

openSUSE

www.suse.com

2012/08/12

リファレンス



リファレンス

Copyright © 2006–2012 Novell, Inc. and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled 「GNU Free Documentation License」.

For Novell trademarks, see the Novell Trademark and Service Mark list <http://www.novell.com/company/legal/trademarks/tmlist.html>. All other third party trademarks are the property of their respective owners. A trademark symbol (® , # etc.) denotes a Novell trademark; an asterisk (*) denotes a third party trademark.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither Novell, Inc., SUSE LINUX Products GmbH, the authors, nor the translators shall be held liable for possible errors or the consequences thereof.

下記に上記の日本語翻訳を掲載します。日本語の翻訳は公式なものではないことに注意してください。

Copyright © 2006–2012 Novell, Inc. および貢献者が全権利を留保しています。

この文書を、フリーソフトウェア財団発行の GNU フリー文書利用許諾契約書 バージョン 1.2 または (希望すれば) 1.3 が定める条件の下で複製、頒布、あるいは 改変することを許可する。ただし、この著作権とライセンス表記については変更不可部分 とする。この利用許諾契約書の複製物は「GNU フリー文書利用許諾契約書」という章に含まれている。

Novell 社の商標については、Novell 社の商標とサービスマーカー覧 <http://www.novell.com/company/legal/trademarks/tmlist.html> をご覧ください。Linux は Linus Torvalds 氏による登録商標です。その他の商標は 各所有者の所有物です。商標シンボル (®, # など) は それぞれ Novell 社の商標であることを示しています。また、アスタリスク (*) は 第三者の商標を示しています。

この書籍内にある全ての情報は細部に至るまで最大限の注意を払って制作されていますが、完全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、本書籍内の誤りとそこから生じる結果について、一切の保証はいたしません。

目次

このガイドについて	ix
パート I インストールと配置	1
1 YaST を利用したインストール	3
1.1 インストールメディアの選択	3
1.2 インストール方法の選択	5
1.3 インストール手順	9
1.4 インストール向けのシステムスタートアップ	9
1.5 起動画面	10
1.6 ようこそ	13
1.7 インストールモード	14
1.8 時刻とタイムゾーン	17
1.9 デスクトップの選択	18
1.10 パーティション設定の提案	19
1.11 新規ユーザの作成	22
1.12 インストール設定	26
1.13 インストールの実行	31
1.14 インストール済みシステムの設定	32
1.15 グラフィカルなログイン	37
2 リモートインストール	39
2.1 リモートインストールの手順	39
2.2 インストール元のデータを保存するサーバの構築	48
2.3 ターゲットシステムの起動準備	58
2.4 インストールのためのターゲットシステムの起動	68
2.5 インストール処理の監視	71
3 高度なディスク設定	75
3.1 YaST パーティション設定の利用	75
3.2 LVM の設定	87
3.3 ソフトウェア RAID の設定	92

4	64 ビット環境における 32 ビットおよび 64 ビットアプリケーション	99
4.1	ランタイムサポート.	99
4.2	ソフトウェア開発.	100
4.3	両プラットフォーム対応のソフトウェアコンパイル.	101
4.4	カーネル仕様.	102
5	Linux システムの起動	103
5.1	Linux の起動処理.	103
6	systemd デーモン	109
6.1	基本的な使いかた.	110
6.2	システムの起動とターゲットの管理.	117
6.3	高度な使い方.	125
6.4	さになる情報.	128
7	ブートローダ GRUB	129
7.1	GRUB での起動.	130
7.2	YaST を利用したブートローダの設定.	141
7.3	Linux ブートローダのアンインストール.	147
7.4	起動 CD の作成.	147
7.5	グラフィカルな SUSE スクリーン.	149
7.6	トラブルシューティング.	149
7.7	さらなる情報.	151
8	ブートローダ GRUB2	153
8.1	GRUB Legacy との主な違い.	153
8.2	設定ファイルの構造.	154
8.3	YaST を利用したブートローダの設定.	166
8.4	Linux ブートローダのアンインストール.	171
8.5	グラフィカルな SUSE スクリーン.	171
8.6	トラブルシューティング.	172
8.7	さらなる情報.	173
9	特殊なシステム機能	175
9.1	特殊なソフトウェアパッケージに関する情報.	175
9.2	仮想コンソール.	182
9.3	キーボードマッピング.	183
9.4	言語と国の設定.	183

10	udev による動的なカーネルデバイス管理	189
10.1	/dev ディレクトリ	189
10.2	カーネルの uevents と udev	190
10.3	ドライバ、カーネルモジュール、デバイス	190
10.4	起動と初期デバイス設定	191
10.5	udev デモンの稼働監視	192
10.6	udev ルールによるカーネル側デバイスイベント処理への影響	193
10.7	固定のデバイス命名	200
10.8	udev で使用するファイル	201
10.9	さらなる情報	201
パート III	サービス	203
11	ネットワークの基礎	205
11.1	IP アドレスとルーティング	208
11.2	IPv6 一次世代のインターネット	211
11.3	名前解決	221
11.4	YaST を利用したネットワーク接続の設定	223
11.5	NetworkManager	244
11.6	手動でのネットワーク設定方法	247
11.7	ダイヤルアップ接続支援としての smpppd	264
12	ネットワーク内の SLP サービス	267
12.1	インストール	267
12.2	SLP の有効化	268
12.3	openSUSE での SLP フロントエンド	268
12.4	SLP 経由でのインストール	269
12.5	SLP 経由でのサービス提供	269
12.6	さらなる情報	270
13	ドメインネームシステム	271
13.1	DNS 用語	271
13.2	インストール	272
13.3	YaST を利用した設定	273
13.4	BIND ネームサーバの起動	281
13.5	/etc/named.conf 設定ファイル	283
13.6	ゾーンファイル	287
13.7	ゾーンデータの動的な更新	291
13.8	機密を保持する通信	292
13.9	DNS セキュリティ	293
13.10	さらなる情報	294

14 DHCP	295
14.1 YaST での DHCP サーバ設定.	296
14.2 DHCP ソフトウェアパッケージ.	300
14.3 DHCP サーバ dhcpd.	300
14.4 さらなる情報.	304
15 NTP を利用した時刻同期	305
15.1 YaST を利用した NTP クライアントの設定.	305
15.2 ネットワーク内にある NTP の手動設定.	310
15.3 システム稼働時の動的な時刻同期.	311
15.4 ローカル参照時計の設定.	312
16 NFS でのファイル共有	313
16.1 用語.	313
16.2 NFS サーバのインストール.	314
16.3 NFS サーバの設定.	314
16.4 クライアントの設定.	324
16.5 さらなる情報.	327
17 Samba	329
17.1 用語.	329
17.2 Samba サーバのインストール.	331
17.3 Samba の起動と停止.	331
17.4 Samba サーバの設定.	331
17.5 クライアントの設定.	339
17.6 ログインサーバとしての Samba の利用.	340
17.7 さらなる情報.	341
18 Apache HTTP サーバ	343
18.1 クイックスタート.	343
18.2 Apache の設定.	345
18.3 Apache の起動と停止.	361
18.4 モジュールのインストール／有効化／設定.	364
18.5 CGI スクリプトを動作させる方法.	372
18.6 SSL で通信の機密を保持する Web サーバの設定.	375
18.7 セキュリティ問題の回避.	382
18.8 トラブルシューティング.	384
18.9 さらなる情報.	385
19 YaST を利用した FTP サーバの設定	389
19.1 FTP サーバの起動.	391

19.2	FTP の一般的な設定.	392
19.3	FTP パフォーマンス設定.	393
19.4	認証.	393
19.5	詳細設定.	394
19.6	さらなる情報.	394
パート IV	モバイル環境	395
20	Linux でのモバイルコンピューティング	397
20.1	ラップトップ.	397
20.2	モバイルハードウェア.	404
20.3	携帯電話と PDA.	405
20.4	さらなる情報.	405
21	電源管理	407
21.1	省電力機能.	407
21.2	Advanced Configuration and Power Interface (ACPI).	408
21.3	ハードディスクの休止.	411
21.4	トラブルシューティング.	413
21.5	さらなる情報.	415
22	無線 LAN	417
22.1	無線 LAN 標準.	417
22.2	動作モード.	418
22.3	認証.	419
22.4	暗号化.	421
22.5	YaST を利用した設定.	422
22.6	無線 LAN 設定における豆知識.	430
22.7	トラブルシューティング.	431
22.8	さらなる情報.	433
23	NetworkManager の使用	435
23.1	NetworkManager の利用例.	435
23.2	NetworkManager の有効化と無効化.	436
23.3	ネットワーク接続の設定.	437
23.4	KDE NetworkManager フロントエンドの使用.	441
23.5	GNOME NetworkManager の使用.	444
23.6	NetworkManager と VPN.	447
23.7	NetworkManager とセキュリティ.	448
23.8	よくある質問.	450
23.9	トラブルシューティング.	452

23.10	さらなる情報.	453
-------	---------	-----

24 タブレット PC の使用 **455**

24.1	タブレット PC パッケージのインストール.	456
24.2	タブレットデバイスの設定.	456
24.3	仮想キーボードの使用.	457
24.4	ディスプレイの回転表示.	457
24.5	ジェスチャー認識の使用.	458
24.6	ペンを利用したメモ取りとスケッチ.	460
24.7	トラブルシューティング.	462
24.8	さらなる情報.	463

25 ファイルのコピーと共有 **465**

25.1	シナリオ.	466
25.2	アクセス方法.	467
25.3	直接接続によるファイルアクセス.	469
25.4	同一のコンピュータにおける異なる OS 上のファイルへのアクセス.	470
25.5	Linux コンピュータ間のファイルコピー.	471
25.6	SSH を利用した Linux と Windows コンピュータのファイルコピー.	479
25.7	Linux コンピュータ間のファイル共有.	480
25.8	Samba を利用した Linux と Windows のファイル共有.	483
25.9	さらなる情報.	486

A サンプルネットワーク **487**

B GNU ライセンス **489**

B.1	GNU General Public License.	489
B.2	GNU 一般公衆利用許諾契約書 (日本語訳).	493
B.3	GNU Free Documentation License.	497
B.4	GNU フリー文書利用許諾契約書.	502

このガイドについて

このマニュアルは、openSUSE® に関する一般的な理解を深めるためのものです。主に基本的な管理知識のあるシステム管理者と一般家庭ユーザに向けて書かれています。このマニュアル内の様々な箇所をお読みになり、日々の生活で必要なアプリケーションの選択や高度なインストール方法の説明、設定シナリオ などをご確認ください。

高度な配置シナリオ

openSUSE を遠隔から配置したり、複雑なディスク設定を行なったりする方法を示しています。

ソフトウェアの管理と更新

YaST やコマンドライン、1 クリックインストール 機能 を利用した、ソフトウェアのインストールと削除方法のほか、システムを最新の状態に保つ手順について示しています。

システム管理

お使いの openSUSE 環境における設定やアップグレードの方法、テキストモードでのシステム管理方法、Linux 管理者が知っておく必要のあるいくつかの重要なユーティリティに関する基礎知識をそれぞれ示しています。

システム

お使いの Linux システムのコンポーネントに関する紹介や、それらの操作に関するより深い情報を示しています。

サービス

openSUSE で提供される様々なネットワークサービスやファイルサービスについて、設定方法を示しています。

モバイル環境

openSUSE でのモバイルコンピューティングに関する紹介のほか、ワイヤレスコンピューティングや電源管理といった様々なオプションについて示しています。

このマニュアルの多くの章には、追加の文書リソースに対するリンクが含まれています。これらの追加文書はシステム内から利用することができるものがあるほか、インターネット上で公開されているようなものもあります。

お使いの製品で利用可能な文書の概要は、<http://www.novell.com/documentation/opensuse114> か、もしくは下記の章を参照してください。

1 利用可能な文書

HTML 版や PDF 版の各マニュアルは、それぞれ各種の言語に翻訳されています。この製品に対しては、それぞれ下記に示す ユーザ向けおよび管理者向けマニュアルが用意されています:

スタートアップ (↑ スタートアップ)

DVD や ISO イメージから openSUSE のインストールを行ない、GNOME や KDE デスクトップの簡単な説明と、そこで動作する主なアプリケーションを紹介するまでの範囲を説明しています。また、LibreOffice の概要説明のほか、文書作成や表計算での作業、およびグラフィックやプレゼンテーションの作成を行なうためのモジュールについても説明しています。

リファレンス (i ページ)

openSUSE に関する一般的な理解を深め、より詳しいシステム管理作業を行なうための情報が書かれています。主にシステム管理者のほか、システム管理知識のあるホームユーザに向けた文書です。また、複雑な配置シナリオやシステムの管理方法、主なシステムコンポーネントとのやりとりや openSUSE が提供するネットワークサービス、ファイルサービスに関する詳しい情報も書かれています。

セキュリティガイド (↑ セキュリティガイド)

ローカル環境やネットワークセキュリティを含めた、システムセキュリティに関する基本的な考え方が書かれています。AppArmor のようなセキュリティソフトウェア (プログラムが読み書きしたり実行したりするファイルをプログラム単位で指定できるもの) の一般的な使い方を示しているほか、セキュリティ関連のイベント情報を確実に収集するための監査システムの使い方も示しています。

システム分析とチューニングガイド (↑ システム分析とチューニングガイド)

問題の検出や解決、最適化に対する管理者向けのガイドです。お使いのシステムに関して監視ツールを利用し点検と最適化を行なう方法や、効率的に資源を管理するための手順が記されています。また、一般的によくある問題やそれに対する解決方法、追加のヘルプや文書資源についても示しています。

KVM を利用した仮想化 (↑ KVM を利用した仮想化)

このマニュアルでは、openSUSE で KVM (カーネルベースの仮想マシン) による仮想化を設定したり、管理したりするための手順を紹介しています。また、libvirt や QEMU を利用した VM ゲストの管理方法についても紹介しています。

ほとんどの製品マニュアルは HTML 版の形で、インストール済みシステムの `/usr/share/doc/manual` に置かれています。またデスクトップのヘルプセンターからもアクセスすることができます。最新の文書は、<http://www.suse.com/documentation> に置いています。ここからお使いの製品について、PDF 版と HTML 版をダウンロードすることができます。

2 フィードバック

いくつかの方法でフィードバックを送ることができます:

バグや機能追加リクエスト

製品のコンポーネントに対してバグの報告を行ったり、もしくは機能の追加リクエストを送信したりしたい場合は、<https://bugzilla.novell.com/> をご利用ください。文書内の間違いについては、各製品の *Documentation* コンポーネントに対してバグ報告をお願いいたします。

Bugzilla を初めてお使いになる場合は、下記の記事をお読みください:

- http://ja.opensuse.org/Submitting_bug_reports
- http://ja.opensuse.org/Bug_reporting_FAQ

ユーザコメント

このマニュアルに対するコメントや提案のほか、この製品に含まれる他のドキュメント類に対するコメントを歓迎します。オンラインドキュメントの場合は、それぞれのページ下部にあるコメント機能をご利用いただくか、もしくは <http://www.suse.com/documentation/feedback.html> からコメントをお送りください。

メール

この製品に対するフィードバックを送信するには、`doc-team@suse.de` 宛のメールもお使いいただけます。それぞれドキュメントのタイトルと製品バージョン、発行日時を添えてお送りください。また、間違いの報告や加筆に対する提案につきましては、その簡潔な説明と、セクション番号およびページ (または URL) をお送りください。

3 文書規約

このマニュアルでは、下記のルールで文書を記述しています:

- `/etc/passwd`: ディレクトリ名やファイル名を示しています
- *placeholder*: 置き換えを示しています *placeholder* を実際の値に置き換えます
- `PATH`: `PATH` という名前の環境変数を示しています
- `ls, --help`: コマンドやオプション、パラメータを示しています
- `user`: ユーザまたはグループ
- `, + F1`: 入力するキーやキーの組み合わせを示しています; キーはキーボードに書かれているとおりに大文字で示されます
- `ファイル, ファイル > 名前を付けて保存`: メニュー項目やボタンなどを示しています
- `ダンシングペンギン` (他のマニュアル内 `ペンギン` の章): 他のマニュアル内にある章を示しています

4 このマニュアルの作成について

この書籍は、DocBook (詳しくは <http://www.docbook.org> をご覧ください) のサブセットである Novdoc で書かれています。XML のソースファイルは `xmllint` で検証された後に `xsltproc` で処理され、Norman Walsh 氏のスタイルシートのカスタマイズ版を利用して XSL-FO に変換されます。最終的な PDF ファイルは RenderX 提供の XEP で生成しています。また、このマニュアルを構築するために使用するオープンソースツールとその環境は、openSUSE と共に公開されている `daps` パッケージ内にあります。なお、`daps` の Web ページは <http://daps.sf.net/> です。

5 ソースコード

openSUSE のソースコードは、どなたにでもご利用いただけます。ダウンロードのリンクやその他の説明については、http://ja.opensuse.org/Source_code をお読みください。

6 謝辞

多数の無償貢献のお陰で、Linux 開発者はその開発にあたってグローバルな協力を 行なうことができています。我々は彼らのそのような努力に感謝します— 彼らの 貢献がなければ本ディストリビューションは存在していませんでした。また、Frank Zappa 氏と Pawar 氏にも感謝しています。もちろん Linus Torvalds 氏には特に 感謝しています。

Have a lot of fun!

SUSE チームより

パート I. インストールと配置

YaST を利用したインストール

お使いのシステムのインストールや、設定を行なうための中枢ツール YaST を利用し、openSUSE® のインストールを行ないます。YaST はインストールの手順案内を行なうほか、基本的なシステム設定を行なうことができます。インストールや設定作業の際、YaST はお使いのシステムにおける現在の設定とハードウェアコンポーネントの状態を分析し、この分析に基づいたインストール設定の提案を表示します。既定では YaST は全てのインストール手順の概要とヘルプをウインドウの左側に表示するようになっています。ヘルプテキストを表示するには、ヘルプボタンを押してください。

openSUSE をはじめてお使いになる場合は、ほとんどの箇所で YaST が提案したとおりの設定に従うのがよいでしょう。もちろん、必要に応じてシステムの設定をチューニングしてもかまいません。ユーザアカウントやシステム言語など、基本的なシステム設定のうちほとんどは、インストール後からでも変更することができます。

1.1 インストールメディアの選択

openSUSE のインストールは、オンラインや小売りの形式で提供されている下記のようなメディアから行なうことができます：

DVD 小売り版

1 枚目のメディアには、32 ビット版と 64 ビット版両方の openSUSE ディストリビューションが含まれています。2 枚目のメディアには、プロプライエタリと呼ばれる商用アドオンソフトウェアが含まれています。

このインストール方法の場合、インストール時におけるネットワークアクセスは必要ありません。openSUSE を完全インストールする場合であっても 外部のリポジトリを利用する必要はありません。もちろん、インストールサーバ からネットワークを経由して、本 DVD の内容にアクセスさせることもできます。

DVD ダウンロード版

32 ビット版または 64 ビット版として、1 枚の DVD (単層) メディアが提供されています。

完全な openSUSE システムを用意したい場合に、このインストール オプションを選択してください。DVD の ISO イメージをダウンロードする 作業以外のネットワーク接続は必要ありません。メディア全体をダウンロードして実際のインストールメディアを書き込んでからインストール作業を行なう ことになります。もちろん、インストールサーバからネットワークを経由して、本 DVD の内容にアクセスさせることもできます。

KDE4/GNOME ライブ CD

ダウンロード可能なライブ CD には、それぞれ KDE4 デスクトップ版と GNOME デスクトップ版があります。それぞれ有名どころのアプリケーションと共に、32 ビット版と 64 ビット版があります。

はじめて openSUSE をご利用になる場合にこのオプションを選択してください。ライブ CD 版は、お使いのコンピュータ内にあるハードディスク の内容を変更したりすることはなく、全て RAM 内で動作します。そのため、インストール作業も不要です。ただし、インストール作業を行ないたい場合は ライブ CD を起動している状態から openSUSE のインストールを行なう こともできます。メディアのダウンロード作業以外にはネットワーク接続の 必要はありません。

ヒント: USB メモリからのライブ CD 起動

ライブ CD は USB メモリの起動イメージとしても利用することができます。コマンドラインプログラム dd を利用することで、起動可能な USB メモリを作成することができます。下記のような書式で 実行してください:

dd if=ISO イメージファイル of=USB メモリのデバイス名 bs=4M

dd は、既定では Linux や MacOS で利用できます。Microsoft Windows 版は <http://www.chrysocome.net/dd> からダウンロードしてください。

警告: dd コマンドを使用すると、USB メモリ内にある全ての データが上書きされます!

ミニ CD

ミニ CD には、インストール作業に必要な最小限の Linux システムが含まれています。インストールシステムそれ自身とインストールデータは、それぞれネットワーク上の資源から読み込むことになります。SLP を利用したネットワークインストールを行なうには、1.2.1 項「SLP を利用したネットワークサーバからのインストール」(7 ページ) で説明されている手順でインストールを行なってください。HTTP, FTP, NFS, SMB の各サーバを利用したネットワークインストールを行なうには、1.2.2 項「SLP を利用しないネットワークソースからのインストール」(8 ページ) をご覧ください。

重要: アドオン CD—追加ソフトウェアのインストール

アドオン CD (拡張またはサードパーティ製品) は単独のインストールメディアとして利用することはできません。その代わり、インストール時の追加ソフトウェア資源として組み込むことができます。現時点では、openSUSE 向けに追加言語と非オープンソースのソフトウェアを提供しています。詳しくは 1.7.1 項「アドオン製品」(15 ページ) をお読みください。

1.2 インストール方法の選択

インストールメディアを選択したら、次に要件に応じたインストール方法と起動オプションを決定してください。

openSUSE メディアからのインストール

マシン単独のインストールを行なって、インストールデータや起動時のインフラにネットワークを利用しない場合に、このオプションを選択してください。1.3 項「インストール手順」(9 ページ) に示されたインストール手順のとおり実施してください。

ライブ CD からのインストール

ライブ CD からのインストールを行なうには、まず CD からライブシステムを起動してください。起動した後は、デスクトップ上にあるインストールアイコンを押すことでインストール処理が起動します。インストール処理の第 1 段階は、デスクトップ上のウィンドウ内で作業を行なうことができます。また、ライブ CD では既存のシステムを更新することはできず、新規のインストール (自動設定付き) のみを行なうことができます。

ネットワークサーバからのインストール

お使いのネットワーク上にインストールサーバをお持ちの場合や、インストールデータを外部のサーバから取得したい場合に選択してください。このイン

ストール方法では物理的なメディア (フロッピー, CD または DVD, ハードディスクなど) のほか、PXE/BOOTP を利用したネットワークブートを 設定して起動することもできます。詳しくは 1.2.1 項「SLP を利用したネットワークサーバからのインストール」(7 ページ) や 1.2.2 項「SLP を利用しないネットワークソースからのインストール」(8 ページ), 第2章 リモートインストール (39 ページ) をそれぞれお読みください。

Windows からの openSUSE 12.2 インストーラを 利用したインストール
Windows から Linux へのスムーズな移行作業を行ないたい場合、このオプションを 選択してください。openSUSE 12.2 インストーラは、Windows のブートローダを修正することで openSUSE のインストール処理を起動できるようにします。このインストールオプションは DVD メディアをご利用の場合にのみ選択できます。詳しくは 1.2.3 項「Windows からの openSUSE 12.2 インストーラを利用したインストール」(8 ページ) をお読みください。

openSUSE では、いくつかの方法から起動オプションを選択することができます。これは利用可能なハードウェアに依存するほか、希望するインストールシナリオに従って選択を行ないます。openSUSE メディアからの 起動や openSUSE 12.2 インストーラの使用が最も素直な選択ですが、要件によっては特別な選択を行なう必要があるかもしれません：

表 1.1 起動オプション

起動オプション	説明
DVD	これが最も簡単な起動オプションです。このオプションは、Linux に 対応しているローカル DVD-ROM ドライブをお持ちの場合に選択できます。
openSUSE 12.2 インストーラ	openSUSE 12.2 インストーラは、Microsoft Windows で 動作するソフトウェアで、インストール処理を直接起動できるように設定します。
PXE または BOOTP	ネットワークからの起動はシステムの BIOS やファームウェアでの対応が 必須であり、ネットワーク上にブートサーバを用意する必要があります。ブートサーバとして他の

起動オプション	説明
	openSUSE システムを利用することもできます。詳しくは下記をお読みください: http://ja.opensuse.org/SDB:PXE_boot_installation 第2章 リモートインストール (39 ページ)
ハードディスク	ハードディスクから openSUSE インストールを起動することもできます。これを行なうには、インストールメディア内の <code>/boot/architecture/</code> ディレクトリにあるカーネル (linux) と インストールシステム (initrd) をそれぞれ ハードディスクにコピーし、インストール済みの openSUSE インストール 内に存在する既存のブートローダに対して、必要な項目を追加してください。

ヒント: UEFI マシン上での DVD からの起動

#amd64 em64t: DVD1 は UEFI (Unified Extensible Firmware Interface) 対応のマシンの起動メディアとしても利用することができます。詳しくは、お使いのマシンの製造元が提供する文書をお読みください。起動がうまく行かない場合は、お使いのファームウェアで CSM (Compatibility Support Module) を有効に 設定することも試してみてください。#

1.2.1 SLP を利用したネットワークサーバからのインストール

ネットワークが OpenSLP に対応するように構築されていて、かつお使いのネットワーク インストール元が自分自身を SLP でアナウンスするよう設定している場合 (2.2項「インストール元のデータを保存するサーバの構築」(48 ページ) にて説明しています) は、システム起動後の起動画面で F4 を押し、表示されるメニューから *SLP* を選択してください。

インストールプログラムは DHCP を利用してネットワーク接続の自動設定を行ない、OpenSLP サーバからネットワーク上のインストール元に関する情報を取得します。DHCP による自動ネットワーク設定がうまくいかない場合は、それぞれ適切なパラメータを手動で指定する必要があります。その後インストール処理は本書で書かれているとおりに進みます。ただし追加のリポジトリを設定するのに必要となるネットワーク設定については行ないません。この作業は既にインストール開始時点で実施済みであり、不要であるためです。

1.2.2 SLP を利用しないネットワークソースからのインストール

お使いのネットワーク環境が、インストール元に関する情報を得るための OpenSLP に対応していない場合は、システム起動後の起動画面で F4 を押し、表示されるメニューから適切なネットワークプロトコル (NFS, HTTP, FTP, SMB/CIFS) を選択してください。また、サーバのアドレスとインストールメディアへのパスも指定する必要があります。

インストールプログラムは DHCP を利用してネットワーク接続の自動設定を行ないます。自動設定がうまくいかない場合は、それぞれ適切なパラメータを手動で指定する必要があります。その後、インストール処理は指定した箇所からインストールデータを取得します。あとのインストール処理は本書で書かれているとおりに進みます。ただし、追加のリポジトリを設定するのに必要となるネットワーク設定については行ないません。この作業は既にインストール開始時点で実施済みであり、不要であるためです。

1.2.3 Windows からの openSUSE 12.2 インストーラを利用したインストール

openSUSE 12.2 インストーラは、BIOS の設定を行なうことなく直接お使いのコンピュータから openSUSE のインストール処理を起動できるよう、準備作業を行なう Microsoft Windows アプリケーションです。DVD メディアからのみご利用いただけます。インストーラを利用するには、Windows 環境下で openSUSE のメディアを挿入してください。openSUSE 12.2 インストーラが自動的に起動します (起動しない場合は、DVD を開いて openSUSE11_2_LOCAL.exe を起動してください)。あとはインストール時に使用する言語を選択して、画面に表示されたそれぞれの指示に従ってください。ここで選択する言語は、openSUSE のインストールで使用する言語にもなります。

準備作業ののち、再起動を行なうことで Microsoft Windows のブートローダが起動します。インストール作業を行なうには、*openSUSE 12.2 Installer*を選択してください。インストールを続けるにはインストール メディアを挿入する必要がありますことに注意してください。インストールは下記に示す 手順のとおりに進行します。その後 Microsoft Windows に戻ると、openSUSE 12.2 Installer は自動的に アンインストールされます。

ヒント: Microsoft Windows と openSUSE の共存

openSUSE と Microsoft Windows は簡単に共存させることができます。下記に示すインストール手順のとおりに行ってください—これにより、既存の Windows インストールを自動的に検出し、それぞれを選択して起動するためのオプション設定が施されるようになっています。Windows がインストール先のハードディスク全体を占有しているような場合にも、インストール処理は openSUSE をインストールするため、既存の Windows パーティションを 縮小するための変更提案を行なうようになっています。インストール作業を行なう前に、1.10.1.1 項「Windows パーティションのサイズ変更」(20 ページ) に書かれた詳細をお読みください。

1.3 インストール手順

openSUSE のインストールは、大きく分けて「準備」「インストール」「設定」の 3 つのパートに分かれています。「準備」の段階では言語や時刻、デスクトップ種類やユーザ、パスワード、ハードディスクの設定とインストール範囲をそれぞれ設定します。その後、対話 処理の必要がない「インストール」の段階に移行し、ソフトウェアをインストールして初回の起動のための準備までを行ないます。「インストール」の段階が終了すると、マシンは新しくインストールした環境に 移行するため、再起動を行ないます。あとは最終的なシステム設定を行なうための「設定」段階になります。「設定」の段階では 完全自動モードで設定するか、もしくは手動設定モードで行なうのかを選択することができます。また、ネットワークとインターネット接続のほか、プリンタなどのハードウェアコンポーネントについての設定を行ないます。

1.4 インストール向けのシステムスタートアップ

openSUSE は openSUSE の CD や DVD のようなローカルインストール 元からインストールすることができるほか、FTP, HTTP, NFS, SMB サーバのよう なネット

ワークインストールを行なうこともできます。いずれの場合とも、インストール作業時にはそれらのインストール元に物理的にアクセスする必要があるだけでなく、キー入力などが必要になります。インストールの手順はインストール元に関わらず同じような流れですが、例外についてはそれぞれ以降の説明で強調して表示しています。

1.5 起動画面

起動画面では、インストール処理に関するいくつかのオプション設定を行ないます。起動当初はメッセージが英語表示になっていますので、まずは F2 を押して言語の一覧の表示させ、カーソルキーで日本語を選んで Enter を押してください。また、既定ではハードディスクから起動 (Boot from Hard Disk) が選択されていて、このまま放っておくとインストール済みのシステムが起動するようになっていきます。これは、インストール作業後にしばしば CD を入れたままにしてしまう場合を想定した作りになっています。インストール作業を行なうには、カーソルキーを利用して上記以外のオプションを選択し、キーを押してください。それぞれの項目の意味は下記のとおりです：

インストール

通常のインストール作業を行ないます。全てのハードウェア機能が有効になるよう設定されます。このインストールがうまく行かない場合は、F5 カーネル (12 ページ) にある起動オプションをお読みのうえ、潜在的な問題を抱えているハードウェアを無効に設定してください。

レスキューシステム

グラフィカルユーザインターフェイスを持たない最小限の Linux システムを起動します。詳しくは 項「レスキューシステムの使用」(付録A ヘルプとトラブルシューティング, ↑ スタートアップ) をお読みください。このオプションは、ライブ CD をご利用の場合には選択できません。

インストールメディアのチェック

このオプションは、ダウンロードした ISO ファイルをメディアに書き込んで起動している場合にのみ、表示される項目です。この場合、インストールメディアの正当性を確認しておく必要があるためです。このオプションを選択すると、インストール作業の前にメディアが正しく読み取れるかどうかをチェックします。チェックが正しく終了すると、通常のインストール処理が始まります。チェックがうまくいかなかった場合は、インストール処理を中止します。

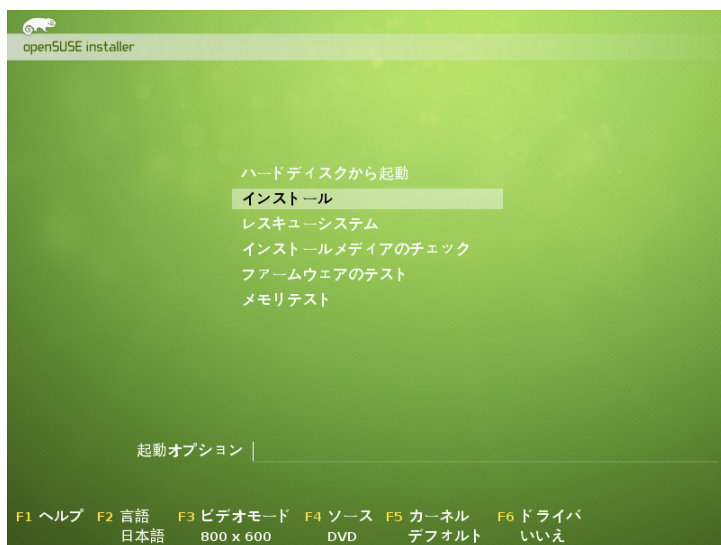
ファームウェアテスト

お使いの BIOS 内に存在する ACPI などの構成が正しいかどうかを検証するため、BIOS チェッカーを起動します。このオプションは、ライブ CD をご利用の場合には 選択できません。

メモリテスト

繰り返しメモリ内を読み書きすることで、お使いのシステムにある RAM をテストします。テストを終了すると、システムを再起動するようになっています。詳しくは 項「起動に失敗する問題」(付録A ヘルプとトラブルシューティング, ↑ スタートアップ)をお読みください。このオプションは、ライブ CD をご利用の場合には選択できません。

図 1.1 起動画面 (日本語選択後)



言語や画面の解像度、インストール元の指定やハードウェア製造元のドライバを追加するには、それぞれ画面の下部に示されたファンクションキーを押してください:

F1 ヘルプ

起動画面での各要素に対応した、状況依存のヘルプ画面を表示します。カーソルキーを利用して閲覧することができます。リンクをたどるには キーを、ヘルプ画面を終了するには キーをそれぞれ押してください。

F2 言語

インストール時に使用する言語と、関連するキーボードレイアウトを選択します。既定の言語は英語 (English) (US) になっています。

F3 ビデオモード

インストール時に使用する画面のディスプレイ解像度を選択します。どの解像度を選択してもうまく表示できない場合は、**テキストモード** を選択してください。

F4 ソース

何も指定しない場合、インストールは挿入されたインストールメディアからインストールを行ないます。ここでは FTP や NFS サーバなど、他のインストール元を選択することができます。インストールを SLP サーバが稼働しているネットワーク上で行なう場合は、そのサーバで対応しているインストール方法を選択してください。SLP については、第12章 ネットワーク内の SLP サービス (267 ページ) をお読みください。

F5 カーネル

通常のインストール方法でうまく起動できない場合は、このメニューを利用して潜在的な問題を抱えたハードウェアを無効化することができます。たとえば お使いのハードウェアが ACPI (advanced configuration and power interface) 対応していない場合は、ACPI を無効化するため **ACPI なし** を選択してください。また、**ローカル APIC なし** を選択すると、ハードウェアによっては問題となる APIC (Advanced Programmable Interrupt Controllers) を無効化することができます。**安全設定** を選択すると、CD/DVD-ROM ドライブ向けの DMA モード設定が無効化されるほか、電源管理機能も無効になります。

どれを選択したらよいのかわからない場合は、まずは **インストーラー-ACPI なし** または **インストーラー-安全設定** のオプションを試してみてください。Linux に詳しい方の場合は、コマンドライン (**起動オプション**) やカーネルパラメータを指定することもできます。

F6 ドライバ

お使いのシステムに対応した openSUSE 向けのオプションドライバをお持ちの場合に、このキーを押してください。それぞれ **ファイル** または **URL** に必要な情報を入力すると、インストールが始まる前にそれらのドライバを直接読み込みます。**はい** を選択すると、インストール 処理の最中に適切な場所に更新ディスクを挿入するよう指示されます。

F7 アーキテクチャ

32 ビットと 64 ビットの両方に対応したインストールメディアからインストールしようとしている場合で、プロセッサが 64 ビット対応のものである場合は、64 ビットと 32 ビットのどちらを利用するかを選択することができます。既定では 64 ビット対応のコンピュータでは 64 ビットのシステムをインストールしようとし、32 ビットのシステムをインストールしたい場合は、F7 キーを押して 32 ビットを選択してください。

ヒント: インストール時の IPv6 の使用について

既定では、インストール時にはお使いのマシンに IPv4 ネットワークアドレスのみを割り当てることができます。インストール時に IPv6 を利用したい場合は、起動オプションにそれぞれ下記のパラメータを入力してください: `ipv6=1` (IPv4 と IPv6 の両方を利用する場合) または `ipv6only=1` (IPv6 のみを利用する場合)

インストール処理が始まると、openSUSE はインストール処理を続けていくために必要な、最小限の Linux システムを読み込んで設定します。この設定処理で出力される起動メッセージやコピーライトメッセージを閲覧するには、Esc キーを押してください。処理が完了すると YaST のインストールプログラムが起動して、グラフィカルなインストーラが動きだします。

ヒント: マウス無しでのインストール

インストーラがマウスを検出できなかったような場合は、キーボードでの操作も行うことができます。Tab キーで項目間の移動を、カーソルキーでスクロールを、Enter キーで項目の選択をそれぞれ行うことができます。また、ボタンや選択項目には下線で示された文字が書いてある場合があります。これらの項目は、Alt + 下線で示された文字を押すことで、Tab キーを使用せずにボタンや選択項目を直接選択することができます。

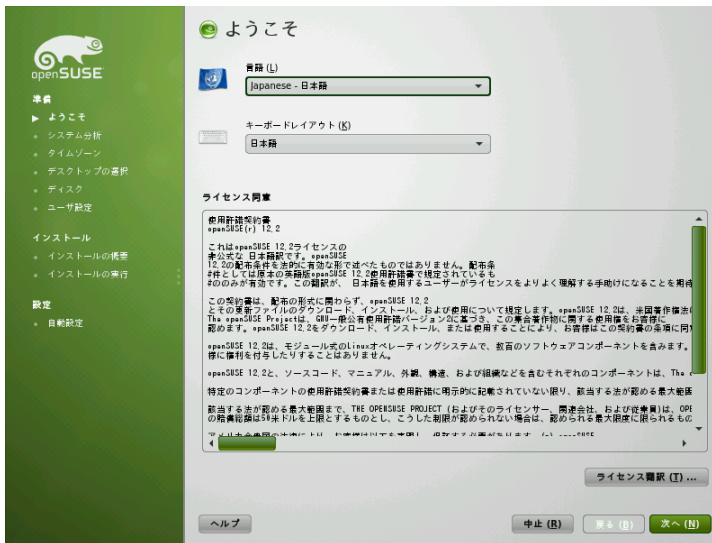
1.6 ようこそ

openSUSE のインストールは、まず言語を選択するところから始まります。言語を選択することで、キーボードレイアウトも自動的に選択されるようになっていきます。自動選択されたものではなく、他のキーボードレイアウトに変更したい場合も、ドロップダウンメニューから行うことができます。また、ここで選択された言語はタイムゾーンの既定値としても使用されます。この設定 (お使いのシステムにインストール

する第二言語についても) は、インストール概要 の画面 (1.12項「インストール設定」(26 ページ)) で修正することもできます。インストール済みのシステムにおける言語設定については、第11章 YaST を利用した言語と国の設定変更 (↑スタートアップ) をお読みください。

言語とキーボードの選択の下には、ライセンス同意が表示されています。各言語への翻訳については、ライセンス翻訳... から 選択してください。ライセンスに同意する場合は、次へ を押してインストールを 継続してください。ライセンスに同意できない場合は、中止 を押してインストールを 中止してください。

図 1.2 ようこそ



1.7 インストールモード

システムの分析 (YaST が記憶デバイスを検出し、お使いのシステムに他の システムがインストールされているかどうかを確認する処理) が完了すると、利用可能なインストールモードが表示されます。ライブ CD からインストールしようとしている場合、インストールモードは表示されません。これは、ライブ CD が自動設定付きの新規インストールにしか対応していないためです。

新規インストール

新しくインストールを行ないたい場合を選択します。

既存のシステムの更新

既存のインストールを新しいバージョンに移行したい場合に選択します。システム更新について、詳しくは 第16章 システムのアップグレードとシステム変更 (↑ スタートアップ) をお読みください。

図 1.3 インストールモード



既定では、新規インストールの場合には自動設定が有効になっています。このモードを選択すると、お使いのハードウェアやネットワークを自動的に設定するようになりますので、入力項目を最小限に抑えることができます。必要であればインストール後に YaST を利用して後から設定を修正することもできます。インストール時に手動で設定したい場合は、*自動設定を利用する* のチェックを外してください。

インストール時にアドオン製品を追加したい場合は、*別途のメディアで提供されるアドオン製品をインストールする* のチェックを入れてください。アドオン製品にはシステムの拡張のほか、お使いのシステム向けのサードパーティ製品やドライバ、追加ソフトウェア や追加言語のサポート などがあります。

次へ を押すと次に進みます。アドオン製品をインストールするよう選択した場合は、1.7.1項「アドオン製品」(15 ページ) に進んでください。そうでない場合は、1.8項「時刻とタイムゾーン」(17 ページ) に進んでください。

1.7.1 アドオン製品

アドオン製品はローカルのインストール元 (CD, DVD, ディレクトリ) や ネットワークのインストール元 (HTTP, FTP, NFS, CIFS など) からインストール することができます。ネットワークからインストールする場合は、この段階で ネットワーク設定をしておく必要があります (ネットワークインストールを行なっている場合は、既存の設定を使用するため不要です)。はい、ネットワークの設定を行ないます を選択し、1.7.1.1項「ネットワーク設定」(16 ページ) に書かれた手順で設定を行なってください。アドオン製品がローカルに存在する場合は、いいえ、ネットワークの設定を飛ばします を選択してください。

次へ を押すと製品のインストール元を指定することができます。利用可能なインストール元として、*CD, DVD, ハードディスク, USB マスストレージ, ローカルディレクトリ, ローカル ISO イメージ Image* を選択することができます (ネットワークが設定されていない場合)。リムーバブルメディア上にアドオン製品が存在する場合は、システム側で自動的に マウント処理を行ない、内容を読み込みます。アドオン製品がハードディスク上に存在 する場合は、ハードディスク を選択してマウントされていない ハードディスクからインストールするか、ローカルディレクトリや ローカル ISO イメージ を選択し、ファイルシステムからの インストールを行なってください。また、アドオン製品はリポジトリとして配布される 場合や、RPM ファイルの集合として配布される場合もあります。後者の場合は、*RPM パッケージだけのディレクトリ* を選択してください。ネットワークが利用できる場合は、HTTP, SLP, FTP などのネットワーク上の インストール元を選択できるほか、URL を直接記述することもできます。

この時点でリポジトリの説明ファイルをダウンロードするには、*リポジトリの説明をダウンロード* を選択してください。選択しない場合は、インストールをはじめる際にダウンロードを行ないます。次へ を押すと必要に応じて CD や DVD の挿入を求められます。また、製品の内容によっては、追加のライセンス同意が表示される場合があります。

アドオン製品は後から設定することもできます。インストール済みのシステムで アドオン製品を利用するには、第8章 *アドオン製品のインストール (↑ スタートアップ)* をお読みください。

1.7.1.1 ネットワーク設定

ネットワーク設定を起動すると、YaST は利用可能なネットワークカードを 検出しようとし、複数のネットワークカードが見つかった場合は一覧が 表示され、どのカードを設定するのかを選択することになります。

ネットワークアダプタのケーブルが接続されていない場合は、警告メッセージ が表示されます。正しくネットワークケーブルが接続されていることを確認し、はい、利用します を選択してください。また、お使いの ネットワーク環境で DHCP サーバが利

用できる場合は、*DHCP* を利用した自動アドレス設定 を選択してください。ネットワークを手動で設定するには、*アドレスの手動設定* を選択して *IP アドレス*, *ネットマスク*, *デフォルトゲートウェイ*, *DNS サーバ IP* をそれぞれ設定してください。

ネットワーク環境によっては、インターネットにアクセスするにあたって、プロキシサーバと呼ばれるサービスを利用しなければならない場合があります。そのような場合は、*インターネット接続にプロキシサーバを使う* を選択して、それぞれ必要な項目に記入してください。受け入れる を押すと、ネットワークの設定を行ないます。あとはアドオン製品やリポジトリの設定に進みます。以降は 1.7.1 項「アドオン製品」(15 ページ) をお読みください。

1.8 時刻とタイムゾーン

このダイアログでは、地域とタイムゾーンを設定します。両方とも開始時に 選択した言語に基づいて適切と思われる項目が事前選択されています。選択を変更するには、地図を利用して指定するか、もしくはドロップダウン リストから *地域* と *タイムゾーン* を選択します。地図を利用する場合は、まず選択する地域を大まかにマウスカーソルで選んで左ボタンを押してください。左ボタンを押すことで地図が 拡大されますので、さらに左ボタンで国や地域を選択してください。右ボタンを押すと世界地図に戻ります。

図 1.4 時刻とタイムゾーン



時刻を設定する場合は、ハードウェアの時刻は UTC に設定 を有効にするかどうか選択してください。お使いのマシンで、たとえば Microsoft Windows などの他のオペレーティングシステムを共存させているような場合、おそらくお使いのシステムはローカルタイム (UTC に設定しない) を使用するよう設定するのがよいでしょう。お使いのマシンで Linux だけを動作させるような場合は、ハードウェアの時刻を UTC に設定して、自動的に標準時から夏時間への調整を行なうよう設定するのがよいでしょう。

この時点でネットワーク設定が完了している場合、時刻は タイムサーバを利用して自動的に同期するようになっています。変更 ボタンを押して NTP の設定を変更するか、手動 を選択して手動で時刻を設定してください。NTP サービスの設定について、詳しくは第15章 *NTP を利用した時刻同期* (305 ページ) をお読みください。設定が完了したら 受け入れる を押すと 次の段階に進みます。

1.9 デスクトップの選択

openSUSE では複数のデスクトップ環境からいずれかを選択することができます。デスクトップ環境でメジャーなものとして用意しているのは、*KDE* と *GNOME* になります。いずれも Windows に似たグラフィカルな デスクトップ環境を提供しています。なお、ライブ CD からの インストールの場合は、既にライブ CD でデスクトップ環境を選択済みであるため、この選択は表示されません。

上記以外のデスクトップ環境を利用する場合は、その他 を選んでさらなるオプションを表示してください。*XFCE* デスクトップや *LXDE* デスクトップは古いハードウェアをお使いの場合に便利な、軽量・高速なデスクトップ環境です。また、最小限の *X Window* システム を選択すると、一般的なデスクトップ統合機能を持たない単独の *X* アプリケーションや、端末ウインドウを表示するためのグラフィカルなウインドウマネージャが インストールされます。最小限のサーバ (テキストモード) を選択すると、コンソール端末のみが利用できるようになります。

図 1.5 デスクトップの選択



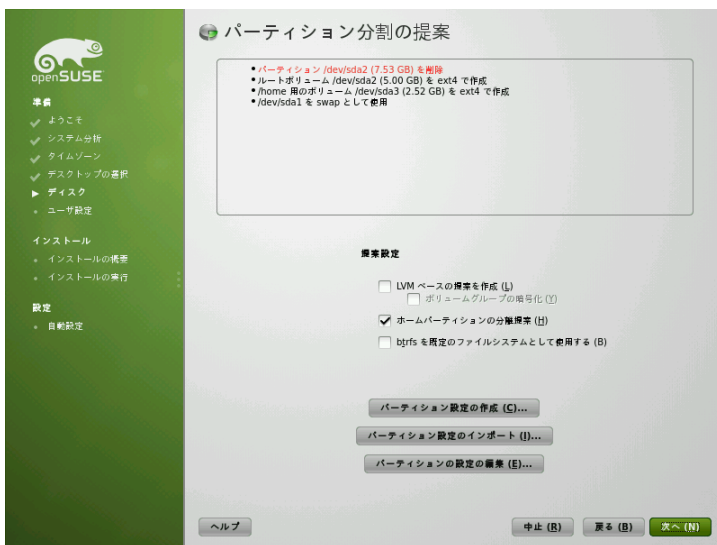
1.10 パーティション設定の提案

この段階では、openSUSE のパーティション設定を行ないます。多くの場合、変更する必要のない適切な設定値が提示されるようになっていきます。インストール 先に選択したディスクに Windows の FAT または NTFS のパーティションしか 存在しない場合、YaST はこれらのパーティションを縮小するよう提案が行なわれます。そのまま 次へ を押すとその提案を受け入れたこと になります。知識のあるユーザであれば、提案内容を修正したり、独自の パーティション設定を作成したりすることができます。

既定では、パーティション設定の提案は パーティションベース で行なわれます。LVM ベース の設定を行ないたい場合は、その旨指定を行なって提案を自動変換してください。LVM (Logical Volume Manager) について、詳しくは 3.2項「LVM の設定」(87 ページ)をお読みください。

提案された内容に対して少しだけ変更したい場合 (たとえばファイルシステムの種類 変更や、暗号化パーティションの設定場合など) は、パーティションの設定の編集を選んで必要な設定変更を行なってください。この手順については、3.1項「YaST パーティション設定の利用」(75 ページ)をお読みください。

図 1.6 パーティション設定の提案



1.10.1 特定のディスクに対するパーティション設定

お使いのマシンに 2 台以上のハードディスクが接続されている環境で、1 大のハードディスクに限ってパーティション提案を行なわせたい場合は、**パーティション設定の作成**を選んでください。その後、一覧から提案を行なうディスクを選択します。選択したハードディスクにパーティションが存在していない場合、ハードディスク全体を使用するよう提案が作成されます。そうでない場合は、既存のパーティションを利用するよう提案します。提案された状態から個別のパーティションを追加するには、**ホームパーティションの分離提案**を選択してください。また、パーティションベースの提案ではなく **LVM ベースの提案を作成** を選択することもできます。次へを 2 回押すと、次の段階に進みます。

1.10.1.1 Windows パーティションのサイズ変更

選択したハードディスクに Windows の FAT または NTFS のパーティションしか含まれていない場合、YaST はこれらのパーティションを削除するか、縮小するよう提案を行ないます。**Windows を完全に削除**を選択すると、Windows のパーティ

ションは削除するよう印が付けられ、Windows 用に使用しているパーティションを openSUSE で利用できる ようになります。

警告: Windows の削除

Windows を削除する場合は、フォーマットが始まった段階で Windows 上にあった全てのデータは修復不可能になります。

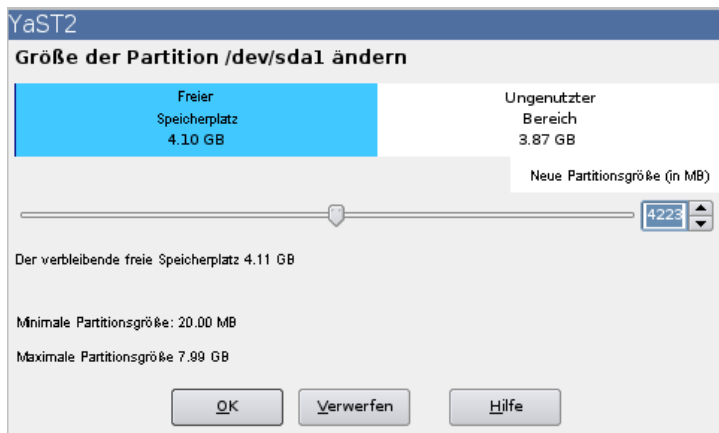
Windows パーティションを縮小するには、縮小処理を行なう前にインストールを中断し、Windows を起動してから下記の準備 作業を行なってください:

1. 仮想メモリ ファイルが有効になっている場合は、まず それらを無効に設定します。
2. スキャンディスク を実行します。
3. デフラグ を実行します。

これらの準備作業が完了したら、openSUSE のインストールを再開してください。パーティションの設定まで以前のとおり手順を進め、Windows パーティションを縮小 を選択します。パーティションに対する簡易なチェックが動作したあと、Windows パーティション を縮小するためのダイアログが開きます。

すると、Windows で占有されているディスク領域と利用可能なディスク領域が棒グラフで表示されます。提案された設定を変更するには、スライダーを動かすか、パーティションサイズの項目にサイズ設定を入力してください。

図 1.7 Windows パーティションの縮小



次へ を押してダイアログを終了すると、設定が保存されて 以前の表示に戻ります。実際のサイズ変更処理は、ハードディスクを フォーマットする前に (つまり、今すぐではなく後から) 行ないます。

重要: NTFS パーティションへの書き込み

既定では Windows は NTFS ファイルシステムを使用します。openSUSE でも NTFS ファイルシステムを読み書きする機能が備わっていますが、いくつかの機能には制限があります。具体的には暗号化されているファイルや、圧縮されたファイルの読み書きを行なうことができません。また、Windows での ファイルのアクセス権は無視されます。詳しくは <http://ja.opensuse.org/SDB:NTFS> をお読みください。

1.10.2 カスタムなパーティション設定

パーティション設定の作成 から カスタムなパーティション設定 を選択すると、独自のパーティション設定を作成することができます。熟練者向けパーティション設定 として現在のパーティション設定が表示されます。システムビューの枠内にある ハードディスク 欄の + ボタンを押して 展開してください。ハードディスクの一覧が表示されたら、その中から設定を行ないたいハードディスクを選択します。あとは 追加, 編集, サイズ変更, 削除 のボタンを押すと、それぞれの処理を行なうことができます。カスタムなパーティション設定と高度な機能について、詳しくは 3.1項「YaST パーティション設定の利用」(75 ページ)をお読みください。

1.11 新規ユーザの作成

この段階では、ローカルユーザの作成を行ないます。ローカルユーザの管理は、単独で動作するワークステーション向けの機能です。認証サーバを用いた 中央集権型の認証環境を利用する場合は、変更 ボタンを押して 1.11.1項「熟練者向けの設定」(24 ページ)以降の処理を行なってください。

まずは姓と名を入力します。すると、ユーザがログインするときに利用する ユーザ名 を独自に考慮して表示します。そのままその 名前を利用してもかまいませんし、独自で付与してもかまいません。あとはそのユーザに対するパスワードを指定してください。パスワードは 確認のため 2 度入力します (何らかの理由で入力ミスを起こさないための 機能です)。効果的なセキュリティを実現するため、パスワードは 5 ~ 8 文字の長さで指定してください。パスワードの最大の長さは 72 文字です。特殊な

セキュリティモジュールを読み込まない場合は、最初の 8 文字のみ をパスワードとして利用します。また、パスワードは半角の英数字と記号を利用することができます (大文字と小文字は区別されます)。全角文字 (漢字や全角の記号、ひらがな／カタカナ)、発音記号などは 利用できません。

パスワードについては強度のチェックが行なわれます。推測しやすいパスワード (たとえば辞書に載っている単語や名前) を入力した場合は、警告メッセージが表示されるようになっています。これは、推測しにくいパスワードを使用することがセキュリティ確保の第一歩であるためです。

重要: ユーザ名とパスワード

ここで入力するユーザ名とパスワードは、お使いのシステムにログインする際に 必要となるものです。いずれの情報とも覚えておいてください。

図 1.8 新しいユーザの作成

また、以下の 3 つのオプションもご利用いただけます:

このパスワードをシステム管理者用のものとしても使用する

この項目にチェックを入れると、ユーザに対して設定したものと同一パスワードを、システム管理者である root に設定します。このオプションは、1 人で使用するような単独動作のワークステーションや家庭内のマシンなどに 便利なオプションです。チェックを外した場合は、インストールの次の段階で システム管理

者のパスワードを尋ねられます (1.11.2項「システム管理者 root のパスワード」(25 ページ) をご覧ください)。

システムメールの受信

この項目にチェックを入れると、システムサービスが生成したメッセージを ユーザ宛に送信するようになります。通常はシステム管理者である root 宛にのみ送信します。このオプションはセキュリティ上の理由から、特別な 事情がない限り root でのログインを行なわないほうが安全であるため に用意されているもので、最もよく使用するアカウントに設定しておく と便利 です。

システムサービスから送信されるメールは、ローカルのメールボックス `/var/spool/mail/ユーザ名` に配信されます。ここで、`ユーザ名` は選択した ユーザのログイン名になります。インストールが終わると、KMail や Evolution などの電子メールクライアントからメールを読み込むことができるようになります。

自動ログイン

この項目にチェックを入れると、システムが起動したときに現在のユーザで自動的にログインするようになります。これは主に、1 人で使用する コンピュータを構築する際に便利です。

警告: 自動ログイン

自動ログインを有効にすると、システムの起動後に一切の認証無しでお使いのデスクトップが表示されるまで動いてしまいます。見ず知らずの人間でも 利用できてしまうため、お使いのシステムに機密データなどがある場合は、このオプションを有効にはなりません。

1.11.1 熟練者向けの設定

ユーザ作成のダイアログで **変更** ボタンを押すと、ネットワーク認証や以前のインストールからのユーザ取り込み (存在した場合) を設定することができます。また、このダイアログからパスワードの暗号化方法を変更することもできます。

なお、インストール済みのシステムから追加のユーザを作成したり、ユーザの 認証方法を変更したりすることもできます。ユーザ管理について詳しくは、第10章 *YaST* を利用したユーザ管理 (↑ スタートアップ) をお読みください。

既定の認証方法は `ローカル (/etc/passwd)` に設定されています。`/etc/passwd` ファイルを使用する openSUSE の以前のバージョンや他のシステムが検出される

と、ローカルユーザを取り込むことができます。取り込みを行なうには、以前のインストールからユーザデータを読み込むを押してから、選択を押してください。その後、表示されたダイアログから取り込むユーザを選択し、OKを押してください。

また、下記のネットワーク認証サービスへのアクセスを設定することができます：

LDAP

ネットワーク内に LDAP サーバが動作していて、そこでユーザを一括管理している場合に選択します。詳しくは 項「YaST を利用した LDAP クライアントの設定」(第4章 ディレクトリサービス LDAP, ↑セキュリティガイド) をお読みください。

NIS

ネットワーク内に NIS サーバが動作していて、そこでユーザを一括管理している場合に選択します。詳しくは 項「NIS クライアントの設定」(第3章 NIS の使用, ↑セキュリティガイド) をお読みください。

Windows ドメイン

SMB 認証は、Linux と Windows が混在するネットワーク環境で利用されます。詳しくは 項「Linux クライアントに対して Active Directory を設定する方法」(第5章 Active Directory への対応, ↑セキュリティガイド) をお読みください。

ユーザ管理を LDAP や NIS で行なっている場合は、Kerberos 認証を設定することもできます。この認証を設定するには、Kerberos 認証の設定を押してください。詳しくは 第6章 Kerberos を利用したネットワーク認証 (↑セキュリティガイド) をお読みください。

1.11.2 システム管理者 root のパスワード

直前の手順でこのパスワードをシステム管理者用のものとしても使用するを選択しなかった場合は、ここでシステム管理者 root のパスワード入力を求められます。選択した場合はこの手順は飛ばされます。

root とはスーパーユーザやシステム管理者とも呼ばれるユーザの名前です。通常のユーザ (特定の領域やシステム上で実行するコマンドについて、アクセス権 (制限) を設定される場合がある) とは異なり、root はシステムの設定変更やプログラムのインストール、新しいハードウェアの設定などに制限がありません。また、ユーザがパスワードを忘れてしまったり、システムを利用するにあたって何らかの問題

が発生したりした場合は、root からそれぞれ助けを与えることができます。そのため、root のアカウントはシステム管理やメンテナンス、修復に対してのみ 使用されるべきもので、普段の作業に root を利用するのは危険です: ちょっとしたミスで取り返しの付かないシステムファイルの損失などを引き 起こしてしまう可能性があるためです。

また、確認として root のパスワードは 2 回入力してください。さらに、root のパスワードは忘れずに覚えておいてください。いったん入力するとパスワードを取り出すことができないためです。

root は、システムのインストール後であればいつでも変更することができます。YaST を起動して *セキュリティと ユーザ > ユーザとグループの管理* を選択してください。

警告: root ユーザ

root には、システムを変更するための全ての権利が与えられています。そのため、システム変更の作業を、見ず知らずの利用者に行なわせないように する目的で、root パスワードを設定します。このパスワード無しでは、管理作業を行なうことができないようになります。

1.12 インストール設定

実際のインストールが始まる前の最後の段階として、YaST が提案した インストール設定を修正したり、それまでに設定した内容を確認したりすることができます。それぞれの項目を修正するには *変更* を押して変更したい項目を選択するか、もしくはヘッドラインを選択してください。表示されたダイアログで設定を変更すると、変更した内容が反映 された形でインストール概要の画面に戻ってくることができます。

図 1.9 インストール設定



ヒント: 既定値へのリセット

変更 > 既定値に戻す を押すと、全ての変更内容を取り消してリセットすることができます。YaST は元の提案内容を表示します。

1.12.1 パーティション設定

パーティション設定を再度確認し、必要であれば 以前に指定した 設定を修正してください。パーティション設定の変更は、3.1項「YaST パーティション設定の利用」(75 ページ) Partitioning で書かれている熟練者モードで行ないます。

1.12.2 起動

YaST はお使いのシステムにおける起動設定を提案しています。お使いの コンピュータに、Microsoft Windows や他の Linux システムなどの他の システムがインストールされている場合は、自動的にそれらを検出してブート ロードの設定に加えられます。ただし、起動時に何も操作しなければ openSUSE が起動する設定になります。特に問題がなければ、何も変更する必要はありません。何か変更を行

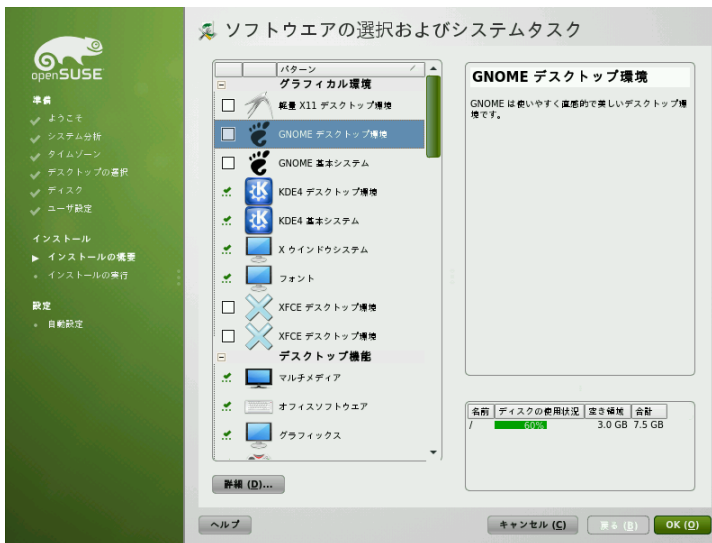
ないたい場合は、提案内容を修正してください。詳しくは 7.2項「YaST を利用したブートローダの設定」(141 ページ) をお読みください。起動方法の変更は、知識のある ユーザ向けの機能です。

1.12.3 ソフトウェア

openSUSE には、様々な用途に応じて多くのソフトウェアパターンが用意されています。パターンの選択や、要件に応じたインストール対象の修正を行なうには、ソフトウェアを選択してください。一覧からパターンを選択することができるほか、各パターンの説明がウインドウの右側に表示されます。それぞれのパターンには、それぞれの機能に応じて複数のソフトウェアパッケージが含まれます (たとえば マルチメディアやオフィスソフトウェアなど)。ソフトウェア パッケージ単位での詳細な選択を行なうには、**詳細** ボタンを押して YaST ソフトウェアマネージャを起動してください。

YaST ソフトウェアマネージャを利用することで、インストール終了後でも お使いのシステムに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削除したりすることができます。詳しくは 第5章 ソフトウェアのインストールと削除 (↑ スタートアップ) をお読みください。

図 1.10 ソフトウェアの選択およびシステムタスク



1.12.4 ロケール設定

ここでは、インストールの最初の段階で設定した、システムの *言語* と *キーボードレイアウト* を変更することができます。また、追加の *言語* を設定することもできます。システムの言語設定を修正するには、*言語* を選択し、一覧から言語を選んでください。第一言語で指定したものがシステムの言語になります。また、現在の設定 から修正したい場合は、第一言語向けのキーボードレイアウトとタイムゾーンを指定することもできます。また、*詳細* を押すと *root* の言語を設定することができるほか、UTF-8 のサポートや詳しい言語指定 (たとえば南アフリカ英語など) を行なうことができます。

第二言語は、切り替え時に追加のパッケージをインストールすることなく 利用できるようにする言語を指定します。詳しくは 第11章 *YaST を利用した言語と国の設定変更* (↑ スタートアップ) をお読みください。

キーボードレイアウトを変更するには、*キーボードレイアウト* を選択してください。既定ではインストール時に選択した言語に あわせて自動的に選択が行なわれます。キーボードレイアウトは、一覧から 選択してください。ダイアログの下部にある *テストフィールド* では、キーボードレイアウトが正しく反映されたかどうかを試す 目的でキー入力を行なうことができます。より細かい設定については、*熟練者向け設定* を押してください。終了したら最後に *受け入れる* を押すとインストール概要に戻ります。

1.12.5 タイムゾーン

ここではタイムゾーンと時刻に関する設定を行ないます。ネットワークが 設定されている場合は、NTP (Network Time Protocol) クライアントを設定 してタイムサーバと時刻同期を行なうよう設定することもできます。ここでの 設定は 1.8項「時刻とタイムゾーン」(17 ページ) で行なったものと同じもの です。

1.12.6 ユーザ設定

ここでは現在の *ユーザ* 設定を変更したり、*root* のパスワードを変更したりすることができます。ここでの設定は 1.11項「新規ユーザの作成」(22 ページ) で行なったものと同じです。

1.12.7 既定のランレベル

openSUSE は様々なランレベルで起動することができます。通常は この項目を修正する必要はありませんが、必要であれば、このダイアログから 既定のランレベルを変更することができます。

1.12.8 システム

このダイアログでは、YaST が収集した全てのコンピュータ情報が表示されます。この項目を選択すると、ハードウェアの検出ルーチンが起動します。お使いのシステム環境に依存しますが、しばらく時間がかかります。それぞれの項目について詳細を確認するには、一覧から選択して *詳細* ボタンを押してください。*ファイルに保存* を選択すると、ローカルのファイルシステムやフロッピーディスクに詳細情報を保存することができます。また、*カーネル設定* を選択すると、PCI ID の設定変更やカーネル設定など、より細かい設定を行なうことができます。

1.12.9 イメージからのインストール

イメージからインストールを行ないと、インストール作業を短時間で素早く行なうことができます。イメージには、選択したソフトウェアパターンに該当するインストール済みシステムの圧縮スナップショットが入っています。イメージに含まれていないパッケージは、イメージの展開後に個別にインストールを行ないます。

ご希望のソフトウェアの選択に該当するイメージが存在しなかった場合を除いて、この機能は既定で *有効* になっています。何か問題が発生した場合は、デバッグ目的で *無効* に設定することもできます。

注記: インストール時のタイムスタンプについて

RPM データベースでは、パッケージをインストールした日時や最後に更新した日時を記録しています (たとえば `rpm -qa --last` などで表示することができます)。イメージからインストールした場合、全てのパッケージのインストール日時はイメージ内に記録されている日時になるため、実際のインストール日時とは異なることになります。

1.12.10 ファイアウォール

既定では、SuSEFirewall2 が全ての設定済みネットワークインターフェイスで有効になっています。このコンピュータ全体でファイアウォール機能を無効化したい場合は、**無効**を選んでください。ファイアウォール 機能を有効に設定したまま SSH (セキュアシェル) によるログインを許可したい 場合は、SSH ポートを **開く** こともできます。

1.13 インストールの実行

全てのインストール設定を終えたら、最後に **インストール** ボタンを押すとインストール作業が始まります。ソフトウェアによっては ライセンス同意が必要なものがありますが、このような場合はそれぞれ ライセンス確認メッセージが表示されます。それぞれ **同意します** を押してソフトウェアパッケージをインストール してください。ライセンスに同意できない場合は **同意しません** を選択すると、それらのソフトウェアパッケージはインストールされなくなります。再度 **インストール** ボタンを押して確認してください。

インストール作業は、システムの性能や選択したソフトウェア範囲によっても異なりますが、一般的に 15 分から 30 分程度かかります。ハードディスクの 準備を行なったのち、ユーザ設定の保存や復元が行なわれ、インストールイメージの配置を行なったからソフトウェアのインストール が始まります。この処理の間、openSUSE に関する様々なことを 紹介するスライドショーが表示されます。**詳細** ボタンを押すとインストールの流れが表示され るほか、**リリースノート** を押すと、マニュアルに書ききれなかった 最新の重要情報を読むことができます。

注記: リリースノート

この段階では、インストール CD 内に同梱されているリリースノートが 表示されます。インターネット上にはこれよりも新しいリリースノートが存在する 可能性がありますが、1.14.2.2項「ネットワーク設定」(33 ページ) に 示す手順でネットワーク設定とインターネット接続の設定を手作業で 行なっていれば、インストール終了後に最新のリリースノートが表示されます。

ソフトウェアのインストールが完了すると、システムの基本的な部分の準備が 完了します。あとは「基礎部分のインストール完了処理」で、ブートローダのインストールやフォントの初期化などの処理を行ないます。引き続き YaST は、インストールが完了した Linux システムの起動を行ない、システム設定を起動します。

ヒント: 既存の SSH ホスト鍵

既存の Linux インストールが存在する状態から openSUSE をインストールした場合は、既存の鍵の中で最も新しいアクセス時刻を持つ SSH 鍵を自動的にインポートします。

1.14 インストール済みシステムの設定

ようやくシステムのインストールが終わりましたが、まだ使い始めるための設定が終わっていません。ハードウェアやネットワーク、その他のサービスなどをここから設定します。既定のインストール手順に従ってインストールした場合、システムは自動的に設定されます。*自動設定* のチェックを外していた場合にのみ、手動によるシステム設定が起動します。

1.14.1 自動システム設定

再起動後にシステムの自動設定が始まります。この処理では、お使いのネットワークとインターネット接続、お使いのハードウェアについてそれぞれ自動設定を試みます。この処理の間は特に作業を行なう必要はありません。自動的に作成された設定は、インストール完了後に YaST を利用して、後から修正することもできます。1.15項「グラフィカルなログイン」(37 ページ) まで読み飛ばしてください。

1.14.2 手動システム設定

再起動後にシステムの手動設定が始まります。この作業中に何らかの設定が失敗するようなことがあった場合は、最後に成功した作業から再開することができます。

1.14.2.1 ホスト名とドメイン名

ホスト名とは、お使いのコンピュータに対して設定する、ネットワーク内での名前のことをいいます。ドメイン名とは、お使いのネットワークの名前です。ホスト名とドメイン名にはそれぞれ既定値が表示されます。システムがネットワークに接続されていて、ネットワーク内の全コンピュータのドメイン名が同じである場合は、ホスト名をネットワーク内で唯一のものにしなければなりません。

多くのネットワークでは、DHCP を利用して自分自身の名前を取得します。この場合は、ホスト名やドメイン名を直接変更する必要はありません。その代わりに

DHCP でホスト名を変更を選択してください。このホスト名でお使いのシステムにアクセスできるようにするには、ネットワークに接続されていない場合であってもホスト名をループバック IP に割り当てるを選択してください。なお、ネットワークサービスを実行しているようなマシンの場合は、チェックを付けないでください。また、デスクトップ環境を再起動することなくネットワーク接続を変更するような使い方をする場合（たとえば異なる無線 LAN ネットワーク間を移動する場合など）は、このオプションを有効にしないでください。/etc/hosts が変更されると、デスクトップシステムに混乱を来すためです。

ホスト名の設定はインストール後に変更することもできます。YaST から ネットワークデバイス > ネットワークの設定を選んでください。詳しくは 11.4.1 項「YaST を利用したネットワークカードの設定」（223 ページ）をお読みください。

1.14.2.2 ネットワーク設定

ラップトップコンピュータに openSUSE をインストールしている場合は、*NetworkManager* でインターフェイスをコントロールする が選択 されています。NetworkManager とは、最小限のユーザ操作で自動的なネットワーク接続を行なうことのできるツールで、主に無線 LAN やモバイル環境に適しています。NetworkManager を使用しない従来の方法を使用したい場合は、*NetworkManager* の無効化 を選択してください。NetworkManager に関する詳しい情報は、第23章 *NetworkManager* の使用（435 ページ）をお読みください。その他の種類の マシンに openSUSE をインストールしている場合は、既定で NetworkManager を使用 しない従来の方法が選択されます。この設定方法では、お使いのシステムでの ネットワークデバイス設定や、ファイアウォール／プロキシなどの セキュリティ関連の設定を行なうことができます。

ネットワークの設定は、システムのインストール作業が終わった後からでも 変更することができます。また、ネットワークの設定を行わずに飛ばすと オフライン状態となり、利用可能な更新を受信できなくなります。後から ネットワーク接続を設定するには、設定をせずに飛ばすを選んでから 次へ を押してください。

この段階では、下記のネットワーク設定を行なうことができます：

一般的なネットワーク設定

前述の通り、まずは NetworkManager を有効にするか無効にするかを選択してください。IPv6 サポートもここで選択できます。既定では IPv6 のサポートは有効に設定されています。無効に設定するには、IPv6 を無効にする を選択してください。IPv6 について、詳しくは 11.2 項「IPv6 一次世代のインターネット」（211 ページ）をお読みください。

ファイアウォール

既定では、SuSEFirewall2 が全ての設定済みネットワークインターフェイスで有効になっています。このコンピュータ全体でファイアウォール機能を無効化したい場合は、*無効*を選んでください。ファイアウォール 機能を有効に設定したまま SSH (セキュアシェル) によるログインを許可したい 場合は、SSH ポートを *開く* こともできます。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* を押してください。詳しくは 項「YaST を利用したファイアウォールの設定」(第13章 マスカレードとファイアウォール, ↑セキュリティガイド) をお読みください。

ネットワークインターフェイス

YaST で検出された全てのネットワークカードが一覧表示されます。インストール時に既にネットワーク設定を行なっている場合 (1.7.1.1項「ネットワーク設定」(16 ページ) に書かれています) は、その設定を行なったインターフェイスは *設定済み* として表示されます。ネットワークインターフェイス を押すと、*ネットワーク設定* ダイアログが開き、既存の設定を変更したり未設定のネットワークカードを設定したり、追加のカードを設定したりすることができます。

DSL 接続, ISDN アダプタ, モデム

お使いのコンピュータに内蔵の DSL モデムや ADSL Fritz カード、ISDN カード、モデムが接続されている場合は、それぞれ対応するヘッドライン を押すことで設定ダイアログを開くことができます。

VNC リモート管理

お使いのマシンに対して、遠隔から VNC を利用してリモート管理を行ないたい場合は、*VNC リモート管理* を押してください。開いたダイアログで *リモート管理を許可する* を選択することができます。ファイアウォールの設定についてもあわせて 変更することができます。

プロキシ

お使いのネットワークからインターネットに接続するにあたって、プロキシ サーバと呼ばれるサービスを利用する必要がある場合があります。このような 場合は、このダイアログからプロキシ URL と認証設定をそれぞれ行なってください。

ヒント: ネットワーク設定の既定値へのリセット

ネットワーク設定を提案された設定値に戻すこともできます。設定を元に戻すには、*変更 > 既定値に戻す* を選択してください。これにより変更点を取り消して元の状態に戻すことができます。

インターネット接続のテスト

ネットワークの設定が完了したら、接続をテストすることができます。接続テストで YaST は openSUSE のサーバに接続を行ない、最新のリリースノートダウンロードします。ダウンロードしたリリース ノートは、インストール完了後に読むことができます。既定のリポジトリ やオンラインでの更新を行なう場合は、このテストを成功させる必要が あります。

複数のネットワークインターフェイスを使用している場合は、インターネットに接続しているデバイスが正しいかどうか確認してください。違っていた場合は、**デバイスの変更** を押して 変更を行なってください。

テストを開始するには、**はい、インターネットとの接続を テストします** を選択して **次へ** を 押してください。次のダイアログでテストの進捗と結果が表示されます。テスト処理の詳細については、**ログの表示** を 押すと表示することができます。テストが失敗した場合は、**戻る** を押してネットワーク設定に戻り、設定を 正しいものに修正してください。

テストが完了したら **次へ** を押してさらに手順を 進めてください。テストが成功した場合は、openSUSE の公式 ソフトウェアリポジトリと、更新リポジトリがそれぞれ設定されます。それぞれリポジトリデータのダウンロードを行ないますので、しばらく の 時間がかかります。

この段階で接続テストを行ないたくない場合は、**いいえ、テストをスキップします** を 選んで **次へ** を押してください。テストを行なわない場合 は、リリースノートのダウンロードと オンライン更新の設定も それぞれ行なわなくなります。これらの作業は、システムを準備したあとで あればいつでも実施することができます。

1.14.2.3 オンライン更新

インターネット接続の設定を行なってインターネットに接続した結果、利用可能な更新が存在した場合は、YaST オンライン更新を利用するか どうかを選択することができます。サーバ上に修正パッケージが存在すれば、既知のバグやセキュリティ問題を修正するため、これらをダウンロードして インストールします。詳しい手順については 第6章 *YaST オンライン更新* (↑ スタートアップ) をお読みください。また、インストール後のシステムでのオンライン更新手順については、項「更新によるシステム維持」(第5章 *ソフトウェアのインストールと削除*, ↑ スタートアップ) や 第6章 *YaST オンライン更新* (↑ スタートアップ) をご覧ください。利用可能な更新が存在していない場合や、インターネット 接続が確立していない場合は、本手順は表示されません。なお、セキュリティ 問題の修正や、お使いのインストール環境で推奨される修正については、自動的に選択されます。**了解** を押すとこれらの インストールを行ない、その後 **次へ** を押すと 次のシステム設定に進みます。

重要: ソフトウェア更新のダウンロード

更新のダウンロードには、インターネット接続の速度や更新ファイルのサイズによりますが、しばらくの時間がかかります。また、修正システムそれ自身が更新された場合は、オンライン更新は起動し直され、さらなる修正をダウンロードする動作になります。カーネルが更新された場合は、設定が完了する前にシステムを再起動します。

1.14.2.4 新規ローカルユーザ

最初のステップでユーザを作成しなかった場合は、このダイアログから作成することができます。さらなるユーザの作成やグループの管理、新規ユーザに対する既定値の変更やネットワーク認証については、*ユーザ管理* を起動してください。また、ユーザ管理について詳しくは、第10章 *YaST を利用したユーザ管理* (↑ スタートアップ) をお読みください。この手順を行わずに飛ばすには、何も入力せずに次へを押してください。

1.14.2.5 リリースノート

ユーザ認証の設定が完了すると、YaST はリリースノートを表示します。このリリースノートにはマニュアルを印刷した段階では書くことができなかった最新の情報が掲載されているため、読んでおくことをお勧めします。インターネット接続のテストが成功している場合は、openSUSE のサーバからダウンロードした最も新しい版のリリースノートが表示されます。インストール後にリリースノートを読むには、YaST を起動して *その他* から *リリースノート* を選択するか、SUSE ヘルプセンターを起動してください。

1.14.2.6 ハードウェア設定

インストールが終了すると、YaST は *グラフィックカード* や *プリンタ* を設定するためのダイアログが表示されます。各ハードウェア設定を開始するには、それぞれ個別のコンポーネント欄を押してください。多くの場合、YaST は自動的にデバイスを検出して設定することができます。

周辺機器の設定については、この時点で設定せずに後から設定することもできます。後から設定する方法については第13章 *YaST を利用したハードウェアコンポーネントの設定* (↑ スタートアップ) をお読みください。この時点での設定を飛ばすには、*設定をせずに飛ばす* を選んで次へを押してください。

ヒント: ハードウェア設定の既定値へのリセット

ハードウェア設定を提案された設定値に戻すこともできます。設定を元に戻すには、**変更 > 既定値に戻す** を選択してください。これにより変更点を取り消して元の状態に戻すことができます。

1.14.2.7 インストール完了

インストール作業が全て完了すると、YaST はインストール完了を知らせるダイアログを表示します。このダイアログでは、AutoYaST を利用して インストールしたシステムを複製するかどうかを選択することができます。システムを複製するには、**このシステムを AutoYaST 用に複製 する** を選択してください。現在のシステム向けのプロファイルが `/root/autoyast.xml` ファイルに保存されます。

AutoYaST は、ユーザの入力無しに複数の openSUSE システムをインストールするための仕組みです。AutoYaST のインストールは、インストールやその後の 設定について、コントロールファイルを利用して判断します。openSUSE のインストールを完了するには、**完了** ボタンを押してください。

1.15 グラフィカルなログイン

openSUSE のインストールと設定は、ようやくここで全て完了となります。自動ログイン機能やランレベルのカスタマイズなどを行なっていないければ、システムにログインするためのユーザ名とパスワードを尋ねるためのグラフィカル なログイン画面が表示されているはずです。自動ログイン機能を有効に設定 している場合は、デスクトップが表示されるころまで進みます。

KDE や GNOME デスクトップ環境に関する簡単な説明は、それぞれ 第3章 *GNOME クイックスタート* (↑ スタートアップ) と 第2章 *KDE クイックスタート* (↑ スタートアップ) を お読みください。これらのマニュアルはいずれも KDE や GNOME の ヘルプ 機能からアクセスすることができます。

リモートインストール

openSUSE® は異なる複数の方法でインストールすることができます。第1章 *YaST* を利用したインストール (3 ページ) で記述されている方法のほか、openSUSE をネットワーク経由でインストールしたり、全く手を触れることなくインストールしたりすることもできます。

それぞれの方法は 2 つの簡単なチェックを行なうところから始まります: 1 つめはその方法を利用するにあたっての前提条件を確認すること、2 つめは基本的な流れを確認することです。詳しい手順は、それぞれのインストール方法を決定することで決まります。

注記

下記の章では、これから openSUSE をインストールしようとしているシステム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。また、*リポジトリ* (以前は「インストールソース」と呼んでいました) は、インストール作業に必要な全てのデータがある場所のことを指します。たとえば物理メディアである CD や DVD のほか、お使いの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などもリポジトリと呼びます。

2.1 リモートインストールの手順

この章では、リモートインストールを行なうにあたって一般的なインストール 手順を示しています。それぞれの手順を利用する場合は、前提条件の一覧と 手順の概要をよくお読みください。それぞれの段階でより詳しい説明が必要となる場合は、それぞれ提供される参照先をお読みください。

重要

X Window System の設定は、リモートのインストール処理では実施することができません。インストール後にシステムに root でログインし、telinit 3 を実行してから 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。

2.1.1 VNC を利用したシンプルなりモートインストール (固定のネットワーク設定)

この種類のインストールでは、ターゲットシステムを起動してインストールの準備を行なうため、ターゲットシステムへの物理的な (ネットワークなどの 遠隔手段に頼らない) アクセスと、ターゲットシステムに対して設定する IP アドレスが必要です。インストールプログラムが起動した後、遠隔のワークステーションからインストールプログラムに対して VNC による接続をし、操作を行ないます。操作手順については第1章 *YaST を利用したインストール* (3 ページ) に書かれているものと同じ手順です。

この種類のインストールを行なうには、下記の要件を満たす必要があります:

- リモートのリポジトリ: NFS, HTTP, FTP, SMB のうちのいずれかのプロトコルに対応したサーバと、そこに接続するためのネットワーク環境
- ネットワークの動作するターゲットシステム
- VNC ビューアと呼ばれるソフトウェア、もしくは Java の利用できるブラウザ (Firefox, Konqueror, Internet Explorer, Opera など) がインストールされた操作端末
- openSUSE のメディアキットに含まれる起動メディア (CD, DVD, USB フラッシュメモリ)。openSUSE のメディアキットについて、詳しくは 1.1 項「インストールメディアの選択」(3 ページ) をお読みください。
- リポジトリ側と操作端末に割り当て済みの有効な固定 IP アドレス
- ターゲットシステムに割り当てた有効な固定 IP アドレス

この方法でインストールを行なうには、下記の手順で行なってください:

- 1 まずは 2.2 項「インストール元のデータを保存するサーバの構築」(48 ページ) に書かれた手順に従ってリポジトリを構築します。NFS, HTTP, FTP のいずれかのネットワークサーバを選択してください。なお、SMB リ

ポジトリを構築する場合は、2.2.5項「SMB リポジトリの管理」(56 ページ)をお読みください。

- 2 openSUSE のメディアキットに含まれる起動メディア (CD, DVD, USB フラッシュメモリ) を利用して、ターゲットシステムを起動します。openSUSE のメディアキットについて、詳しくは 1.1項「インストールメディアの選択」(3 ページ)をお読みください。

- 3 ターゲットシステムでの起動画面が表示されたら、VNC の設定とリポジトリのアドレスを指定するため、起動オプションに入力を行ないます。詳しくは 2.4項「インストールのためのターゲットシステムの起動」(68 ページ)をお読みください。

ターゲットシステムはテキストベースの環境で起動し、VNC ビューアやブラウザでアクセスするため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 によるインストールでは自分自身の存在を OpenSLP で通知するため、ファイアウォールで禁止されていたりしなければ Konqueror を利用して `service:/` や `slp:/` から発見することもできます。

- 4 操作端末側では VNC ビューアのアプリケーションを起動するか、もしくはブラウザを起動して、2.5.1項「VNC インストール」(71 ページ)の方法で接続を行ないます。
- 5 あとは第1章 *YaST* を利用したインストール (3 ページ) で示されているインストール手順に従って行なってください。インストールの最終段階ではターゲットシステムを再起動しますが、この際はターゲットシステムに接続しなおしてください。

- 6 これでインストール作業は完了です。

2.1.2 VNC を利用したシンプルなりモートインストール (動的なネットワーク設定)

この種類のインストールでは、ターゲットシステムを起動してインストールの準備を行なうため、ターゲットシステムへの物理的な (ネットワークなどの遠隔手段に頼らない) アクセスが必要です。ネットワークの設定作業は DHCP を利用して行ないます。インストールプログラムが起動した後、遠隔のワークステーションからインストールプログラムに対して VNC による接続をし、操作を行ないます。

この種類のインストールを行なうには、下記の要件を満たす必要があります：

- リモートのリポジトリ: NFS, HTTP, FTP, SMB のうちのいずれかのプロトコルに対応したサーバと、そこに接続するためのネットワーク環境
- ネットワークの動作するターゲットシステム
- VNC ビューアと呼ばれるソフトウェア、もしくは Java の利用できるブラウザ (Firefox, Konqueror, Internet Explorer, Opera のいずれか) がインストールされた操作端末
- openSUSE のメディアキットに含まれる起動メディア (CD, DVD, USB フラッシュメモリ)。openSUSE のメディアキットについて、詳しくは 1.1 項「インストールメディアの選択」(3 ページ) をお読みください。
- IP アドレスを提供する DHCP サーバ

この方法でインストールを行なうには、下記の手順で行なってください:

- 1 まずは 2.2 項「インストール元のデータを保存するサーバの構築」(48 ページ) に書かれた手順に従ってリポジトリを構築します。NFS, HTTP, FTP のいずれかのネットワークサーバを選択してください。なお、SMB リポジトリを構築する場合は、2.2.5 項「SMB リポジトリの管理」(56 ページ) をお読みください。
- 2 openSUSE のメディアキットに含まれる起動メディア (CD, DVD, USB フラッシュメモリ) を利用して、ターゲットシステムを起動します。openSUSE のメディアキットについて、詳しくは 1.1 項「インストールメディアの選択」(3 ページ) をお読みください。
- 3 ターゲットシステムでの起動画面が表示されたら、VNC の設定とリポジトリのアドレスを指定するため、起動オプションに入力を行ないます。詳しくは 2.4 項「インストールのためのターゲットシステムの起動」(68 ページ) をお読みください。

ターゲットシステムはテキストベースの環境で起動し、VNC ビューアやブラウザでアクセスするため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 によるインストールでは自分自身の存在を OpenSLP で通知するため、ファイアウォールで禁止されていたりしなければ Konqueror を利用して `service:/` や `slp:/` から発見することもできます。

- 4 操作端末側では VNC ビューアのアプリケーションを起動するか、もしくはブラウザを起動して、2.5.1 項「VNC インストール」(71 ページ) の方法で接続を行ないます。

- 5 あとは 第1章 *YaST* を利用したインストール (3 ページ) で示されているインストール手順に従って行なってください。インストールの最終段階ではターゲットシステムを再起動しますが、この際はターゲットシステムに接続しなしてください。
- 6 これでインストール作業は完了です。

2.1.3 VNC を利用したリモートインストール (PXE ブートと Wake on LAN を使用)

このインストール方法の場合は、全く手を触れることなくインストールすることができます。ターゲットマシンは遠隔から開始して起動します。ユーザの操作は 実際のインストール作業でのみ必要になります。これはサイトをまたがるような 配置を行なうのに便利です。

この種類のインストールを行なうには、下記の要件を満たす必要があります:

- リモートのリポジトリ: NFS, HTTP, FTP, SMB のうちのいずれかのプロトコルに対応したサーバと、そこに接続するためのネットワーク環境
- TFTP サーバ
- お使いのネットワーク内で動作している DHCP サーバ
- PXE ブートと Wake on LAN に対応したネットワークデバイスを持ち、ネットワーク環境に接続されたターゲットシステム
- VNC ビューアと呼ばれるソフトウェア、もしくは Java の利用できるブラウザ (Firefox, Konqueror, Internet Explorer, Opera のいずれか) がインストールされた操作端末

この方法でインストールを行なうには、下記の手順で行なってください:

- 1 まずは 2.2 項「インストール元のデータを保存するサーバの構築」(48 ページ) に書かれた手順に従ってリポジトリを構築します。NFS, HTTP, FTP のいずれかのネットワークサーバを選択してください。なお、SMB リポジトリを構築する場合は、2.2.5 項「SMB リポジトリの管理」(56 ページ) をお読みください。

- 2 ターゲットシステムが起動イメージをダウンロードできるよう、TFTP サーバを設定します。詳しい手順については 2.3.2項「TFTP サーバの構築」(60 ページ)をお読みください。
- 3 任意のマシンに IP アドレスを配布し、TFTP サーバの場所を通知するよう DHCP サーバを設定します。詳しくは 2.3.1項「DHCP サーバの構築」(58 ページ)をお読みください。
- 4 ターゲットシステムを PXE ブートができるよう設定します。詳しくは 2.3.5項「PXE ブートのためのターゲットシステムの準備」(67 ページ)をお読みください。
- 5 ターゲットシステムの起動処理は、Wake on LAN を利用して開始します。2.3.7項「Wake on LAN」(67 ページ)をお読みください。
- 6 操作端末側では VNC ビューアのアプリケーションを起動するか、もしくはブラウザを起動して、2.5.1項「VNC インストール」(71 ページ)の方法で接続を行ないます。
- 7 あとは 第1章 *YaST* を利用したインストール (3 ページ) で示されているインストール手順に従って行なってください。インストールの最終段階ではターゲットシステムを再起動しますが、この際はターゲットシステムに接続しなおしてください。
- 8 これでインストール作業は完了です。

2.1.4 SSH を利用したシンプルなりモートインストール (固定のネットワーク設定)

この種類のインストールでは、ターゲットシステムを起動してインストールの準備を行なうため、ターゲットシステムへの物理的な (ネットワークなどの遠隔手段に頼らない) アクセスと、ターゲットシステムに対して設定する IP アドレスが必要です。インストールプログラムが起動した後、遠隔のワークステーションからインストールプログラムに対して SSH による接続をし、操作を行ないます。操作手順については 第1章 *YaST* を利用したインストール (3 ページ) に書かれているものと同じ手順です。

この種類のインストールを行なうには、下記の要件を満たす必要があります:

- リモートのリポジトリ: NFS, HTTP, FTP, SMB のうちのいずれかのプロトコルに対応したサーバと、そこに接続するためのネットワーク環境

- ネットワークの動作するターゲットシステム
- SSH クライアントソフトウェアがインストールされた操作端末
- openSUSE のメディアキットに含まれる起動メディア (CD, DVD, USB フラッシュメモリ)。openSUSE のメディアキットについて、詳しくは 1.1 項「インストールメディアの選択」(3 ページ) をお読みください。
- リポジトリ側と操作端末に割り当て済みの有効な固定 IP アドレス
- ターゲットシステムに割り当てる有効な固定 IP アドレス

この方法でインストールを行なうには、下記の手順で行なってください:

- 1 まずは 2.2 項「インストール元のデータを保存するサーバの構築」(48 ページ) に書かれた手順に従ってリポジトリを構築します。NFS, HTTP, FTP のいずれかのネットワークサーバを選択してください。なお、SMB リポジトリを構築する場合は、2.2.5 項「SMB リポジトリの管理」(56 ページ) をお読みください。
- 2 openSUSE のメディアキットに含まれる起動メディア (CD, DVD, USB フラッシュメモリ) を利用して、ターゲットシステムを起動します。openSUSE のメディアキットについて、詳しくは 1.1 項「インストールメディアの選択」(3 ページ) をお読みください。
- 3 ターゲットシステムでの起動画面が表示されたら、SSH の設定とリポジトリのアドレスを指定するため、起動オプションに入力を行ないます。詳しくは 2.4.2 項「カスタムな起動オプションの使用」(68 ページ) をお読みください。

ターゲットシステムはテキストベースの環境で起動し、SSH クライアントでアクセスするためのネットワークアドレスが表示されます。

- 4 操作端末側では SSH クライアントソフトウェアを起動し、2.5.2.2 項「インストールプログラムへの接続」(74 ページ) の方法で 接続を行ないます。
- 5 あとは 第1章 *YaST を利用したインストール* (3 ページ) で示されているインストール手順に従って行なってください。インストールの最終段階ではターゲットシステムを再起動しますが、この際はターゲットシステムに接続しなおしてください。
- 6 これでインストール作業は完了です。

2.1.5 SSH を利用したシンプルなりモートインストール (動的なネットワーク設定)

この種類のインストールでは、ターゲットシステムを起動してインストールの準備を行なうため、ターゲットシステムへの物理的な (ネットワークなどの 遠隔手段に頼らない) アクセスが必要です。ネットワークの設定作業は DHCP を利用して行ないます。インストールプログラムが起動した後、遠隔のワークステーションからインストールプログラムに対して SSH による接続をし、操作を行ないます。

この種類のインストールを行なうには、下記の要件を満たす必要があります:

- リモートのリポジトリ: NFS, HTTP, FTP, SMB のうちのいずれかのプロトコルに対応したサーバと、そこに接続するためのネットワーク環境
- ネットワークの動作するターゲットシステム
- SSH クライアントソフトウェアがインストールされた操作端末
- openSUSE のメディアキットに含まれる起動メディア (CD, DVD, USB フラッシュメモリ)。openSUSE のメディアキットについて、詳しくは 1.1 項「インストールメディアの選択」(3 ページ) をお読みください。
- IP アドレスを提供する DHCP サーバ

この方法でインストールを行なうには、下記の手順で行なってください:

- 1 まずは 2.2 項「インストール元のデータを保存するサーバの構築」(48 ページ) に書かれた手順に従ってリポジトリを構築します。NFS, HTTP, FTP のいずれかのネットワークサーバを選択してください。なお、SMB リポジトリを構築する場合は、2.2.5 項「SMB リポジトリの管理」(56 ページ) をお読みください。
- 2 openSUSE のメディアキットに含まれる起動メディア (CD, DVD, USB フラッシュメモリ) を利用して、ターゲットシステムを起動します。openSUSE のメディアキットについて、詳しくは 1.1 項「インストールメディアの選択」(3 ページ) をお読みください。
- 3 ターゲットシステムでの起動画面が表示されたら、SSH の設定とリポジトリのアドレスを指定するため、起動オプションに入力を行ないます。詳しくは 2.4.2 項「カスタムな起動オプションの使用」(68 ページ) をお読みください。

ターゲットシステムはテキストベースの環境で起動し、SSH クライアントで アクセスするためのネットワークアドレスが表示されます。

- 4 操作端末側では SSH クライアントソフトウェアを起動し、2.5.2.2項「インストールプログラムへの接続」(74 ページ) の方法で 接続を行ないます。
- 5 あとは 第1章 *YaST* を利用したインストール (3 ページ) で示されているインストール手順に 従って行なってください。インストールの最終段階ではターゲットシステムを 再起動しますが、この際はターゲットシステムに接続しなおしてください。
- 6 これでインストール作業は完了です。

2.1.6 SSH を利用したリモートインストール (PXE ブートと Wake on LAN を使用)

このインストール方法の場合は、全く手を触れることなくインストールすることが できます。ターゲットマシンは遠隔から開始して起動します。

この種類のインストールを行なうには、下記の要件を満たす必要があります：

- リモートのリポジトリ: NFS, HTTP, FTP, SMB のうちのいずれかのプロトコルに 対応したサーバと、そこに接続するためのネットワーク環境
- TFTP サーバ
- IP アドレスを提供する DHCP サーバ
- PXE ブートと Wake on LAN に対応したネットワークデバイスを持ち、ネットワー ク環境に接続されたターゲットシステム
- SSH クライアントソフトウェアがインストールされた操作端末

この方法でインストールを行なうには、下記の手順で行なってください：

- 1 まずは 2.2項「インストール元のデータを保存するサーバの構 築」(48 ページ) に書かれた手順に従ってリポジトリを構築します。NFS, HTTP, FTP のいずれかのネットワークサーバを選択してください。なお、SMB リ ポジトリを構築する場合は、2.2.5項「SMB リポジトリの管理」(56 ページ) をお読みください。

- 2 ターゲットシステムが起動イメージをダウンロードできるよう、TFTP サーバを設定します。詳しい手順については 2.3.2項「TFTP サーバの構築」(60 ページ)をお読みください。
- 3 任意のマシンに IP アドレスを配布し、TFTP サーバの場所を通知するよう DHCP サーバを設定します。詳しくは 2.3.1項「DHCP サーバの構築」(58 ページ)をお読みください。
- 4 ターゲットシステムを PXE ブートができるよう設定します。詳しくは 2.3.5項「PXE ブートのためのターゲットシステムの準備」(67 ページ)をお読みください。
- 5 ターゲットシステムの起動処理は、Wake on LAN を利用して開始します。2.3.7項「Wake on LAN」(67 ページ)をお読みください。
- 6 操作端末側では SSH クライアントソフトウェアを起動し、2.5.2項「SSH インストール」(73 ページ)の方法で 接続を行ないます。
- 7 あとは 第1章 *YaST* を利用したインストール (3 ページ) で示されているインストール手順に従って行なってください。インストールの最終段階ではターゲットシステムを再起動しますが、この際はターゲットシステムに接続しなおしてください。
- 8 これでインストール作業は完了です。

2.2 インストール元のデータを保存するサーバの構築

openSUSE のインストール元として使用するサーバは、動作しているオペレーティングシステムによって様々な設定方法が考えられます。インストールサーバとして使用するのに最も簡単なのは、openSUSE 11.1 以降のバージョンで YaST を利用した場合です。

ヒント

Linux マシンのインストールには Microsoft Windows のマシンを使用することができます。詳しくは 2.2.5項「SMB リポジトリの管理」(56 ページ)をお読みください。

2.2.1 YaST を利用したインストールサーバの構築

YaST では、ネットワークリポジトリを作成するためのグラフィカルツール を提供しています。このツールでは HTTP, FTP, NFS の各ネットワーク インストールサーバを設定することができます。

- 1 まずはインストールサーバとして動作させたいマシンに対して、root でログインします。
- 2 `yast2-instserver` パッケージをインストールします。
- 3 *YaST > その他 > インストールサーバ* を起動します。
- 4 続いてリポジトリの種類 (HTTP, FTP, NFS のいずれか) を選択します。選択したサービスは、システム起動時に自動的に起動されるようになります。お使いのシステムで既に対象のサービスが起動されている状態で、サーバの設定を手動で行ないたい場合は、*ネットワークサービスを設定しない* を選択して自動設定を行なわないようにしてください。また、どちらの場合でもインストールデータを保持するディレクトリは、サーバ内で定義しておく 必要があります。
- 5 必要なりポジトリ種類の設定を行ないます。サービスの種類によって自動設定の手順が異なります。自動設定を行なわないように指定した場合は、この手順は飛ばされます。

FTP や HTTP のサービスを介してインストールデータを公開する際の、ルートディレクトリの別名を設定します。インストールデータはそれぞれ、`ftp://サーバの IP アドレス/別名/名前` (FTP の場合) または `http://サーバの IP アドレス/別名/名前` (HTTP の場合) からアクセスできるようになります。ここで、*名前* にはこの後の手順で設定するリポジトリの 名称が入ります。以前の段階で NFS を指定した場合は、ワイルドカードと エクスポートの指定を行ないます。NFS サービスに対しては、`nfs://サーバの IP アドレス/名前` からアクセスできるようになります。NFS とエクスポートについて、詳しくは 第16章 *NFS でのファイル共有* (313 ページ) をお読み ください。

ヒント: ファイアウォール設定

お使いのシステムのファイアウォール設定で、それぞれ HTTP, NFS, FTP で使用するポートを許可していることを事前に確認しておいてください。ファイア

ウォールでポートを開くを押すと許可することができるほか、ファイアウォールの詳細から設定することもできます。

- 6 ここでリポジトリの設定を行ないます。インストールメディアから目的の場所にコピーを行なう前に、まずはリポジトリの名前を指定します (製品とそのバージョンを短縮した名前を指定しておくのがお勧めです)。YaST では、インストール DVD のコピーを生成する代わりに、メディアの ISO イメージを提供するよう指定することもできます。これを行なうには、関連するチェックボックスを選択して、ISO ファイルがローカル環境のどこに存在しているのかを指定します。このインストールサーバを利用して配布する製品にもよりますが、追加のリポジトリとしてアドオン CD やサービスパック CD を追加しておく必要がある場合があります。また、インストールサーバを OpenSLP 経由で通知したい場合は、関連するオプションを選択してください。
-

ヒント

お使いのネットワーク環境で対応している場合は、お使いのリポジトリを OpenSLP で通知するよう指定しておくことをお勧めします。この指定を行なうことで、それぞれのターゲットマシンでわざわざネットワークパスを指定したりする手間を省くことができます。ターゲットシステムでは単に SLP 起動オプションを利用して起動するだけで、あとの設定を行なうことなくネットワークリポジトリを検出することができます。詳しくは 2.4 項「インストールのためのターゲットシステムの起動」(68 ページ) をお読みください。

- 7 インストールデータのアップロード処理を行ないます。インストールサーバを設定するにあたってもっとも時間のかかる処理は、実際のインストールメディアをコピーする処理です。YaST で指示されたとおりの順序でメディアを挿入して、コピーが完了するまでお待ちください。データのコピーが全て完了すると、既存のリポジトリに関する概要の画面に戻ります。あとは **完了** を押して終了してください。

これでインストールサーバの準備は全て完了し、サービスを提供できるようになります。システムが起動するたびに自動的にサービスが起動しますので、起動時に特別な作業を行なったりする必要はありません。YaST の初期段階でネットワークサービスの自動設定を無効化していた場合のみ、このサービスを手作業で設定して開始する必要があります。

逆にリポジトリを削除するには、削除するリポジトリを選択して **削除** を押してください。インストールデータはシステムから削除されます。ネットワークサービスを無効化するには、関連する YaST モジュールをお使いください。

また、インストールサーバで複数の製品や複数のバージョンのインストールデータを提供したい場合は、YaST インストールサーバモジュールを起動して、概要画面から **追加** ボタンを押して新しいリポジトリを 追加してください。

2.2.2 NFS リポジトリの手動構築

インストールソースとして NFS を設定するには、2 段階の手順で行ないます。1 つめはインストールデータを保存しておくためのディレクトリ構造の作成と インストールメディアのコピー、2 つめはインストールデータをネットワーク 側に公開するためのエクスポート処理です。

インストールデータを保存しておくディレクトリを作成するには、下記の手順で 行ないます:

- 1 root でログインします。
- 2 後の手順でインストールデータを保存しておくためのディレクトリを 作成し、そのディレクトリに移動します。たとえば下記のようになります:

```
mkdir install/製品名/製品バージョン
cd install/製品名/製品バージョン
```

ここで、**製品** は製品名の略称を、**製品バージョン** には製品名とバージョンの入った 文字列をそれぞれ指定します。

- 3 次に、メディアキットに含まれているそれぞれの DVD を挿入し、下記の コマンドを実行します:

- 3a インストール DVD 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/(DVD-ROM ドライブのパス) .
```

ここで、*(DVD-ROM ドライブのパス)* には 実際に DVD ドライブがマウントされているディレクトリを指定します。お使いのシステムで使用しているドライブにもよりますが、`cdrom`, `cdrecorder`, `dvd`, `dvdrecorder` のいずれかを指定します。

- 3b ディレクトリの名称を DVD 番号に名称変更します:

```
mv (DVD-ROM ドライブのパス) DVDx
```

ここで、*x* はコピーを行なった DVD の 番号を指定します。

次に YaST を利用して、NFS によるリポジトリのエクスポートを行ないます。下記の手順で実施してください:

- 1 root でログインします。
- 2 YaST > ネットワーク サービス > NFS サーバ を起動します。
- 3 まずは **開始** と **ファイアウォールでポートを開く** をそれぞれ選択して、**次へ** を押します。
- 4 次に **ディレクトリの追加** を押して、インストール ソースが存在するディレクトリを選択します。ここでは **製品バージョン** を選択してください。
- 5 さらに **ホストの追加** を押し、インストールデータを 公開したい相手マシン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やネットワークアドレスの範囲、もしくはお使いの ネットワークにおけるドメイン名を入力することもできます。あとは必要な エクスポートオプションを指定するか、もしくは多くの環境でうまく動作 できるよう既定値のままで設定します。NFS 共有を公開する際の文法について、詳しくは exports のマニュアルページをお読みください。
- 6 最後に **完了** を押します。これで openSUSE の リポジトリを保持する NFS サーバの設定は完了です。自動的に NFS サーバは 起動され、システム起動時から動作するようになります。

YaST NFS サーバモジュールを利用する代わりに NFS を手動で設定して 公開したい場合は、下記の手順で行ないます:

- 1 root でログインします。
- 2 /etc/exports ファイルを開き、下記の行を入力します:

```
/製品バージョン *(ro,root_squash,sync)
```

上記の設定では、ディレクトリ **/製品バージョン** を、同じネットワーク内に属しているか、もしくはこのサーバに接続することの できる任意のホストに公開します。このサーバへのアクセスを制限するには、汎用ワイルドカード ***** の代わりにネットマスクや ドメイン名を指定してください。詳しくは export のマニュアルページをお読みください。設定ファイルを記入したら、保存して終了します。

- 3 NFS のサービスをシステム起動時に稼働するよう設定するには、下記のコマンドを入力してください:

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

- 4 NFS サーバを起動するには、`rcnfsserver start`と入力します。後から NFS サーバの設定を変更するには、設定ファイルを修正したあと下記のコマンドで NFS デーモンを再起動してください。`rcnfsserver restart`。

OpenSLP 経由で NFS サーバを通知すると、お使いのネットワーク内にある 全てのクライアントに対してそのアドレスを通知することができます。

- 1 `root` でログインします。
- 2 `/etc/slp.reg.d/install.suse.nfs.reg` という名前で 設定ファイルを作成し、下記の行を入力します:

```
# NFS インストールサーバの登録
service:install.suse:nfs:/$HOSTNAME/リポジトリのパス/DVD1,en,65535
description=NFS Repository
```

ここで *リポジトリのパス* には、お使いのサーバにおけるインストール元のパスを指定します。

- 3 最後に `rcslpd start` コマンドで OpenSLP デーモンを 起動してください。

OpenSLP についての詳細は、`/usr/share/doc/packages/openslp/` ディレクトリ以下に配置されているパッケージドキュメンテーションか、第12章 ネットワーク内の SLP サービス (267 ページ) をお読みください。NFS に関する詳細は、第16章 NFS でのファイル共有 (313 ページ) をお読みください。

2.2.3 FTP リポジトリの手動構築

FTP でのリポジトリ作成方法は、NFS リポジトリの作成方法ととても似ています。FTP リポジトリについても OpenSLP を介した通知を行なうことができます。

- 1 2.2.2項「NFS リポジトリの手動構築」(51 ページ) に示された手順に従って、インストール元を保持するディレクトリを作成します。
- 2 インストール元のディレクトリを FTP サーバ経由で公開するよう 設定します:

2a `root` でログインし、YaST ソフトウェア管理を利用して `vsftpd` パッケージ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移動します:

```
cd /srv/ftp
```

- 2c** FTP サーバのルートディレクトリ以下に、インストール元を保存する ためのサブディレクトリを作成します:

```
mkdir リポジトリ
```

ここで、*リポジトリ* には製品名を入力します。

- 2d** インストールリポジトリの内容をマウントし、FTP サーバのルート ディレクトリ以下から閲覧できるようにします:

```
mount --bind リポジトリのパス /srv/ftp/リポジトリ
```

ここで、*リポジトリのパス* and *リポジトリ* には、それぞれ該当する 値を入力してください。このマウントを恒久的に行ないたい場合は、*/etc/fstab* に設定を行なってください。

- 2e** vsftpd コマンドで vsftpd を起動します。

- 3** お使いのネットワーク環境で許可されていれば、OpenSLP 経由で通知を 行なうことができます:

- 3a** */etc/slp.reg.d/install.suse.ftp.reg* という 名前で設定ファイルを作成し、下記の行を入力します:

```
# FTP インストールサーバの登録
service:install.suse:ftp://$HOSTNAME/リポジトリ/DVD1,en,65535
description=FTP Repository
```

ここで *リポジトリ* には、お使いのサーバ内 でリポジトリが存在するディレクトリを入力します。なお、*service:* の行は1行で (改行せずに) 入力しなければ なりません。

- 3b** 最後に *rcslpd start* コマンドで OpenSLP デーモンを 起動してください。

ヒント: YaST を利用した FTP サーバの構築

FTP でのインストールサーバを設定するにあたって、手作業ではなく YaST を利用したい場合は、第19章 *YaST を利用した FTP サーバの設定* (389 ページ) にある YaST FTP サーバモジュールの使い方をお読みください。

2.2.4 HTTP リポジトリの手動構築

HTTP でのリポジトリ作成方法は、NFS リポジトリの作成方法ととても似ています。HTTP リポジトリについても OpenSLP を介した通知を行なうことができます。

- 1 2.2.2項「NFS リポジトリの手動構築」(51 ページ) に示された手順に従って、インストール元を保持するディレクトリを作成します。

- 2 インストール元のディレクトリを HTTP サーバ経由で公開するよう 設定します:

2a 18.1.2項「インストール」(344 ページ) に書かれている手順に従って、Web サーバ 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) に移動し、インストール元を 保持するためのサブディレクトリを作成します:

```
mkdir リポジトリ
```

ここで、*リポジトリ* には製品の名前を入力 します。

2c Web サーバのルートディレクトリ (/srv/www/htdocs) からインストール元 のディレクトリをたどれるよう、シンボリックリンクを 作成します:

```
ln -s リポジトリのパス /srv/www/htdocs/リポジトリ
```

2d HTTP サーバの設定ファイル (/etc/apache2/default-server.conf) を 修正し、シンボリックリンクをたどれるように します。

```
Options None
```

の行を

```
Options Indexes FollowSymLinks
```

に変更してください。

2e あとは `rcapache reload` コマンドで HTTP サーバ の設定を再読み込み させてください。

- 3 お使いのネットワーク環境で許可されていれば、OpenSLP 経由で通知を行な うことができます:

3a /etc/slp.reg.d/install.suse.http.reg という名前で 設定ファイルを 作成し、下記の行を入力 します:

```
# HTTP インストールサーバの登録
service:install.suse:http://$HOSTNAME/repository/DVD1/,en,65535
description=HTTP Repository
```

ここで *リポジトリ* には、お使いのサーバ内 でリポジトリが存在するディレクトリを入力します。なお、`service:` の行は1行で (改行せずに) 入力しなければなりません。

3b 最後に `rcslpd start` コマンドで OpenSLP デモンを 起動してください。

2.2.5 SMB リポジトリの管理

SMB を利用すると、Microsoft Windows のマシンをインストール元として 使用することができます。周囲に Linux マシンが存在しない環境でも Linux の配置を行なうことができます。

Windows 共有を利用して openSUSE のリポジトリを公開するには、下記の手順で行なってください:

- 1 お使いの Windows マシンにログインします。
- 2 インストール元のツリー構造全体を保持するための新しいディレクトリを 作成します。たとえば `INSTALL` のような名前で 作成します。
- 3 Windows の文書に従って、このディレクトリを共有するよう設定します。
- 4 作成したディレクトリに移動して、*製品名* のサブディレクトリを作成します。ここで *製品名* には、実際の製品名を入力します。
- 5 Enter the `INSTALL/製品名` の ディレクトリに移動して、それぞれの DVD を個別のディレクトリ にコピーします。たとえば `DVD1` や `DVD2` のようなサブディレクトリになります。

SMB 共有をリポジトリとしてマウントするには、下記の手順を行ないます:

- 1 インストーラターゲットを起動します。
- 2 *インストール* を選択します。
- 3 `F4` キーを押してリポジトリ選択の画面に移動します。

- 4 SMB を選択して、Windows マシンのホスト名か IP アドレス、および 共有名 (たとえば `INSTALL/製品名/DVD1` のようになります) とユーザ名、パスワードをそれぞれ入力します。

を押すと、YaST が起動して インストール処理が始まります。

2.2.6 サーバ内にある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対してメディアの内容をコピーする代わりに、インストールメディアの ISO イメージをインストールサーバにコピーして インストール時にターゲットにマウントさせることができます。HTTP, NFS, FTP サーバを設定し、メディアの内容をコピーする代わりに ISO イメージを設定するには、下記の手順で行なってください:

- 1 ISO イメージをダウンロードして、インストールサーバ内に保存します。
- 2 `root` でログインします。
- 3 それぞれ 2.2.2項「NFS リポジトリの手動構築」(51 ページ), 2.2.3項「FTP リポジトリの手動構築」(53 ページ), 2.2.4項「HTTP リポジトリの手動構築」(55 ページ) で示されている手順で、インストールデータの配置先を選択および作成 します。
- 4 それぞれの DVD に対してサブディレクトリを作成します。
- 5 最終的な配置先で ISO イメージをマウントします。具体的には下記の コマンドを入力します:

```
mount -o loop ISO ファイルのパス リポジトリのパス/製品名/メディア X
```

ここで、*ISO ファイルのパス* には ダウンロードした ISO イメージファイルのパスを、*リポジトリのパス* にはお使いのサーバにおける公開もとディレクトリを、*製品名* には 製品名を、*メディア X* にはメディアの種類 (CD または DVD) とメディア番号をそれぞれ入力してください。
- 6 それぞれ ISO イメージの枚数分だけ上記の手順を繰り返します。
- 7 あとはそれぞれ 2.2.2項「NFS リポジトリの手動構築」(51 ページ), 2.2.3項「FTP リポジトリの手動構築」(53 ページ), 2.2.4項「HTTP リポジトリの

手動構築」(55 ページ) に書かれた手順で通常通りのインストールを行いません。

システム起動時に自動で ISO イメージをマウントさせたい場合は、それぞれのマウント項目を `/etc/fstab` 内に記入してください。上記の例を `fstab` に記入する場合は、下記ようになります：

ISO ファイルのパス リポジトリのパス/製品名メディア X auto loop

2.3 ターゲットシステムの起動準備

この章では、より複雑な起動方法についての設定手順を示しています。それぞれ DHCP, PXE ブート, TFTP, Wake on LAN の設定例を記載しています。

2.3.1 DHCP サーバの構築

DHCP サーバを構築するには、2 つの方法があります。1 つは openSUSE 固有の方法として YaST のグラフィカルインターフェイスを利用する方法、もう 1 つは手作業で設定ファイルを変更する方法です。DHCP サーバについての詳細は、第 14 章 *DHCP* (295 ページ) をお読みください。

2.3.1.1 YaST を利用した DHCP サーバの構築

ネットワーククライアントに対して TFTP サーバの場所を通知し、インストール ターゲットが使用すべき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 つの項目を追記する必要があります。

- 1 DHCP サーバの動作しているマシンに対して、`root` でログインします。
- 2 `yast2-dhcp-server` パッケージをインストールします。
- 3 *YaST* > ネットワーク サービス > *DHCP* サーバ を起動します。
- 4 セットアップウィザードを利用して基本的な DHCP サーバの設定を済ませます。
- 5 **熟練者設定** を押し、スタートアップダイアログを 抜ける際に表示される警告メッセージが表示されたら、**はい** を選択します。
- 6 まずは **設定済みの宣言** ダイアログでは、新しいシステムが存在するサブネットを選択して **編集** を押します。

- 7 サブネットの設定 ダイアログでは、サブネットの設定に新しいオプションを追加するため、追加 ボタンを押します。
- 8 filename を選択し、値には pxelinux.0 と入力します。
- 9 さらにもう 1 つのオプション (next-server) を追加し、値として TFTP サーバのアドレスを入力します。
- 10 OK ボタンを押してから 完了 ボタンを押し、DHCP サーバ設定を完了します。

特定のホストに対して固定の IP アドレスを割り当てるよう DHCP サーバを設定するには、DHCP サーバモジュール内の 熟練者設定 (ステップ 5 (58 ページ)) を押し、追加 ボタンから新しいホストを追加してください。あとはオプションとして hardware と fixed-address を追加し、それぞれ値として ハードウェアアドレスと割り当てる IP アドレスを指定してください。

2.3.1.2 DHCP サーバの手動構築

お使いのネットワーククライアントに対して自動でアドレスを割り当てるだけでなく、ターゲットマシンからインストールプログラムを起動できるように する目的で、TFTP サーバとその中でファイルを指定する必要があります。

- 1 DHCP サーバの動作しているマシンに対して、root でログインします。
- 2 /etc/dhcpd.conf 内に配置されているお使いの DHCP サーバ設定ファイルについて、下記のような行を追記します:

```
subnet 192.168.1.0 netmask 255.255.255.0 {  
    range dynamic-bootp 192.168.1.200 192.168.1.228;  
    # PXE 関連の項目  
    #  
    # "next-server" には、使用すべき TFTP サーバのアドレスを指定します。  
    next-server TFTP サーバの IP アドレス:  
    #  
    # "filename" には、 /srv/tftpboot 以下に配置する pxelinux のファイル名  
    # を指定します。  
    filename "pxelinux.0";  
}
```

Replace ここで、TFTP サーバの IP アドレス には 実際の TFTP サーバのアドレスを記入します。dhcpd.conf で利用可能なオプションについて、詳しくは dhcpd.conf のマニュアルページをお読みください。

- 3 rcdhcpd restart コマンドを実行し、DHCP サーバを再起動します。

PXE と Wake on LAN を起動時に使用し、SSH でリモートコントロールを行ないたい場合は、インストールターゲットに対して DHCP サーバから固定の IP アドレスを割り当てる必要があります。固定の IP アドレスを割り当てるには、上記の例にさらに下記のような追記を行なう必要があります：

```
group {
    # PXE 関連の項目
    #
    # "next-server" には、使用すべき TFTP サーバのアドレスを指定します。
    next-server TFTP サーバの IP アドレス;
    #
    # "filename" には、 /srv/tftpboot 以下に配置する pxelinux のファイル名
    # を指定します。
    filename "pxelinux.0";
    host test {
        hardware ethernet MAC アドレス;
        fixed-address 割り当てる IP アドレス;
    }
}
```

host の項目では、まずインストールターゲットのホスト名を指定します。指定したホストに対してホスト名と IP アドレスを指定するには、そのホストのハードウェアアドレス (MAC アドレス) を知っておく必要があります。それぞれの値はご自身の環境に応じて修正してください。

DHCP サーバを再起動すると、指定したホストに固定の IP アドレスが割り当てられますので、SSH を介して接続できるようになります。

2.3.2 TFTP サーバの構築

TFTP サーバは YaST で設定することができるほか、xinetd と TFTP に対応した他の Linux オペレーティングシステム上で、手作業による設定を行なうこともできます。TFTP サーバはターゲットシステムが起動するための起動イメージを配信します。

2.3.2.1 YaST を利用した TFTP サーバの構築

- 1 root でログインします。
- 2 yast2-tftp-server パッケージをインストールします。
- 3 *YaST* > ネットワーク サービス > *TFTP* サーバ を 起動し、指示されたとおりにパッケージをインストールします。

- 4 その後 **有効化** を選択し、サーバを起動してシステムの起動処理に組み込まれていることを確認します。これでサーバの起動準備は完了です。xinetd は起動時に tftpd を 開始するようになります。
- 5 なお、お使いの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くため、**ファイアウォールでポートを開く** も選択して おいてください。お使いのサーバでファイアウォールが有効になっていない 場合は、このオプションは利用できません (選択する必要はありません)。
- 6 次に **参照** を押して、起動イメージのディレクトリを 指定します。既定のディレクトリ /tftpboot は 自動的に作成され、選択されています。
- 7 最後に **完了** を押すと設定が保存され、サーバが 起動されます。

2.3.2.2 TFTP サーバの手動構築

- 1 root でログインし、それぞれ tftp と xinetd パッケージをインストールします。
- 2 /srv/tftpboot と /srv/tftpboot/pxelinux.cfg のディレクトリが 存在していなければ、それぞれ作成します。
- 3 2.3.3項「PXE ブートの使用」(62 ページ) で説明されている内容をもとにして、起動イメージとして必要なファイルを配置します。
- 4 /etc/xinetd.d ディレクトリ以下にある xinetd の 設定ファイルを修正し、起動時に TFTP サーバが動作するようにします:
 - 4a tftp ファイルが存在していない場合は touch tftp コマンドでファイルを作成し、chmod 755 tftp コマンドを実行して読み取れる ようにします。
 - 4b tftp ファイルを開いて、下記のとおり入力 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 ファイルを保存し、rcxinetd restart コマンドで xinetd を再起動します。

2.3.3 PXE ブートの使用

PXE の完全な仕様説明や技術的な背景に関する情報は、Preboot Execution Environment (PXE) 仕様として (<http://www.pix.net/software/pxeboot/archive/pxespec.pdf>; 英語) に説明があります。

- 1 インストールリポジトリ内にある boot/<アーキテクチャ>/loader ディレクトリに移動し、linux, initrd, message, biostest, memtest の各ファイルを /srv/tftpboot ディレクトリにコピーします。下記のように行なってください:

```
cp -a linux initrd message biostest memtest /srv/tftpboot
```

- 2 YaST からインストール DVD を利用して syslinux パッケージをインストールします。

- 3 以下のようにして /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 使用するインストールリポジトリのあるディレクトリに移動し、isolinux.cfg ファイルを /srv/tftpboot/pxelinux.cfg/default にコピーします:

```
cp -a boot/<アーキテクチャ>/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default
```

- 5 /srv/tftpboot/pxelinux.cfg/default ファイルを 編集し、それぞれ readinfo, framebuffer で始まる行を削除します。

- 6 それぞれ failsafe と apic ラベルの行の下に、それぞれ下記の追加行を挿入します:

insmod=カーネルモジュール

この行は、PXE クライアントがネットワークインストールを行なうのに 必要な、ネットワークカーネルモジュールを指定しています。カーネルモジュール には、お使いのマシン に接続されたネットワークデバイスに対する適切なモジュール名を入力してください。

netdevice=インターフェイス名

この行は、ネットワークインストールを行なう際に使用するネットワーク インターフェイスの名前を指定しています。この行は、クライアントマシン に複数のネットワークカードが接続されている場合にのみ必要な行です。1 枚のネットワークカードしか接続されていない場合は省略可能です。

install=nfs://インストールサーバの IP アドレス/リポジトリのパス/
DVD1

この行では、クライアントマシンをインストールするための NFS サーバとリポジトリの場所を指定しています。それぞれ インストールサーバの IP アドレス には 利用するインストールサーバの IP アドレスを、リポジトリのパス にはリポジトリへの パスを入力します。なお、HTTP, FTP, SMB の各リポジトリについても 同じような方法で入力します。それぞれ冒頭の部分を http, ftp, smb に書き換えてください。

重要

SSH や VNC の起動パラメータのようなその他の起動オプションを指定したい 場合は、install の行に追記してください。パラメータの概要と使用例は、2.4項「インストールのためのターゲットシステムの起動」(68 ページ)をお読みください。

ヒント: カーネルと initrd ファイル名の変更

カーネルと initrd イメージファイルについては、それぞれ異なる名前を 指定することもできます。これは、同じ起動サーバから異なるオペレーティング システムを提供したい場合に便利な機能です。ただし、TFTP サーバで PXE ブートを行なう場合のファイル名には、1 つまでしかピリオド (.) が 許されないことに注意してください。

下記は /srv/tftpboot/pxelinux.cfg/default ファイルの 例です。お使いのネットワーク設定にあわせてプロトコルのプレフィクス (接頭辞) 部分を変更し、必要であればインストーラへの接続方法についても vnc, vncpassword や useshh, sshpassword などの オプションを追記してください。なお、改行を挟んで行の続きを記入する には、¥ を行末に挿入してください。

```
default harddisk

# default
label linux
    kernel linux
    append initrd=initrd ramdisk_size=65536 ¥
        install=nfs://インストールサーバの IP アドレス/リポジトリのパス/製品名/DVD1

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

```
# bios test
label firmware
    kernel linux
    append initrd=biostest,initrd splash=silent install=exec:/bin/run_biostest showopts

# memory test
label memtest
    kernel memtest

# hard disk
label haddisk
    localboot 0

implicit      0
display       message
prompt        1
timeout       100
```

- 7 ここで、インストールサーバの IP アドレスとリポジトリのパスにはお使いの環境に合わせた値を代入してください。

なお、次の章ではこのセットアップ方法で使用している PXELINUX のオプションについて、簡単な説明を行なっています。詳しい説明は syslinux パッケージの説明をお読みください。/usr/share/doc/packages/syslinux/ 以下のディレクトリに各種文書が配置されています。

2.3.4 PXELINUX 設定オプション

以下には PXELINUX の設定ファイルで利用する全てのオプションが示されています。

DEFAULT カーネルオプション...

既定のカーネルコマンドラインを指定します。PXELINUX で自動的に起動した場合は、DEFAULT の後に続く文字列が起動プロンプトに入力されたものとして扱われます。また、自動起動したことを示すために "auto" オプションも追加されます。

設定ファイルが存在していない場合や、DEFAULT の項目が設定ファイルに存在しなかった場合は、カーネル名「linux」でオプション指定無しであるものとされます。

APPEND オプション...

カーネルのコマンドラインに対して 1 つ以上のオプションを追加します。この項目は自動的に起動された場合も手動で選択した場合も追加されます。オブ

ションはカーネルコマンドラインの先頭のほうから追加されるため、入力されたカーネルオプションは以前のものを上書きするような形になります。

LABEL ラベル名 KERNEL イメージ APPEND オプション...

起動するカーネルとして ラベル名 を入力した場合、PXELINUX は イメージで指定した カーネルを読み込み、ファイルのグローバルセクションのオプション (LABEL コマンドの外側にあるもの) を 本項の APPEND オプションで指定したものに置き換えます。 *image* の既定値は *label* と同じもので、APPEND が書かれていなければ グローバルセクションの値が使用されます。最大で 128 個の LABEL 項目までが入力できます。

なお、GRUB では下記の書式を使用します:

```
title (タイトル)
kernel イメージオプション
initrd initrd ファイル名
```

PXELINUX では下記の書式を使用します:

```
label (タイトル)
kernel イメージ
append オプション
```

ラベルは MS-DOS のファイル名と同じような解釈を行ない、それらは全てユニークでなければなりません。たとえば「v2.6.30」と「v2.6.31」というラベルがあった場合、それらは DOS ファイル 名では同じものを指してしまうため、区別できないものになってしまいます。

また、イメージは必ずしも Linux カーネルである必要はありません; ブートセクターや COMBOOT ファイルでもかまいません。

APPEND -

何も追加しないことを指定します。LABEL セクション内の APPEND の後にパラメータとして 1 文字のハイフンを指定 すると、グローバルセクションの APPEND を上書きする 宣言になります。

LOCALBOOT 種類

PXELINUX では、KERNEL を指定する代わりに LOCALBOOT 0 を指定すると、カーネルを起動する代わりに 指定したローカルディスクを起動するようになります。

種類	説明
0	通常どおりの起動を行ないます

種類	説明
4	Universal Network Driver Interface (UNDI) をメモリ内に保持したまま ローカル起動を行いません
5	Universal Network Driver Interface (UNDI) を含めた PXE スタック全体 をメモリ内に保持したままローカル起動を行いません

その他の値は未定義です。UNDI や PXE スタックについて詳しく知らない 場合は、0 を指定してください。

TIMEOUT 制限時間

自動的な起動を行なうまでの起動プロンプトの待機時間を指定します。単位は 1/10 秒で、何らかのキーボード入力が起こるとコマンドのユーザ 入力が始まったものと見なして自動起動がキャンセルされます。0 を指定 すると、時間切れにならないようになります (既定値)。利用可能な最大の 値は 35996 (1 時間より少し少ない値) です。

PROMPT フラグ

フラグに 0 を指定すると、キーや が押されるか、もしくは Caps Lock や Scroll Lock がロックされている場合にのみ 起動プロンプトを表示します (既定値)。フラグに 1 を 指定すると、起動プロンプトは常に表示されます。

F2 ファイル名
F1 ファイル名
..etc...
F9 ファイル名
F10 ファイル名

起動プロンプトでそれぞれのファンクションキーを押した時に表示する ファイルを指定します。これは起動前のオンラインヘルプ (たとえばカーネルの コマンドラインオプション) を表示する際などに使用することができます。なお、従来のバージョンとの互換性を確保するため、F10 は F0 として入力することもできます。なお、現時点では F11 と F12 にファイル名を割り当てる ことはできません。

2.3.5 PXE ブートのためのターゲットシステムの準備

BIOS での起動順序に PXE 起動を含めるようにして、システムの BIOS が PXE ブートできるように設定します。

警告: BIOS 起動順序

BIOS の設定では、PXE の起動をハードディスクの起動よりも優先するよう設定しないでください。このように設定してしまうと、システム起動時に 毎回 PXE 起動が行なわれてしまい、インストールを毎回繰り返すことになってしまいます。

2.3.6 Wake on LAN のためのターゲットシステムの準備

Wake on LAN (WOL) を利用するには、事前に適切な BIOS オプションを設定しておく必要があります。また、ターゲットシステムの MAC アドレスも知っておく必要があります。MAC アドレスは Wake on LAN の実施に必要な情報です。

2.3.7 Wake on LAN

Wake on LAN は、そのマシンの MAC アドレスを含む特別なネットワークパケットを送信することで電源を入れる仕組みです。世界中にある各マシンにはユニークな MAC 識別子が割り当てられているため、異なるマシンを誤って起動してしまうようなことは考える必要がありません。

重要: 異なるネットワークセグメントをまたがる Wake on LAN

コントロールする側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存在していない場合は、マルチキャストとして WOL (Wake on LAN) パケットを送信するか、同じネットワークセグメント内に存在するマシンを遠隔から操作して WOL パケットを送信すると Wake on LAN を実現することができます。

2.4 インストールのためのターゲットシステムの起動

基本的には 2.3.7項「Wake on LAN」(67 ページ) や 2.3.3項「PXE ブートの使用」(62 ページ) で示したもの以外に、2 種類の方法でのインストール起動方法があります。ファンクションキーで設定して既定のオプションで起動する方法と、特定の ハードウェアを使用する際に、カーネルに指定する必要がある起動オプションを 起動画面で入力する方法です。

2.4.1 既定の起動オプションの使用

起動オプションについては 第1章 *YaST を利用したインストール* (3 ページ) で説明しています。通常は単に *インストール* を選択すればインストールの 起動処理が始まります。

何らかの問題が発生した場合は、*インストーラーACPI なし* を 選択するか、*インストーラー安全 設定* を選択してください。インストール処理時のトラブルシューティングについて、詳しくは 項「インストールの問題」(付録A ヘルプとトラブルシューティング, ↑ スタートアップ) をお読みください。

画面の下の方には、特定の環境で必要となるような拡張機能の案内が示されています。実際のパラメータ (詳しくは 2.4.2項「カスタムな起動オプションの使用」(68 ページ) をお読み ください) を覚えることなく、ファンクションキーを利用してインストール時の 追加オプションを指定することができます。利用可能なファンクションキーについて、詳しくは 1.5項「起動画面」(10 ページ) をお読み ください。

2.4.2 カスタムな起動オプションの使用

適切な起動オプションを使用すると、インストールの処理をより便利に行なう ことができるようになります。多くのパラメータは `linuxrc` のルーチンを利用して後から指定することもできますが、起動オプションを利用した方がより 簡単に指定することができます。セットアップを自動化するような場合は、`initrd` ファイルや `info` ファイルで与えることもできます。

下記の表には、この章で示したインストールシナリオと起動時に必要な パラメータ、および関連する起動オプションの一覧を示しています。それぞれ この表に現われている順序で追記していきましょう。たとえば (全てを 1 行 で記述します):

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

ここでそれぞれの *xxx* には、お使いの環境に合わせた 値を代入してください。

第1章 YaST を利用したインストール (3 ページ)

起動に必要なパラメータ なし

起動オプション 設定不要です

2.1.1項「VNC を利用したシンプルなりモートインストール (固定のネットワーク設定)」 (40 ページ)

起動に必要なパラメータ

- 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 の有効化設定
- VNC パスワード

起動オプション

- `install=(nfs,http,ftp,smb)://インストールメディアのパス`
- `netdevice=ネットワークデバイス` (複数のネットワークデバイスが接続されている場合にのみ、必要な設定です)
- `hostip=IP アドレス`
- `netmask=ネットワークマスク`
- `gateway=IP ゲートウェイ`
- `vnc=1`
- `vncpassword=パスワード`

2.1.2項「VNC を利用したシンプルなりモートインストール (動的なネットワーク設定)」 (41 ページ)

起動に必要なパラメータ

- インストールサーバの場所
- VNC の有効化設定
- VNC パスワード

起動オプション

- `install=(nfs,http,ftp,smb)://インストールメディアのパス`
- `vnc=1`
- `vncpassword=パスワード`

2.1.3項「VNC を利用したリモートインストール (PXE ブートと Wake on LAN を使用)」 (43 ページ)

起動に必要なパラメータ

- インストールサーバの場所
- TFTP サーバの場所
- VNC の有効化設定
- VNC パスワード

起動オプション 起動時のオプションは設定できません; 起動処理は PXE と DHCP で管理される仕組みであるためです

2.1.4項「SSH を利用したシンプルなりモートインストール (固定のネットワーク設定)」 (44 ページ)

起動に必要なパラメータ

- 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 の有効化設定
- SSH パスワード

起動オプション

- `install=(nfs,http,ftp,smb)://インストールメディアのパス`
- `netdevice=ネットワークデバイス` (複数のネットワークデバイスが接続されている場合にのみ、必要な設定です)
- `hostip=IP アドレス`
- `netmask=ネットマスク`
- `gateway=IP ゲートウェイ`
- `usessh=1`
- `sshpassword=パスワード`

2.1.5項「SSH を利用したシンプルなりモートインストール (動的なネットワーク設定)」 (46 ページ)

起動に必要なパラメータ

- インストールサーバの場所
- SSH の有効化設定
- SSH パスワード

起動オプション

- `install=(nfs, http, ftp, smb)://インストールメディアのパス`
- `usessh=1`
- `sshpassword=パスワード`

2.1.6項「SSH を利用したリモートインストール (PXE ブートと Wake on LAN を使用)」 (47 ページ)

- インストールサーバの場所
- TFTP サーバの場所
- SSH の有効化設定
- SSH パスワード

起動オプション 起動時のオプションは設定できません; 起動処理は PXE と DHCP で管理される仕組みであるためです

ヒント: linuxrc 起動オプションに関する詳細

Linux システムを起動するにあたって使用される linuxrc の起動オプション について、詳しくは <http://ja.opensuse.org/SDB:Linuxrc> をお読みください。

2.5 インストール処理の監視

インストール処理を遠隔から監視するには、いくつかの方法があります。インストール時に適切な起動オプションを指定すると、それぞれ VNC または SSH でインストール処理を操作し、遠隔からシステム設定を行なうことができます。

2.5.1 VNC インストール

VNC ビューアと呼ばれるソフトウェアを使用することで、任意のオペレーティング システムが動作するマシンから openSUSE のインストールを遠隔で 操作することが

できます。この章では、VNC ビューアアプリケーションや Web ブラウザを利用した設定方法を示しています。

2.5.1.1 VNC インストールの準備

VNC インストールを行なうにあたって、ターゲットシステムで行なわなければならないことは、インストールの起動段階で必要な起動オプションを設定することだけです (詳しくは 2.4.2 項「カスタムな起動オプションの使用」(68 ページ) をお読みください)。ターゲットシステムはテキストベースの環境で起動し、VNC クライアントがインストールプログラムに接続されるのを待つ動作になります。

その後インストールプログラムは、接続に必要な IP アドレスとディスプレイ 番号を通知します。ターゲットシステムに対して物理的なアクセスを行なうことができる環境の場合は、インストール処理の起動後に情報が提供されます。VNC クライアントを起動して提供された情報を入力し、さらに パスワードも入力してください。

また、インストールターゲットは自分自身を OpenSLP でアナウンスする仕組みになっているため、物理的なアクセスが行なえない環境でもインストール ターゲットに関する情報を SLP ブラウザで取得することができます。OpenSLP 対応のネットワーク環境とマシンで、下記のようにして行なってください:

- 1 KDE のファイルブラウザ兼 Web ブラウザである Konqueror を起動します。
- 2 場所バー内に `service://yast.installation.suse` と入力します。
Konqueror のウインドウ内にターゲットシステムが表示される はずです。あとはそのアイコンを選択することで、KDE の VNC ビューアが 起動され、インストール処理が始まります。また、VNC ビューアを単体で 起動して、提供される IP アドレスの後ろに `:1` を追加した文字列を入力することで接続することもできます。

2.5.1.2 インストールプログラムへの接続

基本的に VNC サーバ (この場合インストールターゲット) に接続するには、2 種類の方法があります。任意のオペレーティングシステムで動作する独立した VNC ビューアを立ち上げる方法と、Java の利用できる Web ブラウザを利用する 方法です。

VNC を利用する場合、他の Linux ディストリビューションや Windows、Mac OS などのような任意のオペレーティングシステムからインストールを操作 することができます。

Linux マシンの場合は、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 マシンの場合は、同アプリケーションの Windows 移植版をインストールしてください。TightVNC の Windows 版は、TightVNC の Web ページ (<http://www.tightvnc.com/download.html>) からダウンロード することができます。

ターゲットマシン上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、下記のようにして行ないます：

- 1 VNC ビューアを起動します。
- 2 SLP ブラウザやインストールプログラム自身が提供する、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それぞれ入力します：

IP アドレス:ディスプレイ番号

あとは通常のローカルインストールの時と同じように、YaST の画面が お使いのウインドウ内に表示されるようになります。

Web ブラウザを利用してインストールプログラムに接続する場合は、VNC ソフトウェアのインストールが不要になるだけでなく、オペレーティング システムについても任意のものを選択することができるようになります。お使いのブラウザアプリケーションが Java に対応しているもの (Firefox, Internet Explorer, Konqueror, Opera など) であれば、どの環境でも Linux システムのインストールを行なうことができます。

VNC インストールを行なうには、下記のようにして行ないます：

- 1 お使いの Web ブラウザを起動します。
- 2 アドレス欄に下記のとおり入力します：
http://ターゲットの IP アドレス:5801
- 3 VNC のパスワードを尋ねられたらパスワードを入力します。あとは 通常のローカルインストールと同様の YaST 画面がブラウザ内に表示 されます。

2.5.2 SSH インストール

SSH を利用すると、任意の SSH クライアントソフトウェアの動作する マシンから、インストール作業の遠隔操作を行なうことができます。

2.5.2.1 SSH インストールの準備

必要なソフトウェアパッケージ (Linux の場合は OpenSSH、Windows の場合は PuTTY) のインストールのほか、SSH インストールには適切な起動オプションを指定する必要があります。詳しくは 2.4.2 項「カスタムな起動オプションの使用」(68 ページ) をお読みください。OpenSSH は SUSE Linux ベースのオペレーティングシステムであれば既定でインストールされます。

2.5.2.2 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なアクセスを行なうことのできる環境であれば、起動時にコンソールに表示された IP アドレスを読んでください。そうでない環境の場合は、DHCP サーバの設定から、そのホストに割り当てられた IP アドレスを取得してください。
- 2 下記のコマンドラインを入力します:

```
ssh -X root@  
ターゲットの IP アドレス
```

ここで、ターゲットの IP アドレス には、実際のインストールターゲットの IP アドレスを記入してください。
- 3 ユーザ名を尋ねられたら、root と入力します。
- 4 パスワードを尋ねられたら、SSH 起動オプションで指定しておいたパスワードを入力します。認証が完了すると、インストールターゲットのコマンドラインプロンプトが表示されます。
- 5 インストールプログラムを起動するため、yast と入力してください。あとは第 1 章 *YaST* を利用したインストール (3 ページ) で示されている通常の YaST 画面が表示されます。

高度なディスク設定

より洗練されたシステム設定を行なう場合、ディスクの設定についても高度な設定を必要とします。YaST では、このような高度な設定を含む、一般的に 利用する全てのパーティション作業に対応しています。たとえばブロック デバイスに対して永続的な名前を設定するには、`/dev/disk/by-id` や `/dev/disk/by-uuid` のような形式を利用します。また Logical Volume Management (LVM) では、通常のセットアップで設定する従来のパーティション方式より、ずっと柔軟な 運用を実現できるよう設計されています。LVM でのスナップショット機能は データバックアップを容易に作成することができますし、いわゆる RAID と呼ばれるディスクの冗長配列機能も提供されていて、データの完全性と性能、耐障害性を補強することができます。また、openSUSE ではマルチパス I/O にも対応しているほか、iSCSI デバイスをネットワークディスクとして利用するオプションも用意されています。

3.1 YaST パーティション設定の利用

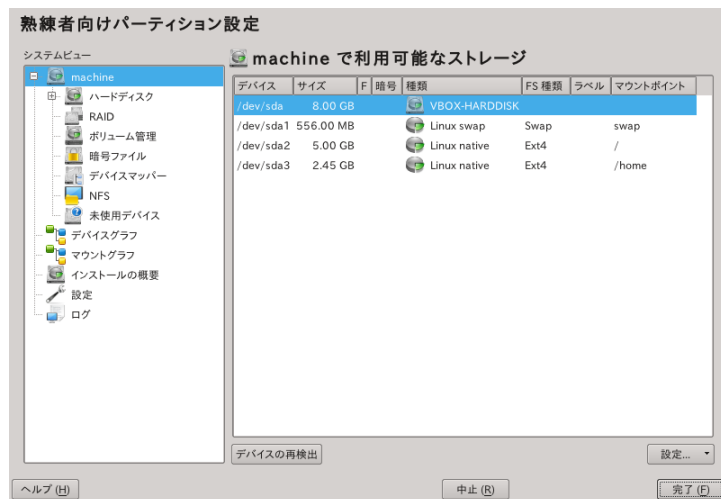
熟練者向けパーティション設定 図3.1「YaST パーティション設定」(76 ページ)では、複数のハードディスクのパーティション設定を変更することができます。パーティションは追加や削除、サイズ変更や編集を行なうことができます。また、この YaST モジュールからソフトウェア RAID や LVM にアクセスすることもできます。

警告: 稼働中のシステムのパーティション変更

お使いのシステムが稼働中であってもパーティション設定を変更することは可能ですが、作業ミスによるデータ損失の可能性がとて高いことに注意する必要があります。可能であればインストール済みのシステムに対するパーティション 設定

の変更は避け、どうしても必要である場合はお使いのデータを完全に バックアップしてから実施してください。

図 3.1 YaST パーティション設定



YaST の 熟練者向けパーティション設定 ダイアログには、利用可能なストレージの一覧に全ての接続済みハードディスク に対する既存のパーティションや、提案されたパーティション設定が表示されています。ハードディスク全体は /dev/sda のように数字無しでの表記に、パーティションは /dev/sda1 のように数字付きでそれぞれ表示されます。それぞれパーティションの サイズや種類、暗号化状態やファイルシステム (FS)、マウントポイントも表示されています。マウントポイントとは、Linux のファイルシステムツリー内のどこに 割り当てるかを指定するためのものです。

左側にある システムビュー には、いくつかの機能を 表示させるためのビューが提供されています。既存のストレージ設定に対する情報 収集や、RAID, ボリューム管理, 暗号ファイル などを設定することができるほか、BTRFS, NFS, TMPFS などの、追加機能付きのファイルシステムを表示したりすることもできます。

インストール時に熟練者向けパーティション設定を実行した場合は、ハードディスクの空き容量についても一覧表示され、自動で選択されている形になっています。openSUSE® に対してさらなるディスク領域を設定するには、一覧表示の 下から (ハードディスクの最後のパーティションから) 順に必要な領域を空けて 行ってください。たとえば既存のシステムに 3 つのパーティションが設定されていた場合、openSUSE に対して 2 つめのパーティションを占有させ、1 つめと 3 つめのパーティションを他のオペレーティングシステムに利用させたり することはできません。

3.1.1 パーティションの種類

それぞれのハードディスクには、最大で 4 つの項目を記録することのできるパーティションテーブルがあります。それぞれの項目はプライマリパーティションや拡張パーティションと呼ばれます。拡張パーティションはハードディスク内で 1 つしか設定できません。

プライマリパーティションは、単純に連続したシリンダ (物理的な ハードディスク領域) から構成されるもので、特定のオペレーティングシステム 向けに割り当てるものです。プライマリパーティションはパーティション テーブルの仕様制限により、ハードディスクごとに最大で 4 つのパーティション までしか作成できません。その代わりとなるのが拡張パーティションです。拡張パーティションもプライマリパーティションと同様に連続したシリンダを 割り当てますが、拡張パーティションはさらにその内側を論理パーティション に分割することができます。論理パーティションはパーティションテーブルには記録されません。言い換えれば、拡張パーティションは論理パーティションの入れ物として動作することになります。

4 つ以上のパーティションが必要である場合は、4 つめのパーティション (3 つめでも 2 つめでもかまいません) に拡張パーティションを作成します。もちろん拡張パーティションは空きのシリンダ範囲に設定しなければなりません。拡張パーティション内に論理パーティションを作成することで、必要な数の パーティションを作成してください。論理パーティションとして設定可能な 最大数は、ディスクの種類に関係なく 63 個までとなります。Linux で パーティションを使用する場合は、どちらのパーティション種類であっても 違いはありません。プライマリパーティション、論理パーティションとも 全く同じに機能します。

3.1.2 パーティションの作成

何もない状態からパーティションを作成するには、ハードディスク を選択してから空き領域のあるハードディスクを選択し、下記の手順でパーティション タブを開いて設定します：

- 1 追加 に押して作成するパーティションの種類 (プライマリ または拡張) を選択します。最大でプライマリパーティションを 4 つ、もしくは プライマリパーティション 3 つに拡張パーティションを 1 つまで作成できます。拡張パーティションを作成する場合は、その後に複数の論理パーティションを 作成することができます (詳しくは 3.1.1 項「パーティションの種類」(77 ページ) をお読みください)。

- 2 次に新しいパーティションのサイズを指定します。ディスク内の未使用領域を 全部占有するように選択することができるほか、独自にサイズを指定することも できます。
- 3 次に利用したいファイルシステムとマウントポイントを選択します。YaST では、それぞれ作成しようとしているパーティションに対して自動的に マウントポイントを提案します。ラベルによるマウントなど、マウント方法を変更するには *fstab* オプションを押してください。
- 4 お使いの環境で、必要であれば追加のファイルシステムオプションを指定 します。たとえば固定のデバイス名でマウントする必要がある場合などに 設定します。利用可能なオプションについて、詳しくは 3.1.3項「パーティションの編集」(80 ページ) をお読みください。
- 5 最後に *完了* を押すと、お使いの環境の パーティション設定が適用され、パーティション設定モジュールを終了することができます。

インストール作業時にパーティション作成を行なっている場合は、インストール概要の画面に戻ります。

3.1.2.1 btrfs のパーティション設定

新しくインストールするシステムに対して、btrfs を既定のファイルシステムとして使用したい場合 (は、パーティション分割の提案 画面の 提案設定 で、*btrfs* を既定のファイルシステムとして使用する を選択します。これを選択することで、インストールシステムは ext3 で /boot を、btrfs でルートディレクトリ / のパーティションを作成し、これをサブボリュームに 対する既定のセットとして設定するようになります。これらの設定は、熟練者向けパーティション設定 ツールを利用することで、後から修正することも可能です。

ルートファイルシステムは既定のサブボリュームであり、作成したサブボリュームの一覧には含まれません。また、既定の btrfs サブボリュームは、通常の ファイルシステムとしてマウントすることができます。

btrfs のサブボリュームについては、スナップショットを作成することもできます。これは手作業で行なうことができるほか、システムのエントを基準にして自動的に 作成することもできます。たとえば zypper でファイルシステムに 対し、何らかの変更を行なった場合は、snapper コマンドを呼び出して、変更前後のスナップショットを採取します。これは特に、zypper で行なった変更の問題があった場合に有効な 仕組みで、このスナップショットを利用することで以前の状態に戻すことができます。なお、zypper から起動される snapper は、既定では ルート ファイルシステムに對す

るスナップショットを採取します。これはスナップ ショット内に不要なデータファイルが紛れ込まないようにするためのもので、YaST が下記のようなディレクトリに対して、個別のサブボリュームを作成 するように促すのも、こういった理由によるものです。

提案で作成される btrfs のサブボリューム

/tmp /var/tmp /var/run

頻繁に変更されるようなコンテンツを含むディレクトリ。

/var/spool

メールなどのユーザデータが含まれるディレクトリ。

/var/log

巻き戻すべきではない、システムやアプリケーションのログを 含むディレクトリ。

/var/crash

カーネルがクラッシュした場合、クラッシュダンプを保存する ディレクトリ。

/srv

FTP や HTTP サーバのデータファイルを含むディレクトリ。

/opt

サードパーティ製のソフトウェアを含むディレクトリ。

ヒント: btrfs パーティションのサイズについて

スナップショットの保存を行なう際には、それなりのディスク領域が必要になるため、スナップショット機能を持たないパーティション (たとえば ext3) よりも空き容量を大きく見積もる必要があります。サブボリュームを設定する場合、ルートファイルシステムでの btrfs パーティションの推奨サイズは、20GB 程度です。

YaST を利用した btrfs サブボリュームの管理

btrfs パーティションのサブボリュームは、YaST の *熟練者向けパーティション設定* モジュールから管理できるようになりました。ここでは新しいサブボリュームを追加したり、既存の サブボリュームを削除したりすることができます。

手順 3.1 YaST を利用した btrfs サブボリュームの管理

- 1 YaST を起動し、システム > パーティション設定 を選択して、*熟練者向けパーティション設定* を起動します。

- 2 左側の システムビュー ペインで、*Btrfs* を選択します。
- 3 管理したいサブボリュームを含む *btrfs* パーティションを選択し、**編集** を押します。
- 4 **サブボリュームの処理** を選択します。すると、選択した *btrfs* パーティション 内にある、既存のサブボリュームがすべて表示されます。ここには複数の `@/. snapshots/xyz/snapshot` が表示される 場合がありますが、これはそれぞれ がスナップショットを表わすもので、複数のサブボリュームをまとめて保存しています。
- 5 それぞれサブボリュームの追加や削除は、下記のようにして行ないます：
 - 5a サブボリュームを削除するには、*既存のサブボリューム* 内の一覧から選択して、**削除** を押します。
 - 5b 新しいサブボリュームを追加するには、*新しいサブボリューム* のテキスト フィールドに名前を入力して、**新規追加** を押します。

3.2 YaST パーティション設定における *btrfs* ボリューム

- 6 作業が終わったら、*OK*, *完了* と押していきます。
- 7 最後に *Finish* を押すと、パーティション設定を終わることが できます。

3.1.3 パーティションの編集

新しいパーティションを作成したり既存のパーティションを変更したりする 場合には、様々なパラメータを設定することができます。新しいパーティション を作成する際には YaST が適切なパラメータを設定しますので、特にそこから 変更する必要はありません。手動でパーティションの設定を変更するには、下記の手順で行ないます：

- 1 パーティションを選択します。
- 2 **編集** を押してパーティションの編集画面を表示させ、必要に応じてパラメータを変更します：

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、パーティションが正しく登録できるようにするため、ファイルシステム ID を設定し

てください。一般的には、*Linux*, *Linux swap*, *Linux LVM*, *Linux RAID* のいずれかを指定します。

ファイルシステム

パーティションのファイルシステムを変更するには、パーティションをフォーマットする を押し、ファイルシステム の一覧からファイルシステムの 種類を選びます。

様々なファイルシステムについて、詳しくは ストレージ管理ガイド をお読みください。openSUSE は複数種類のファイルシステムに対応しています。このうち、Btrfs は高度な機能を必要とする環境では効果的な選択です。たとえば コピーオンライトの機能やスナップショット作成の機能を備えているほか、複数デバイスに跨るファイルシステムの作成やサブボリュームなど、便利な 技術を数多く備えています。また ReiserFS, JFS, XFS, Ext3 は、いずれも ジャーナル機能を持つファイルシステムです。これらのファイルシステムは、システムのクラッシュが発生しても、それらの操作がすべて記録されているため、システムを素早く復元させることができます。Ext2 はジャーナル 機能付きのファイルシステムではありませんが、管理用の領域を小さくすることができ、小さいパーティションには都合の良い選択です。

スワップとは特殊な形式で、パーティションを仮想的なメモリとして扱う ことのできる仕組みです。少なくとも 256 MB 以上のスワップ パーティションを作成してください。ただし、スワップ領域を大きく使用 してしまっているような場合は、スワップ領域の追加よりも物理的な メモリ搭載量の追加をお考えください。

警告: ファイルシステムの変更について

ファイルシステムを変更してパーティションをフォーマットし直すと、そのパーティション内にあるデータはすべて復元不可能な形で削除 されます。

デバイスの暗号化

暗号化を有効に設定すると、全てのデータは暗号化された形でハードディスク に書き込まれます。機密データのセキュリティ向上には貢献するものの、暗号化は時間のかかる処理であるため、システムの性能を落とすことになってしまいます。ファイルシステムの暗号化について、詳しくは 第10章 パーティションとファイルの暗号化 (↑セキュリティガイド) をお読みください。

マウントポイント

ファイルシステムのツリー構造内で、どのディレクトリに割り当てるのかを指定します。YaST が提案する値の中から選択するか、もしくは任意の値を入力します。

fstab オプション

グローバルなファイルシステム管理ファイル (/etc/fstab) では、様々なパラメータを設定することができます。多くの場合は既定の設定で問題はありませんが、たとえばファイルシステムの識別方法をデバイス名から ボリュームラベルに変更したりすることができます。ボリュームラベルでは / とスペースを除く全ての文字を利用することができます。

固定のデバイス名でマウントするよう設定するには、マウントオプションとして *デバイス ID*, *UUID*, *ラベル* のいずれかを選択してください。openSUSE では、固定のデバイス名を既定で利用するようになっています。

パーティションをラベルでマウントしたい場合は、*ボリュームラベル* の欄に値を指定します。たとえば /home にマウントしたい パーティションに対して、HOME のようなラベル名を設定します。

また、ファイルシステム上でクォータを設定したい場合は、*クォータサポートを有効にする* を選択してください。これは YaST の *ユーザとグループの管理* モジュールを利用してクォータを設定する場合、事前に設定しておかなければなりません。クォータの設定について詳しくは、項「クォータの管理」(第 10章 *YaST を利用したユーザ管理*, ↑ *スタートアップ*) をお読みください。

3 *完了* を押すと変更点を保存することができます。

注記: ファイルシステムのサイズ変更

既存のパーティションについてサイズの変更を行なうには、対象のパーティションを選択して *サイズ変更* を押します。なお、パーティション サイズの変更は、マウント中の状態から行なうことはできません。パーティション のサイズ変更を行なう前に、関連するパーティションのマウントは解除してください。

3.1.4 熟練者向けオプション

システムビュー でハードディスクデバイス (たとえば *sda*) を選択すると、**熟練者向けパーティション設定** ウィンドウ内の右下に **熟練者向け機能...** のボタンが表示されます。このメニューには下記のコマンドが含まれています:

新しいパーティションテーブルの作成

このオプションは、選択したデバイスに対して新しいパーティションテーブルを作成します。

警告: 新しいパーティションテーブルの作成について

新しいパーティションテーブルを作成すると、そのデバイス上に存在する全てのパーティションとデータが復元不可能な形で削除されます。

このディスクを複製する

このオプションは、選択したデバイスのパーティションレイアウト (データは含まれません) を利用可能な他のディスクに複製することができます。

3.1.5 高度なオプション

コンピュータのホスト名 (システムビュー の枠内にある ツリーの最上位レベル) を選択すると、**熟練者向けパーティション設定** ウィンドウ内の右下に **設定...** のボタンが表示されます。このメニューには下記のコマンドが含まれています:

iSCSI の設定

SCSI over IP のブロックデバイスにアクセスするには、まず iSCSI について設定を行なう必要があります。この作業を行なうと、パーティション一覧内に 利用可能なデバイスが追加表示されるようになります。

マルチパスの設定

このオプションを選択すると、対応しているマストレージデバイスに対してマルチパスの設定を行なうことができます。

3.1.6 さらなるパーティション設定に関する豆知識

下記の章では、お使いのシステムにパーティションを設定するにあたって 正しい決断を下すための、いくつかのヒントや豆知識を掲載しています。

ヒント: シリンダ数

パーティションツールによっては、パーティションのシリンダの数え方が異なる場合があります。0 から始まるものと、1 から始まるものの 2 種類があります。シリンダ数を数える場合は、シリンダ数の数え方に注意し、必要であれば 1 を足して計算してください。

3.1.6.1 スワップの使用

スワップは利用可能な物理メモリを拡張するための仕組みです。物理的に搭載されているメモリよりも大きなメモリを確保できるようになります。カーネル 2.4.10 以前のメモリ管理システムでは十分な量のスワップが必要でした。その当時は、物理メモリの 2 倍以上のスワップが存在していないと、システムの性能が上がらないことがありました。このような制限は今はありません。

Linux はメモリからディスクに移動するページを選択するのに、「Least Recently Used」(LRU; 参照される頻度が最も低いもの) と呼ばれる方式で選択を行ないます。そのため、動作中のアプリケーションには より大きなメモリを提供し、キャッシュ処理もよりスムーズに動作するようになります。

アプリケーションが利用可能なメモリ量よりも大きなサイズの割り当てを行なおうとした場合は、スワップ関連の問題が生じます。3 つの主なケースが考えられます:

スワップが設定されていないシステム

アプリケーションは利用可能な最大のメモリを取得します。全てのキャッシュデータは開放されることになるため、他の動作中アプリケーションの速度は低下します。数分程度が経過すると、カーネルに用意されたメモリ不足解決器 (out-of-memory kill mechanism (OOM Killer)) が動作し、プロセスが kill されるようになります。

中程度の量のスワップが設定されたシステム (128 MB (メガバイト) から 512 MB)

当初の状態ではシステムはスワップ無しの状態と同じように速度が低下します。全ての物理メモリが割り当てられると、スワップ領域を使い出すようになります。この時点ではシステムの動作は非常に遅くなり、リモートからのコマンド実行がほとんど行なえない状態になります。スワップ領域を設定したハードディスクの速度にもよりますが、システムはシステムはその状態を 10 分から 15 分程度保持し、その後カーネルに用意されたメモリ不足解決器 (out-of-memory kill mechanism (OOM Killer)) が動作し、問題を解決しようとしま

す。なお、コンピュータに「ディスクへのサスペンド」を設定する場合は、ある一定のサイズのスワップ領域が必要になります。この場合、スワップサイズはメモリ内に存在するデータを保持しておくのに十分なサイズ (512 MB から 1 GB 程度) を設定しておく必要があります。

大きな量のスワップが設定されたシステム (GB (ギガバイト) 以上)

過度にスワップしてしまうばかりか、その制御すらきかないようなアプリケーションについては、これを使用しないことが理想ですが、そのようなアプリケーションを使用する必要がある場合は、回復するのに何時間もの時間がかかってしまうようなことがあります。この場合、システムは不確定な状態になってしまい、たとえばそのような欠陥アプリケーションを kill したとしても、他のプロセスはタイムアウトや 処理エラーを発生させてしまいます。この場合は、コンピュータを再起動することで再度問題なく動作できるような状態に戻すことができます。大きな量のスワップは、アプリケーション側でこの機能をどうしても必要としている場合にのみ有効です。そのようなアプリケーション (たとえばデータベースシステムとか、画像加工 プログラムとか) では、必要に応じてハードディスク領域を直接利用するような 仕組みを備えている場合があります。スワップ領域を大きくする代わりに、そのような設定を利用することをご検討ください。

システムが制御不能になっていない状況で、急につらなるスワップ領域が必要になった場合は、スワップ領域をオンラインで拡張することができます。スワップ 領域用にパーティションを準備してあれば、そのパーティションを YaST から 追加するだけで設定できます。そのようなパーティションをお持ちでない 場合は、スワップファイルを利用してスワップの拡張を行なうこともできます。スワップファイルはスワップパーティションよりも一般に速度の面で劣りますが、いずれも物理メモリよりもずっと遅く、大きな違いはありません。

手順 3.2 スワップファイルの手動追加

稼働中のシステムにスワップファイルを追加するには、下記の手順で行ないます：

- 1 まずはお使いのシステムに中身が空のファイルを作成します。たとえば 128 MB (メガバイト) のスワップファイルを `/var/lib/swap/swapfile` ディレクトリ内に作成したい 場合は、下記のコマンドを実行します：

```
mkdir -p /var/lib/swap
dd if=/dev/zero of=/var/lib/swap/swapfile bs=1M count=128
```

- 2 下記のコマンドを実行してスワップファイルの初期化を行ないます。

```
mkswap /var/lib/swap/swapfile
```

- 3 下記のコマンドでスワップを有効に設定します。

```
swapon /var/lib/swap/swapfile
```

スワップファイルを無効化するには、下記のコマンドを入力します。

```
swapoff /var/lib/swap/swapfile
```

- 4 また、現在使用中のスワップ領域を表示するには、下記のコマンドを入力します。

```
cat /proc/swaps
```

なお、上記の手順では一時的に使用するスワップ領域を設定しています。システムを再起動すると、設定したスワップは使用されなくなります。

- 5 このスワップファイルを恒久的に使用するには、下記の行を `/etc/fstab` に追加します：

```
/var/lib/swap/swapfile swap swap defaults 0 0
```

3.1.7 パーティション設定と LVM

熟練者向けパーティション設定 では、システムビュー の枠内にある *ボリューム管理* を利用して LVM 設定を行なうことができます。ただし、お使いのシステムに動作中の LVM 設定が存在している場合は、LVM の初期設定に入る段階で自動的にそれらが有効化されます。この場合、パーティションの存在する全てのディスク (有効化されたボリュームグループ に属するもの) のパーティション設定は変更できません。Linux カーネルは 使用中のパーティションが存在するディスクについて、変更された パーティションテーブルを読み直すことができないためです。既にお使いのシステムで動作する LVM 設定が存在する場合は、物理的なパーティション 設定は必要ではないため、その代わりに論理ボリュームの設定を変更してください。

ボリュームに対する情報は、物理ボリューム (PV) のパーティション冒頭部分に 書き込まれます。それらのパーティションを LVM ではない他の用途に使用する 場合は、ボリュームの冒頭部分を削除しておくことをお勧めします。たとえば ボリュームグループ `system` と物理ボリューム `/dev/sda2` が存在する場合、下記のコマンドで削除することができます。 `dd if=/dev/zero of=/dev/sda2 bs=512 count=1`。

警告: 起動用のファイルシステム

起動中に使用するファイルシステム (ルートファイルシステムか、もしくは `/boot` パーティション) は LVM 論理ボリューム内に 存在させてはなりません。その代わりに、通常の物理パーティション内に 配置してください。

3.2 LVM の設定

この章では、論理ボリュームマネージャ (LVM) の考え方と、その多目的な 使い方について説明しています。YaST で LVM を利用した設定方法については、3.2.2 項「YaST を利用した LVM 設定」(89 ページ) をお読みください。

警告

LVM を使用すると、場合によってはデータ損失などのリスクを増加させてしまうことがあることにご注意ください。アプリケーションのクラッシュや電源の問題、およびコマンドの入力ミスなどのリスクも考えられます。そのため、LVM を 実装したり再設定したりする際には、お使いのデータは必ず保存しておいてください。バックアップ無しでの作業は行なってはなりません。

3.2.1 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に対応した、柔軟なハードディスク領域管理 機能を提供します。これは当初のパーティション設定が終わったあと、システムを 運用中の状態でハードディスク領域を部分的に変更したい、という要件が発生していたことから開発が始まりました。稼働中のシステムではパーティション設定を 変更することが難しいため、LVM では仮想プール (ボリュームグループ、略して VG と呼びます) というメモリ領域を用意することで、必要に応じて論理 ボリューム (LV) を作成できるようにしました。オペレーティングシステムは パーティションにアクセスする代わりに、これらの LV にアクセスします。ボリュームグループは複数のディスクから構成することができます。この方法により、LVM は物理的なディスク構成とは直接関係のない抽象機能を提供します。そのため、物理的なパーティションに比べ、安全かつ容易に部分的な変更を行なうことができるようになっています。物理的なパーティションに関する知識は、3.1.1 項「パーティションの種類」(77 ページ) と 3.1 項「YaST パーティション設定の利用」(75 ページ) をそれぞれお読みください。

図 3.3 物理的なパーティションと LVM

図3.3「物理的なパーティションと LVM」(87 ページ) では物理的なパーティション (左側) と LVM 論理ボリューム (右側) を比較したものです。左側では 1 台のハードディスクを 3 つの物理的なパーティション (PART) に分割していて、それ

それマウントポイント (MP) を設定することにより、オペレーティング システムからのアクセスができるようになっています。右側では 2 台の ハードディスクをそれぞれ 3 つの物理パーティションに分割しています。そこから 2 つの LVM ボリュームグループ (VG 1 と VG 2) を設定しています。VG 1 には DISK 1 から 2 つのパーティション、DISK 2 から 1 つのパーティションをそれぞれ設定しています。また、VG 2 には DISK 2 から残りの 2 つのパーティションを設定しています。LVM では、ボリュームグループ内に取り込まれたディスク パーティションのことを物理ボリューム (PV) と呼びます。ボリュームグループ 内には 4 つの LV (LV 1 から LV 4 まで) を設定していて、オペレーティングシステムはそれぞれ設定されたマウントポイント経由で アクセスできるようになっています。異なる LV 同士の境界は、パーティションの境界と一致している必要はありません。この例では LV 1 と LV 2 の境界をご覧ください。

LVM の機能:

- 複数のハードディスクやパーティションを、大きな論理ボリュームとして 統合することができます。
- 構成が適切であれば、ある LV (たとえば /usr) の 空き領域が枯渇した場合、サイズを拡張することができます。
- LVM を使用することで、稼働中のシステムに対してハードディスクや LV の 追加を行なうことができます。ただし、ホットスワップ (活線挿抜) に対応したハードウェアが必要です。
- LV のデータを複数の PV に分散する "ストライプモード" を利用することができます。PV がそれぞれ異なるディスクに存在していれば、読み書きの性能を 向上させることができます。これは RAID 0 とも呼ばれます。
- スナップショット機能により、稼働中のシステムで矛盾のないバックアップを 採取できるようになります (特にサーバ用途に使用する場合に便利な 機能です)。

このような機能を持つ LVM は、多用される家庭用 PC や小規模サーバに便利な仕組みになっています。LVM はデータ量が増加し続けるユーザ (たとえば データベースや楽曲のアーカイブ、ユーザのディレクトリなど) には適した 仕組みで、物理的なハードディスクのサイズよりも大きなファイルシステムを 作成することができます。また、LVM のもう 1 つの利点は、最大で 256 個 までの LV を追加することができるという点です。ただし LVM は通常の パーティションとは異なる作業を行なわなければなりません。LVM の設定手順 や詳しい情報については、LVM の公式 HOWTO <http://tldp.org/HOWTO/LVM-HOWTO/> をお読みください。

カーネルバージョン 2.6 以降では、LVM バージョン 2 を利用することができます。これは以前のバージョンの LVM と後方互換性があり、古いバージョンの ボリュームグループについても管理できるようになっています。また、新しい ボリュームグループを作成する際には、新しい形式で作成するか古い形式で 後方互換性を保つかを選択することができます。なお、LVM 2 では カーネルパッチを適用する必要がなく、2.6 カーネル内蔵のデバイスマッパー を利用します。特別なパッチを適用していないカーネルでは LVM バージョン 2 にのみ対応しているため、下記の章では LVM バージョン 2 を利用して 話を進めるものとします。

3.2.2 YaST を利用した LVM 設定

YaST からの LVM 設定は、YaST の熟練者向けパーティション設定内の システムビュー にある、*ボリューム管理* から行なうことができます (詳しくは 3.1 項「YaST パーティション設定の利用」(75 ページ) をお読みください)。熟練者向けパーティション設定では既存のパーティションを 編集したり削除したりすることができますほか、LVM で使用するために新しい パーティションを作成することもできます。LVM の作業は、ボリュームグループに 領域を提供するため、PV を作成することからはじまります:

- 1 ハードディスク からハードディスクを選びます。
- 2 パーティション タブに切り替えます。
- 3 *追加* を押し、このディスクに作成する PV のサイズを 指定します。
- 4 パーティションをフォーマットしない を選択し、ファイルシステム ID に *0x8E Linux LVM* を選択します。このパーティションはフォーマットしないでください。
- 5 上記までの手順を、必要な物理ボリューム数だけ繰り返してください。

3.2.2.1 ボリュームグループの作成

お使いのシステムに既存のボリュームグループが存在しない場合、次に それを追加します (図 3.4「ボリュームグループの作成」(90 ページ) をご覧ください)。システムビュー 内の *ボリューム管理* から、*ボリュームグループの追加* を押すことで、追加のボリュームグループを作成することもできます。通常は 1 つのボリュームグループを作成するだけで十分です。

- 1 まずはボリュームグループの名前を入力します (例: system)

- 次に **物理エクステントサイズ** を選択します。この値は、ボリュームグループ内での物理ブロックのサイズを指定します。ボリュームグループ内のディスク領域は、このサイズ単位で処理されます。
- デバイスを選択して **追加** を押すと、ボリュームグループに物理ボリュームを追加することができます。デバイスを選択する際に Ctrl を押しながらか行なうと、複数のデバイスを選択することができます。
- 完了** を押して閉じます。これでボリュームグループの設定が終わり、次の手順に進むことができますようになります。

図 3.4 ボリュームグループの作成

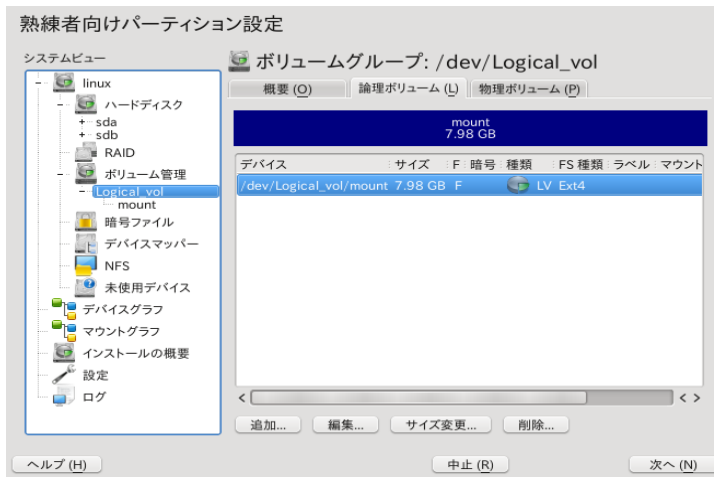


複数のボリュームグループを設定していて PV を追加したり削除したりしたい場合は、まず **ボリューム管理** 内からボリュームグループを選択し、**サイズ変更** ボタンを押してください。その後表示されるウィンドウで、選択したボリュームグループに対する PV を追加または削除することができます。

3.2.2.2 論理ボリュームの設定

物理ボリュームからボリュームグループを設定したら、次にオペレーティングシステムで論理ボリュームを設定します。作成したボリュームグループを選択し、**論理ボリューム** タブに移動してください。**追加**、**編集**、**サイズ変更**、**削除** の各ボタンを利用し、存在するボリュームグループ全てを使用するまで設定してください。少なくとも論理ボリュームには 1 つ以上のボリュームグループを設定する必要があります。

図 3.5 論理ボリューム管理



追加 を押すと、ウィザード形式の ポップアップが表示されます:

1. まずは論理ボリュームの名前を入力します。たとえば /home にマウントさせたい論理ボリュームであれば、それをそのまま説明する HOME などの名前を入力してください。
2. 次に論理ボリュームのサイズとストライプ数を指定します。1 台のハードディスクしか物理ボリュームに存在していない場合は、1 以上のストライプ数を設定することはできません。
3. 続いて論理ボリューム上で使用するファイルシステムと、マウントポイントを指定します。

ストライプを利用することで、複数の物理ボリューム (PV) に対してデータの書き込みを分散させることができますようになります。ただし、ボリュームのストライプは異なる物理ボリュームにまたがる場合にのみ設定できるもので、それぞれの物理ボリュームは少なくともボリュームのサイズ分の容量が必要です。ストライプの最大数は物理ボリューム数と同じで、"1" を指定すると "ストライプ処理を利用しない" 意味になります。また、ストライプは異なるハードディスク上の物理ボリューム上に対して設定した場合にのみ意味を持つもので、同じハードディスク上に対して設定してしまうと、かえって性能が落ちてしまいます。

警告: ストライプ

現時点の YaST ではストライプに関する設定の妥当性を検証する機能が 存在していません。そのため、ここで誤った設定を行なっても事前には チェックされず、LVM を実際に作成する際にチェックされます。

これでお使いのシステムに LVM を設定することができました。これで作成した 論理ボリュームを使用することができます。作成した論理ボリュームには適切な マウントポイントを設定してお使いください。完了 を 押すと YaST 熟練者向けパーティション設定に戻り、作業は完了です。

3.3 ソフトウェア RAID の設定

RAID (Redundant Array of Independent Disks) の目的は、複数のハードディスク パーティションを組み合わせることで 1 つの巨大な 仮想 ディスクを構成し、性能向上とデータの保全のいずれか、または両方を目指した しくみです。多くの RAID コントローラでは、IDE プロトコルよりも多数の ディスクをより効率的に扱うことができるという理由で、SCSI プロトコルを用いています。また、SCSI プロトコルでは並列コマンド処理という機能も 備えています。それ以外にも、IDE や SATA に対応する RAID コントローラも いくつか存在しています。ソフトウェア RAID はハードウェア RAID に比べ、コントローラを購入する追加コストが発生しないという点で有利ですが、CPU 時間を多く消費しメモリも利用してしまうため、高性能なコンピュータを構成する場合には不利な選択です。

openSUSE® では複数のハードディスクを 1 台のソフトウェア RAID システムに組み合わせる仕組みを備えています。RAID はシステム内の構成 方法によって異なる目的や利点、特性をそれぞれ備えています。これらの 違いは *RAID レベル* としても知られています。

一般的な利用される RAID レベルは、下記のとおりです:

RAID 0

このレベルは、各ファイルのブロックを複数のハードディスクに分散させることで、性能の向上を目指すレベルです。実際のところはデータの冗長性が 存在しないことから、厳密な意味での RAID ではありませんが、一般的には *RAID 0* と呼ばれています。RAID 0 では 2 台以上のハードディスクを組み合わせ使用します。性能は向上しますが、いずれかのハードディスクが故障すると、RAID システム全体が破壊される ことになります。

RAID 1

このレベルは、それぞれのハードディスクに同じデータを書き込むことで、お使いのデータの安全性を高めるレベルです。これは **ハードディスクミラーリング** としても知られている方法です。1 台のディスクが故障しても他のディスクにコピーが存在するため、そこから読み出すことができます。最後の 1 台のディスクが壊れるまでは、お使いのデータは通常どおり読み出すことができます。ですが、ディスク障害が検出されず、読み出したデータだけが壊れるタイプの障害が発生した場合は、壊れたデータを壊れていないハードディスクにコピーしてしまいます。これによって本質的には同じデータ損失が発生することになります。コピー処理を行なうため、1 台のディスクを使用する場合に比べて性能が低下します (10 から 20 パーセント程度低下します) が、読み込み性能については 1 台のハードディスクの場合よりも、それなりに速くなります。これは複製したデータを同時並行で検索するためのものです。一般に Level 1 は、1 台のハードディスクと比較して読み込み性能では 2 倍程度、書き込み性能では同等程度の速度が出るものとされています。

RAID 5

RAID 5 はレベル 0 と 1 を統合したもので、性能と冗長性の両方を備えています。領域のサイズは、全てのハードディスクサイズの合計から 1 台分を引いたサイズになります。データは RAID 0 のようにハードディスク内に分散して書き込まれますが、さらに **パリティブロック** と呼ばれるものが、安全上の理由からいずれかのパーティション内に作成されます。パリティは XOR と呼ばれる形式で作成するもので、これによりシステム障害が発生してもパリティブロックから元のデータを作り直すことができるようになっています。RAID 5 では 1 台のディスクが故障してもデータに問題はありませんが、複数台が同時に故障するとデータが修復できなくなります。データ損失を防ぐには、1 台のハードディスクが故障した段階で、早急に交換することが必要になります。

RAID 6

RAID システムに対してさらなる信頼性を提供するには、RAID 6 を使用するのがよいでしょう。このレベルでは、同時に 2 台のディスクが故障してもアレイを復元させることができます。RAID 6 では、最低でも 4 台のハードディスクが必要です。なお、ソフトウェア RAID として構築している場合、この設定を使用すると CPU 時間とメモリがそれなりに消費されます。

RAID 10 (RAID 1+0)

この RAID 実装は RAID 0 と RAID 1 を組み合わせたものです：データは複数のディスクに複製されたあと、それぞれの RAID 0 のアレイに書き込まれます。それぞれの RAID 1 アレイでは、1 台までのディスク障害に耐えられます。RAID 10 は、主にデータ ベースアプリケーションのような、負荷の高い用途に使用されます。

その他の RAID レベル

上記以外にも RAID のレベルがいくつか存在しています (RAID 2, RAID 3, RAID 4, RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50 など)。これらの中にはハードウェアの製造元で独占的な実装を行なっているものもあります。これらのレベルはいずれも汎用的なものではないので、ここでは説明をしません。

3.3.1 YaST を利用した RAID 設定

YaST からの RAID 設定は、YaST の熟練者向けパーティション設定内から行なうことができます (詳しくは 3.1 項「YaST パーティション設定の利用」(75 ページ)をお読みください)。熟練者向けパーティション設定では既存のパーティションを編集したり削除したり することができるほか、新しい RAID を作成することもできます:

- 1 ハードディスク からハードディスクを選びます。
- 2 パーティション タブに切り替えます。
- 3 **追加** を押し、このディスクに作成する RAID パーティション のサイズを指定します。
- 4 **パーティションをフォーマットしない** を選択し、**ファイルシステム ID** に *0xFD Linux RAID* を選択します。このパーティションはフォーマットしないでください。
- 5 上記までの手順を、必要な物理ボリューム数だけ繰り返してください。

RAID 0 と RAID 1 の場合は、少なくとも 2 つのパーティションが必要です; RAID 1 の場合は通常、2 つだけを指定します。RAID 5 の場合は、少なくとも 3 つのパーティションが必要です。また、いずれの RAID レベルであっても、同じサイズのパーティションを 作成し、設定することをお勧めします。さらに RAID パーティションは、ディスクの故障によるデータ損失を防ぐため (RAID 1 と RAID 5 の場合)、または最大限の性能を引き出すため (RAID 0 の場合)、異なるディスク上に配置すべきものです。RAID で使用する全てのパーティション を作成したら、**RAID > RAID の追加** を押して RAID の設定を開始してください。

次のダイアログでは、RAID のレベルを 0, 1, 5, 6, 10 から選択します。そのあと、RAID システムで使用する全ての「Linux RAID」または「Linux native」パーティションを選択します。スワップパーティションや DOS パーティションは表示されません。

図 3.6 RAID パーティション



選択した RAID ボリュームに対して、未割り当てのパーティションを追加するには、対象のパーティションを選択して**追加**を押してください。ここでは RAID に使用する全てのパーティションを割り当ててください。割り当てを行なわないと、そのパーティションは未使用のままになります。全てのパーティションを割り当てたら、**次へ**を押して利用可能な RAID オプションを選択します。

手順の最後では、使用するファイルシステムと暗号化、その RAID ボリュームのマウントポイントをそれぞれ設定します。設定が全て終わったら、**完了**を押してください。熟練者向けパーティション設定では、デバイス `/dev/md0` と RAID と書かれたパーティションが表示されるはずです。

3.3.2 トラブルシューティング

RAID パーティションに障害が発生しているかどうかは、`/proc/mdstat` ファイルから確認してください。何らかの障害が発生していた場合は、Linux システムをシャットダウンし、障害の発生しているハードディスクを新しいものに交換してから、同じ方法でパーティションを設定してください。その後システムを起動し、`mdadm /dev/mdX --add /dev/sdX` (X はお使いのデバイス 識別子に置き換えてください) コマンドを実行すると、RAID システムへの統合と再構築が始まります。

なお、再構築中でもデータにアクセスすることは可能ですが、RAID が完全に構築完了するまでの間は、性能面での問題に遭遇する可能性があります。

3.3.3 さらなる情報

ソフトウェア RAID に関する設定の詳細や、さらなる情報については、下記をお読みください:

- `/usr/share/doc/packages/mdadm/Software-RAID.HOWTO.html` (英語)
- <http://raid.wiki.kernel.org> (英語)

Linux RAID メーリングリスト (英語) もご利用いただけます。<http://marc.info/?l=linux-raid> をご覧ください。

パート II. システム

64 ビット環境における 32 ビットおよび 64 ビットアプリケーション

openSUSE® は 64 ビット環境でも ご利用いただけます。これは、必ずしも全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たことを示しているわけではありません。また、openSUSE は 64 ビット環境下での 32 ビットアプリケーションの使用についてもサポートしています。この章では、64 ビットの openSUSE プラットフォームがどの程度サポートされているのかについて、概要を示しています。それ以外にも、32 ビットアプリケーションがどのように実行されるのか (ランタイム サポート) や、32 ビットと 64 ビットの両方の環境で動作する 32 ビット アプリケーションは、どのようにコンパイルされるべきかについても述べています。さらに、64 ビットカーネルで 32 ビットアプリケーションを動作させるにあたっての カーネル API や、その他の説明などについても記しています。

また、64 ビット環境 である amd64 と Intel 64 向けの openSUSE は、既存の 32 ビットアプリケーションを「そのまま」利用することができます。これは、32 ビットアプリケーションが 64 ビット対応になるのを待つことなく、お使いのアプリケーションを使い続けられることを意味しています。

4.1 ランタイムサポート

重要: アプリケーションバージョン間の矛盾

あるアプリケーションについて、32 ビットと 64 ビットの両方の版が用意されている場合、両方の版を同時にインストールしてしまうと、問題を引き起こしてしまいます。この場合、2 つの版のどちらをインストールするのかを決めておき、いずれか片方だけをインストールしてください。

唯一の例外は PAM (pluggable authentication modules) です。openSUSE では、ユーザとアプリケーションの間を調整する認証プロセスとして PAM を使用しています。32 ビットアプリケーションも動作する 64 ビット オペレーティングシステムでは、常に両方の版の PAM モジュールをインストールしておく必要があります。

正しく動作させるため、それぞれのアプリケーションは様々なライブラリを必要とします。これらライブラリの 32 ビット版と 64 ビット版は、いずれも同じ名前が設定されています。それぞれは間違えないよう、何らかの方法で区別しなければなりません。

32 ビットバージョンとの互換性を確保するため、従来の (32 ビット版の) ライブラリは 32 ビット環境の場合と同じ場所に保存されます。32 ビット版の `libc.so.6` は、32 ビット環境でも 64 ビット環境でも `/lib/libc.so.6` に配置されています。

また、全ての 64 ビット版ライブラリとオブジェクトファイルは、`lib64` と呼ばれる場所に配置されます。従来は `/lib` や `/usr/lib` に配置されていたオブジェクトファイルの 64 ビット版は、それぞれ `/lib64` や `/usr/lib64` に配置されるようになっていきます。逆に言うと、`/lib` や `/usr/lib` は 32 ビット版のライブラリを配置する領域として機能することになるため、いずれのバージョンであっても変更することなくご利用いただけることになります。

ただし、32 ビット版の `/lib` 配下のサブディレクトリに配置していた、ビット数に依存しないデータコンテンツについては、従来通りの配置になっています。この方式は LSB (Linux Standards Base) と FHS (File System Hierarchy Standard) に準拠しています。

4.2 ソフトウェア開発

両対応の開発ツールチェーンを利用すると、32 ビットと 64 ビットの両方のオブジェクトを生成することができます。既定では 64 ビットオブジェクトを生成しますが、32 ビットオブジェクトを生成する際には、特殊なフラグを指定する必要があります。gcc の場合、`-m32` を指定します。

また、全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記述しておく必要があります。インストール済みの 32 ビットおよび 64 ビットライブラリには、インストール済みのヘッダファイルに対応した API (アプリケーション プログラミングインターフェイス) が含まれていなければなりません。通常の openSUSE 環境は、この方針に則った形になっています。ライブラリを手動で更新するような場合は、これらの問題をご自身で解決する必要があります。

4.3 両プラットフォーム対応のソフトウェアコンパイル

両方のアーキテクチャに対応したバイナリを開発するには、それぞれ関連するライブラリに対するもう一つのアーキテクチャ版をインストールしておかなければなりません。これらのパッケージは (RPM 名)-32bit のような名前になっています。また、(RPM 名)-devel のような開発パッケージであれば、(RPM 名)-devel-32bit のような名前で開発パッケージも提供されています。

多くのオープンソースプログラムでは、autoconf をベースにしたプログラム設定を行なっています。もう 1 つの (たとえば 32 ビット) 版に対応するプログラムをコンパイルするよう autoconf で設定を行なうには、configure スクリプトを実行する際に通常のコンパイラおよびリンカーの設定を上書きし、追加の環境変数を設定してください。

下記の例では、x86_64 システムで x86 をもう 1 つのアーキテクチャとして使用しています。

- 1 32 ビットコンパイラを使用するには:

```
CC="gcc -m32"
```

- 2 32 ビットオブジェクトを処理するようリンカーに指示するには (gcc をリンカーのフロントエンドとして使用する場合):

```
LD="gcc -m32"
```

- 3 32 ビットオブジェクトを生成するようアセンブラに指示するには:

```
AS="gcc -c -m32"
```

- 4 32 ビット版のライブラリの場所を指定するなど、リンカのフラグを設定するには:

```
LDFLAGS="-L/usr/lib"
```

- 5 32 ビット版のオブジェクトコードライブラリの場所を指定するには:

```
--libdir=/usr/lib
```

- 6 32 ビット版の X ライブラリの場所を指定するには:

```
--x-libraries=/usr/lib
```

必ずしも全ての変数指定がそれぞれのアプリケーションに必要というわけではありません。それぞれプログラムの要件に従って指定してください。

```
CC="gcc -m32"  
LDFLAGS="-L/usr/lib;"  
./configure --prefix=/usr --libdir=/usr/lib --x-libraries=/usr/lib  
make  
make install
```

4.4 カーネル仕様

x86_64 向けの 64 ビットカーネルでは、64 ビットと 32 ビットの両方のカーネル ABI (アプリケーションバイナリ インターフェイス) を提供しています。32 ビット版の ABI は、32 ビット カーネルが提供するものと同じものです。これにより、32 ビットアプリケーションは 32 ビットカーネルの場合と同様に、64 ビットカーネルと対話することができる、ということになります。

64 ビットカーネルが提供するシステムコールの 32 ビット版には、全ての API が提供されているわけではありません。対応可否はプラットフォームによって異なります。このため、たとえば `lspci` などの少数のアプリケーションについては、コンパイルし直す必要があります。

また 64 ビットのカーネルは、そのカーネル向けにコンパイルされた 64 ビットのカーネルモジュールのみを読み込むことができます。32 ビット版のカーネルモジュールを読み込むことはできません。

ヒント: カーネルの読み込みモジュール

アプリケーションによっては、個別のカーネルモジュールを必要とする場合があります。このような 32 ビットアプリケーションを 64 ビットシステムの環境で使いたい場合は、そのアプリケーションの製造元と SUSE に対して 64 ビット版のカーネルモジュールを提供していないかどうか、および 32 ビット版に対応したカーネル API が存在しているかどうか、それぞれお尋ねください。

Linux システムの起動

Linux システムの起動には、様々なコンポーネントや処理が関わっています。ハードウェア それ自身は BIOS または EFI で初期化され、その後にブートローダからカーネルを読み込みます。この処理が終わると、制御はオペレーティングシステム側に移行し、systemd での処理が始まります。systemd では「ターゲット」と呼ばれる仕組みが用意されていて、日々の使用形態に沿った設定とシステムメンテナンス 作業時の設定の両方を、保持しておくことができるようになっています。

5.1 Linux の起動処理

Linux の起動処理は、それぞれ異なるコンポーネントで提供される複数のステージから構成されています。下記の一覧では起動処理の概要と、利用されるコンポーネントのうちよく知られたものについて述べています:

1. **BIOS/UEFI** コンピュータの電源を入れると、BIOS や UEFI は画面とキーボードを初期化し、メインメモリのテストを行ないます。この時点では、まだマストレージメディア (ハードディスクなど) にはアクセスを行ないません。また、現在の日時や重要な周辺機器に関する情報を、CMOS から読み込みます。1 台目のハードディスクとそのジオメトリ情報を読み込むと、システム処理は BIOS または UEFI からブートローダに渡されます。なお、BIOS/UEFI がネットワーク起動に対応している環境の場合、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 システムでは PXE ブートを行なう必要があります。その他のアーキテクチャでは、一般に BOOTP プロトコルを利用してブートローダを取得します。

2. **ブートローダ** 1 台目のハードディスクにある冒頭の 512 バイトがメインメモリに読み込まれ、そのセクタの冒頭にある **ブートローダ** の処理が始まります。ブートローダで実行するコマンドは、残りの起動処理を行なうための作業になります。そのため、1 台目のハードディスクにある冒頭の 512 バイトは、**マスターブートレコード (MBR)** と呼ばれます。ブートローダはその後、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) に処理を移します。Linux のブートローダである GRUB について、詳しくは 第7章 **ブートローダ GRUB** (129 ページ) をお読みください。ネットワークからの起動を行なう場合、BIOS/UEFI がブートローダとして動作します。ブートサーバから起動イメージを読み込み、システムを起動する 動作です。これはローカルハードディスクとは無関係に、完全に独立した形で動作します。
3. **カーネルと initramfs** システムの制御権を渡す目的で、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) をメモリ内に読み込みます。initramfs の内容はカーネルから直接利用できる形式で、init と呼ばれる小さな実行ファイルが含まれており、実際の ルートファイルシステムをマウントするまでの処理を行ないます。マストレージ (ハードディスクなど) にアクセスする際に特別なハードウェアドライバが必要な場合、それらのドライバは initramfs 内に存在していなければなりません。initramfs について、詳しくは 5.1.1 項「initramfs」(105 ページ) をお読みください。お使いのシステムにローカルのハードディスクが接続されていない場合、initramfs にはカーネルに対応するルートファイルシステムが指定されていなければなりません。これは iSCSI や SAN などのネットワークブロック デバイスでもかまいませんし、NFS をルートデバイスとして指定することもできます。

注記: init プロセスの名称について

一般的には、下記の 2 種類を「init」と表現します:

- a. ルートファイルシステムをマウントするための、initramfs プロセス
- b. システム自身を設定するための、オペレーティングシステムのプログラム

本章では、前者を「initramfs 内の init」と表現し、後者を「systemd」と表現しています。

4. **initramfs 内の init** このプログラムは正しいルートファイルシステムをマウントするために必要な処理を 全て行なうもので、必要なファイルシステム向けのカーネル機能を提供したり、udev を利用してマストレージ (ハードディスク) コントローラを読み込む機能を提供したりしています。ルートファイルシステムが

検出されると、エラーがないか どうかをチェックして、マウントを行ないます。マウントが成功すると `initramfs` は解放され、ルートファイルシステム内の `systemd` を実行します。`initramfs` 内の `init` について、さらに詳しい情報は 5.1.2 項「`initramfs` 内の `init`」(106 ページ)をお読みください。また、`udev` について詳しくは 第10章 *udev* による動的なカーネルデバイス管理 (189 ページ)をお読みください。

5. **systemd** `systemd` は実際のシステム起動処理と、その他のファイルシステムに関する マウント処理を行ないます。`systemd` に関する詳しい説明は、第6章 *systemd* デーモン (109 ページ)をお読みください。

5.1.1 `initramfs`

`initramfs` は小さな `cpio` 形式のアーカイブで、カーネルはこのアーカイブを RAM 内に読み込むことができます。このアーカイブは、実際のルート ファイルシステムが マウントされるまでに必要な、最小限の Linux 環境です。この最小限の Linux 環境は BIOS や UEFI ルーチンからメモリ内に読み込まれるもので、十分なメモリサイズが 存在すること以外に、ハードウェアに対する要件がありません。また `initramfs` のアーカイブには、ルートファイルシステム内の `systemd` プログラムを呼び出すことのできる、`init` と 呼ばれる実行形式が存在しなければなりません。

ルートファイルシステムがマウントできるようになり、オペレーティングシステムが 起動できる状態になるよりも前の段階で、カーネル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、必要なドライバを読み込む必要があります。これらのドライバは、ハードディスクドライブの種類に対応した特別なドライバか、もしくは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の形式になっています。つまり、ルートファイルシステムにアクセスするのに必要なモジュールは `initramfs` 内の `init` によって読み込まれることになります。モジュールを読み込んだ後は、`udev` が `initramfs` とそれに必要なデバイスを提供します。ルートファイルシステムへの変更が完了した後は、デバイスを再生成する必要があります。この処理は `systemd` の `udev.service` が実施するもので、`udevtrigger` のコマンドを実行することで実現しています。

インストール済みのシステムに対してハードウェア (たとえばハードディスク) の 変更を行なう必要があり、カーネルが起動する際に今とは異なるドライバを読み込む 必要がある場合は、`initramfs` を更新しなければなりません。この作業は、`mkinitrd` を呼び出すことで行なうことができます。なにも パラメータをつけずに `mkinitrd`を実行すると、`initramfs` を生成します。`mkinitrd -R`と入力すると、`init` という実行ファイルを生成します。`openSUSE®` では、読み出すべきモジュールの一覧を `/etc/sysconfig/kernel` ファイル内の `INITRD_MODULES` で指定しま

す。インストールが完了すると、上記の変数は自動的に正しい値に設定されます。各モジュールは INITRD_MODULES 内に記述した順に読み込まれます。

重要: initramfs や init の更新

ブートローダは initramfs や init を、カーネルと同じ方法で読み込みます。initramfs や init を更新した場合でも、GRUB を再インストールする必要はありません。これは GRUB が起動する際に正しいファイルを検索する仕組みを備えているためです。

5.1.2 initramfs 内の init

initramfs 内にある init は、実際のルートファイルシステムをマウントするための準備作業と、実際のルートファイルシステムへのアクセス作業を主な目的としています。お使いのシステム設定によって、initramfs 上の init はそれぞれ下記のような作業を行ないます。

カーネルモジュールの読み込み

お使いのハードウェア設定によって、お使いのコンピュータのハードウェアにアクセスするためのドライバが必要となります (最も重要なコンポーネントはハードディスクです)。また、最終的なルートファイルシステムにアクセスするため、カーネルでは適切なファイルシステムドライバも必要です。

ブロックスペシャルファイルの提供

それぞれ読み込んだカーネルモジュールでは、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、必要なブロックスペシャルデバイスを /dev 内にある RAM ファイルシステム内に作成します。これらのスペシャルファイルが存在しないと、ファイルシステムやその他のデバイスにアクセスすることができません。

RAID と LVM の設定管理

お使いのシステムにおけるルートファイルシステムが RAID や LVM の管理下にある場合、initramfs 内の init は LVM や RAID を設定し、後にアクセスすることになるルートファイルシステムを読み込むことができますようにします。RAID や LVM について、詳しくは 第3章 *高度なディスク設定* (75 ページ) をお読みください。

ネットワーク設定の管理

お使いのシステムでネットワークマウント型のルートファイルシステム (NFS を介したマウント) を利用している場合、initramfs 内の init は適切なネット

ワークドライバを読み込み、ルート ファイルシステムへのアクセス手段を準備しなければなりません。

ファイルシステムが iSCSI や SAN のようなネットワークブロックデバイス上に存在する場合は、initramfs 内の init でストレージサーバへの接続も設定する必要があります。

インストール作業の初期段階で initramfs 内の init が呼び出された場合は、上述の手順とは異なる 下記の手順が行なわれます:

インストールメディアの検出

インストール処理を開始する際、お使いのマシンはインストールメディア上にあるインストール用のカーネルと、YaST インストーラの存在する init を読み込みます。YaST インストーラは RAM ファイル システム内で動作するもので、インストールメディアにアクセスしてインストール作業を行ないます。そのため、その場所に関する情報を事前に知っておく必要があります。

ハードウェアの検出と適切なカーネルモジュールの読み込み

5.1.1項「initramfs」(105 ページ) に示しているとおり、起動処理は多くのハードウェア環境で動作するドライバを含んだ最低限のドライバセットで行なわれます。init はお使いのハードウェア環境での適切なドライバを判断するため、初期の ハードウェア検出処理を行ないます。起動処理に必要であると判断したモジュール 名は、/etc/sysconfig/kernel 内の INITRD_MODULES に書き込まれます。モジュール名の 一覧は、システムを起動する際に使用するカスタムな initramfs の作成に利用します。起動時には必要がないものの、あとから読み出す必要があるモジュール については、/etc/sysconfig/hardware/hwconfig-* 内に書き込まれます。このディレクトリ内の設定ファイル内に記述された 全てのデバイスは、起動処理で初期化されます。

インストールシステムの読み込み

ハードウェアを正しく検出して適切なドライバが読み込まれると、udev はスペシャルデバイスファイルを 作成し、init は実際の YaST インストーラである インストールシステムを起動します。

YaST の起動

最後に init は YaST を起動し、パッケージの インストールやシステムの設定を行ないます。

systemd デーモン

systemd プログラムは、プロセス ID が 1 であるプロセスです。これはシステム の起動時に、その初期化処理を指定通りの方法で行なうために利用します。systemd はカーネルから直接起動して使用するもので、通常はプロセスを kill するために使用するシグナル 9 を、無視して動作します。その他のプログラム は systemd から直接起動されるか、もしくは直接起動されたプロセスの子や孫の プロセスとして起動されることになります。

注記: System V init と systemd の違いについて

完全な互換性を確保する目的で、systemd と System V init は、それぞれ その場で置き換えて使用することができます。systemd ではなく System V init を使用したい場合は、起動画面で F5 を押し、*System V* を選択してください。また、System V init を 今後も恒久的に使用したい場合は、sysvinit-init パッケージをインストールし、systemd-init パッケージと入れ替えてください。

openSUSE 12 以降のバージョンでは、System V init デーモンは systemd に置き換えられるようになりました。systemd は System V init との完全な 互換性 (init スクリプトに対応しているため) があるほか、systemd では サービスの起動を同時並行で行なう仕組みになっているため、起動にかかる時間が 大きく短縮されています。これに加えて、systemd ではサービスを必要なときに だけ起動します。たとえば印刷用のデーモンである cupsd はシステムの起動時には開始されませんが、起動後にはじめてユーザが文書を 印刷しようとしたときに起動されます。また、systemd ではカーネルの コントロールグループ (cgroups) にも対応しているほか、システムの状態を スナップショットに保存したり、その状態に復元したりすることもできます。詳しくは <http://www.freedesktop.org/wiki/Software/systemd/> をお読みください。

6.1 基本的な使いかた

System V init の仕組みでは、複数のコマンドを利用してサービスを処理していました。init スクリプトや insserv, telinit などのコマンドがそれにあたります。systemd では、サービスに対する主な処理を実行する際、コマンド 1 つで済むようになっています。それが systemctl で、git や zypper のように、コマンドの後ろにサブコマンドを指定して実行します：

```
systemctl [一般オプション] サブコマンド [サブコマンドのオプション]
```

詳しくは、man 1 systemctl で表示されるマニュアルページをお読みください。

ヒント: 端末の出力と bash の補完について

systemd のコマンドは、出力先が端末である場合 (パイプやファイルなどでない場合)、既定ではページャ機能が動作し、長い出力を順に読むことができるようになっています。この機能を無効化するには、--no-pager オプションをご利用ください。

systemd では、bash による補完にも対応しています。サブコマンドの頭文字 1 文字を入力し、を押すと、サブコマンドの残りを自動的に入力することができます。ただし、この機能は、bash シェルを利用している場合にのみ使うことができるもので、bash-completion パッケージをインストールしておく必要があります。

6.1.1 動作中のシステムに対するサービスの管理

サービスを管理するためのサブコマンドは、System V init でのサービス管理 コマンドと同じ (start, stop, ...) です。一般的な使い方は下記のとおりです：

systemd

```
systemctl reload|restart|start|status|stop|... <my_service(s)>.service
```

SysV init

```
rc<サービス名> reload|restart|start|status|stop|...
```

systemd では、複数のサービスを一括で管理することもできます。init スクリプトをそれぞれ実行しなければならなかった System V init とは異なり、下記のように実行します：

```
systemctl start <1 つめのサービス>.service <2 つめのサービス>.service
```

下記の表には、systemd と System V init におけるサービス管理コマンドを、それぞれ並べています:

表 6.1 サービス管理コマンド

作業	systemd でのサブ コマンド	SysV init でのサブコ マンド
起動	start	start
停止	stop	stop
再起動 サービスを停止し、その後に起動し直します。その時点でサービスが起動していなかった場合は、起動する場合と同じ意味になります。	restart	restart
条件付きの再起動 サービスが現在動作中の場合、サービスを再起動します。動作していなかった場合は、何も行ないません。	try-restart	try-restart
再読み込み サービスの動作を止めることなく、そのサービスに対する設定 ファイルを読み込み直します。これはたとえば、Apache に対して修正後の httpd.conf を読み込ませたりする、などの 使い方をします。全てのサービスが再読み込みに対応しているとは 限らないことに注意してください。	reload	reload
再読み込みまたは再起動 指定のサービスが再読み込みに対応していればそれを行ない、対応し	reload-or-restart	n/a

作業	systemd のサブ コマンド	SysV init でのサブコ マンド
<p>ていなければ再起動を行いません。 その時点でサービスが動作してい なかった場合は、単純に起動を行な います。</p>		
<p>条件付きの再読み込みまたは再起 動</p> <p>指定のサービスが再読み込みに対 応していればそれを行ない、対応し ていなければ再起動を行いません。 その時点でサービスが動作してい なかった場合は、何も行ないません。</p>	reload-or-try-restart	n/a
<p>詳細な状態情報を取得する</p> <p>サービスの状態について、情報を 表示します。systemd のコマンド では、説明や実行ファイル、状態や CGroup のほか、直近でサービス が出力したメッセージなど (詳し くは 6.1.2 項「サービスのデバッ グ」(113 ページ) をお読みくださ い) を表示します。SysV init とは、 表示される詳細のレベルが異なりま す。</p>	status	status
<p>簡潔な状態情報を取得する</p> <p>サービスが動作しているかどうかを 表示します。</p>	is-active	status

6.1.2 サービスのデバッグ

既定では、systemd は過剰に冗長な出力を行いません。サービスの起動が成功した場合は何も出力されず、失敗した場合にのみ短いエラーメッセージを表示します。起動についてデバッグしたり、サービスの操作状態を確認したりしたい場合は、systemctl status コマンドをお使いください。

systemd は、独自のログ機構（「ジャーナル」と呼びます）で システムメッセージを記録します。これにより、サービスの状態メッセージと、そのサービスから出力されたメッセージの両方を表示できるようになっています。また、status コマンドは tail コマンドに似た動作をするようになっています。また、ログメッセージを様々な形式で表示することもできます。これにより、便利なデバッグツールとして 利用できるようになっています。

サービスの起動失敗に関する詳細表示

サービスの起動に失敗した場合は、systemctl status <サービス名>.service のように 実行することで、詳細なエラーメッセージを表示することができます：

```
www.example.com: ~ # systemctl start apache2.service
Job failed. See system journal and 'systemctl status' for details.
www.example.com: ~ # systemctl status apache2.service
  Loaded: loaded (/lib/systemd/system/apache2.service; disabled)
  Active: failed (Result: exit-code) since Mon, 04 Jun 2012 16:52:26 +0200; 29s ago
 Process: 3088 ExecStart=/usr/sbin/start_apache2 -D SYSTEMD -k start (code=exited,
 status=1/FAILURE)
   CGroup: name=systemd:/system/apache2.service

Jun 04 16:52:26 g144 start_apache2[3088]: httpd2-prefork: Syntax error on line
205 of /etc/apache2/httpd.conf: Syntax error on li...alHost>
```

直近 n 行分のサービスメッセージの表示

status サブコマンドは、既定ではサービスが出力した メッセージのうち、直近の 10 行を表示します。表示する行数を変更したい 場合は、--lines= n パラメータを指定して実行してください：

```
systemctl status ntp.service
systemctl --lines=20 status ntp.service
```

追記モードによるサービスメッセージの表示

サービスからのメッセージを「リアルタイムに」表示したい 場合は、--follow オプションを利用します。これは tail -f に似た動作をするものです：

```
systemctl --follow status ntp.service
```

メッセージの出力形式の指定

サービスメッセージの出力形式を変更したい場合は、`--output= モード` パラメータを指定してください。主なモードには、下記のようなものがあります:

`short`

既定の形式です。ログメッセージそのもののほか、人間が読みやすい形式でタイムスタンプが併記されます。

`verbose`

全ての項目を表示する形式です。

`cat`

タイムスタンプを併記しない、簡潔な出力形式です。

6.1.3 サービスに対する恒久的な有効化／無効化

上述のサービスの管理コマンドでは、現在動作中のシステムに対するサービスの操作を行いません。`systemd` では、サービスを恒久的に有効化／無効化し、必要に応じてシステムの起動時に自動的に開始したり、逆に開始しないようにしたりすることもできます。これは YaST やコマンドラインからも実施することができます。

6.1.3.1 コマンドラインからのサービスの有効化／無効化

下記の表には、`systemd` と System V init におけるサービスの有効化／無効化 コマンドを示しています:

重要: サービスの起動について

コマンドラインからサービスを有効化した場合、動作中のシステムでは サービスが起動されず、次のシステム起動またはランレベル／ターゲット変更 の際に起動されることに注意してください。有効化した際、即時にサービスを 起動したい場合は、`systemctl start <サービス名>.service` または `rc<サービス名> start.` のように、明示的にサービスを起動してください。

表 6.2 サービスの有効化／無効化のコマンド

作業	systemd でのサブコマンド	SysV init でのサブコマンド
有効化	systemctl enable <サービス名>.service	insserv <サービス名>
無効化	systemctl disable <サービス名>.service	insserv -r <サービス名>
確認 サービスが有効に設定されているかどうかを表示します。	systemctl is-enabled <サービス名>.service	n/a
再有効化 サービスを再起動するのと似た仕組みで、このコマンドはいったん無効化した後に有効化します。これはサービスの有効化状態を、既定値に戻したい場合に利用します。	systemctl reenabale <サービス名>.service	n/a
マスク サービスを「無効化」しても、コマンドラインから実行することでサービスは起動できてしまいます。サービスを完全に無効化するには、このようにマスクを設定する必要	systemctl mask <サービス名>.service	n/a

作業	systemd でのサブコマンド	SysV init でのサブコマンド
があります。注意してお使いください。		
マスク解除 マスクを行なった場合は、マスクを解除することで再度起動できるようになります。	systemctl unmask <サービス名>.service	n/a

6.1.3.2 YaST を利用したサービスの有効化／無効化

YaST のモジュールを *YaST* > システム > システム サービス (ランレベル) で起動すると、まずは **簡易モード** で表示されます。これは 利用可能な全てのサービスに対して、概要と状態 (詳しくは 図6.1「システムサービス (ランレベル)」(117 ページ) をご覧ください) が表示されるだけのものです。左側の列にはサービスの名前が、中央の列にはサービスの状態が、右側の列には短い説明が表示されます。サービスを選択すると、下側により詳しい説明が表示されます。サービスを有効化するには、表から対象のサービスを選択して **有効にする** を選択してください。サービスを無効化する場合も同様です。

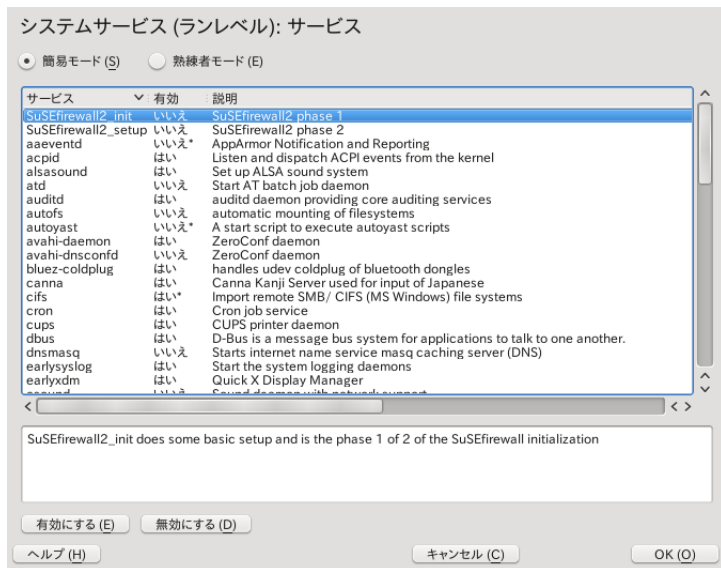
熟練者モード は、ランレベル (詳しくは 6.2.1 項「ターゲットとランレベル」(118 ページ) をお読みください) を詳細に制御するために使用するモードです。現在の既定のランレベルは、画面上部に表示されます。通常、openSUSE システムにおける既定のランレベルは 5 (ネットワークと X Window System を動作させるマルチユーザ環境) です。場合によっては ランレベル 3 (ネットワークを動作させるマルチユーザ環境) が設定されている 場合もあります。

ウインドウ内の表を利用することで、個別のサービスやデーモンを有効化したり無効化したりすることもできます。表内には利用可能なサービスやデーモンの一覧が表示され、お使いのシステムで 現在有効化されているかどうかと、どのランレベルに対して有効に設定されているかが表示されます。マウスでいずれかの行 (サービスやデーモン) を 選択したあと、ランレベルを表すチェックボックスで設定を行ってください。また、現在選択されているサービスやデーモンについて、概要説明が表の下に 表示されます。

警告: ランレベル設定の誤りによって発生する障害について

ランレベルの設定を誤ると、場合によってはお使いのシステムが利用できなくなってしまう。設定を適用する前に、どのような影響があるのかをご確認ください。

図 6.1 システムサービス (ランレベル)



開始／中止／更新を押すと、サービスを開始したり停止したりすることができます。状態を更新を押すと、現在の状態を表示することができます。また、セット／リセットを押すと、行なった変更をシステムに適用したり、ランレベルエディタを起動する前の設定に戻したりすることができます。OKを押すと、変更点をディスクに書き込みます。

6.2 システムの起動とターゲットの管理

システムの起動やシャットダウンに関する全ての処理は、systemd が管理します。このような観点からすると、カーネルは他の全てのプロセスを管理するバックグラウンド (裏側の) プロセスであり、他のプログラムが要求する CPU 時間やハードウェアアクセスを調整する仕組みと考えられます。

6.2.1 ターゲットとランレベル

System V init の環境では、システムは「ランレベル」と呼ばれる 仕組みを利用して起動していました。ランレベルとは、システムやサービスの起動 方法を定義するもので、それぞれ番号を付けて区別していました。よく知られているランレベルとしては、0 (システムのシャットダウン)、3 (ネットワークまでを動作させるマルチユーザ環境)、5 (ネットワークとディスプレイマネージャを動作させる マルチユーザ環境) などがあります。

systemd では、「ターゲットユニット」と呼ばれる新しい仕組みを利用しています (もちろん従来のランレベルの考え方についても、完全な互換性を 備えています)。ターゲットユニットは、番号ではなく名前で識別する仕組みで、それぞれ異なる目的を示しています。たとえば `local-fs.target` や `swap.target` は、それぞれローカルのファイルシステムのマウント、スワップ領域のマウントなどを表わします。

`graphical.target` というターゲットは、ネットワークと ディスプレイマネージャを動作させるマルチユーザ環境で、ランレベル 5 と同じ意味を持っています。このようなターゲットは「メタ」ターゲットと呼ばれるもので、他のターゲットをまとめてセットにしたものを 指しています。このように、systemd は既存のターゲットを組み合わせることで、簡単に独自のターゲットを作成できるため、非常に柔軟な運用を行なうことができます。

下記の表では、systemd で利用される最も重要なターゲットを示しています。全てを網羅した表については、`man 7 systemd.special` で表示 されるマニュアルページをお読みください。

systemd のターゲットユニット

`default.target`

システムの起動時に既定で選択されるターゲットです。これは「実在する」というよりは、他のターゲット (たとえば `graphic.target`) に対するシンボリックリンクという意味合いです。このターゲットは YaST から 恒久的に変更することができる (詳しくは 6.1.3.2 項「YaST を利用したサービスの有効化／無効化」(116 ページ) をお読みください) ようになっています。一時的に変更したい場合は、システムの 起動時、カーネルのコマンドラインオプションに `systemd.unit=<my_target>.target` を指定してください。

`emergency.target`

コンソール上で非常用のシェルを起動します。システム起動時に `systemd.unit=emergency.target` のように指定して 利用します。

`graphical.target`

ネットワークとマルチユーザに対応し、ディスプレイマネージャを起動します。

`halt.target`

システムをシャットダウンします。

`mail-transfer-agent.target`

メールの送受信に必要な全てのサービスを起動します。

`multi-user.target`

ネットワークとマルチユーザに対応した環境を起動します。

`reboot.target`

システムを再起動します。

`rescue.target`

ネットワーク機能無しのシングルユーザモードを起動します。

System V init ランレベルデーモンとの互換性を維持する目的で、`systemd` では `runlevelX.target` のような名前のターゲットが用意されています。それぞれ *X* の部分がランレベルの番号に対応します。

表 6.3 *System V* のランレベルと *systemd* のターゲットユニット

System V ランレベル	systemd ターゲット	用途
0	<code>runlevel0.target</code> , <code>halt.target</code> , <code>poweroff.target</code>	システムのシャットダウン
1, S	<code>runlevel1.target</code> , <code>rescue.target</code> ,	シングルユーザモード
2	<code>runlevel2.target</code> , <code>multi-</code> <code>user.target</code> ,	ネットワーク機能無しのマル チユーザ環境
3	<code>runlevel3.target</code> , <code>multi-</code> <code>user.target</code> ,	ネットワーク機能のあるマル チユーザ環境
4	<code>runlevel4.target</code>	未使用、または独自に定義 して使用するもの

System V ランレベル	systemd ターゲット	用途
5	runlevel5.target, graphical.target,	ネットワークとディスプレイマ ネージャを起動するマルチ ユーザ環境
6	runlevel6.target, reboot.target,	システムの再起動

重要: systemd における /etc/inittab の有効性について

SysV init のシステムにおけるランレベル管理は /etc/inittab で設定しますが、systemd では、このファイルに書かれた設定を読み込むことは *ありません*。独自のターゲットを作成する方法については、6.2.2項「独自のターゲット」(121 ページ)をお読みください。

6.2.1.1 ターゲットの変更を行なうコマンド

下記のコマンドを使用することで、ターゲットユニットを操作することができます:

処理	systemd でのコマンド	SysV init でのコマンド
現在のターゲット／ランレベルの変更	systemctl isolate <my_target>.target	telinit X
既定のターゲット／ランレベルの変更	systemctl default	n/a
現在のターゲット／ランレベルの取得	systemctl list-units -- type=target	who -r or

処理	systemd のコマンド	SysV init のコマンド
	systemd では通常、複数のターゲットを利用します。そのため、上記のコマンドは現在有効なターゲットを全て表示します。	runlevel
既定のランレベルに対する恒久的な変更	YaST のランレベルエディタを使用するか、もしくは下記のコマンドを実行する: ln -sf /lib/systemd/system/<my_target>.target /etc/systemd/system/default.target	YaST のランレベルエディタを使用するか、もしくは /etc/inittab 内の下記の行を変更する: id:X:initdefault:
システム起動時にランレベルを指定する	システム起動時に、下記のようなオプションを指定する systemd.unit=<my_target.target>	システム起動時に、ランレベルの番号を指定する
ターゲットやランレベルの依存関係を表示する	systemctl show -p "Requires" <my_target.target> systemctl show -p "Wants" <my_target.target> 「Requires」を指定すると、ハード依存関係 (必ず解決されなければならない依存関係) を表示します。 「Wants」を指定すると、ソフト依存関係 (可能であれば解決されるべき依存関係) を表示します。	n/a

6.2.2 独自のターゲット

System V init による SUSE システムでは、ランレベル 4 を利用で独自のランレベル 設定を構築できるようになっていました。systemd では、独自のターゲットを作成

することで、任意の数だけ独自の設定を構築することができます。なお、独自のターゲットを構築する場合は、`graphical.target` など既存のターゲットに追加する形で構築することをお勧めします。

警告: カスタマイズ作業時の注意

`systemd` のカスタマイズは `/etc/systemd` ディレクトリ内で 行ない、`/lib/systemd` 内では決して実施しないでください。後者のディレクトリ内でカスタマイズを行なっても、次の `systemd` の更新の際、変更点が上書きされてしまい、元に戻ってしまいます。

手順 6.1 独自のターゲットの作成

- 1 まずは `/lib/systemd/system/graphical.target` の設定ファイルを、`/etc/systemd/system/<ターゲット名>.target` にコピーします。名前は必要に応じて修正してください。
- 2 以前のステップでコピーした設定ファイルは、既に必須とする (「ハード」) 依存関係を構築してある状態になっています。可能であれば解決しておくべき依存関係 (「ソフト」) を構築したい場合は、`/etc/systemd/system/<ターゲット名>.target.wants` という名称のディレクトリを作成してください。
- 3 あとは `/etc/systemd/system/<ターゲット名>.target.wants` ディレクトリ内に、`/lib/systemd/system` からのシンボリックリンクを 作成することで、ソフト依存関係を設定することができます。
- 4 ターゲットの設定が完了したら、あとは新しいターゲットを利用できるように するため、`systemd` に対して設定の再読み込みを指示します:

```
systemctl daemon-reload
```

6.2.3 システム起動に対するデバッグ

`systemd` には、システムの起動処理を分析できる機能が用意されています。この機能により、全てのサービスに対する状態を (`/var/log` を確認する 方法よりは) 便利に確認することができます。また `systemd` では、起動処理を 調査して、サービスの起動にかかっている時間を調べることもできます。

6.2.3.1 サービスの動作の確認

システムの起動後に開始されたサービスの一覧を確認するには、systemctl とだけ入力します。すると、下記のように、有効に設定されている全てのサービスが表示されます。特定のサービスに対して 詳細を読みたい場合は、systemctl status <サービス名>.service と入力してください。

例 6.1 有効なサービスの一覧表示

```
jupiter.example.com: ~ # systemctl
UNIT                                LOAD  ACTIVE SUB    JOB DESCRIPTION
[...]
systemd-random-seed-load.path      loaded active waiting    Random Seed
acpid.service                      loaded active running    ACPI Event Daemon
apache2.service                   loaded failed failed      apache
avahi-daemon.service              loaded active running    Avahi mDNS/DNS-SD Stack
bluez-coldplug.service            loaded active exited     LSB: handles udev coldplug
  of bluetooth dongles
console-kit...-system-start.service loaded active exited     Console System Startup
  Logging
cron.service                      loaded active running    Command Scheduler
cups.service                      loaded active running    CUPS Printing Service
[...]
LOAD    = Reflects whether the unit definition was properly loaded.
ACTIVE  = The high-level unit activation state, i.e. generalization of SUB.
SUB      = The low-level unit activation state, values depend on unit type.
JOB      = Pending job for the unit.

107 units listed. Pass --all to see inactive units, too.
```

起動に失敗したサービスだけを表示したい場合は、--failed オプションを指定してください:

例 6.2 起動に失敗したサービスの表示

```
jupiter.example.com: ~ # systemctl --failed
UNIT                                LOAD  ACTIVE SUB    JOB DESCRIPTION
apache2.service                   loaded failed failed      apache
NetworkManager.service           loaded failed failed      Network Manager
plymouth-start.service            loaded failed failed      Show Plymouth Boot Screen
[...]

```

6.2.3.2 サービスの起動時間のデバッグ

システムの起動にかかった時間をデバッグしたい場合、systemd では systemd-analyze というコマンドが用意されています。これは全体の起動時間や起動時間

順のサービス一覧を表示することができるほか、他のサービスの起動時間と対比するために利用することのできる、SVG 画像を生成することもできます。

システムの起動時間の表示

```
jupiter.example.com: ~ # systemd-analyze
Startup finished in 2666ms (kernel) + 21961ms (userspace) = 24628ms
```

システムの起動時間の詳細表示

```
jupiter.example.com: ~ # systemd-analyze blame
6472ms systemd-modules-load.service
5833ms remount-rootfs.service
4597ms network.service
4254ms systemd-vconsole-setup.service
4096ms postfix.service
2998ms xdm.service
2483ms localnet.service
2470ms SuSEfirewall2_init.service
2189ms avahi-daemon.service
2120ms systemd-logind.service
1210ms xinetd.service
1080ms ntp.service
[...]
75ms fbset.service
72ms purge-kernels.service
47ms dev-vda1.swap
38ms bluez-coldplug.service
35ms splash_early.service
```

サービスの起動時間を表す画像

```
jupiter.example.com: ~ # systemd-analyze plot > jupiter.example.com-startup.svg
```

6.2.3.3 Review the Complete Start-Up Process

上述のコマンドを利用することで、サービスの開始とそれにかかる時間を確認することができます。さらに詳しい情報を読みたい場合は、systemd に対して 起動処理 に対する冗長ログを採取するように設定します。具体的には、システムの 起動時に、 起動パラメータに下記の値を指定します：

```
systemd.log_level=debug systemd.log_target=kmsg
```

上記を設定すると、systemd はログメッセージをカーネルのリングバッファに 書き込むようになります。閲覧の際は dmesg コマンドをご利用ください：

6.3 高度な使い方

下記の章では、システム管理者に対してより高度な作業内容を示しています。本章よりもさらに高度なドキュメンテーションについては、Lennart Poettering 氏による systemd の資料 (<http://0pointer.de/blog/projects>) (英語) をお読みください。

6.3.1 システムのログ

6.1.2項「サービスのデバッグ」(113 ページ) では、それぞれの サービスに対してログを閲覧するための方法を示してきましたが、ログメッセージは サービスからのものだけであるとは限りません。systemd が記録した全てのログ メッセージ(「ジャーナル」と呼びます) に対するアクセス方法も用意 されています。最も古いログから始まる、全てのログを表示するには、systemd-journalctl コマンドをお使いください。なお、フィルタの適用や出力形式の変更について、詳しくは `man 1 systemd-journalctl` で表示されるマニュアルページをお読みください。

6.3.2 スナップショット

systemd には、現在の状態を名前付きのスナップショットとして保存し、後から `isolate` サブコマンドでその状態に戻す機能が 用意されています。これは元に戻すことができることから、サービスや独自のターゲットの テストに便利な仕組みです。なお、スナップショットは現在のセッションに対してのみ有効で、システムを再起動すると自動的に削除されます。また、スナップショットの名前は `.snapshot` で終わるものでなければなりません。

スナップショットの作成

```
systemctl snapshot <スナップショット名>.snapshot
```

スナップショットの削除

```
systemctl delete <スナップショット名>.snapshot
```

スナップショットの表示

```
systemctl show <スナップショット名>.snapshot
```

スナップショットの有効化

```
systemctl isolate <スナップショット名>.snapshot
```

6.3.3 カーネルのコントロールグループ (cgroups)

従来の SysV init システムでは、起動されるサービスに対して、明確なプロセス 設定を行なうことができませんでした。Apache などのように、サードパーティ製の プロセス (CGI や Java のプロセス) を多数起動し、サードパーティ製のプロセス 自身もプロセスを生成するようなシステムの場合は、プロセスに対する制御を 明示的に 行なうことが難しい場合があるほか、場合によっては不可能であることもあります。 またそれに加えて、子プロセスを残したまま終了してしまい、結果として サービスが 正しく終了しないことも考えられます。

systemd では、そのような問題を cgroups を利用することで解決しています。 cgroups はプロセスをまとめて管理するためのカーネルの機能で、全ての子プロ セスを 階層構造で管理します。systemd では、サービスに対して別々の cgroup を 設定します。非特権プロセスでは cgroup を変えることができないため、サービス から起動したプロセスがどれなのかを、簡単に判別できるようになる、という仕組み です。

サービスに属する全てのプロセスを表示するには、systemd-cgls コマンドを使用し ます。実行すると、下記のように (一部省略しています) 表示されます:

例 6.3 サービスに属する全プロセスの表示

```
~ # systemd-cgls --no-pager
├─ user
│   └─ root
│       └─ 1
│           ├── 2279 sshd: root@pts/0
│           ├── 2282 -bash
│           └─ 2541 systemd-cgls --no-pager
└─ system
    ├── 1 /sbin/init splash showopts
    ├── apache2.service
    │   ├── 2535 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D SYSTEMD -k start
    │   ├── 2536 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D SYSTEMD -k start
    │   ├── 2537 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D SYSTEMD -k start
    │   ├── 2538 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D SYSTEMD -k start
    │   ├── 2539 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D SYSTEMD -k start
    │   └─ 2540 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D SYSTEMD -k start
    └─ xdm.service
```

```

|   | 2250 /usr/bin/xdm
|   | 2253 /usr/bin/X -nolisten tcp -br vt7 -auth /var/lib/xdm/authdir/authfiles/A:0-
ii8Goo
|   | 2263 -:0
|   | 2276 /usr/bin/xconsole -notify -nostdin -verbose -exitOnFail
| ntp.service
|   | 2202 /usr/sbin/ntpd -p /var/run/ntp/ntpd.pid -g -u ntp:ntp -c /etc/ntp.conf
| sshd.service
|   | 1743 /usr/sbin/sshd -D

```

cgroups について、詳しくは 第10章 カーネルのコントロールグループ (↑システム分析とチューニングガイド) をお読みください。

6.3.4 サービスの kill (シグナルの送信)

6.3.3項「カーネルのコントロールグループ (cgroups)」(126 ページ) で説明したとおり、SysV init のシステムでは親プロセスを判断することが不可能になってしまふことがありました。このような状態になってしまうと、サービスから起動された多数のプロセスがわからなくなってしまう、子プロセスはゾンビプロセスとして残ってしまいます。

systemd の cgroups 管理の仕組みにより、サービスから起動された子プロセスを容易に判別し、それらに対してまとめてシグナルを送信することができます。サービスに対してシグナルを送信する場合は、systemctl kill コマンドをお使いください。利用可能なシグナルの一覧は、man 7 signals コマンドで表示することができます。

サービスに対する SIGTERM の送信

SIGTERM は、シグナルを送信する際の既定のシグナルです。

```
systemctl kill <サービス名>.service
```

サービスに対する *SIGNAL* の送信

-s オプションを利用することで、送信するシグナルを指定することができます。

```
systemctl kill -s SIGNAL <サービス名>.service
```

プロセスの選択

既定では、kill コマンドは指定した cgroup 内の all (全ての) プロセスに対してシグナルを送信します。systemd では、control (制御) または main (メイン) のプロセスに対してだけ送信することもできます。後者の場合は、特に SIGHUP を送信して設定を再読み込みさせるような場合に有効です：

```
systemctl kill -s SIGHUP --kill-who=main <サービス名>.service
```

6.4 さになる情報

systemd に対してさらに詳しい情報をご希望の場合は、下記のオンラインリソースをお読みください (いずれも英語です):

Web ページ

<http://www.freedesktop.org/wiki/Software/systemd>

systemd for Administrators

systemd の著者のうちの 1 人、Lennart Pottering 氏によるブログにも、詳しい説明が書かれています。本章記述時点では 13 個の投稿があります。

<http://0pointer.de/blog/projects> からお読みください。

Control Centre: The systemd Linux init system

<http://www.h-online.com/open/features/Control-Centre-The-systemd-Linux-init-system-1565543.html>

Booting up: Tools and tips for systemd, a Linux init tool

<http://www.h-online.com/open/features/Booting-up-Tools-and-tips-for-systemd-1570630.html>

ブートローダ GRUB

本章では、openSUSE® で使用されるブートローダ GRUB (Grand Unified Bootloader) について、その設定方法を説明しています。全ての設定は専用の YaST モジュールを利用して行なうことができます。Linux の起動手順について詳しくない場合は、下記の章をお読み のうえ、起動に関する知識を得てください。また、本章では GRUB で起動する際に発生する 可能性のある問題について、その内容と解決方法についても述べています。

本章では、ブートローダ GRUB を利用した起動の管理と設定方法について述べています。起動処理の全体像については 第5章 *Linux システムの起動* (103 ページ) で述べています。ブートローダはマシン (BIOS) とオペレーティングシステム (openSUSE) の橋渡しをするためのもので、ブートローダの設定を変更すると、オペレーティングシステムの開始 方法について直接的な影響を与えることができます。

本章ではそれぞれ下記の用語を使用しています。説明をよくお読みのうえ、以降を読み進めてください:

MBR (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でそれぞれ独立した仕組みになっています。最初の 446 バイトがプログラムコードとして予約されています。この領域には一般に ブートローダプログラムや、オペレーティングシステムを選択するための仕組みの 一部が書き込まれています。次の 64 バイトは、最大で 4 つまでの定義を行なうことができるパーティションテーブルの領域です。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情報と、そのパーティションの種類が含まれています。オペレーティングシステムは、この一覧を利用してパーティションを処理します。通常の MBR では、必ずいずれか 1 つのパーティ

ションに対して アクティブ のマークが付けられています。MBR の最後の 2 バイトは「マジックナンバー」と呼ばれているもので、固定値 (AA55) が書かれています。マジックナンバーが左記の値でない場合、BIOS は MBR を無効なものとして扱い、起動時に読み込みを行なわなくなります。

ブートセクタ

ブートセクタとはハードディスクのパーティション内にある最初のセクタで、他のパーティションに対する「コンテナ」である拡張パーティション 以外の場所に存在しています。これらのブートセクタは 512 バイトから構成 されていて、それぞれのパーティション内にインストールされている、DOS, windows, OS/2 などのオペレーティングシステムを起動するためのコード領域になっています。また、ブートセクタにはファイルシステム内の特別な情報も保持しています。Linux パーティションのブートセクタには、XFS の場合を除き、ファイルシステム 設定後には何も書かれていません。そのため Linux パーティションは、自分自身にカーネルや有効なルートファイルシステムが含まれていたとしても、自分自身で起動を行なうことができません。なお、起動可能なシステムが含まれるパーティションの場合、MBR と同じマジックナンバー (AA55) が書かれています。

7.1 GRUB での起動

GRUB は 2 つのステージから構成されています。第 1 ステージは 512 バイトから構成されているもので、ブートローダの第 2 ステージを読み出す処理だけを行いません。第 2 ステージがブートローダの中心部分です。

設定によっては、これらの中間である第 1.5 ステージを利用することもできます。このステージは適切なファイルシステムから第 2 ステージを読み込むもので、YaST から GRUB を初期設定したとき、可能であればこの方法がとられます。

第 2 ステージでは様々なファイルシステムにアクセスすることができます。現時点では ext2, ext3, reiserfs, minix, Windows で使用される DOS FAT ファイルシステムにそれぞれ対応しています。拡張機能として、XFS, BSD システムで 使用される UFS, FFS にも対応しています。0.95 以降のバージョンで、GRUB は「El Torito」仕様に準拠した ISO 9660 標準ファイルシステムを含む CD または DVD からの起動も行なうことができるようになりました。また GRUB は、ファイルシステムが起動する前であっても、対応する BIOS ディスクデバイス (BIOS で検出されたフロッピーディスク、ハードディスク、CD/DVD ドライブ) 内に あるファイルシステムにアクセスすることができます。そのため、GRUB の設定 ファイル (menu. lst) を書き換えても、ブートマネージャの インストールをやり直す必要がありません。システムが

起動すると、grub は正しい パスからメニューファイルやカーネルのパーティションデータ、初期 RAM ディスク (initrd)などを再度読み込み、場所を確定します。

GRUB における実際の設定は、下記に示す 4 つのファイルから構成されています：

/boot/grub/menu.lst

このファイルには、GRUB から起動することのできるパーティションやオペレーティングシステムに関する全ての情報が保存されています。この情報が存在しないと GRUB はプロンプトを表示し、ユーザに対して 入力を求める動作を行ないます。詳しくは 7.1.1.3項「起動処理時のメニュー項目編集」(136 ページ)をお読みください。

/boot/grub/device.map

このファイルには、GRUB のデバイス名や BIOS 表記法と Linux のデバイス名の変換情報が記載されています。

/etc/grub.conf

このファイルには、ブートローダを正しくインストールするために必要な、GRUB に対するコマンドやパラメータ、オプションが含まれています。

/etc/sysconfig/boot loader

このファイルは perl-bootloader ライブラリから読み込むことができるもので、YaST からブートローダを設定する際、および新しいカーネルがインストールされた 際に利用されます。このファイルにはカーネルパラメータなどの設定オプションが含まれていて、これらはブートローダの設定ファイルに対して既定で追加されます。

GRUB は様々な方法でコントロールすることができます。既存の設定ファイルにある起動項目はグラフィカルなメニュー (スプラッシュスクリーン) で選択することができます。設定は menu.lst ファイルから読み込みます。

GRUB では、起動を行なう前に全ての起動パラメータを変更することができます。たとえばメニューファイルを編集していたときに存在したエラーを、起動時に変更することも可能です。起動コマンドは入力用のプロンプトから対話的に入力することもできます。詳しくは 7.1.1.3項「起動処理時のメニュー項目編集」(136 ページ)をお読みください。また GRUB は、起動前にカーネルの位置や initrd の位置を指定することもできます。この方法により、ブートローダの設定に存在していないインストール済みオペレーティングシステムを起動することができます。

GRUB には 2 つのバージョンが存在します: ブートローダと、通常の Linux プログラム (/usr/sbin/grub) です。後者は *GRUB シェル* と呼ばれる場合もあります。

GRUB シェルは インストール済みのシステムで GRUB のエミュレーションを行ない、GRUB をインストールしたり新しい設定を適用前に確認したりすることができます。ハードディスクや フロッピディスクのブートローダとして GRUB をインストールする機能は、GRUB の内蔵コマンド `setup` を利用して行ないます。このコマンドは、Linux が読み込まれている場合に GRUB シェルで利用できます。

7.1.1 /boot/grub/menu.lst ファイル

起動メニューでのグラフィカルなスプラッシュスクリーンは、GRUB の設定ファイル `/boot/grub/menu.lst` を基礎にしています。このファイルには そのほか、このメニューから起動可能な全てのパーティションとオペレーティングシステムに関する情報も含まれています。

システムが起動する際、GRUB は常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。そのため、GRUB はメニューファイルを変更した場合であっても、再インストールを行なう必要はありません。GRUB の設定ファイルを変更するには、7.2 項「YaST を利用したブートローダの設定」(141 ページ) に書かれている手順で YaST ブートローダモジュールをお使いください。

メニューファイルにはコマンドが含まれていますが、文法はとても単純です。シェルのようにして各行にコマンドを記述し、スペースで区切ってオプションの パラメータを指定するだけです。過去のバージョンとの互換性を保つ理由から、コマンドによっては最初のパラメータの冒頭に `=` を入れる ことができますのももあります。コメントは行頭にハッシュ記号 (`#`) を記入します。

メニュー一覧で項目の識別を行なうため、各項目に対して `title` (タイトル) を設定します。キーワード `title` 以降に設定した スペースを含む任意のテキストを、メニュー内の選択オプションとして表示することができます。`title` 以降の行に続くコマンドは、そのメニュー が選択された場合にのみ実行されます。

最も単純なケースは、他のオペレーティングシステムのブートローダに転送することです。そのときに使用するコマンドは `chainloader` で、その後ろに 続くパラメータとして、他のパーティションのブートブロックを示す値を入力します。GRUB では、ブロックの指定を下記のようにして行ないます：

```
chainloader (hd0,3)+1
```

GRUB でのデバイス名については、7.1.1.1 項「ハードディスクとパーティションの名前ルール」(133 ページ) で説明しています。上記の例では、1 台目のハードディスクの 4 つめの パーティションに対して、最初のブロックを指定しています。

また、kernel コマンドを利用すると、カーネルイメージを指定 することができます。最初のパラメータには、パーティション内でのカーネルイメージの パスを指定します。それ以降のパラメータには、カーネルのコマンドラインを指定します。

カーネル内蔵のドライバではルートパーティションにアクセスできなかったり、高度なホットプラグ機能のある Linux システムであったりする場合は、initrd を個別の GRUB コマンドとして指定しなければなりません。initrd コマンドのパラメータは 1 つだけ、initrd に対する パスを指定します。initrd を読み込む場所は読み込んだ カーネルに書き込まれるため、initrd コマンドは kernel コマンドの後に記述しなければなりません。

root コマンドはカーネルと initrd ファイルの指定を単純化 するための仕組みです。root に指定するパラメータは 1 つだけで、デバイスやパーティションを指定します。ここで指定したデバイスは、各コマンドで 個別にパスを指定せず、かつ次の root コマンドが現われない 限り、全てのカーネルや initrd、もしくはその他のファイル パス指定に使用されます。

boot コマンドは各メニュー項目の最後に実行されるコマンド ですが、メニューファイルでは記入する必要はありません。しかしながら、GRUB を対話的に使用している場合は、最後に boot コマンドを入力 しなければなりません。このコマンド自身には何もパラメータを指定しません。単にそれまでに指定したカーネルイメージやチェーンローダを読み出すだけです。

全てのメニュー項目を記入したら、それらの中のいずれかを default (既定の) 項目として指定します。指定を行わない 場合は、最初の項目 (0 を指定した場合と同じ) を選択 します。また、既定の項目を選択するまでのタイムアウトを timeout コマンドで指定することもできます。timeout と default コマンドは通常、メニュー項目よりも前に記述します。ファイルの記入例は 7.1.1.2 項「メニューファイルの例」(134 ページ) にありますので、こちらを参考にしてください。

7.1.1.1 ハードディスクとパーティションの名前ルール

GRUB でハードディスクやパーティションに対して使用する名前付けは、通常の Linux のデバイス名とは異なるものを使用します。BIOS が使用する単純なディスク 列挙の仕組みにとっても似ていて、文法は BSD システムの方式に似たものになっています。また、GRUB では最初のパーティション番号は 0 になっています。つまり、(hd0, 0) は最初のハードディスク内にある 最初のパーティションを意味することになります。一般的なデスクトップマシン の場合、プライマリマスターに接続されているハードディスクのことを指し、Linux のデバイス名で言うと、/dev/sda1 になります。

4 つまで作成できるプライマリパーティションは、それぞれ 0 から 3 までの間に割り当てられています。論理パーティションは 4 以降になります：

```
(hd0, 0)   最初のハードディスクにある最初のプライマリパーティション
(hd0, 1)   2 つめのプライマリパーティション
(hd0, 2)   3 つめのプライマリパーティション
(hd0, 3)   4 つめのプライマリパーティション（一般的には拡張パーティション）
(hd0, 4)   最初の論理パーティション
(hd0, 5)   2 つめの論理パーティション
```

BIOS でのデバイス表記と同じで、GRUB は PATA (IDE), SATA, SCSI, ハードウェア RAID デバイスを区別せずに使用します。BIOS やその他のコントローラで認識される 全てのハードディスクは、BIOS 内で設定した起動順序に従って番号が付けられます。

残念ながら、Linux のデバイス名を正しく BIOS のデバイス名に変換することはできません。この割り当ては特定のアルゴリズムに従って生成され、device.map ファイルに保存されます。必要であれば、このファイルを編集することもできます。device.map に関する情報は、7.1.2 項「device.map ファイル」(137 ページ)をお読みください。

GRUB で完全なパスを指定するには、まず括弧内にデバイス名を指定したあと、パーティション (ファイルシステム) 内でのパスを記述します。なお、パスはスラッシュから書き始めます。たとえば起動可能なカーネルが 最初の PATA (IDE) ハードディスクにおける最初のパーティションに存在する場合、下記のように指定することができます：

```
(hd0, 0)/boot/vmlinuz
```

7.1.1.2 メニューファイルの例

下記は GRUB メニューファイルの構造を示すための例です。下記のインストール例では起動パーティションが /dev/sda5 に、ルートパーティションが /dev/sda7 に、Windows のインストールが /dev/sda1 にそれぞれ 行なわれている場合を想定しています。

```
gfxmenu (hd0,4)/boot/message❶
color white/blue black/light-gray❷
default 0❸
timeout 8❹

title linux❺
    root (hd0,4)
    kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
    initrd /boot/initrd
```

```

title windows❸
    rootnoverify (hd0,0)
    chainloader +1

title floppy❷
    rootnoverify (hd0,0)
    chainloader (fd0)+1

title failsafe❹
    root (hd0,4)
    kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma ¥
    apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
    initrd /boot/initrd.shipped

```

最初のブロックでは、スプラッシュスクリーンの設定を行なっています:

- ❶ /dev/sda5 パーティション内の /boot ディレクトリにある、message ファイルを、背景イメージとして 使用する設定です。
- ❷ 色の設定を行なっています。前景を白、背景を青に設定し、選択しているものを 黒で、選択の背景をライトグレーで表示します。色の設定はスプラッシュスクリーンには影響しません。Esc でスプラッシュスクリーンを抜けた 場合にのみ意味のある設定です。
- ❸ 最初の (0) メニュー項目である title linux を既定の設定として起動します。
- ❹ ユーザ入力が 8 秒間行なわれないと、GRUB は自動的に既定の項目を起動します。自動起動を無効化するには、timeout の行を 削除してください。timeout 0 を設定すると、既定の 項目を即時起動する意味になります。

2 番目の以降のブロックは、様々なオペレーティングシステムを起動するための 設定です。それぞれのオペレーティングシステムの設定は、title で始まります。

- ❺ 最初の項目 (title linux) は、openSUSE を 起動するための項目です。カーネル (vmlinuz) は 最初のハードディスクにおける最初の論理パーティション (ブートパーティション) 内に位置しています。ルートパーティションや VGA モードなどのカーネル パラメータが後に続いています。ルートパーティションの指定は Linux の 名前付けルールに従って /dev/sda7/ と書かれています。これはこの情報を読むのがカーネルであるためで、GRUB はその値について 何も処理を行なわないためです。initrd についても 同様に、最初のハードディスクにおける最初の論理パーティション内に 位置しています。
- ❻ 2 つめの項目は Windows を読み込むための項目です。Windows は最初の ハードディスク (hd0, 0) における最初のパーティション から起動する設定になっています。chainloader +1 のコマンドは、GRUB に対して指定したパーティションで最初のセクタを 読み出して実行するように指定するコマンドです。

- ⑦ 3 つめの項目は、単に BIOS 設定を変更せずにフロッピーディスクから起動するための項目です。
- ⑧ failsafe と書かれている項目は、問題の発生している マシンであっても Linux を起動できるよう、カーネルパラメータをいくつか 指定して起動するための項目です。

メニューファイルは必要な時に変更することができ、GRUB は次の起動時に 変更済みの設定を使用します。設定の変更は、YaST かエディタなどで編集してください。また、代替策として GRUB の機能を利用して一時的に変更することもできます。詳しくは 7.1.1.3 項「起動処理時のメニュー項目編集」(136 ページ) をお読みください。

7.1.1.3 起動処理時のメニュー項目編集

グラフィカルな起動メニューでは、カーソルキーを利用して起動するオペレーティング システムを選択することができます。なお、Linux システムを選択した場合は、起動プロンプトを利用して追加のパラメータを設定することもできます。個別のメニュー項目を直接編集したい場合は Esc を押し、スプラッシュ スクリーンを抜けて GRUB のテキストベースのメニューを表示させてから、E を押します。このようにして変更した内容は、その時点の 起動でのみ有効で、恒久的に適用されることはありません。

重要: 起動処理時のキーボードレイアウト

起動時には英語 (アメリカ英語) キーボードレイアウトだけを利用できます。詳しくは 図「英語キーボードのレイアウト」(↑ スタートアップ) をお読みください。

メニュー項目の編集を行なうと、うまく起動できないシステムに対する修復を行なうことができます。これは、間違ったブートローダの設定を手作業で修正することで、うまく起動するための回避策を入力することができるためです。起動処理内での手動でのパラメータ入力は、システムの設定を恒久的に変更せず、一時的に新しい設定をテストしたりしたい場合にも便利です。

編集モードを有効にしたあと、まずはカーソルキーを利用して編集する行を選択します。ここからさらに E を押すと、選択した行を編集することができます。この方法で、起動処理を行なう前に間違ったパーティション指定や パス指定を修正してください。編集モードを抜けてメニューに戻るには、Enter を押します。メニューから B を押すと、その設定で起動を行ないます。それ以外の処理は、画面下部のヘルプ テキストに表示されています。

起動オプションを恒久的に変更してそれらの設定をカーネルに渡したい場合は、root ユーザで menu.lst ファイルを開き、それぞれ必要なカーネル パラメータを既存の行に設定してください。複数のパラメータはスペースで区切ります:

```
title linux
    root(hd0,0)
    kernel /vmlinuz root=/dev/sda3 追加のパラメータ
    initrd /initrd
```

GRUB は次の起動時に自動で設定したパラメータを読み込みます。YaST ブートローダモジュールからでも同じことを行なうことができます。上記と同様に、新しいパラメータはスペースで区切って指定します。

7.1.2 device.map ファイル

device.map ファイルは、GRUB や BIOS のデバイス名を Linux のデバイス名に変換するためのファイルです。PATA (IDE) と SCSI のハードディスクが 混在するシステムの場合、GRUB は特殊な手順で起動順序を判断しなければなりません。これは GRUB が起動順序の設定を行なっている BIOS 情報にアクセスできない可能性があるためです。GRUB はこの分析結果を /boot/grub/device.map ファイルに保存します。たとえば BIOS で SCSI よりも PATA を優先して起動するように設定しているシステムでは、device.map ファイルは下記ようになります:

```
(fd0) /dev/fd0
(hd0) /dev/sda
(hd1) /dev/sdb
```

もしくは下記のような場合もあります:

```
(fd0) /dev/fd0
(hd0) /dev/disk-by-id/DISK1 の ID
(hd1) /dev/disk-by-id/DISK2 の ID
```

PATA (IDE) や SCSI、もしくはその他のハードディスクは様々な要素に依存していて、Linux ではその割り当てを識別することができないことから、device.map ファイルのある順序を手動で編集することもできます。起動時に何らかの問題が発生した場合は、このファイル内にある順序が BIOS の順序とあっているかどうかを確認し、GRUB プロンプトから必要に応じて一時的に変更してみてください。その設定で Linux システムが問題なく起動するようであれば、YaST ブートローダモジュールやエディタなどを利用して、device.map ファイルを恒久的に変更してください。

device.map ファイルを手作業で変更した場合は、下記のコマンドを入力して GRUB を再インストールしてください。このコマンドを実行すると、device.map ファイルを読み込み直し、grub.conf ファイルにあるコマンドを実行します:

```
grub --batch < /etc/grub.conf
```

7.1.3 /etc/grub.conf ファイル

menu.lst と device.map に続く 3 番目に重要な GRUB の設定ファイルとして、/etc/grub.conf ファイルがあります。このファイルには GRUB シェルに対するコマンドとパラメータが含まれていて、ブートローダを正しくインストールするのに必要なファイルです：

```
setup --stage2=/boot/grub/stage2 --force-lba (hd0,1) (hd0,1)
quit
```

上記の例では GRUB に対し、最初のハードディスクにある 2 番目のパーティション (hd0,1) にブートローダをインストールし、起動イメージが同じパーティション内に存在していることを示しています。--stage2=/boot/grub/stage2 パラメータは、マウント済みのファイルシステムから 第 2 ステージ のイメージをインストールするために 必要なパラメータです。また、BIOS によっては LBA サポートの実装が誤っている 場合があるため、--force-lba を指定してその間違った実装を 無視するように指定しています。

7.1.4 /etc/sysconfig/bootloader ファイル

この設定ファイルは YaST を利用してブートローダを設定した場合、および 新しいカーネルをインストールした場合にのみ使用されるものです。このファイルは、ブートローダの設定ファイル (たとえば GRUB であれば /boot/grub/menu.lst) を書き換える perl-bootloader ライブラリが解釈します。なお、/etc/sysconfig/bootloader ファイルは GRUB 固有の設定ファイルではありません。openSUSE 上にインストールされたブートローダであれば、どのブートローダにも適用されます。

注記: カーネル更新後のブートローダ設定

新しいカーネルがインストールされると、perl のブートローダモジュールは毎回、新しいブートローダの設定ファイル (たとえば GRUB であれば /boot/grub/menu.lst) を /etc/sysconfig/bootloader に設定された既定値で 作成します。カーネルパラメータをカスタマイズしている場合は、/etc/sysconfig/bootloader を適宜変更し、カーネル更新後も必要な設定が反映されるようにしてください。

LOADER_TYPE

お使いのシステムにインストールされているブートローダを指定します (たとえば GRUB や LILO など)。この項目は手動では変更せず、手順 7.6「ブートロー

ダの種類の設定」(146 ページ) に示されている 手順で YaST を利用し、ブートローダを設定してください。

DEFAULT_VGA / FAILSAFE_VGA / XEN_VGA

起動処理時に使用するフレームバッファについて、画面の解像度と色深度の 設定を行いません。これらはカーネルパラメータ vga に渡される値で、それぞれ既定の起動項目のほか、フェイルセーフ (安全設定) や XEN 設定で使用されます。それぞれ下記の値を設定することができます:

表 7.1 画面解像度と色深度の一覧

	640x480	800x600	1024x768	1280x1024	1600x1200
8 ビット	0x301	0x303	0x305	0x307	0x31C
15 ビット	0x310	0x313	0x316	0x319	0x31D
16 ビット	0x311	0x314	0x317	0x31A	0x31E
24 ビット	0x312	0x315	0x318	0x31B	0x31F

DEFAULT_APPEND / FAILSAFE_APPEND / XEN_KERNEL_APPEND

ブートローダの設定ファイル内で、既定の項目やフェイルセーフ設定、および XEN の起動項目に設定する、カーネルパラメータ (vga 以外) を指定します。

CYCLE_DETECTION / CYCLE_NEXT_ENTRY

ブートサイクルの検出を使用するかどうかと、使用していて起動がうまくいかなかった場合に、/boot/grub/menu.lst 内でどの代替項目 (たとえば フェイルセーフ など) を起動するかを指定します。詳しくは /usr/share/doc/packages/bootcycle/README をお読みください。

7.1.5 起動パスワードの設定

オペレーティングシステムが起動する前であっても、GRUB はファイルシステムに アクセスすることができます。root 権限のないユーザは、この方法で Linux システム内のファイルにアクセスする可能性があります。このようなアクセス方法を 禁止した

り、特定のオペレーティングシステムを起動できないようにしたりしたい 場合は、起動パスワードを設定してください。

重要: 起動パスワードとスプラッシュスクリーン

GRUB で起動パスワードを使用する場合は、スプラッシュスクリーンは表示 されなくなります。

root ユーザから下記の手順を実施することで、起動パスワードを設定することができます:

- 1 まずはコマンドプロンプトから grub-md5-crypt を利用し、パスワードを暗号化します:

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$LS2dv/$J0YcdxIn7CJk9xShzzJVw/
```

- 2 上記の出力で、"Encrypted:" 以降の部分を menu.lst ファイル内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 $1$LS2dv/$J0YcdxIn7CJk9xShzzJVw/
```

上記のように設定することで、起動プロンプトから P を押し、正しいパスワードを入力した場合にのみ、GRUB コマンドを実行することができるようになります。ただし、起動メニュー内に記載されているオペレーティングシステムであれば、パスワードの入力なしでも実行できます。

- 3 起動メニューから 1 つまたは複数のオペレーティングシステムの起動が できないようにするには、パスワード無しでは起動できないように設定することが できます。menu.lst ファイル内のセクションに対して、lock という行を追加してくだ さい。たとえば下記のように なります:

```
title linux
kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
initrd (hd0,4)/initrd
lock
```

上記の設定でシステムを再起動すると、起動メニューから Linux を選択すると 下記のようなエラーメッセージが表示されます:

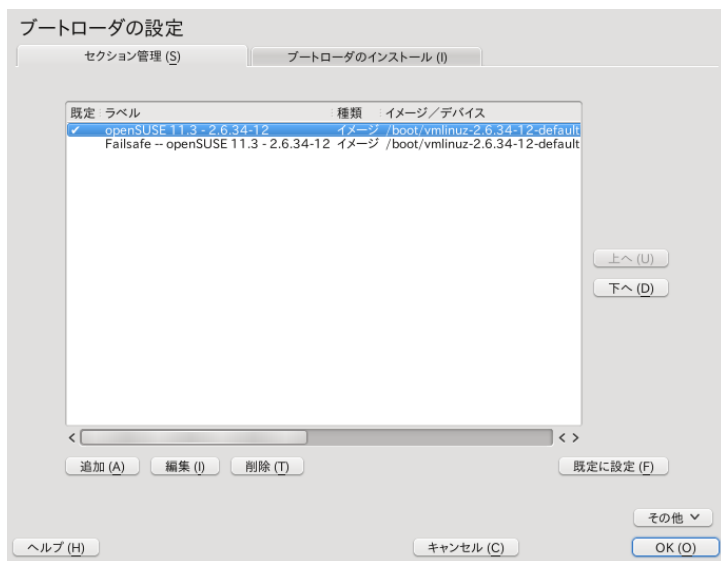
Error 32: Must be authenticated

Enter を押すとメニューに入ることができます。さらに P を押してパスワードプロンプトを表示させ、パスワードを入力して Enter を押してください。すると選択したオペレーティングシステム (この場合は Linux) を起動することができるようになります。

7.2 YaST を利用したブートローダの設定

お使いの openSUSE のブートローダを設定するのに最も簡単な方法は、YaST のモジュールを利用して設定することです。YaST のコントロールセンター から、システム > ブートローダ を選択して設定を行ないます。図7.1「ブートローダの設定」(141 ページ) にあるとおり、ここではお使いのシステムでのブートローダ設定が表示され、変更を行なうことができます。

図 7.1 ブートローダの設定



個別のオペレーティングシステムに関するブートローダのセクションを編集したり変更したり、削除したりするには、**セクション管理** タブを利用します。セクションを追

加するには **追加** を、既存のセクションについて 設定値を変更するにはセクションを選択してから **編集** をそれぞれ 押してください。またセクションを削除するには、削除したい項目を選んで **削除** を押してください。ブートローダのオプションについて詳しく知りたい場合は、まず 7.1 項「GRUB での起動」(130 ページ) をお読みください。

ブートローダの種類やインストール先、または高度なブートローダ設定を閲覧したり変更 したりするには、**ブートローダのインストール** を利用します。

高度なオプションにアクセスするには、**その他** ボタンを押す ことで表示されるドロップダウンメニューを利用します。内蔵のエディタを利用して GRUB の設定ファイルを直接編集することができます。詳しくは 7.1 項「GRUB での起動」(130 ページ) をお読みください。また、既存の設定ファイルを削除して **全く新しい設定を作成** することもできます。また、YaST に対して **新しい設定を提示** するように求めることもできるほか、設定をディスクに書き込んだり、ディスクから既存の 設定を再読み込みしたりすることもできます。インストール時に保存しておいた マスターブートレコード (MBR) に戻すには、**ハードディスクの MBR を 復元する** を選択してください。

7.2.1 既定の起動項目の設定

既定で起動が行なわれるシステムを変更するには、下記の手順で行ないます：

手順 7.1 既定のシステムの設定

- 1 **セクション管理** タブを開きます。
- 2 既定で起動したい項目を一覧から選択します。
- 3 **既定に設定** を押します。
- 4 最後に **OK** を押すと設定を保存することができます。

7.2.2 ブートローダのインストール先の変更

ブートローダの場所を変更するには、下記の手順で行ないます：

手順 7.2 ブートローダのインストール先の変更

- 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** に対して以下のいずれかを 選択してください：

マスターブートレコード (MBR) から起動

これを選択すると、最初のディスク (BIOS で設定された順序で 最初にあたるディスク) の MBR にブートローダをインストールします。

ルートパーティションから起動

これを選択すると、/ ディレクトリに 割り当てたパーティションに対してブートローダをインストールします (これが既定値です)。

ブートパーティションから起動

これを選択すると、/boot ディレクトリに 割り当てたパーティションに対してブートローダをインストールします。

拡張パーティションから起動

これを選択すると、拡張パーティションコンテナに対してブートローダをインストールします。

カスタムブートパーティション

ブートローダの場所を手作業で指定するには、このオプションを選択してください。

2 変更を保存するには、OK を押します。

7.2.3 ブートローダの時間切れ設定

ブートローダは既定の項目を、すぐには起動しません。時間切れとして設定した時間が経過するまでの間、起動するシステムを選択したりカーネルのパラメータを入力したり することができます。ブートローダの時間切れを設定するには、下記の手順で行ないます:

手順 7.3 ブートローダの時間切れ設定

- 1 ブートローダのインストール タブを選択します。
- 2 ブートローダのオプション を押します。
- 3 タイムアウト (秒) の項目を選択して新しい値を入力するか、もしくはマウスやキーボードで矢印キーを操作して値を編集します。
- 4 OK を 2 回押して設定を保存します。

警告: タイムアウトを 0 秒に設定した場合の影響

タイムアウトに 0 秒を設定すると、システムの起動時に GRUB の操作を行なうことができなくなります。同時に Linux 以外のオペレーティング システムを既定の起動項目として設定すると、Linux システムへのアクセス を無効化することができます。

7.2.4 起動パスワードの設定

この YaST モジュールを利用することで、起動を確認するためのパスワードを 設定することができます。これにより追加のセキュリティ保護を実現することができます。

手順 7.4 起動パスワードの設定

- 1 ブートローダのインストール タブを選択します。
- 2 ブートローダのオプション を押します。
- 3 ブートローダをパスワードで保護する のオプションを選択し、起動時に入力させたいパスワードをパスワード の欄にそれぞれ入力します。
- 4 OK を 2 回押して設定を保存します。

7.2.5 ディスク順序の設定

お使いのコンピュータに 2 台以上のハードディスクが接続されている場合、マシンの BIOS 設定に合わせてディスクの起動順序を指定することができます (7.1.2 項「device.map ファイル」(137 ページ) も合わせてご覧ください)。これを行なうには、下記の手順で行ないます:

手順 7.5 ディスク順序の設定

- 1 ブートローダのインストール タブを選択します。
- 2 ブートローダのインストール詳細 を押します。
- 3 複数のディスクが一覧表示されている場合、ディスクを選択してから 上へ または 下へ を押し、ディスクの順序を入れ替えます。

4 OK を 2 回押して設定を保存します。

7.2.6 高度なオプションの設定

高度な起動オプションは、*ブートローダのインストール > ブートローダのオプション* を選択すると設定できるようになります。通常は既定値から変更を行なう必要はありません。

ブートパーティションをアクティブに設定

ブートローダを含むパーティションをアクティブに設定します。いくつかの古いオペレーティングシステム (Windows 98 など) では、アクティブなパーティションからでないとは起動できないものがあるためです。

MBR に汎用ブートコードを書き込む

現在の MBR に対し、オペレーティングシステムに依存しない汎用のコードを書き込みます。

デバッグ用フラグ

GRUB をデバッグモードで動作させ、ディスクの動作についてメッセージを表示するようにします。

ブート時にメニューを隠す

ブートメニューを隠し、既定の項目を起動するように設定します。

警告

ブートメニューを隠した場合、システムの起動時に GRUB にアクセスすることができなくなります。同時に Linux 以外のオペレーティングシステムを既定の起動項目として設定すると、Linux システムへのアクセスを無効化することができます。

信頼済み Grub を使用する

トラステッドコンピューティング機能に対応する信頼済み GRUB を起動するようにします。

聴覚信号を有効にする

GRUB で聴覚信号を有効または無効に設定します。

グラフィカルメニューファイル

起動スクリーンを表示する際に利用するグラフィックファイルのパスを指定します。

シリアルコンソールを使用する

お使いのマシンがシリアルコンソールで操作するものである場合は、この項目を選択して COM ポートと速度を設定してください。詳しくは `info grub` または <http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal> (英語) をお読みください。

7.2.7 ブートローダの種類の設定

ブートローダのインストール タブでは、ブートローダの種類を選択することができます。openSUSE での既定は GRUB ですが、LILO または ELILO を使用したい場合は下記のような手順で変更します:

警告: LILO はサポート対象外です

LILO の使用はお勧めできません—openSUSE では サポート対象外であるためです。特別な場合にのみお使いください。

手順 7.6 ブートローダの種類の設定

- 1 ブートローダのインストール タブを選択します。
- 2 まずは ブートローダ の項目で *LILO* を選択します。
- 3 ダイアログボックスが開いたら、下記のいずれかの処理を選択してください:

新しい設定を提示

YaST に対して、新しい設定を提案させます。

現在の設定を変換

YaST に対して、現在の設定を変換するよう指示します。設定の変換を行うことで、設定のうちのいくつかが失われる場合があります。

新しい設定の作成

カスタムな設定を書き込みます。この処理は openSUSE のインストール時には選択できません。

ディスクに保存された設定の読み込み

`/etc/lilo.conf` ファイルに保存された設定を読み込み ます。この処理は openSUSE のインストール時には選択できません。

4 OK を 2 回押して設定を保存します。

変換にあたっては、古い GRUB の設定がディスクに保存されます。これを使用し直す場合は、ブートローダの種類を GRUB に戻してから *変換前に保存した設定に戻す* を選択してください。この選択肢は、インストール済みのシステムでのみ利用できます。

注記: カスタムなブートローダ

GRUB でも LILO でもないその他のブートローダを使用したい場合は、*ブートローダをインストールしない* を選択してください。このオプションを選択する場合は、事前にお使いのブートローダの文書を良くお読みください。

7.3 Linux ブートローダのアンインストール

YaST では、Linux でのブートローダをアンインストールし、Linux がインストールされる前に存在していた通常の MBR に戻す機能も提供しています。インストール時に YaST は自動で元の MBR をバックアップしているため、必要に応じてそこから書き戻すことができるようになっています。

GRUB をアンインストールするには、YaST を起動して *システム > ブートローダ* を選択し、*ブートローダモジュールを起動します*。そこからさらに *その他 > ハードディスクの MBR を復元する* を選択し、確認のため *はい、上書きします* を押します。

7.4 起動 CD の作成

お使いのシステムを起動マネージャから起動する際に問題が発生した場合や、お使いのハードディスクにブートマネージャをインストールすることができない場合は、Linux を起動するために必要な全てのスタートアップファイルを含んだ、起動 CD を作成することもできます。この作業を行なうには、お使いのシステムに CD ライター (書き込み可能な CD ドライブ) が必要です。

GRUB を利用した起動 CD-ROM 作成を行なうには単純に、特別な形式の第 2 ステージである、stage2_eltorito と、カスタマイズした menu.lst ファイル (必要であれば) を用意するだけです。従来必要だった stage1 と stage2 は、もはや必要ではありません。

手順 7.7 起動 CD の作成

- 1 まずは ISO イメージを作成するためのディレクトリに移動します。たとえば: `cd /tmp`
- 2 下記のようにして GRUB 用のサブディレクトリを作成し、その中の `iso` ディレクトリに移動します:

```
mkdir -p iso/boot/grub && cd iso
```

- 3 それぞれ `iso/boot/` ディレクトリに、カーネルと `stage2_eltorito`, `initrd`, `menu.lst`, `message` ファイルをコピーします:

```
cp /boot/vmlinuz boot/  
cp /boot/initrd boot/  
cp /boot/message boot/  
cp /usr/lib/grub/stage2_eltorito boot/grub  
cp /boot/grub/menu.lst boot/grub
```

- 4 まずは `root (hdx, y)` のように書かれている項目を `root (cd)` のように修正し、お使いの CD-ROM デバイスを 指し示すようにします。また、それぞれメッセージファイルやカーネル、`initrd` についても、`/boot/message` (メッセージファイル), `/boot/vmlinuz` (カーネル), `/boot/initrd` (`initrd`) を指定します。全ての設定が完了すると、`menu.lst` は下記のような形になります:

```
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
```

`splash=verbose` の代わりに `splash=silent` と指定すると、起動処理時に現われる起動メッセージの出力を抑止することができます。

- 5 あとは下記のコマンドで ISO イメージを作成します:

```
genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot ¥  
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 ¥  
-o grub.iso /tmp/iso
```

- 6 できあがったファイル `grub.iso` を、お好きなツールを利用して CD メディアに書き込みます。ただし、ISO イメージをデータファイルとして書き込んだりせず、お使いのユーティリティで CD イメージとして書き込むオプションを指定してください。

7.5 グラフィカルな SUSE スクリーン

グラフィカルな SUSE スクリーンは、カーネルパラメータに `vga=値` を指定した場合にのみ、1 つめのコンソールに表示されるものです。YaST を利用してインストールした場合、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あわせて自動的に有効化されます。SUSE スクリーンを無効化したい場合は、下記の 3 種類の方法で無効化することができます:

必要に応じて SUSE スクリーンを無効化する方法

グラフィカルな画面を無効化するには、`echo 0 >/proc/splash` というコマンドを入力します。再度有効化したい場合は、`echo 1 >/proc/splash` と入力します。

既定で SUSE スクリーンを無効化する方法

お使いのブートローダの設定に、`splash=0` というカーネルパラメータを記入します。詳しい情報は 第7章 ブートローダ *GRUB* (129 ページ) をお読みください。なお、テキストモードをお使いになりたい場合 (古いバージョンでの既定値) は、`vga=normal` と記入します。

完全に SUSE スクリーンを無効化する方法

新しくカーネルをコンパイルし、*framebuffer support* 内の *Use splash screen instead of boot logo* のオプション選択を外します。カーネル内でのフレームバッファサポートを無効化すると、スプラッシュスクリーンについても自動的に無効に設定されます。

警告: サポート対象外です

SUSE では、独自にコンパイルしたカーネルを利用して起動した場合、いかなるサポートをも提供いたしません。

7.6 トラブルシューティング

この章では、GRUB を利用して起動する際に発生しうる問題や、それらの問題に対する解決方法について概要を述べています。いくつかの問題は <http://ja.opensuse.org/SDB:SDB> (日本語) や http://en.opensuse.org/Portal:Support_database/ (英語) にあるサポートデータベースに記載されています。キーワード検索を行なう場合は、*GRUB* や *起動*、または *ブートローダ* などで検索してください。

GRUB と XFS

XFS にはパーティションの起動ブロック内に 第 1 ステージ を保存しておくための領域がありません。そのため、ブートローダの配置場所としては、XFS パーティションを設定しないでください。この問題は、XFS 以外の ファイルシステムでフォーマットする個別の起動パーティションを作成することで、解決することができます。

GRUB が GRUB Geom エラーを報告する問題

GRUB はシステムを起動する際、接続されたハードディスクのジオメトリ情報 (配置情報) を確認します。BIOS は時として矛盾した情報を提供することがあり、これによって GRUB は Geom Error を報告します。この場合は BIOS を更新して 解決してください。

また GRUB は、BIOS で登録されていない追加のハードディスクから Linux を起動しようとした場合にもこのエラーメッセージを表示します。ブートローダの 第 1 ステージ が見つかって正しく 読み込めたものの、第 2 ステージ が見つからない 場合に発生します。このような問題が発生した場合は、新しいハードディスクを BIOS に登録することで解決することができます。

複数のハードディスクを含むシステムで起動できない問題

YaST はインストール時に、ハードディスクの起動順序を正しく判別しない 場合があります。たとえば、BIOS での起動順序が SCSI, PATA (IDE) の順であるにも関わらず、GRUB では PATA (IDE) ディスクを hd0 と認識し、SCSI ディスクを hd1 と認識することがあります。

この場合は GRUB のコマンドラインを利用して、起動処理中にハードディスクの 順序を修正してください。システムを問題なく起動できたら、device.map ファイルを編集し、恒久的に新しい割り当てを 書き込んでください。その後、/boot/grub/menu.lst と /boot/grub/device.map にある GRUB のデバイス名を確認し、下記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
```

Windows を 2 台目のハードディスクから起動する方法

Windows のようなオペレーティングシステムでは、1 台目のハードディスクからのみ 起動することができます。1 台目以外のハードディスクにそのようなオペレーティング システムをインストールした場合は、関連するメニュー項目を編集することで、論理的な 変更を行なうことができます。

```
...
title windows
  map (hd0) (hd1)
  map (hd1) (hd0)
```

```
chainloader(hd1,0)+1  
...
```

上記の例では、Windows が 2 台目のハードディスクから始まっていることを示しています。ハードディスクの論理的な順序は map コマンドで 変更することができます。この仕組みは、GRUB のメニューファイルには影響 しません。そのため、2 台目のハードディスクは chainloader に指定しなければなりません。

7.7 さらになる情報

GRUB に関する広範囲の情報は、<http://www.gnu.org/software/grub/> (英語) に記載されています。grub の info ページを読むことも できます。特定の問題について調べるには、<http://ja.opensuse.org/SDB:SDB> (日本語) または http://en.opensuse.org/Portal:Support_database/ (英語) にある サポートデータベースから、「GRUB」キーワードを指定することで検索 することもできます。

ブートローダ GRUB2

本章では、openSUSE® で使用されるブートローダ GRUB2 (Grand Unified Bootloader) について、その設定方法を説明しています。これは従来の GRUB ブートローダの後継にあたる ソフトウェアです。明示的に区別するため、従来のバージョンは「GRUB Legacy」とも呼ばれます (詳しくは 第7章 ブートローダ *GRUB* (129 ページ) をお読みください)。GRUB2 は openSUSE® バージョンより既定のブートローダとなりました。主な設定は専用の YaST モジュールを利用して行なうことができます。Linux の起動手順について詳しくない場合は、第7章 ブートローダ *GRUB* (129 ページ) をお読みのうえ、起動に関する背景的な知識を得てください。また、起動処理の概要は 第5章 *Linux システムの起動* (103 ページ) で説明しています。

8.1 GRUB Legacy との主な違い

- 設定を複数のファイルに分散して保存するようになりました。また、設定ファイルの書式も変更されています。
- パーティション番号が 1 から始まるようになりました (従来の GRUB Legacy では 0 から始まっていました)。
- さらに多くのファイルシステムに対応しています。
- GRUB2 では LVM や RAID デバイス上のファイルを、直接読めるようになりました。
- メニュー項目の名称を含め、ユーザインターフェイスを翻訳できるようになりました。

- GRUB では、ファイルシステムなどの特定の機能に対応するために、モジュールを読み込む仕組みが追加されています。
- 「ステージ」と呼ばれる仕組みは廃止され、GRUB2 を構成する イメージの構造が変更されています。

8.2 設定ファイルの構造

GRUB2 の設定は、下記に示すファイルで行ないます:

`/boot/grub2/grub.cfg`

このファイルには、GRUB2 のメニュー項目に関する全ての情報が保存されています。これは従来の GRUB Legacy で言うところの `menu.lst` にあたるものです。`grub.cfg` は `grub2-mkconfig` コマンドで構築するもので、通常は手作業で編集すべきではないものです。

`/etc/default/grub`

このファイルは GRUB2 のユーザ設定を制御するためのもので、通常は 背景画像やテーマなど、追加の環境設定が含まれています。

`/etc/grub.d/` 内のスクリプト

このディレクトリ内に存在するスクリプトは、`grub2-mkconfig` コマンドの実行中に読み込まれ、メインの設定ファイル `/boot/grub/grub.cfg` 内に取り込まれます。

`/etc/sysconfig/bootloader`

このファイルは `perl-bootloader` ライブラリから読み込むことができるもので、YaST からブートローダを設定する際、および新しいカーネルがインストールされた際に利用されます。このファイルにはカーネルパラメータなどの設定オプションが含まれていて、これらはブートローダの設定ファイルに対して既定で追加されます。

GRUB2 は様々な方法でコントロールすることができます。既存の設定ファイルにある起動項目はグラフィカルなメニュー (スプラッシュスクリーン) で選択することができます。設定は `grub.cfg` ファイルから読み込まれますが、このファイルはさらに他のファイルの内容から生成されます (詳しくは下記をお読みください)。GRUB2 では、すべての設定ファイルがシステムファイルという位置づけとなるため、これらを編集する際は、`root` の権限が必要となります。また、GRUB2 の設定ファイルを編

集した後は、`grub2-mkconfig -o /boot/grub2/grub.cfg` を忘れずに実行してください。

8.2.1 /boot/grub2/grub.cfg ファイル

起動メニューでのグラフィカルなスプラッシュスクリーンは、GRUB2 の設定ファイル `/boot/grub2/grub.cfg` を基礎にしています。このファイルには そのほか、このメニューから起動可能な全てのパーティションとオペレーティングシステムに関する情報も含まれています。

システムが起動する際、GRUB2 は常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。そのため、GRUB2 はメニューファイルを変更した場合であっても、再インストールを行なう必要はありません。また、`grub.cfg` は カーネルのインストールや削除を行なった場合にも、自動的に再構築されます。

`grub.cfg` は `grub2-mkconfig -o /boot/grub2/grub.cfg` コマンドを実行すると構築することができます。このコマンドは、`/etc/default/grub` ファイルと `/etc/grub.d/` ディレクトリ内に存在するスクリプトを、それぞれ 取り込んで設定を構築する仕組みであるため、このファイルを手作業で修正すべきではありません。その代わりに、`/etc/grub.d/` ディレクトリ内の ソースファイルを編集するか、もしくは YaST ブートローダモジュールを利用して、GRUB2 の設定ファイルを変更してください。YaST での設定方法について、詳しくは 8.3 項「YaST を利用したブートローダの設定」(166 ページ) をお読みください。

8.2.2 /etc/default/grub ファイル

このファイルには、GRUB2 に対するより一般的な設定が含まれています。たとえばメニューの 表示時間のほか、起動に利用する既定の OS などが含まれています。このファイルは、`root` の権限があれば、自由に編集することができます。全てのオプションを一覧表示するには、下記のコマンドを実行して出力された内容をお読みください：

```
grep "export GRUB_DEFAULT" -A50 /usr/sbin/grub2-mkconfig | grep GRUB_
```

既に設定済みの値のほかにも、独自に変数を設定して、`/etc/grub.d` ディレクトリ内のスクリプトから利用することもできます。

`/etc/default/grub` はシステムファイルであるため、このファイルを 編集するには `root` 権限が必要となります。また、このファイルを編集した後は、設定ファイルを更

新するために、`grub2-mkconfig -o /boot/grub2/grub.cfg` を実行する必要があります。

8.2.2.1 一般的なオプション

本章では、`/etc/default/grub` ファイル内で使用する 一般的なオプションを示しています。全てのオプションを参照したい場合は、GNU GRUB manual [<http://www.gnu.org/software/grub/manual/grub.html#Simple-configuration>] (英語) をお読みください。

GRUB_DEFAULT

次回コンピュータが再起動した場合に、起動すべき既定のメニュー項目を設定します。これは数値で指定できるほか、メニューの項目そのものを指定したり、「saved」を設定したりすることもできます。たとえば下記のようになります：

`GRUB_DEFAULT=2` を指定すると、3 番目の (数値は 0 から始まります) メニュー項目を起動します。

`GRUB_DEFAULT=2>0` を指定すると、3 番目のサブメニュー内にある最初の項目を起動します。

`GRUB_DEFAULT="Example boot menu entry"` を指定すると、その名前のメニュー項目を起動します。

`GRUB_DEFAULT=saved` を指定すると、`grub2-reboot` または `grub2-set-default` コマンドで設定した項目を起動します。`grub2-reboot` は次の再起動の際にのみ適用される項目を、`grub2-set-default` は次回以降恒久的に適用される項目を、それぞれ設定します。

GRUB_SAVEDEFAULT

`true` に設定すると、起動メニュー内で選択した OS を、次回以降の既定の起動項目として設定します。この設定を動作させるには、`GRUB_DEFAULT=saved` もあわせて設定する必要があります。

GRUB_HIDDEN_TIMEOUT

指定した秒数だけ、ユーザからのキー入力を待ちます。この待機時間の間は、キー入力が行なわれるまでメニューを表示しません。何もキー入力がないまま、指定した秒数が経過すると、`GRUB_TIMEOUT` に制御が移ります。また、`GRUB_HIDDEN_TIMEOUT=0` を指定すると、起動時に が押されているかどうかをチェックし、押されている場合は起動メニューを表示し、押されていない場合は即時に 既定のメニュー項目を起動します。これは、GRUB2 で認識できる起動可能な OS が 1 つしかない場合の既定値です。

GRUB_HIDDEN_TIMEOUT_QUIET

false を指定すると、GRUB_HIDDEN_TIMEOUT 機能が有効な場合、何もない画面上にカウントダウンタイマーだけが表示されるようになります。

GRUB_TIMEOUT

既定の起動項目を自動的に起動するまでの間、起動メニューを表示して待機する時間を秒単位で設定します。何かキーを押すとカウントダウンは停止し、GRUB2 はいずれかの項目を選択するまで待機します。なお、GRUB_TIMEOUT=-1 を指定すると、起動項目を選択するまでの間、メニューを表示したままずっと待ち続ける意味になります。

GRUB_CMDLINE_LINUX

通常／復元モードなど、それぞれの起動項目のコマンドラインに対して、ここで指定された内容が追加されます。ここにはカーネルに対するオプションなどを設定します。

GRUB_CMDLINE_LINUX_DEFAULT

GRUB_CMDLINE_LINUX とほとんど同じですが、通常モードに対してだけ、この内容が追加されます。

GRUB_TERMINAL

入出力を行なう端末デバイスを指定します。console (PC BIOS/EFI コンソール), serial (シリアルポート端末), ofconsole (Open Firmware コンソール), gfxterm (グラフィックモードの出力; 既定値) の中から、いずれかを指定します。

GRUB_GFXMODE

gfxterm グラフィカル端末で使用する解像度を指定します。ただし、お使いのグラフィックカード (VBE) 側で対応するモードのみを指定できます。既定値は auto で、この場合は最適な解像度を検出して利用します。なお、GRUB2 のコマンドラインで vbeinfo と入力することで、利用可能な画面解像度を表示することができます。コマンドラインは、GRUB2 の起動メニュー画面が表示されたタイミングで、c を押すことで利用することができます。

また、解像度の設定の後ろに、色深 (ビット単位) を指定することもできます。たとえば下記のようになります: GRUB_GFXMODE=1280x1024x24

ヒント

GRUB2 とオペレーティングシステムで同じ解像度を設定すると、システムの起動時間を少し短縮することができます。

GRUB_BACKGROUND

gfxterm グラフィカル端末で使用する、背景画像を設定します。このファイルは起動時に GRUB2 が読み込むことのできるファイルでなければならぬほか、.png, .tga, .jpg, .jpeg のいずれかの拡張子でなければなりません。また必要であれば、画像は画面に適合するようにサイズ調整が行われます。

8.2.3 /etc/grub.d 内のスクリプト

このディレクトリ内にあるスクリプトは、grub2-mkconfig コマンドの実行時に読み込まれ、書かれた命令は /boot/grub2/grub.cfg 内に組み込まれます。また、grub.cfg 内のメニュー項目の順序は、このディレクトリ内での実行順序に従います。実行は数字の小さい順に行われ、たとえば 00_header, 10_linux 40_custom などの順序で実行されます。また、英字のファイル名が存在した場合、これらは数字のファイル名よりも後に実行されます。さらに、grub2-mkconfig の実行時には、実行ファイルだけが参照され、grub.cfg に出力を生成します。既定では、/etc/grub.d ディレクトリ内のすべてのファイルが実行ファイルになっています。

下記に既定のスクリプトを示します。

00_header

システムファイルの場所やビデオの設定、テーマや以前に保存した項目などの、環境変数が設定されています。また、/etc/default/grub 内に保管されている設定情報なども、ここで取り込みます。通常は、このファイルを編集する必要はありません。

10_linux

ルートデバイス上にある Linux カーネルを認識し、関連するメニュー項目を生成するためのスクリプトです。復元モードのオプションについても、有効化されていればここで取り込まれます。なお、メインメニューでは最新のカーネルだけが表示され、その他のカーネルはサブメニューとして構成されます。

30_os-prober

このスクリプトは OS-prober を利用して、Linux やその他のオペレーティングシステムを検出し、それらを GRUB2 のメニューとして配置します。これらは Linux や Windows, Hurd や Mac OS X など、それぞれのオペレーティングシステムを識別したセクションを生成します。

40_custom

grub.cfg 内に挿入されるべき独自の項目を設定する際に利用する、雛形ファイルです。exec tail -n +3 \$0 以下の行の内容と既定のコメントが、grub.cfg 内に直接 (何も変更されることなく) 書き込まれます。

90_persistent

これは `grub.cfg` ファイルの一部をコピーし、それらを 変更することなく出力するための、特殊なスクリプトです。これにより、`grub2-mkconfig` が実行されても元に戻ることなく、`grub.cfg` 内の修正を実施することができます。

8.2.3.1 ハードディスクとパーティションの名前ルール

GRUB2 でハードディスクやパーティションに対して使用する名前付けは、通常の Linux のデバイス名とは異なるものを使用します。BIOS が使用する単純なディスク 列挙の仕組みにとっても似ていて、文法は BSD システムの方式に似たものになっています。また、GRUB2 では最初のパーティション番号は 0 になっています。つまり、`(hd0, 0)` は最初のハードディスク内にある 最初のパーティションを意味することになります。一般的なデスクトップマシン の場合、プライマリマスターに接続されているハードディスクのことを指し、Linux のデバイス名で言うと、`/dev/sda1` になります。

4 つまで作成できるプライマリパーティションは、それぞれ 0 から 3 までの間に割り当てられています。論理パーティションは 4 以降になります：

- `(hd0, 0)` 最初のハードディスクにある最初のプライマリパーティション
- `(hd0, 1)` 2 つめのプライマリパーティション
- `(hd0, 2)` 3 つめのプライマリパーティション
- `(hd0, 3)` 4 つめのプライマリパーティション（一般的には拡張パーティション）
- `(hd0, 4)` 最初の論理パーティション
- `(hd0, 5)` 2 つめの論理パーティション

BIOS でのデバイス表記と同じで、GRUB2 は PATA (IDE), SATA, SCSI, ハードウェア RAID デバイスを区別せずに使用します。BIOS やその他のコントローラで認識される 全てのハードディスクは、BIOS 内で設定した起動順序に従って番号が付けられます。

残念ながら、Linux のデバイス名を正しく BIOS のデバイス名に変換することはできません。この割り当ては特定のアルゴリズムに従って生成され、`device.map` ファイルに保存されます。必要であれば、このファイルを編集することもできます。`device.map` に関する情報は、8.2.4項「`device.map` ファイル」(162 ページ)をお読みください。

GRUB2 で完全なパスを指定するには、まず括弧内にデバイス名を指定したあと、パーティション (ファイルシステム) 内でのパスを記述します。なお、パスはスラッシュから書き始めます。たとえば起動可能なカーネルが 最初の PATA (IDE) ハードディスクにおける最初のパーティションに存在する場合、下記のように指定することができます：

```
(hd0, 0)/boot/vmlinuz
```

8.2.3.2 メニューファイルの例

下記は GRUB2 メニューファイルの構造を示すための例です。下記のインストール例では起動パーティションが /dev/sda5 に、ルートパーティションが /dev/sda7 に、Windows のインストールが /dev/sda1 にそれぞれ行なわれている場合を想定しています。

```
gfxmenu (hd0,4)/boot/message❶
color white/blue black/light-gray❷
default 0❸
timeout 8❹

title linux❺
    root (hd0,4)
    kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
    initrd /boot/initrd

title windows❻
    rootnoverify (hd0,0)
    chainloader +1

title floppy❼
    rootnoverify (hd0,0)
    chainloader (fd0)+1

title failsafe❸
    root (hd0,4)
    kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma ¥
    apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
    initrd /boot/initrd.shipped
```

最初のブロックでは、スプラッシュスクリーンの設定を行なっています：

- ❶ /dev/sda5 パーティション内の /boot ディレクトリにある、message ファイルを、背景イメージとして使用する設定です。
- ❷ 色の設定を行なっています。前景を白、背景を青に設定し、選択しているものを黒で、選択の背景をライトグレーで表示します。色の設定はスプラッシュスクリーンには影響しません。Esc でスプラッシュスクリーンを抜けた場合にのみ意味のある設定です。
- ❸ 最初の (0) メニュー項目である title linux を既定の設定として起動します。
- ❹ ユーザ入力が 8 秒間行なわれないと、GRUB2 は自動的に既定の項目を起動します。自動起動を無効化するには、timeout の行を削除してください。timeout 0 を設定すると、既定の項目を即時起動する意味になります。

2 番目の以降のブロックは、様々なオペレーティングシステムを起動するための設定です。それぞれのオペレーティングシステムの設定は、title で始まります。

- ⑤ 最初の項目 (title linux) は、openSUSE を起動するための項目です。カーネル (vmlinuz) は最初のハードディスクにおける最初の論理パーティション (ブートパーティション) 内に位置しています。ルートパーティションや VGA モードなどのカーネル パラメータが後に続いています。ルートパーティションの指定は Linux の 名前付けルールに従って /dev/sda7/ と書かれています。これはこの情報を読むのがカーネルであるためで、GRUB2 はその値について 何も処理を行なわないためです。initrd についても 同様に、最初のハードディスクにおける最初の論理パーティション内に 位置しています。
- ⑥ 2 つめの項目は Windows を読み込むための項目です。Windows は最初の ハードディスク (hd0, 0) における最初のパーティション から起動する設定になっています。chainloader +1 のコマンドは、GRUB2 に対して指定したパーティションで最初のセクタを 読み出して実行するように指定するコマンドです。
- ⑦ 3 つめの項目は、単に BIOS 設定を変更せずにフロッピーディスクから起動するための項目です。
- ⑧ failsafe と書かれている項目は、問題の発生している マシンであっても Linux を起動できるよう、カーネルパラメータをいくつか 指定して起動するための項目です。

メニューファイルは必要な時に変更することができ、GRUB2 は次の起動時に 変更済みの設定を使用します。設定の変更は、YaST かエディタなどで編集してください。また、代替策として GRUB2 の機能を利用して一時的に変更することもできます。詳しくは 8.2.3.3 項「起動処理時のメニュー項目編集」(161 ページ) をお読みください。

8.2.3.3 起動処理時のメニュー項目編集

グラフィカルな起動メニューでは、カーソルキーを利用して起動するオペレーティング システムを選択することができます。なお、Linux システムを選択した場合は、起動プロンプトを利用して追加のパラメータを設定することもできます。個別のメニュー項目を直接編集したい場合は Esc を押し、スプラッシュ スクリーンを抜けて GRUB2 のテキストベースのメニューを表示させてから、E を押します。このようにして変更した内容は、その時点の 起動でのみ有効で、恒久的に適用されることはありません。

重要: 起動処理時のキーボードレイアウト

起動時には英語 (アメリカ英語) キーボードレイアウトだけを利用できます。詳しくは 図「英語キーボードのレイアウト」(↑ スタートアップ) をお読みください。

メニュー項目の編集を行なうと、うまく起動できないシステムに対する修復を行なうことができます。これは、間違ったブートローダの設定を手作業で修正することで、うまく起動するための回避策を入力することができるためです。起動処理内での手動でのパラメータ入力は、システムの設定を恒久的に変更せず、一時的に新しい設定をテストしたりしたい場合にも便利です。

編集モードを有効にしたあと、まずはカーソルキーを利用して編集する行を選択します。ここからさらに E を押すと、選択した行を編集することができます。この方法で、起動処理を行なう前に間違ったパーティション指定やパス指定を修正してください。編集モードを抜けてメニューに戻るには、Enter を押します。メニューから B を押すと、その設定で起動を行ないます。それ以外の処理は、画面下部のヘルプテキストに表示されています。

起動オプションを恒久的に変更してそれらの設定をカーネルに渡したい場合は、root ユーザで menu.lst ファイルを開き、それぞれ必要なカーネルパラメータを既存の行に設定してください。複数のパラメータはスペースで区切ります：

```
title linux
    root(hd0,0)
    kernel /vmlinuz root=/dev/sda3 additional parameter
    initrd /initrd
```

GRUB2 は次回の起動時に自動で設定したパラメータを読み込みます。YaST ブートローダモジュールからでも同じことを行なうことができます。上記と同様に、新しいパラメータはスペースで区切って指定します。

8.2.4 device.map ファイル

device.map ファイルは、GRUB2 や BIOS のデバイス名を Linux のデバイス名に変換するためのファイルです。PATA (IDE) と SCSI のハードディスクが混在するシステムの場合、GRUB2 は特殊な手順で起動順序を判断しなければなりません。これは GRUB2 が起動順序の設定を行なっている BIOS 情報にアクセスできない可能性があるためです。GRUB2 はこの分析結果を /boot/grub/device.map ファイルに保存します。たとえば BIOS で SCSI よりも PATA を優先して起動するように設定しているシステムでは、device.map ファイルは下記ようになります：

```
(fd0) /dev/fd0
(hd0) /dev/sda
(hd1) /dev/sdb
```

もしくは下記のような場合もあります：

```
(fd0) /dev/fd0
(hd0) /dev/disk-by-id/DISK1 の ID
```


(hd1) /dev/disk-by-id/DISK2 の ID

PATA (IDE) や SCSI、もしくはその他のハードディスクは様々な要素に依存していて、Linux ではその割り当てを識別することができないことから、device.map ファイルのある順序を手動で編集することもできます。起動時に何らかの問題が発生した場合は、このファイル内にある順序が BIOS の順序とあっているかどうかを確認し、GRUB2 プロンプトから必要に応じて一時的に変更してみてください。その設定で Linux システムが問題なく起動するようであれば、YaST ブートローダモジュールやエディタなどを利用して、device.map ファイルを恒久的に変更してください。

device.map ファイルを手作業で変更した場合は、下記のコマンドを入力して GRUB2 を再インストールしてください。このコマンドを実行すると、device.map ファイルを読み込み直し、grub.conf ファイルにあるコマンドを実行します：

```
grub --batch < /etc/grub.conf
```

8.2.5 /etc/sysconfig/bootloader ファイル

この設定ファイルは YaST を利用してブートローダを設定した場合、および 新しいカーネルをインストールした場合にのみ使用されるものです。このファイルは、ブートローダの設定ファイル (たとえば GRUB2 であれば /boot/grub/menu.lst) を書き換える perl-bootloader ライブラリが解釈します。なお、/etc/sysconfig/bootloader ファイルは GRUB2 固有の設定ファイルではありません。openSUSE 上にインストールされたブートローダであれば、どのブートローダにも適用されます。

注記: カーネル更新後のブートローダ設定

新しいカーネルがインストールされると、perl のブートローダモジュールは毎回、新しいブートローダの設定ファイル (たとえば GRUB2 であれば /boot/grub/menu.lst) を /etc/sysconfig/bootloader に設定された既定値で作成します。カーネルパラメータをカスタマイズしている場合は、/etc/sysconfig/bootloader を適宜変更し、カーネル更新後も必要な設定が反映されるようにしてください。

LOADER_TYPE

お使いのシステムにインストールされているブートローダを指定します (たとえば GRUB2 や LILO など)。この項目は手動では変更せず、手順 7.6「ブートローダの種類の設定」(146 ページ) に示されている手順で YaST を利用し、ブートローダを設定してください。

DEFAULT_VGA / FAILSAFE_VGA / XEN_VGA

起動処理時に利用するフレームバッファについて、画面の解像度と色深度の 設定を行いません。これらはカーネルパラメータ vga に渡される値で、それぞれ既定の起動項目のほか、フェイルセーフ (安全設定) や XEN 設定で使用されます。それぞれ下記の値を設定することができます:

表 8.1 画面解像度と色深度の一覧

	640x480	800x600	1024x768	1280x1024	1600x1200
8 ビット	0x301	0x303	0x305	0x307	0x31C
15 ビット	0x310	0x313	0x316	0x319	0x31D
16 ビット	0x311	0x314	0x317	0x31A	0x31E
24 ビット	0x312	0x315	0x318	0x31B	0x31F

DEFAULT_APPEND / FAILSAFE_APPEND / XEN_KERNEL_APPEND

ブートローダの設定ファイル内で、既定の項目やフェイルセーフ設定、および XEN の起動項目に設定する、カーネルパラメータ (vga 以外) を指定します。

CYCLE_DETECTION / CYCLE_NEXT_ENTRY

ブートサイクルの検出を使用するかどうかと、使用していて起動がうまくいかなかった場合に、/boot/grub/menu.lst 内でどの代替項目 (たとえば フェイルセーフ など) を起動するかを指定します。詳しくは /usr/share/doc/packages/bootcycle/README をお読みください。

8.2.6 起動パスワードの設定

オペレーティングシステムが起動する前であっても、GRUB2 はファイルシステムにアクセスすることができます。root 権限のないユーザは、この方法で Linux システム内のファイルにアクセスする可能性があります。このようなアクセス方法を 禁止したり、特定のオペレーティングシステムを起動できないようにしたりしたい 場合は、起動パスワードを設定してください。

重要: 起動パスワードとスプラッシュスクリーン

GRUB2 で起動パスワードを使用する場合は、スプラッシュスクリーンは表示されなくなります。

root ユーザから下記の手順を実施することで、起動パスワードを設定することができます:

- 1 At the root prompt, encrypt the password using grub-md5-crypt:

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$1S2dv/$J0YcdxIn7CJk9xShzzJVw/
```

- 2 上記の出力で、"Encrypted:" 以降の部分を menu.lst ファイル内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$1S2dv/$J0YcdxIn7CJk9xShzzJVw/
```

上記のように設定することで、起動プロンプトから P を押し、正しいパスワードを入力した場合にのみ、GRUB2 コマンドを実行することができるようになります。ただし、起動メニュー内に記載されているオペレーティング システムであれば、パスワードの入力なしでも実行できます。

- 3 起動メニューから 1 つまたは複数のオペレーティングシステムの起動ができないようにするには、パスワード無しでは起動できないように設定することができます。menu.lst ファイル内のセクションに対して、lock という行を追加してください。たとえば下記のように なります:

```
title linux
  kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
  initrd (hd0,4)/initrd
  lock
```

上記の設定でシステムを再起動すると、起動メニューから Linux を選択すると下記のようなエラーメッセージが表示されます:

```
Error 32: Must be authenticated
```

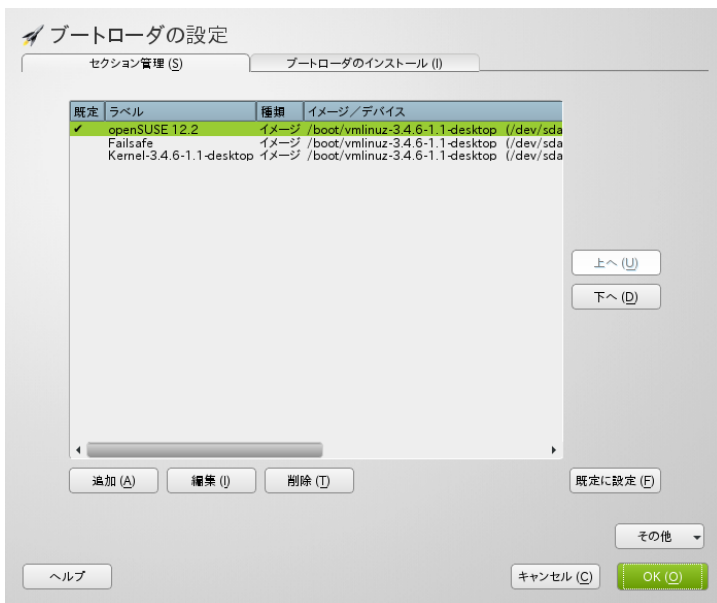
Enter を押すとメニューに入ることができます。さらに P を押してパスワードプロンプトを表示させ、パスワードを入力して Enter を押してください。すると選択し

たオペレーティングシステム (この場合は Linux) を起動することができるようになります。

8.3 YaST を利用したブートローダの設定

一般的に、お使いの openSUSE のブートローダを設定するのに最も簡単な方法は、YaST のモジュールを利用して設定することです。YaST コントロールセンターから、システム > ブートローダ を選択して設定を行ないます。図7.1「ブートローダの設定」(141 ページ) にあるとおり、ここではお使いのシステムでのブートローダ設定が表示され、変更を行なうことができます。

図 8.1 ブートローダの設定



ブートローダの種類やインストール先、または高度なブートローダ設定を閲覧したり変更したりするには、**ブートローダのインストール** を利用します。なお、GRUB2 ブートローダを使用するには、利用可能なブートローダの一覧で選択を行なう必要があります。

8.3.1 既定の起動項目の設定

既定で起動が行なわれるシステムを変更するには、下記の手順で行ないます：

手順 8.1 既定のシステムの設定

- 1 ブートローダのオプション を押し、既定のブートセクション の一覧を開きます。
- 2 既定で起動したい項目を一覧から選択します。なお、項目の一覧内に「>」が書かれている場合、これはサブセクション内に存在していることを示します。
- 3 最後に OK を押すと設定を保存することができます。

8.3.2 ブートローダのインストール先の変更

ブートローダのインストール先を変更するには、下記の手順で行ないます：

手順 8.2 ブートローダのインストール先の変更

- 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 に対して以下のいずれかを 選択してください：

マスターブートレコード (MBR) から起動

これを選択すると、最初のディスク (BIOS で設定された順序で 最初にあたるディスク) の MBR にブートローダをインストールします。

ルートパーティションから起動

これを選択すると、/ ディレクトリに 割り当てたパーティションに対してブートローダをインストールします (これが既定値です)。

ブートパーティションから起動

これを選択すると、/boot ディレクトリに 割り当てたパーティションに対してブートローダをインストールします。

拡張パーティションから起動

これを選択すると、拡張パーティションコンテナに対してブートローダをインストールします。

カスタムブートパーティション

ブートローダの場所を手作業で指定するには、このオプションを選択してください。

2 変更を保存するには、OK を押します。

8.3.3 ブートローダの時間切れ設定

ブートローダは既定の項目を、すぐには起動しません。時間切れとして設定した時間が経過するまでの間、起動するシステムを選択したりカーネルのパラメータを入力したりすることができます。ブートローダの時間切れを設定するには、下記の手順で行ないます: The boot loader does not boot the default system immediately. During the time-out, you can select the system to boot or write some kernel parameters. To set the boot loader time-out, proceed as follows:

手順 8.3 ブートローダの時間切れ設定

- 1 ブートローダのインストール タブを選択します。
- 2 ブートローダのオプション を押します。
- 3 タイムアウト (秒) の項目を選択して新しい値を入力するか、もしくはマウスやキーボードで矢印キーを操作して値を編集します。
- 4 OK を 2 回押して設定を保存します。

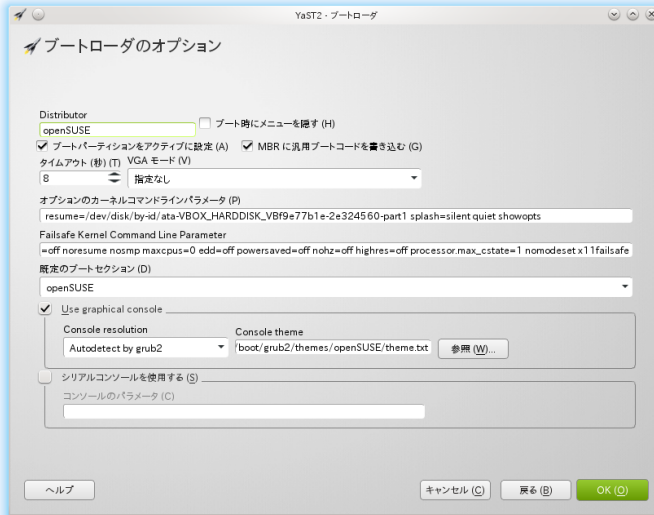
警告: タイムアウトを 0 秒に設定した場合の影響

タイムアウトに 0 秒を設定すると、システムの起動時に GRUB2 の操作を行なうことができなくなります。同時に Linux 以外のオペレーティングシステムを既定の起動項目として設定すると、Linux システムへのアクセスを無効化することができます。

8.3.4 高度なオプションの設定

高度な起動オプションは、ブートローダのインストール > ブートローダのオプション を選択すると設定できるようになります。通常は既定値から変更を行なう必要はありません。

図 8.2 Boot Loader Options



ブートパーティションをアクティブに設定

ブートローダを含むパーティションをアクティブに設定します。いくつかの古いオペレーティングシステム (Windows 98 など) では、アクティブなパーティションからでないと起動できないものがあるためです。

MBR に汎用ブートコードを書き込む

現在の MBR に対し、オペレーティングシステムに依存しない汎用のコードを書き込みます。

ブート時にメニューを隠す

ブートメニューを隠し、既定の項目を起動するように設定します。

グラフィカルコンソールを使用する

これを選択すると、ブートメニューはテキストモードではなく、グラフィカルなスプラッシュ画面を表示ようになります。ブートメニューでの解像度は、コンソールの解像度の一覧から設定することができるほか、コンソールのテーマで、テーマの定義ファイルを選択することもできます。

シリアルコンソールを使用する

お使いのマシンがシリアルコンソールで操作するものである場合は、この項目を選択して COM ポートと速度を設定してください。詳しくは `info grub` または

<http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal>
(英語) をお読みください。

8.3.5 ブートローダの種類の設定

ブートローダのインストール タブでは、ブートローダの種類を 選択することができます。openSUSE での既定は GRUB2 ですが、LILO または ELILO を使用したい場合は下記のような手順で変更します:

警告: LILO はサポート対象外です

LILO の使用はお勧めできません—openSUSE では サポート対象外であるためです。特別な場合にのみお使いください。

手順 8.4 ブートローダの種類の設定

- 1 ブートローダのインストール タブを選択します。
- 2 まずは *ブートローダ* の項目で *LILO* を選択します。
- 3 ダイアログボックスが開いたら、下記のいずれかの処理を選択してください:

新しい設定を提示

YaST に対して、新しい設定を提案させます。

現在の設定を変換

YaST に対して、現在の設定を変換するよう指示します。設定の変換を行なうことで、設定のうちのいくつかが失われる場合があります。

新しい設定の作成

カスタムな設定を書き込みます。この処理は openSUSE のインストール時には選択できません。

ディスクに保存された設定の読み込み

/etc/lilo.conf ファイルに保存された設定を読み込み ます。この処理は openSUSE のインストール時には選択できません。

- 4 OK を 2 回押して設定を保存します。

変換にあたっては、古い GRUB2 の設定がディスクに保存されます。これを使用し直す 場合は、ブートローダの種類を GRUB2 に戻してから *変換前に保存した設定*

に戻す を選択してください。この選択肢は、インストール済みのシステムでのみ利用できます。

注記: カスタムなブートローダ

GRUB2 でも LILO でもないその他のブートローダを使用したい場合は、ブートローダをインストールしない を選択してください。このオプションを選択する場合は、事前にお使いのブートローダの文書を良くお読み ください。

8.4 Linux ブートローダのアンインストール

YaST では、Linux でのブートローダをアンインストールし、Linux がインストールされる前に存在していた通常の MBR に戻す機能も提供しています。インストール時に YaST は自動で元の MBR をバックアップしているため、必要に応じてそこから書き戻す ことができるようになっています。

GRUB2 をアンインストールするには、YaST を起動して システム > ブートローダ を 選択し、ブートローダモジュールを起動します。そこからさらに その他 > ハードディスクの MBR を復元する を選択し、確認のため はい、上書きします を 押します。

8.5 グラフィカルな SUSE スクリーン

グラフィカルな SUSE スクリーンは、カーネルパラメータに vga=値 を指定した場合にのみ、1 つめのコンソールに表示されるものです。YaST を利用してインストールした場合、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あわせて自動的に有効化 されます。SUSE スクリーンを無効化したい場合は、下記の 3 種類の 方法で 無効化することができます:

必要に応じて SUSE スクリーンを無効化する方法

グラフィカルな画面を無効化するには、echo 0 >/proc/splash というコマンドを入力します。再度有効化したい場合は、echo 1 >/proc/splash と入力します。

既定で SUSE スクリーンを無効化する方法

お使いのブートローダの設定に、splash=0 というカーネル パラメータを記入します。詳しい情報は 第8章 ブートローダ GRUB2 (153 ページ) をお読み ください。

ださい。なお、テキストモードをお使いになりたい場合 (古いバージョンでの既定値) は、`vga=normal` と記入します。

完全に SUSE スクリーンを無効化する方法

新しくカーネルをコンパイルし、*framebuffer support* 内の *Use splash screen instead of boot logo* のオプション選択を外します。カーネル内でのフレームバッファサポートを無効化すると、スプラッシュスクリーンについても自動的に無効に設定されます。

警告: サポート対象外です

SUSE では、独自にコンパイルしたカーネルを利用して起動した場合、いかなるサポートをも提供いたしません。

8.6 トラブルシューティング

この章では、GRUB2 を利用して起動する際に発生しうる問題や、それらの問題に対する 解決方法について概要を述べています。いくつかの問題は <http://ja.opensuse.org/SDB:SDB> (日本語) や http://en.opensuse.org/Portal:Support_database/ (英語) にあるサポートデータベースに記載されています。キーワード検索を行なう場合は、*GRUB2* や *起動*、または *ブートローダ* などで検索してください。

GRUB2 と XFS

XFS にはパーティションの起動ブロック内に 第 1 ステージ を保存しておくための領域がありません。そのため、ブートローダの配置場所としては、XFS パーティションを設定しないでください。この問題は、XFS 以外の ファイルシステムでフォーマットする個別の起動パーティションを作成することで、解決することができます。

GRUB2 が GRUB Geom エラーを報告する問題

GRUB2 はシステムを起動する際、接続されたハードディスクのジオメトリ情報 (配置情報) を確認します。BIOS は時として矛盾した情報を提供することがあり、これによって GRUB2 は Geom Error を報告します。この場合は BIOS を更新して 解決してください。

また GRUB2 は、BIOS で登録されていない追加のハードディスクから Linux を起動しようとした場合にもこのエラーメッセージを表示します。ブートローダの 第 1 ステージ が見つかって正しく 読み込めたものの、第 2 ステージ が見

つかからない 場合に発生します。このような問題が発生した場合は、新しいハードディスクを BIOS に登録することで解決することができます。

複数のハードディスクを含むシステムで起動できない問題

YaST はインストール時に、ハードディスクの起動順序を正しく判別しない 場合があります。たとえば、BIOS での起動順序が SCSI, PATA (IDE) の順であるにも関わらず、GRUB2 では PATA (IDE) ディスクを hd0 と認識し、SCSI ディスクを hd1 と認識することがあります。

この場合は GRUB2 のコマンドラインを利用して、起動処理中にハードディスクの 順序を修正してください。システムを問題なく起動できたら、device.map ファイルを編集し、恒久的に新しい割り当てを 書き込んでください。その後、/boot/grub/menu.lst と /boot/grub/device.map にある GRUB2 のデバイス名を確認し、下記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
```

Windows を 2 台目のハードディスクから起動する方法

Windows のようなオペレーティングシステムでは、1 台目のハードディスクからのみ 起動することができます。1 台目以外のハードディスクにそのようなオペレーティング システムをインストールした場合は、関連するメニュー項目を編集することで、論理的な 変更を行なうことができます。

```
...
title windows
    map (hd0) (hd1)
    map (hd1) (hd0)
    chainloader (hd1,0)+1
...
```

上記の例では、Windows が 2 台目のハードディスクから始まっていることを示しています。ハードディスクの論理的な順序は map コマンドで 変更することができます。この仕組みは、GRUB2 のメニューファイルには影響 しません。そのため、2 台目のハードディスクは chainloader に指定しなければなりません。

8.7 さらになる情報

GRUB2 に関する広範囲の情報は、<http://www.gnu.org/software/grub/> (英語) に記載されています。grub の info ページを読むことも できます。特定の問題について調べるには、<http://ja.opensuse.org/SDB:SDB> (日本語) または http://en.opensuse.org/Portal:Support_database/ (英語) にある サポート

データベースから、「GRUB2」キーワードを指定することで検索 することもできます。

特殊なシステム機能

本章では、仮想コンソールやキーボードレイアウトに関する、様々なソフトウェア パッケージに関する情報を提供しています。それぞれ `bash`, `cron`, `logrotate` などのソフトウェア コンポーネントに関して言及していますが、これらは以前のリリース版から変更されたり 拡張されたりしているものであるためです。それらの変更が小規模であったり、重要度の低いものであったりした場合でも、これらのコンポーネントはシステムと強い結びつきがあるため、ユーザ側で既定の振る舞いを変更したい場合があります。また本章では、言語や国固有の設定 (`I18N` や `L10N` と呼ばれるもの) にも言及しています。

9.1 特殊なソフトウェアパッケージに関する情報

システム管理者や多くのユーザにとって、The programs `bash`, `cron`, `logrotate`, `locate`, `ulimit`, `free` などのプログラムはとても 重要な存在です。またマニュアル ページや `info` ページは、それぞれコマンドに に関する情報源になっていますが、両方が常に利用できるというわけではありません。また、GNU Emacs は有名かつとても機能に富んだテキストエディタです。

9.1.1 `bash` パッケージと `/etc/profile`

`bash` は既定のシステムシェルです。ログインシェルとして使用した場合は、いくつかの初期化ファイルを読み込みます。また、`bash` は下記の順序で ファイルを読み込みます：

1. /etc/profile
2. ~/.profile
3. /etc/bash.bashrc
4. ~/.bashrc

カスタムな設定は、~/.profile または ~/.bashrc のいずれかに対して行ないます。これらの ファイルを正しく処理するようにするには、それぞれ /etc/skel/.profile ファイルや /etc/skel/.bashrc ファイルを、ユーザのホーム ディレクトリにコピーしてください。また、システム更新を行なった後は、/etc/skel から設定をコピーすることをお勧めします。なお、下記のように実行すると、個人の設定を失わずに済みます：

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

上記のように実行した後、それぞれ個人の設定を *.old ファイルから反映し直してください。

9.1.2 cron パッケージ

事前に設定した時刻にコマンドを定期的かつ自動的に裏で実行させたい場合は、cron を使うのが便利です。cron は専用のタイムテーブル設定を持っていて、システムで設定されているものが存在するほか、必要であればユーザ側でも設定を行なうことができます。

cron のタイムテーブルは、/var/spool/cron/tabs ディレクトリ内に存在します。また、/etc/crontab には システム全体に反映される cron テーブルが書かれています。このファイルの場合は タイムテーブルとコマンドの間に、コマンドを直接実行させたいユーザのユーザ名を入力します。例9.1「/etc/crontab の項目」(176 ページ) の例では root が入力されています。なお、パッケージ固有のタイムテーブルは /etc/cron.d ファイル内に存在していて、上記と同様の書式になっています。詳しくは /etc/cron.d ファイルのマニュアルページ (man cron) をお読みください。

例 9.1 /etc/crontab の項目

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

なお、`crontab -e` コマンドでは `/etc/crontab` ファイルを編集することはできません。このファイルはエディタで直接開いて編集し、保存しなければなりません。

また、`/etc/cron.hourly`、`/etc/cron.daily`、`/etc/cron.weekly`、`/etc/cron.monthly` の各ディレクトリには、多数のパッケージがシェルスクリプトをインストールします。これらの動作は `/usr/lib/cron/run-crons` が制御しています。`/usr/lib/cron/run-crons` は、メインテーブル (`/etc/crontab`) で定義されているもので、15 分間隔で動作するように設定されています。そのため、実行されずに無視されるかもしれない処理であっても、適切な日時に実行されるようになっています。

毎時間や毎日などのように、定期的にメンテナンススクリプトを実行したい場合は、`/etc/crontab` の項目を利用してタイムスタンプを定期的に除去してください (例9.2「`/etc/crontab`: タイムスタンプファイルの除去」(177 ページ) の例では、毎正時になる前に `hourly` ファイルを削除したり、毎日午前 2:14 に `daily` ファイルを削除したりしています)。

例 9.2 `/etc/crontab`: タイムスタンプファイルの除去

```
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
```

もしくは、`cron.daily` が開始する時刻を、`/etc/sysconfig/cron` ファイル内の `DAILY_TIME` から設定することもできます。また、`MAX_NOT_RUN` の設定を行なうと、`DAILY_TIME` で指定した時刻に長時間コンピュータの電源を入れていなかった場合でも、毎日処理するタスクを処理するようになります。`MAX_NOT_RUN` で指定できる最大値は 14 日です。`DAILY_TIME for a longer period of time. The maximum value of MAX_NOT_RUN is 14 days.`

システムメンテナンスジョブは、それらをわかりやすくするために、複数のスクリプトとして配布されています。これらは `aaa_base` パッケージ内に含まれています。たとえば `/etc/cron.daily` には、`suse.de-backup-rpmdb`、`suse.de-clean-tmp`、`suse.de-cron-local` が含まれています。

9.1.3 ログファイル: `logrotate` パッケージ

システムサービス (デーモン) には多くの種類があり、カーネルそれ自身のほか、システム状態を規則正しく記録したり、固有のイベントを記録したりなどの処理をログファイルに行ないます。そのため、管理者は定期的にその時点でのシステムの

状態を確認できることになり、機能のエラーや失敗などを認識し、ピンポイントの精度でトラブルを解決することができます。これらのログファイルは通常、FHSで規定されている /var/log ディレクトリ内に保存され、日々増加していく形になります。logrotate パッケージは、これらのファイルの増加をコントロールするための手助けを行ないます。

logrotate の設定は、/etc/logrotate.conf で行ないます。また、include を指定すると、読み込むべき追加のファイルを指定することができます。ログファイルを生成するプログラムは、/etc/logrotate.d 内に個別の設定ファイルを生成します。上記のような設定を生成するものとして、たとえば apache2 (/etc/logrotate.d/apache2) や syslogd (/etc/logrotate.d/syslog) などがあります。

例 9.3 /etc/logrotate.conf の設定例

```
# 詳細は "man logrotate" をお読みください
# ログファイルを週単位で切り替える
weekly

# 4 週間分までの過去分を保存する
rotate 4

# 古いログファイルに切り替わったら、新しい（中身のない）ログファイルを生成する
create

# ログファイルを圧縮しておきたい場合、下記の行のコメントを外してください
#compress

# RPM パッケージは下記のディレクトリにログ切り替え情報を配置する
include /etc/logrotate.d

# lastlog や wtmp はパッケージ管理外であるため、独自に切り替える
#/var/log/wtmp {
#   monthly
#   create 0664 root utmp
#   rotate 1
#}

# システム固有のログは下記で設定します
```

logrotate は cron でコントロールするもので、毎日 /etc/cron.daily/logrotate から呼び出されます。

重要

create オプションは、/etc/permissions* ファイル内に管理者が作成した全ての設定を読み込みます。独自の修正を行なった場合は、矛盾が生じないようにご注意ください。

9.1.4 locate コマンド

locate コマンドはファイルを素早く検索するためのコマンドで、標準インストールの範囲には含まれていません。必要であれば `findutils-locate` パッケージをインストールしてください。また、`updatedb` プロセスは毎晩または起動後 15 分経過すると、自動的に開始されます。

9.1.5 ulimit コマンド

`ulimit` (*user limits* (ユーザ制限)) コマンドを利用すると、システム資源の使用について制限を設定することができるほか、設定内容を表示させることができます。`ulimit` は特に、アプリケーションに対するメモリ制限を設定するのに便利です。アプリケーションがシステム資源を多く使いすぎることを防ぎ、オペレーティングシステムがスローダウンしたりハングアップしたりすることを防ぐことができます。

`ulimit` コマンドには様々なオプションを指定することができます。メモリの使用量を制限したい場合は、表 9.1「`ulimit`: ユーザに対する資源設定」(179 ページ)にあるオプションをお使いください。

表 9.1 `ulimit`: ユーザに対する資源設定

<code>-m</code>	最大常駐セットサイズ
<code>-v</code>	シェルに対して解放する仮想メモリの最大値
<code>-s</code>	スタックの最大サイズ
<code>-c</code>	作成するコアファイルの最大サイズ
<code>-a</code>	現在の制限全てを表示

システム全体の設定は、`/etc/profile` に指定することができます。ここではコアファイルの生成 (デバッグ 目的で プログラマが必要とするもの) を有効にしています。通常のユーザは、システム管理者が `/etc/profile` で設定した値を増やすことができませんが、独自の設定を `~/.bashrc` で指定することができます。

例 9.4 `ulimit: ~/.bashrc` 内の設定

```
# 最大常駐セットサイズ (物理メモリ):  
ulimit -m 98304  
  
# 仮想メモリの制限:  
ulimit -v 98304
```

メモリの割り当ては KB (キロバイト) 単位で指定しなければなりません。詳しい情報は、`man bash` をお読みください。

重要

全てのシェルが `ulimit` に対応しているわけではありません。PAM (たとえば `pam_limits`) では、これらの制限を含む 広範囲の機能を提供しています。

9.1.6 `free` コマンド

`free` コマンドは未使用の物理メモリ量と未使用のスワップ量を 表示するほか、カーネルで消費されているバッファとキャッシュの容量も表示することができます。このような *利用可能な RAM* という考え方は、統合的なメモリ管理を行なうよりも前に存在した 考え方です。空きメモリは無駄なメモリの発想は Linux にも当てはまるもので、その結果として Linux は空きまたは未使用のメモリを生じ させずにキャッシュのバランスをとる動作を行なっています。

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関する直接の知識は持っていません。その代わり、アプリケーションやユーザデータを ページキャッシュ 内で管理しています。メモリが不足しはじめると、それらの一部は それらがもともと `mmap` コマンド経由で読み込んでいた スワップパーティションやファイルに書き込まれるようになります (詳しくは `man mmap` をお読みください)。

また、カーネルには上記以外のキャッシュ機能があります。たとえばネットワーク アクセスのキャッシュ情報を保存する *slab* キャッシュ などがあります。これは `/proc/meminfo` 内のカウンタ 間の違いを説明するもので、それらの多く (ただし全てではありません) は `/proc/slabinfo` からアクセスすることができます。

ただし、どれだけの RAM が現在使用中であるのかを知るのが目的である場合は、`/proc/meminfo` ファイルを読むのが良いでしょう。

9.1.7 マニュアルページと `info` ページ

いくつかの GNU アプリケーション (たとえば tar など) では、マニュアルページのメンテナンスが行われていないものがあります。これらのコマンドの場合は、より詳しい手順の書かれている info ページの概要を、`--help` オプションで得ることができます。Info ページは GNU のハイパーテキストシステムです。Info ページ自身の情報については、`info info` と入力することで表示することができます。info ページは emacs から `emacs -f info` と入力することで閲覧できるほか、`info` と入力することで直接読むこともできます。これ以外にも `tkinfo`, `xinfo` やヘルプシステムを利用して閲覧することもできます。

9.1.8 man コマンドを利用したマニュアルページの選択

マニュアルページを読むには、`man ページ名` のように入力します。異なるセクションに同じ名前のもものが存在する場合は、セクション番号の一覧が表示されます。この場合は表示したいセクション番号を指定してください。何も入力せずにしばらく待つと、最初に該当するマニュアルページが表示されます。

このような動作をシステム既定の動作に戻したい場合は、`~/bashrc` などのシェル初期化ファイルに対し、`MAN_POSIXLY_CORRECT=1` を設定してください。

9.1.9 GNU Emacs の設定

GNU Emacs は複雑な作業環境です。本章では、GNU Emacs が起動する際に処理される設定ファイルについて述べています。本章よりも詳しい情報については、<http://www.gnu.org/software/emacs/> をご利用ください。

Emacs は起動時にいくつかのファイルを読み込み、ユーザやシステム管理者、もしくはディストリビュータのカスタマイズや事前設定を反映します。設定ファイル `~/emacs` は `/etc/skel` からそれぞれのユーザのホームディレクトリにインストールされます。また `.emacs` は、`/etc/skel/.gnu-emacs` を読み出す構成になっています。プログラムをカスタマイズするには、`.gnu-emacs` ファイルをホームディレクトリにコピー (`cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) し、必要な設定を記入してください。

`.gnu-emacs` は `~/gnu-emacs-custom` ファイルを、カスタムファイルとして定義しています。Emacs 内で `customize` (カスタマイズ) オプションを利用して設定を行なうと、それらは `~/gnu-emacs-custom` 内に保存されます。

openSUSE では、emacs パッケージは `/usr/share/emacs/site-lisp` 内に `site-start.el` ファイルをインストールします。このファイルは、`~/.emacs` の初期化ファイルよりも先に読み込まれるため、その他のスクリプトとあわせて、Emacs のアドオンパッケージ (たとえば `psgml`) とともに配布される、特別な設定ファイルを自動で読み込むことができるようになっています。この種類の設定ファイルは `/usr/share/emacs/site-lisp` にも含まれ、`suse-start-` で始まるファイル名になっています。ローカルのシステム管理者は、システム全体の設定を `default.el` で指定することができるようになっています。

これらのファイルについてさらに詳しい情報は、Emacs の `info` ファイル内、*Init File* 以下にあります: [info:/emacs/InitFile](#) これらのファイルの (必要に応じて) 読み込みを無効化するための情報についても、この場所に書いてあります。

Emacs のコンポーネントは、複数のパッケージに分割されています:

- `emacs`: 基本パッケージ。
- `emacs-x11`: X11 対応 のプログラム (通常インストールされます)。
- `emacs-nox`: X11 に対応していない プログラム。
- `emacs-info`: `info` フォーマットで書かれたオンラインドキュメント。
- `emacs-el`: Emacs Lisp 形式の非コンパイルライブラリファイル。実行に際して必要となるものではありません。
- `emacs-auctex` (LaTeX), `psgml` (SGML と XML), `gnuserv` (クライアント および サーバ動作) など: 必要に応じて様々なアドオンパッケージをインストールできます。

9.2 仮想コンソール

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 システムであっても便利なもので、テキストモードで 6 つの仮想コンソールが利用できるようになっています。それぞれは `Alt + F1` から `Alt + F6` までを利用して切り替えることができます。7 番目のコンソールは X システム用に予約されているもので、10 番目のコンソールは カーネルのメッセージを表示するためのものです。`/etc/inittab` ファイルを編集することで、コンソールの割り当てを増やしたり減らしたりすることができます。

X システムをシャットダウンせずにコンソールを切り替えたい場合は、Ctrl + Alt + F1 から Ctrl + Alt + F6 までの範囲でキーを押してください。X システムに戻るには、Alt + F7 を押します。

9.3 キーボードマッピング

各プログラムによるキーボードマッピング機能を標準化するため、それぞれ下記のファイルに変更を行ないます：

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.emacs
/etc/skel/.gnu-emacs
/etc/skel/.vimrc
/etc/csh.cshrc
/etc/termcap
/usr/share/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/バージョン/site-lisp/term/*.el
```

これらの変更は terminfo の項目を使用する アプリケーションにだけ影響し、設定ファイルを直接変更する場合 (vi, emacs など) にのみ影響があります システムに同梱されていないアプリケーションは、これらの既定値には 影響されません。

X 環境下では、コンポーズキー (マルチキー) は /etc/X11/Xmodmap に説明されているとおりの方法で 有効にすることができます。

さらなる設定は、X キーボード拡張 (XKB) を使用することで実現できます。この拡張は GNOME (gswitchit) や KDE (kxkb) でも使用されています。

ヒント: さらなる情報

XKB に関する詳しい情報は、/usr/share/doc/packages/xkeyboard-config ファイル (xkeyboard-config パッケージ内) に示されている 文書をお読みください。

9.4 言語と国の設定

システムはかなり広い範囲で国際化対応が行なわれているため、各言語や国の 要件に合わせた設定を行なうことができます。国際化 (*Internationalization*, 略して *I18N*) とは、特定の地域化 (*Localization*, 略して *L10N*) を実施できるようにする

意味で用いられる用語で、それぞれ単語の最初と最後の文字と、省略されている文字数から略称が作られています。

それぞれの国際化設定は、`/etc/sysconfig/language` ファイル内にある `LC_` で始まる変数に設定を行なうことで実現します。これらの変数では *各国語対応* だけでなく、*メッセージ (翻訳)*, *文字セット*, *並べ替え順序*, *日付と時刻*, *数字*, *通貨* などの領域にも適用されます。それぞれの分野は個別の変数を使用して別々に指定を行なうこともできますし、ファイル `language` から間接的に指定することもできます (詳しくは `locale` のマニュアルページをお読みください)。

`RC_LC_MESSAGES` (メッセージ), `RC_LC_CTYPE` (文字分類), `RC_LC_COLLATE` (文字照合), `RC_LC_TIME` (日付と時刻), `RC_LC_NUMERIC` (数値), `RC_LC_MONETARY` (通貨)

これらの変数は `RC_` の接頭辞を抜いた形でシェルに渡され、それぞれの範囲に適用されます。なお、関連するシェル プロファイルは下記に示しています。また、現在の設定は `locale` コマンドで表示できます。

`RC_LC_ALL`

この変数が設定されていれば、上記で説明した変数はそれぞれ上書きされます。

`RC_LANG`

上記の変数がいずれも設定されていない場合は、これが次点の候補となります。既定では `RC_LANG` だけが設定されます。この変数は、それぞれ個別に設定するよりも簡単に利用できるようにするために設けられています。

`ROOT_USES_LANG`

`yes` または `no` の値を設定する変数です。`no` に設定した場合は、`root` ユーザは常に `POSIX` 環境で作業を行なうことになります。

また、これらの値は `YaST sysconfig` エディタから設定することもできます。値として設定する内容には、言語コードのほか国コードやエンコーディング、修飾子などを入れることができます。それぞれの要素はそれぞれ特殊文字で下記のようにつながります:

```
LANG=<言語>[_<国>].<エンコーディング>[@<修飾子>]]
```

9.4.1 いくつかの例

言語と国については常にセットで指定してください。言語には ISO 639 に準拠した値を設定します。詳しくは <http://www.evertype.com/standards/iso639/>

[iso639-en.html](#) と <http://www.loc.gov/standards/iso639-2/> をお読みください。国については ISO 3166 に準拠した値を設定します。詳しくは http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html をお読みください。

なお、設定可能な値の組み合わせについては、`/usr/lib/locale` ディレクトリ内をご覧ください。このディレクトリ以下のサブディレクトリとしてそれぞれ設定可能な組み合わせが存在しています。また、追加の説明ファイルについては、`localedef` コマンドを使用することで `/usr/share/i18n` ディレクトリ以下のファイルから作成することができます。説明ファイルは `glibc-i18ndata` パッケージの構成の一部です。たとえば `en_US.UTF-8` (アメリカ英語) 向けの説明ファイルを作成するには、下記のように入力します:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

```
LANG=en_US.UTF-8
```

上記は、インストール時にアメリカ英語を選択した場合に設定される言語の既定値です。他の言語を選択した場合は、その選択した言語に合わせて設定が作成されますが、UTF-8 については常に有効になります。

```
LANG=en_US.ISO-8859-1
```

上記は言語を英語に、国をアメリカに設定し、文字セットを ISO-8859-1 に設定した場合の例です。この文字セットではユーロ記号に対応していませんが、UTF-8 に対応していないプログラムを動作させる場合には便利な設定です。文字セットの定義 文字列 (この場合は ISO-8859-1) は、`emacs` などのプログラム側で処理されます。

```
LANG=en_IE@euro
```

上記の例は、言語設定にユーロ記号を含めるよう明示的に設定している例です。この設定は、既に UTF-8 ではユーロ記号が含まれることから、古い表現です。この設定は ISO-8859-15 に対応していて UTF-8 には対応していないアプリケーションを動作させる場合にのみ有効です。

従来のリリースでは、`/etc/sysconfig/language` に何らかの変更を行なった場合、`SuSEconfig` を実行する 必要がありました。`SuSEconfig` は `/etc/SuSEconfig/profile` と `/etc/SuSEconfig/csh`、`login` にそれぞれ設定を書き込むようになっていて、ログイン時に `/etc/profile` (`bash` の場合) または `/etc/csh`、`login` (`tcsh` の場合) を読み込むことで 設定を受け継ぐようになっています。

新しいリリースでは、`/etc/SuSEconfig/profile` が `/etc/profile.d/lang.sh` に、`/etc/SuSEconfig/csh`、`login` が `/etc/profile.d/lang.csh` に置き換わっ

ていますが、古いほうのファイルが存在する場合も、古いほうのファイルは従来通り読み込まれます。

この処理は下記のように行なわれます:

- bash 向けには、`/etc/profile` が `/etc/profile.d/lang.sh` を呼び出すようになっていて、ここから `/etc/sysconfig/language` を読み込みます。
- tcsh 向けには、ログイン時に `/etc/csh.login` が `/etc/profile.d/lang.csh` を呼び出すようになっていて、ここから `/etc/sysconfig/language` を読み込みます。

このような仕組みにより、SuSEconfig を実行することなく `/etc/sysconfig/language` ファイルが次のログイン時に読み込まれるようになっています。

なお、ユーザ側でも自分用の設定を行なうことができます。これを行なうには、`~/.bashrc` に設定を行なってください。たとえばシステム側で設定されている `en_US` をプログラムのメッセージ表示に使いたくない場合は、上記のファイルに `LC_MESSAGES=es_ES` という行を追加すると、メッセージはスペイン語で表示されるようになります。

9.4.2 ~/.i18n 内でのロケール設定

お使いのシステム言語設定の既定値に満足できない場合は、bash スクリプトの書式で `~/.i18n` ファイルを作成することで、設定を変更することができます。`~/.i18n` ファイルは、`/etc/sysconfig/language` ファイルにあるシステムの既定値を上書きすることができます。それぞれ `RC_` の接頭辞を抜いて変数を指定してください。たとえば `RC_LANG` を上書きしたい場合は、`LANG` と指定して下記のように指定します:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

9.4.3 言語サポートの設定

メッセージのファイル分類では、決まり事として 関連する言語ディレクトリ (たとえば `en`) だけを次点候補として利用します。たとえば `LANG` を `en_US` に設定している環境の場合、メッセージファイルが `/usr/share/locale/en_US/LC_MESSAGES` 内に存在しなかったときは、`/usr/share/locale/en/LC_MESSAGES` ファイルを次点候補とします。

言語の候補は自由に設定することができます。たとえばブルトン語が存在すればそのメッセージを表示し、存在しない場合はフランス語で表示したい場合は下記のようになります:

```
LANGUAGE="br_FR:fr_FR"
```

また、ガリシア語／スペイン語／ポルトガル語の順で表示したい場合は下記のように設定します:

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

また必要であれば、ノルウェー語のニーノシュクとブークモールを試するような設定を行なうこともできます (さらなる候補として `no` も指定しています):

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

または

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

なお、ノルウェー語では `LC_TIME` もそれぞれ別々に扱われます。

なお、このような設定を利用する場合には 1 つだけ問題が発生する可能性が考えられます。それは、文字間を区切るセパレータ (区切り子) の存在です。たとえば `LANG` 変数に 2 文字の言語コードだけを指定したような場合 (例: `de`)、`glibc` が使用する定義ファイルが `/usr/share/lib/de_DE/LC_NUMERIC` のようなディレクトリに置かれていると、読み出すことができなくなってしまいます。この場合は、`LC_NUMERIC` に `de_DE` のような指定を行なってください。

9.4.4 さらなる情報

- *The GNU C Library Reference Manual* 内の「Locales and Internationalization」章をお読みください。この文書は `glibc-info` パッケージに含まれています。
- <http://www.cl.cam.ac.uk/~mgk25/unicode.html> から参照できる、Markus Kuhn 氏による *UTF-8 and Unicode FAQ for Unix/Linux*

- howto パッケージ に含まれる、Bruno Haible 氏 による *Unicode-Howto*:
<http://tldp.org/HOWTO/Unicode-HOWTO-1.html>

udev による動的なカーネルデバイス管理

10

カーネルには、システムの実行中に任意のデバイスを追加したり削除したりする機能が備わっています。デバイス状態の変化（デバイスが接続されたり削除されたり）はユーザ側に通知する必要がありますし、接続されて認識されるとすぐに設定を行なう必要があります。また、特定のデバイスを利用しているユーザが存在する場合は、そのデバイスの認識状態についても変化を通知する必要があります。udev では、`/dev` ディレクトリ内に存在するデバイスノードファイルとシンボリックリンクについて、動的に管理するために必要なインフラストラクチャを提供しています。また、udev のルールはカーネル デバイスのイベント処理に外部ツールを接続する方法を提供するものです。たとえばカーネルのデバイス処理の一部として特定のスクリプトを追加で実行したり、デバイスの処理時に評価を行なう目的で追加データを要求したり取り込んだりするなど、デバイスの処理方法をカスタマイズすることができます。

10.1 `/dev` ディレクトリ

`/dev` ディレクトリ内にあるデバイスノードは、それぞれ 関連するカーネルデバイスに対して、アクセスを提供するためのものです。udev を利用することで、`/dev` ディレクトリは現在のカーネル状態を反映するようになります。各カーネルデバイスには 1 つのデバイスファイルが存在します。ある デバイスがシステムから取り外されると、デバイスノードが削除されます。

`/dev` ディレクトリの内容はテンポラリファイルシステム 上に存在していて、全てのファイルはシステム起動時に作成されます。設計上、このディレクトリ内に手動でファイルを作成しても、システムを再起動すると ファイルは消えてしまいます。関連するカーネルの状態に関わらず `/dev` ディレクトリ内に存在すべき固定のファイルや

ディレクトリについては、`/lib/udev/devices` ディレクトリ内に配置することができます。システム起動時に左記の ディレクトリ内容は `/dev` ディレクトリに、`/lib/udev/devices` に存在したものと同一所有権設定と パーミッションのままコピーされます。

10.2 カーネルの uevents と udev

必要なデバイス情報は `sysfs` ファイルシステムから受け取る仕組みです。カーネルが検出して初期化した 各デバイスに対して、デバイス名の付いた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情報を含む属性ファイルが入っています。

デバイスが追加されたり削除されたりするたびに、カーネルは `udev` に対して変更を通知するため `uevent` を送信します。`udev` デーモンは、起動時に `/etc/udev/rules.d/*.rules` ファイルから提供される全てのルールを読み込んで処理し、メモリ内に記憶します。ルールファイルを変更したり追加または削除したりした場合は、`udevadm control reload_rules` コマンドを利用して、デーモンに対してメモリ内の記憶を読み込み直すように指定することができます。同じことが `/etc/init.d/boot.udev reload` コマンドでも 行なうことができます。`udev` のルールと書式について、詳しくは 10.6 項「`udev` ルールによるカーネル側デバイスイベント処理への影響」(193 ページ) をお読みください。

それぞれ受信したイベントは、提供されたルールセットとの適合処理を行ないます。各ルールは、追加したりイベントの環境キーを変更したりすることができるほか、作成するデバイスノードに対して特定の名前を要求したり、ノードを示す シンボリックリンクを追加したり、デバイスノード作成後に実行すべきプログラム を追加したりすることができます。ドライバ中枢部分の `uevents` は、カーネルの `netlink` ソケットを利用して受信します。

10.3 ドライバ、カーネルモジュール、デバイス

カーネルのバスドライバは、デバイスに対する探査を行ないます。カーネルはデバイスを 検出すると、それぞれに対して内部用のデバイス構造を作成し、ドライバの中枢部から `uevent` の形で `udev` デーモンに 送信します。バスデバイスは特別に作成した ID の形で、自分自身がどんな種類の デバイスであるのかを識別できる値になっています。通常、これらの ID は製造元 ID と製品 ID、およびサブシステム固有の値から構成されています。各バスは それらの ID について独自の方針を持ってい

て、それらは MODALIAS と呼ばれます。まとめると、カーネルはデバイス情報を取得してそれらの情報から MODALIAS ID 文字列を生成し、イベントとともにその値を送信します。USB マウスの場合、たとえば下記ようになります：

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

各デバイスドライバには、処理可能なそれぞれのデバイスに対して、既知の別名を保持しています。その一覧はカーネルモジュールファイル自身に含まれる形になっています。depmod プログラムは利用可能な全てのモジュールに対して ID の一覧を読み込み、カーネルの /lib/modules ディレクトリ以下の modules.alias ファイルを作成します。このような構造から、モジュールの読み込みは、MODALIAS を含んだ各イベントに対して modprobe を呼び出すだけの簡易な処理で実現できるようになっています。modprobe \$MODALIAS が呼び出されると、モジュールが提供する別名情報の一覧内を検索し、適合する項目があればそのモジュールを読み込むようになっています。これらの処理は全て udev から自動的に実行されます。

10.4 起動と初期デバイス設定

udev が起動する前の起動処理時に発生した全てのデバイスイベントは、読み込むことができません。これはこれらのイベントを処理するための仕組みがルートファイルシステム内に存在していて、その時点ではそれらを利用できないためです。このような損失をカバーするため、カーネルは sysfs ファイルシステム内の各デバイスディレクトリ内に uevent というファイルを提供しています。これらのファイルに add と書き込むことで、起動時に送信され失われてしまったものと同じイベントを再送することができます。/sys 内にある全ての uevent ファイルに対して単純に繰り返して処理するだけで、デバイスノードを作成してデバイスの設定を実施するために必要な、全てのイベントを再送することができます。

たとえば、その時点ではドライバを用意することができない理由から、初期の起動処理で USB マウスの準備は行なわれません。そのためデバイス検出のイベントは失われ、それらのデバイスに対するカーネルモジュールの発見もできなくなってしまいます。接続されている可能性のあるデバイスを手動で検索する代わりに、udev はルートファイルシステムの準備が完了すると、カーネルが検出した全てのデバイスに対してイベントを要求し、USB マウスに対するイベントが再度送信されるようにしています。マウント済みのルートファイルシステム内にカーネルモジュールが見つかったら、USB マウスが利用できるようになります。

ユーザ側からは、デバイスのコールドプラグ（システム起動時から接続すること）と稼働時のデバイス検出には確認できる違いはありません。両方のケースとも同じルールが適用され、同じ設定済みプログラムが実行されます。

10.5 udev デーモンの稼働監視

udevadm monitor プログラムを使用すると、ドライバ中枢部の イベントと udev のイベント処理 タイミングについて視覚化を行なうことができます。

```
UEVENT[1185238505.276660] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1 (usb)
UDEV [1185238505.279198] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1 (usb)
UEVENT[1185238505.279527] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV [1185238505.285573] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10 (input)
UDEV [1185238505.305026] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10 (input)
UEVENT[1185238505.305442] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/mouse2 (input)
UEVENT[1185238505.306440] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/event4 (input)
UDEV [1185238505.325384] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/event4 (input)
UDEV [1185238505.342257] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/mouse2 (input)
```

UEVENT の行には、netlink を介してカーネルが送信した イベントを表示しています。UDEV の行には、完了済みの udev イベントハンドラを表示しています。タイミング情報はマイクロ秒単位で表示されます。UEVENT と UDEV の行の時間差は、udev がそのイベントの処理を行なうために費やした時間か、もしくは関連していたり既に実行中だったりするイベントと同期を待ちあわせるため、実行を遅らせた時間を表わします。たとえばハードディスクのパーティションに対するイベントは、常にディスクそのもののイベントが完了するまで待機します。これは、ディスク全体の イベントが問い合わせるハードウェア情報に依存して動作するためです。

udevadm monitor --env コマンドを入力すると、完全な イベント環境を表示します:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

udev は syslog にもメッセージを送信します。syslog 上のどの場所にメッセージを送信するかを制御する syslog 既定の優先度 (priority) 設定は、udev の設定

ファイル `/etc/udev/udev.conf` で指定することができます。既に起動中のデーモンに対して `priority` を変更するように指定したい場合は、`udevadm control log_priority=レベル/番号` のように実行します。

10.6 udev ルールによるカーネル側デバイスイベント処理への影響

udev のルールは、カーネルがイベント 自身に追加したプロパティ情報や、カーネルが `sysfs` 経由で エクスポートした情報であれば、どんなものにでも適合させることができます。また、ルールでは外部のプログラムから得られる 追加情報を要求することもできます。また、それぞれのイベントは提供された全ての ルールに対して適合性を確認します。全てのルールは `/etc/udev/rules.d` ディレクトリ内に配置します。

ルールファイル内のそれぞれの行には、少なくとも 1 対のキーと値が書かれています。キーには 2 種類のものがあります。それは適合キーと代入キーです。全ての適合キー がその値と適合するとそのルールが適用され、代入キーで指定された値が代入されます。適合ルールにはデバイスノードの名前のほか、ノードを指し示すシンボリックリンクや イベント処理の一部として指定したプログラムを指定することもできます。適合する ルールが見つからない場合は、デバイスノードの作成には既定のデバイスノード名が 使用されます。ルールの文法と提供されている適合キーまたは取り込みデータについては、それぞれ udev のマニュアルページで 説明しています。下記の例では、udev のルール文法に関する基本的な内容を説明しています。下記の例は `/etc/udev/rules.d/50-udev-default.rules` ファイル内に 存在するルールからの抜粋です。

例 10.1 udev ルールの例

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pi lot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

console のルールには 3 種類のキーが含まれています: 1 つは適合キー (KERNEL) で、残りの 2 つは代入キー (MODE, OPTIONS) になっています。KERNEL 適合ルール

では、デバイス一覧を検索して `console` の種類に該当する任意の項目を探します。厳密に一致した項目だけに対して適合と判断し、ルールを実行するように設定されています。また、MODE キーではデバイスノードに対して特別なパーミッションを設定しています。この場合、このデバイスの所有者に対して読み込みと書き込みの権限を付与しています。OPTIONS キーでは、この種類のデバイスに対して適用すべきルールの最後を指定しています。この種類のデバイスに対して、これ以降に何らかのルールが書かれていても、それらは無視されます。

次に `serial devices` のルールは `50-udev-default.rules` 内には現在はありませんが、説明を行なうには便利であるため記載しました。このルールには 2 つの適合キー (KERNEL と ATTRS) と 1 つの代入キー (SYMLINK) が含まれています。KERNEL キーは、`ttyUSB` の種類を持つ全てのデバイスを検索します。ワイルドカード `*` を使用することで、このキーはこれらのデバイスの複数に適合するようになっています。2 つめの適合キーである ATTRS は、任意の `ttyUSB` デバイスに対して、`sysfs` 内の `product` 属性ファイルを読み込んで、特定の文字列が含まれているかどうかを確認しています。代入キー (SYMLINK) では、このデバイスのシンボリックリンクを `/dev/pilot` ディレクトリに追加するように指定しています。このキーで使用されている演算子 (`+=`) は、`udev` に対してこの動作を追加で実行するよう指定しているもので、以前のルールやその後のルールで既にシンボリックリンクを設定済みであっても追加できるようにしているものです。このルールには 2 つの適合キーが存在するため、両方の条件に該当した場合にのみこのルールが適用されます。

また、`printer` のルールは USB プリンタを扱うためのもので、ルール全体を適用するかどうかを判断するための、2 つの適合キー (SUBSYSTEM と KERNEL) が含まれています。3 つ存在する代入キーでは、この種類のデバイスに対する命名 (NAME) とシンボリックリンクの作成 (SYMLINK)、およびこの種類のデバイスに対するグループ指定 (GROUP) を行なっています。KERNEL キー内には `*` というワイルドカードを含んでいるため、複数の `lp` プリンタ デバイスに適合するようになっています。置換文字列はそれぞれ NAME と SYMLINK のキーで使用されていて、内部のデバイス名に置き換えるような作りになっています。たとえば 1 台目の `lp USB プリンタ` であれば、`/dev/usb/lp0` のようになります。

さらに `kernel firmware loader` のルールでは、その実行時に `udev` に対して外部のヘルパースクリプトを起動して、追加のファームウェアを読み込むように指定しています。また、SUBSYSTEM の適合キーでは `firmware` サブシステムを対象としています。ACTION キーは、デバイスが `firmware` サブシステムに属しているかどうかを追加で判断するように指定しています。最後の `RUN+=` キーでは、読み込むべきファームウェアの場所を判断するため、`firmware.sh` スクリプトを実行するように指定しています。

いくつかの汎用ルールを下記に示します：

- 各ルールには 1 つ以上のキーと値の組み合わせが書かれていて、それらはカンマで区切ります。
- キーの操作は演算子で決定します。udev ルールは複数の演算子に対応しています。
- 実値として与える値は、引用符で括らなければなりません。
- ルールのファイル内の各行は 1 つのルールを表わすものです。1 行よりも長いルールを記述する場合は、シェルで利用するのと同じ `¥` 記号を行末に書き込んで連続していることを宣言してください。
- udev のルールでは、シェル形式の パターンマッチを利用することができます。それぞれ `*`, `?`, `[]` を利用することができます。
- udev のルールは置換文字列に 対応しています。

10.6.1 udev ルール内の演算子指定

キーを作成するにあたっては、いくつかの演算子の中から演算子を指定することになります。これは作成したいキーの種類に依存します。適合キーの場合は検索値に該当するかどうかの条件を指定します。適合キーには下記の演算子を利用します:

`==`

等しいかどうかを検証します。キーに検索パターンが含まれている場合、そのパターンに該当するもの全てを有効と見なします。

`!=`

等しくないかどうかを検証します。キーに検索パターンが含まれている場合、そのパターンに該当するもの全てを有効と見なします。

代入キーの場合は、下記の演算子を利用します:

`=`

キーに値を代入します。以前のルール処理で、そのキーに値の一覧が代入されていた 場合は、キーはリセットされて単一の値が代入されます。

`+=`

項目の一覧を保持しているキーに対して、値を追加します。

:=

最終値を代入します。後のルールでの変更を許可しないようになります。

10.6.2 udev ルール内での置換文字列の使用

udev のルールでは、プレースホルダや 置換文字列を使用することができます。これらは他のスクリプトで行なうのと似たような 仕組みになっています。下記に udev で使用できる置換文字列の一覧を示します:

%r, \$root

デバイスディレクトリを表わします。既定では /dev です。

%p, \$devpath

DEVPATH の値を表わします。

%k, \$kernel

KERNEL の値か、もしくは内部デバイス名の値を表わします。

%n, \$number

デバイス番号を表わします。

%N, \$tempnode

デバイスファイルの一時名を表わします。

%M, \$major

デバイスのメジャー番号を表わします。

%m, \$minor

デバイスのマイナー番号を表わします。

%s{*attribute*}, \$attr{*attribute*}

variable で指定した sysfs 属性の値を表わします。

%E{*variable*}, \$attr{*variable*}

variable で指定した 環境変数の値を表わします。

%c, \$result

PROGRAM の出力を表わします。

%%

% 文字そのものを表わします。

\$\$

\$ 文字そのものを表わします。

10.6.3 udev 適合キーの使用

適合キーは、udev のルールを適用する前に判断すべき条件を記述するものです。それぞれ下記の適合キーを利用することができます：

ACTION

イベントの動作種類を表わします。add でデバイスを追加したときに、remove でデバイスを除外したときに 適合と判断します。

DEVPATH

イベントデバイスのデバイスパスを表わします。たとえば DEVPATH=/bus/pci/drivers/ipw3945 のように指定すると、ipw3945 ドライバに関連した全てのイベントを適合と判断するようになります。

KERNEL

イベント対象の内部 (カーネル) での名前を表わします。

SUBSYSTEM

イベント対象のデバイスについて、サブシステムを表わします。たとえば SUBSYSTEM=usb のように指定すると、USB デバイスに関連する全てのイベントに適合するようになります。

ATTR{filename}

イベント対象のデバイスについて、sysfs での属性を表わします。たとえば vendor 属性 ファイル名に対して文字列が含まれているかどうかを確認するには、ATTR{vendor}=="0n[sS]tream" のように指定します。

KERNELS

udev に対して、該当する デバイス名を検索するため上位のデバイスパスを検索するように指定します。

SUBSYSTEMS

udev に対して、該当する サブシステム名を検索するため上位のデバイスパスを検索するように指定します。

DRIVERS

udev に対して、該当する デバイスドライバを検索するため上位のデバイスパスを検索するように指定します。

ATTRS{ファイル名}

udev に対して、該当する sysfs 属性値を検索するため 上位のデバイスパスを検索するように指定します。

ENV{key}

環境変数の値を表わします。たとえば ENV{ID_BUS}="ieee1394" のように指定すると、FireWire のバス ID に関連する全てのイベントに 適合するようになります。

PROGRAM

udev に対して外部プログラムを 実行するように指定します。適合と判断させるには、プログラムは 0 を返さなければ なりません。プログラムが標準出力 (stdout) に出力した内容は、RESULT キーから利用することができます。

RESULT

最後の PROGRAM 呼び出しに対して、出力文字列の適合 処理を行ないます。このキーは PROGRAM キーを指定した のと同じルール内で行なうか、もしくはそれ以降のルールで行なうことが できます。

10.6.4 udev 代入キーの使用

上述の適合キーとは異なり、代入キーは適合すべき条件を表わすことはありません。代入キーは値や名前を代入したり、udev で管理されるデバイスノードに対する動作を指定したりします。

NAME

作成すべきデバイスノード名を表わします。あるルールでいったんノード名が 設定されると、それ以降の全てのルールで NAME キー への代入が無視されるようになります。

SYMLINK

作成すべきノードに関連づけるシンボリックリンク名を表わします。1 つのデバイスノードに対して複数の適合ルールから、作成すべき複数のシンボリックリンクを追加することかできます。1 つのノードに対して 1 つのルールで 複数のシンボリックリンクを指定することもできます。この場合は、複数の シンボリックリンク名の間をスペースで区切ってください。

OWNER, GROUP, MODE

新しく作成するデバイスノードに対して設定する、パーミッションを指定します。設定した値は任意のルールで上書きすることができます。

ATTR{key}

イベントの発生したデバイスに対して書き込むべき、sysfs 属性の値を 指定します。== 演算子を使用すると、このキーは sysfs 属性に対する 適合キーとして解釈されます。

ENV{key}

udev に対して環境変数に 値を設定するように指定します。== 演算子を使用 すると、このキーは環境変数に対する適合キーとして解釈されます。

RUN

udev に対して、この デバイスに対して実行するプログラムの一覧にプログラム を追加するよう 指定します。なお、このデバイスに対する後続のイベント処理を 止めないように する目的で、実行するプログラムは非常に短い時間で完了する タスクにしてください。

LABEL

GOTO からジャンプすることのできるラベルを 指定します。

GOTO

udev に対して、複数のルールを 飛ばしてラベルの位置まで移動するよう指定 します。

IMPORT{種類}

値を外部プログラムの出力などのイベント環境に読み込みます。udev は複数の 種類の値を 取り込むことができます。種類を指定しない場合、udev はファイルパーミッションの 実行許可ビットをベースにして、種類を自分自身で判別しよ うとします。

- program を指定すると、udev は外部プログラムを 実行して、その出力を取り 込みます。
- file を指定すると、テキストファイルを取り込みます。
- parent を指定すると、udev に対して親デバイスから 保存されたキーを取り 込むよう指定します。

WAIT_FOR_SYSFS

udev に対して、特定のデバイスに 対する sysfs ファイルが 作成されるまで待 機するよう指定します。たとえば WAIT_FOR_SYSFS="ioerr_cnt" のように指定 すると、udev は ioerr_cnt ファイルが作成されるまで待機します。

OPTIONS

OPTION キーにはそれぞれ下記の値を指定することができます：

- `last_rule` を指定すると、udev はそれ以降の全てのルールを 無視するようになります。
- `ignore_device` を指定すると、udev はこのイベントを完全に 無視するようになります。
- `ignore_remove` を指定すると、udev はデバイスに対して 後ほど発生するはずの取り外しイベントを無視するようになります。
- `all_partitions` を指定すると、udev はブロックデバイス上の 全ての利用可能なパーティションについて、デバイスノードを作成するようになります。

10.7 固定のデバイス命名

動的なデバイスディレクトリと udev ルールの 仕組みにより、全てのディスクデバイスに対して、その認識順序や接続方法に依存しない固定の 名前が存在するようになっています。カーネルが作成するそれぞれのブロックデバイスは、特定のバスやドライバ種類、ファイルシステムについて知っているツールを実行することで 確認を行ないます。動的なカーネル提供のデバイスノード名とともに、udev ではそのデバイスを指し示す シンボリックリンクの形で、固定の構造を生成する仕組みになっています:

```
/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-02773:0:2 -> ../../sdd
|   |-- usb-02773:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

10.8 udev で使用するファイル

`/sys/*`

Linux カーネルから提供されている仮想ファイルシステムで、既知の全てのデバイスについて情報を公開しています。この情報は、デバイスノードを `/dev` 以下に作成する際に `udev` が使用します。

`/dev/*`

動的に作成されたデバイスノードと、`/lib/udev/devices/*` からコピーされた静的コンテンツの両方が含まれます。

下記のファイルやディレクトリは、`udev` を構成するために欠くことのできないものです：

`/etc/udev/udev.conf`

メインの `udev` 設定ファイルです。

`/etc/udev/rules.d/*`

`udev` イベント適合ルールです。

`/lib/udev/devices/*`

`/dev` に配置される静的なデバイスノードなどを表わすディレクトリです。

`/lib/udev/*`

`udev` ルールから呼び出されるヘルパープログラムです。

10.9 さらなる情報

`udev` の仕組みについてさらなる情報を得るには、下記のマニュアルページをお読みください：

`udev`

`udev` やキー、ルール、その他 重要な設定周りの問題について、一般情報を提供しています。

`udevadm`

`udevadm` は `udev` の実行制御を行なうために使用し、カーネルイベントの要求やイベントキューの管理、およびシンプルなデバッグ機構を提供しています。

udevd

udev イベント管理デーモンに関する 情報が書かれています。

パート III. サービス

ネットワークの基礎

Linux では、様々なネットワーク構成に対応したネットワークツールと機能を 提供しています。YaST を利用することで、ネットワークカードを利用した 接続のほか、モデムなどのデバイスを設定することもできます。もちろん手動 設定も可能です。この章では、基本的なネットワーク機構と関連するネットワーク 設定について述べています。

Linux とその他の Unix オペレーティングシステムでは TCP/IP と呼ばれる プロトコルを使用しています。これは単一のプロトコルを指す言葉ではなく、様々なサービスを提供するネットワークプロトコルの集合体を意味する言葉です。2 台のマシンでデータをやりとりする場合は、表11.1「TCP/IP と関連プロトコル」(205 ページ)に示されているようなプロトコルが用いられます。また、このようにして TCP/IP を世界的に構築したネットワークのことを「インターネット」と言います。

RFC とは *Request for Comments* の略です。RFC では様々なインターネットプロトコルの説明やオペレーティングシステムでの実装方法のほか、アプリケーションについても言及している文書です。各種のプロトコルについて知識を深めるには、それぞれの RFC 文書をお読みください。RFC 文書は <http://www.ietf.org/rfc.html> から利用できます。

表 11.1 TCP/IP と関連プロトコル

プロトコル	説明
TCP	伝送制御プロトコル: 接続という手順を踏んで利用する、信頼性のあるプロトコル です。データはアプリケーション側から連続データとして提供

プロトコル	説明
	<p>され、オペレーティングシステムで適切な形式に変換されます。宛先のホストで必要なアプリケーションに届けられる際には、元のアプリケーションが送信したのと同じデータ形式に変換し直されます。また、TCP ではデータ 転送中の喪失やエラーをチェックすることができます。TCP はデータの 順序性を守るように実装されています。</p>
UDP	<p>ユーザデータグラムプロトコル: 接続を行なわない、信頼性の低いプロトコル です。アプリケーションから送信されたデータは、パケットと呼ばれる形式に 変換されて送信されます。宛先のホストに届いたことは保証されないため、データ喪失が発生する場合があります。UDP はブロック単位でやりとりする アプリケーションに向けた仕組みで、TCP よりも少ない遅延で通信を行なう ことができます。</p>
ICMP	<p>インターネットコントロールメッセージプロトコル: 一般のユーザからは 使用することのないプロトコルですが、エラー報告や TCP/IP のデータ転送に 参加しているマシンの振る舞いについて、操作を行なうことができる特殊な プロトコルです。また、ping と呼ばれるプログラムを利用して、特別な エコーパケットを送信する場合にも使用します。</p>
IGMP	<p>インターネットグループ管理プロトコル: このプロトコルは、IP マルチキャストを実装するマシンについて、その</p>

プロトコル	説明
	振る舞いをコントロール する際に利用するプロトコルです。

図11.1「TCP/IP の簡略化モデル」(207 ページ) に示されているとおり、データのやりとり には複数のレイヤ (階層) が用いられます。実際のネットワーク層は IP (インターネットプロトコル) と呼ばれ、信頼性のないデータ転送を提供する プロトコルです。この IP の上位に TCP (伝送制御プロトコル) を載せることで、データ転送の信頼性を確保しています。また、IP 層は下位のハードウェア 固有プロトコル (たとえばイーサネット) などに載せられて伝送されます。

図 11.1 TCP/IP の簡略化モデル

図ではそれぞれのレイヤに対して 1 つ 2 つ程度の例を示しています。階層は 抽象レベル とも呼べるもので、最も低い階層がもっとも ハードウェアに近く、最も高い階層がハードウェアから最も遠いものになっています。また、それぞれの階層には独自の機能が備わっています。データリンク 層と物理層はイーサネットのようなネットワークで表わされます。

ほぼすべてのハードウェアプロトコルは、パケットを基本にした構造を持っています。送信すべきデータは (一回ですべてを送信できない場合に) パケット 単位でまとめられます。TCP/IP パケットでの 最大長はおおよそ 64KB 程度ですが、ハードウェアプロトコルでのパケットは それよりもずっと小さく、ネットワークのハードウェア側の仕様によって 決まります。たとえばイーサネットの場合は、おおよそ 1500 バイト程度です。イーサネットを介して送信する場合、TCP/IP パケットのサイズはこの値が 上限になります。さらなるデータ転送が必要な場合は、オペレーティングシステム からパケットを分割して送信する必要があります。

それぞれの層にはそれぞれ設計された機能があるため、その機能を実現するための 情報をデータパケット内に保存しなければなりません。これをパケットの ヘッダと呼びます。各層には、データ自身の前に小さな データブロックの形でプロトコルヘッダが割り当てられます。イーサネット ケーブル内でやりとりされる TCP/IP データパケットの例を 図11.2「TCP/IP イーサネットパケット」(207 ページ) に示します。またチェックサムは パケットの冒頭ではなく、パケットの末尾に配置されます。これにより、ネットワークハードウェアでの処理が容易になるようにしています。

図 11.2 TCP/IP イーサネットパケット

アプリケーションがネットワーク上にデータを送信すると、物理層以外ではデータはLinuxカーネルが実装する各層に渡されます。それぞれの層はそれぞれの役割を果たす処理を行なってから次の層に渡します。最も低い層がデータを送信する最終責任を負っています。データを受信したときの処理は、上述の逆の手順で行ないます。タマネギの皮のように、届いたデータから1枚1枚プロトコルヘッダを取り除いていきます。アプリケーションに渡すデータの作成については、トランスポート層が最終責任を負います。この方法により、各層は隣接する層との間だけをやりとりすれば済むような構造になっています。またアプリケーションは、データが100メガビット毎秒のFDDIネットワークを介しているのか、それとも56キロビットのアナログモデムを使用しているのかを気にする必要はありません。さらに言えば、パケットが必要なフォーマットに変換する機能を備えているため、同じく回線の種類についても気にする必要はありません。

11.1 IP アドレスとルーティング

本章ではIPv4ネットワークについてのみ言及しています。IPv4の後継であるIPv6についての情報は、11.2項「IPv6一次世代のインターネット」(211ページ)をお読みください。

11.1.1 IP アドレス

インターネット上に存在するすべてのコンピュータには、ユニークな32ビットのアドレスが付与されています。これら32ビット(または4バイト)のアドレスは、通常は例11.1「IPアドレスの書式」(208ページ)の2行目のように記述します。

例 11.1 IP アドレスの書式

```
IP アドレス (2進数表記): 11000000 10101000 00000000 00010100  
IP アドレス (10進数表記): 192. 168. 0. 20
```

10進数表記では、それぞれ4バイトを1バイトずつ10進数で表記し、間をピリオドで区切ります。IPアドレスはホストやネットワークインターフェイスに割り当てられるもので、世界中で唯一のものでなければなりません。このルールにはいくつかの例外事項がありますが、本章では特に関係のないものなので省略します。

IPアドレスでもう1つ重要な項目として、階層構造のシステムであることが挙げられます。1990年代ではIPアドレスはクラスと呼ばれる方法で限定して分類されていました。しかしながら、このような方法は柔軟性に欠けていたため、現在は使用

されていません。現在は クラスレス ルーティング (CIDR, クラスを使用しない領域間経路制御) を使用しています。

11.1.2 ネットマスクとルーティング

ネットマスクは特定のネットワーク範囲 (サブネットワーク) を定義するために 使用されるものです。2 つのホストが同じサブネットワーク内に存在していれば、それらは直接通信を行なうことができます。異なるサブネットワーク内に存在している場合は、それぞれのホストは自分と同じサブネットワーク内にあるゲートウェイ のアドレスを知って (設定して) おく必要があります。2 つの IP アドレスから 同じサブネットワークかどうかを判断するには、単純に IP アドレスとネットマスクの「論理積」をそれぞれ計算します。結果が同じであればそれらの IP アドレスは同じサブネット内にあることになりますし、結果が異なっていれば ゲートウェイを介して通信しなければならないことを示します。

ネットマスクの動作について学ぶには、例11.2「IP アドレスとネットマスクのつながり」(209 ページ) をお読みください。ネットマスクは 32 ビットで表わされるもので、その ネットワーク内にどれだけの数の IP アドレスが属しているのかを表わしています。1 になっているビットがネットワークを表わすビットで、0 になっているビットがネットワーク内を表わすビットです。これを言い換えると、1 のビットが多ければ多いほど そのサブネットのサイズが小さくなることを示しています。ネットマスクは常に 1 のビットが連続するため、単にそのビット数を数えるだけの 方法でネットマスクを表記する場合もあります。例11.2「IP アドレスとネットマスクのつながり」(209 ページ) の 1 つめの例では 24 ビット分が 1 になっているため、192.168.0.0/24 と記述する場合もあります。

例 11.2 IP アドレスとネットマスクのつながり

```
IP アドレス   (192.168.0.20):  11000000 10101000 00000000 00010100
ネットマスク (255.255.255.0):  11111111 11111111 11111111 00000000
```

```
-----
論理積の結果:      11000000 10101000 00000000 00000000
10 進数表記:      192.      168.      0.      0
```

```
IP アドレス   (213.95.15.200): 11010101 10111111 00001111 11001000
ネットマスク (255.255.255.0):  11111111 11111111 11111111 00000000
```

```
-----
論理積の結果:      11010101 10111111 00001111 00000000
10 進数表記:      213.      95.      15.      0
```

もう 1 つの例を示します: 同じイーサネットケーブルに接続されたすべての マシンは、通常同じサブネットワーク内に属していて、直接接続することができます。サブ

ネットがスイッチやブリッジで区切られていた場合でも、これらのホストは直接アクセスすることができます。

自分のサブネットとは異なる IP アドレスに対しては、目的のネットワークに 接続可能なゲートウェイが存在する場合にのみ、通信を行なうことができます。もっともよくある例としては、外部とやりとりを行なうすべての通信を処理する 1 台のゲートウェイが設置されている例などが考えられます。もちろん、異なるサブネットに対してそれぞれ別々のゲートウェイを設定することも できます。

ゲートウェイを設定すると、すべての外部宛の IP パケットが適切なゲートウェイに送信されるようになります。このゲートウェイはパケットを受信すると、同じ方法で他のホストにパケットを転送します。これは宛先のホストに到達するか、もしくは TTL (time to live; 生存時間) が切れるまで行なわれます。

表 11.2 様々なアドレス

アドレスの種類	説明
通常のネットワークアドレス	これは 例11.2「IP アドレスとネットマスクのつながり」(209 ページ)内に示されている アドレス (とネットマスク) です。このアドレスは、他のホストで同じものを設定することはできません。
ブロードキャストアドレス	これは端的に言う と、「そのサブネット内にあるすべてのホストに アクセスする」という意味になります。このアドレスを生成するには、ネットマスクの値を 2 進数で反転し、ネットワークアドレスとの論理和を 計算してください。たとえば上記の例では 192.168.0.255 のようになります。このアドレスは特定のホストに設定す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 各ホストでの「ループバックデバイス」に割り当てられています。このアドレスを利用することで、自分自身に対する接続を行なう ことができます。IPv4 でルー

アドレスの種類	説明
	ブバックデバイスのネットワークを正確に書くと、127.0.0.0/8 のアドレスになります。IPv6 の場合には単に 1 つのアドレス (::1) となります。

IP アドレスは世界で唯一のものでなければならぬため、ランダムにアドレスを割り当てたりするようなことができません。そのため、プライベートな IP ベース ネットワークを構築する目的で、3 種類のアドレス領域が提供されています。これらのアドレスは、インターネット側から通信を行なうことができないように設定されているため、インターネット上では利用できません。これらのアドレス 範囲は RFC 1597 または 表11.3「プライベート IP アドレス領域」(211 ページ) に記されています。

表 11.3 プライベート IP アドレス領域

ネットワーク／ネットマスク	範囲
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

11.2 IPv6一次世代のインターネット

WWW (World Wide Web) の出現により、インターネットは爆発的なまでに成長し、過去 15 年間で TCP/IP の通信を行なうコンピュータが急増しました。特に CERN (<http://public.web.cern.ch>) の Tim Berners-Lee が 1990 年に WWW を発明してから、インターネットに接続するホストは数千 程度のものから 1 億程度にまで増加しました。

上述のとおり、IPv4 のアドレスは 32 ビット分しかありません。また、かなりの IP アドレスが失われています。これらの失われたアドレスは、ネットワーク の管理上の問題から、使用することができません。これは、あるネットワークで 利用可能なアドレス数が 2 のべき乗から 2 を引いた数でなければならないという 制約に基づくものです。たとえばインターネットに 128 個のホストを接続する 場合、256 個のサブネットを構築して 254 個のアドレスを確保しなければ なりません。差し引かれた 2 個

分は、ネットワークの構造そのものを管理するために必要なアドレスであるためです: これらはブロードキャストアドレス、ネットワークアドレスとそれぞれ呼ばれています。

また、現在の IPv4 プロトコルでは、DHCP や NAT (ネットワークアドレス変換) の仕組みを利用して、潜在的なアドレス不足を解決するようにしています。プライベートとパブリックという 2 種類のアドレスを組み合わせることで、これらの方法はアドレス不足の問題を和らげることができています。さらに、これらの問題は設定作業にも影響していて、設定を面倒にしているだけでなく、管理への負担を強めています。IPv4 ネットワーク内にホストを設定する場合、ホスト自身の IP アドレスとサブネットマスク、ゲートウェイアドレスと (必要であれば) ネームサーバのアドレスをそれぞれ設定しなければなりません。これらの全ての情報を知っておくか、もしくはどこから取得しておく必要があることになります。

IPv6 では、アドレスの不足や複雑な設定項目といった厄介ごとが過去のものになっています。下記の章では、IPv6 でもたらされる改善点と利点、および古いプロトコルからの移行方法についてそれぞれ述べています。

11.2.1 利点

新しいプロトコルによってもたらされる最も重要、かつ最も目に見える改善点は、そのアドレス領域の拡張にあります。IPv6 アドレスは旧来の 32 ビットから、128 ビットに拡張されました。これにより、はるかに多いアドレスを割り当てる ことができるようになっています。

IPv6 アドレスは単に前身となるプロトコルから長さが増えただけのものではありません。IPv6 では内部構造が異なり、属しているシステムとネットワークに関する情報を多く含む仕組みになっています。これらの拡張について、詳しくは 11.2.2 項「アドレスの種類と構造」(214 ページ) をお読みください。

新しいプロトコルに関する他の利点を下記に列挙します:

自動設定

IPv6 はネットワークを「プラグ & プレイ」対応にすることができます。これは新しく設定したシステムを (ローカルの) ネットワークに 接続する際、手作業での設定を行なう必要がないことを意味しています。新しいホストは近隣のルータから *neighbor discovery* (ND) と呼ばれるプロトコルを利用して得られた情報から、自分自身のアドレスを 割り出して設定します。この方法では管理者が介入することなくアドレスを 設定することができるほか、アドレスの割り当てについて中央にサーバを用意する必要もありません。IPv4 では DHCP サーバとし

て中央にサーバを 設置するか、もしくは ARP を利用して 169.254.0.0/16 の アドレス帯域を 使用する必要がありました。

ルータがスイッチに接続されている場合でも、ルータはネットワーク内の ホストに対して通信を行なうことができるよう、フラグ付きの定期通知を 行なう必要があります。詳しい情報については RFC 2462 をお読みになるか、もしくは radvd.conf(5) のマニュアルページと RFC 3315 をそれぞれお読みください。

可動性

IPv6 では、同時に複数のアドレスを 1 つのネットワークインターフェイスに 設定することができます。これにより、携帯電話会社が提供する国際ローミング サービスに比べ、複数のネットワークへの接続が簡単になります: たとえばお使いの携帯電話を海外に持って行くと、電話機側がそれを自動で 判断して海外の サービスに接続し、どこでも同じ番号を利用することができる ようになるほか、電話機側から発信を行なっても自宅と同じ番号で発信できるようになります。

機密通信

IPv4 ではネットワークセキュリティが追加機能として提供されていました。IPv6 では IPsec を中枢機能のうちの 1 つに位置づけていて、インターネット 上の第三者から盗み聞きされないよう、機密のチャンネルを設定して通信を 行なうことができます。

後方互換性

現実的には、インターネット全体の IPv4 から IPv6 への移行は不可能です。そのため、インターネット上で両方のプロトコルが共存するだけでなく、特定のシステム上でも共存させなければなりません。これは互換アドレス (IPv4 アドレスから IPv6 アドレスへの変換) の形で提供されているほか、複数のトンネル機能で実現されています。詳しくは 11.2.3 項「IPv4 と IPv6 の共存」(219 ページ) をお読みください。また、システムは *デュアルスタック IP* 技術を利用して、両方のプロトコルに同時対応しています。そのため、システム内では完全に区切られた 2 つのネットワークスタックが存在していて、両プロトコルバージョンの衝突は起こらないようになっています。

マルチキャストを利用したカスタムなサービス

IPv4 では SMB などのサービスで、ローカルネットワーク内の全ホストに 一斉通知するためにブロードキャストを利用しています。IPv6 では、グループに属しているホストに対して通知を行なう *マルチキャスト* を利用し、より洗練されたホスト/サーバ間の通知機能を実現しています (ブロードキャスト の場合は全てのホスト宛に通知を 行ないますし、ユニキャスト の場合は個別に通知を 行ないます)。それぞれのホストはアプリケーションごとのグループの形で 管理されます。事前に定義されているグループとして、全てのネームサーバ (全ネーム

サーバのマルチキャストグループ) や 全てのルータ (全ルータのマルチキャストグループ) などがあります。

11.2.2 アドレスの種類と構造

上述のとおり、現在の IP プロトコルには 2 つの重要な要素が欠けています: 1 つは IP アドレスの枯渇への対応、もう 1 つはネットワークの設定やルーティング テーブル (経路制御表) の複雑化と負担の増大です。IPv6 では前者の問題に対して、アドレス領域を 128 ビットに拡大することで対応しています。後者の問題に対しては、マルチホーミング (1 台の機器に対して複数のアドレスを割り当て、複数のネットワークへのアクセスを提供する技術) など、ネットワークアドレスの割り当てを上手に行なって、階層的なアドレス構造を構築することで対応しています。

IPv6 を取り扱う場合は、3 種類のアドレス種類があることを知っておく必要があります:

ユニキャスト

この種類のアドレスは、1 つのネットワークインターフェイスに対して割り当てられるものです。このようなアドレスを持ったパケットは、単一の宛先に対して配信されます。そのため、ユニキャストはローカルネットワーク やインターネットでのホスト間通信に利用します。

マルチキャスト

この種類のアドレスは、複数のネットワークインターフェイスに対して割り当てられるものです。このようなアドレスを持ったパケットは、グループに属する複数の宛先に配信されます。マルチキャストアドレスは主に管理されたネットワーク環境で利用され、特定のネットワークサービスからホストのグループに対して通信を行なう場合に利用します。

エニーキャスト

この種類のアドレスは、複数のネットワークインターフェイスに対して割り当てられるものです。このようなアドレスを持ったパケットは、ルーティング (経路制御) プロトコルの方針に従って、送信元から最も近いグループのメンバーに対して配信されます。エニーキャストのアドレスは特定のネットワーク領域で利用されるもので、あるサービスを提供するサーバを見つけやすくするために用いられるものです。同じ種類のサーバは、全て同じアドレスを設定します。あるホストからサービスを要求すると、ルーティングプロトコルの判断で最も近い場所に存在するサーバがパケットを受信し、サービスを提供する仕組みです。サーバが何らかの理由でサービスを提供できない場合は、プロトコル側で自動的に次の候補を選択していきます。

IPv6 アドレスは 4 桁の項目 8 つから構成されています。それぞれの項目は 16 ビットで、16 進数による表記を行ないます。また、各項目はコロン (:) で区切ります。それぞれの項目内が 0 から始まる 桁であった場合にはその 0 を省略しますが、途中や最後が 0 であった場合には 省略は行ないません。また、0 が連続する場合はダブルコロン (::) で省略を行ないます。ただし、ダブルコロンはアドレスごとに 1 回までしか 使用できません。具体的な短縮表記方法を 例11.3「IPv6 アドレスの例」(215 ページ) に示します。これらはいずれも同じアドレスを指す表記です。

例 11.3 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 アドレスの各部分には機能が割り当てられています。最初の数バイトは プレフィクスとアドレス種類を規定しています。それに続くネットワーク アドレスの中間部分は、アドレスのネットワーク部分を表わします (使用されていない場合もあります)。最後にアドレスのホスト部分がつながる形になっています。IPv6 では、ネットマスクをアドレスの後にスラッシュ (/) を入れて記述します。このネットマスクはプレフィクスの長さで指定します。たとえば 例11.4「プレフィクス長を指定する IPv6 アドレス」(215 ページ) のアドレスでは、64 ビット分がネットワークを表わす部分で、残りの 64 ビットがホストを表わす 部分であることを示しています。言い換えれば、64 は ネットマスクが左から 64 ビット分だけ 1 で埋められた値であることを 示しています。ここから IPv4 のように IP アドレスとネットマスクから計算 された値で論理積を計算すれば、同じサブネット上にあるものかどうかを判別 できることになります。

例 11.4 プレフィクス長を指定する IPv6 アドレス

```
fe80::10:1000:1a4/64
```

IPv6 では、事前に規定されたプレフィクスが存在しています。これらのうちの いくつかを 表11.4「様々な IPv6 プレフィクス」(215 ページ) に示します。

表 11.4 様々な IPv6 プレフィクス

プレフィクス (16 進)	定義
00	IPv4 アドレスと IPv4 over IPv6 で使用する互換アドレスです。これらのアドレスは IPv4 との互換性を維持するために使用され、IPv6 パケットを IPv4 パケットに変換することのできるルータで 使用されます。なお、

プレフィクス (16 進)	定義
	ループバックデバイス用などの特殊なアドレス についても、このプレフィクス内に存在します。
1 桁目が 2 または 3 で始まるもの	グローバルなユニキャストアドレスの集まりです。IPv4 の場合と同様に、特定のサブネットワークの一部としてインターフェイスに割り当てます。現時点では下記のアドレス領域が存在しています: 2001::/16 (商用品質のアドレス領域) と 2002::/16 (6to4 用の アドレス領域)
fe80::/10	リンクローカルのアドレスです。このプレフィクスを持つアドレスは経路 制御されるべきものではないため、同じサブネット内でのみ通信可能です。
fec0::/10	サイトローカルのアドレスです。経路制御を行なってもかまいませんが、属する団体内でのみ行なわれるべきものです。実際には 10. x. x. x のように、プライベートネットワークアドレスの IPv6 版として使用することができます。
ff	マルチキャストアドレスです。

また、ユニキャストのアドレスは 3 つの要素から構成されています:

公衆部

最初の要素 (上述でのプレフィクス) は、公衆インターネットを介して パケットの経路制御を行なうための部分です。企業や団体がインターネット 接続を行なう際の情報として使用します。

サイト部

2 番目の部分には、パケットを配信するために必要なサブネットの経路情報が含まれています。

インターフェイス ID

3 番目の部分では、パケットを配信する先のインターフェイス識別子が含まれています。この部分には MAC アドレスを設定することもできます。MAC アドレスは世界で唯一のアドレスで、ハードウェアの製造元が割り当てた 固定長の識別コードをデバイスに設定しています。実際には設定作業が単純化されていて、アドレスの最初の 64 ビットが EUI-64 トークンと呼ばれています。その 64 ビットのうち最後の 48 ビットが MAC アドレスを、残りの 24 ビットがトークンの種類に関する特殊な情報を含むものになっています。これにより、EUI-64 トークンを MAC アドレスを持たないデバイス、たとえば PPP や ISDNなどをベースにした デバイスに設定することができるようになっています。

上記の基本構造のほか、IPv6 では下記の 5 種類のようなユニキャストアドレスが存在します:

:: (未設定のアドレス)

このアドレスは、起動した直後にインターフェイスを設定する際に利用するもので、発信元のアドレスとして使用します。インターフェイスを設定する段階ではアドレスを決めることができないため、このような形態をとっています。

:::1 (loopback)

これはループバックデバイスを表わします。

IPv4 互換アドレス

この IPv6 アドレスは IPv4 アドレスから生成されるもので、96 個のゼロビットから始まるアドレスになっています。この互換アドレスはトンネリング (11.2.3 項「IPv4 と IPv6 の共存」(219 ページ) をお読みください) で使用するもので、IPv4 と IPv6 のホストが純粋な IPv4 環境で通信できるようにするためのものです。

IPv6 にマッピングされた IPv4 アドレス

この種類のアドレスは、IPv6 のアドレス表記で IPv4 アドレスを表わすために使用します。

ローカルアドレス

この種類のアドレスには、2 種類の使用方法があります:

リンクローカル

この種類のアドレスは、内部のサブネットワーク内でのみ使用することができます。この種類のアドレスを宛先や発信元に持つパケットは、インターネットやその他のサブネットワークに転送されるべきではありません。このようなリンクローカルアドレスには特殊なプレフィクス (fe80::/10) が設定されていて、ネットワークカードのインターフェイス ID との間はゼロバイトで埋め

られた形になっています。また、この種類の アドレスは自動設定の過程で
利用し、同じサブネットワークに属する ホストと通信する際に利用します。

サイトローカル

この種類のアドレスはサブネットワーク内でやりとりをすることが できます
が、インターネットの世界では利用できないものです。つまり、企業や団体
などの内部ネットワークでのみ使用しなければなりません。このようなアド
レスはイントラネットなどで使用されるもので、IPv4 で言うところのプライ
ベートアドレスと等価なアドレスです。このようなサイトローカルアドレスに
は特殊なプレフィクス (fec0::/10) が設定されていて、ネットワークカードの
インターフェイス ID との 間は 16 ビットのサブネットワーク ID を指定しま
す。残りの部分はゼロバイトで埋めます。

また、IPv6 で全く新しく作成された機能として、各ネットワークインターフェイス に
対して複数の IP アドレスを設定できる、という機能があります。これにより、同じ イン
ターフェイスから同時に複数のネットワークへアクセスできるよう になっています。同
時にアクセスするネットワークのうち、一方は IPv6 が有効化 されるとすぐに利用で
きるリンクローカルアドレスを利用して、ローカル ネットワーク内にある全ホストと通
信のできる状態にし、さらに MAC アドレスと 既知のプレフィクスを組み合わせで完
全自動設定を行ないます。MAC アドレスが アドレスの一部に組み入れられている
ため、世界中でユニークな IP アドレスを 構築することができるという仕組みになっ
ています。アドレス内で変更可能な 部分はそれぞれ *サイト部* と *公衆部* を指定す
る部分で、これらはホストが現在接続しているネットワークに依存して 決まるもので
す。

複数のネットワークの間を行き来するホストの場合は、少なくとも 2 つのアドレス を
必要とします。それらのうちの一方は *ホームアドレス* と呼ばれ、インターフェイス ID
を含むだけでなく、通常所属するそのネットワーク 自身の識別子 (およびそれに結
びつくプレフィクス) が含まれています。ホームアドレスはアドレス設定を固定して使
用するもので、通常の運用では変更を 行なわないものとします。そのような環境で
も、ホームネットワーク内かどうかに関わらず、移動端末のような接続で全てのパ
ケットを配信することができます。これは IPv6 で新たに提供されるようになった機
能で実現されているもので、それぞれ *stateless autoconfiguration* (*状態管理の
ない自動設定*) や *neighbor discovery* (*近隣検出*) と呼ばれています。ホームアド
レスに加え、移動端末ではローミング先の環境に合わせて 1 つまたはそれ以上の
追加アドレスを取得します。これらは *care-of* (気付) アドレスと呼びます。ホームネッ
トワークでは、その移動端末が外部で ローミングしている間に、その端末に対してパ
ケットを転送する機能を備えています。IPv6 環境では、この作業は *ホームエージェ
ント* が行なう もので、そのホームアドレス宛に届いたパケットをトンネル経由で中継
します。他方ではこのような *care-of* アドレスに届いたパケットについては、そのまま
何の加工もせずに届けることができますようになっています。

11.2.3 IPv4 と IPv6 の共存

インターネットに接続された全てのホストに対する IPv4 から IPv6 への移行作業は、ゆるやかに行なわれています。ホストによっては両方のプロトコルを共存させている 場合もあります。単一のシステムにおけるプロトコルの共存は、両方のプロトコルに 存在する デュアルスタック の実装によって作られています。ここで疑問点として残るのが、どのようにして IPv6 の利用できるホストから IPv4 のホストに通信を行なうのか、および IPv6 パケットが現在のネットワーク、特に IPv4 ベースのネットワークに対してどのような変換を行なうのかという点です。これらの問題を解決するのが、トンネリングと互換アドレスという仕組みです (詳しくは 11.2.2 項「アドレスの種類と構造」(214 ページ) をお読みください)。

(世界中に広がった) IPv4 のネットワークでは、IPv6 のホストはトンネルを介して通信を行なうことができます: IPv6 パケットは IPv4 パケットの中にカプセル化 されて IPv4 のネットワーク内を移動します。このような 2 つの IPv4 ホスト間の接続を、トンネル と呼びます。これを実現するには、パケットには IPv6 の宛先アドレスだけでなく、トンネルの反対側で受信処理を行なう IPv4 のアドレスを設定しなければなりません。基本的なトンネルであれば、それは両方のホストの管理者が合意するだけで手動設定を行なうことができます。これを *静的トンネル* と呼びます。

しかしながら、静的なトンネルを設定したり管理したりすることは、日々の通信 要件をまかなっていくには面倒な作業になってしまいます。そのため、IPv6 では 3 種類の異なる方法で *動的トンネル* を設定する機能を提供しています:

6over4

IPv6 パケットを自動で IPv4 パケットにカプセル化し、マルチキャスト対応 の IPv4 ネットワークを介して転送する方法です。IPv6 側から見ると、ネットワーク全体 (インターネット) が巨大なローカルエリアネットワーク (LAN) のように見えます。これにより、IPv4 トンネルの反対側で自動的に パケットを受信できるようになるという仕組みです。しかしながら、この 方法は規模が拡大する場合には向いておらず、IP マルチキャストが インターネット上でほとんど利用されていないことも、普及の妨げになっています。そのため、この方法は小規模の企業や学術的なネットワークなど、マルチキャストの利用できる環境に向いています。この方法の詳しい仕様は RFC 2529 で記載されています。

6to4

この方法では IPv4 アドレスを IPv6 のアドレスから自動生成し、IPv6 のホストからは IPv4 のネットワーク上で通信を行ないます。しかしながら、このような IPv6 ホストとインターネット間の通信にはいくつかの問題点が報告されています。この方法は RFC 3056 に記載されています。

IPv6 トンネルブローカー

この方法では、IPv6 ホスト向けのトンネル専用サーバを利用して通信を行います。詳しくは RFC 3053 をお読みください。

11.2.4 IPv6 の設定

IPv6 を設定する場合は、通常的环境であれば個別の端末に対して設定を行なう必要はありません。IPv6 は規定で有効化されています。インストール中であれば、1.14.2.2項「ネットワーク設定」(33 ページ)にあるネットワーク設定の手順で無効化することができます。インストール済みのシステムで IPv6 を有効または無効に設定したい場合は、YaST から *ネットワークの設定* を選択します。*グローバルオプション* のタブから、必要に応じて *IPv6 を有効にする* のチェックを入れるか外すかして設定してください。設定ファイルから IPv6 を設定する場合は、`/etc/modprobe.d/50-ipv6.conf` を編集してシステムを再起動してください。無効化している状態から、次の再起動までの間だけ一時的に有効化したい場合は、`root` から `modprobe -i ipv6` を実行してください。なお、IPv6 モジュールを読み込んでしまうと、基本的に読み込みを外すことはできません。

IPv6 は自動設定を基本とした仕組みであるため、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。通常はワークステーション側で経路表 (ルーティングテーブル) の管理は行ないません。ワークステーションからネットワークルータに対して *ルータ広告プロトコル* を利用して問い合わせを行ない、設定すべきプレフィクスとゲートウェイを知る仕組みになっています。IPv6 ルータとして動作するには、このプロトコルに対応した `radvd` プログラムを利用します。このプログラムはワークステーションに対して、IPv6 アドレスのプレフィクスとルータのアドレスを通知します。また、両方の自動設定や経路制御を行なう目的で、`zebra/quagga` を使用することもできます。

また、`/etc/sysconfig/network` ファイルを利用して 様々な種類のトンネルを構築したい場合は、`ifcfg-tunnel (5)` のマニュアル ページをお読みください。

11.2.5 さらなる情報

ここまでの概要説明では不足している点が数多くあり、広範囲にわたる説明はできていません。新しいプロトコルに対するより深い説明については、下記のオンライン文書や書籍をお読みください:

<http://www.ipv6.org/> (英語)

IPv6 に関しては、ここからお読みになることをお勧めします。

<http://www.ipv6day.org> (英語)

独自の IPv6 ネットワークを構築するための全情報が提供されています。

<http://www.ipv6-to-standard.org/>

The list of IPv6-enabled products.

<http://www.bieringer.de/linux/IPv6/> (英語)

ここには Linux における IPv6 の HOWTO のほか、各トピックに関連した 多数のリンクが掲載されています。

RFC 2640

IPv6 に関する基礎を説明する RFC です。

IPv6 Essentials

Silvia Hagen (ISBN 0-596-00125-8) 氏の著作で、IPv6 に関する 重要な要素について、全ての説明が記されています。

11.3 名前解決

DNS は IP アドレスから 1 つまたは複数の名前に、および名前から IP アドレスにそれぞれ変換する機能を提供します。Linux からは、このような変換は専用のソフトウェア bind を利用してサービスを提供します。この変換を行なうマシンのことを、ネームサーバと呼びます。DNS における 名前は、各要素をピリオドで区切った階層構造になっています。この名前の階層 構造は、上述した IP アドレスの階層構造とは独立したものになっています。

jupiter.example.com のような完全な 名前は、ホスト名、ドメイン のような書式で記述します。完全な名前は **完全修飾ドメイン名** と呼び、ホスト名とドメイン (example.com) から構成されます。また、ドメイン名には **トップレベルドメイン** (TLD) (com) が含まれます。

TLD の割り当ては歴史的な理由により、かなり複雑な仕組みになっています。古くはアメリカで 3 文字のドメイン名が使用されていて、残りの国については 2 文字の ISO 国コードが標準として提供されていました。それに加えて、2000 年からは長い TLD も提供されるようになりました。これらはドメイン名の 役割を示しているものです (たとえば .info, .name, .museum など)。

インターネットの黎明期 (1990 年以前) では、/etc/hosts ファイルを利用してインターネット上の全ホストの情報を保存していました。これはインターネットに接続するコンピュータの数が急増していくことで、現実的な解法ではなくなってしまいました。この理由により、世界中に分散させる 方法で分散型データベースを構築し、ホ

スト名を保存する仕組みが開発されました。このデータベースはネームサーバに似た仕組みで、インターネット上の全ての ホストに関するデータを持つことはなく、その代わりに他のネームサーバに対して リクエストを投げることができる仕組みを備えていました。

階層構造の最上位は ルートネームサーバ によって占有 されています。これらの ルートネームサーバはトップレベルドメインを管理 するもので、ネットワークインフォメーションセンター (NIC) が稼働させている サービスです。各ルートネームサーバは、それぞれのトップレベルドメインに対する ネームサーバ情報を知っていて、それらの情報を提供する役割を持っています。トップレベルドメインの NIC について、詳しくは <http://www.internic.net> (英語) をお読みください。

DNS はホスト名を解決するだけのものではありません。ネームサーバは、特定のドメインに対して電子メールを受信するホストが何であるのかを 知っている存在でもあります。このような情報を、メールエクスチェンジャ (MX) と呼びます。

お使いのマシンから IP アドレスの解決を行なうためには、少なくとも 1 台の ネームサーバとその IP アドレスを知っておかなければなりません。YaST からはネームサーバを簡単に設定することができます。ダイヤルアップ接続の 場合は、ネームサーバの設定は手作業で行なう必要は全くありません。これは、ダイヤルアッププロトコル上で、接続が完了したときに自動でネームサーバの アドレスを取得するためです。openSUSE® でのネームサーバの設定については、11.4.1.4項「ホスト名と DNS の設定」(232 ページ) をお読みください。ご自身で ネームサーバを立ち上げる場合は、第13章 ドメインネームシステム (271 ページ) をお読みください。

whois プロトコルは DNS との関連性が高いプロトコルです。このプログラムを利用すると、指定したドメインの担当者の情報などを 素早く得ることができます。

注記: MDNS と .local のドメイン名

.local トップレベルドメインは、DNS 解決器側でリンク ローカルのドメインとして取り扱われます。DNS のリクエストは通常の DNS リクエストではなく、マルチキャスト DNS として送信されます。すでにお使いの ネームサーバ設定で .local ドメインをお使いの場合は、/etc/host.conf ファイルでこのオプションを無効に設定しなければなりません。詳しい情報は host.conf のマニュアルページをお読みください。

また、インストール時に MDNS を使用しないように設定するには、起動パラメータに nomdns=1 を指定してください。

マルチキャスト DNS について、詳しくは <http://www.multicastdns.org> (英語) をお読みください。

11.4 YaST を利用したネットワーク接続の設定

Linux では、多種のネットワークに対応しています。これらのうちの多くはそれぞれ異なるデバイス名を使用し、設定ファイルもファイルシステム内で 様々な箇所に存在しています。手作業によるネットワーク設定については、11.6項「手動でのネットワーク設定方法」(247 ページ) をお読みください。

ラップトップコンピュータ上にインストールを行なっている 場合 (既定で NetworkManager が有効になっているはずです) は、YaST が検出された 全てのデバイスに対して設定を行ないます。NetworkManager が有効になっていない 場合は、リンクの確立している (ネットワークケーブルが接続されている) 最初の デバイスだけを自動で設定します。その他のハードウェアについては、インストール 済みのシステムから必要なときに設定を行なうことができます。下記の章では、openSUSE で対応している全てのネットワーク接続について、説明を行なっています。

11.4.1 YaST を利用したネットワークカードの設定

有線または無線ネットワークカードを YaST から設定するには、ネットワークデバイス > ネットワークの設定 を選択してください。モジュールが起動すると、YaST は下記の 4 つのタブを含む ネットワーク設定 ダイアログを表示します: グローバルオプション, 概要, ホスト名/DNS, ルーティング

グローバルオプション タブでは、NetworkManager を使用するかどうかや IPv6 を使用するかどうか、および DHCP オプション設定などの 一般的なネットワーク設定を行ないます。詳しくは 11.4.1.1項「グローバルネットワーク設定」(224 ページ) をお読みください。

概要 タブでは、インストール済みのネットワーク インターフェイスとその設定が表示されています。正しく検出された全ての ネットワークカードを、その名前と共に表示しています。このダイアログから 新しいネットワークカードを手動設定することもできますし、削除や変更など を行なうこともできます。自動では検出されていないネットワークカードを 設定したい場合は、11.4.1.3項「未検出のネットワークカードの設定」(231 ページ) を お読みください。また、既に設定済みのネットワークカー

ドについて、設定を 変更したい場合は、11.4.1.2項「ネットワークカードの設定変更」(225 ページ) をお読みください。

ホスト名／DNS タブでは、お使いのマシンのホスト名と 使用するネームサーバをそれぞれ設定します。詳しくは 11.4.1.4項「ホスト名と DNS の設定」(232 ページ) をお読みください。

ルーティング タブでは、経路制御 (ルーティング) に 関わる設定を行ないます。詳しくは 11.4.1.5項「ルーティング (経路制御) の設定」(234 ページ) をお読みください。

図 11.3 ネットワークの設定

ネットワーク設定

グローバルオプション | 概要 | ホスト名／DNS | ルーティング

ネットワークの設定方法

☐ NetworkManager を使ってユーザが制御 (U)

☒ ifup を使用した従来の方法 (I)

IP プロトコル設定

☒ IPv6 を有効にする

DHCP クライアントオプション

DHCP クライアント識別子 (I)

送信するホスト名 (H)

AUTO

☒ DHCP で既定のルートを変更する

ヘルプ (H) | キャンセル (C) | OK (O)

11.4.1.1 グローバルネットワーク設定

YaST ネットワーク設定 モジュール内の グローバルオプション タブでは、NetworkManager を使用するかどうかや IPv6 を使用するかどうか、および DHCP オプション設定などの 重要なグローバルネットワーク設定を行ないます。これらの設定は、全ての ネットワークインターフェイスに対して適用されます。

ネットワークの設定方法 では、ネットワークの接続を 管理するための方法を選択します。NetworkManager のデスクトップアプレットを利用して 全てのインターフェイスの接続管理を行ないたい場合は、*NetworkManager を使ってユーザが制御* を選択してください。このオプションは複数の有線／無線ネットワークを切り替える

場合に便利な選択です。デスクトップ環境 (GNOME や KDE) を使用しない環境であったり、お使いのコンピュータが Xen サーバの仮想システムであったりした場合、もしくはお使いのネットワークに対して DHCP や DNS などのネットワーク サービスを提供する環境の場合は、*ifup* を使用した従来の方法を選択してください。NetworkManager を使用するよう選択すると、nm-applet を利用してネットワーク オプションを設定するようになりますので、ネットワーク設定 内の 概要, ホスト名 / DNS, ルーティング の各タブは利用できなくなります。NetworkManager についての詳しい情報は、第23章 *NetworkManager* の使用 (435 ページ) をお読みください。

IPv6 プロトコル設定 では、IPv6 プロトコルを使用するか どうかを設定します。IPv4 と IPv6 を同時に使用することもできます。既定では IPv6 が有効に設定されていますが、IPv6 を使用しないネットワーク 環境では、IPv6 プロトコルを無効化したほうが処理を高速に行なうことができます。IPv6 を無効化するには、*IPv6 を有効にする* オプションの チェックを外してください。これにより、IPv6 のカーネルモジュールを自動では 読み込まないようになります。設定はシステムの再起動後に反映されます。

DHCP クライアントオプション では、DHCP クライアントの オプション設定を行ないます。*DHCP クライアント識別子* には、ネットワーク内の DHCP クライアントを唯一に識別する識別子を入力します。何も入力しなければ、既定でネットワークインターフェイスのハードウェアアドレス を利用します。ただし、お使いのマシンで同じネットワークインターフェイス を使用する複数の仮想マシンを利用する場合は、ハードウェアアドレスが全て同じものになってしまうため、ここにそれぞれを識別するための情報を入力してください。

送信するホスト名 では、dhcpcd が DHCP サーバに送信する ホスト名のオプションフィールドを指定します。DHCP サーバによっては、この ホスト名情報を元にしてゾーン情報 (正引きと逆引き) を更新したりすることがある (動的 DNS) ためのものです。また DHCP サーバによっては、*送信するホスト名* のオプションフィールドに対して、何らかの 文字列を設定する必要がある場合もあります。なお、この項目に AUTO を指定すると、現在のホスト名 (/etc/HOSTNAME に設定 したもの) を送信します。何も指定しない場合はホスト名を送信しないようになります。また、DHCP サーバから提供されたデフォルトゲートウェイ情報 を 利用しないようにするには、*DHCP で既定のルートを変更する* のチェックを外してください。

11.4.1.2 ネットワークカードの設定変更

ネットワークカードの設定を変更するには、YaST 内の ネットワーク設定 > 概要 から設定したいネットワークカードを選択し、編集 を押します。ネットワークカードの設

定 ダイアログが表示されたら、それぞれ *一般*, *アドレス*, *ハードウェア* タブから設定を行ないます。無線 LAN カードの場合について、詳しくは 22.5 項「YaST を利用した設定」(422 ページ)をお読みください。

IP アドレスの設定

ネットワークカードの設定 ダイアログ内の *アドレス* タブを利用すると、ネットワークカードの IP アドレスを設定することができるほか、IP アドレスの決定方法を選択することもできます。また、このタブは IPv4 と IPv6 の両方のアドレスに対応しています。アドレスの設定方法は *アドレスを設定しない* (ボンド機能で使います), *固定 IP アドレス* (IPv4 と IPv6) を選択することができるほか、*可変 IP アドレス* を選択した場合は、さらにアドレスの設定方法を *DHCP*, *Zeroconf* のいずれか、もしくはその両方を選択することができます。

なお、*可変 IP アドレス* を選択した場合は、さらに *バージョン 4 のみでの DHCP* (IPv4), *バージョン 6 のみでの DHCP* (IPv6), *バージョン 4 と 6 の両方での DHCP* (IPv4, IPv6 の両方) を選択することができます。

また、インストール時にリンクの確立したネットワークカードが存在した場合、1 枚目のネットワークカードについては、DHCP を利用した自動アドレス取得が設定されます。ラップトップコンピュータの場合は NetworkManager が自動的に有効化され、全てのネットワークカードが設定されます。

DHCP の設定は、お使いのインターネット接続が DSL による接続契約になっている、ISP (インターネットサービスプロバイダ) から固定の IP アドレスを割り当てられていない場合にも、使用場合があります。DHCP を使用する場合は、YaST のネットワーク設定モジュールから、*ネットワーク設定* ダイアログの *グローバルオプション* 内、*DHCP クライアントオプション* で詳細を設定してください。同じインターフェイスを使用して、他のホストとも通信を行なう仮想ホスト設定を利用する場合は、*DHCP クライアント識別子* の欄に適切な値を入力し、これらを区別する必要があります。

DHCP はクライアントの設定には便利なオプションですが、サーバで使用する場合には適切ではありません。固定の IP アドレスを設定するには、下記のようにして行ないます:

- 1 YaST ネットワーク設定モジュールを起動し、表示されたダイアログ内で *概要* タブを選択します。すると検出されたカードの一覧が表示されますので、設定したいネットワークカードを選択して、*編集* を押します。
- 2 *アドレス* タブでは、*固定 IP アドレス* を選択します。

- 3 *IP アドレス* に設定したい IP アドレスを入力します。IPv4 と IPv6 の両方のアドレスを設定することができます。さらに *サブネットマスク* にも値を入力します。IPv6 アドレスを使用している場合は、/64 のような形でプレフィクス長を入力してください。

またオプションで、このアドレスに対する完全修飾ホスト名を *ホスト名* に入力することができます。ここに設定を行なうと、`/etc/hosts` 設定ファイルに書き込みが行なわれます。

- 4 *次へ* を押します。
- 5 設定を有効にするには、さらに *OK* を押します。

固定アドレスを使用する場合は、ネームサーバとデフォルトゲートウェイの設定は自動では行なわれません。ネームサーバを設定するには 11.4.1.4 項「*ホスト名と DNS の設定*」(232 ページ) の手順を、ゲートウェイの設定を行なうには 11.4.1.5 項「*ルーティング (経路制御) の設定*」(234 ページ) の手順をそれぞれお読みください。

別名の設定

1 つのネットワークデバイスに対して複数のアドレスを割り当てることができます。これを別名と呼びます。

注記: 互換機能としての別名設定

別名と呼ばれる機能は IPv4 でのみ利用されるものです。IPv6 の場合はこれらの設定は無視されます。iproute2 を利用し、ネットワークインターフェイスに対して複数のアドレスを設定してください。

YaST を利用してネットワークカードに別名を設定するには、下記のようにして行ないます:

- 1 YaST ネットワーク設定モジュールを起動し、表示されたダイアログ内で *概要* タブを選択します。すると検出されたカードの一覧が表示されますので、設定したいネットワークカードを選択して、*編集* を押します。
- 2 *アドレス > 追加アドレス* タブ内で、*追加* を押します。
- 3 それぞれ *別名*, *IP アドレス*, *ネットマスク* を入力します。別名にはインターフェイスそのものの名前は入力しないでください。

- 4 *OK* を押します。
- 5 続けて *次へ* を押します。
- 6 設定を有効にするには、さらに *OK* を押します。

デバイス名と udev ルールの変更

ネットワークカードのデバイス名は、使用の際に名前を変更することができます。udev でネットワークカードを認識する際に、ハードウェア (MAC) アドレスか、もしくはバス ID で識別を行ないます。大規模なサーバで使用する際には、カードの活線挿抜が簡単にできるようになりますので、後者のバス ID による識別をお勧めします。これらのオプションを YaST から設定するには、下記のようにして行ないます:

- 1 YaST ネットワーク設定モジュールを起動し、表示されたダイアログ内で *概要* タブを選択します。すると検出されたカードの 一覧が表示されますので、設定したいネットワークカードを選択して、*編集* を押します。
- 2 *ハードウェア* タブを選択します。現在のデバイス名が *udev ルール* 内に表示されます。ここから *変更* を押します。
- 3 udev のカード識別方法を、*MAC Address* (MAC アドレス) または *Bus ID* (バス ID) から選択します。それぞれ現在選択中のカードに対する MAC アドレスとバス ID が表示されています。
- 4 デバイス名を変更する場合は、*デバイス名の変更* を選択し、名前を編集してください。
- 5 *OK* を押してから、*次へ* を押します。
- 6 設定を有効にするには、さらに *OK* を押します。

ネットワークカードのカーネルドライバの変更

ネットワークカードによっては、複数のカーネルドライバの中から選択を行なうことができます。カードが既に設定済みの場合は、YaST を利用して 利用可能なカーネルドライバ内から選択することができます。また、カーネルドライバ に対するオプションを設定することもできます。YaST を利用してこれらの オプションを設定するには、下記のようにして行ないます:

- 1 YaST ネットワーク設定モジュールを起動し、表示されたダイアログ内で **概要** タブを選択します。すると検出されたカードの 一覧が表示されますので、設定したいネットワークカードを選択して、**編集** を押します。
- 2 **ハードウェア** タブに移動します。
- 3 まずは **モジュール名** 内で、使用するカーネルドライバを 選択します。また、**オプション** の欄には必要なオプションを 入力します。オプションは **オプション=値** の形式で入力してください。複数のオプションはスペースで区切ります。
- 4 **OK** を押してから、**次へ** を押します。
- 5 設定を有効にするには、さらに **OK** を押します。

ネットワークデバイスの有効化

ifup を利用した従来の方法を利用する場合には、お使いのデバイスを起動時に 有効にすることもできますし、ケーブル接続時やカードの検出時に有効にしたり、手動による有効化を行なったり、さらには全く有効にしないこともできます。デバイスの起動方法を変更するには、下記のようにして行ないます:

- 1 YaST ネットワーク設定モジュールを起動し、表示されたダイアログ内で **概要** タブを選択します。すると検出されたカードの 一覧が表示されますので、設定したいネットワークカードを選択して、**編集** を押します。
- 2 **一般** タブを選択し、**デバイスの有効化** 内から起動方法を選択します。

起動時 を選択すると、システム起動時に該当デバイスを 有効化します。ケーブル接続時 を選択すると、インターフェイスに対して物理的な接続が行なわれているかどうかを監視する ようになります。ホットプラグ を選択すると、利用可能な 状態になるとすぐに該当デバイスを有効化します。これは **起動時** に似た設定ですが、システム起動時にインターフェイスが存在していなくても エラーにならない、という点で異なります。**手動** の場合は、ifup コマンドを利用して手動でインターフェイスを 有効化する意味になります。また、**開始しない** を選択すると、デバイスを全く有効化しなくなります。最後にある **NFSroot** は **起動時** に似たオプションですが、rcnetwork stop コマンドを入力しても、インターフェイスが停止されないようになります。この設定は、ルートファイルシステムに NFS や iSCSI をお使いの場合にご利用ください。

- 3 **次へ** を押します。

- 4 設定を有効にするには、さらに *OK* を押します。

通常はシステム管理者のみが、ネットワークインターフェイスを有効にしたり 無効にしたりすることができます。KInternet を利用して、一般のユーザから でもインターフェイスを操作できるようにしたい場合は、*Kinternet* を利用して *root* 以外のユーザにもデバイス操作を許す を選択してください。

最大転送単位 (MTU) の設定

インターフェイスに対して、最大転送単位 (MTU) を設定することができます。MTU はパケットの最大サイズをバイト単位で設定するもので、大きく設定すれば するほど高速な通信回線での効率を上げることができます。しかしながら、大きすぎる MTU を設定すると、次のパケットを送信するまでに時間がかかってしまい、かえって速度が遅くなってしまう場合もあります。

- 1 YaST ネットワーク設定モジュールを起動し、表示されたダイアログ内で *概要* タブを選択します。すると検出されたカードの 一覧が表示されますので、設定したいネットワークカードを選択して、*編集* を押します。
- 2 *一般* タブを選択し、*MTU を設定* の一覧から、適切な値を選択します。
- 3 *次へ* を押します。
- 4 設定を有効にするには、さらに *OK* を押します。

ファイアウォールの設定

項「YaST を利用したファイアウォールの設定」(第13章 マスカレードとファイアウォール, ↑セキュリティガイド) で示されているような 詳細なファイアウォール設定を行なわなくても、デバイス設定の一部として 基本的なファイアウォール設定を行なうことができます。具体的には 下記のようにして行ないます:

- 1 YaST を開いて *ネットワークデバイス > ネットワーク設定* モジュールを起動します。 *概要* タブを選択し、検出されたカードの中から設定したい カードを選択して、*編集* を押します。
- 2 *ネットワークカードの設定* ダイアログから、*一般* タブを選択します。
- 3 インターフェイスに設定したいファイアウォールゾーンを選択します。下記のオプションを選択することができます:

ファイアウォールを無効にする

このオプションは、ファイアウォールが無効化されている場合にのみ表示される項目で、ファイアウォールを全く起動しない場合に選択します。このオプションは、別途に存在するファイアウォールによってネットワーク全体が保護されている場合にのみ、選択してください。

内部ゾーン (保護しない)

ファイアウォールを起動するものの、このインターフェイスに対しては 特に関のルールも適用しない場合に選択します。このオプションは、別途に 存在するファイアウォールによってネットワーク全体が保護されている場合にのみ、選択してください。また、マシンに複数のインターフェイスが 存在していて、選択したインターフェイスが内部ネットワークに 接続されている場合にも便利な選択です。

非武装ゾーン

非武装ゾーンとは内部ネットワークと (敵が攻めてくる) インターネット の中間に位置する、追加の防御線を意味するものです。このゾーンの先に接続された ホストは、内部ネットワークとインターネットの両方からアクセスすることが できますが、それらのホストから内部ネットワークにはアクセスできません。

外部ゾーン

ファイアウォールをこのインターフェイス上で動作させ、攻撃に対する 完全な防御を設定します。この値が既定値になっています。

4 次へ を押します。

5 設定を有効にするには、さらに OK を押します。

11.4.1.3 未検出のネットワークカードの設定

お使いのネットワークカードによっては、正しく検出できない場合があります。この場合、検出済みのカード一覧に表示されなくなってしまうます。お使いの システムに適切なドライバが含まれている場合には、設定を手動で行なうことも できます。また、ブリッジやボンド、TUN、TAP などの特殊な種類のネットワーク デバイスを設定することもできます。未検出のネットワークカード (または特別なデバイス) を設定するには、下記のようにして行ないます:

1 YaST から ネットワークデバイス > ネットワーク設定 > 概要 を開き、追加 を押します。

- 2 ハードウェアダイアログ 内では、まず **デバイス種類** と **設定名** を選択します。設定しようとしているネットワークカードが PCMCIA や USB のデバイスである場合は、それぞれチェックボックスで選択を行ない、**次へ** を押します。それ以外のネットワークカードの場合、必要であればそのカードに使用するカーネルの **モジュール名** を選択し、**オプション** を入力します。

Ethtool オプションの欄には、インターフェイスを起動する際に ifup が使用する ethtool 向けのオプションを入力します。利用可能なオプションの一覧については、ethtool のマニュアルページをお読みください。また、オプション文字列が - で始まる場合 (たとえば -K インターフェイス名 rx on) は、文字列内の 2 番目は現在のインターフェイス名に置き換えられます。それ以外の場合 (たとえば autoneg off speed 10)、ifup は -s インターフェイス名として扱います。

- 3 **次へ** を押します。
- 4 一般, アドレス, ハードウェア の各タブを利用して、IP アドレスや デバイスの有効化、そのインターフェイスに適用するファイアウォールゾーンなどをそれぞれ設定します。これらの設定オプションについて、詳しくは 11.4.1.2 項「ネットワークカードの設定変更」(225 ページ)をお読みください。
- 5 デバイスの種類に **無線** を選択した場合は、次のダイアログで無線接続に関する設定を行ないます。
- 6 **次へ** を押します。
- 7 設定を有効にするには、さらに **OK** を押します。

11.4.1.4 ホスト名と DNS の設定

インストール時にネットワークの設定を変更せず、有線 LAN カードがその時点から利用可能な状態であった場合、お使いのコンピュータに対するホスト名は自動的に割り当てられ、DHCP が有効化されます。ネームサービスに関する情報についても同様です。お使いのネットワークカードに対する設定で DHCP を使用すると、ネームサーバの設定は DHCP サーバからの情報が適用されます。固定のネームサーバを設定したい場合は、そのように設定することもできます。

お使いのコンピュータの名前を変更したり、ネームサーバの設定と検索リストを変更したりしたい場合は、下記のようにして行ないます:

- 1 YaST の **ネットワークデバイス** モジュールを起動し、**ネットワーク設定 > ホスト名 / DNS** タブを選択します。

- 2 まずは *ホスト名* と *ドメイン名* を入力します。ドメイン名については指定しなくてもかまいません。またドメイン名は、このマシンがメールサーバである場合に、特に重要な設定です。なお、ホスト名はグローバル設定で、全てのネットワークインタフェースに対して適用されることにご注意ください。

IP アドレスの取得に DHCP を利用している場合、お使いのコンピュータ に対するホスト名を DHCP 経由で自動取得することができます。異なるネットワークに接続することで別のホスト名が設定されてしまい、グラフィカルなデスクトップ環境を利用する場合に混乱してしまうような場合には、このような動作を無効化することもできます。IP アドレスを DHCP 経由で取得している環境で、ホスト名を変更したくない場合は、*DHCP でホスト名を変更* のチェックを外してください。

ホスト名をループバック IP に割り当てる を選択すると、`/etc/hosts` ファイル内で `127.0.0.2` (ループバック) のアドレスに設定したホスト名が記入されるようになります。これは有効なネットワーク接続がないような状況でもホスト名を解決したい場合に便利な機能です。

- 3 *DNS 設定の修正* では、DNS 設定 (ネームサーバ、検索リストなどの `/etc/resolv.conf` ファイルの内容) の変更方法を選択することができます。

既定のポリシーを使用する を選択すると、設定は `netconfig` スクリプトで処理され、手動で設定したデータ (YaST や設定ファイルで設定したもの) と動的に取得したデータ (DHCP クライアントや NetworkManager などで設定したもの) を合成して使用します。既定のポリシーは、ほとんどの環境で適切な選択です。

手動のみ を選択すると、`netconfig` スクリプトは `/etc/resolv.conf` ファイルを修正できなくなります。手動での (エディタなどでの) 編集は通常どおり行なうことができます。

カスタムポリシーを使用する を選択すると、手動設定と自動設定の合成方法を指定する、*カスタムポリシールール* 文字列を設定することができるようになります。文字列はインターフェイス名をカンマ区切りで指定するもので、正しい設定元であるものと判断するインターフェイスを指定します。インターフェイス名にはワイルドカードを指定することもできます。たとえば `eth* ppp?` を指定すると、最初に全てのイーサネット デバイス (eth) を対象にし、その後に `ppp0` から `ppp9` までのインターフェイスを対象とします。これ以外にも、`/etc/sysconfig/network/config` ファイルで指定する手動設定との合成方法について、2 種類の特別なポリシー設定が存在します:

STATIC

手動設定と動的な設定の両方を合成するルールです。

STATIC_FALLBACK

動的な設定が利用できない場合にのみ、手動設定を利用するルールです。

詳しい情報は `man 8 netconfig` で表示されるマニュアルページをお読みください。

- 4 それぞれ **ネームサーバ** と **ドメイン検索** に入力を行ないます。ネームサーバは 192.168.1.116 などの形で、ホスト名ではなく IP アドレスで指定しなければなりません。**ドメイン検索** の枠内 には、ドメインを指定せずにホスト名だけを指定した場合に自動的に補完するドメイン名を指定します。**ドメイン検索** に複数のドメインを 指定する場合は、カンマか空白で区切ってください。
- 5 設定を有効にするには、*OK* を押します。

11.4.1.5 ルーティング (経路制御) の設定

お使いのマシンから他のネットワーク上にあるマシンと通信を行ないたい場合は、ネットワーク通信が正しい経路を通るようにするため、ルーティング (経路) 情報を設定しなければなりません。DHCP を利用している場合、ルーティング情報は自動的に設定されます。手動設定を使用している場合は、この設定も手動で 行なわなければなりません。

- 1 YaST から **ネットワーク設定 > ルーティング** を選択します。
- 2 それぞれ **デフォルトゲートウェイ** に IP アドレスを設定します (IPv4 および IPv6 (必要である場合のみ) に設定します)。**デフォルトゲートウェイ** は その他のルーティング情報に該当しなかった場合にのみ利用されるもので、該当する その他のルーティング情報が存在した場合には、デフォルトゲートウェイの代わりに、そちらの情報が使用されます。
- 3 **ルーティングテーブル** には、必要なだけルーティング情報を 入力することができます。それぞれ **宛先** のネットワークの IP アドレスと **ゲートウェイ** の IP アドレス、および **ネットマスク** を設定してください。また、指定した宛先にたどり着くための **デバイス** を指定することもできます (任意のデバイスを使用させたい場合は、マイナス記号を選択してください)。これらの値のうちのいずれかを省略したい場合は、いずれもマイナス記号 - を指定してください。一覧内にデフォルトゲートウェイを設定したい場合は、**宛先** に default と記入してください。

注記

複数のデフォルトゲートウェイを設定する場合は、それぞれの優先順位を設定するためにメトリックと呼ばれる値を設定することができます。メトリックのオプションを設定するには、*オプション* の項目内に *- metric 数値* と入力してください。数値が少ないほど優先順位が高いものとなり、最も高い優先順位を持つ経路が既定で使用されるようになります。ネットワークデバイスの接続が切れた場合は、そのルーティング情報は削除され、次点の候補が使用されます。ただし、現在のカーネルでは静的なルーティング設定でメトリックを使用することはありません。multipathd などのルーティングデーモンを利用した場合にのみ有効です。

- 4 なお、お使いのシステムをルータとして機能させる場合は、*ネットワーク設定* 内の *IP 転送を有効にする* を選択してください。
- 5 設定を有効にするには、*OK* を押します。

11.4.2 モデム

YaST コントロールセンターからは、*ネットワークデバイス > モデム* を選択することで、モデム設定を行なうことができます。お使いのモデムが自動で検出されない場合は *モデムデバイス* のタブに移動し、*追加* を押して手動設定を行なってください。手動設定では、*モデムデバイス* の欄にモデムの接続されているインターフェイスを指定します。

ヒント: CDMA モデムと GPRS モデム

YaST から、対応している CDMA および GPRS モデムを設定する場合は、通常のモデムと同様に *モデム モジュール* から設定を行ないます。

図 11.4 モデムの設定

モデムのパラメータ

モデムデバイス (V)
/dev/modem

ダイヤルプレフィクス (必要時のみ) (X)

ダイヤルモード

☒ トーンダイヤル (T)
☐ パルスダイヤル (P)

特別の設定

☒ スピーカーを動作させる (S)
☒ ダイヤルトーンの検出 (E)

詳細 (D)

ヘルプ (H) 戻る (B) キャンセル (C) 次へ (N)

お使いの電話回線が構内交換機 (PBX) 内に設置されている回線である場合は、ダイヤルプレフィクスを入力する必要がある場合があります。通常は 0 を指定しますが、詳しくは PBX に添付されている手順書をお読みください。また、ダイヤルモードとしてトーンまたはパルスを選択することができるほか、ダイヤルトーンを検出するかどうかを設定することもできます。このほか、交換機に接続されている環境の場合は、ダイヤルトーン検出を無効に設定する必要があります。

また、**詳細** ボタンを利用すると、ボーレートやモデムの初期化文字列などを設定することができます。お使いのモデムが自動で検出されなかったり、データ転送を働かせるために特殊な設定が必要なモデムであったりする場合にのみ設定を変更してください。これは主に ISDN のターミナルアダプタの場合に当てはまります。詳細ダイアログを終了するには、**OK** を押します。また、**root** の権限を与えることなく一般ユーザにモデムの操作を許可するには、**KInternet** を利用して **root** 以外のユーザにもデバイス操作を許すを選択してください。この場合、管理者権限を持たないユーザでもインターフェイスの有効化と無効化を行なうことができるようになります。さらに **ダイヤルプレフィクス正規表現** では正規表現を指定します。一般ユーザでも修正することのできる **KInternet** 内の **ダイヤルプレフィクス** は、この正規表現にマッチしていなければならない、という制約が課せられます。この項目に何も記入しない場合は、管理者権限がないと異なる **ダイヤルプレフィクス** を設定することができなくなります。

次のダイアログでは ISP を選択します。まずはご利用の 国 を選択すると、事前に設定されている一覧から ISP を選択することができます。また *新規* を押すと、ご利用になる ISP のデータを独自に入力することもできます。独自入力を行なう場合は、ご利用の ISP の名称と電話番号、ログイン名とパスワードをそれぞれ入力してください。また、*常にパスワードを尋ねる* を選択すると、接続するたびに パスワードを尋ねる動作になります。

最後のダイアログでは、追加の接続オプションを指定します：

ダイヤルオンデマンド

ダイヤルオンデマンド を選択すると、必要に応じてダイヤル アップ接続を行なうようになります。また、この機能を設定する場合は、1 つ 以上のネームサーバを設定してください。なお、インターネットへのデータ要求を 定期的に行なう種類のソフトウェアが存在することから、インターネット接続の 課金がそれほど高くない環境でのみご利用になることをお勧めします。

接続時に DNS を変更する

このオプションを選択すると、インターネットに接続するごとにネームサーバの アドレスを更新するようになります。この設定は既定で有効になっています。

自動的に DNS 情報を取得する

お使いのプロバイダが接続時にドメインネームサーバの設定を送信しない場合、このオプションの選択を外して DNS を手動で設定してください。

自動再接続

このオプションを選択すると、接続が切れると自動的に再接続を行なうようになります。

プロンプトの無視

このオプションを選択すると、ダイヤルアップサーバに接続した際に検出されるプロンプトを無視するようになります。接続が遅かったり全く動作しなかったりした場合は、このオプションを試してみてください。

外部ファイアウォールインターフェイス

このオプションを選択すると、ファイアウォールを有効化して外部インターフェイスとして登録するようになります。これを利用すると、インターネット接続の利用中に 受けた攻撃から、身を守ることができるようになります。

無通信タイムアウト (秒)

このオプションは、何もネットワーク上の通信を行なわなかった場合に、モデムの 接続を自動で切断するための設定です。

IP の詳細

これを押すと、アドレス設定のダイアログが開きます。お使いの ISP が接続したホストに対して動的な IP アドレスを割り当てない場合は、*可変 IP アドレス* のチェックを外して、独自のローカル IP アドレスとリモートの IP アドレスを入力します。詳しくはお使いのプロバイダにご確認ください。デフォルトルートについては有効に設定したまま、*OK* を押してダイアログを閉じてください。

次へ を押す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。最後に *OK* を押すと、ダイアログを閉じることができます。

11.4.3 ISDN

このモジュールを利用することで、お使いのシステムにある 1 つまたは複数の ISDN カードを設定することができます。YaST で ISDN カードを認識しない場合は、*ISDN デバイス* タブ内にある *追加* ボタンを押して、手動でカードを追加してください。複数のインターフェイスを設定することができますが、複数の ISP を 1 つのインターフェイスに設定することはできません。続いて表示されるダイアログで、カードの動作に必要な ISDN オプションを設定します。

図 11.5 ISDN の設定

contrcontr0 に関する ISDN のローレベル設定

ISDN カードの情報	
製造元	U.S.Robotics
ISDN カード	ISDN PCI Card TA
ドライバ (V)	HiSax driver

ISDN プロトコル	国 (C)	コード (D)
<input checked="" type="radio"/> Euro-ISDN (EDSS1) (E)	ドイツ	+49
<input type="radio"/> 1TR6 (6)		
<input type="radio"/> 専用回線 (L)		
<input type="radio"/> NIT (1)		
	市外局番 (A)	ダイヤルプレフィックス (D)
	<input type="checkbox"/> ISDN 記録を開始する (I)	

デバイスの有効化 (D)

起動時

ヘルプ (H) 戻る (B) キャンセル (C) OK (O)

図11.5「ISDN の設定」(238 ページ) に示しているとおり、次のダイアログでは使用するプロトコルを選択します。既定は *Euro-ISDN (EDSS1)* ですが、古い交換

機や大きな交換機を使用するような場合は、*1TR6* を選択してください。また、アメリカ国内でお使いの場合は、*N/1* を選択してください。続いて国を選択すると、適切な国コードが項目に記入されます。最後に、必要に応じて *市外局番* と *ダイヤルプレフィックス* を入力してください。ISDN の通信について全ての記録をとりたくない場合は、*ISDN 記録を開始する* のチェックを外してください。option.

また、*デバイスの有効化* では、ISDN インターフェイスの開始方法を指定することができます。*起動時* を選択すると、システムの起動時に ISDN デバイスを初期化するようになります。*手動* を選択した場合は、ISDN ドライバを読み込むのに root から `rcisdn start` を実行しなければなりません。PCMCIA や USB のデバイスに対して設定する *ホットプラグ* では、デバイスが接続されたときにドライバを自動で読み込むようになります。これらの設定を行ない、*OK* を押します。

次のダイアログでは ISDN カードのインターフェイス種類を指定するほか、既存のインターフェイスに対して ISP を追加することもできます。インターフェイスは SyncPPP, RawIP のうちから選択しますが、多くの ISP は下記で説明するとおり SyncPPP モードで動作します。

図 11.6 ISDN インターフェイス設定

SyncPPP インターフェイス ipppnet0 の追加

接続設定

自分の電話番号(P)

デバイスの有効化 (D)

手動

☒ QInternet を利用して root 以外のユーザにもデバイス操作を許

☒ ChargeHUP (H)

☐ チャネルを束ねる (A)

☒ 外部ファイアウォールインターフェイス (W)

☒ ファイアウォールの再起動 (W)

詳細 (D)...

ヘルプ (H) 戻る (B) キャンセル (C) 次へ (N)

次に、*自分の電話番号* を入力します。これはお使いの環境によって入力する値が異なります：

回線に直接接続された ISDN カードの場合

標準の ISDN 回線では、3 種類の電話番号 (複数契約者番号、MSN と呼びます) が用意されています (翻訳者注: 日本国内では、別途契約しない限り 1 種類の電話番号だけになります)。契約者が申し込むことで、最大 10 種類までの番号を用意することができます (翻訳者注: 日本国内では 最大 3 種類までです)。この項目には、これらのうちのいずれかの番号を入力しますが、市外局番は含めずに入力してください。正しくない番号を入力した場合は、お使いの ISDN に割り当てられている最初の番号が自動的に使用されます。

構内交換機 (PBX) に接続された ISDN カードの場合

利用している機器によって、設定方法が異なります:

1. 家庭用などの小規模の交換機 (PBX) の場合、多くは内部の呼び出しに Euro-ISDN (EDSS1) プロトコルを使用しています。これらの交換機は内部に S0 バスが存在し、機器の呼び出しには内部番号を使用します。

この場合は、内部番号のうちのいずれかを電話番号として設定してください。直接の外部発信に対応するよう設定されている交換機であれば、交換機側の電話番号を使用することもできます。この設定でうまくいかない場合は、電話番号として 1 桁だけの "0" を設定してみてください。詳しい情報は、お使いの交換機に付属している文書をお読みください。

2. 企業用などの大規模な構内交換機の場合は、内部の呼び出しに 1TR6 プロトコルを使用しています。これらの電話番号は EAZ と呼ばれ、通常は 外線番号と対応した番号になっています。Linux では、EAZ の最後の 1 桁を指定します。うまくいかない場合は、1 から 9 までの各番号を試してみるのもよいでしょう。

次の課金タイミングになる前に回線を切断したい場合は、*ChargeHUP* を選択してください。ただし、この機能は全ての ISP で動作するというわけではないことにご注意ください。また、これ以外にも *チャンネルを束ねる* を設定することで、マルチチャンネル設定 (マルチリンク PPP) を設定することができます。さらに *外部ファイアウォールインターフェイス* と *ファイアウォールの再起動* を選択することで、回線接続に対してファイアウォールを設定することもできますし、*KInternet* を利用して *root* 以外のユーザにもデバイス操作を許すを選択すると、管理者権限のない一般ユーザからでもインターフェイスの有効化／無効化を行なうことができます。

詳細 を押すと、一般家庭の環境ではあまり使用しない、より細かい設定画面を開くことができます。*OK* ボタンを押すと *詳細* ダイアログを終了することができます。

次のダイアログでは、IP アドレス関連の設定を行ないます。お使いのプロバイダから固定の IP アドレスを割り当てられている場合を除き、*可変 IP アドレス* を選択し

てください。割り当てがある場合は、ISP の提供 情報に従ってローカルとリモートの IP アドレスをそれぞれ入力してください。また、このインターフェイスをインターネットに対する既定のルートに設定したい 場合は、**デフォルトルート** を選択します。各ホストには 既定のルートに設定するインターフェイスを 1 つだけ設定できます。設定が終わったら、**次へ** を押します。

次のダイアログでは国とプロバイダを選択することができます。一覧には、迂回ダイヤルサービス (call-by-call や dial around service と呼ばれる場合もあります) に対応したプロバイダのみが掲載されています。お使いの ISP が 一覧に存在しない場合は、**新規** を押してください。すると **プロバイダパラメータ** ダイアログが開き、ISP に関する 情報を入力できるようになります。なお電話番号を入力する際は、番号の途中に 空白やカンマを入れないでください。最後に ISP から提供されているユーザ名と パスワードを入力します。設定が終わったら **次へ** を押します。

単独のワークステーションで **ダイヤルオンデマンド** (必要なときにダイヤルする) を行なうには、ネームサーバ (DNS サーバ) の設定も 必要です。多くの ISP では動的な DNS 設定に対応していて、ネームサーバの IP アドレスは ISP への接続時に取得することができるようになっています。単独の ワークステーションの場合は、**ダミーデータ**として 192.168.22.99 のようなアドレスを 設定しておく必要があります。お使いの ISP が動的な DNS に対応していない場合、ISP 側のネームサーバの IP アドレスを設定してください。また、必要であれば 無通信タイムアウトを設定することもできます。これは、何もネットワーク上の 通信を行なわなかった場合に、接続を自動で切断するための設定 (秒単位) です。さらに **次へ** を押してください。YaST はインターフェイスの 設定概要を表示します。表示された設定を適用するため、最後に **OK** を押してください。

11.4.4 ケーブルモデム

国によっては、インターネットへの接続を行なう手段としてケーブル TV のネットワークを利用するのが一般的である場合があります。ケーブル TV の契約者は、一方を TV ケーブルに接続し、他方をコンピュータのネットワークカード (10Base-T の ツイストペアケーブル) に接続するタイプのモデムを受け取ります。そのモデムは ケーブルモデムと呼び、固定または可変の IP アドレスが割り当てられる種類の、専用線によるインターネット接続が提供されます。

お使いのネットワークカードを設定する際には、お使いの ISP が提供する手順に従って設定し、**可変 IP アドレス** または **固定 IP アドレス** のいずれかを選択してください。現在、多くのプロバイダ では DHCP を利用していますが、特別なビジネスアカウントを取得することで 固定の IP アドレスが割り当てられる場合もあります。

11.4.5 DSL

DSL デバイスを設定するには、YaST の ネットワークデバイス 内にある *DSL* モジュールを選択してください。この YaST モジュールには、それぞれ下記のプロトコルに対応した、DSL リンクのパラメータ 設定ダイアログが含まれています：

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoATM)
- CAPI for ADSL (Fritz カード)
- Point-to-Point Tunneling Protocol (PPTP) (オーストリア)

DSL の設定概要 ダイアログ内の *DSL* デバイス タブには、設定済みの DSL デバイスの一覧が表示されています。DSL デバイスの設定を変更するには、一覧からデバイスを選択して *編集* を押してください。新しい DSL デバイスを手動で 追加する場合は、*追加* を押してください。

PPPoE や PPTP をベースにした DSL 接続の設定では、接続を行なうネットワークカードの設定を正しく行なっておく必要があります。ネットワークカードの設定を行っていない場合は、まず *ネットワークカードの設定* を押して設定を行ってください（詳しくは 11.4.1 項「YaST を利用したネットワークカードの設定」（223 ページ）をお読みください）。DSL 接続の場合、アドレスは DHCP ではない手段で自動配布 される場合がありますが、*可変 IP アドレス* を選択せず、その代わりに、192.168.22.1 のようなダミーの固定 IP アドレスを指定してください。また、サブネットマスク にもダミーの値 255.255.255.0 を 指定してください。単独のワークステーションで利用している場合は、*デフォルトゲートウェイ* を設定する必要はありません。

ヒント

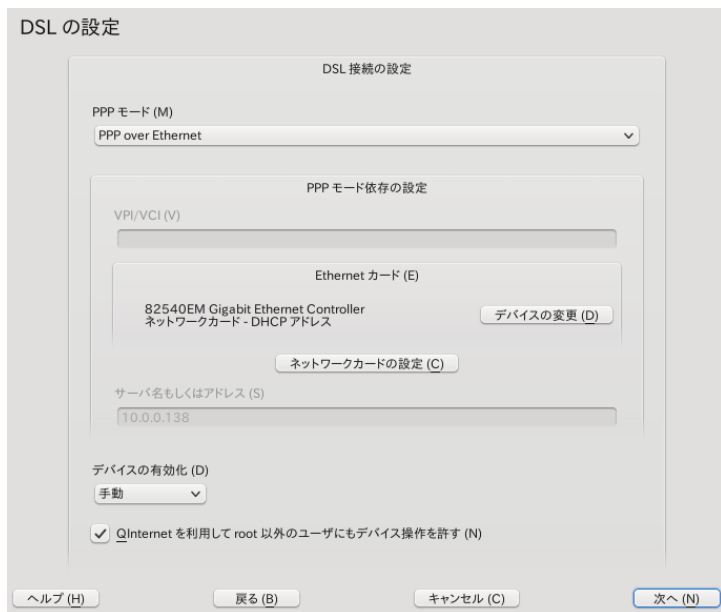
IP アドレス と *サブネットマスク* の 値は、いずれもダミーの値です。ネットワークカードの起動を行なうために必要な 設定であり、DSL の接続設定とは無関係です。

最初の DSL 設定ダイアログ (図11.7「DSL の設定」(243 ページ)) では、*PPP* モードと DSL モデムが接続されている *Ethernet カード* をそれぞれ選択します (多くの場合、eth0 を選択します)。その後、システムの起動時に DSL リンクを確立させるかどうかを指定する、*デバイスの有効化* を選択します。また、*KInternet* を利用して *root* 以外のユーザにもデバイス操作を許す を選択すると、KInternet 経由

で root 権限のない一般ユーザがインターフェイスの有効化／無効化を行なうことができるようになります。

次のダイアログでは国とプロバイダを選択することができます。この次の DSL 設定ダイアログは、これまでに選択したオプションによって異なります。利用可能なオプションについての詳細は、ダイアログ内から利用できるヘルプをお読みください。

図 11.7 DSL の設定



DSL 接続の設定

PPP モード (M)
PPP over Ethernet

PPP モード依存の設定

VPI/VCI (V)

Ethernet カード (E)
82540EM Gigabit Ethernet Controller
ネットワークカード - DHCP アドレス
デバイスの変更 (D)

ネットワークカードの設定 (C)

サーバ名もしくはアドレス (S)
10.0.0.138

デバイスの有効化 (D)
手動

☒ QInternet を利用して root 以外のユーザにもデバイス操作を許す (N)

ヘルプ (H) 戻る (B) キャンセル (C) 次へ (N)

単独のワークステーションで **ダイヤルオンデマンド** (必要なときにダイヤルする) を行なうには、**ネームサーバ (DNS サーバ)** の設定も 必要です。多くの ISP では動的な DNS 設定に対応していて、ネームサーバの IP アドレスは ISP への接続時に取得することができるようになっています。単独のワークステーションの場合は、**ダミーデータ**として 192.168.22.99 のようなアドレスを設定しておく必要があります。お使いの ISP が動的な DNS に対応していない場合、ISP 側のネームサーバの IP アドレスを設定してください。

また、**無通信タイムアウト (秒)** を設定することもできます。これは、何もネットワーク上の通信を行なわなかった場合に、接続を自動で切断するための設定 (秒単位) です。通常のタイムアウトは 60 から 300 秒程度を指定します。**ダイヤルオンデマンド**を有効にしていない場合は、このタイムアウト値をゼロに設定することで、自動切断を無効化することができます。

T-DSL の設定は、DSL の設定によく似ています。プロバイダとして *T-Online* を選択すると、YaST は T-DSL の設定ダイアログを表示します。このダイアログから、T-DSL に必要ないくつかの追加情報 (ライン ID, T-Online 番号, ユーザコード, パスワード) を入力してください。これらの情報は、T-DSL の契約時に受け取った中に含まれているものを入力します。

11.5 NetworkManager

NetworkManager はラップトップ機やその他の可搬型コンピュータをご利用の場合は便利な ツールです。NetworkManager を利用することで、移動中にネットワークが切り替わっても ネットワークインターフェイスの設定やその切り替えについて、心配する必要がなくなります。

11.5.1 NetworkManager と ifup

NetworkManager は全ての環境において便利なものとは言えませんが、ネットワーク接続管理を行なうにあたって、従来の方法 (ifup) と NetworkManager のどちらを利用するのか、選択する だけの価値はあります。NetworkManager でお使いのネットワーク接続を管理したい場合は、23.2項「NetworkManager の有効化と無効化」(436 ページ) に書かれている手順で YaST のネットワーク設定モジュールを起動し、NetworkManager を有効に設定してください。あとは NetworkManager で ネットワークの設定を行なうだけです。NetworkManager の用途と設定手順の説明について、詳しくは 第23章 *NetworkManager の使用* (435 ページ) をお読みください。

ifup と NetworkManager には下記のような違いがあります:

root 権限

ネットワークの設定に NetworkManager を使用する場合、お使いのデスクトップ環境内にある アイコンを利用することで、自由にネットワークを切り替えたり停止したり、起動したりすることができます。また NetworkManager では、root 権限を必要とすることなく無線ネットワークカードの接続設定を行なうことができます。このため、モバイルワークステーション環境の場合 NetworkManager は申し分のない解法となるでしょう。

ifup による従来の設定方法でも、ユーザ管理デバイスのように介入無しに接続を切り替えたり 停止したり、開始したりすることができます。しかしながら、この方法ではネットワーク デバイスの変更や設定には root の権限が必要となります。

す。これは特に、事前に接続する可能性のある全てのネットワークを設定しなければならないという点で、モバイル環境の場合に問題となります。

ネットワーク接続の種類

従来の方でも NetworkManager でも、無線ネットワーク (WEP, WPA-PSK, WPA-Enterprise でのアクセス) やダイアルアップ、有線の設定を取り扱うことができます。DHCP や固定のアドレス設定、VPN 経由の接続にも対応しています。NetworkManager を利用する場合は、モバイルブロードバンド (3G) モデムを利用した接続を行なうこともできます。こちらは従来の方では利用できません。

NetworkManager は利用可能なネットワーク接続から、最も良いものを常に選択してつなぎ続けるように動作します。ネットワークケーブルが誤って外されてしまった場合でも、再接続を試みるようになっています。また無線接続の場合は、設定された無線接続の中から最も信号品質の良いネットワークを判断して自動接続する仕組みを備えています。ifup で同じ機能を利用するには、様々な設定を施さなければ実現できません。

11.5.2 NetworkManager の機能と設定ファイル

NetworkManager での個別のネットワーク設定は設定プロファイルに保存されます。NetworkManager または YaST で設定したシステム接続は、`/etc/networkmanager/system-connections/*` または `/etc/sysconfig/network/ifcfg-*` ファイル内に保存されます。ユーザ側で設定した接続は、GNOME の場合は GConf 内に

何もプロファイルを設定していない場合、NetworkManager は自動的にプロファイルを作成し、Auto `$INTERFACE-NAME` の名前を設定します。これにより、できる限り多くの場合において設定作業を行なうことなく、安全な設定を使用することができるようになっています。自動で作成された設定が要件にあわない場合は、KDE や GNOME が提供するネットワーク接続設定ダイアログを利用して、必要な設定作業を行なってください。詳しくは 23.3 項「ネットワーク接続の設定」(437 ページ) をお読みください。

11.5.3 NetworkManager の機能のコントロールと無効化

集中管理されているマシンでは、一部の NetworkManager 機能が操作されていたり、無効化されていたりする場合があります。たとえば管理者が設定した接続をユーザ側で修正することを許すかどうかや、ユーザ側で独自のネットワーク設定を作成することができるかどうか などがあります。NetworkManager でのポリシー設定を閲覧したり変更したりするには、PolicyKit 向けのグラフィカルな 認可 ツールを起動してください。左側の ツリーで *network-manager-settings* の項目を選択して設定を 行ないます。

下記に nm; に関連する PolicyKit の識別子の概要を示します:

表 11.5 NetworkManager における PolicyKit の識別子

識別子	説明
org.freedesktop.NetworkManager.enable-disable-network	システムのネットワーク接続の有効化／無効化。
org.freedesktop.NetworkManager.sleep-wake	NetworkManager をスリープ状態にする、もしくはスリープを解除する。
org.freedesktop.NetworkManager.enable-disable-wwan	モバイルのブロードバンドデバイスを有効化／無効化する。
org.freedesktop.NetworkManager.enable-disable-wimax	WiMAX モバイルブロードバンドデバイスを有効化／無効化する。
org.freedesktop.NetworkManager.network-control	ネットワーク接続の制御を許可する。
org.freedesktop.NetworkManager.enable-disable-wifi	WiFi デバイスを有効化／無効化する。
org.freedesktop.NetworkManager.settings-modify-hostname	固定で設定されているホスト名の修正。

識別子	説明
org.freedesktop.network-manager-settings.modify.system	全てのユーザに対して設定された接続の修正。
org.freedesktop.network-manager-settings.modify.own	個人用のネットワーク接続の修正。
org.freedesktop.network-manager-settings.system.wifi.share.open	オープンな WiFi ネットワークを介した接続共有。
org.freedesktop.network-manager-settings.system.wifi.share.protected	保護された WiFi ネットワークを介した接続共有。

11.6 手動でのネットワーク設定方法

手動でのネットワーク設定は最後の手段として用意されているものです。特に問題がない限り、YaST での設定をお勧めします。しかしながら、YaST でのネットワーク設定を行なうにあたり、基礎になっている情報を 知っておくと、より便利に利用することができると考えています。

カーネルがネットワークカードを検出して関連するネットワークインターフェイスを作成すると、デバイスの認識順序とカーネルモジュールの読み込み順序に従って デバイス名が割り当てられます。規定でカーネルが割り当てる名前は非常に単純に推測できるもので、ハードウェア環境の変更を難しくしてしまっています。稼働中にハードウェアを追加したり削除したり、もしくはデバイスの設定を自動化しているようなシステムでは、再起動を行なうたびにデバイス名が異なることになってしまい、安定したデバイス名の割り当てを期待することができません。

しかしながら、全てのシステム設定ツールはインターフェイス名を基準にして設定を管理しています。このような問題を解決するのが udev です。udev の固定ネットワーク デバイス生成の機能 (`/lib/udev/rules.d/75-persistent-net-generator.rules`) を利用すると、条件に該当するハードウェア (規定ではハードウェアアドレスを使用します) に対して、固定のインターフェイス名を割り当てることができます。udev のネットワークインターフェイスに対するデータベースは、`/etc/udev/rules.d/70-persistent-net.rules` ファイル内に 保存されます。上記ファ

イルの各行には単一のネットワークインターフェイス名と、そのインターフェイスに割り当てた固定の名前が記述されています。システム管理者は `NAME=""` の項目を編集することで、割り当てられた名前を変更 することができます。それぞれの設定は YaST から変更を行なうこともできます。

表11.6「手動ネットワーク設定を行なう場合の関連スクリプト」(248 ページ) には、ネットワーク設定に関する最も重要な スクリプトファイルを列挙しています。

表 11.6 手動ネットワーク設定を行なう場合の関連スクリプト

コマンド	機能
<code>ifup</code> , <code>ifdown</code> , <code>ifstatus</code>	<code>if</code> スクリプトはネットワークインターフェイスの起動や 停止、および指定したインターフェイスの状態確認を行なうためのスクリプト です。詳しくは <code>ifup</code> のマニュアルページをお読みください。
<code>rcnetwork</code>	<code>rcnetwork</code> スクリプトは全てのネットワークインターフェイス (または指定した 1 つのインターフェイス) を起動したり停止したりするために、使用するスクリプトです。 <code>rcnetwork stop</code> でネットワーク インターフェイスの停止を、 <code>rcnetwork start</code> で起動を、 <code>rcnetwork restart</code> で再起動をそれぞれ行ないます。なお、ある 1 つのネットワークインターフェイスだけ停止や起動、再起動を行ないたい場合は、コマンドの後ろにインターフェイス名を指定してください。たとえば <code>rcnetwork restart eth0</code> のようになります。また、 <code>rcnetwork status</code> コマンドでは、インターフェイス の状態と IP アドレス、および DHCP クライアントの稼働状態がそれぞれ表示 されます。さらに <code>rcnetwork stop-all-dhcp-clients</code> や <code>rcnetwork restart-</code>

コマンド	機能
	all-dhcp-clients では、それぞれ全てのネットワークインターフェイスに対して動作している DHCP クライアントを 停止したり、再起動したりすることができます。

udev と固定のデバイス名について、詳しくは 第10章 *udev* による動的なカーネルデバイス管理 (189 ページ) をお読みください。

11.6.1 設定ファイル

本章には、ネットワーク関連の設定ファイルとそれらの目的説明、および 使用する書式について説明を行なっています。

11.6.1.1 /etc/sysconfig/network/ifcfg-*

これらのファイルはネットワークインターフェイスの設定ファイルです。開始モードや IP アドレスなどの設定が書かれています。利用可能なパラメータについては、ifup のマニュアルページをお読み ください。また、特定のインターフェイスに対してだけ一般的な設定を行ないたい 場合は、dhcp, wireless にある ほとんどの値を ifcfg-* ファイルで設定することができます。なお、/etc/sysconfig/network/config 内にある多くの 値はグローバル設定であるため、ifcfg ファイルでは上書きすることができません。たとえば NETWORKMANAGER や NETCONFIG_* の値などがグローバル設定です。

また、ifcfg.template ファイルについては、11.6.1.2項「/etc/sysconfig/network/config, /etc/sysconfig/network/dhcp, /etc/sysconfig/network/wireless」(249 ページ) をお読みください。

11.6.1.2 /etc/sysconfig/network/config, /etc/sysconfig/network/dhcp, /etc/sysconfig/network/wireless

config ファイルは、ifup, ifdown, ifstatus の各ファイルの 動作に関して、一般的な設定を行なうためのファイルです。また、dhcp ファイルには DHCP の設定が、wireless ファイルには無線 LAN カードの設定がそれぞれ 書かれています。

これら 3 種類のファイルで利用する設定は、それぞれコメント 内に書かれています。また、`/etc/sysconfig/network/config` ファイル内の設定値のうちのいくつかを `ifcfg-*` で 利用することができます。`ifcfg-*` 側に設定値を入力した 場合は、`config` よりも優先されます。なお、`/etc/sysconfig/network/ifcfg.template` ファイルでは、インターフェイス単位で利用可能な設定値の一覧を示しています。しかしながら、多くの `/etc/sysconfig/network/config` にある多くの変数はグローバル設定で、`ifcfg-*` ファイルでは 上書きできないことにご注意ください。たとえば `NETWORKMANAGER` や `NETCONFIG_*` がグローバル設定です。

11.6.1.3 `/etc/sysconfig/network/routes` と `/etc/sysconfig/network/ifroute-*`

このファイルには、スタティックルート (静的な経路情報) を設定します。様々なシステム処理に必要な全てのスタティックルートを、`/etc/sysconfig/network/routes` ファイルに設定することができます: ホストへの経路のほか、ゲートウェイ経由のホスト経路、ネットワーク への経路などがあります。各インターフェイスに対して個別の経路を設定する必要がある場合は、追加の設定ファイル `/etc/sysconfig/network/ifroute-*` を作成してください。ここで、* にはインターフェイスの 名前を入力します。経路設定ファイルの設定は、たとえば下記ようになります:

# 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

最初の列には経路の宛先が示されています。ネットワークやホストの IP アドレスのほか、ネームサーバに 接続できる 環境であれば、完全修飾ドメイン名 (FQDN) やホスト名を利用することもできます。

2 列目には、既定のゲートウェイまたは特定のホストやネットワークに到達するためのゲートウェイが書かれています。3 列目にはネットワークのネットマスクか、もしくはゲートウェイの向こう側にあるホストが書かれています。たとえば ゲートウェイの向こう側にあるホストを設定する場合、マスクは `255.255.255.255` になります。

4 列目はループバックやイーサネット, PPP やダミーデバイスなどに接続されているネットワークでのみ意味を持つものです。ここにはデバイス名を入力します。

(オプションで) 5 つめの列に入力することもできます。ここでは経路の種類を設定します。この列にはパーサーが正しくコマンドを解釈するために利用する、- 記号を設

定する必要はありません。詳しくは routes(5) のマニュアルページをお読みください。

IPv4 および IPv6 向けには、下記の統合フォーマットを利用することができます：

プレフィクス/長さ ゲートウェイ - [インターフェイス]

また、下記のような互換フォーマットを利用することもできます：

プレフィクス ゲートウェイ 長さ [インターフェイス]

IPv4 に対しては、ネットマスクを利用した古い形式を利用することもできます：

IPv4 ネットマスク ゲートウェイ IPv4 ネットマスク [インターフェイス]

それぞれ下記に示す例が等価な表現になります：

2001:db8:abba:cafe::/64	2001:db8:abba:cafe::dead	-	eth0
208.77.188.0/24	208.77.188.166	-	eth0
2001:db8:abba:cafe::	2001:db8:abba:cafe::dead	64	eth0
208.77.188.0	208.77.188.166	24	eth0
208.77.188.0	208.77.188.166	255.255.255.0	eth0

11.6.1.4 /etc/resolv.conf

このファイルには、ホストが属するドメイン名を入力する (search キーワードを使用します) ほか、アクセスするネームサーバのアドレス (nameserver キーワード) も入力します。このファイルには複数のドメイン名を入力することができます。完全修飾型ではない名前を解決する場合、search に書かれたそれぞれのドメイン名を付加して 1 回ずつ解決を試みます。複数のドメイン名は複数行に分けて設定するものとし、それぞれ nameserver から書き始めてください。また、コメントは # 文字を行頭に入れてください。例 11.5「/etc/resolv.conf」(252 ページ) には /etc/resolv.conf の記述例を示しています。

ただし、/etc/resolv.conf は手作業による編集は行なうべきではありません。このファイルは netconfig スクリプトが生成するものであるためです。YaST を利用せずに固定の DNS 設定を行ないたい場合は、/etc/sysconfig/network/config ファイル内の該当項目を修正してください：

NETCONFIG_DNS_STATIC_SEARCHLIST

ホスト名の参照に際して、利用する DNS ドメイン名。

NETCONFIG_DNS_STATIC_SERVERS

ホスト名の参照時に利用する、ネームサーバの IP アドレス。

NETCONFIG_DNS_FORWARDER

設定すべき DNS フォワーダの名前。

netconfig を利用した DNS 設定を無効化するには、NETCONFIG_DNS_POLICY=' ' を設定してください。また、netconfig について詳しくは man 8 netconfig をお読みください。

例 11.5 /etc/resolv.conf

```
# ドメイン名の指定
search example.com
#
# ネームサーバとして dns.example.com (192.168.1.116) を使用する設定
nameserver 192.168.1.116
```

11.6.1.5 /sbin/netconfig

netconfig は追加のネットワーク設定を管理するための モジュール型ツールです。本ソフトウェアは、事前に定義しておいた設定と DHCP や PPP など取得した動的な情報を、事前に定義したポリシーに従って 合成することができます。必要な変更は、各設定ファイルの修正を行なって サービスの再起動などを行なう netconfig モジュールを呼び出すことで、システムに反映される形になります。

netconfig は 3 つの主なアクションから構成されています。netconfig modify と netconfig remove は DHCP や PPP デーモンから呼び出されるもので、netconfig に対して設定を変更したり削除したりする場合に利用します。ユーザからは netconfig update コマンドだけが 利用できます:

modify

netconfig modify コマンドは、現存するインターフェイス やサービス固有の動的な設定を変更し、ネットワークの設定を更新するコマンド です。netconfig は標準入力またはファイル (--lease-file ファイル名 を指定します) から設定を読み込み、システムの再起動 (または次の修正や削除動作) までの間、内部でそれらを保持します。あるインターフェイスやサービスに対する設定がすでに 存在していた場合は、それらは上書きされます。インターフェイスは -i インターフェイス名 で指定 するほか、サービスの場合は -s サービス名 で指定します。

remove

netconfig remove コマンドは、指定したインターフェイスや サービスに対して以前に設定した設定を削除し、ネットワークの設定を更新する コマンドです。イ

インターフェイスは `-i` インターフェイス名 で指定 するほか、サービスの場合は `-s` サービス名 で指定します。

update

`netconfig update` コマンドは、現在の内容でネットワーク 設定を更新するコマンドです。これはポリシーや静的な設定を更新した場合に 便利なコマンドです。また、指定したサービス (`dns`, `nis`, `ntp`) に対してのみ 更新を行ないたい場合は、`-m` モジュールタイプ パラメータをご利用ください。

`netconfig` のポリシーや静的な設定は `/etc/sysconfig/network/config` ファイルに書かれているもので、手動で行なうことができるほか、YaST を利用して設定することも できます。DHCP や PPP のような自動設定ツールが提供する動的な設定は、これらのツールから直接通知されるか、`netconfig modify` や `netconfig remove` コマンドで通知されます。また、NetworkManager でも `netconfig modify` や `netconfig remove` コマンドを使用する場合があります。NetworkManager が有効になっている 場合 (auto ポリシーモードの場合) は、従来の `ifup` 方式での 全てのインターフェイス設定が無視されます。NetworkManager がいかなる設定も 提供しない場合に限り、静的な設定が次点候補として使用されます。NetworkManager と従来の `ifup` 方式の混在には対応していません。

`netconfig` について詳しくは、`man 8 netconfig` で表示されるマニュアルページをお読みください。

11.6.1.6 /etc/hosts

例11.6「`/etc/hosts`」(253 ページ) に示してあるとおり、このファイルには IP アドレスとホスト名の対が書かれています。ネームサーバが設定されていない 場合は、IP 接続を行なう可能性のある全てのホストについて、本ファイル内に 設定しておく必要があります。各ホスト 1 行とし、IP アドレスと完全修飾ドメイン名、ホスト名をそれぞれ記入します。IP アドレスは行頭に記述し、タブかスペースで区切って残りの項目を記入します。コメントを記入する場合は、コメントの前に `#` を記入してください。

例 11.6 `/etc/hosts`

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

11.6.1.7 /etc/networks

このファイルでは、ネットワーク名とネットワークアドレスの変換を行ないます。書式は `hosts` ファイルに似ていますが、ネットワーク名 の後にアドレスが続く点が異なります。詳しくは 例11.7「`/etc/networks`」(254 ページ) をご覧ください。

例 11.7 `/etc/networks`

```
loopback      127.0.0.0
localnet      192.168.0.0
```

11.6.1.8 `/etc/host.conf`

このファイルでは、*リゾルバ*と呼ばれるライブラリを利用してホスト名やネットワーク名を名前解決する際、その解決処理を設定します。このファイルは `libc4`, `libc5` にリンクされているライブラリでのみ 使用します。現行の `glibc` プログラムの場合は、`/etc/nsswitch.conf` ファイルの設定を参照してください。パラメータはそれぞれ 1 行に 1 つずつ入力します。コメントを記入する場合は、コメントの前に `#` を入力してください。利用可能なパラメータについては 表11.7「`/etc/host.conf` のパラメータ」(254 ページ) を、`/etc/host.conf` の設定例については 例11.8「`/etc/host.conf`」(255 ページ) をそれぞれお読みください。

表 11.7 `/etc/host.conf` のパラメータ

<code>order hosts, bind</code>	名前解決を行なう場合アクセス順序を指定します。利用可能なパラメータは 下記の通りです (スペースまたはカンマで区切ります):
	<code>hosts</code> : <code>/etc/hosts</code> ファイルを 検索して名前解決を行ないます。
	<code>bind</code> : ネームサーバにアクセスして名前解決を試みます。
	<code>nis</code> : NIS を使用します。
<code>multi on/off</code>	<code>/etc/hosts</code> ファイル内に入力したホストについて、複数の IP アドレスを許すかどうかを設定します。
<code>nospoof on spoofalert on/off</code>	これらのパラメータはネームサーバの 偽装 検知に 影響するパラメータ

	です。ネットワーク設定には影響しません。
trim ドメイン名	ホスト名の解決後、指定したドメイン名をホスト名から取り除くことを指定します (ホスト名にドメイン名が含まれていた場合のみ)。このオプションは /etc/hosts ファイル内にローカルドメインのホスト名 だけが含まれていて、それらを指定したドメイン名として認識したい場合に 指定します。

例 11.8 /etc/host.conf

```
# ネームサーバが起動しています
order hosts bind
# 複数アドレスを有効にする
multi on
```

11.6.1.9 /etc/nsswitch.conf

GNU C ライブラリ 2.0 以降では、*Name Service Switch* (NSS) を利用するようになりました。詳しくは `nsswitch.conf(5)` のマニュアルページや、*GNU C ライブラリ参考文献マニュアル* をお読みください。

問い合わせの順序は `/etc/nsswitch.conf` ファイルで指定します。`nsswitch.conf` の設定例は 例11.9「`/etc/nsswitch.conf`」(255 ページ) にあります。コメントを記入する場合は、コメントの前に `#` を記入してください。この例で `hosts` データベース 内の項目は、名前解決の要求が `DNS` を介して `/etc/hosts (files)` に送信される 設定になっています。

例 11.9 /etc/nsswitch.conf

```
passwd:      compat
group:       compat

hosts:       files dns
networks:    files dns

services:    db files
protocols:   db files
rpc:         files
ethers:      files
netmasks:    files
```

```
netgroup:  files nis
publickey: files

bootparams: files
automount:  files nis
aliases:    files nis
shadow:     compat
```

NSS 上で利用可能なデータベースは、表11.8「/etc/nsswitch.conf から利用できるデータベース」(256 ページ) に一覧で示されています。NSS データベースとして利用可能なオプションは、表11.9「NSS「データベース」の設定オプション」(257 ページ) 内に書かれています。

表 11.8 /etc/nsswitch.conf から利用できるデータベース

aliases	sendmail で実装されているメール別名; 詳しくは man 5 aliases をお読みください。
ethers	イーサネットアドレス。
netmasks	ネットワークの一覧やサブネットマスク。サブネットを設定する場合にのみ必要です。
group	getgrent で使用するユーザグループ。group のマニュアルページも併せてお読みください。
hosts	gethostbyname などの関数で取得できる、ホスト名や IP アドレス。
netgroup	アクセス許可を設定する目的で使用する有効なホストとユーザの一覧; 詳しくは netgroup(5) のマニュアルページをお読みください。
networks	getnetent で使用するネットワーク名とアドレス。
publickey	NFS や NIS+ で使用する、Secure_RPC 用の公開／機密鍵。

passwd	getpwent で使用されるユーザパスワード; 詳しくは passwd(5) のマニュアルページをお読みください。
protocols	getprotoent で使用するネットワークプロトコル; 詳しくは protocols(5) のマニュアルページをお読みください。
rpc	getrpcbyname などの関数で取得できる、リモートプロシージャコール (RPC) の名前とアドレス。
services	getservent で使用するネットワークサービス。
shadow	getspnam で使用するユーザのシャドウパスワード; 詳しくは shadow(5) のマニュアルページをお読みください。

表 11.9 NSS「データベース」の設定オプション

files	ファイルへの直接アクセスを指定します。たとえば /etc/aliases などのファイルにアクセスします。
db	データベース経由でのアクセス。
nis, nisplus	NIS を使用します。詳しくは 第3章 <i>NIS の使用</i> (↑セキュリティガイド)をお読みください。
dns	hosts と networks に対してのみ 設定可能な拡張です。
compat	passwd, shadow, group に対してのみ設定可能な拡張です。

11.6.1.10 /etc/nscd.conf

このファイルは、nscd (name service cache daemon; ネームサービスのキャッシュ デーモン) を設定するために使用します。詳しくは nscd(8) および nscd.conf(5) のマニュアルページをお読みください。既定では、システムの passwd と groups の項目について、nscd でキャッシュを行なう (メモリ上に一時記憶する) よう設定されています。このサービスを利用しないと、NIS や LDAP などのディレクトリサービスを 提供している場合、接続が発生するたびに名前やグループへのアクセスを行なってしまうため、性能面で重要な仕組みになっています。既定では hosts をキャッシュしないように設定されていますが、これは nscd のキャッシュ機能を利用してしまうと、ローカルシステム側から正引きや逆引きの確認が行なえなくなってしまうためです。nscd で名前のキャッシュを行なう代わりに、DNS サーバ側でキャッシュを設定してください。

なお、passwd ファイルをキャッシュするように設定している 場合は、新しいユーザを追加してから認識されるまでに 15 秒ほどの時間がかかります。このような待機時間を減らすには、rcnscd restart コマンドで nscd を再起動してください。

11.6.1.11 /etc/HOSTNAME

このファイルには、ドメイン名を含む完全修飾ホスト名が書かれています。このファイルは、マシンの稼働中に複数のスクリプトから読み取られます。ファイルはホスト名を含む 1 行でなければなりません。

11.6.2 設定のテスト

変更した設定を設定ファイルに書き込む前に、設定をテストすることができます。設定のテストを行なうには、ip コマンドをご利用ください。また、接続のテストを行なうには、ping コマンドをご利用ください。もちろん従来が存在する ifconfig や route コマンドもご利用いただけます。

ip, ifconfig, route の各コマンドは、設定ファイルに保存を行なうことなく、設定そのものを直接 変更するためのコマンドです。適切な設定ファイル内に設定を書き込まない限り、変更した設定はシステムの再起動を行なうことでリセットされてしまいます。

11.6.2.1 ip を利用したネットワークインターフェイスの設定

ip コマンドはネットワークデバイスやルーティングの設定のほか、ポリシールーティングやトンネルを設定したり、設定を閲覧したりするためのツールです。

ip コマンドはとても複雑なツールです。一般的には ip オプション オブジェクト コマンド のような書式で記述します。オブジェクトには下記のことを設定することができます：

link

ネットワークデバイスを表わすオブジェクトです。

address

デバイスの IP アドレスを表わすオブジェクトです。

neighbor

ARP や NDISC キャッシュ項目を表わすオブジェクトです。

route

ルーティングテーブルの項目を表わすオブジェクトです。

rule

ルーティングポリシーデータベース内のルールを表わすオブジェクトです。

maddress

マルチキャストのアドレスを表わすオブジェクトです。

mroute

マルチキャストのルーティングキャッシュの項目を表わすオブジェクトです。

tunnel

IP 経由でのトンネルを表わすオブジェクトです。

コマンドを指定しない場合は、既定のコマンドが指定されたものとして扱われます (通常は list です)。

デバイスの状態を変更するには、ip link set デバイス名 コマンド のように入力します。たとえば eth0 デバイスを無効化したい場合は、ip link set eth0 down と入力します。再度有効化する場合は、ip link set eth0 up と入力してください。

デバイスを有効化したら、次に設定を行ないます。IP アドレスを設定するには、ip addr add IP アドレス + dev デバイス名 のように入力します。たとえば、eth0 インターフェイスに対して 192.168.12.154/30 のアドレスを設定し、標

準のブロードキャストアドレスを設定 (brd オプション) するには、`ip addr add 192.168.12.154/30 brd + dev eth0` と入力します。

接続を行なうことができるようにするためには、さらにデフォルトゲートウェイを設定しなければなりません。お使いのシステムにデフォルトゲートウェイを設定するには、`ip route add` ゲートウェイの IP アドレス のように入力します。また、アドレス変換を行ないたい場合は、`nat` キーワードを指定し、下記のように入力します: `ip route add nat IP アドレス via 他の IP アドレス`

全てのデバイスを表示するには、`ip link ls` と入力してください。稼働中のインターフェイスのみを表示する場合は `ip link ls up` を、デバイスごとのインターフェイス統計情報を表示するには、`ip -s link ls` デバイス名 のように入力してください。また、お使いのデバイスに設定したアドレスを確認するには、`ip addr` コマンドを使用します。`ip addr` コマンドでは、MAC アドレスの情報も表示されます。さらに、全ての経路情報を表示するには、`ip route show` コマンドをご利用ください。

上記以外にも `ip` コマンドには様々な機能が備わっています。`ip` コマンドについてさらに詳しい情報は、`ip help` と入力するか、もしくは `ip(8)` のマニュアルページをお読みください。なお、`help` オプションは `ip` のサブコマンドに対しても動作します。たとえば `ip addr` コマンドの使い方について知りたい場合は、`ip addr help` と入力してください。`ip` コマンドのマニュアルは、`/usr/share/doc/packages/iproute2/ip-cref.pdf` にもあります。

11.6.2.2 ping を利用した接続テスト

`ping` コマンドは TCP/IP 接続が正しく動作するかどうかをテストするための標準ツールです。本コマンドは ICMP と呼ばれるプロトコルを利用し、`ECHO_REQUEST` と呼ばれる小さなデータを宛先のホストに送信し、即時の応答を求めます。うまく動作すれば `ping` コマンドはその結果を表示し、ネットワークの接続の基本部分が正しく動作していることを表わします。

また、`ping` コマンドは 2 台のコンピュータ間での接続テストを行なうだけではありません。本コマンドは接続品質に関する基本情報も提供します。例 11.10「`ping` コマンドの出力」(261 ページ) に示している例は、`ping` コマンドの出力例です。最後から 2 行目の部分には、送信されたパケット数と損失数、および `ping` コマンドの実行時間が表示されています。

また、本コマンドで指定する宛先には IP アドレスだけでなくホスト名を指定することもできます。たとえば `ping example.com` や `ping 192.168.3.100` のように入力することができます。なお、本コマンドは `Ctrl + C` を押すまでパケットを送信し続けます。

基本的な接続確認だけを行ないたい場合は、`-c` オプションを 設定して送信数を制限することもできます。たとえば 3 パケットだけ送信したい 場合は、`ping -c 3 example.com` のように入力してください。

例 11.10 `ping` コマンドの出力

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): 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
```

既定のパケット送信間隔は 1 秒に設定されています。この送信間隔を変更 するには、`-i` オプションを指定してください。たとえば 10 秒間隔で送信する場合は、`ping -i 10 example.com` のように入力します。

また、複数のネットワークデバイスを利用している場合は、`ping` コマンドに 対して特定のインターフェイスアドレスを利用するように指定したほうが便利 である場合があります。このような場合は、`-I` オプション でインターフェイス名を指定してください。たとえば `ping -I wlan1 example.com` のように入力します。

`ping` コマンドについてさらに詳しい情報については、`ping -h` で出力されるヘルプ か、もしくは `ping (8)` のマニュアルページをお読みください。

ヒント: IPv6 アドレスに対する `ping`

IPv6 アドレスの場合は `ping6` コマンドを使用します。なお、リンクローカルア ドレスに対して `ping` を送信する場合は、`-I` オプションを利用してインターフェイスを 指定しなければなりません。たとえば 下記のコマンドでは、`eth1` を介して指定し たアドレスに 通信ができるかどうかを確認します:

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

11.6.2.3 `ifconfig` を利用したネットワーク設定

`ifconfig` コマンドは、ネットワークを設定するための ツールです。

注記: `ifconfig` コマンドと `ip` コマンド

`ifconfig` プログラムは古いソフトウェアです。できる限り `ip` コマンドをご利用く ださい。また、`ip` コマンドと比べると `ifconfig` はインターフェイスの 設定しか行 ないことができません。また、インターフェイス名は 9 文字までに 限定されます。

パラメータを何も指定しない場合、ifconfig は現在有効に 設定されているインターフェイスの状態を表示します。出力例は 例11.11「ifconfig コマンドの出力例」(262 ページ) の通りです。ifconfig は詳細な情報をうまく整理して出力します。また出力の最初の行には、お使いの デバイスに対する MAC アドレス (HWaddr) が含まれます。

例 11.11 ifconfig コマンドの出力例

```
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 を利用するにあたっての詳しいオプション設定などの情報は、ifconfig -h と入力して表示 することのできるヘルプか、もしくは ifconfig (8) のマニュアルページをお読みください。

11.6.2.4 route を利用したルーティング設定

route コマンドは、IP ルーティング (経路制御) テーブルを操作するためのプログラムです。ルーティング情報を閲覧することができのほか、追加や削除を行なうこともできます。

注記: route コマンドと ip コマンド

route プログラムは古いソフトウェアです。できる限り ip コマンドをご利用ください。

route は、ルーティング関連の問題が発生した場合に、ルーティング設定に関する情報を素早く確実に得るには便利なツールです。現在のルーティング情報を閲覧するには、root から route-n と入力します。

例 11.12 route -n コマンドの出力例

```
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 を利用するにあたっての詳しいオプション設定などの情報は、route -h と入力して表示 することのできるヘルプか、もしくは route (8) のマニュアルページをお読みください。

11.6.3 起動時のスクリプト

上記までの章で説明した設定ファイルのほかに、マシンを起動する際に ネットワークプログラムを読み込むための各種スクリプトが存在します。これらのスクリプトは、システムが マルチユーザのランレベル のいずれかに移行すると、すぐに実行されるものです。これらのスクリプトのうち、いくつかを 表11.10「ネットワークプログラムのスクリプト」(263 ページ) で説明します。

表 11.10 ネットワークプログラムのスクリプト

/etc/init.d/network	このスクリプトは、ネットワークインターフェイスの設定を処理するためのものです。network サービスが開始されなかった場合、ネットワークインターフェイスは利用できなくなります。
/etc/init.d/xinetd	このスクリプトは、xinetd を起動するためのものです。xinetd はシステ

	ム上でサービスを提供するための使用されるプログラムで、たとえば FTP の接続があった場合に vsftpd を起動したりすることができます。
<code>/etc/init.d/rpcbind</code>	このスクリプトは、RPC プログラム番号をユニバーサルアドレスに変換する rpcbind ユーティリティを起動するためのものです。NFS サーバなどの RPC サービスで必要になります。
<code>/etc/init.d/nfsserver</code>	このスクリプトは、NFS サーバを起動するためのものです。
<code>/etc/init.d/postfix</code>	このスクリプトは、postfix プロセスを制御するためのものです。
<code>/etc/init.d/ypserv</code>	このスクリプトは、NIS サーバを起動するためのものです。
<code>/etc/init.d/ypbind</code>	このスクリプトは、NIS クライアントを起動するためのものです。

11.7 ダイアルアップ接続支援としての smpppd

ホームユーザの場合、インターネットに対する専用の回線を持っておらず、ダイアルアップ接続を利用している場合があります。ダイアルアップの方式 (ISDN や DSL) によって、接続を `ipppd` で操作するのか `pppd` で操作するのかが変わります。基本的にはインターネット接続を行なうのに必要なものは、これらのツールが全てです。

ダイアルアップ接続を行なうのに追加の料金がかからない固定料金制の接続をご利用の場合は、単に関連するデーモンを起動するだけです。デスクトップのアプレットや コマンドラインインターフェイスを利用してダイアルアップ接続を制御してください。

い。インターネットのゲートウェイが今現在使用中のホストとは異なるものであったりする場合は、ネットワークホストを経由してダイヤルアップ接続を利用することもできます。

こういう場合に smpppd (SUSE Meta PPP Daemon) が役に立ちます。smpppd は補助 プログラムに対する統一インターフェイスとして動作し、双方向の仲介を行いません。smpppd では、pppd と ipppd のどちらを利用するのかを判断し、ダイヤルアップ接続の 操作を行いません。また、ユーザプログラムに対して様々なプロバイダが利用できるよう 情報を提供するほか、接続状態についての情報を送信することもできます。smpppd はネットワーク経由でもコントロールできますので、プライベートなサブネット内に 存在する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を コントロールする場合に便利です。

11.7.1 smpppd の設定

smpppd が提供する接続は、YaST から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 についても設定が行なわれます。リモートコントロールなど、smpppd の追加機能を利用する場合にのみ、手動設定が必要となります。

smpppd の設定ファイルは /etc/smpppd.conf にあります。既定ではリモートコントロールは無効に設定されています。この設定ファイルで最も 重要なオプションは、下記の通りです:

`open-inet-socket = yes/no`

smpppd をネットワーク経由で操作させたい場合は、このオプションを yes に設定してください。smpppd はポート 3185 で待ち受けます。このパラメータを yes に設定する場合は、bind-address, host-range, password についてもそれぞれ設定を行なってください。

`bind-address = ip アドレス`

ホストに複数の IP アドレスが設定されている場合は、このパラメータを利用して smpppd が受け付ける IP アドレスを指定します。既定では全てのアドレス宛の 接続を受け付けます。

`host-range = 最小 IP最大 IP`

host-range パラメータでは、ネットワークの範囲を指定 します。smpppd では、指定した範囲の中にある IP アドレスからの接続だけを 受け入れます。範囲外のアドレスからのアクセスは全て拒否されます。

password = パスワード

パスワードを割り当てると、ネットワーク経由での操作を行なうのにパスワードを入力しなければならなくなります。ただしここで指定するパスワードには何も暗号化を行わないため、設定しないよりは良い、程度のものだとお考えください。何もパスワードを指定しないと、全てのクライアントから smpppd にアクセスできるようになります。

slp-register = *yes/no*

このパラメータを設定すると、smpppd サービスは SLP を介してアナウンスされるようになります。

smpppd についてさらに詳しい情報については、smpppd(8) や smpppd.conf(5) のマニュアルページをお読みください。

11.7.2 リモートで使用するための qinternet の設定

qinternet は、ローカルやリモートの smpppd を操作することができます。cinternet はコマンドラインツールで、KInternet はグラフィカルなツールです。これらのユーティリティをリモートの smpppd に対して使用するには、設定ファイル /etc/smpppd-c.conf を手作業で編集するか、もしくは qinternet を使用する必要があります。このファイルには 4 つのオプションだけがあります：

sites = サイトの一覧

フロントエンドが smpppd を検索する際に利用する、*サイトの一覧* を指定します。フロントエンドは、ここで指定した順序どおりにオプションを試します。local を指定するとローカルの smpppd に対して接続を行なう指定となるほか、gateway を指定するとゲートウェイ上の smpppd に対して接続を行なおうとします。config-file を指定すると、それぞれ /etc/smpppd-c.conf で指定する server と port の設定に従って接続を行ないます。slp を指定すると、SLP 経由で smpppd を見つけるようになります。

server = サーバ

smpppd が動作しているホストを指定します。

port = ポート

smpppd が動作しているポートを指定します。

password = パスワード

smpppd に接続するためのパスワードを指定します。

ネットワーク内の SLP サービス

service location protocol (SLP) は、ローカル ネットワーク内にあるクライアントに対して設定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、必要となる様々なサービスを含め、従来は管理者に対してネットワーク内のサーバについての詳しい知識が求められて きました。SLP は特定のサービスが提供されていることを、ローカルネットワーク 内の全てのクライアントに対して通知します。SLP に対応したアプリケーションは、配布された情報を利用してサービスにアクセスできるようになり、自動で設定したり することもできるようになります。

openSUSE® では SLP 経由で通知されたインストール元からのインストールに 対応しているほか、SLP に対応した多くのシステムサービスが含まれています。また、YaST や Konqueror では SLP のフロントエンドも提供されています。お使いのシステム内にあるインストールサーバやファイルサーバ、印刷サーバなど 集中型の機能について、ネットワーク対応のクライアントに SLP 経由で通知して 使用してもらうように設定することもできます。

重要: openSUSE での SLP サポート

SLP に対応するサービスには、cupsd, rsyncd, ypserv, openldap2, ksysguardd, saned, kdm, vnc, login, smpppd, rpasswd, postfix, sshd (fish 経由) があります。

12.1 インストール

SLP サービスを利用するのに必要な全てのパッケージは、既定でインストールされるようになっています。逆に SLP を介してサービスを提供したい場合は、`openslp-`

server 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。また、SLP のデーモンのサーバ設定を行なうには、yast2-slp-server パッケージをインストールしてください。

12.2 SLP の有効化

SLP でサービスを公開するには、お使いのシステムで slpd を実行しなければなりません。お使いのマシンがクライアントとしてのみ動作するもので、サービスの提供を行わない場合は、slpd を実行する必要はありません。openSUSE での多くのサービスのように、slpd デーモンは個別の init スクリプト経由で起動および停止することができます。インストール後、何も設定しない 場合はサービスは起動しません。一時的に有効化したい場合は、root で rcslpd start と入力すると起動を行なうことができますし、rcslpd stop と入力すると停止することができます。それ以外にも、再起動や状態チェックを restart や status で行なうことができます。起動時に slpd を常に開始させたい場合は、YaST から システム > システム サービス (ランレベル) を選択して slpd を有効にするか、もしくは root で insserv slpd コマンドを実行してください。

12.3 openSUSE での SLP フロントエンド

お使いのネットワーク内で提供されているサービスを SLP 経由で見つけるには、slptool (openslp パッケージ) のような SLP フロントエンドを利用するか、もしくは YaST を利用します:

slptool

slptool はコマンドラインプログラムで、ネットワーク内に対して SLP の問い合わせを投げたり、独自のサービスをアナウンスしたりすることができます。slptool --help のように実行すると、利用可能なオプションと機能を表示することができます。たとえば現在のネットワークで、自分自身の存在をアナウンスしている ネットワーク時刻サーバを見つけるには、下記のように入力します:

```
slptool findsrvs service:ntp
```

YaST

YaST でも SLP ブラウザを利用することができます。ただしこのブラウザは YaST のコントロールセンターの一覧には用意されていません。この YaST モ

ジョーブルを起動するには、root で `yast2 slp` と入力してください。左側にあるサービス種類の項目を選択すると、サービスに関するさらに詳しい情報を得ることができます。

12.4 SLP 経由でのインストール

openSUSE のインストールメディアを利用して、お使いのネットワーク内に インストールサーバを立ち上げたい場合は、SLP で登録および提供することができます。詳しくは 2.2 項「インストール元のデータを保存するサーバの構築」(48 ページ)をお読みください。選択した起動メディアからシステムを起動し、SLP インストールを選択すると、linuxrc は SLP の問い合わせを行なって見つかったソースを表示します。

12.5 SLP 経由でのサービス提供

openSUSE 内の多くのアプリケーションは、`libslp` を使用することで SLP に対応しています。あるサービスについて SLP に対応したコンパイルが行なわれていない場合は、下記のいずれかの方法で SLP 対応にすることができます：

`/etc/slp.reg.d` への手動登録

それぞれ新しいサービスに対して、個別の登録ファイルを作成するやり方です。下記はスキャナサービスを登録するためのファイル例です：

```
## このシステムにある saned サービスを登録します。
## en は英語という意味です。
## 65535 はタイムアウトを無効にするための指定で、サービスの登録時には更新を
## 必要としない意味になります。
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:` で始まる サービス URL の行です。この行にはまず、サービスの種類 (`scanner, sane`) と、サービスを利用できるアドレスが書かれています。なお、`$HOSTNAME` は自動的に自身の完全修飾ホスト名に置き換えられます。また、コロン (`:`) で区切ってサービスを提供している TCP ポートの名前を入力することもできます。あとの項目はサービスで使用されている言語と登録間隔 (秒単位) が書かれています。サービス URL との区切りは、それぞれカンマを使用します。登録間隔は 0 から 65535 までの間で、0 を指定すると登録を行なわない意味になり、65535 を指定すると全ての制限を取り除く意味になります。

また、登録ファイルには watch-port-tcp と description の項目も書かれています。watch-port-tcp は SLP サービスアナウンスと 関連するサービスの有効性をつなげるもので、このポートに接続可能かどうかで サービスが提供されているかどうかを確認します。もう 1 つの項目はサービスに 対する詳しい説明を書くための項目で、ブラウザを利用することで表示することの できる項目です。

/etc/slp.reg への手動登録

この登録と /etc/slp.reg.d での登録との違いは、全てのサービスが単一のファイルに書かれているという点です。

slptool を利用した動的な登録

あるサービスについて、設定ファイル無しで動的に登録する必要がある場合は、slptool コマンドラインユーティリティを使用するのがよいでしょう。同じツールを利用することで、slpd の再起動を行なうことなく既存のサービスを 削除することができます。

12.6 さらなる情報

RFC 2608, 2609, 2610

RFC 2608 では一般的な SLP の定義について記述しています。RFC 2609 では サービス URL についてさらに詳しい文法を説明しているほか、RFC 2610 では SLP 経由での DHCP について扱っています。

<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、openslp-server パッケージに 添付されているドキュメンテーションのほか、README.SuSE ファイルとして openSUSE での詳細や RFC、2 種類の入門 HTML 文書が 配置されます。SLP の機能を使用したいプログラマの場合は、openslp-devel パッケージに 含まれる “プログラマーズガイド” をお読みになるのが よいでしょう。

ドメインネームシステム

DNS (ドメインネームシステム) はドメイン名やホスト名を IP アドレスに変換するのに必要なサービスです。この方法により、たとえば 192.168.2.100 は jupiter というホスト名と対応づけることができます。独自のネームサーバを設定する前に、11.3項「名前解決」(221 ページ) に示されている DNS に関する一般情報をお読みください。また、下記の設定例では BIND を利用しています。

13.1 DNS 用語

ゾーン

ドメインの名前領域は、ゾーンと呼ばれる部分に分割されています。たとえば example.com というドメインでは、com と呼ばれるドメイン内の example という部分 (ゾーン) を示していることになります。

DNS サーバ

DNS サーバは、それぞれのドメインに対して、その名前と IP アドレスの情報を保持しているサーバです。マスターゾーンとしてプライマリ DNS サーバを、スレーブゾーンとしてセカンダリ DNS サーバを持つことができるほか、ゾーンを持たないキャッシュ専用のスレーブサーバを持つこともできます。

マスターゾーンの DNS サーバ

マスターゾーンには、お使いのネットワークに関する全ての情報が含まれていて、ドメインに対する全ホストに関する最新情報が保存されています。

スレーブゾーンの DNS サーバ

スレーブゾーンはマスターゾーンのコピーです。スレーブゾーンの DNS サーバは、マスターサーバからゾーン転送処理を通して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、そのゾーンデータが有効である限り (有効期限が 切れない限り)、そのゾーンに対して権威のある (authoritative な) 応答を 返却します。スレーブはそのゾーンデータの最新情報が得られない場合、そのゾーンに対する応答を停止します。

フォワーダ

フォワーダとは、お使いの DNS サーバが応答のできない場合に問い合わせを転送する先のことを言います。1 つの設定で複数の設定ソースを指定するには、netconfig を使用します (詳しくは `man 8 netconfig` をお読みください)。

レコード

レコードとは名前や IP アドレスに関する情報のことを言います。それぞれ対応しているレコードとその文法については、BIND のドキュメンテーションに 書かれています。また、下記のような特殊なレコードがあります:

NS レコード

NS レコードとは、指定したドメイン名を担当するネームサーバのマシンがどこにあるのかを知らせるためのものです。

MX レコード

MX (メールエクスチェンジ) レコードとは、インターネットを介して直接 メールをやりとりする場合に使用する、通信相手のマシンを教えるための ものです。

SOA レコード

SOA (権威の開始) レコードとは、ゾーンファイルの最初のレコードです。SOA レコードは、DNS を通じて複数のコンピュータ間でデータを同期する場合に利用します。

13.2 インストール

DNS サーバをインストールするには、YaST を起動して **ソフトウェア > ソフトウェア管理** を選択します。そこからさらに **ビュー > パターン** を選択し、*DHCP and DNS Server* を選択してください。あとはインストール処理を完了するため、個別のパッケージのインストールについて確認を行なってください。

13.3 YaST を利用した設定

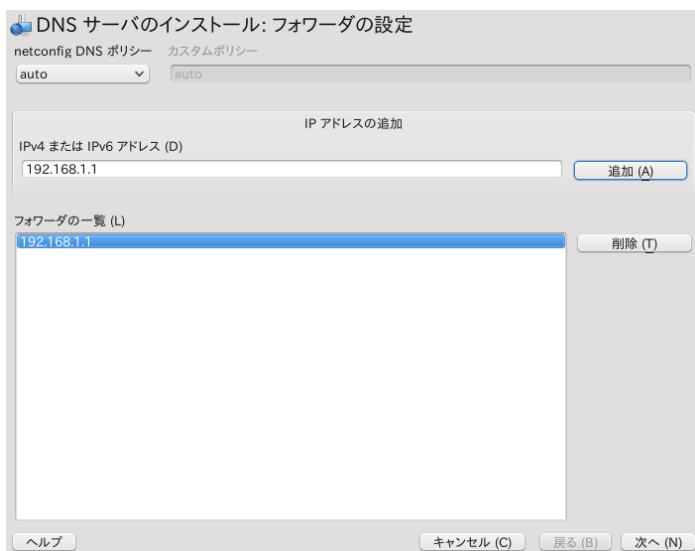
YaST DNS モジュールを利用することで、お使いのローカルネットワークに対する DNS サーバの設定を行なうことができます。最初にモジュールを起動したときにはウィザードが起動し、サーバを起動するにあたっていくつか決めておかねばならない基本設定について質問が行なわれます。この初期設定作業はサーバの基本的な設定を行なうもので、アクセス制御 (ACL) やログ記録、TSIG 鍵のオプションなど、高度な設定作業については、熟練者モードをご利用ください。

13.3.1 ウィザードによる設定

ウィザードは 3 段階の手順 (ダイアログ) から構成されています。それぞれダイアログ内の適切な箇所から、熟練者モードに入ることができます。

- 1 最初にモジュールを起動したときには、図13.1「DNS サーバのインストール: フォワーダの設定」(273 ページ) に示されている *フォワーダ設定* の画面が開きます。*netconfig DNS* ポリシーでは、どのデバイスから フォワーダにアクセスするかを設定できるほか、*フォワーダの一覧* から独自の一覧を設定することもできます。*netconfig* について詳しくは、`man 8 netconfig` で表示されるマニュアルページをお読みください。

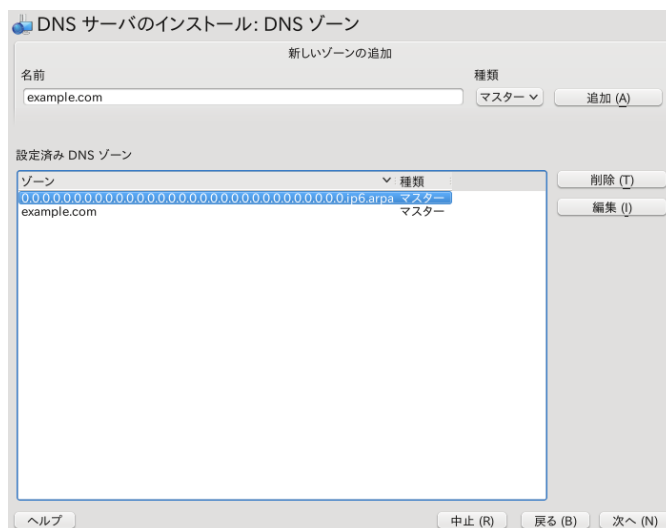
図 13.1 DNS サーバのインストール: フォワーダの設定



フォワーダとは、お使いの DNS サーバが問い合わせを送信する先のことで、自分自身では解決できない問い合わせの場合に利用します。フォワーダの IP アドレスを入力してから **追加** を押してください。

- 2 次の DNS ゾーン ダイアログは 13.6 項「ゾーンファイル」(287 ページ)にあるとおり複数のパーツから構成され、ゾーンファイルの管理について設定を行います。新しいゾーンを作成するには、**名前** に名前を入力してください。逆引きゾーンを追加する場合、名前は `.in-addr.arpa` で終わらなければなりません。最後に **種類** (マスター、スレーブ、転送のいずれか) を選択してください。詳しくは 図13.2「DNS サーバのインストール: DNS ゾーン」(274 ページ)をお読みください。既存のゾーンについてその他の設定を変更するには、設定済み DNS ゾーンから選択して、**編集** ボタンを押してください。ゾーンを削除するには同じくゾーンを選択してから **削除** ボタンを押してください。

図 13.2 DNS サーバのインストール: DNS ゾーン



- 3 最後のダイアログでは、**ファイアウォールでポートを開く** を選択することでファイアウォール内の DNS ポートを開くように設定することができます。また、DNS サーバをシステム起動時に開始するかどうか (**オン** または **オフ**) を選択することもできます。またそれ以外にも、LDAP に対応するよう設定することもできます。詳しくは 図13.3「DNS サーバのインストール: ウィザードの完了」(275 ページ)をご覧ください。

13.3.2.2 フォワーダ

お使いの DNS サーバが要求に応答できない場合、フォワーダで設定した転送先に対して要求を転送します。フォワーダの一覧に手動で追加してください。ダイヤルアップ接続のなどのようにフォワーダが随時 変わるような場合は、*netconfig* が設定を扱います。*netconfig* について、詳しくは `man 8 netconfig` で表示されるマニュアルページをお読みください。

13.3.2.3 基本オプション

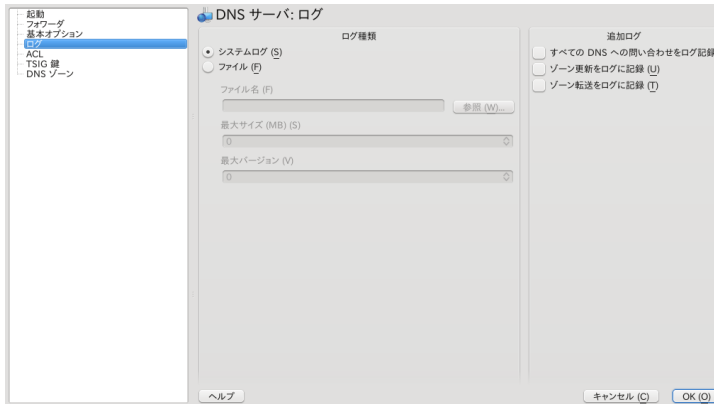
このセクションでは、サーバに対する基本的な設定を行ないます。オプションメニュー内から設定したい項目を選び、必要な 値を設定してください。追加 ボタンを押すと新しい項目を追加することができます。

13.3.2.4 ログ

DNS サーバのログ機能について、何を採取するのか、どのように採取するのかをログから設定します。ログ種類では、DNS サーバがログデータをどこに書き込むのかを設定します。`/var/log/messages` のようなシステム全体のログに対して記録を行なうにはシステムログを、個別のファイルに保存するにはファイルを選択します。後者の場合はログファイル名とメガバイト単位での最大サイズ、および保存する過去ログの最大数をそれぞれ指定してください。

さらなるオプション設定は、追加ログから利用できます。すべての DNS への問い合わせをログ記録を選択すると、それぞれの問い合わせに対し、ログ記録を行なうようになります。ログファイルは非常に大きいものになるため、デバッグ目的以外の使用は適切とは言えません。また、DHCP サーバや DNS サーバの間でのゾーン更新トラフィックを記録するには、ゾーン更新をログに記録を選択してください。また、マスターサーバからスレーブサーバに対して行なわれたゾーン転送トラフィックを記録するには、ゾーン転送をログに記録を選択してください。詳しくは 図 13.4「DNS サーバ: ログ」(277 ページ) をご覧ください。

図 13.4 DNS サーバ: ログ



13.3.2.5 ACL

このダイアログでは、ACL (アクセス制御リスト) を設定し、アクセスに対する制限を設定することができます。それぞれ固有の *名前* を設定したあと、*値* IP アドレス (ネットマスク付き、または単独) の欄に下記の形式で入力します:

```
{ 192.168.1/24; }
```

設定ファイルの書式仕様により、アドレスはセミコロン (;) で終わり、かつ 中括弧でくくる必要があります。

13.3.2.6 TSIG 鍵

TSIG (トランザクション署名) の主な目的は、DHCP や DNS サーバ間での通信について、機密を保持することにあります。詳しい説明は 13.8 項「機密を保持する通信」(292 ページ) で行なっています。

TSIG 鍵を生成するには、*鍵 ID* の欄に固有の名前を入力し、保存先のファイル名 (*ファイル名*) を指定します。最後に *生成* を押すと鍵が生成されます。

以前に作成した鍵を使用するには、*鍵 ID* の項目に何も記入しない状態で、鍵ファイルが保存されている場所を *ファイル名* で指定します。最後に *追加* を押すと追加することができます。

13.3.2.7 DNS ゾーン (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* ゾーンを選んでから ゾーン種類として *スレーブ* を選択し、ゾーンの名前を入力してから *追加* を押します。

ゾーンエディタ のサブダイアログでは、マスター *DNS* サーバの *IP* を指定し、どのサーバからデータを取得するかを 設定してください。また、サーバに対するアクセスを制限するには、ACL の一覧から それぞれ選択してください。

13.3.2.8 DNS ゾーン (マスターゾーンの追加)

マスターゾーンを追加するには、*DNS* ゾーンを選んでから ゾーン種類として *マスター* を選択し、ゾーンの名前を入力してから *追加* を押します。マスターゾーンを追加する場合は、それら対応する逆引きゾーンも必要です。たとえば 192.168.1.0/24 というサブネット内にあるホストを示す example.com というドメインを追加する場合は、それらの IP アドレス範囲をカバーする逆引きゾーンを追加する必要があります。たとえば 1.168.192.in-addr.arpa のように 設定します。

13.3.2.9 DNS ゾーン (マスターゾーンの編集)

マスターゾーンを編集するには、*DNS* ゾーンを選んでから 一覧内のマスターゾーンのいずれかを選択し、*編集* を押します。表示されるダイアログにはいくつかのページが含まれます: *基本* (最初に表示されるページ)、*NS* レコード、*MX* レコード、*SOA*、*レコード* があります。

図13.5「DNS サーバ: ゾーンエディタ (基本)」(279 ページ) で示されている基本ダイアログでは、動的 DNS とクライアントに対するゾーン転送のアクセスオプション、および スレーブのネームサーバを設定することができます。ゾーンに対して動的な更新を許可するには、*動的な更新の許可* を選択して関連する TSIG 鍵を選んでください。この鍵は更新動作が始まる前までに設定しておかなければなりません。ゾーン転送を許可するには、必要な ACL をを選んでください。この段階までに ACL を設定しておかなければなりません。

基本 ダイアログでは、ゾーン転送を有効にするかどうかを 指定します。また、どのホストからゾーンをダウンロードできるかを ACL で指定します。

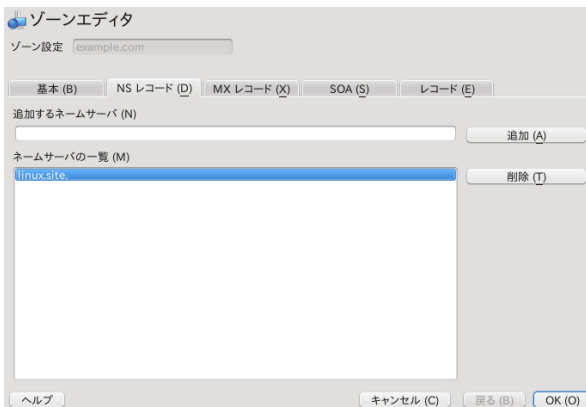
図 13.5 DNS サーバ: ゾーンエディタ (基本)



ゾーンエディタ (NS レコード)

NS レコード ダイアログでは、指定したゾーンに対する 代替のネームサーバを設定することができます。一覧内にはご自身が管理される ネームサーバだけが含まれていることをご確認ください。レコードを追加するには、**追加するネームサーバ** の欄にアドレスを入力し、**追加** を押します。詳しくは 図13.6「DNS サーバ: ゾーンエディタ (NS レコード)」(279 ページ) をご覧ください。

図 13.6 DNS サーバ: ゾーンエディタ (NS レコード)



ゾーンエディタ (MX レコード)

現在のゾーンに対してメールサーバを一覧に追加するには、まずそれぞれ適切な アドレスと値を入力します。入力を行なったら **追加** を押します。詳しくは 図

13.7「DNS サーバ: ゾーンエディタ (MX レコード)」(280 ページ) をご覧ください。

図 13.7 DNS サーバ: ゾーンエディタ (MX レコード)

ゾーンエディタ
ゾーン設定 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)

0 追加 (A)

メール中継一覧

メールサーバ ▼ 優先度

削除 (T)

ヘルプ キャンセル (C) 戻る (B) OK (O)

ゾーンエディタ (SOA)

このページでは、SOA (権威の開始) レコードを作成することができます。各オプションについての説明は、例13.6「/var/lib/named/example.com.zone ファイル」(287 ページ) をお読みください。

図 13.8 DNS サーバ: ゾーンエディタ (SOA)

ゾーンエディタ
ゾーン設定 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 (F) 単位 (I)

2010121802 3 時間 ▼

TTL (L) 再試行間隔 (Y) 単位 (U)

2 1 時間 ▼

有効期限 (P) 単位 (N)

1 週 ▼

最小値 (M) 単位 (T)

1 日 ▼

ヘルプ キャンセル (C) 戻る (B) OK (O)

ゾーンエディタ (レコード)

このダイアログでは、名前解決の管理を行ないます。*レコードキー* にホスト名を入力し、種類を選択してください。*A レコード* を主に設定します。この場合、値には IP アドレスを入力します。また、*CNAME* では別名を指定します。なお、*NS* や *MX* の各レコードについては、それぞれ *NS レコード* や *MX レコード* で設定した情報について、より詳細な設定を行なったり、部分的に修正したりする場合にお使いください。これら 3 種類のレコードでは、いずれも既存の *A レコード* を参照します。また、*PTR* は逆引きゾーンを表わします。これは *A レコード* の逆を意味するもので、たとえば下記のように なります:

```
hostname.example.com. IN A 192.168.0.1
1.0.168.192.in-addr.arpa IN PTR hostname.example.com.
```

注記: 逆引きゾーンの編集

正引きゾーンを追加したあと、メインメニューに戻ってから編集したい逆引きゾーンを選択して *基本* タブを表示すると、*以下のものから自動的にレコードを生成* チェックボックスを利用することができるようになります。このチェックボックスを選択してゾーンを選択すると、自動的に逆引きゾーンを生成することができます。この方法を利用すると、正引きゾーンを書き換えるだけで自動的に逆引きゾーンにも反映されるようになります。

13.4 BIND ネームサーバの起動

openSUSE® システムでは、ネームサーバ BIND (*Berkeley Internet Name Domain*) が事前構築される形で提供されていて、インストールを行なうだけですぐに動作するようになっています。そのため、インターネット接続を利用できる環境であれば、ネームサーバを設定したあと、ネームサーバのアドレスに 127.0.0.1 (つまり localhost) を指定すれば、プロバイダから DNS サーバの情報を得ることなく名前解決ができることを示しています。この場合、BIND はルートネームサーバから名前解決を行なおうとするため、著しく動作が遅くなってしまいます。通常の運用であれば /etc/named.conf 内の forwarders 設定に対してプロバイダのネームサーバを設定して効率を高めますが、このような方法で名前解決を行なう場合、そのネームサーバはそのゾーンに対し、純粋な *キャッシュのみ* のネームサーバとして動作することになります。設定例はドキュメンテーション /usr/share/doc/packages/bind/config をお読みください。

ヒント: 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種類によっては、ネームサーバの情報を自動的に現在の状況に合わせることができます。これを

行なうには、`/etc/sysconfig/network/config` ファイル内にある `MODIFY_NAMED_CONF_DYNAMICALY` 変数を `auto` に設定してください。

ただし、責任ある団体でドメインが割り当てられない限りは、公式なドメインを設定してはなりません。独自のドメインをお持ちの場合で、それがプロバイダ側の管理下にあるものであっても使用しないほうがお勧めです。使用してしまうと、BIND は 要求を転送してしまうためです。たとえばプロバイダ内の Web サーバなどから、このドメインにアクセスできなくなってしまうです。

ネームサーバを開始するには、`root` ユーザから `named start` コマンドを実行します。右側に緑色で「done」と表示されれば `named` (ネームサーバのプロセス) は正しく起動したことを示します。起動後は `host` プログラムや `dig` プログラムを利用してローカルシステムからネームサーバの動作テストを行なうことができます。既定のサーバに対して `localhost` を問い合わせ、`127.0.0.1` が返却されれば成功です。応答が返されなかったり、正しいアドレスになっていなかったりした場合は、`/etc/resolv.conf` に正しいネームサーバのアドレスが書かれていないか、もしくは全く設定されていないことが考えられます。まずは最初のテストとして `host 127.0.0.1` と入力してみてください。このコマンドは設定にかかわらず常に成功すべきものであるため、これがエラーになるようであれば、まず `named status` を実行してサーバが実際に動作しているかどうかを確認してください。ネームサーバが起動してなかったり、期待通りの動作をしていなかったりした場合は、`/var/log/messages` ファイルから原因を調査してください。

プロバイダが提供するネームサーバで転送機能が提供されている場合は (もしくはお使いのネットワークで転送機能の利用できるネームサーバが動作している場合は)、`options` セクション内の `forwarders` に、それらの IP アドレスを入力してください。例13.1「`named.conf` 内の転送設定」(282 ページ) に例を示します。お使いの環境でそれぞれアドレス設定を変えてお使いください。

例 13.1 `named.conf` 内の転送設定

```
options {
    directory "/var/lib/named";
    forwarders { 10.11.12.13; 10.11.12.14; };
    listen-on { 127.0.0.1; 192.168.1.116; };
    allow-query { 127/8; 192.168/16 };
    notify no;
};
```

`options` 項目は `localhost` や `0.0.127.in-addr.arpa` のゾーン項目の後に続く項目です。「`.`」に対する `type hint` の項目も存在すべき項目です。それぞれのファイルをわざわざ編集する必要はなく、そのままの形で動作するはずでです。また、各項目の行末に「`;`」が付けられていることと、適切な箇所に中括弧が入っていることも

あわせてご確認ください。設定ファイル `/etc/named.conf` やゾーンファイルを編集したら、`rndc reload` コマンドで BIND に対して設定を読み直すように指示してください。サーバを再起動することでも同じことを行なうことができます。再起動を行なうには `rndc restart` コマンドを入力してください。また、サーバを停止するには、`rndc stop` と入力します。

13.5 `/etc/named.conf` 設定ファイル

BIND ネームサーバに対する全ての設定は、`/etc/named.conf` ファイル内に保存されます。ただし、応答を返すべきドメインに対するゾーンデータ (ホスト名や IP アドレスなど) については、`/var/lib/named` ディレクトリ内にある個別のファイルに保存します。ゾーンファイルについての詳細は 後述します。

`/etc/named.conf` ファイルは大きく分けて 2 つの領域に 分かれています。1 つは `options` セクションで 一般的な設定を行ない、もう 1 つは `zone` セクションでドメインごとの設定を行ないます。`logging` セクションや `acl` (アクセス制御リスト) のセクションは 必要に応じて指定します。コメント行は `#` から書き始めるか、もしくは `//` から書き始めます。`/etc/named.conf` の最小限の設定は、例13.2「`/etc/named.conf` の基本設定」(283 ページ) に示しているとおりです。

例 13.2 `/etc/named.conf` の基本設定

```
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";
};
```

13.5.1 重要な設定オプション

directory "ファイル名";

BIND がゾーンデータを見つける際に利用するディレクトリを指定します。通常、この値は /var/lib/named に設定します。

forwarders { *IP アドレス*; };

自分自身で直接解決できない場合に、DNS の要求を転送する先になる ネームサーバ (一般にプロバイダ提供のネームサーバ) を指定します。*IP アドレス* の欄には、192.168.1.116 のように設定してください。

forward first;

DNS 要求に対して、ルートネームサーバ経由での解決を行なう前に転送を試すように指示します。forward first の代わりに forward only と設定すると、全ての要求をルートネームサーバに送信せず、転送ようになります。ファイアウォールの設定を行なう場合に意味のある項目です。

listen-on port 53 { 127.0.0.1; *ip-address*; };

BIND に対して、どのインターフェイスとポートでアクセスを待ち受けるのかを指定します。port 53 については既定のポートであるため、明示的に指定する必要はありません。また、127.0.0.1 と指定すると、ローカルホストからの要求だけを許可ようになります。この項目を設定しない場合は、既定で全てのインターフェイスを待ち受けます。

listen-on-v6 port 53 {any; };

BIND に対して、IPv6 クライアントからの要求を処理するように指定します。any 以外には none しか指定できません。IPv6 に関しては、全アドレスからのアクセスを受け付ける ことになります。

query-source address * port 53;

このオプションは、ファイアウォールによって外向きの DNS 要求がブロック されてしまう場合に必要な設定です。上記の設定では、BIND の要求をポート 53 から行ない、1024 以上のポートを使用しないように指定しています。

query-source-v6 address * port 53;

IPv6 での問い合わせ時に使用するポートを設定します。

allow-query { 127.0.0.1; ネットワーク; };

DNS の要求を受け付けるネットワークを指定します。ネットワーク は実際のアドレス (たとえば 192.168.2.0/24) に置き換えてください。なお、/24 とは ネットマスクの省略表現です (この場合、255.255.255.0 を意味します)。

`allow-transfer ! *;;`

どのホストに対してゾーン転送を許可するかを制御します。この例では！ * を指定しているため、ゾーン転送を完全に拒否 するようになります。この項目を設定しないと、ゾーン転送に対する制限が 行なわれず、どのホストからでも行なうことができるようになります。

`statistics-interval 0;`

この項目を設定しないと、BIND は複数の行から構成される統計情報を 1 時間 おきに /var/log/messages に出力します。0 を指定するとこれらの統計情報を省略することができます。それ以外の値であれば、分単位で出力間隔を指定することになります。

`cleaning-interval 720;`

このオプションでは、BIND がその内蔵キャッシュを消去する時間間隔を指定します。この時間間隔で /var/log/messages に対して情報が出力 されます。時間は分単位で指定します。既定値は 60 分です。

`interface-interval 0;`

BIND では定期的にネットワークインターフェイスの追加や削除を検索します。この値を 0 にすると、ネットワークインターフェイスの 検出作業を行なわなくなり、起動時に検出したインターフェイスに対してのみ 要求を受け付けるようになります。0 以外の設定を行なうと、それは分単位での設定になります。既定値は 60 分です。

`notify no;`

no を設定すると、ゾーンデータの変更やネームサーバの 再起動が発生するごとに発生していた、ネームサーバ宛の通知を行なわなくなります。

利用可能なオプションの一覧については、man 5 named.conf で表示されるマニュアルページをお読みください。

13.5.2 ログ

BIND では、何をどのように、どこでログを採取するかを広範囲に設定することができます。通常は既定の設定のままで問題ありません。例13.3「ログ出力を無効化する場合の設定」(285 ページ) では、このようなログを完全に省略するために 最も簡単な方法を提示しています。

例 13.3 ログ出力を無効化する場合の設定

```
logging {  
    category default { null; };
```

```
};
```

13.5.3 ゾーン項目

例 13.4 *example.com* のゾーン項目

```
zone "example.com" in {  
    type master;  
    file "example.com.zone";  
    notify no;  
};
```

まず、zone の後に管理したいドメインの名前を指定し (上記の例では example.com)、さらに in を指定します。あとは関連するオプションを記述するための中括弧を記述し、例13.4「example.com のゾーン項目」(286 ページ) のような構成になります。スレーブゾーンを定義する場合は type に対して slave を指定し、このゾーンを管理するネームサーバ (別のサーバ) を master で指定します。たとえば 例13.5「example.net のゾーン項目」(286 ページ) のようになります。

例 13.5 *example.net* のゾーン項目

```
zone "example.net" in {  
    type slave;  
    file "slave/example.net.zone";  
    masters { 10.0.0.1; };  
};
```

ゾーンのオプションには下記のようなものがあります:

type master;

master を指定すると、BIND に対してこのゾーンをこのネームサーバで管理するようになります。また、ゾーンファイルは正しい書式で作成されているものと解釈します。

type slave;

このゾーンは、他のネームサーバから情報を転送することで成立させるゾーンです。masters の設定とともに使用しなければなりません。

type hint;

hint タイプが設定された . ゾーンは、ルートネームサーバを設定するために使用します。このゾーンの定義はそのまま残しておいてください。

file example.com.zone または file 「slave/example.net.zone」;

この設定では、そのゾーンに対するゾーンデータがどのファイルに保存されているものなのかを指定します。スレーブゾーンの場合は、このファイルは他のネー

ム サーバから転送してくることになるため、存在している必要はありません。マスターゾーンの場合とスレーブゾーンの場合の違いは、slave というディレクトリを使用しているかどうかの違いです。

```
masters { サーバの IP アドレス;};
```

この項目は、スレーブゾーンでのみ必要な設定です。ゾーンファイルをどのネームサーバから転送するのかを指定します。

```
allow-update {! *;};
```

このオプションでは、外部からの書き込みアクセス (DNS の項目をクライアント側に作成する機能を与えるもの) を制御します。通常はセキュリティ上の理由から使用することはありません。この項目を設定しないと、ゾーンの更新は全く行なうことができません。上記の設定は何も指定しない場合と同じ意味で、! * で全てに対する拒否を行なっています。

13.6 ゾーンファイル

ゾーンファイルについては、2 種類のものが必要です。1 つはホスト名に対して IP アドレスを割り当てるもの、もう 1 つはその逆で、IP アドレスに対する ホスト名を割り当てるものです。

ヒント: ゾーンファイル内でのドット (ピリオド、終止符) の使用

ゾーンファイル内では ”.” は重要な意味を持ちます。ホスト名の最後が . で終わっていない場合、該当するゾーン が付加されます。完全修飾ドメイン名で指定したい場合は、さらにドメインが 付加されることを避けるため、. で終わらなければなりません。ネームサーバの設定ミスとしては、"." を付け忘れていたり、正しい位置に付けなかったりなどが、よくあります。

最初に考慮しなければならないことはゾーンのファイル名で、たとえば example.com というドメインに対しては、example.com.zone のような名前を設定します。たとえば 例13.6「/var/lib/named/example.com.zone ファイル」(287 ページ) のようになります。

例 13.6 /var/lib/named/example.com.zone ファイル

```
1. $TTL 2D
2. example.com. IN SOA      dns root.example.com. (
3.                  2003072441 ; serial
4.                  1D        ; refresh
5.                  2H        ; retry
6.                  1W        ; expiry
```

```

7.          2D )          ; minimum
8.
9.          IN NS         dns
10.         IN MX         10 mail
11.
12. gate     IN A          192.168.5.1
13.          IN A          10.0.0.1
14. dns      IN A          192.168.1.116
15. mail     IN A          192.168.3.108
16. jupiter  IN A          192.168.2.100
17. venus    IN A          192.168.2.101
18. saturn   IN A          192.168.2.102
19. mercury  IN A          192.168.2.103
20. ntp      IN CNAME      dns
21. dns6     IN A6 0       2002:c0a8:174::

```

1 行目:

\$TTL では、このファイル内の全ての項目に対して適用する、既定の生存時間 (Time To Live) を設定します。この例では、項目は 2 日間 有効であり続けます (2 D)。

2 行目:

この行から SOA (権威の開始) の制御レコードが始まります:

- まずは管理対象のドメイン名を記述します (example.com)。このドメイン名は必ず ”.” で終わるものとしてください。そうでないとドメイン名の後ろに再度ドメイン名が付加されてしまいます。なお、ここには @ を入れることもできます。これは 関連する /etc/named.conf の項目からドメイン名を自動的に取り出す場合に使用します。
- IN SOA に続いて、このゾーンに対するマスターの ネームサーバ名を指定します。ここでは dns と指定していますが、これは ”.” で終わっていないため、自動的に dns.example.com の形に展開されます。
- ネームサーバ名に続いて、このドメインの担当者のメールアドレスを指定します。なお、ゾーンファイルで @ 記号は特別な意味を持つものであるため、この記号の代わりに ”.” で指定してください。たとえば root@example.com というメール アドレスであれば、root.example.com. と指定します。なお、この指定も ”.” で終わらせてください。そうでないとドメイン名がさらに付加されてしまいます。
- (から) までの間は SOA レコードの詳細情報を指定するための括りです。

3 行目:

ここでは シリアル番号 を指定します。シリアル番号は 任意に付与することのできる番号で、このファイルの更新が行なわれるごとに数字を 増やさなければ

ならない項目です。このシリアル番号は、他のネームサーバ (スレーブサーバなど) に対して変更の通知を行なう際に必要となります。ここでは 10 桁の数値で年月日と追加の数字を設定しています (YYYYMMDDNN の形式) が、これは慣習的にこのようにしているものです。

4 行目:

ここでは 更新間隔 を指定します。更新間隔は他のネームサーバ (スレーブサーバなど) に対して、シリアル番号 を検証する間隔を指定します。この場合、1 日間隔の意味になります。

5 行目:

ここでは 再試行間隔 を指定します。再試行間隔は他のネームサーバ (スレーブサーバなど) からのアクセスが失敗したときに、プライマリネームサーバ (マスターサーバ) に再接続する間隔を指定します。ここでは 2 時間に 設定されています。

6 行目:

ここでは 有効期限 を指定します。有効期限は他のネームサーバ (スレーブサーバ) からプライマリネームサーバ (マスターサーバ) へのアクセスが回復しない場合に、他のネームサーバがキャッシュデータを捨てるまでの 時間間隔を指定します。ここでは 1 週間に設定されています。

7 行目:

ここが SOA レコードの最後の部分で、ネガティブキャッシュの 生存時間を指定します。これは、このドメインに対する問い合わせに 対し、該当レコードが存在しない旨の応答を受けつけたときに、キャッシュする時間 間隔を指定します。

9 行目:

IN NS では、このドメインに対して管理責任を持つネームサーバを指定します。dns は "." で終わっていないため、dns.example.com に展開されます。この行は、プライマリ (マスター) ネームサーバとセカンダリ (スレーブ) ネームサーバのように、複数個を指定することもできます。/etc/named.conf 内で notify に対し no と設定されていない場合は、ここで指定した全てのネームサーバに対してゾーンデータの更新を通知します。

10 行目:

MX レコードには、そのドメイン (この例では example.com) に対するメールを受け付け、必要に応じて処理や転送を行なうメールサーバを指定します。この例では、mail.example.com がそのメールサーバであることを示しています。ホスト名の前につく数字は優先順位で、複数の MX レコードが存在する場合、ま

ずは最も小さい値を持つメールサーバに対して配送が 試みられ、それが失敗した場合は次に小さい値を持つメールサーバに対して配送を 行なおうとします。

12 行目から 19 行目:

これらの行で、複数のホスト名と IP アドレスの対応を記述しています。ここに記述された名前には “.” が付けられておらず、ドメイン名が記述されていないため、それら全てに対して example.com が付加されます。なお、ホスト gate には 2 つのアドレスが割り当てられていますが、これはこのマシンに 2 枚のネットワークカードが接続されているためです。ホストのアドレスが従来のもの (IPv4) である場合は、このレコードは A レコードになります。ホストのアドレスが IPv6 アドレスである場合には、AAAA レコードを指定します。

注記: IPv6 での文法

IPv6 レコードは IPv4 とは異なる文法で記述されます。IPv6 では断片的なアドレス表記を行なうことができるため、アドレスの途中に「0」が続く場合は、その箇所に 2 つのコロン (:) を記述してください。

```
pluto      AAAA 2345:00C1:CA11::1234:5678:9ABC:DEF0
pluto      AAAA 2345:00D2:DA11::1234:5678:9ABC:DEF0
```

20 行目:

dns ホストの別名として、ntp を提供するための記述です (CNAME とは、*canonical name* (公式に認められた名前) の 意味です)。

疑似ドメイン in-addr. arpa は、IP アドレスからホスト名に 逆引きする際に利用します。アドレスのネットワーク部を逆順で表記したものを付加してドメイン名とします。たとえば 192. 168 のアドレスに対する逆引き疑似ドメインは、168. 192. in-addr. arpa になります。例13.7「逆引き」(290 ページ) をご覧ください。

例 13.7 逆引き

```
1. $TTL 2D
2. 168. 192. in-addr. arpa.      IN SOA dns. example. com. root. example. com. (
3.                               2003072441          ; serial
4.                               1D                   ; refresh
5.                               2H                   ; retry
6.                               1W                   ; expiry
7.                               2D )                 ; minimum
8.
9.                               IN NS               dns. example. com.
10.
11. 1. 5                          IN PTR       gate. example. com.
12. 100. 3                       IN PTR       www. example. com.
```


1 行目:

\$TTL では、このゾーンの全てに適用される標準 TTL (生存時間) を指定します。

2 行目:

このゾーンファイルでは、192.168 に対する逆引きゾーンを設定しています。そのための擬似的なゾーン (ドメイン) は 168.192.in-addr.arpa で、このドメインは実際に存在するものではありません。そのため、全てのホスト名は完全修飾の (つまりドメイン名を付けた) 形であり、かつ ”.” で終わるもの) で指定しなければなりません。それ以外の項目については example.com の例と同じです。

3 行目から 7 行目:

example.com での例と同じですので、そちらをお読みください。

9 行目:

この行では、このゾーンに対して管理責任を持つネームサーバを指定しています。ここで指定する名前は通常のドメインのものとは異なり、ドメイン指定を含んだ完全修飾の形で、”.” で終わらなければなりません。

11 行目から 13 行目:

これらは、それぞれの IP アドレスに対するホスト名を指定するポインタレコードです。これらはいずれも ”.” で終わっておらず、行頭には IP アドレスの末尾部分しか書かれていないため、ゾーンが自動的に付加されます。実際の IP アドレスに変換する場合は、.in-addr.arpa を取り除いて ”.” ごとに逆から読んでください。

通常は、異なる BIND のバージョン間でも、問題なくゾーンの転送を行なうことができます。

13.7 ゾーンデータの動的な更新

動的な更新 とは、マスターサーバ上のゾーンファイル内の項目を追加したり変更したり、削除したりする操作のことを指します。この仕組みは RFC 2136 で規定されています。動的な更新は、任意指定の allow-update や update-policy の設定を行なうことで、ゾーンごとに個別の設定を行なうことができます。動的に更新されるゾーンの場合、そのゾーンファイルは手作業で編集すべきではありません。

サーバに対して更新すべき項目を送信するには、nsupdate コマンドを使用します。このコマンドに対する正確な文法については、nsupdate の マニュアルページ (man 8 nsupdate) をお読みください。なおセキュリティ上の理由により、13.8項「機密を保持する通信」(292 ページ) で書かれているとおり、このような更新には TSIG 鍵を使用すべきものです。

13.8 機密を保持する通信

機密を保持して通信するには、共有の機密鍵 (TSIG 鍵とも呼ばれます) をベースにした、トランザクション署名 (TSIG) を利用して行ないます。この章では、このような鍵をどのようにして生成するのかと、その使い方について述べています。

機密を保持する通信は、異なるサーバ間の通信やゾーンデータの動的な更新を行なう 場合に必要となります。また、鍵をベースにしたアクセス制御を利用すると、単純に IP アドレスに依存した制御よりもより安全になります。

TSIG 鍵を生成するには、下記のコマンドを実行します (詳しくは man dnssec-keygen をお読みください):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

このコマンドを実行すると、下記のような 2 つのファイルが生成されます:

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

鍵それ自身 (ejIkuCyyGJwwuN3xAteKgg== のような文字列) が 両方のファイル内に存在するはずでず。通信時にこの鍵を使用するには、あらかじめ 2 つめのファイル (Khost1-host2.+157+34265.key) を リモートホスト側に安全な方法で (たとえば scp) 転送しておかなければなりません。リモートのサーバでは host1 と host2 の間で機密通信を行なうため、/etc/named.conf ファイル内で 鍵を設定しなければなりません:

```
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 のパーミッション設定で、ファイルへの アクセスが正しく制限されていることを確認してください。このファイルの既定の パーミッションは 0640 で、所有者が root に、グループが named にそれぞれ設定されているはずでず。パーミッションを設定する以外 にも、特別にアクセスを制限した別ファイルを

作成し、そのファイルを `/etc/named.conf` から参照させる方法もあります。外部のファイルを参照させるには、下記のように設定します:

```
include "filename"
```

ここで `filename` には、鍵ファイルの絶対パスを指定します。

`host1` のサーバに対して `host2` (アドレス `10.1.2.3`) と通信する際、鍵を使用するように設定するには、サーバ側の `/etc/named.conf` に下記のルールを追加しなければなりません:

```
server 10.1.2.3 {  
    keys { host1-host2. ; };  
};
```

`/etc/named.conf` 側の設定ファイルにも、似たような設定を行わなければなりません。

通信の機密性を保持するには、IP アドレスやアドレス範囲に対して設定した任意の ACL (アクセス制御リスト。ファイルシステムのアクセス制御リストと混同しないでください) に TSIG 鍵を追加することもできます。たとえば下記のように設定します:

```
allow-update { key host1-host2. ;};
```

これらの詳細については、*BIND Administrator Reference Manual* 内の `update-policy` で説明しています。

13.9 DNS セキュリティ

DNSSEC または DNS セキュリティは、RFC 2535 で規定されています。DNSSEC 向けのツールについては、BIND マニュアル内で説明されています。

機密を保持すべきと考えるゾーンには、それに結びつけられた 1 つ以上のゾーン鍵が存在しなければなりません。このゾーン鍵は、ホスト鍵と同様に `dnssec-keygen` で作成することができます。これらの鍵を生成する際は、DSA 暗号化アルゴリズムが使用されます。関連するゾーンファイルから `$INCLUDE` ルールを利用して、公開鍵を登録してください。

`dnssec-signzone` コマンドを利用すると、生成した鍵 (`keyset-` ファイル) のセットを作成することができます。これを親ゾーンに対して機密を保持した通信で送信し、署名を実施してください。あとは生成されたファイルを `/etc/named.conf` 内の各ゾーンに登録してください。

13.10 さらになる情報

さらになる情報や説明については、bind-doc パッケージに含まれる *BIND Administrator Reference Manual* をお読みください。このパッケージは /usr/share/doc/packages/bind/ 内にファイルをインストールします。また、マニュアルや BIND に含まれている マニュアルページから参照されている各 RFC についても、それぞれお読みください。また、/usr/share/doc/packages/bind/README. SuSE には、openSUSE での BIND について、最新情報を提供しています。

DHCP

Dynamic Host Configuration Protocol (DHCP) の目的は、それぞれのワークステーションで別々の設定を行なうのではなく、中央でネットワーク 設定を管理して (サーバから) 設定を割り当てることにあります。DHCP を使用するよう設定したホストには、固定で設定するようなアドレスはありません。サーバからの 指示に従って自動的に設定を行なうことができます。クライアント側で NetworkManager を使用している場合は、クライアント側で設定すべきことは何ともありません。これは、1 つのネットワークインターフェイスを利用して複数のネットワーク環境を 切り替えるマシンで、便利な設定です。ただし、DHCP サーバの動作するマシンでは NetworkManager を動作させてはなりません。

DHCP サーバを設定するための 1 つの方法として、ネットワークカードのハードウェア アドレスを利用して各クライアントを識別する方法があります (多くの場合、ハードウェアアドレスは固定で割り当てられています)。この方法では、クライアントが サーバに接続するごとに同じ設定を割り当てます。もう 1 つの方法として、この目的用に 確保したアドレス帯域を設定し、クライアントに対して動的な割り当てを行なうことも できます。後者の場合でも、DHCP サーバはクライアントから要求が届くごとに同じ アドレスを割り当てようとします。それはたとえ期限を超過した場合でも同じです。ただし、この方法はアドレスの全体数よりもクライアント数のほうが少ない場合にのみ 動作します。

DHCP はシステム管理者の手間を省きます。アドレスやネットワークの設定など、大きな 設定変更が起こった場合でも、サーバ側の設定ファイルを編集するだけで作業が完了します。これは、多数のワークステーションの設定を変更しなければならないような場合よりは ずっと手間を省くことができます。特に新しいマシンをネットワークに接続するような 場合には、アドレス帯域から IP アドレスを自動で割り当てることになるため、とても 作業が簡単になります。DHCP サーバから取得した適切な

ネットワーク設定を受け取る 仕組みであるため、異なるネットワークで使用するようなラップトップでは便利に使う ことができます。

この章では、DHCP サーバをワークステーションと同じサブネット 192.168.2.0/24 で動作させる場合を想定しています。ゲートウェイは 192.168.2.1 で、DHCP サーバのアドレスは 192.168.2.254、割り当てるアドレス帯域は 192.168.2.10 から 192.168.2.20 までと、192.168.2.100 から 192.168.2.200 までを設定する ものとします。

DHCP サーバは IP アドレスとネットマスクを提供するだけではなく、各クライアントが利用するホスト名やドメイン名、ゲートウェイやネームサーバの設定も提供します。またこれら以外にも、現在時刻を問い合わせるための時刻サーバや印刷サーバなど、様々な情報を中央から配布することができます。

14.1 YaST での DHCP サーバ設定

DHCP サーバをインストールするには、YaST を起動して **ソフトウェア > ソフトウェア管理** を選択します。続いて **フィルタ > パターン** を選択し、**DHCP および DNS サーバ** を選択します。あとはインストール処理を完了し、依存関係の パッケージをインストールする確認に答えてください。

重要: LDAP 対応

YaST の DHCP モジュールの設定を ローカル (DHCP サーバ自身) に保存することができるほか、LDAP サーバに 保存することもできます。LDAP を利用して設定を保存したい場合は、DHCP サーバを設定する前に LDAP サーバを設定してください。

LDAP について、詳しくは 第4章 **ディレクトリサービス LDAP** (↑セキュリティガイド) をお読みください。

YaST DHCP モジュール (yast2-dhcp-server) では、ローカルネットワーク用の DHCP サーバを設定することができます。また、このモジュールはウィザードモードと熟練者向け設定モードのいずれかで 動作させることができます。

14.1.1 初期設定 (ウィザード)

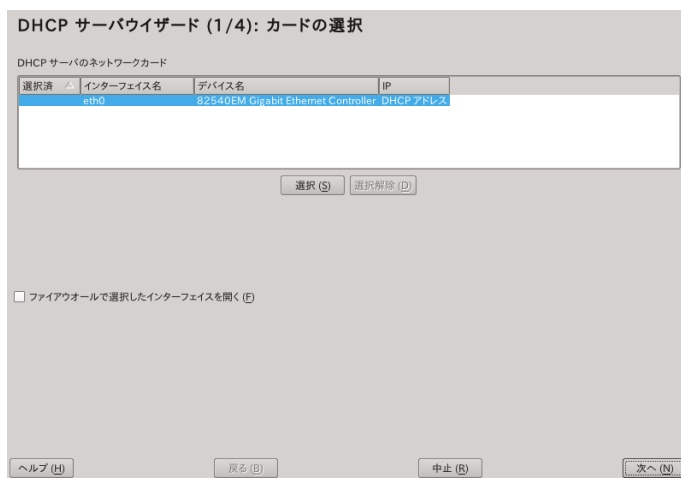
最初にモジュールを起動したときにはウィザードが起動し、サーバを起動するにあたっていくつか決めておかなければならない基本設定について質問が行なわれま

す。この初期設定作業はサーバを機能させるためのごく基本的な設定だけです。高度な設定作業については、熟練者モードをご利用いただくことができます。

カードの選択

最初の手順では、YaST はお使いのシステム内で利用可能なネットワーク インターフェイスに確認し、一覧を表示します。一覧から DHCP サーバのサービスを提供したいインターフェイスを選択し、**選択** を押してください。選択のあとは、このインターフェイスに対してファイアウォールを開くため、**ファイアウォールで選択したインターフェイスを開く** を選択してから **次へ** を押してください。詳しくは 図14.1「DHCP サーバ: カードの選択」(297 ページ) をご覧ください。

図 14.1 DHCP サーバ: カードの選択



グローバル設定

まずは DHCP の設定を LDAP サーバ内に保存するかどうか、チェックボックスで 選択 します。またそれぞれの入力フィールドに対して、DHCP サーバが管理すべき全クライアント用のネットワーク設定を指定してください。ドメイン名やタイムサーバ、プライマリまたはセカンダリのネームサーバ、印刷サーバや WINS サーバ (Windows と Linux のクライアントが混在する環境の場合)、ゲートウェイアドレスや貸与時間をそれぞれ設定します。詳しくは 図14.2「DHCP サーバ: グローバル設定」(298 ページ) をご覧ください。

図 14.2 DHCP サーバ: グローバル設定

DHCP サーバウィザード (2/4): グローバル設定

☐ LDAP サポート (L)

DHCP サーバ名 (N) (オプション)

ドメイン名 (D)

example.org

NTP 時刻サーバ (T)

ntp.nict.jp

プライマリネームサーバ IP (P)

192.168.1.254

プリントサーバ (P)

セカンダリネームサーバ IP (S)

WINS サーバ (W)

デフォルトゲートウェイ (ルータ) (G)

192.168.1.200

既定の貸与時間 (L)

10

単位 (U)

分

ヘルプ (H) 戻る (B) 中止 (R) 次へ (N)

ダイナミック DHCP

この段階では、どのようにして動的な IP アドレスの配布を行なうのかについて設定を行ないます。まずは DHCP クライアントに対してサーバから配布する IP アドレスの範囲を設定します。これらのアドレスは同じネットワーク内を示すものでなければなりません。また、クライアントが期限の延長を申請することなく IP アドレスを使い続けることのできる、既定の貸与時間も設定します。また、最大の貸与時間も設定することができます。これはサーバが特定のクライアントに対する IP アドレスを予約しておく時間の意味です。詳しくは 図14.3「DHCP サーバ: ダイナミック DHCP」(299 ページ) をご覧ください。

図 14.3 DHCP サーバ: ダイナミック DHCP

DHCP サーバウィザード (3/4): ダイナミック DHCP

サブネット情報

現在のネットワーク (N)	現在のネットマスク (M)	ネットマスクビット (T)
<input type="text" value="10.0.2.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="24"/>
最小 IP アドレス (I)	最大 IP アドレス (X)	
<input type="text" value="10.0.2.1"/>	<input type="text" value="10.0.2.254"/>	

IP アドレス範囲

最初の IP アドレス (F)	最後の IP アドレス (L)
<input type="text"/>	<input type="text"/>

☐ 動的 BOOTP の許可 (B)

貸与時間

既定 (D)	単位 (U)	最大値 (X)	単位 (T)
<input type="text" value="4"/>	<input type="text" value="時間"/>	<input type="text" value="2"/>	<input type="text" value="日"/>

DNS サーバと同期 (S) ...

ヘルプ (H) 戻る (B) 中止 (R) 次へ (N)

設定の完了と開始モードの設定

3 段階目の設定ウィザードを完了すると、DHCP サーバをどのようにして起動するかを設定する最後のダイアログが表示されます。ここでは DHCP サーバをシステム 起動時に自動で起動するか、もしくは必要に応じて手動で起動するか (たとえば テスト用に起動する場合など) を選択することができます。設定を完了したら、**完了** を押してください。詳しくは 図14.4「DHCP サーバ: 起動」(299 ページ) をご覧ください。

図 14.4 DHCP サーバ: 起動

DHCP サーバウィザード (4/4): 起動

サービスの開始

☐ システム起動時 (B)

☒ 手動 (M)

DHCP サーバ熟練者設定 (E) ...

ヘルプ (H) 戻る (B) 中止 (R) 完了 (F)

14.2 DHCP ソフトウェアパッケージ

openSUSE では、DHCP サーバと DHCP クライアントの両方が提供されています。DHCP サーバとしては `dhcpcd` (Internet Systems Consortium 提供) が公開されていますが、DHCP クライアントとしては 2 種類のクライアントが 公開されています: `dhcp-client` (上記と同様に ISC 提供のもの) と `dhcpcd` パッケージがあります。

openSUSE では既定で `dhcpcd` がインストールされています。このプログラムはとも扱いやすく、それぞれのシステム起動時に DHCP サーバのチェックを行なうために自動で起動するようになっています。`dhcpcd` はその処理を行なうにあたって設定 ファイルを必要とせず、多くの標準的なセットアップ環境でうまく動作するようになっています。より複雑な環境の場合は ISC の `dhcp-client` をお使いいただき、設定ファイル `/etc/dhclient.conf` で細かい制御を行なってください。

14.3 DHCP サーバ `dhcpcd`

DHCP システムの中核は、dynamic host configuration protocol (DHCP) のデーモンです。このサーバは設定ファイル `/etc/dhcpd.conf` での設定に基づき、アドレスを貸与し、それらがどのように使用されているかを監視します。このファイルのパラメータや値を変更することで、システムの管理者は様々な方法でプログラムの動きを制御することができます。まずは 例14.1「設定ファイル `/etc/dhcpd.conf`」(300 ページ) にある基本設定例 `/etc/dhcpd.conf` をお読みください。

例 14.1 設定ファイル `/etc/dhcpd.conf`

```
default-lease-time 600;          # 10 minutes
max-lease-time 7200;             # 2 hours

option domain-name "example.com";
option domain-name-servers 192.168.1.116;
option broadcast-address 192.168.2.255;
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0
{
    range 192.168.2.10 192.168.2.20;
    range 192.168.2.100 192.168.2.200;
}
```

このようなシンプルな設定ファイルだけで、DHCP サーバに対してネットワーク内のアドレス割り当てを実施させることができます。なお、各行の末尾にはセミコロンがきちんと付けられていることを確認してください。そうでないと `dhcpcd` を起動することができません。

このサンプルファイルは 3 つのセクションから構成されています。1 つめのセクションには、クライアントからアドレスを要求されたときに、既定でどれだけの期間更新無しで貸し出すのか (`default-lease-time`) を設定しています。このセクションでは、DHCP サーバが IP アドレスを貸与したあと、更新無しでどれだけの期間アドレスを保持しておくか (`max-lease-time`) も設定しています。

2 つめのセクションには、グローバルな範囲でいくつかの基本的なネットワークパラメータを指定しています：

- `option domain-name` の行では、お使いのネットワークにおける既定のドメインを設定しています。
- `option domain-name-servers` を設定すると、ホスト名から IP アドレス、またはその逆の変換のため、最大で 3 つまでの DNS サーバを指定することができます。理想的にはお使いのマシン上で動作しているネームサーバや、お使いのネットワーク内のどこかにあるネームサーバを設定します。なお、これらのネームサーバでは、それぞれ動的に割り当てられるアドレスに対して、ホスト名を定義しておくべきものです。ネームサーバの設定方法について、詳しくは 第13章 ドメインネームシステム (271 ページ) をお読みください。
- `option broadcast-address` の行では、クライアントが使用すべきブロードキャストアドレスを指定しています。
- `option routers` では、ローカルネットワークだけでは到達できないホストとの通信を行なう際、データパケットを送信する宛先を指定します (発信元と送信先のアドレス、およびサブネットマスクから判断します)。多くの場合、特に小さなネットワークの場合は、ルータとインターネットゲートウェイは同じものです。
- `option subnet-mask` では、クライアントに割り当てるサブネットマスクを指定します。

設定ファイルの最後の部分では、サブネットマスクを含むネットワークを定義しています。また括弧内では、DHCP デーモンがクライアントに対して割り当てるべきアドレス範囲を指定しています。例14.1「設定ファイル `/etc/dhcpcd.conf`」(300 ページ) の例では、192.168.2.10 から 192.168.2.20 までの範囲と、192.168.2.100 から 192.168.2.200 までの範囲でそれぞれ割り当てを行ないます。

これらのうちいくつかを環境に応じて変更したら、あとは `rcdhcpd start` コマンドで DHCP サーバを起動することができます。これですぐにサービスを利用できるようになります。また、設定ファイルについて大まかな文法チェックを行ないたい場合は、`rcdhcpd check-syntax` コマンドを入力してください。設定について予期しない問題に直面した場合 (サーバがエラー終了するか、起動時に `done` が表示されない場合) は、メインのシステムログである `/var/log/messages` を利用して何が間違っているのかを確認することができるほか、コンソール 10 でエラー出力を確認することもできます (`Ctrl + Alt + F10` を押してください)。

既定の openSUSE システムでは、DHCP はセキュリティ上の理由から、`chroot` 環境で起動されます。設定ファイルはデーモンから読み取ることができるよう、`chroot` の環境下にコピーしなければなりません。通常は `rcdhcpd start` コマンドで自動的にファイルをコピーするため、これらのことについて心配する必要はありません。

14.3.1 固定 IP アドレスのクライアント

DHCP では、特定のクライアントに対して固定のアドレスを事前に定義し、割り当てることもできます。明示的に指定したアドレスは、帯域からの動的な割り当てよりも常に優先して動作します。また固定のアドレスは動的なアドレスと異なり、クライアントに配布するアドレスよりも利用可能なアドレスが少ない場合に発生するような、有効期限の問題もありません。

固定のアドレスを各クライアントに割り当てるにあたり、DHCP ではハードウェア アドレス (たとえば `00:30:6E:08:EC:80`) を利用して、ネットワーク デバイスを識別します (世界中で唯一の番号が割り振られるもので、6 バイトから構成される数値コードです)。具体的には例 14.2「設定ファイルへの追記」(302 ページ) に示すような設定を例 14.1「設定ファイル `/etc/dhcpd.conf`」(300 ページ) に追加することで、特定のクライアントに対して同じデータを割り当てるようになります。

例 14.2 設定ファイルへの追記

```
host jupiter {  
  hardware ethernet 00:30:6E:08:EC:80;  
  fixed-address 192.168.2.100;  
}
```

各クライアントの名前 (`host` ホスト名の部分、ここでは `jupiter`) が最初の行に記述され、2 行目に MAC アドレスが記述されています。Linux ホストでは、MAC アドレスは `ip link show` コマンドで表示させることができます。このコマンドの後ろにネットワークデバイス (たとえば `eth0`) を指定してください。出力には下記のような行があるはずです。

Link/ether 00:30:6E:08:EC:80

上記の例では、00:30:6E:08:EC:80 という MAC アドレスが設定されている クライアントに対して、192.168.2.100 というアドレスと jupiter というホスト名を自動的に割り当てる 動作になります。ほとんどの場合、ハードウェアの種類 (hardware) には ethernet を指定しますが、IBM システムなどでは token-ring である場合もあります。DHCP ではどちらにも対応しています。

14.3.2 openSUSE バージョン

セキュリティをよりよくするため、ISC 提供の DHCP サーバの openSUSE 版では、Ari Edelkind 氏が開発した non-root/chroot パッチを適用した状態で公開しています。これにより、dhcpd をユーザ ID nobody で実行し、chroot 環境 (/var/lib/dhcp) で動作させることができるようになっています。また、この機能を実現するため、設定ファイル dhcpd.conf は /var/lib/dhcp/etc に配置しなければなりません。起動時の 起動スクリプトでこのディレクトリへの設定ファイルコピーを行っています。

この機能に関するサーバの動作を制御するには、/etc/sysconfig/dhcpd ファイルを編集してください。dhcpd を chroot 環境で動作させないようにするには、/etc/sysconfig/dhcpd ファイル内の DHCPD_RUN_CHROOTED 変数に、「no」を設定してください。

dhcpd に対し、chroot 環境下からでもホスト名を解決できるようにするには、いくつかの設定ファイルについてもコピーしておかなければなりません：

- /etc/localtime
- /etc/host.conf
- /etc/hosts
- /etc/resolv.conf

これらのファイルは、起動時に初期化スクリプトが /var/lib/dhcp/etc/ にコピーします。これらのコピーは /etc/ppp/ip-up のようなスクリプトから動的に更新される場合に必要となります。しかしながら、この設定ファイルは IP アドレスだけ (ホスト名ではなく) を指定する仕組みであるため、特に心配する必要はありません。

また、お使いの設定ファイルから外部のファイルを参照するように設定している場合は、それらを chroot 環境にコピーする必要があります。このような外部ファイル

については、`/etc/sysconfig/dhcpd` ファイル内の `DHCPD_CONF_INCLUDE_FILES` 変数に設定を行なってください。また、`syslog-ng` が再起動しても DHCP のログ機能が正しく動作するようにするため、`/etc/sysconfig/syslog` 内に `SYSLOGD_ADDITIONAL_SOCKET_DHCP` という設定を用意しています。

14.4 さらになる情報

DHCP に関する詳しい情報は、*Internet Systems Consortium* の Web サイト (<http://www.isc.org/products/DHCP/>) (英語) をお読みください。`dhcpd`, `dhcpd.conf`, `dhcpd.leases`, `dhcp-options` についての各マニュアルページも提供されています。

NTP を利用した時刻同期

NTP (Network Time Protocol; ネットワーク時刻プロトコル) は、ネットワークを介して時刻同期を行なうためのプロトコルです。NTP サービスでは最初に、信頼の置ける時刻発信源であるサーバから時刻を取得します。その後、マシンは自分自身がネットワーク内の他のコンピュータに対して、時刻を発信できるように動作します。つまり NTP サービスには、絶対時刻の管理とネットワーク内の全マシンに対するシステム時刻の同期、という 2 つの目的が存在することになります。

正確なシステム時刻を保つことは、様々な状況で重要な要件となります。内蔵のハードウェア (BIOS) 時計では、データベースやクラスタなどのアプリケーションの要件に足りていない場合がしばしばあります。かといってシステム時刻を手作業で修正すると、たとえば時刻の巻き戻りによって、重要なアプリケーションに障害が発生してしまったりするなど、場合によっては深刻な問題になってしまうことがあります。ネットワーク内では一般に、全てのマシンのシステム時刻を同期しておく必要がありますが、手作業による調整は悪いアプローチと言わざるを得ません。NTP を利用すると、これらの問題を解決することができます。ネットワーク内にある信頼している時刻発信源の情報を頼りに、システム時刻を継続的に調整します。時刻の発信源としては、電波時計のようなローカル参照時計を利用することもできます。

15.1 YaST を利用した NTP クライアントの設定

ntp パッケージに含まれる NTP デーモン (ntpd) は、自分自身の時計を時刻発信源として使用するように事前設定されています。しかしながら (BIOS の) 時計は、

より精度の高い時刻発信源が存在しない場合の代替手段として使用されるべきものです。そのため、YaST を利用して NTP クライアントの設定を行なってください。

15.1.1 基本設定

YaST での NTP クライアント設定 (ネットワークサービス > *NTP 設定*) は複数のタブから構成されています。*一般設定* のタブで ntpd の起動モードを設定します。

図 15.1 より高度な NTP クライアント設定: 一般設定

高度な NTP 設定

一般設定 セキュリティ設定

NTP デーモンを起動する

☐ 手動でのみ起動 (M)

☐ デーモンを使用せずに同期する (S)

☒ 今すぐ開始し、システム起動時に開始するよう設定 (B)

実行時設定ポリシー (R) カスタムポリシー (C)

自動

同期間隔 [分] (I)

5

同期種類 アドレス

サーバー ig.pool.ntp.org

自分自身の時計 (ローカル)

追加 (A) 編集 (I) 削除 (T) ログの表示 (L)...

ヘルプ (H) キャンセル (C) OK (O)

手動でのみ起動

全ての項目を手作業で設定したい場合は、*手動でのみ起動* を選択します。

デーモンを使用せずに同期する

ラップトップやその他のマシンで自動的にサスペンドするような環境の場合、*デーモンを使用せずに同期する* を選択します。このモードでは YaST は同期を行なうのに ntpd を開始することは行ないません。その代わりに、YaST は crontab の項目 (/etc/cron.d/novell.ntp-synchronize) を作成し、*同期間隔 (分)* の項目で指定した間隔で時刻サーバに時刻を問い合わせるようにします。cron について、詳しくは 9.1.2 項「cron パッケージ」(176 ページ) をお読みください。

今すぐ開始し、システム起動時に開始するよう設定

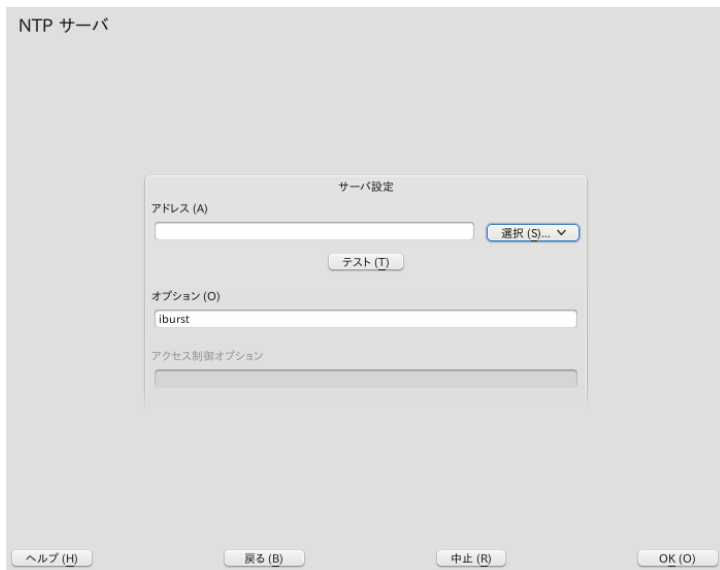
システムの起動時に ntpd を自動的に開始するように設定 するには、今すぐ開始し、システム起動時に開始するよう設定 を選択します。なお、0. opensuse.pool.ntp.org, 1. opensuse.pool.ntp.org, 2. opensuse.pool.ntp.org, 3. opensuse.pool.ntp.org のいずれかが 事前 に選択されています。

15.1.2 基本的な設定の変更

時刻サーバなど、クライアントに設定する時刻発信源は、一般設定 タブで表示される画面の下半分で設定を行ないます。必要に応じて、それぞれ 追加, 編集, 削除 を行なってください。ログの表示 を押すと、お使いのクライアント におけるログファイルを閲覧することができます。

追加 ボタンを押すと、時刻の発信源を追加することができます。まずは表示されるダイアログから、時刻同期の種類を選択します。下記のうちの いずれかを選択することができます:

図 15.2 YaST: NTP サーバ



サーバ

選択 のプルダウンリスト (図15.2「YaST: NTP サーバ」 (307 ページ) をご覧ください) から、お使いのローカルネットワークにあるタイムサーバを利用して時刻同期を設定することができる (**ローカル NTP サーバ**) ほか、ご利用のタイムゾーンに合わせてインターネット上で公開されているタイムサーバを利用して時刻同期を設定することができます (**公開 NTP サーバ**)。ローカルの時刻サーバの場合は、**検索** ボタンを押して SLP の問い合わせを送信し、利用可能なタイムサーバが存在しないかどうかを確認することができます。検索結果から適切なタイムサーバを選択し、**OK** ボタンを押してダイアログを完了してください。公開タイムサーバの場合は、ご利用の国 (タイムゾーン) を選んでから **公開 NTP サーバ** の一覧からサーバを選択し、**OK** ボタンを押してダイアログを完了してください。メインダイアログに戻ったあと、選択したサーバとの通信が確立するかどうかを **テスト** ボタンで確認することができます。

次のダイアログで NTP サーバを選択することができます。システムの起動時にサーバとクライアントの間で時刻情報を同期させたい場合は、**このサーバを初期同期に使用する** を選択してください。オプションでは、ntpd に対するさらなるオプションを設定することができます。

アクセス制御オプション を利用すると、お使いのコンピュータ上で動作しているデーモンに対して、遠隔のコンピュータから通信があった場合の動作を制限することができます。この項目は、**セキュリティ設定** タブ内 (図15.3「より高度な NTP クライアント設定: セキュリティ設定」 (309 ページ) をご覧ください) にある **NTP サービスを設定したサーバに制限する** にチェックを入れた場合にのみ設定できます。このオプションは、`/etc/ntp.conf` ファイル内の `restrict` に該当する設定です。たとえば `nomodify notrap noquery` を設定すると、そのサーバからお使いのコンピュータに対して NTP 設定の修正を禁止し、トラップ機能 (遠隔イベントログ機能) を無効化するように設定することになります。このような制限は、接続しようとしているサーバが外部の企業や団体に管理されているもの (たとえばインターネット上のサーバ) である場合に推奨される設定です。

詳しくは `/usr/share/doc/packages/ntp-doc` 内にある文書 (ntp-doc パッケージ内に含まれます) をお読みください。

ピア

ピアとは対称型の同期を行なうようにするための設定で、互いに両方がサーバ兼クライアントとして動作することになります。同じネットワーク内でサーバの代わりにピアを利用する場合は、そのシステムのアドレスを入力してください。残りのダイアログは **サーバ** の場合と同じです。

ラジオクロック

お使いのシステムで、ラジオクロックを時刻同期に利用したい場合の設定です。それぞれクロック種類とユニット番号、デバイス名とその他のオプションを入力してください。ドライバに対して細かい調整を加えるには、*ドライバの調整* を押してください。ローカルに接続された ラジオクロックに関する詳しい操作方法は、`/usr/share/doc/packages/ntp-doc/refclock.html` をお読みください。

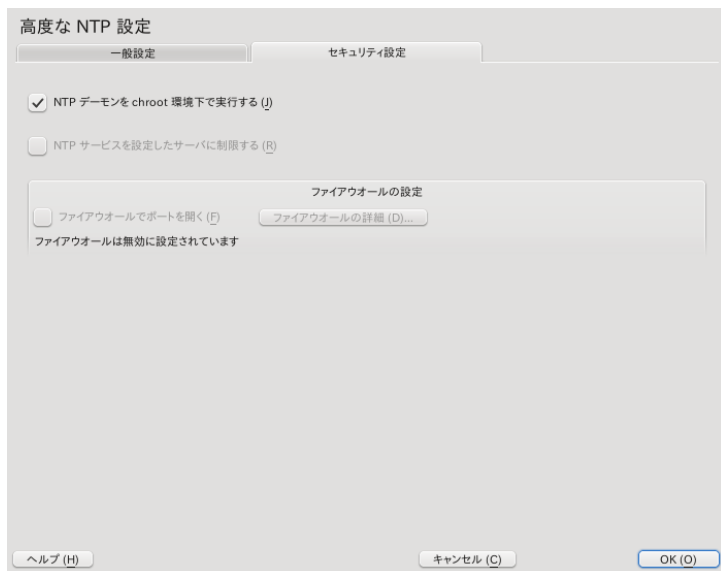
送信ブロードキャスト

時刻情報とその問い合わせを、ネットワーク内のブロードキャスト送信で行なうことができます。この設定では、このようなブロードキャストを送信する際の宛先を指定します。ラジオコントロールの時計など、信頼の おける時刻発信源をお持ちでない場合は、ブロードキャストを有効に設定 しないでください。

受信ブロードキャスト

お使いのクライアントでブロードキャストによる時刻情報受信を行ないたい 場合は、それらのパケットをどこから受信するのかを設定します。

図 15.3 より高度な NTP クライアント設定: セキュリティ設定



セキュリティ設定 のタブ (図15.3「より高度な NTP クライアント設定: セキュリティ設定」(309 ページ) をご覧ください) では、`ntpd` を `chroot` 環境 (文書によっては `chroot jail` と呼ばれる場合もあります) 下で 起動するかどうかを設定することができます。既定では *NTP デーモンを chroot 環境下で実行する* が選択されてい

て、有効になっています。この設定は ntpd に対してセキュリティ欠陥を狙う攻撃に対する防御を高めるもので、たとえ攻撃が成功してもシステム全体にまで被害をもたらさないようにするための仕組みです。

また、*NTP サービスを設定したサーバに制限する* を選択すると、遠隔のコンピュータから NTP の設定を閲覧したり修正したり、リモートイベントログのトラップ機能を使用したりする行為を禁止し、お使いのシステムに対するセキュリティを高めることができます。この選択は全ての 遠隔コンピュータに対して適用されます。ただし時刻の発信源として個別に コンピュータを設定し、*一般設定* タブでアクセス制御 オプションを設定した場合は、そちらの設定が優先されます。それ以外の 遠隔のコンピュータからは、ローカル時刻の問い合わせだけが許可されます。

さらに、SuSEfirewall2 が動作している (既定で起動されます) 場合は、*ファイアウォールでポートを開く* を選択することもできます。ポートを閉じたままにしていると、時刻サーバに対する接続を行なうことができなくなります。

15.2 ネットワーク内にある NTP の手動設定

ネットワーク内の時刻サーバを使用するための最も簡単な方法は、サーバの パラメータを設定することです。たとえば時刻サーバに対して、ntp.example.com という名前でネットワーク内から アクセスできる場合、下記のようにその名前を /etc/ntp.conf に記入するだけです:

```
server ntp.example.com
```

複数の時刻サーバを追加したい場合は 1 行 1 サーバで記述し、各行の行頭にキーワード *server* を付与してください。rcntp start のコマンドで ntpd を 起動すると、おおよそ 1 時間程度で時刻が安定するようになり、ローカルの時刻を 調整するためのドリフトファイルと呼ばれるものが作成されます。ドリフトファイルは、コンピュータの起動後から計算されるハードウェア時刻の変動パラメータで、その調整データは次回以降にすぐに反映されるようになります。これにより、システム 時刻の安定性を高めることができるようになっています。

NTP の仕組みをクライアント側で使用する場合には、2 つの方法が考えられます: 1 つめは既知のサーバに対して定期的な間隔で時刻を問い合わせる方法です。多くのクライアントが存在する場合、このアプローチではサーバの負荷が高くなってしまいます。2 つめはネットワーク内で時刻サーバが NTP ブロードキャストを送信す

るのを待つ方法です。このアプローチの場合はサーバの品質に関する情報が不明で、万が一サーバが誤った情報を配布してしまうと、致命的な問題になってしまいます。

時刻をブロードキャスト経由で取得する場合は、サーバ名を指定する必要はありません。設定ファイル `/etc/ntp.conf` 内に `broadcastclient` と書いた行を追加するだけです。既知の時刻サーバを 1 つ以上設定する場合は、`servers` で始まるサーバ指定を行なってください。

15.3 システム稼働時の動的な時刻同期

ネットワーク接続無しでシステムが稼働している場合、`ntpd` は起動することができないものの、設定ファイル内に設定されている時刻サーバに対して DNS の名前解決をすることができなくなります。これは暗号化された無線 LAN を設定した Network Manager 環境でも発生する問題です。

稼働中に `ntpd` に対して DNS のホスト名解決を行なわせたい場合は、`dynamic` オプションを設定しなければなりません。この場合、起動後にネットワークの接続が確立すると、`ntpd` は名前解決をやり直してタイムサーバにアクセスし、時刻を取得できるようになります。

手作業で `/etc/ntp.conf` ファイルを編集し、`server` の項目 (1 つまたは複数) に対して `dynamic` 句を追加してください:

```
server ntp.example.com dynamic
```

もしくは、YaST を利用して下記のように行なってください:

- 1 YaST を起動して **ネットワークサービス > NTP 設定** を選択します。
- 2 設定したいサーバを選択し、**編集** ボタンを押します。
- 3 **オプション** の項目を選択し、`dynamic` という文字列を追加します。既に何らかのオプションが書かれていた場合は、半角スペースで区切って入力してください。
- 4 編集ダイアログを閉じるには **Ok** ボタンを押します。ここまでの手順を、設定したいサーバ全てに対して繰り返します。
- 5 最後に **Ok** ボタンを押し、設定を保存してください。

15.4 ローカル参照時計の設定

ソフトウェアパッケージ `ntp` には、ローカル参照時計に接続するためのドライバが用意されています。対応している時計の一覧は、`ntp-doc` パッケージ内の `/usr/share/doc/packages/ntp-doc/refclock.html` ファイルに書かれています。各ドライバには番号が振られていて、`ntp` の設定ではその番号に基づく疑似的な IP アドレスを指定します。そのため、`/etc/ntp.conf` の設定ファイルからは、ネットワーク内にそれらの時計が存在するかのような書式になります。疑似 IP アドレスは下記のような形式です: `127.127.t.u` ここで、*t* には時計の種類と使用するドライバを、*u* には使用するインターフェイスをそれぞれ数字で指定します。

通常、それぞれのドライバにはより細かい設定を行なうための特別なパラメータが用意されています。個別のドライバに関する詳しい情報は、`/usr/share/doc/packages/ntp-doc/drivers/driverMM.html` (ここで、*MM* にはドライバの番号が入ります) をお読みください。たとえば「タイプ 8」の時計 (シリアルポートに接続されたラジオ時計) であれば、時計をより細かく指定するための追加モードを指定します。たとえば Conrad DCF77 レシーバモジュールをお使いの場合は、`mode 5` を指定します。また、この時計を優先的に参照させるには、`prefer` キーワードを指定します。Conrad DCF77 モジュールを利用するための `server` 設定は、下記のようになります:

```
server 127.127.8.0 mode 5 prefer
```

他の時計でも同じような指定を行ないます。`ntp-doc` パッケージをインストールすると、`/usr/share/doc/packages/ntp-doc` ディレクトリ内に文書が用意されますので、そちらをお読みください。`/usr/share/doc/packages/ntp-doc/refclock.html` ファイルには、ドライバのパラメータ説明が書かれているドライバページのリンク集があります。

NFS でのファイル共有

ネットワークを介したファイルシステムの公開や共有は、企業内のネットワーク などでは一般的に行なわれているものです。NFS は 電話帳のような機能を提供する NIS プロトコルとともにうまく動作する仕組みです。LDAP と Kerberos を利用した、より機密を保持するプロトコルをお使いになる場合は、NFSv4 に関する項目をお読みください。

NIS と NFS を同時に稼働させると、ユーザに対してネットワークを透過的に見せることができるようになります。NFS ではネットワークを介して任意のファイル システムを公開することができますので、適切な設定を行なうことにより、利用している 端末にかかわらず同じ環境で作業を行なうことができるようになります。

重要: DNS の必要性

原理上、全てのエクスポートは IP アドレスだけを利用して行なわれますが、タイム アウトを防ぐ目的から、DNS システムを動作させる必要があります。また、mountd では逆引きの参照を行なうため、ログ用途でも必要となります。

16.1 用語

YaST モジュールでは、下記のような用語を使用します。

エクスポート

NFS サーバで 公開 されているディレクトリ。クライアント側では、システムの一部として組み込むことができます。

NFS クライアント

NFS クライアントは、NFS サーバの提供するサービスを利用する側の システムを指します。Linux カーネルには最初から TCP/IP プロトコルが 統合されているため、追加のソフトウェアをインストールする必要はありません。

NFS サーバ

NFS サーバは、クライアントに対して NFS サービスを提供する側です。サーバとして動作するには、それぞれ下記のデーモンを起動する必要があります：nfsd (ファイル公開), idmapd (ユーザとグループの 名前を ID に、もしくはその逆の処理を行なう), statd (ファイルの施錠 (ロック)), mountd (マウント要求用)

16.2 NFS サーバのインストール

NFS サーバのソフトウェアは、既定のインストールには含まれていません。16.3項「NFS サーバの設定」(314 ページ) の手順に従って設定を行なうと、必要なパッケージをインストールするように自動的に促されます。また、YaST や zypper を利用して、nfs-kernel-server パッケージをインストールしてもかまいません。

NIS と同様に、NFS もクライアント／サーバ型のシステムです。ただし、1 台の マシンで両方を同時に実行、つまりネットワークを介してファイルシステムを提供 (エクスポート) しながら、かつ他のホストのファイルシステムを取り込む (インポート) ことができます。

16.3 NFS サーバの設定

NFS サーバの設定は YaST から実施することができるほか、手作業でも実施 できます。また、認証については Kerberos と組み合わせることもできます。

16.3.1 YaST を利用したファイルシステムのエクスポート

YaST では、お使いのホストをネットワーク内の NFS サーバとして動作させることができます。NFS サーバとは、アクセス権を設定したホストに対してディレクトリや ファイルを共有 (エクスポート) するということです。これにより、アプリケーションを 各ホ

ストのローカルにインストールすることなく、グループ内の全メンバーに提供することができるようになります。サーバの設定は下記のようにして行ないます：

- 1 YaST を起動して ネットワークサービス > NFS サーバ を選択します。すると、図 16.1「NFS サーバ設定ツール」(315 ページ) のようなダイアログが表示されます。

図 16.1 NFS サーバ設定ツール

NFS サーバの設定

NFS サーバ

☒ 開始 (S)
☐ 起動しない (N)

ファイアウォール

☐ ファイアウォールでポートを開く (F) [ファイアウォールの詳細 \(D\)...](#)

ファイアウォールは無効に設定されています

NFSv4 を有効にする

☒ NFSv4 を有効にする (V)

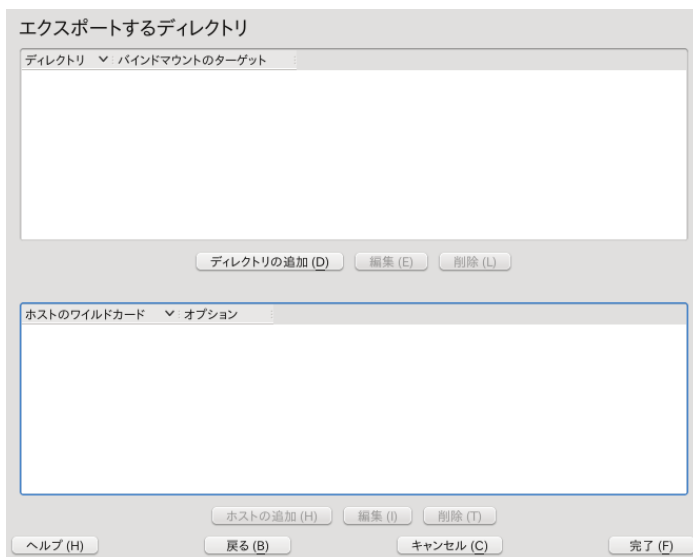
NFSv4 ドメイン名を入力してください (M):
localdomain

☐ GSS セキュリティを有効にする (G)

ヘルプ (H) 戻る (B) キャンセル (C) 次へ (N)

- 2 ダイアログが表示されたら、まずは **開始** のラジオ ボタンを選択してから、**NFSv4 ドメイン名** に 入力を行ないます。
- 3 サーバに対して機密を保持する接続を行ないたい場合は、**GSS セキュリティを有効にする** を選択します。これを行なうには、お使いの ドメインにあらかじめ Kerberos をインストールし、サーバとクライアントの両方で Kerberos の設定を行なっておく必要があります。設定を完了したら **次へ** を押します。
- 4 次に上半分のテキストフィールドでは、エクスポートするディレクトリを入力します。下半分のテキストフィールドでは、それらへのアクセスを許可するホストを指定します。詳しくは 図16.2「YaST を利用した NFS サーバの設定」(316 ページ) をご覧ください。

図 16.2 YaST を利用した NFS サーバの設定



この図では以前のダイアログで NFSv4 を選択した場合のもので、バインドマウントのターゲット が右側に表示されています。詳しくは左側に表示されるヘルプをお読みください。ダイアログの下半分では、各ホストに対して下記の 4 種類のオプションを設定することができます: single host, netgroups, wildcards, IP networks。これらのオプションについて、詳しくは exports のマニュアルページをお読みください。

5 設定を完了するには、完了 ボタンを押します。

重要: 自動的なファイアウォール設定

お使いのシステムでファイアウォール (SuSEfirewall2) が動作している場合、ファイアウォールでポートを開くを選択すると、YaST は nfs サービスを有効化することで ファイアウォールの NFS サーバ向け設定を実施します。

16.3.1.1 NFSv4 クライアント向けのエクスポート

NFSv4 のクライアントに対応するには、NFSv4 を有効にするを選択します。正しくエクスポートされていれば、NFSv3 のクライアントからも アクセスできるようになり

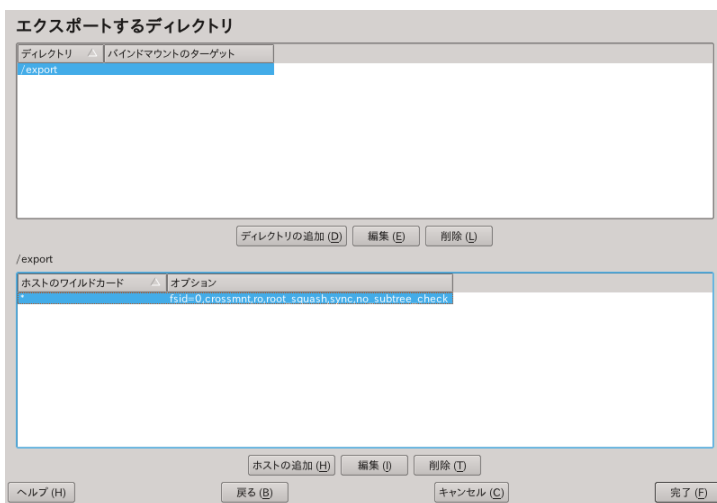
ます。詳しくは 16.3.1.3 項「v3 と v4 エクスポートの共存」(320 ページ) をお読みください。

NFSv4 を有効にしたあとは、適切なドメイン名を入力してください。なお、入力したドメイン名は、NFSv4 クライアント側にある `/etc/idmapd.conf` ファイル内のどこかに存在していることを確認してください。このパラメータは `idmapd` サービスが利用するもので、NFSv4 に対応する場合にサーバおよびクライアントの両方で必要となります。特に要件がなければ、`localdomain` のままでもかまいません。詳しくは 16.5 項「さらなる情報」(327 ページ) にあるリンクをご覧ください。

指定が終わったら **次へ** を押します。すると、2 つのセクション から構成されるダイアログが表示されます。上半分は 2 つの列から構成され、それぞれ **ディレクトリ** と **バインドマウントのターゲット** という名前が設定されています。**ディレクトリ** は直接編集可能な列で、エクスポートするディレクトリを設定します。

クライアントが固定されている場合であれば、2 種類のディレクトリをエクスポートすることができます。1 つは擬似的なルートファイルシステムとして動作するディレクトリ、もう 1 つは疑似ファイルシステムのうちの何らかのサブディレクトリとしてバインドするものとしてエクスポートできます。この擬似的な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する全てのファイルシステムについて、ベースポイントとして動作するようになります。単一または複数のクライアントに対しては、サーバ上のいずれか 1 つのディレクトリだけをエクスポート用に設定することができます。このクライアントの場合は、擬似的なルート内に複数の既存のサブディレクトリをバインドすることで、複数のディレクトリをエクスポートすることができます。

図 16.3 NFSv4 を利用したディレクトリのエクスポート



ダイアログの下半分では、各ディレクトリに対するクライアント（ワイルドカード）とエクスポートオプションを設定します。上半分でディレクトリを追加した後であれば、クライアントとエクスポートオプションを設定する追加ダイアログが自動で表示されます。後から新しいクライアント（クライアントセット）を追加したい場合は、**ホストの追加**を押してください。

開いた小さいダイアログでは、まずホストのワイルドカードを指定します。各ホストに対して、4 種類の方法でワイルドカードを指定することができます：単一ホスト（ホスト名または IP アドレス）、ネットグループ、ワイルドカード（* を指定した場合は全てのマシンを意味します）、IP ネットワークの 4 種類です。次に **オプション** の項目では、疑似ルートディレクトリを作成する場合は `fsid=0` を含めてカンマ区切りのリストを作成します。また設定中のディレクトリが、既に設定済みの疑似ルート下にある他のディレクトリに対し、バインドされる必要がある場合は、`bind=/target/path` のような形式でターゲットのバインドパスをオプション一覧に追加してください。

たとえば `/exports` を疑似ルートディレクトリとして選択し、全てのクライアントに対してサーバへのアクセスを許可する場合を考えます。上半分ではこのディレクトリを追加し、そのオプションには `fsid=0` を設定します。その他のディレクトリ、たとえば `/data` を NFSv4 でエクスポートする必要がある場合も、上半分にディレクトリを追加します。ただし、このディレクトリに対するオプション入力では、一覧の中に `bind=/exports/data` を設定し、`/exports` 以下に `/exports/data` というサブディレクトリが存在していることを確認してください。 `bind=/target/path` オプション内の変更は、追加／変更／削除とも **バインドマウントのターゲット** に反映されます。この列は

直接編集可能ではありませんが、ディレクトリの概要や性質を表わしたものになります。設定を全て完了したら、**完了** を押してください。サービスはすぐに利用できるようになります。

16.3.1.2 NFSv3 と NFSv2 のエクスポート

最初のダイアログでは、**次へ** を押す前に *NFSv4 を有効にする* のチェックが付けられていないことを 確認してください。

次のダイアログは 2 つの部分から構成されます。上半分のテキストフィールドにはエクスポートするディレクトリを入力します。下半分ではそれらにアクセスする権利のあるホストを指定します。各ホストに対して、4 種類の方法でワイルドカードを指定することができます: 単一ホスト (ホスト名または IP アドレス), ネットグループ, ワイルドカード (* を指定した場合は全てのマシンを意味します), IP ネットワークの 4 種類です。

ここでのダイアログは 図16.4「NFSv2 と v3 を利用したディレクトリのエクスポート」(319 ページ) に示されているとおりです。これらのオプションについて、詳しい説明は `man exports` をお読みください。**完了** を押すと設定を完了します。

図 16.4 NFSv2 と v3 を利用したディレクトリのエクスポート

16.3.1.3 v3 と v4 エクスポートの共存

NFSv3 と NFSv4 のエクスポートは、サーバ内で共存させることができます。設定ダイアログの冒頭で NFSv4 を有効に設定したあとは、オプション内に `fsid=0` や `bind=/target/path` が記述されていないものが v3 エクスポートと判断されます。図16.2「YaST を利用した NFS サーバの設定」(316 ページ)にある 設定例から `/data2` のような他のディレクトリを追加する場合は、*ディレクトリの追加* を押し、オプション 内に `fsid=0` や `bind=/target/path` を含めないようにして設定すると、そのエクスポートを v3 エクスポートとして利用できるようになります。

重要

自動的なファイアウォール設定

お使いのシステムでファイアウォール (SuSEfirewall2) が動作している場合、ファイアウォールで *ポートを開く* を選択すると、YaST は nfs サービスを有効化することで ファイアウォールの NFS サーバ向け設定を実施します。

16.3.2 手作業でのファイルシステムのエクスポート

NFS のエクスポートサービスで利用する設定ファイルは、`/etc/exports` と `/etc/sysconfig/nfs` です。これらのファイルに加え、NFSv4 サーバの設定には `/etc/idmapd.conf` ファイルが必要です。また、サービスを 開始したり再起動したりするには、`rcnfsserver restart` コマンドを実行します。このコマンドでサービスを起動すると、`/etc/sysconfig/nfs` で NFSv4 を設定している場合、`rpc.idmapd` についても起動を行ないます。なお、NFS サーバを起動するには RPC portmapper が動作している必要があります。そのため、`rcrpcbind restart` を実行して、portmapper サービスについても起動または再起動を行なってください。

16.3.2.1 NFSv4 を利用したファイルシステムのエクスポート

NFSv4 は openSUSE における最新の NFS プロトコルバージョンです。NFSv4 でディレクトリをエクスポートするための設定は、従来の NFS バージョンの設定とは少し異なります。

/etc/exports

/etc/exports ファイルには項目の一覧が書かれています。それぞれの項目には、共有されるディレクトリと、それをどのように 共有するかを記述します。/etc/exports ファイル での一般的な設定は下記の形式で記述します：

/共有する/ディレクトリ ホスト(オプション)

たとえば、下記のように記述します：

```
/export 192.168.1.2(rw,fsid=0,sync,crossmnt)
/export/data 192.168.1.2(rw,bind=/data,sync)
```

ここで、IP アドレス 192.168.1.2 は利用を許す クライアントを識別するために使用しています。ホスト名を使用することも できますし、ワイルドカードを利用してホストの集合を指定することも できます (* . abc. com や * などのようになります) し、ネットグループを 指定することもできます (@my-hosts) 。

また、fsid=0 を指定したディレクトリは特別な ディレクトリで、エクスポートされるファイルシステムの根幹 (ルート) を形成するものです。これは擬似ルートファイルシステムとも呼ばれ、NFSv4 で正しく動作するには、crossmnt オプションも あわせて設定しなければなりません。NFSv4 経由でエクスポートされる その他全てのディレクトリは、このポイント以下にマウントされなければ なりません。この擬似ルート以下に存在していないディレクトリを エクスポートしたい場合は、エクスポート済みのツリーに結びつける方法をとらなければなりません。このような結びつけは、bind=文法によって行ないます。

たとえば上記の例では /data は /export 以下には存在していませんが、これを エクスポートしたい場合は /export/data としてエクスポートし、そのエクスポート位置に /data を結びつけて (バインドして) エクスポートしてください。なお /export/data ディレクトリは存在していなければ ならず、通常は中には何も存在しないディレクトリであるべきものです。

クライアントからこのサーバにマウントを行なう場合は、servername:/export ではなく servername:/ としてマウントを行ないます。なお、servername:/data をマウントする必要はなく、servername:/ をマウントするだけでそのディレクトリが 見えるようになります。

/etc/sysconfig/nfs

/etc/sysconfig/nfs ファイルには、NFSv4 サーバ デーモンの動作を決定するいくつかのパラメータが含まれています。なお、NFS4_SUPPORT パラメータで yes を設

定しなければならないことに注意してください。と設定することです。NFS4_SUPPORTにより、NFS サーバが NFSv4のエクスポートとクライアントに対応するかどうかが決まります。

/etc/idmapd.conf

Linux マシンにおいて、各ユーザには名前と ID が割り当てられています。idmapd はサーバに対して NFSv4 リクエストが届いた場合に、名前から ID への変換を行ない、クライアントに応答する仕組みを備えています。NFSv4 では名前だけで通信を行なう都合から、サーバとクライアントの両方で動作していなければなりません。

なお、NFS を利用してファイルシステムの共有を行なうマシン間では、ユーザ名と ID (uid) が共通化されるように設定してください。NIS や LDAP などの方法や、それ以外のドメイン認証の仕組みをお使いの環境で利用することで、これを設定することができます。

また、/etc/idmapd.confファイル内の Domain パラメータは、サーバとクライアントで同じになるように設定してください。よくわからない場合は、サーバとクライアントで両方とも既定の localdomain ドメインのままにしておいてください。設定ファイルは、たとえば下記のように なります：

```
[General]
```

```
Verbosity = 0  
Pipefs-Directory = /var/lib/nfs/rpc_pipefs  
Domain = localdomain
```

```
[Mapping]
```

```
Nobody-User = nobody  
Nobody-Group = nobody
```

より詳しい参照先として、idmapd と idmapd.conf の各マニュアルページがあります。それぞれ `man idmapd`, `man idmapd.conf` コマンドでお読みください。

サービスの起動と停止

/etc/exports や /etc/sysconfig/nfs を変更したあとは、`rcnfsserver restart` を実行し、NFS サーバサービスを開始または再起動してください。/etc/idmapd.conf ファイルを変更した場合は、`killall -HUP rpc.idmapd` コマンドで設定ファイルを再読み込みさせてください。

NFS サービスをシステムの起動時に開始させたい場合は、`chkconfig nfsserver on` コマンドを実行してください。

16.3.2.2 NFSv2 と NFSv3 を利用したファイルシステムのエクスポート

この章では、NFSv3 と NFSv2 でのエクスポートについて扱っています。NFSv4 の場合は、16.3.1.1 項「NFSv4 クライアント向けのエクスポート」(316 ページ) をお読みください。

NFS 経由でのファイルシステムのエクスポートを行なうには、2 つの設定 ファイルを編集する必要があります。1 つは `/etc/exports` で、もう 1 つは `/etc/sysconfig/nfs` です。`/etc/exports` ファイルでの一般的な設定は 下記の形式で記述します:

```
/共有する/ディレクトリ   ホスト(オプション)
```

たとえば下記のようになります:

```
/export   192.168.1.2(rw, sync)
```

上記の例では、ディレクトリ `/export` はホスト 192.168.1.2 に対して公開され、オプションとして `rw, sync` が指定されています。上記の IP アドレスは クライアントのホスト名で書くこともできますし、ワイルドカードを利用した指定 (たとえば `*.abc.com`) やネットグループを利用する方法でも指定 することができます。

全てのオプションとそれらの意味について、詳しくは `exports` のマニュアルページをお読みください (`man exports` コマンド で表示することができます)。

`/etc/exports` や `/etc/sysconfig/nfs` を変更したあとは、`rcnfsserver restart` を実行し、nfs サーバサービスを開始または再起動してください。

16.3.3 Kerberos を利用する場合の NFS 設定

NFS の認証として Kerberos を利用するには、まず GSS セキュリティを有効にしなければなりません。これを行なうには、YaST NFS サーバの最初のダイアログで、*GSS セキュリティを有効にする* を選択してください。なお、この機能を利用するには、あらかじめ動作する Kerberos サーバを用意 しておく必要があります。YaST ではサーバを設定することはできず、その機能を利用することしか行なうことができません。YaST の設定に加えて Kerberos の認証を利用したい場合は、NFS の設定を行なう前に少なくとも下記の 手順を実施しておいてください:

- 1 まずサーバとクライアントの両方で、同じ Kerberos ドメインを設定していることを確認します。これは、サーバとクライアントの両方で同じ KDC (鍵配布

センター) を利用し、`krb5.keytab` ファイル (既定ではどのマシンでも `/etc/krb5.keytab` 内に 存在します) を共有しなければならないことになります。Kerberos について、詳しくは 第6章 *Kerberos を利用したネットワーク認証* (↑セキュリティガイド) をお読みください。

- 2 クライアント側で `rcgssd start` コマンドを実行し、`gssd` サービスを起動します。
- 3 さらに `rcsvcgssd start` コマンドを実行し、サーバ上で `svcgssd` サービスを起動します。

NFS を Kerberos 化するための設定について、詳しい情報は 16.5項「さらなる情報」(327 ページ)にある それぞれのリンクを参照してください。

16.4 クライアントの設定

お使いのホストを NFS クライアントとして動作するように設定するにあたっては、特に追加のソフトウェアをインストールする必要はありません。必要なすべてのパッケージは既定でインストールされます。

16.4.1 YaST を利用したファイルシステムのインポート

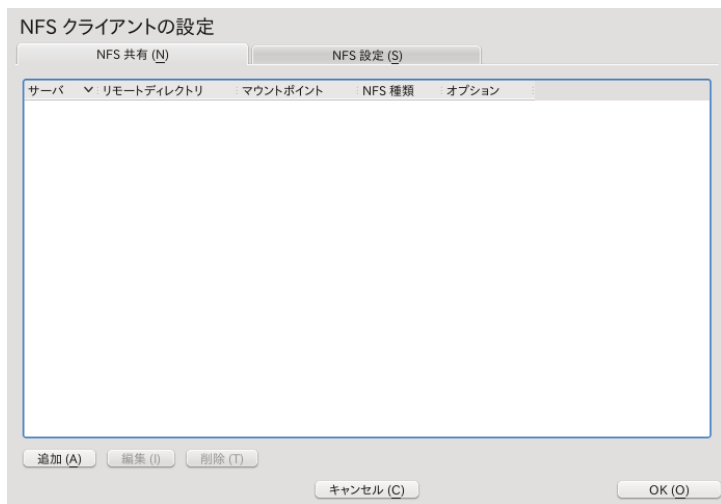
権限を与えられたユーザであれば、YaST NFS クライアントモジュールを利用して NFS サーバからディレクトリをマウントすることができます。これは YaST のモジュールである *NFS クライアント* を利用して行なうことができます。モジュールを起動してから *追加* を押し、NFS サーバのホスト名とインポートする ディレクトリ、そしてどのディレクトリにつなげるかをそれぞれ指定してください。これらの 変更は、最初のダイアログで *完了* ボタンを押した時に実施されます。

また、*NFS 設定* のタブでは、リモートのコンピュータが提供する サービスに対してアクセスを許可するため、*ファイアウォールでポートを開く* を選択することができます。ファイアウォールの状態はチェックボックスの下に表示されます。NFSv4 を利用する場合は、*NFSv4 を有効にする* のチェックが入っているかどうかを確認し、*NFSv4 ドメイン名* に NFS サーバと同じ設定を入力してください。既定ではドメイン名は `localdomain` になっています。

最後に設定を保存するため、*OK* を押します。図16.5「YaST を利用した NFS クライアント設定」(325 ページ)をご覧ください。

設定ファイルは /etc/fstab に書き込まれ、指定したファイルシステム がマウントされます。後から YaST 設定モジュールを起動したときには、このファイルから 既存の設定を読み込みます。

図 16.5 YaST を利用した NFS クライアント設定



16.4.2 手作業でのファイルシステムのインポート

手作業でファイルシステムをマウントするには、事前に RPC portmapper を起動しておく必要があります。RPC portmapper は root から `rcrpcbind start` と入力することで 起動することができます。起動が完了したら、リモート側のエクスポート済みファイル システムは、下記のようにハードディスクをマウントするのに似たコマンドラインで マウントできるようになります：

`mount ホスト:リモート側のパスローカル側のパス`

たとえば `nfs.example.com` マシン上のユーザディレクトリを インポートしたい場合は、下記のようなコマンドを入力します：

```
mount nfs.example.com:/home /home
```

16.4.2.1 automount サービスの利用

autofs デーモンは、リモートのファイルシステムを自動でマウントするのに使用することができます。これを行なうには、お使いの `/etc/auto.master` ファイルに対し、下記のような設定を行ないます:

```
/nfsmounts /etc/auto.nfs
```

上記の設定を行ない、`auto.nfs` ファイルでの設定を行なうと、`/nfsmounts` ディレクトリは全 NFS クライアント側マウントの ルートとして動作するようになります。`auto.nfs` という ファイル名にしたのは単に利便性を考慮しただけのもので、任意の名前を設定することができます。上記で指定したファイル (上記の例では `auto.nfs`) には下記のような項目を記入します:

```
localdata -fstype=nfs server1:/data
nfs4mount -fstype=nfs4 server2:/
```

あとは `root` から `rcautofs start` を実行すると、設定を 反映させることができます。この例では `/nfsmounts/localdata` ディレクトリに `server1` の `/data` ディレクトリを NFS でマウントし、`server2` の `/nfsmounts/nfs4mount` ディレクトリを NFSv4 でマウントします。

autofs が動作している状態で `/etc/auto.master` を編集した場合は、`automounter` に変更を反映させるため、`rcautofs restart` を 実行して再起動を行なわなければなりません。

16.4.2.2 /etc/fstab の手作業での編集

一般的な NFSv3 マウントの場合、`/etc/fstab` には 下記のように設定します:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

NFSv4 マウントについても `/etc/fstab` に設定 することができます。NFSv4 のマウントの場合は、3 つめの列を `nfs` ではなく、`nfs4` と設定し、リモート 側のファイルシステムの指定である 1 列目の `nfs.example.com:` の後が `/` になっていることを確認してください。一般的な NFSv4 マウントの場合、`/etc/fstab` は下記のように なります:

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

`noauto` オプションは、システムの起動時に自動でファイルシステム をマウントしないようにする設定です。上記のようなファイルシステムを手作業でマウント する場合は、マウント時に下記のようなコマンドでマウントポイントだけを指定することで、マウントを行なうことができます:

`mount /local/path`

`noauto` オプションを指定しない場合は、システムの起動時にこれらの ファイルシステムが処理され、マウントされるようになります。

16.5 さらなる情報

`exports`, `nfs`, `mount` の各マニュアルページに加え、NFS サーバやクライアントを設定するための 情報が `/usr/share/doc/packages/nfsidmap/README` ファイルに存在しています。さらなる文書については、それぞれ下記の Web ドキュメントにあります:

- SourceForge [<http://nfs.sourceforge.net/>]: オンラインでの詳細な技術文書 (英語)
- NFS バージョン 4 オープンソース参照実装 [<http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html>]: Kerberos 化した NFS を設定するための手順 (英語)
- Linux NFSv4 よくある質問 (Frequently Asked Questions) [<http://www.citi.umich.edu/projects/nfsv4/linux/faq/>]: NFSv4 について何らかの質問がある場合の参照先。

Samba

Samba を利用することで、Unix マシンを Mac OSX や Windows, OS/2 マシン向けの ファイルサーバ兼印刷サーバとして設定することができます。Samba はそれ単体で 完結する製品であり、それなりに複雑な仕組みを備えています。YaST から Samba を設定することができるほか、SWAT (Web インターフェイス) や設定ファイルを 手作業で編集することでも設定を行なうことができます。

17.1 用語

Samba のドキュメンテーション内、および YaST のモジュールでは、下記に示すいくつかの用語を使用します。

SMB プロトコル

Samba では、NetBIOS と呼ばれるサービスを ベースにした SMB (server message block) プロトコルを利用しています。Microsoft では本プロトコルを公開しているため、他のソフトウェアの製造元から Microsoft のドメインネットワークに接続できるようになっています。Samba では、SMB プロトコルは TCP/IP プロトコル上で動作するようになっているため、全てのクライアントで TCP/IP プロトコルをインストールしなければなりません。

CIFS プロトコル

CIFS (common Internet file system) は Samba でサポートされている もう 1 つのプロトコルです。CIFS はネットワークを介してリモートの ファイルシステムにアクセスするプロトコルで、ユーザグループ内で共同作業を行なうことができるほか、ネットワークを介して文書を共有したりすることができます。

NetBIOS

NetBIOS はマシン間で名前解決サービスを提供するために設計された、通信向け ソフトウェア インターフェイス (API) です。マシンに対してネットワーク内での 名前を予約する機能を持つものです。名前の予約が行なわれると、予約した名前を通してアクセスできるようになります。NetBIOS では名前を集中的に管理する マシンが存在するわけではなく、その名前がネットワーク内で使用されていない ことを確認することで、名前の予約を実現しています。また、NetBIOS の インターフェイスは異なるネットワーク構造でも実装できるような仕組みになっています。実装は NetBEUI と呼ばれる、ネットワークハードウェアに近いプロトコル上で動作するように作られていますが、こちらについても NetBIOS と呼ぶ場合があります。なお NetBIOS で利用可能なプロトコルとしては、Novell 社が開発した IPX プロトコルや、TCP/IP (NetBIOS via TCP/IP) があります。

TCP/IP 上の NetBIOS で利用する名前は、`/etc/hosts` で定義したものや DNS で設定したものとは無関係です。NetBIOS ではこれらの名前 解決方法は利用せず、完全独自の解決方法を利用しています。ただし、管理上の 都合や DNS を併用する都合から、DNS のホスト名と一致させておくことを お勧めします。Samba ではこれが既定で設定されています。

Samba サーバ

Samba サーバは、SMB/CIFS と NetBIOS over IP の名前解決サービスを提供するサーバです。Linux では 3 種類のデーモンを利用します: SMB/CIFS サービスには `smbd` を、名前解決サービスには `nmdbd` を、認証サービスには `winbind` をそれぞれ利用します。

Samba クライアント

Samba クライアントは、SMB プロトコルを利用して Samba サーバにアクセスするシステムのことで、Mac OS X や Windows, OS/2 などが SMB プロトコルに対応しています。なお、各コンピュータには TCP/IP プロトコルをインストールしておかなければなりません。また Samba では多くの UNIX システムに対応する クライアントを提供しています。Linux の場合は SMB 向けのカーネルモジュールが存在し、Linux システムのレベルで SMB 資源を利用することができるようになっています。Samba クライアントの場合は、デーモンを動作させる必要はありません。

共有

SMB サーバがクライアントに資源を提供する場合、共有と呼ばれる方法で提供を行ないます。共有はサーバに設定されたプリンタやディレクトリ (サブディレクトリを含む) を指す言葉で、共有に設定された名前 で資源を公開し、クライアントは その名前 でアクセスを行ないます。共有名には任意の名前を設定するこ

とができ、ディレクトリを公開するにあたってディレクトリとは別の名前を設定することができます。プリンタの場合にも名前を設定し、クライアントからはその名前でアクセスを行いません。

DC

ドメインコントローラ (DC) は、そのドメイン内でのアカウントを処理する サーバです。データの複製を行なうには、追加のドメインコントローラを用意する必要があります。

17.2 Samba サーバのインストール

Samba 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 **ソフトウェア > ソフトウェア管理** を選択してください。ソフトウェア管理のモジュールが起動したら、**フィルタ > パターン** を選択してから **File Server** を選択し、インストールしてください。最後にインストール処理を完了するため、インストールされるパッケージ内容を確認します。

17.3 Samba の起動と停止

Samba サーバは自動で (システムの起動時に) 起動したり停止したりすることができますほか、手動で開始したり停止したりすることができます。起動や停止のポリシーについて 設定を行なうには、YaST の Samba サーバ設定を利用します。詳しくは 17.4.1 項「YaST を利用した Samba サーバの設定」(332 ページ) をお読みください。

YaST から Samba サービスを起動したり停止したりするには、YaST から **システム > システムサービス (ランレベル)** を選択します。そこからそれぞれ winbind, smb, nmb について選択してください。コマンドラインから実施する場合は、`rcsmb stop && rcnmb stop` コマンドを実行すると Samba の停止を、`rcnmb start && rcsmb start` コマンドを実行すると Samba の起動をそれぞれ行なうことができます。なお、rcsmb で winbind の処理を行なうため、winbind について作業を行なう 必要はありません。

17.4 Samba サーバの設定

openSUSE® では、Samba サーバを 2 種類の方法で設定することができます。1 つは YaST を利用した設定、もう 1 つは手作業での設定です。手作業での設定は

より細かい設定を行なうことができますが、YaST の GUI で提供されるような 利便性はありません。

17.4.1 YaST を利用した 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 を選択します。

17.4.1.1 初期の Samba 設定

初回にモジュールを起動したときには *Samba* インストール のダイアログが起動し、まずはサーバの管理に関していくつかの基本設定を行ないます。その手順の最後は Samba の root に対してパスワードを設定することで完了となります。2 回目以降の起動の場合は、*Samba* サーバ設定 ダイアログが開きます。

Samba インストール ダイアログは、以下の 2 つのステップ から構成されます：

ワークグループまたはドメイン名

既存の名前を ワークグループまたはドメイン名 から選択するか、新しい名前を入力して 次へ を押します。

Samba サーバの種類

次のステップでは、お使いのサーバをプライマリドメインコントローラ (PDC)、もしくはバックアップドメインコントローラ (BDC)、非ドメイン コントローラのいずれかで動作させるのかを選択します。指定を終えたら 次へ を押します。

詳細なサーバ設定に移動したくない場合は、ここで *OK* を押してください。あとは最後のポップアップ表示で *Samba* の管理者 (*root*) パスワードを入力します。

このダイアログで設定した項目は、*Samba* 設定 のダイアログ内の *起動*、*共有*、*識別情報*、*信頼するドメイン*、*LDAP の設定* の各タブを利用することで、後から変更することができます。

17.4.1.2 高度な Samba 設定

Samba サーバモジュールを初回に起動すると、17.4.1.1 項「初期の Samba 設定」(332 ページ) で説明しているとおり、*Samba* の設定 ダイアログが表示され、2 段階の手順で設定を行ないます。高度な設定は、この作業を終えた後に設定を調整する場合に利用します。

設定を変更したあとは、*OK* を押すと設定を保存することができます。

サーバの起動

起動 タブでは、Samba サーバの起動方法を設定することができます。お使いのシステムを起動する際にサービスを開始したい場合は、*システム起動時* を選択してください。手作業で開始したい場合は、*手動* を選択してください。Samba サーバの起動方法について、詳しくは 17.3 項「Samba の起動と停止」(331 ページ) をお読みください。

また、このタブでは、お使いのファイアウォールでポートを開く設定を行なうこともできます。これを行なうには、*ファイアウォールでポートを開く* を選択してください。お使いの環境に複数のネットワークインターフェイスが存在する場合は、*ファイアウォールの詳細* を押してネットワーク インターフェイスを選択し、*OK* を押してください。

共有

共有 タブでは、有効化する Samba 共有を設定することができます。共有の中には、ホームディレクトリやプリンタなど、いくつか事前に設定されているものが存在します。共有を選択して *状態変更* を押すと、*有効* と *無効* を切り替えることができます。*追加* を押すと新しい共有を追加することができますし、*削除* を押すと選択した共有を削除することができます。

ユーザにディレクトリの共有を許可する を選択すると、*許可するグループ* のメンバーが、自分自身の ディレクトリを他のユーザに公開できるようになります。たとえばローカルのグループを設定する場合は *users* のように、ドメインのグループを設定する場合は *DOMAIN\Users* のように指定します。なお、各ユーザはファイルシステム側のパーミッション 設定でも、アクセスを許可していなければならないことに注意してください。また、*最大共有数* では、作成可能な共有数の上限を設定することができます。ユーザが作成した共有に対して認証無しでアクセスできるようにしたい場合は、*ゲストアクセス可能* を選択してください。

識別情報

識別情報 タブでは、そのホストに対して関連づけるドメインを設定することができます (*基本設定* 内)。また、ネットワーク内で代替のホスト名を利用したい場合も、ここで設定を行ないます (*NetBIOS* ホスト名)。このタブでは、名前解決に Microsoft Windows Internet Name Service (WINS) を利用するかどうかを設定することもできます。これを利用する場合は、*ホスト名の解決に WINS を使用する* を選択し、必要に応じて *DHCP* で *WINS* サーバのアドレスを取得

度なグローバル設定やユーザ認証ソースを設定したい場合は、*詳細設定* を押してください。

信頼するドメイン

他のドメインのユーザに対してお使いのドメインにアクセスできるようにするには、*信頼するドメイン* タブ内で必要な設定を行ないます。新しいドメインを追加するには *追加* ボタンを、選択したドメインを削除するには *削除* ボタンを押します。

LDAP の設定

LDAP の設定 タブでは、認証に使用する LDAP サーバについて設定を行なうことができます。LDAP サーバとの接続をテストするには、*接続のテスト* ボタンを押してください。高度な LDAP 設定を行なう場合や、既定の値を使用したい場合は、*詳細設定* を押してください。

LDAP の設定について、詳しくは 第4章 *ディレクトリサービス LDAP* (↑セキュリティガイド) をお読みください。

17.4.2 SWAT を利用した Web 管理

Samba サーバを管理するための代替ツールとして、SWAT (Samba Web Administration Tool) があります。SWAT はシンプルな Web インターフェイスを提供するもので、Samba サーバを設定する機能を提供します。SWAT を利用するには、root ユーザになっている状態で Web ブラウザから <http://localhost:901> を Web ブラウザで開いてください。Samba 用の root アカウントを設定していない場合は、システムの root アカウントをお使いください。

注記: SWAT の有効化

初期段階の Samba サーバインストールを完了しても、SWAT は有効化されません。SWAT を有効化するには、YaST から *ネットワークサービス > ネットワークサービス (xinetd)* を開き、ネットワークサービスの設定を開いてください。その状態から一覧内にある *swat* を選択し、*状態を変更する (オン/オフ)* を押して切り替えてください。

17.4.3 手作業でのサーバ設定

Samba をサーバとして利用したい場合は、samba パッケージをインストールしてください。Samba で中心となる設定ファイルは `/etc/samba/smb.conf` で、このファ

イルは大きく分けて 2 つのパートから構成されています。[global] セクション にはサーバ全体の設定が含まれ、[share] セクションでは 個別のファイルまたはプリンタ共有に関する設定が含まれています。この設定の 仕組みにより、共有に関する詳細設定と [global] セクションの 設定はそれぞれ別々に行なうことができるため、設定ファイルの構造的な透過性が 保たれるようになっています。

17.4.3.1 グローバルセクション

[global] セクション内の下記のパラメータは、お使いのネットワーク環境に合わせて変更すべき箇所で、Windows 環境の 他のマシンからお使いの Samba サーバにアクセスするため、必要な項目です。

workgroup = TUX-NET

この行では、Samba サーバに対してワークグループを設定しています。お使いの環境にあわせて TUX-NET を適切な文字列に 変更してください。その名前が別のマシンに割り当てられていない限り、ご利用の Samba サーバは DNS に登録した名前で現われるようになります。DNS に名前を登録することができない場合は、netbiosname=名前 の書式でサーバ名を設定してください。このパラメータについて、詳しくは smb.conf のマニュアルページをお読みください。

os level = 20

このパラメータは、お使いの Samba サーバがワークグループ内の LMB (ローカルマスターブラウザ) になるかどうかを指定するものです。Samba バージョン 3 シリーズでは、既定の値 (20) を上書き する必要はほとんどありません。また、誤った Samba サーバの設定によって 既存の Windows ネットワークが混乱することを防ぐため、2 のようなとても低い値に設定しておいてください。この話題について、詳しくは Samba 3 Howto 内の Network Browsing (ネットワークブラウズ) 関連の章をお読みください。Samba 3 Howto については 17.7 項「さらなる情報」(341 ページ)をお読みください。

お使いのネットワーク内に他の SMB サーバ (Windows 2000 Server など) が存在しない場合や、ローカル環境の全システムの一覧を Samba サーバで管理したい場合は、os level の値をより高い値に設定してください (たとえば 65 など)。これによりお使いの Samba サーバは、ローカルネットワーク内での LMB として動作するようになります。

なお、この設定を変更する場合は、既存の Windows ネットワーク環境にどのような 影響があるのかをよく確かめてから行なってください。まずは本番の環境とは 切り離されたネットワークやそれほど重要ではないネットワークで、設定を試して みてください。

wins support と wins server

お使いの Samba サーバを WINS サーバの存在する既存の Windows ネットワークに追加する場合は、wins server オプションを有効に設定し、WINS サーバの IP アドレスを設定してください。

お使いの Windows マシンが別のサブネットに接続されていて、Samba サーバとは互いに存在を通知しあいたい場合は、WINS サーバを設定する必要があります。Samba サーバで WINS サーバの機能を動作させるには、wins support = Yes のオプションを設定してください。なお、同じネットワーク内では 1 台までの Samba サーバで有効に設定してください。また、smb.conf ファイルでは wins server と wins support の両方をいっぺんに設定してはなりません。

17.4.3.2 共有

下記の例では、CD-ROM ドライブとユーザディレクトリ (homes) を SMB クライアントに公開する場合を想定し、設定例を示しています。

[cdrom]

CD-ROM ドライブを誤って共有してしまうことを防ぐため、下記の行はコメントマークを利用して無効化してあります (この設定ファイルの場合はセミコロンを書きます)。CD-ROM ドライブを Samba で共有する場合は、各行の冒頭にあるセミコロンを取り除いてください。

例 17.1 CD-ROM 共有 (無効化)

```
:[cdrom]
;      comment = Linux CD-ROM
;      path = /media/cdrom
;      locking = No
```

[cdrom] と comment

[cdrom] の項目は、ネットワーク上から SMB クライアントが参照する名前です。comment 行を利用することで、さらに細かい説明を追加することができます。

path = /media/cdrom

path オプションでは、/media/cdrom ディレクトリを公開するよう指定しています。

なお、既定の設定は安全性を第一に考えられたものであるため、これらの共有はこのシステムに存在するユーザに対してのみ公開されます。この共有を誰にでも利用できるようにするには、設定内に guest ok = yes という行を追加し

てください。この設定を行なうことで、ネットワーク内の 誰にでも読み取りアクセスを許可できるようになります。なお、このパラメータを利用するにあたっては、[global] セクションでの設定 よりも優先して動作することにご注意ください。

[homes]

[homes] 共有は特別な意味を持つ共有です。Linux の ファイルサーバ内に有効なアカウントとパスワードが存在し、かつそのユーザが ホームディレクトリを持っていれば、この共有にアクセスできるようになります。

例 17.2 [homes] 共有

```
[homes]
comment = Home Directories
valid users = %S
browseable = No
read only = No
create mask = 0640
directory mask = 0750
```

[homes]

SMB サーバに対して接続しているユーザと同じ名前の共有が存在しない限り、[homes] 共有の設定で共有が動的に生成されます。共有の名前はユーザ名と同じです。

valid users = %S

%S は接続が正しく行なわれたときに実際の共有名に 置き換えられる部分で、[homes] の共有では常に ユーザ名に置き換えられます。そのため、ユーザ名の共有はそのユーザに 対してだけ許可される仕組みになっています。

browseable = No

この設定を行なうと、ネットワーク環境から参照することができない ようになります。

read only = No

既定では Samba は read only = Yes の設定が有効に なっていて、いかなる共有に対する書き込みアクセスも禁止される仕組みに なっています。共有に書き込みできるようにするには、read only = No を設定してください。writable = Yes でも同じ設定になります。

create mask = 0640

MS Windows NT をベースにしていないシステムでは UNIX のパーミッションを解釈することができないため、ファイルを作成する際に割り当てるパーミッションを設定しておく必要があります。create mask のパラメータ

では、新しく作成するファイルに対して 設定するパーミッションを設定します。なお、この設定は書き込み可能な 共有に対してのみ効果がある項目です。上記の設定では、所有者自身は読み込み および書き込みの権限を持ち、所有者のプライマリグループのメンバーは 読み込みの権限だけを持ちます。ただし、valid users = %S の設定が存在するため、グループに対して読み込み権限があるものの、その 権限は実際には有効になりません。グループに対して読み込みや書き込みの 権限を与えるには、valid users = %S の行を 無効化する必要があります。

17.4.3.3 セキュリティレベル

セキュリティを改善するため、それぞれの共有にはパスワードを設定することができ
ます。SMB では下記の方法で許可をチェックすることができます：

共有レベルセキュリティ (security = share)

共有に対してパスワードを設定します。このパスワードを知っている ユーザだけが、この共有にアクセスできます。

ユーザレベルセキュリティ (security = user)

この設定は SMB のユーザに対する考え方を提供するものです。この設定では、あらかじめ各ユーザをサーバに登録し、パスワードを設定しなければなりません。登録後、サーバはそのユーザ名に対して許可した共有にアクセスできるようになります。

サーバレベルセキュリティ (security = server)

クライアントに対しては、Samba はユーザレベルと同じ振る舞いを見せます。ただしユーザレベルセキュリティとは異なり、入力されたパスワードは他のサーバに転送され、そこで認証を行ないます。この設定の場合、追加の password server パラメータを設定する必要があります。

ADS レベルセキュリティ (security = ADS)

このモードでは、Samba は Active Directory 環境のドメインメンバーとして 動作します。このモードで動作するには、Samba の動作するマシンに Kerberos をインストールし、設定しておかなければなりません。また、そのマシンは Samba を利用して ADS の領域に参加しなければなりません。これらの設定は、YaST *Windows* ドメインメンバーシップ モジュールから 行なうことができます。

ドメインレベルセキュリティ (security = domain)

このモードは、そのマシンが Windows NT ドメインに参加している場合にのみ動作します。この設定で Samba は、ユーザ名とパスワードを Windows NT の

プライマリまたはバックアップのドメインコントローラに送信し、検証を行いません。これは Windows NT Server が行なう方法と同じです。なお、暗号化パスワードを指定するパラメータについて、yes に設定する必要があります。

共有／ユーザ／サーバ／ドメインの各レベルのセキュリティは、サーバ全体に適用されます。共有レベルのセキュリティとユーザレベルのセキュリティを混在させた共有を設定してサーバ設定を行なうことはできません。ただし、システムに設定した各 IP アドレスに対し、別々の Samba サーバを設定して起動することは可能です。

この種類の話題について、より詳しい情報は Samba 3 HOWTO に書いてあります。1 つのシステムで複数のサーバを立ち上げる場合は、`interfaces` と `bind interfaces only` の各オプションについて注意して設定してください。

17.5 クライアントの設定

Samba クライアントでは、TCP/IP で提供される Samba サーバにのみアクセスすることができます。NetBEUI や IPX 上の NetBIOS ではアクセスできません。

17.5.1 YaST を利用した Samba クライアントの設定

Samba サーバや Windows サーバ上に存在する資源 (ファイルやプリンタ) にアクセスするには、Samba クライアントを設定します。ネットワークサービス > *Windows ドメインメンバーシップ* で表示されるダイアログで、それぞれ NT ドメインや Active Directory ドメイン、または ワークグループ名を入力してください。*Linux の認証にも SMB の情報を使用する* を選択すると、ユーザ認証を Samba や NT、または Kerberos サーバ上で行なうようになります。

高度な設定オプションを表示するには、*熟練者向け設定* を押します。たとえば認証時にサーバのホームディレクトリを自動でマウントしたい場合は、*サーバディレクトリのマウント* を選択します。この方法を利用することで、ユーザは CIFS 経由で提供されたホームディレクトリにアクセスできるようになります。詳しくは `pam_mount` のマニュアルページをお読みください。

全ての設定を終えたら、*完了* を押して設定を完了してください。

17.6 ログインサーバとしての Samba の利用

主として Windows クライアントが多く存在するネットワークでは、有効なアカウントとパスワードだけを登録しておくことが望めます。Windows ベースのネットワークでは、これはプライマリドメインコントローラ (PDC) を利用して行ないます。PDC として設定済みの Windows NT server を利用して設定することもできますが、Samba サーバを利用することでもこの作業を行なうことができます。なお、smb.conf ファイル内の [global] セクションに対し、例 17.3「smb.conf のグローバルセクション」(340 ページ) で示されるような設定を行なっておかなければなりません。

例 17.3 smb.conf のグローバルセクション

```
[global]
    workgroup = TUX-NET
    domain logons = Yes
    domain master = Yes
```

ユーザ認証時に暗号化パスワードを利用する場合、Samba サーバでもこれを有効に設定しなければなりません。[global] セクション内で encrypt passwords = yes を設定することでこれを実現することができます (Samba バージョン 3 では、これが既定値になっています)。また Windows の慣習に従うため、ユーザアカウントとパスワードの情報についても暗号化した書式が必要になります。これを行なうには、smbpasswd -a name を実行してください。また、Windows のドメインの考え方が必要となる、ドメイン内のコンピュータアカウントを作成するには、下記のコマンドを実行します：

```
useradd hostname%$
smbpasswd -a -m hostname
```

なお、useradd コマンドにドル記号が追加されていることに注意してください。smbpasswd コマンドについては、-m パラメータを指定することで自動的にドル記号が追加されます。設定例 (/usr/share/doc/packages/samba/examples/smb.conf.SUSE) のコメント内に、この処理を自動化するための設定が書かれています。

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" %
-s /bin/false %m%$
```

Samba サーバで上記のスクリプトを正しく実行できるようにするため、Samba ユーザに対して必要な管理者権限と ntadmin グループへの追加を行なってくださ

い。これを行なったあと、この Linux グループに属する 全ユーザを Domain Admins に割り当てるため、下記のコマンドを実行します:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

この種類の話題について詳しい情報は、Samba 3 HOWTO 内の第 12 章に書かれています。/usr/share/doc/packages/samba/Samba3-HOWTO.pdf をお読みください。

17.7 さらになる情報

Samba に関する詳細な情報は、デジタル文書で提供されています。コマンドラインから `apropos samba` を実行して 複数のマニュアルページを参照するか、Samba のドキュメンテーションがインストール されている場合は、/usr/share/doc/packages/samba ディレクトリ内をお読みのうえ、オンライン文書と設定例を参照してください。examples サブディレクトリ内には、コメントの付けられた設定例 ファイル (smb.conf, SUSE) があります。

また、Samba チーム提供の Samba 3 HOWTO には、トラブルシューティングに関する章があります。これに加え、文書の Part V には設定を確認するための手順が書かれています。Samba 3 HOWTO は samba-doc パッケージに含まれ、/usr/share/doc/packages/samba/Samba3-HOWTO.pdf ファイル からアクセスすることができます。

また、openSUSE wiki の Samba ページ <http://ja.opensuse.org/Samba> についてもお読みください。

Apache HTTP サーバ

Apache HTTP サーバ (Apache) は、<http://www.netcraft.com/> の調査によると 50% 以上ものシェアを持つ Web サーバで、世界で最もよく使用されている Web サーバです。Apache Software Foundation (<http://www.apache.org/>) で開発されている Apache は 多くのオペレーティングシステムで利用することができます。openSUSE® には Apache バージョン 2.2 が含まれています。この章では、Apache Web サーバのインストールから設定、SSL や CGI の使用方法、およびトラブル発生時の解決方法について、それぞれ言及しています。

18.1 クイックスタート

この章を読み進めていくことで、Apache の設定と起動を簡単に行なうことができます。Apache のインストールと設定は、root の状態から行ないます。

18.1.1 事前要件

Apache Web サーバを設定する前に、下記の要件を全て満たしていることをご確認ください:

1. 対象となるマシンのネットワーク設定が正しく行なわれていることを確認してください。詳しくは 第11章 *ネットワークの基礎* (205 ページ) をお読みください。
2. 対象となるマシンのシステム時刻が、タイムサーバを利用して正確に同期できていることを確認してください。これは、HTTP プロトコルがシステムの時刻に依存して動作していることによるものです。詳しくは 第15章 *NTP を利用した時刻同期* (305 ページ) をお読みください。

3. 最新のセキュリティ更新がインストールされていることを確認してください。YaST オンライン更新を利用することで、最新かどうかを確認することができます。
4. 既定の Web サーバポート (ポート 80) がファイアウォールで 開くように設定されていることを確認してください。これを行なうには、SuSEFirewall2 で外部ゾーンに対し、*HTTP* サーバを許可するよう設定する必要があります。この作業は YaST から行なうことができます。詳しくは 項「YaST を利用したファイアウォールの設定」(第13章 マスカレードとファイアウォール, ↑セキュリティガイド) をお読みください。

18.1.2 インストール

openSUSE において、Apache は既定ではインストールされません。「すぐに使うことのできる」標準設定でインストールを行なうには、下記の 手順を行ないます:

手順 18.1 既定の設定での Apache インストール

- 1 YaST を起動し、ソフトウェア > ソフトウェア管理 を選択します。
- 2 フィルタ > パターン を選択し、サーバ機能 内の Web および LAMP サーバ を選択します。
- 3 依存関係のパッケージのインストールについて確認を行ない、インストール処理を完了します。

上記の手順でのインストールには、PHP5 モジュールと apache2-prefork マルチプロセッシングモジュールと PHP5 モジュールが含まれています。モジュールについて、詳しくは 18.4項「モジュールのインストール／有効化／設定」(364 ページ) をお読みください。

18.1.3 起動

Apache はシステムの起動時に自動起動するように設定することができるほか、手動で 起動するようにも設定できます。

手順 18.2 Apache の自動起動設定

- 1 まずはランレベル 3 および 5 で システムが起動する際、Apache が自動的に起動するかどうかを確認します。具体的には下記のコマンドを入力します:

```
chkconfig -a apache2
```

- 2 上記以外にも、YaST を起動して **システム > システム サービス (ランレベル)** を選択することでも設定することができます。
- 3 *apache2* の項目を探し、**有効にする** ボタンを押してサービスを有効に設定します。

これで Web サーバが即時に起動します。

- 4 最後に設定を保存するため、**完了** ボタンを押します。

これでシステムの起動時、ランレベルが 3 および 5 であれば Apache が自動で起動するようになります。

シェルを利用して Apache を手動で起動するには、`rcapache2 start` コマンドを実行します。

手順 18.3 *Apache が起動しているかどうかの確認*

Apache の起動時に何もエラーメッセージが表示されていなければ、通常 Web サーバ は起動している状態になっているはずです。確認は下記の手順で行ないます:

- 1 ブラウザを起動し、<http://localhost/> を開きます。

Apache が起動していて問題なく動作していれば、「It works!」で始まるテストページが表示されるはずです。

- 2 上記のページが表示されない場合は、18.8項「トラブルシューティング」(384 ページ) をお読みください。

これで Web サーバを起動することができました。必要なドキュメントを追加したり、必要に応じて設定を調整したり、モジュールをインストールして機能を追加したり することができるようになっています。

18.2 Apache の設定

openSUSE における Apache は、2 種類の方法で設定することができます:

- Apache の手作業による設定 (349 ページ)
- YaST を利用した Apache の設定 (354 ページ)

手作業での設定ではより細かい設定を行なうことができますが、YaST GUI のような利便性は 備わっていません。

重要: 設定変更後の Apache の再読み込みまたは再起動について

設定のうちの多くは、変更された設定を反映するために Apache の再読み込み (または再起動) が必要です。手作業で Apache を再読み込みさせるには、`rcapache2 reload` コマンドを実行するか、もしくは 18.3 項「Apache の起動と停止」(361 ページ) に書かれている再起動オプションを利用します。

YaST を利用して Apache を設定する場合、18.2.3.2 項「HTTP サーバ設定」(359 ページ) に書かれている *HTTP サービス* が *有効* に設定されていると、YaST が自動で判断して処理を行ないます。

18.2.1 Apache の設定ファイル

この章では、Apache の設定ファイルについて概要を示しています。YaST を利用して 設定を行なう場合は、これらのファイルを直接操作する必要はありません—ただし、後から手作業による設定に切り替える場合に備え、これらの情報を知っておくとよい でしょう。

Apache の設定ファイルは 2 箇所の異なる場所に配置されています:

- `/etc/sysconfig/apache2` (346 ページ)
- `/etc/apache2/` (347 ページ)

18.2.1.1 `/etc/sysconfig/apache2`

`/etc/sysconfig/apache2` では、読み込むべきモジュール や取り込むべき追加設定ファイル、サーバ起動時の設定フラグやコマンドラインに 追加すべきフラグなど、Apache に関するいくつかのグローバル設定を保持しています。このファイル内にある各設定オプションは詳しくドキュメント化されているため、ここでは敢えて説明を行ないません。一般用途の Web サーバであれば、`/etc/sysconfig/apache2` 内にある設定だけで十分に 要件を満たすことができます。

18.2.1.2 /etc/apache2/

/etc/apache2/ では Apache に必要な全ての設定ファイル を保持しています。下記ではこのディレクトリ以下にある各ファイルの目的について 説明を行ないます。各ファイルにはいくつかの設定オプション (ディレクティブと表現する場合があります) が含まれていて、これらのファイルに含まれる設定 オプションは詳しくドキュメント化されているため、ここでは一つずつの設定 オプションについて説明を行なうことはしません。

Apache の設定ファイルは下記のような構成になっています:

```
/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.conv

様々な言語に対して使用する文字セットを指定するファイルです。編集を行なってはけません。

conf.d/*.conf

他のモジュールから追加される設定ファイルです。これらの設定ファイルは、必要に応じてお使いの仮想ホスト設定から取り込むことができます。例として

vhosts.d/vhost.template ファイルを お読みください。これを行なうことで、それぞれの仮想ホストで別々の モジュールを利用することができます。

default-server.conf

全ての仮想ホストに適用されるグローバルな設定で、多くの既定値が設定されています。これらの値を変更するのではなく、各仮想ホスト側の設定で 設定を上書きしてください。

errors.conf

Apache がどのようにしてエラー応答を行なうのかを指定します。全ての仮想ホストに対してエラーメッセージをカスタマイズするには、このファイルを 編集してください。お使いの各仮想ホストの設定内でこれらを上書きすること もできます。

httpd.conf

Apache サーバの設定ファイルのメインです。このファイルについては変更 は避けてください。このファイルは主にグローバルな設定を取り込む ための仕組みを用意しています。それぞれのグローバルな設定を変更する 際は、この一覧内にある適切な設定ファイルに設定してください。また、各仮想ホストの設定 (たとえばドキュメントルートなど) は、仮想ホストの 設定で行なってください。

listen.conf

Apache に対して、待ち受けるべき IP アドレスとポートを指定するファイルです。名前ベースの仮想ホストについても、こちらで設定を行ないます。詳しくは「名前ベースの仮想ホスト」(351 ページ) をお読みください。

magic

mime_magic モジュールが使用するデータで、Apache が未知のファイルについて MIME タイプを自動判別するのに使用します。変更しないでください。

mime.types

システムで既知となっている MIME タイプの一覧です (実際には /etc/mime.types へのリンクになっています)。編集はしないでください。ここに記載されていない MIME タイプを新しく 追加したい場合は、mod_mime-defaults.conf ファイルに追記してください。

mod_*.conf

既定でインストールされるモジュール向けの設定です。詳しくは 18.4 項「モジュールのインストール／有効化／設定」(364 ページ) をお読みください。なお、任意指定のモジュールに関する設定は、conf.d ディレクトリ内にあります。

server-tuning.conf

様々な MPM (MPM については 18.4.4 項「マルチプロセッシングモジュール (MPM)」(369 ページ) をお読みください) に対する設定ディレクティブが含まれているほか、Apache の性能を決める一般的な設定オプションが含まれています。これらの項目について変更する場合は、よくテストを行なってください。

ssl-global.conf and ssl.*

グローバルな SSL 設定と SSL の証明書データが含まれています。詳しくは 18.6 項「SSL で通信の機密を保持する Web サーバの設定」(375 ページ) をお読みください。

sysconfig.d/*.conf

/etc/sysconfig/apache2 の設定から自動生成された設定ファイルです。これらのファイルは直接編集を行わず、/etc/sysconfig/apache2 ファイルのほうを編集してください。また、このディレクトリには自動生成されるファイル以外は配置してはなりません。

uid.conf

Apache が動作する際のユーザおよびグループ ID を指定するファイルです。変更はしないでください。

vhosts.d/*.conf

構築したい仮想ホストの設定をここに配置します。このディレクトリには SSL 無しの場合と有りの場合の両方について、仮想ホストの雛型ファイルが含まれています。また、このディレクトリ内に存在し、.conf で終わるファイルは、Apache の設定内に自動で取り込まれる仕組みになっています。詳しくは 18.2.2.1 項「仮想 (バーチャル) ホストの設定」(349 ページ) をお読みください。

18.2.2 Apache の手作業による設定

Apache を手作業で設定する場合、ユーザ root からテキスト形式の設定ファイルを編集して行ないます。

18.2.2.1 仮想 (バーチャル) ホストの設定

仮想ホストとは、1 台の Apache から複数の URI (統一資源識別子) に対するサービスを提供する仕組みです。たとえば `www.example.com` と `www.example.net` のように、物理的に 1 台だけのマシンで動作する単一の Web サーバで、複数のドメインを取り扱うこともできます。

仮想ホストは、管理面の手間を省くため (管理する Web サーバを 1 台にまとめることができる) と、ハードウェアの費用を削減するため (各ドメインで専用の サーバを必要としない) に使用します。仮想ホストはホスト名 (名前ベース) を 基準に設定することができるほか、IP アドレスを基準にしたりポート番号を基準 にしたりすることもできます。

全ての設定済み仮想ホストを表示するには、`httpd2 -S` を利用します。これにより既定のサーバと全ての仮想ホストが表示され、それらの IP アドレスやポート番号などがあわせて表示されます。さらに、設定ファイル 内で仮想ホストが設定されている場所についても表示されます。

仮想ホストは「仮想ホスト」(357 ページ) に書かれている手順で YaST から設定することができるほか、設定ファイルを手作業で 変更することによっても設定できます。openSUSE の既定では、仮想ホストごとに 1 つの 設定ファイルを `/etc/apache2/vhosts.d/` 内に作成する 仕組みになっています。このディレクトリ内にあり、かつファイル名が `.conf` で終わるファイルは、自動的に設定として 取り込まれるようになっています。また、仮想ホストを設定する際のテンプレート についても、このディレクトリ内に配置されています。それぞれ `vhost.template` (SSL 無し) と `vhost-ssl.template` (SSL 有り) のファイルがあります。

ヒント: 仮想ホストの設定の必要性について

設定しようとしている Web サーバが 1 つのドメインだけをまかなうものであった場合であっても、仮想ホストの設定ファイルを常に作成しておくことをお勧めします。これを行なうと、ドメイン固有の設定を別途のファイルに分けて保存することになる ので、単純に仮想ホストの設定ファイルを移動／削除／名前変更するだけで、うまく 動作していたはずの元の基本設定に戻すことができるようになります。また同じ 理由から、仮想ホストごとに別々の設定ファイルを作成してください。

なお名前ベースの仮想ホストを使用する場合、どの仮想ホスト設定にも該当しないドメイン名でアクセスが行なわれた場合に対して、既定の仮想ホスト設定を追加して おくことをお勧めします。既定の仮想ホストは設定ファイルとして最初に読み込まれるファイルで、設定ファイルの読み込み順序はファイル名で判断される 仕組みになっています。そのため、アンダースコア文字 (`_`) で 始まるファイル (たとえば `_default_vhost.conf`) を 作成して設定することをお勧めします。

`<VirtualHost></VirtualHost>` のブロックには、それぞれのドメインに適用される情報が記載されています。Apache が設定済みのホストに対するリクエストを受け取ったときは、このセクション 内のディレクティブを参照します。この仮想ホスト設定の内側では、ほとんど全ての ディレクティブを参照することができます。Apache の

設定ディレクティブについて、詳しくは <http://httpd.apache.org/docs/2.2/mod/quickreference.html> をお読みください。

名前ベースの仮想ホスト

名前ベースの仮想ホストの場合、IP アドレス 1 つに対して複数の Web サイトを構築することができます。この方法では、Apache はクライアントから送信された ホスト名フィールドと各仮想ホスト内の ServerName を比較し、一致する仮想ホストを検索します。ServerName に該当するものが存在しない場合、最初に設定した仮想ホストを既定のホストとして 使用します。

また、NameVirtualHost ディレクティブは Apache に対し、IP アドレスや (必要であれば) ポート番号のほか、HTTP ヘッダ内に含まれる ホスト名フィールドでも仮想ホストを使用するよう設定します。このオプションは設定ファイル /etc/apache2/listen.conf 内で設定します。

NameVirtualHost に設定する最初のパラメータは 完全修飾ドメイン名ですが、IP アドレスで設定することをお勧めします。2 番目の パラメータはポート番号で、必ずしも指定する必要はありません。既定では Listen ディレクティブでの設定から、ポート 80 を使用します。

また IP アドレスやポート番号の指定には、ワイルドカード * を指定することもできます。この場合は全てのインターフェイスに対するリクエストを仮想ホストとして設定することを意味します。また、IPv6 アドレスを設定する 場合は、大括弧で括らなければなりません。

例 18.1 様々な名前ベースの VirtualHost 設定

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.3.100:80
NameVirtualHost 192.168.3.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:364::]:80
```

VirtualHost の開始タグのパラメータには、NameVirtualHost で設定した IP アドレス (または 完全修飾ドメイン名) を指定します。NameVirtualHost で設定したポート番号については任意指定です。

IP アドレスの代用として、ワイルドカード * を指定する こともできます。このワイルドカードは NameVirtualHost * を設定した場合にのみ利用できます。IPv6 アドレスを利用する場合、そのアドレス 指定は大括弧で括らなければなりません。

例 18.2 *Name-Based VirtualHost Directives*

```
<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

この仮想ホスト方法を利用するには、対象のマシンに複数の IP アドレスを設定する必要があります。それぞれの IP に割り当てられたドメインに対し、Apache は 1 つのインスタンスで動作します。

IP ベースの仮想ホストでは、それぞれの仮想ホストに対して 1 つの IP アドレスを設定しなければなりません。お使いのマシンに複数のネットワークカードが存在しない場合でも、仮想的なネットワークインターフェイス (IP エイリアス) も設定することができます。

下記は IP アドレス 192.168.3.100 で動作するマシンの Apache 設定例で、追加の IP アドレス 192.168.3.101 および 192.168.3.102 でそれぞれ 1 つずつのドメインをまかなう場合のものです。下記のとおりそれぞれの仮想ホストに対し、別々の VirtualHost ブロックを設定する必要があります。

例 18.3 *IP ベースの VirtualHost 設定*

```
<VirtualHost 192.168.3.101>
...
</VirtualHost>

<VirtualHost 192.168.3.102>
...
</VirtualHost>
```

ここで VirtualHost は、192.168.3.100 以外のインターフェイスに対してのみ設定していることに注意してください。Listen ディレクティブで 192.168.3.100 のアドレスについても 設定する場合、そのアドレス宛に届いた HTTP リクエストに応答するには、別途の IP ベース仮想ホストを追加しなければなりません。設定しなかった場合は、既定のサーバ設定 (/etc/apache2/default-server.conf) が使用されます。

基本的な仮想ホスト設定

それぞれの仮想ホストを設定するには、少なくとも各仮想ホストの設定内に下記のディレクティブを設定する必要があります。さらに詳しいオプション設定を行ないたい場合は、/etc/apache2/vhosts.d/vhost.template をお読みください。

ServerName

その仮想ホストに割り当てる完全修飾ドメイン名を指定します。

DocumentRoot

このホストから Apache がファイルを提供するにあたって、基準となる ディレクトリを指定します。なおセキュリティ上の理由から、ファイルシステム 全体に対するアクセスは既定では禁止されるようになっています。そのため、Directory コンテナを利用することで、明示的に 禁止を解除するよう設定してください。

ServerAdmin

サーバ管理者の電子メールアドレスを指定します。たとえば、このアドレスは Apache が生成するエラーページで表示されます。

ErrorLog

この仮想ホストに対するエラーログファイルを指定します。仮想ホスト ごとに個別のエラーログを作成する必要はありませんが、デバッグが容易になることから、個別に作成しておくことをお勧めします。/var/log/apache2/ が Apache のログファイルに関する既定のディレクトリです。

CustomLog

この仮想ホストに対するアクセスログです。仮想ホストごとに個別のエラー ログを作成する必要はありませんが、各ホストについて個別の分析を行なうことができるという理由から、個別に作成しておくことをお勧めします。/var/log/apache2/ が Apache のログファイルに関する既定のディレクトリです。

上記のように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 既定で禁止されています。そのため、Apache がサービスを提供すべき ディレクトリについては、明示的に禁止を解除しなければなりません。たとえば DocumentRoot であれば、下記のようになります：

```
<Directory "/srv/www/www.example.com/htdocs">
    Order allow,deny
    Allow from all
</Directory>
```

基本的な設定をそろえると、下記ようになります:

例 18.4 基本的な *VirtualHost* 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>
```

18.2.3 YaST を利用した Apache の設定

YaST を利用して Web サーバを設定するには、YaST を起動してから ネットワーク サービス > HTTP サーバ を選択します。このモジュールを初めて起動した場合は HTTP サーバ ウィザード が起動し、サーバ管理についていくつかの基本事項を質問します。このウィザードを終了すると、以降の HTTP サーバ モジュールの起動では HTTP サーバ 設定 ダイアログが表示されるようになります。

18.2.3.1 HTTP サーバ ウィザード

HTTP サーバ ウィザードは 5 つの段階から構成されています。ダイアログの最後の段階では、熟練者向けの設定を行なってより詳しい設定を施すことができます。

ネットワークデバイスの選択

ここでは Apache が要求を受け付けるために利用する、ネットワークインターフェイスを指定します。既存のネットワークインターフェイスと IP アドレスから、任意の組み合わせで選択することができます。また、他のサービスが予約していない任意のポート (既知の (Well-known) ポートや登録済みのポート、および動的なポートやプライベートなポート) を使用することができます。既定の設定では、全てのネットワークインターフェイスに対して 80 番のポートで待ち受ける設定になっています。

Web サーバが待ち受けるポートについて、ファイアウォール側でポートを開くには、ファイアウォールで **ポートを開く** を選択します。この設定は LAN や WAN、インターネットなどのネットワークに対して Web サーバを公開する場合に必要な設定です。ポートを閉じたままにする設定は、テストなどで外部からのアクセスを禁止したい場合にのみ有用な設定です。複数のネットワーク インターフェイスをご利用の場合は、**ファイアウォールの詳細...** を押してポートを開きたいインターフェイスを選択してください。

次へ を押すと設定を続けることができます。

モジュール

モジュール 設定オプションでは、Web サーバがサポートすべき スクリプト言語を有効にしたり無効にしたりすることができます。その他のモジュールを設定するには、「サーバモジュール」(360 ページ) をお読みください。**次へ** を押すと設定を続けることができます。

既定のホスト

この設定では既定のホストを設定します。18.2.2.1 項「仮想 (バーチャル) ホストの設定」(349 ページ) で説明しているとおり、Apache は単一のマシンで複数の仮想ホストを稼働させることができます。設定ファイル内で最初に設定したホストのことを **既定のホスト** と言いますが、ここではこれを設定します。それぞれの仮想ホストは既定のホストの設定を引き継ぎます。

ホストの設定 (ディレクティブとも呼ばれます) を編集するには、表内から変更したい項目を選んで **編集** を押します。新しいディレクティブを追加するには **追加** を、ディレクティブを削除するには対象のものを選んで **削除** を押してください。

図 18.1 HTTP サーバウイザード: 既定のホスト

HTTPサーバウイザード (3/5) -- 既定のホスト

オプション	値
ドキュメントルート	<code>*/srv/www/htdocs*</code>
Directory	<code>*/srv/www/htdocs*...</code>
Alias	<code>/icons/ */usr/share/apache2/icons/*</code>
Directory	<code>*/usr/share/apache2/icons*...</code>
ScriptAlias	<code>/cgi-bin/ */srv/www/cgi-bin/*</code>
Directory	<code>*/srv/www/cgi-bin*...</code>
mod_userdir.c	
Include	<code>/etc/apache2/conf.d/*.conf</code>
Include	<code>/etc/apache2/conf.d/apache2-manual?conf</code>
サーバ名	linux
サーバ管理者のメールアドレス	geso-degeso@linux

追加 (A) 編集 (I) 削除 (T)

ヘルプ (H) 戻る (B) キャンセル (C) 次へ (N)

それぞれ下記にサーバの設定項目を示します:

ドキュメントルート

このホストが提供すべきファイルが存在するディレクトリを指定します。既定では `/srv/www/htdocs` に設定されています。

Alias

Alias ディレクティブを使用することで、URL と 物理的なファイルの場所について、割り当てを変更することができます。これにより ファイルシステム内の ドキュメントルート 以外の場所に ファイルを配置し、URL 経由でアクセスさせることができるようになります。

openSUSE の既定値では、Alias の設定として `/icons` が `/usr/share/apache2/icons` を指すように設定されています。これにより Apache からディレクトリ一覧を 参照すると、アイコンが表示されるようになっています。

ScriptAlias

これは Alias ディレクティブに似た設定で、ScriptAlias も URL とファイルシステムの場所について割り当てを設定します。ただし ScriptAlias は CGI の場所を変更するためのもので、指定した場所で CGI を実行できるようにすることができます。

Directory

Directory を利用すると、指定したディレクトリ に対してのみ適用させる設定群を作成することができます。

既定ではそれぞれ /srv/www/htdocs, /usr/share/apache2/icons, /srv/www/cgi-bin ディレクトリに対する設定が存在しています。既定の設定から変更すべきではありません。

Include

Include ディレクティブを利用すると、追加の 設定ファイルを取り込むように設定することができます。既定では 2 つの Include が設定されています: /etc/apache2/conf.d/ は外部のモジュールから もたらされる設定を取り込むためのもので、これによりそのディレクトリ内に 存在する .conf で終わるファイルを全て取り込みます。2 つめは /etc/apache2/conf.d/apache2-manual.conf が設定されていて、apache2-manual の設定ファイルを取り込むようになっています。

サーバ名

ここではクライアントが Web サーバと通信を行なうにあたって、既定で使われるサーバ名を指定します。http://*FQDN*/ でアクセスすることができるように完全修飾ドメイン名 (FQDN) を指定するか、もしくは IP アドレスを指定します。ここでは任意の名前を入力することはできず、指定したサーバ名で名前を解決できなければなりません。

サーバ管理者のメールアドレス

サーバ管理者のメールアドレスを指定します。ここで指定したアドレスは、たとえば Apache がエラーページを生成した場合などに表示されます。

既定のホスト の手順を終了したら、次へ を押すと設定を続けることができます。

仮想ホスト

この段階では、ウィザードは設定済みの仮想ホストを表示します (詳しくは 18.2.2.1 項「仮想 (バーチャル) ホストの設定」(349 ページ) をご覧ください)。YaST HTTP ウィザードを開始するまでに特に何も設定していない 場合は、何も仮想ホストが表示されません。

ホストを追加するには *追加* ボタンを押します。すると、作成する ホストについて基本設定を行なうためのダイアログが表示されます。ここでは *サーバ名*, *サーバコンテンツのルート* (ドキュメントルート), *管理者のメールアドレス* などを設定します。ま

た、サーバ解決では、ホストの識別方法を指定します (名前ベースまたは IP ベース)。仮想ホスト ID の変更を押して、名前または IP アドレスを指定してください。

次へを押すと、次の仮想ホスト設定ダイアログに進みます。

仮想ホスト設定の 2 番目のダイアログでは、CGI を有効にするかどうかを設定することができるほか、これらのスクリプトをどのディレクトリに配置するかを設定することができます。また、SSL についても有効化を設定することができます。SSL を有効に設定する場合は、証明書のパスについても設定を行わなければなりません。SSL と証明書について、詳しくは 18.6.2 項「SSL を利用する Apache の設定」(380 ページ)をお読みください。またディレクトリインデックス オプションでは、クライアントがディレクトリへのアクセスを要求した場合に出力するファイル (既定では index.html) を指定します。ここには 1 つまたは複数のファイル (複数の場合は半角スペースで区切ります) を指定してください。また、公開 HTML を有効にするを選択すると、ユーザの公開ディレクトリ (~ユーザ名/public_html/) にあるファイルを `http://www.example.com/~ユーザ名` から公開することができるようになります。

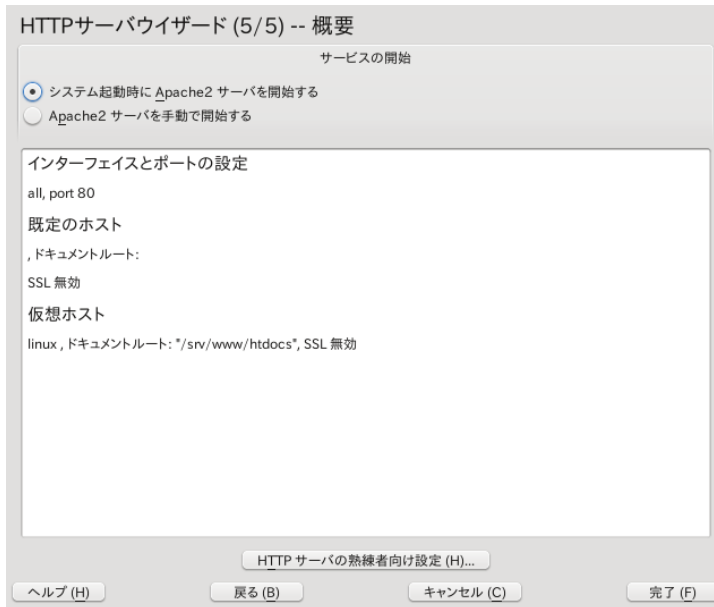
重要: 仮想ホストの作成

仮想ホストは好き勝手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利用している場合、ネットワーク上でそれぞれのホスト名を解決できなければなりません。IP ベースの仮想ホストを利用している場合は、それぞれ IP アドレスごとに 1 つの仮想ホストだけを割り当てることができます。

概要

これがウイザードの最終段階です。ここでは Apache サーバの起動方法と起動タイミング (システム起動時、または手動) を設定することができます。またこれ以外にも、これまでに設定してきた項目の概要が表示されます。これまでの設定で問題がなければ、完了を押して設定を完了させてください。何らかの設定を変更したい場合は、戻るを押して必要なダイアログまで戻って設定し直してください。また、HTTP サーバの熟練者向け設定を押すと、18.2.3.2 項「HTTP サーバ設定」(359 ページ)に示されているダイアログが表示されるようになっています。

図 18.2 HTTP サーバウイザード: 概要



18.2.3.2 HTTP サーバ設定

HTTP サーバ設定 ダイアログでは、ウィザードよりも細かい 設定を行なうことができます (ウィザードは Web サーバの初回設定時にのみ表示 されます)。このダイアログは下記に示す 4 つのタブから構成されていますが、いずれの設定ともすぐに反映されることはありません。設定を有効にするには、**完了** を押して設定を確認しておかなければなりません。なお、**中止** を押すと設定モジュールを終了して変更内容を 破棄することができます。

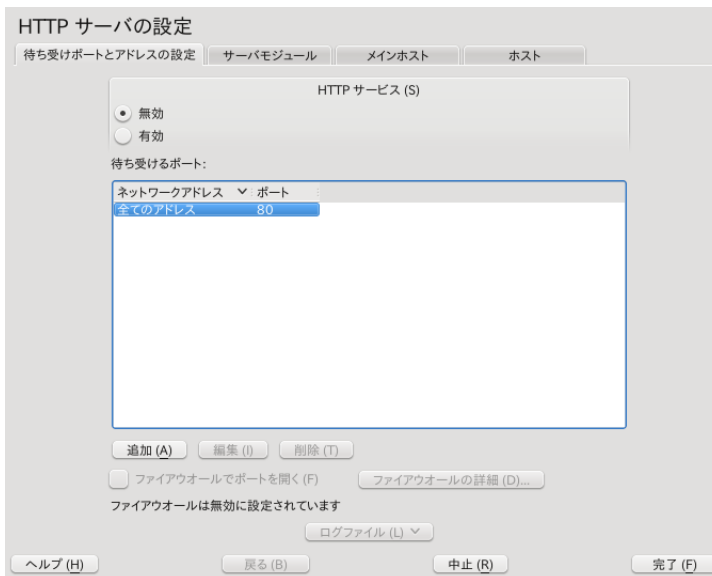
待ち受けポートとアドレス

HTTP サービス の枠内では、Apache を起動するか (**有効**) 起動しないか (**無効**) を選択 することができます。待ち受けるポート の枠内では、Apache サーバのサービスを提供させたいインターフェイスやポートをそれぞれ **追加**、**編集**、**削除** することができます。既定では全てのインターフェイスにてサービスを提供し、ポート 80 で待ち受けるように設定されています。また、Web サーバを他のホストからアクセスできるようにするため、**ファイアウォールでポートを開く** についてもご確認ください。ポートを閉じたままにする設定は、テストなどの目的で Web サーバに対して外部からの

アクセスを拒否したい場合にのみ有用なものです。なお、お使いのマシンに複数のネットワークインターフェイスが存在する場合は、[ファイアウォールの詳細...](#) を押して、ポートを開くべきインターフェイスを設定することもできます。

さらに **ログファイル** ボタンでは、アクセスログやエラーログを参照することができます。これはお使いのサーバ設定をテストしたい場合などに便利です。ログファイルは個別のウィンドウで表示され、そこから Web サーバの再起動や 再読み込みなどを行なうことができます。詳しくは 18.3項「Apache の起動と停止」(361 ページ)をお読みください。これらのコマンドはすぐに反映され、それらのログメッセージも 即時に表示されます。

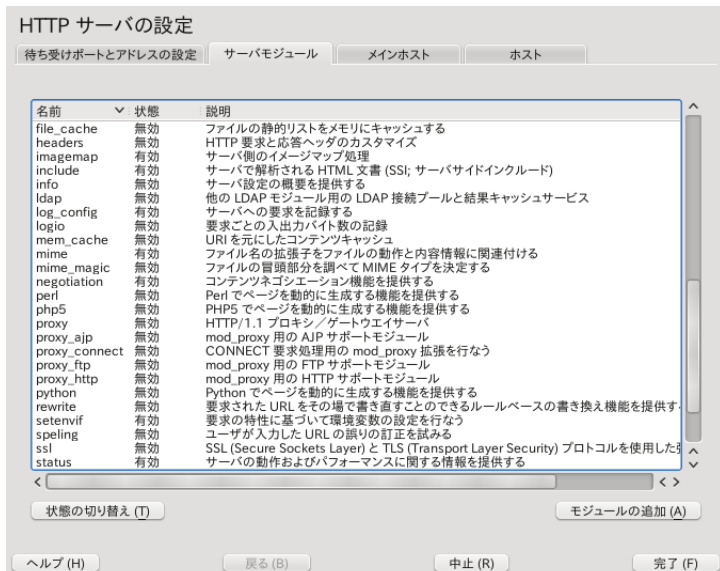
図 18.3 HTTP サーバ設定: 待ち受けポートとアドレス



サーバモジュール

それぞれモジュールを選んで **状態の切り替え** ボタンを押すと、Apache2 モジュールの状態 (有効／無効) を切り替えることができます。モジュールの**追加** ボタンを押すと、インストールされているものの一覧に表示されていない新しいモジュールを追加することができます。モジュールについて、詳しくは 18.4項「モジュールのインストール／有効化／設定」(364 ページ)をお読みください。

図 18.4 HTTP サーバ設定: サーバモジュール



メインホストおよびホスト

これらのダイアログについては、それぞれ「既定のホスト」(355 ページ)と「仮想ホスト」(357 ページ)をお読みください。

18.3 Apache の起動と停止

18.2.3項「YaST を利用した Apache の設定」(354 ページ)に書かれている手順で YaST から設定を行なうと、ランレベル 3 および 5 であれば Apache はシステム起動時に開始され、0, 1, 2, 6 であれば停止するようになっています。YaST のランレベルエディタを利用することで、この振る舞いを変えることができるほか、コマンドラインツール `chkconfig` を利用することでも同じことを行なうことができます。

起動中のシステムから Apache を開始したり停止したり、もしくは操作したりしたい場合は、init スクリプト `/usr/sbin/rcapache2` をご利用ください。`rcapache2` コマンドは下記のようなパラメータを受け付けます:

`status`

Apache が起動しているかどうかを確認します。

start

Apache が起動していない場合、起動を行ないます。

startssl

Apache が起動していない場合、SSL を有効にして起動を行ないます。SSL の有効化について、詳しくは 18.6 項「SSL で通信の機密を保持する Web サーバの設定」(375 ページ) をお読みください。

stop

親プロセスを終了させることで、Apache を停止します。

restart

Apache を停止したあと、起動を行ないます。その時点で起動していなかった場合は、単に起動だけを行ないます。

try-restart

Apache が既に起動している場合にのみ、停止した後に起動を行ないます。

reload または graceful

Apache の全てのプロセスに対して、その時点で処理中の全てのリクエストを処理したあとに停止するよう働きかけます。それぞれのプロセスが終了すると、それらは新しく作成したプロセスに置き換えられ、最終的には Apache の「再起動」が行なわれるようにします。

ヒント: 本番環境での Apache 再起動

接続が強制的に切断されたりすることなく設定を反映するには、`rcapache2 reload` コマンドをご利用ください。

restart-graceful

全ての要求に対して応答することのできる 2 つめの Web サーバを起動します。従来まで存在していた 1 つめの Web サーバについては、`GracefulShutdownTimeout` で設定した時間間隔だけ 要求に対する処理を続け、最終的には停止するようにします。

`rcapache2 restart-graceful` は 新しいバージョンへのアップグレードを行なった場合や、再起動を必要とする設定 変更を行なった場合に便利な方法です。このオプションを使用すると、サービスの 停止時間を最小限にすることができます。

`GracefulShutdownTimeout` の設定については 必ず値を入力してください。設定を行なわないと `restart-graceful` は通常の `restart` と同じ意味になって

しまいます。なお、この値に 0 を設定すると、残っている全てのリクエストを全て処理しきるまで、無期限に待機するようになります。

また `restart-graceful` は、必要な全ての資源を元の Apache プロセスが解放しない場合、失敗する場合があります。この場合、このコマンドは `stop-graceful` と同じ動作になります。

`stop-graceful`

既存の全てのリクエストが処理されるようにするため、`GracefulShutdownTimeout` で設定した時間間隔だけ 要求に対する処理を続け、最終的には停止します。

`GracefulShutdownTimeout` の設定については 必ず値を入力してください。設定を行なわないと `stop-graceful` は通常の `restart` と同じ意味になってしまいます。なお、この値に 0 を設定すると、残っている全てのリクエストを全て処理しきるまで、無期限に待機するようになります。

`configtest` または `extreme-configtest`

現在実行中の Web サーバに影響を与えることなく、設定ファイルの文法を確認します。この文法確認はサーバを起動／再読み込み (`reload`)／再起動する際に毎回行なわれるようになっているため、テストだけを明示的に行なう必要はありません (設定エラーが見つかった場合は、Web サーバの起動／再読み込み (`reload`)／再起動は行なわれません)。また `extreme-configtest` オプションでは `nobody` ユーザで Web サーバを起動し、実際に設定の読み込みを行なってさらなるエラーを検出しようとします。ただし SSL の証明書については `nobody` で読み込むことができないため、SSL 関連の設定についてはテストを行なうことができません。

`probe`

再読み込みが必要かどうかを検出 (設定が変更されたかどうかを確認し)、`rcapache2` コマンドに設定するパラメータを提案します。

`server-status` および `full-server-status`

それぞれ簡潔なサーバ状態か、もしくは完全なサーバ状態を表示します。`mod_status` モジュールを有効化しておく必要があるほか、`lynx` または `w3m` をインストールする必要があります。また、`/etc/sysconfig/apache2` ファイル内の `APACHE_SERVER_FLAGS` に、`status` を追加しなければなりません。

ヒント: 追加フラグ

`rcapache2` に追加のフラグを指定すると、それらは Web サーバに渡されます。

18.4 モジュールのインストール／有効化／設定

Apache のソフトウェアはモジュールの形で部品化されています。いくつかの中枢機能を 除き、それらの機能は全てモジュールとして提供されています。たとえば HTTP でさえも モジュール (http_core) の形になっています。

Apache のモジュールはそのソフトウェアをコンパイルする際に Apache に内蔵させる ことができるほか、実行時に動的に読み込むこともできます。どのようにして動的に 読み込むのかについては、18.4.2項「有効化と無効化」(365 ページ) をお読みください。

Apache のモジュールは下記の 4 つに分類できます：

基本モジュール

基本モジュールは既定で Apache に内蔵されます。openSUSE の Apache では mod_so (他のモジュールを読み込むために必要な モジュール) と http_core だけが内蔵されるようになっています。その他のモジュールは全て共有オブジェクトになっていて、サーバの実行ファイル 自身に含まれることはなく、実行時に取り込むことで動作する仕組みになっています。

拡張モジュール

一般的に、拡張と呼ばれるモジュールについても Apache ソフトウェアパッケージ内 に含まれていますが、通常はサーバに内蔵されることはありません。openSUSE では、それらは共有オブジェクトとして提供され、実行時に Apache に読み込むこと ができるようになっています。

外部モジュール

外部モジュールは公式の Apache 配布物には含まれていないものを指します。しかしながら、openSUSE ではいくつかの外部モジュールを提供しています。

マルチプロセッシングモジュール (MPM)

マルチプロセッシングモジュール (MPM) は Web サーバに対するリクエストを受け付けたり処理したりする責任を負ったソフトウェアで、Web サーバソフトウェアの 中枢部を表わすものです。

18.4.1 モジュールのインストール

18.1.2項「インストール」(344 ページ) に書かれている既定の手順で Apache をインストールした場合、全ての基本モジュールと拡張モジュールのほか、マルチプロセッシングモジュールである Prefork MPM と外部モジュール `mod_php5`, `mod_python` がそれぞれ インストールされます。

YaST から **ソフトウェア > ソフトウェア管理** を起動することで、追加の 外部モジュールをインストールすることができます。ソフトウェア管理を起動したら、**フィルタ > 検索** を利用し、`apache` と入力することで、利用可能な 全ての外部モジュールを表示することができます。

18.4.2 有効化と無効化

それぞれのモジュールは YaST から有効にしたり無効にしたりすることができますほか、手作業でもこれを行なうことができます。YaST では、18.2.3.1項「HTTP サーバウイザード」(354 ページ) に書かれている手順で スクリプト言語モジュール (PHP5, Perl, Python) を有効にしたり無効にしたりすることができます。それ以外のモジュールについては、「サーバモジュール」(360 ページ) に書かれている手順で有効／無効を設定することができます。

モジュールを手作業で有効／無効に設定したい場合は、`a2enmod mod_foo` コマンドか、もしくは `a2dismod mod_foo` コマンドをご利用ください。また、`a2enmod -l` を実行することで、有効に設定されている全モジュールの一覧を表示することができます。

重要: 外部モジュール向けの設定取り込み

外部モジュールを手作業で有効化した場合は、全ての仮想ホスト設定で外部モジュール 向けの設定ファイルが読み込まれることを確認してください。外部モジュール向けの 設定ファイルは `/etc/apache2/conf.d/` ディレクトリ内に 置かれ、既定では読み込まれません。それぞれの仮想ホストで同じモジュールを必要とする場合は、このディレクトリ内にある `*.conf` ファイルを 取り込む (include) こともできます。それ以外の場合は、個別に取り込んでも かまいません。設定例については、`/etc/apache2/vhost.d/vhost.template` ファイルをお読みください。

18.4.3 基本モジュールと拡張モジュール

全ての基本モジュールと拡張モジュールは、Apache のドキュメンテーション内で詳しく説明されています。最も重要なモジュールについては、概要だけが説明 され

ています。各モジュールの詳しい説明は、<http://httpd.apache.org/docs/2.2/mod/> をお読みください。

`mod_actions`

特定の MIME タイプ (たとえば `application/pdf`) や特定の拡張子 (たとえば `.rpm`)、もしくは特定の リクエスト種別 (たとえば `GET`) が要求された 際に、スクリプトを実行する手段を提供します。このモジュールは既定で有効に 設定されます。

`mod_alias`

`Alias` および `Redirect` ディレクティブを提供するモジュールで、URI を特定のディレクトリに割り当てたり (`Alias`)、要求された URL を別の URL に転送したり することができます。このモジュールは既定で有効に設定されます。

`mod_auth*`

認証モジュールは、様々な認証方法を提供するためのモジュールです。`mod_auth_basic` では基本認証を、`mod_auth_digest` ではダイジェスト認証をそれぞれ提供します。Apache 2.2 におけるダイジェスト認証は、実験中の ものとして提供されています。

なお、`mod_auth_basic` と `mod_auth_digest` の各モジュールは、それぞれ 認証プロバイダモジュール `mod_authn_*` と 認可モジュール `mod_authz_*` をあわせて使用する 必要があります。たとえば `mod_authn_file` は テキストファイルを利用した認証を提供するほか、`mod_authz_user` はユーザ認可を提供します。

認証や認可について、詳しくは <http://httpd.apache.org/docs/2.2/howto/auth.html> にある *Authentication HOWTO* をお読みください。

`mod_autoindex`

`autoindex` モジュールは、索引ファイル (たとえば `index.html` ファイル) が存在しない場合に、自動でディレクトリの索引を生成するための モジュールです。外観については設定を変更することもできます。このモジュールは 既定で有効に設定されていますが、`Options` ディレクティブで生成が無効に設定されています。ディレクトリ一覧を自動生成 させるには、それぞれの仮想ホスト内で設定を上書きしてください。このモジュール の既定の設定値は、`/etc/apache2/mod_autoindex-defaults.conf` に書かれています。

`mod_cgi`

`mod_cgi` は CGI スクリプトを実行する際に必要な モジュールです。このモジュールは既定で有効に設定されています。

mod_deflate

このモジュールを利用することで、Apache はクライアントに特定の種類のファイルを転送する際、圧縮して転送することができますようになります。

mod_dir

mod_dir は、ディレクトリに対するアクセスがあった場合に、どのファイルを転送するかを選択する、DirectoryIndex ディレクティブを提供するモジュールです。既定では index.html が設定されています。このモジュールではほかにも、ディレクトリに対するアクセスがあった場合、URI への最後がスラッシュで終わっていないと、それを自動で補完する機能も備わっています。このモジュールは既定で有効に設定されています。

mod_env

CGI スクリプトや SSI のページに渡される、環境変数を制御するモジュールです。httpd プロセスから起動されるシェルに対し、環境変数を設定したり設定を消したりすることができます。このモジュールは既定で有効に設定されています。

mod_expires

mod_expires を利用すると、Expires ヘッダを利用して期限切れ日時を設定することができます。期限切れ日時はプロキシサーバや ブラウザが一時記憶 (キャッシュ) のために使用します。このモジュールは既定で有効に設定されています。

mod_include

mod_include はサーバサイドインクルード (Server Side Includes; SSI) を提供するモジュールで、HTML ページを動的に生成するための基本機能を提供します。このモジュールは既定で有効に設定されています。

mod_info

ブラウザから <http://localhost/server-info/> の URL にアクセスすることで、サーバ設定に関する広範囲の概要を提供するモジュールです。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しておかなければなりません。既定では localhost だけがアクセスを許されるようになっています。mod_info は /etc/apache2/mod_info.conf で設定します。

mod_log_config

このモジュールを利用することで、Apache のログファイルについて設定を行なうことができます。このモジュールは既定で有効に設定されています。

`mod_mime`

MIME モジュールは、そのファイル名の拡張子に基づいて正しい MIME ヘッダを付与するモジュールです (たとえば HTML ドキュメントの場合は `text/html` に設定します)。このモジュールは既定で有効に設定されています。

`mod_negotiation`

コンテンツネゴシエーションと呼ばれる機能を提供するモジュールです。詳しくは <http://httpd.apache.org/docs/2.2/content-negotiation.html> をお読みください。このモジュールは既定で有効に設定されています。

`mod_rewrite`

`mod_alias` に似た機能を提供するモジュールですが、ずっと高機能で柔軟性に富んだ設定を行なうことができます。`mod_rewrite` を利用すると、複数のルールを設定し URL 転送を行なうことができるほか、リクエストヘッダを元にした転送なども行なうことができます。

`mod_setenvif`

クライアントのリクエスト内容に応じて環境変数を設定するモジュールです。たとえばクライアントが送信したブラウザ文字列のほか、クライアントの IP アドレスなどを基準にすることができます。このモジュールは既定で有効に設定されています。

`mod_speling`

`mod_speling` は URL の入力ミスやスペルミスについて、自動修正を試みるモジュールです。たとえば大文字と小文字の間違いなどを修正することができます。

`mod_ssl`

Web サーバとクライアントの間で、暗号化接続を行なうことができるようにするモジュールです。詳しくは 18.6 項「SSL で通信の機密を保持する Web サーバの設定」(375 ページ) をお読みください。このモジュールは既定で有効に設定されています。

`mod_status`

サーバの動作や性能情報を `http://localhost/server-status/` から公開することのできるモジュールです。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しておかなければなりません。既定では `localhost` だけがアクセスを許されるようになっています。`mod_status` は `/etc/apache2/mod_status.conf` で設定します。

`mod_suexec`

`mod_suexec` は、CGI スクリプトを特定のユーザや グループで実行させるためのモジュールです。このモジュールは既定で有効に 設定されています。

`mod_userdir`

`~ユーザ名/` のディレクトリ から、ユーザ固有のディレクトリを提供するモジュールです。設定ファイル内で `UserDir` ディレクティブを 指定しなければなりません。このモジュールは既定で有効に設定されています。

18.4.4 マルチプロセッシングモジュール (MPM)

openSUSE では、Apache 向けに 2 種類のマルチプロセッシングモジュール (MPM) を提供しています:

- Prefork MPM (369 ページ)
- 18.4.4.2項「Worker MPM」(369 ページ)

18.4.4.1 Prefork MPM

Prefork MPM はスレッドを使用しない MPM で、あらかじめ fork しておくことで 動作する Web サーバを提供します。Web サーバの動きは Apache バージョン 1.x に似たものとなり、各リクエストは独立して動作する子プロセスが処理する形になります。そのため、問題のあるリクエストが届いた場合であっても他のプロセスの 動作を止めたりすることなく、Web サービスが停止してしまったりすることを 防ぐことができます。

このようにプロセスを基準にしたアプローチは安定性を提供する一方、欠点として worker MPM と比べ多くの資源を必要としてしまいます。Prefork MPM は Unix ベースのオペレーティングシステムでは既定の MPM として採用されています。

重要: このドキュメント内での MPM

この文書内で、Apache は Prefork MPM を使用した場合を想定しています。

18.4.4.2 Worker MPM

Worker MPM はスレッドを利用する Web サーバです。スレッドとはプロセスよりも「軽量の」仕組みで、プロセスよりも少ない資源で動作するものです。Worker

MPM では子プロセスを fork するだけでなく、そのプロセス内で複数の スレッドを起動してリクエストを処理します。このアプローチにより、Prefork MPM よりも少ない資源で高い性能を発揮するような仕組みになっています。

Worker MPM の最大の欠点はその安定性で、ある特定のスレッドが何らかの理由で破壊されてしまうと、そのスレッドを管理していたプロセス全体が影響を受けてしまいます。最悪の場合、サーバクラッシュにもつながる可能性があります。特に Apache で Common Gateway Interface (CGI) を利用していて負荷が高くなると、システム資源との通信が行なえなくなることによって Internal Server Error が発生してしまいます。また Worker MPM は、Apache に添付されているモジュールの一部がスレッドセーフ (複数のスレッドから同時に呼び出されても安全に動作すること) ではないため、それらは Worker MPM と同時に使用することができません。

警告: PHP を利用する場合の MPM について

PHP モジュールの一部はスレッドセーフではありません。mod_php を使用する場合は、Worker MPM を使用しないことを強くお勧めします。

18.4.5 外部モジュール

openSUSE に同梱されている全ての外部モジュールを下記に列挙しています。各モジュールのドキュメンテーションについては、それぞれのディレクトリをご覧ください。

mod_apparmor

mod_php5 や mod_perl などのモジュールで処理される Apache 内の各 CGI スクリプトに対し、AppArmor の制限を設定します。

パッケージ名: apache2-mod_apparmor

さらなる情報: パート「AppArmor を利用した権利制限」(↑セキュリティガイド)

mod_mono

mod_mono を利用すると、お使いのサーバ内で ASP.NET ページを実行することができます。

パッケージ名: apache2-mod_mono

設定ファイル: /etc/apache2/conf.d/mod_mono.conf

mod_perl

mod_perl を利用すると、Perl スクリプトを内蔵の インタプリタで実行することができるようになります。サーバ内でインタプリタが 恒久的に保持される形になるため、外部のインタプリタを起動する場合と比べて、起動時のオーバーヘッドを小さくすることができます。

パッケージ名: apache2-mod_perl

設定ファイル: /etc/apache2/conf.d/mod_perl.conf

さらなる情報: /usr/share/doc/packages/apache2-mod_perl

mod_php5

PHP はサーバ内で動作するプラットフォーム非依存の HTML 内蔵型 スクリプト言語です。

パッケージ名: apache2-mod_php5

設定ファイル: /etc/apache2/conf.d/php5.conf

さらなる情報: /usr/share/doc/packages/apache2-mod_php5

mod_python

mod_python は Apache HTTP サーバ内に Python 機能を 内蔵させるためのもので、性能を相当に改善することができるほか、Web ベースの アプリケーションを構築する際の柔軟性を追加することができます。

パッケージ名: apache2-mod_python

さらなる情報: /usr/share/doc/packages/apache2-mod_python

mod_tidy

mod_tidy は TidyLib を利用するモジュールで、それぞれ発信される HTML ページを検証することができるものです。検証エラーが発生すると、エラー一覧ページが表示されます。エラーにならなかった場合は 元の HTML ページが表示されます。

パッケージ名: apache2-mod_tidy

設定ファイル: /etc/apache2/mod_tidy.conf

さらなる情報: /usr/share/doc/packages/apache2-mod_tidy

18.4.6 コンパイル

Apache では知識のあるユーザがカスタムなモジュールを作成することで、その機能を 拡張することができます。Apache のモジュールを開発したりサードパーティ

製のモジュールをコンパイルしたりしたい場合は、開発ツールのほかに `apache2-devel` パッケージが必要となります。`apache2-devel` パッケージには `apxs2` と呼ばれるツールが含まれ、これを利用することで Apache 向けの追加モジュールをコンパイルできるようになっています。

`apxs2` はソースコードからモジュールをコンパイルしたりインストールしたりすることができます (インストール作業では、設定ファイルに対して行なう変更も同時に行なうことができます)。これにより、Apache の実行時に読み込まれる *動的共有ライブラリ* (DSO) を作成することができます。

`apxs2` 関連のバイナリは、`/usr/sbin` 以下に配置されます:

- `/usr/sbin/apxs2`—任意の MPM で動作する拡張モジュールを構築するのに便利なツールです。インストールを行なう際、インストール先は `/usr/lib/apache2` になっています。
- `/usr/sbin/apxs2-prefork`—`prefork` MPM 用のモジュールを構築するのに便利なツールです。インストールを行なう際、インストール先は `/usr/lib/apache2-prefork` になっています。
- `/usr/sbin/apxs2-worker`—`worker` MPM 用のモジュールを構築するのに便利なツールです。インストールを行なう際、インストール先は `/usr/lib/apache2-worker` になっています。

ソースコードからモジュールをコンパイルし、インストールしたあとに有効に設定するには、下記のように入力します:

```
cd /ソースコードのパス; apxs2 -cia  
    mod_foo.c
```

ここで、`-c` オプションはモジュールのコンパイルを、`-i` オプションはモジュールのインストールを、`-a` オプションはモジュールの有効化をそれぞれ指定しています。`apxs2` に対するその他のオプションは、`apxs2(1)` のマニュアルページ内に記述されています。

18.5 CGI スクリプトを動作させる方法

Apache が用意している汎用ゲートウェイインターフェイス (Common Gateway Interface; CGI) は、プログラムやスクリプトから動的なコンテンツを生成するための仕組みで、CGI スクリプトなどとも呼ばれるものです。CGI スクリプトでは、任

意のプログラミング 言語を使用することができます。通常はスクリプト言語として、Perl や PHP などを使用します。

Apache に対して CGI スクリプトの実行と動的コンテンツの生成を許可するには、mod_cgi モジュールと mod_alias モジュールを有効に設定する必要があります。両方とも既定では有効に設定されるモジュールです。モジュールの有効化について、詳しくは 18.4.2 項「有効化と無効化」(365 ページ)をお読みください。

警告: CGI セキュリティ

サーバに対して CGI スクリプトの実行を許可すると、それは潜在的なセキュリティ ホールになる場合があります。詳しくは 18.7 項「セキュリティ問題の回避」(382 ページ)をお読みください。

18.5.1 Apache の設定

openSUSE 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るようになっていました。このディレクトリは CGI スクリプトを実行するために設定済みの ディレクトリですが、既に仮想ホストの設定を行なっている場合(18.2.2.1 項「仮想 (バーチャル) ホストの設定」(349 ページ)を参照)で、仮想ホスト別のディレクトリに CGI スクリプトを配置したい場合は、ディレクトリを設定し、禁止を解除しなければなりません。

例 18.5 仮想ホストでの CGI 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 このように設定することで、上記のディレクトリ内にある各ファイルを CGI と見なし、実行できるようになります。
- ❷ CGI スクリプトの実行を有効に設定します。
- ❸ .pl と .cgi の拡張子をもつファイルに対し、CGI スクリプトとして実行するように指定しています。この行は必要に応じて変更してください。
- ❹ Order と Allow の各ディレクティブは既定のアクセス制御を設定し、Allow と Deny のどちらを 先に解釈するのかを指定します。この設定の場合、「deny」ディレクティブが「allow」ディレクティブよりも先に解釈され、既定でアクセスは許可されるようになります。

18.5.2 サンプルスクリプトの実行

CGI のプログラミングは「通常の」プログラミングとは異なり、Content-type: text/html のような MIME 種類のヘッダを出力しなければなりません。このヘッダはクライアントに送信され、クライアント側で解釈されます。また、CGI スクリプトの出力はクライアント (一般に Web ブラウザ) が解釈可能な形式でなければなりません。多くの場合は HTML やテキスト形式ですが、たとえば画像などでもかまいません。

Apache のパッケージには、シンプルなテスト用スクリプト `/usr/share/doc/packages/apache2/test-cgi` が含まれています。これはいくつかの環境変数をテキスト形式で出力するものです。このファイルは `/srv/www/cgi-bin/` ディレクトリにコピーするか、もしくはお使いの仮想ホスト内のスクリプトディレクトリ (`/srv/www/www.example.com/cgi-bin/`) にコピーし、`test.cgi` のようなファイル名を設定してください。

また、Web サーバがアクセスするファイルは、root ユーザに所有権があるファイルであるべきものです。詳しい情報は 18.7 項「セキュリティ問題の回避」(382 ページ) をお読みください。Web サーバは root とは異なるユーザで動作することから、CGI スクリプトは全てのユーザに対して実行と読み込みを許可しなければなりません。CGI のディレクトリに移動して `chmod 755 test.cgi` コマンドを実行すると、必要なパーミッションを設定することができます。

全ての設定が完了したら、`http://localhost/cgi-bin/test.cgi` にアクセスするか、もしくは `http://www.example.com/cgi-bin/test.cgi` にアクセスしてください。アクセスすると「CGI/1.0 test script report」のような表示が現われるはずです。

18.5.3 CGI のトラブルシューティング

テストプログラムの出力が現われず、エラーメッセージが表示された場合は、下記の項目を確認してください:

CGI トラブルシューティング

- 設定を変更したあと、再起動を行ないましたか? `rcapache2 probe` を実行して確認してください。
- カスタムな CGI ディレクトリを設定している場合、それらを正しく設定してありますか? 不確かな場合は、テスト用のスクリプトを既定の CGI ディレクトリ `/srv/`

www/cgi-bin/ にコピーし、ブラウザで `http://localhost/cgi-bin/test.cgi` を開いてみてください。

- ファイルのパーミッションは正しく設定されていますか？ CGI をコピーした ディレクトリに移動し、`ls -l test.cgi` を実行してください。パーミッションは、下記のように表示されなければなりません：

```
-rwxr-xr-x 1 root root
```

- スクリプトにプログラムエラーが存在しないことを確認してください。`test.cgi` をコピーしただけで変更を行っていない場合は 起こりませんが、独自のプログラムを作成したり修正したりした場合は、プログラム エラーが無いかどうかを確認してください。

18.6 SSL で通信の機密を保持する Web サーバの設定

クレジットカード情報などの機密データは、Web サーバとクライアントの間で機密を 保持する目的で暗号化を行ない、認証を設定しておくことが望めます。`mod_ssl` では、Secure Sockets Layer (SSL) や Transport Layer Security (TLS) プロトコルを利用し、Web サーバとクライアント間の HTTP 通信に 強い暗号化を提供します。SSL や TLS を利用することで、Web サーバとクライアントの間で秘密の通信を確立することができます。データの整合性についても確認が行なわれるほか、サーバとクライアントの間で相互の認証を行なうことができます。

この暗号化通信を成立させるため、サーバは URL を受け付ける前に、自分自身の正当性を証明する SSL 証明書を送信します。これによりクライアントは、サーバが偽装されたものではなく、通信を開始してよいものかどうかを確認することができます。また証明書は、機密データを危険にさらすリスクを負うことのないように、サーバとクライアントの間で 情報をやりとりするための、暗号化接続を生成する機能を備えています。

`mod_ssl` 自身では SSL/TLS プロトコルを実装することはしておらず、Apache と SSL ライブラリの間のインターフェイスとして動作する仕組みになっています。`openSUSE` では、OpenSSL ライブラリを利用しています。Apache をインストールすると、OpenSSL も自動でインストールされます。

Apache で `mod_ssl` を利用した場合、URL が `http://` ではなく `https://` になるという 点が最もよくわかる違いです。

ヒント: 証明書のサンプル

apache2-example-certificates パッケージをインストールすると、疑似企業「Snake Oil」用の証明書が利用できるようになります。

18.6.1 SSL 証明書の作成

Web サーバで SSL/TLS を使用するためには、SSL の証明書を作成する必要があります。この証明書は Web サーバとクライアントの間で認証を行なうために必要なもので、個人や企業同士で相互に所在確認を行なうことができます。証明書の正当性を確かなものにするには、多くのユーザが信頼する企業や団体によって電子署名されたものでなければなりません。

作成可能な証明書としては、下記の 3 種類があります。テスト用の「ダミー」証明書、公的な信頼を必要としない特定のユーザ範囲で利用する自己署名証明書、独立した公的認証機関 (CA) が電子署名する証明書の 3 種類です。

証明書の作成は、基本的に 2 段階の作業で行ないます。1 つめは認証機関向けの機密鍵作成、2 つめはその鍵を利用したサーバ証明書への署名です。

ヒント: さらなる情報

SSL/TSL について、考え方や定義をより詳しく知るには、http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html をお読みください。

18.6.1.1 「Dummy」証明書の作成

dummy 証明書の作成は簡単に行なうことができます。単純に /usr/bin/gensslcert スクリプトを実行するだけです。これにより下記に示すファイルを生成するか、上書きします。gensslcert に指定するパラメータを変えることで、作成する証明書を細かく調整することができます。詳しくは /usr/bin/gensslcert -h を実行して表示されるヘルプをお読みください。

- /etc/apache2/ssl.crt/ca.crt
- /etc/apache2/ssl.crt/server.crt
- /etc/apache2/ssl.key/server.key
- /etc/apache2/ssl.csr/server.csr

- /root/.mkcert.cfg

ダウンロード用に `ca.crt` のコピーが `/srv/www/htdocs/CA.crt` に作成されます。

重要: テスト目的にのみご利用ください

Dummy 証明書は本番環境では使用しないでください。テスト目的でのみお使いください。

18.6.1.2 自己署名証明書の作成

イントラネット内の機密 Web サーバを構築する場合や、特定のユーザに対する 機密 Web サーバを構築する場合は、ご自身で証明機関 (CA) を作成し、そこで 署名を行えば十分です。

自己署名証明書を作成するには、対話処理で 9 段階の作業を行ないます。まずは `/usr/share/doc/packages/apache2` ディレクトリに 移動し、下記のコマンドを実行します: `./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/` `custom` なお、このコマンドは上記のディレクトリ以外からは実行しないでください。このプログラムは複数の問い合わせを表示する仕組みで動作し、それぞれに答えていくことによって証明書を作成します。

手順 18.4 *mkcert.sh* を利用した自己署名証明書の作成

1 Decide the signature algorithm used for certificates

古いブラウザでは DSA を利用したときに問題が発生する可能性があるため、RSA を選択 (R, 既定値) してください。

2 Generating RSA private key for CA (1024 bit)

特に何も操作する必要はありません。

3 Generating X.509 certificate signing request for CA

ここから証明機関の識別名を作成します。それぞれ国名や団体名など、いくつかの項目に回答します (訳注: スクリプトの仕様上、英語表記であることにご注意ください)。ここで入力するデータはそれぞれ証明書に記載されるため、正しいデータを入力してください。また、全ての質問に対して何らかの入力を行なう必要はなく、該当しないものや入力しないままにしておきたい場合は、「`.`」を入力して

ください。Common name (共通名) は証明機関 自身の名前を入力します。*My company CA* など のように、わかりやすい名前を入力してください。

重要: 証明機関の共通名について

証明機関の共通名はサーバの共通名とは異なるものでなければなりません。そのため、この段階では完全修飾ドメイン名は入力しないでください。

4 Generating X.509 certificate for CA signed by itself

証明書のバージョンを選択します。3 (既定値) を選んでください。

5 Generating RSA private key for SERVER (1024 bit)

特に何も操作する必要はありません。

6 Generating X.509 certificate signing request for SERVER

サーバ用の鍵を作成するための識別名を入力します。証明機関の識別名を入力した 場合とほとんど同じ質問内容で、それぞれ Web サーバに関する情報を入力してください。なお、証明機関のデータと同じものである必要はありません (たとえば サーバが別の場所に存在する場合など)。

重要: 共通名の選択

ここで入力する共通名は、サーバの完全修飾ドメイン名でなければなりません (たとえば *www.example.com*)。そうでないとブラウザから Web サーバにアクセスした際、証明書に記載されている共通名とサーバの完全修飾ドメイン名が異なるとして、警告が発生してしまいます。

7 Generating X.509 certificate signed by own CA

証明書のバージョンを選択します。3 (既定値) を選んでください。

8 Encrypting RSA private key of CA with a passphrase for security

証明機関の機密鍵については、暗号化しておくことを強くお勧めします。そのため、ここでは Y と回答してパスワードを入力してください。

9 Encrypting RSA private key of SERVER with a passphrase for security

サーバの鍵を暗号化すると、Web サーバの起動時に毎回パスワードの入力を求められるようになります。これはシステム起動時にサーバを自動で開始することができなくなるほか、Web サーバの再起動にも手間がかかることになります。そのため、一般的にこの質問に対しては N と回答してください。ただしパスワードで暗号化しない場合、その鍵は自分自身を保護する術を持たない ことになるので、その鍵の利用を許すユーザだけがアクセスできることを確認してください。

重要: サーバ鍵の暗号化

サーバの暗号鍵をパスワードで保護した場合は、`/etc/sysconfig/apache2` ファイル内の `APACHE_TIMEOUT` 設定の値を増やしてください。増やさない場合はパスワードを入力するための十分な時間が確保されず、サーバが意図せず停止してしまう可能性があります。

スクリプトでの入力完了すると、生成された証明書と鍵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である `conf` ではなく、`/etc/apache2/` ディレクトリに作成されます。

最後にやるべきことは、証明機関の証明書ファイルを `/etc/apache2/ssl.crt/ca.crt` からご利用のユーザがアクセスできる場所にコピーし、各ブラウザに信頼のおける証明機関として登録してもらうことです。各ブラウザで登録を行わないと、ブラウザからアクセスを行なった 際に、未知の発信元として警告が表示されてしまいます。なお、証明書は 1 年間 有効です。

重要: 自己署名証明書

自己署名証明書は、その証明書を信頼してもらうことのできる特定のユーザだけがアクセスする Web サーバを構築する際にのみ、お使いください。たとえば一般的な 店舗などのような、不特定多数がアクセスするサーバには不適切です。

18.6.1.3 公式に署名された証明書の取得

お使いの証明書に対して署名を行なうことのできる、公的な証明機関がいくつか 存在しています。証明書は信頼のできる第三者によって署名されるため、それらの 証明書を完全に信頼できるようになります。不特定多数がアクセスし、機密を保持 する Web サーバでは、一般に公的な署名のある証明書を利用します。

最もよく知られた証明機関としては、Thawte (<http://www.thawte.com/>) や Verisign (<http://www.verisign.com>) などがあります。これらを含む 公的な証明

機関はあらかじめ全てのブラウザに登録されているため、これらの 証明機関が署名した証明書は、ブラウザ側で自動的に受け付けられます。

公的に署名された証明書を取得する場合は、その証明書そのものを証明機関に送付 する必要はありません。その代わりに、証明書署名要求 (CSR) を送信します。CSR を作成するには、`/usr/share/ssl/misc/CA.sh -newreq` コマンドを実行してください。

まず上記のスクリプトは、CSR を暗号化する際のパスワードを尋ねます。そのあと識別名の入力を行ないます。それぞれ国名や団体名など、いくつかの 項目に回答します (訳注: スクリプトの仕様上、英語表記であることにご注意 ください)。ここで入力するデータはそれぞれ証明書に記載されるため、正しい データを入力してください。また、全ての質問に対して何らかの入力を行なう必要 はなく、該当しないものや入力しないままにしておきたい場合は、「.」を入力してください。Common name (共通名) は証明機関 自身の名前を入力します。*My company* CA など のように、わかりやすい名前を入力してください。最後にチャレンジパスワードと 呼ばれるパスワードの入力と、代替の企業名をそれぞれ入力します。

作成された CSR は、スクリプトを実行したときのディレクトリ内に配置されます。ファイル名は `newreq.pem` になっています。

18.6.2 SSL を利用する Apache の設定

Web サーバで SSL と TLS を利用する場合、既定のサーバ側のポートは 443 です。「通常の」設定を Apache に行なっていれば、ポート 80 での http とポート 443 での SSL/TLS (https) という形になるため、特に矛盾が発生することはありません。実際、単一の Apache が起動している状態で、HTTP と HTTPS の 両方に対応することができます。通常はそれぞれポート 80 とポート 443 で別々の 仮想ホストを設定し、サービスを提供します。

重要: ファイアウォール設定

Apache で SSL をポート 443 で有効化する場合、ファイアウォールを開くことも忘れずに実施してください。これは 項「YaST を利用したファイアウォールの設定」(第13章 マスカレードとファイアウォール, ↑セキュリティガイド) に書かれている手順で YaST から設定することができます。

サーバ全体の設定として、SSL モジュールは既定で有効化されています。お使いの仮想ホストで無効化している場合は、`a2enmod ssl` コマンドで 有効化することができます。最終的に SSL を有効にするには、サーバを起動する際に「SSL」フラグを付

けて起動する必要があります。これを行なうには、`a2enflag SSL` を実行してください。このとき、サーバの証明書 をパスワードで暗号化するようにしている場合は、`/etc/sysconfig/apache2` ファイル内の `APACHE_TIMEOUT` の値を増やしておく必要があります。これで Apache を起動する際にパスワード入力を行なうのに十分な時間を稼ぐことができます。この変更を行なう場合は、サーバを再起動してください。再読み込みでは 不十分です。

なお、仮想ホストのディレクトリ内のファイル `/etc/apache2/vhosts.d/vhost-ssl.template` では、SSL 固有のディレクティブについて詳しい説明が書かれています。一般的な仮想ホストの設定については、18.2.2.1 項「仮想 (バーチャル) ホストの設定」(349 ページ) をお読みください。

仮想ホストの設定を始めるには、上記のテンプレートを `/etc/apache2/vhosts.d/mySSL-host.conf` ファイルなどにコピーしてから編集してください。それぞれ下記のディレクティブを 調整してください:

- `DocumentRoot`
- `ServerName`
- `ServerAdmin`
- `ErrorLog`
- `TransferLog`

18.6.2.1 名前ベースの仮想ホストと SSL

1 つの IP アドレスしか設定されていないサーバでは、SSL 対応の仮想ホストを複数作成することはできません。SSL 対応の仮想ホストを複数設定した場合に ユーザから接続を行なうと、証明書には 1 つのサーバ名しか記述できないため、いずれか 1 つの仮想ホストを除き、証明書のサーバ名と実際のサーバ名とが異なる として、アクセスのたびに警告が表示されてしまいます。

openSUSE では `Server Name Indication (SNI)` と呼ばれる SSL 拡張に対応 していて、SSL のネゴシエーション内でドメイン名を送信することで、この問題を 解決することができます。これにより、早い段階で正しい仮想ホストに「切り替える」こ とができるため、ブラウザに対して正しい証明書を 配信できるようになります。

SNI は openSUSE では既定で有効に設定されています。SSL に対して名前 ベースの仮想ホストを有効にするには、「名前ベースの仮想ホスト」(351 ページ) の

手順に従って設定してください (ただし SSL の場合、ポート番号は 80 ではなく 443 であることに注意してください)。

重要: SNI のブラウザ側対応

SNI はクライアント側でも対応する必要があります。SNI は多くのブラウザで動作しますが、モバイル端末のブラウザや Windows* XP 上で動作する Internet Explorer や Safari の場合、SNI に対応していません。詳しくは http://en.wikipedia.org/wiki/Server_Name_Indication (英語) をお読みください。

また、サーバ側での SNI 非対応のブラウザにおける動作は、SSLStrictSNIVHostCheck ディレクティブで設定を行なうことができます。サーバ全体の設定で on にすると、SNI 非対応のブラウザはすべての仮想ホストで拒否されるようになります。VirtualHost ディレクティブ内で on に設定すると、指定した仮想ホストのみ SNI 非対応 ブラウザのアクセスを拒否します。

サーバ全体の設定で off にすると、サーバは SNI に対応していない場合と同様に動作します。つまり SSL の要求は、すべて *最初に* 設定した仮想ホスト (ポート 443) で処理されます。

18.7 セキュリティ問題の回避

公的なインターネットに晒された Web サーバは、継続的な管理を行なう必要があります。セキュリティの問題が発生することは避けられない問題で、ソフトウェアに関連した問題だけでなく、不用意な設定ミスが発生する場合があります。ここでは、このような問題について、どのように取り扱うべきかを示しています。

18.7.1 最新のソフトウェア

Apache ソフトウェアに脆弱性が発生された場合は、SUSE からセキュリティアドバイザリ (助言／忠告の意味) が発信されます。このアドバイザリには、その脆弱性を修正するための手順が含まれていて、できるかぎり素早い適用を行なう必要があります。SUSE のセキュリティアドバイザリは、下記の方法で受け取ることができます (訳注: 全て英語によるものです):

- **Web ページ** <http://www.novell.com/linux/security/securitysupport.html>

- メーリングリスト (過去ログ) <http://lists.opensuse.org/opensuse-security-announce/>
- RSS フィード http://www.novell.com/linux/security/suse_security.xml

18.7.2 DocumentRoot のパーミッション

openSUSE の既定では、DocumentRoot の ディレクトリ `/srv/www/htdocs` と CGI のディレクトリ `/srv/www/cgi-bin` はそれぞれユーザとグループが `root` に設定されています。これらのパーミッション 設定は変更すべきではありません。ディレクトリが書き込み可能であったりすると、任意のユーザからファイルを配置できるようになってしまいます。これらのファイルは Apache から `wwwrun` の権限下で実行され、ファイル システムの資源に対して望まないアクセスを発生させる結果になってしまいます。仮想ホストの DocumentRoot と CGI の配置先としては `/srv/www` のサブディレクトリを使用するものとし、それらのファイルやディレクトリが `root` ユーザおよびグループに属しているように設定してください。

18.7.3 ファイルシステムのアクセス

既定ではファイルシステム全体へのアクセスが禁止されるよう、`/etc/apache2/httpd.conf` に設定が為されています。これらのディレクティブを変更するのではなく、Apache から全てのディレクトリに アクセスし、必要なファイルを読み込むことができるように設定を追加してください。詳しくは「基本的な仮想ホスト設定」(353 ページ) をお読みください。これを行なうことで、たとえばパスワードやシステムの設定ファイル など、不必要なファイルへのアクセスを禁止し、外部から読み取られないようにすることができます。

18.7.4 CGI スクリプト

Perl, PHP, SSI やその他のプログラミング言語で対話的に動作するスクリプトは、結果的に任意のコマンドを実行できてしまい、広い範囲のセキュリティ問題につながります。また、サーバから実行されるスクリプトは、サーバ管理者が信頼する発信元から公開された ソースコードを利用してインストールしなければなりません。ユーザに対して独自の スクリプトを実行させてしまうことは、一般に良い方法ではありません。全てのスクリプトに 対し、セキュリティ監査を実施しておくことをお勧めします。

スクリプトの管理をできる限り簡単にするため、システム全体で CGI の実行を許可したり することをせず、専用のディレクトリ内でのみ実行できるようにするのが一般

的です。それぞれ `ScriptAlias` や `Option ExecCGI` のディレクティブを設定してください。openSUSE の既定の設定では、任意の場所からの CGI 実行は許可しない設定になっています。

全ての CGI スクリプトは同じユーザで動作するため、異なるスクリプト同士が互いに衝突してしまう場合もあります。このような場合は `suEXEC` を利用し、それぞれ異なるユーザやグループで CGI を実行するように設定してください。

18.7.5 ユーザディレクトリ

ユーザディレクトリを許可する場合 (`mod_userdir` または `mod_rewrite`) は、`.htaccess` の使用を禁止することを強くお勧めします。それは、このファイルがセキュリティの設定を上書きできてしまうものであるためです。少なくとも `AllowOverride` を利用して、ユーザ側で設定できることを制限してください。openSUSE では `.htaccess` が既定で有効に設定されていますが、`mod_userdir` を利用した場合、ユーザに対しては `Option` ディレクティブでの上書きは行なえないようになっています (詳しくは設定ファイル `/etc/apache2/mod_userdir.conf` をお読みください)。

18.8 トラブルシューティング

Apache がうまく起動しない場合や Web ページにアクセスできない場合、もしくはユーザが Web サーバに接続できない場合は、問題の原因を探ることが重要です。ここではよくエラーが発生する場所や、確認しておくべき場所を示します：

rcapache2 の出力

Web サーバの起動や停止を行なう場合、`/usr/sbin/httpd2` のバイナリではなく `rcapache2` スクリプトをお使いください (詳しくは 18.3 項「Apache の起動と停止」(361 ページ)をお読みください)。このスクリプトではより詳しい出力を行なうようになっているため、設定エラーの問題を解決する糸口を見つけやすくなります。

ログファイルとログの詳しさ

致命的なエラーであれそれ以外のエラーであれ、原因を探るには Apache のログファイルを利用するのがよいでしょう。既定では `/var/log/apache2/error_log` に出力されるエラーログファイルが主に役立つことでしょう。また、ログファイル内により詳しい出力を行ないたい場合は、`LogLevel` ディレクティブを利用してログメッセージの詳しさを設定してください。

ヒント: 単純なテスト

Apache のログメッセージを監視するには、`tail -F /var/log/apache2/my_error_log` コマンドを実行するのがよいでしょう。これで監視している状態から、`rcapache2 restart` を実行し、ブラウザで接続するとログの出力を確認することができます。

ファイアウォールとポート

一般的に良くある間違いとしては、Apache 向けのポートをファイアウォール設定で開いていない場合があります。YaST で Apache を設定した場合、この問題に対応するための個別オプションが提供されています (18.2.3 項「YaST を利用した Apache の設定」(354 ページ) をお読みください)。Apache を手作業で設定している場合、HTTP や HTTPS のポートを開くには、YaST のファイアウォールモジュールをご利用ください。

上記のようなやり方を行っても原因がよくわからない場合は、オンラインの Apache バグデータベース (http://httpd.apache.org/bug_report.html) (英語のみ) をご覧ください。また、Apache のメーリングリストを利用してユーザコミュニティに質問することもできます (詳しくは <http://httpd.apache.org/userslist.html> (英語) をお読みください)。それ以外にも、ニュースグループを利用することもできます (comp.infosystems.www.servers.unix) (英語)。

18.9 さらなる情報

apache2-doc パッケージでは、ローカルにインストールされる 各国語対応の Apache マニュアルやリファレンスが提供されています。このパッケージは 既定でインストールされませんので、最も手っ取り早くインストールしたい場合は `zypper in apache2-doc` コマンドでインストールを行ってください。インストールを行なったら、Apache のマニュアルが `ulink url="http://localhost/manual/"` からアクセスできるようになります。また、同マニュアルのオンライン版もご利用いただけます (<http://httpd.apache.org/docs-2.2/>)。SUSE 固有の設定ヒントなどは、`/usr/share/doc/packages/apache2/README.*` ディレクトリにあります。

18.9.1 Apache 2.2

Apache 2.2 での新機能の一覧については、http://httpd.apache.org/docs/2.2/new_features_2_2.html をお読みください。また、バージョン 2.0 か

ら 2.2 にアップグレードする際の情報は、<http://httpd.apache.org/docs-2.2/upgrading.html> をお読みください。

18.9.2 Apache モジュール

18.4.5項「外部モジュール」(370 ページ) に概要が書かれている Apache の外部 モジュールについて、詳しい情報はそれぞれ下記の場所にあります:

mod_apparmor

<http://en.opensuse.org/SDB:AppArmor>

mod_mono

http://www.mono-project.com/Mod_mono

mod_perl

<http://perl.apache.org/>

mod_php5

<http://www.php.net/manual/en/install.unix.apache2.php>

mod_python

<http://www.modpython.org/>

mod_tidy

<http://mod-tidy.sourceforge.net/>

18.9.3 開発

Apache のモジュールを開発したり、Apache の Web サーバプロジェクトに参加したり するための情報については、それぞれ下記の URL をご覧ください (いずれも英語が主体です):

Apache 開発者情報

<http://httpd.apache.org/dev/>

Apache 開発者ドキュメンテーション

<http://httpd.apache.org/docs/2.2/developer/>

Perl と C を利用した Apache モジュールの書き方

<http://www.modperl.com/>

18.9.4 その他の情報源

openSUSE での Apache 固有の問題に直面した場合は、まず <http://ja.opensuse.org/Apache> (日本語) または <http://old-en.opensuse.org/Apache> (英語) にある openSUSE wiki をお読みください。また、Apache の履歴は http://httpd.apache.org/ABOUT_APACHE.html にあります。このページでは、Apache が何故 Apache と呼ばれるようになったのかについても 記述しています。

YaST を利用した FTP サーバの設定

19

YaST *FTP* サーバ モジュールを利用することで、お使いの マシンを FTP (File Transfer Protocol) サーバとして機能するように設定することができます。また、お使いのマシンに匿名ユーザや認証ユーザが接続できるようにしたり、FTP プロトコルを利用してファイルをダウンロードできるようにしたりすることもできます。設定にもよりますが、FTP サーバに対してファイルをアップロードできるように設定することもできます。YaST では、お使いのシステムにインストールされた 各種の FTP サーバデーモンに対し、統一的なインターフェイスを提供しています。

YaST *FTP* サーバ 設定モジュールでは、2 種類の異なる FTP サーバを設定することができます:

- vsftpd (Very Secure FTP Daemon) and
- pure-ftp

設定は事前にサーバをインストールしてある場合にのみ行なうことができます。なお、標準の openSUSE® メディアには pure-ftp パッケージは含まれていません。その代わりに、YaST モジュールを設定することで pure-ftp パッケージをリポジトリ からインストールすることができます。

YaST *FTP* サーバ 設定モジュールは、2 種類の FTP サーバ デーモンに対応しています: vsftpd (Very Secure FTP Daemon の略) と pure-ftp です。インストール済みのソフトウェアのみを設定することができます。標準で配布される openSUSE メディアには pure-ftp の パッケージは同梱されていませんが、他のリポジトリから pure-ftp パッケージを インストールすることで YaST モジュールを利用することができるようになります。

vsftpd と pure-ftpd サーバは、それぞれ少しずつ異なる設定オプションを提供しています。具体的には、*詳細設定* ダイアログ内が少し異なります。この章では、vsftpd (openSUSE での既定のサーバ) を選択した場合を想定して手順を記述しています。

また、YaST FTP サーバモジュールがお使いのシステムに存在しない場合は、yast2-ftp-server パッケージをインストールしてください。

YaST を利用して FTP サーバを設定するには、下記の手順で行ないます:

- 1 YaST コントロールセンターを開き、ネットワーク サービス > *FTP* サーバを選択するか、もしくは root から yast2 ftp-server コマンドを実行します。
- 2 お使いのシステムに FTP サーバがインストールされていない場合は、YaST FTP サーバモジュールの起動時に、どの FTP サーバをインストールするかを選択するよう促されます。サーバを選択して (openSUSE では vsftpd が標準のサーバです) 進めてください。両方ともインストールされている場合は、どちらを使用するかを選択して *OK* を押します。
- 3 まずは *起動* のダイアログで、FTP サーバの起動に関する設定を行ないます。詳しくは 19.1項「FTP サーバの起動」(391 ページ) をお読みください。

次に *一般的な設定* ダイアログに移動します。FTP の ディレクトリや「ようこそ」メッセージ、ファイル作成時のマスクなどの各種設定を行なってください。詳しくは 19.2項「FTP の一般的な設定」(392 ページ) をお読みください。

パフォーマンス ダイアログでは、FTP サーバの性能に影響する 各種のパラメータを設定します。詳しくは 19.3項「FTP パフォーマンス設定」(393 ページ) をお読みください。

さらに *認証* ダイアログでは、匿名ユーザと認証ユーザによる アクセスを許可するかどうかを指定します。詳しくは 19.4項「認証」(393 ページ) をお読みください。

また、*詳細設定* ダイアログでは、FTP サーバの操作モードや SSL 接続、ファイアウォール設定などを行なうことができます。詳しくは 19.5項「詳細設定」(394 ページ) をお読みください。

- 4 最後に *完了* を押すと設定を保存することができます。

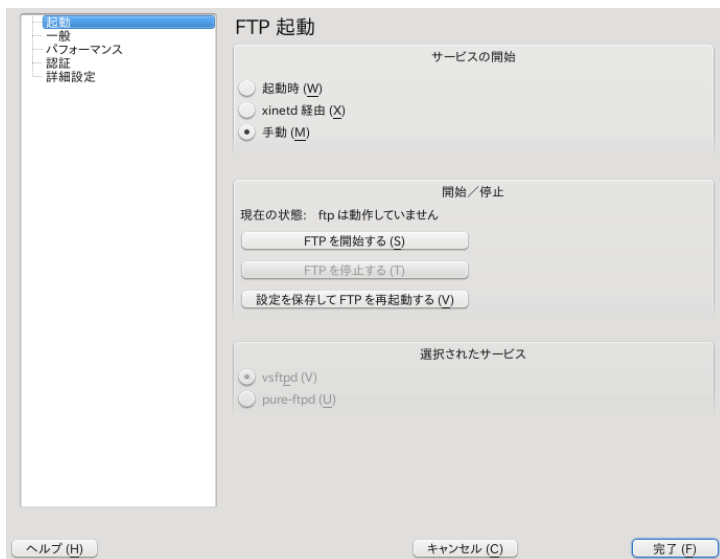
19.1 FTP サーバの起動

FTP 起動 ダイアログ内の *サービスの開始* では、FTP サーバの起動を設定することができます。システムの起動時に自動的に サービスを起動するか、もしくは手動で起動するかを選択することができます。FTP による接続があったときにのみサービスを起動したい場合は、*xinetd 経由* を選択してください。

また、現在の FTP サーバの状態が *FTP 起動* ダイアログ内の *開始／停止* の枠内に表示されます。*FTP を開始する* を選択すると、すぐにサービスを開始することができます。逆に サービスを停止するには、*FTP を停止する* を押してください。サーバの設定を変更した後は、*設定を保存して FTP を再起動する* を押すと設定を保存することができます。また、*完了* ボタンを押すと設定を保存することができます。

FTP 起動 ダイアログ内の *選択されたサービス* の欄には、どの FTP サーバを使用しているのか (vsftpd または pure-ftpd) が表示されます。両方のサーバがインストールされている場合には、これらの間を切り替えることもできます。設定を切り替えた場合、設定は自動的に変換されます。pure-ftpd パッケージは標準の openSUSE メディアには含まれていません。ご利用の場合は異なる インストール元からインストールしておく必要があります。

図 19.1 FTP サーバ設定 - FTP 起動



19.2 FTP の一般的な設定

FTP の一般的な設定 ダイアログ内の *一般的な設定* の枠内では、FTP サーバに接続した際に表示される 'ようこそ' メッセージを設定することができます。

また、全員を *chroot* のオプションを選択すると、全ての ローカルユーザはログイン後、自身のホームディレクトリ内をルートディレクトリ として *chroot jail* に配置されるようになります。この設定はセキュリティ向上の 目的から設定される項目ですが、特にユーザに対してアップロードの許可やシェル へのアクセスを許可している場合は注意して設定してください。

詳細なログ記録 設定を有効に指定すると、全ての FTP リクエスト (要求) とレスポンス (応答) が記録されるようになります。

また、匿名ユーザや認証済みユーザが作成するファイルに対して、*umask* による 許可制限を指定することができます。*umask* はビットで設定し、新しく作成する ファイルのアクセス権に対して「無効化したい (マスクしたい)」ビットを指定します。匿名ユーザに対するファイル作成マスクは *匿名ユーザの umask* に、認証済みユーザに対するファイル作成マスクは *認証ユーザの umask* にそれぞれ入力してください。それぞれのマスク値は 0 で始まる 8 進数の値で入力しなければなりません。*umask* についての詳しい説明は、*umask* のマニュアルページ (`man 1p umask`) をご覧ください。

さらに *FTP ディレクトリ* の枠では、それぞれ匿名ユーザと 認証済みユーザに対するディレクトリを指定することができます。*参照* ボタンを押すと、ローカルのファイルシステムからディレクトリを 選択することができます。匿名ユーザの既定の FTP ディレクトリは `/srv/ftp` に設定されています。なお *vsftpd* では、このディレクトリに対して全てのユーザに書き込みを許可することができません。代わりに、*upload* が作成され、そのディレクトリに対して 書き込み許可が与えられるようになります。

注記: FTP ディレクトリに対する書き込み権限

pure-ftpd サーバでは、このディレクトリに対して匿名ユーザの書き込みを許可することができます。*pure-ftpd* から *vsftpd* にサーバを切り替える際は、*pure-ftpd* で利用していた書き込み許可を取り除いていることをご確認ください。

19.3 FTP パフォーマンス設定

パフォーマンス ダイアログでは、FTP サーバの性能に関する各種のパラメータを設定することができます。*無通信タイムアウト時間* では、リモートのクライアントが最後に FTP コマンドを受信してから 待機する最大の時間 (分単位) を指定します。これ以上長い時間にわたって コマンドが受信できない場合は、リモートとの接続を切断します。*IP アドレスあたりの最大接続数* では、単一の IP アドレスから 最大で どれだけの数の接続を受け付けるかを指定します。また、*最大クライアント数* では、同時に接続可能な最大の クライアント数を指定します。これを超えるクライアントからのアクセスがあった場合 は、それらのクライアントにはエラーが返されます。

また、*認証ユーザの最大通信速度* では、認証済みのユーザに 対して設定する最大のデータ通信速度 (キロバイト毎秒 (KB/s) 単位) を指定することができます。匿名ユーザに対しては *匿名ユーザの最大通信速度* で指定します。既定の設定は 0 で、データ通信速度の制限を 外す意味になります。

19.4 認証

認証 ダイアログ内の *匿名ユーザと認証ユーザの許可* では、FTP サーバに対してどのユーザを許可するかを指定します: 匿名ユーザに対してのみアクセスを許可するか、認証ユーザに対してのみ許可するか、もしくはその両方に許可するかのいずれかを選択します。

FTP サーバでファイルのアップロードを許可するには、*認証* ダイアログ内の *アップロード* 枠内にある *アップロードの許可* を選択してください。匿名ユーザに対してもアップロードや ディレクトリの作成を許可するには、それぞれ関連するチェックボックスを選択してください。

注記: vsftpd—匿名ユーザに対するファイルアップロードの許可

vsftpd サーバを使用していて、かつ匿名ユーザに対してファイルのアップロードやディレクトリの作成を許可したい場合は、匿名 FTP ディレクトリ内にサブ ディレクトリを作成し、そのディレクトリに全てのユーザに対するアクセス許可を設定してください。

19.5 詳細設定

FTP サーバは、アクティブモードとパッシブモードのいずれかで動作します。既定ではサーバはパッシブモードで動作します。アクティブモードで動作させるように切り替えるには、*詳細設定* ダイアログ内の *パッシブモードを許可する* のオプション選択を外してください。またパッシブモードを許可する場合、*パッシブモード時の最小ポート番号* と *パッシブモード時の最大ポート番号* を設定し、データストリームで利用するポート範囲を指定することもできます。

サーバとクライアント間で暗号化通信を行ないたい場合は、*SSL を有効化* することができます。それぞれ SSL 暗号化 通信でサポートすべきプロトコルバージョンと、使用する DSA 証明書を指定してください。

お使いのシステムがファイアウォールで守られている環境の場合は、*ファイアウォールでポートを開く* を選択して FTP サーバへの 接続を許可するように設定することができます。

19.6 さらなる情報

FTP サーバについてさらに詳しく知るには、`vsftpd`, `vsftpd.conf` の各マニュアルページをお読みください。

パート IV. モバイル環境

Linux でのモバイルコンピューティング

20

モバイルコンピューティングとはラップトップコンピュータや PDA、携帯電話などを利用したコンピュータ環境のことで、それらの機器と PC とのデータ交換を行なう際にも利用する用語です。今では外付けのハードディスクやフラッシュドライブ、デジタルカメラなどをラップトップやデスクトップのシステムに接続できるようになっていて、様々なソフトウェアとともに利用することで様々な環境で便利に 使うことができるようになっています。

20.1 ラップトップ

ラップトップのハードウェアは通常のデスクトップとは異なります。これは可搬性や物理的な大きさ、電源消費の要件がより厳しいことによります。モバイル環境で利用できるハードウェアの製造元では、PCMCIA (Personal Computer Memory Card International Association) や Mini PCI, Mini PCIe など様々な標準インターフェイスを開発し、ラップトップのハードウェアを便利にするための努力を行っています。これらの標準は、メモリカードやネットワークインターフェイスカード、ISDN や モデムカード、外付けハードディスクについてもカバーしています。

ヒント: openSUSE とタブレット PC

openSUSE はタブレット PC にも対応しています。タブレット PC はタッチパッドやデジタイザと呼ばれる機器を搭載する PC で、マウスとキーボードを利用する代わりに デジタルペンや指を利用して入力や編集を行ないます。これらは他のシステムと同様に インストールし設定することができます。インストールと設定について、詳しい手順は 第24章 *タブレット PC の使用* (455 ページ) をお読みください。

20.1.1 電源管理

電源管理を最適化できるように設計されたシステムでは、電源の提供されていない環境であっても適切に動作するような構成になっています。このようにエネルギーを内部で保存しておく仕組みは、少なくともオペレーティングシステムが行なう仕組みと同様に重要なものです。openSUSE® では、ラップトップ環境で電力消費に関連する設定や、内蔵のバッテリーを利用した場合の利用時間に関連する設定を各種提供しています。下記の一覧では、電力消費を減らすために必要な設定について、重要なものから順に示しています：

- CPU 速度の低減
- 不要なときに行なうディスプレイの電源断
- 手作業によるディスプレイの電源設定の調整
- 使用されていなかったり、ホットプラグに対応していたりするアクセサリの接続解除 (USB CD-ROM や外付けのマウス、未使用の PCMCIA カードや 無線 LAN など)
- 未使用の際に行なうハードディスクの回転停止

openSUSE での電源管理について、背景となる詳細な情報は、第21章 *電源管理* (407 ページ) をお読みください。

20.1.2 利用環境の変化への対応

モバイルの環境では、お使いのシステムを操作環境にあわせた設定に変更したい場合がよくあります。環境に依存した多くのサービスやクライアントは、それぞれ再設定を行わなければなりません。openSUSE では、このような再設定 作業を自動化するための仕組みを提供しています。

図 20.1 既存の環境に対するモバイルコンピュータの接続

家庭内ネットワークと企業内ネットワークなどの間で移動を行なうラップトップで、影響があると考えられるのはそれぞれ下記のサービスです：

ネットワーク

IP アドレスの割り当て方法や名前解決、インターネットへの接続方法や 他のネットワークへの接続方法を含みます。

印刷

利用可能なプリンタや印刷サーバの一覧は、お使いのネットワーク環境によって異なることがあります。

電子メールとプロキシ

印刷と同様に、関連するサーバの一覧についても変更する必要があります。

X (グラフィカル環境)

お使いのラップトップをプロジェクタや外付けのモニタに一時的に接続する場合、別途のディスプレイ設定を行なう必要があります。

openSUSE では、利用環境の変化に対応するためにいくつかの手段を提供しています：

NetworkManager

NetworkManager は特にラップトップコンピュータでのモバイルネットワーク接続に対応した ソフトウェアです。異なるネットワーク環境やネットワークの種類同士 (たとえば モバイルブロードバンド (GPRS, EDGE, 3G など) や無線 LAN と有線 LAN) で、簡単かつ自動的に切り替える機能を提供します。NetworkManager は無線 LAN の WEP や WPA-PSK の暗号化にも対応しているほか、ダイヤル アップ接続 (smpppd 経由) にも対応しています。なお、両方のデスクトップ環境 (GNOME および KDE) に対応した NetworkManager のフロントエンドが提供されています。フロントエンドについて、詳しくは 23.4 項「KDE NetworkManager フロントエンドの使用」(441 ページ) と 23.5 項「GNOME NetworkManager の使用」(444 ページ) をお読みください。

表 20.1 NetworkManager の使用可否判断

お使いのコンピュータが…	NetworkManager の判断結果
ラップトップコンピュータである	利用をお勧めします
異なる複数のネットワークに接続されるマシンである	利用をお勧めします
ネットワークサービス (DNS や DHCP など) を提供するマシンである	利用はお勧めできません
固定の IP アドレスだけを使用するマシンである	利用はお勧めできません

NetworkManager がネットワーク設定を取り扱わない場合は、YaST を利用してネットワーク の設定を行ないます。

ヒント: DNS の設定とネットワーク接続の種類について

お使いのラップトップを頻繁に屋外に持ち出すような場合で、ネットワーク の 接続方法をいろいろ変えるような場合、NetworkManager は DHCP を介して、すべての DNS アドレスの割り当てを制御することができます。固定の DNS アドレスを 利用する接続をお使いの場合は、`/etc/sysconfig/network/config` ファイル内にある `NETCONFIG_DNS_STATIC_SERVERS` オプションを設定してください。

SLP

Service Location Protocol (SLP) は既存のネットワークに対するラップトップ の接続を簡単にすることができます。SLP を利用しない場合は通常、ラップトップの 管理者はネットワーク内で利用できるサービスについて、細かい知識を得ておく 必要があります。SLP はローカルネットワーク内に存在する全てのクライアントに 対し、提供されている特定のサービスを通知することができます。これにより、SLP に対応したアプリケーションは SLP からの通知情報を受け取り、自動設定を行なう ことができるようになっています。また SLP は、システムのインストールに対しても、必要なインストール元の設定を省略するために利用することができます。SLP について 詳しくは、第12章 ネットワーク内の SLP サービス (267 ページ) をお読みください。

20.1.3 ソフトウェアオプション

モバイル環境で使用する場合の様々な作業には、それぞれ対応した専用のソフトウェア が存在しています。たとえばシステムの監視 (特にバッテリーの充電状況表示) やデータの同期、周辺機器やインターネットとの無線通信などがあります。下記の章では、それぞれの作業に対応した openSUSE における重要なソフトウェア について述べています。

20.1.3.1 システム監視

openSUSE では 2 種類の KDE システム監視ツールが提供されています:

電源管理

電源管理 は、KDE デスクトップの動作のうち、省電力 に関わる箇所を調整 することのできるアプリケーションです。一般的には *バッテリーモニタ* のトレイアイコンからアクセスする もので、現在の電源接続種別に応じて、設定を行なうこ

とができます。この 設定ダイアログを開くもう 1 つの方法として、*Kickoff* アプリケーションランチャー を使用する方法もあります。これは アプリケーション > システム設定 > ハードウェア > 電源管理 からアクセスすることができます。

バッテリーモニタ のトレイアイコンをマウスの左ボタンで 選択すると、動作を設定することができます。動作は 5 種類の中からいずれか 適切なものを選ぶ仕組みで、たとえば プレゼンテーション ではスクリーンセーバーと省電力をすべて無効化し、システムイベントによって プレゼンテーションが邪魔されないようにします。また、*詳細...* を押すとさらに複雑な設定画面が表示されます。ここでは個別のプロファイルを 編集することができるほか、高度な電源管理オプションや通知機能、たとえば ラップトップの蓋を閉じた場合の動作や、バッテリーが残り少なくなった場合の 動作を設定することができます。

システムモニタ

システムモニタ (*KSysguard* と呼ばれています) は、様々なシステムパラメータを収集して単一の監視 環境に表示するプログラムです。出力情報は既定では 2 つのタブから構成 されていて、*プロセステーブル* では現在実行中の プロセスに関する詳細な情報、たとえば CPU の使用率やメモリの使用率、プロセス ID 番号や nice 値などが表示されます。収集された情報の表示 形態とフィルタ設定はカスタマイズすることができます。新しい種類の プロセス情報を追加するには、プロセステーブル内のヘッダをマウスの左 ボタンで押して、表示したい項目を選択します。また、様々なデータページに ある様々なシステムパラメータを監視することができるほか、ネットワークを 介して異なるマシンのデータを同時並行で収集することもできます。また、*KSysguard* は KDE 環境無しでデーモンとして実行させることもできます。このプログラムに関する詳細情報は、統合ヘルプ機能を利用するか、SUSE のヘルプページをお読みください。

GNOME デスクトップでは、*電源管理設定* と システム モニタ をご利用ください。

20.1.3.2 データの同期

携帯型のマシンにおいて、ネットワークから切り離された環境と接続された環境を切り替える場合、データの同期は重要な問題となります。データの同期は電子メールのほか、特定のディレクトリや個別のファイルが対象となり、ネットワークに接続されていない環境でも利用できるようにしておくことが望まれます。このような 要件を満たすには、下記のような方法があります：

電子メールの同期

ネットワーク内での電子メールアカウントについて、IMAP を利用するように 設定してください。あとはお使いの各マシンで IMAP のオフライン環境が利用できる 電子メールクライアント、たとえば Mozilla Thunderbird Mail, Evolution,

KMail などを設定するだけです。なお、電子メールクライアントは必ず設定を行ない、常に同じ送信済みメッセージにアクセスするようにしてください。これにより、全てのメッセージとその状態が同期できるようになります。また、メール送信時にはシステムに添付されている MTA である postfix や sendmail の代わりに、メールクライアントに実装された SMTP 機能を利用して設定してください。これにより未送信のメールに対して正しい応答を得ることができるようになります。

ファイルやディレクトリの同期

ラップトップとワークステーション間でデータを同期するために便利なユーティリティには、いくつかの種類があります。もっとも使われているコマンドラインツールは rsync と呼ばれているものです。詳しくは、第25章 *ファイルのコピーと共有* (465 ページ) をお読みください。

20.1.3.3 無線通信

ラップトップでは、家庭やオフィスで有線のネットワークに接続しているのと同じように無線接続を行なうことができます。無線では他のコンピュータに接続することができるだけでなく、周辺機器や携帯電話、PDA などとも接続することができます。Linux では下記の 3 種類の無線接続に対応しています：

無線 LAN

様々な無線技術により、無線 LAN は大規模な環境にも空間的に離れた環境にも利用できる唯一の技術になっています。マシン同士独立した無線ネットワークを構成して互いに接続することができるほか、そこからインターネットに接続することも可能です。アクセスポイントと呼ばれる機器は、無線 LAN を利用する端末に対するベースステーションとなり、インターネットにアクセスする際の中継機器として動作します。モバイル環境のユーザは、その居場所に依じてアクセスポイントを切り替えることができ、それにより最適な接続状態を維持することができるようになっています。無線 LAN のユーザは、その居場所に縛られることなく携帯電話のような巨大なネットワークにアクセスすることができます。無線 LAN について、詳しくは第22章 *無線 LAN* (417 ページ) をお読みください。

Bluetooth

Bluetooth は全ての無線技術の中で最も広い適用範囲を提供するネットワークです。コンピュータ (ラップトップ) や PDA、携帯電話などのように、IrDA と同程度に広い適用範囲を持っています。また、範囲内にある様々なコンピュータ同士の通信に利用できるほか、無線システムに対応したコンポーネント、たとえばキーボードやマウスなどとの通信にも対応しています。ただし、この技術で

はネットワーク内に ある物理的に離れたシステムに接続できるような仕組みは備えておらず、壁のような 物理的な障壁が存在する環境で通信を行なう場合は、無線 LAN が適切な選択に なります。

IrDA

IrDA は狭い範囲の無線通信に対応する無線技術です。通信する相手は互いに見える 範囲に存在しなければならず、壁のような障害物を越えることはできません。IrDA でよくある適用範囲としては、ラップトップと携帯電話の間でのファイル転送 です。ラップトップと携帯電話がごく近い範囲に存在している場合に IrDA を利用 し、それらが遠い場合には携帯電話などのネットワークを利用します。また、IrDA の適用範囲としては、オフィス内での印刷ジョブ配信などもあります。

20.1.4 データセキュリティ

理想的には、お使いのラップトップ内に存在するデータを望まないアクセスから 保護するための方法はいくつか存在しています。それぞれ下記のセキュリティ基準を考慮する必要があります：

盗難からの保護

可能な限りお使いのシステムを物理的な盗難から常時防いでおく必要があります。様々な保護ツール (たとえばチェーンなど) を量販店などから購入することができます。

強固な認証

ログインとパスワードに対する標準認証に加え、可能であれば生体認証を追加します。openSUSE では指紋認証に対応しています。詳しくは 第7章 *指紋読み取り装置の使用* (↑セキュリティガイド) をお読みください。

システムでのデータ保護

重要なデータは暗号化された通信路を介して転送するだけでなく、ハードディスク内 でも暗号化を行なうべきものです。これによりマシンが盗難被害にあった場合でも データを保護することができます。openSUSE での暗号化パーティションの 作成については、第10章 *パーティションとファイルの暗号化* (↑セキュリティガイド) をお読みください。もう 1 つの方法として、YaST からユーザを作成する際、暗号化ホームディレクトリを 設定することもできます。

重要: データセキュリティとディスクへのサスペンド

暗号化パーティションはディスクへのサスペンド (Suspend to Disk) のイベントが 発生した場合には、マウントが解除されません。そのため、これらの

パーティションにある全てのデータは、ディスクへのサスペンドを行なったマシンではレジューム (復帰) を行なうだけでアクセスできるようになってしまうことに注意してください。

ネットワークセキュリティ

全てのデータ転送は、その転送方法にかかわらず全て暗号化されるべきものです。Linux とネットワークに関する一般的なセキュリティ問題については、第1章 *セキュリティと機密保持* (↑セキュリティガイド) をお読みください。また、無線ネットワークでのセキュリティ基準については、第22章 *無線 LAN* (417 ページ) をお読みください。

20.2 モバイルハードウェア

openSUSE では、FireWire (IEEE 1394) や USB に接続された携帯型ストレージについて、自動検出を行なう機能が用意されています。*携帯型ストレージデバイス* には、FireWire や USB 接続のハードディスクのほか、USB フラッシュメモリやデジタルカメラも含んでいます。これらのデバイスは、システムが各インターフェイス経由で接続されたことを検知すると、自動的に検出され設定されます。GNOME や KDE に対応したファイルマネージャでは、携帯型のハードウェアをうまく処理するための機能を提供しています。これらのメディアを安全にマウント解除するには、それぞれのファイルマネージャから *安全に取り除く* (KDE) または *アンマウント* (GNOME) メニューをご利用ください。

外付けハードディスク (USB または FireWire)

システムから外付けのハードディスクが正しく認識されると、ファイルマネージャにそのアイコンが表示されるようになります。そのアイコンを選択して開くことで、ドライブ内の内容を表示することができます。その状態からファイルやフォルダを作成したりすることもできますし、編集や削除を行なうこともできます。システムが割り当てたハードディスクの名前を変更するには、アイコンの上でマウスの右ボタンを押すと表示されるメニューから、適切なメニューを選択してください。この名前の変更はファイルマネージャ内に表示される名前に対してのみ適用され、`/media` 内にマウントされるデバイス名に対しては反映されませんのでご注意ください。

USB フラッシュメモリ

これらのデバイスは、システムでは外付けのハードディスクと同じ扱いです。ファイルマネージャから名前を変更することもできます。

デジタルカメラ (USB または FireWire)

システムで認識されるデジタルカメラは、ファイルマネージャからは外付けのドライブのように表示されます。KDE では [camera:/](#) から 画像にアクセスすることができます。あとはそれぞれ digiKam や f-spot のようなツールを利用して処理することができます。写真の処理に関する高度な 処理を行なうには、GIMP をお使いください。

20.3 携帯電話と PDA

デスクトップシステムでもラップトップシステムでも、Bluetooth や IrDA を介して 携帯電話と通信を行なうことができます。型式によってはこれらの両方に対応している ものもありますが、いずれか片方にしか対応していないものもあります。これらの プロトコルに関する用途範囲については、20.1.3.3項「無線通信」(402 ページ) をお読みください。また、携帯電話側のこれらの設定方法については、お使いの機器の マニュアルをお読みください。

Palm, Inc. から発売されているハンドヘルドデバイスに対するデータ同期は、Evolution や Kontact で行なうことができます。デバイスに接続するための設定 作業は、ウィザードを利用して簡単に行なうことができます。いったん Palm Pilot に対する接続が完了したあとは、同期するデータを決定するだけです (連絡先、予定など)。

より洗練されたデータ同期を行ないたい場合は、opensync プログラムをお使いください。それぞれ libopensync パッケージと msyncntool パッケージ、および各デバイスに対応したプラグインを利用します。

20.4 さらなる情報

モバイルデバイスと Linux に関する全ての疑問については、<http://tuxmobil.org/> (英語) を読むのがよいでしょう。この Web サイトでは様々なセクションが用意されていて、それぞれラップトップの ハードウェアやソフトウェアのほか、PDA や携帯電話、その他のモバイルハードウェア に対応した情報が掲載されています。

似たようなアプローチをとっているサイトとして、<http://www.linux-on-laptops.com/> が作成した <http://tuxmobil.org/> (英語) というサイトもあります。ラップトップやハンドヘルドに関する情報も掲載されています。

また、SUSE ではラップトップに関するドイツ語の専用メーリングリストも用意しています。詳しくは <http://lists.opensuse.org/opensuse-mobile-de/> をお読みください。このメーリングリストでは、openSUSE でのモバイルコンピューティングについて、ユーザと開発者の双方が議論を行なっています。英語での投稿を行なってもかまいませんが、過去の投稿の多くはドイツ語で書かれていることに注意してください。なお、英語用のメーリングリストとして <http://lists.opensuse.org/opensuse-mobile/> も用意されています。

OpenSync についての情報は、<http://ja.opensuse.org/OpenSync> をお読みください。

電源管理

電源管理は特にラップトップ型のコンピュータでは重要な機能ですが、他のコンピュータであっても便利な仕組みです。その電源管理技術の 1 つである ACPI (Advanced Configuration and Power Interface) は、新しい製品であれば全てのもの (ラップトップ、デスクトップ、サーバ) に搭載されています。電源管理技術には適切なハードウェア構成と BIOS ルーチンが必要ですが、ほとんどのラップトップと多くの新しいデスクトップやサーバに搭載されています。また電源管理技術では、CPU の周波数を制御することで省電力を実現したり、動作音を低減したりすることもできます。

21.1 省電力機能

省電力の機能はラップトップ型コンピュータのモバイル使用に限らず、デスクトップシステムにおいても効果を発揮します。ACPI での主な機能と用途は下記の通りです:

スタンバイ
未対応です。

サスペンド (メモリへの)
このモードでは、システム全体の状態を RAM に書き込みます。その後、RAM を除く全てのシステムはスリープ状態に入ります。この状態により、システム全体の消費電力をととても抑えることができます。この状態の利点は数秒程度でスリープ前の作業を再開できるという点にあり、アプリケーションの起動や再起動が不要です。この機能は ACPI の S3 ステートと呼ばれる機能に対応していま

す。この状態のサポートは現在開発中の段階で、ハードウェア側に 大きく依存した作りになっています。

ハイバネーション (ディスクへのサスペンド)

このモードでは、システム全体の状態がハードディスクに書き込まれ、システムの電源が落とされます。このモードでは、最低でも RAM と同容量のサイズをスワップパーティションに用意して、システム全体の状態を書き込むことができるようにしなければなりません。この状態からの復帰には 30 秒から 90 秒程度の時間が必要で、この復帰処理が完了すると元の状態に戻すことができます。製造元によっては、このモードを組み合わせた機能、たとえば IBM Thinkpad では RediSafe と呼ばれるような機能が用意されている場合もあります。この機能は ACPI の S4 ステートと呼ばれる機能に対応しています。Linux ではディスクへのサスペンドはカーネルルーチンが実施する仕組みになっており、ACPI とは別途の実装になっています。

バッテリーモニタ

ACPI はバッテリーの充電状態をチェックし、その情報を提供します。また、残容量が限界に達した場合の処理を行なうこともできます。

自動電源 OFF

シャットダウンに続いてコンピュータの電源を切ることができる機能です。これは特に、バッテリーの容量が完全になくなる前に自動でシャットダウンを行なうような場合に重要です。

プロセッサの速度制御

CPU については、3 種類の異なる方法で省電力を実現することができます：周波数と電圧の制御 (PowerNow! や Speedstep として知られているもの)、プロセッサに対する減速指定、スリープの指定 (C-ステート) があります。コンピュータの動作モードによって、これらの方法を組み合わせることもできます。

21.2 Advanced Configuration and Power Interface (ACPI)

ACPI はオペレーティングシステムに対して個別のハードウェアコンポーネントを設定し制御できるようにした仕組みです。また、ACPI は Plug and Play (PnP) と Advanced Power Management (APM) に取って代わるもので、バッテリーや AC 電源、温度、冷却ファン、「ノート PC の蓋を閉じた」情報や「バッテリーの残容量が少ない」など、システムイベント情報を配信することができます。

BIOS では、個別のコンポーネントやハードウェアへのアクセス方法に関する情報を含んだ一覧表を提供しています。オペレーティングシステムは、この情報を利用して割り込みの割り当てやコンポーネントの有効化／無効化を設定します。ACPI ではオペレーティングシステムが BIOS 内に保存してあるコマンドを実行するため、ACPI の機能は BIOS の実装に依存することになります。ACPI が検出したり読み込んだりすることができる表については、`/var/log/boot.msg` にレポートが書き込まれます。また、ACPI の問題に対してトラブルシューティングを行なうには、21.2.2項「トラブルシューティング」(410 ページ)をお読みください。

21.2.1 CPU 性能の制御

CPU の省電力制御には 3 種類の方法があります：

- 周波数と電圧の調整
- クロック周波数の低減 (T-ステート)
- プロセッサに対するスリープ状態への移行 (C-ステート)

コンピュータの動作モードにも依存しますが、これらの方法は組み合わせて使用することができます。また、省電力によってシステムの発熱を抑え、頻繁に冷却ファンが動作したりしないようにする効果もあります。

周波数の制御と減速は、プロセッサが何も作業を行っていない場合には最も経済的な C-ステートが適用されるため、何らかの作業を行なっている場合にのみ効果があります。CPU が何らかの作業を行なっている場合は、省電力の実現にあたっては周波数の制御が お勧めです。プロセッサに対しては間欠的な負荷が与えられることがしばしばあるため、周波数を下げることができるという仕組みです。通常、動的な周波数制御はオンデマンドの制御方法でカーネルが行なうのがベストです。

周波数の減速は、高い負荷にもかかわらずバッテリーの動作時間を延ばしたい場合などの 最終手段として利用すべきものです。しかしながら、システムによっては減速時に滑らかに動作しないこともあります。また、CPU の減速は CPU が遅すぎる場合には意味を なさくなります。

より詳しい情報については、第11章 **電源管理** (↑システム分析とチューニングガイド)をお読みください。

21.2.2 トラブルシューティング

電源管理周りの問題としては、2 種類のが考えられます。1 つはカーネル側の ACPI コードにバグが存在していて、正しく認識されない問題です。この場合、解決方法をダウンロードとして提供することができます。また、場合によっては BIOS 側の原因で発生する場合があります。また、他のよく使われているオペレーティングシステムでエラーが発生しないようにするため、わざと BIOS 側の実装を ACPI 仕様から逸脱させてエラーを回避している場合があります。それ以外にも、ACPI 実装に深刻なエラーが存在するようなハードウェアコンポーネントは、Linux カーネル側でブラックリストとして ACPI が動作しないようにもしています。

問題を発見したときに最初にやるべきことは、BIOS を新しいものに更新することです。それでも全く起動できない場合は、下記の起動パラメータを設定することで回避できる場合があります：

`pci=noacpi`

PCI デバイスの設定について ACPI を使用しないようにします。

`acpi=ht`

シンプルナリソース設定だけを行ない、その他の目的では ACPI を使用しないようにします。

`acpi=off`

ACPI を無効に設定します。

警告: ACPI 無しでの起動問題

新しいマシン (特にマルチプロセッサシステムや AMD 64 システム) によっては、ハードウェアを正しく設定するのに ACPI が必要である場合があります。このような場合は、ACPI を無効に設定すると何らかの問題が発生します。

また、USB や FireWire のハードウェアが接続されているマシンでは、マシン側が混乱してうまく起動しない場合があります。うまく起動できない場合は、不要なハードウェアを全て取り外してから再度起動を行なってみてください。

起動後は、`dmesg | grep -2i acpi` コマンドを利用して起動メッセージを確認してください。ACPI 以外の原因で発生している場合も考えられますので、メッセージ全てを確認してもかまいません。ACPI テーブルを処理する際にエラーが発生した場合は、最も重要な DSDT (*Differentiated System Description Table*) テーブルを改善版に置き換えることができます。これを行なうことで、問題のある BIOS 側の DSDT を無視することができます。手順については 21.4.1 項「ハードウェア側で

ACPI が有効化されているのにうまく動作しない場合」(413 ページ)をお読みください。

カーネルの設定では、ACPI デバッグメッセージを有効化するためのスイッチが存在しています。カーネル側の ACPI デバッグ機能がコンパイルされていてインストールされている場合は、知識のあるユーザがエラーの原因を探るための情報を得ることができます。

BIOS やハードウェアの問題に直面した場合は、製造元に尋ねるのがお勧めです。特に製造元が Linux に対する支援を提供しない場合は、彼らにその問題点を提示して解決してもらう必要があります。製造元は、Linux を使用するユーザがある程度の数以上存在すれば、その問題を深刻なものとしてとらえることでしょう。

21.2.2.1 さらに情報

- <http://tldp.org/HOWTO/ACPI-HOWTO/> (詳細な ACPI HOWTO のほか、DSDT パッチも掲載されています)
- <http://www.acpi.info> (Advanced Configuration & Power Interface の仕様について)
- <http://www.lesswatts.org/projects/acpi/> (the Sourceforge 内の ACPI4Linux プロジェクト)
- <http://acpi.sourceforge.net/dsdt/index.php> (Bruno Ducrot 氏によるパッチ)

21.3 ハードディスクの休止

Linux では、不要であればハードディスクを完全にスリープ状態に移行させることもできるほか、省電力や静音モードに移行させることもできます。新しいラップトップであれば、不要な時に自動で省電力や静音のモードに切り替わるため、ハードディスクの電源を手作業で切ったりする必要はありません。しかしながら、最大限の省電力を実現したい場合は、hdparm コマンドを利用する下記の方法を試してみることをお勧めします。

このコマンドは様々なハードディスクの設定を行なうことができます。たとえば `-y` オプションを指定すると、指定したハードディスクをすぐにスタンバイモードに移行することができます。また、`-Y` オプションではスリープ状態に移行することができます。それ以外にも、`hdparm -S x` コマンドでは、一定時間の無動作でディスクの回転を

止める設定を行なうことができます。 x の値はそれぞれ下記のように設定してください: 0 を設定すると機能を無効にし、常に回転し続けるようになります。1 から 240 の値を指定すると、それぞれ 5 を掛けた値の秒数を指定したことになります。また、241 から 251 の値を指定すると、それぞれ 30 分を単位として 1 から 11 倍の時間を指定したことになります。

ハードディスク内部の省電力オプションを制御するには、-B オプションを設定します。0 から 255 までの値を設定し、小さければ小さいほど省電力を設定し、大きければ大きいほど性能を上げる指定になります。この値は使用するハードディスクに依存するため、具体的にどれだけの省電力になるのかは不明です。ハードディスクの動作音を低くしたい場合は、-M を設定してください。それぞれ 128 から 254 までの値で設定します。小さい値ほど静かになります。

ハードディスクをスリープ状態に移行させるのは簡単ではありません。Linux では様々なプロセスがハードディスクへの書き込みを行なうため、スリープを設定したとしても頻繁にスリープを解除させられる結果になります。そのため、Linux がハードディスクに書き込む必要のあるデータをどのように取り扱うのかについては、知っておくことが重要です。何よりもまず、全てのデータは RAM 内にあるバッファに保存されます。このバッファは `pdflush` デーモンが監視し、データが置かれてから一定の時間が経過するか、もしくは一定量まで使用されると、バッファの中身がハードディスクに書き込まれます。バッファサイズは動的に変化し、搭載されているメモリ量とシステムの負荷に依存して変動します。既定では `pdflush` は最大限の整合性保持のため、短い時間間隔に設定されています。既定では、5 秒おきにバッファが確認され、ハードディスクにデータが書き込まれます。それぞれ下記の値で調整することができます:

```
/proc/sys/vm/dirty_writeback_centisecs
```

`pdflush` のスレッドが起動するまでの遅延時間 (1/100 秒単位)

```
/proc/sys/vm/dirty_expire_centisecs
```

ディスクに書き込むべきデータについて、メモリ上に待機させる時間を指定します。既定は 3000 で、30 秒を意味します。

```
/proc/sys/vm/dirty_background_ratio
```

`pdflush` がディスクに書き込むべきデータをメモリ上に保持する最大割合を指定します。既定値は 5% です。

```
/proc/sys/vm/dirty_ratio
```

メモリ上に存在するディスクに書き込むべきデータと全体メモリ量の比較で、この値を上回った場合は、そのプロセスに対してバッファへの書き込みを継続せずにディスクへの書き込みを行なわせるようにします。

警告: データの整合性の損傷

pdflush デーモンの設定を変更すると、データの整合性が損なわれることがあります。

これらのプロセスとは別に、ReiserFS, Ext3, Ext4 などのジャーナリング機能 付きのファイルシステムでは、pdflush とは独立したメタデータの書き込みを行なう機能が備わっています。そのため、これらのファイルシステムを利用することによって、ハードディスクの回転停止が阻害される場合もあります。このような問題を回避するには、モバイルデバイス向けの特別なカーネル拡張を利用する必要があります。詳しくは `laptop-mode-tools` パッケージをインストールし、`/usr/src/linux/Documentation/laptops/laptop-mode.txt` ファイルをお読みください。

また、それ以外にも動作中のプログラムがどのように振る舞うのかについても注意を払う必要があります。たとえば気の利いたエディタであれば、現在編集中的のファイルについて、隠しファイルを利用した定期的なバックアップを行なっていたりすることがあります。このような動作があると、ハードディスクが定期的に動き出す結果になってしまいます。データの整合性は犠牲になりますが、省電力を求める際には、このような機能は無効化しておくのがよいでしょう。

また、これに関連してメールデーモンである postfix には、`POSTFIX_LAPTOP` という変数が存在しています。この 値を `yes` に設定すると、ハードディスクに対して頻繁にアクセスしたりしないようになります。

21.4 トラブルシューティング

全てのエラーメッセージと警告は、`/var/log/messages` ファイルに書き込まれます。本章ではよく発生する問題について記述しています。

21.4.1 ハードウェア側で ACPI が有効化されているのにうまく動作しない場合

ACPI について何らかの問題に直面した場合は、`dmesg` コマンドの 出力から ACPI 固有のメッセージを検索してください。たとえば、`dmesg | grep -i acpi` のように実行します。

また、問題を解決するには BIOS の更新が必要となる場合もあります。お使いのラップトップの製造元 Web ページをご覧ください、BIOS の更新版がないかどうかをご

確認ください。また、最新の ACPI 仕様に準拠しているかどうかも合わせてご確認ください。BIOS を 交しかしても問題が解決しない場合は、下記の手順で問題のある BIOS 内の DSDT テーブル を更新してください:

手順 21.1 BIOS 内の DSDT テーブルの更新

下記の手順を実行する前に、必要なパッケージがインストールされていることをご確認ください。kernel-source, acpica, mkinitrd の各パッケージが必要です。

- 1 お使いのシステムに対応した DSDT を、<http://acpi.sourceforge.net/dsdt/index.php> から ダウンロードします。ファイルが圧縮されている場合はそれを展開してください。ファイルの拡張子が .aml (ACPI マシン言語) になっている場合は手順 3 に移動してください。それ以外の場合は、次の手順を実施してください。
- 2 ダウンロードしたテーブルのファイル拡張子が .asl (ACPI ソース言語) である場合は、下記のコマンドでコンパイルを行なってください。

```
iasl -sa file.asl
```
- 3 ファイル DSDT.aml を任意の場所 (/etc/DSDT.aml がお勧めです) にコピーします。
- 4 /etc/sysconfig/kernel を編集し、DSDT ファイルの パスを指定します。
- 5 あとは mkinitrd コマンドを実行して initrd を作成すれば 完了です。新しいカーネルをインストールした場合は、mkinitrd コマンドを実行すると initrd が作成され、変更済みの DSDT が統合されてシステム起動時に読み込まれるようになります。

21.4.2 CPU の周波数制御がうまく働かない場合

カーネルのソースコードを参照し、お使いのプロセッサに対応しているかどうかを確認してください。また、CPU の周波数制御を働かせるためには特別なカーネルモジュールや モジュールオプションが必要になる場合もあります。kernel-source パッケージがインストール されている場合、これらの情報は /usr/src/linux/Documentation/cpu-freq/* にあります。

21.4.3 サスペンドやスタンバイがうまく働かない場合

ACPI システムでは、誤った DSDT 実装 (BIOS) によってサスペンドやスタンバイに問題が発生する場合があります。このような場合は、BIOS を更新してください。

また、システムが不具合のあるモジュールの読み込みを解除する際には、システムが停止してしまったり、サスペンドのイベントが動作しなかったりする場合があります。同じようなことは、サスペンドを妨害するサービスを停止する際にも発生する場合があります。いずれの場合とも、スリープモードへの移行を妨害しているものを調べてください。ログファイル `/var/log/pm-suspend.log` には、何が行なわれているのかを示す情報と、考えられるエラー情報がそれぞれ記載されています。また、サスペンドやスタンバイに移行する前に読み込みを解除しておきたいモジュールがある場合は、`/usr/lib/pm-utils/defaults` ファイル内の `SUSPEND_MODULES` 変数に設定を行なってください。

なお、サスペンドとそこからの復帰処理について変更を行なうための方法は、<http://ja.opensuse.org/Pm-utils> (日本語) または <http://old-en.opensuse.org/Pm-utils> (英語)、および <http://ja.opensuse.org/S2ram> (日本語) または http://ja.opensuse.org/SDB:Suspend_to_RAM (日本語) をお読みください。

21.5 さらなる情報

- <http://www.acpi.info> (Advanced Configuration and Power Interface の仕様)
- <http://www.lesswatts.org/projects/acpi/> (Sourceforge にある ACPI4Linux プロジェクトのページ)
- <http://acpi.sourceforge.net/dsdt/index.php> (Bruno Ducrot 氏による DSDT パッチ)
- <http://ja.opensuse.org/S2ram> (日本語) または http://wiki.opensuse.org/SDB:Suspend_to_RAM (英語) RAM へのサスペンドを動作させる方法

- <http://ja.opensuse.org/Pm-utils> (日本語) または <http://old-en.opensuse.org/Pm-utils> (英語) 汎用サスペンドフレームワークを修正する方法

無線 LAN

無線 LAN はワイヤレス LAN や WLAN (Wireless Local Area Network) とも呼ばれますが、これはモバイルコンピューティングにおいては欠くことの できない要素になっています。今やほとんどのラップトップコンピュータ には無線 LAN カードが搭載されています。この章では、YaST を利用した 暗号化などの無線 LAN カード設定方法について記しています。なお、無線 LAN は NetworkManager を利用して設定することも できます。詳しくは 第23章 *NetworkManager* の使用 (435 ページ) をお読みください。

22.1 無線 LAN 標準

無線 LAN は IEEE という業界団体が作成した 802.11 標準を利用して通信を行っています。もともとこの標準は最大転送速度を 2 Mbit/s (メガビット毎秒) としていましたが、転送速度を上げる目的で様々な仕様追加 が行なわれました。これらの仕様追加では変調方法や転送出力、転送レート (詳しくは 表22.1「様々な無線 LAN 標準の概要」(417 ページ) をお読みください) の見直しが行なわれました。また、多くの企業ではハードウェアに対して 独占技術や草案段階の機能を追加してきました。

表 22.1 様々な無線 LAN 標準の概要

名前	帯域 (GHz)	最大転送レート (Mbit/s)	注意
802.11 (オリジナル)	2.4	2	古い規格であり、今や対応機

名前	帯域 (GHz)	最大転送レート (Mbit/s)	注意
			器はほとんど存在していません
802.11a	5	54	干渉に強い特性があります
802.11b	2.4	11	今はあまり使われていません
802.11g	2.4	54	11b との後方互換性があり、広く利用されています
802.11n	2.4, 5 (いずれか、または両方)	300	一般的に利用されています

802.11 オリジナルのカードは openSUSE® では対応していません。多くのカードは 802.11a, 802.11b, 802.11g, 802.11n のいずれか (または これらのうちの複数) に対応しているためです。新しいカードでは 802.11n 標準に対応していますが、802.11g としても利用できます。

22.2 動作モード

無線ネットワークにおいては、高速で高品質でかつ機密の高い通信を行なうため、様々な技術と設定が利用されます。動作モードが異なると異なる設定を行なう必要があります。また、正しい認証方法を選択するのは難しく、利用可能な暗号化にもそれぞれ異なるメリットやデメリット、間違いやすい点などが存在しています。

基本的に、無線ネットワークは下記の 3 つのネットワークモードに分類されます：

管理モード (マネージド、またはインフラストラクチャモードとも呼ばれるアクセスポイント経由の通信)

管理ネットワークには、管理要素であるアクセスポイントと呼ばれるものが存在します。管理モードはインフラストラクチャモードとも呼ばれ、このモードでは無

線 LAN を利用するコンピュータの通信は全て そのアクセスポイントを介して行ないます。これにより、アクセスポイントは イーサネットとの接続ポイントとして動作します。また、特定のクライアント だけが接続できるようにするため、様々な認証メカニズム (WPA など) が 使用されます。

アドホックモード (一対一ネットワーク)

アドホックネットワークにはアクセスポイントがありません。それぞれの 無線 LAN コンピュータは直接通信を行なうため、アドホックネットワークは 一般に管理モードよりも高速で通信することができます。ただし、アドホック ネットワークでは転送帯域と参加しているコンピュータ数によって、大幅に 速度が制限されることになります。また、このモードは WPA 認証には対応 していません。そのため、WPA を利用したい場合はアドホックモードを利用 すべきではありません。

マスターモード

マスターモードでは、お使いのネットワークカードをアクセスポイントとして 使用します。このモードを利用するには、お使いの無線 LAN カードがこの モードに対応している必要があります。お使いの無線 LAN カードについて、詳しくは <http://linux-wless.passsys.nl> をお読みください。

22.3 認証

無線ネットワークは有線ネットワークに比べて傍受や妨害が容易であるため、認証や暗号化方法に関する様々な標準が規定されています。オリジナル版の IEEE 802.11 標準では WEP (Wired Equivalent Privacy) という用語で規定 されていました。しかしながら WEP は機密が保てないことが証明されてしまった (22.6.3 項「セキュリティ」(431 ページ) をお読みください) ため、WLAN industry (*Wi-Fi Alliance* に加わりました) は WPA と呼ばれる WEP の弱点を解消する拡張を規定しました。その後 WPA は IEEE 802.11i 標準 となって WPA の仕様を含むこととなり、各種の認証や暗号化 方法を規定する仕組みになりました。旧来の WPA は IEEE 802.11i のドラフト版 をベースにしていたため、IEEE 802.11i は WPA2 と しても知られています。

認可済みの端末だけが接続することができるよう、ネットワーク では下記のように 様々な認証方法が使用されます:

なし (オープン)

オープンシステムでは何も認証を必要としません。任意の端末が ネットワークに参加できます。ただし、WEP 暗号を使用することは可能です。詳しくは 22.4項「暗号化」(421 ページ) をお読み ください。

共有鍵 (IEEE 802.11 による)

この方式では、WEP 鍵を認証に使用します。しかしながら、WEP 鍵を認証に使用してしまうと容易に攻撃を受けてしまうため、認証は必須ではありません。攻撃者がやるべきことは、端末とアクセス ポイントの通信を十分長く受信し続けることだけです。認証処理では両者が 同じ情報を交換します。1 回は暗号化を行なった方式で、もう 1 回は暗号化を行なわない方式で実施します。これにより、適切なツールを利用して鍵を再構築することができるようになります。この方式では認証と暗号化の両方に WEP 鍵を使用するため、ネットワークのセキュリティを高めることにはなりません。また、端末側は認証や暗号化、暗号化解除のために正しい WEP 鍵を設定しておく必要があります。鍵を持っていない端末は受信したパケット 解読できないため、認証を行なうべきかどうかに関わらず通信を行なうことが できなくなります。

WPA-PSK (IEEE 802.1x では WPA-Personal とも呼ばれる)

WPA-PSK (PSK とは Pre Shared Key (事前共有鍵) の略) は、共有鍵と似た手順で通信を行ないます。参加している全ての端末とアクセスポイントに同じ鍵を設定します。鍵は 256 ビットの長さがあり、一般にパスフレーズという形で入力を行ないます。このシステムには WPA-EAP のような複雑な鍵管理は不要であるため、個人使用には便利な仕組みになっています。そのため、WPA-PSK は WPA「Home (家庭用)」と呼ばれる場合もあります。

WPA-EAP (IEEE 802.1x では WPA-Enterprise とも呼ばれる)

実際のところ、WPA-EAP (Extensible Authentication Protocol) 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 は企業のような環境で無線ネットワークを守るために使用します。個人用のネットワークではほとんど使用されません。そのため、WPA-EAP は WPA「Enterprise (企業用)」と呼ばれる場合もあります。

WPA-EAP では Radius サーバと呼ばれるものを使用してユーザを認証します。EAP では、サーバに対して接続と認証を行なうのに、下記に示す 3 種類の方法を利用することができます：

- Transport Layer Security (EAP-TLS): TLS 認証は、サーバとクライアントの間で証明書をお互いに交換し合うことによって認証を実現します。最初にサーバが自身の証明書をクライアントに対して提示し、クライアント側での検証を行ないます。クライアント側でその証明書が正しいものであると判断されると、今度はクライアント側からサーバに対して証明書を送信します。TLS を機密に保つには、お使いのネットワーク内で証明書管理のインフラストラクチャが必要となります。このようなインフラストラクチャは、個人用のネットワークではほとんど用意されていません。

- Tunnelled Transport Layer Security (EAP-TTLS)
- Protected Extensible Authentication Protocol (EAP-PEAP): TTLS と PEAP は、いずれも 2 ステージから構成されるプロトコルです。最初の ステージで機密を保持できる接続を確立し、次のステージでクライアントの 認証データを交換します。TLS による証明書管理インフラストラクチャが 存在する場合でも、証明書を管理するための手間が存在しない分だけ オーバーヘッドがずっと少なくなります。

22.4 暗号化

認可されていないユーザが無線ネットワーク内で交換されているデータを読み 出したり、ネットワークに対するアクセス許可を得てしまったりするこ ことを 防ぐため、様々な暗号化方法が提供されています:

WEP (IEEE 802.11 による)

この標準では RC4 暗号化アルゴリズムを使用します。元々は 40 ビットの鍵長で暗号化を行なっていましたが、のちに 104 ビットの 鍵長にも対応するよう になりました。それぞれ 40 ビット鍵を 64 ビット鍵と表わしたり、104 ビット鍵を 128 ビット 鍵と表わしたりすることもあります。それぞれ 24 ビット分を 初期ベクトルとして使用する分を含めているためです。しかしながら、この標準にはいくつかの弱点が見つ ています。このシステムが生成した 鍵に対する攻撃は、ほとんどの場合で成功してしま います。それでも全く 暗号化を行なわないよりは WEP を使用したほうがまだ適切です。

また、製造元によっては非標準の「動的 WEP 」を実装している場合があります。WEP と全く同じ仕組みで同じ弱点を持っています が、鍵管理サービスを使用して鍵を定期的に変更する点で異なっています。

TKIP (WPA/IEEE 802.11i による)

この鍵管理プロトコルは WPA 標準で規定されているもので、WEP と同じ 暗号化方式を使用しますが、その弱点を克服しています。それは、それぞれのデータパケットで新しい鍵を生成するため、これらの鍵への攻撃は 意味がなくなるためです。TKIP は WPA-PSK と共に使用します。

CCMP (IEEE 802.11i による)

CCMP は鍵管理を規定するものです。一般に WPA-EAP との接続で使用しま すが、WPA-PSK でも使用することができます。暗号化方式は AES を使用するため、WEP 標準である RC4 よりは強い暗号になっています。

22.5 YaST を利用した設定

重要: 無線ネットワークにおけるセキュリティリスク

無線 LAN の接続で暗号化を行なわないと、全てのネットワークデータに対して第三者からの傍受を許す結果になってしまいます。利用可能な認証方法や暗号化のうちのいずれかを利用して、お使いのネットワーク通信が保護されていることをご確認ください。

また、お使いのハードウェアに対応する最適な暗号化方法をお使いください。ただし、特定の暗号化方法を利用するには、ネットワーク内に存在する全てのデバイスがその暗号化方法に対応している必要があります。対応していないデバイスが存在した場合は、それらのデバイスは互いに通信できなくなってしまいます。たとえばお使いのルータが WEP と WPA の両方に対応しているものの、お使いの無線 LAN カードが WEP にしか対応していない場合、共通に利用できる WEP を選択することになります。ただし、WEP による暗号化は 何も暗号化をしないよりは良い程度のものであることに注意してください。詳しくは 22.4 項「暗号化」(421 ページ) と 22.6.3 項「セキュリティ」(431 ページ) をお読みください。

YaST で無線 LAN を設定するには、下記のパラメータを設定する必要があります:

IP アドレス

固定の IP アドレスを設定するか、もしくはインターフェイスに対して動的な割り当てを行なうため、DHCP サーバを利用するように設定します。

操作モード

無線 LAN とお使いのマシンとの接続方法を設定します。これはネットワーク側の要件によって異なります。詳しくは 22.2 項「動作モード」(418 ページ) をお読みください。

ネットワーク名 (ESSID)

ネットワークを識別するための名称を設定します。

認証と暗号化に関する詳細

ネットワーク側で提供されている認証や暗号化方法に依存し、それぞれ 1 つ または複数の暗号鍵や証明書を設定します。

暗号鍵を入力するにあたっては、複数の入力方法があります。パスフレーズ、ASCII (WEP 暗号の場合にのみ利用できます)、16 進のいずれかを選択できます。

22.5.1 NetworkManager の無効化

無線 LAN カードは通常、インストール時に検出されます。お使いのマシンがモバイル用途のコンピュータである場合は、既定で NetworkManager が有効になります。無線 LAN カードを YaST から設定する場合は、まず NetworkManager を無効に設定する必要があります:

- 1 root で YaST を起動します。
- 2 YaST コントロールセンター では、ネットワークデバイス > ネットワークの設定 を選択し、ネットワーク設定 ダイアログを開きます。

お使いのネットワークが NetworkManager で制御されるように設定されている場合、YaST でネットワーク設定を編集できない旨の警告メッセージが表示されます。

- 3 YaST で編集できるようにするには、OK を押して メッセージを閉じ、グローバル オプション タブにある *ifup* を利用した従来の方法 を選択します。
- 4 ここから先の設定については、22.5.2 項「アクセスポイントを利用する設定」(423 ページ) または 22.5.3 項「Ad-Hoc (アドホック) ネットワークの構成」(427 ページ) の手順に従ってください。

設定が終わったら、OK を押してネットワーク設定を 保存します。

22.5.2 アクセスポイントを利用する設定

この章では、お使いの無線 LAN カードを (外付けの) アクセスポイントに接続する設定、もしくはお使いの無線 LAN カード自身をアクセスポイントとする設定 (ただし後者についてはお使いの無線 LAN カード側での対応が必要です) について、手順を示しています。アクセスポイントを利用しない種類のネットワークを設定する場合は、22.5.3 項「Ad-Hoc (アドホック) ネットワークの構成」(427 ページ) をお読みください。

手順 22.1 お使いの無線 LAN カードについてアクセスポイントを利用するよう設定する方法

- 1 YaST を起動し、ネットワーク設定 ダイアログを開きます。

- 2 概要 タブに移動し、システムで検出された全てのネットワーク デバイスを表示します。一般的なネットワーク設定について、詳しくは 11.4 項「YaST を利用したネットワーク接続の設定」(223 ページ) をお読みください。
- 3 一覧から無線 LAN カードを選択し、編集 ボタンを押して ネットワークカードの設定 ダイアログを表示します。
- 4 アドレス のタブでは、お使いのマシンに対して動的な IP を 割り当てるか、もしくは固定で割り当てるかを設定します。通常は 可変 IP アドレス を選択し、DHCP を選びます。
- 5 次へ を押して、無線ネットワークカードの設定 ダイアログに移動します。
- 6 お使いの無線 LAN カードからアクセスポイントに接続する場合は、動作モード を 管理 に設定します。

逆にお使いの無線 LAN カードをアクセスポイントとして設定したい場合は、動作モード を マスター に設定します。ただし、このモードは必ずしも全ての無線 LAN カードで利用できるとは限らない ことに注意してください。

注記: WPA-PSK または WPA-EAP の使用

WPA-PSK または WPA-EAP の認証モードを使用したい場合は、動作モード を 管理 に設定しなければなりません。

- 7 特定のネットワークに接続するには、ネットワーク名 (ESSID) に名称を入力します。名称を直接入力する以外にも、ネットワークの検索 を押して利用可能なネットワークの 一覧から選択することもできます。

無線ネットワーク内に存在し、相互に通信する全ての端末には、同じ ESSID を設定する必要があります。ESSID を設定しない場合、お使いの無線 LAN カードは、自動的に最も強い信号強度のアクセスポイントに接続しようとします。

注記: WPA 認証には ESSID が必要です

WPA 認証を選択した場合、ネットワーク名 (ESSID) は 必ず設定しなければなりません。

- 8 次にお使いのネットワークでの 認証モード を選択します。どのモードが適切であるかについては、お使いの無線 LAN カードのドライバと、ネットワーク内にある他のデバイスの機能に依存して決まります。

- 9 認証モードを暗号化無しに設定した場合は、次へ を押すと設定が完了します。最後に 潜在的なセキュリティリスクに関するメッセージを確認し、概要 タブ (新しく設定した無線 LAN カードが表示されているはずです) から OK を押して終了です。

その他の認証モードを選択した場合は、手順22.2「暗号化の詳細設定の入力」(425 ページ)に進みます。

図 22.1 YaST: 無線ネットワークカードの設定

手順 22.2 暗号化の詳細設定の入力

下記に示す認証モードの場合、暗号鍵を設定する必要があります: *WEP - オープン*, *WEP - 共有鍵*, *WPA-PSK*

WEP の場合は 1 つだけ鍵を指定すれば十分です。ただし、お使いのステーションに対しては最大で 4 つまでの異なる鍵を設定することができます。これらのうちのいずれか 1 つの鍵を既定の鍵として設定し、暗号化に使用することになります。その他の鍵は復号化の際にのみ使用されます。既定では鍵の長さが 128 ビットになっていますが、64 ビットの鍵を選択して設定することもできます。

より高いセキュリティを実現するには、RADIUS サーバを利用してユーザの認証を行なう WPA-EAP をお使いください。サーバで認証を行なう際には、3 種類の認証方法、それぞれ TLS, TTLS, PEAP と呼ばれる方法を利用することができます。WPA-EAP に必要な資格情報と証明書は、RADIUS サーバで利用できる認証方

法によって決まります。YaST は /etc/cert ディレクトリ 以下にある任意の証明書を検索します。そのため、付与された証明書を上記の ディレクトリに保存しておき、これらのファイルに対してアクセスを制限する (パーミッションで 0600、つまり所有者が読み書きだけを行なうことのできる状態) ように設定してください。

1 WEP - オープン または WEP - 共有鍵 の暗号鍵を指定するには、下記の手順で行ないます:

1a まずは **鍵入力種類** を選択します。パスフレーズ、ASCII 16 進数 のいずれかを選択します。

1b 次に **暗号鍵** を必要な分だけ入力します (通常は 1 つの鍵だけを使用します):

パスフレーズを選択した場合は、それぞれ鍵の長さに 合った長さの文字列を入力します (既定では 128 ビット分を指定します)。

ASCII を選択した場合は、64 ビット鍵を利用する 場合は 5 文字を、128 ビット鍵を利用する場合は 13 文字を入力します。

16 進数 を選択した場合は、64 ビット鍵を利用する 場合は 10 文字を、128 ビット鍵を利用する場合は 26 文字をそれぞれ 16 進数で入力します。

1c より短いビット数の鍵に設定するには、**WEP キー** を 選択して **鍵の長さ** を 64 ビットに設定してください。**WEP 鍵** ダイアログでは、それまでに入力された WEP 鍵を表示することができます。また、特に既定の 鍵を設定しない場合、YaST は最初の鍵を既定の鍵として使用します。

1d さらなる WEP 鍵を入力する場合や、いずれかの鍵を変更する場合は、それぞれ 設定したい鍵の項目を選んで **編集** ボタンを押します。その後、**鍵入力種類** を選んで鍵を入力してください。

1e 最後に設定内容を確認し、**OK** を押して閉じます。

2 WPA-PSK の鍵を入力するには、下記の手順で行ないます:

2a まずは鍵の入力方法を、パスフレーズ または 16 進数 のいずれかから選択します。

2b **暗号鍵** の欄に入力方法に従った方法で 鍵を入力します。

パスフレーズモードの場合、入力は 8 文字から 63 文字 までの間で指定します。16 進数 モードの場合、64 文字で指定します。

- 3 WPA-EAP 認証を選択した場合は、次へ を押して WPA-EAP ダイアログに移動し、ネットワーク管理者 から付与された資格情報と証明書を入力します。

3a まずは RADIUS サーバが認証時に使用する EAP モード を選択します。以降の手順では、選択した EAP モード によってそれぞれ異なる情報の入力が必要になります。

3b TLS を選択した場合、識別情報、クライアント証明書、クライアント鍵、クライアント鍵パスワード をそれぞれ設定します。セキュリティを維持するには、サーバの正当性を確認するための項目 サーバ証明書 も合わせて設定するとよいでしょう。

TTLS や PEAP の場合、識別情報 とパスワード を指定します。サーバ証明書 と 匿名 については必要に応じて設定してください。

3c WPA-EAP の設定についてより高度な設定を行なうダイアログを表示するには、詳細 ボタンを押します。

3d まずは EAP-TTLS や EAP-PEAP の通信における第 2 ステージ (内側の認証) の 認証方法 を選択します。RADIUS サーバに対する認証 方法の選択は、以前のダイアログで行なったものになります。

3e 自動決定された設定がうまく動作しない場合、PEAP バージョン の値を設定して特定の PEAP 実装を使用するように強制することもできます。

- 4 設定内容を確認し、OK を押します。概要 タブ内に新しく設定した無線 LAN カードが表示される ようになります。

- 5 最後に OK を押すと設定を完了し、ダイアログを閉じることが できます。

22.5.3 Ad-Hoc (アドホック) ネットワークの構成

環境によっては、無線 LAN カードの搭載された 2 台の PC で直接通信を行なったほうが都合の良い場合があります。YaST を利用してアドホックなネットワーク 環境を構築するには、下記の手順で行ないます:

- 1 YaST を起動し、ネットワーク設定 ダイアログを 開きます。

- 2 **概要** タブに移動し、一覧から無線 LAN カードを選択します。選択したら **編集** ボタンを押し、**ネットワークカードの設定** ダイアログを開きます。
- 3 **固定 IP アドレス** を選択し、下記のデータを入力します:
 - **IP アドレス**: 192.168.1.1 を指定します。もう 1 台のコンピュータでは、たとえば 192.168.1.2 のように 指定します。
 - **サブネットマスク**: /24 を指定します。
 - **ホスト名**: 任意の名前を入力します。
- 4 **次へ** を押して進めます。
- 5 **動作モード** を **アドホック** に設定します。
- 6 **ネットワーク名 (ESSID)** を入力します。ここに 入力する名前は任意の名前を入力することができますが、アドホックネットワーク 内にある全てのコンピュータで同じ名前を設定してください。
- 7 次にお使いのネットワークでの **認証モード** を選択します。どのモードが適切であるかについては、お使いの無線 LAN カードのドライバと、ネットワーク内にある他のデバイスの機能に依存して決まります。
- 8 **認証モード** を **暗号化無し** に設定 した場合は、**次へ** を押すと設定が完了します。最後に 潜在的なセキュリティリスクに関するメッセージを確認し、**概要** タブ (新しく設定した無線 LAN カードが表示されているはずです) から **OK** を押して終了です。

その他の認証モードを選択した場合は、手順22.2「暗号化の詳細設定の入力」(425 ページ) に進みます。
- 9 **smpppd** をインストールしていない 場合は、YaST からインストールするよう促されます。指示に従ってインストールしてください。
- 10 ネットワーク内にある他の無線 LAN カードについても同様に設定します。それぞれ同じ **ネットワーク名 (ESSID)** と **認証モード** を設定しますが、IP アドレスについては 異なるものを設定してください。

22.5.4 その他のパラメータの設定

お使いの無線 LAN カードを設定するにあたっては、通常これらの追加設定を調整する必要はありません。ただしお使いの無線 LAN に接続するのに詳細な設定が必要となる場合、YaST では下記の設定を行なうことができます：

チャンネル

無線 LAN のステーションが動作すべきチャンネルを指定します。これは *アドホック* および *マスター* の動作モードでのみ必要な設定です。*管理* モードでは無線 LAN カードが自動的にアクセスポイントのチャンネルを検索します。

ビットレート

お使いのネットワークの性能に依存して、一方から他方に通信を行なうのにビットレートを設定する必要がある場合があります。既定では *自動* の設定になっていて、システムは利用可能な最大限のビットレートを使用しようとしています。なお、無線 LAN カードによってはビットレートの設定に対応していない場合もあります。

アクセスポイント

複数のアクセスポイントが存在する環境の場合、MAC アドレスを指定してどのアクセスポイントを使用するかを設定することができます。

電源管理

旅行中などの場合、電源管理機能を利用することで、ご利用のバッテリーの動作時間を伸ばすことができます。電源管理機能を利用すると、接続品質に影響があるばかりか、ネットワークの遅延も大きくなることにご注意ください。Using

高度なオプションにアクセスするには、下記のようにして行ないます：

- 1 YaST を起動し、*ネットワーク設定* ダイアログを開きます。
- 2 *概要* タブに移動し、一覧から無線 LAN カードを選択します。選択したら *編集* ボタンを押し、*ネットワークカードの設定* ダイアログを開きます。
- 3 *次へ* を押し、*無線ネットワークカードの設定* ダイアログを表示します。
- 4 *熟練者向け設定* ボタンを押します。
- 5 *アドホック* モードの場合は、お使いのステーションと他のステーションで通信を行なうチャンネル (お使いの国に依存しますが、一般に 11 から 14 まで) を選択します。*マスター* モードの場合は、アクセスポイントの機能を提供するチャンネルを設定します。このオプションの既定値は *自動* になっています。

- 6 また、使用したい **ビットレート** を設定します。
- 7 続いて接続先の **アクセスポイント** の **MAC アドレス** を 入力します。
- 8 さらに **電源管理** を使用するかどうかを選択します。
- 9 設定内容を確認して **OK** を押し、**次へ** を押したあと **OK** を押すと、設定を完了することができます。

22.6 無線 LAN 設定における豆知識

下記に示すツールや知識を利用することで、通信速度や安定性のほか、無線 LAN のセキュリティ要素についても監視したり改善したりすることができます。

22.6.1 ユーティリティ

wireless-tools パッケージには、無線 LAN 固有のパラメータを設定したり、統計情報を表示したりするための 各種ツールが含まれています。詳しくは http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html (英語) をお読みください。

kismet (kismet パッケージ) は無線 LAN の通信トラフィックを聞き取ることできるネットワーク解析ツールです。このツールを利用することで、ネットワークに対する侵入が行なわれた形跡がないかどうかを検出することもできます。詳しくは <http://www.kismetwireless.net/> (英語) とマニュアルページをお読みください。

22.6.2 安定性と速度

無線ネットワークにおける性能と信頼性は、主に参加している端末から他の端末にきれいな信号を送ることができるかどうかに依存します。壁などの障害物が存在している場合は信号を大きく減衰させることになります。信号が減衰するとその分だけ転送速度が落ちることになります。接続中に iwconfig ユーティリティをコマンドラインから実行 (Link Quality の項目) したり、KDE が提供する NetworkManager のアプレットを利用したりして、信号の強さを確認してみてください。信号の品質に何か問題がある場合は、機器やアクセスポイントのアンテナの場所を変えるなどを行なってみてください。また PCMCIA 無線 LAN カードによっては補助 アンテナに対応している場合もあります。このときは補助アンテナを使用

するとそれなりに品質を改善することができる場合があります。また、54 Mbit/s などの製造元が表示している値は、理論上の最大値を示した建前上の値です。実際の最大データスループットは、大きくてもこの値の半分程度です。

また、iwspy というツールを使用すると、無線 LAN の統計情報を表示することができます。

```
iwspy wlan0
wlan0      Statistics collected:
    00:AA:BB:CC:DD:EE : Quality:0  Signal level:0  Noise level:0
    Link/Cell/AP      : Quality:60/94  Signal level:-50 dBm  Noise level:-140 dBm
    (updated)
    Typical/Reference : Quality:26/94  Signal level:-60 dBm  Noise level:-90 dBm
```

22.6.3 セキュリティ

無線ネットワークの設定を行なう場合、セキュリティの仕組みを導入しないと電波の届く範囲にいるユーザであれば誰にでもパケットを傍受できてしまうことにご注意ください。そのため、必ず暗号化を実施してください。全ての無線 LAN カードとアクセスポイントでは WEP 暗号化に対応していますが、これは全く持って安全なものではありません。単に攻撃者に対するちょっとした障害物程度にしかありません。

個人使用の範囲では、できる限り WPA-PSK をお使いください。Linux ではほとんどのハードウェアで WPA に対応していますが、ドライバによっては WPA サポートが提供されていないものもあります。また、古いアクセスポイントや無線対応のルータで WPA に対応していないものもあります。このようなデバイスの場合は、ファームウェアの更新で WPA に対応できないかどうかをご確認ください。WPA が利用できない場合でも、何も暗号化を行なわないよりは WEP を利用するのがよいでしょう。また、高度なセキュリティ要件のある企業用途では、無線ネットワークは WPA のみに対応させるべきです。

お使いの暗号化方法でパスフレーズを設定する際には、より強度の高いパスフレーズを設定してください。たとえば <https://www.grc.com/passwords.htm> では、64 文字分のランダムなパスワードを生成することができます。

22.7 トラブルシューティング

お使いの無線 LAN カードが自動では検出されない場合、まずは openSUSE で対応済みのものかどうかをご確認ください。対応済みの無線 LAN ネットワークカードの一覧は、[http://ja.opensuse.org/HCL/Network_Adapters_\(Wireless\)](http://ja.opensuse.org/HCL/Network_Adapters_(Wireless)) (日本語) または [http://en.opensuse.org/HCL:Network_\(Wireless\)](http://en.opensuse.org/HCL:Network_(Wireless)) (英語) からご

確認ください。お使いのカードが一覧にない場合は、ndiswrapper と呼ばれるソフトウェアを利用して Microsoft Windows のドライバを使用することがあります。詳しくは <http://ja.opensuse.org/SDB:Ndiswrapper> (日本語) または <http://en.opensuse.org/SDB:Ndiswrapper> (英語) をお読みください。

また、お使いの無線 LAN カードが動作しない場合は、下記の要件が満たされているかどうかをご確認ください。

1. お使いの無線 LAN カードに対応するデバイス名は判明していますか？ 通常は wlan0 のような名前になっているはずです。ifconfig ツールを利用してご確認ください。
2. 必要なファームウェアをインストールしてありますか？ 詳しくは /usr/share/doc/packages/wireless-tools/README.firmware をお読みください。
3. お使いのルータから ESSID がブロードキャストされ、閲覧可能な状態 (隠蔽されていない) になっていますか？

22.7.1 状態の確認

iwconfig コマンドを利用することで、ご利用中の無線接続に関する情報を取得することができます。たとえば下記の出力例では、ESSID と 無線モード、周波数、暗号化の可否、リンク品質などが表示されています：

```
iwconfig wlan0
wlan0 IEEE 802.11abg ESSID:"guest"
      Mode:Managed  Frequency:5.22GHz  Access Point: 00:11:22:33:44:55
      Bit Rate:54 Mb/s   Tx-Power=13 dBm
      Retry min limit:7   RTS thr:off   Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality:62/92   Signal level:-48 dBm  Noise level:-127 dBm
      Rx invalid nwid:0   Rx invalid crypt:0   Rx invalid frag:0
      Tx excessive retries:10   Invalid misc:0   Missed beacon:0
```

また、上記の情報を iwlist コマンドから取得することもできます。下記の出力例では、現在のビットレートが表示されています：

```
iwlist wlan0 rate
wlan0    unknown bit-rate information.
         Current Bit Rate=54 Mb/s
```

利用可能なアクセスポイントがどれだけあるのかを知りたい場合は、iwlist コマンドを利用することで調べることができます。下記のような形式で「セル」の一覧が表示されます：

```
iwlist wlan0 scanning
wlan0 Scan completed:
  Cell 01 - Address: 00:11:22:33:44:55
    Channel:40
    Frequency:5.2 GHz (Channel 40)
    Quality=67/70 Signal level=-43 dBm
    Encryption key: off
    ESSID:"Guest"
    Bit Rates: 6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s;
                24 Mb/s; 36 Mb/s; 48 Mb/s
    Mode: Master
    Extra:tsf=0000111122223333
    Extra: Last beacon: 179ms ago
    IE: Unknown: ...
```

22.7.2 複数のネットワークデバイス

最近のラップトップコンピュータには、一般に有線と無線の両方の LAN カードを内蔵しているものがあります。両方のデバイスを DHCP (アドレスの自動割り当て) で設定している場合は、名前の解決やデフォルトゲートウェイの設定で問題が発生する場合があります。これはルータに対して ping が通るのに、インターネットには接続できないという現象で顕在化します。この場合はサポートデータベースにある下記の記事 http://ja.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients (日本語) または http://old-en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients (英語) をお読みください。

22.7.3 Prism2 カードでの問題

Prism2 チップに対しては、利用可能なドライバが複数存在しています。お使いのカードによって、どのドライバが動作するのが異なっている状態です。これらのカードをお使いの場合は、hostap ドライバを利用した WPA 接続が唯一の解決になります。このようなカードが部分的に、もしくは全く動作しないような場合や、WPA をお使いになりたい場合は、`/usr/share/doc/packages/wireless-tools/README.prism2` をお読みください。

22.8 さらなる情報

さらなる情報については、それぞれ下記のページをお読みください：

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html
Wireless Tools と呼ばれる Linux 向け無線 LAN ツール の開発者、Jean Tourrilhes 氏のインターネットページです。無線ネットワーク に関する有用な情報が多数掲載されています。

tuxmobil.org
Linux を利用したモバイルコンピューティングについて、便利な情報が 掲載されています。

<http://www.linux-on-laptops.com>
ラップトップコンピュータで Linux を使用する場合の情報源です。

[http://en.opensuse.org/HCL:Network_\(Wireless\)](http://en.opensuse.org/HCL:Network_(Wireless))
対応している無線 LAN カードの一覧です。

<http://en.opensuse.org/SDB:Ndiswrapper>
Ndiswrapper を利用して Microsoft Windows 向けの無線 LAN カードのドライバを利用する際の、問題回避方法などが記されています。

NetworkManager の使用

NetworkManager はラップトップやその他の移動型コンピュータを利用する際には便利な ソフトウェアです。最先端の暗号化やネットワーク接続に対応していて、802.1X で保護されたネットワークに接続する機能も備えています。802.1X は「IEEE Standard for Local and Metropolitan Area Networks— Port-Based Network Access Control」(ポートごとにネットワーク アクセスの制御を行なう、ローカル／地域ネットワーク向け IEEE 標準) の意味です。NetworkManager を利用すると、ネットワークインターフェイスの設定や移動時の有線／無線 ネットワークの切り替えなどについて、注意を払う必要がなくなります。NetworkManager は既知の無線ネットワークに自動接続する機能を備えているほか、同時に複数のネットワーク 接続を管理することができます—この場合、既定では最も高速な接続を利用します。さらに、利用可能なネットワークを手動で切り替えたりすることができますし、システムトレイ内や上部のバー内のアイコンを利用して、ネットワーク 接続の管理を行なうこともできます。

1 つだけの接続を有効に設定するだけでなく、複数の接続を同時に有効にすることもできます。これによりイーサネット環境から接続を外しても、そのまま 無線接続でつなぎ続けることができます。

23.1 NetworkManager の利用例

NetworkManager は洗練された直感的なユーザインターフェイスを備えていて、ユーザが 容易にネットワーク環境を切り替えることができるようになっています。しかしながら、下記のような用途では NetworkManager は適切な解決方法とは言えません：

- お使いのコンピュータから、ネットワーク上の他のコンピュータに対して ネットワークサービスを提供しているような場合。たとえば DHCP サーバや DNS サーバなど。
- お使いのコンピュータが Xen サーバで、お使いのシステムが Xen 環境下 の仮想システムである場合。

23.2 NetworkManager の有効化と無効化

ラップトップコンピュータの環境では、NetworkManager は既定で有効に設定されています。YaST ネットワーク設定モジュールから有効にしたり無効にしたり することができます。

- 1 YaST を起動し、ネットワークデバイス > ネットワークの設定 を選択します。
- 2 ネットワーク設定 のダイアログが開きます。そこから、グローバルオプション のタブを開きます。
- 3 NetworkManager でお使いのネットワーク接続を設定したり管理したりしたい場合は、下記の手順を実施します：
 - 3a ネットワークの設定方法 の欄で、*NetworkManager* を使ってユーザが制御 を選択します。
 - 3b OK を押して YaST を閉じます。
 - 3c あとは 23.3項「ネットワーク接続の設定」(437 ページ) の手順に従い、NetworkManager を利用してネットワーク接続を設定します。
- 4 NetworkManager を無効化し、ネットワークの設定を従来の方法に戻すには、下記の手順を実施します：
 - 4a ネットワークの設定方法 の欄で、*ifup* を使用した従来の方法 を選択します。
 - 4b OK を押して閉じます。

4c あとは DHCP を利用した自動設定を行なうか、もしくは固定の IP アドレスを設定します。それ以外にも、YaST でモデムを設定することもできます:

- ダイアルアップ接続の場合は、ネットワークデバイス > モデム を選択します。
- 内蔵または USB 接続の ISDN モデムの場合は、ネットワークデバイス > *ISDN* を選択します。
- 内蔵または USB 接続の DSL モデムの場合は、ネットワークデバイス > *DSL* を選択します。

YaST でのネットワーク設定手順について、詳しくは 11.4 項「YaST を利用したネットワーク接続の設定」(223 ページ) と 第22章 *無線 LAN* (417 ページ) をお読みください。

23.3 ネットワーク接続の設定

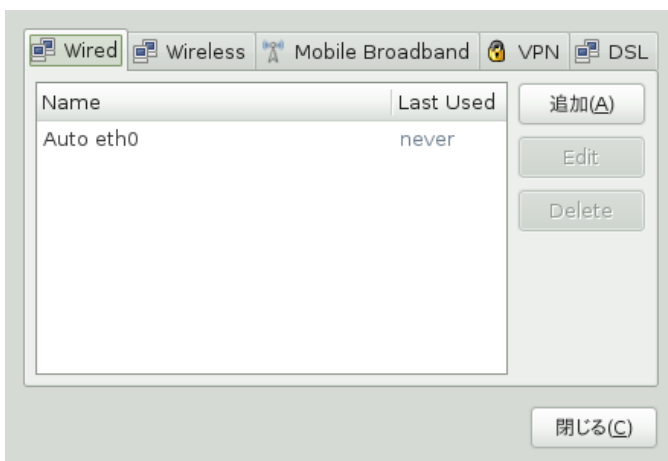
YaST から NetworkManager を有効にしたのち、KDE や GNOME から利用できる NetworkManager のフロントエンドを利用し、ネットワークの設定を行ないます。どちらの環境 向けのフロントエンドであっても、ネットワークの設定ダイアログは似たような表示になっています。有線, 無線, モバイルブロードバンド, DSL, VPN など、全ての種類のネットワーク接続がタブで表示されます。それぞれのタブで接続を追加したり編集したり、削除したりを行なってください。それぞれ入力項目やオプションの上にマウスカーソルを合わせると、詳しい説明が表示されます。また、KDE の設定ダイアログでは、それぞれのタブはお使いのシステムで 利用可能なものである場合にのみ、選択することができます (ハードウェアとソフトウェアの構成に依存します)。

注記: Bluetooth 接続について

現時点では Bluetooth を NetworkManager から設定することはできません。

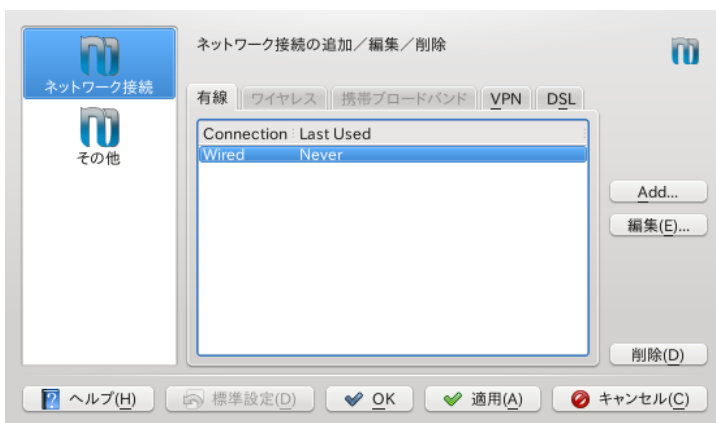
GNOME 環境でネットワーク設定ダイアログを開くには、+ F2 を押してから `nm-connection-editor` と入力します。

図 23.1 GNOME ネットワーク接続ダイアログ



KDE をお使いの場合は、メインメニューを開いて *KDE システム設定* を開きます。その後、*ネットワークと接続* 内から *ネットワーク設定* > *ネットワーク接続* を選択します。

図 23.2 KDE ネットワーク設定ダイアログ



上記の方法以外にも、システムトレイや上部のバー内にある NetworkManager のフロントエンドから、設定ダイアログを開くことができます。KDE の場合は、NetworkManager のアイコンを マウスの左ボタンで選択し、*Manage Connections* を選択してください。GNOME の場合は、アイコンを選択して *Network Settings* > *Options* を選択してください。

注記: 利用できるオプション

お使いのシステム設定によっては、接続の設定変更が許可されない場合があります。機密を保持している環境では、root の権限無しではいくつかの オプション設定がロック (施錠) されている場合があります。詳細はシステム 管理者にお尋ねください。

手順 23.1 接続の追加と編集

NetworkManager でネットワーク接続を設定している場合、全ユーザで共有可能な システム接続 を設定することもできます。システム接続は ユーザ接続 と異なり、NetworkManager が起動 するとユーザのログインがなくても、すぐに利用できるようになるものです。それぞれの接続種類について、詳しくは 23.7.1 項「ユーザとシステムの接続」(449 ページ) をお読みください。

現時点では、システム接続 のオプションは KDE から利用できません。システム接続を設定するには、YaST をご利用ください。

注記: 非公開のネットワーク

「非公開の」ネットワーク (サービスの提供を公開していない サービス) に接続したい場合、それらは自動では検出されないため、その ネットワークの SSID (Service Set Identifier) または ESSID (Extended Service Set Identifier) を知っておく必要があります。

- 1 新しい接続を追加するには *追加* を、既存の接続を編集 するには該当する接続を選択して *編集* を押します。
- 2 ネットワークの設定ダイアログ内で、利用したい接続タイプのタブを選択します。
- 3 まずは *Connection Name* の欄に入力を行ない、接続の詳細をそれぞれ設定します。
- 4 次に、接続種類ごとに複数の物理デバイスが利用できるような環境 (たとえばお使いのマシンに 2 つのイーサネットカードが接続されていたり、2 枚の無線 LAN カードが接続されていたりした場合) では、接続を特定のデバイスに結びつけます。

KDE をお使いの場合は、*Restrict to Interface* オプションをご利用ください。GNOME の場合は、接続対象の MAC アドレス を *MAC address* に設定してください。

- 5 また、特定の接続を自動で使用するよう NetworkManager に設定するには、その接続に対して *Connect Automatically* (または "自動的に接続する") を設定します。
- 6 ある接続を システム接続 として設定したい場合、KDE であれば *System Connection* を、GNOME であれば *Available to all users* を設定してください。システム接続を作成したり編集したりするには、root のアクセス 許可が必要です。

それぞれ追加や編集を行なうと、新しく設定したネットワーク接続が利用可能なネットワークの一覧に現われるようになります。NetworkManager のアイコンをマウスの 左ボタンで選択して表示させてください。

図 23.3 KDE NetworkManager—設定済みまたは利用可能な接続

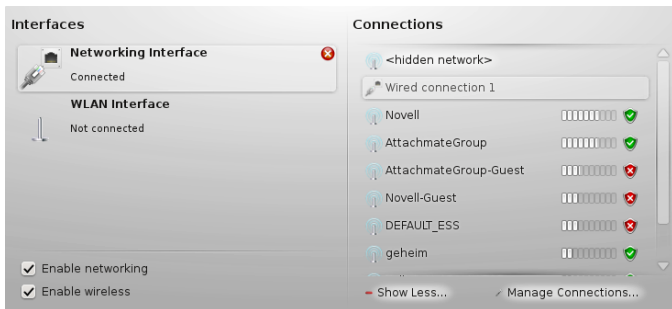
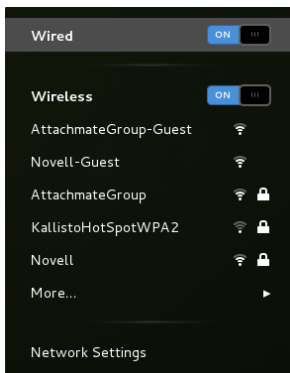


図 23.4 GNOME NetworkManager—設定済みまたは利用可能な接続



23.4 KDE NetworkManager フロントエンドの使用

NetworkManager に対する KDE のフロントエンドは NetworkManager plasmoid と呼ばれるものです。ネットワークを NetworkManager で設定している場合は、デスクトップ環境の起動時に plasmoid が自動的に起動し、システムトレイ内にアイコン表示が行なわれます。

システムトレイ内にネットワーク接続を表わすアイコンが現われない場合、plasmoid はおそらく起動していないものと思われます。パネルツールボックス から **ウィジェットを追加** を選択し、**ネットワーク管理** をダブルクリックしてから **パネルツールボックス** を再度押してください。

KNetworkManager は設定済みの無線ネットワークしか表示しません。また、対象の無線 ネットワークが見つからなかったり、ネットワークケーブルが外されていたりした場合には、それらに該当する接続についても表示されなくなります。そのため、常に利用可能な接続だけを表示している形になっています。

23.4.1 有線ネットワーク接続の管理

お使いのコンピュータがネットワークケーブルで既存ネットワークに 接続されている場合は、NetworkManager フロントエンドを利用してネットワーク接続を 管理します。

- 1 NetworkManager のアイコンをマウスの左ボタンで押し、利用可能な **インターフェイス** (左側) と **接続** (右側) を表示します。現在使用中の接続は太字で表示されます。
- 2 インターフェイスに対する詳細情報と統計情報を表示するには、plasmoid の左側に一覧表示されている **ネットワークインターフェイス** をマウスの左ボタンで選択します。青い矢印アイコンを押すと、元のインターフェイス概要に 戻ります。
- 3 接続を切断したい場合は、右半分の **ネットワークインターフェイス** 内にある該当のアイコン (赤く表示されているはず) を、マウスの左ボタンで押します。
- 4 異なる有線ネットワーク設定を使用したい場合は、*Manage Connections* を押し、新しい有線接続を作成します。詳しくは 手順23.1「**接続の追加と編集**」(439 ページ) をお読みください。

- 5 あとは再度 KNetworkManager のアイコンをマウスの左ボタンで押し、新しく作成した 設定を選択します。
- 6 有線／無線の両方について、すべてのネットワーク接続を切るには、NetworkManager のアイコンをマウスの左ボタンで押し、ネットワークの有効化のチェックを外してください。

23.4.2 無線ネットワーク接続の管理

既定では NetworkManager フロントエンドは設定済みの接続のみを表示します。それぞれの ネットワークの信号の強さは棒グラフで表示され、それぞれ1ブロックが 10%を示す値になっています。暗号化された無線ネットワークの場合は、それぞれ 緑色 (WPA) や黄色 (WEP) の盾印で 表示され、暗号化されていないネットワークは赤い盾印で表示されます。

手順 23.2 無線ネットワークへの接続

- 1 利用可能なすべてのネットワークを表示するため、*Show More* を押します。
- 2 一覧に表示された中からいずれかを選択すると、ネットワーク接続ダイアログを開くことができます。サービスセット識別子 (SSID または ESSID) を通知していない ネットワークに接続したい場合は、*hidden network* を 選択します。あとは接続情報を入力して を 押します。
- 3 NetworkManager のセキュリティ設定によっては (23.7.2項「パスワードと認証情報の保存」(449 ページ) をお読みください)、KWallet のパスワード入力を求められる場合があります。
- 4 あとは NetworkManager が自動的に設定したネットワークに接続を行ないます。

手順 23.3 有効な無線接続の管理

- 1 plasmoid の右半分に一覧表示されている 無線ネットワークインターフェイス をマウスの左ボタンで 選択すると、選択したインターフェイスに対する詳細と統計情報が 表示されます。

図 23.5 KDE NetworkManager— 接続の詳細と統計情報

青い矢印アイコンを押すと、元のインターフェイス概要に 戻ります。

- 2 接続を切断したい場合は、右半分の *無線ネットワークインターフェイス* 内にある赤いアイコンを、マウスの左ボタンで押します。
- 3 無線ネットワーク接続を切るには、*無線の有効化* のチェックを外してください。この機能は、航空機に搭乗している場合やその他の要件で、無線ネットワークの使用が禁止されている場合に便利です。

明示的に選択した無線ネットワークへの接続は、できる限り継続できるよう処理を行いません。無線接続が動作中で、その間にネットワークケーブルが接続された場合も、*Connect Automatically* で設定された接続があれば、それらは自動で接続されます。

23.4.3 お使いの無線カードをアクセスポイントとして設定する

お使いの無線カードがアクセスポイントモードに対応している場合は、NetworkManager を利用してアクセスポイントの設定を行なうことができます。

注記: 利用可能なオプション

お使いのシステム設定に依存しますが、接続の設定を許可していない場合もあります。機密を保持する環境などでは、root からのアクセス許可がない限り、いくつかのオプションがロック (施錠) されることがあります。詳細はシステム管理者にお尋ねください。

- 1 23.3項「ネットワーク接続の設定」(437 ページ) の手順でネットワーク接続の設定 ダイアログを開きます。
- 2 *追加 > 共有* を選択します。
- 3 *無線* タブでは、*接続名* と *SSID* の項目を設定します。
- 4 *Wireless Security* (ワイヤレスセキュリティ) タブで、暗号化の設定を行ないます。

重要: 保護されていないネットワークのセキュリティリスク

Security (セキュリティ) に *None* (なし) を選択すると、誰でもネットワークに接続だけでなく、接続を横取りしたり遮断したりすることもできてしま

います。アクセス ポイントへのアクセスを制限して機密を守るには、暗号化を設定してください。WEP や WPA ベースの様々な暗号化を使用することができます。どの技術が適切であるのかわからない場合は、22.3項「認証」(419 ページ) をお読みください。

5 最後に設定を確認し、OK で閉じます。

23.5 GNOME NetworkManager の使用

GNOME では、NetworkManager を GNOME NetworkManager アイコンから操作することができます。ネットワークを NetworkManager で操作するように設定してある場合は、デスクトップ 環境にログインすると、自動的に上部のバー内に表示されるようになります。

上部にネットワーク接続を表わすアイコンが現われない場合、おそらくは GNOME NetworkManager が起動していないものと思われます。+ F2 を押し、nm-applet と入力して起動してください。

23.5.1 有線ネットワークの管理

お使いのコンピュータがネットワークケーブルで既存ネットワークに 接続されている場合は、NetworkManager アイコンを利用してネットワーク接続を 選択してください。

- 1 アイコンをマウスのボタンで選択し、利用可能なネットワークを 表示させます。現在使用中の接続はメニュー内では一番上に表示され、有効な 接続が以下に続きます。
- 2 すべての有効なインターフェイスに対して、詳細な情報を表示したい場合は、*Network Settings* を選択します。
- 3 接続を切るには、*Wired* の隣にある *OFF* ボタンを押します。
- 4 有線の接続に対して異なる設定を使用したい場合は、ネットワーク接続 ダイアログを開いてから、手順23.1「接続の追加と編集」(439 ページ) の手順で他の

優先接続を追加します。あとは NetworkManager のアイコンをマウスの左ボタンで押して、新しく作成した接続を選択すると、それを有効にすることができます。

- 5 有線／無線とも全てのネットワーク接続を無効にするには、アイコンをマウスの右ボタンで選択し、ネットワークを有効にする のチェックを外してください。

23.5.2 無線ネットワークの管理

GNOME NetworkManager 内には、利用可能で参照可能な (ブロードキャストされている) 無線ネットワークが表示されます。一覧を広げるには、*More Networks* を選択してください。それぞれのネットワークについて、信号強度も表示されます。暗号化された無線ネットワークの場合は、鍵のアイコンが表示されます。

手順 23.4 無線ネットワークへの接続

- 1 無線ネットワークに接続するには、アイコンをマウスのボタンで選択し、利用可能な無線ネットワークの一覧から選択します。
- 2 ネットワークが暗号化されている場合はダイアログが表示され、使用する暗号化方法が表示 (ワイヤレスセキュリティ) されるほか、暗号化方法に応じていくつかの入力項目が表示されます。それぞれ適切な認証情報を入力してください。
- 3 ブロードキャストでサービスセット ID (SSID または ESSID) を通知していないネットワークに接続する場合は、それらは自動では検出されないため、NetworkManager アイコンを選択してから *Network Settings > Wireless > Other* を選択します。
- 4 ダイアログが開いたら接続に関する設定を入力し、*Connect* を押します。
- 5 無線ネットワークを無効に設定するには、アイコンをマウスのボタンで選択し、*Wireless* の隣にある *OFF* ボタンを押してください。この作業は、たとえば航空機に乗っている場合など、無線ネットワークが許可されない環境をご利用の場合に便利です。

明示的に選択した無線ネットワークへの接続は、できる限り継続できるよう処理を行ないます。無線接続が動作中で、その間にネットワークケーブルが接続された場合も、*Connect Automatically* で設定された接続があれば、それらは自動で接続されます。

23.5.3 お使いの無線カードをアクセスポイントとして設定する

お使いの無線カードがアクセスポイントモードに対応している場合は、NetworkManager を利用してアクセスポイントの設定を行なうことができます。

注記: 利用可能なオプション

お使いのシステム設定に依存しますが、接続の設定を許可していない場合もあります。機密を保持する環境などでは、root からのアクセス許可 がない限り、いくつかのオプションがロック (施錠) されることがあります。詳細はシステム管理者にお尋ねください。

- 1 NetworkManager のアイコンをマウスのボタンで選択し、*Network Settings* *Wireless* を選択します。
- 2 *Use as Hotspot* を選択し、表示されるポップアップ メッセージを確認します。その後 root のパスワードを入力して 作業を続けます。

Network Name (SSID) と *Security Key* は自動的に生成され、*Network* ダイアログ内に表示されます。SSID は、お使いのコンピュータのホスト名をベースにした名前になります。接続する側のデバイスは、この情報を利用してアクセスポイントに接続します。

重要: 保護されていないネットワークのセキュリティリスク

アクセスポイントへのアクセスを制限して機密を守るには、暗号化を設定してください。ネットワークカード側の機能にもよりますが、WEP や WPA ベースの様々な暗号化を使用することができます。どの技術が適切であるのかわからない 場合は、22.3項「認証」(419 ページ) をお読みください。

- 3 SSID や暗号化オプション (WEP, WPA など)、およびセキュリティ鍵を変更するには、下記のようにして行ないます:
 - 3a *Stop Hotspot* ボタンの隣にある *Options* を押します。
 - 3b root のパスワードを入力して進みます。
 - 3c *Wireless* タブ内で SSID を変更することができるほか、*Wireless Security* タブでは、暗号化に関する詳細設定を 変更することができます。

注記: WEP 40/128 ビット鍵について (16 進または ASCII)

暗号化方法に WEP 40/128-bit Key (WEP 40/128 ビット鍵) を選択した場合、Key (鍵) の長さは 5, 10, 13 文字のいずれかに限定されます。長さを正しく入力しないと、Save (保存) ボタンを押すことができません。

3d 設定を保存してしばらくすると、*Network* ダイアログ内に 変更が反映されるようになります。

4 アクセスポイントの機能を停止してユーザからの接続を切るには、*Stop Hotspot* を押してください。ポップアップメッセージで 表示される確認に 応答すると、機能が停止します。

23.6 NetworkManager と VPN

NetworkManager では複数の仮想プライベートネットワーク (VPN) 技術を扱うことができます。openSUSE では、各技術を汎用的にサポートするための VPN 基本パッケージを提供しています。さらに、お使いのフロントエンドに対して、関連するデスクトップ固有のパッケージを追加インストールする必要があります。

NovellVPN

この技術を使用する場合は、それぞれ下記をインストールする必要があります。

- NetworkManager-novellvpn
- NetworkManager-novellvpn-kde4 または NetworkManager-novellvpn-gnome

KDE 向けの NovellVPN サポートは現在作成中で、公開されていません。

OpenVPN

この技術を使用する場合は、それぞれ下記をインストールする必要があります。

- NetworkManager-openvpn
- NetworkManager-openvpn-kde4 または NetworkManager-openvpn-gnome

vpnc (Cisco)

この技術を使用する場合は、それぞれ下記をインストールする必要があります。

- NetworkManager-vpnc
- NetworkManager-vpnc-kde4 または NetworkManager-vpnc-gnome

PPTP (Point-to-Point Tunneling Protocol)

この技術を使用する場合は、それぞれ下記をインストールする必要があります。

- NetworkManager-pptp
- NetworkManager-pptp-kde4 または NetworkManager-pptp-gnome

それぞれパッケージをインストールしたら、23.3項「ネットワーク接続の設定」(437 ページ) に書かれている手順で VPN を設定します。

23.7 NetworkManager とセキュリティ

NetworkManager では、信頼済みのものとそうでないものの 2 種類の無線接続を、区別して 使用します。信頼済みの接続とは過去に明示的に選択したネットワークのことを 指します。それ以外の全ては信頼できないものとして扱われます。信頼済みの 接続は、名前とアクセスポイントの MAC アドレスで認識します。MAC アドレス を利用することで、信頼済みのものと同じ名前を持つ異なるアクセスポイントについて、これらを使用しないようにしています。

NetworkManager は定期的な利用可能な無線ネットワークを監視しています。複数の信頼済み ネットワークが見つかった場合は、最も新しく使用したものを自動で 選択します。信頼済みのネットワークが見つからない場合、NetworkManager は ユーザ側での選択を待機 します。

また、名前と MAC アドレスが同じでありながら暗号化設定だけが変わった場合、NetworkManager は接続を行なおうとしますが、新しい暗号化設定とそれに関連する新しい 設定 (たとえば新しい暗号鍵など) を尋ねられます。

さらに、無線接続をオフラインモードに切り替えた場合は、NetworkManager は SSID / ESSID を 空白に設定します。これによりカードの接続を解除することができます。

23.7.1 ユーザとシステムの接続

NetworkManager では、接続を 2 つの種類に分類します。1 つは ユーザ 接続、もう 1 つは システム 接続です。ユーザ接続は ユーザがログインしたときに NetworkManager から利用できるようになる接続です。必要な全ての認証情報はユーザ側で設定し、ユーザがログアウトしたときには 接続は解除され、削除されます。一方、システム接続は全てのユーザ間で共有 される接続で、NetworkManager が起動したあとであれば、ユーザがログインしなくても 利用できるようになります。システム接続の場合、全ての認証情報は接続を 作成する際に指定しておかなければなりません。また、このようなシステム 接続は、認証の必要なネットワークに対して自動接続を行なう用途にも使用 することができます。ユーザ接続、およびシステム接続についてそれぞれ NetworkManager を設定する方法は、23.3項「ネットワーク接続の設定」(437 ページ) をお読みください。

23.7.2 パスワードと認証情報の保存

暗号化されたネットワークに対して、接続のたびに認証情報を入力したくない 場合は、GNOME キーリングマネージャや KWalletManager のような デスクトップ固有のツールをお使いいただき、マスターパスワードで暗号化 した形で、ディスク内に認証情報を保存してください。

なお KDE では認証情報を保存するかどうかと、どのように保存 するかについて、それぞれ設定を行なうことができます。NetworkManager のアイコンを マウスの左ボタンで選択し、*Manage Connections* を 選択してください。さらに *Other > Connection Secrets* を選択し、下記の オプションのうちのいずれかを選択してください:

Do Not Store (Always Prompt)

この設定では、認証情報の保存を行ないません。認証情報を保存してしまうことがセキュリティリスクであるとする 作業環境で、便利な設定です。

In File (Unencrypted)

このオプションを選択した場合、パスワードはそれぞれの接続に対して 作成される接続ファイル内に、暗号化されずに保存されます。

警告: セキュリティリスク

この設定では、認証情報を暗号化せずに保存します。ネットワークの認証情報を暗号化せずに保存してしまうのは、セキュリティ 上のリスクとなります。お

使いのコンピュータにアクセスできる全ての ユーザから認証情報を利用できてしまうため、ネットワーク接続を 横取りされたり、妨害されたりする場合があります。

In Secure Storage (Encrypted)

このオプションを選択すると、認証情報は KWalletManager 内に保存 されます。

23.8 よくある質問

下記には NetworkManager を利用して特別なネットワークオプションを設定するにあたり、よくある質問を掲載しています。

接続を特定のデバイスに結びつけるには？

既定では NetworkManager における接続はデバイスの種類に依存して動作します: つまり、同じ種類の物理デバイス全てに適用される形になります。同じ接続 種類で複数のデバイスが利用できるような環境の場合 (たとえばお使いのマシンに 2 つのイーサネットカードが装備されている場合)、ある接続を 特定のデバイスに結びつけることができます。

GNOME でこれを行なうには、まず対象となるデバイスの MAC アドレスを コマンドラインツール `ifconfig` を利用して調べます。MAC アドレスが判明したら、ネットワーク接続の設定ダイアログを開き、設定を行ないたいネットワーク接続を選択します。それぞれ *Wired* または *Wireless* の タブから、*MAC Address* の欄に MAC アドレスを 入力し、設定を確認すれば完了です。

KDE をお使いの場合は、ネットワーク接続の設定ダイアログを開き、設定を行ないたいネットワーク接続を選択します。それぞれ *Ethernet* または *ワイヤレス* の タブから、*Restrict to Interface* の項目で ネットワークインターフェイスを選択してください。

同じ ESSID を持つ複数のアクセスポイントが検出されるような環境で、特定のアクセスポイントを指定するには？

異なる無線周波数帯 (a/b/g/n) で複数のアクセスポイントが利用できる場合、既定では最も強い信号を出しているアクセスポイントが選択されます。この既定値を上書きするには、無線接続の設定時に *BSSID* の項目に入力を行なってください。

Basic Service Set Identifier (BSSID) は、基本サービスセット ごとに識別機能を提供するためのものです。インフラストラクチャモードの 場合、BSSID は無

線アクセスポイントの MAC アドレスになります。独立 (アドホック) モードの場合、BSSID は乱数から生成される 46 ビットの ローカル管理 MAC アドレスになります。

GNOME の場合は 23.3 項「ネットワーク接続の設定」(437 ページ) に書かれている手順で ネットワーク設定のダイアログを起動します。その後、設定を変更したい 無線接続を選択し、*Edit (または "編集")* を押します。あとは *Wireless (またはワイヤレス)* のタブで BSSID を入力してください。

他のコンピュータとネットワーク共有を行なうには？

プライマリデバイス (インターネットに接続しているデバイス) の場合、特別な設定を行なう必要はありません。しかしながら、ローカルハブやマシン に接続されているデバイスで共有を行なう場合は、下記のように設定する 必要があります：

1. 23.3 項「ネットワーク接続の設定」(437 ページ) の手順に従ってネットワーク接続の 設定ダイアログを起動します。あとは修正したい接続を選んで *編集 (Edit)* を押します。GNOME をお使いの場合は *IPv4 Settings* タブに切り替えたあと *Method* のドロップダウンリストを選択し、*Shared to other computers* を選択します。KDE をお使いの場合は *IPv4 アドレス* タブに切り替えた あと *Configure* のドロップダウンリストを選択 し、*共有されています* を選択します。これにより、IP トラフィックの転送が有効化され、DHCP サーバが動作するようになります。最後に NetworkManager の設定画面を閉じてください。
2. DHCP サーバではポート 67 を使用します。そのため、ファイアウォール でこのポートを塞いでいないことをご確認ください：ネットワーク共有 を提供するマシン側で YaST を起動し、*セキュリティとユーザ > ファイアウォール* を選択します。*許可するサービス* に切り替えたあと、一覧に *DHCPv4 サーバ* が存在していない場合は、*許可するサービス* ボタンを押して *DHCPv4 サーバ* を選び、*追加* を押してください。最後に YaST の設定画面を閉じてください。

自動アドレス設定 (DHCP, PPP, VPN) の環境で、固定の DNS 設定を行なうには？

DHCP サーバが誤った DNS 情報 (または経路情報) を配布しているような場合は、それらを上書きすることができます。まずは 23.3 項「ネットワーク接続の設定」(437 ページ) の手順に従ってネットワーク接続の 設定ダイアログを起動します。あとは修正したい接続を選んで *編集 (Edit)* を押します。GNOME をお使いの場合は *IPv4 Settings* タブに切り替えたあと *Method* のドロップダウンリストを選択し、*Automatic (DHCP) addresses only* を選択します。KDE をお使いの場合は *IPv4 アドレス* に切り替えた あと *Method* のドロップダウンリストを選択 し、*Automatic (DHCP) addresses only* を選択します。あとは

DNS Servers と *Search Domains* の欄にそれぞれ DNS 情報を入力するほか、自動で取得したルートを無視する場合は、タブの上にあるドロップダウンリストから *Routes* を選択し、自動で設定される経路情報を上書きするための設定を入力します。最後に設定画面を閉じてください。

ユーザがログインする前に、パスワード保護されたネットワークに接続するよう NetworkManager を設定するには？

そのような用途で接続を作成したい場合は、システム接続を設定します。詳しくは 23.7 項「NetworkManager とセキュリティ」(448 ページ)をお読みください。

23.9 トラブルシューティング

接続に関する問題が発生する場合があります。NetworkManager まわりでよくある問題としては、フロントエンドが起動しなかったり VPN オプションが失われたりする問題があります。それぞれそれらの問題を解決したり解消したりするには、ご利用のツールによって手順が異なります。

NetworkManager フロントエンドが起動しない

GNOME 環境でも KDE 環境でも、ネットワークが NetworkManager の支配下にある場合には NetworkManager フロントエンドが自動で起動します。フロントエンドが起動しない場合は、まず YaST で NetworkManager が有効に設定されているかどうかをご確認ください。手順は 23.2 項「NetworkManager の有効化と無効化」(436 ページ)をお読みください。また、お使いのデスクトップ環境向けのパッケージについても、インストールされているかどうかご確認ください。KDE4 をお使いの場合は `plasmoid-networkmanagement` パッケージが、GNOME 環境の場合は `NetworkManager-gnome` が、それぞれインストールされていることをご確認ください。

デスクトップに対応したフロントエンドがインストールされているにも関わらず、何らかの理由で起動しないような場合は、GNOME の場合は + F2 を押してから `nm-applet` と入力し、KDE の場合はそれぞれマウスで、パネルツールボックスを選択してから **ウィジェットを追加** を選択します。あとは **ネットワーク管理** を選択してから **パネルツールボックス** をもう一度選択します。

NetworkManager フロントエンドが VPN オプションを表示しない

NetworkManager, フロントエンド, NetworkManager の VPN 対応はそれぞれ別々のパッケージで提供されています。NetworkManager のフロントエンドで必要な VPN オプションを表示しない場合は、お使いの VPN 技術に対応し

た NetworkManager 向けのサポートがインストール されていることをご確認ください。詳しくは 23.6 項「NetworkManager と VPN」(447 ページ) をお読みください。

利用できるネットワーク接続が現われない

お使いのネットワーク接続を正しく設定し、その他のネットワーク接続用の コンポーネント (ルータなど) を正しく設置し動作させている場合は、お使いのコンピュータでネットワークインターフェイスを再起動すると 解決する場合があります。これを行なうには、root でログインして `rcnetwork restart` を実行してください。

23.10 さらになる情報

NetworkManager に関して、さらに詳しい情報は、それぞれ下記の Web サイトやディレクトリ内に あります:

NetworkManager プロジェクトのページ

<http://projects.gnome.org/NetworkManager/>

KDE 版 NetworkManager フロントエンド

<http://userbase.kde.org/NetworkManagement>

パッケージ文書

NetworkManager や GNOME 版および KDE 版の NetworkManager フロントエンドについて、それぞれ最新の情報は下記のディレクトリ内に配置されています:

- `/usr/share/doc/packages/NetworkManager/`,
- `/usr/share/doc/packages/NetworkManager-gnome/`.

タブレット PC の使用

openSUSE® はタブレット PC にも対応しています。下記の章では、お使いのタブレット PC でインストールや設定を行なう方法と、デジタルペンからの入力を受け付ける便利な Linux アプリケーションについて、それぞれ紹介しています。

それぞれ下記のタブレット PC に対応しています:

- シリアルポートまたは USB の Wacom タブレット (ペンを利用するタイプ) や、タッチスクリーン、マルチタッチデバイスの接続 されているタブレット PC
- FinePoint デバイスがあるタブレット PC 。たとえば Gateway C210X/M280E/CX2724, HP Compaq TC1000 などがあります。
- タッチスクリーンがあるタブレット PC 。たとえば Asus R2H, Clevo TN120R, Fujitsu Siemens Computers P-シリーズ, LG C1, Samsung Q1/Q1-Ultra などがあります。

タブレット PC のパッケージをインストールし、デジタイザを正しく設定することで、ペン入力 (スタイラスとも呼ばれます) を下記のアクションやアプリケーションで 利用することができるようになります:

- KDM や GDM を利用したログイン
- KDE や GNOME デスクトップのロック (施錠) 解除
- その他のポインティングデバイス (たとえばマウスやタッチパッド) で実行できる 作業全般。たとえば画面内でのカーソルの移動やアプリケーションの起動と終了、ウィンドウのサイズ変更や移動、ウィンドウフォーカスの切り替えやオブジェクトのドラッグ&ドロップ。

- X ウィンドウシステムのアプリケーションにおけるジェスチャー認識の使用
- GIMP を利用した描画
- Jarnal や Xournal などを利用したメモ書きやスケッチ、Dasher を利用した 巨大テキストの編集。

24.1 タブレット PC パッケージのインストール

タブレット PC に必要なパッケージは、TabletPC という 名称のインストールパターンに含まれています。このパターンをインストール中に 選択すると、下記のパッケージがお使いのシステムにインストールされます：

- cellwriter: 手書き文字入力パネル
- jarnal: Java ベースのメモ書き アプリケーション
- xournal: メモ書き兼スケッチ アプリケーション
- xstroke: X ウィンドウシステム向けのジェスチャー認識プログラム
- xvkbd: X ウィンドウシステム向けの仮想キーボード
- x11-input-fujitsu: Fujitsu P-シリーズ タブレット PC 向け X 入力モジュール
- x11-input-evtouch: タッチスクリーン搭載タブレット PC 向け X 入力モジュール
- xorg-x11-driver-input: Wacom デバイスのモジュールを含む、入力デバイス向けの X 入力モジュール

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コマンドラインからこれらをインストールすることができるほか、YaST から TabletPC のパターンを選択することもインストールを行なうことができます。

24.2 タブレットデバイスの設定

インストールの際には、既定でお使いのタブレットやタッチデバイスが設定されます。お使いの Wacom デバイスでの設定に何か問題がある場合は、これらの設定を変更するためにコマンドラインから `xsetwacom` コマンドを利用することができます。

24.3 仮想キーボードの使用

KDE や GNOME デスクトップへのログインを行なったり、画面のロック (施錠) を解除したりする場合、通常はユーザ名とパスワードを入力しますが、ログイン画面の下に表示された仮想キーボード (xvkbd) を利用して入力することもできます。仮想キーボードを設定したり内蔵のヘルプにアクセスしたりしたい場合は、画面左下の *xvkbd* フィールドを選択し、xvkbd のメインメニューを表示してください。

なお、入力が確認できない場合 (または必要なウインドウに入力を送信できない場合) は、xvkbd からフォーカスキーを押してフォーカスを転送し、キーボードイベントを送信したいウインドウを選択してください。

図 24.1 xvkbd 仮想キーボード

F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	BackSpace	xvkbd (v3.2)							
Esc	1	2	3	4	5	6	7	8	9	0	-	^	1	Focus	Num Lock	/	*	Focus		
Tab	q	w	e	r	t	y	u	i	o	p	@	[Delete	7	Home	8	Up	9	PgUp	+
Control	a	s	d	f	g	h	j	k	l	;	:]	Return	4	Left	5	6	Right	-	
Shift	z	x	c	v	b	n	m	,	.	/		Shift	1	End	2	Down	3	PgDn		
xvkbx	Caps	Alt	Meta						かな	←	→	↑	↓	0	Ins		.	Del	Enter	

ログイン後に xvkbd を使用したい場合は、メインメニューから選択を行なうか、もしくはシェルから xvkbd を実行してください。

24.4 ディスプレイの回転表示

お使いのディスプレイをその場で回転させたりサイズ変更したりしたい場合は、KRandRTray (KDE) や gnome-display-properties (GNOME) をお使いください。KRandRTray、gnome-display-properties のどちらも、X サーバの RANDR 拡張を利用するアプレットです。

メインメニューから KRandRTray または gnome-display-properties を起動するか、もしくはシェルから krandrtray または gnome-display-properties を起動します。アプレットを起動すると、アプレットのアイコンがシステムトレイ内に表示されます。gnome-display-properties のアイコンがシステムトレイ内に自動で表示されない場合は、ディスプレイの設定ダイアログ内にあるこの設定アイコンをパネルの中表示するを選択しているかどうかご確認ください。

KRandRTray でお使いのディスプレイを回転させたい場合は、アイコンの上でマウスの 右ボタンを押し、**ディスプレイを設定** を選択します。表示された 設定ダイアログを利用し、必要な向きに設定してください。

gnome-display-properties でお使いのディスプレイを回転させたい場合は、アイコンの 上でマウスの右ボタンを押し、必要な向きを選択してください。お使いのディスプレイは、すぐにその方向になるように調整されます。グラフィックタブレットの向きについても 同じく変更が行なわれるため、電子ペンの動きもそれに合わせて設定されます。

お使いのデスクトップの向きを変更する際に何らかの問題が発生した場合は、24.7項「トラブルシューティング」(462 ページ) をお読みください。

24.5 ジェスチャー認識の使用

openSUSE では、CellWriter と xstroke と呼ばれるジェスチャー認識 アプリケーションが提供されています。いずれのアプリケーションとも、ペンやその他の ポインティングデバイスで実施したジェスチャーを認識し、X ウィンドウシステムに 対して 入力を送信することができます。

24.5.1 CellWriter の使用

CellWriter では、セルと呼ばれる枠の中に文字を書くことができます。記入した文字は すぐに文字として認識され、現在フォーカスのあるアプリケーションに対して、入力を 送信することができます。なお、CellWriter をジェスチャー認識として使用する前に、あらかじめトレーニングを行なって手書き認識を調整する必要があります。それぞれの 文字についてトレーニングを行ない、他の文字との区別を学習させてください。なお、トレーニングを行っていない文字は有効な形で表示されず、使用することが できないことに注意してください。

手順 24.1 *CellWriter のトレーニング*

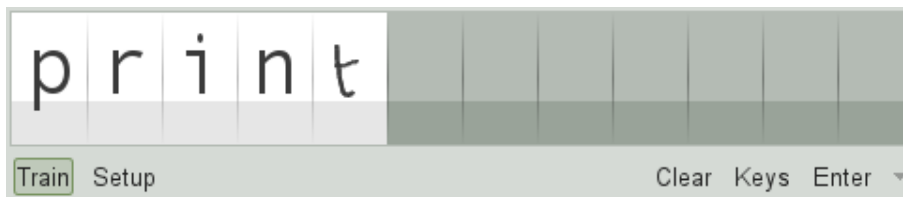
- 1 メインメニューから CellWriter を開始するか、もしくはコマンドラインから `cellwriter` コマンドを実行します。最初の起動では CellWriter は自動でトレーニングモードに移行します。トレーニングモードでは、選択されたキーマップの文字について一覧が表示されます。
- 2 それぞれの文字のセルに対してジェスチャーを入力してください。最初の入力では 背景色が白色に、文字自身が明るい灰色で表示されます。その文字が黒く表

示されるようになるまで、何回もジェスチャーを繰り返してください。トレーニングが行なわれていない文字は明るい灰色で表示されるか、茶色の背景で表示されます (お使いのデスクトップの色スキームに依存します)。

- 3 この手順を繰り返し、必要な全ての文字に対して CellWriter がトレーニング済みになるようにします。
- 4 CellWriter をその他の言語でできるようにトレーニングしたい場合は、*Setup* ボタンを押すと表示されるダイアログから、*Languages* タブを選択し、必要な言語 (日本語訳注: 日本語環境であれば "Hiragana" (ひながな), "Katakana" (カタカナ), "CJK Unified Ideographs" (漢字) になります。ただし漢字は文字数が多いので 注意が必要です) を選択してください。あとは *CellWriter* のウインドウから *Train* ボタンを押してトレーニングモードに 移行し、右下のドロップダウンボックスから必要な文字セットを選択して、トレーニングを行ってください。
- 5 キーマップのトレーニングが完了したら、*Train* ボタンを 再度押して通常モードに戻してください。

通常モードでは、CellWriter ウインドウはジェスチャーを入力するための複数の 空のセルが表示します。記入した文字は *Enter* ボタンを押す までは、他のアプリケーションに送信されることはありません。そのため、入力として 扱う前に、正しくない文字を修正したり削除したりすることができます。なお、認識 時にアプリケーション側で確認のもてない字については、ハイライト表示が行なわれる になっています。入力を修正するには、セルを選んでマウスの右ボタンを押し、表示されるコンテキストメニューを選択してください。文字を削除するにはペンの 消しゴム機能を利用するか、もしくはセルを選択してマウスの中央ボタンを押してください。CellWriter での入力を完了したら、送信先のアプリケーションウインドウ をマウスで選択してから、*Enter* を押してください。

24.2 CellWriter によるジェスチャー認識



なお、CellWriter で *Keys* ボタンを押すと、手書き文字認識 の代わりに仮想的なキーボードを利用して入力することもできます。

CellWriter を隠すには、CellWriter のウィンドウを閉じてください。アプリケーションがシステムトレイ内に隠れます。再度入力ウィンドウを表示させる には、システムトレイ内のアイコンをマウスで選択してください。

24.5.2 Xstroke の使用

xstroke では、ペンやその他のポインティングデバイスを利用したジェスチャー を認識し、X ウィンドウシステムのアプリケーションに対して入力を行なうことが できます。xstroke のアルファベットは一筆書きのアルファベットで、そこから 実際のアルファベットを構築するようになっています。xstroke を有効にすると、入力は現在フォーカスの設定されているウィンドウに対して送信します。

- 1 メインメニューから xstroke を開始するか、もしくはシェルから xstroke を実行します。これらにより、システムトレイに 鉛筆型のアイコンが表示されるようになります。
- 2 ペンを利用してテキスト入力を行ないたいアプリケーションを開始します (たとえば端末ウィンドウやテキストエディタ、LibreOffice Writer などを 起動します)。
- 3 ジェスチャー認識モードを有効にするには、鉛筆型のアイコンを 1 回押します。
- 4 お使いのグラフィックタブレット内でペンやその他のポインティングデバイスを 利用し、ジェスチャーを実施してください。xstroke はジェスチャーを取り込んで 認識し、フォーカスのあるアプリケーションに対して入力を送信します。
- 5 フォーカスを他のウィンドウに移動するには、必要なウィンドウをペンなどで選択し、しばらく選択したままにします (もしくはお使いのデスクトップのコントロールセンターで設定したキーボードショートカットを利用してもかまいません)。
- 6 ジェスチャー認識モードを解除するには、再度鉛筆型のアイコンを押してください。

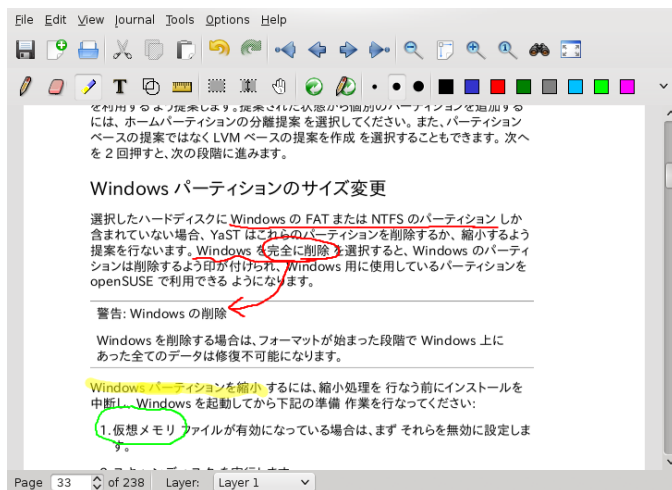
24.6 ペンを利用したメモ取りとスケッチ

ペンを利用して絵を描く作業を行ないたい場合は、GIMP のようなプロフェッショナル向けのグラフィックエディタを使用するほか、Xournal や Jarnal のようなメモを書くための アプリケーションを試してみるのがよいでしょう。Xournal や Jarnal ではペンを利用して メモを書くことができるほか、絵を描いたり PDF ファイルにコメントを書いたりすることができます。Jarnal については、いくつかのプ

ラットフォーム向けに Java ベースの アプリケーションが提供されているため、基本的な共同作業 (コラボレーション) 用の機能も 備わっています。詳しくは <http://www.dklevine.com/general/software/tc1000/jarnal-net.htm> をお読みください。また書いた内容を保存する際、SVG ファイルを含むアーカイブ フォーマット (*.jaj) で保存を行ないます。

メインメニューから Jarnal または Xournal を起動するか、シェルから jarnal または xournal と入力します。たとえば Xournal で PDF ファイルにコメントを付けたい場合は、*File > Annotate PDF* を 選択し、お使いのファイルシステムにある PDF ファイルを開きます。あとはペンや その他のポインティングデバイスを利用して記入を行なってください。作業が終わったら *File > Export to PDF* を選択すると保存を行なうことができます。

図 24.3 Xournal による PDF への注釈付け

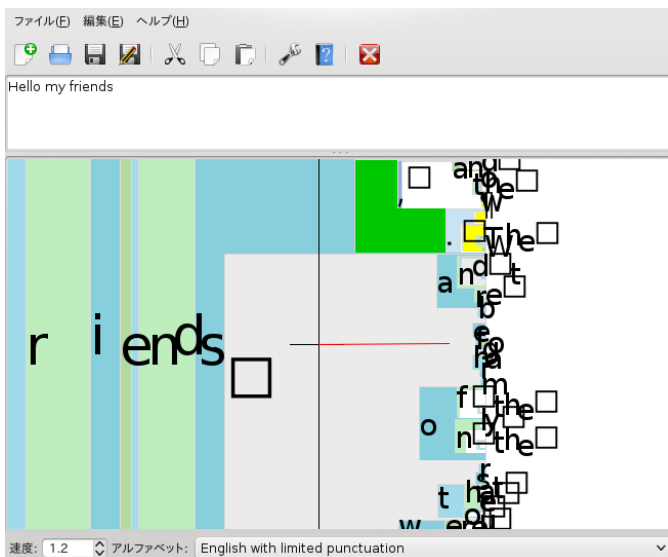


Dasher はもう一つの便利なアプリケーションです。キーボード入力が実用的でない 環境や利用できない環境を主眼において開発されたアプリケーションで、ちょっとした トレーニングを行なうだけでペン (またはその他の入力デバイス。アイトラッカー を 利用することもできます) を利用した大規模なテキスト入力を素早く行なうことができるソフトウェアです。

メインメニューから Dasher を起動するか、シェルから dasher と入力します。ペンを 一方に動かすと右側にある文字が拡大していきます。真ん中にある 十字の線を文字が通過すると、テキストが作成されるか予測され、ウインドウの上部に 入力が行なわれます。書き込みを停止したり開始したりしたい場合は、ペンを利用して ディス

プレイ上の任意の場所で押してください。また、拡大の早さを修正するには、ウインドウの下側で設定してください。

図 24.4 *dasher* を利用したテキスト編集



Dasher の考え方は多くの言語で利用できます。詳しくは Dasher の Web サイト <http://www.inference.phy.cam.ac.uk/dasher/> (英語) をお読みください。広範囲のドキュメンテーションやデモ、トレーニングテキストなどが存在します。

24.7 トラブルシューティング

仮想キーボードがログイン画面に現われない

時折、ログイン画面に仮想キーボードが表示されない場合があります。これを解決するには、++ を 2 回押して X サーバを再起動するか、もしくはタブレット PC で必要な キーを押してください (内蔵キーボードを搭載していないスレート型の型式をご利用の場合)。それでも仮想キーボードが表示されない場合は、お使いの PC に 外付けキーボードを接続し、ハードウェアのキーボードからログインを行なってください。

Wacom グラフィックタブレットの向きが変更できない

xrandr コマンドを利用すると、シェルからディスプレイの 向きを変更することができます。利用可能なオプションの一覧を表示するには、xrandr --help コマ

ンドを実行してください。同時にお使いのグラフィックタブレットの向きを変えたい場合は、下記のようにコマンドを修正する必要があります:

- 通常の向き (0 度の回転):

```
xrandr -o normal && xsetwacom --set "Serial Wacom Tablet" Rotate NONE
```

- 90 度の回転 (時計回り、ポートレート):

```
xrandr -o right && xsetwacom --set "Serial Wacom Tablet" Rotate CW
```

- 180 度の回転 (ランドスケープ):

```
xrandr -o inverted && xsetwacom --set "Serial Wacom Tablet" Rotate HALF
```

- 270 度の回転 (反時計回り、ポートレート):

```
xrandr -o left && xsetwacom set --"Serial Wacom Tablet" Rotate CCW
```

なお、上記のコマンドは `xsetwacom list` コマンドの 出力結果次第であることに注意してください。また、`"Serial Wacom Tablet"` の部分は、それぞれスタイラスやタッチデバイスの 出力結果を指定してください。タッチサポート付きの Wacom デバイス (指でカーソルを動かせるタイプ) をお使いの場合は、タッチデバイスについても回転を設定する必要があります。

24.8 さらなる情報

ここで説明したアプリケーションは、場合によっては統合されたオンラインヘルプが提供されていない場合があります。このような場合は、使用や設定方法に関するドキュメントが `/usr/share/doc/package/パッケージ名` のディレクトリに存在するか、もしくは下記の Web サイト (いずれも英語) にあります:

- Xournal のマニュアルについては、<http://xournal.sourceforge.net/manual.html> をお読みください。
- Jarnal のドキュメンテーションについては、<http://www.dklevine.com/general/software/tc1000/jarnal.htm#documentation> をお読みください。
- xstroke のマニュアルページは <http://davesource.com/Projects/xstroke/xstroke.txt> をお読みください。
- Linux 上の X システムで Wacom デバイスを設定する方法については、<http://linuxwacom.sourceforge.net/index.php/howto/x11> をお読みください。

- Dasher プロジェクトについて有益な情報は、<http://www.inference.phy.cam.ac.uk/dasher/> をお読みください。
- CellWriter に関するさらなる情報とドキュメンテーションについては、<http://risujin.org/cellwriter/> をお読みください。
- gnome-display-properties に関する情報は、<http://old-en.opensuse.org/GNOME/Multiscreen> をお読みください。

ファイルのコピーと共有

複数のオペレーティングシステム (OS) を同時にお使いの環境では、それらの OS 間で ファイルを共有する要件がしばしば発生します。同じマシンでそれぞれ別々のパーティションに異なるシステムが存在する場合がありますし、ネットワークを介して異なるシステム同士が接続されている場合もあります。ここでは、それらの異なるシステム同士でファイル交換を行なう方法と、間違いやすい点をそれぞれ記述しています。

警告: 下記の手順は個人用／家庭用ネットワーク専用の手順です

下記に示す手順は、ファイアウォールで守られた個人用／家庭用のネットワーク以外では実施してはなりません。ファイアウォールで保護されていないネットワークや、企業用のネットワークにおいては、より高度なセキュリティ要件とそれに伴う設定が必要となりますが、本章では言及していないことをご了承ください。

データの交換を行なうためには、下記のいずれかの作業で実現します:

コピー

一方のシステムから他方のシステムにデータを転送することでデータの交換を行なう方法です。結果として、両方のシステムに同じデータが存在するようになります。

データの同期とは、データのコピーを特別な方法で行なうことを指します。一方のコンピュータでファイルを変更すると、同期を行なうことで他方のコンピュータにも自動で変更が反映されるようになります。たとえばお使いのラップトップに修正済みのファイルが存在し、その修正をデスクトップ側にも反映させたいような場合に該当します。

共有

クライアント／サーバの関係を設定して、お使いのファイルを共有する方法です。サーバ側からは、クライアント側からアクセスできる形式でファイルを提供します。ファイルを変更すると、その変更はサーバ内で実施されるため、クライアント側にはデータが残らなくなります。一般的にファイルサーバとは、クライアントに対して同時に多数のファイルを提供する仕組みです。

25.1 シナリオ

下記には、ファイル転送を行なう際に考えられるシナリオの一覧を示しています：

同じコンピュータ内での異なる OS の使用

多くのユーザがお使いのコンピュータには、製造元がインストールしたオペレーティングシステムが存在していて、それとは異なるパーティション上で Linux が動作しているはずです。詳しくは 25.4 項「同一のコンピュータにおける異なる OS 上のファイルへのアクセス」(470 ページ)をお読みください。

ネットワークで接続されていない異なるコンピュータ

任意のメディア (CD, DVD, USB フラッシュメモリ, 外付けハードディスクなど) にデータを保存し、複製先のマシンに接続 (または挿入) してください。この方法はコストがかからず直感的で、かつ直接的な方法です。ただし、両方のコンピュータに適切なドライブやポートが必要になってしまうほか、両方のマシンのオペレーティングシステムで認識可能なファイルシステムを利用しなければなりません。

また、各メディアのサイズまでのファイルしかいっぺんに転送することができません。恒久的にファイルをコピーするような要件の場合は、ネットワークによる接続をお考えください。

同じネットワークに接続されている異なるコンピュータ

一方のコンピュータにサーバを設定し、サーバとクライアントを接続してファイルをコピーしてください。この作業を行なうためのプロトコルは多くの種類が存在するため、要件とお使いの方の知識にあったものを選んでお使いください。

クライアント／サーバの設定作業には知識が必要となるほか、管理の手間も発生してしまいますが、日々の作業でファイルを交換する必要がある場合や、複数のシステムで交換する必要がある場合にはよりよい選択肢となります。特に恒久的なファイル交換をご希望の場合は、クライアント／サーバの設定を選んでください。この方法では、ファイル交換時のサイズ制限などはありません。詳しくは 25.2 項「アクセス方法」(467 ページ)をお読みください。

異なるネットワークに接続されている異なるコンピュータ

このシナリオの場合は、それぞれのネットワークが接続されている必要がありますが、接続のための作業は本章の範囲外であるため、記述されていません。コンピュータがネットワークで接続されていないものとして、ファイルを転送してください。

25.2 アクセス方法

下記には、ファイル転送やファイル共有を行なうために利用する方法やプロトコルを示しています：

FTP

ファイルの交換を異なるユーザと頻繁に行なうような場合は、FTP (File Transfer Protocol; ファイル転送プロトコル) を利用するのがお勧めです。FTP サーバの一方のシステムに設定し、クライアントからそこにアクセスするだけの作業です。Windows や MacOS, Linux などの多くの OS 向けにグラフィカルな FTP クライアントソフトウェアが存在しています。どのような FTP サーバを利用するのかにもよりますが、一般に読み書きの権限を設定して使用します。FTP について、詳しくは 25.5.4 項「FTP を利用したファイルコピー」(477 ページ) をお読みください。

NFS

NFS (Network File System; ネットワークファイルシステム) はクライアント／サーバ型のシステムです。サーバは 1 つまたはそれ以上のディレクトリをクライアント からインポートできるように公開します。詳しくは 第16章 *NFS* でのファイル共有 (313 ページ) をお読みください。

ファイルの交換を異なるユーザと頻繁に行なうような環境では NFS がお勧めです。一般に、このプロトコルは Windows よりも Linux でより一般的な方法です。NFS で公開 (エクスポート) したディレクトリは、お使いの Linux システムにうまく統合することができ、ローカルマシンのフォルダと同じような方法でディレクトリ構造にアクセスすることができるようになります。ご利用の設定にもよりますが、サーバ上で読み込みまたは書き込み、もしくはその両方を設定して使用します。通常は個人／一般家庭使用の範囲では読み書きの権限を設定して使用します。

rsync

それほど大規模に変更がかからないような巨大データについて、それらを定期的に転送したい場合は、rsync を使用するのがお勧めです。このプロトコ

ルは Linux および Windows に対応し、一般的には rsync をデータのバックアップ管理として 使用します。詳しくは rsync のマニュアルページか、もしくは 25.5.2 項「rsync を利用したファイル転送」(473 ページ) をお読みください。

Unison

Unison は rsync の代替プロトコルで、異なるコンピュータ間で定期的な同期を行なうためのものですが、rsync とは異なり双方向で同期を行なうことができます。詳しくは Unison のマニュアルページか、もしくは 25.5.3 項「Unison を利用したファイル転送」(475 ページ) のマニュアルページをお読みください。なお、Unison は Linux および Windows に対応しています。

CSync

CSync は Unison の代替手段です。Unison と同様にディレクトリを双方向に同期 することができます。そのうえモジュール形式で構成されているため、プラグインでの 拡張が可能です。詳しくは <http://www.csync.org> をお読みください。

SMB

Samba はクライアント／サーバ型のシステムで、SMB プロトコルを実装したソフトウェアです。SMB プロトコルは一般に Windows ネットワークで使用される ものですが、複数のオペレーティングシステムに対応しています。Samba について 詳しくは、第17章 *Samba* (329 ページ) をお読みください。

ファイル交換を頻繁に行なう環境で、特に Windows システムを利用する複数の ユーザを相手にして共有する必要がある場合に、Samba がお勧めです。Samba は Linux だけの環境ではあまり使用されておらず、代わりに NFS を使用します。Samba サーバの設定について、詳しくは 25.8 項「Samba を利用した Linux と Windows のファイル共有」(483 ページ) をお読みください。

SSH

SSH (セキュアシェル; Secure Shell) はコンピュータ間で機密を保持した形で通信を行なうことができます。SSH の一式には複数のコマンドが含まれていて、ユーザを認証するのに公開鍵を使用することができます。詳しくは 第12章 *SSH: 機密を保護する通信* (↑セキュリティガイド) をお読みください。

ファイルのコピー頻度が低く、信頼できないネットワークを介して通信を行なう必要がある場合のほか、これを行なうのが 1 人だけである場合に SSH がお勧めです。グラフィカルなユーザインターフェイスも利用できますが、SSH は一般的にコマンドラインユーティリティを利用するものと考えられています。Linux や Windows にそれぞれ対応しています。

25.3 直接接続によるファイルアクセス

この章では、イーサネットのクロスオーバーケーブルを利用し、2 台のコンピュータを接続してファイルを交換するための手順を示しています。

それぞれ下記のものを用意します:

- イーサネットのクロスオーバーケーブル。詳しくは <http://ja.wikipedia.org/wiki/%E3%82%A4%E3%83%BC%E3%82%B5%E3%83%8D%E3%83%83%E3%83%88%E3%83%BB%E3%82%AF%E3%83%AD%E3%82%B9%E3%82%AA%E3%83%BC%E3%83%90%E3%83%BC%E3%83%BB%E3%82%B1%E3%83%BC%E3%83%96%E3%83%AB> をお読みください。
- 両方のコンピュータでの openSUSE の起動
- ネットワークの接続。
- 両方のマシンでの SSH デーモンの起動。サービスを起動するには、root で `rcsshd start` のコマンドを実行します。

下記のようにして行ないます:

手順 25.1 GNOME

- 1 Nautilus を起動します。
- 2 ファイル > サーバへ接続 を選択します。
- 3 サービスの種類 では `ssh` を選択します。
- 4 相手のコンピュータの IP アドレスと、ポート番号 (既定値は 22) を入力します。
- 5 相手のコンピュータ上で、開きたいフォルダを入力します。
- 6 接続する を押します。

手順 25.2 KDE

- 1 Dolphin を起動します。
- 2 ネットワーク を選択し、ネットワークフォルダを追加 を押します。上記が表示されない場合は、表示 > パネル > 場所 を選択してください。

- 3 ネットワークフォルダのタイプには *セキュアシェル (ssh)* を 選択します。
- 4 それぞれ IP アドレス、ポート (既定値は 22)、相手のコンピュータにおけるフォルダ 名をそれぞれ入力します。下の方にあるチェックボックスにチェックを入れることで、この接続に対するアイコンを作成することもできます。Dolphin では、ネットワーク タブに表示されます。
- 5 ダイアログで *保存して接続* を押すと、パスワードを尋ねられる ので入力を行ないます。

上記の手順を行なうことで、相手側のコンピュータにあるフォルダを開くことができます。

25.4 同一のコンピュータにおける異なる OS 上のファイルへのアクセス

新しく購入したコンピュータの場合、一般に何らかのオペレーティングシステム (OS)、多くは Windows がインストールされています。Linux を異なるパーティションに インストールした場合、それらのオペレーティングシステムとファイルを交換するような要件が発生する場合があります。

Windows の既定では、Linux のパーティションを読み込むことができません。これらの オペレーティングシステム間でファイルを交換したい場合は、一般に「交換用のパーティション」を作成して対応します。より直接的な方法で 解決したい場合は、Windows 側で ext2 ファイルシステムにアクセスできるドライバを利用する方法があります。詳しくは <http://www.fs-driver.org/> (英語) をお読みください。なお、交換用のパーティションとして Windows と Linux の両方から アクセスできるようにするには、下記のいずれかのファイルシステムを利用します:

FAT

この種類のファイルシステムは、MS-DOS や Windows 95, Windows 98 などで利用 されています。YaST を利用することで、この種類のファイルシステムを作成することができるとともに、Linux から FAT パーティションにアクセスし、読み込みや書き込みを行なうことができます。FAT パーティションのサイズ (およびファイル 1 つ あたりの最大サイズ) には制限があり、利用する FAT バージョンによって異なっています。FAT ファイルシステムについて、詳しくは <http://ja.wikipedia.org/wiki/VFAT> をお読みください。

NTFS

NTFS ファイルシステムは Windows で使用されているファイル システムです。openSUSE には NTFS ファイルシステムに対して書き込みを行なうことのできる機能が用意されています。詳しくは <http://en.opensuse.org/SDB:NTFS> (英語) をお読みください。

openSUSE のインストール時に Windows パーティションが存在すると、それらは検出され設定されますので、インストールが終われば Windows パーティションがマウントされます。お使いの Windows 側のデータにアクセスする方法は以下のものがあります:

KDE

まずは + F2 を押し、`sysinfo:/` と入力します。新しいウインドウが開いて、お使いのマシンに関する各種の情報が表示されます。*Disk Information* には接続されているハードディスクのパーティション情報が表示されますので、*Filesystem* の欄が `ntfs` または `vfat` になっているものを選び、マウスのボタンを押してください。パーティションがマウントされていない場合は、KDE がマウントを行なって中身を表示します。

コマンドライン

`/windows` ディレクトリの一覧を表示することで、お使いの Windows ドライブに含まれているコンテンツを表示することができます。たとえば Windows 側での `C:` ドライブが `/windows/c` ディレクトリになるように割り当てられます。

注記: Windows パーティションのアクセス権変更

ファイルシステムへのダメージを防ぐため、通常のユーザに対しては読み込みだけを 行なうことができるような形でマウントが行なわれます。Windows のパーティションに 通常のユーザから書き込みを含む完全なアクセス権を与えるには、これらの Windows パーティションのマウント方法を変更する必要があります。それぞれ `vfat` については `mount` コマンドのマニュアルページを、NTFS については `ntfs-3g` のマニュアルページをお読みください。

25.5 Linux コンピュータ間のファイルコピー

Linux では、コンピュータ間でファイルをコピーするためのプロトコルが多く用意されています。どのプロトコルを使用すべきかについては、どの程度の労力をかける

のかと Windows インストールとの互換性がどうかによって決まります。本章では、Linux コンピュータからファイルをコピーしたり、Linux コンピュータにファイルをコピーしたりするための各種の手順を示しています。なお、本章ではネットワークを利用したコピーを行なうため、あらかじめネットワークの環境設定が完了していることを想定しています。また、全てのシナリオでは名前解決が動作する必要もあります。お使いのネットワークにネームサービスがない場合、IP アドレスを直接使用するか、もしくは全てのホストの `/etc/hosts` にホスト名と IP アドレスの対応を記述してください。

下記の例では、それぞれ下記の IP アドレスとホスト名を使用します：

宛先ホスト名	jupiter.example.com
宛先 IP	192.168.2.100
コピー元ホスト名	venus.example.com
コピー元 IP	192.168.2.101
ユーザ	tux

25.5.1 SSH を利用したファイルコピー

SSH 経由でアクセスする両方のコンピュータは、下記の要件を全て満たしてなければなりません：

1. ホスト名を使用してアクセスする場合は、それぞれのホスト名が両方のコンピュータ内の `/etc/hosts` ファイルに記載されていること（詳しくは 11.6.1.6 項「`/etc/hosts`」(253 ページ) をお読みください）。IP アドレスで SSH アクセスを行なう場合、上記は特に必要ではありません。
2. ファイアウォールをお使いの場合は、SSH のポートを開くこと。これを行なうには、YaST を起動して **セキュリティとユーザ > ファイアウォール** を選択します。その状態から **許可するサービス** を選択し、**SSH** が一覧に載っているかどうかを確認します。一覧に載っていない場合は、**許可するサービス** で SSH を選択して、**追加** を押します。あとは **次へ 完了** と押していき、変更内容を保存して YaST を終了します。

一方のコンピュータから他方のコンピュータにファイルをコピーするには、そのファイル がどこに存在しているのかを知っておく必要があります。たとえば

jupiter.example.com というコンピュータにある単一のファイル /srv/foo_file をカレントディレクトリにコピーするには、下記のような scp コマンドを実行します (ドットはコピー先を 指定しているもので、カレントディレクトリを意味します):

```
scp tux@jupiter.example.com:/srv/foo_file .
```

ディレクトリ構造全体をコピーしたい場合は、下記のような scp の再帰モードを利用します:

```
scp -r tux@jupiter.example.com:/srv/foo_directory .
```

ネットワーク内で名前解決を行なうことができない場合は、サーバの IP アドレスを直接指定します:

```
scp tux@192.168.2.100:/srv/foo_file .
```

どこにファイルが存在するのかわからない場合は、sftp コマンドを利用します。KDE や GNOME で SFTP を利用したファイルのコピーを行なうのはとても簡単です。下記のようにして行ないます:

- 1 + F2 を押します。
- 2 コマンドの欄に下記を記入します (お使いの環境に合わせて変更してください):
`sftp://tux@jupiter.example.com`
- 3 サーバが提示する鍵情報について確認が行なわれたあと、jupiter.example.com 上のユーザ tux に対して、パスワードを入力します。
- 4 必要なファイルやディレクトリを、お使いのデスクトップなどのローカルディレクトリからドラッグ&ドロップで配置します。

KDE では sftp が利用できない場合、fish と呼ばれるもう 1 つのプロトコルを利用することができます。このプロトコルは sftp とよく似た使い方になっていて、単に sftp を fish に置き換えるだけで 動作するようになっています:

```
fish://tux@jupiter.example.com
```

25.5.2 rsync を利用したファイル転送

rsync はデータをコピーしたりアーカイブを作成したりするのに便利なソフトウェアであるほか、デーモンとして起動することでネットワーク側にディレクトリを提供することができます (詳しくは 手順25.3「rsync 同期に対する高度な設定」(474 ページ))。

異なるコンピュータ間で `rsync` を利用したファイルやディレクトリの同期を行なう 前に、下記の要件が満たされていることをご確認ください:

1. `rsync` パッケージがインストール されていること。
2. 両方のシステムに同じユーザが存在すること。
3. サーバ側に十分なディスク領域が存在すること。
4. `rsync` の能力を完全に引き出したい場合は、サーバ側として利用するシステムに `rsyncd` がインストールされていること。

25.5.2.1 `rsync` 基本モード

`rsync` を基本モードで利用する場合には、特別な設定は不要です。`rsync` では 他のシステムに存在するディレクトリについて、完全な複製を作成します。`scp` などの通常のコピーツールと大きく異なるようなことはありません。たとえば 下記のコマンドでは、`jupiter` と呼ばれるバックアップ サーバ上にあるユーザ `tux` のホームディレクトリについて、バックアップを採取します:

```
rsync -Hbaz -e ssh /home/tux/ tux@jupiter:backup
```

バックアップから復元を行なう場合は、下記のコマンドを実行します (`-b` オプション無しで実行します):

```
rsync -Haz -e ssh tux@jupiter:backup /home/tux/
```

25.5.2.2 `rsync` デーモンモード

`rsync` の全ての機能を利用できるようにするため、一方のシステムで `rsyncd` デーモンを 起動します。このモードでは、アカウント無しでアクセスすることのできる同期ポイント (モジュール) を作成することができます。`rsync` デーモンを使用するには、下記のようにして行ないます:

手順 25.3 *`rsync` 同期に対する高度な設定*

- 1 `root` でログインを行ない、`rsync` パッケージをインストールします。
- 2 同期ポイントを `/etc/rsyncd.conf` ファイルに設定します。大括弧内に同期ポイントの名前を入力し、`path` キーワード に続いて実際のパスを入力します。たとえば以下ようになります:


```
[FTP]
path = /srv/ftp
comment = An Example
```

- 3 root の状態から `rcrsyncd start` コマンドを実行し、`rsyncd` デーモンを起動します。システム起動時に自動的に `rsync` サービスを起動するように設定したい場合は、`insserv rsyncd` コマンドを実行します。

- 4 `/srv/ftp` ディレクトリ内にある全てのファイルを一覧表示 するには、下記のように実行します (コロンが二重に付けられていることに注意):

```
rsync -avz jupiter::FTP
```

- 5 宛先のディレクトリ (この場合はドットを指定していて、カレントディレクトリにコピーする意味です) を指定すると、実際の転送を行なうことができます:

```
rsync -avz jupiter::FTP .
```

既定では `rsync` を利用して同期を行なう限り、ファイルが削除されることはありません。ファイルの削除を行なうには、`--delete` オプションを指定してください。なお、`--delete` オプションで新しいファイルが 削除されないようにしたい場合は、代わりに `--update` オプションを 指定してください。これにより発生する矛盾は、それぞれ手作業で解決する必要があります。

25.5.3 Unison を利用したファイル転送

異なるコンピュータ間で `Unison` を利用してファイルやディレクトリの同期を行なう前に、下記の要件が満たされていることをご確認ください:

1. `unison` パッケージがインストールされていること。
2. ローカルとリモートのコンピュータに、それぞれ十分なディスク容量があること。
3. `Unison` の能力を完全に引き出したい場合は、リモートのコンピュータにも `Unison` がインストールされていて、かつ起動していること。

ヘルプを必要とする場合は、`Unison` に `-doc topics` オプション を付けて起動し、利用可能なオプション一覧を表示させてください。

恒久的に設定を保存する場合、`Unison` は同期すべきディレクトリ (ルート) や無視する ファイルタイプなどのような各種設定を保存するための、`プロファイル` を作成することができます。プロファイルはテキストファイル形式で保存され、`~/unison` ディレクトリ以下に `*.prf` という拡張子で保存します。

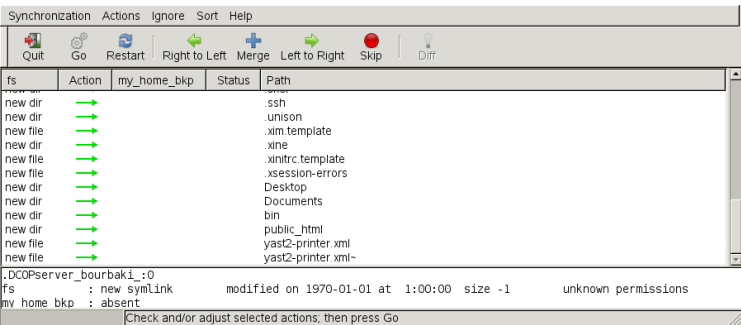
25.5.3.1 GUI の使用

Unison の GUI を利用して異なるディレクトリを同期するには、下記のようにして 行 ないます:

- 1 + F2 を押し、入力するコマンドに unison と入力して Unison を起動します。
- 2 Unison を始めた起動した場合、何もオプションを指定しなければ、複製元のディレクトリを尋ねられます。同期対象の複製もとディレクトリを入力して、OK を押します。
- 3 次に宛先のディレクトリを指定します。これはローカルでもリモートでもかまいません。リモートのディレクトリと同期を行ないたい場合は、方法 (SSH, RSH, ソケット) を選択し、ホスト名とユーザ名 (任意指定) も入力します。
- 4 以前にこれら 2 つのディレクトリについて同期を行なったことがない場合は、Unison がこれからこれらのディレクトリの比較を行なう旨の警告メッセージが表示されます。OK を押して警告メッセージを閉じると、Unison は両方のディレクトリの情報収集を行ないます。これが完了するまで 待機すると、メインウィンドウに両方のディレクトリの差が表示されるようになります。

左側の列には選択した比較元ディレクトリの一覧が表示され、右側には比較 先のディレクトリが表示されます。これらのディレクトリに差異があると、Action 列に作業提案が表示されます。緑色の矢印は、比較もとまたは比較先のディレクトリでファイルが更新／追加／削除されたことを示しています。矢印の向きが同期方向で、同期実行時にどちらからコピーを行なうのかを指定します。クエスチョンマークは矛盾を示していて、両方の ファイルが更新されていることにより、どちらを最新のものとして扱えば よいのかかわからないことを示しています。

図 25.1 ファイル同期の提案



- 5 それぞれのファイルに対して Unison が表示した提案を変更する (たとえば同期方向を変更するなど) には、ファイルを選択して *Right to Left* (右から左に) または *Left to Right* (左から右に) を押します。 *Skip* を押すとファイルを同期対象から外します。それぞれ *Action* の列の表示が選択にあわせて変化します。
- 6 同期作業を開始するには、 *Go* を押します。

次回以降に Unison を起動した場合は、既存のプロファイルを示すダイアログ ボックスが表示され、同期すべきディレクトリの対を指定します。プロファイルの一覧から選択を行なうか、もしくは新しいプロファイルを作成 (ディレクトリの対を新規に追加し、設定した同期作業を行なうこと) になります。

25.5.3.2 コマンドラインの使用

Unison はコマンドラインを利用して操作することもできます。ローカルディレクトリとリモートのコンピュータとの間で同期を行なうには、下記のようにして行ないます:

- 1 シェルを開き、下記のコマンドを入力します:

```
unison -ui text ディレクトリ  
ssh://tux@jupiter.example.com//パス
```

それぞれディレクトリとパスの項目には必要な値を入力してください。

- 2 Unison はファイルやディレクトリに対して何を行なうのかを尋ねてきます。たとえば:

```
local                jupiter  
    <---- new file  dir [f]
```

- 3 Unison の推奨どおりに作業を行なうには、 *F* を押します。それ以外のコマンドについては *?* を入力してください。
- 4 更新内容を適用するには、 *y* を押します。

25.5.4 FTP を利用したファイルコピー

FTP サーバを設定する前に、下記の要件が満たされていることを ご確認ください:

1. vsftpd パッケージが インストールされていること。
2. FTP サーバに対して root アクセスができること。

3. お使いのコンピュータに十分なディスク容量があること。

警告: 家庭内で使用するネットワーク限定の設定です

この設定は、家庭内で使用するネットワークに適した設定です。ファイアウォールで保護されていないネットワークに配置したり、不特定多数のアクセスを許す設定にしたりしてはなりません。

FTP サーバを設定するには、下記の手順で行ないます:

1 FTP サーバを準備します:

- 1a** シェルを開いて root でログインし、`/etc/vsftpd.conf` ファイルのバックアップ コピーを作成します:

```
cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
```

- 1b** 匿名 FTP 用のアクセスポイントを作成します:

```
mkdir ~ftp/incoming  
chown -R ftp:ftp ~ftp/incoming
```

- 2** 希望するシナリオに沿って、設定ファイルを書き換えます (詳しい設定オプションについては、`vsftpd.conf` の マニュアルページをお読みください):

匿名アクセスによる読み込み／書き込みの許可

```
#  
listen=YES  
  
# FTP サーバに対する匿名アクセスの許可  
anonymous_enable=YES  
  
#  
local_enable=YES  
# 書き込みアクセスの許可  
write_enable=YES  
anon_upload_enable=YES  
anon_mkdir_write_enable=YES  
dirmessage_enable=YES  
# ログファイルの書き込み  
xferlog_enable=YES  
connect_from_port_20=YES  
chown_uploads=YES  
chown_username=ftp  
ftpd_banner=Welcome to FTP service.  
anon_root=/srv/ftp
```

FTP ユーザに対してアクセスの限定を指定

```
chroot_local_users=YES
```

3 FTP サーバを再起動します:

```
rcvsftpd start
```

クライアント側では、お使いのブラウザや FTP クライアントから `ftp://ホスト` と入力します。`ホスト` はお使いの環境に合わせて、サーバのホスト名 または IP アドレスに置き換えてください。なお、FTP サーバのコンテンツに アクセスするのに便利なグラフィカルユーザインターフェイスも多数存在しています。YaST パッケージマネージャから "FTP" と入力すると、それらを一覧表示 することができます。

25.6 SSH を利用した Linux と Windows コンピュータのファイルコピー

SSH を利用して Linux と Windows の間でファイルを転送するには、下記のいずれかのアプリケーションを利用します:

PuTTY

PuTTY は SSH デーモンと通信を行なうためのコマンドラインツール集です。<http://www.chiark.greenend.org.uk/~sgtatham/putty.html> からダウンロードを行なうことができます。

WinSCP

WinSCP は PuTTY にとてもよく似たアプリケーションですが、グラフィカルな ユーザインターフェイスを持つという点が異なります。エクスプローラ型と Norton Commander 型のいずれかを選択することができます。<http://winscp.net> からダウンロードを行なうことができます。

PuTTY を利用して Windows から Linux にファイルをコピーするには、下記のようにして行ないます (Windows マシン側での作業です):

- 1 PSCP を起動します。
- 2 SSH サーバのホスト名を入力します。
- 3 SSH サーバに対するログインとパスワードを入力します。

WinSCP を利用して Windows から Linux に接続するには、下記のようにして 行 ないます (Windows マシン側の作業です):

- 1 WinSCP を起動します。
- 2 SSH サーバのホスト名と、ユーザ名を入力します。
- 3 *Login* を押し、表示される警告を了解します。
- 4 WinSCP のウインドウを利用して、ファイルやディレクトリをドラッグ&ドロップ で 転送します。

注記: SSH フィンガープリント

PuTTY や WinSCP では、初回のログイン時に SSH のフィンガープリントを受け 入れ なければなりません。

25.7 Linux コンピュータ間のファイル共 有

本章では、データを共有するための様々な方法を紹介しています。恒久的なデータ 共有を希望する場合は、これらの方法のうちのいずれかを利用するのがよいでしょ う。

25.7.1 NFS を利用したファイル転送

サーバを設定するには、下記の手順で行ないます:

- 1 システムの準備を行ないます:
 - 1a シェルを開き、root でログインしてから全ユーザに対して書き込み許可を 設定します:

```
mkdir /srv/nfs
chgrp users /srv/nfs
chmod g+w /srv/nfs
```
 - 1b 次に、クライアント側で利用しているユーザ名とユーザ ID が、サーバ上でも 登録済みであることを確認します。ユーザアカウントの作成や管理につ

いては、第10章 *YaST を利用したユーザ管理* (↑ スタートアップ) に詳細な手順があります。

2 NFS サーバを準備します:

2a root で YaST を起動します。

2b ネットワークサービス > *NFS* サーバ を選択します (このモジュールは既定では インストールされません。YaST 内に表示されない場合は、`yast2-nfs-server` パッケージをインストールしてください)。

2c まずは *開始* を選択し、NFS サービスを有効にします。

2d ファイアウォールをお使いの場合は、*ファイアウォールでポートを開く* を選択してファイアウォールのポートを開きます。

3 ディレクトリを公開します:

3a *ディレクトリの追加* を押し、`/srv/nfs` を選択します。

3b オプション設定には下記のように指定します:

`rw, root_squash, async`

3c 複数のディレクトリを公開する場合は、上記の手順を繰り返します。

4 最後に設定を保存して終了します。これで NFS サーバを利用することができるようになります。

NFS サーバを手作業で起動するには、root から `rcnfsserver start` と入力します。サーバを停止するには、`rcnfsserver stop` と入力します。既定では、YaST はシステム起動時にこのサービスの起動を管理します。

クライアントの設定を行なうには、下記の手順で行ないます:

1 NFS クライアントを準備します:

1a root で YaST を起動します。

1b ネットワークサービス > *NFS* クライアント を選択します。

1c ファイアウォールをお使いの場合は、*ファイアウォールでポートを開く* を選択してファイアウォールのポートを開きます。

2 リモート側のファイルシステムを取り込みます:

2a *追加* を押します。

2b NFS サーバのホスト名または IP アドレスを入力するか、もしくは *選択* を押してネットワーク上に存在する NFS サーバの 一覧を表示させ、そこから選択します。

2c リモート側のファイルシステムのディレクトリ名を入力するか、もしくは *選択* を押して自動選択します。

2d 適切なマウント先を指定します。たとえば /mnt のように指定します。なお、この手順を繰り返す 場合は、それぞれ異なるマウントポイント (もちろん /mnt 以外のマウントポイント) を指定します。

2e 複数のディレクトリを取り込む場合は、上記の手順を繰り返します。

3 最後に設定を保存して終了します。これで NFS クライアントの設定は完了です。

なお、NFS クライアントを手作業で起動するには、`rcnfs start` と入力します。

注記: 一貫したユーザ名の使用

ごく少数のユーザでネットワーク環境をお使いの場合は、それぞれのマシンに対して 同じユーザを設定してください。大規模なネットワークなどで多数のユーザを登録する 必要があるような場合は、NIS や LDAP を利用してユーザデータを管理することをお勧めします。詳しくは 第3章 *NIS の使用* (↑セキュリティガイド) と 第4章 *ディレクトリサービス LDAP* (↑セキュリティガイド) をお読みください。

25.7.2 Samba を利用したファイル共有

この章では、Samba サーバ上にあるファイルに対してアクセスを行なうための 各種の方法を説明しています。なお KDE や GNOME には、Samba の共有にアクセスするためのグラフィカルなツールが用意されているほか、Samba サーバにアクセスするためのコマンドラインツールも存在しています。

25.7.2.1 KDE と GNOME を利用した共有へのアクセス

KDE と GNOME のデスクトップでは、ファイルブラウザを利用して Samba の共有にアクセスを行ないます。下記の手順で行なってください:

- 1 + F2 を押し、`smb://jupiter.example.com/共有名` のように入力します。

URL の書式は `smb://ホスト/共有名` で、それぞれ `ホスト` には Samba サーバのホスト名 (`jupiter.example.com`) または IP アドレスを、`共有名` には共有名を指定します。詳しくは ステップ 3b (485 ページ) をお読みください。

- 2 ユーザ名とパスワードを入力してログインします。パスワードは ステップ 4 (485 ページ) の手順で設定するか、パスワードを必要としない環境であれば、何も入力せずに を押します。
- 3 開いたウィンドウを利用して、ドラッグ&ドロップでファイルやディレクトリを操作します。

なお、お使いのネットワーク環境のワークグループ名がわからない場合は、`smb:/` と入力すると一覧を表示することができます。Smb4K ツール (`smb4k` パッケージ) では、ネットワーク上に存在する全ワークグループを表示することができるほか、必要に応じてマウントを行なうことができます。

25.7.2.2 コマンドラインからの共有へのアクセス

コマンドラインを利用してアクセスしたい場合は、`smbclient` コマンドを利用します。Samba サーバにログインするには、下記のコマンドを実行してください：

```
smbclient //jupiter/share -U tux
```

既に `tux` ユーザになっている場合、`-U` は不要です。正常にログインが完了すると、それぞれ `ls` (ディレクトリ一覧の表示)、`mkdir` (ディレクトリの作成)、`get` (ファイルのダウンロード)、`put` (ファイルのアップロード) などのコマンドが利用できるようになります。利用可能な全てのコマンドを表示するには、`help` と入力してください。詳しくは `smbclient` のマニュアルページをお読みください。

25.8 Samba を利用した Linux と Windows のファイル共有

Samba は Windows と Linux マシンの間でファイルを転送する際、第一に選択すべきものです。Samba を利用するにあたっては、下記のような使用形態が考えられます：

SMB スキームを利用した Linux から Windows へのファイル転送

Linux サーバを設定する必要が無いため、もっとも簡単な方法です。`smb:/` というスキームを利用してアクセスを行ないます。詳しくは 25.7.2.1 項「KDE と

GNOME を利用した共有へのアクセス」(482 ページ)をお読みください。なお、両方のシステムでワークグループの設定が同じに設定されていて、ディレクトリを共有していることをご確認ください。

サーバを利用した Windows から Linux へのファイル転送
お使いの Linux コンピュータ側で Samba サーバの設定を行ないます。詳しくは 手順25.4「Samba サーバの設定」(484 ページ)をお読みください。

ヒント: お使いの Windows システムにおけるレジストリ設定の適用

Windows のバージョン (95, 98) によっては、異なる認証方法を有効にするため、レジストリを少しだけ変更する必要があります。これを簡単に行なうには、samba-doc パッケージをインストールして /usr/share/doc/packages/samba/registry 内にあるファイルを Windows ドライブにコピーしてください。あとは Windows 側でそのファイルをダブルクリックすると、変更を適用することができます。

手順 25.4 Samba サーバの設定

Samba サーバを設定するには、下記の手順で行ないます:

1 Samba サーバを準備します:

1a root で YaST を起動します。

1b samba パッケージをインストールします。

1c ディレクトリを作成します (以降では /srv/share ディレクトリを作成するものとします)。

2 サーバ設定を作成します:

2a ネットワークサービス > Samba サーバを選択します。

2b 表示されたワークグループ名からいずれかを選択するか、もしくは新しいワークグループ名を入力します (以降では Penguin ワークグループを選択したものとします)。

2c プライマリドメインコントローラ (PDC) を選択します。

2d お使いのコンピュータの起動時、毎回 Samba サーバを自動で起動したい場合は、*起動時の動作* を選択します。それ以外の場合は *手動* を選択します。

2e ファイアウォールをお使いの場合は、*ファイアウォールでポートを開く* を選択してファイアウォールのポートを開きます。

3 Windows 共有を作成します:

3a *共有* タブに移動し、*追加* を押します。

3b 共有名と説明を入力します。*共有名* には、クライアント からアクセスする際の名前を入力します。*共有の説明* には、この共有の目的を記入します。

3c パスを選択します (たとえば `/src/share` を選択します)。

3d *OK* を押して先に進みます。

3e *ユーザにディレクトリの共有を許可する* を選択します。

4 このサービスの利用を許可する全てのユーザに対して、下記のようにしてパスワードを設定します:

```
smbpasswd -a tux
```

設定を簡単にするには、*だけ* を押してパスワードを何も設定しないのがよいでしょう。なお、お使いの Windows と Linux ではそれぞれアカウントの管理体系が異なるため、同じユーザ名を持つ ユーザを設定するようにしてください。

5 Samba サーバを起動します:

```
rcnmb start  
rcsmb start
```

正しく設定を行なうことができているかどうかを確認するには、下記のように入力します:

```
smbclient -L localhost
```

を押すと、下記のような表示が 現われるはずです:

```
Anonymous login successful  
Domain=[PENGUIN] OS=[Unix] Server=[Samba 3.0.22-11-SUSE-CODE10]
```

Sharename	Type	Comment
-----	----	-----
share	Disk	Shared directory
netlogon	Disk	Network Logon Service
IPC\$	IPC	IPC Service (Samba 3.0.22-11-SUSE-CODE10)
ADMIN\$	IPC	IPC Service (Samba 3.0.22-11-SUSE-CODE10)

Anonymous login successful
Domain=[PENGUIN] OS=[Unix] Server=[Samba 3.0.22-11-SUSE-CODE10]

Server	Comment
-----	-----
SUSE-DESKTOP	Samba 3.0.22-11-SUSE-CODE10

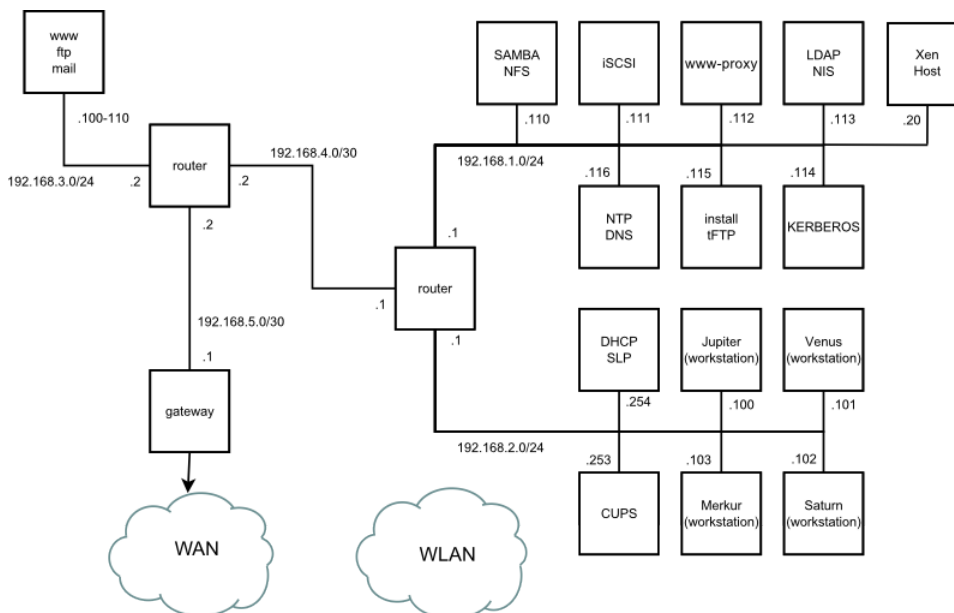
Workgroup	Master
-----	-----
TUX-NET	jupiter

25.9 さらなる情報

- <http://ja.wikipedia.org/wiki/VFAT>
- <http://ja.wikipedia.org/wiki/NTFS>
- <http://en.wikipedia.org/wiki/Fstab> (英語)
- http://ja.wikipedia.org/wiki/Network_File_System
- http://ja.wikipedia.org/wiki/File_Transfer_Protocol
- http://ja.wikipedia.org/wiki/Secure_Shell
- <http://ja.wikipedia.org/wiki/Rsync>
- <http://ja.wikipedia.org/wiki/Samba>

サンプルネットワーク

下記に示すサンプルネットワークは、openSUSE® ドキュメンテーションに おける ネットワーク関連の記述で利用されます。





GNU ライセンス

本付録には、GNU General Public License バージョン 2 と GNU Free Documentation License バージョン 1.2 を掲載しています。

なお、八田真行氏 (mhatta@gnu.org) [<mailto:mhatta@gnu.org>] による各ライセンスの日本語訳を併記しています。

ただし、各日本語訳は *非公式*なものであり、フリーソフトウェア財団 (the Free Software Foundation) によって発表されたものではないことにご注意ください。法的に有効なものは常に原文 (つまり英語版) 側であり、日本語訳は各ライセンスをよりよく理解する支援を行なう目的で 作成されたもの、という扱いです。

また、日本語訳は DocBook (novdoc) に合わせて段落を分割しているほか、引用符のタグ化 ("blah" -> <quote>blah</quote>) とリンクの生成 (ulink) を行なっています。

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The «Program», below, refers to any such program or work, and a «work based on the Program» means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term «modification».) Each licensee is addressed as «you».

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and [any later version], you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.  
Copyright (C) yyyy name of author
```

```
This program is free software; you can redistribute it and/or  
modify it under the terms of the GNU General Public License  
as published by the Free Software Foundation; either version 2  
of the License, or (at your option) any later version.
```

```
This program is distributed in the hope that it will be useful,  
but WITHOUT ANY WARRANTY; without even the implied warranty of  
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the  
GNU General Public License for more details.
```

```
You should have received a copy of the GNU General Public License  
along with this program; if not, write to the Free Software  
Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author  
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details  
type `show w' . This is free software, and you are welcome  
to redistribute it under certain conditions; type `show c'  
for details.
```

The hypothetical commands "show w" and "show c" should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than "show w" and "show c"; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright
```

```
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.
```

```
signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License [<http://www.fsf.org/licenses/lgpl.html>] instead of this License.

GNU 一般公衆利用許諾契約書 (日本語訳)

バージョン 2, 1991年6月

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

この利用許諾契約書を、一字一句そのままに複製し頒布することは許可する。しかし変更は認めない。

はじめに

ソフトウェア向けライセンスの大半は、あなたがそのソフトウェアを共有したり 変更したりする自由を奪うように設計されています。対照的に、GNU 一般公衆利用許諾契約書は、あなたがフリーソフトウェアを共有したり変更したりする自由を保証する--すなわち、ソフトウェアがそのユーザすべてにとってフリー であることを保証することを目的としています。この一般公衆利用許諾契約書は、フリーソフトウェア財団のソフトウェアのほとんどに適用されており、また GNU GPLを適用すると決めたフリーソフトウェア財団以外の作者によるプログラムにも適用されています(いくつかのフリーソフトウェア財団のソフトウェアには、GNU GPLではなくGNU ライブラリー一般公衆利用許諾契約書が適用されています)。あなたもまた、ご自分のプログラムにGNU GPLを適用することが可能です。

私たちがフリーソフトウェアと言うとき、それは利用の自由について言及している のであって、価格は問題にしていません。私たちの一般公衆利用許諾契約書は、あなたがフリーソフトウェアの複製物を頒布する自由を保証するよう設計されています (希望に応じてその種のサービスに手数料を課す自由も保証されます)。また、あなたがソースコードを受け取るか、あるいは望めばそれを入手することが可能であるということ、あなたがソフトウェアを変更し、その一部を新たなフリーの プログラムで利用できるとのこと、そして、以上で述べたようなことができる ということがあなたに知られるということも保証されます。

あなたの権利を守るため、私たちは誰かがあなたの有するこれらの権利を否定する ことや、これらの権利を放棄するよう要求することを禁止するという制限を加える 必要があります。よって、あなたがソフトウェアの複製物を頒布したりそれを変更 したりする場合には、そういった制限のためにあなたにある種の責任が発生することになります。

例えば、あなたがフリーなプログラムの複製物を頒布する場合、有料が無料に 関わらず、あなたは自分が有する権利を全て受領者に与えなければなりません。また、あなたは彼らもソースコードを受け取るか手に入れることができるよう 保証しなければなりません。そして、あなたは彼らに対して以下で述べる条件を示し、彼らに自らの持つ権利について知らしめるようにしなければなりません。

私たちはあなたの権利を二段階の手順を踏んで保護します。(1) まずソフトウェアに対して著作権を主張し、そして (2) あなたに対して、ソフトウェアの複製や頒布または改変についての法的な許可を 与えるこの契約書を提示します。

また、各作者や私たちを保護するため、私たちはこのフリーソフトウェアには 何の保証も無いということを誰もが確実に理解するようにし、またソフトウェアが 誰か他人によって改変され、それが次々と頒布されていったとしても、その受領者は 彼らが手に入れたソフトウェアがオリジナルのバージョンでは無いこと、そして 原作者の名声は他人によって持ち込まれた可能性のある問題によって影響される ことがないということを周知させたいと思います。

最後に、ソフトウェア特許がいかなるフリーのプログラムの存在にも不断の脅威を 投げかけていますが、私たちは、フリーなプログラムの再頒布者が個々に特許 ライセンスを取得することによって、事実上プログラムを独占的にしてしまうという 危険を避けたいと思います。こういった事態を予防するため、私たちはいかなる特許も 誰もが自由に利用できるようライセンスされるか、全くライセンスされないかの どちらかでなければならないことを明確にしました。

(訳注: 本契約書で「独占的(proprietary)」とは、ソフトウェアの利用や再頒布、改変が禁止されているか、許可を得ることが必要とされているか、あるいは厳しい 制限が課されている自由にならずにすることが事実上できなくなっている状態のことを指す。詳しくは <http://www.gnu.org/philosophy/categories.ja.html#ProprietarySoftware> [<http://www.gnu.org/philosophy/categories.ja.html#ProprietarySoftware>] を参照せよ。)

複製や頒布、改変についての正確な条件と制約を以下で述べていきます。

複製、頒布、改変に関する条件と制約

0. この利用許諾契約書は、そのプログラム(またはその他の著作物)を この一般公衆利用許諾契約書の定める条件の下で頒布できる、という告知が 著作権者によって記載されたプログラムまたはその他の著作物全般に適用される。以下では、「プログラム」とはそのようにしてこの契約書が適用され プログラムや著作物全般を意味し、また「プログラムを基にした著作物」とは「プログラム」やその他の著作権法の下で派生物と見なされるもの 全般を指す。すなわち、「プログラム」かその一部を、全く同一の ままか、改変を加えたか、あるいは他の言語に翻訳された形で含む

著作物のことである(「改変」という語の本来の意味からはずれるが、以下では 翻訳も改変の一種と見なす)。それぞれの契約者は「あなた」と表現される。

複製や頒布、改変以外の活動はこの契約書ではカバーされない。それらはこの契約書の 対象外である。「プログラム」を実行する行為自体に制限はない。また、そのような「プログラム」の出力結果は、その内容が「プログラム」を基にした著作物を構成する場合のみ この契約書によって保護される(「プログラム」を実行したことによって 作成されたということは無関係である)。このような線引きの妥当性は、「プログラム」が何を
するのかに依存する。

1. それぞれの複製物において適切な著作権表示と保証の否認声明(disclaimer of warranty) を目立つよう適切に掲載し、またこの契約書および一切の保証の不在に触れた 告知すべてをそのまま残し、そしてこの契約書の複製物を「プログラム」のいかなる受領者にも「プログラム」と共に頒布する限り、あなたは「プログラム」のソースコードの複製物を、あなたが受け取った通りの形で複製または頒布することができる。媒体は問わない。

あなたは、物理的に複製物を譲渡するという行為に関して手数料を課しても良いし、希望によっては手数料を取って交換における保護の保証を提供しても良い。

2. あなたは自分の「プログラム」の複製物かその一部を改変して「プログラム」を基にした著作物を形成し、そのような改変点や 著作物を上記第1節の定める条件の下で複製または頒布することができる。ただし、そのためには以下の条件すべてを満たしていなければならない:

a) あなたがそれらのファイルを変更したということと変更した日時が良く 分かるよう、改変されたファイルに告示しなければならない。

b) 「プログラム」またはその一部を含む著作物、あるいは「プログラム」かその一部から派生した著作物を頒布あるいは 発表する場合には、その全体をこの契約書の条件に従って第三者へ無償で 利用許諾しなければならない。

c) 改変されたプログラムが、通常実行する際に対話的にコマンドを読むようになっているならば、そのプログラムを最も一般的な方法で対話的に実行する際、適切な著作権表示、無保証であること(あるいはあなたが保証を提供するということ)、ユーザがプログラムをこの契約書で述べた条件の下で頒布することができる、ということ、そしてこの契約書の複製物を閲覧するにはどうしたらよいかというユーザへの説明を含む告知が印刷されるか、あるいは画面に表示される ようにしなければならない(例外として、「プログラム」そのものは対話的であっても通常そのような告知を印刷しない場合には、「プログラム」を基にしたあなたの著作物に そのような告知を 印刷させる必要はない)。

以上の必要条件是全体としての改変された著作物に適用される。著作物の一部が「プログラム」から派生したのではないと確認でき、それら自身 別の独立した著作物であると合理的に考えられるならば、あなたがそれらを別の 著作物として分けて頒布する場合、そういった部分にはこの契約書とその条件は 適用されない。しかし、あなたが同じ部分を「プログラム」を基にした 著作物全体の一部として頒布するならば、全体としての頒布物は、この契約書が 課す条件に従わなければならない、というのは、この契約書が他の契約者に与える 許可は「プログラム」丸ごと全体に及び、誰が書いたかは関係なく各部分のすべてを保護するからである。

よって、すべてあなたによって書かれた著作物に対し、権利を主張したりあなたの 権利に異議を申し立てることはこの節の意図するところではない。むしろ、その趣旨は「プログラム」を基にした派生物ないし集合著作物の 頒布を管理する権利を行使することにある。

また、「プログラム」を基にしていないその他の著作物を「プログラム」(あるいは「プログラム」を基にした著作物)と一緒に集めただけのものを一巻の保管装置ないし頒布媒体に収めても、その他の 著作物までこの契約書が保護する対象になるということにはならない。

3. あなたは上記第1節および2節の条件に従い、「プログラム」(あるいは 第2節における派生物)をオブジェクトコードないし実行形式で複製または頒布 することができる。ただし、その場合あなたは以下のうちどれか一つを実施 しなければならない:

a) 著作物に、『プログラム』に対応した完全かつ機械で読み取り可能な ソースコードを添付する。ただし、ソースコードは上記第1節および2節の条件に従いソフトウェアの交換で習慣的に使われる媒体で頒布しなければならない。あるいは、

b) 著作物に、いかなる第三者に対しても、『プログラム』に対応した完全かつ 機械で読み取り可能なソースコードを、頒布に要する物理的コストを上回らない 程度の手数料と引き換えに提供する旨述べた少なくとも3年間は有効な書面 になった申し出を添える。ただし、ソースコードは上記第1節および2節の条件に 従いソフトウェアの交換で習慣的に使われる媒体で頒布しなければならない。あるいは、

c) 対応するソースコード頒布の申し出に際して、あなたが得た情報を一緒に引き渡す (この選択肢は、営利を目的としない頒布であって、かつあなたが上記小節bで 指定されているような申し出と共にオブジェクトコードあるいは実行形式の プログラムしか入手していない場合に限り許可される)。

著作物のソースコードとは、それに対して改変を加える上で好ましいとされる 著作物の形式を意味する。ある実行形式の著作物にとって完全なソースコードとは、それが含むモジュールすべてのソースコード全部に加え、関連するインターフェース 定義ファイルのすべてとライブラリのコンパイルやインストールを制御するために 使われるスクリプトをも加えたものを意味する。しかし特別な例外として、そのコンポーネント自体が実行形式に付随するのでは無い限り、頒布されるものの 中に、実行形式が実行されるオペレーティングシステムの主要なコンポーネント (コンパイラやカーネル等)と通常一緒に(ソースかバイナリ形式のどちらかで) 頒布されるものを含んでいる必要はないとする。

実行形式またはオブジェクトコードの頒布が、指定された場所からコピーするための アクセス手段を提供することで為されるとして、その上でソースコードも同等の アクセス手段によって同じ場所からコピーできるようになっているならば、第三者が オブジェクトコードと一緒にソースも強制的にコピーさせられるようになって いくこともソースコード頒布の条件を満たしているものとする。

4. あなたは「プログラム」を、この契約書において明確に提示された 行為を除き複製や改変、サブライセンス、あるいは頒布してはならない。他に「プログラム」を複製や改変、サブライセンス、あるいは頒布する 企てはすべて無効であり、この契約書の下でのあなたの権利を自動的に終結させる ことになろう。しかし、複製物や権利をこの契約書に従ってあなたから得た人々に 関しては、そのような人々がこの契約書に完全に従っている限り彼らのライセンスまで 終結することはない。

5. あなたはこの契約書を受諾する必要は無い。というのは、あなたはこれに署名して いないからである。しかし、この契約書以外にあなたに対して「プログラム」やその派生物を改変または頒布する許可を与えるものは 存在しない。これらの行為は、あなたがこの契約書を受け入れない限り

法によって 禁じられている。そこで、「プログラム」(あるいは「プログラム」を基にした著作物全般)を改変しない頒布することにより、あなたは自分がそのような行為を行うためにこの契約書を受諾したということ、そして「プログラム」とそれに基づく著作物の複製や頒布、改変について この契約書が課す制約と条件をすべて受け入れたということを示したものと見なす。

6. あなたが「プログラム」(または「プログラム」を基にした著作物全般)を再頒布するたびに、その受領者は元々のライセンス許可者から、この契約書で指定された条件と制約の下で「プログラム」を複製や頒布、あるいは改変する許可を自動的に得るものとする。あなたは、受領者がここで認められた権利を行使することに関してこれ以上他のいかなる制限も課してはならない。あなたには、第三者がこの契約書に従うことを強制する責任はない。

7. 特許侵害あるいはその他の理由(特許関係に限らない)から、裁判所の判決あるいは 申し立ての結果としてあなたに(裁判所命令や契約などにより)このライセンスの 条件と矛盾する制約が課された場合でも、あなたがこの契約書の条件を免除される わけではない。もしこの契約書の下であなたに課せられた責任と他の関連する責任を 同時に満たすような形で頒布できないならば、結果としてあなたは「プログラム」を頒布することが全くてできないことである。例えば特許ライセンスが、あなたから直接間接を問わずコピーを受け取った人が 誰でも「プログラム」を使用 料無料で再頒布することを認めていない場合、あなたがその制約とこの契約書を両方とも満たすには「プログラム」の頒布を完全に中止するしかないだろう。

この節の一部分が特定の状況の下で無効ないし実施不可能な場合でも、節の残りの 部分は適用されるよう意図されている。その他の状況では 節が全体として適用されるよう 意図されている。

特許やその他の財産権を侵害したり、そのような権利の主張の効力に異議を唱えたり するようあなたを誘惑することがこの節の目的ではない。この節には、人々によって ライセンス慣行として実現されてきた、フリーソフトウェア頒布のシステムの完全性を 護るという目的しかない。多くの人々が、フリーソフトウェアの頒布システムが首尾一貫して適用されているという信頼に基づき、このシステムを通じて頒布される多様な ソフトウェアに 寛大な貢献をしてきたのは事実であるが、人がどのようなシステム を通じてソフトウェアを頒布したいと思うかはあくまでも作者/寄与者次第であり、あなたが選択を押しつけることはできない。

この節は、この契約書のこの節以外の部分の一帰結になると考えられるケースを 徹底的に明らかにすることを目的としている。

8. 「プログラム」の頒布や利用が、ある国においては特許または著作権が 主張されたインターフェースのいずれかによって制限されている場合、「プログラム」にこの契約書を適用した元の著作権者は、そういった 国々を排除した明確な地理的頒布制限を加え、そこで排除されていない国の中や それらの国々の間でのみ頒布が許可されるようにしても構わない。その場合、そのような制限はこの契約書本文で書かれているのと同様に 見なされる。

9. フリーソフトウェア財団は、時によって改訂または新版の一般公衆利用許諾書を 発表することができる。そのような新版は現在のバージョンとその精神においては 似たものになるだろうが、新たな問題や懸念を解決するため細部では異なる可能性がある。

それぞれのバージョンには、見分けが付くようにバージョン番号が振られている。「プログラム」においてそれに適用されるこの契約書のバージョン番号が 指定されていて、更に「それ以降のいかなるバージョン(any later version)」も適用して 良いとなっていた場合、あなたは従う条件と制約として、指定のバージョンが、フリーソフトウェア財団によって発行された指定のバージョン以降の版のどれか一つの どちらかを選ぶことが出来る。「プログラム」でライセンスのバージョン番号が 指定されていないならば、あなたは今までにフリーソフトウェア財団から発行された バージョンの中から好きに選んで構わない。

10. もしあなたが「プログラム」の一部を、その頒布条件がこの契約書と 異なる他のフリーなプログラムと統合したいならば、作者に連絡して許可を求めよ。フリーソフトウェア財団が著作権を保有するソフトウェアについては、フリーソフトウェア財団に連絡せよ。私たちは、このような場合のために特別な例外を 設けることもある。私たちが決定を下すにあたっては、私たちのフリーソフトウェアの 派生物すべてがフリーな状態に保たれるということと、一般的にソフトウェアの共有と 再利用を促進するという二つの目標を規準に検討されるであろう。

無保証について

11. 「プログラム」は代価無しに利用が許可されるので、適切な法が 認める限りにおいて、「プログラム」に関するいかなる保証も 存在しない。書面で別に述べる場合を除いて、著作権者、またはその他の団体は、「プログラム」を、表明されたか言外にかかわらず、商業的適性を保証する ほどのめかしやある特定の目的への適合性(に限られない)を含む一切の 保証無しに「あるがまま」で提供する。「プログラム」の質と性能に関する リスクのすべてはあなたに帰属する。「プログラム」に欠陥があると判明した場合、あなたは必要な保守点検や補修、修正に要する コストのすべてを引き受けることにする。

12. 適切な法が書面での同意によって命ぜられない限り、著作権者、または上記で 許可されている通りに「プログラム」を改変または再頒布した その他の団体は、あなたに対して「プログラム」の利用ないし 利用不能で生じた通常損害や特別損害、偶発損害、間接損害(データの消失や 不正確な処理、あなたが第三者が被った損失、あるいは「プログラム」が他のソフトウェアと一緒に動作しないという不具合などを含むがそれらに限らない)に一切の責任を負わない。そのような損害が生ずる可能性について彼らが忠告 されていたとしても同様である。

条件と制約終わり

以上の条項をあなたの新しいプログラムに適用する方法

あなたが新しいプログラムを開発したとして、公衆によってそれが利用される 可能性を最大にしたいなら、そのプログラムをこの契約書の条項に従って誰でも 再頒布あるいは変更できるようフリーソフトウェアにするのが最善です。

そのためには、プログラムに以下のような表示を添付してください。その場合、保証が排除されているということを最も効果的に伝えるために、それぞれの ソースファイルの冒頭に表示を添付すれば最も安全です。少なくとも、「著作権表示」という行と全文がある場所へのポインタだけは 各ファイルに含めて置いてください。

one line to give the program's name and an idea of what it does.
Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

(訳)

プログラムの名前と、それが何をするかについての簡単な説明。Copyright (C) 西暦年 作者の名前

このプログラムはフリーソフトウェアです。あなたはこれを、
フリーソフトウェア財団によって発行された GNU 一般公衆利用許諾契約書
(バージョン2か、希望によってはそれ以降のバージョンのうちどれか)の
定める条件の下で再頒布または改変することができます。

このプログラムは有用であることを願って頒布されますが、*全くの無保証*
です。商業可能性の保証や特定の目的への適合性は、言外に示されたものも
含め全く存在しません。詳しくはGNU 一般公衆利用許諾契約書をご覧ください。

あなたはこのプログラムと共に、GNU 一般公衆利用許諾契約書の複製物を一部
受け取ったはずですが、もし受け取っていない場合は、フリーソフトウェア財団
まで請求してください(宛先は the Free Software Foundation, Inc., 59
Temple Place, Suite 330, Boston, MA 02111-1307 USA)。

電子ないし紙のメールであなたに問い合わせる方法についての情報も書き加えましょう。

プログラムが対話的なものならば、対話モードで起動した際に出力として 以下のような短い告知が表示されるようにしてください:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w'. This is free software, and you are welcome
to redistribute it under certain conditions; type `show c'
for details.

(訳)

Gnomovision バージョン 69, Copyright (C) 西暦年 作者の名前
Gnomovision は*全くの無保証*で提供されます。詳しくは
`show w' とタイプして下さい。
これはフリーソフトウェアであり、ある条件の下で再頒布することが
奨励されています。詳しくは `show c' とタイプして下さい。

ここで、仮想的なコマンド `show w' と `show c' は 一般公衆利用許諾契約書の適切な部分を表示するようになっていなければなりません。
もちろん、あなたが使うコマンドを `show w' や `show c' と呼ぶ必然性はありませんので、あなたのプログラムに 合わせてマウスのクリックやメ
ニューのアイテムにしても結構です。

また、あなたは、必要ならば(プログラマーとして働いていたら)あなたの 雇用主、あるいは場合によっては学校から、そのプログラムに関する「著作権放棄声明(copyright disclaimer)」に署名してもらうべきです。以下は例ですので、名前を変えてください:

```
Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.
```

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

(訳)

Yoyodyne社はここに、James Hackerによって書かれた
プログラム `Gnomovision' (コンパイラへ通すプログラム)
に関する一切の著作権の利益を放棄します。

Ty Coon氏の署名、1989年4月1日
Ty Coon、副社長

この一般公衆利用許諾契約書では、あなたのプログラムを独占的なプログラムに 統合することを認めていません。あなたのプログラムがサブルーチンライブラリ ならば、独占的なアプリケーションとあなたのライブラリをリンクすることを 許可したほうがより便利であると考えられるかもしれません。もしこれがあなたの 望むことならば、この契約書の代わりに GNU ライブラリー一般公衆利用許諾契約書 [<http://www.fsf.org/licenses/lgpl.html>] を適用してください。

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA.
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member

of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties; any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and

legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O.Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the

aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

GNU フリー文書利用許諾契約書

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA この利用許諾契約書を、一字一句そのままに複製し頒布することは許可する。しかし変更は認めない。

This is an unofficial translation of the GNU Free Documentation License into Japanese. It was not published by the Free Software Foundation, and does not legally state the distribution terms for documents that uses the GNU FDL--only the original English text of the GNU FDL does that. However, we hope that this translation will help Japanese speakers understand the GNU FDL better.

(訳: 以下はGNU Free Documentation Licenseの非公式な日本語訳です。これはフリーソフトウェア財団 (the Free Software Foundation)によって発表されたものではなく、GNU FDLを適用した文書の頒布条件を法的に有効な形で述べたものではありません。頒布条件としてはGNU FDLの英語版テキストで指定されているもののみが有効です。しかしながら、私たちはこの翻訳が、日本語を使用する人々にとってGNU FDLをより良く理解する助けとなることを望んでいます。)

0. はじめに

この利用許諾契約書の目的は、この契約書が適用されるマニュアルや教科書、その他機能本位で実用的な文書を(無料ではなく)自由という意味で「フリー」とすること、すなわち、改変の有無あるいは目的の営利非営利を問わず、文書を複製し再頒布する自由をすべての人々に効果的に保証することです。加えてこの契約書により、著者や出版者が自分たちの著作物に対して相応の敬意と賞賛を得る手段も保護されます。また、他人が行った改変に対して責任を負わずに済むようになります。

この利用許諾契約書は「コピーレフト」的なライセンスの一つであり、この契約書が適用された文書から派生した著作物は、それ自身もまた原本と同じ意味でフリーでなければなりません。この契約書は、フリーソフトウェアのために設計されたコピーレフトなライセンスであるGNU一般公衆利用許諾契約書を補足するものです。

(訳注: コピーレフト(copyleft)の概念については <http://www.gnu.org/copyleft/copyleft.ja.html> を参照せよ)

この利用許諾契約書は、フリーソフトウェア用のマニュアルに適用することを目的として書かれました。フリーソフトウェアはフリーな文書を必要としており、フリーなプログラムはそのソフトウェアが保証するのと同じ自由を提供するマニュアルと共に頒布されるべきだからです。しかし、この契約書の適用範囲はソフトウェアのマニュアルに留まりません。対象となる著作物において扱われる主題が何であれ、あるいはそれが印刷された書籍として出版されるか否かに関わらず、この契約書は文字で書かれたいかなる著作物にも適用することが可能です。私たちとしては、主にこの契約書を解説や参照を目的とする著作物に適用することをお勧めします。

1. この利用許諾契約書の適用範囲と用語の定義

著作物がこの利用許諾契約書の定める条件の下で頒布される旨の告知を、著作権者がその中に書いたすべてのマニュアルあるいはその他の著作物は、いかなる媒体上にあってもこの契約書の適用対象となる。そのような告知を置くことで、全世界において、著作権使用料を必要とせず、許可の存続期間を限定されること無く、この契約書の中で述べられている条件の下で当該著作物を利用できるという許可を与えることとする。以下において、「『文書』(Document)」とはそのような告知が記載されたマニュアルないし著作物すべてを指す。公衆の一員ならば誰でも契約の当事者となることができ、この契約書中では「あなた」と表現される。あなたは、著作権法の下で許可を必要とするような方法で著作物を複製や改変、あるいは頒布することにより、この契約書を受諾することになる。

『文書』の「改変版 (Modified Version)」とは、一字一句忠実に複製したが、あるいは改変や他言語への翻訳を行ったかどうかに関わらず、その『文書』の全体あるいは一部分を含む著作物すべてを意味する。

「補遺部分 (Secondary Section)」とは、『文書』中でその旨指定された補遺ないし本文に先だって前付けとして置かれる一部分であり、『文書』の出版者あるいは著者と、『文書』全体の主題 (あるいはそれに関連する事柄)との関係のみを論じ、全体としての主題の範疇に直接属する内容を

全く含まないものである (たとえば、『文書』の一部が数学の教科書だった場合、補遺部分では数学について何も解説してはならない)。補遺部分で扱われる関係は、その主題あるいは関連する事柄との歴史的なつながりのことかも知れないし、それらに関する法的、商業的、哲学的、倫理的、あるいは政治的立場についてかも知れない。

「変更不可部分 (Invariant Sections)」とは補遺部分の一種で、それらが変更不可部分であることが、『文書』をこの利用許諾契約書の下で発表する旨述べた告知中においてその部分の題名と共に明示されているものである。ある部分が上記のような「補遺」性の定義にそぐわない場合は、その部分を「変更不可」として指定することは認められない。『文書』は、変更不可部分を全く含まなくても良い。『文書』において変更不可部分が全く指定されていないければ、その『文書』に変更不可部分は存在しないということである。

「カバーテキスト (Cover Texts)」とは、『文書』がこの利用許諾契約書の指定する条件の下で発表される旨述べた告知において、「表カバーテキスト」あるいは「裏カバーテキスト」として列挙された短い文章のことを指す。表カバーテキストは最大で5語、裏カバーテキストは最大で25語までとする。

『文書』の「透過的」複製物とは、機械による読み取りが可能な『文書』の複製物のことを指す。透過的な複製物の文書形式は、その仕様が一般の人々に入手可能で、『文書』の内容を一般的なテキストエディタ、または(画素で構成される画像ならば)一般的なペイントプログラム、あるいは(図面ならば)いくつかの広く入手可能な製図エディタで簡単に改訂するのに適しており、なおかつテキストフォーマットへの入力に適する(あるいはテキストフォーマットへの入力に適する諸形式への自動的な変換に適する)ものでなければならない。透過的なファイル形式への複製であっても、マークアップ、あるいはマークアップの不在が読者によるそれ以降の改変をわざと邪魔し阻害するように仕組まれたものは透過的であるとは見做されない。ある画像形式が、相当量のテキスト文章を表現するために使われた場合、それは透過的ではない。透過的ではない複製は「非透過的」複製と呼ばれる。

透過的複製に適した形式の例としては、マークアップを含まないプレーンな ASCII 形式、Texinfo 入力形式、LaTeX 入力形式、一般に入手可能な DTD を用いた SGML あるいは XML、または人間による改変を想定して設計された、標準に準拠したシンプルなもの HTML や PostScript、PDF などが挙げられる。透過的な画像形式の例には、PNG や XCF、JPG が含まれる。非透過な形式としては、独占的なワードプロセッサでのみ閲覧編集できる独占的なファイル形式、普通には入手できない DTD または処理系を使った SGML や XML、ある種のワードプロセッサが生成する、出力のみを目的とした機械生成の HTML や PostScript、PDF などが含まれる。

「題扉 (Title Page)」とは、印刷された書籍に於いては、実際の表紙自身のみならず、この利用許諾契約書が表紙に掲載することを義務づける文章や図などを、読みやすい形で載せるのに必要なだけの、表紙に引き続き数ページをも意味する。表紙に類するものが無い形式で発表される著作物においては、「題扉」とは本文の始まりに先だって、その著作物の題名が最も目立つ形で現れる場所の近くに置かれる文章のことを指す。

「XYZ」と題された (Entitled XYZ) 部分とは、『文書』において「XYZ」と名付けられた一部分であり、その題名は正確に「XYZ」であるか、「XYZ」を他の言語に翻訳した上でその後ろに「XYZ」をそのまま括弧で括ったものを含む記述のどちらかである(ここでの「XYZ」とは、この利用許諾契約書において以下で言及される特定の部分名を意味している。例えば「謝辞 (Acknowledgements)」、「献辞 (Dedications)」、「推薦の辞 (Endorsements)」、「履歴 (History)」)。あなたが『文書』を改変する場合、そのような部分の「題名を保存する (Preserve the Title)」とは、「XYZ」と題された」部分として、ここでの定義に従い題名を残すということである。

『文書』は、「保証否認警告 (Warranty Disclaimers)」を、この利用許諾契約書が『文書』に適用されると述べた告知の次に含んでも良い。この種の保証否認警告は、この契約書からの言及という形で利用条件に含まれるものと解されるが、保証の否認に関することについてののみ有効とする。こういった保証否認警告で示うその他のいかなる含意も無効であり、この契約書の効能には何ら影響を持たない。

2. 逐語的に忠実な複製

この利用許諾契約書、著作権表示、この契約書が『文書』に適用される旨述べた告知の三つがすべての複製物に複製され、かつあなたがこの契約書で指定されている以外のいかなる条件も追加しない限り、あなたはこの『文書』を、商用であるか否かを問わずいかなる形で複製頒布することができる。あなたは、あなたが作成あるいは頒布する複製物に対して、閲覧や再複製を技術的な手法によって妨害、規制してはならない。しかしながら、複製と引き換えに代価を得てもかまわない。あなたが相当量の複製物を頒布する際には、本契約書第3項で指定される条件にも従わなければならない。

またあなたは、上記と同じ条件の下で、複製物を貸与したり複製物を公に開示することができる。

3. 大量の複製

もしあなたが、『文書』の印刷された (あるいは通常は印刷された表紙を持つ媒体における)複製物を100部を超えて出版し、また『文書』の利用許諾告知がカバーテキストの掲載を要求している場合には、指定されたすべてのカバーテキストを、表カバーテキストは表表紙に、裏カバーテキストは裏表紙に、はっきりと読みやすい形で載せた表紙の中に複製物本体を綴じ込まなければならない。また、両方の表紙において、それらの複製物の出版者としてのあなたをはっきりとかつ読みやすい形で確認できなければならない。表表紙では『文書』の完全な題名を、題名を構成するすべての語が等しく目立つようにして、視認可能な形で示さなければならない。それらの情報に加えて、表紙に他の文章や図などを加えることは許可される。表紙のみを変更した複製物は、それが『文書』の題名を保存し上記の条件を満たす限り、ほかの点では逐語的に忠実な複製物として扱われる。

もしどちらかの表紙に要求されるカバーテキストの量が多すぎて読みやすく収めることが不可能ならば、あなたはテキスト先頭の一文(あるいは適切に収まるだけ)を実際の表紙に載せ、続きは隣接したページに載せるべきである。

あなたが『文書』の「非透過的」複製物を100部を超えて出版あるいは頒布する場合、それぞれの非透過な複製物と一緒に機械で読み取り可能な透過的複製物を添付するか、それぞれの非透過な複製物(あるいはそれに付属する文書)中で、公にアクセス可能なコンピュータネットワーク上の所在地を記述しなければならない。その場所には、非透過な複製物と内容的に寸分違わず、余計なものが追加されていない完全な『文書』の透過的複製物が置かれ、またそこから、ネットワークを利用する一般公衆が、一般に標準的と考えられるネットワークプロトコルを使ってダウンロードすることができなければならない。もしあなたが後者の選択肢を選ぶならば、その版の非透過な複製物を公衆に(直接、あるいはあなたの代理人ないし小売業者が)最後に頒布してから最低1年間は、その透過的複製物が指定の場所でアクセス可能であり続けることを保証するよう、非透過な複製物の大量頒布を始める際に十分に慎重な手順を踏まなければならない。

これは要望であり必要条件ではないが、『文書』の著者に、『文書』の更新された版をあなたに提供する機会を与えるため、透過非透過を問わず大量の複製物を再頒布し始める前には彼らにきちんと連絡しておいてほしい。

4. 改変

『文書』の改変版を、この利用許諾契約書と細部まで同一の契約の下で発表する限り、すなわち原本の役割を改変版で置き換えた形での頒布と改変を、その複製物を所有するすべての人々に許可する限り、あなたは改変版を上記第2項および第3項が指定する条件の下で複製および頒布することができる。さらに、あなたは改変版において以下のことを行わなければならない。

- A. 題扉に(もしあればその他の表紙にも)、『文書』および『文書』のそれ以前の版と見分けがつく題名を載せること(もし以前の 版があれば、『文書』の「履歴 (History)」の部分に列記されているはずで ある)。もし元の版の出版者から許可を得たならば、以前の版と同じ題名を使ってもいい。
- B. 題扉に、改変版における改変を行った1人以上の人物 が団体名を列記すること。あわせて元の『文書』の著者として、最低5人(もし5人以下ならばすべて)の主要著者を列記すること。ただし元の著者たちが この条件を免除した場合は除く。
- C. 題扉に、改変版の出版者名を出版者として記載すること。
- D. 『文書』にあるすべての著作権表示を残すこと。
- E. 他の著作権表示の近くに、あなたの改変に対する適 当な著作権表示を追加すること。
- F. 著作権表示のすぐ後に、改変版をこの契約書の条件 の下で利用することを公衆に対して許可する告知を含めること。その形式は この契約書の末尾にある付記で示されている。
- G. 元の『文書』の利用許諾告知に書かれた、変更不可 部分の完全な一覧と、要求されるカパーテキストとを、改変版の利用許諾告知 中でもそのまま残すこと。
- H. この契約書の、変更されていない複製物を含めること。
- I. 「履歴 (History)」と題された部分とその題名を保存し、そこに改変版の、少なくとも題名、出版年、新しく変更した部分の著 者名、出版者名を、題扉に掲載するのと同じように記載した一項を加えること。もし『文書』中に「履歴」と題された部分が存在しない場合には、『文 書』の題名、出版年、著者、出版者を題扉に掲載するのと同じように記載した部分を用意し、上記で述べたような、改変版を説明する一項を加えること。
- J. 『文書』中に、『文書』の透過的複製物への公共的 アクセスのために指定されたネットワークの所在地が記載されていたならば、それを保存すること。同様に、その『文書』の元になった以前の版で指定 されていたネットワークの所在地も載っていたならば、それも保存すること。これらの情報は「履歴(History)」の部分に置いてもいい。ただし、それが『文書』自身より少なくとも4年前に出版された著作物の情報であったり、あるいは改変版が参考としている版の元々の出版者から許可を得たならば、その情報を削除してもかまわない。
- K. 「謝辞 (Acknowledgement)」あるいは「献辞 (Dedication)」等と題されたいかなる部分も、その部分の題名を保存し、そ の部分の内容(各貢献者への謝意あるいは献呈の意)と語調を保存すること。
- L. 『文書』の変更不可部分を、その本文および題名を 変更せずに保存すること。章番号やそれに相当するものは部分の題名の一 部とは見做さない。
- M. 「推薦の辞 (Endorsement)」というような章名が題 された部分はすべて削除すること。そのような部分を改変版に含めてはならない。
- N. すでに存在する部分を「推薦の辞 (Endorsement)」と題されるように改名したり、題名の点で変更不可部分のどれかと衝突する ように改名してはならない。
- O. 保証否認警告を保存すること。

もし改変版に、補遺部分としての条件を満たし、かつ『文書』から複製物された文章や図などをいっさい含んでいない、前書き的な章あるいは付録が新しく含まれるならば、あなたは希望によりそれらの部分の一部あるいはすべてを変更不可と宣言することができる。変更不可を宣言するためには、それらの部分の題名を改変版の利用許諾告知中の変更不可部分一覧に追加すれば良い。これらの題名は他の章名とは全く別のものでなければならない。

含まれる内容が、さまざまな集団によるあなたの改変版に対する推薦の辞のみである限り、あなたは、「推薦の辞 (Endorsement)」と題された章を追加することができる。推薦の辞の例としては、ピアレビューの陳述、あるいは文書がある標準の権威ある定義としてその団体に承認されたという声明などがある。

あなたは、5語までの一文を表カパーテキストとして、25語までの文を表表紙テキストとして、改変版のカバーテキスト一覧の末尾に加えることができる。一個人ないし一団体が直接(あるいは団体内で結ばれた協定によって)加えることができるのは、表カパーテキストおよび裏カパーテキストとしてそれぞれ一文ずつのみである。もし以前すでにその文書において、表裏いずれかの表紙にあなたの(またはあなたが代表する同じ団体内で為された協定に基づく)カパーテキストが含まれていたならば、あなたが新たに追加することはできない。しかしあなたは、その古い文を加えた以前の出版者から明示的な許可を得たならば、古い文を置き換えることができる。

『文書』の著者あるいは出版者は、この利用許諾契約書によって、彼らの名前を利用することを許可しているわけではない。彼らの名前を改変版の宣伝に使ったり、改変版への明示的あるいは黙示的な保証のために使うことを許可するものではない。

5. 文書の結合

あなたは、上記第4項において改変版に関して定義された条件の下で、この利用許諾契約書の下で発表された複数の文書の一つにまとめることができる。その際、原本となる文書にある変更不可部分を全て、改変せずに結合後の著作物中に含め、それらをあなたが統合した著作物の変更不可部分としてその利用許諾告知において列記し、かつ原本にある全ての保証否認警告を保存しなければならない。

結合後の著作物についてはこの契約書の複製物一つ含んでいれよく、同一内容の変更不可部分が複数ある場合には一つで代用してよい。もし同じ題名だが内容の異なる変更不可部分が複数あるならば、そのような部分のそれぞれの題名の最後に、(もし分かっているならば)その部分の原著者あるいは出版者の名前で、あるいは他と重ならないような番号を括弧で括って記載することで、それぞれ見分けが付くようにしなければならない。結合後の著作物の利用許諾告知における変更不可部分の一覧においても、章の題名に同様の調整をすること。

結合後の著作物においては、あなたはそれぞれの原本の「履歴 (History)」と題されたあらゆる部分をまとめて、「履歴 (History)」と題された一章にしなければならない。同様に、「謝辞 (Acknowledgements)」あるいは「献辞 (Dedications)」と題されたあらゆる部分もまとめなければならない。あなたは「推薦の辞 (Endorsements)」と題されたあらゆる部分も削除しなければならない。

6. 文書の収集

あなたは、この利用許諾契約書の下で発表された複数の文書で構成される収集著作物を作ることができる。その場合、それぞれの文書が逐語的に忠実に複製されることを保障するために他のすべての点でこの契約書の定める条件に従う限り、さまざまな文書中のこの契約書の個々の複製物を、収集著作物中に複製物一つ含めることで代用することができる。

あなたは、このような収集著作物から文書一つ取り出し、それをこの契約書の下で頒布することができる。ただしその際には、この契約書の複製物を抽出された文書に挿入し、またその他のすべての点でこの文書の逐語的に忠実な複製に関してこの契約書が定める条件に従わなければならない。

7. 独立した著作物の集積

『文書』あるいはその派生物を、他の別の独立した文書あるいは著作物と一緒にし、一巻の記憶装置あるいは頒布媒体に収めた編集著作物は、編集に起因する著作権が編集著作物に含まれる個々の著作物がその利用者に許可した法的権利を制限するよう行使されない限り、「集積」著作物と呼ばれる。『文書』が集積著作物に含まれる場合、この契約書は、『文書』と共にまとめられた他の独立した著作物には、それら自身が『文書』の派生物で無い限り適用されることにはならない。

このような『文書』の複製物において、この利用許諾契約書の第3項によりカバーテキストの掲載が要求されている場合、『文書』の量が集積著作物全体の2分の1以下であれば、『文書』のカバーテキストは集積著作物中で『文書』そのものの周りを囲む中表紙、あるいは『文書』が電子的形式である場合には表紙の電子的等価物にのみ配置するだけでよい。その場合以外は、カバーテキストは集積著作物全体を取り巻く印刷された表紙に掲載されなければならない。

8. 翻訳

翻訳は改変の一種と見做すので、あなたは『文書』の翻訳をこの利用許諾契約書の第4項の定める条件の下で頒布することができる。変更不可部分を翻訳によって置き換えるには著作権者の特別許可を必要とするが、元の変更不可部分に追加する形で変更不可部分の全てないし一部の翻訳を含めることはかまわない。この契約書や『文書』中の利用許諾告知、保証否認警告すべての英語原本も含める限り、あなたはこの契約書、告知、警告の翻訳を含めることができる。契約書や告知、警告に関して翻訳と英語原本との間に食い違いが生じた場合、英語原本が優先される。

典型的な例として、『文書』のある部分が原文で「Acknowledgements」、「Dedications」、あるいは「History」と題されていた場合、実際の題名を変更するには、題名を保存する(この契約書の第1項)ための条件(同第4項)を満たすことが必要となる。

9. 契約の終了

この利用許諾契約書の下で明確に提示されている場合を除き、あなたは『文書』を複製、改変、サブライセンス、あるいは頒布してはならない。このライセンスで指定されている以外の、『文書』の複製、改変、サブライセンス、頒布に関するすべての企ては無効であり、この契約書によって保証されるあなたの権利を自動的に終結させることとなる。しかし、この契約書の下であなたから複製物ないし諸権利を得た個人や団体に関しては、そういった人々がこの契約書に完全に従ったままである限り、彼らに与えられた許諾は終結しない。

10. 将来における本利用許諾契約書の改訂

フリーソフトウェア財団は、時によってGNU フリー文書利用許諾契約書の新しい改訂版を出版することができる。そのような新版は現在の版と理念においては似たものになるであろうが、新たに生じた問題や懸念を解決するため細部においては違ったものになるだろう。詳しくは <http://www.gnu.org/copyleft/> を参照せよ。

GNU フリー文書利用許諾契約書のそれぞれの版には、新旧の区別が付くようなバージョン番号が振られている。もし『文書』において、この契約書のある特定の版が「それ以降のどの版でも」適用して良いと指定されている場合、あなたはフリーソフトウェア財団から発行された(草稿として発表されたものを除く)指定の版かそれ以降の版のうちどれか一つを選び、その条項や条件に従うことができる。もし『文書』がこの契約書のバージョン番号を指定していない場合には、あなたはフリーソフトウェア財団から今までに出版された(草稿として発表されたものを除く)版のうちからどれか一つを選ぶことができる。

付録: この利用許諾契約書をあなたの文書に適用するには

Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.

(訳:

Copyright (C) 西暦年 あなたの名前。
この文書を、フリーソフトウェア財団発行の GNU フリー文書利用許諾契約書(バージョン1.2かそれ以降から一つを選択)が定める条件の下で複製、頒布、あるいは改変することを許可する。変更不可部分、表カバーテキスト、裏カバーテキストは存在しない。この利用許諾契約書の複製物は「GNU フリー文書利用許諾契約書」という章に含まれている。
)

もし変更不可部分や表カバーテキスト、裏カバーテキストがあれば、「変更不可部分…は存在しない。」というところを以下で置き換えてください:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

(訳:

(章の題名を列記)は変更不可部分であり、(表カバーテキストを列記)は表カバーテキスト、(裏カバーテキストを列記)は裏カバーテキストである。

)

変更不可部分はあるがカバーテキストは存在しないなど、その他の三者の組み合わせに関しては、状況に合わせて上記二つの選択肢を混ぜてください。

あなたの文書に、他に類を見ない独自のプログラムコードのサンプルが含まれる場合、フリーソフトウェアにおいてそのコードを利用することを許可するために、そういったサンプルに関してはこの利用許諾契約書と同時にGNU 一般公衆許諾契約書のようなフリーソフトウェア向けライセンスのうちどれか一つを選択して適用してもよい、というような条件の下で発表することを推奨します。

