SUSE Linux Enterprise Server

11 SP3

www.suse.com

2013 年 6 月 10 日

管理ガイド

管理ガイド

目次

このガイドについて

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

このガイドでは、次の内容が取り上げられています。

サポートと共通タスク
: SUSE Linux Enterpriseには、システムのさまざまな側面をカスタマイズするための幅広いツールが用意されています。この部分では、これらのツールの一部を紹介しています。利用できるさまざまなデバイス技術、可用性の高い構成、および高度な管理機能など、管理者にとって役立つさまざまな機能を紹介します。

システム
: このパートを参照して、OSの詳細を学習してください。SUSE Linux Enterpriseは多数のハードウェアアーキテクチャをサポートしているので、この特長を利用すると、独自のアプリケーションをSUSE Linux Enterpriseでの実行に適応させることができます。また、Linuxシステムの仕組みを理解し、独自のカスタムスクリプトやアプリケーションに応用するために役立つ、ブートローダや、ブート手順についても説明しています。

モバイルコンピュータ
: ラップトップおよびモバイルデバイス(PDA、携帯電話など)/SUSE Linux Enterprise間の通信には、特別な配慮が必要です。電力の節約、および変化するネットワーク環境への各種デバイスの統合に留意してください。また、必要な機能を提供する背景技術を知ることも大事です。

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

トラブルシューティング
: トラブルシューティングでは、詳細情報が必要な場合や特定のタスクを自分のシステムで実行する場合に、ヘルプや追加ドキュメントを見つけられる場所の概要がわかります。また、最も頻繁に発生する問題や厄介事も収録されており、それらの問題を自分で解決する方法を学ぶことができます。

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

ご使用製品の利用可能なマニュアルと最新のドキュメントアップデートの概要については、http://www.suse.com/docを参照してください。

1 利用可能なマニュアル

これらのガイドブックは、HTMLおよびPDFの各バージョンを複数の言語で提供しています。この製品については、次のユーザー用および管理者用マニュアルがあります。

導入ガイド (↑*導入ガイド*)
: 単一または複数のシステムをインストールする方法および展開インフラストラクチャに製品本来の機能を活用する方法を示します。ローカルインストールまたはネットワークインストールサーバの使用から、リモート制御の高度にカスタマイズされた自動リモートインストール技術による大規模展開まで、多様なアプローチから選択できます。

管理ガイド (i ページ)
: 当初のインストールシステムの保守、監視、およびカスタマイズなど、システム管理タスクについて説明します。

Security Guide (セキュリティガイド) (↑*Security Guide (セキュリティガイド)*)
システムセキュリティの基本概念を紹介し、ローカルセキュリティ/ネットワークセキュリティの両方の側面を説明します。製品固有のセキュリティソフトウェア(プログラムが読み込み/書き込み/実行の対象にするファイルをプログラムごとに指定できるAppArmorなど)、およびセキュリティ関係のイベント情報を確実に収集する監査システムを使用する方法を示します。

Security and Hardening Guide (↑*Security and Hardening Guide*)
セキュアSUSE Linux Enterprise Server、およびそのインストールのセキュリティを保護し強化するために必要なその他のポストインストールプロセスのインストールおよび設定について詳しく説明します。セキュリティ関連の選択や決定を行う管理者をサポートします。

System Analysis and Tuning Guide (システム分析およびチューニングガイド) (↑*System Analysis and Tuning Guide (システム分析およびチューニングガイド)*)
問題の検出、解決、および最適化に関する管理者ガイド。ツールの監視によってシステムを検査および最適化する方法およびリソースを効率的に管理する方法を見つけることができます。よくある問題と解決、および追加のヘルプとドキュメントリソースの概要も含まれています。

Virtualization with Xen (↑*Virtualization with Xen*)
ご使用製品の仮想化技術を紹介します。SUSE Linux Enterprise Serverでサポートされているプラットフォームのアプリケーションとインストールタイプに関するさまざまなフィールドの概要、およびインストール手順の簡単な説明について記載しています。

Virtualization with KVM for IBM System z (↑*Virtualization with KVM* for IBM System z)
SUSE Linux Enterprise ServerでのKVM (Kernel-based Virtual Machine)による仮想化のセットアップと管理について紹介します。libvirtまたはQEMUでKVMを管理する方法を学習してください。このガイドには、要件、制限事項、およびサポートの状態に関する詳細な情報も含まれています。

AutoYaST (↑*AutoYaST*)
AutoYaSTは、インストールデータと設定データを含むAutoYaSTプロファイルを使用して、ユーザの介入なしで、自動的に、1つ以上のSUSE Linux Enterpriseシステムをインストールするためのシステムです。マニュアルに従って、自動インストールの基本的な手順(準備、インストール、および設定)を実行できます。

ストレージ管理ガイド (↑*ストレージ管理ガイド*)
SUSE Linux Enterprise Server上のストレージデバイスの管理方法について説明します。

総合的なマニュアルに加えて、クイックスタートガイドも利用できます。

クイックスタートのインストール (↑*クイックスタートのインストール*)
システム要件を一覧し、DVDまたはISOイメージからのSUSE Linux Enterprise Serverのインストールをステップごとに順を追って説明します。

Linux Audit Quick Start (Linux監査クイックスタート)
監査システムを有効にし設定する方法と、主要タスク(監査ルールの設定、レポートの生成、ログファイルの分析など)を実行する方法を簡単に説明します。

AppArmor Quick Start (AppArmorクイックスタート)
Novell® AppArmorの背景をなす主要概念を説明します。

Virtualization with Linux Containers (LXC) (↑*Virtualization with Linux Containers (LXC)*)
LXC(軽量の「仮想化」方式)について簡単に紹介し、LXCホストおよびLXCコンテナの設定方法を説明します。

ほとんどの製品マニュアルのHTMLバージョンは、インストールしたシステム内の`/usr/share/doc/manual`か、ご使用のデスクトップのヘルプセンターで見つけることができます。マニュアルの最新の更新バージョンは、`http://www.suse.com/doc`にあります。ここでは、製品のマニュアルのPDFまたはHTMLバージョンをダウンロードできます。

2 フィードバック

次のフィードバックチャネルがあります。

バグと機能拡張の要求
製品に利用できるサービスとサポートについては、`http://www.suse.com/support/`を参照してください。

製品コンポーネントのバグを報告するには、http://www.suse.com/support/からNovell Customer Centerにログインし、［マイサポート］>［サービス要求］の順に選択します。

ユーザからのコメント
本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインドキュメントの各ページの下にあるユーザコメント機能を使用するか、またはhttp://www.suse.com/doc/feedback.htmlにアクセスして、コメントを入力してください。

メール
この製品のドキュメントについてのフィードバックは、doc-team@suse.de宛のメールでも送信できます。ドキュメントのタイトル、製品のバージョン、およびドキュメントの発行日を明記してください。エラーの報告または機能拡張の提案では、問題について簡潔に説明し、対応するセクション番号とページ(またはURL)をお知らせください。

3 マニュアルの表記規則

本書では、次の書体を使用しています。

- `/etc/passwd`:ディレクトリ名とファイル名
- *`placeholder`*:*`placeholder`*は、実際の値で置き換えられます
- `PATH`:環境変数PATH
- `ls`, `--help`:コマンド、オプション、およびパラメータ
- `user`:ユーザまたはグループ
- <Alt、Alt + F1:押すためのキーまたはキーの組み合わせ、キーはキーボードと同様に、大文字で表示されます
- ［*ファイル*］、［*ファイル*］>［*名前を付けて保存*］:メニュー項目、ボタン

- ►**amd64 em64t ipf:** この説明は、`amd64`、`em64t`、および`ipf`の各アーキテクチャにのみ当てはまります。矢印は、テキストブロックの先頭と終わりを示します。◄

  ►**ipseries zseries:** この説明は、`System z`および`ipseries`にのみ当てはまります。矢印は、テキストブロックの先頭と終わりを示します。◄

- *Dancing Penguins*(「*Penguins*」の章、↑他のマニュアル):他のマニュアル中の章への参照です。

パート I. サポートと共通タスク

1 YaSTオンラインアップデート

Novellは製品に対して、継続的にソフトウェアセキュリティアップデートを提供しています。デフォルトでは、システムを最新の状態に維持するために更新アプレットが使用されます。更新アプレットの詳細については、項 「システムのアップデート」 (第9章 *ソフトウェアをインストールまたは削除する*, ↑*導入ガイド*)を参照してください。この章では、ソフトウェアパッケージを更新する代替ツールとして、YaST オンラインアップデートを紹介します。

SUSE® Linux Enterprise Server用の最新のパッチは、アップデートソフトウェアリポジトリ中に自動的に設定されます。 インストール時に製品を登録した場合、アップデートリポジトリはすでに設定されています。SUSE Linux Enterprise Serverを登録しなかった場合は、YaSTで、［*ソフトウェア*］>［*オンラインアップデートの設定*］の順にクリックし、［*詳細*］>［*Register for Support and Get Update Repository*］の順に選択します。または、信頼できるソースから、手動でアップデートリポジトリを追加することもできます。リポジトリを追加または削除するには、YaSTで、［*ソフトウェア*］>［*Software Repositories*］の順に選択して、リポジトリマネージャを起動します。リポジトリマネージャの詳細については、項 「ソフトウェアリポジトリおよびサービスの操作」 (第9章 *ソフトウェアをインストールまたは削除する*, ↑*導入ガイド*)を参照してください。

注記: アップデートカタログのアクセス時のエラー

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

アップデートカタログへのアクセスが拒否された場合は、Novell Customer Centerにアクセスして登録状態を確認するように推奨する警告メッセージが表示されます。Novell Customer Centerには、http://www.novell.com/center/からアクセスできます。

Novellは、各種の関連性レベルを持つアップデートを提供します。

セキュリティアップデート
: セキュリティアップデートは、重大なセキュリティハザードを修復するので、必ずインストールする必要があります。

推奨アップデート
: コンピュータに損害を与える可能性のある問題を修復します。

オプションアップデート
: セキュリティに関連しない問題を修復したり、拡張機能を提供します。

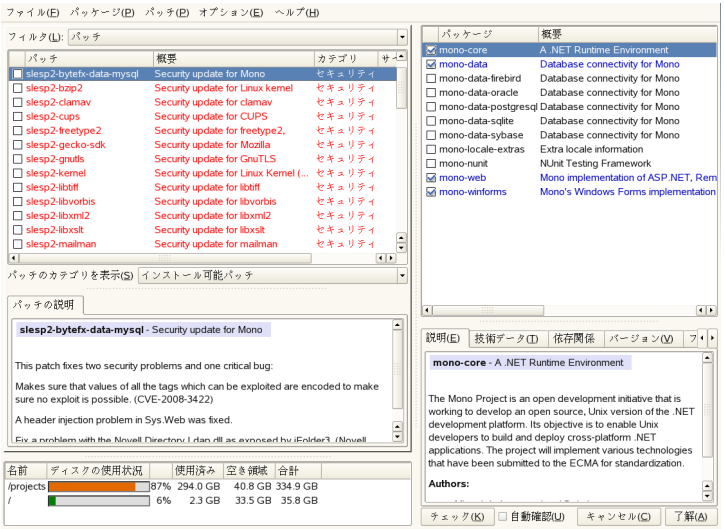
1.1 オンライン更新ダイアログ

YaSTの［*オンライン更新*］ダイアログは、2つのツールキットタイプで使用できます(GNOMEの場合はGTK、KDEの場合はQt)。両方のインタフェースは、ルックアンドフィールで異なりますが、基本的に同じ機能を提供します。以降の項では、各インタフェースについて手短に説明します。このダイアログを開くには、YaSTを起動し、［ソフトウェア］>［*オンライン更新*］の順に選択します。または、`yast2 online_update`で、コマンドラインからオンラインアップデートを開始します。

1.1.1 KDEインタフェース(Qt)

［オンラインアップデート］ウィンドウは、4つのセクションから成り立っています。

図 1.1　YaSTオンラインアップデート—Qtインタフェース



左側の［*概要*］セクションには、SUSE Linux Enterprise Serverの使用可能なパッチが一覧されます。パッチはセキュリティの関連性によってソートされます(`security`、`recommended`、および`optional`)。［*概要*］セクションのビューは、［*パッチのカテゴリを表示*］から、以下のオプションの1つを選択することによって変更できます。

［*Needed Patches*］(デフォルトビュー)
: システムにインストールされたパッケージに適用される、インストールされなかったパッチ。

［*Unneeded Patches*］
: システムにインストールされていないパッケージに適用されるパッチか、または(該当するセキュリティがすでに別のソースで更新されたので)要件がすでに満たされているパッチ。

［すべてのパッチ］
: SUSE Linux Enterprise Serverに使用できるすべてのパッチ。

［*概要*］セクションの各リストエントリは、記号とパッチ名で構成されています。可能な記号とそれらの意味の概要については、Shift + F1を押してください。`Security`パッチおよび`Recommended`パッチで要求されるアクション

は、自動的に設定されます。アクションは、［*自動インストール*］、［*自動更新*］、および［*自動削除*］です。

アップデートリポジトリ以外のリポジトリから最新のパッケージをインストールする場合、そのパッケージのパッチ要件はそのインストールで満たされる場合があります。この場合、パッチ概要の前にチェックマークが表示されます。パッチは、インストール用にマークするまでリストに表示されます。これによってパッチは実際にはインストールされませんが(パッチはすでに最新であるため)、インストール済みとしてパッチをマークします。

［*概要*］セクションでエントリを選択すると、ダイアログの左下隅に短い［*パッチの説明*］が表示されます。左上のセクションには、選択されたパッチに含まれているパッケージが一覧されます(パッチは複数のパッケージから成ることがあります)。右上のセクションでエントリをクリックすると、パッチに含まれている各パッケージの詳細が表示されます。

1.1.2 GNOMEインタフェース(GTK)

［*オンライン更新*］ウィンドウは、4つの主要セクションから成り立っています。

図 1.2 YaSTオンラインアップデート—GTKインタフェース

右上のセクションに、SUSE Linux Enterprise Serverの使用可能な(またはインストール済みの)パッチが一覧されます。パッチをそのセキュリティ関連性に

従ってフィルタするには、ウィンドウの左上のセクションで対応する［*優先度*］エントリをクリックします(`Security`、`Recommended`、`Optional`、または`All patches`)。

すべての使用可能なパッチがすでにインストール済みの場合は、右上のセクションの［*パッケージリスト*］にエントリが表示されません。左下セクションのボックスには、使用可能なパッチとインストール済みパッチの両方の数が表示されます。このビューは、［*利用可能*］と［*インストール済み*］間でトグルできます。

［パッケージリスト］セクションでエントリを選択すると、ダイアログの右下隅にパッチの説明と詳細が表示されます。パッチは複数のパッケージから成ることがあるので、右下のセクションで［*適用項目*］をクリックすると、各パッチにどのパッケージが含まれているか見ることができます。

ウィンドウの下側にあるパッチについて詳細情報を表示するには、パッチのエントリをクリックして行を開きます。ここにはパッチの詳細な説明と使用可能なバージョンが表示されます。オプションのパッチを［*インストールする*］することも選択できます。［セキュリティ］パッチおよび［推奨］パッチはすでにインストール用に事前選択されています。

1.2 パッチのインストール

YaSTオンラインアップデートのダイアログでは、すべての利用可能なパッチを一度にインストールしたり、システムに適用したいパッチを手動で選択したりできます。システムに適用済みのパッチを元に戻すこともできます。

デフォルトでは、お使いのシステムで現在使用できる新しいパッチ(ただし、`optional`以外) はすべて、すでにインストール用にマークされています。［*受諾*］または［*適用*］をクリックすると、これらのパッチが自動的に適用されます。

手順 1.1　YaSTオンラインアップデートによるパッチの適用

1 YaSTを起動して、［ソフトウェア］>［*オンライン更新*］の順に選択します。

2 システムで現在使用可能なすべての新しいパッチ(ただし、optional以外)を自動的に適用するには、［*適用*］または［*受諾*］のクリックで続行して事前選択されているパッチのインストールを開始します。

3 適用したいパッチの選択を変更するには:

3a GTKインタフェースとQtインタフェースが提供するフィルタとビューをそれぞれ使用します。詳細については、1.1.1項「KDEインタフェース(Qt)」 (4 ページ)と1.1.2項 「GNOMEインタフェース (GTK)」 (6 ページ)を参照してください。

3b ニーズと好みに従ってパッチを選択または選択解除するには、各チェックボックスを有効または無効にするか(GNOME)、またはパッチを右クリックしてコンテキストメニューから各アクションを選択します(KDE)。

重要: セキュリティ更新は常時適用

ただし、非常に良い理由がない限り、security関係のパッチは選択解除しないでください。これらのパッチは、重大なセキュリティハザードを修復し、システムの悪用を防ぎます。

3c 大部分のパッチには、複数のパッケージのアップデートが含まれています。単一パッケージに対するアクションを変更する場合は、パッケージビューでパッケージを右クリックしてアクションを選択します(KDE)。

3d 選択を確認し、選択したパッチを適用するには、［*適用*］または［*受諾*］をクリックして続行します。

4 インストールの完了後、［*完了*］をクリックして、YaSTの［*オンライン更新*］を終了します。これで、システムが最新の状態になりました。

ヒント: deltarpmの無効化

デフォルトでは、アップデートは、deltarpmとしてダウンロードされます。deltarpmからのrpmパッケージの再構築は、メモリとCPU時間を消費するので、セットアップまたはハードウェア構成によっては、パフォーマンス上の理由によりdeltarpmの使用を無効にする必要があります。

deltarpmの使用を無効にするには、ファイル/etc/zypp/zypp.confを編集してdownload.use_deltarpmをfalseに設定します。

1.3 自動オンラインアップデート

YaSTでは、毎日、毎週、または毎月のスケジュールで自動更新を設定することもできます。各モジュールを使用するには、［yast2-online-update-configurationをインストールする必要があります。

手順 1.2 *自動オンラインアップデートの設定*

1 インストール後、YaSTを起動し、［ソフトウェア］>［*オンラインアップデートの設定*］の順に選択します。

または、コマンドラインから、yast2 online_update_configurationを使用してモジュールを起動します。

2 ［*自動オンラインアップデート*］を有効にします。

3 ［*毎日*］、［*毎週*］、または［*毎月*］のどれで更新するか選択します。

一部のパッチ(カーネルの更新やライセンス契約を必要とするパッケージなど)は、自動アップデート手順を停止させるユーザ介入を必要とします。

4 更新手順を完全に自動的に進行させたい場合は、［*インタラクティブパッチをスキップする*］を選択します。

重要: パッチのスキップ

介入を必要とするパッケージのスキップを選択した場合は、時折、［*オンライン更新*］を手動で実行して、それらのパッチもインストールしてください。さもないと、重要なパッチをインストールできないことがあります。

5 ライセンス契約を自動的に受諾するには、［*ライセンスに同意する*］を有効にします。

6 アップデートパッケージによって推奨されるすべてのパッケージを自動的にインストールするには、［*推奨されるパッケージを含む*］を有効にします。

7 セキュリティや推奨など、カテゴリ別にパッチをフィルタリングするには、［*カテゴリ別にフィルタ*］を有効にしてリストから適切なカテゴリを追加します。選択したカテゴリのパッチのみがインストールされます。それ以外はスキップされます。

8 入力した設定を確認して、［*OK*］をクリックします。

2 サポート用システム情報の収集

問題が発生した場合は、supportconfigコマンドを使用してシステムレポートを作成できます。このツールは、現在のカーネルのバージョン、ハードウェア、インストールされているパッケージ、パーティション設定などのシステム情報を収集します。このレポートは、Novellテクニカルサービスがお客様の問題を特定したりサポートを提供したりする場合に役立ちます。このコマンドは、デフォルトでインストールされるパッケージsupportutilsによって提供されます。

2.1 概要

Novell Support Link (NSL)はSUSE Linux Enterprise Serverの新しい機能です。システム情報を収集し、収集したデータを別のサーバにアップロードして詳細な分析を行えるツールです。

Novell Support Linkを使用するには、次の2つの方法があります。

1. YaSTサポートモジュールを使用する。

2. コマンドラインユーティリティsupportconfigを使用します。

YaSTサポートモジュールはsupportconfigを呼び出してシステム情報を収集します。

2.2 supportconfigを使用した情報収集

次のセクションではYaSTでコマンドラインを使用するsupportconfigの使い方と、その他のオプションについて説明します。

2.2.1 YaSTの使用

YaSTでシステム情報を収集するには、次の手順に従います。

1. URL http://www.novell.com/center/eserviceを開き、サービス要求番号を作成します。
2. YaSTを起動します。
3. ［サポート］モジュールを開きます。
4. ［*Create report tarball*］をクリックします。
5. ラジオボタンリストからオプションを選択します。この設定をテストしたい場合は、［*Only gather a minimum amount of info*］を使用します。［次へ］で続行します。
6. 連絡先情報を入力します。ステップ 1 (12 ページ)で作成したサービス要求番号を［*Novell社の11桁サービスリクエスト番号*］とラベル付けされたテキストフィールドに入力します。［次へ］で続行します。
7. 情報の収集が開始します。プロセスが完了したら、［次へ］で続行します。
8. データコレクションを確認します。［次へ］で続行します。
9. tarballを保存します。Novellカスタマセンタへアップロードする場合は、［*Upload log files tarball into URL*］が有効になっていることを確認してください。［次へ］で操作を終了します。

2.2.2 supportconfigの直接使用

コマンドラインからsupportconfigを使用する場合は、次の手順に従います。

1 シェルを開きrootになります。

2 オプションなしでsupportconfigを実行します。デフォルトのシステム情報が収集されます。

3 ツールが操作を完了するまで待機します。

4 デフォルトのアーカイブ場所は、/var/log のファイル名形式 nts_*HOST_DATE_TIME*.tbzです。

2.2.3 共通のSupportconfigオプション

supportconfigユーティリティは、通常、オプションなしで呼び出されます。supportconfig –helpで、すべてのオプションを一覧表示するか、マニュアルページを参照してください。よくある使用事例については、以下のリストで簡単に説明します。

- 収集される情報のサイズを削減するには、最小オプション(–m)を使用します。

  ```
  supportconfig –m
  ```

- 出力に追加連絡先情報を含めます(1行で)。

  ```
  supportconfig –E tux@example.org –N "Tux Penguin" –O "Penguin Inc." ...
  ```

- トラブルシューティング時には、現在作業中の問題のある領域についてのみ、情報を収集したい場合があります。たとえば、LVMに問題があり、最近デフォルトのsupportconfig出力に問題が見つかった場合です。変更を終えたら、現在のLVMの情報を収集する必要があります。supportconfigとLVMの最低限の情報のみを収集するには以下を使用します。

  ```
  supportconfig –i LVM
  ```

  完全な機能リストを見るには、次を実行します。

```
supportconfig -F
```

逆の操作が必要な場合は、-xオプションで領域を除外します。-iおよび-xの両方のオプションを組み合わせることができます。

- すでに実行されているログファイルを収集します。これは、大規模なログを行う環境や、syslogが再起動後にログを実行していてカーネルクラッシュが発生した場合に特に有効です。

```
supportconfig -l
```

2.3 Novellへの情報の送信

システム情報をNovellへ送信するには、YaSTサポートモジュールまたはsupportconfigコマンドラインユーティリティを使用できます。サーバに問題がありNovellのサポートを希望する場合、サービス要求を開いてサーバ情報をNovellに送信する必要があります。YaSTとコマンドラインの両方の方法について説明されています。

注記: プライバシーポリシー

Novellは、システムレポートを機密データとして扱います。詳細はhttp://www.novell.com/company/legal/privacy/のプライバシーポリシーを参照してください。

手順 2.1 *YaSTを使用したNovellへの情報の送信*

1. URL http://www.novell.com/center/eserviceを開き、サービス要求番号を作成します。
2. 11桁のサービス要求番号を記入します。次の例ではサービス要求番号が12345678901であると想定しています。
3. YaSTサポートモジュールウィンドウで、［*レポートtarアーカイブを作成*］をクリックします。
4. ［*Use custom*］ラジオボタンを選択します。［*次へ*］で続行します。
5. 連絡先情報を入力し、［*Novell 社の11桁サービスリクエスト番号*］を入力して、Novelllのアップロードターゲットの URLを含めます。

- 安全なアップロードターゲットには、https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}を使用します。
- 通常のFTPアップロードターゲットには、ftp://ftp.novell.com/incoming (米国のお客様)またはftp://support-ftp.suse.com/in (EMEA、ヨーロッパ、中東、およびアフリカ)を使用します。

［次へ］で続行します。情報の収集が開始します。プロセスが完了したら、［次へ］で続行します。

6 データのコレクションを確認し、Novellにアップロードされたtarballから除外したいファイルがあれば［データから*削除*］を使用して削除します。［次へ］で続行します。

7 デフォルトではtarballのコピーが/rootに保存されます。前述したNovellアップロードターゲットの1つを使用していることを確認し、［*URL にログファイルの tar アーカイブをアップロード*］が有効になっていることを確認してください。［次へ］をクリックして完了します。

8 ［完了］をクリックします。

手順 2.2 *supportconfig を使用した Novell への情報の送信*

1 URL http://www.novell.com/center/eserviceを開き、サービス要求番号を作成します。

2 11桁のサービス要求番号を記入します。次の例ではサービス要求番号が12345678901であると想定しています。

3 インターネット接続のあるサーバの場合

3a デフォルトのアップロードターゲットを使用するには、次を実行します。

```
supportconfig -ur 12345678901
```

3b 安全なアップロードターゲットには、次を1行で使用します。

```
supportconfig -r 12345678901 -U
'https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}'
```

4 インターネット接続のないサーバの場合

4a 次を実行します。

```
supportconfig -r 12345678901
```

4b tarball(/var/log/nts_SR12345678901*tbz)を弊社FTPサーバ(米国のお客様はftp://ftp.novell.com/incomingを使用、ヨーロッパ、中東、アフリカのお客様はftp://support-ftp.suse.com/inを使用)に手動でアップロードします。

4c サービス要求URL http://www.novell.com/center/eserviceを使用してtarballをサービス要求に添付することもできます。

5 FTPサーバの着信ディレクトリにtarballが届くと、お客様のサービス要求に自動的に添付されます。

2.4 詳細情報

システム情報の収集の詳細については、次のドキュメントを参照してください。

- man supportconfig—supportconfigのマニュアルページ
- man supportconfig.conf—supportconfig設定ファイルのマニュアルページ
- http://www.novell.com/communities/print/node/4097—「A Basic Server Health Check with Supportconfig」
- http://www.novell.com/communities/print/node/4827—「Create Your Own Supportconfig Plugin」
- http://www.novell.com/communities/print/node/4800—「Creating a Central Supportconfig Repository」

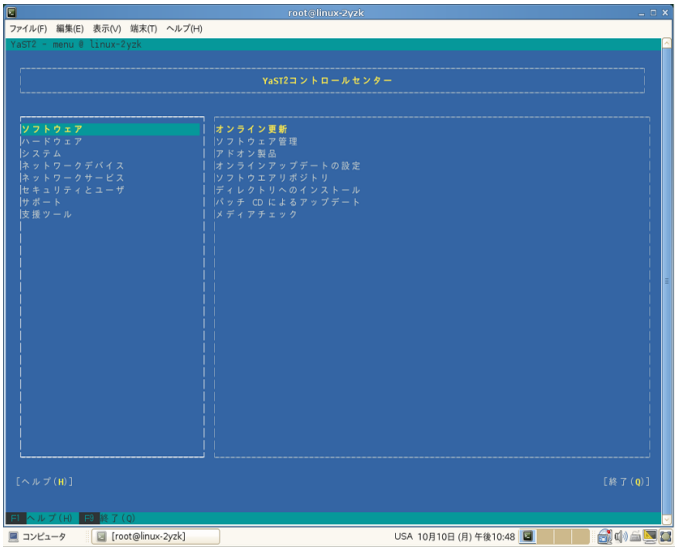
3

テキストモードのYaST

このセクションは、システムでXサーバを実行せずに、テキストベースのインストールツールを使用しているシステム管理者や専門家の方を対象にしています。ここでは、YaSTをテキストモードで開始、操作するための、基本的な情報を説明しています。

テキストモードのYaSTは、ncursesライブラリを使用して、使いやすい擬似グラフィカルユーザインタフェースを提供します。ncursesライブラリは、デフォルトでインストールされています。YaSTを実行するためのターミナルエミュレータの最小サポートサイズは、80x25文字です。

図 3.1　テキストモードのYaSTのメインウィンドウ



YaSTをテキストモードで起動すると、YaSTコントロールセンターが表示されます(図3.1を参照してください)。このメインウィンドウは、以下の3つの主要領域で構成されています。左側のフレームのカテゴリには、さまざまなモジュールがあります。このフレームはYaSTが起動したときにアクティブになり、白い太線でマークされます。アクティブなカテゴリが選択されています。右側のフレームには、アクティブなカテゴリで使用できるモジュールの概要が表示されます。下方のフレームには、［ヘルプ］および［終了］用ボタンがあります。

YaSTコントロールセンターを起動すると、カテゴリ［*Software*］が自動的に選択されます。カテゴリを変更するには、↑と↑を使用します。カテゴリからモジュールを選択するには、→で右側のフレームをアクティブにして、↑と↓を使用してモジュールを選択します。矢印キーを押したままにして、使用可能なモジュールのリストをスクロールします。選択したモジュールがハイライトされます。<Enter>を押してアクティブなモジュールを起動します。

モジュールのさまざまなボタンまたは選択フィールドで、文字がハイライト表示されています(デフォルトは黄色)。そのままTabキーでナビゲートするする代わりに、直接ボタンを選択するには、Alt＋highlighted_letterを使用します。Alt＋Qを押すか、または［終了］を選択してEnterを押して、YaSTコントロールセンターを終了します。

ヒント: YaSTダイアログウィンドウの更新

ウィンドウのサイズを変更した場合など、YaSTのダイアログウィンドウが破損または変形した場合は、Ctrl + Lを押すとコンテンツを更新し復元できます。

3.1 モジュールでのナビゲーション

以降のYaSTモジュール内のコントロール要素の説明では、ファンクションキーとAltキーの組み合わせがすべて機能し、別のグローバル機能を割り当てられていないことを前提としています。可能性のある例外事項については、3.2項 「キーの組み合わせの制約」 (21 ページ)を参照してください。

ボタンおよび選択リスト間のナビゲーター
: 選択リストを含むボタンおよびフレーム間でナビゲートするには、Tabキーを使用します。逆の順序でナビゲートするには、Alt+TabまたはShift+Tabの組み合わせを使用します。

選択リストでのナビゲーター
: 選択リストを含むアクティブフレーム内の個々の要素間でナビゲートするには、矢印キー(↑と↓)を使用します。フレーム内の個別エントリがその幅を超える場合は、Shift+→またはShift+←を使用して、右または左にスクロールします。代わりにCtrl+EまたはCtrl+Aを使用することもできます。この組み合わせは、コントロールセンターの場合のように、→または←を使用すると、アクティブフレームまたは現在の選択リストが変更されてしまう場合に使用できます。

ボタン、ラジオボタン、およびチェックボックス
: [] が付いているボタン(チェックボックス)または()が付いているボタン(ラジオボタン)を選択するには、Spaceキーまたは<Enter>キーを押します。または、Alt + highlighted_letterでラジオボタンおよびチェックボックスを直接選択することもできます。この場合、<Enter>キーによる確認は不要です。Tabキーでアイテムにナビゲートする場合は、<Enter>キーを押して、選択したアクションを実行するか、対応するメニューアイテムをアクティブにします。

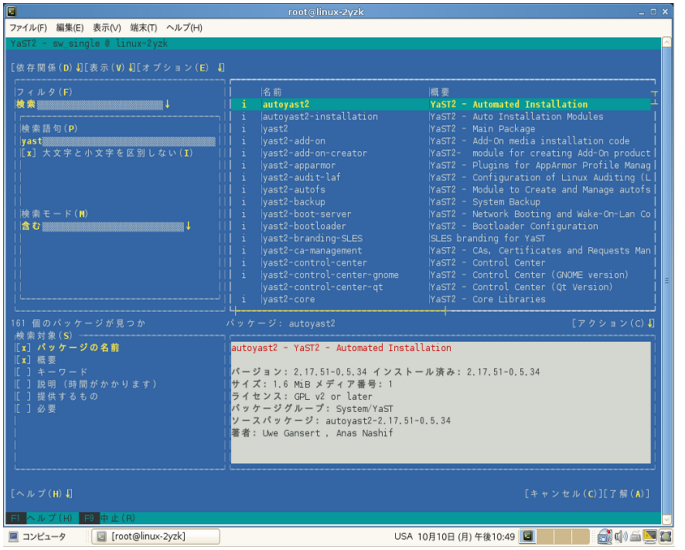
ファンクションキー

FキーのF1からF12を使用すると、さまざまなボタンの機能をすばやく利用できます。使用可能なFキーのショートカットは、YaST画面の一番下の行に表示されます。どのファンクションキーが実際にどのボタンにマップされているかは、アクティブになっているYaSTモジュールによります。提供されるボタン(［詳細］、［情報］、［追加］、［削除］など)は、モジュールごとに異なるからです。F10は、［*受諾*］、［*OK*］、［*次へ*］、および［*完了*］の代わりに使用します。F1を押して、YaSTヘルプにアクセスします。

ncursesモードのナビゲーションツリーの使用

一部のYaSTモジュールでは、ウィンドウの左部分にあるナビゲーションツリーを使用して、設定ダイアログを選択します。矢印キー(↑と↓)を使用して、ツリー内を移動します。Spaceを使用して、ツリー項目を開閉します。ncursesモードでは、ナビゲーションツリーでの選択後、選択したダイアログを表示するには<Enter>を押す必要があります。これは意図的な動作であり、これによって、ナビゲーションツリーのブラウズ時に時間のかかる再表示を節約できます。

図 3.2　ソフトウェアインストールモジュール



3.2 キーの組み合わせの制約

ウィンドウマネージャがグローバルな<Alt>キーの組み合わせを使用していると、YaSTでの<Alt>キーの組み合わせが機能しない場合があります。<Shift>や<Alt>などのキーは、端末の設定に専有されている場合もあります。

<Alt>キーをEscキーの代用とする
: <Alt>ショートカットは<Alt>の代わりに<Esc>キーでも実行できます。たとえば、Esc – Hは、Alt + Hの代わりとなります。(まず<Esc>を押して、次にHを押します)

Ctrl + FとCtrl + Bによる前後のナビゲーション
: <Alt>と<Shift>の組み合わせがウィンドウマネージャまたは端末に専有されている場合は、Ctrl + F(進む)とCtrl + B(戻る)を代わりに使用できます。

ファンクションキーの制約
: Fキーは、各種機能にも使用されます。一部のファンクションキーは、端末に専有され、YaSTで使用できない場合があります。ただし、<Alt>キーのキーの組み合わせとファンクションキーは、ピュアテキストコンソールでは常に完全に使用できます。

3.3 YaSTコマンドラインオプション

テキストモードのインターフェースのほか、YaSTには、シンプルなコマンドラインインターフェースがあります。YaSTコマンドラインオプションのリストを表示するには、次のように入力します。

```
yast -h
```

3.3.1 個別モジュールの起動

時間節約のため、個別のYaSTモジュールを直接起動できます。モジュールを起動するには、次のように入力します。

```
yast <module_name>
```

「yast -l」または「yast --list」と入力して、システムで使用可能になっているすべてのモジュールのリストを表示します。たとえば、「yast lan」と入力して、ネットワークモジュールを起動します。

3.3.2 コマンドラインからのパッケージのインストール

パッケージ名が既知であり、パッケージが有効なインストールリポジトリに用意されている場合は、コマンドラインオプション-iを使用してパッケージをインストールできます。

```
yast -i <package_name>
```

または

```
yast --install <package_name>
```

*package_name*は、1つの短いパッケージ名にするか(たとえば、依存性チェック付きでインストールされるgvim)、またはrpmパッケージへの完全なパスにすることができます(依存性チェックなしでインストールされる)。

YaSTから提供される機能を超える機能を持つコマンドラインベースのソフトウェア管理ユーティリティを必要とする場合は、zypperの使用をご検討ください。この新しいユーティリティは、YaSTパッケージマネージャの基礎でもある同じソフトウェア管理ライブラリを使用します。zypperの基本的使用法については、6.1項 「Zypperの使用」 (55 ページ)で説明されています。

3.3.3 YaSTモジュールのコマンドラインパラメータ

スクリプトでYaST機能を使用するため、YaSTでは、個々のモジュールのコマンドラインサポートを用意しています。ただし、すべてのモジュールにコマンドラインサポートがあるわけではありません。モジュールで利用できるオプションを表示するには、次のように入力します。

```
yast <module_name> help
```

モジュールにコマンドラインサポートがない場合、モジュールはテキストモードで起動され、次のメッセージが表示されます。

```
This YaST module does not support the command line interface.
```

4 Snapperによるスナップショットとロールバック

Linuxでファイルシステムのスナップショットを作成し、ロールバックできるようにすることは、過去に要望の多かった機能です。Snapperを、Btrfsファイルシステムまたはシンプロビジョンの LVMボリュームと併用することによって対応できます。

Btrfsは、Linux用の新しい書き込み時コピー方式のファイルシステムで、サブボリューム(各物理パーティション内の1つまたは複数の個別にマウント可能なファイルシステム)のファイルシステムスナップショット(特定時点におけるサブボリュームの状態のコピー)をサポートします。Snapperを使用してこれらのスナップショットを管理できます。Snapperには、コマンドラインおよびYaSTインタフェースがあります。

デフォルトで、SUSE Linux Enterprise ServerのSnapperおよびBtrfsは、YaSTおよびzypperによるシステム変更を「元に戻すツール」として設定されます。YaSTモジュールまたはzypperの実行前と実行後にスナップショットが作成されます。Snapperを使用して、2つのスナップショットを比較し、その変更を元に戻すことができます。また、このツールは、システムのサブボリュームに対して毎時のスナップショットを作成することにより、システムのバックアップとしても機能します。

4.1 要件

SUSE Linux Enterprise ServerではBtrfsがスナップショットに対応した唯一のファイルシステムであるため、「スナップショット」を利用したいすべてのパーティションまたはサブボリュームで、このファイルシステムが必要です。

4.1.1 スナップショットとディスク容量

スナップショットを作成すると、スナップショットとスナップショット元のファイルは、いずれもファイルシステム内の同じブロックを指します。そのため、最初は、スナップショットが余分にディスク容量を占めることはありません。元のファイルシステムのデータが変更されると、変更されたデータブロックがコピーされ、古いデータブロックはスナップショットのように保持されます。このため、スナップショットは、変更されたデータと同じ容量を占めます。こうして、時間が経過するにつれて、スナップショットの領域は大きくなっていきます。その結果、スナップショットを含むBtrfsファイルシステムからファイルを削除しても、ディスクの空き容量が*増えない*ことがあります。

注記: スナップショットの場所

スナップショットは常に、「スナップショット作成元」と同じパーティションまたはサブボリュームに保存されます。別のパーティションまたはサブボリュームにスナップショットを保存することはできません。

その結果、スナップショットを含むパーティションは、「通常の」パーティションよりも大きくする必要があります。具体的な容量は、保持するスナップショット数やデータの変更頻度によって異なります。一般的には、通常のファイルシステムの2倍程度を検討してください。

ヒント: 容量を空ける/ディスクの使用率

スナップショットを含むBtrfsパーティションの容量を空けるには、ファイルではなく、不要なスナップショットを削除する必要があります。古いスナップショットは、最近のスナップショットよりも多くの領域を使用します。

Btrfsファイルシステムではdfが正しいディスクの使用率を表示しないため、コマンドbtrfs filesystem df *MOUNT_POINT*を使用する必要があります。現時点では、Btrfsツールで、スナップショットが使用するディスク容量を表示できません。

あるサービスパックから別のサービスパックにアップグレードすると、多くのデータが変更される(パッケージのアップデート)ので、スナップショットにより、システムのサブボリュームで多くのディスク容量が使用されま

す。これらのスナップショットが不要になった場合は、手動で削除することをお勧めします。

Snapperを使用して、ext3またはXFSでフォーマットされたシンプロビジョンのLVMボリュームでもスナップショットを作成および管理できます(4.6項「シンプロビジョンLVMボリュームでのSnapper使用」 (46 ページ)を参照)。

4.2 Snapperによるシステム変更の取り消し

SUSE Linux Enterprise ServerのSnapperは、zypperやYaSTで行った変更を取り消すことができるツールとしてあらかじめ設定されています。 このために、Snapperは、zypperおよびYaSTの実行前後に1対のスナップショットを作成します。また、Snapperを使用して、誤って削除または変更したシステムファイルを復元することもできます。このために、毎時のバックアップが作成されます。

上記の自動スナップショットは、デフォルトでルートパーティションとそのサブボリュームに対して設定されます。カスタム設定を作成すれば、/homeなど、他のパーティションに対してスナップショット機能を利用できます。

4.2.1 YaSTおよびzypperによる変更の取り消し

インストール時にルートパーティションをBtrfsで設定すると、Snapper(YaSTまたはzypperによる変更のロールバックがあらかじめ設定されている)が自動的にインストールされます。YaSTモジュールまたはzypperトランザクションを開始するたびに、2つのスナップショットが作成されます。モジュール開始前のファイルシステムの状態をキャプチャした「事前スナップショット」と、モジュール完了後の状態をキャプチャした「事後スナップショット」です。

YaSTのSnapperモジュールまたはsnapperコマンドラインツールを使用して、「事前スナップショット」からファイルを復元し、YaST/zypperによる変更を元に戻すことができます。また、2つのスナップショットを比較して、どの

ファイルが変更されているか調べることができます。2つのバージョンのファイルの違いを表示することもできます(diff)。

Linuxはマルチタスクシステムなので、事前スナップショットと事後スナップショットの間に、YaSTまたはzypper以外のプロセスがデータを変更してしまう場合があります。この場合、事前スナップショットに戻してしまうと、他のプロセスによる変更も取り消されてしまいます。多くの場合、これは望ましくありません。このため、ロールバックを開始する前に、2つのスナップショットの間の変更点をよく確認してください。他のプロセスによる変更を維持したい場合は、ロールバックするファイルを選択してください。

重要: 制限

Snapperのロールバック機能を使用する前に、Snapperの制限について理解しておいてください。詳細については、4.4項 「制限」 (43 ページ)を参照してください。

注記: スナップショットの保存期間

デフォルトで、YaSTおよびzypperのスナップショットは、新しいものから100個が保持されます。この数を超えると、もっとも古いスナップショットが削除されます。

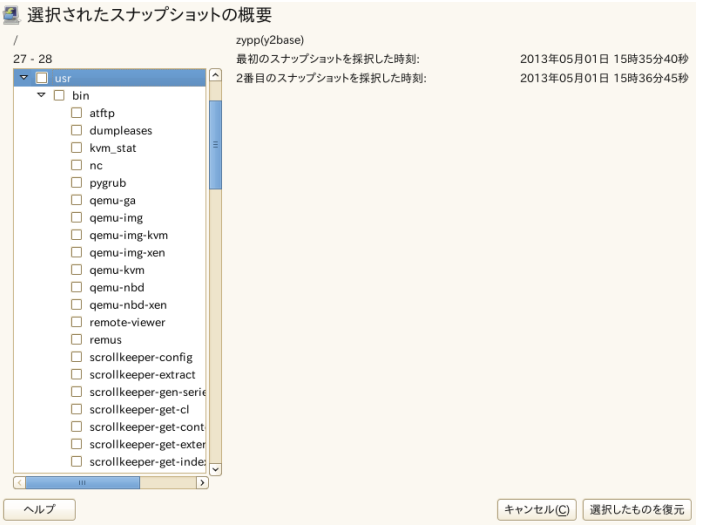
手順 4.1　YaSTの［Snapper］モジュールによる変更の取り消し

1. YaSTの［*その他*］セクションにある［*Snapper*］モジュールを起動するか、`yast2 snapper`と入力します。

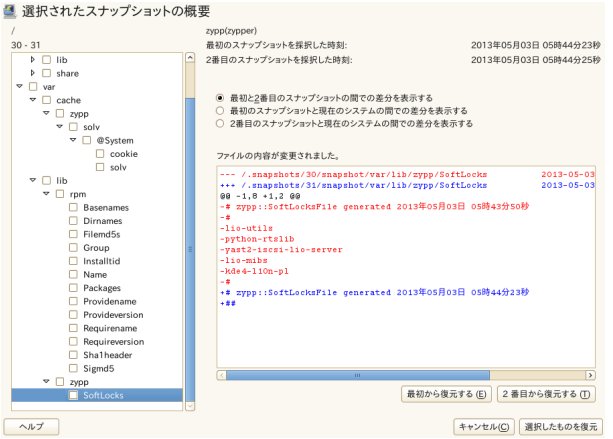
2. ［*現在の設定*］が［*root*］になっていることを確認します。 独自のSnapper設定を手動で追加していない限り、常にそのようになっています。

3. リストから事前スナップショットと事後スナップショットのペアを選択します。YaSTのスナップショットペアもzypperのスナップショットペアも、種類は［*事前および事後*］です。YaSTのスナップショットの場合は[説明]に「`yast モジュール名`」 [] と表示され、zypperのスナップショットの場合は「`zypp (zypper)`」と表示されます。

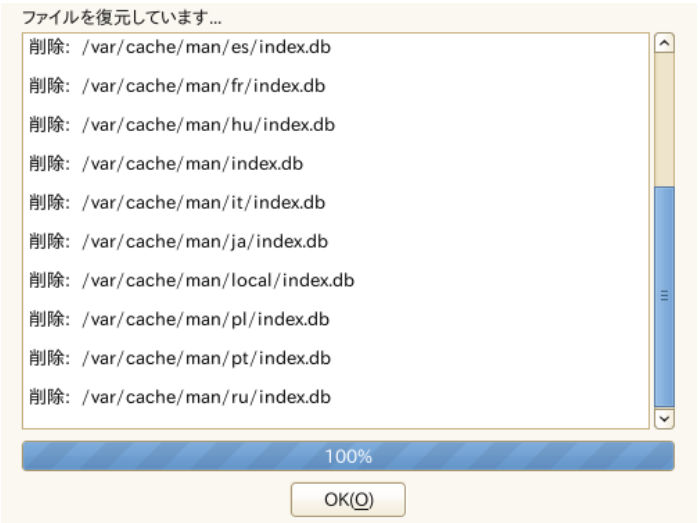
4 ［変更点の表示］をクリックすると、2つのスナップショット間のファイルの差異がリスト表示されます。下の図は、ユーザtesterを追加した後に変更されたファイルのリストです。



5 ファイルのリストを確認します。事前と事後のファイル間の「「差異」」を表示するには、リストからファイルを選択します。下の図は、ユーザ `tester`を追加した後の`/etc/passwd`の変更を示しています。



6 ファイルのセットを復元するには、該当するチェックボックスをオンにして、ファイルまたはディレクトリを選択します。［*選択したものを復元*］をクリックし、［*はい*］をクリックして操作を確認します。



単一のファイルを復元する場合は、ファイル名をクリックして差分を表示します。［*最初から復元する*］をクリックし、［*はい*］をクリックして操作を確認します。

手順 4.2　snapperコマンドによる変更の取り消し

1 `snapper list -t pre-post`を実行すると、YaSTおよびzypperのスナップショットリストが表示されます。YaSTのスナップショットの場合は[説明]に「`yast` *モジュール名*」［］と表示され、zypperのスナップショットの場合は「`zypp (zypper)`」と表示されます。

```
~ # snapper list -t pre-post
     Pre # | Post # | Pre Date                | Post Date               | Description

------+--------+-------------------------+-------------------------+----------------------+

     4    | 5     | Tue Jan 10 14:39:14 2012 | Tue Jan 10 14:39:33 2012 | yast system_settings

     65    | 66     | Thu Jan 12 17:18:10 2012 | Thu Jan 12 17:18:23 2012 | zypp(zypper)
     68    | 69     | Thu Jan 12 17:25:46 2012 | Thu Jan 12 17:27:09 2012 | zypp(zypper)
     73    | 74    | Thu Jan 12 17:32:55 2012 | Thu Jan 12 17:33:13 2012 | yast system_settings

     75    | 76     | Thu Jan 12 17:33:56 2012 | Thu Jan 12 17:34:42 2012 | yast users
     77    | 92     | Thu Jan 12 17:38:36 2012 | Thu Jan 12 23:13:13 2012 | yast snapper
     83    | 84     | Thu Jan 12 22:10:33 2012 | Thu Jan 12 22:10:39 2012 | zypp(zypper)
     85    | 86     | Thu Jan 12 22:16:58 2012 | Thu Jan 12 22:17:09 2012 | zypp(zypper)
     88    | 89     | Thu Jan 12 23:10:42 2012 | Thu Jan 12 23:10:46 2012 | zypp(zypper)
     90    | 91     | Thu Jan 12 23:11:40 2012 | Thu Jan 12 23:11:42 2012 | zypp(zypper)
     108   | 109    | Fri Jan 13 13:01:06 2012 | Fri Jan 13 13:01:10 2012 | zypp(zypper)
```

2 スナップショットのペア間で変更されたファイルのリストを取得するには、以下を実行します。`snapper status` *PREPOST*. 内容が変更されたファイルには［*c*］のマーク、追加されたファイルには［+］のマーク、削除されたファイルには［-］のマークが付いています。 下の例は、パッケージ`ncftp`のインストール前後のスナップショットペアです。

```
~ # snapper status 108..109
     +... /usr/bin/ncftp
     +... /usr/bin/ncftpbatch
     +... /usr/bin/ncftpget
     +... /usr/bin/ncftpls
     [...]
     +... /usr/share/man/man1/ncftpspooler.1.gz
     c... /var/cache/zypp/solv/@System/cookie
     c... /var/cache/zypp/solv/@System/solv
     c... /var/lib/rpm/Basenames
     c... /var/lib/rpm/Dirnames
     c... /var/lib/rpm/Filemd5s
     c... /var/lib/rpm/Group
     c... /var/lib/rpm/Installtid
```

```
c... /var/lib/rpm/Name
c... /var/lib/rpm/Packages
c... /var/lib/rpm/Providename
c... /var/lib/rpm/Provideversion
c... /var/lib/rpm/Requirename
c... /var/lib/rpm/Requireversion
c... /var/lib/rpm/Sha1header
c... /var/lib/rpm/Sigmd5
c... /var/lib/zypp/SoftLocks
```

3 特定のファイルの差異を表示するには、以下を実行します。snapper diff *PRE..POST ファイル名*ファイル名を指定しない場合は、すべてのファイルの差異が表示されます。

```
~ # snapper diff 108..109 /var/lib/zypp/SoftLocks
     --- /.snapshots/108/snapshot/var/lib/zypp/SoftLocks 2012-01-12
23:15:22.408009164 +0100
     +++ /.snapshots/109/snapshot/var/lib/zypp/SoftLocks 2012-01-13
13:01:08.724009131 +0100
     @@ -1,4 +1,2 @@
     -# zypp::SoftLocksFile generated Thu Jan 12 23:10:46 2012
     -#
     -ncftp
     -#
     +# zypp::SoftLocksFile generated Fri Jan 13 13:01:08 2012
     +##
```

4 1つまたは複数のファイルを復元するには、以下を実行します。snapper -v undochange *PRE..POST ファイル名* ファイル名を指定しない場合は、変更されたすべてのファイルが復元されます。

```
~ # snapper -v undochange 108..109
     create:0 modify:16 delete:21
     undoing change...
     deleting /usr/share/man/man1/ncftpspooler.1.gz
     deleting /usr/share/man/man1/ncftpput.1.gz
     [...]
     deleting /usr/bin/ncftpls
     deleting /usr/bin/ncftpget
     deleting /usr/bin/ncftpbatch
     deleting /usr/bin/ncftp
     modifying /var/cache/zypp/solv/@System/cookie
     modifying /var/cache/zypp/solv/@System/solv
     modifying /var/lib/rpm/Basenames
     modifying /var/lib/rpm/Dirnames
     modifying /var/lib/rpm/Filemd5s
     modifying /var/lib/rpm/Group
     modifying /var/lib/rpm/Installtid
     modifying /var/lib/rpm/Name
     modifying /var/lib/rpm/Packages
```

```
modifying /var/lib/rpm/Providename
modifying /var/lib/rpm/Provideversion
modifying /var/lib/rpm/Requirename
modifying /var/lib/rpm/Requireversion
modifying /var/lib/rpm/Sha1header
modifying /var/lib/rpm/Sigmd5
modifying /var/lib/zypp/SoftLocks
undoing change done
```

4.2.2 Snapperによる定期バックアップからのファイル復元

YaSTおよびzypperのスナップショット以外に、Snapperは、システムパーティション(/)の毎時スナップショットを作成します。このバックアップ用スナップショットを使用して、誤って削除または変更したファイルを復元できます。Snapperの差分抽出機能を使用して、ある時点でどのファイルが変更されたのか調べることもできます。

毎時バックアップのスナップショットは、種類がSingleで、timelineという説明が付いています。これらのスナップショットからファイルを復元したい場合は、手順4.1「YaSTの［*Snapper*］モジュールによる変更の取り消し」 (28 ページ)または手順4.2「snapperコマンドによる変更の取り消し」 (31 ページ)の手順に従ってください。

注記: スナップショットの保存期間

デフォルトで、最近10日間、10カ月間、10年間の最初のスナップショットが保持されます。詳細については、例4.1「タイムラインの設定例」 (36 ページ)を参照してください。

4.2.3 Snapper設定の作成と変更

Snapperの動作は、各パーティションまたはBtrfsサブボリュームに固有の設定ファイルで定義できます。これらの設定ファイルは、/etc/snapper/configs/に保存されます。/ディレクトリに対してSnapperでインストールされるデフォルトの設定ファイルがrootです。このファイルは、YaSTとzypperのスナップショットを作成し管理するほか、/に対する毎時のバックアップスナップショットも作成および管理します。

Btrfsでフォーマットされたその他のパーティションやBtrfsパーティション上の既存のサブボリュームに対して、独自の設定ファイルを作成できます。以下の例では、/srv/wwwにマウントされたBtrfsフォーマットのパーティションに保存されたWebサーバデータをバックアップするSnapper設定を作成します。

snapper自体またはYaSTの［*Snapper*］モジュールを使用して、これらのスナップショットからファイルを復元できます。YaSTの場合は［*現在の設定*］を選択する必要があります。snapperの場合は、グローバルスイッチ-cを使用して設定を指定する必要があります(例:snapper -c myconfig list)。

新しいSnapper設定を作成するには、snapper create-configを実行します。

```
snapper -c www-data❶ create-config
   /srv/www❷
```

❶ 設定ファイルの名前。
❷ スナップショットを作成するパーティションまたはBtrfsサブボリュームのマウントポイント。

このコマンドにより、新しい設定ファイル/etc/snapper/config-templates/www-dataが作成され、/etc/snapper/config-templates/defaultから取得されたデフォルト値が使用されます。

ヒント: 設定のデフォルト

新しい設定ファイルのデフォルト値は/etc/snapper/config-templates/defaultから取得されます。独自のデフォルトセットを使用する場合は、同じディレクトリ内にこのファイルのコピーを作成し、必要に応じて調整してください。作成したファイルを使用するには、create-configコマンドで-tオプションを指定します。

```
snapper -c www-data create-config -t my_defaults /srv/www
```

4.2.3.1 設定ファイルの調整

設定ファイルを調整するには、エディタで変更します。設定ファイルには、キー=*値*の形式でキーと値のペアが含まれています。 変更できるのは*値*だけです。

SUBVOLUME
スナップショットを作成するパーティションまたはサブボリュームのマウントポイント。変更しません。

FSTYPE
パーティションのファイルシステムタイプ。変更しません。

NUMBER_CLEANUP
合計スナップショット数がNUMBER_LIMITで指定した数を超え、かつNUMBER_MIN_AGEで指定した保存期間を超えた場合に、古いスナップショットを自動的に削除するかどうか定義します。有効な値:yes(はい)、no(いいえ)

注記: 制限と保存期間

NUMBER_LIMITとNUMBER_MIN_AGEは常に両方が評価されます。スナップショットが削除されるのは、*両方*の条件を満たしている場合のみです。保存期間に関係なく一定数のスナップショットを常に保持したい場合は、NUMBER_MIN_AGEを0に設定します。 一方、一定の保存期間を超えたスナップショットをすべて削除したい場合は、NUMBER_LIMITを0に設定します。

NUMBER_LIMIT
NUMBER_CLEANUPがyesに設定されている場合に、保持するスナップショットの数を定義します。

NUMBER_MIN_AGE
スナップショットが自動削除の対象となるまでの最短期間を秒単位で定義します。

TIMELINE_CREATE
yesに設定されている場合、毎時のスナップショットが作成されます。現時点では、これがスナップショットを自動的に作成する唯一の方法なので、yesに設定することを強くお勧めします。有効な値:yes(はい)、no(いいえ)

TIMELINE_CLEANUP
スナップショット数が*TIMELINE_LIMIT_**オプションで指定した数を超え、かつTIMELINE_MIN_AGEで指定した保存期間を超えた場合に、古い

スナップショットを自動的に削除するかどうか定義します。 有効な値:yes(はい)、no(いいえ)

TIMELINE_MIN_AGE
スナップショットが自動削除の対象となるまでの最短期間を秒単位で定義します。

TIMELINE_LIMIT_HOURLY、TIMELINE_LIMIT_DAILY、TIMELINE_LIMIT_MONTHLY、TIMELINE_LIMIT_YEARLY
1時間、1日、1カ月間、1年間に保持するスナップショット数です。

*例 **4.1** タイムラインの設定例*

```
TIMELINE_CREATE="yes"
        TIMELINE_CLEANUP="yes"
        TIMELINE_MIN_AGE="1800"
        TIMELINE_LIMIT_HOURLY="10"
        TIMELINE_LIMIT_DAILY="10"
        TIMELINE_LIMIT_MONTHLY="10"
        TIMELINE_LIMIT_YEARLY="10"
```

この設定例では、毎時スナップショットが自動的に削除されます。TIMELINE_MIN_AGEとTIMELINE_LIMIT_*は常に両方が評価されます。この例では、スナップショットが削除対象となるまでの最短期間が30分(180秒)に設定されています。毎時のスナップショットを作成するので、最新のスナップショットだけが保持されることになります。TIMELINE_LIMIT_DAILYをゼロ以外に設定すると、1日の最初のスナップショットが保持されることになります。

保持されるスナップショット

- 1時間ごと:最新の10個のスナップショットが保持されます。
- 1日ごと:それぞれの日の最初のスナップショットが、直近の10日分保持されます。
- 1カ月ごと:それぞれの月の最後の日に作成された最初のスナップショットが、直近の10カ月分保持されます。
- 1年ごと:それぞれの年の最後の日に作成された最初のスナップショットが、直近の10年分保持されます。

4.2.3.2 通常ユーザとしてSnapperを使用する

デフォルトでは、rootしかSnapperを使用できません。しかし、以下のような場合、特定のグループまたはユーザがスナップショットを作成したり、スナップショットを使って変更を取り消したりできる必要があります。

- Webサイトの管理者が/srv/wwwのスナップショットを作成する
- データベース管理者がデータベースのスナップショットを作成する
- ユーザが自分のホームディレクトリのスナップショットを作成する

このような場合、ユーザやグループにパーミッションを与えるSnapper設定を作成できます。この設定変更だけでなく、指定されたユーザが、対応する.snapshotsディレクトリを読み取ることができ、このディレクトリにアクセスできる必要があります。

手順 4.3 *通常ユーザによるSnapper使用の有効化*

以下のすべての手順をrootとして実行してください。

1. ユーザがSnapperを使用するパーティションまたはサブボリュームにSnapper設定がない場合は、作成します。手順については、4.2.3項「Snapper設定の作成と変更」 (33 ページ)を参照してください。例:

   ```
   snapper --config web_data create /srv/www
   ```

2. /etc/snapper/configs/*NAME*に設定ファイルを作成します。NAMEは、上記の手順で-c/--configを使用して指定される値です(/etc/snapper/configs/web_dataなど)。 必要に応じて設定ファイルを調整します。詳細は4.2.3.1項 「設定ファイルの調整」 (34 ページ)を参照してください。

3. ALLOW_USERSとALLOW_GROUPS、またはその一方の値を設定し、ユーザやグループにパーミッションを与えます。複数のエントリはSpaceで区切ってください。たとえば、ユーザwww_adminにパーミッションを与えるには、次のように入力します。

   ```
   ALLOW_USERS="www_admin"
   ```

4 スナップショットディレクトリ*PATH*/.snapshotsの読み取りおよびアクセスパーミッションを与えます。*PATH*は、この手順の最初のステップで指定したサブボリュームに置き換えてください。例:

```
chmod a+rx /srv/www/.snapshots
```

これで、指定されたユーザやグループが特定のSnapper設定を使用できます。以下のようにlistコマンドを使ってテストできます。

```
www_admin:~ > snapper -c web_data list
```

4.2.4 自動スナップショットの無効化

インストール時にBtrfsでルートパーティションを設定すると、Snapperは自動的にシステムの毎時スナップショットを作成するほか、YaSTおよびzypperの処理の前後にスナップショットを作成します。それぞれのタスクを無効にするには、以下の手順を実行します。

毎時スナップショットの無効化

/etc/snapper/configs/rootを編集し、TIMELINE_CREATEをnoに設定します。

```
TIMELINE_CREATE="no"
```

zypperスナップショットの無効化

snapper-zypp-pluginパッケージをアンインストールします。

YaSTスナップショットの無効化

/etc/sysconfig/yast2を編集し、USE_SNAPPERをnoに設定します。

```
USE_SNAPPER="no"
```

4.3 スナップショットを手動で作成および管理する

Snapperは設定によって自動的にスナップショットを作成および管理するだけのものではありません。コマンドラインツールまたはYaSTモジュールを使用して、手動でスナップショットのペア(「事前および事後」)や単一のスナップショットを作成することもできます。

Snapperのすべての操作は既存の設定に対して実行されます(詳細は4.2.3項「Snapper設定の作成と変更」 (33 ページ)を参照)。スナップショットを作成するには、対象のパーティションまたはボリュームに対して設定が存在する必要があります。デフォルトで、システム設定(`root`)が使用されます。独自の設定に対してスナップショットを作成または管理する場合は、明示的にその設定を選択する必要があります。YaSTの［*現在の設定*］ドロップダウンメニューを使用するか、コマンドラインで`-c`を指定します(`snapper -c` *`MYCONFIG COMMAND`*)。

4.3.1 スナップショットのメタデータ

各スナップショットには、スナップショット自体とメタデータが含まれています。スナップショットを作成する場合は、メタデータも指定する必要があります。スナップショットを修正すると、メタデータが変更されます。コンテンツを修正することはできません。各スナップショットについて、以下のメタデータを利用できます。

- **Type(種類)**:スナップショットの種類です。詳細は4.3.1.1項「スナップショットの種類」 (40 ページ)を参照してください。このデータは変更できません。
- **Number(番号)**:スナップショットの一意の番号。このデータは変更できません。
- **Pre Number(前番号)**:対応する事前スナップショットの番号を指定します。事後スナップショットにのみ適用されます。このデータは変更できません。
- **Description(説明)**:スナップショットの説明です。
- **Userdata(ユーザデータ)**:カンマ区切りの「キー=値」のリスト形式でカスタムデータを指定できる、拡張用の項目です。(例:`reason=testing_stuff, user=tux`)。
- **Cleanup-Algorithm(クリーンアップアルゴリズム)**:スナップショットのクリーンアップアルゴリズムです。詳細は4.3.1.2項 「クリーンアップアルゴリズム」 (40 ページ)を参照してください。

4.3.1.1 スナップショットの種類

Snapperには、事前(pre)、事後(post)、および単一(single)の3種類のスナップショットがあります。これらは物理的には同じものですが、Snapperでは別のものとして扱われます。

`pre`(事前)
: 変更*前*のファイルシステムのスナップショットです。各`pre`(事前)スナップショットには、対応する`post`(事後)スナップショットがあります。自動YaST/zypperスナップショットなどに使用されます。

`post`(事後)
: 変更*後*のファイルシステムのスナップショットです。各`post`(事後)スナップショットには、対応する`pre`(事前)スナップショットがあります。自動YaST/zypperスナップショットなどに使用されます。

`single`(単一)
: スタンドアロンのスナップショットです。自動毎時スナップショットなどに使用されます。これは、スナップショットを作成する際のデフォルトの種類です。

4.3.1.2 クリーンアップアルゴリズム

Snapperには、古いスナップショットのクリーンアップアルゴリズムが3種類あります。このアルゴリズムは、日次のcronジョブとして実行されます。クリーンアップの頻度は、パーティションまたはサブボリュームのSnapper設定で定義されます(詳細は4.2.3.1項 「設定ファイルの調整」 (34 ページ)を参照)。

number(番号)
: スナップショットが特定の数に達すると、古いスナップショットを削除します。

time line(タイムライン)
: 特定の期間が経過したスナップショットを削除しますが、毎時、毎日、毎月、および毎年のスナップショットを一定数保持します。

empty-pre-post(事前事後の差分なし)
: 事前と事後のスナップショットに差分がない場合、そのペアを削除します。

4.3.2 スナップショットの作成

スナップショットを作成するには、`snapper create`を実行するか、YaSTモジュールの［*Snapper*］で［*Create*］をクリックします。以下は、コマンドラインを使ってスナップショットを作成する場合の例です。YaSTインタフェースを使用する場合、簡単に採用できるはずです。

ヒント: Snapshot Description

後で識別しやすくするため、わかりやすい説明を指定しておいてください。ユーザデータオプションを使って、さらに情報を指定することもできます。

`snapper create --description "Snapshot for week 2 2013"`
説明付きのスタンドアロンのスナップショット(種類はsingle）を、デフォルト(`root`)設定で作成します。クリーンアップアルゴリズムは指定されていないので、自動的にスナップショットが削除されることはありません。

`snapper --config home create --description "Cleanup in ~tux"`
説明付きのスタンドアロンのスナップショット(種類はsingle)を、カスタム設定`home`で作成します。クリーンアップアルゴリズムは指定されていないので、自動的にスナップショットが削除されることはありません。

`snapper --config home create --description "Daily data backup" --cleanup-algorithm timeline`
説明付きのスタンドアロンのスナップショット(種類はsingle)を、カスタム設定`home`設定で作成します。設定のタイムライン(time line)クリーンアップアルゴリズムで指定された条件が満たされると、ファイルが自動的に削除されます。

`snapper create --type pre--print-number--description "Before the Apache config cleanup"`
種類が`pre`のスナップショットを作成し、スナップショット番号を出力します。「事前」と「事後」の状態を保存するために使用されるスナップショットペアを作成するために必要な、最初のコマンドです。

`snapper create --type post--pre-number 30--description "After the Apache config cleanup"`
番号30のpreスナップショットとペアになるpostスナップショットを作成します。「事前」と「事後」の状態を保存するために使用されるスナップショットペアを作成するために必要な、2番目のコマンドです。

`snapper create --command` *`COMMAND`*`--description "Before and after COMMAND"`
*COMMAND*の実行前後に自動的にスナップショットを作成します。このオプションを使用できるのは、コマンドラインでsnapperを使用する場合のみです。

4.3.3 スナップショットのメタデータ修正

Snapperでは、説明、クリーンアップアルゴリズム、およびスナップショットのユーザデータを修正できます。それ以外のメタデータは変更できません。以下は、コマンドラインを使ってスナップショットを修正する場合の例です。YaSTインタフェースを使用する場合、簡単に採用できるはずです。

コマンドラインでスナップショットを修正するには、スナップショットの番号がわかっている必要があります。`snapperlist`を実行すると、すべてのスナップショットとその番号が表示されます。

YaSTの［*Snapper*］モジュールでは、すでにすべてのスナップショットがリスト表示されています。リストからスナップショットを選択し、［*Modify*］をクリックします。

`snapper modify --cleanup-algorithm "timeline" 10`
デフォルト(`root`)設定のスナップショット10番のメタデータを修正します。クリーンアップアルゴリズムが`timeline`に設定されます。

`snapper --config home modify --description "daily backup" -cleanup-algorithm "timeline"120`
カスタム設定`home`のスナップショット120番のメタデータを修正します。新しい説明が設定され、クリーンアップアルゴリズムを無しに設定します。

4.3.4 スナップショットの削除

YaSTの［*Snapper*］モジュールを使用してスナップショットを削除するには、リストからスナップショットを選択して［*Delete*］をクリックします。

コマンドラインツールを使ってスナップショットを削除するには、スナップショットの番号が分かっている必要があります。`snapper list`を実行して番号を調べます。スナップショットを削除するには、`snapper delete` *`NUMBER`*を実行します。

ヒント: スナップショットペアの削除

`pre`スナップショットを削除する場合は、必ず、対応する`post`スナップショットを削除する必要があります(逆も同様です)。

`snapper delete 65`
　デフォルト(`root`)設定のスナップショット65番を削除します。

`snapper -c home delete 89 90`
　カスタム設定`home`のスナップショット89番および90番を削除します。

ヒント: 古いスナップショットほどディスク容量を使用

ハードディスクの容量を空けるためにスナップショットを削除する場合(詳細は4.1.1項 「スナップショットとディスク容量」 (26 ページ)を参照)は、古いスナップショットから削除します。古いスナップショットほど、多くの容量を使用します。

スナップショットは、日次のcronジョブでも自動的に削除されます。詳細については、4.3.1.2項 「クリーンアップアルゴリズム」 (40 ページ)を参照してください。

4.4 制限

`Btrfs`およびSnapperは本番環境で使用可能な製品ですが、引き続き開発が行われています。現時点で以下の制限があります。これらの問題は、将来のリリースで解決される予定です。

4.4.1 データの整合性

スナップショットを作成する際に、データの整合性を確保するメカニズムがありません。スナップショットを作成するのと同時にファイルが書き込まれると(データベースなど)、ファイルが破損したり、ファイルへの書き込みが部分的になります。このようなファイルを復元すると、問題が発生することがあります。このため、必ず変更されたファイルとその差分をよく確認してください。どうしてもロールバックが必要なファイルのみ復元してください。

4.4.2 ユーザ追加の取り消し

通常、/homeは別のパーティションにあります。このような別のパーティションは、YaSTのロールバックのデフォルト設定に含まれません。このため、Snapperを使用してユーザの追加を取り消しても、ユーザのホームパーティションは削除されません。YaSTの［*ユーザとグループの管理*］ツールを使用してユーザを削除することを強くお勧めします。

4.4.3 /bootやブートローダの変更をロールバックできない

現時点で、SUSE Linux Enterprise ServerはBtrfsパーティションからブートできません。このため、システムパーティションにBtrfsを使用してインストールすると、/boot用に個別のパーティションが作成されます。/bootはスナップショットに対応していないため、YaST/zypperのロールバックについて以下の制限が適用されます。

ブートローダに対する設定変更はロールバックできない
: ロールバックできるファイルは、/etc内のブートローダ設定ファイルのみです。メインの設定ファイルは/bootの下に保存され、ロールバックできません。

カーネルのインストールについて完全なロールバックはできない
: カーネル自体とinitrdは、/bootパーティションにインストールされますが、カーネルモジュールとソースコードはそれぞれ/var/libおよび/usr/srcにインストールされます。また、カーネルをインストールすると/bootのブートローダ設定も変更されます。このため、カーネルのインストール

を元に戻す作業を含むロールバックを行う場合は、/bootからカーネルとそのinitrdを手動で削除し、カーネルのブートエントリを削除してブートローダ設定を調整する必要があります。

4.5 よくある質問とその回答

Snapperでは/var/log、/tmpなどのディレクトリの変更が表示されませんが、なぜですか？

一部のディレクトリについては、「スナップショット」を無効にしています(/var/logなど)。これは、ログを削除してしまうと問題の調査が難しくなるためです。「スナップショット」からパスを除外するため、これらのパス用にサブボリュームを作成しています。SUSE Linux Enterprise Serverでは、以下のマウントポイントが「スナップショット」の対象外です。

- /opt
- /srv
- /tmp
- /var/crash
- /var/log
- /var/run
- /var/spool
- /var/tmp

ブートローダからスナップショットをブートできますか？

現時点ではできません。SUSE Linux Enterprise Serverのブートローダは、現時点で、Btrfsパーティションからのブートに対応していません。

4.6 シンプロビジョンLVMボリュームでのSnapper使用

Snapperは、`Btrfs`ファイルシステムのスナップショット作成だけでなく、ext3またはXFSでフォーマットされたシンプロビジョンLVMボリュームの「スナップショット作成」にも対応しています(通常のLVMボリュームのスナップショットには対応していません)。詳細および設定の手順については、項 「LVMの設定」 (第15章 *高度なディスクセットアップ*, ↑*導入ガイド*)を参照してください。

シンプロビジョンLVMボリュームでSnapperを使用するには、そのようにSnapper設定を作成する必要があります。LVMで、`--fstype=lvm(`*`FILESYSTEM`*`)` を使用してファイルシステムを指定する必要があります。現在ext3およびXFSがサポートされているので、`ext3`または`xfs`が*`FILESYSTEM`*の有効な値です。例:

```
snapper -c lvm create-config --fstype="lvm(xfs)" /thin_lvm
```

4.2.3.1項 「設定ファイルの調整」 (34 ページ)で説明したように、必要に応じてこの設定を調整できます。これで、Snapperを使用して、スナップショットの作成と管理、ファイルの復元、変更の取り消しができるようになりました。

5 VNCによるリモートアクセス

VNC (Virtual Network Computing)では、グラフィカルなデスクトップを使用してリモートコンピュータを制御できます。これは、リモートシェルアクセスとは対照的です。VNCはプラットフォームに依存しないので、VNCを使用すれば、任意のオペレーティングシステムからリモートマシンにアクセスできます。

SUSE Linux Enterprise Serverでは、次の2種類のVNCセッションをサポートしています:クライアントからのVNC接続が続く限り、「存続する」一時的セッション、および明示的に終了されるまで「存続する」な永続的セッション。

注記: セッションタイプ

両方のタイプのセッションを1つのコンピュータの異なるポートから同時に提供ができます。ただし、オープンセッションを1つのタイプからもう一方のタイプに変換することはできません。

5.1 一時的VNCセッション

一時的セッションは、リモートクライアントによって開始されます。これにより、サーバにグラフィカルなログイン画面が開きます。この画面でセッションを開始するユーザを選択できます。さらに、ログインマネージャでサポートされている場合はデスクトップ環境も選択できます。そのようなVNCセッションへのクライアント接続を終了すると、そのセッション内で開始したアプリケーションもすべて終了します。一時的なVNCセッションは共用できませんが、1つのホストで同時に複数のセッションを実行することは可能です。

手順 5.1 *一時的VNCセッションを有効にする*

1 まず、［*YaST*］>［*ネットワークサービス*］>［*リモート管理(VNC)*］の順に選択します。

2 ［*(リモート管理を許可する*］にチェックマークを付けます。

3 必要な場合は、［*ファイアウォールでポートを開く*］にもチェックマークを付けます(たとえば、ネットワークインタフェースを外部ゾーンに属するように設定する場合)。ネットワークインタフェースが複数ある場合は、［*ファイアウォールの詳細*］で、特定のインタフェースにだけファイアウォールポートを開くように制限します。

4 ［*完了*］で設定を確認します。

5 必要なパッケージの一部をまだ入手できない場合は、足りないパッケージのインストールを承認する必要があります。

注記: 使用可能な設定

SUSE Linux Enterprise Serverのデフォルト設定では、1024x768ピクセルの解像度と16ビットの色数でセッションが提供されます。セッションで使用できるポートは、「正規の」 VNCビューアの場合はポート5901(VNCディスプレイ1に相当)、Webブラウザの場合はポート5801です。

その他の設定は、異なるポートで使用できます。5.1.2項 「一時的VNCセッションを設定する」 (49 ページ)を参照してください。

VNCディスプレイ番号とXディスプレイ番号は、一時的セッションでは互いに独立しています。VNCディスプレイ番号は、サーバがサポートするすべての設定に手動で割り当てられます(上記の例では1)。VNCセッションは、設定の1つを使用して開始されるたびに、自動的に未使用のXディスプレイ番号を取得します。

5.1.1 一時的VNCセッションを開始する

一時的VNCセッションを開始するには、VNCビューアをクライアントコンピュータにインストールしておく必要があります。SUSE Linux製品の標準

ビューアは、tightvncパッケージで提供されるvncviewerです。Webブラウザとjavaアプレットの使用によっても、VNCセッションを表示できます。

VNCビューアを起動し、サーバのデフォルト設定でセッションを開始するには、次のコマンドを使用します。

```
vncviewer jupiter.example.com:1
```

VNCディスプレイ番号の代わりに、2つのコロンを使用してポート番号を指定することもできます。

```
vncviewer jupiter.example.com::5901
```

または、Javaを有効にしたWebブラウザで、URLとして`http://jupiter.example.com:5801`を入力することにより、VNCセッションを表示できます。

5.1.2 一時的VNCセッションを設定する

デフォルト設定を変更する必要も意志もない場合は、このセクションをスキップできます。

一時的VNCセッションは、xinetdデーモンを介して開始されます。設定ファイルは、/etc/xinetd.d/vncにあります。このファイルは、デフォルトで、6つの設定ブロックを提供します:VNCビューア用に3ブロック(vnc1からvnc3まで)、Javaアプレット用に3ブロック(vnchttpd1からvnchttpd3まで)。デフォルトでは、vnc1 と vnchttpd1だけが有効です。

設定を有効にするには、disable = yes行の最初のカラムに#文字を付けて行をコメント化するか、その行を完全に削除します。設定を無効にするには、その行をコメント解除するか、追加します。

Xvncサーバは、server_argsオプションで設定できます。オプションのリストについては、Xnvc --helpを参照してください。

カスタム設定を追加する際には、それらの設定が、同じホスト上の他の設定、他のサービス、または既存の永続的VNCセッションですでに使用中のポートを使用しないことを確認してください。

設定の変更を有効にするには、次のコマンドを入力します:

```
rcxinetd reload
```

重要: ファイアウォールとVNCポート

手順5.1「一時的VNCセッションを有効にする」 (48 ページ)で説明されているように、リモート管理をアクティブにすると、ファイアウォール内でポート5801および5901が開きます。VNCセッションで使用されるネットワークインタフェースがファイアウォールで保護されている場合、VNCセッションの追加ポートをアクティブにする際には各ポートを手動で開く必要があります。手順については、第15章 *Masquerading and Firewalls* (↑*Security Guide (セキュリティガイド)*)を参照してください。

5.2 永続的VNCセッション

永続的VNCセッションは、サーバ上で開始されます。セッションとこのセッションで開始されたすべてのアプリケーションは、クライアント接続とは関わりなく、セッションが終了するまで実行されます。

永続的セッションは、複数のクライアントから同時にアクセスすることが可能です。この機能は、1つのクライアントがフルアクセスをもち、他のすべてのクライアントが表示オンリーアクセスを持つデモに最適です。また、トレイナが訓練生のデスクトップにアクセスする必要があるトレーニングでも使用できます。ただし、ほとんどの場合、VNCセッションの共用が必要とされることはありません。

ディスプレイマネージャを起動する一時的セッションとは対照的に、永続的セッションでは、操作準備のできたデスクトップを起動し、そのデスクトップがVNCセッションを開始したユーザとしてセッションを実行します。

永続的セッションへのアクセスは、可能な2タイプのパスワードによって保護されます:

- フルアクセスを付与する通常のパスワード。または、
- 非対話的(表示オンリー)アクセスを付与するオプションの表示オンリーパスワード。

1つのセッションに、両方の種類のクライアント接続が一度に複数存在できます。

手順 5.2　永続的VNCセッションを開始する

1 シェルを開き、VNCセッションを所有するユーザとしてログインしていることを確認します。

2 VNCセッションで使用されるネットワークインタフェースがファイアウォールで保護されている場合は、ファイアウォール内でセッションによって使用されるポートを手動で開く必要があります。複数のセッションを開始する場合は、一連のポートを開くことができます。ファイアウォールの設定方法の詳細については、第15章 *Masquerading and Firewalls* (↑*Security Guide (セキュリティガイド)*)を参照してください。

`vncserver`は、ディスプレイ`:1`にはポート`5901`、ディスプレイ`:2`にはポート`5902`という順序でポートを使用します。永続的セッションの場合、VNCディスプレイとXディスプレイは、通常、同じ番号です。

3 1024x769ピクセルの解像度と16ビットの色数でセッションを開始するには、次のコマンドを入力します。

```
vncserver -geometry 1024x768 -depth 16
```

`vncserver`コマンドは、何も指定されない場合、未使用のディスプレイ番号を選択し、その選択内容をプリントします。追加オプションについては、`man 1 vncserver`を参照してください。

初めて`vncviewer`を実行すると、セッションへのフルアクセス用パスワードが要求されます。必要な場合は、セッションへの表示オンリーアクセス用パスワードも入力できます。

ここで指定するパスワードは、同じユーザによって開始される今後のセッションにも使用されます。それらのパスワードは、`vncpasswd`コマンドで変更できます。

重要: セキュリティ上の考慮事項

必ず、かなりの長さ(8文字以上)の強力なパスワードを使用してください。これらのパスワードは共用しないでください。

VNC接続は暗号化されていないので、2つのコンピュータ間のネットワークを傍受できる者たちによってセッション開始時に転送されるパスワードが読み取られる恐れがあります。

VNCセッションを終了するには、通常のローカルXセッションのシャットダウンのように、VNC環境内部で実行中のデスクトップ環境をVCNビューアからシャットダウンします。

セッションを手動で終了したい場合は、VNCサーバでシェルを開き、終了したいVNCセッションを所有するユーザとしてログインしていることを確認します。次のコマンドを実行して、ディスプレイ:1で実行されているセッションを終了します: `vncserver -kill :1`

5.2.1 永続的VNCセッションに接続する

永続的VNCセッションに接続するには、VCNビューアをインストールする必要があります。SUSE Linux製品の標準ビューアは、`tightvnc`パッケージで提供される`vncviewer`です。WebブラウザとJavaアプレットの使用によっても、VNCセッションを表示できます。

VNCビューアを起動し、VNCサーバのディスプレイ:1に接続するには、次のコマンドを使用します。

```
vncviewer jupiter.example.com:1
```

VNCディスプレイ番号の代わりに、2つのコロンを使用してポート番号を指定することもできます。

```
vncviewer jupiter.example.com::5901
```

または、Javaを有効にしたWebブラウザで、URLとして`http://jupiter.example.com:5801`を入力することにより、VNCセッションを表示できます。

5.2.2 永続的VNCセッションを設定する

永続的VNCセッションは、`$HOME/.vnc/xstartup`を編集することによって設定できます。デフォルトでは、このシェルスクリプトは、`xterm`と`twm`ウィンドウマネージャを起動します。代わりとして、GNOMEまたはKDEを起動するには、`twm`で始まる行を次のいずれかで置き換えます。

```
/usr/bin/gnome     # GNOME
/usr/bin/startkde  # KDE
```

注記: ユーザごとに1つの設定

永続的VNCセッションは、ユーザごとの単一設定として設定されます。1人のユーザが開始する複数のセッションでは、すべて同じ起動ファイルとパスワードファイルが使用されます。

コマンドラインツールによるソフトウェアの管理

6

この章では、ソフトウェア管理の２つのコマンドラインツールとして、ZypperとRPMについて説明します。このコンテキストで使用される述語(たとえば、`repository`、`patch`、`update`など)の定義については、項 「用語の定義」(第9章 *ソフトウェアをインストールまたは削除する*,↑*導入ガイド*)を参照してください。

6.1 Zypperの使用

Zypperは、パッケージのインストール、更新、削除、およびリポジトリの管理を行うためのコマンドラインパッケージマネージャです。zypperの構文はrugに類似しています。rugとは対照的に、zypperではzmdデーモンが背後で実行している必要はありません。rugの互換性の詳細は、`man zypper`、「COMPATIBILITY WITH RUG」の項を参照してください。 これは特に、リモートソフトウェア管理タスクの実行、またはシェルスクリプトからのソフトウェアの管理で役立ちます。

6.1.1 一般的な使用方法

Zypperの一般的な構文は次のとおりです。

```
zypper [global-options]command[command-options][arguments] ...
```

ブラケットで囲まれたコンポーネントは必須ではありません。Zypperを実行する最も簡単な方法は、その名前の後にコマンドを入力することです。たと

えば、システムタイプに必要なすべてのパッチを適用するには、次のようにします。

```
zypper patch
```

さらに、グローバルオプションをコマンドの直前に入力することによって、1つ以上のグローバルオプションから選択することができます。たとえば`--non-interactive`では、何も入力を求められることなく、コマンドを実行できます(自動的にデフォルトの解答が適用されます)。

```
zypper --non-interactive patch
```

特定のコマンドに固有のオプションを使用する場合は、コマンドの直後にそのオプションを入力します。たとえば、`--auto-agree-with-licenses`は、ライセンスの確認を求めることなく、システムで必要なすべてのパッチを適用します(自動的に受け入れられます)。

```
zypper patch --auto-agree-with-licenses
```

一部のコマンドでは、1つ以上の引数が必要です。たとえば、インストールコマンドを使用する場合、インストールするパッケージを指定する必要があります。

```
zypper install mplayer
```

また一部のオプションでは、引数が必要です。次のコマンドでは、すべての既知のパターンが表示されます。

```
zypper search -t pattern
```

上記のすべてを結合できます。たとえば、次のコマンドは、冗長モードで、`factory`リポジトリから`mplayer`と`amarok`パッケージをインストールします。

```
zypper -v install --from factory mplayer amarok
```

`--from`オプションは、指定されたリポジトリからパッケージを要求する際に、すべてのリポジトリを(依存関係の解決のため)有効に保ちます。

ほとんどのZypperコマンドには、指定のコマンドのシミュレーションを行う`dry-run`オプションがあります。このオプションは、テストの目的で使用できます。

```
zypper remove --dry-run MozillaFirefox
```

zypperは、トランザクションを識別する目的で、グローバルオプション `--userdata string`をサポートします。ユーザ定義文字列が、`/var/log/zypp/history`のzypper履歴ログおよびSnapperに渡されます。

```
zypper --userdata string patch
```

6.1.2 Zypperを使ったソフトウェアのインストールと削除

パッケージをインストールまたは削除するには、次のコマンドを使用します。

```
zypper install package_name
zypper remove package_name
```

Zypperでは、インストールコマンドおよび削除コマンドでパッケージを指定するために、次のようなさまざまな方法が可能です。

正確なパッケージ名を指定します(およびバージョン番号)

```
zypper install MozillaFirefox
```

または

```
zypper install MozillaFirefox-3.5.3
```

リポジトリエイリアスおよびパッケージ名を指定します

```
zypper install mozilla:MozillaFirefox
```

ここで`mozilla`は、インストールするリポジトリのエイリアスです。

ワイルドカードを使用してパッケージ名を指定します
次のコマンドでは、名前の先頭に「Moz」が付くすべてのパッケージがインストールされます。特にパッケージを削除する場合には、慎重に行うことが必要です。

```
zypper install 'Moz*'
```

機能によって指定します
たとえば、パッケージ名を知らずにperlモジュールをインストールする場合は、機能による指定が有用です。

```
zypper install 'perl(Time::ParseDate)'
```

機能、アーキテクチャ、および(または)バージョンを指定します
: 機能とともに、アーキテクチャ(i586またはx86_64など)、および(または)バージョンを指定できます。バージョンの前には、演算子として、<(未満)、<=(以下)、=(等しい)、=>(以上)、または>(より大きい)を付ける必要があります:

```
zypper install 'firefox.x86_64'
zypper install 'firefox>=3.5.3'
zypper install 'firefox.x86_64>=3.5.3'
```

RPMファイルへのパスによって指定します
: また、パッケージに対するローカルパスまたはリモートパスを指定できます。

```
zypper install /tmp/install/MozillaFirefox.rpm
zypper install
http://download.opensuse.org/repositories/mozilla/SUSE_Factory/x86_64/MozillaFirefox-3.5.3-1.3.x86_64.rpm
```

パッケージのインストールおよび削除を同時に行うには、+/-修飾子を使用します。emacsのインストールとvimの削除を同時に行うには、次のコマンドを使用します。

```
zypper install emacs -vim
```

emacsの削除とvimのインストールを同時に行うには、次のコマンドを使用します。

```
zypper remove emacs +vim
```

名前の先頭に-が付くパッケージ名がコマンドオプションとして解釈されないようにするには、常に第2引数としてその名前を使用します。これが可能でない場合は、名前の前に--を付けます。

```
zypper install -emacs +vim       # Wrong
zypper install vim -emacs        # Correct
zypper install -- -emacs +vim    # same as above
zypper remove emacs +vim         # same as above
```

指定したパッケージの削除後に、(その特定のパッケージとともに)不要になったパッケージを自動的に削除したい場合は、--clean-depsオプションを使用します。

```
rm package_name --clean-deps
```

Zypperではデフォルトで、選択したパッケージのインストールまたは削除の前に、あるいは問題が発生した際には、確認が求められます。この動作は、

--non-interactiveオプションを使用することで上書きされます。このオプションは、次のように、実際のコマンド(install、remove、patch)の前に指定する必要があります。

```
zypper --non-interactive install package_name
```

このオプションは、スクリプトおよびcronジョブでZypperを使用できます。

警告: 必須システムパッケージは削除しないでください。

glibc、zypper、kernelなどのパッケージは削除しないでください。これらのパッケージはシステムで必須であり、削除するとシステムが不安定になったり、すべての動作が停止したりする場合があります。

6.1.2.1 ソースパッケージのインストールまたはダウンロード

パッケージの対応するソースパッケージをインストールする場合は、次を使用します。

```
zypper source-install package_name
```

このコマンドにより、指定したパッケージの構築依存もインストールされます。この処理が必要でない場合は、次のようにスイッチ-Dを追加します。ビルドの依存関係のみをインストールするには、-dを使用します。

```
zypper source-install -D package_name # source package only
zypper source-install -d package_name # build dependencies only
```

もちろん、リポジトリリストで有効にしたソースパッケージを含むリポジトリが存在する場合にのみ動作します(ソースパッケージはデフォルトで追加されますが、有効にはなりません)。リポジトリの管理の詳細については、6.1.5項 「Zypperによるリポジトリの管理」 (67 ページ)を参照してください。

リポジトリで使用可能なすべてのソースパッケージのリストは、次のコマンドで参照できます。

```
zypper search -t srcpackage
```

また、すべてのインストール済みパッケージのソースパッケージをローカルディレクトリにダウンロードすることもできます。ソースパッケージをダウンロードするには、以下を使用します。

```
zypper source-download
```

デフォルトのダウンロードディレクトリは/var/cache/zypper/source-downloadです。これは、--directoryオプションを使って変更できます。ダウンロードや削除を行わず、不足パッケージや不要パッケージの表示のみを行う場合は、--statusオプションを使用します。不要なソースパッケージを削除するには、--deleteオプションを使用します。削除を無効にするには、--no-deleteオプションを使用します。

6.1.2.2 ユーティリティ

すべての依存関係が依然として満たされていることを確認し、欠如する依存関係を修復するには、次のコマンドを使用します。

```
zypper verify
```

必要とされる依存関係に加えて、一部のパッケージでは他のパッケージが「推奨されます」。これらの推奨対象パッケージは、実際に使用可能でインストール可能な場合のみインストールされます。推奨側のパッケージがインストールされた後で、(パッケージまたはハードウェアの追加により)推奨対象パッケージが使用可能になった場合は、次のコマンドを使用します。

```
zypper install-new-recommends
```

このコマンドは、WebcamまたはWLANデバイスにプラグインした後で非常に役に立ちます。このコマンドは、デバイスのドライバと関連ソフトウェアが利用できる場合には、それらをインストールします。ドライバと関連ソフトウェアは、一定のハードウェア依存関係が満たされている場合のみインストールできます。

6.1.3 Zypperによるソフトウェアの更新

Zypperを使用してソフトウェアを更新するには3つの方法があります。パッチをインストールする、パッケージの新しいバージョンをインストールする、または配布全体を更新する方法です。最後の方法は、6.1.4項 「zypperによるディストリビューションアップグレード」 (64ページ)で説明されているzypper dist-upgradeコマンドで行うことができます。

6.1.3.1 パッチのインストール

正式にリリースされたすべてのパッチをインストールしてシステムに適用するには、次のコマンドを実行するだけです。

```
zypper patch
```

この場合、リポジトリで利用可能なすべてのパッチが関連性についてチェックされ、必要に応じてインストールされます。SUSE Linux Enterprise Serverインストールを登録した後、このようなパッチを含む正式な更新リポジトリがシステムに追加されます。上記のコマンドを入力すれば、いつでも必要なときにこれらを適用できます。

Zypperでは、パッチの可用性について問い合わせるための3つの異なるコマンドが認識されます。

`zypper patch-check`
: 必要なパッチの数を示します(システムに適用されていてもまだインストールされていないパッチ)。

```
~ # zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

`zypper list-patches`
: 必要なすべてのパッチを示します(システムに適用されていてもまだインストールされていないパッチ)。

```
~ # zypper list-patches
Loading repository data...
Reading installed packages...

Repository                          | Name      | Version | Category | Status
------------------------------------+-----------+---------+----------+-------
Updates for openSUSE 11.3 11.3-1.82 | lxsession | 2776    | security | needed
```

`zypper patches`
: すでにインストールされているか、インストールに適用されているかどうかにかかわらず、SUSE Linux Enterprise Serverで使用可能なすべてのパッチを表示します。

また、特定の問題に関連するパッチを表示およびインストールすることもできます。特定のパッチを表示するには、次のオプションでzypper list-patchesコマンドを使用します。

--bugzilla[=*number*]
: Bugzilla発信番号で必要なすべてのパッチを表示します。オプションとして、この特定のバグのパッチを一覧するだけの場合は、バグ番号を指定できます。

--cve[=*番号*]
: CVE (Common Vulnerabilities and Exposures)問題に関して必要なすべてのパッチ、または特定のCVE番号に一致するパッチだけ(番号を指定した場合)を一覧します。

特定のBugzillaまたはCVEの問題に対するパッチをインストールするには、次のコマンドを使用します。

```
zypper patch --bugzilla=number
```

または

```
zypper patch --cve=number
```

たとえば、CVE番号がCVE-2010-2713のセキュリティパッチをインストールするには、次のコマンドを実行します。

```
zypper patch --cve=CVE-2010-2713
```

6.1.3.2 更新のインストール

リポジトリに新しいパッケージのみが存在し、パッチが提供されていない場合は、zypper patchは無効です。インストールされているパッケージをすべて新しく入手可能なバージョンで更新するには、次を使用します。

```
zypper update
```

個別のパッケージを更新するには、更新コマンドまたはインストールコマンドのいずれかでパッケージを指定します。

```
zypper update package_name
zypper install package_name
```

インストール可能なすべての新しいパッケージのリストを、次のコマンドで取得できます。

```
zypper list-updates
```

ただし、このコマンドは、次の基準と一致するパッケージのみ一覧します。

- すでにインストール済みのパッケージと同じベンダである
- すでにインストール済みのパッケージと同等以上の優先度をもつリポジトリによって提供される
- インストール可能である(すべての依存関係が満たされている)

次のコマンドを使用すると、(インストール可能かどうかに関わらず)すべての新しい使用可能なパッケージのリストを取得できます。

```
zypper list-updates --all
```

新しいパッケージをインストールできない理由を見つけるには、上記で説明されているように、`zypper install`コマンドまたは`zypper update`コマンドを使用します。

6.1.3.3 新しい製品バージョンへのアップグレード

インストールを新しい製品バージョンに簡単にアップグレードするには(たとえば、SUSE Linux Enterprise Server 11からSUSE Linux Enterprise Server 11 SP1へのアップグレード)、まず、現在のSUSE Linux Enterprise Serverリポジトリに一致するようにリポジトリを調整します。詳細については、6.1.5項 「Zypperによるリポジトリの管理」 (67 ページ)を参照してください。次に、必要なリポジトリに関して`zypper dist-upgrade`コマンドを使用します。このコマンドにより、現在有効なリポジトリからすべてのパッケージがインストールされます。詳細の説明については、6.1.4項 「zypperによるディストリビューションアップグレード」 (64 ページ)を参照してください。

ディストリビューションアップグレードを特定のリポジトリのパッケージに制限しながら、他のリポジトリも考慮に入れて依存関係を満たすには、`--from`オプションを使用して、リポジトリをその別名、番号、またはURIで指定します。

注記: **zypper update**と**zypper dist-upgrade**の相違

システムの整合性を維持しながら製品のバージョンで使用可能な新しいバージョンにパッケージを更新する場合は、zypper updateを選択します。zypper updateは、次のルールに従います。

ベンダは変更されません
アーキテクチャは変更されません
ダウングレードされません
インストール済みパッケージが保持されます

zypper dist-upgradeを実行すると、すべてのパッケージが現在有効なリポジトリからインストールされます。このルールを適用した場合、パッケージによりベンダまたはアーキテクチャが変更されるか、ダウングレードされる場合もあります。アップグレード後に依存関係が満たされていないすべてのパッケージはアンインストールされます。

6.1.4 zypperによるディストリビューションアップグレード

zypperコマンドラインユーティリティを使用すると、次のバージョンのディストリビューションにアップグレードできます。最も重要なことは、実行中のシステムからシステムアップグレードのプロセスを開始できることです。

これは、リモートアップグレードや、同様な設定の多数のシステムでアップグレードを実行したい高度なユーザにとって魅力的な機能です。

6.1.4.1 zypperによるアップグレードを開始する前に

zypperを使用したアップグレード中に予期しないエラーが発生しないようにするには、リスクの高いコンステレーションを最小限にします。

- できるだけ多くのアプリケーションや不要なサービスを終了し、すべての通常ユーザをログアウトします。
- アップグレードの開始前にサードパーティーのリポジトリを無効にしたり、それらのリポジトリの優先度を下げることによって、デフォルトのシステ

ムリポジトリからのパッケージが優先されるようにします。アップグレード後にそれらのリポジトリを再度有効にし、それらのバージョン文字列を編集して、アップグレードした現在実行中のシステムのディストリビューションのバージョン番号に一致させます。

6.1.4.2 アップグレード手順

警告: システムのバックアップを確認してください。

アップグレード手順を実際に開始する前に、システムのバックアップが最新であり、復元可能であることを確認します。以降のステップの多くで手動入力が必要なので、これは特に重要です。

プログラムzypperは、長いコマンド名と短いコマンド名をサポートしています。たとえば、`zypper install`を短縮して`zypper in`にすることができます。次のテキストでは、短いコマンド名が使用されています。

1 オンラインアップデートを実行して、ソフトウェア管理スタックを最新にします。詳細については、第1章 *YaSTオンラインアップデート* (3 ページ)を参照してください。

2 更新のソースとして使用するリポジトリを設定します。これを正しく設定することは非常に重要です。YaST(項「ソフトウェアリポジトリおよびサービスの操作」 (第9章 *ソフトウェアをインストールまたは削除する*, ↑*導入ガイド*)参照)または`zypper`(6.1項 「Zypperの使用」 (55 ページ)参照)のいずれかを使用します。 以降のステップで使用するリポジトリの名前は、カスタマイズの仕方によって若干異なることがあります。

独自のインストールサーバを準備または更新するとします。背景情報については、項 「YaSTを使ったインストールサーバのセットアップ」 (第14章 *リモートインストール*, ↑*導入ガイド*)を参照してください。

現在のリポジトリを表示するには、次のコマンドを入力します。

```
zypper lr -u
```

2a 次のようなコマンドで、システムリポジトリのバージョン番号を「11-SP2」から「11-SP3」に増やし、新しいリポジトリを追加します。

```
server=http://download.example.org
zypper ar $server/distribution/11-SP3/repo/oss/ SLE-11-SP3
zypper ar $server/update/11-SP3/ SLE-11-SP3-Update
```

次に、古いリポジトリを削除します。

```
zypper rr SLE-11-SP2
zypper rr SLE-11-Update
```

2b サードパーティのリポジトリまたは他のOpen Build Serviceリポジトリを無効にします。これは、`zypper dup`がデフォルトリポジトリのみを操作するように保証するためです。(replace *`repo-alias`*を、無効にしたいリポジトリの名前で置き換えます):

```
zypper mr -d repo-alias
```

または、これらのリポジトリの優先順位を下げることもできます。

注記: 未解決の依存関係の処理

`zypper dup`は、未解決の依存関係を持つすべてのパッケージを削除します。ただし、無効化されたリポジトリのパッケージについては、それらの依存関係が正常である限り、それらを保持します。

`zypper dup`を使用すると、すべてのインストール済みパッケージは利用可能なリポジトリの1つをソースとします。zypper dupは、インストールパッケージのバージョン、アーキテクチャ、ベンダを考慮に入れず、フレッシュインストールをエミュレートします。リポジトリ内で利用可能でなくなったパッケージは、孤立したと見なされます。そのようなパッケージは、その依存関係が正常でなければ、アンインストールされます。依存関係が正常な場合は、そのようなパッケージのインストールは保持されます。

2c これらの処理が終了したら、次のコマンドでリポジトリの設定を確認します。

```
zypper lr -d
```

3 ローカルメタデータとリポジトリの内容を、`zypper ref`で更新します。

4 zypper up zypperを使用して、zyppeとパッケージ管理スタックを11 SP1リポジトリから取り込みます。

5 zypper dupで、実際のディストリビューションアップグレードを実行します。SUSE Linux Enterpriseのライセンスと一部のパッケージ(インストール済みパッケージのセットによって異なる)のライセンスの確認を要求されます。

6 SuSEconfigで、基本的なシステム設定を実行します。

7 shutdown -r nowで、システムをリブートします。

6.1.5 Zypperによるリポジトリの管理

Zypperのすべてのインストールまたはパッチのコマンドは、既知のリポジトリのリストに応じて異なります。システムで既知のすべてのリポジトリのリストを表示するには、次のコマンドを使用します。

```
zypper repos
```

結果は、次の出力のようになります。

例 6.1 Zypper—既知のリポジトリのリスト

```
# | Alias                              | Name
   | Enabled | Refresh
--+------------------------------------+-----------------------------------+---------+--------
1 | SUSE-Linux-Enterprise-Server 11-0 | SUSE-Linux-Enterprise-Server 11-0
  | Yes     | No
2 | SLES-11-Updates                    | SLES 11 Online Updates
   | Yes     | Yes
3 | broadcomdrv                        | Broadcom Drivers
   | Yes     | No
```

各種コマンドのリポジトリを指定するには、エイリアス、URI、またはリポジトリ番号をzypper reposコマンド出力から使用できます。リポジトリの別名は、リポジトリ操作コマンド用の短いリポジトリ名です。ただし、リポジトリリストの変更後に、リポジトリ番号が変わる可能性があります。エイリアスは変更されることはありません。

デフォルトでは、URIやリポジトリの優先度など、詳細情報は表示されません。すべての詳細を表示するには、次のコマンドを使用します。

```
zypper repos -d
```

6.1.5.1 リポジトリの追加

リポジトリを追加するには、次を実行します。

```
zypper addrepo URIalias
```

*URI*は、インターネットリポジトリ、ネットワークリソース、ディレクトリ、CDまたはDVDのいずれかです(詳細については、http://en.opensuse.org/openSUSE:Libzypp_URIsを参照してください)。*別名*は、リポジトリの短い固有のIDです。このIDは、固有であること以外は自由に選択できます。すでに使用されているエイリアスを指定した場合、Zypperでは警告が発行されます。

6.1.5.2 リポジトリの削除

リストからリポジトリを削除する場合は、コマンド`zypper removerepo`を使用し、削除するリポジトリのエイリアスまたは番号を指定します。たとえば例6.1「Zypper—既知のリポジトリのリスト」 (67 ページ)の3番目のエントリとして表示されているリポジトリを削除するには、次のコマンドを使用します。

```
zypper removerepo 3
```

6.1.5.3 リポジトリの変更

`zypper modifyrepo`によりリポジトリを有効または無効にします。また、このコマンドにより、リポジトリのプロパティ(動作、名前、優先度の更新など)を変更できます。次のコマンドは、`updates`という名前のリポジトリを有効にし、自動更新をオンにし、リポジトリの優先度を 20に設定します。

```
zypper modifyrepo -er -p 20 'updates'
```

リポジトリの変更は、単一のリポジトリに制限されません。リポジトリグループを操作することもできます。

`-a`: すべてのリポジトリ

-l: ローカルリポジトリ
-t: リモートリポジトリ
-m タイプ:特定のタイプのリポジトリ(ここで、タイプには、次のいずれかを指定できます: http、https、ftp、cd、dvd、dir、file、cifs、smb、nfs、hd、iso)。

リポジトリエイリアスの名前を変更するには、renamerepoコマンドを使用します。次の例では、エイリアスをMozilla Firefoxから単なるfirefoxに変更しています。

```
zypper renamerepo 'Mozilla Firefox' firefox
```

6.1.6 Zypperによるリポジトリおよびパッケージのクエリ

Zypperでは、リポジトリまたはパッケージをクエリするためのさまざまな方法が提供されています。使用可能なすべての製品、パターン、パッケージ、またはパッチのリストを取得するには、次のコマンドを使用します。

```
zypper products
zypper patterns
zypper packages
zypper patches
```

特定のパッケージについてすべてのリポジトリをクエリするには、searchを使用します。searchは、パッケージの名前、またはパッケージの概要と説明(オプション)に関して機能します。検索語では、ワイルドカード*および?を使用できます。デフォルトでは、検索で大文字と小文字が区別されません。

```
zypper search firefox       # simple search for "firefox"
zypper search "*fire*"      # using wildcards
zypper search -d fire      # also search in package descriptions and summaries
zypper search -u firefox    # only display packages not already installed
```

特定の機能を提供するパッケージを検索するには、コマンドwhat-providesを使用します。たとえば、どのパッケージがperlモジュールSVN::Coreを提供するか確認したい場合は、次のコマンドを使用します。

```
zypper what-provides 'perl(SVN::Core)'
```

単一のパッケージをクエリするには、infoを使用し、引数として正確なパッケージ名を指定します。パッケージに関する詳細情報を表示します。パッケー

ジの要求や推奨も表示するには、--requiresオプションや--recommendsオプションを使用します。

```
zypper info --requires MozillaFirefox
```

what-provides パッケージはrpm -q --whatprovides パッケージに似ていますが、rpmではRPMデータベース(つまり、すべてのインストール済みパッケージのデータベース)のみを問い合わせることができます。それに対してZypperは、インストール済みのパッケージだけでなく、すべてのリポジトリから機能プロバイダに関する情報を表示します。

6.1.7 Zypperの設定

Zypperには、現在、設定ファイルが付属しています。この設定ファイルを使用すれば、Zypperの動作を(システム全体またはユーザ固有のでどちらかで)永続的に変更できます。システム全体に渡って変更する場合は、/etc/zypp/zypper.confを編集します。ユーザ固有に変更する場合は、~/.zypper.confを編集します。~/.zypper.confがまだ存在していない場合は、テンプレートとして/etc/zypp/zypper.confを使用できます。このテンプレートを~/.zypper.confにコピーして、好みに合わせて調整してください。利用できるオプションのヘルプについては、ファイル内のコメントを参照してください。

6.1.8 トラブルシューティング

設定済みのリポジトリからのパッケージへのアクセスに問題がある場合(たとえば、一定のパッケージがリポジトリの1つに存在することを知っていても、zypperでそのリポジトリを見つけられない場合など)は、次のコマンドでリポジトリを更新すると有効なことがあります。

```
zypper refresh
```

それも役に立たない場合は、次のコマンドを試してください。

```
zypper refresh -fdb
```

このコマンドは、生メタデータの強制ダウンロードを含むデータベースの完全な更新と再構築を強制します。

6.1.9 btrfsファイルシステムでのZypperロールバック機能

ルートパーティションでBtrfsファイルシステムが使用され、snapperがインストールされている場合に、ファイルシステムに対する変更をコミットして適切なファイルシステムスナップショットを作成すると、zypperは(snapperによってインストールされるスクリプト経由で)自動的にsnapperを呼び出します。これらのスナップショットは、zypperによって行われた変更を元に戻す場合に使用できます。snapperの詳細については、man snapperを参照してください。

現時点で、zypper(およびYaST)ではルートファイルシステムのスナップショットのみ作成できます。それ以外のサブボリュームは設定できません。この機能は、デフォルトファイルシステムではサポートされていません。

6.2 RPM—パッケージマネージャ

RPM (RPM Package Manager)がソフトウェアパッケージを管理するのに使用されます。RPMの主要コマンドは、rpmとrpmbuildです。ユーザ、システム管理者、およびパッケージの作成者は、強力なRPMデータベースでクエリーを行って、インストールされているソフトウェアに関する情報を取得できます。

基本的にrpmには、ソフトウェアパッケージのインストール、アンインストール、アップデート、RPMデータベースの再構築、RPMベースまたは個別のRPMアーカイブの照会、パッケージの整合性チェック、およびパッケージへの署名の5種類のモードがあります。rpmbuildは、元のソースからインストール可能なパッケージを作成する場合に使用します。

インストール可能なRPMアーカイブは、特殊なバイナリ形式でパックされています。それらのアーカイブは、インストールするプログラムファイルとある種のメタ情報で構成されます。メタ情報は、ソフトウェアパッケージを設定するためにrpmによってインストール時に使用されるか、または文書化の目的でRPMデータベースに格納されています。通常、RPMアーカイブには拡張子.rpmが付けられます。

ヒント: ソフトウェア開発パッケージ

多くのパッケージにおいて、ソフトウェア開発に必要なコンポーネント(ライブラリ、ヘッダ、インクルードファイルなど)は、別々のパッケージに入れられています。それらの開発パッケージは、最新のGNOMEパッケージのように、ソフトウェアを自分自身でコンパイルする場合にのみ、必要になります。それらのパッケージは、名前の拡張子`-devel`で識別できます(`alsa-devel`パッケージ、`gimp-devel`パッケージ、`libkde4-devel`. パッケージなど)。

6.2.1 パッケージの信頼性の検証

RPMパッケージにはGPG署名があります。RPMパッケージの署名を検証するには、`rpm --checksig` *パッケージ*`-1.2.3.rpm`コマンドを使用して、Novell/SUSEまたはその他の信頼できるツールから送信されたパッケージかどうか判別します。これは、インターネットからアップデートパッケージを入手する場合には、特に推奨されます。

6.2.2 パッケージの管理:インストール、アップデート、およびアンインストール

通常RPMアーカイブのインストールはとても簡単です。`rpm -i` *`package`*`.rpm`の用に入力します。このコマンドで、パッケージをインストールできます。ただし、依存関係が満たされており、他のパッケージとの競合がない場合に限られます。`rpm`では、依存関係の要件を満たすためにインストールしなければならないパッケージがエラーメッセージで要求されます。バックグランドで、RPMデータベースは競合が起きないようにします。ある特定のファイルは、1つのパッケージだけにしか属せません。別のオプションを選択すると、`rpm`にこれらのデフォルト値を無視させることができますが、この処置を行うのは専門知識のある人に限られます。それ以外の人が行うと、システムの整合性を危うくするリスクが発生し、システムアップデート機能が損なわれる可能性があります。

`-U`または`--upgrade`と`-F`または`--freshen`の各オプションは、パッケージをアップデートするのに使用できます(たとえば、`rpm -F` *`package`*`.rpm`)。このコマンドは、古いバージョンのファイルを削除し、新しいファイルをた

だちにインストールします。2つのバージョン間の違いは、-Uがシステムに存在していなかったパッケージをインストールするのに対して、-Fがインストールされていたパッケージを単にアップデートする点にあります。アップデートする際、rpmは、以下のストラテジーに基づいて設定ファイルを注意深くアップデートします。

- 設定ファイルがシステム管理者によって変更されていない場合、rpmは新しいバージョンの適切なファイルをインストールします。システム管理者は、何も行う必要はありません。

- アップデートの前に設定ファイルがシステム管理者によって変更されている場合、rpmは変更されたファイルに拡張子.rpmorigまたは.rpmsave(バックアップファイル)を付けて保存し、新しいパッケージからファイルをインストールします。ただしこれは、元々インストールされていたファイルと新しいファイルのバージョンが異なる場合に限ります。異なる場合は、バックアップファイル(.rpmorigまたは.rpmsave)と新たにインストールされたファイルを比較して、新しいファイルに再度、変更を加えます。後ですべての.rpmorigと.rpmsaveファイルを必ず削除して、今後のアップデートで問題が起きないようにします。

- 設定ファイルがすでに存在しており、またnoreplaceラベルが.specファイルで指定されている場合、.rpmnewファイルが作成されます。

アップデートが終了したら、.rpmsaveファイルと.rpmnewファイルは、比較した後、将来のアップデートの妨げにならないように削除する必要があります。ファイルがRPMデータベースで認識されなかった場合、ファイルには拡張子.rpmorigが付けられます。

認識された場合には、.rpmsaveが付けられます。言い換えれば、.rpmorigは、RPM以外の形式からRPMにアップデートした結果として付けられます。.rpmsaveは、古いRPMから新しいRPMにアップデートした結果として付けられます。.rpmnewは、システム管理者が設定ファイルに変更を加えたかどうかについて、何の情報も提供しません。それらのファイルのリストは、/var/adm/rpmconfigcheckにあります。設定ファイルの中には(/etc/httpd/httpd.confなど)、操作が継続できるように上書きされないものがあります。

-Uスイッチは、単に-eオプションでアンインストールして、-iオプションでインストールする操作と同じではありません。可能なときは必ず–Uを使用します。

パッケージを削除するには、「rpm –e *package*.rpm」と入力します。解決されていない依存関係がない場合にパッケージのみを削除します。他のアプリケーションがTcl/Tkを必要とする限り、Tcl/Tkを削除することは理論的に不可能です。その場合でも、RPMはデータベースに援助を要求します。他の依存関係がない場合でも、また、どのような理由があってもそのような削除が不可能であれば、--rebuilddbオプションを使用してRPMデータベースを再構築するのがよいでしょう。

6.2.3 RPMとパッチ

システムの運用上のセキュリティを保証するには、ときどきアップデートパッケージをシステムにインストールする必要があります。以前は、パッケージ内のバグは、パッケージ全体を交換しなければ取り除けませんでした。バグのある小さなファイルが含まれる大きなパッケージでは、このようなシナリオに陥りがちでした。しかし、SUSE RPMを使用すると、パッケージ内にパッチをインストールできます。

最も重要な考慮事項について、pineを例として説明します。

パッチRPMはシステムに適したものか。
: これを検査するには、はじめにインストールされたパッケージでクエリーを行います。pineでは、次のコマンドを実行します。

```
rpm –q pine
pine-4.44-188
```

: パッチRPMがこのバージョンのpineに適しているかどうかを検証します。

```
rpm –qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

: このパッチは、3種類のバージョンのpineに適しています。例でインストールされたバージョンもリストされています。パッチはインストールできます。

どのファイルがパッチで置き換えられるか。

パッチの影響を受けるファイルは、パッチRPMで簡単に見つけられます。rpmの-Pパラメータを使用すると、特殊なパッチ機能を選択できます。次のコマンドでファイルをリストします。

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

パッチがすでにインストールされていれば、次のコマンドを使用します。

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

パッチRPMをどのようにシステムにインストールするか。

パッチRPMは、通常のRPMと同様に使用されます。唯一の違いは、適切なRPMがすでにインストールされていなければならない点です。

どのパッチがシステムにインストールされており、それらはどのパッケージバージョンのものか。

システムにインストールされているすべてのパッチのリストは、コマンドrpm -qPaで表示できます。(この例のように)新しいシステムに1つのパッチだけがインストールされている場合、リストは次のようになります。

```
rpm -qPa
pine-4.44-224
```

後日、オリジナルとしてインストールされていたパッケージのバージョンを知りたい場合、その情報はRPMデータベースから得られます。pineの場合、その情報は次のコマンドで表示できます。

```
rpm -q --basedon pine
pine = 4.44-188
```

RPMのパッチ機能に関する情報を含む詳細な情報は、man rpmコマンドとrpmbuildコマンドのマニュアルページで収集できます。

注記: SUSE Linux Enterprise Serverの公式アップデート

アップデートのダウンロードサイズをできる限り小さくするため、SUSE Linux Enterprise Serverの公式アップデートはパッチRPMとしてではなく、デ

ルタRPMパッケージとして提供されます。詳細については、6.2.4項 「デルタRPMパッケージ」 (76 ページ)を参照してください。

6.2.4 デルタRPMパッケージ

デルタRPMパッケージには、RPMパッケージの新旧バージョン間の違いが含まれています。デルタRPMを古いRPMに適用すると、まったく新しいRPMになります。デルタRPMは、インストールされているRPMとも互換性があるので、古いRPMのコピーを保管する必要はありません。デルタRPMパッケージは、パッチRPMよりもさらに小さく、パッケージをインターネット上で転送するのに便利です。欠点は、デルタRPMが組み込まれたアップデート操作の場合、そのままのRPMまたはパッチRPMに比べて、CPUサイクルの消費が目立って多くなることです。

prepdeltarpm、writedeltarpm、およびapplydeltarpmバイナリは、デルタRPMスィート(deltarpmパッケージ)の一部であり、デルタRPMパッケージの作成と適用に際して役立ちます。次のコマンドを使用して、new.delta.rpmというデルタRPMを作成します。次のコマンドでは、old.rpmおよびnew.rpmが存在することが前提となります。

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

最後に、一時作業ファイルold.cpio、new.cpio、およびdeltaを削除します。

古いパッケージがすでにインストールされていれば、applydeltarpmを使用して、ファイルシステムから新たにRPMを構築できます。

```
applydeltarpm new.delta.rpm new.rpm
```

ファイルシステムにアクセスすることなく、古いRPMから構築するには、-rオプションを使用します。

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

技術的な詳細については、/usr/share/doc/packages/deltarpm/READMEを参照してください。

6.2.5 RPMクエリー

-qオプションを使用すると、rpmはクエリを開始し、(-pオプションを追加することにより)RPMアーカイブを検査できるようにして、インストールされたパッケージのRPMデータベースでクエリを行えるようにします。必要な情報の種類を指定する複数のスイッチを使用できます。詳細については、表6.1「最も重要なRPMクエリーのオプション」 (77 ページ)を参照してください。

表 6.1 *最も重要なRPMクエリーのオプション*

-i	パッケージ情報
-l	ファイルリスト
-f FILE	ファイル*FILE*を含むパッケージでクエリーを行います(*FILE*にはフルパスを指定する必要があります)。
-s	ステータス情報を含むファイルリスト(-lを暗示指定)
-d	ドキュメントファイルだけをリストします (-lを暗示指定)。
-c	設定ファイルだけをリストします (-lを暗示指定)。
--dump	詳細情報を含むファイルリスト (-l、-c、または-d と共に使用します)
--provides	他のパッケージが--requiresで要求できるパッケージの機能をリストします。
--requires, -R	パッケージが要求する機能

`--scripts`	インストールスクリプト (preinstall、postinstall、uninstall)

たとえば、コマンド`rpm -q -i wget`は、例6.2「rpm -q -i wget」 (78 ページ)に示された情報を表示します。

例 6.2 rpm -q -i wget

```
Name        : wget                         Relocations: (not relocatable)
Version     : 1.11.4                            Vendor: openSUSE
Release     : 1.70                          Build Date: Sat 01 Aug 2009
09:49:48 CEST
Install Date: Thu 06 Aug 2009 14:53:24 CEST      Build Host: build18
Group       : Productivity/Networking/Web/Utilities   Source RPM:
wget-1.11.4-1.70.src.rpm
Size        : 1525431                           License: GPL v3 or later
Signature   : RSA/8, Sat 01 Aug 2009 09:50:04 CEST, Key ID b88b2fd43dbdc284
Packager    : http://bugs.opensuse.org
URL         : http://www.gnu.org/software/wget/
Summary     : A Tool for Mirroring FTP and HTTP Servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

オプション`-f`が機能するのは、フルパスで完全なファイル名を指定した場合だけです。必要な数のファイル名を指定します。たとえば、次のコマンドを実行します。

```
rpm -q -f /bin/rpm /usr/bin/wget
```

出力は次のとおりです。

```
rpm-4.8.0-4.3.x86_64
wget-1.11.4-11.18.x86_64
```

ファイル名の一部分しかわからない場合は、例6.3「パッケージを検索するスクリプト」 (78 ページ)に示すようなシェルスクリプトを使用します。実行するときに、ファイル名の一部を、パラメータとして示されるスクリプトに渡します。

例 6.3 パッケージを検索するスクリプト

```
#! /bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
```

```
    echo ""
done
```

rpm -q --changelog rpm コマンドは、特定のパッケージ(この場合はrpmパッケージ)に関する詳細な変更情報を日付順に一覧しますの詳細なリストを表示します。

インストールされたRPMデータベースを使うと、確認検査を行うことができます。それらの検査は、-V、-y、または--verifyオプションを使用して開始します。このオプションを使うと、rpmは、パッケージ内にあり、インストール以降変更されたことがあるすべてのファイルを表示します。rpmは、次の変更に関するヒントを表示するのに、8文字の記号を使用します。

表 6.2　RPM確認オプション

5	MD5チェックサム
S	ファイルサイズ
L	シンボリックリンク
T	変更時間
D	メジャーデバイス番号とマイナーデバイス番号
U	所有者
G	グループ
M	モード (許可とファイルタイプ)

設定ファイルの場合は、文字cが表示されます。/etc/wgetrc(wgetパッケージ)の変更例を以下に示します。

```
rpm -V wget
S.5....T c /etc/wgetrc
```

RPMデータベースのファイルは、/var/lib/rpmに格納されています。パーティション/usrのサイズが1GBであれば、このデータベースは、完全なアップデート後、およそ 30 MB占有します。データベースが予期していたよりも

はるかに大きい場合は、オプション--rebuilddbでデータベースを再構築するようにします。再構築する前に、古いデータベースのバックアップを作成しておきます。cronスクリプトのcron.dailyは、データベースのコピー(gzipでパックされる)を毎日作成し、/var/adm/backup/rpmdbに格納します。コピー数は/etc/sysconfig/backupにある変数MAX_RPMDB_BACKUPSで制御します(デフォルト:5)。1つのバックアップのサイズは、1GBの/usrに対しておよそ1MBです。

6.2.6 ソースパッケージのインストールとコンパイル

すべてのソースパッケージには、拡張子.src.rpm(ソースRPM)が付けられています。

注記: インストール済みのソースパッケージ

ソースパッケージは、インストールメディアからハードディスクにコピーされ、YaSTを使用して展開できます。ただし、ソースパッケージは、パッケージマネージャでインストール済み([i])というマークは付きません。これは、ソースパッケージがRPMデータベースに入れられないためです。*インストールされた*オペレーティングシステムソフトウェアだけがRPMデータベースにリストされます。ソースパッケージを「インストールする」場合、ソースコードだけがシステムに追加されます。

(/etc/rpmrcなどのファイルでカスタム設定を指定していない限り)以下のディレクトリが、/usr/src/packagesの下でrpmとrpmbuildから使用可能でなければなりません。

SOURCES
: オリジナルのソース(.tar.gzファイルや.tar.gzファイルなど)とディストリビューション固有の調整ファイル(ほとんどの場合.difファイルや.patchファイル)用です。

SPECS
: *ビルド*処理を制御する、メタMakefileに類似した.specファイル用です。

BUILD
すべてのソースは、このディレクトリでアンパック、パッチ、およびコンパイルされます。

RPMS
完成したバイナリパッケージが格納されます。

SRPMS
ソースRPMが格納されます。

YaSTを使ってソースパッケージをインストールすると、必要なすべてのコンポーネントが/usr/src/packagesにインストールされます。ソースと調整はSOURCES、関連する.specファイルはSPECSに格納されます。

警告

システムコンポーネント(glibc、rpm、sysvinitなど)で実験してはいけません。システムが正しく動作しなくなります。

次の例は、wget.src.rpmパッケージを使用します。ソースパッケージをインストールすると、次のようなファイルが生成されます。

```
/usr/src/packages/SOURCES/wget-1.11.4.tar.bz2
/usr/src/packages/SOURCES/wgetrc.patch
/usr/src/packages/SPECS/wget.spec
```

rpmbuild -b *X* /usr/src/packages/SPECS/wget.specコマンドは、コンパイルを開始します。*X*は、ビルド処理のさまざまな段階に対して使用されるワイルドカードです(詳細については、--helpの出力またはRPMのドキュメントを参照してください)。以下に簡単な説明を示します。

-bp
/usr/src/packages/BUILD内のソースを用意します。アンパック、パッチしてください。

-bc
-bpと同じですが、コンパイルを実行します。

-bi
: -bpと同じですが、ビルドしたソフトウェアをインストールします。警告: パッケージがBuildRoot機能をサポートしていない場合は、設定ファイルが上書きされることがあります。

-bb
: -biと同じですが、バイナリパッケージを作成します。コンパイルに成功すると、バイナリパッケージは、/usr/src/packages/RPMSに作成されるはずです。

-ba
: -bbと同じですが、ソース RPMを作成します。コンパイルに成功すると、バイナリは/usr/src/packages/SRPMSに作成されるはずです。

--short-circuit
: 一部のステップをスキップします。

作成されたバイナリRPMは、rpm -iコマンドまたはrpm -Uコマンドでインストールできます。rpmを使用したインストールは、RPMデータベースに登場します。

6.2.7 buildによるRPMパッケージのコンパイル

多くのパッケージにつきものの不都合は、ビルド処理中に不要なファイルが稼働中のシステムに追加されてしまうことです。これを回避するには、パッケージのビルド先の定義済みの環境を作成するbuildを使用します。このchroot環境を確立するには、build スクリプトが完全なパッケージツリーと共に提供されなければなりません。パッケージツリーは、NFS経由で、またはDVDから ハードディスク上で利用できるようにすることができます。build --rpms *directory*で、位置を指定します。rpmと異なり、buildコマンドは、ソースディレクトリで.specファイルを検索します。/media/dvdの下でシステムにマウントされているDVDを使用して(上記の例と同様に)wgetをビルドするには、次のコマンドをrootとして使用します。

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

これで、最小限の環境が/var/tmp/build-rootに確立されます。パッケージは、この環境でビルドされます。処理が完了すると、ビルドされたパッケージは/var/tmp/build-root/usr/src/packages/RPMSに格納されます。

buildスクリプトでは、他のオプションも多数使用できます。たとえば、スクリプトがユーザ独自のRPMを処理するようにするには、ビルド環境の初期化を省略するか、rpmコマンドの実行を上記のビルド段階のいずれかに制限します。build --helpコマンドとman buildコマンドで、詳細な情報が得られます。

6.2.8 RPMアーカイブとRPMデータベース用のツール

Midnight Commander (mc)は、RPMアーカイブの内容を表示し、それらの一部をコピーできます。アーカイブを仮想ファイルシステムとして表し、Midnight Commanderの通常のメニューオプションを使用できます。<F3>キーを使用してHEADERを表示します。カーソルキーとEnterキーを使ってアーカイブ構造を表示します。F5キーを使用してアーカイブコンポーネントをコピーします。

フル機能のパッケージマネージャをYaSTモジュールとして使用できます詳細については、第9章 *ソフトウェアをインストールまたは削除する* (↑*導入ガイド*)を参照してください。

7 BashとBashスクリプト

今日、多数のユーザが、KDEやGNOMEなどのGUI(グラフィカルユーザインターフェース)を介してコンピュータを使用しています。GUIは多くの機能を備えていますが、自動タスクの実行という点では、その用途は限られます。シェルは、GUIに追加すると便利なツールです。この章では、シェル(ここではBash)のいくつかの側面について概説します。

7.1 「シェル」とは何か?

従来、*シェル*とは、Bash(Bourne again Shell)のことでした。この章では、Bashを「シェル」と呼びます。実際にはシェルはBashの他にもあり(ash、csh、ksh、zsh、…)、異なる機能と特性を持っています。他のシェルの詳細については、YaSTで*シェル*を検索してください。

7.1.1 Bash設定ファイルの知識

シェルは、次のようにして呼び出すことができます。

1. **対話型ログインシェル** コンピュータへのログイン時に、`--login`オプションを使用してBashを呼び出す場合か、SSHを使用してリモートコンピュータへログインする場合に使用します。

2. **「通常の」対話型シェル** xtermやkonsole、gnome-terminalなどのツールの起動時には、通常、この形式を使用します。

3. **非対話型シェル** コマンドラインからシェルスクリプトを呼び出す場合に使用します。

使用するシェルのタイプによって、異なる設定ファイルを読み込みます。次のテーブルには、それぞれ、ログインシェル設定ファイルと非ログインシェル設定ファイルが示されています。

表 7.1 *ログインシェル用Bash設定ファイル*

ファイル	説明
`/etc/profile`	このファイルは変更しないでください。変更しても、次の更新で変更内容が破棄される可能性があります。
`/etc/profile.local`	`/etc/profile`を拡張する場合は、このファイルを使用します。
`/etc/profile.d/`	特定プログラムのシステム全体に渡る設定ファイルを含みます。
`~/.profile`	ログインシェル用のユーザ固有の設定をここに挿入します。

表 7.2 *非ログインシェル用Bash設定ファイル*

`/etc/bash.bashrc`	このファイルは変更しないでください。変更しても、次の更新で変更内容が破棄される可能性があります。
`/etc/bash.bashrc.local`	Bashのシステム全体に渡る変更を挿入する場合のみ、このファイルを使用します。
`~/.bashrc`	ユーザ固有の設定をここに挿入します。

さらに、Bashでは、次のファイルも使用します。

表 7.3　Bash用特殊ファイル

ファイル	説明
~/.bash_history	入力したすべてのコマンドのリストを含みます。
~/.bash_logout	ログアウト時に実行されます。

7.1.2 ディレクトリの構造

次のテーブルでは、Linuxシステムの最も重要な上位レベルディレクトリについて、短い概要を示します。それらのディレクトリおよび重要なサブディレクトリの詳細については、後続のリストを参照してください。

表 7.4　標準的なディレクトリツリーの概要

ディレクトリ	目次
/	ルートディレクトリ—ディレクトリツリーの開始点
/bin	システム管理者および通常ユーザの両者が必要とするコマンドなどの必須バイナリファイル。通常、Bashなどのシェルも含みます。
/boot	ブートローダの静的ファイル
/dev	ホスト固有のデバイスのアクセスに必要なファイル
/etc	ホスト固有のシステム設定ファイル
/home	システムにアカウントを持つすべてのユーザのホームディレクトリを格納します。ただし、rootの

ディレクトリ	目次
	ホームディレクトリは、/homeでなく、/rootにあります。
/lib	必須の共有ライブラリおよびカーネルモジュール
/media	リムーバブルメディアのマウントポイント
/mnt	ファイルシステムを一時的にマウントするためのマウントポイント
/opt	アドオンアプリケーションのソフトウェアパッケージ
/root	スーパーユーザrootのホームディレクトリ
/sbin	必須のシステムバイナリ
/srv	システムで提供するサービスのデータ
/tmp	一時ファイルを格納するディレクトリ
/usr	読み込み専用データを含む第二階層
/var	ログファイルなどの可変データ
/windows	システムにMicrosoft Windows*とLinuxの両方がインストールされる場合のみ利用可能。Windowsデータを含みます。

次のリストでは、さらに詳しい情報を提供し、ディレクトリに含まれるファイルおよびサブディレクトリの例を示します。

/bin
: rootと他のユーザの両者が使用できる基本的なシェルコマンドを含みます。これらのコマンドは、ls、mkdir、cp、mv、rm、rmdirなどです。/binには、SUSE Linux Enterprise Serverのデフォルトシェルである Bashも含まれます。

/boot
: ブートに必要なデータ(ブートローダやカーネルのデータなど)と、その他のデータ(カーネルがユーザモードプログラムの実行を開始する前に使用)が含まれます。

/dev
: ハードウェアコンポーネントを記述したデバイスファイルを格納します。

/etc
: X Window Systemなどのプログラムの動作を制御するローカル設定ファイルを含みます。/etc/init.dサブディレクトリは、ブートプロセスで実行されるスクリプトを含みます。

/home/*username*
: システムにアカウントを持つすべてのユーザの個人データを格納します。このディレクトリ内のファイルは、その所有者またはシステム管理者しか変更できません。デフォルトでは、電子メールのディレクトリとパーソナルデスクトップの設定が、非表示のファイルおよびディレクトリとして、ここに格納されます。デスクトップ用個人設定データは、KDEユーザの場合は.kde4、GNOMEユーザの場合は.gconfに格納されています。

注記: ネットワーク環境でのホームディレクトリ

ネットワーク環境で作業するユーザのホームディレクトリは、/home以外のファイルシステム内のディレクトリにマップできます。

/lib
: システムのブートとルートファイルシステムでのコマンドの実行に必要な必須共有ライブラリを含みます。Windowsで共有ライブラリに相当するものは、DLLファイルです。

/media
CD-ROM、USBスティック、デジタルカメラ(USBを使用する場合)など、リムーバブルメディアのマウントポイントを含みます。/mediaでは、一般にシステムのハードディスク以外のあらゆるタイプのドライブが保持されます。リムーバブルメディアをシステムに挿入または接続し、マウントを完了すると、ただちに、そのメディアにこのディレクトリからアクセスできます。

/mnt
このディレクトリは一時的にマウントされるファイルシステムのマウントポイントを提供します。rootがここでファイルシステムをマウントできます。

/opt
サードパーティのソフトウェアのインストール用に予約されています。オプションソフトウェアや大型アドオンプログラムのパッケージをここに格納できます。

/root
rootユーザのホームディレクトリ。rootの個人データがここに保存されます。

/sbin
sで示唆されるように、このディレクトリはスーパーユーザ用のユーティリティを格納します。/sbinには、/bin内のバイナリとともにシステムのブート、復元、および回復に不可欠なバイナリを含みます。

/srv
FTPやHTTPなど、システムによって提供されるサービスのデータを格納します。

/tmp
ファイルの一時的保管を必要とするプログラムによって使用されます。

重要: ブート時の/tmpのクリーンアップ

/tmpに保存したデータは、システムのリブート後も残っているかは保証できません。これは、たとえば、/etc/sysconfig/cron内の設定によって左右されます。

/usr
: /usrは、ユーザとは無関係であり、UNIX system resourcesを意味する略語です。/usr内のデータは静的な読み込み専用データです。このデータは、FHS(Filesystem Hierarchy Standard)に準拠するホスト間で共有できます。このディレクトリは、すべてのアプリケーションプログラムを含み、ファイルシステム内の第二階層を形成します。KDE4とGNOMEも、このディレクトリに格納されています。/usrには、/usr/bin、/usr/sbin、/usr/local、/usr/share/docなど、多数のサブディレクトリがあります。

/usr/bin
: 一般ユーザがアクセスできるプログラムを含みます。

/usr/sbin
: 修復関数など、システム管理者用に予約されたプログラムを含みます。

/usr/local
: このディレクトリには、システム管理者がディストリビューションに依存しないローカルな拡張プログラムをインストールできます。

/usr/share/doc
: システムのドキュメントファイルおよびリリースノートを格納します。manualサブディレクトリには、このマニュアルのオンラインバージョンが格納されます。複数の言語をインストールする場合は、このディレクトリに各言語のマニュアルを格納できます。

  packagesには、システムにインストールされたソフトウェアパッケージに含まれているドキュメントが格納されます。パッケージごとに、サブディレクトリ/usr/share/doc/packages/*packagename*が作成されます。このサブディレクトリには、多くの場合、パッケージのREADMEファイルが含まれます。例、設定ファイル、または追加スクリプトが含まれる場合もあります。

  HOWTOをシステムにインストールした場合は、/usr/share/docにhowtoサブディレクトリも含まれます。このサブディレクトリには、Linuxソフトウェアの設定および操作に関する多数のタスクの追加ドキュメントが格納されます。

/var
: /usrは静的な読み込み専用データを含みますが、/varは、システム動作時に書き込まれる可変データ(ログファイル、スプールデータなど)のディレクトリです。/var/log/にある重要なログファイルの概要は、表35.1「ログファイル」 (604 ページ)を参照してください。

7.2 シェルスクリプトの作成

シェルスクリプトは、データの収集、テキスト内のワードやフレーズの検索など、あらゆる種類の多数の有用なタスクの実行に便利な方法です。次の例では、小型のシェルスクリプトでテキストをプリントします。

例 7.1 テキストをプリントするシェルスクリプト

```
#!/bin/sh ❶
# Output the following line: ❷
echo "Hello World" ❸
```

❶ 1行目は、このファイルがスクリプトであることを示す*Shebang*文字(#!)で始まります。スクリプトは、Shebang文字の後に指定されたインタープリタ(ここでは、/bin/sh)を使用して実行されます。

❷ 2行目は、ハッシュ記号で始まるコメントです。スクリプトの動作を覚えにくい行には、コメントすることをお勧めします。

❸ 3番目の行で、組み込みコマンドechoを使用して、対応するテキストを出力します。

このスクリプトの実行には、次の前提条件が必要です。

1. 各スクリプトは、Shebang行を含む必要があります(この例はすでに示しました)。スクリプトにこの行がない場合は、手動でインタープリタを呼び出します。

2. スクリプトの保存場所はどこでも構いません。ただし、シェルの検索先ディレクトリを保存場所にすることをお勧めします。シェルのサーチパスは、環境変数PATHで設定されます。一般に、標準ユーザには/usr/binへの書き込みアクセスはありません。このため、スクリプトはユーザのディレクトリ~/bin/に保存することを推奨します。上記の例では、名前はhello.shです。

3. スクリプトには、実行可能パーミッションが必要です。次のコマンドで、パーミッションを設定してください。

```
chmod +x ~/bin/hello.sh
```

これらの前提条件をすべて満たしたら、次の方法でスクリプトを実行できます。

1. **絶対パス** スクリプトは絶対パスで実行できます。この例では、`~/bin/hello.sh`です。

2. **任意の場所** `PATH`環境変数にスクリプトが存在するディレクトリが含まれている場合、スクリプトを`hello.sh`だけで実行できます。

7.3 コマンドイベントのリダイレクト

各コマンドは、入力または出力用として、3つのチャネルを使用できます。:

- **標準出力** デフォルトの出力チャネル。コマンドで何かをプリントする際には標準出力チャネルが使用されます。
- **標準入力** コマンドでユーザまたは他のコマンドからの入力を必要とする場合は、このチャネルが使用されます。
- **標準エラー** このチャネルは、エラーレポーティングに使用されます。

これらのチャネルをリダイレクトするには、次の方法を使用できます。

`Command > File`
: コマンド出力をファイルに保存します。既存ファイルは削除されます。たとえば、`ls`コマンドの出力を`listing.txt`ファイルに書き込みます。

```
ls > listing.txt
```

`Command >> File`
: コマンド出力をファイルに追加します。たとえば、`ls`コマンドの出力を`listing.txt`ファイルに追加します。

```
ls >> listing.txt
```

Command < File
: ファイルを読み込み、指定されたコマンドへの入力とします。たとえば、ファイルのコンテンツをreadコマンドで読み込み、変数に入力します。

```
read a < foo
```

Command1 | Command2
: 左側のコマンドの出力を右側のコマンドの入力にします。たとえば、catコマンドは/proc/cpuinfoファイルの内容を出力します。この出力をgrepで使用して、cpuを含む行のみをフィルタします。

```
cat /proc/cpuinfo | grep cpu
```

各チャネルには、対応するファイル記述子があります。標準入力には0(ゼロ)、標準出力には1、標準エラーには2が割り当てられています。このファイル記述子を<文字または>文字の前に挿入できます。たとえば、次の行では、fooで始まるファイルを検索しますが、そのファイルを/dev/nullにリダイレクトすることでエラーメッセージを抑制します。

```
find / -name "foo*" 2>/dev/null
```

7.4 エイリアスの使用

エイリアスは、1つ以上のコマンドのショートカット定義です。エイリアスの構文は、次の通りです。

```
alias NAME=DEFINITION
```

たとえば、次の行は、エイリアスltを定義しています。このエイリアスは、長いリストを出力し(-lオプション)、そのリストを変更時刻でソートし(-tオプション)、ソート順と逆の順序で出力します(-rオプション)。

```
alias lt='ls -ltr'
```

すべてのエイリアス定義を表示するには、aliasを使用します。unaliasで対応するエイリアス名を指定して、エイリアスを削除します。

7.5 Bashでの変数の使用

シェル変数は、グローバル変数またはローカル変数として使用できます。グローバル変数(つまり、環境変数)は、すべてのシェルでアクセスできます。対照的に、ローカル変数は、現在のシェルでのみアクセスできます。

すべての環境変数を表示するには、printenvコマンドを使用します。変数の値を知る必要がある場合は、変数の名前を引数として挿入します。

```
printenv PATH
```

変数はグローバルでもローカルでも、echoで表示できます。

```
echo $PATH
```

ローカル変数を設定するには、変数名の後に等号を入れ、その後に値を指定します。

```
PROJECT="SLED"
```

等号の前後にスペースを挿入しないでください。スペースを挿入すると、エラーになります。環境変数を設定するには、exportを使用します。

```
export NAME="tux"
```

変数を削除するには、unsetを使用します。

```
unset NAME
```

次のテーブルに、シェルスクリプトで使用できる共通環境変数を示します。

表 7.5 便利な環境変数

HOME	現在のユーザのホームディレクトリ
HOST	現在のホスト名
LANG	ツールをローカライズする場合、ツールは、この環境変数からの言語を使用します。英語をCに設定することも可能です。

PATH	シェルのサーチパス。コロンで区切ったディレクトリのリスト
PS1	各コマンドの前にプリントされる通常のプロンプトを指定します。
PS2	複数行コマンドの実行時にプリントされるセカンダリプロンプトを指定します。
PWD	現在の作業ディレクトリ
ユーザ	現在のユーザ

7.5.1 引数変数の使用

たとえば、スクリプトfoo.shは、次のように実行できます。

```
foo.sh "Tux Penguin" 2000
```

スクリプトに渡される引数すべてにアクセスするには、位置パラメータが必要です。これらのパラメータは、最初の引数には$1、2つ目の引数には$2という順序で割り当てます。パラメータは最大9つまで使用できます。スクリプト名を取得するには、$0を使用します。

次のスクリプトfoo.shは、1から4までのすべての引数をプリントします。

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

このスクリプトを既出例の引数を使用して実行すると、次の結果が出力されます。

```
"Tux Penguin" "2000" "" ""
```

7.5.2 変数置換の使用

変数置換では、変数のコンテンツに、左側または右側からパターンを適用します。次のリストに、可能な構文形式を示します。

`${VAR#pattern}`
左側から最も短い一致を削除します。

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##pattern}`
左側から最も長い一致を削除します。

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

`${VAR%pattern}`
右側から最も短い一致を削除します。

```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%pattern}`
右側から最も長い一致を削除します。

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

`${VAR/pattern_1/pattern_2}`
*VAR*のコンテンツを*pattern_1*から*pattern_2*に置換します。

```
file=/home/tux/book/book.tar.bz2
echo ${file/tux/wilber}
/home/wilber/book/book.tar.bz2
```

7.6 コマンドのグループ化と結合

シェルでは、条件付き実行のため、コマンドを結合し、グループ化することができます。各コマンドが返す終了コードにより、コマンドの成功または失敗が判別されます。終了コードが0(ゼロ)の場合、コマンドは成功しました。それ以外はすべて、コマンド固有のエラーをマークします。

次のリストでは、コマンドをグループ化する方法を一覧します。

`Command1 ; Command2`
コマンドをシーケンシャルに実行します。終了コードはチェックされません。次の行では、各コマンドの終了コードにかかわらず、catでファイルのコンテンツを表示し、次に、lsでファイルプロパティをプリントします。

```
cat filelist.txt ; ls -l filelist.txt
```

`Command1 && Command2`
左のコマンドが成功した場合、右のコマンドを実行します(論理AND)。次の行では、ファイルのコンテンツを表示し、そのコマンドが成功した場合のみ、ファイルのプロパティをプリントします(このリストの前の項目と比較してください)。

```
cat filelist.txt && ls -l filelist.txt
```

`Command1 || Command2`
左のコマンドが失敗した場合、右のコマンドを実行します(論理OR)次の行では、/home/tux/fooでのディレクトリ作成に失敗した場合のみ、/home/wilber/bar内にディレクトリを作成します。

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

`funcname(){ ... }`
シェル関数を作成します。位置パラメータを使用して、関数の引数にアクセスできます。次の行では、短いメッセージをプリントする関数helloを定義します。

```
hello() { echo "Hello $1"; }
```

この関数は、次のように呼び出せます。

```
hello Tux
```

結果は、次のようにプリントされます。

```
Hello Tux
```

7.7 よく使用されるフローコンストラクトの操作

スクリプトのフローを制御するため、シェルでは、while、if、for、およびcaseの各構文を使用します。

7.7.1 if制御コマンド

ifコマンドは、式のチェックに使用されます。たとえば、次のコードは、現在のユーザがTuxであるかどうかをテストします。

```
if test $USER = "tux"; then
  echo "Hello Tux."
else
  echo "You are not Tux."
fi
```

テスト式は、複雑にすることも、シンプルにすることも可能です。次の式は、ファイルfoo.txtが存在するかどうかをチェックします。

```
if test -e /tmp/foo.txt ;
then
  echo "Found foo.txt"
fi
```

test式は、角括弧で短縮することもできます。

```
if [ -e /tmp/foo.txt ] ; then
  echo "Found foo.txt"
fi
```

その他の役に立つ式については、http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lsst/ch03sec02.htmlを参照してください。

7.7.2 ｆorコマンドによるループの作成

forループを使用すると、エントリのリストにコマンドを実行できます。たとえば、次のコードは、現在のディレクトリ内のPNGファイルの情報をプリントします。

```
for i in *.png; do
 ls -l $i
done
```

7.8 詳細情報

Bashに関する重要な情報は、マニュアルページman shに記載されています。このトピックの詳細については、次のリストを参照してください。

- http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html—「Bash Guide for 」
- http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html—「BASH Programming - Introduction HOW-TO」
- http://tldp.org/LDP/abs/html/index.html—「Advanced Bash-Scripting Guide」
- http://www.grymoire.com/Unix/Sh.html—「Sh - the Bourne Shell」

パート II. 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

8

SUSE® Linux Enterprise Serverは、複数の64ビットプラットフォームで利用できます。ただし、付属のすべてのアプリケーションが64ビットプラットフォームに移植されている訳ではありません。SUSE Linux Enterprise Serverは、32ビットアプリケーションの64ビットシステム環境での使用をサポートしています。この章では、このサポートを64ビットSUSE Linux Enterprise Server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についても説明します。

64ビットプラットフォームia64、ppc64、System z、およびx86_64版SUSE Linux Enterprise Serverは、64ビット環境で既存の32ビットアプリケーションをそのまま実行できるように設計されています。「」対応する32ビットプラットフォームには、ia64のx86、ppc64のppc、およびx86_64のx86があります。このサポートにより、対応する 64ビット移植版が使用可能になるのを待たなくても、使用したい 32ビットアプリケーションを引き続き使用できます。現在のppc64システムは、大部分のアプリケーションを 32ビットモードで実行しますが、 64ビットアプリケーションを実行することもできます。

8.1 ランタイムサポート

重要: アプリケーションバージョン間の競合

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。

PAM(プラグ可能認証モジュール)は、このルールの例外です。SUSE Linux Enterprise Serverは、ユーザとアプリケーションを仲介するレイヤとしての認証プロセスでPAMを使用します。また、 32ビットアプリケーションも実行する64ビットオペレーティングシステムでは、常に両バージョンのPAMモジュールをインストールする必要があります。

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じシステム内の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および/usr/libの下にある64ビットのオブジェクトファイルは、/lib64および/usr/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および/usr/libの下になっています。

ワードサイズに依存しないデータコンテンツを持つ、32ビットの/libディレクトリ中のサブディレクトリは移動されません。このスキームは、LSB (Linux Standards Base)とFHS (File System Hierarchy Standard)に準拠しています。

► **ipf:** ia64用の64ビットライブラリは、標準libディレクトリ内にあり、lib64ディレクトリもlib32ディレクトリも存在しません。ia64は、32ビットx86コードをエミュレーションで実行します。基本的なライブラリセットは、/emul/

ia32-linux/libおよび/emul/ia32-linux/usr/libにインストールされます。 ◀

8.2 ソフトウェア開発

すべての64ビットアーキテクチャで、64ビットオブジェクトの開発がサポートされています。32ビットコンパイル機能のサポートレベルは、アーキテクチャによって異なります。32ビットコンパイル機能は、GCC (GNU Compiler Collection)やbinutilsによるツールチェーンの各種実装オプションになっています。Binutilsには、アセンブラasとリンカーldが含まれています。

biarchコンパイラ
: 32ビットと64ビットのオブジェクトはどちらもbiarch開発ツールチェーンで生成できます。biarch開発ツールチェーンを使用して、32ビットと64ビットのオブジェクトを生成できます。ほぼすべてのプラットフォームにおいて、デフォルトでは64ビットオブジェクトのコンパイルが実行されます。32ビットオブジェクトは、特殊なフラグを使用すれば生成できます。この特殊なフラグは、GCCでは-32です。binutilsのフラグはアーキテクチャによって異なりますが、GCCは正しいフラグをリンカーやアセンブラに転送します。現在では、amd64(x86とamd64の開発をサポート)、System z、およびppc64用のbiarch開発ツールチェーンが存在します。通常、32ビットオブジェクトはppc64プラットフォームで作成されます。-m64フラグは、64ビットオブジェクトの生成に使用する必要があります。

未サポート
: SUSE Linux Enterprise Serverでは、すべてのプラットフォームで32ビットソフトウェアを直接開発できるとは限りません。ia64でx86用のアプリケーションを開発するには、対応する32ビットバージョンのSUSE Linux Enterprise Serverを使用します。

すべてのヘッダファイルは、アーキテクチャに依存しない形式で作成する必要があります。インストール済みの32ビットと64ビットのライブラリには、インストール済みのヘッダファイルに対応するAPI (アプリケーションプログラミングインタフェース)が必要です。標準のSUSE Linux Enterprise Server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。

8.3 biarchプラットフォームでのソフトウェアのコンパイル

biarchアーキテクチャで他のアーキテクチャ向けのバイナリを開発するには、対象のアーキテクチャのそれぞれのライブラリをさらにインストールする必要があります。こうしたパッケージは、対象のアーキテクチャが-32ビットアーキテクチャである場合はrpmname- 32bitまたはrpmname-x86(ia64の場合)と呼ばれ、対象のアーキテクチャが-64ビットアーキテクチャである場合はrpmname- 64bitと呼ばれます。さらに、rpmname-develパッケージからそれぞれのヘッダとライブラリ、また、rpmname-devel-32bitまたはrpmname-devel-64bitから対象のアーキテクチャ向けの開発ライブラリも必要です。

たとえば、対象のアーキテクチャが32ビットアーキテクチャ(x86_64またはSystem z)であるシステムでlibaioを使用するプログラムをコンパイルするには、次のRPMが必要です。

libaio-32bit
: 32ビットランタイムパッケージ

libaio-devel-32bit
: 32ビット開発用のヘッダとライブラリ

libaio
: 64ビットランタイムパッケージ

libaio-devel
: 64ビット開発用のヘッダとライブラリ

ほとんどのオープンソースプログラムでは、autoconfベースのプログラム設定が使用されています。対象のアーキテクチャ向けプログラムの設定にautoconfを使用するには、autoconfの標準のコンパイラとリンカーの設定に上書きするために、さらに環境変数を指定してconfigureスクリプトを実行します。

次の例は、対象のアーキテクチャとしてx86を採用しているx86_64システムを示しています。対象のアーキテクチャとしてppcを採用しているppc64の場合

も同様です。この例は、32ビットパッケージをビルドできないia64には適用されません。

1 32ビットコンパイラを使用します。

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

2 リンカーに32ビットオブジェクトの処理を指示します(リンカーのフロントエンドには常にgccを使用)。

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

3 32ビットオブジェクトを生成するためにアセンブラを設定します。

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

4 次に示すような、32ビットライブラリの場所などのリンカフラグを指定します。

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

5 32ビットオブジェクトコードライブラリの場所を指定します。

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

6 32ビットXライブラリの場所を指定します。

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

こうした変数のすべてがどのプログラムにも必要なわけではありません。それぞれのプログラムに合わせて使用してください。

x86__64、ppc64、またはSystem zでネイティブの32ビットアプリケーションをコンパイルする場合の、configureコールの例を次に示します。

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

8.4 カーネル仕様

x86_64、ppc_64およびSystem z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すべてのAPIをサポートしていません。ただし、このサポートの有無はプラットフォームによって異なります。このため、`lspci`などの少数のアプリケーションは、正しく機能するように64ビットプログラムとして非ppc64プラットフォームでコンパイルする必要があります。IBM System zでは、32ビットカーネルABIで利用できないioctls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。

ヒント: カーネルロード可能モジュール

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したい場合は、このアプリケーションおよびSUSEのプロバイダに問い合わせて、このモジュール用に、カーネルにロード可能なモジュールの64ビットバージョンとカーネルAPIの32ビットコンパイルバージョンを入手できるかどうか確認してください。

---

9 Linuxシステムのブートと設定

Linuxシステムのブートには、さまざまなコンポーネントが関係しています。ハードウェアはBIOSにより初期化され、BIOSはブートローダでカーネルを起動します。それ以後は、オペレーティングシステムが`init`とランレベルを含むブートプロセスを完全にコントロールします。ランレベルのコンセプトにより、日常使用のセットアップを保持できるほか、システム上でタスクを保守することもできます。

9.1 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、それぞれ別のコンポーネントが実行しています。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** コンピュータの電源を入れた後、BIOSが画面とキーボードを初期化し、メインメモリをテストします。この段階まで、コンピュータは大容量ストレージメディアにアクセスしません。続いて、現在の日付、時刻、および最も重要な周辺機器に関する情報が、CMOS値からロードされます。最初のハードディスクとそのジオメトリが認識されると、システム制御がBIOSからブートローダに移ります。BIOSがネットワークブートをサポートしている場合は、ブートローダを提供するブートサーバを設定することもできます。x86システムの場合、PXEブートを利用する必要があります。他のアーキテクチャの場合は、通常BOOTPプロトコルを使ってブートローダを取得します。

2. **ブートローダ** 最初のハードディスクの先頭の512バイト物理データセクタがメインメモリにロードされ、このセクタの先頭に常駐するブートローダが起動します。ブートローダによって実行されたコマンドがブートプロセスの残りの部分を確定します。したがって、最初のハードディスクの先頭512バイトのことをマスタブートレコード(MBR)といいます。次に、ブートローダは、実際のオペレーティングシステム(この場合はLinuxカーネル)に制御を渡します。GRUB(Linuxブートローダ)の詳細については、 第10章 *ブートローダGRUB* (127 ページ)を参照してください。ネットワークブートを行う場合、BIOSがブートローダとしての役割を果たします。BIOSは、ブートサーバから起動するためのイメージを取得し、システムを起動します。この作業にローカルのハードディスクからは完全に独立した処理として行われます。

3. **カーネルと`initramfs`** システムに制御を渡すため、ブートローダは、カーネルとRAMベースの初期ファイルシステム(`initramfs`)をメモリにロードします。カーネルは、`initramfs`のコンテンツを直接使用できます。`initramfs`には、実際のルートファイルシステムのマウント処理を行う`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。大容量ストレージにアクセスするために特別なハードウェアドライバが必要な場合、それらは`initramfs`内になければなりません。`initramfs`の詳細については、 9.1.1項 「`initramfs`」 (111 ページ)を参照してください。システムにローカルハードディスクがない場合、`initramfs`がルートファイルシステムをカーネルに提供する必要があります。そのためには、iSCSIやSANなどのネットワークブロックデバイスを利用しますが、NFSをルートデバイスとして使うことも可能です。

4. **`initramfs`上の`init`** このプログラムは、適切なルートファイルシステムをマウントするために必要なすべてのアクションを実行します。たとえば、必要なファイルシステムにカーネル機能を提供したり、大容量ストレージコントローラ用のデバイスドライバに`udev`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で`init`プログラムが実行されます。`init`の詳細については、 9.1.2項 「`initramfs`上の`init`」 (112ページ)を参照してください。`udev`の詳細については、第14章 *`udev`による動的カーネルデバイス管理* (197 ページ)を参照してください。

5. **init** initは、いくつかの異なるレベルでシステムの実際のブートを処理し、さまざまな機能を提供しますinitについては、9.2項 「initプロセス」 (114 ページ)で説明されています。

9.1.1 initramfs

initramfsは、カーネルがRAMディスクにロードできる、小さなcpioアーカイブです。また、実際のルートファイルシステムがマウントされる前にプログラムを実行できるようにする最低限のLinux環境を提供します。この最小Linux環境は、BIOSルーチンによってメモリにロードされ、十分なメモリを必要とする以外、特定のハードウェア要件はありません。initramfsは、必ず、initという名前の実行可能ファイルを提供する必要があります。このファイルは、ルートファイルシステム上で実際のinitプログラムを実行することによりブートプロセスを進行させます。

ルートファイルシステムをマウントして実際のオペレーティングシステムを起動する前に、カーネルには、ルートファイルシステムが配置されているデバイスにアクセスするための対応ドライバが必要です。こうしたドライバには、特定のハードディスク用の特殊なドライバや、ネットワークファイルシステムにアクセスするためのネットワークドライバが含まれる場合もあります。ルートファイルシステムに必要なモジュールは、initramfs上のinitによってロードされます。モジュールをロードしたら、udevによって必要なデバイスがinitramfsに提供されます。ブートプロセス後半で、ルートファイルシステムが変更された後、デバイスを再生成する必要があります。これには、udevtriggerコマンドでboot.udevを実行します。

インストール済みのシステムのハードウェア(たとえば、ハードディスク)を変更する必要が生じ、このハードウェアはブート時にカーネル内に存在する他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initの場合と同様に、mkinitrdを呼び出して行うことができます。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、initが作成されます。SUSE® Linux Enterprise Serverでは、ロードするモジュールは/etc/sysconfig/kernel内の変数INITRD_MODULESで指定されます。インストール後、この変数は自動的に正しい値に設定されます。モジュールは、INITRD_MODULESに指定されている順序で正確にロードされます。このことは、デバイスファイルの/dev/sd?の設定の正確性に依存している場合にの

み重要になります。ただし、現在のシステムで/dev/disk/ディレクトリ下にあるデバイスファイルを使用することもできます。これらのファイルは、by-id、by-path、およびby-uuidなどのサブディレクトリに分類されており、常に同じディスクを表します。これは、該当するマウントオプションの指定により、インストール時にも可能です。

重要: initramfsまたは initの更新

ブートローダは、カーネルと同じようにinitramfsまたはinitをロードします。GRUBはブート時に正しいファイルのディレクトリを検索するので、initramfsまたはinitを更新した後にGRUBを再インストールする必要はありません。

9.1.2 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アクセスの準備をすることです。システム設定に応じて、initは次のタスクを実行します。

カーネルモジュールのロード
: ハードウェア設定によっては、使用するコンピュータのハードウェアコンポーネント(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。

ブロック特殊ファイルの提供
: ロードされるモジュールごとに、カーネルはデバイスイベントを生成します。udevは、これらのイベントを処理し、RAMファイルシステム上で必要なブロック特殊ファイルを/dev内に生成します。これらの特殊ファイルがないと、ファイルシステムや他のデバイスにアクセスできません。

RAIDとLVMのセットアップの管理
: RAIDまたはLVMの下でルートファイルシステムを保持するようにシステムを設定した場合、initはLVMまたはRAIDをセットアップして、後でルートファイルシステムにアクセスできるようにします。第15章 *高度な*

ディスクセットアップ(↑*導入ガイド*)でRAIDとLVMに関する情報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を介してマウント)を使用するようにシステムを設定した場合、`init`は適切なネットワークドライバがロードされ、ドライバがルートファイルシステムにアクセスできるように設定されていることを確認する必要があります。

  ファイルシステムがiSCSIやSANなどのネットワークブロックデバイスに常駐している場合は、ストレージサーバへの接続も`initramfs`によって設定されます。

初期ブート時にインストールプロセスの一環として`init`が呼び出される場合、そのタスクは上記で説明したタスクと異なります。

インストールメディアの検出
: インストールプロセスを開始すると、使用するコンピュータでは、YaSTインストーラでインストールカーネルと特殊な`init`がインストールメディアからロードされます。RAMファイルシステムで実行されるYaSTインストーラには、インストールメディアにアクセスしてオペレーティングシステムをインストールするために、そのメディアの場所に関する情報が必要になります。

ハードウェア認識の開始および適切なカーネルモジュールのロード
: で説明しているように、ブートプロセスは、ほとんどのハードウェア設定で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。9.1.1項 「`initramfs`」 (111 ページ)ブートプロセスに必要なモジュール名は、`/etc/sysconfig/kernel`ディレクトリ中の`INITRD_MODULES`に書き込まれます。これらの名前は、システムをブートするために必要なカスタム`initramfs`を生成するために使用されます。ブートではなくcoldplugで必要なモジュールは、`/etc/sysconfig/hardware/hwconfig-*`ディレクトリに書き込まれます。ブートプロセス時には、このディレクトリ中の設定ファイルに記述されているすべてのデバイスが初期化されます。

インストールシステムまたはレスキューシステムのロード
: ハードウェアが適切に認識されると、適切なドライバがただちにロードされ、`udev`は特殊なデバイスファイルを作成し、`init`は実際のYaSTイン

ストーラでインストールシステムを起動するか、またはレスキューシステムを起動します。

YaSTの開始
: 最後に、initはYaSTを起動し、これによってパッケージのインストールとシステム設定が開始されます。

9.2 initプロセス

initプログラムは、プロセスIDが1のプロセスです。このプロセスでは、要求された方法でシステムの初期化を行います。initは直接カーネルから起動され、プロセスを強制終了するsignal 9で終了することはできません。他のすべてのプログラムは、initまたはその子プロセスの1つによって直接起動されます。

initは、/etc/inittabファイルで一元的に設定されます。*ランレベル*はこのファイルで定義されます(9.2.1項 「ランレベル」 (114 ページ)を参照)。このファイルはまた、各ランレベルで利用可能な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はいくつかのスクリプトを実行します。デフォルトでは、ブート後に最初に開始するスクリプトは、/etc/init.d/bootです。システムの初期設定が完了すると、/etc/init.d/rcスクリプトで、ランレベルがデフォルトのランレベルに変更されます。わかりやすくするために、これらの*init*スクリプトと呼ばれるスクリプトはすべて、ディレクトリ/etc/init.dにあります(9.2.2項 「initスクリプト」 (117 ページ)を参照)。

システムの起動からシャットダウンまでのプロセス全体がinitによって保持されます。この見地から、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を保持し、CPU時間とハードウェアアクセスを調整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。

9.2.1 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。参照先表9.1「ランレベルの種類」(115ページ).別の方法として、ランレベルをブート時に(たとえばブートプロンプトにランレベル番号を追加する)指定することもできます。パラメータは、カーネル自体が直接評価するもの以外はすべて、initに渡されます。ランレベル3にブートするには、ブートプロンプトに単一の番号3を追加します。

*表 **9.1** ランレベルの種類*

ランレベル	説明
0	システム停止
Sまたは1	シングルユーザモード
2	リモートネットワーク(NFSなど)なしのローカルマルチユーザモード
3	ネットワークを使用するフルマルチユーザモード
4	［ユーザ定義］。管理者が設定しない限り使用されないランレベル。
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: パーティションがNFSマウントされている場合にはランレベル2は避ける

システムでNFSを介して/usrなどのパーティションをマウントする場合は、ランレベル 2を使用しないでください。NFSサービスは、ランレベル2(リモートネットワークのないローカルマルチユーザモード)では使用できないため、プログラムファイルまたはライブラリがない場合、システムは予想しない動作をする可能性があります。

システムの稼動中にランレベルを変更するには、telinitの後に、ランレベルに対応する番号を引数として入力します。これができるのは、システム管理者だけです。次のリストは、ランレベルに関連した最も重要なコマンドの概要です。

`telinit 1`または`shutdown now`
: システムは*シングルユーザモード*に入ります。このモードは、システムメンテナンスや管理タスクで使用します。

`telinit 3`
: (ネットワークを含む)すべての重要なプログラムとサービスが起動します。グラフィック環境はありませんが、一般ユーザは、システムにログインして作業することができます。

`telinit 5`
: グラフィック環境は有効になります。通常、XDM、GDMまたはKDMなどのディスプレイマネージャが起動します。自動ログインが有効な場合、ローカルユーザは事前に選択されているウィンドウマネージャ(GNOME、KDEまたはその他のウィンドウマネージャ)にログインします。

`telinit 0`または`shutdown -h now`
: システムは停止します。

`telinit 6`または`shutdown -r now`
: システムは停止した後、再起動します。

ランレベル5は、すべてのSUSE Linux Enterprise Server標準インストールにおけるデフォルトのランレベルです。ユーザは、グラフィカルインタフェースでログインするように求められます。デフォルトユーザの場合は自動的にログインされます。

警告: `/etc/inittab`のエラーのため、システムブートが失敗することがある

`/etc/inittab`が破損した場合、システムが正しく起動しないことがあります。そのため、`/etc/inittab`を編集する場合は細心の注意を払ってください。また、コンピュータを再起動する前には、常に`telinit q`コマンドを使用して、`init`に`/etc/inittab`を再読み込みさせてください。

ランレベルを変更するときには、一般に2つの操作が行われます。1つは、現在のランレベルの停止スクリプトが起動し、現在のランレベルに必要なプログラムを終了します。次に、新しいランレベルの起動スクリプトが起動します。ここで、ほとんどの場合、プログラムがいくつか起動します。たとえば、ランレベルを3から5に変更する場合、次の操作が行われます。

1. 管理者(root)がtelinit 5を入力して、initにランレベルを変更するように要求します。

2. initは現在のランレベル(runlevel)を調べ、新しいランレベルをパラメータとして/etc/init.d/rcを起動する必要があるかどうか判断します。

3. ここでrcは、現在のランレベルの停止スクリプトであって、新しいランレベルの起動スクリプトがないものを呼び出します。この例では、元のランレベルが3なので、/etc/init.d/rc 3.dの中のKで始まるすべてのスクリプトが対象となります。Kの次の番号は、stopパラメータを使ってスクリプトを実行する順番を示します(検討する必要がある依存関係が存在するため)。

4. 最後に、新しいランレベルの起動スクリプトを起動します。この例では/etc/init.d/rc5.dの中のSで始まるスクリプトがそれにあたります。この場合も、Sの次の番号が、スクリプトの実行順序を表します。

現在のランレベルと同じランレベルに変更する場合、initは/etc/inittabで変更部分だけをチェックし、適切な手順を開始します。たとえば、別のインタフェースでgettyを起動します。telinit qコマンドを使用しても同じ操作を実行できます。

9.2.2 initスクリプト

/etc/init.d内に、2種類のスクリプトがあります。

initによって直接実行されるスクリプト
: これは、ブートプロセスの実行中、または即座のシステムシャットダウンを行ったとき(電源障害またはユーザがCtrl＋Alt＋Delキーを押した場合)にのみ適用されます。IBM System zシステムの場合、ブートプロセスの実行中または即座のシステムシャットダウンを行ったとき(電源障害または「シ

グナルによる停止」)にのみ適用されます。こうしたスクリプトの実行は、/etc/inittabで定義されます。

initによって間接的に実行されるスクリプト
: これらは、ランレベルの変更時に実行され、関連スクリプトの正しい順序を保証するマスタスクリプト/etc/init.d/rcを常に呼び出します。

すべてのスクリプトは、/etc/init.dにあります。ブート時に実行されるスクリプトは、/etc/init.d/boot.dからのシンボリックリンク経由で呼び出されます。ランレベルを変更するスクリプトもサブディレクトリの1つからのシンボリックリンク(/etc/init.d/rc0.dから/etc/init.d/rc6.dへ)経由で呼び出されます。これは単にわかりやすくして、複数のランレベルで使用されている場合にスクリプトが重複するのを防ぐためです。すべてのスクリプトは、起動スクリプトとしても停止スクリプトとしても実行できるので、これらのスクリプトはパラメータのstartとstopを認識する必要があります。また、これらのスクリプトはrestart、reload、force-reload、およびstatusのオプションも認識します。これらのオプションについては、表9.2「initスクリプトのオプション」 (118 ページ)で説明します。initによって直接実行されるスクリプトには、これらの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 9.2　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。
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、

オプション	説明
	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/usr/lib/lsb/install_initdスクリプトを使用して)、このようなリンクを追加または削除することができます。詳細については、「man 8 insserv」を参照してください。

これらの設定は、YaSTモジュールにより変更されることもあります。コマンドラインからステータスを確認するには、chkconfigツールを使用します。このツールについては、man 8 chkconfigのマニュアルページで説明されています。

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の起動時に実行されます。選択したランレベルから独立で、一度だけ実行されます。これによって /procファイルシステムと/dev/ptsファイルシステムがマウントされ、blogd(ブートログ出力デーモン)が有効化されます。システムがアップデートまたはインストール後初めてブートされる場合、初期システム設定が起動します。

  blogdデーモンは、bootおよびrcによって最初に起動されるサービスです。このサービスは、これらのスクリプトにより開始されたアクション(たとえば特殊なブロックファイルを利用可能にするなど、多数のサブスクリプトの実行)が完了すると停止します。blogdは、/varが読み書き可能でマウントされている場合にのみ、画面出力をログファイル/var/log/boot.msgに出力します。そうでない場合は、/varが利用できるようになるまで、blogdがすべての画面データをバッファします。 blogdの詳細情報を取得するには、man 8 blogdを使用します。

bootスクリプトは、/etc/init.d/boot.dの中のSで始まる名前のスクリプトもすべて起動します。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。最後に実行されるスクリプトは、boot.localです。

boot.local
: ブート時、ランレベルへの移行前に実行する追加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。

halt
: このスクリプトは、ランレベル0または6への移行時にのみ実行されます。initまたはinitのいずれかとして実行されます。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。シャットダウン時に特別なコマンドが必要な場合は、それらのコマンドをinitスクリプトに追加してください。

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。/etc/init.d/bootスクリプトと同様、このスクリプトは、目的のランレベルをパラメータとして使用して、/etc/inittabから呼び出します。

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設定、名前付け、および構成方法については、LSBの仕様と、init、init.d、chkconfig、およびinsservのマニュアルページを参照してください。加えて、startprocおよびkillprocのマニュアルページも参照してください。

警告: initスクリプトのエラーはシステムの停止につながる場合がある

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する場合があります。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スクリプトの有益な情報については、9.2.1項「ランレベル」 (114 ページ)を参照してください。

所定のプログラムまたはサービス用のカスタム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、必要に応じて、関連のプログラムやファイル名、パス、その他の詳細を編集します。場合によっては、initプロシージャで正しいアクションが開始されるように、独自の改良をスクリプトに加える必要があります。

最初に記載されているINIT INFOブロックはスクリプトの必須部分で、次のように編集する必要があります。詳細については、例9.1「最低限のINIT INFOブロック」 (121 ページ)を参照してください。

*例 **9.1** 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:行とRequired-Stop:行では、サービス自体が停止しても実行中の状態を維持する必要の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 *new-script-name*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/)内の起動スクリプトと停止スクリプト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、9.2.3項 「YaSTを使用したSystem Services (Runlevel)の設定」 (122 ページ)の説明に従って、YaSTのランレベルエディタを使用します。

/etc/init.d/にすでに存在するスクリプトを既存のランレベルスキーマに統合する場合は、はじめにinsservを使用するか、YaSTのランレベルエディタで対応するサービスを有効にすることにより、ランレベルディレクトリにリンクを作成します。変更内容は、次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。手動で追加されたサービスは、このスクリプトに対するinsservの次回実行時に削除されます。

9.2.3 YaSTを使用したSystem Services (Runlevel)の設定

［*YaST*］>［システム］>［*System Services (Runlevel)*］の順に選択して、このYaST moduleを起動すると、利用可能なすべてのサービスの概要と、各サービスの現在のステータス(有効か無効か)が表示されます。モジュールを［*単純モード*］と［エキスパートモード］のどちらで使用するかを決定します。ほとんどの場合、デフォルトの［*単純モード*］で十分です。左の列にはサービスの名前、中央の列にはその現在のステータス、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。

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、最初に［エキスパートモード］を選択します。上部には、現在のデフォルトのランレベル、つまり「initdefault」(システムのブート時にデフォルトで入るランレベル)が表示されます。通常、SUSE Linux Enterprise Server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9.1「ランレベルの種類」 (115 ページ)を参照)。また、このウィンドウのテーブルを使用して、個々のサービスやデーモンを有効、無効にできます。テーブルには、利用可能なサービスとデーモンが一覧表示され、現在ご使用のシステム上で有効かどうか、有効な場合はそのランレベルが表示されます。マウスで行を選択し、ランレベルを表すチェックボッ

クス([*B*] 、 [*0*] 、 [*1*] 、 [*2*] 、 [*3*] 、 [*5*] 、 [*6*] 、 [*S*])をクリックして、選択しているサービスまたはデーモンが実行されるランレベルを定義します。ランレベル4は、カスタムランレベルを作成できるように未定義になっています。最後に現在選択しているサービスまたはデーモンの簡単な説明が、テーブルの概要の下に表示されます。

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、システムを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。

図 9.1 *System Services (Runlevel)*

［スタート］、［中止］、または［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］または［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。［*OK*］を選択すると、設定の変更がディスクに保存されます。

9.3 /etc/sysconfigによるシステム設定

SUSE Linux Enterprise Serverの主な設定は、/etc/sysconfigに格納されている設定ファイルで指定できます。/etc/sysconfigディレクトリの個々のファイルは、それらが関係するスクリプトによってのみ読み込まれます。これにより、たとえば、ネットワークはネットワーク関連のスクリプトでのみ解析されるようになります。

システム設定を編集するには、2通りの方法があります。YaSTのsysconfigエディターを使う方法と、設定ファイルを手動で編集する方法です。

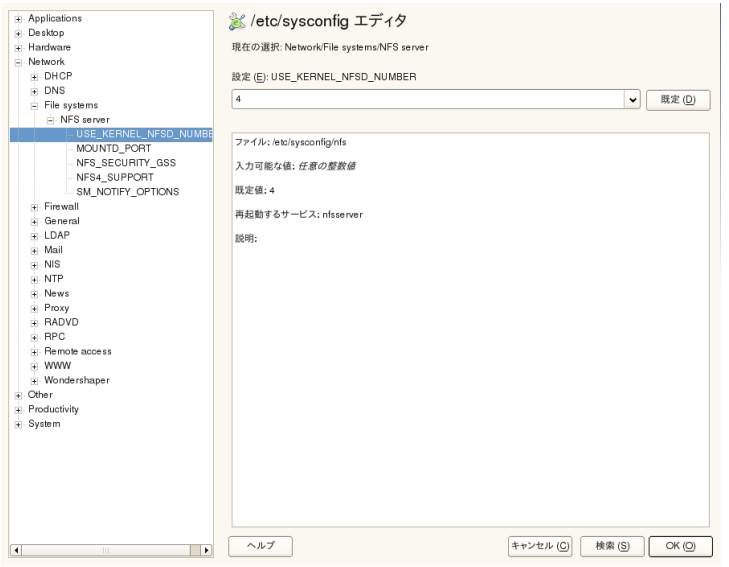
9.3.1 YaSTのsysconfigエディターを使ってシステム設定を変更する

YaSTのsysconfigエディタは、使いやすい、システム設定のフロントエンドです。変更する必要のある設定用変数の実際の場所がわからなくても、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。また、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、サービスの再起動は、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。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 9.2　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。

9.3.2 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 telinit 1コマンドで、システムをシングルユーザモード(ランレベル 1)にします。

3 必要に応じて、設定ファイルを、自分が使っているエディタで変更します。

/etc/sysconfigの設定ファイルの変更にYaSTを使用しない場合、空の変数値は2つの引用符(KEYTABLE="")によって表し、空白を含む値へ引用符で囲むことに注意してください。語の値は、引用符で囲む必要はありません。

4 SuSEconfigを実行して、変更が有効になっていることを確認します。

5 telinit *default_runlevel*などのコマンドで、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で作業するには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。

ヒント: 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。

---

10 ブートローダGRUB

この章では、SUSE® Linux Enterprise Serverで使用されているブートローダGRUB(Grand Unified Bootloader)の設定方法について説明します。すべての設定操作には、特殊なYaSTモジュールを使用できます。Linuxでのブートに不慣れな場合は、以降の各セクションを読んで背景情報を理解してください。また、この章では、GRUBでのブート時に頻繁に発生する問題とその解決策についても説明します。

注記: UEFIを使用するコンピュータ上にGRUBがない

通常GRUBは従来のBIOSを備え、UEFI (Unified Extensible Firmware Interface)上にあるコンピュータにインストールされます。CSMが有効になっていないUEFIコンピュータでは、`eLILO`が自動的にインストールされます (DVD1が正常に起動した場合)。詳細については、ご使用のシステムの`/usr/share/doc/packages/elilo/`にあるeLILOマニュアルを参照してください。

この章は、ブート管理とGRUBブートローダの設定に重点を置いています。ブート手順は、総じて第9章*Linux*システムのブートと設定(109ページ)で説明しています。ブートローダは、マシン(BIOS)とオペレーティングシステム(SUSE Linux Enterprise Server)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。

MBR (マスターブートレコード)
: MBRの構造は、オペレーティングシステムに依存しない規則に従って定義されます。最初の446バイトは、プログラムコード用に予約されています。通常、ここにはブートローダプログラムやオペレーティングシステムセレクタの一部が保管されています。次の64バイトは、最大4つのエントリからなるパーティションテーブル用のスペースです。パーティションテーブルには、ハードディスクのパーティション分割とファイルシステムのタイプに関する情報が含まれています。オペレーティングシステムでハードディスクを処理するには、このテーブルが必要です。MBRの従来の汎用コードでは、1つのパーティションにだけアクティブのマークを付ける必要があります。MBRの最後の2バイトは、静的な「「マジックナンバー」」(AA55)を含む必要があります。一部のBIOSでは、異なる値を持つMBRは無効とみなされ、ブートの対象とはみなされません。

ブートセクタ
: ブートセクタは、拡張パーティションを除くハードディスクパーティションの最初のセクタであり、その他のパーティションの「コンテナ」として機能するだけです。これらのブートセクタのうち512バイトのスペースは、関連パーティションにインストールされているオペレーティングシステムをブートするためのコードが占有します。これは、フォーマット済みのDOS、Windows、およびOS/2パーティションのブートセクタに該当し、ファイルシステムの重要な基本データも一部含まれています。これに対して、Linuxパーティションのブートセクタは、XFS以外のファイルシステムの設定直後は当初空になっています。そのため、Linuxパーティションは、カーネルと有効なルートファイルシステムが含まれている場合にも、単独ではブートできません。システムブート用の有効なコードを含むブートセクタの場合、最後の2バイトにはMBRと同じマジックナンバー(AA55)があります。

10.1 GRUBによるブート

GRUBは、2つのステージで構成されています。ステージ1は、512バイトから成り、そのタスクは、ブートローダの第2ステージをロードすることだけです。その後、stage2が読み込まれます。このステージにいは、ブートローダの主要部分が含まれています。

一部の設定では、適切なファイルシステムからステージ2を検出し、ロードする中間ステージの1.5を使用できます。可能であれば、デフォルトでインストール時、またはYaSTを使用したGRUBの初回セットアップ時に、こ

stage2は、多くのファイルシステムにアクセスできます。現在、Windowsで使用されているext2、ext3、ReiserFS、Minix、およびDOS FATファイルシステムがサポートされます。BSDシステムで使用されているXFS、UFS、およびFFSも、特定の範囲までサポートされます。バージョン0.95GRUBには、「El Torito」仕様に準拠するISO 9660標準ファイルシステムを含むCDまたはDVDからブートする機能も用意されています。システムをブートする前にも、GRUBはサポートされているBIOSディスクデバイス(BIOSにより検出されるフロッピーディスクまたはハードディスク、CDドライブ、およびDVDドライブ)のファイルシステムにアクセスできます。したがって、GRUBの設定ファイル(`menu.lst`)を変更しても、ブートマネージャを新たに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、次の4つのファイルに基づきます。

`/boot/grub/menu.lst`
: このファイルには、GRUBでブートできるパーティションまたはオペレーティングシステムに関する情報がすべて含まれています。この情報がない場合、GRUBコマンドラインは、どのように処理を続行するかユーザの指示を求めます(詳細については、10.1.1.3項「ブート手順実行中のメニューエントリの編集」 (135 ページ)を参照してください)。

`/boot/grub/device.map`
: このファイルは、デバイス名をGRUBとBIOSの表記法からLinuxデバイス名に変換するために使います。

`/etc/grub.conf`
: このファイルには、GRUBシェルでブートローダを正常にインストールするために必要なコマンド、パラメータ、およびオプションが含まれています。

`/etc/sysconfig/bootloader`
: このファイルはperl-bootloaderライブラリが読み取ります。これはブートローダをYaSTで設定するときと、新しいカーネルがインストールされる

たびに使用されます。カーネルパラメータなどの設定オプションが含まれ、これはブートローダ設定ファイルにデフォルトで追加されます。

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、ブートコマンドは、一種の入力プロンプトで対話的に入力することもできます。詳細については、10.1.1.3項「ブート手順実行中のメニューエントリの編集」 (135 ページ)を参照してください。GRUBには、ブート前にカーネルとinitrdの位置を判別する機能が用意されています。この機能を使用すると、ブートローダ設定にエントリが存在しないインストール済みオペレーティングシステムでもブートできます。

GRUBは、2種類のバージョンで存在します。ブートローダとして、または/usr/sbin/grub中のLinuxプログラムとしてです。このプログラムを*GRUBシェル*と呼びます。GRUBシェルは、インストールされたシステムにGRUBのエミュレーションを提供し、GRUBのインストールまたは新規設定の適用前のテストに使用できます。ハードディスクやフロッピーディスクにGRUBをブートローダとしてインストールする機能は、コマンドsetup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。

10.1.1 ファイル/boot/grub/menu.lst

ブートメニューを含むグラフィカルスプラッシュ画面は、GRUBの設定ファイル/boot/grub/menu.lstに基づいており、このファイルにはメニューを使用してブートできるパーティションまたはオペレーティングシステムに関する情報がすべて含まれています。

システムをブートするたびに、ファイルシステムからメニューファイルを読み込みます。このため、ファイルを変更するたびにGRUBを再インストールする必要がありません。10.2項「YaSTによるブートローダの設定」 (140 ページ)で説明しているように、YaSTのブートローダを使用してGRUBの設定を変更します。

メニューファイルにはコマンドが含まれています。構文はきわめて単純です。各行には、コマンド1つとオプションのパラメータがシェルと同様にスペースで区切って指定されています。これまでの経緯が理由で、一部のコマンドでは最初の引数の前に等号(=)を使用することができます。コメントを記述するには、行頭にシャープ記号(#)を入力します。

メニュー概要の中にあるメニュー項目を識別できるように、各エントリに対してtitle (タイトル)を設定します。キーワードtitleの後に続くテキスト(半角スペースも使用できます)は、メニューの中で、選択可能なオプションとして表示されます。そのメニュー項目が表示された場合、次のtitleまでに記述されているすべてのコマンドが実行されます。

最も簡単な例は、他のオペレーティングシステムのブートローダにリダイレクトすることです。該当するコマンドはchainloaderであり、引数は通常、他のパーティション内にあるブートブロックをGRUBのブロック表記に従って記述したものです。たとえば、次のようにします。

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

GRUBでのデバイス名については、10.1.1.1項「ハードディスクとパーティションに関する命名規則」 (132 ページ)を参照してください。この例では、1台目のハードディスクの4番目のパーティションの最初のブロックを指定しています。

カーネルイメージを指定するには、kernelコマンドを使用します。最初の引数は、パーティションにあるカーネルイメージを表すパスです。他の引数は、そのコマンドラインでカーネルに渡されます。

ルートパーティションへのアクセスに必要なビルトインドライバがカーネルに用意されていない場合、または高度なhotplug機能のある新しいLinuxシステムが使用されていない場合は、initrdファイルへのパスを示す引数だけを指定して、別のGRUBコマンドでinitrdを指定する必要があります。initrdのロードアドレスは、ロードされるカーネルイメージに書き込まれるので、initrdコマンドは、kernelコマンドの後に記述する必要があります。

rootコマンドは、kernelとinitrdの各ファイルの指定を簡略化します。rootの引数は、デバイスまたはパーティションだけです。このデバイスは、すべてのカーネル、initrd、または次のrootコマンドまでデバイスが明示的に指定されて「ない他のファイルのパスに使用されます。

bootコマンドは各メニューエントリの最後に必ず含まれています。そのため、メニューファイルにこのコマンドを記述する必要はありません。ただし、GRUBをブート時に対話形式で使用する場合は、bootコマンドを最後に入力する必要があります。このコマンド自体は、引数を使用しません。単純に、読み込み済みのカーネルイメージ、または指定のチェーンローダをブートします。

すべてのメニューエントリを記述した後、その1つをdefaultエントリとして定義します。デフォルトエントリを指定しなかった場合、最初のエントリ(エントリ0)が使用されます。デフォルトエントリがブートされるまでのタイムアウトを秒単位で指定することもできます。通常、timeout およびdefaultは、メニューエントリより先に記述します。サンプルファイルについては、10.1.1.2項 「メニューファイルの例」 (133 ページ)を参照してください。

10.1.1.1 ハードディスクとパーティションに関する命名規則

GRUBを使用する、ハードディスクとパーティションの命名規則は、通常のLinuxデバイスの命名規則と異なっています。どちらかというと、BIOSが使用する単純なディスクエミューレーションに似ており、構文は一部のBSDデリバティブで使用されているものに類似しています。GRUBでは、パーティション番号は0から始まります。これは、(hd0,0)は最初のハードディスクの最初のパーティションになります。ハードディスクがプライマリマスタとして接続されている一般的なデスクトップマシンでは、対応するLinuxデバイス名は/dev/sda1になります。

可能な4つの基本パーティションに、パーティション番号}0〜3が割り当てられます。論理パーティション番号は4から始まります。

```
(hd0,0)   first primary partition of the first hard disk
(hd0,1)   second primary partition
(hd0,2)   third primary partition
(hd0,3)   fourth primary partition (usually an extended partition)
(hd0,4)   first logical partition
(hd0,5)   second logical partition
```

GRUBは、BIOSデバイスに依存しているので、PATA(IDE)、SATA、SCSIおよびハードウェアRAIDの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。

一般に、GRUBには、Linuxデバイス名をBIOSデバイス名に正確にマップする機能がありません。このマッピングはアルゴリズムを使用して生成され、device.mapファイルに保存されるため、必要に応じて編集できます。ファイルdevice.mapについては、10.1.2項「device.mapファイル」(136ページ)を参照してください。

GRUBのフルパスは、カッコ内のデバイス名と、指定のパーティションにあるファイルシステム内のファイルへのパスで構成されます。このパスはスラッシュで始まります。たとえば、単一PATA(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
```

10.1.1.2 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/sda5、ルートパーティションが/dev/sda7、およびWindowsのインストールファイルが/dev/sda1にあります。

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

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

title windows❻
   rootnoverify (hd0,0)
   chainloader +1

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

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

最初のブロックは、スプラッシュ画面の設定を定義します。

❶ 背景画像messageは、/dev/sda5パーティションの /bootディレクトリにあります。

❷ カラースキーマ:白(前景色)、青(背景色)、黒(選択項目)、明るい灰色(選択項目の背景色)です。配色はスプラッシュ画面には影響しません。影響を受けるのは、Escキーを押してスプラッシュ画面を終了するとアクセスできるカスタマイズ可能なGRUBメニューだけです。

❸ デフォルトでは、最初の(0)メニューエントリtitle linuxがブートされます。

❹ 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。

❺ 最初のエントリ(title linux)は、SUSE Linux Enterprise Server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。この情報を読み込むのはLinuxカーネルであり、GRUBは関係しないため、ルートパーティションは、Linuxの命名規則(/dev/sda7/)に従って指定されます。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。

❻ 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。

❼ 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。

❽ 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。詳細については、10.1.1.3項 「ブート手順実行中のメニューエントリの編集」 (135 ページ)を参照してください。

10.1.1.3 ブート手順実行中のメニューエントリの編集

グラフィカルブートメニューでは、ブートするオペレーティングシステムを矢印キーで選択します。Linuxシステムを選択した場合は、ブートプロンプトからブートパラメータを追加入力できます。個々のメニューエントリを直接編集するには、Escキーを押してスプラッシュ画面を終了し、GRUBテキストベースメニューを表示してからEキーを押します。この方法で加えた変更は、現在のブートだけに適用され、永続的に採用されることはありません。

重要: 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。詳細については、図35.3「USキーボードレイアウト」 (613 ページ)を参照してください。

メニューエントリの編集により、障害が発生してブートできなくなったシステムを容易に修復できます。これは、ブートローダの設定ファイルの誤りをパラメータの手動入力により回避できるからです。ブート手順の中でパラメータを手動で入力する方法は、ネイティブシステムを損傷せずに新規設定をテストする際にも役立ちます。

編集モードを有効にした後、矢印キーを使用して、設定を編集するメニューエントリを選択します。設定を編集可能にするには、もう一度Eキーを押します。このようにして、不正なパーティションまたはパス指定を、ブートプロセスに悪影響を及ぼす前に編集します。Enterキーを押して編集モードを終了し、メニューに戻ります。次に、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、ユーザのrootでファイルmenu.lstを開き、関連カーネルパラメータをスペースで区切って既存の行に追加します。

```
title linux
   root(hd0,0)
     kernel /vmlinuz root=/dev/sda3 additional parameter
   initrd /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。

10.1.2 device.mapファイル

device.mapファイルは、GRUBおよびBIOSのデバイス名をLinuxのデバイス名にマップします。PATA(IDE)とSCSIの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別を試みる必要があります。これは、GRUBがブートシーケンスに関するBIOS情報にアクセスできない場合があるためです。GRUBはこの分析の結果をファイル/boot/grub/device.mapに保存します。BIOS内のブートシーケンスをSCSIの前にPATAに設定するシステムのdevice.mapファイルは、たとえば、次のようになります:

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

または

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

PATA(IDE)やSCSIなどのハードディスクの順序はさまざまな要因によって左右され、Linuxではそのマッピングを識別できないので、device.mapファイル内のシーケンスは手動で設定することができます。ブート時に問題に直面した場合、このファイル内のシーケンスが、BIOS内のシーケンスに対応しているかどうかチェックします。さらに、必要に応じてGRUBは、前者を一時的に変更するように指示します。Linuxシステムのブート後に、YaSTブートロー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。

注記: ハードディスクの最大数

GRUBは、ハードディスクのアドレス指定にBIOSサービスを使用します。これには、ソフトウェア割り込みInt13hが使用されます。Int13hは最大8ディスクしか操作できないので、9ディスク以上存在する場合でも(マルチパスシステムではよくある事例)、GRUBは、Int13hが操作するディスクからしかブートできません。したがって、インストール時に作成されたdevice.mapファイルは、Int13hで操作された最大8つのディスクしか含みません。

---

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
```

10.1.3 /etc/grub.confファイル

menu.lstおよびdevice.mapの次に重要な第3のGRUB設定ファイルは、/etc/grub.confです。このファイルには、GRUBシェルでブートローダを正常にインストールするために必要なコマンド、パラメータ、およびオプションが含まれています。

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

このコマンドは、同じパーティションに存在するブートイメージを使用して、最初のハードディスク(hd0、1)の第2パーティションにブートローダを自動的にインストールするようにGRUBに指示します。マウントされたファイルシステムからstage2イメージをインストールするには、--stage2=/boot/grub/stage2パラメータが必要です。一部のBIOSは、LBAサポート実装に欠陥があります。これを無視する解決策として、--force-lbaを使用します。

10.1.4 ファイル/etc/sysconfig/bootloader

この設定ファイルは、ブートローダをYaSTで設定するときと、新しいカーネルがインストールされる際にのみ、使用されます。perl-bootloaderライブラリで評価され、それに従ってブートローダ設定ファイル(GRUBの/boot/grub/menu.lstなど)が変更されます。/etc/sysconfig/bootloaderはGRUB固有の設定ファイルではありません。値はSUSE Linux Enterprise Serverにインストールされたブートローダすべてに適用されます。

注記: カーネルアップデート後のブートローダ設定

新しいカーネルがインストールされるたびに、perlブートローダは/etc/sysconfig/bootloaderで指定されたデフォルトを使用して、新しいブートローダ設定ファイル(たとえば、GRUBの/boot/grub/menu.lstなど)を作成します。カスタマイズしたカーネルパラメータのセットを使用してい

る場合、必要に応じて/etc/sysconfig/bootloaderの該当するデフォルト値を調整してください。

LOADER_TYPE
: システムにインストールされたブートローダを指定します(GRUBやLILOなど)。変更は勝手にしないでください。ブートローダは、手順10.6「ブートローダのタイプの変更」(145ページ)に説明されているように、YaSTを使用して変更します。

DEFAULT_VGA / FAILSAFE_VGA / XEN_VGA
: 起動時に使用されるフレームバッファの画面解像度と色深度は、カーネルパラメータvgaで設定されます。これらの値は、デフォルトブートエントリ、フェイルセーフ、XENエントリに使用する解像度と色深度を定義します。有効な値は次のとおりです。

表 10.1 画面解像度および色深度の参照

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

DEFAULT_APPEND / FAILSAFE_APPEND / XEN_KERNEL_APPEND
: ブートローダ設定ファイルのデフォルト、フェイルセーフ、XENブートエントリに自動的に付加されるカーネルパラメータ(vga以外)。

CYCLE_DETECTION / CYCLE_NEXT_ENTRY
: ブートサイクル検出を使用するかどうか設定します。使用する場合は、リブートサイクルの際に/boot/grub/menu.lstから使用する代替エントリ(たとえば、Failsafe)を設定します。詳細は、/usr/share/doc/packages/bootcycle/READMEを参照してください。

10.1.5 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: ブートパスワードとスプラッシュ画面

GRUBにブートパスワードを使用する場合、通常のスプラッシュ画面は表示されません。

ユーザrootとして、次の手順に従ってブートパスワードを設定します。

1 rootプロンプトで、grub-md5-cryptを使ってパスワードを暗号化します。

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

2 暗号化後の文字列を、menu.lstファイルのグローバルセクションに貼り付けます。

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$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。

3 ブートメニューから1つまたは複数のオペレーティングシステムをブートする操作を禁止するには、menu.lst内で、パスワードを入力しなければブートできないようにする必要のある各セクションにエントリlockを追加します。たとえば、次のようにします。

```
title linux
   kernel (hd0,4)/vmlinuz root=/dev/sda7 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。

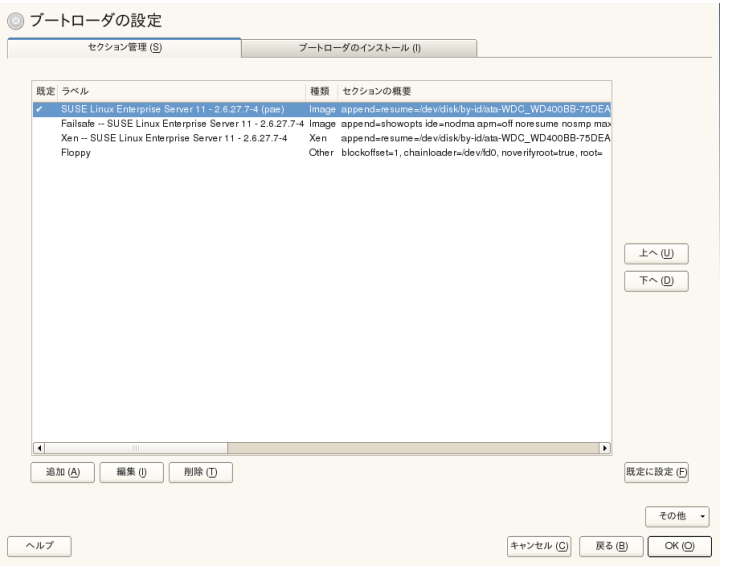
```
Error 32: Must be authenticated
```

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。

10.2 YaSTによるブートローダの設定

SUSE Linux Enterprise Serverシステムでブートローダを設定する最も簡単な方法は、YaSTモジュールを使用することです。YaSTコントロールセンターで、［システム］＞［ブートローダ］の順に選択します。図10.1「ブートローダの設定」(140 ページ)で説明しているように、システムの現在のブートローダ設定が表示され、設定を変更できます。

図 10.1　ブートローダの設定



［セクション*管理*］タブを使用して、各オペレーティングシステムのブートローダセクションの編集、変更、削除を行うことができます。オプションを追加するには、［*追加*］をクリックします。既存のオプションの値を変更するには、マウスで選択してから［*編集*］をクリックします。既存のエントリを削除するには、エントリを選択して［*削除*］をクリックします。ブートローダのオプションをよくご存知でない場合には、はじめに10.1項「GRUBによるブート」 (128 ページ)を参照してください。

［*ブートローダのインストール*］タブで、タイプ、場所、高度なローダ設定に関する設定を表示および変更できます。

［*その他*］をクリックして、高度な設定オプションにアクセスします。組み込みエディタでGRUB設定ファイルを変更できます。詳細については、10.1項「GRUBによるブート」 (128 ページ)を参照してください。既存の設定を削除して［*新しい設定を作成*］したり、YaSTで［*新しい設定を提案*］できます。設定をディスクに書き込んだり、ディスクから設定を読み直すこともできます。インストール時に保存した最初のMBR(Master Boot Record) j を復元するには、［*ハードディスクのMBRの復元*］を選択します。

10.2.1 デフォルトブートエントリの調整

デフォルトでブートされるシステムを変更するには、次の手順に従います。

手順 10.1 *標準のシステムの設定*

1 ［*セクション管理*］タブを開きます。

2 リストから目的の項目を選択します。

3 ［*デフォルトにする*］をクリックします。

4 ［*OK*］をクリックしてこれらの変更を有効にします。

10.2.2 ブートローダの場所の変更

ブートローダの場所を変更するには、次の手順に従います。

手順 10.2　ブートローダの場所の変更

1 ［ブートローダのインストール］タブを選択し、［ブートローダの場所］で、次のオプションの1つを選択します。

［マスタブートレコードからブート］
最初のディスクのMBRにブートローダをインストールします(BIOS 中のブートシーケンスプリセットによる)。

［ルートパーティションからブート］
/パーティションのブートセクタにブートローダがインストールされます(デフォルト)。

［ブートパーティションからブート］
/bootパーティションのブートセクタにブートローダがインストールされます。

［拡張パーティションからブート］
拡張パーティションコンテナにブートローダがインストールされます。

［カスタムブートパーティション］
このオプションを選択すると、手動でブートローダの場所を指定できます。

2 ［*OK*］をクリックして、変更を適用します。

10.2.3 ブートローダのタイムアウトの変更

ブートローダは、標準のシステムを直ちにブートするわけではありません。タイムアウト中、ブートまたはカーネルパラメータを書き込むシステムを選択できます。ブートローダのタイムアウトを設定するには、次の手順に従います。

手順 10.3　ブートローダのタイムアウトの変更

1 ［ブートローダのインストール］タブを開きます。

2 ［ブートローダのオプション］をクリックします。

3 新しい値を入力するか、マウスで矢印キーをクリックするか、またはキーボードの矢印キーを使って、［タイムアウト*(秒)*］の値を変更します。

4 ［*OK*］を2回クリックして、変更内容を保存します。

警告: タイムアウト0秒

タイムアウトを0秒に設定すると、ブート中にGRUBにアクセスできなくなります。同時に、デフォルトブートオプションをLinux以外のオペレーティングシステムに設定すると、結果としてLinuxシステムもアクセスできなくなります。

10.2.4 ブートパスワードの設定

このYaSTモジュールでは、ブートを保護するためのパスワードを設定することもできます。そうすれば、セキュリティに付加的なレベルを追加できます。

手順 10.4 *ブートローダパスワードの設定*

1 ［*ブートローダのインストール*］タブを開きます。

2 ［*ブートローダのオプション*］をクリックします。

3 ［*パスワードでブートローダを保護する*］オプションをクリックして有効にし、［*パスワード*］を2回入力します。

4 ［*OK*］を2回クリックして、変更内容を保存します。

10.2.5 ディスク順序の変更

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、コンピュータのBIOSセットアップと一致するように指定できます(「10.1.2項 「device.mapファイル」 (136 ページ)」を参照してください)。次の手順に従います。

手順 10.5 *ディスクの順序の設定*

1 ［*ブートローダのインストール*］タブを開きます。

2 ［*ブートローダのインストールの詳細*］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［*上へ*］または［*下へ*］をクリックして、ディスクの表示順を変更します。

4 ［*OK*］を2回クリックして、変更内容を保存します。

10.2.6 詳細オプションの設定

詳細なブートオプションは、［*ブートローダのインストール*］>［*ブートローダのオプション*］の順に選択して、設定できます。通常は、デフォルト設定を変更する必要はありません。

［*ブートパーティション用パーティションテーブルにアクティブフラグを設定*］
ブートローダを含むパーティションをアクティブにします。Windows 98のような一部のレガシーオペレーティングシステムは、アクティブパーティションからのみブートできます。

［*MBRに汎用ブートコードを書き込む*］
現在のMBRを、オペレーティングシステムに依存しない独立した汎用コードで置換します。

［*デバッグフラグ*］
Sets GRUBを、ディスクアクティビティを示すメッセージを表示するデバッグモードに設定します。

［*ブートメニューを隠す*］
ブートメニューを隠し、デフォルトエントリをブートします。

警告

ブートメニューを隠すと、ブート中にGRUBにアクセスできなくなります。同時に、デフォルトブートオプションをLinux以外のオペレーティングシステムに設定すると、結果としてLinuxシステムもアクセスできなくなります。

［*信頼できるGRUBを使用する*］
信頼性の高いコンピューティング機能をサポートする信頼できるGRUBを起動します。

［グラフィカルメニューファイル］
ブート画面の表示時に使用されるグラフィックファイルへのパスを設定します。

［シリアル接続パラメータ］
コンピュータがシリアルコンソールで制御されている場合は、どのCOMポートをどの速度で使用するか指定できます。さらに、［ターミナル定義］を「serial」に設定します。詳細については、`info grub`または`http://www.gnu.org/software/grub/manual/grub.html`を参照してください。

［シリアルコンソールの使用］
コンピュータがシリアルコンソールで制御されている場合は、このオプションを有効にして、どのCOMポートをどの速度で使用するか指定します。`info grub`または`http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal`を参照してください。

10.2.7 ブートローダタイプの変更

［ブートローダのインストール］でブートローダのタイプを設定します。SUSE Linux Enterprise ServerのデフォルトブートローダはGRUBです。LILOまたはELILOを使用するには、次の手順に従います。

警告: LILOはサポートされていません

LILOの使用は推奨されません。SUSE Linux Enterprise Serverではサポートされていません。特殊な場合にのみ、使用してください。

手順 10.6 *ブートローダのタイプの変更*

1 ［ブートローダのインストール］タブを選択します。

2 ［ブートローダ］で、［*LILO*］を選択します。

3 表示されるダイアログボックスで、次のオプションのうち、いずれかを選択します。

［*Propose New Configuration (新しい設定を提案する)*］
YaSTは新しい設定を提案します。

［*Convert Current Configuration (現在の設定を変換する)*］
YaSTは現在の設定を変換します。設定を変換すると、いくつかの設定内容が失われることがあります。

［*Start New Configuration from Scratch (新しい設定を新規に作成する)*］
カスタム設定を書き込みます。この操作は、SUSE Linux Enterprise Serverのインストール時には利用できません。

［*Read Configuration Saved on Disk (ディスクに保存されている設定を読み込む)*］
独自の`/etc/lilo.conf`をロードします。この操作は、SUSE Linux Enterprise Serverのインストール時には利用できません。

4 ［*OK*］を2回クリックして、変更内容を保存します。

変換中に、古いGRUB設定はディスクに保存されます。これを使用するには、ブートローダのタイプをGRUBに戻し、［*Restore Configuration Saved before Conversion*］を選択します。この操作は、インストール済みのシステムでのみ実行可能です。

注記: カスタムのブートローダ

GRUBやLILO以外のブートローダを使用する場合は、［*ブートローダはインストールしないでください*］を選択します。このオプションを選択する場合には、あらかじめ、ブートローダのドキュメントをよくお読みください。

10.3 Linuxブートローダのアンインストール

YaSTを使用してLinuxブートローダをアンインストールし、MBRをLinuxインストール前の状態に戻すことができます。インストール中に、YaSTは自動的にオリジナルMBRのバックアップコピーを作成しており、要求があるとMBRを復元します。

GRUBをアンインストールするには、YaST を起動して［システム］>［ブートローダ］の順にクリックして、ブートローダモジュールを起動します。［そ

の他］>［*ハードディスクのMBRの復元*］を選択し、［*はい、上書きします*］で確認します。

10.4 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にブートマネージャをインストールできない場合は、Linux用の、すべての起動ファイルを収録したブート可能な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。

手順 10.7 *ブートCDの作成*

1 ISOイメージの作成先ディレクトリに移動します。例:`cd /tmp`

2 GRUBのサブディレクトリを作成し、新たに作成された`iso`ディレクトリに移動します。

```
mkdir -p iso/boot/grub && cd iso
```

3 カーネル、`stage2_eltorito`、`initrd`、`menu.lst`、および`message`ファイルを`iso/boot/`にコピーします。

```
cp /boot/vmlinuz boot/
cp /boot/initrd boot/
cp /boot/message boot/
cp /usr/lib/grub/stage2_eltorito boot/grub
cp /boot/grub/menu.lst boot/grub
```

4 `root (hd`*x*、*y*`)`エントリを`root (cd)`で置き換えて、CD_ROMデバイスをポイントします。また、メッセージファイル、カーネル、およびinitrdに対するパスを調整することが必要になる場合があります。これらのパスはそれぞれ、`/boot/message`、`/boot/vmlinuz`、および`/boot/initrd`を指す必要があります。調整を行った後、`menu.lst`は次の例のようになります。

```
timeout 8
default 0
gfxmenu (cd)/boot/message

title Linux
   root (cd)
   kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
   splash=verbose showopts
   initrd /boot/initrd
```

ブート処理時にブートメッセージの表示を防止するには、「splash=verbose」の代わりに「splash=silent」を使用します。

5 次のコマンドでISOイメージを作成します。

```
genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 \
-o grub.iso /tmp/iso
```

6 好みのユーティリティを使用して、生成されたファイルgrub.isoをCDに書き込みます。ISOイメージをデータファイルとして書き込まず、お使いのCD書き込みユーティリティのCDイメージ書き込みオプションを使用します。

10.5 SUSEのグラフィカル画面

オプションvga=*value*がカーネルパラメータとして使用されている場合、SUSEのグラフィカル画面が1番目のコンソール上に表示されます。YaSTを使用してインストールする場合、このオプションは、選択した解像度とグラフィックカードに基づいて自動的に使用されます。必要な場合にSUSEの画面を無効にするには、3つの方法があります。

必要に応じてSUSE画面を無効にする。
: コマンドラインでコマンド「echo 0 >/proc/splash」を入力し、グラフィカル画面を無効にします。画面を再度有効にするには、「echo 1 >/proc/splash」コマンドを入力します。

デフォルトでSUSE画面を無効にする。
: カーネルパラメータsplash=0をブートローダの設定に追加します。これについては、第10章 *ブートローダGRUB* (127ページ)を参照してください。

ただし、以前のバージョンではデフォルトになっていたテキストモードを使用したい場合は、`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。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。

警告: 未サポート

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。

10.6 トラブルシューティング

ここでは、GRUBを使用してブートする際に頻繁に発生する一部の問題と、考えられる解決策の概略について説明します。一部の問題については、Knowledgebase(ナレッジベース)に記事が提供されています(`http://www.suse.com/support`のSupport Database(サポートデータベース)にあります)。「*GRUB*」、「ブート」、および「ブートローダ」などのキーワードを使って検索を行うには、検索ダイアログを使用します。

GRUBとXFS
XFSの場合、パーティションブートブロックには`stage1`のための余地がありません。そのため、ブートローダの位置としてXFSパーティションを指定しないでください。この問題は、XFSでフォーマットされていない別のブートパーティションを作成することで解決できます。

GRUBのGRUB Geom Errorレポート
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。この場合、BIOSをアップデートします。

また、LinuxがBIOSに登録されていない追加ハードディスクにインストールされている場合にも、GRUBはこのエラーメッセージを戻します。ブートローダの*stage1*は正常に検出されロードされますが、*stage2*は検出され

ません。この問題は、新規ハードディスクをBIOSに登録することで解消できます。

いくつかのハードディスクを搭載したシステムがブートしない
: インストール中、YaSTは、ハードディスクのブートシーケンスを誤って判断する場合があります。たとえば、GRUBがPATA(IDE)ディスクを`hd0`、SCSIディスクを`hd1`と見なしても、BIOS内ではブートシーケンスが逆順(PATAの*前に*SCSI)である場合があります。

  この場合は、ブートプロセス中にGRUBコマンドラインを使用してハードディスクを訂正します。システムのブート後に、`device.map`ファイルを編集して新規マッピングを永続的に適用します。次に、`/boot/grub/menu.lst`ファイルと`/boot/grub/device.map`ファイルでGRUBデバイス名を検査し、次のコマンドでブートローダを再インストールします。

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

2台目のハードディスクからのWindowsのブート
: Windowsのような一部のオペレーティングシステムは、1台目のハードディスクからのみブートできます。この種のオペレーティングシステムが2台目以降のハードディスクにインストールされている場合は、関連メニューエントリに対して論理的な変更を加えることができます。

```
...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

  この例では、Windowsは2台目のハードディスクから起動されます。この目的で、`map`を使用して、ハードディスクの論理的な順序を変更します。この変更は、GRUBのメニューファイル内のロジックには影響を及ぼしません。したがって、2台目のハードディスクは`chainloader`に対して指定する必要があります。

10.7 詳細情報

GRUBの詳細情報は、http://www.gnu.org/software/grub/で入手できます。また、`grub`情報ページも参照してください。「にあるTechnical Information Search(技術情報検索)で、キーワード」GRUBhttp://www.novell

.com/support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。

UEFI (Unified Extensible Firmware Interface)

11

UEFI (Unified Extensible Firmware Interface) は、システムハードウェアに付属のファームウェア、システムのすべてのハードウェアコンポーネント、およびオペレーティングシステムの間のインタフェースです。

UEFIは、従来のPC-BIOSに代わって、PCで幅広く利用されるようになっています。例えば、UEFIは64ビットシステムを適切にサポートし、最も重要な機能の1つである安全なブート(「セキュアブート」、ファームウェアバージョン2.3.1c以降が必要)を提供します。最後に、UEFIを使用すると、すべてのx86プラットフォームで標準のファームウェアが利用可能になります。

さらに、UEFIには以下の利点があります。

- GUIDパーティションテーブル(GPT)を使う大きなディスク(2 TiB以上)からのブート。
- CPUに依存しないアーキテクチャおよびドライバ。
- ネットワーク機能を持つ柔軟なプレOS環境。
- PC-BIOSライクなエミュレーション経由でレガシーオペレーティングシステムのブートをサポートするCSM(Compatibiity Support Module)。

詳細については、http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interfaceを参照してください。以下のセクションは、UEFIの一般的な概要を示すものではなく、SUSE Linux Enterpriseに機能を実装する際のヒントです。

11.1 セキュアブート

UEFIの世界では、ブートストラッププロセスの保護とは、信頼チェーンの確立を意味します。SUSE Linux Enterpriseのコンテキストにおいて、「プラットフォーム」はこの信頼チェーンのルートであり、マザーボードおよびオンボードファームウェアが「プラットフォーム」とみなされます。また、別の言い方をすれば、ハードウェアベンダー、およびそのハードウェアベンダーからコンポーネントの製造元やOSベンダーなどにつながる信頼チェーンです。

信頼は公開鍵の暗号で表されます。ハードウェアベンダーは、ファームウェアにいわゆるプラットフォームキー(PK)を設定し、信頼のルートを表します。オペレーティングシステムベンダーなどとの信頼関係は、このプラットフォームキーを使ってキーに署名することによって文書化されます。

最後に、これらの「信頼された」キーのいずれかで署名されていない限りファームウェアがコード(OSブートローダも、PCI Expressカードやディスクのフラッシュメモリに保存されたドライバも、ファームウェアのアップデートも)を実行できないようにすることによって、セキュリティが確立されます。

基本的に、セキュアブートを使用するには、ファームウェアによって信頼されたキーで署名されたOSローダが必要であり、読み込むカーネルが信頼できることを検証するためにOSローダが必要です。

キー交換キー(KEK)をUEFIキーデータベースに追加できます。この方法で、PKのプライベート部分で署名されている限り、他の証明書を使用できます。

11.1.1 SUSE Linux Enterpriseへの実装

Microsoftのキー交換キー(KEK)がデフォルトでインストールされます。

注記: GUIDパーティションテーブル(GPT)が必要

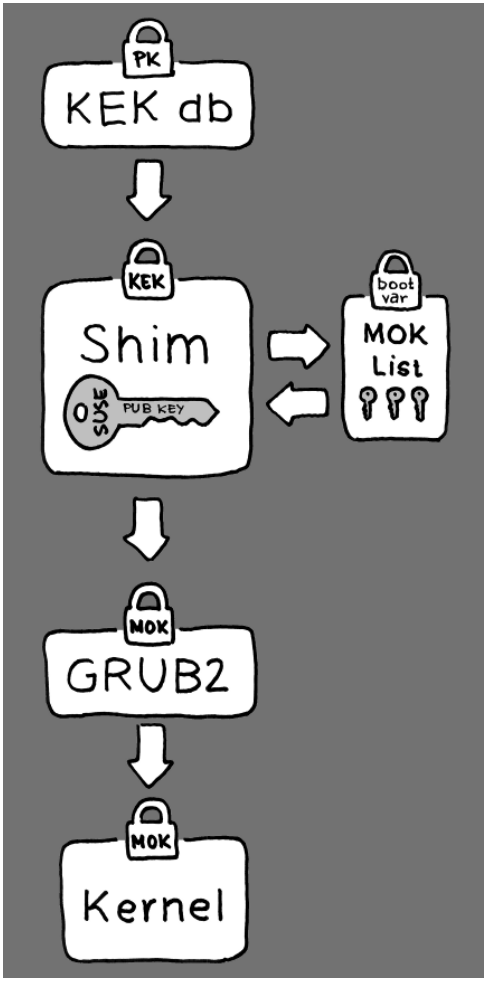
セキュアブート機能を使用するには、マスタブートレコード(MBR)を使用した古いパーティションをGUIDパーティションテーブル(GPT)に置換する必要があります。

YaSTは、インストール時にEFIモードを検出すると、GPTパーティションの作成を試みます。 UEFIでは、FATフォーマットのEFIシステムパーティション(ESP)上でEFIプログラムが見つかるものと想定されます。

UEFIセキュアブートに対応するには、基本的に、ブートローダがデジタル署名されており、ファームウェアがそのデジタル署名を信頼されたキーとして認識することが必要です。SUSE Linux Enterpriseのお客様の利便性を考え、このキーはファームウェアによってあらかじめ信頼されているので、手動介入は不要です。

これには2つの方法があります。1つは、ハードウェアベンダーにSUSEキーを署名してもらい、SUSEがその署名を使ってブートローダに署名する方法です。もう1つは、MicrosoftのWindows Logo Certificationプログラムを利用してブートローダの認定を受け、MicrosoftにSUSE署名キーを認識してもらう(つまり、MicrosoftのKEKを使って署名してもらう)方法です。これで、SUSEは、UEFI署名サービス(この場合はMicrosoft)によって署名されたローダを入手できます。

図 11.1　UEFIのセキュアブートプロセス



実装階層においてSUSEはshimローダを使用します。これは法的問題を回避するスマートなソリューションで、証明書および署名の手順が大幅に簡素化されます。shimローダのジョブは、eLILOやGRUB2などのブートローダをロードすることです。次にこのブートローダが、SUSEキーのみで署名されたカーネルをロードします。SUSEは、UEFIセキュアブートが有効化されたSLE11 SP3の新規インストールで、この機能を提供します。

信頼ユーザには2種類あります。

- 1つ目は、キーを保持するユーザです。プラットフォームキー(PK)によって、ほとんどすべてのことが許可されます。キー交換キー(KEK)では、PKの変更を除き、PKに可能なすべてのことが許可されます。

- 2つ目は、マシンに物理的にアクセスできる任意のユーザです。物理的にアクセスできるユーザは、マシンを再起動したりUEFIを設定したりできます。

UEFIには、これらのユーザのニーズを満たすため、2種類の変数があります。

- 1つ目は「認証変数」と呼ばれるもので、ブートプロセス(いわゆるブートサービス環境)および実行中のOSの両方から更新できますが、更新できるのは、古い変数値の署名に使用されたものと同じキーを使って新しい変数値が署名されている場合のみです。また、この変数は、より大きなシリアル番号を持つ値にのみ追加または変更できます。

- 2つ目は、「ブートサービス専用変数」と呼ばれるものです。この変数は、ブートプロセス中に動作する任意のコードにアクセスできます。ブートプロセスの終了後、OSが起動する前に、ブートローダは`ExitBootServices`コールを呼び出す必要があります。その後、これらの変数にはアクセスできなくなり、OSはこれらに触れられません。

さまざまなUEFIキーリストは1つ目のタイプなので、オンラインでの更新、追加、および、キー/ドライバ/ファームウェアの指紋のブラックリスト登録ができます。セキュアブートの実装に役立つのは、2つ目の「Boot Service Only Variable(ブートサービス専用変数)」です。これは、安全かつオープンソースで使いやすくなっており、GPL v3と互換性があるためです。

SUSEは、最初にFedoraによった開発された`shim`(小さくシンプルなEFIブートローダ)で起動します。システム上のUEFIキーデータベースで利用可能なKEKにもとづいて、SUSE KEKで署名された証明書およびMicrosoft発行の証明書によって署名されます。

これによって`shim`のロードおよび実行が可能になります。

`shim`は、続いて、ロードしようとしているブートローダが信頼されていることを確認します。 デフォルトで、`shim`は、本体に組み込まれている独自のSUSE証明書を使用します。また、`shim`は、追加のキーを「登録」してデフォルトのSUSEキーを上書きできます。以下、これらを「マシン所有者キー」、または省略してMOKと呼びます。

次に、ブートローダはカーネルを検証および起動し、カーネルがモジュールで同じことを実行します。

11.1.2 Machine Owner Key(マシン所有者キー、MOK)

ユーザ(「マシンの所有者」)がブートプロセスの任意のコンポーネントを置換する場合は、Machine Owner Key(マシン所有者キー、MOK)を使用します。mokutilsツールがコンポーネントの署名およびMOKの管理を支援します。

登録プロセスでは、まずマシンを起動し、shimのロードで(キーを押すなどして)ブートプロセスを中断します。これによってshimが登録モードに移行するので、ユーザは、デフォルトのSUSEキーをブートパーティションのファイルに含まれるキーに置換できます。ユーザがこの処理を選択すると、shimはそのファイルのハッシュを計算し、結果を「Boot Service Only(ブートサービス専用)」変数にします。これによってshimは、ブートサービス以外でファイルが変更された場合にその変更を検出でき、ユーザ承認済みのMOKリストの改ざんを回避できます。

これらすべてがブート時に行われ、検証済みのコードのみが実行されます。このため、コンソールにいるユーザのみがマシン所有者のキーセットを使用できます。OSにリモートアクセスするマルウェアやハッカーではあり得ません。ハッカーやマルウェアはファイルの変更しかできず、「Boot Service Only(ブートサービス専用)」変数に保存されたハッシュを変更できないためです。

いったんロードされshimによって検証されたブートローダは、カーネルを検証する場合はshimにコールバックします(検証コードの複製を避けるため)。shimはMOKと同じリストを使用し、カーネルをロードできるかどうかをブートローダに知らせます。

このようにして、独自のカーネルまたはブートローダをインストールできます。物理的にそこにいることによって新しいキーセットをインストールしそれを認証する必要があるのは、最初の再起動時のみです。MOKは単一のMOKではなくリストなので、shimに複数のベンダーのキーを信頼させることができ、ブートローダからのデュアルブートやマルチブートが可能です。

11.1.3 カスタムカーネルのブート

以下はhttp://en.opensuse.org/openSUSE:UEFI#Booting_a_custom_kernelにもとづいています。

セキュアブートでは、セルフコンパイルカーネルを使用できます。ただし、独自の証明書を使って署名し、その証明書をファームウェアまたはMOKに知らせる必要があります。

1 カスタムのX.509キー、および署名に使用される証明書を作成します。

```
openssl req -new -x509 -newkey rsa:2048 -keyout key.asc \
  -out cert.pem -nodes -days 666 -subj "/CN=$USER/"
```

証明書の作成の詳細については、http://en.opensuse.org/openSUSE:UEFI_Image_File_Sign_Tools#Create_Your_Own_Certificateを参照してください。

2 PKCS#12形式でキーと証明書をパッケージ化します。

```
openssl pkcs12 -export -inkey key.asc -in cert.pem \
  -name kernel_cert -out cert.p12
```

3 pesignとともに使用するNSSデータベースを生成します。

```
certutil -d . -N
```

4 PKCS#12に含まれるキーおよび証明書をNSSデータベースにインポートします。

```
pk12util -d . -i cert.p12
```

5 pesignを使用して、新しい署名でカーネルを「bless」します。

```
pesign -n . -c kernel_cert -i arch/x86/boot/bzImage \
  -o vmlinuz.signed -s
```

6 カーネルイメージの署名をリスト表示します。

```
pesign -n . -S -i vmlinuz.signed
```

その時点で、通常通り/bootにカーネルをインストールできます。カーネルにはカスタム署名があるため、署名に使用された証明書をUEFIファームウェアまたはMOKにインポートする必要があります。

7 ファームウェアまたはMOKにインポートするため、証明書をDERフォーマットに変換します。

```
openssl x509 -in cert.pem -outform der -out cert.der
```

8 よりアクセスしやすくするため、証明書をESPにコピーします。

```
sudo cp cert.der /boot/efi/
```

9 mokutilを使用して自動的にMOKリストを起動します。

また、MOKを手動で起動する場合は以下の手順を実行します。

9a 再起動

9b GRUBメニューで「c」キーを押します。

9c 以下のコマンドをタイプします。

```
chainloader $efibootdir/MokManager.efi
boot
```

9d ［*Enroll key from disk*］を選択します。

9e cert.derファイルに移動してEnterキーを押します。

9f 指示に従ってキーを登録します。通常、「0」を押してから「y」を押して確認します。

また、ファームウェアメニューに、署名データベースに新しいキーを追加する方法が用意されている場合があります。

11.1.4 制限

セキュアブートモードでブートする場合、以下の制限が適用されます。

- ハイブリッド化されたISOイメージは、UEFIシステムでブート可能とみなされません。このため、USBデバイスからのUEFIブートは、SP3でサポートされません。
- セキュアブートを簡単に回避できないようにするため、セキュアブートで実行する場合は一部のカーネル機能が無効になっています。
- ブートローダ、カーネル、およびカーネルモジュールが署名されている必要があります。
- kexecおよびkdumpが無効になっています。
- ハイバネーション(ディスクの休止)は無効になっています。
- ルートユーザであっても、`/dev/kmem`および`/dev/mem`にアクセスできません。
- ルートユーザであっても、I/Oポートにアクセスできません。すべてのX11グラフィカルドライバはカーネルドライバを使用する必要があります。
- sysfs経由でPCI BARにアクセスすることはできません。
- ACPIの`custom_method`は使用できません。
- asus-vmiモジュールに対してdebufgsを使用できません。
- `acpi_rsdp`パラメータはカーネルに影響を及ぼしません。

11.2 さらに詳細な説明が必要な場合は

- http://www.uefi.org —UEFIのホームページです。現在のUEFI仕様が掲載されています。
- Olaf Kirch氏およびVojtěch Pavlík氏によるブログ記事(上の章の内容はこれらの記事にもとづいています)。
    - http://www.suse.com/blogs/uefi-secure-boot-plan/
    - http://www.suse.com/blogs/uefi-secure-boot-overview/

    - http://www.suse.com/blogs/uefi-secure-boot-details/

- http://en.opensuse.org/openSUSE:UEFI —UEFIとopenSUSEに関するページです。

12 特別なシステム機能

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。

12.1 特殊ソフトウェアパッケージ

bash、cron、logrotate、locate、ulimit、freeといったプログラムは、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。

12.1.1 bashパッケージと/etc/profile

Bashはデフォルトのシステムシェルです。ログインシェルとして使用する場合には、いくつかの初期化ファイルを読み込みます。Bashは、各ファイルを次の順序で処理します。

1. /etc/profile

2. ~/.profile

3. /etc/bash.bashrc

4. ~/.bashrc

~/.profileまたは~/.bashrcに、カスタム設定を行います。これらのファイルを正しく処理するには、基本設定ファイル/etc/skel/.profileまたは/etc/skel/.bashrcを、ユーザのホームディレクトリにコピーする必要があります。更新後、/etc/skelから設定ファイルをコピーすることをお勧めします。次のシェルコマンドを実行して、既存の個人別設定が失われるのを防止します。

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

それから、個人的な調整点を、*.oldファイルから書き戻します。

12.1.2 cronパッケージ

コマンドを、前もって決めた時間に、定期的かつ自動的にバックグラウンドで実行したい場合、cronを用います。cronは特別な形式のタイムテーブルに従って起動します。その一部はシステムに付属しています。ユーザは必要に応じ、独自のテーブルを作成できます。

cronテーブルは、/var/cron/tabsにあります。/etc/crontabはシステム全体のcronテーブルとして機能します。ユーザ名を入力して、タイムテーブルの後、コマンドの前に直接コマンドを実行するようにします。例12.1 「/etc/crontab内のエントリ」 (164 ページ)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です。cronのマニュアルページを参照してください(man cron使用)。

例 12.1　/etc/crontab内のエントリ

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

/etc/crontabを、crontab -eコマンドで編集することはできません。これは、エディタに直接ロードして、変更し、保存する必要があります。

複数のパッケージによりシェルスクリプトが/etc/cron.hourly、/etc/cron.daily、/etc/cron.weekly、および/etc/cron.monthlyの各ディレクトリにインストールされます。これらの実行は、/usr/lib/cron/run-cronsによって制御されます。/usr/lib/cron/run-cronsは、15分おきにメインテーブル(/etc/crontab)から実行されます。これにより、無視されていたプロセスが、適切な時刻に実行されることが保証されます。

hourly、daily、または他の特定の周期の管理スクリプトをカスタム時間で実行するには、/etc/crontabのエントリを使用して、定期的にタイムスタンプファイルを削除します(例12.2「/etc/crontab:タイムスタンプファイルの削除」 (165 ページ)を参照してください。そこでは、hourlyという名前の付いているファイルが毎時59分に、dailyという名前の付いているファイルが毎日午前2時14分に削除されるようになっています)。

例 12.2　/etc/crontab:タイムスタンプファイルの削除

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

または、/etc/sysconfig/cronのDAILY_TIMEをcron.dailyを起動する時刻に設定します。MAX_NOT_RUNの設定では、ユーザが長期間、指定したDAILY_TIMEにコンピュータを起動しなくても、毎日のタスクの実行がトリガされるようにします。MAX_NOT_RUNの最大値は14日です。

日常のシステムメンテナンスジョブは、わかりやすいようにさまざまなスクリプトに分散されています。これらはパッケージaaa_baseに含まれています。/etc/cron.dailyに含まれています。このパッケージには、たとえば、コンポーネントsuse.de-backup-rpmdb、suse.de-clean-tmp、またはsuse.de-cron-localが含まれています。

12.1.3 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ス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、一定間隔で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で実行できます。通常、これらのログファイルは、FHSで指定されるように/var/log内に格納され、毎日記録が追加されるためにサイズが増大します。logrotateパッケージを使用して、これらのファイルが増大するのを制御できます。

/etc/logrotate.confファイルを使用して、logrotateを設定します。特に、includeには、最初に読み込む追加ファイルを設定します。ログファイルを生成しないプログラムは、個別の環境設定ファイルを/etc/logrotate.dにインストールします。たとえば、そのようなファイルは、出荷時には、apache2パッケージ (/etc/logrotate.d/apache2)およびsyslogdパッケージ (/etc/logrotate.d/syslog)に含まれています。

例 12.3　/etc/logrotate.confの例

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotateは、cronによって制御され、/etc/cron.daily/logrotateにより毎日呼び出されます。

重要

createオプションは、管理者によって/etc/permissions*内に作成されるすべての設定を読み取ります。個人的な変更によっていずれの競合も発生することがないようにしてください。

12.1.4 locateコマンド

ファイルをすばやく検索するためのコマンドlocate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findutils-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。

12.1.5 ulimitコマンド

ulimit(*user limits*)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定して、それを表示できます。ulimitはアプリケーションが使用できるメモリの制限に特に役立ちます。これを使用して、アプリケーションがシステムリソースを過剰に使用して速度が低下したり、オペレーティングシステムをハングさせたりすることを防止できます。

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12.1「ulimit:ユーザのためのリソースの設定」(167ページ)に示すオプションを使用します。

表 12.1　ulimit:ユーザのためのリソースの設定

-m	最大常駐セットサイズ
-v	シェルが使用できる仮想メモリの最大量
-s	最大スタックサイズ
-c	作成されるコアファイルの最大サイズ

-a	すべての現在の制限値の報告

システム全体のエントリは、/etc/profileで設定できます。コアファイルの作成を有効にします(プログラマがデバッグを行うために必要)。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 12.4　ulimit:~/.bashrc中の設定

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

メモリ割り当ては、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

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。

12.1.6 freeコマンド

freeコマンドは、空いている物理メモリ、使用済み物理メモリ、システム内のスワップ領域のほか、カーネルによって消費されたバッファとキャッシュの合計量を表示します。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。

ただし、目的が現在のRAM使用量である場合は、/proc/meminfoで情報を見つけてください。

12.1.7 manページとinfoページ

一部のGNUアプリケーション(tarなど)では、manページが提供されなくなりました。manページが用意されていたコマンドについては、--helpオプションを使用して簡単な概要を表示するか、詳細な手順を説明するinfoページを使用します。infoは、 GNUのハイパーテキストシステムです。このシステムについての説明は、「info info」と入力してください。Infoページは、「emacs -f info」コマンドを入力してEmacsを起動するか、コンソールで直接「info」と入力します。あるいは、tkinfo、xinfo、またはヘルプシステムを使用して、infoページを表示できます。

12.1.8 manコマンドを使用したマニュアルページの選択

マニュアルページを読み込むには、man マニュアルページを入力します。同じ名前でさまざまなセクションに存在するマニュアルページは、対応するセクション番号とともに一覧表示されます。表示するマニュアルページを選択します。セクション番号を数秒内に入力しないと、最初のマニュアルページが表示されます。

これをデフォルトのシステム動作に戻すには、~/.bashrcなどのシェル初期化ファイルでMAN_POSIXLY_CORRECT=1を設定します。

12.1.9 GNU Emacs用の設定

GNU Emacsは、複合作業環境です。ここでは、GNU Emacsを起動する際に処理される設定ファイルについて説明します。詳細については、http://www.gnu.org/software/emacs/を参照してください。

Emacsは起動時に、カスタマイズまたは事前設定に関するユーザ、システム管理者、およびディストリビュータの設定が含まれるいくつかのファイルを読み取ります。~/.emacs初期化ファイルは、/etc/skelから各ユーザのホームディレクトリにインストールされます。その後、.emacsは、/etc/skel/.gnu-emacsファイルを読み取ります。プログラムをカスタマイズするには、.gnu-emacsをホームディレクトリにコピーし(cp /etc/skel/.gnu-emacs ~/.gnu-emacsを使用)、このディレクトリで希望どおりに設定します。

.gnu-emacsは、~/.gnu-emacs-customファイルをcustom-fileとして定義します。Emacsでcustomizeを使用して設定を行う場合、この設定は、~/.gnu-emacs-customに保存されます。

SUSE Linux Enterprise Serverでは、emacsパッケージはsite-start.elファイルを /usr/share/emacs/site-lispディレクトリにインストールします。site-start.elファイルは、~/.emacs初期化ファイルの前にロードされます。site-start.elは、psgmlなどのEmacsアドオンパッケージと共に配布される特殊な設定ファイルが自動的にロードされるようにします。この種類の設定ファイルも/usr/share/emacs/site-lispに置かれ、ファイル名は常にsuse-start-で始まります。ローカルのシステム管理者は、default.elでシステム全体の設定を指定できます。

これらのファイルに関する詳しい説明は、*Init File*: info:/emacs/InitFile. これらのファイルを無効にする(必要な場合)方法についても記載されています。

Emacsのコンポーネントは、いくつかのパッケージに分かれています。

- 基本パッケージのemacs。
- emacs-x11(通常インストールされている): *X11*をサポートしているプログラム。

- `emacs-nox`: *X11*をサポートしていないプログラム。
- `emacs-info`: info形式のオンラインマニュアル。
- `emacs-el`: Emacs Lisp内のコンパイルされていないライブラリファイル。これらは、実行時には必要ありません。
- 必要に応じて`emacs-auctex`(LaTeX)、`psgml`(SGMLおよびXML)、`gnuserv`(クライアント/サーバ操作)など、さまざまなアドオンパッケージをインストールできます。

12.2 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。Alt＋F1からAlt＋F6を使用して切り替えます。7番目のコンソールはX用に予約されており、10番目のコンソールにはカーネルメッセージが表示されます。コンソールの割り当て数は、`/etc/inittab`ファイルを修正すれば変更できます。

Xを終了せずにXからコンソールに切り替えるには、Ctr＋Alt＋F1からCtrl＋Alt＋F6を使用します。Xに戻るには、Alt＋F7を押します。

12.3 キーボードマッピング

プログラムのキーボードマッピングを標準化するために、次のファイルに変更が行われました。

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.emacs
/etc/skel/.gnu-emacs
/etc/skel/.vimrc
/etc/csh.cshrc
/etc/termcap
/usr/share/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

これらの変更は、terminfoエントリを使用するアプリケーション、または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、emacsなど)にのみ影響します。システムに付随しないアプリケーションは、これらのデフォルト値に合わせる必要があります。

Xの下では、<compose>キー(マルチキー)を/etc/X11/Xmodmapで説明されているように有効化できます。

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。

ヒント: 詳細情報

XKBに関する情報は、/usr/share/doc/packages/xkeyboard-config(xkeyboard-configパッケージの一部)に記載されている文書を参照してください。

12.4 言語および国固有の設定

本システムは、非常に広い範囲で国際化されており、現地の状況に合わせて柔軟に変更できます。言い換えれば、国際化(*I18N*)が特定のローカライズ(*L10N*)を可能にします。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_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、RC_LANGだけが設定されます。これにより、ユーザが独自の変数を入力しやすくなります。

ROOT_USES_LANG
: yesまたはno変数。noに設定するとrootが常にPOSIX環境で動作します。

変数は、YaSTのsysconfigエディタで設定できます(9.3.1項 「YaSTのsysconfigエディターを使ってシステム設定を変更する」 (124ページ)を参照してください)。このような変数の値には、言語コード、国コード、エンコーディング、および修飾子が入っています。個々のコンポーネントは特殊文字で接続されます。

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

12.4.1 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ISO 3166にリストされています(http://en.wikipedia.org/wiki/ISO_3166を参照)。

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。この設定は今では廃止され、UTF-8もユーロ記号を表現します。アプリケーションがISO-8859-15をサポートし、UTF-8をサポートしない場合にのみ役に立ちます。

以前のリリースでは、/etc/sysconfig/languageの変更後は必ず、SuSEconfigを実行する必要がありました。その場合、SuSEconfigは、変更内容を/etc/SuSEconfig/profile と/etc/SuSEconfig/csh.loginに書き込みました。これらのファイルは、ログイン時に、/etc/profile(Bashの場合)または/etc/csh.login (tcshの場合)によって読み込まれました。

最近のリリースでは、/etc/SuSEconfig/profileは/etc/profile.d/lang.shで置換され、/etc/SuSEconfig/csh.loginは/etc/profile.de/lang.cshで置換されています。ただし、それらのレガシファイルが存在する場合には、ログイン時にそれらのファイルがまだ読み込みまれます。

現在のプロセスチェーンは、次のとおりです。

- Bashの場合は、/etc/profileによって読み込まれた/etc/profile.d/lang.shが、/etc/sysconfig/languageを解析します。
- tcshの場合は、ログイン時に/etc/csh.loginによって読み込まれた/etc/profile.d/lang.cshが、/etc/sysconfig/languageを解析します。

これによって、/etc/sysconfig/languageに加えられたすべての変更が、SuSEconfigを実行しなくても、各シェルへの次回ログイン時に使用可能になります。

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。

12.4.2 ~/.i18nでのロケール設定

ロケールシステムのデフォルトが不十分な場合、Bashスクリプトの構文に従って~/.i18nの設定を変更してください。~/.i18n内のエントリは、/etc/sysconfig/languageのシステムデフォルトを上書きします。同じ変数名の、RC_ネームスペースプレフィクスなしで使用します。たとえば、RC_LANGではなく、LANGを使用します。

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

12.4.3 言語サポートの設定

カテゴリ*Messages*のファイルは、フォールバックを確保するため、対応する言語ディレクトリ(たとえば、en)にのみ格納されることになっています。たとえばLANGをen_USに設定したが、messageファイルが/usr/share/locale/en_US/LC_MESSAGESに存在しない場合は、/usr/share/locale/en/LC_MESSAGESにフォールバックされます。

フォールバックチェーンも定義できます。たとえば、ブルターニュ語、次いでフランス語、またはガリシア語、次いでスペイン語、次いでポルトガル語の順にフォールバックするには、次のように設定します。

```
LANGUAGE="br_FR:fr_FR"

LANGUAGE="gl_ES:es_ES:pt_PT"
```

必要に応じて、次のようにノルウェー語の方言であるニーノシクやブークモールをノルウェー語の代わりに使用できます(noへのフォールバックを追加します)。

```
LANG="nn_NO"

LANGUAGE="nn_NO:nb_NO:no"
```

または

```
LANG="nb_NO"

LANGUAGE="nb_NO:nn_NO:no"
```

ノルウェー語では、LC_TIMEの扱いも違うので注意してください。

生じる可能性のある1つの問題は、数字の桁を区切るための文字が正しく認識されないことです。このことは、LANGがdeのような2文字の言語コードにのみ設定されているのに、glibcが使用している定義ファイル/usr/share/lib/de_DE/LC_NUMERICに存在している場合に生じます。それで、区切り文字の定義がシステムに認識されるようにするには、LC_NUMERICをde_DEに設定する必要があります。

12.4.4 詳細情報

- 『*The GNU C Library Reference Manual*』の「Locales and Internationalization」の章。glibc-infoパッケージに格納されています。パッケージは、SUSE Linux Enterprise SDKから入手できます。SDKは、SUSE Linux Enterpriseのアドオン製品であり、http://www.novell.com/developer/sle_sdk.htmlからダウンロードできます。
- 『*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。http://tldp.org/HOWTO/Unicode-HOWTO-1.html.

13 プリンタの運用

SUSE® Linux Enterprise Serverは、リモートネットワークプリンタも含め、さまざまな種類のプリンタを使った印刷をサポートしています。プリンタは手動、またはYaSTを使用して設定できます。設定の詳細については、項「プリンタの設定」 (第8章 *YaSTによるハードウェアコンポーネントの設定*, ↑*導入ガイド*)を参照してください。プリントジョブの開始、管理には、グラフィカルインタフェースまたはコマンドラインユーティリティの両方を利用できます。プリンタが正常に動作しない場合は、13.7項 「トラブルシューティング」 (187 ページ)を参照してください。

CUPS(Common Unix Printing System)は、SUSE Linux Enterprise Serverの標準印刷システムです。

プリンタは、インタフェース(USB、ネットワークなど)と、プリンタ言語によって区別できます。プリンタの購入時には、プリンタにご利用のハードウェアで利用できるインタフェース(USBやパラレルポートなど)が搭載されていること、およびプリンタの対応言語が正しいことをご確認ください。プリンタは、次の3つのプリンタ言語クラスに基づいて分類できます。

PostScriptプリンタ
: PostScriptは、LinuxとUnix環境のほとんどの印刷ジョブを生成する際に使用されるプリンタ言語であり、内部の印刷システムもこの言語を使用して処理を行います。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。

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としては、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があります。これらのプリンタ言語は、通常、Linuxによってサポートされており、十分な印刷結果が得られています。Linuxは、一部の特殊な印刷機能に対応できない場合があります。HPが開発したHPLIP(HP Linux Imaging and Printing)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ライセンスでそれらをLinuxディストリビュータに提供するプリンタメーカは存在しません。

独自規格のプリンタ(GDIプリンタ)
: これらのプリンタは、共通のプリンタ言語をサポートしていません。これらのプリンタは独自のプリンタ言語を使用しており、新しいエディション/モデルがリリースされると、プリンタ言語も変更される可能性があります。一般的にこのようなプリンタでは、Windowsドライバしか利用できません。詳細については、13.7.1項「標準的なプリンタ言語をサポートしないプリンタ」 (187 ページ)を参照してください。

新しいプリンタを購入する前に、次の各ソース(情報源)を参照し、購入を予定しているプリンタがどの程度までサポートされているかを確認してください。

http://www.linuxfoundation.org/OpenPrinting/
: プリンタデータベースのあるOpenPrintingホームページです。このデータベースは、最新のLinuxサポートステータスを示します。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「完全にサポート済み」と評価されているプリンタであっても、最新バージョンのSUSE Linux Enterprise Server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。

http://pages.cs.wisc.edu/~ghost/
: GhostscriptのWebページ。

/usr/share/doc/packages/ghostscript-library/catalog.devices
付属するドライバのリスト

13.1 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の情報から構成されますが、その情報には、プリンタの名前またはプリンタキューの名前だけでなく、必要に応じて、プリンタ固有のオプションなど、フィルタに関する情報も含まれます。

各プリンタには、1つ以上の専用プリンタキューが存在しています。指定のプリンタがデータを受け取れるようになるまで、スプーラは印刷ジョブをキュー内に留めています。プリンタの準備が整うと、スプーラはフィルタおよびバックエンドを経由して、プリンタにデータを送信します。

このフィルタは、印刷中のアプリケーションが生成したデータ(通常的はPostScriptやPDFですが、ASCII、JPEGなどの場合もあります)を、プリンタ固有のデータ(PostScript、PCL、ESC/Pなど)に変換します。プリンタの機能については、PPDファイルに記述されています。PPDファイルには、プリンタ固有のオプションが記述されています。各オプションに対しては、プリンタでそのオプションを有効にするために必要なパラメータが指定されています。フィルタシステムは、ユーザが有効として選択したオプションを確認します。

PostScriptプリンタを選択すると、フィルタシステムがデータをプリンタ固有のPostScriptに変換します。この変換にプリンタドライバは必要ありません。PostScript非対応プリンタを使用すると、フィルタシステムが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。

13.2 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。

► **System z:** IBM System zのメインフレームとローカルに接続するz/VMによって提供されるプリンタおよびその類似デバイスは、CUPSまたはLPRngのどちらにもサポートされていません。これらのプラットフォーム上では、ネットワーク経由の印刷だけを利用できます。ネットワークプリンタのケーブリング(ケーブル接続)は、プリンタメーカの指示にしたがって設置する必要があります。 ◄

警告: 稼働中システムのケーブル接続の変更

プリンタをコンピュータに接続する場合、コンピュータの動作中に接続と取り外しを行って良いのはUSBデバイスだけであることに注意してください。システムやプリンタの損傷を回避するために、USB以外の接続を変更する場合は、あらかじめシステムをシャットダウンしてください。

13.3 ソフトウェアのインストール

PPD (PostScript printer description、PostScriptプリンタ記述)は、PostScriptプリンタの特性(解像度など)やオプション(両面印刷ユニットなど)を記述するコンピュータ言語です。これらの記述は、CUPS側でさまざまなプリンタオプションを使用するために必須です。PPDファイルがない場合、印刷データは「raw」(ロー、未加工)状態でプリンタへ送信されますが、そのことは通常は望ましくありません。SUSE Linux Enterprise Serverのインストール時に、多数のPPDファイルがプレ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。および13.7.2項 「特定のPostScriptプリンタに適したPPDファイルが入手できない」 (188 ページ)を参照してください。13.6.2項 「各種パッケージ内のPPDファイル」 (185 ページ)

新しいPPDファイルは、`/usr/share/cups/model/`ディレクトリ内に保存するか、YaSTで印刷システムに追加できます(項 「YaSTによるドライバの追加」 (第8章 *YaSTによるハードウェアコンポーネントの設定*, ↑*導入ガイド*)参照)。その後は、プリンタのセットアップ時にPPDファイルを選択できるようになります。

プリンタメーカーがソフトウェアパッケージ全体をインストールさせようとする場合には注意してください。第一に、このタイプのインストールを行うと、SUSE Linux Enterprise Serverによって提供されているサポートが失われる場合があります。第二に、印刷コマンドが異なる動作をする可能性があり、システムが他のメーカーのデバイスに対応できなくなる場合があります。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。

13.4 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が標準化されているので、一部のメーカーは標準を変更します。そして、メーカーは、2、3のオペレーティングシステムにのみ対応するドライバを提供します。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。

socket
: ソケットは、プレインプリントデータのTCPソケットへの直接送信に使用される接続です。一般的に使用されるsocketのポート番号のいくつかは、`9100`または`35`です。デバイスURI (uniform resource identifier)の構文は、socket://*プリンタの`IP`:ポート*です(たとえば、`socket://192.168.2.202:9100/`)。

LPD (line printer daemon、ラインプリンタデーモン)
: LPDプロトコルについては、RFC 1179で説明されています。このプロトコルの下では、プリンタキューのIDなど、一部のジョブ関連データが送信されてから、実際の印刷データが送信されます。したがって、LPDプロトコルの設定時には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。LPDサービスが使用するポート番

号は515です。デバイスURIの例は、lpd://192.168.2.202/LPT1です。

IPP (Internet Printing Protocol、インターネット印刷プロトコル)
IPPは、HTTPプロトコルに基づいた比較的新しい(1999年)プロトコルです。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。IPPを正しく設定するには、印刷キューの名前は必須です。IPPのポート番号は631です。デバイスURIの例は、ipp://192.168.2.202/psおよびipp://192.168.2.202/printers/psです。

SMB (Windows共有)
CUPSは、Windows共有に接続されたプリンタへの印刷もサポートしています。この目的で使用されるプロトコルは、SMBです。SMBは、ポート番号137、138、および139を使用します。デバイスURIの例は、smb://user:password@workgroup/smb.example.com/printer、smb://user:password@smb.example.com/printer、およびsmb://smb.example.com/printerです。

設定を行う前に、プリンタがサポートしているプロトコルを決定する必要があります。メーカーから必要な情報が提供されていない場合は、コマンドnmap(nmapパッケージに付属)を使用して、プロトコルを推定します。nmapはホストのオープンポートを確認します。例:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

13.4.1 コマンドラインツールによるCUPS設定

CUPSは、lpinfo、lpadmin、lpoptionsなどのコマンドラインツールで設定できます。バックエンド(パラレルなど)とパラメータで構成されるデバイスURIが必要です。システム上の有効なデバイスURIを決定するには、コマンドlpinfo -v | grep ":/"を使用します。

```
# lpinfo -v | grep ":/"
direct usb://ACME/FunPrinter%20XL
direct parallel:/dev/lp0
```

lpadminを使用すると、CUPSサーバ管理者は、印刷キューの追加、削除、または管理を実行できます。プリントキューを追加するには、次の構文を使用します。

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

このデバイス(-v)は、指定したPPDファイル(-P)を使用して、queue(-p)として使用できます。プリンタを手動で設定する場合は、このPPDファイルとデバイスのURIを把握しておく必要があります。

-Eは、最初のオプションとして使用しないでください。どのCUPSコマンドでも、-Eを最初の引数として使用した場合、暗号化接続を使用することを暗示的に意味します。プリンタを使用可能にするには、次の例に示す方法で-Eを使用する必要があります。

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

ネットワークプリンタの設定例:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

lpadminのオプションの詳細は、lpadmin(8)のマニュアルページを参照してください。

プリンタのセットアップ時には、一部のオプションがデフォルトとして設定されています。これらのオプションは、各印刷ジョブ用に変更できます(使用される印刷ツールに依存)。YaSTを使用して、これらのデフォルトオプションを変更することもできます。コマンドラインツールを使用して、デフォルトオプションを次のように設定します。

1 最初に、すべてのオプションを列挙します。

```
lpoptions -p queue -l
```

例:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

アクティブになったデフォルトオプションは、先頭にアスタリスク(*)が付いています。

2 次のようにlpadminを使用してオプションを変更します。

```
lpadmin -p queue -o Resolution=600dpi
```

3 新しい設定値の確認:

```
lpoptions -p queue -l

Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

標準ユーザがlpoptionsを実行すると、設定が~/.cups/lpoptionsに書き込まれます。ただし、root設定は/etc/cups/lpoptionsに書き込まれます。

13.5 コマンドラインからの印刷

コマンドラインから印刷するには、コマンド「lp -d *queuenamefilename*」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。

13.6 SUSE Linux Enterprise Serverでの特殊機能

CUPSの多くの機能は、SUSE Linux Enterprise Server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。

13.6.1 CUPSとファイアウォール

SUSE Linux Enterprise Serverのデフォルトインストールの実行後、SuSEFirewall2はアクティブになり、ネットワークインタフェースは着信トラフィックをブロックするExternal Zoneに設定されます。SuSEFirewall2設定の詳細については、項 「SuSEfirewall2」 (第15章 *Masquerading and Firewalls*, ↑*Security Guide (セキュリティガイド)*)を参照してください。

13.6.1.1 CUPSクライアント

通常、CUPSクライアントはファイアウォール内部の信頼されるネットワーク環境の通常のワークステージョンで実行されます。この場合、ネットワークインタフェースを内部ゾーンに設定し、ワークステーションにネットワーク内部から到達できるようにすることを推奨します。

13.6.1.2 CUPSサーバ

CUPSサーバがファイアウォールで保護された信頼済みネットワーク環境の一部の場合、ネットワークインタフェースはファイアウォールの内部ゾーンに設定します。CUPS設定で特別なファイアウォールルールおよびセキュア設定により保護する場合を除いて、信頼できないネットワーク環境でCUPSサーバを設定することはお勧めできません。

13.6.2 各種パッケージ内のPPDファイル

YaSTのプリンタ設定では、`/usr/share/cups/model/`にインストールされたPPDファイルを使用して、CUPSのキューがセットアップされます。プリンタモデルに適合するPPDファイルを見つけるため、YaSTはハードウェア検出時に判別されたベンダおよびモデルを、すべてのPPDファイル内の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。

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。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、`gutenprint`パッケージ内にあるGutenprint 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。

13.6.2.1 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

13.6.2.2 cups-driversパッケージ内のPPDファイル

通常、Foomaticプリンタフィルタのfoomatic-ripは、PostScript非対応プリンタ用のGhostscriptと組み合わせて使用されます。適切なFoomatic PPDファイルには、*NickName: ... Foomatic/Ghostscript driverおよび*cupsFilter: ... foomatic-ripのエントリがあります。これらのPPDファイルは、cups-driversパッケージ内にあります。

YaSTでは一般に、manufacturer-PPDファイルが優先されます。ただし、適切なmanufacturer-PPDファイルが存在しない場合は、*NickName: ... Foomatic ... (recommended)エントリを含むFoomatic PPDファイルが選択されます。

13.6.2.3 gutenprintパッケージのGutenprint 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、Gutenprint(以前のGIMP-Print)から取得したCUPSフィルタrastertogutenprintを使用できます。このフィルタと、適切なGutenprint PPDファイルは、gutenprintパッケージ内に用意されています。Gutenprint PPDファイルは/usr/share/cups/model/gutenprint/内に配置されていて、そのファイル内にエントリ*NickName: ... CUPS+Gutenprintおよび*cupsFilter: ... rastertogutenprintがあります。

13.6.2.4 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。manufacturer-PPDsパッケージから得られたPPDファイルが優先されます。ただし、モデル名が一致しない場合は、YaSTがmanufacturer-PPDパッケージからのPPDファイルを使用することはできません。これは、Funprinter 12xxシリーズなど、類似モデルについて1つのPPDファイルのみがmanufacturer-PPDパッケージに含まれる場合に該当します。この場合は、YaSTで対応するPPDファイルを手動で選択します。

13.7 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。GDIプリンタ、PPDファイル、およびポート設定などのトピックをカバーしています。一般的なネットワークプリンタに関する問題、印刷に問題がある場合、およびキュー処理についても対処しています。

13.7.1 標準的なプリンタ言語をサポートしないプリンタ

これらのプリンタは、共通のプリンタ言語をサポートしておらず、独自のコントロールシーケンスを使用しないと対処できません。そのため、これらのプリンタは、メーカがドライバを添付した特定のバージョンのオペレーティングシステムでのみ動作します。GDIは、Microsoft*がグラフィックデバイス用に開発したプログラミングインタフェースです。通常、メーカーはWindows用のドライバだけを提供しており、WindowsドライバはGDIインタフェースを使用しているため、これらのプリンタは「*GDIプリンタ*」と呼ばれることもあります。実質的な問題は、このプログラミングインタフェースではなく、これらのプリンタを制御できるのは、各プリンタモデルが採用している独自のプリンタ言語のみという事実にあります。

いくつかのGDIプリンタは、GDIモードと標準的なプリンタ言語のいずれかの間で操作を切り替えることができます。切り替えができるかどうかは、プリンタのマニュアルを参照してください。モデルによっては、切り替えを行うために特別なWindowsソフトウェアが必要なこともあります(Windowsから印刷する場合、Windowsプリンタドライバは常にプリンタをGDIモードに切り替える場合があることに注意してください)。他のGDIプリンタでは、標準のプリンタ言語を利用するための拡張モジュールが用意されています。

一部のメーカは、プリンタに独自規格のドライバを提供しています。独自規格のプリンタドライバの欠点は、インストール済みの印刷システムとそのドライバを組み合わせたときに動作するという保証も、さまざまなハードウェアプラットフォームに適しているという保証もないことです。一方、標準的なプリンタ言語をサポートするプリンタは、特殊なバージョンの印刷システムや特殊なハードウェアプラットフォームに依存しません。

専有のLinuxドライバを機能させようと時間を費やす代わりに、標準プリンタ言語(PostScript推奨)をサポートするプリンタを購入する方が費用効率が高い場合があります。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。

13.7.2 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`パッケージに、PostScriptプリンタに適したPPDファイルが含まれていない場合は、プリンタメーカのドライバCDにあるPPDファイルを使用したり、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ます。

PPDファイルがzipアーカイブ(.zip)または自己展開zipアーカイブ(`.exe`)の形で提供されている場合、`unzip`を使用してそのファイルを展開します。最初に、PPDファイルのライセンス(許諾契約)条項を読みます。次に`cupstestppd`ユーティリティを使って、PPDファイルが「Adobe PostScript Printer Description File Format Specification, version 4.3」に準拠しているかどうかを確認します。「FAIL」ユーティリティから失敗が返された場合は、PPDファイル中のエラーは深刻なもので、問題を引き起こす可能性があります。`cupstestppd`によって報告された問題点は、取り除く必要があります。必要に応じて、適切なPPD

ファイルが入手できるかどうかをプリンタメーカに問い合わせることも考えられます。

13.7.3 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アドレス:378 (16進)
- 割り込み:無関係
- モード:Normal (通常)、SPP、またはOutput Only (出力専用)
- DMA:無効

これらの設定値を使用した場合でも、パラレルポートに接続したプリンタを使用できない場合、BIOS内での設定値に合わせて、I/Oアドレスを0x378という形で/etc/modprobe.conf内に明示的に入力します。2つのパラレルポートが存在し、それぞれのI/Oアドレスが378と278 (16進)に設定されている場合、それらを0x378,0x278という形で入力します。

割り込み(IRQ) 7が空いている場合、例13.1「/etc/modprobe.conf:最初のパラレルポートの割り込みモード」(189ページ)に示すエントリを使用して、その割り込みを有効にすることもできます。割り込みモードを有効にする前に、/proc/interruptsファイルを参照して、すでに使用中の割り込みを調べます。現時点で使用中の割り込みだけが表示されます。どのハードウェアコンポーネントがアクティブになっているかに応じて、この表示は変化することがあります。パラレルポート用の割り込みは、他のどのデバイスも使用してはなりません。自信がない場合、irq=noneを指定してポーリングモードを使用します。

例 13.1　/etc/modprobe.conf:最初のパラレルポートの割り込みモード

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

13.7.4 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ネットワークの確認
: TCP/IPネットワークと名前解決が正しく機能していることが必要です。

リモートlpdの確認
: 次のコマンドを使用して、*host*上のlpd(ポート515)に対するTCP接続を確立できるかどうかをテストします。

```
netcat -z host 515 && echo ok || echo failed
```

lpdへの接続を確立できない場合、lpdがアクティブになっていないか、ネットワークの基本的な問題があります。

rootユーザで次のコマンドを使用し、リモート*host*上の*queue*に関するステータスレポート(おそらく、非常に長い)を照会することもできます。これは、該当のlpdがアクティブで、そのホストが照会を受け付けることを前提にしています。

```
echo -e "\004queue" \
| netcat -w 2 -p 722 host 515
```

lpdが応答しない場合、それがアクティブになっていないか、ネットワークの基本的な問題が発生している可能性があります。lpdが応答する場合、その応答は、host上にあるqueueを介して印刷ができない理由を示すはずです。例13.2「lpdからのエラーメッセージ」(190ページ)で示す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 13.2　lpdからのエラーメッセージ

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

リモートcupsdの確認
: CUPSネットワークサーバは、デフォルトで、UDPポート631から30秒ごとにキューをブロードキャストできます。したがって、次のコマンドを使

用すると、ブロードキャストするCUPSネットワークサーバがネットワーク内に存在しているかどうかテストすることができます。コマンドを実行する前に、ローカルCUPSデーモンが終了していることを確認します。

```
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13.3「CUPSネットワークサーバからのブロードキャスト」 (191 ページ)に示すようになります。

例 13.3　CUPSネットワークサーバからのブロードキャスト

```
ipp://192.168.2.202:631/printers/queue
```

► **System z:** IBM System zのイーサネットデバイスが、デフォルトではブロードキャストを受信しないことを考慮してください。 ◄

次のコマンドを使用して、*host*上のcupsd(ポート631)に対するTCP接続を確立できるかどうかをテストすることができます。

```
netcat -z host 631 && echo ok || echo failed
```

cupsdへの接続を確立できない場合は、cupsdが有効になっていないか、基本的なネットワークの問題が発生している可能性があります。lpstat -h *host* -l -tは、*host*上のすべてのキューに関するステータスレポート(非常に長い場合がある)を返しますが、それぞれのcupsdが有効になっていて、ホストがクエリを受け入れることが前提になります。

次のコマンドを使用して、*host*上の*queue*が、1つのキャリッジリターン(CR、改行)文字からなる印刷ジョブを受け付けるかどうかをテストできます。何も印刷されないのが妥当です。おそらく、空白のページが排出されるはずです。

```
echo -en "\r" \
| lp -d queue -h host
```

ネットワークプリンタまたは印刷サーバボックスのトラブルシューティング

プリントサーバボックス上のスプーラは時々、複数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。これはプリントサーバボックスのスプーラで発生するため、この問題を解決する方法はありません。回避策として、TCPソケットを使用して、プリントサーバボックスに接続されているプリンタに直接送信することで、プリントサーバボックス内のスプーラを使用しないようにします。詳細については、13.4項 「ネットワークプリンタ」 (181 ページ)を参照してください。

この方法により、印刷サーバボックスは異なる形式のデータ転送(TCP/IPネットワークとローカルプリンタ接続)間の単純なコンバータになります。この方法を使用するには、印刷サーバボックス内にある、該当するTCPポートについて把握する必要があります。プリンタがプリント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、プリントサーバボックスの電源をオンにした後、しばらく経過した時点で、nmapパッケージのnmapユーティリティを使用することにより、このTCPポートを特定できます。たとえば、nmap *IP-address*は、印刷サーバボックスに関して次のような出力をすることがあります。

```
Port        State       Service
23/tcp      open        telnet
80/tcp      open        http
515/tcp     open        printer
631/tcp     open        cups
9100/tcp    open        jetdirect
```

この出力は、印刷サーバボックスに接続されているプリンタが、ポート9100上のTCPソケットを介して使用できることを示します。nmapはデフォルトでは、/usr/share/nmap/nmap-services内でリストされている多数の一般的な既知のポートだけを確認します。可能性のあるすべてのポートをチェックするには、nmap -p *from_port-to_portIP-address*コマンドを使用します。これは、ある程度の時間を要することがあります。詳細な情報については、nmapのマニュアルページを参照してください。

次のようなコマンドを入力します。

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

これは、このポートを通してプリンタを使用できるかどうかをテストするために、該当のポートへ文字列またはファイルを直接送信します。

13.7.5 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)、印刷システムはこれを検出しません。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PPDファイルを選択します。

13.7.6 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と報告される前に、バックエンドは何回の試行の失敗が妥当で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はそれぞれのキュー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cupsenable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。

13.7.7 CUPS参照:印刷ジョブの削除

CUPSネットワークサーバが参照機能を使用して自らのキューをクライアントホストへブロードキャストし、クライアントホスト側で適切なローカルcupsdがアクティブになっている場合、クライアント側のcupsdはアプリケーションから印刷ジョブを受け付け、サーバ側のcupsdへそれらを転送します。サーバ上でcupsdが印刷ジョブを受け付けると、そのジョブには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で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時点で、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したい場合、lpstat -h cups.example.com -oなどのコマンドを使用してサーバ上のジョブ番号を判断します。サーバがまだその印刷ジョブを完了していない(つまり、プリンタへ完全に送信していない)ことが前提条件です。このジョブ番号を使用して、サーバ上にある印刷ジョブを削除できます。

```
cancel -h cups.example.com queue-jobnumber
```

13.7.8 異常な印刷ジョブとデータ転送エラー

印刷プロセス中にプリンタの電源を切ったり、コンピュータをシャットダウンすると、印刷ジョブはキュー内に残ります。コンピュータ(またはプリンタ)の電源を再度投入すると、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。この状況を修正するには、次の手順に従います。

1 プリンタの動作を停止するために、インクジェットプリンタの場合、すべての用紙を取り除きます。レーザープリンタの場合、用紙トレイを開けます。上位機種のプリンタでは、現在のプリントアウトをキャンセルするボタンを用意していることもあります。

2 この時点で、印刷ジョブはキューに残っている可能性があります。ジョブがキューから削除されるのは、ジョブ全体をプリンタへ送信した後に限られるからです。`lpstat -o`(または`lpstat -h cups.example.com -o`)を使用して、どのキューが現在印刷に使用されているかを確認します。`cancel` *`queue-jobnumber`*(または`cancel -h cups.example.com` *`queue-jobnumber`*)を使用して、該当の印刷ジョブを削除します。

3 印刷ジョブがすでにキューから削除されたにもかかわらず、一部のデータが依然として、プリンタへ送信され続けることもあります。CUPSバックエンドプロセスが、引き続き該当のキューを対象として動作しているかどうかをチェックし、その処理を終了します。たとえば、プリンタがパラレルポートに接続されている場合、`fuser -k /dev/lp0`コマンドを使用して、引き続きそのプリンタ(より正確に表現すると、パラレルポート)にアクセスしているすべてのプロセスを終了することができます。

4 ある程度の時間にわたって電源をオフにして、プリンタを完全にリセットします。その後、紙を元に戻し、プリンタの電源をオンにします。

13.7.9 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*内のメッセージを確認し、問題の原因を識別します。

13.7.10 詳細情報

SUSE Knowledgebase (http://www.suse.com/support/)では、さまざまな個別の問題のソリューションが紹介されています。CUPSのテキスト検索機能により関連する記事を見つけてください。

14 udevによる動的カーネルデバイス管理

実行中のシステムで、カーネルは、ほとんどどのデバイスでも追加または削除できます。デバイス状態の変更(デバイスが接続されているか、または取り外されたか)をユーザスペースに反映させる必要があります。デバイスは、接続後、検出されるとすぐに設定されなければなりません。特定のデバイスのユーザは、このデバイスの認識された状態が変更された場合は通知される必要があります。udevは、/devディレクトリのデバイスノートファイルおよびシンボリックリンクを動的に維持するために必要なインフラストラクチャを提供します。udev規則は、外部ツールをカーネルデバイスイベント処理に接続する方法を提供します。これにより、カーネルデバイス処理の一部として実行する特定のスクリプトを追加するなど、udevデバイス処理をカスタマイズしたり、デバイス処理中に評価する追加データを要求およびインポートしたりできます。

14.1 /devディレクトリ

/devディレクトリ内のデバイスノードを使用して、対応するカーネルデバイスにアクセスできます。udevにより、 /devディレクトリにカーネルの現在の状態が反映されます。カーネルデバイスは、それぞれ1つの対応するデバイスファイルを持ちます。デバイスがシステムから取り外されると、そのデバイスノードは削除されます。

/devディレクトリのコンテンツは一時的なファイルシステム内で管理され、すべてのファイルはシステムの起動時にレンダリングされます。意図的に、手動で作成または変更されたファイルはリブート時に復元されません。対応

するカーネルデバイスの状態にかかわらず、/devディレクトリ内に常駐する静的ファイルおよびディレクトリは、/lib/udev/devicesディレクトリ内に保管できます。システムの起動時、そのディレクトリのコンテンツは、/lib/udev/devices内のファイルと同じ所有者およびパーミッションの/devディレクトリ内にコピーされます。

14.2 カーネルのueventとudev

必要なデバイス情報は、sysfsファイルシステムによってエクスポートされます。カーネルが検出および初期化するすべてのデバイスについて、そのデバイス名を含んだディレクトリが作成されます。このディレクトリには、デバイス固有のプロパティのある属性ファイルが含まれます。

デバイスが追加または削除されるたびに、カーネルはueventを送信して、udevに変更を通知します。udevデーモンは、起動時に 1 回、/etc/udev/rules.d/*.rulesファイルから提示されたすべてのルールを読み込んで解析し、メモリ内に保存します。規則ファイルが変更、追加、または削除されると、このデーモンは、udevadm control reload_rulesコマンドで、すべての規則をメモリに再ロードできます。これは、/etc/init.d/boot.udev reloadの実行時にも行われます。udevのルールとそれらの構文の詳細については、14.6項 「udevルールによるカーネルデバイスイベント処理への影響」 (201 ページ)を参照してください。

着信したイベントは、すべて一連のプロバイダルールと一致します。規則によって、イベント環境キーを追加または変更したり、作成するデバイスノードに特定の名前を要求したり、ノードを指すシンボリックリンクを追加したり、またはデバイスノードの作成後に実行するプログラムを追加したりできます。ドライバのコアueventは、カーネルのネットリンクソケットから受信されます。

14.3 ドライバ、カーネルモジュールおよびデバイス

カーネルバスドライバは、デバイスを検出します。検出されたデバイスごとに、カーネルは内部デバイス構造を作成し、ドライバコアは、ueventをudevデーモンに送信します。バスデバイスは、デバイスの種類を示す特別な形式のIDを識別します。通常、これらのIDは、ベンダー、製品IDおよびサブシステム固有の値で構成されています。各バスには、これらのIDに対してMODALIASという独自のスキームを持ちます。カーネルは、デバイス情報を読み取り、この情報からMODALIAS ID文字列を作成し、イベントとともに文字列を送信します。USBマウスの場合、次のようになります。

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

各デバイスドライバは、既知の処理可能デバイスのエイリアスのリストを持ちます。このリストは、カーネルモジュールファイル自体にも含まれています。depmodプログラムは、IDリストを読み取り、現在使用可能なすべてのモジュールについて、カーネルの/lib/modulesディレクトリ内にmodules.aliasを作成します。このインフラストラクチャにより、MODALIASキーを持つイベントごとにmodprobeを呼び出すだけで簡単にモジュールをロードできます。modprobe $MODALIASが呼び出されると、そのデバイスに付けられたデバイスエイリアスとモジュールによって提示されるエイリアスとが一致します。一致したエントリが見つかると、そのモジュールがロードされます。これはすべてudevによって自動的にトリガされます。

14.4 ブートおよび初期デバイスセットアップ

udevデーモンが実行される前のブートプロセスで発生するすべてのデバイスイベントは失われます。これは、これらのイベントを処理するインフラストラクチャがルートファイルシステムに常駐し、その時点で使用できないからです。その消失の埋め合せに、カーネルは、sysfsファイルシステム内の各デバイスのデバイスディレクトリにueventファイルを生成します。そのファイルにaddと書き込むことにより、カーネルは、ブート時に消失したものと同じイベントを再送します。/sys内のすべてのueventファイルを含む単純な

ループにより、すべてのイベントが再びデバイスノードを作成し、デバイスセットアップを実行します。

たとえば、ブート時に存在するUSBマウスは、ドライバがその時点で使用できないため、初期のブートロジックでは初期化されない場合があります。デバイス検出イベントは、消失し、そのデバイスのカーネルモジュールは検出されません。接続されている可能性のあるデバイスを手動で検索する代わりに、ルートファイルシステムが使用可能になった後で、udevがカーネルからすべてのデバイスイベントを要求します。これにより、USBマウスデバイスのイベントが再び実行されます。これで、マウントされたrootファイルシステム上のカーネルモジュールが検出され、USBマウスが初期化されます。

ユーザスペースでは、実行時のデバイスのcoldplugシーケンスとデバイス検出との間に明らかな違いはありません。両方の場合も、同じ規則を使用して一致検出が行われ、同じ設定されたプログラムが実行されます。

14.5 実行中のudevデーモンの監視

udevadm monitorプログラムを使用すると、ドライバのコアイベントとudevイベントプロセスのタイミングをビジュアル化できます。

```
UEVENT[1185238505.276660] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV  [1185238505.279198] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV  [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV  [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

UEVENT行は、カーネルがnetlinkで送信したイベントを示します。UDEV行は、完了したudevイベントハンドラを示します。タイミングは、マイクロ秒で出

力されます。UEVENTおよびUDEV間の時間は、udevがこのイベントの処理に要した時間、またはudevデーモンがこのイベントと関連する実行中のイベントとの同期の実行に遅れた時間です。たとえば、パーティションイベントは、メインディスクイベントがハードウェアに問い合わせたデータに依存する可能性があるため、ハードディスクパーティションのイベントは常に、メインデバイスイベントが完了するのを待ちます。

`udevadm monitor --env`は、完全なイベント環境を表示します。

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

udevは、syslogにもメッセージを送信します。どのメッセージをsyslogに送信するかを左右するデフォルトのsyslog優先度は、udev設定ファイル `/etc/udev/udev.conf`で指定されています。実行中のデーモンのログ優先度は、`udevadm control log_priority=`*`level/number`*で変更できます。

14.6 udevルールによるカーネルデバイスイベント処理への影響

udevルールは、カーネルがイベント自体に追加する任意のプロパティや、カーネルがsysfsにエクスポートする任意の情報と一致することができます。また、この規則で、外部プログラムからの追加情報を要求することもできます。各イベントは、指定されたすべての規則と一致します。すべての規則は、`/etc/udev/rules.d`ディレクトリにあります。

規則ファイル内の各行には、少なくとも1つのキー値ペアが含まれています。これらは、一致と割り当てキーという2種類のキーです。すべての一致キーが各値と一致する場合、その規則が適用され、割り当てキーに指定された値が割り当てられます。一致する規則がある場合、デバイスノードの名前を指定、ノードを指すシンボリックリンクを追加、またはイベント処理の一部として

指定されたプログラムを実行できます。一致する規則がない場合、デフォルトのデバイスノード名を使用して、デバイスノードが作成されます。ルールの構文とデータの一致またはインポート用に提供されているキーの詳細については、udevのマニュアルページで説明されています。以下に示すルール例では、udevルール構文の基本を紹介します。これらのルール例は、すべて、/etc/udev/rules.d/50-udev-default.rulesの下にあるudevデフォルトルールセットに含まれています。

*例 **14.1**　udevルールの例*

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

consoleルールは、3つのキーで構成されています。その内訳は、一致キーが1つ(KERNEL)、割り当てキーが2つ(MODE、OPTIONS)です。KERNEL一致ルールはconsoleタイプのアイテムをデバイスリストから検索します。正確な一致だけが有効であり、このルールの実行をトリガします。MODEキーは、特別パーミッションをデバイスノードに割り当てます。この例では、読み取り/書き込みパーミッションをこのデバイスの所有者にのみ割り当てます。OPTIONSキーは、この規則をこのタイプのデバイスに適用される最後の規則にします。以降の規則は、この特定デバイスタイプとマッチしても、どのような結果も生じません。

serial devicesルールは、50-udev-default.rulesには存在しなくなりましたが、依然その知識は重要です。この規則は、2つの一致キー(KERNEL、ATTRS)および1つの割り当てキー(SYMLINK)で構成されます。KERNELキーは、ttyUSBタイプのすべてのデバイスを検索します。このキーで*ワイルドカードを使用すると、これらのデバイスのいくつかとマッチします。2つ目の一致キーATTRSは、ttyUSBデバイスのsysfsにあるproduct属性ファイルに一定の文字列が含まれているかどうかをチェックします。割り当てキー(SYMLINK)は、/dev/pilotの下に、このデバイスへのシンボリックリンクを追加します。このキーで演算子(+=)を使用すると、前/後の規則が他のシンボリックリンクを追加した場合でも、udevはこの操作を追加実行します。こ

の規則は、2つの一致キーを含むので、両方の条件が満たされる場合のみ適用されます。

printerルールは、USBプリンタを対象とし、2つの一致キー(SUBSYSTEM、KERNEL)を含みます。規則全体を適用するには、これらのキーを両方とも適用する必要があります。3つの割り当てキーは、このデバイスタイプの名前付け(NAME)、シンボリックデバイスリンクの作成、(SYMLINK)、およびこのデバイスタイプのグループメンバーシップ(GROUP)を処理します。KERNELキーで*ワイルドカードを使用すると、いくつかのlpプリンタデバイスとマッチします。NAMEおよびSYMLINKの両キーで置き換えを使用すると、これらの文字列を内部デバイス名で拡張できます。たとえば、最初のlp USBプリンタへのシンボリックリンクは/dev/usblp0となります。

kernel firmware loaderルールでは、ランタイム時の外部ヘルパースクリプトで、udevが追加ファームウェアをロードします。SUBSYSTEM一致キーは、firmwareサブシステムを検索します。ACTIONキーは、firmwareサブシステムに属するデバイスが追加されているかどうかをチェックします。RUN+=キーは、firmware.shスクリプトの実行をトリガして、ファームウェアを見つけます。

すべての規則に共通する一般的特性は次のとおりです。

- 各規則は、カンマで区切られた1つ以上のキー値ペアで構成されます。
- キーの動作は、演算子で決定されます。udevルールは、いくつかの異なる演算子をサポートします。
- 指定する各値は、引用符で囲む必要があります。
- 規則ファイルの各行が1つの規則に相当します。規則が1行を超える場合は、shell構文のように、\を使用して異なる行を結合してください。
- udevルールは、shell型のパターンをサポートします。このパターンは、*、?、および[]の各パターンとマッチします。
- udevルールは、置換をサポートします。

14.6.1 udevルールでの演算子の使用

キーを作成する場合は、作成するキーのタイプによって、いくつかの異なる演算子から選択できます。一致キーは、通常、検索値とマッチするか、明示的にミスマッチする値を見つけるためにだけ使用されます。一致キーは、次の演算子のいずれかを含みます。

==
: 等価の比較。キーに検索パターンが含まれている場合は、そのパターンと一致するすべての結果が有効です。

!=
: 非等価の比較。キーに検索パターンが含まれている場合は、そのパターンと一致するすべての結果が有効です。

割り当てキーでは、次のどの演算子でも使用できます。

=
: 値をキーに割り当てます。すでに値のリストで構成されているキーはリセットされ、指定した1つの値だけが割り当てられます。

+=
: エントリのリストを含むキーに値を追加します。

:=
: 最終値を割り当てます。以降の規則による変更は許可されません。

14.6.2 udevルールでの置換の使用

udevルールは、プレースホルダと置換の使用をサポートします。それらは、他のスクリプトでの使用と同様な方法で使用します。udevルールでは、次の置換を使用できます。

%r、$root
: デフォルトのデバイスディレクトリ/dev。

%p、$devpath
: DEVPATHの値。

%k、$kernel
KERNELの値または内部デバイス名。

%n、$number
デバイス番号。

%N、$tempnode
デバイスファイルの一時名。

%M、$major
デバイスのメジャー番号。

%m、$minor
デバイスのマイナー番号。

%s{*attribute*}、$attr{*attribute*}
sysfs属性の値(*attribute*で指定)。

%E{*variable*}、$attr{*variable*}
環境変数の値(*variable*で指定)。

%c、$result
PROGRAMの出力。

%%
%文字。

$$
$文字。

14.6.3 udev一致キーの使用

一致キーは、udevルールの適用前に満たす必要のある条件を記述します。次の一致キーが使用可能です。

ACTION
イベント動作の名前。たとえば、addまたはremove(デバイスの追加または削除の場合)。

DEVPATH
イベントデバイスのデバイスパス。たとえば、DEVPATH=/bus/pci/drivers/ipw3945(ipw3945ドライバに関連するすべてのイベントを検索する場合)。

KERNEL
イベントデバイスの内部(カーネル)名。

SUBSYSTEM
イベントデバイスのサブシステム。たとえば、SUBSYSTEM=usb(USBデバイスに関連するすべてのイベント用)。

ATTR{*filename*}
イベントデバイスのsysfs属性。vendor属性ファイル名に含まれた文字列とマッチするには、たとえば、ATTR{vendor}=="On[sS]tream"を使用できます。

KERNELS
udevにデバイスパスを上方に検索させ、一致するデバイス名を見つけます。

SUBSYSTEMS
udevにデバイスパスを上方に検索させ、一致するデバイスサブシステム名を見つけます。

DRIVERS
udevにデバイスパスを上方に検索させ、一致するデバイスドライバ名を見つけます。

ATTRS{*filename*}
udevにデバイスパスを上方に検索させ、一致するsysfs属性値を持つデバイスを見つけます。

ENV{*key*}
環境変数の値。たとえば、ENV{ID_BUS}="ieee1394でFireWire bus IDに関連するすべてのイベントを検索します。

PROGRAM
udevに外部プログラムを実行させます。成功の場合は、プログラムが終了コードとしてゼロを返します。stdoutに印刷されるプログラムの出力は、RESULTキーで使用できます。

RESULT
最後のPROGRAM呼び出しの出力文字列とマッチします。このキーは、PROGRAMキーと同じ規則に含めるか、それ以降のキーに含めてください。

14.6.4 udev割り当てキーの使用

上記で説明した一致キーに対し、割り当てキーでは満たすべき条件を記述しません。値、名前、アクションをudevが保守するデバイスノードに割り当てます。

NAME
作成するデバイスノードの名前。いったん規則でノード名が設定されると、このノードのNAMEキーを持つ他の規則はすべて無視されます。

SYMLINK
作成するノードに関連するシンボリックリンクの名前。複数の一致ルールで、デバイスノードとともに作成するシンボリックリンクを追加できます。1つのルール内で、スペース文字でシンボリックリンク名を区切ることで、1つのノードに複数のシンボリックリンクを指定することもできます。

OWNER、GROUP、MODE
新しいデバイスノードのパーミッションここで指定する値は、すでにコンパイルされている値を上書きします。

ATTR{*key*}
イベントデバイスのsysfs属性に書き込む値を指定します。==演算子を使用すると、このキーは、sysfs属性の値とのマッチングにも使用されます。

ENV{*key*}
環境への変数のエクスポートをudevに指示します。==演算子を指定すると、このキーは、環境変数とのマッチングにも使用されます。

RUN
このデバイスに対して実行されるプログラムのリストにプログラムを追加するように、udevに指示します。このデバイスのイベントをブロックしないようにするため、これは非常に短いタスクに限定してください。

LABEL
GOTOのジャンプ先にするラベルを追加します。

GOTO
いくつかのルールをスキップし、GOTOキーで参照されるラベルを含むルールから続行するように、udevに指示します。

IMPORT{*type*}
変数をイベント環境(外部プログラムの出力など)にロードします。udevは、いくつかの異なるタイプの変数をインポートします。タイプが指定されていない場合、udevは、ファイルパーミションの実行可能ビットに基づいてタイプを決定しようとします。

- program – 外部プログラムを実行し、その出力をインポートします。
- file – テキストファイルをインポートします。
- parent – 親デバイスから保存されたキーをインポートします。

WAIT_FOR_SYSFS
一定のデバイスに指定されたsysfsファイルが作成されるまで、udevを待機させます。たとえば、WAIT_FOR_SYSFS="ioerr_cnt"では、ioerr_cntファイルが作成されるまで、udevを待機させます。

オプション
OPTIONキーには、次の可能な値があります。

- last_rule – 以降のすべての規則を無視します。
- ignore_device – このイベントを完全に無視します。
- ignore_remove – このデバイスの以降のすべての削除イベントを無視します。

- `all_partitions` – ブロックデバイス上のすべての使用可能なパーティションにデバイスノードを作成します。

14.7 永続的なデバイス名の使用

動的デバイスディレクトリおよびudevルールインフラストラクチャによって、認識順序やデバイスの接続手段に関わらず、すべてのディスクデバイスに安定した名前を指定することができます。カーネルが作成する適切なブロックデバイスはすべて、特定のバス、ドライブタイプまたはファイルシステムに関する特別な知識を備えたツールによって診断されます。動的カーネルによって指定されるデバイスノード名とともに、udevは、デバイスをポイントする永続的なシンボリックリンクのクラスを維持します。

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

14.8 udevで使用するファイル

/sys/*
Linuxカーネルによって提供される仮想ファイルシステム。現在知られているデバイスをすべてエクスポートします。この情報は、udevが使用して/dev内にデバイスノードを作成します。

/dev/*
動的に作成されるデバイスノードと静的コンテンツ。ブート時に/lib/udev/devices/*からコピーされます。

以下のファイルおよびディレクトリには、udevインフラストラクチャの重要な要素が含まれています。

/etc/udev/udev.conf
メインudev設定ファイル

/etc/udev/rules.d/*
規則と一致するudevイベント.

/lib/udev/devices/*
静的/devコンテンツ

/lib/udev/*
udevルールから呼び出されるヘルパープログラム

14.9 詳細情報

udevインフラストラクチャの詳細については、以下のマニュアルページを参照してください。

udev
udev、キー、ルールなどの重要な設定課題に関する一般情報

udevadm
udevadmは、udevのランタイム動作を制御し、カーネルイベントを要求し、イベントキューを管理し、簡単なデバッグメカニズムを提供します。

udevd
    udevイベント管理デーモンに関する情報

15 X Windowシステム

X Window System (X11)は、UNIX系のグラフィカルユーザインタフェースで、事実上の標準となっています。Xはネットワークベースであり、あるホスト上で起動されたアプリケーションを、任意のネットワーク(LANやインターネット)を介して接続されている他のホスト上で表示できるようにします。この章ではX Window System環境のセットアップと最適化について説明し、SUSE® Linux Enterprise Serverでのフォント使用の背景情報を提供します。

ヒント: IBM System z:グラフィカルユーザインタフェースの設定

IBM System zには、X.Orgがサポートする入出力デバイスはありません。そのため、このセクションで説明している環境設定手順は適用されません。IBM zSeriesの関連情報は、第4章 *IBM System z*へのインストール (↑*導入ガイド*)を参照してください。

15.1 X Window システムの手動設定

デフォルトでは、X Windowシステムは項「グラフィックカードとモニタの設定」(第8章 *YaSTによるハードウェアコンポーネントの設定*,↑*導入ガイド*)に説明されているSaX2インタフェースを使って設定されます。代わりに設定ファイルを編集して、手動設定することもできます。

警告: X環境設定ファイルに不適切な設定を行うとハードウェアが損傷する可能性があります

X Window Systemの設定は慎重に行う必要があります。設定が完了するまでは、X Window Systemを起動しないでください。システムが正しく設定されていないと、ハードウェアが復元不能な損傷を受ける可能性があります(特に固定周波数モニタの場合)。本書およびSUSE Linux Enterprise Serverの作成者は、このような原因による損傷や損害に対していかなる責任も負いません。この情報は慎重に調査されたものですが、ここで説明する方法がすべて正しく、ハードウェアが損傷を受けないという保証はありません。

コマンド`sax2`で`/etc/X11/xorg.conf`ファイルが作成されます。これはX Window Systemの基本設定ファイルです。このファイルには、グラフィックカード、マウス、およびモニタに関する設定がすべて含まれています。

重要: X -configureの使用

SUSE Linux Enterprise ServerのSaX2で失敗した場合は、`X -configure`を使ってXセットアップの設定を行ってください。セットアップにバイナリのみの専有ドライバが使用される場合、`X -configure`は動作しません。

ここでは、設定ファイル`/etc/X11/xorg.conf`の構造について説明します。xorg.confは複数のセクションで構成され、各セクションは設定の特定の側面を取り扱います。各セクションは、キーワード`Section <designation>`で始まってキーワード`EndSection`で終わります。すべてのセクションで、以下の表記規則を使用します。

```
Section "designation"
  entry 1
  entry 2
  entry n
EndSection
```

使用可能なセクションのタイプのリストは表15.1「/etc/X11/xorg.confのセクション」 (215 ページ)にあります。

表 **15.1** */etc/X11/xorg.conf*のセクション

タイプ	意味
`Files`	フォントとRGBカラーテーブルで使用するパス。
`ServerFlags`	サーバ動作の汎用スイッチ。
`Module`	サーバがロードする必要があるモジュールリスト
`InputDevice`	キーボードや特殊入力デバイス(タッチパッド、ジョイスティックなど)といった入力デバイスを設定します。このセクションで重要なパラメータは`Driver`と、`Protocol`および`Device`を定義するオプションです。通常、コンピュータに接続した1つのデバイスごとに1つの`InputDevice`があります。
`Monitor`	使用するモニタ。このセクションの重要な要素は、後で`Screen`の定義で参照する`ID`、リフレッシュレートの`VertRefresh`、および同期周波数の制限(`HorizSync`および`VertRefresh`)です。設定値はMHz、kHz、およびHz単位です。通常、サーバはモニタ仕様に対応しないmodelineを拒否します。このため、意図せずに高すぎる周波数がモニタに送信されるのを防止できます。
`Modes`	特定の画面解像度のmodelineパラメータ。これらのパラメータは、ユーザ指定の値に基づいてSaX2で

タイプ	意味
	計算でき、通常は変更不要です。固定周波数モニタに接続する場合などは、この時点で手動で介入します。個々の数値の意味の詳細については、HOWTOファイル/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTOを参照してください(howtoenhパッケージ内)。VESAモードを手動で計算する場合は、ツールcvtを使用できます。たとえば、1680x1050@60Hzモニタのmodelineを計算する場合は、コマンドcvt 1680 1050 60を使用します。
Device	特定のグラフィックカード。グラフィックカードは記述名で参照されます。このセクションで利用可能なオプションは、使用するドライバに大きく依存します。たとえば、i810ドライバを使用する場合では、マニュアルページman 4 i810に使用可能なオプションの詳細が記載されています。
Screen	MonitorとDeviceを組み合わせて、X.Orgに必要な設定を形成します。Displayサブセクションでは、仮想画面のサイズ(Virtual)、ViewPort、およびこの画面で使用するModesを指定します。 一部のドライバでは、いずれかの場所にあるDisplayセクションに

タイプ	意味
	すべての使用設定が存在しなければならないことに注意してください。たとえば、ラップトップを使用している場合で、内部LCDより大きい外部モニタを使用するときは、内部LCDによりサポートされる以上の分解能をModes行の最後に追加することが必要になる場合があります。
ServerLayout	シングルまたはマルチヘッド設定のレイアウト。このセクションにより、入力デバイスInputDeviceと表示デバイスScreenがバインドされます。
DRI	DRI(Direct Rendering Infrastructure)の情報を提供します。

ここでは、Monitor、Device、およびScreenについて詳しく説明します。他のセクションの詳細については、X.Orgおよびxorg.confのマニュアルページを参照してください。

xorg.confには、複数の異なるMonitorおよびDeviceセクションを記述できます。複数のScreenセクションを記述することも可能です。ServerLayoutセクションでは、このセクションのうち使用するものを判定します。

15.1.1 Screenセクション

Screenセクションでは、MonitorセクションとDeviceセクションを組み合わせて、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15.1「ファイル/etc/X11/xorg.confのScreenセクション」 (218 ページ)のようになります。

例 15.1　ファイル/etc/X11/xorg.confのScreenセクション

```
Section "Screen"❶
  DefaultDepth  16❷
  SubSection "Display"❸
    Depth       16❹
    Modes       "1152x864" "1024x768" "800x600"❺
    Virtual     1152x864❻
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"❼
  Monitor       "Monitor[0]"
EndSection
```

❶ Sectionはセクションタイプを判定し、この場合はScreenになります。

❷ DefaultDepthは、色深度が明示的に指定されていない場合にデフォルトで使用する色深度を示します。

❸ 各色深度に対して、異なるDisplayサブセクションが指定されます。

❹ Depthは、このセットのDisplay設定とともに使用する色深度を示します。8、15、16、24、および32を指定できますが、すべてのXサーバモジュールまたは解像度がこれらの値をすべてサポートしている訳ではありません。

❺ Modesセクションは、可能な画面解像度のリストから成り立っています。Xサーバは、このリストを左から右に検査します。解像度ごとに、XサーバはModesセクション内で適切なModelineを検索します。Modelineは、モニタとグラフィックカード両方の機能に応じて異なります。Monitor設定により、Modelineが決まります。

最初に検出される解像度はDefault modeです。Ctrl + Alt + +(数字パッド上のキー)を使用すると、リスト内で右隣の解像度に切り替えることができます。以前の値に切り替えるには、Ctrl+Alt+–(数字パッド上のキー)を使用します。これにより、Xの実行中に解像度を変更できます。

❻ Depth 16が指定されているDisplayサブセクションの最終行は、仮想画面のサイズを指します。仮想画面の最大許容サイズは、モニタの最大解像度ではなく、グラフィックカードにインストールされているメモリの容量と必要なカラー設定に応じて異なります。この行を省略すると、仮想解像度は物理解像度と同じになります。最近のグラフィックカードはビデオメモリ容量が大きくなってきているため、きわめて大型の仮想デスクトップを作成できます。ただし、ビデオメモリのほとんどが仮想デスクトップを占めると、3D機能を使用できなくなる場合があります。たとえば、カードのビデオRAMが16MBであれば、仮想画面には8ビットカラー深度で最大4096x4096ピクセルのサイズを設定できます。ただし、特にアクセラレータカードの場合は、仮想画面にメモリすべてを使用しないことをお勧めします。この種のカードのメモリは、複数のフォントやグラフィックキャッシュにも使用されるからです。

❼ Identifier行(ここではScreen[0])では、このセクションに以降のServerLayoutセクションで固有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。

15.1.2 Deviceセクション

Deviceセクションでは、特定のグラフィックカードを記述します。名前が異なっていれば、キーワードIdentifierを使用してxorg.conf内で必要な数だけデバイスエントリを指定できます。複数のグラフィックカードをインストールしている場合、セクションには順番に番号が付けられます。最初のセクションはDevice[0]、2番目のセクションはDevice[1]となります。次のファイルは、Matrox Millennium PCIグラフィックカードが搭載されているコンピュータのDeviceセクションから抜粋したものです(SaX2が設定)。

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"❶
  Driver        "mga"❷
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

❶ BusIDは、グラフィックカードがインストールされているPCIスロットまたはAGPスロットの定義です。これは、lspciコマンドで表示されるIDと一致します。Xサーバは10進形式による詳細を必要としますが、lspciではこれらが16進形式で表示されます。BusIDの値は、SaX2が自動検出します。

❷ Driverの値はSaX2が自動的に検出し、グラフィックカードで使用するドライバを指定します。カードがMatrox Millenniumである場合は、ドライバモジュールはmgaと呼ばれます。Xサーバは、driversサブディレクトリのFilesセクションで定義されているModulePathを検索します。標準インストールでは、これは/usr/lib/xorg/modules/driversディレクトリ、または64ビットオペレーティングシステムディレクトリでは/usr/lib64/xorg/modules/driversディレクトリです。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/share/doc/package*package_name*内のドライバモジュールの記述ファイル内にあります。通常、有効なオプションについてはマニュアルページ(man xorg.conf、man 4 <*ドライバモジュール*>、およびman 4 *chips*)でも確認できます。

グラフィックカードに複数のビデオコネクタがある場合、この1枚のカードの異なるデバイスを単一ビューとして設定できます。SaX2を使用してグラフィックインタフェースをこのように設定します。

15.1.3 MonitorセクションとModesセクション

Deviceセクションと同様に、MonitorセクションとModesセクションでもモニタを1つずつ記述します。設定ファイル/etc/X11/xorg.confでは、Monitorセクションを必要な数だけ指定できます。Monitorセクションはそれぞれ、UseModes行があるModesセクションを参照します。Monitorセク

ションにModesセクションがない場合、Xサーバは該当する値を一般的な同期の値から計算します。サーバレイアウトセクションでは、どのMonitorセクションが関係するかを指定します。

熟練者以外は、モニタ定義を設定しないでください。modelineは、Monitorセクションで重要な役割を果たします。modelineでは、関連解像度の水平と垂直のタイミングを設定します。モニタ特性、特に許容周波数は、Monitorセクションに格納されます。標準VESAモードは、ユーティリティcvtにより生成できます。詳細については、マニュアルページcvtman cvtを参照してください。

警告

モニタおよびグラフィックカード機能の詳細な知識がない場合は、modelineを変更しないでください。モニタに重大な損傷が生じることがあります。

独自のモニタ記述を作成する場合は、/usr/share/X11/doc内のドキュメントを熟読する必要があります。PDFおよびHTMLページを参照するために、パッケージxorg-x11-docをインストールします。

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大半の組み合わせに機能します。

15.2 フォントのインストールと設定

SUSE Linux Enterprise Server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(15.2.1項「X11コアフォント」 (223ページ)を参照)。フォントの使用を有効にするには、インストールディレクトリが/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(15.2.2項「Xft」 (224ページ)を参照)。または、このファイルを/etc/fonts/suse-font-dirs.confに入れなければなりません。

以下は、/etc/fonts/fonts.confから抜粋したものです。このファイルは、大半の設定に適合する標準設定ファイルです。また、インクルード済みのディレクトリ/etc/fonts/conf.dを定義します。このディレクトリには、すべてのファイルまたは2桁の数字で始まるシンボリックリンクがfontconfigによりロードされます。この機能の詳細な説明は、/etc/fonts/conf.d/READMEを参照してください。

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/.fonts</dir>
```

/etc/fonts/suse-font-dirs.confが自動的に生成されて、LibreOffice、Java、またはAdobe Readerなどのアプリケーション(ほとんどの場合サードパーティ製)に付属のフォントを取り込みます。エントリの例を次に示します。

```
<dir>/usr/lib/Adobe/Reader9/Resource/Font</dir>
<dir>/usr/lib/Adobe/Reader9/Resource/Font/PFM</dir>
```

システム全体に追加フォントをインストールするには、フォントファイルを/usr/share/fonts/truetypeなどの適切なディレクトリに手動コピーしてください(rootとして)。また、この作業は、KDEコントロールセンターでKDEフォントインストーラを使用して行うこともできます。結果は同じです。

フォントを実際にコピーする代わりに、シンボリックリンクを作成することもできます。たとえば、マウントされているWindowsパーティション上にライセンスを取得しているフォントがあり、それらのフォントを使用したい場合は、シンボリックリンクを作成します。次に、SuSEconfig--module fontsコマンドを実行します。

SuSEconfig--module fontsコマンドは、フォントを設定するスクリプト、/usr/sbin/fonts-configを実行します。このスクリプトの詳細については、マニュアルページ(man fonts-config)を参照してください。

手順は、ビットマップフォント、TrueTypeフォントとOpenTypeフォント、およびType1 (PostScript)フォントの場合と同様です。これらのタイプのフォントはすべて、任意のディレクトリにインストールできます。

X.Orgには、従来の［*X11コアフォントシステム*］と、新たに設計された［*Xftおよびfontconfig*］システムの2種類のまったく異なるフォントシステムが含まれています。以降のセクションでは、これらの2つのシステムについて簡単に説明します。

15.2.1 X11コアフォント

今日、X11コアフォントシステムは、ビットマップフォントだけでなく、Type1フォント、TrueTypeとOpenTypeフォントなどのスケーラブルフォントもサポートしています。スケーラブルフォントは、アンチエイリアスとサブピクセルレンダリングなしでサポートされており、多数の言語用のグリフを持つ大きいスケーラブルフォントのロードには時間がかかります。Unicodeフォントもサポートされていますが、使用すると時間がかかり、より多くのメモリが必要になります。

X11コアフォントシステムには、その他にも固有の弱点がいくつかあります。時代遅れになっており、これ以上拡張することはできません。下位互換性のために保持されていますが、可能なときはいつでも、新しいXftおよびfontconfigシステムを使用してください。

Xサーバは、操作のためにどのようなフォントが使用可能で、そのフォントがシステム内のどこにあるかを認識する必要があります。この情報は、有効なすべてのシステムフォントディレクトリへのパスを含む`FontPath`変数で処理されます。これらの各ディレクトリでは、ファイル`fonts.dir`にそのディレクトリ内で使用可能なフォントのリストがあります。`FontPath`は、起動時にXサーバにより生成されます。設定ファイル`/etc/X11/xorg.conf`の各`FontPath`エントリ内で、有効なファイル`fonts.dir`が検索されます。これらのエントリは、`Files`セクションにあります。実際の`FontPath`を表示するには、`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。不要なパスを削除するには、`xset-fp <path>`を使用します。

Xサーバがすでにアクティブである場合、マウントされたディレクトリに新たにインストールされたフォントは、コマンド`xsetfp rehash`で使用可能にできます。このコマンドは、`SuSEconfig--module fonts`によって実行されます。コマンド`xset`が実行中のXサーバにアクセスする必要がある場合、これは、`SuSEconfig--module fonts`が実行中のXサーバにアクセスできるシェルから起動されている場合にのみ可能です。これを実行する簡単な方

法は、suとrootパスワードを入力して、root パーミッションを取得することです。suによってXサーバを起動したユーザのアクセス許可がrootシェルに転送されます。フォントが正しくインストールされ、X11コアフォントシステムを介して使用可能かどうか検査するには、コマンドxlsfontsを使用して、すべての使用可能なフォントのリストを表示します。

デフォルトでは、SUSE Linux Enterprise ServerはUTF-8ロケールを使用します。そのため、Unicodeフォントを使用するようにします(xlsfontsの出力中でiso10646-1で終了するフォント名)。使用可能なすべてのUnicodeフォントは、xlsfonts| grep iso10646-1コマンドでリストを表示できます。SUSE Linux Enterprise Server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)。

15.2.2 Xft

最初から、Xftのプログラムは、アンチエイリアスを含むスケーラブルフォントが適切にサポートされるようにしています。Xftが使用された場合、フォントは、X11コアフォントシステムにおけるXサーバではなく、そのフォントを使用するアプリケーションによってレンダリングされます。このようにすると、それぞれのアプリケーションは実際のフォントファイルにアクセスでき、グリフのレンダリング方法を完全に制御できます。これが、多数の言語においてテキストを正しく表示するための基本となっています。フォントファイルに直接アクセスできることは、印刷のためにフォントを組み込んで、画面出力と同じ印刷出力を得るのに役立ちます。

SUSE Linux Enterprise Serverでは、2種類のデスクトップ環境(KDEとGNOME、Mozilla)、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によって制御されます。特別設定は、/etc/fonts/local.confおよびユーザ固有の設定ファイル~/.fonts.confに追加する必要があります。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>
```

この場合、すべてのフォントのアンチエイリアスが無効になります。また、

```
<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(:scalable=true)のうち、どのフォントがHebrew (:lang=he)に必要なすべてのグリフ、それらのフォント名(family)、それらのスタイル(style)、それらの幅(weight)、およびフォントを含むファイルの名前を含んでいるか調べるには、次のコマンドを入力します。

```
fc-list ":lang=he:scalable=true" family style weight
```

上記のコマンドの出力は、以下のようになります。

```
Lucida Sans:style=Demibold:weight=200
DejaVu Sans:style=Bold Oblique:weight=200
Lucida Sans Typewriter:style=Bold:weight=200
DejaVu Sans:style=Oblique:weight=80
Lucida Sans Typewriter:style=Regular:weight=80
DejaVu Sans:style=Book:weight=80
DejaVu Sans:style=Bold:weight=200
Lucida Sans:style=Regular:weight=80
```

fc-listで調べることができる重要なパラメータ：

*表 **15.2** 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。たとえば、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。

15.3 詳細情報

X11に関する詳細情報を入手するには、xorg-x11-docおよびhowtoenhパッケージをインストールしてください。X11開発の詳細情報は、プロジェクトのホームページhttp://www.x.orgで参照できます。

パッケージxorg-x11-driver-videoで配布されるドライバの大半については、マニュアルページに詳細が記載されてます。たとえば、nvドライバを使用する場合は、man 4 nvでドライバの詳細を参照できます。

サードパーティーのドライバ情報は、/usr/share/doc/packages/<package_name>に記載されています。たとえば、x11-video-nvidiaG01の場合、パッケージのインストール後は、/usr/share/doc/packages/x11-video-nvidiaG01でマニュアルを参照できます。

FUSEによるファイルシステムへのアクセス

16

FUSEは、*file system in userspace*の頭字語です。これは、特権のないユーザとしてファイルシステムを設定およびマウントできることを意味します。通常、このタスクを行うためには、`root`にいる必要があります。FUSE自体は、カーネルモジュールです。FUSEは、プラグインと組み合わせることで、ほとんどすべてのファイルシステムにアクセスするように拡張できます(リモートSSH接続、ISOイメージなど)。

16.1 FUSEの設定

FUSEを使用するには、まず、`fuse`パッケージをインストールする必要があります。使用するファイルシステムによって、別々のパッケージとして使用できるプラグインを追加する必要があります。FUSEプラグインはSUSE Linux Enterpriseに付属していません。

一般的には、FUSEは設定の必要がなく、そのまま使用します。ただし、すべてのマウントポイントを結合するディレクトリの作成をお勧めします。たとえば、ディレクトリ`~/mounts`を作成し、そこに、各種のファイルシステムのサブディレクトリを挿入します。

16.2 利用可能なFUSEプラグイン

FUSEはプラグインに依存します。次のテーブルに、よく利用されるプラグインを一覧します。FUSEプラグインはSUSE Linux Enterpriseに付属していません。

表 16.1　利用可能なFUSEプラグイン

`fuseiso`	ISO9660ファイルシステムを含むCD-ROMをマウントします。
`ntfs-3g`	NTFSボリュームをマウントします（読み込み/書き込みサポート付き)。
`sshfs`	SSHファイル転送プロトコルに基づくファイルシステムクライアント。
`wdfs`	WebDAVファイルシステムをマウントします。

16.3 詳細情報

詳細については、FUSEのホームページ`http://fuse.sourceforge.net`を参照してください。

パート III. モバイルコンピュータ

Linuxでのモバイルコンピューティング

17

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、そしてこれらを使ったデータ交換ではないでしょうか。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は、ラップトップやデスクトップシステムに接続できます。多くのソフトウェアコンポーネントで、モバイルコンピューティングを想定しており、一部のアプリケーションは、モバイル使用に合わせて特別に作成されています。

17.1 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、空間要件、電力消費などの基準を考慮する必要があるためです。モバイルハードウェアメーカーは、ラップトップハードウェアを拡張するために使用可能なPCMCIA(Personal Computer Memory Card International Association)、Mini PCI、Mini PCIeなどの標準インタフェースを開発してきました。この標準ではメモリカード、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をカバーします。

ヒント: SUSE Linux Enterprise ServerおよびタブレットPC

SUSE Linux Enterprise Serverはまた、タブレットPCをサポートします。タブレットPCには、タッチパッド/デジタイザが付属しており、マウスとキーボードを使用するのではなく、デジタルペンやさらに指による操作で画面上で直接データを編集できます。タブレットPCは、他のシステムとまったく同じようにインストールおよび設定されます。タブレットPCのインストー

ルおよび設定について詳しくは、第20章 *タブレットPCの使用* (273 ページ)を参照してください。

17.1.1 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、電源に接続しなくてもシステムを快適に使用できるようにしています。電源の管理に関するこうした貢献は少なくともオペレーティングシステムの貢献度と同じくらい重要です。SUSE® Linux Enterprise Serverはラップトップの電源消費量に影響する様々なメソッドをサポートすることで、バッテリー使用時の操作に数々の効果をあげています。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。

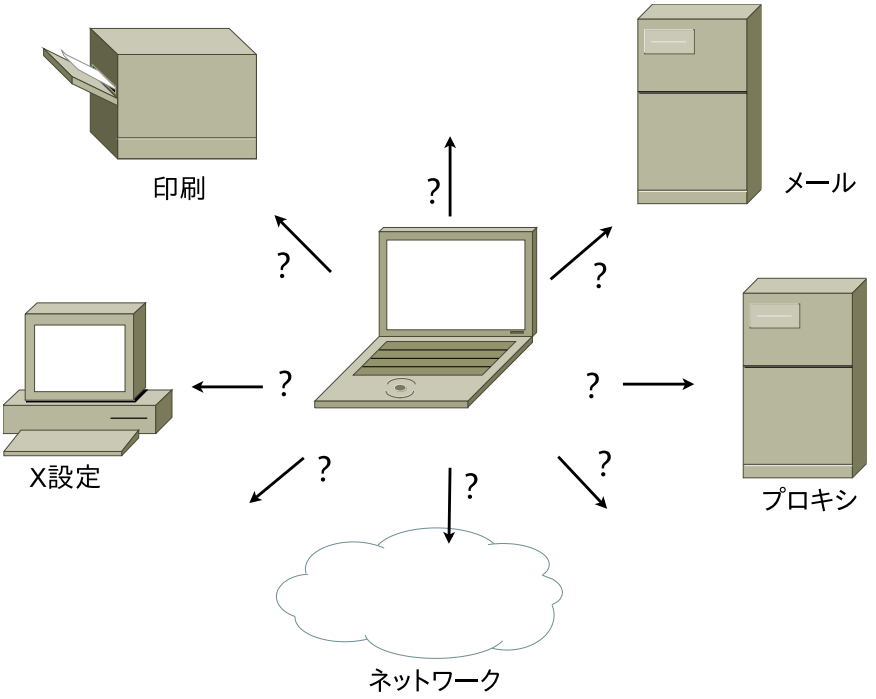
- CPUの速度を落とす。
- 休止中にディスプレイの照明を切る。
- ディスプレイの明るさを手動で調節する。
- ホットプラグ対応の使用していないアクセサリを切断する(USB CD-ROM、外付けマウス、使用していないPCMCIAカード、WLANなど)。
- アイドル中にはハードウェアディスクをスピンダウンする。

SUSE Linux Enterprise Serverでの電源管理の詳細な背景情報は、第19章 *電源管理* (263 ページ)に示されています。

17.1.2 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。多くのサービスは環境に依存するので、環境を構成するクライアントの再設定が必要です。SUSE Linux Enterprise Server はこうしたタスクをユーザに代わって実行します。

図 17.1 既存環境でのモバイルコンピュータの統合



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
: IPアドレスの割り当て、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。

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(グラフィック環境)
: ご使用のラップトップがプロジェクタまたは外付けモニタに一時的に接続されている場合、別のディスプレイ設定が使用可能になっている必要があります。

SUSE Linux Enterprise Serverではラップトップを既存の操作環境に統合させる複数の方法を提供しています。

NetworkManager
: NetworkManagerは、ラップトップでのモバイルネットワーキング用に特別に作成されています。NetworkManagerは、ネットワーク環境間、またはモバイルブロードバンド(GPRS、EDGE、または3G)、ワイヤレスLAN、Ethernetなどのさまざまなタイプのネットワーク間を容易に、自動的に切り替える方法を提供します。NetworkManagerは、ワイヤレスLANでのWEPおよびWPA-PSKの暗号化をサポートします。また、(smpppdにより)ダイアルアップ接続をサポートします。両方のデスクトップ環境(GNOMEおよびKDE)には、NetworkManagerのフロントエンドが含まれています。デスクトップアプレットの詳細については、26.4項 「KNetworkManagerの使用」 (424 ページ)および26.5項 「GNOME NetworkManagerアプレットの使用」 (429 ページ)を参照してください。

表 *17.1* *NetworkManagerの使用*

マイコンピュータ...	NetworkManagerの使用
ラップトップである	対応
別のネットワークに接続される場合がある	対応
ネットワークサービスを提供する(DNSまたはDHCP)	非対応
スタティックIPアドレスのみを使用する	非対応

NetworkManagerがネットワーク設定を扱うのが適切でない場合、YaSTツールを使用してネットワークを設定します。

ヒント: DNS設定と、各種ネットワーク接続

ラップトップを持って移動し、ネットワーク接続の種類を頻繁に変更する場合、すべてのDNSアドレスがDHCPで正常に割り当てられている場合はNetworkManagerは正常に機能します。一部の接続で静的DNSアドレスを使用する場合は、そのアドレスを`/etc/sysconfig/network/config`内の`NETCONFIG_DNS_STATIC_SERVERS`オプションに追加します。

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も使用でき、適切なインストールソースの検索作業が最小化されます。SLPの詳細については、第22章 *ネットワーク上のSLPサービス* (361 ページ)を参照してください。

17.1.3 ソフトウェアオプション

モバイル用途には、専用ソフトウェアにより対応される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、インターネットなど、さまざまな特別タスク領域が存在します。次のセクションでは、SUSE Linux Enterprise Server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。

17.1.3.1 システムモニタリング

SUSE Linux Enterprise Server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。

電源管理

［*電源管理*］は、KDEデスクトップの省エネ関係の動作を調整できるアプリケーションです。このアプリケーションには、通常、［バッテリモニタ］トレイアイコンでアクセスします。このアイコンは、現在の電源タイプに応じて変化します。設定ダイアログを開くには、［*Kickoff*アプリケーションランチャ］を使用する方法もあります:［アプリケーション］>［デスクトップの設定］>［*詳細*］>［*電源管理*］

［バッテリモニタ］トレイアイコンをクリックして、動作を設定するオプションにアクセスします。表示された5つの電源プロファイルから、自分のニーズに最も適合する1つを選択できます。たとえば、［プレゼンテーション］スキーマは一般にスクリーンセーバーと電源管理を無効にするため、プレゼンテーションはシステムイベントによって中断されません。［*詳細...*］をクリックして、さらに複雑な設定の画面を表示します。ここで、個々のプロファイルを編集し、ラップトップのカバーが閉じられている場合やバッテリ残量が低い場合の処置など、高度な電源管理に関するオプションや通知を設定できます。

システムモニタ

［システムモニタ］(［*K*システムガード］とも呼ぶ)は、測定可能なシステムパラメータを1つのモニタリング環境に集めます。このモニタは、デフォルトでは、2つのタブに出力情報を表示します。［*プロセステーブル*］は、CPUロード、メモリ使用量、プロセスのID番号と適切な値など、現在実行中のプロセスの詳細情報を提供します。収集されたデータのプレゼンテーションとフィルタリングはカスタマイズできます。新しいタイプのプロセス情報を追加するには、プロセステーブルのヘッダを左クリックし

て、隠したい欄やビューに追加したい欄を選択します。さまざまなデータページで各種のシステムパラメータを監視したり、ネットワーク上でさまざまなコンピュータにあるデータを並行して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SUSEヘルプページを参照してください。

GNOME環境では、［*電源管理の設定*］と［システムモニタ］を使用します。

17.1.3.2 データの同期化

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要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。

電子メールの同期化
: オフィスネットワークで電子メールを保存するためにIMAPアカウントを使用します。これで電子メールは、KMail、Evolution、またはMozilla Thunderbird Mailなどのような切断型IMAP対応電子メールクライアントを使用するワークステーション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される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。最もよく使用されるものには、`rsync`というコマンドラインツールがあります。詳細については、そのマニュアルページを参照してください(`man 1 rsync`)。

17.1.3.3 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
: WLANは、これらの無線テクノロジの中では最大規模で、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。個々のマシンを相互に接続して、独立した無線ネットワークを構築することも、インターネットにアクセスすることも可能です。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応じ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の詳細については、第18章 *無線LAN* (245 ページ)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。また範囲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、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。

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。

17.1.4 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、さまざまな防犯ツールが小売店で販売されています。

強力な認証
: ログインとパスワードによる標準の認証に加えて、生体認証を使用します。SUSE Linux Enterprise Serverでは、指紋認証がサポートされます。詳細については、第7章 *Using the Fingerprint Reader* (↑*Security Guide (セキュリティガイド)*)を参照してください。

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 Enterprise Serverでの暗号化パーティションの作成については第11章 *Encrypting Partitions and Files* (↑*Security Guide (セキュリティガイド)*)に記載されています。また、YaSTによりユーザーを追加するときに暗号化されたホームディレクトリを作成する場合もあります。

重要: 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
: データの転送には、転送方法に関わらず、セキュリティ保護が必要です。Linuxおよびネットワークに関する一般的なセキュリティ問題については、第1章 *Security and Confidentiality* (↑*Security Guide (セキュリティガイド)*)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第18章 *無線LAN* (245 ページ)に記載されています。

17.2 モバイルハードウェア

SUSE Linux Enterprise Server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、対応するインタフェースを介してシステムに接続されるとすぐに自動的に検出されて設定されます。GNOMEとKDEのファイルマネージャは、いずれもモバイルハードウェアアイテムを柔軟に処理します。これらのメディアを安全にアンマウントするには、いずれかのファイルマネージャの［*安全に取り外す*］(KDE) 機能または［*Unmount Volume*］(GNOME) 機能を使用します。

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ファイルマネージャに表示されます。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にマウントされているデバイスのデスクリプタは、これには影響されません。

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。

17.3 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17.1.3.3項「無線通信」(240ページ)ですでに説明しました。携帯電話側の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。

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。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のサポートを設定し終えたら、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。

17.4 詳細情報

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://tuxmobil.org/ではhttp://www.linux-on-laptops.com/、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。詳細については、http://lists.opensuse.org/opensuse-mobile-de/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 Enterprise Server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。英語の投稿ではhttp://lists.opensuse.org/opensuse-mobile/を使用します。

OpenSyncの詳細については、http://en.opensuse.org/OpenSyncを参照してください。

18 無線LAN

無線LAN(無線ローカルエリアネットワーク、WLAN)は、モバイルコンピューティングの必須要素になりました。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。この章では、YaSTでWLANカードを設定し、伝送を暗号化する方法とその使用に関するヒントについて説明します。

18.1 WLAN標準

無線LANカードは、IEEEが開発した802.11標準を使用して通信します。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18.1「各種WLAN規格の概要」 (245 ページ)参照)。さらに、多数の企業が専有権またはドラフト機能を持つハードウェアを実装しています。

表 18.1 各種WLAN規格の概要

名前	帯域(GHz)	最大伝送速度 (MBit/s)	メモ
802.11レガシー	2.4	2	廃止、実質上、使用可能なエンドデバイスはなし
802.11a	5	54	干渉が少ない

名前	帯域(GHz)	最大伝送速度 (MBit/s)	メモ
802.11b	2.4	11	あまり普及せず
28.29oz	2.4	54	広く普及、11bと後方互換
802.11n	2.4および/または5	300	Common(通常のネットワーキング)
802.11ad	2.4/5/60	最大7000	2012年にリリース、現時点ではあまり普及せず

802.11レガシーカードは、SUSE® Linux Enterprise Serverではサポートされません。802.11a、802.11b、802.11g、および802.11nを使用する大半のカードがサポートされています。通常、新しいカードは802.11n規格に準拠していますが、802.11gを使用するカードもまだあります。

18.2 動作モード

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。

基本的に、無線ネットワークは次の3つのネットワークモードに分類できます。

管理対象アクセスポイントを経由するモード(インフラストラクチャモード)
: 管理ネットワークには、管理要素のアクセスポイントがあります。このモード(インフラストラクチャモードとも呼ばれます)では、ネットワーク内のWLAN局の接続はすべてアクセスポイント経由で行われ、イーサネッ

トへの接続としても機能できます。権限のある局だけが接続できるようにするため、さまざまな認証メカニズム(WPAなど)が使用されます。

アドホックモード(ピアツーピアネットワーク)
: Ad-hocネットワークには、アクセスポイントはありません。アドホックネットワークでは、局同士が直接に通信するので、通常、アドホックネットワークは管理ネットワークより高速です。ただし、アドホックネットワークでは、参加局の伝送範囲と数が大幅に制限されます。それらのネットワークでは、WPA認証もサポートしません。WPAセキュリティを使用する場合は、アドホックモードを使用しないでください。

マスタモード
: マスタモードでは、ネットワークカードがアクセスポイントとして使用されます。無線LANカードでこのモードがサポートされる場合にのみ使用できます。無線LANカードの詳細については、http://linux-wless.passys.nlを参照してください。

18.3 認証

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 (Wired Equivalent Privacy)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(18.6.3項 「セキュリティ」 (259 ページ))、WLAN業界(*Wi-Fi Alliance*という団体名で協力)はWPAという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。より最近のIEEE 802.11i規格には、WPAとその他の認証/暗号化方式が含まれています。IEEE 802.11iは、WPA2とも呼ばれます。これは、WPAが802.11iのドラフトバージョンに基づいているからです。

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。

なし(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。それにも関わらず、WEP暗号化を使用できます(18.4項 「暗号化」 (249 ページ)参照)。

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準拠では、WPA-Personal)

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準拠では、WPA-Enterprise)

実際には、WPA-EAP(Extensible Authentication Protocol)は認証システムではなく、認証情報を転送するためのプロトコルです。WPA-EAPは、企業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では、サーバに接続および認証する3つの異なる方法を提供します。

- EAP-TLS (Transport Layer Security): TLS認証は、サーバ/クライアント両方の証明書の相互交換に依存しています。はじめに、サーバがクライアントに対して証明書を提示し、それが評価されます。証明書が有効であるとみなされた場合には、今度がクライアントがサーバに対して証明書を提示します。TLSはセキュアですが、ネットワーク内で証明書管理のインフラストラクチャを運用することが必要になります。このインフラストラクチャは、プライベートネットワークでは通常存在しません。

- EAP-TTSL (Tunneled Transport Layer Security)
- EAP-PEAP (Protected Extensible Authentication Protocol): TTLSとPEAPは、両方とも2段階のプロトコルです。最初の段階ではセキュリティ接続が確立され、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。

18.4 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。

  非標準の「ダイナミックWEP」を実装しているベンダーもいます。これは、WEPとまったく同様に機能し、同じ弱点を共有しますが、キーがキー管理サービスによって定期的に変更されます。

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。

18.5 YaSTでの設定

重要: 無線ネットワークでのセキュリティリスク

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。必ず、サポートされている認証方式と暗号化方式を使用して、ネットワークトラフィックを保護してください。

ご使用のハードウェアで使用できる最良の暗号化方式を使用してください。ただし、特定の暗号化方式を使用するには、ネットワーク内のすべてのデバイスでこの方式がサポートされる必要があります。さもないと、デバイスが相互に通信できません。たとえば、ルータはWEPとWPAの両方をサポートしますが、WLANカードのドライバはWEPしかサポートしない場合は、WEPが使用できる最小公分母になります。WEPにおる弱い暗号化でも、まったくないよりましです。詳細については、18.4項 「暗号化」 (249 ページ)と18.6.3項 「セキュリティ」 (259 ページ)を参照してください。

YaSTで無線LANを設定するには、次のパラメータを定義する必要があります。

IPアドレス
: 静的IPアドレスを使用するか、またはDHCPサーバでIPアドレスをインタフェースに動的に割り当てます。

動作モード
: ネットワークトポロジに応じて、コンピュータをWLANに統合する方法を定義します。の背景情報については、18.2項 「動作モード」 (246 ページ)を参照してください。

ネットワーク名(ESSID)
: ネットワークを識別するユニークな文字列。

認証と暗号化の詳細
: ネットワークが使用する認証および暗号化の方式に応じて、1つ以上のキーおよび/または証明書を入力する必要があります。

  各キーの入力については、次の入力オプションがあります。［*パスフレーズ*］、［*ASCII*］(WEP認証方式にのみ使用可能)、および［*16進*］。

18.5.1 NetworkManagerの無効化

WLANカードは通常、インストール時に検出されます。コンピュータがモバイルの場合、デフォルトでは、通常、NetworkManagerが有効になっています。WLANカードをYaSTで設定したい場合は、まず、NetworkManagerを無効にする必要があります。

1 ユーザ`root`としてYaSTを起動します。

2 YaST Control Centerで、［*ネットワークデバイス*］>［*ネットワーク設定*］の順に選択して、［*ネットワーク設定*］ダイアログを開きます。

ネットワークが現在、NetworkManagerによって制御されている場合は、ネットワーク設定をYaSTで編集できないことを警告するメッセージが表示されます。

3 YaSTによる編集を可能にするには、［*OK*］でメッセージから出て、［*グローバルオプション*］タブで、［*ifupを使用した従来の方法*］を有効にします。

4 さらに設定を続けたい場合は、18.5.2項 「アクセスポイント用設定」 (251 ページ) または 18.5.3項 「アドホックネットワークの確立」 (256 ページ)に進みます。

そうでない場合は、［*OK*］で変更を確認して、ネットワーク設定を書き込みます。

18.5.2 アクセスポイント用設定

この項では、(外部)アクセスポイントに接続するようにWLANカードを設定する方法、またはWLANカードをアクセスポイントとして使用する方法(WLANカードがこの機能をサポートしている場合)について学習します。アクセスポイントのないネットワークの設定については、 18.5.3項 「アドホックネットワークの確立」 (256 ページ)を参照してください。

手順 18.1 *アクセスポイントを使用するようにWLANカードを設定する*

1 YaSTを起動し、［*ネットワーク設定*］ダイアログを開きます。

2 ［*概要*］タブに切り替えると、システムにより検出されたすべてのネットワークカードが表示されます。一般的なネットワーク設定の詳細については、21.4項 「YaSTによるネットワーク接続の設定」 (307 ページ)を参照してください。

3 リストから目的のワイヤレスカードを選択し、［*編集*］をクリックして、ネットワークカード設定ダイアログを開きます。

4 ［*アドレス*］タブで、コンピュータに動的IPまたは静的IPのどちらを使用するか設定します。通常は、［*DHCP*］を使用する［*可変IPアドレス*］で十分です。

5 ［*次へ*］をクリックして、［*無線ネットワークカードの環境設定*］ダイアログに進みます。

6 WLANカードを使用してアクセスポイントに接続するには、［*動作モード*］を［*管理*］に設定します。

ただし、WLANカードをアクセスポイントとして使用したい場合は、［*動作モード*］を［マスタ］に設定します。ただし、すべてのWLANカードがこのモードをサポートしているわけではないので注意してください。

注記: WPA-PSKまたはWPA-EAPを使用する

認証モードとしてWPA-PSKまたはWPA-EAPを使用する場合は、［動作モード］を［*管理*］に設定する必要があります。

---

7 特定のネットワークに接続するには、［*ネットワーク名(ESSID)*］に入力します。または、［*ネットワークの検索*］をクリックし、使用可能な無線ネットワークのリストからネットワークを選択します。

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。ESSIDを指定しないと、WLANカードは、最良の信号強度を持つアクセスポイントに自動的に接続します。

注記: WPA認証ではESSIDが必須

［*WPA*］認証を選択した場合は、ネットワーク名(ESSID)を設定する必要があります。

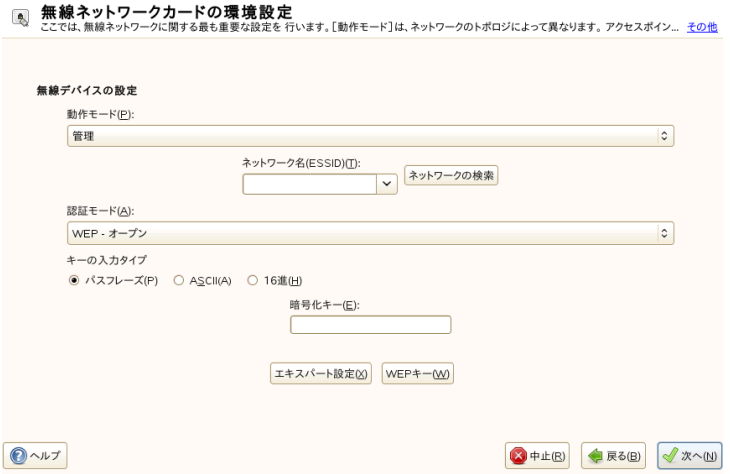
---

8 ネットワークの［*認証モード*］を選択します。適切なモードは、WLANカードのドライバとネットワーク内の他のデバイスの機能によって決まります。

9 ［*認証モード*］を［*暗号化しない*］に設定することを選択した場合は、［*次へ*］をクリックして設定を完了してください。可能なセキュリティリスクに関するメッセージを確認し、［*OK*］をクリックして［*概要*］タブ(新しく設定されたWLANカードを表示)から出ます。

他の認証モードを選択した場合は、手順18.2「暗号化の詳細を入力する」 (253 ページ)に進んでください。

図 18.1　YaST:無線ネットワークカードの設定



手順 18.2　暗号化の詳細を入力する

次の認証方式では、暗号化キーが必要です: ［*WEP - オープン*］、［*WEP - 共有鍵*］、および［*WPA-PSK*］

WEPの場合、通常、キーだけが必要です。ただし、ご使用の局に対して最大4つの異なるWEPキーを定義できます。それらの1つを、デフォルトキーとして設定し、暗号化に使用します。他のキーは復号化に使用します。デフォルトでは、128ビットのキー長が使用されますが、キー長を64ビットに設定することもできます。

セキュリティを高めるため、WPA-EAPでは、RADIUSサーバでユーザを認証します。サーバでの認証では、3つの異なる方式(TLS、TTLS、PEAP)を使用で

きます。WPA-EAP用に必要な資格情報と証明書は、RADIUSサーバ用の認証方法によって異なります。必要な情報と資格情報については、システム管理者にその提供を要求してください。YaSTは/etc/certから証明書を検索します。したがって、付与された証明書はこの場所に保存し、これらのファイルへのアクセスを0600(所有者による読み取り/書き込み)に制限してください。

1 ［*WEP - オープン*］または［*WEP - 共有鍵*］のキーを入力するには:

1a ［*キーの入力タイプ*］を［*パスフレーズ*］、［*ASCII*］、または［*16進*］のいずれかに設定します。

1b 各［*暗号化*キー］を入力します(通常、1つのキーだけが使用されます)。

［*パスフレーズ*］を選択した場合は、指定のキー長(デフォルトで128ビット)に従って、キーにな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。

1c キー長を最も低いビットレートに調節するには(古いハードウェア用に必要な場合)、［*WEP*キー］をクリックして、［キー*長*］を［*64*］ビットに設定します。［*WEP*キー］ダイアログに、今まで入力されたWEPキーも表示されます。別のキーがデフォルトとして明示的に設定されていない限り、YaSTでは、常に最初のキーがデフォルトとして使用されます。

1d WEPの追加キーを入力したり、キーの1つを変更するには、各エントリを選択して、［*編集*］をクリックします。［*キーの入力タイプ*］を選択して、キーを入力します。

1e ［*OK*］をクリックして、変更を確認します。

2 ［*WPA-PSK*］のキーを入力するには:

2a 入力方式として、［*パスフレーズ*］または［*16進*］を選択します。

2b 各［*暗号化キー*］を入力します。

［*Passphrase*］モードでは、 8から 63文字を入力する必要があります。［*16進*］モードでは、64文字を入力します。

3 ［*WPA-EAP*］認証を選択した場合は、［*次へ*］をクリックして［*WPA-EAP*］ダイアログに切り替えます。このダイアログでは、ネットワーク管理者によって与えられた資格情報と証明書を入力します。

3a RADIUSサーバが認証に使用する［*EAPモード*］を選択します。以下で入力する必要のある詳細情報は、選択した［*EAPモード*］によって決まります。

3b TLSの場合は、［*識別情報*］、［*クライアント証明書*］、［*クライアント鍵*］、および［*クライアント鍵パスワード*］に適切な値を入力します。セキュリティを増大するには、サーバの信憑性の検証に使用される［*サーバ証明書*］を設定することもできます。

TTLSおよびPEAPでは、［*識別情報*］と［*パスワード*］は必須ですが、［*サーバ証明書*］と［*匿名識別情報*］はオプションです。

3c WPA-EAPセットアップ用の高度な認証ダイアログに入るには、［*詳細*］をクリックします。

3d EAP-TTLSまたはEAP-PEAP通信の第2段階(内部認証)の［*認証方法*］を選択します。選択する方式は、前のダイアログで選択したRADIUSサーバの認証方法によって決まります。

3e 自動的決定された設定が適切でない場合は、特定の［*PEAPバージョン*］を選択して、特定のPEAP実装の使用を強制してください。

4 ［*OK*］をクリックして、変更を確認します。［*概要*］タブに、新しく設定したWLANカードの詳細が表示されます。

5 ［*OK*］をクリックして設定を確定し、ダイアログを終了します。

18.5.3 アドホックネットワークの確立

場合によっては、無線LANカードを装着した2つのコンピュータを接続すると便利です。YaSTによりアドホックネットワークを確立するには、次の操作を行います。

1. YaSTを起動し、［*ネットワーク設定*］ダイアログを開きます。
2. ［*概要*］タブに切り替え、リストから無線カードを選択し、［*編集*］をクリックして［*ネットワークカードの設定*］ダイアログを開きます。
3. ［*固定IPアドレス*］を選択し、次のデータを入力します。
   - ［*IPアドレス*］：`192.168.1.1`。たとえば、第2のコンピュータでこのアドレスを`192.168.1.2`に変更します。
   - ［*サブネットマスク*］：`/24`
   - ［*ホスト名*］：自由に名前を選択します。
4. ［*次へ*］で続行します。
5. ［*動作モード*］を［*アドホック*］に設定します。
6. ［*ネットワーク名(ESSID)*］を選択します。これは任意の名前にすることできますが、アドホックネットワーク内のすべてのコンピュータでこの名前を使用する必要があります。
7. ネットワークの［*認証モード*］を選択します。適切なモードは、WLANカードのドライバとネットワーク内の他のデバイスの機能によって決まります。
8. ［*認証モード*］を［*暗号化しない*］に設定することを選択した場合は、［*次へ*］をクリックして設定を完了してください。この設定に潜在するセキュリティリスクに関するメッセージを確認し、［*OK*］をクリックして、新しく設定したWLANカードが表示されている［*概要*］タブを出ます。

他の認証モードを選択した場合は、手順18.2「暗号化の詳細を入力する」 (253 ページ)に進んでください。

9 smpppdをインストールしていない場合は、YaSTによりsmpppdをインストールするように求められます。

10 ネットワーク内の他のWLANカードを、同じ［*ネットワーク名(ESSID)*］と同じ［*認証モード*］、異なる IPアドレスを使用して、適宜設定します。

18.5.4 追加の環境設定パラメータを設定する

通常、WLANカードの設定時には、事前設定された設定値を変更する必要はありません。ただし、WLAN接続の詳細な環境設定が必要な場合は、YaSTでは、次の設定を微調整できます。

チャネル
: WLAN局が使用するチャネルの仕様。これは、［*アドホック*］モードと［マスタ］モードにいる場合のみ必要です。［*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。

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
: 旅行中は、電力節減技術でバッテリの動作時間を最大限にすることができます。電源管理に関する詳細については第19章 *電源管理* (263 ページ)を参照してください。電源管理を使用すると、接続品質に影響したり、ネットワーク待ち時間が増大する場合があります。

高度なオプションにアクセスするには:

1 YaSTを起動し、［*ネットワーク設定*］ダイアログを開きます。

2 ［*概要*］タブに切り替え、リストから無線カードを選択し、［*編集*］をクリックして［*ネットワークカードの設定*］ダイアログを開きます。

3 ［*次へ*］をクリックして、［*無線ネットワークカードの環境設定*］ダイアログに進みます。

4 ［*エキスパート設定*］をクリックします。

5 ［*アドホック*］モードでは、自局と他局との通信用に提供されているチャンネル(国によって11から14局)から1つを選択します。［マスタ］モードで、カードがどの［*チャネル*］でアクセスポイントの機能を提供するか決定します。このオプションのデフォルト設定は［*自動*］です。

6 使用する［*ビットレート*］を選択します。

7 接続したい［*アクセスポイント*］のMACアドレスを入力します。

8 ［*電源管理を使用する*］かどうか選択します。

9 ［*OK*］で変更を確認し、［*次へ*］と［*OK*］をクリックして設定を完了します。

18.6 WLANのセットアップに関するヒントとテクニック

次のツールとヒントを使用すると、WLANの速度と安定性だけでなく、セキュリティの側面についても監視と改善が容易になります。

18.6.1 ユーティリティ

パッケージwireless-toolsには、無線LAN固有のパラメータの設定と統計の取得を可能にするユーティリティが含まれています。詳細については、http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.htmlを参照してください。

18.6.2 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、コマンドライン(`Link Quality`フィールド)で、`iwconfig`ユーティリティを指定するか、またはKDEまたはGNOMEで提供されるNetworkManagerアプレットを使用して、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。

`iwspy`コマンドを使用すると、WLANの統計情報を表示できます。

```
iwspy wlan0
wlan0      Statistics collected:
    00:AA:BB:CC:DD:EE : Quality:0  Signal level:0  Noise level:0
    Link/Cell/AP      : Quality:60/94  Signal level:-50 dBm   Noise level:-140
 dBm (updated)
    Typical/Reference : Quality:26/94  Signal level:-60 dBm   Noise level:-90
 dBm
```

18.6.3 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。

個人使用には、利用できる場合はWPA-PSKを使用します。Linuxは大半のハードウェアコンポーネントでWPAをサポートしますが、WPAに対応しないドライバもあります。WPAは、WLAN機能をもつ古いアクセスポイントやルータで使用できない場合もあります。そのようデバイスでは、ファームウェアの更新によってWPAを実装できるかどうかチェックしてください。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。

認証方法に強力なパスワードを使用します。たとえば、Webページhttps://www.grc.com/passwords.htmでは、ランダムな64文字のパスワードが生成されます。

18.7 トラブルシューティング

WLANカードの応答がない場合は、次の前提条件をチェックします。

1. WLANカードのデバイス名を知っていますか?通常、デバイス名はwlan0です。ツールifconfigでチェックします。

2. 必要なファームウェアをチェックしましたか?詳細については、/usr/share/doc/packages/wireless-tools/README.firmwareを参照してください。

3. ルータのESSIDはブロードキャストされ、表示されますか(非表示ではありませんか)?

18.7.1 ネットワークステータスをチェックする

コマンドiwconfigで、無線接続に関する重要な情報が得られます。たとえば、次の行にはESSID、無線モード、周波数、信号が暗号化されているかどうか、リンク品質などの情報が表示されます

```
iwconfig wlan0
wlan0  IEEE 802.11abg  ESSID:"guest"
       Mode:Managed   Frequency:5.22GHz  Access Point: 00:11:22:33:44:55
       Bit Rate:54 Mb/s   Tx-Power=13 dBm
       Retry min limit:7   RTS thr:off   Fragment thr:off
       Encryption key:off
       Power Management:off
       Link Quality:62/92   Signal level:-48 dBm  Noise level:-127 dBm
       Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
       Tx excessive retries:10  Invalid misc:0   Missed beacon:0
```

また、iwlistコマンドで前回の情報を取得できます。たとえば、次の行には現在のビットレートが表示されます。

```
iwlist wlan0 rate
wlan0     unknown bit-rate information.
          Current Bit Rate=54 Mb/s
```

使用可能なアクセスポイント数の概要が必要な場合についても、iwlistコマンドを使用できます。これにより、次のような「セル」のリストが表示されます。

```
iwlist wlan0 scanning
wlan0    Scan completed:
   Cell 01 - Address: 00:11:22:33:44:55
             Channel:40
             Frequency:5.2 GHz (Channel 40)
             Quality=67/70  Signal level=-43 dBm
             Encryption key: off
             ESSID:"Guest"
             Bit Rates: 6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s;
                        24 Mb/s; 36 Mb/s; 48 Mb/s
             Mode: Master
             Extra:tsf=0000111122223333
             Extra: Last beacon: 179ms ago
             IE: Unknown: ...
```

18.7.2 複数のネットワークデバイス

通常、最近のラップトップにはネットワークカードとWLANカードが搭載されています。DHCP(自動アドレス割り当て)を使用して両方のデバイスを構成すると、名前解決とデフォルトゲートウェイに問題が発生することがあります。これは、ルータはpingできるがインターネット上でナビゲーションできないことを示しています。詳細については、http://old-en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clientsにある Support Databas (サポートデータベース)を参照してください。

18.7.3 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。

18.8 詳細情報

詳細については、次のページを参照してください。

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html
: 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。

tuxmobil.org
: Linuxを使用するモバイルコンピュータの有用な実践情報

http://www.linux-on-laptops.com
: ラップトップ上のLinuxの詳細情報

19 電源管理

► **System z:** この章で説明する機能とハードウェアは、IBM System zには存在しないため、この章はこれらのプラットフォームには無関係です。 ◄

電源管理はラップトップコンピュータで特に重要ですが、他のシステムでも役に立ちます。ACPI(Advanced Configuration and Power Interface)は、最近のすべてのコンピュータ(ラップトップ、デスクトップ、サーバ)で使用できます。電源管理テクノロジでは、適切なハードウェアとBIOSルーチンを必要とします。ほとんどのラップトップと多くの新型デスクトップおよびサーバは、これらの必要条件を満たしています。電源の節約や騒音の低減のために、CPU周波数を制御することもできます。

19.1 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。ACPI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
: サポートされていない。

サスペンド(メモリに保存)
: このモードでは、システム状態をすべてRAMに書き込みます。その後、RAMを除くシステム全体がスリープします。この状態では、コンピュータの消費電力が非常に小さくなります。この状態の利点は、ブートやアプ

リケーションの再起動をせずに、数秒でスリープ前の作業をスリープの時点から再開できることです。この機能は、ACPI状態S3に対応します。

ハイバーネーション(ディスクに保存)
: この動作モードでは、システム状態がすべてハードディスクに書き込まれ、システムの電源がオフになります。すべてのアクティブデータを書き込むには、少なくともRAMの大きさのスワップパーティションが必要です。この状態から再開するには、30〜90秒かかります。サスペンド前の状態が復元されます。メーカの中には、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、システムは、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。

プロセッサ速度の制御
: CPUとの接続では、次の3つの方法で省エネできます:周波数と電圧の調節(PowerNow!またはSpeedstep)、スロットリング、およびプロセッサをスリープ状態(C-states)にすること。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。

19.2 ACIP(詳細設定と電源インタフェース)

ACPI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し、制御できるように設計されています。ACPIは、PnP(Power Management Plug and Play)とAPM(Advanced Power Management)の両方に優先します。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、19.2.2項「トラブルシューティング」 (266 ページ)を参照してください。

19.2.1 CPUパフォーマンスの制御

CPUには、3つの省エネ方法があります。

- 周波数と電圧の調節
- クロック周波数のスロットリング(T-states)
- プロセッサのスリープ状態への切り替え(C-states)

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。

周波数調節とスロットリングに意味があるのは、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、常に、最も経済的なC-stateが適用されるからです。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。通常、カーネルのオンデマンドガバナによって動的に制御される動的な周波数調節が最良のアプローチです。

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。

詳細については、第11章 *Power Management* (↑*System Analysis and Tuning Guide (システム分析およびチューニングガイド)*)を参照してください。

19.2.2 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=ht
: 単純なリソース設定のみを実行します。ACPIを他の目的には使用しません。

acpi=off
: ACPIを無効にします。

警告: ACPIなしに起動できない場合

一部の新型のコンピュータは(特に、SMPシステムとAMD64システム)、ハードウェアを正しく設定するためにACPIが必要です。これらのコンピュータでACPIを無効にすると、問題が生じます。

コンピュータは時折、USBまたはFireWireを介して接続されたハードウェアと混同されることがあります。コンピュータが起動を拒否した場合、必要のないハードウェアのプラグをすべてはずして再試行してください。

システムのブートメッセージを調べてみましょう。そのためには、ブート後にコマンド`dmesg | grep -2i acpi`を使用します(または、問題の原因がACPIだとは限らないので、すべてのメッセージを調べます)。ACPIテーブルの解析時にエラーが発生した場合は、最も重要なテーブルDSDT(*Differentiaed System Description Table*)を改善されたバージョンと置き換えることができま

す。この場合、BIOSで障害のあるDSDTが無視されます。具体的な手順については19.4項「トラブルシューティング」(269ページ)を参照してください。

カーネルの設定には、ACPIデバッグメッセージを有効にするスイッチがあります。ACPIデバッグを有効にした状態でカーネルをコンパイルおよびインストールすると、詳細情報が発行されます。

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。

19.2.2.1 詳細情報

- http://tldp.org/HOWTO/ACPI-HOWTO/ (詳細なACPI HOWTO、DSDTパッチが含まれています)
- http://www.acpi.info (Advanced Configuration and Power Interface: 詳細設定と電源インタフェース)
- http://www.lesswatts.org/projects/acpi/ (SourceforgeによるACPI4Linuxプロジェクト)
- http://acpi.sourceforge.net/dsdt/index.php (Bruno DucrotによるDSDTパッチ)

19.3 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、最大限に省電力したい場合は、次の方法のいくつかを`hdparm`コマンドでテストしてください。

このコマンドを使用すると、各種のハードディスク設定を変更できます。`-y`オプションは、簡単にハードディスクをスタンバイモードに切り替えます。

-Yを指定すると、スリープ状態になります。hdparm -S xを使用すると、一定時間アクティビティがなければハードディスクが回転を停止します。*x*は、次のように置換します。0を指定するとこの機構が無効になり、ハードディスクは常時稼働します。1から240までの値を指定すると、指定した値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。はじめに、すべてのデータがRAMにバッファされます。このバッファは、pdflushデーモン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、データの完全性を最大まで高めるように、pdflushの間隔が短く設定されています。pdflushデーモンはバッファを5秒おきにチェックし、データをハードディスクに書き込みます。次の変数が使用できます。

/proc/sys/vm/dirty_writeback_centisecs
: pdflushスレッドが起動するまでの遅延(100分の1秒台)を含みます。

/proc/sys/vm/dirty_expire_centisecs
: ダーティページが次に最新の変更を書き込まれるまでの時間枠を定義します。デフォルト値は3000(つまり 30秒)です。

/proc/sys/vm/dirty_background_ratio
: pdflushが書き込みを始めるまでのダーティページの最大割合。デフォルトは5パーセントです。

/proc/sys/vm/dirty_ratiol
メモリ全体の中でダーティページの割合がこの値を超えると、プロセスは書き込みを続けずに、短時間でダーティバッファを書き込むように強制されます。

警告: データの完全性に関する障害

pdflush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、Btrfs、Ext3、Ext4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pdflushとは無関係に書き込むので、ハードディスクがスピンダウンしなくなります。

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。

19.4 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。以下のセクションでは、最も頻繁に起こる問題について解説します。

19.4.1 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に問題がある場合は、dmesg|grep -i acpiコマンドを使用して、dmesgの出力を調べ、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。

手順 19.1　BIOSでのDSDTテーブルの更新

以下の手順の場合、次の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:`kernel-source`、`pmtools`、および`mkinitrd`

1 http://acpi.sourceforge.net/dsdt/index.phpからシステムに適したDSDTをダウンロードします。以下に示すようにファイルを解凍し、コンパイル後ファイル拡張子が`.aml` (ACPI machine language)になっていることを確認します。拡張子が.amlの場合はステップ3に進みます。

2 ダウンロードしたテーブルのファイル拡張子が`.asl` (ACPI source language)である場合は、次のコマンドを実行してファイルをコンパイルします。

```
iasl -sa file.asl
```

3 (結果の)ファイル`DSDT.aml`を任意の場所(`/etc/DSDT.aml`を推奨)にコピーします。

4 `/etc/sysconfig/kernel`を編集し、DSDTファイルに応じてパスを変更します。

5 `mkinitrd`を起動します。カーネルをインストールし、`mkinitrd`を使用して`initrd`ファイルを作成するたびに、システムのブート時に、変更されたDSDTが組み込まれ、ロードされます。

19.4.2 CPU周波数調節が機能しません。

カーネルのソースを参照して、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。`kernel-source`パッケージがインストールされている場合は、この情報を`/usr/src/linux/Documentation/cpu-freq/*`で入手できます。

19.4.3 サスペンドとスタンバイが機能しません。

ACPIシステムでは問題のあるDSDTを実装していることにより(BIOS)、サスペンドとスタンバイに関する問題が発生する可能性があります。そのような場合は、BIOSをアップデートしてください。

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。ログファイル`/var/log/pm-suspend.log`には、エラーのの内容と場所に関する詳細情報が含まれます。`/usr/lib/pm-utils/defaults`の`SUSPEND_MODULES`変数を変更し、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。

19.5 詳細情報

- `http://en.opensuse.org/SDB:Suspend_to_RAM`—「How to get Suspend to RAM working」
- `http://old-en.opensuse.org/Pm-utils`—「How to modify the general suspend framework」

20 タブレットPCの使用

SUSE® Linux Enterprise Serverでは、タブレットPCをサポートします。ここでは、タブレットPCのインストールと設定の方法を学び、デジタルペンで入力できるLinux* アプリケーションの利便性を理解します。

次のタブレットPCが使用できます。

- シリアルおよびUSB接続のWacomタブレット（ペンベース)、タッチスクリーン、またはマルチタッチのデバイスを含むタブレットPC。
- FinePointデバイス(Gateway C210X/M280E/CX2724、HP Compaq TC1000など)を含むタブレットPC。
- Asus R2H、Clevo TN120R、Fujitsu Siemens Computers P-Series、LG C1、Samsung Q1/Q1-Ultraなどのタッチスクリーンデバイスを含むタブレットPC。

タブレットPCパッケージをインストールしてデジタイザを正しく設定すると、スタイラスと呼ばれるペンによる入力を、次のアクションとアプリケーションに使用できます。

- KDMまたはGDMへのログイン
- KDEとGNOMEデスクトップの画面のロック解除
- カーソルの画面上の移動、アプリケーションの起動、終了、サイズ変更、ウィンドウの移動、ウィンドウのフォーカス移動、オブジェクトのドラッグドロップなど、その他のポインティングデバイス(マウスやタッチパッドなど)によって起動されるアクション

- X Window Systemのアプリケーションのジェスチャ認識の使用
- GIMPによる描画
- JarnalまたはXournalなどのアプリケーションでのメモ作成またはスケッチ、またはDasherによる大量のテキストの編集

20.1 タブレットPCパッケージのインストール

タブレットPC用に必要なパッケージは、`TabletPC`インストールパターンに含まれています。インストール時にTabletPCを選択した場合は、次のパッケージがすでにシステムにインストールされているはずです。

- `cellwriter`: 文字ベースの手書き入力パネル
- `jarnal`: Javaベースのメモ作成用アプリケーション
- `xournal`: メモ作成およびスケッチ用アプリケーション
- `xstroke`: X Windows System向けジェスチャー認識プログラム
- `xvkbd`: X Window System向け仮想キーボード
- `x11-input-fujitsu`: Fujitsu P-Seriesタブレット向けX入力モジュール
- `x11-input-evtouch`: タッチスクリーンのある一部のタブレットPCのX入力モジュール
- `xorg-x11-driver-input`: Wacomデバイス向けモジュールなど、入力デバイスのX入力モジュール

これらのパッケージがインストールされていない場合は、必要なパッケージをコマンドラインから手動でインストールするか、YaST内で`TabletPC`インストール用パターンを選択します。

20.2 タブレットデバイスの設定

タブレットまたはタッチデバイスは、インストール時にデフォルトで設定されます。このWacomデバイスの設定に問題がある場合は、コマンドラインで`xsetwacom`を使用して、設定を変更してください。

20.3 仮想キーボードの使用

KDEまたはGNOMEデスクトップにログインしたり、画面のロックを解除するには、ユーザ名とパスワードを、通常通りに入力するか、ログインフィールドの下に表示される仮想キーボードxvkbdから入力します。キーボードを設定するには、または統合ヘルプにアクセスするには、左下隅の［*xvkbd*］フィールドをクリックしてxvkbdメインメニューを開きます。

入力が表示されない場合(または表示されるべきウィンドウに転送されない場合)、xvkbdで［*Focus*］キーをクリックしてフォーカスをリダイレクトしてから、キーボードイベントを反映させるウィンドウをクリックします。

図 20.1　xvkbd仮想キーボード

ログイン後にxvkbdを使用するには、メインメニューから起動するか、またはシェルから`xvkbd`で起動します。

20.4 ディスプレイの回転

KRandRTray(KDE)またはgnome-display-properties(GNOME)を使用すると、オンザフライで、ディスプレイの回転やサイズ変更を手動で行うことができます。

KRandRTrayおよびgnome-display-propertiesは両方とも、XサーバのRANDR拡張用アプレットです。

メインメニューからKRandRTrayまたはgnome-display-properties を起動するか、「krandrtray」または「gnome-display-properties」を入力して、シェルからアプレットを起動します。アプレットを起動すると、通常、アプレットアイコンがシステムトレイに追加されます。gnome-display-propertiesアイコンがシステムトレイに自動的に表示されない場合は、［*Show Displays in Panel*］が［*Monitor Resolution Settings*］ダイアログでオンになっているかかどうかを確認してください。

KRandRTrayでディスプレイを回転するには、アイコンを右クリックし、［ディスプレイの設定］を選択します。設定ダイアログから、該当する向きを選択します。

gnome-display-propertiesでディスプレイを回転するには、アイコンを右クリックし、該当する向きを選択します。ディスプレイが新しい方向にすぐに回転します。また、グラフィックタブレットの向きも変更されるので、(ディスプレイの向きが変わっても)ペンの動きを正しく解釈できます。

デスクトップの向きの変更で問題がある場合は、20.7項「トラブルシューティング」 (281 ページ)で詳細を参照してください。

20.5 ジェスチャ認識の使用

SUSE Linux Enterprise Serverには、ジェスチャ認識用にCellWriterおよびxstrokeの両方が含まれます。どちらのアプリケーションでも、ペンまたはその他のポインティングデバイスによるジェスチャを、X Window Systemのアプリケーションへの入力として使用できます。

20.5.1 CellWriterの使用

CellWriterを使用すると、セルのグリッドに文字を書き込むことができ、書き込んだ内容は文字ベースで即座に認識されます。書き込みが終了したら、入力を現在フォーカスされているアプリケーションに送信できます。ジェスチャ認識にCellWriterを使用できるようにするには、最初にアプリケーションがユーザの手書き文字を認識できるよう学習させる必要があります。文字を1つずつ

特定のキーのマップで覚えさせます(覚えさせていない文字はアクティブ化されないため使用できません)。

手順 20.1 *CellWriterのトレーニング*

1. メインメニューから、またはコマンドラインから「`cellwriter`」を入力してCellWriterを起動します。最初の起動時には、CellWriterは自動的にトレーニングモードで起動します。トレーニングモードでは、現在選択されているキーマップの文字セットが示されます。

2. 各文字のセルに文字に使用するジェスチャを入力します。最初の入力時に背景の色が白に変わり、文字は薄いグレーで表示されます。文字の色が黒に変わるまでジェスチャを複数回繰り返します。トレーニングされていない文字は薄いグレーまたは茶色の背景で表示されます(デスクトップのカラースキームによる)。

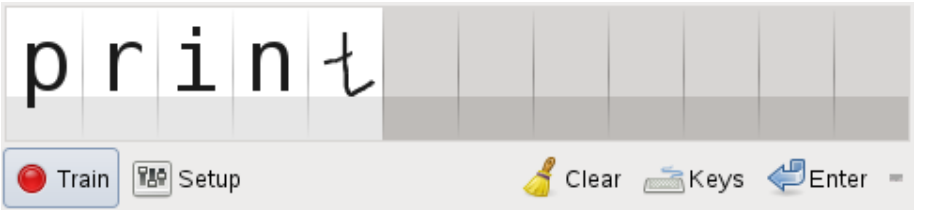
3. CellWriterが必要な文字をすべて覚えるまでこの手順を繰り返します。

4. CellWriterに別の言語を覚えさせるには、［*Setup*］ボタンをクリックして［*言語*］タブから言語を選択します。［*閉じる*］をクリックして設定ダイアログを閉じます。［*Train*］ボタンをクリックし、［*CellWriter*］ウインドウの右下にあるドロップダウンボックスからキーマップを選択します。新しいキーのマップについてトレーニングを繰り返します。

5. キーマップのトレーニングが終了したら、［*Train*］ボタンをクリックして通常モードに切り替えます。

通常のモードでは、CellWriterウィンドウにジェスチャを入力するための空のセルがいくつか表示されます。［*Enter*］ボタンをクリックするまで文字は別のアプリケーションには送信されません。文字を入力として使用する前に修正したり削除できます。認識の確実度が低い文字はハイライト表示されます。入力を修正するには、セルを右クリックすると表示されるコンテキストメニューを使用します。文字を削除するには、ペンの消しゴムを使用するか、マウスで中央をクリックしてセルをクリアします。CellWriterで入力が終了したら、アプリケーションのウィンドウをクリックして入力の送信先となるアプリケーションを定義します。［*Enter*］をクリックしてアプリケーションに入力を送信します。

図 20.2　CellWriterのジェスチャ認識



CellWriterの［*Keys*］ボタンをクリックすると、仮想キーボードが表示され、手書き認識の変わりに使用できます。

CellWriterを非表示にするには、CellWriterウィンドウを閉じます。これでこのアプリケーションはシステムトレー内にアイコンで表示されます。入力ウィンドウを再表示するには、システムトレイのアイコンをクリックします。

20.5.2 Xstrokeの使用

xstrokeでは、ペンまたはその他のポインティングデバイスでのジェスチャを、X Window Systemのアプリケーションへの入力として使用できます。xstrokeアルファベットは、Graffiti*アプレットに類似のユニストロークアルファベットです。有効にすると、xstrokeは入力を現在フォーカスされているウィンドウに送信します。

1. メインメニューから、またはシェルから`xstroke`を使用して、xstrokeを起動します。これで、ペンシルアイコンがシステムトレイに追加されます。

2. ペンでテキスト入力を作成したいアプリケーション(たとえば、ターミナルウィンドウ、テキストエディタ、LibreOffice Writerなど)を起動します。

3. ジェスチャー認識モードを有効にするため、ペンシルアイコンを1回クリックします。

4. ペンまたは別のポインティングデバイスで、グラフィックタブレット上で何らかのジェスチャを行います。xstrokeはジェスチャをキャプチャし、テキストに転送してフォーカスのあるアプリケーションウィンドウに表示します。

5 フォーカスを別のウィンドウに移すには、目的のウィンドウをペンでクリックしてしばらくそのままにします(または、デスクトップのコントロールセンターで定義したキーボードショートカットを使用します)。

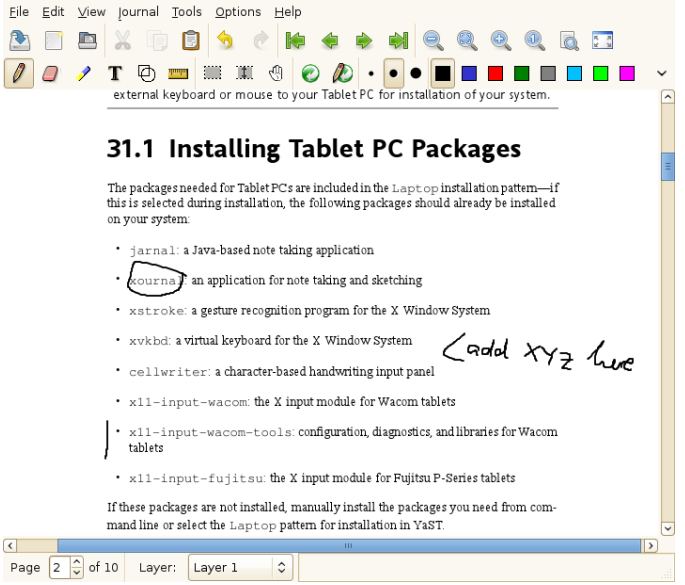
6 ジェスチャ認識モードを無効にするには、ペンシルアイコンをもう一度クリックします。

20.6 ペンを使用したメモの作成とスケッチ

ペンで図を描くには、GIMPなどのプロ向けグラフィックエディタを使用したり、XournalまたはJarnalなどのメモ作成アプリケーションを使用します。XournalとJarnalの両方を使用し、ペンを使って、メモを取ったり、図を作成したり、PDFファイルにコメントを付けたりすることができます。いくつかのプラットフォームで使用できるJavaベースのアプリケーションとして、Jarnalには基本的なコラボレーション機能もあります。詳細については、http://www.dklevine.com/general/software/tc1000/jarnal-net.htmを参照してください。コンテンツを保存するとき、Jarnalはデータをアーカイブ形式(*.jaj)にデータを保存し、これにはSVG形式のファイルも含まれます。

JarnalまたはXournalをメインメニューから、またはシェルに「jarnal」または「xournal」と入力して起動します。XournalでPDFファイルにコメントを付けるには、［*ファイル*］>［*Annotate PDF*］を選択して、ファイルシステムからPDFファイルを開きます。ペンまたは別のポインティングデバイスを使用してPDFに注釈を付け、［*ファイル*］>［*Export to PDF*］の順に選択して変更内容を保存します。

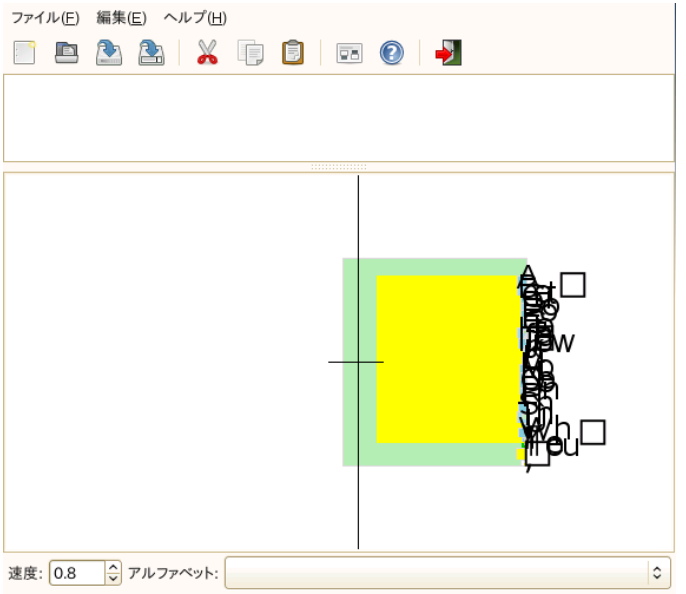
図 20.3　XournalによるPDFへの注釈



Dasherも便利なアプリケーションです。キーボード入力が実用的ではない、または利用できない場合に適しています。少し訓練することで、ペンだけで大量のテキストを高速に入力できるようになります(または、視線追跡手段などによるペン以外の入力デバイス)。

メインメニューから、またはシェルから「`dasher`」と入力してDasherを起動します。ペンをある方向に動かすと、アプリケーションが右側の文字にズームインし始めます。中央の十字を過ぎた文字から、テキストが作成または予測され、ウィンドウ上部に出力されます。書き込みを停止または開始するには、ディスプレイをペンで1回クリックします。ウィンドウ下部でズーム速度を変更します。

図 20.4　Dasherによるテキストの編集



Dasherの概念は、多くの言語で動作します。詳細はDasherのWebサイトを参照してください。包括的なドキュメント、デモ、トレーニング用テキストがあります。http://www.inference.phy.cam.ac.uk/dasher/をご覧ください。

20.7 トラブルシューティング

仮想キーボードがログイン画面に表示されない

時々、ログイン画面が仮想キーボードに表示されないことがあります。これを解決するには、Ctrl + Alt + <—を押すか、またはタブレットPCの該当するキー(内蔵キーボードのないスレートモデルを使用している場合)を押して、X Serverを再起動します。仮想キーボードがまだ表示されない場合は、外部キーボードをスレートモデルに接続し、ハードウェアキーボードを使用してログインします。

Wacomグラフィックタブレットの向きが変わらない

xrandrコマンドで、シェルからディスプレイの向きを変更できます。「xrandr--help」と入力すると、使用できるオプションが表示されま

す。グラフィックタブレットの向きも同時に変更するには、コマンドを以下のように変更します。

- 通常の方向(0度回転):

```
xrandr –o normal && xsetwacom –-set "Serial Wacom Tablet" Rotate
NONE
```

- 90度回転(時計回り、縦):

```
xrandr –o right && xsetwacom –-set "Serial Wacom Tablet" Rotate CW
```

- 180度回転(横):

```
xrandr –o inverted && xsetwacom –-set "Serial Wacom Tablet" Rotate
HALF
```

- 270度回転(反時計回り、縦):

```
xrandr –o left && xsetwacom set –-"Serial Wacom Tablet" Rotate CCW
```

ただし、上記のコマンドは、`xsetwacom list`コマンドの出力に依存します。`"Serial Wacom Tablet"`は、スタイラスまたはタッチデバイスの出力で置き換えます。タッチサポート(指を使ってカーソルを移動できる)の備わったWacomデバイスの場合、タッチデバイスを回転させることも必要です。

20.8 詳細情報

ここで説明したアプリケーションの一部には統合オンラインヘルプがありませんが、使用方法および設定についての便利な情報が、インストールしたシステムの/usr/share/doc/package/*packagename*またはWeb上にあります。

- Xournalのマニュアルは、http://xournal.sourceforge.net/manual.htmlを参照してください。
- Jarnalのドキュメントは、http://jarnal.wikispaces.com/にあります。
- xstrokeのマニュアルページは、http://davesource.com/Projects/xstroke/xstroke.txtにあります。
- Linux上でXを設定する方法は、Wacom Webサイト(http://sourceforge.net/apps/mediawiki/linuxwacom/index.php?title=Configuring_X)を参照してください。
- Dasherプロジェクトについては、Webサイトhttp://www.inference.phy.cam.ac.uk/dasher/に詳細な情報があります。
- CellWriterの詳細およびドキュメントについては、http://risujin.org/cellwriter/を参照してください。
- gnome-display-propertiesについては、http://old-en.opensuse.org/GNOME/Multiscreenを参照してください。

パート IV. サービス

21 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。ネットワークカード、モデム、その他のデバイスを使用したネットワークアクセスは、YaSTで設定できます。手動による環境設定も可能です。この章では、基本的メカニズムと関連のネットワーク設定ファイルのみを解説します。

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21.1「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」 (288 ページ)に示した各プロトコルが提供されています。TCP/IPによって結合された世界規模のネットワークを「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習得するには、適切なRFC文書を参照してください。これらは、`http://www.ietf.org/rfc.html`から入手できます。

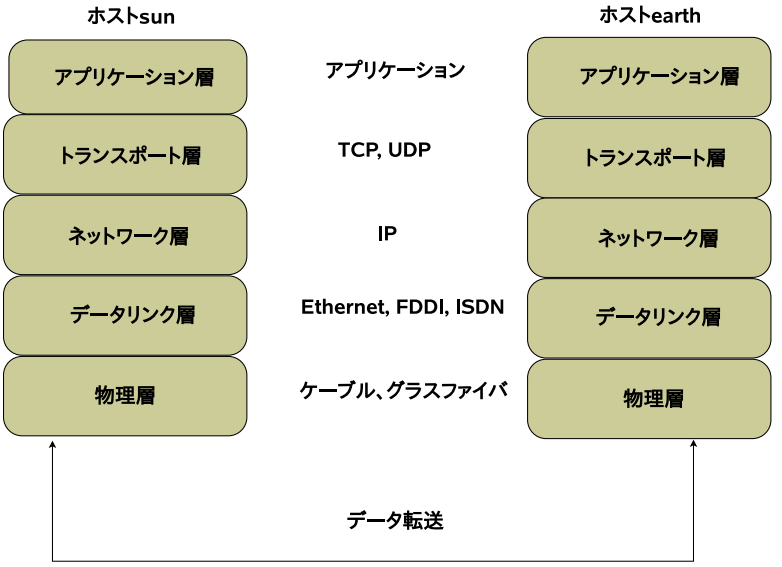
表 21.1　TCP/IPプロトコルファミリーを構成する主要なプロトコル

プロトコル	説明
TCP	TCP(Transmission Control Protocol): 接続指向型の安全なプロトコルです。転送データは、まず、アプリケーションによってデータストリームとして送信され、オペレーティングシステム.によって適切なフォーマットに変換されます。データは、送信当初のデータストリーム形式で、宛先ホストのアプリケーションに着信します。TCPは転送中に損失したデータや順序が正しくないデータがないか、判定します。データの順序が意味を持つ場合は常にTCP/IPが実装されます。
UDP	UDP(User Datagram Protocol): コネクションレスで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があります。UDPはレコード指向のアプリケーションに適しています。TCPよりも遅延時間が小さいことが特徴です。
ICMP	ICMP (Internet Control Message Protocol):基本的にはエンドユーザ向けのプロトコルではありませんが、エラーレポートを発行し、TCP/IPデータ転送にかかわるマシンの動作を制御できる特別な制御プロトコルです。またICMPには特

プロトコル	説明
	別なエコーモードがあります。エコーモードは、pingで使用されています。
IGMP	IGMP (Internet Group Management Protocol):このプロトコルは、IPマルチキャストを実装した場合のコンピュータの動作を制御します。

に示したように、データのやり取りはさまざまなレイヤで実行されます。図21.1「TCP/IPの簡易レイヤモデル」(289ページ)実際のネットワークレイヤは、IP (インターネットプロトコル)によって実現される確実性のないデータ転送です。IPの上で動作するTCP(転送制御プロトコル)によって、ある程度の確実性のあるデータ転送が保証されます。IPレイヤの下層には、イーサネットなどのハードウェア依存プロトコルがあります。

図 21.1　TCP/IPの簡易レイヤモデル



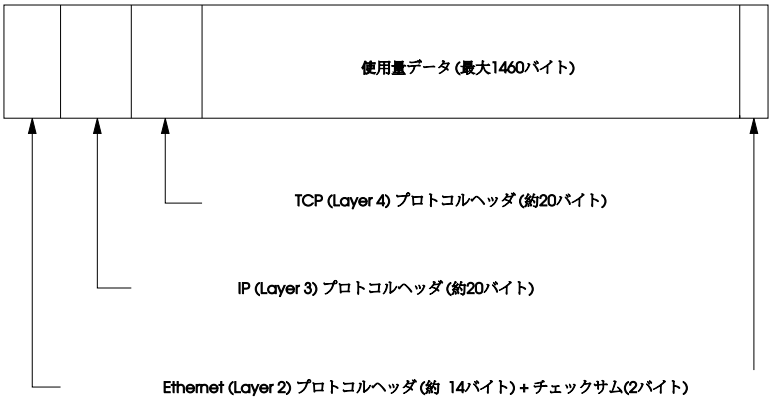
図では、各レイヤに対応する例を1つまたは2つ示しています。レイヤは*抽象化レベル*に従って並べられています。最下位レイヤは最もハードウェアに近

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、パケットにまとめられます(一度に全部を送信できません)。TCP/IPパケットの最大サイズは約64KBです。パケットサイズは通常、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21.2「TCP/IPイーサネットパケット」 (290 ページ)に、イーサネットケーブル上に送出されるTCP/IPデータパケットの例を示します。誤り検出のためのチェックサムは、パケットの先頭ではなく最後に付加されます。これによりネットワークハードウェアの処理が簡素化されます。

図 21.2　TCP/IPイーサネットパケット



アプリケーションがデータをネットワーク経由で送信すると、データは各レイヤを通過します。これらのレイヤは、物理レイヤを除き、すべてLinuxカー

ネルに実装されています。各レイヤは、隣接する下位レイヤに渡せるようにデータを処理します。最下位レイヤは、最終的にデータを送信する責任を負います。データを受信したときには、この手順全体が逆の順序で実行されます。重なり合ったたまねぎの皮のように、各レイヤで伝送データからプロトコルヘッダが除去されていきます。最後に、トランスポートレイヤが、着信側のアプリケーションがデータを利用できるように処理します。この方法では、1つのレイヤが直接やり取りを行うのは隣接する上下のレイヤのみです。データが伝送される物理的なネットワークは、100MBit/sのFDDIかもしれませんし、56Kbit/sのモデム回線かもしれませんが、アプリケーションがその違いを意識することはありません。同様に、物理ネットワークは、パケットの形式さえ正しければよく、伝送されるデータの種類を意識することはありません。

21.1 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、21.2項 「IPv6 —次世代のインターネット」 (294 ページ)を参照してください。

21.1.1 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、固有の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21.1「IPアドレスの表記」 (291 ページ)の2行目に示すような形式で表記されます。

例 21.1 IPアドレスの表記

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.     168.       0.      20
```

10進表記では、4つの各バイトが10進数で表記され、ピリオドで区切られます。IPアドレスは、ホストまたはネットワークインタフェースに割り当てられます。使用できるのは1回のみです。このルールには例外もありますが、次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。

21.1.2 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台のホストが同じサブネットワークに存在する場合、相互に直接アクセスできます。同じサブネットワークにない場合は、サブネットワークのすべてのトラフィックを処理するゲートウェイのアドレスが必要です。2つのIPアドレスが同じサブネットワークに属しているかどうかを確認するには、両方のアドレスとネットマスクの「AND」を求めます。結果が同一であれば、両方のIPアドレスは同じローカルネットワークに属しています。相違があれば、それらのIPアドレス、そしてそれらに対応するインタフェースが連絡するには、ゲートウェイを通過する必要があります。

ネットマスクの役割を理解するには、例21.2「IPアドレスとネットマスクの論理積(AND)」 (292 ページ)を参照してください。ネットマスクは、そのネットワークにいくつのIPアドレスが属しているかを示す、32ビットの値から成っています。1になっているビットは、IPアドレスのうち、特定のネットワークに属することを示すビットに対応します。0になっているビットは、サブネットワーク内での識別に使われるビットに対応します。これは、1になっているビット数が多いほど、サブネットワークが小さいことを意味します。ネットマスクは常に連続する1のビットから構成されているので、その数だけでネットマスクを指定することができます。例21.2「IPアドレスとネットマスクの論理積(AND)」 (292 ページ)の、24ビットからなる第1のネットワークは、`192.168.0.0/24`と書くこともできます。

例 21.2　IPアドレスとネットマスクの論理積(AND)

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

また、たとえば同じイーサネットケーブルに接続しているすべてのマシンは、普通同じサブネットに属し、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 21.2　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21.2「IPアドレスとネットマスクの論理積 (AND)」 (292 ページ)のANDをとった結果を参照。このアドレスは、どのホストにも割り当てることができません。
ブロードキャストアドレス	ブロードキャストアドレスは、基本的には「サブネットワーク内のすべてのホストにアクセスする」ためのアドレスです。」このアドレスを生成するには、2進数形式のネットマスクを反転させ、基本ネットワークアドレスと論理和をとります。そのため上記の例では、192.168.0.255になります。このアドレスをホストに割り当てることはできません。

アドレスのタイプ	説明
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。このアドレスと、IPv4で定義された完全な127.0.0.0/8ループバックネットワークからのすべてのアドレスで、自分のマシンへの接続を設定できます。IPv6では、ループバックアドレスは1つだけです(::1)。

IPアドレスは、世界中で固有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21.3「プライベートIPアドレスドメイン」(294ページ)に示すとおりに定められています。

表 21.3 *プライベートIPアドレスドメイン*

ネットワーク/ネットマスク	ドメイン
10.0.0.0/255.0.0.0	10.x.x.x
172.16.0.0/255.240.0.0	172.16.x.x – 172.31.x.x
192.168.0.0/255.255.0.0	192.168.x.x

21.2 IPv6 —次世代のインターネット

重要: IBM System z: IPv6サポート

IPv6は、IBM System zハードウェアのCTCおよびIUCVネットワーク接続ではサポートされていません。

WWW(ワールドワイドウェブ)の出現により、ここ10年間でTCP/IP経由で通信を行うコンピュータの数が増大し、インターネットは爆発的に拡大しました。CERN (http://public.web.cern.ch)のTim Berners-Leeが1990年にWWWを発明して以来、インターネットホストは、数千から約1億まで増加しました。

前述のように、IPv4のアドレスはわずか32ビットで構成されています。しかも、多くのIPアドレスが失われています。というのは、ネットワークの編成方法のせいで、使われないIPアドレスが無駄に割り当てられてしまうからです。サブネットで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。

21.2.1 長所

この新しいプロトコルがもたらした最大かつ最もわかりやすい進歩は、利用可能なアドレス空間の飛躍的な増加です。IPv6アドレスは、従来の32ビットではなく、128ビットで構成されています。これにより、2の128乗、つまり、約3.4×1038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、21.2.2項 「アドレスのタイプと構造」 (297 ページ)を参照してください。

以下に、この新しいプロトコルの利点をいくつか紹介します。

自動環境設定機能
: IPv6を使用すると、ネットワークが「プラグアンドプレイ」対応になります。つまり、新しくシステムをセットアップすると、手動で環境設定しなくても、(ローカル)ネットワークに統合されます。新しいホストは自動環境設定メカニズムを使用して、*ネイバーディスカバリ* (ND)と呼ばれるプロトコルにより、近隣のルータから得られる情報を元に自身のアドレスを生成します。この方法は、管理者の介入が不要なだけでなく、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。

  それでもルータがスイッチに接続されていれば、ルータは、ネットワークのホストに相互に通信する方法を通知するフラグ付きのアドバタイズを定期的に送信します。詳細は、RFC 2462および`radvd.conf(5)`のマニュアルページ、RFC 3315を参照してください。

モバイル性
: IPv6を使用すると、複数のアドレスを1つのネットワークインタフェースに同時に割り当てることができます。これにより、ユーザは複数ネットワークに簡単にアクセスできます。このことは、携帯電話会社が提供する国際ローミングサービスにたとえられます。携帯電話を海外に持って行った場合、現地会社のサービス提供エリアに入ると自動的に携帯電話はそのサービスにログインし、同じ番号で普段と同じように電話をかけることができます。

安全な通信
: IPv4では、ネットワークセキュリティは追加機能です。IPv6にはIPSecが中核的機能の1つとして含まれているので、システムが安全なトンネル経由で通信でき、インターネット上での部外者による通信傍受を防止します。

後方互換性
: 現実的に考えて、インターネット全体を一気にIPv4からIPv6に切り替えるのは不可能です。したがって、両方のプロトコルが、インターネット上だけでなく1つのシステム上でも共存できることが不可欠です。これは、一方ではアドレスの互換性によって(IPv4アドレスは容易にIPv6アドレスに変換できます)、他方ではトンネルの使用によって保証されています。参照先21.2.3項「IPv4とIPv6の共存」(303ページ). また、システムはデュアルスタック*IP*テクニックによって、両方のプロトコルを同時にサポートできるので、2つのプロトコルバージョン間に相互干渉のない、完全に分離された2つのネットワークスタックが作成されます。

マルチキャストによるサービスの詳細なカスタマイズ
: IPv4では、いくつかのサービス(SMBなど)が、ローカルネットワークのすべてのホストにパケットをブロードキャストする必要があります。IPv6では、これよりはるかにきめ細かいアプローチが取られ、サーバがマルチキャストという、複数のホストをグループの一部として扱う技術によって、ホストにデータを送信します(これは、すべてのホストにデータを送信するブロードキャストとも、各ホストに個別に送信するユニキャストとも異なります)。どのホストを対象グループに含めるかは、個々のアプリケーションによって異なります。事前定義のグループには、たとえば、すべてのネームサーバを対象とするグループ(全ネームサーバマルチキャストグループ)やすべてのルータを対象とするグループ(全ルータマルチキャストグループ)があります。

21.2.2 アドレスのタイプと構造

これまでに述べたように、現在のIPプロトコルには、IPアドレス数が急激に不足し始めているということと、ネットワーク設定とルーティングテーブルの管理がより複雑で煩雑な作業になっているという、2つの重要な問題があります。IPv6では、1つ目の問題を、アドレス空間を拡張することによって解決しています。2番目の問題には、階層的なアドレス構造を導入し、ネットワークアドレスを割り当てる高度なテクニックとマルチホーミング(1つのデバイスに複数のアドレスを割り当てることによって、複数のネットワークへのアクセスを可能にします)を組み合わせて対応しています。

IPv6を扱う場合は、次の3種類のアドレスについて知っておくと役に立ちます。

ユニキャスト
: このタイプのアドレスは、1つのネットワークインタフェースだけに関連付けられます。このようなアドレスを持つパケットは、1つの宛先にのみ配信されます。したがって、ユニキャストアドレスは、パケットをローカルネットワークまたはインターネット上の個々のホストに転送する場合に使用します。

マルチキャスト
: このタイプのアドレスは、ネットワークインタフェースのグループに関連します。このようなアドレスを持つパケットは、そのグループに属するすべての宛先に配信されます。マルチキャストアドレスは、主に、特定のネットワークサービスが、相手を特定のグループに属するホストに絞って通信を行う場合に使用されます。

エニーキャスト
: このタイプのアドレスは、インタフェースのグループに関連します。このようなアドレスを持つパケットは、基盤となるルーティングプロトコルの原則に従い、送信側に最も近いグループのメンバに配信されます。エニーキャストアドレスは、特定のネットワーク領域で特定のサービスを提供するサーバについて、ホストが情報を得られるようにするために使用します。同じタイプのすべてのサーバは、エニキャストアドレスが同じになります。ホストがサービスを要求すると、ルーティングプロトコルによって最も近い場所にあるサーバが判断され、そのサーバが応答します。何らかの理由でこのサーバが応答できない場合、プロトコルが自動的に2番目のサーバを選択し、それが失敗した場合は3番目、4番目が選択されます。

IPv6アドレスは、4桁の英数字が入った8つのフィールドで構成され、それぞれのフィールドが16進数表記の16ビットを表します。各フィールドは、コロン(:)で区切られます。各フィールドで先頭の0は省略できますが、数字の間にある0や末尾の0は省略できません。もう1つの規則として、0のバイトが5つ以上連続する場合は、まとめて2つのコロン(::)で表すことができます。ただし、アドレスごとに::は1回しか使用できません。この省略表記の例については、例21.3「IPv6アドレスの例」 (298ページ)を参照してください。この3行はすべて同じアドレスを表します。

例 21.3　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。に示すアドレスには、最初の64ビットがアドレスのネットワーク部分を構成する情報、最後の64ビットにホスト部分を構成する情報が入っています。例21.4「プレフィクスの長さを指定したIPv6アドレス」 (299ページ)言い換えると、64は、ネットマスクに64個の1ビット値が左から埋められていることを意味します。IPv4と同様、IPアドレスとネットマスクのANDをとることにより、ホストが同じサブネットワークにあるかそうでないかを判定します。

例 21.4 *プレフィクスの長さを指定したIPv6アドレス*

```
fe80::10:1000:1a4/64
```

IPv6は、事前に定義された複数タイプのプレフィクスを認識します。に、一部のプレフィクスタイプを示します。表21.4「IPv6のプレフィクス」 (299 ページ)

表 21.4 *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(実稼動品質のアドレス空間)と

プレフィクス(16進)	定義
	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(21.2.3項 「IPv4とIPv6の共存」 (303 ページ)を参照)として使用されます。

IPv6にマッピングされたIPv4アドレス
このタイプのアドレスは、IPv6表記で純粋なIPv4アドレスを指定します。

ローカルアドレス
ローカルで使用するアドレスのタイプには、以下の2種類があります。

リンクローカル
リンクローカル このタイプのアドレスは、ローカルのサブネットワークでのみ使用できます。このタイプの送信元または宛先アドレスを持つパケットをインターネットまたは他のサブネットワークにルーティングしてはなりません。これらのアドレスは、特別なプレフィクス(fe80::/10)とネットワークカードのインタフェースID、およびヌルバイトからなる中間部分からなります。このタイプのアドレスは、自動環境設定のとき、同じサブネットワークに属する他のホストと通信するために使用されます。

サイトローカル
: このタイプのアドレスを持つパケットは、他のサブネットワークにはルーティングできますが、それより広いインターネットにはルーティングしてはなりません。つまり、組織自体のネットワークの内側だけで使用するよう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。

21.2.3 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(21.2.2項 「アドレスのタイプと構造」 (297 ページ)を参照)。

ワールドワイドなIPv4ネットワークと隔離されているIPv6ホストは、トンネルを使って通信を行うことができます。IPv6パケットをIPv4パケットにカプセル化すれば、それをIPv4ネットワークに送ることができます。2つのIPv4ホスト間のこのような接続を*トンネル*と呼びます。これを行うには、パケットにIPv6の宛先アドレス(または対応するプレフィクス)とともに、トンネルの受信側にあるリモートホストのIPv4アドレスも含める必要があります。基本的なトンネルは、ホストの管理者間が合意すれば、手動で設定が可能です。これは、*静的トンネリング*とも呼ばれます。

ただし、静的トンネルの環境設定とメンテナンスは、あまりに手間がかかるので、多くの場合、日常の通信には向きません。そこで、IPv6は、*動的トンネリング*を実現する3つの異なる方法を提供しています。

6over4
: IPv6パケットが自動的にIPv4パケットとしてカプセル化され、マルチキャスト対応のIPv4ネットワークによって送信されます。IPv6は、ネットワーク全体(インターネット)を巨大なLAN (local area network)だと思い込んで動作することになります。これにより、IPv4トンネルの着信側の端を自動的に判定できます。ただし、この方法は拡張性に欠けているだけではなく、IPマルチキャストがインターネット上で広く普及しているとはいえないという事実も障害となります。したがってこの解決方法を採用できるのは、マルチキャストが利用できる小規模な企業内ネットワークだけです。この方式の仕様は、RFC 2529に規定されています。

6to4
: この方式では、IPv6アドレスからIPv4アドレスを自動的に生成することで、隔離されたIPv6ホストがIPv4ネットワーク経由で通信できるようにします。しかし、隔離されたIPv6ホストとインターネットの間の通信に関し

て、多くの問題が報告されています。この方式は、RFC 3056で規定されています。

IPv6トンネルブローカ
: この方式は、IPv6ホスト専用のトンネルを提供する特殊なサーバに依存します。この方式は、RFC 3053で規定されています。

21.2.4 IPv6の設定

IPv6を設定するには、通常、個々のワークステーションの設定を変更する必要はありません。IPv6は、デフォルトで有効になっています。インストール時にネットワーク設定ステップで、これを無効にすることができます。項「ネットワーク設定」 (第6章 *YaSTによるインストール*, ↑*導入ガイド*)を参照してください。インストール済みシステムでIPv6を有効または無効にするには、YaSTの［*Network Settings*］モジュールを使用します。［*グローバルオプション*］タブで、必要に応じて［*IPv6を有効にする*］オプションをオン/オフします。次回のリブートまで一時的に有効にするには、`modprobe -i ipv6`と`root`として入力します。ipv6モジュールがロードされた後にアンロードすることは、基本的に不可能です。

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/quaggaを使用してアドレスとルーティングの両方を自動設定することもできます。

`/etc/sysconfig/network`ファイルを使用して各種のトンネルを設定する方法については、ifcfg-tunnel (5)のマニュアルページを参照してください。

21.2.5 詳細情報

ここでの概要は、IPv6に関する情報を網羅しているわけではありません。IPv6の詳細については、次のオンラインドキュメントや書籍を参照してください。

http://www.ipv6.org/
: IPv6のあらゆる情報にここからリンクできます。

http://www.ipv6day.org
: 独自のIPv6ネットワークを開始するには、すべての情報が必要です。

http://www.ipv6-to-standard.org/
: IPv6対応製品のリスト。

http://www.bieringer.de/linux/IPv6/
: Linux IPv6-HOWTOと多くの関連トピックへのリンクが用意されています。

RFC2640
: 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。

21.3 ネームレゾリューション

DNSはIPアドレスに1つまたは複数のホスト名を割り当てるとともに、ホスト名をIPアドレスに割り当てます。Linuxでは、この変換は通常、bindという特別な種類のソフトウェアによって行われます。また、この変換を行うマシンをネームサーバと呼びます。ホスト名は、その名前構成要素がピリオド(.)で区切られた階層システムを構成しています。しかしながら名前の階層構造は、先に述べたIPアドレスの階層構造とは無関係です。

`hostname.domain`形式で書かれた完全な名前(たとえば、`jupiter.example.com`)について検討してみましょう。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 Enterprise Serverによるネームサーバアクセスの設定については、21.4.1.4項 「ホスト名とDNSの設定」 (318 ページ)に説明があります。独自のネームサーバの設定については、第24章 *ドメインネームシステム* (375 ページ)に説明があります。

whoisプロトコルは、DNSと密接な関係があります。このプログラムを使用すると、特定のドメインの登録者名をすぐに検索できます。

注記: MDNSおよび.localドメイン名

.localトップレベルドメインは、リゾルバではリンクローカルドメインとして処理されます。DNS要求は通常のDNS要求ではなく、マルチキャスト要求として送信されます。ネームサーバ構成で.localドメインをすでに使用

している場合は、このオプションを/etc/host.confでオフに変更する必要があります。詳細については、host.confのマニュアルページを参照してください。

インストール中にMDNSをオフにするには、nomdns=1をブートパラメータとして使用してください。

マルチキャストDNSの詳細は、http://www.multicastdns.orgを参照してください。

21.4 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、21.6項「ネットワークの手動環境設定」(335 ページ)を参照してください。

NetworkManagerがデフォルトでアクティブなSUSE Linux Enterprise Desktop上では、すべてのネットワークカードが設定されます。NetworkManagerがアクティブでない場合は、リンクアップしている(つまり、ネットワークケーブルが接続している)最初のインタフェースだけが自動的に設定されます。インストール済みのシステムには、付加的なハードウェアを設定することができます。以下のセクションでは、SUSE Linux Enterprise Server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。

ヒント: IBM System z: ホットプラグ対応ネットワークカード

IBM System zプラットフォームでは、ホットプラグ可能なネットワークカードがサポートされていますが、DHCPを介したネットワークの自動統合は(PCの場合とは異なり)サポートされていません。検出後はインタフェースを手動で設定してください。

21.4.1 YaSTでのネットワークカードの設定

YaSTで無線/有線ネットワークカードを設定するには、［*ネットワークデバイス*］>［*ネットワーク設定*］の順に選択します。モジュールの開始後に、YaSTは［*ネットワーク設定*］ダイアログを表示します。ダイアログには［*グローバルオプション*］、［*概要*］、［*ホスト名/DNS*］、および［*ルーティング*］の4つのタブがあります。

［*グローバルオプション*］タブでは、NetworkManager、IPv6、一般的なDHCPオプションの使用など、一般的なネットワークオプションを設定できます。詳細については、21.4.1.1項 「グローバルネットワークオプションの設定」 (309 ページ)を参照してください。

［*概要*］タブには、インストールされたネットワークインタフェースと環境設定に関する情報が含まれています。正しく検出されたネットワークカードの名前が表示されます。このダイアログでは、手動で新しいカードを設定し、それらの設定内容を削除または変更できます。自動検出されなかったカードを手動で設定する場合は、21.4.1.3項 「検出されないネットワークカードの設定」 (317 ページ)を参照してください。すでに設定済みのカードの設定を変更する場合については、21.4.1.2項 「ネットワークカードの設定の変更」 (310 ページ)を参照してください。

［*ホスト名/DNS*］タブでは、マシンのホスト名を設定し、使用サーバに名前を付けることができます。詳細については、21.4.1.4項 「ホスト名とDNSの設定」 (318 ページ)を参照してください。

［*ルーティング*］タブは、ルーティングの設定で使用します。詳細については、21.4.1.5項 「ルーティングの設定」 (320 ページ)を参照してください。

図 21.3　ネットワーク設定の実行

21.4.1.1 グローバルネットワークオプションの設定

YaST［*ネットワーク設定*］モジュールの［*グローバルオプション*］タブを使用して、NetworkManager、IPv6およびDHCPのクライアントオプションの使用など、重要なグローバルネットワークオプションを設定できます。この設定は、すべてのネットワークインタフェースに適用されます。

［*ネットワークのセットアップ方法*］では、ネットワーク接続を管理する方法を選択します。NetworkManagerデスクトップアプレットですべてのインタフェースの接続を管理する場合は、［*NetworkManagerでユーザを制御*］を選択します。このオプションは、複数の有線ネットワークおよび無線ネットワーク間の切り替えに適しています。デスクトップ環境(GNOMEまたはKDE)を実行しない場合、またはコンピュータがXenサーバ(仮想システム)であるか、ネットワーク内でDHCPやDNSなどのネットワークサービスを提供する場合は、［*ifupを使用した従来の方法*］を使用します。NetworkManagerを使用する場合は、`nm-applet`を使用して、ネットワークオプションを設定する必要があります。［*ネットワーク設定*］モジュールのタブである［*概要*］、［*ホスト名/DNS*］、および［*ルーティング*］は無効になります。NetworkManagerの詳細については、第26章 *NetworkManagerの使用* (419 ページ)を参照してください。

［*IPv6プロトコル設定*］で、IPv6プロトコルを使用するかどうかを選択します。IPv4とともにIPv6を使用できます。デフォルトでは、IPv6が選択されています。ただし、IPv6プロトコルを使用しないネットワークでは、IPv6プロトコルを無効にした方が応答時間がより短くなる場合があります。IPv6を無効にする場合は、［*IPv6を有効にする*］オプションをオフにします。これにより、IPv6のカーネルモジュールの自動ロードが無効になります。これは、再起動後に適用されます。

［*DHCPクライアントオプション*］では、DHCPクライアントのオプションを設定します。 常にその応答をブロードキャストするようにサーバに要求することをDHCPクライアントに求める場合は、［*ブロードキャスト応答の要求*］をオンにします。この機能は、マシンが異なるネットワーク間を移動する場合に必要になることがあります。［*DHCPクライアントID*］は、単一ネットワーク上の各DHCPクライアントで異なる必要があります。空白のままにした場合は、デフォルトでネットワークインタフェースのハードウェアアドレスになります。ただし、同じネットワークインタフェース、したがって同じハードウェアアドレスを使用して複数の仮想マシンを実行している場合は、ここで自由形式の固有識別子を指定します。

［*送信するホスト名*］では、dhcpcdがDHCPサーバにメッセージを送信するときに、ホスト名オプションフィールドで使用される文字列を指定します。一部のDHCPサーバでは、このホスト名(ダイナミックDNS)に応じて、ネームサーバゾーン(順レコードおよび逆レコード)を更新します。また一部のDHCPサーバでは、クライアントからのDHCPメッセージで、［*送信するホスト名*］オプションフィールドに特定の文字列が含まれることが必要です。現在のホスト名(`/etc/HOSTNAME`で定義されたホスト名)を送信する場合は、［自動］のままにします。ホスト名を送信しない場合は、このオプションフィールドを空のままにします。DHCPからの情報に従ったデフォルトのルートを変更しない場合は、［*Change Default Route via DHCP*］をオフにします。

21.4.1.2 ネットワークカードの設定の変更

ネットワークカードの設定を変更するには、YaSTの［*ネットワーク設定*］>［*概要*］で検出されたカードのリストから目的のカードを選択し、［*編集*］をクリックします。［*ネットワークカードの設定*］ダイアログが表示されます。このダイアログの［*一般*］、［*アドレス*］、および［*ハードウェア*］タブを使用してカードの設定を変更します。無線カードの設定については、18.5項 「YaSTでの設定」 (250 ページ)を参照してください。

IPアドレスの設定

［*Network Card Setup*］ダイアログの［アドレス］タブで、ネットワークカードのIPアドレス、またはそのIPアドレスの決定方法を設定できます。IPv4およびIPv6の両アドレスがサポートされます。ネットワークカードは、［*IPアドレスなし*］(ボンドデバイスで有用)の場合や、［*静的に割り当てられたIPアドレス*］(IPv4またはIPv6)、あるいは［*DHCP*］または［*Zeroconf*］のいずれかまたは両方を経由して割り当てられる［*動的アドレス*］を持つ場合もあります。

［*Dynamic Address*］を使用する場合は、［*DHCP Version 4 Only*］(IPv4の場合)、［*DHCP Version 6 Only*］(IPv6の場合)、または［*DHCP Both Version 4 and 6*］のいずれを使用するかを選択します。

可能であれば、インストール時に利用可能なリンクを持つ最初のネットワークカードがDHCPによる自動アドレス設定を使用するように自動的に設定されます。NetworkManagerがデフォルトでアクティブなSUSE Linux Enterprise Desktop上では、すべてのネットワークカードが設定されます。

注記: **IBM System zとDHCP**

IBM System zプラットフォームでは、DHCPベースのアドレス設定はMACアドレスを持つネットワークカードの場合にのみサポートされます。これに該当するのは、OSAカードおよびOSA Expressカードだけです。

DSL回線を使用していてISP(Internet Service Provider)からスタティックIPが割り当てられていない場合も、DHCPを使用する必要があります。DHCPを使用することを選択する場合は、YaSTネットワークカード設定モジュールの［*ネットワーク設定*］ダイアログにある［*グローバルオプション*］タブの［*DHCPクライアントオプション*］で詳細を設定します。 常にその応答をブロードキャストするようにサーバにDHCPクライアントが要求するかどうかを［*ブロードキャスト応答の要求*］で指定します。このオプションは、マシンがネットワーク間を移動するモバイルクライアントである場合に必要になることがあります。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［*DHCPクライアントID*］が必要になります。

DHCPは、クライアント設定には適していますが、サーバ設定には適していません。静的なIPアドレスを設定するには、以下の手順に従ってください。

1 YaSTネットワークカード設定モジュールの［*概要*］タブの検出されたカード一覧から目的のカードを選択し、［*編集*］をクリックします。

2 ［*アドレス*］タブで、［*Statically Assigned IP Address*］を選択します。

3 ［*IP*アドレス］を入力します。IPv4およびIPv6の両アドレスを使用できます。［サブネットマスク］にネットワークマスクを入力します。IPv6アドレスが使用されている場合は、フォーマット/64のプレフィックス長に対する［サブネットマスク］を使用します。

オプションで、このアドレスの完全修飾［ホスト名］を入力できます。このホスト名は、/etc/hosts設定ファイルに書き込まれます。

4 ［次へ］をクリックします。

5 環境設定を有効にするには、［*OK*］をクリックします。

静的アドレスを使用する場合、ネームサーバとデフォルトゲートウェイは、自動的には設定されません。ネームサーバを設定するには、21.4.1.4項「ホスト名とDNSの設定」(318 ページ)に従って手順を進めます。ゲートウェイを設定するには、21.4.1.5項 「ルーティングの設定」 (320 ページ)に従って手順を進めます。

エイリアスの設定

1台のネットワークデバイスに、複数のIPアドレスを割り当てることをできます。追加するIPアドレスは、エイリアスと呼ばれます。

注記: エイリアスは互換機能です

これらのいわゆるエイリアスresp. labelsは、IPv4でのみ動作します。IPv6では、無視されます。iproute2ネットワークインタフェースを使用する場合、1つ以上のアドレスを持つことができます。

YaSTを使用してネットワークカードにエイリアスを設定するには、次の手順に従います。

1 YaSTネットワークカード設定モジュールの［*概要*］タブの検出されたカード一覧から目的のカードを選択し、［*編集*］をクリックします。

2 ［アドレス］>［*追加アドレス*］タブで、［*追加*］をクリックします。

3 ［エイリアス名］、［*IP*アドレス］、および［ネットマスク］に適切な値を入力します。エイリアス名にはインタフェースを含めないでください。

4 ［*OK*］をクリックします。

5 ［*次へ*］をクリックします。

6 環境設定を有効にするには、［*OK*］をクリックします。

デバイス名およびUdevルールの変更

ネットワークカードのデバイス名が使用されている場合、ネットワークカードのデバイス名を変更できます。また、ハードウェア(MAC)アドレスまたはバスIDを介してudevによりネットワークカードを識別するかどうかを選択できます。大型のサーバでは、カードのホットスワッピングを容易にするために後者のオプションが適しています。YaSTを使ってこうしたオプションを設定するには、次の手順に従います。

1 YaST［*ネットワーク設定*］モジュールの［*概要*］タブの検出されたカード一覧から目的のカードを選択し、［*編集*］をクリックします。

2 ［ハードウェア］タブを開きます。現在のデバイス名が［*Udevルール*］に表示されます。［*変更*］をクリックします。

3 udevで［*MACアドレス*］または［*バスID*］によりカードを識別するかどうかを選択します。カードの現在のMACアドレスおよびバスIDがダイアログに表示されます。

4 デバイス名を変更するには、［*Change Device Name*］オプションをオンにし、名前を編集します。

5 ［*OK*］および［*次へ*］をクリックします。

6 環境設定を有効にするには、［*OK*］をクリックします。

ネットワークカードカーネルドライバの変更

一部のネットワークカードには、複数のカーネルドライバを使用できます。カードがすでに設定されている場合は、YaSTで利用可能で適切なドライバのリストから、使用するカーネルドライバを選択できます。また、カーネルドライバのオプションを指定することもできます。YaSTを使ってこうしたオプションを設定するには、次の手順に従います。

1 YaSTネットワークカード設定モジュールの［*概要*］タブの検出されたカード一覧から目的のカードを選択し、［*編集*］をクリックします。

2 ［ハードウェア］タブを開きます。

3 ［*モジュール名*］で、使用するカーネルドライバを選択します。選択したドライバのオプションを、［*オプション*］に`option=value`の形式で入力します。他にもオプションを使用する場合は、スペースで区切る必要があります。

4 ［*OK*］および［次へ］をクリックします。

5 環境設定を有効にするには、［*OK*］をクリックします。

ネットワークデバイスの有効化

ifupを使った従来の方法を使用している場合、デバイスをブート時、ケーブル接続時、カード検出時、または手動で起動するように設定したり、起動しないように設定することができます。デバイスの起動方法を変更するには、以下の手順に従ってください。

1 YaSTで、［*ネットワークデバイス*］>［*ネットワーク設定*］で検出されたカードの一覧からカードを選択し、［*編集*］をクリックします。

2 ［*一般*］タブの［*デバイスの起動*］から、適切な項目を選択します。

システムブート中にデバイスを起動するには、［*ブート時*］を選択します。［*ケーブル接続時*］では、インタフェースで物理接続が存在するかどうかが監視されます。［*ホットプラグ時*］では、インタフェースは可能な限り早急に設定されます。これは、［*ブート時*］オプションに似ていますが、インタフェースがブート時に存在しない場合にエラーが発生しない点のみが異なります。［*ifup*］でインタフェースを手動で制御する場合は、［手

動］を選択します。デバイスを全く起動しない場合は、［*起動しない*］を選択します。［*NFSrootオン*］は［*ブート時*］に似ていますが、インタフェースは`rcnetwork stop`コマンドではシャットダウンしません。このオプションは、nfsまたはiscsiのルートファイルシステムを使用する場合に選択します。

3 ［*次へ*］をクリックします。

4 環境設定を有効にするには、［*OK*］をクリックします。

通常、システム管理者のみがネットワークインタフェースを有効および無効にできます。KInternetを利用して誰でもこのインタフェースを有効化できるようにしたい場合は、［*Kinternetを利用してroot以外のユーザにもデバイス操作を許す*］を選択します。

最大転送単位サイズの設定

インタフェースの最大転送単位(MTU)を設定できます。MTUでは、最大許容パケットサイズ(バイト)を参照します。MTUが大きいと、帯域幅の効率が高くなります。ただし、パケットが大きくなると、低速なインタフェースの処理がしばらく阻止され、以降のパケットの遅延が増加する場合があります。

1 YaSTで、［*ネットワークデバイス*］>［*ネットワーク設定*］で検出されたカードの一覧からカードを選択し、［*編集*］をクリックします。

2 ［*一般*］タブの［*Set MTU*］リストから、適切な項目を選択します。

3 ［*次へ*］をクリックします。

4 環境設定を有効にするには、［*OK*］をクリックします。

ファイアウォールの設定

項 「Configuring the Firewall with YaST」 (第15章 *Masquerading and Firewalls*, ↑*Security Guide (セキュリティガイド)*)で説明しているような詳細なファイアウォール設定を行わずに、デバイスに基本的なファイアウォールを設定することができます。次の手順に従います。

1 YaST［*ネットワークデバイス*］>［*ネットワーク設定*］モジュールを開きます。［*概要*］タブで、検出されたカードの一覧からカードを選択し、［*編集*］をクリックします。

2 ［*ネットワーク設定*］ダイアログの［*一般*］タブを表示します。

3 インタフェースを割り当てるファイアウォールゾーンを指定します。次のオプションを指定できます。

Firewall Disabled
: このオプションは、ファイアウォールが無効であり、ファイアウォールがまったく実行しない場合にのみ利用可能です。コンピュータが、外部ファイアウォールにより保護されている、より規模の大きいネットワークに接続している場合にのみ、このオプションを使用してください。

自動割り当てゾーン
: このオプションは、ファイアウォールが有効になっている場合のみ、利用できます。ファイアウォールが実行中であり、インタフェースがファイアウォールゾーンに自動的に割り当てられます。こうしたインタフェースには、anyキーワードを含むゾーンまたは外部ゾーンが使用されます。

内部ゾーン(未保護)
: ファイアウォールを実行しますが、このインタフェースを保護するルールは使いません。コンピュータが、外部ファイアウォールにより保護されている、より規模の大きいネットワークに接続している場合に、このオプションを使用してください。また、マシンに追加ネットワークインタフェースが存在する場合、内部ネットワークに接続するインタフェースで使用できます。

非武装地帯(DMZ)
: 非武装地帯ゾーンは、内部ネットワークと(悪意のある)インターネットとの中間にあたるゾーンです。このゾーンに割り当てられたホストは、内部ネットワークおよびインターネットからアクセスされますが、ホストから内部ネットワークにアクセスすることはできません。

外部ゾーン
: このインタフェースでファイアウォールを実行し、(危険な可能性のある)他のネットワークトラフィックからインタフェースを保護します。これはデフォルトの設定です。

4 ［次へ］をクリックします。

5 環境設定を有効にするには、［*OK*］をクリックします。

21.4.1.3 検出されないネットワークカードの設定

カードは適切に検出されない場合があります。このような場合、検出されたカードのリストに、そのカードは表示されません。システムにそのカード用のドライバが間違いなく含まれている場合は、そのようなカードを手動で設定することができます。特殊なネットワークデバイスタイプ(ブリッジ、ボンド、TUN、TAPなど)も設定できます。未検出のネットワークカードまたは特殊なデバイスを設定するには、次の手順に従います。

1 YaSTの［*ネットワークデバイス*］>［*ネットワーク設定*］>［*概要*］ダイアログで［*追加*］をクリックします。

2 ［ハードウェア］ダイアログで、使用可能なオプションからインタフェースの［*デバイスの型*］と［*環境設定名*］を設定します。ネットワークカードが、PCMCIAデバイスかUSBデバイスの場合、それぞれのチェックボックスを選択して、［次へ］をクリックしダイアログを終了します。それ以外の方法では、必要に応じて、カードとその［*オプション*］で使用されるカーネルの［*モジュール名*］を定義できます。

   ［*Ethtoolオプション*］では、インタフェースの`ifup`により使用される`ethtool`オプションを設定できます。使用可能なオプションについては、`ethtool`マニュアルページを参照してください。オプション文字列が`-`で始まる場合(たとえば`-K` *`interface_name`* `rx on`)、文字列内の2番目の単語が現在のインタフェースの名前に置換されます。それ以外の場合(たとえば`autoneg off speed 10`)、`-s` *`interface_name`*の前に`ifup`が追加されます。

3 ［次へ］をクリックします。

4 ［*一般*］、［*アドレス*］、および［*ハードウェア*］タブで、インタフェースのIPアドレス、デバイス起動方法、ファイアウォールゾーンなどの必要なオプションを設定します。環境設定オプションの詳細については、21.4.1.2 項「ネットワークカードの設定の変更」(310ページ)を参照してください。

5 インタフェースのデバイスタイプとして、［*ワイヤレス*］を選択した場合は、次のダイアログで無線接続の設定を行います。無線デバイスの設定方法の詳細は、第18章 *無線LAN* (245 ページ)を参照してください。

6 ［*次へ*］をクリックします。

7 ネットワーク設定を有効にするには、［*OK*］をクリックします。

21.4.1.4 ホスト名とDNSの設定

有線ネットワークカードがすでに利用できる状態で、インストール時にネットワーク設定を変更しなかった場合、コンピュータのホスト名が自動的に生成され、DHCPが有効になります。また、ホストがネットワークに参加するために必要なネームサービス情報も自動的に生成されます。ネットワークアドレス設定にDHCPを使用している場合は、ドメインネームサーバのリストは自動的に記入されます。静的設定を利用する場合は、これらの項目を手動で設定してください。

コンピュータ名を変更し、ネームサーバの検索リストを修正するには、以下の手順に従ってください。

1 YaST内の［*ネットワークデバイス*］モジュールの［*ネットワーク設定*］>［*ホスト名/DNS*］タブに移動します。

2 ［*ホスト名*］にホスト名を入力し、必要に応じて［*ドメイン名*］にドメイン名を入力します。マシンがメールサーバである場合、ドメインは特に重要です。ホスト名はグローバルであり、すべての設定ネットワークインタフェースに適用されることに注意してください。

IPアドレスを取得するためにDHCPを使用している場合、DHCPによりコンピュータのホスト名が自動的に設定されます。異なるネットワークに接続する場合は、異なるホスト名が割り当てられることがあり、ランタイムにホスト名が変更されるとグラフィックデスクトップが混同される可能性があるので、この機能を無効にした方が良い場合もあります。DHCPを使用

したIPアドレスの取得を無効にするには、［*DHCPでホスト名を変更する*］をオフにします。

［*ホスト名をループバックIPに割り当てる*］では、ホスト名を/etc/hosts内の127.0.0.2(loopback)IPアドレスに関連付けます。アクティブネットワークが存在しないときでも常に解決可能なホスト名を必要とする場合に有用なオプションです。

3 ［*Modify DNS Configuration*］では、DNS設定(ネームサーバ、検索リスト、/etc/resolv.confファイルの内容)を変更する方法を選択します。

［*Use Default Policy*］オプションを選択した場合、(DHCPクライアントまたはNetworkManagerから)動的に取得されたデータと、(YaSTまたは設定ファイルで)静的に定義されたデータをマージするnetconfigスクリプトにより設定が処理されます。ほとんどの場合、デフォルトのポリシーで十分です。

［*手動でのみ*］オプションを選択した場合、netconfigでは/etc/resolv.confファイルを変更できません。ただし、このファイルは手動で編集できます。

［*Custom Policy*］オプションを選択した場合、マージポリシーを定義する［*Custom Policy Rule*］文字列を指定する必要があります。この文字列は、設定の有効なソースとみなされるインタフェース名のカンマで区切られたリストから構成されます。完全なインタフェース名を除いて、複数のインタフェースに一致する基本的なワイルドカードを使用することもできます。たとえばeth* ppp?は、先頭がethであり、以降にppp0-ppp9を含むすべてのインタフェースが対象になります。/etc/sysconfig/network/configファイルで定義された静的な設定を適用する方法を示す次の2つの特別なポリシー値が存在します。

STATIC
: 静的な設定は、動的な設定とマージされる必要があります。

STATIC_FALLBACK
: 静的な設定は、動的設定が利用できない場合のみ使用されます。

詳細については、man 8 netconfigを参照してください。

4 ［ネームサーバ］および［*ドメイン検索*］リストに入力します。ネームサーバは、ホスト名ではなく、192.168.1.116などのIPアドレスにより指定する必要があります。［*ドメイン検索*］タブで指定した名前は、ドメインが指定されていないホスト名の解決のために使用されるドメイン名です。複数の［*ドメイン検索*］を使用する場合は、カンマまたは空白でドメインを区切ります。

5 環境設定を有効にするには、［*OK*］をクリックします。

コマンドラインからYaSTを使用してホスト名を編集することもできます。YaSTによる変更はすぐに有効になります(`/etc/HOSTNAME`ファイルを手動で編集する場合はすぐに有効にはなりません)。ホスト名を変更するには、次のコマンドを実行します。

```
yast dns edit hostname=hostname
```

ネームサーバを変更するには、次のコマンドを実行します。

```
yast dns edit nameserver1=192.168.1.116
yast dns edit nameserver2=192.168.1.116
yast dns edit nameserver3=192.168.1.116
```

21.4.1.5 ルーティングの設定

コンピュータを他のコンピュータやネットワークと通信させるには、ネットワークトラフィックが正しい経路を通過するように、ルーティング情報を設定する必要があります。DHCPを使用している場合、この情報は自動的に設定されます。静的アドレスを使用する場合は、このデータを手作業で追加する必要があります。

1 YaSTで、［*ネットワーク設定*］>［*ルーティング*］の順に移動します。

2 ［*デフォルトゲートウェイ*］のIPアドレス(必要に応じてIPv4およびIPv6)を入力します。デフォルトゲートウェイは、すべての宛先に一致しますが、必要なアドレスに一致する他のエントリが存在する場合は、デフォルトルートの代わりにそのエントリが使用されます。

3 ［*ルーティングテーブル*］には、さらに追加エントリを入力できます。［*宛先*］のネットワークIPアドレス、［*ゲートウェイ*］のIPアドレス、および［*ネットマスク*］を入力します。定義されたネットワークにトラフィックがルーティングされる［*デバイス*］を選択します(マイナス記号はデバイス

を表わします)。このいずれかの値を省略する場合は、マイナス記号(–)を使用します。デフォルトゲートウェイをテーブルに入力するには、［*宛先*］フィールドを`default`のままにします。

注記

追加のデフォルトルートが使用されている場合、より高い優先度を持つルートを決定するためのメトリックオプションを指定できます。メトリックオプションを指定するには、［*オプション*］に`- metric`*番号*を入力します。最も高いメトリックを持つルートがデフォルトとして使用されます。ネットワークデバイスが切断している場合は、そのルートが削除され、次のルートが使用されます。ただし、現在のカーネルは静的なルーティングでメトリックを使用せず、multipathdなどのルーティングデーモンのみがメトリックを使用します。

---

4 システムがルータである場合は、［*ネットワーク設定*］で［*IP転送を有効にする*］オプションをオンにします。

5 環境設定を有効にするには、［*OK*］をクリックします。

21.4.2 モデム

ヒント: IBM System z:モデム

このタイプのハードウェアの設定は、IBM System zプラットフォームではサポートされていません。

YaSTコントロールセンターで、［*ネットワークデバイス*］>［モデム］の順に選択して、モデム設定にアクセスします。モデムが自動的に検出されなかった場合は、［*モデムデバイス*］タブに移動し、手動設定用のダイアログを［*追加*］のクリックで開きます。［*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。

ヒント: CDMAおよびGPRSモデム

YaSTの［モデム］モジュールを使って、通常のモデムの設定と同様に、サポートするCDMAおよびGPRSモデムを設定します。

図 21.4 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、［*Kinternetを利用してroot以外のユーザにもデバイス操作を許す*］を有効にします。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。インターネットに定期的にデータを要求するプログラムが存在するために、インターネット接続が低コストである場合にのみこの機能を使用します。

［*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。

［*Automatically Reconnect*］
　このオプションが有効である場合、障害の後で接続が自動的に再確立されます。

［*ドライブを無視する*］
　このオプションは、ダイヤルアップサーバからのプロンプトの検出を無効にします。接続の構成が低速であるか、まったく機能しない場合は、このオプションを試みてください。

［*外部ファイアウォールインタフェース*］
　このオプションを選択すると、ファイアウォールが有効になり、インタフェースが外部として設定されます。このようにして、インターネット接続時に外部からの攻撃から保護されます。

［*アイドルタイムアウト(秒)*］
　このオプションでは、ネットワークがアイドル状態になってからモデムが自動的に切断されるまでの時間を指定します。

［*IP Details(IP詳細設定)*］
このオプションを選択すると、アドレス設定ダイアログが開きます。ISPからホストにダイナミックIPアドレスが割り当てられていない場合は、［*ダイナミックIPアドレス*］を無効にして、ホストのローカルIPアドレスとリモートIPアドレスを入力します。この情報については、ISPにお問い合わせください。［*デフォルトルート*］は有効なままにし、［*OK*］を選択してダイアログを閉じます。

［*次へ*］を選択すると、元のダイアログに戻り、モデム設定の概要が表示されます。［*OK*］をクリックしてこのダイアログを閉じます。

21.4.3 ISDN

ヒント: IBM System z: ISDN

このタイプのハードウェアの設定は、IBM System zプラットフォームではサポートされていません。

このモジュールは、システムの1つ以上のISDNカードを設定します。YaSTによってISDNカードが検出されなかった場合は、［*ISDNデバイス*］タブで［*追加*］をクリックして手動で選択してください。複数のインタフェースを設定することも可能ですが、1つのインタフェースに複数のISPを設定することも可能です。以降のダイアログでは、カードが正しく機能するために必要なISDNオプションを設定します。

図 21.5　ISDNの設定

図21.5「ISDNの設定」(325ページ)に示すダイアログでは、使用するプロトコルを選択します。デフォルトは、［*Euro-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［*市外局番*］と［*ダイヤルプレフィックス*］を入力します。すべてのISDNトラフィックをログに記録しない場合は、［*ISDN記録を開始する*］オプションをオフにします。

［*デバイスの起動*］は、ISDNインタフェースの起動方法を定義します。［*ブート時*］を選択すると、システムブート時にISDNドライバが毎回初期化されます。［*Manually*］を選択した場合は、rootとしてrcisdn startコマンドを実行して、ISDNドライバをロードする必要があります。［*On Hotplug*］は、PCMCIAやUSBデバイスに使用します。デバイスを装着したときにドライバがロードされます。これらの設定が完了したら、［*OK*］を選択します。

次のダイアログでは、ISDNカードのインタフェースタイプを指定し、既存のインタフェースにISPを追加します。インタフェースタイプには、SyncPPPまたはRawIPのどちらかを指定できますが、たいていのISPは、SyncPPPモードで運用しています。このモードについては後述します。

図 21.6　ISDNインタフェースの設定

［*自分の電話番号*］に入力する番号は、次の設定によって異なります。

電話線引出口に直接接続されたISDNカード
: 標準のISDN回線では、3つの電話番号を使用できます(MSN(multiple subscriber number)と呼ばれる)。加入者によっては、最大10個まである場合もあります。これらの電話番号の1つをここに入力します。ただし、市外局番は入力しないでください。間違った番号を入力すると、お使いのISDN回線に付与された最初のMSNが、電話交換手によって自動的に使用されます。

PBX ()に接続されたISDNカード PBX
: 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、［*外部ファイアウォールインタフェース*］と［*ファイアウォールの再起動*］を選択して、使用している回線でファイアウォールを有効にします。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、［*Enable Device Control for Non-root User via Kinternet*］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カンマを挿入しないように注意してください。最後に、ISPから提供されたログインIDとパスワードを入力します。入力したら、［*次へ*］をクリックします。

スタンドアロンワークステーションで［*ダイヤルオンデマンド*］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。これらの設定を有効にするには、［*OK*］を選択します。

21.4.4 ケーブルモデム

ヒント: IBM System z:ケーブルモデム

このタイプのハードウェアの設定は、IBM System zプラットフォームではサポートされていません。

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、［*Dynamic Address*］または［*Statically Assigned IP Address*］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。

21.4.5 DSL

ヒント: IBM System z: DSL

このタイプのハードウェアの設定は、IBM System zプラットフォームではサポートされていません。

DSLデバイスを設定するには、YaSTの［ネットワークデバイス］セクションから［*DSL*］モジュールを選択します。このモジュールは、次のいずれかのプ

ロトコルに基づいてDSLリンクのパラメータを設定する複数のダイアログで構成されます。

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoATM)
- CAPI for ADSL (Fritz Cards)
- ポイントツーポイントトンネリングプロトコル(PPTP)—オーストリア

［*DSLの環境設定の概要*］ダイアログの［*DSLデバイス*］タブに、インストール済みのDSLデバイスのリストが表示されます。DSLデバイスの設定を変更するには、リストでデバイスを選択し、［*編集*］をクリックします。［*追加*］をクリックすることで、新しいDSLデバイスを手動で設定できます。

PPPoEまたはPPTPに基づくDSL接続を設定するには、対応するネットワークカードが正しく設定されている必要があります。ネットワークカードをまだ設定していない場合は、はじめに、［［*ネットワークカードの設定*］を選択してカードを設定してください(21.4.1項 「YaSTでのネットワークカードの設定」 (308ページ)参照)。DSLリンクの場合は、IPアドレスが自動的に割り当てられる場合もありますが、その場合でもDHCPは使用されません。そのため、［*Dynamic Address*］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。

ヒント

［*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。

最初の［DSLの環境設定］ダイアログ(図21.7「DSLの設定」 (330ページ)参照)で、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、［*Activate Device*］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、［*Enable Device Control for Non-root User via Kinternet*］を選択します。

次のダイアログでは、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。

図 21.7　DSLの設定

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。

21.4.6 IBM System z:ネットワークデバイスの設定

IBM System z用のSUSE Linux Enterprise Serverは、さまざまな種類のネットワークインタフェースをサポートしています。これらのインタフェースは、YaSTを使って設定することができます。

21.4.6.1 qeth-hsiデバイス

`qeth-hsi`(Hipersocket)インタフェースをインストール済みのシステムに追加するには、YaSTで［*ネットワークデバイス*］>［*ネットワーク設定*］モジュールを起動します。READデバイスアドレスとして使用するため、［*Hipersocket*］とマークされたデバイスの1つを選択して、［*編集*］をクリックします。読み込みチャネル、書き込みチャネル、および制御チャネルのデバイス番号を入力します(デバイス番号形式の例: `0.0.0600`)。［次へ］をクリックします。［*ネットワークアドレスの設定*］ダイアログで、新しいインタフェースのIPアドレスとネットマスクを指定し、［次へ］と［*OK*］をクリックしてネットワークの設定を終了します。

21.4.6.2 qeth-ethernetデバイス

`qeth-ethernet`(IBM OSA Expressイーサネットカード)インタフェースをインストール済みのシステムに追加するには、YaSTで［*ネットワークデバイス*］>［*ネットワーク設定*］モジュールを起動します。READデバイスアドレスとして使用するため、［*IBM OSA Expressイーサネットカード*］とマークされたデバイスの1つを選択して［*編集*］をクリックします。読み込みチャネル、書き込みチャネル、および制御チャネルのデバイス番号を入力します(デバイス番号形式の例: `0.0.0600`)。必要なポート名、ポート番号(該当する場

合)、および追加オプション(『*Linux for IBM System z: Device Drivers, Features, and Commands*』マニュアル参照http://www.ibm.com/developerworks/linux/linux390/documentation_novell_suse.html)のほか、IPアドレスおよび適切なネットマスクを入力します。［*次へ*］と［*OK*］をクリックして、ネットワークの設定を終了します。

21.4.6.3 ctcデバイス

ctc(IBMパラレルCTCアダプタ)インタフェースをインストール済みのシステムに追加するには、YaSTで［*ネットワークデバイス*］>［*ネットワーク設定*］モジュールを起動します。READデバイスアドレスとして使用する［*IBMパラレルCTCアダプタ*］というマークの付いたデバイスの1つを選択して、［*設定*］をクリックします。お使いのデバイスに合わせて［*デバイス設定*］を選択します(通常は、［*互換モード*］)。自分のIPアドレスとリモートのIPアドレスを指定します。必要に応じて、［*詳細*］>［*詳細設定*］の順に選択してMTUサイズを調整します。［*次へ*］と［*OK*］をクリックして、ネットワークの設定を終了します。

警告

このインタフェースを使用することはお勧めしません。今後のSUSE Linux Enterprise Serverのリリースでは、このインタフェースはサポートされません。

21.4.6.4 lcsデバイス

lcs(IBM OSA-2アダプタ)インタフェースをインストール済みのシステムに追加するには、YaSTで［*ネットワークデバイス*］>［*ネットワーク設定*］モジュールを起動します。［*IBM OSA-2アダプタ*］というマークの付いたデバイスの1つの選択して、［*設定*］をクリックします。ポート番号や他のオプション(『*Linux for IBM System z: Device Drivers, Features, and Commands*』マニュアルを参照、http://www.ibm.com/developerworks/linux/linux390/documentation_novell_suse.html)、IPアドレス、およびネットマスクを入力します。［*次へ*］と［*OK*］をクリックして、ネットワークの設定を終了します。

21.4.6.5 IUCVデバイス

iucv(IUCV)インタフェースをインストール済みのシステムに追加するには、YaSTで［ネットワークデバイス］＞［ネットワーク設定］モジュールを起動します。［*IUCV*］とマークされたデバイスを選択し、［*編集*］をクリックします。IUCVパートナーの名前を入力するように要求されます(［ピア］)。パートナー名(大文字小文字も区別する)を入力して、［次へ］をクリックします。自分の［*IPアドレス*］と、パートナーの［*リモートIPアドレス*］の両方を指定します。必要な場合は、［*Set MTU*］サイズを［*一般*］タブで設定します。［次へ］と［*OK*］をクリックして、ネットワークの設定を終了します。

警告

このインタフェースを使用することはお勧めしません。今後のSUSE Linux Enterprise Serverのリリースでは、このインタフェースはサポートされません。

21.5 NetworkManager

NetworkManagerは、ラップトップなどの携帯用コンピュータのための理想的ソリューションです。NetworkManagerを使用すると、移動時のネットワーク間の切り替えおよびネットワークインタフェースの設定について心配する必要がなくなります。

21.5.1 NetworkManagerおよびifup

ただし、NetworkManagerはすべての場合に適合するソリューションではありません。したがって、依然としてネットワーク接続管理のための伝統的方法(ifup)とNetworkManagerの間で選択を行うことができます。NetworkManagerでネットワーク接続を管理する場合は、26.2項 「NetworkManagerの有効化と無効化」 (420ページ)に従ってYaSTネットワーク設定モジュールでNetworkManagerを有効にし、NetworkManagerでネットワーク接続を設定します。ユースケースのリスト、およびNetworkManagerを設定および使用する方法の詳細については、第26章 *NetworkManagerの使用* (419 ページ)を参照してください。

次に、ifupとNetworkManagerの相違をいくつか示します。

root特権
ネットワークセットアップにNetworkManagerを使用する場合、アプレットを使用するデスクトップ環境内からいつでも簡単にネットワーク接続を切り替え、停止または開始できます。NetworkManagerでは、必要なroot権限なしに、ワイヤレスカード接続の変更および設定もできます。この理由から、NetworkManagerは、モバイルワークステーションに理想的なソリューションと言えます。

ifupを使用する従来の設定では、ユーザ管理デバイスのようなユーザの介入があってもなくても、接続を切り替え、停止または開始する方法がいくつか用意されています。ただし、この場合は常に、ネットワークデバイスを変更または設定するためのroot権限が必要です。このことは、多くの場合、考えられるすべての接続を事前に設定することができないモバイルコンピューティングでは問題になります。

ネットワーク接続のタイプ
従来の設定とNetworkManagerの両方で、無線ネットワーク(WEP、WPA-PSK、およびWPA-Enterpriseアクセスを使用)および有線ネットワーク(DHCPと静的設定を使用)とのネットワーク接続を操作できます。これらの設定では、ダイヤルアップ、DSL、およびVPNによる接続もサポートします。NetworkManagerでは、モバイルブロードバンド(3G)モデムも接続できますが、これは従来の設定では不可能です。

NetworkManagerは、コンピュータが常に最適な接続を使用して接続されるようにします。ネットワークケーブルの接続が誤って切断された場合は、再接続しようとします。また、ワイヤレス接続のリストから信号強度が最高のネットワークを検出し、自動的にそれを使用して接続します。ifupと同じ機能を得るため、多くの設定作業が必要です。

21.5.2 NetworkManagerの機能および環境設定ファイル

NetworkManagerで作成された個別のネットワーク接続設定は、設定プロファイルに保存されます。NetworkManagerまたはYaSTで設定されたシステム接続は、/etc/networkmanager/system-connections/*か、または/etc/sysconfig/network/ifcfg-*に保存されます。すべてのユーザ定義接続は、GNOMEの場合にはGConf、KDEの場合には$HOME/.kde4/share/apps/networkmanagement/*に保存されます。

プロファイルが設定されていない場合は、NetworkManagerにより自動的にプロファイルが作成され、`Auto $INTERFACE-NAME`という名前が付けられます。これは、(安全性を確保しながら)可能な限り多くの場合に、設定なしで動作することを目的として作成されます。自動的に作成されたプロファイルが適切でない場合は、KDEまたはGNOMEにより提供されるネットワーク接続設定ダイアログを使用して必要に応じてプロファイルを変更します。詳細については、26.3項 「ネットワーク接続の設定」 (421 ページ)を参照してください。

21.5.3 NetworkManager機能の制御およびロックダウン

中央管理されたコンピュータでは、たとえばユーザが管理者の定義した接続の変更を許可されている場合、またはユーザが独自のネットワーク設定を定義することが許可されている場合に、PolicyKitにより特定のNetworkManager機能を制御するか、または無効にできます。対応するNetworkManagerポリシーを表示または変更するには、PolicyKitのグラフィカル［*認証*］ツールを起動します。このポリシーは、左側のツリーで、［*network-manager-settings*］エントリの下にあります。PolicyKitの概要、およびその使用方法の詳細については、 第9章 *PolicyKit* (↑*Security Guide (セキュリティガイド)*)を参照してください。

21.6 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。

カーネルは、ネットワークカードを検出し、対応するネットワークインタフェースを作成する際に、デバイスディスカバリの順序またはカーネルモジュールのロード順序によって、デバイスに名前を割り当てます。デフォルトのカーネルデバイス名は、非常にシンプルまたは厳しく制御されたハードウェア環境でのみ予測可能です。ランタイム時にハードウェアの追加や削除が可能なシステム、またはデバイスの自動設定をサポートするシステムでは、カーネルにより割り当てられたネットワークデバイス名がリブート後も変わらないと期待することはできません。

しかし、すべてのシステム設定ツールは、永続的なインタフェース名に依存しています。この問題は、udevで解決されます。udevの永続的ネットジェネレータ(/lib/udev/rules.d/75-persistent-net-generator.rules)は、ハードウェアを照合するルール(デフォルトでは、そのハードウェアアドレスを使用)を生成し、ハードウェアに永続的に固有のインタフェースを割り当てます。udevのネットワークインタフェースデータベースは、ファイル/etc/udev/rules.d/70-persistent-net.rulesに保存されます。このファイルの行ごとに、1つのネットワークインタフェースが記述され、永続名が指定されます。システム管理者は、NAME=""項目を編集することにより、割り当て名を変更できます。永続的ルールも、YaSTで変更できます。

表21.5「手動ネットワーク環境設定用スクリプト」(336ページ)に、ネットワークの環境設定関連の最も重要なスクリプトをまとめます。

表 21.5 *手動ネットワーク環境設定用スクリプト*

コマンド	機能
ifup、ifdown、ifstatus	ifスクリプトは、ネットワークインタフェースの起動や停止を行ったり、指定のインタフェースのステータスを返したりします。詳細については、ifupのマニュアルページを参照してください。
rcnetwork	rcnetworkスクリプトを使用すると、すべてのネットワークインタフェースまたは特定のネットワークインタフェースだけを起動、停止、または再起動できます。ネットワークインタフェースの停止にはrcnetwork stop、起動にはrcnetwork start、再起動にはrcnetwork restartを使用します。1つのインタフェースだけを停止、起動、または再起動したい場合は、コマンドの後にインタフェース名を指定します(たとえば、rcnetwork restart

コマンド	機能
	eth0)。rcnetwork statusコマンドを使用すると、インタフェースの状態、IPアドレス、およびDHCPクライアントが実行中かどうかが表示されます。rcnetwork stop-all-dhcp-clientsまたはrcnetwork restart-all-dhcp-clientsを使用すると、ネットワークインタフェースで実行中のDHCPクライアントを停止または再起動できます。

udevおよび永続的デバイス名については、第14章 *udevによる動的カーネルデバイス管理* (197 ページ)を参照してください。

21.6.1 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。

21.6.1.1 /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含まれています。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ファイルのほとんどの変数をifcfg-*ファイルで使用できます。ただし、/etc/sysconfig/network/configの変数の大半はグローバル変数であり、ifcfgファイル内で上書きすることはできません。たとえば、NETWORKMANAGER変数やNETCONFIG_*変数はグローバルです。

ifcfg.templateについては、21.6.1.2項 「/etc/sysconfig/network/configと/etc/sysconfig/network/dhcp」 (338 ページ)を参照してください。

► **System z:** IBM System zは、USBをサポートしていません。インタフェースファイル名とネットワークエイリアスには、qethのようにSystem z固有の要素が含まれます。 ◄

21.6.1.2 /etc/sysconfig/network/config と/etc/sysconfig/network/dhcp

configファイルは、ifup、ifdown、およびifstatusの動作の一般設定を含み、dhcpは、DHCの設定を含みます。両方の設定ファイルの変数はコメント付きです。/etc/sysconfig/network/config内の一部の変数は、ifcfg-*ファイルでも使用できます。このファイルでは、高い優先度が設定されます。/etc/sysconfig/network/ifcfg.templateファイルは、インタフェースごとに指定できる変数を一覧表示します。ただし、/etc/sysconfig/network/configの変数の大半はグローバル変数であり、ifcfgファイル内で上書きすることはできません。たとえば、NETWORKMANAGERやNETCONFIG_*は、グローバル変数です。

21.6.1.3 /etc/sysconfig/network/routes と/etc/sysconfig/network/ifroute-*

TCP/IPパケットの静的ルーティングが設定されています。ホストへのルート、ゲートウェイ経由のホストへのルート、およびネットワークへのルートなど、さまざまなシステムタスクが必要とするすべての静的ルートは、/etc/sysconfig/network/routesファイルに指定できます。個別のルーティングが必要な各インタフェースに対して、付加環境設定ファイル/etc/sysconfig/network/ifroute-*を定義します。*はイン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-を記入してください。これは、パーサがコマンドを正しく解釈できるようにするためです。詳細は、`routes(5)`マニュアルページを参照してください。

IPv4とIPv6の統合形式は、次のようになります。

```
prefix/lengthgateway -            [interface]
```

いわゆる互換形式は、次のようになります。

```
prefixgatewaylength       [interface]
```

IPv4については、ネットマスクを使用する古い形式もまだ使用できます。

```
ipv4-networkgatewayipv4-netmask [interface]
```

次の例は、互いに同等です。

```
2001:db8:abba:cafe::/64 2001:db8:abba:cafe::dead  -            eth0
208.77.188.0/24         208.77.188.166            -            eth0

2001:db8:abba:cafe::    2001:db8:abba:cafe::dead 64            eth0
208.77.188.0            208.77.188.166           24            eth0

208.77.188.0            208.77.188.166           255.255.255.0 eth0
```

21.6.1.4 /etc/resolv.conf

このファイルには、ホストが属するドメイン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）。このファイルでは、複数のドメイン名を指定できます。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、nameserverで始まる複数行で指定できます。コメントの先頭には#記号が付きます。例21.5「/etc/resolv.conf」 (340 ページ)には、/etc/resolv.confの可能な内容が示されています。

ただし、/etc/resolv.confは、手動では編集しないでください。このファイルは、netconfigスクリプトで生成されます。YaSTを使用せずに静的DNS設定を定義するには、/etc/sysconfig/network/configファイルの該当する変数を手動で編集します。

NETCONFIG_DNS_STATIC_SEARCHLIST
　ホスト名の検索に使用されるDNSドメイン名のリスト

NETCONFIG_DNS_STATIC_SERVERS
　ホスト名の検索されるネームサーバIPアドレスのリスト

NETCONFIG_DNS_FORWARDER
　設定する必要のあるDNSフォワーダの名前の定義

netconfigでDNS環境設定を無効にするには、NETCONFIG_DNS_POLICY=''を設定します。netconfigの詳細については、man 8 netconfigを参照してください。

例 21.5　/etc/resolv.conf

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

21.6.1.5 /sbin/netconfig

netconfigは、追加のネットワーク環境設定を管理するモジュール式ツールです。このツールは、事前定義されたポリシーに従って、 DHCPまたはPPPな

どの自動設定メカニズムにより提供される設定と、静的に定義された設定をマージします。要求された変更は、netconfigモジュールの呼び出しによって適用されます。このモジュールは、環境設定ファイルの変更と、サービスまたは同様のアクションの再起動を行います。

netconfigは、3つの主要なアクションを認識します。netconfig modifyコマンドとnetconfig removeコマンドは、 DHCPやPPPなどのデーモンによって使用され、netconfigの設定値を提供したり、削除します。ユーザが使用できるのは、netconfig updateコマンドだけです。

変更
: netconfig modifyコマンドは、現在のインタフェースとサービス固有の動的設定を変更し、ネットワーク設定を更新します。netconfigは、標準入力からか、または--lease-file *filename*オプションで指定されたファイルから設定を読み込み、システムのリブートまたは次の変更/削除アクションまで、それらの設定を内部的に保存します。同じインタフェースとサービスの組み合わせに関する既存設定は、上書きされます。インタフェースは、-i *interface_name*パラメータで指定されます。サービスは、-s *service_name*パラメータで指定されます。

削除
: netconfig removeコマンドは、特定のインタフェースとコマンドの組み合わせに対する変更アクションによる動的設定を削除し、ネットワーク設定を更新します。インタフェースは、-i *interface_name*パラメータで指定されます。サービスは、-s *service_name*パラメータで指定されます。

update
: netconfig updateコマンドは、現在の設定で、ネットワーク設定を更新します。これは、ポリシーや静的環境設定が変更された場合に便利です。指定したサービスのみ(dns、nis、またはntp)を更新するには、-m *module_type*パラメータを使用します。

netconfigポリシーおよび静的環境設定は、手動またはYaSTを使用して、/etc/sysconfig/network/configファイル内で定義します。dhcpやpppなどの自動設定ツールで提供された動的設定は、netconfig modifyおよびnetconfig removeのアクションで、これらのツールによって直接配信されます。NetworkManagerは、netconfig modifyおよびnetconfig remove

アクションも使用します。NetworkManagerが有効な場合、netconfig(ポリシーモード-autoは、NetworkManagerの設定のみを使用し、従来のifup方式で設定された他のインタフェースからの設定を無視します。NetworkManagerが設定を提供しない場合は、静的設定がフォールバックとして使用されます。NetworkManagerと従来のifup方式の混合使用はサポートされません。

netconfigの詳細については、man 8 netconfigを参照してください。

21.6.1.6 /etc/hosts

このファイル(例21.6「/etc/hosts」 (342 ページ)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 21.6 */etc/hosts*

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

21.6.1.7 /etc/networks

このファイルには、ネットワーク名とネットワークアドレスの対応が記述されています。形式は、ネットワーク名をアドレスの前に指定すること以外は、hostsファイルと同様です。詳細については、例21.7「/etc/networks」 (342 ページ)を参照してください。

例 21.7 */etc/networks*

```
loopback      127.0.0.0
localnet      192.168.0.0
```

21.6.1.8 /etc/host.conf

名前解決(*リゾルバライブラリ*を介したホストおよびネットワーク名の解釈)は、このファイルにより制御されます。このファイルは、libc4またはlibc5にリンクされているプログラムについてのみ使用されます。最新のglibcプログ

ラムについては、/etc/nsswitch.confの設定を参照してください。パラメータは、その行内で常に独立しています。コメントは#記号の後に記入します。表21.6「/etc/host.confファイルのパラメータ」 (343ページ)に、利用可能なパラメータを示します。/etc/host.confの例については、例21.8「/etc/host.conf」 (344 ページ)を参照してください。

表 21.6　/etc/host.confファイルのパラメータ

order *hosts*,*bind*	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を使用します。
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、ネットワークの環境設定には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)。ローカルドメインにある名前は/etc/hostsファイルにありますが、付加されるドメイン名でも認識する必要がある場合には便利なオプションです。

例 21.8　/etc/host.conf

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

21.6.1.9 /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21.9「`/etc/nsswitch.conf`」 (344 ページ)を参照してください。コメントの先頭には#記号が付きます。この例では、`hosts`データベースの下のエントリは、要求がDNSを介して、`/etc/hosts`(`files`)に送信されることを意味しています(第24章 *ドメインネームシステム*(375ページ)参照)。

例 21.9　/etc/nsswitch.conf

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files
rpc:        files
ethers:     files
netmasks:   files
netgroup:   files nis
publickey:  files

bootparams: files
automount:  files nis
aliases:    files nis
shadow:     compat
```

NSSで利用できる「データベース」については、表21.7「/etc/nsswitch.confで利用できるデータベース」 (345 ページ)を参照してください。 NSSデータベースの環境設定オプションについては、表21.8「NSS 「データベース」の環境設定オプション」 (346 ページ)を参照してください。

表 21.7　/etc/nsswitch.confで利用できるデータベース

aliases	sendmailによって実行されたメールエイリアス。man 5 aliasesコマンドで、マニュアルページを参照してください。
ethers	イーサネットアドレス。
netmasks	ネットワークとそのサブネットマスクのリスト。サブネットを使用する場合のみ必要です。
group	getgrentによって使用されるユーザグループ。groupのマニュアルページも参照してください。
hosts	gethostbynameおよび同類の関数によって使用されるホスト名とIPアドレス。
netgroup	アクセス許可を制御するための、ネットワーク内にある有効なホストとユーザのリスト。netgroup(5) manページを参照してください。
networks	ネットワーク名とアドレス。getnetentによって使用されます。
publickey	NFSとNIS+によって使用されるSecure_RPCの公開鍵と秘密鍵。
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 21.8　NSS 「データベース」の環境設定オプション

ファイル	直接アクセスファイル。たとえば/etc/aliases。
db	データベース経由のアクセス。
nis、nisplus	NIS。第3章 *Using NIS* (↑*Security Guide (セキュリティガイド)*)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。

21.6.1.10 /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)マニュアル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。

21.6.1.11 /etc/HOSTNAME

このファイルには、ドメイン名付きで完全修飾されたホスト名が含まれています。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。

21.6.2 設定のテスト

設定内容を設定ファイルに書き込む前に、それをテストすることができます。テスト環境を設定するには、ipコマンドを使用します。接続をテストするには、pingコマンドを使用します。また、以前の設定ツールのifconfigやrouteも使用することができます。

ip、ifconfig、およびrouteコマンドは、ネットワーク設定を直接変更します。ただし、変更内容は設定ファイルに保存されません。正しい設定ファイルに変更内容を保存しない限り、変更したネットワーク設定は再起動時に失われてしまいます。

21.6.2.1 ipによるネットワークインタフェースの設定

ip は、ネットワークデバイス、ルーティング、ポリシールーティング、およびトンネルの表示と設定を行うツールです。

ipは非常に複雑なツールです。一般的には、ip *options object command*の形式で指定します。objectの部分には、次のオブジェクトを指定することができます。

リンク
　ネットワークデバイスを表します。

アドレス
　デバイスのIPアドレスを表します。

隣接
　ARPまたはNDISCキャッシュエントリを表します。

route
　ルーティングテーブルエントリを表します。

ルール
　ルーティングポリシーデータベース中のルールを表します。

maddress
　マルチキャストアドレスを表します。

mroute
　マルチキャストルーティングキャッシュエントリを表します。

tunnel
　IPトンネルを表します。

commandを指定しないと、デフォルトのコマンド(通常はlist)が使用されます。

デバイスの状態を変更するには、ip link set *device_name command*コマンドを使用します。たとえば、デバイスeth0を無効にするには、ip link seteth0 downを実行します。このデバイスを再び有効にする場合は、ip link seteth0 upを実行します。

デバイスを有効にしたら、そのデバイスを設定することができます。デバイスのIPアドレスを使用する場合は、`ip addr add`*`ip_address`* `+ dev` *`device_name`*を使用します。たとえば、インタフェースeth0にアドレス「192.168.12.154/30」を設定し、標準のブロードキャスト(`brd`オプション)を使用する場合は、「`ip addradd 192.168.12.154/30 brd + dev eth0`」と入力します。

接続を実際に利用可能にするには、デフォルトゲートウェイの設定も必要です。システムのゲートウェイを設定するには、「`ip route add`gateway_ip_address」を入力します。あるIPアドレスを別のIPアドレスに変換するには、`nat: ip route add nat ip_address via other_ip_address`を使用します。

すべてのデバイスを表示する場合は、`ip link ls`を使用します。動作しているインタフェースだけを表示する場合は、`ip link ls up`を使用します。デバイスのインタフェース統計情報を印刷する場合は、「`ip -s link lsdevice_name`」と入力します。デバイスのアドレスを表示する場合は、「`ip addr`」と入力します。`ip addr`の出力には、デバイスのMACアドレスに関する情報も表示されます。すべてのルートを表示する場合は、`ip route show`を使用します。

`ip`の使用方法の詳細については、`iphelp`を入力するか、または`ip(8)`マニュアルページを参照してください。`help`オプションは、すべての`ip`サブコマンドに関して利用できます。たとえば、`ip addr`のヘルプが必要な場合は、`ipaddr help`と入力します。`ip`マニュアルについては、`/usr/share/doc/packages/iproute2/ip-cref.pdf`を参照してください。

21.6.2.2 pingを使った接続のテスト

`ping`コマンドは、TCP/IP接続が正常に動作しているかどうかを調べるための、標準ツールです。pingコマンドはICMPプロトコルを使って、小さなデータパケットECHO_REQUESTデータグラムを、宛先ホストに送信し、即時応答を要求します。この作業が成功した場合、`ping`コマンドは、その結果を知らせるメッセージを表示します。これは、ネットワークリンクが基本的に機能していることを意味します。

`ping`は、2台のコンピュータ間の接続機能をテストするだけでなく、接続品質に関する基本的な情報も提供します。ping例21.10「pingコマンドの出

力」 (350 ページ)コマンドの実行結果例は、を参照してください。最後から2番目の行に、転送パケット数、失われたパケット数、およびpingの実行時間の合計が記載されています。

PINGの宛先には、ホスト名またはIPアドレスを指定することができます。たとえば、pingexample.comまたはping192.168.3.100のように指定します。pingコマンドを実行すると、Ctrl + Cを押すまでの間、継続的にパケットが送信されます。

接続されているかどうかを確認するだけで良い場合は、-cオプションを使って送信するパケット数を指定することができます。たとえば、PINGを3パケットに制限する場合は、「ping -c 3 example.com」を入力します。

*例 **21.10** pingコマンドの出力*

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

デフォルトでは、pingは1秒ごとにパケットを送信します。間隔を変更するには、 -i オプションを指定します。たとえば、pingの間隔を10秒に増大する場合は、ping -i 10 example.comを入力します。

複数のネットワークデバイスを持つシステムの場合、特定のインタフェースアドレスを指定してpingを実行することができます。その場合は、-Iオプションを、選択したデバイスの名前とともに使用します。たとえば、ping -I wlan1 example.comと指定します。

pingのオプションと使用方法の詳細は、「ping-h」を入力するか、またはping(8)マニュアルページを参照してください。

ヒント: IPv6アドレスのping

IPv6の場合は、ping6コマンドを使用します。ただし、リンクローカルアドレスをpingするには、-Iでインタフェースを指定する必要があります。アドレスがeth1を介して到達可能な場合は、次のコマンドが有効です。

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

21.6.2.3 ifconfigを使ったネットワークの設定

ifconfigは、ネットワーク設定ツールです。

注記: ifconfigとip

ifconfigツールは廃止されました。代わりに、ipを使用してください。ipと異なり、ifconfigは、インタフェースの設定にのみ使用できます。ただし、インタフェース名は9文字までに制限されます。

---

ifconfigに引数を指定しないと、現在アクティブなインタフェースのステータスが表示されます。例21.11「ifconfigコマンドの出力」(351 ページ)が示すように、ifconfigは、非常にわかりやすく表示された詳細情報を出力します。この出力では、デバイスのMACアドレス(HWaddrの値)も1行目に表示されています。

例 21.11 ifconfigコマンドの出力

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 MB)
```

ifconfigのオプションと使用方法の詳細については、ifconfig-hを入力するか、またはifconfig(8)マニュアルページを参照してください。

21.6.2.4 routeによるルーティングの設定

routeは、IPルーティングテーブルを操作するプログラムです。このコマンドを使用すると、ルーティングの設定を表示したり、ルートを追加または削除できます。

注記: routeとip

routeプログラムは廃止されました。代わりに、ipを使用してください。

---

routeは、総合的なルーティング情報を素早く参照して、ルーティングに関する問題を探す場合などに役立ちます。現在のルーティング設定を表示するには、rootとして「route-n」を入力します。

例 21.12　route -nコマンドの出力

```
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.20.0.0       *               255.255.248.0   U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
loopback        *               255.0.0.0       U         0 0          0 lo
default         styx.exam.com   0.0.0.0         UG        0 0          0 eth0
```

routeのオプションと使用方法の詳細については、「route-h」を入力するか、またはroute (8)マニュアルページを参照してください。

21.6.3 スタートアップスクリプト

前述の環境設定ファイルに加え、マシンのブート時にネットワークプログラムをロードするさまざまなスクリプトも用意されています。これらは、システムがマルチユーザランレベルのいずれかに切り替わったときに起動します。これらのスクリプトの一部は、表21.9「ネットワークプログラム用スタートアップスクリプト」 (353 ページ)で説明されています。

表 21.9　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。networkサービスが開始されなかった場合、ネットワークインタフェースは実装されません。
/etc/init.d/xinetd	xinetdを開始します。xinetdを使用すると、サーバサービスがシステム上で利用できるようになります。たとえば、FTP接続の開始時に必ずvsftpdを起動することができます。
/etc/init.d/rpcbind	RPCプログラム番号をユニバーサルアドレスに変換するrpcbindユーティリティを起動します。NFSサーバなどのRPCサービスで必要です。
/etc/init.d/nfsserver	NFSサーバを起動します。
/etc/init.d/postfix	postfixプロセスを制御します。
/etc/init.d/ypserv	NISサーバを起動します。
/etc/init.d/ypbind	NISクライアントを起動します。

21.7 ボンディングデバイスの設定

システムによって、通常のEthernetデバイスの規格のデータセキュリティ/可用性の要件を超えるネットワーク接続の実装が望ましいことがあります。その場合、数台のEthernetデバイスを集めて1つのボンディングデバイスを設定できます。

ボンディングデバイスの設定には、ボンディングモジュールオプションを使用します。ボンディングデバイスの振る舞いは、主にボンディングデバイス

のモードによって影響されます。デフォルトの動作は、`mode=active-backup`であり、アクティブなスレーブに障害が発生すると、別のスレーブデバイスがアクティブになります。

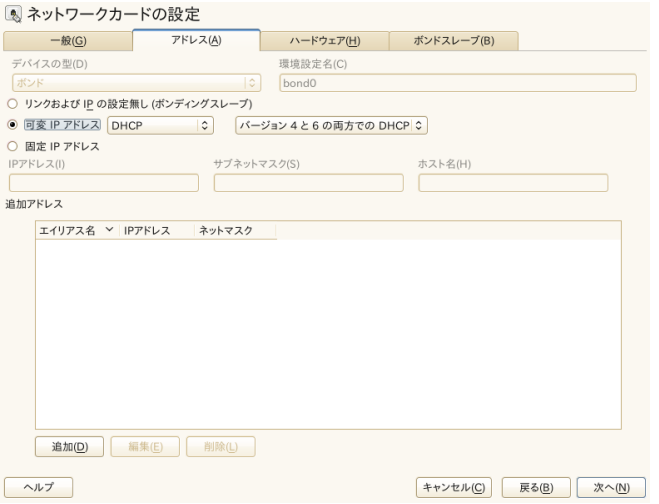
ヒント: ボンディングとXen

ボンディングデバイスの使用が有用なのは、利用可能なネットワークカードが複数あるマシンの場合のみです。大半の設定では、Domain0でのみボンディング設定を使用する必要があることになります。 VM Guestシステムに複数のネットワークカードが割り当てられている場合のみ、VM Guestでのボンド設定が役立つかもしれません。

ボンディングデバイスを設定するには、次の手順に従います。

1 ［*YaST*］ > ［*ネットワークデバイス*］ > ［*ネットワーク設定*］の順に選択します。

2 ［*追加*］を使用し、［*デバイスの型*］を［*ボンド*］に変更します。［*次へ*］で続行します。



3 IPアドレスをボンディングデバイスに割り当てる方法を選択します。3つの方法から選択できます。

- IPアドレスなし
- 可変IPアドレス(DHCPまたはZeroconf)
- 固定IPアドレス

ご使用の環境に適合する方法を使用します。

4 ［*ボンドスレーブ*］タブで該当するチェックボックスをオンにして、ボンドに含めるEthernetデバイスを選択します。

5 ［*ボンドドライバオプション*］を編集します。設定には次のモードを使用できます。

- balance-rr
- active-backup
- balance-xor
- ブロードキャスト
- 802.3ad
- balance-tlb
- balance-alb

6 パラメータ`miimon=100`が［*ボンドドライバオプション*］に追加されていることを確認します。このパラメータがないと、データの整合性が定期的にチェックされません。

7 ［*次へ*］をクリックし、［*OK*］で YaST を終了して、デバイスを作成します。

すべてのモードと他の多数のオプションの詳細は、「［*Linux Ethernet Bonding Driver HOWTO*］」に記載されています。このドキュメントは、kernel-sourceをインストールすると、`/usr/src/linux/Documentation/networking/bonding.txt`で読むことができます。

21.7.1 ボンディングスレーブのホットプラグ

特定のネットワーク環境(高可用性など)では、ボンディングスレーブインタフェースを別のものに置換しなければならないことがあります。ネットワークデバイスで頻繁に障害が発生するなどの理由があります。解決方法として、ボンディングスレーブのホットプラグを設定します。

ボンドは以下のように(man 5 ifcfg-bondingに従って)通常通りに設定されます。たとえば、

```
ifcfg-bond0
          STARTMODE='auto' # or 'onboot'
          BOOTPROTO='static'
          IPADDR='192.168.0.1/24'
          BONDING_MASTER='yes'
          BONDING_SLAVE_0='eth0'
          BONDING_SLAVE_1='eth1'
          BONDING_MODULE_OPTS='mode=active-backup miimon=100'
```

ただし、スレーブはSTARTMODE=hotplugおよびBOOTPROTO=noneで指定されます。

```
ifcfg-eth0
          STARTMODE='hotplug'
          BOOTPROTO='none'

ifcfg-eth1
          STARTMODE='hotplug'
          BOOTPROTO='none'
```

BOOTPROTO=noneはethtoolオプション(提供されている場合)を使用しますが、ifup eth0でリンクを設定しません。これは、スレーブインタフェースがボンドマスターによって制御されるためです。

STARTMODE=hotplugにより、スレーブインタフェースが利用可能になるとすぐに、ボンドに自動的に追加されます。

MACアドレスではなく、バスIDでデバイスを照合するように、/etc/udev/rules.d/70-persistent-net.rulesのudevルールを変更する必要があります(hwinfo --netcardに表示されるudev KERNELSキーワードを"SysFS BusID"とします)。これによって障害のあるハードウェアを置換(同じスロットで、MACが異なるネットワークカードを使用)できるよ

うになり、ボンドがすべてのスレーブのMACアドレスを変更するので混乱を避けられます。

たとえば、

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
KERNELS=="0000:00:19.0", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"
```

ブート時に/etc/init.d/networkはホットプラグスレーブを待機しませんが、ボンドの準備が整うのを待機します。これには少なくとも1つのスレーブが利用可能であることが必要です。スレーブインタフェースの1つがシステムから削除されると(NICドライバからアンバインド、NICドライバのrmmod、または実際のPCIホットプラグ取り外し)、カーネルによってボンドから自動的に削除されます。システムに新しいカードが追加されると(スロットのハードウェアが置換されると)、udevは、バスベースの永続名規則を使って名前をスレーブ名に変更し、ifupを呼び出します。ifup呼び出しによって、ボンドに自動的に追加されます。

21.8 ダイアルアップアシスタントとしてのsmpppd

一部のホームユーザは、インターネット接続専用の回線を持っていません。代わりにダイアルアップ接続を使用しています。接続は、ダイアルアップ方法(ISDNまたはDSL)に応じてipppdまたはpppdで制御されます。基本的には、これらのプログラムを正常に起動するだけでオンラインで接続できます。

ダイアルアップ接続時に追加費用が発生しない定額接続を使用している場合は、単に該当するデーモンを起動します。ダイアルアップ接続の管理には、デスクトップ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 (SUSE Meta PPP Daemon)は、ここで関与します。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。

21.8.1 smpppdの設定

smpppdによる接続は、YaSTにより自動的に設定されます。実際のダイ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管理するには、このオプションをyesに設定します。smpppdはポート3185でリッスンします。このパラメータをyesに設定した場合は、パラメータbind-address、host-range、およびpasswordもそれに応じて設定する必要があります。

bind-address = *ip address*
: ホストに複数のIPアドレスがある場合は、このパラメータを使用してsmpppdで接続の受け入れに使用するIPアドレスを指定します。デフォルトでは、すべてのアドレスでリッスンします。

host-range = *min ipmax 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。

21.8.2 cinternetのリモート使用設定

cinternetは、ローカルまたはリモートのsmpppd制御に使用できます。cinternetは、グラフィックKInternetのコマンドライン版です。これらのユーティリティをリモートsmpppdで使用できるようにするには、設定ファイル`/etc/smpppd-c.conf`を手動またはc internetの使用によって編集します。このファイルでは、次の4つのオプションのみを使用します。

sites = *list of sites*
　フロントエンドがsmpppdを検索するサイトのリスト。フロントエンドは、ここに記述されている順序でオプションをテストします。`local`は、ローカルsmpppdへの接続の確立を指定します。`gateway`は、ゲートウェイ上のsmpppdをポイントします。`config-file`は、`/etc/smpppd-c.conf`ファイルの`server`オプションと`port`オプションで指定されたsmpppdに対して接続を確立することを指定しています。`slp`は、フロントエンドを、SLPで検出されたsmpppdに接続することを指定します。

server = *server*
　smpppdを実行するホスト。

port = *port*
　smpppdを実行するポート。

password = *password*
　smpppdに選択されたパスワード。

smpppdがアクティブな場合、アクセスしようとします。たとえば、`cinternet --verbose --interface-list`とします。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)`のマニュアルページを参照してください。

22 ネットワーク上のSLPサービス

サービスロケーションプロトコル*(SLP)*は、*ローカルネットワークに接続されているクライアントの構成を簡略化するために開発されました*。ネットワーククライアントを設定するには、すべての必要なサービスを含め、管理者はネットワークで利用できるサーバに関する詳しい知識が必要とされました。SLPは、ローカルネットワーク上にあるすべてのクライアントに対して特定のサービスを利用できることを通知します。このような通知情報を利用してSLPをサポートする各種アプリケーションを自動的に設定することができます。

SUSE® Linux Enterprise Serverは、SLPによって提供されるインストールソースを使用するインストールをサポートしています。また、多くのシステムサービスは、統合SLPをサポートしています。YaSTとKonquerorは、どちらもSLP用の適切なフロントエンドを持っています。ご利用のシステムでインストールサーバ、ファイルサーバ、印刷サーバなどのSLPを使用することにより、ネットワークに接続されたクライアントに一元的な管理機能を提供します。

重要: SUSE Linux Enterprise ServerでのSLPサポート

SLPサポートを提供するサービスにはcupsd、rsyncd、ypserv、openldap2、ksysguardd、saned、kdm、vnc、login、smpppd、およびrpasswd 、postfix、およびsshd(fish経由)があります。

22.1 インストール

必要なすべてのパッケージがデフォルトでインストールされます。ただし、SLPによりサービスを提供する場合は、パッケージopenslp-serverがインストールされていることを確認します。

22.2 SLPをアクティブ化する

SLPサービスを提供するには、システム上でslpdを実行する必要があります。マシンがクライアントとしてのみ動作し、サービスを提供しない場合は、slpdを実行する必要はありません。SUSE Linux Enterprise Server中のほとんどのシステムサービスと同様、slpdデーモンは別のinitスクリプトを使用して制御されます。インストール後に、このデーモンはデフォルトで非アクティブになります。一時的にこのデーモンを有効化するには、rcslpd startをrootで実行し、rcslpd stopで停止します。restartで再始動、またはstatusでステータスチェックを実行します。ブート後にslpdを常にアクティブにする必要がある場合は、YaSTで［システム］＞［システムサービス(ランレベル)］の順に選択してslpdを有効にするか、またはinsserv slpdコマンドをrootとして実行します。

22.3 SUSE Linux Enterprise ServerのSLPフロントエンド

ネットワーク内のSLPから提供されているサーバを見つけるには、slptool (openslp package)などのSLPフロントエンドか、YaSTを使用します。

slptool
: slptoolは、ネットワーク内でSLP照会をアナウンスしたり、プロプライエタリサービスをアナウンスするために使用できるコマンドラインプログラムです。slptool --helpは、すべての使用可能なオプションと機能を一覧します。たとえば、現在のネットワークで自己をアナウンスするすべての時間サーバを検索するには、次のコマンドを実行します。

```
slptool findsrvs service:ntp
```

YaST
: YaSTは、SLPブラウザも提供します。ただし、このブラウザをYaSTコントロールセンターから利用することはできません。このブラウザを起動するには、`yast2 slp`を`root`ユーザとして実行します。サービスの詳細を取得するには、左側にある［*サービスタイプ*］をクリックします。

22.4 SLP経由のインストール

ネットワーク内にSUSE Linux Enterprise Serverインストールメディアをもつインストールサーバがある場合は、このメディアをSLPに登録し、SLPを介して提供することができます。詳細については、項 「インストールソースを保持するサーバのセットアップ」 (第14章 *リモートインストール*, ↑*導入ガイド*)を参照してください。SLPインストールが選択されると、選択したブートメディアからシステムがブートして検出されたソースを表示した後に、linuxrcがSLP照会を開始します。

22.5 SLPによるサービスの提供

SUSE Linux Enterprise Server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を介して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。次の例では、スキャナサービスを登録します。

```
## 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TービスURLと分けるようにします。0から65535で登録期間の値を設定します。0の場合は登録する必要がありません。65535はすべての制限を削除します。

登録ファイルにはまた、2つの変数watch-port-tcpおよびdescriptionが含まれます。watch-tcp-portはSLPサービスアナウンスとリンクして、slpdにサービスのステータスをチェックさせることにより、関連サービスがアクティブかどうか確認します。descriptionには、正しいブラウザを使用している場合に表示される、さらに詳細なシステム名が含まれています。

ヒント: YaSTとSLP

インストールサーバ、YOUサーバなどのようにYaSTが処理を行うサービスの一部では、モジュールダイアログでSLPがアクティブになった時点で自動的にこの登録が実行されます。続いてYaSTはこれらのサービスの登録ファイルを作成します。

/etc/slp.regによる静的登録
: この方法と、/etc/slp.reg.dによる手続きの唯一の違いは、すべてのサービスが中央のファイルにグループ化されることです。

slptoolによる動的登録
: 設定ファイルなしでサービスを動的に登録する必要がある場合は、slptoolコマンドラインユーティリティを使用します。同じユーティリティを使用して、slpdを再起動しないで、既存の提供サービスの登録を取り消すことができます。

22.6 詳細情報

RFC 2608、2609、2610
: 一般的にRFC 2608はSLPの定義を取り扱います。RFC 2609は、使用されるサービスURLの構文を詳細に扱います。またRFC 2610ではSLPを使用したDHCPについて説明しています。

http://www.openslp.org
OpenSLPプロジェクトのホームページです。

/usr/share/doc/packages/openslp
このディレクトリには、 SUSE Linux Enterprise Serverの詳細を含むREADME.SuSE、RFC、および2つの紹介的なHTMLドキュメントなど、openslp-serverパッケージ付属のSLPのドキュメントが格納されています。SLP機能を使用するプログラマに役立つより詳細な情報については、openslp-develパッケージに含まれる『プログラマガイド』を参照してください。

23 NTPによる時刻の同期

NTP (network time protocol)メカニズムは、システムの時刻をネットワーク上で同期させるためのプロトコルです。最初に、マシンは信頼できる時刻を持つサーバに時刻を照会できます。次に、ネットワーク上の他のコンピュータがこのマシン自体に対し、時刻を照会できます。目的は2つあり、絶対的な時間を維持することと、ネットワーク内のすべてのマシンのシステム時刻を同期させることです。

正確なシステムタイムを維持することはさまざまな場で重要です。ハードウェア組み込み型クロックがデータベースやクラスタなどのアプリケーション要件に合致しないことがよくあります。システムタイムを手動で修正することは時に問題を発生させる可能性があります。たとえば、時間を逆廻りに戻すことで重要なアプリケーションの誤動作を誘発することもあります。ネットワーク内では、すべてのマシンのシステムタイムを同期させることが通常必要とされますが、手動での時刻調整はよい方法ではありません。NTPには、これらの問題を解決するメカニズムがあります。NTPサービスは、ネットワーク内の信頼できるタイムサーバのヘルプによって、システム時間を継続的に調整します。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。

23.1 YaSTでのNTPクライアントの設定;

`ntp`パッケージ付属のNTPデーモン(`ntpd`)は、ローカルコンピュータを時間の参照に使用するように事前設定されています。ただし、ハードウェアクロックは、より正確な時間ソースが利用できない場合の予備としてのみ使用され

ます。YaSTを利用すれば、NTPクライアントを簡単に設定することができます。

23.1.1 基本的な設定

YaST NTPクライアントの設定(［ネットワークサービス］>［*NTP環境設定*］)は、タブで構成されています。ntpdの起動モードと照会先のサーバは、［*一般的な設定*］タブで設定します。

［*手動でのみ*］
　［*手動でのみ*］は、ntpdデーモンを手動で開始する場合に選択します。

［*今すぐ開始し、システム起動時に開始するよう設定*］
　システムのブート時に自動的にntpdを起動するには、［*今すぐ開始し、システム起動時に開始するよう設定*］を選択します。この設定をお勧めします。 次に、23.1.2項 「基本的な設定の変更」 (368 ページ)で説明されているようにサーバを設定します。

23.1.2 基本的な設定の変更

［*一般の設定*］タブの下部には、クライアントに対するサーバおよび時刻情報のその他の情報源が表示されます。必要に応じて、［*追加*］、［*削除*］、および［*編集*］を使用してこのリストを変更します。［］Display Log］では、クライアントのログファイルを表示できます。

時刻情報の情報源を追加するには、［*追加*］をクリックします。表示されるダイアログで、時刻同期に使用する情報源のタイプを選択します。次のオプションを指定できます。

図 23.1　YaST: NTPサーバ

サーバ

［*選択*］プルダウンリスト(図23.1「YaST: NTPサーバ」 (369 ページ)参照)で、ローカルネットワーク上のタイムサーバ(［*ローカルNTPサーバ*］)または目的のタイムゾーンを担当するインターネット上のタイムサーバ(［*公開NTPサーバ*］)のどちらを使用して時刻の同期を設定するか決定します。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、［*受諾*］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、［*受諾*］をクリックしてダイアログを閉じます。メインダイアログの［テスト］を使用して、選択されているサーバの可用性をテストします。［*オプション*］では、`ntpd`の追加オプションを指定できます。

［*Access Control Options*］を使用すると、コンピュータ上で実行するデーモンによりリモートコンピュータが実行可能なアクションを制限できます。このフィールドは、［*セキュリティの設定*］タブで［*NTP サービスを設定したサーバに制限する*］にチェックマークを入れた後でのみ有効になります(図23.2「高度なNTP設定:セキュリティの設定」 (371 ページ)参照)。このオプションは、`/etc/ntp.conf`内の`restrict`節に対応しま

す。たとえばnomodify notrap noqueryは、サーバがコンピュータのNTP設定を変更し、NTPデーモンのトラップ機能(リモートイベントのログ記録機能)を使用することを拒否します。自身の管理下にないサーバについては(たとえばインターネット上のサーバなど)、こうした制限を適用することをお勧めします。

詳細については、/usr/share/doc/packages/ntp-doc(ntp-docパッケージの一部)を参照してください。

ピア
ピアは、対称的な関係が確立されたコンピュータで、タイムサーバとクライアントの両方の役割を果たします。サーバの代わりに、同じネットワーク内のピアを使用するには、そのピアシステムのアドレスを入力します。ダイアログのそれ以外の内容は［サーバ］ダイアログと同じです。

ラジオクロック
時刻同期にシステムのラジオクロックを使用するには、クロックタイプ、ユニット番号、デバイス名、およびその他のオプションをこのダイアログで指定します。ドライバを微調整するには、［*ドライバの調整*］をクリックします。ローカルラジオクロックの動作の詳細については、/usr/share/doc/packages/ntp-doc/refclock.html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。

図 23.2　高度なNTP設定:セキュリティの設定

［セキュリティの設定］タブで(図23.2「高度なNTP設定:セキュリティの設定」 (371 ページ)参照)、`ntpd`をchroot jailで起動するかどうか指定します。デフォルトでは、［*Run NTP Daemon in Chroot Jail*］が選択されています。このオプションは、攻撃によってシステム全体が危険な状態に陥ることを防ぐので、`ntpd`が攻撃された場合のセキュリティを強化します。

［*Restrict NTP Service to Configured Servers Only*］は、リモートコンピュータがユーザのコンピュータのNTP設定を表示および変更すること、およびリモートイベントログのトラップ機能を使用することを拒否し、それによってシステムのセキュリティを向上させます。［*一般の設定*］タブの時間ソースのリストで、個別のコンピュータに対するアクセス制御オプションを上書きしない限り、こうした制限は有効になるとすべてのリモートコンピュータに適用されます。他のすべてのリモートコンピュータでは、ローカルタイムのクエリのみが許可されます。

SuSEfirewall2がアクティブな場合、［*ファイアウォール内でポートを開く*］を有効にします(デフォルト)。ポートを閉じたままにすると、タイムサーバと接続を確立することはできません。

23.2 ネットワークでのntpの手動設定

ネットワーク内のタイムサーバを使用するには、serverパラメータを設定するのが最も簡単です。たとえば、タイムサーバntp.example.comがネットワークから接続可能な場合、その名前をファイル/etc/ntp.confに行として追加します。

```
server ntp.example.com
```

別のタイムサーバを追加するには、別の行にキーワードの「server」を挿入します。rcntp startコマンドでntpdを初期化後、時間が安定し、ローカルコンピュータのクロックを修正するドリフトファイルが作成されるまで、約1時間かかります。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。

NTP機構をクライアントとして使用するには、2種類の方法があります。まず、クライアントは既知のサーバに定期的に時間を照会することができます。クライアント数が多い場合、この方法はサーバの過負荷を引き起こす可能性があります。2つ目は、ネットワークでブロードキャストを行う時刻サーバから送信されるNTPブロードキャストを、クライアントが待機する方法です。この方法には不利な面があります。サーバの精度が不明なこと、そしてサーバから送信される情報が誤っていた場合、深刻な問題が発生する可能性があることです。

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。

23.3 ランタイム時の動的時刻同期

ネットワークに接続せずにシステムが起動すると、ntpdは起動しますが、設定ファイルで設定されたタイムサーバのDNS名を解決できません。これは、暗号化されたWLANでネットワークマネージャを使用するときに発生します。

ランタイム時にntpdでDNS名を解決するには、dynamicオプションを設定する必要があります。ネットワークが起動後に確立されると、ntpdは再度名前を検索し、時刻を取得するタイムサーバに到達します。

/etc/ntp.confを手動で編集して、dynamicを1つ以上のserverエントリに追加します。

```
server ntp.example.com dynamic
```

または、YaSTを使用して、次の手順に従います。

1 YaSTで、［ネットワークサービス］＞［*NTP環境設定*］の順にクリックします。

2 設定するサーバを選択します。［*編集*］をクリックします。

3 ［*オプション*］フィールドを有効にして、［dynamic］を追加します。他のオプションが入力されている場合は、スペースで区切ります。

4 ［*OK*］をクリックして、編集ダイアログを閉じます。前の手順を繰り返して、必要に応じてすべてのサーバを変更します。

5 最後に、［*OK*］をクリックして設定を保存します。

23.4 ローカルリファレンスクロックの設定

ntpdソフトウェアパッケージには、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、ntp-docパッケージの/usr/share/doc/packages/ntp-doc/refclock.htmファイルに記載されています。各ドライバには、番号が関連付けられています。NTPでは、実際の設定は疑似IPアドレスを使用して行われます。クロックは、ネットワークに存在しているものとして/etc/ntp.confファイルに入力されます。このため、これらのクロックには127.127.*t*.*u*という形式の特別なIPアドレスが割り当てられます。ここで、*t*はクロックのタイプを示し、使用されているドライバを決定します。*u*はユニットのタイプを示し、使用されているインタフェースを決定します。

通常、各ドライバは設定をより詳細に記述する特別なパラメータを持っています。/usr/share/doc/packages/ntp-doc/driver*NN*.html(ここで*NN*はドライバの番号)ファイルは、特定のクロックタイプの情報を提供します。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。ntp-docパッケージのインストール後は、ntpのマニュアルを/usr/share/doc/packages/ntp-docディレクトリで参照できます。ドライバパラメータについて説明するドライバページへのリンクは、ファイル/usr/share/doc/packages/ntp-doc/refclock.htmに記述されています。

23.5 ETR（External Time Reference)とのクロックの同期

ETR（External Time Reference）とのクロック同期のサポートを利用できます。ETRは、2**20(2の20乗)マイクロ秒ごとに、発振器信号と同期信号を送信して、すべての接続先サーバのTODクロックの同期を保ちます。

可用性のため、2ユニットのETRをコンピュータに接続できます。クロックが同期チェックの許容値を超えた場合は、すべてのCPUがマシンをチェックし、クロックが同期していないことを示します。この事態が発生した場合は、XRC対応デバイスへのすべてのDASD I/Oがクロックの再同期まで停止します。

ETRサポートは2つのsysfs属性を介して有効化されます。rootとして以下のコマンドを実行します。

```
echo 1 > /sys/devices/system/etr/etr0/online
echo 1 > /sys/devices/system/etr/etr1/online
```

24 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192.168.2.100がホスト名jupiter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、21.3項 「ネームレゾリューション」 (305 ページ)で DNS に関する一般的な説明を参照してください。以降に示す設定例はBINDの場合のものです。

24.1 DNS用語

ゾーン
: ドメインのネームスペースは、ゾーンと呼ばれる領域に分割されます。たとえば、example.comの場合は、comドメインのexampleセクション(つまりゾーン)を表します。

DNSサーバ
: DNSサーバは、ドメインの名前とIP情報を管理するサーバです。マスタゾーン用にプライマリDNSサーバ、スレーブゾーン用にセカンダリサーバ、またはキャッシュ用にいずれのゾーンも持たないスレーブサーバを持つことできます。

  マスタゾーンのDNSサーバ
  : マスタゾーンにはネットワークからのすべてのホストが含まれ、DNSサーバのマスタゾーンにはドメイン内のすべてのホストに関する最新のレコードが格納されます。

スレーブゾーンのDNSサーバ
: スレーブゾーンはマスタゾーンのコピーです。スレーブゾーンのDNSサーバは、ゾーン転送操作によりマスタサーバからゾーンデータを取得します。スレーブゾーンのDNSサーバは、有効なゾーンデータである(期限切れでない)限り、ゾーンに適切に応答します。スレーブがゾーンデータの新規コピーを取得できない場合、ゾーンへの応答を停止します。

フォワーダ
: フォワーダは、DNSサーバがクエリに回答できない場合に、そのクエリの転送先になるDNSサーバです。1つの環境設定内で複数の設定ソースを有効にするには、`netconfig`を使用します(`man 8 netconfig`も参照)。

レコード
: レコードは、名前とIPアドレスに関する情報です。サポートされているレコードおよびその構文は、BINDのドキュメントで説明されています。次は、特別なレコードの一部です。

NSレコード
: NSレコードは、指定のドメインゾーンの担当マシンをネームサーバに指定します。

MXレコード
: MX(メール交換)レコードは、インターネット上でメールを転送する際に通知するマシンを説明します。

SOAレコード
: SOA (Start of Authority)レコードは、ゾーンファイル内で最初のレコードです。SOAレコードは、DNSを使用して複数のコンピュータ間でデータを同期化する際に使用されます。

24.2 インストール

DNSサーバをインストールするには、YaSTを起動してから、［ソフトウェア］>［*ソフトウェア管理*］の順に選択します。［*表示*］>［パターン］の順に選択して、［*DHCPおよびDNSサーバ*］を選択します。依存関係のあるパッケージのインストールを確認して、インストールプロセスを完了します。

24.3 YaSTでの設定

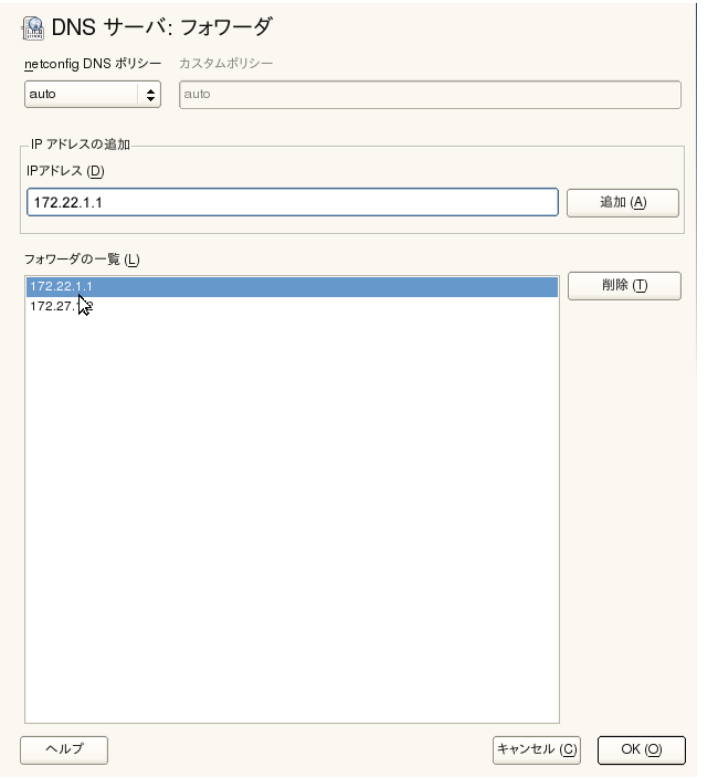
YaSTモジュールを使用して、ローカルネットワーク用にDNSサーバを設定します。このモジュールを初めて起動すると、サーバ管理に関して2、3の決定を行うように要求されます。この初期セットアップを完了すると、基本的なサーバ設定が生成されます。エキスパートモードを使用すると、より詳細な設定タスク(ACLのセットアップ、ロギング、TSIGキーなどのオプション)を処理できます。

24.3.1 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。

1 モジュールを初めて起動すると、のような［フォワーダの設定］図24.1 「DNSサーバのインストール:フォワーダの設定」 (378 ページ)ダイアログが表示されます。［*Netconfig DNS Policy*］を使用すると、フォワーダを提供するデバイスを決定したり、独自の［*Forwarder List*］を指定するかどうかを決定できます。netconfigの詳細については、`man 8 netconfig`を参照してください。

図 24.1　DNSサーバのインストール:フォワーダの設定



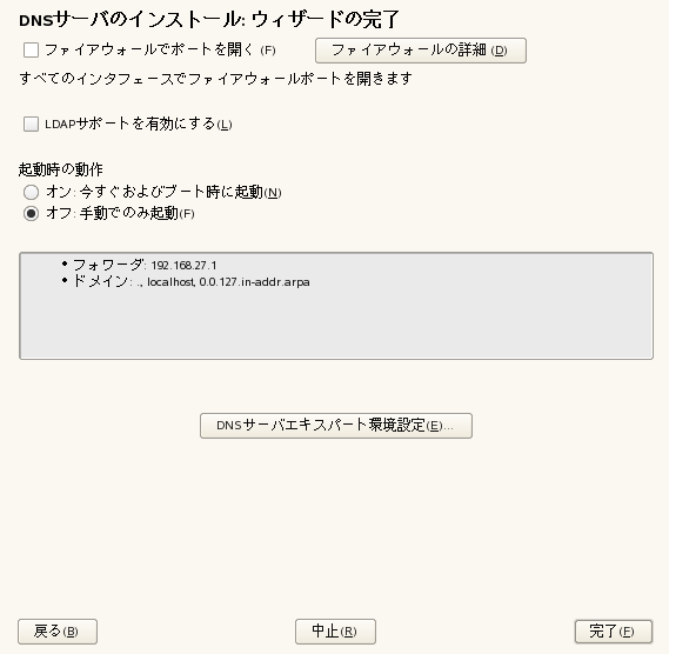
フォワーダは、ご使用のDNSサーバが回答できないクエリの送信先とするDNSサーバです。フォワーダのIPアドレスを入力して、［*追加*］をクリックします。

2　［*DNS*ゾーン］ダイアログは、複数の部分で構成されており、24.6項「ゾーンファイル」(393ページ)で説明するゾーンファイルの管理に関する項目を設定します。新しいゾーンの場合は、［*名前*］にゾーン名を入力します。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、［タイプ］(マスタ、スレーブ、または転送)を選択します。図24.2「DNSサーバのインストール:DNSゾーン」(379ページ)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、［*Edit*］をクリックします。ゾーンを削除するには、［*Delete*］をクリックします。

図 24.2　DNSサーバのインストール:DNSゾーン

3 最後のダイアログでは、［ファイアウォールで開いているポート］をクリックして、ファイアウォールのDNSポートを開くことができます。次に、ブート時にDNSサーバ を起動するかどうか(［オン］か、［オフ］か)を決定します。LDAPサポートを有効にすることもできます。詳細については、図24.3「DNSサーバのインストール:完了ウィザード」(380ページ)を参照してください。

図 24.3　DNSサーバのインストール:完了ウィザード



24.3.2 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。

24.3.2.1 起動

［*起動*］では、DNSサーバを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指定します。DNSサーバをすぐに起動するには、［［*今すぐDNSサーバを起動する*］を選択します。DNSサーバを停止するには、［［*今すぐDNSサーバを停止する*］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、今すぐDNSサーバをリロードする*］を選択します。 ファイアウォールのDNSポートを開くには［*ファイアウォール内でポートを開く*］を、

ファイアウォールの設定を変更するには［*Firewall Details*］をクリックします。

［*LDAPサポートを有効にする*］を選択すると、ゾーンファイルがLDAPデータベースによって管理されるようになります。ゾーンデータを変更してそれがLDAPデータベースに書き込まれると、設定を再ロードするように要求されます。DNSサーバを再起動すると、変更がすぐに反映されます。

24.3.2.2 フォワーダ

ローカルDNSサーバは、要求に応答できない場合、要求を［フォワーダ］に転送しようとします(そのように設定されている場合)。このフォワーダは、手動で、［*Forwarder List*］に追加できます。フォワーダが、ダイアルアップ接続でのように静的でない場合は、［*netconfig*］が設定を処理します。netconfigの詳細については、`man 8 netconfig`を参照してください。

24.3.2.3 基本的なオプション

このセクションでは、基本的なサーバオプションを設定します。［*オプション*］メニューから設定する項目を選択して、対応する入力フィールドに値を指定します。新しいエントリを追加するには、［*追加*］を選択してください。

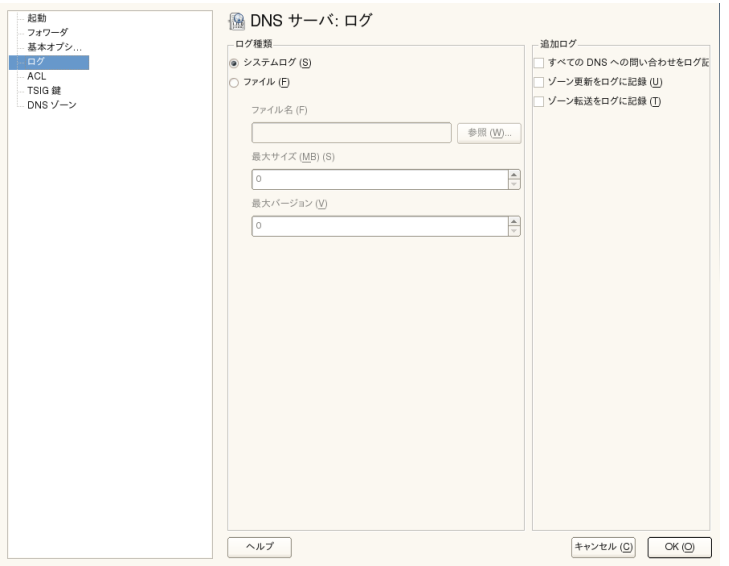
24.3.2.4 ログ

DNSサーバがログに記録する内容とログの方法を設定するには、［*ログ記録*］を選択します。［*Log Type*］に、DNSサーバがログデータを書き込む場所を指定します。システム全体のログファイル`/var/log/messages`を使用する場合は［*システムログ*］を、別のファイルを指定する場合は［*ファイル*］を選択します。別のファイルを指定する場合は、ファイル名、ログファイルの最大サイズ(メガバイト(MB))と保管するログファイル数(バージョン)も指定します。

［*追加ログ*］には、さらに詳細なオプションが用意されています。［*すべてのDNSクエリをログに記録*］を有効にすると、すべてのクエリがログに記録されるため、ログファイルが非常に大きくなる可能性があります。ですから、このオプションを有効にするのはデバッグ時だけにすることをお勧めします。DHCPサーバとDNSサーバ間でのゾーン更新時のデータトラフィックをログに記録するには、［*ゾーン更新をログに記録*］を有効にします。マスタからス

レーブへのゾーン転送時のデータトラフィックをログに記録するには、［ゾーン*転送をログに記録*］を有効にします。詳細については、図24.4「DNSサーバ:ログの記録」 (382 ページ)を参照してください。

図 24.4　DNSサーバ:ログの記録



24.3.2.5 ACL

このダイアログでは、アクセス制限を強制するACL(アクセス制御リスト)を定義します。［*名前*］に個別名を入力したら、次の形式で、［*値*］にIPアドレス(ネットマスクは省略可)を指定します。

```
{ 192.168.1/24; }
```

設定ファイルの構文に従って、アドレスの末尾にはセミコロンを付け、中カッコで囲む必要があります。

24.3.2.6 TSIGキー

TSIG (トランザクションシグネチャー)の主な目的は、DHCPおよびDNSサーバ間で安全な通信を行うことです。24.8項 「安全なトランザクション」 (398 ページ)を参照してください。

TSIGキーを生成するには、［キー*ID*］フィールドに個別名を入力し、キーを格納するファイルを［*ファイル名*］フィールドに入力します。［*生成*］をクリックすると、選択内容が確定されます。

作成済みのキーを使用するには、［キー*ID*］フィールドを空白のままにして、［*ファイル名*］で、そのキーが保存されているファイルを選択します。その後、［*追加*］をクリックすると、入力内容が確定されます。

24.3.2.7 DNSゾーン(スレーブゾーンの追加)

スレーブゾーンを追加するには、［*DNS*ゾーン］を選択し、ゾーンタイプに［スレーブ］を選択し、新規ゾーンの名前を書き込み、［*追加*］をクリックします。

［マスタ*DNS*サーバの*IP*］の下の［ゾーンエディタ］サブダイアログで、スレーブがデータをプル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。

24.3.2.8 DNSゾーン(マスタゾーンの追加)

マスタゾーンを追加するには、［*DNS*ゾーン］を選択し、ゾーンタイプに［マスタ］を選択し、新規ゾーンの名前を書き込み、［*追加*］をクリックします。マスタゾーンの追加時には、逆引きゾーンも必要です。たとえば、ゾーン`example.com`(サブネット`192.168.1.0/24`内のホストをポイントするゾーン)を追加する際には、カバーされるIPアドレス範囲の逆引きゾーンも追加する必要があります。定義上、このゾーンの名前は、`1.168.192.in-addr.arpa`となります。

24.3.2.9 DNSゾーン(マスタゾーンの編集)

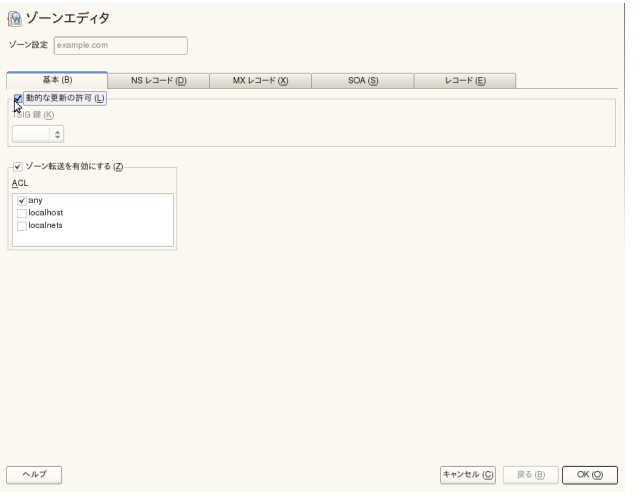
マスタゾーンを編集するには、［*DNS*ゾーン］を選択し、テーブルからマスタゾーンを選択し、［*編集*］をクリックします。このダイアログには、［*基本*］(最初に表示される)、［*NS*レコード］、［*MX*レコード］、［*SOA*］、および［*レコード*］のページがあります。

に示す基本ダイアログを使用すると、ダイナミックDNSの設定と、クライアントおよびスレーブネームサーバへのゾーン転送に関するアクセスオプションを定義できます。図24.5「DNSサーバ: ゾーンエディタ(基本)」 (384ページ)

ゾーンの動的更新を許可するには、［*動的アップデートの許可*］および対応するTSIGキーを選択します。このキーは、更新アクションの開始前に定義しておく必要があります。ゾーン転送を有効にするには、対応するACLを選択します。ACLは事前に定義しておく必要があります。

［基本］ダイアログで、ゾーン転送を有効にするかどうか選択します。リストされたACLを使用して、ゾーンをダウンロードできるユーザを定義します。

図 24.5 *DNSサーバ: ゾーンエディタ(基本)*



ゾーンエディタ(NSレコード)
: ［*レコード*］ダイアログでは、指定したゾーンの代替ネームサーバを定義できます。リストに自分が使用しているネームサーバが含まれていることを確認してください。レコードを追加するには、［*追加*するネームサーバ］にレコード名を入力し、［*追加*］をクリックして確定します。詳細については、図24.6「DNSサーバ:ゾーンエディタ(NSレコード)」 (385ページ)を参照してください。

図 24.6　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。詳細については、図24.7「DNSサーバ:ゾーンエディタ(MXレコード)」 (385 ページ)を参照してください。

図 24.7　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24.6「The /var/lib/named/example.comゾーンファイル」 (394 ページ)を参照してください。LDAPを介して管理される動的ゾーンの場合、SOAレコードの変更がサポートされないので注意してください。

図 24.8 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、次の例のように、Aレコードとは反対です。

```
hostname.example.com. IN A 192.168.0.1
1.0.168.192.in-addr.arpa IN PTR hostname.example.com.
```

注記: 逆引きゾーンの編集

正引きゾーンの追加後、メインメニューに戻って、編集用の逆引きゾーンを選択します。次に、タブ［基本］で、チェックボックス［*Automatically Generate Records From*］にチェック印を入れ、正引きゾーンを選択します。これにより、正引きゾーンでのすべての変更が、逆引きゾーンで自動的に更新されます。

24.4 BINDネームサーバの起動

SUSE® Linux Enterprise Serverシステムでは、ネームサーバBIND (*Berkeley Internet name domain*)は、事前設定されて提供されるので、インストールが正常に完了すればただちに起動できます。すで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、すで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、そのゾーンを設定してはじめて、正しいDNSにすることができます。簡単な例については、`/usr/share/doc/packages/bind/config`のドキュメントを参照してください。

ヒント: ネームサーバ情報の自動取得

インターネット接続やネットワーク接続のタイプによっては、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`ファイルの`NETCONFIG_DNS_POLICY`変数を`auto`に設定します。

ただし、公式のドメインは、その1つが責任のある機関によって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、rcnamed statusを使用して、サーバが実際に起動されていることを確認します。ネームサーバが起動しない場合、または予想しない動作をしている場合、多くはログファイル/var/log/messagesでその原因が明らかになります。

プロバイダのネームサーバ(またはすでにネットワーク上で動作しているネームサーバ)をフォワーダとして使用する場合は、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。に含まれているアドレスは、単なる例です。例24.1「named.confファイルの転送オプション」 (388 ページ)各自サイトの設定に合わせて変更してください。

例 24.1 *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; 192.168.1.116; };
        allow-query { 127/8; 192.168/16 };
        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。

24.5 The /etc/named.conf環境設定ファイル

BINDネームサーバ自体のすべての設定は、/etc/named.confファイルに格納されます。ただし、処理するドメインのゾーンデータ(ホスト名、IPアドレスなどで構成されている)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24.2「基本的な/etc/named.confファイル」 (389 ページ)に示します。

例 24.2 *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";
};
```

24.5.1 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192.168.1.116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 { 127.0.0.1; *ip-address*; }; 53
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`192.168.2.0/24`のように指定します。末尾の`/24`は、ネットマスクの短縮表記で、この場合`255.255.255.0`を表します。

allow-transfer ! *;;
: ゾーン転送を要求できるホストを制御します。この例では、`!`が使用されているので、ゾーン転送要求は完全に拒否されます。`*`. このエントリがなければ、ゾーン転送をどこからでも制約なしに要求できます。

statistics-interval 0;
: このエントリがなければ、BINDは1時間ごとに数行の統計情報を生成して`/var/log/messages`に保存します。0を指定すると、統計情報をまったく生成しないか、時間間隔を分単位で指定します。

cleaning-interval 720;
: このオプションは、BINDがキャッシュをクリアする時間間隔を定義します。キャッシュがクリアされるたびに、`/var/log/messages`にエントリが追加されます。時間の指定は分単位です。デフォルトは60分です。

statistics-interval 0;
: BINDは定期的にインタフェースを検索して、新しいインタフェースや存在しなくなったインタフェースがないか確認します。この値を`0`に設定すると、この検索が行われなくなり、BINDは起動時に検出されたインタフェースのみをリッスンします。0以外の値を指定する場合は分単位で指定します。デフォルトは60分です。

notify no;
: `no`に設定すると、ゾーンデータを変更したとき、またはネームサーバが再起動されたときに、他のネームサーバに通知されなくなります。

すべての利用可能なオプションのリストについては、マニュアルページ`man 5 named.conf`を参照してください。

24.5.2 ロギング

BINDでは、何を、どのように、どこにログ出力するかを詳細に設定できます。通常は、デフォルト設定のままで十分です。例24.3「ログを無効にするエ

ントリ」 (392 ページ)に、このエントリの最も簡単な形式、すなわちログをまったく出力しない例を示します。

例 24.3　ログを無効にするエントリ

```
logging {
        category default { null; };
};
```

24.5.3 ゾーンエントリ

例 24.4　example.comのゾーンエントリ

```
zone "example.com" in {
      type master;
      file "example.com.zone";
      notify no;
};
```

zoneの後、管理対象のドメイン名(example.com)を指定し、その後に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24.4「example.comのゾーンエントリ」 (392 ページ)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24.5「example.netのゾーンエントリ」 (392 ページ)参照)*。これが他のマスタのスレーブとなることもあります。

例 24.5　example.netのゾーンエントリ

```
zone "example.net" in {
      type slave;
      file "slave/example.net.zone";
      masters { 10.0.0.1; };
};
```

ゾーンオプション

type master;
: masterを指定して、BINDに対し、ゾーンがローカルネームサーバによって処理されるように指示します。これは、ゾーンファイルが正しい形式で作成されていることが前提となります。

type slave;
: このゾーンは別のネームサーバから転送されたものです。必ずmastersとともに使用します。

type hint;
: ルートネームサーバの設定には、ゾーン.(hintタイプ)を使用します。このゾーン定義はそのまま使用できます。

example.com.zoneファイルまたは「slave/example.net.zone」ファイル
: 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。スレーブの場合は、このデータを他のネームサーバから取得するので、このファイルは不要です。マスタとスレーブのファイルを区別するには、スレーブファイルにディレクトリslaveを使用します。

masters { *server-ip-address*; };
: このエントリは、スレーブゾーンにのみ必要です。ゾーンファイルの転送元となるネームサーバを指定します。

allow-update {! *; };
: このオプションは、外部書き込みアクセスを制御し、クライアントにDNSエントリへの書き込み権を付与することができます。ただし、これは通常、セキュリティ上の理由で好ましくありません。このエントリがなければ、ゾーンの更新は完全に拒否されます。!*によってそのような操作が禁止されるため、前述のエントリは同じものをアーカイブします。

24.6 ゾーンファイル

ゾーンファイルは2種類必要です。一方はIPアドレスをホスト名に割り当て、もう一方は逆にIPアドレスのホスト名を提供します。

ヒント: ゾーンファイルでのドット(ピリオド、フルストップ)の使用

フィルタフィールドの右側にある "."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。ネームサーバ設定エラーの原因として最も頻繁に挙げられるのは、おそらくピリオド「.」の打ち忘れや位置の間違いです。

最初に、ドメインexample.comの責任を負うゾーンファイルexample.com.zoneについて検討します(例24.6「The /var/lib/named/example.comゾーンファイル」 (394 ページ)参照)。

例 24.6 *The /var/lib/named/example.comゾーンファイル*

```
1.  $TTL 2D
2.  example.com. IN SOA      dns  root.example.com. (
3.                2003072441  ; serial
4.                1D          ; refresh
5.                2H          ; retry
6.                1W          ; expiry
7.                2D )        ; minimum
8.
9.                IN NS       dns
10.               IN MX       10 mail
11.
12. gate          IN A        192.168.5.1
13.               IN A        10.0.0.1
14. dns           IN A        192.168.1.116
15. mail          IN A        192.168.3.108
16. jupiter       IN A        192.168.2.100
17. venus         IN A        192.168.2.101
18. saturn        IN A        192.168.2.102
19. mercury       IN A        192.168.2.103
20. ntp           IN CNAME    dns
21. dns6          IN A6  0    2002:c0a8:174::
```

1行目:
$TTL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、先頭のexample.comです。この末尾には、「.」(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。この名前は、末尾に「.」(ピリオド)が付いていないので、dnsからdns.example.com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。@記号はすで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@example.comの場合、エントリはroot.example.com.となります。フィルタフィールドの右側にある"."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。ここでは、1週間です。

7行目:

SOAレコードの最後のエントリは、ネガティブキャッシュTTLです。これは、DNSクエリが解決できないという他のサーバからの結果をキャッシュしておく時間です。

9行目:

IN NSでは、このドメインを担当するネームサーバを指定します。dnsは、dns.example.comに拡張されます。これは、末尾に「.」が付いていないためです。このように、プライマリネームサーバと各セカンダリネームサーバに1つずつ指定する行がいくつかあります。/etc/named.confでnotifyをnoに設定しない限り、ゾーンデータが変更されると、ここにリストされているすべてのネームサーバにそれが通知されます。

10行目:

MXレコードは、ドメインexample.com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mail.example.comが指定されています。ホスト名の前の数字は、プリファレンス値です。複数のMXエントリが存在する場合、値が最も小さいメールサーバが最初に選択され、このサーバへのメール配信ができなければ、次に小さい値のメールサーバが試みられます。

行12–19:

これらは、ホスト名に1つ以上のIPアドレスが割り当てられている実際のアドレスレコードです。ここでは、名前が「.」なしでリストされています。これは、これらの名前にはドメインが含まれていないためです。したがって、これらの名前にはすべて、example.comが追加されます。ホストgateには、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AAAA が付きます。

注記: IPv6の構文

IPv6レコードの構文は、IPv4と少し異なっています。断片化の可能性があるため、アドレスの前に消失したビットに関する情報を入力する必要があります。IPv6アドレスを必要な数の「0」で満たすには、アドレス内の正しい位置に2つコロンを追加します。

```
pluto     AAAA 2345:00C1:CA11::1234:5678:9ABC:DEF0
pluto     AAAA 2345:00D2:DA11::1234:5678:9ABC:DEF0
```

20行目:
別名ntpをdnsのアドレス指定に使用できます(CNAMEは*canonical name(標準化名)*を意味する)。

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は、168.192.in-addr.arpaに解決されます。参照先 例24.7「逆引き」 (397 ページ)。

例 24.7 *逆引き*

```
1.  $TTL 2D
2.  168.192.in-addr.arpa.   IN SOA dns.example.com. root.example.com. (
3.                          2003072441      ; serial
4.                          1D              ; refresh
5.                          2H              ; retry
6.                          1W              ; expiry
7.                          2D )            ; minimum
8.
9.                          IN NS           dns.example.com.
10.
11. 1.5                     IN PTR          gate.example.com.
12. 100.3                   IN PTR          www.example.com.
13. 253.2                   IN PTR          cups.example.com.
```

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の逆引きを有効にします。Givenゾーン名は168.192.in-addr.arpaであり、これはホスト名に追加しません。そのため、すべてのホスト名はドメインの最後に「.」を付けた完全形式で入力します。残りのエントリは、前のexample.comの例で説明した通りです。

行3–7:
前のexample.comの例を参照してください。

9行目:
正引きの場合と同様、この行は、このゾーンを担当するネームサーバを指定します。ただし、ホスト名はドメインと末尾の「.」(ピリオド)が付いた完全な形で指定されます。

行 11–13:
これらはそれぞれのホスト上でのIPアドレスを示すポインタレコードです。IPアドレスの最後の部分のみが、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、ゾーン転送は、異なるバージョンのBIND間でも問題なく行えるはずです。

24.7 ゾーンデータの動的アップデート

動的アップデートという*用語は、マスタサーバのゾーンファイル内のエントリが追加、変更、削除される操作を指します*。この仕組みは、RFC 2136に記述されています。動的アップデートをゾーンごとに個別に構成するには、オプションのallow-updateルールまたはupdate-policyルールを追加します。動的に更新されるゾーンを手動で編集してはなりません。

サーバに更新エントリを転送するには、nsupdateコマンドを使用します。このコマンドの詳細な構文については、nsupdateのマニュアルページ(man8 nsupdate)を参照してください。セキュリティ上の理由から、こうした更新はTSIGキーを使用して実行するようにしてください(24.8項「安全なトランザクション」 (398 ページ)参照)。

24.8 安全なトランザクション

安全なトランザクションは、共有秘密キー(TSIGキーとも呼ばれる)に基づくトランザクション署名(TSIG)を使用して実現できます。ここでは、このキーの生成方法と使用方法について説明します。

安全なトランザクションは、異なるサーバ間の通信、およびゾーンデータの動的アップデートに必要です。アクセス制御をキーに依存する方が、単にIPアドレスに依存するよりもはるかに安全です。

TSIGキーの生成には、次のコマンドを使用します(詳細については、mandnssec-keygenを参照)。

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

これにより、次のような形式の名前を持つファイルが2つ作成されます。

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

キー自体(ejIkuCyyGJwwuN3xAteKgg==のような文字列)は、両方のファイルにあります。キーをトランザクションで使用するには、2番目のファイル(Khost1-host2.+157+34265.key)を、できれば安全な方法で(たとえばscpを使用して)、リモートホストに転送する必要があります。host1とhost2の間で安全な通信ができるようにするには、リモートサーバでキーを/etc/named.confファイルに含める必要があります。

```
key host1-host2 {
 algorithm hmac-md5;
 secret "ejIkuCyyGJwwuN3xAteKgg==";
};
```

警告: /etc/named.conf *のファイルパーミッション*

/etc/named.confのファイルパーミッションが適切に制限されていることを確認してください。このファイルのデフォルトのパーミッションは0640で、オーナーがroot、グループがnamedです。この代わりに、パーミッションが制限された別ファイルにキーを移動して、そのファイルを/etc/named.conf内にインクルードすることもできます。外部ファイルをインクルードするには、次のようにします。

```
include  "filename"
```

ここで、filenameには、キーを持つファイルへの絶対パスを指定します。

サーバhost1がhost2(この例では、アドレス10.1.2.3)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 10.1.2.3 {
  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。

24.9 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。

dnssec-signzoneコマンドを使用すると、生成されたキーのセット(keyset-ファイル)を作成し、それらを安全な方法で親ゾーンに転送し、署名することができます。これによって、/etc/named.conf内のゾーンごとにインクルードするファイルが生成されます。

24.10 詳細情報

ここで扱ったトピックの詳細については、*/usr/share/doc/packages/bind/*ディレクトリにインストールされるbind-docパッケージ内の『BIND Administrator Reference Manual』を参照してください。BINDに付属のマニュアルやマニュアルページで紹介されているRFCも、必要に応じて参照してください。/usr/share/doc/packages/bind/README.SuSEには、SUSE Linux Enterprise ServerのBINDに関する最新情報が含まれています。

25

DHCP

DHCP(*Dynamic Host Configuration Protocol*)の目的は、ネットワーク設定を各ワークステーションでローカルに行うのではなく、(サーバから)一元的に割り当てることです。DHCPを使用するように設定されたクライアントは、自身の静的アドレスを制御できません。サーバからの指示に従って、すべてが自動的に設定されるからです。クライアント側でNetworkManagerを使用する場合は、クライアントを設定する必要はありません。これは、環境を変更し、一度に1つのインタフェースしかない場合に便利です。DHCPサーバが実行しているマシン上ではNetworkManagerを使用しないでください。

ヒント: IBM System z:DHCPサポート

IBM System zプラットフォーム上では、OSAおよびOSA Expressネットワークカードを使用しているインタフェースに対してのみDHCPを使用できます。DHCPの自動環境設定機能に必要なMACアドレスを持つのは、これらのカードだけです。

DHCPサーバの設定方法の1つとして、ネットワークカードのハードウェアアドレス(ほとんどの場合、固定)を使用して各クライアントを識別し、そのクライアントがサーバに接続するたびに同じ設定を提供する方法があります。DHCPはサーバが用意したアドレスプールから、アドレスを各関連クライアントに動的に割り当てるように設定することもできます。後者の場合、DHCPサーバは要求を受信するたびに、接続が長期にわたる場合でも、クライアントに同じアドレスを割り当てようと試みます。これは、ネットワークにアドレス以上のクライアントが存在しない場合にのみ機能します。

DHCPは、システム管理者の負担を軽減します。サーバの環境設定ファイルを編集して、アドレスに関するあらゆる変更(大きな変更であっても)と一般的なネットワークの環境設定を一元的に実装できます。これは、多数のワークステーションをいちいち再設定するのに比べてはるかに簡単です。また、特に新しいコンピュータ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。

この章では、192.168.2.1をゲートウェイとし、DHCPサーバをワークステーション192.168.2.0/24と同じサブネットで実行します。このサーバは、固定IPアドレス192.168.2.254を持ち、2つのアドレス範囲(192.168.2.10～192.168.2.20および192.168.2.100～192.168.2.200)を操作対象とします。

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。

25.1 YaSTによるDHCPサーバの設定

DNSサーバをインストールするには、YaSTを起動して、［ソフトウェア］>［*ソフトウェア管理*］の順に選択します。［フィルタ］>［パターン］の順に選択してから、［*DHCPおよびDNSサーバ*］を選択します。依存関係のあるパッケージのインストールを確認して、インストールプロセスを完了します。

重要: LDAPのサポート

SUSE® Linux Enterprise DHCPモジュールは、サーバ設定をローカルに(DHCPサーバを実行するホスト上に)保存するか、その設定データをLDAPサーバに管理させるように、セットアップできます。LDAPを使用するには、LDAP環境を設定してからDHCPサーバを設定してください。

LDAPの詳細については、第4章 *LDAP—A Directory Service* (↑*Security Guide (セキュリティガイド)*)を参照してください。

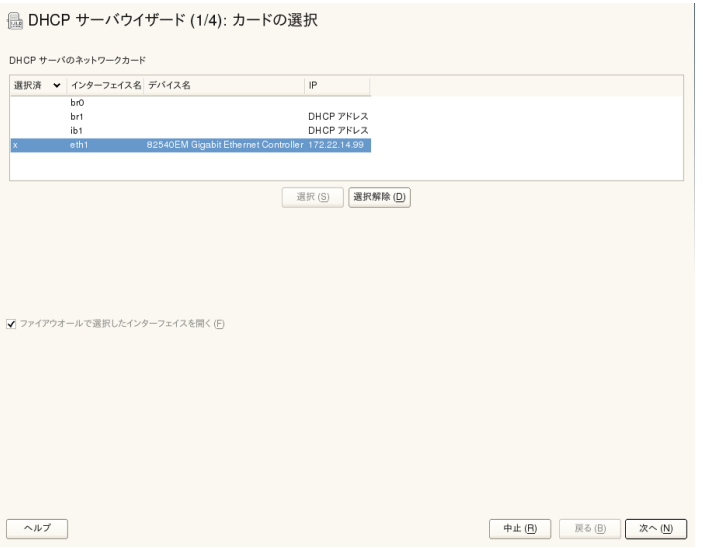
YaSTのDHCPモジュール(`yast2-dhcp-server`)を使用すると、ローカルネットワーク用に独自のDHCPサーバをセットアップできます。このモジュールは、ウィザードモードまたはエキスパート設定モードで実行できます。

25.1.1 初期設定(ウィザード)

このモジュールを初めて起動すると、ウィザードが開始して、サーバ管理に関していくつかの基本的な事項を決定するように要求されます。この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。次の手順に従います。

1 そのリストから、DHCPサーバがリスンするインタフェースを選択し、［*選択*］をクリックします。この後、［*選択したインタフェースのファイアウォールを開く*］を選択して、このインタフェース用のファイアウォールを開き、［*次へ*］をクリックします。詳細については、図25.1「DHCPサーバ:カードの選択」 (403 ページ)を参照してください。

図 25.1 DHCPサーバ:カードの選択



2 チェックボックスを使って、LDAPサーバがDHCP設定を自動的に格納する必要があるかどうかを指定します。エントリフィールドに、DHCPサーバで管理する全クライアントのネットワークを指定します。この指定には、ドメイン名、タイムサーバのアドレス、プライマリネームサーバとセカンダリネームサーバのアドレス、印刷サーバとWINSサーバのアドレス(Windowsクライアントと Linuxクライアントの両方が混在するネットワークを使用する場合)、ゲートウェイアドレスおよびリース期間が含まれます。詳細については、図25.2「DHCPサーバ:グローバル設定」 (404 ページ)を参照してください。

図 25.2　DHCPサーバ:グローバル設定

3 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アドレスを保持する期間を指定します。詳細については、図25.3「DHCPサーバ:ダイナミックDHCP」 (405 ページ)を参照してください。

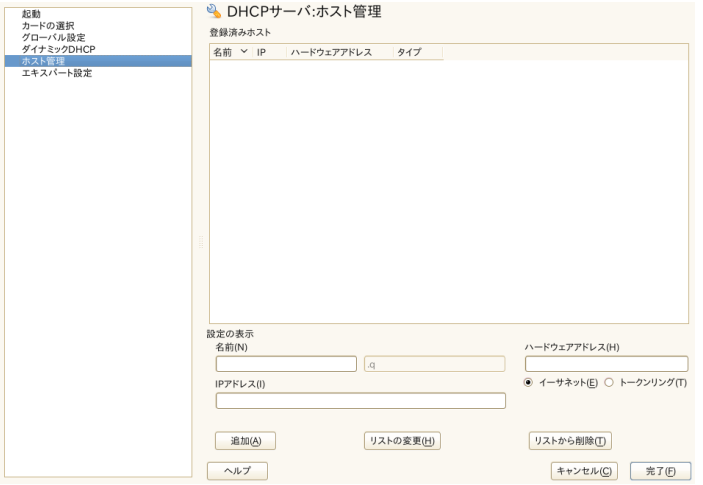
図 25.3　DHCPサーバ:ダイナミックDHCP

4 DHCPサーバ開始方法を定義します。システムのブート時にDHCPサーバを自動的に起動するか、必要に応じて(たとえば、テスト目的で)手動で起動するか指定します。［完了］をクリックして、サーバの環境設定を完了します。詳細については、図25.4「DHCPサーバ:起動」 (406 ページ)を参照してください。

図 25.4　DHCPサーバ:起動

5 前のステップで説明した方法で動的DHCPを使用するかわりに、アドレスを疑似静的方式で割り当てるようにサーバを設定することもできます。下部のエントリフィールドを使用して、この方法で管理するホストのリストを指定します。具体的には、［［*名前*］と［［*IPアドレス*］に、この種のクライアントに与える名前とIPアドレスを指定し、さらに［［*ハードウェアアドレス*］と［［*ネットワークタイプ*］(トークンリングまたはイーサネット)を指定します。上部に表示されるクライアントリストを修正するには、［［*追加*］、［［*編集*］、および［［*削除*］を使用します。詳細については、図25.5「DHCPサーバ:ホスト管理」(407 ページ)を参照してください。

図 25.5　DHCPサーバ:ホスト管理

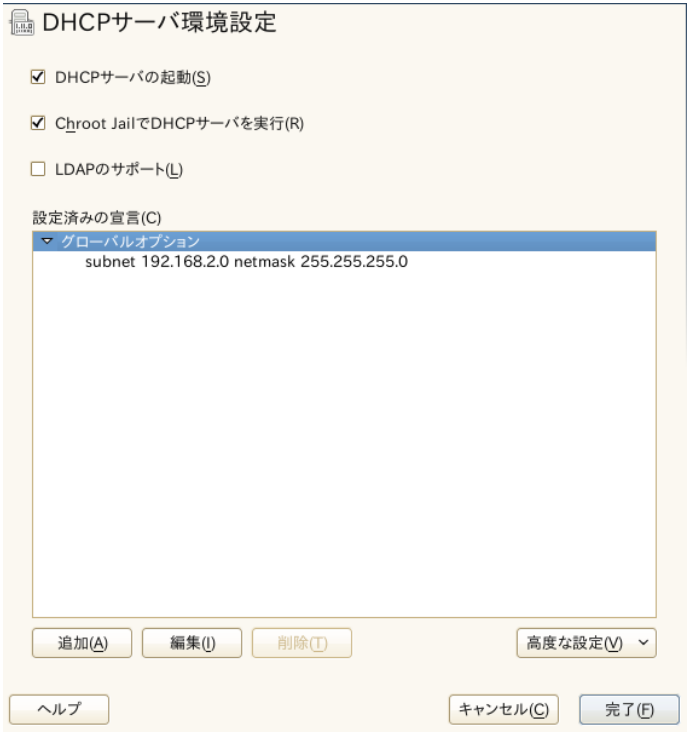


25.1.2 DHCPサーバ設定(エキスパート)

前述の環境設定方法に加えて、DHCPサーバのセットアップを詳細に変更できるようにエキスパート設定モードが用意されています。エキスパート環境設定を開始するには、［スタートアップ］ダイアログの［*DHCPサーバエキスパート環境設定*］をクリックします(図25.4「DHCPサーバ:起動」 (406 ページ)を参照)。

chroot環境と宣言
: この最初のダイアログで［*DHCPサーバの起動*］を選択し、既存の環境設定を編集可能にします。DHCPサーバの動作のうち、重要なのはchroot環境またはchroot jailで動作してサーバホストを保護する機能です。DHCPサーバが外部からの攻撃にさらされるとしても、攻撃者はchroot jailの中にとどまるためシステムの残りの部分には進入できません。ダイアログの下部には、定義済みの宣言を示すツリービューが表示されます。これらの修正には、［*追加*］、［*削除*］、および［*編集*］を使用します。［*詳細*］を選択すると、上級者用のダイアログが追加表示されます。図25.6「DHCPサーバ:Chroot Jailと宣言」 (408 ページ)を参照してください。 ［*追加*］を選択後、追加する宣言の種類を定義します。［*詳細*］から、サーバのログファイルの表示、TSIGキー管理の設定、およびDHCPサーバのセットアップに応じたファイアウォール設定の調整を行うことができます。

図 25.6　DHCPサーバ:Chroot Jailと宣言



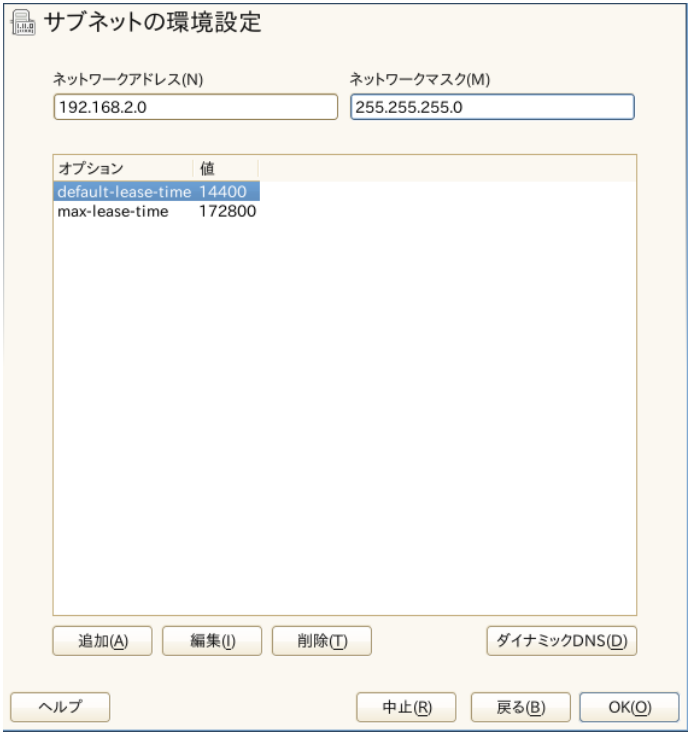
宣言タイプの選択

DHCPサーバの［*グローバルオプション*］は、多数の宣言で構成されています。このダイアログでは、宣言タイプ［サブネット］、［ホスト］、［*共有ネットワーク*］、［*グループ*］、［アドレスプール］、および［クラス］を設定できます。この例は、新しいサブネットワークの選択を示しています(図25.7「DHCPサーバ:宣言タイプの選択」 (409 ページ)を参照)。

図 25.7　DHCPサーバ:宣言タイプの選択

サブネットの設定
　このダイアログでは、IPアドレスとネットマスクを使用して新しいサブネットを指定できます。ダイアログの中央部分で［*追加*］、［*編集*］、および［*削除*］を使用して、選択したサブネットのDHCPサーバ起動オプションを変更します。サブネットのダイナミックDNSを設定するには、［ダイナミック*DNS*］を選択します。

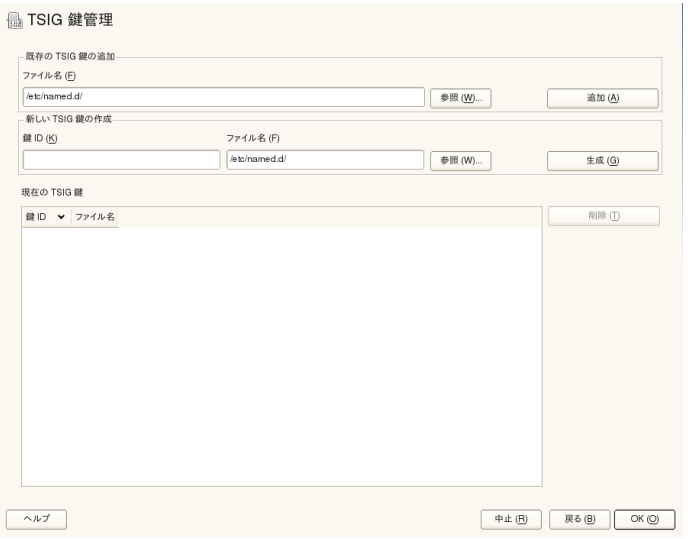
図 25.8　DHCPサーバ:サブネットの設定



TSIGキー管理

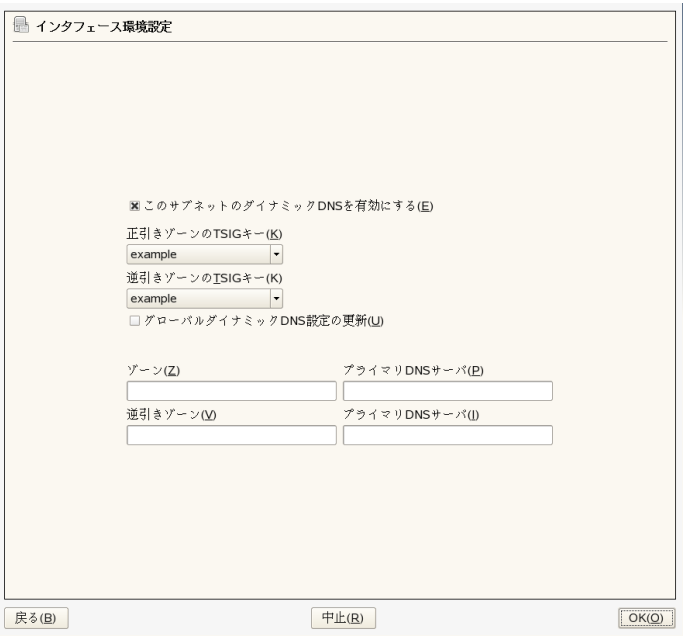
前のダイアログでダイナミックDNSを設定するように選択した場合は、セキュアゾーン転送用のキー管理を設定できます。［*OK*］を選択すると別のダイアログが表示され、ダイナミックDNSのインタフェースを設定できます(図25.10「DHCPサーバ:ダイナミックDNS用のインタフェースの設定」 (412 ページ)を参照)。

図 25.9　DHCPサーバ:TSIGの設定



ダイナミックDNS:インタフェースの設定
: ここでは、［*このサブネットでダイナミックDNSを有効にする*］を選択して、サブネットのダイナミックDNSを有効化できます。その後、ドロップダウンリストを使用して正引きゾーンと逆引きゾーン両方のTSIGキーを選択し、そのキーがDNSとDHCPサーバに共通であることを確認します。［*グローバルダイナミックDNS設定の更新*］を使用すると、ダイナミックDNS環境に従ってグローバルDHCPサーバ設定を自動的に更新および調整できます。最後に、ダイナミックDNSに従って更新する正引きゾーンと逆引きゾーンについて、プライマリネームサーバの名前を個別に指定し、この2つのゾーンを定義します。［*OK*］を選択すると、サブネットの設定ダイアログに戻ります(図25.8「DHCPサーバ:サブネットの設定」(410ページ)を参照)。［［*OK*］を選択すると、エキスパート設定ダイアログに戻ります

図 25.10　DHCPサーバ:ダイナミックDNS用のインタフェースの設定



ネットワークインタフェースの環境設定

DHCPサーバがリスンするインタフェースを定義し、ファイアウォール設定を調整するには、［エキスパート環境設定］ダイアログで［*詳細*］>［*インタフェースの設定*］の順に選択します。表示されるインタフェースリストから、DHCPサーバがリッスンするインタフェースを1つ以上選択します。すべてのサブネット内のクライアントがサーバと通信できるようにする必要があり、サーバホストでもファイアウォールを実行する場合は、ファイアウォールを適宜調整してください。調整するには、［*Adapt Firewall Settings(ファイアウォール設定の調整)*］を選択します。設定を完了した後、［*OK*］をクリックして元のダイアログに戻ると、YaSTがSuSEfirewall2のルールを、新しい条件に調整します(図25.11「DHCPサーバ:ネットワークインタフェースとファイアウォール」 (413 ページ)を参照)。

図 25.11　DHCPサーバ:ネットワークインタフェースとファイアウォール

設定ステップをすべて完了した後、［*OK*］を選択してダイアログを閉じます。これでサーバは新規環境設定に従って起動します。

25.2 DHCPソフトウェアパッケージ

お使いの製品では、DHCPサーバとDHCPクライアントのどちらも利用できます。用意されているDHCPサーバは、Internet Systems Consortiumによって公開されたdhcpdです。クライアント側で、`dhcp-client`(ISCから)または`dhcpcd`パッケージにあるDHCPクライアントデーモンの、いずれかのDHCPクライアントプログラムを選択します。

デフォルトでは、`dhcpcd`がインストールされています。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 `dhcp-client`を使用します。

25.3 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25.1「環境設定ファイル/etc/dhcpd.conf」 (414 ページ)で、`/etc/dhcpd.conf`ファイルの基本的な例を見てみましょう。

例 25.1 *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 "example.com";
option domain-name-servers 192.168.1.116;
option broadcast-address 192.168.2.255;
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0
 {
  range 192.168.2.10 192.168.2.20;
  range 192.168.2.100 192.168.2.200;
 }
```

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。

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サーバがコンピュータにIPアドレスを割り当てた場合に、コンピュータ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、第24章 *ドメインネームシステム* (375ページ)を参照してください。

- option broadcast-addressの行は、要求しているクライアントで使用されるブロードキャストアドレスを定義します。

- option routersの行では、ローカルネットワークでホストに配信できないデータパケットの送信先を(指定されたソース/ターゲットホストアドレスおよびサブネットに応じて)が指定されます。ほとんどの場合、特に小規模ネットワークでは、このルータはインターネットゲートウェイと同一です。

- option subnet-maskでは、クライアントに割り当てるネットマスクを指定します。

ファイルの最後のセクションでは、サブネットマスクを含め、ネットワークを定義します。最後に、DHCPが対象のクライアントにIPアドレスを割り当てるために使用するアドレス範囲を指定します。例25.1「環境設定ファイル/etc/dhcpd.conf」 (414 ページ)では、クライアントに、192.168.2.10と192.168.2.20の間および192.168.2.100と192.168.2.200の間の任意のアドレスを与えることができます。

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。rcdhcpd check-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 Enterprise Serverシステムでは、セキュリティ上の理由から、chroot環境でDHCPデーモンを起動します。デーモンが見つけられるように、環境設定ファイルは、chroot環境にコピーします。このファイルは、rcdhcpd startコマンドによって自動的にこのファイルがコピーされるので、通常は、手動でコピーする必要はありません。

25.3.1 固定IPアドレスを持つホスト

DHCPは、事前定義の静的アドレスを特定のクライアントに割り当てる場合にも使用できます。明示的に割り当てられるアドレスは、プールから割り当てられる動的アドレスに常に優先します。たとえばアドレスが不足していて、サーバがクライアント間でアドレスを再配布する必要がある場合でも、静的アドレスは動的アドレスと違って期限切れになりません。

静的アドレスを使用して設定されるクライアントを識別するために、dhcpdは、ハードウェアアドレス(6つのオクテットペアから成るグローバルにユニークな固定数値コード)を使用して、すべてのネットワークデバイスを識別します(たとえば、`00:30:6E:08:EC:80`)。たとえば、例25.2「環境設定ファイルへの追加」 (416 ページ)のような数行を例25.1「環境設定ファイル/etc/dhcpd.conf」 (414 ページ)に示す環境設定ファイルに追加すると、DHCPデーモンはあらゆる状況で、対応するホストに同じデータのセットを割り当てます。

例 25.2 *環境設定ファイルへの追加*

```
host jupiter {
hardware ethernet 00:30:6E:08:EC:80;
fixed-address 192.168.2.100;
}
```

クライアントの名前を1行目に(`host`*`hostname`*(ここでは`jupiter`に置き換わる）)、MACアドレスを2行目に入力します。LinuxホストでMACアドレスを確認するには、`ip link show`コマンドの後にネットワークデバイス(たとえば、`eth0`)を指定して実行します。出力例を次に示します。

```
link/ether 00:30:6E:08:EC:80
```

上の例では、MACアドレス`00:30:6E:08:EC:80`のネットワークカードが搭載されたクライアントに、IPアドレス`192.168.2.100`とホスト名`jupiter`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。

25.3.2 SUSE Linux Enterprise Serverバージョン

セキュリティ向上のため、ISC DHCPサーバのSUSE Linux Enterprise Serverバージョンは、Ari Edelkind氏開発の非root/chrootパッチが適用されて出荷されます。これにより、dhcpdをユーザID `nobody`で実行したり、chroot環境で実行したりできます(`/var/lib/dhcp`)。こ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、`etc/sysconfig/dhcpd`ファイルの`DHCPD_CONF_INCLUDE_FILES`変数で、これらのファイルを設定します。syslog-ngデーモンの再起動後もDHCPロギング機能が継続して動作するようにするには、`/etc/sysconfig/syslog`ファイル内の`SYSLOGD_ADDITIONAL_SOCKET_DHCP`エントリを指定します。

25.4 詳細情報

DHCPの詳細については、*Internet Systems 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のマニュアルページにも詳細が記載されています。

26 NetworkManagerの使用

NetworkManagerは、ラップトップなどの携帯用コンピュータのための理想的ソリューションです。NetworkManagerは、802.1x保護ネットワークへの接続など、ネットワーク接続のための最新の暗号化タイプおよび標準をサポートしています。802.1Xは、「IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control」(ポートごとにネットワークアクセスの制御を行う、ローカル/メトロポリタンエリアネットワーク向けIEEE標準)です。NetworkManagerを使用すれば、ネットワークインタフェースの設定や移動時の有線/無線ネットワーク間の切り換えにわずらわされる必要がなくなります。NetworkManagerでは、既知の無線ネットワークに自動的に接続するか、または複数のネットワーク接続を並行して管理できます。後者の場合、最も高速な接続がデフォルトとして使用されます。さらに、利用可能なネットワーク間を手動で切り換えたり、システムトレイのアプレットを使用してネットワーク接続を管理できます。

単一の接続をアクティブにする代わりに、複数の接続を一度にアクティブにできます。これにより、Ethernetからラップトップの接続プラグを抜いても、無線接続により接続が維持されます。

26.1 NetworkManagerの使用

NetworkManagerは、高度で直感的なユーザインタフェースを提供します。このインタフェースを使用すると、ネットワーク環境を簡単に切り換えることができます。ただし、NetworkManagerは、次の場合には適しません。

- コンピュータが、DHCPまたはDNSサーバなど、ネットワーク内で他のコンピュータにネットワークサービスを提供している場合。
- コンピュータがXenサーバの場合、またはシステムがXen内の仮想システムである場合。

26.2 NetworkManagerの有効化と無効化

ラップトップコンピュータでは、 NetworkManagerがデフォルトで有効です。ただし、YaSTネットワーク設定モジュールでいつでも有効または無効にできます。

1 YaSTを実行し、［*ネットワークデバイス*］>［*Network Settings*］の順に選択します。

2 ［*Network Settings*］ダイアログが開きます。［*グローバルオプション*］タブを開きます。

3 NetworkManagerを使用してネットワーク接続を設定および管理するには、以下の手順を実行します。

3a ［*ネットワークのセットアップ方法*］フィールドで、［*NetworkManagerを使ってユーザが制御*］を選択します。

3b ［*OK*］をクリックしてYaSTを閉じます。

3c 26.3項 「ネットワーク接続の設定」 (421 ページ)に従って、NetworkManagerを使用してネットワーク接続を設定します。

4 NetworkManagerを無効にして従来の方法でネットワークを制御するには、以下の手順を実行します。

4a ［*ネットワークのセットアップ方法*］フィールドで、［*ifupを使用した従来の方法*］

4b ［*OK*］をクリックします。

4c DHCP経由の自動環境設定または静的IPアドレスによる手動設定で、YaSTでネットワークカードを設定します。別の方法として、YaSTを使用してモデムを設定します。

- ダイヤルアップ接続の場合は、［ネットワークデバイス］>［モデム］を使用します。
- 内部またはUSB ISDNモデムを設定するには、［ネットワークデバイス］>［*ISDN*］の順に選択します。
- 内部またはUSB DSLモデムを設定するには、［ネットワークデバイス］>［*DSL*］の順に選択します。

YaSTを使用したネットワーク接続の詳細については、21.4項 「YaSTによるネットワーク接続の設定」 (307 ページ)および第18章 *無線LAN* (245 ページ)を参照してください。

26.3 ネットワーク接続の設定

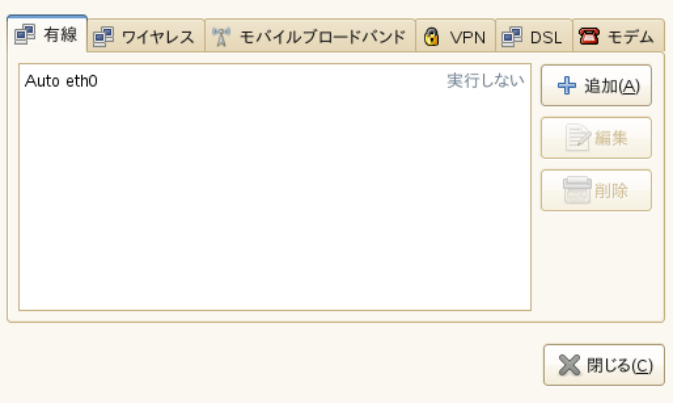
YaSTでNetworkManagerを有効にした後、KDEおよびGNOMEで使用可能なNetworkManagerフロントエンドでネットワーク接続を設定します。両フロントエンドのネットワーク設定ダイアログは非常に似ています。有線、無線、モバイルブロードバンド、DSL、およびVPN接続など、あらゆるタイプのネットワーク接続に対応するタブが表示されます。各タブで、該当するタイプの接続の追加、編集、または削除を行うことができます。KDE設定ダイアログでは、接続タイプがシステムで使用可能であれば(ハードウェアおよびソフトウェアによる)、適切なタブのみがアクティブになります。また、KNetworkManagerではデフォルトで、各タブで使用可能な入力フィールドおよびオプションに対して包括的なツールヒントが表示されます。

注記: **Bluetooth**接続

現在、Bluetooth接続は、NetworkManagerでは設定できません。

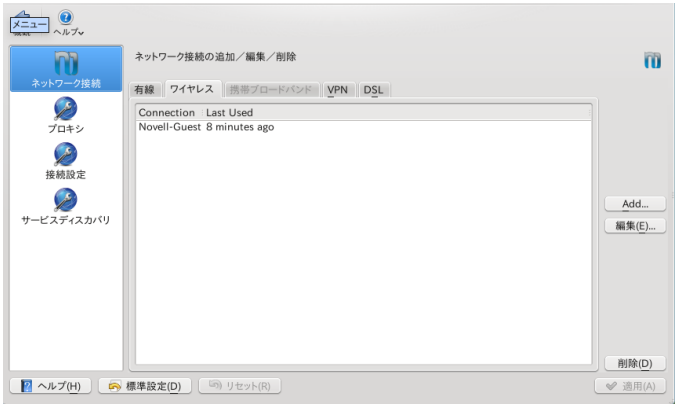
GNOMEでネットワーク設定ダイアログを開くには、メインメニューを開き、右側にある［ネットワーク］エントリをクリックします。その代わり、Alt + F2を押して`nm-connection-editor`を入力するか、GNOMEコントロールセンターで［システム］>［*ネットワーク接続*］の順に選択します。

図 26.1　GNOMEネットワーク接続のダイアログ



KDEを使用している場合は、メインメニューを開き、［*デスクトップの設定*］をクリックします。［*個人設定*］で、［*一般*］タブの［*ネットワークの設定*］を選択し、ネットワーク設定ダイアログを開きます。

図 26.2　KDEネットワーク設定ダイアログ



システムトレイにあるNetworkManagerアプレットから設定ダイアログを起動することもできます。KDEでは、アイコンを左クリックし、［*接続の管理*］を選択します。GNOMEでは、アイコンを右クリックし、［*接続の編集*］を選択します。

注記: オプションの可用性

システムセットアップによっては、接続を設定できない場合があります。安全な環境では、一部のオプションがロックされているか、またはroot許可を必要とする場合があります。詳細は、システム管理者にお問い合わせください。

手順 26.1 *接続の追加または編集*

NetworkManagerでネットワーク接続を設定する場合、すべてのユーザが共有できるシステム接続を定義することもできます。ユーザ接続とは対照的に、システム接続は、NetworkManagerの起動直後、ユーザがログインする前に使用可能になります。両タイプの接続について詳細は、26.7.1項「ユーザおよびシステムの接続」 (433 ページ)を参照してください。

現在、KDEではsystem connectionオプションは使用できません。システム接続を設定するには、この場合はYaSTを使用する必要があります。

注記: 非表示のネットワーク

「隠れた」ネットワーク(サービスをブロードキャストしないネットワーク)に接続するには、そのネットワークのSSID (Service Set Identifier)またはESSID (Extended Service Set Identifier)を知っている必要があります。隠れたネットワークは、自動的に検出できません。

1. ネットワーク設定のダイアログで、使用したい接続タイプのタブをクリックします。
2. ［*追加*］をクリックして新しい接続を作成するか、既存の接続を選択して［*編集*］をクリックします。
3. ［*接続名*］および接続の詳細を入力します。
4. 非表示のネットワークでは、ESSIDおよび暗号化パラメータを入力します。
5. 1つの接続タイプについて複数の物理デバイスが使用可能な場合(たとえば、コンピュータに2つのethernetカードまたは2つの無線カードが取り付けられている場合)、特定のデバイスに接続を関連付けることができます。

KDEを使用している場合は、このために［*インタフェースの制限*］オプションを使用します。GNOMEを使用する場合は、接続を関連付けるデバイスの［*MACアドレス*］を入力し、設定を確認します。

6 NetworkManagerが自動的に特定の接続を使用するようにするには、この接続に対してオプション［*Connect Automatically*］(KDEの場合)または［*Stay connected when possible*］(GNOMEの場合)を有効にします。

7 接続をシステム接続にするには、［*すべてのユーザが使用可能*］を有効にします(GNOME)。システム接続を作成および編集するには、`root`パーミッションが必要です。

変更を確定した後、NetworkManagerアプレットを左クリックすると、新たに設定されたネットワーク接続が使用可能なネットワークのリストに表示されます。

図 26.3　KNetworkManager - 設定済みおよび使用可能な接続

26.4 KNetworkManagerの使用

NetworkManager向けKDEフロントエンドは、KNetworkManagerアプレットです。ネットワークがNetworkManagerコントロール用に設定されている場合、通常、アプレットはデスクトップ環境とともに自動的に起動し、システムトレイにアイコンとして表示されます。

システムトレイにネットワーク接続アイコンが表示されない場合は、おそらくアプレットが起動していません。アプレットを手動で起動するには、Alt + F2を押し、「`knetworkmanager`」を入力します。

KNetworkManagerでは、接続を設定した無線ネットワークのみが表示されます。無線ネットワークの範囲外である場合またはネットワークケーブルが接

続されていない場合は接続が非表示になります。したがって、使用される接続を示す明確なビューが常に提示されます。

26.4.1 有線ネットワーク接続の管理

コンピュータがネットワークケーブルで既存のネットワークに接続している場合、KNetworkManagerアプレットを使用してネットワーク接続を選択します。

1 アプレットアイコンで左クリックすると、使用可能なネットワークがメニューに表示されます。現在使用されている接続は、このメニューで選択され、［アクティブ］としてマークされます。

2 有線ネットワークで異なる設定を使用する場合は、［*接続の管理*］をクリックし、手順26.1「接続の追加または編集」(423ページ)の説明に従って別の有線接続を追加します。

3 KNetworkManagerアイコンをクリックし、新たに設定した接続を選択してアクティブにします。

26.4.2 無線ネットワーク接続の管理

KNetworkManagerではデフォルトで、接続を設定した無線ネットワークのうち、使用可能であり表示可能であるネットワークのみが表示されます。最初に無線ネットワークに接続するには、次の手順に従います。

手順 26.2 *ワイヤレスネットワークへの接続*

1 アプレットアイコンを左クリックし、［*ネットワーク接続の作成*］を選択します。KNetworkManagerには、信号強度およびセキュリティの詳細を含めて、使用可能であり表示可能な無線ネットワークのリストが表示されます。

2 表示可能なネットワークに接続するには、リストからネットワークを選択し、［*接続*］をクリックします。ネットワークが暗号化されている場合は、ダイアログが開きます。ネットワークが使用する［セキュリティ］のタイプを選択し、適切な資格情報を入力します。

3 サービスセット識別子(SSIDまたはESSID)をブロードキャストしないため自動的に検出されないネットワークに接続するには、［*WLANを使用して他のネットワークに接続*］を選択します。

4 表示されるダイアログでSSIDまたはESSIDを入力し、必要に応じて暗号化パラメータを設定します。

5 変更を確認し、［*OK*］をクリックします。NetworkManagerで、新しい接続がアクティブになります。

6 接続を終了し、無線ネットワークを無効にするには、アプレットアイコンをクリックし、［*ワイヤレスの有効化*］のチェックをオフにします。飛行機内など、ワイヤレスネットワーキングが使用できない環境にいる場合は、この設定が役に立つことがあります。

明示的に選択された無線ネットワークは、可能な限り接続が維持されます。その時点でネットワークケーブルが接続されていれば、無線接続の稼動中に、［*自動的に接続*］に設定したすべての接続が確立されます。

26.4.3 ワイヤレスカードのアクセスポイントとしての設定

お使いのワイヤレスカードでアクセスポイントモードがサポートされている場合、NetworkManagerを使用して設定できます。

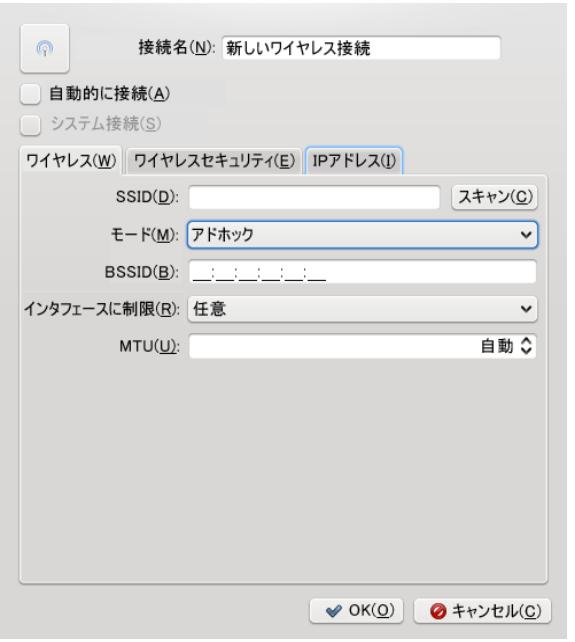
注記: オプションの可用性

システムセットアップによっては、接続を設定できない場合があります。安全な環境では、一部のオプションがロックされているか、または`root`許可を必要とする場合があります。詳細は、システム管理者にお問い合わせください。

---

1 KNetworkManagerアプレットをクリックし、［*ネットワーク接続の作成*］>［*新しいアドホックネットワーク*］の順に選択します。

2 次の設定ダイアログで、［*SSID*］フィールドにネットワークの名前を入力します。



3 ［*無線セキュリティ*］タブで暗号化を設定します。

重要: 保護されていないワイヤレスネットワークによるセキュリティリスク

［*Security*］を［なし］に設定した場合、誰でもネットワークに接続し、コネクティビティを再利用し、ネットワーク接続を傍受できるようになります。アクセスをアクセスポイントに制限して接続を安全なものにするには、暗号化を使用します。さまざまなWEP/WPAベースの暗号化を選択できます。いずれのテクノロジが最適であるか不明な場合は、18.3項「認証」 (247 ページ)を参照してください。

4 ［*IPアドレス*］タブで、［*設定*］オプションが［*共有*］(アドホックネットワークのデフォルトオプション)に設定されていることを確認します。

5 入力した設定を確認して、［［*OK*］をクリックします。

26.4.4 KNetworkManagerのカスタマイズ

KNetworkManager:のさまざまな要素(システムトレイに表示するアイコンの数、表示するツールヒント、およびネットワーク接続のパスワードと資格情報を保存する方法)をカスタマイズできます。最後の要素についての詳細は、26.7.2項 「パスワードと資格情報の保存」 (434 ページ)を参照してください。

使用可能なオプションを探すには、NetworkManagerシステムトレイアイコンを右クリックし、設定ダイアログの左側で、［*接続の管理*］を選択して［*その他*］をクリックします。

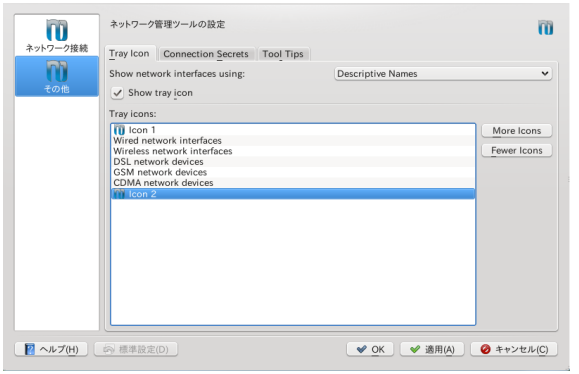
手順 26.3 *KNetworkManagerの複数のトレイアイコンの構成*

KNetworkManagerでは、複数の接続を同時にアクティブに維持できるので、複数の接続の接続状態に関する情報を一度に表示できれば便利です。システムトレイで、それぞれが異なる接続タイプグループを表す複数のNetworkManagerアイコンを使用することにより、これが可能になります(たとえば、有線接続について1つのアイコン、無線接続について別のアイコンを使用します)。

1 設定ダイアログで、［*トレイアイコン*］タブに切り替えます。

2 ［*追加アイコン*］をクリックします。新しいアイコンエントリがリストに表示されます。

3 このアイコンによって表されるネットワーク接続タイプを選択し、対応するアイコンでグループ化します。



4 変更内容を確認します。

これでシステムトレイには複数のNetworkManagerアイコンが表示され、そこからアイコンに関連付けられた接続タイプにアクセスできます。

KNetworkManagerではまた、手順26.1「接続の追加または編集」 (423 ページ)の説明に従ってネットワーク接続を設定すると、この接続に対して表示されたアイコンをカスタマイズできます。アイコンを変更するには、［*接続名*］の隣にあるアイコンボタンをクリックし、次のダイアログで目的のアイコンを選択します。変更を確認した後、システムトレイのKNetworkManagerアイコンをクリックすることにより、使用可能な接続のリストに新しいアイコンが表示されます。

26.5 GNOME NetworkManagerアプレットの使用

In GNOMEでは、NetworkManagerはGNOME NetworkManagerアプレットを使用して制御できます。ネットワークがNetworkManagerコントロール用に設定されている場合、通常、アプレットはデスクトップ環境とともに自動的に起動し、システムトレイにアイコンとして表示されます。

システムトレイにネットワーク接続アイコンが表示されない場合は、おそらくアプレットが起動していません。アプレットを手動で起動するには、Alt + F2を押し、「`nm-applet`」を入力します。

26.5.1 有線ネットワーク接続の管理

コンピュータがネットワークケーブルで既存のネットワークに接続している場合、NetworkManagerアプレットを使用してネットワーク接続を選択します。

1 アプレットアイコンで左クリックすると、使用可能なネットワークがメニューに表示されます。メニューでは、現在使用されている接続が選択されています。

2 別のネットワークに切り替えるには、リストから選択します。

3 有線と無線のすべてのネットワーク接続を切り替えるには、アプレットアイコンを右クリックして［*Enable Networking*］を選択解除します。

26.5.2 無線ネットワーク接続の管理

使用可能な可視のワイヤレスネットワークは、［*Wireless Networks*］の下のGNOME NetworkManagerアプレットメニューにリストされます。各ネットワークの信号強度もメニューに表示されます。暗号化された無線ネットワークには、シールドアイコンが付きます。

手順 26.4 *ワイヤレスネットワークへの接続*

1 ワイヤレスネットワークに接続するには、アプレットアイコンを左クリックして、使用できるワイヤレスネットワークのリストからエントリを選択します。

2 ネットワークが暗号化されている場合は、ダイアログが開きます。ネットワークで使用されている暗号化のタイプ(［*無線セキュリティ*］)が示され、対応する暗号化および認証設定に従って入力フィールド数が維持されます。適切な資格情報を入力します。

3 サービスセット識別子(SSIDまたはESSID)をブロードキャストしないため自動的に検出されないネットワークに接続するには、NetworkManagerアイコンを左クリックし、［*非表示の無線ネットワークへの接続*］を選択します。

4 表示されるダイアログの［*ネットワーク名*］に、SSIDまたはESSIDを入力し、必要に応じて暗号化パラメータを設定します。

5 ワイヤレスネットワーキングを無効にするには、アプレットアイコンで右クリックし、［*ワイヤレスの有効化*］のチェックを外します。飛行機内など、ワイヤレスネットワーキングが使用できない環境にいる場合は、この設定が役に立つことがあります。

明示的に選択された無線ネットワークは、可能な限り接続が維持されます。その時点でネットワークケーブルが接続されていれば、無線接続の稼働中に、［*Stay connected when possible*］に設定したすべての接続が確立されます。

26.5.3 ワイヤレスカードのアクセスポイントとしての設定

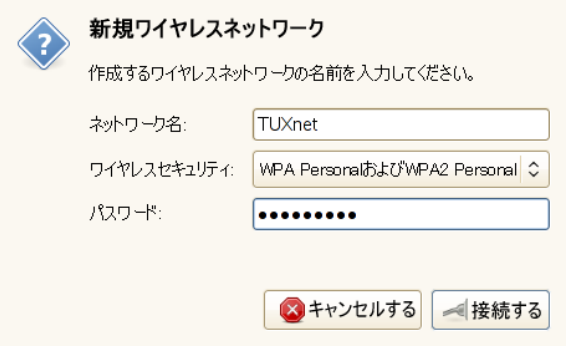
お使いのワイヤレスカードでアクセスポイントモードがサポートされている場合、NetworkManagerを使用して設定できます。

注記: オプションの可用性

システムセットアップによっては、接続を設定できない場合があります。安全な環境では、一部のオプションがロックされているか、またはroot許可を必要とする場合があります。詳細は、システム管理者にお問い合わせください。

---

1 NetworkManagerアプレットをクリックし、［*新しい無線ネットワークを作成*］を選択します。



2 ［ネットワーク名］に入力し、［*無線セキュリティ*］ドロップダウンリストで使用する暗号化を設定します。

重要: 保護されていないワイヤレスネットワークによるセキュリティリスク

［*Wireless Security*］を［なし］に設定した場合、誰でもネットワークに接続し、コネクティビティを再利用し、ネットワーク接続を傍受できるようになります。アクセスをアクセスポイントに制限して接続を安全なものにするには、暗号化を使用します。さまざまなWEP/WPAベースの暗

号化を選択できます。いずれのテクノロジが最適であるか不明な場合は、18.3項 「認証」 (247 ページ)を参照してください。

26.6 NetworkManagerとVPN

NetworkManagerは、数種類のVPN(Virtual Private Network)技術をサポートしています. 各技術について、SUSE Linux Enterprise ServerにはNetworkManagerの一般的なサポートを提供する基本パッケージが付属しています。加えて、アプレットに対応するデスクトップ固有のパッケージをインストールすることも必要です。

NovellVPN
このVPN技術を使用するには、次のアイテムをインストールします:

- `NetworkManager-novellvpn`、および
- `NetworkManager-novellvpn-kde4`または `NetworkManager-novellvpn-gnome`

NovellVPNサポート(KDE用)はまだ利用できませんが、現在準備中です。

OpenVPN
このVPN技術を使用するには、次のアイテムをインストールします:

- `NetworkManager-openvpn`、および
- `NetworkManager-openvpn-kde4`または `NetworkManager-openvpn-gnome`

vpnc (Cisco)
このVPN技術を使用するには、次のアイテムをインストールします:

- `NetworkManager-vpnc`、および
- `NetworkManager-vpnc-kde4`または `NetworkManager-vpnc-gnome`

PPTP(ポイントツーポイントトンネリングプロトコル)
このVPN技術を使用するには、次のアイテムをインストールします:

- `NetworkManager-pptp`、および
- `NetworkManager-pptp-kde4`または `NetworkManager-pptp-gnome`

パッケージのインストールを完了したら、VPN接続を設定します(26.3項「ネットワーク接続の設定」 (421 ページ)参照)

26.7 NetworkManagerとセキュリティ

NetworkManagerは、ワイヤレス接続を「信頼された」と「信頼なし」という2種類で区別します。「信頼された」接続とは、過去に明示的に選択したネットワークです。その他は「信頼なし」です。信頼された接続は、アクセスポイントのMACアドレスと名前で識別されます。MACアドレスを使用して、信頼された接続が同じ名前でも、異なるアクセスポイントを使用できないようにすることができます。

NetworkManagerにより、定期的に、使用可能なネットワークがスキャンされます。信頼されたネットワークが複数検出された場合、最近使用されたものが自動的に選択されます。すべてのネットワークが信頼されないネットワークの場合は、 NetworkManagerはユーザ選択を待機します。

暗号化設定が変更されても、名前とMACアドレスが同じままの場合は、NetworkManagerは接続を試みますが、まず、新しい暗号化設定の確認とアップデート(新しいキーなど)の提供を求めるプロンプトが表示されます。

無線接続を使用している状態からオフラインモードに切り替えると、NetworkManagerでSSIDまたはESSIDが空白になります。これにより、カードの接続解除が確保されます。

26.7.1 ユーザおよびシステムの接続

NetworkManagerは、`user`および`system`という2種類の接続を認識します。ユーザ接続は、最初のユーザがログインしたとき、NetworkManagerで利用可能になる接続です。ユーザは、必要な資格情報を要求されます。ユーザがログアウトすると、接続は切断され、NetworkManagerから削除されます。システム接続として定義された接続は、すべてのユーザが共有でき、NetworkManagerの起動直後で、どのユーザもまだログインしていないとき、

利用可能になります。システム接続の場合、すべての資格情報を接続作成時に提供する必要があります。そのようなシステム接続は、認証を要求するネットワークへの自動接続に使用することができます。NetworkManagerでユーザ接続またはシステム接続を設定する方法については、26.3項 「ネットワーク接続の設定」 (421 ページ)を参照してください。

KDEの場合は、NetworkManagerを使用するシステム接続の設定は、現在サポートされていません(代わりにYaSTを使用)。

26.7.2 パスワードと資格情報の保存

暗号化されたネットワークに接続するたびに資格情報を再入力したくない場合は、デスクトップ固有ツールのGNOMEキーリングマネージャまたはKWalletManagerを使用して、資格情報を暗号化してディスク上に保存し、マスタパスワードで安全を確保できます。

NetworkManagerは、安全な接続(暗号化された有線、無線、またはVPNの接続など)のための証明書を証明書ストアから取得することもできます。詳細については、第12章 *Certificate Store* (↑*Security Guide (セキュリティガイド)*)を参照してください。

26.8 よくある質問とその回答

NetworkManagerによる特別なネットワークオプションの設定に関するよくある質問は、次のとおりです。

特定のデバイスには、どのようにして接続しますか?
: デフォルトでは、NetworkManager内の接続は、デバイスタイプ固有の接続であり、同じタイプのすべての物理デバイスに適用されます。1つの接続タイプについて複数の物理デバイスが使用可能である場合(たとえば、コンピュータに2つのイーサネットカードが取り付けられている場合)、特定のデバイスに接続を関連付けることができます。

  GNOMEでこれを行うには、まずデバイスのMACアドレスを調べます。このために、アプレットから入手できる［*接続情報*］か、またはコマンドラインツール(`nm-tool`または`ifconfig`など)の出力を使用します。次に、ネットワーク接続を設定するためのダイアログを起動し、変更する接続を

選択します。［*有線*］タブまたは［*無線*］タブで、デバイスの［*MACアドレス*］を入力し、変更を確定します。

KDEを使用している場合は、ネットワーク接続を設定するためのダイアログを起動し、変更する接続を選択します。［*Ethernet*］タブまたは［*無線*］タブで、［*インタフェースの制限*］オプションを使用し、接続を関連付けるネットワークインタフェースを選択します。

同じESSIDを持つ複数のアクセスポイントが検出された場合、どのようにして特定のアクセスポイントを指定しますか？

異なる無線帯域(a/b/g/n)を持つ複数のアクセスポイントが利用可能な場合、デフォルトでは、最も強い信号を持つアクセスポイントが自動的に選択されます。このデフォルトを無効にするには、ワイヤレス接続の設定時に［*BSSID*］フィールドを使用します。

BBSID (Basic Service Set Identifier)は、各Basic Service Setを固有に識別します。インフラストラクチャBasic Service Setでは、BSSIDは、ワイヤレスアクセスポイントのMACアドレスです。独立型(アドホック)Basic Service Setでは、BSSIDは、46ビットの乱数から生成されローカルに管理されるMACアドレスです。

26.3項「ネットワーク接続の設定」(421 ページ)に説明されているように、ネットワーク接続を設定するダイアログを開始します。変更したいワイヤレス接続を選択し、［*編集*］をクリックします。［*ワイヤレス*］タブで、BSSIDを入力します。

どのようにして、ネットワーク接続を他のコンピュータと共用しますか?

プライマリデバイス(インターネットに接続するデバイス)には、特別な設定は必要ありません。ただし、ローカルハブまたはローカルコンピュータに接続するデバイスは、次の手順で設定する必要があります。

1. 26.3項 「ネットワーク接続の設定」 (421 ページ)に説明されているように、ネットワーク接続を設定するダイアログを開始します。変更したい接続を選択し、［*編集*］をクリックします。GNOMEを使用している場合は、［*IPv4設定*］タブに切り替えて、［*方法*］ドロップダウンリストから［*他のコンピュータと共有*］を選択します。KDEを使用している場合は、［*IPアドレス*］タブに切り替え、［*設定*］ドロップダウンリストから［*共有*］を選択します。これで、IPトラフィックの転送が有効になり、デバイス上でDHCPサーバが実行されます。NetworkManagerで変更内容を確認します。

2. DCHPサーバは、ポート67を使用するので、そのポートがファイアウォールによってブロックされていないことを確認してください。そのためには、接続を共有するコンピュータで、YaSTを起動して、［セキュリティとユーザ］＞［ファイアウォール］の順に選択します。［*許可されるサービス*］カテゴリに切り替えます。［*DCHP Server*］が［*許可されるサービス*］として表示されていない場合は、［*Services to Allow*］から［*DCHP Server*］を選択し、［*追加*］をクリックします。YaSTで変更内容を確認してください。

静的DNSアドレスに、どのようにして自動(DHCP, PPP, VPN)アドレスを提供しますか?

DHCPサーバが無効なDNS情報(および/またはルート)を提供する場合は、次の手順でそれを無効にできます。26.3項 「ネットワーク接続の設定」 (421 ページ)に説明されているように、ネットワーク接続を設定するダイアログを開始します。変更したい接続を選択し、［*編集*］をクリックします。GNOMEを使用している場合は、［*IPv4設定*］タブに切り替えて、［*方法*］ドロップダウンリストから［*自動(DHCP)アドレスのみ*］を選択します。KDEを使用している場合は、［*IPアドレス*］タブに切り替え、［*設定*］ドロップダウンリストから［*自動(DHCP)アドレスのみ*］を選択します。［*DNS Servers*］および［*Search Domains*］のフィールドにDNS情報を入力します。［*自動で取得したルートを無視する*］場合は、［*Routes*］をクリックして該当するチェックボックスをオンにする(GNOME)か、タブの一番下にあるドロップダウンリストから［*Routes*］を選択して該当するチェックボックスをオンにします(KDE)。変更内容を確認します。

どのようにしたら、ユーザがログインする前に、パスワード保護されたネットワークにNetworkManagerを接続できますか?

そのような目的に使用できる`system connection`を定義します。詳細については、26.7項 「NetworkManagerとセキュリティ」 (433 ページ)を参照してください。

26.9 トラブルシューティング

接続に関する問題が発生する可能性があります。NetworkManagerに関してよく発生する問題としては、アプレットが起動しない、VPNオプションがないなどがあります。これらの問題の解決、防止方法は、使用ツールによって異なります。

NetworkManagerデスクトップアプレットが起動しない
: ネットワークがNetworkManager制御に設定されている場合、GNOMEおよびKDENetworkManagerアプレットが自動的に開始します。アプレットが起動しない場合は、26.2項 「NetworkManagerの有効化と無効化」 (420 ページ)の説明に従って、YaST内でNetworkManagerが有効になっているかどうかチェックしてください次に、デスクトップ環境に適切なパッケージがインストールされていることを確認します。KDE 4を使用する場合、該当するパッケージは`NetworkManager-kde4`です。GNOMEを使用する場合、該当のパッケージは`NetworkManager-gnome`です

  デスクトップアプレットがインストールされているが、何らかの理由で実行されない場合は、手動でアプレットを起動してください。デスクトップアプレットがインストールされているのに、何らかの理由で実行していないときは、コマンド`nm-applet` (GNOME)または`knetworkmanager`(KDE)で手動で開始します。

NetworkManagerアプレットにVPNオプションが表示されない
: NetworkManager,アプレットと NetworkManager用VPNのサポートは、個別のパッケージで配布されます。NetworkManagerアプレットにVPNオプションがない場合は、ご使用のVPN技術のNetworkManagerサポートを含むパッケージがインストールされているかどうか確認してください。詳細については、26.6項 「NetworkManagerとVPN」 (432 ページ)を参照してください。

ネットワーク接続を使用できない
: ネットワーク接続が正しく設定され、ネットワーク接続の他のすべてのコンポーネントも(ルータなど)、正常に機能している場合は、コンピュータ上でネットワークインタフェースを再起動すると、問題が解決する場合があります。そのためには、コマンドラインで`root`としてログインし、`rcnetwork restart`を実行します。

26.10 詳細情報

NetworkManagerの詳細は、次のウェブサイトおよびディレクトリから入手できます。

NetworkManagerプロジェクトページ
: http://projects.gnome.org/NetworkManager/

KDE NetworkManagerフロントエンド
: http://userbase.kde.org/NetworkManagement

パッケージのドキュメント
: NetworkManagerおよびGNOMEとKDEのNetworkManagerアプレットの最新情報については、次のディレクトリの情報も参照してください。

  - /usr/share/doc/packages/NetworkManager/,
  - /usr/share/doc/packages/NetworkManager-kde4/、および
  - /usr/share/doc/packages/NetworkManager-gnome/。

27 Samba

Sambaを使用すると、Mac OS X、Windows、OS/2マシンに対するファイルサーバおよびプリントサーバをUnixマシン上に構築できます。Sambaは、今や成熟の域に達したかなり複雑な製品です。Sambaは、YaST、SWAT(Webインタフェース)を使用するか設定ファイルを手動で編集して設定します。

27.1 用語

ここでは、Samba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。

SMBプロトコル
: SambaはSMB(サーバメッセージブロック)プロトコルを使用します。SMBはNetBIOSサービスを基にしています。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。

ヒント: IBM System z:NetBIOSサポート

IBM System zではSMB over TCP/IPのみがサポートされています。これら2つのシステムではNetBIOSをサポートしていません。

CIFSプロトコル

CIFS (common Internet file system)プロトコルは、Sambaがサポートしているプロトコルです。CIFSは、ネットワーク上で使用する標準のリモートファイルシステムで、ユーザグループによる共同作業およびネットワーク間でのドキュメントの共有ができるようにします。

NetBIOS

NetBIOSは、マシン間通信用に設計された、ネームサービスを提供するソフトウェアインタフェース(API)です。これにより、ネットワークに接続されたマシンが、それ自体の名前を維持できます。予約を行えば、これらのマシンを名前によって指定できます。名前を確認する一元的なプロセスはありません。ネットワーク上のマシンでは、すでに使用済みの名前でない限り、名前をいくつでも予約できます。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か、DNSをネイティブで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。

Sambaサーバ

Sambaサーバは、SMB/CIFSサービスおよびNetBIOS over IPネーミングサービスをクライアントに提供します。Linuxの場合、3種類のSambaサーバデーモン(SMB/CIFSサービス用smnd、ネーミングサービス用nmbd、認証用winbind)が用意されています。

Sambaクライアント

Sambaクライアントは、SMBプロトコルを介してSambaサーバからSambaサービスを使用するシステムです。Mac OS X、Windows、OS/2などの一般的なオペレーティングシステムは、すべてSMBプロトコルをサポートしています。TCP/IPプロトコルは、すべてのコンピュータにインストールする必要があります。Sambaは、異なるUNIXフレーバーに対してクライアントを提供します。Linuxでは、SMB用のカーネルモジュールがあり、

Linuxシステムレベルでの SMB リソースの統合が可能です。Sambaクライアントに対していずれのデーモンも実行する必要はありません。

共有
: SMBサーバは、そのクライアントに対し、共有によってリソースを提供します。共有は、サーバ上のサブディレクトリのあるディレクトリおよびプリンタです。これは名前によってエクスポートされ、名前によってアクセスされます。共有名にはどのような名前も設定できます。エクスポートディレクトリの名前である必要はありません。プリンタにも名前が割り当てられます。クライアントはプリンタに名前でアクセスできます。

DC
: ドメインコントローラ(DC)はドメインのアカウントを処理するサーバです。データレプリケーションには、1つのドメインの中で追加のドメインコントローラが使用できます。

27.2 Sambaの起動および停止

Sambaサーバは、自動(ブート中)か手動で起動または停止できます。ポリシーの開始および停止は、27.3.1項 「YaSTによるSambaサーバの設定;」 (442ページ)で説明しているように、YaST Sambaサーバ設定の一部です。

YaSTを使用して実行中のSambaサービスを停止または起動するには、［システム］>［システムサービス（ランレベル）］の順に選択し、winbind、smb、nmbにチェックを付けます。コマンドラインで、「`rcsmb stop && rcnmb stop`」を入力して、Sambaに必要なサービスを停止し、「`rcnmb start && rcsmb start`」を入力して起動します。rcsmbは必要に応じてwinbindを処理します。

27.3 Sambaサーバの設定

SUSE® Linux Enterprise ServerのSambaサーバは、YaSTを使って、または手動で設定することができます。手動で設定を行えば細かい点まで調整できますが、YaSTのGUIほど便利ではありません。

27.3.1 YaSTによるSambaサーバの設定;

Sambaサーバを設定するには、YaSTを起動して、［ネットワークサービス］>［*Samba*サーバ］の順に選択します。

27.3.1.1 初期Samba設定

このモジュールを初めて起動すると、［*Samba*インストール］ダイアログが起動して、サーバ管理に関していくつかの基本的な事項を決定するように要求されます。設定の最後に、Samba管理者パスワードを要求されます(［*Samba*ルートパスワード］)。次回起動時には、［*Samba Configuration*］ダイアログが表示されます。

［*Samba*インストール］ダイアログは、次の2つのステップとオプションの詳細設定で構成されています。

ワークグループまたはドメイン名
: ［*Workgroup or Domain Name*］から既存の名前を選択するか、新しい名前を入力し、［次へ］を入力します。

Sambaサーバのタイプ
: 次のステップでは、サーバをPDC(プライマリドメインコントローラ)として機能させるか、BDC(バックアップドメインコントローラとして機能させるか、またはドメインコントローラとしては機能させないかを指定します。［次へ］で続行します。

詳細なサーバ設定に進まない場合は、［*OK*］を選択して確認します。次に、最後のポップアップボックスで、［*Samba*ルートパスワード］を設定します。

この設定はすべて、後から［*Samba*の設定］ダイアログで［*起動*］、［*共有*］、［*識別情報*］、［*信頼されたドメイン*］、［*LDAP*設定］の各タブを使用して変更することができます。

27.3.1.2 Sambaの詳細設定

Sambaサーバモジュールの初回起動中、2つの初期化ステップ(27.3.1.1項 「初期Samba設定」 (442 ページ)参照)の直後に［*Samba*の設定］ダイアログが表示されます。ここでは、Sambaサーバの設定を編集することができます。

設定を編集し終わったら、［*OK*］をクリックして設定を保存します。

サーバを起動する

［Start Up］［*タブで、Sambaサーバの起動に関する設定を行います。*］システムのブート時に毎回サービスが起動されるようにするには、［*During Boot*］を選択します。手動起動を有効化するには、［*Manually*］を選択します。Sambaサーバの起動の詳細については、27.2項 「Sambaの起動および停止」 (441 ページ)を参照してください。

このタブで、ファイアウォールのポートを開くこともできます。そのためには、［*Open Port in Firewall*］を選択します。複数のネットワークインタフェースがある場合は、［*Firewall Details*］をクリックし、インタフェースを選択した後、［*OK*］をクリックして、Sambaサービス用のネットワークインタフェースを選択します。

共有

［共有］［*タブで、有効にするSambaの共有を指定します。*］homesおよびプリンタなど、事前定義済みの共有がいくつかあります。［*状態の変更*］を使用して、［*有効*］と［*無効*］の間で切り替えます。新規の共有を追加するには［*追加*］、共有を削除するには［*削除*］をクリックします。

［*ユーザにディレクトリの共有を許可する*］を選択すると、［*許可するグループ*］中のグループメンバーに、各自のディレクトリを他のユーザと共有させることができます。たとえば、ローカルの範囲の`users`、あるいはドメインの範囲では`DOMAIN\Users`を設定します。また、ユーザにはファイルシステムへのアクセスを許可するパーミッションがあることを確認してください。［*最大共有数*］で、共有の最大数を制限することができます。認証なしでユーザ共用へのアクセスを許可するには、［*ゲストアクセスを許可*］を有効にします。

ID

［*識別情報*］タブで、ホストが関連付けられているドメイン(［*基本設定*］)と、ネットワークで代替ホスト名を使用するかどうか(［*NetBIOS Hostname*］)を指定します。 名前解決にMicrosoft Windows Internet Name Service(WINS)を使用することもできます。この場合、［*Use WINS for Hostname Resolution*］を有効にし、DHCP経由でWINSサーバを取得(［*Retrieve WINS server via DHCP*］を使用)するかどうか決定します。TDBデータベースではなくLDAPなど、エキ

スパートグローバル設定またはユーザ認証ソースを設定するには、［*詳細設定*］をクリックします。

信頼されたドメイン

他のドメインのユーザを、自分のドメインにアクセスさせるには、［*Trusted Domains*］タブで適切な設定を行います。新しいドメインを追加するには、［*追加*］をクリックします。選択したドメインを削除するには、［*削除*］をクリックします。

LDAP設定

［LDAP Settings］［*タブでは、認証に使用するLDAPサーバを設定することができます。*］LDAPサーバへの接続をテストするには、［*Test Connection*］をクリックします。エキスパートLDAP設定を設定するか、デフォルト値を使用する場合、［*詳細な設定*］をクリックします。

LDAP設定に関する詳細については、第4章 *LDAP—A Directory Service* (↑*Security Guide (セキュリティガイド)*)を参照してください。

27.3.2 SWATを使用したWeb管理

Sambaサーバ管理の代替ツールは、SWAT(Samba Web管理ツール)です。このプログラムには、Sambaサーバを設定するための簡単なWebインタフェースがあります。SWATを使用するには、Webブラウザで、`http://localhost:901`を開き、`root`ユーザでログインします。特別なSamba rootアカウントがない場合、システムの`root`アカウントを使用します。

注記: SWATの有効化

Sambaサーバのインストール後、SWATは有効化されていません。SWATを有効化するには、YaSTで［ネットワークサービス］ > ［ネットワークサービス*(xinetd)*］の順に開き、ネットワークサービス設定を有効にし、テーブルから［*swat*］を選択し、［*状態の変更(オンまたはオフ)*］をクリックします。

27.3.3 サーバの手動設定

Sambaをサーバとして使用する場合は、sambaをインストールします。Sambaの主要設定ファイルは、/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。

27.3.3.1 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。このパラメータに関する詳細については、smb.confのマニュアルページを参照してください。

os level = 20
: 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 3リリースシリーズでは、デフォルト設定(20)を上書きする必要はほとんどなくなりました。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(たとえば2)を選択します。この重要なトピックの詳細については、『Samba 3 Howto』のネット「ワークブラウジング」の章を参照してください。『Samba 3 Howto』の詳細については、27.7項 「詳細情報」 (453 ページ)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 2000サーバ)が存在せず、ローカル環境に存在するすべてのシステムのリストをSambaサーバ

に保存する場合は、os levelの値を大きくします(たとえば、65)。これでSambaサーバが、ローカルネットワークのLMBとして選択されました。

この設定を変更するときは、それが既存のWindowsネットワーク環境にどう影響するかを慎重に検討する必要があります。はじめに、隔離されたネットワークで、または影響の少ない時間帯に、変更をテストしてください。

wins supportとwins server
: アクティブなWINSサーバをもつ既存のWindowsネットワークにSambaサーバを参加させる場合は、wins serverオプションを有効にし、その値をWINSサーバのIPアドレスに設定します。

  各Windowsマシンの接続先サブネットが異なり、互いを認識させなければならない場合は、WINSサーバをセットアップする必要があります。SambaサーバをWINSサーバなどにするには、wins support = Yesオプションを設定します。ネットワーク内でこの設定が有効なSambaサーバは1台だけであることを確認します。smb.confファイル内で、オプションwins serverとwins supportは同時に有効にしないでください。

27.3.3.2 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 27.1 CD-ROMの共有(無効)

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

[cdrom]およびコメント
: [cdrom]セクションエントリは、ネットワーク上のすべてのSMBクライアントが認識できる共有の名前です。さらにcommentを追加して、共有を説明することができます。

`path = /media/cdrom`
: pathオプションで、/media/cdromディレクトリをエクスポートします。

デフォルトを非常に制約的に設定することによって、このシステム上に存在するユーザのみがこの種の共有を利用できるようになります。この共有をあらゆるユーザに開放する場合は、設定に`guest ok = yes`という行を追加します。この設定は、ネットワーク上の全ユーザに読み込み許可を与えます。このパラメータを使用する場合には、相当な注意を払うことをお勧めします。またこのパラメータを`[global]`セクションで使用する場合には、さらに注意が必要です。

`[homes]`
: `[homes]`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 **27.2** [homes]共有*

```
[homes]
 comment = Home Directories
 valid users = %S
 browseable = No
 read only = No
 create mask = 0640
 directory mask = 0750
```

[homes]
: SMBサーバに接続しているユーザの共有名を他の共有が使用していない限り、`[homes]`共有ディレクティブを使用して共有が動的に生成されます。生成される共有の名前は、ユーザ名になります。

`valid users = %S`
: `%S`は、接続が正常に確立されるとすぐに、具体的な共有名に置き換えられます。[homes]共有の場合、これは常にユーザ名です。したがって、ユーザの共有に対するアクセス権は、そのユーザだけに付与されます。

`browseable = No`
: この設定を行うと、共有がネットワーク環境で認識されなくなります。

`read only = No`
: デフォルトでは、Sambaは`read only = Yes`パラメータによって、エクスポートされた共有への書き込みアクセスを禁止します。共有に書き込めるように設定するには、`read only = No`値を設定します。これは`writable = Yes`と同値です。

`create mask = 0640`
: MS Windows NTベース以外のシステムは、UNIXのパーミッションの概念を理解しないので、ファイルの作成時にアクセス権を割り当てることができません。`create mask`パラメータは、新しく作成されたファイルに割り当てられるアクセス権を定義します。これは書き込み可能な共有にのみ適用されます。実際、この設定はオーナーが読み書き権を持ち、オーナーの一次グループのメンバが読み込み権を持つことを意味します。`valid users = %S`を設定すると、グループに読み込み権が与えられても、読み込みアクセスができなくなります。グループに読み書き権を付与する場合は、`valid users = %S`という行を無効にしてください。

27.3.3.3 セキュリティレベル

セキュリティを向上させるため、各共有へのアクセスは、パスワードによって保護されています。SMBでは、次の方法で権限を確認できます。

共有レベルのセキュリティ(セキュリティ=共有)
: パスワードが共有に対し確実に割り当てられています。このパスワードを持っているユーザ全員が、その共有にアクセスできます。

ユーザレベルのセキュリティ(セキュリティ=ユーザ)
: このセキュリティレベルは、ユーザという概念をSMBに取り入れています。各ユーザは、サーバにパスワードを登録する必要があります。登録後、エクスポートされた個々の共有へのアクセスは、ユーザ名に応じてサーバが許可します。

サーバレベルのセキュリティ(セキュリティ=サーバ)
: クライアントに対しては、Sambaがユーザレベルモードで動作しているように見えます。しかし、Sambaはすべてのパスワードクエリを別のユーザレベルモードサーバに渡し、ユーザレベルモードサーバが認証されます。この設定では、追加の`password server`パラメータが必要になります。

ADSレベルのセキュリティ(セキュリティ=ADS)
: このモードでは、Sambaはアクティブディレクトリ環境のドメインメンバーとして動作します。このモードで操作するには、Sambaを実行しているコンピュータにKerberosがインストールされ設定済みであることが必要です。Sambaを使用してコンピュータをADSレルムに結合させる必要があります。これは、YaSTの［*Windows*ドメインメンバーシップ］を使用して行います。

ドメインレベルのセキュリティ(セキュリティ=ドメイン)
: このモードは、コンピュータがWindows NTドメインに結合している場合に正しく動作します。Sambaはユーザ名とパスワードをWindows NT PrimaryまたはBackup Domain Controllerに渡すことによって、これらを検証しようとします。Windows NT Serverが行うのと同じ方法です。暗号化されたパスワードパラメータが`yes`に設定されている必要があります。

共有、ユーザ、サーバ、またはドメインレベルのセキュリティの設定は、サーバ全体に適用されます。個別の共有ごとに、ある共有には共有レベルのセキュリティ、別の共有にはユーザレベルセキュリティを設定するといったことはできません。しかし、システム上に設定したIPアドレスごとに、別のSambaサーバを実行することは可能です。

この詳細については、『Samba 3 HOWTO』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。

27.4 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。

27.4.1 YaSTによるSambaクライアントの設定

SambaクライアントをSambaサーバまたはWindowsサーバ上のリソース(ファイルまたはプリンタ)にアクセスするように設定します。NTまたはActive Directoryのドメインまたはワークグループを、［ネットワークサービス］>［*Windows*ドメインメンバーシップ］の順に選択して表示したダイアログに入力します。

［*Linuxの認証にもSMBの情報を使用する*］を有効にした場合、ユーザ認証は、Samba、NT、またはKerberosのサーバ上で実行されます。

［エキスパート設定］をクリックして、高度な設定オプションを設定します。たとえば、認証による自動的なサーバホームディレクトリのマウントを有効化するには、［サーバディレクトリのマウント］のテーブルを使用します。これにより、CIFS上でホストされると、ホームディレクトリにアクセスできるようになります。詳細については、pam_mountのマニュアルページを参照してください。

すべての設定を完了したら、ダイアログを確認して設定を終了します。

27.5 ログインサーバとしてのSamba

Windowsクライアントが大部分を占めるネットワークでは、ユーザが有効なアカウントとパスワードを持つ場合のみ登録できることが求められるのが普通です。Windowsベースのネットワークでは、このタスクはPDC (プライマリドメインコントローラ)によって処理されます。Windows NTサーバをPDCとして使用することもできますが、Sambaサーバを使用しても処理できます。例27.3「smb.confファイルのグローバルセクション」 (450ページ)に示すように、smb.confの[global]セクションにエントリを追加する必要があります。

例 27.3 *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目的で使用される場合、Sambaサーバはこれを処理できるはずです。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 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。

```
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。

```
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正常に実行できるようにするため、必要な管理者権限を持つSamba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
```

このトピックの詳細については、/usr/share/doc/packages/samba/Samba3-HOWTO.pdfにある『Samba 3 HOWTO』の第12章を参照してください。

27.6 Active Directoryネットワーク内のSambaサーバ

LinuxサーバとWindowsサーバの両方を利用する場合、2つの独立した認証システムまたはネットワークを作成するか、または単一の中央認証システムを持つ単一のネットワークに両方のサーバを接続します。SambaはActive Directoryドメインと連携できるため、お使いのSUSE Linux Enterprise ServerをActive Directory (AD)に参加できます。

既存のActive Directoryドメインに参加するには、インストール時に設定を行うか、または後でYaSTを使って、SMBユーザ認証を有効にします。インストール時にドメインへの参加を設定する方法については、項「ユーザ認証方法」(第6章 *YaSTによるインストール*;, ↑*導入ガイド*)を参照してください。

稼働中のシステムをActive Directoryドメインに参加させるには、以下の手順に従ってください。

1 rootとしてログインし、YaSTを起動します。

2 ［ネットワークサービス］>［*Windows Domain Membership*］の順に選択します。

3 ［*Windows Domain Membership*］画面の［*Domain or Workgroup*］に、参加するドメインを入力します。

図 27.1　Windowsドメインメンバーシップの決定

4 SUSE Linux Enterprise ServerでLinux認証にSMBソースを使用する場合は、［*Linuxの認証にもSMBの情報を用いる*］を選択します。

5 ドメインへの参加を確認するメッセージが表示されたら、［*OK*］をクリックします。

6 Active DirectoryサーバのWindows管理者用パスワードを入力し、［*OK*］をクリックします。

Active Directoryドメインコントローラから、すべての認証データを取得できるようになりました。

27.7 詳細情報

Sambaについての詳細な情報は、デジタルドキュメントの形で入手できます。コマンドラインから「apropossamba」と入力するとマニュアルページを参照できます。または、Sambaマニュアルがインストールされている場合は、/usr/share/doc/packages/sambaディレクトリに格納されているオンラインマニュアルと例を参照できます。また、コメント付きの設定例(smb.conf.SuSE)がexamplesサブディレクトリに用意されています。

Sambaチームが作成した『Samba-3 HOWTO』にはトラブルシューティングについても説明されています。またマニュアルのPart Vでは、手順を追って設定を確認するためのガイドが用意されています。samba-docパッケージのインストール後、/usr/share/doc/packages/samba/Samba3-HOWTO.pdfで、『Samba-3 HOWTO』を参照できます。

28 NFS共有ファイルシステム

ネットワーク上でファイルシステムを分散して共有することは、企業環境では一般的なタスクです。十分に実績のあるネットワークファイルシステム (*NFS*)は、*NIS* (Yellow Pagesプロトコル)と連携して機能します。*LDAP*と連携して機能し、Kerberosも使用できるより安全なプロトコルについては、*NFSv4*をチェックしてください。pNFSとの組み合わせで、パフォーマンスのボトルネックをなくすことができます。

NFSをNISと連携して使用すると、ネットワークをユーザに対し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任意のファイルシステムを分散できます。適切なセットアップを行えば、現在どの端末を使用しているかに係わりなく、常に同じ環境で作業できます。

重要: DNSの必要性

原則として、すべてのエクスポートはIPアドレスのみを使用して実行できます。タイムアウトを回避するには、機能するDNSシステムが必要です。mountdデーモンは逆引きを行うので、少なくともログ目的でDNSは必要です。

28.1 用語集

以下の用語は、YaSTモジュールで使用されています。

エクスポート
NFSサーバによってエクスポートされ、クライアントがシステムに統合できるディレクトリ。

NFSクライアント
NFSクライアントは、ネットワークファイルシステムプロトコルを介してNFSサーバからのNFSサービスを使用するシステムです。TCP/IPプロトコルはLinuxカーネルにすでに統合されており、追加ソフトウェアをインストールする必要はありません。

NFSサーバ
NFSサーバは、NFSサービスをクライアントに提供します。`nfsd`(ワーカー)、`idmapd` (IDへのユーザおよびグループ名のマッピングと、その逆のマッピング)、`statd`(ファイルのロック)、および`mountd` (マウント要求)。

pNFS
パラレル NFS。NFSv4のプロトコル拡張。 任意のpNFSクライアントは、NFSサーバ上のデータに直接アクセスできます。

28.2 NFSサーバのインストール

NFSサーバソフトウェアは、デフォルトインストールの一部ではありません。28.3項 「NFSサーバの設定」 (456 ページ)に従ってNFSサーバを設定すると、必要なパッケージのインストールを自動的に求められます。別の方法として、YaSTまたはzypperと共にパッケージ`nfs-kernel-server`をインストールします。

NIS同様、ANFSはクライアント/サーバシステムです。ただし、ファイルシステムをネットワーク経由で提供し(エクスポート)、同時に他のホストからファイルシステムをマウントする(インポート)ことができます。

28.3 NFSサーバの設定

NFSサーバの設定は、YaSTを使用するか、または手動で完了できます。認証の場合は、NFSをKerberosと組み合わせることもできます。

28.3.1 YaSTによるファイルシステムのエクスポート

YaSTを使用して、ネットワーク上のホストをNFSサーバに変更し、そのホストへのアクセスを許可されたすべてのホストに、ディレクトリやファイルをエクスポートすることができます。サーバは、ホストごとにローカルにアプリケーションをインストールしなくても、グループの全メンバーにアプリケーションを提供することもできます。

そのようなサーバをセットアップするには、次の手順に従います。

手順 28.1 *NFSv3サーバの設定*

1 YaSTを起動し、［ネットワークサービス］＞［*NFS*サーバ］の順に選択します(図28.1「NFSサーバ設定ツール」(457ページ)参照)。追加のソフトウェアをインストールするよう求められることがあります。

図 28.1 *NFSサーバ設定ツール*

2 ［*開始*］ラジオボタンをオンにします。

3 システム(SuSEfirewall2)でファイアウォールが有効になっている場合は、［*ファイアウォールでポートを開く*］をオンにします。YaSTは、`nfs`サービスを有効にすることによってNFSサーバの設定を適用します。

4 ［*NFSv4を有効にする*］チェックボックスはオフのままにしてください。

5 サーバに安全にアクセスするには、［*GSSセキュリティを有効にする*］をクリックします。この手順の前提条件として、ドメインにKerberosをインストールし、サーバとクライアントの両方でKerberosを有効にしておく必要があります。［*次へ*］をクリックします。

6 ディレクトリをエクスポートするには、ダイアログの上半分にある［*ディレクトリの追加*］をクリックします。

7 許可されるホストをまだ設定していない場合は、自動的に別のダイアログが表示されるので、クライアント情報およびオプションを入力します。ホストを示すワイルドカードを入力します(通常はデフォルト設定のまま使用できます)。

4種類の方法でホストを指定することができます。1台のホスト(名前またはIPアドレス)(single host)、ネットグループ(netgroups)、ワイルドカード(すべてのコンピュータがサーバにアクセスできることを示す*など)(wild cards)、およびIPネットワーク(IP networks)です。

8 ［*完了*］をクリックして設定を完了します。

28.3.1.1 NFSv4クライアント用のエクスポート

NFSv4クライアントに対してエクスポートできるディレクトリには、疑似rootファイルシステムの役割を果たすディレクトリと、疑似ファイルシステムのサブディレクトリにバインドされるディレクトリの2種類があります。疑似ファイルシステムは、同じクライアントに対してエクスポートされたすべてのファイルシステムをまとめる、ルートディレクトリの役割を果たします。クライアントに対しては、サーバ上の1つのディレクトリのみを、エクスポート用の疑似rootディレクトリとして設定できます。このクライアントに複数のディレクトリをエクスポートするには、それらのディレクトリを、疑似root中の既存サブディレクトリにバインドします。

たとえば、サーバにアクセスするすべてのクライアントの疑似ディレクトリとして、`/exports`を使用する場合を考えてみましょう。この場合、エクス

ポートするディレクトリのリストにこのディレクトリを追加して、このディレクトリのオプションにfsid=0を指定します。別に/dataディレクトリもNFSv4を使ってエクスポートする必要がある場合は、このディレクトリもリストに追加します。このディレクトリに関するオプションを設定する際には、リストにbind=/exports/dataを指定します。また、/exports/dataがすでに/exportsの既存のサブディレクトリとなっていることを確認してください。オプションbind=/target/pathに対する変更(値の追加、削除、または変更)はすべて、［*Bindmount*ターゲット］に反映されます。

サーバでNFSv4を使ったディレクトリのエクスポートを設定するには、手順28.1「NFSv3サーバの設定」(457ページ)の全般的なガイドラインに従います。ただし、以下の手順を変更します。

1 最初のダイアログで［*NFSv4*を有効にする］をオンにします。

2 最初のダイアログで適切なNFSv4ドメイン名を入力します。

ここで指定する名前は、このサーバにアクセスするNFSv4クライアントの/etc/idmapd.confファイルで指定された名前にする必要があります。このパラメータは、NFSv4サポートに必要なidmapdデーモンが使用します(サーバとクライアントの両方で)。特に必要のない限り、そのままlocaldomain(デフォルト)を使用してください。

［次へ］をクリックした後に表示されるダイアログには、2つのセクションがあります。上部のセクションには、［ディレクトリ］と［*Bindmount*ターゲット］の2つの列があります。サービスがただちに利用できるようになります。

3 ディレクトリをエクスポートするには、ダイアログの上半分にある［ディレクトリの*追加*］をクリックし、［*Ok*］で確認します。

4 ［ホストのワイルドカード］テキストフィールドのホスト名およびオプションを入力します。

［オプション］テキストフィールドに、疑似rootにするディレクトリを設定する場合は、カンマ区切り形式のオプションリストにfsid=0を指定します。このディレクトリを、すでに疑似rootとして設定されているディレクトリ下の別のディレクトリにバインドする場合は、オプションリストにターゲットのバインドパスをbind=/target/pathの形式で指定します。

［*Bindmount Targets*］列は直接編集可能な列ではなく、ディレクトリとその性質を要約している列です。

5 ［完了］をクリックして設定を完了します。

28.3.1.2 NFSv3およびNFSv2エクスポート

初期ダイアログで［*NFSv4を有効にする*］の選択が解除されていることを確認してから、［次へ］をクリックします。

次のダイアログは、2つの部分に分かれています。上部のテキストフィールドに、エクスポートするディレクトリを入力します。下部に、それらのディレクトリへのアクセスを許可するホストを入力します。4種類の方法でホストを指定することができます。1台のホスト(名前またはIPアドレス)(single host)、ネットグループ(netgroups)、ワイルドカード(すべてのコンピュータがサーバにアクセスできることを示す*など)(wild cards)、およびIPネットワーク(IP networks)です。

に示すダイアログボックスが表示されます。図28.2「NFSv2およびNFSv3を使ったディレクトリのエクスポート」(461ページ)これらのオプションの詳細は、`man exports`を実行して表示される、マニュアルページを参照してください。［完了］をクリックして設定を完了します。

図 28.2　NFSv2およびNFSv3を使ったディレクトリのエクスポート

28.3.1.3 NFSv3エクスポートとNFSv4エクスポートの共存

1台のサーバ上に、NFSv3エクスポートとNFSv4エクスポートを共存させることができます。初期設定ダイアログでNFSv4サポートを有効にすると、オプションリストに`fsid=0`と`bind=/target/path`が指定されていないエクスポートは、NFSv3エクスポートとみなされます。

28.3.1.1項「NFSv4クライアント用のエクスポート」(458ページ)の例を参考に説明します。［ディレクトリの追加］を使って［*/data2*］ディレクトリを追加したけれども、そのオプションに`fsid=0`や`bind=/target/path`を指定しなかった場合、このエクスポートはNFSv3エクスポートとして処理されます。

重要

自動ファイアウォール設定

システムでSuSEfirewall2が有効になっている場合に、［ファイアウォールでポートを開く］を選択すると、YaSTはnfsサービスの有効化により、そのNFSサーバ設定を適応させます。

28.3.2 ファイルシステムの手動エクスポート

NFSエクスポートサービスの環境設定ファイルは、/etc/exportsと/etc/sysconfig/nfsです。NFSv4サーバ環境設定には、これらのファイルに加えて/etc/idmapd.confも必要です。サービスを起動または再起動するには、rcnfsserver restartを実行します。これにより、NFSv4が/etc/sysconfig/nfsで設定されている場合は、rpc.idmapdも起動します。NFSサーバは、RPCポートマッパーに依存しています。したがって、rcportmap restartコマンドで、ポートマッパーサービスも起動/再起動してください。

28.3.2.1 NFSv4を使ったファイルシステムのエクスポート

NFSv4は、SUSE Linux Enterprise Serverで利用できる最新版のNFSプロトコルです。NFSv4でエクスポートするディレクトリの設定方法は、以前のNFSバージョンと多少異なっています。

/etc/exports

/etc/exportsファイルには、エントリのリストが含まれています。各エントリはそれぞれ共有するディレクトリと共有方法を示します。/etc/exports中の一般的なエントリは、次の項目から成り立っています。

```
/shared/directory   host(option_list)
```

たとえば、次のような指定内容です。

```
/export   192.168.1.2(rw,fsid=0,sync,crossmnt)
/export/data   192.168.1.2(rw,bind=/data,sync)
```

ここでは、許可されたクライアントを識別するためにIPアドレス192.168.1.2が使われています。ホスト名、ホストを表すワイルドカード、または(*.abc.comや*など)ネットグループ（@my-hosts）を使用できます。

fsid=0を指定するディレクトリは特別です。このディレクトリは、擬似ルートファイルシステムと呼ばれることのある、エクスポートされるファイルシステムのルートです。また、このディレクトリはNFSv4で正しく動作するためにcrossmntが必要です。NFSv4 経由でエクスポートされた他のすべてのディレクトリは、これより下の地点にマウントする必要があります。エクスポートされたルートにないディレクトリをエクスポートする場合は、エクスポートされたツリーにバインドする必要があります。これはbind=構文を使用して行うことができます。

上の例では、/dataは/exportにないため、/export/dataをエクスポートし、/dataディレクトリがその名前にバインドされるよう指定します。ディレクトリ/export/dataが存在し、通常は空である必要があります。

クライアントがこのサーバからマウントする場合、servername:/exportではなくservername:/をマウントするだけです。servername:/dataは、servername:/がマウントされると必ずその下に自動的に表示されるのでマウントする必要はありません。

/etc/sysconfig/nfs

/etc/sysconfig/nfsファイルには、NFSv4サーバデーモンの動作を決定する小数のパラメータが含まれています。NFS4_SUPPORTパラメータをyesに設定することが重要です。NFS4_SUPPORTは、NFSサーバがNFSv4エクスポートとクライアントをサポートするかどうかを決定します。

/etc/idmapd.conf

Linuxコンピュータ上の各ユーザには、ユーザ名とIDがあります。idmapdは、サーバへのNFSv4リクエストやクライアントへのNFSv4応答用に、名前とID間のマッピングサービスを提供しています。NFSv4はその通信に名前だけを使用するので、idmapdは、NFSv4のサーバとクライアントの両方で実行されている必要があります。

NFSを使ってファイルシステムを共有するコンピュータ間では、ユーザへのユーザ名とID (uid)の割り当てには同じ方法を使用してください。そのためには、NIS、LDAP、または他の同一ドメイン認証機構を利用することができます。

/etc/idmapd.confファイルのDomainパラメータは、クライアントとサーバの両方に対して同じ値に設定する必要があります。確信のない場合には、クライアントとサーバの両方のファイルで、localdomainをそのまま使用してください。環境設定ファイルの例を次に示します。

```
[General]

Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]

Nobody-User = nobody
Nobody-Group = nobody
```

詳細は、idmapdとidmapd.confのマニュアルページを参照してください。参照するには、man idmapd、man idmapd.confを実行します。

サービスの起動と停止

/etc/exportsまたは/etc/sysconfig/nfsを変更したら、rcnfsserver restartコマンドを実行して、NFSサーバサービスを起動/再起動します。/etc/idmapd.confを変更したら、killall -HUP rpc.idmapdコマンドで、環境設定ファイルを再ロードします。

NFSサービスをブート時に開始する必要がある場合は、chkconfig nfsserver onコマンドを実行します。

28.3.2.2 NFSv2とNFSv3を使ったファイルシステムのエクスポート

ここでは、NFSv2エクスポートとNFSv3エクスポートに固有のトピックを取り上げます。NFSv4エクスポートについては、28.3.1.1項 「NFSv4クライアント用のエクスポート」 (458 ページ)を参照してください。

NFSを使ってファイルシステムをエクスポートする場合、/etc/exportsと/etc/sysconfig/nfsの2つの環境設定ファイルが関わってきます。一般的な/etc/exportsファイルには、各エントリが次のような形式で指定されています。

```
/shared/directory   host(list_of_options)
```

たとえば、次のような指定内容です。

```
/export   192.168.1.2(rw,sync)
```

ここで、/exportディレクトリはホスト192.168.1.2と共有されています。オプションリストには、rw,syncが設定されています。このIPアドレスは、特定のクライアント名、ワイルドカードを使った複数のクライアント(*.abc.comなど)、またはネットグループで置き換えることができます。

すべてのオプションとそれらの意味の詳細については、exportsのマニュアルページを参照してください(man exports)。

/etc/exportsまたは/etc/sysconfig/nfsを変更したら、rcnfsserver restartコマンドを実行して、NFSサーバを起動/再起動します。

28.3.3 NFSでのKerberosの使用

NFSでKerberos認証を使用するには、GSSセキュリティを有効にする必要があります。最初のYaST NFSサーバのダイアログで、［*GSSセキュリティを有効にする*］を選択します。ただし、この機能を使用するには、機能するKerberosサーバが必要です。YaSTtは、このサーバの設定は行いません。その提供機能を使用するだけです。YaST環境設定に加えて、Kerberos認証も使用する場合は、NFS設定を実行する前に、少なくとも次の手順を完了してください。

1. サーバとクライアントの両方が、同じKerberosドメインにあることを確認します。つまり、クライアントとサーバが同じKDC(Key Distribution Center)サーバにアクセスし、krb5.keytabファイル(the default location on any machine is /etc/krb5.keytab)を共有していなければなりません。Kerberosの詳細については、第6章 *Network Authentication with Kerberos* (↑*Security Guide (セキュリティガイド)*)を参照してください。

2. クライアントでrcgssd startコマンドを実行して、gssdサービスを開始します。

3. サーバでrcsvcgssd startコマンドを実行して、svcgssdサービスを開始します。

Kerberos化されたNFSの設定の詳細については、28.5項「詳細情報」(470ページ)のリンクを参照してください。

28.4 クライアントの設定

ホストをNFSクライアントとして設定する場合、他のソフトウェアをインストールする必要はありません。必要なすべてのパッケージは、デフォルトでインストールされます。

28.4.1 YaSTによるファイルシステムのインポート

認証されたユーザは、YaST NFSクライアントモジュールを使用して、NFSディレクトリをNFSサーバからローカルファイルツリーにマウントできます。次の手順に従います。

手順 28.2 *NFSディレクトリのインポート*

1 YaST NFSクライアントモジュールを起動します。

2 ［*NFS共有*］タブで［*追加*］をクリックします。NFSサーバのホスト名、インポートするディレクトリ、およびこのディレクトリをマウントするマウントポイントを入力します。

3 ファイアウォールを使用しており、リモートコンピュータのサービスにアクセスを許可する場合は、［*NFS設定*］タブで［*ファイアウォールでポートを開く*］をオンにします。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。

4 NFSv4を使用する場合は、［*NFSv4を有効にする*］チェックボックスが選択され、［*NFSv4ドメイン名*］にNFSv4サーバによって使用される値と同じ値が入力されていることを確認してください。デフォルトドメインは、`localdomain`です。

5 ［*OK*］をクリックして変更内容を保存します。

設定は`/etc/fstab`に書かれ、指定されたファイルシステムがマウントされます。後でYaST設定クライアントを起動した時に、このファイルから既存の設定が取得されます。

28.4.2 ファイルシステムの手動インポート

NFSサーバからファイルシステムを手動でインポートするには、RPCポートマッパーが実行していることが前提条件です。「rcrpcbind start」をrootとして入力してインポートを実行します。次に、mountを使用して、ローカルパーティションと同様に、リモートファイルシステムをファイルシステムにマウントできます。

```
mount host:remote-pathlocal-path
```

たとえば、nfs.example.comコンピュータからユーザディレクトリをインポートするには、次の構文を使用します。

```
mount nfs.example.com:/home /home
```

28.4.2.1 自動マウントサービスの使用

autofsデーモンを使用して、リモートファイルシステムを自動的にマウントすることができます。/etc/auto.masterファイルに次のエントリを追加します。

```
/nfsmounts /etc/auto.nfs
```

これで、/nfsmountsディレクトリがクライアント上のすべてのNFSマウントのルートディレクトリの役割を果たすようになります(auto.nfsファイルが正しく設定されている場合)。ここでは、auto.nfsと言う名前を使用しましたが、任意の名前を選択することができます。auto.nfsで、次のようにしてすべてのNFSマウントのエントリを追加します。

```
localdata -fstype=nfs server1:/data
nfs4mount -fstype=nfs4 server2:/
```

rootとしてrcautofs startを実行して、設定をアクティブにします。この例で、server1の/dataディレクトリの/nfsmounts/localdataは、NFSでマウントされ、server2の/nfsmounts/nfs4mountはNFSv4でマウントされます。

autofsサービスの動作中に/etc/auto.masterファイルを編集した場合、変更内容を反映するには、rcautofs restartで自動マウント機能を再起動する必要があります。

28.4.2.2 /etc/fstabの手動編集

/etc/fstab内の典型的なNFSv3マウントエントリは、次のようになります:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

/etc/fstabファイルにNFSv4マウントを追加することもできます。これらのマウントの場合、3列目にnfsの代わりにnfs4を指定します。また、1列目の*nfs.example.com:*の後に、リモートファイルシステムを/として必ず指定してください。たとえば、/etc/fstab内のNFSv4マウント行は、次のようになります。

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

noautoオプションを使用すると、起動時にファイルシステムが自動マウントされません。対応するファイルシステムを手動でマウントする場合は、マウントポイントのみを指定してmountコマンドを短くできます。

```
mount /local/path
```

ただし、noautoオプションを入力しないと、起動時に、システムのインストールスクリプトによって、それらのファイルシステムがマウントされます。

28.4.3 パラレルNFS(pNFS)

NFSは、1980年代に開発された、もっとも古いプロトコルの1つです。そのため、小さなファイルを共有したい場合は、通常、NFSで十分です。しかし、大きなファイルを送信したい場合や多数のクライアントがデータにアクセスしたい場合は、NFSサーバがボトルネックとなり、システムのパフォーマンスに重大な影響を及ぼします。これは、ファイルのサイズが急速に大きくなっているのに対し、Ethernetの相対速度が追い付いていないためです。

「通常の」NFSサーバにファイルを要求すると、サーバはファイルのメタデータを検索し、すべてのデータを収集して、ネットワークを介してクライアントに送信します。しかし、ファイルが小さくても大きくてもパフォーマンスのボトルネックが問題になります。

- 小さいファイルでは、メタデータの収集に時間がかかる
- 大きいファイルでは、サーバからクライアントへのデータ送信に時間がかかる

pNFS(パラレルNFS)は、ファイルシステムメタデータをデータの場所から分離することによって、この制限を克服します。このため、pNFSには2種類のサーバが必要です。

- データ以外のすべてのトラフィックを扱うメタデータまたは*制御*サーバ
- データを保持する1台または複数のストレージサーバ

メタデータサーバとストレージサーバによって、単一の論理NFSサーバが構成されます。クライアントが読み込みまたは書き出しを行う場合、メタデータサーバがNFSv4クライアントに対して、ファイルのチャンクにアクセスするにはどのストレージサーバを使用すればよいかを指示します。クライアントはサーバのデータに直接アクセスできます。

SUSE Linux Enterpriseはクライアント側でのみpNFSをサポートします。

28.4.3.1 YaSTを使用したpNFSクライアントの設定

手順28.2「NFSディレクトリのインポート」 (466 ページ)に従って進めます。ただし、［*pNFS (v4.1)*］チェックボックスをクリックし、オプションで［*NFSv4共有*］をクリックします。 YaSTが必要な手順をすべて実行し、必要なすべてのオプションをファイル`/etc/exports`に書き出します。

28.4.3.2 pNFSクライアントの手動設定

28.4.2項 「ファイルシステムの手動インポート」 (467 ページ)を参照して開始します。ほとんどの設定はNFSv4サーバによって行われます。pNFSを使用する場合に異なるのは、`minorversion`オプションおよびメタデータサーバ*MDS_SERVER*を`mount`コマンドに追加することだけです。

```
mount -t nfs4 -o minorversion=1 MDS_SERVER MOUNTPOINT
```

デバッグを支援するために、`/proc`ファイルシステムの値を変更します。

```
echo 32767 > /proc/sys/sunrpc/nfsd_debug
echo 32767 > /proc/sys/sunrpc/nfs_debug
```

28.5 詳細情報

NFSサーバとクライアントの設定情報は、exports、nfs、およびmountのマニュアルページのほか、/usr/share/doc/packages/nfsidmap/READMEからも入手できます。オンラインドキュメンテーションについては、次のWebサイトを参照してください。

- 詳細な技術ヘルプについては、SourceForge [http://nfs.sourceforge.net/]を参照してください。
- NFSでのKerberosの設定方法は、NFS Version 4 Open Source Reference Implementation [http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html]を参照してください。
- Linux NFSv4 [http://www.citi.umich.edu/projects/nfsv4/linux/faq/]には、NFSv4に関するFAQが用意されています。

29 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、タブレット、またはスマートフォン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。すべてのコンピュータで最新バージョンのデータを使用できるように、どのコンピュータでも作業ができて、ファイルの変更ができればと考えるでしょう。

29.1 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。

29.1.1 CVS

CVSは、多くの場合プログラムソースのバージョン管理に使用されるプログラムで、複数のコンピュータでファイルのコピーを保存する機能を持っています。したがって、データ同期にも適しています。CVSはサーバ上に一元的なリポジトリを設定し、ファイルおよびファイルの変更内容を保存します。ローカルに実行された変更はリポジトリにコミットされ、更新によって他のコンピュータに取得されます。両方の処理はユーザによって実行される必要があります。

CVSは、複数のコンピュータで変更が行われた場合、非常に優れたエラー回復力を発揮します。変更内容がマージされ、同じ行が変更された場合は、競合がレポートされます。競合が生じても、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。

29.1.2 rsync

バージョン管理は不要であっても、低速ネットワーク接続を使用して大きなディレクトリ構造を同期させる必要がある場合は、ツールrsyncの適切に開発されたメカニズムを使用して、ファイル内の変更箇所のみを送信できます。この処理では、テキストファイルのみでなくバイナリファイルも対象となります。ファイル間の差分を検出するために、rsyncはファイルをブロック単位で分割してチェックサムを計算します。

変更内容の検出処理は高コストを伴います。rsyncの使用量に合わせて、同期対象となるシステムの規模を調整する必要があります。特に、RAMが重要です。

29.2 プログラムを選択する場合の決定要因

使用するプログラムを決定する際に重要な要因がいくつかあります。

29.2.1 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、CVSが使用します。

もう1つは、すべてのネットワークホストがそれぞれのデータをピアとして相互に同期させるモデルです。rsyncは、実際にクライアントモードで動作しますが、任意のクライアントがサーバとして動作できます。

29.2.2 移植性

CVS、およびrsyncは、各種のUNIXおよびWindowsシステムなど、他の多くのオペレーティングシステムでも使用できます。

29.2.3 インタラクティブと自動制御

CVSでは、ユーザが手動によってデータの同期を開始します。これにより、データの同期を詳細に制御でき、競合の処理も容易です。ただし、同期の間隔が長すぎると、競合が起こりやすくなります。

29.2.4 競合:問題と解決策

複数のユーザが大きなプログラミングプロジェクトにかかわっている場合も、CVSでは、競合はまれにしか発生しません。これはドキュメントが個別の行単位でマージされるためです。競合が起こると、影響を受けるのは1台のクライアントだけです。CVSでは、通常、競合が容易に解決できます。

rsyncには、競合処理の機能はありません。ユーザは、意図せずにファイルを上書きしないように注意し、考えられる競合はすべて手動で解決する必要があります。安全のために、RCSなどのバージョン管理システムを追加採用できます。

29.2.5 ファイルの選択と追加

CVSでは、新しいディレクトリやファイルは、コマンド`cvs add`を使って明示的に追加する必要があります。これにより、同期の対象となるファイルについて、ユーザがより詳細に制御できます。しかし他方で、新しいファイルが見過ごされることが多く、特に`cvs update`の出力に表示される疑問符は、ファイルの数が多いためにたびたび無視されます。

29.2.6 履歴

CVSは追加機能として、古いバージョンのファイルが再構成できます。変更を行うたびに簡単な編集コメントを挿入しておくと、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。

29.2.7 データ量と必要なハードディスク容量

同期の対象となるすべてのホストには、分散されたデータを処理できるだけの十分なハードディスクの空き容量が必要です。CVSでは、サーバ上のリポジトリデータベースに余分な容量が必要となります。ファイルの履歴もサーバに保存されるため、このための容量も別に必要です。テキスト形式のファイルが変更されたときには、変更された行だけを保存すれば足ります。バイナリファイルは、ファイルが変更されるたびに、ファイルのサイズと同じだけの容量が必要なため、テキストより必要な容量が多くなります。

29.2.8 GUI

CVSを使い慣れたユーザは、通常、コマンドラインでプログラムを制御します。しかし、cervisiaのようなLinux用のグラフィカルユーザインタフェースがあり、また他のオペレーティングシステム用にwincvsなども用意されています。kdevelopなどの開発ツールやEmacsなどのテキストエディタの多くが、CVSをサポートしています。競合の解決は、これらのフロントエンドの方が、はるかに容易です。

29.2.9 使いやすさ

rsyncは、より使いやすく初心者向けです。CVSは、より操作が難しくなっています。ユーザはレポジトリとローカルデータの間のインタラクションを理解する必要があります。データを変更すると、最初にローカルでリ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`または`update`で実行します。次にコマンド`cvs`または`commit`でデータをリポジトリに送信する必要があります。この手順をいったん理解すれば、初心者の方でもCVSを簡単に利用できるようになります。

29.2.10 攻撃に備えるセキュリティ

伝送中、データは妨害や改ざんから保護される必要があります。CVSやrsyncはいずれもssh(セキュアシェル)経由で容易に使用できるため、この種の攻撃からセキュリティ保護されます。CVSをrsh(リモートシェル)経由で実行するのは避けるべきです。また、安全でないネットワークで*pserver*メカニズムを使用してCVSにアクセスすることもお勧めできません。

29.2.11 データ損失からの保護

CVSは、プログラミングプロジェクト管理のため長期間にわたって開発者に使用されてきたため、きわめて安定しています。CVSでは開発履歴が保存されるため、誤ってファイルを削除するといったユーザの誤操作にも対応できます。

表 29.1　ファイル同期化ツールの機能: -- = とても悪い、- = 悪い、または利用不可、o = 普通、+ = 良好、++ = とても良好、x = 利用可能

	CVS	**rsync**
クライアント/サーバ	C-S	C-S
移植性	Lin、Un*x、Win	Lin、Un*x、Win
対話処理	x	x
Speed	o	+
競合	++	o
ファイル選択	Sel./file, dir.	ディレクトリ
履歴	x	-
ハードディスクスペース	--	o
GUI	o	-
難度	o	+
攻撃	+ (ssh)	+(ssh)
データ損失	++	+

29.3 CVSの概要

CVSは、個々のファイルが頻繁に編集され、ASCIIテキストやプログラムソーステキストのようなファイル形式で保存される場合の同期に適しています。CVSを使用して他の形式、たとえばJPEGファイルのデータを同期させることは可能ですが、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ため、結果としてデータ量が膨大になります。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。

29.3.1 CVSサーバの設定

サーバとは、すべてのファイルの最新バージョンを含め、有効なファイルが配置されるホストです。固定のワークステーションであれば、どれでもサーバとして使用できます。可能であれば、CVSレポジトリのデータを定期バックアップに含めます。

CVSサーバを設定するとき、できればユーザアクセスをSSH経由で許可します。ユーザがサーバにtuxとして認識され、CVSソフトウェアがサーバとクライアントにインストールされている場合、次の環境変数をクライアント側に設定する必要があります。

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

コマンドcvsinitを使用して、クライアント側からCVSサーバを初期化します。これは一度だけ実行すれば、後は必要ありません。

最後に、同期に名前を付ける必要があります。クライアント上で、CVSで管理するファイルのディレクトリ(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
```

29.3.2 CVSの使用

これで、すべてのホストがcvsco synchomeを使用して同期リ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、cvscommit 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、cvsadd 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、cvscommit 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リポジトリからチェックアウトしていない場合は、ここでチェックアウトします。

サーバとの同期は、cvs updateを使用して起動します。cvs update file1 directory1を使用すると、ファイルやディレクトリを個別に更新できます。現行のファイルとサーバに格納されているバージョンとの違いを確認するには、コマンドcvs diffまたはcvs diff file1 directory1を使用します。更新によって変更されたファイルを確認する場合は、cvs -nq updateを使用します。

更新時に表示されるステータス記号の例を次に示します。

U
: ローカルバージョンが更新されました。この更新はサーバが提供しているすべてのファイル、およびローカルにシステムに存在しないすべてのファイルに影響します。

M
: ローカルバージョンが変更されました。サーバ上で変更があれば、その差分がローカルコピーに取り込まれていることがあります。

P
: ローカルバージョンに対し、サーバ上のバージョンからパッチが適用されました。

C
: ローカルファイルが、レポジトリの現在のバージョンと競合しています。

?
　このファイルがCVSに存在しません。

ステータスMは、ローカルで変更されたファイルを示します。ローカルコピーをサーバにコミットするか、ローカルファイルを削除して更新を再実行します。この場合、不足しているファイルは、サーバから取得されます。ローカルに変更したファイルをコミットしたが、そのファイルで同じ行に変更があり以前にコミットされている場合は、競合がCで示されて表示されることがあります。

この場合、ファイル内の競合マーク(「>>」および「<<」)を確認し、2つのバージョンのどちらを採用するか決定します。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。

29.4 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。

29.4.1 設定と操作

rsyncには2つの操作モードがあります。このプログラムを使用してデータをアーカイブまたはコピーできます。そのためには、ターゲットシステム上にsshなどのリモートシェルがあれば十分です。ただし、rsyncをdaemonとして使用し、ネットワークにディレクトリを提供することもできます。

rsync の基本操作モードの場合、特別な設定は不要です。rsync では、ディレクトリ全体を別のシステムに直接ミラー化できます。たとえば、次のコマンドでは、tuxのホームディレクトリのバックアップがバックアップサーバsun上に作成されます。

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

次のコマンドは、ディレクトリを復元する場合に使用します。

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

ここまでの操作は、scpのような通常のコピーツールの場合とほぼ同じです。

rsyncのすべての機能を完全に使用可能にするには、「rsync」モードで操作する必要があります。そのためには、いずれかのシステムでrsyncdデーモンを起動します。設定はファイル/etc/rsyncd.conf内で行います。たとえば、rsyncでディレクトリ/srv/ftpを使用可能にするには、次の設定を使用します。

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

次に、rcrsyncdstartを使用してrsyncdを起動します。また、ブート処理中にrsyncdを自動的に起動する方法もあります。このようにセットアップするには、このサービスをYaSTのランラベルエディタで有効にするか、またはコマンド「insservrsyncd」を入力します。かわりに、xinetdからrsyncdを起動することもできます。ただし、この方法はrsyncdの使用頻度が低いサーバの場合にのみ使用してください。

この例では、すべての接続を示すログファイルも作成されます。このファイルは/var/log/rsyncd.logに格納されます。

これで、クライアントシステムからの転送をテストできます。そのためには次のコマンドを使用します。

```
rsync -avz sun::FTP
```

このコマンドを入力すると、サーバのディレクトリ/srv/ftpにあるファイルがすべてリストされます。このリクエストはログファイル/var/log/rsyncd.logにも記録されます。実際の転送を開始するには、ターゲットディレクトリを指定します。現在のディレクトリには..を使用してください。たとえば、次のようにします。

```
rsync -avz sun::FTP .
```

デフォルトでは、rsyncでの同期中にファイルは削除されません。ファイルを削除する必要がある場合は、オプション「--delete」を追加してください。新しい方のファイルが削除されないように、代わりにオプション--updateを使用することもできます。競合が発生した場合は、手動で解決する必要があります。

29.5 詳細情報

CVS

CVSの重要情報については、ホームページ「http://www.cvshome.org」を参照してください。

rsync

rsyncに関する重要な情報は、マニュアルページmanrsyncおよびmanrsyncd.confを参照してください。rsyncの基本原則に関する技術情報については、/usr/share/doc/packages/rsync/tech_report.psを参照してください。rsyncの最新ニュースについては、このプロジェクトのWebサイトhttp://rsync.samba.org/を参照してください。

30 Apache HTTPサーバ

Apache HTTPサーバ(Apache)は、世界で50%を超える市場シェアを持つ、最も広く利用されているWebサーバです(http://www.netcraft.com/の調査)。Apacheは、Apache Software Foundation (http://www.apache.org/)により開発され、ほとんどのオペレーティングシステムに対応しています。SUSE® Linux Enterprise Serverには、Apache version 2.2が付属しています。この章では、Webサーバのインストール/設定/セットアップの方法、SSL、CGI、および追加モジュールの使用方法、およびApacheのトラブルシュート方法について説明します。

30.1 クイックスタート

このセクションでは、Apacheを迅速に設定し、起動します。Apacheは、`root`としてインストールし、設定する必要があります。

30.1.1 要件

Apache Webサーバをセットアップする前に、次の要件が満たされていることを確認してください。

1. マシンのネットワークが適切に設定されているか。この項目の詳細については、第21章 *ネットワークの基礎* (287 ページ)を参照してください。

2. マシンの正確なシステム時間は、タイムサーバとの同期により維持されます。これは、HTTPプロトコルの一部が正確な時間に依存するために必要で

す。この項目の詳細については、第23章 *NTPによる時刻の同期*(367 ページ)を参照してください。

3. 最新のセキュリティアップデートがインストールされています。不明な場合は、YaSTオンラインアップデートを実行します。

4. ファイアウォールで、デフォルトのWebサーバポート(80)が開いています。ポートを開くには、外部ゾーンでの［*HTTPサーバ*］サービスが可能になるように、SuSEFirewall2lを設定します。これには、YaSTを使用します。詳細については、項 「Configuring the Firewall with YaST」 (第15章 *Masquerading and Firewalls*, ↑*Security Guide (セキュリティガイド)*)を参照してください。

30.1.2 インストール

SUSE Linux Enterprise Server上のApacheは、デフォルトではインストールされません。「そのまますぐに」実行できる標準の事前定義された設定を使用してインストールするには、次の手順を使用します。

手順 30.1 *デフォルト設定でApacheをインストールする*

1 YaSTを起動して、［*ソフトウェア*］>［*ソフトウェア管理*］の順に選択します。

2 ［*フィルタ*］>［*パターン*］の順に選択し、［*サーバ機能*］から［*Webおよび*LAMP*サーバ*］を選択します。

3 依存関係のあるパッケージのインストールを確認して、インストールプロセスを完了します。

このインストールには、`apache2-prefork` マルチプロセシングモジュールとPHP5モジュールが含まれています。モジュールの詳細については、30.4項「モジュールのインストール、有効化および設定」(505 ページ)を参照してください。

30.1.3 開始

Apacheは、ブート時に自動的に起動することも、手動で起動することもできます。

手順 30.2　Apacheを自動的に起動する

1 Apacheをランレベル3および5でブート時に自動的に起動するには、次のコマンドを実行します。

```
chkconfig -a apache2
```

2 または、YaSTを起動して［システム］>［システムサービス(ランレベル］の順に選択します。

3 サービスの［*apache2*］および［*有効*］を検索します。

Webサーバがすぐに起動します。

4 ［*完了*］をクリックして、変更を保存します。

ブート時にランレベル3および5で自動的にApatcheを起動するようにシステムが設定されます。

SUSE Linux Enterprise Serverでのランレベルの詳細、およびYaSTランレベルエディタについては、9.2.3項 「YaSTを使用したSystem Services (Runlevel)の設定」 (122 ページ)を参照してください。

シェルを使用してApacheを手動で起動するには、`rcapache2 start`を実行します。

手順 30.3　Apacheが実行中かどうかチェックする

Apacheの起動時にエラーメッセージが表示されなければ、通常、このWeb serverが実行されています。これをテストするには:

1 ブラウザを起動し、`http://localhost/`を開きます。

Apacheが立ち上がって稼動している場合は、「It works!」で始まるテストページが表示されます。

2 このページが表示されない場合は、30.8項 「トラブルシューティング」 (526 ページ)を参照してください。

Webサーバの起動後は、ドキュメントを追加、必要に応じて設定を調整、およびモジュールをインストールして機能を追加することができます。

30.2 Apacheの設定

SUSE Linux Enterprise Serverには、次の2つの設定オプションがあります。

- Apacheを手動で設定する (490 ページ)
- ApacheをYaSTで設定する (495 ページ)

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: 設定変更後のApacheのリロードまたは再起動

設定の変更は、ほとんどの場合、Apacheをリロード(または再起動)しないと有効になりません。`rcapache2 reload`を使用してApacheを手動でリロードするか、30.3項 「Apacheの起動および停止」 (502 ページ)に示されている再起動オプションの1つを使用します。

YaSTでApatcheを設定する場合、これを自動化するには、30.2.3.2項 「HTTPサーバの設定」 (500 ページ)で説明されているように、［*HTTPサービス*］を［*有効*］に設定します。

30.2.1 Apache設定ファイル

このセクションでは、Apache設定ファイルの概要を示します。環境設定にYaSTを使用する場合は、これらのファイルを操作する必要はありません。ただし、後で手動設定に切り替える場合に、この情報が役立つことがあります。

Apache設定ファイルは、次の2つの場所にあります。

- `/etc/sysconfig/apache2` (486 ページ)
- `/etc/apache2/` (487 ページ)

30.2.1.1 /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の内容を設定するだけで十分でしょう。

30.2.1.2 /etc/apache2/

/etc/apache2/には、Apacheのすべての設定ファイルが含まれます。ここでは、各ファイルの目的について説明します。各ファイルには、複数の設定オプション(*ディレクティブ*)が含まれています。これらのファイルの各設定オプションについては、詳細なドキュメントがあるので、ここでは説明しません。

Apache設定ファイルは、次のように編成されます。

```
/etc/apache2/
     |
     |- charset.conv
     |- conf.d/
     |   |
     |   |- *.conf
     |
     |- default-server.conf
     |- errors.conf
     |- httpd.conf
     |- listen.conf
     |- magic
     |- mime.types
     |- mod_*.conf
     |- server-tuning.conf
     |- ssl.*
     |- ssl-global.conf
     |- sysconfig.d
     |   |
     |   |- global.conf
     |   |- include.conf
     |   |- loadmodule.conf . .
     |
     |- uid.conf
     |- vhosts.d
     |   |- *.conf
```

「etc/apache2」内のApache設定ファイル

`charset.conv`
各言語に使用する文字セットを指定します。このファイルは、編集しないでください。

`conf.d/*.conf`
他のモジュールによって追加される設定ファイル。これらの設定ファイルは、必要に応じて仮想ホスト設定に含めることができます。その例として、`vhosts.d/vhost.template`を参照してください。設定ファイルを仮想ホスト設定に含めることにより、仮想ホストごとに別のモジュールセットを指定できます。

`default-server.conf`
すべての仮想ホストに対応するグローバル設定で、それぞれ適切なデフォルト値が指定されています。デフォルト値を変更する代わりに、仮想ホスト設定で上書きします。

`errors.conf`
Apacheによるエラーの対処方法を定義します。すべての仮想ホストに対してこれらのメッセージをカスタマイズするには、このファイルを編集します。カスタマイズしない場合は、仮想ホスト設定内のこれらのディレクティブを上書きします。

`httpd.conf`
メインのApacheサーバ設定ファイル。このファイルは変更しません。インクルード文およびグローバル設定が含まれています。ここに記載されている設定ファイルのグローバル設定を上書きします。仮想ホスト設定内のホスト固有の設定(ドキュメントルートなど)を変更します。

`listen.conf`
ApacheをIPアドレスおよびポートにバインドします。名前ベースの仮想ホスティングもこのファイルで設定します。詳細については、「名前ベースの仮想ホスト」 (491 ページ)を参照してください。

`magic`
Apacheが自動的に不明なファイルのMIMEタイプを判別できるようにするmime_magicモジュール用のデータ。このファイルは、変更しないでください。

mime.types
: システムで認識されるMIMEタイプ(実際には/etc/mime.typesへのリンク)。このファイルは、編集しないでください。このリスト以外にMIMEタイプを追加する必要がある場合は、mod_mime-defaults.confに追加します。

mod_*.conf
: デフォルトでインストールされるモジュール用の設定ファイル。詳細については、30.4項 「モジュールのインストール、有効化および設定」 (505 ページ)を参照してください。オプションのモジュール用の設定ファイルは、conf.dディレクトリ内にあります。

server-tuning.conf
: 各MPMの設定ディレクティブ(30.4.4項 「マルチプロセシングモジュール」 (510 ページ)を参照)、およびApacheのパフォーマンスを制御する一般的な設定オプションが含まれています。このファイルを変更する場合は、Webサーバを適切にテストしてください。

ssl-global.conf and ssl.*
: グローバルSSL設定およびSSL証明書データ。詳細については、30.6項 「SSLをサポートするセキュアWebサーバのセットアップ」 (517 ページ)を参照してください。

sysconfig.d/*.conf
: /etc/sysconfig/apache2から自動的に生成される設定ファイル。これらのファイルは、いずれも変更しません。その代わりに、/etc/sysconfig/apache2を編集します。このディレクトリに、他の設定ファイルを格納しないでください。

uid.conf
: Apacheを実行する際に使用するユーザおよびグループIDを指定します。このファイルは、変更しないでください。

vhosts.d/*.conf
: 仮想ホストの設定はこのファイルにあるはずです。このディレクトリには、SSLの有無に関わらず、仮想ホストのテンプレートファイルが格納されます。このディレクトリ内の .confで終わるファイルは、すべて自動的にApache設定に含まれます。詳細については、30.2.2.1項 「仮想ホスト設定」 (490 ページ)を参照してください。

30.2.2 Apacheを手動で設定する

Apacheを手動設定するには、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。

30.2.2.1 仮想ホスト設定

*仮想ホスト という用語は、同じ物理マシンから複数のURI (universal resource identifiers)のサービスを行えるApacheの機能を指し*ています。これは、たとえばwww.example.comやwww.example.netのような複数のドメインが、1台の物理コンピュータ上で動作する単一のWebサーバで処理されていることを表します。

管理の手間(1つのWebサーバを維持すればよい)とハードウェアの費用(ドメインごとの専用のサーバを必要としない)を省くために仮想ホストを使うことは、よく行われています。仮想ホストは名前ベース、IPベース、またはポートベースのいずれかになります。

すべての既存仮想ホストをリストするには、コマンドhttpd2 -Sを使用します。デフォルトサーバおよびすべての仮想ホストが、それらのIPアドレスおよびリスニングポートとともにリストに表示されます。リストには、各仮想ホストの設定ファイル内での位置を示すエントリも含まれています。

仮想ホストを設定するには、YaSTを使用するか(「仮想ホスト」 (498 ページ)で説明)、または設定ファイルを手動で編集します。SUSE Linux Enterprise ServerのApacheは、デフォルトでは、/etc/apache2/vhosts.d/内の仮想ホストごとに1つの設定ファイルを使用するようになっています。このディレクトリ内で、拡張子が.confのファイルは、すべて自動的に設定に含まれます。仮想ホストの基本的なテンプレートはこのディレクトリ内に用意されています(vhost.template、またはSSLサポートのある仮想ホストの場合はvhost-ssl.template)。

ヒント: 常に仮想ホスト設定を作成する

Webサーバに1つのドメインしか存在しない場合でも、常に仮想ホストの設定ファイルを作成することをお勧めします。そうすることによって、ドメイン固有の設定が1つのファイルにまとまるだけでなく、仮想ホストの設定ファイルを移動、削除、または名前変更することによって使用可能な基本

設定に常時フォールバックできます。同じ理由で、仮想ホストごとに個別の設定ファイルも作成します。

名前ベースの仮想ホストを使用する際、ドメイン名が仮想ホスト設定と一致しない場合に使用されるデフォルト設定を設定することを推奨します。デフォルト仮想ホストは、その設定が最初にロードされるホストです。設定ファイルの順序は、ファイル名で決定されるので、デフォルト仮想ホスト設定のファイル名は、下線文字(_)で始めて(たとえば、_default_vhost.conf)、そのファイルが最初にロードされるようにします。

<VirtualHost></VirtualHost>ブロックには、特定のドメインに適用される情報を記述します。Apacheは、クライアントから定義済みの仮想ホストへの要求を受け取ると、このセクションに記述されているディレクティブを使用します。仮想ホストでは、ほぼすべてのディレクティブを使用できます。Apacheの設定ディレクティブの詳細については、http://httpd.apache.org/docs/2.2/mod/quickreference.htmlを参照してください。

名前ベースの仮想ホスト

名前ベースの仮想ホストでは、1つのIPアドレスで複数のWebサイトを運用することができます。Apacheは、クライアントから送られたHTTPヘッダのホストフィールドを使用して、仮想ホスト宣言の1つの、一致するServerNameエントリに要求を接続します。一致するServerNameが見つからない場合には、指定されている最初の仮想ホストがデフォルトとして用いられます。

NameVirtualHostディレクティブは、HTTPヘッダ内のドメイン名を含むクライアントからの要求に関して、どのIPアドレス(オプションとして、どのポート)をリスンすべきかApatcheに指示しますこのオプションは、/etc/apache2/listen.conf設定ファイルで設定されます。

最初の引数には完全修飾ドメイン名を指定することができますが、IPアドレスを使用することをお勧めします。2番目の引数はポートで、オプションです。デフォルトでは、ポート80が使用され、Listen ディレクティブで設定されます。

ワイルドカード*は、IPアドレスとポート番号の両方で使用することができます。その場合、すべてのインタフェースでの要求を受け取ります。IPv6のアドレスは、角カッコの中に記述する必要があります。

例 30.1　名前ベースのVirtualHostエントリの応用例

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.3.100:80
NameVirtualHost 192.168.3.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:364::]:80
```

VirtualHost開始タグには、名前ベースの仮想ホスト設定でNameVirtualHostを引数として使用して以前に宣言されたIPアドレス(または完全修飾ドメイン名)が採用されます。NameVirtualHostディレクティブで以前に宣言されたポート番号はオプションです。

ワイルドカード*をIPアドレスの代わりに使うこともできます。この構文は、ワイルドカードをNameVirtualHost *として組み合わせて使用する場合にのみ有効です。IPv6アドレスを使用する場合には、アドレスを角カッコの中に記述することが必要です。

例 30.2　名前ベースのVirtualHostディレクティブ

```
<VirtualHost 192.168.3.100:80>
  ...
</VirtualHost>

<VirtualHost 192.168.3.100>
  ...
</VirtualHost>

<VirtualHost *:80>
  ...
</VirtualHost>

<VirtualHost *>
  ...
</VirtualHost>

<VirtualHost [2002:c0a8:364::]>
  ...
</VirtualHost>
```

IPベースの仮想ホスト

この仮想ホスト設定では、1つのコンピュータに対して複数のIPアドレスを設定する必要があります。Apacheの1つのインスタンスが、複数のドメインにホストとしてサービスを提供し、各ドメインに別のIPアドレスが割り当てられることになります。

物理サーバは、IPベースの仮想ホストごとに、1つのIPアドレスを持つ必要があります。マシンに複数のネットワークカードがない場合には、仮想ネットワークインタフェース(IPエイリアス)を使用することもできます。

次の例では、IP 192.168.3.100のマシンでApacheが実行されており、付加的なIP192.168.3.101および192.168.3.102をホストしています。すべての仮想サーバについて、VirtualHostブロックが個別に必要です。

例 30.3 IPベースのVirtualHostディレクティブ

```
<VirtualHost 192.168.3.101>
  ...
</VirtualHost>

<VirtualHost 192.168.3.102>
  ...
</VirtualHost>
```

ここでは、VirtualHostディレクティブは、192.168.3.100以外のインタフェースに対してのみ指定されています。Listenディレクティブが192.168.3.100に対しても設定される場合、このインタフェースへのHTTP要求に応答するために別のIPベースの仮想ホストを作成する必要があります。作成しない場合、デフォルトのサーバ設定(/etc/apache2/default-server.conf)内のディレクティブが適用されます。

基本的な仮想ホスト設定

仮想ホストをセットアップするには、少なくとも次のディレクティブが各仮想ホスト設定に含まれている必要があります。オプションについては、/etc/apache2/vhosts.d/vhost.templateを参照してください。

ServerName
: ホストに割り当てられている完全修飾ドメイン名。

DocumentRoot
: Apacheがこのホストにファイルをサービスする際に使用されるディレクトリパス。セキュリティ上の理由から、ファイルシステム全体へのアクセスはデフォルトで禁じられているため、Directoryコンテナ内でこのディレクトリを明示的にロック解除する必要があります。

ServerAdmin
: サーバ管理者の電子メールアドレス。このアドレスは、Apacheが作成するエラーページなどに表示されます。

ErrorLog
: この仮想ホストに関するエラーログファイル。仮想ホストごとに個別のエラーログファイルを作成する必要はありませんが、エラーのデバッグが簡単にできるため、作成されるのが一般的です。/var/log/apache2/はApacheのログファイルのデフォルトディレクトリです。

CustomLog
: この仮想ホストに関するアクセスログファイル。仮想ホストごとに個別のアクセスログファイルを作成する必要はありませんが、ホストごとのアクセス統計を個別に分析できるため、作成されるのが一般的です。/var/log/apache2/はApacheのログファイルのデフォルトディレクトリです。

セキュリティ上の理由から、ファイルシステム全体へのアクセスはデフォルトで禁じられています。したがって、DocumentRootなど、Apacheによりサービスされるファイルを保管したディレクトリを明示的にロック解除する必要があります。

```
<Directory "/srv/www/www.example.com/htdocs">
  Order allow,deny
  Allow from all
</Directory>
```

完全な設定ファイルは次のようになります。

例 30.4 *基本的な仮想ホスト設定*

```
<VirtualHost 192.168.3.100>
  ServerName www.example.com
  DocumentRoot /srv/www/www.example.com/htdocs
  ServerAdmin webmaster@example.com
  ErrorLog /var/log/apache2/www.example.com_log
  CustomLog /var/log/apache2/www.example.com-access_log common
  <Directory "/srv/www/www.example.com/htdocs">
    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

30.2.3 ApacheをYaSTで設定する

YaSTを使用してWebサーバを設定するには、YaSTを起動して、［ネットワークサービス］>［*HTTP*サーバ］の順に選択します。このモジュールを初めて起動するときに、［*HTTP*サーバウィザード］が起動して、サーバ管理に関していくつかの基本的な事項を決定するように要求されます。このウィザードの完了後、［*HTTP*サーバ］のモジュールを呼び出すたびに、［*HTTP*サーバの*環境設定*］ダイアログが起動します。詳細については、30.2.3.2項 「HTTPサーバの設定」 (500 ページ)を参照してください。

30.2.3.1 HTTP Server Wizard

HTTP Server Wizardには、5つのステップがあります。ダイアログの最後のステップでは、上級者用の設定モードに入って、さらに詳細な設定を行うかどうか選択できます。

Network Device Selection (ネットワークデバイスの選択)

ここでは、Apacheが着信リクエストをリスンするために使用する、ネットワークインタフェースとポートを指定します。既存のネットワークインタフェースとそれらに対応するIPアドレスから、任意のものを組み合わせて選択できます。他のサービスによって予約されていないものであれば、3つの範囲(ウェルノウンポート、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、ポート80ですべてのネットワークインタフェース(IPアドレス)をリスンします。

ファイアウォールでWebサーバがリスンするポートを開くには、［ファイアウォールで*ポートを開く*］をクリックします。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。外部からのWebサーバへのアクセスが不要なテスト段階でのみ、ポートを閉じておくことは有用です。複数のネットワークインタフェースが存在する場合は、［ファイアウォールの*詳細*...］をクリックして、ポートを開くインタフェースを指定します。

［次へ］ をクリックして設定を続けます。

モジュール

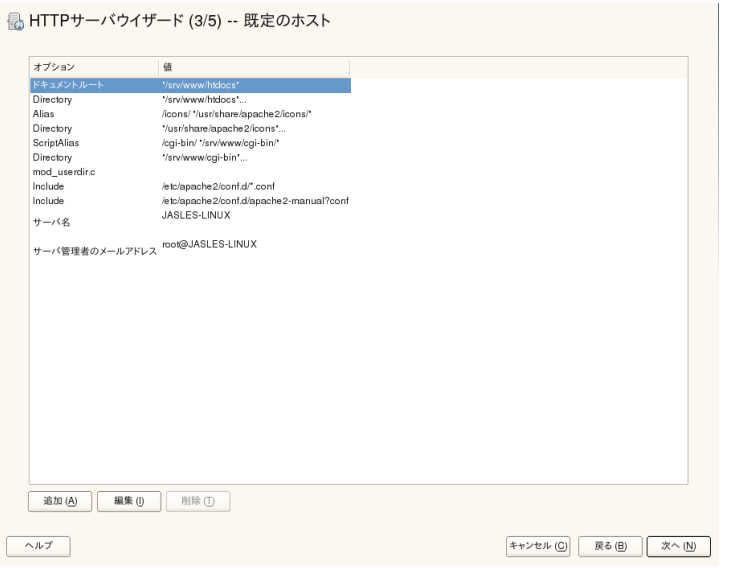
［モジュール］設定オプションによって、Webサーバでサポートされるスクリプト言語の有効化または無効化を設定できます。他のモジュールの有効化または無効化の詳細については、「サーバモジュール」 (501 ページ)を参照してください。［次へ］をクリックして次のダイアログに進みます。

Default Host (デフォルトのホスト)

このオプションは、デフォルトのWebサーバに関連しています。30.2.2.1項 「仮想ホスト設定」 (490 ページ)で説明されているように、Apacheは、1つの物理的マシンで複数の仮想ホストに使用することができます。設定ファイルで最初に宣言された仮想ホストは通常、デフォルトのホストと呼ばれます。各仮想ホストは、デフォルトホストの設定を継承します。

ホストの設定(*ディレクティブ*)を編集するには、テーブル内の適切なエントリを選択して、［*編集*］をクリックします。新しいディレクティブを追加するには、［*追加*］をクリックします。ディレクティブを削除するには、そのアカウントを選択し、［*削除*］をクリックします。

図 30.1 *HTTP Server Wizard:デフォルトホスト*



これはサーバのデフォルト設定のリストです。

ドキュメントルート
: Apacheがこのホストにファイルを送るときに使用されるディレクトリパス。/srv/www/htdocsはデフォルトの場所です。

別名
: Aliasディレクティブを使えば、URLを物理的なファイルシステムの場所にマップすることができます。このことは、パスのURLエイリアスを行えば、ファイルシステムのDocument Rootの外にあるパスでもアクセスできることを意味しています。

  デフォルトのSUSE Linux Enterprise Server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。

ScriptAlias
: Aliasディレクティブと同様に、ScriptAliasディレクティブはURLをシステム内の場所にマップします。相違点は、ScriptAliasはターゲットディレクトリをCGIの場所として指定するということです。つまり、その場所にあるCGIスクリプトが実行されます。

ディレクトリ
: ［ディレクトリ］設定を使用して、指定したディレクトリにのみ適用される設定オプションのグループを含めることができます。

  /srv/www/htdocs、/usr/share/apache2/icons、/srv/www/cgi-binディレクトリのアクセスおよび表示オプションをここで設定します。デフォルトを変更する必要はありません。

対象項目
: インクルードにより、他の設定ファイルを指定できます。2つのインクルードディレクティブが設定済みです。/etc/apache2/conf.d/は外部モジュールに付属する設定ファイルを保持するディレクトリです。このディレクティブにより、このディレクトリ内の.confで終わるすべてのファイルが対象となります。もう1つのディレクティブでは、/etc/apache2/conf.d/apache2-manual.confというapache2-manual設定ファイルが対象となります。

サーバ名
: クライアントがWebサーバとコンタクトするために使うデフォルトのURLを指定します。http://FQDN/にあるWebサーバへの接続用FQDN(完全修飾ドメイン名)か、またはそのIPアドレスを使用します。ここでは任意の名前は選択できません。サーバはこの名前で「認識」されなければなりません。

Server Administrator E-Mail
: サーバ管理者の電子メールアドレス。このアドレスは、Apacheが作成するエラーページなどに表示されます。

［デフォルトホスト］のステップを完了したら、［*次へ*］をクリックして、設定を続けます。

仮想ホスト

このステップでは、ウィザードはすでに設定されている仮想ホストのリストを表示します(30.2.2.1項 「仮想ホスト設定」 (490 ページ)を参照)。YaST HTTPウィザードを起動する前に手動で変更を行っていなければ、仮想ホストは表示されません。

ホストを追加するには、［*追加*］をクリックし、［*サーバ名*］、［*サーバのコンテンツルート*］(DocumentRoot)、［*管理者電子メール*］などホストに関する基本情報を入力するためのダイアログを開きます。［*サーバ解像度*］は、ホストの識別方法を決めるために使用されます(名前ベースまたはIPベース)。［*仮想ホストIDの変更*］で名前またはIPアドレスを指定します。

［*次へ*］をクリックして、仮想ホスト設定ダイアログの2番目の部分に進みます。

仮想ホスト設定のパート2では、CGIスクリプトを有効にするかどうか、およびこれらのスクリプトを使用するディレクトリを指定できます。また、SSLも有効にできます。SSLを有効化する場合は、証明書のパスも指定する必要があります。SSLおよび証明書の詳細については、30.6.2項 「SSLサポートのあるApacheの設定」 (522 ページ)を参照してください。［*ディレクトリインデックス*］オプションを使用して、クライアントがディレクトリを要求するときに表示するファイルを指定できます(デフォルトではindex.html)。ファイルを変更する場合は、1つ以上のファイル名(スペースで区切る)を追加します。［*公開HTMLを有効にする*］で、ユーザのパブリックディレクトリ(~*user*/public

_html/)のコンテンツが、サーバのhttp://www.example.com/~*user*からアクセスできるようにします。

重要: 仮想ホストの作成

仮想ホストを自由に追加することはできません。名前ベースの仮想ホストを使用する場合は、各ホスト名がネットワーク内で解決されている必要があります。IPベースの仮想ホストを使用する場合は、使用可能な各IPアドレスに対し1つのホストのみを割り当てることができます。

概要

これはウィザードの最後のステップです。ここでは、Apacheサーバをいつ、どのようにして起動するか(ブート時に起動するか、手動で起動するか)を指定します。また、ここまで行った設定の簡単な要約を確認します。この設定でよければ、［*完了*］をクリックして、設定を完了します。変更する場合は、希望のダイアログまで［*戻る*］をクリックして戻ります。［*HTTPサーバのエキスパート環境設定*］をクリックして、30.2.3.2項 「HTTPサーバの設定」 (500 ページ)で説明しているダイアログを開きます。

図 30.2 HTTP Server Wizard:概要

30.2.3.2 HTTPサーバの設定

［*HTTPサーバの設定*］ダイアログでは、ウィザード(Webサーバを最初に設定する場合にのみ実行)よりも詳細に設定を調整できます。このダイアログは、次で説明する4つのタブで構成されています。ここで変更する設定オプションは、すぐには適用されません。変更を適用するには、常に［*完了*］をクリックして変更を確認する必要があります。［*中止*］をクリックすると、設定モジュールを終了し、変更が破棄されます。

待ち受けポートおよびアドレス

［*HTTPサービス*］で、Apacheを実行するか(［*有効にする*］)、または停止するか(［*無効*］)を選択します。［*Listen on Ports*］で、サーバが使用可能なアドレスおよびポートについて［*追加*］、［*編集*］、または［*削除*］を選択します。デフォルトでは、ポート80ですべてのインタフェースをリスンします。常に［*ファイアウォールでポートを開く*］にチェックマークを入れておく必要があります。そうしないと、外部からWebサーバにアクセスできなくなります。外部からのWebサーバへのアクセスが不要なテスト段階でのみ、ポートを閉じておくことは有用です。複数のネットワークインタフェースが存在する場合は、［*ファイアウォールの詳細...*］をクリックして、ポートを開くインタフェースを指定します。

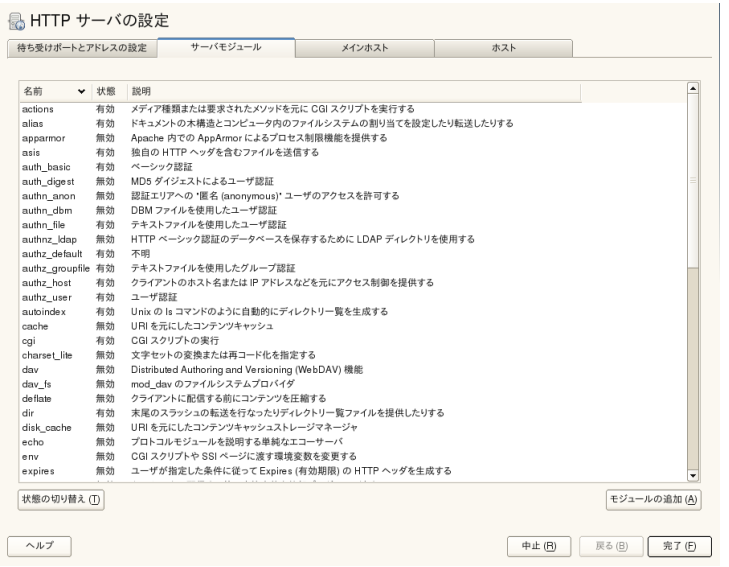
［*ログファイル*］で、アクセスログまたはエラーログのいずれかを確認します。これは、設定をテストする場合に便利です。ログファイルは別個のウィンドウに表示されますが、そこから、Webサーバを再起動または再ロードすることも可能です。詳細については、30.3項 「Apacheの起動および停止」 (502 ページ)を参照してください。これらのコマンドはすぐに有効になり、ログメッセージもすぐに表示されます。

*図 **30.3*** *HTTP Server Configuration:設定:リッスンポートとアドレス*

サーバモジュール

［*状態の変更*］をクリックして、Apache2モジュールのステータス(有効または無効)を変更できます。すでにインストールされているがリストに含まれていない新規モジュールを追加するには、［*Add Module*］をクリックします。モジュールの詳細については、30.4項 「モジュールのインストール、有効化および設定」 (505 ページ)を参照してください。

図 30.4　HTTP Server Configuration:サーバモジュール



メインホストまたはホスト

これらのダイアログは、すでに説明したものと同じです。詳細については、「Default Host (デフォルトのホスト)」 (496 ページ)および「仮想ホスト」 (498 ページ)を参照してください。

30.3 Apacheの起動および停止

Apacheは、30.2.3項 「ApacheをYaSTで設定する」 (495 ページ)の説明のようにYaSTで設定されると、ブート時にランレベル3および5で起動され、ランレベル0、1、2、および6で停止されます。YaSTのランレベルエディタまたはコマンドラインツールのchkconfigを使って、この動作を変更することができます。

実行中のシステムでApacheを起動、停止、操作するには、initスクリプト/usr/sbin/rcapache2を使用します。initスクリプトの一般的な情報については、9.2.2項 「initスクリプト」 (117 ページ)を参照してください。rcapache2コマンドでは、次のパラメータが使用されます。

`status`
Apacheが起動したかどうかチェックします。

`start`
Apacheが実行中でない場合に起動します。

`startssl`
SSLサポートのあるApacheが実行中でない場合に起動します。SSLサポートについての詳細は、30.6項 「SSLをサポートするセキュアWebサーバのセットアップ」 (517 ページ)を参照してください。

`stop`
親プロセスを終了して、Apacheを終了します。

`restart`
Apacheをいったん停止し、再起動します。Apacheが実行中でなかった場合は、新規に起動します。

`try-restart`
停止し、すでに実行している場合のみApacheを再起動します。

`reload`または`graceful`
フォークしたすべてのApacheプロセスに、シャットダウンする前に要求を完了させて、それからWebサーバを停止します。1つのプロセスが終了するたびに、新たに開始したプロセスで置き換えられるので、最終的にはApacheの完全な「再起動」になります。

ヒント: 運用環境でApacheを再起動する

接続を中断しないでApacheの変更を有効にするには、`rcapache2 reload`コマンドを使用します。

`restart-graceful`
すべての着信要求をただちに処理する2つ目のウェブサーバを起動します。ウェブサーバの以前のインスタンスは`GracefulShutdownTimeout`で設定された一定時間、引き続きすべの既存要求を処理します。

`rcapache2 restart-graceful`は、新しいバージョンへのアップグレード時、または再起動が必要な設定オプションの変更時に便利です。このオプションを使用すると、サーバのダウンタイムが最小限になります。

GracefulShutdownTimeoutの設定が必要です。これを設定しないと、restart-gracefulを指定しても、通常の再起動が行われます。ゼロに設定した場合、残っている要求がすべて完全に処理されるまで、サーバが無制限に待機します。

最初のApacheインスタンスが必要なリソースをすべてクリアできなかった場合、graceful restartは失敗します。この場合、コマンドの結果はgraceful stopとなります。

stop-graceful
既存要求の処理を完了できるように、GracefulShutdownTimeoutで設定された一定時間の経過後にウェブサーバを停止します。

GracefulShutdownTimeoutの設定が必要です。これを設定しないと、stop-gracefulを指定しても、通常のstopが実行されます。ゼロに設定した場合、残っている要求がすべて完全に処理されるまで、サーバが無制限に待機します。

configtestまたはextreme-configtest
実行中のWebサーバに影響することなく、設定ファイルの構文をチェックします。このチェックは、サーバが起動、再ロード、または再起動されるたびに強制されるので、通常は、明示的に実行する必要はありません(ただし、設定エラーが検出されると、ウェブサーバの起動/再ロード/再起動は行われません)。extreme-configtestオプションを指定すると、Webサーバがユーザnobodyとして起動し、設定を実際にロードするので、より多くのエラーを検出できます。ただし、設定はロードされますが、nobodyではSSL証明書を読み取れないため、SSLセットアップをテストすることはできません。

probe
再ロードの必要性を検出し(設定が変更されたかどうかを確認)、rcapache2コマンドに必要な引数を提示します。

server-status and full-server-status
それぞれ、簡単または完全ステータス画面を表示します。lynxまたはw3mのいずれかがインストールされ、モジュールmod_statusが有効になっている必要があります。これに加え、statusを/etc/sysconfig/apache2ファイルのAPACHE_SERVER_FLAGSに追加する必要があります。

ヒント: その他のフラグ

rcapache2にその他のフラグを指定すると、これらのフラグはWebサーバを通過します。

30.4 モジュールのインストール、有効化および設定

Apacheソフトウェアは、モジュール形式で構築されており、一部の主要タスクを除いてはモジュールごとに処理されます。この方法で、HTTPさえもモジュールによって処理されています(http_core)。

Apacheのモジュールは、ビルド時にApacheのバイナリに組み込むことも、実行時に動的にロードすることもできます。動的なモジュールのロード方法の詳細については、30.4.2項 「有効化と無効化」 (506 ページ)を参照してください。

Apacheモジュールは、次の4つのカテゴリに分類されます。

基本モジュール
: 基本モジュールは、デフォルトでApacheにコンパイルされています。SUSE Linux Enterprise ServerのApacheでは、mod_so(他のモジュールのロードに必要)およびhttp_coreのみがコンパイルされています。他のモジュールは、サーバのバイナリに入れる代わりに、ランタイム時に入れるように共有オブジェクトとして利用できます。

拡張モジュール
: 一般に、拡張とされているモジュールは、Apache ソフトウェアパッケージに含まれてはいますが、通常、サーバに静的にはコンパイルされていません。SUSE Linux Enterprise Serverでは、これらは実行時にApacheにロードすることができる共有オブジェクトとして利用可能になっています。

外部モジュール
: 外部とラベルされているモジュールは、公式のApacheのディストリビューションには含まれていません。ただし、SUSE Linux Enterprise Serverでは、そのいくつかを提供します。

MPM(マルチプロセシングモジュール)
MPMは、Webサーバへのリクエストを受け取って処理する役割を果たすもので、Webサーバソフトウェアの中核となっています。

30.4.1 モジュールのインストール

30.1.2項「インストール」(484ページ)で説明されているデフォルトインストールを行った場合は、すべての基本モジュールと拡張モジュール、マルチプロセシングモジュール、プリフォークMPM、および外部モジュールの`mod_php5`と`mod_python`がすでにインストールされています。

YaSTを起動し、［ソフトウェア］>［*ソフトウェアの管理*］の順に選択して、その他の外部モジュールをインストールできます。［フィルタ］>［*検索*］の順に選択し、*［apache］*を検索します。他のパッケージの中で、使用可能な外部Apacheモジュールがすべて検索結果のリストに表示されます。

30.4.2 有効化と無効化

特定モジュールの有効化/無効化は、手動で行うか、YaSTを使用します。YaSTでは、30.2.3.1項「HTTP Server Wizard」(495ページ)で説明されているモジュール設定を使用して、スクリプト言語モジュール(PHP5、Perl、およびPython)を有効または無効にする必要があります。その他のすべてのモジュールは、「サーバモジュール」(501ページ)で説明しているように有効化または無効化できます。

手動でモジュールを有効化または無効化する場合は、`a2enmod` *`mod_foo`*または`a2dismod`*`mod_foo`*コマンドをそれぞれ使用します。`a2enmod -l`は、すべての現在アクティブなモジュールのリストを出力します。

重要: 外部モジュール用の設定ファイルを含める

手動で外部モジュールを有効化した場合は、各設定ファイルがすべての仮想ホスト設定にロードされていることを確認します。外部モジュール用の設定ファイルは、`/etc/apache2/conf.d/`内に位置し、デフォルトではロードされません。各仮想ホスト上に同じモジュールが必要な場合は、このディレクトリ内の`*.conf`を含めることができます。必要でない場合は、

個々のファイルを含めます。その例として、「/etc/apache2/vhost.d/vhost.template」を参照してください。

30.4.3 基本および拡張モジュール

すべての基本および拡張モジュールは、Apacheのマニュアルに詳しく説明されています。ここでは、主要なモジュールについて簡単に説明します。各モジュールの詳細については、http://httpd.apache.org/docs/2.2/mod/を参照してください。

mod_actions
: 特定のMIMEタイプ(application/pdfなど)、特定の拡張子を持つファイル(.rpmなど)、または特定の要求方法(GETなど)が要求された場合に、常にスクリプトを実行する方法を提供します。このモジュールは、デフォルトで有効です。

mod_alias
: AliasおよびRedirectディレクティブを提供します。これにより、特定のディレクトリにURIをマップ(Alias)、または要求されたURLを別の場所にリダイレクトできます。このモジュールは、デフォルトで有効です。

mod_auth*
: 認証モジュールは、mod_auth_basicを使用する基本認証やmod_auth_digestを使用するダイジェスト認証などさまざまな認証方法を提供します。Apache 2.2のダイジェスト認証は実験的なものであると考えなくてはなりません。

  mod_auth_basicおよびmod_auth_digestは、認証プロバイダモジュールのmod_authn_*(たとえば、テキストファイルベースの認証用のmod_authn_file)および認証モジュールのmod_authz_*(たとえば、ユーザ認証用のmod_authz_user)と組み合わせる必要があります。

  この項目の詳細は、http://httpd.apache.org/docs/2.2/howto/auth.htmlの「*Authentication HOWTO*」で説明されています。

mod_autoindex
: Autoindexは、インデックスファイル(index.htmlなど)が存在しない場合にディレクトリリストを生成します。これらのインデックスのルックアン

ドフィールは設定可能です。このモジュールは、デフォルトで有効です。ただし、ディレクトリリストは、デフォルトでOptionsディレクティブを経由して無効化されています。仮想ホスト設定でこの設定を上書きします。このモジュール用のデフォルト設定は、/etc/apache2/mod_autoindex-defaults.confに存在します。

mod_cgi
: mod_cgiは、CGIスクリプトを実行するのに必要です。このモジュールは、デフォルトで有効です。

mod_deflate
: このモジュールを使用して、配信前にファイルタイプを圧縮するようにApacheを設定できます。

mod_dir
: mod_dirは、DirectoryIndexディレクティブを提供します。これを使用して、ディレクトリが要求されたときに(デフォルトではindex.html)自動的に配信されるファイルを設定できます。ディレクトリ要求に末尾のスラッシュが含まれていない場合は、正しいURLへの自動リダイレクトも提供します。このモジュールは、デフォルトで有効です。

mod_env
: CGIスクリプトやSSIページに渡す環境を制御します。環境変数を設定、設定解除したり、httpdプロセスを起動したシェルから渡すことができます。このモジュールは、デフォルトで有効です。

mod_expires
: mod_expiresを使用すると、Expiresヘッダの送信によって、プロキシとブラウザのキャッシュがドキュメントを更新する頻度を制御できます。このモジュールは、デフォルトで有効です。

mod_include
: mod_includeは、動的にHTMLページを生成するための基本機能を提供するSSI (Server-Side Includes)を使用できるようにします。このモジュールは、デフォルトで有効です。

mod_info
: http://localhost/server-info/にサーバ設定の包括的な概要を表示します。セキュリティ上の理由から、このURLへのアクセスは常に制限されます。デ

フォルトでは、localhostにのみ、このURLへのアクセスが許可されます。mod_infoは、/etc/apache2/mod_info.confで設定されます。

mod_log_config
: このモジュールを使用して、Apacheログファイルの書式を設定できます。このモジュールは、デフォルトで有効です。

mod_mime
: mimeモジュールは、ファイル名の拡張子(HTMLドキュメント用のtext/htmlなど)に基づいた、適切なMIMEヘッダを使用してファイルが配信されるようにします。このモジュールは、デフォルトで有効です。

mod_negotiation
: コンテンツネゴシエーションに必要です。詳細については、http://httpd.apache.org/docs/2.2/content-negotiation.htmlを参照してください。このモジュールは、デフォルトで有効です。

mod_rewrite
: mod_aliasの機能を提供しますが、それ以外の機能と柔軟性も提供します。mod_rewriteを使用すると、複数の規則、要求ヘッダなどに基づいてURLをリダイレクトできます。

mod_setenvif
: クライアントから送信されたブラウザ文字列やIPアドレスなどの、クライアントからのリクエスト詳細に基づいて環境変数を設定します。このモジュールは、デフォルトで有効です。

mod_speling
: mod_spelingは、大文字小文字の違いなど、URLの表記エラーの訂正を自動的に試みます。

mod_ssl
: Webサーバとクライアント間の暗号化接続を有効化します。詳細については、30.6項 「SSLをサポートするセキュアWebサーバのセットアップ」 (517 ページ)を参照してください。このモジュールは、デフォルトで有効です。

mod_status
: サーバの動作およびパフォーマンスに関する情報をhttp://localhost/server-status/に表示します。セキュリティ上の理由から、このURLへのアクセスは常に制限する必要があります。デフォルトでは、localhostにのみ、このURLへのアクセスが許可されます。mod_statusは、/etc/apache2/mod_status.confで設定されます。

mod_suexec
: mod_suexecは、CGIスクリプトを別のユーザとグループで実行できるようにします。このモジュールは、デフォルトで有効です。

mod_userdir
: ~*user*/の下に、ユーザ固有のディレクトリを用意します。UserDirディレクティブを設定で指定する必要があります。このモジュールは、デフォルトで有効です。

30.4.4 マルチプロセシングモジュール

SUSE Linux Enterprise Serverには、Apacheで使用するための2つの異なるMPM(マルチプロセシングモジュール)が用意されています。

- プリフォークMPM (510 ページ)
- 30.4.4.2項 「ワーカーMPM」 (511 ページ)

30.4.4.1 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。プリフォークMPMは、各要求を分離し、個々の子プロセスの分岐で処理するApacheバージョン 1.xと同じように、このWebサーバを動作させます。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: 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。

30.4.4.2 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マルチスレッドになります。このアプローチでは、プリフォークMPMの場合よりもシステムリソースの消費が少なくなるので、Apacheの性能が良くなります。

主な欠点としては、ワーカーMPMの安定性の問題が挙げられます。スレッドが壊れた場合、プロセスのすべてのスレッドに影響してしまいます。最悪の場合には、サーバがクラッシュすることがあります。特に、ApacheでCGI (Common Gateway Interface)を使用している場合、負荷が大きくなると、スレッドがシステムリソースと通信できなくなり、内部サーバエラーが生じることがあります。ワーカーMPMを使用すべきでないという意見の別の根拠は、利用できるApacheのモジュールのすべてがスレッドセーフになっているわけではなく、そのためワーカーMPMと組み合わせて使用することはできないという点です。

警告: MPMと組み合わせてPHPモジュールを使用する

利用可能なPHPモジュールのすべてがスレッドセーフになっているわけではありません。ワーカーMPMと`mod_php`は併用しないでください。

30.4.5 外部モジュール

ここでは、SUSE Linux Enterprise Serverに付属しているすべての外部モジュールのリストを示します。

mod-apparmor
: mod_php5やmod_perlなどのモジュールが処理する個々のCGIスクリプトに対して、AppArmor制限を提供するために、Apacheにサポートを追加します。

  パッケージ名:apache2-mod_apparmor
  詳細: パート 「Confining Privileges with AppArmor」 (↑*Security Guide (セキュリティガイド)*)

mod_mono
: mod_auth_kerbにより、Kerberos認証がApache Webサーバに提供されます。

  パッケージ名:apache2-mod_auth_kerb
  詳細: http://modauthkerb.sourceforge.net/configure.html

mod_mono
: mod_monoを使用すると、サーバでASP.NETページを実行できます。

  パッケージ名: apache2-mod_mono
  環境設定ファイル: /etc/apache2/conf.d/mod_mono.conf

mod_perl
: mod_perlは、埋め込まれているインタプリタでPerlスクリプトを実行できるようにします。サーバに埋め込まれている永続的なインタプリタにより、外部インタプリタの起動のオーバーヘッド、およびPerlの起動時間のペナルティを回避できます。

  パッケージ名: apache2-mod_perl
  環境設定ファイル: /etc/apache2/conf.d/mod_perl.conf
  詳細: /usr/share/doc/packages/apache2-mod_perl

mod_php5
: PHPは、サーバ側クロスプラットフォームのHTML埋込みスクリプト言語です。

  パッケージ名: apache2-mod_php5
  環境設定ファイル: /etc/apache2/conf.d/php5.conf
  詳細: /usr/share/doc/packages/apache2-mod_php5

mod_python
: mod_pythonは、Apache HTTPサーバへのPythonの埋込みができるようにし、Webベースのアプリケーションの設計で、さらに柔軟性を持たせ、パフォーマンスを向上させます。

パッケージ名: apache2-mod_python
詳細: /usr/share/doc/packages/apache2-mod_python

mod_security
: mod_securityにより、さまざまな範囲の攻撃からWebアプリケーションを保護するためのファイアウォールがWebアプリケーションに提供されます。さらに、HTTPトラフィックモニタリングおよびリアルタイム分析も可能です。

パッケージ名: apache2-mod_security2
環境設定ファイル: /etc/apache2/conf.d/mod_security2.conf
詳細: /usr/share/doc/packages/apache2-mod_security2
マニュアル: http://modsecurity.org/documentation/

30.4.6 コンパイル

上級ユーザは、カスタムのモジュールを記述してApacheを拡張することができます。Apache用のモジュールを開発したり、サードパーティのモジュールをコンパイルしたりするには、apache2-develパッケージ、および対応する開発ツールが必要です。apache2-develには、Apache用の追加モジュールのコンパイルに必要なapxs2ツールも含まれています。

apxs2は、ソースコードからモジュールをコンパイルし、インストールすることを可能にします(設定ファイルへの必要な変更も含みます)。これは、実行時にApacheにロードされる、*ダイナミック共有オブジェクト* (DSO)を作成します。

apxs2バイナリは、/usr/sbinの下層にあります

- /usr/sbin/apxs2—MPMと共に動作する拡張モジュールを構築するのに適しています。インストール場所は/usr/lib/apache2です。

- /usr/sbin/apxs2-prefork—プリフォークMPMモジュールに適しています。インストール場所は/usr/lib/apache2-preforkです。
- /usr/sbin/apxs2-worker—ワーカーMPMモジュールに適しています。インストール場所は/usr/lib/apache2-workerです。

次のコマンドで、ソースコードからモジュールをインストールして、アクティブにします。

```
cd /path/to/module/source; apxs2 -cia
    mod_foo.c
```

ここで、-cはモジュールをコンパイルし、-iはモジュールをインストールし、-aはモジュールをアクティブにします。apxs2のその他のオプションについては、apxs2(1) manページを参照してください。

30.5 CGIスクリプトの実行

ApacheのCGI (Common Gateway Interface)により、通常CGIスクリプトとして呼ばれるスクリプトまたはプログラムを含んだ動的コンテンツを作成できます。CGIスクリプトは、どのプログラム言語でも作成できます。通常、PerlまたはPHPなどのスクリプト言語が使用されます。

ApacheがCGIスクリプトで作成されたコンテンツを配信できるようにするには、mod_cgiを有効にする必要があります。mod_aliasも必要です。デフォルトでは、両モジュールとも有効化されています。モジュールの有効化の詳細については、30.4.2項 「有効化と無効化」 (506 ページ)を参照してください。

警告: CGIセキュリティ

サーバがCGIスクリプトを実行できるようになると、潜在的なセキュリティホールが発生します。詳細については、30.7項 「セキュリティ問題の回避」 (524 ページ)を参照してください。

30.5.1 Apacheの設定

SUSE Linux Enterprise Serverでは、CGIスクリプトの実行は、/srv/www/cgi-bin/ディレクトリでのみ許可されています。この場所は、すでにCGIスクリ

プトを実行するように設定されています。仮想ホスト設定を作成しておらず(30.2.2.1項「仮想ホスト設定」(490ページ)を参照してください)、ホスト固有のディレクトリにスクリプトを配置する場合は、このディレクトリのロックを解除し、設定する必要があります。

*例 **30.5** VirtualHost CGIの設定*

```
ScriptAlias /cgi-bin/ "/srv/www/www.example.com/cgi-bin/"❶

<Directory "/srv/www/www.example.com/cgi-bin/">
 Options +ExecCGI❷
 AddHandler cgi-script .cgi .pl❸
 Order allow,deny❹
 Allow from all
</Directory>
```

❶ このディレクトリ内のすべてのファイルをCGIスクリプトとして処理するようにApacheに指示します。

❷ CGIスクリプトの実行を有効化します。

❸ .plおよび.cgiの拡張子が付いたファイルをCGIスクリプトとして処理するようにサーバに指示します。必要に応じて調整します。

❹ `Order`ディレクティブと`Allow`ディレクティブは、デフォルトのアクセス状態と、許可および拒否のディレクティブが評価される順序を制御します。この場合、「deny」文の前に「allow」文が評価され、ユニバーサルアクセスが有効になります。

30.5.2 テストスクリプトの実行

CGIプログラミングは通常のプログラミングとは異なり、CGIプログラムとスクリプトの前に`Content-type: text/html`などのMIMEタイプヘッダを記述する必要があります。このヘッダはクライアントに送信されるので、クライアントは、受信したコンテンツによってコンテンツの種類を識別します。次に、このスクリプトの出力は、通常、Webブラウザなどのクライアントが認識できる形式(たいていの場合はHTML、プレーンテキスト、画像など)でなければなりません。

Apacheパッケージの一部として、`/usr/share/doc/packages/apache2/test-cgi`内に簡単なテストスクリプトが含まれています。このスクリプトは、いくつかの環境変数の内容をプレーンテキストとして出力します。このスクリプトを`/srv/www/cgi-bin/`か、仮想ホストのスクリプトディレクト

リ/srv/www/example.com_cgi-bin/のいずれかにコピーし、「test.cgi」という名前を付けます。

Webサーバがアクセスできるファイルは、rootユーザが所有している必要があります。詳細については、30.7項「セキュリティ問題の回避」(524ページ)を参照してください。Webサーバは別のユーザ名で実行しているので、CGIスクリプトはworld-executableおよびworld-readableである必要があります。CGIディレクトリに移動し、chmod 755 test.cgiコマンドを使用して適切なパーミッションを適用します。

次に、http://localhost/cgi-bin/test.cgiまたはhttp://www.example.com/cgi-bin/test.cgiを呼び出します。「CGI/1.0 test script report」を参照してください。

30.5.3 CGIトラブルシューティング

テストプログラムの出力の代わりにエラーメッセージが表示される場合は、次を確認します。

CGIトラブルシューティング

- 設定を変更した後、サーバを再ロードしましたか? rcapache2 probeを使用して確認します。
- カスタムCGIディレクトリを設定した場合、適切に設定されていますか?不明な場合は、デフォルトのCGIディレクトリの/srv/www/cgi-bin/内にあるスクリプトを実行し、http://localhost/cgi-bin/test.cgiを呼び出します。
- ファイルのパーミッションは正しいですか?CGIディレクトリに移動して、ls -l test.cgiを実行します。その出力が次で始まっているかどうかを確認します。

```
-rwxr-xr-x  1 root root
```

- そのスクリプトにプログラミングエラーがないかどうか確認します。test.cgiを変更しなかった場合は該当しませんが、独自のプログラムを使用する場合は、必ず、プログラミングエラーがないかどうか確認してください。

30.6 SSLをサポートするセキュアWebサーバのセットアップ

クレジットカード情報などの機密データをWebサーバやクライアント間で送信する場合は必ず、認証を使用して、安全で、暗号化された接続の確立を推奨します。mod_sslは、クライアントとWebサーバ間のHTTP通信にセキュアソケットレイヤ(SSL)プロトコルとトランスポートレイヤセキュリティ(TLS)プロトコルを使用して、強力な暗号化を行います。SSL/TLSを使用することにより、Webサーバとクライアント間でプライベートな接続が確立されます。データの整合性が保証され、クライアントとサーバ間で相互認証ができるようになります。

この目的で、サーバは、URLに対するリクエストに応答する前に、サーバの有効な識別情報を含むSSL証明書を送ります。これにより、サーバが唯一の正当な通信相手であることが保証されます。加えて、この証明書は、クライアントとサーバの間の暗号化された通信が、重要な内容がプレーンテキストとして見られる危険なしに、情報を転送できることを保証します。

mod_sslは、SSL/TSLプロトコル自体は実装しませんが、ApacheとSSLライブラリ間のインタフェースとして機能します。SUSE Linux Enterprise Serverでは、OpenSSLライブラリが使用されます。OpenSSLは、Apacheとともに自動的にインストールされます。

Apacheでmod_sslを使用した場合の最も明白な効果は、URLのプレフィックスがhttp://ではなくhttps://となることです。

ヒント: 証明書サンプル

パッケージapache2-example-certificatesをインストールすると、架空会社「Snake Oil」の証明書のサンプルを入手できます。

30.6.1 SSL証明書の作成

SSL/TSLをWebサーバで使用するには、SSL証明書を作成する必要があります。この証明書は、両者が互いに相手を識別できるように、Webサーバとク

ライアント間の認証に必要です。証明書の整合性を確認するには、すべてのユーザが信用する者によって署名される必要があります。

3種類の証明書を作成することができます。テストの目的のみの「ダミー証明書」、あらかじめ定義されている信用する一部のユーザグループ用の自己署名付き証明書、および公的な独立団体のCA (Certificate Authority)によって署名される証明書です。

証明書の作成には、基本的に2つのステップで行うことができます。はじめに、CAの秘密鍵が生成され、次に、この鍵を使用してサーバ証明書が署名されます。

ヒント: 詳細情報

SSL/TSLの概念および定義の詳細については、http://httpd.apache.org/docs/2.2/ssl/ssl_intro.htmlを参照してください。

30.6.1.1 ダミー「証明書の作成」

ダミー証明書の生成は簡単です。/usr/bin/gensslcertスクリプトを呼び出すだけです。次のファイルを作成または上書きします。gensslcertのオプションのスイッチを使用して、証明書を微調整します。詳細は、/usr/bin/gensslcert -hを呼び出してください。

- /etc/apache2/ssl.crt/ca.crt
- /etc/apache2/ssl.crt/server.crt
- /etc/apache2/ssl.key/server.key
- /etc/apache2/ssl.csr/server.csr
- /root/.mkcert.cfg

ca.crtのコピーは、ダウンロード用に/srv/www/htdocs/CA.crtにも配置されます。

重要: テスト専用

ダミー証明書は、実働システム上では使用しないでください。テストの目的のみで使用してください。

30.6.1.2 自己署名付き証明書の作成

イントラネットまたは定義されている一部のユーザグループ用にセキュアWebサーバをセットアップするとき、独自のCA (Certificate Authority)を通じて証明書に署名するので\'8f\'5c分な場合があります。

自己署名付き証明書の作成手順は、対話形式の9つのステップで構成されています。/usr/share/doc/packages/apache2ディレクトリに移動し、次のコマンドを実行します。/mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/ customこのディレクトリ以外からこのコマンドを実行しないでください。プログラムは、一連のプロンプトを表示します。この一部には、ユーザ入力が必要なものもあります。

手順 30.4 *mkcert.shを使用した自己署名付き証明書の作成*

1 証明書を使用してシグネチャアルゴリズムを決定します

一部の古いブラウザでDSAを使用すると問題があるため、RSA (デフォルトのR)を選択します。

2 CA用RSA秘密鍵を生成(1024ビット)

操作の必要はありません。

3 CAへのX.509証明書署名要求を生成

ここで、CAの識別名を作成します。このとき、国名または組織名など、いくつかの質問に答える必要があります。ここで入力した内容が証明書に含まれるため、有効なデータを入力します。すべての質問に答える必要はありません。該当しない、または空白のままにする場合は、「.」を使用します。一般名は、CA自体の名前です。*My company* CAなど、意味のある名前を選択します。

重要: CAの一般名

CAの一般名はサーバの一般名と異なる名前にする必要があるため、この手順では完全修飾ホスト名は選択しないでください。

4 CAによる署名用のX.509証明書を生成

証明書バージョン3を選択します(デフォルト)。

5 SERVER用のRSA秘密鍵を生成(1024ビット)

操作の必要はありません。

6 SERVERへのX.509証明書署名要求を生成

ここで、サーバの鍵の識別名を作成します。質問は、CAの識別名で答えたものとほぼ同じです。ここで入力するデータがWebサーバに適用されますが、CAのデータと同一である必要はありません(サーバが別の場所に位置する場合など)。

重要: 一般名の選択

ここで入力する一般名は、セキュアサーバの完全修飾ホスト名(www.example.comなど)である必要があります。完全修飾ホスト名でない場合、Webサーバへのアクセス時、証明書がサーバと一致していないという警告がブラウザに表示されます。

7 独自のCAによる署名付きX.509証明書を生成

証明書バージョン3を選択します(デフォルト)。

8 セキュリティ用パスフレーズのあるCAのRSA秘密鍵の暗号化

CAの秘密鍵をパスワードで暗号化することをお勧めします。そのため、Yを選択し、パスワードを入力します。

9 セキュリティ用パスフレーズのあるSERVERのRSA秘密鍵の暗号化

秘密鍵をパスワードで暗号化すると、Webサーバを起動するたびにこのパスワードを入力するよう求められます。このため、Webサーバのブートお

よび再起動時にサーバを自動的に起動するのが難しくなります。したがって、一般的に、この質問にはNと答えます。パスワードで暗号化しないと鍵は保護されないため、この鍵へのアクセスは許可されたユーザのみに限定する必要があることに注意してください。

重要: サーバ鍵の暗号化

サーバ鍵をパスワードで暗号化する場合は、`/etc/sysconfig/apache2`の`APACHE_TIMEOUT`の値を増やします。値を増やさないと、サーバを起動しようとする試みが停止する前に、パスフレーズを入力するのに十分な時間がなくなります。

スクリプトの結果ページに、生成された鍵と証明書のリストが表示されます。スクリプトの出力とは異なり、ファイルはローカルディレクトリの`conf`内ではなく、適切な場所である、`/etc/apache2/`内に生成されます。

最後のステップとして、Webブラウザ内の認識および信用されたCAのリストに含まれるように、ユーザがアクセスできる場所に`/etc/apache2/ssl.crt/ca.crt`からCA証明書ファイルをコピーします。コピーしない場合、ブラウザは、この証明書が不明な認証局から発行されたものであると見なします。証明書は1年間有効です。

重要: 自己署名付き証明書

自己署名付き証明書は、CA (Certificate Authority)として認識および信用するユーザによってアクセスされるWebサーバ上でのみ使用します。自己署名付き証明書をパブリックショップなどで使用することはお勧めしません。

30.6.1.3 公式に署名された証明書の取得

証明書に署名する公式なCA (Certificate Authority)は、多数存在します。証明書は、信用のあるサードパーティによって署名されるため、完全に信用できます。通常、一般に運営されているセキュアWebサーバでは、証明書が公式に署名されます。

最も良く知られている公式なCAには、Thawte (`http://www.thawte.com/`)またはVerisign (`http://www.verisign.com`)があります。これらや、その

他のCAは、すべてのブラウザにすでにコンパイルされているため、これらのCAによって署名された証明書は、ブラウザによって自動的に許可されます。

公式に署名された証明書を要求するとき、CAに証明書を送信しません。代わりに、CSR (Certificate Signing Request)を発行します。CSRを作成するには、`/usr/share/ssl/misc/CA.sh -newreq`スクリプトを呼び出します。

はじめに、スクリプトは、CSRの暗号化に使用されているパスワードを問い合わせてきます。その後、識別名を入力するよう求められます。このとき、国名または組織名など、いくつかの質問に答える必要があります。ここで入力した内容が証明書に含まれ、確認されるため、有効なデータを入力します。すべての質問に答える必要はありません。該当しない、または空白のままにする場合は、「.」一般名は、CA自体の名前です。*`My company`* CAなど、意味のある名前を選択します。最後に、チャレンジパスワードおよび代替の企業名を入力する必要があります。

スクリプトを呼び出したディレクトリでCSRを検索します。ファイルには、`newreq.pem`という名前が付きます。

30.6.2 SSLサポートのあるApacheの設定

WebサーバのSSLとTLS要求用のデフォルトのポートは443です。ポート80をリスンする「通常」のApacheと、ポート443をリスンするSSL/TL対応のApacheとの間に競合は生じません。通常、ポート80とポート443への要求はそれぞれ別の仮想ホストが処理し、別の仮想サーバに送られます。

重要: ファイアウォール設定

ポート443でSSL対応のApache用のファイアウォールを開くことを忘れないでください。ファイアウォールは、項 「Configuring the Firewall with YaST」 (第15章 *Masquerading and Firewalls*, ↑*Security Guide (セキュリティガイド)*) で説明されているように、YaSTを使用して設定できます。

SSLモジュールはグローバルサーバ設定でデフォルトで有効になっています。ホストで無効にされている場合は、コマンド`a2enmod ssl`で有効にします。最終的にSSLを有効にするには、サーバをフラグ「SSL」で起動する必要があります。このためには、`a2enflag SSL`を呼び出します。サーバ証明書をパスワードで暗号化している場合は、`/etc/sysconfig/apache2`で

APACHE_TIMEOUTの値を増やし、Apacheの起動時にパスフレーズを入力するのに十分な時間が与えられるようにします。これらの変更を適用するため、サーバを再起動します。再ロードでは不十分です。

仮想ホスト設定ディレクトリには、SSL固有ディレクティブが詳細に記述されている/etc/apache2/vhosts.d/vhost-ssl.templateテンプレートが含まれています。一般的な仮想ホスト設定については、30.2.2.1項「仮想ホスト設定」 (490 ページ)を参照してください。

始めるには、テンプレートを/etc/apache2/vhosts.d/*mySSL-host*.confにコピーして編集します。次のディレクティブの値を調整するだけです。

- DocumentRoot
- ServerName
- ServerAdmin
- ErrorLog
- TransferLog

30.6.2.1 名前ベースの仮想ホストとSSL

IPアドレスが1つだけのサーバで、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。名前ベースの仮想ホスティングでは、要求されたサーバ名をApacheが知っている必要があります。SSL接続の問題は、SSL接続が(デフォルトの仮想ホストの使用により)確立された後でのみ、そのような要求の読み込みが可能なことです。その結果、証明書がサーバ名に一致しないという警告メッセージが表示されます。

SUSE Linux Enterprise Serverは、SNI (Server Name Indication)と呼ばれるSSLプロトコルの拡張を組み込んでおり、仮想ドメインの名前をSSLネゴシエーションの一部として送信することで、この問題を解決します。これにより、サーバが正しい仮想ドメインに早く「切り替わり」、ブラウザに正しい証明書を提示することが可能になります。

SUSE Linux Enterprise Serverでは、デフォルトでSNIが有効になっています。名前ベースの仮想ホストをSSLで使用可能にするには、「名前ベースの仮想ホ

スト」(491ページ)で説明されているようにサーバを設定します(ただし、SSLでは、ポート80ではなく、ポート443を使用)。

重要: SNIブラウザのサポート

SNIは、クライアント側でもサポートされる必要があります。SNIは、ほとんどのブラウザでサポートされていますが、モバイルハードウェアの一部のブラウザやWindows* XP上のInternet ExplorerとSafariにはSNIのサポートがありません。詳細については、http://en.wikipedia.org/wiki/Server_Name_Indicationを参照してください。

ディレクティブSSLStrictSNIVHostCheckを使用して、SNIに非対応のブラウザを処理する方法を設定しますSNI非対応ブラウザは、サーバ設定でonに設定されると、すべての仮想ホストに関して拒否されます。VirtualHostディレクティブ内でonに設定されると、この特定のホストへのアクセスが拒否されます。

サーバ設定でoffに設定されると、サーバはSNIサポートがないかのように動作します。SSL要求は、(ポート443に対して)定義された*最初の*仮想ホストによって処理されます。

30.7 セキュリティ問題の回避

公共のインターネットに公開しているWebサーバについては、管理面での不断の努力が求められます。ソフトウェアと、偶然の設定ミスの両方に関連したセキュリティの問題が発生することは避けられません。それらに対処するためのいくつかのヒントを紹介します。

30.7.1 最新版のソフトウェア

Apacheソフトウェアに脆弱性が見つかると、SUSEからセキュリティ上の勧告が出されます。これには、脆弱性を修正するための指示が含まれているので、可能な限り早期の適用が必要です。SUSEセキュリティ通知は、次の場所から入手できます。

- **Webページ** http://www.novell.com/linux/security/securitysupport.html

- メーリングリストのアーカイブ http://lists.opensuse.org/opensuse-security-announce/
- RSSフィード http://www.novell.com/linux/security/suse_security.xml

30.7.2 DocumentRootのパーミッション

SUSE Linux Enterprise Serverのデフォルトでは、DocumentRootディレクトリの/srv/www/htdocsおよびCGIディレクトリの/srv/www/cgi-binは、ユーザおよびグループrootに属します。これらのパーミッションは変更しないでください。ディレクトリにすべてのユーザが書き込み可能な場合、どのユーザもそれらのディレクトリにファイルを格納できます。その後これらのファイルは、Apacheによりwwwrunのパーミッションで実行されます。その結果、意図しない仕方で、ユーザがファイルシステムのリソースにアクセスできるようになる可能性があります。/srv/wwwのサブディレクトリを使用して仮想ホストのDocumentRootおよびCGIディレクトリを配置し、このユーザおよびグループのrootがディレクトリとファイルの所有者であることを確認します。

30.7.3 ファイルシステムアクセス

デフォルトでは、ファイルシステム全体へのアクセスは、/etc/apache2/httpd.confで定義されています。これらのディレクティブは決して上書きしないでください。ただし、Apacheが読み込む必要のあるすべてのディレクトリに対するアクセスは有効にしてください。詳細については、「基本的な仮想ホスト設定」(493ページ)を参照してください。このためには、パスワードまたはシステム設定ファイルなど重要なファイルは外部から読み取ることができないことを確認します。

30.7.4 CGIスクリプト

Perl、PHP、SSIまたは他のプログラミング言語によるインタラクティブなスクリプトは、事実上、任意のコマンドを実行できるため、一般的なセキュリティの問題が存在します。サーバから実行されるスクリプトは、サーバの管理者が信用するソースからのみインストールされる必要があります。一般的

には、ユーザが独自のスクリプトを実行できる環境は適切ではありません。また、すべてのスクリプトに対してセキュリティ監査を行うこともお勧めします。

スクリプトの管理をできるだけ簡単にするため、CGIスクリプトの実行をグローバルに許可するのではなく、通常、特定のディレクトリに制限されています。設定には、ディレクティブのScriptAliasおよびOption ExecCGIが使用されます。SUSE Linux Enterprise Serverのデフォルト設定では、任意の場所からのCGIスクリプトの実行は許可されません。

すべてのCGIスクリプトは同一のユーザとして実行するため、異なるスクリプトが互いに競合する可能性があります。suEXECモジュールは、CGIスクリプトを別のユーザとグループで実行できるようにします。

30.7.5 ユーザディレクトリ

ユーザディレクトリを(mod_userdirまたはmod_rewriteを使用して)有効化する場合は、.htaccessファイルを許可しないことをお勧めします。これらのファイルは、ユーザによるセキュリティ設定の上書きを可能にするからです。AllowOverRideディレクティブを使用して、少なくとも、ユーザの操作を制限する必要があります。SUSE Linux Enterprise Serverでは、.htaccessファイルはデフォルトで有効化されていますが、ユーザはmod_userdirの使用時にいずれのOptionディレクティブも上書きできません(詳細は、/etc/apache2/mod_userdir.conf設定ファイル参照)。

30.8 トラブルシューティング

Apacheが起動しないと、Webページにアクセスすることはできず、ユーザがWebサーバに接続することもできないので、問題の原因を見つけ出すことは重要です。次に、エラーが説明されている場所とチェックすべき重要事項について説明します。

rcapache2の出力
: Webサーバをバイナリの/usr/sbin/httpd2で起動/停止する代わりに、rcapache2スクリプトを使用します(30.3項 「Apacheの起動および停止」 (502 ページ)参照)。このスクリプトは、エラーを詳細に説明し、設定エラーを修正するコツやヒントも提供します。

ログファイルと冗長性レベル
: 致命的エラーと致命的でないエラーの両方について、Apacheログファイル(主に、デフォルトで/var/log/apache2/error_logにあるエラーログファイル)をチェックしてください。さらに、ログファイルにさらに詳細な情報を記録することが必要な場合には、LogLevelディレクティブで、記録されるメッセージの詳細を制御することができます。

ヒント: 簡単なテスト

`tail -F /var/log/apache2/`*`my_error_log`*コマンドで、Apacheのログメッセージを確認します。それから、`rcapache2 restart`を実行します。そして、ブラウザでの接続をもう一度試みて、出力を確認してください。

ファイアウォールとポート
: よくある間違いで、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があります。YaSTでApacheを設定する場合には、この点を扱うための別のオプションが存在します(30.2.3項 「ApacheをYaSTで設定する」 (495 ページ)を参照してください)。Apacheを手動で設定する場合は、YaSTのファイアウォールモジュールを使用してHTTPとHTTPS用のファイアウォールポートを開きます。

このようにしても、エラーを特定できない場合には、http://httpd.apache.org/bug_report.htmlの、オンラインのApacheバグデータベースをチェックしてください。加えて、http://httpd.apache.org/userslist.htmlのメーリングリストで、Apacheのユーザコミュニティに参加することができます。お勧めできるニュースグループは、comp.infosystems.www.servers.unixです。

30.9 詳細情報

apache2-docパッケージには、ローカルインストールおよび参照用にそれぞれローカライズされている完全なApacheマニュアルが含まれています。これは、デフォルトではインストールされません。このマニュアルを最も素早くインストールするには、`zypper in apache2-doc`コマンドを使用します。Apacheマニュアルは、インストールされると、http://localhost/manual/から表示できるようになります。また、Webのhttp://httpd.apache.org/

docs-2.2/からもアクセスできます。SUSE固有の設定に関するヒントについては、/usr/share/doc/packages/apache2/README.*を参照してください。

30.9.1 Apache 2.2

Apache 2.2の新機能のリストは、http://httpd.apache.org/docs/2.2/new_features_2_2.htmlを参照してください。バージョン2.0から2.2へのアップグレード情報もhttp://httpd.apache.org/docs-2.2/upgrading.htmlで参照できます。

30.9.2 Apacheモジュール

30.4.5項 「外部モジュール」 (511 ページ)で簡単に説明されている外部Apacheモジュールの詳細は、次の場所で入手できます。

mod-apparmor
http://en.opensuse.org/SDB:AppArmor

mod-auth_kerb
http://modauthkerb.sourceforge.net/

mod_mono
http://www.mono-project.com/Mod_mono

mod_perl
http://perl.apache.org/

mod_php5
http://www.php.net/manual/en/install.unix.apache2.php

mod_python
http://www.modpython.org/

mod_security
http://modsecurity.org/

30.9.3 開発

Apacheモジュールの開発、またはApache Webサーバプロジェクトへの参加に関する情報については、次を参照してください。

Apache開発情報
http://httpd.apache.org/dev/

Apache開発者ドキュメント
http://httpd.apache.org/docs/2.2/developer/

PerlおよびCを使用したApacheモジュールの作成
http://www.modperl.com/

30.9.4 その他の情報源

SUSE Linux Enterprise ServerのApacheに固有な問題が発生した場合は、Technical Information Search (http://www.novell.com/support)を参照してください。Apacheの沿革は、http://httpd.apache.org/ABOUT_APACHE.html で参照できます。このページでは、Apacheというサーバ名の由来についても説明しています。

YaSTを使用したFTPサーバの設定

31

YaST［*FTP*サーバ］モジュールを使用すると、コンピュータをFTP(File Transfer Protocol)サーバとして機能するように設定できます。匿名および/または認証されたユーザがコンピュータに接続し、FTPプロトコルを使用してファイルをダウンロードできます。設定によっては、それらのユーザがFTPサーバにファイルをアップロードすることも可能です。YaSTは、システムにインストールされた各種のFTPサーバデーモンに統一された設定インタフェースを提供しています。

YaST［*FTP サーバ*］設定モジュールを使用すると、2つの異なるFTPサーバデーモンを設定できます。

- `vsftpd` (Very Secure FTP Daemon) 、および
- `pure-ftpd`

設定できるのは、インストール済みサーバだけです。

vsftpdサーバとpure-ftpdサーバの設定オプションは多少異なります(特に、［エキスパート設定］ダイアログ)。この章では、vsftpdサーバ

YaST FTPサーバモジュールがシステム内にない場合は、`yast2-ftp-server` パッケージをインストールしてください。

YaSTで、FTPサーバを設定するには、次の手順に従います。

1 YaSTコントロールセンターを開き、［*ネットワークサービス*］>［*FTP Server*］の順に選択するか、rootとしてyast2 ftp-serverコマンドを実行します。

2 システムにFTPサーバがインストールされていない場合は、YaST FTPサーバモジュールの起動時に、インストールするサーバをどれにするか質問されます。サーバを選択し、ダイアログで確認します。2つのサーバがインストールされている場合は、サーバを選択して、［*OK*］をクリックします。

3 ［*起動*］ダイアログで、FTPサーバの起動に関するオプションを設定します。詳細については、31.1項 「FTPサーバの起動」 (532 ページ)を参照してください。

［*一般*］ダイアログで、FTPディレクトリ、歓迎メッセージ、ファイル作成マスクなどの各種パラメータを設定します。詳細については、31.2項 「FTP一般設定」 (533 ページ)を参照してください。

［*Performance*］ダイアログで、FTPサーバの負荷に影響するパラメータを設定します。詳細については、31.3項 「FTPパフォーマンス設定」 (534 ページ)を参照してください。

［*認証*］ダイアログで、匿名および/または認証されたユーザに対してFTPサーバを使用可能にするかどうか設定します。詳細については、31.4項 「認証」 (535 ページ)を参照してください。

［エキスパート*設定*］ダイアログで、FTPサーバの操作モード、SSL接続、およびファイアウォール設定を設定します。詳細については、31.5項 「エキスパート設定」 (535 ページ)を参照してください。

4 ［*完了*］を押して設定を保存します。

31.1 FTPサーバの起動

［*FTP Start-Up*］ダイアログの［*サービス開始*］フレームで、FTPサーバを起動する方法を設定します。システムブート時の自動的なサーバ起動とサーバの手動起動のどちらかを選択できます。FTP接続要求後にのみFTPサーバを起動する場合は、［*xinetd経由*］を選択します。

FTPサーバの現在のステータスが、［*FTP Start-Up*］ダイアログの［*開始/停止*］フレームに表示されます。［*FTPを開始する*］をクリックして、FTPサーバを起動します。サーバを停止するには、［*FTPを停止する*］をクリックします。サーバの設定を変更したら、［*設定を保存してFTPを再起動する*］をクリックします。［*完了*］を押して設定モジュールを終了すると、設定が保存されます。

［*FTP起動*］ダイアログの［*選択されたサービス*］フレームに、使用されるFTPサーバ(vsftpdまたはpure-ftpd)が表示されます。両方のサーバがインストールされている場合、それらの間で切り替えることができます。現在の設定は自動的に変換されます。

図 31.1　FTPサーバの設定 ― 起動

31.2 FTP一般設定

［*FTP General Settings*］ダイアログの［*一般の設定*］フレームで、FTPサーバへの接続後に表示される［*Welcome message*］を設定できます。

［*Chroot Everyone*］オプションをオンにした場合は、すべてのローカルユーザが、ログイン後、ホームディレクトリのchroot jailに配置されます。このオ

プションは、セキュリティに影響します(特に、ユーザがアップロードパーミッションまたはシェルアクセスを持つ場合)。したがって、このオプションの有効化には、注意が必要です。

［*Verbose Logging*］オプションをオンにすると、すべてのFTP要求と応答がログされます。

匿名および/または認証されたユーザが作成するファイルのパーミッションは、umaskで制限できます。［*Umask for Anonymous*］)］で匿名ユーザ用のファイル作成マスクを設定し、［*Umask for Authenticated Users*］で認証されたユーザ用のファイル作成マスクを設定します。マスクは、必ずゼロで始まる8進数として入力してください。umaskの詳細については、umaskマニュアルページ(`man 1p umask`)を参照してください。

［*FTP Directories*］フレームで、匿名/認証されたユーザ用のディレクトリを設定します。［*参照*］をクリックすると、ローカルファイルシステムから使用できるディレクトリを選択できます。匿名ユーザのデフォルトFTPディレクトリは、`/srv/ftp`です。ただし、vsftpdでは、このディレクトリにすべてのユーザが書き込むことはできません。代わりに、書き込みパーミッション付きのサブディレクトリ`upload`が匿名ユーザ用に作成されます。

注記: FTPディレクトリの書込みパーミッション

pure-ftpdサーバでは、匿名ユーザ用のFTPディレクトリを書き込み可能にできます。サーバ間で切り換えを行う場合は、vsftpdサーバに戻す前に、pure-ftpdで使用したディレクトリから書き込みパーミッションを削除したことを確認してください。

31.3 FTPパフォーマンス設定

［パフォーマンス］ダイアログで、FTPサーバの負荷に影響するパラメータを設定します。［*Max Idle Time*］は、リモートクライアントがFTPのコマンド間で待機できる最大時間(分)です。これよりアクティビティのない時間が長くなると、リモートクライアントの接続は切断されます。［*Max Clients for One IP*］では、1つのIPアドレスから接続できるクライアントの最大数を決定します。［*最大クライアント*］では、接続できるクライアントの最大数を決定します。クライアントをさらに追加すると、エラーメッセージが表示されます。

最大データ転送速度(KB/秒)の設定は、ローカルの認証されたユーザについては［*Local Max Rate*］、匿名クライアントについては［*Anonymous Max Rate*］で行います。速度設定のデフォルト値は、0であり、無制限のデータ転送速度を意味します。

31.4 認証

［*認証*］ダイアログの［*Enable/Disable Anonymous and Local Users*］フレームでは、どのユーザにFTPサーバへのアクセスを許可するか設定できます。次のオプションのいずれかを選択できます: 匿名ユーザのみ、(システムにアカウントのある)認証されたユーザのみ、またはその両方のタイプのユーザにアクセスを付与します。

FTPサーバへのファイルのアップロードを許可するには、［*認証*］ダイアログの［*Uploading*］フレームにある［*Enable Upload*］をオンにします。ここでは、各ボックスにチェック印を入れることで、匿名ユーザにも、アップロードまたはディレクトリの作成を許可できます。

注記: **vsftp—匿名ユーザのファイルのアップロードを許可する**

vsftpdサーバを使用し、匿名ユーザにファイルをアップロードさせたり、ディレクトリを作成させる場合は、すべてのユーザ用書き込みパーミッション付きのサブディレクトリを、匿名FTPディレクトリ内に作成する必要があります。

31.5 エキスパート設定

FTPサーバは、アクティブモードまたはパッシブモードで実行できます。デフォルトでは、サーバはパッシブモードで実行されます。アクティブモードに切り換えるには、［エキスパート設定］ダイアログの［*パッシブモードを許可する*］オプションのチェックをオフにするだけです。データストリーム用に使用するサーバのポート範囲を変更することもできます。このためには、［*Min Port for Pas. Mode*］と［*Max Port for Pas. Mode*］のオプションを微調整します。

クライアントとサーバ間で暗号化された通信が必要な場合は、［*SSLを有効に*］できます。サポートされるプロトコルのバージョンをチェックし、SSL暗号化接続で使用されるDSA証明書を指定します。

システムがファイアウォールで保護されている場合は、［*ファイアウォール内でポートを開く*］をオンにして、FTPサーバへの接続を有効にします。

31.6 さらに詳細な説明が必要な場合は

FTPサーバの詳細については、`pure-ftpd`、`vsftpd`、および`vsftpd.conf`のマニュアルページを参照してください。

32 Squidプロキシサーバ

Squidは、LinuxおよびUNIXプラットフォームで普及しているプロキシキャッシュです。これは、WebまたはFTPサーバなど、要求されたインターネットオブジェクトを、サーバよりも要求しているワークステーションに近いマシン上に格納することを意味します。Squidは、応答時間や低帯域幅の使用を最適化するために複数の階層上でセットアップされます。エンドユーザにとって透過的なモードである場合さえあります。squidGuardを利用すれば、Webコンテンツをフィルタリングすることができます。

Squidはプロキシキャッシュとして機能します。クライアント(この場合はWebブラウザ)からのオブジェクト要求をサーバにリダイレクトします。要求されたオブジェクトがサーバから到着すると、クライアントに配信され、そのコピーがディスクキャッシュに格納されます。キャッシングの利点の1つは、様々なクライアントが同じオブジェクトを要求した場合に、これらのオブジェクトをハードディスクのキャッシュから提供できることです。これにより、クライアントはインターネットから取得する場合に比べてはるかに高速にデータを受信できます。また、ネットワークトラフィックも減少します。

Squidは、実際のキャッシングとともに、プロキシサーバの通信階層にまたがる負荷の分散、プロキシにアクセスする全クライアントの厳密なアクセス制御リストの定義、他のアプリケーションを使用した特定のWebページへのアクセスの許可または拒否、ユーザのアクセスパターンの調査を目的としたアクセス回数の多いWebサイトに関する統計の生成など、多様な機能を備えています。Squidは汎用プロキシではありません。通常は、HTTP接続のみのプロキシを行います。また、FTP、Gopher、SSL、およびWAISの各プロトコルをサポートしていますが、Real Audio、news、またはビデオ会議など、他のインターネットプロトコルはサポートしていません。Squidは様々なキャッシュ

間に通信を提供するUDPプロトコルのみをサポートしているため、他の多くのマルチメディアプログラムはサポートされません。

32.1 プロキシキャッシュに関する注意事項

プロキシキャッシュとして、Squidは複数の方法で使用されます。ファイアウォールと組み合わせると、セキュリティに役立ちます。複数のプロキシを一緒に使用できます。また、キャッシュされるオブジェクトのタイプ、およびその期間も決定できます。

32.1.1 Squidとセキュリティ

Squidをファイアウォールと併用し、プロキシキャッシュを使用して社内ネットワークを外部から保護することもできます。ファイアウォールは、Squidを除く外部サービスに対する全クライアントのアクセスを拒否します。すべてのWeb接続は、プロキシを使用して確立する必要があります。この設定では、SquidはWebアクセスを完全に制御します。

ファイアウォール設定にDMZが含まれている場合、プロキシはこのゾーン内で動作しなければなりません。「*透過的な*」プロキシの実装方法については、32.5項 「透過型プロキシの設定」 (550 ページ)を参照してください。この場合、プロキシに関する情報が必要とされないので、クライアントの設定が簡略化されます。

32.1.2 複数のキャッシュ

複数のSquidインスタンスを設定して、これらの間でオブジェクトを交換できます。これにより、システム全体の負荷を削減し、ローカルネットワーク内の既存のオブジェクトの検出率を高めることができます。また、キャッシュから兄弟キャッシュまたは親キャッシュにオブジェクト要求を転送できるように、キャッシュ階層を設定することも可能です。これにより、ローカルネットワーク内の他のキャッシュから、またはソースから直接、オブジェクトを取得できるようになります。

ネットワークトラフィック全体が増大することは望ましくないため、キャッシュ階層に適切なトポロジを選択することがきわめて重要です。大規模ネットワークの場合は、サブネットワークごとにプロキシサーバを設定して親プロキシに接続し、親プロキシはISPのプロキシキャッシュに接続すると有効です。

この通信はすべて、UDPプロトコルの最上位で実行されるICP (Internet cache protocol)により処理されます。キャッシュ間のデータ転送は、TCPベースのHTTP (hyper text transmission protocol)により処理されます。

どのサーバからオブジェクトを取得するのが最も適切であるかを検出するために、あるキャッシュからすべての兄弟プロキシにICPリクエストが送信されます。各兄弟プロキシは、オブジェクトが検出された場合はHITコード、検出されなかった場合はMISSを使用し、ICPレスポンスを介してリクエストに応答します。複数のHITレスポンスが検出された場合、プロキシサーバは、最も短時間で応答したキャッシュまたは最も近接するキャッシュなどのファクタに従ってダウンロード元のサーバを決定します。リクエストを満たすレスポンスが受信されなければ、リクエストは親キャッシュに送信されます。

ヒント

ネットワーク上の様々なキャッシュ内でオブジェクトの重複を回避するために、CARP (Cache Array Routing Protocol)やHTCP (Hypertext Cache Protocol)など、他のICPプロトコルが使用されます。ネットワーク上で維持されるオブジェクトが多くなるほど、必要なオブジェクトを検出できる可能性が高くなります。

32.1.3 インターネットオブジェクトのキャッシュ

ネットワーク上で使用可能なオブジェクトがすべてスタティックであるとは限りません。動的に生成されるCGIページ、アクセス件数カウンタ、暗号化されたSSLコンテンツドキュメントが多数存在します。この種のオブジェクトは、アクセスされるたびに変化するためキャッシュされません。

その他のオブジェクトについても、キャッシュにどのくらいの期間残しておくかという問題があります。これを決定するために、オブジェクトが取り得るさまざまな状態を定義し、キャッシュ内のすべてのオブジェクトに1つの状

態を割り当てます。Webサーバとプロキシサーバは、これらのオブジェクトに「Last modified」や「Expires」などのヘッダおよび対応する日付を追加することで、オブジェクトの状態を検出します。その他、オブジェクトをキャッシュしないように指定するヘッダも使用されます。

ハードディスクの空き容量不足が原因で、通常、キャッシュ内のオブジェクトはLRU (Least Recently Used)などのアルゴリズムを使用して置換されます。これは、基本的には、長期間要求されていないオブジェクトがプロキシにより消去されることを意味します。

32.2 システム要件

最も重要なのは、システムにかかる最大ネットワーク負荷を判断することです。ピーク時の負荷は1日の平均負荷の4倍を超えることもあるため、負荷のピークに注意する必要があります。疑わしい場合は、システム要件を多めに見積もることをお勧めします。これは、Squidの動作状態が処理能力の限界に近づくと、サービス品質が著しく低下する可能性があるためです。次の各項では、システム要件を重要度に従って説明します。

32.2.1 ハードディスク

速度はキャッシュ処理に重要な役割を果たすため、この要件には特に注意する必要があります。ハードディスクの場合、このパラメータはランダムシーク*時間*と呼ばれ、ミリ秒単位で計測されます。Squidがハードディスクとの間で読み書きするデータブロックは比較的少数である傾向があるため、データのスループットよりもハードディスクのシーク時間の方が重要です。プロキシに使用する場合は、回転速度の高い(つまり読取り/書込みヘッドが必要な位置に迅速に移動する)ハードディスクを選択するのが適切です。システムを高速化するには、同時に多数のディスクを使用する方法や、ストライピングRAIDアレイを使用する方法があります。

32.2.2 ディスクキャッシュのサイズ

キャッシュ容量が小さいと、簡単にいっぱいになってしまい、要求頻度の低いオブジェクトが新規オブジェクトで置換されるため、HIT (要求された既存のオブジェクトの検出)の可能性は低くなります。逆に、キャッシュに1GBが

使用可能で、ユーザが1日に10MB分しかアクセスしなければ、キャッシュがいっぱいになるまでに100日以上かかることになります。

必要なキャッシュサイズを判断する場合に最も簡単なのは、接続の最大転送速度を考慮することです。1MBit/sの接続の場合、最大転送速度は125KB/sになります。このトラフィックがすべてキャッシュに入ると、1時間で合計450MBとなり、このトラフィックがすべて8時間の営業時間帯にのみ発生すると仮定すれば、1日に3.6GBに達します。通常、接続が上限まで使用されることはないため、キャッシュで処理される合計データ量は約2GBと想定できます。このため、Squidで1日にブラウズされたデータをキャッシュに保持する例では、2GBのディスク容量が必要となります。

32.2.3 RAM

Squidに必要なメモリ容量(RAM)は、キャッシュ内のオブジェクト数に比例します。また、Squidでは、キャッシュオブジェクト参照と要求頻度の高いオブジェクトの検索を高速化するために、これらのデータがメインメモリに格納されます。ランダムアクセスメモリの方が、ハードディスクよりも高速です。

その他、Squidでは、処理された全IPアドレスの表、正確なドメインネームキャッシュ、最もアクセス頻度の高いオブジェクト、アクセス制御リスト、バッファなどのデータもメモリに保持する必要があります。

ディスクにスワップする必要があるとシステムパフォーマンスが大幅に低下するため、Squidプロセス用に十分なメモリを用意する必要があります。キャッシュメモリの管理には、cachemgr.cgiツールを使用できます。このツールの詳細については、32.6項 「cachemgr.cgi」 (553 ページ)を参照してください。

32.2.4 CPU

Squidは、CPU集約型のプログラムではありません。プロセッサの負荷が増大するのは、キャッシュの内容がロードまたはチェックされる間のみです。マルチプロセッサマシンを使用しても、システムパフォーマンスは向上しません。効率を高めるには、高速ディスクまたは増設メモリを購入することをお薦めします。

32.3 Squidの起動

まだインストールしていない場合は、squidパッケージをインストールします。squidはデフォルトのSUSE Linux Enterprise Serverインストールスコープに含まれていません。

Squidは SUSE® Linux Enterprise Serverで事前に設定されているため、インストール直後に起動できます。スムーズに起動するように、インターネットおよび少なくとも1つのネームサーバにアクセスできるようにネットワークを設定してください。ダイナミックDNS設定でダイヤルアップ接続を使用すると、問題が発生する可能性があります。このような場合は、少なくともネームサーバを明確に入力してください。というのは、/etc/resolv.conf内でDNSサーバが検出されないとSquidが起動しないためです。

32.3.1 Squidの起動コマンドと停止コマンド

Squidを起動するには、root権限でコマンドラインに「rcsquid start」と入力します。初期起動時には、最初に /var/cache/squid内でキャッシュのディレクトリ構造を定義する必要があります。この操作は、/etc/init.d/squid起動スクリプトにより自動的に実行され、完了までに数秒ないし数分かかります。右側に緑で完了と表示されたら、Squidは正常にロードされています。ローカルシステム上でSquidの機能をテストするには、ブラウザでプロキシとして「localhost」、ポートとして「3128」を入力します。

ユーザ全員にSquidおよびインターネットへのアクセスを許可するには、設定ファイル/etc/squid/squid.conf内のエントリをhttp_access deny allからhttp_access allow allに変更します。ただし、その場合は、この操作によりSquidが完全に誰でもアクセス可能になることに注意してください。したがって、プロキシへのアクセスを制御するACLを定義します。この詳細については、32.4.2項 「アクセス制御オプション」 (548 ページ)ファイルを参照してください。

設定ファイル/etc/squid/squid.confを変更した後、Squidで変更後の設定ファイルを再ロードする必要があります。それには、rcsquid reloadを使用します。または、「rcsquid restart」と入力してSquidを完全に再起動します。

プロキシが稼動しているかどうかを確認するには、rcsquidstatusコマンドを使用します。Squidをシャットダウンするには、rcsquidstopコマンドを使用します。Squidは、クライアントへの接続が切断されてデータがディスクに書き込まれるまで最大30秒(/etc/squid/squid.confのshutdown_lifetimeオプション）待機するため、終了までに少し時間がかかることがあります。

警告: Squidの終了

killまたはkillallを使ってSquidを終了すると、キャッシュが破損してしまう可能性があります。Squidを再起動できるようにするには、破損したキャッシュを完全に削除する必要があります。

Squidが正常に起動しても短時間で停止する場合は、ネームサーバエントリに誤りがないかどうかと、/etc/resolv.confファイルが欠落していないかどうかを確認してください。起動エラーの原因は、Squidにより/var/log/squid/cache.logファイルに記録されます。システムのブート時にSquidを自動的にロードする必要がある場合は、YaSTランレベルエディタを使用してSquidを必要なランレベルで有効にしてください。詳細については、9.2.3項 「YaSTを使用したSystem Services (Runlevel)の設定」 (122 ページ)を参照してください。

Squidをアンインストールしても、キャッシュ階層やログファイルは削除されません。これらを削除するには、/var/cache/squidディレクトリを手動で削除します。

32.3.2 ローカルDNSサーバ

サーバで独自ドメインを管理しない場合も、ローカルDNSサーバをセットアップすると有効です。ローカルDNSサーバは単にキャッシュ専用ネームサーバとして機能し、特に設定しなくてもルートネームサーバを介してDNSリクエストを解決できます(24.4項 「BINDネームサーバの起動」 (387 ページ)を参照)。ローカルDNSサーバを有効にする方法は、インターネット接続の設定時にダイナミックDNSを選択したかどうかによって異なります。

ダイナミックDNS
: 通常、ダイナミックDNSを使用すると、インターネット接続の確立時にプロバイダによってDNSサーバが設定され、ローカルの/etc/resolv.conf

ファイルが自動的に調整されます。この動作は/etc/sysconfig/network/configファイルのNETCONFIG_DNS_POLICY sysconfig変数で制御されます。YaST sysconfigエディタで、NETCONFIG_DNS_POLICYを""に設定します(9.3.1項 「YaSTのsysconfigエディターを使ってシステム設定を変更する」 (124ページ)を参照してください)。次に、/etc/resolv.confファイルに、ローカルのDNSサーバとして「localhost」、そのIPアドレスとして「127.0.0.1」を入力します。このようにすれば、Squidは常に、起動時にローカルのネームサーバを検出できます。

プロバイダのネームサーバにアクセスするには、/etc/named.conf設定ファイル内のforwardersにサーバ名とそのIPアドレスを入力します。ダイナミックDNSを使用すると、sysconfig変数のNETCONFIG_DNS_POLICYを「auto」に設定することによって、この動作を接続の確立時に自動的に実行することができます。

スタティックDNS
: スタティックDNSを使用する場合は、接続の確立時にいずれの自動DNS調整も行われないため、sysconfig変数を変更する必要はありません。ただし、/etc/resolv.confファイルにローカルのDNSサーバを入力する必要があります。また、プロバイダのスタティックなネームサーバにアクセスするには、/etc/named.confファイルに、サーバ名forwardersとそのIPアドレスを手動で入力する必要があります。

ヒント: DNSとファイアウォール

ただし、ファイアウォールを実行している場合は、DNSリクエストがファイアウォールを通過できることを確認してください。

32.4 etc/squid/squid.conf設定ファイル

Squidのプロキシサーバ設定は、すべて/etc/squid/squid.confファイル内で行います。Squidを初めて起動する場合、このファイル内で設定を変更する必要はありませんが、外部クライアントは最初はアクセスを拒否されます。プロキシはlocalhostに使用できます。デフォルトポートは3128です。プリインストール済みの/etc/squid/squid.conf設定ファイルには、オプ

ションの詳細と多数の例が用意されています。ほぼすべてのエントリは(コメント行を示す) #記号で始まり、関連する指定が行末にあります。示されている値は、ほぼ常にデフォルト値に関係しているため、パラメータを実際に変更せずにコメント記号を削除しても、ほとんどの場合に影響はありません。サンプルはそのまま残し、変更したパラメータと共にオプションを次の行に挿入することをお勧めします。この方法では、簡単にデフォルト値に戻し、変更と比較することができます。

ヒント: 更新後の設定ファイルの変更について

Squidを旧バージョンから更新した場合は、新規の`/etc/squid/squid.conf`を編集し、旧バージョンのファイルで行った変更のみを適用することをお勧めします。旧バージョンの`squid.conf`ファイルを使用すると、オプションが変更されたり新たな変更が加えられているために、設定が機能しなくなる危険性があります。

32.4.1 一般設定オプション(選択)

http_port 3128
: これは、Squidがクライアントリクエストをリスンするポートです。デフォルトポートは`3128`ですが、`8080`も一般的です。必要な場合は、複数のポート番号を空白で区切って指定します。

cache_peer *`hostnametypeproxy-porticp-port`*
: ここでは、たとえばISPのプロキシを使用する場合に、親プロキシを入力します。*`hostname`*には、使用するプロキシの名前またはIPアドレスを入力し、*`type`*には親プロキシを入力します。*`proxy-port`*には、ブラウザで使用する親の演算子でも指定されているポート番号(通常は`8080`)を入力します。icp-portは、7に設定するか、親の`ICP`ポートが不明で、その使用がプロバイダに無関係な場合は0に設定します。また、ICPプロトコルの使用を禁止するため、ポート番号に続けて`default`および`no-query`を指定することもできます。このように指定すると、Squidはプロバイダのプロキシに関する限り通常のブラウザのように動作します。

cache_mem 8 MB
: このエントリは、Squidで頻繁に求められる応答に対して使用できるメモリ容量を定義します。デフォルトは`8MB`です。これは、Squidのメモリ使用量を指定せず、メモリ使用量を超えても構いません。

cache_dir ufs /var/cache/squid/ 100 16 256

*cache_dir*エントリは、すべてのオブジェクトが格納されるディスク上のディレクトリを定義します。末尾の数値は、使用される最大ディスク領域(単位MB)と第1レベルと第2レベルのディレクトリ数を示します。`ufs`パラメータは残しておく必要があります。デフォルトでは、`/var/cache/squid`ディレクトリに100MBのディスク領域を使用して16個のサブディレクトリが作成され、各サブディレクトリにそれぞれ256個以上のサブディレクトリが含まれます。使用するディスク領域を指定するときには、予備のディスク領域を十分に残しておきます。ここでは、使用可能ディスク領域の50～80%が最も有効です。ディレクトリが多すぎるとパフォーマンスが低下する可能性があるため、ディレクトリに関する最後の2つの数値を増やす場合は注意してください。複数のディスクでキャッシュを共有する場合は、複数の*cache_dir*行を入力します。

cache_access_log /var/log/squid/access.log , cache_log /var/log/squid/cache.log , cache_store_log /var/log/squid/store.log

これらの3つのエントリは、Squidによるすべてのアクションの記録先のパスを指定します。通常、ここでは何も変更しません。Squidの使用負荷が大きい場合は、キャッシュとログファイルを複数のディスクに分散すると有効な場合があります。

emulate_httpd_log off

このエントリを*on*に設定すると、読込み可能なログファイルが生成されます。ただし、一部の評価プログラムではこの形式のログファイルを解釈できません。

client_netmask 255.255.255.255

このエントリを使用して、ログファイルでクライアントのIPアドレスをマスクします。ここで「`255.255.255.0`」と入力すると、IPアドレスの最終桁はゼロに設定されます。このようにして、クライアントのプライバシーを保護できます。

ftp_user Squid@

このエントリでは、Squidで匿名FTPログインに使用する必要のあるパスワードを設定します。一部のFTPサーバには電子メールアドレスの妥当性が確認されるため、ここでは有効な電子メールアドレスを指定できます。

cache_mgr webmaster

Squidが予期せずにクラッシュした場合のメッセージ送信先となる電子メールアドレスを指定します。デフォルトは*webmaster*です。

logfile_rotate 0

`squid -k rotate`を実行すると、Squidは保護されたログファイルを循環利用することができます。このプロセス中にファイルに番号が割り当てられ、指定した値に達すると最も古いファイルが上書きされます。SUSE Linux Enterprise Serverではログファイルのアーカイブと削除が設定ファイル`/etc/logrotate/squid`内で検出された自動実行ジョブにより実行されるため、デフォルト値は`0`です。

append_domain <domain>

append_domainには、*未指定の場合に自動的に追加されるドメインを指定します*。通常、ブラウザに「*www*」と入力して独自Webサーバにアクセスできるように、このエントリには独自ドメインを入力します。

forwarded_for on

このエントリを*off*に設定すると、SquidではHTTPリクエストからクライアントのIPアドレスとシステム名が削除されます。設定しない場合は、次のような行がヘッダに追加されます。

```
X-Forwarded-For: 192.168.0.1
```

negative_ttl 5 minutes; negative_dns_ttl 5 minutes

通常、これらの1を変更する必要はありません。ただし、ダイヤルアップ接続を使用する場合は、インターネットが一時的にアクセス不能になる場合があります。Squidは、失敗したリクエストを記録してから新規リクエストの発行を拒絶しますが、インターネット接続は再確立されています。このような場合は、*minutes*を*seconds*に変更します。次にブラウザの*更新*をクリックすると、数秒後にダイヤルアッププロセスが再開されます。

never_direct allow *acl_name*

Squidがインターネットからリクエストを直接取り込むのを防ぐには、上記のコマンドを使用して他のプロキシに強制的に接続します。このプロキシは、あらかじめ*cache_peer*に入力しておく必要があります。*acl_name*として`all`を指定すると、すべてのリクエストは「*親*」に直接転送されます。たとえば、プロキシの使用を奨励しているプロバイダや、ファイアウォールによるインターネットへのダイレクトアクセスを拒否しているプロバイダを使用している場合は、この設定が必要な場合があります。

32.4.2 アクセス制御オプション

Squidには、プロキシへのアクセスを制御する詳細システムが用意されています。ACLを実装することで、このシステムを簡単かつ包括的に設定できます。そのためには、順次処理されるルールを持ったリストが必要です。ACLは定義しなければ使用できません。*all*や*localhost*などのデフォルトACLがいくつか用意されています。ただし、ACLを定義しただけで、実際に適用されるわけではありません。実際に適用するには、*http_access*ルールも共に定義する必要があります。

acl <acl_name> <type> <data>

ACLの定義には、3つ以上の指定が必要です。名前<*acl_name*>は任意に選択できます。<type>は、/etc/squid/squid.conf*ファイル*のACCESS CONTROLSセクションにある多数のオプションから選択できます。<*data*>の指定は個々のACLタイプに応じて異なり、ホスト名、IPアドレスまたはURLを使用するなど、ファイルから読み込むこともできます。次に単純な例を示します。

```
acl mysurfers srcdomain .my-domain.com
acl teachers src 192.168.1.0/255.255.255.0
acl students src 192.168.7.0-192.168.9.0/255.255.255.0
acl lunch time MTWHF 12:00-15:00
```

http_access allow <acl_name>

*http_access*では、プロキシの使用を許可されるユーザと、インターネット上でどのユーザが何にアクセスできるかを定義します。この場合、ACLを設定する必要があります。*localhost*および*all*の定義はすでに前述しており、この2つのACLでは*deny*または*allow*を介してアクセスを拒否または許可できます。多数の*http_access*エントリを含むリストを作成できます。各エントリは上から下へと処理され、発生順に従って個々のURLへのアクセスが許可または拒否されます。最後のエントリは、常に*http_access deny all*にする必要があります。次の例では、*localhost*はすべてに自由にアクセスできますが、他のホストはいずれもアクセスを完全に拒否されます。

```
http_access allow localhost
http_access deny all
```

また、このルールの使用を示す次の例では、グループteachersは常にイン^ーネットへのアクセス権を持ちます。グループstudentsは月曜日から金曜日のランチタイム中にのみアクセス権を取得します。

```
http_access deny localhost
http_access allow teachers
http_access allow students lunch time
http_access deny all
```

*http_access*エントリを含むリストは、読みやすいように/etc/squid/squid.confファイルの指定の位置にのみ入力してください。つまり、次の2つの間に入力します。

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

および最後の

```
http_access deny all
```

redirect_program /usr/bin/squidGuard
: このオプションでは、squidGuardなど、望ましくないURLをブロックできるリダイレクタを指定します。プロキシ認証と適切なACLを利用すれば、さまざまなユーザグループ個別にインターネットアクセスを制御することができます。squidGuardを使用する場合は、個別にインストール、設定する必要があります。

auth_param basic program /usr/sbin/pam_auth
: ユーザのプロキシ認証が必要な場合は、pam_authなどの対応するプログラムを設定します。ユーザがpam_authに初めてアクセスすると、ログインウィンドウが表示され、ユーザ名とパスワードを入力することになります。また、有効なログインを持つクライアント以外はインターネットを使用できないように、ACLも必要です。

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

*proxy_auth*の後の*REQUIRED*は、許可されるユーザ名のリストまたはそのリストへのパスで置き換えることができます。

ident_lookup_access allow <acl_name>
: ここでは、ACLで定義されたクライアントすべてについてidentリクエストを実行させ、各ユーザの識別情報を検索させます。*<acl_name>*に*all*を適用すると、すべてのクライアントに対して有効になります。また、すべて

のクライアントでidentデーモンを実行する必要があります。Linuxの場合、そのためにはpidentdパッケージをインストールします。Microsoft Windowsの場合は、インターネットからダウンロードできるフリーソフトウェアが提供されています。identが正常に検索されたクライアントのみが許可されるように、対応するACLをここで定義します。

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

この場合も、*REQUIRED*を許可されるユーザ名のリストで置き換えることができます。*ident*を使用すると、その検索がリクエストごとに繰り返されるため、アクセス速度が少し低下する場合があります。

32.5 透過型プロキシの設定

一般的なプロキシサーバの作業では、Webブラウザがプロキシサーバの特定のポートに要求を送信し、プロキシが要求に応じて必要なオブジェクトを提供します。ネットワークで操作する場合には、次のような状況が発生することがあります。

- セキュリティ上の理由から、すべてのクライアントがインターネットでのナビゲーションにはプロキシを使用することを推奨される場合。
- すべてのクライアントが、認識するかどうかに関係なくプロキシを使用する必要がある場合。
- ネットワーク上でプロキシが移動しても、既存のクライアントは古い設定を保持する必要がある場合。

いずれの場合も、透過型プロキシを使用できます。原則はきわめて簡単で、プロキシはWebブラウザのリクエストを捕捉して応答するため、Webブラウザは要求したページを出所を認識せずに受信します。透過型プロキシと呼ばれるのは、このプロセス全体が透過的に実行されるためです。

32.5.1 /etc/squid/squid.conf内の設定オプション

squidを透過的なプロキシとして動作させるには、メインの設定ファイル/etc/squid/squid.conf内でhttp_portタグのtransparentオプションを使用します。squidの再起動後に必要なことは、httpポートをhttp_portで指定されたポートにリダイレクトするようファイアウォールを再設定することだけです。次のsquid設定ラインでは、これはポート3128になっています。

```
http_port 3128 transparent
```

32.5.2 SuSEfirewall2を使用したファイアウォール設定

ファイアウォールを介して受信するリクエストをすべて、Squidポートへのポート転送ルールに従ってリダイレクトします。そのためには、項「Configuring the Firewall with YaST」 (第15章 *Masquerading and Firewalls*, ↑*Security Guide (セキュリティガイド)*)で説明されているように、同梱のツールsusefirewall;lを使用します。このツールの設定ファイルは/etc/sysconfig/SuSEfirewall2にあります。この設定ファイルは、適切なエントリで構成されています。透過型プロキシを設定するには、次に示すようにいくつかのファイアウォールオプションを設定する必要があります。

- インターネットを指すデバイス:FW_DEV_EXT="eth1"
- インターネットを指すデバイス:FW_DEV_INT="eth0"

インターネットなど、信頼されない(外部)ネットワークからアクセスが許可される、ファイアウォール上のポートとサービスを定義します(/etc/servicesを参照)。この例では、外部に対してWebサービスのみが提供されます。

```
FW_SERVICES_EXT_TCP="www"
```

安全な(内部)ネットワークからのアクセスが許可される、ファイアウォール上のポートとサービス(TCPサービスとUDPサービスの両方)を定義します(/etc/servicesを参照)。

```
FW_SERVICES_INT_TCP="domain www 3128"
FW_SERVICES_INT_UDP="domain"
```

この例では、WebサービスとSquid(デフォルトポートは3128)へのアクセスが許可されます。 domain「サービスはDNS (ドメインネームサービス)を意味します。」このサービスは一般に使用されます。一般に公開しない場合は、単に上記のエントリから削除して次のオプションをnoに設定します。

```
FW_SERVICE_DNS="yes"
```

最も重要なのは15番目のオプションです。

例 32.1 *ファイアウォールの設定:オプション15*

```
# 15.)
# Which accesses to services should be redirected to a local port on
# the firewall machine?
#
# This option can be used to force all internal users to surf via
# your squid proxy, or transparently redirect incoming webtraffic to
# a secure webserver.
#
# Format:
# list of <source network>[,<destination network>,<protocol>[,dport[:lport]]
# Where protocol is either tcp or udp. dport is the original
# destination port and lport the port on the local machine to
# redirect the traffic to
#
# An exclamation mark in front of source or destination network
# means everything EXCEPT the specified network
#
# Example: "10.0.0.0/8,0/0,tcp,80,3128 0/0,172.20.1.1,tcp,80,8080"
```

上記のコメントは、次の構文を示しています。最初に、プロキシファイアウォールにアクセスする内部ネットワークのIPアドレスとネットマスクを入力します。次に、これらのクライアントからのリクエストの送信先となるIPアドレスとネットマスクを入力します。Webブラウザの場合は、ネットワーク0/0を指定します。これは、「あらゆる場所」を意味するワイルドカードです。」その後、これらのリクエストの送信先となるオリジナルポートを入力し、最後に全リクエストのリダイレクト先となるポートを入力します。SquidはHTTP以外のプロトコルをサポートしているため、要求は他のポートからFTP (ポート21)、HTTPSまたはSSL (ポート443)などのプロキシにリダイレクトされます。この例では、Webサービス(ポート80)がプロキシポート(ポート3128)にリダイレクトされます。他にも追加するネットワークやサービスがある場合は、対応するエントリに空白1個で区切って指定する必要があります。

```
FW_REDIRECT="192.168.0.0/16,0/0,tcp,80,3128"
```

ファイアウォールとそれを使用した新規設定を開始するには、/etc/sysconfig/SuSEfirewall2ファイル内のエントリを変更します。エントリSTART_FWを"yes"に設定する必要があります。

32.3項 「Squidの起動」 (542 ページ)のように、Squidを起動します。すべてが正常に機能していることを確認するには、/var/log/squid/access.logのSquidログを確認します。 すべてのポートが正常に設定されていることを確認するには、ネットワーク外部の任意のコンピュータから、マシンのポートスキャンを実行します。Webサービス(ポート80)のみがオープンしている必要があります。nmapコマンドを使用してポートを検索する場合の構文は、nmap -O IP_addressです。

32.6 cachemgr.cgi

キャッシュマネージャ(cachemgr.cgi)は、実行中のSquidプロセスによるメモリ使用状況に関する統計を表示するCGIユーティリティです。また、キャッシュを管理し、サーバのロギングなしで統計を表示できる便利な手段でもあります。

32.6.1 設定

最初に、システムでWebサーバを稼働させる必要があります。で説明しているように、Apacheを設定します。第30章*Apache HTTP*サーバ(483 ページ)Apacheがすでに稼働しているかどうかを確認するには、rootとして「rcapachestatus」コマンドを入力します。次のようなメッセージが表示される場合は、マシンでApacheが実行されています。

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

Apacheはそのマシンで実行されています。実行していない場合は、「rcapachestart」を入力して、SUSE Linux Enterprise Serverのデフォルト設定でApacheを起動します。最後に、cachemgr.cgiファイルをApacheの

ディレクトリcgi-binにコピーします。32ビットの場合は次のようになります。

```
cp /usr/lib/squid/cachemgr.cgi /srv/www/cgi-bin/
```

64ビット環境では、cachemgr.cgiファイルは/usr/lib64/squid/の下に位置しており、これをApacheディレクトリにコピーするコマンドは次のとおりです。

```
cp /usr/lib64/squid/cachemgr.cgi /srv/www/cgi-bin/
```

32.6.2 /etc/squid/squid.conf内のキャッシュマネージャACL

キャッシュマネージャの場合は、オリジナルファイル内で次のようなデフォルト設定が必要です。最初に、2つのACLを定義し、http_accessオプションがこれらのACLを使用して、CGIスクリプトからSquidへのアクセスを付与するようにします。キャッシュマネージャはcache_objectプロトコルを用いてSquidと通信するため、最初のACLが最も重要です。

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

次の規則によって、ApacheにSquidへのアクセス権が付与されます。

```
http_access allow manager localhost
http_access deny manager
```

これらの規則は、WebサーバとSquidが同じマシンで実行されている場合を想定しています。キャッシュマネージャとSquidとの通信が他のコンピュータ上のWebサーバで開始される場合は、例32.2「アクセスルール」 (554 ページ)に示すACLを追加します。

例 32.2　アクセスルール

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # webserver IP
```

次に、例32.3「アクセスルール」 (555 ページ)に規則を追加して、Webサーバからのアクセスを許可します。

例 32.3　アクセスルール

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

キャッシュのリモートクローズやキャッシュ詳細情報の表示など、より多数のオプションにアクセスする場合は、マネージャのパスワードを設定します。そのためには、マネージャ用のパスワードと表示するオプションのリストを指定してエントリcachemgr_passwdを設定します。このリストは、/etc/squid/squid.confにエントリのコメントの一部として表示されます。

設定ファイルを変更するたびにSquidを再起動してください。それには、rcsquid reloadコマンドを使用します。

32.6.3 統計情報の表示

対応するWebサイトのhttp://webserver.example.org/cgi-bin/cachemgr.cgiに移動します。［*続行*］をクリックして様々な統計情報をブラウズします。

32.7 squidGuard

このセクションでは、squidGuardの詳細な設定については説明しません。ごく基本的な設定のみを紹介し、squidGuardの使用法についていくつか助言するに留めます。詳細な設定については、squidGuardのWebサイトhttp://www.squidguard.orgを参照してください。

squidGuardは、Squid用の無償(GPL)で柔軟で高速なフィルタ、リダイレクタおよびアクセスコントローラプラグインです。squidGuardを利用すれば、Squidキャッシュ上にある異なるユーザグループに対して、異なる制限を持つ複数のアクセスルールを定義することができます。squidGuardは、Squidの標準リダイレクタインタフェースを使用しています。squidGuardの機能を以下に示します。

- 一部のユーザによるWebアクセスを、許可されているか既知のWebサーバまたはURLのリストに限定します。

- リストまたはブラックリストに含まれたWebサーバまたはURLへの、一部のユーザによるアクセスをブロックします。
- 正規表現または語のリストと一致するURLへの、一部のユーザによるアクセスをブロックします。
- ブロックしたURLを「インテリジェント」CGIベースの情報ページにリダイレクトします。
- 未登録ユーザを登録フォームにリダイレクトします。
- バナーを空のGIFにリダイレクトします。
- 時刻、曜日、日付などに基づいて異なるアクセスルールを使用します。
- ユーザグループごとに異なるルールを使用します。

squidGuardとSquidは、以下の用途には使用できません。

- ドキュメント内のテキストの編集、フィルタ処理または検閲。
- JavaScriptやVBscriptなど、HTML埋込みスクリプト言語の編集、フィルタ処理または検閲。

squidGuardを使用するにははじめに、インストールします。最小限の設定ファイルとして`/etc/squidguard.conf`を設定します。に設定例が用意されています。`http://www.squidguard.org/Doc/examples.html`最小限の設定で正常に動作したら、より複雑な設定を試してみてください。

次に、クライアントがブラックリストに含まれるWebサイトを要求した場合にSquidをリダイレクトするために、ダミーの「アクセス拒否」ページまたは複雑度の異なるCGIページを作成します。Apacheを使用することをお薦めします。

ここで、squidGuardを使用するようにSquidを設定します。/etc/squid.confファイル内の次のエントリを使用してください。

```
redirect_program /usr/bin/squidGuard
```

他の`redirect_children`と呼ばれるオプションには、コンピュータ上で動作するリダイレクト(この場合はsquidGuard)プロセス数を設定します。「」プ

ロセスをより多く設定すると、RMMもそれだけ多く必要になります。最初は少ない数(4など)を試してみください。

```
redirect_children 4
```

最後に、rcsquidreloadを実行し、Squidに新規設定をロードさせます。ここで、ブラウザで設定をテストします。

32.8 Calamarisを使用したキャッシュレポート生成

Calamarisは、ASCIIまたはHTML形式でキャッシュアクティビティレポートを生成するためのPerlスクリプトです。このスクリプトはネイティブのSquidアクセスログファイルを処理します。Calamarisのホームページは`http://Calamaris.Cord.de/`にあります。このツールはSUSE Linux Enterprise Serverデフォルトインストールスコープには含まれていません。これを使用するには、calamarisパッケージをインストールしてください。

rootとしてログインし、「`cat access.log | calamaris options > reportfile`」と入力します。複数のログファイルをパイプする場合は、各ログファイルを古いものから時系列順に指定する必要があります。このプログラムには、次のようなオプションがあります。

ヒント: シェルとファイルの順序

access.log.1、access.log.2などのような類似ファイルが複数ある場合、 デフォルトのシェルbashはこれらのファイルを番号以外の順序でソートして、access.log.を一覧表示します。*.この問題を解決するには、次の構文を使用できます。access.log.{1..42}。これによって1〜42の数字拡張子の付いたファイルのリストが生成されます。

-a
: 使用可能な全レポートを出力

-w
: HTMLレポートとして出力

-l
　レポートヘッダにメッセージまたはロゴを挿入

各種オプションの詳細については、「mancalamaris」と入力してプログラムのマニュアルページで参照できます。

典型的な例を次に示します。

```
cat access.log.{10..1} access.log | calamaris -a -w \
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

このコマンドでは、レポートがWebサーバのディレクトリに生成されます。レポートを表示するにはApacheが必要です。

32.9 詳細情報

にあるSquidのホームページにアクセスしてください。http://www.squid-cache.org/ここにはS「quid User Guide」が置かれており、Squidに関する広範囲なFAQ集もあります。

透過型プロキシの使用方法に関する簡潔な情報は、/usr/share/doc/howto/en/txt/TransparentProxy.gzにhowtoenhとして含まれています。また、squid-users@squid-cache.orgで、Squidに関するメーリングリストに登録できます。このアーカイブはhttp://www.squid-cache.org/mail-archive/squid-users/にあります。

SFCBを使用したWebベースの企業管理

33

33.1 概要および基本概念

SUSE® Linux Enterprise Server (SLES)は、異種コンピューティングシステムおよび環境を統合管理するためのオープンスタンダードベースのツールのコレクションを提供しています。弊社の企業ソリューションでは、Distributed Management Task Forceが提案する標準を実装しています。ここでは、基本コンポーネントについて説明します。

Distributed Management Task Force, Inc (DMTF)は、企業およびインターネットの環境に対する管理標準の開発を推進する業界団体です。DMTFは、管理の標準とイニシアチブを統合し、管理ソリューションを、より高い統合性とコスト効果を持つ、より相互運用可能なものにすることを目的としています。DMTF標準は、制御および通信のための共通システム管理コンポーネントを提供します。こうしたソリューションは、プラットフォームや技術に依存しません。*Web*ベースの*企業管理*および*共通情報モデル*は重要な技術の1つです。

Webベースの企業管理(WBEM)は、管理およびインターネット標準技術群です。WBEMは、企業のコンピューティング環境の管理を統合するために開発されました。Webテクノロジを使用した統一管理ツールコレクションを作成する機能を業界に提供するものです。WBEMは、次の標準で構成されます。

- データモデル: CIM(Common Information Model)標準
- 符号化規格: CIM-XML符号化規格

- 伝送メカニズム: CIM operations over HTTP

共通情報モデルは、システム管理について記述した概念的な情報モデルです。特別な実装は必要なく、管理システム、ネットワーク、サービス、およびアプリケーション間で管理情報を交換できます。CIMには、2つのパート(CIM仕様とCIMスキーマ)があります。

- *CIM仕様*は、言語、ネーミング、およびメタスキーマを記述します。メタスキーマは、モデルの公式な定義です。メタスキーマは、モデルの内容、使用方法、および意味の説明に使う用語を定義します。メタスキーマの要素は、*クラス*、*プロパティ*、および*メソッド*です。また、メタスキーマは、*指示*と*関連付け*を*クラス*のタイプとして、*参照*を*プロパティ*としてサポートします。

- *CIM*スキーマは、実際のモデルを記述します。このスキーマは、管理対象環境について利用可能な情報を編成できる汎用の概念的なフレームを提供する、プロパティと関連を持つ一連の名前が付けられたクラスです。

Common Information Model Object Manager (CIMOM)は、CIM標準に基づいてオブジェクトを管理するアプリケーションです(CIM Object Manager)。CIMOMは、CIMOMプロバイダと、管理者がシステムを管理するCIMクライアントの間の通信を管理します。

*CIMOMプロバイダ*は、クライアントアプリケーションから要求された特定のタスクをCIMOM内で実行するソフトウェアです。各プロバイダは、CIMOMのスキーマの1つまたは複数の機能や役割を果たします。これらのプロバイダは、ハードウェアを直接操作します。

*SBLIM (Standards Based Linux Instrumentation for Manageability)*は、Webベースの企業管理(WBEM)をサポートするために設計されたツールのコレクションです。SUSE® Linux Enterprise Serverは、*コンパクトなフットプリントのCIMブローカ*と呼ばれるSBLIMプロジェクトのオープンソースCIMOM(またはCIMサーバ)を使用します。

*コンパクトなフットプリントのCIMブローカ*は、リソースに制限のある環境または埋め込み環境での使用を対象としたCIMサーバです。このサーバは、モジュール性と軽量性を同時に備えた設計になっています。このサーバはオープンスタンダードをベースとし、CMPIプロバイダ、CIM-XMLエンコーディング、および*管理オブジェクトフォーマット(MOF)*をサポートします。これは高度に設定可能なサーバであり、プロバイダがクラッシュしても動作は安定しています。また、HTTP、HTTPS、Unixドメインソケット、サービスロ

ケーションプロトコル(SLP)、Javaデータベース接続(JDBC)など、さまざまなトランスポートプロトコルがサポートされるために、簡単にアクセスできます。

33.2 SFCBの設定

コンパクトなフットプリントCIMブローカ(SFCB)環境を設定するには、SUSE Linux Enterprise Serverのインストール時にYaSTの［*Web*ベースの企業管理］パターンが選択されていることを確認します。また、すでに実行中のサーバにインストールするコンポーネントとしてこれを選択します。次のパッケージがシステムにインストールされていることを確認します。

cim-schema、CIM (Common Information Model)スキーマ
: 共通情報モデル(CIM)が含まれます。CIMは、ネットワーク/企業環境内の総合的な管理情報を記述するモデルです。CIMは仕様とスキーマで構成されます。仕様は、他の管理モデルとの統合に関する詳細を定義しています。スキーマは、実際のモデルを記述しています。

cmpi-bindings-pywbem
: CMPIタイプのCIMプロバイダをPythonで記述および実行するためのアダプタが含まれます。

cmpi-pywbem-base
: 基本システムのCIMプロバイダが含まれます。

cmpi-pywbem-power-management
: DSP1027に基づく電源管理プロバイダが含まれます。

python-pywbem
: 管理対象オブジェクトをクエリおよび更新するために、WBEMプロトコルを使用してCIM操作呼び出しを行うためのPythonモジュールが含まれます。

cmpi-provider-register、CIMOM中立プロバイダ登録ユーティリィティ
: システム上に存在するすべてのCIMOMをCMPIプロバイダパッケージに登録できるユーティリィティが含まれます。

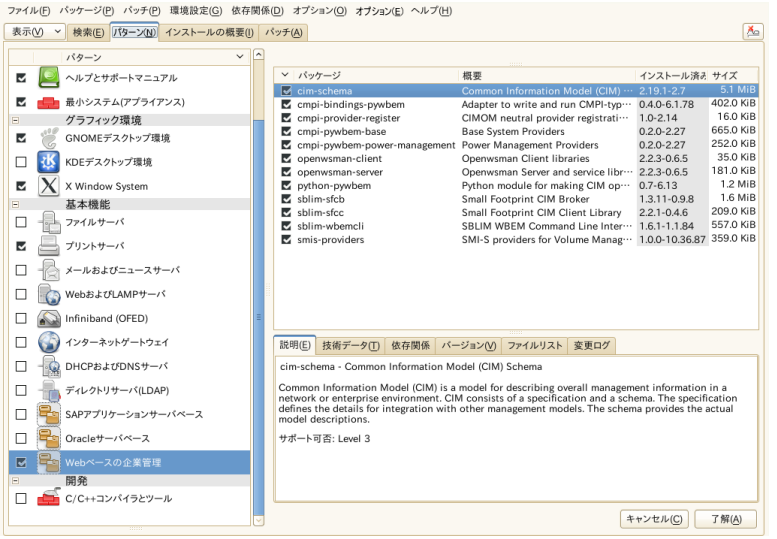
sblim-sfcb、コンパクトなフットプリントのCIMブローカ
: コンパクトなフットプリントのCIMブローカが含まれます。これは、CIM Operations over HTTPプロトコルに準拠するCIMサーバです。堅牢でリソース消費が抑制されているために、埋め込み環境およびリソースが制約された環境に特に適しています。SFCBでは、Common Manageability Programming Interface (CMPI)に対して記述されたプロバイダがサポートされます。

sblim-sfcc
: コンパクトなフットプリントのCIMクライアントライブラリのランタイムライブラリが含まれます。

sblim-wbemcli
: WBEMコマンドラインインタフェースが含まれます。これは、特に基本的なシステム管理タスクに適したスタンドアロンコマンドラインWBEMクライアントです。

smis-providers
: Linuxファイルシステム上のボリュームおよびスナップショットを計測するためのプロバイダが含まれます。これらのプロバイダはそれぞれ、SNIAのSMI-Sボリューム管理プロファイルおよびコピーサービスプロファイルに基づきます。

図 33.1　Webベースの企業管理パターンのパッケージ選択



33.2.1 追加プロバイダのインストール

SUSE® Linux Enterprise Serverソフトウェアリポジトリには、Webベースの企業管理インストールパターンにない追加CIMプロバイダが含まれます。YaSTソフトウェアインストールモジュールでパターンsblim-cmpi-を検索することにより、プロバイダのリストやインストールの状態を簡単に参照できます。これらのプロバイダは、dhcp、NFS、カーネルパラメータ設定など、システム管理のさまざまなタスクに対応します。SFCBとともに使用するプロバイダをインストールしておくと役立ちます。

図 33.2　追加CIMプロバイダのパッケージ選択

33.2.2 SFCBの起動、終了、およびステータスの確認

CIMサーバのsfcbdデーモンは、Webベースの企業管理ソフトウェアとともにインストールされ、システム起動時にデフォルトで開始されます。次の表で、sfcbdの起動、停止、および確認ステータスを説明します。

表 33.1　sfcbdの管理用コマンド

タスク	Linuxコマンド
Start sfcbd	コマンドラインでrootとして「rcsfcb start」と入力します。
sfcbdを停止します。	コマンドラインでrootとして「rcsfcb stop」と入力します。
sfcbdのステータスをチェックします。	コマンドラインでrootとして「rcsfcb status」と入力します。

33.2.3 セキュアアクセスの確保

SFCBのデフォルトのセットアップは、比較的安全(セキュア)です。ただし、SFCBコンポーネントに対するアクセスが組織で必要とされる安全性を満たしていることを確認します。

33.2.3.1 証明書

安全にSSL (Secure Socket Layers)通信を行うには、証明書が必要になります。SFCBがインストールされている場合、自己署名付き証明書が生成されています。

/etc/sfcb/sfcb.cfgのsslCertificateFilePath:*path_filename*設定を変更することで、デフォルトの証明書のパスを商用証明書または自己署名付きの証明書のパスに置き換えることができます。ファイルは、PEMフォーマットであることが必要です。

デフォルトで生成されたサーバ証明書は、次の場所に置かれています。

```
/etc/sfcb/server.pem
```

注記: SSL証明書のパス

デフォルトで生成される証明書ファイルservercert.pemおよびserverkey.pemは、/etc/ssl/servercertsディレクトリに保存されています。ファイル/etc/sfcb/client.pem、/etc/sfcb/file.pem、および/etc/sfcb/server.pemは、これらのファイルへのシンボリックリンクです。

新しい証明書を生成する場合は、rootとしてコマンドラインに次のコマンドを入力します。

```
tux@mercury:~> sh /usr/share/sfcb/genSslCert.sh
Generating SSL certificates in .
Generating a 2048 bit RSA private key
.....................................................................+++
.+++
writing new private key to '/var/tmp/sfcb.0Bjt69/key.pem'
-----
```

デフォルトでは、このスクリプトにより現在の作業ディレクトリに証明書client.pem、file.pem、およびserver.pemが生成されます。スクリプトにより/etc/sfcbディレクトリに証明書を生成する場合は、コマンドにこのディレクトリを追加する必要があります。これらのファイルがすでに存在する場合、警告メッセージが表示されます。古い証明書は上書きされません。

```
tux@mercury:~> sh /usr/share/sfcb/genSslCert.sh /etc/sfcb
Generating SSL certificates in .
WARNING: server.pem SSL Certificate file already exists.
         old file will be kept intact.
WARNING: client.pem SSL Certificate trust store already exists.
         old file will be kept intact.
```

ファイルシステムから古い証明書を削除し、このコマンドを再実行する必要があります。

SFCBで証明書を使用する方法を変更する場合は、33.2.3.3項 「認証」 (566 ページ)を参照してください。

33.2.3.2 ポート

デフォルトでは、SFCBはセキュアなポート5989を使用するすべての通信を受け入れるように設定されます。ここでは、通信ポートのセットアップと推奨される設定について説明します。

ポート5989(セキュア)
: SFCB通信がHTTPSサービスを介して使用するセキュアなポート。デフォルトの設定です。この設定で、CIMOMとクライアントアプリケーション間のすべての通信は、サーバとワークステーション間でインターネットを通じて送信されるときに暗号化されます。ユーザは、SFCBサーバにアクセスするためにクライアントアプリケーションで認証を受ける必要があります。この設定を記録しておくことをお勧めします。ルータやファイアウォールがクライアントアプリケーションとモニタリングされるノードとの間に存在する場合に、SFCB CIMOMが必要なアプリケーションと通信できるようにするには、このポートを開いておく必要があります。

ポート5988(非セキュア)
: SFCB通信がHTTPSサービスを介して使用する非セキュアなポート。デフォルトでは、この設定は無効にされています。この設定では、CIMOMとクライアントアプリケーション間のすべての通信は、サーバとワークステーション間でインターネットを通じて送信されるときに、誰でも認証なしで開き、レビューできます。この設定は、CIMOMの問題をデバッグするときのみに使用することをお勧めします。問題が解決されたら、すぐにセキュアでないポートオプションを無効にしてください。SFCB CIMOMがセキュアでないアクセスを要求する必要なアプリケーションと通信できるようにするには、クライアントアプリケーションとモニタリングされるノードとの間に存在するルータやファイアウォールでこのポートを開いておく必要があります。

デフォルトのポートの割り当てを変更する場合は、33.2.3.2項 「ポート」 (565 ページ)を参照してください。

33.2.3.3 認証

SFCBでは、HTTP基本認証、およびクライアント証明書に基づく認証がサポートされます(HTTP over SSL接続)。基本HTTP認証は、SFCB環境設定ファイル(デフォルトでは`/etc/sfcb/sfcb.cfg`)で、`doBasicAuth=`*`true`*を指定することにより有効になります。SFCBのSUSE® Linux Enterprise Serverインストールでは、プラグ可能認証モジュール(PAM)アプローチがサポートされます。したがって、ローカルルートユーザは、ローカルルートユーザの資格情報によりSFCB CIMOMに対して認証を行うことができます。

`sslClientCertificate`設定プロパティが*`accept`*または*`require`*に設定されている場合、SFCB HTTPアダプタは、HTTP over SSL (HTTPS)で接続した

時にクライアントに証明書を要求します。*require*が指定された場合、(*sslClientTrustStore*を介して指定されたクライアント信頼ストアに従って)クライアントは有効な証明書を提供する必要がありますクライアントが証明書を提供しない場合、接続はCIMサーバにより拒否されます。

sslClientCertificate=*accept*という設定は、明確でないことがあります。基本認証およびクライアント証明書認証が両方許可されている場合に、この設定は非常に役立ちます。クライアントが有効な証明書を提供できれば、HTTPS接続が確立され、基本認証手順は実行されません。この機能で証明書を検証できない場合、HTTP基本認証が代わりに実行されます。

33.3 SFCB CIMOM設定

SFCBは、CIMサーバの軽量な実装ですが、高度に設定可能です。複数のオプションによりその動作を制御できます。基本的に、SFCBサーバは次の3つの方法で制御できます。

- 適切な環境変数を設定する
- コマンドラインオプションを使用する
- 環境設定ファイルを変更する

33.3.1 環境変数

いくつかの環境変数は、SFCBの動作に直接影響します。これらの環境変数の変更を有効にするには、rcsfcb restartでSFCBデーモンを再起動する必要があります。

PATH
: sfcbdデーモンおよびユーティリティへのパスを指定します。

LD_LIBRARY_PATH
: sfcbランタイムライブラリへのパスを指定します。また、このパスをシステムワイドの動的ローダ設定ファイル/etc/ld.so.confに追加できます。

SFCB_PAUSE_PROVIDER
: プロバイダ名を指定します。SFCBサーバは、プロバイダが最初にロードされた後に一時停止します。その後、デバッグの目的でプロバイダのプロセスにランタイムデバッガを接続できます。

SFCB_PAUSE_CODEC
: SFCBコーデックの名前を指定します(現在、httpのみサポートしています)。SFCBサーバは、コーデックが最初にロードされた後に一時停止します。その後、プロセスにランタイムデバッガを接続できます。

SFCB_TRACE
: SFCBのデバッグメッセージレベルを指定します。有効な値は、0(デバッグメッセージなし)、または1(重要なデバッグメッセージ)～4(すべてのデバッグメッセージ)です。デフォルトは1です。

SFCB_TRACE_FILE
: 有効な値は、0(デバッグメッセージなし)または1(主要なデバッグメッセージ)～4(すべてのデバッグメッセージ)です。この変数を設定すると、指定のファイルにデバッグメッセージが代わりに書き込まれます。

SBLIM_TRACE
: SBLIMプロバイダのデバッグメッセージレベルを指定します。有効な値は、0(デバッグメッセージなし)、または1(重要なデバッグメッセージ)～4(すべてのデバッグメッセージ)です。

SBLIM_TRACE_FILE
: デフォルトでは、SBLIMプロバイダはトレースメッセージをSTDERRに出力します。この変数を設定すると、指定のファイルにトレースメッセージが代わりに書き込まれます。

33.3.2 コマンドラインオプション

SFCBデーモンsfcbdには、特定のランタイム機能をオン/オフするためのコマンドラインオプションがあります。SFCBデーモンの開始時に、これらのオプションを入力します。

`-c, --config-file=`*`FILE`*
SFCBデーモンの開始時に、デフォルトで`/etc/sfcb/sfcb.cfg`から設定が読み込まれます。このオプションでは、代替の環境設定ファイルを指定できます。

`-d, --daemon`
バックグラウンドで実行するようにsfcbdとその子プロセスを強制します。

`-s, --collect-stats`
ランタイム統計情報の収集をオンにします。現在の作業ディレクトリの`sfcbStat`ファイルに、さまざまなsfcbdランタイム統計情報が書き込まれます。デフォルトでは、統計情報は収集されません。

`-l, --syslog-level=`*`LOGLEVEL`*
syslogの冗長レベルを指定します。*`LOGLEVEL`*は、LOG_INFO、LOG_DEBUG、またはLOG_ERR(デフォルト)のいずれかになります。

`-k, --color-trace=`*ログレベル*
プロセスごとに異なる色でトレース出力を印刷して、デバッグを容易にします。

`-t, --trace-components=`*`NUM`*
*`NUM`*がトレースするコンポーネントを定義するORビットマスク整数である場合に、コンポーネントレベルのトレースメッセージをアクティブにします。`-t ?`を指定した後すべてのコンポーネントおよび関連する整数ビットマスクが表示されます。

```
tux@mercury:~> sfcbd -t ?
---   Traceable Components:     Int        Hex
---         providerMgr:          1 0x0000001
---         providerDrv:          2 0x0000002
---          cimxmlProc:          4 0x0000004
---          httpDaemon:          8 0x0000008
---             upCalls:         16 0x0000010
---            encCalls:         32 0x0000020
---     ProviderInstMgr:         64 0x0000040
---    providerAssocMgr:        128 0x0000080
---           providers:        256 0x0000100
---         indProvider:        512 0x0000200
---    internalProvider:       1024 0x0000400
---          objectImpl:       2048 0x0000800
---               xmlIn:       4096 0x0001000
---              xmlOut:       8192 0x0002000
---             sockets:      16384 0x0004000
```

```
---            memoryMgr:      32768 0x0008000
---              msgQueue:      65536 0x0010000
---           xmlParsing:     131072 0x0020000
---      responseTiming:     262144 0x0040000
---            dbpdaemon:     524288 0x0080000
---                  slp:    1048576 0x0100000
```

sfcbdの内部機能を表示し、メッセージを生成しすぎない有用な値は`-t` *2019*です。

33.3.3 SFCB環境設定ファイル

SFCBは、起動後に環境設定ファイル`/etc/sfcb/sfcb.cfg`からランタイム設定を読み込みます。この動作は、起動時に`-c`オプションを使用して上書きできます。

環境設定ファイルには、オプション : *値*のペアが1行に1つずつ含まれています。このファイルに変更を加える場合は、使用している環境にネイティブな形式でファイルを保存するどのテキストエディタでも使用できます。

オプションがシャープ記号(#)でコメントアウトされている設定では、デフォルト設定が使用されます。

次のオプションリストは、完全でない可能性があります。完全なリストについては、`/etc/sfcb/sfcb.cfg`と`/usr/share/doc/packages/sblim-sfcb/README`を参照してください。

33.3.3.1 httpPort

目的

CIMクライアントからのHTTP(非セキュア)要求を受信するためにsfcbdがリスンするローカルポート値を指定します。デフォルトは`5988`です。

構文

`httpPort:` *`port_number`*

33.3.3.2 enableHttp

目的

SFCBがHTTPクライアント接続を受け入れるかどうかを指定します。デフォルトは`false`です。

構文

`enableHttp:` *`option`*

オプション	説明
true	HTTP接続を有効にします。
false	HTTP接続を無効にします。

33.3.3.3 httpProcs

目的

新しい着信HTTP要求を拒否するまでの同時HTTPクライアント接続の最大数を指定します。デフォルトは8です。

構文

`httpProcs:` *`max_number_of_connections`*

33.3.3.4 httpUserSFCB、httpUser

目的

これらのオプションは、httpサーバを実行するユーザを管理します。`httpUserSFCB`が`true`の場合、httpは、SFCBメインプロセスとして同じユーザが実行します。`false`の場合は、`httpUser`で指定されたユーザ名が使用されます。この設定は、httpとhttpsの両方のサーバに使用されます。

httpUserSFCBをfalseに設定する場合は、httpUserを指定する必要があります。デフォルトは、trueです。

構文

```
httpUserSFCB: true
```

33.3.3.5 httpLocalOnly

目的

HTTP要求をローカルホストだけに制限するかどうか指定します。デフォルトはfalseです。

構文

```
httpLocalOnly: false
```

33.3.3.6 httpsPort

目的

sfcbdがCIMクライアントからのHTTPS要求をリスンするローカルポート値を指定します。デフォルトは5989です。

構文

```
httpsPort: port_number
```

33.3.3.7 enableHttps

目的

SFCBがHTTPSクライアント接続を受け入れるかどうかを指定します。デフォルトはtrueです。

構文

`enableHttps: option`

オプション	説明
true	HTTPS接続を有効にします。
false	HTTPS接続を無効にします。

33.3.3.8 httpsProcs

目的

新しい着信HTTPS要求を拒否するまでの同時HTTPSクライアント接続の最大数を指定します。デフォルトは8です。

構文

`httpsProcs: max_number_of_connections`

33.3.3.9 enableInterOp

目的

SFCBで表示サポートに*interop*名前空間を提供するかどうかを指定します。デフォルトは`true`です。

構文

`enableInterOp: option`

オプション	説明
true	interop名前空間を有効にします。

オプション	説明
false	interop名前空間を無効にします。

33.3.3.10 provProcs

目的

同時プロバイダプロセスの最大数を指定します。この時点以降、新しい着信要求により新しいプロバイダのロードが必要になった場合は、既存のプロバイダのいずれかが最初に自動的にアンロードされます。デフォルトは32です。

構文

`provProcs: max_number_of_procs`

33.3.3.11 doBasicAuth

目的

要求を受け入れる前に、クライアントユーザーIDに基づいて基本認証のオンまたはオフを切り替えます。デフォルト値は`true`で、基本的なクライアント認証が実行されます。

構文

`doBasicAuth: option`

オプション	説明
true	基本認証を有効にします。
false	基本認証を無効にします。

33.3.3.12 basicAuthLib

目的

ローカルライブラリ名を指定します。SFCBサーバは、クライアントユーザIDを認証するためにライブラリをロードします。デフォルトは`sfcBasicPAMAuthentication`です。

構文

`provProcs:` *`max_number_of_procs`*

33.3.3.13 useChunking

目的

このオプションは、HTTP/HTTPSの「チャンク」使用のオンまたはオフを切り替えます。オンに切り替えた場合、サーバは大量の応答データを、バッファして1つの「チャンク」ですべてを返信するのではなく、小さなチャンクでクライアントに返信します。デフォルトは`true`です。

構文

`useChunking:` *`option`*

オプション	説明
true	HTTP/HTTPSデータチャンクを有効にします。
false	HTTP/HTTPSデータチャンクを無効にします。

33.3.3.14 keepaliveTimeout

目的

1つの接続で、2つの要求の間、要求がなされてから接続を閉じるまでSFCB HTTPプロセスが待機する最大時間を秒数で指定します。0に設定すると、HTTP keep-aliveが無効になります。デフォルトは0です。

構文

```
keepaliveTimeout: secs
```

33.3.3.15 keepaliveMaxRequest

目的

1つの接続で連続して受け付ける要求の最大数を指定します。0に設定すると、HTTP keep-aliveが無効になります。デフォルト値は10です。

構文

```
keepaliveMaxRequest: number_of_connections
```

33.3.3.16 registrationDir

目的

プロバイダの登録データ、ステージング領域、および静的リポジトリを含む登録ディレクトリを指定します。デフォルトは/var/lib/sfcb/registrationです。

構文

```
registrationDir: dir
```

33.3.3.17 providerDirs

目的

SFCBがプロバイダライブラリを検索するディレクトリのリストをスペースで区切って指定します。デフォルトは/usr/lib64 /usr/lib64 /usr/lib64/cmpiです。

構文

```
providerDirs: dir
```

33.3.3.18 providerSampleInterval

目的

プロバイダマネージャが待機中のプロバイダをチェックする間隔を秒で指定します。デフォルトは30です。

構文

```
providerSampleInterval: secs
```

33.3.3.19 providerTimeoutInterval

目的

待機中のプロバイダがプロバイダマネージャによりアンロードされるまでの間隔を秒で指定します。デフォルトは60です。

構文

```
providerTimeoutInterval: secs
```

33.3.3.20 providerAutoGroup

目的

プロバイダ登録ファイルで他のグループを指定しておらず、このオプションを*true*に設定されている場合、同じ共有ライブラリのすべてのプロバイダが同じプロセス内で実行されます。

構文

`providerAutoGroup:` *option*

オプション	説明
true	プロバイダのグループを有効にします。
false	プロバイダのグループを無効にします。

33.3.3.21 sslCertificateFilePath

目的

サーバ証明書を含むファイルの名前を指定します。ファイルは、PEM (Privacy Enhanced Mail、RFC 1421、およびRFC 1424)フォーマットであることが必要です。このファイルは、`enableHttps`が`true`に設定されている場合にのみ必要です。デフォルトは`/etc/sfcb/server.pem`です。

構文

`sslCertificateFilePath:` *path*

33.3.3.22 sslKeyFilePath

目的

サーバ証明書の秘密鍵が含まれるファイルの名前を指定します。このファイルはPEMフォーマットであることが必要であり、パスフレーズによって保護できない場合があります。このファイルは、enableHttpsがtrueに設定されている場合にのみ必要です。デフォルトは/etc/sfcb/file.pemです。

構文

sslKeyFilePath: *path*

33.3.3.23 sslClientTrustStore

目的

CAまたはクライアントの自己署名付きの証明書のいずれかを含むファイルの名前を指定します。このファイルはPEMフォーマットであることが必要であり、sslClientCertificateがacceptまたはrequireに設定されている場合にのみ必要になります。デフォルトは/etc/sfcb/client.pemです。

構文

sslClientTrustStore: *path*

33.3.3.24 sslClientCertificate

目的

SFCBがクライアント証明書に基づく認証を処理する方法を指定します。ignoreに設定した場合、クライアントに証明書は要求されません。acceptに設定した場合、クライアントに証明書が要求されますが、クライアントが証明書を提示しなくとも失敗しません。requireに設定した場合、クライアントが証明書を提示しないときは、クライアント接続が拒否されます。デフォルト値はignoreです。

構文

`sslClientCertificate: option`

オプション	説明
ignore	クライアント証明書の要求を無効にします。
承諾	クライアント証明書の要求を無効にします。 証明書が存在しなくとも失敗しません。
必要	有効な証明書を持たないクライアント接続を拒否します。

33.3.3.25 certificateAuthLib

目的

クライアント証明書に基づいてユーザ認証を要求するローカルライブラリの名前を指定します。この設定は、`sslClientCertificate`が`ignore`に設定されていない場合にのみ必要です。デフォルト値は`sfcCertificateAuthentication`です。

構文

`certificateAuthLib: file`

33.3.3.26 traceLevel

目的

SFCBのトレースレベルを指定します。この設定は、環境変数SFCB_TRACE_LEVELを設定することにより上書きできます。デフォルト値は0です。

構文

```
traceLevel: num_level
```

33.3.3.27 traceMask

目的

SFCBのトレースマスクを指定します。この設定は、コマンドラインオプション--trace-componentsで上書きできます。デフォルト値は0です。

構文

```
traceMask: mask
```

33.3.3.28 traceFile

目的

SFCBのトレースファイルを指定します。この設定は、環境変数SFCB_TRACE_LEVELを設定することにより上書きできます。デフォルト値は、stderr(標準エラー出力)です。

構文

```
traceFile: output
```

33.4 高度なSFCBタスク

この章では、SFCBの使用方法に関連するより高度なトピックを取り上げます。このトピックを理解するには、Linuxファイルシステムの基礎知識とLinuxコマンドラインの使用経験が必要です。この章には、次のタスクが含まれています。

- CMPIプロバイダのインストール
- SFCBのテスト
- `wbemcli` CIMクライアントの使用

33.4.1 CMPIプロバイダのインストール

CMPIプロバイダをインストールするには、`providerDirs`設定オプションにより指定されたいずれかのディレクトリに共有ライブラリがコピーされていることを確認する必要があります。33.3.3.17項 「providerDirs」 (577 ページ)を参照してください。プロバイダはまた、`sfcbstage`コマンドおよび`sfcbrepos`コマンドを使用して適切に登録されていることが必要です。

プロバイダパッケージは通常、SFCB用に準備されます。したがって、インストールにより適切な登録が行われます。大半のSBLIMプロバイダは、SFCB用に準備されています。

33.4.1.1 クラスリポジトリ

*クラスリポジトリ*は、SFCBがCIMクラスに関する情報を保存する場所です。通常これは、名前空間コンポーネントから成るディレクトリツリーから構成されます。一般的なCIM名前空間は`root/cimv2`または`root/interop`であり、ファイルシステム上のクラスリポジトリディレクトリパスにそれぞれ変換されます。

```
/var/lib/sfcb/registration/repository/root/cimv2
```

および

```
/var/lib/sfcb/registration/repository/root/interop
```

各名前空間ディレクトリには、ファイルclassSchemasが含まれます。ファイルには、その名前空間の下に登録されたすべてのCIMクラスのコンパイル済みバイナリ表現があります。また、CIMスーパークラスに関して必要な情報も含まれます。

さらに各名前空間ディレクトリには、名前空間のすべての修飾子を含むファイル修飾子が含まれます。sfcbdの再起動時に、クラスプロバイダはディレクトリ/var/lib/sfcb/registration/repository/およびそのすべてのサブディレクトリをスキャンして、登録済みの名前空間を決定します。次に、classSchemasファイルがデコードされ、各名前空間のクラス階層が構築されます。

33.4.1.2 新しいクラスの追加

SFCBは、ライブCIMクラス操作を生成できません。クラスをオフラインで追加、変更、または削除し、rcsfcb restartでSFCBサービスを再起動して変更内容を登録します。

SFCBは、プロバイダクラスおよび登録情報を保存するために、*ステージング領域*と呼ばれる場所を使用します。SUSE® Linux Enterprise Serverシステムでは、これは/var/lib/sfcb/stage/の下にあるディレクトリ構造です。

新しいプロバイダを追加するには、次の操作が必要です。

- プロバイダクラス定義ファイルを、ステージング領域ディレクトリの/mofsサブディレクトリ(/var/lib/sfcb/stage/mofs)にコピーします。
- クラス(複数可)の名前およびプロバイダタイプを含む登録ファイル、および実行可能なライブラリファイルの名前を/regsサブディレクトリにコピーします。

ステージングディレクトリには、2つのデフォルト「mof」(クラス定義)ファイル(indication.mofとinterop.mof)があります。ルートステージングディレクトリ/var/lib/sfcb/stage/mofsの下にあるMOFのファイルは、sfcbreposコマンドの実行後に各名前空間にコピーされます。interop.mofは、*interop*名前空間に対してのみコンパイルされます。

ディレクトリレイアウトは、次の例のようになります。

```
tux@mercury:~> ls /var/lib/sfcb/stage
default.reg  mofs  regs

tux@mercury:~> ls /var/lib/sfcb/stage/mofs
indication.mof  root

tux@mercury:~> ls /var/lib/sfcb/stage/mofs/root
cimv2  interop  suse  virt

tux@mercury:~> ls -1 /var/lib/sfcb/stage/mofs/root/cimv2 | less
Linux_ABIParameter.mof
Linux_BaseIndication.mof
Linux_Base.mof
Linux_DHCPElementConformsToProfile.mof
Linux_DHCPEntity.mof
[..]
OMC_StorageSettingWithHints.mof
OMC_StorageVolumeDevice.mof
OMC_StorageVolume.mof
OMC_StorageVolumeStorageSynchronized.mof
OMC_SystemStorageCapabilities.mof

tux@mercury:~> ls -1 /var/lib/sfcb/stage/mofs/root/interop
ComputerSystem.mof
ElementConformsToProfile.mof
HostSystem.mof
interop.mof
Linux_DHCPElementConformsToProfile.mof
[..]
OMC_SMIElementSoftwareIdentity.mof
OMC_SMISubProfileRequiresProfile.mof
OMC_SMIVolumeManagementSoftware.mof
ReferencedProfile.mof
RegisteredProfile.mof

tux@mercury:~> ls -1 /var/lib/sfcb/stage/regs
AllocationCapabilities.reg
Linux_ABIParameter.reg
Linux_BaseIndication.reg
Linux_DHCPGlobal.reg
Linux_DHCPRegisteredProfile.reg
[..]
OMC_Base.sfcb.reg
OMC_CopyServices.sfcb.reg
OMC_PowerManagement.sfcb.reg
OMC_Server.sfcb.reg
RegisteredProfile.reg

tux@mercury:~>  cat /var/lib/sfcb/stage/regs/Linux_DHCPRegisteredProfile.reg
[Linux_DHCPRegisteredProfile]
   provider: Linux_DHCPRegisteredProfileProvider
   location: cmpiLinux_DHCPRegisteredProfile
   type: instance
   namespace: root/interop
#
```

```
[Linux_DHCPElementConformsToProfile]
   provider: Linux_DHCPElementConformsToProfileProvider
   location: cmpiLinux_DHCPElementConformsToProfile
   type: instance association
   namespace: root/cimv2
#
[Linux_DHCPElementConformsToProfile]
   provider: Linux_DHCPElementConformsToProfileProvider
   location: cmpiLinux_DHCPElementConformsToProfile
   type: instance association
   namespace: root/interop
```

SFCBは、各プロバイダについてカスタムプロバイダ登録ファイルを使用します。

注記: SBLIMプロバイダ登録ファイル

SBLIM Webサイト上のすべてのSBLIMプロバイダには、すでに、SFCB用の.regファイルを生成するための登録ファイルが含まれています。

SFCB登録ファイルのフォーマットは次のとおりです。

```
[<class-name>]
   provider: <provide-name>
   location: <library-name>
   type: [instance] [association] [method] [indication]
   group: <group-name>
   unload: never
   namespace: <namespace-for-class> ...
```

ここで:

`<class-name>`
: CIMクラス名(必須)

`<provider-name>`
: CMPIプロバイダ名(必須)

`<location-name>`
: プロバイダライブラリ名(必須)

`type`
: プロバイダのタイプ(必須)。これは、`instance`、`association`、`method`、または`indication`の任意の組み合わせです。

<group-name>
複数のプロバイダをグループ化し、単一のプロセスの下で実行することで、さらにランタイムリソースを最小化できます。同じ<group-name>の下で登録されたすべてのプロバイダは、同じプロセスの下で実行します。デフォルトでは、各プロバイダは別個のプロセスとして実行します。

unload
プロバイダのアンロードポリシーを指定します。現在サポートされている唯一のオプションはneverであり、これはプロバイダが待機時間について監視されず、決してアンロードされないことを指定します。デフォルトでは、待機時間が環境設定ファイルで指定された値を超えたときに各プロバイダがアンロードされます。

namespace（ネームスペース）
このプロバイダが実行できる名前空間のリストです。この設定は必須ですが、大半のプロバイダで*root/cimv2*になります。

すべてのクラス定義およびプロバイダ登録ファイルがステージング領域に保存されたら、コマンドsfcbrepos -fでSFCBクラスリポジトリを再構築する必要があります。

このようにしてクラスの追加、変更、または削除を行うことができます。クラスリポジトリを再構築した後、コマンドrcsfcb restartでSFCBを再起動します。

またSFCBパッケージには、プロバイダクラスmofファイルおよび登録ファイルを、ステージング領域の適切な場所にコピーするユーティリィティが含まれています。

```
sfcbstage -r [provider.reg] [class1.mof] [class2.mof] ...
```

このコマンドを実行した後、さらにクラスリポジトリを再構築し、SFCBサービスを再起動する必要があります。

33.4.2 SFCBのテスト

SFCBパッケージには、2つのテストスクリプト(wbemcatとxmltest)が含まれます。

wbemcatは、未加工のCIM-XMLデータをHTTPプロトコル経由で、ポート5988上でリスンする指定されたSFCBホスト(デフォルトではlocalhost)に送信します。次に、返された結果を表示します。次のファイルには、標準的なEnumerateClasses要求のCIM-XML表現が含まれます。

```
<?xml version="1.0" encoding="utf-8"?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
  <MESSAGE ID="4711" PROTOCOLVERSION="1.0">
    <SIMPLEREQ>
      <IMETHODCALL NAME="EnumerateClasses">
        <LOCALNAMESPACEPATH>
          <NAMESPACE NAME="root"/>
          <NAMESPACE NAME="cimv2"/>
        </LOCALNAMESPACEPATH>
        <IPARAMVALUE NAME="ClassName">
          <CLASSNAME NAME=""/>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="DeepInheritance">
          <VALUE>TRUE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="LocalOnly">
          <VALUE>FALSE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="IncludeQualifiers">
          <VALUE>FALSE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="IncludeClassOrigin">
          <VALUE>TRUE</VALUE>
        </IPARAMVALUE>
      </IMETHODCALL>
     </CIM></SIMPLEREQ>
  </MESSAGE>
</CIM>
```

SFCB CIMOMにこの要求を送信すると、登録済みのプロバイダが存在するすべてのサポートクラスのリストが返されます。ファイルをcim_xml_test.xmlとして保存した場合を考えます。

```
tux@mercury:~> wbemcat cim_xml_test.xml | less
HTTP/1.1 200 OK
Content-Type: application/xml; charset="utf-8"
Content-Length: 337565
Cache-Control: no-cache
CIMOperation: MethodResponse

<?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0">
<SIMPLERSP>
<IMETHODRESPONSE NAME="EnumerateClasses">
[..]
```

```
<CLASS NAME="Linux_DHCPParamsForEntity" SUPERCLASS="CIM_Component">
<PROPERTY.REFERENCE NAME="GroupComponent" REFERENCECLASS="Linux_DHCPEntity">
</PROPERTY.REFERENCE>
<PROPERTY.REFERENCE NAME="PartComponent" REFERENCECLASS="Linux_DHCPParams">
</PROPERTY.REFERENCE>
</CLASS>
</IRETURNVALUE>
</IMETHODRESPONSE>
</SIMPLERSP>
</MESSAGE>
</CIM>
```

表示されるクラスは、システムにインストールされているプロバイダに応じて異なります。

2番目のスクリプトxmltestもまた、未加工のCIM-XMLテストファイルをSFCB CIMOMに送信するために使用されます。次に、以前に保存された「良好な」結果ファイルに対して、返された結果を比較します。対応する「良好」なファイルがまだ存在しない場合は、後から使用できるように作成されます。

```
tux@mercury:~> xmltest cim_xml_test.xml
Running test cim_xml_test.xml ... OK
 Saving response as cim_xml_test.OK
tux@mercury:~> xmltest cim_xml_test.xml
Running test cim_xml_test.xml ... Passed
```

33.4.3 コマンドラインCIMクライアント: wbemcli

SBLIMプロジェクトには、wbemcatおよびxmltestに加えて、より高度なコマンドラインCIMクライアントであるwbemcliが含まれます。このクライアントは、SFCBサーバにCIM要求を送信し、返された結果を表示するために使用されます。これはCIMOMライブラリに依存せず、WBEMに準拠するすべての実装で使用できます。

たとえば、SFCBに登録済みのSBLIMプロバイダにより実装されたすべてのクラスを表示する必要がある場合は、「EnumerateClasses」(ec)要求をSFCBに送信します。

```
tux@mercury:~> wbemcli -dx ec http://localhost/root/cimv2
To server: <?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0"><SIMPLEREQ><IMETHODCALL \
    NAME="EnumerateClasses"><LOCALNAMESPACEPATH><NAMESPACE NAME="root"> \
    </NAMESPACE><NAMESPACE NAME="cimv2"></NAMESPACE> \
```

```
    </LOCALNAMESPACEPATH>
<IPARAMVALUE NAME="DeepInheritance"><VALUE>TRUE</VALUE> \
    </IPARAMVALUE>
<IPARAMVALUE NAME="LocalOnly"><VALUE>FALSE</VALUE></IPARAMVALUE>
<IPARAMVALUE NAME="IncludeQualifiers"><VALUE>FALSE</VALUE> \
    </IPARAMVALUE>
<IPARAMVALUE NAME="IncludeClassOrigin"><VALUE>TRUE</VALUE> \
    </IPARAMVALUE>
</IMETHODCALL></SIMPLEREQ>
</MESSAGE></CIM>
From server: Content-Type: application/xml; charset="utf-8"
From server: Content-Length: 337565
From server: Cache-Control: no-cache
From server: CIMOperation: MethodResponse
From server: <?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0">
<SIMPLERSP>
<IMETHODRESPONSE NAME="EnumerateClasses">
<IRETURNVALUE>
<CLASS NAME="CIM_ResourcePool" SUPERCLASS="CIM_LogicalElement">
<PROPERTY NAME="Generation" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="ElementName" TYPE="string">
</PROPERTY>
<PROPERTY NAME="Description" TYPE="string">
</PROPERTY>
<PROPERTY NAME="Caption" TYPE="string">
</PROPERTY>
<PROPERTY NAME="InstallDate" TYPE="datetime">
</PROPERTY>
[..]
<CLASS NAME="Linux_ReiserFileSystem" SUPERCLASS="CIM_UnixLocalFileSystem">
<PROPERTY NAME="FSReservedCapacity" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="TotalInodes" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="FreeInodes" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="ResizeIncrement" TYPE="uint64">
<VALUE>0</VALUE>
</PROPERTY>
<PROPERTY NAME="IsFixedSize" TYPE="uint16">
<VALUE>0</VALUE>
</PROPERTY>
[..]
```

-dxオプションでは、wbemcliでSFCBに送信された実際のXMLも、受信した実際のXMLも表示されます。上記の例では、多数返されるクラスのうちの第1のクラスがCIM_ResourcePool、第2のクラスが

Linux_ReiserFileSystem.です。他の登録済みの全クラスでも、同様のエントリが表示されます。

-dxオプションを省略した場合、wbemcliは返却されたデータのコンパクト表現のみを表示します。

```
tux@mercury:~> wbemcli ec http://localhost/root/cimv2
localhost:5988/root/cimv2:CIM_ResourcePool Generation=,ElementName=, \
    Description=,Caption=,InstallDate=,Name=,OperationalStatus=, \
    StatusDescriptions=,Status=,HealthState=,PrimaryStatus=, \
    DetailedStatus=,OperatingStatus=,CommunicationStatus=,InstanceID=, \
    PoolID=,Primordial=,Capacity=,Reserved=,ResourceType=, \
    OtherResourceType=,ResourceSubType=, \AllocationUnits=
localhost:5988/root/cimv2:Linux_ReiserFileSystem FSReservedCapacity=, \
    TotalInodes=,FreeInodes=,ResizeIncrement=,IsFixedSize=,NumberOfFiles=, \
    OtherPersistenceType=,PersistenceType=,FileSystemType=,ClusterSize=, \
    MaxFileNameLength=,CodeSet=,CasePreserved=,CaseSensitive=, \
    CompressionMethod=,EncryptionMethod=,ReadOnly=,AvailableSpace=, \
    FileSystemSize=,BlockSize=,Root=,Name=,CreationClassName=,CSName=, \
    CSCreationClassName=,Generation=,ElementName=,Description=,Caption=, \
    InstanceID=,InstallDate=,OperationalStatus=,StatusDescriptions=, \
    Status=,HealthState=,PrimaryStatus=,DetailedStatus=,OperatingStatus= \
    ,CommunicationStatus=,EnabledState=,OtherEnabledState=,RequestedState= \
    ,EnabledDefault=,TimeOfLastStateChange=,AvailableRequestedStates=, \
    TransitioningToState=,PercentageSpaceUse=
    [..]
```

33.5 詳細情報

WBEMおよびSFCBの詳細については、次の資料を参照してください。

http://www.dmtf.org
Distributed Management Task Force Webサイト

http://www.dmtf.org/standards/wbem/
Webベースの企業管理(WBEM) Webサイト

http://www.dmtf.org/standards/cim/
共通情報モデル(CIM) Webサイト

http://sblim.wiki.sourceforge.net/
Standards Based Linux Instrumentation (SBLIM) Webサイト

http://sblim.wiki.sourceforge.net/Sfcb
Small Footprint CIM Broker (SFCB) Webサイト

http://sblim.wiki.sourceforge.net/Providers
SBLIMプロバイダパッケージ

パート V. トラブルシューティング

34 ヘルプとドキュメント

SUSE® Linux Enterprise Serverは、さまざまな情報源とドキュメントとともに提供されますが、その多くは、ご使用のインストール済みシステムにすでに統合されています。

`/usr/share/doc`内のドキュメント
: この従来のヘルプディレクトリには、システムのさまざまなドキュメントファイルやリリースノートが格納されます。このディレクトリの`packages`サブディレクトリには、インストール済みパッケージの情報も含まれています。詳細については34.1項 「ドキュメントディレクトリ」 (596 ページ)を参照 てください。

シェルコマンドのマニュアルページと情報ページ
: シェルを使用する場合は、コマンドのオプションを記憶しておく必要はありません。シェルは以前からマニュアルページおよび情報ページによって統合ヘルプを提供しています。詳細については34.2項 「manページ」 (598 ページ)および34.3項 「情報ページ」 (599 ページ)を参照してください。

デスクトップヘルプセンター
: KDEデスクトップ(KDE help center)とGNOMEデスクトップ(Yelp)の両方のヘルプセンターでは、システムの最も重要なドキュメントリソースに検索可能な形式で一元的にアクセスできます。これらのリソースにはインストール済みのアプリケーションのオンラインヘルプ、マニュアルページ、情報ページ、製品に付属しているNovell/SUSEマニュアルが含まれます。

一部のアプリケーション用の別なヘルプパッケージ
YaSTを使って新しくソフトウェアをインストールした場合、通常はそのソフトウェアのドキュメントも自動的にインストールされ、デスクトップのHelp Centerに表示されます。ただし、GIMPなどの一部のアプリケーションは、YaSTとは別個にインストールされる独自のオンラインヘルプパッケージを利用しており、ヘルプセンターには表示されない場合があります。

34.1 ドキュメントディレクトリ

インストールされたLinuxシステム上のドキュメント検索用の従来のディレクトリは、/usr/share/docです。このディレクトリには通常、リリースノート、マニュアルなどに加えて、システムにインストールされたパッケージに関する情報が含まれます。

注記: インストール済みパッケージに依存する内容

Linuxの世界では、ソフトウェアのように、多くのマニュアル、その他の文書がパッケージ形式で用意されています。/usr/share/docs内の情報の種類および内容は、インストールされている(文書)パッケージに応じて異なります。ここに記載されているサブディレクトリが見つからない場合は、対応するパッケージがシステムにインストールされているかどうかを確認し、必要に応じてYaSTに追加してください。

34.1.1 Novell/SUSEマニュアル

これらのガイドブックは、HTMLおよびPDFの各バージョンを複数の言語で提供しています。manualサブディレクトリでは、製品で使用可能な大半のNovell/SUSEマニュアルのHTMLバージョンがあります。製品で使用可能なすべての文書の概要については、マニュアルの序文を参照してください。

複数の言語がインストールされている場合、/usr/share/doc/manualには異なる言語版のマニュアルが含まれる場合があります。Novell/SUSEマニュアルのHTMLバージョンは、両デスクトップのヘルプセンターでも入手可能です。インストールメディアで文書のPDF版およびHTML版の検索場所については、SUSE Linux Enterprise Serverのリリースノートを参照してください。これらの文書は、インストールされたシステムの/usr/share/doc/release

-notes/、またはオンラインの製品固有のWebページ(http://www.suse.com/doc/)で参照できます。

34.1.2 HOWTO(操作方法)

howtoパッケージがシステムにインストールされている場合、/usr/share/docにはhowtoサブディレクトリも含まれます。このサブディレクトリには、Linuxソフトウェアのセットアップおよび操作に関連するさまざまなタスクの追加文書があります。

34.1.3 パッケージのドキュメント

packagesの下で、システムにインストールしたソフトウェアパッケージに含まれているドキュメントを見つけてください。各パッケージについて、サブディレクトリ/usr/share/doc/packages/*packagename*が作成されます。このサブディレクトリには、パッケージのREADMEファイルが含まれます。さらにサンプル、環境設定ファイル、または追加スクリプトが含まれることがあります。次のリストに、/usr/share/doc/packagesの下にある一般的なファイルを示します。これらの項目はいずれも必須ではなく、多くのパッケージがその一部のみを含みます。

AUTHORS
: 主な開発者のリスト。

BUGS
: 既知のバグまたは誤動作。また、Bugzilla Webページへのリンクがあり、そこでバグを検索できる場合があります。

CHANGES , ChangeLog
: バージョン間の変更点の概要です。非常に詳細なものなので、通常は、開発者にとって興味あるものです。

COPYING , LICENSE
: ライセンス情報。

FAQ
: メーリングリストやニュースグループから集められた質問と答えが含まれています。

INSTALL
: システムにこのパッケージをインストールする方法。このファイルに目を通している時点でパッケージがすでにインストールされており、このファイルの内容を無視しても問題はありません。

README, README.*
: ソフトウェアに関する一般的な情報。たとえば、ソフトウェアの目的および使用方法などです。

TODO
: まだ実装されていないものの、今後実装される予定の機能についての説明です。

MANIFEST
: ファイルのリストと、それぞれの簡単な概要です。

NEWS
: このバージョンでの新しい点が記されています。

34.2 manページ

マニュアルページは、どのLinuxシステムにおいても重要な役割を担っています。マニュアルページでは、コマンドと利用可能なオプションおよびパラメータについての使用法が説明されています。マニュアルページは、manの後にコマンド名(たとえば「man ls」)を入力して開くことができます。

マニュアルページは、シェルに直接表示されます。ナビゲートするには、Page ↑およびPage ↓を使用して上下に移動します。<Home>キーと<End>キーを使用すると、それぞれドキュメントの最初と最後に移動できます。 Qキーを押すと、この表示モードが終了します。manコマンド自体の詳細については、man manと入力します。マニュアルページは、表34.1「マニュアルページ—カテゴリと説明」 (599 ページ)(マニュアルページ自身から抽出)に示すように、カテゴリ別にソートされています。

*表 **34.1** マニュアルページ—カテゴリと説明*

数値	説明
1	実行可能プログラムまたはシェルコマンド
2	システムコール(カーネルによって提供される機能)
3	ライブラリコール(プログラムライブラリ内での機能)
4	特別なファイル(通常は/dev内にあります)
5	ファイル形式と命名規則(/etc/fstab)
6	ゲーム
7	その他(マクロパッケージおよび規則)、例： man(7)、groff(7)
8	システム管理コマンド(通常はrootに関するもののみ;)
9	カーネルルーチン(非標準)

各マニュアルページは、*NAME*、*SYNOPSIS*、*DESCRIPTION*、*SEE ALSO*、*LICENSING*および*AUTHOR*といういくつかのパートで構成されています。 コマンドのタイプによっては、他のセクションが追加されている場合があります。

34.3 情報ページ

情報ページは、システム上にあるもう1つの重要な情報ソースです。 通常、情報ページの内容はマニュアルページよりも詳細です。特定のコマンドのinfo

ページを表示するには、infoの後にコマンド名(たとえば「info ls」)を入力します。シェルで直接ビューアを使用してinfoページを参照し、「ノード」と呼ばれるさまざまなセクションを表示できます。と呼ばれるさまざまなセクションを表示できます。Spaceを使用して前に移動し、<—を使用して後ろに移動します。ノード内で、Page ↑およびPage ↓を使用して参照することもできますが、前および後ろのノードにも移動できるのはSpaceおよび<—のみです。Qを押すと、表示モードを終了します。すべてのマニュアルページにinfoページが付属するわけではありません。逆も同様です。

34.4 リソースのオンライン化

オンラインバージョンのNovellマニュアル(/usr/share/docにインストールされます)に加えて、Webで製品固有のマニュアルやドキュメントにアクセスすることもできます。利用可能なすべてのSUSE Linux Enterprise Serverマニュアルの概要については、製品固有のドキュメントに関するWebページ(http://www.novell.com/documentation/)をご覧してください。

製品ごとの追加情報を検索する場合は、次のWebサイトも参照してください。

Novellテクニカルサポートナレッジベース
: Novellテクニカルサポートのナレッジベースは、http://www.novell.com/support/で見つけることができます。このナレッジベースは、SUSE Linux Enterprise Serverの技術的な問題に対するソリューションとして書かれた記事を提供します。

Novellフォーラム
: Novell製品に関して議論できるいくつかのフォーラムがあります。リストについては、http://forums.novell.com/を参照してください。

Cool Solutions
: 記事、ヒント、質疑応答、およびダウンロードできる無料ツールを提供するオンラインコミュニティ(http://www.novell.com/communities/coolsolutions)

KDEマニュアル
: KDEの多数の側面を解説するユーザと管理者向けのマニュアル(http://www.kde.org/documentation/)

GNOMEマニュアル
: GNOMEユーザ、管理者、および開発者向けのマニュアル(http://library.gnome.org/)

Linux Documentation Project
: TLDP(Linux Documentation Project)は、Linux関係のマニュアルを作成するボランティアチームによって運営されています(http://www.tldp.org参照)。これは、おそらく、Linuxに関する最も総合的なドキュメントリソースです。マニュアルのセットには初心者向けのチュートリアルも含まれますが、主にシステム管理者などの経験者向けの内容になっています。TLDPは、HOWTO(操作方法)、FAQ(よくある質問)、ガイド(ハンドブック)を無償で提供しています。TLDPからのドキュメントの一部は、SUSE Linux Enterprise Server上でも利用できます。

汎用の検索エンジンも使用できます。たとえば、CDへの書き込みやLibreOfficeファイルの変換でトラブルがある場合は、検索する語句として`Linux CD-RW help`(Linux CD-RWヘルプ)または`OpenOffice file conversion problem`(OpenOfficeファイルの変換の問題)を使用します。また、Google™にはLinux用の検索エンジンhttp://www.google.com/linuxも用意されています。このエンジンを利用すれば、有益な情報を探し出すことができます。

最も頻繁に起こる問題およびその解決方法

35

この章では、一連の潜在的な問題とその解決法について説明します。ここで状況が正確に記載されていなくても、問題解決のヒントになる類似した状況が見つかる場合があります。

35.1 情報の検索と収集

Linuxでは、非常に詳細なレポートが提供されます。システムの使用中に問題が発生した場合、調べる必要のあるところが何箇所かあります。それらのほとんどは、Linuxシステム一般で標準とされるもので、残りのいくつかはSUSE Linux Enterprise Serverシステムに関連するものです。大半のログファイルはYaSTを使って表示することができます(［*その他*］ > ［*起動ログを表示*］)。

YaSTでは、サポートチームが必要な情報の大半を収集することができます。の利用 ［*その他*］ > ［*サポート*］の順に選択し、問題のカテゴリを選択します。すべての情報が収集されたら、それをサポートリクエストに添付します。

最も頻繁にチェックされるログファイルのリストの後には、一般的な目的に関する説明があります。~を含むパスは、現在のユーザのホームディレクトリを参照します。

表 35.1 ログファイル

ログファイル	説明
~/.xsession-errors	現在実行中のデスクトップアプリケーションからのメッセージです。
/var/log/apparmor/	AppArmorからのログファイル。詳細については、パート「Confining Privileges with AppArmor」(↑*Security Guide (セキュリティガイド)*)を参照してください。
/var/log/audit/audit.log	システムのファイル、ディレクトリ、またはリソースに対するすべてのアクセスを追跡し、システムコールをトレースする監査からのログファイル。
/var/log/boot.msg	ブートプロセス時にレポートされたカーネルから受け取るメッセージ。
/var/log/mail.*	メールシステムから受け取るメッセージです。
/var/log/messages	起動中に、カーネルおよびシステムのログデーモンから継続的に受け取るメッセージです。
/var/log/NetworkManager	NetworkManagerからのログファイルで、ネットワーク接続についての問題を収集します。
/var/log/samba/	Sambaサーバおよびクライアントのログメッセージを含んでいるディレクトリです。

ログファイル	説明
/var/log/SaX.log	SaXディスプレーとKVMシステムから受け取るハードウェアメッセージです。
/var/log/warn	カーネルおよびシステムのログデーモンから受け取る、「警告」レベル以上のすべてのメッセージ。
/var/log/wtmp	現在のコンピュータセッションのユーザのログインレコードを含むバイナリファイルです。lastコマンドを使用して表示させます。
/var/log/Xorg.*.log	Windowシステムから受け取る、起動時および実行時のさまざまなログです。Xの失敗した起動をデバッグするのに役に立ちます。
/var/log/YaST2/	YaSTのアクションとその結果を保管するディレクトリ。
/var/log/zypper.log	zypperのログファイル。

ログファイルとは別に、稼働中のシステムの情報も提供されます。詳細については、「表35.2: /procファイルシステムによるシステム情報」を参照してください。

*表 **35.2** /procファイルシステムによるシステム情報*

ファイル	説明
/proc/cpuinfo	プロセッサのタイプ、製造元、モデル、およびパフォーマンスなどを含む情報を表示します。

ファイル	説明
/proc/dma	どのDMAチャネルが現在使用されているかを表示します。
/proc/interrupts	どの割り込みが使用されているか、各割り込みの使用回数を表示します。
/proc/iomem	I/Oメモリの状態を表示します。
/proc/ioports	その時点でどのI/Oポートが使用されているかを表示します。
/proc/meminfo	メモリステータスを表示します。
/proc/modules	個々のモジュールを表示します。
/proc/mounts	現在マウントされているデバイスを表示します。
/proc/partitions	すべてのハードディスクのパーティション設定を表示します。
/proc/version	現在のLinuxバージョンを表示します。

Linuxカーネルは、/procファイルシステムの場合を除いて、メモリ内ファイルシステムであるsysfsモジュールで情報をエクスポートします。このモジュールは、カーネルオブジェクトとその属性および関係を表します。sysfsの詳細については、第14章 *udevによる動的カーネルデバイス管理*(197ページ)でudevのコンテキストを参照してください。表35.3には、/sysの下にある最も一般的なディレクトリの概要が含まれています。

表 **35.3** */sys*ファイルシステムによるシステム情報

ファイル	説明
`/sys/block`	システム内で検出された各ブロックデバイスのサブディレクトリが含まれています。一般に、これらの大半はディスクタイプのデバイスです。
`/sys/bus`	各物理バスタイプにのサブディレクトリが含まれます。
`/sys/class`	デバイスの機能タイプとしてグループ化されたサブディレクトリが含まれます(graphics、net、printerなど)。
`/sys/device`	グローバルなデバイス階層が含まれます。

Linuxには、システム解析とモニタリング用のさまざまなツールが含まれています。システム診断で使用される最も重要なツールの選択については、第2章 *System Monitoring Utilities* (↑*System Analysis and Tuning Guide (システム分析およびチューニングガイド)*)を参照してください。

次の各シナリオは、問題を説明するヘッダに続いて、推奨される解決方法、より詳細な解決方法への利用可能な参照、および関連する他のシナリオへの相互参照が書かれた、1つまたは2つの段落から構成されています。

35.2 インストールの問題

インストールの問題とは、コンピュータがインストールに失敗した状態のことを指します。インストールが全体において失敗する、またはグラフィカルインストーラが起動できないという可能性があります。ここでは、通常経験するような問題のいくつかに集中して説明し、そのような場合に考えられる解決方法または回避方法を示します。

35.2.1 メディアの確認

SUSE Linux Enterprise Serverインストールメディアの使用時に問題が発生した場合は、［ソフトウェア］>［メディアチェック］の順に選択してインストールメディアの整合性をチェックします。メディアの問題は、自身で書き込むメディアで発生する可能性がより高いです。SUSE Linux Enterprise Serverのメディアをチェックするには、メディアをドライブに挿入し、YaSTの［メディアチェック］画面で［チェック*開始*］をクリックします。これには少し時間がかかります。問題が検出された場合、インストール用にこのメディアを使用しないでください。

図 35.1　メディアの確認

35.2.2 ハードウェア情報

［*ハードウェア*］>［*ハードウェア情報*］を使用して、検出されたハードウェアおよび技術データを表示します。デバイスの詳細については、任意のツリーノードをクリックします。サポートを依頼するときに、ハードウェアに関する情報が必要な場合などに、このモジュールが特に役立ちます。

［*ファイルに保存*］をクリックして、表示されたハードウェア情報をファイルに保存します。希望するディレクトリとファイル名を選択し、［*保存*」］をクリックしてファイルを作成します。

図 35.2　ハードウェア情報の表示

35.2.3 ブート可能なDVDドライブが利用不可

お使いのコンピュータにブート可能なDVD-ROMドライブがない場合、または使用しているドライブがLinuxでサポートされていない場合、内蔵DVD-ROMドライブを使用しないでコンピュータをインストールするオプションがいくつかあります。

フロッピーディスクからのブート
: ブートフロッピーを作成し、DVDの代わりにフロッピーディスクからブートします。

外付けブートデバイスの使用
: BIOSおよびインストールカーネルによりサポートされる場合、外部DVDドライブから起動します。

PXE経由のネットワークブート
: コンピュータにDVDドライブがない場合でも、使用可能なイーサネット接続がある場合は、完全にネットワークベースのインストールを実行します。詳細については、項 「VNC経由のリモートインストール—PXEブートとWake on LAN」 (第14章 *リモートインストール*, ↑*導入ガイド*)と項 「SSH経由のリモートインストール—PXEブートとWake on LAN」 (第14章 *リモートインストール*, ↑*導入ガイド*)を参照してください。

35.2.3.1 フロッピーディスク(SYSLINUX)からのブート

旧式のコンピュータには、ブート可能なDVDドライブはなく、フロッピーディスクドライブしかないものがあります。そのようなシステムにインストールするには、ブートディスクを作成し、それを使ってシステムを起動します。

ブートディスクには、SYSLINUXというローダとプログラムlinuxrcも含まれています。SYSLINUXを使用すると、ブート時にカーネルを選択し、使用するハードウェアに必要なパラメータを指定できます。プログラムlinuxrcは、使用するハードウェア用のカーネルモジュールのローディングをサポートし、その後インストールを開始します。

ブートディスNからブートする際は、ブート処理は、ブートローダー SYSLINUX(パッケージ`syslinux`)によって開始されます。システムが起動すると、SYSLINUXは、以下のステップで構成される、最小限のハードウェア検出検査を実行します。

1. ブートローダは、BIOSがVESA 2.0準拠のフレームバッファサポートを提供しているかどうかを調べ、適宜、カーネルを起動します。

2. モニタデータ(DDC info)が読み込まれます。

3. 1番目のハードディスクの最初のブロック(MBR)が読み込まれ、BIOS IDとLinuxのデバイス名がブートローダの設定時に対応付けられます。ブート

ローダは、BIOSのlba32関数を使用して当該ブロックを読み込み、BIOSがそれらの関数をサポートしているかどうかを判別します。

SYSLINUXの開始時に、Shiftキーを押したままにすると、上記のステップはすべてスキップされます。トラブルシューティングの目的で、

```
verbose 1
```

syslinux.cfgに次の行を挿入した場合、ブートローダは、現在実行中のアクションを表示します。

マシンがフロッピーディスクからブートしない場合は、BIOS内のブートシーケンスを`A,C,CDROM`に変更しなければならないことがあります。

35.2.3.2 外付けブートデバイス

Linuxでは、既存のDVDドライブはほとんどサポートされます。システムにDVDドライブまたはフロッピーディスクが存在しない場合でも、USB、FireWire、またはSCSIを通じて接続する外部DVDドライブを使用してシステムをブートできます。これは、BIOSおよびご利用のハードウェアのインタラクションに大きく依存します。問題が発生した場合、BIOSアップデートにより解決する場合があります。

35.2.4 インストールメディアからのブートに失敗する

コンピュータでインストールメディアが起動しない理由の1つとして、BIOS内のブートシーケンスの設定が誤っている場合があります。BIOSブートシーケンスでは、ブート用の最初のエントリとしてDVDドライブがセットされている必要があります。そうでない場合、コンピュータは他のメディア(通常ハードディスク)からブートを試みます。BIOSのブートシーケンスを変更するための説明は、マザーボードに付属するマニュアルまたは次の段落に記載されています。

BIOSとはコンピュータの非常に基本的な機能を有効にするソフトウェアです。マザーボードを供給するベンダが、独自のハードウェア用のBIOSを供給します。通常、BIOSセットアップは特別な時(マシンのブート時)にだけアクセスされます。この初期化段階の間に、マシンは数多くのハードウェア診断テストを実行します。そのうちの1つとして、メモリカウンタにより示されるメモ

リチェックがあります。メモリカウンタが表示されたとき、通常カウンタの下または画面の下部の辺りに、BIOSセットアップにアクセスするために押すキーについて表示されています。通常は、Del、F1、またはEscのいずれかのキーを押します。BIOSセットアップ画面が表示されるまでこのキーを押します。

手順 35.1　BIOSのブートシーケンスの変更

1 ブートルーチンによって宣言されたように、適切なキーを使用してBIOSを入力します。その後、BIOS画面が表示されるのを待ちます。

2 AWARD BIOSでブートシーケンスを変更するには、［*BIOS FEATURES SETUP*］エントリを探してください。他のメーカでは、［*ADVANCED CMOS SETUP*］といった違う名前が使用されています。エントリが見つかったなら、そのエントリを選択して、Enterキーを押して確定します。

3 開いた画面で、［*BOOT SEQUENCE*］または［*BOOT ORDER*］というサブエントリを探します。ブートシーケンスは、C,AまたはA,Cなどのように記載されています。C,Aの場合、マシンは最初にハードディスク(C)を検索し、次にフロッピーディスクドライブ(A)を検索して、ブート可能なメディアを検出します。ブートシーケンスがA,CDROM,Cになるまで PgUpキーまたはPgDownキーを押して、設定を変更します。

4 Escキーを押してBIOS設定画面を終了します。設定を保存するには、［*SAVE & EXIT SETUP*］を選択し、F10キーを押します。設定が保存されていることを確認するには、Yキーを押します。

手順 35.2　SCSI BIOS (Adaptecホストアダプタ)内でのブートシーケンスの変更

1 Ctrl＋Aを押してセットアップを開きます。

2 ［ディスクユーティリティ］を選択します。これで、接続したハードウェアコンポーネントが表示されるようになります。

ご使用のDVDドライブに割り当てられているSCSI IDの記録をとります。

3 Escキーを押して、メニューを閉じます。

4 ［アダプタセッティングの設定］を開きます。［*追加オプション*］で、［*Boot Device Options(ブートデバイスオプション)*］を選択し、Enterキーを押します。

5 DVDドライブのIDを入力して、再度Enterキーを押します。

6 Escキーを2回押して、SCSI BIOSの起動画面に戻ります。

7 ［*はい*］を押して、この画面を終了しコンピュータを起動します。

最終的なインストールが使用する言語やキーボードレイアウトに関係なく、BIOS設定では、通常以下の図に示されているようなUSキーボードレイアウトが使用されます。

図 35.3　USキーボードレイアウト

35.2.5 ブートできない

ハードウェアのタイプ(主にかなり旧式かごく最近のタイプ)では、インストールが失敗するものもあります。多くの場合、インストールカーネル内でこのタイプのハードウェアのサポートが欠けているか、または、ある種のハードウェアに問題を引き起こすACPIのような、カーネルに含まれている特定の機能が原因の可能性があります。

最初のインストールブート画面から、標準の［*インストール*］モードを使用してインストールするのに失敗した場合、以下のことを試してみてください。

1 DVDがドライブにまだ入った状態であれば、Ctrl＋Alt＋Delを押すか、ハードウェアリセットボタンを使用して、コンピュータを再起動します。

2 ブート画面が表示されたら、F5キーを押すか、キーボードの矢印キーを使用して、［*ACPIなし*］を探し、<Enterキーを押してブートおよびインストールプロセスを開始します。このオプションはACPIの電源管理技術を無効にします。

3 第6章 *YaSTによるインストール*;(↑*導入ガイド*)の中での説明に従って、インストールを進めます。

これが失敗する場合、以上で述べた手順の代わりに［セーフ設定］を選択してインストール処理を続行します。このオプションはACPIおよびDMAサポートを無効化します。このオプションを使うと、ほとんどのハードウェアが起動します。

両方のオプションともに失敗する場合、ブートオプションプロンプトを使用して、ハードウェアタイプをサポートするのに必要な追加のパラメータをインストールカーネルに渡します。ブートオプションとして使用可能なパラメータの詳細については、`/usr/src/linux/Documentation/kernel-parameters.txt`にあるカーネルマニュアルを参照してください。

ヒント: カーネルマニュアルの取得

kernel-sourceパッケージをインストールして、カーネルマニュアルを表示します。

他にさまざまなACPI関連のカーネルパラメータがあります。それらのパラメータは、インストールのために起動する前のブートプロンプトで入力できます。

`acpi=off`
: このパラメータは、コンピュータ上の完全ACPIサブシステムを無効にします。これはコンピュータがACPIをまったく処理できない場合、またはコンピュータのACPIが問題を引き起こしていると考えられる場合に役に立ちます。

`acpi=force`
: 2000年より前の日付が付けられた古いBIOSを持つコンピュータであっても、常にACPIを有効にします。このパラメータは、`acpi=off`に加えて設定された場合、ACPIも有効にします。

`acpi=noirq`
: ACPIはIRQルーティングには使用しません。

`acpi=ht`
: hyper-threadingを有効化するのに十分なACPIのみ実行します。

`acpi=strict`
厳密にはACPI仕様互換ではないプラットフォームに対する耐性が弱くなります。

`pci=noacpi`
新しいACPIシステムのPCI IRQルーティングを無効にします。

`pnpacpi=off`
このオプションは、BIOSセットアップに誤った割り込みまたはポートがある場合のシリアルまたはパラレルの問題向けです。

`notsc`
タイムスタンプカウンタを無効にします。このオプションを使用して、システムのタイミングについての問題に対処できます。これは最近の機能で、コンピュータに特に時間や全面的なハングなどの遅れが見られる場合に、このオプションを試す価値があります。

`nohz=off`
nohz機能を無効にします。マシンがハングした場合、このオプションが役に立ちます。それ以外の場合は、使用しません。

一旦パラメータの正しい組み合わせを決定したら、システムが次回適切に起動することを確実にするために、YaSTは自動的にそれらのパラメータをブートローダーの設定に書き込みます。

カーネルのロード中、またはインストール中に説明できないエラーが発生した場合は、ブートメニューから［メモリテスト］を選択し、メモリを確認します。［メモリテスト］がエラーを返す場合、それは通常はハードウェアのエラーです。

35.2.6 グラフィカルインストーラを起動できない

メディアをドライブに挿入しコンピュータを再起動した後に、インストール画面が表示されますが、［インストール］を選択すると、グラフィカルインストーラは起動しません。

この問題に対処する方法はいくつかあります。

- インストールダイアローグ用に、他の画面解像度を選択してみます。
- インストール用に［テキストモード］を選択します。
- VNCを介して、グラフィカルインストーラを使ってリモートインストールをします。

手順 35.3　インストール時の画面解像度の変更

1 インストールのために起動します。

2 F3キーを押して、インストール用に低解像度を選択するメニューを開きます。

3 ［*インストール*］を選択し、第6章 *YaSTによるインストール; (↑導入ガイド)* の中の説明に従ってインストールを続行します。

手順 35.4　テキストモードのインストール

1 インストールのために起動します。

2 F3キーを押して、［テキストモード］を選択します。

3 ［*インストール*］を選択し、第6章 *YaSTによるインストール; (↑導入ガイド)* の中の説明に従ってインストールを続行します。

手順 35.5　VNCによるインストール

1 インストールのために起動します。

2 ブートオプションプロンプトに以下のテキストを入力します。

```
vnc=1 vncpassword=some_password
```

*some_password*の部分はVNCインストール用に使用するパスワードに置き換えます。

3 ［*インストール*］を選択し、キーを押してインストールを開始します。Enter

グラフィカルインストールルーチンに入るかわりに、システムはテキストモードで実行され、その後停止します。その際、IPアドレスおよびポート番号が含まれるメッセージが表示されますが、これらは、ブラウザインタ

フェースまたはVNCビューアアプリケーションを使用してインストーラにアクセスできるようにするために必要です。

4 ブラウザを使用してインストーラにアクセスする場合、ブラウザを起動して将来SUSE Linux Enterprise Serverが起動するコンピュータ上のインストール手順で与えられたアドレス情報を入力し、<Enterキーを押します。

```
http://ip_address_of_machine:5801
```

ブラウザウィンドウでは、VNCのパスワードを入力するように要求するダイアログが開かれます。パスワードを入力し、第6章 *YaSTによるインストール;* (↑*導入ガイド*)の説明に従ってインストールを続行します。

重要

ＶＮＣ経由のインストールでは、Javaサポートが有効化されていれば、オペレーションシステムやブラウザの種類を問いません。

プロンプトが表示されたら、VNCビューアにIPアドレスとパスワードを入力します。インストールダイアログを表示するウィンドウが開きます。通常のようにインストールを続行します。

35.2.7 最低限のブート画面だけが起動する

メディアをドライブに挿入して、BIOSルーチンは終了しますが、システム上でグラフィカルブート画面が開始しません。その代わりに、最小限のテキストベースのインタフェースが起動されます。これは、グラフィカルブート画面を表示するのに十分なグラフィックメモリを持っていないコンピュータを使用する場合に起こる可能性がります。

テキストのブート画面は最小限にに見えますが、グラフィカルブート画面が提供する機能とほぼ同じものを提供します。

ブートオプション
: グラフィカルインタフェースとは違い、キーボードのカーソルキーを使って異なるブートオプションを選択することはできません。テキストモードのブート画面のブートメニューでは、ブートプロンプトで入力するキーワードが表示されます。これらのキーワードはグラフィカルバージョンで提供されているオプションにマップしています。任意の選択を入力し<Enterキーを押して、ブートプロセスを起動します。

カスタムブートオプション
ブートオプションを選択したあと、ブートプロンプトで適切なキーワードを入力するか、35.2.5項 「ブートできない」 (613 ページ)の中で説明されているカスタムブートオプションを入力します。インストールプロセスを起動するには、<Enterキーを押します。

画面解像度
Fキーを使用して、インストール用の画面解像度を判別します。テキストモードで起動する必要がある場合は、キーを選択します。

35.3 ブートの問題

ブートの問題とは、システムが適切に起動しないような場合を指します(意図したランレベルおよびログイン画面まで起動しない場合)。

35.3.1 GRUBブートローダのロードに失敗する

ハードウェアが問題なく機能している場合、ブートローダが壊れてしまってLinuxがコンピュータ上で起動できない可能性があります。このような場合、ブートローダを再インストールする必要があります。ブートローダを再インストールするには、以下の手順に従います。

1 インストールメディアをドライブに挿入します。

2 コンピュータを再起動します。

3 ブートメニューから［*インストール*］を選択します。

4 言語を選択します。

5 使用許諾契約に同意します。

6 ［*インストールモード*］画面で、［*インストール済みのシステムを修復*］を選択します。

7 YaSTシステム修復モジュールの中で、［エキスパート*設定用ツール*］を選択し、［*新しいブートローダのインストール*］を選択します。

8 元の設定を復元し、ブートローダを再インストールします。

9 YaSTシステム修復を修復し、システムを再起動します。

コンピュータが起動しない理由は他にBIOS関連のものが考えられます。

BIOS設定
: ハードドライブを参照するためのBIOSを確認してください。ハードドライブ自体が現在のBIOS設定に見つからない場合、GRUBが単に開始されない可能性があります

BIOSブートオーダー
: お使いのシステムのブートオーダーがハードディスクを含んでいるか確認します。ハードディスクオプションが有効になっていない場合、システムは適切にインストールされていますが、ハードディスクへのアクセスが要求される際に起動に失敗する可能性があります。

35.3.2 グラフィカルログインはありません

コンピュータは起動するものの、グラフィカルログインマネージャが起動しない場合は、デフォルトのランレベルの選択、あるいはX Window Systemの設定のいずれかに問題があると考えられます。ランレベルの設定を確認するには、`root`ユーザでログインし、コンピュータがランレベル5(グラフィカルデスクトップ)に起動する設定になっているか確認します。この確認を手軽にする方法は、`/etc/inittab`の内容を以下のように調べることです。

```
tux@mercury:~> grep "id:" /etc/inittab
id:5:initdefault:
```

返された行は、コンピュータのデフォルトランレベル(`initdefault`)が5に設定されており、グラフィカルデスクトップに起動するはずであることを示しています。ランレベルが5以外の数に設定されていた場合は、YaSTのランレベルエディタモジュールを使用して、5に設定します。

重要

ランレベル設定を手動で編集しないでください。手動で編集すると、SuSEconfig (YaSTによって実行される)が次回起動した際に、変更を上書きしてしまいます。手動で変更が必要な場合、将来のSuSEconfigによる変更を、*CHECK_INITTAB* (/etc/sysconfig/suseconfig内にある)をnoに設定して無効にします。

ランレベルが5に設定されている場合、デスクトップまたはX Windowsソフトウェアがおそらく誤って設定されているか、破損しています。/var/log/Xorg.*.logのログファイルから、Xサーバが開始する際にログされる詳細メッセージを調べます。開始中にデスクトップが失敗する場合、/var/log/messagesにエラーメッセージが書き込まれる可能性があります。これらのエラーメッセージがXサーバの設定の問題を示唆している場合は、これを直すようにしてください。それでもグラフィカルシステムが起動しない場合は、グラフィカルデスクトップを再インストールすることを考えてください。

ヒント: X Windowシステムを手動で起動する

簡単なテスト:startxコマンドは、ユーザが現在コンソールにログインしている場合、X Window Systemを設定されたデフォルトで開始するように強制します。これがうまくいかない場合は、コンソールにエラーがログされるはずです。

35.4 Loginの問題

ログインの問題とは、お使いのコンピュータが予期されるようこそ画面またはログインプロンプトまで実際に起動するが、ユーザ名およびパスワードを受け付けない、または受け付けるが、その後適切な動きをしない場合です(グラフィックデスクトップ開始の失敗、エラーの発生、コマンドラインに落ちる、など)。

35.4.1 有効なユーザ名とパスワードを使っても失敗する

この問題は、一般的にシステムがネットワーク認証またはディレクトリサービスを使用するように設定されており、何らかの理由で、設定されたサーバから結果を取得できない場合に発生します。このような場合でも、rootユーザは唯一のローカルユーザとしてこれらのコンピュータにログインできます。次に、コンピュータが一見機能しているように見えるのにログインを正しく処理できない一般的な理由をいくつか挙げます。

- ネットワークが機能していません。この場合の更なる対処方法については、35.5項 「ネットワークの問題」 (629 ページ)を参照してください
- DNSが機能していないです。(これによりGNOMEまたはKDEは動かず、システムは安全なサーバに有効なリクエストを送れません)。すべてのアクションに対して、コンピュータに極端に長い時間かかる場合は、この問題の可能性があります。このトピックの詳細は、35.5項 「ネットワークの問題」 (629 ページ)を参照してください。
- システムがKerberosを使用するように設定されている場合、システムのローカルタイムは、Kerberosサーバのタイムとの間で許容される相違を超えてしまっている可能性があります(通常 300秒)。NTP (network time protocol)が適切に動いていない、またはローカルのNTPサーバが動いていない場合、Kerberos の認証は機能しなくなります。その理由は、この認証はネットワーク間の一般的なクロック同期に依存しているからです。
- システムの認証設定が間違って設定されています。関連するPAM設定ファイルの中に誤字や命令の順序違いがないか確認します。PAMおよび関連する設定ファイルの構文に関する背景情報の詳細については、第2章 *Authentication with PAM* (↑*Security Guide (セキュリティガイド)*)を参照してください。
- ホームパーティションが暗号化されています。このトピックの詳細は、35.4.3項 「暗号化されたホームパーティションへのログインが失敗します」 (626 ページ)を参照してください。

外部のネットワーク問題を含まない他のすべての問題については、解決方法としてシステムをシングルユーザモードに再起動して、動作モードに再び起

動してログインし直す前に、設定を修復します。シングルユーザモードで起動するには、次の手順に従います。

1 システムを再起動します。ブート画面の表示に続き、プロンプトが表示されます。

2 ブートプロンプトでは、「1」を入力し、システムブートがシングルユーザモードになるようにします。

3 root用のユーザ名とパスワードを入力します。

4 すべての必要な変更をします。

5 コマンドラインに「telinit 5」を入力して、ネットワークありフルマルチユーザモードに起動します。

35.4.2 有効なユーザ名とパスワードが受け付けられない

これは、今のところユーザが経験する問題のうち、最も一般的なものです。その理由は、この問題が起こる原因がたくさんあるからです。ローカルのユーザ管理および認証を使用するか、ネットワーク認証を使用するかによって、異なる原因によりログイン失敗が発生します。

ローカルユーザ管理は、次の原因により失敗する可能性があります。

- 間違ったパスワードを入力した可能性があります。
- ユーザのホームディレクトリが、破損または書き込み保護されたデスクトップ設定ファイルを含んでいます。
- この特定のユーザを認証するのに、X Window Systemに何らかの問題があります。特に、ユーザのホームディレクトリが、現在のLinuxをインストールする以前の他のLinuxディストリビューションによって使用されている場合です。

ローカルログイン失敗の原因を発見するには、次の手順に従います。

1 認証方式全体をデバッグする前に、ユーザがパスワードを正しく覚えているか確認します。ユーザが正しいパスワードを覚えていない場合は、YaSTユーザ管理モジュールを使用してそのユーザのパスワードを変更します。Caps Lockキーに注意し、必要に応じてそのロックを解除します。

2 rootユーザでログインし、ログインプロセスおよびPAMのエラーメッセージがないかどうか/var/log/messagesを確認します。

3 コンソールからログインしてみます(Ctrl＋Alt＋F1キーを使用)。これが成功する場合、PAMには問題はありません。その理由は、そのユーザをそのコンピュータ上で認証可能だからです。X Window Systemまたはデスクトップ(GNOMEまたはKDE)で問題がないか探してみてください。詳細については、35.4.4項 「ログインは成功したがGNOMEデスクトップが失敗する」 (626 ページ)および35.4.5項 「ログインは成功したがKDEデスクトップが失敗する」 (627 ページ)を参照してください。

4 ユーザのホームディレクトリが他のLinuxディストリビューションによって使用されている場合、ユーザのホームにあるXauthorityファイルを削除します。Ctrl＋Alt＋F1キーを押してコンソールログインを使用し、rm .Xauthorityをこのユーザとして実行します。これにより、X認証の問題はこのユーザに関してはなくなるはずです。グラフィカルログインを再試行します。

5 グラフィカルログインがまだ失敗する場合、Ctrl＋Alt＋F1キーでコンソールログインを行ってください。他のディスプレイ上でXセッションを開始します。最初のもの(:0)はすでに使用中です。

```
startx -- :1
```

これによってグラフィカル画面とデストップが表示されます。表示されない場合は、X Window Systemのログファイル(/var/log/Xorg.*displaynumber*.log)を確認するか、デスクトップアプリケーションのログ(ユーザのホームディレクトリにある.xsession-errors)を確認して、異常な点がないか調べます。

6 設定ファイルが壊れていて、デスクトップが開始できなかった場合、35.4.4項「ログインは成功したがGNOMEデスクトップが失敗する」 (626ページ)または35.4.5項 「ログインは成功したがKDEデスクトップが失敗する」 (627 ページ)を続行します。

以下では、特定のユーザのネットワーク認証が、特定のコンピュータ上で失敗するのかの一般的な理由のいくつかを挙げます。

- 間違ったパスワードを入力した可能性があります。
- コンピュータのローカル認証ファイルの中に存在し、ネットワーク認証システムからも提供されるユーザ名が競合しています。
- ホームディレクトリは存在しますが、それが壊れている、または利用不可能です。書き込み保護がされているか、その時点でアクセスできないサーバ上にディレクトリが存在するかのどちらかの可能性があります。
- 認証システム内で、ユーザがその特定のサーバにログインする権限がありません。
- コンピュータのホスト名が何らかの理由で変更されていて、そのホストにユーザがログインする権限がありません。
- コンピュータが、認証サーバまたはそのユーザの情報を含んでいるディレクトリサーバに接続できません。
- この特定のユーザを認証するのに、X Window Systemに何らかの問題があります。特に、ユーザのホームが、現在のLinuxをインストールする以前に他のLinuxディストリビューションによって使用されている場合です。

ネットワーク認証におけるログイン失敗の原因を突き止めるには、次の手順に従います。

1. 認証方式全体をデバッグする前に、ユーザがパスワードを正しく覚えているか確認します。
2. 認証用にマシンが利用するディレクトリサーバを判別し、それがきちんと動作しており、他のマシンと適切に通信していることを確認します。
3. ユーザのユーザ名およびパスワードが他のマシン上でも使用できるかを判別し、そのユーザの認証データが存在し、適切に配布されていることを確認します。
4. 他のユーザが、問題のある動きをしているコンピュータにログインできるか観察します。その他のユーザが問題なくログインできたか、`root`でログインできた場合、ログイン後、`/var/log/messages`ファイルの内容を調

べます。ログインの試行に対応するタイムスタンプを見つけ出し、PAMによって、エラーメッセージが生成されていないか判別します。

5 コンソールからログインしてみます(Ctrl＋Alt＋F1キーを使用)。これが成功する場合、PAMやユーザのホームがあるディレクトリサーバには問題はありません。その理由は、そのユーザをそのコンピュータ上で認証可能だからです。X Window SystemまたはデスクトップGNOMEまたはKDEで問題がないか探してみてください。詳細については、35.4.4項 「ログインは成功したがGNOMEデスクトップが失敗する」 (626ページ)および35.4.5項「ログインは成功したがKDEデスクトップが失敗する」 (627ページ)を参照してください。

6 ユーザのホームディレクトリが他のLinuxディストリビューションによって使用されている場合、ユーザのホームにある`Xauthority`ファイルを削除します。Ctrl＋Alt＋F1キーを押してコンソールログインを使用し、`rm .Xauthority`をこのユーザとして実行します。これにより、X認証の問題はこのユーザに関してはなくなるはずです。グラフィカルログインを再試行します。

7 グラフィカルログインがまだ失敗する場合、Ctrl＋Alt＋F1キーでコンソールログインを行ってください。他のディスプレイ上でXセッションを開始します。最初のもの(`:0`)はすでに使用中です。

```
startx -- :1
```

これによってグラフィカル画面とデストップが表示されます。表示されない場合は、X Window Systemのログファイル(`/var/log/Xorg.`*`displaynumber`*`.log`)を確認するか、デスクトップアプリケーションのログ(ユーザのホームディレクトリにある`.xsession-errors`)を確認して、異常な点がないか調べます。

8 設定ファイルが壊れていて、デスクトップが開始できなかった場合、35.4.4項「ログインは成功したがGNOMEデスクトップが失敗する」 (626ページ)または35.4.5項 「ログインは成功したがKDEデスクトップが失敗する」 (627 ページ)を続行します。

35.4.3 暗号化されたホームパーティションへのログインが失敗します

ラップトップでは暗号化されたホームパーティションの使用が推奨されます。ラップトップにログインできない場合、通常その理由は簡単です。パーティションのロックを解除できなかったためです。

起動時に、暗号化されたパーティションのロックを解除するためにパスフレーズを入力する必要があります。パスフレーズを入力しない場合、パーティションがロックしたまま起動プロセスが続行します。

暗号化されたパーティションのロックを解除するには、次の手順に従います。

1 Ctrl + Alt + F1でテキストコンソールに切り替えます。

2 `root`になります。

3 次のコマンドにより、ロックを解除するプロセスを再開します。

```
/etc/init.d/boot.crypto restart
```

4 暗号化されたパーティションのロックを解除するためのパスフレーズを入力します。

5 テキストコンソールを終了し、Alt + F7でログイン画面に切り替えます。

6 通常通りログインします。

35.4.4 ログインは成功したがGNOMEデスクトップが失敗する

この場合に、GNOME環境設定ファイルが破損している可能性があります。兆候としては、キーボードがうまく動かない、画面のジオメトリが歪んでいる、または画面が空の灰色領域として表示されるなどがあります。この問題の重要な特徴は、他のユーザがログインする場合は、コンピュータは普通に機能するという点です。このような場合、問題のユーザのGNOME設定ディレクトリを単に新しい場所に移すことで、が新しいデスクトップを初期化するので、

比較的簡単にこの問題を解決できます。ユーザはGNOMEの再設定を強いられますが、データが失われません。

1 Ctrl + Alt + F1を押して、テキストコンソールを切り替えます。

2 ユーザ名でログインします。

3 ユーザのGNOME設定ディレクトリを、一時的な場所に移動します。

```
mv .gconf  .gconf-ORIG-RECOVER
mv .gnome2 .gnome2-ORIG-RECOVER
```

4 ログアウトします。

5 もう一度ログインします。ただし、アプリケーションは何も実行しないでください。

6 次のようにして、~/.gconf-ORIG-RECOVER/apps/ディレクトリを、新しい~/.gconfディレクトリにコピーすることで個々のアプリケーション設定データ(Evolutionの電子メールクライアントデータを含む)を回復します。

```
cp -a .gconf-ORIG-RECOVER/apps .gconf/
```

これによってログインの問題が生じる場合は、重要なアプリケーションデータのみの回復を試み、アプリケーションの残りを再設定します。

35.4.5 ログインは成功したがKDEデスクトップが失敗する

KDEデスクトップがユーザのログインを許可しない理由にはいくつかあります。壊れたKDEデスクトップ設定ファイルと同様に壊れたキャッシュデータもログインの問題を引き起こします。

キャッシュデータは、デスクトップの起動時にパフォーマンスを向上させるため使用されます。このデータが壊れていると、起動が遅くなったり、完全に失敗したりします。キャッシュデータを削除すると、デスクトップ起動のルーチンが最初から開始します。これには一般の起動よりも時間がかかりますが、その後はデータは無事でユーザはログインできます。

KDEデスクトップのキャッシュファイルを削除するには、rootユーザで以下のコマンドを実行します。

```
rm -rf /tmp/kde-user /tmp/ksocket-user
```

*user*は、ご使用のユーザ名に置き換えます。これらのディレクトリを削除しても、単に壊れたキャッシュファイルが削除されるだけです。この手順で実際のデータが削除されることはありません。

壊れたデスクトップ設定ファイルは、いつでも初期の設定ファイルに置き換えることができます。ユーザの調整を回復する場合は、デフォルトの設定値を使用して設定が復元されたあとに、一時的な場所からこれらのユーザの調整内容を慎重にコピーします。

壊れたデスクトップ設定ファイルを初期の設定ファイルに置き換えるには、以下の手順に従います。

1 Ctrl + Alt + F1を押して、テキストコンソールを切り替えます。

2 自分のユーザ名でログインします。

3 KDE設定ディレクトリおよび.skelファイルを一時的な場所に移動します。

- KDE3では、次のコマンドを使用します。

```
mv .kde  .kde-ORIG-RECOVER
mv .skel .skel-ORIG-RECOVER
```

- KDE4では、次のコマンドを使用します。

```
mv .kde4  .kde4-ORIG-RECOVER
mv .skel .skel-ORIG-RECOVER
```

4 ログアウトします。

5 もう一度ログインします。

6 デスクトップが正常に開始したら、ユーザ自身の設定を元の場所にコピーします。

```
cp -a KDEDIR/share .kde/share
```

*KDEDIR*をステップ 3 (628 ページ)のディレクトリに置き換えます。

重要

ユーザ自身による調整によりログインが失敗し、その状態が続く場合は、`.kde/share`ディレクトリはコピーせずに上記の手順を繰り返します。

35.5 ネットワークの問題

システム上の問題は、最初はそうは見えないのですが、ネットワークに関する問題であることが多いです。例えば、システムにユーザがログインできない理由は、ある種のネットワークの問題であったりします。ここでは、ネットワークの問題に直面した場合の簡単なチェックリストを紹介します。

手順 35.6 *ネットワークの問題を識別する方法*

コンピュータとネットワークの接続の確認をする場合、以下の手順に従ってください。

1 イーサネット接続を使用する場合、はじめにハードウェアを確認します。ネットワークケーブルがきちんとコンピュータおよびルータ(またはハブなど)に差し込んであることを確認してください。イーサネットコネクタの隣に管理用ライトがある場合、その両方がアクティブである必要があります。

接続に失敗する場合、お使いのネットワークケーブルが他のコンピュータでは使用可能かどうか確認します。使用可能な場合、ネットワークカードに問題の原因があります。ネットワークのセットアップにハブやスイッチを使用している場合は、それらが誤っている可能性もあります。

2 無線接続を使用7る場合、他のコンピュータからワイヤレスリンクが確立できるかどうか確認します。そうでない場合は、無線ネットワークの管理者にお問い合わせください。

3 基本的なネットワーク接続を確認し終わったら、どのサービスが応答していないかを探します。お使いの構成上のすべてのネットワークサーバのアドレス情報を集めます。適切なYaSTモジュール内で探すか、システム管理者に問い合わせてください。以下のリストには、ある構成内に含まれる一般的なネットワークサーバを、それらの故障の兆候とともに表わしています。

DNS (ネームサービス)
: 壊れた、あるいは誤作動しているネームサービスは、ネットワークの機能にさまざまな形で影響を与えます。ローカルコンピュータの認証がネットワークサーバによって行われ、それらのサーバが名前解決に問題があるために見つからない場合、ユーザはローカルコンピュータにログインすることもできません。壊れたネームサーバが管理するネットワーク上のコンピュータは、お互いを「認識」し、通信することができません。

NTP (タイムサービス)
: 誤作動している、または完全に壊れたNTPサービスは、Kerberosの認証およびXサーバの機能に影響を与えます。

NFS (ファイルサービス)
: NFSによってマウントされたディレクトリ内のデータを必要とするアプリケーションがあった場合、このNFSサービスがダウンしてるか、間違って設定されていると、そのアプリケーションは起動できないか、または正しく機能しません。最悪のケースとしては、 `.gconf`または`.kde`サブディレクトリを含んでいる、あるユーザのホームディレクトリが、NFSサーバの故障のために検出されなかった場合、そのユーザ個人のデスクトップ設定が起動しません。

Samba (ファイルサービス)
: アプリケーションが、故障したSambaサーバ上のディレクトリに保存されたデータを必要とする場合、アプリケーションは起動できないか、または正しく機能しません。

NIS (ユーザ管理)
: SUSE Linux Enterprise Serverシステムがユーザデータを提供するために故障したNISサーバを使用している場合、ユーザはこのコンピュータにログインできません。

LDAP (ユーザ管理)
: SUSE Linux Enterprise Serverシステムがユーザデータを提供するために故障したLDAPサーバを使用している場合、ユーザはこのコンピュータにログインできません。

Kerberos (認証)
: 認証が機能せず、すべてのコンピュータへのログインが失敗します。

CUPS (ネットワーク印刷)
ユーザが印刷できません。

4 ネットワークサーバが起動しているか、ネットワーク上で接続を確立できる設定になっているか、を確認します。

重要

次で説明するデバッグの手順は、内部ルーティングを必要としない、簡単なネットワークサーバ/クライアント設定にのみ適用されます。サーバとクライアントの両方が、追加でルーティングする必要のない同じサブネットのメンバーであることが前提です。

4a `ping` *`IP address`*または*`hostname`* (*`hostname`*はサーバのホスト名で置き換えます)を使って、サーバが起動中で、ネットワークに反応するかどうか確認します。このコマンドが成功する場合は、目的のホストは起動しており、ネットワークのネームサービスは正しく設定されていることがわかります。

pingが「`destination host unreachable`」というメッセージで失敗する場合、お使いのシステムまたは宛先のサーバが正しく設定されていないか、ダウンしています。その場合、他のコンピュータから`ping` *`IP address`*または*`your_hostname`*を実行して、お使いのシステムに到達可能か確認してください。他のコンピュータからお使いのコンピュータへ到達可能な場合、宛先のサーバが起動していないか、正しく設定されていません。

pingが「`unknown host`」というメッセージで失敗する場合、ネームサービスが正しく設定されていないか、使用したホスト名が正しくありません。この問題を詳細に調べるには、ステップ4b(631ページ)を参照してください。それでもpingが失敗する場合は、ネットワークカードが正しく設定されていないか、ネットワークのハードウェアに障害があります。

4b `host` *`hostname`*を使用して、接続しようとしているサーバのホスト名が適切なIPアドレスに変換され、またその逆も問題ないか確認します。このコマンドによって、このホストのIPアドレスが返される場合、ネームサービスは起動中です。この`host`コマンドが失敗する場合、お使いのホスト上の名前とアドレス解決に関係するすべてのネットワーク設定ファイルを確認します。

/etc/resolv.conf
: このファイルは、ネームサーバおよび現在使用中のドメインを管理するために使用されます。このファイルは手動で変更するか、YaSTまたはDHCPによる自動調整が可能ですが、自動調整のほうをお勧めします。ただし、このファイルが以下のような構造およびネットワークアドレスを含んでいること、さらにドメイン名が正しいことを確認してください。

```
search fully_qualified_domain_name
nameserver ipaddress_of_nameserver
```

このファイルには1つ以上のネームサーバのアドレスを含むことができますが、その中の少なくとも1つは、お使いのホストの名前解決が正しくできる必要があります。必要に応じて、YaSTネットワーク設定モジュール(［ホスト名/DNS］タブ)を使用してこのファイルを修正します。

お使いのネットワークの接続がDHCP経由の場合、YaST DNSおよびHostnameモジュール内で、［*DHCP経由でのホスト名の変更*］および［*DHCP経由でのネームサービスおよび検索リストの更新*］を選択し、DHCPを有効化してホスト名およびネームサービス情報を変更します。

/etc/nsswitch.conf
: このファイルは、Linuxがネームサービス情報を探す場所を示します。このようになります。

```
 ...
hosts: files dns
networks: files dns
...
```

dnsエントリは必須です。これにより、Linuxは外部のネームサーバを使用するようになります。通常、これらのエントリはYaSTにより自動的に管理されますが、慎重にチェックする必要があります。

ホスト上で、すべての関連エントリが正しい場合は、システム管理者に依頼して、正しいゾーン情報に関するDNSサーバの設定を確認してもらいます。DNSの詳細については、第24章 *ドメインネームシステム* (375 ページ)を参照してください。お使いのホストのDNS設定およびDNSサーバが正しいことが確認できた場合、

ネットワークおよびネットワークデバイス設定の確認に進みます。

4c お使いのシステムがネットワークサーバに接続できない状況で、ネームサービスの問題を障害原因の可能性リストから除外した場合は、ネットワークカードの設定を確認します。

`ifconfig` *`network_device`* (`root`ユーザで実行)コマンドを使用して、このデバイスが適切に設定されているか確認します。`inet`アドレスおよびマスクの両方が正しく設定されていることを確認してください。IPアドレス内に間違いがある場合、またはネットワークマスク内で不明のビットがある場合は、ネットワーク設定が使用不可能になります。必要であれば、サーバ上でもこの確認をしてください。

4d ネームサービスおよびネットワークサービスが正しく設定され起動している場合でも、外部のネットワーク接続がタイムアウトするのに時間がかかったり、完全に失敗する場合は、`traceroute` *`fully_qualified_domain_name`* (`root`ユーザで実行)コマンドを使用して、リクエストがネットワーク上でどのルートを使用するか追跡します。このコマンドは、お使いのコンピュータのリクエストが宛先に到達するまでに経由するゲートウェイ(ホップ)をリストします。各ホップの応答時間およびこのホップにそもそも到達可能か否かをリストします。tracerouteおよびpingコマンドを組み合わせて原因を追究し、管理者に知らせてください。

ネットワーク障害の原因を突き止めたら、自身でそれを解決するか(自分のコンピュータ上に問題がある場合)、お使いのネットワークのシステム管理者に原因について報告し、サービスを再設定するか、必要なシステムを修理してもらってください。

35.5.1 NetworkManagerの問題

ネットワーク接続に問題がある場合は、手順35.6「ネットワークの問題を識別する方法」 (629 ページ)の説明に従って原因を絞り込んでください。NetworkManagerが原因と考えられる場合は、以降の説明に従ってNetworkManager障害の理由を調べるために役立つログを取得してください。

1 シェルを開いて、rootとしてログインします。

2 NetworkManagerを再起動します。

```
rcnetwork restart -o nm
```

3 一般ユーザとしてhttp://www.opensuse.orgなどのWebページを開いて、正常に接続できているかどうかを確認します。

4 /var/log/NetworkManagerにある、NetworkManagerに関する情報を収集します。

NetworkManagerについての詳細は、第26章 *NetworkManagerの使用* (419 ページ)を参照してください。

35.6 データの問題

データの問題とは、コンピュータが正常に起動するかしないかに関係なく、システム上でデータが壊れており、システムの修復が必要な場合を言います。このような状況では、システムに障害が発生する前の状態にシステムを復元するために、重要なデータをバックアップする必要があります。SUSE Linux Enterprise Serverには、システムのバックアップ/復元や、救済システム(壊れたシステムを外部から復元するのに使用できる)用に、専用のYaSTモジュールが用意されています。

35.6.1 パーティションイメージの管理

パーティション全体、さらにはハードディスク全体からバックアップを実行することが必要になる場合があります。Linuxには、ディスクの正確なコピーを作成できるddツールが付属しています。gzipと組み合わせることで、若干の領域の節約になります。

手順 35.7 *ハードディスクのバックアップと復元*

1 ユーザrootとしてシェルを起動します。

2 ソースデバイスを選択します。これは、/dev/sdaなどが一般的です(*SOURCE* というラベルが付きます)。

3 イメージを保存する場所を決めます(*BACKUP_PATH*というラベルが付きます)。これは、ソースデバイスとは異なる場所にする必要があります。つまり、/dev/sdaからバックアップを作成する場合、イメージファイルは/dev/sdaに保存しないでください。

4 コマンドを実行して圧縮イメージファイルを作成します。

```
dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
```

5 次のコマンドによりハードディスクを復元します。

```
gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
```

バックアップするパーティションのみが必要な場合は、*SOURCE*プレースホールダーを対応するパーティションに置き換えます。この場合、イメージファイルを同じハードディスクにおくことができます。ただし、パーティションは異なります。

35.6.2 重要なデータのバックアップ

YaSTシステムバックアップモジュールを使用すれば、システムのバックアップは簡単に管理できます。

1 rootユーザでYaSTを開始し、［システム］>［システムバックアップ］を順に選択します。

2 バックアップに必要な詳細のすべて、アーカイブファイルのファイル名、スコープ、およびバックアップタイプを含むバックアッププロファイルを作成します。

2a ［*プロファイル管理*］>［*追加*］の順にクリックします。

2b アーカイブの名前を入力します。

2c ローカルバックアップをしたい場合は、そのバックアップの場所へのパスを入力します。ネットワークサーバ上にバックアップをアーカイブしたい場合は、IPアドレスまたはサーバの名前、およびアーカイブを保存するディレクトリを入力します。

2d アーカイブタイプを決め［次へ］をクリックします。

2e どのパッケージにも属さないファイルをバックアップするか、アーカイブ作成の前にファイルのリストを表示させるかなど、使用するバックアップオプションを決定します。また、変更されたファイルが、時間のかかるMD5メカニズムを使用して識別されるようにするのかも決定します。

［エキスパート］を使用して、ハードディスク領域全体のバックアップのためのダイアログに入ります。現在、このオプションはExt2ファイルシステムのみに適用されます。

2f 最後に、ロックファイルまたはキャッシュファイルなど、バックアップの必要のない一部のシステム領域を、バックアップ領域から除外するための検索条件を設定します。項目を追加、編集、または削除して、必要にあった条件を設定し、［*OK*］を押して終了します。

3 プロファイル設定を終了したら、［*Create Backup (バックアップの作成)*］を使用した即時バックアップの開始、または自動バックアップの設定ができます。他のさまざまな目的のために設定されたプロファイルも作成できます。

特定のプロファイル用に自動バックアップを設定するには、以下の手順に従います。

1 ［*プロファイル管理*］メニューから、［*自動バックアップ*］を選択します。

2 ［*バックアップの自動開始*］を選択します。

3 バックアップの頻度を決定します。［*毎日*］、［*毎週*］、または［*毎月*］を選択します。

4 バックアップの開始時間を決定します。これらの設定は選択されたバックアップの頻度に依存します。

5 古いバックアップを保存するか、保存する場合は何世代にするかを決定します。バックアッププロセスの自動的に生成されたステータスメッセージを受け取るには、［*rootユーザにサマリメールを送信する*］にチェックを入れます。

6 設定内容を適用し、指定した時刻にバックアップを開始するには、［*OK*］をクリックします。

35.6.3 システムバックアップの復元

YaSTシステムリストアモジュールを使用して、バックアップからシステム設定を復元します。バックアップの全体を復元するか、壊れたために古い状態にリセットする必要のある、特定のコンポーネントのみを選択します。

1 ［*YaST*］ > ［システム］ > ［*システムの復元*］の順にクリックします。

2 バックアップファイルの場所を入力します。ローカルファイル、ネットワーク上でマウントされたファイル、またはフロッピーディスクおよびDVDなどの取り外し可能なデバイス上のファイルなどがあります。次に、［*次へ*］をクリックします。

次のダイアログでは、ファイル名、作成日、バックアップのタイプ、およびオプションのコメントなどのアーカイブプロパティのサマリが表示されます。

3 ［*アーカイブの内容*］をクリックして、アーカイブされた内容を参照します。［*OK*］をクリックすると、［*アーカイブプロパティ*］ダイアログに戻ります。

4 ［*エキスパート用オプション*］では、復元プロセスを微調整するダイアログが開きます。［*OK*］をクリックすると、［*アーカイブプロパティ*］ダイアログに戻ります。

5 ［*次へ*］をクリックすると、復元するパッケージのビューが開きます。［*承認*］［*を押して、アーカイブ内のすべてのファイルを復元するか、*］［Select Al l］［、］［Deselect All］［、*および*］［Select Files］［*ボタンを使って、選択内容の微調整をします。*］RPMデータベースが壊れているか削除され、バックアップにこのファイルが含まれている場合にのみ、［*RPMデータベースの復元*］オプションを使用します。

6 ［*承認*］をクリックすると、バックアップが復元されます。［*完了*］をクリックして、復元プロセスが完了したあと、モジュールを終了します。

35.6.4 壊れたシステムの復旧

システムが起動し正常に稼動するのに失敗する理由はいくつか考えられます。最も一般的な理由としては、システムクラッシュによるファイルシステムの破損や、ブートローダ設定の破損があります。

これらの状況を解決するため、SUSE Linux Enterprise Serverでは、2種類の方法を用意してます。それらは、YaSTシステム修復機能の使用、またはレスキューシステムの起動です。以下のセクションでは、両方のタイプのシステム修復方法について説明します。

35.6.4.1 YaSTシステム修復の使用

注記: キーボードと言語設定

ブート後に言語設定を変更すると、キーボードの設定もそれに応じて変更されます。

YaSTシステム修復モジュールを起動する前に、お客さまのニーズを一番満たすように、モジュールを起動するモードを決めます。システム障害の重大度と原因(および担当者の専門知識)に応じて、3つのモードから選択できます。

自動修復
: 不明な原因でシステムに障害が起こった場合で、そもそもシステムのどの部分が失敗の原因となっているか分からない場合は、［*自動修復*］を使用します。広範囲に及ぶ自動化されたチェックがお使いのシステム上のすべてのコンポーネントで実行されます。この手順の詳細な説明については、「自動修復」 (639 ページ)を参照してください。

カスタム修復
: システムに障害が発生し、その原因がどのコンポーネントにあるか分かっている場合、［*カスタム修復*］を使用して、コンポーネントに対して行うシステム分析の範囲を限定することにより、冗長なシステムチェックを短縮できます。例えば、障害の前のシステムメッセージに、パッケージデータベースのエラーの可能性を示唆する記述があれば、分析と修復手順を、システムのこの側面の検査および復元に限定できます。この手順の詳細な説明については、「カスタム修復」 (641 ページ)を参照してください。

エキスパート設定用ツール
: 障害が発生したコンポーネントとその修復方法がはっきりわかっている場合は、分析を実行せずに、直接、該当するコンポーネントの修復に必要なツールを適用できます。詳細については、「エキスパート設定用ツール」 (642 ページ)を参照してください。

前で説明した修復モードから1つを選択し、以下で概説するようにシステム修復を続行します。

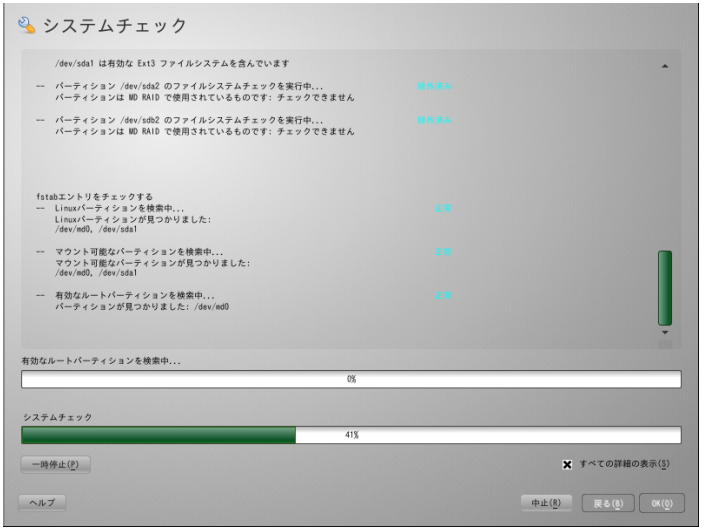
自動修復

YaSTシステム修復の自動修復モードを起動するには、次の手順に従います。

1. SUSE Linux Enterprise Serverのインストールメディアを DVDドライブに挿入します。
2. システムを再起動します。
3. ブート画面で、［*インストール済みシステムの修復*］を選択します。
4. 使用許諾契約に同意したら、［*次へ*］をクリックします。
5. ［自動修復］［*を選択します。*］

   YaSTは、ここでインストールされたシステムの広範囲に及ぶ分析を起動します。このプロシージャの進捗状況は、画面下部にある2つの進捗バーで表示されます。上のバーは現在実行中のテストの進捗状況を示します。下のバーは解析の全体の進捗状況を示します。上部のログウィンドウで、現在実行中のテストおよび結果を追跡することができます。詳細については、図35.4「自動修復モード」 (640 ページ)を参照してください。

図 35.4　自動修復モード



以下のメインテストは、自動修復を実行すると毎回実行されます。さらに、それらには、多数のサブテストが含まれています。

パーティションテーブルのチェック
: 検出された全ハードディスクのパーティションテーブルの妥当性と一貫性が検査されます。

スワップエリアのチェック
: インストール済みのシステムのスワップパーティションが検出およびテストされ、適用可能な場合は、それらのパーティションをアクティブにすることができます。システム修復の速度を上げるには、このアクティベーションを承諾する必要があります。

ファイルシステムのチェック
: 検出されたすべてのファイルシステムがファイルシステム固有の検査の対象となります。

fstabエントリのチェック
: このファイルのエントリの完全性と一貫性が検査されます。有効なパーティションは、すべてマウントされます。

パッケージデータベースのチェック
: 最小構成のインストールの運用に必要なすべてのパッケージが存在しているか、検査されます。基本パッケージの解析もオプションとして可能ですが、基本パッケージの数が多いので、これは長時間かかります。

ブートローダの設定のチェック
: インストールされているシステムのブートローダ設定(GRUBかLILO)の完全性と一貫性が検査されます。ブートデバイスとrootデバイスが調べられ、initrdモジュールの可用性が検査されます。

6 エラーを検出するたびに、プロシージャが一時停止し、エラーの詳細および可能な解決策を提示するダイアログが表示されます。

提案された修復を承認する前に、画面のメッセージを注意深く読みます。提案された修復を断る場合、システムは修復なしの状態のままになります。

7 修復プロセスが正常に終了した後に、［*OK*］および［*完了*］をクリックし、インストールメディアを取り出します。システムは自動的に再起動します。

カスタム修復

［*カスタム修復*］モードを起動し、システムのコンポーネントの一部を選択的に検査するには、次の手順に従います。

1 SUSE Linux Enterprise ServerのインストールメディアをDVDドライブに挿入します。

2 システムを再起動します。

3 ブート画面で、［*インストール済みシステムの修復*］を選択します。

4 使用許諾契約に同意したら、［*次へ*］をクリックします。

5 ［*カスタム修復*］を選択します。

［*カスタム修復*］では、実行可能なテストのリストが、最初は、すべて実行対象として選択された状態で表示されます。全部のテスト範囲は、自動修復と合致します。損傷が存在していない個所が、既に判明している場合、対応するテストのチェックマークを消します。［*続行*］をクリックすると、

より狭い範囲のテストプロシージャが開始され、実行時間が大幅に短縮されます。

すべてのテストグループを個別に実行できるわけではありません。fstab エントリの解析は常に、既存のスワップパーティションも含めたファイルシステムの検証と結び付いています。YaSTでは、このような依存性の条件が自動的に満たされ、必要なテストが最少数で実行されます。YaSTは、暗号化されたパーティションをサポートしません。そのようなパーティションがある場合は、YaSTから通知されます。

6 エラーを検出するたびに、プロシージャが一時停止し、エラーの詳細および可能な解決策を提示するダイアログが表示されます。

提案された修復を承認する前に、画面のメッセージを注意深く読みます。提案された修復を断る場合、システムは修復なしの状態のままになります。

7 修復プロセスが正常に終了した後に、［*OK*］および［*完了*］をクリックし、インストールメディアを取り出します。システムは自動的に再起動します。

エキスパート設定用ツール

SUSE Linux Enterprise Serverについて十分な知識があり、システム内の修復の対象が明確にわかっている場合は、システム分析をスキップして、直接、ツールを適用します。

YaSTシステム修復の［エキスパート*設定用ツール*］の機能を使用するには、以下の手順に従います。

1 SUSE Linux Enterprise Serverのインストールメディアを DVD ドライブに挿入します。

2 システムを再起動します。

3 ブート画面で、［*インストール済みシステムの修復*］を選択します。

4 使用許諾契約に同意したら、［次へ］をクリックします。

5 ［エキスパート*設定用ツール*］をクリックし、修復オプションを選択します。

6 修復プロセスが正常に終了した後に、［*OK*］および［*完了*］をクリックし、インストールメディアを取り出します。システムは自動的に再起動します。

［*エキスパート設定用ツール*］では、次のオプションで、障害の発生したシステムを修復できます。

［*新しいブートローダをインストールする*］
YaSTのブートローダの設定モジュールを起動します。詳細については、10.2項「YaSTによるブートローダの設定」(140ページ)を参照してください。

［*インストールしたシステムをブートする*］
すでにインストールされているLinuxシステムのブートを試行します。

［*パーティションツールの起動*］
YaSTのパーティションのエキスパート設定ツールが起動します。

［*ファイルシステムの修復*］
インストール済みのシステムのファイルシステムを検査します。はじめに、検出された全パーティションの中から1つを選択するダイアログが表示され、検査対象を選択することができます。

［*失われたパーティションの復旧*］
損傷したパーティションテーブルの再構築を試みることができます。はじめに、検出されたハードディスクのリストが表示され、対象を選択します。［*OK*］をクリックすると検証が開始されます。コンピュータの速度およびハードディスクのサイズと速度によっては、このプロセスにしばらく時間がかかることがあります。

重要: ［*パーティションテーブルの再構築*］

パーティションテーブルの再構築は、難しい処理です。YaSTでは、ハードディスクのデータセクタを解析することにより、失われたパーティションの認識が試みられます。認識が成功すると、失われたパーティションが再構築したパーティションテーブルに追加されます。ただし、これは予想可能なすべての事例で成功するわけではありません。

［*システム設定のフロッピーへの保存*］
このオプションは、重要なシステムファイルをフロッピーディスクに保存します。それらのファイルの1つが損傷した場合は、ディスクから復元できます

［*インストールされたソフトウェアの確認*］
パッケージデータベースの整合性と、最も重要なパッケージの可用性を検査します。このツールを使うと、損傷しているインストールパッケージを再インストールできます。

35.6.4.2 レスキューシステムの使用

SUSE Linux Enterprise Serverは、レスキューシステムを装備しています。レスキューシステムは、RAMディスクにロードして、ルートファイルシステムとしてマウントできる小さなLinuxシステムで、これを利用して外部からLinuxパーティションにアクセスすることができます。レスキューシステムを使用して、システムの重要な部分を復元したり、適切な変更を行ったりできます。

- 任意の種類の設定ファイルを操作できます。
- ファイルシステムの欠陥をチェックして、自動修復プロセスを開始することができます。
- インストールされているシステムを、「他のルート」環境内からアクセスすることができます。
- ブートローダーの設定を確認、変更、および再インストールできます。
- 正常にインストールされていないデバイスドライバや使用不能なカーネルを修復できます。
- partedコマンドを使って、パーティションサイズを変更できます。このツールの詳細については、GNU PartedのWebサイト(http://www.gnu.org/software/parted/parted.html)を参照してください。

レスキューシステムは、さまざまなソースや場所からロードすることができます。一番簡単な方法は、オリジナルのインストールメディアからレスキューシステムをブートすることです。

1 インストールメディアをDVDドライブに挿入します。

2 システムを再起動します。

3 ブート画面で、F4を押し、［*DVD-ROM*］を選択します。次に、メインメニューから［*レスキューシステム*］を選択します。

4 `Rescue:`プロンプトに「`root`」と入力します。パスワードは必要ありません。

次の例は、リモートブートの場合です。DVDなど、他のブートメディアを使用する場合は、`info`ファイルを適宜変更し、通常のインストールと同様にブートします。

1 PXEブートセットアップの設定を入力し、`install=`*`protocol`*`://`*`instsource`*行と`rescue=1`行を追加します。修復システムを起動する必要がある場合は、代わりに`repair=1`を使用します。通常のインストールと同様に、*`protocol`*はサポートする任意のネットワークプロトコル(NFS、HTTP、FTPなど)を表しています。また、*`instsource`*は、ネットワークインストールソースへのパスを表します。

2 項 「Wake on LAN」 (第14章 *リモートインストール*, ↑*導入ガイド*)に説明したように、「Wake on LAN」を使用してシステムをブートします。

3 `Rescue:`プロンプトに「`root`」と入力します。パスワードは必要ありません。

レスキューシステムが起動したら、Alt＋F1～Alt＋F6を使って、仮想コンソールを使用することができます。

シェルおよび他の多くの便利なユーティリティ(マウントプログラムなど)は、`/bin`ディレクトリにあります。`sbin`ディレクトリには、 ファイルシステムを検討し、修復するための重要なファイルおよびネットワークユーティリティが入っています。このディレクトリには、最も重要なバイナリも入っています。たとえばステムメンテナンス用にはfdisk、mkfs、mkswap、mount、mount、init、およびshutdownがあり、ネットワークメンテナンス用にはifconfig、ip、route、およびnetstatがあります。`/usr/bin`ディレクトリには、vi editor、find、less、およびsshがあります。

システムメッセージを表示するには、`dmesg`コマンドを使用するか、または`/var/log/messages`ファイルを参照してください。

設定ファイルの確認と修正

レスキューシステムを使った環境設定情報の修正例として、環境設定ファイルが壊れたためシステムが正常にブートできなくなった場合を考えてみましょう。このような場合は、レスキューシステムを使って設定ファイルを修復します。

環境設定ファイルを修正するには、以下の手順に従ってください。

1 前述のいずれかの方法を使って、レスキューシステムを起動します。

2 /dev/sda6下にあるルートファイルシステムをレスキューシステムにマウントするには、以下のコマンドを使用します。

```
mount /dev/sda6 /mnt
```

システム中のすべてのディレクトリが、/mnt下に配置されます。

3 マウントしたルートファイルシステムのディレクトリに移動します。

```
cd /mnt
```

4 問題の発生している設定ファイルを、viエディタで開きます。次に、設定内容を修正して、ファイルを保存します。

5 レスキューシステムから、ルートファイルシステムをアンマウントします。

```
umount /mnt
```

6 コンピュータを再起動します。

ファイルシステムの修復と確認

一般的に、稼動システムではファイルシステムを修復できません。重大な問題が見つかった場合、ルートファイルシステムをブートできなくなることさえあります。この場合、システムブートは「カーネルパニック」で終了します。この場合、外部からシステムを修復するしか方法はありません。この作業には、YaSTシステム修復の使用を強くお勧めします(詳細は35.6.4.1項「YaSTシステム修復の使用」(638ページ)参照)。ただし、手動でファイルシステムを確認、修復する必要がある場合は、レスキューシステムを起動します。レスキューシステムには、btrfs、ext2、ext3、ext4、reiserfs、xfs、

dosfs、およびvfatの各ファイルシステムを確認し、修復するユーティリティが用意されています。

インストール済みシステムへのアクセス

レスキューシステムからインストール済みのシステムにアクセスする必要がある場合は、それを*change root*(ルート変更)環境で行う必要があります。これは、たとえば、ブートローダの設定を変更したり、ハードウェア設定ユーティリティを実行するために行います。

インストール済みシステムに基づいたchange root(ルート変更)環境を設定するには、以下の手順に従ってください。

1. まず、インストールしたシステムからのルートパーティションとデバイスファイルシステムをマウントします(デバイス名を現在の設定に変更します)。

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

2. 新しい環境に「change root」(ルート変更)します。

```
chroot /mnt
```

3. /procおよび/sysをマウントします。

```
mount /proc
mount /sys
```

4. 最後に、インストール済みシステムから、残りのパーティションをマウントします。

```
mount -a
```

5. これで、インストール済みシステムにアクセスできるようになります。システムを再起動する前に、umount -aを使ってパーティションをアンマウントし、exitコマンドを実行して「change root」(ルート変更)環境を終了してください。

警告: 制限

インストール済みシステムのファイルやアプリケーションにフルアクセスできますが、いくつかの制限事項もあります。実行中のカーネルは、レスキューシステムでブートされたカーネルであり、ルート変更環境でブートされたカーネルではありません。このカーネルは、必要最低限のハードウェアしかサポートしておらず、カーネルのバージョンが完全に一致しない限り、インストール済みシステムからカーネルモジュールを追加することはできません。常に、現在実行中の(レスキュー)カーネルのバージョンを`uname -r`でチェックし、次に、一致するサブディレクトリがchange root環境の`/lib/modules`ディレクトリに存在するかどうか調べてください。存在する場合は、インストールされたモジュールを使用できます。そうでない場合は、USBやスティックなど、他のメディアにある正しいバージョンを提供する必要があります。多くの場合、レスキューカーネルのバージョンは、インストールされているバージョンと異なります。その場合は、たとえば、サウンドカードなどに簡単にアクセスすることはできません。また、GUIも利用できません。

また、Alt + F1からAlt + F6を使ってコンソールを切り替えると、「change root」(ルート変更)環境は終了することに注意してください。

ブートローダの変更と再インストール

場合によっては、ブートローダが壊れてしまい、システムをブートできなくなることもあります。たとえば、ブートローダが正常に機能しないと、起動ルーチンは物理ドライブとそのLinuxファイルシステム中の場所とを関連付けられず、正常な処理を行うことができません。

ブートロードの設定を確認し、ブートロードを再インストールするには、以下の手順に従ってください。

1 の説明に従って、インストール済みシステムにアクセスするための適切な作業を行います。「インストール済みシステムへのアクセス」 (647 ページ)

2 次のファイルが第10章 *ブートローダGRUB* (127 ページ)に示されているGRUBの設定ルールに従って正しく設定されているかどうかチェックし、必要に応じて修正します。

- `/etc/grub.conf`

- /boot/grub/device.map
- /boot/grub/menu.lst
- /etc/sysconfig/bootloader

3 以下のコマンドシーケンスを使って、ブートローダを再インストールします。

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

4 パーティションをアンマウントして、「change root」(ルート変更)環境からログアウトします。次に、システムを再起動します。

```
umount -a
exit
reboot
```

カーネルインストールの修復

カーネルアップデートによって、システムの操作に影響する可能性のある新しいバグが導入される場合があります。たとえば、一部のシステムハードウェアのドライバに障害が発生し、そのハードウェアのアクセスや使用ができなくなることがあります。その場合は、機能した最後のカーネルに戻すか(システムで使用可能な場合)、インストールメディアから元のカーネルをインストールします。

ヒント: 更新後も最後のカーネルを保持する方法

正常でないカーネルアップデート後にブートできなくなることを防ぐには、カーネルの複数バージョン機能を使用して、更新後にどのカーネルを保持するかlibzyppに指示します。

たとえば、最後の2つのカーネルと現在実行中のカーネルを常に保持するには、次のコードを、

```
multiversion.kernels = latest,latest-1,running
```

/etc/zypp/zypp.confファイルに追加します。

また、SUSE Linux Enterprise Serverでサポートされていないデバイスのドライバが破損し、その再インストールまたは更新が必要な場合があります。たとえば、ハードウェアベンダが、ハードウェアRAIDコントローラなどの特定のデバイスを使用している場合は、オペレーティングシステムによって認識されるバイナリドライバが必要です。ベンダは、通常、要求されたドライバの修正または更新バージョンを含むドライバアップデートディスクをリリースします。

両方のケースで、レスキューモードでインストールされているシステムにアクセスし、カーネル関係の問題を修正する必要があります。さもないと、システムが正しくブートしないことがあります。

1 SUSE Linux Enterprise Serverのインストールメディアからブートします。

2 正常でないカーネルアップデート後に修復を行っている場合、次のステップはスキップしてください。DUD(ドライバアップデートディスク)を使用する必要がある場合は、F6を押して、ブートメニューの表示後にドライバアップデートをロードし、ドライバアップデートへのパスまたはURLを選択して、［*はい*］をクリックして確認します。

3 ブートメニューから［*レスキューシステム*］を選択し、Enterを押します。DUDの使用を選択した場合は、ドライバアップデートの保存先を指定するように要求されます。

4 `Rescue:`プロンプトに「`root`」と入力します。パスワードは必要ありません。

5 ターゲットシステムを手動でマウントし、新しい環境に「change root」(ルート変更)します。詳細については、「インストール済みシステムへのアクセス」 (647 ページ)を参照してください。

6 DUDを使用する場合は、障害のあるデバイスドライバパッケージのインストール/再インストール/更新を行います。インストールされたカーネルバージョンがインストールするドライバのバージョンと正確に一致することを常に確認してください。

障害のあるカーネルアップデートのインストールを修復する場合は、次の手順で、インストールメディアから元のカーネルをインストールできます。

6a DVDデバイスを`hwinfo --cdrom`で識別し、識別したデバイスを`mount /dev/sr0 /mnt`でマウントします。

6b DVD上のカーネルファイルが保存されているディレクトリにナビゲートします(たとえば、 `cd /mnt/suse/x86_64/`)。

6c 必要なパッケージ`kernel-*`、`kernel-*-base`、および`kernel-*-extra`のカスタマイズしたバージョンを、`rpm -i`コマンドでインストールします。

6d インストールが完了したら、新しくインストールしたカーネルに関する新しいメニューエントリがブートローダの設定ファイルに追加されたかどうかチェックします(grubの場合は`/boot/grub/menu.lst`)。

7 設定ファイルを更新し、必要に応じてブートローダを再初期化します。詳細については、「ブートローダの変更と再インストール」(648ページ)を参照してください。

8 システムドライブからブート可能なメディアをすべて除去し、再起動します。

35.7 IBM System z:initrdのレスキューシステムとしての使用

IBM System z用のSUSE® Linux Enterprise Serverカーネルをアップグレード、変更した場合、何らかの原因でシステムが不整合な状態で再起動されると、インストールされているシステムのIPL標準処理が失敗する可能性があります。一般的にこの問題は、アップデートされたSUSE Linux Enterprise Serverカーネルをインストールした後で、IPLレコードをアップデートするziplプログラムをまだ実行していない場合に発生します。この場合、レスキューシステムとして標準のインストールパッケージを使用して、そこからziplプログラムを実行してIPLレコードをアップデートしてください。

35.7.1 レスキューシステムのIPL処理

重要: インストールデータを利用できるようにする

この方法を使用する場合、IBM System z版SUSE Linux Enterprise Serverのインストールデータが利用可能でなければなりません。詳細については、項「インストールデータを利用できるようにする」 (第4章 *IBM System zへのインストール*, ↑*導入ガイド*)を参照してください。また、SUSE Linux Enterprise Serverのルートファイルシステムを含むデバイスのチャネル番号、およびデバイス内のパーティション番号が必要になります。

まず、項 「インストールの準備」 (第4章 *IBM System zへのインストール*, ↑*導入ガイド*)の説明に従って、IBM System z用SUSE Linux Enterprise Serverインストールシステムを IPL処理します。IPL処理すると、ネットワークアダプタのリストが表示されます。

レスキューシステムを開始するには［*インストール処理またはシステムを開始する*］を選択してから［*レスキューシステムを開始する*］を選択します。次に、インストール環境に応じて、ネットワークアダプタやインストールソースに関するパラメータを指定する必要があります。レスキューシステムがロードされ、ログインプロンプトが表示されます。

```
Skipped services in runlevel 3:  nfs nfsboot

Rescue login:
```

`root`として、パスワードを指定しないでログインすることができます。

35.7.2 ディスクの設定

この状態では、設定されているディスクはありません。作業を続行する前に、ディスクを設定する必要があります。

手順 35.8 *DASDの設定*

1 DASDを設定するには、以下のコマンドを使用します。

```
dasd_configure 0.0.0150 1 0
```

ここで、「0.0.0150」は、DASDが接続されているチャネルを表します。`1`は、ディスクをアクティブにすることを表しています(ここに`0`を指定する

と、ディスクが無効になる)。0は、ディスクに「DIAGモード」でアクセスしないことを表します(ここに1を指定すると、ディスクへのDAIGアクセスが有効になります)。

2 DASDがオンラインになり(cat /proc/partitionsで確認)、コマンドを使用できるようになります。

手順 35.9 zFCPディスクの設定

1 zFCPディスクを設定するには、まずzFCPアダプタを設定する必要があります。そのためには次のコマンドを使用します。

```
zfcp_host_configure 0.0.4000 1
```

0.0.4000はアダプタが接続されているチャネルを、1(ここに0を指定するとアダプタが無効になる)はアクティブにすることを示します。

2 アダプタをアクティブにしたら、ディスクを設定することができます。そのためには次のコマンドを使用します。

```
zfcp_disk_configure 0.0.4000 1234567887654321 8765432100000000  1
```

0.0.4000は前に使われていたチャネルIDを、1234567887654321はWWPN(World wide Port Number)を、そして8765432100000000はLUN(論理ユニット番号)を表しています。1(ここに0を指定するとディスクが無効になる)は、ディスクをアクティブにすることを表しています。

3 zFCPディスクがオンラインになり(cat /proc/partitionsで確認)、コマンドを使用できるようになります。

35.7.3 ルートデバイスのマウント

必要なディスクがすべてオンラインになったら、ルートデバイスをマウントします。ここでは、DASDの2番目のパーティション(/dev/dasda2)にルートデバイスがあると仮定します。この場合、使用するコマンドはmount /dev/dasda2 /mntになります。

重要: ファイルシステムの整合性

インストール済みシステムが正しくシャットダウンされなかった場合は、マウント前にファイルシステムの整合性を確認しておくことをお勧めします。整合性を確認することによって、予期せぬ事態によるデータ消失の危険を回避することができます。この例では、`fsck /dev/dasda2`コマンドを実行して、ファイルシステムの整合性を確認します。

mountコマンドを実行するだけでも、ファイルシステムが正しくマウントされたかどうかを確認することができます。

例 35.1 mountコマンドの出力

```
SuSE Instsys suse:/ # mount
shmfs on /newroot type shm (rw,nr_inodes=10240)
devpts on /dev/pts type devpts (rw)
virtual-proc-filesystem on /proc type proc (rw)
/dev/dasda2 on /mnt type reiserfs (rw)
```

35.7.4 マウントされているファイルシステムの変更

`ziplコマンド`実行時に、レスキューシステムからではなく、インストール済みシステムのルートデバイスから設定ファイルを読み込ませるためには、`chrootコマンド`を使ってルートデバイスをインストール済みシステムに変更します。

例 35.2 chrootを使ったマウントするファイルシステムの変更

```
SuSE Instsys suse:/ # cd /mnt
SuSE Instsys suse:/mnt # chroot /mnt
```

35.7.5 ziplの実行

次に、`zipl`を実行して、IPLレコードを正しい値に書き換えます。

例 35.3 ziplを使ったIPLレコードのインストール

```
sh-2.05b# zipl
building bootmap : /boot/zipl/bootmap
adding Kernel Image : /boot/kernel/image located at 0x00010000
adding Ramdisk : /boot/initrd located at 0x00800000
```

```
adding Parmline : /boot/zipl/parmfile located at 0x00001000
Bootloader for ECKD type devices with z/OS compatible layout installed.
Syncing disks....
...done
```

35.7.6 レスキューシステムの終了

レスキューシステムを終了するには、まずchrootコマンドで開かれたシェルをexitコマンドで終了します。データ消失を防ぐために、syncコマンドを使って、バッファ上にあるまだ書き込まれていないデータをすべてディスクに書き込みます。次に、レスキューシステムのルートディレクトリに移動して、IBM System z版SUSE Linux Enterprise Serverのルートデバイスをアンマウントします。

例 35.4 *ファイルシステムのアンマウント*

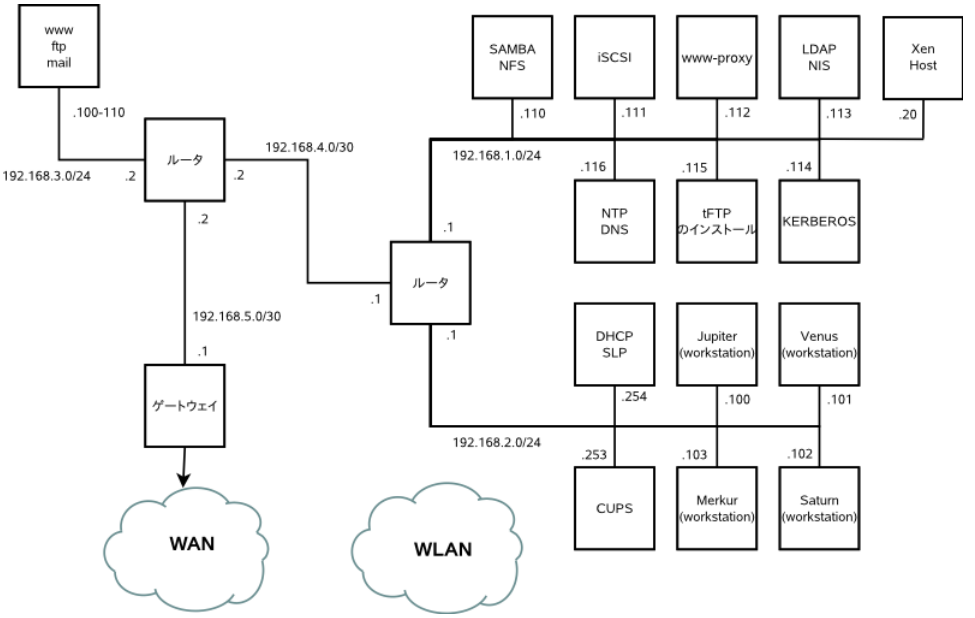
```
SuSE Instsys suse:/mnt # cd /
SuSE Instsys suse:/ # umount /mnt
```

最後に、haltコマンドを実行して、レスキューシステムを終了します。項「IBM System z: インストール済みシステムのIPL処理」 (第6章 *YaSTによるインストール;*, ↑*導入ガイド*)で説明されているように、SUSE Linux Enterprise ServerシステムのIPL処理が行われます。

A

サンプルネットワーク

このサンプルネットワークは、SUSE® Linux Enterprise Serverドキュメントのすべてのネットワーク関連の章で使用されます。



GNU Licenses

B

This appendix contains the GNU Free Documentation License version 1.2.

GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.