SUSE Linux
リファレンス

www.novell.com

10.0 | 09/13/2005

リファレンス

List of Authors: Arndt Jörg [FAMILY Given], Behlert Stefan [FAMILY Given], Bodammer Frank [FAMILY Given], Branam James [FAMILY Given], Buzek Volker [FAMILY Given], Cihlarova Klara [FAMILY Given], Dirsch Stefan [FAMILY Given], Donjak Olaf [FAMILY Given], Drahtmüller Roman [FAMILY Given], Dubiel Thorsten [FAMILY Given], Duwe Torsten [FAMILY Given], Fehr Thomas [FAMILY Given], Fent Stefan [FAMILY Given], Fink Werner [FAMILY Given], Garloff Kurt [FAMILY Given], Gleißner Joachim [FAMILY Given], Groß Carsten [FAMILY Given], Grünbacher Andreas [FAMILY Given], Gunreben Berthold [FAMILY Given], Hassels Franz [FAMILY Given], Jaeger Andreas [FAMILY Given], Jaeger Jana [FAMILY Given], Kämpf Klaus [FAMILY Given], Kleen Andi [FAMILY Given], Mantel Hubert [FAMILY Given], Marowsky-Bree Lars [FAMILY Given], Mason Chris [FAMILY Given], Meixner Johannes [FAMILY Given], Müller Lars [FAMILY Given], Nagorni Matthias [FAMILY Given], Nashif Anas [FAMILY Given], Olschner Siegfried [FAMILY Given], Parzefall Edith [FAMILY Given], Pöml Peter [FAMILY Given], Renninger Thomas [FAMILY Given], Reinecke Hannes [FAMILY Given], Rölz Thomas [FAMILY Given], Rommel Heiko [FAMILY Given], Schäfer Marcus [FAMILY Given], Schraitle Thomas [FAMILY Given], Singvogel Klaus [FAMILY Given], Vogelsang Hendrik [FAMILY Given], Wagner Klaus G. [FAMILY Given], Walter Rebecca [FAMILY Given], Zoz Christian [FAMILY Given]

ご意見やご感想は、documentation@suse.deまでお寄せください。

Contents

このガイドについて

このマニュアルでは、SUSE Linuxの全体的な事柄を説明します。 対象となる読者は、システム管理者と、システム管理についての基本的な知識を持っているホームユーザです。 毎日の作業で必要となるいくつかのアプリケーションと、高度なインストールおよび設定シナリオの詳しい内容について説明します。

高度な導入シナリオ
: 複雑な環境にSUSE Linuxを導入する方法を説明します。

インターネット、マルチメディア、オフィス、グラフィックス
: ホームユーザが必要とする最も重要なアプリケーションについて説明します。

モバイル性
: SUSE Linuxでのモバイルコンピューティングと、ワイヤレスコンピューティング、電源管理、プロファイル管理のさまざまなオプションの設定方法について説明します。

管理
: SUSE Linuxをセキュアにする方法、ファイルシステムへのアクセスを制御する方法、Linux管理者にとって銃容易ないくつかのユーティリティについて説明します。

システム
: Linuxシステムのコンポーネントと、それら相互の働きの深い内容について説明します。

サービス
: SUSE Linuxに付属するさまざまなネットワークおよびファイルサービスの設定方法について説明します。

1 フィードバック

私たちは、このマニュアル、およびこの製品に含まれている他のドキュメントについての皆さんのコメントや提案をお聞きしたいと思っています。 どうか、オンラインドキュメントの各ページの下部にあるユーザコメント機能を

使うか、またはhttp://www.novell.com/documentation/feedback.htmlを訪問して、コメントを入力してください。

2 付加的なマニュアル

SUSE Linux製品には、以下のような他のマニュアルがあり、http://www.novell.com/documentation/で入手できます。または、インストール済みシステムの/usr/share/doc/manual/にあります。

起動
このガイドでは、SUSE Linuxの最初のステップについて説明します。このドキュメントのオンライン版はhttp://www.novell.com/documentation/suse10/にあります。

Novell AppArmor Powered by Immunix 1.2 Installation and QuickStart Guide
このガイドでは、*AppArmor*製品の最初のインストール手順について説明しています。このドキュメントのオンライン版はhttp://www.novell.com/documentation/apparmor/にあります。

Novell AppArmor Powered by Immunix 1.2 Administration Guide
このガイドでは、自分の環境で*AppArmor*を使用する方法についての詳しい点を説明しています。このドキュメントのオンライン版はhttp://www.novell.com/documentation/apparmor/にあります。

3 ドキュメントの規則

本書では、次の書体を使用しています。

- /etc/passwd：ファイル名およびディレクトリ名
- *プレースホルダ：placeholder*は、実際の値で置き換えられます。
- PATH：環境変数PATH
- ls、--help: コマンド、オプション、およびパラメータ

- `user`： ユーザまたはグループ
- <Alt>、Alt + F1: 押すためのキーまたはキーの組み合わせ
- ［*ファイル*］、*[ファイル] → [名前を付けて保存]*:メニュー項目、ボタン
- *Dancing Penguins* (Chapter Penguins、↑*リファレンス*): これは、他の本の章への参照です。

4 謝辞

Linuxの開発は、世界中で多数のLinux開発者がボランティアとして参加することにより、進められています。世界中のLinux開発者の貢献に感謝します。このディストリビューションは、このような人々の協力なしには存在し得ませんでした。加えて、Frank ZappaとPawarにも感謝します。当然のことですが、Linus Torvaldsにも深く感謝します。

大いに楽しんでください。

SUSEチームより

パート I. 高度な導入シナリオ

1 リモートインストール

SUSE Linuxは複数の方法でインストールすることができます。 SUSE Linuxをインストールするには、章 *YaSTによるインストール* (↑起動)で説明されている、通常のCDやDVDによるインストールの他に、ネットワークベースのさまざまなアプローチや、完全自動のアプローチも選択できます。

それぞれの方式は、2つの短いチェックリストで紹介されています。 1つはその方式の前提条件で、もう1つは基本的な手順の説明です。 その後、これらのインストールシナリオの中で用いられているすべての方式についての詳細を説明します。

注意

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

1.1 リモートインストールのインストールシナリオ

このセクションでは、リモートインストールを行う場合の、最も一般的なインストールシナリオについて説明します。 それぞれのシナリオについて、前提条件のリストを注意深くチェックし、シナリオで説明されている手順に従っ

てください。 特定のステップについての詳細な説明が必要な場合には、用意されているリンクを参照してください。

重要項目

X Window Systemの設定は、リモートインストールプロセスの一部ではありません。 インストールが完了したら、ターゲットシステムにルートとしてログインして、`init 3`を入力し、項35.1. 「SaX2によるX11の設定」 (page 567)で説明されているように、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。

1.1.1 VNCによる単純なリモートインストール—静的なネットワーク設定

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

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

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

- ターゲットシステムに割り当てる有効な静的IPアドレス

このタイプのインストールを実行するには、以下の手順に従います。

1. 項1.2.「インストールソースを保持するサーバのセットアップ」 (page 31)で説明されている方法でインストールソースをセットアップします。

2. SUSE Linux media kitの最初のCDまたはDVDを使って、ターゲットシステムをブートします。

3. ターゲットシステムのブート画面が表示されたら、ブートオプションプロンプトで、適切なVNCオプションと、インストールソースのアドレスを設定します。この詳細は、項1.4.「ターゲットシステムをインストールのためにブートする」 (page 52)で説明しています。

   ターゲットシステムはテキストベースの環境でブートします。VNCビューアアプリケーションまたはブラウザで使用するための、グラフィックインストール環境用のネットワークアドレスとディスプレイ番号が表示されます。 VNCインストールのアナウンス自体はOpenSLPによって行われ、Konquerorの`service:`//または`slp:`//モードで表示できます。

4. 制御用のワークステーションで、VNC表示アプリケーションまたはWebブラウザを開き、項1.5.1.「VNCによるインストール」 (page 57)に説明されている方法でターゲットシステムに接続します。

5. 章 *YaSTによるインストール* (↑起動)に説明されている方法でインストールを実行します。

   インストールの最後の部分のためにターゲットシステムがリブートしたら、もう一度接続する必要があります。

6. インストールを完了します。

1.1.2 VNCによる単純なリモートインストール—DHCPによる動的なネットワーク設定

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

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

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

このタイプのインストールを実行するには、以下の手順に従います。

1. 項1.2.「インストールソースを保持するサーバのセットアップ」 (page 31)で説明されている方法でインストールソースをセットアップします。 NFS、HTTP、またはFTPのネットワークサーバを選択します。 SMBのインストールソースの場合は、項1.2.5.「SMBインストールソースの管理」 (page 40)を参照してください。
2. SUSE Linux media kitの最初のCDまたはDVDを使って、ターゲットシステムをブートします。

3 ターゲットシステムのブート画面が表示されたら、ブートオプションプロンプトで、適切なVNCオプションと、インストールソースのアドレスを設定します。 この詳細は、項1.4.「ターゲットシステムをインストールのためにブートする」 (page 52)で説明しています。

ターゲットシステムはテキストベースの環境でブートします。VNCビューアアプリケーションまたはブラウザで使用するための、グラフィックインストール環境用のネットワークアドレスとディスプレイ番号が表示されます。 VNCインストールのアナウンス自体はOpenSLPによって行われ、Konquerorの`service:`//または`slp:`//モードで表示できます。

4 制御用のワークステーションで、VNC表示アプリケーションまたはWebブラウザを開き、項1.5.1.「VNCによるインストール」 (page 57)に説明されている方法でターゲットシステムに接続します。

5 章 *YaSTによるインストール* (↑起動)に説明されている方法でインストールを実行します。

インストールの最後の部分のためにターゲットシステムがリブートしたら、もう一度接続する必要があります。

6 インストールを完了します。

1.1.3 VNCによるリモートインストール—PXEブートとWake on LAN

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

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

- リモートのインストールソース: ネットワーク接続が動作するNFS、HTTP、FTP、またはSMB
- TFTPサーバ

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

このタイプのインストールを実行するには、以下の手順に従います。

1. 項1.2.「インストールソースを保持するサーバのセットアップ」(page 31)で説明されている方法でインストールソースをセットアップします。NFS、HTTP、またはFTPのネットワークサーバを選択するか、項1.2.5.「SMBインストールソースの管理」(page 40)で説明されている方法でSMBのインストールソースを設定します。
2. ターゲットシステムから取得するためのブートイメージを保持するTFTPサーバをセットアップします。これは項1.3.2.「TFTPサーバのセットアップ」(page 43)で説明されています。
3. すべてのマシンにIPアドレスを提供し、ターゲットシステムにTFTPサーバの場所を知らせるためのDHCPサーバをセットアップします。これは項1.3.1.「DHCPサーバのセットアップ」(page 42)で説明されています。
4. ターゲットシステムでPXEブートの準備をします。この詳細は、項1.3.5.「ターゲットシステムでPXEブートの準備をする」(page 50)で説明しています。
5. Wake on LAN機能を使って、ターゲットシステムでブートプロセスを開始します。これは項1.3.7.「Wake on LAN」(page 51)で説明されています。
6. 制御用のワークステーションで、VNC表示アプリケーションまたはWebブラウザを開き、項1.5.1.「VNCによるインストール」(page 57)に説明されている方法でターゲットシステムに接続します。
7. 章 *YaSTによるインストール* (↑起動)に説明されている方法でインストールを実行します。

インストールの最後の部分のためにターゲットシステムがリブートしたら、もう一度接続する必要があります。

8 インストールを完了します。

1.1.4 SSHによる単純なリモートインストール—静的なネットワーク設定

このタイプのインストールでは、インストール時のブートと、インストールターゲットのIPアドレスの決定のため、ターゲットシステムにある程度物理的にアクセスすることが必要となります。 インストール自体は、SSHを使用してインストーラに接続することにより、リモートのワークステーションによって完全に制御されます。 章 *YaSTによるインストール* (↑起動)で説明されている通常のインストールの場合と同様に、ユーザ操作も必要です。

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

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

このタイプのインストールを実行するには、以下の手順に従います。

1 項1.2.「インストールソースを保持するサーバのセットアップ」 (page 31)で説明されている方法でインストールソースをセットアップします。

2 SUSE Linux media kitの最初のCDまたはDVDを使って、ターゲットシステムをブートします。

3 ターゲットシステムのブート画面が表示されたら、ブートオプションプロンプトで、ネットワーク接続、インストールソースのアドレス、SSHの有効化のための適切なパラメータを設定します。 この詳細は、項1.4.3.「カスタムのブートオプションを使用する」 (page 54)で説明しています。

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

4 制御用のワークステーションで、ターミナルウィンドウを開いて、インストールプログラムへの接続項 (page 60)で説明されている方法でターゲットシステムに接続します。

5 章 *YaSTによるインストール* (↑起動)に説明されている方法でインストールを実行します。

インストールの最後の部分のためにターゲットシステムがリブートしたら、もう一度接続する必要があります。

6 インストールを完了します。

1.1.5 SSHによる単純なリモートインストール—DHCPによる動的なネットワーク設定

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

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

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

このタイプのインストールを実行するには、以下の手順に従います。

1. 項1.2.「インストールソースを保持するサーバのセットアップ」 (page 31)で説明されている方法でインストールソースをセットアップします。NFS、HTTP、またはFTPのネットワークサーバを選択します。 SMBのインストールソースの場合は、項1.2.5.「SMBインストールソースの管理」 (page 40)を参照してください。

2. SUSE Linux media kitの最初のCDまたはDVDを使って、ターゲットシステムをブートします。

3. ターゲットシステムのブート画面が表示されたら、ブートオプションプロンプトで、ネットワーク接続、インストールソースの場所、SSHの有効化のための適切なパラメータを設定します。 これらのパラメータの使用方法についての詳細は、項1.4.3.「カスタムのブートオプションを使用する」 (page 54)を参照してください。

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

4. 制御用のワークステーションで、ターミナルウィンドウを開いて、インストールプログラムへの接続項 (page 60)で説明されている方法でターゲットシステムに接続します。

5. 章 *YaSTによるインストール* (↑起動)に説明されている方法でインストールを実行します。

インストールの最後の部分のためにターゲットシステムがリブートしたら、もう一度接続する必要があります。

6 インストールを完了します。

1.1.6 SSHによるリモートインストール—PXEブートとWake on LAN

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

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

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

このタイプのインストールを実行するには、以下の手順に従います。

1 項1.2.「インストールソースを保持するサーバのセットアップ」 (page 31)で説明されている方法でインストールソースをセットアップします。NFS、HTTP、またはFTPのネットワークサーバを選択します。 SMBのインストールソースの設定は、項1.2.5.「SMBインストールソースの管理」 (page 40)を参照してください。

2 ターゲットシステムから取得するためのブートイメージを保持するTFTPサーバをセットアップします。これは項1.3.2.「TFTPサーバのセットアップ」 (page 43)で説明されています。

3 すべてのマシンにIPアドレスを提供し、ターゲットシステムにTFTPサーバの場所を知らせるためのDHCPサーバをセットアップします。これは項1.3.1. 「DHCPサーバのセットアップ」 (page 42)で説明されています。

4 ターゲットシステムでPXEブートの準備をします。この詳細は、項1.3.5. 「ターゲットシステムでPXEブートの準備をする」 (page 50)で説明しています。

5 Wake on LAN機能を使って、ターゲットシステムでブートプロセスを開始します。これは項1.3.7. 「Wake on LAN」 (page 51)で説明されています。

6 制御用のワークステーションで、ターミナルウィンドウを開いて、項1.5.2. 「SSHによるインストール」 (page 59)で説明されている方法でターゲットシステムに接続します。

7 章 *YaSTによるインストール* (↑起動)に説明されている方法でインストールを実行します。

   インストールの最後の部分のためにターゲットシステムがリブートしたら、もう一度接続する必要があります。

8 インストールを完了します。

1.2 インストールソースを保持するサーバのセットアップ

SUSE Linux用のネットワークインストールソースとして使用するマシンで動作しているオペレーティングシステムに応じて、サーバ設定のためのいくつかのオプションがあります。インストールサーバをセットアップする最も簡単な方法は、SUSE LINUX Enterprise Server 9またはSUSE Linux 9.3以降でYaSTを使うことです。SUSE LINUX Enterprise ServerまたはSUSE Linuxの他のバージョンでは、インストールソースのセットアップを手動で行います。

ティップ

Linuxの導入のために、Microsoft Windowsマシンをインストールサーバとして用いることもできます。詳細については、項1.2.5. 「SMBインストールソースの管理」 (page 40)を参照してください。

1.2.1 YaSTを使ってインストールサーバをセットアップする

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

1 インストールサーバにするマシンにrootとしてログインします。

2 *[YaST]* → *[その他]* → *[インストールサーバ]*の順に選択します。

3 サーバのタイプを選択します(HTTP、FTP、またはNFS)

選択したサーバサービスは、システムの起動時ごとに自動的に開始されます。 選択したタイプのサービスがシステム上ですでに動作していて、サーバ用に手動で設定する場合には、［*Do not configure any network services*］をオンにして、サーバサービスの自動設定を無効にします。どちらの場合でも、サーバ上のインストールデータを保管するディレクトリを設定してください。

4 必要なサーバタイプを設定します。

このステップは、サーバサービスの自動設定と関係しています。 自動設定を無効にした場合にはスキップされます。 インストールデータを置くFTPまたはHTTPサーバのルートディレクトリのエイリアスを定義してください。 後ほど、インストールソースは `ftp://Server-IP/Alias/Name` (FTP)、または `http://Server-IP/Alias/Name` (HTTP)に置かれます。 *Name*はインストールソースの名前を表すもので、次のステップで定義します。前のステップでNFSを選択した場合には、ワイルドカードとエクスポートオプションを指定します。 NFSサーバは、`nfs://Server-IP/Name`

としてアクセスできます。NFSとエクスポートについての詳細は、章 42. *NFS共有ファイルシステム* (page 691)を参照してください。

5 インストールソースを設定します。

インストール用メディアをコピーする前に、インストールソースの名前を定義します(容易に覚えられる、製品とバージョンの略が望ましいでしょう)。 YaSTでは、インストールCDのコピーの代わりに、メディアのISOイメージを使うことができます。 そうする場合には、対応するチェックボックスをオンにして、ISOファイルをローカルに保管するディレクトリのパスを指定します。 このインストールサーバで配布する製品によっては、製品を完全にインストールするために、アドオンのCDやサービスパックのCDが必要になることもあります。 [*Prompt for Additional CDs*]をオンにすると、YaSTは自動的に、これらのメディアを用意すべきことを思い出させます。 ネットワーク内のインストールサーバについて知らせるためにOpenSLPを使う場合には、適切なオプションをオンにします。

ティップ

ネットワークセットアップでサポートされている場合には、OpenSLPを使ってインストールソースを知らせることを考慮してみてください。 そうすれば、すべてのターゲットマシンでネットワークインストールパスを入力しなくてもよくなります。 SLPブートオプションでブートされたターゲットシステムは、他の設定を行わなくても、ネットワークインストールソースを見つけます。 このオプションについての詳細は、項1.4. 「ターゲットシステムをインストールのためにブートする」 (page 52)を参照してください。

---

6 インストールデータをアップロードします。

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

インストールサーバは完全に設定されて、使用する準備ができました。これはシステムが起動するたびに、自動的に開始します。 それ以上の操作は必要ありません。 必要なのは、YaSTの最初のステップで選択し

たネットワークサービスの自動設定を無効にしていた場合に、サービスを手動で正しく設定し、開始することだけです。

インストールソースを無効にするには、概要で［*Change*］を選択して、利用可能なすべてのインストールソースのリストを表示します。 削除するエントリを選択して、［*Delete*］を選択します。 この削除の手順では、サーバサービスを無効にしているだけです。 インストールデータ自体は、選択したディレクトリに残っています。 しかし、これは手動で削除することができます。

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

1.2.2 NFSインストールソースの手動セットアップ

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

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

1. rootとしてログインします。

2. 後ほどインストールデータを保持するディレクトリを作成し、このディレクトリに移動します。次に例を示します。

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

   *product*は製品名(この場合はSUSE Linux)の略語で、*productversion*は製品名とバージョンを含む文字列で置き換えてください。

3. メディアキットに含まれているCDごとに、以下のコマンドを実行します。

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

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

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

b ディレクトリの名前をCDの番号に合わせて変更します。

```
mv path_to_your_CD-ROM_drive CDx
```

*x*は、CDの実際の番号で置き換えてください。

YaSTを使用してNFSでインストールソースをエクスポートするには、以下の手順に従います。

1 rootとしてログインします。

2 *[YaST]* → *[ネットワークサービス]* → *[NFSサーバ]*の順に選択します。

3 ［*Start NFS Server*］および［*Open Port in Firewall*］をオンにして、［*Next*］をクリックします。

4 ［*Add Directory*］をクリックして、インストールデータを保持しているディレクトリへのパスを入力します。 この場合は、 */productversion* になります。

5 ［*Add Host*］をクリックして、インストールデータのエクスポート先になる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、ネットワークアドレス、または単にネットワークのドメイン名を使用することもできます。 適切なエクスポートオプションを入力するか、デフォルトのままにします。デフォルトでもほとんどのセットアップでは正しく動作します。 NFS共有のエクスポートで私用される構文の詳細については`export`のmanページを参照してください。

6 ［*Finish*］をクリックします。

SUSE Linuxのインストールソースを保持しているNFSサーバは自動的に起動します。またこれはブートプロセスに含められます。

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

1 rootとしてログインします。

2 /etc/exportsファイルを開いて、次の行を入力します。

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

これにより、ディレクトリ*/productversion*は、ネットワークに属している任意のホスト、またはこのサーバに接続している任意のホストにエクスポートされます。 このサーバへのアクセスを制限するには、一般的なワイルドカード*の代わりにネットマスクまたはドメイン名を使用してください。 詳細は、exportのmanページを参照してください。設定ファイルを保存して終了します。

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

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

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

4 次のコマンドで、NFSサーバを起動します。

```
rcnfsserver start
```

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

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

1 rootとしてログインします。

2 /etc/slp.reg.d/ディレクトリに入ります。

3 以下の行を含む、install.suse.nfs.regという名前の設定ファイルを作成します。

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

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

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

```
rcslpd start
```

OpenSLPについての詳細は、/usr/share/doc/packages/openslp/のパッケージのドキュメント、または章 39. *ネットワーク上のSLPサービス* (page 657)を参照してください。

1.2.3 FTPインストールソースの手動セットアップ

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

1 項1.2.2. 「NFSインストールソースの手動セットアップ」 (page 34)で説明されているように、インストールソースを保持するディレクトリを作成します。

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

   a rootとしてログインし、YaSTのパッケージマネージャを使ってpure-ftpdパッケージ(軽量なFTPサーバ)をインストールします。

   b FTPサーバのルートディレクトリに入ります。

```
cd/srv/ftp
```

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

```
mkdirinstsource
```

*instsource*は製品名で置き換えてください。

d すべてのインストールCDの内容を、FTPサーバのルートディレクトリにコピーします(項1.2.2. 「NFSインストールソースの手動セットアップ」 (page 34)、ステップ 3 (page 34)で説明されているの同様の手順)。

または、既存のインストールレポジトリの内容を、FTPサーバのルート環境にマウントします。

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

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

e pure-ftpdを起動します。

```
pure-ftpd &
```

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

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

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

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

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

```
rcslpd start
```

1.2.4 HTTPインストールソースの手動セットアップ

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

1. 項1.2.2. 「NFSインストールソースの手動セットアップ」 (page 34)で説明されているように、インストールソースを保持するディレクトリを作成します。
2. インストールディレクトリの内容を配布するためのHTTPサーバを設定します。
   - **a** rootとしてログインし、YaSTのパッケージマネージャを使って`apache2`をインストールします。
   - **b** HTTPサーバのルートディレクトリ(`/srv/www/htdocs`)に入り、インストールソースを保持するサブディレクトリを作成します。

     ```
     mkdir instsource
     ```

     *`instsource`*は製品名で置き換えてください。
   - **c** インストールソースの場所からWebサーバのルートディレクリ(`/srv/www/htdocs`)への、シンボリックリンクを作成します。

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

     ```
     Options None
     ```

を次の行で置き換えます。

```
Options Indexes FollowSymLinks
```

e `rcapache2 restart`でHTTPサーバを再起動します。

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

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

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

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

1.2.5 SMBインストールソースの管理

SMB (Samba)を使えば、Linuxマシンがなくても、Microsoft Windowsサーバからインストールソースをインポートして、Linuxの導入を開始することができます。

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

1 Windowsマシンにログインします。

2 エクスプローラを起動して、インストールツリー全体を保持する新しいフォルダを作成し、`INSTALL`のような名前を付けます。

3 この共有を、Windowsのドキュメントで説明されている方法に従ってエクスポートします。

4 この共有に入って、*`product`*という名前のサブフォルダを作成します。*`product`*は、実際の製品名(この場合はSUSE Linux)で置き換える必要があります。

5 SUSE LinuxのCDを個別のフォルダにコピーし、それらにCD1、CD2、CD3などの名前を付けます。

6 エクスポートされた共有の最上位ディレクトリ(この例ではINSTALL)に入り、*product*/CD1から以下のファイルをコピーします。content、media.1、control.xmlおよびboot

7 INSTALLの下に新しいフォルダを作成し、yastと名前を付けます。

8 yastフォルダに入り、orderおよびinstorderというファイルを作成します。

9 orderファイルを開いて、次の行を入力します。

```
/NLD/CD1 smb://user:password@hostname/productCD1
```

*user*は、Windowsマシンで使用するユーザ名で置き換えます。または、この共有でゲストログインを有効にする場合には、Guestを使います。*password*は、ログインパスワードで置き換えます。ゲストログインの場合は、任意の文字列にします。*hostname*は、Windowsマシンのネットワーク名で置き換えます。

10 instorderファイルを開いて、次の行を入力します。

```
/product/CD1
```

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

1 インストールターゲットをブートします。

2 ［*Installation*］を選択します。

3 インストールソースの選択のために、F4を押します。

4 SMBを選択し、Windowsマシンの名前またはIPアドレス、共有名(この例ではINSTALL)、ユーザ名、パスワードを入力します。

Enterを押すと、YaSTが起動して、インストールを実行します。

1.3 ターゲットシステムのブートの準備

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

1.3.1 DHCPサーバのセットアップ

SUSE Linuxでは、DHCPサーバのセットアップは、適切な設定ファイルを手動で編集することによって行います。 このセクションでは、既存のDHCPサーバの構成を拡張して、TFTP、PXE、およびWOL環境でサービスを行うのに必要なデータを提供する方法について説明します。

DHCPサーバの手動セットアップ

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

1. DHCPサーバのホストとなるマシンにrootとしてログインします。

2. `/etc/dhcpd.conf`というDHCPサーバの設定ファイルに、以下の行を追加します。

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

   *ip_of_the_tftp_server*は、TFTPサーバの実際のIPアドレスで置き換えてください。

dhcpd.confで利用可能なオプションの詳細については、dhcpd.confのmanページを参照してください。

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

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

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

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

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

1.3.2 TFTPサーバのセットアップ

TFTPサーバの設定は、YaSTで行えます。または、xinetdとtftpをサポートしているLinuxオペレーティングシステムであれば手動で行えます。TFTPサーバは、ターゲットシステムがブートして要求を送ったときに、ブートイメージを提供します。

YaSTによるTFTPサーバのセットアップ

1 rootとしてログインします。

2 *[YaST]* → *[ネットワークサービス]* → *[TFTPサーバ]*の順に選択して、要求されたパッケージをインストールします。

3 ［*Enable*］をクリックして、サーバが起動し、ブートルーチンに含まれるようにします。この点についてはこれ以上の操作は必要ありません。xinetdはブート時にtftpdを起動します。

4 ［*Open Port in Firewall*］をクリックして、マシンで動作しているファイアウォールで適切なポートを開きます。サーバでファイアウォールが動作していない場合には、このオプションは利用できません。

5 ［*Browse*］をクリックして、ブートイメージのディレクトリをブラウズします。

デフォルトのディレクトリ`/tftpboot`が作成され、自動的に選択されます。

6 ［*Finish*］をクリックして、設定内容を適用し、サーバを起動します。

TFTPサーバの手動セットアップ

1 rootとしてログインして、`tftp`および`xinetd`パッケージをインストールします。

2 もしまだ存在していなければ、`/srv/tftpboot`および`/srv/tftpboot/pxelinux.cfg`ディレクトリを作成します。

3 項1.3.3.「PXEブート」 (page 45)で説明されているように、ブートイメージに必要な、適切なファイルを追加します。

4 `/etc/xinetd.d/`にあるxinetdの設定ファイルを修正して、ブート時にftfpサーバが起動するようにします。

a もしまだ存在していなければ、`touch tftp`コマンドで、このディレクトリに`tftp`というファイルを作成します。それから`chmod 755 tftp`を実行します。

b `tftp`ファイルを開いて、次の行を入力します。

```
service tftp
{
```

```
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /tftpboot
        disable                 = no
}
```

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

1.3.3 PXEブート

PXE (Preboot Execution Environment)の仕様書(ftp://download.intel.com/labs/manage/wfm/download/pxespec.pdf)では、いくらかの技術的な背景情報と、PXEの完全な仕様について知ることができます。

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

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

2 YaSTを使い、インストールCDまたはDVDから直接syslinuxパッケージをインストールします。

3 次のコマンドを入力して、/usr/share/syslinux/pxelinux.0ファイルを/srv/tftpbootディレクトリにコピーします。

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

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

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

5 /srv/tftpboot/pxelinux.cfg/defaultファイルを編集して、gfxboot、readinfo、およびframebufferで始まる行を削除します。

6 デフォルトのfailsafeおよびapicラベルのappend行に、以下のエントリを挿入します。

insmod=e100
このエントリにより、Intel 100MBit/sネットワークカード用のカーネルモジュールがPXEクライアントにロードされます。 このエントリはクライアントのハードウェアに依存するので、それに応じて調整してください。 Broadcom GigaBitネットワークカードの場合には、このエントリをinsmod=bcm5700にします。

netdevice=eth0
このエントリは、ネットワークインストールで使用する、クライアントのネットワークインタフェースを定義します。 これは、クライアントに複数のネットワークカードが装着されている場合にのみ必要です。適切に調整してください。 ネットワークカードが1枚の場合には、このエントリは省略できます。

install=nfs://*ip_instserver*/*path_instsource*/CD1
このエントリは、NFSサーバとクライアントインストールのインストールソースを定義します。 *ip_instserver*は、インストールサーバの実際のIPアドレスで置き換えてください。 *path_instsource*は、インストールソースの実際のパスで置き換えてください。HTTP、FTP、またはSMBソースも同様の仕方で指定できます。プロトコルのプレフィックスはhttp、ftp、またはsmbになります。

重要項目

SSHまたはVNCブートパラメータなどの、他のブートオプションをインストールルーチンに渡す必要がある場合には、それらをinstallエントリに追加します。 パラメータの概要といくつかの例は、項1.4.「ターゲットシステムをインストールのためにブートする」 (page 52)を参照してください。

/srv/tftpboot/pxelinux.cfg/defaultファイルの例は、次のようなものです。 インストールソースのプロトコルプレフィックスは、ネットワークのセットアップにマッチするように調整してください。そ

して、使用する接続方法を指定するために、installエントリにvncとvncpasswordまたはsshとsshpasswordオプションを追加してください。 \で区切られている行は、改行や \なしに、連続する1行として入力する必要があります。

```
default linux

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

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

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

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

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

#  memory test
label memtest
  kernel memtest

# hard disk
label harddisk
  kernel linux
  append SLX=0x202

implicit     0
display      message
prompt       1
timeout      100
```

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

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

1.3.4 PXELINUXの設定オプション

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

DEFAULT *kernel options...*

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

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

APPEND *options...*

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

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

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

GRUBは次の構文を使用することに注意してください。

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

一方、PXELINUXは次の構文を使用します。

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

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

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

APPEND -

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

LOCALBOOT *type*

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

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

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

TIMEOUT *time-out*

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

タイムアウトの最大値は35996です(1時間よりほんの少しだけ短い時間です)。

PROMPT *flag_val*

`flag_val`を0に設定すると、Shiftか Altが押された場合、またはCaps Lockか Scroll lockがセットされている場合にのみ、ブートプロンプトを表示します(これがデフォルトです)。`flag_val`を1に設定すると、常にブートプロンプトを表示します。

```
F2  filename
F1  filename
..etc...
F9  filename
F10filename
```

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

1.3.5 ターゲットシステムでPXEブートの準備をする

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

警告

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

1.3.6 ターゲットシステムでWake on LANの準備をする

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

1.3.7 Wake on LAN

Wake on LANを使えば、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が送られたときに、マシンの電源を入れることができます。 世界中のすべてのマシンは一意のMAC識別子を持っているので、間違って別なマシンの電源を入れてしまう心配はありません。

重要項目

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

1.3.8 手動によるWake on LAN

1 rootとしてログインします。

2 *[YaST]* → *[ソフトウェアのインストール/削除]*の順に選択して、`netdiag`パッケージをインストールします。

3 ターミナルを開き、rootとして次のコマンドを入力して、ターゲットを起動します。

```
ether-wake mac_of_target
```

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

1.4 ターゲットシステムをインストールのためにブートする

基本的に、項1.3.7. 「Wake on LAN」 (page 51)と項1.3.3. 「PXEブート」 (page 45)で説明されているものを別にして、インストール用のブートプロセスをカスタマイズする方法は2とおりあります。デフォルトのブートオプションとFキーを使用することもできますし、インストールブート画面のブートオプションプロンプトを使って、特定のハードウェアでインストールカーネルが必要とするブートオプションを渡すこともできます。

1.4.1 デフォルトのブートオプションを使う

ブートオプションについての詳細は、章 *YaSTによるインストール*(↑起動)ですでに説明されています。

一般に、［*Installation*］を選択すれば、インストールブートプロセスが開始します。 問題が生じたときには、［*Installation—ACPI Disabled(インストール—ACPI無効)*］または［*Installation—Safe Settings(インストール—セーフ設定)*］オプションを使えば、回避できる場合があります。

インストールプロセスでのトラブルシューティングについての詳細は、項「インストールの問題」 (章 9. *最も頻繁に起こる問題およびその解決方法*, ↑起動)を参照してください。

1.4.2 Fキーを使う

画面の下部にあるメニューバーには、セットアップで必要になる、いくつかの高度な機能が用意されています。 Fキーを使えば、ブートオプションに渡

す場合のようにパラメータの詳細な構文について知らなくても、インストールルーチンに渡す付加的なオプションを指定することができます(項1.4.3.「カスタムのブートオプションを使用する」 (page 54)を参照)。

利用可能なオプションについては、次のテーブルを参照してください。

表 1.1　インストール時に使用できるFキー

キー	目的	利用可能なオプション	デフォルト値
F1	ヘルプを表示する	なし	なし
F2	インストール時の言語を選択する	サポートされているすべての言語	English (英語)
F3	インストール時の画面解像度を変更する	• テキストモード • VESA • 解像度#1 • 解像度#2 • ...	• デフォルト値は、使用しているグラフィックハードウェアによって異なります。
F4	インストールソースを選択する	• CD-ROM/DVD • SLP • FTP • HTTP • NFS • SMB	CD-ROM/DVD

キー	目的	利用可能なオプション	デフォルト値
		• ハードディスク	
F5	ドライバアップデートディスクを適用する	Driver (ドライバ)	なし

1.4.3 カスタムのブートオプションを使用する

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

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

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

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

表 1.2 *この章で用いられているインストール(ブート)シナリオ*

インストールシナリオ	ブートに必要なパラメータ	ブートオプション
章 *YaSTによるインストール* (↑起動)	なし、システムは自動的にブートする	必要なし

インストールシナリオ	ブートに必要なパラメータ	ブートオプション
項1.1.1. 「VNCによる単純なリモートインストール—静的なネットワーク設定」 (page 22)	• インストールサーバの場所 • ネットワークデバイス • IPアドレス • ネットマスク • ゲートウェイ • VNCの有効化 • VNCのパスワード	• `install=(nfs,http,ftp,smb)://path_to_instmedia` • `netdevice=some_netdevice` (複数のネットワークデバイスが利用可能な場合にのみ必要) • `hostip=some_ip` • `netmask=some_netmask` • `gateway=ip_gateway` • `vnc=1` • `vncpassword=some_password`
項1.1.2. 「VNCによる単純なリモートインストール—DHCPによる動的なネットワーク設定」 (page 24)	• インストールサーバの場所 • VNCの有効化 • VNCのパスワード	• `install=(nfs,http,ftp,smb)://path_to_instmedia` • `vnc=1` • `vncpassword=some_password`
項1.1.3. 「VNCによるリモートインストール—PXEブートとWake on LAN」 (page 25)	• インストールサーバの場所 • TFTPサーバの場所 • VNCの有効化 • VNCのパスワード	適用されない。プロセスはPXEとDHCPによって管理される

インストールシナリオ	ブートに必要なパラメータ	ブートオプション
項1.1.4.「SSHによる単純なリモートインストール—静的なネットワーク設定」 (page 27)	• 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 • SSHのパスワード	• `install=(nfs,http,ftp,smb)://path_to_instmedia` • `netdevice=some_netdevice`(複数のネットワークデバイスが利用可能な場合にのみ必要) • `hostip=some_ip` • `netmask=some_netmask` • `gateway=ip_gateway` • `usessh=1` • `sshpassword=some_password`
項1.1.5.「SSHによる単純なリモートインストール—DHCPによる動的なネットワーク設定」 (page 28)	• インストールサーバの場所 • SSHの有効化 • SSHのパスワード	• `install=(nfs,http,ftp,smb)://path_to_instmedia` • `usessh=1` • `sshpassword=some_password`
項1.1.6.「SSHによるリモートインストール—PXEブートとWake on LAN」 (page 30)	• インストールサーバの場所 • TFTPサーバの場所 • SSHの有効化 • SSHのパスワード	適用されない。プロセスはPXEとDHCPによって管理される

ティップ

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

1.5 インストールプロセスのモニタ

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

1.5.1 VNCによるインストール

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

VNCによるインストールの準備

VNCによるインストールを準備するために、インストールターゲット上で行う必要のあることは、インストールのための初期ブートで適切なブートオプションを選択することだけです(項1.4.3.「カスタムのブートオプションを使用する」 (page 54)を参照)。 ターゲットシステムはテキストベースの環境にブートして、VNCクライアントがインストールプログラムに接続するのを待ちます。

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

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

1 KDEのファイルおよびWebブラウザであるKonquerorを起動します。

2 場所バーに`service://yast.installation.suse`と入力します。

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

インストールプログラムに接続する

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

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

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

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

1 VNCビューアを起動します。

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

ip_address:*display_number*

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

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

VNCでのインストールを実行するには、以下の手順に従います。

1. 使用しているWebブラウザを起動します。
2. アドレスに以下のように入力します。

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

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

1.5.2 SSHによるインストール

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

SSHによるインストールの準備

ソフトウェアパッケージ(LinuxではOpenSSH、WindowsではPuTTY)のインストールの他に、SSHによるインストールのために適切なブートオプションを渡す必要があります。詳細については、項1.4.3.「カスタムのブートオプションを使用する」 (page 54)を参照してください。 OpenSSHは、SUSE Linuxベースのオペレーティングシステムであれば、デフォルトでインストールされています。

インストールプログラムへの接続

1 インストールターゲットのIPアドレスを取得します。

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

2 コマンドラインで次のコマンドを入力します。

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

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

3 ユーザ名を要求されたら、`root`と入力します。

4 パスワードを要求されたら、SSHのブートオプションで設定したパスワードを入力します。

正しく認証されると、インストールターゲットのコマンドプロンプトが表示されます。

5 `yast`と入力して、インストールプログラムを起動します。

章 *YaSTによるインストール* (↑起動)で説明されているように、ウィンドウが開いて、通常のYaSTの画面が表示されます。

2 高度なディスクセットアップ

高性能のシステムを設定するには、特定のディスクセットアップが必要となります。 SCSIデバイスに永続的なデバイス名をつけるには、固有のスタートアップスクリプトを使用します。 LVM (Logical Volume Management)は、ディスクパーティショニング用のスキーマで、標準的なセットアップで使用される物理パーティショニングよりもずっと柔軟性が高くなるように設計されています。 そのスナップショット機能を使えば、簡単にデータのバックアップを作成できます。 RAID (Redundant Array of Independent Disks)を使えば、データの完全性、パフォーマンス、フォールトトレランスの機能が高くなります。

2.1 SCSIデバイス用の永続的なデバイス名

システムをブートすると、SCSIデバイスに動的な方法でデバイスファイル名が割り当てられます。これはデバイス数または設定に変更がない限り問題にはなりません。ただし、新しいSCSIハードディスクが追加され、古いハードディスクが検出される前に新しいハードディスクが検出されると、古いディスクに新しい名前が割り当てられるためマウントテーブルのエントリ `/etc/fstab`は一致しません。

この問題を避けるため、システムスタートアップスクリプト`boot.scsidev`を使用できます。 `/sbin/insserv`を使用して、このスクリプトを有効化し、 `/etc/sysconfig/scsidev`にあるこのスクリプト用のパラメータを設定します。スクリプト `/etc/rc.d/boot.scsidev`は、ブート処理中にSCSI

デバイスのセットアップを処理し、 /dev/scsi/下に永続的デバイス名を入力します。次にこれらの名前が、 /etc/fstab内で使用されます。 /etc/scsi.aliasが、SCSI設定における固定的な名前を定義するために使用されます。 /etc/scsi内でのデバイスの命名規則は、 man scsidevを参照してください。

ランレベルエディタのエキスパートモードで、レベルBに対してboot.scsidevを有効化します。ブート処理中に名前を生成するために必要なリンクが、次に/etc/init.d/boot.dに作成されます。

ティップ: デバイス名とudev

SUSE Linuxの場合は、boot.scsidevが依然としてサポートされていますが、永続的なデバイス名を作成する適切な方法は、udevを使用して/dev/by-id/内の永続的な名前を使用するデバイスノードを作成することです。

2.2 LVMの設定

このセクションでは、LVMの基本原則と様々な状況で役立つ基本的な機能を簡単に説明します。項2.2.2. 「YaSTによるLVMの設定」 (page 65)では、YaSTを使用したLVMのセットアップ方法を学びます。

警告

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

2.2.1 論理ボリュームマネージャ(LVM)

論理ボリュームマネージャ(LVM)は、複数のファイルシステム上でハードディスクスペースを柔軟に割り振ることができます。これは、インストール中の初期パーティショニングを終了した後になってハードディスクスペースの区分を変更する必要が時として発生するために開発されました。稼動中のシス

テムでパーティションを変更することは困難なため、LVMは必要に応じて論理ボリューム(LV)を作成できるメモリスペースの仮想プール(ボリュームグループ(VG))を提供します。オペレーティングシステムは物理パーティションの代わりにこれらのLVにアクセスします。ボリュームグループは2つ以上のディスクを使用することができます。また、複数のディスクまたはその一部が連続した1つのVGを形成することも可能です。この方法でLVMは物理ディスクスペースから一種の抽象層を提供します。この抽象層により、物理的にパーティショニングを再度行うよりもより簡単かつ安全な方法で区分に変更を加えられるようになります。物理パーティショニングに関連する背景情報についてはパーティションのタイプ項 (章 1. *YaSTによるインストール*, ↑起動) および項 「パーティション分割ツール」 (章 3. *YaSTでのシステム設定*, ↑起動) を参照してください。

図 2.1 *物理パーティショニング対LVM*

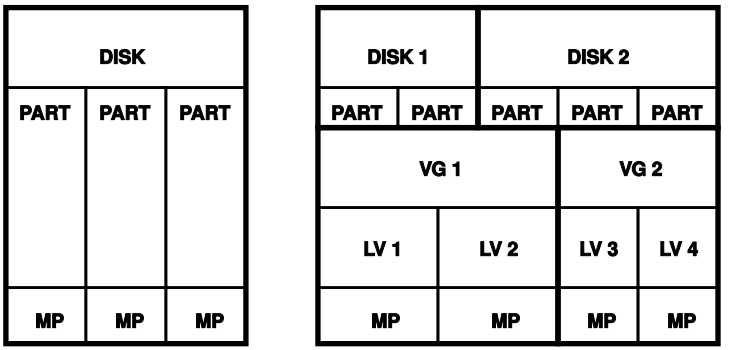


図 2.1. 「物理パーティショニング対LVM」 (page 63)では物理パーティショニング(左)とLVM区分(右)を比較しています。左側は、1つのディスクが割り当てられたマウントポイント(MP)をもつ3つの物理パーティション(PART)に分かれています。これによりオペレーティングシステムはそれぞれのパーティションにアクセスできます。右側では2つのディスクがそれぞれ3つの物理パーティションに分かれています。2つのLVMボリュームグループ(VG 1およびVG 2)が定義されています。VG 1にはDISK 1とDISK 2の2つのパーティションが含まれます。VG 2はDISK 2の2つのパーティションを除いた残り部分になります。LVMではボリュームグループに組み込まれた物理ディスクパーティションは物理ボリューム(PV)と呼ばれます。ボリュームグループ内に4つの論理ボリューム(LV 1からLV 4)が定義されています。これらのボリュームは、それぞれに関連づけられたマウントポイントを介してオペレーティングシステムに使用されます。 別の論理ボリュームとの境界とパーティションの境界を並べることはできません。この例ではLV 1およびLV 2の間に境界があります。

LVMの機能:

- 複数のハードディスクまたはパーティションを大きな論理ボリュームにまとめることができます。
- 提供された設定が適切であれば、LV(/usrなど)は空きスペースがなくなったときに拡張することができます。
- LVMを使用することで、実行中のシステムにハードディスクまたはLVが追加されます。ただし、こうしたディスクやLVを追加するには、ホットスワップ可能なハードウェアが必要になります。
- 複数の物理ボリューム上に論理ボリュームのデータストリームを割り当てる「ストライピングモード」を有効にすることもできます。これらの物理ボリュームが別のディスクに存在する場合、RAID 0と同様に読み込みおよび書き込みのパフォーマンスを向上できます。
- スナップショット機能は稼動中のシステムで一貫性のある(特にサーバ)バックアップを取得できます。

これらの機能とともにLVMを使用することは、頻繁に使用されるホームPCや小規模サーバではそれだけでも意義があります。データベース、音楽アーカイブ、ユーザディレクトリなどの増え続けるデータストックがある場合は、LVMが最適と言えます。LVMは物理ハードディスクより大きなファイルシステムを利用できます。LVMのもう1つの利点は最大256個のLVを追加できることです。ただし、LVMでの作業は従来のパーティションでの作業とは異なることに留意してください。LVMの設定についての指示および詳しい情報は http://tldp.org/HOWTO/LVM-HOWTO/の公式LVM HOWTOからご利用いただけます。

カーネルバージョン2.6から開始して、LVMバージョン2を利用することができます。これはLVMの前バージョンとの下方互換になり、これまでのボリュームグループを管理できるようにします。新しいボリュームグループを作成する場合は、新しいフォーマットまたは下方互換バージョンのどちらを使用するか決定します。LVM2にはいずれのカーネルパッチも必要ありません。LVM2によりデバイスマッパーがカーネル2.6に統合されます。このカーネルはLVMバージョン2のみをサポートします。そのため、このセクションでLVMについて記述している場合は常にLVMバージョン2を参照します。

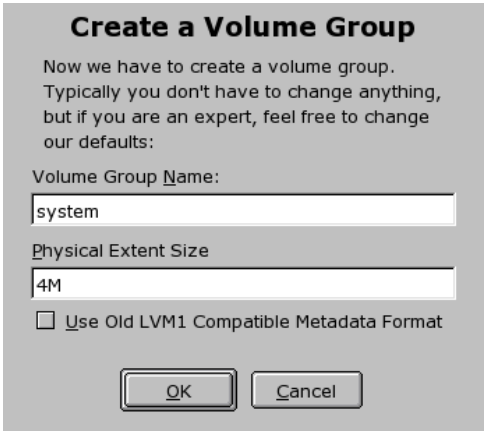
2.2.2 YaSTによるLVMの設定

YaSTのLVM設定には、YaSTのパーティションモジュールのエキスパートページ(項 「パーティション分割ツール」 (章 3. *YaSTでのシステム設定*, ↑起動)を参照)からアクセスできます。この専用パーティショニングツールにより、既存のパーティションを編集、および削除できます。また、LVMで使用する新規パーティションを作成することもできます。次に*[作成]* → *[Do not format(フォーマットしない)]*を最初にクリックし、続いて［*0x8E Linux LVM*］をパーティションIDとして選択します。 LVMで使用するすべてのパーティションを作成した後に、［*LVM*］をクリックして、LVMの設定を開始します。

ボリュームグループの作成

システムにまだボリュームグループが存在しない場合、ボリュームグループを追加するようにプロンプトされます(図 2.2. 「ボリュームグループの作成」 (page 66)を参照)。［*Add group(グループを追加)*］で追加グループを作成することができますが、通常はボリュームグループは1つで十分です。SUSE Linuxシステムファイルがあるボリュームグループの名前としては`system`が推奨されます。物理エクステントサイズではボリュームグループの物理ブロックサイズを定義します。ボリュームグループにある全ディスクスペースはこの物理ブロックサイズ内で使用されます。 この値は通常4MBに設定され、物理ボリュームおよび論理ボリュームには最大サイズとして256GB使用できます。物理エクステントは論理ボリュームとして256GB以上必要な場合のみ、8、16、32MBのように増やしてください。

図 2.2　ボリュームグループの作成

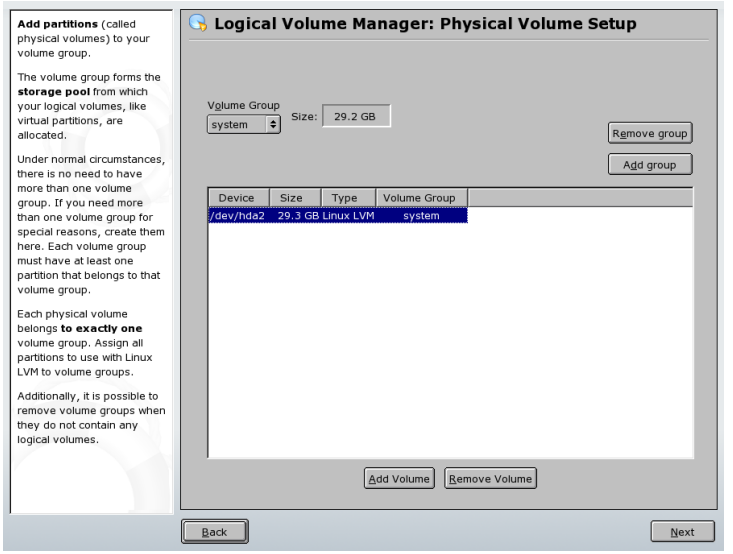


物理ボリュームの設定

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

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

図 2.3　物理ボリュームの設定



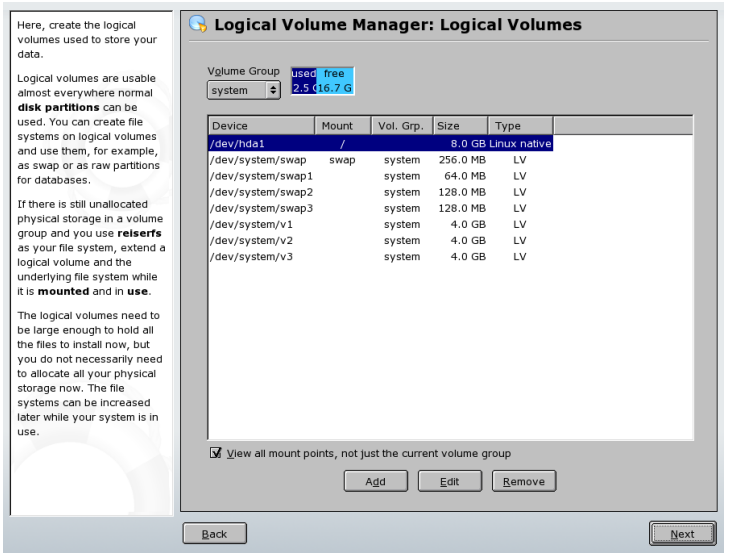
これまで未割り当てだったパーティションを選択したボリュームグループに追加するには、そのパーティションをクリックしてから［*ボリュームの追加*］をクリックします。この時点で、そのボリュームグループの名前が選択したパーティションの隣に入力されます。LVM用に予約されているパーティションをすべて1つのボリュームグループに割り当ててください。すべてのパーティションを割り当てないと、パーティションのスペースが未使用のまま残ります。ダイアログを終了する前に、すべてのボリュームグループを少なくとも1つの物理ボリュームに割り当てる必要があります。すべての物理ボリュームを割り当て終えた後、［次へ］をクリックして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

物理ボリュームの設定

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

すべての領域がなくなるまで、必要に応じて論理ボリュームの［*追加*］、［*編集*］、［*削除*］を実行します。各ボリュームグループに少なくとも1つの論理ボリュームを割り当ててください。

図 2.4 *論理ボリューム管理*

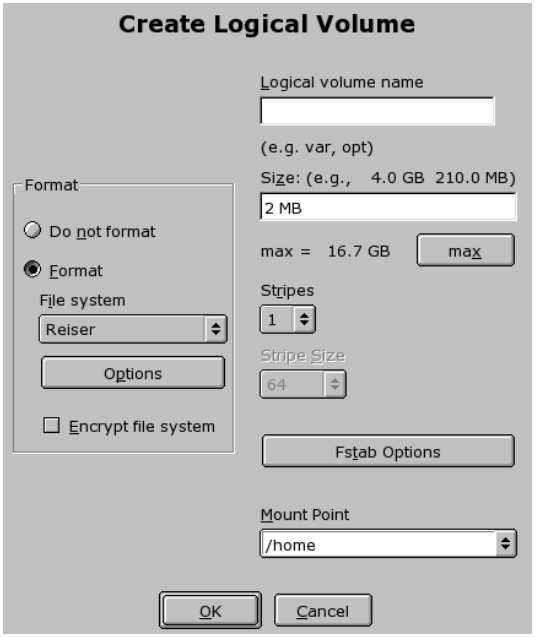


新しい論理ボリュームを作成するには［*追加*］をクリックし、開いたポップアップの内容を埋めます。パーティショニングの場合、サイズ、ファイルシステム、およびマウントポイントを入力します。通常、ReiserFSまたはExt2などのファイルシステムは論理ボリューム上に作成され、マウントポイントを指定します。この論理ボリューム上に格納されたファイルは、インストールしたシステム上の該当するマウントポイントで検出することができます。さらに、複数の物理ボリューム上(ストライピング)に存在する論理ボリュームにデータストリームを分配することも可能です。これらの物理ボリュームが別のハードディスクに存在する場合、こ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

警告: ストライピング

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

図 2.5　論理ボリュームの作成



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

LVMの直接管理

LVMをすでに設定し、一部に変更を加えるのみの場合は、別の方法でLVMにアクセスすることができます。 YaSTコントロールセンターで*[システム]* → *[LVM]*の順に選択します。 このダイアログでは基本的に、先に説明したアクションと同じことを実行できます。ただし物理パーティショニングは除きま

す。2つのリストに既存の物理ボリュームと論理ボリュームが表示されます。これにより、先に説明した方法を使用して、LVMシステムを管理できます。

2.3 ソフトウェアRAID設定

RAID (redundant array of inexpensive disks)の目的は、複数のハードディスクパーティションを1つの大きい*仮想*ハードディスクに結合し、パフォーマンスとデータのセキュリティを最適化することです。ただし、この方法を用いると、1つの利点が生かされるために他の利点が犠牲になります。ほとんどのRAIDコントローラはSCSIプロトコルを使用します。 これは、IDEプロトコルも効率的な方法で多数のハードディスクのアドレスを指定でき、コマンドのパラレル処理に適しているからです。一方、IDEまたはSATAハードディスクをサポートしているRAIDコントローラもあります。`http://cdb.suse.de`にアクセスして「Hardware Database」(ハードウェアデータベース)を参照してください。

2.3.1 ソフトウェアRAID

非常に高価なRAIDコントローラと同様に、ソフトウェアRAIDも上記のタスクを実行できます。SUSE Linuxでは、YaSTを使用することにより、複数のハードディスクを1つのソフトウェアRAIDシステムに結合するオプション、つまり、非常にリーズナブルな、ハードウェアRAIDの代替機能を提供します。RAIDは、それぞれが異なる目標、利点、および属性を持ついくつかのハードディスクを1つのRAIDシステムに結合するためのいくつかの戦略を含んでいます。これらは通常、*RAIDレベル*と呼ばれます。

一般的なRAIDレベルは次のとおりです。

RAID 0

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

RAID 1

このレベルでは、データが他のハードディスクに一対一でコピーされるため、データに対する適切なセキュリティが提供されます。これは、ハードディスクミラーリングとして知られています。一方のディスクが破壊された場合、そのディスク内容のコピーが他方のディスク上で利用できます。一方のディスクが破壊されても、データが危険にさらされることはありません。単一ディスクアクセスを使用した場合を比較すると、コピー処理において書き込みのパフォーマンスが若干、低下しますが(10から20%遅くなる)、読み取りアクセスは通常の物理ハードディスクに比べ、大幅に速くなります。これは、データが複製されており、並列にスキャンできるためです。一般的に、レベル1は、単一ディスクのほぼ2倍の読み取りトランザクション速度と、単一ディスクとほぼ同じ書き込みトランザクション速度を提供します。

RAID 2およびRAID 3

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

RAID 4

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

RAID 5

RAID 5は、レベル0とレベル1の間をパフォーマンスおよび冗長性の面で調整して、最適化したものです。ハードディスクスペースは、使用されるディスク数から1を引いたものに等しくなります。データは、RAID 0の場合のようにハードディスク間で分散されます。パーティションの1つで作成されたパリティブロックがあるのは、セキュリティ上の理由からです。各パーティションはXORによって互いにリンクされているので、システム障害の場合に、XORを介して内容が対応するパリティブロックによって再構築されます。RAID 5の場合、同時に複数のハードディスクが障害を起こすことはありません。1つのハードディスクに障害がある場合は、そのハードディスクをできるだけ早く交換して、データ消失の危険性をなくす必要があります。

その他のRAIDレベル

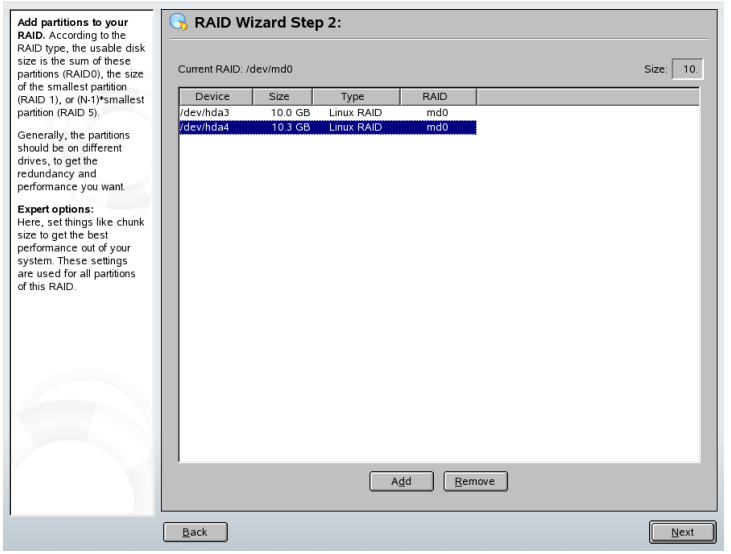
他のRAIDレベル(RAIDn、RAID 10、RAID 0+1、RAID 30、RAID 50など)が開発されていますが、そのうちのいくつかはハードウェアベンダによって独自規格で作成される実装となります。これらのレベルは、広く使用されてはいないため、ここでの説明は省略します。

2.3.2 YaSTによるソフトウェアRAID設定

YaSTソフトウェアRAID設定には、YaST Expert Partitioner (項 「パーティション分割ツール」 (章 3. *YaST*でのシステム設定, ↑起動)を参照)からアクセスできます。このプロフェッショナル向けのパーティション設定ツールを使用すると、既存のパーティションを編集および削除したり、ソフトウェアRAIDで使用する新規パーティションを作成できます。ここでは、RAIDパーティションを作成します。最初に*[作成]* → *[Do not format (フォーマットしない)]*の順にクリックし、次にパーティション識別子として［*0xFD Linux RAID*］を選択します。RAID 0およびRAID 1の場合、少なくとも2つのパーティションが必要です。RAID 1の場合、パーティションは2つだけです。RAID 5を使用する場合、少なくとも3つのパーティションが必要です。同じサイズのパーティションだけを使用するようにお勧めします。RAIDパーティションを異なるハードディスクに保存すると、1つが損傷した場合のデータ消失のリスクが削減され(RAID 1と5)、またRAID 0のパフォーマンスを最適化できます。RAIDで使用するすべてのパーティションを作成したら、*[RAID]* → *[Create RAID (RAIDの作成)]*の順にクリックして、RAID設定を開始します。

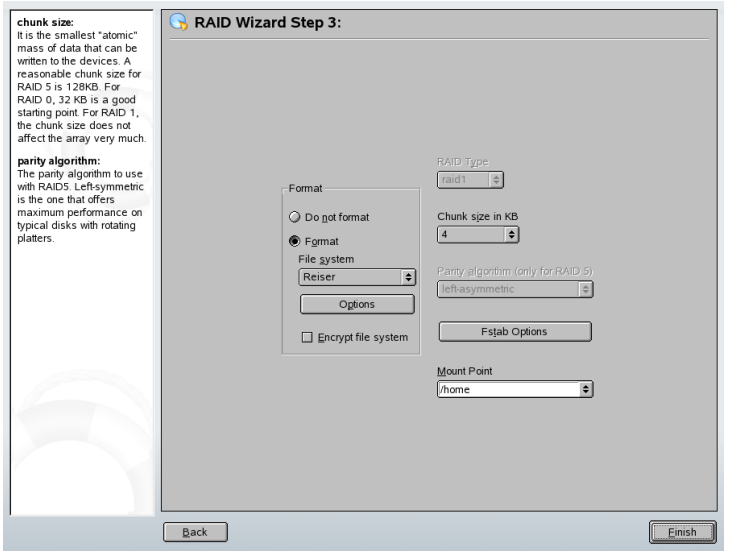
次のダイアログでは、RAIDレベル 0、1、および5の間で選択します。詳細については、項2.3.1.「ソフトウェアRAID」 (page 70)を参照してください。［次へ］をクリックすると、次のダイアログにタイプが「Linux RAID」または「Linux Native」であるすべてのパーティションのリストが表示されます(図2.6.「RAIDパーティション」 (page 73)を参照)。スワップパーティションまたはDOSパーティションは表示されません。パーティションがRAIDボリュームにすでに割り当てられている場合は、RAIDデバイスの名前(たとえば`/dev/md0`)がリストに表示されます。割り当てられていないパーティションは、「--」で示されます。

図 2.6　RAIDパーティション



前に割り当てを解除したパーティションを、選択したRAIDボリュームに追加するには、そのパーティションをクリックしてから、［*ボリュームの追加*］をクリックします。この時点で、そのRAIDデバイスの名前が選択したパーティションの隣に入力されます。すべてのパーティションをRAID用の予約パーティションとして割り当てます。すべてのパーティションを割り当てないと、パーティションのスペースが未使用のまま残ります。すべてのパーティションを割り当てたら、［次へ］をクリックして、設定ダイアログに進みます。このダイアログではパフォーマンスを微調整できます(図 2.7.「ファイルシステム設定」 (page 74)を参照)。

図 2.7　ファイルシステム設定



従来のパーティションの場合と同様の設定以外だけでなく、暗号化とRAIDボリュームのマウントポイントを使用するように、ファイルシステムを設定します。［*Persistent Superblock*］チェックボックスを有効にすると、起動時などにRAIDパーティションが認識されるようになります。［完了］をクリックして設定を完了した後で、パーティションモジュールのエキスパートページ上にある［*RAID*］と示された`/dev/md0`デバイスと他のデバイスを観察してください。

2.3.3　トラブルシューティング

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

2.3.4 関連資料

ソフトウェアRAIDの設定方法と詳細情報が、次のHOWTOにあります。

- /usr/share/doc/packages/raidtools/Software-RAID-HOWTO.html
- http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html

Linux RAIDメーリングリストも使用できます。たとえば、http://www.mail-archive.com/linux-raid@vger.rutgers.eduなどがあります。

パート II. インターネット

3

WebブラウザKonqueror

Konquerorは、多目的のファイルマネージャであるだけではありません。これは新しいタイプのWebブラウザでもあります。パネルの［ウェブブラウザ］アイコン(地球の周囲に歯車が付いている形)をクリックすると、Konquerorは Webブラウズプロファイルを使ってブラウザとして起動されます。ブラウザとしてのKonquerorは、タブブラウズ、画像を含むWebページの保存、インターネットキーワード、およびブックマークの機能を提供し、JavaとJavaScriptをサポートします。

Konquerorは、メインメニューから起動するか、または`konqueror`コマンドを入力して起動します。Webページをロードするには、場所ツールバーにそのアドレス(`http://www.suse.com`など)を入力します。Konquerorはこのアドレスにアクセスして、ページを表示しようと試みます。アドレスの先頭にプロトコル(この場合は`http://`)を入力することは必須ではありません。アドレスをプログラムで自動的に完成させることができますが、これが確実に機能するのはWebアドレスの場合だけです。FTPアドレスについては、入力フィールドの先頭に必ず`ftp://`と入力する必要があります。

図 3.1　Konquerorのブラウザウィンドウ

3.1　タブブラウズ

一度に複数のWebページを使用することがよくある場合は、タブブラウズ機能を使用すると、ページの切り替えが容易になります。この機能は、複数のWebサイトを1つのウィンドウ内の個別のタブにロードします。これにより、デスクトップ上に1つのメインウィンドウだけが表示されるので、デスクトップを管理しやすくなります。ログアウト後は、KDEのセッション管理によって、KonquerorにWebセッションを保存できます。次回のログイン時に、最後にアクセスしたURLがロードされます。

新しいタブを開くには、［ウィンドウ］→［新しいタブ］を選択するか、Ctrl＋Shift＋Nを押します。タブの動作を設定するには、［設定］→［Konquerorを設定］を選択します。表示されるダイアログボックスで、［Web動作］→［タブブラウズ］を選択します。ウィンドウを開く代わりに新しいタブを開くには、［リンクは新しいウィンドウではなく、新規タブで開く］を有効にします。［一つのタブしかオープンしていない場合、タブバーを非

表示にする］を使用して、タブバーを非表示にすることもできます。他のオプションを表示するには、［*詳細オプション*］をクリックします。

タブをURLおよびウィンドウの位置とともにプロファイルに保存できます。この機能は、前述のセッション管理とは少し異なります。プロファイルを使用すると、保存したタブを手元に置くことができるため、セッション管理のように起動時だけではなく、いつでもタブを復元できます。

Konquerorで、*［設定］→［ビューのプロファイルを設定］*を選択して、プロファイル名を指定します。プロファイルには、該当するオプションを使用してウィンドウサイズも保存できます。［*プロファイルにURLを保存*］が選択されていることを確認します。［*保存*］をクリックします。次回「タブコレクション」が必要になったときに、*［設定］→［ビューのプロファイルを読み込み］*を選択すると、指定したプロファイル名がメニューに表示されます。名前を選択すると、タブが復元されます。

3.2 Webページと画像の保存

Konquerorでは、他のブラウザと同様にWebページを保存できます。これには、*［場所］→［名前を付けて保存］*を選択し、HTMLファイルの名前を指定します。ただし、イメージは保存されません。 イメージを含むWebページ全体をアーカイブするには、*［ツール］→［WEBページをアーカイブに］*を選択します。Konquerorは、ユーザが通常そのまま使用できるようなファイル名を提案します。ファイル名は、Webアーカイブを示す拡張子`.war`が末尾に付きます。保存したWebアーカイブを後で表示する場合は、ファイルをクリックするだけで、Konquerorにイメージとともに表示されます。

3.3 インターネットキーワード

Konquerorを使用してWeb検索を行うことは、非常に簡単です。Konquerorは、70を超える検索フィルタに対して、特定のショートカットを自動的に定義します。インターネット上で特定のトピックを検索するには、ショートカットとキーワードをコロン(:)で区切って入力します。これにより、検索結果を含むページが表示されます。

定義済みのショートカットを確認するには、*［設定］→［Konquerorを設定］*を選択します。ダイアログボックスが表示されるので、［*Web*ショートカッ

ト］を選択します。検索プロバイダとショートカットの名前が表示されます。Konquerorは、たとえば、Google、Yahoo、Lycosのような「「お馴染みの」」検索エンジンから、Acronym Database、インターネット映画データベース、KDEアプリケーション検索のような一般的にあまり使用されないフィルタまで、多数の検索フィルタを定義しています。

好みの検索エンジンがなければ、新しい検索エンジンを簡単に定義できます。たとえば、サポートデータベースで特定の記事を検索するには、通常は `http://portal.suse.com/`にアクセスして検索ページを探し、クエリを入力します。この操作はショートカットを使用して簡略化できます。ダイアログボックスで、［*新規*］を選択し、［*検索プロバイダ名*］でショートカットの名前を指定します。［*URIショートカット*］に略語を入力します。複数の略語を入力する場合は、コンマで区切って入力します。重要なテキストフィールドは［*検索URI*］です。Shift+F1を押してフィールドをクリックすると、簡単なヘルプが表示されます。検索クエリは`\{@}`で指定されます。これがチャレンジによって正しい位置に挿入されます。この場合は、SUSEサポートデータベースの設定は次のようになります。［*検索プロバイダ名*］がSUSEサポートデータベース、［*検索URI*］が(1行で) `https://portal.suse.com/PM/page/search.pm?q=\{@}&t=optionSdbKeywords&m=25&l=en&x=true`、そして［*URIショートカット*］が`sdb_en`です。

［*OK*］を2回クリックして設定を確定したら、Konquerorの場所バーにクエリを入力します。たとえば、「`sdb_en:kernel`」と入力します。結果は現在のウィンドウに表示されます。

3.4 ブックマーク

頻繁にアクセスするサイトのURLアドレスを記憶してそのつど入力する代わりに、［ブックマーク］メニューを使用すると、これらのURLをブックマークとして保存できます。この方法で、Webページのアドレスのほか、ローカルディスク上のディレクトリをブックマークとして保存することもできます。

Konquerorで新しいブックマークを作成するには、［ブックマーク］→［ブックマークに*追加*］をクリックします。以前に追加したすべてのブックマークが、メニュー項目として表示されます。さまざまな項目を見つけやすいように、ブックマークをテーマ別に階層構造に整理することをお勧めします。ブックマークの新しいサブグループを作成するには、［*新規ブックマークフォルダ*］を使用します。［ブックマーク］→［ブックマークを*編集*］を選択する

と、ブックマークエディタが表示されます。このプログラムを使用すると、ブックマークを整理、変更、削除することができます。

Netscape、Mozilla、またはFirefoxもあわせて使用している場合、ブックマークを再度作成する必要はありません。ブックマークエディタで［ファイル］、→［インポート］、［*Netscape*のブックマークをインポート］の順に選択すると、NetscapeとMozillaのブックマークを最新のブックマークに統合できます。逆方向の統合も、［*Netscape*へブックマークをエクスポート］を使用して実行できます。

ブックマークを変更するには、エントリを右クリックします。ポップアップメニューが表示されるので、切り取り、コピー、削除などのアクションを選択します。変更が完了したら、［ファイル］→［保存］を選択して、ブックマークを保存します。名前またはリンクのみ変更する場合は、ブックマークツールバーでエントリを右クリックし、［プロパティ］を選択します。名前と場所を変更し、［*Update (更新)*］をクリックします。

ブックマークのリストを保存し、それに簡単にアクセスできるようにするには、ブックマークをKonquerorに表示します。［設定］→［ツールバー］→［ブックマークツールバー*(Konqueror)*］を選択してください。現在のKonquerorウィンドウに、ブックマークパネルが自動的に表示されます。

3.5 JavaとJavaScript

この2つの言語を混同しないでください。Javaは、Sun Microsystemsによるプラットフォームに依存しないオブジェクト指向のプログラミング言語です。Javaは通常、小さなプログラム(アプレット)に使用され、オンラインバンキング、チャット、ショッピングでインターネットを経由して実行されます。JavaScriptは、主に、メニューやその他の効果などのWebページのダイナミック構造化に使用されるインタプリタスクリプト言語です。

Konquerorでは、この2つの言語を有効または無効にできます。これはドメインごとに設定できるので、一部のホストにはアクセスを許可し、他のホストへのアクセスをブロックすることができます。JavaおよびJavaScriptは、セキュリティ上の理由で無効にすることがよくあります。ただし、正しく表示するためにJavaScriptが必要なWebページもあります。

3.6 関連資料

Konquerorでの作業中に不明な点や問題が発生した場合は、*［ヘルプ］*メニューからアクセスできる、アプリケーションのハンドブックを参照してください。KonquerorのWebページ(http://www.konqueror.org)を参照することもできます。

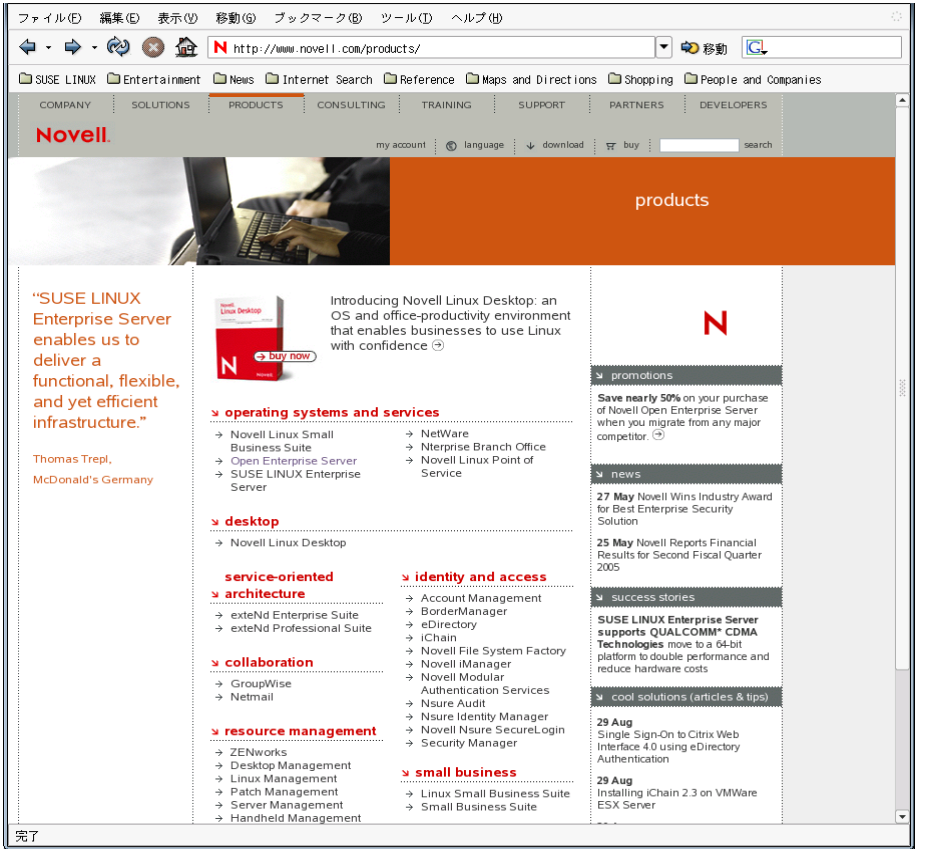
4 Firefox

SUSE Linuxには、Mozilla FirefoxのWebブラウザが付属しています。Firefoxには、タブ、ポップアップウィンドウのブロック機能、ダウンロードおよび画像管理などの、最新のWeb技術が統合されています。1つの画面で、複数のWebページを表示できます。動作を遅くするだけの、わずらわしい広告や画像を無効にできます。複数の検索エンジンに簡単にアクセスできるので、必要な情報を探しやすくなっています。メインメニューから、またはコマンド`firefox`を入力することで、このプログラムを起動します。以降では、このプログラムの主要な機能について説明します。

4.1 Webサイトのナビゲート

Firefoxのルックアンドフィールは他のブラウザととてもよく似ています。このツールを図 4.1. 「Firefoxのブラウザウィンドウ」 (page 86)に示します。ナビゲーションツールバーには、［*Forward (進む)*］と［*Back (戻る)*］、およびWebアドレスを指定するためのロケーションバーがあります。素早くアクセスするために、ブックマークを使用することもできます。Firefoxのさまざまな機能についての詳細は、［ヘルプ］メニューを使用してください。

図 4.1　Firefoxのブラウザウィンドウ



4.1.1　タブブラウズ

一度に複数のWebページを使用することがよくある場合は、タブブラウズ機能を使用すると、ページの切り替えが容易になります。この機能は、複数のWebサイトを1つのウィンドウ内の個別のタブにロードします。

タブを開くには、*[ファイル] → [New Tab (新しいタブ)]*の順に選択します。これにより、Firefoxウィンドウに空のタブが表示されます。代わりに、リンクを右クリックし、［*Open link in new tab (リンクを新しいタブで開く)*］を選択することもできます。タブそのものを右クリックすると、その他のタブオプ

ションにアクセスできます。新しいタブを作成したり、1つのタブまたは残りのすべてのタブで再読み込みしたり、またはそれらを閉じたりできます。

4.1.2 サイドバーの使用

ブラウザウィンドウの左側を使用して、ブックマークやブラウズ履歴を表示できます。拡張機能によって、サイドバーを使用するための新しい方法が追加されることがあります。サイドバーを表示するには、*[表示]* → *[サイドバー]*の順に選択し、目的のコンテンツを選択します。

4.2 情報の検索

Firefoxで情報を検索する方法は2つあります。検索バーとページ内検索バーです。検索バーがページを検索するのに対し、ページ内検索バーは現在のページに含まれている情報を検索します。

4.2.1 検索バーの使用

Firefoxには検索バーがあり、Google、Yahoo、Amazonなどのさまざまな検索エンジンにアクセスできます。たとえば、現在のエンジンでSUSEに関する情報を検索したい場合は、検索バー内をクリックしてからSUSEと入力し、Enterを押します。検索結果がウィンドウに表示されます。検索エンジンを選択するには、検索バー内のアイコンをクリックします。メニューが開き、利用可能な検索エンジンのリストが表示されます。

4.2.2 ページ内検索バーの使用

Web内を検索するには、*[編集]* → *[Find in This Page (このページの検索)]*の順にクリックするか、またはCtrl + Fを押して、ページ内検索バーを表示します。通常、このバーはウィンドウの一番下に表示されます。入力フィールドに、検索条件を入力します。Firefoxによって、条件を満たすフレーズがすべて反転表示されます。［*Highlight (反転表示)*］を使用すると、反転表示の有効と無効を切り替えられます。

4.3 ブックマークの管理

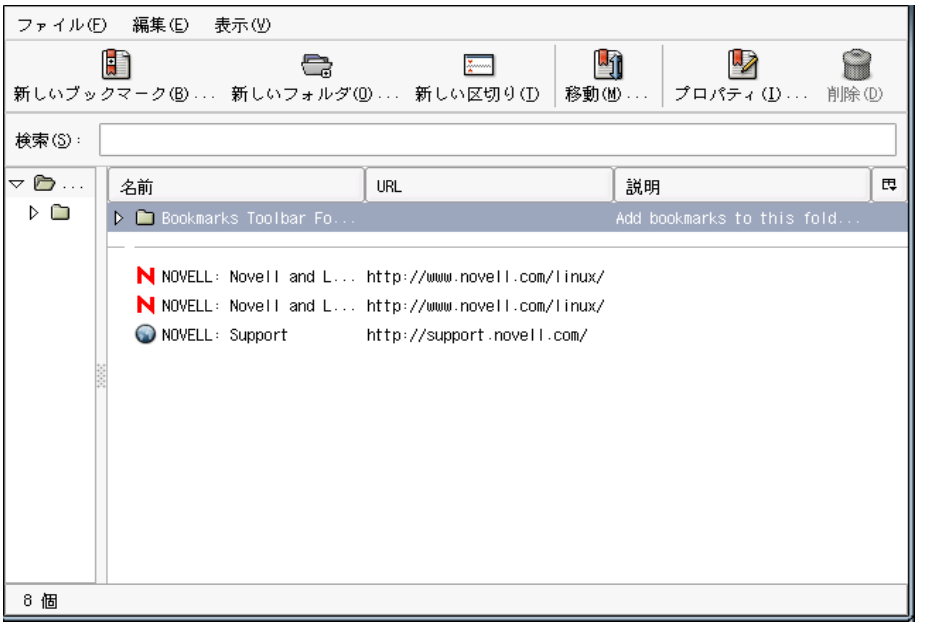
ブックマークにより、お気に入りのWebサイトへのリンクを保存しておくことができます。現在のWebサイトをブックマークのリストへ追加するには、*[ブックマーク] → [Bookmark This Page (このページをブックマーク)]*の順にクリックします。ブラウザのタブに複数のWebサイトが表示されている場合は、現在選択されているタブだけが、ブックマークのリストへ追加されます。

ブックマークを追加するときは、ブックマークの名前を新たに指定したり、Firefoxでの保存先フォルダを指定できます。 ブックマークのリストからWebサイトを削除するには、［ブックマーク］をクリックし、リスト内で対象のブックマークを右クリックしてから［*削除*］をクリックします。

4.3.1 ブックマークの管理の使用

ブックマークの管理を使用すると、各ブックマークのプロパティ(名前とURL)を管理したり、ブックマークをフォルダやセクション内に分類したりできます。この機能は、図 4.2.「Firefoxにおけるブックマークの管理の使用」(page 89)に示しています。

図 4.2　Firefoxにおけるブックマークの管理の使用



ブックマークの管理を開くには、*[ブックマーク] → [Manage Bookmarks (ブックマークの管理)]*の順にクリックします。ウィンドウが開き、ブックマークが表示されます。［*New Folder (新しいフォルダ)*］を使用すると、新しいフォルダを作成して、その名前と説明を指定できます。 新しいブックマークを作成するには、［*New Bookmark (新しいブックマーク)*］をクリックします。これにより、ブックマークの名前、場所(URL)、キーワード、および説明を指定することができます。キーワードは、ブックマークへのショートカットになります。新しく作成したブックマークをサイドバー内に表示する場合は、［*Load this bookmark in the sidebar (このブックマークをサイドバーに読み込む)*］にチェックマークをつけます。

4.3.2　ブックマークの移動

今までに別のブラウザを使用していた場合、設定内容やブックマークをFirefoxでも使用したいはずです。現在インポート可能なのは、Netscape 4.x、6、7、Mozilla 1.xおよびOperaのブックマークです。

設定内容をインポートするには、*[ファイル]* → *[インポート]*の順にクリックします。設定内容をインポートする対象ブラウザを選択します。［次へ］をクリックすると、設定がインポートされます。インポート済みのブックマークは、新しく作成された「From（から）」のついた名前のフォルダ内にあります。

4.3.3 ライブブックマーク

ライブブックマークは、最新のニュースを確認できるように、ブックマークメニュー内に見出しを表示する機能です。これにより、お気に入りのサイトの情報をすぐに見ることができるので、時間を節約できます。

多くのサイトとブログは、この形式をサポートしています。こういったWebサイトでは、右下隅に「RSS」と書かれたオレンジ色の四角形が表示されます。それをクリックして、［*ライブブックマークに追加*］を選択します。ダイアログボックスが表示されて、ライブブックマークの名前と場所を選択できます。［*追加*］クリックして確認してください。

実際にはニュースフィードをサポートしていても、そのことをFirefoxには知らせないサイトもあります。ライブブックマークを手動で追加するには、フィードのURLが必要です。次の手順に従ってください。

手順 4.1 *ライブブックマークを手動で追加する*

1. *[ブックマーク]* → *[ブックマークの管理]*でブックマークマネージャを表示します。新しいウィンドウが開きます。
2. *[ファイル]* → *[新しいライブブックマーク]*を選択します。ダイアログボックスが開きます。
3. たとえばhttp://www.novell.com/newsfeeds/rss/coolsolutions.xmlのように、ライブブックマークの名前とそのURLを入力します。Firefoxはライブブックマークを更新します。
4. ブックマークマネージャを閉じます。

4.4　ダウンロードマネージャの使用

ダウンロードマネージャを使用すると、現在行っているダウンロードおよび過去のダウンロードを管理できます。ダウンロードマネージャを開くには、*[ツール] → [ダウンロード]*の順にクリックします。Firefoxにより、ダウンロードに関するウィンドウが開かれます。ファイルのダウンロード中には、進行状況を示すバーと現在のファイルが表示されます。必要に応じて、ダウンロードを中止し、後で再開することができます。ダウンロードしたファイルを開くには、［*開く*］をクリックします。［*削除*］を使用すると、メディアからファイルを削除できます。ファイルについての情報が必要な場合は、ファイル名を右クリックし、［*プロパティ*］を選択します。

ダウンロードマネージャをもっと制御する必要がある場合は、*[編集] → [Preferences (初期設定)]*の順に選択して設定ウィンドウを開き、［ダウンロード］タブを表示します。このタブでは、ダウンロードフォルダ、ダウンロードマネージャの動作方法、ファイルタイプの設定を指定します。

4.5　Firefoxのカスタマイズ

Firefoxでは、拡張機能をインストールしたり、テーマを変更したり、オンライン検索用のキーワードを追加することで、その機能を縦横にカスタマイズできます。

4.5.1　拡張機能

MozillaFirefoxは多機能アプリケーションであり、これは、拡張機能と呼ばれるアドオンをダウンロードしてインストールできることを意味します。たとえば、最新のダウンロードマネージャやマウスジェスチャの追加などです。これにより、Firefox本体のサイズを小さいままに保つことができます。

拡張機能を追加するには、*[ツール] → [Extensions （拡張機能)]*の順にクリックします。右下隅にある［*Get More Extensions (新しい拡張機能を入手)*］をクリックして、Mozillaの拡張機能更新用Webページを表示し、利用可能な拡張機能の中から目的の機能を選択します。 インストール対象の拡張機能を選択したら、その拡張機能をダウンロードしてインストールするためのリンクをクリックします。Firefoxを再起動すると、新しく追加した拡張機能が使用で

きるようになります。さまざまな拡張機能については、http://update.mozilla.org/.でも参照できます。

図 4.3　Firefox拡張機能のインストール

4.5.2　テーマの変更

Firefoxの標準的なルックアンドフィールが気に入らない場合は、新しいテーマをインストールします。テーマを変更しても、ブラウザの外観が変わるだけで機能そのものに影響はありません。テーマをインストールしようとすると、まず、Firefoxによって確認を求められます。インストールを許可するか、またはキャンセルします。インストールが正常に完了すると、新しいテーマを有効にすることができます。

1. *[ツール]* → *[テーマ]*の順にクリックします。

2. 新しいダイアログが表示されます。［*Get More Themes (新しいテーマを入手)*］をクリックします。テーマがすでにインストールされている場合は、図 4.4.「Firefoxテーマのインストール」 (page 93)に示すように、リスト内から探します。

図 4.4　Firefoxテーマのインストール

3 新しいウィンドウが開き、Webサイト`https://update.mozilla.org`が表示されます。

4 テーマを選択し、［*Install Now*］をクリックします。

5 ダウンロードとインストールを確認します。

6 テーマのダウンロードが終了すると、ダイアログにテーマのリストが表示されます。［*Use Theme (テーマ変更)*］を使用して、新しいテーマを有効にします。

7 ウィンドウを閉じ、Firefoxを再起動します。

テーマがインストールされると、*[ツール] → [テーマ]*の順に選択してから、［*Use Theme (テーマ変更)*］を使用することで、再起動することなく、いつでも別のテーマに切り替えることができます。テーマを使用する予定がない場合は、同じダイアログで［アンインストール］を使用するとテーマを削除できます。

4.5.3 オンライン検索へのスマートキーワードの追加

インターネットでの検索は、ブラウザで実行できる主要なタスクの1つです。Firefoxでは、独自のスマートキーワードを定義できます。スマートキーワードとは、Webの検索で、「コマンド」として使用する略語のことです。たとえば、ウィキペディアを頻繁に使用する場合、スマートキーワードを使用することで、このタスクを簡略化できます。

1. `http://en.wikipedia.org`を参照してください。
2. FirefoxでWebページを表示したら、検索テキストフィールドに注目してください。フィールドを右クリックして表示されるメニューから、［*Add a Keyword for this Search (この検索にキーワードを設定)*］を選択します。
3. ［*ブックマークに追加*］ダイアログが表示されます。［*名前*］には、このWebページの名前を、たとえば「*Wikipedia (en)*」のように入力します。
4. ［キーワード］には、このWebページの略語を、たとえば「*Wiki*」のように入力します。
5. ［*Create in (作成先)*］では、ブックマークセクションにおけるエントリの場所を選択します。［クイックサーチ］内に保存することができますが、その他のフォルダでもかまいません。
6. ［*追加*］を使用して操作を完了します。

これで新しいキーワードが作成されました。ウィキペディアを調べる必要があるときは、もうURL全体を入力する必要はありません。`wiki Linux`と入力するだけで、Linuxの情報をすべて表示できます。

4.6 Firefoxからの印刷

Firefoxで、表示されたコンテンツをどのように印刷するかは、［*ページ設定*］ダイアログで設定します。*[ファイル] → [ページ設定]*の順にクリックしてから、［*Format & Options (書式とオプション)*］タブで、印刷ジョブの配置方法

を選択します。拡大/縮小または自動調整することができます。背景を印刷するには、［*Print Background (colors & images) (背景を印刷(配色と画像))*］を選択します。［*Margins & Header/Footer (余白とヘッダ/フッタ)*］タブをクリックすると、余白を調整したり、ヘッダとフッタに含める対象を選択できます。

設定を指定した後は、*[ファイル] → [印刷]*の順に選択して、Webページを印刷します。プリンタを選択するか、または出力内容を保存するファイルを選択します。［*プロパティ*］を使用すると、用紙サイズの設定、印刷コマンドの指定、グレースケールまたは色の選択、および余白の指定ができます。設定値を入力したら、［*印刷*］を使用して実行します。

4.7 関連資料

Firefoxの詳細は、オフィシャルホームページhttp://www.mozilla.org/products/firefox/で入手してください。特定のオプションや機能についての詳細は、Firefoxに統合されているヘルプを参照してください。

Linphone—Linuxデスクトップ用のVoIP

5

Linphoneは、Linuxデスクトップ用の小さなWeb電話アプリケーションです。これを使えば、インターネット上での二者通話が可能になります。特別なハードウェアは必要ありません。適切に設定されたサウンドカード、マイクロフォン、およびスピーカまたはヘッドフォンが接続された標準のワークステーションがあれば、Linphoneを使うことができます。

5.1 Linphoneの設定

Linphoneを使う前に、いくつかの基本的な事柄を決め、いくらかの設定を行う必要があります。まず、Linphoneの実行モードを決めて設定し、使用する接続タイプを決め、それからLinphoneの設定を始めて(*[Go]* → *[設定]*の順に選択)、必要な調整を行います。

5.1.1 Linphoneの実行モードを決める

Linphoneは、実行しているデスクトップのその設定のタイプに応じて、2種類のモードで実行することができます。

通常のアプリケーション
: Linphoneソフトウェアをインストールすると、GNOMEやKDEのアプリケーションメニューから、またはコマンドラインから起動できるようになります。Linphoneを実行していないときには、かかってきた電話を受信することはできません。

GNOMEパネルのアプレット

Linphoneは、GNOMEパネルに追加することができます。パネルの空白の部分を右クリックして［*パネルへ追加*］を選択し、Linphoneを選択します。Linphoneは恒久的にパネルに追加され、ログイン時に自動的に起動します。電話がかかってこない間は、バックグラウンドで実行されます。電話がかかってくると、メインウィンドウが開くので、電話を受けることができます。電話をかけるには、アプレットのアイコンをクリックしてメインウィンドウを開きます。

5.1.2 接続タイプを決める

Linphoneで電話をかけるには、何通りかの方法があります。どのように電話をかけ、相手方に接続するかは、ネットワークまたはインターネットに接続している方法に応じて決まります。

Linphoneは、リモートのホストとの接続を確立するために、SIP (session initiation protocol)を使用します。SIPでは、それぞれの通話者が、以下のようなSIP URLによって識別されます。

`sip:` *`username@hostname`*

*`username`*はLinuxマシンへのログイン名で、*`hostname`*は使用しているコンピュータの名前です。SIPプロバイダを使用している場合には、URLは次の例のようになります。

`sip:` *`username@sipserver`*

*`username`*は、SIPサーバに登録したときに選択したユーザ名です。*`sipserver`*は、SIPサーバまたはSIPプロバイダのアドレスです。登録方法についての詳細は、項5.1.5. 「SIPオプションの設定」 (page 101)を参照し、プロバイダの登録関連のドキュメントを確認してください。ご使用の目的に適したプロバイダのリストは、項5.8. 「関連資料」 (page 108)で言及されているWebページで確認してください。

使用するURLは、選択した接続のタイプに応じて決まります。SIPプロバイダによるルーティングなしに、相手側に直接電話をかける場合には、最初のタイプのURLを入力します。SIPサーバを経由して相手側に電話をかける場合には、2番目のタイプのURLを入力します。

同じネットワーク内での通話

同じネットワークに所属している友人や同僚に電話をかける場合には、正しいユーザ名とホスト名があれば、有効なSIP URLを作成できます。同じことは、相手がこちらに電話をかけようとする場合にも当てはまります。自分と相手側との間にファイアウォールがなければ、これ以上の設定は必要ありません。

ネットワークを越える、またはインターネットを使用する通話(静的IPでのセットアップ)

静的なIPアドレスを使用してインターネットに接続している場合、相手側が電話をかけてきたいときには、こちらのユーザ名と、ワークステーションのホスト名またはIPアドレスがあれば、同じネットワーク内での通話項 (page 99)で説明されているように有効なSIP URLを作成できます。こちら側、または相手側が、着信および発信トラフィックのフィルタ処理を行うファイアウォールの背後にいる場合には、Linphoneのトラフィックがファイアウォールを通過できるように、SIPポート(5060)およびRTPポート(7078)を開いてください。

ネットワークを越える、またはインターネットを使用する通話(動的IPでのセットアップ)

お使いのIPセットアップが静的でなく、インターネットに接続するたびに新しいIPアドレスを動的に取得している場合には、どの相手側からも、こちら側のユーザ名とIPアドレスに基づいて有効なSIP URLを作成することは不可能です。このような場合には、SIPプロバイダから提供されているサービスを使うか、またはDynDNSセットアップを使用して、外部の相手側が正しいホストマシンに接続できるようにしてください。DynDNSの詳細については、http://en.wikipedia.org/wiki/Dynamic_DNSを参照してください。

ネットワークおよびファイアウォールを越える通話

ファイアウォールの背後に隠れているマシンは、そのIPアドレスをインターネットに公開しません。そのため、そのようなマシンを使用しているユーザに電話をかけようとしても、直接接続することはできません。Linphoneは、SIPプロキシの使用、または通話をSIPプロバイダに転送することにより、ネッ

トワークやファイアウォールを越えた通話をサポートします。外部のSIPサーバを使用するために必要な調整についての詳細は、項5.1.5.「SIPオプションの設定」 (page 101)を参照してください。

5.1.3 ネットワークパラメータの設定

［ネットワーク］タブのほとんどの設定は、調整する必要はありません。これらを変更しなくても、そのまま通話することができるはずです。

NAT Traversal Options

このオプションは、ファイアウォールの背後のプライベートネットワークに接続していて、通話を転送するSIPプロバイダを使用しない場合にのみ、有効にします。チェックボックスをオンにして、ファイアウォールのIPアドレスを`192.168.34.166`のようなドット表記で入力してください。

RTPのプロパティ

Linphoneは、通話の音声データを転送するのに、RTP (real-time transport protocol)を使用します。RTPのポートは`7078`に設定されています。他のアプリケーションがこのポートを使っている場合以外には、変更しないでください。ジッタ補正(jitter compensation)のパラメータは、Linphoneがオーディオパッケージを実際に再生する前にどの程度バッファするかを制御します。このパラメータを大きくすれば、転送音声の品質は改善されます。バッファするパッケージの数を増やせば、「遅れて届いたパッケージ」も再生できる可能性が大きくなります。一方、バッファするパッケージの数を増やすと、レイテンシも大きくなり、相手の声がいくらか送れて聞こえるようになります。このパラメータを変更するときには、これらの2つの要素のバランスに注意してください。

Other

VoIPと通常の電話を組み合わせて使う場合、DTMF (dual tone multiplexed frequency)テクノロジを使って特定の動作をトリガし、特定のキーを押すとボイスメールをリモートチェックする、などの設定が行えるようにしたいと思うかもしれません。Linphoneは、DTMF伝送の2つのプロトコル、SIP INFOおよびRTP rfc2833をサポートしています。LinphoneでDTMF機能が必要な場合、これらのプロトコルのいずれかをサポートしているSIPプロバイダを選択してください。VoIPプロバイダの詳しいリストは、項5.8.「関連資料」 (page 108)を参照してください。

5.1.4 サウンドデバイスの設定

サウンドカードがLinuxによって正しく検出されていれば、Linphoneは自動的に、検出されたデバイスをデフォルトのサウンドデバイスとして使用します。［*使用するサウンドデバイス*］はそのままにしておいてください。［*録音する音源*］では、どの録音ソースを使うかを決めます。ほとんどの場合、これはマイクロホンになるでしょう(マイク入力)。カスタムの呼び出し音を選択するには、［*参照*］でいずれかを選択し、［*Listen*］でテストします。［*適用*]をクリックして、変更内容を確認します。

5.1.5 SIPオプションの設定

［*SIP*］ダイアログには、SIP関連のすべての設定が含まれています。

SIPのポート
SIPユーザエージェントが動作するポートを決めます。デフォルトのSIPのポート番号は5060です。他のアプリケーションまたはプロトコルがこのポートを必要としていない限り、デフォルト設定は変更しないでください。

個人情報
相手側がSIPプロキシやSIPプロバイダを使わずに直接電話をかけたいと思う場合には、こちら側の有効なSIPアドレスを知っている必要があります。Linphoneは、有効なSIPアドレスを作成します。

リモートのサービス
このリストには、ユーザアカウントを作成した1つまたは複数のSIPサービスプロバイダを記述します。サーバ情報はいつでも追加、修正、削除できます。登録の手順についての詳細は、SIPプロキシの追加とリモートのSIPサーバへの登録 (page 102)を参照してください。

Authentication Information
リモートのSIPサーバに登録するには、パスワードやユーザ名など、特定の認証データを入力する必要があります。Linphoneは、いったん入力されたデータを保管します。セキュリティ上の理由のためにこのデータを破棄するには、［*Clear all stored authentification data*］をクリックします。

［*リモートのサービス*］リストには、リモートのSIPプロキシやサービスプロバイダの複数のアドレスを設定できます。

手順 5.1　SIPプロキシの追加とリモートのSIPサーバへの登録

1. 適切なSIPプロバイダを選択し、そこにユーザアカウントを作成します。
2. Linphoneを開始します。
3. ［*Go]* → *[Preferences]* → *[SIP]*の順に選択します。
4. ［*Add proxy/registrar*］をクリックして、登録フォームを開きます。
5. ［*Registration Period][SIP Identity][SIP Proxy*］および［*Route*］に適切な値を入力します。ファイアウォールの背後から使用する場合には、［*Send registration*］をオンにして、［*Registration Period*］に適切な値を入力します。これにより、一定の時間が経過した後にオリジナルの登録データを再送信して、Linphoneが必要とするポートをファイアウォールに開け続けさせることができます。こうしないと、ファイアウォールがこのタイプのパッケージを受け取らなかった場合、これらのポートは自動的に閉じられます。登録データの再送信は、SIPサーバに、接続の現在のステータスおよび発信側の場所を知らせ続けさせるためにも必要です。［*SIP identity*］には、ローカルの通話の場合に使用するSIP URLを入力します。このサーバをSIPプロキシとしても使用するには、［*SIP Proxy*］にも同じ値を入力します。最後に、必要であればオプションとしてルート情報を入力し、［*OK*］をクリックしてダイアログを閉じます。

5.1.6　オーディオコーデックの設定

Linphoneは、音声データの伝送のために、複数のコーデックをサポートしています。接続のタイプを設定し、リストウィンドウで使用したいコーデックを選択してください。現在の接続タイプに適していないコーデックは赤い色で表示され、選択することはできません。

5.2　Linphoneのテスト

Linphoneの設定は、Linphoneからの呼び出しに応答する小さなテストプログラムである`sipomatic`を使ってチェックできます。

手順 5.2　Linphoneのセットアップのテスト

1. 端末を開きます。
2. コマンドラインプロンプトに`sipomatic`と入力します。
3. Linphoneを開始します。
4. ［*SIP address*］アドレスとして`sip:robot@127.0.0.1:5064`を入力し、［*電話をかける 電話に出る*をクリックします。
5. Linphoneが正しく設定されていれば、呼び出し音が鳴り、少ししてから短いメッセージが聞こえます。

この手順が成功した場合には、オーディオのセットアップとネットワークのセットアップは正しく動作しています。このテストに失敗した場合には、サウンドデバイスが正しく設定されていて、再生のレベルが適切な値に設定されているかどうかをチェックしてください。それでも何も聞こえない場合には、SIPとRTPのポート番号を含む、ネットワーク設定をチェックしてください。他のアプリケーションやプロトコルが、Linphoneが使用することになっているこれらのデフォルトのポートを使用している場合には、ポートを変更してから、再試行してみてください。

5.3　電話をかける

いったんLinphoneを正しく設定すれば、電話は簡単にかけられます。通話のための手順は、通話のタイプ(項5.1.2.「接続タイプを決める」 (page 98)を参照)に応じて少し違います。

1. メニューまたはコマンドラインからLinphoneを起動します。
2. ［*SIPアドレス*］に、相手のSIPアドレスを入力します。アドレスは、直接電話をかける場合には`sip:username@domainname`または`username@hostname`のように、プロキシやSIPプロバイダのサービスを使用する場合には`username@sipserver`または`userid@sipserver`のようになります。

3 SIPサービスプロバイダやプロキシを使用している場合には、*Proxy to use*から適切なプロキシまたはプロバイダを選択し、このプロキシで必要な認証データを入力します。1

4 ［*電話をかける 電話に出る*］をクリックして、相手が電話を受けるのを待ちます。

5 通話が終わった、または終わらせる場合には、［*電話を切る 会話を拒否*］をクリックして、Linphoneを終了します。

通話中にサウンドのパラメータを調整する必要が生じた場合には、［*詳細*］をクリックします。さらに多くのオプションがある4つのタブが表示されます。最初の［サウンド］タブには、［*受話音量*］と［*送話音量*］のオプションがあります。必要に合わせてスライダで調整してください。

［*状態*］タブでは、自分の現在のオンライン状態を設定できます。この情報は、相手が電話をかけようとしたときに伝えることができます。長い時間席を離れていて、このことを相手に知らせたい場合には、［*退席中*］を選択します。しばらくの間忙しいものの、後ほどまた連絡してほしい場合には、［*今席をはずしています。...分*］を選択して、連絡可能になるまでの時間を指定します。連絡可能になったら、状態をデフォルト(［*在席中*］)に戻してください。相手側がこちらのオンライン状態をチェックできるかどうかは、項5.5.「電話帳を使用する」 (page 105)で説明しているように、電話帳の［*Subscribe Policy*］で設定できます。電話帳に載っている相手のオンライン状態は、［*My online friends*］タブでモニタすることができます。

［*DTMF*］タブでは、ボイスメールをチェックするためのDTMFコードを入力できます。ボイスメールをチェックするには、適切なSIPアドレスを入力し、［*DTMF*］タブのキーパッドを使って、ボイスメールのコードを入力します。最後に、通常の電話をかける場合と同じように、［*電話をかける 電話に出る*］をクリックします。

5.4 電話に出る

Linphoneで選択した実行モードに応じて、着信を知るための複数の方法があります。

通常のアプリケーション
: 着信は、Linphoneがすでに実行している場合にのみ、受け付けて応答することができます。着信音は、ヘッドセットまたはスピーカから聞こえます。Linphoneを実行していないときには、電話を受けることはできません。

GNOMEパネルのアプレット
: 通常、Linphoneのパネルアプレットは、目立たない仕方で動作しています。着信があると、Linphoneのメインウィンドウが表示され、着信音がヘッドセットまたはスピーカから聞こえます。

着信に気づいたら、*電話をかける* *電話に出る*をクリックすれば、電話を取って会話を始めることができます。電話に出たくない場合には、［*電話を切る* *会話を拒否*］をクリックします。

5.5 電話帳を使用する

Linphoneには、SIPによる連絡先を管理する機能があります。電話帳を開くには、*[Go]* → *[電話帳]*の順に選択します。空白のリストが表示されます。連絡先を追加するには、［*追加*］をクリックします。

有効な連絡先を作成するには、以下のエントリを入力する必要があります。

名称
: 連絡先の名前を入力します。フルネームも入力できますが、またはニックネームも使用できます。相手をすぐに思い出せるような名前を選んでください。相手のオンライン状態を表示するように選択すると、メインウィンドウの［*My online friends*］タブにその名前が表示されます。

SIPアドレス
: 連絡先の有効なSIPアドレスを入力します。

Proxy to Use
: 必要な場合には、この接続で使用するプロキシを入力します。ほとんどの場合、これは使用するSIPサーバのSIPアドレスになります。

Subscribe Policy
: サブスクライプポリシー(subscribe policy)では、自分の在席または退席の状態を相手に知らせるかどうかを決めます。

電話帳に載っている連絡先に電話をかけるには、マウスで連絡先を選択し、［*選択する*］をクリックします。メインウィンドウのアドレスのフィールドにそのアドレスが表示されるので、通常のように［*電話をかける 電話に出る*］で電話をかけます。

5.6 トラブルシューティング

電話をかけようとしましたが、接続を確立することができません。
通話に失敗する理由としては、いくつかの事柄が考えられます。

インターネットへの接続が切れています。
Liphoneは通話を中継するためにインターネットを使用するので、コンピュータがインターネットに正しく接続されていて、設定されているかどうか確認してください。これは、ブラウザでWebページを表示できるかどうか試してみれば、簡単にわかります。インターネット接続が正しい場合には、相手側が連絡可能でないのかもしれません。

電話をかけようとした相手に連絡できません。
相手が会話を拒否している場合には、接続することはできません。こちらから電話をかけようとしたときに、相手のマシン上でLinphoneが実行されていない場合には、接続することはできません。相手のインターネット接続が切れている場合には、接続することはできません。

電話をかけてつながったようですが、何も聞こえません。
まず、サウンドデバイスが正しく設定されているかどうか確認してください。そのためには、メディアプレーヤなど、サウンド出力を使う他のアプリケーションを起動してみます。Linphoneに、このデバイスを開くためのパーミッションが与えられているかどうか確認してください。リソースの競合を避けるため、サウンドデバイスを使う他のすべてのプログラムを閉じてください。

上でチェックした点がすべて正常なのに、やはり何も聞こえない場合には、［*サウンド*］タブで受話音量を上げてください。

両方の側のサウンドが奇妙に歪んでいます。
*[設定]→[ネットワーク]*の順に選択し、［*RTPのプロパティ*］で、音声パッケージの遅れを補正するために、ジッタバッファを調整してみてください。その場合には、レイテンシが大きくなることに注意してください。

DTMFが動作しません。

DTMFパッドを使ってボイスメールをチェックしようとしたのに、接続が確立されませんでした。DTMFデータの伝送には3種類のプロトコルが使われていますが、Linphoneがサポートしているのは2種類だけです(SIP INFOおよびRTP rfc2833)。プロバイダがこれらのいずれかをサポートしているかどうかチェックしてください。Linphoneが使用するデフォルトのプロトコルはrfc2833ですが、これでうまく行かないようなら、*[設定]* → *[ネットワーク]* → *[Other]*の順に選択して、プロトコルをSIP INFOに設定してください。どちらのプロトコルでも動作しない場合には、LinphoneでDTMF伝送を行うことはできません。

5.7 用語集

このドキュメントで使用されている最も重要な専門用語とプロトコルについて、簡単に説明します。

VoIP

*voice over Internet protocol*の略です。このテクノロジにより、通常の電話の通話を、パケットでリンクされたルートにより、インターネット上で伝送することができます。音声情報は、IPによってインターネット上で伝送される他のデータと同様に、パケットに分割されて送信されます。

SIP

*session initiation protocol*の略です。このプロトコルは、ネットワーク上でメディアセッションを確立するために使用されます。Linphoneの場合、SIPは、相手側のマシン上で呼び出し音を鳴らし、通話を開始して、どちらかが会話を終えたら通話を終了させるための働きをします。音声データの実際の伝送はRTPによって扱われます。

RTP

*real-time transport protocol*の略です。UDP上で動作し、ネットワーク上でメディアストリームを伝送することを可能にします。データは、番号が付けられ、タイムスタンプに従って運ばれる個別のパケットによって伝送されます。これによって、データを正しい順番に並べて、パッケージが失われた場合に検出することができます。

DTMF

DTMF円コーダは、通常の電話と同じように、様々なキーを表す2種類のトーンを使います。それぞれのキーは、高いトーンと低いトーン1つずつ

の、個別の組み合わせと関連付けられています。デコーダは、これらのトーンの組み合わせを、数字に戻します。LinphoneはDTMFのシグナルをサポートしており、ボイスメールのチェックなど、リモートの動作をトリガすることができます。

コーデック
コーデックとは、オーディオおよびビデオデータを圧縮するために特別に設計されたアルゴリズムのことです。

ジッタ
ジッタとは、接続内でのレイテンシ(遅れ)のばらつきのことです。オーディオデバイスや、ISDNやPSTNのような接続指向のシステムは、データの連続したストリームを必要とします。この点を補正するために、VoIPの端末とゲートウェイにはジッタバッファが実装されており、パケットをいったん集めてから、オーディオデバイスや(ISDNのような)接続指向のラインに中継します。ジッタバッファのサイズを大きくすれば、データが失われる可能性は小さくなりますが、接続のレイテンシは大きくなります。

5.8 関連資料

VoIPについての一般的な情報は、http://voip-info.org/tiki-index.phpのVoIP Wikiをチェックしてください。お住まいの国でVoIPサービスを提供しているプロバイダの広範なリストは、http://voip-info.org/wiki-VOIP+Service+Providers+Residentialを参照してください。

6 KGpgによる暗号化

KGpgは、Linuxシステムの暗号化インフラストラクチャのうち、重要なコンポーネントです。このプログラムの支援を得て、必要とされるすべての鍵の生成と管理を行います。 そのエディタ機能を使用してファイルの迅速な作成と暗号化するか、パネル内にあるアプレットを使用して、ドラッグ&ドロップ形式で暗号化または復号化することができます。電子メールプログラム(KontactまたはEvolution)のような他のプログラムは、鍵データにアクセスして、署名済みまたは暗号化済みの内容を処理します。この章では、暗号化済みファイルに関する毎日作業する上で必要になる基本的な機能について説明します。

6.1 新しい鍵ペアの生成

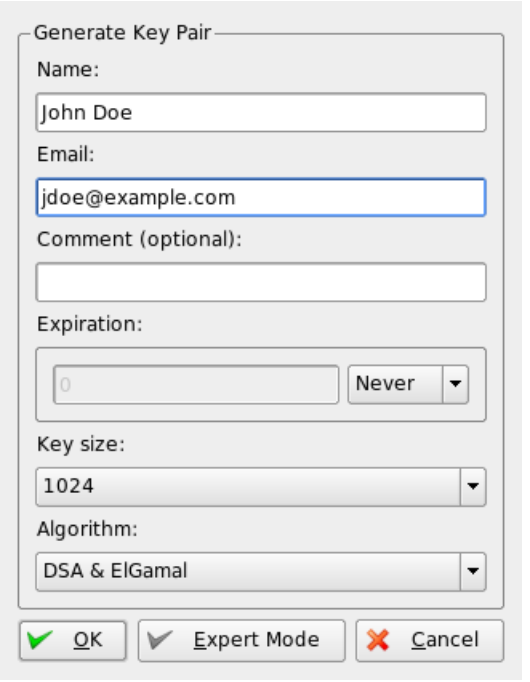
暗号化済みメッセージを他のユーザとの間で交換するには、最初に自分専用の鍵ペアを生成します。その1つである*公開鍵*(公開キー)は、通信相手に対して配布するものであり、通信相手はファイルや電子メールメッセージを送信する前に、公開鍵を使用してそれらを暗号化します。鍵ペアのもう一方は、*秘密鍵*(秘密キー)です。 これは、暗号化済みの内容を復号化する目的で使用されます。

重要項目: 秘密鍵と公開鍵

公開鍵は、公開されること、およびすべての通信相手に対して配布されることを意図しています。一方、秘密鍵にアクセスするのはそれを所有しているユーザだけです。秘密鍵のデータにアクセスすることを他のユーザに許可しないでください。

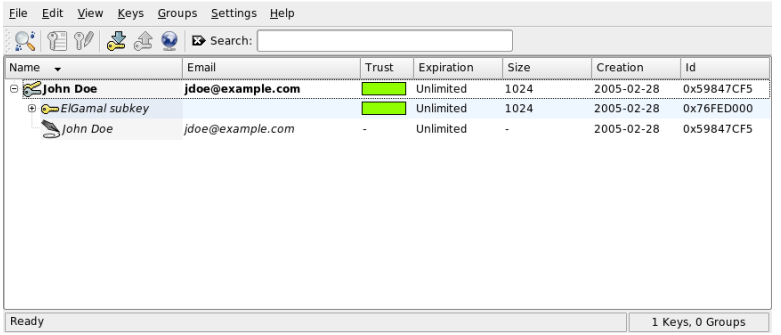
KGpgを開始するには、メインメニューで*[ユーティリティ]* → *[KGpg]*の順に選択するか、コマンドラインでkgpgと入力します。プログラムを初めて起動すると、設定手順を支援するアシスタントが開きます。鍵の作成が要求される時点まで、アシスタントの指示に従って進みます。名前と電子メールアドレス、そして必要に応じて、コメントを入力します。デフォルト設定が適当でない場合は、鍵の有効期限、サイズ、および使用する暗号化アルゴリズムも設定します。図 6.1. 「KGpg:キーの作成」 (page 110)を参照してください。

図 6.1 *KGpg:キーの作成*



入力した設定を確認して、［*OK*］をクリックします。次に、パスワードを2回入力するように求めるダイアログが表示されます。次にプログラムによって鍵ペアが生成され、概要が表示されます。失効証明書をすぐに保存または印刷することをお勧めします。この証明書は、秘密鍵のパスワードを忘れた場合に鍵を無効にするときに必要になります。［*OK*］をクリックすると、KGpgのメインウィンドウが表示されます。図6.2.「鍵マネージャ」 (page111)を参照してください。

図 6.2　鍵マネージャ



6.2　公開鍵のエクスポート

鍵ペアを生成した後で、公開鍵を他のユーザが利用できるようにします。その結果、他のユーザが自分(鍵生成者)にメッセージやファイルを送信する前に、その公開鍵を使用して暗号化または署名できるようになります。公開鍵を他のユーザが利用できるようにするには、*[鍵] → [公開鍵をエクスポート]* の順に選択します。ダイアログが表示され、4つのオプションが表示されます。

電子メール
公開鍵は、選択した受信者へ電子メールで送信できます。このオプションを選択し、［*OK*］をクリックしてその選択結果を確定した場合は、KMailで新しい電子メールを作成するためのダイアログが開きます。受信者を入力し、［*送信*］をクリックします。受信者は、生成された鍵を受信し、その後は、暗号化された内容を鍵生成者へ送信することができます。

クリップボード
鍵生成者は自分の公開鍵の操作を続ける前に、その公開鍵をクリップボードに書き込んでおくことができます。

デフォルト鍵サーバ
自分の公開鍵を幅広いユーザが利用できるようにするには、インターネット上に存在する鍵サーバのいずれかにその鍵をエクスポートします。詳細については、項6.4.「鍵サーバダイアログ」 (page 113)を参照してください。

ファイル
自分の鍵を電子メールで送信する代わりに、データメディア上のファイルとしてその鍵を配布することもできます。このオプションをクリックし、ファイルのパスと名前をデフォルト値のままにするか変更を加え、［*OK*］をクリックします。

6.3 鍵のインポート

ファイルの形で(たとえば、電子メールへの添付物として)鍵を受け取った場合、［*鍵をインポート*］を使用してその鍵を自分の鍵束に統合し、その送信者との間で暗号化された通信を行う場合にその鍵を使用します。この手順は、既に説明した、鍵をエクスポートする手順に似ています。

6.3.1 鍵への署名

他のファイルと同様に、鍵に署名して、その鍵の正当性と整合性を保証することもできます。インポート済みの鍵が、所有者として明示されている個人に所属していることが確かな場合は、その鍵に自分が署名することにより、その鍵の正当性を自分が信頼していると表明することができます。

重要項目: 信頼の連鎖の確立

暗号化された通信がセキュア(安全)であるのは、配布されている公開鍵を、指定されたユーザに積極的に関連付けている場合だけです。それらの鍵を互いにチェックし、署名することは、信頼の連鎖の確立につながります。

鍵リストの中にある、署名する鍵を選択します。*[鍵] → [鍵に署名]*の順に選択します。続いて表示されるダイアログで、署名に使用する秘密鍵を指定します。署名する前に、その鍵の正当性を確認するよう注意する警告が表示されます。この確認を行った後で、［*続行*］をクリックし、次のステップで、選択した秘密鍵に対応するパスワードを入力します。他のユーザは、自分への公開鍵を使用することにより、その署名をチェックできます。

6.3.2 鍵の信頼レベル

通常、対応するプログラムによって、鍵を信頼しているかどうか（承認された所有者が本当にその鍵を使用していると考えているかどうか）について問い合わせされます。この問い合わせは、メッセージを復号化する、または署名を確認する必要があるたびに行われます。これを防ぐには、新しくインポートした鍵の信頼レベルを編集します。

新しくインポートした鍵を右クリックすると、鍵管理用の小さなコンテキストメニューにアクセスできます。そのメニューから［*ターミナル内で鍵を編集*］を選択します。KGpgによってテキストコンソールが開かれます。その中で、いくつかのコマンドを実行して信頼レベルを設定します。

テキストコンソールのプロンプト(`Command >>`)で、`trust`と入力します。インポートした鍵に署名したユーザが、この鍵の所有者の真の身元をチェックしたことについてどれだけ信頼しているかを表すために、`1`(信頼してよいか不明な場合)から`5`(確実に信頼してよい場合)の範囲で数値を割り当てます。`Your decision?`プロンプトで、選択した値を入力します。署名したユーザが確実に信頼できる場合は、`5`と入力します。`y`を入力することにより、続く質問に回答します。最後に、`quit`と入力してコンソールを閉じ、鍵のリストへ戻ります。その結果、この鍵は、`Ultimate`の信頼レベルを持つようになりました。

鍵束内における鍵の信頼レベルは、鍵名の隣にある色の付いたバーにより表示されます。信頼レベルがより低ければ、鍵が署名された真の身元を確認する鍵の署名者をより信頼していないことを意味します。署名者の身元が確実に信頼できる場合でも、鍵を署名する前に他の人々の身元を確認する事を署名者が怠る可能性があります。したがって、署名者と署名者の鍵を信頼しても、署名者により署名された他の鍵については低い信頼レベルを使用して署名できます。信頼レベルの目的は一種のリマインダです。KGpgによって自動的にアクションがトリガされることはありません。

6.4 鍵サーバダイアログ

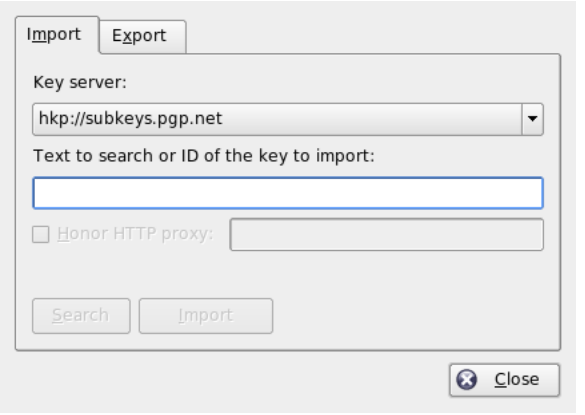
インターネットベースの鍵サーバのいくつかは、多くのユーザの公開鍵を提供しています。多くのユーザとの間で暗号化された通信を実施するには、それらのサーバを使用して、公開鍵を配布します。この目的を果たすには、公

開鍵をそれらのサーバのいずれかにエクスポートします。同様に、KGpgを使用して、特定のユーザに対応する鍵を保持しているそれらのサーバのいずれかを検索すること、またはサーバからそれらのユーザの公開鍵をインポートすることができます。*[ファイル] → [鍵サーバダイアログ]*の順に選択して、鍵サーバダイアログを開きます。

6.4.1 鍵サーバからの鍵のインポート

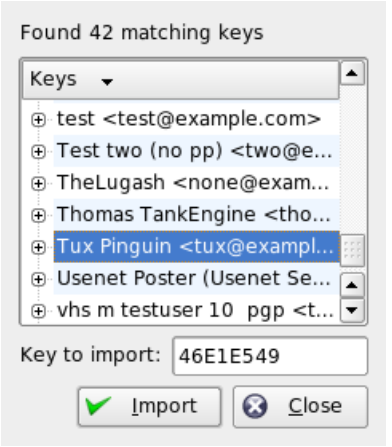
［鍵サーバ］ダイアログの［*インポート*］タブを通して、インターネットベースの鍵サーバのいずれかから公開鍵をインポートします。ドロップダウンメニューを使用して、構成済みの鍵サーバのいずれかを選択し、検索文字列(通信相手の電子メールアドレス)または検索する鍵のIDを入力します。*検索*] をクリックすると、使用中のシステムがインターネットに接続し、指定された鍵サーバから、指定に一致する鍵を検索します。詳細については、図6.3.「鍵をインポートするための検索画面」 (page 114)を参照してください。

図 6.3　鍵をインポートするための検索画面



鍵サーバに対する検索が成功した場合、取得したすべてのサーバエントリからなるリストが新しいウィンドウ内で表示されます。鍵束に含めたい鍵を選択し、［*インポート*］をクリックします。図 6.4.「検索成功とインポート」(page 115)を参照してください。メッセージが表示されたら［*OK*］をクリックして確認し、［*閉じる*］をクリックして［鍵サーバ］ダイアログを閉じます。これで、インポート済みの鍵は、［鍵マネージャ］のメインウィンドウ内にある概要の中で表示され、使用可能になります。

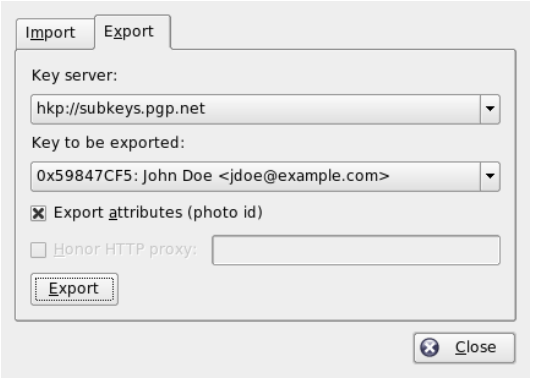
図 6.4　検索成功とインポート



6.4.2　鍵サーバへの鍵のエクスポート

鍵を、インターネット上で自由にアクセス可能な鍵サーバのいずれかにエクスポートするには、［鍵サーバ］ダイアログの［エクスポート］タブを選択します。2つのドロップダウンメニューを使って、エクスポート先のサーバと、エクスポートする鍵を指定します。次に、［エクスポート］を使用して、エクスポートを開始します。

図 6.5　鍵サーバへの鍵のエクスポート



6.5 テキストとファイルの暗号化

KGpgを使用して、テキスト、またはクリップボードの内容を暗号化することもできます。錠前のアイコンをクリックすると、［*クリップボードを暗号化*］および［*クリップボードを復号化*］の各オプションや、内蔵エディタを開くためのオプションが表示されます。

6.5.1 クリップボードの暗号化と復号化

クリップボードへコピーしたファイルは、数回のクリックで簡単に暗号化できます。［KGpg］アイコンをクリックすると、メニューが表示されます。このメニューから、［*クリップボードを暗号化*］を選択し、使用する鍵を指定します。暗号化の手順に関するステータスメッセージがデスクトップ上に表示されます。必要に応じて、この時点で、暗号化済みの内容をクリップボードから取得し、処理を進めることができます。クリップボードの内容を復号化する作業も簡単です。同じように、［KGpg］アイコンを右クリックしてメニューを表示し、［*クリップボードを復号化*］を選択し、自分の秘密鍵に関連付けられているパスワードを入力します。この時点で、利用可能な復号化済みのバージョンが、クリップボード内、およびKGpgのエディタ内にあります。

6.5.2 ドラッグ&ドロップによる暗号化と復号化

ファイルを暗号化または復号化するには、デスクトップまたはファイルマネージャ内でそのファイルのアイコンをクリックし、パネル内にある錠前までそれらをドラッグし、そこでそのアイコンをドロップします。そのファイルがまだ暗号化されていない場合、KGpgは、どの鍵を使用するのか問い合わせてきます。ユーザが鍵を選択した時点で、そのファイルは暗号化されます。他のメッセージは表示されません。ファイルマネージャ内では、暗号化済みのファイルは、`.asc`というサフィックス(接尾辞)付きで表示され、錠前のアイコンも付いています。それらのファイルを復号化するには、ファイルのアイコンをクリックし、パネル内にあるKGpgのシンボルまでドラッグし、そこでそのアイコンをドロップします。その後、ファイルを復号化して保存するのか、それともエディタ内で表示するのかを選択します。

6.5.3 KGpgのエディタ

暗号化する目的で、外部エディタの中で内容を作成し、上記の方法のいずれかを使用してファイルを暗号化する代わりに、KGpgの内蔵エディタを使用してファイルを作成することができます。エディタを開き(コンテキストメニューから［*エディタを開く*］を選択します)、必要なテキストを入力し、［*暗号化*］をクリックします。次に、使用する鍵を選択し、暗号化の手順を完了させます。ファイルを復号化するには、［*復号化*］を使用し、秘密鍵に関連付けられているパスワードを入力します。

署名の生成と確認は、エディタから直接暗号化するのと同様に簡単です。*[署名]→[署名を作成]*の順に選択し、表示されるダイアログから、署名するファイルを選択します。次に、使用する秘密鍵を指定し、それに関連付けられているパスワードを入力します。KGpgから、署名の生成に成功したことが通知されます。単純に［*署名/確認*］をクリックする方法で、エディタからファイルに署名することもできます。署名済みのファイルを確認するには、*[署名]→[署名を確認]*の順に選択し、続いて表示されるダイアログで、確認するファイルを選択します。ユーザが選択結果を了承した後に、KGpgは署名を確認し、その結果が報告されます。もう1つの手段は、署名済みのファイルをエディタ内にロードし、［*署名/確認*］をクリックすることです。

6.6 関連資料

暗号化の手法に関する理論的な背景情報については、`http://www.gnupg.org/documentation/howtos.html.en`にあるGnuPGプロジェクトページを参照してください。 簡潔で明瞭な説明があります。このドキュメント内で、他の情報ソースからなるリストも参照できます。

パート III. マルチメディア

7

Linux環境のサウンド

Linuxには、幅広いサウンドとマルチメディアのアプリケーションが含まれます。一部のアプリケーションはメインのデスクトップ環境の構成要素になっています。ここで説明するアプリケーションを使用すると、再生のボリュームとバランスを調整し、CDと音楽ファイルを再生し、各自のオーディオデータを録音して圧縮できます。

7.1 ミキサー

ミキサーは、音量、サウンド出力とコンピュータの入力のバランスをコントロールする使いやすい方法です。多様なミキサー間の相違点には、ユーザインタフェースの外観も含まれています。ただし、特定のハードウェア用に設計されたミキサーもあります。たとえば、envy24controlはEnvy 24サウンドチップ専用のミキサーです。もう1つの例は、RME Hammerfallカード専用のhdspmixerです。使用可能なミキサーの中から、ニーズに最適なミキサーを選択します。

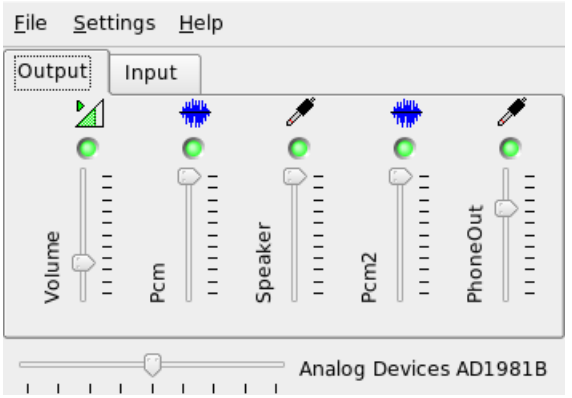
ティップ: ミキサーのテスト

一般に、ミキサーアプリケーションは、他のサウンドアプリケーションより前に開いておくことをお勧めします。ミキサーを使用して、サウンドカードの入力と出力のコントロール設定を調整します。

7.1.1 KDEミキサーアプレット

KMixは、KDEミキサーアプリケーションです。KMixは、システムトレーの小さなパネルアプレットとしてKDEパネルに統合されています。パネルアイコンをクリックすると、コントロールスライダを使用してスピーカのボリュームを調整できます。アイコンを右クリックすると、KMixのコンテキストメニューが表示されます。サウンド出力をオフにする場合は、［ミュート］を選択します。パネルアイコンの外観が変化します。再び［ミュート］をクリックすると、ボリュームのミュートが解除されます。サウンド設定を微調整するには、［ミキサーウィンドウを表示］を選択し、［*出力*］、［*入力*］、および［スイッチ］を設定します。設定するデバイスには、デバイスアイコンを右クリックして表示されるそれぞれのコンテキストメニューがあります。各デバイスは、個別にミュートまたは隠すことができます。

図 7.1　KMix ミキサー

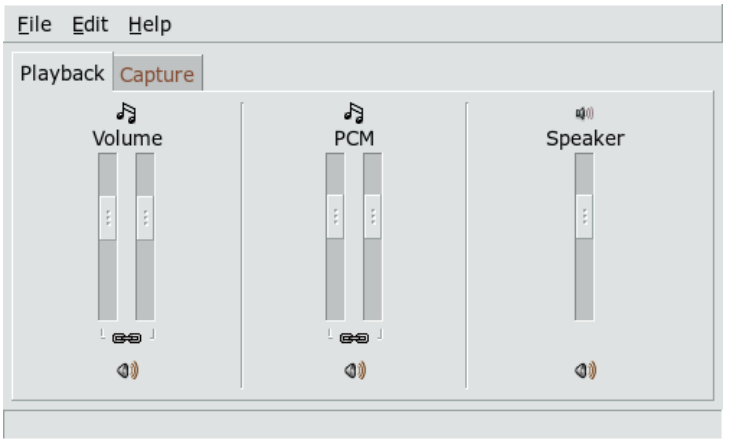


7.1.2 GNOMEミキサーアプレット

GNOMEデスクトップ用のボリュームコントロールアプレットであるGMixは、GNOMEパネルに統合されています。パネルアイコンをクリックすると、簡単なコントロールスライダを使用してスピーカのボリュームを調整できます。サウンド出力をオフにするには、アイコンを右クリックして［ミュート］を選択します。ボリュームコントロールアイコンの外観が変化します。サウンド出力のミュートを解除するには、再びアイコンを右クリックして［ミュート］を選択します。［*Open Volume Control (ボリュームコントロールを開く)*］

を選択すると、図 7.2. 「GNOMEミキサーアプレット」 (page 123)に示すミキサーの高度な機能にアクセスできます。各サウンドデバイスには、それぞれのミキサータブがあります。

図 7.2　GNOMEミキサーアプレット



7.1.3　alsamixer

alsamixerは、X環境を使用せずにコマンドラインから実行できるため、キーボードショートカットのみを使用して完全に制御できます。alsamixerウィンドウは、常に、次の要素で構成されます。最初の行にはカードとチップのタイプに関する基本情報、選択されている表示タイプ、ミキサー項目が表示され、情報エリアの下にはボリュームバーが表示されます。画面にすべてのコントロールが表示されない場合は、←キーと→キーを使用して左または右にスクロールします。コントロールの名前はコントロールの下に表示され、選択されているコントロールは赤で表示されます。すべてのミキサーコントロールは、Mキーを使用してミュートとミュートの解除を切り替えることができます。ミュートされているコントロールの名前の下には［*MM*］と表示されます。キャプチャ(録音)機能を持っているコントロールには、赤のキャプチャフラグが表示されます。

alsamixerには、［*再生*］、［*Capture (キャプチャ)*］、および［*All (すべて)*］の3つのビューモードがあります。デフォルトでは、alsamixerは［*再生*］モードで起動されるため、再生に関連するミキサーコントロール(マスタボリューム、PCM、CDなど)のみが表示されます。［*Capture (キャプチャ)*］を選択す

ると、録音に使用するコントロールのみが表示されます。［*All (すべて)*］を選択すると、使用できるすべてのコントロールが表示されます。ビューモードの切り替えには、F3、F4、およびF5を使用します。

チャネルを選択するには、→と←、またはNとPを使用します。ボリュームを調整するには、↑と↓、または+と-を使用します。ステレオチャネルを個別に制御することもできます。ボリュームを大きくするにはQ、W、およびEを使用し、ボリュームを小さくするにはZ、X、およびCを使用します。0～9までの数字キーは、絶対ボリュームをすばやく変更するために使用できます。各数字キーは、最大ボリュームの0～90パーセントに対応します。

7.1.4 ミキサーアプリケーションのルックアンドフィール

alsamixerのルックアンドフィールは、使用するサウンドカードのタイプによって異なります。SB Live!などの一部のドライバには制御(チューニング)可能な多くのミキサー要素があり、プロ用のサウンドカードのドライバにはまったく異なる名前の要素があります。

オンボードサウンドチップ

ほとんどのPCIオンボードサウンドチップは、AC97コーデックに基づいています。［マスタ］を使用すると、前面スピーカのメインボリュームを調整できます。［サラウンド］、［*中央*］、および［*LFE*］を使用すると、リアスピーカ、センタースピーカ、およびバスブーストスピーカを調整できます。各スピーカには、ミュートスイッチがあります。さらに、［ヘッドホン］と［マスタモノラル］ボリュームがあるボードもあります。後者は一部のラップトップの内蔵スピーカに使用されています。

［*PCM*］は、デジタルWAVE再生の内部ボリュームレベルを制御します。PCMは、デジタル信号形式の1つであるPulse Code Modulationの略称です。このコントロールには、個別のミュートスイッチがあります。

［*CD*］、［ライン］、［マイク］、［*補助入力*］などのその他のボリュームは、対応する入力からメイン出力までのループバックボリュームを制御します。これらは再生ボリュームのみに影響し、録音レベルには影響しません。

録音する場合は、［*Capture (*キャプチャ*)*］スイッチをオンにします。これがマスタ録音スイッチです。［*Capture (*キャプチャ*)*］ボリュームは、録音の入力ゲインです。このスイッチは、デフォルトでゼロに設定されます。［ライン］または［*録音*］などの録音ソースを選択します。録音ソースは排他のため、同時に2つのソースを選択することはできません。［*Mix (*ミックス*)*］は、特別な録音ソースです。このソースからは、再生中の信号を録音できます。

AC97コーデックチップによっては、3D、低音/高音などの特殊効果も使用できます。

SoundBlaster Live!とAudigyファミリ

SoundBlaster Live!とSB Audigy1には、AC97コーデックチップとDSPエンジンのための多くのミキサーコントロールがあります。これまでに説明したコントロールに加えて、内部信号のルーティング、PCMの減衰、WaveTable MIDI、およびAC97ミキシングを制御するための［ウェーブ］、［*音楽*］、および［*AC97*］ボリュームがあります。すべてを再生する場合は、ボリュームを100%にします。SB Audigy2(モデルに依存)のコントロールはSB Liveより少ないですが、［ウェーブ］と［*音楽*］コントロールはあります。

SB Liveの録音機能は、オンボードチップと同様です。再生されているPCMとWaveTableの信号を録音するための追加録音ソースとしては、［ウェーブ］と［*音楽*］を選択できます。

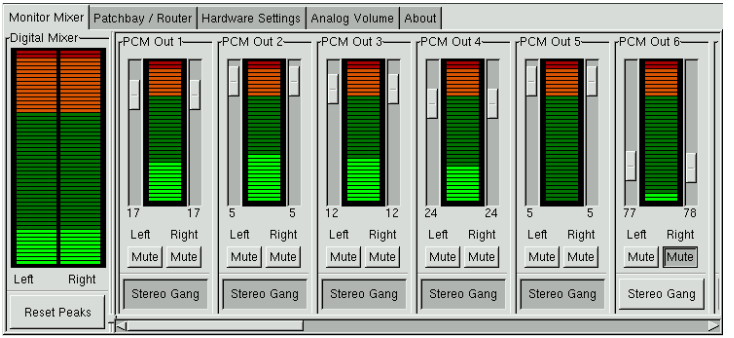
USBオーディオデバイス

USBオーディオデバイスのミキサーコントロールの数は一般的に多くはありません。何もない場合もあります。ほとんどのデバイスには、再生ボリュームを調整するための［マスタ］または［*PCM*］コントロールスイッチがあります。

7.1.5 サウンドチップEnvy24対応のミキサー

envy24controlは、Envy24 (ice1712)チップを搭載したサウンドカード用のミキサーアプリケーションです。Envy24チップの柔軟性の結果、サウンドカードごとにその機能は異なります。このサウンドチップに関する最新情報は、`/usr/share/doc/packages/alsa-tools/envy24control`ファイルに記載されています。

図 7.3　envy24controlのモニタとデジタルミキサー



envy24controlの[*Monitor Mixer*]タブには、サウンドカード内でデジタルにミキシング可能な信号レベルが表示されます。［*PCM Out*]と指定された信号は、PCMデータをサウンドカードに送るアプリケーションにより生成されます。アナログ入力信号は、[*H/W In*]に表示されます。［*S/PDIF*]入力は、右側に表示されます。[*Analog Volume*]タブでアナログチャネルの入力レベルと出力レベルを設定します。

[*Monitor Mixer*]スライダを使用して、デジタルミキシングを行います。それぞれのレベルが[*Digital Mixer*]に表示されます。各出力チャネルの[*Patchbay*]タブには、チャネルソースを選択するための一連のラジオボタンがあります。

アナログからデジタルおよびデジタルからアナログへのコンバータ用のアンプを[*Analog Volume*]で調整します。出力チャネルには［*DAC*］スライダを使用し、入力チャネルには［*ADC*］スライダを使用します。

S/PDIFチャネルの設定は、[ハードウェアの設定]タブで行います。Envy24チップは音量の変更に、[*Volume Change*]で設定可能な遅延時間の経過後に反応します。

7.2　マルチメディアプレーヤー

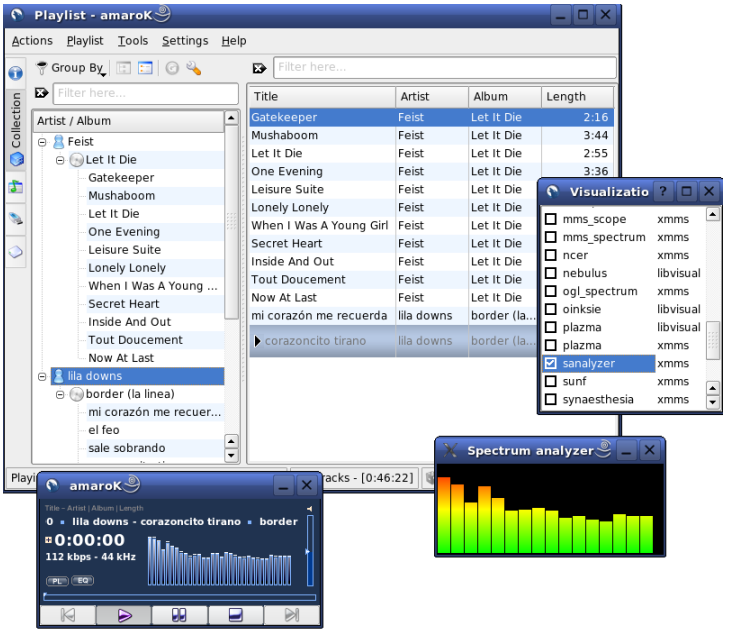
7.2.1　amaroK

amaroKメディアプレーヤーはさまざまなオーディオ形式に対応し、インターネットラジオ局のストリーミングオーディオ放送を再生できます。amaroKは

バックエンドとして動作するサウンドサーバがサポートするファイルタイプを処理できます(現在はaRtsまたはGStreamer)。

amaroKは最初に、amaroKをセットアップするための［*初回起動ウィザード*］を起動します。このステップで、amaroKのルックアンドフィールを設定できます。プレーヤーとプレイリストを個別のウィンドウに表示するか(図 7.4. 「amaroKメディアプレーヤー」 (page 127)を参照)、1つのウィンドウに統合するかを選択します。2番目のステップでは、amaroKが音楽コレクションを探す場所を指定します。amaroKは、指定されたフォルダをスキャンして再生可能なメディアを探します。デフォルトでは、amaroKは選択されているフォルダを再帰的に(すべてのサブディレクトリを含めて)スキャンし、ディレクトリの内容の変化を監視し、そこに含まれるすべてのプレイリストをインポートするように設定されます。ウィザードで指定したすべての設定は、*[ツール] → [初回起動ウィザード]*を使用して後で再びウィザードを起動して変更できます。

図 7.4　amaroKメディアプレーヤー



プレイリストの管理

amaroKは起動時にウィザードで指定した設定に基づいて、ファイルシステムのマルチメディアファイルをスキャンします。プレイリストウィンドウの右側には、見つかったプレイリストが表示されます。曲タイトルは、好みの順番で並べることができます。プレイリストが見つからない場合は作成されます。これには、ウィンドウの左側のサイドバーを使用するのが最適です。一番左に、さまざまなビューを開くためのいくつかのタブがあります。これらの各ビューから、個々のタイトルまたはディレクトリ全体をドラッグし、プレイリストにドロップして、プレイリストに追加します。次に、各タブの機能について説明します。

[関連情報]

このタブには、各自のコレクションおよび現在のアーティストに関する情報が表示されます。たとえば、好きな曲に関する情報、コレクションに追加された新しい曲などの詳細を表示できます。［*Home (ホーム)*］ビューには、各自のリスニング傾向、お気に入りリスト、最新リスト、および再生頻度が最も少ないトラックの統計情報が表示されます。［*現在のトラック*］には、再生中のトラックに関するアルバムカバー(カバーマネージャ項(page 129)を参照)、このトラックのリスニング統計情報などのデータが表示されます。トラックの歌詞が必要な場合は、［*Lyrics*］タブを使用して表示します。

［Collection Browser (コレクションブラウザ)］

このタブは、曲タイトルの個人コレクションを管理し、表示するために使用します。このビューには、さまざまな場所からのファイルを含めることができます。ツールバーのレンチのアイコンによって、音楽ファイルをスキャンする場所を指定できます。ディレクトリを選択すると、スキャンは自動的に始まります。スキャン結果はツリー構造で表示されます。［*第1階層*]と[*第2階層*]を使用して、[*アルバム*]、[*アーティスト*]、[*ジャンル*]、[*年*]の各基準に従って、ツリーの最初と2番目のブランチを整理します。ツリービューが完成したら、入力フィールドにタイトルを入力することにより、タイトルを検索できます。o入力を始めると自動的に、ツリービュー内の最初に一致するエントリに移動します。コレクションデータを更新するには、*[ツール] → [コレクションを再スキャン]*の順に使用してファイルシステムの再スキャンを開始します。

［Playlist Browser (プレイリストブラウザ)］

プレイリストブラウザは、2つの部分に分かれています。上部のリストには、プレイリストウィンドウにトラックをドラッグして［*プレイリストに*

名前をつけて保存］をクリックして作成したすべてのカスタムプレイリストが表示されます。プレイリストの内容を表示するには、プレイリストの名前の横の［+］をクリックします。プレイリストを変更するには、ドラッグアンドドロップ操作を使用します。プレイリストをロードするには、目的のプレイリストをダブルクリックします。

重要項目: 他のプレーヤーとのプレイリストの共有

プレイリストは、同じ形式を使用する他のプレーヤーと共有できるように、`m3u`または`pls`形式で保存してください。

---

amaroKでは、便利なプレイリスト(「Smart Playlists (スマートプレイリスト)」)を編成できます。プレイリストブラウザの下のリストを使用してスマートプレイリストを選択するか、［*スマートプレイリスト作成*］をクリックしてカスタムスマートプレイリストを定義します。名前、検索条件、順序、および、必要に応じてトラック数の上限を入力します。

[ファイル]
このタブはファイルブラウザを開きます。これは、ファイルシステムを操作する通常のコントロールを含む、標準のKDEファイル選択ダイアログに対応しています。テキスト入力フィールドに、URLまたはディレクトリを直接入力します。表示されたコンテンツから要素をプレイリストにドラッグして、プレイリストに追加します。特定のファイル内で、あるファイルを再帰検索することもできます。ファイルを検索するには、タイトルのテキスト文字列を入力し、検索を開始する場所を指定します。次に、[*検索*]を選択します。検索結果は、ウィンドウの下側に表示されます。

カバーマネージャ

amaroKでは、カバーマネージャを使用して再生するアルバムの音楽とイメージデータを照合できます。［*カバーマネージャ*］は、*[ツール]* → *[カバーマネージャ]*の順に選択して起動します。ウィンドウの左側のツリービューには、コレクションのすべてのアルバムが表示されます。Amazonから取得されるカバーは、ウィンドウの右側に表示されます。［*表示*］を使用して、カバーリストビューに表示する内容を選択します。［*全てのアルバム*］を選択すると、カバーイメージがあるかどうかに関係なく、コレクションのすべてのアルバムが表示されます。［*カバー取得済みアルバム*］を選択するとカバーがあるアルバムのみが表示され、［*カバー未取得アルバム*］を選択するとカバーがないアルバムが表示されます。カバーデータを取得するには、［*Amazonの*

ロケール］を選択し、［*未取得のカバーを取得*］を選択します。amaroKは、コレクションに含まれるすべてのアルバムのカバーを取得しようとします。

効果

イコライザ、ステレオバランス、ホール効果など、音響効果を有効にし、設定するダイアログを開くには、プレーヤーウィンドウで[*FX*]ボタンを選択するか、amaroKのアプリケーションメニューを使用します。希望する効果を選択し、可能であれば、各効果の設定を調整します。

視覚化

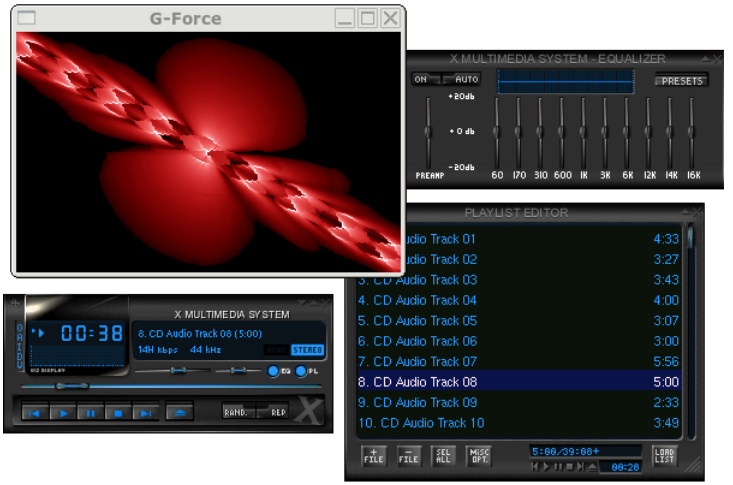
amaroKには、再生されている音楽に対するグラフィカル効果を表示するいくつかの視覚化機能が含まれています。プレーヤーウィンドウには、amaroK自体に含まれている視覚化機能が表示されます。アニメーションをクリックすると、表示モードを切り替えることができます。

前述の視覚化機能に加え、amaroKではXMMSメディアプレーヤーの視覚化プラグインもサポートされています。これらのプラグインを使用するには、`xmms-plugins`パッケージをインストールし、その後にamaroKメニューの[ビジュアライゼーション]を選択します。使用可能なプラグインをリストするウィンドウが開きます。XMMSプラグインは常に別のウィンドウに表示されます。場合によっては、フルスクリーンモードで表示するためのオプションが表示されることもあります。プラグインによっては、アクセラレイティッドグラフィックスカードを使用していない限り、スムーズな視覚効果が得られないこともあります。

7.2.2 XMMS

XMMSもまた、多様なオーディオサポート機能を提供するフル機能のメディアプレーヤーです。XMMSでの音楽の再生時には、音の途切れはほとんど発生しません。このアプリケーションの使用方法は簡単です。メニューを表示するボタンがプログラムウィンドウの左上隅にあります。GNOMEのルックアンドフィールを希望するユーザのために、XMMSのGTK2バージョンである、Beep Media Playerもあります。`bmp`パッケージをインストールしてください。ただし、XMMSのこのバージョンでは、サポートされていないXMMSプラグインもあります。

図 7.5　XMMSおよびそのEqualizer、OpenGL Spectrum Analyze、Infinityの各プラグイン



*[オプション] → [設定] → [オーディオ入出力プラグイン]*で、出力プラグインモジュールを選択します。`xmms-kde`パッケージがインストールされている場合、aRtsサウンドサーバをここで設定できます。

重要項目: Disk Writerプラグインの使用

XMMSは、設定されているサウンドカードが見つからない場合、その出力を自動的に[*Disk Writer Plugin (Disk Writerプラグイン)*]にリダイレクトします。この場合、再生したファイルは、WAVファイルとしてハードディスクに保存されます。時間表示は、出力をサウンドカードを使用して再生するより速くなります。

---

*[オプション] → [設定] → [視覚化プラグイン]*の順に使用して、各種の視覚化プラグインを起動します。3Dアクセレーション機能があるグラフィックカードの場合、OpenGLスペクトルアナライザなどのアプリケーションを選択します。`xmms-plugins`パッケージがインストールされている場合、Infinityプラグインを試してみます。

メニューボタンの下には5つのボタンがあり、異なる文字(O、A、I、D、U)が付いています。この5つのボタンによって、追加メニュー、ダイアログ、およ

び設定にすばやくアクセスできます。［*PL*］を使用してプレイリストを開き、［*EQ*］を使用してイコライザを開きます。

7.3 CD：再生とリッピング

音楽トラックを再生するには、多くの方法があります。CDを再生するか、そのデジタル化バージョンを再生します。ここでは、CDプレーヤーアプリケーションをいくつか取り上げ、オーディオCDをリッピングしてエンコードするためのアプリケーションについても説明します。

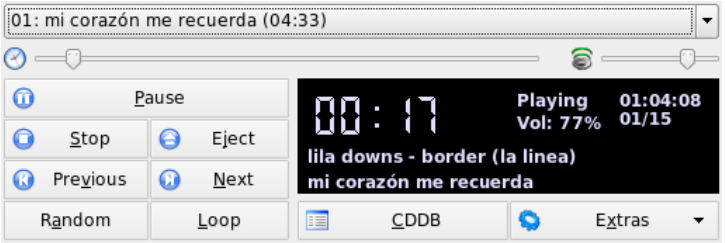
重要項目: CDDAとアナログCDの再生

オーディオCDを再生するには、2つの方法があります。アナログCDを再生できるCD/DVDドライブは、オーディオデータを読み出してサウンド出力デバイスに送ります。PCMCIA、FireWire、またはUSBを使用して接続されている外付けドライブは、CDDA (Compact Disk Digital Audio)を使用してオーディオデータを抽出してからデジタルPCMとして再生する必要があります。ここで取り上げるプレーヤーはCDDAをサポートしていません。CDDAのサポートを必要とする場合は、XMMSを使用してください。

7.3.1 KsCD—オーディオCDプレーヤー

KsCDは使いやすいオーディオCDプレーヤーです。KsCDはKDEタスクバーに統合して、CDが挿入されると自動的に再生されるように設定できます。設定メニューにアクセスするには、*[エクストラ] → [Configure KsCD (KsCDの設定)]*の順に選択します。KsCDは、インターネットでCDDBサーバからアルバムとトラック情報を取得するように設定できます。CDDB情報をアップロードして他のユーザと共有することもできます。情報の取得とアップロードには、［*CDDB*］ダイアログを使用します。

図 7.6　KsCDのユーザインタフェース



7.3.2　GNOME CDプレーヤーアプレット

これは、GNOMEパネルに統合される簡単なアプレットです。ツールアイコンを使用して、このアプレットの動作を設定し、テーマを選択します。プレーヤーウィンドウの下部のボタンを使用するか、パネルアイコンまたはプレーヤーウィンドウを右クリックして表示されるコンテキストメニューを使用して再生を制御します。

7.3.3　オーディオデータの圧縮

オーディオ圧縮は、さまざまなツールによって実行できます。ここでは、コマンドラインを使用してオーディオデータをエンコードして再生する方法について説明します。一部のグラフィカルアプリケーションにはオーディオ圧縮機能もあります。

オーディオデータのエンコードと再生のためのコマンドラインツール

Ogg Vorbis (`vorbis-tools`パッケージ)は無償のオーディオ圧縮形式で、現在では大部分のオーディオプレーヤーおよびポータブルMP3プレイヤーでもサポートされています。このプロジェクトのWebページは`http://www.xiph.org/ogg/vorbis`です。

SUSE Linuxには、Ogg Vorbisをサポートするツールが付属します。`oggenc`は、WAVファイルをOggにエンコードするために使用するコマンドラインツールです。指定された`.wav`ファイルをOgg Vorbisに変換するには、`oggenc`

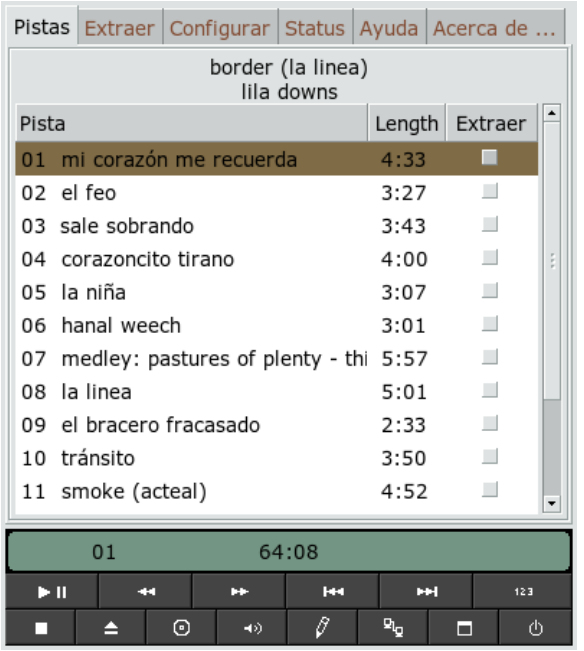
*myfile.wav*を実行します。-hオプションで、その他のパラメータの概要が表示されます。Oggencは可変ビットレートでのエンコードをサポートします。この方法で、より高度な圧縮も実現できます。ビットレートの代わりに、必要な品質を-qパラメータで指定することもできます。-bパラメータは、平均ビットレートを決定します。-mと-Mを使用すると、最小と最大のビットレートを指定できます。

ogg123は、コマンドラインOggプレーヤーです。`ogg123 mysong.ogg`などのコマンドを使用して起動します。

Gripによるオーディオデータの圧縮

GripはGNOME CDプレーヤーとリッパーです(図 7.7.「Gripによるオーディオ CDのリッピング」 (page 135)を参照)。CDプレーヤー機能は、ウィンドウ下部のボタンを使用して制御します。リッピングとエンコードの機能は、ウィンドウ上部のタブを使用して制御します。トラックとアルバムの情報を表示して編集したり、リッピングするトラックを選択するには、［トラック］タブを開きます。トラックを選択するには、トラックのタイトルの横のチェックボックスをクリックします。トラックの情報を編集するには、［*Toggle disc editor (ディスクエディタのトグル)*］をクリックして変更内容を送信します。［リップ］タブを使用すると、リップモードを選択し、リッププロセスを制御できます。Grip全体の設定にアクセスするには、［設定］タブを使用します。［*Status (ステータス)*］を使用してアプリケーションのステータスを確認します。

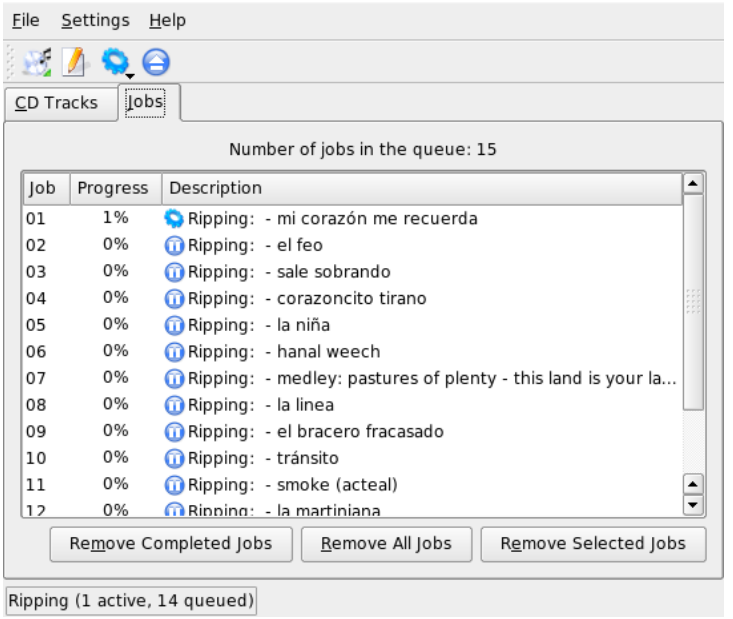
図 7.7　Gripによるオーディオ CDのリッピング



KAudioCreatorによるオーディオデータの圧縮

は、軽量のCDリッパーアプリケーションです(図 7.8. 「KAudioCreatorによるオーディオCDのリッピング」 (page 136)を参照)。KAudioCreatorを起動すると、CDのすべてのトラックが［*CD*トラック］タブに表示されます。リップしてエンコードするトラックを選択します。トラック情報を編集するには、*[ファイル]→[アルバムを編集]*の［アルバムエディタ］を使用します。または、*[ファイル]→[リッピングを選択]*の順に選択してリッピングとエンコードを開始します。このジョブの処理状況は、［ジョブ］タブを使用して確認します。KAudioCreatorは選択内容に応じてプレイリストファイルを生成することもできます。amaroK、XMMSなどのプレーヤーは、これを使用して再生できます。

図 7.8　KAudioCreatorによるオーディオCDのリッピング



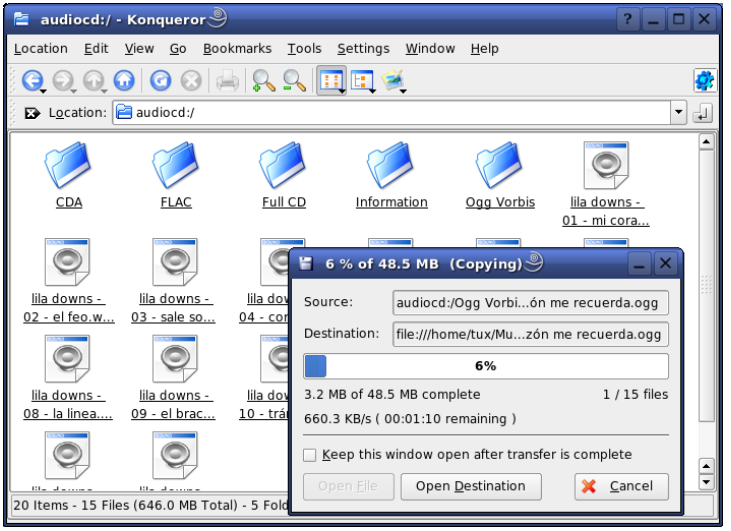
KonquerorによるオーディオCDの圧縮

Konquerorを使用して実際のリッピングプロセスを開始する前に、KDEコントロールセンターでオーディオCDとOgg Vorbisエンコーダの処理方法を設定します。*[サウンド&マルチメディア]* → *[オーディオCD]*の順に選択します。設定モジュールは、［*一般*］、［*名前*］、および［*Ogg Vorbis Encoder (Ogg Vorbis エンコーダ)*］の3つのタブに分割されます。通常、適切なCDデバイスが自動的に検出されます。自動検出が失敗し、CDデバイスを手動で設定する必要がない限り、このデフォルト設定を変更しないでください。エラー修正およびエンコーダー優先度もここで設定できます。［*Ogg Vorbis Encoder (Ogg Vorbis エンコーダ)*］タブでは、エンコードの品質を指定します。リッピングしたオーディオデータのアルバム、トラック、およびアーティストの情報をオンラインで検索するように設定するには、［*トラック情報の追加*］を選択します。

リッピングプロセスは、CDをCD-ROMデバイスに挿入し、［*場所*］バーに「`audiocd: /`」と入力して開始します。Konquerorは、CDとフォルダのトラッ

クを表示します(図 7.9. 「Konquerorによるオーディオデータのリッピング」(page 137)を参照)。

図 7.9　Konquerorによるオーディオデータのリッピング

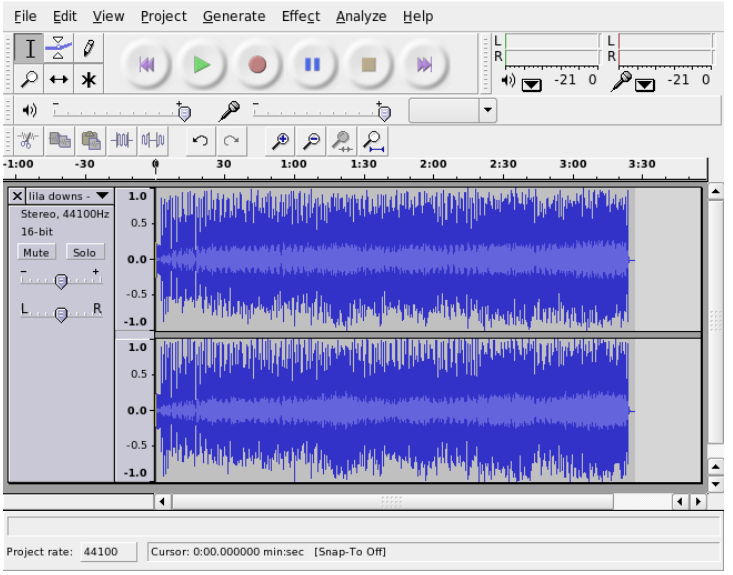


解凍されたオーディオデータをディスクに保持するには、`.wav`ファイルを選択して別のKonquerorウィンドウにドラッグし、最終保存場所にコピーします。Ogg Vorbisのエンコードプロセスを開始するには、`Ogg Vorbis`フォルダを別のKonquerorウィンドウにドラッグします。Ogg Vorbisフォルダを目的の場所にドロップすると、すぐにエンコードが始まります。

7.4 Audacityによるハードディスク録音

audacity (`audacity`パッケージ)を使用して、オーディオファイルを録音して編集します。これはハードディスク録音と呼ばれます。プログラムを初めて起動した時点で、言語を選択します。それ以外の場合、*[ファイル] → [初期設定] → [インタフェース]*で言語を設定します。言語の変更が有効になるのは、プログラムの次回の起動時です。

図 7.10　オーディオデータと特殊ビュー



7.4.1　WAVファイルの録音とファイルのインポート

赤い録音ボタンをクリックして、空のステレオトラックを生成し、録音を開始します。標準のパラメータを変更するには、*[ファイル] → [初期設定]*で必要な設定を行います。[*Audio I/O*] [*Quality*]は、録音時に重要です。トラックが既に存在する場合でも、録音ボタンを押すことにより、新しいトラックが作成されます。初期状態では、このようなトラックを標準サイズのプログラムウィンドウで見ることはできないため、紛らわしいかもしれません。

オーディオファイルをインポートするには、*[プロジェクト] → [Import Audio]*の順に選択します。このプログラムは、WAV形式と圧縮されたOgg Vorbis形式をサポートします。この形式の詳細については、項7.3.3.「オーディオデータの圧縮」 (page 133)を参照してください。

7.4.2 オーディオファイルの編集

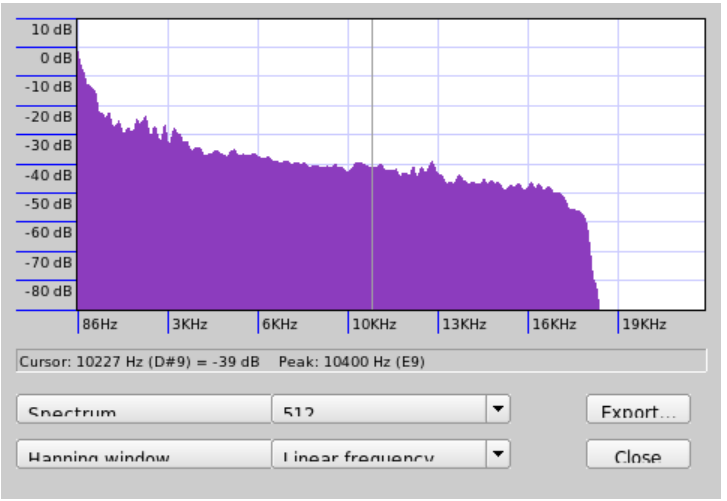
トラックの左の［*オーディオトラック*］メニューを開きます。このメニューには、各種のビューと基本的な編集操作のためのオプションがあります。トラックの名前を変更するには、［*名前*］を選択して新しい名前を入力します。Audacityには、［*波形*］、［*波形(dB)*］、［*Spectrum (スペクトル)*］、および［*Pitch (ピッチ)*］ビューがあります。必要に応じてビューを選択します。ステレオトラックの各チャネルを個別に編集する場合は、［*Split Track (トラックの分割)*］を選択します。各チャネルが個別のトラックとして処理されます。各トラックに対して、［*Sample Format (サンプル形式)*］(ビット)と［*Sample Rate (サンプルレート)*］(Hz)を設定します。

［*編集*］メニューにあるほとんどのツールは、使用する前に編集するトラックのチャネルとセグメントを選択する必要があります。選択すると、すべての種類の変更と効果を適用できるようになります。

*[View] → [Set Selection Format]*には、選択したファイルの種類に応じて、セグメント選択用のビュー形式があります。[*Set Snap-To Mode*]では、セグメント境界は自動的に選択したビューの形式に合わせて調整されます。たとえば、[*PAL frames*]をビュー形式として選択して、[*Snap-To*]をアクティブにした場合、セグメント境界は常に複数のフレームで選択されます。

すべての編集ツールにはツールヒントが表示されるため、使いやすくなっています。*[View] → [History]*で利用できる[*Undo History*]機能では、最近行った編集ステップを表示して、リストをクリックすることにより元に戻すことができます。[*Discard*]を使用すると、リストから編集ステップが削除されるため注意してください。削除した処理を元に戻すことはできません。

図 7.11　スペクトル



内蔵のスペクトルアナライザは、ノイズを迅速に追跡するのに役立ちます。選択したセグメントのスペクトルは、*[View]* → *[Plot Spectrum]*の順に選択して表示します。オクターブ内の対数周波数軸は、[*Log frequency*]を使用して選択します。マウスポインタをスペクトル内に移動すると、ピークの周波数が、対応する音符と共に自動的に表示されます。

不要な周波数は、*[Effect]* → *[FFT Filter]*の順に選択して削除します。フィルタ処理と関連して、[*Amplify*]を使用してシグナルの振幅を再調整する必要が生じることがあります。さらに、［*Amplify (増幅)*］を使用して振幅を確認します。デフォルトでは、[*New Peak Amplitude*]は0.0dBに設定されています。この値は、選択したオーディオ形式の最大限の振幅を表しています。［*Amplification*]は、選択したセグメントをこのピーク振幅にまで増幅するのに必要な値を示しています。負の値は、増幅過多であることを示しています。

7.4.3　保存とエクスポート

プロジェクト全体を保存するには、*[ファイル]* → *[プロジェクトを保存]*または[*Save Project As*]を選択します。これにより、拡張子が.aupのXMLファイルが生成されます(内容はプロジェクトの説明です)。実際のオーディオデータは、プロジェクト名の後に_dataを追加した名前のディレクトリに保存されます。

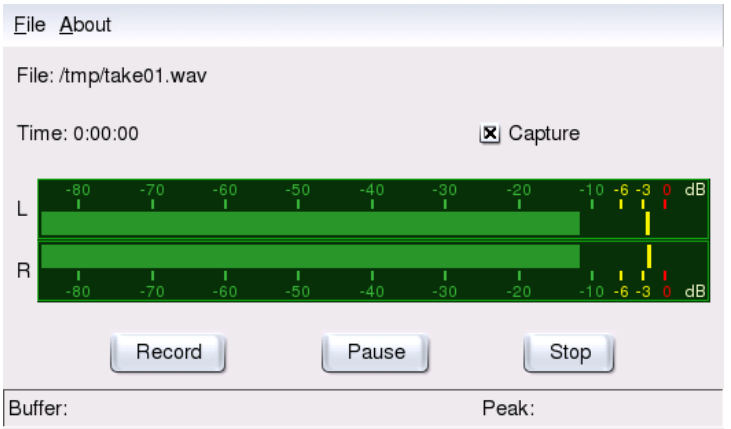
プロジェクト全体または現在選択されているセグメントも、ステレオ WAV ファイルとしてエクスポートできます。プロジェクトをOgg Vorbis形式でエクスポートするには、項7.3.3.「オーディオデータの圧縮」 (page 133)を参照してください。

7.5 WAVファイルの直接録音と再生

alsaパッケージのarecordコマンドとaplayコマンドは、PCMデバイスにシンプルで柔軟なインタフェースを提供します。arecordコマンドとaplayコマンドを使用すると、WAVおよびその他の形式のオーディオデータを録音および再生できます。arecord -d 10 -f cd -t wav mysong.wavコマンドは、10秒間のWAVファイルをCD品質(16ビット、44.1kHz)で録音します。arecordコマンドとaplayコマンドのすべてのオプションのリストが、各コマンドで--helpを指定すると表示されます。

qaRecord(kalsatoolsパッケージ)は、グラフィカルインタフェースとレベル表示のシンプルな録音プログラムです。このプログラムは約1MBの内部バッファ(--buffersizeオプションで設定可能)を使用するため、低速ハードウェアでも中断のない録音が可能です。特に、リアルタイムの優先度で実行する場合に効果的です。録音中に、現在使用中のバッファサイズが[*Buffer*]の下にあるステータス行に表示されます。そして、この録音に必要な最大バッファサイズが[*Peak*]の下に表示されます。

図 7.12 QARecord：シンプルなハードディスク録音アプリケーション



TV、ビデオ、ラジオ、およびWebカメラ

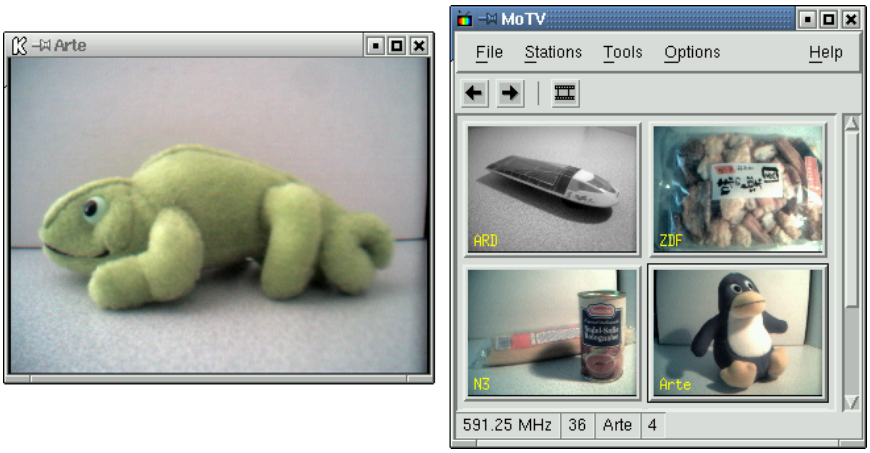
8

この章では、Linuxの基本的なビデオ、ラジオ、およびWebカメラのアプリケーションについて説明します。さらに、motvを設定してアナログテレビを見る方法、Webカメラの使い方、およびビデオテキストの閲覧について学習します。デジタルビデオ放送にはxawtv4を使用します。Webカメラはgqcamを使用して実行します。EPG情報には、nxtvepgまたはxawtv4を使用してアクセスします。

8.1 motvによるTVの視聴

motvは、xawtvの後継アプリケーションです。すべての重要な機能がユーザインタフェースに組み込まれています。このアプリケーションを起動するには、*[マルチメディア]* → *[ビデオ]* → *[MoTV]*の順に選択します。コマンドラインでは、`motv`と入力して起動します。アプリケーションが起動すると、最初にTVウィンドウだけが表示されます。メニューウィンドウを右クリックしてメニューを開きます。

図 8.1　TVアプリケーションmotv



8.1.1　ビデオソースとネットワーク検索

[Settings] → *[Input]*で、ビデオソースを選択します。ここで［*Television*］を選択すると、アプリケーションを起動する前に放送ネットワークが設定されます。これはネットワーク検索とともに自動的に行われます。また、［*Settings*］メニューでも実行できます。［*Save settings*]をクリックすると、検出されたネットワークが、ホームディレクトリの.xawtvファイルに保存され、次回アプリケーションを起動したときに使用できます。

ティップ: チャネルの選択

利用可能なチャネルをすべて検出する必要がない場合は、Ctrl + ↑で次のチャネルを検索します。その後必要に応じて、←または→で放送周波数を調整します。

8.1.2　オーディオデータの取得

TVカードの音声出力は、サウンドカードのライン入力、スピーカ、またはアンプに接続されています。TVカードの中には、音声出力のボリュームを変更できるカードもあります。この場合、ボリュームは、*[Settings]* → *[Slider]*を選

択して表示されるスライダで設定できます。このウィンドウにはまた、輝度、明度、および色を設定するためのスライダもあります。

オーディオ再生にサウンドカードを使用するには、項7.1.「ミキサー」(page 121)で説明するgamixを使用してミキサ設定をチェックします。AC97仕様に準拠するサウンドカードの場合は、［*Input-MUX*］を［*Line*］に設定します。次に、［*Master*］と［*Line*］のスライダで、ボリュームを調整できます。

8.1.3 縦横比とフル画面モード

ほとんどのテレビ画像は、縦横比が4:3です。この比率は、*[ツール]* → *[画面の大きさ]*で設定できます。ここで［*4:3*］(デフォルト)を選択すると、ディスプレイサイズが変わっても、画面の大きさは維持されます。

F を押すか、または*[Tools]* → *[Fullscreen]*の順に選択すると、フル画面モードに切り替えることができます。フル画面のTV画像がフルモニタサイズにサイズ変更できない場合は、微調整が必要になります。多くのグラフィックスカードは、グラフィカルモードを変更することなく、フル画面モードのテレビ画像をフルモニタサイズにサイズ変更できます。使用しているカードがこの機能をサポートしていない場合、グラフィックスモードをフル画面モードに切り替えるためには、解像度を640x480に変更する必要があります。このための設定は、*[Settings]* → *[Configuration]*で行います。フルサイズモードに切り替えた場合、motvを再起動すると、モニタモードも変更されています。

ティップ: .xawtvへの設定の保存

[Settings] → *[Save settings]*の順にクリックすると、`.xawtv`ファイルが自動的に作成されて更新されます。これで、テレビ局とその設定が保存されました。設定ファイルの詳細については、`xawtvrc`のマニュアルページを参照してください。

8.1.4 ランチャメニュー

ランチャメニューを使用して、motvと併用するアプリケーションを起動することができます。キーボードショートカットなどを使用して音声ミキサgamixとビデオテキストアプリケーションalevtを起動します。motvから起動するア

プリケーションは、.xawtvファイルに入力する必要があります。エントリは、次のように入力します。

```
[launch] Gamix = Ctrl+G, gamix AleVT = Ctrl+A, alevt
```

コマンドがアプリケーションの起動に使用するショートカットが、アプリケーション名の後ろに表示されます。[launch]で入力されたアプリケーションは、［*Tool*］メニューから起動できます。

8.2 ビデオテキストのサポート

alevtを使用して、ビデオテキストページをブラウズします。アプリケーションを起動するには、*[マルチメディア]→[ビデオ]→[alevt]*の順に選択するか、またはコマンドラインで`alevt`と入力します。

motvでアクティブ化され、選択された配信局のすべてのページが保存されます。ページをブラウズするには、ページ番号を入力するか、ページ番号をクリックします。ウィンドウの下部のマージンにある[<<]または[>>]をクリックすると、ページを前後に移動できます。

motvの最新版およびその後継のxawtv4には、独自のビデオテキストビューアアプリケーションであるmtt (motv)とmtt4 (xawtv4)が含まれます。mtt4はDVBカードもサポートします。.

8.3 Webカメラとmotv

Linuxでサポートされているwebカメラを使用している場合は、motvでアクセスできます。サポートされているUSBデバイスの要約は、`http://www.linux-usb.org`にあります。Webカメラにアクセスする前に、motvを使用して既にTVカードにアクセスしている場合は、bttvドライバがロードされています。WebカメラがUSBに接続されると、Webカメラのドライバが自動的にロードされます。コマンドラインで`-c /dev/video1`パラメータを指定してmotvを起動し、Webカメラにアクセスします。TVカードにアクセスする場合のパラメータは、`motv -c /dev/video0`です。

(たとえば、TVアプリケーションを起動して) bttvドライバが自動的にロードされる前に、WebカメラをUSBに接続すると、`/dev/video0`がWebカメラ用

に予約されます。この場合、`-c /dev/video1`パラメータを指定してmotvを起動し、TVカードにアクセスしようとすると、bttvドライバが自動的にロードされていないので、エラーメッセージが発生することがあります。この問題を解決するには、CAPIドライバの機能をテストします。ユーザ`root`で、`modprobe bttv`コマンドを実行し、ドライバを別にロードします。システム上の設定可能なビデオデバイスの概要にアクセスするには、`motv -hwscan`を使用します。

8.4 nxtvepg：PC用のTVマガジン

配信局によっては、EPG信号(Electronic Program Guide)とビデオテキスト信号を伝送している局もあります。この電子ガイドは、nxtvepgプログラムを使用すれば簡単に表示できます。ただし、これには、bttvドライバがサポートするTVカードがあり、EPGによって放送されるチャネルのいずれかが受信可能である必要があります。

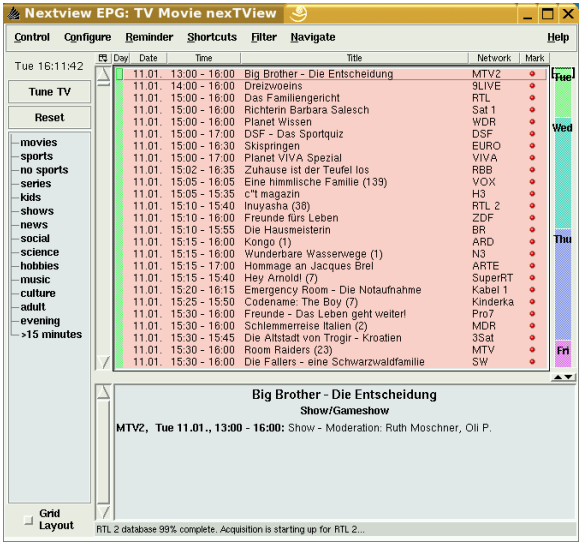
nxtvepgを使用すると、配信局がチャネルとトピックごとにソートされ(［*映画*］、［スポーツ］など)、基準(*ライブ*、*ステレオ*、*字幕*など)に従ってフィルタリングされます。アプリケーションを起動するには、*[マルチメディア]* → *[ビデオ]* → *[nxtvepg]*の順に選択するか、またはコマンドラインで`nxtvepg`と入力します。

8.4.1 EPGデータベースのインポート

EPG信号経由のプログラムデータベースを設定、更新するには、TVカードのチューナをEPGを配信する局に設定します。これには、motv、nxtvepgなどのTVアプリケーションを使用します。チューナにアクセスできるのは一度に1つのアプリケーションだけです。

motvにEPG局を設定すると、nxtvepgは最新のTVプログラムリストのインポートを即座に開始します。進捗状況が表示されます。

図 8.2　電子TVマガジンnxtvepg



TVアプリケーションを起動していない場合は、nxtvepgを使用してEPG局を検索します。これには、*[Configure]* → *[Provider scan]*の順に選択します。［*Use .xatv*］がデフォルトでアクティブになります。これは、このファイルに保存された局にnxtvepgがアクセスしていることを示します。

ティップ: トラブルシューティング

問題がある場合は、［*TV card input*］で正しいビデオソースを選択しているかを確認します。

[Configure] → *[Select Provider]*の表示から、EPGプロバイダを選択します。*[Configure]* → *[Merge Providers]*の順に選択しても、さまざまなプロバイダデータベースと柔軟に関連付けることができます。

8.4.2　プログラムのソート

nxtvepgには、膨大な数の番組を管理できる便利なフィルタ機能があります。これには、*[Configure]* → *[Show networks]*の順に選択して、ネットワーク選択リストをアクティブ化します。［*Filter*］メニューには、多くのフィルタ機能が用意されています。プログラムリストを右クリックすると特別なフィルタ

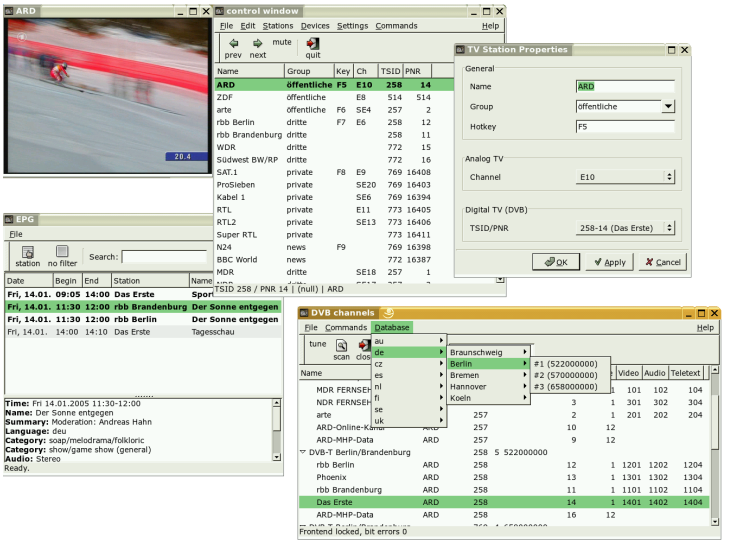
メニューが開き、コンテキストフィルタ機能をアクティブ化することができます。

特に便利なのが、［*Navigate*］メニューです。これはEPGデータから直接構築され、ネットワークが提供する言語で表示されます。

8.5 xawtv4によるデジタルビデオ放送の視聴

YaSTによってハードウェアが適切に設定されているので、メインメニューからxawtv4を起動します(*[マルチメディア] → [ビデオ] → [xawtv4]*)。目的の放送を実際に見る前にDVB局のデータベースを構築する必要があります。

図 8.3 xawtv4の実行



スタートウィンドウを右クリックしてコントロールウィンドウを開きます(図 8.3, 「xawtv4の実行」 (page 149)を参照)。*[Edit (編集)] → [Scan DVB (DVBのスキャン)]*の順に選択して、使用できるDVB局のスキャンを開始します。チャネルスキャナとブラウザウィンドウが開きます。ブーケを選択してスキャンを準備します。これは、ブーケの調整パラメータを既に知っている場合、ま

たは*[Database (データベース)] → [_country_] → [_channel number_]*(`_country_`と`_channel_number_`は各自の場所の値で置き換えます)を使用してxawtv4のビルトインデータベースからブーケの調整パラメータを取得した場合、*[Commands (コマンド)] → [Tune manually (手動調整)]*を使用して手動で行うことができます。

スキャナの調整が完了すると、すぐにブラウザウィンドウに最初のデータが表示されます。使用できるすべての局の完全なスキャンを実行するには、*[Command (コマンド)] → [Full Scan (フルスキャン)]*の順に選択します。スキャナの実行中は、好みの局を選択してコントロールウィンドウにドラッグするだけで局リストに追加できます。チャネルスキャナを残し、チャネルを選択して放送の視聴を開始します。

ティップ: 局リストの編集

キーボードショートカットを使用すれば、キーボードを使用してチャネル選択を制御できます。局リストに含まれる局にショートカットを設定するには、局を選択し、*[Edit (編集)] → [Edit Station (局の編集)]*の順に選択します。［*TV Station Properties (TV局のプロパティ)*］というダイアログが表示されます。ショートカット入力し、［*OK*］をクリックしてダイアログを閉じます。このダイアログでは、局をグループ化するためのサブメニューを定義することもできます(「ニュース」、「プライベート」など)。

---

xawtv4ソフトウェアパッケージには、さらに便利なスタンドアロンのマルチメディアアプリケーションが含まれます。

pia4
: xawtv4で録画されたムービーストリームを再生するための軽量のコマンドライン制御ムービープレーヤーです。

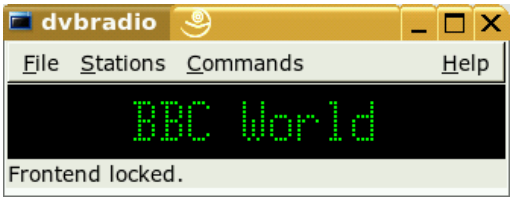
mtt4
: ビデオテキストブラウザです(図 8.4. 「mtt4ビデオテキストブラウザ」(page 151)を参照)。

図 8.4　mtt4ビデオテキストブラウザ

alexplore
スタンドアロンのDVBチャネルスキャナアプリケーションです。このアプリケーションの機能はxawtv4に統合されています。

dvbradio
DVBラジオプレーヤーです。最初の局スキャンを完了した後にDVB-Sラジオストリームを再生するために使用します(図8.5.「DVBラジオ」 (page 151)を参照)。

図 8.5　DVBラジオ



dvbrowse

EPGブラウザアプリケーションです。最初の局スキャンを完了した後にEPG情報を取得するために使用します。

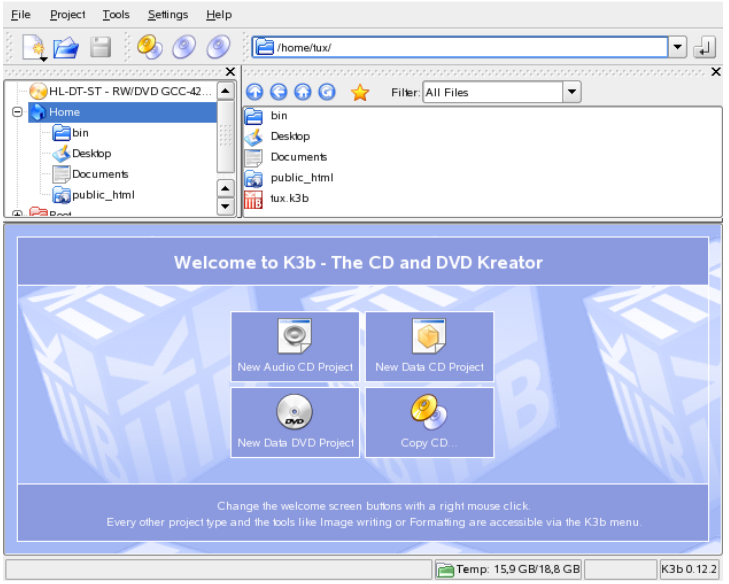
9 K3b—CDまたはDVDの書き込み

K3bは、データCDとオーディオCD、DVDの書き込みを行う総合的なプログラムです。メインメニューから［マルチメディア］、［CD/DVDの作成］の順に選択するか、`k3b`コマンドを入力して、このプログラムを起動します。ここでは、Linuxで初めてCDまたはDVDを作成するユーザのために、基本の書き込みプロセスを開始する方法について簡単に説明します。

9.1 データCDの作成

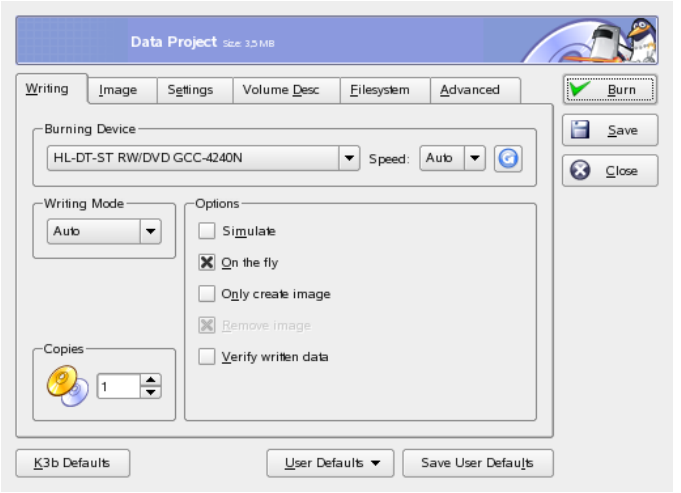
データCDを作成するには、*［ファイル］*、→ *［新しいプロジェクト］*、→ *［新しいデータCDプロジェクト］*の順に選択します。図 9.1.「新しいデータCDの作成」 (page 154)に示すように、ウィンドウの下側にプロジェクトビューが表示されます。自分のホームディレクトリ内にある、希望のディレクトリや個別のファイルをドラッグし、このビューへドロップします。*［ファイル］*、→ *［名前を付けて保存］*を選択して任意の名前を付け、このプロジェクトを保存します。

図 9.1　新しいデータCDの作成



それから、ツールバーの［*Burn*］をクリックするか、Ctrl＋Bを押します。CDに書き込むためのさまざまなオプション用の6つのタブがあるダイアログが表示されます。図 9.2.「書き込みプロセスのカスタマイズ」 (page 155)を参照してください。

図 9.2　書き込みプロセスのカスタマイズ



［*書き込み*］タブには、書き込みデバイス、速度、および書き込みオプションの設定があります。次のオプションがあります。

Burning Device

このポップアップメニューには、検出された書き込みデバイスが表示されます。 ここでは書き込み速度も選択できます。

警告: 書き込み速度を選択する際の注意

通常は［*Auto*］を選択してください。これにより、可能な最大速度が選択されます。 しかし、この値を大きく設定して、システムがそれに十分な速度でデータを転送できない場合には、バッファアンダーランの可能性が大きくなります。

書き込みモード

このオプションは、レーザーがCDに書き込む方法を決定します。［DAO］(disk at once、ディスクアットワンス)モードでは、CDに書き込んでいる間、レーザーを無効にしません。オーディオCDを作成する場合、このモードをお勧めします。ただし、すべてのCDライタがこのモードをサポートしているわけではありません。［TAO］(track at one、トラックアットワンス)モードでは、個別の書き込みプロセスが個々のトラックごとに使用されます。［RAW］(ロー)モードは使用頻度があまり高くありませんが、ライタ

がデータ補正を何も行わないのが特徴です。最善の設定値は［*自動*］であり、最適な設定値をK3bに特定させることができます。

シミュレート
この機能を使用して、使用中のシステムが、選択された書き込み速度をサポートしているかどうかチェックすることができます。システムをテストするために、レーザーを無効にして書き込みます。

On the Fly
イメージファイルを最初に作成することなく、希望のデータを書き込みます(パフォーマンスの低いコンピュータでは、この機能を使用しないでください)。イメージファイルはISOイメージとも呼びますが、CDの内容全体を保持しているファイルであり、通常はこのファイルを作成した後、その内容をそのままCDに書き込みます。

Only create image
このオプションは、イメージファイルを作成します。［*一時ファイル*］の中で、このファイルの作成先パスを設定します。後で、このイメージファイルをCDに書き込むことができます。この作業を行うには、*［ツール］*、→ *［CD］*、→ *［CDイメージを書き込む］*の順に選択します。このオプションを使用する場合、このセクション内にある他のすべてのオプションは無効になります。

Remove Image
書き込みが終了するときに、一時イメージファイルをハードディスクから削除します。

Verify Written Data
元のデータと書き込まれたデータのMD5チェックサムを比較することによって、書き込まれたデータの完全性を確認します。

［*Image*］タブは、［*Only create image*］をオンにした場合にのみ表示されます。この場合、ISOイメージを書き込む場所を指定できます。

［*Settings*］タブには、［*Datatrack Mode*］と［*Multisession Mode*］という2つのオプションがあります。［*Datatrack Mode*］オプションでは、データトラックの書き込み方法を設定できます。通常は、［*Auto*］を選択すれば最適な方法になります。［*Multisession*］は、書き込みが行われたものの、まだファイナライズされていないCDにデータを追加するために使います。

［ボリュームの*ID*］タブで、このデータプロジェクトを識別するために使用できる一般情報、発行者と作成者、このプロジェクトの作成に使用されたアプリケーションとオペレーティングシステムを入力します。

［ファイルシステム］タブで、CD上で使用するファイルシステムの設定値(RockRidge、Joliet、UDF)を指定します。また、シンボリックリンク、ファイルのパーミッション、および空白を扱う方法も決定します。［*詳細*］タブでは、経験のあるユーザが追加の設定項目を指定することができます。

必要に応じてすべての設定を調整したら、［*書き込む*］を使用して実際の書き込みプロセスを開始します。または、これらの設定を将来の使用や調整に備えて、［*保存*］を使用して保存します。

9.2 オーディオCDの作成

基本的に、オーディオCDの作成とデータCDの作成に大きな違いはありません。*［ファイル］、→［新しいオーディオCDプロジェクト］*の順に選択します。個別のオーディオトラックをプロジェクトフォルダにドラッグアンドドロップします。オーディオデータは、WAVまたはOgg Vorbisのどちらかの形式でなければなりません。プロジェクトフォルダ内でトラックを上下に移動することにより、トラックの順序を決定します。

CD Textを使えば、CDのタイトル、アーティスト名、トラック名などのテキスト情報をCDに追加できます。この機能をサポートしているCDプレーヤは、この情報を読み取って表示することができます。オーディオトラックにCD Text情報を追加するには、まずトラックを選択します。右クリックして［プロパティ］を選択します。新しいウィンドウが表示され、情報を入力することができます。

オーディオCDを書き込むためのダイアログは、データCDを書き込むためのダイアログと大差ありません。しかし、［*DAO*］と［*TAO*］のモードは大きな違いをもたらします。［*TAO*］モードでは、各トラックの後に2秒の中断時間を挿入します。

ティップ: データの完全性の維持

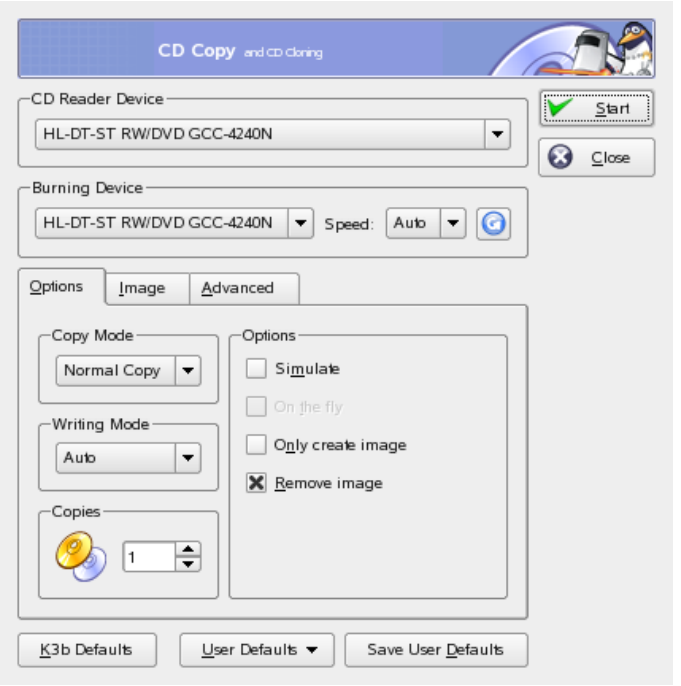
オーディオCDを書き込むときは、低速の書き込み速度を選択した方が書き込みエラーが発生する可能性は低くなります。

必要に応じてすべての設定を調整したら、［書き込む］を使用して実際の書き込みプロセスを開始します。または、これらの設定を将来の使用や調整に備えて、［保存］を使用して保存します。

9.3 CDまたはDVDのコピー

メディアに応じて、［ツール］、→［CDをコピー］か［ツール］、→［DVDをコピー］を選択します。表示されたダイアログで、図 9.3.「CDのコピー」(page 158)に示すように、読み取りデバイスと書き込みデバイスに関する設定を行います。これまでに説明した書き込みオプションは、ここでも使用できます。 追加の機能により、CDやDVDのコピー枚数を指定することもできます。

図 9.3 CDのコピー



データを読み込んでからすぐにCDに書き込む場合は［オンザフライ］を選択します。［*Temp Directory(一時ディレクトリ)*］、→［*Write image file to (イ*

メージファイルの書き込み先)］に指定されたパスにイメージを作成して、そのイメージを後で書き込む場合は［*Only create image (イメージの作成のみ)*］を選択します。

9.4 ISOイメージの書き込み

すでにISOイメージが手元にある場合、［*ツール*］、→［*CD*］、→［*CDイメージを書き込む*］の順に選択します。［*書き込むイメージ*］の場所を入力するためのウィンドウが表示されます。K3bによってチェックサムが計算され、［*MD5 Sum*］行にその値が表示されます。そのISOファイルがインターネットからダウンロードしたものである場合、このチェックサムはダウンロードが成功したかどうかを示します。

［*オプション*］と［*詳細*］の各タブを使用して、自分の好みに合う値を設定します。CDに書き込むには、［*開始*］をクリックします。

9.5 マルチセッションCDまたはDVDの作成

マルチセッションのディスクでは、データを複数回にわたって書き込むことができます。 この機能は、メディアよりも小さなバックアップを書き込む場合などに役立ちます。 セッションごとに、バックアップファイルを追加していくことができます。 興味深い点として、この機能はデータCDやDVDだけに限られているわけではありません。 マルチセッションディスクにオーディオセッションを追加することもできます。

マルチセッションのディスクを作成するには、以下の手順に従います。

1. まず、データディスクを作成して、すべてのファイルを追加します。 オーディオCDセッションから開始することはできません。 ディスクがいっぱいになっていないことを確認してください。そうでないと、新しいセッションを追加することができないからです。

2. ［*プロジェクト*］、→［*Burn*］.の順に選択します。 ダイアログボックスが表示されます。

3 ［*Settings*］タブで、［*Start Multisession*］を選択します。

4 必要に応じて他のオプションを設定します。項9.1.「データCDの作成」(page 153)も参照してください。

5 ［*Burn*］をクリックして、書き込みセッションを開始します。

書き込みセッションが正常に完了すれば、マルチセッションのディスクになります。 メディアに空きスペースがある限り、必要に応じてセッションを追加することができます。 ディスクのファイナライズは、新しいセッションを追加する必要がない場合、またはスペースが残っていない場合にのみ行ってください。

注意: マルチセッションのディスクの容量

マルチセッションのディスクでは、セッションのすべてのエントリを管理するためのスペースが必要であることに注意してください。 そのため、ディスクの使用可能な容量は小さくなり、セッション数に応じて変わります。

9.6 関連資料

K3bには、これまでに説明した2つの主要な機能のほかに、DVDコピーの作成、WAVフォーマットのオーディオデータの読み取り、CDへの追加書き込み、統合されたオーディオプレーヤでの音楽の再生など、他の機能もあります。このプログラムで使用可能なすべての機能の詳細は、`http://k3b.sourceforge.net`で入手できます。

パート IV. オフィスソフトウェア

10 OpenOffice.orgオフィススイート

OpenOffice.orgは機能が豊富なLinuxオフィススイートで、テキスト文書の作成、表計算ドキュメントの使用、図形やプレゼンテーションの作成など、あらゆる種類のオフィスタスクに対応するツールを備えています。OpenOffice.orgでは、異なるコンピューティングプラットフォーム間で、同じデータを共用します。また、必要であれば、Microsoft Office形式でファイルを開いて編集し、この形式に戻して保存することもできます。ここでは、OpenOffice.orgを初めて使用するユーザに必要な基本的な事項について説明します。このアプリケーションは、SUSEメニューまたは`ooffice`コマンドを使用して起動します。

OpenOffice.orgは、互いに連携する複数のプログラムモジュールで構成されています。モジュールの一覧は、表 10.1.「OpenOffice.orgアプリケーションモジュール」 (page 163)にあります。この章では、Writerに焦点を合わせて説明します。各モジュールの詳細については、項10.6.「関連資料」 (page 170)で説明するオンラインヘルプを参照してください。

表 10.1 *OpenOffice.orgアプリケーションモジュール*

Writer	強力なワードプロセッサアプリケーション
Calc	グラフ作成機能を持つ表計算アプリケーション
Draw	ベクタ図形を作成するための描画アプリケーション
Math	数式生成アプリケーション

Impress	プレゼンテーション作成アプリケーション
Base	データベースアプリケーション

アプリケーションの外観は、使用しているデスクトップやウィンドウマネージャによって異なります。さらに、使用しているデスクトップのオープンと保存のダイアログ形式が使用されます。外観に関係なく、基本的なレイアウトと機能は同じです。

10.1 他のOfficeアプリケーションとの互換性

OpenOffice.orgは、Microsoft Office文書、スプレッドシート、プレゼンテーション、およびデータベースと連携して使用できます。これらは他のファイルと同様にシームレスに開いて、同じ形式で保存できます。Microsoftの形式は非公開で、詳しい仕様は他のアプリケーションで利用できないので、書式の問題が発生することがあります。文書の問題が発生した場合は、元のアプリケーションで開き、テキスト文書の場合はRTF、スプレッドシートの場合はCSVなどのオープン形式で再び保存してみます。

アプリケーションを初めて切り替える場合など、多くの文書を変換する場合は、*[ファイル] → [ウィザード] → [ドキュメント変換]*の順に選択します。変換前のファイル形式を選択します。StarOfficeとMicrosoft Officeの複数の形式が用意されています。形式を選択したら［*次へ*］をクリックし、OpenOffice.orgによって変換するテンプレートおよび文書の場所と、変換済みファイルの保存場所を指定します。次に進む前に、すべての設定が正しいことを確認します。［*次へ*］をクリックして、実行するアクションの要約を確認します。設定がすべて正しいかをもう一度確認します。最後に、［*変換*］をクリックして変換を開始します。

重要項目: Windowsファイルの検索

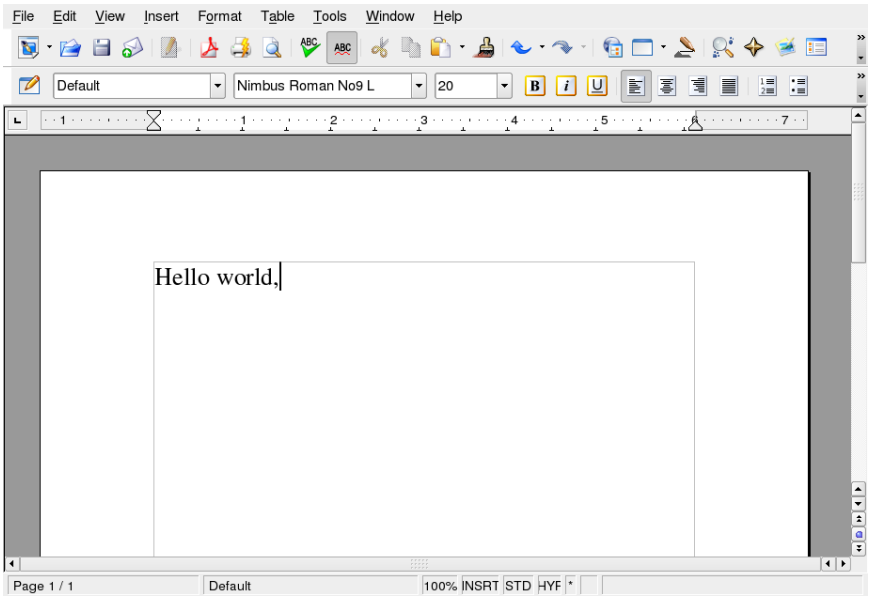
Windowsパーティションにある文書は、通常、`/windows`のサブディレクトリにあります。

他のアプリケーションと文書を共有する場合は、いくつかの方法があります。受信側が文書を読み出すだけの場合は、*[ファイル] → [Export as PDF (PDFとしてエクスポート)]*の順に選択してPDFファイルにエクスポートします。PDFファイルは、Adobe Acrobat Readerなどのビューアを使用して任意のプラットフォームで参照できます。文書を編集するために共有する場合は、標準的な文書形式を使用します。デフォルトの形式はOASISの標準XML形式に準拠しています。この形式では、多くのアプリケーション間で互換性が確保されます。TXTとRTF形式は書式設定に制限がありますが、テキスト文書には良い選択肢です。CSVは、スプレッドシートに有効です。OpenOffice.orgでは、受信側が希望する形式、特にMicrosoft形式で提供できる場合があります。

OpenOffice.orgは、多くのオペレーティングシステムで使用できます。このため、OpenOffice.orgはユーザのグループが頻繁にファイルを共有する必要があり各自のコンピュータのシステムが異なる場合、有効なツールになります。

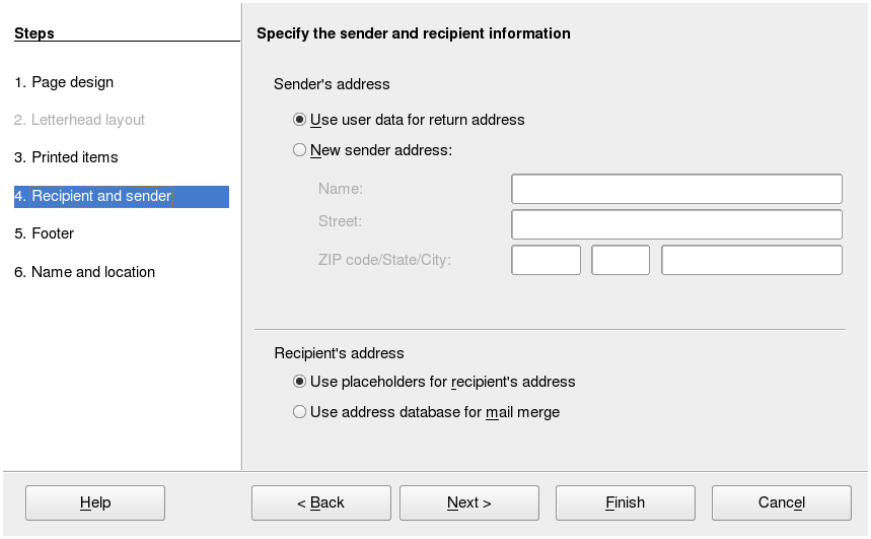
10.2 Writerによる文書作成

図 10.1 *OpenOffice.org Writer*



新しい文書を作成するには、次の2つの方法があります。最初から文書を作成する場合は、*[ファイル] → [新規] → [文書ドキュメント]*の順に選択します。作成する文書に標準形式や定義済みの形式を使用する場合は、ウィザードを使用します。ウィザードは小さなユーティリティで、基本的な決定を行うと、テンプレートからレディメードの文書が作成されます。たとえば、ビジネスレターを作成する場合は、*[ファイル] → [ウィザード] → [レター]*の順に選択します。ウィザードのダイアログを使用すれば、標準書式を使用する基本文書を簡単に作成できます。ウィザードのダイアログのサンプルは、図 10.2.「OpenOffice.orgウィザード」 (page 166)にあります。

図 10.2　OpenOffice.orgウィザード



必要に応じて文書ウィンドウにテキストを入力します。［*Formatting (書式設定)*］ツールバーまたは［*Format (書式)*］メニューを使用して文書の外観を調整します。［*ファイル*］メニューまたはツールバーの該当するボタンを使用して、文書を印刷または保存します。［*挿入*］メニューのオプションを使用すれば、文書にテーブル、画像、図などの項目を追加できます。

10.2.1　テキストの選択

テキストを選択するには、選択領域の開始位置をクリックし、マウスボタンを押したままカーソルを範囲の終了位置まで移動します(選択対象は、文字、

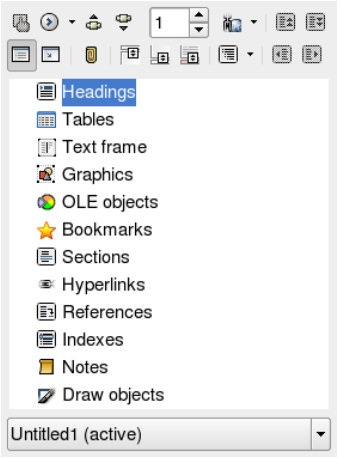
線、または段落全体です)。目的の範囲のテキストを選択したらボタンを放します。選択している間、テキストが反転色で表示されます。選択領域を右クリックすると、コンテキストメニューが表示されます。コンテキストメニューを使用すれば、フォント、フォントスタイル、およびその他のテキストプロパティを変更できます。

選択したテキストは、クリップボードに切り取りまたはコピーできます。切り取りまたはコピーされたテキストは、文書内の別の位置に貼り付けることができます。コンテキストメニュー、［*編集*］、または対応するツールバーアイコンを使用すれば、これらの機能にアクセスできます。

10.2.2 大きな文書内の移動

ナビゲータには、文書の内容についての情報が表示されます。また、ナビゲータでは、含まれているさまざまな要素にすばやくジャンプすることができます。たとえば、ナビゲータを使用して、すべての章を概観したり、文書に含まれているイメージのリストを表示したりすることができます。ナビゲータを開くには、*[編集]* → *[ナビゲータ]*の順に選択します。図 10.3.「Writerで動作するナビゲータ」 (page 167)に、動作中のナビゲータを示します。Navigatorに表示される要素は、Writerにロードされている文書によって異なります。

図 10.3 *Writerで動作するナビゲータ*



10.2.3　スタイルによる書式設定

*[Format (書式)] → [Styles and Formatting (スタイルと書式設定)]*の順に選択して開くダイアログを使用すれば、さまざまな方法でテキストを書式設定できます。このダイアログの最下部にあるドロップダウンリストを［*自動*］に設定すると、OpenOffice.orgは、実行中のタスクに関連するスタイルだけを選択肢として表示します。［*すべてのスタイル*］を選択すると、現在アクティブなグループで利用できるすべてのスタイルが表示されます。上部のボタンでグループを選択します。

この方法によるテキストの書式設定は、*ソフト書式設定*と呼ばれ、テキストは間接的に書式設定されます。代わりに、スタイルが適用されます。スタイルは簡単に変更でき、それによって、スタイルが割り当てられているすべてのテキストの書式が自動的に変更されます。

段落にスタイルを割り当てるには、使用するスタイルを選択し、［*Styles and Formatting (スタイルと書式設定)*］の水やりモードのアイコンをクリックします。次に、スタイルを割り当てる段落をクリックします。スタイルの割り当てを解除するには、Escを押すか、または水やりモードのアイコンを再びクリックします。

［*Format (書式)*］メニューまたはツールバーを使用して段落または文字を書式設定すれば、独自のスタイルを簡単に作成できます。スタイルをコピーする書式設定された部分を選択します。次に、［*Styles and Formatting (スタイルと書式設定)*］のバケツの右のボタンをクリックしてボタンを押した状態にし、表示されるメニューから［*選択スタイルから新規作成*］を選択します。スタイルの名前を入力し、［*OK*］をクリックします。このスタイルを他のテキストに適用することもできます。

スタイルの詳細を変更するには、それをリストで選択し、右クリックしてメニューから［*変更*］を選択します。これにより、利用可能な書式プロパティを示すダイアログが表示され、書式を変更することができます。

10.3　Calcの使い方

Calcは、OpenOffice.orgのスプレッドシートアプリケーションです。*[ファイル] → [新規] → [スプレッドシート]*の順に選択するか、または*[ファイル] →*

*[開く]*の順に選択してファイルを開きます。Calcは、Microsoft Excelの形式で読み出しおよび保存ができます。

スプレッドシートのセルには、固定データまたは式を入力します。式を使用すれば、他のセルからのデータを操作して、式を挿入したセルの値を生成できます。セルの値からグラフを作成することもできます。

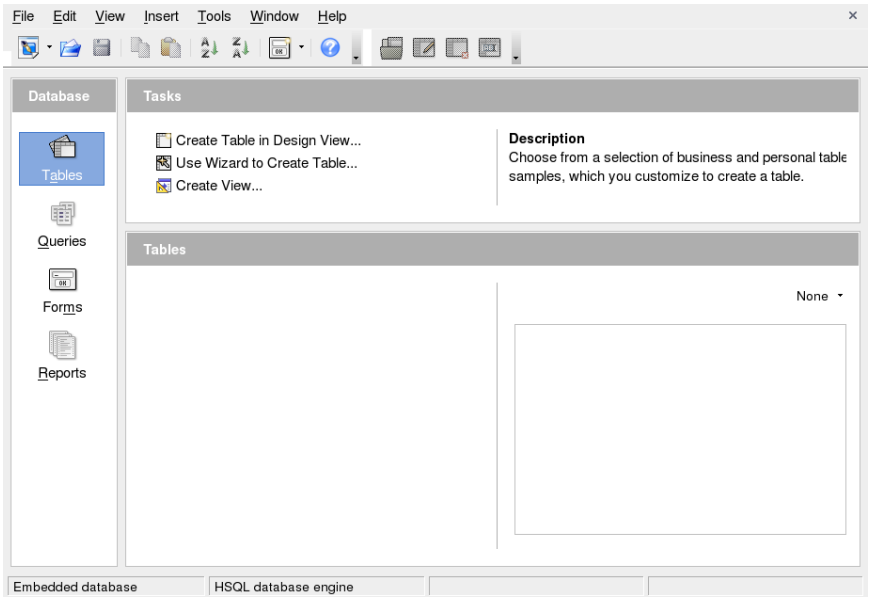
10.4 Impressの使い方

Impressは、画面表示または透明シートなどに印刷するためのプレゼンテーションを作成するためのアプリケーションです。プレゼンテーションを最初から作成する場合は、*[ファイル]* → *[新規]* → *[プレゼンテーション]*の順に選択します。ウィザードを使用してプレゼンテーションを作成する場合は、*[ファイル]* → *[ウィザード]* → *[プレゼンテーション]*の順に選択します。既存のプレゼンテーションを開く場合は、*[ファイル]* → *[開く]*の順に選択します。Impressは、Microsoft PowerPointプレゼンテーションを開いて保存できます。

10.5 Baseの使い方

OpenOffice 2.0には、新しいデータベースモジュールが導入されています。データベースを作成する場合は、*[ファイル]* → *[新規]* → *[データベース]*の順に選択します。データベースの作成を支援するウィザードが開きます。BaseもMicrosoft Accessデータベースと連携して使用できます。

図 10.4　Base—OpenOffice.orgのデータベース



テーブル、フォーム、クエリ、およびレポートは、手動で作成するか、または便利なウィザードを使用して作成できます。たとえば、テーブルウィザードには、ビジネスおよび個人用途のための一連の共通フィールドがあります。Baseで作成されたデータベースは、フォームレターを作成する場合などのデータソースとして使用できます。

10.6　関連資料

OpenOffice.orgには、さまざまなレベルの情報を提供する多くの情報オプションがあります。ヘルプの詳細については、*[ヘルプ] → [OpenOffice.org Help (OpenOffice.orgのヘルプ)]*を選択して参照してください。このヘルプシステムは、OpenOffice.org(Writer、Calc、Impressなど)の各モジュールに関する詳細情報を提供します。

アプリケーションを初めて起動するときは、マウスポインタをボタンの上に置いたときに表示される短い情報である［ヒント］、および実行されるアクションに基づく情報を提示する［ヘルプエージェント］が表示されます。［ヒント］がボタンについて提供する内容よりも詳しい情報を取得するには、*[ヘ*

*ルプ] → [これは何?]*の順に選択し、目的のボタンにマウスのポインタを移動します。［*これは何?*］モードを終了するには、再びクリックします。この機能を頻繁に必要とする場合は、*[ツール] → [オプション] → [OpenOffice.org] → [General (全般)]*の［*詳細ヒント*］を有効にしてください。［ヘルプエージェント］と［ヒント］もここで有効/無効を切り替えることができます。

OpenOffice.orgのWebサイトは、http://www.openoffice.orgです。このサイトには、メーリングリスト、ニュース、およびバグ情報があります。このサイトでは、各種のオペレーティングシステム用のバージョンをダウンロードできます。

11 Evolution: 電子メールとカレンダのプログラム

Evolutionは、通常の電子メール機能のほかに、タスクリストやカレンダのような拡張機能も備えたグループウェアスイートです。 このアプリケーションには、完成度の高いアドレス帳も用意されていて、連絡先情報を、vCard形式で他のユーザに送信することもできます。

Evolutionを起動するには、メインメニュー、または`evolution`コマンドを使用します。初めて起動した場合、Evolution設定アシスタントが起動されます。使用方法については、項11.3.1.「アカウントの設定」 (page 176)を参照してください。

重要項目: Microsoft Exchangeアカウント

EvolutionをMicrosoft Exchangeと連携させるには、`ximian-connector`パッケージのインストールが必要です。 このパッケージをYaSTを使用してインストールします。

11.1 他のメールプログラムからの電子メールのインポート

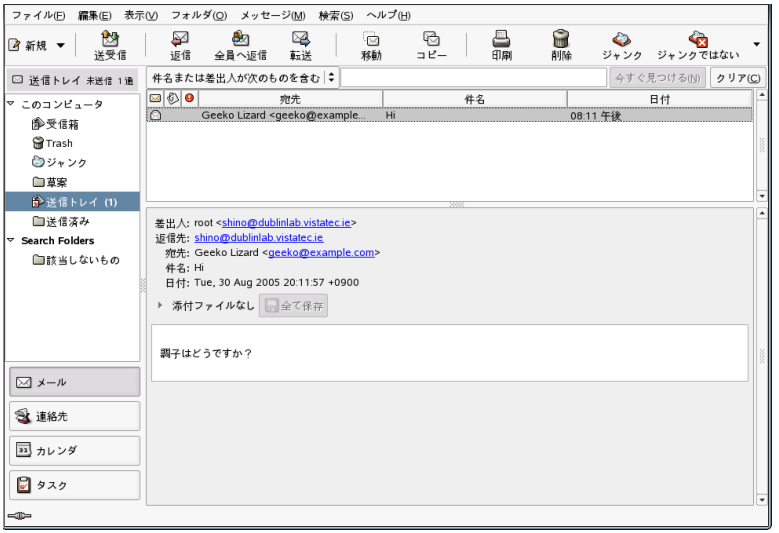
Netscapeのような他の電子メールプログラムからメールをインポートするには、*[ファイル]→[インポート]*の順に選択します。mbox形式の場合は、［*ファイル単体をインポートする*］を選択します。Netscapeからインポートする場合は、［*以前のバージョンからデータとその設定をインポートする*］を選択します。KMailなどのmaildir形式を使用しているプログラムのデータを処理する

には、そのメールのディレクトリにアクセスするためのアカウントを設定します。

11.2 Evolutionの概要

デフォルトのウィンドウビューを、図 11.1.「Evolutionウィンドウでのメール表示」(page 174)に示します。使用可能なメニュー、メニュー項目、およびツールバー内のアイコンは、使用中のコンポーネントごとに異なります。 左側にあるフレームを使用すると、右側のフレーム内に表示される情報を選択できます。フレームのサイズは、境界線をドラッグして調整できます。

図 11.1 Evolutionウィンドウでのメール表示



11.2.1 メール

このビューでは、ウィンドウの上側に現在のフォルダの内容を表示します。下側は、選択されているメールメッセージを表示するプレビューペインです。別なフォルダを表示するには、左側のフレームのフォルダのリストからフォルダを選択します。

フォルダ内のメッセージを検索するには、検索バーを使用します。 メッセージをテーブルのヘッダでソートするには、希望するヘッダをクリックします。右側の矢印は、そのコラムが昇順と降順のどちらでソートされているかを示しています。 メッセージが希望する順序でソートされるまで、コラムのヘッダをクリックしてください。

11.2.2 連絡先

このビューでは、アドレス帳の中にあるすべての連絡先を表示します。特定の連絡先を検索するには、検索バーを使用するか、連絡先のラストネームのうち、最初の文字の表示より右にあるボタンをクリックします。連絡先またはリストを追加するには、ツールバーを使用します。

11.2.3 カレンダ

初期の表示では、現在の日付に関する1日の表示があり、それより右に月とタスクリストを示す追加のペインがあります。ツールバーまたは［*表示*］メニューを使用して、週、営業日を示す週、または月単位の表示を利用することもできます。 検索バーでは、カレンダに入力された予定を検索することができます。予定とタスクを追加するには、ツールバー内のボタンを使用します。 カレンダのページ間で移動する場合や、特定の日付に移動する場合も、ツールバーを使用します。

11.2.4 タスク

［タスク］は、タスクリストを表示します。タスクを選択すると、その詳細がウィンドウの下側に表示されます。新しいタスクを追加するには、*[ファイル] → [新規作成] → [タスク]*の順に選択します。タスクを検索するには、検索バーを使用します。タスクを他のユーザに割り当てるには、目的のタスクを右クリックして［*Assign Task (タスクの割り当て)*］を選択します。タスクに期日や実行状況などの詳細を追加するには、［*開く*］を使用します。

11.3　メール

Evolutionのメールコンポーネントは、複数のアカウントをさまざまな形式で動作させることができます。検索結果の表示や迷惑メール選別のための仮想フォルダなど、便利な機能を提供します。アプリケーションの設定は、*[編集]* → *[初期設定]*の順に選択します。

11.3.1　アカウントの設定

Evolutionは、複数のメールアカウントから電子メールを取得できます。 電子メールを送信する際に使用するアカウントは、メッセージを作成する際に選択できます。メールアカウントの設定は、*[編集]* → *[初期設定]* → *[メールアカウント]*の順に選択します。既存のアカウント設定を変更するには、そのアカウントを選択し、［*編集*］をクリックします。アカウントを削除するには、そのアカウントを選択し、［*削除*］をクリックします。

新しいアカウントを追加するには、［*追加*］をクリックします。これを選択すると、設定アシスタントが起動されます。［*Forward (次へ)*］をクリックしてこれを使用します。フィールドに名前と電子メールアドレスを入力します。必要に応じて、他の情報を入力します。メール作成時にこのアカウントを使用するには、［*これをデフォルトのアカウントにする*］をオンにします。［*Forward (次へ)*］をクリックします。

［*サーバ種別*］で、このアドレスに着信する電子メールの適切な形式を選択します。リモートサーバから電子メールをダウンロードする場合、［*POP*］は最も一般的な形式です。［*IMAP*］は、特別なサーバ上に存在するメールフォルダと組み合わせた場合に機能します。この情報は、使用中のISPまたはサーバの管理者から入手してください。［サーバ種別］を選択すると、他の関連フィールドが表示されるので、それらに値を入力します。作業が完了したら、［*Forward (次へ)*］をクリックします。使用できる場合は、必要な［*返信オプション*］を選択します。［*Forward (次へ)*］をクリックします。

次に、メール配信オプションを設定します。ローカルシステムへ発信電子メールを送信する場合は、［*Sendmail*］を選択します。リモートサーバを使用する場合は、［*SMTP*］を選択します。詳細情報は、使用中の ISP またはサーバの管理者から入手してください。SMTPを使用する場合は、選択後に表示されるフィールドに値を入力します。作業が完了したら、［*Forward (次へ)*］をクリックします。

デフォルトでは、アカウントを識別する名前として、電子メールアドレスが使用されます。必要に応じて、他の名前を入力します。［*Forward (次へ)*］をクリックします。［*適用*］をクリックしてアカウントの設定を保存します。

あるアカウントを、電子メールを送信するためのデフォルトアカウントにするには、該当のアカウントを選択し、［*デフォルト*］をクリックします。あるアカウントでの電子メールの取得を無効にするには、そのアカウントを選択し、［*無効*］をクリックします。無効にしたアカウントは、送信時に引き続き使用することもできますが、そのアカウント宛の着信電子メールがチェックされることはありません。必要に応じて、［*有効*］を使用し、そのアカウントを再び有効にすることもできます。

11.3.2 メッセージの作成

新しいメッセージを作成するには、*[新規] → [メッセージ]*の順にクリックします。メッセージに返信または転送する場合も、同じメッセージエディタが起動します。［*差出人:*］の右隣のリストボックスで、メッセージの送信元として使用するアカウントを選択します。［宛先］フィールドに、電子メールアドレス全体を入力するか、アドレス帳に入力されている氏名またはアドレスの一部を入力します。入力した文字に一致する項目がアドレス帳の中で見つかった場合、選択リストが表示されます。希望の連絡先をクリックします。入力に一致する項目が見つからなかった場合は、最後まで入力します。アドレス帳から宛先を直接選択するには、［*宛先:*］または［*Cc:*］をクリックします。

Evolutionでは、電子メールをプレーンテキストまたはHTML形式で送信できます。HTML形式のメールにするには、ツールバーで［*Format (フォーマット)*］を選択します。添付ファイルを送信するには、［*添付*］を選択するか、*[挿入] → [ファイルの添付...]*の順に選択します。

メッセージを送信するには、［*送信*］をクリックします。すぐに送信する準備ができていない場合は、［*ファイル*］メニューの他の項目を選択します。たとえば、［草案の保存］を選択して、後で送信します。

11.3.3 暗号化された電子メールと署名

Evolutionは、PGPによる電子メールの暗号化をサポートしています。電子メールに署名すること、および署名済みの電子メールメッセージをチェックする

ことができます。これらの機能を使用するには、gpgまたはKGpgなどの外部アプリケーションを使用して鍵の生成と管理を行います。

電子メールメッセージを送信する前にそのメッセージに署名するには、*[セキュリティ] → [PGPサイン]*の順に選択します。［*送信*］をクリックした時点で、自分の秘密鍵に関連付けられているパスワードを要求するダイアログが表示されます。該当するパスワードを入力し、［*OK*］をクリックしてそのダイアログを閉じると、署名済みの電子メールが送信されます。これと同じセッション内で、秘密鍵を毎回「ロック解除」することなく、他の電子メールに署名するには、［*Remember this password for the remainder of this session (このセッションのリマインダとしてこのパスワードを記憶)*］を有効にします。

署名済み電子メールを他のユーザから受信した場合、小さな錠前(南京錠)アイコンがメッセージの最後に表示されます。そのアイコンをクリックすると、Evolutionは外部プログラム(gpg)を起動して、署名をチェックします。その署名が正当な場合は、錠前アイコンの隣に、緑のチェックマークが表示されます。その署名が正当でない場合は、破損した錠前が表示されます。

電子メールの暗号化と復号化は簡単です。電子メールメッセージを作成した後で、*[セキュリティ] → [PGPによる暗号化]*の順に選択し、次にその電子メールメッセージを送信します。 暗号化メッセージを受信した場合、自分の秘密鍵に関連付けられているパスワードを要求するダイアログが表示されます。パスフレーズを入力すると、その電子メールメッセージを復号化できます。

11.3.4 フォルダ

電子メールメッセージをさまざまなフォルダに分類すると、便利になることはよくあります。フォルダのツリーは左側のフレームに表示されます。IMAPを介してメールにアクセスしている場合、このフォルダバーの中にIMAPフォルダも表示されます。POPや他のほとんどの形式では、自分のフォルダはローカルに格納されていて、［*ローカルフォルダ*］内で分類されています。

いくつかのフォルダは、デフォルトで用意されています。［*受信箱*］は、サーバから取得した新しいメッセージを最初に配置する場所です。［*送信箱*］は、送信済みの電子メールメッセージのコピーを保存する目的で使用されます。［*送信トレイ*］は、まだ送信されていない電子メールの一時的な格納場所です。オフラインで作業している場合や、発信メールサーバが一時的に到達不可能になっている場合は、このフォルダが役立ちます。［*草案箱*］ は、完成していない電子メールメッセージを保存する目的で使用されます。［*ゴミ箱*］

フォルダは、削除済みアイテムを一時的に格納する目的で使用されます。［ジャンク］は、迷惑メールを選別するためのものです。

新しいフォルダは、［このコンピュータ］の直下に、または既存のフォルダのサブフォルダとして作成できます。必要に応じて、フォルダ階層を細かく作成します。新しいフォルダを作成するには、*[ファイル] → [新規] → [メールフォルダ]*の順に選択します。フォルダの作成ダイアログで、新しいフォルダの名前を入力します。マウスを使用して、新しいフォルダの配置先になる親フォルダを決定します。［*OK*］をクリックして、このフォルダを閉じます。

メッセージをフォルダへ移動するには、移動するメッセージを選択します。右クリックすると、コンテキストメニューが表示されます。［*フォルダへ移動*］を選択し、開いたダイアログの中で、移動先フォルダを選択します。［*OK*］をクリックして、そのメッセージを移動します。 元のフォルダ内にあったメッセージのヘッダには抹消線が付き、そのメッセージがフォルダから削除されたことを示します。そのメッセージは、新しいフォルダ内に格納されます。同様の方法で、メッセージをコピーすることもできます。

多数のメッセージを手動で他のフォルダへ移動すると、時間がかかる場合があります。フィルタを使用して、この手順を自動化することもできます。

11.3.5　フィルタ

Evolutionでは、電子メールをフィルタ処理するためのオプションを多数提供しています。フィルタを使用すると、メッセージを特定のフォルダへ移動したり、メッセージを削除することが可能です。フィルタを使用して、メッセージを直接ゴミ箱へ移動することもできます。新しいフィルタを作成するには、2つのオプションがあります。フィルタを完全に新規作成する方法と、フィルタ処理するメッセージに基づいてフィルタを作成する方法です。メーリングリスト宛てに送信されるメッセージをフィルタ処理する場合、後者は非常に役立ちます。

フィルタの作成

*[ツール] → [フィルタ]*の順に選択します。ここで開くダイアログボックスには、既存のフィルタがリストされますが、これらを編集または削除することもできます。新しいフィルタを作成するために、［*追加*］をクリックします。

または、メッセージに基づいてフィルタを作成するには、メッセージを選択してから*[ツール] → [メッセージからフィルタの作成]*の順に選択します。

［*ルール名*］に新しいフィルタの名前を入力します。そのフィルタで使用する条件を入力します。使用可能なオプションは、［差出人］、［宛先］、［ソースのアカウント］、［件名］、［送信日］、［受信日］、［ステータス］などです。［*以下を含むもの*］が最初に表示されているドロップダウンボックスには、［*が次のものを含む*］、［*が次のものと一致する*］、［*が次のものと一致しない*］など、さまざまなオプションがあります。適切なオプションを選択します。次に、検索(フィルタ)対象のテキストを入力します。フィルタの条件を追加するには、［*追加*］をクリックします。フィルタを適用する際に、入力した条件すべてが成立している必要があるか、一部だけでも成立していればよいかを決定するには、［*次の条件で実行する*］を使用します。

このウィンドウの下側では、フィルタの条件が成立したときに実施されるアクションを決定します。たとえば、メッセージを特定のフォルダへ移動またはコピーすることや、特別な色を割り当てることができます。 移動やコピーを行うには、移動またはコピー先のフォルダをクリックして選択します。表示されるフォルダリストから、目的のフォルダを選択します。 新しいフォルダを作成するには、[*新規*]をクリックします。適切なフォルダを選択した後で、［*OK*］をクリックします。作業が完了したら、［*OK*］をクリックします。

フィルタの適用

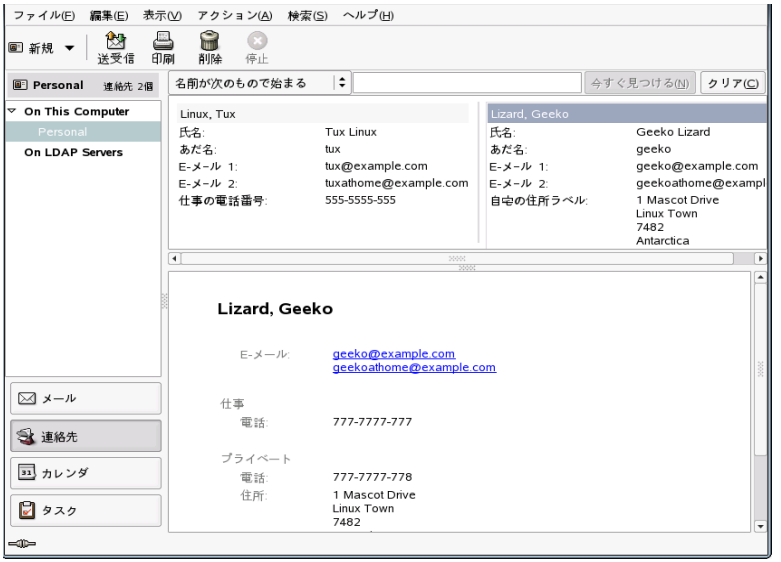
*[ツール] → [フィルタ]*の順に選択したときに開くダイアログ内にリストされている順序に従って、フィルタが適用されます。フィルタの順序は、特定のフィルタを反転表示し、［*上る*］または［*下がる*］をクリックすることにより変更できます。作業が完了したら、［*OK*］をクリックして［フィルタ］ダイアログを閉じます。

フィルタは、新しいメールメッセージすべてに対して適用されます。既にフォルダ内に存在しているメールに対して適用されることはありません。既に受信したメッセージに対してフィルタを適用するには、適用対象のメッセージを選択し、次に*[アクション] → [フィルタの適用]*の順に選択します。

11.4　連絡先

Evolutionでは、複数の異なるアドレス帳を使用できます。使用可能なアドレス帳は、左側フレームのリスト内に表示されています。特定の連絡先を検索するには、検索バーを使用します。*[ファイル]* → *[インポート]*の順に選択すると、複数の形式の連絡先をEvolutionアドレス帳へ追加できます。連絡先を右クリックするとメニューが開き、連絡先の転送や連絡先のvCardとしての保存など、さまざまなオプションを選択することができます。連絡先を編集するには、対象の連絡先をダブルクリックします。

図 11.2　Evolutionのアドレス帳



11.4.1　連絡先の追加

Evolutionでは、氏名と電子メールアドレスのほかに、個人に関する他のアドレスと連絡先の情報を格納することもできます。 メッセージプレビューで、マークされているアドレスを右クリックすると、差出人の電子メールアドレスを連絡先として簡単に追加できます。新しい連絡先を詳細に入力する場合は、［*連絡先*］ビューで［*新規*］をクリックします。どちらの場合も、表示されたダイアログで連絡先情報を入力します。

［*連絡先*］タブで、連絡先の名前、電子メールアドレス、電場番号およびインスタントメッセージのIDを入力します。［*個人情報*］には、Webアドレスおよび他の詳細情報を入力します。［*メールの住所*］には、連絡先に関する他のアドレス情報を入力します。連絡先に関する情報をすべて入力し終わったら、［OK］をクリックしてその連絡先をアドレス帳に追加します。

11.4.2　リストの作成

特定の人々に対して電子メールメッセージを頻繁に送信する場合、それらの人々のアドレスを含むリストを作成することにより、作業を簡略化できます。*[ファイル] → [新規] → [連絡先の一覧]*の順にクリックします。［連絡先一覧エディタ］が起動されます。その一覧の名前を入力します。ボックス内にアドレスを入力して［*追加*］をクリックする方法、または［*連絡先*］ビューから連絡先をドラッグしてこのボックス内にドロップする方法のどちらかでアドレスを追加します。受信者が、同じメールを受け取った他の受信者(同報受信者)を表示できるかどうかを制御するには、［*メールをこの一覧に送付したらアドレスを隠す*］をオンまたはオフにします。作業が完了したら、［*OK*］をクリックします。この一覧は、自分の連絡先の1つになり、最初の数文字を入力すると作成ウィンドウ内に表示されるようになります。

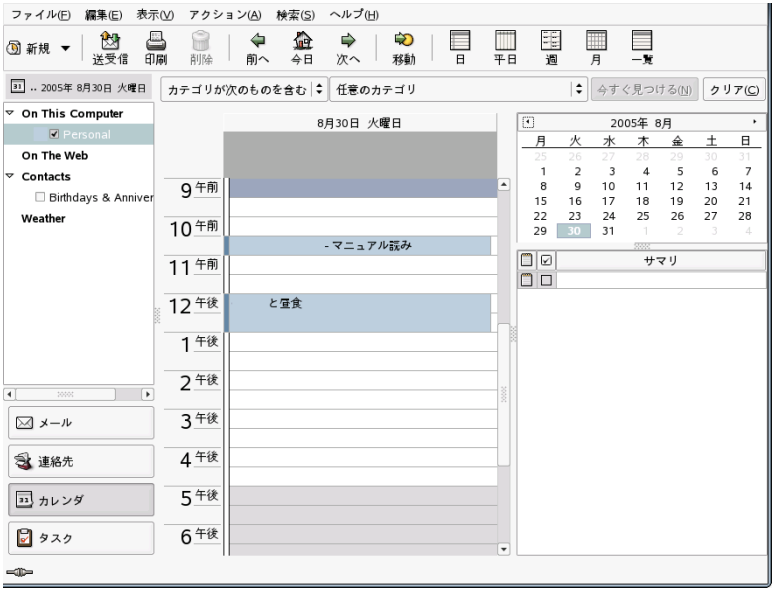
11.4.3　アドレス帳の追加

対象アカウントのアカウント設定に、GroupWiseおよびExchangeのアドレス帳を追加設定します。ローカルまたはLDAPのアドレス帳を追加するには、*[ファイル] → [新規] → [アドレス帳]*の順に選択します。 ダイアログが表示されたら、アドレス帳の種別を選択し、必要情報を入力します。

11.5　カレンダ

Evolutionでは複数のカレンダを動作させることができます。iCalendar形式でカレンダをインポートするには、*[ファイル] → [インポート]*の順に選択します。カレンダは、予定を入力したり、他のユーザとの会議をスケジュールするために使用します。 必要であれば、スケジュールされた予定が始まることを知らせるためのリマインダを設定できます。

図 11.3　Evolutionカレンダ



11.5.1　予定の追加

使用中のカレンダに新しい予定を追加するには、*[ファイル] → [新規] → [予定]*の順にクリックします。［*予定*］タブで、その予定の詳細を入力します。後で検索とソートが簡単に行えるように、必要に応じてカテゴリを選択します。 オプションとして、［アラームを*鳴らす*］を使えば、予定が始まる前に思い出させるためのアラームをセットすることができます。 その予定が定期的に実施されるようにする場合は、［*繰り返し*］タブで、繰り返される日付を設定します。すべての設定作業が終わった後で、［*OK*］をクリックします。これにより、新しい予定が使用中のカレンダ内に表示されるようになります。

11.5.2　会議のスケジュール設定

他のユーザとの会議をスケジュールするには、*[ファイル] → [新規] → [会議]*の順に選択します。その予定で自分が何を行うかに関する情報を入力します。［*招待*］または［*スケジュール*］内に出席者を追加します。 出席者をアドレ

ス帳から入力するには、［*連絡先*］を使用して、アドレス帳の連絡先のリストを開きます。［スケジュール］を使用すると、すべての出席者の都合がつく日時をスケジュール設定することもできます。 出席者が設定した後に、日時を自動的に選択するには、［*自動ピックアップ*］をクリックします。

11.5.3　カレンダの追加

GroupWiseおよびExchangeのカレンダは、アカウント設定内で指定する必要があります。ローカルまたはWebのカレンダを追加するには、*[ファイル] → [新規] → [カレンダ]*の順に選択します。目的の種別を選択し、必要情報を入力します。

11.6　ハンドヘルドとのデータの同期

Evolutionは、Palmなどのハンドヘルドデバイスとの同期がとれるように設計されています。同期をとるには、GNOME Pilotを使用します。*[ツール] → [Pilot Settings (パイロット設定)]*の順に選択して、環境設定ウィザードを起動します。詳細については、ヘルプを参照してください。

11.7　EvolutionとGroupWiseユーザ

GroupWiseのユーザは、ほとんど何の問題もなく、Evolutionで自分のGroupWiseアカウントにアクセスできます。 EvolutionとGroupWiseは、非常によく似た用語を使っています。 一方のシステムに慣れたユーザは、もう一方についても容易に学ぶことができるでしょう。

11.7.1　GroupWiseシステムにアクセスするようにEvolutionを設定する

GroupWiseシステムにアクセスするようにEvolutionを設定するには、Evolutionのメール設定アシスタントを使います。 Evolutionのメール設定アシスタントを開始するには、*[設定] → [メールのアカウント] → [追加]*の順に選択して、［*進む*］をクリックします。

身元情報のページで、GroupWiseシステムの電子メールアドレス(joe@example.comなど)を入力して、［*進む*］をクリックします。

［メールの受信］ページで、［サーバ種別］リストから［*IMAP*］を選択して、［ホスト］フィールドにGroupWiseサーバのホスト名を入力し、［Receiving Options］ページで自分のシステムに適した他の設定を行ってから、［*進む*］をクリックします。

［メールの送信］ページで、［サーバ種別］リストから［*SMTP*］を選択して、［ホスト］フィールドにGroupWiseサーバのホスト名を入力し、自分のシステムに適した他の設定を行ってから、［*進む*］をクリックします。

［アカウント管理］ページで、Evolutionの設定ページにこのアカウントが表示されるときの名前を指定して、［*進む*］をクリックします。

［*適用*］をクリックして、GroupWiseアカウントを作成します。 これで、利用可能な電子メールアカウントのリストに、GroupWiseのメールボックスが表示されます。

11.8 関連資料

Evolutionは、包括的なヘルプページを統合しています。この情報にアクセスするには、［*ヘルプ*］メニューを使用します。Evolutionの詳細については、http://www.gnome.org/projects/evolution/にあるプロジェクトのWebサイトを参照してください。

12 Kontact: 電子メールとカレンダのプログラム

Kontactは、複数のKDEアプリケーションの機能を1つの使いやすいインタフェースに統合した個人情報管理ツールです。これらのアプリケーションには、KMail (電子メール)、KOrganizer (カレンダ)、KAddressbook (連絡先管理)、およびKNotes (ノート) が含まれます。 データをPalmPilotや他のハンドヘルドデバイスなど、外部デバイスと同期させることもできます。KontactはKDEデスクトップの空いている領域に容易に配置できます。また、Kontactはさまざまなグループウェアサーバに接続します。スパムやウィルスのフィルタリング、RSSリーダなどの追加機能も備えています。

Kontactを起動するには、メインメニューで *［オフィス］*、→ *［Kontact］* の順に選択します。代わりに、コマンドラインで、「`kontact`」と入力して起動することもできます。一部の機能だけが必要な場合には、複合のアプリケーションとしてではなく、個々のコンポーネントを開くこともできます。

12.1 他のメールプログラムからの電子メールのインポート

他のアプリケーションから電子メールをインポートするには、Kontactのメールビューで *［ツール］*、→ *［メッセージをインポート］* を選択します。 現在、Outlook Express、mbox形式、電子メールテキスト形式、Pegasus Mail、Opera、およびEvolutionなどのインポートフィルタがサポートされています。インポートユーティリティは、`kmailcvt`コマンドを使用して単独で起動することもできます。

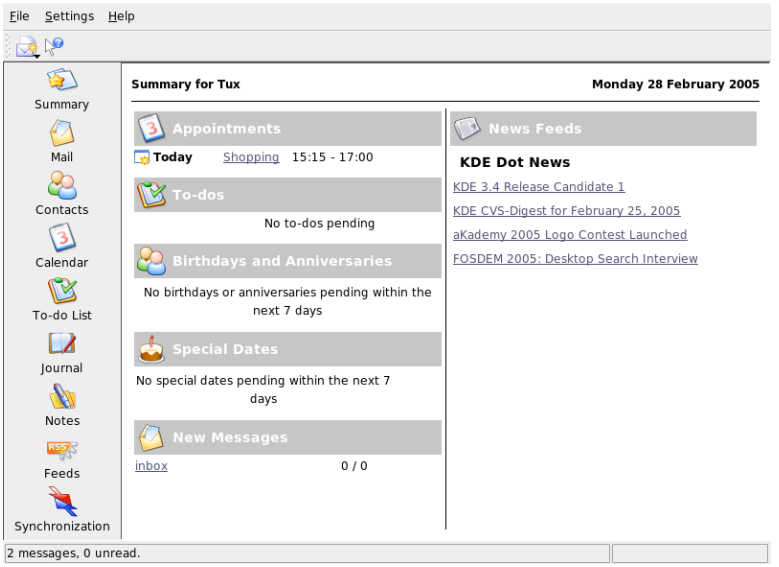
対応するアプリケーションを選択し、［次へ］をクリックします。選択したタイプによっては、ファイルまたはフォルダを指定する必要があります。その後、Kontactによって、自動的にプロセスが完了されます。

12.2 Kontactの概要

デフォルトのウィンドウビューには、図12.1.「概要が表示されたKontactウィンドウ」 (page 188)に示すように、［*概要*］が表示されます。別のコンポーネントにアクセスするには、左側のセクションにあるボタンを使用します。

［*要約*］には、近づいている誕生日やTo-Do、天気、およびKPilotの状態などの基本情報が表示されます。ニュースセクションでは、RSSフィードにアクセスして興味のある最新ニュースを読むことができます。表示される情報を設定するには、［*設定*］、→［*概要表示の設定*］を選択します。

図 12.1 概要が表示されたKontactウィンドウ



12.2.1 メール

左側のフォルダ領域には、自分のメールフォルダ(メールボックス)から成るリストがあり、メッセージの総数と未読の件数が表示されます。特定のフォルダを選択するには、そのフォルダをクリックするだけです。 そのフォルダ内のメッセージが、右上のフレームに表示されます。 フォルダ内のメッセージの件数は、アプリケーションウィンドウの下端にあるステータスバーにも表示されます。

各メッセージの件名、送信者、および受信日時が、右側のヘッダ領域に表示されます。特定のメッセージをクリックすると、そのメッセージが選択され、メッセージウィンドウ内に表示されます。列の見出し(件名、送信者、日時など)のいずれかをクリックすると、メッセージをソートできます。現在選択されているメッセージの内容は、ウィンドウのメッセージフレームに表示されます。 添付ファイルは、その添付ファイルが使用しているMIMEタイプに基づき、メッセージの最後にあるアイコンとして、またはインラインで表示されます。

さまざまなステータスフラグを使用して、メッセージにマークを付けることができます。ステータスを変更するには、*［メッセージ］*、→ *［メッセージをマーク］*を選択します。 この機能を使えば、メッセージに「重要」や「スパム」などのステータスを割り当てることができます。 たとえば、覚えておきたい重要なメッセージを強調表示することができます。検索バーの［*状態*］を使用すると、特定の状態のメッセージだけを表示できます。

12.2.2 連絡先

このコンポーネントの左上のフレームには、現在有効なアドレス帳に登録されているすべてのアドレスが表示されます。 左下のフレームには、アドレス帳と、各人が現在アクティブかどうかがリスト表示されます。右側のフレームには、現在選択されている連絡先が表示されます。上にある検索バーを使用して、特定の連絡先を検索できます。

12.2.3 To-Do List

［*To-do リスト*］には、タスクのリストが表示されます。リストに新しいタスクを追加するには、上にあるフィールドをクリックします。既存のタスクの

列を右クリックすると、その列の値を変更できます。タスクをいくつかのサブタスクに分割できます。サブタスクを作成するには、タスクを右クリックして［*新規サブTo-Do*］を選択します。 タスクを他の人々に割り当てることもできます。

12.2.4 カレンダ

カレンダビューは、複数のフレームに分割されています。デフォルトでは、今月の小さなカレンダを含むフレームと、今週の週表示を含むフレームが表示されます。To-Doリスト、現在のイベントまたはTo-Doの詳細表示、およびそれぞれの状態を示すカレンダリストもあります。別の表示を選択するには、ツールバーまたは［*表示*］メニューを使用します。

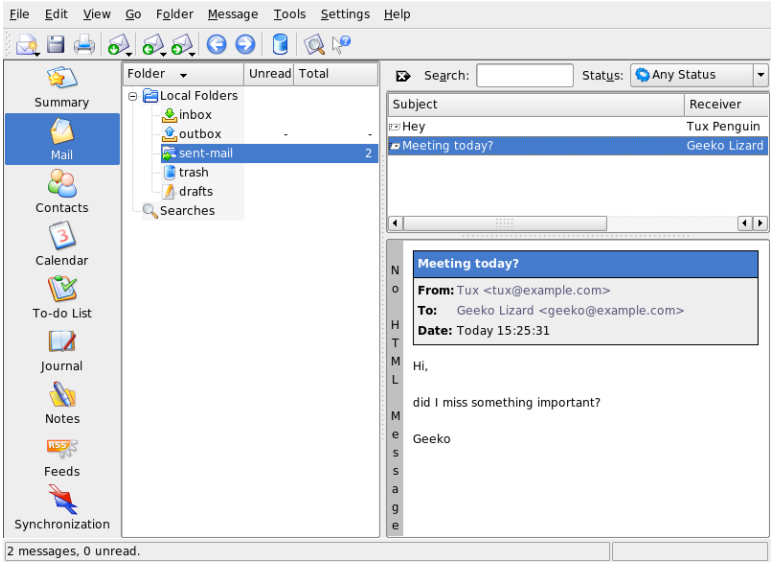
12.2.5 ノート

このコンポーネントは、覚え書きとして使用します。 KDEを使用している場合は、システムトレイのKNoteアイコンを使用すると、デスクトップに表示されるようになります。

12.3 メール

Kontactは、電子メールコンポーネントとしてKMailを使用します。KMailを設定するには、*［設定］*、→ *［KMail設定］*を選択します。KMailは機能豊富な電子メールクライアントであり、多くのプロトコルをサポートしています。［*ツール*］には、不必要なメールを管理するのに役立ついくつかのツールがあります。［*検索*］を使用すると、メッセージを詳しく検索できます。［*アンチスパムウィザード*］は不要な商用電子メールをフィルタするのに役立つ管理ツールです。［*アンチウィルスウィザード*］は電子メールウィルススキャナを管理します。これらの2つのウィザードは、外部のスパムおよびウィルスソフトウェアと連動します。 これらのオプションを無効にする場合は、スパムやウィルスに対処するための付加的なパッケージをインストールしてください。

図 12.2　Kontactのメールコンポーネント



12.3.1　アカウントの設定

Kontactでは、複数の電子メールアカウント(たとえば、自分の個人用電子メールアドレスと、ビジネス用のアドレス)を管理することができます。電子メールの作成時には、*［表示］*、→ *［個人情報］*をクリックして、定義済みのいずれかのIDを選択します。新しいIDのプロファイルを作成するには、*［設定］*、→ *［KMail設定］*を選択し、続いて、*［Identities (個人情報)］*、→ *［新規］*の順に選択します。開いたダイアログボックスで、新しいIDに付ける名前(「private」(プライベート)や「office」(オフィス)など)を入力します。［*OK*］をクリックして、追加情報を入力するためのダイアログボックスを開きます。フォルダに識別情報を割り当てて、そのフォルダ内のメッセージに返信する際に、割り当てておいた識別情報が選択されるようにすることもできます。

［*一般*］タブで［あなたの名前］、［組織］、および［E メールアドレス］を入力します。［*Cryptography*］タブでは、電子的に署名された、または暗号化されたメッセージを送信するための鍵を選択します。暗号化機能を使用するには、章 6. *KGpgによる暗号化* (page 109)で説明しているKGpgを使用して鍵を事前に作成しておく必要があります。

［*詳細*］タブでは、［返信アドレス(Reply-To)］および［BCCアドレス］の指定、辞書の選択、完成していないメッセージや送信済みメッセージを格納するフォルダの選択、およびメッセージの送信方法の定義を行えます。［*署名*］タブでは、各メッセージの最後に署名テキストを付加するかどうかを指定します。 たとえば、各メールに自分の連絡先情報を署名として追加することができます。 署名を有効にするには、［*署名を有効にする*］を選択し、ファイル、入力フィールド、コマンドの出力のいずれから署名を取得するのかを指定します。すべてのID設定が完了したら、［*OK*］をクリックして確定します。

［ネットワーク］では、Kontactによる電子メールの送受信方法を設定します。この中には2つのタブがあり、1つはメール送信用、もう1つはメール受信用です。この2つのタブの設定値の多くは、使用するメールサーバのシステムと配置先ネットワークによって大きく異なります。どのような設定値と項目を使用すればいいのかわからない場合は、ご利用のISP、またはシステム管理者に問い合わせてください。

発信用メールボックスを作成するには、［*送信*］タブで［*追加*］をクリックします。 SMTPとSendmailのいずれかの転送タイプを選択します。 ほとんどの場合、SMTPの選択が適しています。選択すると、SMTPサーバのデータを入力するためのウィンドウが表示されます。サーバの名前とアドレス(ISPによって指定されている)を入力します。サーバによって認証が要求されている場合は、［*サーバは認証が必要です*］を有効にします。［セキュリティ］タブには、セキュリティ設定項目があります。ここで、使用する暗号化手法を指定します。

［*受信*］タブ内で、電子メールの受信用の設定を行います。［*追加*］をクリックして、新しいアカウントを作成します。［ローカルメールボックス］(MboxまたはMaildir形式)、［POP3］、［IMAP］などさまざまな方法の中から、メールの取得方法を選択します。設定値は、使用するサーバに合わせてください。

12.3.2 メッセージの作成

新しいメッセージを作成するには、［*メッセージ*］、→［*新規メッセージ*］を選択するか、ツールバーの該当するアイコンをクリックします。他の電子メールアカウントからメッセージを送信するには、項12.3.1.「アカウントの設定」 (page 191)の説明に従って設定したIDのいずれかを選択します。［*宛先*に、電子メールアドレス全体を入力するか、アドレス帳に入力されている氏名またはアドレスの一部を入力します。入力した文字に一致する項目がアド

レス帳の中で見つかった場合、選択リストが表示されます。希望の連絡先をクリックします。入力に一致する項目が見つからなかった場合は、最後まで入力します。 アドレス帳から直接選択するには、アドレスのフィールドの隣にある［*Select...*］ボタンをクリックします。

メッセージにファイルを添付するには、クリップのアイコンをクリックして、添付するファイルを選択します。代わりに、デスクトップまたは他のフォルダから［*メール作成*］ウィンドウまでファイルをドラッグするか、［*添付*］メニュー内でオプションのいずれかを選択することもできます。通常は、ファイルの形式は正しく認識されます。 形式が正しく認識されない場合は、ファイルのアイコンを右クリックします。表示されるメニューから、［*プロパティ*］を選択します。 次のダイアログで形式とファイル名を設定し、説明を追加します。また、添付ファイルを署名または暗号化するかどうかも指定できます。

メッセージの作成が完了したら、［*メッセージ*］、→［*送信*］を選択して直ちに送信するか、［*メッセージ*］、→［*送信待ち*］を選択して［送信待ち］フォルダに移動します。 メールを送信すると、メッセージは正常に送信された後に［送信済みメール］フォルダにコピーされます。［送信待ち］フォルダに移動されたメッセージは、編集または削除することもできます。

12.3.3 暗号化された電子メールと署名

電子メールを暗号化するには、章 6. *KGpgによる暗号化* (page 109)で説明されているように、鍵ペアを最初に生成します。暗号化手順の詳細を設定するには、［*設定*］、→［*KMail設定*］、→［*Identities (個人情報)*］の順に選択します。次に、暗号化メッセージまたは署名済みメッセージを送信する際に使用するIDを指定します。［*変更*］をクリックします。［*OK*］をクリックして確定すると、対応するフィールドに鍵が表示されます。［*OK*］をクリックして、設定ダイアログを閉じます。

12.3.4 フォルダ

メッセージフォルダを使用すると、メッセージを整理することができます。デフォルトでは、メッセージフォルダは`~/.kde/share/apps/kmail/mail`ディレクトリにあります。 KMailを初めて起動すると、いくつかのフォルダが作成されます。［受信箱］は、サーバから取得されたメッセージが最初に置かれるフォルダです。 ［送信箱］は、送信待ちのメッセージの一時的な格

納場所です。［送信済みメール］には、送信済みのメッセージのコピーが格納されます。［ごみ箱］には、Delまたは*［編集］*、→ *［削除］*を使用して削除されたすべての電子メールのコピーが格納されます。［下書き］は、書きかけのメッセージを保存する場所です。IMAPを使用している場合は、ローカルフォルダの下にIMAPフォルダも表示されます。フォルダリストには、ローカルやIMAPなど、着信メールサーバごとのフォルダが表示されます。

メッセージを整理するためにフォルダを追加するには、*［フォルダ］*、→ *［新規フォルダ］*の順に選択してフォルダを作成します。ウィンドウが表示されるので、新しいフォルダの名前と形式を指定できます。

フォルダを右クリックすると、コンテキストメニューが表示されて、フォルダに対する操作が行えます。［*Expire*］を選択すれば、既読および未読のメッセージの保存期間と、削除やフォルダへの移動など、その期間の終了後に行う処理を指定できます。メーリングリストのメッセージを格納するためにフォルダを使用する場合には、*［フォルダ］*、→ *［Mailing List Management］*の順に選択して、必要なオプションを設定します。

あるフォルダから別のフォルダに1つ以上のメッセージを移動するには、移動対象のメッセージを選択し、Mを押すか、*［メッセージ］*、→ *［移動］*を選択します。フォルダのリストが表示されるので、メッセージの移動先として使用するフォルダを選択します。上のウィンドウ内にあるメッセージをドラッグし、左のウィンドウ内にある適切なフォルダにドロップする方法で、メッセージを移動することもできます。

12.3.5　フィルタ

フィルタは、着信メールを自動的に処理するための便利な方法です。送信者やサイズなどのメールの特徴に基づいて、メールを特定のフォルダに移動したり、不要なメールを削除したり、メールを送信者に返送します。

フィルタの作成

フィルタを新規に作成するには、*［設定］*、→ *［フィルタの設定］*を選択します。既存のメッセージに基づいてフィルタを作成するには、見出しリストでメッセージを選択して右クリックし、*［ツール］*、→ *［フィルタを作成］*を選択して、フィルタの条件を選択します。

フィルタ条件の照合方法(すべて、またはいずれか)を選択します。次に、対象のメッセージだけに適用する条件を選択します。［*フィルタアクション*］で、条件に一致するメッセージに対するフィルタのアクションを設定します。［*詳細オプション*］では、フィルタをいつ適用するか、対象のメッセージに対してフィルタを追加するかどうかを設定します。

フィルタの適用

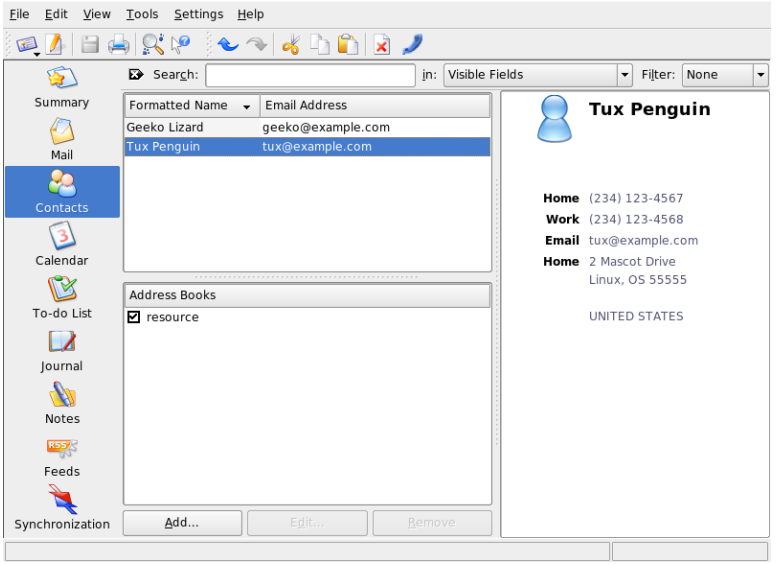
フィルタは、右クリックして*［設定］→［フィルタを作成］*を選択したときに開くダイアログ内にリストされている順序に従って、適用されます。特定のフィルタを選択し、矢印ボタンをクリックすることにより、順序を変更できます。フィルタは、［詳細オプション］で指定した新着メッセージと送信メッセージだけに適用されます。受信済みのメッセージにフィルタを適用するには、適用対象のメッセージを選択して、*［メッセージ］、→［フィルタの適用］*を選択します。

フィルタが期待どおりに機能しない場合は、*［ツール］、→［フィルタログビューア］*を使用して監視できます。このダイアログでログ機能を有効にすると、フィルタがどのようにメッセージを処理したか記録されるので、問題の特定に役立ちます。

12.4　連絡先

Kontactは、連絡先コンポーネントとしてKAddressBookを使用します。KAddressBookを設定するには、*［設定］、→［KAddressBookを設定］*を選択します。特定の連絡先を検索する場合は、検索バーを使用します。［*フィルタ*］を使用すると、特定のカテゴリの連絡先だけを表示できます。連絡先を右クリックするとメニューが表示され、さまざまなオプションを選択できます。たとえば、電子メールで連絡先情報を送信することができます。

図 12.3　Kontactのアドレス帳



12.4.1　連絡先の追加

電子メール内の名前や電子メールアドレスを使用して連絡先を追加するには、メール内のアドレスを右クリックして［*アドレス帳で開く*］を選択します。新しい連絡先を追加するには、［*ファイル*］、→［*新規連絡先*］を選択します。どちらの方法でもダイアログが表示されるので、連絡先に関する情報を入力します。

［*一般*］タブでは、名前、電子メールアドレス、電話番号などの連絡先の基本情報を入力します。カテゴリを使用してアドレスをソートすることもできます。［*詳細*］では、誕生日や配偶者の名前など、より個人的な情報を入力します。

連絡先でインスタントメッセンジャを使用している場合は、［*IMアドレス*］にそのIDを追加できます。この操作を実行して、KopeteなどのKDEチャットプログラムをKontactとともに実行すると、これらのIDに関する状態情報がKontactに表示されます。［*暗号設定*］には、連絡先の暗号化データ(公開鍵など)を入力します。

［*その他*］には、写真や予定の有無情報の場所など、ユーザの追加情報を入力します。連絡先またはアドレス帳に自分自身の情報を追加する場合は、［*カスタムフィールド*］を使用します。

連絡先をさまざまな形式でインポートすることもできます。インポートするには、*［ファイル］*、→ *［インポート］*を使用して形式を選択します。次に、インポートするファイルを選択します。

12.4.2 配布リストの作成

特定のグループの人々に頻繁に電子メールのメッセージを送信する場合には、配布リストを作れば、複数のメールアドレスを1つの連絡先項目として保管できるので、グループにメールを送信するたびに、個々の名前を入力する必要がなくなります。まず、*［設定］*、→ *［拡張バーを表示］*、→ *［送付リストエディタ］*の順に選択します。表示される新しいセクションで、［*新規リスト*］をクリックします。リストの名前を入力し、［*OK*］をクリックします。連絡先をアドレスリストから送付リストウィンドウにドラッグアンドドロップして、リストに追加します。このリストは、メールを作成するときに、個人の連絡先と同じように使用できます。

12.4.3 アドレス帳の追加

重要項目: グループウェアのアドレス帳

グループウェアリソースを追加するには、個別のツールであるGroupware Wizardを使用するのが最善の方法です。 これを使用するには、Kontactを終了してから、コマンドラインで`groupwarewizard`を実行するか、KDEメニューのオフィスのグループから選択します。表示されるリストからSLOX、Groupwise、Exchangeなどのサーバタイプを選択し、アドレスと認証データを入力します。使用可能なリソースがKontactに追加されます。

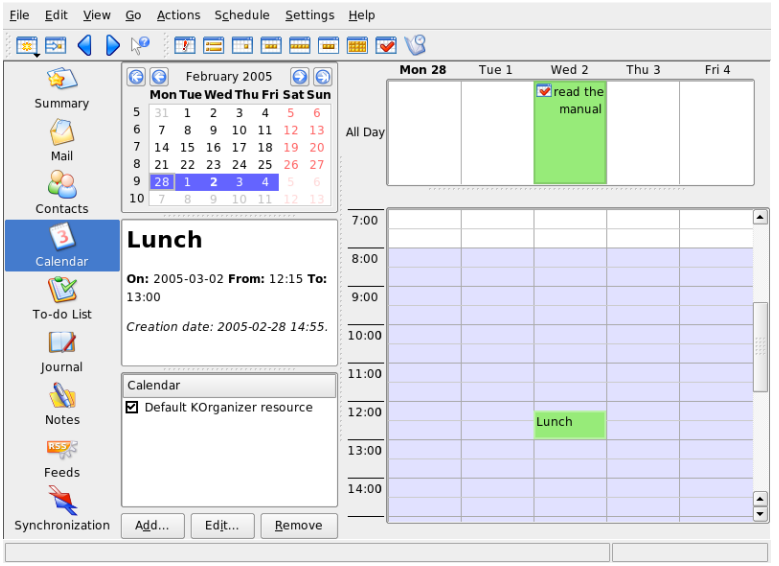
Kontactは複数のアドレス帳にアクセスできます。たとえば、Novell GroupWiseやLDAPサーバが提供する共有のアドレス帳があります。現在のアドレス帳を表示するには、*［設定］*、→ *［拡張バーを表示］*、→ *［アドレス帳］*の順に選択します。アドレス帳を追加する場合は、［*追加*］をクリックし、タイプを選択して必要な情報を入力します。

アドレス帳の前のチェックボックスは、それぞれの有効状態を示します。 アドレス帳を削除せずに非表示にするには、そのチェックボックスをオフにします。［*削除*］を選択すると、選択したアドレス帳がリストから削除されます。

12.5　カレンダ

Kontactは、カレンダコンポーネントとしてKOrganizerを使用します。KOrganizerを設定するには、［*設定*］、→［*KOrganizerの設定*］を選択します。カレンダでは、アポイントを入力したり、会議をスケジューリングしたりします。必要に応じて、今後のイベントの通知を設定できます。［ファイル］メニューのオプションを使用して、カレンダのインポート、エクスポート、およびアーカイブを行うこともできます。

図 12.4　Kontactのカレンダ



12.5.1　イベントのスケジューリング

新しいイベントまたは会議を追加するには、［*アクション*］、→［*新規イベント*］を選択します。必要な詳細情報を入力します。 ［アラーム］では、出

席者にイベントを通知する時間(何日前、何時前、何分前など)を正確に指定します。 繰り返し実施されるイベントの場合は、間隔を指定します。カレンダの特定の時点にイベントを作成するもう1つの方法は、プログラムのいずれかのカレンダビューで、対応するフィールドをダブルクリックすることです。これによって、メニューから実行した場合と同じダイアログウィンドウが表示されます。 または、カレンダ表示で時間の範囲を選択して、右クリックします。

ダイアログに手動でデータを入力するか、またはアドレス帳からデータを挿入してイベントの出席者を指定します。 手動で入力する場合は、［*新規*］を選択します。データをアドレス帳からインポートする場合は、［*アドレスの選択*］をクリックしてダイアログから該当するエントリを選択します。出席者の予定に合わせてイベントをスケジューリングするには、［*予定の有無*］を選択して［*日付を選択*］をクリックします。

定期的に実施されるイベントを設定するには、［*繰り返し*］タブを使用します。その他の情報(議事録など)をイベントにリンクするには、［*添付ファイル*］を使用できます。

12.5.2 カレンダの追加

重要項目: グループウェアのカレンダ

グループウェアリソースを追加するには、個別のツールであるGroupware Wizardを使用するのが最善の方法です。 これを使用するには、Kontactを終了してから、コマンドラインで`groupwarewizard`を実行するか、KDEメニューのオフィスのグループから選択します。表示されるリストからSLOX、Groupwise、Exchangeなどのサーバタイプを選択し、アドレスと認証データを入力します。 使用可能なリソースがKontactに追加されます。

カレンダモジュールは、同時に複数のカレンダに接続できます。この機能は、個人のカレンダを組織のカレンダに統合する場合などに役立ちます。新しいカレンダを追加するには、［*追加*］をクリックしてカレンダタイプを選択します。必須フィールドにデータを入力します。

カレンダの前のチェックボックスは、それぞれの有効状態を示します。 カレンダを削除せずに非表示にするには、そのチェックボックスをオフにします。［*削除*］を選択すると、選択したカレンダがリストから削除されます。

12.6 ハンドヘルドとのデータの同期

Kontactは、データをPalmなどのハンドヘルドデバイスと同期できるように設計されています。KPilotの状態に関する情報が概要に表示されます。KPilotの設定と使用方法の詳細については、章13.*KPilotによるハンドヘルドコンピュータの同期* (page 203)を参照してください。

12.7 KontactとGroupWiseユーザ

GroupWiseの使用に慣れていれば、ほとんど問題なくKontactに合わせることができるでしょう。これら2つのプログラムは多くの概念を共有しており、提供しているサービスの多くも共通しています。このセクションでは、注意すべき用語の違いと、GroupWiseユーザがKontactを十分に活用するためのヒントについて説明します。

12.7.1 用語の違い

次のテーブルでは、KontactとGroupWiseでの用語の主要な違いを示しています。

表 12.1 KontactとGroupWiseの用語の違い

GroupWise	Kontact
予定	イベント
予定の有無	Free/Busy
ノート	Journalのエントリ
ポストされた/ポストされていない項目	出席者のないイベントは、ポストされます。イベントに主席者がある場合には、送信済みの項目になります。
タスク	To-do

12.7.2 GroupWiseユーザのためのヒント

このセクションでは、GroupWiseのユーザが、GroupWiseとKontactの相違点に対処するために役立つヒントを説明します。

連絡先情報

GroupWise Messengerと電子メールの連絡先は、Kontactの連絡先情報に追加することができます。. それから、［コンタクト］表示の名前を右クリックして、電子メールを作成したり、インスタントメッセージングセッションを開始したりすることができます。

カラーコード

GroupWiseの項目、および他のソースからの項目にカラーコードを付けると役立ちます。 カラーコードを付ければ、電子メール、連絡先、特定のソースからの項目についての他の情報をスキャンするのが簡単になります。

イベントに出席者を招待する

GroupWiseとは異なり、Kontactでは、自分がスケジュールしたイベントに自分自身を自動的に出席者として入れることはありません。 自分自身を招待することを忘れないようにしてください。

12.8 関連資料

Kontactには、Kontactとその各種コンポーネントのヘルプが含まれています。ヘルプにアクセスするには、*［ヘルプ］*、→ *［Kontact Handbook (Kontactハンドブック)］*を選択します。このプロジェクトのWebページhttp://www.kontact.orgも参考になります。

KPilotによるハンドヘルドコンピュータの同期 13

ハンドヘルドコンピュータは、スケジュール、To-doリスト、メモなどをどこにでも持ち歩くユーザの間に広く普及しています。多くの場合、ユーザはデスクトップとポータブルデバイスの両方で同じデータを使用することを求めます。そこで役に立つのがKPilotです。これは、ハンドヘルドのデータをKontactの構成要素であるKAddressBook、KOrganizer、KNotesなどのKDEアプリケーションと同期するためのツールです。

KPilotの主な目的は、ハンドヘルドコンピュータのアプリケーションとそれに対応するKDEアプリケーション間のデータの共有です。KPilotには、メモビューア、アドレスビューア、およびファイルインストーラが組み込まれていますが、これらはKPilot環境以外では使用できません。しかしファイルインストーラを除いて、これらの機能はすべて、別の独立したKDEアプリケーションで実現できます。

KPilotは、ハンドヘルドと別のデスクトッププログラム間の通信をコンジットによって処理しています。KPilot自体は、2つのコンピュータデバイス間のデータ交換を監視するプログラムです。ハンドヘルドの特定の機能をデスクトップコンピュータで使用するには、対応するコンジットを有効にして設定する必要があります。ほとんどの場合、コンジットは特定のKDEプログラムとの連携を前提に設計されているので、一般に、他のデスクトップアプリケーションでは使用できません。

時間同期コンジットは、ユーザが表示できるプログラムを持たない点で特殊です。これは同期操作のたびにバックグラウンドでアクティブ化されますが、ネットワークタイムサーバを使用して時間のずれを修正するコンピュータ上でしか有効化できません。

同期を開始すると、コンジットが次々にアクティブ化され、データ転送を実行します。次の2とおりの同期方法があります。HotSync操作は、コンジットが有効化されているデータのみを同期させるのに対し、バックアップ操作はハンドヘルド上に格納されているすべてのデータの完全バックアップを実行します。

中には同期操作時に一定のファイルを開くコンジットもあるので、操作時には対応するプログラムを終了しておく必要があります。特に、KOrganizerは同期操作中には実行しないでください。

13.1 KPilotが使用するコンジット

KPilotで使用できるコンジットを有効化して設定するには、*[設定] → [KPilotを設定]*の順に選択します。以下では、いくつかの重要なコンジットを紹介します。

アドレス帳
このコンジットは、ハンドヘルドのアドレス帳とのデータ交換を処理します。この連絡先を管理するKDEの対応アプリケーションはKAddressBookです。これは、メインメニューまたは`kaddressbook`コマンドを使用して起動します。

KNotes/Memos
このコンジットは、KNotesで作成したメモをハンドヘルドのメモアプリケーションに転送します。このKDEアプリケーションは、メインメニューまたは`knotes`コマンドを使用して起動します。

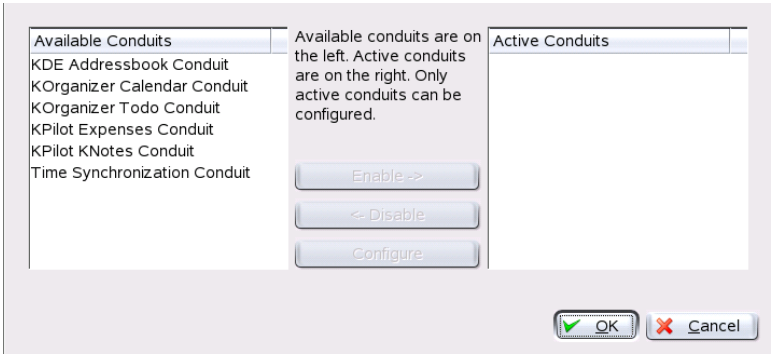
Calendar (KOrganizer)
このコンジットは、ハンドヘルドの予定(イベント)を同期します。これに対応するKDEアプリケーションはKOrganizerです。

ToDos (KOrganizer)
このコンジットは、タスク(to-do)アイテムを同期します。これに対応するKDEアプリケーションはKOrganizerです。

時間同期コンジット
このコンジットを有効化すると、同期操作時にハンドヘルドのクロックがデスクトップコンピュータのクロックに合わせて調整されます。これは、

デスクトップコンピュータ自体のクロックが、タイムサーバによって頻繁に修正されている場合のみお勧めします。

図 13.1　利用可能なコンジットが表示された設定ダイアログ



13.2　ハンドヘルド接続の設定

KPilotを使用するには、まず、ハンドヘルドコンピュータとの接続をセットアップします。設定は、ハンドヘルドで使用するクレードル(ドッキングユニット)のタイプによって異なります。これには、USBクレードル(またはケーブル)とシリアルクレードル(またはケーブル)の2種類があります。

13.2.1　KPilotでの接続の設定

接続をセットアップする最も簡単な方法は、設定ウィザードを使用することです。*[設定] → [Configuration Assistant (設定ウィザード)]*の順に選択してウィザードを起動します。最初のステップでは、ユーザ名およびハンドヘルドが接続されているデバイスの名前を入力します。［*Autodetect Handheld & Username (ハンドヘルドとユーザ名を自動検出)*］をオンにすると、ウィザードは自動検出を試みます。自動検出に失敗した場合は、項13.2.2.「/dev/pilotリンクの作成」 (page 206)を参照してください。

［次］をクリックすると、同期に使用するアプリケーションを指定するように求められます。［General KDE-PIM suite］(デフォルト)、［Evolution］、［No sync, just backup］の中から選択できます。アプリケーションを選択したら、［完了］をクリックしてウィンドウを閉じます。

13.2.2 /dev/pilotリンクの作成

シリアルハンドヘルドクレードルとの接続のセットアップ方法は、USBクレードルの場合と異なります。どちらのクレードルを使用しているかによって、/dev/pilotという名前のシンボリックリンクの作成が必要になることがあります。

USB
通常、USBクレードルは自動検出されるため、上記のシンボリックリンクを作成する必要はありません。

シリアル
シリアルクレードルの場合は、実際にどのシリアルポートに接続されているのかを調べる必要があります。シリアルデバイスには、/dev/ttyS?という名前が付けられています。最初のポートを使用しているデバイスの名前は、/dev/ttyS0です。第1シリアルポートに接続されているクレードルをセットアップするには、次のコマンドを入力します。

```
ln -s /dev/ttyS0 /dev/pilot
```

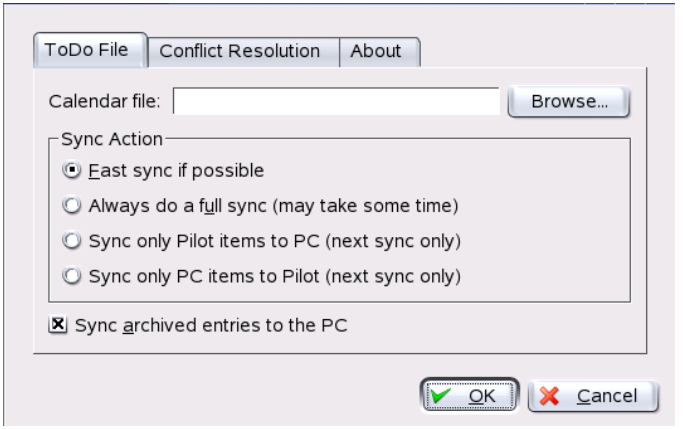
13.3 KAddressBookコンジットの設定

最初は、デフォルト設定を変更せずにKAddressBookコンジットを有効にするだけで十分です。詳しい設定は、初めてデータを同期した後に行います。設定するのは、競合が発生した場合の処理、バックアップデータベースの保存方法、ハンドヘルドに格納されている特定のフィールドをKAddressBookで想定されるフィールドに割り当てる方法などです。

13.4 タスク(to-do)アイテムとイベントの管理

KDEデスクトップでは、to-do(タスク)とイベント(予約)がKOrganizerによって管理されます。このアプリケーションは、メインメニューまたはkorganizerコマンドを使用して起動するか、またはKontactの一部として起動します。KPilotのカレンダとto-doのコンジットを有効にした後、オプションを設定してから使用します。

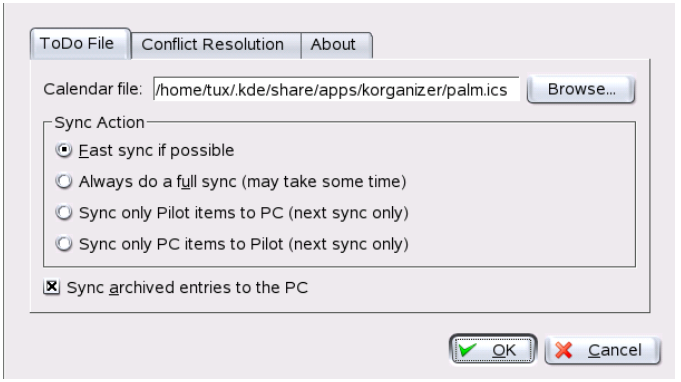
図 13.2　KPilotの設定



KOrganizerは、ファイルを`~/.kde/share/apps/korganizer`ディレクトリに格納します。しかし、`.kde/`ディレクトリはピリオドで始まっているので、ファイル選択ダイアログに表示されないことがあります。この場合、完全パスを手動で入力するか、またはファイル選択ダイアログで隠しファイル(ドットファイル)を表示するように明示的に切り替えます。そのためのデフォルトのショートカットはF8です。

`~/.kde/share/apps/korganizer`ディレクトリを開いたら、KOrganizerがカレンダファイルとして使用できるファイルを選択します。 この例では、`palm.ics`ファイルです。ユーザ名が`tux`の場合、完全パス名は`/home/tux/.kde/share/apps/korganizer/palm.ics`になります(図 13.3.「KOrganizerのカレンダファイルへのパスを示すダイアログ」 (page 208)を参照)。

図 13.3　KOrganizerのカレンダファイルへのパスを示すダイアログ

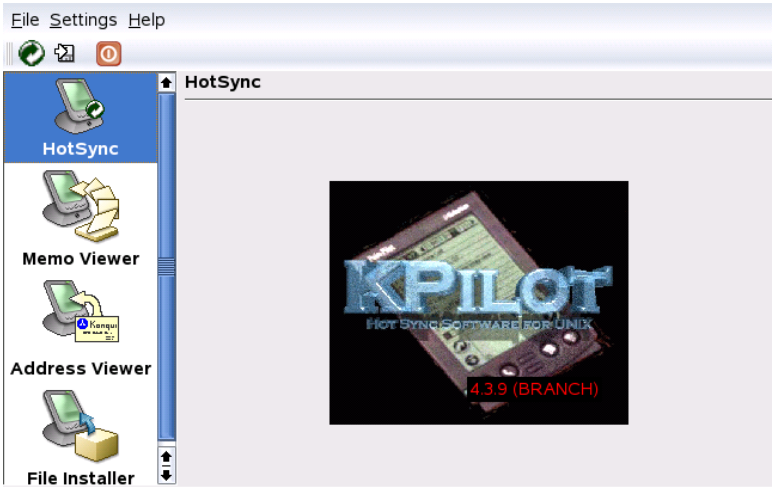


ハンドヘルドとのデータ交換中にKOrganizerは実行しないでください。実行すると、KPilotは同期操作に失敗します。

13.5　KPilotの使用

KDEアプリケーションのデータは、簡単にハンドヘルドコンピュータのデータと同期できます。KPilotを起動し、クレードルのHotSyncボタンを押して同期操作を開始するだけです。

図 13.4　KPilotのメインウィンドウ



13.5.1　ハンドヘルドのデータのバックアップ

完全バックアップを行うには、*[ファイル]* → *[バックアップ]*の順に選択します。バックアップは次の同期操作の際に実行されます。その後、メニューから*[ファイル]* → *[HotSync]*の順に選択して通常の同期に戻します。そうしなければ、次の同期操作の際に、時間のかかる完全バックアップが再度実行されます。

完全バックアップを行うと、ハンドヘルドのすべてのプログラムとデータベースが`~/.kde/share/apps/kpilot/DBBackup/USERNAME`に格納されます。ここで、*USERNAME*は、ハンドヘルドに登録されているユーザ名です。

KPilotには内蔵ビューアが2つあり、アドレスやメモを簡単に確認するために使用できますが、実際にこのデータを管理することはできません。前に触れたKDEアプリケーションの方が、はるかにこのような作業に適しています。

13.5.2 ハンドヘルドへのプログラムのインストール

［ファイルインストーラ］モジュールは、ハンドヘルドプログラムをインストールするための便利で興味深いツールです。ハンドヘルドプログラムの拡張子は一般に.prcで、ハンドヘルドにアップロードするとすぐに起動します。このようなアドオンプログラムを使用する前に、付属のライセンスと説明を確認してください。

13.5.3 アドレス帳とカレンダの同期

カレンダとアドレスを同期するには、KDEのMultiSynKツールを使用します。このツールは、`multisynk`コマンドを使用して起動します。データを同期する前にKonnectorペアを作成してください。*[ファイル]* → *[新規作成]*の順に選択し、各自のKonnectorを選択します。［*Ok*］を選択して終了します。

名前がメインウィンドウに表示されます。ハンドヘルドコンピュータとの間で同期するには、*[ファイル]* → *[Sync]*の順に選択します。

14

Beagleを使う

Beagleは、個人の情報スペースにインデックスを作成して、必要な情報を見つけ出すのを助けるサーチツールです。Beagleを使えば、ドキュメント、電子メール、Webの履歴、インスタントメッセンジャーやITCの会話記録、ソースコード、イメージ、音楽ファイル、アプリケーションやその他のものを検索できます。

Beagleは、以下のデータソースをサポートしています。

- ファイルシステム
- アプリケーションランチャ
- Evolutionのメールとアドレス帳
- Gaimのインスタントメッセージングのログ
- FirefoxのWebページ(すでに閲覧したもの)
- BlamおよびLifereaのRSS記録
- Tomboyのメモ

また、以下のファイル形式もサポートしています。

- OpenOffice.org
- Microsoft Office (doc、ppt、xls)

- HTML
- PDF
- イメージ(jpeg、png)
- オーディオ(mp3、ogg、flac)
- AbiWord
- Rich Text Format (rtf)
- Texinfo
- manページ
- ソースコード(C、C++、C#、Fortran、Java、JavaScript、Pascal、Perl、PHP、Python)
- プレーンテキスト

Beagleは、ホームディレクトリにあるすべてのものからインデックスを作成しますが、特定のファイルやディレクトリを除外するように指定することもできます。Beagleには、データを検索するために使える様々なツールも含まれています。

14.1 データのインデックス作成

Beagleデーモン(`beagled`)は、すべてのインデックス作成を自動的に行います。デフォルトでは、ホームディレクトリにあるすべてのものがインデックス作成の対象になります。Beagleは、ホームディレクトリに加えられた変更を検出して、それに応じてデータのインデックスを作り直します。

- ファイルは、作成されるとすぐにインデックスが作成され、修正されるとインデックスが作り直され、削除されるとインデックスから除外されます。
- 電子メールのインデックスは、受信したときに作成されます。

- IMの会話のインデックスは、チャットを行っているときに同時に作成されます。

インデックスを作成するにはCPUパワーをかなりの程度必要としますが、Beagleデーモンはできる限り影響の少ない仕方で行うように努めます。デーモンはスケジューラを持っており、ワークステーションが実際に使用中なのかどうかに基づいて、タスクの優先順位を決め、CPUの使用状況を制御します。

14.1.1 ファイルやディレクトリをインデックス作成の対象から除外する

特定のディレクトリ(およびそのすべてのサブディレクトリ)をインデックス作成の対象から除外したい場合には、`.noindex`という名前の空のファイルを作成し、それをそのディレクトリに置いてください。ファイルやディレクトリのリストを`.noindex`ファイルに記述すれば、それらのファイルやディレクトリをインデックス作成の対象から除外することができます。`.noindex`ファイルでは、ワイルドカードを使用することができます。

また、インデックス作成を行わないファイルのリストを`.neverindex`ファイルに記述して、ホームディレクトリに置くこともできます。このファイルでも、ワイルドカードを使用することができます。`glob`コマンドと同じワイルドカードを使用することができます(たとえば`f*le??.txt`など)。また、パターンの前後にスラッシュを置けば、さらに強力な正規表現を使うこともできます(たとえば、`/file.*.txt/`など)。詳細は、glob-UNIXのWebサイト(http://docs.python.org/lib/module-glob.html)を参照してください。

14.1.2 手動でのインデックス作成

Beagleは、いつインデックスを作成したらよいかを判断する効率的なシステムを持っており、実行されている他のアプリケーションに影響を及ぼさないように努めます。デスクトップの使用に悪影響が出ないように、負荷と、システムがアイドル状態かどうかに基づいて、インデックスの作成を行います。しかし、ホームディレクトリのインデックスをすぐに作成させたい場合には、Beagleを実行する前に、ターミナルウィンドウで次のコマンドを入力してください。

```
export BEAGLE_EXERCISE_THE_DOG=1
```

14.1.3 インデックスのステータスをチェックする

Beagleには次のコマンドが含まれており、これを使って現在のインデックスのステータスを確認することができます。

`beagle-index-info`
いくつのドキュメントのインデックスが作成されたかということと、それらのドキュメントのタイプを表示します。

`beagle-status`
Beagleデーモンが現在行っていることを、リアルタイムで表示します。

14.2 データの検索

Beagleには以下のツールが用意されており、作成されたインデックスに基づいてデータ全体を検索することができます。

14.2.1 Best

Best (Bleeding Edge Search Tool)は、インデックスが付けられた情報全体を検索するためのグラフィカルツールです。Bestは、インデックスのクエリを直接行うわけではありません。検索語をBeagleデーモンに渡して、マッチした結果を受け取ります。それから結果を表示し、マッチしたオブジェクトに対する操作を行えるようにします。

KDEでBestを起動するには、*[K Menu]* → *[システム]* → *[ファイルシステム]* → *[Beagle Search]*を選択します。GNOMEでは、*[アプリケーション]* → *[システム]* → *[ファイルシステム]* → *[Beagle Search]*を選択します。

Bestを使うには、上部にある入力ボックスに検索するテキストを入力して、Enterを押すか、［*Find*］をクリックします。Bestはインデックスが付けられたファイルに対してクエリを行い、結果を返します。

図 14.1　Beagleの検索結果

結果のリストを基にして、ファイルを開く、ファイルをメールで送る、インスタントメッセージを送る、ファイルを再生する、ファイルを転送する、ファイルマネージャでファイルを表示するなどの操作を行うことができます。行える操作は、ファイルのタイプごとに異なります。

また、［*Anywhere*］を使って、検索するファイルの対象を、アドレス帳やWebページなど特定の場所に制限すること、または結果リストの中の特定のタイプのファイルだけを表示することもできます。

14.2.2 beagle-query

Beagleには、Beagleのインデックスを検索するためのコマンドラインツールがあります。このツールを使うには、ターミナルウィンドウから次のコマンドを入力します。

```
beagle-query search
```

*search*の部分を検索するテキストで置き換えてください。beagle-queryツールは結果を返します。1このコマンドではワイルドカードが使えます。

`beagle-query --verbose` *search*を使えば、検索結果についての詳細な情報を表示することができます。

パート V. グラフィックス

15 デジタルカメラとLinux

正しいツールがある場合、カメラで撮った写真を管理するのは楽しいことです。Linuxには、写真をソートし整理するために簡単に使用できる複数の手段があります。これにはgphoto2、Konqueror、Digikam、およびf-spotが含まれます。

サポートされているカメラの詳しいリストは、`http://www.gphoto.org/proj/libgphoto2/support.php`で入手できます。gphoto2がインストールされている場合、`gphoto2 --list-cameras`コマンドを使用して、このリストを取得できます。利用できるコマンドに関する詳細は、`gphoto2 --help`コマンドを参照してください。

ティップ: サポートされないカメラ

gphotoのリスト内にご使用のカメラがない場合でも、あきらめることはありません。ご使用のカメラが、USB大容量ストレージデバイスとしてサポートされている可能性があります。詳細情報については、項15.2.「カメラへのアクセス」 (page 220)を参照してください。

15.1 カメラへの接続

デジタルカメラをコンピュータにすばやく、そして最も便利に接続する方法は、USBを使用することです。 この場合、カーネル、カメラ、およびコンピュータがUSBをサポートしていることが条件になります。標準的なSUSE

カーネルは、USBサポートを提供しています。ほかに、適切なケーブルも必要です。

単純にカメラをUSBポートに接続し、カメラの電源をオンにします。カメラを特別なデータ転送モードに切り替える必要が生じることもあります。実際の手順については、使用中のデジタルカメラのマニュアルを参照してください。

15.2 カメラへのアクセス

カメラにある写真にアクセスするには3つの方法があります。その方法は、カメラとカメラがサポートするプロトコルによって異なります。通常、これはUSBマスストレージで、hotplugシステム、またはPTP (PictBridgeとも呼ばれる)によって扱われます。カメラのモデルによっては、どちらのプロトコルでも動作しないことがあります。このようなものをサポートするために、gphoto2には固有のドライバが含まれています。

最も簡単なのは、ご使用のカメラがUSB大容量ストレージをサポートする場合です。この方法が使用できるか不明な場合は、ご使用のカメラのマニュアルを参照してください。PTP、USB大容量ストレージといった2つのプロトコルをサポートするカメラもあります。残念なことに、独自のプロトコルを使用して通信するカメラもあり、この場合は作業が複雑になります。ご使用のカメラが、USB大容量ストレージまたはPTPをサポートしない場合、以下の説明は機能しません。`gphoto2 --list-cameras`および`http://www.gphoto.org/`にある情報を試してください。

ご使用のカメラがUSB大容量ストレージデバイスに切り替えることができる場合、このオプションを選択してください。ご使用のカメラをご使用のコンピュータにUSBポートを使用して接続し、電源を投入します。カメラはホットプラグシステムにより検出されます。これによりデバイスは自動的にマウントされますので、簡単にアクセス可能になります。マウントが成功した後にKDEデスクトップにカメラアイコンが表示されます。

カメラのマウントが成功した後に、`/media`の下の新しいディレクトリに、`usb`といろいろな数字で始まる新しいディレクトリが作成されます。ベンダと製品それぞれに一意の数字が割り当てられるので、デバイスをコンピュータに接続すると、いつも同じ名前になります。USBバスに接続したものの種類により、異なるエントリが表示されます。残る問題はご使用のカメラのエ

ントリを見つけることです。これらのディレクトリ(`DCIM/xxx`)の1つをリストし、どのような結果が生じるかを確認してください。それぞれのカメラは異なるツリー構造を持っているので、ツリー構造に関する一般的なルールはありません。JPEGファイルがディレクトリ内にあるならば、おそらくそれがカメラのエントリです。

正確なディレクトリが見つかった後に、Konquerorのようなファイルマネージャまたは単純なシェルコマンド(項27.3.「Linuxの重要なコマンド」 (page 437)および「リファレンス」を参照してください)を使用して、ご使用のカメラのファイルをコピー、移動、または削除できます。

15.3 Konquerorの使用方法

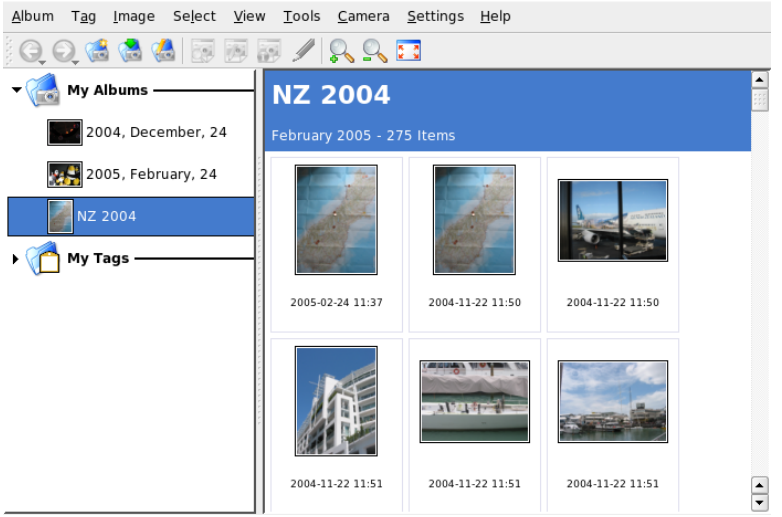
KDEユーザは、使い慣れたKonquerorインタフェースを使用して、デジタルカメラに容易にアクセスすることができます。まず、カメラをUSBポートに接続します。カメラのアイコンがデスクトップ上に表示されるはずです。そのアイコンをクリックすると、Konqueror内に、カメラの内容が表示されます。Konqueror内でURL`camera:/`を入力する方法で、そのカメラにアクセスすることもできます。ファイルが表示されるまで、カメラのディレクトリ構造内を順に移動します。Konquerorの通常のファイル管理機能を使用して、必要に応じてファイルをコピーします。Konquerorの使用方法に関する詳細は、章 3. *Webブラウザ Konqueror* (page 79)を参照してください。

15.4 Digikamの使用方法

Digikamは、デジタルカメラから写真をダウンロードするKDEのプログラムです。Digikamを初めて実行すると、フォトアルバムを保存する場所を尋ねます。写真のコレクションがすでに含まれているディレクトリを指定した場合、Digikamは各サブフォルダをアルバムとして扱います。

Digikamを起動すると、2つの部分からなるウィンドウが表示されます。ユーザのアルバムは左側に表示され、現在のアルバムの写真は右側に表示されます。図 15.1.「Digikamのメインウィンドウ」 (page 222)を参照してください。

図 15.1　Digikamのメインウィンドウ



15.4.1　カメラの設定

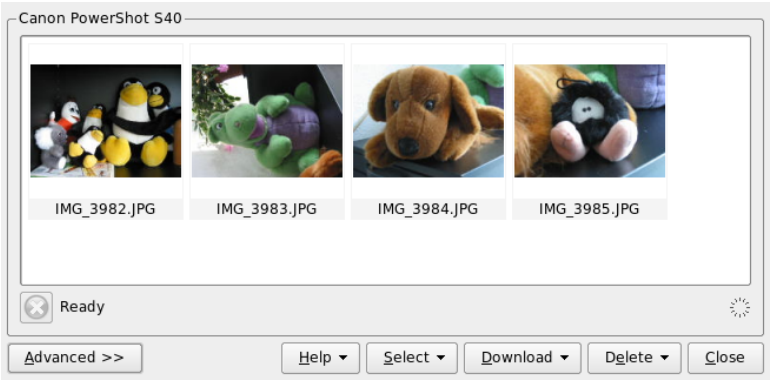
Digikam内でカメラを設定するには、*[カメラ] → [Add Camera(カメラの追加)]* の順に選択します。 最初に、［*Auto-Detect*］を使用して、カメラの自動検出を試します。この方法が失敗した場合、［*追加*］を使用して、リストを参照して、使用中のモデルを探します。使用中のカメラモデルがこのリスト内にない場合は、それより古いモデルを試してみます。または［*USB/IEEE mass storage camera (USB/IEEE大容量ストレージカメラ)*］を使用します。［*Ok*］をクリックして、設定を確定してください。

15.4.2　カメラからの写真ダウンロード

カメラを正しく設定した後に、［カメラ］メニューおよび項15.4.1.「カメラの設定」 (page 222)ダイアログ内で指定した名前を使用してカメラを接続します。Digikamはウィンドウを開き、サムネイルのダウンロードを開始し、図15.2.「カメラからの写真ダウンロード」 (page 223)のようにサムネイルを表示します。1つのイメージを右クリックしてポップアップメニュー開きます。そこには［表示する］、［プロパティ］および［*EXIF Information(EXIF情報)*］の表示、［ダウンロード］または［*削除*］のオプションがイメージに対して用意

されています。［*Advanced(詳細)* >>］をクリックし、名前の変更オプションを選択すると、カメラが提供する情報(EXIF)を取り扱えます。

図 15.2　カメラからの写真ダウンロード



名前変更オプションは、ご使用のカメラが有意なファイル名を使用しない場合に便利です。Digikamに自動的に写真名を変更させることができます。固有のプレフィックス、およびオプションとして、日付、時刻、または連番を指定してください。残りの部分はDigikamによって行われます。

左マウスボタンをクリックするか、Ctrlを押しながら個別の写真をクリックすることにより、すべての写真を選択し、ダウンロードの対象にします。選択された写真は、反転色で表示されます。［ダウンロード］をクリックします。リストからダウンロード先を選択するか、［*New Album(新しいアルバム)*］を使用して新しいアルバムを作成し、ダウンロード先に選択します。この方法は自動的に、現在の日付をファイル名として提示します。［*Ok*］をクリックして確定し、ダウンロードプロセスを開始します。

15.4.3　情報の入手

写真に関する情報を入手することは難しいことではありません。サムネイルにマウスカーソルを合わせると、ツールのヒントとして小さな要約が表示されます。より詳しい情報を得るには、写真を右クリックし、メニューから［プロパティ］を選択します。［*一般*］、［*EXIF*］、［*Histogram(ヒストグラム)*］という3つのタブがあるダイアログボックスが開きます。

［*一般*］は、名前、タイプ、オーナ、および他の基本的な情報を表示します。より興味深いのは、［*EXIF*］タブです。カメラは各写真ごとにメタデータを保存します。Digikamはメタデータのプロパティを読み込み、リストに表示します。露光時間、ピクセルの大きさなどについても表示します。選択したリストエントリに関する情報をさらに得るには、Shift + F1を押してください。これにより短いツールのヒントが表示されます。最後のタブ、［*Histogram(ヒストグラム)*］は、統計情報を表示します。

15.4.4 アルバムの管理

Digikamは、デフォルトで、すべての写真を集める［*My Albums(マイアルバム)*］を挿入します。後で、それらをサブフォルダに保存できます。アルバムは、ディレクトリレイアウトごと、アルバムプロパティに設定されたコレクション名ごと、アルバムが最初に作成された日付(この日付は各アルバムのプロパティ内でも変更できます)ごとに保存できます。

新しいアルバムを作成するには、次に示すいくつかの方法があります。

- カメラから新しい写真をアップロードする
- ツールバーにある［*New Album(新しいアルバム)*］ボタンをクリックして、新しいアルバムを作成する
- ハードディスクから写真が保存されている既存のフォルダをインポートする(*[アルバム] → [インポート] → [Import Folders(フォルダインポート)]*の順に選択)
- ［*My Albums(マイアルバム)*］を右クリックし、［*New Album(新しいアルバム)*］を選択する

作成を選択して、適切な方法でアルバムを作成すると、ダイアログボックスが表示されます。アルバムにタイトルを付けます。オプションで、コレクションの選択、コメントの挿入、アルバムの日付の選択ができます。コレクションは一般的なラベルごとにアルバムを構成する1つの方法です。このラベルは、*[表示する] → [アルバム] → [By Collection(コレクションごと)]*の順に選択した場合に使用されます。コメントはメインウィンドウの最上部のバナーに表示されます。アルバムの日付は、*[表示する] → [アルバム] → [By Date(日付ごと)]*の順に選択した場合に使用されます。

Digikamは、アルバム内の最初の写真を［*My Albums(マイアルバム)*］リストのプレビューアイコンとして使用します。異なる写真を選択するには、任意の写真を右クリックし、コンテキストメニューから［*Set as Album Thumbnail(アルバムサムネイルとして設定)*］を選択します。

15.4.5　タグの管理

異なるアルバムの多くの異なる写真を管理することは、手間のかかる場合があります。個々の写真を整理するために、Digikamは［*My Tag(マイタグ)*］システムを提供します。

たとえば、さまざまな場面で友人のJohnの写真を撮り、それらすべての写真を1つの独立したアルバムに集めるとします。これによりそれらすべての写真を容易に見つけることができます。最初に、*[My Tag(マイタグ)]* → *[People(人々)]*の順にクリックし、新しいタグを作成します。コンテキストメニューから、［*New Tag(新しいタグ)*］を選択します。表示されるダイアログボックス内で、タイトルとして［*John*］と入力し、オプションでアイコンを設定します。［*Ok*］をクリックして、設定を確定してください。

タグを作成した後に、必要な写真にそのタグを割り当てます。各アルバムを選択し、それぞれの写真を選択します。右クリックし、表示されるメニューから、*[Assign Tag(タグの割り当て)]* → *[People(人々)]* → *[John]*の順に選択します。［*My Tags(マイタグ)*］の下にあるタグ名に写真をドラッグし、ドロップする方法もあります。必要に応じて、他のアルバムでもこの手順を繰り返します。*[My Tags(マイタグ)]* → *[People(人々)]* → *[John]*の順にクリックしすべての写真を表示します。各写真に1つ以上のタグを割り当てることができます。

タグとコメントを編集するのは面倒な場合があります。この作業を簡単にするには、写真を右クリックし、［*Edit Comments & Tags(コメントとタグの編集)*］を選択します。これにより、プレビュー、コメントフィールド、タグリストがあるダイアログボックスが開きます。これにより、必要なタグを挿入し、コメントを追加することができます。［*Forward(前進)*］および［*Back(後退)*］を使用して、アルバム内を移動できます。［*適用する*］をクリックして変更を保存し、［*Ok*］をクリックして終了します。

15.4.6 画像コレクションのエクスポート

Digikamには、個人の画像コレクションのアーカイブと公開に役立つ、いくつかのエクスポートオプションがあります。CDやDVDへのアーカイブ(k3bを使う)、HTMLへのエクスポート、リモートギャラリへのエクスポートが行えます。

画像コレクションをCDまたはDVDに保存するには、以下の手順に従います。

1. *[File] → [Export] → [Archive to CD/DVD (CD/DVDへのアーカイブ)]*を選択します。

2. ［*Create CD/DVD Archive*］ダイアログのいくつかのサブメニューで、必要な調整を行います。それから、［*OK*］をクリックして、書き込みプロセスを開始します。

   a. ［*Selection*］:アルバムおよびタグを選択して、コレクションのうちのどの部分をアーカイブするかを決めます。

   b. ［*HTML Interface*］:画像コレクションをHTMLインタフェ-スを介してアクセスできるようにするか、そしてCD/DVDアーカイブにオートラン機能を追加するかどうかを決めます。コレクションのタイトル、イメージ、フォント、および背景のプロパティを設定してください。

   c. ［*Media Volume Descriptor*］:必要に応じて、ボリュームの記述についての設定を変更します。

   d. ［*Media Burning*］:必要に応じて、書き込みオプションを調整します。

画像コレクションのHTMLエクスポートを作成するには、以下の手順に従います。

1. *[File] → [Export] → [HTML Export]*を選択します。

2. ［*Create Image Galleries*］のいくつかのサブメニューで、必要な調整を行います。完了したら、［*OK*］をクリックして、ギャラリの作成を開始します。

a ［*Selection*］:アルバムおよびタグを選択して、コレクションのうちのどの部分をアーカイブするかを決めます。

b ［*Look*］:HTMLギャラリのタイトルと外観を設定します。

c ［*Album*］:ディスク上のギャラリの場所と、イメージのサイズ、圧縮、フォーマット、および作成されるギャラリ内に表示されるメタデータの量を決めます。

d ［*Thumbnails*］:ターゲットイメージと同様に、ギャラリの操作で使用するサムネイルのサイズ、圧縮、ファイルタイプを指定します。

コレクションをインターネット上の外部イメージギャラリにエクスポートするには、以下の手順に従います。

1 ギャラリを置く外部Webサイトのアカウントを取得します。

2 *[File] → [Export] → [Export to Remote Gallery]*を選択して、必要とされた場合は、外部サイトのURL、ユーザー名、パスワードを入力します。

Digikamは、指定されたサイトへの接続を確立して、［*Gallery Export*］というウィンドウを表示します。

3 ギャラリ内の新しいアルバムの場所を決めます。

4 ［*New Album*］をクリックして、Digikamから求められたら情報を入力します。

5 ［*Add Photos*］で、新しいアルバムにイメージをアップロードします。

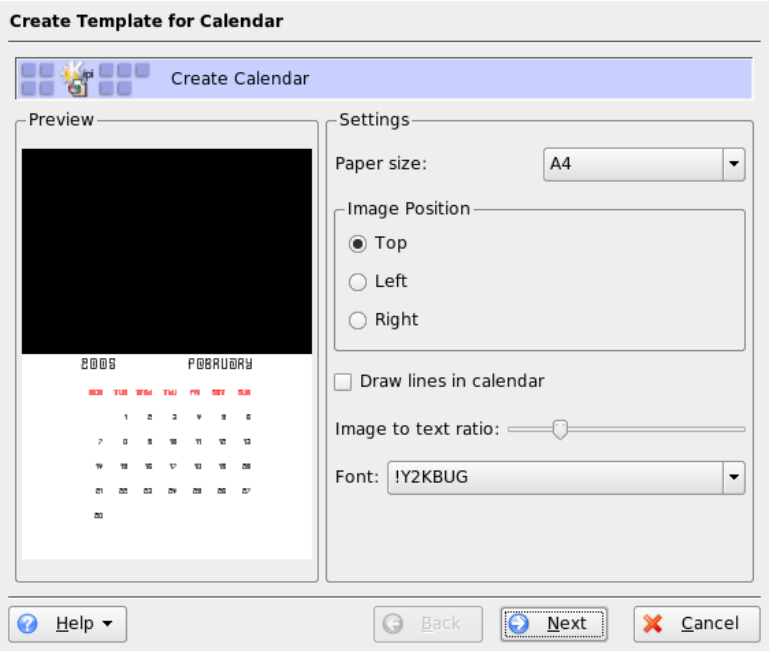
15.4.7 便利なツール

Digikamには、一部のタスクを簡単にする、いくつかのツールがあります。それらのツールは、［ツール］メニュー内に用意されています。以下に使用できるツールを少し示します。

カレンダの作成

誰かを喜ばせたい場合、カスタムカレンダは良い贈り物になることでしょう。*[ツール] → [Create Calendar(カレンダの作成)]*の順に移動すると、図 15.3.「カレンダのテンプレートの作成」 (page 228)にあるようなウィザードダイアログが開きます。

図 15.3　カレンダのテンプレートの作成



設定(用紙サイズ、画面のレイアウト、フォントなど)をカスタマイズし、［次へ］をクリックして確定します。これで、年を入力し、使用するイメージを選択できます。［次へ］を再度クリックした後に、概要を確認します。最後に［次へ］をクリックすると、［KDEプリンタ］ダイアログが開きます。ここで、プレビューを表示するか、PDFとして保存するか、または直接印刷するかを指定します。

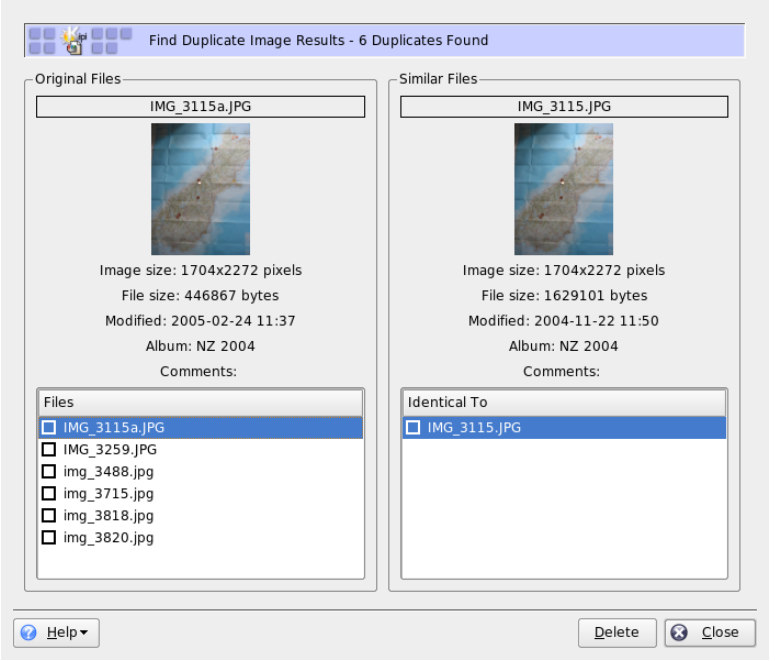
重複する写真の検出

同じシーンを繰り返し撮ってしまい、一番良い写真だけを保持したい場合があるかもしれません。この場合には、［*Find Duplicate(重複の検出)*］プラグインを使用することが最善です。

[Tools] → *[Find Duplicate Images]*を選択します。処理するアルバムまたはタグを選択します。［*Method & Cache(方法とキャッシュ)*］で、より正確またはより高速な検索方法のどちらかを選択します。［*Ok*］をクリックして確定した後に、Digikamは調査を開始します。

重複する写真を検出した場合、図 15.4.「検出結果」 (page 229)のようなウィンドウ内に結果を表示します。目的とするチェックボックスを有効にすることにより削除する写真を決定し、次に［*削除*］をクリックします。［*閉じる*］を使用してウィンドウを終了します。

図 15.4 *検出結果*



バッチプロセス

Digikamは、多くのファイルで特定の処理を実行するバッチプロセスも提供します。これにより、名前変更、変換、サイズ変更などさまざまな事柄が処理できます。このバッチプロセスは、*[ツール] → [Batch Processes(バッチプロセス)]*に用意されています。

15.4.8 Digikamによる基本的なイメージの表示および編集

Digikamには、簡単な画像表示および編集プログラムが含まれています。これは、イメージのサムネイルをダブルクリックすると、自動的に起動します。

このツールを使えば、カメラからダウンロードしたばかりのイメージに対し、基本的な画像編集を行うことができます。イメージの切り抜き、回転、反転、基本的な色調整、様々なカラーフィルタ(カラーイメージを白黒としてエクスポートする、など)、人物写真の赤目除去を行えます。

最も重要なメニューは以下のとおりです。

画像
: 特定のイメージにコメントを入力し、タグ(カテゴリ)をこのイメージに割り当てるには、［*Edit Comments & Tags*］を使います。［*Properties*］を選択すると、このイメージの全般的な情報、EXIF情報、ヒストグラムを表示する3つのタブからなるウィンドウが表示されます。

Fix
: このメニューには、デジタル写真で最も必要とされる編集機能のいくつかが含まれています。［*Colors*］は、すべての基本的な色設定を修正できるサブメニューを表示します。また、写真全体または選択したイメージの一部をぼかしたりシャープにしたりすることもできます。人物写真の赤目を除去するには、左マウスポインタをクリックしたまま、範囲を少しずつ拡大して、顔の目あたりを選択してから、［*Red Eye Reduction*］を選択し、目の部分全体を選択したか、それとも目だけを選択したかに応じて、除去の程度を選択します。

Transform
［*Transform*］メニューでは切り抜き、回転、反転、サイズ変更が行えます。また、［*Aspect Ratio Crop*］オプションでは、固定された縦横比の切り抜きを作成できます。

フィルタ
カラー写真を白黒に変換する場合、または写真をアンティーク写真のようにしたい場合には、［*Filters*］メニューの様々なエクスポートオプションから選択してください。

このツールのさらに詳細な説明は、*digiKam Image Editor*のDigikamのオンラインヘルプにあります。これは、Digikamのメニューバーの［*Help*］ボタンから開くことができます。

ティップ: 高度な画像処理

プロフェッショナルな画像編集は、GIMPで行えます。GIMPの詳細については、章 17. *GIMPによるグラフィックスの操作* (page 249)を参照してください。

15.5 f-spotの使用

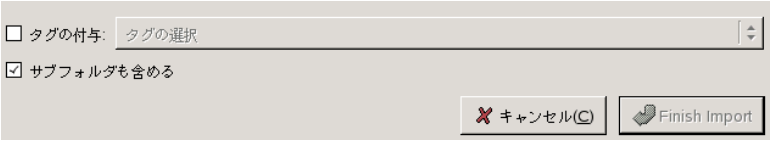
f-spotは、GNOMEデスクトップ用にカスタマイズされた、デジタル画像のコレクションの管理ツールです。これを使えば、イメージに異なるタグを割り当てて分類できます。また、様々な画像編集オプションがあります。

f-spotの最初の起動時には、イメージをどこからf-spotのコレクションにインポートするかを指定してください。ハードディスクにすでにイメージのコレクションがある場合には、そのディレクトリへのパスを入力します。オプションとしてサブフォルダを含めることができます。f-spotはこれらのイメージをデータベースにインポートします。

ティップ: インポート時にイメージにタグを付ける

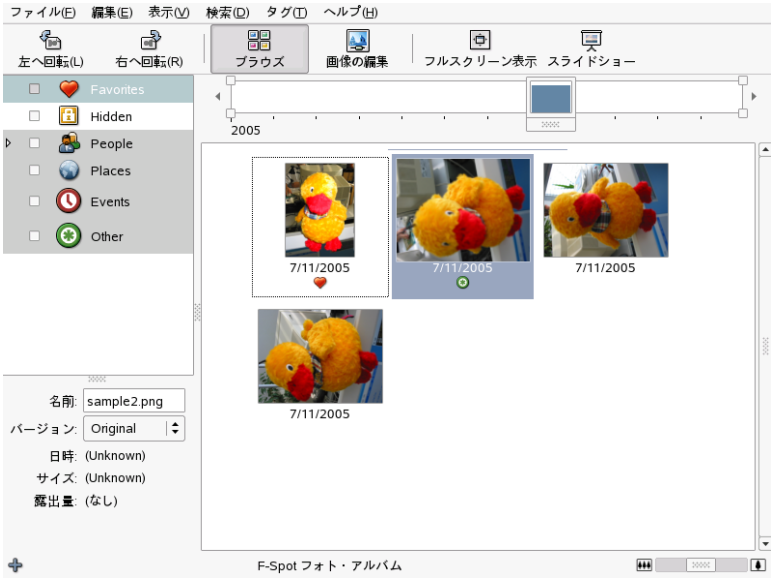
インポートするすべてのイメージが同じカテゴリに属している場合には、インポート時に適切なタグを付けることができます。［*Attach Tag*］を選択し、ドロップダウンメニューから適切なタグを選択してください。

図 15.5　f-spotにイメージをインポートする



f-spotのメインウィンドウは、3つの主要なエリアに分かれています。選択したイメージのカテゴリ、タグ、詳細情報が左側のサイドバーに、そして選択したタグまたはカテゴリのすべてのイメージのサムネイル、または何も選択していない場合にはコレクション全体が、ウィンドウの右側の部分に表示されます。

図 15.6　f-spotのメインウィンドウ



ウィンドウの最上部にあるメニューバーを使えば、主なメニューにアクセスできます。その下のツールバーでは、アイコンによって示されている、以下のような機能を利用できます。

Rotate (左または右)
　このショートカットでは、イメージの向きを変更できます。

Browse
［*Browse*］モードでは、コレクション全体、または特定のタグのついたサブセットの表示と検索を行えます。また、タイムラインを使用して、作成日に基づいてイメージを検索することもできます。

Edit Image
このモードでは、1つのイメージを選択して、基本的な画像処理を行えます。詳細については、項15.5.6.「f-spotでの基本的な画像処理」 (page 238)を参照してください。

Fullscreen
全画面表示モードに切り替えます。

Slideshow
スライドショーを開始します。

15.5.1　カメラからの写真ダウンロード

ご使用のコンピュータのUSBポートに接続されたデジタルカメラから新しいイメージをインポートするには、*[File]* → *[Import from Camera]*を使います。カメラのタイプは自動的に検出されます。

図 15.7　カメラからのインポート

f-spotはプレビューウィンドウを開きます。ここには、カメラからダウンロードできるすべてのイメージが表示されます。ファイルは、［*Copy Files to*］で指定したターゲットディレクトリにコピーされます。［*Import files after copy*］を選択すると、カメラからコピーされたすべてのイメージは、f-spotのデータベースに自動的にインポートされます。［*Select Tags*］で適切なタグを選択していれば、インポート時にタグを付けることができます。カメラからのすべてのイメージをデータベースにインポートしたくない場合には、プレビューウィンドウで不必要なものを選択解除してください。

15.5.2　情報の入手

イメージを選択すると、ウィンドウの左下の部分に、そのイメージについての基本的な統計情報が表示されます。これにはファイル名、バージョン(コ

ピーかそれともオリジナルのイメージか)、作成日、サイズ、およびそのイメージを作成する際に用いられた露光値が含まれます。イメージファイルに関連付けられたEXIFデータを表示するには、*[View]* → *[EXIF Data]*を選択します。

15.5.3 タグの管理

画像を分類して、コレクション内で管理できるサブセットを作成するには、タグを使います。たとえば、家族や友人の写真をさらに分類したい場合には、以下のようにします。

1. f-spotで［*Browse*］モードを選択します。
2. f-spotのウィンドウの左側のフレームで、［*People*］カテゴリを選択し、それを右クリックして、［*Create New Tag*］を選択します。［*People*］カテゴリの下に、サブカテゴリとして新しいタグが表示されます。
   a. `Friends`という新しいタグを作成します。
   b. `Family`という新しいタグを作成します。
3. タグをイメージまたは選択したイメージのグループに添付します。イメージを右クリックし、［*Attach Tag*］を選択し、そのイメージに適したタグを選択します。イメージのグループにタグを添付するには、最初のイメージをクリックしてShiftキーを押し、Shiftキーを押したまま残りのイメージをクリックします。右クリックしてタグのメニューを表示し、適切なカテゴリを選択します。

イメージを分類したら、コレクションをタグによってブラウズすることができます。*[People]* → *[Family]*だけをオンにして、`Family`というタグがついているイメージだけが表示されるようにしてください。*[Find]* → *[Find by Tag]*を選択すれば、コレクションをタグで検索することもできます。検索の結果は、サムネイルの概要ウィンドウに表示されます。

1つのイメージまたはイメージのグループからタグを削除する場合には、添付したときと同様の方法で行えます。タグ編集機能は、上部のメニューバーの［*Tags*］メニューからアクセスすることもできます。

15.5.4 検索

項15.5.3.「タグの管理」 (page 235)で説明したように、特定のイメージを検索するためにタグを使うことができます。別の方法として、f-spotのユニークな機能である、ツールバーの下の［*Timeline(タイムライン)*］を使うこともできます。このタイムラインに沿って小さなフレームをドラッグすれば、サムネイルの概要に、選択した期間内に撮影されたイメージだけが表示されるようにすることができます。f-spotはデフォルトのタイムフレームを適切に選択しますが、スライダをタイムラインの端に向かって左右に移動すれば、いつでも時間の範囲を変更できます。

15.5.5 画像コレクションのエクスポート

f-spotの*[File]* → *[Export]*には、コレクションをエクスポートする複数の方法が用意されています。おそらく最もよく用いられるのは、［*Export to Web Gallery (Web*ギャラリへのエクスポート*)*］と［*Export to CD (CD*へのエクスポート*)*］でしょう。

選択したイメージをWebギャラリにエクスポートするには、以下の手順に従います。

1. エクスポートするイメージを選択します。

2. *[File]* → *[Export]* → *[Export to Web Gallery]*を選択して、イメージをエクスポートするギャラリを選択するか、新しいものを追加します。.f-spotは、Webギャラリとして選択されたWebの場所への接続を確立します。画像をエクスポートするアルバムを選択し、画像のサイズ変更を自動的に行うかどうか、そしてタイトルとコメントのエクスポートを行うかどうかを指定します。

図 15.8　イメージをWebギャラリにエクスポートする

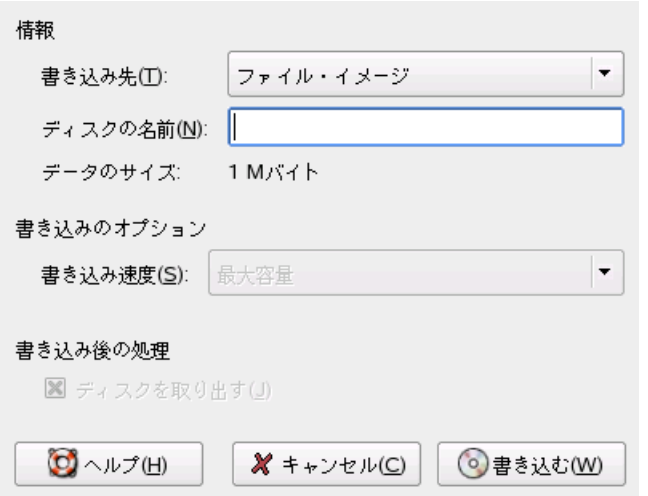
選択したイメージをCDにエクスポートするには、以下の手順に従います。

1. エクスポートするイメージを選択します。

2. *[File]* → *[Export]* → *[Export to CD]*をクリックして、［*OK*］をクリックします。

   f-spotはファイルをコピーし、CD書き込みダイアログを表示します。イメージディスクに名前を割り当て、書き込み速度を指定します。［*Write*］をクリックして、CDの書き込みプロセスを開始します。

図 15.9　イメージをCDにエクスポートする



15.5.6　f-spotでの基本的な画像処理

f-spotには、いくつかの非常に基本的な画像編集機能があります。f-spotの編集モードに入るには、ツールバーの［*Edit Image*］アイコンをクリックするか、編集するイメージをダブルクリックします。イメージを切り替えるには、右下にある矢印キーを使います。以下のような編集機能を選択できます。

シャープ
: この機能には、*[Edit]* → *[Sharpen]*からアクセスします。必要に合わせて［*Amount (量)*］、［*Radius (半径)*］、および［*Threshold (しきい値)*］の値を調整し、［*OK*］をクリックします。

イメージの切り取り
: イメージを選択して切り取るには、左下のドロップダウンメニューから切り取る縦横比を選択するか、［*No Constraint (制限なし)*］オプションを選択し、切り取る範囲を選択して、縦横比メニューの隣のはさみのアイコンをクリックします。

赤目除去
: 人物写真の、顔の赤い眼の部分を選択し、赤い目のアイコンをクリックします。

色の調整
: 写真の作成の際に用いられたヒストグラムを表示し、必要に応じて、露光値や色温度を調節します。

ティップ: 高度な画像処理

プロフェッショナルな画像編集は、GIMPで行えます。GIMPの詳細については、章 17. *GIMPによるグラフィックスの操作* (page 249)を参照してください。

15.6 関連資料

Linuxと共にデジタルカメラを使用する方法については、次のWebサイトを参照してください。

- `http://digikam.sourceforge.net/` Digikamに関する情報
- `http://www.gphoto.org` gPhoto2に関する情報
- `http://www.gphoto.org/proj/libgphoto2/support.php` サポートしているカメラ全般のリスト
- `http://www.thekompany.com/projects/gphoto/` gPhoto2用のKDEフロントエンドであるKameraに関する情報

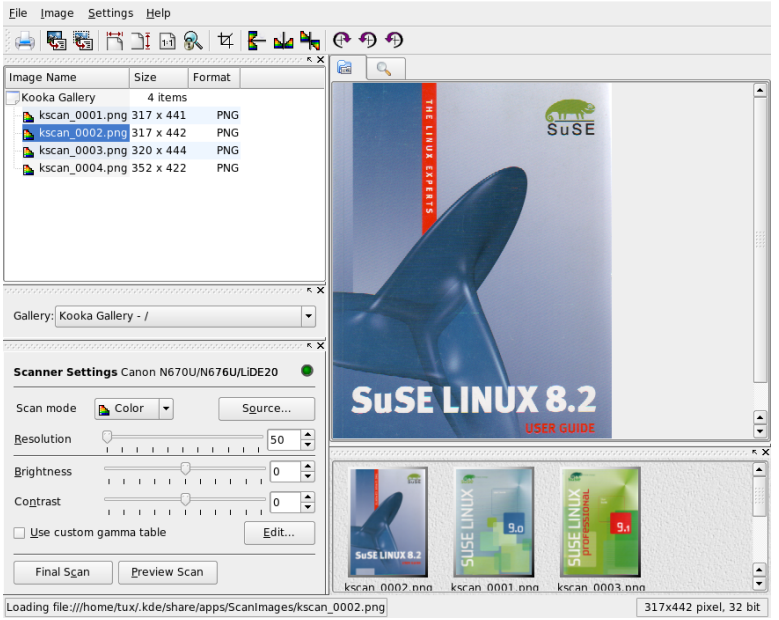
16 Kooka—スキャンアプリケーション

Kookaは、スキャンを行うKDEアプリケーションです。この章では、このアプリケーションのユーザインタフェースと機能について説明します。Kookaには、写真や雑誌などの印刷物からイメージファイルを作成する機能だけでなく、文字読み取り機能もあります。つまり、紙に書かれたテキストを編集可能なテキストファイルに変換できます。

Kookaは、メインメニューから、またはコマンド「`kooka`」を入力して起動します。Kookaを起動すると、3つのフレームから成るウィンドウが表示されます。ウィンドウの左上にメニューバーがあり、その下にはツールバーがあります。ウィンドウはすべて、マウスを使用して自由に調整や配置をし直すことができます。またKookaウィンドウからフレームを1つだけ取り出して、デスクトップ上の任意の場所に配置することも可能です。フレームを移動するには、フレームの上の細い二重線をクリックしてドラッグします。メインウィンドウを除いて、すべてのフレームは他のフレーム内に移動でき、上下左右の線に合わせて、または中央に配置できます。中央に配置された同じサイズのウィンドウは重ねられ、タブをクリックして前面に移動することができます。

［*画像*ビューア］フレームと［*プレビュー*］フレームは、デフォルトで1つのウィンドウを共有します。これらのフレームは、タブによって切り替えられます。左側のフレームはギャラリです。これはスキャンするイメージにアクセスするための小さなファイルブラウザです。右下のフレームはOCR(光学式文字読み取り装置)とサムネイルによって共有され、マウスを一度クリックするだけで［画像ビューア］にロードできます。図 16.1. 「Kookaメインウィンドウ」 (page 242)を参照してください。

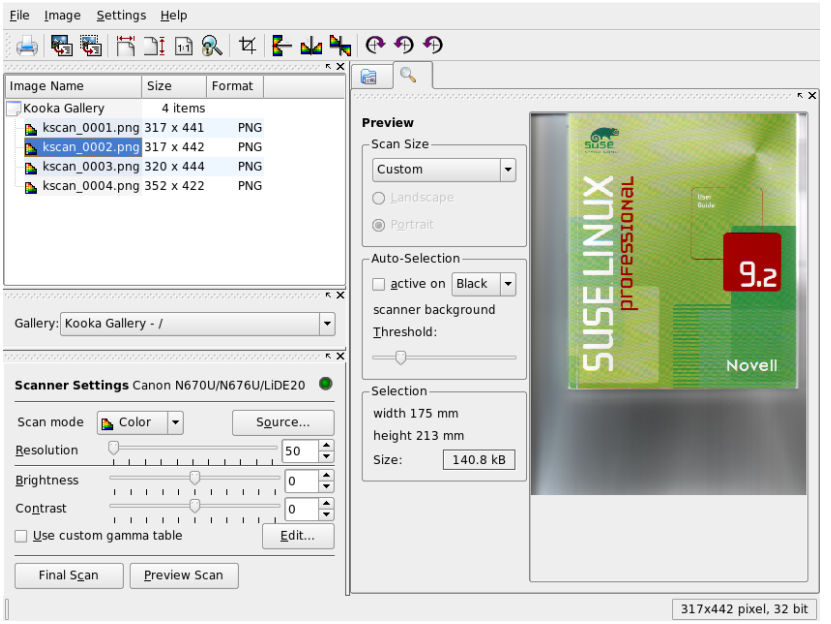
図 16.1　Kookaメインウィンドウ



16.1　プレビュー

プレビューは、スキャンするオブジェクトがスキャン領域全体よりも小さい場合、常に作成されます。これには、プレビューフレームの左にあるパラメータを設定します。［カスタム］または標準形式からスキャンサイズを選択します。図 16.2.「Kookaプレビューウィンドウ」 (page 243)を参照してください。［カスタム］設定を使用すると、マウスで対象の領域を選択できるので、柔軟性が最も高くなります。設定を完了したら、［スキャンパラメータ］の［プレビュースキャン］をクリックして、スキャンするイメージのプレビューを要求します。

図 16.2　Kookaプレビューウィンドウ

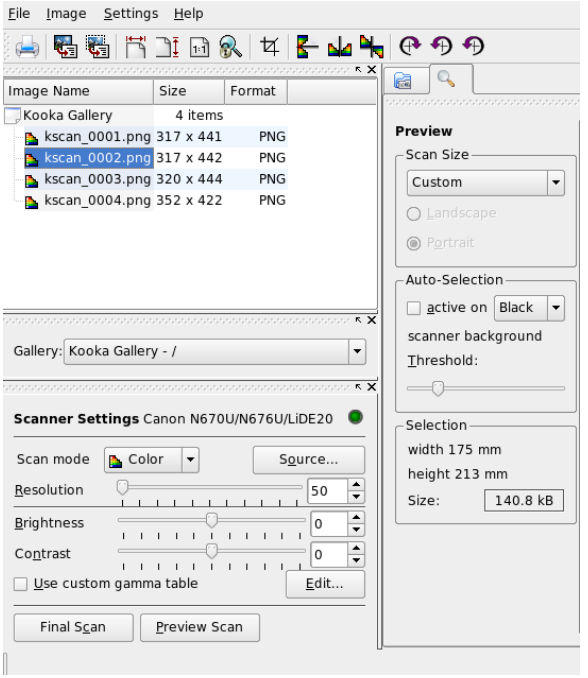


16.2　最終スキャン

スキャンサイズに［カスタム］を選択した場合は、マウスを使用してスキャンする四角形の領域を選択します。選択した領域が点線で囲まれます。

スキャンがカラーか白黒かを選択し、スライダで解像度を設定します。図16.3.「Kookaのスキャンパラメータ」 (page 244)を参照してください。解像度が高くなると、スキャンしたイメージの品質がよくなります。しかし、高解像度では、それに対応してファイルが大きくなり、スキャン処理に非常に時間がかかることがあります。［*Use custom gamma table (ユーザ定義のガンマテーブルを使用する)*］を有効にし［*編集*］をクリックして、明度、コントラスト、およびガンマの設定を変更します。

図 16.3　Kookaのスキャンパラメータ



すべての設定が完了したら、［*最終スキャン*］をクリックしてイメージをスキャンします。スキャンされたイメージは、［画像ビューア］にサムネイルとして表示されます。プロンプトが表示されたら、イメージの保存形式を選択します。それ以降、すべてのイメージを同じ形式で保存するには、対応するボックスをオンにします。［*OK*］クリックして、設定を確認してください。

16.3　メニュー

ツールバーの機能の中には、［*ファイル*］メニューと［*画像*］メニューから選択できる機能もあります。Kookaの環境設定を変更するには、［*設定*］メニューを使用します。

ファイル

このメニューは、KPrinter印刷アシスタントの起動、イメージ用の新規フォルダの作成、およびファイルの保存、削除、終了に使用します。スキャンしたテキスト文書のOCRの結果は、このメニューで保存できます。また、このメニューはKookaの終了にも使用します。

画像

［*画像*］メニューを使用すると、イメージの後処理または光学式文字読み取りを行うグラフィックスアプリケーションを起動できます。OCR操作で読み取られたテキストは、専用のフレームに表示されます。またイメージのサイズ変更、回転、反転のためのさまざまなツールが用意されています。これらの機能は、ツールバーからもアクセスできます。［*選択範囲から作成*］を使用すると、マウスでマークしたイメージの領域が保存できます。

設定

［*設定*］メニューを使用すると、Kookaのルックアンドフィールを設定できます。ツールバーとステータスバーはオン/オフを切り替えることができ、またメニューエントリのキーボードショートカットが定義できます。［*ツールバーを設定*］には、ツールバーで利用可能なすべての機能のリストがあります。［*Kookaを設定*］を使用すると、設定ダイアログが開き、Kookaのルックアンドフィールを変更できます。しかし、通常はデフォルト設定で十分です。［*ツールビュー*］では、サムネイルビューア、プレビュー、ギャラリ、スキャンパラメータ、およびOCR結果ウィンドウの有効と無効を切り替えます。

ヘルプ

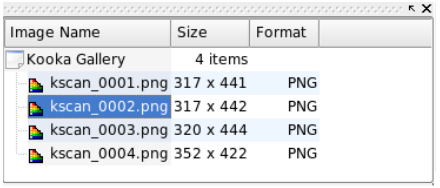
［*ヘルプ*］メニューを選択すると、Kookaのオンラインヘルプマニュアルを表示できます。また問題点や要望を集めたフィードバックチャネルにもアクセスできます。さらに、KookaとKDEのバージョン、作成者、ライセンスについての情報もこのメニューから表示できます。

16.4　ギャラリ

ギャラリウィンドウは、Kookaがすべてのイメージファイルを格納するデフォルトフォルダを表示します。図16.4.「Kookaギャラリ」 (page 246)に例を示します。イメージを個人のホームディレクトリに保存するには、サムネイルをクリックして選択し、［*ファイル*］、→［*画像を保存*］を順に選択します。

次に、個人のホームディレクトリに移動し、ファイルにわかりやすい名前を指定します。

図 16.4　Kookaギャラリ

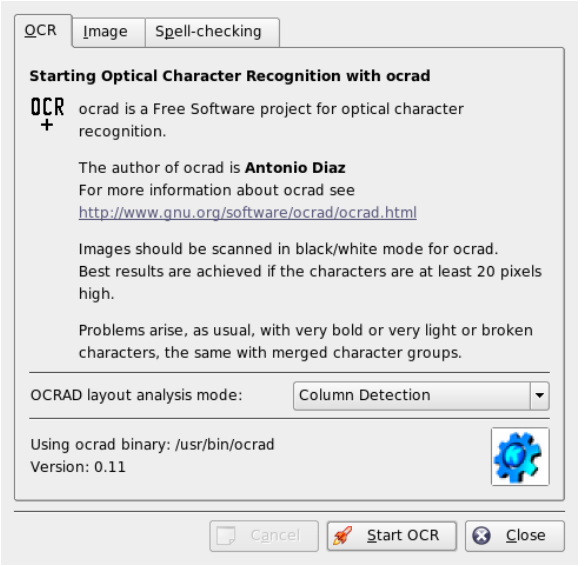


ギャラリにイメージを追加するには、Konquerorからイメージをドラッグアンドドロップします。Konquerorを起動し、ギャラリに追加するイメージがあるディレクトリに移動し、イメージをマウスでKookaギャラリのフォルダにドラッグします。

16.5　光学式文字読み取り

文字読み取りモジュールがインストールされている場合、文書をラインアートモードでスキャンし、指定した形式で保存してから、［*画像*］メニューからテキスト読み取りの処理を行うことができます。文書全体を処理することも、あらかじめ選択した領域のみを処理することも可能です。設定ダイアログには、元のテキストが印刷用活字、手書き、標準の活字のいずれであるかが表示されます。また、モジュールが文書を正しく処理できるよう、言語も設定されます。図 16.5.「KookaによるOCR」 (page 247)を参照してください。

図 16.5　KookaによるOCR



［*OCR画像結果テキスト*］ウィンドウに切り替えて、テキストを確認します(テキストは、校正が必要なことがあります)。これには、［*ファイル*］、→［*OCR画像結果テキストを保存*］を選択してテキストを保存します。これにより、テキストをOpenOffice.orgまたはKWriteで処理できるようになります。

17 GIMPによるグラフィックスの操作

GIMP (*The GNU Image Manipulation Program*)は、ピクセルグラフィックスの作成と編集を行うためのプログラムです。ほとんどの面で、その機能はAdobe Photoshopや他の市販プログラムに匹敵するレベルにあります。写真のサイズ変更とレタッチ、Webページ用のグラフィックスの作成、カスタムCDのカバーの作成、その他さまざまなグラフィックスプロジェクトにGIMPを活用することができます。また、アマチュアとプロフェッショナル両方のニーズを満たすことができます。

Linuxの他の多くのプログラムと同様、GIMPは、作業時間と作成したコードをプロジェクトに提供している、世界中にいるボランティア開発者の共同作業により開発されています。 このプログラムは今も継続的に開発が進められているため、使用中のSUSE Linuxに付属しているバージョンが、ここで説明されているバージョンとはわずかに異なっている可能性もあります。個別のウィンドウや、ウィンドウ内のセクションのレイアウトは、特に違いが生じやすい箇所です。

GIMPは、非常に複雑なプログラムです。この章で説明するのは、限られた範囲の機能、ツール、およびメニュー項目です。このプログラムの詳細情報については、項17.6. 「関連資料」 (page 257)を参照してください。

17.1 グラフィックファイルの形式

グラフィックファイルには、大きく分けてピクセルとベクタという2つの形式があります。GIMPは、ピクセルグラフィックスだけを対象として機能します。写真や、スキャンした画像の場合、これが普通の形式です。ピクセルグ

ラフィックスは、色の付いた小さな点で構成されていて、それらの集合体が画像全体を形成しています。この理由で、ファイルはすぐに、非常に大きくなる傾向があります。また、画質を低下させることなくピクセル画像のサイズを大きくすることはできません。

ピクセルグラフィックスとは異なり、ベクタグラフィックスは個々の点すべてに関する情報を格納しているわけではありません。代わりに、画像の点、線、または面がどのようにグループ化されているか、という情報を格納しています。ベクタ画像は、非常に簡単に拡大縮小することもできます。たとえば、OpenOffice.orgの描画(ドロー系)アプリケーションでは、この形式が採用されています。

17.2 GIMPの起動

GIMPはメインメニューから起動します。代わりに、コマンドラインで、「gimp」と入力することもできます。

17.2.1 初期設定

GIMPの最初の起動時には、準備となる設定を行うための設定ウィザードが表示されます。ほとんどの用途では、デフォルト設定をそのまま使用することができます。設定項目に精通していてセットアップを変更する場合以外は、各ダイアログで何も変更しないで［次へ］をクリックします。

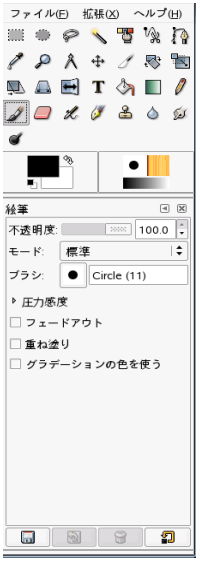
17.2.2 デフォルトのウィンドウ

デフォルトでは、3つのウィンドウが表示されます。画面内でこれらを整列させることや、必要がなくなった時点でツールボックス以外を閉じることもできます。ツールボックスを閉じると、このアプリケーションも閉じます。デフォルトの設定では、GIMPは終了時にウィンドウの位置を保存します。終了時に表示されていたダイアログは、次回にこのプログラムを起動すると、再び表示されます。

ツールボックス

図 17.1.「メインウィンドウ」 (page 251)に示すGIMPのメインウィンドウには、このアプリケーションのメインコントロールがあります。このウィンドウを閉じると、このアプリケーションは終了します。最上部にあるメニューバーを使用すると、ファイル機能、拡張機能、およびヘルプを使用できます。その下には、さまざまなツールに対応したアイコンがあります。これらのアイコンの上にマウスポインタを移動すると、そのアイコンに関する情報が表示されます。

図 17.1　メインウィンドウ



現在の前景色と背景色が、重なっている2つの長方形で表示されます。デフォルトの色は、前景色が黒、背景色が白です。長方形をクリックすると、その色を変更するダイアログが表示されます。2つの長方形の右上にある曲がった矢印記号をクリックすると、前景色と背景色が入れ替わります。左下にある黒と白の記号をクリックすると、色をデフォルトに戻すことができます。

前景色と背景色の右には、現在のブラシ、パターン、およびグラデーションが表示されます。表示されているいずれかをクリックすると、その選択ダイアログが表示されます。 ウィンドウの下の部分では、現在のツールに対し、さまざまな設定を行えるようになっています。

レイヤー、チャンネル、パス、アンドゥ

最初のセクションでは、ドロップダウンボックスを使用して、タブが参照する画像を選択します。［*自動*］をクリックして、アクティブな画像が自動的に選択されるかどうかを制御することができます。デフォルトでは、［*自動*］は有効になっています。

［*レイヤー*］は、現在の画像内にあるさまざまなレイヤーを表示します。また、レイヤーを操作することもできます。*チャンネル*]は、画像のカラーチャンネルを表示しますが、ここでそれらを操作することもできます。

パスは、画像の一部を選択するための高度な方法です。パスを使用して描画することもできます。［パス］は、画像に関連して使用できるパスを表示し、パス機能にアクセスする手段を提供します。［アンドゥ］は、現在の画像に対して加えられた変更からなる、限られた数の履歴を表示します。

このウィンドウの下端には、3つのタブがあります。それらを使用すると、現在のブラシ、グラデーション、およびパターンを選択できます。

17.3　GIMPでの作業開始

GIMPを初めて使用する場合、少々使いにくく感じるかもしれませんが、一度基本操作を覚えてしまえば、操作は簡単であることがわかります。不可欠な基本機能は、画像を作成し、開き、保存することです。

17.3.1　新しい画像の作成

新しい画像を作成するには、*［ファイル］*、→ *［新規］*の順に選択するか、Ctrl + Nを押します。新しい画像に関する設定を行うためのダイアログが表示されます。必要に応じて、［テンプレートから］を使用し、新しい画像のベースとなるテンプレートを選択することもできます。が用意されているので、そこから選択できます。カスタムテンプレートを作成するには、*［ファイル］*、→ *［ダイアログ］*、→ *［テンプレート］*の順に選択し、表示されたウィンドウにあるコントロールを使用します。

［*画像のサイズ*］セクションで、作成する画像のサイズをピクセルまたは他の単位で設定します。それ以外の単位を使用するには、使用可能な単位から

なるリストを使用して、希望の単位をクリックします。ピクセルと他の単位との比率は、［*解像度*］で設定されており、［*拡張オプション*］セクションを開くと設定値を確認できます。72ピクセル/インチという解像度は、画面表示に対応しています。Webページの画像として使用する場合は、これで十分です。画像を印刷する場合は、これより高い解像度を使用してください。ほとんどのプリンタでは、300ピクセル/インチの解像度を使用すると、許容可能な画質になります。

［*色空間*］で、画像をカラー(［*RGB*］)と［*グレースケール*］のどちらにするかを選択します。新しい画像を作成する場合は、[*塗りつぶしの種類*] も選択します。［*描画色*］と［*背景色*］は、ツールボックスで選択された色を使用します。［*白*］は、画像の背景色として白を使用します。［*透明*］は、クリアな画像を作成します。［*透明部分*］は、灰色のチェッカーパターン(格子模様)で表現されます。［コメント］には、新しい画像に関する説明を入力します。

設定値がニーズを満たした時点で、［*OK*］をクリックします。デフォルト設定に戻すには、［*リセット*］をクリックします。［キャンセル］をクリックすると、新規画像の作成を取り消します。

17.3.2 既存の画像を開く

既存の画像を開くには、［*ファイル*］、→［*開く*］の順に選択するか、Ctrl+O を押します。ダイアログが開いたら、希望のファイルを選択します。［*OK*］をクリックすると、選択した画像が表示されます。［キャンセル］をクリックすると、画像を開く作業を取り消します。

17.3.3 画像ウィンドウ

新しい画像、または開かれた画像は、別のウィンドウ内に表示されます。それらのウィンドウの最上部にあるメニューバーを使用して、すべての画像機能を利用することができます。メニューバーの代わりに、画像を右クリックするか、ルーラの左隅にある小さな矢印をクリックする方法でメニューを使用することもできます。

［ファイル］メニューには、［*保存*］や［*Print (印刷)*］など、標準的なファイルオプションがあります。［*閉じる*］は、現在の画像を閉じます。［*終了*］は、このアプリケーション全体を終了させます。

［*表示*］メニュー内の項目を使用して、画像と画像ウィンドウの表示方法を制御します。［*新規ビュー*］は、現在の画像を表示する2番目の表示ウィンドウを開きます。1つのビューに加えた変更は、その画像を表示している他のすべてのビューに反映されます。追加のビューは、あるビューで画像を拡大表示して操作しながら、他のビューで画像全体を表示する場合に役立ちます。現在のウィンドウの拡大レベルを調整するには、［ズーム］を使用します。［*ウィンドウに合わせる*］が選択されている場合、現在の画像表示サイズに合わせて、画像ウィンドウのサイズが適切に変更されます。

17.4 画像の保存

最も重要な画像機能の処理手順は、*［ファイル］*、→ *［保存］*です。保存の回数が少なすぎるより、多すぎる方が適切です。新しいファイル名で画像を保存するには、*［ファイル］*、→ *［別名で保存］*の順に選択します。何段階か異なる名前を使用して画像を保存すること、または他のディレクトリ内にバックアップを作成することは良い考えです。その結果、以前の状態に簡単に戻ることができます。

初めて保存する場合や、［*別名で保存*］を使用する場合、ファイルの名前と種類を指定するためのダイアログが表示されます。最上部にある［名前］フィールドに、ファイルの名前を入力します。［*Save in folder (フォルダに保存)*］の場合は、共通で使用するディレクトリの一覧から、ファイルを保存するディレクトリを選択します。異なるディレクトリを使用、またはディレクトリを新規作成する場合は、［*Browse for other folder(他のフォルダを参照)*］を開きます。［*Select File Type (ファイル形式の決定)*］は、［*拡張子で判別*］のままにしておくことをお勧めします。この設定の場合、GIMPはファイル名に追加された拡張子に基づいてファイルの形式を決定します。使用頻度の高いファイル形式は、次のとおりです。

XCF
: これは、GIMPのネイティブの形式です。画像だけでなく、すべてのレイヤー情報とパス情報を保存します。他の形式の画像を必要とする場合であっても、将来の変更を簡略化するために、XCF形式でコピーを保存しておくことは、通常は良い考えです。

PAT

これは、GIMPのパターンに関して使用される形式です。画像をこの形式で保存すると、その画像をGIMP内の塗りつぶしパターンとして使用できるようになります。

JPG

JPGまたはJPEGは、写真や、Webページ用で透過性のないグラフィックスを処理するための一般的な形式です。その圧縮方法はファイルサイズを縮小しますが、圧縮を行う際に一部の情報が失われます。圧縮レベルを調整する際に、プレビューオプションを使用するのは良い考えです。85〜75%のレベルを選択すると、多くの場合、許容可能な画像品質(画質)で、妥当な圧縮を達成することができます。同時に、XCFなどロスレス(情報損失なし)の形式で、バックアップを保存しておくこともお勧めします。画像を編集する場合は、完成した画像だけをJPGとして保存します。JPGをロードして保存する作業を繰り返すと、画像品質がすぐに低下する可能性があります。

GIF

GIFは透過性をサポートするグラフィックスとして、以前は非常に人気がありましたが、現在はライセンスの問題が原因となり、使用頻度が低下しています。GIFは、動画(アニメーション画像)を処理する場合にも使用されています。この形式では、インデックス画像の保存だけを実行できます。数色のみを使用すると、多くの場合、ファイルサイズは非常に小さくなることがあります。

PNG

PNGには、透過性のサポート、ロスレス(情報損失なし)圧縮のサポート、フリー(ライセンス料不要)入手と配布が可能、およびブラウザでのサポートが拡大中という特徴があるので、透過性を使用するWebグラフィックスとしてGIFを凌駕する勢いです。さらに、追加された利点として、PNGは部分的な透過性をサポートしています。これは、GIFがサポートしていない特徴です。この結果、色付きの領域から透過領域へのスムーズな遷移(アンチエイリアシング)が可能になります。

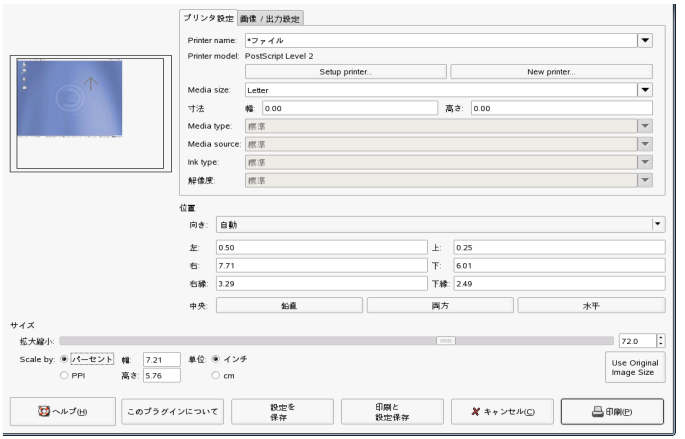
選択した形式で画像を保存するには、［*保存*］をクリックします。保存を中止するには、［キャンセル］をクリックします。画像が、選択した形式では保存できない機能を利用している場合、その状況を解決する選択肢を示すダイアログが表示されます。［エクスポート］が表示される場合、通常はそれを選択することによって、望ましい結果が得られます。次に、使用可能な形

式をオプションとして表示するウィンドウが表示されます。妥当なデフォルト値が用意されています。

17.5 画像の印刷

画像を印刷するには、画像メニューから［*ファイル*］、→［*印刷*］の順に選択します。使用中のプリンタをSUSE環境内で既に設定した場合、リスト内にそのプリンタが表示されるはずです。特定の状況では、［*プリンタの設定*］を使用して適切なドライバを選択する必要があることがあります。［*用紙サイズ*］を使用して適切な用紙サイズを選択し、［*用紙の種類*］を使用して種類を選択します。他の設定項目は、［*画像/出力設定*］タブ内で指定できます。

図 17.2 ［印刷］ダイアログ



このウィンドウの下側部分で、画像のサイズを調整します。［*Use Original Image Size(元の画像サイズを使用する)*］をクリックすると、これらの設定値を画像自体から取得できます。画像側で適切な印刷サイズと解像度を既に設定済みの場合は、これを使用することをお勧めします。ページ内での画像の位置を調整するには、［*位置*］内のフィールドを使用するか、［*プレビュー*］内で画像をドラッグします。

設定値の入力後、［*印刷*］をクリックします。将来の使用に備えてこれらの設定値を保存するには、代わりに［*印刷と設定保存*］を使用します。［キャンセル］は、印刷を取り消します。

17.6 関連資料

次に、GIMPユーザにとって役立つ可能性のあるいくつかのリソースを示します。残念なことに、多くのリソースのバージョンは旧版のままです。

- ［ヘルプ］を使用すると、統合されているヘルプシステムにアクセスできます。このマニュアルは、HTMLおよびPDF形式であり、http://docs.gimp.orgで入手できます。
- GIMP User Groupは、http://gug.sunsite.dkで、情報を掲載した、興味深いWebサイトを運営しています。
- http://www.gimp.orgは、GIMPのオフィシャルWebページです。
- Carey Bunks氏による『*Grokking the GIMP*』は、古いバージョンのGIMPに基づく優れた書籍です。このプログラムのいくつかの要素は変更されましたが、この書籍は、画像操作に関する優れた案内を掲載しています。この書籍のオンラインバージョンは、http://gimp-savvy.com/BOOK/で入手できます。
- http://gimp-print.sourceforge.netは、GIMPの印刷プラグインを掲載しているWebページです。このサイトで入手できるユーザマニュアルには、このプログラムの環境設定と使用方法に関する詳細情報が記載されています。

パート VI. モバイル性

18 Linuxでのモバイルコンピューティング

この章ではモバイルコンピューティングにLinuxを使用した様々な例について説明します。様々な分野での使用例を簡潔に紹介し、使用されているハードウェアの基本的な機能についても解説します。電源消費量を最小限に抑える実現性とともに、パフォーマンスを最大限に引き出す特別な要件とオプションに適したソフトウェアソリューションを提案します。この章の終わりでは、今回のテーマに関する最も重要な情報ソースについて説明します。

モバイルコンピューティングという言葉から連想されるのはラップトップ、PDA、携帯電話、そしてそれらとのデータ交換ではないでしょうか。この章ではラップトップやデスクトップシステムに接続可能な外付けハードディスク、フラッシュドライブ、デジタルカメラなどのモバイルハードウェアコンポーネントにまで範囲を広げて追っていきます。

18.1 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システムとは異なります。これは交換可能性、占有スペース、消費電力などの基準が関係するためです。モバイルハードウェアの製造元によりPCMCIA (Personal Computer Memory Card International Association)標準が開発されました。この標準にはメモリカード、ネットワークインタフェースカード、ISDNおよびモデムカード、そして外部ハードディスクなどが含まれます。このようなハードウェアのサポートをどのようにLinuxに実装するか、構成中に考慮すべきことは何か、PCMCIAを制御するために使用可能なソフトウェアは何か、起こりうる障害をどのようにトラブルシューティングするか、などの情報は章 19. *PCMCIA* (page 273)に記述されています。

18.1.1 電源消費量

ラップトップの製造時、消費電力を最適化したシステムコンポーネントを組み込むことで、電源網にアクセスする必要性を極力減らし、システムを快適に使用できるようにしています。それらによる電力消費の軽減は、少なくとも、オペレーティングシステムによるものと同じほど重要です。SUSE Linuxは、ラップトップの電力消費に影響を及ぼす様々な方式をサポートしています。それらの方式の、バッテリ電源での使用時間に対する影響はそれぞれ異なります。次のリストでは電源消費量節約への貢献度の高い順に各項目を示します。

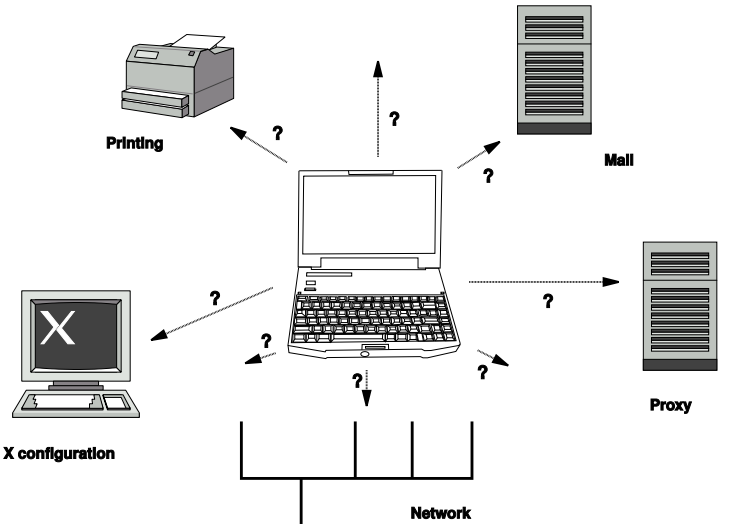
- CPUの速度を落とす
- 休止中にディスプレイの照明を切る
- ディスプレイの明るさを手動で調節する
- ホットプラグ対応の使用していないアクセサリを切断する(USB CD-ROM、外付けマウス、使用していないPCMCIAカードなど)
- アイドル中にはハードウェアディスクをスピンダウンする

SUSE Linuxでの電源管理およびYaSTの電源管理モジュールに関する背景情報は章 21. *電源管理* (page 287)に記載されています。

18.1.2 操作環境の変化の統合

モバイルコンピューティングに使用する場合、ご使用のシステムを操作環境の変化に順応させる必要があります。環境とそこに存在するクライアントに応じて、多くのサービスを再設定する必要があります。SUSE Linuxは、それらの作業をユーザに代わって行います。

図 18.1　ネットワークでのラップトップの統合



スモールホームネットワークとオフィスネットワーク間でラップトップを持ち運びする場合に影響のあるサービスは次のとおりです。

［ネットワークの設定］
IPアドレスの割り振り、名前解決、インターネット接続、およびその他のネットワークへの接続が含まれます。

印刷
使用可能なプリンタの現在のデータベース、および使用可能なプリントサーバが、ネットワークに応じて表示されなければなりません。

E-Mail (電子メール)とプロキシ
印刷と同様、現在の環境に対応するサーバが表示されなければなりません。

X Window Systemの設定
ご使用のラップトップが一時的にプロジェクタまたは外付けモニタに接続されている場合、異なるディスプレイ設定が使用可能になっていなければなりません。

SUSE Linuxではラップトップを既存の操作環境に統合させる2つの方法を提供しています。これらは組み合わせが可能です。

SCPM
SCPM (システム設定プロファイル管理)では任意のシステム設定状態を*プロファイル*と呼ばれる一種の「「スナップショット」」として格納することができます。プロファイルは異なる状況でも作成できます。プロファイルはシステムが異なる環境(ホームネットワーク、オフィスネットワーク)で操作される場合に便利です。常にプロファイルを切り替えることができます。SCPMについての情報は章 20. *システム設定プロファイル管理* (page 275)を参照してください。kickerアプレットであるKDEのProfile Chooserによりプロファイル間での切り替えが可能です。アプリケーションは切り替える際にrootパスワードを要求します。

SLP
サービスロケーションプロトコル(SLP)は既存のネットワークでのラップトップの接続を容易にします。SLPがなければラップトップの管理者は通常ネットワークで使用可能なサービスに関する詳細な知識が必要になります。SLPはローカルネットワーク上のすべてのクライアントに対し、使用可能な特定のタイプのサービスについてブロードキャストします。SLPをサポートするアプリケーションはSLPとは別に情報を処理し、自動的に設定することが可能です。SLPはシステムのインストールに使用することもできます。これを使用することで適切なインストールソースの検索を行う必要がなくなります。SLPについての詳細な情報は章 39. *ネットワーク上のSLPサービス* (page 657)を参照してください。

SCPMの重要性は再現可能なシステム条件を有効にし、保持することです。SLPはネットワークに接続されたコンピュータの設定のほとんどを自動化することで設定自体を容易にしています。

18.1.3 ソフトウェアオプション

モバイルでの使用を前提として専用ソフトウェアによってカバーされる様々な特殊タスク領域があります。次に例をあげます。システムモニタリング(特にバッテリの充電)、データ同期、周辺機器との無線通信、インターネット。次のセクションでは、SUSE Linuxが各タスクに提供する最も重要なアプリケーションについて説明します。

システムモニタリング

SUSE Linuxでは2種類のKDEシステムモニタリングツールを提供しています。ラップトップに備えられている再充電可能バッテリの単純状態の表示は、kickerのアプレットKPowersaveによって処理されます。複雑なシステムモニタリングはKSysguardによって実行されます。GNOMEを使用している場合、前述の機能はGNOME ACPI (パネルアプレットとして)およびSystem Monitorによって提供されます。

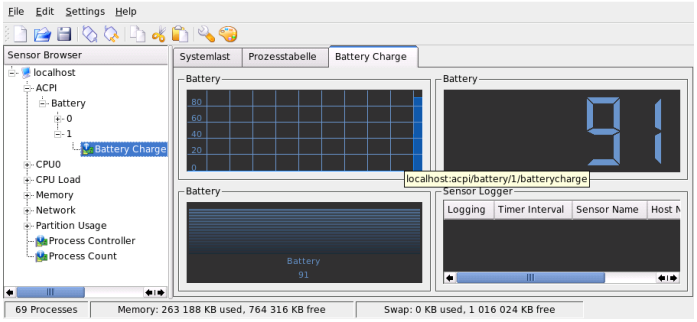
KPowersave

KPowersaveはコントロールパネルで再充電可能なバッテリの状態を表示するアプレットです。アイコンは電源のタイプを表示するように設計されています。AC電源で作業する場合、小さな電源のアイコンが表示されます。バッテリで作業する場合は、アイコンがバッテリに変わります。rootパスワードの入力が要求された後、対応するメニューにより電源管理用のYaSTモジュールが開きます。これにより異なるタイプの電源でもシステムの動作を設定することができます。電源管理および対応するYaSTモジュールについての情報は章 21. *電源管理* (page 287)を参照してください。

KSysguard

KSysguardは重要なシステムパラメータをすべて、モニタリング環境に集める独立したアプリケーションです。KSysguardはACPI (バッテリ状態)、CPUのロード、ネットワーク、パーティショニング、メモリ使用状況などを監視します。また、すべてのシステムプロセスを監視し、表示することも可能です。また、収集した情報の表示およびフィルタリングをカスタマイズできます。様々なデータページにある異なるシステムパラメータを監視したり、ネットワーク上で別々のマシンにあるデータを同時に収集することも可能です。KSysguardはKDE環境がなくてもマシン上でデーモンとして実行できます。このプログラムについての詳細な情報は、プログラムに組み込まれたヘルプ機能かヘルプページを参照してください。

図 18.2　KSysguardでのバッテリ状況のモニタリング



データの同期

ネットワークから切断されたモバイルマシンと、オフィスのネットワーク上にあるワークステーションの両方で作業を行う場合、すべての場合で処理したデータを同期しておくことが必要になります。これには電子メールフォルダ、ディレクトリ、個別の各ファイルなど、オフィスでの作業時と同様、オフィス外で作業する場合にも必須となるものが含まれます。両方の場合のソリューションを次に示します。

電子メールの同期

オフィスのネットワークの電子メールを格納するためにIMAPアカウントを使用します。これで電子メールはMozilla Thunderbird Mail、Evolution、またはスタートアップで説明されているKMailなどのような、切断されたIMAP対応の電子メールクライアントからアクセスできるようになります。送信メッセージで常に同じフォルダを使用するには、電子メールクライアントでの設定が必要になります。また、この機能により、同期プロセスが完了した時点でステータス情報とともにすべてのメッセージが使用可能になります。未送信メールについての信頼できるフィードバックを受信するためには、システム全体で使用するMTA postfixまたはsendmailの代わりに、メッセージ送信用のメールクライアントに実装されたSMTPサーバーを使用します。

ファイルと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のデータの同期に対応するユーティリティが複数あります。詳細については、章 47. *ファイルの同期* (page 789)を参照してください。

無線通信

ラップトップはケーブルを使用して自宅やオフィスのネットワークに接続するのと同様に、他のコンピュータ、周辺機器、携帯電話、PDAなどに無線接続することもできます。Linuxは3種類のタイプの無線通信をサポートします。

WLAN

これらの無線テクノロジの中では最大規模で、特にWLANは規模が大きく、ときに物理的に離れているネットワークでの運用に適している唯一のテクノロジと言えます。1台のマシンは独立した無線ネットワークやインターネットを介して互いに接続することができます。アクセスポイントと呼ばれるデバイスがWLAN対応デバイスの基地局として機能し、インターネットへの中継点としての役目を果たします。モバイルユーザは、場所や、どのアクセスポイントが最適な接続を提供するかによって、様々なアクセスポイントを切り替えることができます。WLANユーザは携帯電話網と同様の、特定のアクセス場所にとらわれる必要のない大規模ネットワークを使用できます。WLANについての詳細は項22.1.「無線LAN」 (page 313)を参照してください。

Bluetooth

Bluetoothはすべての無線テクノロジに対するブロードキャストアプリケーション周波数を使用します。BluetoothはIrDAのように、コンピュータ(ラップトップ)およびPDAまたは携帯電話間で通信するために使用できます。また視界内に存在する別のコンピュータと接続するために使用することもできます。Bluetoothはまたキーボードやマウスなど無線システムコンポーネントとの接続にも用いられます。ただし、このテクノロジはリモートシステムをネットワークに接続するほどには至っていません。壁のような物理的な障害物をはさんで行う通信にはWLANテクノロジが適しています。bluetooth、専用アプリケーション、および設定についての詳細は項22.2.「Bluetooth」 (page 324)を参照してください。

IrDA

IrDAは狭い範囲での無線テクノロジです。通信を行う両者は相手の見える位置にいなくてはなりません。壁のような障害物をはさむことはできません。IrDAで利用できるアプリケーションはラップトップと携帯電話間でファイルの転送を行うアプリケーションです。ラップトップから携帯電話までの距離が短い場合はIrDAを使用できます。ファイル受信者への長距離におよぶファイルの転送はモバイルネットワークが送信します。IrDAのもう1つのアプリケーションは、オフィスでの印刷ジョブを無線転送するア

プリケーションです。IrDAの詳細情報については、項22.3. 「赤外線データ通信」 (page 336)を参照してください。

18.1.4 データのセキュリティ

無認証のアクセスに対し、複数の方法でラップトップ上のデータを保護するのが理想的です。実行可能なセキュリティ対策は次の領域になります。

盗難からの保護
常にシステムを物理的な盗難から守ることを心がけます。チェーンなどのような様々な防犯ツールが小売店で販売されています。

システム上のデータの保護
重要なデータは転送時のみでなく、ハードディスク上に存在する時点でも暗号化するべきです。これは盗難時の安全性確保にも有効な手段です。SUSE Linuxでの暗号化パーティションの作成については項23.3. 「パーティションとファイルの暗号化」 (page 361)に記載されています。

重要項目: データの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のイベントの際にもアンマウントされません。それで、これらのパーティション上のデータは、ハードウェアが盗まれた場合、ハードディスクのレジュームを行うことで、誰にでも入手できるようになります。

ネットワークセキュリティ
データの転送はどのような状況下でも、必ず保護されていなくてはなりません。Linuxおよびネットワーク上での一般的なセキュリティ問題については項23.4. 「セキュリティと機密性」 (page 364)を参照してください。無線ネットワークについてのセキュリティ対策は章 22. *無線通信* (page 313)に記載されています。

18.2 モバイルハードウェア

SUSE LinuxはFireWire (IEEE 1394)またはUSB経由のモバイルストレージデバイスを自動検出します。*モバイルストレージデバイス*という用語は、FireWire、USBハードディスク、USBフラッシュドライブ、デジタルカメラのいずれに

も適用されます。これらのデバイスは専用のインタフェースからシステムに接続されると同時にホットプラグを介して自動的に検出、設定されます。subfsおよびsubmountはこれらのデバイスがファイルシステムの対応するロケーションに確実にマウントされたことを確認します。ユーザはSUSE Linuxの前バージョンのような手動によるマウント、アンマウントを行う必要がありません。デバイスは、プログラムがデバイスへのアクセスを終了した段階で、すぐに切断できます。

外付けハードディスク(USBおよびFireWire)
システムが外付けハードディスクを正しく認識するとすぐに、外付けハードディスクのアイコンがマイコンピュータ(KDE)またはコンピュータ(GNOME)のマウント済みリストに表示されます。アイコンをクリックすると、ドライブの内容が表示されます。ここでフォルダやファイルの作成および編集、削除を実行できます。システムに指定されたハードディスクの名前を変更するには、アイコンを右クリックしたときに開くメニューから、対応するメニューアイテムを選択します。この名前変更はファイルマネージャでの表示に限られています。`/media/usb-xxx`または`/media/ieee1394-xxx`でデバイスがマウントされているデバイスのデスクリプタは変更されず、そのままになります。

USBフラッシュドライブ
システムはこれらのデバイスを外付けハードディスクと同じように扱います。同様にファイルマネージャでエントリの名前変更をすることが可能です。

デジタルカメラ(USBおよびFireWire)
システムによって識別されたデジタルカメラもまた、ファイルマネージャの概要に外付けドライブのように表示されます。KDEではURL`camera:/`から写真を読み取ったり、アクセスしたりできます。さらに画像はdigikamまたはThe GIMPを使用して処理できます。GNOMEを使用している場合は、Nautilusのフォルダに写真が表示されます。簡単な画像処理および管理ユーティリティはf-spotです。高度な写真処理はThe GIMPで行います。デジタルカメラとイメージ管理の詳細については、章 15. *デジタルカメラとLinux* (page 219)を参照してください。

18.3 携帯電話とPDA

デスクトップシステムまたはラップトップはbluetoothまたはIrDAを介して携帯電話と通信できます。一部のモデルで両方のプロトコルをサポートしていますが、どちらか一方のみしかサポートしていないものもあります。これら2つのプロトコルの使用可能エリア、およびそれぞれの拡張マニュアルは無線通信項 (page 267)ですでに説明しました。携帯電話側におけるこれらのプロトコルの設定はそれぞれのマニュアルに記載されています。Linux側の設定は項22.2. 「Bluetooth」 (page 324)および項22.3. 「赤外線データ通信」 (page 336)を参照してください。

Plam社製のハンドヘルドデバイスを用いた同期のサポートはEvolutionおよびKontactにすでに組み込まれています。どちらの場合もデバイスとの初期接続はウィザードを利用して簡単に実行できます。Palm Pilotsのサポートがいったん設定されると、同期するデータのタイプ(アドレス、アポイントなど)を決定する必要があります。どちらのグループウェアについてもスタートアップに記載されています。

Kontactに統合プログラムであるKPilotは独立したユーティリティとしても利用可能です。これについてはスタートアップを参照してください。プログラムKitchenSyncもアドレスデータの同期に使用することができます。

18.4 関連資料

モバイルデバイスおよびLinuxに関連するすべてのお問い合わせは`http://tuxmobil.org/`を参照してください。このWebサイトではラップトップのハードウェア、ソフトウェア、PDA、携帯電話、その他のモバイルハードウェアについて複数のセクションで取り扱います。

`http://www.linux-on-laptops.com/`では、`http://tuxmobil.org/`と同様の内容について参照できます。ラップトップおよびハンドヘルドデバイスについての情報はここを参照してください。

SUSEはラップトップを主題としたドイツ語の専用メーリングリストを運営しています。`http://lists.suse.com/archive/suse-laptop/`を参照してください。このリストではユーザと開発者がSUSE Linuxでのモバイルコン

ピューティングに関するあらゆるテーマを話題にしています。英語での投稿には回答されますが、アーカイブされた情報のほとんどはドイツ語です。

ラップトップでのSUSE Linuxの電源管理に関して問題がある場合は、/usr/share/doc/packages/powersaveにあるREADMEファイルを確認することを推奨します。このディレクトリにはテスターや開発者からの最終段階でのフィードバックが盛り込まれます。そのため問題のソリューションについて、有用なヒントが含まれている場合があります。

19 PCMCIA

ここでは、PCMCIA ハードウェアおよびソフトウェアのラップトップ固有の側面について説明します。PCMCIAは*Personal Computer Memory Card International Association* の頭文字で、関連するハードウェアとソフトウェアの総称として使用されています。

19.1 ハードウェア

最も重要なコンポーネントはPCMCIAカードです。次の2つのタイプがあります。

PCカード
このタイプのカードは、PCMCIAの黎明期から存在しています。データ伝送に16ビットバスを使用するため、通常はごく廉価です。最近の一部のPCMCIAブリッジは、この種のカードを検出できない場合があります。しかし、検出されれば通常は円滑に動作し、問題が発生することはありません。

CardBusカード
PCカードより新しい標準です。ビットバスを使用しているため高速ですが、価格も高価です。この種のカードもPCIカードと同様にシステムに統合され、円滑に動作します。

2番目に重要なコンポーネントは、カードとPCIバス間の接続を確立するPCMCIAコントローラ、PCカードまたはCardBusブリッジです。共通モデルはすべてサ

ポートされています。内蔵PCIデバイスの場合は、コマンドlspci -vtを実行すると、詳細情報が表示されます。

19.2 ソフトウェア

現行のカーネルでは、PCMCIAブリッジおよびPCMCIAカードはホットプラグサブシステムによって処理されます。各ブリッジには、pcmcia_socketおよびpcmciaのイベントがあります。udevdは必要なモジュールすべてをロードし、デバイス設定に必要なツールを呼び出します。これらのアクションは、/etc/udev/rules.d/の中で定義されています。

/etc/pcmcia/config.optsはリソース設定に使用されます。必要なドライバは、ドライバ内のデバイステーブルによって判別されます。Information about the ソケットおよびカードの現在の状態についての情報は、/sys/class/pcmcia_socket/内およびpccardctl経由で入手できます。

PCMCIAシステムでは、引き続き変更が加えられているので、このマニュアルは不完全です。包括的な概要については、/usr/share/doc/packages/pcmciautils/README.SUSEファイルを参照してください。

20 システム設定プロファイル管理

SCPM (system configuration profile management)を使用して、さまざまな操作環境やハードウェア設定に合わせてコンピュータの設定を調整します。SCPMは、さまざまなシナリオに合わせた一連のシステムプロファイルを管理します。SCPMを使用すると、システムプロファイル間での切り替えが容易になり、システムを手動で再設定する必要がなくなります。

環境に応じてシステム設定を変更しなければならない場合があります。さまざまな場所で使用されるモバイルコンピュータなどは特にこのケースに該当します。また、デスクトップシステムでも通常使用しているのとは違うハードウェアコンポーネントを一時的に使用する必要がある場合などに、SCPMは有用です。元のシステム設定を簡単に復元できることはもとより、システム設定の変更を再現することも可能です。SCPMでは、システム設定のどの部分でもカスタマイズしたプロファイルとして保存できます。

SCPMが主に利用されるのは、ラップトップのネットワーク設定です。多くの場合、ネットワーク設定が違えば、電子メールやプロキシなど、他のサービスの設定も変更が必要になります。他の要素も同様です。自宅と会社で異なるプリンタを使用する、会議のマルチメディアプロジェクタ用にカスタマイズされたXサーバ設定を行う、外出先で特別な電源管理を適用する、外国支店で異なるタイムゾーンを使用するなど、さまざまな要因が考えられます。

20.1 用語

ここでは、SCPMのマニュアルやYaSTモジュールで使用される用語について説明します。

- *システム設定*という用語は、コンピュータの設定全体を指します。たとえば、ハードディスクパーティションの使用、ネットワーク設定、タイムゾーンの選択、およびキーボードマッピングなどの基礎的な設定をすべて含みます。

- *プロファイル*は、*設定プロファイル*とも呼ばれ、保存されていつでも復元可能な状態を指します。

- *有効なプロファイル*とは、最後に選択したプロファイルです。設定はいつでも変更できるので、現在のシステム設定が有効なプロファイルと同じだとは限りません。

- SCPMでいう*リソース*とは、システム設定に影響する要素を指します。これは、ファイルまたはソフトリンク(ユーザ、許可、またはアクセス時間などのメタデータを含む)です。また、このプロファイルでは動作するが、他のプロファイルでは動作しないシステムサービスも含まれます。

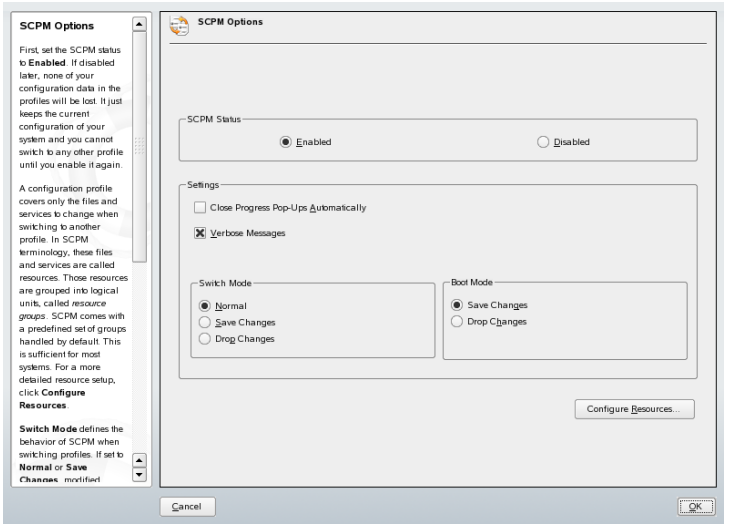
- すべてのリソースは、特定の*リソースグループ*に属します。リソースグループは論理的に共通なリソースで構成されます。ほとんどのグループには、サービスとその設定ファイルの両方が含まれています。SCPMによって管理されるリソースは、対象のサービスの設定ファイルに関する知識を必要としないため、ごく簡単に組み合わせることができます。SCPMには事前にリソースグループが設定されており、ほとんどの場合はそれらで対応できます。

20.2 YaSTのプロファイルマネージャを使う

YaSTコントロールセンターからYaSTのプロファイルマネージャを開始します(*[システム] → [プロフィール・マネージャ]*の順に選択)。または開始時に［*SCPMのオプション*］ダイアログで［*作動*］を選択することでSCPMを明示的に有効にします。図20.1.「YaSTのSCPMのオプション」 (page 277)を参照してください。［*設定*］では、ご使用のSCPMで進展ポップアップを自動的に閉じるか、進展に関するメッセージに詳しいメッセージを指定するかなどを決定します。［*切替えモード*では、プロファイルが切り替えられたとき、有効なプロファイルの変更されたリソースを保存するか、破棄するかを指定します。［*切替えモード*］が［*通常*］に設定されている場合、有効なプロファイルで行われたすべての変更は、プロファイルが切り替えられる時点で保存さ

れます。ブート時のSCPMの動作を定義するには［ブートモード］を［*変更を保存する*］(デフォルト設定)または［*変更を無視する*］に設定します。

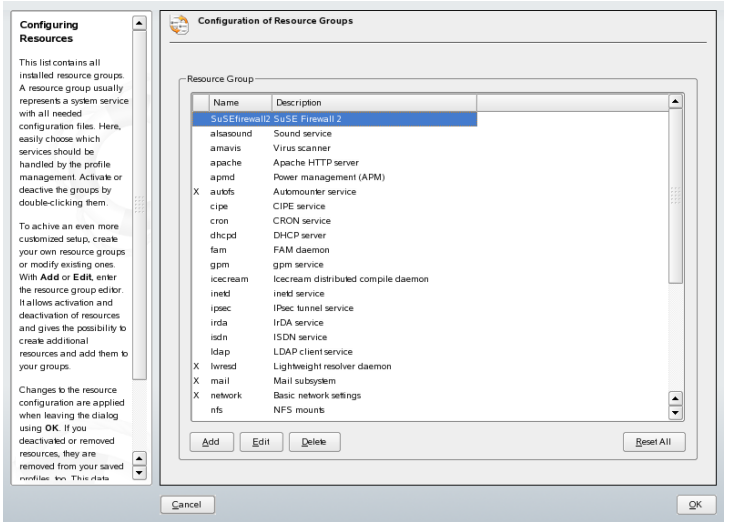
図 20.1 *YaSTのSCPMのオプション*



20.2.1 リソースグループの設定

現在のリソース設定を変更するには［*SCPMのオプション*］ダイアログで［*リソースを設定する*］オプションを選択します。その後のダイアログ(図 20.2. 「リソースグループの設定」 (page 278)を参照)には、システムで使用可能なすべてのリソースグループが一覧表示されます。リソースグループを追加または編集するには、［*リソースグループ*］および［*記述*］を指定、または編集します。LDAPサービスの場合は、たとえば［*リソースグループ*］に`ldap`、さらに［*記述*］にはLDAPクライアントサービスと入力します。続いて適切なリソース(サービス、設定ファイル、または両方)を入力するか、既存の設定を変更します。次に使用されていないリソースグループを削除します。選択したリソースの状態をリセットするには、つまりこれまでの変更内容をすべて破棄し、初期の設定値に戻すには、［*グループをリセットする*］を選択します。変更は有効なプロファイルに保存されています。

図 20.2　リソースグループの設定

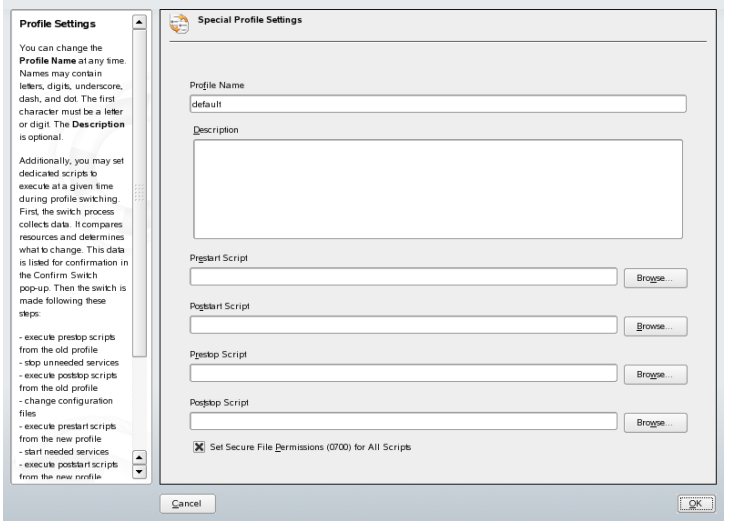


20.2.2　新規プロファイルの作成

新規プロファイルを作成するには開始ダイアログ(［*システム設定のプロファイル管理*］)で［*追加*］をクリックします。ウィンドウが開きます。ここでは新規プロファイルで、現在のシステム設定(SCPMが自動的に現在の設定を取得し、プロファイルが入力されます)をベースにするか、または既存のプロファイルを使用するかを選択します。新規プロファイルのベースとして現在のシステム設定を使用する場合、新規プロファイルを新規の有効なプロファイルに指定できます。この方法では旧プロファイルに対する変更は行われず、サービスを開始したり停止したりすることはありません。

続くダイアログで新規プロファイルの名前と簡潔な記述を入力します。SCPMでプロファイルを切り替えるために特別なスクリプトを実行するには、各実行可能ファイルのパスを入力します(図 20.3.「特別なプロファイルの設定」(page 279)を参照してください)。詳細については、項20.3.4.「詳細なプロファイル設定」(page 283)を参照してください。SCPMは新規プロファイルのリソースチェックを実行します。テストが正常に終了すると、新規プロファイルが使用可能になります。

図 20.3　特別なプロファイルの設定



20.2.3　既存のプロファイルの設定

既存のプロファイルを変更するには開始ダイアログ(［*システム設定のプロファイル管理*］)で［*編集*］をクリックします。次に必要に応じて名前、記述、スクリプト、およびリソースを編集します。

20.2.4　プロファイルの切り替え

プロファイルを切り替えるには、プロファイルマネージャを開きます。有効なプロファイルは矢印でマークされています。切り替えるプロファイルを選択し、［*切替え*］をクリックします。SCPMは新規または変更されたリソースを確認し、必要に応じてそれらを追加します。

リソースが変更されると、YaSTにより［*切替えを確認する*］ダイアログが表示されます。［*有効なプロファイル中の変更されたリソースグループ*］は、変更されただけでまだ有効なプロファイルに保存されていないリソースグループを一覧表示します。現在選択されているリソースグループの［*保存または無視する*］では、このリソースグループへの変更を有効なプロファイルに保存するか、または破棄するかを指定します。または、各リソースを選択して

［*詳細*］をクリックし、変更点を詳細に確認します。これにより編集されたリソースグループに含まれる設定ファイル、または実行可能ファイルがすべて一覧表示されます。新旧のバージョンを1行ずつ比較するには［*変更を表示する*］をクリックします。変更の確認が終了したら、［アクション］で変更へのアクションを指定します。アクションには以下のような項目があります。

リソースを保存する
　このリソースを有効なプロファイルに保存しますが、他のすべてのプロファイルへの変更は行いません。

リソースを無視する
　有効なリソースへの変更を行いません。この変更は破棄されます。

すべてのプロファイルに保存する
　このリソースの設定全体をすべてのプロファイルにコピーします。

全てのプロファイルにパッチを当てる
　すべてのプロファイルに最新の変更のみを適用します。

［*全てを保存または無視する*］はそのまま保存するか、またはこのダイアログに表示されているすべてのリソースの変更を破棄します。

有効なプロファイルの変更を確認した後、［*了解*］をクリックして［*切替えを確認する*］ダイアログを終了します。これでSCPMが新規プロファイルに切り替わります。切り替えている間、旧プロファイルに対しprestopおよびpoststopスクリプトを実行し、新規プロファイルにprestartおよびpoststartスクリプトを実行します。

20.3　コマンドラインを使用したSCPMの設定

このセクションではコマンドラインを使用してSCPMを設定する方法を説明します。まず初めに開始方法を説明し、続いて設定方法、そしてプロファイルの利用方法について説明します。

20.3.1 SCPMの起動とリソースグループの定義

SCPMは使用する前に有効にする必要があります。SCPMを有効にするには、コマンドscpm enableを使用します。SCPMを初めて実行すると初期化が行われますが、これには数秒かかります。SCPMはいつでもscpm disableで無効にできます。これにより誤ってプロファイルが切り替わらないようにすることができます。その後、再度有効にするには、初期化を再開するだけです。

デフォルトでは、SCPMはネットワークやプリンタだけでなく、X.Orgの設定も処理します。特別なサービスや設定ファイルを管理するには、それぞれのリソースグループを有効にします。事前定義のリソースグループを一覧表示するには、scpm list_groupsを使用します。既に有効なグループのみを表示するには、scpm list_groups -aを使用します。これらのコマンドは、コマンドラインでrootとして実行します。

```
scpm list_groups -a

nis                 Network Information Service client
mail                Mail subsystem
ntpd                Network Time Protocol daemon
xf86                X Server settings
autofs              Automounter service
network             Basic network settings
printer             Printer settings
```

グループを有効または無効にするには、それぞれscpm activate_group NAMEとscpm deactivate_group NAMEを使用します。ここでNAMEは、対象のグループ名に置き換えて使用してください。

20.3.2 プロファイルの作成と管理

SCPMを有効にすると、defaultという名前のプロファイルが自動的に作成されます。利用可能なプロファイルを一覧表示するには、scpm listを実行します。この既存プロファイルが有効なプロファイルでもあります。コマンドscpm activeで確認できます。プロファイルdefaultは基本設定であり、これを元に他のプロファイルを作成することが可能です。このため、すべてのプロファイルで同一になる設定をあらかじめすべて設定してしまいます。

続いてこれらの変更内容をコマンドscpm reloadを使用して、有効なプロファイルに保存します。次回からはdefaultプロファイルを新規プロファイルのベースとしてコピーし、名前を変更して使用できます。

新しいプロファイルを追加する方法は2つあります。プロファイルdefaultをベースにして、新規プロファイル(ここではworkとします)を作成する場合は、コマンドscpm copy default workを実行します。コマンドscpm switch workを実行すると、新しいプロファイルに切り替わり、変更が可能になります。特別な用途に合わせてシステム設定を変更し、変更内容を新しいプロファイルに保存できます。この場合、コマンドscpm add workを実行すると、新しいプロファイルが作成されるとともに、作成されたプロファイルworkに現在のシステム設定が保存され、有効を示すマークが付きます。scpm reloadを実行すると、変更内容がプロファイルworkに保存されます。

プロファイルの名前の変更または削除には、それぞれコマンドscpm rename x yおよびscpm delete zを使用します。たとえば、workという名前をprojectに変更するには、scpm rename work projectと入力します。projectを削除するには、コマンドscpm delete projectを入力します。有効なプロファイルは削除できません。

20.3.3 設定プロファイルの切り替え

コマンドscpm switch workを実行すると、別のプロファイル(ここでは、プロファイルwork)に切り替えることができます。有効なプロファイルに切り替えると、変更したシステム設定が組み込まれます。これは、コマンドscpm reloadに対応します。

プロファイルを切り替えると、まずSCPMは有効なプロファイルのリソースが変更されているかを確認します。次に、各リソースの変更内容を有効なプロファイルに追加するか、削除するかを確認するメッセージが表示されます。リソースを別に一覧表示する場合(以前のバージョンのSCPMのように)は、スイッチコマンドで-rパラメータを使用して、scpm switch -r workのように指定してください。

```
scpm switch -r work
```

変更したリソースの確認、
開始/シャットダウンするリソースの確認、

次にSCPMは、現在のシステム設定と切り替えた後のプロファイルを比較します。この段階で、SCPMは相互依存への対応や設定変更の反映のために停止または再起動が必要なシステムサービスを評価します。これは、部分的なシステムリブートのようなもので、システムのごく一部だけがリブートし、残りの部分は変更なく動作し続けます。システムサービスが停止し、変更されたすべてのリソース(たとえば、設定ファイル)が書き込まれ、システムサービスが再起動されるのは、この時点のみです。

20.3.4 詳細なプロファイル設定

すべてのプロファイルには説明を入力できます。説明はscpmlistを使って表示できます。有効なプロファイルに説明を入力するには、`scpm set description "text"`を実行します。有効なプロファイル以外のプロファイル名を使用するには、たとえば、`scpm set description "text" work`のように指定します。場合によっては、プロファイルの切り替え時に、SCPMが提供する以外のアクションを実行することがあります。各プロファイルには、最高4つの実行可能ファイルを添付することができます。これらはそれぞれ、切り替え処理において起動する段階が異なります。これら4つの段階を次に示します。

prestop
　切り替え前、サービス停止前

poststop
　切り替え前、サービス停止後

prestart
　切り替え後、サービス停止前

poststart
　切り替え後、サービス停止後

これらのアクションを挿入するには、コマンドsetを、`scpm set prestop filename`、`scpm set poststop filename`、`scpm set prestart filename`、`scpm set poststart filename`のように使用します。スク

リプトが実行可能ファイルであることと、正しいインタプリタを参照することが必要です。

警告: カスタムスクリプトの統合

SCPMにより実行されるその他のスクリプトを、スーパーユーザ(root)が読み取って実行できるようにする必要があります。他のユーザは誰もこれらのファイルにアクセスできないようにします。コマンド`chmod 700 filename`および`chown root: root filename`を入力して、rootにファイルへの排他アクセス権を付与します。

setコマンドで追加した設定を表示するには、コマンドgetを使用します。たとえば、コマンド`scpm get poststart`を実行すると、poststartの名前が返されるか、何も添付していない場合は何も返されません。このような設定は、""を使って上書きできます。`scpm set prestop ""`を実行すると、添付したprestopプログラムが削除されます。

すべてのsetコマンドとgetコマンドは、コメントを追加する場合と同じように任意のプロファイルに適用できます。たとえば、`scpm get prestop filename work`または`scpm get prestop work`となります。

20.4 プロファイル選択アプレットを使う

GNOMEまたはKDEデスクトップパネルのプロファイル切り替えアプレットを使えば、SCPMの設定を簡単に制御できます。項20.2. 「YaSTのプロファイルマネージャを使う」 (page 276)で説明しているように、YaSTでプロファイルを作成、修正、削除して、プロファイルを切り替えてください。プロファイルの切り替えは、システム管理者が許可していれば、通常のユーザとして実行できます。*[システム] → [デスクトップアプレット] → [Profile Chooser]*の順に選択して、Profile Chooserを起動します。

通常のユーザがプロファイルを切り替えるには、デスクトップパネル上のProfile Chooserのアイコンを右クリックして、表示されるメニューから［*Allow user switching*］を選択します。rootのパスワードを入力します。システム上の、認可を受けたユーザであれば、この後プロファイルを切り替えることができます。

Profile Chooserのアイコンをクリックすると、YaSTの直接の呼び出し、または［*Start YaST2 Profile Manager Module*］によって、YaSTで設定されたすべてのプロファイルが表示されます。カーソルキーを使っていずれかを選択すると、SCPM葉新しいプロファイルに自動的に切り替わります。

20.5 トラブルシューティング

このセクションではSCPMでよく起こる問題について説明します。どのようにして問題が起こるか、そしてどのようにこれらの問題を解決するかについても説明します。

20.5.1 切り替えプロセス中の終了

SCPMが切り替えプロシージャ中に動作を停止することがあります。ユーザによる中止操作や電源障害、外部要因によって起こることもありますし、SCPM自体のエラーによることもあります。このような場合、次回SCPMを起動すると、SCPMがロックされているというエラーメッセージが表示されます。これはシステムの安全を確保するための措置です。なぜならデータベースに格納されているデータと、システムの状態とが食い違うことがあるからです。この問題を解決するには、`scpm recover`を実行します。SCPMが前回実行できなかったすべての操作を実行します。また、`scpm recover -b`を実行することもできます。これは前回実行時に実行された操作のアンドゥを試みます。YaSTプロファイルマネージャを使用している場合は、開始時に修復ダイアログが表示されます。このダイアログでは前述のコマンドを実行できます。

20.5.2 リソースグループ設定の変更

SCPMの初期化が完了した後にリソースグループの設定を変更するには、グループを追加または削除してから`scpm rebuild`と入力します。これにより、すべてのプロファイルに新規リソースが追加され、削除したリソースは完全に削除されます。削除したリソースの設定が各種プロファイル内で異なっている場合、この設定データは失われます。ただし、システム内の最新バージョンはそのまま残ります。YaSTで設定を変更する場合、rebuildコマンドを入力する必要はありません。これはYaSTにより処理されます。

20.6 システムブート時のプロファイル選択

システムのブート時にプロファイルを選択するには、ブート画面上でF3を押して、使用可能なプロファイルのリストを表示します。矢印キーを使用してプロファイルを選択し、Enterキーで決定します。これで選択したプロファイルがブートオプションとして使用されます。

20.7 関連資料

最新のドキュメントは、SCPMのinfoページで利用可能です(info scpm)。開発者向けの詳細については、 `/usr/share/doc/packages/scpm`を参照してください。

21 電源管理

電源管理はラップトップコンピュータで特に重要ですが、他のシステムでも役に立ちます。APM (advanced power management)とACPI (advanced configuration and power interface)という、2つのテクノロジが利用可能です。これらに加えて、電源の節約や騒音の低減のために、CPU周波数を制御することもできます。これらのオプションは手動で、または専用のYaSTモジュールを使って設定することができます。

従来、電源管理用としてラップトップのみで使用されてきたAPMとは異なり、ハードウェアの情報および設定を管理するツールであるACPIは、近年、ラップトップ、デスクトップ、サーバなど、あらゆるコンピュータ上で利用されています。どのような電源管理テクノロジでも、適切なハードウェアとBIOSルーチンを必要とします。ほとんどのラップトップと多くの新型デスクトップおよびサーバは、これらの必要条件を満たしています。

APMは、従来型のコンピュータで多く使われてきました。APMは、ほとんどがBIOSに実装された関数セットからなるため、APMサポートのレベルはハードウェアによって異なります。より複雑なACPIでは、この傾向がさらに強まります。このため、どちらか片方を推奨することは無理です。さまざまな手順をハードウェア上でテストし、最も適切なサポートが実現できるテクノロジを選択してください。

重要項目: AMD64プロセッサの電源管理

64ビットカーネルを搭載したAMD64プロセッサは、ACPIのみをサポートしています。

21.1 省電力機能

省電力機能はラップトップをモバイル使用する場合に限らず、デスクトップシステムでも重要です。APMおよびACPI電源管理システムの主要な機能と、その使用目的は、以下のとおりです。

スタンバイ
この動作モードは、ディスプレイの電源をオフにします。プロセッサのパフォーマンスを低下させるコンピュータも一部あります。この機能は、すべてのAPMの実装で利用可能とは限りません。この機能は、ACPI状態S1またはS2に対応します。

サスペンド(メモリに保存)
このモードでは、システム状態をすべてRAMに書き込みます。その後、RAMを除くシステム全体がスリープします。この状態では、コンピュータの消費電力が非常に小さくなります。この状態の利点は、ブートやアプリケーションの再起動をせずに、数秒でスリープ前の作業をスリープの時点から再開できることです。通常、APMを使用するデバイスは、ふたを閉じればサスペンドし、開ければ再開します。この機能はACPI状態S3に対応します。この状態のサポートはまだ開発中なので、ハードウェアに大幅に依存します。

ハイバーネーション(ディスクに保存)
この動作モードでは、システム状態がすべてハードディスクに書き込まれ、システムの電源がオフになります。この状態から再開するには、30〜90秒かかります。サスペンド前の状態が復元されます。メーカの中には、このモードを便利なハイブリッド仕様にして提供するものもあります(たとえば、IBM ThinkpadのRediSafe)。対応するACPI状態は、S4です。Linux環境では、suspend to diskはAPMおよびACPIから独立したカーネルルーチンにより実行されます。

バッテリモニタ
ACPIとAPMは、バッテリをチェックして、充電ステータスに関する情報を提供します。また、どちらのシステムも、重要な充電ステータスに達した時点で実行するようにアクションを調整します。

自動電源オフ
シャットダウンの後、コンピュータの電源が切れます。これは、バッテリが空になる直前に自動シャットダウンが行われる場合に特に重要です。

システムコンポーネントのシャットダウン
システム全体を考えた場合、電力消費量を抑えるという点では、ハードディスクをオフにすることが最も重要です。システム全体の信頼性に応じて、しばらくハードディスクをスリープ状態にすることは可能です。ただし、スリープ時間が長くなれば、データ損失のリスクも高くなります。他のコンポーネントは、(少なくとも理論的には)ACPIによって無効にでき、またBIOSセットアップによって永久に無効にすることもできます。

プロセッサ速度の制御
CPUに関連する省エネルギー方法は次の3つです。周波数調節と電圧調節(PowerNow!またはSpeedstep)、スロットリング、およびプロセッサのスリープ状態(C状態)への切り替えです。コンピュータの動作モードによっては、この3つの方法を併用することもできます。

21.2 APM

省電力機能の中には、APM BIOS自体によって実行される機能もあります。多くのラップトップにおいて、スタンバイ状態とサスペンド状態は、特別なオペレーティングシステムの機能を使用するのではなく、キーの組み合わせによって、またはふたを閉じることによって有効になります。しかし、コマンドを使用してこれらのモードを有効にするには、システムがサスペンドする前に、特定のアクションがトリガされなければなりません。さらに、バッテリの充電レベルを表示するには、特殊なプログラムパッケージと適切なカーネルが必要になります。

SUSE Linuxのカーネルは、ビルトインでAPMをサポートしています。しかし、APMが有効になるのは、ACPIがBIOSに実装されておらず、APM BIOSが検出された場合に限られます。APMサポートを有効にするには、ブートプロンプトで`acpi=off`を実行してACPIを無効にする必要があります。APMが有効かどうかを確認するには、`cat /proc/apm`を入力します。ここでさまざまな値が出力されれば、すべて正常であることを意味します。ここで、コマンド`shutdown -h`を実行して、コンピュータをシャットダウンします。

BIOS実装が規格に完全に準拠していないと、APMに問題が発生することがあります。一部の問題は、特殊なブートパラメータで回避できます。すべてのパラメータは、ブートプロンプトで、`apm=parameter`の形式で入力します。

onまたはoff
APMサポートの有効化または無効化

(no-)allow-ints
BIOS機能の実行中の中断を許可します。

(no-)broken-psr
BIOSの「GetPowerStatus」機能が正しく動作しません。

(no-)realmode-power-off
シャットダウンの前にプロセッサをリアルモードにリセットします。

(no-)debug
APMイベントをシステムログに記録します。

(no-)realmode-power-off
シャットダウンの後、システムの電源を切断します。

bounce-interval=*n*
サスペンドイベントの後、別のサスペンドイベントが無視される時間を1/100秒単位で表した数値です。

idle-threshold=*n*
システムのアイドル状態がこの値に達するとBIOSの`idle`関数が実行されます(0=常時、100=実行しない)。

idle-period=*n*
システムアクティビティを測定した後の時間を1/100秒単位で表した数値。

APMデーモン(apmd)は廃止になりました。その機能はACPIおよびCPUの周波数調節もサポートする新しいpowersavedで処理されます。

21.3 ACPI

ACPI (advanced configuration and power interface)は、オペレーティングシステムが個々のハードウェアコンポーネントをセットアップ、および制御できるように設計されています。ACPIは、PnPとAPMの両方の後継となります。また、ACPIはバッテリ、ACアダプタ、温度、ファン、および「close lid」や「battery low」などのシステムイベントに関する情報も提供します。

BIOSには個々のコンポーネントとハードウェアアクセス方法についての情報が入ったテーブルがあります。オペレーティングシステムは、この情報を使用して、割り込みまたはコンポーネントの有効化と無効化などのタスクを実行します。BIOSに格納されているコマンドを、オペレーティングシステムが実行するとき、機能はBIOSの実装方法に依存します。ACPIが検出可能で、ロードできるテーブルは、 /var/log/boot.msgにレポートされます。ACPIに生じた問題のトラブルシューティングについては、項21.3.4.「トラブルシューティング」 (page 296)を参照してください。

21.3.1 動作中のACPI

システムのブート時に、カーネルがACPI BIOSを検出する場合、ACPIが自動的に有効になり、APMが無効になります。旧式のコンピュータでは、ブートパラメータacpi=onを指定しなければならない場合があります。コンピュータは、ACPI 2.0以降をサポートする必要があります。 /var/log/boot.msgのカーネルブートメッセージで、ACPIが有効にされていることを確認します。

続いて、複数のモジュールがロードされます。これは、powersaveデーモンの起動スクリプトによって行われます。 これらのモジュールのいずれかに問題が発生すると、対応するモジュールが/etc/sysconfig/powersave/commonでのロードまたはアンロードから除外されます。 システムログ(/var/log/messages)には、モジュールのメッセージが入っているので、どのコンポーネントが検出されたことがわかります。

/proc/acpiには、システム状態に関する情報を提供するファイルや、状態を変更するために使用できるファイルが多数含まれています。一部の機能はまだ開発中であるため動作しません。また、一部の機能はメーカの実装状況に大きく依存するためサポートされていない場合もあります。

すべてのファイル(dsdtおよびfadt)は、コマンドcatで読み取ることができます。一部のファイルでは、echoで設定を変更できます。たとえば、echo X > fileでXに適した値を指定します。この情報と制御オプションにアクセスするには、常にコマンドpowersaveを使用します。以下で最も重要なファイルについて説明します。

/proc/acpi/info
ACPIに関する一般的な情報

/proc/acpi/alarm
システムがいつスリープ状態から回復するかを指定します。現在、この機能は完全にはサポートされていません。

/proc/acpi/sleep
さまざまなスリープ状態に関する情報を提供します。

/proc/acpi/event
すべてのイベントがここにレポートされ、Powersaveデーモン(powersaved)で処理されます。Powerボタンの押下げ、またはふたを閉じるなど、いずれのデーモンもこのファイルにアクセスしないイベントは、cat /proc/acpi/eventによって読み取ることができます(Ctrl+Cで終了します)。

/proc/acpi/dsdtおよび/proc/acpi/fadt
これらのファイルにはACPIテーブルのDSDT (differentiated system description table)とFADT (fixed ACPI description table)が含まれています。これらは、acpidmp、acpidisasm、およびdmdecodeで読み取ることができます。これらのプログラムとマニュアルは、パッケージpmtoolsにあります。たとえば、acpidmp DSDT | acpidisasmなどです。

/proc/acpi/ac_adapter/AC/state
ACアダプタが接続されているかを示します。

/proc/acpi/battery/BAT*/{alarm,info,state}
バッテリ状態についての詳細情報です。充電レベルを読み取るには、infoのlast full capacityとstateのremaining capacityを比較します。これをもっと円滑に行うには、項21.3.3.「ACPIツール」 (page 296)で説明する特別なプログラムの1つを使用します。バッテリイベントがトリガされる充電レベルは、alarmで指定できます。

/proc/acpi/info
このディレクトリには、さまざまなスイッチについての情報が入っています。

/proc/acpi/fan/FAN/state
ファンが現在、作動しているかを示します。ファンは、このファイルに0(オン)か3(オフ)かを書き込むことによって、オンまたはオフにできます。

ただし熱が上がりすぎた場合は、カーネルとハードウェア(またはBIOS)の両方のACPIコードによってこの設定が上書きされます。

/proc/acpi/processor/*
システムに搭載されているCPUごとに、個別のサブディレクトリが保持されます。

/proc/acpi/processor/*/info
プロセッサの省エネオプションに関する情報。

/proc/acpi/processor/*/power
現在のプロセッサ状態に関する情報。C2の横にアスタリスクが付いている場合、プロセッサがアイドル状態です。usageに示すように、これが最もよくある状態です。

/proc/acpi/processor/*/throttling
プロセッサクロックの減速の設定に使用できます。通常、スロットリングは8つのレベルで使用できます。これは、CPUの周波数制御とは独立しています。

/proc/acpi/processor/*/limit
パフォーマンス(廃止)とスロットリングがデーモンによって自動的に制御される場合、上限をここで指定できます。上限の一部はシステムによって定義されますが、ユーザが調整できる上限もあります。

/proc/acpi/thermal_zone/
すべてのサーマルゾーンに対し、個別の下位ゾーンが存在します。サーマルゾーンとは、よく似たサーマルプロパティを持ち、ハードウェアメーカによって番号と名前が指定された領域です。しかし、ACPIが持つ可能性の多くは、ほとんど実装されていません。そして、温度制御は相変わらずBIOSによって管理されています。オペレーティングシステムが介入すると、ハードウェアの寿命が短くなるので、オペレーティングシステムが介入する機会はあまりありません。したがって、一部のファイルの内容は、単なる理論上の値です。

/proc/acpi/thermal_zone/*/temperature
サーマルゾーンの現在の温度です。

/proc/acpi/thermal_zone/*/state
この状態は、すべてがokなのか、またはACPIがアクティブまたはパッシブ冷却を適用しているかを示します。ACPI独立のファン制御の場合、この状態は常にokです。

/proc/acpi/thermal_zone/*/cooling_mode
ACPIで制御される冷却化方式を選択します。パッシブ(パフォーマンスは低いが経済的)またはアクティブ(フルパフォーマンス、ファンノイズ)のどちらかを選択できます。

/proc/acpi/thermal_zone/*/trip_points
パッシブ/アクティブ冷却、サスペンション(hot)、またはシャットダウン(critical)など、特定のアクションをトリガする温度を設定します。可能なアクションは、DSDT(デバイス依存)内で定義されます。ACPI仕様で定義されているトリップポイントは、critical、hot、passive、active1、およびactive2です。実装されていないトリップポイントがあっても、このファイルにはすべてを常にこの順序で入力する必要があります。たとえば、エントリ echo 90: 0: 70: 0: 0 > trip_points は、critical の温度を 90、passive の温度を 70 に設定します (温度はすべて摂氏)。

/proc/acpi/thermal_zone/*/polling_frequency
温度が変化してもtemperatureの値が自動的に更新されない場合は、ポーリングモードをここでオンにします。コマンド echo X > /proc/acpi/thermal_zone/*/polling_frequency を使用すると、X秒ごとに温度の問い合わせが行われます。ポーリングを無効にするには、X=0に設定します。

これらの設定、情報、イベントは、いずれも手動で編集する必要はありません。編集はPowersaveデーモン(powersaved)および各種アプリケーション(powersave、kpowersave、wmpowersaveなど)で実行できます。項21.3.3.「ACPIツール」 (page 296)を参照してください。powersavedには古いacpidの機能が含まれているため、acpidは不要です。

21.3.2 CPUパフォーマンスの制御

CPUには、3つの省電力方法があります。コンピュータの動作モードによっては、この3つの方法を併用することもできます。また、省電力とは、システム

の温度上昇が少なく、ファンが頻繁にアクティブにならないことを意味します。

周波数と電圧の調節

PowerNow!とSpeedstepは、AMD社とIntel社が使用するこのテクノロジの名称です。ただし、このテクノロジは他のメーカのプロセッサにも適用されます。CPUのクロック周波数とそのコア電圧が同時に低下し、段階的な省エネよりも大きな効果が得られます。つまり、周波数が半分になると(半分のパフォーマンス)、消費電力も半分以下になります。このテクノロジはAPMにもACPIにも依存せず、周波数と所要電流をパフォーマンスに合わせて調整するデーモンを必要とします。設定は、ディレクトリ`/sys/devices/system/cpu/cpu*/cpufreq/`内で行うことができます。

クロック周波数のスロットリング(速度を抑える)

このテクノロジでは、CPUのクロック信号インパルスが一定割合だけ省略されます。25%のスロットリングでは、4回に1回の割合でインパルスが省略されます。87.5%では、プロセッサにインパルスが届くのは8回に1回だけになります。ただし、省エネ度が減速の割合に比例して増えることはありません。通常、スロットリングが使用されるのは、周波数調節を使用できない場合、または省電力を最大限に使用する場合だけです。このテクノロジも、特殊なプロセスで制御する必要があります。システムインタフェースは、`/proc/acpi/processor/*/throttling`です。

プロセッサのスリープ状態への切り替え

オペレーティングシステムは、何も実行することがない場合にプロセッサをスリープ状態にします。この場合、オペレーティングシステムはCPUに`halt`コマンドを送ります。 C1、C2、C3という3つの状態があります。最も経済的な状態C3では、プロセッサキャッシュとメインメモリとの同期も停止します。そのため、この状態を適用できるのは、バスマスタアクティビティを介してメインメモリの内容を変更している他のデバイスが存在しない場合だけです。一部のドライバでは、C3を使用できません。現在の状態は、`/proc/acpi/processor/*/power`に表示されます。

周波数調節とスロットリングが関係するのは、プロセッサがビジー状態の場合だけです。これは、プロセッサがアイドル状態のときには、最も経済的なC状態が常に適用されるためです。CPUがビジー状態の場合、省電力方式として周波数調節を使用することをお勧めします。通常、プロセッサは部分的な負荷でのみ動作します。この場合は、低周波数で実行できます。一般に、powersavedのようなデーモンで制御される動的な周波数調節が最善の方法とい

えます。低周波数をスタティックに設定する方法は、バッテリ使用時やコンピュータを冷却または静止させたい場合に役立ちます。

スロットリングは、システムが高負荷であるにもかかわらずバッテリ使用時間を延長する場合など、最後の手段として使用する必要があります。ただし、スロットリングの割合が高すぎると、スムーズに動作しないシステムがあります。さらに、CPUの負荷が小さければ、CPUスロットリングは無意味です。

SUSE Linuxでは、これらのテクノロジはpowersaveデーモンで制御されます。この設定については、項21.5.「powersaveパッケージ」 (page 299)を参照してください。

21.3.3 ACPIツール

総合的と呼べるACPIユーティリティには、バッテリ充電レベルや温度などの情報を表示するだけのツール(acpi、klaptopdaemon、wmacpimonなど)、`/proc/acpi`内の構造へのアクセスを容易にするツール、変化の監視を補助するツール(akpi、acpiw、gtkacpiw)、BIOS内のACPIテーブルを編集するためのツール(パッケージ`pmtools`)などが含まれています。

21.3.4 トラブルシューティング

問題を2つに大別できます。1つはカーネルのACPIコードに、未検出のバグが存在する可能性があることです。この場合は、いずれ修正プログラムがダウンロードできるようになります。ただし、問題の多くはBIOSが原因になっています。また、場合によっては、他の広く普及しているオペレーティングシステムにACPIを実装した場合にエラーが起きないよう、BIOSにおけるACPIの指定を故意に変えていることがあります。ACPIに実装すると重大なエラーを生じるハードウェアコンポーネントは、ブラックリストに記録され、これらのコンポーネントに対してLinuxカーネルがACPIを使用しないようにします。

問題に遭遇したときに最初に実行することは、BIOSの更新です。コンピュータがまったくブートしない場合、次のブートパラメータは有用です。

pci=noacpi
PCIデバイスの設定にACPIを使用しません。

acpi=oldboot
単純なリソース設定のみを実行します。ACPIを他の目的には使用しません。

acpi=off
ACPIを無効にします。

警告: ACPIなしに起動できない場合

一部の新型のコンピュータは(特に、SMPシステムとAMD64システム)、ハードウェアを正しく設定するためにACPIが必要です。これらのコンピュータでACPIを無効にすると、問題が生じます。

システムのブートメッセージを調べてみましょう。そのためには、ブート後にコマンド`dmesg | grep -2i acpi`を使用します(または、問題の原因がACPIだとは限らないので、すべてのメッセージを調べます)。ACPIテーブルの解析中に問題が発生した場合は、最も重要なテーブル(DSDT)を改良版に置き換えます。この場合、BIOSで障害のあるDSDTが無視されます。処理手順については、項21.5.4.「トラブルシューティング」 (page 305)を参照してください。

カーネルの設定には、ACPIデバッグメッセージを有効にするスイッチがあります。ACPIデバッグを有効にした状態でカーネルをコンパイルし、インストールすると、詳細な情報を表示するエラーのエキスパート検索がサポートできるようになります。

BIOSまたはハードウェアに問題がある場合は、常にメーカに連絡することをお勧めします。特に、Linuxに関するサポートを常に提供していないメーカには、問題を通知する必要があります。なぜなら、メーカは、自社の顧客の無視できない数がLinuxを使用しているとわかってやっと、問題を真剣に受け止めるからです。

関連資料

ACPIに関する補足資料とヘルプ

- `http://www.cpqlinux.com/acpi-howto.html`(詳細なACPI HOWTO、DSDTパッチが含まれています)

- http://www.intel.com/technology/iapc/acpi/faq.htm(IntelのACPIに関するFAQ)
- http://acpi.sourceforge.net/(SourceforgeによるACPI4Linuxプロジェクト)
- http://www.poupinou.org/acpi/(Bruno DucrotによるDSDTパッチ)

21.4 ハードディスクの休止

Linux環境では、不要な場合にハードディスクを完全にスリープ状態にしたり、より経済的な静止モードで動作させることができます。最近のラップトップの場合、ハードディスクを手動でオフに切り替える必要はありません。不要な場合は自動的に経済的な動作モードになります。ただし、省電力レベルを最大限にする場合は、次の方法をいくつかテストしてください。機能のほとんどは、powersavedおよびYaST電源管理モジュールでコントロールできます。その詳細については、項21.6. 「YaST電源管理モジュール」 (page 308)を参照してください。

hdparmアプリケーションを使用して、各種のハードディスク設定を変更できます。オプション-yは、簡単にハードディスクをスタンバイモードに切り替えます。 オプション-Yはハードディスクをスリープにします。 コマンド hdparm -S xを使用すると、一定時間アクティビティがなければハードディスクが回転を停止します。xは、次のように使用します。0にすると、このメカニズムが無効になり、ハードディスクがずっと回り続けます。1から240までの値を指定すると、指定した値x5秒が設定値になります。241から251は、30分の1倍から11倍(30分から5.5時間)に相当します。

ハードディスクの内部省電力オプションは、オプション-Bで制御できます。0 (最大限の省電力)～255 (最大限のスループット)の値を選択します。結果は使用するハードディスクに応じて異なり、査定するのは困難です。ハードディスクを静止状態に近づけるにはオプション-Mを使用します。128(静止)～254(高速)の値を選択します。

ハードディスクをスリープにするのは、多くの場合簡単ではありません。Linuxでは、多数のプロセスがハードディスクに書き込むので、ウェイクアップが常に繰り返されています。したがって、ハードディスクに書き込むデータを、Linuxがどのように処理するかを理解することは重要です。まず、すべての

データがRAMにバッファされます。このバッファは、カーネル更新デーモン(kupdated)によって監視されます。データが一定の寿命に達するか、バッファがある程度一杯になると、バッファの内容がハードディスクにフラッシュされます。バッファサイズはダイナミックであり、メモリサイズとシステム負荷に対応して変化します。デフォルトでは、kupdatedの間隔が短く設定されて、完全性を最大まで高めます。バッファが5秒毎にチェックされ、データが30秒以上経過していたり、バッファの使用レベルが30%に達すると、bdflushデーモンに通知されます。するとbdflushデーモンが、データをハードディスクに書き込みます。このデーモンはまた、たとえば、バッファが一杯のときに、kupdatedと無関係に書き込みます。

警告: データの完全性に関する障害

カーネル更新デーモンの設定を変更すると、データの完全性が損なわれる可能性があります。

これらのプロセスとは別に、ReiserFSやExt3などのジャーナリングファイルシステムは、それらが持つメタデータをbdflushとは無関係に書き込むので、ハードディスクが回転を停止しなくなります。モバイル機器では、これを避けるために特別なカーネル拡張が開発されています。詳細については、`/usr/src/linux/Documentation/laptop-mode.txt`を参照してください。

もう1つの重要な要因は、アクティブプログラムが動作する方法です。たとえば、優れたエディタは、変更中のファイルを定期的にハードディスクに自動バックアップし、これによってディスクがウェイクアップされます。データの完全性を犠牲にすれば、このような機能を無効にできます。

この接続では、メールデーモンpostfixが変数`POSTFIX_LAPTOP`を使用します。この変数を`yes`に設定すると、postfixがハードディスクにアクセスする頻度は大幅に減少します。しかしながら、kupdatedの間隔が広くなると、このことは重要でなくなります。

21.5 powersaveパッケージ

`powersave`パッケージは、ラップトップでバッテリ使用時に省電力機能をサポートします。この機能の一部はサスペンド、スタンバイ、ACPIボタン機能、およびIDEハードディスクをスリープ状態に切り替える場合など、通常のワークステーションやサーバでも有用です。

このパッケージにはご使用のコンピュータの電源管理機能がすべて含まれます。電源管理機能はACPI、APM、IDEハードディスク、PowerNow!またはSpeedStepテクノロジを使用してハードウェアをサポートします。apmd、acpid、ospmd、cpufreqd(現在はcpuspeed)などの各パッケージの機能がpowersaveパッケージに統合されています。これらのパッケージのデーモンをpowersaveデーモンと同時に実行することは避けてください。

ご使用のシステムに前述のハードウェア要素の一部が含まれていないとしても、省電力機能の制御にはpowersaveデーモンを使用してください。ACPIおよびAPMは相互排他的であるため、ご使用のシステムではこれらのシステムのどちらか一方しか使用できません。このデーモンはハードウェア構成に変更があった場合、これを自動的に検出します。

21.5.1 powersaveパッケージの設定

通常、powersaveの設定は複数のファイルに分散されています。

/etc/sysconfig/powersave/common
このファイルにはpowersaveデーモンの一般的な設定が含まれます。たとえば、エラーメッセージの量(/var/log/messages内の)は、変数POWERSAVE_DEBUGの値を増加させることで増やせます。

/etc/sysconfig/powersave/events
powersaveデーモンはシステムイベントを処理するためにこのファイルを必要とします。1つのイベントには外部アクションまたはデーモン自体が実行したアクションを割り当てることができます。外部アクションの場合、デーモンは/usr/lib/powersave/scripts/にある外部ファイルを実行しようとします。事前定義された内部アクションは次のとおりです。

- ignore
- throttle
- dethrottle
- suspend_to_disk
- suspend_to_ram

- standby
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby

throttleは、MAX_THROTTLINGで指定された値に従ってプロセッサの速度を遅くします。この値は現在のスキーマに依存します。dethrottleはプロセッサをフルパフォーマンスに設定します。suspend_to_disk、suspend_to_ram、およびstandbyはスリープモード用のシステムイベントを生成します。これら3つのアクションは一般的にスリープモードのトリガとなりますが、常に、これらを特定のシステムイベントと関連付けるようにしてください。

ディレクトリ/usr/lib/powersave/scriptsにはイベントを処理するための各種スクリプトが含まれます。

notify
コンソール、X Window、またはアコースティック(音による)シグナルのイベントに関する通知です。

screen_saver
スクリーンセーバを作動させます。

switch_vt
サスペンドやスタンバイの後に画面が戻らない場合に有用です。

wm_logout
設定を保存し、GNOME、KDE、または他のウィンドウマネージャからログアウトします。

wm_shutdown
GNOMEまたはKDEの設定を保存し、システムをシャットダウンします。

たとえば、変数
EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk"が設定されている場合、ユーザがスリープモード用のコマンドであるsuspend to diskをpowersavedに対して発行する

とすぐに、2つのスクリプトまたはアクションが指定された順番で処理されます。デーモンは外部スクリプトである/usr/lib/powersave/scripts/prepare_suspend_to_diskを実行します。このスクリプトが正常に実行されると、重要なモジュールがスクリプトによりアンロードされ、各種サービスが停止された後、デーモンが内部アクションであるdo_suspend_to_diskを実行し、コンピュータをスリープモードにします。

sleepボタンのイベントを処理するアクションはEVENT_BUTTON_SLEEP="notify suspend_to_disk"のように変更することができます。この場合、外部スクリプトnotifyがユーザにサスペンドを通知します。その結果、イベントEVENT_GLOBAL_SUSPEND2DISKが生成され、前述のアクションが実行されて、システムはサスペンドモードに入ります。スクリプトnotifyは/etc/sysconfig/powersave/commonにある変数NOTIFY_METHODを使用してカスタマイズできます。

/etc/sysconfig/powersave/cpufreq
動的CPU周波数の設定を最適化するための変数が含まれます。

/etc/sysconfig/powersave/battery
バッテリの制限とその他のバッテリ固有設定が含まれます。

/etc/sysconfig/powersave/sleep
このファイルでは、スリープモードを有効にし、サスペンドイベントまたはスタンバイイベントの前にアンロードすべき重要なモジュールと、停止すべき各種サービスを指定します。システムが再開されるとこれらのモジュールは再ロードされ、各種サービスも再開されます。また、ファイルを保存するなどのために、トリガされたスリープモードを遅らせることも可能です。デフォルト設定は主にUSBおよびPCMCIAモジュールに関係しています。サスペンドまたはスタンバイの障害は通常、ある一定のモジュールによって発生します。エラーの特定の詳細については項21.5.4.「トラブルシューティング」 (page 305)を参照してください。

/etc/sysconfig/powersave/thermal
冷却コントロールおよびサーマルコントロールを有効にします。このテーマの詳細については、ファイル/usr/share/doc/packages/powersave/README.thermalを参照してください。

/etc/sysconfig/powersave/scheme_*
これらは特定の導入シナリオに応じて消費電力を最適化するさまざまなスキーマです。多くのスキーマが事前に設定され、そのまま使用できます。また、カスタムスクリプトをここに保存することもできます。

21.5.2 APMおよびACPIの設定

サスペンドおよびスタンバイ

デフォルトではスリープモードは無効になっています。これはスリープモードが一部のコンピュータではまだ機能しないためです。次に示すように、3種類の基本ACPIスリープモードおよび2種類のAPMスリープモードがあります。

サスペンド(ディスク)(ACPI S4、APMサスペンド)
メモリの内容全部をハードディスクに保存します。コンピュータは完全に電源オフの状態になり、電力は消費されません。

サスペンド(RAM)(ACPI S3、APMサスペンド)
デバイス全体の状態をメインメモリに保存します。メインメモリ以外からの電力消費はありません。

スタンバイ(ACPI S1、APMスタンバイ)
一部のデバイスの電源をオフにします(メーカにより異なる)。

サスペンド、スタンバイ、再開を正しく処理するため、ファイル/etc/sysconfig/powersave/eventsで次のデフォルトオプションが設定されていることを確認してください(SUSE Linuxインストール時のデフォルト設定)。

```
EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk do_suspend_to_disk"
EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
    "prepare_standby do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

バッテリ状態のカスタマイズ

ファイル /etc /sysconfig /powersave /batteryで3通りのバッテリ充電レベル(パーセント指定)を定義します。バッテリの充電量がこれらのレベルに達すると、システムアラートが生成されたり、特定のアクションが実行されたりします。

```
BATTERY_WARNING=20
BATTERY_LOW=10
BATTERY_CRITICAL=5
```

充電レベルが指定された制限値を下回った場合に実行されるアクションまたはスクリプトは、設定ファイル /etc /sysconfig /powersave /eventsに定義されています。各種ボタンの標準アクションは項21.5.1.「powersaveパッケージの設定」 (page 300)に示されているように変更できます。

```
EVENT_BATTERY_NORMAL="ignore"
EVENT_BATTERY_WARNING="notify"
EVENT_BATTERY_LOW="notify"
EVENT_BATTERY_CRITICAL="wm_shutdown"
```

さまざまな条件に応じた電力消費の最適化

システムの動作は電源のタイプによって調整することができます。システムがAC電源を使用せずバッテリで稼動している場合は、システムの電力消費を抑えねばなりません。また、システムがAC電源に接続された場合はすぐ、自動的にパフォーマンスを上げる必要があります。このように、CPUの周波数、IDEの省電力機能、他のさまざまなパラメータを変更することができます。

コンピュータがAC電源に接続されている場合、またはされていない場合に実行される各種アクションは、 /etc /sysconfig /powersave /eventsで定義されています。以下で /etc /sysconfig /powersave /commonで使用するスキーマを選択します。

```
AC_SCHEME="performance"
BATTERY_SCHEME="powersave"
```

各スキーマは /etc /sysconfig /powersaveにあるファイルに保存されています。ファイル名はscheme_name-of-the-schemeという形式になっています。次に2つのスキーマを例としてあげます。scheme_performanceおよびscheme_powersaveには、performance、powersave、presentation、およびacousticが事前定義されています。項21.6.「YaST電源管理モジュー

ル」 (page 308)で説明されている、YaSTの電源管理モジュールを使用して、既存のスキーマの編集、作成、削除、別の電源状態との関連付けを行うことができます。

21.5.3 その他のACPI機能

ACPIを使用している場合、*ACPI*ボタン(電源、スリープ、ラップトップを開く、ラップトップを閉じる)に対するシステム応答を制御することができます。 `/etc/sysconfig/powersave/events`でアクションの実行を設定します。個別のオプションについての説明はこの設定ファイルを参照してください。

EVENT_BUTTON_POWER="wm_shutdown"
電源ボタンが押されると、システムは応答して該当するウィンドウマネージャ(KDE、GNOME、fvwmなど)を閉じます。

EVENT_BUTTON_SLEEP="suspend_to_disk"
スリープボタンが押されると、システムはsuspend-to-diskモードに設定されます。

EVENT_BUTTON_LID_OPEN="ignore"
ラップトップのふたが開いている状態でアクションは発生しません。

EVENT_BUTTON_LID_CLOSED="screen_saver"
ラップトップが閉じられると、スクリーンセーバが有効になります。

指定した時間内に、CPUの負荷が指定した制限を越えない場合、さらにCPUのパフォーマンスを低下させることも可能です。負荷制限値を`PROCESSOR_IDLE_LIMIT`に、タイムアウトを`CPU_IDLE_TIMEOUT`に指定します。CPUの負荷が制限値を越えない状態が、タイムアウトで指定した時間よりも長く続いた場合には、`EVENT_PROCESSOR_IDLE`で設定されたイベントが有効になります。CPUが再びビジーになると、`EVENT_PROCESSOR_BUSY`が実行されます。

21.5.4 トラブルシューティング

すべてのエラーメッセージおよびアラートはファイル`/var/log/messages`に記録されます。必要な情報が得られない場合、ファイル`/etc/sysconfig/`

powersave/commonにある、DEBUGを使用してpowersaveに関連するメッセージの冗長度を上げます。変数の値を7または15まで増やし、デーモンを再起動します。/var/log/messagesで利用可能なより詳しいエラーメッセージは、エラーの発見に役立ちます。以下のセクションではpowersaveで最も頻繁に起こる問題について解説します。

ACPIはハードウェアサポートで有効になっていますが、各機能を使用できません。

ACPIで問題が発生した場合は、コマンドdmesg| grep -i acpiを使用し、dmesgの出力からACPI固有のメッセージを検索します。問題を解決するためにBIOSのアップデートが必要になる場合があります。ラップトップメーカのホームページにアクセスし、BIOSの更新バージョンを検索してインストールします。メーカに最新のACPI仕様に準拠していることを確認してください。BIOSの更新後もエラーが継続する場合は、以下の手順に従い、BIOS内で問題が発生しているDSDTテーブルを更新されたDSDTに置き換えます。

1. http://acpi.sourceforge.net/dsdt/tablesからシステムに適したDSDTをダウンロードします。以下に示すようにファイルを解凍し、コンパイル後ファイル拡張子が.aml (ACPI machine language)になっていることを確認します。拡張子が.amlの場合はステップ3に進みます。

2. ダウンロードしたテーブルのファイル拡張子が.asl (ACPI source language)である場合は、iasl (pmtoolsパッケージ)でコンパイルします。コマンドiasl -sa file.aslを入力してください。iasl (Intel ACPIコンパイラ)の最新バージョンは、http://developer.intel.com/technology/iapc/acpi/downloads.htmで入手できます。

3. ファイルDSDT.amlをいずれかのロケーション(/etc/DSDT.amlが推奨されています)にコピーします。/etc/sysconfig/kernelを編集し、DSDTファイルに応じてパスを変更します。mkinitrd(mkinitrdパッケージ)を開始します。カーネルをアンインストールし、mkinitrdを使用してinitrdを作成する場合は常に、変更されたDSDTが組み込まれ、システムブート時にロードされます。

CPU周波数調節が機能しません。

カーネルソース(kernel-source)を参照して、ご使用のプロセッサがサポートされているか確認してください。CPU周波数制御を有効にするには特別なカーネルモジュールまたはモジュールオプションが必要になる場合があります。この情報については/usr/src/linux/Documentation/cpu-freq/*を参照してください。特別なモジュールまたはモジュールオプションが必要な場合その設定は、ファイル/etc/sysconfig/powersave/cpufreqにある変数CPUFREQD_MODULEおよびCPUFREQD_MODULE_OPTSで行います。

サスペンドとスタンバイが機能しません。

ACPIシステムにはサスペンドおよびスタンバイの不具合の原因になる、カーネル関連の問題が複数報告されています。以下を参照してください。

- 現在、RAMが1GB以上のシステムでは、サスペンドはサポートされていません。
- 現在、マルチプロセッサシステムおよびP4プロセッサ(ハイパースレッディング搭載)では、サスペンドはサポートされていません。

エラーメッセージはDSDTの実装(BIOS)の不具合が原因である可能性もあります。この場合、新しいDSDTをインストールします。

ACPIおよびAPMシステムの場合:システムが不具合のあるモジュールをアンロードしようとすると、システムは停止するか、またはサスペンドイベントがトリガされません。また、サスペンドに入らない原因となるモジュールをアンロードしない、またはそうしたサービスを停止しない場合、同様の状態に陥る可能性があります。どちらの場合でも、スリープモードに入らない原因となっている障害モジュールを識別してください。このモジュールの判別には/var/log/sleep modeにあるpowersaveによって生成されたログファイルが大変有用です。コンピュータがスリープモードにならない場合、その原因は最後にアンロードされたモジュールに関係しています。/etc/sysconfig/powersave/sleepにある以下の設定を変更し、サスペンドまたはスタンバイがトリガされる前に問題のあるモジュールをアンロードします。

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
```

```
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES=""
```

SambaやNISといったネットワーク環境の変更時、またはリモートでマウントされたファイルシステムとの接続時にサスペンドまたはスタンバイを使用する場合、オートマウンタを使用してそれらをマウントするか、それぞれのサービスを追加するようにします。たとえば、前述の変数では、`smbfs`または`nfs`などが該当します。サスペンドまたはスタンバイの前に、アプリケーションがリモートでマウントされたファイルシステムにアクセスすると、このサービスは正常に停止されません。このためファイルシステムを正常にアンマウントすることができなくなります。このようなことが原因で、システムを再開した後、ファイルシステムに障害が発生したり、再マウントが必要になったりする場合があります。

ACPIを使用した場合、Powersaveがバッテリレベルの低下を識別しません。

ACPIを使用する場合、オペレーティングシステムはBIOSに対し、バッテリの充電レベルが一定の基準を下回った場合にメッセージを送信するよう要求できます。バッテリを定期的に確認することはコンピュータのパフォーマンス低下につながる恐れがあります。このメソッドの利点はその必要がないことです。ただし、充電レベルが指定値を下回った場合、BIOSがこの機能をサポートしているのにもかかわらず、通知されない場合があります。この現象がご使用のシステムで発生する場合は、ファイル`/etc/sysconfig/powersave/battery`にある変数`POWERSAVED_FORCE_BATTERY_POLLING`の値を`yes`に設定し、バッテリの確認を強制的に行うようにします。

21.5.5 関連資料

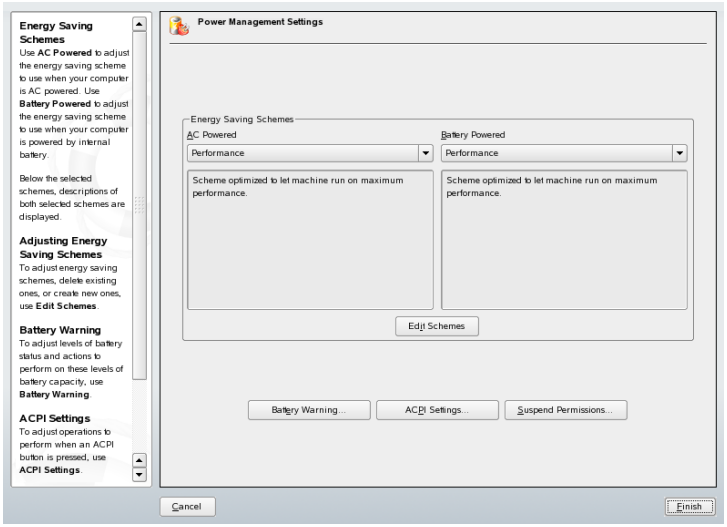
powersaveパッケージは`/usr/share/doc/packages/powersave`でも利用できます。

21.6 YaST電源管理モジュール

YaST電源管理モジュールではこれまで解説してきたすべての電源管理を設定できます。YaSTコントロールセンターから*[システム]*→*[電源管理]*でモジュー

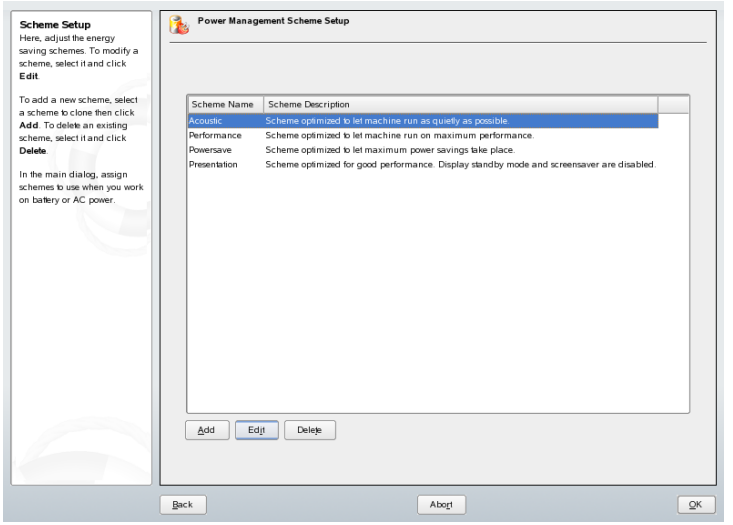
ルを開始すると、モジュールの最初のダイアログが開きます。このツールを図 21.1. 「スキーマの選択」 (page 309)に示します。

図 21.1　スキーマの選択



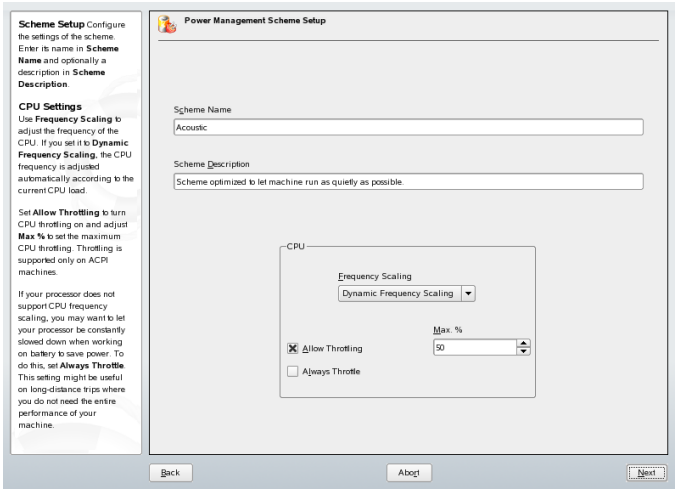
このダイアログでバッテリ使用時およびAC電源使用時に適用するスキーマを選択します。スキーマを追加、または変更するには［スキーマ*編集*］をクリックします。これにより、既存のスキーマの概要が表示されます。図 21.2. 「既存のスキーマの概要」 (page 310)を参照してください。

図 21.2　既存のスキーマの概要



スキーマの概要で変更するスキーマを選択し、［*編集*］をクリックします。新しいスキーマを追加するには、[*追加*]をクリックします。どちらを使用した場合でも、図 21.3.「スキーマの設定」 (page 310)に示す同じダイアログが表示されます。

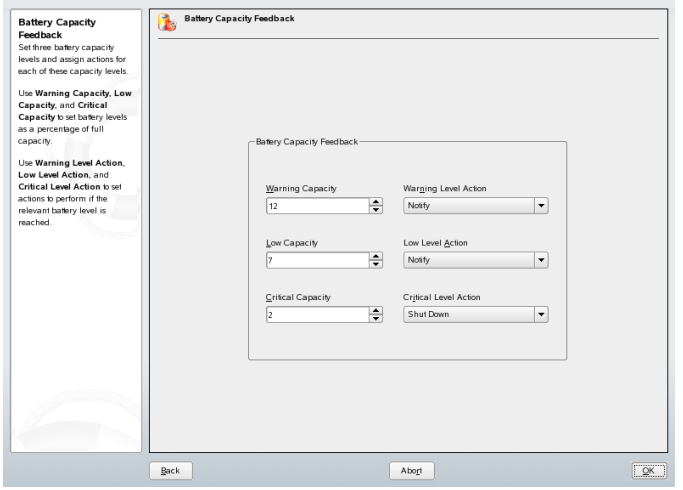
図 21.3　スキーマの設定



まず初めに、新規または編集するスキーマに適切な名前と説明を指定します。このスキーマを使用した場合、CPUパフォーマンスを制御するか、さらにどのように制御するかを決定します。また、周波数の調整およびスロットル(減速)の使用の有無、およびその使用範囲を指定します。続くダイアログはハードディスクの設定です。ここでは最大パフォーマンス使用時または省電力時の［*スタンバイポリシー*］を定義します。［*音のポリシー*］ではハードディスクのノイズレベルを制御します(ハードディスクによってはサポートされていません)。［*冷却ポリシー*］は使用する冷却メソッドを決定します。残念ながら、このタイプの温度制御をサポートしているBIOSはほとんどありません。`/usr/share/doc/packages/powersave/README.thermal`で、ファンおよびパッシブ冷却メソッドの使用方法を参照してください。

また、最初のダイアログの［*バッテリ警告*］、［*ACPIの設定*］、または［*サスペンドを有効化*］を使用して、全体的な電源管理設定を行うことも可能です。［*バッテリ警告*］をクリックし、図21.4.「バッテリ充電レベル」 (page 311)に示す、バッテリ充電レベルのダイアログを開きます。

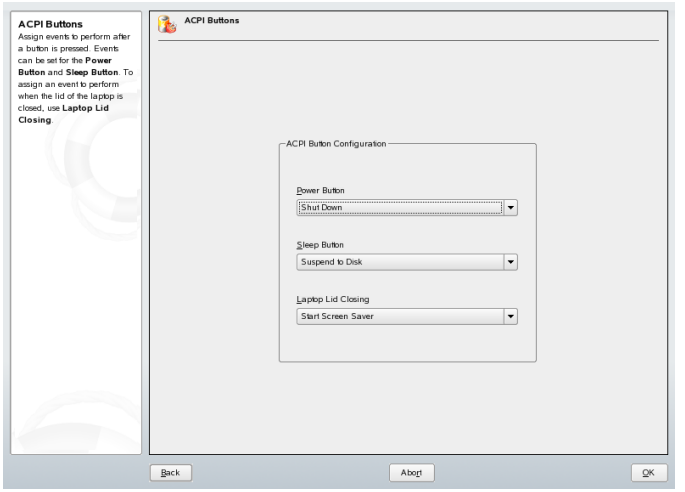
図 21.4 *バッテリ充電レベル*



充電レベルが一定の基準値を下回った段階で、システムのBIOSはオペレーティングシステムに通知します。このダイアログでは、［*警告容量*］、［*低容量*］、および［*致命的容量*］の3つの基準値を定義します。充電レベルがこれらの基準値を下回ると特定のアクションがトリガされます。通常、初めの2つの状態ではユーザへの通知がトリガされるのみです。3つめの致命的なレベル

ではシャットダウンをトリガします。これは残りの電力ではシステムのオペレーションを維持することが困難であるためです。適切な充電レベルとそれに応じて実行するアクションを選択し、［*了解*］をクリックして開始ダイアログに戻ります。

図 21.5 *ACPIの設定*



［*ACPIの設定*］を使用してACPIボタンを設定するダイアログを開きます。このツールを図 21.5.「ACPIの設定」 (page 312)に示します。ACPIボタンの設定は特定のスイッチに対するシステムの応答を決定します。電源ボタンが押された場合、スリープボタンが押された場合、ラップトップが閉じられた場合のそれぞれに応じて、システムがどのように応答するかを設定します。［*了解*］をクリックして設定を終了し、開始ダイアログに戻ります。

［*サスペンドを有効化*］ダイアログを開きます。このダイアログではこのシステムのユーザがサスペンドまたはスタンバイ機能を使用できるか、さらにそれらをどのように使用するかを決定します。［*了解*］をクリックしてメインダイアログに戻ります。［*了解*］を再度クリックしてモジュールを終了し、電源管理設定を確認してください。

22 無線通信

Linuxシステムを使用して他のコンピュータ、携帯電話、または周辺デバイスと通信するには、いくつかの方法があります。WLAN (無線LAN)は、ラップトップをネットワーク化するために使用できます。Bluetoothを使用すると、個々のシステムコンポーネント(マウス、キーボード)、周辺デバイス、携帯電話、PDA、および個々のコンピュータを互いに接続できます。PDAまたは携帯電話との通信には、IrDAがよく使用されます。この章では、3つのテクノロジとその設定のすべてを紹介します。

22.1 無線LAN

無線LANは、モバイルコンピューティングに不可欠な側面となってきています。現在、ほとんどのラップトップにはWLANカードが内蔵されています。WLANカードによる無線通信に関する802.11規格がIEEEにより策定されました。当初、この規格は最大伝送速度2MBit/sについて提供されましたが、その後、データ伝送速度を高めるために複数の補足事項が追加されています。これらの補足事項では、モジュレーション、伝送出力、および伝送速度などの詳細が定義されています。

表 22.1　各種WLAN規格の概要

名称	帯域(GHz)	最大伝送速度 (MBit/s)	注
802.11	2.4	2	廃止、実質上、使用可能なエンドデバイスはなし
802.11b	2.4	11	普及
802.11a	5	54	あまり普及せず
802.11g	2.4	54	11bとの下位互換性あり

また、最大伝送速度22MBit/sのTexas Instrumentsの802.11bバージョン(802.11b+)のような独自規格もあります。ただし、この規格を使用するカードは一般的ではありません。

22.1.1　ハードウェア

802.11カードは、SUSE Linuxではサポートされていません。802.11a、802.11b、および802.11gを使用するカードのほとんどは、サポートされています。通常、新しいカードは802.11g規格に準拠していますが、802.11bを使用するカードも使用可能です。一般に、次のチップを内蔵したカードがサポートされています。

- Aironet 4500, 4800
- Atheros 5210、5211、5212
- Atmel at76c502、at76c503、at76c504、at76c506
- Intel PRO/Wireless 2100、2200BG、2915ABG
- Intersil Prism2/2.5/3
- Intersil PrismGT
- Lucent/Agere Hermes

- Ralink RT2400, RT2500
- Texas Instruments ACX100、 ACX111
- ZyDAS zd1201

普及していたが廃止になった古いカードも、多数サポートされています。WLAN カードと使用チップについての詳細なリストは、http://www.linux-wlan.org/docs/wlan_adapters.html.gzにある*AbsoluteValue Systems*のWebサイトを参照してください。http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatzは、各種WLANチップの概要を提供しています。

一部のカードの場合は、ドライバの初期化時にファームウェアイメージをカードにロードする必要があります。Intersil PrismGT、Atmel、TI ACX100およびACX111がその例です。ファームウェアは、YaSTオンラインアップデートを使用して簡単にインストールできます。Intel PRO/Wirelessカード用のファームウェアはSUSE Linuxに内蔵されており、この種のカードが検出されるとただちに、YaSTによって自動的にインストールされます。このトピックに関する詳細は、インストール済みシステムの/usr/share/doc/packages/wireless-tools/README.firmwareを参照してください。

ネイティブLinuxサポートのないカードは、ndiswrapperアプリケーションを実行すれば使用できます。ndiswrapperは、ほとんどのWLANカードに同梱されるWindowsドライバを使用します。ndiswrapperについては、/usr/share/doc/packages/ndiswrapper/README.SUSEを参照してください(ただしndiswrapperがインストールされている場合)。ndiswrapperについての詳細は、プロジェクトのWebサイトhttp://ndiswrapper.sourceforge.net/support.htmlを参照してください。

22.1.2 機能

無線ネットワークでは、高速で高品質、そして安全な接続を確保するために、さまざまなテクニックや設定が使用されています。動作のタイプが違えば、それに適したセットアップ方式も異なります。適切な認証方式を選択するのは難しいことがあります。利用可能な暗号化方式には、それぞれ異なる利点と欠点があります。

動作モード

基本的に、無線ネットワークは管理ネットワークとAd-hocネットワークに分類できます。管理ネットワークには管理用の要素であるアクセスポイントがあります。このモード(インフラストラクチャモードとも呼ばれます)では、ネットワーク内のWLAN局の接続はすべてアクセスポイント経由で行われ、イーサネットへの接続としても機能できます。Ad-hocネットワークには、アクセスポイントはありません。局は相互に直接通信します。Ad-hocネットワークの場合は、伝送範囲と参加局の数が大幅に制限されます。そのため、通常はアクセスポイントを使用する方が効率的です。また、WLANカードをアクセスポイントとして使用することも可能です。ほとんどのカードは、この機能をサポートしています。

有線ネットワークよりも無線ネットワークの方がはるかに盗聴や侵入が容易なので、各種の規格には認証方式と暗号化方式が含まれています。IEEE 802.11規格のオリジナルバージョンでは、これらがWEPという用語で説明されています。ただし、WEPは安全でないことが判明したので(セキュリティ項 (page 322))、WLAN業界(*Wi-Fi Alliance*という団体名で協力)はWPAという新規の拡張機能を定義しており、これによりWEPの弱点がなくなるものと思われます。その後のIEEE 802.11i規格には、WPAと他の認証方式および暗号化方式が含まれています(WPAはドラフトバージョンの802.11iに基づいているので、この規格はWPA2と呼ばれることもあります)。

認証

認可された局だけが接続できるように、管理ネットワークでは各種の認証メカニズムが使用されます。

オープン

オープンシステムとは、認証を必要としないシステムです。任意の局がネットワークに参加できます。ただし、WEP暗号化(暗号化項 (page 318)を参照)は使用できます。

共有キー(IEEE 802.11に準拠)

この方式では、認証にWEPキーが使用されます。ただし、WEPキーが攻撃にさらされやすくなるので、この方式はお勧めしません。攻撃者は、局とアクセスポイント間の通信を長時間リスニングするだけで、WEPキーを奪取できます。認証処理中には、通信の両側が1度は暗号化形式、1度は暗号化されていない形式で同じ情報を交換します。そのため、適当なツールを

使えば、キーを再構成することが可能です。この方式では認証と暗号化にWEPキーを使用するので、ネットワークのセキュリティは強化されません。適切なWEPキーを持っている局は、認証、暗号化および復号化を行うことができます。キーを持たない局は、受信したパケットを復号化できません。したがって、自己認証を行ったかどうかに関係なく、通信を行うことができません。

WPA-PSK (IEEE 802.1xに準拠)

WPA-PSK (PSKはpreshared keyの略)の機能は、共有キー方式と同様です。すべての参加局とアクセスポイントは、同じキーを必要とします。キーの長さは256ビットで、通常はパスフレーズとして入力されます。この方式では、WPA-EAPのような複雑なキー管理を必要とせず、個人で使用するのに適しています。したがって、WPA-PSKはWPA 「Home」とも呼ばれます。

WPA-EAP (IEEE 802.1xに準拠)

実際には、WPA-EAPは認証システムではなく、認証情報を転送するためのプロトコルです。WPA-EAPは、企業内の無線ネットワークを保護するために使用されます。プライベートネットワークでは、ほとんど使用されていません。このため、WPA-EAPはWPA 「Enterprise」とも呼ばれます。

WPA-EAPは、ユーザを認証するのにRadiusサーバを必要とします。EAPは、サーバに接続して認証するために、TLS (Transport Layer Security)、TTLS (Tunneled Transport Layer Security)、およびPEAP (Protected Extensible Authentication Protocol)という、3通りの方式を提供しています。簡単に説明すると、これらのオプションは以下のように働きます。

EAP-TLS

TLSの認証は、サーバとクライアント両方の、証明書の相互交換に依存しています。まず、サーバがクライアントに対して証明書を提示し、それが評価されます。証明書が有効であるとみなされた場合には、今度がクライアントがサーバに対して証明書を提示します。TLSはセキュアですが、ネットワーク内で証明書管理のインフラストラクチャを運用することが必要になります。このインフラストラクチャは、プライベートネットワークでは通常存在しません。

EAP-TTLSとPEAP

TTLSとPEAPは両方とも、2段階からなるプロトコルです。最初の段階ではセキュリティが確立され、2番目の段階ではクライアントの認証

データが交換されます。これらの証明書管理のオーバヘッドは、もしあるとしても、TLSよりずっと小さいものです。

暗号化

権限のないユーザが無線ネットワークで交換されるデータパケットを読み込んだりネットワークにアクセスしたりできないように、さまざまな暗号化方式が存在しています。

WEP (IEEE 802.11で定義)
この規格では、RC4暗号化アルゴリズムを使用します。当初のキー長は40ビットでしたが、その後104ビットも使用されています。通常、初期化ベクタの24ビットを含めるものとして、長さは64ビットまたは128ビットとして宣言されます。ただし、この規格には一部弱点があります。このシステムで生成されたキーに対する攻撃が成功する場合があります。それでも、ネットワークをまったく暗号化しないよりはWEPを使用する方が適切です。

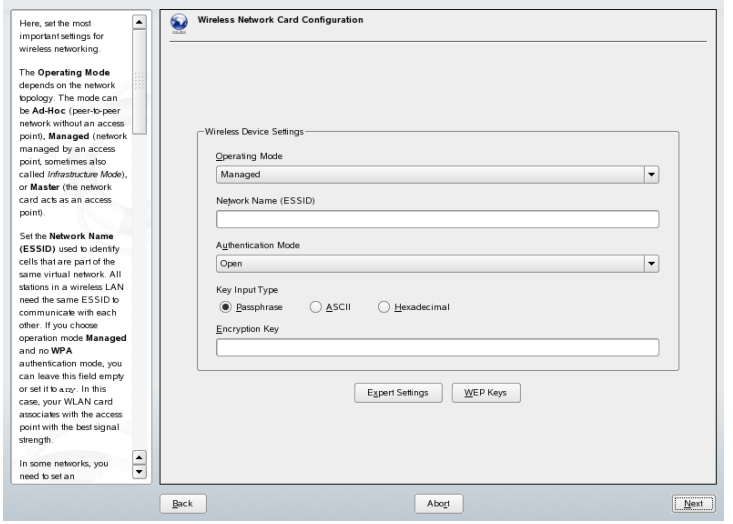
TKIP (WPA/IEEE 802.11iで定義)
このキー管理プロトコルはWPA規格で定義されており、WEPと同じ暗号化アルゴリズムを使用しますが、弱点は排除されています。データパケットごとに新しいキーが生成されるので、これらのキーに対する攻撃は無駄になります。TKIPはWPA-PSKと併用されます。

CCMP (IEEE 802.11iで定義)
CCMPは、キー管理を記述したものです。通常は、WPA-EAPに関連して使用されますが、WPA-PSKとも併用できます。暗号化はAESに従って行われ、WEP規格のRC4暗号化よりも厳密です。

22.1.3 YaSTでの設定

無線ネットワークカードを設定するには、YaSTの［ネットワーク・カード］モジュールを起動します。［ネットワークアドレスの設定］で、デバイスタイプ［無線］を選択して［次へ］をクリックします。[無線ネットワークカードの設定] で (図 22.1. 「YaST:: 無線ネットワークカードの設定」 (page 319)を参照)、WLAN 操作の基本設定を行います。

図 22.1　YaST:: 無線ネットワークカードの設定



動作モード
: WLANでは、局を3つのモードで統合できます。適切なモードは、通信に使用するネットワークに応じて異なります。選択肢は、［*Ad-hoc*］(アクセスポイントなしのpeer-to-peerネットワーク)、［*Managed*］(アクセスポイントで管理されているネットワーク)、または［*Master*］(ネットワークカードをアクセスポイントとして使用)です。WPA-PSKまたはWPA-EAPモードを使用するには、動作モードを［*Managed*］に設定する必要があります。

ネットワーク名(ESSID)
: 無線ネットワークのすべての局が相互に通信するには、同じESSIDが必要です。何も指定しなければ、カードは自動的にアクセスポイントを選択しますが、それが意図したアクセスポイントとは異なる場合があります。

認証モード
: ネットワークに合った認証方式を選択します。選択できるものは［*Open*］、［*Shared Key*］、［*WPA-PSK*］、または［*WPA-EAP*］です。WPA認証を選択した場合は、ネットワーク名を設定する必要があります。

エキスパート設定
: このボタンをクリックすると、WLAN接続の詳細設定用ダイアログが開きます。このダイアログの詳細については後述します。

基本設定を完了すると、自局がWLANで運用可能になります。

重要項目: 無線ネットワークでのセキュリティ

ネットワークトラフィックを保護するために、サポートされている認証方式と暗号化方式の1つを必ず使用してください。暗号化されていないWLAN接続では、第三者がすべてのネットワークデータを盗聴することができます。弱い暗号化(WEP)でも、まったく暗号化しないよりはましです。詳細については、暗号化項 (page 318)とセキュリティ項 (page 322)を参照してください。

選択した認証方式によっては、の別のダイアログで設定を微調整するように要求されます。［*オープン*］を選択した場合、何も設定項目はありません。この設定では、認証なしの暗号化されない動作が実装されるからです。

キーの入力タイプ

キーの入力タイプを設定します。［*パスフレーズ][ASCII*］、［*16進*］のいずれかを選択します。最大4つの異なるキーを使用して伝送データを暗号化できます。［*複数のキー*］をクリックしてキー設定ダイアログを開きます。キーの長さを選択します。選択できるのは、［*128ビット*］または［*64ビット*］です。デフォルト設定は、［*128ビット*］ビットです。ダイアログ下部にあるリスト領域では、局で暗号化に使用するキーを最大4つまで指定できます。［*デフォルト設定とする*］を押して、4つのうち1つをデフォルトキーとして定義します。この方法で変更しない限り、YaSTでは最初に入力したキーがデフォルトキーとして使用されます。標準キーが削除された場合は、残りのキーの1つを手動でデフォルトキーに設定する必要があります。［*編集*］ をクリックし、既存のリストエントリを変更するか、新規のキーを作成します。新規作成の場合、ポップアップウィンドウが表示され、キーの入力タイプ(［パスフレーズ］、［*ASCII*］、または［*16進*］)を選択する必要があります。［*パスフレーズ*］ を選択した場合は、前に指定した長さに従ってキーの生成に使用するワードまたは文字列を入力します。［*ASCII*］を選択した場合は、64ビットキーであれば5文字、128ビットキーであれば13文字を入力する必要があります。［*Hexadecimal*］を選択した場合は、64ビットキーであれば10文字、128ビットキーであれば26文字を16進表記で入力します。

WPA-PSK

WPA-PSK用のキーを入力するには、入力方法として［パスフレーズ］または［*16進*］を選択します。［*Passphrase*］モードでは、8から63文字を入

力する必要があります。［*Hexadecimal*］モードでは、64文字を入力します。

WPA-EAP
ネットワーク管理者から受け取った証明書を設定します。TLSの場合、［*Client Certificate*］および［*Server Certificate*］を設定します。TTLSとPEAPでは、［*Identity*］と［*Password*］が必要です。［*Server Certificate*］はオプションです。YaSTは、`/etc/cert`で証明書を探すので、受け取った証明書はこの場所に保存し、これらのファイルに対するアクセス権は`0600`(所有者の読み取りと書き込み)に制限してください。

［エキスパート設定］をクリックしてWLAN接続の基本設定ダイアログを終了し、上級者用の設定に入ります。このダイアログでは、次のオプションを使用できます。

チャンネル
WLAN局が使用するチャンネルの指定を必要とするのは、［*Ad-hoc*］モードと［マスタ］モードだけです。［*管理*］モードでは、カードはアクセスポイントに使用可能なチャネルを自動的に検索します。［*Ad-hoc*］モードでは、自局と他局との通信用に提供されている12のチャンネルから1つを選択します。［マスタ］モードでは、使用するカードがアクセスポイント機能を提供する必要のあるチャネルを指定します。このオプションのデフォルト設定は［*自動*］です。

転送ビットレート
ネットワークのパフォーマンスに応じて、あるポイントから別のポイントへの伝送について特定のビットレートを設定できます。デフォルト設定の［*自動*］では、システムは最大許容データ伝送速度を使用しようとします。ビットレートの設定をサポートしていないWLANカードもあります。

アクセスポイント
複数のアクセスポイントがある環境では、MACアドレスを指定することで、その1つを事前に選択できます。

電源管理を使用
外出先では、省電力テクノロジを使用してバッテリの動作時間を最長にします。電源管理の詳細については、章 21. *電源管理* (page 287)を参照してください。

22.1.4 ユーティリティ

WLANカードをアクセスポイントとして使用するには、hostap (`hostap`パッケージ)を使用します。このパッケージの詳細については、プロジェクトのホームページ(`http://hostap.epitest.fi/`)を参照してください。

kismet (`kismet`パッケージ)は、WLANパケットトラフィックのリスニングに使用するネットワーク診断ツールです。このツールを使用すると、ネットワーク内の侵入試行も検出できます。詳細については、`http://www.kismetwireless.net/`とマニュアルページを参照してください。

22.1.5 WLANのセットアップに関するヒントとテクニック

これらのヒントでは、速度と安定性を微調整する方法や、WLANのセキュリティの側面について説明します。

安定性と速度

無線ネットワークのパフォーマンスと信頼性は、主として参加局が他局からクリーンな信号を受信するかどうかに依存します。壁などの障害物があると、信号が大幅に弱くなります。信号強度が低下するほど、伝送速度も低下します。操作中には、コマンドライン(`Link Quality`フィールド)でiwconfigユーティリティを使用するか、またはKDEでkwifimanagerを使用して、信号強度をチェックします。信号品質に問題がある場合は、他の場所でデバイスをセットアップするか、またはアクセスポイントのアンテナ位置を調整してください。多くのPCMCIA WLANカードの場合、受信品質を実質的に向上させる補助アンテナを利用できます。メーカ指定のレート(54MBit/sなど)は、理論上の上限を表す公称値です。実際の最大データスループットは、この値の半分以下です。

セキュリティ

無線ネットワークをセットアップする際には、セキュリティ対策を導入しなければ、伝送範囲内の誰もが簡単にアクセスできることを忘れないでください。したがって、必ず暗号化方式をアクティブにする必要があります。すべ

てのWLANカードとアクセスポイントが、WEP暗号化をサポートしています。これでも完全に安全とは言えませんが、潜在的な攻撃者に対する障害物は存在することになります。通常、プライベート用であればWEPで十分です。WPA-PSKも適していますが、WLAN機能を持つ古いアクセスポイントやルータには実装されていません。デバイスによっては、ファームウェア更新を使用してWPAを実装できます。さらに、Linuxは、すべてのハードウェアコンポーネントでWPAをサポートしているわけではありません。このマニュアルの制作時点では、WPAが機能するのは、Atheros、Intel PRO/Wireless、またはPrism2/2.5/3チップを使用するカードの場合だけです。Prism2/2.5/3の場合、WAPが機能するのはhostapドライバを使用している場合だけです(Prism2カードの問題項 (page 323)を参照)。WPAが使用できない場合、暗号化しないよりはWEPを使用することをお勧めします。高度なセキュリティ要件を持つ企業では、無線ネットワークの運用にWPAを使用する必要があります。

22.1.6 トラブルシューティング

WLANカードが応答しない場合は、必須ファームウェアをダウンロードしたかどうかを確認します。詳細については、項22.1.1.「ハードウェア」 (page 314)を参照してください。ここでは、判明している一部の問題について説明します。

複数のネットワークデバイス

最新のラップトップでは、通常ネットワークカードとWLANカードが装備されています。両端のデバイスをDHCP(自動アドレス割り当て)で設定している場合は、名前解決およびデフォルトゲートウェイで問題が発生する可能性があります。これは、ルータはpingできるがインターネット上でナビゲーションできないことを示しています。詳細については、`http://portal.suse.com`にあるSupport Databas(サポートデータベース)を参照してください。この記事を検索するには、検索ダイアログに「DHCP」と入力します。

Prism2カードの問題

Prism2チップ搭載のデバイスには、複数のドライバが用意されています。各種カードがスムーズに動作するかどうかは、ドライバに応じて異なります。この種のカードの場合、WPAに使用できるのはhostapドライバだけです。この種のカードが正常に動作しない場合、まったく動作しない場合、またはWPA

を使用する必要がある場合は、/usr/share/doc/packages/wireless-tools/README.prism2を参照してください。

WPA

WPAのサポートは、SUSE Linuxでも非常に新しいことで、まだ発展途上にあります。そのため、YaSTはすべてのWPA認証方式の設定をサポートしているわけではありません。また、すべてのワイヤレスLANカードやドライバがWPAをサポートしているわけでもありません。カードの中には、WPAを有効にするためにファームウェアのアップデートを必要とするものがあります。WPAを使用する場合は、/usr/share/doc/packages/wireless-tools/README.wpaを参照してください。

22.1.7 関連資料

Linux用の*無線ツール*を開発したJean Tourrilhesのインターネットページには、無線ネットワークに関して役立つ情報が多数提供されています。http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.htmlを参照してください。

22.2 Bluetooth

Bluetoothは、各種デバイス(携帯電話、PDA、周辺装置、ラップトップなど)やシステムコンポーネント(キーボードやマウスなど)の接続に使用される無線テクノロジです。このテクノロジ名は、スカンジナビア紛争でさまざまな対立党派を統一したデンマーク王Harold Bluetoothに由来しています。Bluetoothのロゴは、「H」(星型)と「B」を表すルーン文字に基づいています。

BruetoothをIrDAと比較すると、さまざまな側面に重要な違いがあります。まず初めに個々のデバイスが相互を直接「認識」する必要がなく、次に複数のデバイスをネットワーク上で接続することができます。ただし、最大データ転送速度は720Kbps (現行バージョン1.2の場合)です。理論上、Bluethoothは壁を隔てた通信が可能です。ただし、実際には壁の性質やデバイスクラスに依存します。10mから100mの通信範囲に、3つのデバイスクラスがあります。

22.2.1 基本事項

ここではBluetoothの機能に関する基本原則一般について概説します。必要なソフトウェア要件、Bluetoothによるシステムとの対話方法、Bluetoothプロファイルの機能などについて説明します。

ソフトウェア

Bluetoothを使用するためには、Bluetoothアダプタ(内蔵アダプタまたは外部デバイス)、ドライバ、およびBluetoothプロトコルスタックが必要です。Linuxカーネルには、すでにBluetooth用の基本ドライバが組み込まれています。Bluezシステムがプロトコルスタックとして使用されます。アプリケーションをBluetoothと確実に機能させるためには、基本パッケージ`bluez-libs`および`bluez-utils`をインストールする必要があります。この2つのパッケージには、必須サービスとユーティリティが多数用意されています。また、BroadcomやAVM BlueFritz!など、`bluez-firmware`パッケージのインストールを必要とするアダプタもあります。`bluez-cups`パッケージは、Bluetooth接続を介した印刷処理を可能にします。

一般的な相互作用

Bluetoothシステムは、必要な機能を提供する、4種類の関連するレイヤーから構成されています。

ハードウェア
ハードウェアアダプタと、Linuxカーネルによるサポートに適したドライバです。

環境設定ファイル
Bluetoothシステムの制御に使用されます。

デーモン
設定ファイルにより制御されるサービスで、各種機能を提供します。

アプリケーション
アプリケーションにより、ユーザはデーモンが提供する機能を使用、および制御できます。

Bluetoothアダプタを挿入すると、ホットプラグシステムによりそのドライバがロードされます。ドライバがロードされた後、システムは設定ファイルを検査してBluetoothを起動する必要があるかどうかを確認します。起動を必要とする場合は、どのサービスを起動するかが判別されます。この情報に基づいて、関連デーモンが起動されます。Bluetoothアダプタはインストール中に認識されます。1つ以上のアダプタが検出されると、Bluetoothを有効にします。ここで検出されない場合は、Bluetoothシステムは無効のままになります。そのため後から追加されたBluetoothデバイスは手動で有効にする必要があります。

プロファイル

Bluetoothでは、プロファイルによってサービスが定義されます。プロファイルには、ファイル転送プロファイル、基本印刷プロファイル、およびパーソナルエリアネットワークプロファイルなどがあります。 デバイスパッケージやマニュアルでは説明されていないことがよくありますが、他方のデバイスのサービスを使用できるように設定するには、双方のデバイスが同じプロファイルを認識する必要があります。残念ながら、メーカが個々のプロファイルの定義に厳密に準拠していない場合もあります。こうした背景にもかかわらず、デバイス間の通信は通常、円滑に行われます。

次の説明で、ローカルデバイスとはコンピュータに物理的に接続された状態のデバイスを指します。アクセスに無線接続を必要とする他のデバイスはすべて、リモートデバイスと呼びます。

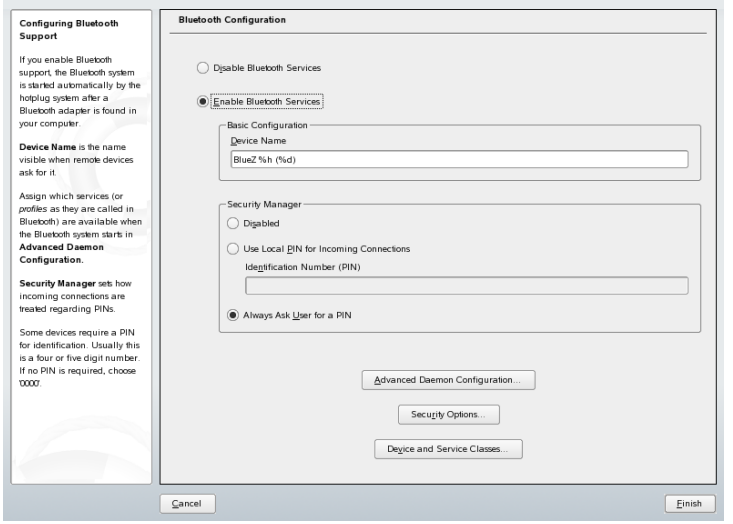
22.2.2 環境設定

ここではBluetoothの設定について説明します。関係する各種設定ファイル、必要な各種ツール、を使用して、または手動によるBluetoothの設定方法について解説します。

YaSTによるBluetoothの設定

YaST Bluetoothモジュール(図 22.2. 「YaSTのBluetooth 設定」 (page 327)を参照)を使用して、システム上でBluetoothサポートを設定します。ホットプラグがシステム上でBluetoothを検出すると、(たとえば、ブート中アダプタをプラグインした場合)、このモジュールで設定された値を使用して、Bluetoothが自動的に起動されます。

図 22.2　YaSTのBluetooth 設定



最初の設定ステップでは、システムでBluetoothサービスを開始する必要があるかどうかを決定します。Bluetoothサービスが有効になっている場合、次の2つを設定できます。最初は［デバイス名］です。この名前はご使用のコンピュータが他のデバイスに検出された場合に、他のデバイス側に表示されるデバイス名です。これには次の2種類のプレースホルダを組み合わせることも可能です。`%h`はシステムのホスト名を表します(たとえば、DHCPによって動的に割り当てられる場合に有用)。`%d`はインタフェース番号を指定します。(ご使用のコンピュータに複数のBluetoothアダプタがある場合にのみ有用)。たとえば、フィールドに`Laptop %h`と入力し、ご使用のコンピュータがDHCPから`unit123`を割り当てられた場合、他のリモートデバイスはご使用のコンピュータを`Laptop unit123`として識別します。

［*Security Manager (セキュリティマネージャ)*］パラメータは、リモートデバイスからの接続を検知した場合にローカルシステムがどのように対処するか、ということに関係しています。違いはPIN番号の取り扱いです。PINなしですべてのデバイスに接続を許可するか、PINが必要な場合に正しいPINが指定されたかを判別します。PIN(設定ファイルに格納)は、適切な入力フィールドに指定できます。あるデバイスが接続を試みた場合、最初にこのPINが使用されます。ここで認証に失敗すると、PINを使用しないように変更されます。 セキュリティを高めるためには、［*Always ask user for PIN(常時ユーザにPINを確*

認する)］を指定するのが最善と言えます。このオプションにより、異なる(リモート)デバイスに対して別のPINを使用できるようになります。

次に[*拡張デーモン設定*]をクリックすると、使用可能なサービス(Bluetoothでは*プロファイル*)の選択および設定用ダイアログが表示されます。使用可能なサービスがすべてリストに表示されます。ここでは[*有効にする*]または[*無効にする*]をクリックしてサービスを有効または無効にすることができます。［*編集*］をクリックするとダイアログが開き、選択したサービス(デーモン)に対する引数を追加指定できます。変更は、サービスを十分に理解している場合にのみ行ってください。デーモンの設定を完了後に、[*了解*]をクリックしてこのダイアログを終了します。

メインダイアログに戻り、[*セキュリティオプション*]をクリックしてセキュリティダイアログを表示し、暗号化、認証、およびスキャン設定を行います。次に、セキュリティダイアログを終了してメインダイアログに戻ります。［*Finish*]をクリックしてメインダイアログを閉じると、Bluetoothシステムが使用可能になります。

メインダイアログから［*デバイスおよびサービスクラス*］ダイアログにも移動できます。 各Bluetoothデバイスはさまざまなデバイスクラスに分類されています。このダイアログで［*Desktop*］、［*Laptop*］など、ご使用のコンピュータに適したデバイスクラスを選択してください。 デバイスクラスは、ここで同時に設定できるサービスクラスとは異なり、それほど重要ではありません。携帯電話のようなリモートのBluetoothデバイスでは、相手のシステム上で適切なサービスクラスを検出できた場合にのみ使用できるようになる、特定の機能を備えている場合があります。これは多くの場合携帯電話に当てるケースです。携帯電話では「オブジェクト転送」と呼ばれるクラスを待機した後、コンピュータ間のファイル転送を許可します。ここでユーザは複数のクラスを選択できます。ただし、「念のため」とすべてのクラスを選択することは実用的ではありません。通常の場合はデフォルト設定で問題ありません。

Bluetoothを使用してネットワークをセットアップする場合は、［*拡張デーモン設定*］ダイアログで［*PAND*］を有効にし、*編集*でデーモンのモードを設定します。Bluetoothネットワーク接続を機能させるには、一方のpandが[*ネットワーク接続(受信モード)*]で動作し、ピアが[*ネットワーク接続(検索モード)*]で動作する必要があります。デフォルトでは、[*ネットワークデーモンをリッスンモードに設定*]モードが事前に設定されています。ローカルpandの動作を調整します。さらに、YaSTの[*ネットワークカード*]モジュールで`bnepX`インタフェース(`X`はシステム内のデバイス番号)を設定します。

Bluetoothの手動設定

Bluezシステムの各コンポーネントの設定ファイルは、ディレクトリ /etc/bluetoothにあります。ただし、コンポーネント起動用のファイル /etc/sysconfig/bluetoothは、YaSTモジュールにより変更されます。

ここで説明する設定ファイルは、ユーザrootのみが変更できます。現在のところ、すべての設定を変更できるグラフィカルユーザインタフェースはありません。YaST Bluetoothモジュールを使用して指定できる最も重要な設定はYaSTによるBluetoothの設定項 (page 326)に記載されています。その他のすべての設定は経験のあるユーザ向けであり、特殊な場合以外、必要ではありません。通常、デフォルト設定はそのままで適切です。

PIN番号は、不正な接続を防止するための基本的な保護手段です。携帯電話は、最初に接続するときに(またはデバイスから電話への接続をセットアップするときに)、通常PIN番号を問い合わせます。2つのデバイスが通信を行うためには、両方が同じPIN番号で互いを識別する必要があります。コンピュータ上では、PINはファイル /etc/bluetooth/pinにあります。

重要項目: Bluetooth接続のセキュリティ

PINを使用しても、2つのデバイス間の通信が完全に安全なわけではありません。デフォルトでは、Bluetooth接続の認証と暗号化は無効になっています。認証と暗号化を有効にすることで、結果的に一部のBluetoothデバイス間では、通信時の問題につながる可能性があります。

デバイス名やセキュリティモードなど、さまざまな設定を設定ファイル /etc/bluetooth/hcid.confで変更できます。通常、デフォルト設定はそのままで適切です。このファイルには、さまざまな設定のオプションを説明するコメントが含まれています。

インクルードファイルの2つのセクションがoptionsおよびdeviceとして指定されています。最初のセクションには、hcidで起動に使用される一般情報が含まれています。次のセクションには、個々のローカルBluetoothデバイスの設定が含まれています。

optionsセクションで最も重要な設定の1つがsecurity auto;です。autoに設定すると、hcidは着信接続にローカルPINを使用します。ローカルPINで接続に失敗すると、PINがnoneに切り替わり、いずれにしても接続を確立し

ます。セキュリティレベルを高めるために、このデフォルト設定をuserに指定し、接続の確立時にユーザに対して必ずPINの入力を促すようにする必要があります。

deviceセクションでは、接続先のデバイスで表示される、このコンピュータの表示名を設定します。デバイスクラス(Desktop、Laptop、Serverなど)も、このセクションで定義します。認証と暗号化も、ここで有効または無効にします。

22.2.3 システムコンポーネントとユーティリティ

Bluetoothの操作性は、さまざまなサービスとの対話に依存します。これには次のようなバックグラウンドデーモンが少なくとも2つ必要です。 1つは、Bluetoothデバイスのインタフェースとして機能し、デバイスを制御するhcid(ホストコントローラインタフェースデーモン)、もう1つは、ホストが提供するサービスをデバイス側で確認するためのsdpd(サービスディスカバリプロトコルデーモン)です。システムを起動したときにこれらが自動的に有効になっていない場合は、rcbluetooth startを使用してhcidとsdpdを有効にできます。このコマンドは、rootとして実行する必要があります。

ここでは、Bluetoothの操作に使用できる最も重要なシェルツールについて説明します。現在、Bluetoothの制御に使用できるグラフィカルコンポーネントが多数出回ってはいますが、これらのツールプログラムについても調べてみるだけの価値はあります。

コマンドの中には、rootとしてのみ実行できるコマンドもあります。リモートデバイスのテストに使用するl2ping *device_address*もそのようなコマンドの1つです。

hcitool

hcitoolは、ローカルおよびリモートのデバイスが検出されたかどうかを判断するために使用します。コマンドhcitool devを実行すると、ローカルデバイスが一覧表示されます。出力には、検出されたすべてのローカルデバイスについて、*interface_name device_address*という形式で1行に1つのデバイスが表示されます。

コマンドhcitool inqを使用してリモートデバイスを検索します。 検出されたすべてのデバイスについて、デバイスアドレス、クロックオフセット、およびデバイスクラスの3つの値が表示されます。デバイスアドレスは、他のコマンドでターゲットデバイスを識別するために使用する重要な値です。クロックオフセットは、主に技術的な目的で使用されます。クラスには、デバイスタイプとサービスタイプが16進数で指定されます。

コマンドhcitool name *device-address*は、リモートデバイスのデバイス名を確認するために使用します。リモートコンピュータの場合、クラスとデバイス名は/etc/bluetooth/hcid.conf内の情報に対応します。ローカルデバイスのアドレスを指定すると、エラーが出力されます。

hciconfig

コマンド/usr/sbin/hciconfigを実行すると、ローカルデバイスの詳細情報が表示されます。引数を指定せずにhciconfigを実行すると、出力にはデバイス名(hciX)、物理デバイスアドレス(00:12:34:56:78形式の12桁の番号)などのデバイス情報と、伝送済みデータ量に関する情報が表示されます。

hciconfig hci0 nameを実行すると、リモートデバイスから要求を受信したときにコンピュータから戻される名前が表示されます。hciconfigは、ローカルデバイスの設定のクエリだけでなく、これらの設定の変更にも使用できます。たとえば、hciconfig hci0 name TESTを実行すると、名前がTESTに設定されます。

sdptool

プログラムsdptoolは、特定のデバイスでどのサービスが利用可能かを確認するために使用します。コマンドsdptool browse *device_address*を実行すると、デバイスのすべてのサービスが一覧表示されます。コマンドsdptool search *service_code*を使用して特定のサービスを検索します。このコマンドを実行すると、要求したサービスからアクセスできるすべてのデバイスがスキャンされます。そのデバイスのいずれかがサービスを提供している場合、プログラムはこのデバイスから返された(完全な)サービス名と簡単な説明を出力します。パラメータなしでsdptoolと入力することにより、提供されている全サービスコードの一覧を表示します。

22.2.4 グラフィックアプリケーション

Konquerorで、URL`sdp:/`を入力してローカルとリモートのBluetoothデバイスのリストを表示します。デバイスをダブルクリックすると、そのデバイスが提供するサービスの概要が表示されます。指定したサービスの1つにマウスを合わせると、そのサービスに使用されているプロファイルがブラウザのステータスバーに表示されます。サービスをクリックするとダイアログが開き、実行する操作を選択できます。保存、サービスの使用(アプリケーションの起動が必要)、またはアクションの取り消しのいずれかを選択します。ダイアログを再表示せず、選択したアクションを常に実行する場合は、チェックボックスをオンにします。一部、まだサポートが使用可能になっていないサービスや、追加パッケージのインストールを必要とするサービスがあります。

22.2.5 例

このセクションではBluetoothのシナリオとして想定される典型的な例を2つ取り上げます。最初の例では2つのホスト間でBluetooth経由のネットワーク接続がどのように確立されるかについて説明します。次の例ではコンピュータと携帯電話間の接続について説明します。

2台のホスト間のネットワーク接続

最初の例では、ホスト*H1*と*H2*の間にネットワーク接続が確立されます。この2つのホストのBluetoothデバイスアドレスは*baddr1*と*baddr2*(前述のように両方のホスト上でコマンド`hcitool dev`を使用して判別)です。この2つのホストをIPアドレス`192.168.1.3` (*H1*)および`192.168.1.4` (*H2*)で識別する必要があります。

Bluetooth接続は、pand (パーソナルエリアネットワーキング)を使用して確立されます。次に示す各コマンドは、ユーザ`root`として実行する必要があります。ここでは、Bluetooth固有のアクションを中心に説明し、ネットワークコマンド`ip`の詳細は省略します。

`pand -s`を入力して、ホスト*H1*でpandを起動します。次に、`pand -c` *`baddr1`*を使用することで、ホスト*H2*での接続を確立できます。一方のホストで`ip link show`と入力すると、使用可能なネットワークインタフェースのリストが表示されます。出力には、次のようなエントリが含まれています。

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
 link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

出力には、00:12:34:56:89:90の代わりにローカルデバイスのアドレス*baddr1*または*baddr2*が含まれているはずです。ここで、このインタフェースにIPアドレスを割り当て、有効にする必要があります。*H1*で、そのために以下の2つのコマンドを使用します。

```
ip addr add 192.168.1.3/24 dev bnep0 ip link set bnep0 up
```

*H2*で実行するコマンド:

```
ip addr add 192.168.1.4/24 dev bnep0 ip link set bnep0 up
```

これで*H1*は、*H2*からIP 192.168.1.3で、アクセスできます。コマンドssh 192.168.1.4を使用して、*H1*から*H2*にアクセスします(*H2*が、SUSE Linuxによってデフォルトで有効にされたsshdを実行していると仮定します)。コマンドssh 192.168.1.4は、一般ユーザとしても実行できます。

携帯電話からコンピュータへのデータ転送

2つ目の例では、携帯電話内蔵のデジタルカメラで撮った写真を、(マルチメディアメッセージの転送に必要になる余分なコストをかけずに)コンピュータに転送する方法を示します。携帯電話は機種によってメニュー構造が異なりますが、手順は通常、ほとんど同じです。必要であれば、携帯電話のマニュアルを参照してください。この例では、Sony Ericssonの携帯電話からラップトップに写真を転送する方法について説明します。サービスObex-Pushがコンピュータ上で利用でき、コンピュータが携帯電話からのアクセスを許可している必要があります。最初のステップでは、サービスをラップトップで利用できるようにします。これには、パッケージbluez-utilsにあるopdデーモンを使用します。次のコマンドでデーモンを起動します。

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

--sdpは、sdpdを使用してサービスを登録します。--path /tmpは、プログラムに対し、受信データの保存場所(ここでは、/tmp)を指定します。書き込みアクセス権を持つ他のディレクトリを指定することもできます。

次に、携帯電話がコンピュータを認識するように設定する必要があります。これには、電話側で[*Connect(接続)*]メニューの[*Bluetooth*]を選択します。必要に応じて、[*My devices(マイデバイス)*]を選択する前に、[*Turn On(オン)*]をクリックします。[*New device(新規デバイス)*]を選択すると、携帯電話がラップ

トップを探査します。デバイスが検出されると、ディスプレイに名前が表示されます。ラップトップに関連付けられているデバイスを選択します。PINの入力を求められたら、/etc/bluetooth/pinに指定されているPINを入力します。これで、携帯電話がラップトップを認識し、ラップトップとデータを交換できるようになりました。現在のメニューを終了し、イメージメニューに移動します。転送するイメージを選択し、[*More(詳細)*]を押します。次のメニューでは、[*Send(送信)*]を押して通信モードを選択します。［*Via Bluetooth(Bluetooth経由)*]を選択します。ラップトップがターゲットデバイスとして表示されます。ラップトップを選択し、通信を開始します。イメージは、opdコマンドで指定したディレクトリに保存されます。オーディオトラックも、同じ方法でラップトップに転送できます。

22.2.6 トラブルシューティング

接続が確立できないときは、次のリストに従って作業を行います。エラーは接続の片端または両端で発生する可能性があることに注意してください。できれば、別のBluetoothデバイスで問題を再生し、そのデバイスに問題がないことを確認してください。

`hcitool dev`の出力にローカルデバイスが表示されますか？
: この出力にローカルデバイスが表示されない場合は、hcidが起動していないか、デバイスがBluetoothデバイスとして認識されていません。これにはさまざまな原因が考えられます。デバイスに不具合がある、正しいドライバがない、などです。Bluetooth内蔵ラップトップの場合、通常は無線デバイス(WLANやBluetoothなど)用のオン/オフスイッチが備えられています。この種のスイッチがデバイスにあるかどうかをラップトップのマニュアルで確認してください。コマンド`rcbluetooth restart`でBluetoothシステムを再起動し、/var/log/messagesにエラーが報告されるかどうかを調べます。

Bluetoothアダプタにはファームウェアファイルが必要ですか？
: ファームウェアファイルが必要な場合は、`bluez-bluefw`をインストールし、`rcbluetooth restart`でBluetoothシステムを再起動します。

`hcitool inq`の出力に他のデバイスが表示されますか？
: このコマンドは何度かテストしてください。Bluetoothの周波数帯が他のデバイスでも使用されているため、接続に干渉が発生している可能性があります。

PINは一致していますか？

コンピュータのPIN番号(`/etc/bluetooth/pin`内)がターゲットデバイスと一致しているかどうかを確認してください。

リモートデバイスは使用中のコンピュータを「認識」できますか？

リモートデバイスから接続を行ってみます。このデバイスがコンピュータを認識するかを確認します。

ネットワーク接続を確立できますか(2台のホスト間のネットワーク接続項 (page 332)を参照)？

2台のホスト間のネットワーク接続項 (page 332)で説明したセットアップは、いくつかの理由でうまく動作しないことがあります。たとえば、2台のコンピュータの一方がsshプロトコルをサポートしていない可能性があります。`ping 192.168.1.3`または`ping 192.168.1.4`を試してみます。このコマンドが実行できる場合は、次にsshdが有効かどうかを確認します。他に考えられる原因としては、例で使用しているアドレス`192.168.1.X`と競合するネットワーク設定が既に一方のデバイスで使用されている場合です。この場合、`10.123.1.2`と`10.123.1.3`のような異なるアドレスを試してみます。

ラップトップはターゲットデバイスとして表示されますか(携帯電話からコンピュータへのデータ転送項 (page 333)を参照)?携帯デバイスは、ラップトップのObex-Pushを認識しますか?

[*My devices(マイデバイス)*]で各デバイスを選択し、[*Services(サービス)*]のリストを表示します。(リストを更新しても) Obex-Pushが表示されない場合は、ラップトップ上のopdが原因です。opdはアクティブですか?指定したディレクトリに対して、書き込みアクセスができますか？

携帯電話からコンピュータへのデータ転送項 (page 333)で説明したシナリオは他の方法でも機能しますか？

`obexftp`パッケージがインストールされている場合は、一部のデバイスでこの操作にコマンド`obexftp -b device_address -B 10 -p image`を使用できます。複数のSiemensおよびSony Ericssonモデルではテストを完了し、機能することが確認されています。`/usr/share/doc/packages/obexftp`ディレクトリのドキュメントを参照してください。

22.2.7 関連資料

Bluetoothの使用方法と設定についての詳細な説明は、http://www.holtmann.org/linux/bluetooth/で入手可能です。その他、次の情報および指示が役立ちます。

- カーネルに統合されているBluetoothプロトコルスタックの公式HOWTO: http://bluez.sourceforge.net/howto/index.html
- PalmOS PDAへの接続: http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html

22.3 赤外線データ通信

IrDA (Infrared Data Association)は赤外線による無線通信の標準規格名です。現在販売されている多くのラップトップにはプリンタ、モデム、LAN、他のラップトップなど、リモートデバイスとの通信を可能にするIrDA互換トランシーバが装備されています。通信速度は2400 bpsから4M bpsの範囲になります。

IrDA操作モードには2種類あります。SIRは標準モードで、シリアルインタフェースを使用して赤外線ポートにアクセスします。このモードはほぼどのシステムでも機能し、ほとんどの要件に対応します。一方、より高速なFIRモードにはIrDAチップ用の特別なドライバが必要になります。しかるべきドライバがないため、FIRモードでサポートされていないチップタイプもあります。コンピュータのBIOSで必要なIrDAモードを設定します。また、BIOSではSIRモードで使用されるシリアルインタフェースも表示します。

IrDAについての情報は、http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.htmlでWerner Heuser著の『Linux Infrared HOWTO』を参照してください。また、http://irda.sourceforge.net/のLinux IrDA Project Webサイトも参照してください。

22.3.1 ソフトウェア

必要なカーネルモジュールは、カーネルパッケージに組み込まれています。irdaパッケージでは赤外線通信インタフェースをサポートするために必要な

各種アプリケーションを提供しています。このマニュアルはパッケージをインストールした後、 /usr/share/doc/packages/irda/README で参照できます。

22.3.2 環境設定

IrDAシステムサービスはシステムのブート時に自動的に開始されません。YaSTのIrDAモジュールを使用して有効にします。このモジュールで変更できる設定は1つだけです。赤外線デバイスのシリアルインタフェースのみが変更可能です。テストウィンドウに2種類の出力が表示されます。1つは irdadump の出力です。IrDAを介したすべての送受信パケットを記録します。この出力にはコンピュータ名および、通信圏内にあるすべての赤外線デバイス名が表示されます。項22.3.4.「トラブルシューティング」 (page 338)で、これらのメッセージ例を参照できます。IrDA接続を持つすべてのデバイスがウィンドウの下部に表示されます。

IrDAは相当な量の電力を消費します。周辺機器を検出するために数秒間隔でディスカバリパケットを送信するためです。そのため、電源がバッテリのみの場合は、必要なとき以外はIrDAを開始しないようにします。コマンド rcirda start でIrDAを有効に、またコマンド rcirda stop で無効にします。インタフェースが有効なった時点で、必要なカーネルモジュールがすべて自動的にロードされます。

ファイル /etc/sysconfig/irda を使用して、手動による設定が可能です。このファイルに含まれるのは変数 IRDA_PORT のみです。この変数はSIRモードで使用するインタフェースを決定します。

22.3.3 使用方法

印刷用のデータをデバイスファイル /dev/irlpt0 に送信できます。デバイスファイル /dev/irlpt0 は、データ送信が赤外線を使用して無線で行われる以外、通常のケーブル接続されたインタフェースである、 /dev/lp0 と同様に動作します。印刷時には、プリンタがコンピュータの赤外線インタフェースから見える範囲にあり、赤外線サポートが開始されていることを確認してください。

赤外線インタフェースを介してプリンタを操作する場合、プリンタモジュールを使用してプリンタを設定できます。プリンタは自動検出されないため、［*その他(未検出)*］をクリックし、手動で設定してください。その後にダイアログで［*IrDA*プリンタ］を選択します。通常、`irlpt0`が正しい接続になります。Linuxでのプリンタ操作に関する詳細については、章 31. *プリンタの運用* (page 511)を参照してください。

その他のホストおよび、携帯電話またはそれに類するデバイスとの通信は、デバイスファイル`/dev/ircomm0`を介して行われます。たとえば、携帯電話のSiemens S25、Nokia 6210といった機種では、赤外線インタフェースを使用するwvdialアプリケーションで、ダイヤルおよびインターネットへの接続が可能です。Palm Pilotとのデータ同期も可能です。対応するアプリケーションのデバイス設定は、`/dev/ircomm0`に指定されています。

必要に応じて、プリンタまたはIrCOMMプロトコルをサポートするデバイスのみ指定できます。3Com Palm PilotのようなIROBEXプロトコルをサポートするデバイスにはirobexpalmおよびirobexreceiveなどの特別なアプリケーションを使用してアクセスできます。.詳細については、*IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`)を参照してください。`irdadump`の出力で、デバイス名の隣にあるカッコ内にデバイス別にサポートされるプロトコルが一覧表示されます。IrLANプロトコルのサポートは現在「開発中」です。

22.3.4 トラブルシューティング

赤外線ポートに接続されたデバイスが応答しない場合は、コマンド`irdadump` (`root`で)を使用して、コンピュータが他のデバイスを認識しているか確認します。Canon BJC-80プリンタがコンピュータの通信可能範囲内にあると、例 22.1.「irdadumpの出力」 (page 338)のような内容が定期的に表示されます。

例 22.1 *irdadumpの出力*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* earth
                        hint=0500 [ PnP Computer ] (21)
```

出力が得られない、または他のデバイスが応答しない場合は、インタフェースの設定を確認してください。正しいインタフェースが使用されていることを確認します。赤外線インタフェースが/dev/ttyS2または/dev/ttyS3にあったり、IRQ3以外の割り込みが使用されていたりする場合もあります。ほぼすべてのラップトップのBIOS設定メニューから、これらの設定を確認および変更できます。

簡単なビデオカメラでも赤外線LEDライトが点灯しているかどうかを確認できます。多くのビデオカメラは人間の眼に見えない赤外線を感知することができるためです。

パート VII. 管理

23 Linuxのセキュリティ

マスカレードとファイアウォールを使用すると、データフローとデータの送受信を確実に管理できるようになります。SSH (Secure Shell) を使用すると、暗号化された接続を介してリモートホストにログインできます。ファイルまたはパーティション全体を暗号化すれば、第三者によってシステムに侵入された場合でも、データを保護できます。Linuxネットワークでのセキュリティと、関連する技術的な事柄について学んでください。

23.1 マスカレードとファイアウォール

ネットワーク環境でLinuxを使用する場合は常に、ネットワークパケットを操作するカーネル機能を使用して内部ネットワークと外部ネットワークを隔離できます。Linuxのnetfilterフレームワークは、複数のネットワークを隔離する効果的なファイアウォールを構築する手段を提供します。ルールセットを定義する汎用的なテーブル構造体であるiptablesを使用すれば、ネットワークインタフェースを通すパケットを詳細に制御することが可能です。このようなパケットフィルタは、SuSEfirewall2および対応するモジュールを使用して簡単にセットアップできます。

23.1.1 iptablesによるパケットフィルタリング

netfilterコンポーネントおよびiptablesコンポーネントは、ネットワークアドレス変換(NAT)に加え、ネットワークパケットのフィルタリングと操作の機能を備えています。フィルタ条件およびそれに関連付けられたアクションはルールセットとして格納され、受信したネットワークパケットに対して1つずつ個別に照合されます。使用されるフィルタ条件とアクションのセットはテーブルに格納されます。これらのテーブルおよびルールセットに変更を加えるには、`iptables`コマンドを使用します。

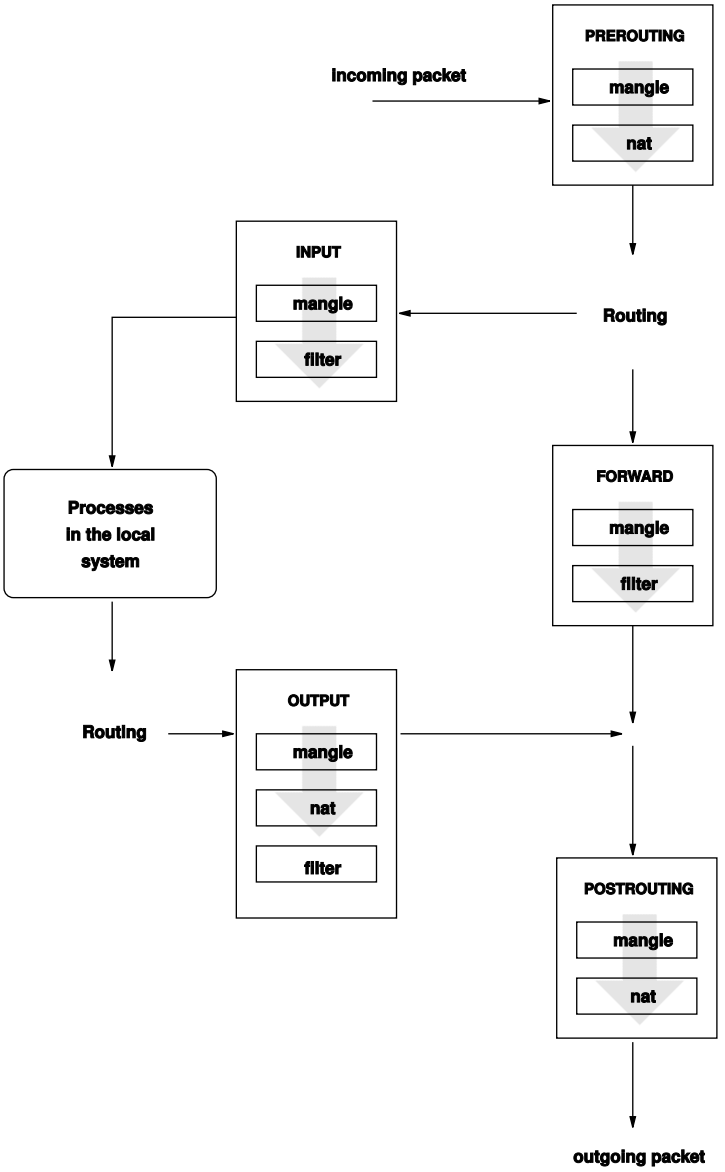
Linuxカーネルは、以下の3つのテーブルを管理します。各テーブルは、パケットフィルタの特定の機能カテゴリに対応しています。

filter
: このテーブルは、狭い意味での「パケットフィルタリング」メカニズムを実装するもので、フィルタルールの大半を含んでいます。たとえば、パケットを通すか(`ACCEPT`)破棄するか(`DROP`)を判定します。

nat
: このテーブルは、パケットの送信元アドレスと宛先アドレスに対する変更内容を定義します。これらの機能を使用して、「マスカレード」を実装できます。マスカレードは、プライベートネットワークとインターネットをリンクするNATの一種です。

mangle
: このテーブルのルールを使用して、IPヘッダ内の値(サービスタイプなど)を操作できます。

図 23.1　iptables: パケットの可能な経路



これらのテーブルには、パケットと照合される次のような複数の事前定義ルールセットが含まれています。

PREROUTING
このルールセットは、着信パケットに適用されます。

INPUT
このルールセットは、システムの内部プロセス宛てのパケットに適用されます。

FORWARD
このルールセットは、システムを通過するだけのパケットに適用されます。

OUTPUT
このルールセットは、このシステム自身が送信元であるパケットに適用されます。

POSTROUTING
このルールセットは、すべての発信パケットに適用されます。

あるシステムにおけるネットワークパケットの伝送経路を図 23.1. 「iptables: パケットの可能な経路」 (page 345)に示します。簡略化するために、この図ではテーブルをルールセットの一部として示してありますが、実際にはこれらのルールセットはテーブル自体に格納されています。

最も単純なケースとして、システム宛の着信パケットが`eth0`インタフェースに届いた場合を考えてみます。このパケットはまず`mangle`テーブルの`PREROUTING`ルールセットと照合され、次に`nat`テーブルの`PREROUTING`ルールセットと照合されます。パケットのルーティングに関する次のステップでは、パケットの実際の宛先がシステム自身のプロセスであることが確認されます。`mangle`テーブルおよび`filter`テーブルの`INPUT`ルールセットを経た後、このパケットは、`filter`テーブルのルールに実際に適合していれば、最終的に宛先に届きます。

23.1.2 マスカレードの基礎知識

マスカレードは、Linux固有のNAT (ネットワークアドレス変換)です。マスカレードを使用すると、小規模LAN(ホストがプライベート範囲のIPアドレスを使用するネットワーク—項38.1.2. 「ネットマスクとルーティング」 (page 615)を参照)をインターネット(パブリックIPアドレスを使用するネットワーク)に接続することができます。このLANのホストをインターネットに接続するた

めには、プライベートアドレスをパブリックアドレスに変換する必要があります。この変換処理は、LANとインターネット間のゲートウェイとして動作するルータで行います。 ルータの基本原理は単純です。ルータとは、複数のネットワークインタフェース(通常、ネットワークカードおよびそれとは別のインターネット接続用インタフェース)を備えたネットワーク装置です。インターネット接続用インタフェースは外部に接続し、その他のインタフェースはLAN上のホストに接続します。ルータのネットワークカード(`eth0`など)に接続されているローカルネットワーク内のホストは、ローカルネットワーク以外の宛先を持つすべてのパケットをデフォルトゲートウェイ、つまりルータに送信します。

重要項目: 正しいネットワークマスクの使用

ネットワークを設定する際は、すべてのローカルホストに同じブロードキャストアドレスとネットマスクを設定する必要があります。 そうしないと、パケットが正しく転送されません。

前述のように、LAN上のホストがインターネット上のアドレス宛にパケットを送信すると、そのパケットは常にデフォルトルータに送信されます。しかし、そのためには、これらのパケットを転送できるようにルータを設定しておく必要があります。 セキュリティ上の理由から、SUSE Linuxのインストール時のデフォルト設定では、この転送処理が有効になっていません。有効にするには、 `/etc/sysconfig/sysctl`ファイルの`IP_FORWARD`変数を`IP_FORWARD=yes`に設定します。

宛先ホストからは、ルータは参照できますが、内部ネットワーク内の送信元ホストに関する情報は一切分かりません。この技術がマスカレード(masquerading:「変装」の意)と呼ばれているのは、このためです。アドレス変換が行われているため、あらゆる応答パケットはまずルータに届きます。ルータはこれらの着信パケットを識別し、宛先アドレスを変換して、ローカルネットワーク内の正しいホストにパケットを転送します。

着信トラフィックのルーティングはマスカレードテーブルによって決まるため、外部から内部ホストへの接続を開く方法はありません。テーブルには、そのような接続に関するエントリがありません。また、確立済みの接続に対してはテーブルでステータスエントリが割り当てられるため、そのエントリは他の接続では使用されません。

このため、マスカレードを使用すると、ICQ、cucme、IRC (DCC、CTCP)、FTP (PORTモード)などいくつかのアプリケーションプロトコルで問題が発生

する可能性があります。標準的なFTPプログラムであるNetscapeは、PASVモードを使用しています。PASVモードを使用すれば、パケットフィルタとマスカレードに関する問題が発生する可能性はかなり低くなります。

23.1.3 ファイアウォールの基礎知識

「ファイアウォール」は、ネットワーク間のリンクを提供、管理し、ネットワーク間のデータフローを制御するメカニズムを表す用語として、おそらくもっとも広く知られています。ただし、厳密にいうと、このセクションで説明するメカニズムは「パケットフィルタ」と呼ばれるものです。パケットフィルタは、プロトコル、ポート、IPアドレスなどに関する一定の条件に従ってデータフローを規制します。これにより、アドレスに応じて内部ネットワークに到達しないように定められているパケットが、ブロックされます。たとえば、社内のWebサーバを外部に公開するには、対応するポートを明示的に開きます。ただし、パケットフィルタは、社内のWebサーバ宛てのパケットなど、正当なアドレスを持つパケットの内容はスキャンしません。たとえば、着信パケットがWebサーバ上のCGIプログラムの破壊を目的としたものである場合でも、パケットフィルタはそれをそのまま通してしまいます。

より効果的な、しかしより複雑なメカニズムとして、いくつかのタイプのシステムを組み合わせる方法があります。たとえば、パケットフィルタと、プロキシと呼ばれるアプリケーションゲートウェイを連携動作させます。この場合、パケットフィルタは、無効なポートへのパケットをすべて拒否し、アプリケーションゲートウェイ宛てのパケットのみを受け入れます。このゲートウェイ、つまりプロキシは、サーバの実際のクライアントであるかのように振る舞います。ある意味で、このようなプロキシは、アプリケーションによって使用されるプロトコルレベルのマスカレードホストと見なすことができます。プロキシの例としては、HTTPプロキシサーバのSquidがあります。Squidを使用するには、プロキシ経由で通信するようにブラウザを設定する必要があります。要求したHTTPページはまずプロキシのキャッシュ内で検索され、キャッシュに見つからなかったページのみがプロキシによってインターネットから取得されます。別の例としては、FTPプロトコルのプロキシサーバであるSUSE proxy-suite (`proxy-suite`)があります。

次のセクションでは、SUSE Linuxに付属するパケットフィルタについて説明します。パケットフィルタとファイアウォールに関するより詳細な説明については、`howto`パッケージに含まれている『Firewall HOWTO』を参照してください。このパッケージがインストールされていれば、

`less /usr/share/doc/howto/en/Firewall-HOWTO.gz`で『Firewall HOWTO』を参照できます。

23.1.4 SuSEfirewall2

SuSEfirewall2は、`/etc/sysconfig/SuSEfirewall2`から変数を読み取って一連のiptablesルールを生成するスクリプトです。このスクリプトは、次に示す3つのセキュリティゾーンを定義します(ただし、以降のサンプル設定では1番目と2番目のセキュリティゾーンについてのみ考察します)。

外部ゾーン
: 外部ネットワークで何が発生しているかを制御できないことを考えれば、ホストを外部ネットワークから保護する必要があることがわかります。外部ネットワークはほとんどの場合インターネットですが、WLANなどそれ以外の安全でないネットワークであることもあります。

内部ゾーン
: これはプライベートネットワークを表します。ほとんどの場合はLANになります。内部ネットワーク内のホストがプライベート範囲のIPアドレス(項38.1.2.「ネットマスクとルーティング」 (page 615)を参照)を使用している場合、ネットワークアドレス変換(NAT)を有効にして内部ネットワークのホストが外部ネットワークにアクセスできるようにします。

非武装地帯(DMZ)
: このゾーンのホストには外部ネットワークと内部ネットワークの両方からアクセスできますが、このゾーンのホストは自身では内部ネットワークにアクセスできません。DMZ内のシステムは内部ネットワークから隔離されるため、内部ネットワークの周りに追加の防衛線を設けたい場合にこのゾーンを設定します。

フィルタリングルールセットで明示的に許可されていないあらゆる種類のネットワークトラフィックは、iptablesによって抑止されます。したがって、着信トラフィックを持つそれぞれのインタフェースは、3つのゾーンのいずれかに配置する必要があります。各ゾーンに対して、許可するサービスやプロトコルを定義します。ルールセットは、外部ホストから送信されたパケットにのみ適用されます。ローカルに生成されたパケットは、ファイアウォールによって捕捉されません。

設定はYaSTで行うことができます(YaSTによる設定項 (page 350)を参照)。または、ファイル /etc /sysconfig /SuSEfirewall2に手動で設定することもできます。このファイルには、詳しい注釈が付けられています。また、さまざまな設定例が /usr /share /doc /SuSEfirewall2 /EXAMPLESに格納されています。

YaSTによる設定

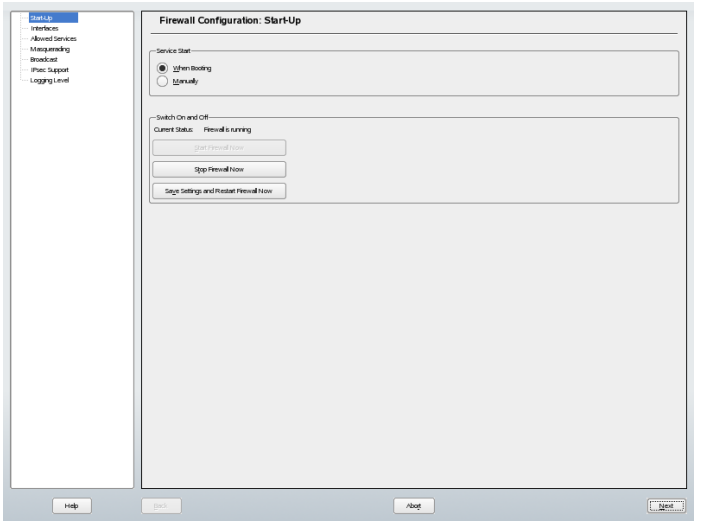
重要項目: 自動ファイアウォール設定

インストール後に、YaSTは、すべての設定済みインタフェース上で自動的にファイアウォールを起動します。システム上でサーバが設定されており有効になっていれば、は、サーバ設定モジュールの［*ファイアウォールで開いているポート*］オプションまたは［*Open Ports on Selected Interface in Firewall(選択したインタフェースでファイアウォールを開く)*］オプションを使用して、生成されたファイアウォール設定に自動的に変更を加えます。サーバモジュールの一部のダイアログでは、［*ファイアウォールの詳細*］ボタンをクリックすると、追加のサービスとポートを有効にできます。YaSTのファイアウォール設定モジュールは、ファイアウォールを有効または無効にする作業、あるいは再設定する作業に使用できます。

グラフィカル設定用のYaSTダイアログには、YaSTコントロールセンターからアクセスできます。*[セキュリティとユーザ] → [ファイアウォール]*を選択してください。設定は7つのセクションに分かれており、画面左側のツリー構造で各セクションに直接ジャンプすることができます。

起動
: このダイアログでは起動動作を設定します。デフォルトのインストールでは、SuSEfirewall2は自動的に起動します。このダイアログで、ファイアウォールを起動または停止することもできます。動作中のファイアウォールに新しい設定を適用するには、［*Save Settings and Restart Firewall Now*］をクリックします。

図 23.2　YaSTでのファイアウォールの設定



[インタフェース]

ここには、認識されているすべてのネットワークインタフェースがリストされます。 ゾーンからインタフェースを削除するには、削除するインタフェースを選択して、［*Change*］をクリックし、［*No Zone Assigned*］を選択します。ゾーンにインタフェースを追加するには、追加するインタフェースを選択して、［変更］をクリックし、使用可能のいずれかのゾーンを選択します。［*Custom*］を使用して、ユーザ固有の設定で特殊なインタフェースを作成することもできます。

[許可されるサービス]

このオプションは、システムに対するアクセスが禁止されているゾーンに対してシステムサービスを提供するために使用します。デフォルトでは、システムには、外部ゾーンからの保護だけが設定されています。外部のホストで利用可能にするサービスだけを、明示的に許可してください。［*Allowed Services for Selected Zone*］でゾーンを選択してから、サービスを有効化します。

[マスカレード]

マスカレードは、インターネットのような外部のネットワークから内部のネットワークを隠します。その一方で、内部のネットワークのホストからは外部のネットワークに透過的にアクセスできるようにします。外部ネットワークから内部ネットワークへの要求はブロックされますが、内部ネッ

トワークからの要求は、外部から見ると、マスカレードサーバから発信されたように見えます。内部ホストの特殊なサービスを外部ネットワークから利用可能にする必要がある場合は、そうしたサービス用の特殊なリダイレクトルールを追加します。

［ブロードキャスト］
このダイアログでは、ブロードキャストが可能なUDPポートを設定します。各ゾーンで必要なポート番号またはサービス名を、スペースで区切って指定してください。1/etc/servicesも参照してください。

ここでは、受け付けられなかったブロードキャストについてのログを有効にすることもできます。ただし、Windowsホストは、互いを認識するためにブロードキャストを使用するため、大量のパケットが禁止されることになります。このため、ログを有効にすると大量のパケットがすべてログに記録されてしまいます。

［IPsecサポート］
このダイアログでは、外部ネットワークに対するIPsecサービスを利用できるようにするかどうかを設定します。どのパケットを信頼するかは、［*Details*］で設定します。

［ログレベル］
ログには、受け付けられたパケットと受け付けられなかったパケットについての、2つのルールがあります。受け付けられなかったパケットは、捨てられるか拒否されます。その両方について、［*Log All (すべてログに記録する)*］、［*Log Critical(重要なパケットを記録する)*］、［*Do Not Log Any (ログに何も記録しない)*］のいずれかを選択します。

機能設定が終わったら、［*次へ*］をクリックしてダイアログを閉じます。ゾーンごとのファイアウォール設定の概要が表示されます。設定がすべて正しいかどうかチェックしてください。このサマリーには、許可されたすべてのサービス、ポート、プロトコルがリストされます。設定を修正するには、［*Back*］をクリックします。設定内容を保存するには、［*Accept*］をクリックします。

手動による設定

以降では、適切に設定するための手順を順を追って説明します。各設定項目には、ファイアウォールとマスカレードのどちらに関連するかを示してあります。設定ファイルで述べられているDMZ (非武装地帯)関連の設定については、ここでは取り上げません。DMZは、大規模な組織に見られる複雑なネッ

トワークインフラストラクチャ(企業ネットワークなど)でのみ使用されるものであり、広範な設定とこの分野に関する深い知識を必要とします。

まず、YaSTのシステムサービスモジュール(ランレベル)を使用して、使用中のランレベル(通常3または5)でSuSEfirewall2を有効にします。これにより、/etc/init.d/rc?.d/ディレクトリ内のSuSEfirewall2_*スクリプトへのシンボリックリンクが設定されます。

FW_DEV_EXT (ファイアウォール、マスカレード)
インターネットへの接続デバイス。モデム接続の場合は、ppp0を指定します。IDSNリンクの場合は、ipppp0を指定します。DSL接続には、dsl0を指定します。デフォルトルートに対応するインタフェースを使用する場合は、autoを指定します。

FW_DEV_INT (ファイアウォール、マスカレード)
内部プライベートネットワークへの接続デバイス(eth0など)。内部ネットワークがなく、ファイアウォールが動作するホストのみを保護する場合は、空にします。

FW_ROUTE (ファイアウォール、マスカレード)
マスカレード機能が必要な場合は、yesに設定します。内部ホストのネットワークアドレス(例: 192.168.x.x)がインターネットルータで無視されるようになるため、内部ホストは外部から見えなくなります。

マスカレード機能なしのファイアウォールで、内部ネットワークへのアクセスを許可する場合は、これをyesに設定します。この場合、内部ホストでは公式のIPアドレスを使用する必要があります。ただし、外部ネットワークから内部ネットワークへのアクセスは*許可しない*のが普通です。

FW_MASQUERADE (マスカレード)
マスカレード機能が必要な場合は、yesに設定します。これにより、内部ホストからインターネットへの仮想的な直接接続が実現されます。内部ネットワークのホストとインターネット間にプロキシを設定すると、セキュリティが強化されます。プロキシサーバが提供するサービスにはマスカレードは必要ありません。

FW_MASQ_NETS (マスカレード)
マスカレードを行うホストやネットワークを指定します。各エントリはスペースで区切ります。次に例を示します。

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (ファイアウォール)
内部ネットワークからの攻撃に対してファイアウォールホストを保護するには、yesに設定します。サービスは、明示的に有効にした場合にのみ、内部ネットワークに対して提供されます。FW_SERVICES_INT_TCPおよびFW_SERVICES_INT_UDPも参照してください。

FW_SERVICES_EXT_TCP (ファイアウォール)
使用可能にするTCPポートを指定します。一般的な自宅用のワークステーションでは、通常サービスは提供していないため、空にします。

FW_SERVICES_EXT_UDP (ファイアウォール)
UDPサービスを実行しており、それを外部から使用できるようにする場合を除き、空にします。UDPを使用したサービスとしては、DNSサーバ、IPSec、TFTP、DHCPなどがあります。これらのサービスを使用可能にする場合は、使用するUDPポートを指定します。

FW_SERVICES_INT_TCP (ファイアウォール)
この変数には、内部ネットワークに対して使用可能にするサービスを指定します。記述形式はFW_SERVICES_EXT_TCPと同じですが、この設定は*内部*ネットワークに適用されます。この変数は、FW_PROTECT_FROM_INTをyesに設定した場合のみ設定します。

FW_SERVICES_INT_UDP (ファイアウォール)
FW_SERVICES_INT_TCPの項を参照してください。

ファイアウォールの設定が完了したら、設定をテストします。ファイアウォールのルールセットは、root権限でSuSEfirewall2 startを実行すると作成されます。次に、telnetを使用して、たとえば外部ホストから接続が実際に拒否されるかどうかを確認します。その後、/var/log/messagesを参照します。次のようなログが記録されているはずです。

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEBC0000000001030300)
```

他にも、nmapやnessusといったパッケージを使用して、ファイアウォールの設定をテストできます。パッケージをインストールすると、nmapのドキュメ

ントは/usr/share/doc/packages/nmapに、nessusのドキュメントは/usr/share/doc/packages/nessus-coreに置かれます。

23.1.5 関連資料

SuSEfirewall2の最新情報およびその他のドキュメントは、/usr/share/doc/packages/SuSEfirewall2で参照できます。また、netfilter/iptablesプロジェクトのホームページhttp://www.netfilter.orgでは、さまざまな文書を多くの言語で参照できます。

23.2 SSH:安全なネットワーク操作

ネットワーク環境に多数のコンピュータがインストールされるほど、遠隔地からホストへのアクセスが必要となります。通常、これはユーザが認証のためにログイン文字列とパスワード文字列を送信することを意味します。これらの文字列が平文で転送される限り、パケットが盗聴されて、転送元ユーザのアカウントにアクセスするために、そのアカウントを知る権限ユーザを使用せずに不正使用される恐れがあります。これはユーザのファイルがすべて攻撃者に公開されてしまうだけでなく、不正なアカウントを使用して管理者やrootユーザのアクセス権を取得したり、他のシステムに侵入できることにもなります。従来、リモート接続の確立にはtelnetが使用されていましたが、telnetには暗号化形式や他のセキュリティメカニズムのパケット盗聴に対する防護機能が用意されていません。その他にも、従来のFTPプロトコルや一部のリモートコピープログラムのように、保護機能のない通信チャネルが存在します。

SSHスイートは、認証文字列(通常はログイン名とパスワード)およびホスト間でやりとりされる他のすべてのデータを暗号化することで、必要な保護を提供します。SSHを使用した場合も、データフローを第三者に記録される可能性は残りますが、内容は暗号化されており、暗号鍵を知らない限り平文に戻すことはできません。そのため、SSHを使用すると、インターネットのように安全でないネットワーク上でも安全な通信が可能になります。 SUSE Linuxに付属しているSSHは、OpenSSHです。

23.2.1 OpenSSHパッケージ

SUSE Linuxでは、デフォルトでパッケージOpenSSHがインストールされます。これによりtelnet、rlogin、rsh、rcp、およびftpの代わりにプログラムssh、scp、およびsftpが使用可能になります。 デフォルト設定では、SUSE Linuxシステムのシステムアクセスは、OpenSSHユーティリティを使用し、ファイアウォールがアクセスを許可した場合にのみ可能になります。

23.2.2 sshプログラム

sshプログラムを使用すると、リモートシステムにログインして対話形式で作業できます。このプログラムは、telnetおよびrloginに代わるものです。sloginプログラムは、sshを指す単なるシンボリックリンクです。 たとえば、コマンドssh sunを使用してホストsunにログインするとします。 ホストはsunのパスワードを求めるプロンプトを表示します。

認証に成功すると、リモートのコマンドラインで作業したり、などの対話型アプリケーションを使用できます。ローカルユーザ名がリモートユーザ名と異なる場合は、ssh -l augustine またはssh augustine@を使用して、異なるログイン名でログインできます。

さらに、sshでは、rshから既知されるリモートシステム上でコマンドを実行できます。次の例では、ホストsun上でコマンドuptimeを実行し、tmpというディレクトリを作成します。 プログラムの出力は、ホストearthのローカル端末に表示されます。

```
ssh otherplanet "uptime; mkdir tmp"
tux@otherplanet's password:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

この例では、両方のコマンドを1つのコマンドで送信するために、引用符が必要です。 2つ目のコマンドもsun上で実行するには、このように引用符で囲む必要があります。

23.2.3 scp—Secure Copy

scpは、ファイルをリモートマシンにコピーします。これは、rcpに対する安全で暗号化機能を持つ代替策です。 たとえば、scp MyLetter.tex sun:は、

ファイルMyLetter.texをホストearthからホストsunにコピーします。 earth上でのユーザ名がsun上でのユーザ名と異なる場合は、後者をusername@host形式で指定します。このコマンドには-lオプションがありません。

正しいパスワードを入力すると、scpによりデータ転送が開始され、進行状況バーをシミュレートする一連のアスタリスクが表示されます。また、進行状況バーの右端への到達予想時間も表示されます。すべての出力を抑制するには、オプション-qを指定します。

scpには、ディレクトリ全体の再帰コピー機能も用意されています。コマンドscp -r src/ sun:backup/を入力すると、ディレクトリsrcの内容全体がすべてのサブディレクトリを含めてホストsun上のbackupディレクトリにコピーされます。このサブディレクトリが存在しない場合は、自動的に作成されます。

オプション-pはscpに対して、変更のないファイルのタイムスタンプを残すように指示します。-Cを指定するとデータ転送が圧縮されます。この場合、データ転送量は最小限ですみますが、プロセッサにかかる負荷が大きくなります。

23.2.4 sftp—安全なファイル転送

安全なファイル転送のために、scpの代わりにsftpプログラムを使用できます。sftpセッション中は、ftpで認識される多数のコマンドを使用できます。特にファイル名がわからないデータを転送する場合に、sftpプログラムはscpよりも優れた選択肢です。

23.2.5 SSHデーモン(sshd)—サーバ側

SSHのクライアントプログラムであるsshおよびscpを操作する場合は、サーバであるSSHデーモンをバックグラウンドで実行し、TCP/IP port 22で接続をリスンする必要があります。このデーモンは、初回起動時に鍵のペアを3組生成します。鍵のペアはそれぞれ、秘密鍵と公開鍵で構成されます。そのため、このプロシージャは公開鍵ベースと呼ばれます。SSHを介した通信のセキュリティを保証するために、秘密鍵ファイルへのアクセスはシステム管理者に限定する必要があります。ファイルアクセス権は、デフォルトインストールにより適切に設定されます。秘密鍵はSSHデーモンでローカルにのみ必要であり、他人には付与しないでください。公開鍵コンポーネント(拡張子.pub

で識別)は、接続を要求しているクライアントに送信されます。これは、ユーザ全員が読み込み可能です。

接続はSSHクライアントにより開始されます。待機中のSSHデーモンと要求側のSSHクライアントは、プロトコルとソフトウェアのバージョンを比較して不正なポートを介した接続を防止するために、識別データを交換します。オリジナルのSSHデーモンの子プロセスが要求に応答するため、同時に複数のSSH接続を確立できます。

SSHサーバとSSHクライアントとの通信の場合、OpenSSHはバージョン1および、2のSSHプロトコルをサポートします。新規にインストールされたSUSE Linuxシステムは、デフォルトでバージョン2に設定されます。更新後も引き続きバージョン1を使用する場合は、/usr/share/doc/packages/openssh/README.SuSE内の指示に従ってください。このドキュメントには、SSH 1環境を数ステップでSSH 2作業環境に変換する方法も含まれています。

バージョン1のSSHを使用する場合、サーバはホスト公開鍵とSSHデーモンにより1時間ごとに再生成されるサーバ鍵を送信します。この両方を使用すると、SSHクライアントは自由に選択したセッション鍵を暗号化でき、この鍵がSSHサーバに送られます。また、SSHクライアントはサーバに対して、どの暗号化方式(暗号)を使用するかも指示します。

バージョン2のSSHプロトコルはサーバ鍵を必要としません。クライアント側とサーバ側は、Diffie-Helmanのアルゴリズムを使用して鍵を交換します。

セッション鍵を復号化するにはホストとサーバの秘密鍵が不可欠であり、公開部分からは導出できません。秘密鍵を使用してセッション鍵を復号化できるのは、接続相手のSSHデーモンのみです(man /usr/share/doc/packages/openssh/RFC.nroffコマンドでマニュアルページを参照してください)。この初期接続フェーズは、SSHクライアントの詳細デバッグオプション–vをオンにすると緊密に監視できます。

デフォルトではバージョン2のSSHプロトコルが使用されます。バージョン1のプロトコルを使用するには、–1スイッチを指定してこの設定を上書きします。クライアントでは、すべてのホスト公開鍵がリモートホストとの初期接続後に~/.ssh/known_hostsに格納されます。このため、man-in-the-middle攻撃、つまり、外部SSHサーバが他の名前とIPアドレスを偽装して使用しようとする攻撃が防止されます。この種の攻撃は、~/.ssh/known_hostsに含まれていないホスト鍵が使用されたことで検出されるか、適切な秘密鍵がないためにサーバがセッション鍵を復号化できないことで検出されます。

/etc/ssh/に格納された秘密鍵と公開鍵のバックアップを、外部の安全な場所に保管することをお薦めします。これにより、鍵の変更を検出でき、再インストール後は古い鍵を再び使用できます。また、ユーザの動揺を招くような警告を出す必要もなくなります。警告にも関わらず実際には正しいSSHサーバであることが確認された場合は、このシステムに関する既存のエントリを~/.ssh/known_hostsから削除する必要があります。

23.2.6 SSHの認証メカニズム

この時点で実際の認証が発生します。 最も単純な形式の認証は、前述のようにパスワードを入力することからなっています。SSHの目標は、使いやすく安全なソフトウェアを提供することでした。これは、rshおよびrloginにとって代わるという側面もあるため、SSHは日常的な使用に適した認証方式も提供できるようにする必要があります。そのために、SSHはもう1つ、ユーザが生成する鍵のペアを使用します。SSHパッケージには、そのためのヘルパープログラムが用意されています。ssh-keygenです。ssh-keygen -t rsaまたはssh-keygen -t dsaを入力すると鍵のペアが生成され、鍵を格納するベースファイルの名前を求めるプロンプトが表示されます。

デフォルト設定を確認し、パスフレーズ要求に応答します。 ソフトウェアから空のパスフレーズが提示された場合も、ここで説明する手順には10〜30文字のテキストを使用することをお勧めします。短くて単純な語句は使用しないでください。また、パスフレーズを再入力して確認してください。その後、秘密鍵と公開鍵の格納場所(この例ではファイルid_rsaおよびid_rsa.pub)が表示されます。

古いパスフレーズを変更するには、ssh-keygen -p -t rsaまたはssh-keygen -p -t dsaを使用します。公開鍵コンポーネント(この例ではid_rsa.pubファイル)をリモートマシンにコピーし、~/.ssh/authorized_keysファイルに保存します。次回の接続確立時には、パスフレーズで自己認証するように要求されます。このプロンプトが表示されない場合は、これらのファイルの位置と内容を確認してください。

長時間実行する場合、この手順はその都度パスワードを入力するよりも煩雑です。そのため、SSHパッケージにはssh-agentというツールが用意されており、Xセッションの存続期間中は秘密鍵が保持されます。Xセッション全体はssh-agentの子プロセスとして開始されます。この場合に最も簡単な方法は、.xsessionファイルの先頭にある変数usesshをyesに設定し、KDMやXDM

などのディスプレイマネージャを介してログインすることです。また、`ssh-agent startx`と入力する方法もあります。

これで、sshまたはscpを通常どおり使用できます。前述のように公開鍵を配布している場合、パスワードを求めるプロンプトは表示されなくなります。Xセッションを終了するか、xlockなどのパスワード保護アプリケーションでロックすることに注意してください。

バージョン2のSSHプロトコル導入に関連する変更は、すべてファイル`/usr/share/doc/packages/openssh/README.SuSE`にも記載されています。

23.2.7 X、認証および転送メカニズム

前述したセキュリティ関連の改善に加えて、SSHを使用するとリモートXアプリケーションの使用も簡略化されます。オプション`-X`を指定して`ssh`を実行すると、リモートマシン上でDISPLAY変数が自動的に設定され、すべてのX出力が既存のSSH接続を介してリモートマシンにエクスポートされます。それと同時に、権限のないユーザは、この方法でリモートで起動してローカルに表示していたXアプリケーションのパケットを盗聴できなくなります。

オプション`-A`を追加すると、ssh-agentの認証メカニズムが次のマシンに繰り越されます。これにより、事前に接続先ホストに公開鍵を配布してそこで適切に保存している場合にのみ、パスワードを入力しなくても様々なマシンから作業できます。

デフォルト設定では両方のメカニズムが無効になっていますが、システム単位の設定ファイル`/etc/ssh/sshd_config`またはユーザの`~/.ssh/config`ファイル内でいつでも永続的に有効にすることができます。

sshを使用してTCP/IP接続をリダイレクトすることもできます。次の例では、SSHに対してそれぞれSMTPポートとPOP3ポートをリダイレクトするように指定しています。

```
ssh -L 25:sun:25 earth
```

このコマンドを使用すると、earthのport 25 (SMTP)に送られた接続は、すべて暗号化チャネルを介してsunのSMTPポートにリダイレクトされます。これが特に役立つのは、SMTP-AUTHまたはPOP-before-SMTP機能のないSMTPサーバを使用する場合です。ネットワークに接続している任意の場所から「ホーム」メールサーバに電子メールを転送して配信できます。 同様に、次のコマ

ンドを使用すると、earth上のすべてのPOP3要求(ポート110)をsunのPOP3ポートに転送できます。

```
ssh -L 110:sun:110 earth
```

どちらのコマンドも、権限付きのローカルポートに接続するためrootユーザで実行する必要があります。電子メールは、既存のSSH接続で標準ユーザにより送受信されます。これを機能させるには、SMTPとPOP3のホストをlocalhostに設定する必要があります。追加情報は、前述の各プログラムのマニュアルページおよび/usr/share/doc/packages/openssshにある該当ファイルを参照してください。

23.3 パーティションとファイルの暗号化

どのユーザも、第三者がアクセスできないようにするべき機密データを持っています。 接続環境やモバイル環境が充実すればするほど、データの取り扱いに細心の注意を払わなければならなくなります。 他の人がネットワーク接続によるアクセスや直接の物理的アクセスを行える場合には、ファイルまたはパーティション全体を暗号化することをお勧めします。

警告: メディアの暗号化による保護には限界がある

このセクションで説明している方法を使用しても、運用しているシステムを危険から保護できるわけではないことに注意してください。 暗号化されたメディアが正常にマウントされると、適切なパーミッションを持つ人なら誰でもそれにアクセスできます。 暗号化が意味を持つのは、コンピュータを紛失するか盗まれて、権限のない人物が機密のデータを読み出そうとする場合です。

以下に、想定される使用状況をいくつか挙げます。

ラップトップ
ラップトップを携えて出張する場合は、ハードディスク上の機密データを格納するパーティションを暗号化するとよいでしょう。 データは暗号化ファイルシステムまたは1つの暗号化ファイル内にあるため、ラップトップの紛失や盗難の際にアクセスされる心配はありません。

リムーバブルメディア
USBフラッシュドライブや外付けハードディスクには、ラップトップと同様、盗難の危険があります。ファイルシステムを暗号化すれば、第三者によるアクセスから保護できます。

ワークステーション
自分のコンピュータにほとんど誰でもアクセスできるような会社では、パーティションや単一のファイルを暗号化することには意味があります。

23.3.1 YaSTによる暗号ファイルシステムのセットアップ

を使用して、インストール時に、またはインストール済みのシステムで、ファイルやパーティションを暗号化できます。 暗号化ファイルは既存のパーティションレイアウトにうまく組み込めるので、いつでも作成できます。パーティション全体を暗号化するには、パーティションレイアウト内に暗号化用の専用パーティションが必要になります。ただし、によって提示されるデフォルトの標準パーティション設定には、暗号化パーティションは含まれていません。暗号化パーティションは、パーティション設定用のダイアログで手動で設定します。

インストール時の暗号化パーティションの作成

警告: パスワード入力

暗号化パーティションのパスワードを設定する際は、パスワードのセキュリティに関する警告をよく読み、パスワードをきちんと記憶してください。パスワードがないと、暗号化したデータのアクセスや復元を行えなくなります。

YaSTの［Expert Patitioner］ダイアログ(項「パーティション分割ツール」 (章 3. *YaST*でのシステム設定, ↑起動)を参照)には、暗号化パーティションの作成に必要なオプションが用意されています。通常のパーティションを作成するときと同様、［*作成*］をクリックします。表示されるダイアログで、フォーマット方式、マウントポイントなど、新しいパーティションのパーティションパラメータを指定します。［*Encrypt File System*］をクリックして暗号化パーティションを作成します。次のダイアログで、パスワードを2回入力します。

パーティション作成ダイアログで［*了解*］をクリックすると、新しい暗号化パーティションが作成されます。ブート時に、オペレーティングシステムは、そのパーティションをマウントする前にパスワードを要求します。

起動時に暗号化パーティションをマウントしたくない場合は、パスワードの入力が求められたときにEnterキーを押します。その後、再度パスワードの入力が求められたらそれを拒否します。 この場合、暗号化されたファイルシステムはマウントされません。オペレーティングシステムはブートを続けますが、データへのアクセスは遮断します。パーティションは、いったんマウントされるとすべてのユーザが使用できるようになります。

必要な場合にのみ暗号化ファイルシステムをマウントするには、［*Fstabのオプション*］ダイアログの［*システムスタート時にマウントしない*］をオンにします。 そのパーティションは、システムのブート時にはマウントされなくなります。その後、そのパーティションを使用可能にするには、`mount` *`name_of_partition mount_point`*を実行して手動でマウントします。要求されたときにはパスワードを入力してください。 そのパーティションでの作業を終えたら、`umount name_of_partition`を実行してアンマウントし、他のユーザからアクセスされないようにします。

稼動中のシステムでの暗号化パーティションの作成

警告: 稼動中のシステムでの暗号化のアクティブ化

インストール時と同様に、稼動中のシステムに暗号化パーティションを作成することもできます。ただし、既存のパーティションを暗号化すると、そのパーティションの格納データはすべて失われます。

稼動しているシステムのYaSTコントロールセンターで、*[システム]* → *[ディスクの分割]*の順に選択します。［*はい*］をクリックして続行します。先ほどの［*作成*］ではなく、［*編集*］をクリックします。以降の手順は同じです。

暗号化ファイルのインストール

パーティションの使用の代わりに、単一のファイル内に機密データを保持する暗号化ファイルシステムを作成することもできます。 暗号化ファイルシステムの作成にも同じYaSTダイアログを使用します。［*暗号化ファイル*］を選択し、作成するファイルのパスを予定サイズとともに入力します。フォーマッ

ト設定およびファイルシステム種別については、提示される設定をそのまま使用します。 次に、マウントポイントを指定し、その暗号化ファイルシステムをブート時にマウントするかどうかを指定します。

暗号化ファイルの長所は、ハードディスクのパーティショニング操作を行わなくても追加できるという点です。 暗号化ファイルは、ループデバイスを活用してマウントされ、通常のパーティションのように動作します。

viを使用したファイルの暗号化

暗号化パーティションの短所は、パーティションをマウントしている間、少なくともrootはデータにアクセスできるという点です。 このことを防ぐため、viを暗号化モードで使用することができます。

`vi -x` *`filename`*を使用して新しいファイルを編集します。 viはパスワードの設定を促し、その後ファイルの内容を暗号化します。 このファイルにアクセスするたびに、viは正しいパスワードを要求します。

さらにセキュリティを向上させるため、暗号化されたファイルを暗号化されたパーティションに置くことができます。 viによる暗号化はそれほど強力ではないので、このことが勧められます。

23.3.2 リムーバブルメディアの内容の暗号化

YaSTは、リムーバブルメディアを外部ハードディスクと同様に扱い、USBフラッシュドライブを他のハードディスクと同様に扱います。 これらのメディアのファイルやパーティションは、前述の方法で暗号化することができます。しかし、これらのメディアをシステムのブート時にマウントするようには選択しないでください。これらは通常、システムの実行中にのみ接続するからです。

23.4 セキュリティと機密性

LinuxまたはUNIXシステムの主な特性は、同時に複数のユーザを処理できること(マルチユーザ)と、これらのユーザが同じコンピュータ上で同時に複数の

タスクを実行できること(マルチタスキング)です。さらに、オペレーティングシステムはネットワークを意識させません。通常、ユーザは自分が使用しているデータやアプリケーションが各自のマシンからローカルに提供されているのか、ネットワークを介して使用可能になっているかを意識することはありません。

マルチユーザ機能を使用する場合、様々なユーザのデータを別々に格納する必要があります。また、セキュリティとプライバシーを保証する必要があります。データのセキュリティは、コンピュータをネットワーク経由でリンクできるようになる以前から、すでに重要な問題になっていました。現在と同様に、最重要課題は、データメディア(ほとんどの場合はハードディスク)が消失したり他の方法で破損した場合にも、データを使用可能な状態で維持する機能でした。

この章では、主として機密性の問題とユーザのプライバシーを保護する手段について重点的に説明します。ただし、定期的に更新されて作業可能なテスト済みバックアップを常に備えておくための手順を確立することが包括的なセキュリティの概念には不可欠であるという点については、詳しく説明しません。この手順がなければ、何らかのハードウェア障害が発生した場合のみでなく、誰かが不正にアクセスしてファイルを改ざんしたという疑いが生じた場合にも、データの復旧作業に手間と時間がかかることになります。

23.4.1 ローカルセキュリティとネットワークセキュリティ

データにアクセスするには、次のような複数の方法があります。

- 必要な情報を持っているユーザとの個人的な通信、またはコンピュータ上のデータへのアクセス
- コンピュータのコンソールからの直接アクセス(物理アクセス)
- シリアル回線を介したアクセス
- ネットワークリンクを使用したアクセス

いずれの場合も、ユーザが問題のリソースやデータにアクセスするには、認証を受ける必要があります。この点ではWebサーバはあまり限定的ではあり

ませんが、すべての個人データを第三者に公開しないようにする必要はあります。

上記のリストのうち、最初の項目では、銀行の担当者に連絡したときに自分が口座名義人であるという証明を要求される場合のように、多くの対話を必要とします。この場合は、署名、PINまたはパスワードなど、自分の身元を証明する情報を提供するように要求されます。場合によっては、単に知っている情報を断片的に述べ、言葉巧みに信頼させて相手から情報を引き出す可能性もあります。その結果、情報が少しずつ明らかになり、そのことに気づかないことさえあります。ハッカーの間では、この行為を「ソーシャルエンジニアリング」と呼んでいます。この行為を防止するには、人々を教育し、言語や情報を自覚して取り扱うしかありません。通常、攻撃者はコンピュータシステムに侵入する前に、受付係、会社のサービススタッフ、家族などをターゲットにしようとします。多くの場合、このようなソーシャルエンジニアリングに基づく攻撃は、はるか後になるまで発見されません。

他人のデータに不正にアクセスしようとする第三者は、従来の方法を使用して他人のハードウェアに直接接続を試みることもあります。そのため、マシンは他人にコンポーネントを削除、交換または無効化されないように、あらゆる改ざんから保護する必要があります。これは、バックアップ、ネットワークケーブル、電源コードにも当てはまります。また、一部のキーの組合せは異常動作を引き起こす場合があるため、ブート手順も保護してください。自己防衛のためには、BIOSとブートローダーのパスワードを設定する必要があります。

シリアルポートに接続されたシリアル端末は、従来から多くの場所で使用されています。ネットワークインタフェースとは異なり、ホストとの通信をネットワークプロトコルに依存しません。デバイス間での単なる文字のやりとりには、単純なケーブルまたは赤外線ポートが使用されます。このようなシステムでは、ケーブル自体が最大の弱点です。古いプリンタがケーブルに接続されていれば、ケーブル経由で伝達される情報を記録するのは簡単です。攻撃対象によっては、プリンタで実行できることであれば他の方法でも実行できます。

ホスト上でファイルをローカルに読み込むには、他のホスト上でサーバとのネットワーク接続をオープンする以外のアクセスルールが必要です。ローカルセキュリティとネットワークセキュリティには、違いがあります。つまり、データをどこかにパケット単位で送信する必要がある場合には、回線が使用されます。

ローカルセキュリティ

ローカルセキュリティは、コンピュータが稼働している場所の物理環境から始まります。マシンは、セキュリティ上の要件やニーズに沿った場所に設置してください。ローカルセキュリティの主な目標は、誰も他人の権限や識別情報を偽れないように、常にユーザを相互に分離しておくことです。これは遵守すべき原則ですが、ユーザ`root`の場合はシステム上で最高の権限を持つため、このことが特に重要になります。`root`ユーザは、パスワードを求めるプロンプトなしで、他のすべてのローカルユーザの識別情報を使用して、ローカルに格納されているファイルをすべて読み込むことができます。

パスワード

Linuxシステムでは、パスワードが平文として格納されることはなく、入力されたテキスト文字列が保存されているパターンと単に照合されるのでもありません。平文として格納され、保存されているパターンと照合されるのみであれば、対応するファイルに誰かがアクセスした直後に、システム上のすべてのアカウントが危険にさらされることになります。代わりに、格納されているパスワードは暗号化されており、入力されるパスワードもそのたびに再び暗号化され、暗号化された2つの文字列が比較されます。この方法でセキュリティレベルが向上するのは、暗号化されたパスワードを逆算して元のテキスト文字列に戻せない場合のみです。

実際には、この処理は特殊なアルゴリズムによって達成されます。このアルゴリズムは、一方向にしか機能しないため、「*トラップドアアルゴリズム*」とも呼ばれます。暗号化された文字列を攻撃者が入手しても、単に同じアルゴリズムを再適用するだけでは他人のパスワードを取得できません。代わりに、暗号化すると他人のパスワードになる組合せが見つかるまで、考えられる文字の組合せをすべてテストする必要があります。パスワードが長さ8文字であれば、計算が必要な組合せの候補は膨大な数になります。

1970年代には、使用されていたアルゴリズムが比較的低速で、1つのパスワードを暗号化するだけで数秒かかっていたため、この方法が他の方法よりも安全であると言われていました。ただし、その後はPCのパフォーマンスが向上し、毎秒数10万～数100万回の暗号化を実行できるようになっています。このため、暗号化されたパスワードは通常のユーザが参照できないようにする必要があります(通常のユーザは`/etc/shadow`ファイルを読み込めません)。さらに重要なのは、何らかのエラーが原因でパスワードファイルが参照可能になった場合に備えて、簡単に推測できないパスワードを使用することです。

したがって、「tantalise」のようなパスワードを「t@nt@1ls3」に「変換」したとしても、実際には役に立ちません。

語句の一部の文字を数字に同じパターンで置き換えただけでは、安全とは言えません。辞書を使用して語句を推測するパスワードクラックプログラムも、これと同様の置換を行います。そこで、「The Name of the Rose」 by Umbert Eco(ウンベルトエーコ著『薔薇の名前』)のように、文や書名に含まれる語句の頭文字など、一般的な意味はなく、自分にしか意味のない語句を作成するのが適切な方法です。こうして作成される次のようなパスワードは安全と言えます。「TNotRbUE9」。これに対して、「beerbuddy」や「jasmine76」のようなパスワードは、ユーザに関してわずかしか知識のない他人でさえ簡単に推測できます。

ブート手順

システムは、ドライブ全体を取り外すか、BIOSパスワードを設定してハードディスクからでなければブートできないようにBIOSを設定し、フロッピーやCDからはブートできないように設定してください。通常、Linuxシステムはブートローダーから起動するため、ブートしたカーネルに追加のオプションを渡すことができます。`/boot/grub/menu.lst`内でパスワードを追加設定し、他のユーザがこの種のパラメータをブート時に使用できないようにしてください(章 29. ブートローダ (page 473)を参照)。これはシステムのセキュリティに不可欠です。カーネル自体が`root`権限で実行されるのみでなく、システム起動時に`root`権限を付与する最初の認可でもあります。

ファイルのパーミッション

通常は、特定のタスクに可能な最も限定的な権限で作業します。たとえば、電子メールを読み書きするには、`root`ユーザである必要はありません。メールプログラムにバグがあると、このバグが攻撃にさらされ、起動時にプログラムのパーミッションが正確に処理されてしまう可能性があります。限定的な権限のルールに従って、考えられる損害を最小限に抑えてください。

SUSEのディストリビューションパッケージに付属する200,000以上のファイルについては、パーミッションが慎重に選択されています。ソフトウェアや他のファイルを追加インストールするシステム管理者は、特にパーミッションビットの設定時には細心の注意を払う必要があります。経験豊富でセキュリティ意識の高いシステム管理者は、常にコマンド`ls`で`-l`オプションを使用し

て広範なファイルリストを取得します。これにより、不正なファイルパーミッションを即時に検出できます。不正なファイル属性は、そのファイルが変更または削除された可能性を意味するだけではありません。このように変更されたファイルがrootユーザにより実行される可能性や、設定ファイルの場合はこの種のファイルがプログラムでrootユーザの権限で使用される可能性があります。このため、攻撃者が侵入する可能性が大幅に増大します。このような攻撃は、カッコウが他の鳥をだまして自分の卵を孵化させるのと同様に、プログラム(卵)が他のユーザ(鳥)によって実行(孵化)されるため、カッコウの卵と呼ばれます。

SUSE Linuxシステムでは、ファイルpermissions、permissions.easy、permissions.secure、およびpermissions.paranoidがすべてディレクトリ/etcにあります。これらのファイルの目的は、world-writableなディレクトリなどの特殊な権限や、ファイルに対するsetuser IDビットを定義することです(setuser IDビットが設定されているプログラムは、それを起動したユーザの権限ではなく、ファイル所有者、ほとんどの場合はrootユーザの権限で実行されます)。管理者は、ファイル/etc/permissions.localを使用して自分専用の設定を追加できます。

前述のファイルのうち、SUSEの設定プログラムで権限の設定に使用されるファイルを定義するには、YaSTで[セキュリティ]を選択します。このトピックの詳細は、/etc/permissions内のコメントまたはchmodのマニュアルページを(manchmodコマンドを実行して)参照してください。

バッファオーバーフローと書式文字列のバグ

プログラムがユーザによる変更が可能なデータを処理すると思われる場合は、特に注意する必要がありますが、これは通常のユーザよりもアプリケーションプログラマにとって問題です。 プログラマは、小さすぎてデータを保持できないメモリ領域に書き込むことなく、自分のアプリケーションでデータが適切に解析されることを確認する必要があります。また、プログラムでは、専用に定義されたインタフェースを使用して、データを一貫した方法で受け渡す必要があります。

実際のメモリバッファのサイズを考慮しないと、そのバッファへの書き込み時に「バッファオーバーフロー」が発生する可能性があります。また、このデータ(ユーザが生成)に使用される領域が、バッファ内で使用可能な領域を超える場合があります。その結果、データはそのバッファ領域の終わりを超えて書き込まれ、状況によってはプログラムで単にユーザデータが処理される

のではなく、ユーザ(プログラマではなく)が変更したプログラムシーケンスが実行される可能性があります。この種のバグは、特にプログラムが特殊な権限で実行されている場合には、重大な結果を招きます(ファイルのパーミッション項 (page 368)を参照)。

*書式文字列*のバグの場合、動作は少し異なりますが、プログラムの異常動作を引き起こす可能性のあるユーザ入力です。ほとんどの場合、この種のプログラミングエラーは、setuidプログラムやsetgidプログラムなど、特殊な権限で実行されるプログラムに見られます。これも、対応する実行権限をプログラムから削除することで、データとシステムをこの種のバグから保護できることを意味します。また、最善の方法は、考えられる最小権限を使用するというポリシーを適用することです(ファイルのパーミッション項 (page 368)を参照)。

バッファオーバーフローと書式文字列のバグがユーザデータの処理に関連するバグであるとすれば、アクセス権がローカルアカウントに付与されている場合にのみ発生するわけではありません。レポートされているバグの多くは、ネットワークリンク上でも利用される可能性があります。したがって、バッファオーバーフローと書式文字列のバグは、ローカルセキュリティとネットワークセキュリティの両方に関連する問題として分類する必要があります。

ウィルス

通説とは異なり、Linux上で動作するウィルスは存在します。ただし、判明しているウィルスは、テクニックが意図したとおりに動作することを証明するために、作成者が*自分のアイデアの証明*としてリリースしたものです。この種のウィルスは、これまでのところいずれも*一般には*検出されていません。

ウィルスは、活動するホストがなければ存続も拡散もできません。たとえば、ホストがプログラムやシステムの重要な記憶領域(マスターブートレコードなど)であり、そこにウィルスのプログラムコードを書き込む必要があるとします。Linuxにはマルチユーザ機能があるため、特定のファイルへの書き込みアクセスを制限でき、これは特にシステムファイルの場合に重要です。したがって、`root`権限で通常の作業を実行すると、システムがウィルスに感染する可能性が増大します。これに対して、考えられる最小権限を使用するという原則に従えば、ウィルスに感染する可能性は低下します。

それとは別に、実際には知らないインターネットサイトからはプログラムを実行しないようにする必要があります。のRPMパッケージは、その作成に必要な措置が講じられたデジタルラベルとして暗号署名を使用します。ウィル

スは、管理者やユーザにセキュリティに関して必要な自覚が欠けており、設計によって高度に保護されているシステムであっても危険にさらす可能性があることを示す典型的な兆候です。

ウィルスをワームと混同しないようにする必要があります。ワームの対象はネットワーク全体です。ワームの拡散にはホストを必要としません。

ネットワークセキュリティ

ネットワークセキュリティは、外部で開始される攻撃から保護する場合に重要です。ユーザ認証にユーザ名とパスワードを必要とする典型的なログイン手順は、ローカルセキュリティの課題です。ネットワーク経由の特殊なログインの場合は、2つのセキュリティの課題を区別してください。実際の認証までに発生する処理はネットワークセキュリティに関連し、その後に発生する処理はローカルセキュリティに関連します。

X Window SystemとX認証

冒頭に述べたように、ネットワーク透過性は、UNIXシステムの中核的な特性の1つです。UNIXオペレーティングシステムのウィンドウシステムであるXは、この機能を優れた方法で実現します。Xを使用すると、リモートホストでログインしてグラフィカルプログラムを起動しても基本的には問題はなく、グラフィカルプログラムはネットワーク経由で送信されてコンピュータに表示されます。

Xサーバを使用してXクライアントをリモートで表示する必要がある場合、Xサーバは管理対象のリソース(ディスプレイ)を不正アクセスから保護する必要があります。より厳密には、クライアントプログラムに特定の権限を付与する必要があります。X Window Systemでは、この権限付与を ホストベースのアクセスコントロールおよびCookieベースのアクセスコントロールと呼ばれる2通りの方法で実行できます。前者は、クライアントが実行されるホストのIPアドレスに依存します。これを制御するプログラムがxhostです。xhostは正当なクライアントのIPアドレスをXサーバに属する小型データベースに入力します。ただし、認証はIPアドレスに依存するため、安全度は高くありません。たとえば、クライアントプログラムを送信中のホストで第2のユーザが作業している場合、そのユーザはXサーバにもアクセスできます。IPアドレスを盗む第三者はこれと同じことをしているに過ぎません。このような欠点があるため、ここではこの認証方式について詳述しません。詳細は、`man xhost`を参照してください。

Cookieベースのアクセスコントロールの場合は、ある種のIDカードと同様に、Xサーバと正当なユーザにのみ認識される文字列が生成されます。このCookie(通常のクッキーを意味するのではなく、エピグラムが入っている中国のフォーチュンクッキー)は、ログイン時にユーザのホームディレクトリのファイル.Xauthorityに格納され、Xサーバを使用してウィンドウを表示しようとするすべてのXクライアントで使用できます。ファイル.Xauthorityは、ユーザがツールxauthを使用して検査できます。.Xauthorityの名前を変更したり、意図せずにホームディレクトリから削除すると、新規のウィンドウやXクライアントをオープンできなくなります。 X Window Systemのセキュリティメカニズムの詳細は、Xsecurityのmanページを参照してください(man Xsecurity)。

SSH(セキュアシェル)を使用すると、ユーザには暗号化メカニズムを意識させることなく、ネットワーク接続を完全に暗号化してXサーバに透過的に転送(フォーワード)することができます。この処理は「X転送」とも呼ばれます。X転送は、サーバ側でXサーバをシミュレートし、リモートホスト上でシェルのDISPLAY変数を設定することで行われます。SSHについての詳細な情報は項23.2. 「SSH:安全なネットワーク操作」 (page 355)を参照してください。

警告

ログイン先のホストに対して、ホストの保護を考慮していない場合は、X転送を使用しないでください。X転送を有効にすると、攻撃者がユーザのSSH接続を介して認証し、Xサーバに侵入し、ユーザになりすましてキーボード入力などを行う可能性があります。

バッファオーバーフローと書式文字列のバグ

バッファオーバーフローと書式文字列のバグ項 (page 369)で説明したように、バッファオーバーフローと書式文字列のバグは、ローカルセキュリティとネットワークセキュリティの両方に関係する課題として分類する必要があります。この種のバグのローカルバリエーションと同様に、ネットワークプログラムでのバッファオーバーフローは、首尾よく利用されてしまうと、ほとんどの場合はrootの権限の取得に使用されます。それ以外の場合にも、攻撃者がバグを利用して権限のないローカルアカウントにアクセスし、システムに存在する他の脆弱部分を利用する可能性があります。

ネットワークリンク経由で利用される恐れのあるバッファオーバーフローと書式文字列のバグは、リモート攻撃全体で最も頻度の高い形式であることは

確実です。これらのセキュリティ上の弱点(これらの新しく見つかったセキュリティホールを攻撃するためのプログラム)はしばしばセキュリティ関連のメーリングリストに投稿されます。この情報を使用すると、コードの詳細を知らなくても脆弱部分を絞り込むことができます。多年の経験では、オペレーティングシステムメーカーは自社ソフトウェアの問題を修正せざるを得ないため、悪用可能なコードを知ることがオペレーティングシステムのセキュリティレベル向上に役立つことが判明しています。無償ソフトウェアを使用すれば、誰でもソースコードにアクセスでき(の場合は、ソースコードがすべて使用可能です)、脆弱部分とその悪用可能なコードを見つけたユーザは誰でも、対応するバグ修正のためのパッチを発行できます。

Denial of Service

サービス拒否(denial of service、DoS)攻撃の目的はサーバプログラムやシステム全体をブロックしてしまうことです。これを実行するには次のような様々な手段があります。サーバのオーバーロード、ガベージパケットによって絶えずビジー状態にする、リモートバッファオーバーフローを利用するなどがあげられます。 通常、DoS攻撃はサービスの消失のみを目的として実行されます。ただし、特定のサービスが使用不能になると、*man-in-the-middle*攻撃(パケット盗聴、TCP接続のハイジャック、偽装攻撃)やDNSポイゾニングなどに対して脆弱になる可能性があります。

Man in the Middle:パケット盗聴、ハイジャック、偽装攻撃

一般に、通信中のホスト間に割り込む攻撃者が実行するリモート攻撃は、「*man-in-the-middle*攻撃」と呼ばれます。ほぼすべてのタイプのman-in-the-middle攻撃に共通するのは、通常、ユーザは何が起きているのかに気づかないことです。 攻撃者が接続要求をターゲットマシン宛てに転送するなど、様々なバリエーションが考えられます。その場合、相手のマシンは有効な接続先マシンであるかのように偽装されているので、知らないうちに不正なホストとの接続が確立されることになります。

最も単純なタイプのman-in-the-middle攻撃は*sniffer*と呼ばれ、攻撃者はネットワークトラフィックをリスンするだけです。より複雑な「man in the middle」攻撃は、すでに確立された接続を乗っ取ろうとします(ハイジャック)。これを実現するため、攻撃者は一定時間だけパケットを分析し、接続に属するTCPシーケンス番号を予測できる必要があります。攻撃者が最終的にターゲット

ホストのロールを停止すると、エラーのため接続が終了したことを示すエラーメッセージが表示されるため、このことがわかります。暗号化を介してハイジャックから保護されるプロトコルはなく、接続の確立時には単純認証手順しか実行されないことが、攻撃を容易にしています。

*偽装攻撃*は、パケットが偽のソースデータ(通常はIPアドレス)を含むように変更される攻撃です。攻撃に利用させる手段の多くは偽のパケット(Linuxマシンではスーパーユーザである`root`のみしか実行できないようなパケット)を送りつける方法です。

前述の攻撃の多くは、DoSと組み合わせて実行されます。特定のホストを短時間でも突然停止できることが攻撃者にわかれば、ホストは攻撃で一定時間は干渉できなくなるため、攻撃者は容易にアクティブ攻撃をかけられるようになります。

DNSポイゾニング

DNSポイゾニングとは、攻撃者が偽装したDNSリプライパケットで応答し、サーバの情報を要求しているユーザに対して、そのサーバから特定のデータを送信するよう試みることにより、DNSサーバのキャッシュを破壊することを意味します。多くのサーバは、IPアドレスまたはホスト名に基づいて他のホストとの信頼関係を維持しています。攻撃者は、ホスト間の信頼関係の実際の構造を詳細に理解した上で、自分を信頼のおけるホストの1つとして偽装する必要があります。通常、攻撃者はサーバから受信した一部のパケットを分析し、必要な情報を取得します。また、しばしば攻撃者はネームサーバも適切なタイミングによるDoS攻撃のターゲットとする必要があります。接続先ホストの識別情報を確認できる、暗号化された接続を使用することで、自分自身を保護してください。

ワーム

ワームはしばしばウィルスと混同されますが、両者には明らかな違いがあります。ウィルスとは異なり、ワームはホストプログラムに感染しなくても活動できます。 代わりに、ネットワーク構造上でできるだけ迅速に拡散するように特化されています。Ramen、Lion、Adoreなど、これまでに出現したワームは、bind8やlprNGなどのサーバプログラムの周知のセキュリティホールを使用しています。ワームからの保護は、比較的容易です。セキュリティホールが検出されてからワームがサーバに侵入するまでにある程度の時間があれば、影響を受けるプログラムの更新バージョンが間に合う可能性が大きくな

ります。これが役立つのは、管理者が問題のシステムにセキュリティ更新を実際にインストールする場合のみです。

23.4.2 セキュリティ全般のヒントとテクニック

セキュリティの問題に適切に対処するには、新規の開発に遅れをとらず、常に最新のセキュリティ問題に関する情報を入手することが重要です。システムをあらゆる種類の問題から保護するために、セキュリティ通知で推奨されているパッケージ更新版をできるだけ迅速に入手してインストールすることをお薦めします。SUSEのセキュリティ通知はメーリングリストで公開されており、リンクhttp://www.novell.com/linux/security/securitysupport.htmlで参加できます。リストsuse-security-announce@suse.deは、パッケージ更新版に関する最初の情報源であり、アクティブな貢献者の中でもSUSEのセキュリティチームのメンバーが含まれています。

メーリングリストsuse-security@suse.deは、必要なセキュリティ問題の説明の参照先として活用できます。 同じWebページから参加してください。

bugtraq@securityfocus.comは、世界中で最もよく知られているセキュリティメーリングリストです。このリストは1日15〜20件を受け付けているため、このリストを参照することをお勧めします。詳細は、http://www.securityfocus.comを参照してください。

ここでは、基本的なセキュリティ問題に対処する上で役立つルールについて説明します。

- ジョブごとに考えられる最も限定的な権限セットを使用するというルールに従い、日常的なジョブはrootユーザで実行しないようにします。これにより、カッコウの卵やウィルスに感染する危険性が減少し、自分自身のミスも防止できます。
- 可能な限り、リモートマシンでの作業には常に暗号化された接続を使用します。telnet、ftp、rshおよびrloginの代わりにssh(セキュアシェル)を使用することを、習慣づけてください。
- IPアドレスのみに基づく認証方式は使用しないでください。

- 最も重要なネットワーク関連パッケージは常に更新し、対応するメーリングリストにサブスクライブして、この種のプログラム(bind、sendmail、sshなど)の新バージョンに関する通知を受け取ります。これは、ローカルセキュリティに関連するソフトウェアの場合も同じです。

- /etc/permissionsファイルを変更し、システムのセキュリティに不可欠なファイルのパーミッションを最適化します。プログラムからsetuidビットを削除すると、そのジョブは意図した方法で実行できなくなる場合があります。一方、ほとんどの場合、プログラムの潜在的なセキュリティリスクもなくなることを考慮してください。同様のアプローチは、world-writableなディレクトリおよびファイルにも適用できます。

- サーバの正常動作に不可欠でないネットワークサービスを停止します。これにより、システムの安全性が向上します。ソケットがLISTEN状態のオープンポートは、プログラムnetstatで検出できます。オプションとして`netstat -ap`または`netstat -anp`を使用することをお薦めします。`-p`オプションを使用すると、指定した名前のポートを使用しているプロセスを確認できます。

  netstatの結果を、ホスト外部から実行したポートスキャンの結果と比較します。このジョブに適したプログラムはnmapで、マシンのポートがチェックされるのみでなく、その背後で待機中のサービスについてもある程度の情報が得られます。ただし、ポートスキャンは攻撃的な行為と解釈される場合があるため、管理者から明示的な承認を受けない限りホスト上では実行しないでください。最後に、TCPポートのみでなくUDPポートも検出することが重要であることを忘れないでください(オプション`-sS`および`-sU`を使用します)。

- システムのファイルの整合性を信頼できる方法で監視するには、SUSE Linuxで利用可能なプログラムAIDE (Advanced Intrusion Detection Environment)を使用します。 他人に改ざんされないように、AIDEで作成されたデータベースは暗号化します。さらに、マシン外部から使用可能なこのデータベースのバックアップは、ネットワークリンクで接続されていない外部データメディアに格納します。

- サードパーティソフトウェアのインストール時には、適切な措置を講じます。幸いにして迅速に発見されたものの、ハッカーがセキュリティソフトウェアパッケージのtarアーカイブにトロイの木馬を組み込んでいた事例があります。バイナリパッケージをインストールする場合は、それをダウンロードしたサイトを信頼します。

SUSEのRPMパッケージにはgpgの署名が付いています。 SUSEが署名に使用している鍵は、次のとおりです。

ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>

Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

コマンド`rpm--checksig package.rpm`を実行すると、アンインストールされたパッケージのチェックサムと署名が正しいかどうかを確認できます。この鍵は、配布パッケージCDの1枚目と、世界中のほとんどのキーサーバにあります。

- ユーザファイルとシステムファイルのバックアップを定期的にチェックします。バックアップが動作するかどうかをテストしなければ、実際には役に立たない可能性があることを考慮してください。
- ログファイルをチェックします。可能な場合は、小型スクリプトを記述して疑わしいエントリを検索します。実際、これは些細な作業ではありません。結局のところ、どのエントリが例外的でどのエントリがそうでないかがわかるのは自分だけです。
- `tcp_wrapper`を使用して、サービスに接続できるIPアドレスを明示的に制御できるように、マシンで実行中の個々のサービスへのアクセスを制限します。 `tcp_wrapper`の詳細は、tcpdおよびhosts_accessのmanページを参照してください(`man 8 tcpd`、`man hosts_access`)。
- SuSEfirewallを使用して、tcpdが提供するセキュリティを強化します(tcp_wrapper)。
- 冗長性のあるセキュリティ対策を設計します。メッセージが2度表示される方が、まったく表示されないよりも有効です。

23.4.3 Central Security Reporting Addressの使用

セキュリティ関連の問題を発見した場合は(まず使用可能な更新パッケージをチェックしてから)、`security@suse.de`に電子メールでお送りください。その際に、問題の詳しい説明と、関係するパッケージのバージョン番号をお知らせください。 SUSEは、できる限り迅速にお答えするように努めていま

す。電子メールメッセージはpgpで暗号化することをお薦めします。 SUSEのpgp鍵は次のとおりです。

```
ID: 3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

この鍵はhttp://www.novell.com/linux/security/securitysupport.htmlからもダウンロードできます。

24 Linuxのアクセス制御リスト

この章では、LinuxファイルシステムのPOSIX ACL(アクセス制御リスト)の背景と機能を簡潔に説明します。ACLは、ファイルシステムオブジェクトに対する従来のパーミッション概念の拡張として使用できます。ACLを使用すれば、従来のパーミッション概念で許されていた以上のパーミッションを柔軟に定義できます。

*POSIX ACL*という用語は、このACLが真のPOSIX(*Portable Operating System Interface*)規格であることを示唆しています。ドラフト規格のPOSIX 1003.1eとPOSIX 1003.2cは、いくつかの理由で白紙に戻されました。それにもかかわらず、UNIXファミリに属している多くのシステムに見られるACLは、これらのドラフト規格に基づいており、この章で説明するファイルシステムACLの実装も同様にこの2つの規格に従っています。これらの規格については、`http://wt.xpilot.org/publications/posix.1e/`を参照してください。

24.1 ACLの利点

従来どおり、Linuxシステムのファイルオブジェクトごとに3セットのパーミッションが定義されます。この3セットには、読み取り(`r`)、書き込み(`w`)、実行(`x`)の各パーミッションがあり、それぞれが3種類のユーザ(ファイル所有者、グループ、その他のユーザ)ごとに設定されます。そのほかに、*ユーザID設定*ビット、*グループID設定*ビット、*スティッキビット*を設定できます。この無駄のない概念は、ほとんどの実際的なケースに十分適しています。ただし、複雑なシナリオまたは高度なアプリケーションの場合、以前は、システム管理者が従来のパーミッション概念の制限を回避するために多くの仕掛けを施す必要がありました。

ACLは、従来のファイルパーミッション概念を拡張する必要がある場合に使用できます。ACLを使用すれば、パーミッションが元の所有者や所有者の所属グループに対応していない場合でも個々のユーザまたはグループにそうしたパーミッションを割り当てることができます。アクセス制御リストは、Linuxカーネルの機能であり、現在ReiserFS、Ext2、Ext3、JFS、およびXFSでサポートされています。ACLを使用すると、アプリケーションレベルで複雑なパーミッションモデルを実装しなくても複雑なシナリオを実現できます。

ACLの利点は、WindowsサーバをLinuxサーバに置き換えるような場合にはっきりします。接続した一部のワークステーションは、移行後も引き続きWindowsの下で動作できます。Linuxシステムは、Sambaを搭載したWindowsクライアントにファイルサービスと印刷サービスを提供します。Sambaがアクセス制御リストをサポートしている場合は、LinuxサーバおよびWindows(Windows NT以降のみ)のどちらでもグラフィカルユーザインタフェースでユーザパーミッションを設定できます。winbinddを使用すれば、Linuxサーバ上にアカウントのない、Windowsドメインにしか存在していないユーザにパーミッションを割り当てることもできます。

24.2 定義

ユーザクラス
: 従来のPOSIXのパーミッション概念では、ファイルシステムでパーミッションを割り当てるための3つのユーザクラス(所有者、所有者の所属グループ、その他のユーザ)が使用されます。読み取り(`r`)、書き込み(`w`)、および実行(`x`)を可能にする3つのパーミッションビットは、ユーザクラスごとに設定できます。

アクセスACL
: あらゆる種類のファイルシステムオブジェクト(ファイルやディレクトリ)のユーザアクセスパーミッションとグループアクセスパーミッションは、アクセスACLによって決定されます。

デフォルトACL

: デフォルトACLは、ディレクトリにしか適用できません。このACLでは、ファイルシステムオブジェクトが作成されたときにその親ディレクトリから継承するパーミッションが決定されます。

ACLエントリ
各ACLは、ACLエントリセットから成ります。ACLエントリには、タイプ(表 24.1. 「ACLエントリタイプ」 (page 382)を参照)、エントリが参照するユーザまたはグループのクォリファイア、およびパーミッションセットが含まれます。一部のエントリタイプの場合、グループまたはユーザのクォリファイアは定義されていません。

24.3 ACLの処理

表 24.1. 「ACLエントリタイプ」 (page 382)に、考えられる6つのACLエントリタイプをまとめています。各エントリで、ユーザまたはユーザグループのパーミッションが定義されます。*所有者*エントリでは、ファイルまたはディレクトリを所有しているユーザのパーミッションが定義されます。*所有者の所属グループ*エントリでは、ファイルの所有者の所属グループのパーミッションが定義されます。スーパーユーザは、`chown`または`chgrp`を使用して所有者または所有者の所属グループを変更できます。その場合、所有者と所有者の所属グループエントリは、新しい所有者と所有者の所属グループを参照します。各*名前付きユーザ*エントリでは、エントリのクォリファイアフィールドで指定されたユーザのパーミッションが定義されます。クォリファイアフィールドとは、表 24.1. 「ACLエントリタイプ」 (page 382)に示すテキスト書式の中央のフィールドのことです。各*名前付きグループ*エントリでは、エントリのクォリファイアフィールドで指定されたグループのパーミッションが定義されます。名前付きユーザと名前付きグループのエントリのクォリファイアフィールドだけが指定されます。*その他*のエントリでは、他のすべてのユーザのパーミッションが定義されます。

マスクエントリでは、*名前付きユーザ*、*名前付きグループ*、および*所有者の所属グループ*のエントリで与えられたパーミッションをさらに制限するために、それらのエントリのパーミッションのどれが有効で、どれをマスクするかが定義されます。パーミッションは、マスク内と同様にこのいずれかのエントリ内にも存在する場合に有効です。マスクだけまたは実際のエントリだけに指定されているパーミッションは有効ではありません。つまり、パーミッションは与えられません。*所有者*と*所有者の所属グループ*のエントリで定義されているすべてのパーミッションは常に有効です。表 24.2. 「アクセスパーミッションのマスキング」 (page 382)の例に、このメカニズムを示しています。

基本的なACLクラスには、次の2つがあります。*最小*ACLには、*所有者*、*所有者の所属グループ*、および*その他*というタイプのエントリだけが含まれます。

これらのエントリは、ファイルやディレクトリの従来のパーミッションビットに対応しています。*拡張*ACLは、このACLを越えるものです。このACLには、マスクエントリが必ず含まれ、*名前付きユーザ*と*名前付きグループ*のタイプのエントリがいくつか含まれている場合があります。

表 24.1 *ACLエントリタイプ*

タイプ	テキスト書式
所有者	`user::rwx`
名前付きユーザ	`user:name:rwx`
所有者の所属グループ	`group::rwx`
名前付きグループ	`group:name:rwx`
マスク	`mask::rwx`
その他	`other::rwx`

表 24.2 *アクセスパーミッションのマスキング*

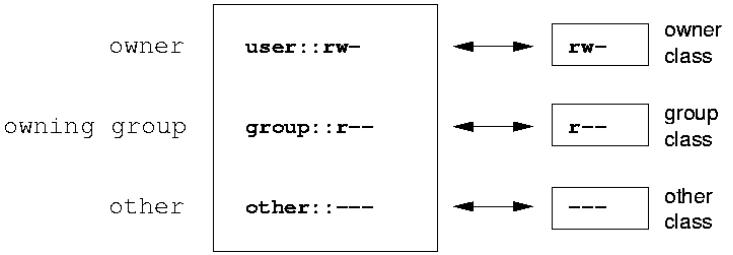
エントリタイプ	テキスト書式	パーミッション
名前付きユーザ	`user:geeko:r-x`	`r-x`
マスク	`mask::rw-`	`rw-`
	有効なパーミッション:	`r--`

24.3.1 ACLエントリとファイルモードのパーミッションビット

図 24.1. 「最小ACL: ACLエントリとパーミッションビットとの比較」 (page 383)と図 24.2. 「拡張ACL: ACLエントリとパーミッションビットとの比較」 (page 383)に、最小ACLと拡張ACLの2つのケースを示しています。図は、3つ

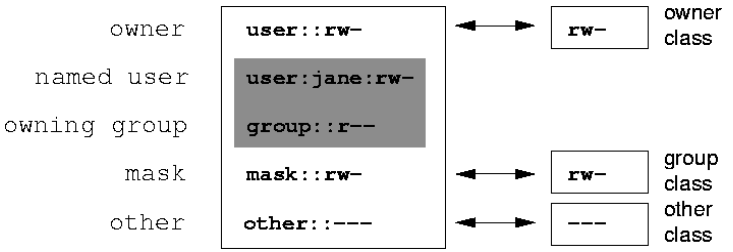
のブロックから成ります。左側のブロックはACLエントリのタイプを示し、中央のブロックはACLの例を示しています。右側のブロックは、従来のパーミッション概念に基くそれぞれのパーミッションビット(`ls -l`などで表示される)を示します。どちらのケースも、*所有者クラス*のパーミッションは、ACLエントリ*所有者*に割り当てられます。*その他のクラス*のパーミッションは、それぞれのACLエントリに割り当てられます。しかし、*グループクラス*のパーミッションの割り当ては、2つのケースで異なります。

図 24.1 *最小ACL: ACLエントリとパーミッションビットとの比較*



最小ACL(マスクなし)の場合、*グループクラス*のパーミッションは、ACLエントリ*所有者の所属グループ*に割り当てられます。このようすを図 24.1.「最小ACL: ACLエントリとパーミッションビットとの比較」 (page 383)に示しています。拡張ACL(マスクあり)の場合、*グループクラス*のパーミッションは、マスクエントリに割り当てられます。このようすを図 24.2.「拡張ACL: ACLエントリとパーミッションビットとの比較」 (page 383)に示しています。

図 24.2 *拡張ACL: ACLエントリとパーミッションビットとの比較*



この割り当て方法により、アプリケーションがACLをサポートしているかどうかにかかわらず、アプリケーションとのスムーズなインタラクションができます。パーミッションビットによって割り当てられたアクセスパーミッションは、ACLで他のすべてのパーミッションを「微調整」する場合の上限を表

します。パーミッションビットの変更は、ACLに反映されます。その逆も同様です。

24.3.2 アクセスACLが設定されたディレクトリ

アクセスACLの処理については、次の例に示します。

ディレクトリを作成する前に、umaskコマンドを使用して、ファイルオブジェクトを作成するたびにどのアクセスパーミッションをマスクする必要があるかを定義します。 コマンドumask 027では、デフォルトパーミッションを設定するために、所有者にすべてのパーミッションを与え(0)、グループ書き込みアクセスを拒否して(2)、その他のユーザにはパーミッションを与えません(7)。 umaskは、実際に対応するパーミッションビットをマスクするか、それらをオフにします。詳細については、対応するmanページ(man umask)を参照してください。

mkdir mydirは、umaskで設定されたデフォルトパーミッションでmydirディレクトリを作成する必要があります。ls -dl mydirを使用して、すべてのパーミッションが正しく割り当てられたかどうかをチェックします。このコマンドの出力例は、次のとおりです。

```
drwxr-x--- ... tux project3 ... mydir
```

getfacl mydirでは、ACLの初期状態をチェックします。このコマンドでは、次のような情報が得れられます。

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

getfaclの出力には、項24.3.1. 「ACLエントリとファイルモードのパーミッションビット」 (page 382)で説明したパーミッションビットの割り当てとACLエントリが正確に反映されます。最初の3つの出力行には、名前、所有者、およびディレクトリの所有者の所属グループが表示されています。次の3行には、*所有者*、*所有者の所属グループ*、および*その他*という3つのACLエントリ

が表示されています。実際には、この最小ACLの場合、getfaclコマンドではlsで取得できなかった情報は生成されません。

読み取り、書き込み、実行の各パーミッションをさらにユーザgeekoとグループmascotsに割り当てるには、次のようにします。

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

オプション-mを指定すると、setfaclに対して既存のACLの変更が求められます。このオプションの後の引き数は、変更するACLエントリを示します(複数のエントリはカンマで区切られます)。最後の部分には、こうした変更を適用するディレクトリの名前を指定します。設定されたACLを確認するには、getfaclコマンドを使用します。

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

ユーザgeekoとグループmascots向けのエントリのほかに、マスクエントリが生成されました。 このマスクエントリは、すべてのパーミッションが有効になるように自動的に設定されます。setfaclは、既存のマスクエントリを変更済みの設定に自動的に合わせます。ただし、-nを指定してこの機能を無効にした場合は除きます。 マスクでは、*グループクラス*のすべてのエントリに対する最大限に有効なアクセスパーミッションが定義されます。こうしたエントリには、*名前付きユーザ*、*名前付きグループ*、および*所有者の所属グループ*があります。ls -dl mydirで表示された*グループクラス*のパーミッションビットは、maskエントリに対応しています。

```
drwxrwx---+ ... tux project3 ... mydir
```

出力の最初のカラムには、この項目に*拡張*ACLがあることを示すためにさらに+が表示されます。

lsコマンドの出力に従って、マスクエントリのパーミッションには書き込みアクセスが追加されています。従来どおり、そのようなパーミッションビットは、*所有者の所属グループ*(ここではproject3)もディレクトリmydirに書き込みアクセスできることを表します。ただし、*所有者の所属グループ*の有

効なアクセスパーミッションは、*所有者の所属グループ*向けおよびマスク用に定義されたパーミッションの重複部分に相当します。この部分は、この例ではr-xです(表 24.2. 「アクセスパーミッションのマスキング」 (page 382)を参照)。この例の*所有者の所属グループ*の有効なパーミッションに関する限り、ACLエントリを追加した後も何も変わりませんでした。

マスクエントリを編集するには、setfaclまたはchmodを使用します。たとえば、chmod g-w mydirを使用すると、ls -dl mydirでは、次のように表示されます。

```
drwxr-x---+ ... tux project3 ... mydir
```

getfacl mydirでは、次の出力が得られます。

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascots:rwx       # effective: r-x
mask::r-x
other::---
```

chmodコマンドを実行して*グループクラス*ビットから書き込みパーミッションを削除した後に、lsコマンドの出力を見れば、マスクビットが相応に変更されている、つまり、書き込みパーミッションが再びmydirの所有者に制限されていることを十分に確認できます。getfaclの出力でこの確認を行います。この出力に、有効なパーミッションビットが元のパーミッションと一致しないすべてのエントリのコメントが含まれる理由は、それらのビットがマスクエントリに基いてフィルタ処理されるためです。chmod g+w mydirを使用すれば、いつでも元のパーミッションに戻すことができます。

24.3.3 デフォルトACLが設定されたディレクトリ

ディレクトリには、デフォルトACLを設定できます。デフォルトACLとは、ディレクトリのオブジェクトを作成するときにそうしたオブジェクトが継承するアクセスパーミッションを定義する特別な種類のACLのことです。デフォルトACLは、サブディレクトリとファイルに作用します。

デフォルトACLの作用

ディレクトリのデフォルトACLのパーミッションをそのディレクトリ内のファイルやサブディレクトリに渡す方法は、次の2種類があります。

- サブディレクトリは、そのデフォルトACLおよびアクセスACLとして親ディレクトリのデフォルトACLを継承します。
- ファイルは、そのアクセスACLとしてデフォルトACLを継承します。

ファイルシステムオブジェクトを作成するすべてのシステムコールは、新たに作成したファイルシステムオブジェクトのアクセスパーミッションを定義するmodeパラメータを使用します。親ディレクトリにデフォルトACLが設定されていない場合、umaskで定義されたパーミッションビットは、modeパラメータで渡されるパーミッションから取り去られ、その結果が新しいオブジェクトに割り当てられます。親ディレクトリのデフォルトACLが存在する場合、新しいオブジェクトに割り当てられるパーミッションビットは、modeパラメータのパーミッションとデフォルトACLで定義されているパーミッションの重複部分に相当します。この場合、umaskは無視されます。

デフォルトACLのアプリケーション

次の3つの例は、ディレクトリとデフォルトACLの主要な操作を示しています。

1. 次のコマンドで、既存のディレクトリmydirにデフォルトACLを追加します。

   ```
   setfacl -d -m group:mascots:r-x mydir
   ```

   setfaclコマンドのオプション-dを指定することによって、setfaclは、後続の変更(オプション-m)をデフォルトACLに加えるように求められます。

   このコマンドの結果を詳しく見てみます。

   ```
   getfacl mydir

   # file: mydir
   # owner: tux
   # group: project3
   user::rwx
   ```

```
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

getfaclは、アクセスACLとデフォルトACLを返します。デフォルトACLは、defaultで始まるすべての行によって生成されます。デフォルトACLのmascotsグループのエントリでsetfaclコマンドを実行しただけですが、setfaclで他のすべてのエントリが自動的にアクセスACLからコピーされ、有効なデフォルトACLが作成されました。デフォルトACLが、アクセスパーミッションに即時に作用することはありません。デフォルトACLは、ファイルシステムオブジェクトが作成された場合にのみ作用し始めます。こうした新しいオブジェクトは、それぞれの親ディレクトリのデフォルトACLからのみパーミッションを継承します。

2. 次の例では、mkdirでmydirにサブディレクトリを作成しています。このサブディレクトリは、デフォルトACLを継承します。

```
mkdir mydir/mysubdir

getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: project3
user::rwx
group::r-x
group:mascots:r-x
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

予想どおり、新たに作成されたサブディレクトリmysubdirには、親ディレクトリのデフォルトACLからのパーミッションが設定されています。mysubdirのアクセスACLは、mydirのデフォルトACLを正確に反

映しています。このディレクトリからその下位オブジェクトにも同じデフォルトACLが継承されます。

3. touchコマンド(touch mydir/myfileなど)でmydirディレクトリにファイルを作成します。次に、ls -l mydir/myfileを実行すると、次のように表示されます。

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

getfacl mydir/myfileの出力は、次のようになります。

```
# file: mydir/myfile
# owner: tux
# group: project3
user::rw-
group::r-x          # effective:r--
group:mascots:r-x   # effective:r--
mask::r--
other::---
```

touchコマンドは、新しいファイルの作成時に値0666を指定してmodeを使用します。この値は、umaskおよびデフォルトACLにほかに制限がなければ、すべてのユーザクラスのファイルが読み取りと書き込みのパーミッションで作成されることを表します(デフォルトACLの作用項(page 387)を参照)。つまり、mode値に含まれていないアクセスパーミッションはすべて、それぞれのACLエントリから削除されます。パーミッションは、グループクラスのACLエントリから削除されていませんが、マスクエントリは、modeで設定されていないパーミッションをマスクするように変更されています。

この方法により、ACLが設定されたアプリケーション(コンパイラなど)とのスムーズなインタラクションができます。制限付きアクセスパーミッションでファイルを作成し、作成したファイルを後で実行可能ファイルとしてマークすることができます。maskメカニズムでは、正当なユーザやグループが必要に応じて実行可能ファイルを実行できることが保証されます。

24.3.4 ACLチェックアルゴリズム

任意のプロセスまたはアプリケーションがACL保護されたファイルシステムオブジェクトにアクセスできるようになる前に、チェックアルゴリズムが適用されます。基本的なルールとして、ACLエントリは、*所有者*、*名前付き*ユー

ザ、*所有者の所属グループ*または*名前付きグループ*、および*その他*の順に調べられます。アクセスは、プロセスに最も適したエントリに従って処理されます。パーミッションは累積しません。

プロセスが複数のグループに属し、複数のグループエントリに適する可能性がある場合は、さらに複雑になります。エントリは、必要なパーミッションを備えた適切なエントリから無作為に選択されます。どのエントリによって最終結果「アクセス許可」が実行されるかには関係ありません。同様に、適切なグループエントリのどれにも必要なパーミッションが設定されていない場合は、無作為に選択されたエントリによって最終結果「アクセス拒否」が実行されます。

24.4 アプリケーションでのACLサポート

ACLを使用すれば、最新のアプリケーションの要件を満たす非常に複雑なパーミッションシナリオを実現できます。従来のパーミッション概念とACLは、洗練された方法で組み合わせることができます。基本的なファイルコマンド(`cp`、`mv`、`ls`など)では、ACLをサポートします。Sambaでも同様です。

残念ながら、多くのエディタやファイルマネージャでは、依然としてACLをサポートしていません。たとえば、Konquerorでファイルをコピーすると、ファイルのACLは失われます。エディタでファイルを変更すると、使用するエディタのバックアップモードによっては、ファイルのACLが維持されるときもあれば、維持されないときもあります。エディタが元のファイルに変更を書き込む場合、アクセスACLは維持されます。エディタで更新内容を新しいファイルに保存し、そのファイルの名前を後で古いファイル名に変更しても、ACLは失われるおそれがあります。ただし、エディタがACLをサポートしている場合は除きます。starアーカイバ以外に、ACLを維持するバックアップアプリケーションは現在ありません。

24.5 関連資料

ACLの詳細については、`http://acl.bestbits.at/`を参照してください。`getfacl(1)`、`acl(5)`、および`setfacl(1)`については、manページも参照してください。

25 システムモニタリングユーティリティ

システムのステータスは、多数のプログラムやメカニズムを使用して検査できます。ここではその一部について説明します。また、日常作業に役立つ一部のユーティリティとその最も重要なパラメータについても説明します。

ここでは、コマンドごとに関連出力の例を示してあります。これらの例の1行目はコマンド自体です(ドル記号プロンプトの後)。コメントは、大カッコ[...]で示されており、長い行は必要に応じて折り返されています。長い行の改行はバックスラッシュ(\)で示されています。

```
$ command -x -y
output line 1
output line 2
output line 3 この行は少し長いので\
 次のように分割します
output line 3
[...]
output line 98
output line 99
```

できるだけ多数のユーティリティを紹介できるように、簡潔に説明しています。すべてのコマンドの詳細は、マニュアルページで確認できます。また、ほとんどのコマンドではパラメータ--helpが認識されます。このパラメータを指定すると、使用可能なパラメータの簡略リストが表示されます。

25.1 開いているファイルのリスト:lsof

プロセスIDが*PID*のプロセスについて開いている全ファイルのリストを表示するには、-pを使用します。たとえば、現行のシェルで使用されている全ファイルを表示するには、次のように入力します。

```
$ lsof -p $$
COMMAND  PID USER   FD   TYPE DEVICE    SIZE     NODE NAME
zsh     4694   jj  cwd    DIR   0,18     144 25487368 /suse/jj/t
(totan:/real-home/jj)
zsh     4694   jj  rtd    DIR    3,2     608        2 /
zsh     4694   jj  txt    REG    3,2  441296    20414 /bin/zsh
zsh     4694   jj  mem    REG    3,2  104484    10882 /lib/ld-2.3.3.so
zsh     4694   jj  mem    REG    3,2   11648    20610
/usr/lib/zsh/4.2.0/zsh/rlimits.so
[...]
zsh     4694   jj  mem    REG    3,2   13647    10891 /lib/libdl.so.2
zsh     4694   jj  mem    REG    3,2   88036    10894 /lib/libnsl.so.1
zsh     4694   jj  mem    REG    3,2  316410   147725 /lib/libncurses.so.5.4
zsh     4694   jj  mem    REG    3,2  170563    10909 /lib/tls/libm.so.6
zsh     4694   jj  mem    REG    3,2 1349081    10908 /lib/tls/libc.so.6
zsh     4694   jj  mem    REG    3,2      56    12410
/usr/lib/locale/de_DE.utf8/LC_TELEPHONE
[...]
zsh     4694   jj  mem    REG    3,2      59    14393
/usr/lib/locale/en_US/LC_NUMERIC
zsh     4694   jj  mem    REG    3,2  178476    14565
/usr/lib/locale/en_US/LC_CTYPE
zsh     4694   jj  mem    REG    3,2   56444    20598
/usr/lib/zsh/4.2.0/zsh/computil.so
zsh     4694   jj    0u   CHR 136,48                50 /dev/pts/48
zsh     4694   jj    1u   CHR 136,48                50 /dev/pts/48
zsh     4694   jj    2u   CHR 136,48                50 /dev/pts/48
zsh     4694   jj   10u   CHR 136,48                50 /dev/pts/48
```

この例では、値としてシェルのプロセスIDをとる特殊なシェル変数$$が使用されています。

パラメータを指定せずにコマンドlsofを入力すると、現在開いている全ファイルがリストされます。開いているファイルの数が何千にも達することがあるので、そのすべてをリストすることはほとんど無意味です。ただし、開いているすべてのファイルのリストを検索機能と組み合わせて使用すると、役立つリストが生成されます。たとえば、次のように使用されているすべてのキャラクタデバイスのリストを表示します。

```
$ lsof | grep CHR
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
zsh        4694      jj    0u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    1u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    2u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj   10u   CHR 136,48               50 /dev/pts/48
X          6476    root  mem    CHR    1,1             38042 /dev/mem
lsof      13478      jj    0u   CHR 136,48               50 /dev/pts/48
lsof      13478      jj    2u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    1u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    2u   CHR 136,48               50 /dev/pts/48
```

25.2 ファイルにアクセス中のユーザ:fuser

現在一定のファイルにアクセスしているプロセスまたはユーザを判別しておくことは有効です。たとえば、/mntにマウントされているファイルシステムをアンマウントするとします。umountでは、「デバイスがビジー」状態が返されます。ここで次のようにコマンドfuserを使用すると、デバイスにアクセスしているプロセスを判断することができます。

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt
                     jj        26597 f....  less
```

別の端末で実行中であったlessプロセスの終了後は、ファイルシステムを正常にアンマウントできます。

25.3 ファイルのプロパティ:stat

コマンドstatは、ファイルのプロパティを表示します。

```
$ stat xml-doc.txt
  File: `xml-doc.txt'
  Size: 632             Blocks: 8          IO Block: 4096   regular file
Device: eh/14d  Inode: 5938009     Links: 1
Access: (0644/-rw-r--r--)  Uid: (11994/      jj)   Gid: (   50/    suse)
Access: 2004-04-27 20:08:58.000000000 +0200
```

```
Modify: 2003-06-03 15:29:34.000000000 +0200
Change: 2003-07-23 17:48:27.000000000 +0200
```

パラメータ--filesystemを指定すると、指定したファイルが置かれているファイルシステムのプロパティの詳細が出力されます。

```
$ stat  . --filesystem
  File: "."
    ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388   Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

zシェル(zsh)を使用する場合、zシェルには異なるオプションと出力形式を使用するシェル内蔵statがあるため、/usr/bin/statと入力する必要があります。

```
% type stat
stat is a shell builtin
% stat .
device  769
inode   4554808
mode    16877
nlink   12
uid     11994
gid     50
rdev    0
size    4096
atime   1091536882
mtime   1091535740
ctime   1091535740
blksize 4096
blocks  8
link
```

25.4 USBデバイス:lsusb

コマンドlsusbは、すべてのUSBデバイスのリストを表示します。オプション-vを使用すると、詳細なリストが印刷されます。この詳細は、ディレクトリ/proc/bus/usb/から読み込まれます。次に示すものは、USBメモリスティックが取り付けられたあとのlsusbの出力です。最後のほうの行は、新規デバイスがあることを示します。

```
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
```

```
Bus 001 Device 001: ID 0000:0000
Bus 001 Device 018: ID 0402:5634 ALi Corp.
```

25.5 SCSIデバイスに関する情報:scsiinfo

コマンドscsiinfoは、SCSIデバイスに関する情報のリストを表示します。オプション-lを使用すると、システムに登録されているすべてのSCSIデバイスのリストが表示されます(同様の情報は、コマンドlsscsiでも入手できます)。次に示すものは、scsiinfo -i /dev/sdaの出力です。この場合、ハードディスクに関する情報が表示されます。オプション-aで、詳細が表示されます。

```
Inquiry command
---------------
Relative Address                    0
Wide bus 32                         0
Wide bus 16                         1
Synchronous neg.                    1
Linked Commands                     1
Command Queueing                    1
SftRe                               0
Device Type                         0
Peripheral Qualifier                0
Removable?                          0
Device Type Modifier                0
ISO Version                         0
ECMA Version                        0
ANSI Version                        3
AENC                                0
TrmIOP                              0
Response Data Format                2
Vendor:                     FUJITSU
Product:                    MAS3367NP
Revision level:             0104A0K7P43002BE
```

ハードディスクの不良ブロックを示す次の2つのテーブルからなる欠陥リストがあります。1つはメーカによって提供されるもの(メーカテーブル)で、もう1つは操作中に発生する不良ブロックのリスト(成長テーブル)です。成長テーブル内のエントリ数が増えた場合、ハードディスクを交換するほうが良いでしょう。

25.6　プロセス:top

コマンドtop ("table of processes" =プロセステーブルを意味します)は、2秒間隔で更新されるプロセスリストを表示します。プログラムを終了するには、Qキーを押します。パラメータ-n 1を指定すると、プロセスリストが1回表示された後にプログラムが終了します。次に示すものは、コマンドtop -n 1の出力例です。

```
top - 14:19:53 up 62 days,  3:35, 14 users,  load average: 0.01, 0.02, 0.00
Tasks: 102 total,   7 running,  93 sleeping,   0 stopped,   2 zombie
Cpu(s):   0.3% user,   0.1% system,   0.0% nice,  99.6% idle
Mem:    514736k total,   497232k used,    17504k free,    56024k buffers
Swap:  1794736k total,   104544k used,  1690192k free,   235872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  Command
 1426 root      15   0  116m  41m  18m S  1.0  8.2  82:30.34 X
20836 jj        15   0  820  820  612 R  1.0  0.2   0:00.03 top
    1 root      15   0  100   96   72 S  0.0  0.0   0:08.43 init
    2 root      15   0    0    0    0 S  0.0  0.0   0:04.96 keventd
    3 root      34  19    0    0    0 S  0.0  0.0   0:00.99 ksoftirqd_CPU0
    4 root      15   0    0    0    0 S  0.0  0.0   0:33.63 kswapd
    5 root      15   0    0    0    0 S  0.0  0.0   0:00.71 bdflush
       [...]
 1362 root      15   0   488  452  404 S  0.0  0.1   0:00.02 nscd
 1363 root      15   0   488  452  404 S  0.0  0.1   0:00.04 nscd
 1377 root      17   0    56    4    4 S  0.0  0.0   0:00.00 mingetty
 1379 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
 1380 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
```

topの実行中にFキーを押すと、メニューが開き、出力形式を大幅に変更できます。

パラメータ-U UIDを指定すると、特定のユーザに関連したプロセスのみがモニタされます。*UID*は、ユーザのユーザIDに置き換えます。top -U $(id -u username)は、ユーザ名を基本としたユーザのUIDを返し、そのプロセスを表示します。

25.7　プロセスリスト:ps

コマンドpsは、プロセスのリストを作成します。パラメータrを追加すると、現在計算時間を使用しているプロセスだけが表示されます。

```
$ ps r
  PID TTY      STAT   TIME COMMAND
22163 pts/7    R      0:01 -zsh
 3396 pts/3    R      0:03 emacs new-makedoc.txt
20027 pts/7    R      0:25 emacs xml/common/utilities.xml
20974 pts/7    R      0:01 emacs jj.xml
27454 pts/7    R      0:00 ps r
```

このパラメータは、マイナス記号なしで指定する必要があります。さまざまなパラメータが、マイナス記号付きで指定されたり、マイナス記号なして指定されたりします。マニュアルページは潜在的ユーザを簡単に驚かせることもありますが、幸いなことに、ps --helpコマンドは簡単なヘルプページを作成します。

実行中のemacsプロセスの数をチェックするには、次のものを使用します。

```
$ ps x | grep emacs
 1288 ?        S      0:07 emacs
 3396 pts/3    S      0:04 emacs new-makedoc.txt
 3475 ?        S      0:03 emacs .Xresources
20027 pts/7    S      0:40 emacs xml/common/utilities.xml
20974 pts/7    S      0:02 emacs jj.xml

$ pidof emacs
20974 20027 3475 3396 1288
```

パラメータ-pは、次のようにプロセスIDを通じてプロセスを選択します。

```
$ ps www -p $(pidof xterm)
  PID TTY      STAT   TIME COMMAND
 9025 ?        S      0:01 xterm -g 100x45+0+200
 9176 ?        S      0:00 xterm -g 100x45+0+200
29854 ?        S      0:21 xterm -g 100x75+20+0 -fn \
  -B&H-LucidaTypewriter-Medium-R-Normal-Sans-12-120-75-75-M-70-iso10646-1
 4378 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
25543 ?        S      0:02 xterm -g 100x45+0+200
22161 ?        R      0:14 xterm -g 100x45+0+200
16832 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
16912 ?        S      0:00 xterm -g 100x45+0+200
17861 ?        S      0:00 xterm -bg DarkSeaGreen1 -g 120x45+40+300
19930 ?        S      0:13 xterm -bg LightCyan
21686 ?        S      0:04 xterm -g 100x45+0+200 -fn \
lucidasanstypewriter-12
23104 ?        S      0:00 xterm -g 100x45+0+200
26547 ?        S      0:00 xterm -g 100x45+0+200
```

プロセスリストは、必要に応じてフォーマットできます。オプション-Lを指定すると、すべてのキーワードのリストが返されます。次のコマンドを入力すると、メモリ使用量順の全プロセスのリストが発行されます。

```
$ ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2    0 [ksoftirqd/0]
    3    0 [events/0]
   17    0 [kblockd/0]
[...]
10164 5260 xterm
31110 5300 xterm
17010 5356 xterm
 3896 29292 /usr/X11R6/bin/X -nolisten tcp -br vt7 -auth
/var/lib/xdm/authdir/au
```

25.8 プロセスツリー:pstree

pstreeコマンドは、プロセスリストをツリー形式で出力します。

```
$ pstree
init-+-atd
     |-3*[automount]
     |-bdflush
     |-cron
  [...]
     |-usb-storage-1
     |-usb-storage-2
     |-10*[xterm---zsh]
     |-xterm---zsh---mutt
     |-2*[xterm---su---zsh]
     |-xterm---zsh---ssh
     |-xterm---zsh---pstree
     |-ypbind---ypbind---2*[ypbind]
     `-zsh---startx---xinit4-+-X
                             `-ctwm-+-xclock
                                    |-xload
                                    `-xosview.bin
```

パラメータ-pを指定すると、プロセス名にプロセスIDが追加されます。コマンドラインも表示させるには、-aパラメータを使用します。

```
$ pstree -pa
init,1
  |-atd,1255
[...]
  `-zsh,1404
      `-startx,1407 /usr/X11R6/bin/startx
          `-xinit4,1419 /suse/jj/.xinitrc [...]
              |-X,1426 :0 -auth /suse/jj/.Xauthority
              `-ctwm,1440
                  |-xclock,1449 -d -geometry -0+0 -bg grey
```

```
|-xload,1450 -scale 2
`-xosview.bin,1451 +net -bat +net
```

25.9 実行者と実行内容:w

コマンドwを使用すると、システムにログオンしているユーザと、そのユーザが実行している操作を確認できます。次に例を示します。

```
$ w
 15:17:26 up 62 days,  4:33, 14 users,  load average: 0.00, 0.04, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
jj       pts/0     30Mar04  4days  0.50s  0.54s xterm -e su -l
jj       pts/1     23Mar04  5days  0.20s  0.20s -zsh
jj       pts/2     23Mar04  5days  1.28s  1.28s -zsh
jj       pts/3     23Mar04  3:28m  3.21s  0.50s -zsh
[...]
jj       pts/7     07Apr04  0.00s  9.02s  0.01s w
jj       pts/9     25Mar04  3:24m  7.70s  7.38s mutt
[...]
jj       pts/14    12:49   37:34   0.20s  0.13s ssh totan
```

最後の行は、ユーザjjがコンピュータtotanへのセキュアシェル(ssh)接続を確立したことを示します。他のシステムのユーザがリモートログインしている場合は、パラメータ-fを指定すると、そのユーザがどのコンピュータから接続を確立したかが出力されます。

25.10 メモリの使用状況:free

ユーティリティfreeはRAMの使用状況を検査します。空きメモリと使用済みメモリ(およびスワップ領域)の両方について詳細が表示されます。

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

-mを指定すると、すべてのサイズがMB単位で表されます。

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

実際に必要な情報は、次の行に含まれています。

```
-/+ buffers/cache:        191        311
```

ここでは、バッファとキャッシュで使用されているメモリの量が計算されます。パラメータ-d delayを指定すると、表示が*delay*秒間隔で確実に更新されます。たとえば、free -d 1.5と入力すると1.5秒ごとに更新されます。

25.11 カーネルリングバッファ:dmesg

Linuxカーネルは、リングバッファに一定のメッセージを保持します。これらのメッセージを表示するには、コマンドdmesgを入力します。

```
$ dmesg
[...]
sdc : READ CAPACITY failed.
sdc : status = 1, message = 00, host = 0, driver = 08
Info fld=0xa00 (nonstd), Current sd00:00: sense key Not Ready
sdc : block size assumed to be 512 bytes, disk size 1GB.
sdc: test WP failed, assume Write Enabled
 sdc: I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 unable to read partition table
 I/O error: dev 08:20, sector 0
nfs: server totan not responding, still trying
nfs: server totan OK
```

最終行は、NFSサーバtotanに一時的な問題が発生していたことを示しています。ここまでの行は、USBフラッシュドライブの挿入によって発生しています。古いイベントは、ファイル/var/log/messagesおよび/var/log/warnに記録されています。

25.12 ファイルシステムと使用状況:mount、df、およびdu

コマンドmountは、どのファイルシステム(デバイスとタイプ)がどのマウントポイントにマウントされているかを出力します。

```
$ mount
/dev/hdb2 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /data type ext2 (rw)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
automount(pid1012) on /suse type autofs \
    (rw,fd=5,pgrp=1012,minproto=2,maxproto=3)
totan:/real-home/jj on /suse/jj type nfs \
    (rw,nosuid,rsize=8192,wsize=8192,hard,intr,nolock,addr=10.10.0.1)
```

コマンドdfを使用して、ファイルシステムの使用状況に関する合計情報を入手してください。パラメータ-h(または--human-readable)を指定すると、出力は通常のユーザが理解できる形式に変換されます。

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdb2             7.4G  5.1G  2.0G  73% /
/dev/hda1              74G  5.8G   65G   9% /data
shmfs                 252M     0  252M   0% /dev/shm
totan:/real-home/jj   350G  324G   27G  93% /suse/jj
```

NFSファイルサーバtotanのユーザは、ホームディレクトリを遅延なしで空にする必要があります。指定したディレクトリとそのサブディレクトリの全ファイルの合計サイズを表示するには、コマンドduを使用します。パラメータ-sを指定すると、詳細情報は出力されません。-hを指定すると、データは通常のユーザが理解できる形式に再び変換されます。次のコマンドを使用したとします。

```
$ du -sh ~
361M    /suse/jj
```

自分のホームディレクトリに使用されている容量が表示されます。

25.13 /procファイルシステム

/procファイルシステムは、カーネルにより重要な情報が仮想ファイルの形式で保持される疑似ファイルシステムです。たとえば、次のコマンドを使用すると、CPUのタイプを確認できます。

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

割り込みの割り当てと使用は、次のコマンドでクエリできます。

```
$ cat /proc/interrupts
           CPU0
  0:  537544462          XT-PIC  timer
  1:     820082          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          2          XT-PIC  rtc
  9:          0          XT-PIC  acpi
 10:      13970          XT-PIC  usb-uhci, usb-uhci
 11:  146467509          XT-PIC  ehci_hcd, usb-uhci, eth0
 12:    8061393          XT-PIC  PS/2 Mouse
 14:    2465743          XT-PIC  ide0
 15:       1355          XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

重要なファイルとその内容の一部は次のとおりです。

/proc/devices
　使用可能なデバイス

/proc/modules
　ロードされたカーネルモジュール

/proc/cmdline
　カーネルコマンドライン

/proc/meminfo
　メモリ使用状況に関する詳細情報

/proc/config.gz
　gzip-現在実行中のカーネルの圧縮設定ファイル

詳細は、テキストファイル/usr/src/linux/Documentation/filesystems/proc.txtにあります。現在実行中のプロセスについては、/proc/*NNN*ディレクトリで確認できます。この場合、*NNN*は関連プロセスのプロセスID (PID)です。/proc/self/を指定すると、プロセスとその特有の特性を確認できます。

```
$ ls -l /proc/self
lrwxrwxrwx  1 root root 64 Apr 29 13:52 /proc/self -> 27585

$ ls -l /proc/self/
total 0
dr-xr-xr-x  2 jj suse 0 Apr 29 13:52 attr
-r--------  1 jj suse 0 Apr 29 13:52 auxv
-r--r--r--  1 jj suse 0 Apr 29 13:52 cmdline
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 cwd -> /suse/jj/t
-r--r--r--  1 jj suse 0 Apr 29 13:52 delay
-r--------  1 jj suse 0 Apr 29 13:52 environ
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 exe -> /bin/ls
dr-x------  2 jj suse 0 Apr 29 13:52 fd
-rw-------  1 jj suse 0 Apr 29 13:52 mapped_base
-r--r--r--  1 jj suse 0 Apr 29 13:52 maps
-rw-------  1 jj suse 0 Apr 29 13:52 mem
-r--r--r--  1 jj suse 0 Apr 29 13:52 mounts
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 root -> /
-r--r--r--  1 jj suse 0 Apr 29 13:52 stat
-r--r--r--  1 jj suse 0 Apr 29 13:52 statm
-r--r--r--  1 jj suse 0 Apr 29 13:52 status
dr-xr-xr-x  3 jj suse 0 Apr 29 13:52 task
-r--r--r--  1 jj suse 0 Apr 29 13:52 wchan
```

実行可能ファイルとライブラリのアドレス割り当ては、mapsファイルに含まれています。

```
$ cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:02 22890      /bin/cat
0804c000-0804d000 rw-p 00003000 03:02 22890      /bin/cat
0804d000-0806e000 rwxp 0804d000 00:00 0
40000000-40016000 r-xp 00000000 03:02 10882      /lib/ld-2.3.3.so
40016000-40017000 rw-p 00015000 03:02 10882      /lib/ld-2.3.3.so
40017000-40018000 rw-p 40017000 00:00 0
4002b000-40135000 r-xp 00000000 03:02 10908      /lib/tls/libc.so.6
40135000-4013d000 rw-p 0010a000 03:02 10908      /lib/tls/libc.so.6
4013d000-40141000 rw-p 4013d000 00:00 0
```

```
bfffe000-c0000000 rw-p bfffe000 00:00 0
ffffe000-fffff000 ---p 00000000 00:00 0
```

25.14 vmstat、iostat、およびmpstat

ユーティリティvmstatは、仮想メモリ統計を報告します。このユーティリティは、ファイル/proc/meminfo、/proc/stat、および/proc/*/statを読み取ります。これは、システムのパフォーマンスの障害を判別するのに役立ちます。 コマンドiostatは、CPUとデバイスおよびパーティションでの入出力に関する統計を報告します。表示される情報は、ファイル/proc/statおよび/proc/partitionsから取られます。この出力は、ハードディスク間の入出力バランスを改善するために使用できます。コマンドmpstatは、CPU関連の統計を報告します。

25.15 procinfo

/procファイルシステムからの重要情報のサマリを確認するには、コマンドprocinfoを使用します。

```
$ procinfo
Linux 2.6.4-54.5-default (geeko@buildhost) (gcc 3.3.3 ) #1 1CPU [roth.suse.de]


Memory:      Total        Used        Free      Shared     Buffers
Mem:        516696      513200        3496           0       43284
Swap:       530136        1352      528784

Bootup: Wed Jul  7 14:29:08 2004    Load average: 0.07 0.04 0.01 1/126 5302

user  :       2:42:28.08   1.3%  page in :         0
nice  :       0:31:57.13   0.2%  page out:         0
system:       0:38:32.23   0.3%  swap in :         0
idle  :    3d 19:26:05.93  97.7%  swap out:         0
uptime:    4d  0:22:25.84         context :207939498

irq  0: 776561217 timer                  irq  8:          2 rtc

irq  1:    276048 i8042                  irq  9:      24300 VIA8233

irq  2:         0 cascade [4]           irq 11:   38610118 acpi, eth0, uhci_hcd

irq  3:         3                       irq 12:    3435071 i8042
```

```
irq  4:          3                          irq 14:    2236471 ide0

irq  6:          2                          irq 15:        251 ide1
```

すべての情報を表示するには、パラメータ-aを使用します。パラメータ-nNを指定すると、情報がN秒間隔で更新されます。この場合、プログラムを終了するにはQキーを押します。

デフォルトでは、累積値が表示されます。パラメータ-dを入力すると、別の値が作成されます。procinfo -dn5を入力すると、過去5秒間に変化した値が表示されます。

```
Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:             0           2          -2           0           0           0
Swap:            0           0           0

Bootup: Wed Feb 25 09:44:17 2004    Load average: 0.00 0.00 0.00 1/106 31902

user  :       0:00:00.02   0.4%  page in :         0  disk 1:         0r        0w
nice  :       0:00:00.00   0.0%  page out:         0  disk 2:         0r        0w
system:       0:00:00.00   0.0%  swap in :         0  disk 3:         0r        0w
idle  :       0:00:04.99  99.6%  swap out:         0  disk 4:         0r        0w
uptime:  64d  3:59:12.62         context :      1087

irq  0:       501 timer                  irq 10:          0 usb-uhci, usb-uhci
irq  1:         1 keyboard               irq 11:         32 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]            irq 12:        132 PS/2 Mouse
irq  6:         0                        irq 14:          0 ide0
irq  8:         0 rtc                    irq 15:          0 ide1
irq  9:         0 acpi
```

25.16 PCI リソース:lspci

コマンドlspciはPCIリソースをリストします。

```
$ lspci
00:00.0 Host bridge: VIA Technologies, Inc.  \
    VT8366/A/7 [Apollo KT266/A/333]
00:01.0 PCI bridge: VIA Technologies, Inc.  \
    VT8366/A/7 [Apollo KT266/A/333 AGP]
00:0b.0 Ethernet controller: Digital Equipment Corporation  \
    DECchip 21140 [FasterNet] (rev 22)
00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)
00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge
00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B  \
    PIPC Bus Master IDE (rev 06)
```

```
00:11.5 Multimedia audio controller: VIA Technologies, Inc.  \
    VT8233 AC97 Audio Controller (rev 50)
01:00.0 VGA compatible controller: Matrox Graphics, Inc.  \
    MGA G550 AGP (rev 01)
```

–vを使用すると、さらに詳細なリストが出力されます。

```
$ lspci -v
[...]
01:00.0 \
 VGA compatible controller: Matrox Graphics, Inc. MGA G550 AGP (rev 01) \
    (prog-if 00 [VGA])
 Subsystem: Matrox Graphics, Inc. Millennium G550 Dual Head DDR 32Mb
 Flags: bus master, medium devsel, latency 32, IRQ 10
 Memory at d8000000 (32-bit, prefetchable) [size=32M]
 Memory at da000000 (32-bit, non-prefetchable) [size=16K]
 Memory at db000000 (32-bit, non-prefetchable) [size=8M]
 Expansion ROM at <unassigned> [disabled] [size=128K]
 Capabilities: <available only to root>
```

デバイス名の解決に関する情報は、ファイル/usr/share/pci.idsから取得されます。このファイルにないPCI IDは、「Unknown device」で示されます。

パラメータ–vvを指定すると、プログラムが問い合わせ可能な情報がすべて出力されます。数値のみを表示するには、パラメータ–nを指定する必要があります。

25.17 実行中のプログラムのシステム呼び出し:strace

ユーティリティstraceを使用すると、現在実行中のプロセスのシステム呼び出しをすべてトレースできます。行頭のstraceに続けてコマンドを通常どおり入力します。

```
$ strace -e open ls

execve("/bin/ls", ["ls"], [/* 88 vars */]) = 0
uname({sys="Linux", node="edison", ...}) = 0
brk(0)                                  = 0x805b000
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
          = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=76333, ...}) = 0
old_mmap(NULL, 76333, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
```

```
[...]
ioctl(1, SNDCTL_TMR_TIMEBASE or TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=53, ws_col=110, ws_xpixel=897, ws_ypixel=693}) = 0
open(".", O_RDONLY|O_NONBLOCK|O_LARGEFILE|O_DIRECTORY) = 3
fstat64(3, {st_mode=S_IFDIR|0755, st_size=144, ...}) = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
getdents64(3, /* 5 entries */, 4096)    = 160
getdents64(3, /* 0 entries */, 4096)    = 0
close(3)                                = 0
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 48), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
          = 0x40018000
write(1, "ltrace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

たとえば、特定のファイルを開く試みをすべてトレースするには、以下を入力します。

```
$ strace -e open ls myfile.txt

open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/tls/librt.so.1", O_RDONLY)   = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libselinux.so.1", O_RDONLY)  = 3
open("/lib/tls/libc.so.6", O_RDONLY)    = 3
open("/lib/tls/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
open("/proc/mounts", O_RDONLY)          = 3
[...]
open("/proc/filesystems", O_RDONLY)     = 3
open("/proc/self/attr/current", O_RDONLY) = 4
```

すべての子プロセスをトレースするには、パラメータ`-f`を使用します。strace の動作と出力形式は厳密に制御できます。詳細については、`man strace`を参照してください。

25.18 実行されたプログラムによるライブラリ呼び出し:ltrace

コマンド`ltrace`を使用すると、プロセスによるライブラリ呼び出しをトレースできます。このコマンドの使用方法は、`strace`と同様です。パラメータ`-c`を指定すると、発生したライブラリ呼び出しの回数と持続期間が出力されます。

```
$ ltrace -c find /usr/share/doc
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 86.27    1.071814          30     35327           write
 10.15    0.126092          38      3297           getdents64
  2.33    0.028931           3     10208           lstat64
  0.55    0.006861           2      3122         1 chdir
  0.39    0.004890           3      1567         2 open
[...]
  0.00    0.000003           3         1           uname
  0.00    0.000001           1         1           time
------ ----------- ----------- --------- --------- ----------------
100.00    1.242403                 58269         3 total
```

25.19 必須ライブラリの指定:ldd

コマンドlddを使用すると、引数として指定した動的実行可能ファイルをロードするライブラリを確認できます。

```
$ ldd /bin/ls
linux-gate.so.1 =>  (0xffffe000)
librt.so.1 => /lib/tls/librt.so.1 (0x4002b000)
libacl.so.1 => /lib/libacl.so.1 (0x40033000)
libselinux.so.1 => /lib/libselinux.so.1 (0x40039000)
libc.so.6 => /lib/tls/libc.so.6 (0x40048000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x4015d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
libattr.so.1 => /lib/libattr.so.1 (0x4016d000)
```

静的バイナリファイルには、動的ライブラリは不要です。

```
$ ldd /bin/sash
        not a dynamic executable
$ file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, statically linked, stripped
```

25.20 ELFバイナリに関する補足情報

バイナリの内容は、readelfユーティリティを使用して読み込むことができます。このユーティリティは、他のハードウェアアーキテクチャ用に作成されたELFファイルにも使用できます。

```
$ readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
```

```
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8049b40
  Start of program headers:          52 (bytes into file)
  Start of section headers:          76192 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           40 (bytes)
  Number of section headers:         29
  Section header string table index: 26
```

25.21 プロセス間通信:ipcs

コマンドipcsは、現在使用中のIPCリソースのリストを出力します。

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x000027d9 5734403    toms       660        64528      2
0x00000000 5767172    toms       666        37044      2
0x00000000 5799941    toms       666        37044      2

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x000027d9 0          toms       660        1

------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

25.22 timeを使用した時間測定

コマンドの所要時間は、timeユーティリティで判断できます。このユーティリティには2つのバージョンがあります。一方はシェルビルトインで、他方はプログラム(/usr/bin/time)です。

```
$ time find . > /dev/null

real    0m4.051s
```

```
user    0m0.042s
sys     0m0.205s
```

パート VIII. システム

64ビットシステム環境での32ビットと64ビットのアプリケーション 26

SUSE Linuxは、複数の64ビットプラットフォームで利用できます。これは、同梱されているすべてのアプリケーションがすでに64ビットプラットフォームに移植されているという意味ではありません。SUSE Linuxは、64ビットシステム環境での32ビットアプリケーションの使用をサポートしています。この章では、このサポートを64ビットのSUSE Linuxプラットフォームで実装する方法について簡潔に説明します。また、32ビットアプリケーションの実行方法(ランタイムサポート)、および32ビットと64ビットのシステム環境の両方で実行できるように32ビットアプリケーションをコンパイルする方法について説明します。さらに、カーネルAPIに関する情報、および32ビットアプリケーションを64ビットカーネルで実行する方法の説明もあります。

64ビットプラットフォームAMD64、およびEM64Tに対応したSUSE Linuxは、既存の32ビットアプリケーションが64ビット環境で「出荷してすぐに」動作するように設計されています。このサポートにより、対応する64ビット移植版が使用可能になるのを待たなくても、使用したい32ビットアプリケーションを引き続き使用できます。

26.1 ランタイムサポート

重要項目: アプリケーションバージョン間の競合

アプリケーションが32ビットと64ビットの両方の環境で使用可能な場合に、両方のバージョンを同時にインストールすると問題が生じます。そのような場合は、2つのバージョンのどちらかだけをインストールして使用してください。

正しく実行するために、すべてのアプリケーションにはライブラリが必要です。しかし残念ながら、32ビットバージョンと64ビットバージョンのライブラリの名前は同じです。そのため、ライブラリを別の方法で区別する必要があります。

32ビットバージョンとの互換性を維持するために、ライブラリは32ビット環境の場合と同様にシステムの同じ場所に格納されます。`libc.so.6`の32ビットバージョンは、32ビットと64ビットのどちらの環境でも`/lib/libc.so.6`の下にあります。

64ビットのすべてのライブラリとオブジェクトファイルは、`lib64`というディレクトリにあります。通常、`/lib`、`/usr/lib`、および`/usr/X11R6/lib`の下にあると想定されている64ビットのオブジェクトファイルは、`/lib64`、`/usr/lib64`、および`/usr/X11R6/lib64`の下にあります。つまり、両方のバージョンのファイル名を変更しなくても済むように、32ビットライブラリ用の領域は`/lib`、`/usr/lib`、および`/usr/X11R6/lib`の下になっています。

データの内容がワードサイズに左右されないオブジェクトディレクトリのサブディレクトリは、移動されません。たとえば、X11フォントは、これまでどおり`/usr/X11R6/lib/X11/fonts`の下の通常の場所にあります。このスキームは、LSB (Linux Standards Base)とFHS (File System Hierarchy Standard)に準拠しています。

26.2 ソフトウェア開発

biarch開発ツールチェーンでは、32ビットと64ビットのオブジェクトを生成できます。デフォルトは、64ビットオブジェクトのコンパイルです。特殊なフラグを使用すれば、32ビットオブジェクトを生成できます。GCCの場合、この特殊なフラグは`-m32`です。

すべてのヘッダファイルは、アーキテクチャに依存しない形式で作成する必要があります。インストール済みの32ビットと64ビットのライブラリには、インストール済みのヘッダファイルに対応するAPI (アプリケーションプログラミングインタフェース)が必要です。標準のSUSE環境は、この原則に従って設計されています。ライブラリを手動で更新した場合は、各自でAPIの問題を解決してください。

26.3 biarchプラットフォームでのソフトウェアのコンパイル

biarchアーキテクチャで他のアーキテクチャ向けのバイナリを開発するには、対象のアーキテクチャのそれぞれのライブラリをさらにインストールする必要があります。これらのパッケージには、 rpmname-32bitという名前が付けられています。さらに、rpmname-develパッケージからそれぞれのヘッダとライブラリ、また、rpmname-devel-32bitから対象のアーキテクチャ向けの開発ライブラリも必要です。

ほとんどのオープンソースプログラムでは、autoconfベースのプログラム設定が使用されています。対象のアーキテクチャ向けプログラムの設定にautoconfを使用するには、autoconfの標準のコンパイラとリンカーの設定に上書きするために、さらに環境変数を指定してconfigureスクリプトを実行します。

次の例は、対象のアーキテクチャとしてを採用しているAMD64またはEM64Tのシステムを示しています。

1. 32ビットコンパイラを使用するためにautoconfを設定します。

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

2. 32ビットオブジェクトを処理するようにリンカーに指示します。

   ```
   LD="ld -m elf64_i386"
   ```

3. 32ビットオブジェクトを生成するためにアセンブラを設定します。

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

4. libtoolなどのライブラリが/usr/libから得られたか確認します。

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

5. ライブラリがlibサブディレクトリに格納されているか確認します。

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

6. 32ビットXライブラリが使用されているか確認します。

```
      --x-libraries=/usr/X11R6/lib/
```

こうした変数のすべてがどのプログラムにも必要なわけではありません。それぞれのプログラムに合わせて使用してください。

```
CC="gcc -m64"            \
LDFLAGS="-L/usr/lib64;"  \
  .configure       \
    --prefix=/usr   \
    --libdir=/usr/lib64
make
make install
```

26.4 カーネル仕様

AMD64およびEM64T向けの64ビットカーネルには、64ビットと32ビットのカーネルABI (アプリケーションバイナリインタフェース)が用意されています。32ビットのカーネルABIは、該当する32ビットカーネルのABIと同じものです。つまり、32ビットアプリケーションが、32ビットカーネルの場合と同様に64ビットカーネルと通信できるということです。

64ビットカーネルのシステムコールの32ビットエミュレーションでは、システムプログラムで使用される多くのAPIをサポートしていません。ただし、このサポートの有無はプラットフォームによって異なります。このため、`lspci`やLVM管理プログラムなどの少数のアプリケーションは、正しく機能するように64ビットプログラムとしてコンパイルする必要があります。

64ビットカーネルでは、このカーネル用に特別にコンパイルされた64ビットカーネルモジュールしかロードできません。したがって、32ビットカーネルモジュールを使用することはできません。

ティップ

一部のアプリケーションには、カーネルでロード可能な個々のモジュールが必要です。64ビットシステム環境でそのような32ビットアプリケーションを使用する予定がある場合は、このアプリケーションおよびのプロバイダに問い合わせて、このモジュール向けのカーネルでロード可能な64ビットバージョンのモジュールと32ビットコンパイルバージョンのカーネルAPIを入手できるかを確認してください。

---

27 シェルの使用

グラフィカルユーザインタフェースは、今日、Linuxにおいてますます重要性を増していますが、日常業務を行うのにマウスを使うことが常に最良というわけではありません。コマンドラインが非常に柔軟で効率的だからです。テキストベースのアプリケーションは、遅いネットワークリンク上でコンピュータを制御する場合、またはxtermのコマンドラインで`root`としてタスクを実行する場合に、特に重要です。バッシュシェルは、SUSE Linuxのデフォルトのコマンドラインインタプリタです。

Linuxはマルチユーザのシステムで、ファイルへのアクセスはユーザパーミッションによって制御されています。コマンドラインとGUIのどちらを使う場合でも、パーミッションの概念を理解しておくことは役立ちます。コマンドラインを使う場合、多数のコマンドが重要です。viテキストエディタは、コマンドラインからシステムを設定する場合によく用いられます。これはまた、多くのシステム管理者および開発者の間で人気があります。

27.1 コマンドラインでバッシュを使用する

KDEタスクバーの中には、貝殻付きのモニタの形のアイコンがあります。このアイコンをクリックすると、コマンドを入力するためのコンソールウィンドウが表示されます。ターミナルプログラムであるKonsoleは通常、GNUプロジェクトの一部として開発されたプログラムであるバッシュ(Bourne again shell)を実行します。GNOMEデスクトップでは、 上部のパネルにあるコンピュー

タモニタの形をしたアイコンをクリックするとターミナルが起動し、通常はバッシュを実行します。

このシェルを開き、最初の行にあるプロンプトを確認します。このプロンプトは通常、ユーザ名、ホスト名、および現在のパスによって構成されていますが、カスタマイズすることもできます。カーソルがこのプロンプトの右端にあるときは、使用中のコンピュータシステムに対してコマンドを直接入力できます。

27.1.1 コマンドの入力

1つのコマンドは複数の要素によって構成されています。最初の要素は必ず、実際のコマンド自体であり、その後にパラメータまたはオプションが続きます。Enterを押した時点で、そのコマンドが実行されます。このキーを押す前は、コマンドラインの編集、オプションの追加、または入力ミスの訂正などを簡単に行えます。非常に使用頻度の高いコマンドの1つに、`ls`、というコマンドがあります。 これは、引数ありでも、引数なしでも使用できます。引数なしで`ls`コマンドを入力すると、カレントディレクトリの内容が表示されます。

オプションのプリフィックス(接頭辞)として、ハイフンを付けます。たとえば、`ls -l`コマンドは、同じディレクトリの内容を詳しい情報付きで表示します(長いリスト形式)。各ファイル名の隣に、そのファイルの作成日、バイト単位のサイズ、および後で紹介する他の詳細情報が表示されます。多くのコマンドで使用可能な重要なオプションの1つに、`--help`オプションがあります。`ls --help`と入力すると、`ls`コマンドのすべてのオプションが表示されます。

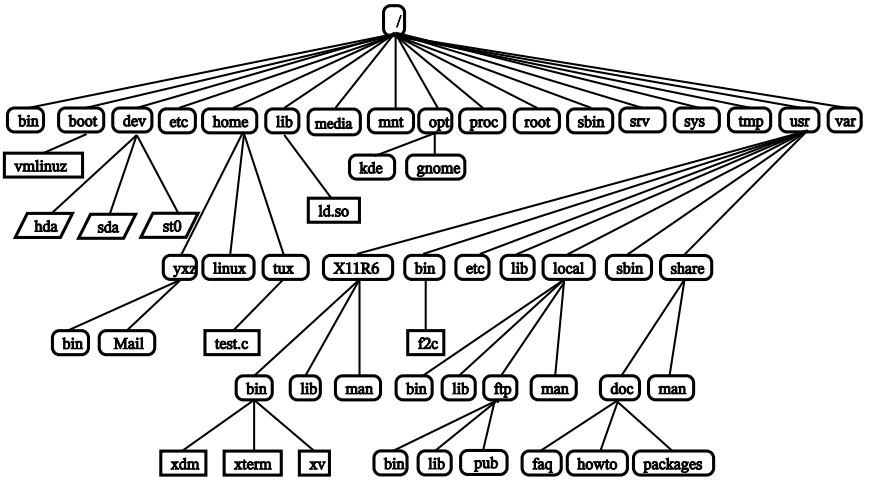
「引用符」を正しく付けることは重要です。ファイル名にスペースが含まれている場合には、バックスラッシュ(\)でスペースをエスケープするか、ファイル名を一重または二重引用符で囲んでください。そうしないと、バッシュは、`My Documents`のようなファイル名を、2つのファイルまたはディレクトリ名と解釈します。一重および二重引用符の違いは、二重引用符の場合には変数の展開が行われるという点にあります。一重引用符を使えば、シェルは、囲まれた文字列をそのまま用います。

27.1.2 ファイルとディレクトリ

シェルを効率よく使用するために、Linuxシステムのファイルおよびディレクトリの構造についてある程度知っておくと、非常に役立ちます。ディレクトリは、ファイル、プログラム、およびサブディレクトリが保存されている電気的なフォルダと考えることができます。階層の最上位にあるディレクトリはルートディレクトリであり、 /で表されます。ここから、他のすべてのディレクトリにアクセスできます。

/homeディレクトリは、各ユーザが自らの個人用ファイルを格納するためのディレクトリです。図 27.1.「標準的なディレクトリツリーの例」 (page 419)は、xyz、linux、およびtuxというサンプルユーザのホームディレクトリを含む、Linuxの標準的なディレクトリツリーを示しています。Linuxシステムのディレクトリツリーは、*FHS (Filesystem Hierarchy Standard)*に準拠する機能的な構造を採用しています。次に、Linux環境内にある標準的なディレクトリに関してリスト形式で簡単に説明します。

図 27.1　標準的なディレクトリツリーの例



/
　ルートディレクトリ(ディレクトリツリーの開始場所)

/home
　ユーザの個人的なディレクトリ

/dev
ハードウェアコンポーネントを表すデバイスファイルを格納するディレクトリ

/etc
システム設定に関する重要なファイルを格納するディレクトリ

/etc/init.d
ブートスクリプトを格納するディレクトリ

/usr/bin
一般的にアクセス可能なプログラムを格納するディレクトリ

/bin
ブートプロセスの初期に必要なプログラムを格納するディレクトリ

/usr/sbin
システム管理者用のプログラムを格納するディレクトリ

/sbin
システム管理者用で、ブート時に必要なプログラムを格納するディレクトリ

/usr/include
Cコンパイラ用のヘッダファイルを格納するディレクトリ

/usr/include/g++
C++コンパイラ用のヘッダファイルを格納するディレクトリ

/usr/share/doc
さまざまなドキュメントファイルを格納するディレクトリ

/usr/share/man
システムマニュアルページ(manページ)を格納するディレクトリ

/usr/src
システムソフトウェアのソースコードを格納するディレクトリ

/usr/src/linux
カーネルソースコードを格納するディレクトリ

/tmp、/var/tmp
一時ファイルを格納するディレクトリ

/usr
すべてのアプリケーションプログラムを格納するディレクトリ

/var
設定ファイル(たとえば/usrからリンクされるファイル)を格納するディレクトリ

/var/log
システムログファイルを格納するディレクトリ

/var/adm
システム管理データを格納するディレクトリ

/lib
共有ライブラリ(動的にリンクされるプログラム用)を格納するディレクトリ

/proc
プロセスファイルシステムを格納するディレクトリ

/sys
カーネルに関するすべてのデバイス情報が集められる「system」ファイルシステムを格納するディレクトリ

/usr/local
ディストリビューションに依存しないローカルな拡張ファイル群を格納するディレクトリ

/opt
オプションのソフトウェア、たとえば大規模なアドオンプログラムパッケージ(KDE、GNOME、Netscapeなど)を格納するディレクトリ

27.1.3 バッシュの機能

このシェルには、作業を容易にする2つの重要な機能があります。

履歴

ヒストリー(履歴)機能以前に入力したコマンドを再実行したい場合は、そのコマンドがプロンプト上に表示されるまで、↑を押します。↓を押すと、以前に入力したコマンドが、その時点からの入力順で表示されます。コマンドラインを編集するには、矢印キーを使用して希望の場所までカーソルを移動し、編集を行います。次のキーCtrl + Rを使用すると、履歴を検索することができます。

補完

一意に識別できる最初の数文字が入力された後、ファイル名を展開してファイル名全体を自動的に表示する機能です。これを行うには、最初の数文字を入力してからTabを押します。それらの文字で始まるファイルが複数存在する場合は、Tabを2回押すと、それらのファイルのリストが表示されます。

最初の例:ファイルの管理

ここまでで、コマンドの形式、内に存在するディレクトリ、およびバッシュを使用して迅速に作業する方法を学んだので、それらの知識を活用して簡単な作業を練習として実際に行ってみましょう。

1. シェルのアイコンをクリックして、KDEまたはGNOMEデスクトップからコンソールを開きます。

2. `ls`コマンドを入力して、自分のホームディレクトリの内容を表示します。

3. `mkdir`コマンド(*make directory* の略称)を使用して、`test`という新しいサブディレクトリを作成します。`mkdir test`と入力します。

4. 次に、Alt + F2を押し、KDEでは`kate`と入力してKateを、GNOMEでは`gedit`と入力してGeditを起動します。このエディタ内で任意の数文字を入力し、そのファイルを`Testfile`というファイル名で自分のホームディレクトリ内に保存します。Linuxでは、大文字と小文字が区別されます。この例では、最初の文字のTを大文字にします。

5. 自分のホームディレクトリの内容をもう一度表示します。`ls`コマンドをもう一度入力する代わりに、↑を2回押します。以前に入力した`ls`コマンドがプロンプト上に再び表示されます。このコマンドを実行するに

は、Enterを押します。新しく作成されたtestディレクトリが青い文字、Testfileが黒い文字で表示されます。この表示形式により、コンソール上でディレクトリとファイルを区別することができます。

6. mvコマンドを使用して、Testfileをtestサブディレクトリへ移動します。この作業をすばやく実行するために、展開機能を使用します。mv Tと入力し、Tabを押します。ディレクトリ内に、この文字で始まるファイルが他に存在しない場合、シェルはファイル名を自動的に展開し、*estfile*という文字列を追加します。または、1文字か2文字を自分で追加入力し、そのたびにTabキーを押して、シェルがファイル名を展開できるかどうかを確認します。最後に、スペースキーを押して、展開したファイル名の後に、testと入力し、Enterキーを押してコマンドを実行します。

7. この時点で、Testfileは、このディレクトリ内に存在していないはずです。もう一度lsコマンドを入力して、このことを確認します。

8. ファイルの移動が成功したかどうかを確認するために、cd testコマンドを入力して、testディレクトリへ移動します。そこで、もう一度lsコマンドを実行します。今度は、リスト内にTestfileが見つかるはずです。いつでも、cdとだけ入力してコマンドを実行すると、自分のホームディレクトリへ戻ることができます。

9. ファイルのコピーを作成するには、cpコマンドを使用します。たとえば、cp Testfile Testbackupと入力すると、TestfileをTestbackupにコピーすることができます。ここでも、lsコマンドを使用して、両方のファイルがディレクトリ内に存在しているかどうかを確認できます。

27.1.4 パスの指定

ファイルまたはディレクトリの作業をする場合、正しいパスを指定することが重要です。しかし、ルートから個別のファイルに到達するためにパス全体(絶対パス)を入力する必要はありません。カレントディレクトリを開始場所として使用することができます。表記~を使用して、自分のホームディレクトリを指定できます。したがって、testディレクトリ内のTestfileファイルをリストする方法は2つあります。相対パスを使用してls testと入力する方法と、絶対パスを使用してls ~/testと入力する方法です。

他のユーザのホームディレクトリの内容をリストするには、`ls ~username`と入力します。例となっているディレクトリツリーでは、サンプルユーザの1人が`tux`という名前です。この場合、`ls ~tux`と入力すると、`tux`のホームディレクトリの内容をリストできます。

カレントディレクトリは、ドット(.)で表します。ツリー内で、それよりすぐ上にあるレベルは、2つのドット(..)で表します。`ls ..`と入力すると、カレントディレクトリに対する親ディレクトリの内容が表示されます。`ls ../..`コマンドは、その階層内で2つ上のレベルにあるディレクトリの内容を表示します。

2番目の例:パスを使用する作業

ここでは、SUSE Linuxシステムのディレクトリ間で移動するためのもう1つの方法の例を挙げます。

1. 自分のホームディレクトリへ移動するために、引数なしの`cd`コマンドを使用します。次に、そのディレクトリ内に`test2`というディレクトリを作成するために、`mkdir test2`と入力します。

2. `cd test2`と入力して、その新しいディレクトリへ移動し、`subdirectory`という名前のサブディレクトリを作成します。そのサブディレクトリへ移動するために、展開機能を使用します。`cd su`と入力し、Tabを押します。シェルは、ディレクトリ名の残りの部分を展開します。

3. 今度は、ディレクトリ間で移動することなく、以前に作成した`Testbackup`ファイルをカレントディレクトリ(`subdirectory`)へ移動する作業を試してみましょう。この作業を実行するには、そのファイルを表す相対パスを指定します。`mv ../../test/Testbackup .`というコマンドです。(最後にドットがあることに注意してください)。このコマンドの最後にあるドットは、このファイルの移動先がカレントディレクトリであることをシェルに伝えるために必要です。この例の`../../`という表記は、自分のホームディレクトリを表しています。

27.1.5 ワイルドカード

このシェルは、パス名を展開するためのワイルドカードという、もう1つの規則も用意しています。バッシュでは、次のような3種類のワイルドカードを利用できます。

?
任意の1文字に対応します。

*****
任意の数文字に対応します。

[set]
角かっこの中で指定されたグループのうち、どれか1つの文字に対応します。 ここでは、*set*という文字列で代替しています。*set*の一部として、*[:class:]*という構文で、文字のクラスを指定することができます。ここでclassは、`alnum`(英数字)、`alpha`(英字)、`ascii` (ASCII文字)などのいずれかです。

グループの先頭で! または^を使用した場合には(*[!set]*)、*set*で識別されるもの以外の1文字にマッチします。

たとえば、`test`ディレクトリの中に、`Testfile`、`Testfile1`、`Testfile2`、および`datafile`という各ファイルがあるとします。`ls Testfile?`コマンドは、`Testfile1`と`Testfile2`をリストします。`ls Test*`コマンドを使用すると、`Testfile`もリスト内に含まれます。`ls *fil*`コマンドは、上記のサンプルファイルすべてを表示します。最後に、ワイルドカード`set`を使用して、最後が数字であるサンプルファイルすべてを表示してみます。`ls Testfile[1-9]`、またはクラスを使って、`ls Testfile[[:digit:]]`と入力します。

これら4種類のワイルドカードのうち、最も包括性が高いのは、アスタリスク(*)です。1つのコマンドを実行するだけで、あるディレクトリ内に含まれているすべてのファイルを他のディレクトリへコピー、またはすべてのファイルを削除することができます。たとえば、`rm *fil*`コマンドは、カレントディレクトリ内で、*fil*という文字列をファイル名の一部として使用しているすべてのファイルを削除します。

27.1.6 lessとmore

Linuxには、テキストファイルをシェル内で直接表示する小さな2つのプログラムが付属しています。エディタを起動してReadme.txtのようなファイルを読み取る代わりに、less Readme.txtコマンドを入力して、テキストをコンソールウィンドウ内で表示します。Spaceを押すと、1ページ下へスクロールします。Page UpとPage Downを使用すると、テキスト内を前方または後方へ移動できます。lessを終了するには、Qを押します。

lessの代わりに、それより古いプログラムであるmoreを使用することもできます。しかし、後方(上)へのスクロールができないので、利便性は劣ります。

lessプログラムは、*less is more*(少ない方が豊か)ということわざに由来する名前であり、他のコマンドの出力を便利な方法で表示する目的で使用することもできます。このコマンドの機能について理解するには、項27.1.7.「パイプとリダイレクト」 (page 426)を参照してください。

27.1.7 パイプとリダイレクト

通常、シェル内の標準出力は画面またはコンソールウィンドウであり、標準入力はキーボードです。あるコマンドの出力をlessのような他のアプリケーションへ転送するには、*パイプライン*を使用します。

testディレクトリ内にあるファイルを表示するには、ls test | lessコマンドを入力します。lessコマンドにより、testディレクトリの内容が表示されます。これらの組み合わせに意味があるのは、lsコマンドによる通常の出力が非常に長い場合だけです。たとえば、ls /devコマンドを使用してdevディレクトリの内容を表示する場合、参照できるのは、ウィンドウ内に表示されているわずかな部分だけです。ls /dev | lessコマンドを使用すると、リスト全体を参照できます。

コマンドの出力をファイル内に保存することもできます。たとえば、echo "test one" > Contentというコマンドは、test oneという語句を含むContentという名前のファイルを生成します。less Contentコマンドを使用すると、このファイルの内容を表示できます。

ファイルをコマンドの入力として使用することもできます。たとえば、trを使って、ファイルContentからリダイレクトされた標準入力の文字を置換し、

結果を標準出力に書き出すことを考えてみます。tをxで置き換えるために、tr t x < Contentと入力します。trの出力は、画面へ送信されます。

出力を格納する新しいファイルが必要な場合、trコマンドの出力をファイルへパイプ(リダイレクト)することができます。これをテストするには、内容をtestに変更してから、コマンドtr t x < ../Content > newを実行します。最後に、newの内容をless newで確認します。

標準出力と同様、標準エラー出力も画面へ送信されます。しかし、標準エラー出力をerrorsというファイルへリダイレクトするには、該当のコマンドに対して2> errorsを指定します。>&alloutputを追加した場合は、標準出力と標準エラー出力の両方が、alloutputという1つのファイルに保存されます。最後に、コマンドの出力を既存のファイルに追加するには、そのコマンドの最後に、1つの > ではなく、>> を指定する必要があります。

27.1.8 アーカイブとデータ圧縮

ここまでで、多くのファイルとディレクトリを作成しました。次に、アーカイブとデータ圧縮について説明します。ここでは、testディレクトリ全体をパックして1つのファイルに記録し、そのファイルのバックアップコピーをフロッピーディスクに保存するか、電子メールで送信できるようにしたいと思います。この作業を行うには、tar (*tape archiver*の略称)コマンドを使用します。tar --helpコマンドを使用すると、tarコマンドのすべてのオプションを表示できます。これらのオプションのうち、重要度の高いものを以下で説明します。

-c
(createの略)新しいアーカイブを作成します。

-t
(tableの略)新しいアーカイブの目次(table of contents)を作成します。

-x
(extractの略)アーカイブをアンパック(展開)します。

-v
(verboseの略)アーカイブの作成中に、すべてのファイルを画面に表示します。

-f

(fileの略)アーカイブファイルに割り当てるファイル名を指定します。アーカイブを作成する場合、このオプションを最後に指定する必要があります。

testディレクトリ、およびその配下のすべてのファイルとサブディレクトリをパックしてtestarchive.tarというアーカイブファイル内に保存するには、-cと-fの各オプションを使用します。この例では、テストの目的で、-vも指定して、アーカイブの進行状況を確認します。このオプションは必須ではありません。cdコマンドを使用して、testディレクトリの配置先である自分のホームディレクトリへ移動した後、tar -cvf testarchive.tar testコマンドを入力します。その後、tar -tf testarchive.tarコマンドを使用して、このアーカイブファイルの内容を表示します。testディレクトリ、およびその配下のすべてのファイルとディレクトリは、そのままハードディスク上に残ります。このアーカイブをアンパック(展開)するには、tar -xvf testarchive.tarコマンドを入力します。 しかし、今の時点では、このコマンドを実行しないでください。

ファイル圧縮の場合、よく使われるのはgzipです。bzip2を使えば、さらに圧縮率が良くなります。 gzip testarchive.tarと入力します(またはbzip2 testarchive.tarと入力することもできますが、この例ではgzipを使います)。lsコマンドを使用すると、testarchive.tarが存在しなくなっていること、代わりにtestarchive.tar.gzが作成されたことがわかります。このファイルはかなり小さいので、電子メールによる転送やUSBメモリへの保存に適しています。

次に、以前に作成したtest2ディレクトリ内で、このファイルをアンパック(圧縮解除)してみます。この作業を行うには、cp testarchive.tar.gz test2と入力し、このファイルを上記のディレクトリへコピーします。cd test2コマンドを使用して、そのディレクトリへ移動します。拡張子が.tar.gzの圧縮済みアーカイブをunzipするには、gunzipコマンドを使用します。gunzip testarchive.tar.gzと入力します。 その結果、testarchive.tarを取り出すことができます。このファイルは、tar -xvf testarchive.tarコマンドを使用して展開、または*圧縮解除(tar解除)* する必要があります。unzipと圧縮アーカイブの展開は、tar -xvf testarchive.tar.gzで一度に行うこともできます(-zオプションの追加は、必要なくなりました)。lsコマンドを使用すると、新しいtestディレク

トリが作成されたことを確認できます。 その内容は、自分のホームディレクトリ内にあるtestディレクトリとまったく同じものです。

27.1.9 mtools

mtoolsとは、MS-DOSファイルシステムの作業をするための一連のコマンドのことです。mtools内のコマンドを使用すると、1台目のフロッピーディスクドライブをMS-DOS環境と同様にa: として扱ったり、mが接頭辞になる(先頭に付く)点を除き、MS-DOSコマンドに似たコマンドが使用可能になります。

mdir a:
a: ドライブ内にあるフロッピーディスクの内容を表示します。

mcopy Testfile a:
Testfileファイルをフロッピーディスクにコピーします。

mdel a:Testfile
a: にあるTestfileを削除します。

mformat a:
フロッピーディスクをMS-DOS形式でフォーマットします(内部でfdformatコマンドを使用します)。

mcd a:
a: をカレントディレクトリにします。

mmd a:test
フロッピーディスク上にtestサブディレクトリを作成します。

mrd a:test
フロッピーディスクからtestサブディレクトリを削除します。

27.1.10 クリーンアップ

この入門コースで、Linuxのシェル、言い換えるとコマンドラインの基本について理解できたはずです。rmとrmdirコマンドを使用して、テスト用のさまざまなファイルとディレクトリを削除することにより、自分のホームディレ

クトリをクリーンアップすることもできます。項27.3.「Linuxの重要なコマンド」 (page 437)には、最も重要なコマンドと、それらの機能についての簡単な説明が記されています。

27.2　ユーザとアクセス権

1990年代初期の開始以来、Linuxはマルチユーザシステムとして開発が進められてきました。任意の数のユーザがLinux上で同時に作業することができます。ユーザは各自のワークステーションでセッションを開始する前に、システムにログインする必要があります。各ユーザは、各自のユーザ名およびそれに対応するパスワードを持っています。このようにユーザが区別されているので、権限のないユーザが、アクセス権のないファイルを表示できないことが保証されています。新しいプログラムをインストールするなど、より大きな変更をシステムに加える作業は、一般のユーザは通常は実行できないか、制約を加えられています。rootユーザ、またはスーパユーザだけが、システムに変更を加える制限なしの権限と、すべてのファイルに対する制限なしのアクセス権を持っています。この概念を理解した上で、必要な場合にのみ`root`ユーザでログインし、完全なアクセス権を使用することが求められます。その結果、意図せずにデータを失うリスクを軽減することができます。一般的な状況では、システムファイルの削除やハードディスクのフォーマットを実行できるのはrootユーザだけです。そのため、一般ユーザとしてログインしていれば、*トロイの木馬*や、破壊的なコマンドを誤って入力することに起因する脅威を大幅に軽減できます。

27.2.1　ファイルシステムのパーミッション

基本的に、Linuxファイルシステム内にある各ファイルは、1人のユーザと1つのグループに所属しています。この所有グループと他のすべてのユーザに対して、これらのファイルへの書き込み、読み取り、または実行を許可することができます。

この状況では、グループとは、特定のいくつかの権利を共通に持つ、互いに関連付けられた一連のユーザと定義することができます。たとえば、あるプロジェクトに携わっているグループを`project3`と呼ぶことにします。Linuxシステム内のあらゆるユーザは、少なくとも1つの所有グループ、通常は`users`グループのメンバに所属します。1つのシステム内に、必要に応じてグループをいくつ作成してもかまいませんが、グループを追加できるのは`root`ユーザ

だけです。どのユーザも、groupsコマンドを使用して、自分が所属しているグループを確認することができます。

ファイルアクセス

ファイルシステム内でのパーミッション(アクセス権)の編成は、ファイルごと、ディレクトリごとに異なります。ファイルのパーミッション情報は、ls -lコマンドを使用して表示できます。出力例については、例27.1.「ファイルパーミッションを示すサンプル出力」(page431)を参照してください。

例 27.1 *ファイルパーミッションを示すサンプル出力*

```
-rw-r----- 1 tux project3 14197 Jun 21  15:03 Roadmap
```

3番目の列が示しているように、このファイルはユーザtuxに所属しています。また、このファイルはグループproject3に対して割り当てられています。Roadmapファイルのユーザパーミッションを調べるには、最初の列を詳細に検討する必要があります。

-	rw-	r--	---
タイプ	ユーザパーミッション	グループパーミッション	他のユーザのパーミッション

この列は、先頭に1つの文字があり、その後に3文字ずつ3つのブロック、つまり9つの文字が続く構成です。10文字のうち最初の1文字は、ファイルシステムコンポーネントのタイプを表す略称です。ダッシュ(-)は、これがファイルであることを意味します。ディレクトリ(d)、リンク(l)、ブロックデバイス(b)、またはキャラクタデバイスが代わりに表示されることもあります。

続く3つのブロックは、標準的なパターンに従っています。各ブロックの最初の文字は、ファイルが読み取り可能(r)またはそうでないこと(-)を意味します。中間の位置にあるwは、対応するオブジェクトが編集可能であることを示し、ダッシュ(-)であれば、ファイルへの書き込みが不可能であることを意味します。3番目の位置にあるxは、そのオブジェクトが実行可能であることを意味します。この例のファイルはテキストファイルなの

で、実行可能ではありません。したがって、この特定のファイルに対する実行可能アクセス権は必要ありません。

この例では、tuxはRoadmapファイルの所有者として、読み取りアクセス権(r)および書き込みアクセス権(w)を持っていますが、このファイルを実行する(x)ことはできません。project3グループのメンバは、このファイルを読み取ることはできますが、変更や実行はできません。他のユーザは、このファイルに対するアクセス権が何もありません。他のパーミッションは、アクセス制御リスト(ACL)を使用して割り当てることができます。背景となる情報は、項27.2.6.「アクセス制御リスト(ACL)」 (page 436)を参照してください。

ディレクトリパーミッション

ディレクトリに対応するアクセス権は、タイプがdと表示されています。ディレクトリの場合、個別のパーミッションは、やや異なる意味を持ちます。

例 27.2 *ディレクトリパーミッションを示すサンプル出力*

```
drwxrwxr-x 1 tux project3 35 Jun 21 15:15  ProjectData
```

例 27.2.「ディレクトリパーミッションを示すサンプル出力」 (page 432)では、ディレクトリProjectDataの所有者(tux)と所有グループ(project3)を簡単に識別できます。ファイルアクセス (page 431)で説明したファイルのアクセス権(パーミッション)とは異なり、読み取りアクセス権(r)を持つことは、ディレクトリの内容を表示できることを意味します。書き込みアクセス権(w)の場合は、新しいファイルを作成できることを意味します。実行可能アクセス権(x)の場合は、ユーザがこのディレクトリに変更を加えられることを意味します。上記の例では、ユーザtuxとproject3グループのメンバがProjectDataディレクトリに変更を加え(x)、内容を表示し(r)、このディレクトリにファイルを追加する(w)ことができることを表します。一方、他のユーザに対して与えられているのは、それより少ないアクセス権です。このディレクトリにアクセスし(x)、内容を閲覧する(r)ことはできますが、新しいファイルを作成する(w)ことはできません。

27.2.2 ファイルパーミッションの変更

アクセス権の変更

ファイルまたはディレクトリに対するアクセス権を変更できるのは、所有者とrootユーザです。chmodコマンドで、パーミッションを変更するパラメータと1つ以上のファイル名を指定することにより変更します。パラメータは、次のカテゴリに分けられます。

1. 対象ユーザ

- u (ユーザ)—ファイルの所有者
- g (グループ)—ファイルの所有者が所属するグループ
- o (*その他*)—その他のユーザ(パラメータが何も指定されていない場合、変更はすべてのカテゴリに対して適用されます)

2. 削除 (–)、セット(=)、または挿入(+)を表す文字

3. 略称

- r—*読み取り*
- w—*書き込み*
- x—*実行*

4. 空白によって区切られた1つ以上のファイル名

たとえば、例 27.2.「ディレクトリパーミッションを示すサンプル出力」(page 432)で、tuxユーザが、その他のユーザに対してProjectDataディレクトリへの書き込み(w)アクセス権を許可する場合、chmod o+w ProjectDataコマンドを使用します。

また、自分以外のユーザに対する書き込みパーミッションを拒否する場合は、chmod go-w ProjectDataコマンドを入力します。すべてのユーザに対して、ProjectDataディレクトリに新しいファイルを追加することを禁止するには、chmod -w ProjectDataと入力します。その場合、このディレクトリの所有者であっても、最初に書き込みパーミッションを再

確立するまでは、このディレクトリ内でファイルを作成することができません。

所有に関するパーミッションの変更

ファイルシステムコンポーネントの所有に関するパーミッションを制御する他の重要なコマンドは、chown (change owner)コマンドとchgrp(change group)コマンドです。chownコマンドを使用すると、ファイルの所有権を他のユーザに移すことができます。しかし、このような変更を行うことができるのは、rootユーザだけです。

例 27.2.「ディレクトリパーミッションを示すサンプル出力」 (page 432)のRoadmapファイル所有権を、tuxではなく、geekoユーザにするとします。 その場合、rootユーザで、chown geeko Roadmapコマンドを入力します。

chgrpコマンドは、ファイル所有者の所属グループを変更します。ただし、そのファイルの所有者は、新しいグループのメンバでなければなりません。この方法により、例 27.1.「ファイルパーミッションを示すサンプル出力」 (page 431)のtuxユーザは、chgrp project4 ProjectDataコマンドを使用して、ProjectDataファイル所有者の所属グループをproject4に切り替えることができます。ただし、このユーザが、この新しいグループのメンバであることが条件です。

27.2.3 setuidビット

特定の状況では、アクセス権の制約が強すぎることがあります。したがって、Linuxは、特定のアクションが実行できるように、現在のユーザとグループのID(身分とその権限)を一時的に変更できるようにする追加の設定項目を用意しています。たとえば、passwdプログラムでは、一般に/etc/passwdにアクセスする際にrootユーザのパーミッションが必要です。このファイルには、ユーザのホームディレクトリ、ユーザとグループのIDなどの重要情報が含まれます。したがって、このファイルへのアクセスをすべてのユーザに許可することは危険が大きいので、一般ユーザはpasswdを変更できません。この問題の解決策は*setuid*メカニズムです。 setuid (set user ID)は、特別なファイル属性であり、マークされたプログラムを特定のユーザIDで実行するようシステムに指示します。次のようなpasswdコマンドを検討してみます。

```
-rwsr-xr-x  1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

sという文字が表示されていて、ユーザパーミッションでsetuidビットがセットされていることを示しています。setuidビットによって、passwdコマンドを実行するすべてのユーザは、rootで実行できます。

27.2.4 setgidビット

setuidビットはユーザに適用されます。ただし、グループにも*setgid*ビットという同等のプロパティがあります。この属性がセットされているプログラムは、どのユーザがそのプログラムを起動したかにかかわりなく、そのプログラムと共に保存されているグループIDを使用して動作します。したがって、setgidビットがオンになっているディレクトリ内では、新しく作成されるすべてのファイルとサブディレクトリは、そのディレクトリが所属しているグループに対して割り当てられます。次のサンプルディレクトリについて考えてみます。

```
drwxrws--- 2 tux archive 48 Nov 19 17:12
   backup
```

sという文字が表示されていて、グループパーミッションでsetgidビットがセットされていることを示しています。ディレクトリの所有者とarchiveグループのメンバは、このディレクトリにアクセスできます。このグループのメンバではないユーザは、適切なグループに「マップ」されます。書き込まれたすべてのファイルの有効なグループIDはarchiveです。.たとえば、グループIDarchiveで実行されるバックアッププログラムは、ルート権限なしにこのディレクトリにアクセスできます。

27.2.5 sticky(スティッキー)ビット

*sticky(スティッキー)ビット*もあります。このビットは、実行可能プログラムとディレクトリのどちらに所属しているかにより意味が異なります。このビットがプログラムに所属している場合、このようにマークが付けられたファイルは、使用するたびにハードディスクにアクセスする必要がないようにRAMにロードされます。現在のハードディスクは十分高速なので、この属性はほとんど使用されなくなっています。このビットをディレクトリに割り当てた場合、各ユーザが他のユーザのファイルを削除することが防止されます。一般的な使用例として、/tmpと/var/tmpの各ディレクトリを挙げることができます。

```
drwxrwxrwt   2 root  root   1160 2002-11-19 17:15 /tmp
```

27.2.6　アクセス制御リスト(ACL)

伝統的なパーミッションの概念は、ファイルやディレクトリなど、Linuxのファイルシステムオブジェクトを対象にしていますが、ACL(アクセス制御リスト)は、この概念を拡張できます。ACLを使用すると、ファイルシステムオブジェクトの元の所有者や所有グループ以外に、個別のユーザまたはグループにパーミッションを割り当てることができます。

拡張アクセス権が有効になっているファイルまたはディレクトリは、簡単な`ls -l`コマンドを使用して検出できます。

```
-rw-r--r--+ 1 tux project3 14197 Jun 21  15:03 Roadmap
```

`Roadmap`ファイルの所有者は`tux`で、このユーザは`project3`グループに所属しています。`tux`はこのファイルに対する書き込みと読み取りの両方のアクセス権を持っています。グループおよびその他のすべてのユーザは読み取りアクセス権を持っています。このファイルを、ACLなしのファイルと区別するための唯一の違いは、パーミッションビットを保持する最初の列で、追加の+が表示されていることです。

ACLの詳細を把握するために、`getfacl Roadmap`コマンドを実行してみます。

```
# file: Roadmap
# owner: tux
# group: project3
user::rw-
user:jane:rw-       effective: r--
group::r--
group:djungle:rw-   effective: r--
mask::r--
other::---
```

出力のうち最初の3行は、`ls -l`コマンドから得られるのと同じ情報であり、独自の情報はありません。これらの行は、ファイル名、所有者、および所有グループだけを示しています。4行目から9行目は、ACLエントリを保持しています。従来のアクセス権は、ACLを使用したときに利用可能になる属性の一部だけを表すことになります。上記のサンプルにおけるACLは、ファイルの所有者およびユーザ`jane`に対して読み取りと書き込みのアクセス権を許可しています(4行目と5行目)。従来の概念が拡張されて、追加ユーザによるアクセスを許可するようになりました。同じことは、グループアクセスを扱う際にも適用されます。所有グループは読み取りアクセス権(6行目)を保持し、

djungleグループは読み取りと書き込みのアクセス権を保持しています。8行目のmaskエントリは、ユーザjaneとdjungleグループの有効なアクセス権を減らして、読み取りアクセスのみにしています。他のユーザとグループは、このファイルに対して、アクセス権を何も持っていません(9行目)。

ここまでで、ごく基本的な情報だけを紹介しました。ACLについての詳細は、章 24. *Linuxのアクセス制御リスト* (page 379)を参照してください。

27.3 Linuxの重要なコマンド

ここでは、SUSE Linuxシステムの非常に重要なコマンドについて説明します。この章に掲載した以外にも、多くのコマンドがあります。個別のコマンドとそのパラメータを掲載し、必要な場合は一般的なサンプルアプリケーションを紹介します。さまざまなコマンドの詳細については、マニュアルページ(manページ)を参照してください。manの後にコマンド名、たとえば、man lsと入力すると、そのコマンドのマニュアルページを表示できます。

manページでは、PgUpとPgDnを使用して上下に移動できます。HomeとEndを使用すると、それぞれドキュメントの最初と最後に移動できます。Qを押すと、この表示モードが終了します。manコマンド自体の詳細については、man manと入力します。

以下の概要では、各コマンド要素を本文とは異なる書体で表記しています。実際のコマンド名とその必須オプションは、command optionの形式で表記します。必須ではない詳細指定やパラメータは、[ ](角かっこ)内で表記します。

設定値は、実際の状況に合わせて変更してください。ls fileという入力は、fileというファイルが実際に存在している場合以外は、意味がありません。ほかに、通常は、複数のパラメータを組み合わせることができます。 たとえば、ls -l -aの代わりに、ls -laと入力することができます。

27.3.1 ファイル関連コマンド

以降のセクションでは、ファイル管理に使用する非常に重要なコマンドについて説明します。一般的なファイル管理からファイルシステムのACL操作まであらゆる事柄を説明します。

ファイル管理

ls [options] [files]

パラメータなしでlsコマンドを実行した場合、このプログラムはカレントディレクトリの内容を短い形式でリストします。

-l
詳しいリストを表示します。

-a
隠しファイルを表示します。

cp [options] source target

sourceをtargetにコピーします。

-i
必要な場合、つまりtargetfileが既に存在し、そのファイルへ上書きする場合は、確認を求めます。

-r
再帰コピーを行います(サブディレクトリもコピーします)。

mv [options] source target

sourceをtargetへコピーし、元のsourceを削除します。

-b
移動する前に、sourceのバックアップコピーを作成します。

-i
必要な場合、つまりtargetfileが既に存在し、そのファイルへ上書きする場合は、確認を求めます。

rm [options] files

指定されたファイルをファイルシステムから削除します。-rオプションを指定しない限り、rmコマンドを使用してディレクトリを削除することはできません。

-r
既存のサブディレクトリをすべて削除します。

-i
各ファイルを削除する前に、確認を求めます。

ln [options] source target

sourceからtargetへの内部リンクを作成します。通常、このリンクは、同じファイルシステム上のsourceを直接指しています。しかし、-sオプションを指定してlnコマンドを実行した場合、このコマンドは、sourceが存在しているディレクトリを指すだけのシンボリックリンクを作成します。 その結果、ファイルシステム間でのリンクが可能になります。

-s
シンボリックリンクを作成します。

cd [options] [directory]

カレントディレクトリを変更します。cdコマンドにパラメータを指定しない場合、そのユーザのホームディレクトリへ移動します。

mkdir [options] directory

新しいディレクトリを作成します。

rmdir [options] directory

指定されたディレクトリが既に空である場合、そのディレクトリを削除します。

chown [options] username[:[group]] files

ファイルの所有権を、指定されたユーザ名を持つユーザへ移動します。

-R
すべてのサブディレクトリ内にあるファイルとディレクトリを変更します。

chgrp [options] groupname files

特定のfileに対するグループ所有権を、指定されたグループ名を持つグループへ移動します。ファイル所有者は、現在のグループと新しいグループ両方のメンバーである場合に限って、グループ所有権を変更できます。

chmod [options] mode files

アクセス権を変更します。

modeパラメータは、group、access、およびaccess typeという3つの部分で構成されています。group(グループ)は、次の各文字を受け付けます。

u
user

g
group

o
others

access(アクセス)は、+でアクセスを許可し、-でアクセスを拒否します。

access type(アクセスタイプ)を制御するには、次のオプションを使用します。

r
read

w
write

x
実行—ファイルの実行、または指定ディレクトリへの移動を可能にします。

s
uidビットの設定-あたかもファイルの所有者が起動したかのように、アプリケーションまたはプログラムを起動します。

代わりに、数値コードを使用することもできます。このコードを構成する4桁の各数字は、4、2、および1の中から状況に応じて選択された値を合算したものです つまり、2進(バイナリ)マスクの合計を10進表記したものです。最初の桁で、設定するユーザID (set user ID、SUID) (4)、設定するグループID (2)、およびスティッキー(sticky) (1)の各フラグを設定します。2番目の桁で、ファイルの所有者に割り当てるアクセス権を定義します。3番目の桁で、グループメンバーに割り当てるアクセス権を定義します。最後の桁では、他のすべてのユーザに割り当てるアクセス権を設定します。読み取りアクセス権を設定するには4、書き込みアクセス権を設定するには2、およびファイルの実行アクセス権を設定するには1を使用します。ファイルの所有者の場合、通常は6または7が実行可能ファイルに指定されます。

gzip [parameters] files

このプログラムは、複雑な算術アルゴリズムを使用して、ファイルの内容を圧縮します。この方法で圧縮されたファイルは.gz拡張子を割り当てられ、使用する前に圧縮解除する必要があります。複数のファイルまたはディレクトリ全体を圧縮するには、tarコマンドを使用します。

-d
パックされたgzipファイルを圧縮解除して元のサイズに戻し、通常の方法で処理できるようにします(gunzipコマンドに似ています)。

tar options archive files

tarコマンドは、1つ以上のファイルを1つのアーカイブ内に格納します。圧縮はオプションです。tarコマンドは、多くのオプションを持つ、かなり複雑なコマンドです。使用頻度の高いオプションは、以下のとおりです。

-f
出力を画面ではなくファイルに書き込みます。 これは一般的な使用方法です。

-c
新しいtarアーカイブを作成します。

-r
既存のアーカイブにファイルを追加します。

-t
アーカイブの内容を出力します。

-u
ファイルを追加する際に、対応するファイルが既にアーカイブ内に存在している場合、追加するファイルがアーカイブ内のファイルより新しければ追加します。

-x
アーカイブ内のファイルをアンパック(*展開*)します。

-z
生成されたアーカイブを、gzipコマンドを使用してパックします。

-j
生成されたアーカイブを、bzip2コマンドを使用して圧縮します。

-v
処理されたファイルをリストします。

tarコマンドが作成したアーカイブファイルの最後には、.tarが付きます。gzipコマンドを使用してtarアーカイブを圧縮した場合、ファイル名の最後は.tgzまたは.tar.gzになります。bzip2コマンドを使用して圧縮した場合、ファイル名の最後は.tar.bz2になります。応用例は、項27.1.8.「アーカイブとデータ圧縮」 (page 427)を参照してください。

locate patterns

このコマンドはfindutils-locateパッケージをインストールした場合にのみ、利用できます。locateコマンドは、指定されたファイルが存在するディレクトリを検索できます。必要に応じて、ワイルドカードを使用して、ファイル名を指定することができます。このプログラムは(ファイルシステム全体を検索する代わりに)専用に作成したデータベースを使用するので、非常に高速です。しかし、この事実は、大きな欠点も抱えています。locateは、データベースの最新の更新より後に作成されたファイルを見つけることができません。このデータベースを生成するには、rootユーザでupdatedbコマンドを使用します。

updatedb [options]

このコマンドは、locateコマンドが使用するデータベースを更新します。既存のすべてのディレクトリ内にあるファイルをこのデータベースに登録するには、rootユーザでこのプログラムを実行します。アンパサンド(&)を追加してこのプログラムをバックグラウンドで実行することには、意味があります。 その場合、同じコマンドライン(updatedb &)上で、直ちに作業を続けることができるからです。このコマンドは通常、毎日cronジョブとして実行します(cron.dailyを参照してください)。

find [options]

findコマンドを使用すると、特定のディレクトリ内でファイルを検索することができます。最初の引数は、検索を開始するディレクトリを指定します。-nameオプションの後には、検索文字列を指定する必要があります。その中でワイルドカードを使用することもできます。データベースを使用するlocateとは異なり、findコマンドは実際のディレクトリを検索します。

ファイルの内容にアクセスするコマンド

cat [options] files

catコマンドは、ファイルの内容を表示します。特に、ファイルの内容全体を、一時停止なしで画面に出力します。

-n
出力の左マージンに、行番号を表示します。

less [options] files

このコマンドは、指定されたファイルの内容を閲覧する目的で使用できます。PgUpとPgDnを使用して画面を半ページだけ上または下にスクロールすることや、Spaceを使用して画面1ページ分を下に移動することができます。HomeとEndを使用すると、ファイルの最初または最後に移動できます。Qを押すと、このプログラムが終了します。

grep [options] searchstring files

grepコマンドは、指定された1つ以上のファイルの中で、特定の検索文字列を見つけます。検索文字列が見つかった場合、searchstringを含む行と該当のファイル名が表示されます。

-i
大文字と小文字を区別しません。

-H
該当するファイルの名前だけを表示し、テキスト行を表示しません。

-n
文字列が見つかった行の行番号も追加で表示します。

-l
searchstringを含んでいないファイルの名前だけを出力します。

diff [options] file1 file2

diffコマンドは、指定された2つのファイルの内容を比較します。このプログラムの出力は、一致していないすべての行をリストします。プログラマがソースコード全体ではなく、プログラムの変更箇所だけを送信する必要が生じた場合に、このコマンドがよく使用されます。

-q
2つのファイルに違いがあるかどうかだけを報告します。

-u
「統合された」diffを出力します。出力がより読みやすくなります。

ファイルシステム

mount [options] [device] mountpoint

このコマンドを使用すると、ハードディスク、CD-ROMドライブ、および他のドライブなど、あらゆるデータメディアを、Linuxファイルシステムのディレクトリにマウントすることができます。

-r
読み取り専用でマウントします。

-t filesystem
ファイルシステムを指定します。最も一般的なのは、Linuxハードディスクを表すext2、MS-DOSメディアを表すmsdos、Windowsファイルシステムを表すvfat、およびCDを表すiso9660です。

/etc/fstabファイル内で定義されていないハードディスクについては、デバイスタイプも指定する必要があります。この場合、マウントを実行できるのはrootユーザだけです。他のユーザがファイルシステムをマウントする必要がある場合、/etc/fstabファイル内の該当行にuserオプションを入力し、その変更結果を保存します。複数のユーザを指定する場合はカンマ(,)で区切ります。詳細については、mount(1)のmanページを参照してください。

umount [options] mountpoint

このコマンドは、マウント済みドライブをファイルシステムからマウント解除(アンマウント)します。データの損失を防止するために、リムーバブルデータメディアをドライブから取り出す前に、このコマンドを実行してください。通常、mountコマンドとumountコマンドを実行できるのはrootユーザだけです。他のユーザもこれらのコマンドを実行できるようにするには、/etc/fstabファイルを編集し、該当するドライブに対してuserオプションを指定します。

27.3.2 システム関連コマンド

以降のセクションでは、システム情報を検索し、プロセスし、ネットワーク制御のために必要な非常に重要なコマンドのいくつかを説明します。

システム情報

df [options] [directory]

df (disk free)コマンドをオプションなしで使用した場合、マウント済みのすべてのドライブに関する全ディスク容量、現在使用中のディスク容量、

および空き容量を表示します。ディレクトリを指定した場合、そのディレクトリの配置先ドライブに関する情報だけが表示されます。

-h
使用中のブロック数を、ギガバイト(GB)、メガバイト(MB)、またはキロバイト(KB)単位で表示します。一般的に読みやすい形式です。

-T
ファイルシステムのタイプ(ext2、nfsなど)を表示します。

du [options] [path]

このコマンドをパラメータなしで実行した場合、カレントディレクトリ内にある各ファイルとサブディレクトリが使用している全ディスク容量を表示します。

-a
個別のファイルのサイズを表示します。

-h
一般的に読みやすい形式で出力します。

-s
計算後の合計サイズだけを表示します。

free [options]

`free`コマンドは、RAMとスワップ領域の使用状況、および両方のカテゴリでの全容量と使用中容量に関する情報を表示します。詳細については、項30.1.6. 「freeコマンド」 (page 502)を参照してください。

-b
バイト単位で出力します。

-k
キロバイト(KB)単位で出力します。

-m
メガバイト(MB)単位で出力します。

date [options]

この簡単なプログラムは、現在のシステム時刻を表示します。rootユーザでこのコマンドを実行した場合、システム時刻を変更することもできます。このプログラムの詳細については、date(1)のmanページを参照してください。

プロセス

top [options]

topコマンドは、現在動作しているプロセスの概要を表示します。Hを押すと、このプログラムをカスタマイズするための主要なオプションについて簡単に説明しているページにアクセスできます。

ps [options] [process ID]

オプションなしで実行した場合、このコマンドは現在のユーザ独自のプログラムまたはプロセスすべてからなる表を表示します。それらは、現在のユーザが起動したものを意味します。このコマンドでオプションを指定する場合、ハイフンは付けません。

aux
所有者に関係なく、すべてのプロセスからなる詳しいリストを表示します。

kill [options] process ID

作業中、プログラムが通常の方法で終了できなくなることがあります。ほとんどの場合、該当するプロセスID(topコマンドとpsコマンドを参照)を指定し、killコマンドを実行することにより、そのような暴走したプログラムを終了させることができます。killコマンドは、*TERM*シグナルを送信します。このシグナルは、そのようなプログラムに対して、自らを終了するよう指示します。これだけでは解決しない場合、次のパラメータを使用できます。

-9
*TERM*シグナルの代わりに*KILL*シグナルを送信します。これで、ほとんどすべての場合、指定されたプロセスが終了します。

killall [options] processname

このコマンドはkillコマンドに似ていますが、引数として(プロセスIDではなく)プロセス名を使用し、その名前を持つすべてのプロセスを終了させます。

ネットワーク

ping [options] hostnameまたはIP address

pingコマンドは、TCP/IPネットワークの基本的な機能をテストする標準的なツールです。小さいデータパケットを送信先ホストへ送信し、即座の応答を要求します。この作業が成功した場合、pingコマンドは、その結果を知らせるメッセージを表示します。これは、ネットワークリンクが基本的に機能していることを意味します。

-c *number*
送信するパケットの総数を決定し、それらをディスパッチし終わった後で処理を終了します(デフォルトでは、上限は設定されていません)。

-f
flood ping(pingの洪水): できるだけ多くのデータパケットを送信します。一般的には、rootがネットワークをテストする目的で使用します。

-i *value*
2つのデータパケットの間の間隔を秒単位で指定します(デフォルトは、1秒です)。

nslookup

ドメインネームシステム(DNS)は、ドメイン名からIPアドレスへの変換を行います。このツールは、ネームサーバ(DNSサーバ)に問い合わせを送信します。

telnet [options] hostnameまたはIP address [port]
Telnetは、実際のところ、ネットワーク経由でリモートホスト上での操作を可能にするインターネットプロトコルの1つです。telnetは、このプロトコルを使用してリモートコンピュータ上での操作を可能にするLinuxプログラムの名前でもあります。

警告

第三者が「傍受」可能なネットワークを経由する場合、telnetを使用しないでください。特にインターネットを経由する場合、パスワードが悪用されるリスクを回避するために、sshコマンドのような暗号化された伝送方法を使用してください(sshコマンドのmanページを参照してください)。

その他

passwd [options] [username]

ユーザはこのコマンドを使用することにより、自分のパスワードをいつでも変更できます。管理者rootはこのコマンドを使用して、システム上に存在するあらゆるユーザのパスワードを変更できます。

su [options] [username]

suコマンドは、実行中のセッションから、他のユーザ名を使用してログインできるようにします。ユーザ名と、対応するパスワードを指定してください。rootユーザはあらゆるユーザのID (身元)を使用することが承認されているので、rootがこのコマンドを使用する場合は、パスワードの入力を要求されません。ユーザの名前を指定しないでこのコマンドを使用する場合、rootのパスワードの入力を求めるプロンプトが表示され、スーパーユーザ(root)に変更されます。

-

別なユーザとしてログインシェルを開始するには、su -を使います。

halt [options]

データの損失を防止するために、システムをシャットダウンする場合、必ずこのコマンドを使用することをお勧めします。

reboot [options]

システムが直ちにリブートすることを除き、このコマンドは、haltコマンドと同じ処理を実行します。

clear

このコマンドは、コンソールの表示領域すべてをクリアします。オプションはありません。

27.3.3 関連資料

この章に掲載した以外にも、多くのコマンドがあります。他のコマンドの概要、またはより詳しい情報については、オライリー刊の*Linux in a Nutshell*(邦訳『Linux クイックリファレンス』)をお勧めします。

27.4 viエディタ

プログラミングのみでなく、多くのシステム管理タスクにも、相変わらずテキストエディタが使用されています。Unixでは、viは使いやすい編集機能を提供し、マウスサポート機能を持つ多数のエディタに比べて人間工学の面から優れたエディタとなっています。

27.4.1 動作モード

基本的にviは、次の3つの動作モードを使用します。それは*挿入*モード、コマンドモード、および*拡張*モードです。キーの機能は動作モードに応じて異なります。起動時には、通常、viはコマンドモードに設定されます。まず、モード間で切り替える方法について説明します。

コマンドモードから挿入モードへ
さまざまな方法があり、追加の場合は[a]、挿入の場合は[i]、現在行の下に新規行を挿入する場合は[o]を使用します。

挿入モードからコマンドモードへ
*挿入*モードを終了するには、[Esc]を押します。 viは、*挿入*モードになっていると、終了できません。[Esc]を押す習慣を付けることが大切です。

コマンドモードから拡張モードへ
viの*拡張*モードを有効にするには、コロン([:])を入力します。*拡張*(*ex*)モードは、単純なものから複雑なものまで各種タスクに使用できる行単位のエディタです。

拡張モードからコマンドモードへ
*拡張*モードでコマンドを実行した後、エディタは自動的にコマンドモードに戻ります。*拡張*モードでコマンドを実行しないことにした場合は、←でコロンを削除します。エディタはコマンドモードに戻ります。

*挿入*モードから*拡張*モードに直接切り替えることはできません。まず、コマンドモードに切り替える必要があります。

他のエディタと同様に、viにも独自の終了手順があります。*挿入*モードではviを終了できません。最初に、Escを押して*挿入*モードを終了します。その後は、次の2つの選択肢があります。

1. *変更内容を保存せずに終了:* 変更内容を保存せずにエディタを終了するには、コマンドモードで:–q–!と入力します。感嘆符(!)を付けると、viでは変更内容が無視されます。

2. *変更内容を保存して終了:* 変更内容を保存してエディタを終了するには、複数の方法があります。コマンドモードではShift+Z+Zを使用します。*拡張*モードで変更内容をすべて保存してエディタを終了するには、:–W–Qを入力します。*拡張*モードでは、wは「書き込み」、qは「終了」を表します。

27.4.2 操作中のvi

viを標準エディタとして使用できます。*挿入*モードで、テキストの入力と削除に←とDelキーを使用します。カーソル移動には矢印キーを使用します。

ただし、これらのコントロールキーを使用するとしばしば問題が発生します。これは、特殊なキーコードを使用する端末タイプが多数存在するからです。これは、コマンドモードに影響します。Escを押して*挿入*モードからコマンドモードに切り替えます。コマンドモードでは、H、J、K、およびLを使用してカーソルを移動します。各キーの機能は、以下のとおりです。

H
左に1文字分移動します。

J
下に1行分移動します。

K
上に1行分移動します。

L
右に1文字分移動します。

コマンドモードでは、コマンドを使用してさまざまな操作を行うことができます。コマンドを2度以上実行するには、単に反復回数を入力してから実際のコマンドを入力します。たとえば、5Lと入力すると、カーソルは右に5文字分移動します。

表27.1.「viエディタの簡単なコマンド」 (page 452)では、いくつかの重要なコマンドが説明されています。これはごく簡単なものです。詳細なリストは、項27.4.3.「関連資料」 (page 453)のドキュメント内で利用できます。

表 27.1 *viエディタの簡単なコマンド*

Esc	コマンドモードに変更します。
I	挿入モードに変更します(文字は現在のカーソル位置に表示されます)。
A	挿入モードに変更します(文字は現在のカーソル位置の後に挿入されます)。
Shift + A	挿入モードに変更します(文字は行末に追加されます)。
Shift + R	置換モードに変更します(古いテキストを上書きします)。
R	カーソルの下の文字を置き換えます。
O	挿入モードに変更します(現在の行の後に新しい行が挿入されます)。
Shift + O	挿入モードに変更します(現在の行の前に新しい行が挿入されます)。
X	現在の文字を削除します。
D – D	現在の行を削除します。

D – W	現在の語の終わりまで削除します。
C – W	挿入モードに変更します(現在の語の残りの文字が次に入力するエントリに上書きされます)。
U	最後のコマンドを取り消します。
Ctrl + R	取り消された変更を再実行します。
Shift + J	次の行を現在の行と連結します。
.	最後のコマンドを繰り返します。

27.4.3 関連資料

viは多様なコマンドをサポートしています。マクロ、ショートカット、名前付きバッファ、および他の多数の便利な機能を使用できます。各種オプションの詳細については、このマニュアルでは説明しません。SUSE Linuxには、viの改良版であるvim (vi improved)が付属しています。このアプリケーションについては、さまざまな情報源があります。

- vimtutorは、vimの対話形式のチュートリアルです。
- vimで:helpコマンドを入力すると、さまざまなヘルプトピックが表示されます。
- vimに関するマニュアルは、http://www.truth.sk/vim/vimbook-OPL.pdfからオンラインで入手できます。
- http://www.vim.orgにあるvimプロジェクトのWebページでは、あらゆる種類のニュース、メーリングリスト、およびその他のドキュメントが提供されます。
- インターネットでは、多数のvimソースが提供されています。 http://www.selflinux.org/selflinux/html/vim.html, http://www.linuxgazette.com/node/view/9039, and http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html.チュートリアルへのリンク

については、http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html を参照してください。

重要項目: VIMライセンス

vimは、「無償ソフトウェア」です。つまり、作者からはソフトウェアの代金を請求されませんが、資金援助による非営利プロジェクトの支援が奨励されます。このプロジェクトは、ウガンダの貧しい子供たちに対する援助を求めています。詳細については、http://iccf-holland.org/index.html、http://www.vim.org/iccf/、および http://www.iccf.nl/ でオンライン情報を参照してください。

---

28 Linuxシステムのブートと設定

Linuxシステムのブートには、さまざまなコンポーネントが関係しています。この章では、基本になっている原則と、関係しているコンポーネントについて説明します。ランレベルの概念および`sysconfig`によるSUSEのシステム設定についても、この章で説明します。

28.1 Linuxのブートプロセス

Linuxのブートプロセスは、いくつかの段階から成り、それぞれを別のコンポーネントが代表しています。次のリストに、主要なすべてのコンポーネントが関与するブートプロセスと機能を簡潔にまとめています。

1. **BIOS** コンピュータに電源を投入すると、BIOSで画面とキーボードの初期化およびメインメモリのテストが行われます。この段階まで、コンピュータは大容量ストレージメディアにアクセスしません。続いて、現在の日付、時刻、および最も重要な周辺機器に関する情報が、CMOS値からロードされます。最初のハードディスクとそのジオメトリが認識されると、システム制御がBIOSからブートローダに移ります。

2. **ブートローダ** 最初のハードディスクの先頭の512バイト物理データセクタがメインメモリにロードされ、このセクタの先頭に常駐するブートローダが起動します。ブートローダによって実行されたコマンドがブートプロセスの残りの部分を確定します。したがって、最初のハードディスクの先頭512バイトのことを*マスタブートレコード*(MBR)といいます。次に、ブートローダは実際のオペレーティングシステム(この場合はLinux

カーネル)に制御を渡します。GRUB(Linuxのブートローダ)の詳細については、章 29. ブートローダ (page 473)を参照してください。

3. **カーネルとinitramfs**　システムに制御を渡すために、ブートローダは、カーネルとRAMベースの初期ファイルシステム(initramfs)をメモリにロードします。 初期RAMファイルシステムの内容は、カーネルから直接使用されます。 初期RAMファイルシステムには、initと呼ばれる小さな実行可能ファイルが含まれています。これは本当のルートファイルシステムのマウントを行います。 SUSE Linuxの以前のバージョンでは、これらのタスクはそれぞれinitrdとlnuxrcによって実行されていました。 initramfsについての詳細は、項28.1.1. 「initramfs」 (page 456)を参照してください。

4. **initramfs上のinit**　このプログラムは、適切なルートファイルシステムをマウントするために必要なすべてのアクションを実行します。たとえば、必要なファイルシステム用のカーネル機能や、大容量ストレージコントローラ用のデバイスドライバを提供します。 ルートファイルシステムが見つかると、エラーをチェックしてからマウントします。 これが正常に実行されれば、initramfsはクリアされ、ルートファイルシステムのinitが実行されます。 initについての詳細は、項28.1.2. 「initramfs上のinit」 (page 457)を参照してください。

5. **init**　initは、さまざまなレベルでシステムの実際のブートを処理し、各種の機能を提供します。initについては、項28.2. 「initプロセス」 (page 459)で説明しています。

28.1.1　initramfs

initramfsは、カーネルがRAMディスクにロードできる、小さなファイルシステムです。また、実際のルートファイルシステムがマウントされる前にプログラムを実行できるようにする最低限のLinux環境を提供します。 この最低限のLinux環境は、BIOSルーチンでメモリにロードされます。十分な容量のメモリがあること以外には具体的なハードウェア要件はありません。 initramfsには必ず、initという名前の実行可能ファイルがあります。これは、ブートプロセスが進行するにつれて、ルートファイルシステム上の本当のinitプログラムを実行することになります。

実際のルートファイルシステムをマウントして実際のオペレーティングシステムを起動する前に、カーネルには、ルートファイルシステムが配置されて

いるデバイスにアクセスするための対応ドライバが必要です。 こうしたドライバには、特定のハードディスク用の特殊なドライバや、ネットワークファイルシステムにアクセスするためのネットワークドライバが含まれる場合もあります。 ルートファイルシステムで必要となるモジュールは、initramfs上のinitによってロードされます。 initramfsは、ブートプロセス中はずっと利用可能です。 これにより、ブート中に生成されたすべてのhotplugイベントを処理することが可能になります。

インストール済みのシステムのハードウェア(ハードディスク)を変更する必要が生じ、このハードウェアがブート時にカーネル内に存在している以外のドライバを必要とする場合には、initramfsを更新する必要があります。 これは、initramfsの前身であるinitrdの場合と同様に、`mkinitrd`を呼び出すことによって行えます。 引数を付けずに`mkinitrd`を呼び出すと、initramfsが作成されます。 `mkinitrd -R`を呼び出すと、initrdが作成されます。 SUSE Linuxでは、ロードするモジュールは、 `/etc/sysconfig/kernel`の変数`INITRD_MODULES`で指定されます。 インストール後に、この変数は自動的に正しい値に設定されます。モジュールは、`INITRD_MODULES`に指定されている順序で正確にロードされます。複数のSCSIドライバが使用されている場合は、この順序が特に重要です。その理由は、順序が正しくなければハードディスクの名前が変わってしまうためです。厳密に言えば、ルートファイルシステムにアクセスするために必要なドライバをロードするだけで十分でしょう。 しかし、後でロードすると問題が生じることがあるため、initramfsは、インストールに必要なすべてのSCSIドライバをロードします。

重要項目: initramfsまたはinitrdの更新

ブートローダは、カーネルと同じようにinitramfsまたはinitrdをロードします。 GRUBはブート時にディレクトリ内の正しいファイルを検索するので、initramfsまたはinitrdの更新後にGRUBを再インストールする必要はありません。

28.1.2 initramfs上のinit

initramfs上のinitの主な目的は、実際のルートファイルシステムのマウントとそのファイルシステムへのアクセスの準備です。 実際のシステム設定に基づいて、initは以下のタスクを実行します。

カーネルモジュールのロード

ハードウェア設定によっては、使用するコンピュータのハードウェアコンポーネント(ハードディスクになる最も重要なコンポーネント)にアクセスするために特殊なドライバが必要になる場合があります。最終的なルートファイルシステムにアクセスするには、カーネルが適切なファイルシステムドライバをロードする必要があります。

RAIDとLVMのセットアップの管理

RAIDまたはLVMの下でルートファイルシステムを保持するようにシステムを設定した場合、initはLVMまたはRAIDをセットアップして、後でルートファイルシステムにアクセスできるようにします。RAIDについては、項2.3. 「ソフトウェアRAID設定」 (page 70)を参照してください。LVMについては、項2.2. 「LVMの設定」 (page 62)を参照してください。

ネットワーク設定の管理

ネットワークマウントしたルートファイルシステム(NFSを介したマウント)を使用するようにシステムを設定した場合、linuxrcは適切なネットワークドライバがロードされ、ドライバがルートファイルシステムにアクセスできるように設定されていることを確認する必要があります。

初期ブート時にlinuxrcがインストールプロセスの一環として呼び出される場合、そのタスクは前に説明したタスクと異なります。

インストールメディアの検出

インストールプロセスを開始すると、使用するコンピュータでは、インストーラでインストールカーネルと特殊なinitrdがインストールメディアからロードされます。RAMファイルシステムで実行されるインストーラには、インストールメディアにアクセスしてオペレーティングシステムをインストールするために、そのメディアの実際の場所に関する情報が必要になります。

ハードウェア認識の開始および適切なカーネルモジュールのロード

項28.1.1. 「initramfs」 (page 456)で説明しているように、ブートプロセスは、ほとんどのハードウェア設定で使用できる最小限のドライバセットで開始されます。 initは、ハードウェア設定に適したドライバセットを確定する、初期ハードウェアスキャンプロセスを開始します。こうした値は、それ以降のブートプロセスでカスタムinitrdを使用できるように、後で`/etc/sysconfig/kernel`の`INITRD_MODULES`に書き込まれます。 インストールプロセスの間に、initはこの変数で指定されたモジュールセットをロードします。

インストールシステムまたはレスキューシステムのロード
ハードウェアが正しく認識され、適切なドライバがロードされるとすぐに、linuxrcはインストールシステムを起動します。このシステムには、実際のインストーラまたはレスキューシステムが含まれています。

YaSTの開始
最後に、initはYaSTを起動します。これはパッケージのインストールとシステム設定を開始します。

28.2 initプロセス

プログラムinitは、プロセス番号1のプロセスであり、必要な方法でシステムの初期化を実行します。initは特別な役割を果たします。initはカーネルによって直接起動され、通常はプロセスを強制終了するシグナル9が使えないようにします。他のすべてのプログラムは、initまたは子プロセスのいずれかによって直接起動されます。

initの中心的な設定は、`/etc/inittab`ファイルで行われています。このファイルはランレベルを定義しています(項28.2.1. 「ランレベル」 (page 459)を参照)。このファイルはまた、各レベルで利用可能なサービスとデーモンを指定しています。`/etc/inittab`のエントリに応じて、initが複数のスクリプトを実行します。わかりやすくするために、*init*スクリプトと呼ばれるこれらのスクリプトはすべて、ディレクトリ`/etc/init.d`にあります(項28.2.2. 「initスクリプト」 (page 462)を参照)。

システムを起動し、シャットダウンするプロセス全体は、initによって管理されます。この点から見ると、カーネルは、他のプログラムからの要求に従って、他のすべてのプロセスとCPU時間やハードウェアアクセスを管理するバックグラウンドプロセスと考えることができます。

28.2.1 ランレベル

Linuxでは、ランレベルはシステムの起動方法および稼動中のシステムで使用可能なサービスを定義します。ブート後、システムは`/etc/inittab`の`initdefault`行での定義に従って起動します。通常のランレベルは3または5です。表28.1. 「ランレベルの種類」 (page 460)を参照してください。別の方法として、ランレベルをブート時に(たとえばブートプロンプトで)指定するこ

ともできます。パラメータは、カーネル自体が直接評価するもの以外、initに渡されます。

表 28.1　ランレベルの種類

ランレベル	説明
0	システム停止
S	シングルユーザモード(ブートプロンプトからUSキーボードマッピングで入力された場合)
1	シングルユーザモード
2	リモートネットワーク(NFSなど)なしのローカルマルチユーザモード
3	ネットワークを使用するフルマルチユーザモード
4	未使用
5	ネットワークとXディスプレイマネージャのKDM、GDM、またはXDMを使用するフルマルチユーザモード
6	システム再起動

重要項目: /usrパーティションがNFSマウントされている場合にはランレベル2は避ける

システムでNFSを介して/usrパーティションをマウントする場合は、ランレベル2を使用しないでください。/usrディレクトリには、システムが正しく機能するために不可欠な重要なプログラムが入っています。NFSサービスはランレベル2(リモートネットワークのないローカルマルチユーザモード)で利用できるようになっていないので、システムが多くの側面で重大な制約を課されます。

システムの稼動中にランレベルを変更するには、initの後に、ランレベルに対応する番号を引数として入力します。これができるのは、システム管理者

だけです。 次のリストは、ランレベルに関連した最も重要なコマンドの概要です。

init 1またはshutdown now
システムはシングルユーザモードに入ります。 このモードは、システムメンテナンスや管理タスクで使用します。

init 3
(ネットワークを含む)すべての重要なプログラムとサービスが起動します。 グラフィック環境はありませんが、一般ユーザは、システムにログインして作業することができます。

init 5
グラフィック環境は有効になります。 これはデスクトップ(GNOMEまたはKDE)、またはウィンドウマネージャのいずれかになります。

init 0またはshutdown -h now
システムは停止します。

init 6またはshutdown -r now
システムは停止した後、再起動します。

ランレベル5は、すべてのSUSE Linux標準インストールにおけるデフォルトのランレベルです。 ユーザはグラフィックインタフェースでログインするように求められます。デフォルトのランレベルは3で、ランレベルを5に切り替えるには、章 35. *X Windowシステム* (page 567)で説明するようにX Window Systemを正しく設定している必要があります。その後、`init 5`を入力して、システムが意図したとおりに動作するかを確認します。 すべてが意図したとおりに動作した場合は、YaSTを使用してデフォルトのランレベルを5に設定します。

警告: /etc/inittab内のエラーのためシステムブートが失敗することがある

`/etc/inittab`が破損した場合、システムが正しく起動しないことがあります。したがって、`/etc/inittab`の編集はきわめて慎重に行う必要があります。また、必ず変更前のバージョンをバックアップしてください。破損したファイルを修復するには、ブートプロンプトのカーネル名の後に、`init=/bin/sh`と入力して、直接シェルからブートしてみます。その後、コマンド`mount -o remount,rw /`でルートファイルシステムを書き込み可能にし、`cp`を使用して`/etc/inittab`をバックアップバージョンで置き

換えます。ファイルシステムエラーを防止するには、再起動する前にルートファイルシステムを読み取り専用に変更します(`mount -o remount,ro /`)。

ランレベルを変更するときには、一般に2つの操作が行われます。1つは、現在のランレベルの停止スクリプトが起動し、現在のランレベルに必要なプログラムを終了します。次に、新しいランレベルの起動スクリプトが起動します。ここで、ほとんどの場合、プログラムがいくつか起動します。たとえば、ランレベルを3から5に変更する場合、次の操作が行われます。

1. 管理者(`root`)が`init 5`を入力して、initにランレベルを変更することを伝えます。

2. initはその設定ファイル(`/etc/inittab`)を調べ、新しいランレベルをパラメータとして使用して`/etc/init.d/rc`を起動する必要があるかどうか判断します。

3. ここで`rc`は、現在のランレベルの停止スクリプトであって、新しいランレベルの起動スクリプトがないものだけをすべて呼び出します。この例では、元のランレベルが3なので、`/etc/init.d/rc3.d`の中の`K`で始まるすべてのスクリプトが対象となります。依存性を考慮する必要がありますが、`K`の後の数字によって、一定の起動順序を指定します。

4. 最後に、新しいランレベルの起動スクリプトを起動します。この例では`/etc/init.d/rc5.d`の中の`S`で始まるスクリプトがそれにあたります。順序に関して、それらを起動したときに適用されたのと同じ手順が、ここでも適用されます。

現在のランレベルと同じランレベルに変更する場合、initは`/etc/inittab`の変更部分だけをチェックし、適切な手順を開始します。たとえば、別のインタフェースで`getty`を起動します。

28.2.2 initスクリプト

`/etc/init.d`内に、2種類のスクリプトがあります。

initによって直接実行されるスクリプト
これは、ブートプロセスの実行中、または即座のシステムシャットダウンを行ったとき(電源障害またはユーザがCtrl+Alt+Delを押した場合)にのみ適用されます。こうしたスクリプトの実行は、/etc/inittabで定義されます。

initによって間接的に実行されるスクリプト
これらは、ランレベルの変更時に実行され、関連するスクリプトの正しい順序を保証するマスタスクリプト/etc/init.d/rcを常に呼び出します。

すべてのスクリプトは、/etc/init.dにあります。ランレベルを変更するスクリプトも同じディレクトリにありますが、サブディレクトリの1つからのシンボリックリンク(/etc/init.d/rc0.dから/etc/init.d/rc6.dへ)経由で呼び出されます。これは単にわかりやすくして、複数のランレベルで使用されている場合にスクリプトが重複するのを防ぐためです。すべてのスクリプトは、起動スクリプトとしても停止スクリプトとしても実行できるので、これらのスクリプトはパラメータstartとstopを認識する必要があります。また、これらのスクリプトはrestart、reload、force-reload、およびstatusのオプションも認識します。これらのオプションについては、表28.2.「initスクリプトのオプション」 (page 463)で説明します。initによって直接実行されるスクリプトには、このようなリンクはありません。こうしたスクリプトは、必要なときにランレベルとは無関係に実行されます。

表 28.2　initスクリプトのオプション

オプション	説明
start	サービスを起動します。
stop	サービスを停止します。
restart	サービスが実行中の場合は、停止して再起動します。実行中でない場合は、起動します。
reload	サービスの停止や再起動をせずに、設定を再ロードします。

オプション	説明
force-reload	サービスが設定の再ロードをサポートする場合は、それを実行します。サポートしない場合は、restartが指定された場合と同じ操作を行います。
status	サービスの現在のステータスを表示します。

ランレベル固有のサブディレクトリにあるリンクによって、スクリプトを複数のランレベルに関連付けることができます。パッケージのインストールまたはアンインストール時に、プログラムinsservを使用して(またはこのプログラムを呼び出すスクリプト/usr/lib/lsb/install_initdを使用して)、このようなリンクを追加または削除することができます。 詳細は、insserv(8)のmanページを参照してください。

次に、最初または最後に起動するブートスクリプトおよび停止スクリプトの概略を示すとともに、保守スクリプトについて説明します。

boot

initを直接使用してシステムを起動するときに実行されます。選択したランレベルから独立で、一度だけ実行されます。これによってprocとptsファイルシステムがマウントされ、blogd(ブートログ出力デーモン)が有効化されます。システムがアップデートまたはインストール後初めてブートされる場合、初期システム設定が起動します。

blogdデーモンは、bootおよびrcによって最初に起動されるサービスです。これらのスクリプトによってトリガされたアクション(たとえば、複数のサブスクリプトを実行するなど)が完了すると停止します。blogdは、すべての画面出力をログファイル/var/log/boot.msgに書き込みますが、これは/varが読み書き権を設定してマウントされた場合のみです。そうでない場合は、/varが利用できるようになるまで、blogdがすべての画面データをバッファします。 blogdについての詳細は、blogd(8)のmanページを参照してください。

スクリプトbootはまた、/etc/init.d/boot.dの中のSで始まる名前のスクリプトをすべて起動します。そこで、ファイルシステムがチェックされ、必要に応じてループデバイスが設定されます。加えて、システム時間が設定されます。ファイルシステムの自動チェックや修復中にエラーが発

生した場合、システム管理者はルートパスワードを入力して介入することができます。最後に、スクリプトboot.localが実行されます。

boot.local
ブート時、ランレベルへの移行前に実行する追加のコマンドを入力します。これは、DOSシステムのAUTOEXEC.BATに相当します。

boot.setup
このスクリプトは、シングルユーザモードから他のランレベルへの移行時に実行され、キーボードレイアウトや仮想コンソールの初期化に関する基本的な設定を行います。

halt
このスクリプトは、ランレベル0または6への移行時のみ実行され、haltまたはrebootとして機能します。システムがシャットダウンするかリブートするかは、haltの呼び出され方に依存します。

rc
このスクリプトは、現在のランレベルの適切な停止スクリプトと、新しく選択したランレベルの起動スクリプトを呼び出します。

独自のスクリプトを作成して、先に説明したスキーマに容易に組み込むことができます。カスタムスクリプトの形式、名前付け、および構成方法は、LSBの仕様と、init、init.d、およびinsservのmanページを参照してください。加えて、startprocおよびkillprocのmanページも参照してください。

警告: initスクリプトのエラーはシステムの停止につながる

initスクリプトに問題があると、コンピュータがハングアップします。このようなスクリプトは最大限の注意を払って編集し、可能であれば、マルチユーザ環境で徹底的にテストします。initスクリプトについては、項28.2.1.「ランレベル」 (page 459)の情報が役立ちます。

特定のプログラムまたはサービス用にカスタムのinitスクリプトを作成する場合は、テンプレートとしてファイル/etc/init.d/skeletonを使用します。このファイルのコピーを別名で保存し、関連のプログラムやファイル名、パス、その他の詳細を必要に応じて編集します。また場合によっては、initプロシージャで正しいアクションが実行されるように、独自の改良をスクリプトに加える必要があります。

最初に記載されているINIT INFOブロックはスクリプトの必須部分で、次のように編集する必要があります。例 28.1. 「最低限のINIT INFOブロック」 (page 466)を参照してください。

例 28.1 最低限のINIT INFOブロック

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

INFOブロックの最初の行では、Provides: の後に、このinitスクリプトで制御するプログラムまたはサービスの名前を指定します。 Required-Start: とRequired-Stop: の2行に、サービス自体が起動または停止する前に、それぞれ起動または停止する必要があるすべてのサービスを指定します。この情報は後で、ランレベルディレクトリに表示するスクリプト名に対し、番号を生成するために使用します。 Default-Start: およびDefault-Stop: の後に、サービスが自動的に起動または停止する際のランレベルを指定します。最後に、Description: の下に、対象のサービスについての簡単な説明を記載します。

ランレベルディレクトリ(/etc /init. d /rc?. d /)から /etc /init. d /内の対応するスクリプトへのリンクを作成するには、コマンドinsserv *新しいスクリプト名*を入力します。insservプログラムは、INIT INFOヘッダを評価して、ランレベルディレクトリ(/etc /init. d /rc?. d /)のスクリプトを起動、停止するために必要なリンクを作成します。このプログラムはまた、必要な番号をこれらのリンクの名前に取り込むことによって、ランレベルごとに正しい起動、停止の順序を管理します。グラフィックツールを使用してリンクを作成する場合は、項28.2.3. 「YaSTでのシステムサービス(ランレベル)の設定」 (page 467)の説明に従って、YaSTのランレベルエディタを使用します。

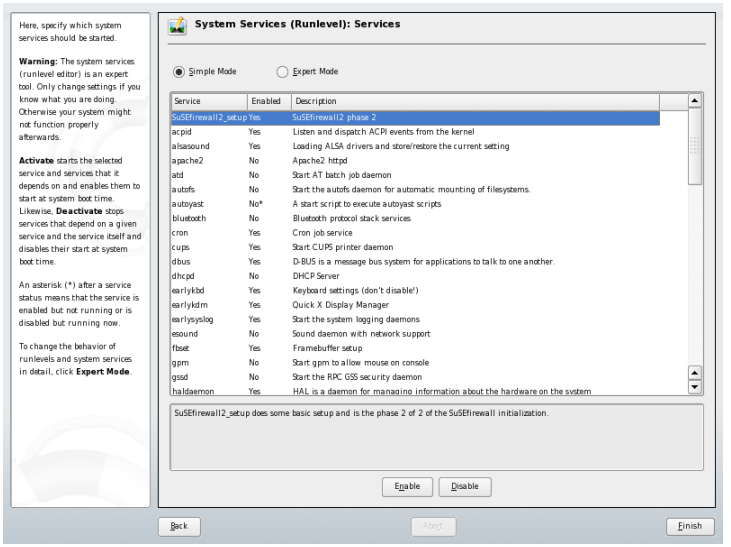
/etc /init. d /にすでに存在するスクリプトを既存のランレベルスキーマに統合する場合は、まずinsservを使用するか、YaSTのランレベルエディタで対応するサービスを有効にすることにより、ランレベルディレクトリにリンクを作成します。 変更内容は、次回のブート時に適用され、新しいサービスが自動的に起動します。

作成したリンクは手動で設定しないでください。INFOブロック内に誤りがある場合は、後で他のサービスに対してinsservを実行すると問題が生じます。

28.2.3 YaSTでのシステムサービス(ランレベル)の設定

*[YaST] → [システム] → [ランレベル・エディター]*の順に選択すると、利用可能なすべてのサービスの概要と、各サービスの現在のステータス(有効か無効か)が表示されます。モジュールを［*単純モード*］と［エキスパートモード］のどちらで使用するかを決定します。ほとんどの場合、デフォルトの［*単純モード*］で十分です。左の列にはサービスの名前が、中央の列にはその現在のステータスが、右の列には簡単な説明が表示されます。ウィンドウの下部には、選択したサービスについての詳細な説明が表示されます。サービスを有効にするには、表でそれを選択し、［*有効にする*］を選択します。同じ手順で、サービスを無効にできます。

図 28.1 *ランレベル・エディター*



サービスの起動または停止時のランレベルを詳細に制御する場合、またはデフォルトのランレベルを変更する場合は、まず［エキスパートモード］を選択します。 上部には、現在のデフォルトのランレベル、つまり「initdefault」

(システムのブート時にデフォルトで入るランレベル)が表示されます。通常、SUSE Linuxシステムのデフォルトのランレベルは5 (ネットワークありフルマルチユーザモードおよびX)です。適切な代替の設定は、ランレベル3 (ネットワークありフルマルチユーザモード)です。

YaSTのダイアログボックスでは、ランレベルのいずれか1つを新しいデフォルトとして選択できます(表 28.1.「ランレベルの種類」 (page 460)を参照)。また、このウィンドウのテーブルを使用して、個々のサービスやデーモンを有効、無効にできます。テーブルには、利用可能なサービスとデーモンが一覧表示され、現在システム上で有効かどうかと、有効な場合はそのランレベルが表示されます。マウスで行を選択し、ランレベルを表すチェックボックス([*B*] 、 [*0*] 、 [*1*] 、 [*2*] 、 [*3*] 、 [*5*] 、 [*6*] 、 [*S*])をクリックして、選択しているサービスまたはデーモンが実行されるランレベルを定義します。ランレベル4は、カスタムランレベルを作成できるように、初期設定は未定義です。最後に現在選択しているサービスまたはデーモンの簡単な説明が、テーブルの概要の下に表示されます。

[*スタート／中止／更新*] をクリックして、サービスを有効化するかどうかを決定します。現在の状態が自動的に確認されなかった場合は、 [*状態を更新*] を使用して確認することができます。 [*設定／リセット*] をクリックすると、変更をシステムに適用するか、ランレベルエディタの起動前に存在していた設定を復元するかを選択できます。 [*完了*] を選択すると、設定の変更がディスクに保存されます。

警告: ランレベルの設定を誤るとシステムに害が及ぶことがある

ランレベルの設定が誤っていると、システムが使用できなくなることがあります。変更を実際に適用する前に、どういう結果が出るかをよく確認してください。

28.3 /etc/sysconfigによるシステム設定

SUSE Linuxの主な設定は、 `/etc/sysconfig`ディレクトリに格納されている設定ファイルで指定できます。 `/etc/sysconfig`ディレクトリの個々のファイルは、それらが関係するスクリプトによってのみ読み込まれます。これにより、たとえば、ネットワークはネットワーク関連のスクリプトでのみ解析

されるようになります。 /etc/sysconfigディレクトリ内の設定に従って生成される他の多くのシステム設定ファイルも存在します。この作業は、SuSEconfigによって実行されます。たとえば、ネットワーク設定を変更すると、ネットワーク設定に関連するファイルの1つである /etc/host.conf も、SuSEconfigによって変更されます。この概念により、ユーザはシステムを再起動せずに基本的な設定を変更できます。

システム設定を編集するには、2通りの方法があります。 YaSTのsysconfigエディターを使う方法と、設定ファイルを手動で編集する方法です。

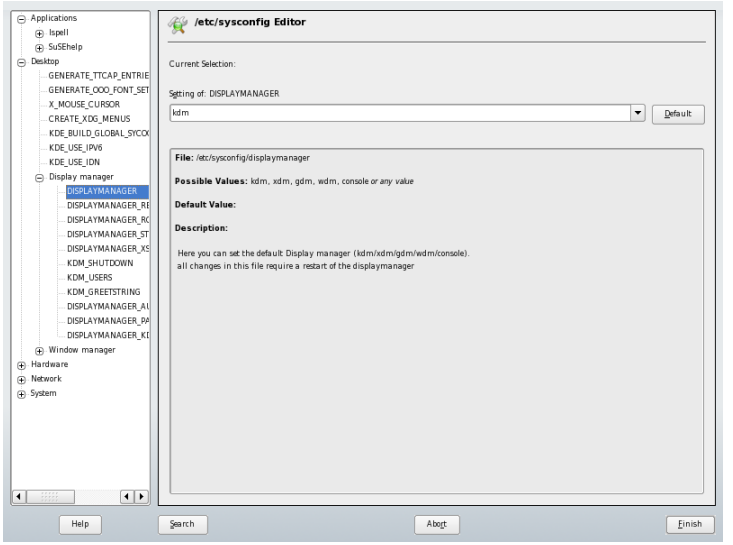
28.3.1 YaSTのsysconfigエディターを使ってシステム設定を変更する

YaSTのsysconfigエディターは、使いやすいシステム設定のフロントエンドです。 変更する必要のある設定用変数の実際の場所が分からなくても、このモジュールに内蔵された検索機能を使うだけで、必要に応じて設定用変数の値を変更できますし、これらの変更の適用、sysconfigで設定されている値に基づく設定の更新、サービスのリスタートは、YaSTが行います。

警告: /etc/sysconfig/*ファイルの変更はインストールに害を及ぼすことがある

知識や経験が豊富でない限り、 /etc/sysconfigファイルは変更しないでください。場合によっては、システムに相当なダメージを与えることがあります。 /etc/sysconfigのファイルには、各変数が持つ実際の効果を説明する簡単なコメントが付いています。

図 28.2　sysconfigエディタを使用したシステム設定



YaSTのsysconfigダイアログは、3つの部分に分かれています。ダイアログの左側には、すべての設定変数がツリー表示されます。変数を選択した段階で、右側に現在選択されている変数と、この変数の現在の設定が表示されます。その下の3番目のウィンドウには、変数の目的、有効な値、デフォルト値、およびこの変数が設定されている実際の設定ファイルについての簡単な説明が表示されます。このダイアログボックスには、変数の変更後に実行された設定スクリプトや、変更の結果起動された新しいサービスについての情報も表示されます。YaSTにより変更の確認が求められ、［完了］を選択してダイアログを終了した後にどのスクリプトが実行されるかが通知されます。現在は実行しないサービスやスクリプトを選択すると、それらが後で実行されます。YaSTはすべての変更を自動的に適用し、変更と関係のあるすべてのサービスをリスタートします。

28.3.2　システム設定を手動で変更する

システム設定を手動で変更するには、以下の手順に従います。

1 `root`になります。

2 init 1コマンドで、システムをシングルユーザモード(ランレベル1)にします。

3 必要に応じて、設定ファイルを、自分が使っているエディタで変更します。

/etc/sysconfigの設定ファイルの変更にYaSTを使用しない場合、空の変数値は2つの引用符(KEYTABLE="")によって表し、空白を含む値は引用符で囲むことに注意してください。語の値は、引用符で囲む必要はありません。

4 SuSEconfigを実行して、変更が有効になっていることを確認します。

5 init *default_runlevel*のようなコマンドで、システムを以前のランレベルに戻します。*default_runlevel*の部分は、システムのデフォルトのランレベルで置き換えてください。ネットワークとXのあるフルマルチユーザモードに戻るには5を、ネットワークのあるフルマルチユーザモードに戻るには3を選択します。

この手順は主に、ネットワーク設定など、システム全体の設定を変更する場合に必要です。小さな変更であれば、シングルユーザモードに移行する必要はありませんが、関与するすべてのプログラムが正しく再起動することを絶対的に保証する必要がある場合は、移行しても差し支えありません。

ティップ: 自動システム設定機能の設定

SuSEconfigの自動システム設定機能を無効にするには、/etc/sysconfig/suseconfigのENABLE_SUSECONFIGをnoに設定します。SUSEのインストールサポートを使用する場合は、SuSEconfigを無効にしないでください。無効にすると、自動設定も部分的に無効になる可能性があります。

---

29 ブートローダ

この章では、SUSE Linuxで現在使用されているブートローダであるGRUBの設定方法について説明します。すべての設定操作には、特殊なYaSTモジュールを使用できます。Linuxでのブートに不慣れな場合は、以降の各セクションを読んで背景情報を理解してください。また、この章では、でのブート時に頻繁に発生する問題とその解決策についても説明します。

この章は、ブート管理とGRUBブートローダの設定に重点を置いています。ブート手順は、総じて章 28. *Linuxシステムのブートと設定* (page 455)で説明しています。ブートローダは、マシン(BIOS)とオペレーティングシステム(SUSE Linux)の間のインタフェースになります。ブートローダの設定は、オペレーティングシステムの起動に直接影響を及ぼします。

次の用語は、この章で頻繁に使用されており、少し説明を加えた方がよいと思われるものです。

マスタブートレコード

MBRの構造は、オペレーティングシステムに依存しない規則に従って定義されます。最初の446バイトは、プログラムコード用に予約されています。通常、この領域にはブートローダプログラム(この場合はGRUB)が保持されます。次の64バイトは、最大4つのエントリからなるパーティションテーブル用のスペースです(パーティションのタイプ項(章 1. *YaSTによるインストール*, ↑起動)を参照)。パーティションテーブルには、ハードディスクのパーティション分割とファイルシステムのタイプに関する情報が含まれています。オペレーティングシステムでハードディスクを処理するには、このテーブルが必要です。MBRの最後の2バイトは、静的な「マジックナン

バー」(AA55)を含む必要があります。異なる値を含むMBRは、BIOSおよびすべてのPCのオペレーティングシステムにより無効と見なされます。

ブートセクタ

ブートセクタは、拡張パーティションを除くハードディスクパーティションの最初のセクタであり、その他のパーティションの「「コンテナ」」として機能するだけです。これらのブートセクタのうち512バイトのスペースは、関連パーティションにインストールされているオペレーティングシステムをブートするためのコードが占有します。これは、フォーマット済みのDOS、Windows、およびOS/2パーティションのブートセクタに該当し、ファイルシステムの重要な基本データも一部含まれています。これに対して、Linuxパーティションのブートセクタは、ファイルシステムの設定直後は空になっています。そのため、Linuxパーティションは、カーネルと有効なルートファイルシステムが含まれている場合にも、*単独ではブートできません*。システムブート用の有効なコードを含むブートセクタの場合、最後の2バイトにはMBRと同じマジックナンバー(`AA55`)があります。

29.1 ブート管理

最も単純なケース、つまりコンピュータにオペレーティングシステムが1つしかインストールされていない場合には、ブート管理はこれまでに説明したように行われます。コンピュータに複数のオペレーティングシステムがインストールされている場合は、次の選択肢があります。

2番目以降のシステムを外部メディアからブートする

オペレーティングシステムのいずれかをハードディスクからブートします。他のオペレーティングシステムは、外部メディア(フロッピーディスク、CD、USBストレージメディア)にインストールされているブートマネージャを使用してブートします。

ブートマネージャをMBRにインストールする

ブートマネージャを使用すると、1台のコンピュータに同時に複数のシステムをインストールし、それらを切り替えて使用できます。 ユーザは、ブートプロセス中にブートするシステムを選択できます。別のシステムに切り替えるには、コンピュータを再起動する必要があります。この操作が可能なのは、選択したブートマネージャにインストール済みオペレーティ

ングシステムとの互換性がある場合だけです。 SUSE LinuxではGRUBがブートマネージャとして使用されています。

29.2 ブートローダの選択

SUSE Linuxでは、デフォルトでGRUBブートローダが使用されます。 ただし、特殊なハードウェアやソフトウェアなど、状況によっては、LILOの方が適している場合があります。 LILOを使用していた古いバージョンのSUSE Linuxをアップデートすると、LILOがインストールされます。

LILOのインストールと設定についての詳細は、サポートデータベースのキーワードLILOの下、または /usr /share /doc /packages /lilo を参照してください。

29.3 GRUBによるブート

GRUB (Grand Unified Bootloader)は、2つのステージで構成されています。 stage1は512バイトから成り、MBR、またはハードディスクパーティションやフロッピーディスクのブートセクタに書き込まれます。その後、stage2が読み込まれます。このステージには、実際のプログラムコードが含まれています。最初のステージのタスクは、ブートローダの第2ステージを読み込むことだけです。

stage2には、ファイルシステムにアクセスする機能があります。現在、Windowsで使用されているExt2、Ext3、ReiserFS、Minix、およびDOS FATファイルシステムがサポートされます。BSDシステムで使用されているJFS、XFS、UFS、およびFFSも、特定の範囲までサポートされます。バージョン0.95以降のGRUBには、「El Torito」仕様に準拠するISO 9660標準ファイルシステムを含むCDまたはDVDからブートする機能も用意されています。システムをブートする前にも、はサポートされているBIOSディスクデバイス(BIOSにより検出されるフロッピーディスクまたはハードディスク、CDドライブ、およびDVDドライブ)のファイルシステムにアクセスできます。 したがって、GRUBの設定ファイル(menu. lst)を変更しても、ブートマネージャを再インストールする必要はありません。システムをブートすると、GRUBはメニューファイルと共にカーネルまたは初期RAMディスク(initrd)の有効なパスとパーティションデータを再読み込みし、これらのファイルを検索します。

GRUBの実際の設定は、以下の3つのファイルに基づきます。

/boot/grub/menu.lst

このファイルには、でブートできるパーティションまたはオペレーティングシステムに関する情報がすべて含まれています。この情報がなければ、システム制御をオペレーティングシステムに渡すことができません。

/boot/grub/device.map

このファイルは、デバイス名をGRUBとBIOSの表記法からLinuxデバイス名に変換するために使います。

/etc/grub.conf

このファイルには、シェルでブートローダを正常にインストールするために必要なパラメータとオプションが含まれています。

GRUBは、さまざまな方法で制御できます。グラフィカルメニュー(スプラッシュ画面)を使用して、既存の設定からブートエントリを選択できます。設定は、ファイル`menu.lst`から読み込まれます。

GRUBでは、すべてのブートパラメータをブート前に変更できます。たとえば、メニューファイルを間違って編集した場合は、この方法で訂正できます。また、一種の入力プロンプトからブートコマンドを対話形式で入力することもできます(ブート手順実行中のメニューエントリの編集項(page 481)を参照)。GRUBには、ブート前にカーネルと`initrd`の位置を判別する機能が用意されています。この機能を使用すると、ブートローダ設定にエントリが存在しないインストール済みオペレーティングシステムでもブートできます。

*GRUBシェル*は、インストール済みシステムのGRUBをエミュレートします。このシェルを使用すると、GRUBをインストールしたり、適用前に新規設定をテストできます。項29.3.4.「GRUBシェル」 (page 484)を参照してください。

29.3.1 GRUBのブートメニュー

ブートメニューを含むグラフィカルスプラッシュ画面は、GRUBの設定ファイル`/boot/grub/menu.lst`に基づいており、このファイルにはメニューを使

用してブートできるパーティションまたはオペレーティングシステムに関する情報がすべて含まれています。

システムをブートするたびに、はファイルシステムからメニューファイルを読み込みます。このため、ファイルを変更するたびにを再インストールする必要がありません。項29.4.「YaSTによるブートローダの設定」 (page 486)で説明しているように、YaSTのブートローダを使用してGRUBの設定を変更します。

メニューファイルにはコマンドが含まれています。構文はきわめて単純です。各行には、コマンド1つとオプションのパラメータがシェルと同様にスペースで区切って指定されています。これまでの経緯が理由で、一部のコマンドでは最初の引数の前に等号(=)を使用することができます。コメントを記述するには、行頭にシャープ記号(#)を入力します。

メニュー概要の中にあるメニュー項目を識別できるように、各エントリに対してtitle (タイトル)を指定します。キーワードtitleの後に続くテキスト(半角スペースも使用できます)は、メニューの中で、選択可能なオプションとして表示されます。そのメニュー項目が表示された場合、次のtitleまでに記述されているすべてのコマンドが実行されます。

最も簡単な例は、他のオペレーティングシステムのブートローダにリダイレクトすることです。該当するコマンドはchainloaderであり、引数は通常、他のパーティション内にあるブートブロックをGRUBのブロック表記に従って記述したものです。次に例を示します。

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

GRUBでのデバイス名については、ハードディスクとパーティションに関する命名規則項 (page 478)を参照してください。先ほどの例では、1台目のハードディスクの4番目のパーティションの最初のブロックを指定しています。

カーネルイメージを指定するには、kernelコマンドを使用します。最初の引数は、パーティションにあるカーネルイメージを表すパスです。他の引数は、コマンドラインでカーネルに渡されます。

ルートパーティションへのアクセスに必要なビルトインドライバがカーネルに用意されていない場合は、initrdファイルへのパスを示す引数だけを指定して、別のGRUBコマンドでinitrdを指定する必要があります。initrdの読み込みアドレスは、読み込まれるカーネルイメージに書き込まれているので、initrdコマンドは、kernelコマンドの直後に記述する必要があります。

rootコマンドは、kernelとinitrdの各ファイルの指定を簡略化します。rootの唯一の引数は、GRUBデバイス、またはGRUBデバイス上のパーティションです。このデバイスは、すべてのカーネル、initrd、または次のrootコマンドまでデバイスが明示的に指定されていない他のファイルのパスに使用されます。インストール時に生成されるmenu.lstファイル内では、このコマンドは使用されていません。単純に手動で編集する際に使用するものです。

bootコマンドは各メニューエントリの最後に必ず含まれています。そのため、メニューファイルにこのコマンドを記述する必要はありません。ただし、GRUBをブート時に対話形式で使用する場合は、bootコマンドを最後に入力する必要があります。このコマンド自体は、引数を使用しません。単純に、読み込み済みのカーネルイメージ、または指定のチェーンローダをブートします。

すべてのメニューエントリを記述した後、その1つをdefaultエントリとして定義します。デフォルトエントリを指定しなかった場合、最初のエントリ(エントリ0)が使用されます。 デフォルトエントリがブートされるまでのタイムアウトを秒単位で指定することもできます。通常、timeoutおよびdefaultは、メニューエントリより先に記述します。サンプルファイルについては、メニューファイルの例項 (page 479)を参照してください。

ハードディスクとパーティションに関する命名規則

でのハードディスクとパーティションの命名規則は、通常のLinuxデバイスの命名規則と異なっています。GRUBでは、パーティション番号は0から始まります。そのため、(hd0,0)は最初のハードディスクの最初のパーティションとなります。ハードディスクがプライマリマスタとして接続されている一般的なデスクトップマシンでは、対応するLinuxデバイス名は/dev/hda1になります。

可能な4つの基本パーティションに、パーティション番号0～3が割り当てられます。論理パーティション番号は4から始まります。

```
(hd0,0)    最初のハードディスクの最初の基本パーティショ
(hd0,1)    2番目の基本パーティショ
(hd0,2)    3番目の基本パーティショ
(hd0,3)    4番目の基本パーティション(通常は拡張パーティション)
(hd0,4)    最初の論理パーティショ
(hd0,5)    2番目の論理パーティション
```

GRUBは、IDE、SCSI、RAIDの各デバイスを区別しません。BIOSまたは他のディスクコントローラで認識されるすべてのハードディスクには、BIOSの中で事前に設定されたブートシーケンスに従って番号が割り当てられます。

には、Linuxデバイス名をBIOSデバイス名に正確にマップする機能がありません。このマッピングはアルゴリズムを使用して生成され、device.mapファイルに保存されるため、必要に応じて編集できます。ファイルdevice.mapについては、項29.3.2.「device.mapファイル」 (page 483)を参照してください。

のフルパスは、カッコ内のデバイス名と、指定のパーティションにあるファイルシステム内のファイルへのパスで構成されます。このパスはスラッシュで始まります。たとえば、単一IDEハードディスクの最初のパーティションにLinuxを含んでいるシステムでは、ブート可能カーネルを次のように指定できます。

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

メニューファイルの例

次の例は、GRUBのメニューファイルの構造を示しています。このインストール例では、Linuxのブートパーティションが/dev/hda5、ルートパーティションが/dev/hda7、およびWindowsのインストールファイルが/dev/hda1にあります。

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
 kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
 initrd (hd0,4)/initrd

title windows
 chainloader(hd0,0)+1

title floppy
 chainloader(fd0)+1

title failsafe
 kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
 apm=off acpi=off vga=normal nosmp maxcpus=0 3
 initrd (hd0,4)/initrd.shipped
```

最初のブロックは、スプラッシュ画面の設定を定義します。

gfxmenu (hd0,4)/message
背景画像messageは、/dev/hda5にあります。

color white/blue black/light-gray
配色は、白(前景色)、青(背景色)、黒(選択項目)、明るい灰色(選択項目の背景色)です。配色はスプラッシュ画面には影響しません。影響を受けるのは、Escキーを押してスプラッシュ画面を終了するとアクセスできるカスタマイズ可能なGRUBメニューだけです。

default 0
最初のメニューエントリtitle linuxは、デフォルトでのブート対象です。

timeout 8
ユーザ入力がないまま8秒が経過した場合、GRUBは自動的にデフォルトエントリをブートします。 自動ブートを無効にするには、timeoutの行を削除します。 timeout 0と設定すると、GRUBは待ち時間なしでデフォルトのエントリをブートします。

2番目の(最大)ブロックは、ブート可能な各種オペレーティングシステムを示します。個々のオペレーティングシステムに関するセクションはtitleで始まります。

- 最初のエントリ(title linux)は、SUSE Linuxをブートする役割を果たします。カーネル(vmlinuz)は、1台目のハードディスクの最初の論理パーティション(ブートパーティション)内に配置されています。ルートパーティションやVGAモードなどのカーネルパーティションは、ここに追加されます。ルートパーティションは、Linuxの命名規則に従って指定されたものです(/dev/hda7)。この情報を読み込むのはLinuxカーネルであり、GRUBは関係しないからです。initrdも、1台目のハードディスクの最初の論理パーティション内に配置されています。

- 第2のエントリは、Windowsを読み込む役割を果たします。Windowsは、1台目のハードディスク(hd0,0)の最初のパーティションからブートされます。chainloader +1コマンドは、指定されたパーティションの最初のセクタを読み取って実行するようGRUBに指示します。

- 次のエントリは、BIOS設定を変更することなく、フロッピーディスクからブートすることを可能にします。

- ブートオプションfailsafeは、問題のあるシステム上でもLinuxのブートを可能にするカーネルパラメータを選択してLinuxを起動します。

メニューファイルは必要に応じて変更できます。その場合、GRUBは変更後の設定を次回のブート時に使用します。このファイルを永続的に編集するには、YaSTまたは好みのエディタを使用します。また、対話形式で一時的に変更するには、GRUBの編集機能を使用します。ブート手順実行中のメニューエントリの編集項 (page 481)を参照してください。

ブート手順実行中のメニューエントリの編集

のグラフィカルブートメニューでは、ブートするオペレーティングシステムを矢印キーで選択します。Linuxシステムを選択した場合は、ブートプロンプトからブートパラメータを追加入力できます。個々のメニューエントリを直接編集するには、Escキーを押してスプラッシュ画面を終了してからEキーを押します。この方法で加えた変更は、現在のブート手順だけに適用され、永続的に採用されることはありません。

重要項目: ブート手順実行中のキーボードレイアウト

ブート時は、USキーボードレイアウトだけが使用可能です。

編集モードを有効にした後、矢印キーを使用して、設定を編集するメニューエントリを選択します。設定を編集可能にするには、もう一度Eキーを押します。このようにして、不正なパーティションまたはパス指定を、ブートプロセスに悪影響を及ぼす前に編集します。Enterキーを押して編集モードを終了し、メニューに戻ります。次に、Bキーを押してこのエントリをブートします。下部のヘルプテキストに、さらに可能なアクションが表示されます。

変更後のブートオプションを永続的に入力してカーネルに渡すには、ユーザrootでファイルmenu.lstを開き、関連カーネルパラメータをスペースで区切って既存の行に追加します。

```
title linux
   kernel (hd0,0)/vmlinuz root=/dev/hda3 additional parameter
   initrd (hd0,0)/initrd
```

GRUBは、次回のシステムブート時に新規パラメータを自動的に使用します。または、この変更をYaSTのブートローダモジュールで行うこともできます。新規パラメータをスペースで区切って既存の行に追加します。

ワイルドカードを使用したブートカーネルの選択

特にカスタムカーネルを開発または使用する場合は、menu.lst内のエントリを変更するか、またはコマンドラインを編集して現在のカーネルとinitrdのファイル名を反映する必要があります。この手順を単純化するには、GRUBのカーネルリストを動的に更新するために*ワイルドカード*を使用します。その結果、特定のパターンと一致するすべてのカーネルイメージが、ブート可能なイメージのリストに自動的に追加されます。この機能についてはサポートがないので注意してください。

ワイルドカードオプションを有効にするには、menu.lstにさらにメニューエントリを入力します。実用になるように、すべてのカーネルイメージとinitrdイメージには、カーネルをその関連するinitrdに対応させる共通の基本名と識別子が必要です。次のセットアップを考えてみます。

```
initrd-default
initrd-test
vmlinuz-default
vmlinuz-test
```

この場合には、1つのGRUB設定で両方のブートイメージを追加できます。メニューエントリlinux-defaultとlinux-testを取得するには、menu.lstに次のエントリが必要です。

```
title linux-*
   wildcard (hd0,4)/vmlinuz-*
   kernel (hd0,4)/vmlinuz-* root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-*
```

この例では、はワイルドカードに対応するエントリのパーティション(hd0,4)を検索します。 こうしたエントリを使用してGRUBメニューの新しいエントリが生成されます。 先ほどの例では、GRUBは、次のエントリがmenu.lstにあるかのように動作します。

```
title linux-default
   wildcard (hd0,4)/vmlinuz-default
   kernel (hd0,4)/vmlinuz-default root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-default
title linux-test
   wildcard (hd0,4)/vmlinuz-test
   kernel (hd0,4)/vmlinuz-test root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-test
```

このような設定で、ファイル名が一貫して使用されていない場合や、展開されたファイルのいずれか(initrdイメージなど)が失われている場合には、問題が発生するおそれがあります。

29.3.2 device.mapファイル

device.mapファイルは、GRUBのデバイス名をLinuxのデバイス名にマップします。 IDEとSCSIの各ハードディスクが混在するシステムでは、GRUBは特殊プロシージャを使用してブートシーケンスの判定を試みる必要があります。これは、GRUBはBIOSのブートシーケンス情報にアクセスできないからです。GRUBはこの分析の結果をファイル/boot/grub/device.mapに保存します。BIOS内でブートシーケンスがIDE、SCSIの順に設定されているシステムの場合、ファイルdevice.mapは次のようになります。

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

IDE、SCSI、および他のハードディスクのシーケンス(順序)は、さまざまな要因によって異なり、Linuxではマッピングを識別できないため、device.mapファイル内のシーケンスは手動で設定できます。ブート時に問題に直面した場合は、このファイル内のシーケンスがBIOS内のシーケンスに対応しているかどうかをチェックします。さらに、必要に応じてGRUBシェルを使用し、ファイル内のシーケンスを一時的に変更します(項29.3.4. 「GRUBシェル」(page 484)を参照)。 Linuxシステムのブート後に、YaSTブートローダモジュールまたは好みのエディタを使用して、device.mapファイルを永続的に変更できます。

device.mapを手動で編集した後、次のコマンドを実行してGRUBを再インストールします。このコマンドにより、device.mapファイルが再読み込みされ、grub.confに指定されているコマンドが実行されます。

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

29.3.3 /etc/grub.confファイル

menu.lstおよびdevice.mapのほかに重要な第3のGRUB設定ファイルは、 /etc/grub.confです。このファイルには、grubコマンドでブートロー

ダを正常にインストールするために必要なパラメータとオプションが含まれています。

```
root (hd0,4)
   install /grub/stage1 d (hd0) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
   quit
```

各エントリの意味:

root (hd0,4)
このコマンドは、に対して後続のコマンドを1台目のハードディスクの最初の論理パーティション(ブートファイルの位置)に適用するように指示します。

installパラメータ
grubコマンドは、installパラメータを指定して実行する必要があります。 ブートローダのstage1は、1台目のハードディスクのMBR内にインストールする必要があります(/grub/stage1 d (hd0))。 stage2は、メモリアドレス0x8000に読み込む必要があります(/grub/stage2 0x8000)。最後のエントリ((hd0,4)/grub/menu.lst)は、メニューファイルを探す場所をGRUBに伝えます。

29.3.4 GRUBシェル

GRUBは実際には2つのバージョンがあります。ブートローダと、/usr/sbin/grubにある通常のLinuxプログラムです。 このプログラムを*GRUBシェル*と呼びます。 ハードディスクやフロッピーディスクにGRUBをブートローダとしてインストールする機能は、installコマンドとsetupコマンドの形でGRUBに組み込まれています。 この機能は、Linuxの読み込み時にGRUBシェル内で使用できます。

ただし、setupコマンドとinstallコマンドは、Linux起動前のブート手順でも使用できます。これにより、障害が発生してブートできなくなったシステムを容易に修復できます。これは、ブートローダの設定ファイルの誤りをパラメータの手動入力により回避できるからです。ブート手順の中でパラメータを手動で入力する方法は、ネイティブシステムを損傷せずに新規設定をテストする際にも役立ちます。単に、menu.lstの場合と同様の構文を使用して、実験的な設定ファイルを入力します。次に、既存の設定ファイルは変更せずに、このエントリの機能をテストします。たとえば、新規カーネルをテ

ストするには、kernelコマンドと新規カーネルへのパスを入力します。ブートプロシージャが失敗した場合、次回のブート時にはオリジナルのmenu.lstを引き続き使用できます。同様に、訂正後のパラメータを入力することで、menu.lstファイルの誤りに関係なくコマンドラインインタフェースを使用してシステムをブートすることもできます。稼働中のシステムでは、menu.lstに正しいパラメータを入力して、システムを永続的にブート可能にすることができます。

GRUBデバイスからLinuxデバイスへのマッピングが関係するのは、GRUBシェルを(項29.3.2.「device.mapファイル」 (page 483)の説明に従ってgrubを入力して) Linuxプログラムとして実行する場合だけです。この目的で、このプログラムはdevice.mapファイルを読み取ります。詳細については、項29.3.2.「device.mapファイル」 (page 483)を参照してください。

29.3.5 ブートパスワードの設定

オペレーティングシステムのブート前でも、GRUBはファイルシステムへのアクセスを可能にします。rootパーミッションを持たないユーザは、システムのブート後、アクセス権のないLinuxシステム上のファイルにアクセスできます。この種のアクセスを阻止したり、ユーザによる特定のオペレーティングシステムのブートを防止するために、ブートパスワードを設定できます。

重要項目: ブートパスワードとスプラッシュ画面

にブートパスワードを使用する場合、通常のスプラッシュ画面は表示されません。

ユーザrootとして、次の手順に従ってブートパスワードを設定します。

1. rootプロンプトで、grubと入力します。
2. GRUBシェル内でパスワードを暗号化します。

```
grub> md5crypt
Password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

3. 暗号化後の文字列を、menu.lstファイルのグローバルセクションに貼り付けます。

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

これで、ブートプロンプトからGRUBコマンドを実行するには、先にPキーを押してパスワードを入力する操作が必要になります。しかし、ユーザはブートメニューから引き続き任意のオペレーティングシステムをブートすることができます。

4 ブートメニューから1つまたは複数のオペレーティングシステムをブートする操作を禁止するには、`menu.lst`内で、パスワードを入力しなければブートできないようにする必要のある各セクションにエントリ`lock`を追加します。次に例を示します。

```
title linux
kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
initrd (hd0,4)/initrd
lock
```

システムをリブートしてブートメニューからLinuxエントリを選択すると、次のエラーメッセージが表示されます。

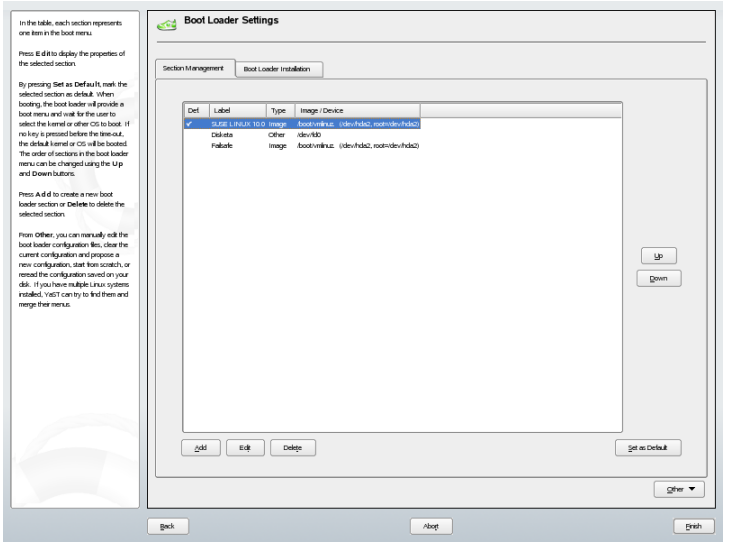
```
Error 32: Must be authenticated
```

Enterキーを押してメニューを表示します。次に、Pキーを押してパスワードプロンプトを表示します。パスワードを入力してEnterキーを押すと、選択したオペレーティングシステム(この場合はLinux)がブートします。

29.4 YaSTによるブートローダの設定

SUSE Linuxシステムでブートローダを設定する最も簡単な方法は、YaSTのモジュールを使用することです。YaSTコントロールセンターで、*[システム]* → *[ブート・ローダーの設定]*の順に選択します。システムの現在のブートローダ設定が表示され、必要な変更が可能になります。図 29.1. 「YaSTによるブートローダの設定」 (page 487)を参照してください。

図 29.1　YaSTによるブートローダの設定



メインウィンドウは、以下の2つのタブで構成されています。

Section Management (セクション管理)
　このタブでは、各オペレーティングシステムのブートローダセクションの編集、変更、削除が行えます。オプションを追加するには、［*追加*］をクリックします。既存のオプションの値を変更するには、マウスで選択してから［*Edit*］をクリックします。既存のオプションをまったく使用しない場合は、選択して［*Delete*］をクリックします。ブートローダのオプションがよく分からない場合には、まず項29.3.「GRUBによるブート」 (page 475)を読んでください。

Boot Loader Installation (ブートローダのインストール)
　このタブでは、タイプや場所に関連した設定、またはブートローダの他の設定を表示し、変更することができます。

29.4.1　ブートローダのタイプ

ブートローダのタイプは、［*Boot Loader Installation*］タブで設定します。SUSE Linuxのデフォルトのブートローダは GRUBです。 LILOを使用するには、以下の手順に従います。

手順 29.2　ブートローダのタイプの変更

1 ［*Boot Loader Installation*］タブを開きます。

2 ［*Type*］パネルで、［*Boot Loader*］メニューをクリックして［*LILO*］を選択します。

3 ポップアップメニューから、以下の動作のいずれかを選択します。

新しい設定を提案する
YaSTは新しい設定を提案します。

Convert Current Configuration (現在の設定を変換する)
YaSTは現在の設定を変換します。 設定を変換すると、いくつかの設定内容が失われることがあります。

Start New Configuration from Scratch (新しい設定を新規に作成する)
カスタムの設定を作成するには、このオプションを選択します。 この動作は、SUSE Linuxのインストール時には利用できません。

Read Configuration Saved on Disk (ディスクに保存されている設定を読み込む)
このオプションは、自分独自の `/etc/lilo.conf` をロードする場合に使います。 この動作は、SUSE Linuxのインストール時には利用できません。

4 ［*OK*］をクリックして、変更内容を保存します。

5 メインのダイアログウィンドウで［*Finish*］をクリックして、変更を有効にします。

変換後に、古いGRUB設定はディスクに保存されます。 これを使うには、ブートローダのタイプをGRUBに戻し、ポップアップメニューから［*Restore Configuration Saved before Conversion*］を選択してください。 この操作は、インストール済みのシステムでのみ実行可能です。

注意: カスタムのブートローダ

GRUBやLILO以外のブートローダを使用する場合には、［*Do Not Install Any Boot Loader*］を選択します。 このオプションを選択する場合には、前もって、ブートローダのドキュメントを注意深く読んでください。

29.4.2 ブートローダの場所

ブートローダの場所を変更することが必要になる場合もあります。 このYaSTモジュールはこの点で助けになります。

手順 29.3 ブートローダの場所の変更

1 ブートローダの場所を変更するには、［*Boot Loader Installation*］タブをクリックし、［*Boot Loader Location*］メニューから以下のオプションのいずれかを選択します。

Master Boot Record of /dev/hdX
ディスクのマスタブートです。 これは、システムがこの方法でブートできるとSUSEが判定した場合にはいつでも勧められています。 Xはハードディスクの識別記号で、a、b、c、dのいずれかになります。

```
hda => ide0 master
     hdb => ide0 slave
     hdc => ide1 master
     hdd => ide1 slave
```

Boot Sector of Boot Partition /dev/hdXY
/bootパーティションのブートセクタです。このオプションは、ハードディスクに複数のオペレーティングシステムをインストールしている場合のデフォルトです。 Y はパーティションの番号で、1、2、3、4、5などになります。 それで、エントリは、次のようになります。

```
/dev/hda1
```

Boot Sector of Root Partition /dev/hdXY
/(ルート)パーティションのブートセクタです。 このオプションも、ハードディスクに複数のオペレーティングシステムをインストールしていて、古いブートマネージャを使用し続けたい場合に用いられます。

Other
このオプションを選択すれば、ブートローダの場所を指定できます。

2 ［*Finish*］をクリックして、変更を有効にします。

29.4.3 標準のシステム

標準のシステムを手動で変更するには、以下の手順に従います。

手順 29.4 標準のシステムの設定

1 ［*Section Management*］タブを開きます。

2 マウスで希望するシステムをリストから選択するか、［*up*］または［*down*］をクリックします。

3 ［*Set as Default*］をクリックします。

4 ［*Finish*］をクリックして、変更を有効にします。

29.4.4 ブートローダのタイムアウト

ブートローダは、標準のシステムを直ちにブートするわけではありません。このタイムアウト時間中に、標準のシステムのブートを中止して、ブートするシステムを変更したり、何らかのカーネルパラメータを書き込んだりすることができます。 ブートローダのタイムアウトを変更するには、以下の手順に従います。

手順 29.5 ブートローダのタイムアウトを変更する

1 ［*Boot Loader Installation*］タブを開きます。

2 ［*Boot Loader Options*］をクリックします。

3 ［*Show Boot Menu*］をオンにします。

4 ［*Boot Menu*］で、新しい値を入力するか、マウスで矢印キーをクリックするか、またはキーボードの矢印キーを使って、［*Boot Menu Time-Out*］の値を変更します。

5 [*OK*]をクリックします。

6 ［*Finish*］をクリックして、変更を有効にします。

［*Continue Booting after a Time-Out*］をオンにすれば、カウントダウンを行わずに、ブートメニューを永続的に表示することができます。

29.4.5 セキュリティ設定

このYaSTモジュールでは、ブートローダをプロテクトするためのパスワードを設定することもできます。 そうすれば、セキュリティに付加的なレベルを追加できます。

手順 29.6 *ブートローダのパスワードを設定する*

1 ［*Boot Loader Installation*］タブを開きます。

2 ［*Boot Loader Options*］をクリックします。

3 ［*Password Protection*］で、［*Protect Boot Loader with Password*］をオンにして、パスワードを設定します。

4 [*OK*]をクリックします。

5 ［*Finish*］をクリックして、変更を有効にします。

29.4.6 ディスク順序

コンピュータに複数のハードディスクがある場合、ディスクのブートシーケンスを、マシンのBIOSセットアップで定義したのと同じように指定できます(項29.3.2. 「device.mapファイル」 (page 483)を参照)。 次の手順に従います。

手順 29.7　ディスクの順序の設定

1. ［*Boot Loader Installation*］タブを開きます。
2. ［*Boot Loader Installation Details*］をクリックします。
3. 複数のディスクが表示されている場合には、ディスクを選択してから［*Up*］または［*Down*］をクリックして、ディスクの表示順を変更します。
4. ［*OK*] をクリックして、変更内容を保存します。
5. ［*Finish*］をクリックして、変更を有効にします。

このモジュールを使えば、マスタブートレコードを汎用のコード(アクティブなパーティションをブートする)で置き換えることもできます。［*Disk System Area Update*］の［*Replace MBR with Gerneric Code*］をクリックします。また、同じペインの［*Activate Boot Loader Partition*］をクリックすれば、ブートローダのあるパーティションをアクティブにすることができます。［*Finish*］をクリックして、変更を有効にします。

29.5　Linuxブートローダのアンインストール

を使用してLinuxブートローダをアンインストールし、MBRをLinuxインストール前の状態に戻すことができます。インストール中に、YaSTは自動的にオリジナルMBRのバックアップコピーを作成しており、要求があるとGRUBを上書きしてMBRを復元します。

GRUBをアンインストールするには、YaSTブートローダモジュールを起動します(*[システム] → [ブートローダの設定]*)。最初のダイアログで、*[リセット] → [ハードディスクのMBRを戻す]*を選択し、［完了］を選択してダイアログを終了します。MBR内で、GRUBがオリジナルMBRのデータで上書きされます。

29.6 ブートCDの作成

ブートマネージャを使用してシステムをブートできない場合、またはハードディスクやフロッピーディスクのMBRにブートマネージャをインストールできない場合は、Linuxに必要なすべての起動ファイルを使用してブート可能CDを作成することもできます。そのためには、システムにCDライタがインストールされている必要があります。

GRUBでは、stage2_eltoritoという特殊形式の*stage2*とカスタマイズされたmenu.lst(オプション)を使用するだけで、ブート可能CD-ROMを作成することができます。従来のファイルstage1およびstage2は不要です。

cd /tmpおよびmkdir isoなどを使用して、ISOイメージの作成場所となるディレクトリを作成します。また、mkdir -p iso/boot/grubでGRUBのサブディレクトリも作成します。ファイルstage2_eltoritoをディレクトリgrubにコピーします。

```
cp /usr/lib/grub/stage2_eltorito iso/boot/grub
```

また、カーネル(/boot/vmlinuz)、initrd(/boot/initrd)、およびファイル/boot/messageをiso/boot/にコピーします。

```
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
cp /boot/message iso/boot/
```

これらをGRUBで使用できるように、ファイルmenu.lstをiso/boot/grubにコピーし、CD-ROMデバイスを指すようにパスエントリを調整します。そのためには、パス名に(hd*)形式で表示されるハードディスクのデバイス名を、CD-ROMドライブのデバイス名(cd)で置き換えます。

```
gfxmenu (cd)/boot/message
timeout 8
default 0

title Linux
 kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1
splash=verbose showopts
 initrd (cd)/boot/initrd
```

最後に、次のコマンドでISOイメージを作成します。

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso iso
```

次に、好みのユーティリティを使用して、生成されたファイルgrub.isoをCDに書き込みます。

29.7 SUSEのグラフィカル画面

SUSE Linux 7.2 以降は、オプション「vga=<value>」がカーネルパラメータとして使用されている場合、SUSEのグラフィカル画面が1番目のコンソール上に表示されます。を使用してインストールする場合、このオプションは、選択した解像度とグラフィックカードに基づいて自動的に使用されます。 必要な場合にSUSEの画面を無効にするには、3つの方法があります。

必要に応じてSUSE画面を無効にする。
コマンドラインでコマンドecho 0 > /proc/splashを入力し、グラフィカル画面を無効にします。画面を再度有効にするには、echo 1 > /proc/splashコマンドを入力します。

デフォルトでSUSE画面を無効にする。
カーネルパラメータsplash=0をブートローダの設定に追加します。これについては、章29. ブートローダ(page 473)を参照してください。ただし、前のバージョンでデフォルトとなっていたテキストモードを選択する場合は、vga=normalを設定します。

SUSE画面を完全に無効にする。
新しいカーネルをコンパイルし、［*framebuffer support*］でオプション［*Use splash screen instead of boot logo*］を無効にします。

ティップ

カーネルでフレームバッファのサポートを無効にすると、スプラッシュ画面も自動的に無効になります。 システムをカスタムカーネルで実行した場合、SUSEはサポートを何も提供することができません。

29.8 トラブルシューティング

ここでは、を使用してブートする際に頻繁に発生する一部の問題と、考えられる解決策の概略について説明します。一部の問題については、http://

portal.suse.de/sdb/en/index.htmlのSupport Database (サポートデータベース)に記事が提供されています。特定の問題がこのリストに含まれていない場合は、https://portal.suse.com/PM/page/search.pmにアクセスしてSupport Databaseの検索ダイアログを使用し、*GRUB*、*boot*、*boot loader*などのキーワードで検索してください。

GRUBとXFS

XFSの場合、パーティションブートブロックにはstage1のための余地がありません。そのため、ブートローダの位置としてXFSパーティションを指定しないでください。この問題は、XFSでフォーマットされていない別のブートパーティションを作成することで解決できます。

GRUBとJFS

GRUBとJFS を組み合わせることは技術的には可能ですが、問題が生じる可能性があります。この場合は、別のブートパーティション(/boot)を作成し、Ext2でフォーマットします。このパーティションにGRUBをインストールしてください。

GRUBでGRUB Geom Errorがレポートされる

GRUBは、システムのブート時に、接続されているハードディスクのジオメトリを検査します。ときには、BIOSから一貫性のない情報が戻され、GRUBがGRUB Geom Errorをレポートする場合があります。このような場合は、LILOを使用するか、BIOSを更新します。LILOのインストール、設定、および保守の詳細については、Support Database (サポートデータベース)でキーワードLILOを使用すると検索できます。

また、LinuxがBIOSに登録されていない追加ハードディスクにインストールされている場合にも、GRUBはこのエラーメッセージを戻します。ブートローダの*stage1*は正常に検出され読み込まれますが、*stage2*は検出されません。この問題は、新規ハードディスクをBIOSに登録することで解消できます。

IDEハードディスクとSCSIハードディスクを搭載したシステムがブートしない

インストール中に、がハードディスクのブートシーケンスを誤って判別する(およびユーザがそれを訂正していない)場合があります。たとえば、GRUBが/dev/hdaをhd0、/dev/sdaをhd1と見なしても、BIOS内ではブートシーケンスが逆(IDEの*前*にSCSI)になっている場合があります。

この場合は、ブートプロセス中にコマンドラインを使用してハードディスクを訂正します。システムのブート後に、device.mapファイルを編集して新規マッピングを永続的に適用します。次に、/boot/grub/menu.lstファイルと/boot/grub/device.mapファイルでGRUBデバイス名を検査し、次のコマンドでブートローダを再インストールします。

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

2台目のハードディスクからのWindowsのブート

Windowsのような一部のオペレーティングシステムは、1台目のハードディスクからのみブートできます。この種のオペレーティングシステムが2台目以降のハードディスクにインストールされている場合は、関連メニューエントリに対して論理的な変更を加えることができます。

```
...
title windows
map (hd0) (hd1)
map (hd1) (hd0)
chainloader(hd1,0)+1
...
```

この例では、Windowsは2台目のハードディスクから起動されます。この目的で、mapを使用して、ハードディスクの論理的な順序を変更します。この変更は、GRUBのメニューファイル内でのロジックには影響を及ぼしません。したがって、2台目のハードディスクはchainloaderに対して指定する必要があります。

29.9 関連資料

GRUBの詳細情報は、http://www.gnu.org/software/grub/で入手できます。使用中のコンピュータにtexinfoがインストールされている場合、info grubと入力して、シェルの中でGRUBの情報ページを参照できます。http://portal.suse.de/sdb/en/index.htmlにあるSupprt Database (サポートデータベース)で、キーワード「GRUB」を検索して、特別な事項に関する情報を入手することもできます。

30 SUSE Linuxの特別な機能

この章では、まず、さまざまなソフトウェアパッケージ、バーチャルコンソール、およびキーボードレイアウトについて説明します。bash、cron、およびlogrotateといったソフトウェアコンポーネントについても説明します。これらは、前回のリリースサイクルで変更または強化されたからです。これらのコンポーネントはそれほど重要ではないと思われるかもしれませんが、システムと密接に結びついているものなので、デフォルトの動作を変更したい場合もあることでしょう。この章の最後では、言語および国固有設定(I18NおよびL10N)について説明します。

30.1 特殊ソフトウェアパッケージ

bash、cron、logrotate、locate、ulimit、およびfreeといったプログラム、およびresolv.confファイルは、システム管理者および多くのユーザにとって非常に重要です。manのページとinfoのページは、コマンドについての2つの役立つ情報源ですが、その両方が常に利用できるとは限りません。GNU Emacsは、人気のある、自由度に設定できるテキストエディタです。

30.1.1 パッケージBashと/etc/profile

bashはSUSE Linuxのデフォルトのシェルです。ログインシェルとして使用する場合には、いくつかの初期化ファイルを読み込みます。Bashは、各ファイルを次の順序で処理します。

1. /etc/profile

2. ~/.profile

3. /etc/bash.bashrc

4. ~/.bashrc

カスタムの設定は、~/.profileファイルまたは~/.bashrcファイルに指定できます。これらのファイルを正しく処理するには、基本設定ファイル/etc/skel/.profileまたは/etc/skel/.bashrcを、ユーザのホームディレクトリにコピーする必要があります。更新後、/etc/skelディレクトリから設定ファイルをコピーすることをお勧めします。次のシェルコマンドを実行して、既存の個人別設定が失われるのを防止します。

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

それから、個人的な調整点を、*.oldファイルから書き戻します。

30.1.2 cronパッケージ

コマンドを、前もって決めた時間に、定期的かつ自動的にバックグラウンドで実行したい場合、通常はcronを用います。cronは、特別な書式のいくつかのタイムテーブルによって駆動されます。その一部はシステムに付属しています。ユーザは必要に応じ、自分自身のテーブルを書くことができます。

cronテーブルは、/var/cron/tabsにあります。/etc/crontabはシステム全体のcronテーブルとして機能します。タイムテーブルの後に、コマンドを直接実行する必要のあるユーザの名前を入力します。例 30.1.「/etc/crontab内のエントリ」 (page 498)では、rootが入力されています。/etc/cron.dにあるパッケージ固有のテーブルも同じ形式を持ちます。cronのmanページを参照してください(man cron)。

例 30.1 /etc/crontab内のエントリ

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

/etc/crontabを、crontab -eコマンドによって編集することはできません。これは、エディタに直接ロードして、変更し、保存する必要があります。

複数のパッケージによりシェルスクリプトがディレクトリ /etc/cron.hourly、/etc/cron.daily、/etc/cron.weekly、および /etc/cron.monthlyにインストールされます。これらの命令は、/usr/lib/cron/run-cronsによって制御されます。/usr/lib/cron/run-cronsは、15分おきにメインテーブル(/etc/crontab)から実行されます。これにより、無視されていたプロセスが、適切な時刻に実行されることが保証されます。

管理用のスクリプトを1時間ごと、毎日、または他の特定の周期で実行するには、/etc/crontabのエントリで、定期的に、使用するタイムスタンプファイルを削除します(例 30.2. 「/etc/crontab:タイムスタンプファイルの削除」 (page 499)を参照してください。そこでは、hourlyという名前の付いているファイルが毎時59分に、dailyという名前の付いているファイルが毎日午前2:14に削除されるようになっています)。

例 30.2　/etc/crontab:タイムスタンプファイルの削除

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

日常のシステムメンテナンスジョブは、わかりやすいようにさまざまなスクリプトに分散されました。これらはパッケージaaa_baseに含まれています。たとえば、/etc/cron.dailyディレクトリには、コンポーネントsuse.de-backup-rpmdb、suse.de-clean-tmp、またはsuse.de-cron-localがあります。

30.1.3　ログファイル:パッケージlogrotate

カーネルそのものと一緒になって、定期的にシステムスのテータスおよび特定イベントをログファイルに記録するシステムサービス(デーモン)が数多くあります。これにより、管理者は、一定時におけるシステムのステータスを定期的にチェックし、エラーまたは障害のある機能を認識し、そのトラブルシューティングをピンポイントの精度で実行できます。これらのログファイルは、通常、FHSによって指定された/var/logに格納され、日々大きさを増していきます。こうしたログファイルの増大の制御には、logrotateパッケージが役立ちます。

環境設定

logrotateは、 /etc/logrotate.confファイルを使って設定します。特に、includeの指定では主に、読み込む追加のファイルを設定します。SUSE Linuxでは、ログファイルを作成する各プログラムの設定ファイルは、 /etc/logrotate.dにインストールされるようにしています。たとえば、そのようなプログラムは、 apache2パッケージ(/etc/logrotate.d/apache2)およびsyslogdパッケージ(/etc/logrotate.d/syslog)に付属しています。

例 30.3 /etc/logrotate.confの例

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotateは、cronを通じて制御され、毎日 /etc/cron.daily/logrotateによって呼び出されます。

重要項目

作成オプションでは、管理者が/etc/permissions*内に定義したすべての設定が読み取られます。 人による変更で矛盾が出ないことを確認してください。

30.1.4 locate コマンド

ファイルをすばやく検索するためのlocateコマンドは、標準のインストール済みソフトウェアには含まれていません。必要であれば、パッケージ`find-locate`をインストールしてください。updatedbプロセスは、毎晩、またはシステムをブートしてから約15分で自動的に起動します。

30.1.5 ulimitコマンド

`ulimit`(*使用制限*)コマンドを使用すると、システムリソースの使用量に制限を設けたり、これらの制限を表示したりすることができます。`ulimit`は、アプリケーションでの使用可能メモリを制限する場合に特に便利です。1つのアプリケーションが大量のメモリを独占するとシステムが停止してしまいますが、これを使用することで、それが避けられます。

`ulimit`コマンドには、さまざまなオプションがあります。メモリの使用量を制限するには、表30.1.「`ulimit`:ユーザのためのリソースの設定」 (page 501)に示すオプションを使用します。

表 30.1 *ulimit:ユーザのためのリソースの設定*

`-m`	物理メモリの最大サイズ
`-v`	仮想メモリの最大サイズ
`-s`	スタックの最大サイズ
`-c`	コアファイルの最大サイズ
`-a`	制限セットの表示

システム全体の設定は、`/etc/profile`で設定できます。コアファイルの作成を有効にします。 これはプログラマがデバッグを行うために必要です。通常のユーザは、`/etc/profile`ファイルでシステム管理者が指定した値を大きくすることはできませんが、`~/.bashrc`に特別なエントリを作成することは可能です。

*例 **30.4***　*ulimit:~/.bashrc での設定*

```
# Limits of physical memory:
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

メモリの量は、KB単位で指定する必要があります。詳細については、man bashコマンドでmanページを参照してください。

重要項目

すべてのシェルがulimitディレクティブをサポートするわけではありません。ユーザが制約を包括的に設定する必要がある場合、PAM(たとえば、pam_limits)を使用すれば、包括的な調整が可能になります。

30.1.6　freeコマンド

現在使用されているRAMの容量を確認することが目的ならば、freeコマンドは、少々誤解を招くかもしれません。そのような情報は、/proc/meminfoで表示できます。今日では、Linuxのような最新のオペレーティングシステムにアクセスする場合、ユーザはメモリについてそれほど深刻に考える必要はありません。*利用可能なRAM*という概念は、統一的なメモリ管理が生まれる以前の遺物です。*空きメモリは悪いメモリ*というスローガンは、Linuxにぴったりです。結果として、Linuxでは、空きメモリや未使用メモリを実質的に発生させず、キャッシュの量を調整するよう努力が重ねられてきました。

基本的に、カーネルは、アプリケーションやユーザデータについての直接的な知識はありません。その代わりにカーネルは、ページキャッシュのアプリケーションとユーザデータを管理します。メモリが不足すると、その一部はスワップパーティションかファイルに書き込まれ、そこからmmapコマンドで読み込まれます(man mmapコマンドでmanページを参照)。

カーネルには、たとえば、ネットワークアクセスに使用されたキャッシュが格納されている*slab*キャッシュなどの別のキャッシュがあります。これが/proc/meminfoのカウンタ間の違いになります。全部ではありませんが、これらのキャッシュのほとんどは、/proc/slabinfoでアクセスできます。

30.1.7 ファイル/etc/resolv.conf

ドメイン名は、ファイル /etc/resolv.conf を使用して管理されます。詳細については、章 40. ドメインネームシステム (page 661)を参照してください。

このファイルを更新できるのは、スクリプト /sbin/modify_resolvconf のみで、他のプログラムには /etc/resolv.conf ファイルを直接変更するパーミッションがありません。このルールを強制することによってのみ、システムのネットワークの環境設定と関連のファイルが一貫性のある状態に維持されます。

30.1.8 manページとinfoページ

一部のGNUアプリケーション(tarなど)では、manページが提供されなくなりました。manページが用意されていたコマンドについては、--helpオプションを使用して簡単な概要を表示するか、詳細な手順を説明するinfoページを使用します。 infoは、GNUのハイパーテキストシステムです。このシステムについての説明は、info infoを入力して表示します。Info ページは、emacs -f infoコマンドを入力してEmacsを起動するか、コンソールで直接infoと入力します。あるいは、tkinfo、xinfo、またはSUSEヘルプシステムを使用して、infoページを表示します。

30.1.9 GNU Emacs用の設定

GNU Emacsは、複合作業環境です。次の項では、 GNU Emacsの起動時に処理される設定ファイルについて説明します。詳しい説明は、http://www.gnu.org/software/emacs/にあります。

起動時に、Emacsは、カスタマイズおよび事前環境設定用のユーザ、システム管理者、およびディストリビュータ設定が入っているいくつかのファイルを読み取ります。 初期化ファイル~/.emacsが/etc/skelから個々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。代わって.emacsがファイル /etc/skel/.gnu-emacsを読み取ります。プログラムをカスタマイズするには、.gnu-emacsをホームディレクトリ(cp /etc/skel/.gnu-emacs ~/.gnu-emacsを伴う)にコピーして、必要な設定をそこに作成します。

.gnu-emacsは、ファイル~/.gnu-emacs-customをcustom-fileとして定義します。ユーザがEmacsのcustomizeオプションで設定を作成すると、その設定が~/.gnu-emacs-customに保存されます。

SUSE Linuxを使用すると、emacsパッケージでファイルsite-start.elがディレクトリー/usr/share/emacs/site-lispにインストールされます。ファイルsite-start.elは、初期化ファイル~/.emacsの前に読み込まれます。その他では、site-start.elによって、psgmlなど、Emacsアドオンパッケージによって配布された特殊な設定ファイルが自動的に読み込まれます。このタイプの設定ファイルも/usr/share/emacs/site-lispにあり、常にsuse-start-で始まる名前になっています。ローカルシステム管理者は、default.el内にシステム全体の設定を指定できます。

これらのファイルに関する詳しい説明は、*Init File*:info:/emacs/InitFileの下のEmacs infoファイルにあります。必要な場合、これらのファイルの読み込みを防止する方法に関する説明もこの場所にあります。

Emacsのコンポーネントは、次のいくつかのパッケージに分かれています。

- 基本パッケージemacs。
- emacs-x11(通常インストール済み):X11サポートのあるプログラム。
- emacs-nox:X11サポートのないプログラム。
- emacs-nox:info形式のオンライン文書。
- emacs-el:Emacs Lisp内の未コンパイルのライブラリファイル。これらは、実行時には必要ありません。
- 必要なら多くのアドオンパッケージをインストールできます。emacs-auctex (LaTeX版)、 psgml (SGMLおよびXML版)、 gnuserv (クライアント/サーバ運用用)、その他。

30.2 バーチャルコンソール

Linuxは、マルチユーザ、マルチタスクのシステムです。これらの機能は、スタンドアロンのPCシステム上でも利用できます。テキストモードでは、6つの

バーチャルコンソールが使用できます。これらの切り替えには、Alt+F1からAlt+F6を使用します。7番目のコンソールはX用に予約されており、10番目のコンソールにはカーネルメッセージが表示されます。コンソールの割り当て数は、/etc/inittabファイルを修正すれば変更できます。

Xを終了せずにXからコンソールを切り替えるには、Ctrl+Alt+F1からCtrl+Alt+F6までを使用します。Xに戻るには、Alt+F7を押します。

30.3 キーボードマッピング

プログラムのキーボードマッピングを標準化するために、次のファイルに変更が行われました。

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/<VERSION>/site-lisp/term/*.el
```

これらの変更は、terminfoエントリを使用するか、その設定ファイルが直接変更されるアプリケーション(vi、lessなど)にのみ影響します。 .SUSE Linuxに付随しないアプリケーションは、これらのデフォルト値に合わせる必要があります。

Xでは、Composeキー(マルチキー)は、Ctrl+Shift(右)を使用してアクセスできます。対応するエントリも/usr/X11R6/lib/X11/Xmodmapに示されます。

詳しい設定は、Xキーボード拡張(XKB)を使って行うことができます。この拡張機能は、デスクトップ環境GNOME(gswitchit)およびKDE (kxkb)によっても使用されます。

ティップ: 関連資料

XKBに関する説明は、/etc/X11/xkb/README とそこにリストされた文書にあります。

中国語、日本語、および韓国語(CJK)に関する詳しい説明は、Mike Fabianのページにあります。 http://www.suse.de/~mfabian/suse-cjk/input.html.

30.4 言語および国固有の設定

SUSE Linuxは、非常に広い範囲で国際化されており、現地の状況に合わせて柔軟に変更できます。言い換えれば、国際化(*I18N*)によって具体的なローカライズ(*L10N*)が可能になっています。I18NとL10Nという略語は、語の最初と最後の文字の間に、省略されている文字数を挟み込んだ表記です。

設定は、ファイル/etc/sysconfig/languageの変数RC_LC_で定義します。これは、単なる*現地語サポート*だけでなく、*Messages* (メッセージ) (言語)、*Character Set* (文字セット)、*Sort Order* (ソート順)、*Time and Date* (時刻と日付)、*Numbers* (数字)および*Money* (通貨)の各カテゴリも指します。これらのカテゴリはそれぞれ、独自の変数を使用して直接定義することも、ファイルlanguageにあるマスタ変数を使用して間接的に定義することも可能です(man localeコマンドでmanページを参照)。

RC_LC_MESSAGES, RC_LC_CTYPE, RC_LC_COLLATE, RC_LC_TIME, RC_LC_NUMERIC, RC_LC_MONETARY
: これらの変数は、プレフィクスRC_を付けずにシェルに渡され、前述のカテゴリを表します。関連するシェルプロファイルについては後で説明します。現在の設定は、コマンドlocaleを使用して表示できます。

RC_LC_ALL
: この変数は、すでに参照された変数の値を上書きします。

RC_LANG
: 前述の変数がまったく設定されていない場合、これがフォールバックとなります。デフォルトでは、SUSE LinuxはRC_LANGだけを設定します。これにより、ユーザが独自の変数を入力しやすくなります。

ROOT_USES_LANG
: yesまたはno変数。noに設定するとrootが常にPOSIX環境で動作します。

他の変数は、YaSTの［/etc/sysconfigエディタ］で設定できます(項28.3.1.「YaSTのsysconfigエディターを使ってシステム設定を変更する」 (page 469)を参照)。このような変数の値には、言語コード、国コード、エンコーディング、および修飾子が入っています。個々のコンポーネントは特殊文字で接続されます。

```
LANG=<language>[[ _<COUNTRY>].<Encoding>[ @<Modifier>]]
```

30.4.1 例

言語コードと国コードは必ず一緒に設定する必要があります。言語の設定は、http://www.evertype.com/standards/iso639/iso639-en.htmlおよびhttp://www.loc.gov/standards/iso639-2/で入手できる、ISO 639規格に従います。国コードは、http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.htmlで入手できる、ISO 3166にリストされています。

使用可能な説明ファイルが/usr/lib/localeに存在する場合のみ、値を設定する意味があります。追加の記述ファイルは、/usr/share/i18nのファイルを使用し、コマンドlocaledefを実行して作成できます。記述ファイルは、glibc-i18ndataパッケージに含まれています。en_US.UTF-8の説明ファイル(英語および米国)は以下のように作成します。

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

LANG=en_US.UTF-8
インストール時にAmerican Englishを選択すると、これがデフォルトの設定になります。他の言語を選択した場合、その言語が有効になりますが、文字コードはUTF-8が使用されます。

LANG=en_US.ISO-8859-1
これにより、言語が英語、国が米国、文字セットがISO-8859-1に設定されます。この文字セットは、ユーロ記号をサポートしませんが、UTF-8がサポートされていない、更新前のプログラムを使用する方が便利なこともあります。文字セット(この状況ではISO-8859-1)を定義する文字列は、Emacsのようなプログラムによって評価されます。

LANG=en_IE@euro
上記の例では、ユーロ記号が言語設定に明示的に組み込まれています。厳密に言うと、この設定は今では古くなっています。UTF-8もユーロ記号を

扱うからです。この設定が役立つのは、アプリケーションがUTF-8ではなく、ISO-8859-15しかサポートしない場合だけです。

SuSEconfigは、 /etc/sysconfig/languageにある変数を読み込み、必要な変更を /etc/SuSEconfig/profileと /etc/SuSEconfig/csh.cshrcに書き込みます。 /etc/SuSEconfig/profileは /etc/profileによって読み込まれます。 つまり、 ソースとして使用されます。 /etc/SuSEconfig/csh.cshrcは /etc/csh.cshrcのソースとして使用されます。 これにより、設定はシステム全体に渡って使用できるようになります。

ユーザは、同様に~/.bashrcファイルを編集して、システムのデフォルトを上書きすることができます。たとえば、システム設定のen_USをプログラムメッセージに使用しない場合は、LC_MESSAGES=es_ES を指定してメッセージが英語の代わりにスペイン語で表示されるようにします。

30.4.2 言語サポートの設定

カテゴリ*Messages*のファイルは、フォールバックを確保するため、対応する言語ディレクトリ(たとえば、en)にのみ格納されることになっています。たとえばLANGをen_USに設定したが、*message*ファイルが /usr/share/locale/en_US/LC_MESSAGESに存在しない場合は、 /usr/share/locale/en/LC_MESSAGESにフォールバックされます。

フォールバックチェーンも定義できます。 たとえば、ブルターニュ語、次いでフランス語、またはガリシア語、次いでスペイン語、次いでポルトガル語の順にフォールバックするには、次のように設定します。

```
LANGUAGE="br_FR:fr_FR"

LANGUAGE="gl_ES:es_ES:pt_PT"
```

必要に応じて、次のようにノルウェー語の方言であるニーノシクやブークモールをノルウェー語の代わりに使用できます(noへのフォールバックを追加します)。

```
LANG="nn_NO"

LANGUAGE="nn_NO:nb_NO:no"
```

または

```
LANG="nb_NO"

LANGUAGE="nb_NO:nn_NO:no"
```

ノルウェー語では、LC_TIMEの扱いも違うので注意してください。

生じる可能性のある1つの問題は、数字の桁を区切るための文字が正しく認識されないことです。このことは、LANGがdeのような2文字の言語コードにのみ設定されているのに、glibcが使用している定義ファイル/usr/share/lib/de_DE/LC_NUMERICに存在している場合に生じます。それで、区切り文字の定義がシステムに認識されるようにするには、LC_NUMERICをde_DEに設定する必要があります。

30.4.3 関連資料

- 『*The GNU C Library Reference Manual*』の「Locales and Internationalization」の章。glibc-infoパッケージに格納されています。
- 『*UTF-8 and Unicode FAQ for Unix/Linux*』、Markus Kuhn 著。 Web ページ http://www.cl.cam.ac.uk/~mgk25/unicode.html (現在のアドレス)を参照してください。
- 『*Unicode-Howto*』(Bruno Haible著)を参照してください。/usr/share/doc/howto/en/html/Unicode-HOWTO.html

31 プリンタの運用

CUPSは、SUSE Linuxでの標準的な印刷システムです。CUPSは、特にユーザ中心の構造(ユーザ志向の設計)です。多くの状況ではLPRngとの互換性があるか、比較的少ない作業で適応させることができます。 LPRngは、互換性を維持する理由でのみ、SUSE Linuxに付属しています。

プリンタは、インタフェース(USB、ネットワークなど)と、プリンタ言語によって区別できます。プリンタを購入するときは、ハードウェア(コンピュータ)がサポートしているインタフェースを採用していること、および適切なプリンタ言語が使用できることを確認してください。プリンタは、次の3つのプリンタ言語クラスに基づいて分類できます。

PostScriptプリンタ
PostScriptは、LinuxとUnix環境のほとんどの印刷ジョブを生成する際に使用されるプリンタ言語であり、内部の印刷システムもこの言語を使用して処理を行います。この言語はかなり古いのですが、かなり効率的です。使用中のプリンタがPostScriptドキュメントを直接処理でき、印刷システム側で追加のステージを使用して変換を行う必要がない場合、潜在的なエラーの原因の数が減少します。PostScriptプリンタは多額のライセンスコストの対象になるので、通常、これらのプリンタは、PostScriptインタプリタを内蔵しないプリンタよりコストが高くなります。

標準的なプリンタ(PCLおよびESC/Pなどの言語)
これらのプリンタ言語はかなり古いのですが、プリンタで新機能を実現するために、引き続き拡張が行われています。既知のプリンタ言語の場合、印刷システムはGhostscriptの支援により、PostScriptのジョブを該当のプリンタ言語へ変換できます。この処理ステージを「解釈」(interpreting)と呼びます。非常によく知られている言語は、ほとんどのHPのプリンタおよび互

換モデルが採用しているPCLと、Epsonのプリンタが採用しているESC/Pです。これらのプリンタ言語は、通常はLinuxによってサポートされていて、まずまずの印刷結果をもたらします。最新のプリンタや特殊なプリンタの機能は、Linuxがサポートしていないことがあります。オープンソースの開発者は、それらの機能に関してまだ作業をしている可能性もあります。HPが開発したhpijsドライバを除き、現時点では、Linuxドライバを開発してオープンソース条項に基づきそれらをLinuxのディストリビュータに提供しているプリンタメーカは存在しません。これらのプリンタのほとんどは、中間の価格帯にあります。

独自規格のプリンタ(通常はGDIプリンタ)
独自規格のプリンタでは通常、1つまたは複数のWindowsドライバだけが使用可能です。これらのプリンタは、一般的なプリンタ言語をどれもサポートしていませんし、これらのプリンタが使用しているプリンタ言語は、新しいモデルがリリースされた段階で変更される可能性もあります。詳細については、項31.7.1.「標準的なプリンタ言語をサポートしないプリンタ」(page 529)を参照してください。

新しいプリンタを購入する前に、次の各ソース(情報源)を参照し、購入を予定しているプリンタがどの程度までサポートされているかをチェックしてください。

- http://cdb.suse.de/—SUSE Linuxプリンタデータベース
- http://www.linuxprinting.org/—LinuxPrinting.orgのプリンタデータベース
- http://www.cs.wisc.edu/~ghost/—GhostscriptのWebページ
- /usr/share/doc/packages/ghostscript/catalog.devices—付属するドライバのリスト

オンラインデータベースはいつでも、Linuxによるサポートの最新のステータスを示しています。しかし、Linuxのディストリビューションが統合できるのは、製造の時点で使用可能だったドライバだけです。 したがって、現時点で「perfectly supported」(完全にサポート済み)と評価されているプリンタであっても、最新バージョンのSUSE Linuxがリリースされた時点では、そのステータスに達していなかった可能性があります。そのため、これらのデータベースは必ずしも正しいステータスを表しているとは限らず、おおよその状況を提示するだけにとどまっています。

31.1 印刷システムのワークフロー

ユーザが印刷ジョブを作成します。印刷ジョブは、印刷するデータとスプーラに対する情報から構成されますが、その情報には、プリンタの名前またはプリンタキューの名前だけでなく、必要に応じて、プリンタ固有のオプションなど、フィルタに関する情報も含まれます。

すべてのプリンタには専用のプリンタキューが存在します。指定のプリンタがデータを受け取れるようになるまで、スプーラは印刷ジョブをキュー内に留めています。プリンタの準備が整うと、スプーラはフィルタおよびバックエンドを経由して、プリンタにデータを送信します。

フィルタを使用すると、ユーザが印刷するデータ(ASCII、PostScript、PDF、JPEGなど)がプリンタ固有のデータ(PostScript、PCL、ESC/Pなど)に変換されます。プリンタの機能については、PPDファイルに記述されています。PPDファイルには、プリンタ固有のオプションが記述されています。各オプションに対しては、プリンタでそのオプションを有効にするために必要なパラメータが指定されています。フィルタシステムは、ユーザが有効として選択したオプションを確認します。

PostScriptプリンタを選択すると、フィルタシステムがデータをプリンタ固有のPostScriptに変換します。この変換にプリンタドライバは必要ありません。PostScript非対応プリンタを使用すると、フィルタシステムがGhostscriptを使用して、データをプリンタ固有データに変換します。この変換には、使用しているプリンタに適応したGhostscriptプリンタドライバが必要です。バックエンドは、プリンタ固有データをフィルタから受信し、そのデータをプリンタに送信します。

31.2 プリンタに接続するための方法とプロトコル

プリンタをシステムに接続するには、さまざまな方法があります。CUPS印刷システムの設定は、ローカルプリンタと、ネットワーク経由でシステムに接続されているプリンタを区別しません。Linux環境では、ローカルプリンタは、プリンタメーカのマニュアルに記載されているとおりに接続する必要があります。CUPSは、シリアル、USB、パラレル、およびSCSI接続をサポートしています。プリンタ接続の詳細については、http://portal.suse.com

にアクセスしてSupport Database (サポートデータベース)で記事「*CUPS in a Nutshell*」を参照してください。検索ダイアログに「*cups*」と入力すると、この記事を検索できます。

警告: コンピュータへのケーブル接続

プリンタをコンピュータに接続する場合、コンピュータの動作中に接続と取り外しを行って良いのはUSBデバイスだけであることに注意してください。他の種類の接続を使用する場合、変更を加える前に、システム(コンピュータ)をシャットダウンする必要があります。

31.3 ソフトウェアのインストール

PPD (PostScript printer description、PostScriptプリンタ記述)は、PostScriptプリンタの特性(解像度など)やオプション(両面印刷ユニットなど)を記述するコンピュータ言語です。これらの記述は、CUPS側でさまざまなプリンタオプションを使用するために必須です。PPDファイルがない場合、印刷データは「raw」(ロー、未加工)状態でプリンタへ送信されますが、そのことは通常は望ましくありません。SUSE Linuxのインストール時には、PostScriptサポート機能のないプリンタでも使用できるように、多数のPPDファイルが事前インストールされます。

PostScriptプリンタを設定する場合、最善のアプローチは、適切なPPDファイルを入手することです。この種の多数のPPDファイルは、標準インストールの範囲内で自動的にインストールされるパッケージ`manufacturer-PPDs`に用意されています。項31.6.3.「各種パッケージ内のPPDファイル」 (page 526)と項31.7.2.「特定のPostScriptプリンタに適したPPDファイルが入手できない」(page 530)を参照してください。

新しいPPDファイルは、`/usr/share/cups/model/`ディレクトリ内に保存するか、YaSTで印刷システムに追加できます(手動設定項 (page 516)を参照)。その結果、インストールの際にPPDファイルを選択できるようになります。

ユーザが設定ファイルを変更するのみでなくソフトウェアパッケージ全体をインストールすることを、プリンタメーカが望んでいるかどうかに注意してください。第一に、このようなタイプのインストールを行うと、SUSE Linuxによって提供されているサポートが失われる結果になります。第二に、印刷コマンドが異なる方法で機能する可能性があり、システムは他のメーカのデ

バイスに対応できなくなる可能性もあります。この理由で、メーカのソフトウェアをインストールすることをお勧めしません。

31.4 プリンタの設定

プリンタをコンピュータに接続し、ソフトウェアをインストールした後、システム内でプリンタ(論理プリンタ)をインストールする必要があります。可能であれば、この操作にはSUSE Linuxに付属のツールを使用してください。SUSE Linuxはセキュリティに最大の注意を払っていますが、サードパーティのツールは多くの場合、セキュリティ上の制限に関して課題を残しており、最終的には、利点より煩雑さが勝る傾向があります。トラブルシューティングの詳細については、項31.6.1.「CUPSサーバとファイアウォール」 (page 523)および項31.6.2.「CUPS印刷サービスの変更点」 (page 524)を参照してください。

31.4.1 ローカルプリンタ

ログイン時に未設定のローカルプリンタが検出されると、YaSTはその設定を開始します。この場合、設定についての次の説明と同じダイアログが使用されます。

プリンタを設定するには、YaSTコントロールセンターで*[ハードウェア]* → *[プリンタ]*の順に選択します。これでプリンタ設定のメインウィンドウが開きます。このウィンドウでは、検出されたデバイスのリストが上部に表示されます。下の部分にはこれまでに設定されているすべてのキューのリストが表示されます。使用しているプリンタが検出されない場合は、手動で設定します。

重要項目

［プリンタ］エントリがYaSTコントロールセンターで使用できない場合は、その原因としてほとんどの場合、`yast2-printer`パッケージがインストールされていない可能性があります。この問題を解決するには、`yast2-printer`パッケージをインストールして、YaSTを再起動します。

自動設定

パラレルまたはUSBポートを自動的に設定し、接続されたプリンタを検出できる場合、YaSTはプリンタを自動で構成できます。プリンタデータベース内には、自動ハードウェア検出のときにYaSTが検索するプリンタID文字列も必要です。ハードウェアIDがモデル指定と異なっている場合は、手動でモデルを選択します。

すべてが正しく機能できるようにするために、各設定をYaSTの印刷テスト機能でチェックしてください。 テストページには、テストする設定についての重要な情報もあります。

手動設定

自動設定の条件が満たされない場合、またはカスタム設定が必要な場合は、プリンタを手動で設定します。自動検出の成功の条件およびプリンタモデルについてデータベース中に見つかる情報の量に応じて、YaSTが正しい設定を自動的に判別できる場合もあれば、最低限の適切な事前選択を行う場合もあります。

設定する必要があるパラメータは次のとおりです。

ハードウェア接続(ポート)
ハードウェア接続の設定は、YaSTがハードウェアの自動検出のときに、プリンタを検出できるようになっていたかどうかによって異なります。プリンタモデルを自動的に検出できる場合、YaSTは、プリンタ接続がハードウェアレベルで機能し、この点では設定変更が必要ないと判断します。YaSTがプリンタモデルを自動検出できない場合は、 ハードウェアレベルでの接続に問題がある可能性があります。この場合、接続の設定にある程度の手動介入が必要になります。

［*プリンタ設定*］ダイアログで、［*設定*］を押して手動設定ワークフローを開始します。ここで、お使いの［*プリンタタイプ*］(例えば、USBプリンタなど)を選択し、［次へ］をクリックして、［*プリンタ接続*］を入力し、デバイスを選択します。

キューの名前

キュー名は、印刷コマンドを実行するときに使用します。名前は比較的短いものにし、英小文字と数字だけを使用して指定してください。次のダイアログ(*キュー名*)で、［*印刷用の名前*］を入力します。

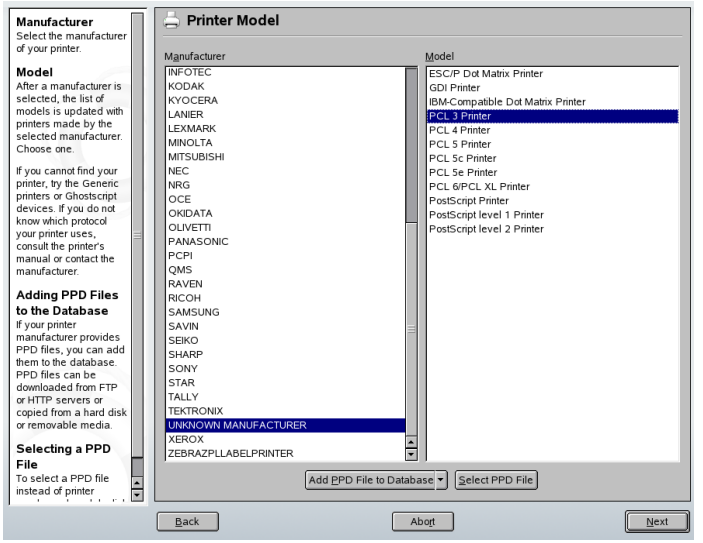
プリンタモデルおよびPPDファイル

使用するGhostscriptドライバやドライバ用のプリンタフィルタに関するパラメータなど、プリンタ固有パラメータはすべて、PPD (PostScript Printer Description)ファイルに保存されます。PPDファイルの詳細については、項 31.3. 「ソフトウェアのインストール」 (page 514)を参照してください。

多くのプリンタモデルでは、いくつかのGhostscriptドライバが特定のモデルで機能する場合などに、複数のPPDファイルを使用できます。次のダイアログ(［*プリンタモデル*］)でメーカおよびモデルを選択すると、YaSTがプリンタに対応するPPDファイルを選択します。モデルに対して複数のPPDファイルを使用できる場合、YaSTはそれらのうちの1つ(通常は、推奨とマーク付けされています)をデフォルトとします。選択されたPPDファイルは次のダイアログの［*編集*］で変更できます。

PostScript以外のモデルの場合、プリンタ固有のデータはすべて、Ghostscriptドライバによって作成されます。この理由から、ドライバ設定は、出力品質を左右する最も重要な要因の1つです。印刷出力は、選択したGhostscriptドライバの種類(PPDファイル)とその指定したオプションの両方の影響を受けます。必要に応じて、［*編集*］を選択して(PPDファイルで使用できるようにした場合のように)追加オプションを変更します。

図 31.1　プリンタモデルの選択



テストページを印刷して、設定が予想どおりに機能するかどうかを確認してください。たとえば、数ページがほとんど何も印刷されない状態になるなど、出力が文字化けした場合は、最初にすべての用紙を取り出し、YaSTがテストを実行できないようにすると、プリンタを停止できます。

プリンタデータベースに使用中のモデルのエントリが含まれていない場合、［*Add PPD File to Database (PPDファイルをデータベースに追加)*］を選択して、新しいPPDファイルを追加したり、基本PPDファイルのコレクションを使用して、プリンタを標準プリンタ言語で機能させることができます。このためには、プリンタメーカとして［*UNKNOWN MANUFACTURER (不明なメーカ)*］を選択します。

詳細な設定
: 通常、詳細設定を変更する必要はありません。

31.4.2　ネットワークプリンタ

ネットワークプリンタは、さまざまなプロトコルをサポートできますし、その複数を同時にサポートすることも可能です。サポートされているプロトコルのほとんどは標準化されたものですが、いくつかのメーカはその標準に拡

張(変更)を加えました。それらのメーカは標準を正しく実装していないシステムのテストや、標準では使用できない特定の機能を提供することを望んでいます。そのような場合、メーカは少数のオペレーティングシステム用にのみドライバを提供し、自社のシステムにつきまとう課題を排除します。残念なことに、Linuxドライバはめったに提供されません。現在の状況では、あらゆるプロトコルがLinux環境で円滑に動作するという仮定に基づいて行動することはできません。したがって、機能する設定を実現するために、さまざまなオプションを実験する必要があります。

CUPSは`socket`、`LPD`、`IPP`、および`smb`の各プロトコルをサポートしています。ここでは、これらのプロトコルに関する詳細な情報について説明します。

socket

*socket*は、データのハンドシェイクを最初に行うことなく、データをインターネットソケットへ送信する接続を意味します。一般的に使用されるsocketのポート番号のいくつかは、`9100`または`35`です。デバイスURIの例は、`socket://host-printer:9100/`です。

LPD (line printer daemon、ラインプリンタデーモン)

実証されてきたLPDプロトコルは、RFC1179で説明されています。このプロトコルを使用する場合、プリンタキューのIDのようなジョブ関連データの一部は、実際の印刷データより先に送信されます。したがって、データを送信するために、LPDプロトコルを設定する際にプリンタキューを指定する必要があります。さまざまなプリンタメーカによる実装は、プリンタキューとして任意の名前を受け入れる柔軟性を備えています。必要に応じて、使用可能な名前がプリンタのマニュアルに提示されています。多くの場合、LPT、LPT1、LP1、または他の類似した名前が使用されています。CUPSシステムを採用している他のLinuxホストまたはUnixホスト上で、LPDキューを設定することもできます。LPDサービスが使用するポート番号は`515`です。デバイスURIの例は、`lpd://host-printer/LPT1`です。

IPP (Internet Printing Protocol、インターネット印刷プロトコル)

IPPは比較的新しい(1999年)プロトコルであり、HTTPプロトコルに基づいています。IPPを使用する場合、他のプロトコルより、ジョブとの関連性が高いデータが送信されます。CUPSは、IPPを使用して内部のデータ送信を行います。これは、2台のCUPSサーバ間でキューを転送する上で優先されるプロトコルです。IPPを正しく設定するには、印刷キューの名前は必須です。IPPのポート番号は`631`です。デバイスURIの例は、
`ipp://host-printer/ps`および
`ipp://host-cupsserver/printers/ps`です。

SMB (Windows共有)

CUPSは、Windows共有に接続されたプリンタへの印刷もサポートしています。この目的で使用されるプロトコルは、SMBです。SMBは、ポート番号137、138、および139を使用します。デバイスURIの例は、`smb://user:password@workgroup/server/printer`、`smb://user:password@host/printer`、および`smb://server/printer`です。

設定を行う前に、プリンタがサポートしているプロトコルを決定する必要があります。必要な情報をメーカが提供していない場合、`nmap`コマンド(`nmap`パッケージ)を使用して、プロトコルを推定します。`nmap`は、ホストでオープンしているポートをチェックします。次に例を示します。

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

YaSTを使用するネットワーク内でのCUPSの設定

ネットワークプリンタは、YaSTを使用して構成する必要があります。YaSTは、設定を簡単にし、CUPSでのセキュリティ制約の扱いに最も優れています(項31.6.2.「CUPS印刷サービスの変更点」 (page 524)を参照)。ネットワークでのCUPSのインストールのガイドラインについては、`http://portal.suse.com`にアクセスしてSupport Database (サポートデータベース)で記事「*CUPS in a Nutshell*」を参照してください。

［*その他(未検出)*］を選択し、［*設定*］をクリックします。ネットワーク管理者に別途指示されていない場合は、［*ネットワークプリンタへのディレクトリの印刷*］を選択して、具体的な必要条件にしたがって進みます。

コマンドラインツールによる設定

代わりに、`lpadmin`や`lpoptions`などのコマンドラインツールを使用してCUPSを設定することもできます。バックエンド(usbなど)とパラメータ(`/dev/usb/lp`など)で構成されるデバイスURI (uniform resource identifier)が必要です。たとえば、完全URIは`parallel:/dev/lp0` (パラレルポート1に接続されているプリンタ)または`usb:/dev/usb/lp0` (USBポートに接続されている最初に検出されたプリンタ)などとなります。

`lpadmin`で、CUPSサーバ管理者の追加、削除、またはクラスおよび印刷キューの管理ができます。プリンタキューを追加するには、次の構文を使用します。

```
lpadmin -p queue -v device-URI \
-P PPD-file -E
```

デバイス(-v)は、キュー(-p)として、指定されたPPDファイル(-P)を使用して利用可能になります。これは、プリンタを手動で設定する場合は、PPDファイルおよびデバイスの名前を知っておく必要があるということを意味します。

-Eは、最初のオプションとして使用しないでください。どのCUPSコマンドでも、-Eを最初の引数として使用した場合、暗号化接続を使用することを暗示的に意味します。プリンタを使用可能にするには、次の例に示す方法で-Eを使用する必要があります。

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

ネットワークプリンタの設定例:

```
lpadmin -p ps -v socket://192.168.1.0:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

lpadminのオプションの詳細については、lpadminのマニュアルページを参照してください。

システムのインストール時には、一部のオプションがデフォルトとして設定されています。これらのオプションは、各印刷ジョブ用に変更できます(使用される印刷ツールに依存)。YaSTを使用して、これらのデフォルトオプションを変更することもできます。コマンドラインツールを使用して、デフォルトオプションを次のように設定します。

1. 最初に、すべてのオプションを列挙します。

   ```
   lpoptions -p queue -l
   ```

   例:

   ```
   解像度/出力解像度: 150dpi *300dpi 600dpi
   ```

   有効になっているデフォルトのオプションは、左側にあるアスタリスク(*)によって明示されます。

2. 次のようにlpadminを使用してオプションを変更します。

   ```
   lpadmin -p queue -o Resolution=600dpi
   ```

3. 新しい設定値のチェック:

```
lpoptions -p queue -l

解像度/出力解像度: 150dpi 300dpi *600dpi
```

通常のユーザが`lpoptions`を実行すると、設定が`~/.lpoptions`に書き込まれます。`root`の設定は`/etc/cups/lpoptions`に書き込まれます。

31.5 アプリケーション用の設定

アプリケーションは、コマンドラインツールの場合と同様に、既存のプリンタキューに依存しています。通常は、特定のアプリケーション用にプリンタを再設定する必要はありません。使用可能なキューを使用して、アプリケーションから印刷できるようになっています。

コマンドラインから印刷するには、コマンド`lp -d` *`queuename filename`*」を入力し、*`queuename`*および*`filename`*を対応する名前で置き換えます。

一部のアプリケーションでは、印刷処理を`lp`コマンドに依存しています。この場合、アプリケーションの印刷ダイアログで正しいコマンドを入力します。ただし、通常は*`filename`*を指定しません。たとえば、`lp -d` *`queuename`* と入力します。KDEプログラムでこの処理を行うには、［*Print through an external program (外部プログラムによる印刷)*］を有効にします。このオプションを有効にしないと、印刷コマンドを入力できません。

xppやKDEプログラムkprinterなどのツールは、キューを選択したり、CUPS標準オプションとPPDファイルを介して使用可能になるプリンタ固有オプションの両方を設定するための、グラフィカルなインタフェースを提供します。kprinterは、KDE以外のアプリケーションの印刷ダイアログで`kprinter`または`kprinter --stdin`を印刷コマンドとして指定すると、そのようなアプリケーションの標準印刷インタフェースとして使用できます。これら2つのコマンドのどちらが選択されるかは、アプリケーション自身の動作によって決定されます。設定が適切であれば、アプリケーションから印刷ジョブが発行されると、アプリケーションはkprinterのダイアログを表示します。このダイアログを使用してキューを選択し、他の印刷オプションを設定できます。この場合、アプリケーション自身の印刷設定がkprinterの印刷設定と競合が発生せず、kprinterが使用可能になった後で、印刷オプションの変更がkprinterによってのみ行われる必要があります。

31.6 SUSE Linuxの特別な機能

CUPSの多くの機能は、SUSE Linuxで使用できるように調整されています。ここでは、最も重要な変更点について説明します。

31.6.1 CUPSサーバとファイアウォール

CUPSをネットワークサーバのクライアントとして設定するには、複数の方法があります。

1. ネットワークサーバ上のキューごとに、すべてのジョブを対応するネットワークサーバに転送するときに使用するローカルキューを設定できます。ネットワークサーバの設定に変更があるたびに、すべてのクライアントマシンの再設定が必要になるため、通常、この方法はお勧めしません。

2. 印刷ジョブを1つのネットワークサーバに直接転送することもできます。このタイプの設定では、CUPSデーモンを実行しないでください。`lp`(または他のプログラムの対応ライブラリコール)により、ジョブをネットワークサーバに直接送信できます。ただし、ローカルプリンタで印刷する必要がある場合、この設定は機能しません。

3. CUPSデーモンは、使用可能なキューを通知するために他のネットワークサーバから送信されるIPPブロードキャストパケットをリスニングできます。この方法を使用するには、ポート631/UDPを着信パケット用にオープンしておく必要があります。

   これは、リモートCUPSサーバを介した印刷に最適のCUPS設定です。ただし、攻撃者がキューと共にデーモンのIPPブロードキャストを送信し、ローカルデーモンが偽のキューにアクセスする危険性があります。その場合、問題のキューがローカルサーバ上の別のキューと同じ名前で表示されると、ジョブが実際には攻撃者のサーバに送信されているのに、ジョブの所有者はローカルサーバに送信されていると考える可能性があります。

YaSTは、すべてのネットワークホストをスキャンして、このサービスが提供されているかどうかを確認し、IPPブロードキャストをリスニングして、CUPSサーバを検索できます。第2の方法は、提案用にCUPSサーバを検出するため

に、システムインストールのときに使用されます。この方法を使用するには、ポート631/UDPを着信パケット用にオープンしておく必要があります。第2の方法でポートをオープンしてリモートキューへのアクセスを設定する操作には、セキュリティ上のリスクを伴います。これは、ユーザが受け入れるサーバを攻撃者がブロードキャストする可能性があるからです。

提案ダイアログに表示されるファイアウォールのデフォルト設定では、インタフェースでのIPPブロードキャストは許可されていません。したがって、リモートキューを検出する第2の方法と、リモートキューにアクセスする第3の方法は機能しません。そのため、インタフェースの1つを`internal` (デフォルトでポートをオープン)として指定するか、`external`インタフェースのポートを明示的にオープンして、ファイアウォール設定を変更する必要があります。 セキュリティ上の理由から、デフォルトでは開いているポートはありません。

CUPSがインストール時にリモートキューを検出し、通常の操作中にローカルシステムから各種リモートサーバにアクセスできるように、提案されるファイアウォール設定を変更する必要があります。または、ユーザがローカルネットワークホストをスキャンするか、すべてのキューを手動で設定することにより、CUPSサーバを検出することもできます。ただし、このセクションの始めのほうで述べられている理由から、この方法はお勧めしません。

31.6.2 CUPS印刷サービスの変更点

これらの変更は、初めにSUSE Linux 9.1に適用されました。

lpユーザとしてのcupsdの実行

起動時に、`cupsd`は`root`ユーザから`lp`ユーザへの切り替えを行います。これは、セキュリティをより高いレベルに引き上げます。CUPS印刷サービスは、無制限のパーミッションを使用する代わりに、印刷サービスで必要とされるパーミッションだけを使用して動作するためです。

しかし、認証(より正確に表現すると、パスワードのチェック)は、`/etc/shadow`を介して実行することはできません。`lp`には、`/etc/shadow`へのアクセス権がないためです。代わりに、`/etc/cups/passwd.md5`を介したCUPS特有の認証を使用する必要があります。この目的で、CUPS管理グループである`sys`に所属していて、CUPSパスワードの割り当てを受けたCUPS管理者

を、/etc/cups/passwd.md5ファイル内に記述する必要があります。この作業を行うには、rootとして、次のコマンドを入力します。

```
lppasswd -g sys -a CUPS-admin-name
```

この設定は、Webフロントエンド(CUPS)またはプリンタ管理ツール(KDE)を使用して管理を行う場合にも重要です。

lpでcupsdを実行した場合、/etc/printcapを生成することはできません。lpは、/etc/直下にファイルを作成することを許可されていないためです。そのため、cupsdは/etc/cups/printcapを生成します。アプリケーションが/etc/printcapからキュー名の読み取りのみを実行して引き続き正常に動作できることを保証するために、/etc/printcapは、/etc/cups/printcapを指すシンボリックリンクになっています。

lpでcupsdを実行した場合、ポート631をオープンすることはできません。そのため、rccups reloadを使用してcupsdを再ロードすることはできません。代わりに、rccups restartを使用してください。

BrowseAllowとBrowseDenyの一般化された機能

BrowseAllowとBrowseDenyに対して設定されたアクセスパーミッションは、cupsdに対して送信されたすべてのタイプのパッケージに適用されます。/etc/cups/cupsd.conf内にあるデフォルトの設定値は、次のとおりです。

```
BrowseAllow @LOCAL
BrowseDeny All
```

および

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

この方法では、LOCALホストだけが、CUPSサーバ上のcupsdにアクセスできます。LOCALホストとは、PPPインタフェース以外(より正確に表現すると、IFF_POINTOPOINTフラグがセットされていないインタフェース)に所属する

IPアドレスを使用し、そのIPアドレスがCUPSサーバと同じネットワークに所属しているホストのことです。他のすべてのホストから着信したパケットは、即座に拒否されます。

cupsdがデフォルトで有効化

標準的なインストールでは、cupsdは自動的に有効になり、追加で手動の操作を行うことなく、CUPSネットワークサーバのキューに対して適切にアクセスすることができます。この機能を使用するには、lpユーザとしてのcupsdの実行項 (page 524)およびBrowseAllowとBrowseDenyの一般化された機能項 (page 525)内の項目が必須の前提条件になります。それらが満たされていない場合、cupsdを自動的に有効にする状況で、セキュリティが不十分になります。

31.6.3 各種パッケージ内のPPDファイル

YaSTのプリンタ設定機能は、システムの/usr/share/cups/model/内に記述されたPPDファイルのみを使用して、CUPS用のキューをセットアップします。プリンタモデルに適したPPDファイルを決定するために、YaSTはハードウェア検出の際に判断されたベンダおよびモデルを、システムの/usr/share/cups/model/内で使用可能なすべてのPPDファイル内にあるベンダおよびモデルと比較します。この目的で、YaSTのプリンタ設定機能は、PPDファイルから抽出したベンダおよびモデルの情報に基づいて、データベースを生成します。ベンダおよびモデルのリストから特定のプリンタを選択した場合、そのベンダおよびモデルに対応するPPDファイルを受け取ることになります。

PPDファイルのみを使用し、他の情報ソースを使用しない設定には、/usr/share/cups/model/内のPPDファイルを自由に変更できるという利点があります。YaSTのプリンタ設定機能は、変更結果を認識し、ベンダおよびモデルからなるデータベースを再生成します。たとえば、PostScriptプリンタのみを使用している場合、通常はcups-driversパッケージ内にあるFoomatic PPDファイルや、cups-drivers-stpパッケージ内にあるGimp-Print PPDファイルを必要としません。代わりに、使用中のPostScriptプリンタ用のPPDファイルを/usr/share/cups/model/へ直接コピーし(それらがまだmanufacturer-PPDsパッケージ内に存在していない場合)、使用中のプリンタに合わせて最適な設定を行うこともできます。

cupsパッケージ内のCUPS PPDファイル

cupsパッケージ内にある基本PPDファイルは、PostScript Level 1およびLevel 2プリンタに適応したFoomatic PPDファイルによって補足されます。

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

cups-driversパッケージ内のPPDファイル

通常、Foomaticプリンタフィルタのfoomatic-ripは、PostScript非対応プリンタ用のGhostscriptと組み合わせて使用されます。適切なFoomatic PPDファイルには、エントリ*NickName: ... Foomatic/Ghostscript driverおよび*cupsFilter: ... foomatic-ripがあります。これらのPPDファイルは、cups-driversパッケージ内にあります。

YaSTがFoomatic PPDファイルを採用するのは、Foomatic PPDファイルにエントリ*NickName: ... Foomatic ...(推奨)があり、そのファイルがプリンタモデルに一致し、manufacturer-PPDsパッケージにより適したPPDファイルが含まれない場合です。

cups-drivers-stpパッケージ内のGimp-Print PPDファイル

多くのPostScript非対応プリンタでは、foomatic-ripの代わりに、Gimp-Printから取得したCUPSフィルタrastertoprinterを使用できます。このフィルタと、適切なGimp-Print PPDファイルは、cups-drivers-stpパッケージ内に用意されています。Gimp-Print PPDファイルは/usr/share/cups/model/stp/内に配置されていて、そのファイル内にエントリ*NickName: ... CUPS+Gimp-Printおよび*cupsFilter: ... rastertoprinterが記述されています。

manufacturer-PPDsパッケージ内にあるプリンタメーカからのPPDファイル

manufacturer-PPDsパッケージには、十分自由なライセンスに基づいてプリンタメーカから提供されたPPDファイルが含まれています。PostScriptプリンタは、プリンタメーカの適切なPPDファイルを使用して設定するのが妥当です。このファイルを使用すると、そのPostScriptプリンタの機能すべてを活用できるためからです。YaSTは、次の各条件が満たされている場合、manufacturer-PPDsパッケージから得られたPPDファイルを優先します。

- ハードウェア検出の際に決定されたベンダおよびモデルが、manufacturer-PPDsパッケージから得られたPPDファイル内にあるベンダおよびモデルと一致しています。

- manufacturer-PPDsパッケージから得られたPPDファイルは、そのプリンタモデルに適した唯一のPPDファイルです。または、同じくそのプリンタモデルに一致する*NickName:... Foomatic/Postscript（推奨）エントリがあるFoomatic PPDファイルです。

したがって、YaSTは次のような状況では、manufacturer-PPDsパッケージから得られたどのPPDファイルも使用しません。

- manufacturer-PPDsパッケージから得られたPPDファイルが、プリンタのベンダおよびモデルに一致していません。これは、manufacturer-PPDsパッケージに同様のモデル用にPPDファイルが1つしかない場合、たとえば、一連のモデルの個々のモデルに別々のPPDファイルがないが、PPDファイル内にFunprinter 1000 seriesのような形式でモデル名が指定されている場合に発生します。

- Foomatic PostScript PPDファイルは、推奨されていません。プリンタモデルは、PostScriptモードでは十分効率よく動作しないことがあるからです(たとえば、メモリが少なすぎるためにこのモードではプリンタの信頼性が低い、またはプリンタ内蔵プロセッサの能力が低いために動作が遅すぎる、などです)。デフォルトでは、プリンタがPostScriptをサポートしていないこともあります。たとえば、PostScriptサポートがオプションのモジュールという形でしか使用できない場合などです。

manufacturer-PPDsパッケージから得られたPPDファイルが特定のPostScriptプリンタに適しているが、上記で説明された理由によってYaSTがそのファイ

ルを設定できない場合、YaST内で該当のプリンタモデルを手動で選択してください。

31.7 トラブルシューティング

ここでは、プリンタハードウェアおよびソフトウェアに最も一般的に発生する問題と、それを解決または回避する方法について説明します。

31.7.1 標準的なプリンタ言語をサポートしないプリンタ

一般的なプリンタ言語をどれもサポートせず、特殊な制御シーケンスのみに依存して動作するプリンタを、「*GDI プリンタ*」と呼びます。これらのプリンタは、メーカがドライバを添付した特定のバージョンのオペレーティングシステムでのみ動作します。*GDI*は、Microsoftがグラフィックデバイス用に開発したプログラミングインタフェースです。実質的な問題は、このプログラミングインタフェースではなく、GDIプリンタを制御できるのは、各プリンタモデルが採用している独自のプリンタ言語のみという事実にあります。

いくつかのプリンタは、GDIモードと標準的なプリンタ言語のいずれかの間で切り替えることができます。一部のメーカは、GDIプリンタに独自規格のドライバを提供しています。独自規格のプリンタドライバの欠点は、インストール済みの印刷システムとそのドライバを組み合わせたときに動作するという保証も、さまざまなハードウェアプラットフォームに適しているという保証もないことです。一方、標準的なプリンタ言語をサポートするプリンタは、特殊なバージョンの印刷システムや特殊なハードウェアプラットフォームに依存しません。

独自規格に対応するLinuxドライバを正常に機能させるために時間を費やすより、サポートされているプリンタを購入する方がコスト効率が良いこともあります。この方法により、ドライバの問題を一度だけで、そしてあらゆる状況で解決できます。特殊なドライバソフトウェアのインストールと設定を行う必要はなく、新しい印刷システムの開発に伴ってドライバのアップデートを入手する必要もありません。

31.7.2 特定のPostScriptプリンタに適したPPDファイルが入手できない

manufacturer-PPDsパッケージの中に、特定のPostScriptプリンタに適したPPDファイルが含まれていない場合、プリンタメーカ製のドライバCDに収録されているPPDファイルを使用すること、またはプリンタメーカのWebページから適切なPPDファイルをダウンロードすることができるはずです。

PPDファイルがzipアーカイブ(.zip)または自己展開zipアーカイブ(.exe)の形で提供されている場合、unzipを使用してそのファイルを展開します。最初に、PPDファイルのライセンス(許諾契約)条項を読みます。次に、cupstestppdユーティリティを使用して、そのPPDファイルが「Adobe PostScript Printer Description File Format Specification, version 4.3」(Adobe PostScriptプリンタ記述ファイルフォーマット仕様、バージョン4.3)に準拠しているかどうかを確認します。このユーティリティが「FAIL」を返した場合、PPDファイル内のエラーは重大なものであり、おそらく大きな問題を引き起こすと考えられます。cupstestppdによって報告された問題点は、取り除く必要があります。必要に応じて、適切なPPDファイルが入手できるかどうかをプリンタメーカに問い合わせることも考えられます。

31.7.3 パラレルポート

最も安全なアプローチは、プリンタを最初のパラレルポートに直接接続し、BIOS内で次のパラレルポート設定値を選択することです。

- I/O address (I/O アドレス):378 (16進)
- Interrupt (割り込み):無関係
- Mode (モード):Normal (通常)、SPP、またはOutput Only (出力専用)
- DMA:disabled (無効)

これらの設定値を使用した場合でも、パラレルポートに接続したプリンタを使用できない場合、BIOS内での設定値に合わせて、I/Oアドレスを0x378という形で/etc/modprobe.conf内に明示的に入力します。2つのパラレルポー

トが存在し、それぞれのI/Oアドレスが378と278 (16進)に設定されている場合、それらを0x378,0x278という形で入力します。

割り込み(IRQ) 7が空いている場合、例 31.1. 「/etc/modprobe.conf:最初のパラレルポート用の割り込みモード」 (page 531)に示すエントリを使用して、その割り込みを有効にすることもできます。割り込みモードを有効にする前に、/proc/interruptsファイルを参照して、すでに使用中の割り込みを調べます。現時点で使用中の割り込みだけが表示されます。どのハードウェアコンポーネントがアクティブになっているかに応じて、この表示は変化することがあります。パラレルポート用の割り込みは、他のどのデバイスも使用してはなりません。自信がない場合、irq=noneを指定してポーリングモードを使用します。

例 31.1　/etc/modprobe.conf:最初のパラレルポート用の割り込みモード

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

31.7.4　ネットワークプリンタ接続

ネットワークの問題の識別
プリンタをコンピュータに直接接続します。テストの目的で、そのプリンタをローカルプリンタとして設定します。この方法で動作する場合、問題はネットワークに関連しています。

TCP/IPネットワークのチェック
TCP/IPネットワークと名前解決が正しく機能していることが必要です。

リモートlpdのチェック
次のコマンドを使用して、*host*上のlpd (ポート515)に対するTCP接続を確立できるかどうかをテストします。

```
netcat –z host 515 && echo ok || echo failed
```

lpdへの接続を確立できない場合、lpdがアクティブになっていないか、ネットワークの基本的な問題があります。

rootユーザで次のコマンドを使用し、リモート*host*上の*queue*に関するステータスレポート(おそらく、非常に長い)を照会することもできます。

これは、該当のlpdがアクティブで、そのホストが照会を受け付けることを前提にしています。

```
echo -e "\004queue" \
  | netcat -w 2 -p 722 host 515
```

lpdが応答しない場合、それがアクティブになっていないか、ネットワークの基本的な問題が発生している可能性があります。lpdが応答する場合、その応答は、host上にあるqueueを介して印刷ができない理由を示すはずです。例 31.2.「lpdからのエラーメッセージ」 (page 532)のような応答を受け取った場合、問題はリモートのlpdにあります。

例 31.2 *lpdからのエラーメッセージ*

```
lpd: ホストにラインプリンタへのアクセス権lpdがない。
キューにプリンタが存在しない。
スプーリングでプリンタが使用できない。
印刷が使用できな
```

リモートcupsdのチェック

デフォルトでは、CUPSネットワークサーバはUDPポート631を使用して、自らのキューを30秒ごとにブロードキャストします。したがって、次のコマンドを使用して、ネットワーク内にCUPSネットワークサーバが存在しているかどうかをテストすることができます。

```
netcat -u -l -p 631 & PID=$!  ; sleep 40 ; kill $PID
```

ブロードキャストを行っているCUPSネットワークサーバが存在している場合、出力は例 31.3.「CUPSネットワークサーバからのブロードキャスト」 (page 532)に示すようになります。

例 31.3 *CUPSネットワークサーバからのブロードキャスト*

```
ipp://host.domain:631/printers/queue
```

次のコマンドを使用して、*host*上のcupsd(ポート631)に対するTCP接続を確立できるかどうかをテストすることができます。

```
netcat -z host 631 && echo ok || echo failed
```

cupsdに対する接続を確立できない場合、cupsdがアクティブになっていないか、ネットワークの基本的な問題があります。lpstat -h host -l -tこのコマンドは、*host*上にあるすべてのキューに関するステータスレ

ポート(おそらく、非常に長い) を返します。これは、該当のcupsdがアクティブで、そのホストが照会を受け付けることを前提にしています。

次のコマンドを使用して、*host*上の*queue*が、1つのキャリッジリターン(CR、改行)文字からなる印刷ジョブを受け付けるかどうかをテストできます。何も印刷されないのが妥当です。おそらく、空白のページが排出されるはずです。

```
echo -en "\r" \
  | lp -d queue -h host
```

ネットワークプリンタまたは印刷サーバボックスのトラブルシューティング

印刷サーバボックス上のスプーラは時々、大量の印刷ジョブを処理する必要が生じた場合、問題を引き起こすことがあります。これは印刷サーバボックス内のスプーラに起因しているので、ほとんどの場合、管理者が実行できる対策はありません。 回避策として、印刷サーバボックス内のスプーラを使用することを避け、TCPソケットを使用して、印刷サーバボックスに接続されているプリンタに直接送信できます。項31.4.2.「ネットワークプリンタ」 (page 518)を参照してください。

この方法により、印刷サーバボックスは異なる形式のデータ転送(TCP/IPネットワークとローカルプリンタ接続)間の単純なコンバータになります。この方法を使用するには、印刷サーバボックス内にある、該当するTCPポートについて把握する必要があります。プリンタが印刷サーバボックスに接続されていて、電源がオンになっている場合、印刷サーバボックスの電源をオンにした後、しばらく経過した時点で、nmapパッケージのnmapユーティリティを使用することにより、このTCPポートを特定できます。たとえば、nmap *IP-address*は、印刷サーバボックスに関して次のような出力をすることがあります。

```
Port        State       Service
23/tcp      open        telnet
80/tcp      open        http
515/tcp     open        printer
631/tcp     open        cups
9100/tcp    open        jetdirect
```

この出力は、印刷サーバボックスに接続されているプリンタが、ポート9100上のTCPソケットを介して使用できることを示します。nmapはデフォルトでは、 /usr/share/nmap/nmap-services内でリストされている多数の一般的な既知のポートだけをチェックします。可能性のあるすべてのポートをチェックするには、nmap -p *from_port-to_port IP-address*コマンドを使用します。これは、

ある程度の時間を要することがあります。詳細については、man nmapを参照してください。

次のようなコマンドを入力します。

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

これは、このポートを通してプリンタを使用できるかどうかをテストするために、該当のポートへ文字列またはファイルを直接送信します。

31.7.5 エラーメッセージを生成しない異常なプリントアウト

印刷システムの観点では、CUPSバックエンドが受信側(プリンタ)へのデータ転送を完了した段階で、印刷ジョブは完了します。受信側でそれ以降の処理が失敗した場合(たとえば、プリンタがそのプリンタ固有のデータを印刷できない)、印刷システムはそのことを検出しません。プリンタがそのプリンタ固有のデータを印刷できない場合、そのプリンタにより適していると考えられる他のPPDファイルを選択します。

31.7.6 無効にされたキュー

受信側へのデータ転送が数回の試行後に完全に失敗した場合、usbやsocketなどのCUPSバックエンドは印刷システム(より正確にはcupsd)にエラーを報告します。データ転送が不可能であると報告する前に、バックエンドは、試行に意味があるかどうか、また何回の試行に意味があるかを判断します。それ以上の試行は無駄に終わる可能性があるので、cupsdは該当のキューへの印刷を無効にします。問題の原因を取り除いた後、システム管理者は/usr/bin/enableコマンドを使用して、印刷を再度有効にする必要があります。

31.7.7 CUPSの参照:印刷ジョブの削除

CUPSネットワークサーバが参照機能を使用して自らのキューをクライアントホストへブロードキャストし、クライアントホスト側で適切なローカルcupsdがアクティブになっている場合、クライアント側のcupsdはアプリケーショ

ンから印刷ジョブを受け付け、サーバ側のcupsdへそれらを転送します。cupsdが印刷ジョブを受け付けた段階で、そのジョブに新しいジョブ番号が割り当てられます。したがって、クライアントホスト上のジョブ番号は、サーバ上のジョブ番号とは異なっています。印刷ジョブは通常、即座に転送されるので、クライアントホスト上でジョブ番号を使用してそのジョブを削除することはできません。 クライアント側のcupsdは、サーバ側のcupsdへの転送が完了した段階で、その印刷ジョブは完了したと考えるからです。

サーバ上にある印刷ジョブを削除するには、`lpstat -h print-server -o`などのコマンドを使用してサーバ上でのジョブ番号を判断します。サーバがまだその印刷ジョブを完了していない(つまり、プリンタへ送信していない)ことが前提条件です。このジョブ番号を使用して、サーバ上にある印刷ジョブを削除できます。

```
cancel -h print-server queue-jobnnumber
```

31.7.8 異常な印刷ジョブとデータ転送エラー

印刷プロセスの実行中に、管理者がプリンタの電源をオフにして再度オンにした場合、またはコンピュータをシャットダウンしてリブートした場合、印刷ジョブはキュー内にとどまっていて、印刷が再開されます。異常な印刷ジョブは、cancelを使用してキューから削除する必要があります。

印刷ジョブが異常な場合、またはホストとプリンタの間で通信エラーが発生した場合、プリンタはデータを正しく処理できなくなるので、文字化けのような大量のページを印刷することがあります。この状態を処理するには、次の処理を実行します。

1. プリンタの動作を停止するために、インクジェットプリンタの場合、すべての用紙を取り除きます。 レーザープリンタの場合、用紙トレイを開けます。上位機種のプリンタでは、現在のプリントアウトをキャンセルするボタンを用意していることもあります。

2. この時点で、印刷ジョブはキューに残っている可能性があります。ジョブがキューから削除されるのは、ジョブ全体をプリンタへ送信した後に限られるからです。`lpstat -o` (または`lpstat -h` *`print-server`* `-o`)を使用して、どのキューが現在印刷に使用されているかをチェックします。`cancel` *`queue-jobnumber`* (または`cancel -h`

print-server queue-jobnumber)を使用して、該当の印刷ジョブを削除します。

3 印刷ジョブがすでにキューから削除されたにもかかわらず、一部のデータが依然として、プリンタへ送信され続けることもあります。CUPSバックエンドプロセスが、引き続き該当のキューを対象として動作しているかどうかをチェックし、その処理を終了します。たとえば、プリンタがパラレルポートに接続されている場合、`fuser -k /dev/lp0`コマンドを使用して、引き続きそのプリンタ(より正確に表現すると、パラレルポート)にアクセスしているすべてのプロセスを終了することができます。

4 ある程度の時間にわたって電源をオフにして、プリンタを完全にリセットします。その後、紙を元に戻し、プリンタの電源をオンにします。

31.7.9 CUPS印刷システムのデバッグ

CUPS印刷システムの問題を特定するために、次の一般的な処理を実行してください。

1 `/etc/cups/cupsd.conf`内に、`LogLevel debug`を設定します。

2 `cupsd`コマンドを停止します。

3 `/var/log/cups/error_log*`を削除して、大規模なログファイルから検索を行うことを避けます。

4 `cupsd`を起動します。

5 問題の原因となったアクションをもう一度実行します。

6 `/var/log/cups/error_log*`内のメッセージをチェックし、問題の原因を識別します。

31.7.10 関連資料

多くの具体的問題に対する解決策は、Support Database (サポートデータベース)にあります。プリンタに関する問題が発生した場合は、Support Database

(サポートデータベース)の記事「*Installing a Printer*」および「*Printer Configuration from SUSE Linux 9.2*」を参照してください。キーワード*printer*を使用して、これらの記事を検索できます。

32 ホットプラグシステム

ホットプラグシステムでコンピュータのほとんどのデバイスの初期化を管理します。ホットプラグシステムは、稼動中に取り付け/取り外しできるデバイスに使用されるだけでなく、システムのブート中に検出されるすべてのデバイスにも使用されます。また、sysfsファイルシステムやudev(章 33. *udevをもつ動的デバイスノード* (page 547)を参照)と密接に連携します。

カーネルのブートが完了するまでは、バスシステム、ブートディスク、およびキーボードのような絶対に必要なデバイスだけが初期化されます。カーネルは、検出されたすべてのデバイスのホットプラグイベントをトリガします。udevdデーモンはこれらのイベントをリスンしてudevを実行し、デバイスノードを作成してデバイスを設定します。旧式のISAカードなど、自動的に検出することができないデバイスの場合には、静的な設定が使用されます。

過去の少数の例外を除き、ほとんどのデバイスは、システムのブート時またはデバイスの接続時にアクセス可能になり次第、すぐに初期化されます。初期化中に、インタフェースはカーネルに登録されます。この登録によって、それぞれのインタフェースを自動的に設定させるためのホットプラグイベントがさらにトリガされます。

SUSE Linuxの以前のバージョンでは、デバイスを初期化する基礎として一連の静的な設定データが使用されていました。ホットプラグイベントは、エージェントと呼ばれる個別のスクリプトで処理されました。SUSE Linuxのこのリリースでは、 ホットプラグサブシステムがudevに統合され、以前のホットプラグエージェントの機能はudevルールによって提供されるようになりました。

ホットプラグサブシステムの一般設定は、/etc/sysconfig/hotplugに記述されています。すべての変数にはコメントが付いています。一般的なデバイス設定は、/etc/udev/rules.dで見つかった、一致するルールに基づいて行われます(章 33. *udevをもつ動的デバイスノード* (page 547)を参照)。特定のデバイスの設定ファイルは、/etc/sysconfig/hardware内に配置されます。以前のバージョンのSUSE Linuxで用いられていたホットプラグイベントコールバックについては、/proc/sys/kernel/hotplugは通常空白です。udevdはホットプラグメッセージをnetlinkソケットから受け取るからです。

32.1 デバイスとインタフェース

ホットプラグシステムでは、デバイスだけでなくインタフェースも設定します。デバイスは通常、バスに接続され、インタフェースで必要とされる機能を提供します。インタフェースは、デバイス全体、またはデバイスの特定のサブセットの、ユーザーから見える抽象化となっています。デバイスが正しく動作するためには、通常、カーネルモジュールの形式でのデバイスドライバを必要とします。加えて、ユーザにインタフェースを提供するために、より高いレベルの特定のドライバが必要になることもあります。ほとんどのインタフェースは、udevによって作成されたデバイスノードで表されます。全体的な概念を把握するには、デバイスとインタフェースを区別することが重要です。

sysfsファイルシステム内に入力されたデバイスは、/sys/devices内で見つかります。インタフェースは、/sys/classまたは/sys/blockの下に配置されています。sysfs内のすべてのインタフェースには、それぞれのデバイスへのリンクが必要です。ただし、このリンクを自動的に追加しないドライバもあります。該当するリンクがない場合は、このインタフェースがどのデバイスに属しているかが不明なので、適切な設定を検索することができません。

デバイスのアドレス指定には、デバイス記述が使用されます。これには、sysfs内のデバイスパス(/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0)、接続ポイントの記述(bus-pci-0000:02:00.0)、および個々のID(id-32311AE03FB82538)などがあります。従来、インタフェースは名前で処理されていました。こうした名前は既存のデバイスの単純な番号

を表しており、デバイスが追加または削除されると変更されることがありました。

関連デバイスの記述を使用してインタフェースをアドレス指定することもできます。通常、コンテキストは、記述がデバイス自体を指すのか、またはそのインタフェースを指すのかを示します。デバイス、インタフェース、および記述の標準的な例として、次のものを挙げることができます。

PCIネットワークカード

PCIバス(/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0またはbus-pci-0000:02:00.0)に接続され、ネットワークインタフェース(eth0、id-00:0d:60:7f:0b:22またはbus-pci-0000:02:00.0)を持つ1つのデバイス。ネットワークインタフェースはネットワークサービスに使用されるか、トンネルやVLANなど、インタフェースを持つ仮想ネットワークデバイスに接続されます。

PCI SCSIコントローラ

複数の物理インタフェースをバス(/sys/class/scsi_host/host1)の形式で使用可能にする1つのデバイス(/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0またはbus-scsi-1:0:0:0)。

SCSIハードディスク

複数のインタフェース(/sys/block/sda*)を使用する1つのデバイス(/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0またはbus-scsi-1:0:0:0)。

32.2 ホットプラグイベント

各デバイスと各インタフェースには、ホットプラグイベントが関連付けられていて、udevがそれらのイベントを処理します。ホットプラグイベントは、デバイスへのリンクの確立時または解除時、あるいはドライバによるインタフェースの登録時または削除時に、カーネルによりトリガされます。SUSE Linux 9.3以降は、udevdでホットプラグイベントが受信および処理されます。udevdがカーネルからnetlinkメッセージを直接リッスンするか、または/sbin/udevsendを/proc/sys/kernel/hotplugに指定する必要があります。udevdは、ルールのセットに従ってデバイスを設定します(章33. *udevをもつ動的デバイスノード* (page 547)を参照)。

32.3 ホットプラグデバイスの設定

ホットプラグエージェントは、SUSE Linux 10.0の時点で廃止されることになりました。すべてのデバイス設定は、すでにudevルールで行われることになっています。udevは、既存のカスタムエージェントを呼び出すための、互換性のあるルールを提供しています。しかし、カスタムエージェントをudevルールに変換することも考慮すべきです。

ホットプラグエージェントとは、イベントに対して適切なアクションを実行する実行可能なプログラムのことです。デバイスイベントのエージェントは、/etc/hotplug.d/イベント名および/etc/hotplug.d/defaultにあります。これらのディレクトリ内の、拡張子が.hotplugのすべてのプログラムは、アルファベット順に実行されます。

デバイス設定を行うには、通常、カーネルモジュールをロードすれば十分です。適切なデバイス設定を行うために、付加的なコマンドを呼び出すことが必要な場合もあります。 SUSE Linuxでは、これは一般的にudevルールによって処理されます。しかし、カスタムデバイスの設定が必要な場合には、デバイス設定は/sbin/hwupまたは/sbin/hwdownによって行われます。これらのプログラムは、デバイスに適した設定をディレクトリ/etc/sysconfig/hardware内で検索して適用します。たとえば、特定のデバイスが初期化されないようにするには、適切な名前で設定ファイルを作成して、実行モードをmanualまたはoffにします。 /sbin/hwupは何も設定を見つけられなかった場合、MODALIASという環境変数を探します。存在すれば、modprobeは自動的に対応するモジュールをロードします。MODALIAS変数は、モジュールのロードが必要なデバイスのカーネルホットプラグイベントによって、自動的に生成されます。詳細については、項32.4.「自動的なモジュール読み込み」(page 544)を参照してください。 /sbin/hwupの詳細については、/usr/share/doc/packages/sysconfig/README ファイルおよびマニュアルページ(man hwup)を参照してください。

インタフェースエージェントが呼び出される前に、通常は、udevでシステムがアクセスできるデバイスノードが生成されます。udevを使用すると、インタフェースに永続的な名前を割り当てることができます。詳細については、章 33. *udevをもつ動的デバイスノード*(page 547)を参照してください。インタフェース自体は、その後に、対応するudevルールに従ってセットアップされます。ここでは、一部のインタフェースに関する手順を説明します。

32.3.1 ネットワークインタフェースの有効化

/sbin/ifupを使用してネットワークインタフェースを初期化し、/sbin/ifdownを使用して無効にします。詳細については、ファイル/usr/share/doc/packages/sysconfig/README およびifupのmanページを参照してください。

異なるドライバを使用する複数のネットワークデバイスがコンピュータに存在する場合、別のドライバを読み込む方が高速であれば、システムのブート中にインタフェース指定を変更できます。SUSE Linuxは、番号付けがなるべく変更されないようにします。デバイスは、設定時に割り当てられたインタフェース名を保ちます。この割り当てはudevルールによって行われます。後で割り当てを変更するには、udevルールを変更する必要があります。

ただし、最善の解決策は永続的なインタフェース指定を活用することです。設定ファイルで個々のインタフェースの名前を指定できます。この方法の詳細については、/usr/share/doc/packages/sysconfig/README を参照してください。SUSE Linux 9.3以降、デバイスノードではありませんが、ネットワークインタフェースもudevで処理されます。このため、より標準化された方法で永続的なインタフェース名を使用できます。

32.3.2 ストレージデバイスの有効化

ストレージデバイスにアクセスするには、そのインタフェースをマウントする必要があります。この作業は、完全に自動化するか事前に設定できます。さらに、SUSE Linuxはシステムデバイスとユーザデバイスを区別します。システムデバイスは、/etc/fstabにエントリを作成することによる、自動的なマウントだけが可能です。ユーザデバイスは、デフォルトではhalによって処理されます。ユーザデバイスで別な設定が必要な場合には、これらのデバイスを/etc/fstabに加えることができます。. または、このデバイスのhalでの処理を変更することができます。halについての詳細は、/usr/share/doc/packages/hal/hal-spec.html を参照してください。

永続的なデバイス名を使用することをお勧めします。この理由は、初期化シーケンスによっては従来のデバイス名が変更される場合があるためです。永続

的なデバイス名の詳細については、章 33. *udevをもつ動的デバイスノード* (page 547)を参照してください。

32.4 自動的なモジュール読み込み

/sbin/hwupが設定ファイルを検出するのに失敗すると、modprobeが、環境変数MODALIASの内容に基づいて、対応するモジュールを検索します。この環境変数は、カーネルが、対応するホットプラグイベントに対して生成します。カーネルの標準ドライバ以外のドライバを使用するには、/etc/sysconfig/hardware内に適切なハードウェア設定ファイルを作成してください。

32.5 ブートスクリプトcoldplug

boot.coldplugは、ブート時に設定されなかったデバイスの初期化を行います。単に、/etc/sysconfig/hardware/hwcfg-static-*として指定されているスタティックなデバイス設定ごとにhwupを呼び出します。この後で、/lib/klibc/eventsに記録されているすべてのイベントを再生して、すべてのデバイスを初期化します。

32.6 エラーの解析

32.6.1 ログファイル

特に指定がない限り、hotplugは少数の重要なメッセージをsyslogに送信します。詳細情報を取得するには、/etc/sysconfig/hotplugファイル内で変数HOTPLUG_DEBUGをyesに設定します。この変数をmaxという値に設定した場合、あらゆるホットプラグスクリプトに関して、すべてのシェルコマンドがログに記録されます。これは、syslogによるすべてのメッセージの格納先となる/var/log/messagesが非常に大きくなることを意味します。しかし、hotplugとcoldplugが終了した後、ブートプロセスの最中にsyslogが起動されるため、最初のメッセージはログに記録されない場合があります。

それらのメッセージが重要な場合、HOTPLUG_SYSLOG変数を通して他のログファイルを指定します。このトピックに関する情報は、/etc/sysconfig/hotplug内に記載されています。

32.6.2 ブートの問題

コンピュータがブートプロセスの最中にハングする場合、ブートプロンプトでNOHOTPLUG=yesまたはNOCOLDPLUG=yesと入力し、hotplugまたはcoldplugを無効にします。hotplugが無効になると、カーネルはホットプラグイベントを発行しません。稼働中のシステムでは、コマンド/etc/init.d/boot.hotplug startを入力してホットプラグを有効にすることができます。その時点までに生成されたイベントはすべて発行され、処理されます。キューにあるイベントを拒否するには、まず/proc/sys/kernel/hotplugに/bin/trueと入力し、後でこのエントリを/sbin/hotplugにリセットします。coldplugが無効になると、スタティックな設定は適用されません。スタティックな設定を適用するには、後で/etc/init.d/boot.coldplug startを入力します。

hotplugによってロードされた特定のモジュールがこの問題に関係しているかどうかを調べるには、ブートプロンプトでHOTPLUG_TRACE=<N>と入力します。読み込むすべてのモジュールの名前が画面に表示され、*N*秒後に実際に読み込まれます。この動作の進行中は、介入(操作)ができません。

32.6.3 イベントレコーダ

udevルールにより、イベントごとにスクリプト/sbin/hotplugeventrecorderが実行されます。/eventsディレクトリが存在している場合、すべてのホットプラグイベントは個別のファイルとしてこのディレクトリ内に格納されます。これにより、テストのためにイベントを再生できます。このディレクトリが存在しなければ、何も記録されません。

33 udevをもつ動的デバイスノード

Linuxカーネル2.6は、動的デバイスのディレクトリ/devに対して、新しいユーザ空間ソリューションを導入し、持続的なデバイス指定を実現しました。udevがこれに該当します。これは、実際に存在するデバイスにのみファイルを提供します。通常、/devディレクトリに存在するデバイスノードファイルを作成または削除し、ネットワークインタフェースの名前を変更することができます。devfsによる動的な/devの以前の実装は機能しなくなり、udevへ置き換えられました。

従来は、デバイスノードはLinuxシステム上の/devディレクトリ内に格納されていました。システム内に実際に存在しているかどうかにかかわりなく、使用可能なすべてのデバイスタイプに対して1つのノードが存在していました。その結果、このディレクトリには何千もの使用されていないファイルが含まれていました。新しく追加したサブシステムやカーネルデバイスを利用する前に、対応するノードを、特別なアプリケーションで作成する必要がありました。devfsファイルは大きな改善をもたらしました。実際に存在するものとしてカーネルに通知されたでばいすだけが、/dev内のデバイスノードを与えられたからです。

udevは、デバイスノードを作成する新しい方法を採用しました。カーネルはその内部状態をsysfsにエクスポートし、デバイスがカーネルによって認識されるたびに、sysfs内の情報を更新して、ユーザスペースにイベントを送信します。情報がsysfsによって利用可能になると、udevは簡単なルール構文と、適用されたデバイス属性とのマッチングを行い、対応するデバイスノードの作成または削除を行います。

ユーザは、新しいデバイスのためのudevルールを作成する必要はありません。あるデバイスが接続された場合、適切なデバイスノードが自動的に作成されます。しかし、ルールは、ノードの名前を定義するためのポリシーを導入します。これは、あいまいなデバイス名を覚えやすい名前へ置き換える規則を提供し、また、同じタイプのデバイスが同時に2台接続された状況で、持続するデバイス名を実現します。

仮に、高画質なカラーレーザプリンタと、白黒のインクジェットプリンタの2台のプリンタを持っていて、どちらもUSBに接続されているとしましょう。これらは/dev/usb/lpXのようになります。ここでXは、接続の順序に応じた番号です。udevを使い、カスタムのudevルールを作成すれば、一方のプリンタに/dev/colorlaserという名前を付け、もう一方に/dev/inkprinterという名前を付けることができます。これらのデバイスノードは、デバイスの特性に基づいてudevにより作成されたものなので、接続の順序やステータスにはかかわりなく、常に正しいデバイスを指します。

33.1 ルールの作成

udevは、/devの下にデバイスノードを作成する前に、/etc/udev/rules.d内で拡張子.rulesをもつすべてのファイルをアルファベット順に読み取ります。デバイスに当てはまる最初のルールが使用されます。たとえ、他のルールも当てはまる場合であってもです。コメントを記述するには、行頭にシャープ記号(#)を入力します。ルールは、次の形式を使用します。

```
key, [key,...]NAME [, SYMLINK]
```

少なくとも1つのキーを指定する必要があります。これらのキーに基づいて、ルールがデバイスに対して割り当てられるからです。また、名前を指定することも重要です。この名前は、/dev内で作成されるデバイスノードに使用されます。オプションのsymlinkパラメータを使用すると、他の場所にノードを作成できます。プリンタに関するルールは、次の形式を使用します。

```
BUS=="usb", SYSFS{serial}=="12345", NAME="lp_hp", SYMLINK+="printers/hp"
```

この例では、BUSとSYSFS{serial}という2つのキーがあります。udevは、シリアル番号をUSBバスに接続されたデバイスのシリアル番号と比較します。名前lp_hpを/devディレクトリ内のデバイスに割り当てるには、すべてのキーが同じである必要があります。さらに、このデバイスノードを参照する、シンボリックリンク/dev/printers/hpも作成されます。この操作を実行し

ている間に、printersディレクトリが自動的に作成されます。その後、印刷ジョブは/dev/printers/hpまたは/dev/lp_hpへ送信できます。

33.2 プレースホルダの置き換え

NAMEおよびSYMLINKのパラメータを使えば、プレースホルダを使用して、特別な値に置き換えることができます。簡単な例を使用して、この手順を説明します。

```
BUS=="usb", SYSFS{vendor}=="abc", SYSFS{model}=="xyz", NAME="camera%n"
```

名前の一部として使用されている演算子%nは、カメラデバイスの番号へ置き換えられます。たとえば、camera0やcamera1のようになります。役に立つもう1つの演算子は、%kです。これは、カーネルが保持している標準的なデバイス名へ置き換えられます。たとえば、hda1のようになります。udevルール内で外部プログラムを呼び出し、NAMEおよびSYMLINK値に返される文字列を使用することもできます。可能なプレースホルダについての詳細なリストは、udev manページに記されています。

33.3 キーのパターンマッチング

udevルールのキーでは、ワイルドカードとして知られるシェルスタイルのパターンマッチングを使用できます。たとえば、*字は任意の複数文字を表すプレースホルダ、?は任意の1文字を表すプレースホルダとして使用できます。

```
KERNEL="ts*", NAME="input/%k"
```

このルールは、文字「ts」で始まる指定を持つデバイスに対して、標準的なディレクトリ内でカーネルが使用する標準的な名前を割り当てます。udevルールの中でパターンマッチングを使用する方法についての詳細は、udevのmanページを参照してください。

33.4 キーの選択

デバイスを一意に識別し、複数のデバイスを相互に区別するためには、使用するudevルールでの一意なプロパティが重要となります。ここでは、標準的なキーに関するいくつかの例を示します。

SUBSYSTEM
デバイスが属しているサブシステム

BUS
デバイスのバスタイプ

KERNEL
カーネルが使用するデバイス名

ID
バスのデバイス番号(たとえば、PCIバスのID)

SYSFS{...}
ラベル、ベンダー、またはシリアル番号のような、sysfsのデバイス属性

SUBSYSTEMとIDの各キーは役に立つこともありますが、通常はBUS、KERNEL、およびSYSFS{...}の各キーが使用されています。udevの設定は、外部スクリプトを呼び出してその結果を評価するためのキーも用意しています。詳細は、udevのmanページを参照してください。

ファイルシステムsysfsは、ハードウェアについての情報をディレクトリツリーとして公開しています。一般的に、各ファイルにはデバイス名、メーカ、シリアル番号など、ただ1項目の情報が含まれます。これらの各ファイルは、キーとマッチングするために用いられます。しかし、1つのルールで複数のSYSFSキーを使用する場合、同じディレクトリの中にあるファイルだけがキー値として使用できます。有効で一意なキー値を見つけるには、ツールudevinfoが役に立ちます。

該当のデバイスを参照していて、devファイルが含まれている/sysの1つのサブディレクトリを見つける必要があります。これらのディレクトリはいずれも、/sys/blockまたは/sys/classの下に配置されています。デバイスにデバイスノードがすでに存在している場合は、udevinfoが正しいサブディレクトリを見つけられます。udevinfo -q path -n /dev/sdaコマンド

は、/block/sdaという出力をします。これは、必要とするディレクトリが/sys/block/sdaであることを意味します。今度は、コマンドudevinfo -a -p /sys/block/sdaを使用して、udevinfoを呼び出します。これら2つのコマンドを組み合わせて、たとえばudevinfo -a -p `udevinfo -q path -n /dev/sda`のようにすることもできます。次に、出力の一部を抜粋します。

```
BUS=="scsi"
ID=="0:0:0:0"
SYSFS{detach_state}=="0"
SYSFS{type}=="0"
SYSFS{max_sectors}=="240"
SYSFS{device_blocked}=="0"
SYSFS{queue_depth}=="1"
SYSFS{scsi_level}=="3"
SYSFS{vendor}==" "
SYSFS{model}=="USB 2.0M DSC"
SYSFS{rev}=="1.00"
SYSFS{online}=="1"
```

出力情報から、変化しない適切なキーを探します。1つのルール内では、他のディレクトリにあるキーを使用できないことに注意してください。

33.5 大容量ストレージデバイスの持続的な名前

SUSE Linuxには、初期化の順序に関係なく、ハードディスクと他のストレージデバイスに同じ指定を割り当てられるようにする定義済みのルールが装備されています。ハードウェアのシリアル番号、UUID、またはファイルシステムのラベルなどの一意なデバイス属性は、udevに付属する小さなヘルパープログラムで読み出すことができます。このヘルパープログラムは、udevのルール処理で利用可能な、固有のデバイス情報を作成します。次の簡単な例では、最初のルールは、udev環境内のSCSIデバイスから集められた値をインポートします。2番目のルールは、インポートした値を用いて、永続的なシンボリックリンクを作成します。

```
KERNEL="sd*[!0-9]", IMPORT="/sbin/scsi_id -g -x -s $p -d %N"
KERNEL="sd*[!0-9]", SYMLINK+="$env{ID_TYPE}/by-id/$env{ID_BUS}-$env{ID_SERIAL}"
```

大容量ストレージデバイス用のドライバは、ロードされた直後に、使用可能なハードディスクすべてをカーネルに登録します。各ハードディスクはホッ

トプラグブロックイベントをトリガし、各イベントはudevを呼び出します。次にudevはルールを読み取って、symlink(シンボリックリンク)を作成する必要があるかどうかを判断します。

initrdをとおしてドライバをロードした場合、ホットプラグイベントは失われます。しかし、すべての情報はsysfs内に格納されます。udevstartユーティリティは、/sys/blockおよび/sys/classの下にあるすべてのデバイスファイルを見つけ、udevを起動します。

ブートプロセスの間にすべてのデバイスノードを再作成する開始スクリプトboot.udevも存在します。しかし、開始スクリプトは、YaSTのランレベルエディタ、またはinsserv boot.udevコマンドを使用してアクティブにする必要があります。

34 Linuxのファイルシステム

Linuxは、互いに異なる多数のファイルシステムをサポートしています。この章では、非常に一般的なLinuxファイルシステムの短い概要を紹介し、それらの設計の概念、利点、および適用分野について説明します。Linux環境でのLFS (Large File Support、大規模ファイルのサポート)に関する詳細情報も説明します。

34.1 用語

メタデータ(metadata)
ファイルシステムの内部にあるデータ構造で、ディスク上にあるすべてのデータが適切に編成され、アクセス可能であることを保証します。本質的には、「データに関するデータ」です。ほぼすべてのファイルシステムが、メタデータからなる独自の構造を採用していますが、各ファイルシステムが互いに異なるパフォーマンス特性を示すのは、それが1つの理由になっています。メタデータが破損しないよう維持するのは、非常に重要なことです。もし破損した場合、ファイルシステム内にあるすべてのデータがアクセス不能になる可能性があるからです。

inode
inodeには、ファイルに関するさまざまな情報、たとえばサイズ、リンクの数、作成された日時、変更された日時、アクセスされた日時、およびファイルの内容を実際に格納しているディスクブロックへのポインタなどが記録されています。

ジャーナル(journal)
ファイルシステムの用語では、ジャーナルとはディスク上に存在する構造であり、ファイルシステムのメタデータに対して加えられた変更を記録するためにファイルシステムが格納するさまざまなログを保持しています。ジャーナル機能は、Linuxシステムの回復時間を大幅に短縮します。システム起動時に、ファイルシステム全体をチェックする冗長な検索プロセスを不要にするからです。ただし、それはジャーナルが再現できる場合に限定されます。

34.2 Linuxの主要なファイルシステム

2、3年前とは異なり、Linuxシステムで使用するファイルシステムを選択するのは、数秒で済む問題(Ext2とReiserFSのどちらにするか)ではありません。カーネル2.4およびそれ以降では、さまざまなファイルシステムが選択できるようになりました。この後で、各ファイルシステムの基本的な動作原理、およびそれらが提供する利点の概要について説明します。

あらゆる用途で最適な単一のファイルシステムなど存在しない、ということを考慮しておくことが重要です。各ファイルシステムには特定の利点と欠点があり、それらを考慮する必要があります。最も洗練されたファイルシステムであっても、妥当なバックアップの方針を何か他の機能で置き換えることはできません。

この章で「*データの完全性*」および「*データの一貫性*」という用語が登場した場合、それらはユーザスペースのデータ(アプリケーションが自らのファイルに書き込むデータ)の一貫性を指していません(メタデータの一貫性を指します)。ユーザスペースのデータが一貫しているかどうかは、アプリケーション自体が管理する必要があります。

重要項目: ファイルシステムのセットアップ

この章では特に注記がない限り、パーティションやファイルシステムのセットアップまたは変更するために必要なステップすべては、のモジュールを使用して実行できます。

34.2.1 ReiserFS

ReiserFSは、公式にはカーネル2.4リリース時の主要な機能の1つですが、SUSE Linuxバージョン6.4以降で、ReiserFSは2.2.x SUSEカーネルに対するカーネルパッチとして使用可能でした。ReiserFSは、Hans Reiser(ハンス・ライザー)とNamesys社の開発チームによって設計されました。ReiserFSは、古いExt2に代わる強力な選択肢であることを実証してきました。その主要な利点は、より良いディスクスペース使用効率、より良いディスクアクセスパフォーマンス、およびより高速なクラッシュ回復機能です。

ReiserFSの利点をより詳細に記述すると、以下のようになります。

より良いディスクスペース使用効率
ReiserFSでは、すべてのデータは、B*-Tree(バランスドツリー)と呼ばれる構造内で編成されています。このツリー構造は、より良いディスクスペース使用効率に貢献しています。小さなファイルは、B*-Treeのリーフノードに直接格納されるからです。そのようなファイルをどこか他の場所に格納して、ディスク上の実際の場所を指すポインタを維持するより優れています。それに加えて、ストレージ(記憶領域)は1KBまたは4KBのチャンク単位で割り当てられるのではなく、実際に必要なサイズの構成部分(エクステント)を割り当てられます。もう1つの利点は、inodeの動的割り当てに関係しています。これは、ファイルシステムの作成時にinodeの密度を指定する必要のある、Ext2のような従来のファイルシステムに比べて、ファイルシステムの柔軟性を高めます。

より良いディスクアクセスパフォーマンス
小規模なファイルでは、多くの場合、ファイルのデータと「stat_data」(inode)情報が互いに隣り合って保存されます。これらは1回のディスクI/O操作で読み取れるので、ただ1回のディスクアクセスで、必要な情報すべてを取得できることを意味します。

高速なクラッシュ回復機能
ジャーナルを使用して、メタデータに加えられた最新の変更結果を記録しているので、ファイルシステムが大規模な場合を含め、ファイルシステムを数秒でチェックできます。

データジャーナリングによる信頼性
ReiserFSは、Ext3のセクション項34.2.3. 「Ext3」 (page 557)で説明した概念に類似したデータジャーナリングおよび順序データモードをサポートしています。デフォルトのモードは、`data=ordered`です。このモードでは、

データとメタデータの完全性は保証されますが、メタデータのジャーナリングだけが行われます。

34.2.2 Ext2

Ext2の起源は、Linuxの歴史の初期にさかのぼります。その前身であったExtended File Systemは、1992年4月に実装され、Linux 0.96cに統合されました。Extended File Systemは多くの変更を加えられ、Ext2として数年にわたって、最も人気のあるLinuxファイルシステムになりました。その後、他のジャーナルファイルシステムが作成され、非常に短い回復時間を達成したため、Ext2の重要性は低下しました。

Ext2の利点に関する短い要約を読むと、かつて幅広く好まれ、そして今でも一部の分野で多くのLinuxユーザから好まれるLinuxファイルシステムである理由を理解するのに役立ちます。

堅牢性

「古くからある標準」として、Ext2は過去に多くの改良を受け、集中的にテストされてきました。このような理由で、多くの人はExt2を岩のように堅牢(rock-solid)と呼びます。ファイルシステムが正常にアンマウントできず、システムが機能停止した場合、e2fsckはファイルシステムのデータの分析を開始します。メタデータは一貫した状態に戻り、保留されていたファイルとデータブロックは、指定のディレクトリ(`lost+found`という名前)に書き込まれます。ジャーナルファイルシステムとは対照的に、e2fsckは、最近変更されたわずかなメタデータだけではなく、ファイルシステム全体を分析します。この結果、ジャーナルファイルシステムがログデータだけをチェックするのに比べて、かなり長い時間を要します。ファイルシステムのサイズにもよりますが、この手順は30分またはそれ以上を要することがあります。したがって、高可用性を必要とするどのようなサーバでも、Ext2を選択することは望ましくありません。ただし、Ext2はジャーナルを維持せず、非常にわずかなメモリを使用するだけなので、時には他のファイルシステムより高速なことがあります。

容易なアップグレード性

Ext2のコードは、Ext3が次世代ファイルシステムであることを明確に主張するための強力な土台になりました。Ext2の信頼性および堅牢性が、ジャーナルファイルシステムの利点と見事に融合されました。

34.2.3 Ext3

Ext3は、Stephen Tweedieによって設計されました。他のすべての次世代ファイルシステムとは異なり、Ext3は完全に新しい設計理念に基づいているわけではありません。Ext3は、Ext2をベースとしています。これら2つのファイルシステムは、互いに非常に似通っています。Ext3ファイルシステムを、Ext2ファイルシステムの上に構築することも容易です。Ext2とExt3の間にある最も重要な違いは、Ext3がジャーナルをサポートしていることです。要約すると、Ext3には、次の3つの主要な利点があります。

Ext2からの容易で信頼性の高いアップグレード

Ext3はExt2のコードをベースとし、ディスクフォーマットとメタデータフォーマットが共通しているので、Ext2からExt3へのアップグレードは非常に容易です。ReiserFS、JFS、またはXFSのような他のファイルシステムへの移行はかなり手間がかかります(ファイルシステム全体のバックアップを作成し、移行先ファイルシステムを新規に作成する必要があります)が、それとは異なり、Ext3への移行は数分で完了します。ファイルシステム全体を新規に作成する作業は障害なしで完了するとは限りませんが、Ext3への移行にはそのような作業が伴わないので、非常に安全でもあります。ジャーナルファイルシステムへのアップグレードを待つ既存のExt2システムの数を考慮すると、多くのシステム管理者にとってExt3が重要な選択肢になっていることが容易に想像できるはずです。Ext3からExt2へのダウングレードも、アップグレードと同じほど容易です。Ext3ファイルシステムのアンマウントを正常に行い、Ext2ファイルシステムとして再マウントするだけです。

信頼性とパフォーマンス

他のジャーナルファイルシステムは、「メタデータのみ」のジャーナルアプローチに従っています。これは、使用中のメタデータは常に一貫した状態を維持されていますが、ファイルシステムのデータ自体に関しては同じことが自動的に保証されるわけではない、という意味です。Ext3は、メタデータとデータの両方に注意するよう設計されています。「注意」の度合いはカスタマイズできます。Ext3の`data=journal`モードを有効にした場合、最大の保護(データの完全性)を実現しますが、メタデータとデータの両方がジャーナル化されるので、システムの動作が遅くなります。比較的新しいアプローチは、`data=ordered`モードを使用することです。これは、データとメタデータ両方の完全性を保証しますが、ジャーナルを適用するのはメタデータのみです。ファイルシステムドライバは、1つのメタデータの更新に対応するすべてのデータブロックを収集します。これらの

ブロックは、メタデータの更新前にディスクに書き込まれます。その結果、パフォーマンスを犠牲にすることなく、メタデータとデータの両方に関する一貫性を達成できます。3番目のオプションは、data=writebackを使用することです。これは、対応するメタデータをジャーナルにコミットした後で、データをメインファイルシステムに書き込むことを可能にします。多くの場合、このオプションは、パフォーマンスの点で最善と考えられています。しかし、内部のファイルシステムの完全性が維持される一方で、クラッシュと回復を実施した後では、古いデータがファイル内に再登場することを許してしまう可能性があります。管理者が他のオプションを指定しない限り、Ext3はデフォルトでdata=orderedを使用して動作します。

34.2.4 Ext2ファイルシステムからExt3への変換

Ext2からExt3への変換には、2つの個別のステップが関係しています。

ジャーナルの作成

rootとしてログインし、tune2fs -jを実行します。この結果、デフォルトのパラメータを使用してExt3ジャーナルが作成されます。ジャーナルの大きさや、どのデバイスにジャーナルを配置するかを自分で決定するには、代わりにtune2fs -Jを実行し、希望のジャーナルオプションであるsize=およびdevice=を指定します。tune2fsプログラムの詳細については、そのmanページ(tune2fs(8))を参照してください。

/etc/fstab内でのファイルシステムタイプの指定

Ext3ファイルシステムがExt3として正しく認識されることを保証するために、/etc/fstabファイルを編集し、対応するパーティションに対して指定されているファイルシステムタイプをext2からext3に変更します。この変更結果は、次回の再起動後に有効になります。

ルートディレクトリとしてのExt3の使用

Ext3パーティションとしてセットアップされたファイルシステムからブートするには、ext3とjbdの各モジュールをinitrd内に含めます。この作業を行うには、/etc/sysconfig/kernelファイルを編集し、INITRD_MODULESの下でこれら2つのモジュールを記述し、mk_initrdコマンドを実行します。

34.2.5 Reiser4

カーネル2.6のリリース直後に、ジャーナリングファイルシステムのファミリには、もう1つのメンバーReiser4が追加されました。Reiser4は、基本的にその前任のReiserFS(バージョン3.6)と異なります。Reiser4により、ファイルシステム機能を調整するためのプラグインの概念、およびきめ細かなセキュリティの概念が導入されます。

きめ細かなセキュリティの概念
Reiser4を設計する際に、開発者は、セキュリティ関連機能の実装に重点を置きました。したがって、Reiser4には、専用のセキュリティプラグインセットが付属しています。最も重要なプラグインには、ファイル「項目」の概念が導入されています。現在、ファイルアクセス制御はファイル単位に定義されています。複数のユーザ、グループ、またはアプリケーションに関連する情報を格納している大きなファイルがある場合、すべての関係者を含めるには、アクセス権が不明確でした。Reiser4では、そのような大きいファイルをより小さい部分(「項目」)に分割できます。次に、項目ごとおよびユーザごとにアクセス権を個別に設定できるため、ファイルのセキュリティをはるかに正確に管理できます。ちょうどいい例は、`/etc/passwd`です。今のところ、`root`だけはファイルを読み取りおよび編集できますが、`root`以外のユーザはこのファイルに読み取り専用でしかアクセスできません。Reiser4の項目の概念を取り入れると、このファイルを複数の項目(ユーザにつき1項目)に分割できるため、ユーザやアプリケーションがそれぞれのデータを変更できます。ただし、他のユーザのデータにはアクセスできません。この概念では、セキュリティと柔軟性のどちらも付加されます。

プラグインによる拡張性
ファイルシステムで通常使用される多くのファイルシステム関数と外部関数は、Reiser4ではプラグインとして実装されます。このようなプラグインは、ベースシステムに簡単に追加できます。そのため、ファイルシステムに新しい機能を追加するために、カーネルを再コンパイルしたり、ハードディスクを再フォーマットしたりする必要はなくなりました。

遅延アロケーションによる優れたファイルシステムレイアウト
XFSと同様に、Reiser4では遅延アロケーションをサポートしています。項34.2.7.「XFS」 (page 560)を参照してください。メタデータにも遅延アロケーションを使用すれば、レイアウト全体がさらに優れたものになる可能性があります。

34.2.6 JFS

JFSは、*Journaling File System*(ジャーナルファイルシステム)の略で、IBMが開発したものです。 Linuxに移植されたJFSの最初のベータ版は、2000年夏にLinuxコミュニティに対して提供されました。 バージョン1.0.0は、2001年にリリースされました。 JFSは、パフォーマンスを最重要な目標とする高スループットサーバ環境のニーズを満たすようカスタマイズされています。完全64ビットファイルシステムとして、JFSは大規模なファイルと大規模なパーティションの両方をサポートしています。これは、JFSがサーバ環境で使用されるもう1つの理由です。

JFSを詳細に観察すると、このファイルシステムがLinuxサーバにとって適切な選択肢になる理由を知ることができます。

効率的なジャーナル処理
: JFSは、「メタデータのみ」のアプローチに従っています。包括的なチェックではなく、ファイルシステムに関する最近の操作によって発生したメタデータのみの変更結果をチェックしますが、それは回復時の時間を大幅に節約します。並列操作は、複数の並列ログエントリを必要としますが、それらの操作は結合されて1つのグループコミットになり、複数の書き込み操作に伴うファイルシステムのパフォーマンス低下を大幅に低減します。

効率的なディレクトリ編成
: JFSは、2つの異なるディレクトリ編成を採用しています。小規模なディレクトリに対しては、ディレクトリの内容をinodeに直接格納することを許可します。大規模なディレクトリに対しては、B^+-Treeを使用し、優れたディレクトリ管理を行います。

inodeの動的割り当てによるより良いスペース使用効率
: Ext2の場合、inodeの密度(管理情報が占有するスペース)を事前に定義する必要があります。これは、ファイルシステムに記録できるファイルまたはディレクトリの最大数を限定します。JFSは、このような事前の考慮を不要にします。JFSはinodeのスペースを動的に割り当て、必要がなくなった場合はそれらを解放します。

34.2.7 XFS

本来は、IRIX OS用のファイルシステムを意図してSGIがXFSの開発を開始したのは、1990年代初期です。XFSの背後にある考えは、ハイパフォーマンス

の64ビットジャーナルファイルシステムを作成し、非常に要求の多い今日のコンピューティングの課題を満たすことです。XFSは大規模なファイルを操作する点で非常に優れていて、ハイエンドのハードウェアを適切に活用します。しかし、XFSには1つの欠点があります。ReiserFSと同様、XFSはメタデータの完全性には最大の注意を払いますが、データの完全性にはそれほど注意を払いません。

XFSの主要な機能を簡単に観察することにより、ハイエンドのコンピューティング分野で、XFSが他のジャーナルファイルシステムの強力な競合相手という立場を実証している理由を説明できます。

アロケーショングループの採用による高いスケーラビリティ

XFSファイルシステムの作成時に、ファイルシステムの基にあるブロックデバイスは、等しいサイズを持つ8つ以上の線形の領域に分割されます。これらをアロケーショングループと呼びます。各アロケーショングループは、独自のinodeと空きディスクスペースを管理します。実用的には、アロケーショングループを、1つのファイルシステムの中にある複数のファイルシステムと見なすこともできます。アロケーショングループは互いに独立しているのではなく、カーネルから複数を同時にアドレス指定できる、という特徴があります。この特徴は、XFSの高いスケーラビリティの鍵です。独立性の高いアロケーショングループは、性質上、マルチプロセッサシステムのニーズに適しています。

ディスクスペースの効率的な管理によるハイパフォーマンス

空きスペースとinodeは、各アロケーショングループ内のB^+-Treeによって処理されます。B^+-Treeの採用は、XFSのパフォーマンスとスケーラビリティに大きく貢献しています。XFSでは、*遅延アロケーション*を採用しています。XFSはアロケーション(割り当て)を2つのパートに分割して、この操作を処理します。保留されているトランザクションはRAMの中に保存され、適切な量のスペースが確保されます。XFSはこの時点では、データの格納場所(言い換えると、ファイルシステムのどのブロックか)を決定しません。決定可能な最後の瞬間まで、この決定は遅延(先送り)されます。短時間だけ存続する一部の一時データは、ディスクに書き込まれません。XFSがデータの実際の保存場所を決定する時点で、それらのデータは不要になっているからです。したがって、XFSは書き込みのパフォーマンスを向上させ、ファイルシステムの断片化(フラグメンテーション)を減らします。遅延アロケーションは、他のファイルシステムより書き込みイベントの頻度を下げる結果をもたらすので、書き込み中にクラッシュが発生した場合、データ損失が深刻になる可能性が高くなります。

事前割り当てによるファイルシステムの断片化の回避
: データをファイルシステムに書き込む前に、XFSはファイルが必要とする空きスペースを*予約*(プリアロケート、事前割り当て)します。したがって、ファイルシステムの断片化は大幅に減少します。ファイルの内容がファイルシステム全体に分散することがないので、パフォーマンスが向上します。

34.3 サポートされている他のいくつかのファイルシステム

表 34.1.「Linux環境でのファイルシステムのタイプ」 (page 562)は、Linuxがサポートしている他のいくつかのファイルシステムを要約したものです。これらは主に、他の種類のメディアや外部オペレーティングシステムとの互換性およびデータの相互交換を保証することを目的としてサポートされています。

表 34.1 *Linux環境でのファイルシステムのタイプ*

`cramfs`	*Compressed ROM file system* (圧縮ROMファイルシステム): ROM用に圧縮された読み込み専用ファイルシステムです。
`hpfs`	*High Performance File System* (ハイパフォーマンスファイルシステム): IBM OS/2の標準ファイルシステムです。読み取り専用モードでサポートされています。
`iso9660`	CD-ROMの標準ファイルシステム。
`minix`	このファイルシステムは、オペレーティングシステムに関する学術的なプロジェクトを起源とするもので、Linuxで最初に使用されたファイルシステムです。現在では、フロッピーディスク用のファイルシステムとして使用されています。
`msdos`	*fat*、つまり当初はDOSで使用されていたファイルシステムであり、現在はさまざまなオペレーティングシステムで使用されています。

`ncpfs`	Novellのボリュームをネットワーク経由でマウントするためのファイルシステム。
`nfs`	*Network File System* (ネットワークファイルシステム): この場合、ネットワーク内にある任意のコンピュータにデータを格納でき、ネットワーク経由でアクセスを許可できるファイルシステムを指します。
`smbfs`	*Server Message Block* (サーバメッセージブロック): Windowsのような製品が、ネットワーク経由でのファイルアクセスを可能にする目的で採用しています。
`sysv`	SCO UNIX、Xenix、およびCoherent (PC用の商用UNIXシステム)が採用。
`ufs`	BSD、SunOS、およびNeXTstepが採用。読み取り専用モードでサポートされています。
`umsdos`	*UNIX on MSDOS* (MSDOS上のUNIX): 通常の`fat`ファイルシステムに対して適用されるもので、特別なファイルを作成することにより、UNIXの機能(パーミッション、リンク、長いファイル名)を実現します。
`vfat`	*Virtual FAT* (仮想FAT): `fat`ファイルシステムを拡張したものです(長いファイル名をサポートします)。
`ntfs`	*Windows NT file system* (Windows NTファイルシステム)、読み取り専用です。

34.4 Linux環境での大規模ファイルサポート

当初、Linuxは最大2GBのファイルサイズをサポートしていました。マルチメディアが爆発的に普及する前、およびLinux環境で大規模データベースを運用することを誰も試みていないうちは、これで十分でした。サーバコンピューティングの重要性がますます高くなるにつれて、カーネルとCライブラリが変

更され、2GBを超えるファイルサイズをサポートするようになりました。 現在、ほぼすべてのファイルシステムはLFS (Large File Support、大規模ファイルサポート)に対応しているので、管理者やユーザはハイエンドのコンピューティングを実現できます。 表 34.2.「ファイルシステムの最大サイズ(ディスクフォーマット時)」 (page 564)は、Linuxのファイルとファイルシステムに関する現在の制限の概要を示しています。

表 34.2　ファイルシステムの最大サイズ(ディスクフォーマット時)

ファイルシステム	ファイルサイズ(バイト)	ファイルシステムのサイズ(バイト)
Ext2またはExt3 (ブロックサイズ1KB)	2^{34} (16GB)	2^{41} (2TB)
Ext2またはExt3 (ブロックサイズ2KB)	2^{38} (256GB)	2^{43} (8TB)
Ext2またはExt3 (ブロックサイズ4KB)	2^{41} (2TB)	2^{44} (16TB)
Ext2またはExt3 (ブロックサイズ8KB) (Alphaのような8KBページ採用のシステム)	2^{46} (64TB)	2^{45} (32TB)
ReiserFS v3	2^{46} (64GB)	2^{45} (32TB)
XFS	2^{63} (8EB)	2^{63} (8EB)
JFS (ブロックサイズ512バイト)	2^{63} (8EB)	2^{49} (512TB)
JFS (ブロックサイズ4Kバイト)	2^{63} (8EB)	2^{52} (4PB)
NFSv2 (クライアント側)	2^{31} (2GB)	2^{63} (8EB)
NFSv3 (クライアント側)	2^{63} (8EB)	2^{63} (8EB)

重要項目: Linuxカーネルの制限

表 34.2. 「ファイルシステムの最大サイズ(ディスクフォーマット時)」 (page 564)は、ディスクフォーマット時の制限について記載しています。カーネル2.6は、自らが取り扱うファイルとファイルシステムのサイズについて、独自の制限を課しています。それらは、次のとおりです。

ファイルのサイズ
32ビットシステムでは、ファイルは2TB (2^{41}バイト)のサイズを上回ることができません。

ファイルシステムのサイズ
ファイルシステムは最大2^{73}バイトの大きさまでサポートします。しかし、この制限は、現在使用可能なハードウェアが到達可能な範囲を上回っています。

34.5 関連資料

ここまでに説明した各ファイルシステムのプロジェクトには、独自のWebページがあります。そこで詳しいドキュメントとFAQ、さらにメーリングリストを参照することができます。

- http://e2fsprogs.sourceforge.net/
- http://www.zipworld.com.au/~akpm/linux/ext3/
- http://www.namesys.com/
- http://oss.software.ibm.com/developerworks/opensource/jfs/
- http://oss.sgi.com/projects/xfs/

Linuxのファイルシステムに関する包括的で複数のパートからなるチュートリアルは、*IBM developerWorks*のWebページhttp://www-106.ibm.com/developerworks/library/l-fs.htmlから入手できます。Linux環境のさまざまなジャーナルファイルシステムに関する比較は、Juan I. Santos Floridoによる*Linuxgazette*http://www-106.ibm.com/developerworks/library/

*l-fs.html*の*Web*ページを参照してください。Linux環境のLFSに関する興味深い詳しい分析については、Andreas JaegerによるLFS in Linuxサイト http://www.suse.de/~aj/linux_lfs.html を参照してください。 http://www.suse.de/~aj/linux_lfs.html.

X Windowシステム

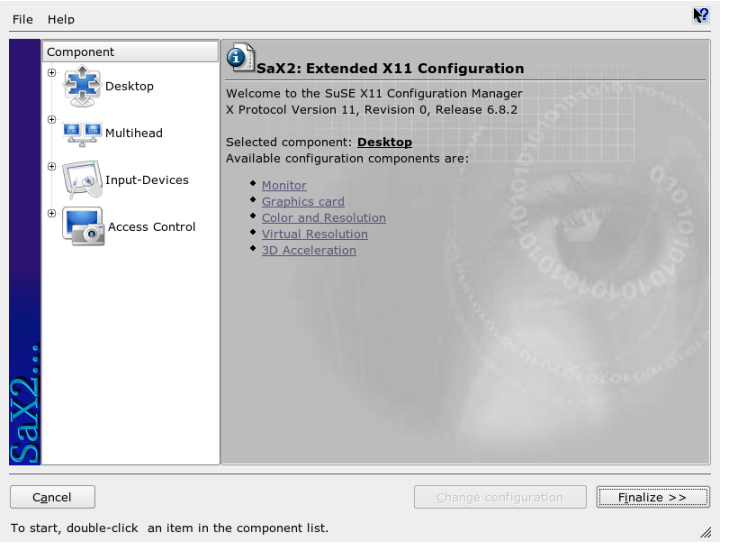
35

X Window System (X11)は、UNIX系のグラフィカルユーザインタフェースで、事実上の標準となっています。Xはネットワークベースであり、あるホスト上で起動されたアプリケーションを、任意のネットワーク(LANやインターネット)を介して接続されている他のホスト上で表示できるようにします。この章では、X Window System環境の設定と最適化、SUSE Linuxでのフォントの使用についての背景情報、およびOpenGLと3Dの設定について説明します。

35.1 SaX2によるX11の設定

グラフィカルユーザインタフェースまたはXサーバによって、ハードウェアとソフトウェアの間の通信が処理されます。KDEやGNOMEなどのデスクトップと、多様なウィンドウマネージャで、ユーザとの対話にXサーバが使用されています。グラフィカルユーザインタフェースは、最初はインストール中に設定されます。設定をあとから変更するには、YaSTコントロールセンターから対応するモジュールを使用するか、コマンドラインから、`sax2`というコマンドを実行して、SaX2を手動で起動します。SaX2のメインウィンドウは、YaSTコントロールセンターから個々のモジュールを一般的に包括するものとして利用されます。

図 35.1　SaX2のメインウィンドウ



左のナビゲーションバーには6つのアイテムがあります。それぞれのアイテムは、YaSTコントロールセンターのそれぞれの設定ダイアログを表示しています。以下の章 *YaST*でのシステム設定(↑起動)の中で言及されているセクションを探してください。

モニタのモデル
モニタおよびグラフィックカード設定の説明については、項「カードおよびモニタのプロパティ」 (章 3. *YaST*でのシステム設定, ↑起動)を参照してください。

マウス
グラフィック環境におけるマウス設定の説明については、項「マウスのプロパティ」 (章 3. *YaST*でのシステム設定, ↑起動)を参照してください。

キーボード
グラフィック環境におけるキーボード設定の説明については、項 「キーボードのプロパティ」 (章 3. *YaST*でのシステム設定, ↑起動)を参照してください。

タブレット
グラフィックタブレット設定の説明については、項「タブレットのプロパティ」 (章 3. *YaST*でのシステム設定, ↑起動)を参照してください。

タッチスクリーン
タッチスクリーン設定の説明については、項「タッチスクリーンのプロパティ」 (章 3. *YaST*でのシステム設定, ↑起動)を参照してください。

VNC
VNC設定の説明については、項 「リモートアクセスのプロパティ」 (章 3. *YaST*でのシステム設定, ↑起動)を参照してください。

35.2 X設定の最適化

X.Orgは、X Window Systemのオープンソース実装です。X Window Systemの新規テクノロジおよび標準の開発にも責任を負っているX.Org Foundationにより、さらに開発が続けられています。

マウス、グラフィックカード、モニタ、キーボードなど、使用可能なハードウェアを最適の方法で使用するために、設定を手動で最適化することができます。ここでは、この最適化の一部の側面について説明します。X Window Systemの設定の詳細については、ディレクトリ `/usr/share/doc/packages/Xorg`にある各種ファイルと`man xorg.conf`のマニュアルページを参照してください。

警告

X Window Systemの設定は慎重に行う必要があります。設定が完了するまでは、X Window Systemを起動しないでください。システムが正しく設定されていないと、ハードウェアが復元不能な損傷を受ける可能性があります(特に固定周波数モニタの場合)。本書およびSUSE Linuxの作成者は、損傷に責任を負うことはできません。この情報は慎重に調査されたものですが、ここで説明する方法がすべて正しく、ハードウェアが損傷を受けないという保証はありません。

プログラムSaX2およびxorgconfigは、デフォルトで`/etc/X11`にファイル`xorg.conf`を作成します。これはX Window Systemの基本設定ファイルです。この

ファイルには、グラフィックカード、マウス、およびモニタに関する設定がすべて含まれています。

ここでは、設定ファイル /etc /X11 /xorg. confの構造について説明します。xorg.confは複数のセクションで構成され、各セクションは設定の特定の側面を取り扱います。各セクションは、キーワードSection <designation>で始まってキーワードEndSectionで終わります。 セクションの形式は次のようなものです。

```
Section designation
  entry 1
  entry 2
  entry n
EndSection
```

使用可能なセクションのタイプのリストは表 35.1. 「/etc/X11/xorg.confのセクション」 (page 570)にあります。

表 35.1 *　/etc/X11/xorg.confのセクション*

タイプ	意味
Files	ここではフォントおよびRGBカラーテーブルに使用されるパスを記述します。
ServerFlags	一般スイッチはここに設定します。
InputDevice	キーボードや特殊入力デバイス(タッチパッド、ジョイスティックなど)といった入力デバイスを設定します。このセクションで重要なパラメータはDriverと、ProtocolおよびDeviceを定義するオプションです。
モニタのモデル	使用するモニタを記述します。このセクションの要素は、後でScreenの定義で参照する名称、bandwidth、および同期周波数の制限(HorizSyncおよびVertRefresh)です。設定値はMHz、kHz、およびHz単位です。通常、サーバはモニタ仕様に対応しないmodelineを拒否します。このため、意図せずに高すぎる周波数がモニタに送信されるのを防止できます。

タイプ	意味
Modes	特定の画面解像度に関するmodelineパラメータが格納されます。これらのパラメータは、ユーザ指定の値に基づいてSaX2で計算でき、通常は変更不要です。固定周波数モニタに接続する場合などは、この時点で手動で介入します。個々の数値の意味の詳細については、HOWTOファイル /usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gzを参照してください。
Device	特定のグラフィックカードを定義します。グラフィックカードは記述名で参照されます。
Screen	このセクションは、MonitorおよびDeviceを使用して、X.Orgに必要なすべての設定を指定します。Displayサブセクションでは、仮想画面(Virtual)のサイズ、ViewPort、およびこの画面で使用するModesを指定します
ServerLayout	シングルヘッド設定またはマルチヘッド設定のレイアウトを定義します。このセクションにより、入力デバイスInputDeviceと表示デバイスScreenがバインドされます。

ここでは、Monitor、Device、およびScreenについて詳しく説明します。他のセクションの詳細については、X.Orgおよびxorg.confのマニュアルページを参照してください。

xorg.confには、複数の異なるMonitorおよびDeviceセクションを記述できます。複数のScreenセクションを記述することも可能です。次のServerLayoutセクションでは、どれを使用するかが決定されます。

35.2.1 Screenセクション

最初に、Screenセクションを調べます。このセクションでは、Monitorセクションと Deviceセクションを組み合わせて、どの解像度とカラー設定を使用する

かを決定します。Screenセクションは例 35.1. 「ファイル/etc/X11/xorg.confのScreenセクション」 (page 572)のようになります。

例 35.1 *ファイル/etc/X11/xorg.confのScreenセクション*

```
Section "Screen"
  DefaultDepth  16
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

Identifier行(ここではScreen[0])では、このセクションに以降のServerLayoutセクションで一意に参照できる定義済みの名前を割り当てています。Device行とMonitor行では、この定義に属しているグラフィックカードとモニタを指定しています。これらは、対応する名前または*識別子*を持つDeviceおよびMonitorセクションにリンクされます。これらのセクションの詳細については、以下を参照してください。

DefaultDepth設定を使用して、特定のカラー設定で起動されない場合にサーバで使用するカラー設定を選択します。各カラー設定ごとにDisplayサブセクションがあります。キーワードDepthで、このサブセクションに有効なカラー設定を割り当てます。Depthに有効な値は8、15、16、および24です。必ずしもすべてのXサーバモジュールがこれらの値をすべてサポートしているわけではありません。

Modesセクションでは、カラー設定に続いて解像度のリストを設定します。Xサーバは、このリストを左から右に検査します。解像度ごとに、Xサーバは

Modesセクション内で適切なModelineを検索します。Modelineは、モニタとグラフィックカード両方の機能に応じて異なります。Monitor設定により、Modelineが決まります。

最初に検出される解像度はDefault modeです。Ctrl + Alt + + (数字パッド上)を使用すると、リスト内で右隣の解像度に切り替えることができます。左隣に切り替えるには、Ctrl + Alt + − (数字パッド上)を使用します。これにより、Xの実行中に解像度を変更できます。

Depth 16が指定されているDisplayサブセクションの最終行は、仮想画面のサイズを指します。仮想画面の最大許容サイズは、モニタの最大解像度ではなく、グラフィックカードにインストールされているメモリの容量と必要なカラー設定に応じて異なります。最近のグラフィックカードはビデオメモリ容量が大きくなってきているため、きわめて大型の仮想デスクトップを作成できます。ただし、ビデオメモリのほとんどが仮想デスクトップを占めると、3D機能を使用できなくなる場合があります。たとえば、カードのビデオRAMが16 MBであれば、仮想画面には8ビットカラーで最大4096x4096ピクセルのサイズを設定できます。ただし、特にアクセラレータカードの場合は、仮想画面にメモリすべてを使用しないことをお勧めします。この種のカードのメモリは、複数のフォントやグラフィックキャッシュにも使用されるからです。

35.2.2 Deviceセクション

Deviceセクションでは、特定のグラフィックカードを記述します。名前が異なっていれば、キーワードIdentifierを使用してxorg.conf内で必要な数だけデバイスエントリを指定できます。原則として、複数のグラフィックカードがインストールされている場合は、各セクションは順に番号を付けられるだけです。最初のセクションはDevice[0]、2番目のセクションはDevice[1]となります。次のファイルは、Matrox Millennium PCIグラフィックカードが搭載されているコンピュータのDeviceセクションから抜粋したものです。

```
Section "Device"
  BoardName      "MGA2064W"
  BusID          "0:19:0"
  Driver         "mga"
  Identifier     "Device[0]"
  VendorName     "Matrox"
  Option         "sw_cursor"
EndSection
```

設定にSaX2を使用すると、Deviceセクションは上記の例のようになります。DriverおよびBusIDは、どちらもコンピュータにインストールされているハードウェアに応じて異なり、SaX2により自動的に検出されます。BusIDは、グラフィックカードがインストールされているPCIスロットまたはAGPスロットの定義です。これは、lspciコマンドで表示されるIDと一致します。Xサーバは10進形式による詳細を必要としますが、lspciではこれらが16進形式で表示されます。

介してドライバパラメータにより、このグラフィックカードに使用するドライバを指定します。カードがMatrox Millenniumである場合は、ドライバモジュールはmgaと呼ばれます。Xサーバは、driversサブディレクトリのFilesセクションで定義されているModulePathを検索します。標準インストールの場合、これはディレクトリ/usr/X11R6/lib/modules/driversです。名前には_drv.oが追加されるので、mgaドライバの場合は、ドライバファイルmga_drv.oがロードされます。

Xサーバやドライバの動作は、その他のオプションを使用して変更することもできます。その一例がDeviceセクションで設定するオプションsw_cursorです。このオプションは、ハードウェアのマウスカーソルを無効にし、ソフトウェアを使用してマウスカーソルを示します。ドライバモジュールによっては、さまざまなオプションを使用できます。各オプションは、ディレクトリ/usr/X11R6/lib/X11/doc内のドライバモジュール記述ファイル内にあります。通常、有効なオプションについてはマニュアルページ(man xorg.confおよびman X.Org)でも確認できます。

35.2.3 MonitorセクションとModesセクション

Deviceセクションと同様に、MonitorセクションとModesセクションでもモニタを1つずつ記述します。設定ファイル/etc/X11/xorg.confでは、Monitorセクションを必要な数だけ指定できます。サーバレイアウトセクションでは、どのMonitorセクションが関係するかを指定します。

熟練者以外は、モニタ定義を設定しないでください。modelineは、Monitorセクションで重要な役割を果たします。modelineでは、関連解像度の水平と垂直のタイミングを設定します。モニタ特性、特に許容周波数は、Monitorセクションに格納されます。

警告

モニタとグラフィックカードの機能を熟知していない場合は、モニタが深刻な損傷を受ける恐れがあるので、modelineを変更しないでください。

独自のモニタ記述を作成する場合は、`/usr/X11/lib/X11/doc`内のドキュメントを熟読する必要があります。ビデオモード関連のセクションには、特に注意する必要があります。ハードウェアの動作とmodelineの作成方法が詳しく記述されています。

modelineの手動指定が必要になることはほとんどありません。最新のマルチシンクモニタを使用している場合、許容周波数と最適解像度は、SaX2設定のセクションで説明したように、原則としてXサーバがDDCを介してモニタから直接読み込みます。何らかの原因で直接読み込めない場合は、Xサーバに付属するVESAモードの1つを使用してください。このモードは、実際にはグラフィックカードとモニタのすべての組み合わせに機能します。

35.3 フォントのインストールと設定

SUSE Linuxで追加のフォントをインストールするのは簡単です。フォントを、X 11フォントパスにある任意のディレクトリにコピーするだけです(項35.3.2.「X11コアフォント」 (page 580)を参照)。フォントを使用できるようにするには、インストール先ディレクトリが、`/etc/fonts/fonts.conf`に設定されているディレクトリのサブディレクトリでなければなりません(項35.3.1.「Xft」 (page 576)を参照)。

フォントファイルは、`/usr/X11R6/lib/X11/fonts/truetype`などの適切なディレクトリに(`root`ユーザで)手動でコピーできます。また、この作業は、KDEコントロールセンターでKDEフォントインストーラを使用して行うこともできます。結果は同じです。

フォントを実際にコピーする代わりに、シンボリックリンクを作成することもできます。たとえば、マウントされているWindowsパーティション上にライセンスを取得しているフォントがあり、それらのフォントを使用したい場合は、シンボリックリンクを作成します。次に、`SuSEconfig--module fonts`コマンドを実行します。

SuSEconfig--module fontsコマンドは、フォントを設定するスクリプト、/usr/sbin/fonts-configを実行します。このスクリプトが実行する事柄については、スプリプトのマニュアルページ(man fonts-config)を参照してください。

手順は、ビットマップフォント、TrueTypeフォントとOpenTypeフォント、およびType1 (PostScript)フォントの場合と同様です。これらのタイプのフォントはすべて、任意のディレクトリにインストールできます。CID-keyedフォントでは、若干異なる手順が必要です。詳細については、項35.3.3.「CID-Keyedフォント」 (page 581)を参照してください。

X.Orgには、完全に異なる2つのフォントシステムがあります。それは、古い*X11*コアフォントシステムと新しく設計された*Xft*および*fontconfig*システムです。以降のセクションでは、これらの2つのシステムについて簡単に説明します。

35.3.1 Xft

最初から、Xftのプログラマは、アンチエイリアスを含むスケーラブルフォントが適切にサポートされるようにしています。Xftが使用された場合、フォントは、X11コアフォントシステムにおけるXサーバではなく、そのフォントを使用するアプリケーションによってレンダリングされます。このようにすると、それぞれのアプリケーションは実際のフォントファイルにアクセスでき、グリフのレンダリング方法を完全に制御できます。これが、多数の言語においてテキストを正しく表示するための基本となっています。フォントファイルに直接アクセスできることは、印刷のためにフォントを組み込んで、画面出力と同じ印刷出力を得るのに役立ちます。

SUSE Linuxでは、2種類のデスクトップ環境KDEとGNOME、Mozilla、および他の多くのアプリケーションが、すでにXftをデフォルトで使用しています。そのため、Xftはすでに、古いX11コアフォントシステムよりも多くのアプリケーションで使用されています。

Xftは、fontconfigライブラリを使ってフォントを検索し、フォントのレンダリング方法を制御します。fontconfigのプロパティは、グローバルな設定ファイル/etc/fonts/fonts.confとユーザ固有の設定ファイル~/.fonts.confによって制御されます。これらのfontconfig設定ファイルはどちらも、以下の行で始まっていなければなりません。

```
<?xml version="1.0"?>
<! DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

さらに、以下の行で終っていなければなりません。

```
</fontconfig>
```

フォントを検索するためのディレクトリを追加するには、以下のような行を付加します。

```
<dir>/usr/local/share/fonts/</dir>
```

ただし、これは通常、必要ありません。デフォルトで、ユーザ固有のディレクトリ~/.fontsは、すでに/etc/fonts/fonts.confに入っています。その結果、追加のフォントをインストールするには、それらのフォントを~/.fontsにコピーするだけです。

また、フォントの見栄えを制御する規則を導入することもできます。例えば、次のように入力して、すべてのフォントについてアンチエイリアスを無効にします。

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

あるいは次のように入力します。

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

この場合、特定のフォントのアンチエイリアスが無効になります。

デフォルトで、ほとんどのアプリケーションは、フォント名のsans-serif(または等価のsans)、serif、あるいはmonospaceを使用します。これらは、実際のフォントではなく、言語設定に応じて適切なフォントに解決されるエイリアスにすぎません。

ユーザは、規則を~/.fonts.confファイルに追加して、それらのエイリアスを簡単に好みのフォントに変換できます。

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

ほとんどすべてのアプリケーションで、これらのエイリアスがデフォルトで使用されるので、システム全体が影響を受けます。そのため、個々のアプリケーションでフォント設定を変更しなくても、ほとんどどこででも好みのフォントを簡単に使用できます。

fc-listを使用して、どのフォントがインストールされており、使用可能になっているか調べます。たとえば、fc-listコマンドを実行すると、すべてのフォントのリストが表示されます。使用可能なスケーラブルフォント(:outline=true)の内、どのフォントがHebrew(:lang=he)に必要なすべてのグリフ、それらのフォント名(family)、それらのスタイル(style)、それらの幅(weight)、およびフォントを含むファイルの名前を含んでいるか調べるには、次のコマンドを入力します。

```
fc-list ":lang=he:outline=true" family style weight
```

上記のコマンドの出力は、以下のようになります。

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
```

```
FreeSans.ttf: FreeSans:style=Medium:weight=80
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

fc-listで調べることができる重要なパラメータ:

*表 **35.2*** *fc-listのパラメータ*

パラメータ	意味と有効な値
family	フォントファミリの名前。たとえば、FreeSans
foundry	フォントメーカ。たとえば、urw
style	フォントスタイル。たとえば、Medium、Regular、Bold、Italic、Heavy
lang	フォントがサポートする言語。例えば、ドイツ語にはde、日本語にはja、繁体字中国語にはzh-TW、簡体字中国語にはzh-CN
weight	フォント幅。たとえば、通常では80、ボールドでは200
slant	スラント。通常、なしでは0、イタリックでは100
file	フォントを含むファイルの名前
outline	アウトラインフォントではtrue、他のフォントではfalse
scalable	スケーラブルフォントではtrue、他のフォントではfalse
bitmap	ビットマップフォントではtrue、他のフォントではfalse

パラメータ	意味と有効な値
pixelsize	ピクセル単位でのフォントサイズ。fc-listとの関連で、このオプションはビットマップフォントでのみ有効

35.3.2 X11コアフォント

今日、X11コアフォントシステムは、ビットマップフォントだけでなく、Type1フォント、TrueTypeとOpenTypeフォント、CID-keyedフォントなどのスケーラブルフォントもサポートしています。Unicodeフォントもかなり前からサポートされています。X11 コアフォントシステムは1987年に、モノクロのビットマップフォントを処理する目的でX11 R1用に開発されました。上記で説明した拡張機能は、後から追加されたものです。

スケーラブルフォントは、アンチエイリアスとサブピクセルレンダリングなしでサポートされており、多数の言語用のグリフを持つ大きいスケーラブルフォントのロードには時間がかかります。Unicodeフォントを使用した場合にも時間がかかり、より多くのメモリが必要になります。

X11コアフォントシステムには、その他にも固有の弱点がいくつかあります。時代遅れになっており、これ以上拡張することはできません。下位互換性のために保持されていますが、可能なときはいつでも、新しいXftおよびfontconfigシステムを使用してください。

Xサーバは、操作のためにどのようなフォントが使用可能で、そのフォントがシステム内のどこにあるかを認識する必要があります。この情報は、有効なすべてのシステムフォントディレクトリへのパスを含むFontPath変数で処理されます。これらの各ディレクトリでは、ファイル`fonts.dir`にそのディレクトリ内で使用可能なフォントのリストがあります。FontPathは、起動時にXサーバにより生成されます。設定ファイル`/etc/X11/xorg.conf`の各`FontPath`エントリ内で、有効なファイル`fonts.dir`が検索されます。これらのエントリは、`Files`セクションにあります。実際のFontPathを表示するには、`xset q`を使用します。このパスは、xset を使用して実行時に変更することもできます。 パスを追加するには、`xset +fp <path>`を使用します。必要のないパスを削除するには、`xset -fp <path>`を使用します。

Xサーバがすでにアクティブである場合、マウントされたディレクトリに新たにインストールされたフォントは、コマンドxset fp rehashで使用可能にできます。このコマンドは、SuSEconfig --module fontsによって実行されます。コマンドxsetが実行中のXサーバにアクセスする必要がある場合、これは、SuSEconfig --module fontsが実行中のXサーバにアクセスできるシェルから起動されている場合にのみ可能です。これを行う最も簡単な方法は、suコマンドとrootパスワードを入力して、権限をrootにすることです。suは、Xサーバを起動したユーザのアクセス権をrootシェルに移します。フォントが正しくインストールされ、X11コアフォントシステムを介して使用可能かどうか検査するには、コマンドxlsfontsを使用して、すべての使用可能なフォントのリストを表示します。

デフォルトでは、SUSE LinuxはUTF-8ロケールを使用します。そのため、Unicodeフォントを使用するようにします(xlsfontsの出力中でiso10646-1で終了するフォント名)。使用可能なすべてのUnicodeフォントは、xlsfonts | grep iso10646-1コマンドでリストを表示できます。SUSE Linuxで使用可能なほとんどすべてのUnicodeフォントには、少なくともヨーロッパ言語に必要なグリフが含まれています(以前はiso-8859-*としてエンコードされていました)。

35.3.3 CID-Keyedフォント

他のフォントタイプとは異なり、CID-keyedフォントは任意のディレクトリに簡単にインストールすることはできません。CID-keyedフォントは、/usr/share/ghostscript/Resource/CIDFontディレクトリにインストールしなければなりません。これは、Xftおよびfontconfigとは関係ありませんが、GhostscriptとX11コアフォントシステムには必要です。

ティップ

X11で使用可能なフォントの詳細については、http://www.xfree86.org/current/fonts.htmlを参照してください。

35.4 OpenGL - 3D 設定

35.4.1 ハードウェアサポート

SUSE Linuxには、3Dハードウェアのサポート用に複数のOpenGLドライバが用意されています。表35.3.「サポートされている3Dハードウェア」 (page 582)で、概要を説明します。

表 35.3 サポートされている3Dハードウェア

OpenGLドライバ	サポートされているハードウェア
nVidia	nVidia Chips:all except Riva 128(ZX)
DRI	3Dfx Voodoo Banshee、 3Dfx Voodoo-3/4/5、 Intel i810/i815/i830M、 Intel 845G/852GM/855GM/865G/915、 Matrox G200/G400/G450/G550、 ATI Rage 128(Pro)/Radeon (9250まで)

初めてYaSTを使用してインストールしている場合には、インストール時にYaSTが3Dサポートを検出すると、3Dアクセラレーションをアクティブにすることができます。nVidiaグラフィックチップの場合は、nVidiaドライバを最初にインストールする必要があります。そのためには、YOU (Online Update)でnVidiaドライバパッチを選択します。ライセンス上の制限により、nVidiaドライバはディストリビューションには含まれていません。

新規インストールではなくアップデートを行う場合、または3Dfxアドオングラフィックアダプタ(Voodoo GraphicsまたはVoodoo-2)を設定する必要がある場合は、3Dハードウェアサポートの設定手順は異なります。手順は、使用するOpenGLドライバによって異なります。次のセクションでさらに詳しく説明します。

35.4.2 OpenGLドライバ

nVidiaとDRIのOpenGLドライバは、SaX2で簡単に設定できます。nVidiaアダプタの場合は、nVidiaドライバを最初にインストールする必要があります。コマンド`3Ddiag`を入力し、nVidiaまたはDRIの設定が正しいかどうか検査します。

セキュリティ上の理由から、グループ`video`に属しているユーザのみに、3Dハードウェアに対するアクセスが許可されています。そのため、すべてのローカルユーザを、このグループにメンバーとして所属させます。`video`グループに属していない場合は、OpenGLアプリケーションに対してOpenGLドライバの低速な*software rendering fallback (ソフトウェアレンダリング代替機能)*が使用されます。コマンド`id`を使用して、現在のユーザが`video`グループに属しているかどうか検査します。属していない場合は、を使用してそのユーザをグループに追加します。

35.4.3 診断ツール3Ddiag

診断ツール3Ddiagを使用すると、SUSE Linuxにおける3D設定を検証できます。3Ddiagは、ターミナルから起動する必要があるコマンドラインツールです。`3Ddiag -h`を入力すると、3Ddiagで使用可能なオプションをリストできます。

設定を検証するために、このツールで、3Dサポートに必要なパッケージがインストールされており、正しいOpenGLライブラリとGLX拡張機能が使用されているかどうかがチェックされます。エラーメッセージが表示された場合は、3Ddiagの指示に従います。すべての設定が正しければ、画面上に表示されるのは完了メッセージのみです。

35.4.4 OpenGLテストユーティリティ

OpenGLをテストするには、プログラム`glxgears`と、`tuxracer`および`armagetron`のようなゲーム(両者のパッケージ名は同じ)が役に立ちます。3Dサポートがアクティブになっている場合、比較的新しいコンピュータ上ではそれらのゲームをスムーズに実行できるはずです。3Dサポートがないと、それらのゲームは非常に遅くなります(コマ送り状態)。`glxinfo` コマンドを使用して、3D がアクティブであることを確認します。 アクティブであれば、`direct rendering: Yes`と表示されます。

35.4.5 トラブルシューティング

OpenGL 3Dのテスト結果が良くない場合(ゲームがスムーズに実行できない場合)は、3Ddiagを使用して、設定に(エラーメッセージ中に)エラーがないか確認します。エラーを訂正しても状況が変わらない場合、あるいは、エラーメッセージが表示されない場合は、のログファイルを参照してください。

多くの場合、のログファイル`/var/log/Xorg.0.log`の中に、`DRI is disabled`という行が見つかります。 正確な原因は、ログファイルを厳密に調べない限り見つかりません。この作業にはある程度の経験が必要になります。

この場合には、3Ddiagですでにエラーが検出されているため、設定エラーは存在しません。そのため、この時点での唯一の選択肢は、DRIドライバのsoftware rendering fallback (ソフトウェアレンダリング代替機能)を使用することです。これは、3Dハードウェアサポートを提供していません。OpenGLの表示エラーが発生したり、OpenGLが不安定な場合にも、3Dサポートを使用することはできません。SaX2を使用して、3Dサポートを完全に使用不可能にします。

35.4.6 インストールのサポート

DRIドライバの`software rendering fallback`(ソフトウェアレンダリング代替機能)を除き、Linuxにおけるすべての OpenGLドライバは開発段階にあり、実験段階のドライバであると見なす必要があります。Linux用の3Dハードウェアアクセラレーションに対する要望が多いため、このドライバは、ディストリビューションに含まれています。OpenGLドライバが実験的な段階にあることを考慮すると、は、3Dハードウェアアクセラレーションに関するインストールのサポートも提供できず、関連する問題に対する支援も行えません。グラフィカルユーザインタフェース(X Window System)の基本設定には、3Dハードウェアアクセラレーションの設定は含まれていません。3Dハードウェアアクセラレーションで問題が発生した場合は、3Dサポートを完全に使用不可にすることをお勧めします。

35.4.7 その他のオンラインドキュメント

DRIの詳細については、 /usr/X11R6/lib/X11/doc/README.DRI (xorg-x11-doc)を参照してください。nvidiaドライバインストールの詳細については、http://ftp.suse.com/pub/suse/i386/supplementary/X/nvidia-installer-HOWTO.htmlを参照してください。

36

PAMを使用した認証

Linuxは、ユーザとアプリケーションを仲介するレイヤとして認証プロセスでPAM (Pluggable Authentication Modules)を使用します。PAMモジュールはシステム単位で使用できるため、どのアプリケーションからもリクエストできます。この章では、モジュラー認証メカニズムの機能とその設定方法について説明します。

通常、システム管理者とプログラマは、システムの一定部分へのアクセスを制限することや、アプリケーションの一定の機能の使用を制限することを望みます。PAMを使用しなければ、新規の認証メカニズム(LDAPやSAMBAなど)が導入されるたびにアプリケーションを調整する必要があります。ただし、このプロセスには時間がかかり、ミスが発生する可能性があります。このような難点を回避する方法の1つは、アプリケーションを認証メカニズムから切り離し、残りは集中管理されるモジュールに任せることです。新しい認証方式が必要になった場合は、問題のプログラムで使用できるように適切なPAMモジュールを調整または記述するだけで済みます。

PAMメカニズムに依存するすべてのプログラムについて、ディレクトリ`/etc/pam.d/<programname>`に専用の設定ファイルがあります。これらのファイルでは、認証に使用するPAMモジュールが定義されます。また`/etc/security`にはほとんどのPAMモジュール用のグローバル設定ファイルがあり、これらのモジュール(`pam_env.conf`、`pam_pwcheck.conf`、`pam_unix2.conf`、`time.conf`など)の正確な動作が定義されます。PAMモジュールを使用する各アプリケーションは、実際には一連のPAM関数を呼び出し、各PAM関数は各種設定ファイルの情報を処理して、その結果を呼び出し元のアプリケーションに戻します。

36.1 PAM設定ファイルの構造

PAM設定ファイルの各行は、次のように最大4列で構成されています。

```
<Type of module> <Control flag> <Module path> <Options>
```

PAMモジュールはスタックとして処理されます。モジュールの用途はタイプごとに異なり、パスワードをチェックするモジュール、システムのアクセス元ロケーションを検証するモジュール、ユーザ固有の設定を読み込むモジュールなどがあります。PAMは、次の4タイプのモジュールを認識します。

auth
: このタイプのモジュールの目的は、ユーザの信憑性をチェックすることです。従来、このチェックのためにパスワードの問い合わせが行われていましたが、チップカードやバイオメトリクス(指紋や虹彩のスキャン)の助けを借りて行うこともできます。

account
: このタイプのモジュールは、ユーザがリクエストしたサービスを使用するための一般許可を付与されているかどうかをチェックします。たとえば、失効したアカウントのユーザ名では誰もログインできないようにするには、この種のチェックを実行する必要があります。

password
: このタイプのモジュールの目的は、認証トークンを変更可能にすることです。ほとんどの場合、このトークンはパスワードです。

セッション
: このタイプのモジュールは、ユーザセッションの管理と設定を受け持ちます。認証の前後に起動され、ログイン試行をシステムログに記録し、ユーザ固有の環境(メールアカウント、ホームディレクトリ、システム制限など)を設定します。

2列目には、起動されたモジュールの動作に影響する制御フラグが含まれています。

required
: このフラグが付いているモジュールは、認証を進める前に正常に処理される必要があります。`required`フラグが付いたモジュールが失敗した後、

同じフラグが付いた他のモジュールがすべて処理されてから、ユーザが認証試行の失敗メッセージを受け取ります。

requisite
このフラグが付いているモジュールも、requiredフラグが付いている場合とほぼ同様に、正常に処理される必要があります。ただし、このフラグが付いたモジュールが失敗した場合は、ユーザに即座にフィードバックが送られ、他のモジュールは処理されません。成功すると、requiredフラグが付いているモジュールの場合とほぼ同様に、続いて他のモジュールが処理されます。requisiteフラグは、正しい認証に不可欠な一定条件の有無をチェックするための基本フィルタとして使用できます。

sufficient
このフラグが付いたモジュールが正常に処理されると、呼び出し元アプリケーションは即時に成功メッセージを受け取り、前にrequiredフラグが付いたモジュールが失敗していなければ、他のモジュールは処理されません。sufficientフラグが付いたモジュールが失敗しても、直接的な結果は発生せず、以降のモジュールはそれぞれの順序で処理されます。

optional
このフラグが付いたモジュールが成功しても失敗しても、直接的な影響はありません。このフラグは、それ以上はアクションを実行しない、メッセージ表示(ユーザへのメール着信通知など)専用のモジュールに便利です。

include
このフラグが設定された場合、引数として指定されたファイルがこの場所に挿入されます。

モジュールがデフォルトディレクトリ/lib/securityにあれば、そのパスを明示的に指定する必要はありません(SUSE Linuxでサポートされるすべての64ビットプラットフォームの場合、このディレクトリは/lib64/securityです)。4列目には、debug(デバッグの有効化)やnullok(空のパスワードの使用を許可)など、対応するモジュール用のオプションが表示される場合があります。

36.2 sshdのPAM設定

PAMの裏付けとなっている理論の機能を示すために、実務的な例としてsshdのPAM設定を考えてみましょう。

例 36.1 sshdのPAM設定

```
#%PAM-1.0
auth     include        common-auth
auth     required       pam_nologin.so
account  include        common-account
password include        common-password
session  include        common-session
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
#session  optional      pam_resmgr.so fake_ttyname
```

アプリケーション(この場合sshd)の通常のPAM設定には、次に示す4つのモジュールタイプの設定ファイルを参照するinclude文が含まれます。common-auth、common-account、common-password、およびcommon-session。これら4つのファイルにはそれぞれのモジュールタイプ用のデフォルト設定があります。各PAMアプリケーションごとにそれぞれのモジュールを個別に呼び出す代わりとしてこれらを組み込むことで、管理者がデフォルトを変更した場合、更新されたPAM設定を自動的に取得します。これまでPAMへの変更があった場合、または新規アプリケーションをインストールした場合には、すべてのアプリケーションの全設定ファイルを手動で調整しなければなりませんでした。現在では、PAMの設定は中心となる設定ファイルで行われ、すべての変更は、各サービスのPAM設定に自動的に継承されます。

最初のincludeファイル(common-auth)はauthタイプの2つのモジュール、pam_envおよびpam_unix2を呼び出します。例 36.2.「authセクションのデフォルト設定」 (page 590)を参照してください。

例 36.2 authセクションのデフォルト設定

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

1つ目はpam_envで、ファイル/etc/security/pam_env.confをロードし、このファイルに指定されている環境変数を設定します。pam_envモジュールはログイン元ロケーションを認識するため、このファイルを使用するとDISPLAY変数を適切な値に設定できます。2つ目のpam_unix2は、ユーザの

ログインとパスワードを /etc /passwdおよび /etc /shadowと比較対照してチェックします。

common-authで指定されたモジュールが正常に呼び出された後、pam_nologinという3番目のモジュールがファイル /etc /nologinの存在する場所をチェックします。このファイルが存在する場合、root以外のユーザはログインできません。authモジュールのスタック全体が処理された後に、sshdがログインの成否に関するフィードバックを取得します。スタックの全モジュールにrequired制御フラグが付いている場合は、すべてが正常に処理されなければ、sshdには成功メッセージが送られません。モジュールが1つでも失敗すると、モジュールスタック全体が処理され、その後にのみsshdに失敗が通知されます。

authタイプのすべてのモジュールが正常に処理された時点で、別のinclude文が処理されます。この例では例 36.3.「accountセクションのデフォルト設定」 (page 591)になります。common-accountに含まれるモジュールはpam_unix2のみです。pam_unix2からユーザが存在するという結果が戻されると、sshdは成功したことを通知するメッセージを受信し、モジュールの次のスタック(password)が処理されます。この処理を例 36.4.「passwordセクションのデフォルト設定」 (page 591)に示します。

例 36.3 *accountセクションのデフォルト設定*

```
account required        pam_unix2.so
```

例 36.4 *passwordセクションのデフォルト設定*

```
password required       pam_pwcheck.so  nullok
password required       pam_unix2.so    nullok use_first_pass use_authtok
#password required      pam_make.so     /var/yp
```

繰り返しになりますが、sshdのPAM設定はcommon-passwordにあるpasswordモジュールのデフォルト設定を参照する1つのinclude文にのみ関係します。アプリケーションが認証トークンの変更をリクエストするたびに、これらのモジュールを正常に完了する必要があります。(制御フラグrequired)。パスワード変更や別の認証トークンについてはセキュリティチェックが必要です。これはpam_pwcheckモジュールで実現可能です。その後に使用されたpam_unix2モジュールがpam_pwcheckから新旧のパスワードを引き継ぐため、ユーザが再認証する必要はありません。また、これでpam_pwcheckによるチェックを回避することもできなくなります。accountまたはauthタイプの

モジュールが期限切れパスワードに関するメッセージを送るように設定されている場合は、passwordタイプのモジュールを使用する必要があります。

例 36.5　sessionセクションのデフォルト設定

```
session required        pam_limits.so
session required        pam_unix2.so
```

最終ステップとして、common-sessionに組み込まれたsessionタイプのモジュールが呼び出され、問題のユーザ用の設定に従ってセッションが設定されます。pam_unix2が再び処理されますが、このモジュール、pam_unix2.confが関連する設定ファイルにnoneオプションが指定されているため、実際の結果はありません。pam_limitsモジュールはファイル/etc/security/limits.confをロードします。このファイルでは、特定のシステムリソースの使用制限が定義されている場合があります。sessionモジュールはユーザのログアウト時に再び呼び出されます。

36.3　PAMモジュールの設定

PAMモジュールの一部は設定可能です。対応する設定ファイルは/etc/securityにあります。この項では、sshdの例(pam_unix2.conf、pam_env.conf、pam_pwcheck.confおよびlimits.conf)について簡単に説明します。

36.3.1　pam_unix2.conf

従来のパスワードベースの認証方式は、PAMモジュールpam_unix2によって制御されます。このモジュールは、必要なデータを/etc/passwd、/etc/shadow、NISマップ、NIS+テーブル、またはLDAPデータベースから読み込むことができます。このモジュールの動作は、アプリケーション自体のPAMオプションを設定して個別に変更するか、/etc/security/pam_unix2.confを編集してグローバルに変更できます。例 36.6.「pam_unix2.conf」(page 593)に、このモジュールの最も基本的な設定ファイルを示します。

例 36.6　pam_unix2.conf

```
auth:    nullok
account:
password:        nullok
session:         none
```

モジュールタイプauthおよびpasswordのnullokオプションは、対応するタイプのアカウントに空のパスワードを許可するように指定します。また、ユーザは自分のアカウントのパスワード変更を許可されます。モジュールタイプsessionのnoneオプションは、代わりにメッセージが記録されないように指定します(デフォルト)。その他の設定オプションの詳細については、ファイル自体のコメントまたはpam_unix2のマニュアルページを参照してください。

36.3.2　pam_env.conf

このファイルを使用すると、pam_envモジュールが呼び出されるたびに設定される、ユーザ用に標準化された環境を定義できます。それにより、次の構文を使用して環境変数を事前設定できます。

```
VARIABLE  [DEFAULT=[value]]  [OVERRIDE=[value]]
```

VARIABLE
　設定する環境変数の名前です。

[DEFAULT=[value]]
　管理者が設定するデフォルト値です。

[OVERRIDE=[value]]
　問い合わせ可能でpam_envによって設定される値です。この値でデフォルト値が上書きされます。

pam_envの典型的な使用例は、DISPLAY変数の取得です。これは、リモートログインが行われるたびに変更されます。このようすを例 36.7.「pam_env.conf」 (page 593)に示しています。

例 36.7　pam_env.conf

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

1行目では、REMOTEHOST変数の値がlocalhostに設定されており、pam_envが他の値を判別できない場合にこの値が使用されます。DISPLAY変数には、REMOTEHOSTの値が含まれています。ファイル/etc/security/pam_env.confでより詳細な情報を参照してください。

36.3.3 pam_pwcheck.conf

この設定ファイルから、pam_pwcheckモジュールがpasswordタイプの全モジュールのオプションを読み込みます。このファイルに格納されている設定は、個々のアプリケーションのPAM設定よりも優先されます。アプリケーション固有の設定が定義されていない場合、アプリケーションではグローバル設定が使用されます。例 36.8. 「pam_pwcheck.conf」 (page 594)はpam_pwcheckに対して空のパスワードとパスワード変更を許可するように指示しています。このモジュールの他のオプションについては、ファイル/etc/security/pam_pwcheck.confを参照してください。

例 36.8 pam_pwcheck.conf

```
password:    nullok
```

36.3.4 limits.conf

ファイルlimits.confでは、ユーザ別またはグループ別のシステム制限を設定できます。このファイルは、pam_limitsモジュールで読み込まれます。このファイルを使用すると、絶対に超過できない厳密な制限と、一時的な超過が許される緩やかな制限を設定できます。構文および使用可能なオプションの詳細については、ファイルに含まれているコメントを参照してください。

36.4 関連資料

インストール済みシステムのディレクトリ/usr/share/doc/packages/pamには、次のドキュメントが用意されています。

READMEs

このディレクトリの最上位レベルには、一般的なREADMEファイルがいくつか入っています。サブディレクトリ`modules`には、使用可能なPAMモジュールのREADMEファイルがあります。

『Linux-PAM System Administrators' Guide』

このマニュアルには、システム管理者を対象としたPAMに関する必須情報がすべて含まれています。設定ファイルの構文からPAMのセキュリティ面に至るまで、広範囲な項目を説明しています。このマニュアルは、PDFファイル、HTML形式およびプレーンテキストで提供されます。

『Linux-PAM Module Writers' Manual』

このマニュアルには、開発者を対象として標準準拠のPAMモジュールを記述する方法の概要が記載されています。このマニュアルは、PDFファイル、HTML形式およびプレーンテキストで提供されます。

『The Linux-PAM Application Developers' Guide』

このマニュアルには、PAMライブラリを使用するアプリケーション開発者に必要な情報がすべて含まれています。このマニュアルは、PDFファイル、HTML形式およびプレーンテキストで提供されます。

Thorsten KukukはSUSE Linux用のPAMモジュールを多数開発しており、その一部の情報は`http://www.suse.de/~kukuk/pam/`で公開されています。

37

Xenによる仮想化

Xenを使用すると、1台の物理的なコンピュータ上でLinuxシステムを複数起動できます。異なるシステム用のハードウェアは仮想的に提供されます。ここでは、この技術の可能性および限界についての概要を説明します。この概要は、Xenのインストール、設定、および起動についての章で構成されています。

仮想コンピュータでは通常、システムが必要とするハードウェアをエミュレートする必要があります。その欠点は、エミュレートされたハードウェアは、実際のハードウェアよりもかなり遅いという点です。Xenでは異なるアプローチを採用しています。それは、できるだけエミュレートするものを少なくするというものです。これを可能にするために、Xenは、*paravirtualization*を使用します。 これは、仮想コンピュータを基礎となるハードウェアと同じように見せますが、同一的には見せないテクニックです。そのため、ホストおよびゲストオペレーティングシステムは、カーネルレベルで適合します。ユーザスペースは変更のないままです。Xenでは、ハードウェアをhypervisorおよびドメイン-0と呼ばれる、制御ゲストによって管理します。これらにより、必要とされるすべての仮想化されたブロックおよびネットワークデバイスが提供されます。ゲストシステムは、これらのバーチャルブロックおよびネットワークブロックを使用してシステムを起動し、他のゲストやローカルネットワークに接続します。Xenが稼動している複数の物理的コンピュータが、仮想ブロックおよびネットワークデバイスを利用可能な状態に設定されている場合、コンピュータの起動中に、あるハードウェアから他のハードウェアにゲストシステムを移動させることもできます。当初、Xenは1台のコンピュータ上に最大100個のシステムを起動するために開発されたのですが、この数字は、動作中のゲストシステムのシステム要件(特にメモリの消費量)に強く左右されました。

CPU使用量を制限するため、Xenのhypervisorでは、3つの異なるスケジューラが用意されています。このスケジューラは、ゲストシステムの動作中に変更することも可能です。これで、動作中のゲストシステムの優先順位を変更することができます。さらに高いレベルでは、利用可能なCPUのパワーをい調整するために、ゲストを移動させることもできます。

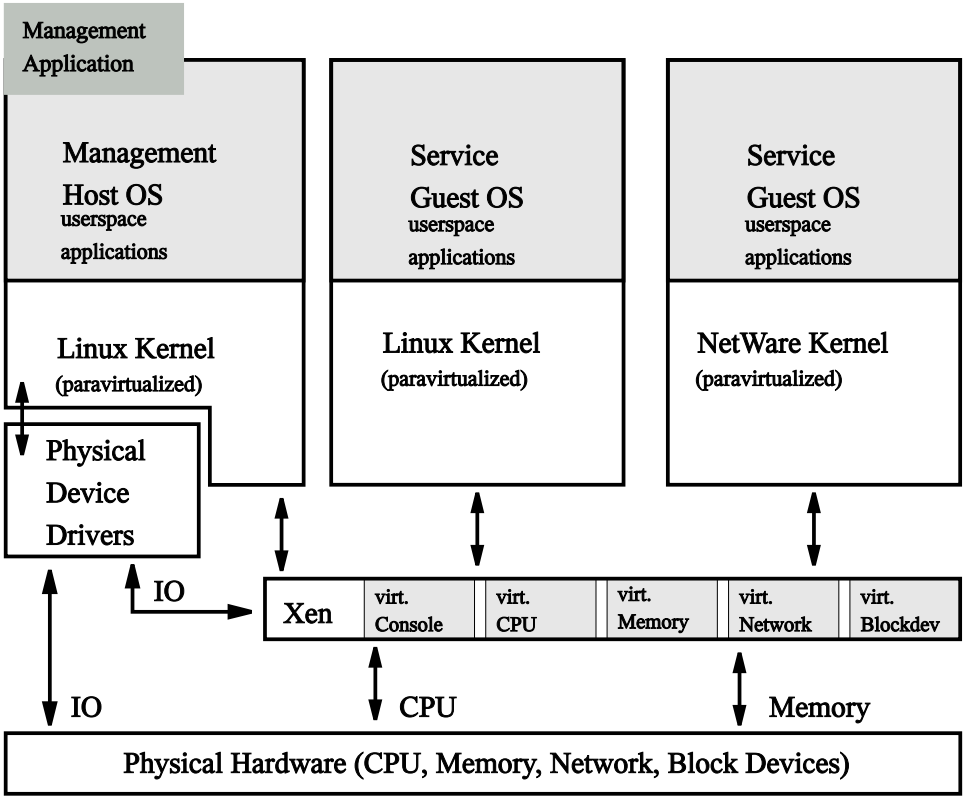
Xen仮想化システムには、サポートされるハードウェアに関して、不利な点もいくつかあります。

- Nvidia社またはATI社から提供されているような、オープンソースでないドライバのいくつかは、予想されたとおりに動作しません。このような場合は、可能であれば、チップの全機能をサポートしていないドライバでも、オープンソースのものを使用する必要があります。WLANチップおよびcardbusブリッジも、Xenを使用する環境ではサポートされていません。

- バージョン2では、XenはPAE(物理アドレス拡張)をサポートしません。つまり、4GBより大きいメモリはサポートしないということです。

- ACPIをサポートしません。電源管理およびその他の、ACPIに依存しているモードは機能しません。

図 37.1　Xenの概要



37.1　Xenのインストール

Xenのインストール手順には、ドメイン-0のドメインの設定およびXenクライアントのインストールが含まれます。初めに、必要なパッケージがインストールされているか確認します。必要なパッケージは、`python`、`bridge-utils`、`xen`、および`kernel-xen`です。SUSEパッケージを使用する場合、Xenは GRUBの設定に追加されます。その他の場合は、`boot/grub/menu.lst`の中にエントリが作成されます。このエントリは以下のような内容である必要があります。

```
title Xen2
    kernel (hd0,0)/boot/xen.gz dom0_mem=458752
```

```
module (hd0,0)/boot/vmlinuz-xen <parameters>
module (hd0,0)/boot/initrd-xen
```

(hd0,0)を、お使いのシステムの /bootディレクトリを格納しているパーティションに置き換えます。章 29. ブートローダ (page 473)も参照してください。dom0_memの数値を、お使いのシステムに合うように変更します。最大値は、システムのメモリ(KBでの値)から65536を引いた値です。<parameters>を、通常Linuxカーネルを起動する際に使用するパラメータに置き換えます。その後、Xenモードで再起動します。これにより、Xen hypervisorおよびほとんどのハードウェアを動作させるドメイン-0としてのLinuxカーネルが起動します。既に説明した例外を除き、すべてが通常通りに動作するはずです。

37.2 ドメインのインストール

ゲストドメインのインストールと設定には、いくつかの手順を実行します。以下では、最初のゲストドメインをインストールし、最初のネットワーク接続のための、異なるタスクのすべてを完了する方法を説明します。

ゲストシステムをインストールするには、ブロックデバイスまたはファイルシステムイメージの中にルートファイルシステムを準備し、設定する必要があります。このシステムにあとでアクセスするには、エミュレートされたコンソールを使用するか、このゲストにネットワーク接続を設定します。SUSE Linuxの1つのディレクトリへのインストールはYaSTによってサポートされています。そのようなゲストのハードウェア要件は、一般的なLinuxのインストールと同様のものです。

すべてのドメインから読み取り専用でマウントされたファイルシステムは、ドメイン間で共有できます。例えば、 /usrあるいは /optのようなファイルシステムです。読み書きモードでマウントされたファイルシステムは共有しないでください。複数のゲストドメイン間で、書き込み可能なデータを共有するには、NFSか、その他のネットワークファイルシステムまたはクラスタファイルシステムを使用します。

警告: ゲストドメインの共有

ゲストドメインを開始する際は、ゲストのファイルシステムが、インストーラまたは制御ドメイン-0によってマウントされていないことを確認します。

最初に行うことは、ゲストのLinuxをインストールするファイルシステムイメージの作成です。

1. /var/tmp/の中にguest1という名前の4GBの空のイメージを作成するには、次のコマンドを使用します。

```
dd if=/dev/zero of=/var/tmp/guest1 seek=1M bs=4096 count=1
```

2. イメージとは、何の情報も含まない大きな空のファイルのことです。この中にファイルを書き込むには、ファイルシステムが必要です。

```
mkreiserfs -f /var/tmp/guest1
```

   コマンドmkreiserfsは、これがブロック特殊デバイスではないことおよびそれの確認を求める情報を表示します。Yを押して、さらにEnterを押して続行します。

3. 実際のインストールはディレクトリ内にされます。そのため、ファイルシステムイメージ/var/tmp/guest1が、ディレクトリにマウントされている必要があります。

```
mkdir -p /var/tmp/dirinstall
mount -o loop /var/tmp/guest1 /var/tmp/dirinstall
```

重要項目

インストールが終了したら、このファイルシステムイメージを再びアンマウントします。YaSTでは、インストール時に、/procファイルシステムもマウントしますので、これもアンマウントしてください。

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall
```

37.2.1 YaSTを使用したゲストドメインのインストール

YaSTでゲストドメインをインストールするには、新規ゲストのためのファイルシステムイメージをあらかじめ準備しておく必要があります。YaSTを開始し、*[ソフトウェア]* → *[XENのディレクトリへのインストール]*の順に選択します。

ディレクトリインストール用のYaSTモジュールには、必要に応じた設定を必要とするオプションがいくつかあります。

- ターゲットディレクトリ: `/var/tmp/dirinstall`

  使用するファイルシステムイメージのマウントポイントにこのオプションを設定します。通常はデフォルトを受け入れます。

- YaSTおよびSuSEconfigを初回起動時に起動する: はい

  このオプションには、［*はい*］を設定します。rootユーザ用のパスワードおよび初めてゲストを開始する際の最初のユーザが要求されます。

- イメージ作成: いいえ

  ここで作成されるイメージは、単なるインストールディレクトリのtarによるアーカイブです。これはここでは必要ではありません。

- ソフトウェア

  使用するインストールのタイプを選択します。最初はデフォルトで構いません。

［*次へ*］をクリックして、インストールをスタートします。パッケージの数によって、インストールに時間がかかる場合があります。インストールの完了後は、tlsライブラリは削除する必要があります。

```
mv /var/tmp/dirinstall/lib/tls /var/tmp/dirinstall/lib/tls.disabled
```

Xenでは、ゲストドメインを開始するのに、ドメイン-0にインストールされたカーネルの1つを使用します。ゲスト内でネットワークを使用するには、このカーネルのモジュールも、ゲストにとって利用可能である必要があります。

```
cp -a /lib/modules/$(rpm -qf --qf %{VERSION}-%{RELEASE}-xen \
    /boot/vmlinuz-xen) /var/tmp/dirinstall/lib/modules
```

ファイルシステムのエラーを防ぐには、インストール後にファイルシステムイメージがアンマウントされている必要があります。

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall/
```

一方でドメイン-0用に特化したカーネルを作成し、他方でゲストシステムに特化したカーネルを作成することもできます。主な違いは、ゲストシステム

ではハードウェアドライバが必要でないという点です。これらのドライバはモジュールでありゲストシステムでは使用されないので、SUSEは、両方のタスクに1つのカーネルのみ供給します。

37.2.2 ゲストドメインとして使用するためのレスキューシステムの設定

システムを素早く稼動状態にするには、SUSE Linuxのレスキューシステムのような、既存のルートファイルシステムを再利用するのが最も簡単な方法です。基本的に、このイメージ内の仮想ブロックおよびネットワークイメージのカーネルイメージおよびデバイストライバを交換します。この作業を簡単にするために利用可能なスクリプト`mk-xen-rescue-img.sh`が、`/usr/share/doc/packages/xen/`の中にあります。

ルートファイルシステムを構築するのにレスキュー方式を使用することの欠点は、結果としてRPMデータベースが作成されないので、RPMを使用して簡単にパッケージを追加できない点です。利点としては、結果としては比較的小規模な構成になるのですが、ネットワークを使用するのに必要な機能のほとんどを備えられるという点です。

スクリプト`mk-xen-rescue-img.sh`を実行するには、少なくともレスキューイメージを持ったディレクトリおよび結果的に生成されるイメージを格納する宛先となる場所が必要です。デフォルトでは、そのディレクトリはディレクトリ`/boot`内の、ブートDVDになります。

```
cd /usr/share/doc/packages/xen
./mk-xen-rescue-img.sh /media/dvd/boot /usr/local/xen 64
```

スクリプトの最初のパラメータは、レスキューイメージのディレクトリです。2番目のパラメータは、イメージファイルの宛先です。オプションのパラメータでは、新規で生成されるゲストドメインおよび使用するカーネルバージョンのディスク容量の要件を指定します。

このスクリプトは、新しい場所にイメージをコピーし、カーネルおよび複数のカーネルモジュールを置き換え、システム内の`tls`ディレクトリを無効化します。最終的な手順として、新規イメージの設定ファイルを、`/etc/xen/`の中に生成します。

37.3 Xenゲストドメインの設定

ゲストドメインの設定方法についてのマニュアルは、それほど詳細な情報を網羅していません。ゲストドメインの設定方法に関するほとんどの情報は、設定ファイルの例 /etc /xen /configで参照することができます。そのファイルでは、デフォルト値あるいは少なくとも設定の例とともに必要なオプションが説明されています。項37.2.1.「YaSTを使用したゲストドメインのインストール」 (page 601)で説明されているインストールを実行するには、ファイル /etc /xen /guest1を以下の内容で作成します。

```
kernel = "/boot/vmlinuz-xen"   ❶
ramdisk = "/boot/initrd-xen"   ❷
memory = 128                   ❸
name = "guest1"                ❹
nics = "1"                     ❺
vif = [ 'mac=aa:cc:00:00:00:ab, bridge=xen-br0' ] ❻
disk = [ 'file:/var/tmp/guest1,hda1,w' ] ❼
root = "/dev/hda1 ro"          ❽
extra = "3"                    ❾
```

❶ ドメイン-0内のXenカーネルへのパスを入力します。このカーネルは、のちほどゲストシステムで稼動します。

❷ Xenカーネル用のデバイスドライバを含んでいる、適切な初期のRAMディスクを選択します。これがないと、カーネルはそのルートファイルシステムをマウントできずに、通常パニックを起こします。

❸ ゲストドメインにはどれほどのメモリが割り当てられるかを指定します。このゲストに利用可能なメモリサイズが不足している場合は、この作業は失敗します。

❹ このゲストの名前です。

❺ ゲストドメインの仮想ネットワークインタフェースの数です。

❻ 仮想ネットワークインタフェースの設定です。これにはインタフェースのMACアドレスおよびそれが接続されるブリッジを含みます。

❼ Xenゲストのために、利用可能な仮想ブロックデバイスを設定します。実際のブロックデバイスを使用するには、['phy:sdb1,hda1,w', 'phy:system/swap1,hda2,w']のようなエントリを作成します。

❽ カーネル用にルートデバイスを設定します。これはゲストには仮想デバイスとして見える必要があります。

❾ ここで特別なカーネルパラメータを追加します。例の3は、ゲストがランレベル3で開始されることを意味します。

37.4 Xenドメインの開始および制御

ゲストドメインが開始されるには、Xen hypervisorが、新規ゲスト用の十分な空きメモリを持っている必要があります。最初に、使用中のメモリの量をチェックします。

```
xm list
Name              Id  Mem(MB)  CPU  State  Time(s)  Console
Domain-0           0      458    0  r----    181.8
```

コンピュータのメモリが512MBの場合、Xen hypervisorは、64MBを消費し、ドメイン-0が残りを専有します。新規ゲストのためにいくらかのメモリを開放するには、コマンド`xm balloon`が使用されます。ドメイン-0のサイズを330MBに設定するには、次のコマンドを`root`rootで入力します。

```
xm balloon 0 330
```

次に`xm list`を実行すると、ドメイン-0のメモリの使用率が330MBまで下がっているはずです。これで、128MBでゲストを開始するのに十分なメモリ領域が確保されました。コマンド`xm start guest1 -c`を実行すると、ゲストが開始され、開始中のゲストのコンソールが現在のターミナルにリンクされます。このゲストが初めて開始する場合は、YaSTを使用してインストールを終了します。

このコンソールを切り離したり、再度接続したりすることは、他のターミナルからいつでもできます。切り離すには、Ctrl +]を使用します。再度接続するには、まず必要なゲストのIDを、`xm list`で確認し、そのIDに、`xm console` *`ID`*で接続します。

Xenのxmツールには、使用可能なパラメータが多く存在します。`xm help`と入力すると、簡単な説明の付いたリストが表示されます。表 37.1. 「xmコマンド」 (page 606)には、まず手始めとして、いくつかの最重要コマンドが説明してあります。

表 37.1　xmコマンド

`xm help`	xmツールで使用可能なコマンドのリストを一覧表示します。
`xm console` *ID*	ゲストの最初のコンソール(tty1)に、ID *ID*で接続します。
`xm balloon` *ID Mem*	ID *ID*のドメインのメモリサイズを、*Mem*(MB単位)に設定します。
`xm create` *domname* `[-c]`	設定ファイル*domname*を使用してドメインを開始します。オプションの`-c`を使用すると、現在のターミナルを新規ゲストの最初のttyにリンクします。
`xm shutdown` *ID*	ID *ID*のゲストを通常どおりにシャットダウンします。
`xm destroy` *ID*	ID *ID*のゲストをただちに強制終了します。
`xm list`	稼動中のすべてのドメインのリストを、それぞれのID、メモリ、およびCPU時間の値とともに一覧表示します。
`xm info`	CPUおよびメモリの情報を含む、Xenホストに関する情報を表示します。

37.5　関連資料

Xenの詳細については、以下のWebサイトで入手可能です。

- `file:/usr/share/doc/packages/xen/user/html/index.html`—Xenユーザのためのオフィシャル情報です。これには、パッケージ`xen-doc-html`が必要です。

- file:/usr/share/doc/packages/xen/interface/html/index.html—技術的なインタフェースのマニュアルです。これにも、パッケージxen-doc-htmlが必要です。
- http://www.cl.cam.ac.uk/Research/SRG/netos/xen/index.html—ドキュメント関連の豊富なリンクを含む、Xenのホームページです。
- http://lists.xensource.com/—Xenに関するメーリングリストがいくつか記載されています。

パート IX. サービス

38 ネットワークの基礎

Linuxには、あらゆるタイプのネットワークストラクチャに統合するために必要なネットワークツールと機能が用意されています。ここでは、一般に使用されるLinuxプロトコルであるTCP/IPについて説明します。 このプロトコルが持つさまざまなサービスや特別な機能について述べます。ネットワークカード、モデム、その他のデバイスを使用したネットワークアクセスは、によって設定できます。手動による環境設定も可能です。この章では、基本的なメカニズムと関連のネットワークの環境設定ファイルのみを扱います。

LinuxおよびUnix系オペレーティングシステムは、TCP/IPプロトコルを使用します。これは1つのネットワークプロトコルではなく、さまざまなサービスを提供する複数のネットワークプロトコルのファミリです。TCP/IPを使用して2台のコンピュータ間でデータをやり取りするために、表 38.1. 「TCP/IPプロトコルファミリーを構成する主要なプロトコル」 (page 612)に示した各プロトコルが提供されています。 TCP/IPによって結合された世界規模のネットワーク全体のことを「インターネット」と呼びます。

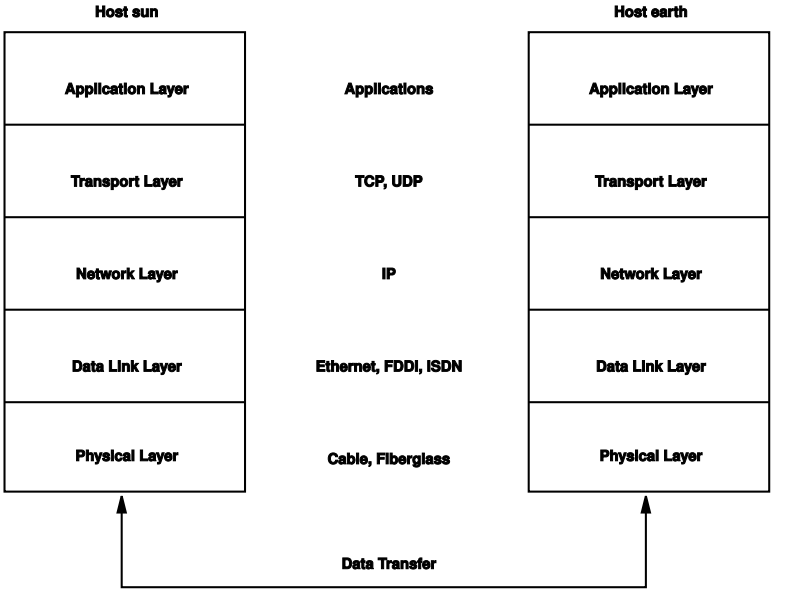
RFCは、*Request for Comments*の略です。RFCは、さまざまなインターネットプロトコルとそれをオペレーティングシステムとそのアプリケーションに実装する手順を定めています。RFC文書ではインターネットプロトコルのセットアップについて説明しています。プロトコルについての知識を広めるには、その種類にかかわらず、適切なRFC文書を参照してください。RFC文書は、`http://www.ietf.org/rfc.html`で参照してください。

表 38.1　TCP/IPプロトコルファミリーを構成する主要なプロトコル

プロトコル	説明
TCP	転送制御プロトコル。接続指向の安全なプロトコルです。転送されるデータはまずアプリケーションによってデータのストリームとして送信され、次にオペレーティングシステムによって適切な形式に変換されます。データは、それが送信されたときの元のデータ形式で、宛先ホストのそれぞれのアプリケーションに到着します。TCPは、伝送中にデータに損失がなかったか、データの混同がないかどうかを確認します。データの順序が意味を持つ場合は常にTCP/IPが実装されます。
UDP	ユーザデータグラムプロトコル。コネクションレスの安全でないプロトコルです。転送されるデータは、アプリケーションで生成されたパケットの形で送信されます。データが受信側に到着する順序は保証されず、データの損失の可能性もあります。UDPはレコード指向のアプリケーションに適しています。TCPよりも遅延時間が小さいことが特徴です。
ICMP	インターネット制御メッセージプロトコル。基本的にはエンドユーザ向けのプロトコルではありませんが、エラーレポートを発行し、TCP/IPデータ転送にかかわるマシンの動作を制御できる特別な制御プロトコルです。またICMPには特別なエコーモードがあります。エコーモードは、pingで使用されています。
IGMP	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している場合に、マシンの動作を制御します。

図 38.1.「TCP/IPの簡易レイヤモデル」 (page 613)に示したように、データのやり取りはさまざまなレイヤで実行されます。 実際のネットワークレイヤは、IP (インターネットプロトコル)によって実現される確実性のないデータ転送です。IPの上で動作するTCP (転送制御プロトコル)によって、ある程度の確実性のあるデータ転送が保証されます。IPレイヤの下層には、イーサネットなどのハードウェア依存プロトコルがあります。

図 38.1　TCP/IPの簡易レイヤモデル



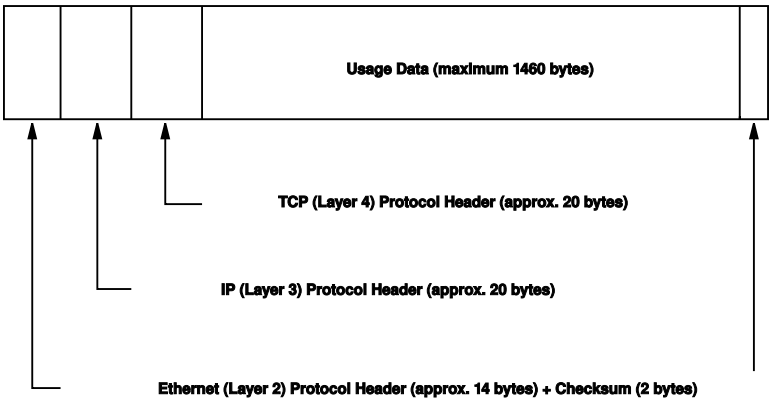
図では、各レイヤに対応する例を1つまたは2つ示しています。 レイヤは*抽象化レベル*に従って並べられています。最下位レイヤは最もハードウェアに近い部分です。一方、最上位レイヤは、ハードウェアがまったく見えないほぼ完全な抽象化になります。各レイヤにはそれぞれの固有の機能があります。各レイヤ固有の機能は、上記の主要プロトコルの説明を読めば大体わかります。データリンクレイヤと物理レイヤは、使用される物理ネットワーク（たとえばイーサネット） を表します。

ほとんどすべてのハードウェアプロトコルは、パケット単位で動作します。転送されるデータは、一度にすべて送信できないので、パケットに分割されます。TCP/IPパケットの最大サイズは約64KBです。しかし、パケットサイズは通常、64KBよりもかなり小さな値になります。これは、ネットワークハードウェアでサポートされているパケットサイズに制限があるからです。イーサネットの最大パケットサイズは、約1500バイトです。イーサネット上に送出されるTCP/IPパケットは、このサイズに制限されます。転送するデータ量が大きくなると、それだけ多くのパケットがオペレーティングシステムによって送信されます。

すべてのレイヤがそれぞれの機能を果たすためには、各レイヤに対応する情報を各データパケットに追加する必要があります。この情報はパケットのヘッ

ダとして追加されます。各レイヤでは、プロトコルヘッダと呼ばれる小さなデータブロックが、作成されたパケットに付加されます。図 38.2.「TCP/IPイーサネットパケット」 (page 614)に、イーサネットケーブル上に送出されるTCP/IPデータパケットの例を示します。誤り検出のためのチェックサムは、パケットの先頭ではなく最後に付加されます。これによりネットワークハードウェアの処理が簡素化されます。

図 38.2　TCP/IPイーサネットパケット



アプリケーションがデータをネットワーク経由で送信すると、データは各レイヤを通過します。これらのレイヤは、物理レイヤを除き、すべてLinuxカーネルに実装されています。各レイヤは、隣接する下位レイヤに渡せるようにデータを処理します。最下位レイヤは、最終的にデータを送信する責任を負います。データを受信したときには、この手順全体が逆の順序で実行されます。重なり合ったたまねぎの皮のように、各レイヤで伝送データからプロトコルヘッダが除去されていきます。 最後に、トランスポートレイヤが、着信側のアプリケーションがデータを利用できるように処理します。この方法では、1つのレイヤが直接やり取りを行うのは隣接する上下のレイヤのみです。データが伝送される物理的なネットワークは、100MBit/sのFDDIかもしれませんし、56-kbit/sのモデム回線かもしれませんが、アプリケーションがその違いを意識することはありません。同様に、物理ネットワークは、パケットの形式さえ正しければよく、伝送されるデータの種類を意識することはありません。

38.1　IPアドレスとルーティング

ここでは、IPv4ネットワークについてのみ説明しています。IPv4の後継バージョンであるIPv6については、項38.2.「IPv6—次世代のインターネット」(page 618)を参照してください。

38.1.1　IPアドレス

インターネット上のすべてのコンピュータは、一意の32ビットアドレスを持っています。この32ビット(4バイト)は、通常、例 38.1.「IPアドレスの表記」(page 615)の2行目に示すような形式で表記されます。

例 38.1　IPアドレスの表記

```
IPアドレス(2進表記):11000000 10101000 00000000 00010100
IPアドレス(10進表記):      192.      168.        0.       20
```

10進表記では、4つの各バイトが10進数で表記され、ピリオドで区切られます。IPアドレスは、ホストまたはネットワークインタフェースに割り当てられます。各アドレスは世界で唯一のアドレスであり、重複して使用されることはありません。 このルールには例外もありますが、以下の説明には直接関係していません。

IPアドレスにあるピリオドは、階層構造を表しています。1990年代まで、IPアドレスは、各クラスに固定的に分類されていました。 しかし、このシステムがあまりに柔軟性に乏しいことがわかったので、今日、そのような分類は行われていません。現在採用されているのは、*クラスレスルーティング*(CIDR: classless inter domain routing)です。

38.1.2　ネットマスクとルーティング

ネットマスクは、サブネットワークのアドレス範囲を定義するために用いられます。2台のホストが同一のサブネットワークに属している場合には、それらは相互に直接連絡できますが、そうでない場合には、サブネットワークとそれ以外の場所との間のトラフィックを処理するゲートウェイのアドレスを必要とします。2つのIPアドレスが同じサブネットワークに属しているかどうかをチェックするには、両方のアドレスとネットマスクの「AND」を求めます。 結果が同一であれば、両方のIPアドレスは同じローカルネットワークに

属しています。 相違があれば、それらのIPアドレス、そしてそれらに対応するインタフェースが連絡するには、ゲートウェイを通過する必要があります。

ネットマスクの役割を理解するには、例 38.2.「IPアドレスとネットマスクの論理積(AND)」 (page 616)を参照してください。 ネットマスクは、そのネットワークにいくつのIPアドレスが属しているかを示す、32ビットの値から成っています。 1になっているビットは、IPアドレスのうち、特定のネットワークに属することを示すビットに対応します。 0になっているビットは、サブネットワーク内での識別に使われるビットに対応します。 これは、1になっているビット数が多いほど、サブネットワークが小さいことを意味します。 ネットマスクは常に連続する1のビットから構成されているので、その数だけでネットマスクを指定することができます。 例 38.2.「IPアドレスとネットマスクの論理積(AND)」 (page 616)の、24ビットからなる第1のネットワークは、`192.168.0.0/24`と書くこともできます。

例 38.2　IPアドレスとネットマスクの論理積(AND)

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask    (255.255.255.0):  11111111 11111111 11111111 00000000
----------------------------------------------------------------
ANDをとった結果:                11000000 10101000 00000000 00000000
進表記:                            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
----------------------------------------------------------------
ANDをとった結果:                11010101 10111111 00001111 00000000
進表記:                            213.       95.       15.        0
```

別の例を挙げましょう。同じイーサネットケーブルに接続しているすべてのマシンは、普通、同じサブネットに属し、直接アクセスできます。 サブネットがスイッチまたはブリッジで物理的に分割されていても、これらのホストは直接アクセス可能です。

ローカルサブネットの外部のIPアドレスには、ターゲットネットワーク用のゲートウェイが設定されている場合にのみ、連絡できます。最も一般的には、外部からのすべてのトラフィックを扱うゲートウェイを1台だけ設置します。ただし、異なるサブネット用に、複数のゲートウェイを設定することも可能です。

ゲートウェイを設定すると、外部からのすべてのIPパケットは適切なゲートウェイに送信されます。 このゲートウェイは、パケットを複数のホストを経

由して転送し、それは最終的に宛先ホストに到着します。ただし、途中でTTL (time to live)に達した場合は破棄されます。

表 38.2　特殊なアドレス

アドレスのタイプ	説明
基本ネットワークアドレス	ネットマスクとネットワーク内の任意のアドレスの論理積をとったもの。例 38.2.「IPアドレスとネットマスクの論理積(AND)」 (page 616)のANDをとった結果を参照。このアドレスは、どのホストにも割り当てることができません。
ブロードキャストアドレス	ブロードキャストアドレスは、基本的には「サブネットワーク内のすべてのホストにアクセスする」ためのアドレスです。このアドレスを生成するには、2進数形式のネットマスクを反転させ、基本ネットワークアドレスと論理和をとります。上の例の場合、この結果は192.168.0.255になります。このアドレスは、どのホストにも割り当てることができません。
ローカルホスト	アドレス`127.0.0.1`は、各ホストの「ループバックデバイス」に割り当てられます。このアドレスを使用すると、自分のマシンに対して接続を確立できます。

IPアドレスは、世界中で一意でなければならないので、自分勝手にアドレスを選択して使うことはできません。 IPベースのプライベートネットワークをセットアップする場合のために、3つのアドレスドメインが用意されています。 これらは、外部のインターネットに直接接続することはできません。インターネット上で転送されることがないからです。このようなアドレスドメインは、RFC 1597で、表 38.3.「プライベートIPアドレスドメイン」 (page 617)に示すとおりに定められています。

表 38.3　プライベートIPアドレスドメイン

ネットワーク/ネットマスク	ドメイン
`10.0.0.0/255.0.0.0`	`10.x.x.x`

ネットワーク/ネットマスク	ドメイン
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

38.2 IPv6—次世代のインターネット

WWW(ワールドワイドウェブ)の出現により、ここ10年間でTCP/IP経由で通信を行うコンピュータの数が増大し、インターネットは爆発的に拡大しました。CERN (http://public.web.cern.ch)のTim Berners-Leeが1990年にWWWを発明して以来、インターネットホストは、数千から約1億まで増加しました。

前述のように、IPv4のアドレスはわずか32ビットで構成されています。しかも、多くのIPアドレスが失われています。というのは、ネットワークの編成方法のせいで、使われないIPアドレスが無駄に割り当てられてしまうからです。サブネットで利用できるアドレスの数は、(2のビット数乗- 2)で与えられます。たとえば、1つのサブネットワークでは、2、6、または14個のアドレスが使用可能です。たとえば128台のホストをインターネットに接続するには、256個のIPアドレスを持つサブネットワークが必要ですが、そのうち2つのIPアドレスは、サブネットワーク自体を構成するのに必要なブロードキャストアドレスと基本ネットワークアドレスになるので、実際に使用できるのは254個だけです。

現在のIPv4プロトコルでは、アドレスの不足を避けるために、DHCPとNAT(ネットワークアドレス変換)の2つのメカニズムが使用されています。これらの方法をパブリックアドレスとプライベートアドレスを分離するという慣習と組み合わせて使用することで、確かにアドレス不足の問題を緩和することができます。問題は、セットアップが面倒で保守しにくいその環境設定方法にあります。IPv4ネットワークでホストをセットアップするには、ホスト自体のIPアドレス、サブネットマスク、ゲートウェイアドレス、そして場合によってはネームサーバアドレスなど、相当数のアドレス項目が必要になります。管理者は、これらをすべて自分で設定しなければなりません。これらのアドレスをどこかから取得することはできません。

IPv6では、アドレス不足と複雑な環境設定方法はもはや過去のものです。ここでは、IPv6がもたらした進歩と恩恵について説明し、古いプロトコルから新しいプロトコルへの移行について述べます。

38.2.1 利点

この新しいプロトコルがもたらした最大かつ最もわかりやすい進歩は、利用可能なアドレス空間の飛躍的な増加です。IPv6アドレスは、従来の32ビットではなく、128ビットで構成されています。これにより、2の128乗、つまり、約3.4×1038個のIPアドレスが得られます。

しかしながら、IPv6アドレスがその先行プロトコルと異なるのはアドレス長だけではありません。IPv6アドレスは内部構造も異なっており、それが属するシステムやネットワークに関してより具体的な情報を有しています。詳細については、項38.2.2.「アドレスのタイプと構造」 (page 620)を参照してください。

以下に、この新しいプロトコルの利点をいくつか紹介します。

自動環境設定機能
IPv6を使用すると、ネットワークが「プラグアンドプレイ」対応になります。つまり、新しくシステムをセットアップすると、手動で環境設定しなくても、(ローカル)ネットワークに統合されます。新しいホストは自動環境設定メカニズムを使用して、*ネイバーディスカバリ* (ND)と呼ばれるプロトコルにより、近隣のルータから得られる情報を元に自身のアドレスを生成します。この方法は、管理者の介入が不要なだけでなく、サアドレス割り当てを1台のサーバで一元的に管理する必要もありません。これもIPv4より優れている点の1つです。IPv4では、自動アドレス割り当てを行うために、DHCPサーバを実行する必要があります。

モバイル性
IPv6を使用すると、複数のアドレスを1つのネットワークインタフェースに同時に割り当てることができます。これにより、ユーザは複数のネットワークに簡単にアクセスできます。 これは携帯電話会社が提供する国際ローミングサービスに似ています。国際ローミングサービスとは、携帯電話を国外に持ち出し、現地サービスのサービス地域に入ると、電話が自動的に現地サービスにログインするというサービスで、これによりどこにいても同じ番号で電話を受けられ、また自国にいるのと同様に電話をかけることができます。

安全な通信
IPv4では、ネットワークセキュリティは追加機能です。IPv6にはIPSecが中核的機能の1つとして含まれているので、システムが安全なトンネル経由で通信でき、インターネット上での部外者による通信傍受を防止します。

下位互換性
現実的に考えて、インターネット全体を一気にIPv4からIPv6に切り替えるのは不可能です。したがって、両方のプロトコルが、インターネット上だけでなく1つのシステム上でも共存できることが不可欠です。これは、一方ではアドレスの互換性によって(IPv4アドレスは容易にIPv6アドレスに変換できます)、他方ではトンネルの使用によって保証されています。項38.2.3.「IPv4とIPv6の共存」 (page 625)を参照してください。また、システムはデュアルスタック*IP*テクニックによって、両方のプロトコルを同時にサポートできるので、2つのプロトコルバージョン間に相互干渉のない、完全に分離された2つのネットワークスタックが作成されます。

マルチキャストによるサービスの詳細なカスタマイズ
IPv4では、いくつかのサービス(SMBなど)が、ローカルネットワークのすべてのホストにパケットをブロードキャストする必要があります。IPv6では、これよりはるかにきめ細かいアプローチが取られ、サーバがマルチキャストという、複数のホストをグループの一部として扱う技術によって、ホストにデータを送信します(これは、すべてのホストにデータを送信するブロードキャストとも、各ホストに個別に送信するユニキャストとも異なります)。どのホストを対象グループに含めるかは、個々のアプリケーションによって異なります。事前定義のグループには、たとえば、すべてのネームサーバを対象とするグループ(全ネームサーバマルチキャストグループ)やすべてのルータを対象とするグループ(全ルータマルチキャストグループ)があります。

38.2.2 アドレスのタイプと構造

前述のように、現行のIPプロトコルには、2つの重要な側面が欠けています。つはIPアドレスの不足の問題が表面化していること、もう1つはネットワークの設定とルーティングテーブルの保守がますます複雑で厄介な作業になりつつあることです。IPv6では、1つ目の問題を、アドレス空間を拡張することによって解決しています。2番目の問題には、階層的なアドレス構造を導入し、ネットワークアドレスを割り当てる高度なテクニックとマルチホーミング(1つのデバイスに複数のアドレスを割り当てることによって、複数のネットワークへのアクセスを可能にします)を組み合わせて対応しています。

IPv6を扱う場合は、次の3種類のアドレスについて知っておくと役に立ちます。

ユニキャスト
このタイプのアドレスは、1つのネットワークインタフェースだけに関連付けられます。このようなアドレスを持つパケットは、1つの宛先にのみ配信されます。したがって、ユニキャストアドレスは、パケットをローカルネットワークまたはインターネット上の個々のホストに転送する場合に使用します。

マルチキャスト
このタイプのアドレスは、ネットワークインタフェースのグループに関連します。このようなアドレスを持つパケットは、そのグループに属するすべての宛先に配信されます。マルチキャストアドレスは、主に、特定のネットワークサービスが、相手を特定のグループに属するホストに絞って通信を行う場合に使用されます。

エニーキャスト
このタイプのアドレスは、インタフェースのグループに関連します。このようなアドレスを持つパケットは、基盤となるルーティングプロトコルの原則に従い、送信側に最も近いグループのメンバに配信されます。エニーキャストアドレスは、特定のネットワーク領域で特定のサービスを提供するサーバについて、ホストが情報を得られるようにするために使用します。同じタイプのすべてのサーバは、エニキャストアドレスが同じになります。ホストがサービスを要求すると、ルーティングプロトコルによって最も近い場所にあるサーバが判断され、そのサーバが応答します。何らかの理由でこのサーバが応答できない場合、プロトコルが自動的に2番目のサーバを選択し、それが失敗した場合は3番目、4番目が選択されます。

IPv6アドレスは、4桁の英数字が入った8つのフィールドで構成され、それぞれのフィールドが16進数表記の16ビットを表します。各フィールドは、コロン(:)で区切られます。各フィールドで先頭の0は省略できますが、数字の間にある0や末尾の0は省略できません。もう1つの規則として、0のバイトが5つ以上連続する場合は、まとめて2つのコロン(::)で表すことができます。 ただし、この2つのコロン: : は、1つのアドレスで一度しか使用できません。この省略表記の例については、例 38.3.「IPv6アドレスの例」 (page 622)を参照してください。 この3行はすべて同じアドレスを表します。

例 38.3　IPv6アドレスの例

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                            : 10 : 1000 : 1a4
```

IPv6アドレスの各部の機能は個別に定められています。最初の4バイトはプレフィクスを形成し、アドレスのタイプを指定します。中間部分はアドレスのネットワーク部分ですが、使用しなくてもかまいません。アドレスの最後の4桁はホスト部分です。IPv6でのネットマスクは、アドレスの末尾のスラッシュの後にプレフィクスの長さを指定して定義します。例 38.4.「プレフィクスの長さを指定したIPv6アドレス」 (page 622)に示すアドレスには、最初の64ビットがアドレスのネットワーク部分を構成する情報、最後の64ビットにホスト部分を構成する情報が入っています。言い換えると、64は、ネットマスクに64個の1ビット値が左から埋められていることを意味します。IPv4と同様、IPアドレスとネットマスクのANDをとることにより、ホストが同じサブネットワークにあるかそうでないかを判定します。

例 38.4　プレフィクスの長さを指定したIPv6アドレス

```
fe80::10:1000:1a4/64
```

IPv6は、事前に定義された複数タイプのプレフィクスを認識します。表 38.4.「IPv6のプレフィクス」 (page 622)に、一部のプレフィクスタイプを示します。

表 38.4　IPv6のプレフィクス

プレフィクス (16進)	定義
00	IPv4アドレスおよびIPv4 over IPv6互換性アドレス。これらは、IPv4との互換性を保つために使用します。これらを使用した場合でも、IPv6パケットをIPv4パケットに変換できるルータが必要です。いくつかの特殊なアドレス(たとえばループバックデバイスのアドレス)もこのプレフィクスを持ちます。
先頭桁が2または3	集約可能なグローバルユニキャストアドレス。IPv4と同様、インタフェースを割り当てて特定のサブネットワークの一部を構成することができます。 現在、2001::/16(実

プレフィクス (16進)	定義
	稼動品質のアドレス空間)と2002::/16 (6to4アドレス空間)の2つのアドレス空間があります。
fe80::/10	リンクローカルアドレス。このプレフィクスを持つアドレスは、ルーティングしてはなりません。 したがって、同じサブネットワーク内からのみ到達可能です。
fec0::/10	サイトローカルアドレス。ルーティングはできますが、それが属する組織のネットワーク内に限られます。 要するに、IPv6版のプライベートネットワークアドレス空間です (たとえば、10.x.x.x)。
ff	マルチキャストアドレス。

ユニキャストアドレスは、以下の3つの基本構成要素からなります。

パブリックトポロジ
最初の部分(前述のいずれかのプレフィクスが含まれる部分)は、パブリックインターネット内でパケットをルーティングするために使用します。ここには、インターネットアクセスを提供する企業または団体に関する情報が入っています。

サイトトポロジ
2番目の部分には、パケットの配信先のサブネットワークに関するルーティング情報が入っています。

インタフェースID
3番目の部分は、パケットの配信先のインタフェースを示します。これを使用して、MACをアドレスの一部に含めることができます。MACは、世界中で重複がない固定の識別子であり、ハードウェアメーカによってデバイスにコーディングされるので、環境設定手順が大幅に簡素化されます。実際には、最初の64アドレスビットが統合されてEUI-64トークンを構成します。このうち、最後の48ビットにはMACアドレス、残りの24ビットにはトークンタイプに関する特別な情報が入ります。これにより、PPPやISDNのインタフェースのようにMACを持たないインタフェースにEUI-64トークンを割り当てられるようになります。

IPv6は、この基本構造の上で、以下の5種類のユニキャストアドレスを区別します。

: : (未指定)
このアドレスは、インタフェースが初めて初期化されるとき、すなわち、アドレスが他の方法で判定できないときに、ホストがそのソースアドレスとして使用します。

: :1 (ループバック)
ループバックデバイスのアドレス。

IPv4互換アドレス
IPv6アドレスが、IPv4アドレスおよび96個の0ビットからなるプレフィクスで作成されます。このタイプの互換アドレスは、IPv4とIPv6のホストが、純粋なIPv4環境で動作している他のホストと通信するためのトンネリング(項38.2.3. 「IPv4とIPv6の共存」 (page 625)を参照)として使用されます。

IPv6にマッピングされたIPv4アドレス
このタイプのアドレスは、IPv6表記で純粋なIPv4アドレスを指定します。

ローカルアドレス
ローカルで使用するアドレスのタイプには、以下の2種類があります。

リンクローカル
リンクローカル このタイプのアドレスは、ローカルのサブネットワークでのみ使用できます。このタイプの送信元または宛先アドレスを持つパケットをインターネットまたは他のサブネットワークにルーティングしてはなりません。これらのアドレスは、特別なプレフィクス(`fe80: : /10`)とネットワークカードのインタフェースID、およびヌルバイトからなる中間部分からなります。このタイプのアドレスは、自動環境設定のとき、同じサブネットワークに属する他のホストと通信するために使用されます。

サイトローカル
このタイプのアドレスを持つパケットは、他のサブネットワークにはルーティングできますが、それより広いインターネットにはルーティングしてはなりません。つまり、組織自体のネットワークの内側だけで使用するように制限する必要があります。このようなアドレスはイントラネット用に使用され、IPv4によって定義されているプライベートアドレス空間に相当します。これらのアドレスは、特殊なプレフィク

ス(`fec0::/10`)とインタフェースID、およびサブネットワークIDを指定する16ビットのフィールドからなります。

IPv6では、各ネットワークインタフェースが複数のIPアドレスを持つことができるというたまったく新しい機能が導入されました。これにより、同じインタフェースで複数のネットワークにアクセスできます。これらのネットワークは、MACと既知のプレフィクスを使用して完全に自動設定できるので、IPv6を有効にすると すぐに、(リンクローカルアドレスを使用して)ローカルネットワーク上のすべてのホストに接続できるようになります。IPアドレスにMACが組み込まれているので、使用されるIPアドレスは世界中で唯一のアドレスになります。アドレスの唯一の可変部分は、ホストが現在動作している実際のネットワークによって、*サイトトポロジ*と*パブリックトポロジ*を指定する部分になります。

複数のネットワークに接続するホストの場合、少なくとも2つのアドレスが必要です。1つは*ホームアドレス*です。ホームアドレスには、インタフェースIDだけでなく、それが通常属するホームネットワークの識別子(および対応するプレフィクス)も含まれています。ホームアドレスは静的アドレスなので、通常は変更されません。しかし、モバイルホスト宛てのパケットは、それがホームネットワーク内にあるかどうかにかかわらず、すべてそのホストに配信できます。これは、IPv6で導入された*ステートレス自動環境設定*や*ネイバーディスカバリ*のようなまったく新しい機能によって実現されました。モバイルホストは、ホームアドレスに加え、ローミング先の外部ネットワークに属するアドレスも取得します。これらは*ケアオブ*アドレスと呼ばれます。ホームネットワークには、ホストが対象エリア外をローミングしている間、そのホスト宛てのすべてのパケットを転送する機能があります。IPv6環境において、このタスクは、*ホームエージェント*によって実行されます。ホームエージェントは、ホームアドレスに届くすべてのパケットを取得してトンネルに リレーします。 一方、ケアオブアドレスに届いたパケットは、特別迂回することなく、直接モバイルホストに転送されます。

38.2.3 IPv4とIPv6の共存

インターネットに接続されている全ホストをIPv4からIPv6に移行する作業は、段階的に行われます。両方のプロトコルは今後しばらく共存することになります。両方のプロトコルを*デュアルスタック*で実装すれば、同じシステム上に共存することが保証されます。しかし、それでもなお、IPv6対応のホストがどのようにしてIPv4ホストと通信するか、また多くがIPv4ベースの現行ネットワークでIPv6パケットをどのように伝送するかなど、解決すべき問題が残

ります。最善のソリューションは、トンネリングと互換アドレスです(項38.2.2.「アドレスのタイプと構造」 (page 620)を参照)。

(世界的な)IPv4ネットワークから隔離されたIPv6ホストですが、トンネルを使用して通信することができます。つまり、IPv6パケットをIPv4パケットとしてカプセル化し、IPv4ネットワークを通じて伝送します。2つのIPv4ホスト間のこのような接続を*トンネル*と呼びます。これを行うには、パケットにIPv6の宛先アドレス(または対応するプレフィクス)とともに、トンネルの受信側にあるリモートホストのIPv4アドレスも含める必要があります。基本的なトンネルは、ホストの管理者間が合意すれば、手動で設定が可能です。これは、*静的トンネリング*とも呼ばれます。

ただし、静的トンネルの環境設定とメンテナンスは、あまりに手間がかかるので、多くの場合、日常の通信には向きません。そこで、IPv6は、*動的トンネリング*を実現する3つの異なる方法を提供しています。

6over4
IPv6パケットが自動的にIPv4パケットとしてカプセル化され、マルチキャスト対応のIPv4ネットワークによって送信されます。IPv6は、ネットワーク全体(インターネット)を巨大なLAN (local area network)だと思い込んで動作することになります。これにより、IPv4トンネルの着信側の端を自動的に判定できます。ただし、この方法は拡張性に欠けているだけではなく、IPマルチキャストがインターネット上で広く普及しているとはいえないという事実も障害となります。したがってこの解決方法を採用できるのは、マルチキャストが利用できる小規模な企業内ネットワークだけです。この方式の仕様は、RFC 2529に規定されています。

6to4
この方式では、IPv6アドレスからIPv4アドレスを自動的に生成することで、隔離されたIPv6ホストがIPv4ネットワーク経由で通信できるようにします。しかし、隔離されたIPv6ホストとインターネットの間の通信に関して、多くの問題が報告されています。この方式は、RFC 3056で規定されています。

IPv6トンネルブローカ
この方式は、IPv6ホスト専用のトンネルを提供する特殊なサーバに依存します。この方式は、RFC 3053で規定されています。

重要項目: 6boneイニシアチブ

「旧式の」インターネットの中核部分では、トンネル経由で接続されたIPv6サブネットのネットワークが既に世界中に広がっています。これは*6bone*ネットワーク(`http://www.6bone.net`)というIPv6テスト環境で、新しいプロトコルの実装に必要な経験を積むために、IPv6ベースのサービスを開発して提供するプログラマやインターネットプロバイダを対象としています。詳細については、同プロジェクトのインターネットサイトを参照してください。

38.2.4 IPv6の設定

通常、IPv6を設定するために、個々のワークステーションの設定を変更する必要はありません。ただし、IPv6サポートをロードする必要はあります。それには、`root`権限で、`modprobe ipv6`コマンドを実行します。

IPv6の自動環境設定の概念があるため、ネットワークカードには、*リンクローカルネットワーク*内のアドレスが割り当てられます。通常、ワークステーション上ではルーティングテーブルの管理を実行しません。ワークステーションは、*ルータアドバタイズプロトコル*を使用して、実装する必要のあるプレフィクスとゲートウェイをネットワークルータに問い合わせます。IPv6ルータは、radvdプログラムを使用して設定できます。このプログラムは、IPv6アドレスに使用するプレフィクスとルータをワークステーションに通知します。または、zebraを使用してアドレスとルーティングを自動環境設定することもできます。

詳細については、ifup(8)のmanマニュアルページを参照してください。`/etc/sysconfig/network`ファイルを使用してさまざまなタイプのトンネルを設定する方法が説明されています。

38.2.5 関連資料

ここでの概要は、IPv6に関する情報を網羅しているわけではありません。IPv6の詳細については、次のオンラインドキュメントや書籍を参照してください。

http://www.ngnet.it/e/cosa-ipv6.php
IPv6の基本的な事項についての詳細を紹介した記事が収録されています。

IPv6に関する優れた入門書です。

http://www.bieringer.de/linux/IPv6/
Linux IPv6-HOWTOと多くの関連トピックへのリンクが用意されています。

http://www.6bone.net/
トンネルIPv6ネットワークに参加するには、このサイトを参照してください。

http://www.ipv6.org/
IPv6のあらゆる情報にここからリンクできます。

RFC 2640
IPv6に関する基本的なRFCです。

IPv6 Essentials
Silvia Hagenによる*IPv6 Essentials* (ISBN 0-596-00125-8)は、このトピックに関するあらゆる重要な面を扱っている本です。

38.3 名前解決

DNSはIPアドレスに1つまたは複数のホスト名を割り当てるとともに、ホスト名をIPアドレスに割り当てます。Linuxでは、この変換は通常、bindという特別な種類のソフトウェアによって行われます。また、この変換を行うマシンをネームサーバと呼びます。ホスト名は、その名前構成要素がピリオド(.)で区切られた階層システムを構成しています。しかしながら名前の階層構造は、先に述べたIPアドレスの階層構造とは無関係です。

`hostname.domain`という形式で書かれた完全な名前、たとえば、`earth.example.com`を考えてみましょう。*完全修飾ドメイン名*(FQDN: fully qualified domain name)と呼ばれるフルネームは、ホスト名とドメイン名(`example.com`)で構成されます。ドメイン名には*最上位ドメイン*(TLD) (`de`)が含まれます。

TLDの割り当ては、これまでの経緯もあって、非常に複雑になっています。従来から、米国では、3文字のドメイン名が使用されています。他の国では、

ISOで制定された2文字の国コードが標準です。これに加えて、2000年には、特定の活動領域を表す、より長いTLDが導入されました(たとえば、.info、.name、.museum)。

インターネットの初期(1990年より前)には、ファイル/etc/hostsに、インターネットで利用されるすべてのマシン名を記述していました。しかし、インターネットに接続されるコンピュータ数の急激な増加により、この方法はすぐに現実的でなくなりました。このため、ホスト名を広く分散して保存するための分散データベースが開発されました。このデータベースは、ネームサーバと同様、インターネット上のすべてのホストに関するデータがいつでも用意されているわけではなく、他のネームサーバに問い合わせを行います。

この階層の最上位には、複数のルートネームサーバがあります。ルートネームサーバは、Network Information Center (NIC)によって運用されており、最上位レベルドメインを管理します。各ルートネームサーバは、特定の最上位ドメインを管理するネームサーバについての情報を持っています。最上位ドメインNICの詳細については、http://www.internic.netを参照してください。

DNSには、ホスト名の解決以外の機能もあります。ネームサーバには、特定のドメイン宛の電子メールをどのホストに転送するかも管理しています(*メールエクスチェンジャ(MX)*)。

マシンがIPアドレスを解決するには、少なくとも1台のネームサーバとそのIPアドレスを知っている必要があります。YaSTを使用すれば、このようなネームサーバを簡単に指定できます。モデムを使ったダイアルアップ接続の場合は、ネームサーバを手動で設定する必要はありません。接続が設定されるときに、ダイアルアッププロトコルによってネームサーバのアドレスが提供されるからです。SUSE Linuxでのネームサーバアクセスの環境設定については、章 40. *ドメインネームシステム* (page 661)を参照してください。

whoisプロトコルは、DNSと密接な関係があります。このプログラムを使用すると、特定のドメインの登録者名をすぐに検索できます。

38.4 YaSTによるネットワーク接続の設定

Linuxでは多くのタイプのネットワーク接続がサポートされています。 その多くは、異なるデバイス名と、ファイルシステム内の複数の場所に分散した設定ファイルを使用しています。 手動によるネットワーク設定のさまざまな面についての詳細は、項38.5.「ネットワークの手動環境設定」 (page 641)を参照してください。

インストール中に、YaSTは検出したすべてのインタフェースを自動的に設定します。インストール済みのシステムの付加的なハードウェアは、インストール後に設定することができます。 以下のセクションでは、SUSE Linuxがサポートするすべてのタイプのネットワーク接続について、その設定方法を説明します。

38.4.1 YaSTでのネットワークカードの設定

モジュールを起動すると、YaSTの汎用のネットワーク設定ダイアログが表示されます。上部には、未設定の全ネットワークカードのリストが表示されます。正しく検出されたカードであれば、その名前が表示されます。 検出できなかったデバイスも、［*Other (not detected)*］を選択すれば、検出されなかったネットワークカードの手動設定項 (page 630)で説明されている方法で設定できます。ダイアログの下部には、設定済みのデバイスがネットワークタイプおよびアドレスと共にリスト表示されます。これで、新規のネットワークカードを設定するか、既存の設定を変更できます。

検出されなかったネットワークカードの手動設定

自動検出されなかった(［*Other*］としてリストされた)ネットワークカードについては、次の項目を設定する必要があります。

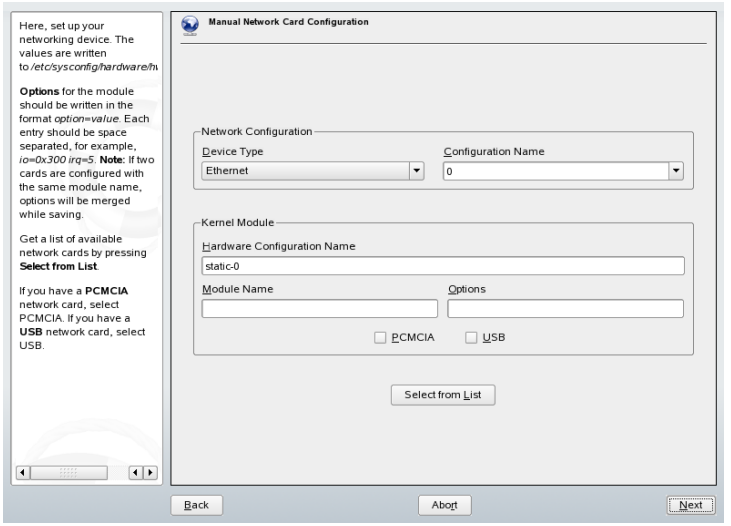
［ネットワークの設定］
利用可能なオプションからインタフェースのデバイスタイプと設定名を選択します。 設定名の命名規則については、`getcfg(8)`のmanページを参照してください。

［カーネルモジュール］

［*Hardware Configuration Name*］では、ネットワークカードのハードウェア設定を記述する /etc/sysconfig/hardware/hwcfg-*ファイルの名前を指定します。 この名前には、適切なカーネルモジュールの名前や、ハードウェアを初期化するために必要なオプションを含めます。 通常は、PCMCIAおよびUSBハードウェアに対しては、妥当な名前がYaSTによって提示されます。 その他のハードウェアに対しては、カードが設定名0で設定されている場合、通常はhwcfg-static-0だけが妥当な名前です。

ネットワークカードが、PCMCIAデバイスかUSBデバイスの場合、［ネットワークカードの手動設定］ダイアログで、［PCMCIA］または［USB］チェックボックスを有効にして、［次へ］をクリックしてダイアログを終了します。 それ以外の場合には、[*Select from List*]でネットワークカードの型式を選択します。 YaSTは自動的に、そのカードに適したカーネルモジュールを選択します。［次へ］をクリックして、このダイアログを終了します。

図 38.3 *ネットワークカードの設定*



ネットワークアドレスの設定

インタフェースのデバイスタイプおよび設定名を設定します。［デバイスの型］で表示されるオプションから該当するデバイスタイプを選択します。ま

た、必要に応じて設定名を指定します。通常は、デフォルト設定のままで問題ありません。設定名の命名規則については、`getcfg(8)`のmanページを参照してください。

［ネットワークの設定］の［デバイスの型］で［*無線*］を選択した場合は、次の［*無線ネットワークカードの設定*］ダイアログで、動作モード、ネットワーク名(ESSID)、および暗号化方式を設定します。［*了解*］をクリックして、カードの設定を完了します。WLANカードの設定の詳細については、項22.1.3.「YaSTでの設定」(page 318)を参照してください。その他のインタフェースタイプの場合は、ネットワークアドレスの設定に進んでください。

［自動アドレス設定(DHCPを介して)］
ネットワーク上でDHCPサーバを稼動している場合は、DHCPサーバからネットワークアドレスを自動的に取得できます。DSL回線を使用していてISPからスタティックIPが割り当てられていなければ、オプションも使用する必要があります。DHCPを使用する場合は、［*DHCPクライアントオプション*］を選択して詳細を設定します。DHCPサーバが常にブロードキャストリクエストを受け付けるかどうか、および使用するIDを指定します。デフォルトでは、DHCPサーバはカードのハードウェアアドレスを使用してインタフェースを識別します。さまざまなホストが同じインタフェースを介して通信するようにバーチャルホストがセットアップされている場合は、各ホストの識別にIDが必要になります。

［スタティックなアドレスの設定］
静的なアドレスがある場合には、このオプションをオンにします。次に、ネットワークのアドレスとサブネットマスクを入力します。事前設定されているサブネットマスクは、典型的なホームネットワークの要件と一致している必要があります。

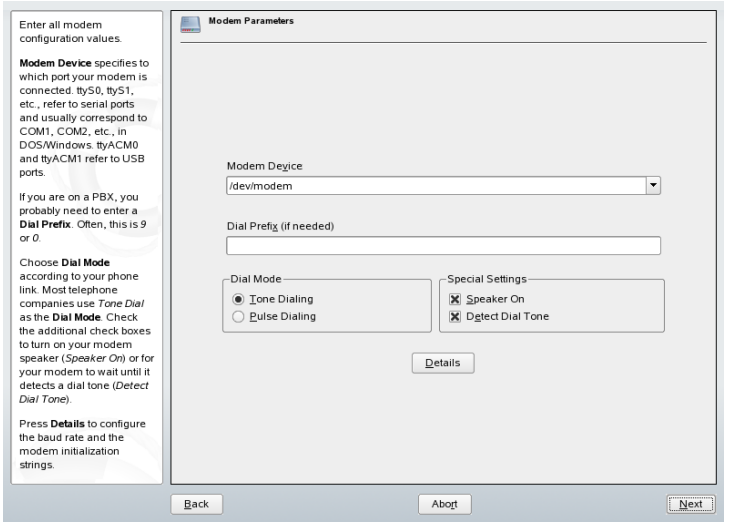
［*Next*］を選択してこのダイアログを終了するか、ホスト名、ネームサーバ、ルーティングの設定に進みます(DNSサーバ (↑起動)およびルーティング (↑起動)を参照)。

［*詳細*］で、より詳細な設定を指定できます。［*詳細設定*］の［*ユーザコントロール*］を使用してネットワークカードの制御を管理者(`root`)から一般ユーザに委任できます。これにより、モバイル環境で、ユーザがインタフェースの有効/無効を自身で制御してネットワーク接続を柔軟に変更できるようになります。MTU (Maximum Transmission Unit)および［*デバイスの起動*］のタイプもこのダイアログで設定できます。

38.4.2 モデム

YaSTコントロールセンターで、［*ネットワークデバイス*］を使用してモデム設定にアクセスします。モデムが自動的に検出されない場合は、手動設定用のダイアログを開きます。開いたダイアログの［*モデムデバイス*］に、モデムの接続先インタフェースを入力します。

図 38.4 *モデム設定*



構内交換機(PBX)経由で接続している場合は、ダイヤルプレフィックスの入力が必要な場合があります。通常、このプレフィックスは0(ゼロ)です。PBX付属の指示書で確認してください。また、トーンダイヤル方式とパルスダイヤル方式のどちらを使用するか、スピーカをオンにするかどうか、およびモデムをダイヤルトーンの検出まで待機させるかどうかも選択します。モデムが交換機に接続されている場合、後者のオプションは無効です。

［*詳細*］で、ボーレートとモデムの初期化文字列を設定します。これらの設定は、モデムが自動検出されなかった場合、またはデータ転送を動作させるために特殊な設定が必要な場合にのみ変更してください。これは、主にISDN端末アダプタを使用する場合です。［*OK*］をクリックしてこのダイアログを閉じます。モデムの制御権をroot権限のない通常のユーザに委任するには、［*ユーザコントロール*］を有効にします。このようにすると、管理者権限のないユーザがインタフェースを有効化または無効化できるようになります。

［*Dial Prefix Regular Expression*］には、正規表現を指定します。この正規表現とKInternetで設定する［ダイヤルプレフィックス］が一致する必要があります。このフィールドを空のままにした場合、管理者権限のないユーザは［ダイヤルプレフィックス］を変更できません。

次のダイアログで、ISP (インターネットサービスプロバイダ)を選択します。事前定義済みの国内ISPリストから選択するには、［*国*］を選択します。または、［*新規*］をクリックしてダイアログを開き、独自ISPのデータを入力します。これには、ダイヤルアップ接続名、ISP名、ISPから提供されるログインとパスワードが含まれます。接続するたびにパスワードを要求させるには、［*常にパスワードを要求する*］を選択します。

最後のダイアログでは、次のようにその他の接続オプションを指定できます。

［必要に応じてダイヤルする］
ダイヤルオンデマンドを有効にする場合は、ネームサーバを少なくとも1つ指定します。

［接続時にDNSを変更する］
このオプションはデフォルトでオンになっていて、インターネットに接続するたびにネームサーバアドレスが更新されます。

［自動でDNS情報を取得］
接続後にプロバイダからドメインネームサーバの情報が送信されない場合は、このオプションをオフにしてDNSの情報を手動で入力します。

［スチューピッドモード］
このオプションは、デフォルトで有効です。その場合、接続プロセスを妨げないように、ISPのサーバから送信される入力プロンプトは無視されます。

［***External Firewall Interface***］および［***Restart Firewall***］
これらのオプションを選択すると、SUSEfirewall2が有効になり、インターネット接続中の外部の攻撃から保護されます。

［アイドルタイムアウト(秒)］
このオプションでは、ネットワークがアイドル状態になってからモデムが自動的に切断されるまでの時間を指定します。

［IP Details(IP詳細設定)］
このオプションを選択すると、アドレス設定ダイアログが開きます。ISPからホストにダイナミックIPアドレスが割り当てられていない場合は、［ダイナミック*IP*アドレス］を無効にして、ホストのローカルIPアドレスとリモートIPアドレスを入力します。この情報については、ISPにお問い合わせください。［デフォルトルート］は有効なままにし、［*OK*］を選択してダイアログを閉じます。

［次へ］を選択すると、元のダイアログに戻り、モデム設定の概要が表示されます。［完了］を選択し、このダイアログを閉じます。

38.4.3 ISDN

このモジュールは、システムの1つ以上のISDNカードを設定します。 YaSTによってISDNカードが検出されなかった場合は、手動で選択してください。複数のインタフェースを設定することも可能ですが、1つのインタフェースに複数のISPを設定することも可能です。以降のダイアログでは、カードが正しく機能するために必要なISDNオプションを設定します。

図 38.5　ISDNの設定

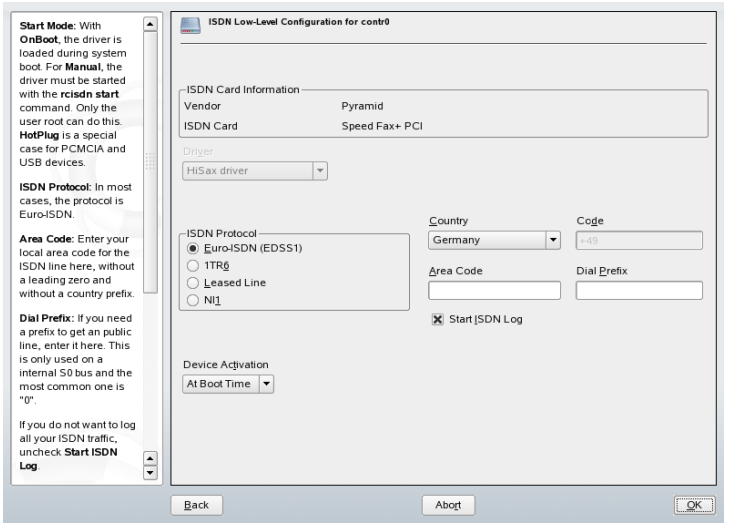


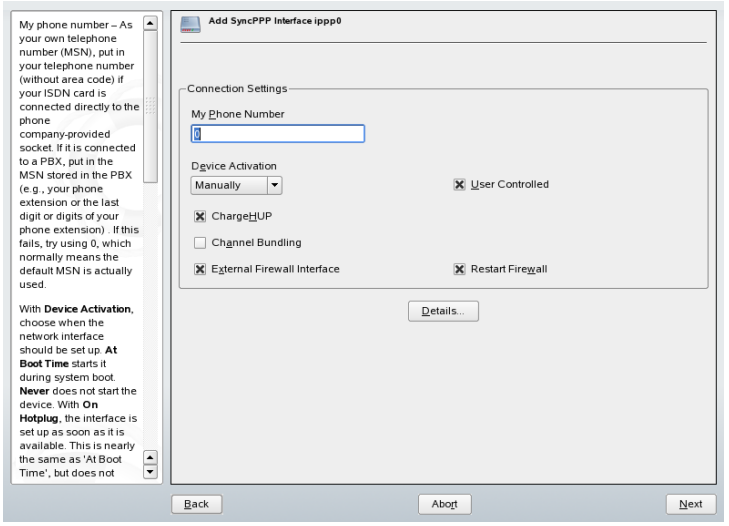
図 38.5. 「ISDNの設定」 (page 635)に示すダイアログでは、使用するプロトコルを選択します。デフォルトは、［*Euro-ISDN (EDSS1)*］ですが、旧式または

大型の交換機の場合は、［*1TR6*］を選択します。米国では、［*NI1*］を選択します。関連するフィールドで国を選択してください。隣接するフィールドに対応する国コードが表示されます。 最後に、必要に応じて［*Area Code (市外局番)*］［*Dial Prefix (ダイヤルプレフィックス)* を入力します。

［*実行モード*］では、ISDNインタフェースの起動方法を定義します。 ［*At Boot Time*］を選択すると、システムをブートするたびにISDNドライバが初期化されます。 ［*Manually*］を選択した場合は、`root`として`rcisdn start`コマンドを実行して、ISDNドライバをロードする必要があります。 ［*On Hotplug*］は、PCMCIAやUSBデバイスに使用します。デバイスを装着したときにドライバがロードされます。 これらの設定がすべて完了したら、［*OK*］をクリックします。

次のダイアログでは、ISDNカードのインタフェースタイプを指定し、既存のインタフェースにISPを追加します。インタフェースタイプには、`SyncPPP`または`RawIP`のどちらかを指定できますが、たいていのISPは、`SyncPPP`モードで運用しています。このモードについては後述します。

図 38.6　ISDNインタフェースの設定



［*自分の電話番号*］に入力する番号は、次の設定によって異なります。

電話線引出口に直接接続されたISDNカード

標準のISDN回線では、3つの電話番号を使用できます(MSN(multiple subscriber number)と呼ばれる)。 加入者が望めば、最大10の電話番号を付与できます。 ここには、いずれか1つのMSNを市外局番なしで入力します。間違った番号を入力すると、お使いのISDN回線に付与された最初のMSNが、電話交換手によって自動的に使用されます。

PBXに接続されたISDNカード

この場合も、設定方法は設置された装置によって異なります。

1. 小型のPBX (private branch exchanges)ではたいてい、内線通話にEuro-ISDN (EDSS1)プロトコルを使用します。これらの交換機にはS0バスが内蔵されており、交換機に接続された装置に内線番号を付与します。

   内線番号の1つをMSNとして使用してください。外線用に付与されたMSNの少なくとも1つは内線用に使用できるはずです。もし使用できない場合は、1つのゼロを試してください。詳細については、交換機付属のマニュアルを参照してください。

2. ビジネス向けに設計された大型の交換機では通常、内線通話に1TR6プロトコルを使用します。このタイプの交換機に付与されるMSNはEAZと呼ばれ、通常直通番号に対応しています。Linuxでの設定では、EAZの最後の数字を入力するだけで十分なはずです。どうしてもうまくいかない場合は、1から9までの数字をすべて試してみてください。

次回の課金単位の直前に接続を切断するようにする場合は、［*ChargeHUP(課金HUP)*］を有効にします。ただし、このオプションはすべてのISPで使用できるわけではないため注意してください。 チャネルバンドル(マルチリンクPPP)を有効にするオプションも用意されています。 最後に、使用している回線でSuSEfirewall2を有効にするには、［*External Firewall Interface*］と［*Restart Firewall*］を選択します。管理者権限のない通常のユーザがインタフェースの有効化と無効化を行えるようにするには、［*ユーザコントロール*］を選択します。

［*詳細*］を選択すると、詳細な接続方式を実装するためのダイアログが開きます。 ただし、これらの設定は、通常の個人ユーザには不要です。 ［*OK*］をクリックして［*Details*］ダイアログを閉じます。

次のダイアログでは、IPアドレスを設定します。プロバイダからスタティックなIPアドレスを与えられていない場合は、［*ダイナミックIPアドレス*］を選択します。スタティックなIPアドレスを与えられている場合は、ISPの指示

に従って、ホストのローカルIPアドレスとリモートIPアドレスを該当するフィールドに入力します。このインタフェースをインターネットへのデフォルトルートにする必要がある場合は、［デフォルトルート］を選択します。各ホストは、デフォルトルートとして設定されたインタフェースを1つだけ持つことができます。［次へ］をクリックして次のダイアログに進みます。

次のダイアログでは、国を設定し、ISPを選択できます。リストに登録されているISPは、call-by-callプロバイダだけです。契約しているISPがリストに登録されていない場合は、［*新規*］を選択します。［*プロバイダパラメータ*］ダイアログが開き、契約しているISPの詳細な情報を入力できます。電話番号を入力するときは、各数字の間に空白やコンマを挿入しないように注意してください。最後に、ISPから提供されたログインIDとパスワードを入力します。入力したら、［次へ］をクリックします。

スタンドアロンワークステーションで［*必要に応じてダイヤルする*］を使用するには、ネームサーバ(DNSサーバ)も指定します。ほとんどのISPはダイナミックDNSをサポートしており、接続するたびにISPからネームサーバのIPアドレスが送信されます。ただし、単一ワークステーションの場合は、`192.168.22.99`のようなプレースホルダアドレスを入力してください。ISPがダイナミックDNSをサポートしていない場合は、ISPから提供されたネームサーバIPアドレスを入力します。必要に応じて、接続タイムアウト、すなわち、ネットワークがアイドル状態になってから接続を自動的に切断するまでの時間(秒)を指定します。［次へ］をクリックすると設定が確定し、YaSTは、設定されたインタフェースの概要を表示します。すべての設定を有効にするには、［完了］を選択します。

38.4.4 ケーブルモデム

オーストリアや米国など、一部の国では、ケーブルテレビネットワークを介したインターネット接続が広く普及しています。ケーブルテレビ加入者は通常、モデムを貸与されます。このモデムは、ケーブルテレビの引出線とネットワークカード(10Base-TGより対線を使用)に接続して使用します。ケーブルモデムを接続すると、固定IPアドレスが付与されたインターネット専用接続が提供されます。

契約しているISPから、ネットワークカードを設定する際に、［*自動アドレス設定(DHCPを介して)*］または［*スタティックなアドレスの設定*］のどちらかを選択するように指示があります。最近では、大半のプロバイダがDHCPを使

用しています。スタティックなIPアドレスは、多くの場合、特殊なビジネス用アカウントの一部として提供されます。

38.4.5 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］セクションから［*DSL*］モジュールを選択します。このモジュールは、次のいずれかのプロトコルに基づいてDSLリンクのパラメータを設定する複数のダイアログで構成されます。

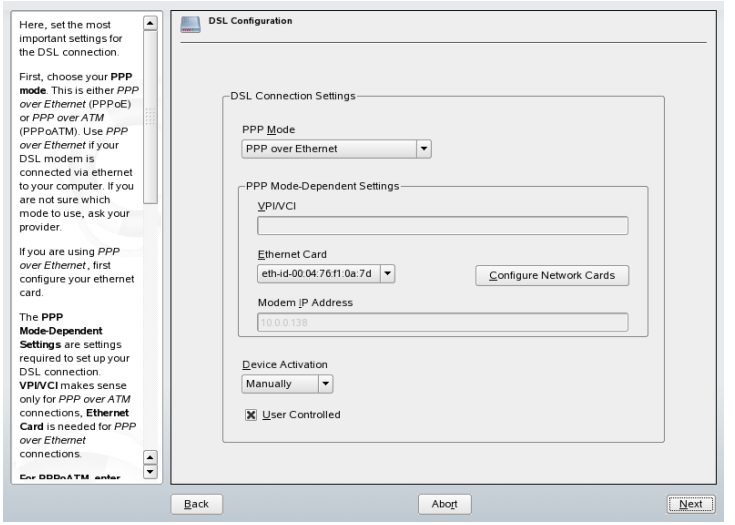
- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoATM)
- CAPI for ADSL (Fritz Cards)
- ポイントツーポイントトンネリングプロトコル(PPTP)—オーストリア

PPPoEまたはPPTPに基づくDSL接続を設定するには、対応するネットワークカードが正しく設定されている必要があります。ネットワークカードをまだ設定していない場合は、まず、［*ネットワークカードの設定*］を選択してカードを設定してください(項38.4.1.「YaSTでのネットワークカードの設定」(page 630)参照)。DSLリンクの場合は、IPアドレスが自動的に割り当てられる場合もありますが、その場合でもDHCPは使用されません。そのため、［*自動アドレス設定(DHCPを介して)*］オプションを有効にしないでください。その代わり、スタティックなダミーアドレス(`192.168.22.1`など)をインタフェースに入力します。［サブネットマスク］には、「`255.255.255.0`」を入力します。スタンドアロンのワークステーションを設定する場合は、［デフォルトゲートウェイ］を空白のままにします。

ティップ

［*IPアドレス*］と［サブネットマスク］の値は単なるプレースホルダーです。これらはネットワークカードを初期化するために必要なだけであって、実際のDSLリンクを表しているわけではありません。

図 38.7　DSLの設定



DSLの設定を始めるには(図 38.7. 「DSLの設定」 (page 640)参照)、まず、PPPモードと、DSLモデムが接続されるイーサネットカードを選択します(ほとんどの場合、`eth0`)。次に、［*デバイスの起動*］で、ブート時にDSLリンクを確立する必要があるかどうかを指定します。管理者権限のない通常のユーザがインタフェースの有効化と無効化を行えるようにするには、［ユーザコントロール］を選択します。このダイアログでは、国とその国で提供されている多くのISPの1つを選択できます。以降のダイアログの詳細は、ここまでで設定したオプションによって異なるため、簡単に触れるだけにとどめておきます。各オプションの詳細については、各ダイアログのヘルプを参照してください。

スタンドアロンワークステーションで［*必要に応じてダイヤルする*］を使用するには、ネームサーバ(DNSサーバ)も指定します。ほとんどのISPはダイナミックDNSをサポートしており、接続するたびにISPからネームサーバのIPアドレスが送信されます。ただし、単一ワークステーションの場合は、`192.168.22.99`のようなプレースホルダアドレスも入力する必要があります。ISPがダイナミックDNSをサポートしていない場合は、ISPのネームサーバIPアドレスを指定してください。

［*切断するまでのアイドル時間(秒数)*］には、ネットワークがアイドル状態になってからモデムを自動的に切断するまでの時間を指定します。 タイムアウ

ト値としては、60秒～300秒が妥当です。［*必要に応じてダイヤルする*］を無効にしている場合は、このタイムアウト値をゼロに設定して自動的に接続が切断されないようにしておきます。

T-DSLの設定はDSLの設定とほぼ同じです。プロバイダとして［*T-Online*］を選択すると、T-DSL設定ダイアログが開きます。このダイアログで、T-DSLに必要な追加情報(ラインID、T-Online番号、ユーザコード、パスワードなど)を指定します。T-DSLに加入すると、プロバイダからこれらの情報がすべて提供されるはずです。

38.5 ネットワークの手動環境設定

ネットワークソフトウェアの手動環境設定は、常に最後の手段です。 設定には可能な限りYaSTを使用してください。 しかし、ネットワークの環境設定に関する背景知識がYaSTでの設定作業に役立つことがあります。

すべての内蔵式のネットワークカードおよびホットプラグのネットワークカード(PCMCIA、USB、一部のPCIカード)は、hotplugによって検出され、設定されます。ネットワークカードの 2 つの側面システムは、ネットワークカードを物理デバイスとインタフェースという 2 つの見方で捉えます。デバイスが挿入または検出されると、ホットプラグイベントが生成されます。 このホットプラグイベントによって、`hwup`スクリプトが実行され、デバイスが初期化されます。ネットワークカードが新しいネットワークインタフェースとして初期化されると、カーネルによって別のホットプラグイベントが生成され、それにより `/sbin/ifup`が実行されてインタフェースがセットアップされます。

カーネルは、登録順に従ってインタフェース名に番号を付けます。割り当てられる名前は、初期化の順序によって決まります。あるネットワークカードの初期化に失敗した場合、その後に初期化されるカードの番号は1つずつずらされます。実際のホットプラグ対応カードでは、デバイスを接続する順序が重要になります。

柔軟な環境設定を可能にするために、デバイス(ハードウェア)の環境設定とインタフェースの環境設定は切り分けられ、デバイスの環境設定とインタフェースの環境設定のマッピングをインタフェース名で管理する方式は廃止されました。デバイスの環境設定は、 `/etc/sysconfig/hardware/hwcfg-*`に格納されます。インタフェースの環境設定は、 `/etc/sysconfig/network/`

ifcfg-*に格納されます。これらの環境設定ファイルには、そのファイルに関連付けられるデバイスまたはインタフェースを表す名前が付けられます。ドライバをインタフェース名にマッピングする従来の方式では静的なインタフェース名が必要なため、このマッピングを/etc/modprobe.confで行うことはできなくなりました。この新しい方式では、このファイルにエイリアスエントリが設定されていると、好ましくない副作用が発生することがあります。

環境設定名、すなわち、hwcfg-またはifcfg-の後の部分では、スロット、デバイス固有のID、インタフェース名などでデバイスを表します。たとえば、PCIカードの環境設定名は、bus-pci-0000:02:01.0 (PCIスロット)、vpid-0x8086-0x1014-0x0549 (メーカー名と製品ID)などになります。対応するインタフェース名は、bus-pci-0000:02:01.0、wlan-id-00:05:4e:42:31:7a (MACアドレス)などになります。

特定のカードではなく特定のタイプのカードにネットワークの環境設定を割り当てる場合は(ただし、同じタイプのカードを同時に2枚以上は装着しない)、もう少し汎用的な設定名を選択します。たとえば、すべてのPCMCIAカードに対してbus-pcmciaという設定名を使用できます。一方、先頭にインタフェースタイプが付いた限定的な設定名も使用できます。たとえば、USBポートに接続するWLANカードにはwlan-bus-usbという設定名を付けることができます。

システムは常に、インタフェースまたはそのインタフェースを提供するデバイスに最適な環境設定を使用します。 最適な環境設定の検索は、getcfgによって行われます。getcfgの出力には、デバイスを記述するために使用できるすべての情報が含まれています。環境設定名の指定の詳細については、getcfgのマニュアルページを参照してください。

この方法により、ネットワークデバイスは常に同じ順序で初期化されるとは限りませんが、ネットワークインタフェースは適切に設定されます。ただし、インタフェース名は、やはり初期化の順序によって決まります。特定のネットワークカードのインタフェースに確実にアクセスするには、次の2とおりの方法があります。

- getcfg-interface*configuration name*を実行すると、対応するネットワークインタフェース名が返されます。 したがって、一部の環境設定ファイルでは、ファイアウォール、dhcpd、ルーティング、各種仮想ネッ

トワークインタフェース(トンネル)などの設定名を、固定的でないインタフェース名の代わりに指定できます。

- 環境設定にインタフェース名が含まれていないすべてのインタフェースには、固定的なインタフェース名を割り当てることができます。これを行うには、インタフェース設定 (`ifcfg-*`) の `PERSISTENT_NAME=`*pname* という名前のエントリを使用します。ただし、固定名*pname*は、カーネルによって自動的に割り当てられる名前とは異なっていなければなりません。そのため、`eth*`、`tr*`、`wlan*`などの名前は使用できません。このような名前ではなく、`net*`または`external`、`internal`、`dmz`.などの説明的な名前を使用します。固定名は、登録直後にのみインタフェースに割り当てることができます。つまり、ネットワークカードのドライバを再ロードするか、`hwup`*デバイス記述*を実行する必要があります。`rcnetworkrestart`コマンドを実行するだけでは不十分です。

重要項目: 固定的なインタフェース名の使用について

固定的なインタフェース名の使用は、一部の領域ではテストされていません。したがって、アプリケーションによっては、自由に選択したインタフェース名を使用できないことがあります。

`ifup`はハードウェアを初期化しないため、すでに存在しているインタフェースを必要とします。ハードウェアの初期化は、`hwup`コマンドによって行われます(このコマンドは`hotplug`または`coldplug`によって実行されます)。デバイスが初期化されると、`hotplug`によって`ifup`が新しいインタフェースに対して自動的に実行され、実行モードが`onboot`、`hotplug`、または`auto`であり`network`サービスが既に起動していれば、インタフェースがセットアップされます。従来は、`ifup`*interfacename*コマンドによってハードウェアの初期化が行われていましたが、新しいバージョンでは処理順序が逆になりました。まず、ハードウェアコンポーネントを初期化してから、その他の処理が行われます。この方法により、可変数のデバイスを、既存の環境設定を用いてできる限り最適な方法で設定できます。

表 38.5.「手動ネットワーク環境設定用スクリプト」 (page 644)に、ネットワークの環境設定関連の最も重要なスクリプトをまとめます。各スクリプトはハードウェアとインタフェースに分類してあります。

表 38.5　手動ネットワーク環境設定用スクリプト

環境設定段階	コマンド	機能
ハードウェア	`hw{up,down,status}`	`hw*`スクリプトは、ホットプラグサブシステムによって実行され、デバイスの初期化、初期化の取り消し、デバイスのステータスの問い合わせを行います。詳細は、`hwup`のマニュアルページを参照してください。
インタフェース	`getcfg`	`getcfg`は、環境設定名またはハードウェア記述に対応するインタフェース名の問い合わせに使用します。詳細は、`getcfg`のマニュアルページを参照してください。
インタフェース	`if{up,down,status}`	`if*`スクリプトは、既存のネットワークインタフェースを起動したり、指定のインタフェースのステータスを表示したりします。詳細は、`ifup`のマニュアルページを参照してください。

ホットプラグおよび固定的なデバイス名の詳細については、章 32. *ホットプラグシステム* (page 539)および章 33. *udevをもつ動的デバイスノード* (page 547)を参照してください。

38.5.1　環境設定ファイル

ここでは、ネットワークの環境設定ファイルの概要を紹介し、その目的と使用される形式について説明します。

/etc/syconfig/hardware/hwcfg-*

これらのファイルには、ネットワークカードおよびその他のデバイスのハードウェアの環境設定が記述されています。これには、カーネルモジュール、実行モード、スクリプトの関連付けなどの必要なパラメータが含まれます。詳細については、hwupのマニュアルページを参照してください。存在しているハードウェアとは無関係に、coldplugの起動時にはhwcfg-static-*が適用されます。

/etc/sysconfig/network/ifcfg-*

これらのファイルには、ネットワークインタフェースの環境設定が記述されています。これには、実行モード、IPアドレスなどが含まれます。指定可能なパラメータについては、ifupのマニュアルページを参照してください。また、一般的設定を1つのインタフェースだけに使用する場合は、dhcp、wireless、およびconfigの各ファイルにあるすべての変数が、ifcfg-*ファイルで使用されます。

/etc/sysconfig/network/config, dhcp, wireless

configファイルには、ifup、ifdown、およびifstatusの動作に関する汎用的な設定が記述されています。また、dhcpにはDHCPの設定が、wirelessには無線LANカードの設定が記述されています。これら3つの環境設定ファイルの変数にはコメントが付けられており、優先度の高い変数としてifcfg-*ファイルでも使用できます。

/etc/sysconfig/network/routes,ifroute-*

TCP/IPパケットの静的ルーティングが設定されています。 各種システムタスクで必要となるすべての静的経路(ホストへの経路、ゲートウェイを介したホストへの経路、ネットワークへの経路)は、 /etc /sysconfig /network/routesファイルに指定します。 個別のルーティングを必要とする各インタフェースには、追加の環境設定ファイル /etc /sysconfig /network/ifroute-*を定義します。*はインタフェース名で読み替えてください。経路の環境設定ファイルのエントリは次のようになります。

```
# Destination     Dummy/Gateway     Netmask            Device
 #
 127.0.0.0         0.0.0.0           255.255.255.0      lo
 204.127.235.0     0.0.0.0           255.255.255.0      eth0
 default           204.127.235.41    0.0.0.0            eth0
 207.68.156.51     207.68.145.45     255.255.255.255    eth1
 192.168.0.0       207.68.156.51     255.255.0.0        eth1
```

第1列は、経路の宛先です。この列には、ネットワークまたはホストのIPアドレスが入ります。*到達可能*なネームサーバの場合は、完全に修飾されたネットワークまたはホスト名が入ります。

第2列は、デフォルトゲートウェイ、すなわちホストまたはネットワークにアクセスする際に経由するゲートウェイです。第3列は、ゲートウェイの背後にあるネットワークまたはホストのネットマスクです。たとえば、ゲートウェイの背後にあるホストのネットマスクは、255.255.255.255になります。

最後の列は、ローカルホスト(ループバック、イーサネット、ISDN、PPP、ダミーデバイスなど)に接続されたネットワークのみに関連します。ここには、デバイス名を指定する必要があります。

(オプションの) 5番目のコラムには、経路のタイプを指定することができます。必要ではないコラムには、マイナス記号-を記述してください。これは、パーサがコマンドを正しく解釈できるようにするためです。 詳細は、routes(5) manページを参照してください。

/etc/resolv.conf

このファイルには、ホストが属するドメインが指定されています(キーワードsearch)。また、アクセスするネームサーバアドレスのステータスのリストも記述されています（キーワードnameserver）。ドメイン名は複数指定することができます。完全修飾でない名前を解決する場合は、searchの各エントリを付加して完全修飾名の生成が試みられます。複数のネームサーバを使用するには、nameserverで始まる行を複数行入力します。/etc/resolv.confコメントは#記号の後に記入します。YaSTは、指定されているネームサーバをこのファイルに記述します。例 38.5. 「/etc/resolv.conf」 (page 647)に/etc/resolv.confの例を示します。

例 38.5 /etc/resolv.conf

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

pppd (wvdial)、ipppd (isdn)、dhcp (dhcpcd、dhclient)、pcmcia、hotplugなどの一部のサービスは、スクリプトmodify_resolvconfを使用してファイル/etc/resolv.confに変更を加えます。ファイル/etc/resolv.confがこのスクリプトによって一時的に変更された場合、変更を加えたサービス、元のファイルがバックアップされている場所、および自動変更メカニズムを無効にする方法を示す事前定義のコメントが付されます。/etc/resolv.confが複数回変更された場合、ファイルには変更内容がネスト形式で保存されます。変更が行われた順序と異なる順序で復元を行った場合も、問題なく元通りに復元できます。このような柔軟性を必要とするサービスには、isdn、pcmcia、およびhotplugがあります。

サービスが通常のクリーンな状態で停止しなかった場合、modify_resolvconfを使用して元のファイルを復元することができます。また、システムブート時に、クリーンアップされていない変更されたresolv.confが存在しないかがチェックされ(たとえば、システムクラッシュがあった場合)、存在する場合は、元の(変更されていない) resolv.confが復元されます。

YaSTは、modify_resolvconf checkコマンドを使用して、resolv.confが変更されているかどうかを確認し、ユーザに対してファイルの復元後は変更内容が失われることを警告します。YaSTはこれ以外の作業でmodify_resolvconfに依存しないため、YaSTを使用してresolv.confを変更した場合の影響は、手動で変更した場合と同じです。どちらの場合も、変更は永久に有効です。一方、前述のサービスによって要求された変更は、一時的に有効なだけです。

/etc/hosts

このファイル(例 38.6. 「/etc/hosts」 (page 648)を参照)では、IIPアドレスがホスト名に割り当てられています。ネームサーバが実装されていない場合は、IP接続をセットアップするすべてのホストをここにリストする必要があります。ファイルには、各ホストについて1行を入力し、IPアドレス、完全修飾ホスト名、およびホスト名を指定します。IPアドレスは、行頭に指定し、各エ

ントリはブランクとタブで区切ります。コメントは常に#記号の後に記入します。

例 38.6　/etc/hosts

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.0 earth.example.com earth
```

/etc/networks

このファイルには、ネットワーク名とネットワークアドレスの対応が記述されています。形式は、ネットワーク名をアドレスの前に指定すること以外は、hostsファイルと同様です。例 38.7.「/etc/networks」 (page 648)を参照してください。

例 38.7　/etc/networks

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

このファイルは、名前解決(*resolver*ライブラリによるホスト名とネットワーク名の変換)を制御します。このファイルは、libc4またはlibc5にリンクされているプログラムについてのみ使用されます。最新のglibcプログラムについては、/etc/nsswitch.confの設定を参照してください。パラメータは、その行内で常に独立しています。コメントは#記号の後に記入します。表 38.6.「/etc/host.confファイルのパラメータ」 (page 648)に、利用可能なパラメータを示します。/etc/host.confの例については、例 38.8.「/etc/host.conf」 (page 649)を参照してください。

表 38.6　/etc/host.confファイルのパラメータ

hosts、*bind*の順序	名前の解決の際、サービスがアクセスされる順序を指定します。有効な引数は次のとおりです(空白またはカンマで区切ります)。 *hosts*: /etc/hostsファイルを検索します。

	bind:ネームサーバにアクセスします。 *nis*:NISを経由します。
multi *on*/*off*	/etc/hostsに指定されているホストが、複数のIPアドレスを持てるかどうかを定義します。
nospoof *on* spoofalert *on*/*off*	これらのパラメータは、ネームサーバ*spoofing*に影響を与えますが、それ以外のネットワークの環境設定に対してまったく影響を与えません。
trim *domainname*	ホスト名が解決された後、指定したドメイン名をホスト名から切り離します(ホスト名にドメイン名が含まれている場合)。このオプションは、ローカルドメインにある名前だけが/etc/hostsファイルに指定されているが、付加されるドメイン名でも認識する必要がある場合に便利です。

例 38.8 /etc/host.conf

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

/etc/nsswitch.conf

GNU C Library 2.0を導入すると、*Name Service Switch* (NSS)も合わせて導入されます。詳細については、nsswitch.conf(5) manページおよび『*The GNU C Library Reference Manual*』を参照してください。

クエリの順序は、ファイル/etc/nsswitch.confで定義します。nsswitch.confの例については、例 38.9.「/etc/nsswitch.conf」 (page 650)を参照してください。コメントは#記号の後に記入します。この例では、hostsデータベースのエントリによると、要求がDNS (章 40. ドメインネームシステム (page 661)を参照)経由で/etc/hosts (files)に送信されています。

例 38.9　/etc/nsswitch.conf

```
passwd:compat
group:compat

hosts:files dns
networks:files dns

services:db files
protocols:db files

netgroup:files
automount:  files nis
```

NSSで利用できる「データベース」については、表38.7.「/etc/nsswitch.confで利用できるデータベース」 (page 650)を参照してください。それらに加えて、automount、bootparams、netmasks、およびpublickeyが近い将来導入される予定です。 NSSデータベースの環境設定オプションについては、表38.8.「NSS「データベース」の環境設定オプション」 (page 651)を参照してください。

表 38.7　/etc/nsswitch.confで利用できるデータベース

aliases	sendmailによって実行されたメールエイリアス。man5 aliasesコマンドで、マニュアルページを参照してください。
ethers	イーサネットアドレス
group	getgrentがユーザグループを調べるとき使用します。groupのマニュアルページも参照してください。
hosts	gethostbynameおよび同様の関数が、ホスト名とIPアドレスを取得するために使用します。
netgroup	アクセス許可を制御するための、ネットワーク内にある有効なホストとユーザのリスト。netgroup(5)manページを参照してください。
networks	ネットワーク名とアドレス。getnetentによって使用されます。

passwd	ユーザパスワード。getpwentによって使用されます。passwd(5) manページを参照してください。
protocols	ネットワークプロトコル。getprotoentによって使用されます。protocols(5) manページを参照してください。
rpc	リモートプロシージャコール名とアドレス。getrpcbynameおよび同様の関数によって使用されます。
services	ネットワークサービス。getserventによって使用されます。
shadow	ユーザのシャドウパスワード。getspnamによって使用されます。shadow(5) manページを参照してください。

表 38.8　NSS「データベース」の環境設定オプション

files	たとえば/etc/aliasesのような直接アクセスファイル。
db	データベース経由のアクセス。
nis、nisplus	NIS。章 41. *NISの使用* (page 683)を参照。
dns	hostsおよびnetworksの拡張としてのみ使用できます。
compat	passwd、shadowおよびgroupの拡張としてのみ使用できます。

/etc/nscd.conf

このファイルは、nscd (name service cache daemon)の環境設定に使用します。nscd(8)およびnscd.conf(5) manページを参照してください。デフォルトでは、nscdによってpasswdとgroupsのシステムエントリがキャッシュされ

ます。 キャッシュが行われないと名前やグループにアクセスするたびにネットワーク接続が必要になるため、このキャッシュ処理はNISやLDAPといったディレクトリサービスのパフォーマンスに関して重要な意味を持ちます。hostsはデフォルトではキャッシュされません。これは、nscdでホストをキャッシュすると、ローカルシステムで正引き参照と逆引き参照のルックアップチェックを信頼できなくなるからです。したがって、nscdを使用して名前をキャッシュするのではなく、キャッシュDNSサーバをセットアップします。

passwdオプションのキャッシュを有効にすると、新しく追加したローカルユーザが認識されるまで、通常、約15秒かかります。この待ち時間を短縮するには、コマンドrcnscdrestartを使用してnscdを再起動します。

/etc/HOSTNAME

このファイルには、ドメイン名の付いていないホスト名が記述されています。このファイルは、マシンの起動時に複数のスクリプトによって読み込まれます。指定できるのは、ホスト名が設定されている1行のみです。

38.5.2 スタートアップスクリプト

前述の環境設定ファイルに加え、マシンのブート時にネットワークプログラムをロードするさまざまなスクリプトも用意されています。 これらは、システムがマルチユーザランレベルのいずれかに切り替わったときに起動します(表 38.9.「ネットワークプログラム用スタートアップスクリプト」 (page 652)も参照)。

表 38.9 ネットワークプログラム用スタートアップスクリプト

/etc/init.d/network	このスクリプトは、ネットワークインタフェースの環境設定を処理します。ハードウェアが事前に(hotplug経由で) /etc/init.d/coldplugによって初期化されている必要があります。networkサービスが起動していないと、ネットワークインタフェースは、ホットプラグ経由で挿入されたときに初期化されません。

/etc/init.d/inetd	xinetdを起動します。xinetdを使用すると、サーバサービスがシステム上で利用できるようになります。たとえば、FTP接続の開始時に必ずvsftpdを起動するといったことができます。
/etc/init.d/portmap	NFSサーバなどのRPCサーバに必要なポートマッパを起動します。
/etc/init.d/nfsserver	NFSサーバを起動します。
/etc/init.d/sendmail	sendmailプロセスを制御します。
/etc/init.d/ypserv	NISサーバを起動します。
/etc/init.d/ypbind	NISクライアントを起動します。

38.6 ダイアルアップアシスタントとしてのsmpppd

ほとんどのユーザは、インターネット接続専用の回線を持っていません。代わりにダイアルアップ接続を使用しています。接続は、ダイアルアップ方法(ISDNまたはDSL)に応じてipppdまたはpppdで制御されます。基本的には、これらのプログラムを正常に起動するだけでオンラインで接続できます。

ダイアルアップ接続時に追加費用が発生しない定額接続を使用している場合は、単に該当するデーモンを起動します。ダイアルアップ接続の管理には、KDEアプレットまたはコマンドラインインタフェースを使用します。インターネットゲートウェイ以外のホストを使用している場合は、ネットワークホスト経由でダイアルアップ接続を管理できます。

smpppdが関係するのはこの部分です。このプログラムは補助プログラム用に一様なインタフェースを提供し、双方向に動作します。第1に、必要なpppdまたはipppdをプログラミングし、そのダイアルアッププロパティを制御します。第2に、各種プロバイダをユーザプログラムで使用できるようにして、現在の

接続ステータスに関する情報を送信します。smpppdはネットワーク経由で制御することもできるため、プライベートサブネットワーク内のワークステーションからインターネットへのダイアルアップ接続の制御に適しています。

38.6.1 smpppdの設定

smpppdによる接続は、YaSTにより自動的に設定されます。実際のダイアルアッププログラムであるkinternetとcinternetも事前に設定済みです。手動設定が必要となるのは、リモート制御など、smpppdの付加的機能を設定する場合のみです。

smpppdの設定ファイルは/etc/smpppd.confです。デフォルトでは、このファイルによるリモート制御はできません。この設定ファイルの最も重要なオプションを次に示します。

open-inet-socket = *yes|no*
: smpppdをネットワーク経由で制御するには、このオプションをyesに設定する必要があります。smpppdがリスンするポートは3185です。このパラメータをyesに設定した場合は、パラメータbind-address、host-rangeおよびpasswordもそれに応じて設定する必要があります。

bind-address = *ip*
: ホストに複数のIPアドレスがある場合は、このパラメータを使用してsmpppdで接続の受け入れに使用するIPアドレスを指定します。

host-range = *min ip max ip*
: パラメータhost-rangeを使用して、ネットワーク範囲を定義します。この範囲内のIPアドレスを持つホストには、smpppdへのアクセス権が付与されます。この範囲外のホストはすべてアクセスを拒否されます。

password = *password*
: パスワードを割り当てることで、クライアントを認可されたホストに限定できます。これはプレーンテキストによるパスワードのため、このパスワードによるセキュリティを過大評価しないでください。パスワードを割り当てないと、すべてのクライアントがsmpppdへのアクセスを許可されます。

slp-register = *yes|no*
このパラメータにより、smpppdサービスがSLPによってネットワーク上にアナウンスされます。

smpppdについての詳細は、`smpppd(8)`および`smpppd.conf(5)` manページを参照してください。

38.6.2 リモートで使用するための kinternet、cinternet、および qinternetの設定

kinternet、cinternet、およびqinternetは、ローカルに使用できるのみではなく、リモートsmpppdの制御にも使用できます。cinternetとはグラフィカルなkinternetに相当するコマンドラインプログラムです。qinternetは基本的にはkinternetと同じですが、KDEライブラリを使用しません。そのためKDEなしで使用することができ、また個別にインストールする必要があります。これらのユーティリティをリモートsmpppdに使用するには、設定ファイル`/etc/smpppd-c.conf`を手動で、またはkinternetを使用して編集します。このファイルでは、以下の3つのオプションのみを使用します。

sites = *list of sites*
このオプションでは、フロントエンドがsmpppdを検索する場所を指定します。フロントエンドは、ここに記述されている順序でオプションをテストします。オプション`local`はローカルsmpppdへの接続の確立を指示します。`gateway`はゲートウェイ上のsmpppdをポイントします。接続は、`config-file`の`server`の指定に従って確立する必要があります。`slp`は、フロントエンドに対してSLPによって検出されたsmpppdに接続するよう指示します。

server = *server*
このオプションでは、smpppdを実行するホストを指定します。

password = *password*
このオプションでは、smpppd用に選択したパスワードを挿入します。

smpppdがアクティブな場合は、これでコマンド`cinternet --verbose --interface-list`などのコマンドを使用してアクセスを試行できます。

この時点でアクセスできない場合は、smpppd-c.conf(5)および
cinternet(8) manページを参照してください。

39 ネットワーク上のSLPサービス

サービスロケーションプロトコル(SLP)は、ローカルネットワークに接続されているクライアントの構成を簡略化するために開発されました。ネットワーククライアントを設定するには、すべての必要なサービスを含め、管理者はネットワークで利用できるサーバに関する詳しい知識が必要とされました。SLPは、ローカルネットワーク上にあるすべてのクライアントに対して特定のサービスを利用できることを通知します。このような通知情報を利用してSLPをサポートする各種アプリケーションを自動的に設定することができます。

SUSE Linusは、SLPによって提供されるインストールソースを使用するインストールをサポートしています。また、多くのシステムサービスは、統合SLPをサポートしています。 YaSTとKonquerorは、どちらもSLP用の適切なフロントエンドを持っています。 SUSE Linuxでインストールサーバ、YOUサーバ、ファイルサーバ、印刷サーバなどのSLPを使用することにより、ネットワークに接続されたクライアントに一元的な管理機能を提供します。

39.1 独自のサービスを登録する

SUSE Linuxのアプリケーションの多くは`libslp`ライブラリを使用することで、最初から統合SLPをサポートしています。サービスがSLPサポートでコンパイルされていない場合は、SLPを利用できるように次の方法のいずれかを使用してください。

`/etc/slp.reg.d`による静的登録
新規サービスに個別の登録ファイルを作成します。次はスキャナサービスを登録するためのファイルの例です。

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

このファイルで最も重要な行は`service:`から開始するサービス*URL*です。このURLにはサービスタイプ(`scanner.sane`)および、サーバ上でサービスが使用可能になるアドレスが含まれます。*`$HOSTNAME`*は自動的に完全ホスト名で置き換えられます。その後ろにはサービスごとのTCPポートの名前がコロンで区切られる形で続きます。さらにサービスを表示する場合に使用される言語、登録の期間を秒単位で入力します。これらはコンマを使用してサービスURLと分けるようにします。`0`から`65535`で登録期間の値を設定します。`0`の場合は登録する必要がありません。`65535`はすべての制限を削除します。

登録ファイルにも、2つの変数である`watch-tcp-port`および`description`が含まれます。 watch-tcp-portは、slpdにサービスのステータスをチェックさせて、どの関連サービスがアクティブかをSLPサービス通知にリンクします。 descriptionには、適切なブラウザを使用している場合に表示される、さらに詳細なシステム名が含まれています。

`/etc/slp.reg`による静的登録
前述の手順と異なるのは、一元的なファイルですべてのサービスをグループ化している点です。

slptoolによる動的登録
専用のスクリプトからサービスをSLPに登録するには、slptoolコマンドラインフロントエンドを使用します。

39.2 SUSE LinuxのSLPフロントエンド

SUSE Linuxには複数のフロントエンドが含まれており、SLP情報がチェックされて、ネットワークで使用されるようにします。

slptool
slptoolはネットワーク上のSLP照会を通知するため、または適切なサービスを通知するために使用される単純なコマンドラインプログラムです。`slptool --help`はすべての利用可能なオプションと機能をリストします。slptoolはSLP情報を処理するスクリプトから呼び出すことができます。

YaSTのSLPブラウザ
YaSTには個別のSLPブラウザが含まれており、［*ネットワークサービス*］→［*SLPブラウザ*］で、SPLによって通知されたローカルネットワークのすべてのサービスがツリーダイアグラム形式でリストされます。

Konqueror
ネットワークブラウザとして使用される場合、Konquerorは`slp:/`のローカルネットワークで使用可能なすべてのSLPサービスを表示できます。メインウィンドウにあるアイコンをクリックして、関連サービスについての詳細情報を参照してください。Konquerorを`service:/`で使用する場合、ブラウザウィンドウで関連するアイコンをクリックして、選択したサービスとの接続をセットアップします。

39.3 SLPをアクティブ化する

サービスを提供する場合、システム上でslpdが実行している必要があります。サービスの照会を作成するだけの場合は、このデーモンを開始する必要はありません。 SUSE Linuxのほとんどのシステムサービスと同様、slpdデーモンは個別の初期化スクリプトを使用して制御されます。このデーモンはデフォルトで非アクティブになっています。セッション中にこのデーモンをアクティブにするには、`rcslpdstart`を`root`で実行してデーモンを開始し、`rcslpd stop`で終了します。`restart`で再始動、または`status`で状態チェックを実行します。slpdをデフォルトでアクティブにするには、`insservslpd`コマンドを`root`で、1度実行します。システムのブート時に開始するサービスセットとしてslpdが自動的に追加されます。

39.4 関連資料

次のソースではSLPについての詳しい情報が提供されています。

RFC 2608、2609、2610
一般的にRFC 2608はSLPの定義を取り扱います。RFC 2609は、使用されるサービスURLの構文を詳細に扱います。またRFC 2610ではSLPを使用したDHCPについて説明しています。

http://www.openslp.com
OpenSLPプロジェクトのホームページです。

file:/usr/share/doc/packages/openslp/*
このディレクトリには、SUSE Linuxの詳細、前述のRFC、および2つの入門用HTMLマニュアルが記載されている`README.SuSE`を含め、SLPに関する利用可能なマニュアルがすべて用意されています。SLPを使用するプログラマは`openslp-devel`パッケージをインストールし、その中で提供される『*Programmers Guide*』を確認してください。

40 ドメインネームシステム

DNS (ドメインネームシステム)は、ドメイン名とホスト名をIPアドレスに解決するために必要です。 これにより、たとえばIPアドレス192.168.0.0がホスト名`earth`に割り当てられます。独自のネームサーバをセットアップする前に、項38.3.「名前解決」 (page 628)でDNSに関する一般的な説明を参照してください。以降に示す設定例はBINDの場合のものです。

40.1 DNSの基本

40.2 YaSTでの設定

のDNSモジュールを使用すると、ローカルネットワーク用のDNSサーバを設定できます。このモジュールを初めて起動すると、サーバ管理に関して少数の基本的な事項を決定するように要求されます。この初期セットアップを完了すると、必要最低限の機能が設定された基本的なサーバ設定が生成されます。 エキスパートモードは、さらに高度な設定タスクを行う場合に使用できます。

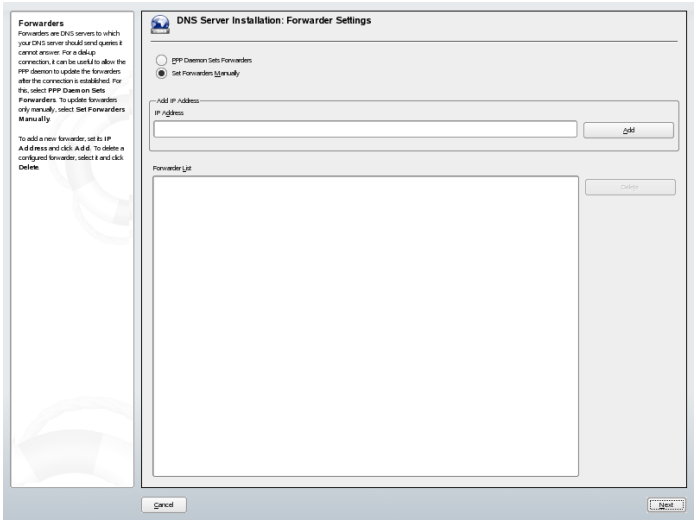
40.2.1 ウィザードによる設定

ウィザードは3つのステップ(ダイアログ)で構成されています。各ダイアログの適切な箇所でエキスパート用の設定モードに入ることができます。

フォワーダの設定

モジュールを初めて起動すると、図 40.1.「DNS サーバのインストール:フォワーダの設定」(page 662)のようなダイアログが表示されます。このダイアログでは、PPPデーモンがDSLまたはISDNを介してダイアルアップ時にフォワーダのリストを提供するか([*PPP*デーモンがフォワーダを設定する])、または独自のリストを指定するか([*手動*でフォワーダを設定する])を指定できます。

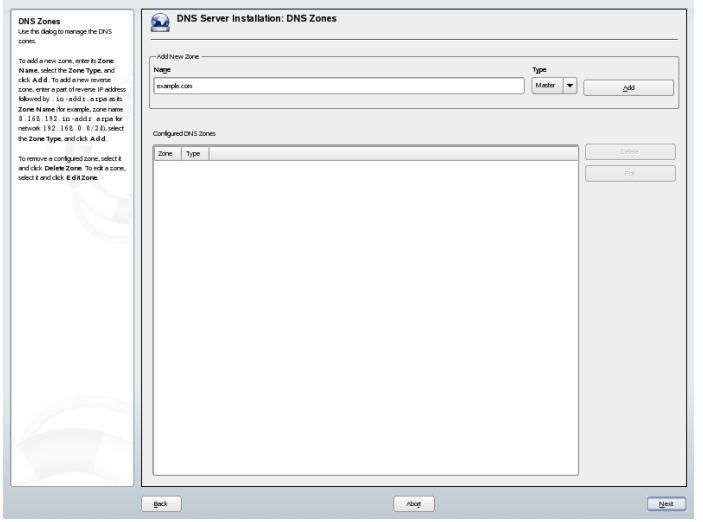
図 40.1　DNS サーバのインストール:フォワーダの設定



DNSゾーン

複数の部分で構成されるこのダイアログでは、項40.5.「ゾーンファイル」(page 676)で説明するゾーンファイルの管理に関する項目を設定します。新しいゾーンを作成する場合は、［ゾーン名］にその名前を入力します。逆引きゾーンを追加する場合は、`.in-addr.arpa`で終わる名前を入力しなければなりません。最後に、［ゾーンのタイプ］(マスターまたはスレーブ)を選択します。図 40.2.「DNS サーバのインストール:DNSゾーン」(page 663)を参照してください。既存のゾーンのその他の項目を設定するには、［ゾーンの*編集*］をクリックします。ゾーンを削除するには、［ゾーンの*削除*］をクリックします。

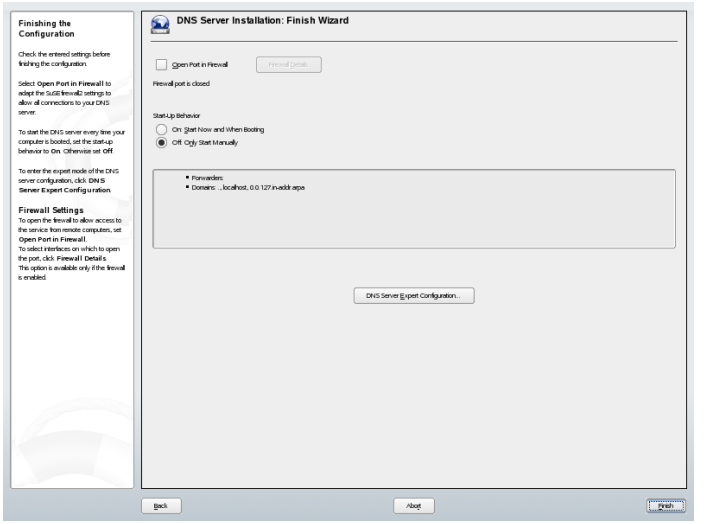
図 40.2　DNS サーバのインストール:DNSゾーン



ウィザードの完了

この最後のダイアログでは、インストール時にアクティブ化されるファイアウォールのDNSサービス用ポートを開いて、DNSを起動するかどうかを決定します。このダイアログからもエキスパート用の設定に入ることができます。図40.3.「DNSサーバのインストール:ウィザードの完了」 (page 664)を参照してください。

図 40.3　DNS サーバのインストール: ウィザードの完了



40.2.2　エキスパート設定

YaSTのモジュールを起動するとウィンドウが開き、複数の設定オプションが表示されます。設定を完了すると、基本的な機能が組み込まれたDNSサーバ設定が作成されます。

起動

［*Booting*］では、DNSサーバをシステムのブート時(システムのブート中)に起動するか、それとも手動で起動するかを指定します。DNSサーバをすぐに起動するには、［*Start DNS Server Now*］を選択します。DNSサーバを停止するには、［*DNSサーバの停止*］を選択します。現在の設定を保存するには、［*設定を保存してDNSを再起動*］を選択します。ファイアウォールのDNSポートを開くには［*ファイアウォールで開いているポート*］を、ファイアウォールの設定を変更するには［*ファイアウォールの詳細*］をクリックします。

フォワーダ

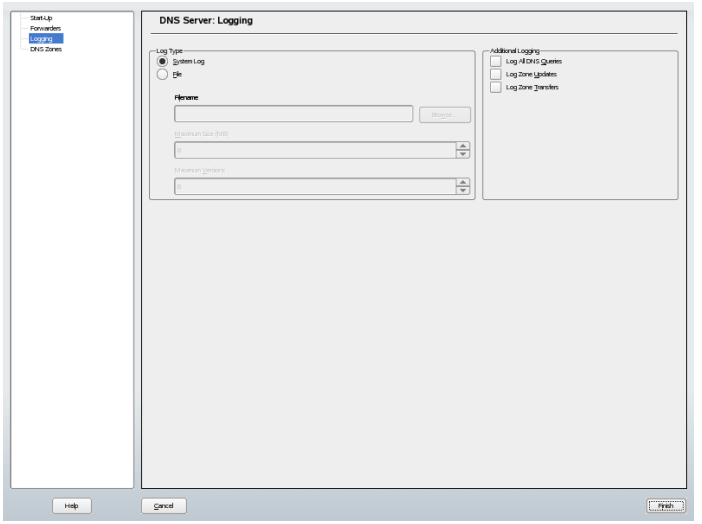
これは、ウィザードの設定を起動したときに開くダイアログと同じです(フォワーダの設定 (page 662)を参照)。

ログ

このセクションでは、DNSサーバがログに記録する内容とログの方法を設定できます。［*ログタイプ*］に、DNSサーバがログデータを書き込む場所を指定します。システム全体のログファイル［`/var/log/messages`］を使用する場合は［*システムログ*］を、別のファイルを指定する場合は［*ファイルに記録*］を選択します。別のファイルを指定する場合は、ログファイルの最大サイズ(メガバイト(MB))とログファイルの数も指定します。

［*追加のログ*］には、さらに詳細なオプションが用意されています。［*Log Named Queries*］を有効にすると、すべてのクエリがログに記録されるため、ログファイルが非常に大きくなる可能性があります。ですから、このオプションを有効にするのはデバッグ時だけにすることをお勧めします。DHCPサーバとDNSサーバ間でのゾーン更新時のデータトラフィックをログに記録するには、［*ゾーン更新をログに記録*］を有効にします。マスタからスレーブへのゾーン転送時のデータトラフィックをログに記録するには、［*ゾーン転送をログに記録*］を有効にします。図40.4.「DNSサーバ：ログ」 (page 665)を参照してください。

図 40.4 *DNSサーバ：ログ*



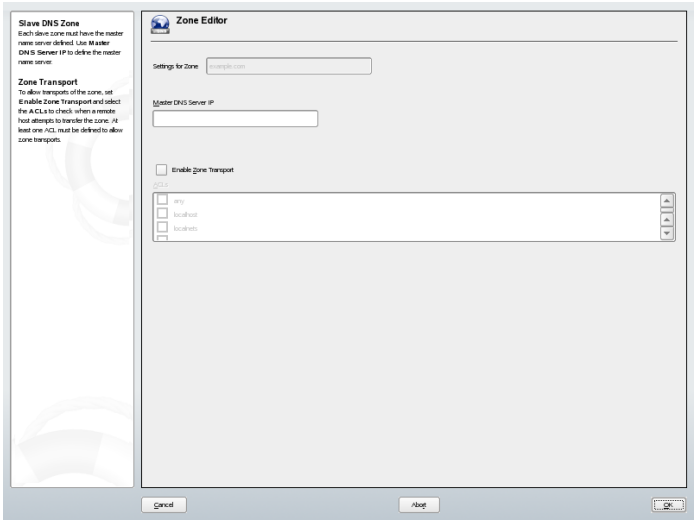
DNSゾーン

このダイアログでは、ウィザードの設定について説明します。項40.2.1.「ウィザードによる設定」 (page 661)を参照してください。

スレーブゾーンエディタ

DNSゾーン (page 665)で説明したステップで、ゾーンタイプとして［スレーブ］を選択すると、このダイアログが開きます。［マスタ*DNS*サーバ］で、データの転送元としてスレーブが使用するマスタを指定します。サーバへのアクセスを制限するために、リストから定義済みのACLを1つ選択します。図 40.5.「DNSサーバ：スレーブゾーンエディタ」 (page 666)を参照してください。

図 40.5 *DNSサーバ：スレーブゾーンエディタ*



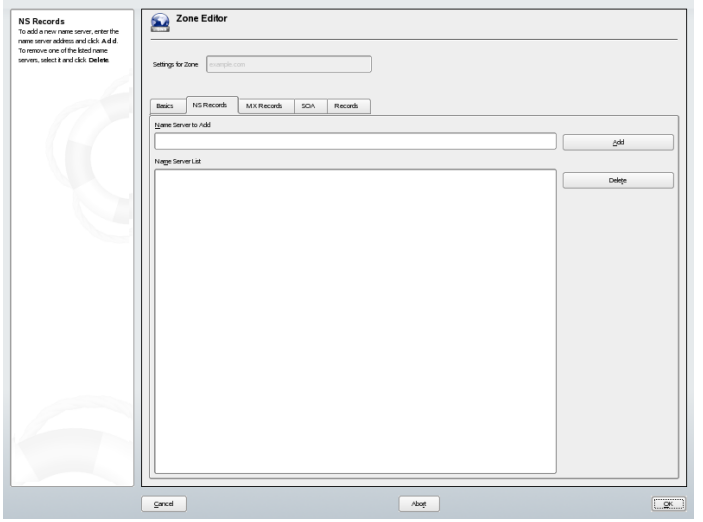
マスタゾーンエディタ

DNSゾーン (page 665)で説明したステップで、ゾーンタイプとして［マスタ］を選択すると、このダイアログが開きます。 このダイアログは、［*Basic*］(最初に開くページ)、［*NS Records*］、［*MX Records*]*[SOA*］、［*Records*］の各ページで構成されます。

ゾーンエディタ(NSレコード)

このダイアログでは、指定したゾーンの代替ネームサーバを定義できます。リストに自分が使用しているネームサーバが含まれていることを確認してください。レコードを追加するには、［*追加*するネームサーバ］にレコード名を入力し、［*追加*］をクリックして確定します。図 40.6.「DNSサーバ：ゾーンエディタ(NSレコード)」 (page 667)を参照してください。

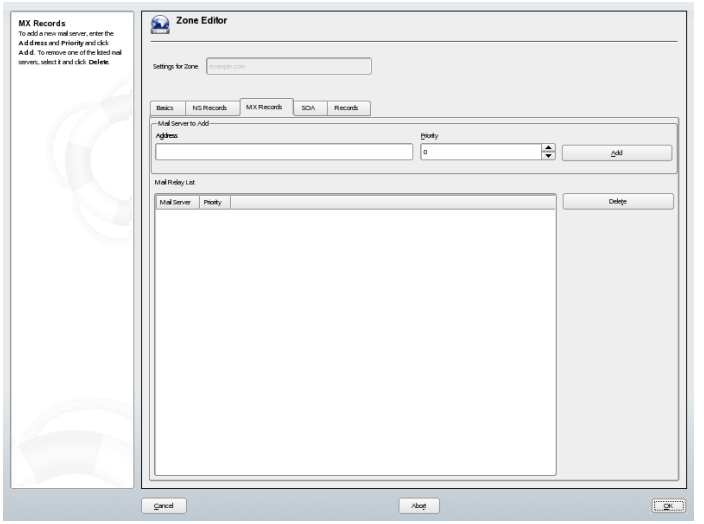
図 40.6　DNSサーバ：ゾーンエディタ(NSレコード)



ゾーンエディタ(MXレコード)

現行ゾーンのメールサーバを既存のリストに追加するには、対応するアドレスと優先順位の値を入力します。その後、［*追加*］を選択して確定します。図 40.7.「DNSサーバ：ゾーンエディタ(MXレコード)」 (page 668)を参照してください。

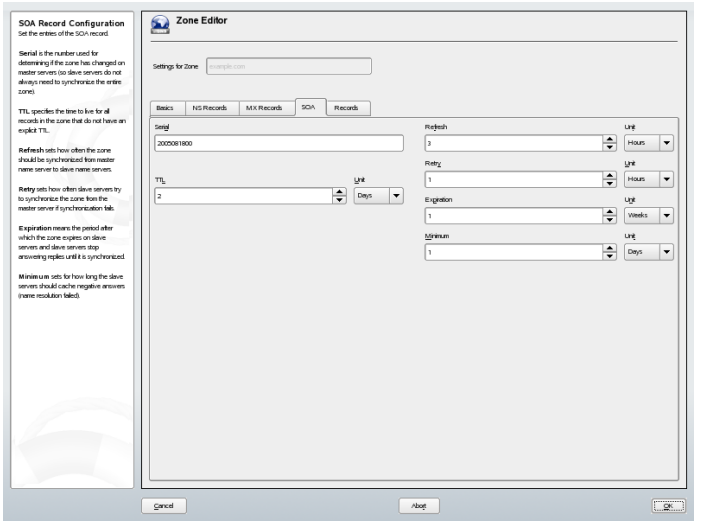
図 40.7　DNSサーバ：ゾーンエディタ(MXレコード)



ゾーンエディタ(SOA)

このページでは、SOA (start of authority)レコードを作成できます。個々のオプションについては、例 40.6. 「/var/lib/named/world.zoneファイル」(page 676)を参照してください。

図 40.8　DNSサーバ：ゾーンエディタ(SOA)



ゾーンエディタ(レコード)
このダイアログでは、名前解決を管理します。［*レコードキー*］では、ホスト名を入力してレコードタイプを選択します。［*A-Record (Aレコード)*］はメインエントリを表します。この値はIPアドレスでなければなりません。［*CNAME*］はエイリアスです。［*NS*］および［*MX*］の各タイプを指定すると、［*NSレコード*］および［*MXレコード*］の各タブで提供される情報に基づいて、詳細レコードまたは部分レコードが展開されます。この3つのタイプのは、既存のAレコードに解決されます。［*PTR*］は逆引きゾーン用レコードです。これは、Aレコードとは反対にIPアドレスに対するホスト名を定義します。

40.3　ネームサーバBINDの起動

SUSE Linuxシステムでは、BIND (*Berkeley Internet name domain*)が事前に設定された状態で提供されているので、インストールが正常に完了すればすぐにネームサーバが起動されます。既にインターネットに接続し、`/etc/resolv.conf`の`localhost`にネームサーバアドレス`127.0.0.1`が入力されている場合、通常、プロバイダのDNSを知らなくても、既に機能する名前解決メカニズムが存在します。この場合、BINDは、ルートネームサーバを介して名前の解決を行うため、処理が非常に遅くなります。通常、効率的で安全な名前

解決を実現するには、forwardersの下の設定ファイル/etc/named.confにプロバイダのDNSとそのIPアドレスを入力する必要があります。いままでこれが機能している場合、ネームサーバは、純粋なキャッシュ*専用*ネームサーバとして動作しています。ネームサーバは、自身のゾーンを設定してはじめて、本当のDNSになります。これの簡単な例については、/usr/share/doc/packages/bind/sample-configのドキュメントを参照してください。

ティップ: ネームサーバ情報の自動取得

インターネット接続やネットワーク接続のタイプによっては、ネームサーバ情報を自動的に現在の状態に適合させることができます。これを行うには、/etc/sysconfig/network/configファイル内でMODIFY_NAMED_CONF_DYNAMICALLY変数にyesを設定します。

ただし、公式ドメインは、管理団体から割り当てられるまでセットアップしないでください。独自のドメインを持っていて、プロバイダがそれを管理している場合でも、BINDはそのドメインに対する要求を転送しないので、そのドメインを使用しないほうが賢明です。たとえば、プロバイダのWebサーバは、このドメインからはアクセスできません。

ネームサーバを起動するには、rootユーザとして、コマンドrcnamedstartを入力します。右側に緑色で「done」と表示されたら、named (ネームサーバプロセス名)が正常に起動しています。サーバが正常に起動したらすぐに、hostまたはdigプログラムを用いてローカルシステム上でネームサーバをテストしてください。デフォルトサーバlocalhostとそのアドレス127.0.0.1が返されるはずです。これが返されない場合は、/etc/resolv.confに含まれているネームサーバエントリが誤っているか、同ファイルが存在しないかのいずれかです。最初のテストとして、host127.0.0.1を入力します。これは常に機能するはずです。エラーメッセージが表示された場合は、rcnamedstatusを使用して、サーバが実際に起動されていることを確認します。ネームサーバが起動しない場合、または予想しない動作をしている場合、多くはログファイル/var/log/messagesでその原因が明らかになります。

プロバイダのネームサーバまたはフォワーダとして既にネットワーク上で動作しているネームサーバを使用する場合は、forwardersの下のoptionsセクションに、対応するIPアドレスまたはアドレスを入力します。例 40.1. 「named.confファイルの転送オプション」 (page 671)に含まれているアドレスは、単なる例です。自サイトの設定に合わせて変更してください。

例 40.1　named.confファイルの転送オプション

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.0.99; };
        allow-query { 127/8; 192.168.0/24; };
        notify no;
        };
```

optionsエントリの後には、ゾーン用のエントリ、localhostと0.0.127.in-addr.arpaが続きます。「.」の下のtype hint(タイプヒント)は必ず存在しなければなりません。対応するファイルは、変更する必要がなく、そのままで機能します。また、各エントリの末尾が「;」で閉じられ、中カッコが適切な位置にあることを確認してください。設定ファイル/etc/named.confまたはゾーンファイルを変更したら、rcnamedreloadを使用して、BINDにそれらを再読み込みさせます。または、rcnamedrestartを使用してネームサーバを停止、再起動しても同じ結果が得られます。サーバはrcnamedstopを入力していつでも停止することができます。

40.4　設定ファイル/etc/named.conf

BINDネームサーバ自体の設定はすべて、ファイル/etc/named.confに格納されます。ただし、ホスト名、IPアドレスなどで構成され、ドメインが処理するゾーンデータは、/var/lib/namedディレクトリ内の個別のファイルに格納されます。 この詳細については、後述します。

/etc/named.confファイルは、大きく2つのエリアに分けられます。1つは一般的な設定用のoptionsセクション、もう1つは個々のドメインのzoneエントリで構成されるセクションです。ログセクションとacl(アクセス制御リスト)エントリは省略可能です。コメント行は、行頭に#記号または//を指定します。最も基本的な/etc/named.confファイルの例を、例 40.2.「基本的な/etc/named.confファイル」 (page 672)に示します。

*例 **40.2*** *基本的な/etc/named.confファイル*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

40.4.1 重要な設定オプション

directory "*filename*";
BINDが検索する、ゾーンファイルが格納されているディレクトリを指定します。通常は/var/lib/namedです。

forwarders { *ip-address*; };
DNS要求が直接解決できない場合、それらが転送されるネームサーバ(ほとんどの場合、プロバイダのネームサーバ)を指定します。*ip-address*には、IPアドレスを10.0.0.1のように指定します。

forward first;
ルートネームサーバでDNS要求の解決を試みる前に、それらを転送するようにします。forward firstの代わりにforward onlyを指定すると、要求が転送されたままになり、ルートネームサーバには送り返されません。このオプションは、ファイアウォール構成で使用します。

listen-on port 53 { 127.0.0.1; *ip-address*; };

BINDがクライアントからのクエリを受け取るネットワークインタフェースとポートを指定します。 port 53はデフォルトポートであるため、明

示的に指定する必要はありません。ローカルホストからの要求を許可するには、127.0.0.1と記述します。このエントリ全体を省略した場合は、すべてのインタフェースがデフォルトで使用されます。

listen-on-v6 port 53 {any; };
BINDがIPv6クライアント要求をリッスンするポートを指定します。any以外で指定できるのはnoneだけです。IPv6に関して、サーバはワイルドカードアドレスのみ受け付けます。

query-source address * port 53;
ファイアウォールが発信DNS要求をブロックする場合、このエントリが必要です。BINDに対し、外部への要求をポート53から発信し、1024を超える上位ポートからは発信しないように指示します。

query-source address * port 53;
BINDがIPv6のクエリに使用するポートを指定します。

allow-query { 127.0.0.1; *net*; };
クライアントがDNS要求を発信できるネットワークを定義します。*net*には、アドレス情報を192.168.1/24のように指定します。末尾の/24は、ネットマスクの短縮表記で、この場合255.255.255.0を表します。

allow-transfer ! *;;
ゾーン転送を要求できるホストを制御します。この例では、！ *が使用されているので、ゾーン転送要求は完全に拒否されます。*このエントリがなければ、ゾーン転送をどこからでも制約なしに要求できます。

statistics-interval 0;
このエントリがなければ、BINDは1時間ごとに数行の統計情報を生成して/var/log/messagesに保存します。0を指定すると、統計情報をまったく生成しないか、時間間隔を分単位で指定します。

cleaning-interval 720;
このオプションは、BINDがキャッシュをクリアする時間間隔を定義します。キャッシュがクリアされるたびに、/var/log/messagesにエントリが追加されます。時間の指定は分単位です。デフォルトは60分です。

statistics-interval 0;
forwardingBINDは定期的にインタフェースを検索して、新しいインタフェースや存在しなくなったインタフェースがないか確認します。この値を0に

設定すると、この検索が行われなくなり、BINDは起動時に検出されたインタフェースのみをリッスンします。0以外の値を指定する場合は分単位で指定します。デフォルトは60分です。

notify no;
noに設定すると、ゾーンデータを変更したとき、またはネームサーバが再起動されたときに、他のネームサーバに通知されなくなります。

40.4.2 ログ

BINDでは、何を、どのように、どこにログ出力するかを詳細に設定できます。 通常は、デフォルト設定のままで十分です。 例 40.3.「ログを無効にするエントリ」 (page 674)に、このエントリの最も簡単な形式、すなわちログをまったく出力しない例を示します。

例 40.3 ログを無効にするエントリ

```
logging {
        category default { null; };
};
```

40.4.3 ゾーンエントリ

例 40.4 my-domain.deのゾーンエントリ

```
zone "my-domain.de" in {
      type master;
      file "my-domain.zone";
      notify no;
};
```

zoneの後、管理対象のドメイン名my-domain.deを指定し、次にinと関連のオプションを中カッコで囲んで指定します(例 40.4.「my-domain.deのゾーンエントリ」 (page 674)参照)。スレーブゾーンを定義するには、typeをslaveに変更し、このゾーンをmasterとして管理することをネームサーバに指定します(例 40.5.「other-domain.deのゾーンエントリ」 (page 675)参照)。これが他のマスタのスレーブとなることもあります。

例 40.5　other-domain.deのゾーンエントリ

```
zone "other-domain.de" in {
      type slave;
      file "slave/other-domain.zone";
      masters { 10.0.0.1; };
};
```

ゾーンオプション

type master;
masterを指定して、BINDに対し、ゾーンがローカルネームサーバによって処理されるように指示します。これは、ゾーンファイルが正しい形式で作成されていることが前提となります。

type slave;
このゾーンは別のネームサーバから転送されたものです。必ずmastersとともに使用します。

type hint;
ルートネームサーバの設定には、hintタイプのゾーン.を使用します。このゾーン定義はそのまま使用できます。

file my-domain.zoneまたはfile 「slave/other-domain.zone」;
このエントリは、ドメインのゾーンデータが格納されているファイルを指定します。スレーブの場合、このデータを他のネームサーバから取得するので、このファイルは不要です。マスタとスレーブのファイルを区別するには、スレーブファイルにディレクトリslaveを使用します。

masters { *server-ip-address*; };
このエントリは、スレーブゾーンにのみ必要です。ゾーンファイルの転送元となるネームサーバを指定します。

allow-update {! *; };
このオプションは、外部書き込みアクセスを制御し、クライアントにDNSエントリへの書き込み権を付与することができます。 ただし、これは通常、セキュリティ上の理由で好ましくありません。このエントリがなければ、ゾーンの更新は完全に拒否されます。 上のエントリでは、！ *によって一切の書き込みを禁止しているので、変更が完全に拒否されるという結果はこのエントリを指定しない場合と同じです。

40.5 ゾーンファイル

ゾーンファイルは2種類必要です。 1つはIPアドレスをホスト名に割り当てるゾーンファイル、もう1つは逆にホスト名をIPアドレスに割り当てるゾーンファイルです。

ティップ: ゾーンファイルでのピリオドの使用

. は、ゾーンファイル内で重要な意味を持ちます。末尾に. のホスト名を指定すると、ゾーンが追加されます。完全なホスト名を完全なドメイン名とともに指定する場合は、末尾に. を付けて、ドメインが追加されないようにします。ピリオドの打ち忘れや位置の間違いは、ネームサーバ設定エラーの原因としておそらく最も頻繁に見られるものです。

最初に、ドメインworld.cosmosに責任を負うゾーンファイルworld.zoneについて示します(例 40.6. 「/var/lib/named/world.zoneファイル」 (page 676)参照)。

*例 **40.6** /var/lib/named/world.zoneファイル*

```
$TTL 2D
world.cosmos. IN SOA      gateway  root.world.cosmos. (
            2003072441  ; serial
            1D          ; refresh
            2H          ; retry
            1W          ; expiry
            2D )        ; minimum

            IN NS       gateway
            IN MX       10 sun

gateway     IN A        192.168.0.1
            IN A        192.168.1.1
sun         IN A        192.168.0.2
moon        IN A        192.168.0.3
earth       IN A        192.168.1.2
mars        IN A        192.168.1.3
www         IN CNAME    moon
```

1行目:

$TTLは、このファイルのすべてのエントリに適用されるデフォルトの寿命(time to live)です。この例では、エントリは2日間(2 D)有効です。

2 行目:

ここから、SOA (start of authority)制御レコードが始まります。

- 管理対象のドメイン名は、先頭にある`world.cosmos`です。これは、末尾に. (ピリオド)が付いています。ピリオドを付けないと、ゾーンが再度末尾に追加されてしまいます。 あるいはピリオドを`@`で置き換えることもできます。 その場合は、ゾーンが`/etc/named.conf`の対応するエントリから抽出されます。

- `IN SOA`の後には、このゾーンのマスタであるネームサーバの名前を指定します。これらの名前は末尾に. (ピリオド)が付いていないので、`gateway`から`gateway.world.cosmos`に拡張されます。

- この後には、このネームサーバの責任者の電子メールアドレスが続きます。`@`記号は既に特別な意味を持つので、ここでは代わりに. (ピリオド)を使用します。`root@world.cosmos`の場合、エントリは`root.world.cosmos.`となります。ここでもゾーンが追加されないよう、`.`を末尾につける必要があります。

- `(`は、`)`までの行をすべてSOAレコードに含める場合に使用します。

3 行目:

シリアル番号は任意の番号で、このファイルを変更するたびに増加します。変更があった場合、セカンダリネームサーバ(スレーブサーバ)に通知する必要があります。これには、日付と実行番号をYYYYMMDDNNという形式で表記した10桁の数値が、慣習的に使用されています。

4 行目:

リフレッシュレートは、セカンダリネームサーバがゾーン`serial number`を確認する時間間隔を指定します。この例では1日です。

5 行目:

再試行間隔は、エラーが生じた場合に、セカンダリネームサーバがプライマリサーバに再度通知を試みる時間間隔を指定します。この例では2時間です。

6 行目:

有効期限は、セカンダリネームサーバがプライマリサーバに再通知できなかった場合に、キャッシュしたデータを廃棄するまでの時間枠を指定します。この例では1週間です。

7 行目:

SOAレコードの最後のエントリは、ネガティブキャッシュTTLです。これは、DNSクエリが解決できないという他のサーバからの結果をキャッシュしておく時間です。

9 行目:

IN NSは、このドメインを担当するネームサーバを指定します。これらの名前は末尾に.(ピリオド)が付いていないので、gatewayからgateway.world.cosmosに拡張されます。このように、プライマリネームサーバと各セカンダリネームサーバに1つずつ指定する行がいくつかあります。/etc/named.confでnotifyをnoに設定しない限り、ゾーンデータが変更されると、ここにリストされているすべてのネームサーバにそれが通知されます。

10 行目:

MXレコードは、ドメインworld.cosmos宛ての電子メールを受領、処理、および転送するメールサーバを指定します。この例では、ホストsun.world.cosmosが指定されています。ホスト名の前の数字は、プリファレンス値です。複数のMXエントリが存在する場合、値が最も小さいメールサーバが最初に選択され、このサーバへのメール配信ができなければ、次に小さい値のメールサーバが試みられます。

12〜17行目:

これらは、ホスト名に1つ以上のIPアドレスが割り当てられている実際のアドレスレコードです。ここにリストされている名前にはドメインが含まれていないので、.(ピリオド)が付いておらず、その結果、すべての名前にworld.cosmosが追加されることになります。ホストgatewayは、ネットワークカードが2枚搭載されているので、2つのIPアドレスが割り当てられます。ホストアドレスが従来型のアドレス(IPv4)の場合、レコードにAが付きます。アドレスがIPv6アドレスの場合、エントリにA6が付きます。以前は、IPv6アドレスがAAAAで示されていましたが、現在では廃止されました。

18 行目:
エイリアスwwwをmondの別名として使用できます(CNAMEは*canonical name(*キャノニカル名*)*という意味です)。

擬似ドメインin-addr.arpaは、IPアドレスからホスト名への逆引き参照に使用されます。このドメインの前に、IPアドレスのネットワーク部分が逆順に指定されます。たとえば、192.168.1は、1.168.192.in-addr.arpaに解決されます。例 40.7.「逆引き」 (page 679)を参照してください。

*例 **40.7***　*逆引き*

```
$TTL 2D
1.168.192.in-addr.arpa.  IN SOA gateway.world.cosmos.  root.world.cosmos. (
                         2003072441      ; serial
                         1D              ; refresh
                         2H              ; retry
                         1W              ; expiry
                         2D )            ; minimum

                         IN NS           gateway.world.cosmos.

1                        IN PTR          gateway.world.cosmos.
2                        IN PTR          earth.world.cosmos.
3                        IN PTR          mars.world.cosmos.
```

1 行目:
$TTLは、このファイルのすべてのエントリに適用される標準のTTLです。

2 行目:
この設定ファイルは、ネットワーク192.168.1.0の逆引きを有効にします。ゾーン名は1.168.192.in-addr.arpaであり、これはホスト名に追加しません。したがって、すべてのホスト名は完全な形で、つまりドメインと末尾の.(ピリオド)が付いて指定されます。残りのエントリは、前のworld.cosmosの例の記述と同じです。

3〜7行目:
前の例のworld.cosmosを参照してください。

9 行目:
正引きの場合と同様、この行は、このゾーンを担当するネームサーバを指定します。ただし、ホスト名はドメインと末尾の.(ピリオド)が付いた完全な形で指定されます。

11〜13行目:
これらはそれぞれのホスト上でのIPアドレスを示すポインタレコードです。IPアドレスの最後のオクテットのみが、行の最初に入力され、末尾に.(ピリオド)は付きません。ゾーンをこれに追加すると(`.in-addr.arpa`を付けずに)、完全なIPアドレスが逆順で生成されます。

通常、異なるバージョンのBIND間のゾーン転送は、問題なく行えるはずです。

40.6 ゾーンデータの動的アップデート

*動的*アップデートという用語は、マスタサーバのゾーンファイル内のエントリが追加、変更、削除される操作を指します。この仕組みは、RFC 2136に記述されています。動的アップデートをゾーンごとに個別に構成するには、オプションの`allow-update`ルールまたは`update-policy`ルールを追加します。動的に更新されるゾーンを手動で編集してはなりません。

サーバに更新エントリを転送するには、`nsupdate`コマンドを使用します。このコマンドの詳細な構文については、nsupdateのマニュアルページ(`man 8 nsupdate`)を参照してください。セキュリティ上の理由から、こうした更新はTSIGキーを使用して実行するようにしてください(項40.7.「安全なトランザクション」 (page 680)参照)。

40.7 安全なトランザクション

安全なトランザクションは、共有秘密キー(TSIGキーとも呼ばれる)に基づくトランザクション署名(TSIG)を使用して実現できます。ここでは、このキーの生成方法と使用方法について説明します。

安全なトランザクションは、異なるサーバ間の通信、およびゾーンデータの動的アップデートに必要です。アクセス制御をキーに依存する方が、単にIPアドレスに依存するよりもはるかに安全です。

TSIGキーの生成には、次のコマンドを使用します(詳細については、`man dnssec-keygen`を参照)。

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

これにより、次のような形式の名前を持つファイルが2つ作成されます。

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

キー自体(ejIkuCyyGJwwuN3xAteKgg==のような文字列)は、両方のファイルにあります。キーをトランザクションで使用するには、2番目のファイル(Khost1-host2.+157+34265.key)を、できれば安全な方法で(たとえばscpを使用して)、リモートホストに転送する必要があります。host1とhost2の間で安全な通信ができるようにするには、リモートサーバでキーをファイル/etc/named.confに含める必要があります。

```
key host1-host2. {
 algorithm hmac-md5;
 secret ";ejIkuCyyGJwwuN3xAteKgg==;
};
```

警告: /etc/named.confのファイルパーミッション

/etc/named.confのファイルパーミッションが適切に制限されていることを確認してください。このファイルのデフォルトのパーミッションは0640で、オーナーがroot、グループがnamedです。この代わりに、パーミッションが制限された別ファイルにキーを移動して、そのファイルを/etc/named.conf内にインクルードすることもできます。

サーバhost1がhost2(この例では、アドレス192.168.2.3)のキーを使用できるようにするには、host1の/etc/named.confに次の規則が含まれている必要があります。

```
server 192.168.2.3 {
  keys { host1-host2. ;};
};
```

同様のエントリがhost2の設定ファイルにも含まれている必要があります。

IPアドレスとアドレス範囲に対して定義されているすべてのACL(アクセス制御リスト—ACLファイルシステムと混同しないこと)にTSIGキーを追加してトランザクションセキュリティを有効にします。対応するエントリは、次のようになります。

```
allow-update { key host1-host2. ;};
```

このトピックについての詳細は、update-policyの下の『*BIND Administrator Reference Manual*』を参照してください。

40.8 DNSセキュリティ

DNSSEC、すなわちDNSセキュリティは、RFC2535に記述されています。DNSSECに利用できるツールについては、BINDのマニュアルを参照してください。

ゾーンが安全だといえるためには、1つ以上のゾーンキーが関連付けられている必要があります。キーはホストキーと同様、dnssec-keygenによって生成されます。現在、これらのキーの生成には、DSA暗号化アルゴリズムが使用されています。生成されたパブリックキーは、$INCLUDEルールによって、対応するゾーンファイルにインクルードします。

生成したすべてのキーは、dnssec-makekeysetコマンドによって1つのセットにパッケージングし、安全な方法で親ゾーンに転送する必要があります。親ゾーンでは、dnssec-signkeyによってセットに署名が付されます。このコマンドによって複数のファイルが生成され、これらのファイルを使用してdnssec-signzoneが実行され、ゾーンに署名が付されます。このときにファイルが生成されて、各ゾーンの/etc/named.confにインクルードされます。

40.9 関連資料

ここで扱ったトピックの詳細については、/usr/share/doc/packages/bind/ディレクトリの『*BIND Administrator Reference Manual*』を参照してください。BINDに付属のマニュアルやマニュアルページで紹介されているRFCも、必要に応じて参照してください。/usr/share/doc/packages/bind/README.SuSEには、SUSE LinuxのBINDに関する最新情報が含まれています。

41 NISの使用

ネットワーク上の複数UNIXシステムが共通のリソースにアクセスするようになると、すべてのユーザおよびグループ識別情報がネットワーク上のすべてのコンピュータで一致していることが重要になります。 ネットワークはユーザにとって透過的でなければなりません。すなわち、使用するコンピュータに関係なく、常に、まったく同じ環境で作業できる必要があります。これを実現するのが、NISおよびNFSサービスです。NFSはネットワーク上にファイルシステムを分散させるシステムです。これについては、章42. *NFS共有ファイルシステム* (page 691)で説明します。

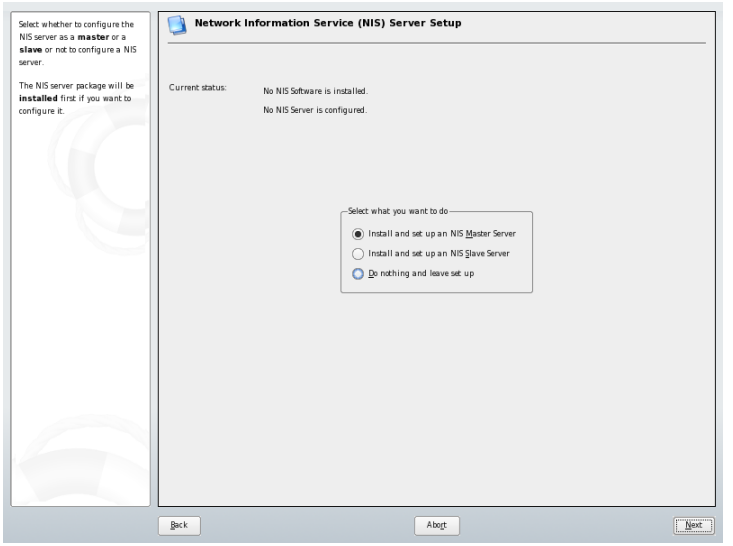
NIS (Network Information Service)は、 `/etc/passwd`、 `/etc/shadow`、 `/etc/group`の各ファイルにネットワーク越しにアクセスできるようにするデータベースサービスと考えることができます。NISの用途はこれ以外にもありますが(`/etc/hosts`や `/etc/services`といったファイルにアクセスできるようにするなど)、ここでは触れません。NISはよく*YP*と呼ばれますが、これは、NISがちょうどネットワークの「イエローページ」のような役割を果たすためです。

41.1 YaSTによるNISサーバの構成

NISサーバを設定するには、YaSTの［ネットワークサービス］モジュールから［*NIS*サーバ］を選択します。 ネットワーク上にNISサーバがまだ存在しない場合は、次の画面で［*Install and set up an NIS Master Server(NIS*マスタサーバのインストールと設定*)*］をオンにしてください。 YaSTは直ちに必要なパッケージのインストールを行います。

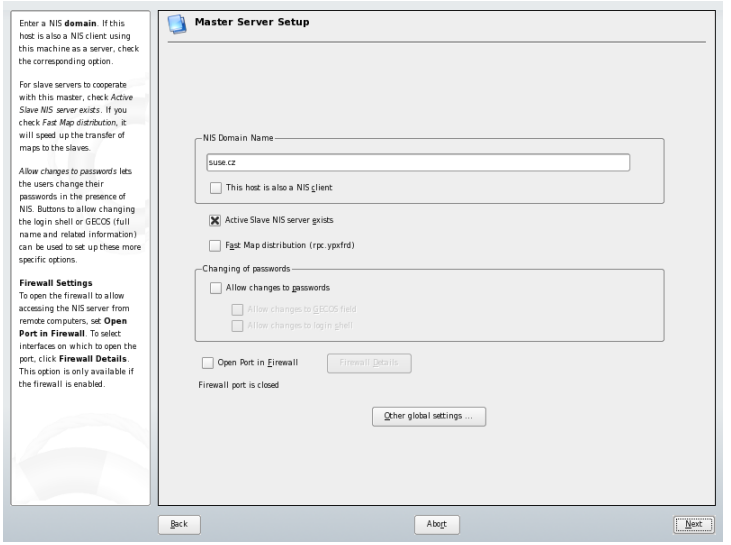
すでにNISソフトウェアをインストールしてある場合には、［*Create NIS Master Server (NISマスタサーバの作成)*］をクリックします。既にNISサーバ(マスタ)が存在する場合は、NISスレーブサーバを追加できます(たとえば、新しいサブネットワークを設定する場合など)。最初に、マスタサーバの設定について説明します。［*Do nothing and leave setup*］をクリックすると、変更を保存せずにYaSTコントロールセンターに戻ります。

図 41.1　NISサーバの設定



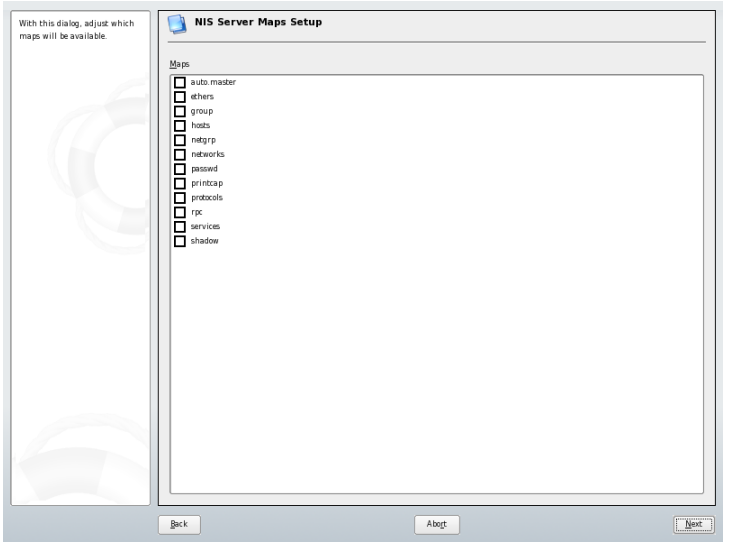
すべてのパッケージがインストールされたら、図 41.1. 「NISサーバの設定」(page 684)に示すように、設定ダイアログの上部にNISドメイン名を入力します。すぐ下のチェックボックスで、このホストをNISクライアントとしても使用するかどうかを指定します。このチェックボックスをオンにすると、ユーザはこのホストにログインしてNISサーバのデータにアクセスできます。［*Changing of paswords*］オプションも含め、適用するすべてのボックスをオンにします。［*Other global settings*］をクリックすると、さらに多くのオプションが表示されます。ここでは、ソースディレクトリの場所、パスワードをマージするかどうか、最小のユーザIDとグループIDを設定できます。［*了解*］をクリックしてメインダイアログに戻ります。［*Next*］をクリックして設定を続けます。

図 41.2 マスタサーバの設定



次の画面では、どのマップを利用可能にするかを設定します。［*Next*］をクリックすると、次の画面が表示されて、どのホストにNISサーバへのクエリを許可するかを指定できます。 ホストは追加、削除、編集が行えます。 ［*Finish*］をクリックして変更を保存し、設定ダイアログを閉じます。

図 41.3　NISサーバマップの設定



後でネットワーク上にNIS(スレーブサーバ)を追加設定できるように、ここで［*Install and set up an NIS Slave Server*］を有効にしておいてください。 NISソフトウェアがすでにインストールされている場合には、［*Create NIS Slave Server*］を選択し、［*Next*］をクリックして継続します。 次の画面では、NISのドメイン名を入力し、適用するチェックボックスをオンにします。

ネットワーク上のユーザが`yppasswd`コマンドを用いてNISサーバ上のパスワードを変更できるようにするには、対応するオプションを有効にします。これにより、［*Allow Changes to GECOS Field*］および［*Allow Changes to Login Shell*］オプションが選択可能になります。前者を選択すると、ユーザが`ypchfn`コマンドを使用して自分の名前とアドレスの設定を変更できるようになります。後者を選択すると、ユーザが、`ypchsh`コマンドを使用してデフォルトのシェルを(たとえばbashからshに)変更できるようになります。

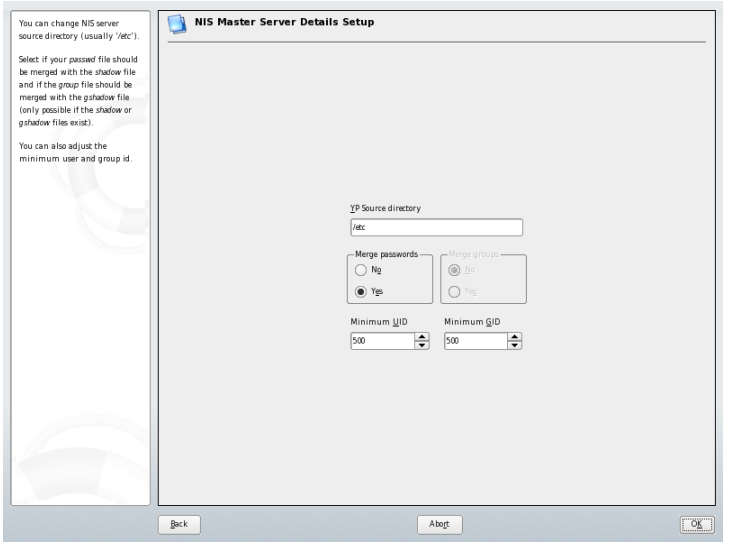
［*Other global settings*］を選択すると、図 41.4.「ディレクトリの変更とNISサーバ用の各ファイルの同期化」 (page 687)に示す画面が表示されます。ここでは、NISサーバのソースディレクトリを変更できます(デフォルトは`/etc`)。また、パスワードとグループを結合することもできます。ここで［はい］を選択して、`/etc/passwd`、`/etc/shadow`、および`/etc/group`の各ファイル間の同期をとるようにしてください。また、最小のユーザIDとグループID

も指定します。［*OK*］をクリックして設定内容を確定すると、前の画面に戻ります。

設定したら、［*Next*］をクリックして次の画面に進みます。次のダイアログでは、利用可能にするマップをオンにし、［*Next*］をクリックして継続します。最後の画面では、どのホストにNISサーバへのクエリを許可するかを指定します。ホストは、適切なボタンをクリックして追加、削除、編集できます。［*Finish*］をクリックして変更を保存し、設定を終えます。

次に、［次へ］をクリックします。

図 41.4 *ディレクトリの変更とNISサーバ用の各ファイルの同期化*



前の画面で［*NISスレーブサーバが存在する*］を選択した場合は、スレーブとして使用するホスト名を入力して［次へ］をクリックします。スレーブサーバを使用しない場合は、スレーブ設定を省略して、データベース設定のダイアログに進んでください。ここでは、マップを指定します。マップとは、NISサーバからNISクライアントに転送される部分データベースのことです。通常は、デフォルトの設定のままで十分です。

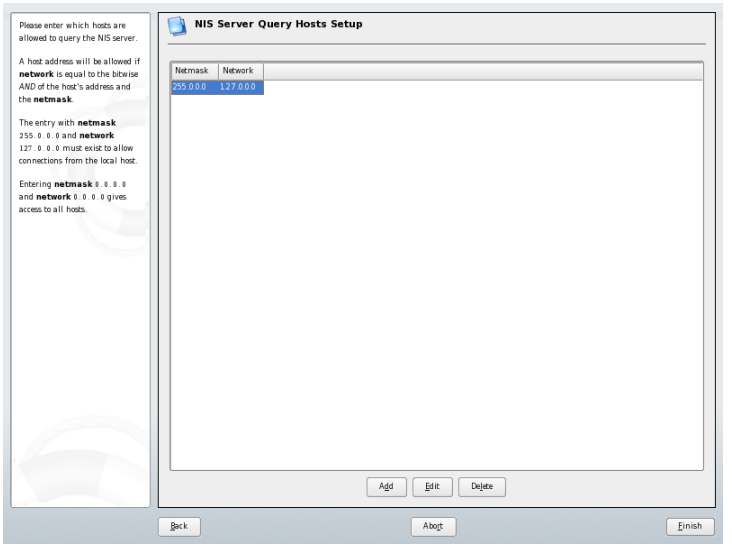
［次へ］をクリックすると最後のダイアログ(図41.5.「NISサーバに対するリクエスト送信許可の設定」 (page 688))に進みます。ここでは、NISサーバにリ

クエストを送信できるネットワークを指定します。通常は、内部ネットワークを指定します。その場合は、次の2つのエントリが必要です。

```
255.0.0.0       127.0.0.0
0.0.0.0         0.0.0.0
```

最初のエントリによって、自分自身、つまりNISサーバからの接続が許可されます。2つ目のエントリによって、同一ネットワークにアクセス可能なすべてのホストがNISサーバにリクエストを送信することを許可されます。

図 41.5　NISサーバに対するリクエスト送信許可の設定



重要項目: 自動ファイアウォール設定

システムでファイアウォール(SuSEfirewall2) が有効になっている場合に、［ファイアウォールで開いているポート］を選択すると、YaSTは、`portmap` サービスを有効にすることでNISサーバ用にファイアウォール設定を変更します。

41.2 NISクライアントの設定

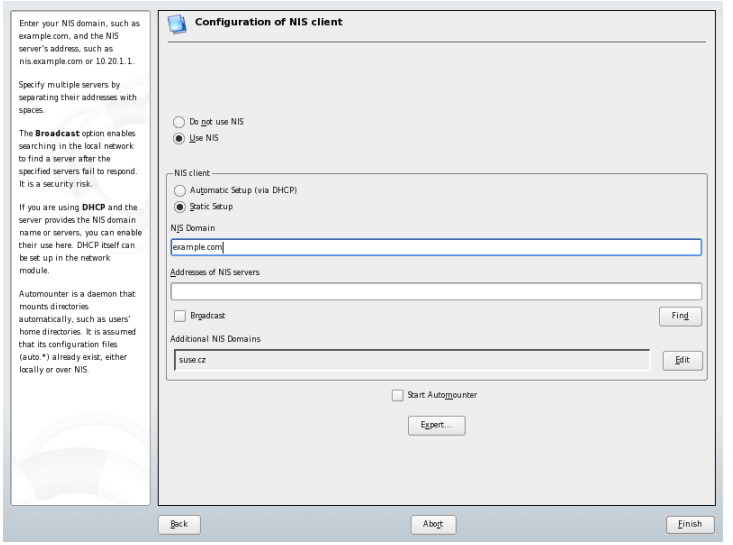
このモジュールではNISクライアントを設定します。NIS、および、必要に応じてオートマウンタを使用するように選択すると、このダイアログが開きます。ホストに静的IPアドレスを割り当てるのか、DHCPから提供されたIPアドレスを使用するのかを選択してください。DHCPからは、NISドメインとNISサーバも提供されます。DHCPについては、章43. *DHCP* (page 699)を参照してください。固定IPアドレスを使用する場合は、NISドメインとNISサーバを手動で指定します。図41.6.「NISサーバのドメインとアドレスの設定」 (page 690)を参照してください。［*Find*］をクリックすると、YaSTはネットワーク上のアクティブなNISサーバを検索します。［*Broadcast*］は、指定したサーバが応答しなかったときに、ローカルネットワークでのサーバの検索を有効にします。

［*Addresses of NIS servers*］にアドレスをスペースで区切って入力することにより、複数のサーバを指定することもできます。

クライアントが使用しているサーバを他のホストに知られたくない場合は、エキスパート設定で、［*Answer Remote Hosts*］をオフにします。［ブロークンサーバ］を有効にすると、クライアントが、特権のないポートを介して通信するサーバからの応答を受信できるようになります。詳細については、`man ypbind`を参照してください。

設定を終えたら、［*Finish*］をクリックして変更を保存し、YaSTコントロールセンターに戻ります。

図 41.6　NISサーバのドメインとアドレスの設定



42 NFS共有ファイルシステム

章 41. *NISの使用* (page 683)で説明したように、NFSをNISと連係して使用すると、ネットワークをユーザにとって透過的にすることができます。NFSでは、ネットワーク経由でファイルシステムを分散できます。ユーザはどの端末からログインしても、常に、同じ環境で作業できます。

NIS と同様、NFS は非対称サービスで、NFS サーバと NFS クライアントがあります。台のマシンがサーバとクライアントの両方になることができます。ファイルシステムをネットワーク経由で提供し(エクスポート)、同時に他のホストからファイルシステムをマウントする(インポート)ことができます。一般に、これらは大容量のハードディスクを搭載したサーバであり、そのファイルシステムが他のクライアントによってマウントされます。

重要項目: DNSの必要性

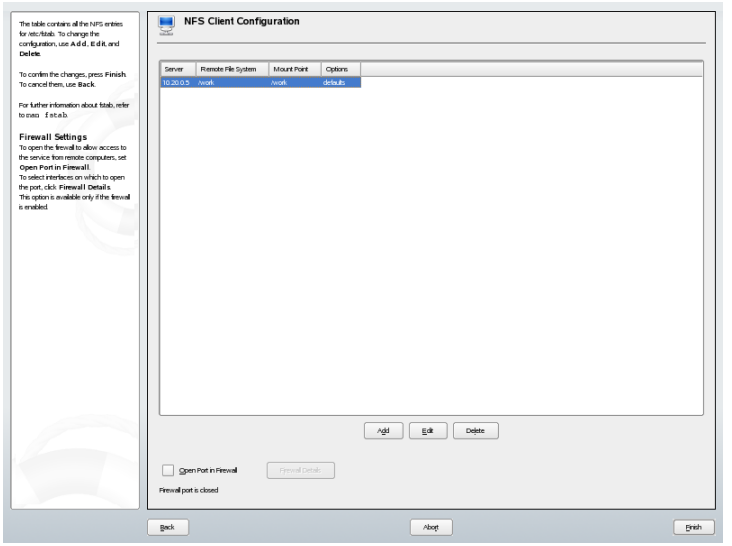
原則として、すべてのエクスポートはIPアドレスのみを使用して実行できます。ただし、タイムアウトを回避するために、実際に動作するDNSシステムを用意しておく必要があります。mountdデーモンは逆引きを行うため、少なくともログ目的にはDNSが必要です。

42.1 YaSTによるファイルシステムのインポート

適切な権限があれば、NFSディレクトリをNFSサーバから自分のファイルツリーにマウントできます。 これには、YaSTの［*NFSクライアント*］モジュー

ルを使用するのが最も簡単です。NFSサーバのホスト名、インポートするディレクトリ、およびこのディレクトリをマウントするマウントポイントを入力するだけです。この操作はすべて、最初のダイアログボックス(図42.1.「YaSTによるNFSクライアント設定」 (page 692)) で [*追加*] をクリックした後に行います。 ［*Open Port in Firewall*］をクリックしてファイアウォールを開き、リモートコンピュータからサービスにアクセスすることを許可します。 チェックボックスの下には、ファイアウォールのステータスが表示されます。 ［*OK*］をクリックして、変更内容を保存します。図42.1.「YaSTによるNFSクライアント設定」 (page 692)を参照してください。

図 42.1 *YaSTによるNFSクライアント設定*



42.2 ファイルシステムの手動インポート

ファイルシステムは、NFSサーバから手動で容易にインポートできます。唯一の前提条件はRPCを実行していることです。RPCを起動するには`root`ユーザとして「`rcportmapstart`」コマンドを入力します。この前提条件さえ満たせば、それぞれのマシン上でエクスポートされたリモートファイルシステムを、自マシンのファイルシステムにマウントして、ローカルのハードディ

スクのように使用することができます。それには、mountコマンドを次の構文で使用します。

```
mount host:remote-path local-path
```

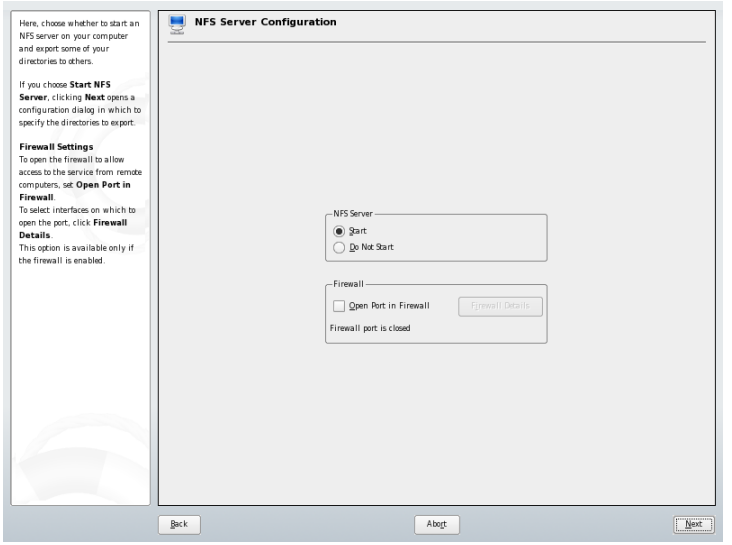
たとえば、マシンからユーザディレクトリをインポートする場合は、次のコマンドを使用します。

```
mount sun:/home /home
```

42.3 YaSTによるファイルシステムのエクスポート

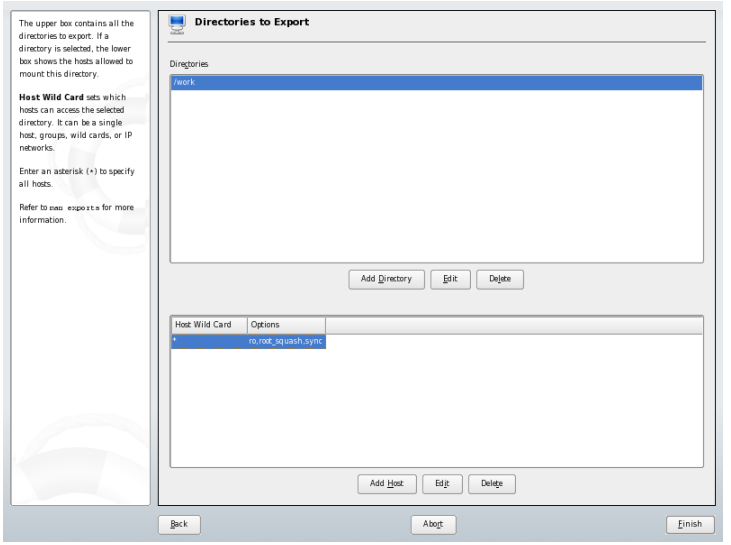
を使用して、ネットワーク上のホストをNFSサーバに変更し、そのホストへのアクセスを許可されたすべてのホストに、ディレクトリやファイルをエクスポートすることができます。 これにより、グループに属する全社員がそれぞれのホストにアプリケーションをローカルにインストールしなくても、全員にアプリケーションを提供できるようになります。NFSサーバをインストールするには、YaSTを起動して、*[ネットワークサービス]* → *[NFSサーバ]*の順に選択します。図 42.2. 「NFSサーバ設定ツール 」 (page 694)に示すダイアログが開きます。

図 42.2　NFSサーバ設定ツール



次に、［*NFSサーバを起動する*］を有効にし、［*次へ*］をクリックします。上部のテキストフィールドに、エクスポートするディレクトリを入力します。下部に、それらのディレクトリへのアクセスを許可するホストを入力します。図 42.3. 「YaSTによるNFSサーバの設定」 (page 695)に示すダイアログボックスが表示されます。 各ホストに対して設定できるオプションは、単独のホスト、ネットグループ、ワイルドカード、およびIPネットワークの4つです。これらのオプションの詳細については、`man exports`を参照してください。［完了］を選択して、設定を完了させます。

図 42.3　YaSTによるNFSサーバの設定



重要項目: 自動ファイアウォール設定

システムでファイアウォール(SuSEfirewall2)が有効になっている場合に、［ファイアウォールで開いているポート］を選択すると、YaSTは、`nfs`サービスを有効にすることでNFSサーバ用にファイアウォール設定を変更します。

42.4　ファイルシステムの手動エクスポート

を使用しない場合は、以下のシステムがNFSサーバ上で稼動していることを確認します。

- RPCポートマッパー(portmap)
- RPCマウントデーモン(rpc.mountd)
- RPC NFSデーモン(rpc.nfsd)

/etc/init.d/portmapスクリプトと/etc/init.d/nfsserverスクリプトを使用して、システムの起動時にこれらのサービスを起動するには、「insserv/etc/init.d/nfsserver」コマンドと「insserv/etc/init.d/portmap」コマンドを入力します。 また、どのファイルシステムを、どのホストにエクスポートするかを設定ファイル/etc/exportsに定義します。

エクスポートするディレクトリごとに1行を指定して、どのマシンがどのようなパーミッションでそのディレクトリにアクセスできるかを設定します。このディレクトリのすべてのサブディレクトリも、自動的にエクスポートされます。 許可するマシンは、通常、フルネーム(ドメイン名付き)で指定しますが、*や?(Bashシェルと同様に展開)のようなワイルドカードを使用することもできます。ここでマシンを指定しない場合、指定したパーミッションで、すべてのマシンがこのファイルシステムにアクセスできます。

エクスポートファイルシステムのパーミッションを、マシン名の後にカッコで囲んで設定します。重要なオプションを表42.1.「エクスポートされるファイルシステムのパーミッション」 (page 696)に示します。

表 42.1 *エクスポートされるファイルシステムのパーミッション*

オプション	意味
ro	ファイルシステムを読み込み専用(read only)パーミッションでエクスポートします(デフォルト)。
rw	ファイルシステムを読み書き可能パーミッションでエクスポートします。
root_squash	インポート側ホストのrootユーザが、このファイルシステムでrootパーミッションを持たないようにします。そのために、ユーザID 0 (rootユーザのID)に、ユーザID 65534が割り当てられます。このユーザIDは、nobody(デフォルト)に設定する必要があります。
no_root_squash	ユーザID 0をユーザID 65534に割り当てず、rootユーザのパーミッションを有効なままにします。

オプション	意味
link_relative	絶対リンク(/で始まるリンク)を../に変換します。これは、マシンのファイルシステム全体がマウントされている場合(デフォルト)のみ使用できます。
link_absolute	シンボリックリンクを変更しません。
map_identity	各ユーザIDがクライアントとサーバの両方で一致します(デフォルト)。
map_daemon	クライアントとサーバに、一致するユーザIDがありません。この結果、nfsdによってユーザIDの変換テーブルが作成されます。変換テーブルの作成には、ugiddデーモンが必要です。

exportsファイルの例を、例 42.1. 「/etc/exports」 (page 697)に示します。/etc/exportsが、mountdとnfsdによって読み込まれます。ファイルをまったく変更しない場合は、mountdとnfsdを再起動して、変更内容を有効にします。再起動は、rcnfsserverrestartによって簡単に実行できます。

例 42.1 /etc/exports

```
#
# /etc/exports
#
/home             sun(rw)    venus(rw)
/usr/X11          sun(ro)    venus(ro)
/usr/lib/texmf    sun(ro)    venus(rw)
/                 earth(ro,root_squash)
/home/ftp         (ro)
# End of exports
```

43

DHCP

dynamic host configuration protocol (DHCP)の目的は、ネットワーク環境設定を各ワークステーションでローカルに行うのではなく、サーバから一元的に割り当てることです。DHCPを使用するように設定されたクライアントは、自身の静的アドレスを制御できません。サーバからの指示に従って、すべてが自動的に設定されるからです。

DHCPの使用法の1つとして、ネットワークカードのハードウェアアドレス(ほとんどの場合、固定)を使用して各クライアントを識別し、そのクライアントがサーバに接続するたびに同じ設定を提供する方法があります。DHCPはまた、サーバが用意したアドレスプールから、アドレスを各クライアントに動的に割り当てるように設定することもできます。後者の場合、DHCPサーバはクライアントから要求を受信するたびに、接続が長期にわたる場合でも、クライアントに同じアドレスを割り当てようと試みます。当然ですが、これは、ホスト数がアドレス数を超えていない場合にのみ機能します。

DHCPはこれらの機能を提供することによって、システム管理者の作業負荷を2つの点で軽減します。サーバの環境設定ファイルを編集して、アドレスに関するあらゆる変更(大きな変更であっても)と一般的なネットワークの環境設定を一元的に実装できます。これは、多数のワークステーションをいちいち再設定するのに比べるてはるかに簡単です。また、特に新しいマシンをネットワークに統合する場合、IPアドレスをプールから割り当てられるので、作業が楽になります。適切なネットワークの環境設定をDHCPサーバから取得する方法は、日常的に、ラップトップをさまざまなネットワークで使用する場合に特に便利です。

DHCPサーバは、クライアントが使用するIPアドレスとネットマスクを供給するだけでなく、ホスト名、ドメイン名、ゲートウェイ、およびネームサーバ

アドレスも供給します。この他にも、DHCPを使用して一元的に設定できるパラメータがあり、たとえば、クライアントが現在時刻をポーリングするタイムサーバやプリントサーバも設定可能です。

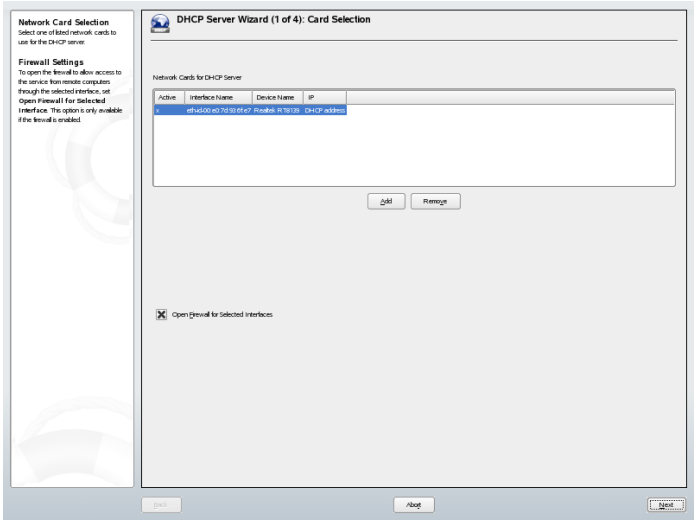
43.1 YaSTによるDHCPサーバの設定

このモジュールを初めて起動すると、サーバ管理に関して少数の基本的な事項を決定するように要求されます。この初期セットアップを完了すると、必要最低限の機能が設定された基本的なサーバ設定が生成されます。エキスパートモードは、さらに高度な設定タスクを行う場合に使用できます。

カードの選択

最初のステップでは、によりシステムで使用可能なネットワークインタフェースが検査され、リスト形式で表示されます。このリストから、DHCPサーバがリッスンするインタフェースを選択して、［*Add*］をクリックし、［*Open Firewall for Selected Interface*］をオンにして、そのインタフェース用にファイアウォールを開きます。図43.1.「DHCPサーバ: カードの選択」(page 700)を参照してください。

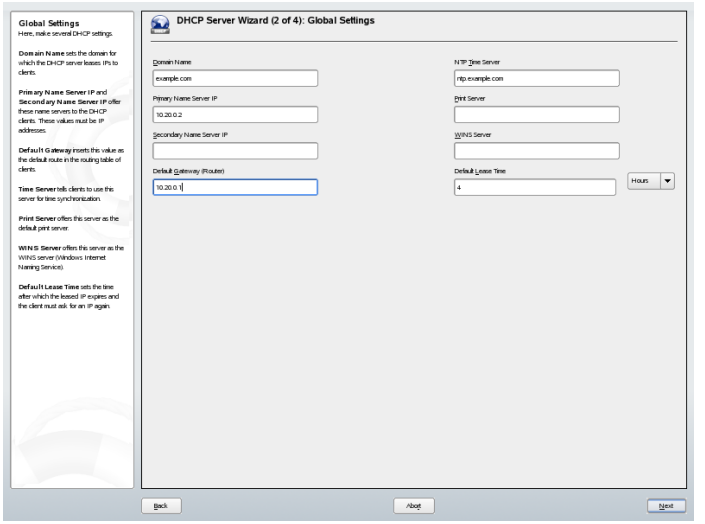
図 43.1 DHCPサーバ: カードの選択



グローバル設定

エントリフィールドに、DHCPサーバで管理する全クライアントのネットワークを指定します。この指定には、ドメイン名、タイムサーバのアドレス、プライマリネームサーバとセカンダリネームサーバのアドレス、印刷サーバとWINSサーバのアドレス(WindowsクライアントとLinuxクライアントの両方が混在するネットワークを使用する場合)、ゲートウェイアドレスおよびリース期間が含まれます。図43.2.「DHCPサーバ:グローバル設定」(page 701)を参照してください。

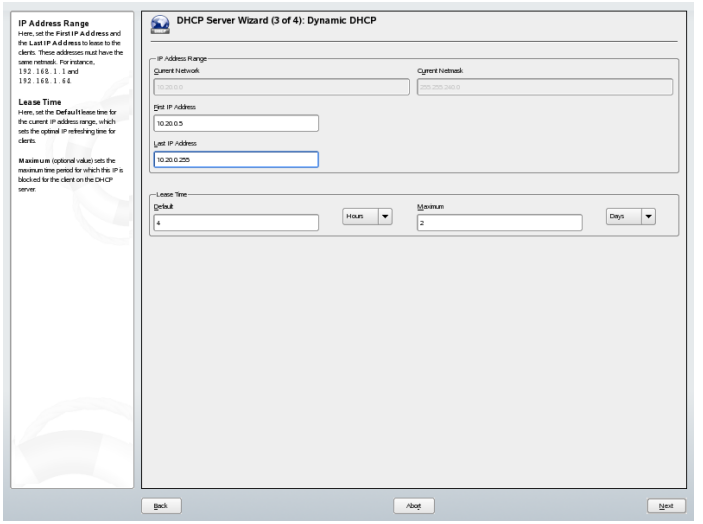
図 43.2　DHCPサーバ:グローバル設定



動的DHCP

このステップでは、クライアントに対する動的IPアドレスの割り当て方法を設定します。そのためには、サーバがDHCPクライアントに割当て可能なIPアドレスの範囲を指定します。これらのアドレスは、すべて同じネットマスクを使用する必要があります。また、クライアントがリースの延長を要求せずにIPアドレスを維持できるリース期間も指定します。必要に応じて、最大リース期間、つまりサーバが特定のクライアントのIPアドレスを保持している期間を指定します。図 43.3.「DHCPサーバ:動的DHCP 」(page 702)を参照してください。

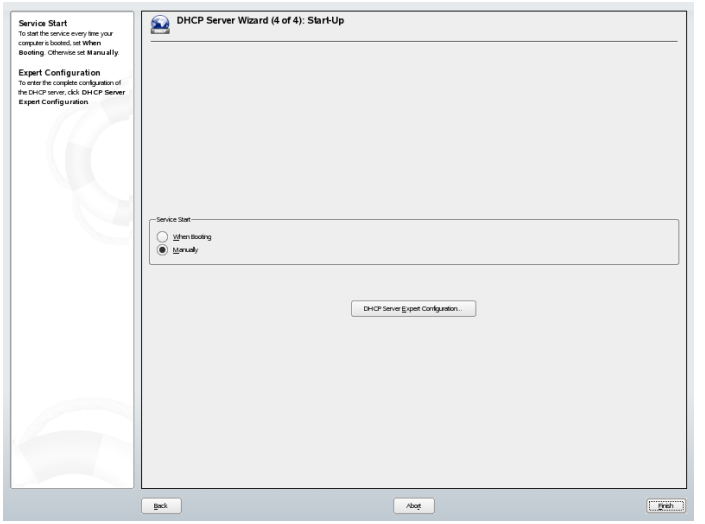
図 43.3　DHCPサーバ:動的DHCP



環境設定の完了と実行モードの設定

環境設定ウィザードの3つ目の手順を終了すると、最後にDHCPサーバの起動方法を定義するダイアログが表示されます。ここでは、システムのブート時にDHCPサーバを自動的に起動するか、テスト時など必要に応じて手動で起動するかを指定します。［完了］をクリックして、サーバの環境設定を完了します。図 43.4.「DHCPサーバ:起動」 (page 703)を参照してください。

図 43.4　DHCPサーバ:起動



43.2　DHCPソフトウェアパッケージ

SUSE Linuxでは、DHCPサーバとDHCPクライアントのどちらも利用可能です。用意されているDHCPサーバは、dhcpd (Internet Software Consortium製)です。 クライアント側では、DHCPクライアントプログラムとして、dhclient (同じくISC製)またはdhcpcdパッケージのDHCPクライアントデーモンのどちらかを選択できます。

SUSE Linuxは、デフォルトでdhcpcdをインストールします。このプログラムは非常に扱いやすく、システムブート時に自動的に起動して、DHCPサーバを監視します。環境設定ファイルは必要ありません。標準的な設定であればほとんどの場合、そのまま使用できます。 複雑な状況で使用する場合は、環境設定ファイル/etc/dhclient.confによって制御されるISC dhclientを使用します。

43.3 DHCPサーバdhcpd

DHCPシステムの中核には、動的ホスト環境設定プロトコルデーモンがあります。このサーバは、環境設定ファイル/etc/dhcpd.confに定義された設定に従ってアドレスをリースし、その使用状況を監視します。システム管理者は、このファイルのパラメータと値を変更して、プログラムの動作をさまざまな方法で調整できます。例43.1.「環境設定ファイル/etc/dhcpd.conf」 (page 704)で、/etc/dhcpd.confファイルの基本的な例を見てみましょう。

例 43.1 *環境設定ファイル/etc/dhcpd.conf*

```
default-lease-time 600;          # 10 minutes
max-lease-time 7200;             # 2  hours

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

DHCPサーバを用いてネットワーク内でIPアドレスを割り当てるには、このサンプルのような環境設定ファイルを用意すれば十分です。各行の末尾にセミコロンが付いていることに注意してください。これがなければ、dhcpdは起動しません。

このサンプルファイルは、3つのセクションに分けられます。最初のセクションは、要求側クライアントにIPアドレスがリースされた場合に、デフォルトで最大何秒間経過すればリースの更新が必要になるか(デフォルトリース時間)が定義されます。このセクションには、DHCPサーバがマシンにIPアドレスを割り当てた場合に、マシンが更新を求めずにそのIPアドレスを保持できる最大時間(max-lease-time)も指定されています。

2つ目のセクションでは、基本的なネットワークパラメータがグローバルレベルで定義されています。

- option domain-nameの行は、ネットワークのデフォルトドメインを定義してます。

- option domain-name-serversエントリには、IPアドレスをホスト名(また逆方向に)に解決するためのDNSサーバを最高3つを指定します。ネームサーバは、DHCPをセットアップする前に、使用しているマシン上またはネットワーク上のどこか他の場所で設定するのが理想的です。ネームサーバではまた、各ダイナミックアドレスに対してホスト名を定義し、またその逆も定義する必要があります。独自のネームサーバを設定する方法については、章 40. ドメインネームシステム (page 661)を参照してください。

- option broadcast-addressの行は、要求側クライアントが使用するブロードキャストアドレスを定義します。

- option routersの行では、ローカルネットワークでホストに配信できないデータパケットの送信先を(指定されたソース／ターゲットホストアドレスおよびサブネットに応じて)サーバに指示します。ほとんどの場合、特に小規模ネットワークでは、このルータはインターネットゲートウェイと同一です。

- option subnet-maskでは、クライアントに割り当てるネットマスクを指定します。

ファイルの最後のセクションでは、サブネットマスクを含め、ネットワークを定義します。最後に、DHCPが対象のクライアントにIPアドレスを割り当てるために使用するアドレス範囲を指定します。この例では、クライアントは192.168.1.10～192.168.1.20および192.168.1.100～192.168.1.200の範囲にある任意のアドレスを与えられます。

これら数行を編集すると、rcdhcpdstartコマンドを使用してDHCPデーモンを有効にできるようになります。DHCPデーモンはすぐに使用できます。rcdhcpdcheck-syntaxコマンドを使用すると、簡単な構文チェックを実行できます。サーバでエラーが発生して中断する、起動時にdoneが返されないなど、環境設定に関して予期しない問題が発生した場合は、メインシステムログ/var/log/messagesまたはコンソール10 (Ctrl+Alt+F10)で情報を探せば、原因が突き止められます。

デフォルトのSUSE Linuxシステムでは、セキュリティを確保するためにchroot環境からDHCPデーモンを起動します。デーモンが見つけられるように、環境設定ファイルは、chroot環境にコピーします。このファイルは、rcdhcpdstartコマンドによって自動的にこのファイルがコピーされるので、通常は、手動でコピーする必要はありません。

43.3.1 固定IPアドレスを持つホスト

前述のように、DHCPを使用すると、特定のクライアントが要求を行うたびに事前に定義した静的アドレスを割り当てることができます。明示的に割り当てられるアドレスは、プールから割り当てられる動的アドレスに常に優先します。また、たとえばアドレスが不足していて、サーバがクライアント間でアドレスを再配布する必要がある場合でも、静的アドレスは動的アドレスと違って期限切れになりません。

*静的*アドレスを割り当てられたホストを識別するために、dhcpdは、ハードウェアアドレスを使用します。ハードウェアアドレスは、6つのオクテットペアで構成される世界で唯一の固定数値コードで、すべてのネットワークデバイスの識別に使用されます(たとえば、`00:00:45:12:EE:F4`)。たとえば、例 43.2. 「環境設定ファイルへの追加」 (page 706)のような数行を例 43.1. 「環境設定ファイル/etc/dhcpd.conf」 (page 704)に示す環境設定ファイルに追加すると、DHCPデーモンはあらゆる状況で、対応するホストに常に同じデータのセットを割り当てます。

例 43.2 *環境設定ファイルへの追加*

```
host earth {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

対応するクライアントの名前(`host`クライアント名、ここでは`earth`)を1行目に、MACアドレスを2行目に入力します。Linuxホストでこのアドレスを確認するには、`ifstatus`コマンドの後にネットワークデバイス(たとえば、`eth0`)指定して実行します。必要に応じて`ifupeth0`を実行し、ネットワークカードを有効にします。出力例を次に示します。

```
link/ether 00:00:45:12:EE:F4
```

上の例では、MACアドレス`00:00:45:12:EE:F4`を持つネットワークカードが装着されたクライアントに、IPアドレス`192.168.1.21`とホスト名earthが自動的に割り当てられます。指定するハードウェアの種類は、ほとんどの場合`ethernet`ですが、IBMシステムでよく使用される`token-ring`もサポートされています。

43.3.2 SUSE Linuxのバージョン

セキュリティ向上のため、バージョンのISC製DHCPサーバには、Ari Edelkind氏開発の非root/chrootパッチが付属しています。これにより、dhcpdをユーザIDnobodyで実行したり、chroot環境で実行したりできます(/var/lib/dhcp)。これの機能を使用するには、環境設定ファイルdhcpd.confが/var/lib/dhcp/etcに存在する必要があります。initスクリプトは、起動時に環境設定ファイルをこのディレクトリに自動的にコピーします。

この機能に関するサーバの動作は、環境設定ファイル/etc/sysconfig/dhcpdのエントリを使用して制御できます。非chroot環境でdhcpdを実行するには、/etc/sysconfig/dhcpd内の変数DHCPD_RUN_CHROOTEDを「no」に設定します。

chroot環境内であっても、dhcpdを有効にしてホスト名を解決するには、次のような他の環境設定ファイルをコピーする必要があります。

- /etc/localtime
- /etc/host.conf
- /etc/hosts
- /etc/resolv.conf

これらのファイルは、initスクリプトの起動時に、/var/lib/dhcp/etc/にコピーされます。コピーされたファイルが/etc/ppp/ip-upのようなスクリプトによって動的に変更されている場合は、必要な変更箇所がないか注意する必要があります。ただし、環境設定ファイルに(ホスト名でなく) IPアドレスだけを指定している場合は、これについて考える必要はありません。

環境設定の中に、chroot環境にコピーすべき追加ファイルが存在する場合は、ファイルetc/sysconfig/dhcpdの変数DHCPD_CONF_INCLUDE_FILESに、これらのファイルを指定します。syslogデーモンの再起動後もDHCPロギング機能が作動していることを確認するには、ファイル/etc/sysconfig/syslogのSYSLOGD_PARAMSにオプション"-a /var/lib/dhcp/dev/log"を追加する必要があります。

43.4 関連資料

DHCPの詳細については、*Internet Software Consortium*のWebサイト(http://www.isc.org/products/DHCP/)を参照してください。また、dhcpd、dhcpd.conf、dhcpd.leases、およびdhcp-optionsの各マニュアルページにも詳細が記載されています。

44 xntpによる時刻の同期

NTP (network time protocol)メカニズムは、システムの時刻をネットワーク上で同期させるためのプロトコルです。最初に、マシンは信頼できる時刻を持つサーバに時刻を照会できます。次に、ネットワーク上の他のコンピュータがこのマシン自体に対し、時刻を照会できます。目的は2つあり、絶対的な時間を維持することと、ネットワーク内のすべてのマシンのシステム時刻を同期させることです。

正確なシステムタイムを維持することはさまざまな場で重要です。ハードウェア組み込み型(BIOS)クロックがデータベースなどのアプリケーション要件に合致しないことがよくあります。システムタイムを手動で修正することは時に問題を発生させる可能性があります。たとえば、時間を逆廻りに戻すことで重要なアプリケーションの誤動作を誘発することもあります。ネットワーク内では、通常すべてのマシンのシステムタイムを同期させておかなければなりませんが、手動での調整は適切な方法ではありません。xntpではこれらの問題を解決するメカニズムを備えています。このメカニズムは常にネットワーク上の信頼できるタイムサーバに照会することで、システムタイムを調整します。さらに、電波時計のようなローカルリファレンスクロックを管理する機能があります。

44.1 YaSTでのNTPクライアントの設定

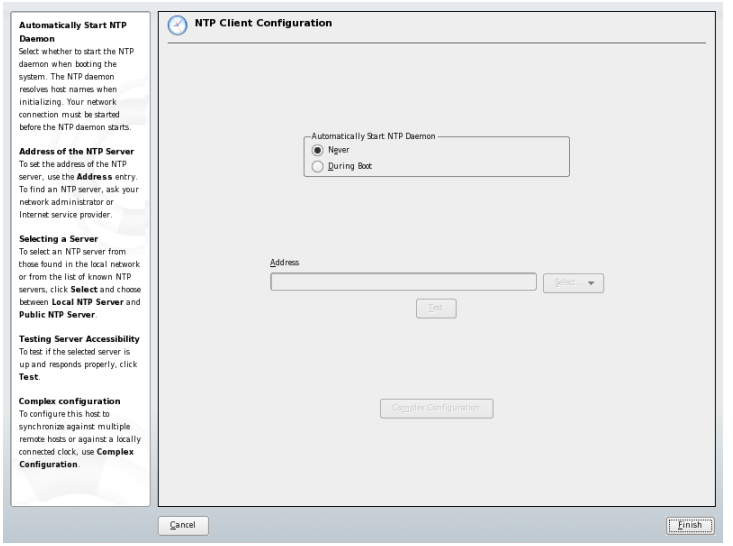
xntpは、ローカルのコンピュータクロックを時刻の標準として参照するように事前に設定されています。ただし、BIOSクロックの使用は、それ以上に正確

な時刻ソースが利用できない場合の代替として以外は避けるようにしてください。SUSE Linuxでは、YaSTによってNTPクライアントの設定を容易に行えます。 保護されているイントラネットの一部になっているので、SuSEfirewallを実行していないクライアントで、簡単な、または複雑な設定を行ってください。これら2つの方法について次に説明します。

44.1.1 NTPクライアントの簡易設定

NTPクライアントの簡易設定(*[ネットワークサービス] → [NTP Client]*の順に選択)には、2つのダイアログがあります。最初のダイアログでは、xntpdの実行モードおよびクエリ先のNTPサーバを設定します。システムのブート時にxntpdを自動起動させるには、[*When Booting System*]をクリックします。次に、[*選択*]をクリックして2番目のダイアログを開きます。このダイアログでは、使用しているネットワークに適したタイムサーバを選択します。

図 44.1 YaST:: NTPクライアントの設定



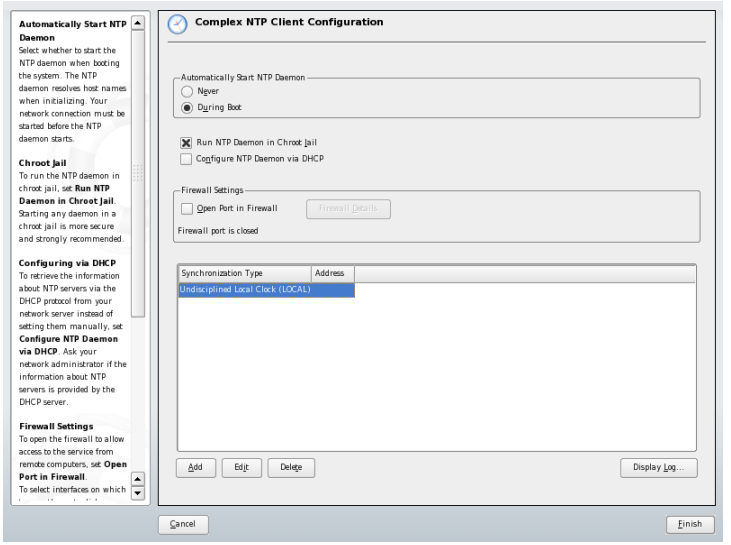
サーバ選択用の詳細ダイアログでは、ローカルネットワーク上のタイムサーバ(［*Local Network*］)とインターネット上のタイムサーバ(［*Public NTP Server*］)のどちらを使用して時刻の同期を行うかを指定します。ローカルタイムサーバを使用する場合は、[*検索*]をクリックして、ネットワーク上の利用可能なタイムサーバを問い合わせるSLPクエリを実行します。検索結果のリストから最

適なタイムサーバを選択し、[*了解*]をクリックしてダイアログを閉じます。インターネット上の公開タイムサーバを使用する場合は、国(タイムゾーン)および適切なタイムサーバを[*公開NTPサーバ*]のリストから選択し、[*了解*]をクリックしてダイアログを閉じます。メインダイアログで、[テスト]をクリックして選択したサーバが利用可能かどうかをテストし、[*完了*]をクリックしてダイアログを閉じます。

44.1.2 NTPクライアントの詳細設定

NTPクライアントの詳細設定は、簡易設定の項目で説明した実行モードを選択した後、[*NTPクライアント*]モジュールのメインダイアログの[*詳細設定*](図 44.1. 「YaST:: NTPクライアントの設定」 (page 710)を参照)をクリックすると表示されます。

図 44.2 YaST:NTPクライアントの詳細設定



[*NTPクライアントの詳細設定*]で、xntpdをchroot jailで実行するかどうかを指定します。このオプションは、xntpd上の攻撃に対するセキュリティを強化し、不正ユーザによってシステム全体が危険な状態に陥ることを防ぎます。 [*DHCPからNTPデーモンを設定*]は、ローカルネットワーク上のNTPサーバのリストをDHCP経由で取得するようにNTPクライアントを設定します。

ダイアログ下部には、クライアントに対するサーバおよび時刻情報のその他の情報源が表示されます。必要に応じて、[*追加*]、[*削除*]、および[*編集*]を使用してこのリストを変更します。［*Display Log*］では、クライアントのログファイルを表示できます。

時刻情報の情報源を追加するには、[*追加*]をクリックします。表示されるダイアログで、時刻同期に使用する情報源のタイプを選択します。使用可能なオプションは次のとおりです。

サーバ:
[同期相手のタイプの選択]ダイアログで、(項44.1.1.「NTPクライアントの簡易設定」 (page 710)で説明したように)NTPサーバを選択できます。システムのブート時にサーバとクライアント間で時刻情報の同期を実行するには、[*初期同期に用いる*]を有効にします。入力フィールドでは、xntpdの追加オプションを指定できます。詳細は、`/usr/share/doc/packages/xntp-doc` (`xntp-doc`パッケージの一部)を参照してください。

ピア
ピアとは対の関係にあるマシンを意味します。たとえば、時刻サーバとクライアントのどちらの役割にもなります。サーバの代わりに、同じネットワーク内のピアを使用するには、そのピアシステムのアドレスを入力します。ダイアログのそれ以外の内容は［サーバ］ダイアログと同じです。

ラジオクロック
時刻同期にシステムのラジオクロックを使用するには、クロックタイプ、ユニット番号、デバイス名、およびその他のオプションをこのダイアログで指定します。ドライバを微調整するには、[*ドライバの調整*]をクリックします。ローカルのラジオクロックに関する詳細な情報は`/usr/share/doc/packages/xntp-doc/html/refclock.htm`を参照してください。

ブロードキャストの発信
時刻情報とクエリは、ネットワーク上にブロードキャストすることができます。このダイアログでは、このブロードキャストの送信先を指定します。電波時計のような信頼できる時刻ソースがない限りブロードキャストをアクティブにしないでください。

ブロードキャストの着信
クライアントで情報をブロードキャスト経由で受け取る場合は、どのアドレスからのパケットを受け入れるかをこのフィールドに指定します。

44.2 ネットワークでのxntp構成

ネットワーク内のタイムサーバを使用するには、serverパラメータを設定するのが最も簡単です。たとえば、ネットワークからntp.example.comという名前のタイムサーバに到達できる場合は、server ntp.example.comという行を追加して、ファイル/etc/ntp.confにこのサーバ名を追加します。別のタイムサーバを追加するには、別の行にキーワードserverを挿入します。rcxntpd startコマンドでxntpdを初期化すると、アプリケーションは時計が安定するまで1時間待機し、ドリフトファイルを作成してローカルコンピュータのクロックを修正します。ドリフトファイルを用いることで、バードウェアクロックの定誤差はコンピュータの電源が入った時点で、すぐに算出されます。修正はすぐに反映されるため、システム時刻がより安定します。

クライアントとしてNTPメカニズムを使用する方法が2つあります。1つ目はクライアントが定期的に既知のサーバに対し、時刻を照会する方法です。クライアント数が多い場合、この方法はサーバの過負荷を引き起こす可能性があります。2つ目は、ネットワークでブロードキャストを行う時刻サーバから送信されるNTPブロードキャストを、クライアントが待機する方法です。この方法には不利な面があります。サーバの精度が不明なこと、そしてサーバから送信される情報が誤っていた場合、深刻な問題が発生する可能性があることです。

ブロードキャスト経由で時刻を取得する場合、サーバ名は必要ではありません。この場合は、設定ファイル/etc/ntp.confに行broadcastclientを記述します。1つ以上の信頼された時刻サーバのみを使用するには、serversで始まる行にサーバの名前を記述します。

44.3 ローカルリファレンスクロックの設定

ソフトウェアパッケージxntpには、ローカルリファレンスクロックに接続するためのドライバが含まれています。サポートされているクロックのリストは、xntp-docパッケージのファイル/usr/share/doc/packages/xntp-doc/html/refclock.htmに記載されています。各ドライバには、番号が関連付けられています。xntpの実際の設定は、疑似IPを使用して行われます。クロックは、ネットワークに存在しているものとしてファイル/etc/ntp.confに

入力されます。このため、これらのクロックには127.127.t.uという形式の特別なIPアドレスが割り当てられます。ここで、tはクロックのタイプを示し、使用されているドライバを決定します。uはユニットのタイプを示し、使用されているインタフェースを決定します。

通常、各ドライバは設定をより詳細に記述する特別なパラメータを持っています。ファイル/usr/share/doc/packages/xntp-doc/html/driverNN.htm(ここでNNはドライバの番号)は特定のクロックタイプに関する情報を提供します。たとえば、「タイプ8」クロック(シリアルインタフェース経由のラジオクロック)はクロックをさらに細かく指定する追加モードを必要とします。また、Conrad DCF77レシーバモジュールはモード5です。このクロックを優先参照として使用するには、キーワードpreferを指定します。Conrad DCF77レシーバモジュールの完全なserver行は次のようになります。

```
server 127.127.8.0 mode 5 prefer
```

他のクロックも同じパターンで記述されます。xntp-docパッケージのインストール後に、ディレクトリ/usr/share/doc/packages/xntp-doc/htmlにあるxntpのマニュアルを参照してください。これらのパラメータについては、説明のあるドライバページへのリンクがファイル/usr/share/doc/packages/xntp-doc/html/refclock.htmに記述されています。

45 LDAP—ディレクトリサービス

LDAP (Lightweight Directory Access Protocol)は、情報ディレクトリへのアクセスと管理を行うために設計されたプロトコルセットです。LDAPは、ユーザおよびグループ管理、システム構成の管理、アドレス管理など、さまざまな目的に使用できます。この章では、OpenLDAPの動作原理とYaSTを使用したLDAPデータの管理方法の基本事項について説明します。LDAPプロトコルには複数の実装方法がありますが、この章ではもっぱらOpenLDAPの実装を中心に説明します。

ネットワーク環境では、重要な情報をすぐに利用できるように整理しておくことは不可欠です。そのため、一般的に使用されているイエローページのようなディレクトリサービスを使用して、情報を整理し、すぐに検索できる形式にしておくことができます。

理想的なケースは、一元的なサーバでデータをディレクトリに保持し、特定のプロトコルを使用してそれをすべてのクライアントに配布するという形態です。データはさまざまなアプリケーションがアクセスできる方法で整理されます。この方法では、個々のカレンダツールや電子メールクライアントが独自のデータベースを持つ必要はありません。一元的なリポジトリにアクセスすればよいためです。これにより、情報管理のための負荷も大幅に軽減されます。LDAP (lightweight directory access protocol)のようなオープンで標準化されたプロトコルを使用すれば、可能な限り多くの異なるクライアントアプリケーションが、このような情報にアクセスできるようになります。

この文脈でのディレクトリとは、高速かつ効果的に読み込みと検索ができるように最適化された一種のデータベースです。

- 膨大な(同時)読み込みとアクセスを可能にするため、書き込みアクセスは、管理者による少量の更新作業に限られます。従来のデータベースは、できる限り大量のデータを短時間に受け付けられるように最適化されます。

- 書き込みアクセスは制約された形でのみ可能なため、ディレクトリサービスは、ほとんどが変更のない静的情報の管理に使用されます。一般に、非常に頻繁に変更されるデータ(*動的*データ)は、従来のデータベースに保存されます。たとえば、企業ディレクトリにある電話番号は、経理で管理する数字ほど頻繁に変更されません。

- 静的データを管理する場合、既存のデータセットの更新は非常にまれです。動的データ、特に銀行口座や経理のデータセットが関与する場合、データの一貫性が最重要課題となります。たとえばある項目から差し引かれた金額を他の項目に加算する場合、データストックで残高を正しく維持するためには、1回の*トランザクション*内で両方の操作が同時に行われる必要があります。データベースはこのようなトランザクションをサポートしますが、ディレクトリではサポートされません。ディレクトリでは、短期的にデータの一貫性が崩れても大きな問題にはなりません。

LDAPなどのディレクトリサービスの設計には、複雑な更新やクエリメカニズムのサポートは含まれません。このサービスにアクセスするすべてのアプリケーションが、すばやく簡単にアクセスできることが主な課題です。

Unixでも他のシステムでも、多くのディレクトリサービスがこれまでに存在し、今なお存在しています。いくつか例を挙げると、Novell NDS、Microsoft ADS、BanyanのStreet Talk、OSI標準のX.500などがあります。LDAPは元々、DAP (directory access protocol)の無駄な機能を省略したサービスであり、X.500へのアクセスを目的として開発されました。X.500標準は、ディレクトリエントリの階層構造を規定しています。

LDAPは、DAPの簡易版です。LDAPでは、X.500エントリ階層が維持されているため、プラットフォーム非依存という特長を持ち、必要なリソースも少なくて済みます。TCP/IPを使用することにより、ドッキングアプリケーションとLDAPサービス間のインタフェースが、非常に簡単に確立できます。

一方でLDAPは、X.500サポートとは別に進化し、スタンドアロンソリューションとして採用されることが多くなっています。LDAPはLDAPv3の*照会*(パッケージ`openldap2`のプロトコルバージョン)をサポートすることによって、分

散データベースを実現しています。SASL (simple authentication and security layer)も新しく採用されています。

LDAPの機能は、当初の計画ではX.500サーバにデータを問い合わせることだけでしたが、現在はそれだけにとどまりません。slapdというオープンソースサーバが存在し、オブジェクト情報をローカルデータベースに格納できます。また複数のLDAPサーバへのレプリケートを行うslurpdという拡張機能もあります。

`openldap2`パッケージの構成は、次のとおりです。

slapd
スタンドアロンのLDAPv3サーバ。オブジェクト情報をBerkeleyDBベースのデータベースで管理します。

slurpd
このプログラムは、データの変更をローカルLDAPサーバから、ネットワーク上にインストールされた他のLDAPサーバへレプリケートします。

システム管理用の追加ツール
`slapcat`、`slapadd`、`slapindex`

45.1 LDAPとNISの比較

Unix系システムの管理者は、従来から、ネットワーク内の名前の解決やデータ配信にNISサービスを使用しています。設定データは`/etc`内のファイルに保存され、`group`、`hosts`、`mail`、`netgroup`、`networks`、`passwd`、`printcap`、`protocols`、`rpc`、および`services`の各ディレクトリは、ネットワーク内の複数のクライアントに分散されています。これらのファイルはシンプルテキストファイルのため、保守にそれほどの手間はかかりません。しかし、構造化されていないため、大量のデータを処理することがますます困難になっています。NISはUnix系プラットフォーム専用に設計されているため、異種ネットワークでの一元的データ管理には採用できません。

LDAPサービスはNISと異なり、純粋なUnix系ネットワークに制限されていません。Windowsサーバ(2000以降)は、LDAPをディレクトリサービスとしてサポートします。NovellもまたLDAPサービスを提供します。前述のアプリケーションタスクは、Unix系以外のシステムでもサポートされます。

LDAPの原則は、一元管理が必要なあらゆるデータ構造に適用可能です。いくつかの例を次に示します。

- NISサービスの代替としての採用
- メールルーティング(postfix、sendmail)
- Mozilla、Evolution、およびOutlookなどのメールクライアント用アドレス帳
- BIND9ネームサーバのゾーン記述の管理
- 異種ネットワークでのSambaのユーザ認証

LDAPはNISと異なり拡張できるため、これら以外にも広範な用途が考えられます。データが明確に定義された階層構造になっているため、検索が容易であり、大量データの管理が非常に容易になります。

45.2 LDAPディレクトリツリーの構造

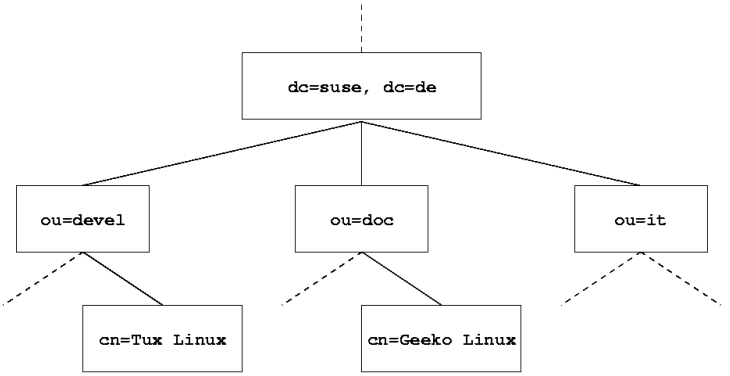
LDAPディレクトリは、ツリー構造です。ディレクトリのすべてのエントリ(オブジェクトと呼びます)には、この階層内に定義された位置があります。この階層は*ディレクトリ情報ツリー*(DIT)と呼ばれます。対象のエントリへの完全パスは、*識別名*(DN)と呼ばれ、確実にエントリを識別します。このエントリへのパス上にある個々のノードを*相対識別名*(RDN)と呼びます。オブジェクトは、一般的に、2つのタイプのいずれかに割り当てられます。

コンテナ
: これらのオブジェクトは、それ自体に他のオブジェクトを持っています。オブジェクトクラスには`root`(ディレクトリツリーのルート要素。実際には存在しません)、`c`(国)、`ou`(組織単位)、`dc`(ドメインコンポーネント)があります。このモデルは、ファイルシステムのディレクトリ(フォルダ)にあたります。

リーフ
: これらのオブジェクトは、ブランチの端にあり、下位のオブジェクトを持ちません。たとえば、`person`、`InetOrgPerson`、または`groupofNames`があります。

ディレクトリ階層の最上位には、ルート要素rootがあります。これには、下位要素として、c (国)、dc (ドメインコンポーネント)、またはo (組織)が含まれます。LDAPディレクトリ内ツリーの関係については、図45.1.「LDAPディレクトリの構造」 (page 719)に示す次の例で詳細に説明します。

図 45.1　LDAPディレクトリの構造



この図は、架空のディレクトリ情報ツリーです。3レベルのエントリが示されています。各エントリは、図内の1つの箱に対応します。最後に、このケースにおける架空のSUSE社員Geeko Linuxの*識別名*をcn=Geeko Linux,ou=doc,dc=suse,dc=deとします。この識別名は、RDNcn=Geeko Linuxを前のエントリのDNou=doc,dc=suse,dc=deに追加して構成されます。

DITに格納するオブジェクトのタイプをグローバルに決定するには、次のスキーマが使用されます。オブジェクトタイプは、*オブジェクトクラス*によって決定されます。オブジェクトクラスは、オブジェクトに割り当てる、または割り当てられる属性を決定します。したがって、スキーマには、すべてのオブジェクトクラスと、想定したアプリケーションシナリオで使用される属性の定義を含む必要があります。RFC 2252と2256では、一般的なスキーマがいくつか用意されています。しかし、LDAPサーバの操作環境で必要になる場合は、カスタムスキーマを作成したり、複数のスキーマを相互補完的に使用することもできます。

表45.1.「一般的に使用されるオブジェクトクラスと属性」 (page 720)では、前述の例で使用されているcore.schemaとinetorgperson.schemaのオブジェクトクラスについて、必要な属性や有効な属性値などの簡単な概要を示します。

表 45.1　一般的に使用されるオブジェクトクラスと属性

オブジェクトクラス	意味	例で使用されているエントリ	必須の属性
dcObject	*domainComponent* (ドメインのコンポーネントの名前を指定します)	suse	dc
organizationalUnit	*organizationalUnit* (組織単位)	doc	ou
inetOrgPerson	*inetOrgPerson* (イントラネットまたはイントラネット用の個人関連情報)	Geeko Linux	snとcn

例 45.1. 「schema.coreからの抜粋」 (page 720)は、説明の付いたスキーマディレクティブからの抜粋です(行番号は説明のために付けられています)。

例 45.1　schema.coreからの抜粋

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName' ) #2
DESC 'RFC2256:organizational unit this object belongs to' #3        SUP name
 )

... #4 objectclass ( 2.5.6.5 NAME 'organizationalUnit' #5        DESC
'RFC2256:an organizational unit' #6        SUP top STRUCTURAL #7        MUST
 ou #8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory $
x121Address $ registeredAddress $ destinationIndicator $
preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
telephoneNumber $ internationaliSDNNumber $ facsimileTelephoneNumber $ street
 $ postOfficeBox $ postalCode $ postalAddress $ physicalDeliveryOfficeName $
 st $ l $ description) ) ...
```

属性タイプ`organizationalUnitName`とそれに対応するオブジェクトクラス`organizationalUnit`がここで例として使用されています。1行目では、属性名、一意のOID(*オブジェクト識別子*)(数値)、および属性値の省略名が指定されています。

2行目には、`DESC`を使用して、属性の簡単な説明が記入されています。この定義がどのRFCに基づいているかもここに記載されます。3行目の`SUP`は、この属性が属する上位属性を示します。

オブジェクトクラスorganizationalUnitの定義は、4行目から始まり、属性の定義と同様、OEDとオブジェクトクラスが最初に定義されます。行目はオブジェクトクラスの簡単な説明です。SUP topで始まる6行目は、このオブジェクトクラスが他のオブジェクトクラスの上位でないことを示します。MUSTで始まる7行目は、タイプorganizationalUnitのオブジェクトで*使用*する必要がある属性値をすべてリストします。MAYで始まる8行目は、このオブジェクトクラスで使用できる属性値をすべてリストします。

スキーマの用途については、OpenLDAPのマニュアルにわかりやすく説明されています。これはインストール後に、/usr/share/doc/packages/openldap2/admin-guide/index.htmlで参照してください。

45.3 slapd.confを使用したサーバの設定

インストールされたシステムでは、/etc/openldap/slapd.confにLDAPサーバの完全な設定ファイルが用意されています。ここでは1つのエントリについて簡単に説明し、必要な調整について説明します。ハッシュ(#)で始まるエントリは無効です。エントリを有効にするには、このコメント文字を削除します。

45.3.1 slapd.conf内のグローバルエントリ

例 45.2 slapd.conf: スキーム用ディレクティブの取り込み

```
include         /etc/openldap/schema/core.schema include
/etc/openldap/schema/cosine.schema include
/etc/openldap/schema/inetorgperson.schema include
/etc/openldap/schema/rfc2307bis.schema include
/etc/openldap/schema/yast.schema
```

例 45.2.「slapd.conf: スキーム用ディレクティブの取り込み」 (page 721)に示すように、slapd.confにある最初のディレクティブは、LDAPディレクトリを編成するスキーマを指定します。エントリcore.schemaは必須です。付加的に必要とされるスキーマは、このディレクティブの後に追加します。詳細については、OpenLDAPのマニュアルを参照してください。

例 45.3　slapd.conf: pidfileとargsfile

```
pidfile  /var/run/slapd/slapd.pid
argsfile  /var/run/slapd/slapd.args
```

この2つのファイルには、PID (プロセスID)とslapdプロセスの起動時に使用される引数が含まれています。これらを変更する必要はありません。

例 45.4　slapd.conf: アクセス制御

```
# Sample Access Control #       Allow read access of root DSE # Allow self
write access #       Allow authenticated users read access #       Allow
anonymous users to authenticate # access to dn="" by * read access to * by
self write by users read by anonymous auth # # if no access controls are
present, the default is: #       Allow read by all # # rootdn can always write!
```

例 45.4. 「slapd.conf: アクセス制御」 (page 722)は、サーバ上のLDAPディレクトリへのアクセス許可を制御するslapd.confの一部です。slapd.confのグローバルセクションで行われている設定は、データベース固有のセクションで、カスタムのアクセス規則が宣言されていない限り有効です。これらはグローバル宣言を上書きするためです。ここで示すように、すべてのユーザはディレクトリの読み込みアクセスができますが、ディレクトリに書き込めるのは管理者(rootdn)のみです。LDAPのアクセス制御の管理は、非常に複雑なプロセスです。次のヒントが役立ちます。

- すべてのアクセス規則は、次の構造に従います。

  ```
  access to <what> by <who> <access>
  ```

- *what*には、アクセスを付与するオブジェクトまたは属性を指定します。個々のディレクトリブランチを、別の規則で明示的に保護することもできます。正規表現を使用して、ディレクトリのある部分を1つの規則で処理することも可能です。slapdは、設定ファイルでリストされている順序で、すべての規則を評価します。一般的な規則は、特定的な規則の後に指定する必要があります。slapdが有効だと考える最初の規則が評価され、それ以降のエントリは無視されます。

- *who*には、*what*で指定された領域へのアクセスを付与されるユーザを指定します。ここでもslapdは、最初に一致するwhoを見つけた後、評価を行わないため、特定の規則は、一般的な規則より前に指定する必要があります。表45.2.「ユーザグループと付与されるアクセス許可」 (page 723)に有効なエントリを示します。

表 45.2　ユーザグループと付与されるアクセス許可

タグ	スコープ
*	例外なくすべてのユーザ
anonymous	認証されていない(「匿名」)ユーザ
ユーザ	認証済みユーザ
self	ターゲットオブジェクトに接続されているユーザ
dn.regex=<regex>	正規表現に一致するすべてのユーザ

- *access*は、アクセスタイプを指定します。表45.3.「アクセスのタイプ」(page 723)に示すオプションを使用してください。

表 45.3　アクセスのタイプ

タグ	アクセスのスコープ
none	アクセス不可
auth	サーバへの連絡用
compare	比較アクセス用のオブジェクト
search	検索フィルタ設定用
read	読み込みアクセス
write	書き込みアクセス

slapdはクライアントが要求するアクセス権をslapd.confで付与されたアクセス権と比較します。要求された権限と比較して、同等または上位の権限が規則によって与えられている場合は、クライアントに対して、アク

セスが許可されます。規則に宣言された権限を越える権限をクライアントが要求した場合、アクセスが拒否されます。

例 45.5.「slapd.conf: アクセス制御の例」 (page 724)に、簡単なアクセス制御の例を示します。このように正規表現を用いて自由にアクセス制御できます。

例 45.5 slapd.conf: アクセス制御の例

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
by user read
by * none
```

この規則は、担当の管理者のみが個別のouエントリに書き込みアクセスできることを宣言します。他のすべての認証済みユーザは読み込みアクセスができ、その他のユーザはアクセスできません。

ティップ: アクセス規則の設定

access to規則または一致するbyディレクティブが存在しない場合、アクセスが拒否されます。付与されるのは、明示的に宣言されたアクセス権だけです。規則がまったく宣言されていない場合、デフォルトの原則として、管理者は書き込みアクセスができ、残りのユーザ全員は読み込みアクセスができます。

詳細な説明およびLDAPのアクセス権の設定例については、インストールしたopenldap2パッケージのオンラインマニュアルを参照してください。

アクセス許可を一元的なサーバ設定ファイル(slapd.conf)で管理する方法以外に、ACI (アクセス制御情報)を使用する方法があります。ACIは、個々のオブジェクトのアクセス情報をLDAPツリーに格納します。アクセス制御のタイプには共通のものがなく、開発者の間では未だ実験的だと考えられています。詳細については、http://www.openldap.org/faq/data/cache/758.htmlを参照してください。

45.3.2 slapd.conf内のデータベース固有のディレクティブ

例 45.6 slapd.conf: データベース固有のディレクティブ

```
database bdb
checkpoint      1024    5
cachesize       10000
suffix "dc=suse,dc=de"
rootdn "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

データベースのタイプ、この場合は、Berkeleyデータベースは、このセクションで最初に判別されます(例 45.6. 「slapd.conf: データベース固有のディレクティブ」 (page 725)を参照)。チェックポイントは、実際のデータベースに書き込まれる前にトランザクションログに維持されるデータの量(キロバイト)to2つの処理の間の時間(分)を判別します。キャッシュサイズは、データベースのキャッシに維持されるオブジェクトの数を設定します。接尾辞は、このサーバが取り扱うLDAPツリーの部分を判別します。.次のrootdnは、このサーバに対して、管理者権限を持つユーザを指定します。ここで宣言されるユーザは、LDAPエントリが必要ではなく、通常ユーザとして存在する必要もありません。管理者パスワードは、rootpwで設定します。ここでsecretを使用する代わりに、slappasswdによって作成した管理者パスワードのハッシュを入力することもできます。directoryディレクティブは、サーバ上でデータベースディレクトリが格納されている(ファイルシステム内の)ディレクトリを示します。最後のディレクティブindex objectClass eqは、すべてのオブジェクトクラスのインデックスを管理します。経験的に、ユーザが最も頻繁に検索しそうな属性をここに追加できます。データベースに対してここで定義されたカスタムのAccess規則は、グローバルAccess規則に代わって使用されます。

45.3.3 サーバの起動と停止

LDAPサーバが完全に設定され、項45.4.「LDAPディレクトリのデータ処理」(page 726)で説明するパターンに従ってすべてのエントリが作成されたら、`root`ユーザで「`rcldap start`」を入力し、LDAPサーバを起動します。実行されているかどうかわからない場合は、`rcldap stop`コマンドを実行します。実行しているLDAPサーバのステータスは、`rcldap status`コマンドを実行して要求します。

YaSTランレベルエディタ(項28.2.3.「YaSTでのシステムサービス(ランレベル)の設定」 (page 467)を参照)を使用して、システムのブートまたは停止時に、サーバを自動的に起動および停止することができます。またコマンドプロンプトで`insserv`コマンドを実行して、起動および停止スクリプトそれぞれへのリンクを作成することもできます。詳細については、項28.2.2.「initスクリプト」 (page 462)を参照してください。

45.4 LDAPディレクトリのデータ処理

OpenLDAPは、LDAPのデータを管理するためのツールを提供しています。ここでは、中でも重要な4つのツール、データストックの追加、削除、検索、および変更について説明します。

45.4.1 LDAPディレクトリへのデータの挿入

`/etc/openldap/slapd.conf`でLDAPサーバを正しく設定し、使用する準備ができたら(`suffix`、`directory`、`rootdn`、`rootpw`、および`index`について適切なエントリが表示されることを確認)、レコード入力に進みます。OpenLDAPでは、`ldapadd`コマンドを使用してこのタスクを実行します。可能であれば、実践的な見地から、バンドルされたデータベースにオブジェクトを追加してください。LDAPは、LDIF形式(LDAP data interchange format)を処理してデータを入力します。LDIFは、任意の数の属性と値が指定されたシンプルテキストファイルです。指定できるオブジェクトクラスと属性については、`slapd.conf`で宣言したスキーマファイルを参照してください。図45.1.「LDAPディレクトリの構造」 (page 719)の例のような簡単なフレームワークを作成するには、例 45.7.「LDIFファイルの例」 (page 727)のLDIFを使用します。

例 45.7　LDIFファイルの例

```
# The SUSE Organization dn:dc=suse,dc=de objectClass:dcObject
objectClass:organization o:SUSE AG dc:suse

# The organizational unit development (devel) dn:ou=devel,dc=suse,dc=de
objectClass:organizationalUnit ou:devel

# The organizational unit documentation (doc) dn:ou=doc,dc=suse,dc=de
objectClass:organizationalUnit ou:doc

# The organizational unit internal IT (it) dn:ou=it,dc=suse,dc=de
objectClass:organizationalUnit ou:it
```

重要項目: LDIFファイルのエンコーディング

LDAPでは、UTF-8 (Unicode)を使用します。ウムラウトは正しくエンコードする必要があります。UTF-8をサポートするエディタ(たとえばKateまたは最近のバージョンのEmacs)を使用してください。それ以外のエディタを使用する場合は、ウムラウトや他の特殊文字の使用を避けるか、`recode`を使用してUTF-8をコード変換します。

ファイルには`.ldif`というサフィックスを付けて保存し、次のコマンドでサーバに渡します。

```
ldapadd -x -D <dn of the administrator> -W -f <file>.ldif
```

`-x`は、認証(この例ではSASL)をオフにします。`-D`は、操作を呼び出すユーザを宣言します。`slapd.conf`での設定と同様、管理者の有効なDNをここに入力します。この例では、`cn=admin,dc=suse,dc=de`です。`-W`を指定すると、コマンドライン(クリアテキスト)でのパスワード入力が不要になり、別のパスワードプロンプトがアクティブ化されます。このパスワードは、`slapd.conf`の`rootpw`で事前に指定されています。`-f`はファイル名を渡します。`ldapadd`の実行方法の詳細については、例 45.8. 「example.ldifでのldapaddの使用」 (page 727)を参照してください。

例 45.8　example.ldifでのldapaddの使用

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f example.ldif

Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

個人ごとのユーザデータは、別のLDIFファイルに分けて作成することができます。 例 45.9.「TuxのLDIFデータ」 (page 728)では、Tuxというユーザを新しいLDAPディレクトリに追加します。

例 45.9　TuxのLDIFデータ

```
# coworker Tux dn:cn=Tux Linux,ou=devel,dc=suse,dc=de objectClass:inetOrgPerson
 cn:Tux Linux givenName:Tux sn:Linux mail:tux@suse.de uid:tux telephoneNumber:
 +49 1234 567-8
```

LDIFファイルには、任意の数のオブジェクトを指定できます。サーバのディレクトリブランチ全体を一度に渡すことも、個別のオブジェクトの例で示すように、その一部だけを渡すことも可能です。一部のデータを比較的頻繁に変更する必要がある場合は、1つのオブジェクトごとに細かく分割することをお勧めします。

45.4.2　LDAPディレクトリのデータの変更

データストックの変更用には、ツールldapmodifyが用意されています。最も簡単な方法は、対応するLDIFファイルを変更してから、変更したファイルをLDAPサーバに渡すことです。Tux社員の電話番号を+49 1234 567-8から+49 1234 567-10に変更するには、 例 45.10.「LDIFファイルtux.ldifの変更」 (page 728)のようにLDIFファイルを編集する必要があります。

例 45.10　LDIFファイルtux.ldifの変更

```
# coworker Tux dn:cn=Tux Linux,ou=devel,dc=suse,dc=de changetype:modify
replace:telephoneNumber telephoneNumber: +49 1234 567-10
```

次のコマンドを使用して、変更したファイルをLDAPディレクトリにインポートします。

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

代わりの方法として、変更する属性を直接ldapmodifyに渡すこともできます。この処理手順を次に示します。

1. ldapmodifyを起動し、パスワードを入力します。

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W Enter LDAP password:
   ```

2. 次に示す順序に従って、慎重に変更を入力します。

```
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de changetype: modify
replace: telephoneNumber telephoneNumber: +49 1234 567-10
```

ldapmodifyについての詳細とその構文は、ldapmodify(1)のmanページを参照してください。

45.4.3 LDAPディレクトリでのデータの検索と読み込み

OpenLDAPには、ldapsearchを使用して、LDAPディレクトリでデータを検索して読み込むコマンドラインツールが用意されています。簡単なクエリの構文は次のとおりです。

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

-bオプションは検索ベース、つまり、検索を実行するツリーのセクションを指定します。この例では、dc=suse,dc=deです。セクション内の特定の部分(たとえば、devel部門内のみ)で精度の高い検索を実行するには、-bを使用してこのセクションをldapsearchに渡します。-xは、簡単な認証を起動するよう要求します。(objectClass=*)は、対象のディレクトリにあるすべてのオブジェクトを読むように宣言します。このコマンドオプションは、新しいディレクトリツリーを作成した後に、すべてのエントリが正しく記録され、サーバが意図したとおりに応答することを確認するために使用されます。ldapsearchの使用の詳細については、対応するマニュアルページ(ldapsearch(1))を参照してください。

45.4.4 LDAPディレクトリでのデータの削除

不要なエントリを削除するには、ldapdeleteを使用します。構文は、これまでに説明した他のコマンドとほぼ同じです。たとえば、Tux Linuxに関するエントリをすべて削除するには、次のコマンドを実行します。

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

45.5 YaST LDAPクライアント

YaSTには、LDAPベースのユーザ管理をセットアップするためのモジュールが組み込まれています。インストール時にこの機能を有効にしなかった場合は、［ネットワークサービス］、→［LDAPクライアント］の順に選択してモジュールを起動します。LDAPに必要なPAMおよびNSS関連の変更が自動的に有効になり、必要なファイルがインストールされます。

45.5.1 標準的な処理手順

クライアントマシンのバックグラウンドで動作しているプロセスについての背景となる知識があれば、YaST LDAPクライアントモジュールの働きを理解するうえで助けになります。 ネットワーク認証のためにLDAPがアクティブ化される、またはYaSTモジュールが呼び出されると、パッケージpam_ldapおよびnss_ldapがインストールされ、対応する2つの設定ファイルが調整されます。 pam_ldapは、ログインプロセスと認証データのソースであるLDAPディレクトリとの間のネゴシエートを受け持つPAMモジュールです。 専用モジュールpam_ldap.soがインストールされ、PAM設定が調整されます(例45.11. 「LDAPに合わせて調整されたpam_unix2.conf」 (page 730)を参照)。

例 45.11 LDAPに合わせて調整されたpam_unix2.conf

```
auth: use_ldap account: use_ldap password: use_ldap session: none
```

LDAPを使用するようにサービスを手動で追加設定する場合は、 /etc/pam.d内のサービスに対応するPAM設定ファイルにPAM LDAPモジュールを組み込みます。 /usr/share/doc/packages/pam_ldap/pam.d/には、個々のサービスに合わせて調整済みの設定ファイルが用意されています。適切なファイルを /etc/pam.dにコピーしてください。

nsswitchメカニズムを介したglibcの名前解決は、LDAPと共にnss_ldapを使用するように調整されています。新しく調整されたファイルnsswitch.confが、このパッケージのインストールと共に /etc/に作成されます。 nsswitch.confの機能の詳細については、項38.5.1. 「環境設定ファイル」 (page 644)を参照してください。LDAPを使用してユーザ管理および認証を行うために、nsswitch.confに次の行が存在する必要があります。 例 45.12. 「nsswitch.confの調整」 (page 731)を参照してください。

例 45.12　nsswitch.confの調整

```
passwd: compat group: compat

passwd_compat: ldap group_compat: ldap
```

この行は、glibcのリゾルバライブラリに対して、最初に/etc内で対応するファイルを評価し、次に認証およびユーザデータのソースとしてLDAPサーバにアクセスするように指示しています。このメカニズムをテストするために、たとえばgetent passwdコマンドを使用してユーザデータベースの内容を読み込みます。返されたセットには、システムのローカルユーザに関する情報と、LDAPサーバに格納されている全ユーザに関する情報が含まれているはずです。

LDAPで管理される通常のユーザがsshまたはloginを使用してサーバにログインするのを防止するには、ファイル/etc/passwdおよび/etc/groupにそれぞれ1行を追加する必要があります。 ★翻訳不要★この行は、/etc/passwdの場合は+::::::/sbin/nologin、/etc/groupの場合は+:::です。

45.5.2　LDAPクライアントの設定

最初にnss_ldapを調整すれば、pam_ldap、/etc/passwd、/etc/groupの設定はYaSTによって行われるので、単にクライアントをサーバに接続すれば、YaSTにLDAPいよるユーザ管理を行わせることができます。この基本的なセットアップは基本的な設定項 (page 731)で説明されています。

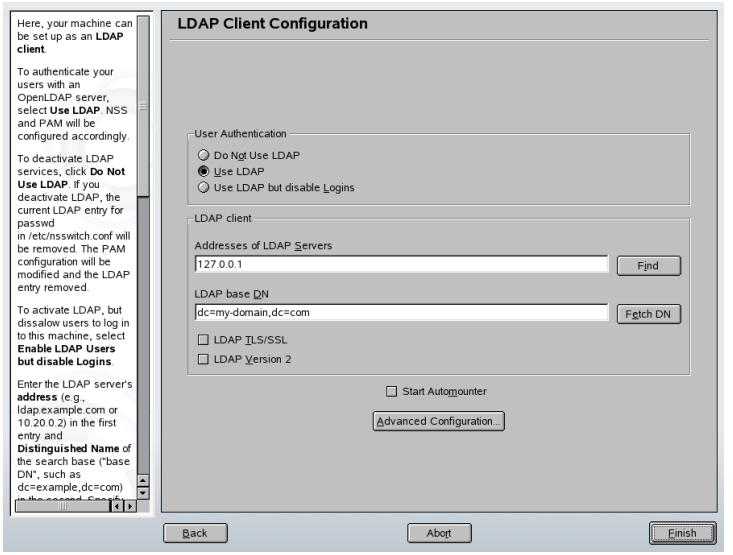
YaSTのグループおよびユーザ設定モジュールをさらに設定するには、YaST LDAPクライアントを使います。これには、新規ユーザおよびグループのデフォルト設定、そしてユーザまたはグループに割り当てられる属性の数と性質を操作することが含まれます。LDAPのユーザ管理を使えば、従来のユーザまたはグループ管理ソリューションより、ユーザやグループにずっと多くの異なった属性を割り当てることができます。これはYaSTのグループおよびユーザ管理のモジュールを設定する項 (page 735)で説明されています。

基本的な設定

インストール時にLDAPユーザ管理を選択するか、インストール後のシステムのYaST Control Centerで［ネットワークサービス］、→［LDAPクライアン

ト］の順に選択すると、基本的なLDAPクライアント設定ダイアログ(図 45.2. 「YaST:LDAPクライアントの設定」 (page 732))が表示されます。

図 45.2　YaST:LDAPクライアントの設定



マシンのユーザをOpenLDAPサーバに対して認証し、OpenLDAPによるゆーざかんりをゆうこうにするには、以下の手順に従います。

1. ［*Use LDAP*］をクリックして、LDAPの使用を有効にします。認証のためにLDAPを使うものの、他のユーザがこのクライアントにログインしないようにする場合には、［*Use LDAP but Disable Logins*］を選択します。

2. 使用するLDAPサーバのIPアドレスを入力します。

3. ［*LDAP base DN*］に入力して、LDAPサーバ上の検索ベースを選択します。

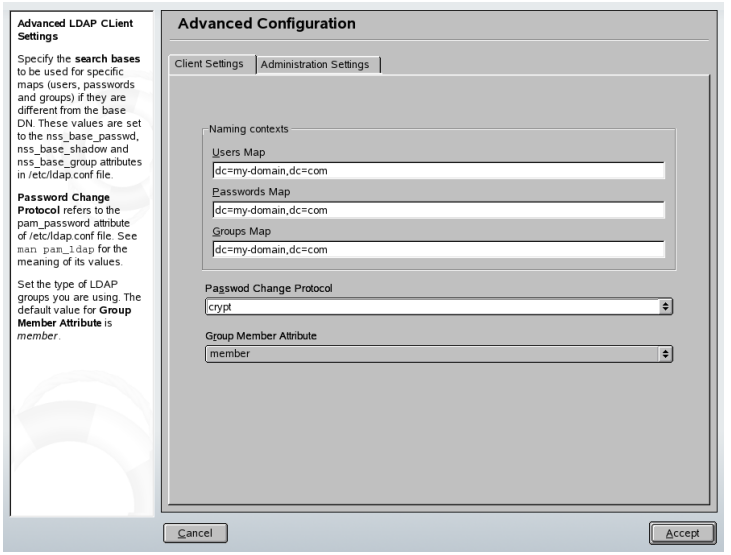
4. サーバとの間でTLSまたはSSLによって保護された通信が必要な場合には［*LDAP TLS/SSL*］を選択します。

5 LDAPサーバがまたLDAPv2を使用している場合には、［*LDAP Version 2*］を選択して、このプロトコルのバージョンの使用を明示的に有効にします。

6 リモートに管理された /homeなど、クライアントにリモートディレクトリをマウントする場合には、［*Start Automounter*］をオンにします。

7 ［*Finish*］をクリックして、設定を適用します。

図 45.3 YaST:詳細な設定



サーバ上のデータを管理者として修正するには、［*詳細な設定*］をクリックします。次のダイアログは2つのタブに分かれています。図 45.3. 「YaST:詳細な設定」 (page 733)を参照してください。

1 ［*Client Settings*］タブで、必要に合わせて以下の設定を調整します。

a ユーザ、パスワード、グループの検索ベースが［*LDAP base DN*］で指定したグローバルな検索ベースとは異なる場合には、［*User Map*］、［*Password Map*］、および［*Group Map*］でそれらの異なる名前付けコンテキストを入力します。

b パスワード変更プロトコルを指定します。パスワードが変更されたときに使用する標準的な方法は`crypt`で、`crypt`によって生成されたパスワードハッシュが使用されることを意味しています。この点や他のオプションの詳細については、`pam_ldap` manページを参照してください。

c ［*Group Member Attribute*］で、使用するLDAPグループを指定します。このデフォルトの値は`member`です。

2 ［*Administration Settings*］で、以下の設定を調整します。

a ［*Configuration Base DN*］で、ユーザ管理データを保管するベースを設定します。

b ［*Administrator DN*］に適切な値を入力します。この特定のユーザがLDAPサーバに保管されたデータを操作できるようにするためには、このDNは、`/etc/openldap/slapd.conf`で指定された`rootdn`値と同一である必要があります。

c サーバ上に基本設定オブジェクトを作成して、LDAPによるユーザ管理を有効にするには、［*Create Default Configuration Objects*］をオンにします。

d お使いのクライアントマシンを、ネットワーク上のホームディレクトリ用のファイルサーバとして動作させ場合には、［*Home Directories on This Machine*］をオンにします。

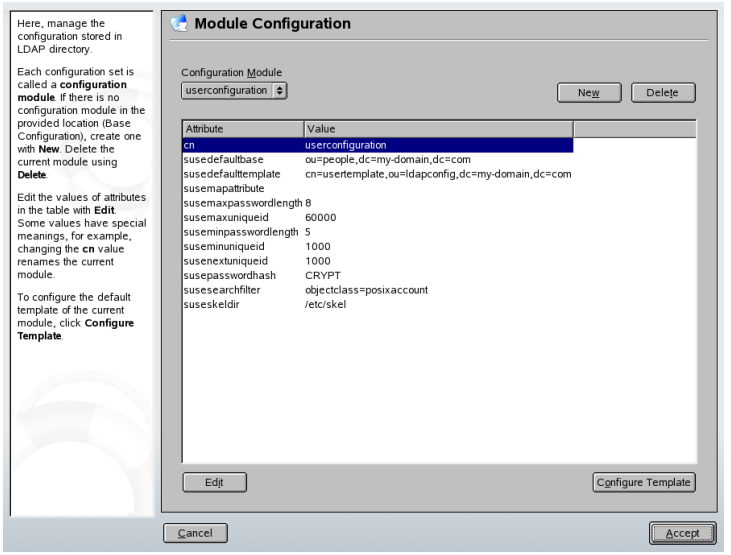
e ［*Accept*］をクリックして［*Advanced Configuration*］を終え、［*Finish*］をクリックして設定を適用します。

［*ユーザ管理の設定*］をクリックし、LDAPサーバ上のエントリを編集します。これにより、サーバに格納されているACLとACIに従って、サーバ上の設定モジュールへのアクセス権が付与されます。YaSTのグループおよびユーザ管理のモジュールを設定する項 (page 735)で概略が説明されている手順に従います。

YaSTのグループおよびユーザ管理のモジュールを設定する

YaSTのLDAPクライアントを使用して、YaSTモジュールをユーザとグループの管理用に調整し、それを必要に応じて拡張します。データの登録を単純化するために、個々の属性のデフォルトの値のテンプレートを定義します。ここで作成した事前設定は、LDAPディレクトリにLDAPオブジェクトとして格納されます。ユーザデータの登録には、通常のYaSTのユーザおよびグループ管理用モジュールが使用されます。登録されたデータはサーバ上にLDAPオブジェクトとして保管されます。

図 45.4　YaST: モジュールの設定



モジュール設定ダイアログ(図 45.4. 「YaST:モジュールの設定」 (page 735))を使用すると、新規モジュールの作成、既存の設定モジュールの選択と変更、およびそれらのモジュールのテンプレートの設計と変更ができます。

新しい設定モジュールを作成するには、以下の手順に従います。

1 ［*New*］をクリックして、作成するモジュールのタイプを選択します。ユーザ設定モジュールの場合には`suseuserconfiguration`を選択し、グループ設定の場合は`susegroupconfiguration`を選択します。

2 新しいテンプレートの名前を選択します。

これにより、コンテンツビューに、このモジュールで許可されている全属性と、それぞれに割り当てられている値がテーブル形式のリストとして表示されます。このリストには、設定されているすべての属性に加えて、現行スキーマで許可されているが現在は使用されていない他の属性もすべて含まれています。

3 プリセットされている値を受け入れるか、それぞれの属性を選択して［*Edit*］を押し、新しい値を入力して、グループおよびユーザ構成で使用するデフォルトを調整します。モジュールの名前を変更するには、モジュールのcn属性を変更します。現在選択しているモジュールを削除するには［*削除*］をクリックします。

4 ［*OK*］をクリックすると、選択メニューに新しいモジュールが追加されます。

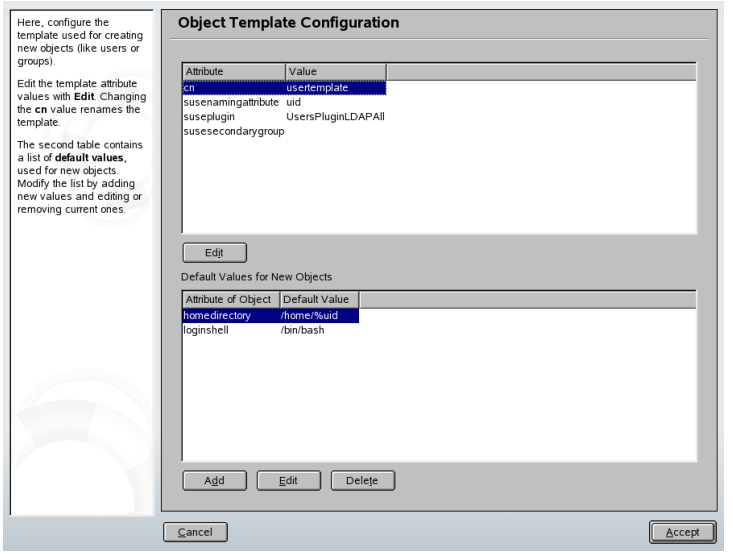
YaSTのグループおよびユーザ管理用モジュールには、重要な標準値が設定されたテンプレートが埋め込まれています。設定モジュールに関連したテンプレートを編集するには、以下の手順に従います。

1 ［*Module Configuration*］ダイアログで、［*Configure Template*］をクリックします。

2 必要に応じて、このテンプレートに割り当てられている一般的な属性の値を決めます。空にしておくこともできます。空の属性は、LDAPサーバ上で削除されます。

3 新しいオブジェクト(LDAPツリー内のユーザまたはグループ設定オブジェクト)のデフォルトの値を修正、削除、または追加します

図 45.5　YaST:: オブジェクトテンプレートの設定



モジュールのsusedefaulttemplate属性値を調整済みテンプレートのDNに設定し、テンプレートを対応するモジュールに接続します。

ティップ

絶対値の代わりに変数スタイルを使用すると、属性のデフォルト値を他の属性から作成できます。たとえば、新規ユーザの作成時には、snとgivenNameの属性値からcn=%sn %givenNameが自動的に作成されます。

すべてのモジュールとテンプレートを適切に設定し、実行する準備が完了したら、新しいグループとユーザを通常の方法でに登録できます。

45.6　YaSTでのLDAPユーザおよびグループの設定

ユーザおよびグループデータの実際の登録手順は、LDAPを使用しない場合とほぼ同様です。次に、ユーザ管理に関連する手順の概略を示します。グループの管理手順も同様です。

1 ［セキュリティとユーザ］、 → ［ユーザを作成あるいは編集する］の順に選択し、YaSTのユーザ管理にアクセスします。

2 ［*Set Filter*］を使って、ユーザの表示をLDAPユーザに制限し、Root DNのパスワードを入力します。

3 ［*Add*］をクリックして、新しいユーザの設定を入力します。4つのタブのある［描画色を変更］ダイアログが開きます。

   a ［*User Data*］タブでユーザ名、ログイン名、およびパスワードを指定します。

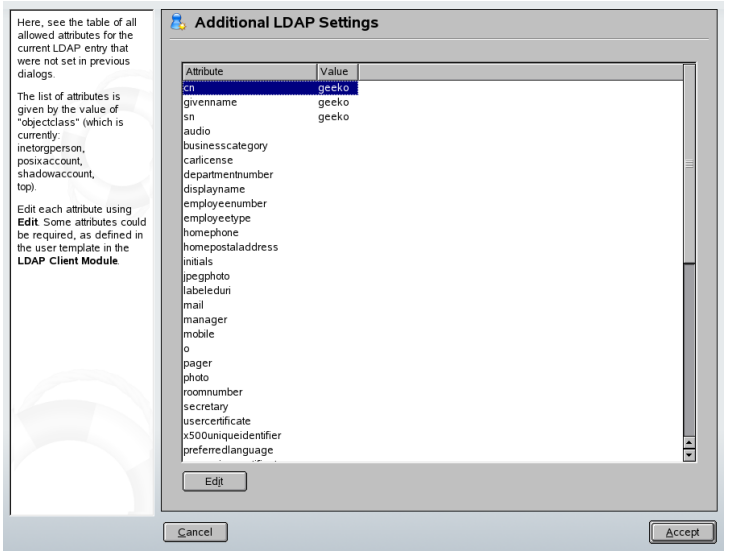
   b ［*Details*］タブをクリックして、新しいユーザの所属するグループ、ログインシェル、およびホームディレクトリを設定します。必要であれば、デフォルトの値を、必要に適した値に変更します。デフォルトの値、およびパスワードの設定は、YaSTのグループおよびユーザ管理のモジュールを設定する項 (page 735)で説明されている手順で設定できます。

   c デフォルトの［*Password Settings*］の設定を修正するか、受け入れます。

   d ［*Plug-Ins*］タブで、LDAPプラグインを選択し、［*Launch*］をクリックして、新規ユーザに割り当てる付加的なLDAP属性を設定します(図 45.6. 「YaST:LDAPの追加設定」 (page 739)を参照)。

4 ［*Accept*］をクリックして設定を適用し、ユーザ設定を終了します。

図 45.6　YaST:LDAPの追加設定



ユーザ管理の初期入力フォームには、［*LDAPオプション*］が用意されています。ここでは、使用可能なユーザのセットにLDAP検索フィルタを適用するか、［*LDAP User and Group Configuration(LDAPユーザとグループの設定)*］を選択してLDAPユーザおよびグループの設定モジュールにアクセスできます。

45.7　関連資料

SASL設定や、複数のスレーブ間で作業不可を分散するためのLDAPサーバのレプリケートの設定などの複雑なトピックについては、ここではあえて触れませんでした。この2つの項目の詳細については、『*OpenLDAP 2.2 Administrator's Guide*』(下記参照)を参照してください。

OpenLDAPプロジェクトのWebサイトには、LDAPの初心者向けや熟練者向けのあらゆるマニュアルが用意されています。

『OpenLDAP Faq-O-Matic』
OpenLDAPのインストール、設定、および運用に関する豊富なQAが集められています。 Find it at `http://www.openldap.org/faq/data/cache/1.html`.

『Quick Start Guide』
LDAPサーバのインストール方法を手順を追って簡単に説明しています。http://www.openldap.org/doc/admin22/quickstart.html、またはインストール済みのシステムで/usr/share/doc/packages/openldap2/admin-guide/quickstart.htmlを参照してください。

『OpenLDAP 2.2 Administrator's Guide』
アクセス制御や暗号化など、LDAP設定の重要な側面を詳細に説明しています。http://www.openldap.org/doc/admin22/、またはインストール済みのシステムで/usr/share/doc/packages/openldap2/admin-guide/quickstart.htmlを参照してください。

『Understanding LDAP』
LDAPの基本原則一般について、詳細に説明しています。http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf.

LDAPに関する書籍

- *LDAP System Administration* by Gerald Carter (ISBN 1-56592-491-6)
- *Understanding and Deploying LDAP Directory Services* by Howes, Smith, and Good (ISBN 0-672-32316-8)

LDAPに関する究極的な参考資料は、RFC 2251～2256です。

46 Apache Webサーバ

http://www.netcraft.comによれば、Apacheは60%以上のシェアを誇る、世界で最も広く使われているWebサーバです。Webアプリケーションをサポートするために、Apacheは多くの場合、Linux、データベースMySQL、およびプログラミング言語のPHPやPerlと組み合わせて使用されます。この組み合わせは、一般にLAMPと呼ばれます。

この章では、WebおよびアプリケーションサーバソフトウェアのApacheバージョン2.xを紹介します。Apacheのインストールと設定、そして利用可能なモジュールのいくつかについて説明します。

46.1 前置きと用語

このセクションでは、Web関連のものとApacheに固有なものの両方について、よく使われる用語を説明します。

重要項目: 用語

このドキュメントでは、*Apache*はApacheバージョン2.xを指しています。Apache 1.xのドキュメントは、ApacheのWebサイトを参照してください。

46.1.1 Webサーバ

Webサーバは、クライアントが要求するHTMLページを発行します。クライアントは、KonquerorのようなWebブラウザの場合もありますし、World Wide

Webに接続された他のデバイスの場合もあります。これらのページは、その全体がディスク上に保管されている場合もありますし(静的なページ)、データベースやWebサービスのような、外部のエンティティのクエリに対する応答として生成される場合もあります(動的なページ)。

46.1.2 HTTP

クライアントとWebサーバ間の通信は、ハイパーテキスト転送プロトコル(HTTP)によって行われます。現行バージョンのHTTP 1.1は、RFC 2068および更新版のRFC 2616に文書化されています。これらのRFCについては、`http://www.w3.org`を参照してください。

46.1.3 URL

URLはuniversal resource locatorの略です。クライアントは、`http://www.example.com/index.html`などのURLを使用して、サーバにページを要求します。URLは、次の各部で構成されています。

プロトコル
次のプロトコルがよく使用されます。

http://
HTTPプロトコル

https://

HTTPに暗号化機能を付加したセキュアプロトコル

ftp://

ファイルのアップロードとダウンロードに使用するファイル転送プロトコル

ドメイン

この例では、ドメインは`www.example.com`です。ドメインはIPアドレスに対応する名前です。それで、`www.example.com`は、123.456.789.1のようなIPアドレスに一意にマップされます。次に、この番号はWebサーバを

実行しているコンピュータを一意に識別します。ドメイン名からIPアドレスへのマッピングは、一般に*名前解決*と呼ばれます。ドメインはいくつかの部分に分かれます。ここではwww、example、およびcomです。ドメイン名の最後の部分はトップレベルドメイン(TLD)と呼ばれます。この例では、comがTLDです。TLDは名前解決プロセスの最上位のレベルを現します。TLDは、汎用のものである場合と(com、org、およびnetなどのgTLD)、国固有のものである場合があります(ドイツを表すdeなど)。ドメインのすべての部分が集まったものを、完全修飾ドメイン名(FQDN)と呼びます。

リソース
: この例では、リソースはindex.htmlです。この部分は、リソースへのフルパスを示します。リソースには、この例のようにファイルを指定できます。CGIスクリプト、JavaServer Page、その他のリソースも指定できます。

このためのインターネットメカニズム(たとえば、ドメインネームシステム、DNS)は、ドメインwww.example.comへのクエリを、リソースを保持する1つ以上のコンピュータに転送します。ここでApacheは、実際のリソース(この例ではページindex.html)をクライアントに配信します。この例ではファイルがトップレベルディレクトリにありますが、http://www.example.com/linux/novell/suseのようにリソースがサブディレクトリにあることもあります。.

46.1.4 ディレクティブ

Apacheを設定する際には、*directive*という用語が、「設定オプション」と同じ意味でよく使われます。ディレクティブは、Apache Webサーバソフトウェアに関連した専門用語です。

46.2 インストール

SUSE LinuxのApacheは、標準の、定義済みの設定で、「そのまま」実行できます。この章の手順に従えば、短い時間でApache Webサーバを設定して、実行することができます。Apacheをインストールして設定するには、rootになる必要があります。

46.2.1 ApacheをYaSTでインストールする

SUSE Linuxのapache2パッケージは、 Apache Web site (http://httpd.apache.org)から入手できる標準のソフトウェアパッケージとは、ファイルシステムやアプリケーションのレイアウトが少し異なっています。 このセクションでは、SUSE Linuxのapache2パッケージのインストール方法の詳細と、存在する相違点について説明します。

簡単なWebサーバをインストールするには、次の手順に従います。

手順 46.1　クイックインストール

1. YaSTをGUIまたはコマンドラインモードで起動します。
2. *[ネットワークサービス]* → *[HTTPサーバ]*の順に選択します。
3. ［*Continue*］をクリックして、apache2およびapache2-preforkパッケージのインストールを確認します。
4. インストールが完了すると、［*Apache Configuration Wizard*］が表示されるので、Webサーバの設定を開始できます。

上記の手順の欠点は、PHPやデータベースのサポートが無いことです。 PHPやデータベースのサポートのある状態でWebサーバをインストールするには、次の手順に従います。

手順 46.2　簡単なWebサーバのインストール

1. YaSTをGUIまたはコマンドラインモードで起動します。
2. *[ソフトウェア]* → *[ソフトウェアのインストール/削除]*の順に選択します。
3. ［*Filter*］で［*Selections*］を選択し、［*Apache2を使用する単純なWWWサーバー*］をオンにします。
4. ［*Accept*］をクリックします。
5. 依存関係のあるパッケージのインストールを確認して、SUSE LinuxのApache2のインストールプロセスを完了します。

上級のユーザは、SUSE Linuxでカスタムのパッケージ選択を行うこともできます。Webサーバのカスタムインストールを行うには、次の手順に従います。

手順 46.3　デフォルトのApache RPMをYaSTでインストールする

1. YaSTをGUIまたはコマンドラインモードで起動します。*[ソフトウェア]* → *[ソフトウェアのインストール/削除]*の順に選択します。
2. ［*Filter*］で［*Search*］を選択し、［*Search*］フィールドに`apache2`と入力します。
3. `apache2`をインストールするように選択します。
4. モジュール選択の場合のステップ2と3を実行します。項46.5.「Apacheのモジュール」 (page 772)を参照してください。
5. 選択したら、［*Accept*］をクリックします。
6. 次に、必須のパッケージ`apache2-MPM`と依存関係にある`apache2-prefork`または`apache2-worker`のどちらかを選択するように促されます。これら2つの相違点についての説明は、項46.2.2.「マルチプロセシングモジュール」 (page 745)を参照してください。よく分からない場合には、`apache2-prefork`パッケージを選択してください。これがUnixベースのオペレーティングシステムでのデフォルトになっています。［*OK*］をクリックします。
7. 依存関係のあるパッケージのインストールを確認して、SUSE Linuxの Apache2のインストールプロセスを完了します。

注意: Webサーバの起動

Apacheをインストールしても、Webサーバが自動的に起動するわけではありません。Apacheの起動とシャットダウンを制御する方法は、項46.3.3.「Apacheの有効化、起動、および停止」 (page 765)を参照してください。

46.2.2　マルチプロセシングモジュール

デフォルトのApache RPMをYaSTでインストールする (page 745)で説明しているように、SUSE Linuxには、Apacheで使用するための2つのマルチプロセシン

グモジュール(MPM)が用意されています。MPMは、Webサーバへのリクエストを受け取って処理する役割を果たすもので、Webサーバソフトウェアの中核となっています。

プリフォークMPM

プリフォークMPMは、スレッド対応でない、プリフォークWebサーバを実装します。Webサーバは、それぞれのリクエストを分離し、個別の子プロセスを分岐することによって処理する、Apacheバージョン1.xと同様の動作を行います。これにより、問題のあるリクエストが他のものに影響することがなくなるので、Webサーバのロックアップを避けられます。

プロセスベースのアプローチによって安定性がもたらされますが、プリフォークMPMは、もう一方のワーカーMPMよりも多くのシステムリソースを消費します。プリフォークMPMは、Unixベースのオペレーティングシステムでのデフォルトの MPMとみなされています。

重要項目: このドキュメントでのMPM

このドキュメントでは、Apacheがプリフォーク MPMで使用されていることを仮定しています。

ワーカーMPM

ワーカーMPMは、マルチスレッド対応のWebサーバを提供します。スレッドとは、「軽い」形態のプロセスです。プロセスよりもスレッドが優れている点は、リソースの消費が少ないことです。ワーカーMPMは、子プロセスを分岐する代わりに、サーバプロセスでスレッドを使用することによってリクエストを処理します。プリフォークした子プロセスは複数のスレッドになります。

このアプローチでは、プリフォークMPMの場合よりもシステムリソースの消費が少なくなるので、Apacheの性能が良くなります。主要な短所の1つは、ワーカーMPMの安定性に関するものです。1つのスレッドが壊れると、プロセスのすべてのスレッドが影響を受けます。最悪の場合には、サーバがクラッシュすることがあります。特に、ApacheでCGIを使用している場合(CGI (Common Gateway Interface)`mod_cgi` 項 (page 774)を参照)、負荷が大きくなると、スレッドがシステムリソースと通信できなくなって、内部サーバエラーが生じることがあります。

ワーカーMPMを使用すべきでないという意見の別の根拠は、利用できるApacheのモジュール(項46.5. 「Apacheのモジュール」 (page 772)を参照)のすべてがスレッドセーフになっているわけではなく、そのためワーカーMPMと組み合わせて使用することはできないという点です。

警告: ApacheモジュールとしてのPHP (mod_php)

利用可能なPHPモジュールのすべてがスレッドセーフになっているわけではありません。ワーカーMPMと`mod_php`を組み合わせることは、絶対に避けてください。

46.2.3 デフォルトのファイルシステムとアプリケーションのレイアウト

SUSE Linuxは、Apacheパッケージのファイルをデフォルトの場所に配置します。最も重要なファイルの場所は、以下のとおりです。

バイナリ

SUSE LinuxのApacheでは、ほとんどの実行ファイルの名前に2が付けられています。これにより、Apache 1.xとApache 2.xを同時にインストールした場合でも、バイナリファイルが区別しやすくなっています。

`/usr/sbin/httpd2`
項46.2.2. 「マルチプロセシングモジュール」 (page 745)で説明した、選択したマルチプロセシングモジュールを指すシンボリックリンクです。デフォルトは`httpd2-prefork`です。このシンボリックリンクは、MPMのシステム設定に従って、起動スクリプトによって維持されています。

`/usr/sbin/httpd2-prefork`
Apache2の実際の実行可能ファイルです。

`/usr/sbin/apache2ctl`
Apache HTTPDプロジェクトによって用意された、Webサーバの起動と停止を行う制御スクリプトです。`/usr/sbin/apache2ctl help`についての詳細、および実行方法は、項46.3.3. 「Apacheの有効化、起動、および停止」 (page 765)を参照してください。

/etc/init.d/apache2

SUSE Linuxのインストールに完全に統合されており、Apacheをブート時に起動する、起動および停止スクリプトです。サーバの起動や停止の前に設定が有効かどうかをチェックします。また、設定の場所を上書きします。他の設定ファイルを含めることや、モジュールをロードすることが容易で、スクリプトを変更しなくても、サーバの個別のインスタンスを起動することができます。

/usr/sbin/rcapache2

`/etc/init.d/apache2`へのシンボリックリンクです。`/etc/init.d/`はデフォルトではパスには含まれていないからです。Apacheを起動するには、`rcapache2 start`と入力します。

/usr/sbin/htpasswd2

`.htaccess`ベースの認証を行うための、暗号化パスワードを生成するユーティリティです。ツールの使用方法についての詳細は、`htpasswd2(1)` manページを参照してください。

設定ファイル

ほとんどの設定ファイルは、`/etc/apache2`の下に置かれます。設定を変更する方法についての詳細は、項46.3.「環境設定」 (page 751)を参照してください。

/etc/apache2/httpd.conf

トップレベルの設定ファイルです。可能であれば、このファイルを変更することは避けてください。このファイルでは、主に他の設定ファイルをインクルードし、グローバル設定を宣言しています。

/etc/apache2/*.conf

外部Apacheモジュールの中には、設定ファイルを`/etc/apache2/`ディレクトリに置くものがあります。通常、名前にはモジュール名が含まれています(`mod_*.conf`)。

/etc/apache2/conf.d/*

特定のパッケージに付属する、他の様々な設定ファイルを保持するディレクトリです。実例は、PHPを使用する: `mod_php4`、`mod_php5`項 (page 780)を参照してください。

/etc/apache2/vhosts.d/*
仮想ホスト用のオプションの設定ファイルを保持するディレクトリです。詳細については、項46.4. 「仮想ホスト」 (page 767)を参照してください。

/etc/sysconfig/apache2
Apache2に関連する、SUSE Linuxの設定ファイルです。Apache Webサーバを制御するための、関連するすべての設定パラメータを保持しています。 `/etc/sysconfig/apache2`は、項46.3.1. 「ApacheをYaSTで設定する」 (page 751)で説明されている方法で、YaSTでApacheを設定するために用いられます。項46.3.2. 「Apacheを手動で設定する」 (page 758)で説明されている方法で、手動で編集することもできます。

ログファイル

デフォルトでは、Apacheはその実行時のステータスについての様々な情報を、以下のファイルに記録します。

/var/log/apache2/error_log
Apacheは、起動およびシャットダウン時の注意事項と、実行時のすべてのエラーを、このファイルに記録します。

/var/log/apache2/access_log
Webサーバへのすべてのリクエストが、このファイルに記録されます。エントリのデフォルトのフォーマットは組み合わせフォーマットで、リクエストを送ったホストとユーザエージェントについての情報、および参照側のURIが記録されます。

ドキュメントルート

物理ディレクトリ `/srv/www/htdocs`は、ApacheがWebページを取得するデフォルトの場所です。これは、クライアントのリクエストに対する「ルートディレクトリ」としての役割を果たします。ApacheでWebページを公開するには、ファイルをこのディレクトリの中または下に、階層構造を構成する仕方で保管してください。

http://www.example.com/index.htmlというURLは、example.comというドメイン名のSUSE Linuxでのデフォルトの Apache設定では、 `/srv/www/htdocs/index.html`を参照します。

46.2.4　モジュールを手動でビルドする

Apacheは、モジュール方式で構築されています。つまり、モジュールがWebサーバソフトウェア本体の機能を提供しています。そのため、上級のユーザは、カスタムのモジュールを書いてApacheを拡張することができます。詳細については、以下で言及するmanページを参照してください。

apache2-devel

Apacheモジュールの開発やサードパーティ製モジュールのコンパイルを行う場合は、パッケージapache2-develを対応する開発ツールとともにインストールします。 apache2-develには、apxs2ツールも含まれています。これは、Apache用の追加モジュールをコンパイルする場合に必要です。

apxs2

apxs2バイナリは、 /usr/sbinの下層にあります

- /usr/sbin/apxs2—MPMと共に動作する拡張モジュールを構築するのに適しています。インストール場所は/usr/lib/apache2です。
- /usr/sbin/apxs2-prefork—プリフォークMPMモジュールに適しています。インストール場所は/usr/lib/apache2-preforkです。
- /usr/sbin/apxs2-worker—ワーカーMPMモジュールに適しています。

apxs2は、どのMPMに対しても使用できるようにモジュールをインストールします。他の2つのプログラムは、それぞれのMPMのみが使用できるように、モジュールをインストールします。 apxs2はモジュールを/usr/lib/apache2にインストールし、apxs2-preforkは/usr/lib/apache2-preforkにインストールします。

apxs2は、ソースコードからモジュールをコンパイルし、インストールすることを可能にします(設定ファイルへの必要な変更も含みます)。 これは、実行時にApacheにロードされる、*ダイナミック共有オブジェクト* (DSO)を作成します。ソースコードからモジュールをインストールするには、コマンドcd /path/to/module/source; apxs2 -c -i *mod_foo*.cを使います。apxs2のその他のオプションについては、apxs2(1)manページを参照してく

ださい。その後、項46.3.2. 「Apacheを手動で設定する」 (page 758)の手順に従って、 `/etc/sysconfig/apache2`内のエントリ`APACHE_MODULES`を使用してモジュールを有効にします。

46.3 環境設定

SUSE LinuxのApacheは、YaSTと手動という、2通りの方法で設定できます。手動で設定を行えば細かい点まで調整できますが、YaSTのGUIほど便利ではありません。

重要項目: 設定の変更

Apacheの特定の設定を変更した場合、Apacheを再起動しないと変更が有効になりません。これは、YaSTで設定を完了し、［*HTTP Service*］の［*Enabled*］をオンにすると、自動的に行われます。手動での再起動については、項46.3.3. 「Apacheの有効化、起動、および停止」 (page 765)を参照してください。ほとんどの設定の変更は、`rcapache2 reload`を実行して再ロードすれば有効になります。

46.3.1 ApacheをYaSTで設定する

YaSTを使えば、ネットワーク内のホストをWebサーバにすることができます。そのようなサーバを設定するには、YaSTを起動して、*[ネットワークサービス] → [HTTPサーバ]*の順に選択します。 このモジュールを初めて起動すると、HTTP Server Wizardが起動して、サーバ管理に関して少数の基本的な事項を決定するように要求されます。

HTTP Server Wizard

HTTP Server Wizardには、5つのステップ、つまりダイアログがあります。 ダイアログの最後のステップでは、上級者用の設定モードに入って、さらに詳細な設定を行うかどうか選択できます。

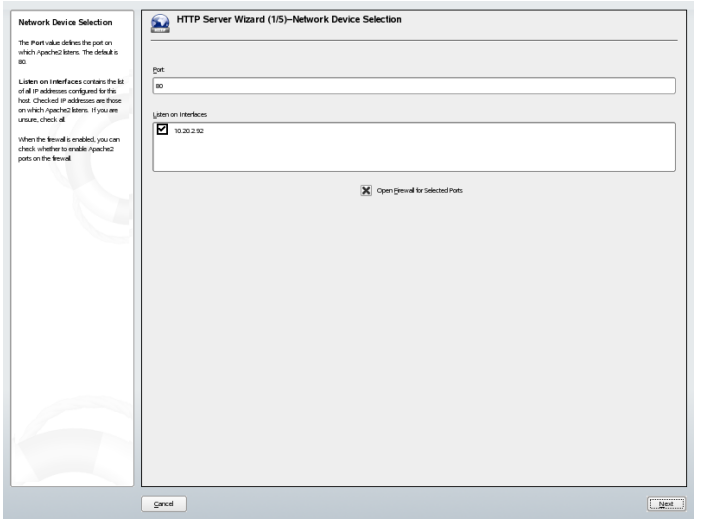
Network Device Selection (ネットワークデバイスの選択)
ここでは、Apacheが着信リクエストをリスンするために使用する、ネットワークインタフェースとポートを指定します。既存のネットワークインタ

フェースとそれらに対応するIPアドレスから、任意のものを組み合わせて選択できます。 他のサービスによって予約されていないものであれば、3つの範囲(ウェルノウンポート、レジスタードポート、ダイナミックまたはプライベートポート)のうちのどのポートでも使用できます。

デフォルトの設定では、すべてのネットワークインタフェース(IPアドレス)のポート80をリスンします。 ファイアウォールが有効になっている場合には、チェックボックスによって、ファイアウォールでApacheのポートを開くかどうかを設定できます。

ファイアウォールで、Webサーバがリスンするポートを開くには、［*Open Firewall for Selected Ports*］をオンにします。 これは、LAN、WAN、または公共のインターネットなど、ネットワーク上でWebサーバを利用可能にする場合には必須です。 外部からWebサーバにアクセスすることが不必要なテスト段階では、リスンするポートを閉じたままにしておくとよいでしょう。 デフォルトの設定を使用する、または必要な変更を加えたなら、［*Next*］をクリックして設定を続けます。

図 46.1 *HTTP Server Wizard: Network Device Selection (ネットワークデバイスの選択)*

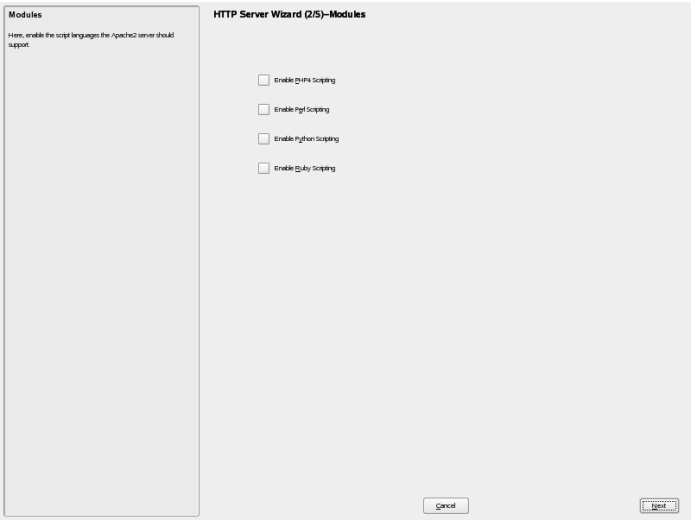


モジュール

SUSE LinuxのApacheパッケージには、さまざまなApacheモジュールが付属しています。 モジュールはApacheの機能を拡張します。いろいろなタスク

を行うものが利用可能です。［*Modules*］設定オプションでは、サーバの起動時に各Apacheモジュールをロードするかどうかを設定できます。モジュールについての詳細は、項46.5.「Apacheのモジュール」 (page 772)を参照してください。［*Next*］をクリックします。

図 46.2　HTTP Server Wizard:モジュール

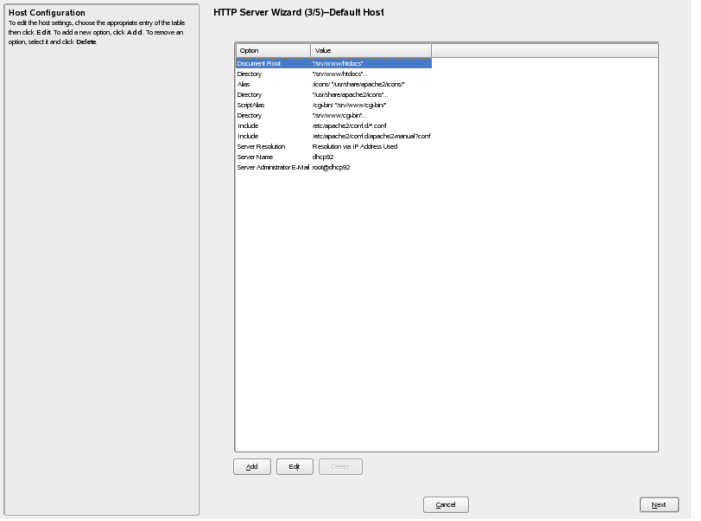


Default Host (デフォルトのホスト)

このオプションは、デフォルトのWebサーバに関連しています。項46.4.「仮想ホスト」 (page 767)で説明しているように、Apacheでは、単一の物理マシンで複数のドメインのサービスを行えます。設定ファイルで最初に宣言されたドメイン(つまり`VirtualHost`)は通常、デフォルトのホストと呼ばれます。ホストの設定を編集するには、テーブル内の適切なエントリを選択して、［*Edit*］をクリックします。新しいホストを追加するには、［*Add*］をクリックします。ホストを削除するには、そのアカウントを選択し、［*Delete*］をクリックします。

このステップでは、ホストの設定にSSL (secure sockets layer)オプションと値を追加するかどうかを決めることができます。この点についての詳細は、SSLサポートの追加項 (page 758)を参照してください。

図 46.3 *HTTP Server Wizard: Default Host (デフォルトのホスト)*



これはサーバのデフォルト設定のリストです。

ドキュメントルート

ドキュメントルート項(page 749)で説明しているように、`/srv/www/htdocs`は、ApacheがWebページを取得するデフォルトの場所です。

Directory

`/srv/www/htdocs`は、Webページのある場所です。

Alias

`Alias`ディレクティブを使えば、URLを物理的なファイルシステムの場所にマップすることができます。このことは、パスのURLエイリアスを行えば、ファイルシステムのドキュメントルートの外にあるパスであってもアクセスできることを意味しています。

デフォルトのSUSE Linuxでは、`Alias /icons`が`/usr/share/apache2/icons`を指しています。ここには、ディレクトリのインデックス表示で使用されるApacheのアイコンがあります。

Directory

`/usr/share/apache2/icons`は`Alias`ディレクトリのある場所です。

Script Alias
`Alias`ディレクティブと同様に、`ScriptAlias`ディレクティブはURLをシステム内の場所にマップします。 相違点は、`ScriptAlias`はターゲットディレクトリをCGIの場所として指定するということです。つまり、その場所にあるCGIスクリプトが実行されます。

Directory
`/srv/www/cgi-bin`は`ScriptAlias`ディレクトリのある場所です。

Include
`/etc/apache2/conf.d/*.conf`は、特定のパッケージに付属する設定ファイルを含むディレクトリです。 `/etc/apache2/conf.d/apache2-manual?conf`は、すべての`apache2-manual`設定ファイルを含むディレクトリです。

Server Resolution
このオプションは、項46.4.「仮想ホスト」 (page 767)を参照してください。

［*Determine Request Server by HTTP Headers*］を選択すると、`VirtualHost`は、そのサーバ名に対する要求に応答します(項46.4.1.「名前ベースの仮想ホスト」 (page 767)を参照)。

［*Determine Request Server by Server IP Address*］を選択すると、Apacheは、クライアントが送信したHTTPヘッダ情報によって、要求に応答するホストを選択します。 IPベースの仮想ホストについての詳細は、項46.4.2.「IPベースの仮想ホスト」 (page 770)を参照してください。

Server Name
クライアントがWebサーバとコンタクトするために使うデフォルトのURLを指定します。 `http://`*FQDN*にあるWebサーバに接続するには、FQDN(ドメイン (page 742)を参照)か、またはそのIPアドレスを使います。

Server Administrator E-Mail
［*Server Administrator E-Mail*］用の、Webサーバ管理者の電子メールアドレスを指定します。

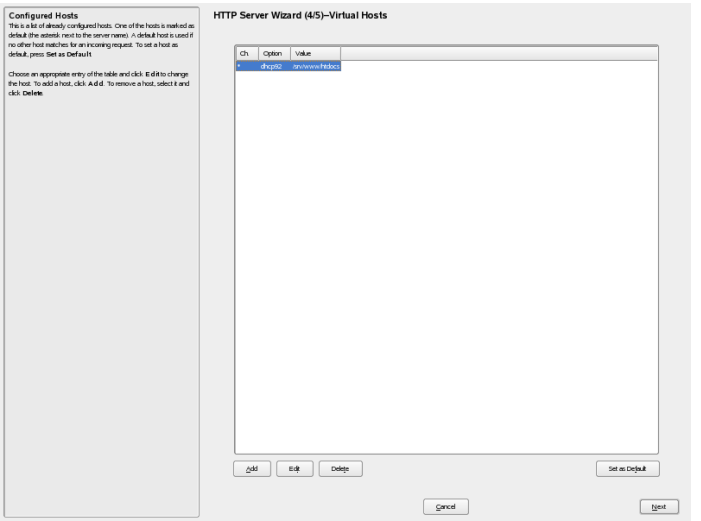
［*Default Host*］のステップを完了したら、［*Next*］をクリックして、設定ダイアログを続けます。

仮想ホスト

このステップでは、ウィザードはすでに設定されている仮想ホストのリストを表示します(項46.4.「仮想ホスト」 (page 767)を参照)。 ホストのうちの1つがデフォルトとして設定されています(サーバ名にアスタリスクの付いているもの)。 デフォルトのホストを設定するには、サーバを選択して［*Set as Default*］をクリックします。

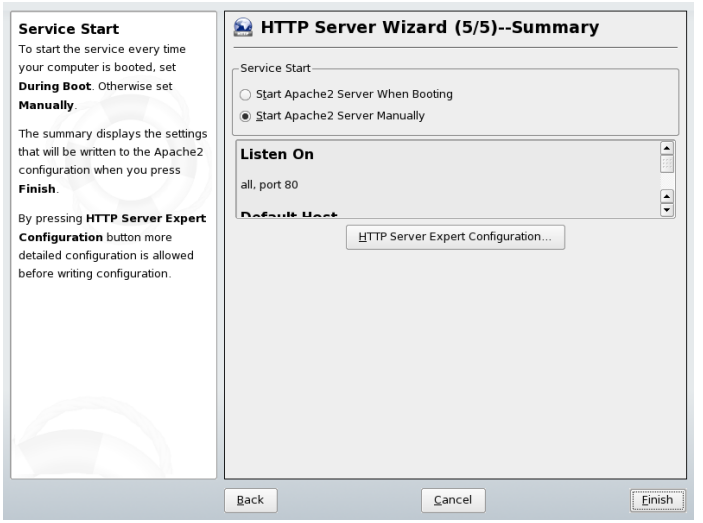
ホストを追加するには、［*Add*］をクリックし、表示されるダイアログにホストについての基本的な情報を入力します。 ［*Server Indentification*］には、サーバ名、サーバのコンテンツのルート、管理者の電子メールアドレスが含まれます。 ウィンドウの左側のフレームに表示されているヘルプテキストでは、これらの項目が詳しく説明されています。 ［*Server Resolution*］は、ホストの識別方法を決めるために用いられます。 それぞれのオプションを選択することにより、HTTPヘッダで要求されたサーバか、またはサーバのIPアドレスによるものかを決められます。 他の可能性としては、クライアントがサーバに接続したときに使用したIPアドレスによって仮想ホストを決める方法もあります。 また、オプションをオンにして、SSLのサポートを有効にすることもできます。 証明書ファイルのパスも指定できます。 ［*Browse*］をクリックすると、デフォルトのディレクトリ `/etc/apache2/ssl.crt`が表示されます。 すべての情報を入力したら、［*Next*］をクリックして、設定の最後のステップに進みます。

図 46.4 *HTTP Server Wizard:仮想ホスト*



[サマリ]
これはウィザードの最後のステップです。ここでは、Apacheサーバの起動をブート時に行うか、それとも手動で行うかを選択できます。先ほど選択したポート、およびデフォルトのホストと仮想ホストも表示されます。この設定でよければ、［*Finish*］をクリックして、設定を完了します。

図 46.5　HTTP Server Wizard:[サマリ]



HTTP Server Expert Configuration (HTTPサーバのエキスパート設定)

HTTPサーバのモジュールも、設定にさらに細かな調整を加えられるようになっています。［*HTTP Server Expert Configuration*］をクリックすると、さらに多くの設定オプションが表示されます。以下の変更が可能です。

Listen On
［*Listen on*］設定を選択して［*Edit*］をクリックすると、新しいウィンドウが表示されて、エントリの追加、削除、編集が行えます。

モジュール
［*Modules*］設定を選択して［*Edit*］をクリックすれば、［*Toggle Status*］によってApache2モジュールのステータスを変更できます。新しいモジュールを追加するには、［*Add Module*］をクリックします。

Default Host (デフォルトのホスト)
［*Default Host*］を選択して［*Edit*］をクリックすれば、ホストの設定を編集できます。 オプションの追加、編集、削除も行えます。

Hosts (ホスト)
［*Hosts*］を選択して［*Edit*］をクリックすれば、ホストの追加、削除、編集、またはホストをデフォルトとして選択することが行えます。

これらのダイアログのどれからでも、［*Log Files*］をクリックすれば、エラーログやアクセスログを表示できます。［*OK*］をクリックして設定を終了し、YaSTコントロールセンターに戻ります。

SSLサポートの追加

ホストにSSLオプションを追加するには、HTTP Server Wizardの3番目のステップ(Default Host)で［*Add*］をクリックします。 サーバがすでにセットアップされているのでウィザードにアクセスできない場合には、HTTP Server Configurationダイアログで［*Default Hosts*］を選択して、［*Edit*］、それから［*Add*］をクリックすれば、SSLオプションをセットアップできます。 どちらの場合でも、ポップアップウィンドウが表示されるので、［*SSL*］オプションまでスクロールし、［*OK*］をクリックして確認します。 次に、選択したオプションの値を入力するよう促されます。 これは、値を*on*または*off*に設定するだけの場合もありますが、ダイアログによっては適切な値を入力することが求められることもあります。 よく分からない場合には、SSLを設定する際に表示される値のパラメータの説明を参照してください。［*OK*］をクリックすると、オプションと値がホストの設定のリストに表示されます。［*Next*］をクリックすると、設定ダイアログの次のステップに進みます。

ホストの設定リストに［*SSL*］が設定されたら、［*Edit*］をクリックしてSSLの設定ダイアログを開きます。 これが表示されない場合には、［*Add*］をクリックし、［*SSL*］を選択して、［*OK*］をクリックすると、ダイアログが自動的に表示されます。 ここではSSLオプションの追加、削除、編集が行えます。［*OK*］をクリックして、HTTP Server Wizardに戻ります。

46.3.2 Apacheを手動で設定する

Apacheを手動で設定するには、`root`ユーザとしてプレーンテキストの設定ファイルを編集する必要があります。

重要項目: Apache2用のSuSEconfigモジュールは存在しない

Apache2用のSuSEconfigモジュールは、SUSE Linuxから削除されました。/etc/sysconfig/apache2を変更した後に、SuSEconfigを実行することはもはや必要ではありません。

/etc/sysconfig/apache2

/etc/sysconfig/apache2は、ロードするモジュール、インクルードする付加的な設定ファイル、サーバを起動するときのフラグ、コマンドラインに追加するべきフラグなど、Apacheのいくつかのグローバル設定を制御します。このファイルの各設定オプションについては、詳細なドキュメントが存在するので、ここでは説明しません。一般的な目的のWebサーバの場合には、/etc/sysconfig/apache2を設定するだけで十分でしょう。特定の設定が必要な場合には、/etc/apache2/httpd.conf内のApacheのディレクティブ: Global Environment 項 (page 760)を参照してください。

重要項目: サーバの起動時に自動的に作成されるファイル

/etc/sysconfig/apache2は、Webサーバの起動または再起動時に、以下のファイルを自動的に作成または編集します。

- /etc/apache2/sysconfig.d/loadmodule.conf—実行時にロードされるモジュール
- /etc/apache2/sysconfig.d/global.conf—サーバ全体の一般設定
- /etc/apache2/sysconfig.d/include.conf—インクルードされた設定ファイルのリスト

これらのファイルは手動で編集しないでください。代わりに、/etc/sysconfig/apache2内の対応する設定を編集してください。

よりきめ細かな設定を行う場合、特に仮想ホスト、グローバル環境、またはメインサーバの手動設定を変更する場合には、/etc/apache2/*のファイルを調べてください。

/etc/apache2/httpd.conf内のApacheのディレクティブ: Global Environment

SUSE Linuxでは、 /etc/apache2/httpd.confを、他の設定ファイルを参照する中心点として用いています。このファイルは、 /etc/sysconfig/apache2では利用できない機能を有効にする場合にのみ、編集してください。 httpd.confの*Global Environment*セクションのディレクティブは、Apacheの全体的な動作に影響を及ぼします。

続くセクションでは、YaSTでは利用できないディレクティブの一部について説明します。Document Root (ドキュメントルート (page 754)) のような中心的なディレクティブは、Global EnvironmentおよびVirtualHostの両方で重要で、必須です。

以下のパラメータとディレクティブは、論理的な関係および設定の影響範囲に従って並べられています。これらはすべて、 /etc/apache2/httpd.conf で設定すべきです。

LoadModule *module_identifier /path/to/module*

LoadModuleディレクティブは、 実行時にロードするApacheモジュールを指定します。*module_identifier*は、ドキュメントに記されているモジュールの名前です。*/path/to/module*は、ファイルへの絶対または相対パスです。

例 46.1 LoadModuleディレクティブ

```
LoadModule rewrite_module /usr/lib/apache2-prefork/mod_rewrite.so
```

On SUSE Linuxでは、LoadModule分を直接使用する必要はありません。代わりに、 /etc/sysconfig/apache2ではAPACHE_MODULEが用いられます。

MaxClients *number*

Apacheが同時に処理できるクライアントの最大数を指定します。MaxClientsは、Webサイトが同時に受けるリクエストを処理できる程度に大きく、すべてのプロセスを処理しても物理RAMが不足することがない程度に小さくする必要があります。

Timeout *seconds*

Apacheが、リクエストのタイムアウトを報告するまでに待つ時間の長さを指定します。

/etc/apache2/httpd.conf内のApacheのディレクティブ: Main Server

Main Serverセクションのディレクティブは、クライアントのリクエストがどのVirtualHostによっても処理されず、そのためメインサーバによって処理される必要がある場合に適用されます。加えて、このコンテキストで定義されたパラメータは、すべての設定済み仮想ホストのデフォルトになります。それで、Main Serverのすべてのディレクティブは VirtualHostコンテキストでも設定することができます。その場合、それらはデフォルトを上書きします。

DirectoryIndex *filenames*

ファイル指定が欠けているURLを補うためにApacheが検索するファイルを設定します。デフォルト値は、index.htmlです。たとえば、クライアントがURLhttp://www.example.com/foo/を要求した場合、ディレクトリfooにファイルindex.htmlがあれば、Apacheはこのページをクライアントに送ります。複数のファイルを指定するには、スペースで区切ります。

例 46.2　DirectoryIndexディレクティブ

```
DirectoryIndex index.html index.shtml start.php begin.pl
```

AllowOverride All | None | *option*

このディレクティブは、<Directory></Directory>宣言の内側でのみ使用できます。Directory (page 754)を参照してください。

AllowOverrideは、.htaccessファイル(またはAccessFileNameで指定された他のファイル、AccessFileName *filenames*項 (page 763)を参照)が、どのアクセスおよび表示オプションを上書きすることができるかを指定します。

可能な値は以下のとおりです。

全て
すべてのオプションは、.htaccessファイルによって上書きすることができます。

なし
.htaccessファイルによって上書きすることができるオプションはありません。

AuthConfig
.htaccessファイルを使用すれば、ディレクトリをパスワードで保護することができます。

FileInfo
.htaccessファイル内でドキュメントタイプを制御するディレクトリの使用を許可します。典型的な例は、ErrorDocumentによるカスタムのエラーページの設定です(http://httpd.apache.org/docs-2.0/mod/core.html#errordocumentを参照)。

Indexes
このパラメータは、DirectoryIndexドキュメントが見つからなかった場合に、Apacheがディレクトリの内容の表示を制御するのを許可します。

Limit
クライアントの、ディレクトリまたは特定のファイルに対するアクセスを制御します。この目的で、ディレクティブAllow、Deny、およびOrderが.htaccessファイル内で使用されます。これらのディレクティブの使用方法については、アクセスモジュールのドキュメントを参照してください(http://httpd.apache.org/docs-2.0/mod/mod_access.html)。

Options
.htaccessファイル内でのOptionsおよびXBitHackディレクティブの使用を許可します。Optionsディレクティブ(http://httpd.apache.org/docs-2.0/mod/core.html#optionsを参照)は、特定のディレクトリでどのサーバ機能を利用可能にするかを制御します。XBitHackディレクティブ(http://httpd.apache.org/docs-2.0/mod/mod_include.html#xbithackを参照)は、SSI (mod_includeによるサーバ側でのインクルード 項 (page 773)を参照)によって解析される実行ビットがセットされたファイルを許可します。

重要項目

これらの設定は、カレントディレクトリとそのサブディレクトリに再帰的に適用されます。これらのオプションは、AllとNoneを除き、スペースで区切って組み合わせることができます。

例 46.3　AllowOverrideディレクティブ

```
<Directory /srv/www/htdocs>
 AllowOverride None
</Directory>
<Directory /srv/www/htdocs/project>
 AllowOverride All
</Directory>
<Directory /srv/www/htdocs/project/webapp>
 AllowOverride Indexes Limit AuthConfig
</Directory>
```

AccessFileName *filenames*

AccessFileNameは、ディレクトリのグローバルアクセス権やその他の設定を上書きできるファイルの名前を設定します (Directory (page 754)を参照)。

デフォルト値は、.htaccessです。複数のファイルを指定するには、スペースで区切ります。

例 46.4　AccessFileNameディレクティブ

```
AccessFileName .htaccess .acl permission.txt
```

ErrorLog *file | "|command"*

Apacheがエラーメッセージのログを出力するファイル名を指定します。また、Apacheはコマンドまたはスクリプトに対してログを出力することもできます。デフォルト設定は/var/log/apache2/error_logです。

例 46.5　ErrorLogディレクティブ

```
ErrorLog /var/log/apache2/error_log
ErrorLog "|/path/to/script"
```

LogLevel *level*

記録されるログメッセージの冗長度を設定します。*level*には以下のものが可能です。下に行くほど、冗長度のレベルが上がり、それほど重大でないメッセージも記録されるようになります。

- emerg（緊急）
- alert（警戒）
- crit（重大）
- error（エラー）
- warn（警告）
- notice（注意）
- info（情報）
- debug（デバッグ）

デフォルトの設定はwarnで、これは通常の運用時に適しています。デバッグを行う場合には、infoやdebugを指定すれば、有用な情報が得られます。

例 46.6　LogLevelディレクティブ

```
LogLevel debug
```

/etc/apache2/httpd.conf内のApacheのディレクティブ: Virtual Hostsセクション

単一の物理マシン上で複数のドメインまたはホスト名を維持するには、VirtualHostコンテナが必要です。これらは設定のVirtual Hostsセクションで宣言します。仮想ホストの構文と機能についての詳細は、項46.4.「仮想ホスト」 (page 767)を参照してください。

46.3.3 Apacheの有効化、起動、および停止

ブート時にApache Webサーバを有効にするには、YaSTのランレベルエディタを使います。起動するには、YaSTで *[システム]* → *[ランレベル・エディター]* の順に選択します。それから、［*apache2*］エントリを探します。マシンのブート時にApacheを自動的に起動するには、［*Enable*］を選択します。経験を積んだユーザは、`chkconfig`ツールを使うこともできます。`/sbin/chkconfig -a apache2`コマンドで同じ結果が得られます。

Apacheを起動または停止するには、`/usr/sbin/rcapache2`スクリプトを`root`ユーザとして実行します。`/usr/sbin/rcapache2`は、Apache Webサーバを起動および停止させる、以下のようなパラメータを受け付けます。

`start`
Apache Webサーバを起動します。

`startssl`
Apache Webサーバを、SSLをサポートする状態で起動します。ApacheがSSLをサポートするように設定する方法についての詳細は、SSLサポートの追加項 (page 758)およびSecure Sockets LayerとApache:`mod_ssl`項 (page 777)を参照してください。

`stop`
Apache Webサーバを停止します。

`configtest`
実際にWebサーバの停止、起動、再起動を行わずに、Apacheの設定をテストします。テストは、サーバを起動、リロード、再起動するたびに強制的に行われるので、通常は明示的にテストを実行する必要はありません。

`restart`
まずWebサーバを停止し、それから再び起動します。

`try-restart`
Webサーバが動作していれば、再起動します。

`restart-hup`
Apache Webサーバを、`SIGHUP`シグナルを送って再起動します。通常は使用しません。

gracefulおよびreload

フォークしたすべてのApacheプロセスに、シャットダウンする前にリクエストを完了させて、それからWebサーバを停止します。1つのプロセスが終了するたびに、新たに開始したもので置き換えられるので、最終的にはApacheが完全に「再起動」したことになります。

ティップ

`rcapache2 reload`は、実働環境でApacheを再起動する場合に推奨されている方法です。接続の切断を行わずに、すべてのクライアントにサービスを提供し続けることができるからです。

---

status

Apache Webサーバの実行時のステータスをチェックします。

*例 **46.7**　Apacheの起動時と停止時の出力例*

```
tux@sun # rcapache2 status
Checking for httpd2:unused

tux@sun # rcapache2 configtest
Syntax OK

tux@sun # rcapache2 start
Starting httpd2 (prefork)                                  done

tux@sun # rcapache2 status
Checking for httpd2:running

tux@sun # rcapache2 graceful
Reload httpd2 (graceful restart)                           done

tux@sun # rcapache2 status
Checking for httpd2:running
```

設定ファイルの記述が間違っていると、Apacheが正しく起動しなかったり、まったく起動しなかったりすることがあります。全く起動しない場合には、メッセージも出力されないことがあります。毎回の起動および再起動時に、メインのエラーログファイルをチェックしてください。

46.4 仮想ホスト

*仮想*ホストという用語は、同じ物理マシンで複数のURI (universal resource identifiers)のサービスを行えるApacheの機能を指しています。これは、www.example.comとwww.example.netのような複数のドメインを、1台の物理マシン上の単一のWebサーバで保持できることを意味しています。

管理の手間(1つのWebサーバを維持すればよい)とハードウェアの費用(ドメインごとの専用のサーバを必要としない)を省くために仮想ホストを使うことは、よく行われています。仮想ホストは名前ベース、IPベース、またはポートベースのいずれかになります。

仮想ホストを設定するには、YaSTを使うか(Default Host (デフォルトのホスト) (page 753)を参照)、または`httpd.conf`の`Virtual Host`セクションを手動で編集します(項46.3.2. 「Apacheを手動で設定する」 (page 758)を参照)。

SUSE LinuxのApacheは、デフォルトでは、`/etc/apache2/vhosts.d/`の仮想ホストごとに1つの設定ファイルを使用するようになっています。仮想ホストの基本的なテンプレートは、このディレクトリ内に用意されています(`vhost.template`)。仮想ホストの設定は、たとえば、1つのファイルに記述してから設定ファイルにインクルードするなど、他の方法でも追加できます。

重要項目

`httpd2 -S`コマンドは、仮想ホストのセットアップをチェックするのにとても便利です。これは、Apacheが解釈している仮想ホストの設定を出力するので、期待したとおりの結果になっているかどうかを確認するのに役立ちます。Apacheに-DSSLのようなフラグを付けている場合には、テストの場合にも、`httpd2 -S -DSSL`のように同じフラグを付けることが必要です。

46.4.1 名前ベースの仮想ホスト

名前ベースの仮想ホストでは、1つのIPアドレスで複数のWebサイトを運用することができます。Apacheは、クライアントから送られたHTTPヘッダのホストフィールドを使用して、要求を、仮想ホスト宣言の1つの、一致する`ServerName`エントリに結び付けます。一致する`ServerName`が見つからな

い場合には、指定されている最初のVirtualHostがデフォルトとして用いられます。

NameVirtualHostは、Apache設定のVirtual Hostセクションを開始します。

NameVirtualHost

NameVirtualHostは、Apache Webサーバに、どのIPアドレス、そしてオプションとしてどのポートをリスンして、HTTPヘッダ内にドメイン名を含むクライアントからのリクエストを受け付けるかを指定します。

最初の引数には完全修飾ドメイン名を指定することができますが、IPアドレスを使用することをお勧めします。2番目の引数はポートで、オプションです。デフォルトでは、ポート80が使用され、Listenディレクティブで設定されます(Network Device Selection (ネットワークデバイスの選択) (page 751)を参照)。

ワイルドカード*は、IPアドレスとポート番号の両方で使用することができます。その場合、すべてのインタフェースでの要求を受け取ります。IPv6のアドレスは、角カッコの中に記述する必要があります。

例 46.8 *名前ベースのVirtualHostエントリの応用例*

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.1.100:80
NameVirtualHost 192.168.1.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:164::]:80
```

名前ベースのコンテキストでの <VirtualHost></VirtualHost>

<VirtualHost></VirtualHost>ブロックには、特定のドメインに適用される情報を記述します。Apacheは、クライアントから定義済みのVirtualHostへの要求を受け取ると、このセクションに記述されているディレクティブを使用します。ここには、VirtualHostコンテキストで許可されている、すべてのApacheディレクティブを使用することができます。VirtualHost開始タグは、名前ベースの仮想ホストの設定では、次の引数を受け付けます。

- NameVirtualHostディレクティブで以前に宣言されたIPアドレス(または完全修飾ドメイン名)。
- NameVirtualHostディレクティブで以前に宣言された、オプションのポート番号。

ワイルドカード*をIPアドレスの代わりに使うこともできます。この構文は、ワイルドカードをNameVirtualHost *として組み合わせて使用する場合にのみ有効です。IPv6アドレスを使用する場合には、アドレスを角カッコの中に記述することが必要です。

例 46.9　名前ベースのVirtualHostディレクティブ

```
<VirtualHost 192.168.1.100:80>
    ServerName www.example.com
    DocumentRoot /srv/www/htdocs/example.com
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com-error_log
    CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>

<VirtualHost 192.168.1.100:80>
    ServerName www.example.net
    DocumentRoot /srv/www/htdocs/example.net
    ServerAdmin webmaster@example.net
    ErrorLog /var/log/apache2/www.example.net-error_log
    CustomLog /var/log/apache2/www.example.net-access_log common
</VirtualHost>

<VirtualHost [2002:c0a8:164::]>
    # 2002:c0a8:164:: is the IPv6 equivalent to 192.168.1.100
    ServerName www.example.org
    DocumentRoot /srv/www/htdocs/example.org
    ServerAdmin webmaster@example.org
    ErrorLog /var/log/apache2/www.example.org-error_log
    CustomLog /var/log/apache2/www.example.org-access_log common
</VirtualHost>
```

この例では、ドメインdomain www.example.comとwww.example.netは両方とも、IPアドレス192.168.1.100のマシンでホストされています。最初のVirtualHostが、Webサーバに送られてくるすべての要求に対するデフォルトとなります。

ディレクティブErrorLog (ErrorLog *file | "|command"* 項 (page 763)を参照)とCustomLog(http://httpd.apache.org/docs-2.0/mod/mod_log

_config.html#customlogを参照)では、ドメイン名を含める必要はありません。ここでは、自由に名前を選択できます。

46.4.2 IPベースの仮想ホスト

この仮想ホスト設定では、1つのコンピュータに対して複数のIPアドレスを設定する必要があります。Apacheの1つのインスタンスが、複数のドメインにホストとしてサービスを提供し、各ドメインに別のIPアドレスが割り当てられることになります。

重要項目: IPアドレスとIPベースの仮想ホスト

物理サーバは、IPベースの仮想ホストごとに、1つのIPアドレスを持つ必要があります。マシンに複数のネットワークカードがない場合には、仮想ネットワークインタフェース(IPエイリアス)を使用することもできます。

IPエイリアスの設定

Apacheで複数のIPアドレスにサービスを提供するには、使用するコンピュータが複数のIPアドレスに対する要求を受け付ける必要があります。これをマルチIPホスティングと呼びます。加えて、カーネルでIPエイリアスを有効にする必要があります。これは、SUSE Linuxのデフォルトの設定です。

カーネルでIPエイリアスを設定すると、コマンドifconfigとrouteを使用して、ホスト上に追加のIPアドレスが設定されます。これらのコマンドは、rootユーザで実行する必要があります。

次の例では、ホストのネットワークデバイスeth0にはすでにIP192.168.0.10が割り当てられているものとします。コマンドifconfigを実行してホストのIPアドレスを確認します。また、次のコマンドでさらにIPアドレスを追加できます。

```
ip addr add 192.168.0.20/24 dev eth0
ip addr add 192.168.0.30/24 dev eth0
```

これらのIPアドレスはすべて、同じ物理ネットワークデバイス(eth0)に割り当てられています。

IPベースのコンテキストでの <VirtualHost></VirtualHost>

いったんIPエイリアスをシステムに設定するか、ホストに複数のネットワークカードを装着すれば、Apacheが設定可能になります。すべての仮想サーバについて、VirtualHostブロックが個別に必要です。

次の例では、IP 192.168.1.10のマシンでApacheが実行されており、付加的なIP 192.168.0.20および192.168.0.30をホストしています。IPアドレス192.168.0.0〜192.168.0.255は公共のインターネットにルーティングされないので、この例はプライベートネットワークでのみ使用できます。

例 46.10　IPベースのVirtualHostディレクティブ

```
<VirtualHost 192.168.0.20>
    ServerName www.example.com
    DocumentRoot /srv/www/htdocs/example.com
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com-error_log
    CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>

<VirtualHost 192.168.0.30>
    ServerName www.example.net
    DocumentRoot /srv/www/htdocs/example.net
    ServerAdmin tux@example.net
    ErrorLog /var/log/apache2/www.example.net-error_log
    CustomLog /var/log/apache2/www.example.net-access_log common
</VirtualHost>
```

ここでは、VirtualHostディレクティブは、192.168.0.10以外のインタフェースに対してのみ指定されています。Listenディレクティブ(Network Device Selection (ネットワークデバイスの選択) (page 751)を参照)を192.168.0.10に対しても設定する場合には、そのインタフェースへのHTTPリクエストに応答する別個のIPベースの仮想ホストを作成する必要があります。そうでなければ、/etc/apache2/httpd.conf (/etc/apache2/httpd.conf内のApacheのディレクティブ: Main Server 項 (page 761)を参照)のMain Serverセクションにあるディレクティブが適用されます。

46.5 Apacheのモジュール

Apacheソフトウェアはモジュール方式で構築されています。コアとなる一部のタスクを除いて、すべての機能はモジュールによって実現されています。この方法で、HTTPさえもモジュールによって処理されています(http_core)。

Apacheのモジュールは、ビルド時にApacheのバイナリに組み込むことも、実行時に動的にロードすることもできます。実行時にロードする方法は、モジュールを手動でロードする場合には`LoadModule module_identifier /path/to/module`項 (page 760)を、YaSTを使う場合にはモジュール (page 752)を参照してください。

SUSE LinuxのApacheには、以下のモジュールが`apache2` RPMの形式で、すぐに使える状態で付属しています(プレフィックスの"mod_"は省略しています)。access、actions、alias、asis、auth、auth_anon、auth_dbm、auth_digest、auth_ldap、autoindex、cache、case_filter、case_filter_in、cern_meta、cgi、charset_lite、dav、dav_fs、deflate、dir、disk_cache、dumpio、echo、env、expires、ext_filter、file_cache、headers、imap、include、info、ldap、log_config、log_forensic、logio、mem_cache、mime、mime_magic、negotiation、proxy、proxy_connect、proxy_ftp、proxy_http、rewrite、setenvif、speling、ssl、status、suexec、unique_id、userdir、usertrack、and vhost_alias。加えて、SUSE Linuxには、以下のApacheモジュールがRPMパッケージとして用意されています。これらは個別にインストールすることが必要です。

`apache2-mod_auth_mysql`、`apache2-mod_fastcgi`、`apache2-mod_macro`、`apache2-mod_murka`、`apache2-mod_perl`、`apache2-mod_php4`、`apache2-mod_php5`、`apache2-mod_python`、and `apache2-mod_ruby`。

これらのモジュールのいくつかについては、このセクションで詳しく説明します。基本ディストリビューションに含まれる他のモジュールについての説明は、`http://httpd.apache.org/docs-2.0/mod/`のApache Modules Webサイトを参照してください。サードパーティのモジュールは、`http://modules.apache.org/`を参照してください。

Apacheのモジュールは、基本モジュール、拡張モジュール、外部モジュールの3津野カテゴリに分けられます。

46.5.1 基本モジュール

基本モジュールは、デフォルトでApacheにコンパイルされています。これらは、ビルド時に明示的に除外しない限り、利用可能です。SUSE LinuxのApacheでは、最小限の基本モジュールだけがコンパイルされていますが、それらはすべて*共有オブジェクト*として利用可能です。`/usr/sbin/httpd2`バイナリ自体に含まれているのではありませんが、`/etc/sysconfig/apache2`の`APACHE_MODULES`を設定することにより、実行時にインクルードすることができます。

mod_includeによるサーバ側でのインクルード

`mod_include`を使えば、データをクライアントに送る前に、ファイルを処理することができます。典型的には、`mod_include`はドキュメントにファイルをインクルードするために用いられます。それからこれらは、クライアントに届けられる前にHTMLとして解析されます。そのためこれは、サーバ側のインクルード(SSI)と呼ばれます。

SSIを使えば、書式設定されたSGMLコメントでトリガされる、特別なコマンドをサーバ側で実行できます。これらのSGMLコマンドの構文は次のとおりです。

```
<!--#element attribute=value -->
```

*element*および*attribute*値のリストは、`http://httpd.apache.org/docs-2.0/mod/mod_include.html`のmod_includeのドキュメントを参照してください。

SUSE Linuxで`mod_include`を使用するには、`/etc/sysconfig/apache2`の`APACHE_MODULES`に`include`を追加するか、モジュール (page 752)で説明されているようにYaSTを使用してください。

ティップ

Apacheに、SSIディレクティブ用に`execute`ビットが設定されたファイルを解析させるには、`XBitHack`ディレクティブ(`http://httpd.apache.org/docs-2.0/mod/mod_include.html#xbithack`)を使用します。

これは、SSI要素を持つものとしてマークするためにファイルの拡張子を変更する代わりに(上の例の.shtml、通常の.htmlファイルを使用して、chmod +x *myfile*.htmlを実行することを意味します。

CGI (Common Gateway Interface)mod_cgi

mod_cgiを使えば、Apacheに、外部のCGI ("Common Gateway Interface")プログラムまたはスクリプトで作成されたコンテンツを配信させることができます。これは、物理マシンで利用可能なプログラミング言語と、Apach Webサーバの間の仲立ちとしての役割を果たします。CGIスクリプトは、理論的にはどのプログラム言語でも作成できます。通常は、PerlやCなどの言語が用いられます。 mod_cgiは、Webサイトに動的なコンテンツを含めるための、最も一般的な方法です。

CGIプログラミングは、HTMLの出力を生成するために、CGIプログラムやスクリプトがContent-type: text/html MIMEタイプを生成できるようになっている必要があるという点で、「通常の」プログラミングとは異なります。

例 46.11 Perlでの簡単なCGIスクリプト

```
#! /path/to/perl
print "Content-type: text/html \n \n";
print "Hello, World. ";
```

1つのプログラミング言語と明確に結び付けられたモジュール(mod_php5など)と、mod_cgiの間の違いは、mod_cgiはmod_suexec (mod_suexecによってCGIを別ユーザとして実行する 項(page 776)参照)と組み合わせることができる、という点にあります。このように組み合わせると、CGIスクリプトを特定のユーザIDで実行することができます。通常、mod_cgiだけ、またはmod_php5を使用するスクリプトは、Apacheユーザ(SUSE Linuxでのデフォルトは wwwrun)のユーザIDで実行されます。プログラミング言語用に設計されたモジュール(mod_php5やmod_rubyなど)は、スクリプトをApacheユーザのIDで実行するための、固定的なインタプリタをApacheに埋め込みます。

こうして、mod_suexecとCGIを組み合わせると、CGIプロセスを、Webサーバ自体の代わりに、個々のユーザに割り当てることができるので、管理がしやすくなります。また、この組み合わせによって、ファイルシステムのセキュリティも向上します。スクリプトは、ユーザのファイルシステムに対する権

限だけを継承するからです。一方、モジュールの場合には、スクリプトはWebサーバユーザのファイルに対する権限を与えられるので、ファイルシステムのデータが意図しない仕方で見えてしまうことがあります。

CGIは、クライアントからWebサーバへのリクエストが終わると、終了します。これは、CGIが永続的なものではなく、終了後には占有していたすべてのリソースを解放することを意味しています。これは利点であり、特にプログラミングにエラーが含まれている場合にそう言えます。モジュールの場合は、インタプリタが固定なので、プログラミングエラーの影響が累積されます。そのため、データベース接続など、リソースを解放しないでしまうことがあり、Apacheの再起動が必要になることがあります。

SUSE Linuxで`mod_cgi`を使用するには、`/etc/sysconfig/apache2`の`APACHE_MODULES`に`cgi`を追加するか、モジュール (page 752)で説明されているようにYaSTを使用してください。SUSE LinuxでのCGIのデフォルトのディレクトリは、`/srv/www/cgi-bin/`です。

Apache設定ファイルを手動で編集する場合には、以下の例を、`mod_cgi`を設定するためのガイドラインとして用いてください。

例 46.12　mod_cgiを手動で有効にする

```
# Global Environment
LoadModule cgi_module /path/to/mod_cgi.so

# Main Server and/or Virtual Host and/or
# Directory and/or .htaccess context
AddHandler cgi-script .cgi .pl

# Main Server and/or Virtual Host context
ScriptAlias /cgi-bin/ /srv/www/cgi-bin/

# Alternatively, explicitly allow CGI scripts in a directory
# Main Server and/or Virtual Host context
<Directory /srv/www/some/dir>
 Options +ExecCGI
<Directory>
```

46.5.2　拡張モジュール

一般に、拡張とされているモジュールは、Apache ソフトウェアパッケージに含まれてはいますが、通常、サーバに静的にはコンパイルされていません。

SUSE Linuxでは、これらはApacheに実行時にロードすることができる共有オブジェクトとして利用可能になっています。

mod_suexecによってCGIを別ユーザとして実行する

mod_suexecとmod_cgi (CGI (Common Gateway Interface)mod_cgi 項 (page 774))を組み合わせれば、 CGIスクリプトを指定したユーザおよびグループとして実行できます。そのためには、 /usr/sbin/suexec2の、suEXECプログラムを使います。これは、CGIスクリプトまたはプログラムが実行されるたびにApacheから呼び出されるラッパーです。それから、ラッパーとプログラムの両方が、設定されたユーザおよびグループIDを取得します。その結果、設定されたユーザまたはグループとして実行されます。

このアプローチは、ユーザが生成するCGIスクリプトに関連したセキュリティリスクをかなりの程度小さくしますが、以下のように、考慮しておくべき重要な点もあります。

suEXECの使用に関連した考慮点

- suEXEC docroot—スクリプトのすべての実行はベースディレクトリに制限されるこれは、docrootの外でスクリプトをsuexecで実行することはできず、エラーになることを意味しています。docrootは、suEXECのコンパイル時に設定され、実行時に変更することはできません。SUSE Linuxでのデフォルトは/srv/wwwです。

- uidmin—これは、suEXECでスクリプトを実行する際に使用するユーザが持っていなければならない、最小のIDを表しています。これにより、スクリプトが、rootなどのシステムユーザとして実行されることを防げます。mod_suexecで使用するのであれば、uidminより小さなIDを持つユーザは作成しないでください。SUSE Linuxでのデフォルトのuidminは96です。

- gidmin—これは、uidminと同様のコンセプトですが、グループIDに関連したものです。 SUSE Linuxでのデフォルトのgidminは96です。

- ディレクトリおよびファイルのパーミッション—対象となるスクリプトは、suEXECのユーザおよびグループとして指定されているのと同じユーザによって所有され、同じグループに属している必要があります。加えて、ファイルは所有者以外による書き込みが禁止になっている必要があり

ます。スクリプトが置かれているディレクトリも、所有者だけが書き込めるようになっている必要があります。

- `suEXEC safepath`—スクリプトで使用されるすべてのプログラム(Perlなど)は、suexecで安全だとラベルされているパス内に置かれている必要があります。`safepath`は、`suEXEC`のコンパイル時に設定され、実行時に変更することはできません。SUSE Linuxでのデフォルトの`safepath`は、`/usr/local/bin:/usr/bin:/bin`です。

`mod_suexec`によってエラーが生じた場合には、suexecのログファイル、`/var/log/apache2/suexec.log`を参照してください。

SUSE Linuxで`mod_suexec`を使用するには、`/etc/sysconfig/apache2`の`APACHE_MODULES`に`suexec`を追加するか、モジュール (page 752)で説明されているようにYaSTを使用してください。suexecを実行するには`mod_cgi`が必要であることに注意してください。

`mod_suexec`は、項46.4.「仮想ホスト」 (page 767)で説明するように、仮想ホスト環境に適用した場合に最も役立ちます。CGIスクリプトを実行する特定のユーザまたはグループを指定するには、仮想ホストの宣言を含んでいるファイル内で(SUSE Linuxでのデフォルトは`/etc/apache2/vhosts.d/*`です)、以下の構文を使用してください。

例 46.13 *mod_suexecの設定*

```
<VirtualHost 192.168.0>
# ..
ScriptAlias /cgi-bin/ /srv/www/vhosts/www.example.com/cgi-bin/
SuexecUserGroup tux users
# ..
</VirtualHost>
```

この例の`SuexecUserGroup` *`username group`*という構文は、`/srv/www/vhosts/www.example.com/cgi-bin/`内のすべてのスクリプトに、tuxのユーザID、そしてusersのグループIDを割り当てます。

Secure Sockets LayerとApache:`mod_ssl`

`mod_ssl`は、クライアントとWebサーバ間のHTTP通信に、SSL (secure sockets layer)およびTLS (transport layer security)プロトコルを使用する、強力な暗号化を提供します。この目的で、サーバは、URLに対するリクエストに応答する

前に、サーバの有効な識別情報を含むSSL証明書を送ります。これにより、サーバが唯一の正当な通信相手であることが保証されます。加えて、この証明書は、クライアントとサーバの間の暗号化された通信が、重要な内容がプレーンテキストとして見られる危険なしに、情報を転送できることを保証します。Apacheで`mod_ssl`を使用する場合の最もはっきりした影響は、URLのプレフィックスが`http://`ではなく`https://`となることです。

Webサーバ側でのSSLおよびTLSリクエストのデフォルトのポートは443です。ポート80をリスンする「通常の」Apacheと、ポート443をリスンするSSL/TLS対応のApacheの間で競合が生じることはありません。実際、HTTPとHTTPSを同一のApacheインスタンスで実行することは可能です。通常、ポート80へのリクエストは1台の仮想ホスト(項46.4. 「仮想ホスト」 (page 767)参照)が処理し、ポート443へのリクエストは別の仮想サーバに送られます。

重要項目: 名前ベースの仮想ホストとSSL

IPアドレスが1つだけの1台のサーバで、複数のSSL対応の仮想ホストを実行することはできません。そのような構成のサーバに接続するユーザは、URLを訪問するたびに、証明書がサーバ名と一致しないという警告メッセージを受け取ることになります。有効なSSL証明書に基づいて通信を行うには、SSL対応のドメインごとに、個別のIPアドレスまたはポートが必要です。

警告メッセージが出されても、有効なSSLサイトと同じレベルの暗号化を利用することはできます。このことは、警告メッセージを受け入れる限り、Webサーバとクライアントの間の通信はセキュアであることを意味しています。ただし、有効なSSL証明書によって保証される、サーバの実体を個別に識別するというコンセプトは、失われます。

SUSE Linuxで`mod_ssl`を有効にするには、`/etc/sysconfig/apache2`の`APACHE_MODULES`に`ssl`を追加するか、モジュール (page 752)で説明されているようにYaSTを使用してください。さらに、標準のHTTPSポート443をリスンするようにWebサーバを構成する必要もあります。これは、`/etc/apache2/listen.conf`で手動で行うか、YaSTの［*Listen*］メニュー項目で行います(Network Device Selection (ネットワークデバイスの選択) (page 751)参照)。

テスト用のSSL証明書は、`root`として`cd /usr/share/doc/packages/apache2; ./certificate.sh`を入力すれば、作成できます。画面に表示される指示に従って、SSL証明書を構築してく

ださい。作成された証明書ファイルは、/etc/apache2/ssl*ディレクトリに置かれます。

グローバルに有効な「実際の」証明書は、Thawte (http://www.thawte.com/)やVerisign (www.verisign.com)などのベンダーから入手できます。

Apache設定ファイルを手動で編集する場合には、以下の例を、mod_sslを設定するためのガイドラインとして用いてください。

例 46.14　mod_sslの手動設定

```
# Global Environment
# listen on the standard SSL port
Listen 443
# load module only if rcapache2 start-ssl was issued
<IfDefine SSL>
LoadModule ssl_module /path/to/mod_ssl.so
</IfDefine>

# Main Server context
# include global (server-wide) SSL configuration
# that is not specific to any virtual host
# only if ssl_module was loaded
<IfModule mod_ssl.c>
Include /etc/apache2/ssl-global.conf
</IfModule>
```

ティップ

SSL対応のApache用に、ファイアウォールのポート443を開くのを忘れないでください。これは、YaSTの *[セキュリティとユーザ]* → *[ファイアウォール]* → *[Allowed Services]*で行えます。 to the list of ［*Allowed Services*］のリストに［*HTTPS Server*］を追加してください。

46.5.3　外部モジュール

公式には、外部とラベルされているモジュールは、Apacheのディストリビューションには含まれていません。しかし、SUSE Linuxでは、それらのいくつかをすぐに使えるように用意しています。この章では、外部モジュールのいくつかと、その機能について、簡単に説明します。

Apacheの管理にPerlを使用する:mod_perl

mod_perlは、Apacheに固定的なPerlインタプリタを埋め込みます。これにより、CGIに対するリクエストがあるたびに外部の実行可能ファイルを呼び出すmod_cgiによるオーバーヘッドを避けられます。mod_perlはさらに、Apacheの機能の様々な面を、Perlプログラミング言語によって制御することを可能にします。

SUSE Linuxでmod_perlを使用するには、apache2-mod_perl RPMをインストールして、モジュールをYaST (モジュール (page 752))で、または/etc/sysconfig/apache2で手動で有効にします。インストールして有効にすると、個別の設定ファイル、mod_perl.confが/etc/apache2/conf.d/に置かれます。さらに、mod_perlの起動スクリプトがmod_perl-startup.plとしてインストールされます。モジュールの使用方法についての詳細は、mod_perlのWebサイト(http://perl.apache.org/)で入手できるドキュメントを参照してください。

PHPを使用する: mod_php4、mod_php5

PHPは、元々Webで使用するために開発された、人気のあるプログラミング言語です。PHP4とPHP5という、2つのバージョンがあります。PHP4は、PHPのクラシックなコンセプトとアプローチを示していますが、PHP5は、新しいオブジェクト指向のプログラミングの可能性と、他の多くの先進的な機能を導入しました。SUSE Linuxでは、mod_php4とmod_php5が両方とも使用できます。これらは、ApacheにPHPインタプリタを永続的なモジュールとして埋め込みます。

SUSE Linuxでmod_php4またはmod_php5を使用するには、それぞれのRPMを(apache2-mod_php4、apache2-mod_php5)インストールして、モジュールをYaST (モジュール (page 752))で、または/etc/sysconfig/apache2で手動で有効にします。

インストールして有効にすると、それぞれのモジュールに対応した個別の設定ファイル(php4.confまたはphp5.conf)が/etc/apache2/conf.d/に置かれます。PHPのWebサイト(http://www.php.net)は、ApacheとPHPを使用するための優れたリソースです。

PythonとApache:mod_python

mod_pythonは、ApachePythonインタプリタを埋め込みます。Pythonは、非常に明快で読みやすい構文を持つ、オブジェクト指向プログラミング言語です。一風変わった、しかし便利な特徴は、プログラムの構造が、beginやendのような通常の区切り要素の代わりに、ソースコードのインデントに基づいているというものです。

SUSE Linuxでmod_pythonを使用するには、apache2-mod_python RPMをインストールして、モジュールをYaST(モジュール (page 752))で、または/etc/sysconfig/apache2で手動で有効にします。モジュールの使用方法についての詳細は、mod_pythonのWebサイト(http://www.modpython.org/)で入手できるドキュメントを参照してください。

ApacheのRubyインタプリタ:mod_ruby

mod_rubyは、Apache WebサーバにRubyインタプリタを埋め込み、RubyのCGIスクリプトをネイティブに実行することを可能にします。Rubyは、比較的新しいオブジェクト指向の高レベルプログラミング言語で、PerlやPythonと似た側面を持っています。Pythonと同様、明快で透明性の高い構文を持ちます。一方、Rubyでは入力ファイルの最終行の番号を$.rで表すなどの省略記法が採用されており、この特徴はプログラマによって賛否両論です。Rubyの基本コンセプトは、Smalltalkに非常によく似ています。

SUSE Linuxでmod_rubyを使用するには、apache2-mod_ruby RPMをインストールして、モジュールをYaST (モジュール (page 752))で、または/etc/sysconfig/apache2で手動で有効にします。モジュールの使用方法についての詳細は、mod_rubyのWebサイト(http://www.modruby.net/en/index.rbx)で入手できるドキュメントを参照してください。

ファイルシステムのネイティブなアクセス:mod_dav

mod_davは、ApacheにWebDAV (Webベースの分散オーサリングおよびバージョニング)機能を追加します。WebDAVは、HTTPプロトコルの拡張で、ユーザがリモートのサーバ上のファイルを共同して編集し、管理することを可能にします。WebDAVの機能はFTPと似ていますが、主な違いは、サーバのアクセスの基礎となるプロトコルとしてHTTPが用いられるということです。

mod_davは、事実上、Apache Webサーバを高度なリモートファイルシステムに変えます。

WebDAVでアクセスできるディレクトリを制限するのは、必要なことではありませんが、良い習慣です。最低限の注意事項は、WebDAVのリソース用にHTTPの基本的な認証をセットアップすることと、Locationディレクティブ内でLimit節を使用することです。

WebDAVのリソースにアクセスするには、クライアント側にWebDAV対応のソフトウェアが必要です。SUSE Linuxにはすでに WebDAV用の機能が備わっています。Konquerorでプレフィックスwebdav://またはwebdavs://(SSL接続でのWebDAVの場合)を使用すれば、Apache WebDAVファイルシステムにアクセスできます。

mod_davはmod_dav_fsモジュールを必要とします。これは、WebDAV用に実際のファイルシステムへのアクセスを提供します。lSUSE Linuxでmod_davを使用するには、モジュールをYaST (モジュール (page 752))で、または/etc/sysconfig/apache2で手動で有効にします。mod_dav_fsについても同じようにします。モジュールの使用方法についての詳細は、mod_davのWebサイト(http://httpd.apache.org/docs-2.0/mod/mod_dav.html)で入手できるドキュメントを参照してください。

ユーザホームページの提供:mod_userdir

SUSE Linuxのmod_userdirは、デフォルトで、各ユーザの~/public_htmlフォルダの内容をパブリックなWebページとして公開します。これらのページにアクセスするためのURLは、http://www.example.com/*~username*/となります。

ティップ

SUSE Linuxのmod_userdirは、rootユーザのホームディレクトリへのアクセスは、セキュリティ上の理由で禁止しています。加えて、以下の構文を使用すれば、特定のユーザのパブリックホームページへのアクセスだけを明示的に許可することができます。

```
# Main server context
UserDir disabled
UserDir enabled tux wilber
```

SUSE Linuxでmod_userdirを使用するには、モジュールをYaST (モジュール (page 752))で、または/etc/sysconfig/apache2で手動で有効にします。モジュールの使用方法についての詳細は、mod_userdirのWebサイト(http://httpd.apache.org/docs-2.0/mod/mod_userdir.html)で入手できるドキュメントを参照してください。

URLのレイアウトを変更する:mod_rewrite

mod_rewriteはよく、「URL操作のスイスアーミーナイフ」に例えられます。これは、リクエストされたURLを、指定されたルールセットに従って、オンザフライで書き換えます。その結果、
http://www.example.com/2/1/deが
http://www.example.com/display.php?cat=2&article=1&lang=de
のようになります。

URL Rewriting Guideでは、この強力ながら複雑なモジュールの長所と短所について説明しています。

「mod_rewriteについては、最初でつまづいて二度と使わないことにするか、そのパワーのために大いに気に入るかの、 どちらかになるでしょう。」

RewriteRuleは、メインサーバ、仮想ホスト、ディレクトリ、.htaccessファイルなどのために、設定コンテキストのどこででも設定できます。mod_rewriteでURLを書き換えるための良い出発点となるのは、 http://httpd.apache.org/docs-2.0/misc/rewriteguide.htmlのURL Rewriting Guideです。

SUSE Linuxでmod_rewriteを使用するには、モジュールをYaST (モジュール (page 752))で、または/etc/sysconfig/apache2で手動で有効にします。

46.6 セキュリティ

公共のインターネットに公開しているWebサーバについては、管理面での不断の努力が求められます。ソフトウェアと、偶然の設定ミスの両方に関連したセキュリティの問題が発生することは避けられません。それらに対処するためのいくつかのヒントを紹介します。

最新の状態を保つ

Apacheソフトウェアに脆弱性が見つかると、SUSEからセキュリティ上の勧告が出されます。これには、脆弱性を修正するための指示が含まれているので、できる限り早く適用すべきです。SUSEによる、セキュリティ関連の発表のメーリングリストは、http://www.suse.com/us/private/support/online_help/mailinglists/で利用可能です。SUSE Linuxパッケージのセキュリティ問題についての最新情報は、http://www.novell.com/linux/security/securitysupport.htmlでも利用可能です。

加えて、Apacheの発表のメーリングリスト(http://httpd.apache.org/lists.html#http-announce)にも加入するべきです。ここでは、新しいリリースとバグ修正がポストされます。

DocumentRootのパーミッション

SUSE Linuxのデフォルトでは、DocumentRootディレクトリ/srv/www/htdocsおよびCGIディレクトリ/srv/www/cgi-binの所有者はユーザrootになっています。これらのパーミッションは変更しないでください。これらのディレクトリにすべてのユーザが書き込めるようにすると、どのユーザでもそこにファイルを配置できるようになります。その後これらのファイルは、Apacheによりwwwrunのパーミッションで実行されます。その結果、意図しない仕方で、ユーザがファイルシステムのリソースにアクセスできるようになる可能性があります。ユーザまたはドメイン固有のデータを整理するには、/srv/www/htdocsおよび/srv/www/cgi-binのサブディレクトリを使用し、Directoryディレクティブと組み合わせてください(Directory (page 754)を参照)。

CGIおよびSSIディレクトリ

Perl、PHP、SSIまたは他のプログラミング言語によるインタラクティブなスクリプトは、事実上、任意のコマンドを実行できます。CGIやSSI (CGI (Common Gateway Interface)、mod_cgi 項 (page 774)、Script Alias (page 755)、およびmod_includeによるサーバ側でのインクルード 項 (page 773)参照)の実行を、グローバルに許可するのではなく、特定のディレクトリに制限することは、リスクを小さくするための1つのオプションです。

別の可能性は、mod_suexec(mod_suexecによってCGIを別ユーザとして実行する 項 (page 776)を参照)を一般のCGIで使用することです。Apacheモジュールでは、PHPを使用する: mod_php4、mod_php5 項 (page 780)で説

明されているように、インタプリタをセキュリティに注意して設定することが、Web環境を安全に保つ上で役立ちます。

アクセス権

多くの場合、特にテスト環境においては、テストという性質のために、Webサーバへのアクセス権が不用意に扱われています。このことは、重要な情報が偶然に明かされたり、さらには、サーバ全体が悪意のある第三者に公開されたりする結果につながります。`Order`ディレクティブ(`http://httpd.apache.org/docs-2.0/mod/mod_access.html#order`)と`.htaccess`ファイル(`AccessFileName` *filenames* 項 (page 763)を参照)を組み合わせて、特定のWebサイトへのアクセスを、特定のユーザまたはクライアントに制限してください。

加えて、「混乱させることによるセキュリティ」と言うアプローチを採用することもできます。典型的な例は、Apacheを標準以外のポートで実行することです(Network Device Selection (ネットワークデバイスの選択) (page 751)を参照)。この場合、`http://www.example.com:8765`のように、URLにポート番号が付加されます。これは、テスト環境では受容できることでしょう。

46.7 トラブルシューティング

Apacheが起動しないと、Webページにアクセスすることはできず、ユーザがWebサーバに接続することもできないので、問題の原因を見つけ出すことは重要です。ここでは、どこを見てエラーの理由を探したらよいかということと、チェックするべき重要な点について説明します。

まず、`rcapache2`(項46.3.3.「Apacheの有効化、起動、および停止」 (page 765)を参照)はエラーについて詳しく報告するので、Apacheの運用で実際に使用すればとても役立ちます。ときには、Webサーバの起動と停止に`/usr/sbin/httpd2`バイナリを使用している場合もあります。これは避けて、代わりに`rcapache2`スクリプトを使用してください。`rcapache2`はまた、設定エラーを解決するためのヒントも提供してくれます。

第2に、ログファイル(ログファイル項 (page 749)を参照)の重要性を十分に認識してください。致命的なエラーとそうでないエラーのどちらの場合でも、Apacheのログファイルを見て、原因を探してください。さらに、ログファイルにさらに詳細な情報を記録することが必要な場合には、`LogLevel`ディレ

クティブ(LogLevel *level* 項 (page 764)を参照)で、記録されるメッセージの詳細さを制御することができます。

ティップ

コマンドtail -F /var/log/apache2/*_log &で、Apacheのログメッセージを確認します。それから、rcapache2 restartを実行します。そして、ブラウザでの接続をもう一度試みて、出力を確認してください。

よくある間違いは、サーバのファイアウォール設定で、Apache用のポートを開けていないことです。YaSTでApacheを設定する場合には、この点を扱うための別個のオプションが存在します。

このようにしても、エラーを特定できない場合には、http://httpd.apache.org/bug_report.htmlの、オンラインのApacheバグデータベースチェックしてください。加えて、http://httpd.apache.org/userslist.htmlのメーリングリストで、Apacheのユーザコミュニティに参加することができます。お勧めできるニュースグループは、comp.infosystems.www.servers.unixです。

46.8 関連資料

Apacheは、広く普及しているWebサーバです。そのため、サポートやヘルプを提供しているWebサイトが数多くあり、その質も様々です。いずれにせよ、Apacheとその可能性を調べるための開始点としては、http://httpd.apache.org/docs-2.0/が最適です。

加えて、RPMパッケージのapache2-docには、Apacheをインストールするためのマニュアルとリファレンスが含まれています。SUSE固有の設定のヒントについては、/usr/share/doc/packages/apache2ファイルにクイックリファレンスが含まれています。

RPMパッケージのapache2-example-pagesには、Webサーバについての情報を表示する、Apache用の例となるページが含まれています。

46.8.1 Apacheのモジュール

項46.5.3.「外部モジュール」 (page 779)の外部Apacheモジュールの詳細については、以下を参照してください。

- http://httpd.apache.org/docs-2.0/mod/
- http://www.php.net/manual/en/install.unix.apache2.php
- http://www.modpython.org/
- http://www.modruby.net/
- http://perl.apache.org/

46.8.2 CGI

mod_cgi (CGI (Common Gateway Interface)mod_cgi 項 (page 774)を参照)の使用方法、およびCGIプログラミングの詳細については、以下を参照してください。

- http://www.modperl.com/
- http://www.modperlcookbook.org/
- http://www.fastcgi.com/
- http://www.boutell.com/cgic/

46.8.3 その他の情報源

SUSE LinuxのApacheに固有な問題が発生したときは、SUSEサポートデータベース(http://portal.suse.com/sdb/en/index.html)を参照してください。

Apacheの沿革は、http://httpd.apache.org/ABOUT_APACHE.htmlで参照できます。このページでは、Apacheというサーバ名の由来についても説明しています。

バージョン1.3から2.0へのアップグレード情報もhttp://httpd.apache.org/docs-2.0/en/upgrading.htmlで参照できます。

47 ファイルの同期

今日、多くの人々が複数のコンピュータを使用しています。自宅に1台、職場に1台またはそれ以上、外出時にラップトップやPDAを携帯することも珍しくありません。これらすべてのコンピュータには、多くのファイルが必要です。どのコンピュータでも作業して、ファイルを変更した後は、すべてのコンピュータで最新バージョンを使用したいと考えるでしょう。

47.1 使用可能なデータ同期ソフトウェア

データの同期は、高速ネットワークで固定接続されているコンピュータ間ではまったく問題なく実現できます。この場合、NFSなどのネットワークファイルシステムを使用し、ファイルをサーバに保存して、すべてのホストがネットワーク経由で同じデータにアクセスすればよいわけです。ところがこの方法は、ネットワーク接続が低速な場合、または固定でない場合には不可能です。ラップトップをもって外出しているとき、必要なファイルをローカルハードディスクにコピーする必要があります。しかし、そうすると今度は、変更したファイルを同期させる必要があります。1台のコンピュータでファイルを変更したときは、必ず他のすべてのコンピュータでファイルを更新しなければなりません。たまにコピーする程度なら、手動でscpまたはrsyncを使用してコピーすればよいでしょう。しかし、ファイルが多い場合、手順が複雑になるだけでなく、新しいファイルを古いファイルで上書きしてしまうといった間違いを防ぐために細心の注意が必要になります。

警告: データ損失の危険

データを同期システムで管理する前に、使用するプログラムをよく理解し、機能をテストしておく必要があります。重要なファイルのバックアップは不可欠です。

このように手動によるデータの同期は、時間がかかる上に間違いが起こりやすい作業ですが、この作業を自動化するためのさまざまな方法を採用したプログラムを使用することで手動による作業は行わずにすみます。ここでの説明は、このようなプログラムの仕組みと使用法について、一般的な理解を図ることを目的としています。実際に使用する場合は、プログラムのマニュアルを参照してください。

47.1.1 Unison

Unisonは、ネットワークファイルシステムではありません。ファイルは単にローカルで保存、編集されます。プログラムUnisonは、手動で実行してファイルを同期させます。同期を初めて実行すると、2台のホスト上にデータベースが作成され、チェックサム、タイムスタンプ、および選択したファイルへのアクセス許可が保存されます。次に実行すると、Unisonはどのファイルが変更されたかを認識でき、ホスト間の伝送を提案します。通常、すべての提案は了承できます。

47.1.2 CVS

CVSは、多くの場合プログラムソースのバージョン管理に使用されるプログラムで、複数のコンピュータでファイルのコピーを保存する機能を持っています。したがって、データ同期にも適しています。CVSはサーバ上に一元的なレポジトリを設定し、ファイルおよびファイルの変更内容を保存します。ローカルに実行された変更はレポジトリにコミットされ、更新によって他のコンピュータに取得されます。両方の処理はユーザによって実行される必要があります。

CVSは、複数のコンピュータで変更が行われた場合、非常に優れたエラー回復力を発揮します。変更内容がマージされ、同じ行が変更された場合は、競合がレポートされます。競合が生じても、データベースは一貫した状態のままです。競合はクライアントホストで解決するためにのみ表示されます。

47.1.3 subversion

「進化を遂げた」CVSとは異なり、subversionは一貫して設計されたプロジェクトです。subversionは、技術面を改良したCVSの後継バージョンとして開発されました。

subversionは、従来のタイプに比べてさまざまな面で改良されています。このような経緯があるため、CVSで維持されるのはファイルのみで、ディレクトリは対象外です。subversionではディレクトリも同様にバージョン履歴をもつため、ファイルと同じようにコピーしたり、名前を変更することができます。また、すべてのファイルとすべてのディレクトリにメタデータを追加できます。このメタデータはバージョニング機能により完全に維持できます。CVSとは異なり、subversionではWebDAV (Web-based Distributed Authoring and Versioning)のような専用プロトコルを介した透過型ネットワークアクセスがサポートされます。WebDAVでは、HTTPプロトコルの機能を拡張して、リモートWebサーバ上のファイルへの書き込みアクセスを共同して行うことを可能にしています。

subversionは既存のソフトウェアパッケージとの組み合わせを念頭に置いて作られています。そのため、Apacheウェブサーバおよび拡張WebDAVは常にsubversionと組み合わせて実行されます。

47.1.4 mailsync

これまでに説明した同期ツールとは異なり、mailsyncはメールボックス間の電子メールの同期だけを実行します。プロシージャは、ローカルのメールボックスファイルとIMAPサーバのメールボックスの両方に適用されます。

電子メールのヘッダに記載されているメッセージIDに基づいて、個々のメッセージを同期させるか、削除します。同期は個別のメールボックス間およびメールボックスの階層間で実行できます。

47.1.5 rsync

バージョン管理は不要であっても、低速ネットワーク接続を使用して大きなディレクトリ構造を同期させる必要がある場合は、ツールrsyncの適切に開発されたメカニズムを使用して、ファイル内の変更箇所のみを送信できます。この処理では、テキストファイルのみでなくバイナリファイルも対象となり

ます。ファイル間の差分を検出するために、rsyncはファイルをブロック単位で分割してチェックサムを計算します。

変更内容の検出処理は高コストを伴います。rsyncの使用量に合わせて、同期対象となるシステムの規模を調整する必要があります。特に、RAMが重要です。

47.2 プログラムを選択する場合の決定要因

47.2.1 クライアントサーバか、ピアツーピアか

一般に、データの配信には2種類のモデルが使用されます。1つは、すべてのクライアントが、そのファイルを一元的なサーバによって同期させるモデルです。サーバはすべてのクライアントから、少なくともいずれかの時点でアクセスできる必要があります。このモデルは、subversion、CVS、およびWebDAVで採用されています。

もう1つは、すべてのネットワークホストがそれぞれのデータをピアとして相互に同期させるモデルです。これは、unisonで採用されている概念です。実際には、rsyncはクライアントモードで動作しますが、すべてのクライアントがサーバとしても動作できます。

47.2.2 移植性

subversion、CVS、およびunisonは、各種のUNIXおよびWindowsシステムなど、他の多くのオペレーティングシステムでも使用できます。

47.2.3 インタラクティブと自動制御

subversion、CVS、WebDAV、およびUnisonでは、ユーザが手動によってデータの同期を開始します。これにより、データの同期を詳細に制御でき、競合

の処理も容易です。ただし、同期の間隔が長すぎると、競合が起こりやすくなります。

47.2.4 競合: 発生と解決法

複数のユーザが大きなプログラミングプロジェクトにかかわっている場合も、subversionまたはCVSでは、競合はまれにしか発生しません。これはドキュメントが個別の行単位でマージされるためです。競合が起こると、影響を受けるのは1台のクライアントだけです。subversionやCVSでは、普通、競合が容易に解決できます。

Unisonは、競合をレポートし、影響を受けたファイルを同期処理から排除します。しかしながら、subversionやCVSでは、変更のマージが容易ではありません。

競合時に変更を部分的に受け入れることができるsubversionやCVSとは対照的に、WebDAVでは、変更が全体的に成功したと見なせる場合にのみチェックインを行います。

rsyncには、競合処理の機能はありません。ユーザは、意図せずにファイルを上書きしないように注意し、考えられる競合はすべて手動で解決する必要があります。安全のために、RCSなどのバージョニングシステムを追加採用できます。

47.2.5 ファイルの選択と追加

標準設定では、Unisonはディレクトリツリー全体の同期が行われます。ファイルシステムに新しく追加したファイルが、自動的に他のコンピュータに表示されます。

subversionまたはCVSでは、新しいディレクトリとファイルは、それぞれコマンド`svn add`または`cvs add`を使用して明示的に追加する必要があります。これにより、同期の対象となるファイルについて、ユーザがより詳細に制御できます。しかし他方で、新しいファイルが見過ごされることが多く、特に`svn update`および`svn status`または`cvs update`の出力に表示される疑問符は、ファイルの数が多いためにたびたび無視されます。

47.2.6 履歴

subversionまたはCVSは追加機能として、古いバージョンのファイルを再構成できます。変更を行うたびに簡単な編集コメントを挿入しておくと、内容とコメントからファイルの作成状況を後で簡単に追跡できます。これは論文やプログラムテキストを作成する際、貴重な支援となります。

47.2.7 データ量と必要なハードディスク容量

同期の対象となるすべてのホストには、分散されたデータを処理できるだけの十分なハードディスクの空き容量が必要です。subversionおよびCVSでは、サーバ上のレポジトリデータベースに余分な容量が必要となります。ファイルの履歴もサーバに保存されるため、このための容量も別に必要です。テキスト形式のファイルが変更されたときには、変更された行だけを保存すれば足ります。バイナリファイルは、ファイルが変更されるたびに、ファイルのサイズと同じだけの容量が必要なため、テキストより必要な容量が多くなります。

47.2.8 GUI

Unisonはグラフィカルユーザインタフェースを備え、Unisonが実行する同期手順を画面に表示します。提案を了承するか、個別のファイルを同期処理から排除します。テキストモードでは、個々の手順を対話型で確認します。

subversionまたはCVSを使い慣れたユーザは、通常、コマンドラインでプログラムを制御します。しかしながら、cervisiaのようなLinux用のグラフィカルユーザインタフェースがあり、また他のオペレーティングシステム用にwincvsなども用意されています。kdevelopなどの開発ツールやemacsなどのテキストエディタの多くが、CVSやsubversionをサポートしています。競合の解決は、これらのフロントエンドの方が、はるかに容易です。

47.2.9　使いやすさ

Unisonとrsyncは使いやすく、初心者にも適しています。CVSとsubversionは、やや操作が難しいプログラムです。ユーザはレポジトリとローカルデータの間のインタラクションを理解する必要があります。データを変更すると、最初にローカルでレポジトリとマージする必要があります。これはコマンド`cvs update`または`svn update`で実行します。次にコマンド`cvs commit`または`svn commit`でデータをレポジトリに送信する必要があります。この手順をいったん理解すれば、初心者でもCVSまたはsubversionを簡単に利用できるようになります。

47.2.10　攻撃に備えるセキュリティ

伝送中、データは妨害や改ざんから保護される必要があります。Unison、CVS、rsync、およびsubversionはいずれもssh(セキュアシェル)経由で容易に使用できるため、この種の攻撃からセキュリティ保護されます。CVSやUnisonをrsh(リモートシェル)経由で実行するのは避けるべきです。 また、安全でないネットワークで*pserver*メカニズムを使用してCVSにアクセスすることもお勧めできません。 subversionは、Apacheで実行することで既に必要なセキュリティ対策を提供しています。

47.2.11　データ損失からの保護

CVSは、プログラミングプロジェクト管理のため長期間にわたって開発者に使用されてきたため、きわめて安定しています。CVSでは開発履歴が保存されるため、誤ってファイルを削除するといったユーザの誤操作にも対応できます。subversionはCVSほど普及してはいませんが、生産的な環境(subversionプロジェクト自体など)に採用されつつあります。

Unisonはまだ比較的新しいプログラムですが、ハイレベルな安定性を誇っています。しかし、ユーザエラーには効果的に対応できません。いったんファイルを削除するという同期処理が確定されたら、そのファイルを復元する手立てはありません。

表 47.1 *ファイル同期ツールの機能:-- = よくない - = あまりよくないまたはサポート対象外、o = 普通、+ = よい、++ = 非常によい、x = サポートされている*

	unison	**CVS/subv.**	**rsync**	**mailsync**
クライアント/サーバ	同等	C-S/C-S	C-S	同等
移植性	Lin、Un*x、Win	Lin、Un*x、Win	Lin、Un*x、Win	Lin、Un*x
対話処理	x	x/x	x	-
速度	-	o/+	+	+
競合	o	++/++	o	+
ファイル選択	ディレクトリ	選択/ファイル、ディレクトリ	ディレクトリ	メールボックス
履歴	-	x/x	-	-
ハードディスクスペース	o	--	o	+
GUI	+	o/o	-	-
難度	+	o/o	+	o
攻撃	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
データ損失	+	++/++	+	+

47.3 Unisonの概要

Unisonは、ディレクトリツリー全体を同期させ、転送するための優れたソリューションです。同期は双方向に実行され、直観的なグラフィカルフロントエンドによって制御できます。コンソールバージョンも使用できます。同期処理を自動化できるため、ユーザとの対話が不要になりますが、使用するには経験が必要です。

47.3.1 必要条件

Unisonは、クライアントとサーバの両方にインストールする必要があります。ここでサーバとは、2番目のリモートホストを指します(CVSとは異なります。項47.1.2. 「CVS」 (page 790)を参照)。

ここでは、Unisonをsshと共に使用します。この場合、SSHクライアントをクライアントにインストールし、SSHサーバをサーバにインストールする必要があります。

47.3.2 Unisonの使用

Unisonで採用されているアプローチは、2つのディレクトリ(*roots*)を互いに関連付けるという方法です。この関連付けはシンボリックです。つまり、オンライン接続があるわけではありません。この例のディレクトリレイアウトは次のとおりです。

クライアント:	`/home/tux/dir1`
サーバ:	`/home/geeko/dir2`

それでは、これらの2つのディレクトリを同期させましょう。ユーザは、クライアント上のtuxおよびサーバ上のgeekoとして認識されています。最初に、クライアントサーバ間通信が有効かどうかをテストします。

```
unison -testserver /home/tux/dir1 ssh://geeko@server//homes/geeko/dir2
```

最もよくある問題は次のとおりです。

- クライアントとサーバで使用されるUnisonのバージョンに互換性がない。
- サーバがSHH接続を使用できない。
- 指定されたパスがどちらも存在しない。

これらに問題がない場合は、オプション`-testserver`を省略します。最初の同期では、Unisonがまだ2つのディレクトリ間の関係を把握していないため、個々のファイルやディレクトリの転送方向についての提案が表示されます。[*Action*]列の矢印は、転送方向を示します。疑問符は、両方のバージョンが変更されている、または両方が新規のため、転送方向についてUnisonが提案を行えないことを示します。

矢印キーを使用して、個々のエントリの転送方向を設定します。表示されているすべてのエントリについて転送方向が適切な場合は、[*Go*]をクリックします。

Unisonの特性(たとえば、問題のないケースについて同期を自動実行するかどうか)は、プログラムの開始時にコマンドラインパラメータで指定して制御することができます。すべてのパラメータのリストは、`unison --help`コマンドで表示できます。

例 47.1 *ファイル ~/.unison/example.prefs*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

各ペアについての同期ログが、ユーザディレクトリ`~/.unison`に保存されます。`~/.unison/example.prefs`のような設定セットもこのディレクトリに保存できます。同期を開始するには、このファイルをコマンドラインパラメータとして`unison example.prefs`のように指定します。

47.3.3 関連資料

Unisonの公式マニュアルは、非常に役に立ちます。そのため、ここでは簡単な概要だけを説明しました。 このマニュアルは、`http://www.cis.upenn.edu/~bcpierce/unison/`とSUSEパッケージ`unison`に完全版が用意されています。

47.4　CVSの概要

CVSは、個々のファイルが頻繁に編集され、ASCIIテキストやプログラムソーステキストのようなファイル形式で保存される場合の同期に適しています。CVSを使用して他の形式、たとえばJPEGファイルのデータを同期させることは可能ですが、データ量が膨大になるとともに、生成される数多くのファイルをCVSサーバに恒久的に保存する必要があります。このような場合、CVSの機能のほとんどが利用できません。CVSを使用したファイルの同期は、すべてのワークステーションが同じサーバにアクセスできる場合のみ可能です。

47.4.1　CVSサーバの設定

サーバとは、すべてのファイルの最新バージョンを含め、有効なファイルが配置されるホストです。固定のワークステーションであれば、どれでもサーバとして使用できます。可能であれば、CVSレポジトリのデータを定期バックアップに含めます。

CVSサーバを設定するとき、できればユーザアクセスをSSH経由で許可します。ユーザがサーバに tux として認識され、CVS ソフトウェアがサーバとクライアントにインストールされている場合、次の環境変数をクライアント側に設定する必要があります。

```
CVS_RSH=ssh CVS_ROOT=tux@server:/serverdir
```

コマンドcvs initを使用して、クライアント側からCVSサーバを初期化します。これは一度だけ実行すれば、後は必要ありません。

最後に、同期に名前を付ける必要があります。クライアント上で、CVSで管理するファイル専用のディレクトリ(空のディレクトリ)を選択するか作成します。ディレクトリには、同期用の名前を付けます。この例で、ディレクトリ名はsynchomeです。このディレクトリに移動し、次のコマンドを入力して、同期名をsynchomeと設定します。

```
cvs import synchome tux wilber
```

CVSの多くはコメントが必要です。このため、CVSはエディタを起動します(環境変数$EDITORで定義されたエディタか、エディタが定義されていない場合はvi)。事前に次の例のようなコマンドラインにコメントを入力しておけば、エディタ呼び出しが避けられます。

```
cvs import -m 'this is a test' synchome tux wilber
```

47.4.2 CVSの使用

これで、すべてのホストがcvs co synchomeを使用して同期レポジトリからチェックアウトできます。これにより、クライアントに新しいサブディレクトリsynchomeが作成されます。変更内容をサーバにコミットするには、ディレクトリsynchome(またはそのサブディレクトリ)に移動し、「cvs commit」と入力します。

デフォルトでは、すべてのファイル(サブディレクトリを含め)がサーバにコミットされます。個別のファイルまたはディレクトリだけをコミットするには、cvs commit file1 directory1のように指定します。新しいファイルとディレクトリは、サーバにコミットする前に、cvs add file1 directory1のようなコマンドを使用してレポジトリに追加する必要があります。この後、cvs commit file1 directory1を実行して、新しく追加したファイルとディレクトリをコミットします。

他のワークステーションに移動する場合、同じワークステーションの以前のセッションで同期レポジトリからチェックアウトしていない場合(前述を参照)は、ここでチェックアウトします。

サーバとの同期は、cvs updateを使用して起動します。cvs update file1 directory1を使用すると、ファイルやディレクトリを個別に更新できます。現行のファイルとサーバに格納されているバージョンとの違いを確認するには、コマンドcvs diffまたはcvs diff file1 directory1を使用します。更新によって変更されたファイルを確認する場合は、cvs -nq updateを使用します。

更新時に表示されるステータス記号の例を次に示します。

U
: ローカルバージョンが更新されました。この更新はサーバが提供しているすべてのファイル、およびローカルにシステムに存在しないすべてのファイルに影響します。

M
: ローカルバージョンが変更されました。サーバ上で変更があれば、その差分がローカルコピーに取り込まれていることがあります。

P
ローカルバージョンに対し、サーバ上のバージョンからパッチが適用されました。

C
ローカルファイルが、レポジトリの現在のバージョンと競合しています。

?
このファイルがCVSに存在しません。

ステータスMは、ローカルで変更されたファイルを示します。ローカルコピーをサーバにコミットするか、ローカルファイルを削除して更新を再実行します。この場合、不足しているファイルは、サーバから取得されます。ローカルに変更したファイルをコミットしたが、そのファイルで同じ行に変更があり以前にコミットされている場合は、競合がCで示されて表示されることがあります。

この場合、ファイルの競合マーク (»> と »>) を確認し、2つのバージョンのどちらを採用するかを決定します。これは厄介な作業のため、変更を破棄し、ローカルファイルを削除して「`cvs up`」と入力し、現在のバージョンをサーバから取得することもできます。

47.4.3 関連資料

ここでは、CVSが持つ多くの機能から、その概要だけを紹介しました。詳細については、多数のマニュアルが次のURLに用意されています。

```
http://www.cvshome.org/
http://www.gnu.org/manual/
```

47.5 subversionの概要

subversionは、無償で公開されているバージョン管理システムであり、一般にCVSの後継と見なされています。つまり、通常、CVSに導入済みの機能はsubversionにも組み込まれています。特に、CVSの長所を考慮しても短所を補いきれないと思われる場合に使用することをお勧めします。この種の機能のほとんどについては、既に項47.1.3.「subversion」 (page 791)で簡単に紹介しています。

47.5.1 Subversionサーバのインストール

サーバにレポジトリーデータベースをインストールする処理は比較的簡単です。subversionには、そのための専用管理ツールが用意されています。新規レポジトリの作成コマンドは、次のとおりです。

```
svnadmin create /path/to/repository
```

svn admin helpを使用すると、その他のオプションをリストできます。CVSとは異なり、subversionはRCSベースではなくBerkeley Databaseベースです。レポジトリはNFS、AFS、またはWindows SMBのようなリモートファイルシステムにインストールしないでください。データベースにはPOSIXロックメカニズムが必要ですが、これらのファイルシステムではこのメカニズムがサポートされていません。

コマンドsvnlookを実行すると、既存のレポジトリに関する情報が表示されます。

```
svnlook info /path/to/repository
```

異なる複数のユーザに対してレポジトリへのアクセスを許可するには、サーバを設定する必要があります。WebDAVとともにApache Webサーバを使用するか、subversionに含まれているサーバパッケージsvnserve を使用します。svnserveを起動すると、svn://またはsvn+ssh://というURLでレポジトリにアクセスできるようになります。svnを呼び出すときに自己認証が必要なユーザは、etc/svnserve.confで設定できます。

Apacheとsvnserveのどちらを使用するかについては、さまざまな判断基準があります。これについては、subversionのマニュアルを参照することをお勧めします。詳細については、項47.5.3.「関連資料」 (page 804)を参照してください。

47.5.2 使用方法と操作

subversionレポジトリにアクセスするには、コマンドsvn(cvsに類似)を使用します。対応するレポジトリに合わせて適切に設定されたサーバから提供されるコンテンツには、どのクライアントからも次のいずれかのコマンドを使用してアクセスできます。

```
svn list http://svn.example.com/path/to/project
```

または

```
svn list svn://svn.example.com/path/to/project
```

既存のプロジェクトを現行のディレクトリに保存(チェックアウト)するには、コマンドsvn checkoutを使用します。

```
svn checkout http://svn.example.com/path/to/project nameofproject
```

チェックアウトすると、クライアント上に新規のサブディレクトリnameofprojectが作成されます。これで、そのサブディレクトリに対して操作(追加、コピー、名前の変更、削除)を実行できます。

```
svn add file
svn copy oldfile newfile
svn move oldfile newfile
svn delete file
```

これらのコマンドは、ディレクトリにも使用できます。subversionでは、ファイルやディレクトリのプロパティも記録できます。

```
svn propset license GPL foo.txt
```

この例では、プロパティlicenseの値GPLを設定しています。プロパティを表示するには、svn proplistを使用します。

```
svn proplist --verbose foo.txt
 Properties on 'foo.txt':
 license : GPL
```

変更内容をサーバに保存するにはsvn commitを使用します。他のユーザはsvn updateを使用してサーバと同期させることで、変更内容を自分の作業ディレクトリに取り込むことができます。

CVSとは異なり、svn statusを使用すると、レポジトリにアクセスしなくてもsubversionの作業ディレクトリのステータスを表示できます。ローカルの変更は5列に表示され、1列目が最も重要です。

''
　変更はありません。

'A'
　オブジェクトには追加マークが付いています。

'D'
　オブジェクトには削除マークが付いています。

'M'
オブジェクトは変更されています。

'C'
オブジェクトは競合しています。

'I'
オブジェクトは無視されました。

'?'
オブジェクトはバージョン管理対象ではありません。

'!'
オブジェクトは欠落としてレポートされています。このフラグが表示されるのは、オブジェクトがsvnコマンドを使用せずに削除または移動された場合です。

'~'
ファイルとして扱われていたオブジェクトがディレクトリで置換された、またはその逆の処理が発生しました。

2列目はプロパティのステータスを示します。他の各列の意味については、subversionのマニュアルを参照してください。

コマンドパラメータの説明を表示するには、コマンドsvn helpを使用します。

```
svn help proplist
proplist (plist, pl): List all properties on files, dirs, or revisions.
usage: 1. proplist [PATH...]
       2. proplist --revprop -r REV [URL]

  1. Lists versioned props in working copy.
  2. Lists unversioned remote props on repos revision.
...
```

47.5.3 関連資料

最初に、http://subversion.tigris.org/にアクセスしてsubversionプロジェクトのホームページを参照してください。パッケージsubversion-docによってディレクトリfile:///usr/share/doc/packages/subversion/html/book.htmlにインストールされるマニュアルも非常に参考になりま

す。このマニュアルはhttp://svnbook.red-bean.com/svnbook/index.htmlでも入手できます。

47.6 rsyncの概要

rsyncは、大量のデータを定期的に送信する必要があるが、変更量はあまり多くない場合に便利です。たとえば、バックアップの作成時などが該当します。もう1つのアプリケーションはステージングサーバに関係します。この種のサーバには、DMZでWebサーバに定期的にミラー化されるWebサーバの完全なディレクトリツリーが格納されます。

47.6.1 設定と操作

rsyncには2つの操作モードがあります。このプログラムを使用してデータをアーカイブまたはコピーできます。そのためには、ターゲットシステム上にsshなどのリモートシェルがあれば十分です。ただし、rsyncをdaemonとして使用し、ネットワークにディレクトリを提供することもできます。

rsync の基本操作モードの場合、特別な設定は不要です。 rsync では、ディレクトリ全体を別のシステムに直接ミラー化できます。 たとえば、次のコマンドでは、tuxのホームディレクトリのバックアップがバックアップサーバsun上に作成されます。

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

次のコマンドは、ディレクトリを復元する場合に使用します。

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

ここまでの操作は、scpのような通常のコピーツールの場合とほぼ同じです。

rsyncのすべての機能を完全に使用可能にするには、「rsync」モードで操作する必要があります。そのためには、いずれかのシステムでrsyncdデーモンを起動します。設定はファイル/etc/rsyncd.conf内で行います。たとえば、rsyncでディレクトリ/srv/ftpを使用可能にするには、次の設定を使用します。

```
gid = nobody
uid = nobody
read only = true
```

```
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

次に、rcrsyncdstartを使用してrsyncdを起動します。また、ブート処理中にrsyncdを自動的に起動する方法もあります。 このようにセットアップするには、このサービスをYaSTのランラベルエディタで有効にするか、またはコマンドinsservrsyncdを入力します。 また、rsyncdをxinetdで起動することもできます。ただし、この方法はrsyncdの使用頻度が低いサーバの場合にのみ使用してください。

この例では、すべての接続を示すログファイルも作成されます。このファイルは/var/log/rsyncd.logに格納されます。

これで、クライアントシステムからの転送をテストできます。そのためには次のコマンドを使用します。

```
rsync -avz sun::FTP
```

このコマンドを入力すると、サーバのディレクトリ/srv/ftpにあるファイルがすべてリストされます。このリクエストはログファイル/var/log/rsyncd.logにも記録されます。実際の転送を開始するには、ターゲットディレクトリを指定します。現在のディレクトリには.を使用してください。次に例を示します。

```
rsync -avz sun::FTP .
```

デフォルトでは、rsyncでの同期中にファイルは削除されません。ファイルを削除する必要がある場合は、オプション--deleteを追加してください。新しい方のファイルが削除されないように、代わりにオプション--updateを使用することもできます。競合が発生した場合は、手動で解決する必要があります。

47.6.2 関連資料

rsyncに関する重要な情報は、マニュアルページman rsyncおよびman rsyncd.confを参照してください。rsyncの基本原則に関する技術情報につい

ては、/usr/share/doc/packages/rsync/tech_report.psを参照してください。rsyncの最新ニュースについては、このプロジェクトのWebサイトhttp://rsync.samba.org/を参照してください。

47.7 mailsyncの概要

mailsyncは、主に次の3種類のタスクに適しています。

- ローカルに保存されている電子メールをサーバに保存されているメールと同期させる。
- メールボックスを異なる形式または異なるサーバに移行する。
- メールボックスの完全性チェックまたは重複の検索を行う。

47.7.1 設定と使用

mailsyncは、メールボックス自体(ストア)と2つのメールボックス間の接続(チャネル)を区別します。ストアとチャネルの定義は、~/.mailsyncで説明されています。ここでは、ストアの例をいくつか示します。

単純な定義は次のようになります。

```
store saved-messages {
   pat Mail/saved-messages
prefix  Mail/
}
```

Mail/とは、ユーザのホームディレクトリのサブディレクトリであって、フォルダsaved-messagesをはじめとする電子メールフォルダが格納されています。mailsyncがmailsync -m saved-messagesで始まっている場合、すべてのメッセージのインデックスは、saved-messagesにリストされます。次のように定義されている場合、

```
store localdir {
pat     Mail/*
prefix  Mail/
}
```

コマンドmailsync -m localdirを実行すると、Mail/の下位に保存されているすべてのメッセージがリストされます。これとは異なり、コマンドmailsync localdirを実行するとフォルダ名がリストされます。IMAPサーバでのストアの指定は次のようになります。

```
store imapinbox {
server {mail.edu.harvard.com/user=gulliver}
ref    {mail.edu.harvard.com}
pat    INBOX
}
```

上の例は、単にIMAPサーバ上のメインフォルダのアドレス指定です。サブフォルダのストアは次のように表示されます。

```
store imapdir {
server {mail.edu.harvard.com/user=gulliver}
ref {mail.edu.harvard.com}
pat INBOX.*
prefix  INBOX.
}
```

IMAPサーバが暗号化接続をサポートしている場合、サーバ指定を次のように変更する必要があります。

```
server {mail.edu.harvard.com/ssl/user=gulliver}
```

変更しなければ、サーバ証明書が次のサーバに認識されません。

```
server {mail.edu.harvard.com/ssl/novalidate-cert/user=gulliver}
```

プレフィクスについては、後で説明します。

ここでMail/の下位のフォルダをIMAPサーバのサブディレクトリに接続する必要があります。

```
channel folder localdir imapdir {
msinfo .mailsync.info
}
```

mailsyncはmsinfoファイルを使用して、既に同期されているメッセージを追跡します。

コマンドmailsync folderを実行すると、次の処理が行われます。

- メールボックスパターンが、両方の側で拡張されます。
- 作成されたフォルダ名からプレフィクスが取り除かれます。

- フォルダがペアとして同期されます(片方が存在しない場合は作成されます)。

これにより、IMAPサーバ上のINBOX.sent-mailが、ローカルフォルダMail/sent-mail(前述の定義が存在する場合)と同期されます。個々のフォルダ間の同期は、次のように実行されます。

- メッセージが両方の側に存在する場合は何も行いません。
- 片側にメッセージが存在せず、新規メッセージ(msinfoファイルに存在しない)の場合は送信されます。
- 単にメッセージが片側に存在し、古いメッセージ(msinfoファイルに存在する)の場合は削除されます(もう片方に以前存在したメッセージが削除されているため)。

同期によって、どのメッセージが送信送され、どのメッセージが削除されるかを事前に確認するには、mailsync folder localdirを使用して、チャネルとストアの*両方*に対しmailsyncを実行します。このコマンドを実行すると、ローカルホストにあるすべての新規メッセージのリストと共に、同期の際にIMAP側で削除されるすべてのメッセージのリストが作成されます。同様に、コマンドmailsync folder imapdirを実行すると、IMAP側にあるすべての新規メッセージのリストと共に、同期の際にローカルホストで削除されるすべてのメッセージのリストが作成されます。

47.7.2 起こり得る問題

データが損失した場合、最も安全な方法は、関連のチャネルログファイルmsinfoを削除することです。これにより、片方だけに存在するメッセージはすべて新規とみなされ、次回の同期の際に送信されます。

同期の対象となるのは、メッセージIDを持つメッセージのみです。メッセージIDのないメッセージは無視され、送信も削除もされません。メッセージIDのないメッセージは、通常、そのメッセージの送信または作成時にプログラムに障害が発生します。

IMAPサーバによっては、メインフォルダがINBOXとして識別され、そのサブフォルダが無作為に選択された名前(INBOXとINBOX.nameではなく)で識別さ

れます。このようなIMAPサーバでは、サブフォルダだけに使用されるパターンを指定することができません。

IMAPサーバにメッセージを正常に送信すると、mailsyncが使用するメールボックスドライバ(c-client)が、特別なステータスフラグを設定します。このため、muttなど一部の電子メールプログラムでは、これらのメッセージを新規として認識できません。この特別なステータスフラグの設定を無効にするには、オプション–nを使用します。

47.7.3 関連資料

mailsyncの/usr/share/doc/packages/mailsync/にあるREADMEには、関連情報が記述されています。またこのトピックに関しては、RFC 2076「Common Internet Message Headers」が特に参考になります。

48

Samba

Sambaを使用すると、DOS、Windows、OS/2マシンに対するファイルサーバおよびプリントサーバをUnixマシン上に構築できます。Sambaは、今や成熟の域に達したかなり複雑な製品です。基本的な機能に加えて、この章では、Sambaの設定に関する基本事項について、およびネットワーク上でのSambaの設定に使用できるYaSTモジュールについて説明します。

Sambaについての詳細な情報は、デジタルドキュメントの形で入手できます。コマンドラインからapropos samba と入力するとマニュアルページを参照できます。または、Sambaをインストール済であれば、/usr/share/doc/packages/sambaディレクトリに格納されているオンラインマニュアルと例を参照できます。また、コメント付きの設定例(smb.conf.SuSE)がexamplesサブディレクトリに用意されています。

付属のバージョン3のsambaパッケージは、次のような重要な新機能を備えています。

- Active Directoryのサポート
- Unicodeサポートの拡張
- 内部認証メカニズムの全面改訂
- Windows 200xおよびXP印刷システムの大幅な機能向上
- Active Directoryドメインのメンバサーバとしてのサーバのセットアップ
- NT4ドメインの採用と、NT4ドメインからSambaドメインへの移行の実現

ティップ: Samba3への移行

Samba 2.xからSamba 3に移行するときは、いくつか特別な配慮が必要です。このトピックについては、『Samba HOWTO Collection』で1章全部を費やして説明されています。`samba-doc`パッケージのインストール後、`/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`でHOWTOを確認してください。

SambaはSMBプロトコル(サーバメッセージブロック)を使用します。SMBはNetBIOSサービスを基にしています。IBMからの圧力によって、Microsoftがこのプロトコルをリリースしたので、他のソフトウェアメーカはMicrosoftドメインネットワークに接続できるようになりました。Sambaでは、SMBプロトコルがTCP/IPプロトコルの上で動作するので、すべてのクライアントにTCP/IPプロトコルをインストールする必要があります。

は、マシン間通信用に設計されたソフトウェアインタフェース(API)です。ここではネームサービスが提供されています。これにより、ネットに接続されたマシンが、それ自体の名前を維持できます。予約を行えば、これらのマシンを名前によって指定できます。名前をチェックする一元的なプロセスはありません。ネットワーク上のマシンは、すでに使用済みの名前でない限り、名前をいくつでも予約できます。現在、NetBIOSインタフェースは、異なるネットワークアーキテクチャ用に実装できるようになっています。ネットワークハードウェアと比較的密接に機能する実装はNetBEUIと呼ばれますが、これはよくNetBIOSとも呼ばれます。NetBIOSとともに実装されるネットワークプロトコルは、Novell IPX (TCP/IP経由の NetBIOS)とTCP/IPです。

TCP/IP経由で送信されたNetBIOS名は、`/etc/hosts`で使用されている名前、またはDNSで定義された名前とまったく共通点がありません。NetBIOSは独自の、完全に独立した名前付け規則を使用しています。しかし、管理を容易にするために、DNSホスト名に対応する名前を使用することをお勧めします。これはSambaが使用するデフォルトでもあります。

Mac OS X、Windows、OS/2などの一般的なオペレーティングシステムは、すべてSMBプロトコルをサポートしています。TCP/IPプロトコルは、すべてのコンピュータにインストールする必要があります。Sambaは、異なるUNIXフレーバーに対してクライアントを提供します。Linuxでは、SMB用のカーネルモジュールがあり、LinuxシステムレベルでのSMBリソースの統合が可能です。

SMBサーバは、そのクライアントに対し、共有によってハードウェア空間を提供します。共有には、サーバ上のディレクトリとそのサブディレクトリが含まれます。これは名前によってエクスポートされ、名前によってアクセスされます。共有名にはどのような名前も設定できます。エクスポートディレクトリの名前である必要はありません。プリンタにも名前が割り当てられます。クライアントはプリンタに名前でアクセスできます。

48.1 サーバの設定

Sambaをサーバとして使用する場合は、sambaをインストールする必要があります。Samba に必要なサービスは、rcnmb start && rcsmb start で起動し、rcsmb stop && rcnmb stop で停止します。

Sambaの主となる設定ファイルは /etc/samba/smb.conf です。このファイルは2つの論理部分に分けられます。[global]セクションには、中心的なグローバル設定が含まれます。[share]セクションには、個別のファイルとプリンタ共有が入っています。このアプローチにより、共有に関する詳細は[global]セクションで個別に、またはグローバルに設定することができ、設定ファイルの構造的透過性が高まっています。

48.1.1 グローバルセクション

[global]の次のパラメータは、ネットワークの設定に応じた必要条件を満たし、Windows環境で他のマシンがSMBを経由してこのSambaサーバにアクセスできるようにするために多少の調整が必要です。

workgroup = TUX-NET

この行は、Sambaサーバをワークグループに割り当てます。TUX-NETを実際のネットワーク環境にある適切なワークグループに置き換えてください。DNS名がネットワーク内の他のマシンに割り当てられていなければ、SambaサーバがDNS名の下に表示されます。DNS名が使用できない場合は、netbiosname=MYNAMEを使用してサーバ名を設定します。このパラメータについての詳細はmansmb.confを参照してください。

os level = 2

このパラメータは、SambaサーバがワークグループのLMB(ローカルマスタブラウザ)になるかどうかのきっかけとなります。Sambaサーバの設定が

誤っていた場合に、既存のWindowsネットワークに支障が出ないよう、小さな値を選択します。この重要なトピックについての詳細は、パッケージマニュアルのtextdocsサブディレクトリにあるBROWSING.txtとBROWSING-Config.txtを参照してください。

ネットワーク内に他のSMBサーバ(たとえば、Windows NTまたは2000サーバ)が存在せず、ローカル環境に存在するすべてのシステムのリストをSambaサーバに保存する場合は、os levelの値を大きくします(たとえば、65)。これでSambaサーバが、ローカルネットワークのLMBとして選択されました。

この設定を変更するときは、それが既存のWindowsネットワーク環境にどう影響するかを慎重に検討する必要があります。まず、隔離されたネットワークで、または影響の少ない時間帯に、変更をテストしてください。

wins supportとwins server

アクティブなWINSサーバをもつ既存のWindowsネットワークにSambaサーバを参加させる場合は、wins serverオプションを有効にし、その値をWINSサーバのIPアドレスに設定します。

各Windowsマシンの接続先サブネットが異なり、互いを認識させなければならない場合は、WINSサーバをセットアップする必要があります。SambaサーバをWINSサーバなどにするには、オプションwins support = Yesを設定します。ネットワーク内でこの設定が有効なSambaサーバは1台だけであることを確認します。smb.confファイル内で、オプションwins serverとwins supportは同時に有効にしないでください。

48.1.2 共有

次の例では、SMBクライアントがCD-ROMドライブとユーザディレクトリ(homes)を利用できるようにする方法を示します。

[cdrom]

CD-ROMドライブが誤って利用可能になるのを避けるため、これらの行はコメントマーク(この場合はセミコロン)で無効にします。最初の列のセミコロンを削除し、CD-ROMドライブをSambaと共有します。

*例 **48.1*** *CD-ROMの共有*

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

[cdrom]および*コメント*

エントリ[cdrom]は、ネットワーク上のすべてのSMBクライアントが認識できる共有の名前です。さらにcommentを追加して、共有を説明することができます。

path = /media/cdrom

pathオプションで、/media/cdromディレクトリをエクスポートします。

デフォルトを非常に制約的に設定することによって、このシステム上に存在するユーザのみがこの種の共有を利用できるようになります。この共有をあらゆるユーザに開放する場合は、設定にguest ok = yesという行を追加します。この設定は、ネットワーク上の全ユーザに読み込み許可を与えます。このパラメータを使用する場合には、相当な注意を払うことをお勧めします。またこのパラメータを[global]セクションで使用する場合には、さらに注意が必要です。

[homes]

[home]共有は、ここでは特に重要です。ユーザがLinuxファイルサーバの有効なアカウントとパスワードを持ち、独自のホームディレクトリを持っていればそれに接続することができます。

*例 **48.2*** *homes共有*

```
[homes]
 comment = Home Directories
 valid users = %S
 browseable = No
 read only = No
 create mask = 0640
 directory mask = 0750
```

[homes]

SMBサーバに接続しているユーザの共有名を他の共有が使用していない限り、[homes]共有ディレクティブを使用して共有が動的に生成されます。 生成される共有の名前は、ユーザ名になります。

valid users = %S
%S は、接続が正常に確立されるとすぐに、具体的な共有名に置き換えられます。[homes]共有の場合、これは常にユーザ名です。したがって、ユーザの共有に対するアクセス権は、そのユーザだけに付与されます。

browseable = No
この設定を行うと、共有がネットワーク環境で認識されなくなります。

read only = No
デフォルトでは、Sambaはread only = Yesパラメータによって、エクスポートされた共有への書き込みアクセスを禁止します。共有に書き込めるように設定するには、値read only = Noを設定します。これはwriteable = Yesと同値です。

create mask = 0640
MS Windows NTベース以外のシステムは、UNIXのパーミッションの概念を理解しないので、ファイルの作成時にアクセス権を割り当てることができません。パラメータcreate maskは、新しく作成されたファイルに割り当てられるアクセス権を定義します。これは書き込み可能な共有にのみ適用されます。実際、この設定はオーナーが読み書き権を持ち、オーナーの一次グループのメンバが読み込み権を持つことを意味します。valid users = %Sを設定すると、グループに読み込み権が与えられても、読み込みアクセスができなくなります。グループに読み書き権を付与する場合は、valid users = %Sという行を無効にしてください。

48.1.3 セキュリティレベル

SMBプロトコルはDOSやWindowsの世界から生まれ、セキュリティの問題についてもよく考慮されています。各共有へのアクセスは、パスワードによって保護されています。SMBには、パーミッションをチェックする方法が3つあります。

共有レベルのセキュリティ(セキュリティ=共有):
パスワードが共有に対し確実に割り当てられています。このパスワードを持っているユーザ全員が、その共有にアクセスできます。

ユーザレベルのセキュリティ(セキュリティ=ユーザ):
このセキュリティレベルは、ユーザという概念をSMBに取り入れています。各ユーザは、サーバにパスワードを登録する必要があります。登録後、エクスポートされた個々の共有へのアクセスは、ユーザ名に応じてサーバが許可します。

サーバレベルのセキュリティ(セキュリティ=サーバ):
クライアントに対しては、Sambaがユーザレベルモードで動作しているように見えます。しかし、Sambaはすべてのパスワードクエリを別のユーザレベルモードサーバに渡し、ユーザレベルモードサーバが認証を行います。設定には追加のパラメータが必要です(`password server=`)。

共有、ユーザ、およびサーバレベルのセキュリティの区別は、サーバ全体に適用されます。個別の共有ごとに、ある共有には共有レベルのセキュリティ、別の共有にはユーザレベルセキュリティを設定するといったことはできません。しかし、システム上に設定したIPアドレスごとに、別のSambaサーバを実行することは可能です。

この詳細については、『Samba HOWTO Collection』を参照してください。つのシステムに複数のサーバをセットアップする場合は、オプション`interfaces`および`bind interfaces only`に注意してください。

ティップ

Sambaサーバでの管理作業を簡単にするため、swatというプログラムも用意されています。このプログラムには、Sambaサーバを便利に設定するための簡単なWebインタフェースがあります。Webブラウザで、`http://localhost:901`を開き、`root`ユーザでログインします。ただし、swatをファイル`/etc/xinetd.d/samba`と`/etc/services`で有効にする必要があります。これには、`/etc/xinetd.d/samba`で`disable`の行を`disable = no`のように編集します。swatの詳細については、マニュアルページを参照してください。

48.2 ログインサーバとしてのSamba

Windowsクライアントが大部分を占めるネットワークでは、ユーザが有効なアカウントとパスワードを持つ場合のみ登録できることが求められるのが普通です。これは、Sambaサーバで実現されます。Windowsベースのネットワー

クでは、このタスクはプライマリドメインコントローラ(PDC)として設定されたWindowsNTサーバによって処理されます。例 48.3. 「smb.confファイルのグローバルセクション」 (page 818)に示すように、smb.confの[global]セクションにエントリを追加する必要があります。

例 48.3　smb.confファイルのグローバルセクション

```
[global]
  workgroup = TUX-NET
  domain logons = Yes
  domain master = Yes
```

暗号化されたパスワードが検証に使用されている場合は(強固に保守されたMS Windows 9xインストール、MS Windows NT 4.0(サービスパック3以降)、およびそれ以降にリリースされた製品でのデフォルト設定)、Sambaサーバでこれを処理できる必要があります。これには、[global]セクションでエントリencrypt passwords = yesを指定します(Sambaバージョン3ではデフォルト)。また、ユーザアカウントとパスワードをWindowsに準拠した暗号化形式で作成する必要があります。そのためにはコマンドsmbpasswd -a nameを実行します。さらに次のコマンドを使用して、Windows NTドメイン概念で必要になるコンピュータのドメインアカウントを作成します。

例 48.4　マシンアカウントのセットアップ

```
useradd hostname\$
smbpasswd -a -m hostname
```

useraddコマンドを使用すると、ドル記号が追加されます。コマンドsmbpasswdを指定すると、パラメータ-mを使用したときにドル記号が自動的に挿入されます。コメント付きの設定例(/usr/share/doc/packages/Samba/examples/smb.conf.SuSE)には、この作業を自動化するための設定が含まれています。

例 48.5　マシンアカウントの自動セットアップ

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Sambaがこのスクリプトを確実に正しく実行できるようにするため、必要な管理者許可を持つSambaユーザを選択します。これには、1人のユーザを選択してntadminグループに追加します。これにより、このLinuxグループに属するすべてのユーザに対し、次のコマンドによってDomain Adminステータスを割り当てることができます。

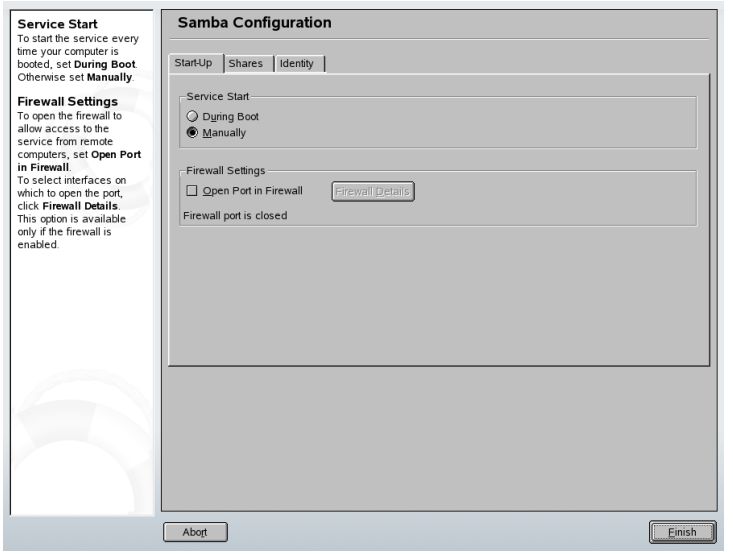
```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

この詳細については、`/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`の『Samba HOWTO Collection』の第12章を参照してください。

48.3 YaSTによるSambaサーバの設定

サーバの設定は、新しいSambaサーバが制御するワークグループまたはドメインを選択することから始めます。［*Workgroup or Domain Name*］から既存のものを選択するか、新しいものを入力してください。次に、サーバをPDC(プライマリドメインコントローラ)とBDC (バックアップドメインコントローラ)のどちらとして動作させるかを指定します。

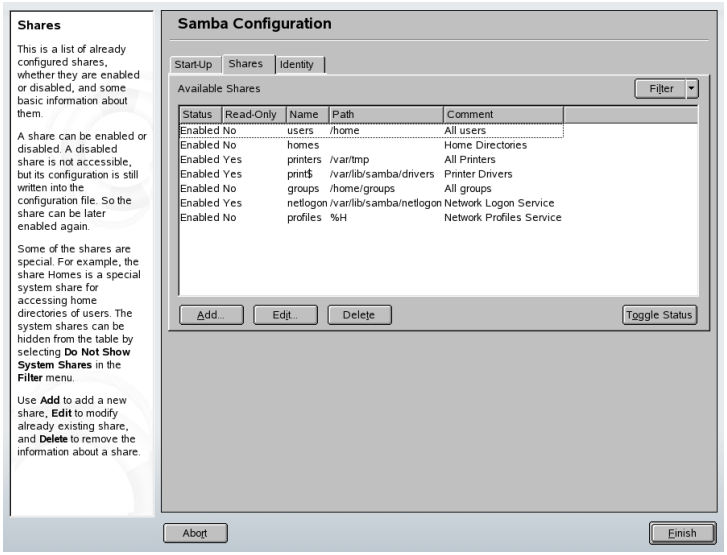
図 48.1 Sambaの設定—起動



［*Start Up*］でSambaをアクティブにします(図 48.1. 「Sambaの設定—起動」(page 819))。Sambaサーバを円滑に運用できるように、サーバ上のファイアウォールですべての外部インタフェースと内部インタフェースに対して`netbios-ns`、`netbios-dgm`、`netbios-ssn`、`microsoft-ds`の各サービ

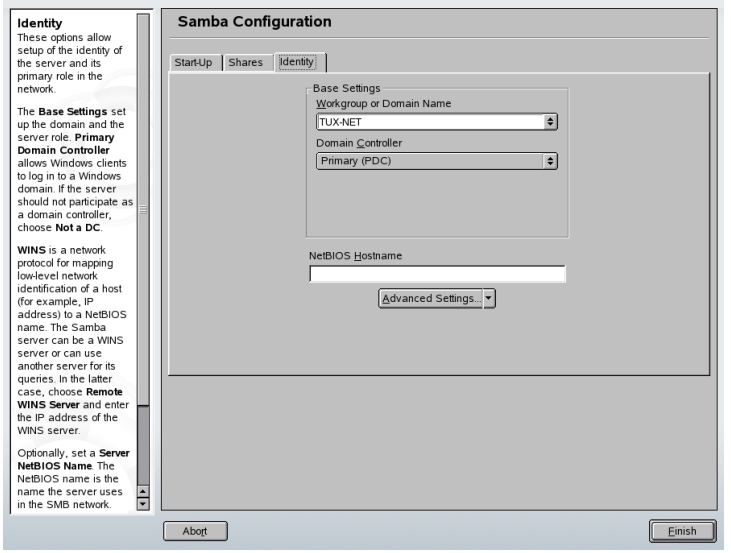
ス用のポートを開くには、[ファイアウォールで開いているポート]を選択して、[ファイアウォールの詳細]を使用します。

図 48.2　Sambaの設定—共有



[*共有*]タブ(図 48.2. 「Sambaの設定—共有」 (page 820))で、有効にするSambaの共有を指定します。［*状態の変更*]を使用して、[*有効*]と[*無効*]の間で切り替えます。新しい共有を追加するには[*追加*]をクリックします。

図 48.3　Sambaの設定—識別



[*Identity*]タブ(図 48.3. 「Sambaの設定—識別」 (page 821))で、ホストが関連付けられているドメイン([*Base Settings*])と、ネットワークで代替ホスト名を使用するかどうか([*NetBIOS Host Name*])を指定します。

48.4　クライアントの設定

クライアントは、TCP/IP経由でのみSambaサーバにアクセスできます。IPX経由のNetBEUIおよびNetBIOSは、Sambaで使用できません。

48.4.1　YaSTによるSambaクライアントの設定

Sambaサーバ上の共有リソース(ファイルまたはプリンタ)にアクセスするSambaクライアントを設定します。［*SAMBA ワークグループ*]ダイアログで、ドメインまたはワークグループを入力します。［*検索*]をクリックすると、使用可能なすべてのグループとドメインが表示され、マウスで選択することができます。［*Linuxの認証にもSMBの情報を用いる*]を有効にした場合、ユーザ認証は

Sambaサーバによって行われます。設定が終わったら、[完了]をクリックします。

48.4.2 Windows 9xおよびME

Windows 9xおよびMEには、あらかじめTCP/IPのサポートが組み込まれています。しかし、デフォルトでインストールされるわけではありません。TCP/IPを追加するには、*[コントロール パネル]*、 → *[システム]*に移動し、*[追加]*、 → *[プロトコル]*、 → *[TCP/IP]*の順に選択します。Windowsマシンをリブートし、デスクトップでネットワーク環境のアイコンをダブルクリックしてSambaサーバを見つけます。

ティップ

Sambaサーバ上でプリンタを使用するには、対応するWindowsバージョンから、標準のプリンタドライバまたはApple-PostScriptプリンタドライバをインストールします。これをLinuxプリンタキュー(Postscriptを入力形式として許容)にリンクするのが最適な方法です。

48.5 最適化

`socket options`は最適化の1つの選択肢であり、ご使用のバージョンのSambaにサンプル設定とともに付属しています。デフォルト設定は、ローカルのイーサネットネットワークを参照します。`socket options`の詳細については、`smb.conf`のマニュアルページの関連セクションと`socket(7)`のマニュアルページを参照してください。詳細については、『Samba HOWTO Collection』の「Samba performance tuning」の章を参照してください。

`/etc/samba/smb.conf`の標準設定は、Sambaチームのデフォルト設定に基づいて、便利な設定ができるよう設計されています。 ただし、ネットワーク設定やワークグループ名の点から、そのまま使える設定をあらかじめ提供するのは不可能です。コマンドサンプル設定`examples/smb.conf.SuSE`には、具体的な必要条件に合わせた調整に役立つ情報が含まれています。

ティップ

Sambaチームが作成した『Samba HOWTO Collection』にはトラブルシューティングについても説明されています。またマニュアルのPart Vでは、手順を追って設定をチェックするためのガイドが用意されています。