニュアルの取得

`kernel-source`パッケージをインストールして、カーネルマニュアルを表示します。

他にさまざまなACPI関連のカーネルパラメータがあります。それらのパラメータは、インストールのために起動する前のブートプロンプトで入力できます。

`acpi=off`

このパラメータは、コンピュータ上の完全ACPIサブシステムを無効にします。これはコンピュータがACPIをまったく処理できない場合、またはコンピュータのACPIが問題を引き起こしていると考えられる場合に役に立ちます。

`acpi=force`

2000年より前の日付が付けられた古いBIOSを持つコンピュータであっても、常にACPIを有効にします。このパラメータは、`acpi=off`に加えて設定された場合、ACPIも有効にします。

`acpi=noirq`

ACPIはIRQルーティングには使用しません。

`acpi=ht`

`hyper-threading`を有効化するのに十分なACPIのみ実行します。

`acpi=strict`

厳密にはACPI仕様互換ではないプラットフォームに対する耐性が弱くなります。

`pci=noacpi`

新しいACPIシステムのPCI IRQルーティングを無効にします。

`pnpcapi=off`

このオプションは、BIOSセットアップに誤った割り込みまたはポートがある場合のシリアルまたはパラレルの問題向けです。

`notsc`

タイムスタンプカウンタを無効にします。このオプションを使用して、システムのタイミングについての問題に対処できます。これは新機能で、マシンに特に時間や全面的なハングなどの遅れが見られる場合に、このオプションを試す価値があります。

`nohz=off`

nohz機能を無効にします。マシンがハングした場合、このオプションが役に立ちます。一般にはこれは不要です。

一旦パラメータの正しい組み合わせを決定したら、システムが次回適切に起動することを確実にするために、YaSTは自動的にそれらのパラメータをブートローダーの設定に書き込みます。

カーネルのロード中、またはインストール中に説明できないエラーが発生した場合は、ブートメニューから [メモリテスト] を選択し、メモリを確認します。 [メモリテスト] がエラーを返す場合、それは通常はハードウェアのエラーです。

51.2.6 グラフィカルインストーラを起動できない

最初のCDまたはDVDをドライブに挿入しコンピュータを再起動した後に、インストール画面が表示されますが、 [インストール] を選択すると、グラフィカルインストーラは起動しません。

この問題に対処する方法はいくつかあります。

- インストールダイアログ用に、他の画面解像度を選択してみます。
- インストール用に [テキストモード] を選択します。

- VNCを介して、グラフィカルインストーラを使ってリモートインストールをします。

インストールのために他の画面解像度に変更するには、以下の手順に従います。

- 1 インストールのために起動します。
- 2 F3キーを押して、インストール用に低解像度を選択するメニューを開きます。
- 3 [インストール] を選択し、**第3章 YaSTによるインストール** (21 ページ) 中の説明に従ってインストールを続行します。

テキストモードでインストールを実行するには、以下の手順に従います。

- 1 インストールのために起動します。
- 2 F3キーを押して、[テキストモード] を選択します。
- 3 [インストール] を選択し、**第3章 YaSTによるインストール** (21 ページ) 中の説明に従ってインストールを続行します。

VNCによるインストールを実行する場合、以下の手順に従います。

- 1 インストールのために起動します。
- 2 ブートオプションプロンプトに以下のテキストを入力します。

```
vnc=1 vncpassword=some_password
```

`some_password`の部分はインストール用に使用するパスワードに置き換えます。

- 3 [インストール] を選択し、キーを押してインストールを開始します。
Enter

グラフィカルインストーラルーチンに入るかわりに、システムはテキストモードで実行され、その後停止します。その際、IPアドレスおよびポート番号が含まれるメッセージが表示されますが、それらは、ブラウザインタフェースまたはVNCビューアアプリケーションを使用してインストーラにアクセスできるようにするために必要です。

- 4 ブラウザを使用してインストーラにアクセスする場合、ブラウザを起動して将来SUSE Linux Enterpriseが起動するコンピュータ上のインストール手順で与えられたアドレス情報を入力し、Enterキーを押します。

`http://ip_address_of_machine:5801`

ブラウザウィンドウでは、VNCのパスワードを入力するように要求するダイアログが開かれます。パスワードを入力し、**第3章 YaSTによるインストール** (21 ページ)の説明に従ってインストールを続行します。

重要項目

VNC経由のインストールでは、Javaサポートが有効化されていれば、オペレーションシステムやブラウザの種類を問いません。

好みのオペレーティングシステム上でVNCビューア(種類を問わない)を使用する場合、要求されたらPアドレスとパスワードを入力します。インストールダイアログを表示するウィンドウが開きます。通常のようにインストールを続行します。

51.2.7 最低限のブート画面だけが起動する

最初のCDまたはDVDをドライブに挿入して、BIOSルーチンは終了しますが、システム上でグラフィカルブート画面が開始しません。その代わりに、最小限のテキストベースのインタフェースが起動されます。これは、グラフィカルブート画面を表示するのに十分なグラフィックメモリを持っていないコンピュータを使用する場合に起こる可能性があります。

テキストのブート画面は最小限に見えますが、グラフィカルブート画面が提供する機能とほぼ同じものを提供します。

ブートオプション

グラフィカルインタフェースとは違い、キーボードのカーソルキーを使って異なるブートオプションを選択することはできません。テキストモードのブート画面のブートメニューでは、ブートプロンプトで入力するキーワードが表示されます。これらのキーワードはグラフィカルバージョンで提供されているオプションにマップしています。任意の選択を入力し<Enter>キーを押して、ブートプロセスを起動します。

カスタムブートオプション

ブートオプションを選択したあと、ブートプロンプトで適切なキーワードを入力するか、**51.2.5項「ブートできない」** (1001 ページ)の中で説明されているカスタムブートオプションを入力します。インストールプロセスを起動するには、<Enter>キーを押します。

画面解像度

Fキーを使用して、インストール用の画面解像度を判別します。テキストモードで起動する必要がある場合は、キーを選択します。

51.3 ブートの問題

ブートの問題とは、システムが適切に起動しないような場合を指します(意図したランレベルおよびログイン画面まで起動しない場合)。

51.3.1 GRUBブートローダのロードに失敗する

ハードウェアが問題なく機能している場合、ブートローダが壊れてしまってLinuxがコンピュータ上で起動できない可能性があります。このような場合、ブートローダを再インストールする必要があります。ブートローダを再インストールするには、以下の手順に従います。

- 1 インストールメディアをドライブに挿入します。
- 2 コンピュータを再起動します。
- 3 ブートメニューから [インストール] を選択します。
- 4 言語を選択します。
- 5 使用許諾契約に同意します。
- 6 [インストールモード] 画面で、[その他] を選択し、インストールモードを [インストールしたシステムの修復に設定します]。

- 7 YaSTシステム修復モジュールの中で、[\[エキスパート設定用ツール\]](#)を選択し、[\[新しいブートローダのインストール\]](#)を選択します。
- 8 元の設定を復元し、ブートローダを再インストールします。
- 9 YaSTシステム修復を修復し、システムを再起動します。

何らかの理由でグラフィックインタフェースが表示されない場合や、システムを手動で修復する場合は、[レスキューシステムの使用項\(1030 ページ\)](#)の手順を参照してください。

コンピュータが起動しない理由は他にBIOS関連のものが考えられます。

BIOS設定

ハードドライブを参照するためのBIOSを確認してください。ハードドライブ自体が現在のBIOS設定に見つからない場合、GRUBが単に開始されない可能性があります

BIOSブートオーダー

お使いのシステムのブートオーダーがハードディスクを含んでいるか確認します。ハードディスクオプションが有効になっていない場合、システムは適切にインストールされていますが、ハードディスクへアクセスする必要がある際に起動に失敗する可能性があります。

51.3.2 グラフィカルログインはありません

コンピュータは起動するものの、グラフィカルログインマネージャが起動しない場合は、デフォルトのランレベルの選択、あるいはX Window Systemの設定のいずれかに問題があると考えられます。ランレベルの設定を確認するには、rootユーザでログインし、コンピュータがランレベル5(グラフィカルデスクトップ)に起動する設定になっているか確認します。この確認を手軽にする方法は、`/etc/inittab`の内容を以下のように調べることです。

```
nld-machine:~ # grep "id:" /etc/inittab
id:5:initdefault:
nld-machine:~ #
```

返された行は、コンピュータのデフォルトランレベル(`initdefault`)が5に設定されており、グラフィカルデスクトップに起動するはずであることを示

しています。ランレベルが}5以外の数に設定されていた場合は、YaSTのランレベルエディタモジュールを使用して、5に設定します。

重要項目

ランレベル設定を手動では編集しないでください。そうしないと、**SuSEconfig** (YaSTによって実行される)が次回起動した際に、変更を上書きしてしまいます。手動で変更が必要な場合、将来の**SuSEconfig**による変更を、`CHECK_INITTAB(/etc/sysconfig/suseconfig内にある)`をnoに設定して無効にします。

ランレベルが5に設定されると、デスクトップや**X Windows**ソフトウェアが壊れてしまう問題が起こる可能性があります。`/var/log/Xorg.*.log`のログファイルから、**X**サーバが開始する際にログされる詳細メッセージを調べます。開始中にデスクトップが失敗する場合、エラーメッセージが`/var/log/messages`に書き込まれる可能性があります。これらのエラーメッセージが**X**サーバの設定の問題を示唆している場合は、これを直すようにしてください。それでもグラフィカルシステムが起動しない場合は、グラフィカルデスクトップを再インストールすることを考えてください。

簡単なテスト:`startx`コマンドは、ユーザが現在コンソールにログインしている場合、**X Window System**を設定されたデフォルトで開始するように強制します。これがうまくいかない場合は、コンソールにエラーがログされるはずです。**X Window System**に関する詳細は、**第26章 *X Window* システム** (529 ページ)を参照してください。

51.4 Loginの問題

ログインの問題とは、お使いのコンピュータが予期されるようこそ画面またはログインプロンプトまで実際起動するが、ユーザ名およびパスワードを受け付けない、または受け付けるが、その後適切な動きをしない場合です(グラフィックデスクトップの開始の失敗、エラーの発生、コマンドラインに落ちる、など)。

51.4.1 有効なユーザ名とパスワードを使っても失敗する

この問題は、一般的にシステムがネットワーク認証またはディレクトリサービスを使用するように設定されており、何らかの理由で、設定されたサーバから結果を取得できない場合に発生します。このような場合でも、rootユーザは唯一のローカルユーザとしてこれらのコンピュータにログインできます。以下では、コンピュータが一見機能しているように見えるのにログインを正しく処理できない一般的な理由をいくつか挙げます。

- ネットワークが機能していません。この場合の更なる対処方法については、[51.5項「ネットワークの問題」](#) (1016 ページ)を参照してください
- DNSが機能していません。(これによりGNOMEまたはKDEは動かず、システムは安全なサーバに有効なリクエストを送れません)。すべてのアクションに対して、コンピュータに極端に長い時間かかる場合は、この問題の可能性があります。このトピックの詳細は、[51.5項「ネットワークの問題」](#) (1016 ページ)を参照してください。
- システムがKerberosを使用するように設定されている場合、システムのローカルタイムは、Kerberosサーバのタイムとの間で許容される相違を超えてしまっている可能性があります(通常300秒)。NTP(network time protocol)が適切に動いていない、またはローカルのNTPサーバが動いていない場合、Kerberosの認証は機能しなくなります。その理由は、この認証はネットワーク間の一般的なクロック同期に依存しているからです。
- システムの認証設定が間違っていて設定されています。関連するPAM設定ファイルの中に誤字や命令の順序違いがないか確認します。PAMおよび関連する設定ファイルの構文に関する背景情報の詳細については、[第27章PAMを使用した認証](#) (545 ページ)を参照してください。

外部のネットワーク問題を含まない他のすべての問題については、解決方法としてシステムをシングルユーザモードに再起動して、動作モードに再び起動してログインし直す前に、設定を修復します。シングルユーザモードで起動するには

- 1 システムを再起動します。ブート画面の表示に続き、プロンプトが表示されます。
- 2 ブートプロンプトでは、1を入力し、システムブートがシングルユーザモードになるようにします。
- 3 `root`用のユーザ名とパスワードを入力します。
- 4 すべての必要な変更をします。
- 5 コマンドラインに`telinit 5`を入力して、ネットワークありフルマルチユーザモードに起動します。

51.4.2 有効なユーザ名とパスワードが受け付けられない

これは、今のところユーザが経験する問題のうち、最も一般的なものです。その理由は、この問題が起こる原因がたくさんあるからです。ローカルのユーザ管理および認証を使用するか、ネットワーク認証を使用するかによって、異なる原因によりログイン失敗が発生します。

ローカルユーザ管理は、次の原因により失敗する可能性があります。

- 間違ったパスワードを入力した可能性があります。
- ユーザのホームディレクトリが、破損または書き込み保護されたデスクトップ設定ファイルを含んでいます。
- この特定のユーザを認証するのに、`X Window System`に何らかの問題があります。特に、ユーザのホームディレクトリが、現在のLinuxをインストールする以前の他のLinuxディストリビューションによって使用されている場合です。

ローカルログイン失敗の原因を発見するには、次の手順に従います。

- 1 認証方式全体をデバッグする前に、ユーザがパスワードを正しく覚えているか確認します。ユーザが正しいパスワードを覚えていない場合は、YaSTユーザ管理モジュールを使用してそのユーザのパスワードを変更します。
- 2 rootユーザでログインし、ログインプロセスおよびPAMのエラーメッセージがないかどうか/var/log/messagesを確認します。
- 3 コンソールからログインしてみます(Ctrl + Alt + F1キーを使用)。これが成功する場合、PAMには問題はありません。その理由は、そのユーザがそのコンピュータ上で認証可能だからです。X Window Systemまたはデスクトップ(GNOMEまたはKDE)で問題がないか探してみてください。詳細については、「51.4.3項「ログインは成功したがGNOMEデスクトップが失敗する」(1013 ページ)」および「51.4.4項「ログインは成功したがKDEデスクトップが失敗する」(1014 ページ)」を参照してください。
- 4 ユーザのホームディレクトリが他のLinuxディストリビューションによって使用されている場合、ユーザのホームにあるXauthorityファイルを削除します。Ctrl + Alt + F1キーを押してコンソールログインを使用し、rm .Xauthorityをこのユーザとして実行します。これにより、X認証の問題はこのユーザに関してはなくなるはずです。グラフィカルログインを再試行します。
- 5 グラフィカルログインがまだ失敗する場合、Ctrl + Alt + F1キーでコンソールログインを行ってください。他のディスプレイ上でXセッションを開始します。最初のもの(:0)はすでに使用中です。

```
startx -- :1
```

これによってグラフィカル画面とデスクトップが表示されます。表示されない場合は、X Window Systemのログファイル(/var/log/Xorg .displaynumber.log)を確認するか、デスクトップアプリケーションのログ(.xsession-errors)を確認して、異常な点がないか調べます。
- 6 設定ファイルが壊れていて、デスクトップが開始できなかった場合、51.4.3項「ログインは成功したがGNOMEデスクトップが失敗する」(1013 ページ)または51.4.4項「ログインは成功したがKDEデスクトップが失敗する」(1014 ページ)を続行します。

以下では、特定のユーザのネットワーク認証が、特定のコンピュータ上で失敗するののかの一般的な理由のいくつかを挙げます。

- 間違ったパスワードを入力した可能性があります。
- コンピュータのローカル認証ファイルの中に存在し、ネットワーク認証システムからも提供されるユーザ名が競合しています。
- ホームディレクトリは存在しますが、それが壊れている、または利用不可能です。書き込み保護がされているか、その時点でアクセスできないサーバ上にディレクトリが存在するかのどちらかの可能性があります。
- 認証システム内で、ユーザがその特定のサーバにログインする権限がありません。
- コンピュータのホスト名が何らかの理由で変更されていて、そのホストにユーザがログインする権限がありません。
- コンピュータが、認証サーバまたはそのユーザの情報を含んでいるディレクトリサーバに接続できません。
- この特定のユーザを認証するのに、**X Window System**に何らかの問題があります。特に、ユーザのホームが、現在の**Linux**をインストールする以前の他の**Linux**ディストリビューションによって使用されてる場合です。

ネットワーク認証におけるログイン失敗の原因を突き止めるには、次の手順に従います。

- 1 認証方式全体をデバッグする前に、ユーザがパスワードを正しく覚えているか確認します。
- 2 認証用にマシンが利用するディレクトリサーバを判別し、それがきちんと動作しており、他のマシンと適切に通信していることを確認します。
- 3 ユーザのユーザ名およびパスワードが他のマシン上でも使用できるかを判別し、そのユーザの認証データが存在し、適切に配布されていることを確認します。
- 4 他のユーザが、問題のある動きをしているコンピュータにログインできるか観察します。その他のユーザが問題なくログインできたか、rootでログインできた場合、ログイン後、`/var/log/messages`ファイルの内容を調べます。ログインの試行に対応するタイムスタンプを見つけ出し、**PAM**によって、エラーメッセージが生成されていないか判別します。

- 5 コンソールからログインを試みます(Ctrl + Alt + F1キーを使用)。これが成功する場合、PAMやユーザのホームがあるディレクトリサーバには問題はありません。その理由は、そのユーザをそのコンピュータ上で認証可能だからです。X Window Systemまたはデスクトップ(GNOMEまたはKDE)で問題がないか探してみてください。詳細については、[51.4.3項「ログインは成功したがGNOMEデスクトップが失敗する」](#) (1013ページ)および[51.4.4項「ログインは成功したがKDEデスクトップが失敗する」](#) (1014ページ)を参照してください。
- 6 ユーザのホームディレクトリが他のLinuxディストリビューションによって使用されている場合、ユーザのホームにあるXauthorityファイルを削除します。Ctrl + Alt + F1キーを押してコンソールログインを使用し、rm .Xauthorityをこのユーザとして実行します。これにより、X認証の問題はこのユーザに関してはなくなるはずです。グラフィカルログインを再試行します。
- 7 グラフィカルログインがまだ失敗する場合、Ctrl + Alt + F1キーでコンソールログインを行ってください。他のディスプレイ上でXセッションを開始します。最初のもの(:0)はすでに使用中です。

```
startx -- :1
```

これによってグラフィカル画面とデスクトップが表示されます。表示されない場合は、X Window Systemのログファイル(/var/log/Xorg.
.displaynumber.log)を確認するか、デスクトップアプリケーションのログ(.xsession-errors)を確認して、異常な点がないか調べます。

- 8 設定ファイルが壊れていて、デスクトップが開始できなかった場合、[51.4.3項「ログインは成功したがGNOMEデスクトップが失敗する」](#) (1013ページ)または[51.4.4項「ログインは成功したがKDEデスクトップが失敗する」](#) (1014ページ)を続行します。

51.4.3 ログインは成功したがGNOMEデスクトップが失敗する

特定のユーザにこのことが当てはまる場合、そのユーザのGNOME設定ファイルが壊れている可能性があります。兆候としては、キーボードがうまく動かない、画面のジオメトリが歪んでいる、または画面が空の灰色領域として表示されるなどがあります。この問題の重要な特徴は、他のユーザがログイン

する場合は、コンピュータは普通に機能するという点です。このような場合、問題のユーザのGNOME設定ディレクトリを単に新しい場所に移すことで、新しいデスクトップを初期化するので、比較的簡単にこの問題を解決できます。ユーザはGNOMEの再設定を強いられますが、データが失われません。

- 1 Ctrl + Alt + F1キーを押して、テキストコンソールを切り替えます。
- 2 ユーザ名でログインします。
- 3 ユーザのGNOME設定ディレクトリを、一時的な場所に移動します。

```
mv .gconf .gconf-ORIG-RECOVER
mv .gnome2 .gnome2-ORIG-RECOVER
```

- 4 ログアウトします。
- 5 もう一度ログインします。ただし、アプリケーションは何も実行しないでください。
- 6 次のようにして、`~/.gconf-ORIG-RECOVER/apps/`ディレクトリを、新しい`~/.gconf`ディレクトリにコピーすることで個々のアプリケーション設定データ(Evolutionの電子メールクライアントデータを含む)を回復します。

```
cp -a .gconf-ORIG-RECOVER/apps .gconf/
```

これによってログインの問題が生じる場合は、重要なアプリケーションデータのみの回復を試み、アプリケーションの残りを再設定します。

51.4.4 ログインは成功したがKDEデスクトップが失敗する

KDEデスクトップがユーザのログインを許可しない理由にはいくつかあります。壊れたKDEデスクトップ設定ファイルと同様に壊れたキャッシュデータもログインの問題を引き起こします。

キャッシュデータは、デスクトップの起動時にパフォーマンスを向上させるため使用されます。このデータが壊れていると、起動が遅くなったり、完全に失敗したりします。キャッシュデータを削除すると、デスクトップ起動の

ルーチンが最初から開始します。これには一般の起動よりも時間がかかりますが、その後はデータは無事でユーザはログインできます。

KDEデスクトップのキャッシュファイルを削除するには、rootユーザで以下のコマンドを実行します。

```
rm -rf /tmp/kde-user /tmp/socket-user
```

userは、実際の値で置き換えられます。これらのディレクトリを削除しても、単に壊れたキャッシュファイルが削除されるだけです。この手順で実際のデータが削除されることはありません。

壊れたデスクトップ設定ファイルは、いつでも初期の設定ファイルに置き換えることができます。ユーザの調整を回復する場合は、デフォルトの設定値を使用して設定が復元されたあとに、一時的な場所からこれらのユーザの調整内容を慎重にコピーします。

壊れたデスクトップ設定ファイルを初期の設定ファイルに置き換えるには、以下の手順に従います。

- 1 Ctrl + Alt + F1キーを押して、テキストコンソールを切り替えます。
- 2 ユーザ名でログインします。
- 3 KDE設定ディレクトリおよび.skelファイルを一時的な場所に移動します。

```
mv .kde .kde-ORIG-RECOVER  
mv .skel .skel-ORIG-RECOVER
```

- 4 ログアウトします。
- 5 もう一度ログインします。
- 6 デスクトップが正常に開始したら、ユーザ自身の設定を元の場所にコピーします。

```
cp -a .kde-ORIG-RECOVER/share .kde/share
```

重要項目

ユーザ自身による調整によりログインが失敗し、その状態が続く場合は、`.kde/share`ディレクトリはコピーせずに上記の手順を繰り返します。

51.5 ネットワークの問題

システム上の問題は、最初はそうは見えないのですが、ネットワークに関する問題であることが多いです。例えば、システムにユーザがログインできない理由は、ある種のネットワークの問題であったりします。ここでは、ネットワークの問題に直面した場合の簡単なチェックリストを紹介します。

コンピュータとネットワークの接続の確認をする場合、以下の手順に従ってください。

- 1 イーサネット接続を使用する場合、はじめにハードウェアを確認します。ネットワークケーブルがきちんとコンピュータに差し込んであることを確認してください。イーサネットコネクタの隣に管理用ライトがある場合、その両方がアクティブである必要があります。

接続に失敗する場合、お使いのネットワークケーブルが他のコンピュータでは使用可能かどうか確認します。使用可能な場合、ネットワークカードに問題の原因があります。ネットワークの設定でハブやスイッチを使用している場合、それらが原因でないかも調べる必要があります。

- 2 無線接続を使用する場合、他のコンピュータからワイヤレスリンクが確立できるかどうか確認します。これ以外の場合は、無線ネットワーク管理者に連絡してください。
- 3 基本的なネットワーク接続を確認し終わったら、どのサービスが応答していないかを探します。お使いの構成上のすべてのネットワークサーバのアドレス情報を集めます。適切なYaSTモジュール内で探すか、システム管理者に問い合わせてください。以下のリストには、ある構成内に含まれる一般的なネットワークサーバを、それらの故障の兆候とともに表わしています。

DNS (ネームサービス)

壊れた、あるいは誤作動しているネームサービスは、ネットワークの機能にさまざまな形で影響を与えます。ローカルコンピュータの認証がネットワークサーバによって行われ、それらのサーバが名前解決に問題があるために見つからない場合、ユーザはローカルコンピュータにログインすることもできません。壊れたネームサーバが管理するネットワーク上のコンピュータは、お互いを「認識」し、通信することができません。

NTP (タイムサービス)

誤作動している、または完全に壊れたNTPサービスは、Kerberosの認証およびXサーバの機能に影響を与えます。

NFS (ファイルサービス)

NFSによってマウントされたディレクトリ内のデータを必要とするアプリケーションがあった場合、このNFSサービスがダウンしてるか、間違っていて設定されていると、そのアプリケーションは起動できないか、または正しく機能しません。最悪のケースとしては、`.gconf`または`.kde`サブディレクトリを含んでいる、あるユーザのホームディレクトリが、NFSサーバの故障のために検出されなかった場合、そのユーザ個人のデスクトップ設定が起動しません。

Samba (ファイルサービス)

Sambaサーバ上にあるディレクトリ内のデータを必要とするアプリケーションがあった場合、このSambaサービスがダウンしたら、そのアプリケーションは開始できないか、適切に機能しません。

NIS (ユーザ管理)

お使いのSUSE Linux Enterpriseシステムが、ユーザデータを提供するためにNISサーバを使用していた場合、NISサービスがダウンすると、ユーザはこのコンピュータにログインできなくなります。

LDAP (ユーザ管理)

お使いのSUSE Linux Enterpriseシステムが、ユーザデータを提供するためにLDAPサーバを使用していた場合、LDAPサービスがダウンしたら、ユーザはこのコンピュータにログインできません。

Kerberos (認証)

認証ができずに、すべてのコンピュータへのログインが失敗します。

CUPS (ネットワーク印刷)
ユーザは印刷できません。

- 4 ネットワークサーバが起動しているか、ネットワーク上で接続を確立できる設定になっているか、を確認します。

重要項目

次で説明するデバッグの手順は、内部ルーティングを必要としない、簡単なネットワークサーバ/クライアント設定にのみ適用されます。サーバとクライアントの両方が、追加でルーティングする必要のない同じサブネットのメンバーであることが前提です。

- 4a `ping hostname` (`hostname`はサーバのホスト名で置き換える)を使って、サーバが起動中で、ネットワークに反応するかどうか確認します。このコマンドが成功する場合は、目的のホストは起動しており、ネットワークのネームサービスは正しく設定されていることが分かります。

`ping`が「`destination host unreachable`」というメッセージで失敗する場合、お使いのシステムまたは宛先のサーバが正しく設定されていないか、ダウンしています。その場合、他のコンピュータから`ping your_hostname`を使用して、お使いのシステムに到達可能か確認してください。他のコンピュータからお使いのコンピュータへ到達可能な場合、宛先のサーバが起動していないか、正しく設定されていません。

`ping`が「`unknown host`」というメッセージで失敗する場合、ネームサービスが正しく設定されていないか、使用したホスト名が正しくありません。`ping -n ipaddress`を使用して、ネームサービスなしでこのホストに接続できるか試してください。これが成功する場合、ホスト名の綴り、およびお使いのネットワーク上のネームサービスが誤って設定されていないか確認します。この問題を詳細に調べるには、[ステップ 4b](#) (1019 ページ)を参照してください。それでも`ping`が失敗する場合は、ネットワークカードが正しく設定されていないか、ネットワークのハードウェアに障害があります。これに関する情報については、[ステップ 4c](#) (1020 ページ)を参照してください。

- 4b** `host hostname`を使用して、接続しようとしているサーバのホスト名が適切なIPアドレスに変換され、またその逆も問題ないか確認します。このコマンドによって、このホストのIPアドレスが返される場合、ネームサービスは起動中です。この`host`コマンドが失敗する場合、お使いのホスト上の名前とアドレス解決に関係するすべてのネットワーク設定ファイルを確認します。

`/etc/resolv.conf`

このファイルは、ネームサーバおよび現在使用中のドメインを管理するために使用されます。このファイルは手動で変更するか、YaSTまたはDHCPによる自動調整が可能です。自動調整のほうをお勧めします。ただし、このファイルが以下のような構造およびネットワークアドレスを含んでいること、さらにドメイン名が正しいことを確認してください。

```
search fully_qualified_domain_name
nameserver ipaddress_of_nameserver
```

このファイルには1つ以上のネームサーバのアドレスを含むことができますが、その中の少なくとも1つは、お使いのホストの名前解決が正しくできる必要があります。必要であれば、YaST DNSおよびHostnameモジュールを使用してこのファイルを調整します。

お使いのネットワークの接続がDHCP経由の場合、YaST DNSおよびHostnameモジュール内で、*[DHCP経由でのホスト名の変更]* および *[DHCP経由でのネームサービスおよび検索リストの更新]* を選択し、DHCPを有効化してホスト名およびネームサービス情報を変更します。

`/etc/nsswitch.conf`

このファイルは、Linuxがネームサービス情報を探す場所を示します。このようになります。

```
...
hosts: files dns
networks: files dns
...
```

dnsエントリは必須です。これにより、Linuxは外部のネームサーバを使用するようになります。通常は、これらのエントリはYaST

によって自動的に作成されますが、内容を確認するのは構いません。

ホスト上で、すべての関連エントリが正しい場合は、システム管理者に依頼して、正しいゾーン情報に関するDNSサーバの設定を確認してもらいます。DNSの詳細については、**第33章 ドメインネームシステム**(673 ページ)を参照してください。お使いのホストのDNS設定およびDNSサーバが正しいことが確認できた場合、ネットワークおよびネットワークデバイス設定の確認に進みます。

- 4c** お使いのシステムがネットワークサーバに接続できない状況で、ネームサービスの問題を障害原因の可能性リストから除外した場合は、ネットワークカードの設定を確認します。

`ifconfig network_device` (rootユーザで実行)コマンドを使用して、このデバイスが適切に設定されているか確認します。inetアドレスおよびマスクの両方が正しく設定されていることを確認してください。IPアドレス内に間違いがある場合、またはネットワークマスク内で不明のビットがある場合は、ネットワーク設定が使用不可能になります。必要であれば、サーバ上でもこの確認をしてください。

- 4d** ネームサービスおよびネットワークサービスが正しく設定され起動している場合でも、外部のネットワーク接続がタイムアウトするのに時間がかかったり、完全に失敗する場合は、`traceroute fully_qualified_domain_name` (rootユーザで実行)コマンドを使用して、リクエストがネットワーク上でどのルートを使用するか追跡します。このコマンドは、お使いのコンピュータのリクエストが宛先に到達するまでに経由するゲートウェイ(ホップ)をリストします。各ホップの応答時間およびこのホップにそもそも到達可能か否かをリストします。`traceroute`および`ping`コマンドを組み合わせ、原因を追究し、管理者に知らせてください。

ネットワーク障害の原因を突き止めたら、自身でそれを解決するか(自分のコンピュータ上に問題がある場合)、お使いのネットワークのシステム管理者に原因について報告し、サービスを再設定するか、必要なシステムを修理してもらってください。

51.5.1 NetworkManagerの問題

ネットワーク接続に問題がある場合は、(1016 ページ)の説明に従って原因を絞り込んでください。NetworkManagerが原因と考えられる場合は、以降の説明に従ってNetworkManager障害の理由を調べるために役立つログを取得してください。

- 1 シェルを開いて、rootとしてログインします。
- 2 NetworkManagerを再起動します。

```
rcnetwork restart -o nm
```
- 3 一般ユーザとして<http://www.opensuse.org>などのWebページを開いて、正常に接続できているかどうかを確認します。
- 4 /var/log/NetworkManagerにある、NetworkManagerに関する情報を収集します。

NetworkManagerについての詳細は、30.6項「NetworkManagerを使用したネットワーク接続の管理」(638 ページ)を参照してください。

51.6 データの問題

データの問題とは、コンピュータが正常に起動するかしないかに関係なく、システム上でデータが壊れており、システムの修復が必要な場合を言います。このような状況では、システムに障害が発生する前の状態にシステムを復元するために、重要なデータをバックアップする必要があります。SUSE Linux Enterpriseには、システムのバックアップ/復元や、壊れたシステムの救済を行うための、専用のYaSTモジュールが用意されています。

51.6.1 重要なデータのバックアップ

YaSTシステムバックアップモジュールを使用すれば、システムのバックアップは簡単に管理できます。

- 1 rootユーザでYaSTを開始し、`[システム] > [システムバックアップ]` を順に選択します。
- 2 バックアップに必要な詳細のすべて、アーカイブファイルのファイル名、スコープ、およびバックアップタイプを含むバックアッププロファイルを作成します。
 - 2a `[プロファイル管理] > [追加]` の順にクリックします。
 - 2b アーカイブの名前を入力します。
 - 2c ローカルバックアップをしたい場合は、そのバックアップの場所へのパスを入力します。ネットワークサーバ上にバックアップをアーカイブしたい場合は、IPアドレスまたはサーバの名前、およびアーカイブを保存するディレクトリを入力します。
 - 2d アーカイブタイプを決め `[次へ]` をクリックします。
 - 2e どのパッケージにも属さないファイルをバックアップするか、アーカイブ作成の前にファイルのリストを表示させるかなど、使用するバックアップオプションを決定します。また、変更されたファイルが、時間のかかるMD5メカニズムを使用して識別されるようにするのも決定します。

`[エキスパート]` を使用して、ハードディスク領域全体のバックアップのためのダイアログに入ります。現在、このオプションはExt2ファイルシステムのみに適用されます。
 - 2f 最後に、ロックファイルまたはキャッシュファイルなど、バックアップの必要のない一部のシステム領域を、バックアップ領域から除外するための検索条件を設定します。項目を追加、編集、または削除して、必要にあった条件を設定し、`[OK]` を押して終了します。
- 3 プロファイル設定を終了したら、`[Create Backup (バックアップの作成)]` を使用した即時バックアップの開始、または自動バックアップの設定ができます。他のさまざまな目的のために設定されたプロファイルも作成できます。

特定のプロファイル用に自動バックアップを設定するには、以下の手順に従います。

- 1 [プロファイル管理] メニューから、[自動バックアップ] を選択します。
- 2 [バックアップの自動開始] を選択します。
- 3 バックアップの頻度を決定します。[毎日]、[毎週]、または[毎月] を選択します。
- 4 バックアップの開始時間を決定します。これらの設定は選択されたバックアップの頻度に依存します。
- 5 古いバックアップを保存するか、保存する場合は何世代にするかを決定します。バックアッププロセスの自動的に生成されたステータスメッセージを受け取るには、[rootユーザにサマリメールを送信する] にチェックを入れます。
- 6 設定内容を適用し、指定した時刻にバックアップを開始するには、[OK] をクリックします。

51.6.2 システムバックアップの復元

YaSTシステムリストアモジュールを使用して、バックアップからシステム設定を復元します。バックアップの全体を復元するか、壊れたために古い状態にリセットする必要のある、特定のコンポーネントのみを選択します。

- 1 [YaST] > [システム] > [システムの復元] の順にクリックします。
- 2 バックアップファイルの場所を入力します。ローカルファイル、ネットワーク上でマウントされたファイル、またはフロッピーディスクおよびCDなどの取り外し可能なデバイス上のファイルなどがあります。次に、[次へ] をクリックします。

次のダイアログでは、ファイル名、作成日、バックアップのタイプ、およびオプションのコメントなどのアーカイブプロパティのサマリが表示されます。
- 3 [アーカイブの内容] をクリックして、アーカイブされた内容を参照します。[OK] をクリックすると、[アーカイブプロパティ] ダイアログに戻ります。
- 4 [エキスパート用オプション] では、復元プロセスを微調整するダイアログが開きます。[OK] をクリックすると、[アーカイブプロパティ] ダイアログに戻ります。
- 5 [次へ] をクリックすると、復元するパッケージのビューが開きます。[承認] を押して、アーカイブ内のすべてのファイルを復元するか、[Select All] 、[Deselect All] 、および [Select Files] ボタンを使って、選択内容の微調整をします。RPMデータベースが壊れているか削除され、バックアップにこのファイルが含まれている場合にのみ、[RPMデータベースの復元] オプションを使用します。
- 6 [承認] をクリックすると、バックアップが復元されます。[完了] をクリックして、復元プロセスが完了したあと、モジュールを終了します。

51.6.3 壊れたシステムの復旧

システムが起動し正常に移動するのに失敗する理由はいくつか考えられます。最も一般的な理由は、システムクラッシュが起こったあとにファイルシステムが壊れている、設定ファイルが壊れている、ブートローダ設定が壊れている、などです。

SUSE Linux Enterpriseでは、この種の状況に対応するために、2つの異なる方法が提供されます。それらは、YaSTシステム修復機能の使用、またはレス

キューシステムの起動です。次のセクションでは、システム修復のための両方の方法について説明します。

YaSTシステム修復の使用

YaSTシステム修復モジュールを起動する前に、お客さまのニーズを一番満たすように、モジュールを起動するモードを決めます。システム障害の度合い、および原因とお客さまの経験に合わせて、選択可能な異なるモードが3つあります。

自動修復

不明な原因でシステムに障害が起こった場合で、そもそもシステムのどの部分が失敗の原因となっているか分からない場合は、**[自動修復]**を使用します。広範囲に及ぶ自動化されたチェックがお使いのシステム上のすべてのコンポーネントで実行されます。この手順の詳細な説明については、**自動修復項 (1025 ページ)**を参照してください。

カスタム修復

システムに障害が発生し、その原因がどのコンポーネントにあるか分かっている場合、**[カスタム修復]**を使用して、コンポーネントに対して行うシステム分析の範囲を限定することにより、冗長なシステムチェックを短縮できます。例えば、障害の前のシステムメッセージに、パッケージデータベースのエラーの可能性を示唆する記述があれば、分析と修復手順を、システムのこの側面の検査および復元に限定できます。この手順の詳細な説明については、**カスタム修復項 (1028 ページ)**を参照してください。

エキスパート設定用ツール

障害が発生したコンポーネントおよびその修復方法がはっきりしている場合は、分析を実行せずに、直接、障害のあるコンポーネントを修復するのに必要なツールを適用できます。詳細については、**エキスパート設定用ツール項 (1029 ページ)**を参照してください。

前で説明した修復モードから1つを選択し、以下で概説するようにシステム修復を続行します。

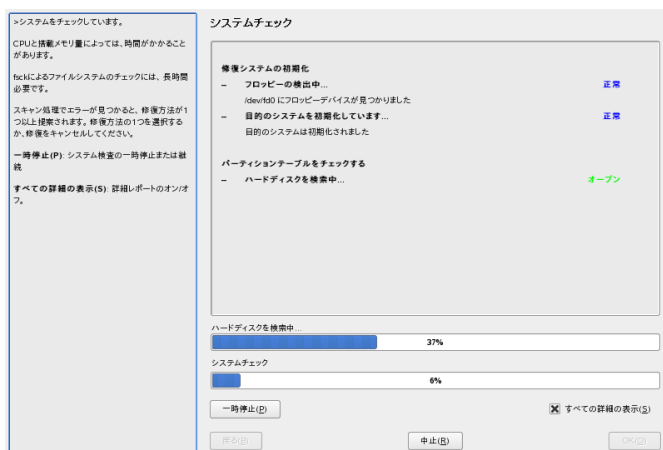
自動修復

YaSTシステム修復の自動修復モードを起動するには、次の手順に従います。

- 1 CD/DVDドライブにSUSE Linux Enterpriseの最初のインストールメディアを挿入します。
- 2 システムを再起動します。
- 3 ブート画面で、[インストール] を選択します。
- 4 言語を選択して、[次へ] をクリックします。
- 5 使用許諾契約に同意したら、[次へ] をクリックします。
- 6 [システム分析] で、[その他] > [インストールしたシステムの修復] の順に選択します。
- 7 [自動修復] を選択します。

YaSTは、ここでインストールされたシステムの広範囲に及ぶ分析を起動します。このプロシージャの進捗状況は、画面下部にある2つの進捗バーで表示されます。上のバーは現在実行中のテストの進捗状況を示します。下のバーは解析の全体の進捗状況を示します。上部のログウィンドウで、現在実行中のテストおよび結果を追跡することができます。参照先 [図 51.2. 「自動修復モード」 \(1026 ページ\)](#). 以下のメインテストは、自動修復を実行すると毎回実行されます。言い換えれば、自動修復には、多数の個別サブテストが含まれています。

図 51.2 自動修復モード



全ハードディスクのパーティションテーブル

検出された全ハードディスクのパーティションテーブルの妥当性と一貫性が検査されます。

スワップパーティション

インストール済みのシステムのスワップ(**swap**)パーティションが検出され、テストされ、適用可能な場合は、スワップエリアを有効にする機会が提供されます。スワップエリアを有効にすると、Vシステムの修復の処理速度が向上します。

ファイルシステム

検出されたすべてのファイルシステムがファイルシステム固有の検査の対象となります。

/etc/fstabファイルのエントリ

このファイルのエントリの完全性と一貫性が検査されます。有効なパーティションは、すべてマウントされます。

ブートローダの設定

インストールされているシステムのブートローダ設定(**GRUB**か**LILO**)の完全性と一貫性が検査されます。ブートデバイスと**root**デバイスが調べられ、**initrd**モジュールの可用性が検査されます。

パッケージデータベース

最小構成のインストールの運用に必要なすべてのパッケージが存在しているか、検査されます。オプションで基本パッケージの解析も可能なので、基本パッケージの数が多いことが原因で、この検査には長時間かかります。

- 8 エラーを検出するたびに、プロシージャが一時停止し、エラーの詳細および可能な解決策を提示するダイアログが表示されます。

提案された修復を承認する前に、画面のメッセージを注意深く読みます。提案された修復を断る場合、システムは修復なしの状態のままになります。

- 9 修復プロセスが正常に終了した後に、**[OK]** および **[完了]** をクリックし、インストールメディアを取り出します。システムは自動的に再起動します。

カスタム修復

[カスタム修復] モードを起動し、システムのコンポーネントの一部を選択的に検査するには、次の手順に従います。

- 1 CD/DVDドライブにSUSE Linux Enterpriseの最初のインストールメディアを挿入します。
- 2 システムを再起動します。
- 3 ブート画面で、[インストール] を選択します。
- 4 言語を選択して、[次へ] をクリックします。
- 5 使用許諾契約に同意したら、[次へ] をクリックします。
- 6 [システム分析] で、[その他] > [インストールしたシステムの修復] の順に選択します。
- 7 [カスタム修復] を選択します。

[カスタム修復] では、実行可能なテストのリストが、最初は、すべて実行対象として選択された状態で表示されます。全部のテスト範囲は、自動修復と合致します。損傷が存在していない個所が、既に判明している場合、対応するテストのチェックマークを消します。[続行] をクリックすると、より狭い範囲のテストプロシージャが開始され、実行時間が大幅に短縮されます。

すべてのテストグループを個別に実行できるわけではありません。fstab エントリの解析は常に、既存のスワップパーティションも含めたファイルシステムの検証と結び付いています。YaSTでは、このような依存性の条件が自動的に満たされ、必要なテストが最少数で実行されます。

- 8 エラーを検出するたびに、プロシージャが一時停止し、エラーの詳細および可能な解決策を提示するダイアログが表示されます。

提案された修復を承認する前に、画面のメッセージを注意深く読みます。提案された修復を断る場合、システムは修復なしの状態のままになります。

- 9 修復プロセスが正常に終了した後に、**[OK]** および **[完了]** をクリックし、インストールメディアを取り出します。システムは自動的に再起動します。

エキスパート設定用ツール

SUSE Linux Enterpriseに関する知識が豊富で、システムの修復に必要な対応策がすでに明確な場合、システム分析をスキップして、直接、ツールを適用します。

YaSTシステム修復の**「エキスパート設定用ツール」**の機能を使用するには、以下の手順に従います。

- 1 最初のインストール時に使用した、元のインストールメディアを使用してシステムを起動します(**第3章 YaSTによるインストール** (21 ページ)に概説されています)。
- 2 **「システム分析」** で、**「その他」** > **「インストールしたシステムの修復」** の順に選択します。
- 3 **「エキスパート設定用ツール」** を選択して、適切な修復オプションを選択します。
- 4 修復プロセスが正常に終了した後に、**[OK]** および **[完了]** をクリックし、インストールメディアを取り出します。システムは自動的に再起動します。

エキスパート設定用ツールには、障害が発生したシステムを修復するために、以下のようなオプションが用意されています。

新しいブートローダをインストールする

YaSTのブートローダの設定モジュールを起動します。詳細については、**21.3項「YaSTによるブートローダの設定」** (457 ページ)を参照してください。

パーティションツールの起動

YaSTのパーティションのエキスパート設定ツールが起動します。

ファイルシステムの修復

インストール済みのシステムのファイルシステムを検査します。はじめに、検出された全パーティションの中から1つを選択するダイアログが表示され、検査対象を選択することができます。

失われたパーティションの復元

損傷したパーティションテーブルの再構築を試みることができます。はじめに、検出されたハードディスクのリストが表示され、対象を選択します。[OK] をクリックすると検証が開始されます。検証には、処理能力とハードディスクのサイズに応じて、時間がかかります。

重要項目: パーティションテーブルの再構築

パーティションテーブルの再構築は、難しい処理です。YaSTでは、ハードディスクのデータセクタを解析することにより、失われたパーティションの認識が試みられます。認識が成功すると、失われたパーティションが再構築したパーティションテーブルに追加されます。ただし、これは予想可能なすべての事例で成功するわけではありません。

システム設定のフロッピーへの保存

このオプションは、重要なシステムファイルをフロッピーディスクに保存します。システムファイルの1つが損傷した場合には、作成しておいたフロッピーディスクからリストアできます。

インストールされたソフトウェアの確認

パッケージデータベースの整合性と、最も重要なパッケージの可用性を検査します。このツールを使うと、損傷しているインストールパッケージを再インストールできます。

レスキューシステムの使用

SUSE Linux Enterpriseにはレスキューシステムが付属しています。レスキューシステムは、RAMディスクにロードして、ルートファイルシステムとしてマウントできる小さなLinuxシステムで、これを利用して外部からLinuxパーティションにアクセスすることができます。レスキューシステムを使用して、システムの重要な部分を復元したり、適切な変更を行ったりできます。

- 任意の種類の設定ファイルを操作できます。

- ファイルシステムの欠陥をチェックして、自動修復プロセスを開始することができます。
- インストールされているシステムを、「他のルート」環境内からアクセスすることができます。
- ブートローダーの設定を確認、変更、および再インストールすることができます。
- `parted`コマンドを使って、パーティションサイズを変更できます。このツールの詳細は、GUN PartedのWebサイト(<http://www.gnu.org/software/parted/parted.html>)を参照してください。

レスキューシステムは、さまざまなソースや場所からロードすることができます。一番簡単な方法は、オリジナルのインストールCD/DVDからレスキューシステムをブートすることです。

- 1 CD/DVDドライブにインストールメディアを挿入します。
- 2 システムを再起動します。
- 3 ブート画面で、`[レスキューシステム]` オプションを選択します。
- 4 `Rescue:`プロンプトに「`root`」と入力します。パスワードは必要ありません。

ハードウェア設定にCD/DVDドライブが含まれていない場合は、ネットワークソースからレスキューシステムを起動することができます。リモートブートを使用する場合の例を以下に示します。フロッピーディスクなどの、他のブートメディアを使用する場合は、それに応じて`info`ファイルを変更してから、通常どおりにブートしてください。

- 1 PXEブートセットアップの環境設定を入力します。ただし、`install=protocol://instsource`は、`rescue=protocol://instsource`に変更してください。通常のインストールと同様に、`protocol`はサポートする任意のネットワークプロトコル(NFS、HTTP、FTPなど)を表しています。また、`instsource`は、ネットワークインストールソースへのパスを表します。

- 2 **4.3.7項「Wake on LAN」** (84 ページ)に説明したように、「Wake on LAN」を使用してシステムをブートします。

- 3 **Rescue:** プロンプトに「root」と入力します。パスワードは必要ありません。

レスキューシステムが起動したら、**Alt + F1**～**Alt + F6**キーを使って、仮想コンソールを使用することができます。

シェルおよび他の多くの便利なユーティリティ(マウントプログラムなど)は、`/bin`ディレクトリにあります。`sbin`ディレクトリには、ファイルシステムを検討し、修復するための重要なファイルおよびネットワークユーティリティが入っています。このディレクトリには、最も重要なバイナリも入っています。たとえばシステムメンテナンス用には`fdisk`、`mkfs`、`mkswap`、`mount`、`mount`、`init`、および`shutdown`があり、ネットワークメンテナンス用には`ifconfig`、`ip`、`route`、および`netstat`があります。`/usr/bin`ディレクトリには、`vi editor`、`find`、`less`、および`ssh`があります。

システムメッセージを表示するには、`dmesg`コマンドを使用するか、または`/var/log/messages`ファイルを参照してください。

設定ファイルの確認と修正

レスキューシステムを使った環境設定情報の修正例として、環境設定ファイルが壊れたためシステムが正常にブートできなくなった場合を考えてみましょう。このような場合は、レスキューシステムを使って設定ファイルを修復します。

環境設定ファイルを修正するには、以下の手順に従ってください。

- 1 前述のいずれかの方法を使って、レスキューシステムを起動します。
- 2 `/dev/sda6`下にあるルートファイルシステムをレスキューシステムにマウントするには、以下のコマンドを使用します。

```
mount /dev/sda6 /mnt
```

システム中のすべてのディレクトリが、`/mnt`下に配置されます。

- 3 マウントしたルートファイルシステムのディレクトリに移動します。

```
cd /mnt
```

- 4 問題の発生している設定ファイルを、viエディタで開きます。次に、設定内容を修正して、ファイルを保存します。

- 5 レスキューシステムから、ルートファイルシステムをアンマウントします。

```
umount /mnt
```

- 6 コンピュータを再起動します。

ファイルシステムの修復と確認

一般的に、稼動システムではファイルシステムを修復できません。重大な問題が見つかった場合、ルートファイルシステムをブートできなくなることさえあります。この場合、システムブートはカーネルパニックで終了します。この場合、外部からシステムを修復するしか方法はありません。このような作業には、YaSTシステム修復モジュールを使用することを強くお勧めします(詳細は[YaSTシステム修復の使用項 \(1025 ページ\)](#)を参照)。ただし、手動でファイルシステムを確認、修復する必要がある場合は、レスキューシステムを起動します。レスキューシステムには、ext2、ext3、reiserfs、xfs、dosfs、およびvfatファイルシステムを確認、修復するためのユーティリティが用意されています。

インストール済みシステムへのアクセス

ブートローダの設定を変更したり、ハードウェア設定ユーティリティを実行するなどの目的で、レスキューシステムからインストール済みシステムにアクセスする必要がある場合は、「change root」(ルート変更)環境で作業を行う必要があります。

インストール済みシステムに基づいた「change root(ルート変更)」環境を設定するには、以下の手順に従ってください。

- 1 まず、インストール済みシステムとデバイスファイルシステムから、ルートパーティションをマウントします。

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

- 2 新しい環境に「change root」(ルート変更)します。

```
chroot /mnt
```

3 /procおよび/sysをマウントします。

```
mount /proc  
mount /sys
```

4 最後に、インストール済みシステムから、残りのパーティションをマウントします。

```
mount -a
```

5 これで、インストール済みシステムにアクセスできるようになります。システムを再起動する前に、`umount -a`を使ってパーティションをアンマウントし、`exit`コマンドを実行して「**change root**」(ルート変更)環境を終了してください。

警告: 制限

インストール済みシステムのファイルやアプリケーションにフルアクセスできますが、いくつかの制限事項もあります。たとえば、レスキューシステムからブートされたカーネルには、制限事項があります。このカーネルは、必要最低限のハードウェアしかサポートしておらず、カーネルのバージョンが完全に一致していない限り(完全一致する場合ほとんどなし)、インストール済みシステムからカーネルモジュールを追加することはできません。そのため、たとえばサウンドカードなどにはアクセスできません。また、GUIも利用できません。

また、**Alt + F1**～**Alt + F6**キーを使ってコンソールを切り替えると、「**change root**」(ルート変更)環境は終了することに注意してください。

ブートローダの変更と再インストール

場合によっては、ブートローダが壊れてしまい、システムをブートできなくなることもあります。たとえば、ブートローダが正常に機能しないと、起動ルーチンは物理ドライブとそのLinuxファイルシステム中の場所とを関連付けられず、正常な処理を行うことができません。

ブートロードの設定を確認し、ブートロードを再インストールするには、以下の手順に従ってください。

- 1 の説明に従って、インストール済みシステムにアクセスするための適切な作業を行います。インストール済みシステムへのアクセス項(1033 ページ)
- 2 で説明されているように、GRUBの環境設定規則に基づいて以下のファイルが正しく設定されているかどうかを確認します。第21章 ブートローダ(445 ページ)

- /etc/grub.conf
- /boot/grub/device.map
- /boot/grub/menu.lst

デバイスマッピング(device.map)やルートパーティションの場所、および環境設定ファイルなどを、必要に応じて修正します。

- 3 以下のコマンドシーケンスを使って、ブートローダを再インストールします。

```
grub --batch < /etc/grub.conf
```

- 4 パーティションをアンマウントして、「change root」(ルート変更)環境からログアウトします。次に、システムを再起動します。

```
umount -a  
exit  
reboot
```

51.7 IBM System z:initrdのレスキューシステムとしての使用

IBM System z用のSUSE® Linux Enterprise Serverカーネルをアップグレード、変更した場合、何らかの原因でシステムが不整合な状態で再起動されると、インストールされているシステムのIPL標準処理が失敗する可能性があります。一般的にこの問題は、アップデートされたSUSE Linux Enterprise Serverカーネルをインストールした後で、IPLレコードをアップデートするziplプログラムをまだ実行していない場合に発生します。この場合、レスキューシス

テムとして標準のインストールパッケージを使用して、そこからziplプログラムを実行してIPLレコードをアップデートしてください。

51.7.1 レスキューシステムのIPL処理

重要項目: インストールデータを利用できるようにする

この方法を使用する場合、IBM System z版SUSE Linux Enterprise Serverのインストールデータが利用可能でなければなりません。詳細は、*Architecture-Specific Information*の項「Making the Installation Data Available」(第2章 *Preparing for Installation*, ↑*Architecture-Specific Information*)を参照してください。また、SUSE Linux Enterprise Serverのルートファイルシステムを含むデバイスのチャンネル番号、およびデバイス内のパーティション番号が必要になります。

まず、『*Architecture-Specific Information*』マニュアルの説明に従って、IBM System zインストールシステムのSUSE Linux Enterprise ServerをIPL処理します。IPL処理すると、ネットワークアダプタのリストが表示されます。

レスキューシステムを開始するには [インストール処理またはシステムを開始する] を選択してから [レスキューシステムを開始する] を選択します。次に、インストール環境に応じて、ネットワークアダプタやインストールソースに関するパラメータを指定する必要があります。レスキューシステムがロードされ、ログインプロンプトが表示されます。

```
Skipped services in runlevel 3:  nfs nfsboot
```

```
Rescue login:
```

rootとして、パスワードを指定しないでログインすることができます。

51.7.2 ディスクの設定

この状態では、設定されているディスクはありません。作業を続行する前に、ディスクを設定する必要があります。

手順 51.3 DASDの設定

1 DASDを設定するには、以下のコマンドを使用します。

```
dasd_configure 0.0.0150 1 0
```

ここで、「0.0.0150」は、DASDが接続されているチャンネルを表します。1は、ディスクをアクティブにすることを表しています(ここに0を指定すると、ディスクが無効になる)。0は、ディスクに「DIAGモード」でアクセスしないことを表します(ここに1を指定すると、ディスクへのDAIGアクセスが有効になります)。

- 2 DASDがオンラインになり(`cat /proc/partitions`で確認)、コマンドを使用できるようになります。

手順 51.4 zFCPディスクの設定

- 1 zFCPディスクを設定するには、まずzFCPアダプタを設定する必要があります。そのためには次のコマンドを使用します。

```
zfcf_host_configure 0.0.4000 1
```

0.0.4000はアダプタが接続されているチャンネルを、1(ここに0を指定するとアダプタが無効になる)はアクティブにすることを示します。

- 2 アダプタをアクティブにしたら、ディスクを設定することができます。そのためには次のコマンドを使用します。

```
zfcf_disk_configure 0.0.4000 1234567887654321 8765432100000000 1
```

0.0.4000は前に使われていたチャンネルIDを、1234567887654321はWWPN(World wide Port Number)を、そして8765432100000000はLUN(論理ユニット番号)を表しています。1(ここに0を指定するとディスクが無効になる)は、ディスクをアクティブにすることを表しています。

- 3 zFCPディスクがオンラインになり(`cat /proc/partitions`で確認)、コマンドを使用できるようになります。

51.7.3 ルートデバイスのマウント

必要なディスクがすべてオンラインになったら、ルートデバイスをマウントします。ここでは、DASDの2番目のパーティション(`/dev/dasda2`)にルート

デバイスがあると仮定します。この場合、使用するコマンドはmount /dev/dasda2 /mntになります。

重要項目: ファイルシステムの整合性

インストール済みシステムが正しくシャットダウンされなかった場合は、マウント前にファイルシステムの整合性を確認しておくことをお勧めします。整合性を確認することによって、予期せぬ事態によるデータ消失の危険を回避することができます。この例では、fsck /dev/dasda2コマンドを実行して、ファイルシステムの整合性を確認します。

mountコマンドを実行するだけでも、ファイルシステムが正しくマウントされたかどうかを確認することができます。

例 51.1 mountコマンドの出力

```
SuSE Instsys suse:/ # mount
shmfs on /newroot type shm (rw,nr_inodes=10240)
devpts on /dev/pts type devpts (rw)
virtual-proc-filesystem on /proc type proc (rw)
/dev/dasda2 on /mnt type reiserfs (rw)
```

51.7.4 マウントされているファイルシステムの変更

ziplコマンド実行時に、レスキューシステムからではなく、インストール済みシステムのルートデバイスから設定ファイルを読み込ませるためには、chrootコマンドを使ってルートデバイスをインストール済みシステムに変更します。

例 51.2 chrootを使ったマウントするファイルシステムの変更

```
SuSE Instsys suse:/ # cd /mnt
SuSE Instsys suse:/mnt # chroot /mnt
```

51.7.5 ziplの実行

次に、ziplを実行して、IPLレコードを正しい値に書き換えます。

例 51.3 ziplを使ったIPLレコードのインストール

```
sh-2.05b# zipl
building bootmap : /boot/zipl/bootmap
adding Kernel Image : /boot/kernel/image located at 0x00010000
adding Ramdisk : /boot/initrd located at 0x00800000
adding Parmline : /boot/zipl/parmfile located at 0x00001000
Bootloader for ECKD type devices with z/OS compatible layout installed.
Syncing disks....
...done
```

51.7.6 レスキューシステムの終了

レスキューシステムを終了するには、まずchrootコマンドで開かれたシェルをexitコマンドで終了します。データ消失を防ぐために、syncコマンドを使って、バッファ上にあるまだ書き込まれていないデータをすべてディスクに書き込みます。次に、レスキューシステムのルートディレクトリに移動して、IBM System z版SUSE Linux Enterprise Serverのルートデバイスをアンマウントします。

例 51.4 ファイルシステムのアンマウント

```
SuSE Instsys suse:/mnt # cd /
SuSE Instsys suse:/ # umount /mnt
```

最後に、haltコマンドを実行して、レスキューシステムを終了します。[3.13.1 項「IBM System z: インストール済みシステムのIPL処理」](#) (39 ページ)で説明されているように、SUSE Linux Enterprise ServerシステムのIPL処理が行われます。

目次

シンボル

64ビットLinux, 421

カーネル仕様, 426

ランタイムサポート, 422

64ビットlinux

ソフトウェア開発, 423

アクセス権 (参照 パーミッション)

アップデート

オンライン, 156-159

パスワードとグループ, 236

パッチCD, 160

問題, 236

アドオン製品, 154

アンインストール

GRUB, 461

Linux, 461

インストール

GRUB, 446

YaST, 21-52

ディレクトリ, 162

パッケージ, 348

手動, 258

インターネット

cinternet, 660

DSL, 632

ISDN, 628

KInternet, 660

qinternet, 660

smpppd, 658-661

TDSL, 634

ダイヤルアップ, 658-661

エディタ

Emacs, 473-474

vi, 414

エラーメッセージ

パーミッションの拒否, 178

不正なインタプリタ, 178

エンコード

ISO-8859-1, 477

カード

グラフィック, 535

サウンド, 168

ネットワーク, 616-617

カーネル

キャッシュ, 472

制限, 527

キーボード

XKB, 475

Xキーボード拡張, 475

アジアの文字, 476

マッピング, 475

マルチキー, 475

作成, 475

レイアウト, 475

設定, 167

クエリーのサポート, 993

グラフィック

カード

ドライバ, 535

グループ

管理, 200

コアファイル, 471

コマンド, 402-414

bzip2, 396

cat, 408

cd, 404

chgrp, 401, 404

chmod, 400, 404

chown, 401, 404

clear, 414

cp, 403

date, 411

df, 410

diff, 409

du, 410

file, 408

find, 407
fonts-config, 538
free, 411, 472
getfacl, 340
grep, 408
grub, 446
gzip, 396, 405
halt, 414
ifconfig, 656
ip, 653
kadmin, 926
kill, 412
killall, 412
kinit, 933
ktadd, 936
ldapadd, 738
ldapdelete, 741
ldapmodify, 740
ldapsearch, 740, 940
less, 408
ln, 403
lp, 494
ls, 402
man, 402
mkdir, 404
mount, 409
mv, 403
nslookup, 413
passwd, 413
ping, 412, 654
ps, 411
reboot, 414
rm, 403
rmdir, 404
route, 657
rpm, 347
rpmbuild, 347
scp, 907
setfacl, 341
sftp, 907

slptool, 664
smbpasswd, 772
ssh, 906
ssh-agent, 910
ssh-keygen, 909
su, 413
tar, 395, 406
telnet, 413
top, 411
umount, 409
updatedb, 407
ヘルプ, 387
検索, 407
コンソール
 グラフィカル, 463
 切り替え, 475
 割り当て, 475
サウンド
 YaSTでの設定, 168
 ミキサー, 258
サービスロケーションプロトコル (参照 SLP)
 シェル, 383-418
 Bash, 384
 コマンド, 402-414
 パイプ, 394
 ワイルドカード, 392
システム
 アップデート, 160
 サービス, 189
 シャットダウン, 414
 セキュリティ, 200
 リソースの使用制限, 471
 レスキュー, 1030
 ローカライズ, 476
 再起動, 414
 言語, 182
 設定, 143-207
システムの修復, 1025
ジョイスティック

- 設定, 167
- スクリプト
 - init.d, 432, 435-439, 657
 - boot, 437
 - boot.local, 437
 - boot.setup, 437
 - halt, 438
 - nfsserver, 658
 - portmap, 658
 - postfix, 658
 - rc, 435, 438
 - squid, 856
 - xinetd, 658
 - ypbind, 658
 - ypserv, 658
 - ネットワーク, 657
 - mkinitrd, 429
 - modify_resolvconf, 473
 - SuSEconfig, 441-444
 - 無効化, 444
- セキュリティ, 963-977
 - DNS, 973
 - RPM署名, 976
 - Samba, 769
 - Squid, 852
 - SSH, 905-911
 - tcpd, 976
 - telnet, 905
 - X, 970
 - ウイルス, 969
 - エンジニアリング, 964
 - シリアル端末, 964-965
 - ネットワーク, 969-973
 - バグ, 968, 971
 - パスワード, 965-966
 - パーミッション, 967-968
 - ヒントとテクニック, 974
 - ファイアウォール, 203, 893
 - ブート, 964-967
 - ローカル, 965-969

- ワーム, 973
- 侵入検出, 259
- 問題のレポート, 977
- 攻撃, 972-973
- 設定, 192-203
- ソフトウェア
 - インストール, 146-154
 - コンパイル, 356
 - 削除, 146-154
- ソフトウェアRAID (参照 RAID)
- ソース
 - コンパイル, 356
- タイムゾーン, 182
- ディスク
 - ブート, 462
- ディレクトリ
 - パス, 389
 - 作成, 404
 - 削除, 404
 - 変更, 404
 - 構造, 387
- ドキュメント (参照 ヘルプ)
- ドメインネームシステム (参照 DNS)
- ドライブ
 - マウント, 409
 - マウント解除, 409
- ネットワーク, 597
 - DHCP, 187, 699
 - DNS, 614
 - SLP, 663
 - TCP/IP, 597
 - YaST, 617
 - IPアドレス, 618
 - エイリアス, 619
 - ゲートウェイ, 621
 - ホスト名, 620
 - 起動, 622
- ネットマスク, 601
- ブロードキャストアドレス, 603
- ルーティング, 191, 601

- ローカルホスト, 603
- 仮想LAN, 636
- 基本ネットワークアドレス, 603
- 環境設定ファイル, 644-652
- 設定, 183-192, 616-634, 640-658
 - IPv6, 613
- 認証
 - Kerberos, 913-920
- ネットワークファイルシステム (参照 NFS)
- ネームサーバ (参照 DNS)
- ハードウェア
 - DASD, 165
 - ISDN, 628
 - ZFCP, 166
 - グラフィックカード, 214
 - ハードディスクコントローラ, 164
 - モニタ, 214
 - 情報, 164, 996
- ハードディスク
 - DMA, 165
- バックアップ, 161
 - YaSTを使用して作成, 170
 - 復元, 171
- バッシュ
 - コマンド, 384
 - パイプ, 394
 - ワイルドカード, 392
 - 機能, 392
- パケットフィルタ (参照 ファイアウォール)
- パス, 389
 - 相対, 389
 - 絶対, 389
- パスワード
 - 変更, 413
- パッケージ
 - buildによるコンパイル, 358
 - LSB, 347
 - RPMs, 347
 - アンインストール, 348
 - インストール, 348
 - コンパイル, 356
 - パッケージマネージャ, 347
 - 検証, 348
- パッケージ管理
 - zmd, 223
- パーティション
 - EVMS, 176
 - fstab, 178
 - LVM, 176
 - RAID, 176
 - タイプ, 174
 - パラメータ, 176
 - パーティションテーブル, 445
 - 作成, 36, 172, 175
 - 再フォーマット, 176
 - 暗号化, 945
- パーミッション, 397
 - ACL, 333-346
 - ディレクトリ, 399
 - ファイル, 398
 - ファイルシステム, 398
 - ファイルパーミッション, 471
 - 変更, 400, 404
 - 表示, 400
- ファイアウォール, 203, 893
 - Squid and, 865
 - SuSEfirewall2, 893, 899
 - パケットフィルタ, 893, 898
- ファイル
 - アーカイブ, 395, 406
 - コピー, 403
 - パス, 389
 - 内容の検索, 408
 - 削除, 403
 - 同期化, 795-806
 - CVS, 796, 800-803
 - rsync, 796
 - 圧縮, 395, 405

- 圧縮解除, 397
- 暗号化, 947
- 検索, 471
- 検索対象, 407
- 比較, 409
- 移動, 403
- 表示, 394, 408
- ファイルサーバ, 188
- ファイルシステム, 517-528
 - ACL, 333-346
 - cryptofs , 943
 - Ext2, 520
 - Ext3, 521-523
 - LFS, 526
 - OCFS2, 317-331, 524-525
 - ReiserFS, 519-520
 - XFS, 523-524
 - サポートする, 525-526
 - 修復, 1033
 - 制限, 527
 - 変更, 176
 - 暗号化, 943
 - 用語, 517
 - 選択, 518
- フォント, 538
 - TrueType, 536
 - X11コア, 538
 - Xft, 539
- ブート, 427
 - CDから, 999
 - GRUB, 445-465
 - initramfs, 429
 - initrd, 429
 - グラフィック, 463
 - フロッピーディスクから, 997
 - ブートセクタ, 445-446
 - ログ, 205
 - 設定
 - YaST, 457
- プロキシ, 190, 851 (参照 Squid)
- キャッシュ, 851
- 利点, 851
- 透過型, 864
- プロセス
 - 概要, 411
 - 終了, 412
- プロトコル
 - CIFS , 762
 - IPv6, 604
 - LDAP, 725
 - SLP, 663
 - SMB, 761
- ヘルプ, 981-985
 - FAQ, 987
 - HOWTO, 987
 - infoページ, 473
 - Linuxドキュメント(TLDP), 986
 - SUSE Help Center, 981
 - SUSEのガイドブック, 988
 - Usenet, 989
 - Wikipedia, 987
- X, 536
 - ガイド, 987
 - ガイドブック , 987
 - パッケージのドキュメント, 988
 - マニュアル, 988
 - マニュアルページ, 473, 985
 - 仕様, 990
 - 情報ページ, 986
 - 規格, 990
- ホスト名, 187
- ポート
 - スキャン, 867
- マウス
 - 設定, 168
- マスカレード, 896
 - SuSEfirewall2による設定 , 899
- マスターブートレコード (参照 MBR)
- マニュアルページ, 402, 473
- メモリ

- RAM, 472
- メールサーバ
 - 設定, 185
- モデム
 - YaST, 625
 - ケーブル, 631
- ユーザ
 - /etc/passwd, 548, 748
 - 管理, 193
- ランレベル, 181, 432-435
 - YaSTでの編集, 440
 - 変更, 434-435
- リリースノート, 50, 205
- ルーティング, 191, 601, 645-646
 - ネットマスク, 601
 - マスカレード, 896
 - ルート, 645
 - 静的, 645
- レスキューシステム, 1030, 1036
 - CDからの起動, 1031
 - ネットワークソースからの起動, 1031
- ログ
 - ログイン試行, 201
- ログファイル, 201, 469
 - boot.msg, 205, 559
 - Squid, 857, 860, 867
 - メッセージ, 205, 685, 904
- ローカライズ, 476
- ローカルAPIC
 - 無効, 25
- ワイルドカード, 407
- 使用許諾契約書, 32
- 印刷, 481
 - CUPS, 494
 - GDIプリンタ, 499
 - kprinter, 494
 - Samba, 763
 - xpp, 494
 - YaSTを使った設定, 485-490
 - ネットワークプリンタ, 490
 - ローカルプリンタ, 485
- コマンドライン, 494
- トラブルシューティング
 - ネットワーク, 501
 - ネットワーク, 501
- 国際化, 476
- 変数
 - 環境, 476
- 暗号化, 943-949
 - viを使ってファイルを, 949
 - YaSTを使用, 944
 - パーティション, 944-946
 - パーティションの作成, 945
 - ファイル, 947-949
 - リムーバブルメディア, 947
- 更新
 - YaST, 237
 - オンライン
 - コマンドライン, 224
 - サウンドミキサー, 258
- 検索, 407
- 環境設定, 441
 - ISDN, 628
- 環境設定ファイル, 644
 - .bashrc, 468, 472
 - .profile, 468
 - .xsession, 910
 - acpi, 560
 - crontab, 468
 - cs.cshrc, 478
 - dhclient.conf, 709
 - dhcp, 645
 - dhcpcd.conf, 710
 - fstab, 409
 - host.conf, 648, 686-695
 - HOSTNAME, 652
 - hosts, 188, 615, 647
 - ifcfg-*, 645
 - inittab, 432, 475

- inputrc, 475
- krb5.conf, 927-928, 930, 937
- krb5.keytab, 935
- named.conf, 684, 857
- nscd.conf, 652
- nsswitch.conf, 649, 748
- openldap, 939
- pam_unix2.conf, 936
- passwd, 236
- powersave.conf, 261
- resolv.conf, 473, 646, 684, 856
- samba, 765
- slapd.conf, 731, 940-941
- smb.conf, 766, 777
- smppd.conf, 659
- smpppd-c.conf, 660
- squid.conf, 856, 858, 865, 868, 870
- squidguard.conf, 870
- sshd_config, 910, 937
- ssh_config, 938
- sysconfig, 181, 441-444
- termcap, 475
- XF86Config, 256
- xorg.conf, 256, 529
 - Device, 534
 - Monitor, 536
 - Screen, 532
- カーネル, 429
- グループ, 236
- サービス, 765, 865
- ネットワーク, 645, 648
- パーミッション, 975
- プロファイル, 467, 471, 478
- ルート, 645
- ワイヤレス, 645
- 言語, 476, 478
- 画面
 - 解像度, 534
- 登録
 - YaST, 156

競合

- GRUB, 446

- 言語, 162, 182

設定

- DASD, 165

- DNS, 187, 673

- DSL, 184, 632

- GRUB, 455

- IPv6, 613

- ISDN, 184

- NFS, 188

- NTP, 189

- PAM, 259

- powertweak, 181

- Samba, 763-770

- クライアント, 191, 770

- サーバ, 191

- Squid, 858

- SSH, 905

- T-DSL, 634

- ZFCP, 166

- グラフィックカード, 214

- グループ, 200

- ケーブルモデム, 631

- サウンドカード, 168

- システム, 143-207

- システムサービス, 189

- セキュリティ, 192-203

- ソフトウェア, 146-161

- タイムゾーン, 182

- ネットワーク, 183-192, 617

- 手動, 640-658

- ネットワークカード, 184

- ハードウェア, 163-170

- ハードディスク

- DMA, 165

- ハードディスクコントローラ, 164

- ファイアウォール, 203

- メールサーバ, 185

- モデム, 184, 625

- モニタ, 214
- ユーザ, 193
- ルーティング, 191, 645
- ワイヤレスカード, 184
- 印刷, 485-490
 - ネットワークプリンタ, 490
 - ローカルプリンタ, 485
- 言語, 182
- 電子メール, 184
- 電源管理, 180
- 設定ファイル
 - .emacs, 474
 - asound.conf, 170
 - fstab, 178
 - grub.conf, 455
 - inittab, 434-435
 - logrotate.conf, 470
 - menu.lst, 448
 - modprobe.d/sound, 170
 - pam_unix2.conf, 747
 - powersave, 559
 - squid.conf, 862
 - suseconfig, 444
- 認証
 - Kerberos, 253
 - PAM, 545-553
- 論理ボリュームマネージャ (参照 LVM)
- 電子メール
 - 設定, 184
- 電源管理, 555-578
 - ACPI, 555, 559-567, 572
 - APM, 557-558, 572
 - cpufrequency, 569
 - cpuspeed, 569
 - powersave, 569
 - YaST, 578
 - サスペンド, 556
 - スタンバイ, 556
 - ハイバーネーション, 556
 - バッテリーモニタ, 556

充電レベル, 573

A

- ACL, 333-346
 - アクセス, 336, 340
 - サポート, 346
 - チェックアルゴリズム, 345
 - デフォルト, 336, 342
 - パーミッションビット, 338
 - マスク, 341
 - 処理, 336
 - 効果, 342
 - 定義, 336
 - 構造, 336
- ACPI
 - 無効, 25
- Apache, 187, 807-849
 - CGIスクリプト, 835
 - Squid, 867
 - SSL, 838-844
 - SSLサポートのあるApacheの設定, 843
 - SSL証明書の作成, 838
 - インストール, 808
 - クイックスタート, 807
 - セキュリティ, 844
 - トラブルシューティング, 846
- モジュール, 826-835
 - インストール, 827
 - マルチプロセッシング, 831
 - 作成, 834
 - 使用可能, 828
 - 外部, 833
- 停止, 824
- 環境設定, 809
 - ファイル, 810
 - 仮想ホスト, 813
 - 手動, 809-817
- 設定

YaST, 817-824
起動, 824
AutoYaST, 204
システムのクローン, 51

B

Bash, 384-397
 .bashrc, 468
 .profile, 468
 プロファイル, 467
BIND, 684-695
BIOS
 ブートシーケンス, 999
bzip2, 396

C

cat, 408
CD
 チェック, 163, 996
 ブート元, 999
cd, 404
chgrp, 401, 404
chmod, 400, 404
chown, 401, 404
CJK, 476
clear, 414
cp, 403
cpuspeed, 569
cron, 468
CVS, 796, 800-803

D

date, 411
deltarpm, 352
df, 410
DHCP, 187, 699-714
 dhcpd, 710-712
 YaSTによる設定, 700
 サーバ, 710-712

 パッケージ, 709
 静的アドレスの割り当て, 712
diff, 409
DNS, 614
 BIND, 684-695
 NIC, 615
 Squid and, 857
 オプション, 687
 セキュリティ, 973
 ゾーン
 ファイル, 690
 トラブルシューティング, 685
 ドメイン, 646
 ネームサーバ, 646
 メールエクスチェンジャ, 615
 ログの記録, 688
 最上位ドメイン, 615
 用語, 673
 設定, 187, 673
 起動, 685
 転送, 685
 逆引き, 694
DOS
 ファイル共有, 761
du, 410

E

Emacs, 473-474
 .emacs, 474
 default.el, 474

F

file, 408
find, 407
Firefox
 URL openコマンド, 263
free, 411

G

GNOME

シェル, 384

grep, 408

GRUB, 445-465

device.map, 447, 454

GRUB Geomエラー, 464

grub.conf, 447, 455

menu.lst, 447-448

アンインストール, 461

コマンド, 446-457

デバイス名, 450

トラブルシューティング, 464

パーティション名, 450

ブート, 446

ブートセクタ, 446

ブートパスワード, 455

ブートメニュー, 448

マスターブートレコード(MBR), 445

メニューエディタ, 453

制限, 446

gunzip, 397

gzip, 396, 405

H

halt, 414

help

マニュアルページ, 402

I

I18N, 476

inetd, 189

infoページ, 473

init, 432

inittab, 432

スクリプト, 435-439

スクリプトの追加, 438

IPアドレス, 601

IPv6, 604

設定, 613

クラス, 601

プライベート, 603

マスカレード, 896

動的割り当て, 699

iSCSI, 297

K

KDE

シェル, 384

Kerberos, 913-920

KDC, 922-927

nsswitch.conf, 923

管理, 933

起動, 926

keytab, 935

LDAP, 938-941

PAMサポート, 936-937

SSH設定, 937

stashファイル, 925

ticket-granting (チケット保証)サービス, 917

インストール, 921-941

オーセンティケータ, 914

クライアント

設定, 927-930

クロックスキュー, 930

セッションキー, 915

チケット, 914, 917

プリンシパル, 914

ホスト, 935

作成, 926

マスタキー, 925

レルム, 921

作成, 925

時計の同期化, 923

管理, 921-941

設定

クライアント, 927-930

資格情報, 914

kill, 412

killall, 412

L

L10N, 476

laptops

電源管理, 555-568

LDAP, 725-759

ACL, 732

Kerberos, 938-941

ldapadd, 737

ldapdelete, 741

ldapmodify, 739

ldapsearch, 740

YaST

クライアント, 747

テンプレート, 748

モジュール, 748

アクセス制御, 735

グループの管理, 755

サーバの設定

YaST, 741

サーバ設定

マニュアル, 731

ディレクトリツリー, 727

データの削除, 741

データの変更, 739

データの検索, 740

データの追加, 737

ユーザの管理, 755

設定

YaST, 741

less, 394, 408

LFS, 526

Lightweight Directory Access Protocol
(参照 LDAP)

Linux

アンインストール, 461

ネットワーク, 597

他のOSとのファイル共有, 761

linuxrc

手動インストール, 258

ln, 403

locate, 471

logrotate, 469

LPARインストール

IPL, 40

ls, 385, 402

LSB

パッケージのインストール, 347

LVM

YaST, 127

M

MBR, 445-446

mkdir, 404

more, 394

mount, 409

mv, 403

N

NAT (参照 マスカレード)

NetBIOS, 762

Network Information Service (参照 NIS)

NetworkManager, 638

NFS, 779

インポート, 781

エクスポート, 790

クライアント, 188, 780

サーバ, 188, 784

マウント, 781

NIS, 715-723

クライアント, 189, 722

サーバ, 189

スレーブ, 715-722

マスタ, 715-722

nslookup, 413

NSS, 649
データベース, 650
NTP
クライアント, 189

O

OpenLDAP (参照 LDAP)
OpenSSH (参照 SSH)
OpenWBEM, 267-296
OS/2
ファイル共有, 761

P

PAM, 545-553
設定, 259
passwd, 413
PBX, 630
PCIデバイス
ドライバ, 179
ping, 412, 654
Pluggable Authentication Modules(プラグ可能な認証モジュール) (参照 PAM)
ports
53, 687
PostgreSQL
更新, 237
powersave, 569
設定, 569
processes, 411
ps, 411

R

RAID
YaST, 137
reboot, 414
RFC, 597
rm, 403
rmdir, 404
RPM, 347-359

deltarpm, 352
rpmnew, 348
rpmorig, 348
rpmsave, 348
SRPMS, 357
アップデート, 349
アンインストール, 350
クエリー, 353
セキュリティ, 976
ツール, 359
データベース
再構築, 350, 356
パッチ, 350
依存関係, 348
検証, 348, 355
rpmbuild, 347
rsync, 796, 803
rug, 224-228

S

Samba, 761-778
CIFS, 762
SMB, 761
swat, 765
TCP/IP, 761
インストール, 763
クライアント, 191, 762-763, 770-771
サーバ, 191, 762-770
シェア, 767
セキュリティ, 769-770
パーミッション, 769
プリンタ, 763
ログイン, 771
停止, 763
共有, 763
印刷, 771
名前, 762
設定, 763-770
起動, 763

SaX2

- キーボードの設定, 219
- グラフィックカード, 215
- グラフィックタブレット, 219
- タッチスクリーン, 220
- ディスプレイデバイス, 216
- ディスプレイ設定, 214
- デュアルヘッド, 216
- マウス設定, 218
- マルチヘッド, 218
- 解像度とカラー設定, 216

SCPM, 181

scripts

- modify_resolvconf, 646

SLP, 663

- Konqueror, 664
- slptool, 664
- サービスの提供, 665
- サービスの登録, 665
- ブラウザ, 664

SMB (参照 Samba)

smbd, 761

spm, 356

Squid, 851

- ACL, 862
- Apache, 867
- cachemgr.cgi , 867, 869
- Calamaris, 871-872
- CPU, 855
- DNS, 857
- RAM, 855
- squidGuard, 869
- アクセス制御, 868
- アンインストール, 857
- オブジェクトステータス, 853
- キャッシュ, 851-852
 - サイズ, 854
 - 破損, 857
- システム要件, 854
- セキュリティ, 852

ディレクトリ, 856

- トラブルシューティング, 857
- パーミッション, 856, 862
- ファイアウォール, 865
- レポート, 871-872
- ログファイル, 857, 860, 867
- 停止, 856
- 機能, 851
- 統計情報, 867, 869
- 設定, 858
- 透過型プロキシ, 864, 867
- 開始, 856

SSH, 905-911

- scp, 907
- sftp, 907
- ssh, 906
- ssh-agent, 910
- ssh-keygen, 909
- sshd, 907
- X, 910
- デーモン, 907
- 認証メカニズム, 909
- 鍵ペア, 908-909

su, 413

SUSEのガイドブック , 988

T

- tar, 395, 406
- TCP/IP, 597
 - ICMP, 598
 - IGMP, 598
 - TCP, 598
 - UDP, 598
 - パケット, 599-600
 - レイヤモデル, 598
- telnet, 413
- TLDP, 986
- top, 411
- Tripwire

AIDEによる置換, 259

U

ulimit, 471

オプション, 471

umount, 409

updatedb, 407

USキーボードレイアウト, 1001

V

VNC

管理, 190

W

whois, 615

Windows

ファイル共有, 761

X

X

SaX2, 530

SSH, 910

TrueTypeフォント, 536

X11コアフォント, 538

xft, 536

Xft, 539

xorg.conf, 530

キーボードの設定, 219

グラフィックカード, 215

グラフィックタブレット, 219

セキュリティ, 970

タッチスクリーン, 220

ディスプレイデバイス, 216

ディスプレイ設定, 214

デュアルヘッド, 216

ドライバ, 535

フォント, 536

フォントシステム, 538

ヘルプ, 536

マウス設定, 218

マルチヘッド, 218

仮想画面, 534

文字セット, 536

解像度とカラー設定, 216

設定, 529-536

X Windowシステム (参照 X)

X.509証明書

YaST, 875

リポジトリ, 879

原理, 875

失効リスト, 878

証明書, 877

X.Org, 529

Xft, 539

xinetd, 189

XKB (参照 キーボード、XKB)

xorg.conf

Depth, 533

Device, 534

Display, 533

InputDevice, 531

modeline, 531

Modeline, 533

Modes, 531, 533

modules, 531

Monitor, 531, 533

ServerFlags, 531

ファイル, 531

色深度, 533

Xキーボード拡張 (参照 キーボード、XKB)

Y

YaST

AutoYaST, 204

CA管理, 202, 880

CD Creator, 204

DASD, 165

- DHCP, 700
- DMA, 165
- DNS, 187
- DSL, 632
- EVMS, 172
- GRUB, 458
- Heartbeat, 172
- ISDN, 628
- Kerberosクライアント, 188
- LDAP, 188
 - クライアント, 747
 - サーバ, 741
- LILO, 458
- LVM, 127, 172
- ncurses, 207
- NFSクライアント, 188
- NFSサーバ, 188
- NISクライアント, 722
- Novell AppArmor, 192
- Novellカスタマセンタ, 156
- NTPクライアント, 189
- PCI デバイスドライバ, 179
- powertweak, 181
- RAID, 137
- rootのパスワード, 42
- Samba
 - クライアント, 191, 770
 - サーバ, 191
- SCPM, 181
- sendmail, 184
- SLP, 191
- SLPブラウザ, 664
- Support Query, 204
- sysconfigエディタ, 181, 442
- T-DSL, 634
- X.509証明書, 875
 - CAオブジェクトのLDAPへのエクスポート, 888
 - CAオブジェクトのファイルへのエクスポート, 889
- CRLの作成, 887
- サブCA, 882
- デフォルト値の変更, 885
- ルートCA, 880
- 一般サーバ証明書のインポート, 890
- 証明書, 883
- ZFCP, 166
- アップデート, 160
- アドオン製品, 33, 154-155
- インストール, 21-52
- インストールの設定, 34
- インストールサーバ, 204
- インストールソース, 155
- インストールモード, 33
- インストール概要, 34
- オンラインアップデート, 156-159
- キーボード, 167
- クエリーのサポート, 993
- クラスタ, 172
- グラフィックカード, 214
- グループ管理, 200
- ケーブルモデム, 631
- コマンドライン, 211
- コントロールセンター, 145
- サウンドカード, 168
- サーバ証明書, 202
- システムの修復, 1025
- システムセキュリティ, 200
- システム起動, 22
- ジョイスティック, 167
- セキュリティ, 192-203
- セーフ設定, 26
- ソフトウェア, 146-161
- ソフトウェアアップデート, 47
- タイムゾーン, 34, 182
- テキストモード, 207-210
- ディレクトリへのインストール, 162
- ドライバCD, 207
- ネットワークカード, 617

- ネットワーク設定, 44, 183-192
- ハードウェア, 163-170
 - 情報, 164, 996
- ハードディスクコントローラ, 164
- バックアップ, 161, 170
- パーティション, 36
- パーティション設定, 172
- ファイアウォール, 203
- ブートローダ
 - タイプ, 458
 - パスワード, 461
 - 場所, 459
- ブート設定, 457
 - セキュリティ, 461
 - タイムアウト, 460
 - デフォルトシステム, 460
- プリンタの設定
 - ローカルプリンタ, 485
- プリンタ設定, 485-490
 - ネットワークプリンタ, 490
- プロファイルマネージャ, 181
- ホスト名, 43, 187
- メディアチェック, 32, 163, 996
- メモリテスト, 26
- メールサーバ, 185
- モデム, 625
- モニタ, 214
- ユーザ管理, 193
- ランレベル, 440
- リリースノート, 205
- ルーティング, 191
- レスキューシステム, 26
- 仮想化, 203
 - インストール, 203
 - ハイパーバイザ, 203
- 更新, 237
- 登録, 156
- 自動インストール, 204
 - プロファイル, 204
- 自動ログイン, 195

- 言語, 29, 144, 162, 182
- 設定, 143-207
- 開始, 22, 143
- 電子メール, 184
- 電源管理, 180, 578
- 高可用性, 172
- YP (参照 NIS)

Z

- z/VMインストール
 - IPL, 40
- ZENworks
 - zmd, 223
- zmd, 223