Red Hat Linux 9

Red Hat Linux カスタマイズガイド

Red Hat Linux 9: Red Hat Linux カスタマイズガイド
製作著作‘
‘
2003 ：Red Hat, Inc.


Red Hat, Inc.

1801 Varsity Drive
Raleigh NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA

rhl-cg(JA)-9-Print-RHI (2003-02-20T01:08)

目次

はじめに

Red Hat Linux カスタマイズガイドへようこそ。

この*Red Hat Linux* カスタマイズガイドでは、Red Hat Linuxシステムを目的に合わせてカスタマイズする方法について解説しています。システムを設定しカスタマイズする手順を、タスクごとにステップバイステップで説明していくガイドをお探しの方に適切なガイドです。このガイドは次のような多くの中級トピックを解説しています。

- ネットワークインターフェイスカード(NIC)の設定
- Kickstartインストールの実行
- Samba共有の設定
- RPMでソフトウェアを管理
- システム情報を確定する
- カーネルのアップグレード

本ガイドの構成は、次のとおりです。

- インストール関連のリファレンス
- ネットワーク関連のリファレンス
- システム設定
- パッケージの管理

このガイドは、ユーザーにRed Hat Linuxシステムの基本的な知識があることを前提としています。デスクトップの設定やオーディオCD-RPMの再生などの基礎知識を説明している参照文書については、「*Red Hat Linux* 入門ガイド」を参照してください。また、Red Hat Linuxファイルシステムの概要など、本書の範囲を超える高度な詳細情報については、「*Red Hat Linux* 参照ガイド」を参照してください。

HTML形式とPDF形式のRed Hat Linuxマニュアルマニュアルはドキュメントに収録されています。英語版はhttp://www.redhat.com/docs/からも入手できます。

注意

このガイドには編集時点での最新情報が反映されていますが、ガイドの発行後に入手可能になった情報については「*Red Hat Linux*リリースノート」をお読みください。そのような情報は、Red Hat Linux CD #1に収録されています。次のWebサイトからオンラインでも入手できます。

```
http://www.redhat.com/docs/manuals/linux
```

1. このガイドでの変更点

今回の改版で読者からの要望に応えるためのトピックと新機能がRed Hat Linux 9に追加されています。このガイドでの主な変更点は次の通りです。

ディスク容量制限の実践

‘ この新しい章はディスク容量制限の設定と管理の方法について説明しています。

認証の設定

‘ この新しい章は **認証設定ツール**の使い方について説明しています。

ユーザー設定

‘ この章はユーザーとグループの管理用コマンドラインユーティリティが追加されています。また、システムに新規ユーザーが追加されるとどうなるのかを説明しています。

Samba

‘ この章は新しい **Samba サーバー設定ツール**が追加されています。

プリンタの設定

‘ この章は**プリンタ設定ツール**の新しいインターフェイス、新**GNOME Print Manager**、パネル上の新しいドラッグアンドドロッププリンタアイコン、などを解説するため書き直されました。

キックスタート

‘ キックスタートの新しいオプションがRed Hat Linux 9に追加され更新しています。また、**Kickstart Configurator**の章に新しい機能がいくつか追加され更新しています。

ネットワーク設定

‘ この章は**ネットワーク管理ツール**の最新インターフェースと機能を解説するために更新されています。

時刻と日付の設定

‘ この章は*Red Hat Linux* 入門ガイドへ移動しています。

2. 表記方法

本マニュアルを読むと、特定の単語が、異なるフォント、書体、サイズ、太さで表記されていることにお気づきになるはずです。この強調表示は規則にしたがって行われています。異なる単語であっても、同じスタイルで表記されている場合は、特定のカテゴリに含まれることを示しています。この様に表記されている単語のタイプには次のような物があります：

`command`

‘ Linux コマンド(場合によっては、その他のオペレーティングシステムコマンド)はこの様に表記します。この様に表記されている場合、その文字列をコマンドラインから入力し、[Enter]キーを押せば、そのコマンドを実行することができます。コマンドの中には、それとは異る表記の部分(例えば、ファイル名)が含まれていることもあります。この場合は、その部分もコマンドの一部であり、全体として1つのコマンドを構成します。例えば：

`cat testfile`コマンドは、現在の作業ディレクトリにある`testfile`という名前のファイルの内容を表示するのに使用します。

`filename`

‘ ファイル名、ディレクトリ名、パス、RPMパッケージ名は、この様に表記します。このスタイルはその名前の特定のファイルやディレクトリがRed Hat Linuxシステム上に存在することを示しています。例えば：

ホームディレクトリの`.bashrc`ファイルには、そのユーザー用のbashシェル定義とエイリアスが保存されています。

`/etc/fstab`ファイルには、各システムデバイスとファイルシステムの情報が保存されています。

Webサーバーのログファイル解析プログラムを使用するためには`webalizer` RPMをインストールしてください。

application

‘ この表記はプログラムがエンドユーザーアプリケーションである(システムソフトウェアではない) ことを示します。例えば：

Mozillaを使用してWebを閲覧します。

[key]

‘ キーボード上のキーは以下のように表記します。例えば：

[Tab]キーによる補完機能を使用するには、1文字入力してから[Tab]キーを押します。端末は、ディレクトリ内のその文字で始まるファイルのリストを表示します。

[key]-[combination]

‘ キーの組み合わせは、次のように表記されます。例えば：

[Ctrl]-[Alt]-[Backspace] キーの組合せはグラフィカル操作を終了させて、グラフィカルログイン画面、又は、コンソールに戻します。

GUI インターフェイス上にあるテキスト

‘ GUIの画面やウィンドウ上に使われる見出しや文字列は、次の様に表記します。この様に表記されている場合、それは特定のGUI画面か、そこにある特定の項目を指す為に使われています。(チェックボックスやフィールドに付けられた文字列など) 例えば：

スクリーンセーバーを停止するときにパスワードを要求するようにしたいときは**パスワードを要求**チェックボックスを選択します。

GUI画面、又はウィンドウ上のメニュー上部

‘ この表記がある時は、それがプルダウンメニューの最上位の項目だということを表します。GUI画面上にあるその文字列をクリックすると、そのメニューの残りが表示されます。例えば：

GNOMEターミナル上の**ファイル**の下に、同じウィンドウ内に複数のシェルプロンプトを開くことが出来る**新規タブ**オプションがあります。

GUIメニューを連続して操作する必要があるときは、次の例のように表記します：

(パネル上の)**メインメニューボタン**=> **プログラム** => **Emacs**と進んで**Emacs**テキストエディタを開始します。

GUI画面、又はウィンドウ上のボタン

‘ この表記は、GUI画面上にクリックできるボタン上にテキストがあることを示します。例えば：

戻る ボタンを押して、最後に表示したウェブページに戻ります。

`computer output`

‘ この表記のテキストがある場合、それはコマンドライン上でコンピュータが表示するテキストを示します。コマンドを入力した結果や、エラーメッセージ、及びスクリプトやプログラムへのユーザー入力の為の対話式プロンプトなど、この表記になります。例えば：

`ls`コマンドを使用してディレクトリの内容を表示します：

```
$ ls
Desktop       about.html   logs    paulwesterberg.png
Mail        backupfiles   mail    reports
```

コマンドの実行結果として表示される出力(この場合は、ディレクトリの内容)は、上記の様に表示されます。

`prompt`

‘ コンピュータが入力待ちであることを示すプロンプトは、この表記で示されます。例えば：

```
$
#
[stephen@maturin stephen]$
leopard login:
```

`user input`

‘ コマンドラインかGUI画面上のテキストボックスにユーザーが入力しなければならない文字列は、このように表記します。次の例では、**`text`**がこの表記で示されています：

システムでテキストベースのインストールプログラムに起動するには、`boot:` プロンプトで、**`text`**と入力する必要があります。

さらには、特定の情報について、ユーザーの注意を引くために幾つかの特策があります。システムに対する重要度に応じて、これらの項目は、ヒント、注意、重要、用心、警告と区分されています。例えば：

注意

Linuxは、大文字/小文字を区別します。つまりROSEとrOsEは異なります。

ヒント

`/usr/share/doc`ディレクトリには、システムにインストールされているパッケージの為の追加のドキュメントが含まれています。

重要

DHCP設定ファイルを変更する場合は、その変更はDHCPデーモンを再起動するまで、有効になりません。

用心

日常の操作はrootで実行しないで下さい。—システム管理の作業に、rootアカウントで操作をする必要があるとき以外は、通常のユーザーアカウントを使用して下さい。


警告

手動でパーティション設定を行わない場合、サーバーシステムインストールを実行すると、インストール先のハードディスクドライブ上にある既存のパーティションはすべて削除されます。保存する必要のあるデータがないことが確実である場合以外は、このインストールクラスは選択しないでください。

3. 今後の発行予定

Red Hat Linux カスタマイズガイドは、Red Hat Linuxユーザーに有益でタイムリーなサポートを提供をするというRed Hatのコミットメントの一環です。今後も、新しいツールやアプリケーションのリリースに合わせて、その内容をガイドに追加し詳述していきます。

3.1. フィードバック

Red Hat Linux カスタマイズガイドに誤植があった場合や、このガイドに関して改善のご意見などあれば、ぜひご連絡ください。`rhl-cg`に関するレポートとしてBugzilla(http://bugzilla.redhat.com/bugzilla/)に提出をお願いします。

本ガイドのIDを忘れず明記していただくようお願いします。

```
rhl-cg(JA)-9-Print-RHI(2003-02-20T01:08)
```

このIDにより、お手持ちのガイドの正確なバージョンを確認することができます。

改善策をお寄せいただく場合には、できるだけ具体的にお知らせください。ガイドの誤りについては、早急に発見できるよう、章及びセクションの番号、前後の文章を添えてお知らせください。

4. サポートを受ける為のユーザー登録

Red Hat Linux 9のエディションのいずれかをお持ちの場合は、忘れずに登録をして、Red Hatの登録ユーザーとしての特典をご利用ください。

購入されたRed Hat Linux製品の種類にしたがって、以下の特典のいくつか、またはすべてをご利用いただけます :

- Red Hat サポート— インストール時の疑問について、Red Hat, Inc.のサポートチームからのサポートが受けられます。
- Red Hat ネットワーク— 簡単にパッケージをアップデートしたり、お使いのシステム用にカスタマイズされたセキュリティ通知を受けることができます。詳細については、http://rhn.redhat.com を参照してください。
- *Under the Brim: The Red Hat E-Newsletter* — 毎月、最新のニュースと製品情報が直接Red Hatから送信されます。

ユーザー登録をするには、http://www.redhat.com/apps/activate/にアクセスして下さい。登録時に使用する製品番号(Product ID)は、Red Hat Linuxボックスの黒と赤と白のカードに記載されています。

Red Hat Linuxの技術サポートについては、*Red Hat Linux* インストールガイドの付録のテクニカルサポートのご利用方法を参照してください。

最後になりましたが、Red Hat Linuxをお選びいただきありがとうございました。

*Red Hat*ドキュメンテーションチーム—同

I. ファイルシステム

ファイルシステムとはコンピュータ上に保存されるファイル及びディレクトリを指します。ファイルシステムはファイルシステムタイプと呼ばれる異なった複数の形式をとることができます。この形式は、情報がファイルまたはディレクトリとしてどのように保存されるかを決定します。冗長性を持つデータのコピーを保存するファイルシステムもあれば、ハードドライブへのアクセスが速いファイルシステムもあります。ここではext3、swap、RAID、LVM のそれぞれのファイルシステムについて説明します。また、パーティションを管理するのに使用するユーティリティ`parted` についても説明します。

目次

第1章

ext3 ファイルシステム

デフォルトのファイルシステムはRed Hat Linux 7.2のリリースから開始され、古くなったext2形式からジャーナリング機能の*ext3*ファイルシステムに変更されました。

1.1. ext3の機能

ext3 ファイルシステムは、根本的にはext2ファイルシステムの強化版です。次のような改善がなされています。

回復力

‘ 予期せぬ停電やシステムクラッシュ(異常なシステム終了とも言います) などの後で、マシン上にマウントされているext2はそれぞれ`e2fsck` プログラムで一貫性のテストをする必要がありました。これが時間のかかるプロセスで特に大量のファイルを抱える大規模のボリュームにとっては、非常に起動時間が遅れる状態でした。この待ち時間の間はボリューム内のデータはどれも使用できない状態でした。

ext3 ファイルシステムに装備されているジャーナリングは、異常システム終了の後でも、上記の様なファイルシステムチェックがもう必要ないという意味を持ちます。唯一、ext3ファイルシステム使用中に一貫性テストが必要になる可能性があるのは、ハードディスク故障などの稀なハードウェア問題の場合です。異常システム終了後のext3ファイルシステムの回復時間は、ファイルシステムのサイズやファイルの数に左右されるのではなく、むしろ一貫性を管理するジャーナルのサイズに影響されます。ハードウェアの速度にもよりますが、デフォルトのジャーナルサイズは回復するのに約1秒かかるだけです。

データの保全性

‘ ext3ファイルシステムは異常システム終了が発生した場合でも、より強健なデータ保全性を提供します。ext3ファイルシステムを使用すると、データ保護のタイプとレベルが選択できます。デフォルトでは、Red Hat Linux 9 はファイルシステムの状態を重んじてext3 ボリュームを設定して、データ一貫性を高レベルに維持します。

速度

‘ データを数回書き込むのにもかかわらず、ジャーナリングシステムがハードディスクのヘッドの回転を最適化するため、ほとんどの場合、ext3はext2よりも高いスループットを持ちます。速度を最適化する為に3つのジャーナリングモードを選択できますが、そうすることでデータ保全性とのトレードオフになります。

簡単な移動

‘ ext2からext3への移動は簡単で、再フォーマットの必要なく強固なジャーナリングファイルシステムの特典を得ることができます。この操作の詳細については項1.3を御覧下さい。

新しくRed Hat Linux 9をインストールする場合は、システムのLinux パーティションに割り当てられるデフォルトのファイルシステムはext3です。ext2パーティションを使用するRed Hat Linuxのあるバージョンからアップグレードしている場合、インストールプログラムが、データを損失することなくそれらのパーティションをext3パーティションに変換してくれます。詳細は*Red Hat Linux* インストールガイドの付録で現在のシステムのアップグレードを御覧下さい。

次のセクションでは、ext3パーティションの作成とチューニングのステップを案内していきます。既にext2パーティションでRed Hat Linux 9を実行している場合、以下のパーティションとフォーマットのセクションは省略して直接、項1.3へ進んで下さい。

1.2. ext3 ファイルシステムの作成

インストール後に、新規のext3ファイルを作成する必要がある場合があります。例えば、Red Hat Linuxシステムに新しいハードドライブを追加した場合、そのドライブのパーティション設定をしたい時に、ext3ファイルシステムを使用します。

ext3ファイルシステムを作成するステップは以下の通りです。

1. `parted`又は`fdisk`を使用してパーティションの作成します。
2. `mkfs`を使用してパーティションをext3ファイルシステムでフォーマットします。
3. `e2label`を使用してパーティションにラベルを付けます。
4. マウントポイントを作成します。
5. パーティションを`/etc/fstab`に追加します。

これらのステップに付いての情報は第5章で参照して下さい。

1.3. ext3ファイルシステムへの変換

`tune2fs`プログラムは、パーティション上のにすでに存在するデータを変更することなく既存のext2ファイルシステムにジャーナル機能を追加します。変換時にファイルシステムがすでにマウントされている場合、ジャーナルはファイルシステムのrootディレクトリ内でファイル`.journal`として見えるようになっています。ファイルシステムがマウントされていない場合、ジャーナルは隠れていて、ファイルシステムには表示されません。

ext2 ファイルシステムからext3へ変換するには、rootでログインして次のようにタイプします：

```
/sbin/tune2fs -j /dev/hdbX
```

上記のコマンドでは、/dev/*hdb*をデバイス名で、そして*X*をパーティション番号で置き換えます。

これが終了したら必ず、`/etc/fstab`内でパーティションタイプをext2からext3へ変更して下さい。

rootファイルシステムを変換している場合、起動するのに`initrd`イメージ(又はラムディスク)が必要になります。これを作成するには、`mkinitrd`プログラムを実行します。`mkinitrd`コマンドの使用法については`man mkinitrd`とタイプしてmanページで確認してください。またGRUB かLILOの設定が`initrd`をロードするようにして下さい。

この変更をしなかった場合、システムはブートしますがファイルシステムは、ext3でなくext2としてマウントされます。

1.4. ext2ファイルシステムへの復元

ext3は比較的に新しい為、幾つかのディスクユーティリティはまだサポートがありません。例えば、`resize2fs`でパーティションを縮小する必要があるとき、これはまだ、ext3をサポートしていません。この状態では、一時的にファイルシステムをext2に復元する必要があります。

パーティションを元に戻す場合、先ず、rootでログインして以下の入力をしてパーティションをアンマウントする必要があります：

```
umount /dev/hdbX
```

上記のコマンドでは、/dev/*hdb*をデバイス名で、また*X*をパーティション番号で置き換えます。このセクションの残りの部分の為に、サンプルのコマンドとしてここでの値は*hdb1*を使用します。

次に、rootで次の入力をしてファイルシステムをext2 に変更します：

```
/sbin/tune2fs -O ^has_journal /dev/hdb1
```

rootとして、以下のコマンドを入力してパーティションのエラーをチェックします：

```
/sbin/e2fsck -y /dev/hdb1
```

そして、以下の入力をしてext2ファイルシステムとしてパーティションをマウントします：

```
mount -t ext2 /dev/hdb1 /mount/point
```

上記のコマンドでは、*/mount/point*をパーティションのマウントポイントで置き換えます。

次に、マウントしているディレクトリへ移動して、パーティションのルートレベルにある.journalファイルを削除するために、次の入力をします：

```
rm -f .journal
```

これでext2 パーティションができました。

パーティションを永久的にext2に変換したい場合、必ず/etc/fstabファイルを更新して下さい。

redhat.

第2章

スワップ領域

2.1. スワップ領域の説明

Linuxの中のスワップ領域は、物理メモリ(RAM)の容量が満杯になった時に使用されるものです。メモリが満杯の時にシステムがもっとメモリリソースを必要とする場合、使用していないメモリのページをスワップ領域に移動します。スワップ領域はマシンを援助する小量のRAMと考えられますが、RAMの代替となるようなものではありません。スワップ領域はハードドライブ内に置かれていて、物理メモリよりもアクセス速度は低下します。

スワップ領域は、専用のスワップパーティション(推奨)、スワップファイル、或は、スワップパーティションとスワップファイルの組合せのどれかであることが出来ます。

スワップ領域の容量は、コンピュータのRAM容量の同等から2倍までの間、あるいは32 MBのどちらか大きい方を選択します。しかし2048 MB(2 GB)以上には出来ません。

2.2. スワップ領域の追加

時には、インストールした後にスワップ領域を増加する必要がでてきます。例えば、RAMの容量を64 MBから128 MBにアップグレードした場合、スワップ領域はそのままでは128 MBしかありません。メモリ使用の多い操作をしたり、大容量メモリを要求するアプリケーションを実行したりする時は、スワップ領域を256 MBまで増加するほうが有利になります。

それには2つのオプションがあります。スワップパーティションを追加するか、またはスワップファイルを追加するかです。スワップパーティションの追加が推奨されますが、空き領域がない場合はそれは簡単にはできません。

スワップパーティションを追加(`/dev/hdb2`を、追加したいスワップパーティションと想定)するには、次の方法で実行します。

1. ハードドライブが使用中であってはいけません(パーティションはマウントされていない状態で、スワップスペースは無効でなければなりません)。これを達成するのに最も簡単な方法は、レスキューモードでシステムをブートすることです。レスキューモードでのブートの仕方は第9章で御覧下さい。ファイルシステムをマウントするように要求された時には、**Skip**を選択します。

   別の方法として、そのドライブが使用中のパーティションを含んでいない場合、それをアンマウントして、`swapoff`コマンドを使用してハードドライブ上の全てのスワップ領域を止めます。

2. `parted`又は`fdisk`を使用して、スワップ領域を作成します。`parted`を使用する方が`fdisk`より簡単ですので、ここでは`parted`のみ説明します。`parted`でスワップ領域を作成するには、次のようにします:

   - シェルプロンプトでrootとして、コマンド`parted /dev/`*`hdb`*をタイプします。ここで/dev/*hdb*は、空き領域を持つハードドライブのデバイス名です。
   - `(parted)`プロンプトで、**`print`**とタイプして、現在のパーティションと空き領域のサイズを表示します。開始と終了の値はメガバイトで表示しています。ハードドライブ上の空き領域を判定し、新しいスワップパーティションに割り当てる容量を決定します。
   - `(parted)`プロンプトで、**`mkpartfs`** ***`part-type`*** **`linux-swap`** ***`startend`***を入力します。ここで、***`part-type`***はプライマリか、拡張か、論理のどれか1つであり、***`start`***とは、パーティションの開始点で、***`end`***とはパーティションの終了点を示します。


警告

変更はすぐに反映されます。注意して正しく入力して下さい。

- **quit**とタイプしてpartedを終了します。

3. これでスワップパーティションが出来ました。コマンドmkswapを使用してスワップパーティションを設定します。rootとして、シェルプロンプトで次を入力します。
   ```
   mkswap /dev/hdb2
   ```
4. すぐにスワップパーティションを有効にするために、次のコマンドをタイプします。
   ```
   swapon /dev/hdb2
   ```
5. ブート時に有効になるように、以下を含むようにして/etc/fstabを編集します：
   ```
   /dev/hdb2      swap          swap   defaults   0 0
   ```
   次にシステムがブートする時には、新しいスワップパーティションが有効になります。
6. 新しいスワップパーティションを追加して有効にした後は、コマンドcat /proc/swaps又は、freeの出力を表示してそれが有効になっていることを確認します。

スワップファイルを追加するには次の方法で実行します。

1. 新しいスワップファイルの容量を判定し、その数値に1024を掛けてブロックサイズを決定します。例えば、64 MBのスワップファイルのブロックサイズは65536となります。
2. シェルプロンプトでrootとして、countが希望のブロックサイズと同じになるようにして次のコマンドを入力します。
   ```
   dd if=/dev/zero of=/swapfile bs=1024 count=65536
   ```
3. 次のコマンドでスワップファイルを設定します：
   ```
   mkswap /swapfile
   ```
4. すぐにスワップファイルを有効にする為に(ブート時に自動的にではない)、次をタイプします。
   ```
   swapon /swapfile
   ```
5. ブート時に有効になるように、以下を含むようにして/etc/fstabを編集します。
   ```
   /swapfile      swap          swap  defaults    0 0
   ```
   次にシステムがブートする時には、新しいスワップファイルが有効になります。
6. 新しいスワップファイルを追加して、有効にした後は、コマンドcat /proc/swaps又はfreeの出力を表示して、それが有効になっていることを確認します。

2.3. スワップ領域の削除

スワップ領域を削除するには次の方法で実行します：

1. ハードドライブが使用中であってはいけません(パーティションはマウントされていない状態で、スワップスペースは無効でなければなりません)。これを達成するのに最も簡単な方法は、レスキューモードでシステムをブートすることです。レスキューモードでのブートの仕方は第9章で御覧下さい。ファイルシステムをマウントするように要求された時には、**Skip**を選択します。

   別の方法として、そのドライブが使用中のパーティションを含んでいない場合、それをアンマウントして、swapoffコマンドを使用してハードドライブ上の全てのスワップ領域を止めます。
2. シェルプロンプトでrootとして、次のコマンドを実行し、スワップパーティションが無効になっていることを確認します。(/dev/hdb2はスワップパーティションとします。)
   ```
   swapoff /dev/hdb2
   ```
3. /etc/fstabからそのエントリを削除します。

4. parted又はfdiskを使用して、パーティションを削除します。ここではpartedについてのみ説明します。partedでパーティションを削除するには、次の様にします：
   - シェルプロンプトでrootとして、コマンドparted /dev/*hdb*をタイプします。ここで/dev/*hdb*は、削除されるスワップ領域を持つハードドライブのデバイス名です。
   - (parted)プロンプトで、**print**とタイプして既存のパーティションを表示し、削除したいスワップパーティションのマイナー番号を確認します。
   - (parted) プロンプトで、**rm*MINOR***を入力します。ここで*MINOR*とは、削除するパーティションのマイナー番号です。

      **警告**

     変更はすぐに反映されます。注意して正しいマイナー番号を入力して下さい。
   - **quit**とタイプして、partedを終了します。

スワップファイルを削除するには次の方法で実行します：

1. シェルプロンプトでrootとして、次のコマンドを実行してスワップファイルを無効にします。(ここで、/swapfileはスワップファイルのことです)。
   ```
   swapoff /swapfile
   ```
2. /etc/fstabからそのエントリを削除します。
3. 次のコマンドで実際のファイルを削除します：
   ```
   rm /swapfile
   ```

2.4. スワップ領域の移動

1つの場所から次の場所へスワップ領域を移動するには、スワップ領域の削除の方法に従います。その後、スワップ領域の追加の方法で新しい場所に追加します。

redhat.

第3章

RAID (Redundant Array of Independent Disks)

3.1. RAIDとは

RAID（Redundant Array of Independent Disks）の基本的な概念は、小容量で安価なディスクドライブをいくつか結合してアレイ（配列）を形成し、大容量かつ高価なドライブでも1台では達成できない性能や冗長性を引き出すというものです。このようなドライブのアレイは、コンピュータからは単一の論理記憶装置またはドライブとして見えます。

RAIDは、ディスクストライピング（RAIDレベル0）、ディスクミラーリング（RAIDレベル1）、パリティ付きディスクストライピング（RAIDレベル5）と呼ばれる技術を使用し、複数のディスクにわたって情報を展開することでディスク読み書きに関する冗長性、低遅延、広帯域幅を実現し、ハードディスククラッシュ時の回復可能性を最大限にする手法のことをいいます。

RAIDの根本にある概念は、一貫した方式で、アレイに属する各ドライブにデータを分散させるということです。そのためには、まずデータを一定サイズの塊(32Kまたは64Kが多いが、その他のサイズも使用可能)に分割します。これらの塊は、使用されているRAIDのレベルに従ってRAIDのハードディスクドライブに書き込まれます。データの読み込み時はこのプロセスが逆になり、複数ドライブが実際に1台の大容量ドライブであるかのような錯覚を与えます。

3.2. RAIDを使用すべきユーザーとは

大量のデータを手元に保持する必要のあるユーザー（たとえばシステム管理者）には、RAID技術を利用するメリットがあります。RAIDを使用するおもな理由として、次のものがあります：

- 高速化
- 単一の仮想ディスクを使用することによる記憶容量の増加
- ディスククラッシュによる影響の低減

3.3. ハードウェアRAIDとソフトウェアRAID

RAIDのアプローチには、ハードウェアRAIDとソフトウェアRAIDの2つがあります。

3.3.1. ハードウェアRAID

ハードウェアベースのRAIDシステムは、RAIDサブシステムをホストから独立したものとして管理します。ホストに、各RAIDアレイ毎に単一のディスクを提供します。

ハードウェアRAIDデバイスの例としては、SCSIコントローラに接続して、RAIDアレイ群を単独のSCSIドライブのようして提供するデバイスです。外部RAIDシステムは、RAIDの処理機能をすべて外部ディスクサブシステムに存在するコントローラに移します。サブシステム全体が通常のSCSIコントローラを介してホストに接続されるため、ホストからは単一のディスクのように見えます。

RAIDコントローラもカードの形をしており、オペレーティングシステムに対するSCSIコントローラのような役割を果たしますが、ドライブとの実際の通信はすべて自分自身で処理します。この場合、ドライブはSCSIコントローラの場合と同様にRAIDコントローラに接続されますが、ドライブはRAIDコントローラの設定に追加されるため、オペレーティングシステムからは違いを認識することはできません。

3.3.2. ソフトウェアRAID

ソフトウェアRAIDは、カーネルディスク(ブロックデバイス)コードでさまざまなRAIDレベルを実装します。これは低価格のソリューションを提供しますので高額なディスク制御カード又は、ホットスワップシャーシ[1] は必要としません。ソフトウェアRAIDは、またSCSIのディスクだけでなく、より低額のIDEのディスクでも機能します。最近の高速CPUを使用すれば、ソフトウェアRAIDの性能はハードウェアRAIDに勝る可能性もあります。

Linuxカーネルに含まれるMDドライバはRAIDソリューションの一例であり、ハードウェアから完全に独立しています。ソフトウェアベースのアレイの性能は、サーバーCPUの性能と負荷に依存します。

Red Hat Linuxインストーレーションプログラムでのソフトウェアの設定については、第10章を参照してください。

ソフトウェアRAIDで実現可能な機能についてさらに詳しく知りたい場合は、以下の重要な機能に注目してください：

- スレッド化された再構築プロセス
- カーネルに基づいた構成
- 再構築せずにLinuxマシン間でアレイを移動可能
- アイドル状態のシステム資源を使用する、バックグラウンドでのアレイ再構築
- ホットスワップ可能なドライブをサポート
- 自動CPU検出により、特定のCPU最適化機能を利用

3.4. RAIDレベルとリニアのサポート

RAIDは、レベル0、1、4、5、リニアなど、さまざまな設定をサポートします。これらのRAIDタイプの定義は以下のとおりです：

- レベル*0*—「ストライピング」とも呼ばれますが、性能を重視した分割データマッピング技術です。つまり、アレイに書き込まれるデータは複数のストライプに分割され、アレイの各メンバーディスクに書き込まれます。このようにして低コストで高い入出力性能が得られますが、冗長性はありません。レベル0アレイの記憶容量は、ハードウェアRAIDのメンバーディスクの総容量またはソフトウェアRAIDのメンバーパーティションの総容量に等しくなります。
- レベル*1*—RAIDレベル1、または「ミラーリング」は、RAIDの形式として最も古くから使用されているものです。レベル1では、冗長性を実現するためにアレイの各メンバーディスクに同じデータを書き込み、各ディスクに「鏡に映したような」コピーを残します。ミラーリングは、その単純さと高いデータ安全性により人気を保っています。レベル1は2台以上のディスクに対して機能するため、読み込み時には並列アクセスを行うことでデータ転送レートの向上を図りますが、入出力トランザクションレートを向上させるために独立して動作するのが一般的です。レベル1ではデータ信頼性が非常に高く、読み込み中心のアプリケーションでの処理速度は向上しますが、コストは比較的高くなります。[2] レベル1のアレイの記憶容量は、ハードウェアRAIDのミラーリングされたハードディスクの1台またはソフトウェアRAIDのミラーリングされたパーティション1つの容量に等しくなります。

---

1. ホットスワップシャーシを使用すると、システムの電源を落さずにハードドライブを取り外すことが出来ます。
2. RAID 1のコストが高くなるのは、アレイに属するすべてのディスクに同じ情報を書き込むため、ドライブの領域を消費するからです。たとえば、ルート（/）パーティションが2台の40Gバイトドライブに存在するようにRAIDレベル1をセットアップした場合、物理的な領域の合計は80Gバイトですが、この80Gバイトのうち、アクセスできるのは40Gバイト分だけです。ほかの40Gバイトは最初の40Gバイトのミラーとなります。

- レベル*4*—RAID 4では、1台のディスクに集められたパリティ[3]を使用してデータを保護します。この方法は、大きいファイルの転送よりも入出力のトランザクションに適しています。パリティ専用のディスクには本質的にボトルネックが存在するため、ライトバックキャッシュなどの技術を併用せずに使用されることはほとんどありません。一部のRAIDパーティション方式ではRAIDレベル4もオプションの1つですが、Red Hat LinuxのRAIDインストールではオプション選択できません。[4] ハードウェアRAIDレベル4の記憶容量は、メンバーディスクの総容量からメンバーディスク1台の容量を差し引いたものと等しくなります。ソフトウェアRAIDレベル4の記憶容量は、メンバーパーティションの総容量からパーティション1つのサイズを差し引いたものと等しくなります（パーティションのサイズが同一である場合）。
- レベル*5* —最も一般的なRAIDのタイプです。アレイに属するメンバードライブディスクの一部または全部にパリティ情報を分散することによって、レベル4固有の書き込み時ボトルネックの問題が解消されています。唯一の性能上のボトルネックは、パリティ計算プロセスです。最近のCPUとソフトウェアRAIDを使用した場合、通常それほど大きな問題にはなりません。レベル4と同様、結果として性能に偏りがあり、読み込み速度が書き込み速度を大幅に上回ります。この偏りを緩和するため、レベル5では多くの場合ライトバックキャッシュが併用されます。ハードウェアRAIDレベル5の記憶容量は、メンバーディスクの総容量からメンバーディスク1台の容量を差し引いたものと等しくなります。ソフトウェアRAIDレベル5の記憶容量は、メンバーパーティションの総容量からパーティション1つのサイズを差し引いたものと等しくなります（パーティションのサイズが同一である場合）。
- リニア*RAID*—リニアRAIDは、ドライブを単純にグループ化して1台の大容量仮想ドライブを作成するものです。リニアRAIDでは、塊は1台のメンバードライブから順に割り当てられ、最初のドライブが完全に一杯になると割り当て対象は次のドライブへ移ります。このようなグループ化では、入出力操作がメンバードライブ間で分割されることはないため、性能上のメリットはありません。リニアRAIDでは冗長化が行われないため、実際には信頼性は低くなります。—メンバードライブのいずれかがクラッシュすると、アレイ全体が使用不可能になります。記憶容量は、全メンバーディスクの合計です。

3. パリティ情報は、アレイに属するほかのメンバーディスクの内容に基づいて計算されます。この情報を使用することによって、アレイに属するディスクがクラッシュしたときも、全体のデータを再構築することができます。クラッシュしたディスクが交換されるまでの間、このディスクへの入出力要求に対応するには、再構築されたデータを使用します。再構築されたデータを使用して、交換されたディスクにデータを戻すこともできます。
4. RAIDレベル4で消費される領域の大きさはRAIDレベル5の場合と同じですが、レベル5にはレベル4をしのぐ利点が多数あります。このような理由により、レベル4はサポートされていません。

第4章

LVM (Logical Volume Manager)

Red Hat Linux 8.0から開始された論理ボリュームマネージャ(LVM)はハードドライブ分配の為に利用できます。

LVMはパーティションを変更するのではなく、サイズ変更が簡単にできる論理ボリュームへハードドライブ領域を割り当てる方法です。

LVMでは、ハードドライブ又は、ハードドライブのセットが1つ又はそれ以上の物理ドライブに割り当てられます。物理ボリュームは1つのドライブ以上に広がることは出来ません。

/bootパーティションは例外として、物理ボリュームを集束して論理ボリュームグループにします。ブートローダーは論理ボリュームグループを読み取れない為、/bootパーティションは論理ボリュームグループ上に存在出来ません。ルート/パーティションを論理ボリューム上に配置する場合は、ボリュームグループの一部ではない場所に別の/bootパーティションを作成する必要があります。

物理ボリュームは1つのドライブ以上に広がることは出来ませんので、論理ボリュームグループを1つ以上のドライブに広げたい場合は、ドライブ毎に1つ又はそれ以上の物理ボリュームを作成する必要があります。

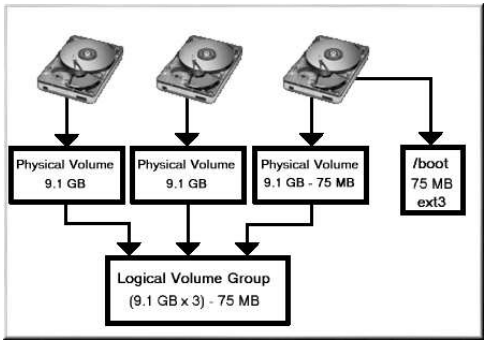


図4-1. 論理ボリュームグループ

論理ボリュームグループは、/home や/のようなマウントポイントに割り当てられる論理ボリュームと、ext3のようなファイルシステムに分けられます。「パーティション」が全容量まで満杯になると、パーティションの容量を増やす為に、論理ボリュームグループの空き領域を論理ボリュームに追加することができます。新しいハードドライブがシステムに追加される時、それは論理ボリュームグループに追加できます。そしてパーティションとして存在する論理ボリュームは拡張することが出来ます。

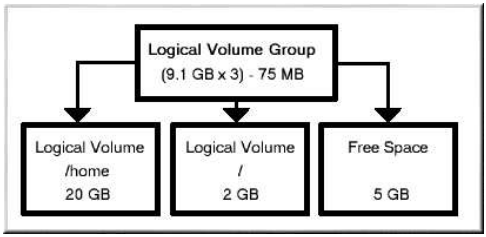


図4-2. 論理ボリューム

その一方、システムがext3ファイルでパーティション設定されていると、ハードドライブは定義されたサイズのパーティションに分けられます。パーティションが満杯になると、パーティションサイズを拡張するのは容易ではありません。パーティションが別のハードドライブに移動された場合でも、元のハードドライブのスペースは別のパーティションとして再分配するか又は使用しないことになります。

LVM サポートはカーネルにコンパイルされる必要があります。Red Hat Linux 9のデフォルトカーネルはLVMサポートでコンパイルしてあります。

Red Hat Linuxインストールプロセス中のLVMの設定の仕方について調べるには第11章を参照して下さい。

redhat.

第5章

ディスク保存の管理

Red Hat Linux システムをインストールした後に、既存のパーティションテーブルを見たり、パーティションのサイズを変更したり、パーティションを削除したり、あるいは空き領域又は追加のハードドライブにパーティションを追加したり、など必要な作業が数多くあります。ユーティリティpartedでこれらのタスクをすべて実行することが出来ます。この章では、コマンドファイルシステムのタスクを実行する為のpartedの使用法を説明します。別の方法として、パーティションサイズ変更以外はこれらのタスクのほとんどを実行できるfdiskの使用があります。fdiskに関する情報はmanページあるいはinfoページでfdiskの項目を参照してください。

システムのディスク領域の使用量を表示したり、モニタしたりしたい場合は、項26.3を参照して下さい。

partedユーティリティを使用するには、partedパッケージをインストールしている必要があります。partedをスタートするには、シェルプロンプトでrootとして、コマンドparted */dev/hdb*をタイプします。ここで*/dev/hdb*は、設定したいドライブのデバイス名です。(parted)プロンプトが表示されます。helpとタイプすると使用可能なコマンドの一覧を表示できます。

パーティションを作成、削除、あるいはサイズ変更などしたい場合、デバイスは使用中であってはいけません。(パーティションはマウントできません。スワップファイルは有効ではいけません。) これを簡単に実現するには、システムをレスキューモードで起動することです。レスキューモードで起動する方法に付いては、第9章を参照して下さい。ファイルシステムをマウントするように要求されたら、**Skip**を選択します。

別の方法として、そのドライブが使用中のパーティションを含んでいない場合、umountコマンドを使用してパーティションをアンマウントして、swapoffコマンドを使用してハードドライブ上の全てのスワップ領域を止めます。

表5-1には、一般的に使用されるpartedコマンドが含まれています。以下に続くセクションでは、それらのコマンドの幾つかをより詳しく説明していきます。

コマンド	説明
check マイナー番号	ファイルシステムに簡単な検査。
cp 転送元 転送先	1つのパーティションから別のパーティションへファイルシステムをコピー。転送元と転送先の部分はそれぞれのパーティションのマイナー番号です。
help	使用可能なコマンドの一覧を表示。
mklabel ラベルの種類	パーティションテーブル用にディスクラベルを作成。
mkfs マイナー番号 ファイルシステムの種類	ファイルシステムの種類タイプのファイルシステムを作成。
mkpart パーティションの種類 ファイルシステムの種類 開始-*mb* 終了-*mb*	パーティションを作成して、新規のファイルシステムは作成しない。
mkpartfs パーティションの種類 ファイルシステムの種類 開始-*mb* 終了-*mb*	パーティションを作成して、指定のファイルシステムを作成。
move マイナー番号 開始-*mb* 終了-*mb*	パーティションを移動。
print	パーティションテーブルを表示。

コマンド	説明
quit	partedを終了。
resize マイナー番号 開始-*mb* 終了-*mb*	パーティションサイズを開始-*mb*から終了-*mb*へ変更。
rm マイナー番号	パーティションを削除
select デバイス	設定するデバイスを別に選択
set マイナー番号 フラグ 状態	パーティションにフラグを設定; 状態はオン又は、オフ。

表5-1. partedのコマンド

5.1. パーティションテーブルの表示

partedを開始した後に、次のコマンドをタイプしてパーティションテーブルを表示します。

```
print
```

以下の様なテーブル(一覧)が表示されます：

```
Disk geometry for /dev/hda: 0.000-9765.492 megabytes
Disk label type: msdos
Minor  Start   End  Type   Filesystem Flags
1    0.031  101.975 primary ext3    boot
2    101.975 611.850 primary linux-swap
3    611.851 760.891 primary ext3
4    760.891 9758.232 extended      lba
5    760.922 9758.232 logical ext3
```

1行目はディスクのサイズを表示します。2行目はディスクのラベルタイプを示し、残りの行でパーティションテーブルの出力を表示します。パーティションテーブルの中では、**マイナー**番号がパーティション番号です。例えば、マイナー番号1を持つパーティションは/dev/hda1に相当します。**開始**と**終了**の値はメガバイトです。**種類**はプライマリ、拡張、論理のどれか1つになります。**ファイルシステム**はファイルシステムタイプであり、これはext2, ext3, FAT, hfs, jfs, linux-swap, ntfs,reiserfs, hp-ufs, sun-ufs, xfsの内のどれか1つになります。**フラグ**の列では、パーティションに設定してあるフラグが表示されます。使用できるフラグはboot, root、swap, hidden, raid, lvm, lbaとなります。

ヒント

partedを再起動せずに別のデバイスを選択するには、selectコマンドの後ろに/dev/hdbなどのデバイス名を付けて実行します。そうするとそのパーティションテーブルの表示や設定が出来るようになります。

5.2. パーティションの作成

警告

使用中のデバイス上ではパーティションの作成をしないで下さい。

パーティションを作成する前に、レスキューモードで起動します。(或は、デバイス上のどのパーティションもアンマウントして、デバイス上のすべてのスワップ領域を止めます)

`parted`をスタートします。ここで、/dev/*hda*はパーティションを作成するデバイス名です。

```
parted /dev/hda
```

現在のパーティションテーブルを表示して、十分な空き領域があるかどうか判定します。

```
print
```

十分な空き領域がない場合、既存のパーティションのサイズを変更することができます。詳細については、項5.4を参照して下さい。

5.2.1. パーティションの構築

パーティションテーブルから新規パーティションの開始点と終了点、及びパーティションタイプを決定します。1つのデバイス上ではプライマリパーティション(基本区画)は4つまでしか作れません。(拡張パーティションがない場合)。4つ以上のパーティションが必要な場合は、3つのプライマリと1つの拡張パーティションを構築し、拡張の中に複数の論理パーティションを含むことが出来ます。ディスクパーティションの概要については、*Red Hat Linux* インストールガイド内の付録にあるディスクパーティションの概要を参照して下さい。

例えば、ハードディスク上の1024メガバイトから2048メガバイトまでをext3ファイルシステムでプライマリパーティションにするには、次のコマンドをタイプします。

```
mkpart primary ext3 1024 2048
```

ヒント

代わりに`mkpartfs`コマンドを使用すると、パーティションが作成された後にファイルシステムが作成されます。しかし`parted`ではext3ファイルシステムの作成はサポートしていません。ext3ファイルシステムを作成したい場合は、`mkpart`を使用し、さらに後で説明があるように`mkfs`コマンドでファイルシステムを作成します。`mkpartfs`はファイルシステムのタイプlinux-swap用には対応します。

変更は[Enter]キーを押した時点で反映されます。ですから実行する前にコマンドを良く確認してください。

パーティションを作成した後で、`print`コマンドを使用してパーティションテーブルの中で正しいパーティションタイプ、ファイルシステムタイプ、及び、サイズになっていることを確認します。またラベルを付けることが出来るように新規パーティションのマイナー番号も記録しておきます。さらに以下の出力も表示すべきです。

```
cat /proc/partitions
```

これでカーネルが新規パーティションを認識することが確実になります。

5.2.2. パーティションのフォーマット

パーティションはまだ、ファイルシステムを持っていません。以下のようにしてファイルシステムを作成します：

```
/sbin/mkfs -t ext3 /dev/hdb3
```


警告

パーティションをフォーマットすると、パーティション上に存在するすべてのデータが永久に消滅します。

5.2.3. パーティションのラベル作成

次に、パーティションにラベルを与えます。例えば、新規パーティションが/dev/hda3で、/workとラベルを付けたい場合は、次のようにします：

```
e2label /dev/hda3 /work
```

デフォルトで、Red Hat Linux インストールプログラムは、ユニークで間違いのない様にパーティションのマウントポイントをラベルとして使用します。しかしユーザーの好みのラベルを使うことが出来ます。

5.2.4. マウントポイントの作成

rootとして以下の操作でマウントポイントを作成します：

```
mkdir /work
```

5.2.5. /etc/fstabへ追加

rootとして、/etc/fstabファイルを編集して新規パーティションを含む様にします。新しい行は以下に似た状態になります。

```
LABEL=/work    /work        ext3  defaults   1 2
```

1番目の列ではLABEL=に続いて、パーティションに付けたラベル名が来ます。2番目の列では新規パーティションのマウントポイント、次の列がファイルシステムタイプ(例えばext3 やswap)となります。フォーマットについてもっと情報が必要な場合は、コマンドman fstabをタイプしてそのmanページを御覧下さい。

4番目の列には、defaultsという言葉があります。このパーティションはブート時にマウントされます。パーティションを再起動せずにマウントするには、rootとして次のコマンドをタイプします：

```
mount /work
```

5.3. パーティションの削除


警告

使用中のデバイス上のパーティションは削除しないで下さい。

パーティションを削除する前にレスキューモードで起動します。(又は、デバイス上のどのパーティションもアンマウントし、デバイス上のどのスワップ領域も停止します。)

partedをスタートします。ここで、/dev/*hda*はパーティションを作成するデバイス名です。

```
parted /dev/hda
```

現在のパーティションテーブルを表示して削除するパーティションのマイナー番号を決定します：

```
print
```

rmコマンドを使用してパーティションを削除します。例えば、マイナー番号3のパーティションを削除するには、次の入力をします：

```
rm 3
```

変更は[Enter]キーを押すとすぐに反映されます。実行する前にコマンドを再確認して下さい。

パーティションを削除した後は、printコマンドを使用してパーティションテーブルから削除されていることを確認します。また、次の出力も表示すべきです。

```
cat /proc/partitions
```

これでカーネルが、パーティションは削除されたと認識することを確実にします。

最後のステップは/etc/fstabファイルからそれを削除することです。削除されたパーティションを表明している行を見付けて、ファイルからそれを削除します。

5.4. パーティションのサイズ変更

警告

使用中のデバイス上のパーティションのサイズ変更はしないで下さい。

パーティションのサイズ変更の前に、レスキューモードで起動します。(又は、デバイス上のどんなパーティションでもアンマウントして、デバイス上のどのスワップ領域も止めます。)

partedをスタートします。ここで、/dev/*hda*はパーティションをサイズ変更するデバイス名です。

```
parted /dev/hda
```

現在のパーティションテーブルを表示してサイズ変更するパーティションのマイナー番号、及びそのパーティションの開始点と終了点を確認します。

```
print
```

警告

サイズ変更をするパーティションの使用済サイズは、新しいサイズより大きい値であってはいけません。

パーティションのサイズを変更するには、resizeコマンドの後ろにパーティションのマイナー番号、開始点と終了点をメガバイトで付けて実行します。例えば、次のようにします。

```
resize 3 1024 2048
```

パーティションのサイズ変更が終了すると、printコマンドでそのパーティションのサイズが正しく変更されたか、正しいパーティションタイプか、正しいファイルシステムタイプかを確認します。

システムをノーマルモードで再起動して、コマンドdfの使用でパーティションがマウントされているか、新しいサイズが認識されているかを確認します。

redhat.

第6章

ディスク容量制限の実践

システム上で使用されるディスク容量をモニタすることに加えて(項26.3.1を参照)、ディスク容量はディスク容量制限を実践することにより規制することが可能で、これによりシステム管理者はあるユーザーがディスク容量を使い過ぎる前に、又はパーティションの1つが満杯になる前に警報を受けることができます。

ディスク容量制限は、個別のユーザーにもユーザーグループにも設定できます。このような柔軟性が各ユーザーには、個人ファイル(メールやレポート)を処理する為の小さな容量制限を与え、それと同時に彼らが担当するプロジェクトにはかなりのサイズの容量制限(そのグループにプロジェクトを与えると想定)を与えることを可能にします。

さらに、容量制限は使用されるディスクブロックの数量を制御する為だけでなくiノードの数量も制御します。iノードはファイル関連の情報を収納する為に使用されますので、それが、作成出来るファイルの数量を制御します。

ディスクの容量制限を実践するためには、quota RPMがインストールされている必要があります。RPMパッケージのインストールについての詳細は、パートVを参照してください。

6.1. ディスク容量制限の設定

ディスク容量制限を実践するには次のステップを使用します：

1. /etc/fstabを修正してファイルシステム単位の容量制限を有効にする
2. ファイルシステムを再マウントする
3. 容量制限ファイルを作成し、ディスク使用テーブルを生成する
4. 容量制限を割り当てる

これらの各ステップは、以下のセクションで詳しく説明されます。

6.1.1. 容量制限を有効にする

rootとして、好みのテキストエディタを使用して、容量制限を必要とするファイルシステムにusrquotaとgrpquotaのどちらか、又は両方のオプションを追加します：

```
LABEL=/     /       ext3  defaults    1 1
LABEL=/boot   /boot     ext3  defaults    1 2
none      /dev/pts    devpts gid=5,mode=620 0 0
LABEL=/home   /home     ext3  defaults,usrquota,grpquota 1 2
none      /proc     proc  defaults    0 0
none      /dev/shm    tmpfs defaults    0 0
/dev/hda2    swap      swap  defaults    0 0
/dev/cdrom    /mnt/cdrom   udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0    /mnt/floppy   auto  noauto,owner,kudzu 0 0
```

この例では、/homeファイルシステムでユーザーとグループの両方の容量制限が有効になっています。

6.1.2. ファイルシステムの再マウント

userquotaとgrpquotaのオプションを追加した後、fstabのエントリが修正されている各ファイルシステムを再マウントします。ファイルシステムがプロセスによって使用中でない場合は、umountコマンドを使用し、その後mount コマンドを使用してファイルシステムを再マウントします。ファイルシステムが現在使用中であれば、最も簡単にファイルシステムを再マウントする手段は、システムの再起動です。

6.1.3. 容量制限ファイルの作成

それぞれの容量制限が有効になったファイルシステムが再マウントされた後には、システムは、ディスク容量制限で動作する状態です。しかし、ファイルシステム自身はまだ容量制限をサポートする準備が出来ていません。次のステップでquotacheckコマンドを実行します。

quotacheckコマンドは容量制限が有効になったファイルシステムを検査して、ファイルシステム毎に現在のディスク使用量のテーブルを構成します。このテーブルはその後オペレーティングシステムのディスク使用量のコピーを更新するのに使用されます。さらにファイルシステムのディスク容量制限ファイルが更新されます。

ファイルシステム上で容量制限ファイル(aquota.userとaquota.group)を作成するには、quotacheckコマンドの-cオプションを使用します。例えば、/homeパーティション用にユーザーとグループの容量制限が有効な場合、/homeディレクトリの中にそのファイルを作成します：

```
quotacheck -acug /home
```

-aオプションは、容量制限が有効かどうか調べる為に、/etc/mtab内のマウントされている非-NFSファイルが全てチェックされると言う意味です。-cオプションは、容量制限が有効な各ファイルシステムの為に容量制限ファイルが作成される様に指定します。-uは、ユーザー容量制限のチェックを指定し、-gオプションはグループ容量制限のチェックを指定します。

-uも-gも指定されていない場合、ユーザー容量制限ファイルだけが作成されます。-gだけが指定してある場合は、グループ容量制限ファイルのみが作成されます。

ファイルが作成された後に、次のコマンドを使用して容量制限有効なファイルシステム毎に現在のディスク使用量のテーブルを生成します：

```
quotacheck -avug
```

これらのオプションは次のようになります：

- a — 全ての容量制限有効なローカルマウントのファイルシステムをチェックする
- v — 容量制限のチェックが進むのと共に詳細進行状態を表示する
- u — ユーザーディスク容量制限情報をチェック
- g — グループディスク容量制限情報をチェック

quotacheckの実行が終了した後は、有効な容量制限(ユーザーとグループの両方又は片方)へ対応する容量制限ファイルは、/homeなどのような各容量制限が有効なファイルシステム用にデータで充填されます。

6.1.4. ユーザー単位で容量制限を割り当てる

最後のステップは、edquotaコマンドを使用してディスク容量制限を割り当てることです。

ユーザー1人に容量制限を設定するには、シェルプロンプトでrootとして次のコマンドを実行します：

```
edquota username
```

容量制限を実践したい各ユーザーに対してこのステップを実行します。例えば、容量制限が、/homeパーティション用(/dev/hda3)に/etc/fstabで有効であり、edquota testuserコマンドが実行された場合、システムのデフォルトとして設定されたエディタに以下の様に表示されます：

```
Disk quotas for user testuser (uid 501):
 Filesystem        blocks   soft   hard  inodes  soft  hard
 /dev/hda3         440436    0     0   37418    0    0
```

注意

EDITOR環境変数で定義されているテキストエディタはedquotaで使用されます。このエディタを変更するには、EDITOR環境変数を好みのエディタのフルパス名へ設定します。

1番目の列は、容量制限が有効になっているファイルシステムの名前です。2番目の列は、ユーザーが現在使用しているブロックの数量を示します。その次の2つの列はファイルシステム上のユーザー用にソフトとハードのブロックリミットを設定するために使用されます。inodesの列はユーザーが使用しているiノードの数を表示します。最後の2つの列はファイルシステムのユーザー用にソフトとハードのiノードリミットを設定するのに使用されます。

ハードリミットとは、ユーザー又はグループが使用出来るディスク容量の絶対最大量です。この限度に到達すると、それ以上のディスク容量は使用できません。

ソフトリミットは使用できるディスク領域の最大量を定義するものです。但し、ハードリミットとは違い、ソフトリミットは一定の期間だけその限度を超過できます。この期間は猶予期間と呼ばれるものです。猶予期間は、秒、分、時間、日、週、又は月で表現できます。

いずれかの値が、0に設定されている場合は、その限度は設定されていないことになります。テキストエディタで目的の限度に修正します。例えば：

```
Disk quotas for user testuser (uid 501):
 Filesystem        blocks   soft   hard  inodes  soft  hard
 /dev/hda3         440436  500000  550000  37418    0    0
```

ユーザーの為の容量制限が設定されたことを確証するには次のコマンドを使用します：

```
quota testuser
```

6.1.5. グループ単位で容量制限を割り当てる

容量制限はグループ単位ベースでも割り当てできます。例えば、devel グループ用にグループ容量制限を設定するには、以下のコマンドを使用します(グループ容量制限をする前にグループが存在している必要があります)：

```
edquota -g devel
```

このコマンドはグループ用の既存の容量制限をテキストエディタで表示します：

```
Disk quotas for group devel (gid 505):
 Filesystem        blocks   soft   hard  inodes  soft  hard
 /dev/hda3         440400    0     0   37418    0    0
```

この限度を修正し、ファイルを保存してそれから容量制限を設定します。

グループの容量制限が設定されたことを確証するには次のコマンドを使用します：

```
quota -g devel
```

6.1.6. ファイルシステム単位で容量制限を割り当てる

容量制限が有効な各ファイルシステムを基にして容量制限を割り当てるには、次のコマンドを使用します：

```
edquota -t
```

他のedquotaコマンドと同様に、これもテキストエディタでファイルシステム用の現在の容量制限を開きます：

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
 Filesystem      Block grace period   Inode grace period
 /dev/hda3          7days         7days
```

ブロックの猶予期間、又はiノードの猶予期間を修正して、そのファイルへの変更を保存し、テキストエディタを終了します。

6.2. ディスク容量制限の管理

容量制限が実践された場合、幾らかの保全が必要となります— ほとんどの場合、容量制限が超過していないことを監視することと、容量制限が正確であることを確証する形になります。当然、ユーザーが繰り返し容量制限を超過したり、常時ソフトリミットに到達するのであれば、システム管理者は、ユーザーのタイプとディスク容量が彼らの仕事に与えるインパクト大きさにより、行動する選択肢を幾つか持ちます。管理者は、ユーザーがディスク容量を少なく使用する方法を決定すること、又は必要であればユーザーのディスク容量制限を増加することのどちらかで援助することが出来ます。

6.2.1. ディスク容量制限の報告

ディスク使用量報告を作成するには、repquota ユーティリティの実行が要求されます。例えば、コマンドrepquota /homeは次の出力を作り出します：

```
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
          Block limits       File limits
User     used  soft  hard grace  used soft hard grace
----------------------------------------------------------------------
root   --   36   0   0      4  0  0
tfox   --  540   0   0     125  0  0
testuser -- 440400 500000 550000    37418  0  0
```

全ての容量制限有効なファイルシステムのディスク使用量報告を表示するには、以下のコマンドを使用します：

```
repquota -a
```

報告は簡単に読めますが、数点だけ説明が必要です。各ユーザーの後に表示されている--はブロック又はiノードリミットが超過しているかどうかを素早く判断する手段です。どちらかのソフトリミットが超過している場合、-に相当する部分に+が表示されます。最初の-がブロック限度を示し、2番目の物がiノード限度の為の表示をします。

graceの列は、通常は空白です。ソフトリミットが超過したとき、この列は猶予期間の残り時間に相当する時間指定を持つことになります。もし猶予期間が終了した場合は、代わりにnoneが表示されます。

6.2.2. 容量制限を正確に維持する

ファイルシステムが、正常にアンマウントされていない時(システムクラッシュなどで)はいつも、quotacheckを実行する必要があります。しかし、quotacheckはシステムがクラッシュしていない時でも定期レベルで実行することも出来ます。以下のコマンドを定期的に実行することにより、容量制限をより正確に維持することが出来ます(使用されるオプションは項6.1.1で説明してあります):

```
quotacheck -avug
```

定期的にチェックを実行する最も簡単な方法はcronの使用です。rootとしてcrontab -eコマンドで定期的なquotacheckのスケジュールを作るか、あるいは以下のいずれかのディレクトリでquotacheckを実行するスクリプトを入れます(ユーザーに目的に応じた間隔を使用する):

- /etc/cron.hourly
- /etc/cron.daily
- /etc/cron.weekly
- /etc/cron.monthly

最も正確な容量制限の統計情報は、ファイルシステムが使用中でない状態で解析される時に得られます。その為、cronのタスクはファイルシステムの使用が最も低下する時にスケジュールすべきです。この時間が、容量制限を持つ別々のファイルシステムで異なる場合、複数のcronタスクで別々の時間にそれぞれのファイルシステム用にquotacheckを実行します。

cron設定の詳細情報は第28章で御覧下さい。

6.2.3. 有効化と無効化

容量制限は、0に設定せずに無効にすることも可能です。全てのユーザーとグループの容量制限を停止するには、次のコマンドを使用します:

```
quotaoff -vaug
```

-uと-gのどちらのオプションも指定されていない場合、ユーザー容量制限のみが無効になります。また-gだけが指定されている場合、グループ容量制限のみが無効になります。

再度、容量制限を有効にするには、同じオプションでquotaon コマンドを使用します。

例えば、全てのファイルシステムのユーザーとグループを有効にするには、以下のようにします:

```
quotaon -vaug
```

/homeなどの特定のファイルシステムの容量制限を有効にするには、以下のコマンドを使用します:

```
quotaon -vug /home
```

-u と-gのどちらのオプションも指定されていない場合は、ユーザー容量制限のみが有効になります。-gのみが指定されている場合は、グループ容量制限のみが有効になります。

6.3. その他のリソース

ディスク容量制限に関する詳細情報については、次のリソースを参照して下さい。

6.3.1. インストールされているドキュメント

- `quotacheck`, `edquota`, `repquota`, `quota`, `quotaon`, 及び`quotaoff`のmanページ

6.3.2. 関連書籍

- *Red Hat Linux システムアドミニストレーションプレミア* — これはwebサイトhttp://www.redhat.com/docs とドキュメントCD上で見ることが出来ます。このマニュアルには、新しいRed Hat Linux システム管理者用の記憶管理に関するバックグランド情報(ディスク容量制限を含む)が含まれています。

II. インストール関連の情報

Red Hat Linux インストールガイドでは、Red Hat Linuxのインストールと基本的なインストール後のトラブルシューティングについて説明します。しかし、このガイドには高度なインストールのオプションが含まれます。ここでは、キックスタート (自動インストール技術)、システムのリカバリモード(通常のランレベルでブートしない場合の、システムのブート方法)、インストール中のRAIDの設定方法、インストール中のLVMの設定方法についての説明をしています。これらの高度なインストール作業をするために、*Red Hat Linux* インストールガイド とあわせてこのパートをお使いください。

目次

第7章

キックスタートインストール

7.1. キックスタートインストールとは

システム管理者の多くは、コンピュータにRed Hat Linuxをインストールする手順を自動化したいと考えています。これに応えて、Red Hatはキックスタートインストールを開発しました。Red Hat Linuxのインストールではいくつかの質問に答えなければなりませんが、キックスタートでは、そのすべての答えをあらかじめ1つのファイルに記述しておくことができます。

1つのサーバシステムにキックスタートファイルを置いておき、各コンピュータがインストール時に読み込むことになります。このインストール法なら、1つのキックスタートファイルで複数のコンピュータにRed Hat Linuxをインストールすることができます。ネットワークとシステムの管理者にとっては理想的なインストール方法です。

キックスタートを使用すれば、Red Hat Linuxのインストール手順を自動化することができます。

7.2. キックスタートインストールの実行方法

キックスタートでは、ローカルCD-ROM、ローカルハードドライブ、NFS、FTP、HTTPなどを使ってインストールすることができます。

キックスタートを使用するには、次の操作を実行する必要があります。

1. キックスタートファイルを作成します。
2. キックスタートファイルでブートディスクを作成するか、ネットワークでキックスタートファイルを使用できるようにします。
3. インストールツリーを使用できるようにします。
4. キックスタートインストールを開始します。

本章では、これらのステップを詳細に説明します。

7.3. キックスタートファイルの作成

キックスタートファイルは単純なテキストファイルです。このファイルはそれぞれキーワードで識別される項目の一覧を含んでいます。**キックスタート設定ツール**アプリケーションを使用して、Red Hat LinuxドキュメントCD-ROMの`RH-DOCS`ディレクトリにある`sample.ks`ファイルのコピーを編集してキックスタートファイルを作成することができます。あるいは、最初から作ることもできます。Red Hat Linuxインストールプログラムは、インストール中に選択したオプションに基づいてサンプルのキックスタートファイルも作成します。これは、 `/root/anaconda-ks.cfg`ファイルに書き込まれます。ASCIIテキストとしてファイルを保存できるものなら、どのテキストエディタやワープロを使っても編集することができます。

まず、キックスタートファイルを作るときは、次の点に注意します。

- セクションは決められた順序で指定してください。セクション内の項目は、指定されない限りは特定の順序である必要はありません。セクションの順は次のようになります。
  - コマンドセクション— キックスタートオプションの一覧は項7.4を参照してください。必要なオプションを含める必要があります。

- %packagesセクション— 詳細は項7.5 を参照してください。
- %preセクションと%postセクション— この2つのセクションの順序はどちらが先でもかまいません。また、必須ではありません。詳細については、項7.6と項7.7を参照してください。

- 必須でない項目は省略可能です。
- 必須項目が省略されている場合は、インストールプログラムは通常のインストールと同様、ユーザーに関連項目の回答を要求してきます。ユーザーが答えると、自動的に続行します(ほかに必須項目が省略されていなければ)。
- 番号記号(#)で始まる行は、コメントとして処理され無視されます。
- キックスタートアップグレードの場合は、必須項目は次のとおりです。
  - 言語
  - 言語サポート
  - インストール方法
  - デバイスの指定(インストールの実行にデバイスが必要な場合)
  - キーボードの設定
  - upgradeキーワード
  - ブートローダの設定

  アップグレードに、ほかの項目を指定しても無視されます(注意、パッケージの選択も無視されます)。

7.4. キックスタートのオプション

キックスタートファイルには、次のオプションを記述することができます。キックスタートファイルを作成するのにグラフィカルインターフェイスを使用する場合は、**キックスタート設定ツール**アプリケーションを使用できます。詳細については第8章 を参照してください。

注意

オプションの後にイコールマーク(=)が来る場合は、その後に値を指定する必要があります。例に上げているコマンドでは、角カッコ([ ])内のオプションはコマンド用のオプション引数です。

autostep (オプション)

‘ interactiveと類似していますが、このコマンドでは次の画面が自動的に表示されます。おもにデバッグに使用します。

auth またはauthconfig (必須)

‘ システムに関する認証オプションをセットアップします。インストール後に使うauthconfigコマンドと似ています。デフォルトでは、パスワードは通常、暗号化され、シャドウ化はされません。

--enablemd5

‘ ユーザーのパスワードにMD5暗号化を使います。

--enablenis

‘ NISサポートを有効にします。デフォルトでは、--enablenisを指定するとネットワーク上で見つかった任意のドメインが使用されます。必ず--nisdomain=オプションでドメインを手動で指定してください。

--nisdomain=

‘ NISサービスに使うNISドメインの名前です。

--nisserver=

‘ NISサービスに使うサーバーです(デフォルトではブロードキャスト)。

--useshadow または--enableshadow

‘ シャドウパスワードを使います。

--enableldap

‘ /etc/nsswitch.conf内のLDAPサポートを有効にします。これによりシステムはユーザーに関する情報(UID、ホームディレクトリ、シェルなど)をLDAPディレクトリから取得できるようになります。このオプションを使うには、nss_ldap パッケージをインストールする必要があります。また、--ldapserver=と--ldapbasedn=を使用して、サーバーとベースDNの指定も必要です。

--enableldapauth

‘ 認証手段としてLDAPを使います。これによりLDAPディレクトリを使ってパスワードを認証、変更するためのpam_ldapモジュールが有効になります。このオプションを使うには、nss_ldapパッケージをインストールしておく必要があります。--ldapserver=と--ldapbasedn=を使用して、サーバーとベースDNの指定も必要です。

--ldapserver=

‘ --enableldapまたは--enableldapauthを指定した場合、利用するLDAPサーバーの名前を指定するこのオプションを使用します。このオプションは、/etc/ldap.confファイルで設定します。

--ldapbasedn=

‘ --enableldapまたは--enableldapauthを指定した場合、ユーザー情報の格納場所であるLDAPディレクトリツリーにおけるDN(識別名)。このオプションは /etc/ldap.confファイルで設定します。

--enableldaptls

‘ TLS(Transport Layer Security)ルックアップを使用します。このオプションによって、LDAPは認証前に暗号化したユーザー名とパスワードをLDAPサーバーに送信できます。

--enablekrb5

‘ Kerberos 5を使ってユーザーを認証します。Kerberos自体にはホームディレクトリ、UID、あるいはシェルという考え方はありません。したがって、Kerberosを有効にする場合は、LDAP、NIS、Hesiodなども有効に設定して、このワークステーションにユーザーのアカウントを認識させる必要があります。あるいは、/usr/sbin/useraddコマンドを使用して、ユーザーのアカウントをこのワークステーションに認識させます。このオプションを使う場合は、pam_krb5パッケージをインストールしておく必要があります。

--krb5realm=

‘ ワークステーションの所属先であるkerberos 5 のrealm(レルム)。

`--krb5kdc=`

‘ realmへの要求に対してサービスを提供するKDC(複数可)。realm内に複数のKDCがある場合には、名前をカンマ(,)で区切って指定します。

`--krb5adminserver=`

‘ realmに属するKDCで、kadmindが動作しているもの。このサーバーはパスワードの変更やその他の管理関連要求を取り扱います。複数のKDCがある場合には、このサーバーはマスターKDC上だけで実行しなければなりません。

`--enablehesiod`

‘ ユーザーのホームディレクトリ、UID、シェルをルックアップするためのHesiodサポートを有効にします。ネットワークでのHesiodの設定と使い方に関しての詳細は`glibc`パッケージの`/usr/share/doc/glibc-2.x.x/README.hesiod`を参照してください。HesiodはDNSの拡張機能であり、DNSレコードを使用してユーザーやグループなどの各種項目に関する情報を保存します。

`--hesiodlhs`

‘ Hesiod LHS(Left-hand side)オプション。`/etc/hesiod.conf`で設定します。このオプションは、Hesiodライブラリが情報を検索する際に、DNSを検索するための名前を決定するときに使用されます。LDAPによるベースDNの使用法と似ています。

`--hesiodrhs`

‘ Hesiod RHS(Reft-hand side)オプション。`/etc/hesiod.conf`で設定します。このオプションは、Hesiodライブラリが情報を検索する際に、DNSを検索するための名前を決定するときに使用されます。LDAPによるベースDNの使用法と似ています。

ヒント

「jim」のユーザー情報を検索するには、Hesiodライブラリは*jim.passwd<LHS><RHS>*を検索します。これにより、ユーザーのpasswdエントリに似たTXTレコード(`jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`)が得られます。グループの場合も、*jim.group<LHS><RHS>*を使うこと以外は同じです。

番号によるユーザーとグループのルックアップは、「jim.passwd」のCNAMEとして「501.uid」を作成し、「jim.group」のCNAMEとして「501.gid」を作成することによって処理されます。ライブラリが検索対象の名前を決定するとき、LHSとRHSの前にはピリオド[.]がないことに注意してください。LHSとRHSは通常ピリオドで始まります。

`--enablesmbauth`

‘ SMBサーバー(通常、SambaまたはWindowsサーバー) に対するユーザーの認証を有効にします。SMB認証サポートにはホームディレクトリ、UID、あるいはシェルという考え方はありません。したがって、SMB認証サポートを有効にする場合は、LDAP、NIS、Hesiodなども有効に設定して、このワークステーションにユーザーのアカウントを認識させる必要があります。あるいは、`/usr/sbin/useradd`コマンドを使用して、ユーザーのアカウントをワークステーションに認識させます。このオプションを使うには、`pam_smb`パッケージをインストールしておく必要があります。

`--smbservers=`

‘ SMB認証に使用するサーバー名。複数のサーバーを指定するには、名前をカンマ(,)で区切ります。

`--smbworkgroup=`

‘ SMBサーバーのワークグループ名。

`--enablecache`

‘ `nscd`サービスを有効にします。`nscd`サービスはユーザーやグループ、その他のさまざまなタイプの情報についての情報をキャッシュします。NIS、LDAP、Hesiodのいずれかを使用してネットワーク上でユーザーやグループについての情報を配信するよう選択した場合、キャッシュ化は特に便利です。

`bootloader` (必須)

‘ ブートローダーのインストール方法と、ブートローダーがLILOまたはGRUBのどちらであるかを指定します。このオプションはインストールとアップグレードの両方に必要です。アップグレードでは`--useLilo`が指定されていなくて、現在のブートローダーがLILOである場合、ブートローダーはGRUBに変更されます。アップグレードでLILOを保存しておくには、`bootloader --upgrade` を使用します。

`--append=`

‘ カーネルパラメータを指定します。複数のパラメータを指定するには、パラメータをスペースで区切ります。例えば、
`bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"`

`--location=`

‘ ブートレコードを書き込む場所を指定します。有効な値は次のようになります。`mbr`(デフォルト)、`partition`(カーネルを収納しているパーティションの最初のセクションにブートローダーをインストール)、または、`none` (ブートローダーをインストールしない)

`--password=`

‘ GRUBを使用している場合、GRUBブートローダーパスワードをこのオプションで指定されているものにします。これはカーネルオプションが随意にパスできるGRUBシェルへのアクセスを制限するために使用されるべきです。

`--md5pass=`

‘ GRUBを使用している場合、パスワードがすでに暗号化されていること以外は、`--password=` に似ています。

`--useLilo`

‘ GRUBの代わりにLILOをブートローダーとして使用します。

`--linear`

‘ LILOを使用する場合、LILOの`linear` オプションを使用します。これは下位互換を目的としています(現在、デフォルトでlinearが使用される)。

`--nolinear`

‘ LILOを使用する場合、LILOの`nolinear` オプションを使用します。linearがデフォルトです。

`--lba32`

‘ LILOを使用する場合、自動検出の代わりにlba32を強制的に使用します。

`--upgrade`

‘ 古いエントリを保存しながら、既存のブートローダー設定をアップグレードします。このオプションはアップグレードでのみ使用できます。

clearpart (オプション)

‘ 新しいパーティションを作る前に、システムからパーティションを削除します。デフォルトでは、パーティションは削除されません。

注意

clearpartコマンドが使用されると、論理パーティションで--onpart コマンドが使用できなくなります。

--linux

‘ Linuxパーティションがすべて消去されます。

--all

‘ システムのすべてのパーティションが消去されます。

--drives=

‘ パーティションを消去するドライブを指定します。例えば、以下のコマンドで、プライマリIDEコントローラの最初の2つのドライブ上のパーティションを消去します。

```
clearpart --drives hda,hdb
```

--initlabel

‘ ディスクラベルをアーキテクチャ用のデフォルトに初期化します(例、x86の場合はmsdos、Itaniumの場合はgpt)。このオプションを利用すれば、新しいハードディスクドライブにインストールする場合、ディスクラベルを初期化するかどうかを確認するメッセージがインストールプログラムによって表示されることはありません。

device (オプション)

‘ ほとんどのPCIシステム上で、インストールプログラムによってイーサネットとSCSIカードは正しく自動検出されます。しかし、古いシステムとPCIシステムのいくつかでは、キックスタートが正常にデバイスを検索するには手がかりが必要になります。インストールプログラムに余分のモジュールをインストールするよう指示するdevice コマンドは次のような形式になっています。

```
device <type> <moduleName> --opts=<options>
```

<type>

‘ scsiか、ethで入れ換えます。

<moduleName>

‘ インストールすべきカーネルモジュールの名前に入れ換えます。

--opts=

‘ カーネルモジュールに渡すオプション。複数のオプションを渡すときは、引用符で囲みます。たとえば、次のようにします。

```
--opts="aic152x=0x340 io=11"
```

`deviceprobe` (オプション)

‘ PCIバスの検出を強制的に実行し、検出されたすべてのデバイスに対応するモジュールを、利用できる場合に、ロードします。

`driverdisk` (オプション)

‘ ドライバディスクはキックスタートインストール時に使用できます。ドライバディスクの内容を、システムのハードドライブ上にあるパーティションのルートディレクトリにコピーする必要があります。次に、`driverdisk`コマンドを使って、インストールプログラムがドライバディスクを検索する場所を指定します。
`driverdisk <partition> [--type=<fstype>]`

`<partition>`

‘ ドライバディスクを収納しているパーティションです。

`--type=`

‘ ファイルシステムタイプです(例、vfatまたはext2)。

`firewall` (オプション)

‘ このオプションは、インストールプログラムの**ファイアウォール設定**に相当します。
`firewall <securitylevel> [--trust=] <incoming> [--port=]`

`<securitylevel>`

‘ 次のセキュリティレベルの1つと入れ換えます。

- `--high`
- `--medium`
- `--disabled`

`--trust=`

‘ この一覧にデバイス(たとえばeth0など)を記述すると、そのデバイスからのすべてのトラフィックはファイアウォールを通り抜けることができます。複数のデバイスを記述するには、`--trust eth0 --trust eth1`のように指定します。`--trust eth0, eth1` のようにカンマで区切ることはできません。

`<incoming>`

‘ 次を1つまたはそれ以上で入れ換えて指定したサービスだけにファイアウォールを通過させます。

- `--dhcp`
- `--ssh`
- `--telnet`
- `--smtp`
- `--http`
- `--ftp`

`--port=`

‘ ファイアウォールの通過を許可するポートを、port:protocolの形式で指定します。たとえば、IMAPアクセスがファイアウォールを通過できるようにするには、`imap:tcp` と指定します。ポートを数値で直接指定することもできます。たとえば、ポート1234上でUDPを許可する場合は`1234:udp`と指定します。ポートが複数ある場合は、カンマで区切って指定します。

`install`(オプション)

‘ システムに対し、既存システムをアップグレードするのではなく、新規にシステムをインストールするよう指示します。これはデフォルトのモードです。インストールのためには、`cdrom`、`harddrive`、`nfs` 、`url`(ftp またはhttp インストール用)の中からひとつインストールタイプを指定する必要があります。`install` コマンドとインストール方法のコマンドは別々の行に入力しなければなりません。

`cdrom`

‘ システムの最初のCD-ROMドライブからインストールします。

`harddrive`

‘ ローカルドライブ上のRed Hatインストールツリーからインストール。VFATまたはext2でなければなりません。

- `--partition=`

  インストール元のパーティション(sdb2など)

- `--dir=`

  インストールツリーの`RedHat` ディレクトリを含むディレクトリ

たとえば、

```
harddrive --partition=hdb2 --dir=/tmp/install-tree
```

`nfs`

‘ 指定したNFSサーバからインストール

- `--server=`

  インストール元とするサーバー(ホスト名またはIP)

- `--dir=`

  インストールツリーの`RedHat` ディレクトリを含むディレクトリ

たとえば、

```
nfs --server=nfsserver.example.com --dir=/tmp/install-tree
```

`url`

‘ FTPまたはHTTP 経由でリモートサーバ上にあるインストールツリーからのインストール

たとえば、

```
url --url http://<server>/<dir>
```

または、

```
url --url ftp://<username>:<password>@<server>/<dir>
```

interactive (オプション)

‘ インストール時にキックスタートファイルで指定された情報を使用しますが、与えられた値を検査し変更することができます。インストールプログラムの各画面にキックスタートファイルからの値が表示されます。次ボタンをクリックして値をそのまま使用するか、値を変更して次ボタンをクリックし、続行します。autostepも参照してください。

keyboard (必須)

‘ システムのキーボードタイプを設定します。i386、Itanium、Alphaなどのマシン上で利用可能なキーボードの一覧を次に示します。

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-nodeadkeys, dk, dk-latin1, dvorak, es, et,
fi, fi-latin1, fr, fr-latin0, fr-latin1, fr-pc, fr_CH, fr_CH-latin1,
gr, hu, hu101, is-latin1, it, it-ibm, it2, jp106, la-latin1, mk-utf,
no, no-latin1, pl, pt-latin1, ro_win, ru, ru-cp1251, ru-ms, ru1, ru2,
ru_win, se-latin1, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querty, slovene, trq, ua,
uk, us, us-acentos
```

また、/usr/lib/python2.2/site-packages/rhpl/keyboard_models.pyもこのリストを含みます。このファイルはrhplパッケージの一部です。

lang (必須)

‘ インストール時に使用する言語を設定します。たとえば、キックスタートファイルに次の行を記述すると、言語は英語に設定されます。

```
lang en_US
```

/usr/share/redhat-config-language/locale-list は各行の最初のコラムに有効な言語コードの一覧を提供するファイルで、redhat-config-languagesパッケージの一部です。

langsupport (必須)

‘ システムにインストールする言語を設定します。langで使用した言語コードと同じ言語コードをlangsupportでも使用できます。

1つの言語をインストールするには、その言語を指定します。たとえば、フランス語fr_FR をインストールして使用する例を次に示します。

```
langsupport fr_FR
```

--default=

‘ 複数言語のサポートをインストールする場合は、デフォルトが識別されなければなりません。

例えば、英語とフランス語をインストールし、英語をデフォルト言語として使用するには、

```
langsupport --default=en_US fr_FR
```

--defaultに言語をひとつだけ付けて使用すると、すべての言語がインストールされて指定した言語をデフォルトに設定します。

lilo (bootloaderに入れ替わりました。)

‘

警告

このオプションに代わって、bootloader が使用されるようになりました。このオプションは、下位互換の目的でのみ使用できます。bootloaderを参照してください。

ブートローダーをインストールする方法を指定します。デフォルトでは、LILOが最初のディスクのMBRにインストールされ、またDOSパーティションが検出されるとデュアルブートシステム

をインストールします(DOS/Windowsシステムは、LILO: プロンプトでdos と入力すれば起動されます)。

--append <*params*>

‘ カーネルパラメータを指定します。

--linear

‘ LILOのlinearオプションを使用します。これは下位互換を目的としています(現在はデフォルトでlinearが使用されます)。

--nolinear

‘ LILOのnolinearオプションを使用します。現在はデフォルトでlinearが使用されます。

--location=

‘ LILOブートレコードを書き込む場所を指定します。有効な値は、mbr (デフォルト)か、partition (そのカーネルが含まれるパーティションの最初のセクタにブートローダーをインストール) です。locationを指定しないと、LILOはインストールされません。

--lba32

‘ 自動検出の代わりにlba32モードを強制的に使用します。

lilocheck (オプション)

‘ lilocheckを指定すると、インストールプログラムは最初のハードドライブのMBR上のLILOをチェックし、見つかった場合はシステムを再起動します。— この場合、インストールは実行されません。このオプションを指定しておけば、インストールされているシステムがキックスタートによって再インストールされてしまうといった事態は避けられます。

logvol (オプション)

‘ 次の構文を使用して、論理ボリューム管理(LVM)用の論理ボリュームを作成します。
logvol *mountpoint* --vgname=*name* --size=*size* --name=*name*

先ず、パーティションを作成して、論理ボリュームグループを構成します。それから、論理ボリュームを作成します。例えば、
```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

mouse (必須)

‘ GUIモードとテキストモードの両方に対して、マウスを設定します。オプションは、

--device=

‘ マウスの接続先デバイス(--device=ttyS0など)

--emulthree

‘ このオプションを指定すると、X Window System は、左右のマウスボタンの同時クリックを中央ボタンのクリックとしてエミュレートします。2ボタンマウスを使っている場合に指定する必要があります。

オプションに続けて、次のようなマウスタイプを指定することができます。
alpsps/2, ascii, asciips/2, atibm, generic, generic3, genericps/2, generic3ps/2, genericwheelps/2, genericusb, generic3usb, genericwheelusb,

geniusnm, geniusnmps/2, geniusprops/2, geniusscrollps/2, geniusscrollps/2+,

thinking, thinkingps/2, logitech, logitechcc, logibm, logimman, logimmanps/2, logimman+, logimman+ps/2, logimmusb, microsoft, msnew, msintelli, msintellips/2, msintelliusb, msbm, mousesystems, mmseries, mmhittab, sun, none

このリストはrhplパッケージの一部である/usr/lib/python2.2/site-packages/rhpl/mouse.pyファイルにもあります。

引数なしでmouseコマンドを指定する場合、またはmouseコマンドを省略した場合は、インストールプログラムによりマウスを自動検出します。最近のマウスであればほとんどは検出されます。

network (オプション)

‘ システムのネットワーク情報を設定します。キックスタートインストールでネットワークの使用が必要ない場合(つまり、NFS、HTTP、FTP経由でインストールしない場合)は、システムのネットワークは設定されません。インストールでネットワークの使用が必要とされ、ネットワーク情報がキックスタートファイルに指定されていない場合、Red Hat Linuxインストールプログラムは、eth0を経由し、動的IPアドレス(BOOTP/DHCP)を使用してインストールするものとみなし、最終的にインストールされたシステムがIPアドレスを動的に決定するように設定します。このnetworkコマンドは、ネットワーク経由のキックスタートインストール及び、最終的にインストールされるシステムのネットワーク情報を設定するものです。

--bootproto=

‘ dhcp、bootp 、static の内のいずれかを入力。

デフォルトはdhcpですが、bootp とdhcp は同じ物として扱われます。

DHCP手法は、DHCPサーバを使用してそのネットワーク設定を取得します。想像できる通り、BOOTP手法も同様のもので、BOOTPサーバを利用してそのネットワーク設定を取得します。システムにDHCP使用を指示するには、

```
network --bootproto=dhcp
```

システムがBOOTPを使ってネットワーク設定を取得するよう指定するには、キックスタートファイルで次の行を使います。

```
network --bootproto=bootp
```

静的IPアドレスを使う場合は、必要なネットワーク情報をすべてキックスタートファイルに記述しておく必要があります。名前のとおりこの情報は静的であり、インストール中だけでなくインストール後も使われます。1行に全てのネットワーク設定情報を含む必要があるため、静的ネットワークの行はより複雑になります。IPアドレス、ネットマスク、ゲートウェイ、ネームサーバを指定する必要があります。例えば、(\は全てが1行に入ることを示します。)

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 \
--gateway=10.0.2.254 --nameserver=10.0.2.1
```

静的アドレスを使う場合、次の2つの制約があることに注意してください。

- 静的なネットワーク設定情報のすべては*1*行で指定しなければなりません。たとえば、バックスラッシュ(\) を使って改行することはできません。
- ここでは、ネームサーバはひとつだけの指定になります。しかし、必要ならキックスタートファイルの%postセクション(項7.7での解説を参照)を使用して、ネームサーバを追加することができます。

`--device=`

‘ インストール時に使用するイーサネットデバイスの選択に使用します。インストールプログラムはネットワークを設定してキックスタートファイルを検索するので、キックスタートファイルがローカルファイル(`ks=floppy` など)でなければ`--device=`の使用は、無意味であることに注意してください。例えば、

```
network --bootproto=dhcp --device=eth0
```

`--ip=`

‘ インストール先コンピュータのIPアドレス。

`--gateway=`

‘ デフォルトのゲートウェイのIPアドレス。

`--nameserver=`

‘ プライマリネームサーバーのIPアドレス。

`--nodns`

‘ DNSサーバーは設定しません。

`--netmask=`

‘ インストールされるシステムのネットマスク。

`--hostname=`

‘ インストールされるシステムのホスト名。

`part` または、`partition` (インストールには必須、アップグレードでは無視)

‘ システムにパーティションを作成します。

システムの別々のパーティションに複数のRed Hat Linux インストールが存在する場合、インストールプログラムはユーザーにどのインストールをアップグレードするか聞いてます。

警告

`--noformat`と`--onpart` が使用されない限り、作成されるパーティションはすべてインストール過程の一部としてフォーマットされます。

<mntpoint>

‘ *<mntpoint>* は、パーティションがマウントされる場所で次のどれかの形態でなければなりません。

- `/`*<path>*

  例えば、`/`、`/usr`、`/home`

- `swap`

  このパーティションはswap領域として使用されます。

  スワップパーティションの容量を自動的に決めるには`--recommended` オプションを使用します。

  ```
  swap --recommended
  ```

  自動的に生成されるswapパーティションの最小サイズは、システムのRAMの容量よりも大きく、その2倍を超えることはありません。

- raid.<*id*>

  このパーティションはソフトウェアRAID (raidを参照)用に使用されます。

- pv.<*id*>

  このパーティションはLVM (logvolを参照)用に使用されます。

--size=

‘ パーティションの最小サイズを、メガバイト単位で入力します。「500」など、整数のみで指定します。数字の後ろにMBを付けないでください。

--grow

‘ (もしあれば)最大許容量までパーティションを拡張する、または、指定限度サイズまで拡張するように指示します。

--maxsize=

‘ パーティションを拡張するように設定する場合に、最大パーティションサイズをメガバイト単位で入力します。整数を使って指定し、数字の後ろにMBを付けないでください。

--noformat

‘ --onpartコマンドを使用する場合、インストールプログラムに対して、パーティションをフォーマットしないように指示します。

--onpart=あるいは--usepart=

‘ パーティションをすでに存在しているデバイス上に設定します。例えば、
partition /home --onpart=hda1

これで/homeパーティションをすでに存在する/dev/hda1デバイス上に設定しました。

--ondisk=または--ondrive=

‘ パーティションが特定のディスク上に作成されるように強制します。例えば、--ondisk=sdbは、システム上の2番目のSCSI ディスクにパーティションを設定します。

--asprimary

‘ プライマリパーティションとして自動アロケーションを強制的に実行します。実行できなければパーティション設定の失敗になります。

--bytes-per-inode=

‘ 指定された番号は、作成された時点のファイルシステム上のinode単位のバイト数を示します。10進法で示す必要があります。このオプションは、ファイルシステム上のinodeの数を増やしたいアプリケーションがあるときに役に立ちます。

--type= (fstypeに入れ換えられました)

‘ このオプションは使用できません。fstypeを使用してください。

--fstype=

‘ パーティション用のファイルシステムタイプを設定します。有効な値は、ext2、ext3、swap、vfatです。

`--start=`

‘ パーティションの開始シリンダを指定します。ドライブを`--ondisk=`または`ondrive=`で指定する必要があります。また、終了シリンダを`--end=`で指定するか、パーティションサイズを`--size=` で指定する必要があります。

`--end=`

‘ パーティションの終了シリンダを指定します。開始シリンダを`--start=`で指定する必要があります。

`--badblocks`

‘ パーティションに不良セクタがないかをチェックするように指定します。

注意

何らかの理由でパーティションの設定ができなかった場合には、診断メッセージが仮想コンソール3で表示されます。

`raid` (オプション)

‘ ソフトウェアRAIDデバイスを構成します。このコマンドの形式は次のとおりです。
`raid` <*`mntpoint`*> `--level=`<*`level`*> `--device=`<*`mddevice`*> <*`partitions*`*>

<*`mntpoint`*>

‘ RAIDファイルシステムをマウントする位置です。これを「`/`」とした場合は、ブートパーティション(`/boot`) が存在しない限り、RAIDレベルは1でなければなりません。ブートパーティションが存在する場合は、`/boot` パーティションがレベル1でなければならず、ルート(「`/`」)パーティションのタイプはどれでもかまいません。<*`partitions*`*> (複数パーティションを列挙できることを表す)は、RAIDアレイに追加するRAID識別子を列挙します。

`--level=`

‘ 使用するRAIDのレベル(0、1、または、5)。

`--device=`

‘ 使用するRAIDデバイスの名前(md0やmd1など)。RAIDデバイスの範囲はmd0からmd7まであり、それぞれ1度だけ使用することができます。

`--spares=`

‘ RAIDアレイに割り当てられたスペアドライブの数を指定します。スペアドライブはドライブが故障した場合にアレイを再構築するために使用します。

`--fstype=`

‘ RAIDアレイのファイルシステムタイプを設定します。有効な値は、ext2、ext3、swap、vfatです。

`--noformat`

‘ RAIDアレイをフォーマットしません。

次に示すのは、「`/`」にRAIDレベル1のパーティションを作成する方法、`/usr`にRAIDレベル5のパーティションを作成する方法の例です。このシステムには3つのSCSI ディスクがあるものとします。また、各ドライブ上にswap パーティションをひとつずつ、計3つ作ります。

```
part raid.01 --size=60 --ondisk=sda
part raid.02 --size=60 --ondisk=sdb
part raid.03 --size=60 --ondisk=sdc
part swap --size=128 --ondisk=sda
part swap --size=128 --ondisk=sdb
part swap --size=128 --ondisk=sdc
part raid.11 --size=1 --grow --ondisk=sda
part raid.12 --size=1 --grow --ondisk=sdb
part raid.13 --size=1 --grow --ondisk=sdc
raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

`reboot` (オプション)

‘ インストールの完了後に再起動します(引数はありません)。通常、キックスタートはメッセージを表示して待機し、ユーザーがキーを押すと再起動します。

`rootpw` (必須)

‘ システムのrootパスワードを<*password*>引数で指定します。
`rootpw [--iscrypted] <password>`

`--iscrypted`

‘ これを設定すると、引数のパスワードはすでに暗号化されているものとみなされます。

`skipx` (オプション)

‘ このオプションを指定すると、インストール先のシステム上にXは設定されません。

`text` (オプション)

‘ キックスタートインストールをテキストモードで実行します。デフォルトでは、キックスタートインストールはグラフィカルモードで実行されます。

`timezone` (必須)

‘ システムのタイムゾーンを<*timezone*>に設定します。`timeconfig`で一覧表示されるタイムゾーンならどれでも使うことができます。
`timezone [--utc] <timezone>`

`--utc`

‘ これを指定すると、ハードウェアクロックがUTC (グリニッジ標準)時間に合わせて設定されているものとみなされます。

`upgrade` (オプション)

‘ システムに対し、新規システムのインストールではなく、既存システムをアップグレードするように指示します。インストールツリーの場所としてcdrom、ハードドライブ、nfs, あるいはurl(ftp やhttp用)のどれかを指定する必要があります。詳細は`install`をご覧ください。

`xconfig` (オプション)

‘ X Window Systemを設定します。このオプションを指定しないと、Xをインストールする場合のインストール中に手動でXを設定する必要があります。最終的にXをシステムにインストールしない場合は、このオプションを指定しないでください。

`--noprobe`

‘ モニタの検証を行いません。

`--card=`

‘ 指定したカードを使用します。このカードの名前は、hwdataパッケージ内の /usr/share/hwdata/Cardsのカード一覧から指定します。この一覧は**キックスタート設定**の**X の設定** 画面にもあります。この引数が指定されていない場合、インストールプログラムはPCIバスのカードを検証します。AGPはPCIバスの一部なので、AGPカードはサポートされていれば検出されます。検証順序はマザーボードのPCIスキャン順序によって決まります。

`--videoram=`

‘ ビデオカードのビデオRAM容量を指定します。

`--monitor=`

‘ 指定したモニタを使用します。このモニタの名前は、hwdataパッケージ内の /usr/share/hwdata/MonitorsDBのモニタ一覧から指定します。この一覧は**キックスタート設定**の**X Configuration**画面にもあります。--hsync または--vsyncが指定されているとこの引数は無視されます。モニタ情報を指定しないと、インストールプログラムによってモニタは自動的に検証されます。

`--hsync=`

‘ モニタの水平同期周波数を指定します。

`--vsync=`

‘ モニタの垂直同期周波数を指定します。

`--defaultdesktop=`

‘ デフォルトのデスクトップをGNOMEまたはKDEに設定します(%packagesによってGNOMEまたはKDEのデスクトップ環境がインストールされていることが前提)。

`--startxonboot`

‘ インストールされたシステムでグラフィカルログインを使います。

`--resolution=`

‘ インストールされたシステムでのX Window System のデフォルト解像度を指定します。有効な値は、640x480、800x600、1024x768、1152x864、1280x1024、1400x1050、1600x1200です。ビデオカードやモニタと互換性のある解像度を指定するようにしてください。

`--depth=`

‘ インストールされたシステムでのX Window System のデフォルトの色の深さを指定します。有効な値は8、16、24、32です。ビデオカードやモニタと互換性のある色の深さを指定するようにしてください。

`volgroup` (optional)

‘ 論理ボリューム管理(LVM)グループを次の構文で作成するのに使用します。
`volgroup` *`name partition`*

先ず、パーティションを作成して、論理ボリュームグループを構成します。それから、論理ボリュームを作成します。例えば、次のようにします。

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

zerombr (オプション)

‘ zerombrにyesを単一引数として指定すると、ディスク上にある不正なパーティションテーブルはすべて初期化されます。その場合、不正なパーティションテーブルがあるディスクの内容はすべて破棄されます。このコマンドは、次の形式で使います。

```
zerombr yes
```

この書式でのみ有効です。

%include

‘ %include */path/to/file* コマンドを使用し、キックスタートファイルの%includeコマンドの場所に内容があったかのように、キックスタートファイルにある別のファイルの内容を含めます。

7.5. パッケージの選択

%packagesコマンドを使用して、インストールしたいパッケージの一覧表示をするキックスタートファイルセクションを開始します(これはインストール専用です。アップグレードの際のパッケージ選択はサポートされていません)。

パッケージは、グループまたは、個別のパッケージ名で指定することができます。インストールプログラムは、関連するパッケージをグループ化したいくつかのグループを定義しています。グループ一覧についてはRed Hat Linux CD-ROMの1枚目にある RedHat/base/comps.xmlを参照してください。それぞれのグループがid、使用レベルの値、名前、説明、及びパッケージ一覧を持ちます。パッケージ一覧の中の分類では、mandatory(必須)と印があるものはグループが選択された場合には常にインストールされ、default(デフォルト)と印があるものはグループが選択された場合にデフォルトで選択されており、optional(オプション)と印があるものは、グループが選択された場合でも、さらに指定される必要があるものです。

ほとんどの場合、目的のグループを一覧にするだけで、個々のパッケージは一覧表示する必要はありません。Core とBaseグループは常にデフォルトで選択されていることに注意してください。このため、 %packagesセクション内で指定する必要がありません。

次に%packagesの例を示します。

```
%packages
@ X Window System
@ GNOME Desktop Environment
@ Graphical Internet
@ Sound and Video
galeon
```

お判りのように、各グループは1行に1つずつ指定されており、@記号から始まり、空白の次にcompsファイル内のグループのフルネームがあります。個別のパッケージは追加の文字なしで指定します(上記の例の galeonの行は個別パッケージを示す)。

また、デフォルトのパッケージ一覧からインストールしないパッケージを指定することもできます。

```
@ Games and Entertainment
-kdegames
```

%packagesオプションには2つのオプションがあります。

`--resolvedeps`

‘ 一覧にしたパッケージをインストールして、自動的にパッケージの依存関係を解決します。このオプションが指定されずパッケージの依存関係が存在した場合は、自動インストールが一時中断してユーザーに知らせます。例えば、

```
%packages --resolvedeps
```

`--ignoredeps`

‘ 未解決の依存関係を無視して、一覧表示された中で依存関係を持たないパッケージをインストールします。例えば、

```
%packages --ignoredeps
```

`--ignoremissing`[1]

‘ インストールプログラムが不足しているパッケージやグループがある度に、インストールを停止してインストールの中断または続行を確認する代わりに、これら不足しているパッケージやグループを無視します。例えば、

```
%packages --ignoremissing
```

7.6. インストール前のスクリプト

`ks.cfg`を解析したらすぐにシステム上で実行させるコマンドを追加することもできます。このセクションは必ずキックスタートファイルの末尾(コマンド群の後)に置き、`%pre`コマンドで始めます。`%pre` セクションではネットワークにアクセスできますが、ただし、この時点ではネームサービスが設定されていないので、IPアドレスしか使えません。

注意

インストール前のスクリプトは、chroot環境で実行されるのではないことに注意してください。

`--interpreter` *`/usr/bin/python`*

‘ Pythonなどの異なるスクリプト言語を指定できます。*`/usr/bin/python`* を目的のスクリプト言語に入れ換えます。

7.6.1. スクリプトの例

`%pre` セクションの例を以下に示します。

```
%pre

#!/bin/sh

hds=""
mymedia=""

for file in /proc/ide/h*
do
 mymedia=‘cat $file/media‘
 if [ $mymedia == "disk" ] ; then
   hds="$hds ‘basename $file‘"
 fi
```

1. これはRed Hat Linux 9 に加えられた新しいオプションです。

```
done

set $hds
numhd=‘echo $#‘

drive1=‘echo $hds | cut -d’ ’ -f1‘
drive2=‘echo $hds | cut -d’ ’ -f2‘

#Write out partition scheme based on whether there are 1 or 2 hard drives

if [ $numhd == "2" ] ; then
 #2 drives
 echo "#partitioning scheme generated in %pre for 2 drives" > /tmp/part-include
 echo "clearpart --all" >> /tmp/part-include
 echo "part /boot --fstype ext3 --size 75 --ondisk hda" >> /tmp/part-include
 echo "part / --fstype ext3 --size 1 --grow --ondisk hda" >> /tmp/part-include
 echo "part swap --recommended --ondisk $drive1" >> /tmp/part-include
 echo "part /home --fstype ext3 --size 1 --grow --ondisk hdb" >> /tmp/part-include
else
 #1 drive
 echo "#partitioning scheme generated in %pre for 1 drive" > /tmp/part-include
 echo "clearpart --all" >> /tmp/part-include
 echo "part /boot --fstype ext3 --size 75" >> /tmp/part-includ
 echo "part swap --recommended" >> /tmp/part-include
 echo "part / --fstype ext3 --size 2048" >> /tmp/part-include
 echo "part /home --fstype ext3 --size 2048 --grow" >> /tmp/part-include
fi
```

このスクリプトはシステム内のハードドライブの数を判定して、ドライブの数に応じて異なるパーティション設定スキムでテキストファイルを書き込みます。キックスタートファイルにパーティション設定コマンドのセットを持つ代わりに、以下の行を含めます。

```
%include /tmp/part-include
```

スクリプト内で選択されたパーティション設定コマンドが使用されます。

7.7. インストール後のスクリプト

インストール完了したら、システム上で実行させるコマンドを追加するオプションです。このセクションは必ずキックスタートファイルの末尾に置き、%postコマンドで始めます。追加のソフトウェアをインストールしたり、追加のネームサーバを設定したりする機能にこのセクションが役に立ちます。

注意

ネームサーバーを含め静的IP情報でネットワークを設定した場合は、%postセクションでネットワークにアクセスしてIPアドレスを解決できます。DHCPのネットワークを設定した場合は、インストールで%post セクションが実行されているときは/etc/resolv.conf ファイルは完了していません。ネットワークにアクセスすることはできますが、IPアドレスは解決できません。したがって、DHCPを使用している場合、%postセクションでIPアドレスを指定する必要があります。

注意

インストール後のスクリプトはchroot環境で実行されることに注意してください。したがって、インストール媒体からスクリプトやRPMをコピーするなどの作業を実行することはできません。

`--nochroot`

‘ これを指定すると、chroot環境の外で実行したいコマンドを指定することができます。

次の例はファイル`/etc/resolv.conf`をインストール直後のファイルシステムにコピーします。

```
%post --nochroot
cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
```

`--interpreter` *`/usr/bin/python`*

‘ Pythonなどの異なるスクリプト言語を指定できます。*`/usr/bin/python`*を目的のスクリプト言語で入れ換えます。

7.7.1. スクリプトの例

サービスを起動したり停止したりします。

```
/sbin/chkconfig --level 345 telnet off
/sbin/chkconfig --level 345 finger off
/sbin/chkconfig --level 345 lpd off
/sbin/chkconfig --level 345 httpd on
```

NFS共有から`runme`と言うスクリプトを実行します。

```
mkdir /mnt/temp
mount 10.10.0.2:/usr/new-machines /mnt/temp
open -s -w -- /mnt/temp/runme
umount /mnt/temp
```

システムにユーザーを追加します。

```
/usr/sbin/useradd bob
/usr/bin/chfn -f "Bob Smith" bob
/usr/sbin/usermod -p 'kjdf$04930FTH/' bob
```

7.8. キックスタートファイルを使用可能にする

キックスタートファイルは、次のいずれかの場所に保存しておかなければなりません。

- ブートディスク(フロッピー)上
- ブートCD-ROM上
- ネットワーク上

通常、キックスタートファイルは、ブートディスク上にコピーするか、ネットワーク上で利用できるように設定します。キックスタートインストールの多くはネットワーク上で実行される傾向にありますので、ネットワークベースの保存とアクセスが一般的になっています。

キックスタートファイルを保存する場所について、さらに詳しく調べてみましょう。

7.8.1. キックスタートブートディスク(フロッピー)の作成

フロッピーディスクベースのキックスタートインストールを実行するには、キックスタートファイルが`ks.cfg` と名付けられる必要があり、そしてブートディスク(フロッピー)の最上位ディレクトリに位置していなければなりません。ブートディスクの作成についての解説は、*Red Hat Linux* インストールガイドのインストールブートディスクの作成を参照してください。Red Hat LinuxブートディスクはMS-DOS形式ですからLinux上でも`mcopy` コマンドを使用してキックスタートファイルを簡単にコピーできます。

```
mcopy ks.cfg a:
```

別の方法として、Windowsを使用してファイルをコピーすることもできます。また、ファイルシステムタイプがvfatでRed Hat Linux内にMS-DOSブートディスクをマウントして、`cp` コマンドを使用しファイルをフロッピーにコピーできます。

7.8.2. キックスタートブートCD-ROMの作成

CD-ROMベースのキックスタートインストールを実行するには、キックスタートファイルが`ks.cfg`と名付けられ、ブートCD-ROMの最上位ディレクトリ位置に位置していなければなりません。CD-ROMは読み取り専用のため、CD-ROMに書き込まれるイメージを作成するのに使用するディレクトリに、ファイルが加えられなければなりません。ブートCD-ROMの作成に関する解説は*Red Hat Linux* インストールガイドのインストールブート*CD-ROM*の作成を参照してください。ただし、`file.iso`イメージファイルを作成する前に、`ks.cfg`キックスタートファイルを`isolinux/`ディレクトリにコピーしてください。

7.8.3. ネットワークでキックスタートファイルを使用可能にする

キックスタートを使ったネットワークインストールはネットワーク上の多数のコンピュータに短時間で簡単にインストールでき、しかも自動化できるため、非常に多く利用されています。ローカルネットワーク上のBOOTP/DHCPサーバーとNFSサーバーを利用する方法が一般的です。クライアントシステムに対して、BOOTP/DHCPサーバーを使ってネットワーク情報を与え、実際にインストールで使うファイルはNFSサーバーを使ってアクセスさせます。この2つのサーバーは1台のコンピュータ上で動作させることが多いのですが、そうしなければならないわけではありません。

ネットワークベースでキックスタートインストールを実行するには、そのネットワーク上にBOOTP/DHCPサーバーがあり、Red Hat Linuxをインストールしようとしているコンピュータ用の設定情報がなければなりません。BOOTP/DHCPサーバーは、クライアントに対して、ネットワーク情報とキックスタートファイルの場所を通知するために使われます。

クライアントシステムは、BOOTP/DHCPサーバーからキックスタートファイルの保存場所を受け取ると、そのファイルのパスをNFSでマウントし、ファイルをクライアントにコピーしてキックスタートファイルとして使います。具体的な設定方法は、使用しているBOOTP/DHCPによって異なります。

以下に示すのは、Red Hat Linuxと共に出荷されるDHCPサーバー用の`dhcpd.conf`ファイルから関連部分を抜粋したものです。

```
filename "/usr/new-machine/kickstart/";
next-server blarg.redhat.com;
```

実際にNFSサーバーの名前を設定するときは、 `filename`の次の部分をキックスタートファイルの名前(あるいはキックスタートファイルを含むディレクトリ)に置き換え、`next-server`の次の部分をNFSサーバー名に置き換える必要があることに注意してください。

BOOTP/DHCPサーバーから返されるファイル名がスラッシュ(/) で終わる場合は、パスのみと解釈されます。この場合、クライアントシステムはNFSでそのパスをマウントし、特定の名前を持つファイルを探します。ここでクライアントが探すファイル名は、次のとおりです。

<*ip-addr*>-kickstart

ファイル名の<*ip-addr*> の部分は、10進ドット記法のIPアドレスに置き換えてください。たとえば、IPアドレスが10.10.0.1であるコンピュータのファイル名は、10.10.0.1-kickstart です。

サーバー名が指定されていない場合、クライアントシステムはBOOTP/DHCP要求に応答したサーバーをNFSサーバーとして使います。パスまたはファイル名が指定されていない場合は、クライアントシステムはBOOTP/DHCP上の/kickstartをマウントし、上と同じく<*ip-addr*> -kickstartというファイル名でキックスタートファイルを検索します。

7.9. インストールツリーを使用可能にする

キックスタートインストールは、インストールツリーにアクセスする必要があります。インストールツリーとは、Red Hat LinuxCD-ROMにあるバイナリのコピーで同じ構造になっています。

CDベースのインストールを実行する場合、キックスタートインストールを始める前に、Red Hat Linux CD-ROM#1をコンピュータに挿入します。

ハードドライブのインストールを実行するには、バイナリRed Hat Linux CD-ROMのISOイメージがコンピュータのハードドライブにあることを確認してください。

ネットワークベース(NFS、FTP、HTTP)のインストールを実行している場合、ネットワーク上でインストールツリーが使用できるようにしなければなりません。詳細については*Red Hat Linux* インストールガイドのネットワークインストールの準備セクションを参照してください。

7.10. キックスタートインストールの開始

キックスタートインストールを開始するには、Red Hat Linuxブートディスク(フロッピー)、Red Hat LinuxブートCD-ROM、Red Hat LinuxCD-ROM #1からシステムをブートしてブートプロンプトで特別のブートコマンドを入力しなければなりません。ksコマンドライン引数がカーネルに渡ると、インストールプログラムがキックスタートファイルをさがします。

ブートディスク(フロッピー)

‘ キックスタートファイルが項7.8.1で示すようにブートディスク(フロッピー)にある場合は、ドライブにあるフロッピーでシステムを起動して、次のコマンドをboot:プロンプトで入力します。
linux ks=floppy

CD-ROM #1 とフロッピーディスク

‘ **linux ks=floppy** コマンドは、ks.cfgファイルがフロッピーディスクにあるvfatファイルシステムまたはext2ファイルシステムにあり、Red Hat Linux CD-ROM #1 からブートする場合にも使用できます。

代わりのブートコマンドは、Red Hat Linux CD-ROM #1をブートしてフロッピーディスク上にあるvfatまたはext2 ファイルシステムのキックスタートファイルを取り出します。実行するには、次のコマンドをboot: プロンプトで入力します。
linux ks=hd:fd0:/ks.cfg

ドライバディスクを使用

‘ キックスタートでドライバディスクを使用する必要がある場合は、**dd** オプションも指定します。例えば、ブートディスクをブートしてドライバディスク使用するには、以下のコマンドをboot: プロンプトで入力します。
linux ks=floppy dd

ブートCD-ROM

- キックスタートファイルが項7.8.2で示すようにブートCD-ROMにある場合は、CD-ROMをシステムに挿入してシステムをブートし、次のコマンドを`boot:`プロンプトで入力します(`ks.cfg`はキックスタートファイルの名前)。
  `linux ks=cdrom:/ks.cfg`

キックスタートインストールを開始するその他のオプションは以下の通りです。

`ks=nfs:<server>:/<path>`

- インストールプログラムは、キックスタートファイルとしてNFSサーバー<*server*>上の<*path*>ファイルを検索します。インストールプログラムはDHCPを使用してイーサネットカードを設定します。たとえば、NFSサーバーがserver.example.comで、キックスタートファイルがNFS共有の`/mydir/ks.cfg` にある場合、正しいブートコマンドは`ks=nfs:server.example.com:/mydir/ks.cfg` となります。

`ks=http://<server>/<path>`

- インストールプログラムは、キックスタートファイルとしてHTTPサーバー<*server*>上の<*path*>ファイルを検索します。インストールプログラムはDHCPを使用してイーサネットカードを設定します。たとえば、HTTPサーバーがserver.example.comで、キックスタートファイルがHTTPディレクトリの `/mydir/ks.cfg`にある場合、正しいブートコマンドは`ks=http:server.example.com:/mydir/ks.cfg` となります。

`ks=floppy`

- インストールプログラムは、`/dev/fd0` にあるフロッピーディスク上のVFATかext2ファイルシステム上で`ks.cfg`ファイルを検索します。

`ks=floppy:/<path>`

- インストールプログラムは、キックスタートファイルとして`/dev/fd0`にあるフロッピーディスク上の<*path*>ファイルを検索します。

`ks=hd:<device>:/<file>`

- インストールプログラムは、<*device*> 上にファイルシステムをマウントし(VFATまたはext2 であることが必須)、キックスタート設定ファイルとして、そのファイルシステム上で<*file*> を検索します(たとえば`ks=hd:sda3/mydir/ks.cfg`)。

注意

2番目のコロンはRed Hat Linux 9の構文変更です。

`ks=file:/<file>`

- インストールプログラムは、ファイルシステムから<*file*>ファイルを読み込もうとします。マウントは行なわれません。キックスタートファイルがすでに`initrd`イメージ上に存在する場合は、通常、この方法を使います。

`ks=cdrom:/<path>`

- インストールプログラムは、キックスタートファイルとしてCD-ROM上の<*path*>ファイルを検索します。

`ks`

‘ `ks`を単独で使用した場合、インストールプログラムはDHCPを使ってシステム内のイーサネットカードを設定します。システムはDHCPレスポンスから「bootServer」をNFSサーバーとして使い、キックスタートファイルを読み込みます(デフォルトでは、これはDHCPサーバーと同じです)。キックスタートファイルの名前は次のいずれかです。

- DHCPを指定し、bootfileが「`/`」で始まる場合は、DHCPで入手するブートファイルがNFSサーバー上で検索されます。
- DHCPを指定し、bootfileが`/` 以外の文字で始まる場合、DHCPで入手するブートファイルがNFSサーバー上の`/kickstart` ディレクトリ上で検索されます。
- DHCPでbootfileを指定していない場合、インストールプログラムは`/kickstart/1.2.3.4-kickstart`ファイルを読み込もうとします。ここで、*`1.2.3.4`* はインストール先のコンピュータの数値IPアドレスです。

`ksdevice=<`*`device`*`>`

‘ インストールプログラムはこのネットワークデバイスを使って、ネットワークに接続します。例えば、eth1デバイスを通してシステムに接続されているNFSサーバ上のキックスタートファイルでキックスタートインストールを開始するには、`boot:`プロンプトでコマンドの`ks=nfs:<`*`server`*`>:/<`*`path`*`> ksdevice=eth1`を使用します。

第8章

キックスタート設定

キックスタート設定を使うと、グラフィカルなユーザーインターフェイスを通してキックスタートファイルを作ることができ、ファイルの正しい構文を覚えておく必要がありません。

キックスタート設定を使用するには、X Window Systemが起動している必要があります。**キックスタート設定**をスタートするには、(パネル上から)**メインメニューボタン**=> **システムツール** => **キックスタート設定**と選択して行きます。または、コマンド`/usr/sbin/redhat-config-kickstart`を入力します。

キックスタートファイルを作成している時、**ファイル** =>**プレビュー**と選択すると、いつでもその時点の選択状況を確認することができます。

8.1. 基本的な設定

図8-1. 基本的な設定

言語メニューからインストール時の使用及びインストール後のデフォルトとして使用する言語を選択します。

キーボードメニューから、システムのキーボードタイプを選択します。

マウスメニューから、システムに使用するマウスを選択します。**No Mouse**を選択すると、マウスの設定は行われません。 **Probe for Mouse**を選択すると、インストールプログラムはマウスの自動検出を試みます。最近のマウスであればほとんどは検出されます。

2つボタン形式のマウスの場合は、**3ボタンのエミュレーション**を選択して3つボタンと同様の機能が得られます。このオプションが選択されている場合は、左右のマウスボタンを同時にクリックすると、中央のマウスボタンをクリックしたものとして認識されます。

タイムゾーンメニューから、システムのタイムゾーンを選択します。UTCを使用するようにシステムを設定するには、**UTC時計を使用**を選択します。

rootパスワードテキスト入力ボックスに、システムのrootパスワードを入力します。暗号化したパスワードとしてファイルに保存するには、**rootパスワードを暗号化**を選択します。ファイルが保存されるときに暗号化のオプションが選択されている場合は、入力したプレーンテキストのパスワードは暗号化されてキックスタートファイルに書き込まれます。すでに暗号化されているパスワードの入力、パスワード暗号化の選択はしないでください。

言語のプルダウンメニューから選択した言語の他に、さらに追加の言語をインストールするには、**言語サポート**の一覧でそれらにチェックを付けます。**言語**のプルダウンメニューから選択した言語はインストール後にデフォルトとして使用されますが、**言語設定ツール** (`redhat-config-language`)を使用すれば、インストール後にデフォルトも変更できます。

インストール後にシステムを再起動を選択すると、インストール終了後にシステムが自動的に再起動します。

デフォルトでは、キックスタートインストールはグラフィカルモードで実行されます。このデフォルトを無効にして、代わりにテキストモードを使用するには、**テキストモードでインストールを実行**ボタンをチェックします。

キックスタートインストールをインタラクティブモードで行うことができます。すなわち、インストールはキックスタートファイルにあらかじめ設定されたすべてのオプションを使用して行われますが、次の画面に進む前にオプションのプレビューを見ることができます。次の画面に進むには、設定を確認、または必要であれば変更して**次**ボタンをクリックします。このようなインストール方法を選択するには、**インタラクティブモードでインストールを実行**ボタンを選択します。

8.2. インストール方法

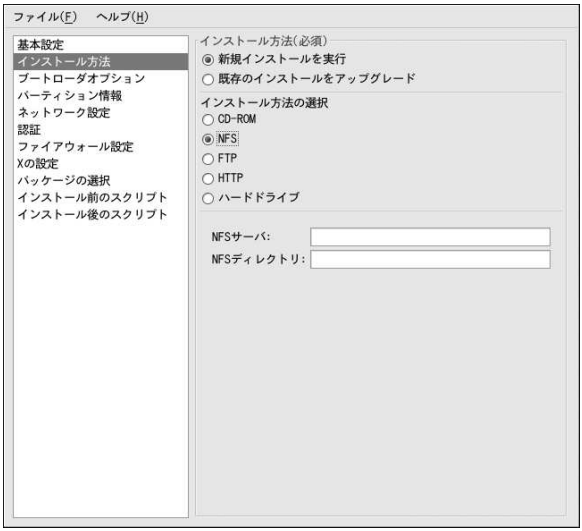


図8-2. インストール方法

インストール方法画面では、新しくインストールをする、または、アップグレードする、のどちらを実行するか選択できます。アップグレードを選択すると、**パーティション情報**オプションと**パッケー**

ジの選択オプションは使用できなくなります。これらのページはキックスタートアップグレードでサポートされません。

また、この画面から実行するキックスタートインストールのタイプも選択します。以下のオプションから選択できます。

- **CD-ROM** — このオプションを選択すると、Red Hat Linux CD-ROM からRed Hat Linux をインストールします。
- **NFS** — NFS共有ディレクトリからRed Hat Linuxをインストールする場合はこのオプションを選択します。NFSサーバーとNFSディレクトリを入力する2つのテキスト入力ボックスが表示されます。NFSサーバーの完全修飾ドメイン名またはIPアドレスを入力します。NFSディレクトリとして、インストールツリーの`RedHat` ディレクトリが含まれるNFSディレクトリの名前を入力します。たとえば、NFSサーバーにディレクトリ `/mirrors/redhat/i386/RedHat`がある場合は、NFSディレクトリとして`/mirrors/redhat/i386` と入力します。
- **FTP** — FTPサーバーからRed Hat Linuxをインストールする場合はこのオプションを選択します。FTPサーバーとFTPディレクトリを入力する2つのテキスト入力ボックスが表示されます。FTPサーバーの完全修飾ドメイン名またはIPアドレスを入力します。FTPディレクトリとして、`RedHat`ディレクトリが含まれるFTP ディレクトリの名前を入力します。たとえば、FTPサーバーにディレクトリ`/mirrors/redhat/i386/RedHat` がある場合は、FTPディレクトリとして `/mirrors/redhat/i386`を入力します。FTPサーバーがユーザー名とパスワードを要求する場合は、それらも同様に指定します。
- **HTTP** — HTTPサーバーからRed Hat Linuxをインストールする場合はこのオプションを選択します。HTTPサーバーとHTTPディレクトリを入力する2つのテキスト入力ボックスが表示されます。HTTPサーバーの完全修飾ドメイン名またはIPアドレスを入力します。HTTPディレクトリとして、`RedHat`ディレクトリが含まれるHTTP ディレクトリの名前を入力します。たとえば、HTTPサーバーにディレクトリ`/mirrors/redhat/i386/RedHat` がある場合は、HTTPディレクトリとして `/mirrors/redhat/i386`を入力します。
- **ハードドライブ** — ハードディスクドライブからRed Hat Linuxをインストールする場合はこのオプションを選択します。ハードドライブパーティションとハードドライブディレクトリを入力する2つのテキスト入力ボックスが表示されます。ハードディスクドライブからのインストールでは、ISO(またはCD-ROM)イメージを使用する必要があります。ISOイメージに問題を確認するには、*Red Hat Linux* インストールガイドで解説している`md5sum` プログラム、同様に`linux mediacheck`ブートオプションを使用します。ISOイメージが含まれるハードドライブパーティション(例、`/dev/hda1`)を**ハードドライブパーティション**テキストボックスに入力します。ISOイメージが含まれるディレクトリを**ハードドライブディレクトリ**テキストボックスに入力します。

8.3. ブートローダーのオプション

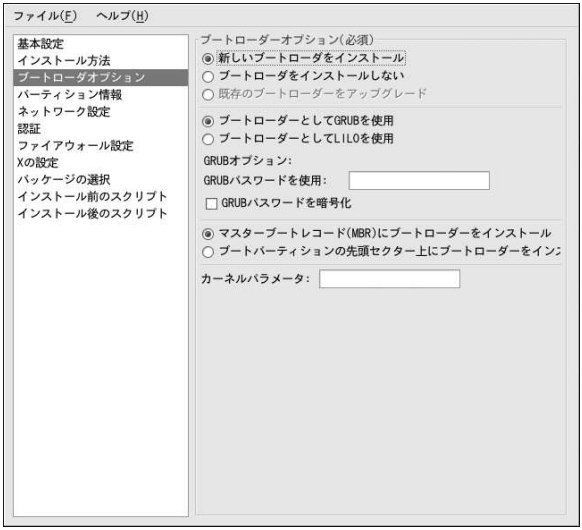


図8-3. ブートローダーのオプション

ブートローダーとしてGRUB かLILOをインストールするオプションがあります。ブートローダーをインストールしない場合は、**ブートローダーをインストールしない**を選択します。ブートローダーをインストールしない選択をする場合は、ブートディスクの作成して、または、他の方法(例えば、他社のブートローダー)で、システムが起動できることを確認しておいてください。

ブートローダーのインストールを選択する場合は、インストールするブートローダーを選択し(GRUBまたはLILO)、ブートローダーのインストール先(マスターブートレコードまたは`/boot`パーティションの最初のセクタ)も選択する必要があります。これをブートローダーとして使用する場合は、MBRにブートローダーをインストールします。ブートローダとして別のブートローダーを使用する場合は、`/boot`パーティションの最初のセクタにLILOまたはGRUBをインストールし、その別のブートローダがRed Hat Linuxを起動するように設定します。

システムの起動時に使用されるカーネルに特定のパラメータを渡すには、そのパラメータを**カーネルパラメータ** テキストフィールドに入力します。たとえば、IDE CD-ROM Writer を使用する場合は、カーネルパラメータとして **`hdd=ide-scsi`**(**hdd**はCD-ROM デバイス)と入力することによって、`cdrecord` を使用する前にロードされなければならないSCSIエミュレーションドライバを使うようにカーネルに指示できます。

ブートローダーとしてGRUBを選択すると、GRUBパスワードを設定することによってパスワードで保護することができます。**GRUBパスワードを使う**テキスト入力エリアにパスワードを入力します。暗号化したパスワードとしてファイルに保存する場合は、**GRUBパスワードを暗号化**を選択します。ファイルが保存されるときに暗号化オプションが選択されている場合、入力したプレーンテキストのパスワードは暗号化されてキックスタートファイルに書き込まれます。すでに暗号化されているパスワードを入力した後のパスワードの暗号化は選択はしないでください。

ブートローダーとしてLILOを選択する場合は、リニアモードを使用するかどうかと、lba32モードの使用を強制するかどうかを選択します。

インストール方法ページで、 **既存のインストールをアップグレード**を選択している場合、**既存のブートローダーをアップグレード**を選択すると、既存のブートローダーをアップグレードして、同時

にその古い既存エントリを保存します。

8.4. パーティション情報

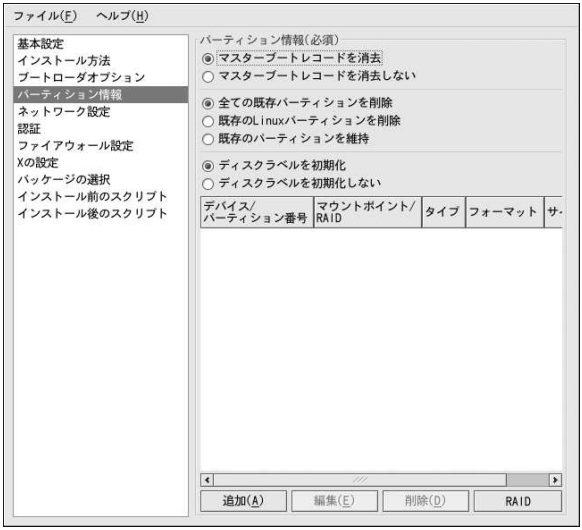


図8-4. パーティション情報

マスターブートレコード(MBR)をクリアするかどうか選択します。また、既存のすべてのパーティションを削除、既存の全てのLinuxパーティションを削除、既存のパーティションを保存、の中からどれかを選択することができます。

ディスクラベルをシステムのアーキテクチャに応じてデフォルトに初期設定できます(例、x86用は`msdos`、Itanium用は`gpt`)。新品のハードクドライブにインストールする場合は、**ディスクラベルを初期化**を選択します。

8.4.1. パーティションの作成

パーティションを作成するには、**追加** ボタンをクリックします。図8-5に示すような**パーティションオプション** ウィンドウが表示されます。新しいパーティションのマウントポイント、ファイルシステムタイプ、パーティションサイズなどを選択します。オプションとして、以下から選択することもできます。

- **追加容量オプション**セクションで、「固定容量」、「指定限度まで使用」、「最大許容量まで使用」の中から選択してパーティションを作成します。swapをファイルシステムタイプとして選択した場合、サイズの指定をする代わりに、インストールプログラムが推奨サイズでswap パーティションを作成するように選択できます。
- パーティションを強制的にプライマリパーティションとして作成
- 特定のハードドライブにパーティションを作成。たとえば、最初のIDEハードディスク(`/dev/hda`)上にパーティションを作成するには、ドライブとして**hda**を指定します。ドライブ名に`/dev`を入力しないでください。

- 既存のパーティションを使用。たとえば、最初のIDEハードディスク(/dev/hda1)上の最初のパーティションにパーティションを作成するには、パーティションとして**hda1**を指定します。パーティション名に/devを入力しないでください。
- 選択されたファイルシステムタイプとしてフォーマットします。

図8-5. パーティションの作成

既存のパーティションを編集するには、一覧からパーティションを選択し、**編集**ボタンをクリックします。パーティションを追加するときに表示されるのと同じ **パーティションオプション**ウィンドウが図8-5のように表示されますが、選択したパーティションの値が表示されている点が異なります。パーティションのオプションを変更し、**OK**をクリックします。

既存のパーティションを削除するには、一覧からパーティションを選択し、**削除**ボタンをクリックします。

8.4.1.1. ソフトウェアRAID パーティションの作成

RAID及び、各種RAIDレベルの詳細については第3章をお読みください。RAID 0、1、5、が設定できます。

ソフトウェアRAIDパーティションを作成するには、以下のステップに従います。

1. **RAID**ボタンをクリックします。
2. **ソフトウェアRAIDパーティションを作成**を選択します。
3. **ソフトウェアRAID**をファイルシステムとして選択する以外は、前述の説明に従いパーティションの設定をします。また、パーティションを作成するハードドライブを指定するか、使用する既存パーティションを指定しなければなりません。

図8-6. ソフトウェアRAIDパーティションを作成

これらのステップを繰り返して、RAID設定に必要な数だけパーティションを作成します。すべてのパーティションがRAIDパーティションである必要はありません。

RAIDデバイスの構成に必要なパーティションをすべて作成し終った後は、次のステップに従います。

1. **RAID**ボタンをクリックします。
2. **RAIDデバイスを作成**を選択します。
3. マウントポイント、ファイルシステムタイプ、RAIDデバイス名、RAIDレベル、RAIDメンバー、ソフトウェアRAIDデバイス用のスペアの数、を選択して、RAIDデバイスをフォーマットするかどうかを選択します。

図8-7. ソフトウェアRAIDデバイスの作成

4. **OK**をクリックして一覧にデバイスを追加します。

8.5. ネットワーク設定

図8-8. ネットワーク設定

キックスタート経由でインストールされるシステムがイーサネットカードを使用しない場合、**ネットワーク設定**ページでイーサネットカードを設定しないでください。

ネットワークは、ネットワークベースのインストール方法(NFS、FTPまたはHTTP)を選択する場合のみ必要です。ネットワークは、**ネットワーク管理ツール**(`redhat-config-network`)を使用すればインストール後も、いつでも設定できます。詳細は第12章を参照してください。

システムの各イーサネットカードに、**ネットワークデバイスの追加**をクリックして、ネットワークデバイスとデバイスのネットワークタイプを選択します。1番目のイーサネットカードならネットワークデバイス名に**eth0** を選択し、2番目のイーサネットカードなら **eth1**を選びます(以降同じ)。

8.6. 認証

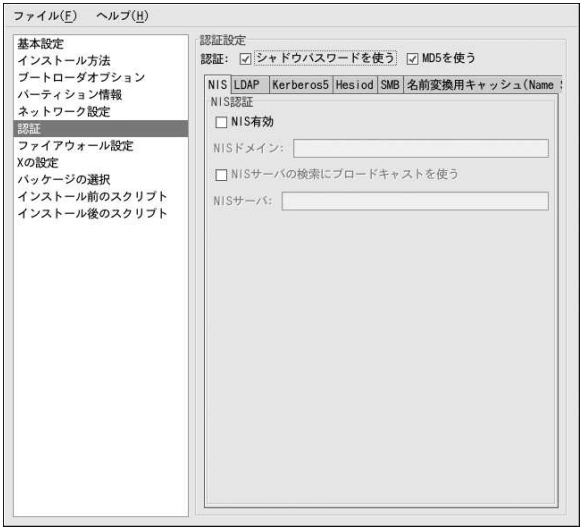


図8-9. 認証

認証セクションで、ユーザーパスワードに対してシャドウパスワードとMD5暗号化を使用するかどうかを選択します。これらのオプションの選択は強く推奨され、またデフォルトで選択されています。

認証設定オプションにより、次の認証方法を設定できます。

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- Name Switch Cache

デフォルトではこれらの方法は有効になっていません。これらの方法を有効にするには、該当のタブをクリックし、 **有効**の横にあるチェックボタンをクリックし、認証方法に対する適切な情報を入力します。

8.7. ファイアウォールの設定

図8-10. ファイアウォールの設定

ファイアウォール設定ウィンドウは、Red Hat Linuxインストールプログラムでの画面と **セキュリティレベル設定ツール**での画面と同じで、機能も同様です。セキュリティレベルを**高**、**中**、**なし**のいずれかで選択します。これらのセキュリティレベルについての詳細は、項13.1を参照してください。

8.8. Xの設定

X Window Systemをインストールする場合、キックスタートのインストール中に、図8-11で示すように**Xの設定**ウィンドウの**X Window System の設定**オプションをクリックして設定することができます。このオプションが選択されていない場合は、X設定オプションは無効になり、`skipx`オプションがキックスタートファイルに書き込まれます。

8.8.1. 全般

X設定の最初のステップとして、デフォルトの色の深さと解像度を選択します。それぞれ対応するプルダウンメニューで選択します。必ず、システムのビデオカード及びモニタと互換性がある色の深さと解像度を指定してください。

図8-11. Xの設定- 全般

GNOMEデスクトップとKDEデスクトップの両方をインストールする場合、どちらをデフォルトとするかを選択する必要があります。デスクトップをひとつだけインストールする場合は、必ずそのデスクトップを選択してください。システムがインストールされると、ユーザーはデフォルトにするデスクトップを選択できます。GNOMEとKDEに関する詳細については、*Red Hat Linux* インストールガイドと*Red Hat Linux* 入門ガイドを参照してください。

次に、システムの起動時にX Window Systemを起動するかどうかを選択します。このオプションが選択されている場合、システムはグラフィカルログイン画面を使用してランレベル5で起動します。システムをインストールした後、`/etc/inittab`設定ファイルを変更することによってこの設定を変更できます。

8.8.2. ビデオカード

デフォルトでは**ビデオカードの調査**が選択されます。インストール中、インストールプログラムによりビデオカードを検出するようこのデフォルトのままにします。最近のビデオカードであればほとんどは検出されます。このオプションを選択し、インストールプログラムがビデオカードをうまく検出できない場合、インストールプログラムはビデオカード設定画面で停止します。インストールプロセスを続行するには、一覧からビデオカードを選択し、**次**をクリックします。

別な方法として、図8-12に示すように**ビデオカード**タブに表示される一覧からビデオカードを選択することができます。**ビデオカードRAM**プルダウンメニューから、選択したビデオカードのビデオRAM容量を指定します。これらの値は、インストールプログラムがX Window Systemを設定するのに使用されます。

図8-12. Xの設定- ビデオカード

8.8.3. モニタ

ビデオカードを設定した後、図8-13に示す**モニタ**タブをクリックします。

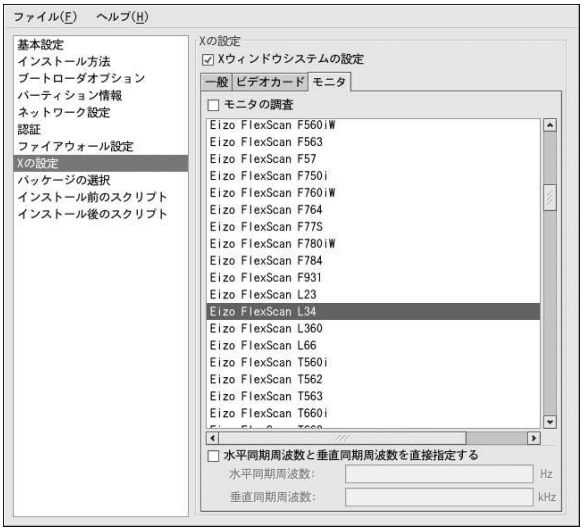


図8-13. Xの設定- モニタ

モニタの調査がデフォルトで選択されています。このままにすると、インストールプログラムがインストール中にモニタを検出します。最近のモニタのほとんどは検出されます。このオプションが選択されインストールプログラムが正常にモニタを検出できない場合は、インストールプログラムはモニタ設定画面で止まります。インストールプロセスを続行するには、一覧からモニタを選択して**次**をクリックします。

別の方法として、一覧からモニタを選ぶことができます。**モニタの代わりに水平同期と垂直同期を指定**オプションをチェックして、特定モニタを選択する代わりに水平と垂直の同期率を指定することもできます。このオプションは、システム用のモニタが一覧にない場合に便利です。このオプションを有効にすると、モニタ一覧は使用できなくなりますので注意してください。

8.9. パッケージの選択

図8-14. パッケージの選択

パッケージの選択ウィンドウでは、インストールするパッケージグループを選択することができます。

また、パッケージ依存関係を自動的に解決するオプションとパッケージ依存関係を無視するオプションがあります。

現在、**キックスタート設定**では、個々のパッケージを選択することはできません。個々のパッケージをインストールするには、保存した後のキックスタートファイルの%packages セクションを編集します。詳細については項7.5を参照してください。

8.10. インストール前のスクリプト

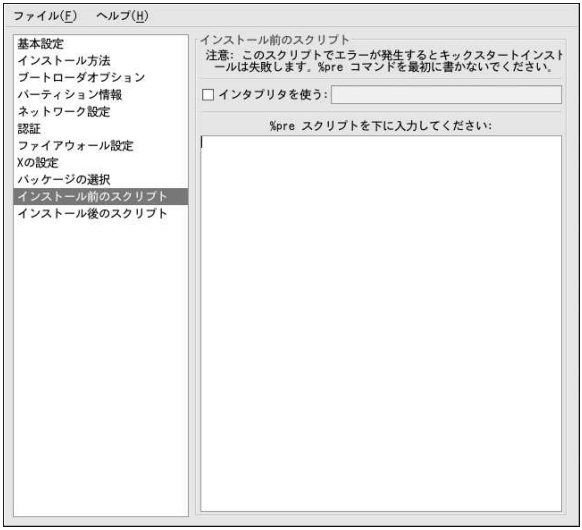


図8-15. インストール前のスクリプト

キックスタートファイルの構文を解析した直後、インストールを開始する前にシステムで実行されるコマンドを追加できます。キックスタートファイルでネットワークを設定している場合、ネットワークはこのセクションが処理される前に有効になります。インストール前のスクリプトを含ませるには、テキストエリアに入力します。

スクリプトを実行するのに使用するスクリプト言語を指定するには、**インタプリタを使う**オプションをクリックして、横にあるテキストボックスにインタプリタを入力します。例えば、**/usr/bin/python2.2**はPython スクリプト用に指定できます。このオプションは、キックスタートファイル内の`%pre --interpreter /usr/bin/python2.2`の使用に該当します。

用心

`%pre`コマンドは入力しないでください。このコマンドは自動的に追加されます。

8.11. インストール後のスクリプト

図8-16. インストール後のスクリプト

インストール完了後にシステムで実行されるコマンドも追加できます。キックスタートファイルに適切なネットワーク設定がされていれば、ネットワークは有効になり、スクリプトはネットワーク上でリソースにアクセスするためのコマンドを含むことができます。キックスタートファイルに含めるインストール後のスクリプトをテキストエリアに入力します。

用心

`%post`コマンドは入力しないでください。このコマンドは自動的に追加されます。

たとえば、新たにインストールされたシステムの本日のメッセージを変更するには、次のコマンドを`%post` セクションに追加します。

```
echo "Hackers will be punished!" > /etc/motd
```

ヒント

他に多くの例を項7.7.1で見ることができます。

8.11.1. chroot環境

インストールス後のクリプトをchroot環境外で実行するには、**インストール後のスクリプト**ウィンドウの先頭に表示されるこのオプションのチェックボタンをクリックします。これは、%postセクションで--nochrootオプションを使用するのと同じです。

chroot環境外でインストール後のセクション内に新しくインストールしたファイルシステムを変更したい場合は、ディレクトリ名に/mnt/sysimageを追加する必要があります。

たとえば、**chroot環境の外で実行** を選択する、前述の例は次のように変更する必要があります。

```
echo "Hackers will be punished!" > /mnt/sysimage/etc/motd
```

8.11.2. インタープリタの使用

スクリプトを実行するのに使用するスクリプト言語を指定するには、**インタプリタを使う**オプションを選択して、横にあるテキストボックスにインタプリタを入力します。例えば、**/usr/bin/python2.2**はPythonスクリプト用に指定できます。このオプションは、キックスタートファイル内で%pre --interpreter */usr/bin/python2.2*を使用するのに該当します。

8.12. ファイルの保存

キックスタートのオプションの選択が完了した後で、キックスタートファイルの内容を確認するには、プルダウンメニューから**ファイル** => **プレビュー**と選択します。

図8-17. プレビュー

キックスタートファイルを保存するには、プレビューウィンドウで**ファイルの保存**ボタンをクリックします。プレビューしないで保存するには、**ファイル** => **ファイルの保存** と順に選択するか、[Ctrl]-[S]キーを同時に押します。ダイアログボックスが現れます。ファイルの保存場所を選択します。

ファイルを保存した後、項7.10を参照して、キックスタートインストールの開始方法を確認してください。

第9章

基本的システムの復元

何か問題が発生した場合、解決するための方法はいくつかあります。ただし、その方法を実行するには、システムを十分に理解していることが必要です。本章では、システムを修復する知識を使用できる、レスキューモード、シングルユーザーモード、及び緊急モードでブートする方法を説明します。

9.1. 一般的な問題

これらの復元モードの1つでブートする必要がでるのは以下の理由のいずれかになります：

- 通常のRed Hat Linux(ランレベル3 又は5)をブート出来ない。
- ハードウェアまたはソフトウェアの問題があるので、システムのハードディスクドライブからいくつかの重要なファイルを取り出したい。
- rootパスワードを忘れてしまった。

9.1.1. Red Hat Linuxを起動できない

この問題はしばしばRed Hat Linuxをインストールした後に、別のオペレーティングシステムをインストールすることで発生します。他のオペレーティングシステムの一部は、コンピュータに他のオペレーティングシステムがないと想定しています。そしてGRUB 又はLILOブートローダに収納されている元来のマスターブートレコード(MBR)を上書きしてしまいます。この状態でブートローダが上書きされると、レスキューモードに入り、ブートローダを再構成しないと、Red Hat Linuxをブートすることが出来ません。

もう1つの一般的な問題は、インストール後にパーティションのサイズ変更、又は空き領域からの新規パーティションの作成をするのにパーティション設定ツールを使用している時に発生し、パーティションの順番が変わってしまいます。/パーティションのパーティション番号が変更された場合、ブートローダはパーティションをマウントするのにそれを見付けることが出来なくなります。この問題を修復するには、レスキューモードでブートし、`/boot/grub/grub.conf`(GRUB使用の場合)、又は`/etc/lilo.conf` (LILOを使用の場合)を修正します。又、LILO設定ファイルを修正した場合は、必ず`/sbin/lilo` コマンドを実行しなければなりません。

9.1.2. ハードウェア/ソフトウェアに問題がある場合

このカテゴリには多種多様の状況があります。2つの例として、ハードドライブが機能しない場合とブートローダ設定ファイル内に無効なルートデバイス、あるいはカーネルを指定する場合があげられます。これらのどちらかが発生すると、Red Hat Linuxを再起動できません。しかし、システム復元モードの1つでブートすると、問題を解決出来る可能性があり、少なくとも重要なファイルをコピーすることは出来ます。

9.1.3. Root パスワード

Rootパスワードを忘れた場合、どうすれば良いのでしょうか? 別のパスワードに設定しなおします。レスキューモード、あるいはシングルユーザーモードで起動し、`passwd`コマンドを使用してRootパスワードを再設定します。

9.2. レスキューモードで起動

レスキューモードは、システムのハードドライブからブートする代わりに、全面的にフロッピィディスク、CD-ROM、又は、他のブート方法で小規模のRed Hat Linux環境をブートする機能を提供します。

名前が示すように、レスキューモードは、ある状態からユーザーをレスキュー（救助）するためのものです。通常の運用では、Red Hat Linuxシステムはプログラムの実行、ファイルの保存など、どのような操作を行うにもシステムのハードディスクドライブにあるファイルを使用します。

しかし、システムのハードドライブのファイルにアクセスするのに充分にRed Hat Linuxを稼働することが出来ない時もあり得ます。レスキューモードを使用すれば、実際にはハードドライブから直接Red Hat Linuxを実行できなくてもシステムのハードドライブ上に保存してあるファイルにアクセス出来ます。

レスキューモードでブートするには、以下の方法のいずれかを使用してシステムをブートできる必要があります：

- `bootdisk.img`イメージから作成したインストールブートディスクからシステムをブートする。[1]
- インストールブートCD-ROMからシステムをブートする[2]
- Red Hat LinuxのCD-ROM 1枚目からシステムをブートする。

以上に説明した方法の1つでブートしたら、インストールブートプロンプトで次のコマンドを入力します：

```
linux rescue
```

言語などを含む、幾つかの簡単な質問に答えるように要求されます。また、どこに有効なレスキューイメージがあるか選択するように要求されます。**Local CD-ROM**, **Hard Drive**, **NFS image**, **FTP**, あるいは**HTTP**の中から選択します。その場所は、有効なインストールツリーを含んでいる必要があり、そのインストールツリーはブート元になるRed Hat Linux CD-ROM 1枚目と同じRed Hat Linuxバージョンのものでなければなりません。レスキューモードを開始するのに、ブートCD-ROMかブートディスクを使用した場合は、インストールツリーはそのメディアの作成元であるツリーと同じである必要があります。ハードドライブ、NFSサーバ、FTPサーバ、HTTPサーバなどでインストールツリーを設定する方法については*Red Hat Linux* インストールガイドを参照して下さい。

ネットワークの接続を必要としないレスキューイメージを選択した場合は、ネットワーク接続を使用したいかどうかを尋ねられます。ネットワークの接続は例えば、別のコンピュータにバックアップをしたり、共有ネットワークの場所からRPMパッケージをインストールしたりするのに役に立ちます。

そして、次のようなメッセージが表示されます：

```
The rescue environment will now attempt to find your Red Hat
Linux installation and mount it under the directory
/mnt/sysimage. You can then make any changes required to your
system. If you want to proceed with this step choose
'Continue'. You can also choose to mount your file systems
read-only instead of read-write by choosing 'Read-only'.
If for some reason this process fails you can choose 'Skip'
and this step will be skipped and you will go directly to a
command shell.
```

---

1. インストールブートディスクを作成するには、空のフロッピィディスクを挿入してRed Hat Linux のCD-ROMの1枚目にある`images/bootdisk.img`ファイルを`dd if=bootdisk.img of=/dev/fd0`コマンドでフロッピィにコピーします。
2. インストールブートCD-ROMを作成する方法は、*Red Hat Linux* インストールガイドの案内を参照して下さい。

Continueを選択すると、ファイルシステムが/mnt/sysimageディレクトリにマウントされる試みがあります。パーティションのマウントが失敗した場合、その通知があります。**Read-Only**を選択すると、ファイルシステムは/mnt/sysimageディレクトリにマウントされますが、読み取り専用モードです。**Skip**を選択すると、ファイルシステムはマウントされません。ファイルシステムが破損していると思われる場合は、**Skip**を選択します。

システムがレスキューモードに入ると、VC（仮想コンソール）1とVC 2に次のプロンプトが表示されます（VC 1にアクセスするには[Ctrl]-[Alt]-[F1]キーを使用し、VC 2にアクセスするには[Ctrl]-[Alt]-[F2]キーを使用します）。

```
-/bin/sh-2.05b#
```

Continueを選択した場合はパーティションが自動的にマウントされ、正常にマウントされると、システムはシングルユーザーモードに入ります。

ファイルシステムがマウントされていても、レスキューモードにいる間のデフォルトのルートパーティションは一時的なルートパーティションであり、通常のユーザーモード(ランレベル3から5)で使用するファイルシステムのルートパーティションではありません。ファイルシステムをマウントする選択をして正常にマウントすると、以下のコマンドを使用することによって、レスキューモード環境のルートパーティションをファイルシステムのルートパーティションに変更することが出来ます。

```
chroot /mnt/sysimage
```

これは、ルートパーティションが/としてマウントされることが要求されるrpmコマンドを実行する必要が有る場合に役に立ちます。chroot環境を終了するには、exitと入力するとプロンプトに戻ります。

Skipを選択した場合でも、まだレスキューモードの中で手動でパーティションをマウントすることが出来ます。これは*/foo* などのディレクトリを作成して、次のコマンドを使用して実行します：

```
mount -t ext3/dev/hda5/foo
```

上記のコマンドで、*/foo*はユーザーが作成したディレクトリ、*/dev/hda5*はマウントするパーティションです。パーティションがext2タイプの場合、ext3ではなくext2を指定します。

パーティションの名前が不明な場合は、次のコマンドを実行すれば一覧が表示されます。

```
fdisk -l
```

プロンプトから、次のような多くの役に立つコマンドを実行することが出来ます。

- list-harddrivesシステム内のハードドライブを一覧表示します
- ssh,scp及びpingネットワークが開始している場合
- dump とrestoreテープドライブのユーザー用
- parted とfdisk パーティションの管理用
- rpm ソフトウェアのインストール又はアップグレード用
- joe設定ファイルの編集用。(他のポピュラーなエディタであるemacs、pico、あるいはviなどをスタートしようとするとjoeエディタが開始されます。)

9.3. シングルユーザーモードでブートする

シングルユーザーモードの利点の1つは、ブート用のフロッピィやCD-ROMが必要ないことです。しかし、ファイルシステムを読み込み専用でマウントするオプションがないか、又は全くマウント出来ない状態です。

シングルユーザーモードでは、コンピュータはランレベル1でブートします。ユーザーのローカルファイルシステムはマウントされますが、ネットワークは起動しません。システム管理のシェルが使用できます。レスキューモードとは異なり、シングルユーザーモードでは自動的にファイルシステムをマウントしようとします。ファイルシステムが正常にマウントされない場合は、シングルユーザーモードは使用しないで下さい。システム上でランレベル1の設定が破損している場合、シングルユーザーモードは使用できません。

システムがブートできる状態で、ブート完了時にログインできない場合は、シングルユーザーモードを試します。

GRUBを使用している場合は、以下のステップに従ってシングルユーザーモードでブートします:

1. GRUBパスワードが設定されている場合は、pと入力し、パスワードを入力します。
2. ブートに使用したいカーネルのバージョンを持つ**Red Hat Linux**を選択して、編集用にeと入力します。選択したタイトル用の設定ファイル内に項目の一覧が表示されます。
3. kernelで始まる行を選択し、eと入力して行を編集します。
4. 行の末尾に移動し、1文字分のスペースを空けて**single**と入力します（[Spacebar]キーを押し、次に**single**と入力します）。[Enter]キーを押して編集モードを終了します。
5. GRUBの画面に戻り、bと入力してシングルユーザーモードでブートします。

LILOを使用している場合、LILOブートプロンプトで(グラフィカルLILOを使用している場合は、[Ctrl]-[x]キーを押してグラフィカル画面を終了してboot:プロンプトに行きます)次のように入力します:

```
linux single
```

9.4. 緊急モードでブートする

緊急モードでは、最小限可能な環境でブートします。ルートファイルシステムは読み込み専用でマウントされ、殆ど何も設定されません。シングルユーザーモードに対する緊急モードの主な利点は、initファイルがロードされないことです。initが破損していたり、動作していなくてもファイルシステムをマウントすることが出来るため、再インストールでは消失する可能性のあるデータを復元できます。

緊急モードでブートするには、一か所以外は項9.3の中にあるようにシングルユーザーモード用に説明してある同じ方法を使用します。キーワード**single**をキーワード**emergency**に入れ換えます。

第10章

ソフトウェアRAIDの設定

最初に第3章を読み、RAIDの概要、ハードウェアRAIDとソフトウェアRAIDの違いと、RAID 0、1、5の違いを理解してください。

ソフトウェアRAIDは、Red Hat Linuxのグラフィカルインストールの時か、又はキックスタートインストールの時でも設定できます。この章では、インストール時に**Disk Druid**を使用したソフトウェアRAIDの設定の方法について説明します。

RAIDデバイスを作成する前に、まず次の各ステップの指示に従ってRAIDパーティションを作成する必要があります：

1. **ディスクパーティションの設定**画面上で、**Disk Druidで手動のパーティション設定**を選択します。
2. **Disk Druid**の中では、**新規**を選択して新しいパーティションを作成します。
3. マウントポイントの入力はできません（RAIDデバイスの作成後に入力できるようになります）。
4. 図10-1に示してあるように**ファイルシステムタイプ**のプルダウンメニューから**ソフトウェアRAID**選択します。

図10-1. 新しいRAIDパーティションの作成

5. **選択可能なドライブ**には、RAIDを作成するドライブを選択します。複数のドライブがある場合は、ここですべてのドライブを選択します。RAIDアレイの作成対象としないドライブの選択は解除してください。
6. 目的のパーティションサイズを入力します。
7. **固定容量**を選択して、特定のサイズのパーティションを作成するか、**指定限度まで使用(MB)**を選択してそのパーティションの範囲を指定するサイズをメガバイト数で入力するか、あるいは**最大許容量まで使用**を選択してハードディスク上の使用可能な容量すべてまで後で成長するようにもできます。1つ以上のパーティションを成長可能にするとそれらのパーティション同士で空き領域を共有することになります。
8. パーティションをプライマリパーティションとする場合は、**プライマリパーティションにする**を選択してください。
9. フォーマットの前にインストールプログラムでハードドライブ上の不良ブロックを確認するには、**不良ブロックをチェック**を選択します。
10. **OK**をクリックしてメインの画面に戻ります。

RAID構成の為に必要なだけの複数パーティションを作成するには、上記のステップを繰り返します。すべてのパーティションがRAID用のパーティションになる必要はないことに注意してください。例えば、/homeパーティションだけをソフトウェアRAIDデバイスとして設定することも出来ます。

すべてのパーティションを**ソフトウェアRAID**パーティションとして作成したあとは、次のステップで進みます：

1. **Disk Druid**のメインのパーティション画面上で**RAID**ボタンを選択します。(図10-3を参照)
2. 次に図10-2 が現れますのでそこで、RAIDデバイスを作成することができます。

図10-2. RAIDデバイスの作成

3. マウントポイントを入力します。
4. パーティション用のファイルシステムタイプを選択します。
5. RAIDデバイス用に**md0**などのデバイス名を選択します。
6. RAIDレベルを選択します。**RAID 0**, **RAID 1**, 及び**RAID 5**から選びます。

注意

/bootのRAIDパーティションを作成している場合は、RAIDレベル1を選択する必要があります。そして最初の2つのドライブ(IDEを1番目、SCSIは2番目)の内の1つを使用しなければなりません。また/bootのRAIDパーティションを作成しないで、/のRAIDパーティションを作成している場合は、これをRAIDレベル1にして最初の2つのドライブ(IDEを1番目、SCSIは2番目)の内の1つを使用しなければなりません。

7. 作成したばかりのRAIDパーティションは**RAIDメンバー**一覧に現れます。これらのパーティションの中から、RAIDデバイスを作成する為に使用するパーティションを選択します。
8. RAID 1、又はRAID 5 を設定している場合、予備のパーティションの数を指定します。ソフトウェアRAIDパーティションに障害が発生した場合に、自動的に予備が代替として使用されます。指定する予備の数に応じて、追加のソフトウェアRAIDパーティションを作成する必要があります（RAIDデバイスのパーティションのほかに）。前のステップで、RAIDデバイスのパーティションと予備のパーティションを選択します。
9. **OK**をクリックすると、図10-3で示してあるように**ドライブの概要**一覧の中にRAID デバイスが表示されます。この時点からインストールプロセスを継続することが出来ます。詳しい案内については*Red Hat Linux* インストールガイドを参照して下さい。

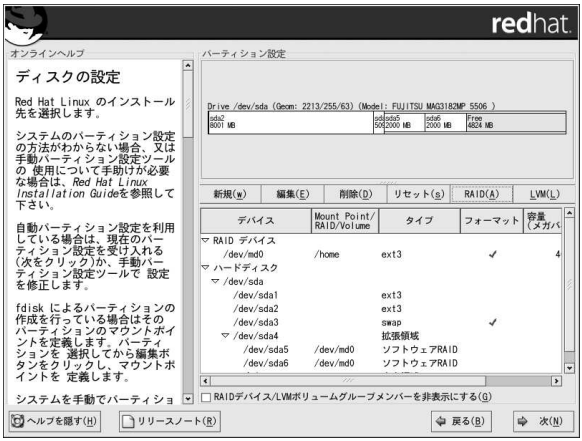


図10-3. 作成されたRAIDアレイ

第11章
LVM の設定

LVM はRed Hat Linuxのグラフィカルインストール時、又はキックスタートインストール時に設定することが出来ます。lvmパッケージのユーティリティを使用すればLVM設定を作成する事が出来ます。但し、その手順案内は、Red Hat Linuxインストール時の**Disk Druid**使用に焦点を置いてこの作業を完了する説明になっています。

最初にLVMに関する知識を得るため、第4章をお読み下さい。LVMを設定するのに必要な工程の概要を以下に示します：

- ハードドライブから物理ボリュームを作成する。
- 物理ボリュームからボリュームグループを作成する。
- ボリュームグループから論理ボリュームを作成し、論理ボリュームマウントポイントを割り当てる。

注意

LVMボリュームグループは、GUIインストールモードでのみ編集できます。テキストモードインストールでは、既存の論理ボリュームにマウントポイントを割り当てる作業は可能です。

Red Hat Linuxインストール時に論理ボリュームで論理ボリュームグループを作成するには以下の工程を実行します：

1. **ディスクパーティション設定**画面で、**Disk Druidを使用して手動でパーティションを設定**を選択します。
2. **新規**を選択します。
3. ここではマウントポイントの入力は出来ません。(ボリュームグループが作成されると可能になります)
4. 図11-1に示してあるように、**ファイルシステムタイプ**のプルダウンメニューから**物理ボリューム(LVM)**を選択します。

図11-1. 物理ボリュームの作成

5. 物理ボリュームは1つのドライブに拘束されなければなりません。**使用可能なドライブ**用に、物理ボリュームを作成するドライブを選択します。複数のドライブがある場合、全てのドライブがここで選択できますが、選択する1つのドライブ以外は選択解除します。
6. 物理ボリュームに与える容量を入力します。
7. **固定容量**を選択して、指定のサイズの物理ボリュームを作成するか、**指定限度まで使用(MB)**を選択して物理ボリュームの範囲を指定するサイズをメガバイト数で入力するか、あるいは**最大許容量まで使用**を選択してハードディスク上の使用可能な全容量まで後で成長するようにもできます。1つ以上を成長可能にするとそれらの物理ボリューム同士でディスク上の空き領域を共有することになります。
8. パーティションをプライマリパーティションとする場合は、**プライマリパーティションにする**を選択してください。
9. フォーマットの前にインストールプログラムでハードドライブ上の不良ブロックを確認するには、**不良ブロックをチェック**を選択します。
10. **OK**をクリックしてメインの画面に戻ります。

LVM設定の為に必要なだけの複数の物理ボリュームを作成するには上記のステップを繰り返します。例えば、ボリュームグループを1つ以上のドライブに広げたい場合は、ドライブ毎に1つの物理ボリュームを作成します。

警告

ブートローダーはボリュームグループを読み取れない為、`/boot`パーティションはボリュームグループ上に存在出来ません。ルート`/`パーティションを論理ボリューム上に位置する場合は、`/boot`パーティションはボリュームグループの一部ではない別の場所に作成する必要があります。

全ての物理ボリュームが作成された後は、次のステップに従います：

1. **LVM**ボタンをクリックして、ボリュームグループ内へ物理ボリュームを集めます。ボリュームグループは基本的に物理ボリュームの集合体です。複数の論理ボリュームグループを所有出来ますが、1つの物理ボリュームは1つのボリュームグループ内にのみ存在できます。

注意

論理ボリュームグループの中には、運営用のディスクスペースが確保されています。その為、物理ボリュームの合計がボリュームグループの容量と同じでなくても表示される論理ボリュームの容量は正しいことになります。

図11-2. LVMデバイスの作成

2. 好みに応じて**ボリュームグループ名**は変更できます。
3. ボリュームグループのすべての論理ボリュームは物理エクステント単位で割り当てる必要があります。デフォルトでは、物理エクステントは4 MBに設定してあります。その為、論理ボリュームの容量は4 MBで割り切れる数字でなければなりません。4 MB単位ではない容量を入力した場合、インストールプログラムは自動的に近い4MB単位の容量を選択します。この設定を変更することは推薦できません。
4. ボリュームグループ用に使用する物理ボリュームを選択します。
5. /homeなどのマウントポイントで論理ボリュームを作成します。/bootは論理ボリュームになれない事を忘れないで下さい。論理ボリュームを追加するには、**論理ボリューム** セクションの**追加**ボタンをクリックします。すると図11-3に示されているようなダイアログウィンドウが表示されます。

図11-3. 論理ボリュームの作成

作成したいボリュームグループ毎にこのステップを繰り返します。


ヒント

将来、論理ボリュームを拡張できるように論理ボリュームグループに空き領域を残しておくとよいでしょう。

図11-4. 論理ボリューム作成完了

III. ネットワーク関連の設定

この章では、ネットワーク設定方法の説明、その後にリモートログインの許可方法、ネットワークでのファイルとディレクトリの共有、Web サーバーの設定などのネットワーク関連の事項について説明します。

目次

第12章

ネットワーク設定

コンピュータがほかのコンピュータと通信するには、ネットワーク接続が必要です。このためには、オペレーティングシステムにインターフェースカード(イーサネット、ISDNモデム、トークンリングなど)を認識させ、ネットワークに接続するようにインターフェースを設定します。

ネットワーク管理ツールは、以下のような種類のネットワークインターフェースの設定に使用できます。

- イーサネット
- ISDN
- モデム
- xDSL
- トークンリング
- CIPE
- ワイヤレスデバイス

ネットワーク管理ツールを使用するには、root権限を持っている必要があります。アプリケーションをスタートするには、**メインメニュー**(パネル上) => **システム設定** => **ネットワーク**の順で進むか、シェルプロンプト(例、**XTerm**または **GNOME terminal**)に`redhat- config-network`とコマンドを入力します。コマンドをタイプする場合、Xが実行していればグラフィカルバージョンが表示されますが、それ以外はテキストベースのバージョンが表示されます。強制的にテキストバージョンを実行するには、`redhat-config- network-tui`コマンドを使用します。

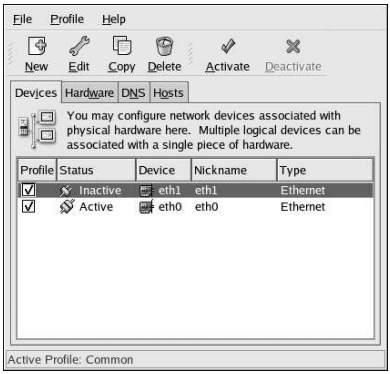


図12-1. ネットワーク管理ツール

設定ファイルを直接変更する場合、その場所と内容を調べるには、*Red Hat Linux* 参照ガイドを参照してください。

ヒント

Red Hat Linuxでハードウェアデバイスがサポートされているかを調べるには、Red Hatハードウェア互換の一覧、http://hardware.redhat.com/hcl/、を参照してください。

12.1. 概要

ネットワーク管理ツールでネットワーク接続を設定するには、以下のステップを実行します。

1. ハードウェアの一覧に物理ハードウェアデバイスを追加します。
2. 物理ハードウェアデバイスに関連付けられたネットワークデバイスを追加します。
3. ホスト名とDNSを設定します。
4. DNSで検索できないホストを設定します。

本章では、ネットワーク接続のタイプごとに各手順を説明します。

12.2. イーサネット接続の確立

イーサネット接続を確立するには、NIC(ネットワークインターフェースカード)、ネットワークケーブル(通常はカテゴリ5ケーブル)、接続先のネットワークが必要です。ネットワークの速度は異なるため、NICが接続先のネットワークと互換性があることを確認します。

イーサネット接続を追加するには、以下の手順に従います。

1. **デバイス**タブをクリックします。
2. ツールバーの**新規**ボタンをクリックします。
3. **デバイスタイプ**一覧から**イーサネット接続**を選択して、**進む**ボタンをクリックします。
4. ハードウェアの一覧にすでにネットワークインターフェースカードが追加されている場合は、**イーサネットカード**の一覧でイーサネットカードを選択します。それ以外は、**他のイーサネットカード**を選択してハードウェアデバイスを追加します。

注意

通常、インストールプログラムによって、サポートされているイーサネットデバイスが検出され、設定をするように求められます。イーサネットデバイスをインストール時に設定した場合は、**ハードウェア**タブのハードウェア一覧に表示されます。

5. **他のイーサネットカード**を選択した場合は、**イーサネットアダプタを選択** ウィンドウが表示されます。イーサネットカードのメーカーとモデルを選択し、デバイス名を選択します。このイーサネットカードがシステムにとって初めての場合なら、デバイス名に**eth0**を選択し、2番目の場合なら**eth1**を選択します。**ネットワーク管理ツール**を使用して、NICのリソースを設定することもできます。**進む**ボタンをクリックして作業を続行します。
6. 図12-2で示しているように、**ネットワークの設定**のウィンドウで、DHCPか静的IPアドレスのどちらかを選択します。ネットワークを接続するたびにデバイスにさまざまなIP アドレスが割り当てられる場合は、ホスト名を指定しないでください。**進む**をクリックして続けます。
7. **イーサネットデバイスの作成** ページで**適用**をクリックします。

図12-2. イーサネットの設定

イーサネットのデバイス設定が完了すると、図12-3のように、デバイス一覧に表示されます。

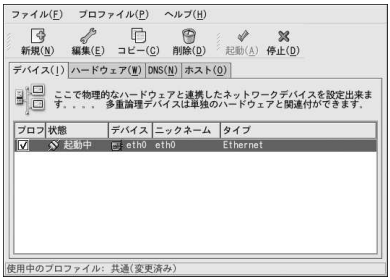


図12-3. イーサネットデバイス

ファイル => **保存** の順で選択して、必ず変更を保存してください。

イーサネットデバイスの追加後に、デバイスの一覧からデバイスを選択して**編集**をクリックすると、設定を編集することができます。たとえば、デバイスを追加したときに、デフォルトでは起動時に開始されるよう設定されます。この設定を変更するには、デバイスを選択して編集し、**コンピュータの起動時にデバイスを起動**、値を修正、変更を保存します。

デバイスが追加されたとき、**無効** ステータスで表示されるように、すぐには起動しません。デバイスを起動するには、そのデバイスをデバイス一覧から選択して**起動**ボタンをクリックします。コンピュータが開始するとき(デフォルト)、システムがデバイスを起動するよう設定されている場合は、この手順を再度行なう必要はありません。

イーサネットカードで複数のデバイスを使用する場合、2番目以降のデバイスはデバイスエイリアスになります。デバイスエイリアスは、物理的にひとつのデバイスで複数の仮想デバイスを設定することができます。従って、ひとつの物理的デバイスに複数のIPアドレスを与えることができます。例えば、eht1デバイスとeth1:1デバイスを設定することができます。詳細については項12.13を参照してください。

12.3. ISDN接続の確立

ISDN接続とは、電話会社が設置した特殊な電話回線を通してISDN モデムカードで確立されるインターネット接続のことです。ISDN接続はヨーロッパで普及しています。

ISDN接続を追加するには、次の手順を実行します。

1. **デバイス**タブをクリックします。
2. ツールバーにある**新規**ボタンをクリックします。
3. **デバイスタイプ**一覧から**ISDN 接続**を選択して**進む**をクリックします。
4. プルダウンメニューからISDNアダプタを選択します。アダプタ用のリソースとDチャンネルプロトコルを設定します。**進む**ボタンをクリックして続行します。

図12-4. ISDNの設定

5. 使用しているISPが設定済ISP一覧にある場合は、それを選択します。なければ、ISPアカウント作成の必要情報を入力します。値がわからない場合はISPに問い合わせてください。**進む**をクリックします。
6. **IP設定**ウィンドウで、**カプセル化モード**を選択して、DHCP経由でIPアドレスを取得するか、静的IPアドレスを設定します。完了したら**進む**をクリックします。
7. **ダイアルアップ接続の作成**ページで、**適用**をクリックします。

設定が完了したISDNデバイスは、図12-5 のように、**ISDN**タイプのデバイスとしてデバイスの一覧に表示されます。

ファイル => **保存** の順で選択して、必ず変更を保存してください。

ISDNデバイスを追加したら、デバイスの一覧からデバイスを選択して**編集**をクリックすると、設定を編集することができます。たとえば、デバイスを追加したときに、デフォルトでは起動時に実行が開始されないように設定されます。この設定を編集して変更することができます。圧縮、PPPオプション、ログイン名、パスワードなども変更することができます。

デバイスが追加されたとき、**無効** ステータスで表示されるように、すぐには起動しません。デバイスを起動するには、そのデバイスをデバイス一覧から選択して**起動**ボタンをクリックします。コンピュータが開始するとき(デフォルト)、システムがデバイスを起動するよう設定されている場合は、この手順を再度行なう必要はありません。

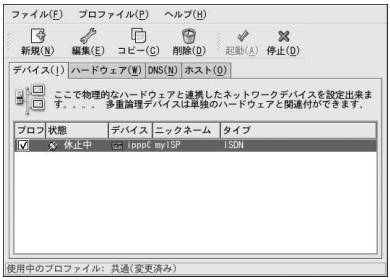


図12-5. ISDNデバイス

12.4. モデム接続の確立

モデムを使用すると、有効な電話回線によるインターネット接続を設定することができます。ISP(インターネットサービスプロバイダ)アカウント(ダイヤルアップアカウントとも呼ばれる) が必要です。

モデム接続を追加するには、次の手順を実行します。

1. **デバイス**タブをクリックします。
2. ツールバーにある**新規**ボタンをクリックします。
3. **デバイスタイプ**一覧から**モデム接続**を選択して**進む**をクリックします。
4. ハードウェア一覧(**ハードウェア** タブにある)に設定済みのモデムがすでにある場合、**ネットワーク管理ツール**は、モデム接続を確立するのにそのモデムが使用されるものと見なします。モデムが設定されていない場合は、システムにあるモデムを検出しようとします。この検索には少し時間がかかります。モデムが検出されない場合は、表示の設定は検索から検出された値ではありませんというメッセージを表示して警告します。
5. 検索されると、図12-6のようなウィンドウが表示されます。

図12-6. モデムの設定

6. モデムデバイス、ボードレート、フロー制御、モデム音量を設定します。値がわからない場合は、モデムが正常に検索されたらデフォルトのままにしてください。タッチトーンダイヤル方式でない場合は、該当するチェックボックスのチェックを外してください。**進む**をクリックします。

7. 使用しているISPが設定済ISP一覧にある場合は、それを選択します。ない場合は、ISPアカウント作成用の必要情報を入力します。値がわからない場合は、ISPに問い合わせてください。**進む**をクリックします。
8. **IP設定**ページで、DHCP経由でIPアドレスの取得を選択するか、静的IPアドレスに設定します。完了したら**進む**をクリックします。
9. **ダイアルアップ接続の設定**ページで、**適用**をクリックします。

モデムデバイスを設定したら、モデムタイプでデバイス一覧に、図12-7のように表示されます。

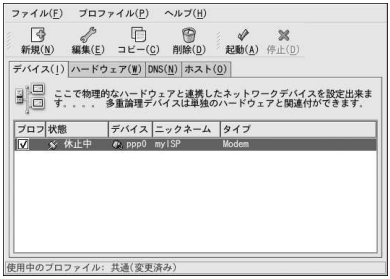


図12-7. モデムデバイス

ファイル => **保存** の順で選択して、必ず変更を保存してください。

モデムデバイスの追加後に、デバイスの一覧からデバイスを選択して**編集**をクリックすると、設定を編集することができます。たとえば、デバイスを追加したときに、デフォルトでは起動時に実行が開始されないように設定されています。この設定を編集して変更することができます。圧縮、PPPオプション、ログイン名、パスワードなども変更することができます。

デバイスが追加されたとき、**無効** ステータスで表示されるように、すぐには起動しません。デバイスを起動するには、そのデバイスをデバイス一覧から選択して**起動**ボタンをクリックします。コンピュータが開始するとき(デフォルト)、システムがデバイスを起動するよう設定されている場合は、この手順を再度行なう必要はありません。

12.5. xDSL接続の確立

DSL はDigital Subscriber Linesの略語です。ADSL、IDSL、SDSLなど数種のDSLタイプがあります。 **ネットワーク管理ツール**はすべてのDSL接続の種類を指してxDSLという言葉を使用します。

イーサネットカードを使用してDHCPからIPアドレスを取得するシステム設定が必要となるDSLプロバイダもあれば、イーサネットカードでPPPoE(Point-to-Point Protocol over Ethernet)接続の設定が必要になるDSLプロバイダもあります。接続方式については、DSLプロバイダに問い合わせてください。

DHCPを使用する必要がある場合、イーサネットカードの設定については、項12.2を参照してください。

PPPoEを使用する必要がある場合は、次の手順を実行します。

1. **デバイス**タブをクリックします。
2. **新規**ボタンをクリックします。
3. **デバイスタイプ**一覧から**xDSL接続**を選択して、**進む**をクリックします。

4. イーサネットカードがハードウェアの一覧にすでに表示されている場合は、図12-8 のプルダウンメニューで**イーサネットデバイス**を選択します。イーサネットカードが表示されていない場合は、**イーサネットアダプタの選択**ウィンドウが表示されます。

注意

インストールプログラムによって、サポートされているイーサネットデバイスが検出され、設定をするように求められます。イーサネットデバイスがインストール時に設定されている場合は、**ハードウェア**タブのハードウェアの一覧に表示されます。

図12-8. xDSLの設定

5. **イーサネットアダプタの選択** ウィンドウが表示された場合は、イーサネットカードの製造元とモデルを選択します。デバイス名を選択します。このイーサネットカードがシステムにとって初めてのイーサネットカードなら、デバイス名に**eth0**を選択し、2番目の場合なら**eth1**を選択します(以降同じ)。**ネットワーク管理ツール**を使用して、NICのリソースを設定することもできます。**進む**ボタンをクリックして続行します。
6. **プロバイダ名**、**ログイン名**、**パスワード**を入力します。T-Online アカウントがある場合は、デフォルトウィンドウに**ログイン名**や**パスワード**を入力する代わりに、**T-Onlineアカウントの設定**ボタンをクリックして必要な情報を入力します。**進む**をクリックして続行します。
7. **DSL 接続の設定**ページで、**適用**をクリックします。

DSL設定が完了すると、図12-7のようにDSL接続がデバイスの一覧に表示されます。

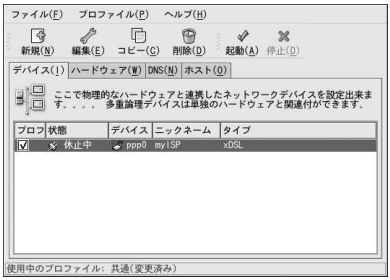


図12-9. xDSLデバイス

ファイル => **保存** の順で選択して、必ず変更を保存してください。

xDSL接続の追加後に、デバイスの一覧からデバイスを選択して**編集**をクリックすると、設定を編集することができます。たとえば、デバイスを追加したときに、デフォルトでは起動時に実行が開始されないように設定されています。この設定を編集して変更することができます。

デバイスが追加されたとき、**無効** ステータスで表示されるように、すぐには起動しません。デバイスを起動するには、そのデバイスをデバイス一覧から選択して**起動**ボタンをクリックします。コンピュータが開始するとき(デフォルト)、システムがデバイスを起動するよう設定されている場合は、この手順を再度行なう必要はありません。

12.6. トークンリング接続の確立

トークンリングネットワークとは、すべてのコンピュータが環状に接続されているネットワークのことです。トークンまたは特殊なネットワークパケットが、トークンリングに沿って伝送され、コンピュータが情報をやり取りすることができます。

ヒント

Linuxでトークンリングを使用する方法については、*Linux Token Ring Project* Webサイトの http://www.linuxtr.netを参照してください。

トークンリング接続を追加するには、次の手順を実行します。

1. **デバイス**タブをクリックします。
2. ツールバーにある**新規**ボタンをクリックします。
3. **デバイスタイプ**一覧から**トークンリング接続**を選択して、**進む**ボタンをクリックします。
4. ハードウェアの一覧にすでにトークンリングカードを追加されている場合は、**トークンリングカード** の一覧でトークンリングカードを選択します。トークンリングカードが追加されていない場合は、**他のトークンリングカード**を選択してハードウェアデバイスに追加します。
5. **他のトークンリングカード**を選択した場合、図12-10 で示されるような**トークンリングアダプタの選択**ウィンドウが表示されます。アダプタのメーカーとモデルを選択します。デバイス名を選択します。このトークンリングカードがシステムにとって初めてのトークンリングカードなら、デバイス名に**tr0**を選択し、2番目なら**tr1**を選択します(以降同じ)。**ネットワーク管理ツール**を使用して、アダプタのリソースをユーザーが設定することもできます。**進む**をクリックして続行します。

図12-10. トークンリングの設定

6. **ネットワークの設定**ページで、DHCPを使用するか、静的IPアドレスを使用するか選択します。デバイス用のホスト名も指定できます。このデバイスがネットワークのスタートの度に動的アドレスを受け取る場合は、ホスト名を指定しないでください。**進む** クリックして続けます。
7. **トークンリングデバイスの作成**のページで**適用**をクリックします。

トークンリングデバイスの設定が完了すると、図12-11のようにトークンリングデバイスがデバイスの一覧に表示されます。

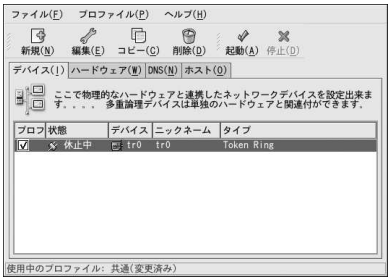


図12-11. トークンリングデバイス

ファイル => **保存** の順で選択して、必ず変更を保存してください。

デバイスの追加後に、デバイスの一覧からデバイスを選択して**編集**をクリックすると、設定を編集することができます。たとえば、起動時にデバイスを開始するかどうかを設定することができます。

デバイスが追加されたとき、**無効** ステータスで表示されるように、すぐには起動しません。デバイスを起動するには、そのデバイスをデバイス一覧から選択して**起動**ボタンをクリックします。コンピュータが開始するとき(デフォルト)、システムがデバイスを起動するよう設定されている場合は、この手順を再度行なう必要はありません。

12.7. CIPE接続の確立

CIPEは、Crypto IP Encapsulationの略です。IPトンネルデバイスを設定するために使用されます。たとえば、CIPEは、外部からVPN (Virtual Private Network)へのアクセスを許可するときに使用します。CIPEデバイスのセットアップをする場合は、正しい値についてシステム管理者にお問い合わせください。

図12-12. CIPEの設定

ヒント

CIPE及びCIPEの設定に関する詳細は、*Red Hat Linux* セキュリティガイドを参照してください。

12.8. ワイヤレス接続の確立

ワイヤレスイーサネットデバイスは、徐々に普及してきています。ワイヤレスデバイスの設定はイーサネットの設定と似ていますが、SSIDやワイヤレスデバイス用のキーなどの設定ができる点で異なります。

ワイヤレスイーサネット接続を追加するには、次の手順を実行します。

1. **デバイス**タブをクリックします。
2. ツールバーにある**新規**ボタンをクリックします。
3. **デバイスタイプ**一覧から**ワイヤレス接続**を選択して、**進む**ボタンをクリックします。
4. ハードウェアの一覧にすでにワイヤレスネットワークインターフェースカードを追加している場合は、**ワイヤレスカード**の一覧でワイヤレスネットワークインターフェイスカードを選択します。追加されていない場合は、**他のワイヤレスカード**を選択してハードウェアデバイスを追加します。

注意

通常、インストールプログラムによって、サポートされているワイヤレスイーサネットデバイスが検出され、設定をするように求められます。ワイヤレスイーサネットデバイスがインストール時に設定されている場合は、**ハードウェア**タブのハードウェアの一覧に表示されます。

5. **他のワイヤレスカード**を選択した場合は、**イーサネットアダプタの選択** ウィンドウが表示されます。イーサネットカードのメーカーとモデル、デバイス名を選択します。このカードがシステムにとって初めてのイーサネットカードなら、デバイス名に**eth0**を選択し、2番目なら**eth1** を選択します(以降同じ)。**ネットワーク管理ツール**を使用して、ワイヤレスネットワークインターフェースカードのリソースをユーザーが設定することもできます。**進む** をクリックして続行します。
6. 図12-13の**ワイヤレス接続の設定**ページで、ワイヤレスデバイス用の設定をします。

図12-13. ワイヤレス設定

7. **ネットワークの設定**ページで、DHCPか静的IPアドレスのどちらかを選択します。デバイスのホスト名を指定することもできます。ネットワークを接続するたびにデバイスに動的IPアドレスが割り当てられる場合は、ホスト名を指定しないでください。**進む**をクリックして続行します。
8. **ワイヤレスデバイスの作成**ページで**適用**をクリックします。

ワイヤレスデバイスの設定が完了すると、ワイヤレスデバイスが図12-14に示すようにデバイスの一覧に表示されます。

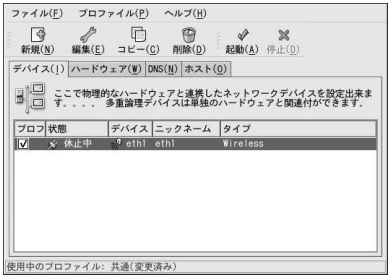


図12-14. ワイヤレスデバイス

ファイル => **保存** の順で選択して、必ず変更を保存してください。

ワイヤレスデバイスの追加後に、デバイスの一覧からデバイスを選択して**編集**をクリックすると、設定を編集することができます。たとえば、起動時にデバイスを有効にするかどうかを設定することができます。

デバイスが追加されたとき、**無効** ステータスで表示されるように、すぐには起動しません。デバイスを起動するには、そのデバイスをデバイス一覧から選択して**起動**ボタンをクリックします。コンピュータが開始するとき(デフォルト)、システムがデバイスを起動するよう設定されている場合は、この手順を再度行なう必要はありません。

12.9. DNS設定の管理

DNSタブは、システムのホスト名、ドメイン、ネームサーバー、検索ドメインを設定します。ネームサーバーはネットワーク上のほかのホストを調べるときに使用します。

DNSサーバー名がDHCPまたはPPPoEからリトリーブされる場合は(あるいは、ISPからリトリーブされる場合は)、1番目、2番目、3番目のDNSサーバーを追加しないでください。

ホスト名がDHCPまたはPPPoEから動的にリトリーブされる場合は(あるいは、ISPからリトリーブされる場合)、ホスト名を変更しないでください。

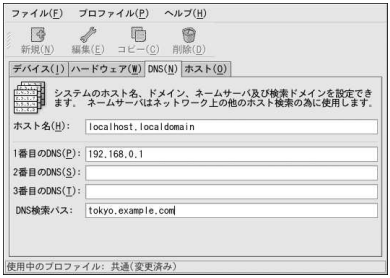


図12-15. DNSの設定

注意

ネームサーバーセクションでは、システムをネームサーバーとして設定しないことに注意してください。その代わり、IPアドレスを決定してホスト名に変換するとき、またはホスト名を決定してIPアドレスに変換するときにこのセクションでネームサーバーを設定します。

12.10. ホストの管理

ホストタブでは、`/etc/hosts` ファイルからホストの追加、編集、削除を行うことができます。このファイルには、IPアドレスと対応するホスト名が含まれています。

システムがホスト名を決定してIPアドレスに変換するときや、IPアドレスのホスト名を決定するとき、(デフォルトのRed Hat Linux設定を使用している場合)ネームサーバーを使用する前に `/etc/hosts`ファイルを参照します。そのIPアドレスが`/etc/hosts`ファイルにある場合、ネーム

サーバーは使用されません。DNSに登録されていないIPアドレスを持ったコンピュータがネットワークにある場合、/etc/hostsファイルにそのIPアドレスを追加することをお勧めします。

/etc/hostsファイルにエントリを追加するには、**ホスト**タブへ行き、ツールバーある **新規**ボタンをクリックして、必要な情報を提供し**OK**をクリックします。**ファイル** => **保存**の順で選択するか、[Ctrl]-[S]キーを同時に押して/etc/hosts ファイルに対する変更を保存します。ネットワークまたはネットワークサービスは、アドレスが変換される度に現在のファイルのバージョンが対応するので、再スタートする必要はありません。

警告

localhost項目は削除しないでください。システムにネットワーク接続がない場合、あるいは常に稼動しているネットワーク接続がある場合でも、ローカルホストループバックインターフェース経由でシステムに接続する必要のあるプログラムがある場合があります。

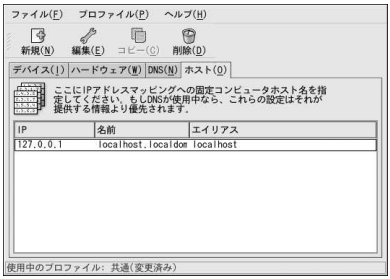


図12-16. ホストの設定

ヒント

検索順序を変更するには、/etc/host.conf ファイルを編集します。order hosts, bind の行は、/etc/hostsがネームサーバーに優先することを指定しています。order bind, hostsの行を変更すると、最初にネームサーバーを使用してホスト名とIPアドレスが決定されます。ネームサーバーでIPアドレスが決定できない場合は、/etc/hostsファイルでIPアドレスを探します。

12.11. デバイスの起動

ネットワークデバイスはブート時に起動する、または起動しないように設定することができます。例えば、モデム接続用のネットワークデバイスは通常、ブート時に起動するように設定されていませんが、イーサネット接続は通常、ブート時に起動するようになっています。ご使用のネットワークデバイスがブート時に起動しない設定になっている場合は、**Red Hat コントロールネットワーク**を使用して、ブートしたら起動するようにできます。この設定を始めるには、(パネル上の)**メインメニューボタン** => **システムツール** => **ネットワークデバイスのコントロール**と選択していきます。または、redhat-control-networkとコマンドを入力します。

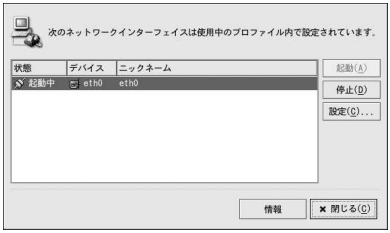


図12-17. デバイスの起動

デバイスを開始するには、それを一覧から選択して**起動**ボタンをクリックします。停止するには、一覧から選択して**停止** ボタンをクリックします。

複数のネットワークプロファイルが設定されている場合は、インターフェースに表示されているので起動することができます。詳細については項12.12を参照してください。

12.12. プロファイルの作業

各物理ハードウェアデバイス用に複数の論理ネットワークデバイスが作成できます。例えば、システム内にひとつだけイーサネットカードがある場合(eth0)、別のニックネームと別の設定オプションで論理ネットワークデバイスを作成し、それをすべてeth0に関連付けることができます。

論理ネットワークデバイスはデバイスエイリアスとは異なります。同一物理デバイスに所属する論理ネットワークデバイスは、別々のプロファイルで存在する必要があり、同時に起動することはできません。デバイスエイリアスも同じ物理ハードウェアデバイスに属しますが、同一物理ハードウェアデバイスのデバイスエイリアスは同時に起動することが可能です。デバイスエイリアスの作成に関する詳細は、項12.13を参照してください。

プロファイルは、異なるネットワーク用に複数の設定セットを作成するのに使用されます。設定セットは論理デバイスだけでなくホストやDNSの設定も含むことができます。プロファイルを設定した後は、**ネットワーク管理ツール**を使用して、複数のプロファイルを切替えることができます。

デフォルトでは、**共通**と呼ばれるプロファイルがひとつだけあります。新規のプロファイルを作成するには、プルダウンメニューから**プロファイル** => **新規**を選択し、そのプロファイル用に独自の名前を入力します。

メインウィンドウの下部にあるステータスバーで表示されるように、新規のプロファイルを修正しています。

すでに一覧にあるデバイスをクリックして、**コピー**ボタンをクリックして既存のデバイスを論理ネットワークデバイスにコピーします。**新規**ボタンを使用すると、正しくないネットワークエイリアスが作成されます。論理デバイスのプロパティを変更するには、そのデバイスを一覧から選択して**編集**をクリックします。例えば、すぐにわかるよう、**eth0_office**などニックネームをわかりやすい名前に変更することができます。

デバイスの一覧の中に、**プロファイル**とラベルの付いたチェックボックスの列があります。それぞれのプロファイル用に、デバイスに対しチェックを入れたり外したりすることができます。チェックのあるデバイスのみが現在選択中のプロファイルに含まれます。例えば、**Office** と呼ばれるプロファイルに**eth0_office**と言う名前の論理デバイスを作成して、そのプロファイルが選択された場合にその論理デバイスを起動したい場合、`eth0` デバイスのチェックをはずし、 `eth0_office`デバイスにチェックを入れます。

例えば、図12-18では、**eth0_office**の論理デバイスを持つ **Office**と呼ばれるプロファイルを示しています。DHCPを使用して最初のイーサネットカードを起動するよう設定されています。

図12-18. オフィスプロファイル

図12-19に表示してあるように、**ホーム**プロファイルは**eth0_home** 論理デバイスを起動します。これは`eth0` と関連しています。

図12-19. ホームプロファイル

また、`eth0`を**オフィス**プロファイルでのみ起動するよう設定して、ppp(モデム) デバイスを**ホーム**プロファイルでのみ起動するよう設定することもできます。もうひとつの例は、**共通**プロファイルで`eth0` を起動して、旅行中に使用するために**Away**プロファイルでpppデバイスを起動するよう設定したプロファイルです。

プロファイルはブート時に起動できません。**共通** プロファイル(デフォルトのプロファイル)でブート時に起動するよう設定したデバイスだけがブート時に起動します。システムがブートしたら、**メインメニュー** (パネル上) => **システムツール** => **ネットワークデバイスのコントロール** (または、`redhat-control- network`とコマンドを入力)の順で進み、プロファイルを選択して起動します。デフォルトの**共通** インターフェース以外にもプロファイルが存在する場合にのみ、プロファイルの起動セクションが**ネットワークデバイスのコントロール**インターフェース内に表示されます。

代わりに、次のコマンドを実行してプロファイルを有効にできます(<*`profilename`*>にプロファイル名を置き換える)。

```
redhat-config-network-cmd --profile <profilename> --activate
```

12.13. デバイスエイリアス

デバイスエイリアスは、同一の物理ハードウェアに属する仮想デバイスですが、異なるIPアドレスを持つことで同時に起動することができます。これらのデバイスは通常、コロンと数字が後ろに付くデバイス名で表示されます(例、eth0:1)。ひとつのネットワークカードしかないシステムで、複数のIP アドレスを持ちたい場合に役に立ちます。

eth0などイーサネットデバイスを設定した後、静的IPアドレス(DHCPはエイリアスで動作しません)を使用するには、**デバイス**タブへ行き、**新規**をクリックします。イーサネットカードを選択してエイリアスで設定し、静的IPアドレスをエイリアス用にセットします。**適用**をクリックして作成します。イーサネットカード用のデバイスがすでに存在するので、作成したものは`eth0:1`などのエイリアスになります。

警告

イーサネットデバイスがエイリアスを持つように設定している場合は、デバイスもエイリアスもDHCPを使用するようには設定できません。IPアドレスを手動で設定する必要があります。

図12-20で、`eth0` デバイス用の任意のエイリアスを例として示しています。`eth0:1`デバイスに注意してください— `eth0`用の1番目のエイリアス。`eth0`用の2番目のエイリアスはデバイス名が`eth0:2`になります(以降同じ)。ブート時に起動するかどうか、エイリアス番号、などデバイスエイリアスの設定を修正するには、一覧からそのデバイスエイリアスを選択して**編集**ボタンをクリックします。

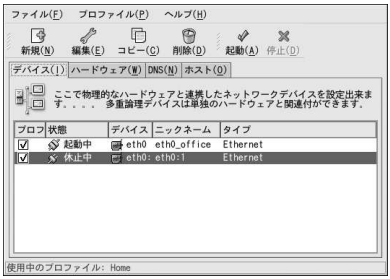


図12-20. ネットワークデバイスエイリアスの例

エイリアスを選択して**起動**ボタンをクリックしてエイリアスを起動します。複数のプロファイルを設定している場合、どのプロファイルがどの設定に入るか選択します。

エイリアスが起動していることを確認するには、コマンド `/sbin/ifconfig`を使用します。その出力が異なるIP アドレスのデバイスとデバイスエイリアスを表示するはずです。

```
eth0   Link encap:Ethernet HWaddr 00:A0:CC:60:B7:G4
     inet addr:192.168.100.5 Bcast:192.168.100.255 Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
     RX packets:161930 errors:1 dropped:0 overruns:0 frame:0
     TX packets:244570 errors:0 dropped:0 overruns:0 carrier:0
     collisions:475 txqueuelen:100
     RX bytes:55075551 (52.5 Mb) TX bytes:178108895 (169.8 Mb)
     Interrupt:10 Base address:0x9000

eth0:1  Link encap:Ethernet HWaddr 00:A0:CC:60:B7:G4
     inet addr:192.168.100.42 Bcast:192.168.100.255 Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
     Interrupt:10 Base address:0x9000

lo    Link encap:Local Loopback
     inet addr:127.0.0.1 Mask:255.0.0.0
     UP LOOPBACK RUNNING MTU:16436 Metric:1
     RX packets:5998 errors:0 dropped:0 overruns:0 frame:0
     TX packets:5998 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:0
RX bytes:1627579 (1.5 Mb) TX bytes:1627579 (1.5 Mb)
```

第13章

基本的なファイアウォール設定

火災の延焼を防止するビルの防火壁と同じように、コンピュータのファイアウォールは、コンピュータウィルスの侵入を防ぎ、不正なユーザーからアクセスされないようにします。ファイアウォールは、コンピュータとネットワークの間に置きます。ファイアウォールでは、ネットワーク上のリモートユーザーがアクセスできるようにするサービスを指定します。ファイアウォールを適切に設定すると、システムのセキュリティを大幅に高めることができます。インターネットに接続されているRed Hat Linuxシステムにはファイアウォールを適切に設定することをお勧めします。

13.1. セキュリティレベル設定ツール

Red Hat Linuxのインストール時に表示される**ファイアウォール設定**画面では、セキュリティレベルを[高]、[中]、[なし]から選択するオプションがあり、また特定のデバイス、着信サービス、ポートだけを許可するオプションもあります。

セキュリティレベル設定ツールを使用すると、インストールの後でもシステムのセキュリティレベルを変更することが出来ます。ウィザードベースのアプリケーションをお好みの場合は項13.2を参照して下さい。

このアプリケーションを開始するには、パネル上から**メインメニュー**=> **システムツール** =>**セキュリティレベル設定**と選択していきます。又はシェルプロンプト(XTermやGNOMEターミナルなど)でコマンド`redhat-config-securitylevel`を入力します。

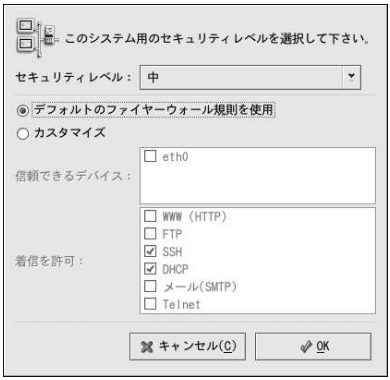


図13-1. セキュリティレベル設定ツール

プルダウンメニューから目的のセキュリティレベルを選択します。

高

‘ **高**を選択すると、システムはユーザが明示的に定義した接続以外(及びデフォルト設定以外)は受け付けられなくなります。デフォルトでは以下の接続のみが許可されます：

- DNS 応答
- DHCP — DHCP を使う任意のネットワークインタフェースは適切に設定できます。

高を使うと、ファイアウォールが以下を許可されません：

- アクティブモードFTP (ほとんどのクライアントで標準で使われているパッシブモードFTPは、適切に動作するはずです)
- IRC DCC ファイル転送
- RealAudio™
- リモートX Window System クライアント

システムをインターネットに接続していても、サーバの運用計画がないなら、これが最も安全な選択肢です。追加サービスが必要な場合は、**カスタマイズ** を選択して、特定サービスにファイアウォールの通過を許可できます。

注意

「中」又は「高」のファイアウォールを選択すると、ネットワーク認証(NIS とLDAP)は正常に動作しません。

中

‘ **中**を選択すると、ファイアウォールはリモートマシンがシステム内の特定のリソースにアクセスできないようにします。デフォルトでは、次のようなリソースへのアクセスが拒否されます：

- 1023以下のポート—**FTP, SSH**,**telnet**,**HTTP, NIS**などのほとんどのシステムサービスで使用される標準予約のポート。
- NFS サーバポート(2049) — NFS はリモートサーバもローカルクライアントも両方無効になります。
- リモートX クライアント用のローカルX Window System ディスプレイ
- X フォントサーバポート(デフォルトでは**xfs**はネットワークをリッスンしません；フォントサーバ内で無効になっています。)

RealAudio™などのリソースを許可し、一方で通常のシステムサービスへのアクセスを阻止したい場合は**中**を選択します。**カスタマイズ**を選択すると特定サービスにファイアウォールの通過を許可できます。

注意

「中」又は「高」のファイアウォールを選択すると、ネットワーク認証(NIS とLDAP)は正常に動作しません。

なし

‘ 「なし」の設定は、全体的なアクセスを許可します。セキュリティチェックは特定のサービスへのアクセスを無効にする機能ですが、この設定では、セキュリティチェックを実行しません。信頼できるネットワーク(インターネットではなく) 上にいるとき、または後でより詳細なファイアウォール設定を実行する予定があるときに限り、この項目の選択を推奨します。

カスタマイズを選択することで、信頼するデバイスを追加するか、又は追加の進入サービスの許可をすることができるようになります。

信頼するデバイス

‘ **信頼するデバイス**として選択したデバイスはファイアウォール規則から除外され、そのデバイスからのトラフィックはすべて許可されます。たとえば、ローカルネットワークを運用していて、PPP ダイヤルアップ経由でインターネットも接続している場合、**eth0**にチェックを付けると、ローカルネットワークからの通信は許可されます。**eth0**を信頼できるデバイスとして選択す

ることは、イーサネットからのすべてのトラフィックは許可し、ppp0インターフェイスにはまだファイアウォール阻止があるという意味になります。ですから、あるインターフェイス上のトラフィックを制限するには、それにチェックを付けないでおく必要があります。

インターネットなどの公衆通信回線と接続したデバイスを**信頼するデバイス**に選択するのは推奨できません。

進入を許可

‘ このオプションを有効にすると、指定したサービスにファイアウォールの通過を許可します。ワークステーションインストールでは、これらのサービスの大部分はシステム上に存在しないことに注意してください。

DHCP

‘ これはDHCP クエリと応答を許可し、DHCP を使ってIP アドレスを決定する任意のネットワークインタフェースを許可します。通常、DHCP は有効にされています。DHCPが有効でない場合、コンピュータはIP アドレスを取得することができません。

SSH

‘ *S*ecure *SH*ell (SSH)は、リモートマシン上でのログインやコマンド実行のためのツールのパッケージです。ファイアウォールを通過してマシンにアクセスするためにSSHツールを使用する計画であれば、リモートマシンにアクセスする為に`openssh-server`パッケージをインストールしておく必要があります。

Telnet

‘ Telnet はリモートマシンにログインするためのプロトコルです。暗号化されないので、ネットワーククラッキング攻撃に対するセキュリティが脆弱です。telnetに進入許可を与えるのは推奨されません。telnetに進入を許可したい場合は、`telnet-server`パッケージをインストールしておく必要があります。

WWW (HTTP)

‘ HTTP は、Apache(又は他のWebサーバ)でWeb ページを提供するために使うプロトコルです。Web サーバを公開する予定がある場合は、このオプションを有効にします。ページをローカルで参照するかWeb ページを開発するには、このオプションは必要ありません。Web ページを提供するには、`apache`パッケージをインストールしておく必要があります。

WWW (HTTP)を有効にすることだけではHTTP用のポートは開けません。使用できるようにするには**他のポート**フィールドでポートを指定する必要があります。

メール(SMTP)

‘ これは受信SMTP メール配信を許可します。リモートホストと使用マシンの直接接続を許可してメール配信する必要があるときは、このオプションを有効にします。POP3 またはIMAP によってISPのサーバからメールを収集するとき、または**fetchmail** などのツールを使うときはこのオプションを有効にする必要はありません。不適切にSMTP サーバを設定すると、リモートマシンにユーザーのサーバを使ったスパム送信を許してしまう可能性があることに注意してください。

FTP

‘ FTP はネットワーク上のマシン間でのファイル転送用に使われるプロトコルです。FTPサーバを公開する予定がある場合は、このオプションを有効にします。このオプションを利用するには`vsftpd`パッケージをインストールしておく必要があります。

ファイアウォールを有効にするには**OK**ボタンをクリックします。クリックした後は、選択されたオプションは、`iptables`コマンドに翻訳され、`/etc/sysconfig/iptables` ファイルに書き込まれま

す。iptablesサービスも開始されて、選択したオプションを保存するとすぐにファイアウォールが有効になります。

警告

/etc/sysconfig/iptablesファイルの中で、ファイアウォールを設定したりファイアウォール規則を持っている場合は、ユーザーがファイアウォールを**なし**に選択して**OK**ボタンを押して変更を保存すると、このファイルは削除されます。

選択されたオプションは/etc/sysconfig/redhat-config-securitylevelファイルにも書き込まれるため、次回アプリケーションが起動される時にその設定を復元できます。このファイルは手動で編集しないで下さい。

ブート時に自動的にiptablesサービスを起動させるには、項13.3で詳細を参照して下さい。

13.2. GNOME Lokkit

GNOME Lokkitでは、基本的なiptablesネットワーク規則を作成することによって、標準的ユーザーのファイアウォール設定を行うことができます。このプログラムでは、規則を書き込む代わりに、ユーザーに対してシステムの使用に関する一連の質問を行い、それをファイル/etc/sysconfig/iptablesに書き込みます。

GNOME Lokkitを使用して複雑なファイアウォール規則を作成することはおすすめできません。このプログラムは、モデム、ケーブル、DSLインターネット接続を使用するときに自分のシステムを保護したい標準的なユーザーを想定しています。詳細なファイアウォール規則の設定については、*Red Hat Linux* 参照ガイドの*iptables*を使用するファイアウォールの章を参照してください。

特定のサービスを無効にし、特定のホストやユーザーを拒否する方法については、第14章を参照してください。

GNOME Lokkitのグラフィカルバージョンを開始するには、**メインメニューボタン** => **システムツール** => **他のシステムツール** => **Lokkit**と選択していきます。又はシェルプロンプトでrootとしてコマンドgnome-lokkitを入力します。X Window Systemがインストールされていない場合や、テキストベースのプログラムを好む場合は、シェルプロンプトでlokkitコマンドを使用して、テキストモードバージョンを起動します。

13.2.1. 基本

図13-2. 基本

プログラムを起動した後、システムのための適当なセキュリティレベルを選択します。

- **高セキュリティ**—このオプションでは、ほとんどのネットワーク接続が無効となりますが、DNS応答とDHCPだけはネットワークインターフェイスが起動できるようにするため有効になります。IRC、ICQ、ほかのインターネットメッセージサービス、RealAudio™等は、プロキシがなければ機能しません。
- **低セキュリティ**—このオプションは、システムへのリモート接続（NFS接続やリモートX Window Systemセッションを含む）を禁止します。ポート1023より下のサービスは接続を受け付けません（FTP、SSH、Telnet、HTTP接続も受け付けられません）。
- **ファイアウォール無効**—このオプションでは、セキュリティ規則を作成しません。このオプションは、システムが信頼できるネットワーク上にある（インターネット上にはない）場合や、システムがより大規模なファイアウォールで保護されている場合、あるいはユーザーが自分のカスタムファイアウォール規則を作成する場合にだけ選択してください。このオプションを選択し、**次**ボタンをクリックしたら、項13.3に進みます。システムのセキュリティは変更されません。

13.2.2. ローカルホスト

システムにイーサネットデバイスがある場合は、**ローカルホスト**ページで、各デバイスへ送信される接続要求にファイアウォール規則を適用するかどうかを設定できます。このデバイスがシステムをファイアウォールで保護されているローカルエリアネットワークに接続し、インターネットに直接接続しない場合は、**はい**ボタンを選択します。イーサネットカードがシステムをケーブルまたはDSLモデムに接続する場合は、**いいえ**ボタンを選択することを推奨します。

図13-3. ローカルホスト

13.2.3. DHCP

システム上でDHCPを使用してイーサネットインターフェイスを有効にする場合は、DHCPについての質問に**はい**を選択しなければいけません。いいえを選択した場合、イーサネットインターフェイスを使用して接続を確立できません。多くのケーブルテレビやDSLインターネットプロバイダーは、DHCPを使用してインターネット接続を確立することを要求します。

図13-4. DHCP

13.2.4. サービスの設定

GNOME Lokkitではまた、一般的なサービスのオン/オフを切り替えることができます。サービスの設定について**はい**を選択した場合、以下のサービスに関するプロンプトが表示されます：

- **Webサーバー**—ユーザーのシステム上で実行しているWebサーバー（Apacheなど）への接続を許可する場合は、このオプションを選択します。自分のシステムまたはネットワーク上のほかのサーバーにあるページを表示する場合は、このオプションを選択する必要はありません。
- **着信メール**—システムで着信メールを受け取る必要がある場合は、このオプションを選択します。IMAP、POP3、またはfetchmailを使用して電子メールを検索する場合は、このオプションを選択する必要はありません。
- **セキュアシェル（ssh）**—SSH（Secure Shell）は、暗号化通信を介してリモートマシンにログインし、コマンドを実行するためのツールのセットです。SSHを通してリモートからマシンにアクセスする必要がある場合は、このオプションを選択します。
- **telnet**—telnetを使用すると、リモートからマシンにログインできます。しかし、これは安全なサービスではありません。このサービスは、ネットワークを介してプレーンテキスト（パスワードを含む）を送信します。リモートからマシンにログインする場合は、SSHを使用することを推奨します。システムにtelnetでアクセスする要求がある場合には、このオプションを選択します。

このほかの不要なサービスを無効にするには、**セキュリティレベル設定ツール**（項14.3を参照）、**ntsysv**（項14.4を参照）、`chkconfig`（項14.5を参照）のいずれかを使用します。

13.2.5. ファイアウォールの起動

完了ボタンをクリックすると、`/etc/sysconfig/iptables`内にファイアウォール規則が書き込まれ、`iptables`サービスをスタートすることによりファイアウォールが起動されます。

警告

`/etc/sysconfig/iptables`ファイルの中でファイアウォールを設定していたりファイアウォール規則を持っている場合、**ファイアウォール無効**を選択し、**完了**のボタンをクリックして変更を保存すると、そのファイルは削除されます。

GNOME Lokkitは必ずそのマシンで実行してください（リモートXセッションから実行するのは避けてください）。システムへのリモートアクセスを無効にした場合に、そのシステムにアクセスできなくなるか、またはファイアウォール規則が無効になります。

ファイアウォール規則を書き込まない場合は、**キャンセル**ボタンをクリックします。

13.2.5.1. メールリレー

メールリレー（転送）は、ほかのシステムからの電子メールの送信を仲介できるシステムです。ユーザーのシステムがメールリレーである場合は、誰かがそれを使用してユーザーのマシンからほかのシステムに対してスパムメールを送る危険性があります。

ファイアウォールを有効にするページの**完了**ボタンをクリックした後でメールサービスを有効にした場合、メールリレーのチェックが要求されます。**はい**を選択してメールリレーをチェックする場合、**GNOME Lokkit**は「*Mail Abuse Prevention System*」のWebサイト（http://www.mail-abuse.org/）に接続し、メールリレーテストプログラムを実行します。テストの結果は、テストが終了したとき表示されます。システムがメールリレーに利用できる場合は、Sendmailでそれを防止するように設定してください。

13.3. iptablesサービスの起動

ファイアウォール規則は、iptablesサービスを実行しているときだけ有効にされます。このサービスを手動で起動する場合は、次のコマンドを使用します：

```
/sbin/service iptables restart
```

システムがブートしたときに必ずこのサービスが起動するように、次のコマンドを発行します。

```
/sbin/chkconfig --level 345 iptables on
```

ipchainsサービスは、iptablesサービスと並行して動作することは出来ません。確実にipchainsサービスが無効になっていることを確認するには、以下のコマンドを実行します：

```
/sbin/chkconfig --level 345 ipchains off
```

サービス設定ツールを使用すれば、iptablesサービスとipchainsサービスを設定することができます。その詳細は項14.3 で御覧下さい。

第14章

サービスに対するアクセスの制御

Red Hat Linuxシステムのセキュリティを維持することが特に重要です。システムのセキュリティを管理する1つの方法として、システムのサービスに対するアクセスを注意深く管理することがあります。特定のサービスに対する公開アクセスを許可する必要があるかもしれません（たとえば、Webサーバーを運営する場合の`httpd`）。ただし、サービスを提供する必要がないならば、バグの影響を受ける可能性を最小限にするためサービスをオフにする必要があります。

システムサービスへのアクセスを管理する手段はいくつかあります。使用する手段は、サービス、システムの設定、Linuxに関するユーザーの専門知識のレベルに基づいて決定します。

サービスに対するアクセスを拒否するための最も簡単な方法は、単純にサービスをオフにすることです。`xinetd`によって管理されるサービス（このセクションの後半で説明します）と、`/etc/rc.d`階層内のサービスの起動/停止を設定するには、次の3つの異なるアプリケーションを使用します：

- **サービス設定ツール** — グラフィカルアプリケーションです。各サービスの説明を表示、各サービスがブート時にスタートしたかどうかを表示(ランレベル3、4、5用)、及び各サービスを起動、停止、再起動を許可することができます。
- **ntsysv** — テキストベースのアプリケーションです。ブート時に各ランレベルで起動させるサービスを設定します。`xinetd`以外のサービスには変更内容はすぐに反映されません。このプログラムを使用して`xinetd`以外のサービスの、起動、停止、または再起動はできません。
- `chkconfig` — コマンドラインユーティリティです。さまざまなランレベルでサービスの起動や停止を実行できます。`xinetd`以外のサービスには変更内容はすぐに反映されません。`xinetd`以外のサービスはこのユーティリティを使用して起動、停止又は再起動をすることは出来ません。

これらのツールの方がほかの手段—(`/etc/rc.d`の下にあるディレクトリ中の多数のシンボリックリンクを手作業で編集したり、`/etc/xinetd.d`の中の`xinetd`設定ファイルを編集したり）よりも使いやすくなっています。

システムサービスへのアクセスを管理するためのもう1つの方法として、`iptables`によってIPファイアウォールを設定することもできます。しかし、Linuxの初心者には、`iptables`が最良の策ではない場合があるということを理解してください。初心者にとって`iptables`の設定は複雑かもしれません。その操作は経験のあるLinuxのシステム管理者に任せるのが最善です。

その半面、`iptables`を使用するメリットは、その柔軟性にあります。たとえば、あるサービスに対するあるホストアクセスを許可するようにカスタマイズしたい場合でも、`iptables`ならば可能です。`iptables`の詳細については、*Red Hat Linux* 参照ガイド及び*Red Hat Linux* セキュリティガイドを参照してください。

別の方法としては、個人のマシンに一般アクセス規則を設定できるユーティリティを探している場合や、初めてLinuxを使用する場合は、**セキュリティレベル設定ツール**(`redhat-config-securitylevel`)を使用してください。これを使用するとRed Hat Linux インストールプログラムにある**ファイアウォールの設定**と同様に、システムの為のセキュリティレベルを選択することができます。また**GNOME Lokkit**を使用することも出来ます。これはユーザーにマシンの使い方について嗜好を尋ねるGUIアプリケーションです。ユーザーの応答に従って、自動的に単純なファイアウォールを設定します。これらのツールに関する詳細は、第13章を参照して下さい。より詳しいファイアウォールの規則については、*Red Hat Linux* 参照ガイドの中の`iptables`の章を御覧下さい。

14.1. ランレベル

サービスへのアクセスを設定する前に、Linuxランレベルを理解する必要があります。ランレベルとは状態、すなわちモードです。これはディレクトリ`/etc/rc.d/rc<x>.d`に一覧表示されたサービスで定義されます（*<x>*はランレベルの数字）。

Red Hat Linuxでは次のランレベルを使用しています：

- 0 —停止
- 1 —シングルユーザーモード
- 2 —未使用（ユーザー定義可能）
- 3 —完全マルチユーザーモード
- 4 —未使用（ユーザー定義可能）
- 5 —完全マルチユーザーモード（Xベースのログイン画面）
- 6 —リブート

テキストログイン画面を使用すると、ランレベル3で実行していることになります。グラフィックスログイン画面を使用すると、ランレベル5で実行していることになります。

デフォルトのランレベルを変更するには、/etc/inittabファイルを変更します。このファイルは、その最上部あたりに次のような1行があります。

```
id:5:initdefault:
```

この行の数字を希望するランレベルに変更します。システムを再ブートするまで変更内容は反映されません。

ランレベルをすばやく変更するには、コマンドtelinitを入力してから、ランレベル番号を続けます。このコマンドを使用するには、rootになる必要があります。

14.2. TCPラッパー

多くのUNIXシステム管理者は、TCPラッパーを使用して特定のネットワークサービスへのアクセスを管理する経験を持ちます。xinetdによって管理されるすべてのネットワークサービス（そしてlibwrapのサポートが組み込まれているプログラム）は、TCPラッパーを使用してアクセスを管理することができます。xinetdは、/etc/hosts.allowと/etc/hosts.denyファイルを使ってシステムサービスへのアクセスを設定することができます。ネームそれ自体が表しているように、hosts.allowには、xinetdによって制御されるネットワークサービスへクライアントのアクセスを許可する規則一覧が含まれ、hosts.denyにはアクセスを拒否する規則が含まれています。hosts.allowファイルはhosts.denyファイルに優先します。アクセスを許可したり、拒否する決定は、各IPアドレス（またはホスト名）か、またはクライアントのパターンに基づいて行われます。詳細については、*Red Hat Linux* 参照ガイド及び、manページ(man 5 hosts_access)のセクション5内のhosts_accessを参照してください。

14.2.1. xinetd

インターネットサービスへのアクセスを制御するには、xinetdを使用します。inetdの代わりになるもので、より安全です。xinetdデーモンはシステム資源を保護し、アクセスを制御し、ログをとります。また、特殊な用途のサーバー群を起動するために使用することもできます。xinetdを使用すれば、特定ホストへのアクセスのみを許可したり、特定ホストへのアクセスを禁止したり、特定の時間帯にのみサービスへのアクセスを許可したり、受信接続の割合や接続による負荷を制限したりすることができます。

xinetdは停止することなく動作し続け、すべてのポート上で管理するサービスを監視します。管理するサービスのいずれかに対する接続要求が到着すると、xinetdは該当するサービスに適したサーバーを起動します。

xinetd用の設定ファイルは/etc/xinetd.confですが、このファイルの内容を調べてみれば、ファイルには、いくつかのデフォルト値と/etc/xinetd.dディレクトリをインクルードするための命令しかないことがわかるでしょう。xinetdサービスを有効または無効にするには、/etc/xinetd.dディレクトリ内の設定ファイルを編集します。disable属性が**yes**に設定されている場合は、サービスは無効です。disable属性が**no**に設定されている場合は、サービスは有効です。**サービス設定ツール**やntsysvあるいはchkconfigを使用して、xinetd設定ファイルを編集し

たり、又は、そのステイタスを変更することが出来ます。xinetdによって制御されているネットワークサービスの一覧は、ls /etc/xinetd.dコマンドを使用して、/etc/xinetd.dディレクトリの内容を確認して下さい。

14.3. サービス設定ツール

サービス設定ツールはRed Hatで開発されたグラフィカルアプリケーションで、ブート時に（ランレベル3、4、5で）/etc/rc.d/init.d内で起動するSysVサービスを設定したり、有効にするxinetdサービスを設定します。さらに、SysVサービスの起動、停止、再起動や、xinetdの再起動も可能です。

デスクトップから**サービス設定ツール**をスタートするには、パネル上の**メインメニューボタン** =>**システム設定** =>**サーバ設定** =>**サービス**と進むか、あるいはシェルプロンプト(例えば、**XTerm**や**GNOME ターミナル**)でredhat-config-servicesコマンドを実行します。

図14-1. サービス設定ツール

サービス設定ツール は現在のランレベルや、現在編集中のランレベルを表示します。別のランレベルを編集するには、プルダウンメニューから**Edit Runlevel**を選択して、ランレベル3、4、5のうちどれかを選択します。ランレベルの説明については、項14.1を参照してください。

サービス設定ツール は/etc/rc.d/init.dディレクトリからのサービスと、xinetdで制御されるサービスを一覧表示します。アプリケーションの左側にある一覧のサービスの名前をクリックすると、そのサービスの説明とその状態が表示されます。サービスがxinetdサービスでない場合、ステータスのウィンドウでそのサービスが現在実行中かどうか表示されます。サービスがxinetdで制御されている場合は、状態のウィンドウは**xinetd service**というフレーズを表示します。

サービスをすぐに起動、停止、再起動するには、一覧からサービスを選択してから、ツールバー(又は、**操作**プルダウンメニューから目的の動作を選択)から、目的のボタンを選択します)。サービスがxinetdサービスの場合、アクションボタンは、個別に開始と停止ができない為、無効になっています。

サービス名の横にあるチェックボックスにチェックを入れたり、外したりすることでxinetdサービスを有効/無効にする場合、プルダウンメニューから**ファイル** => **変更を保存**の順で選択して、xinetdを再起動します。そうするとすぐに変更したxinetdサービスが有効/無効になります。xinetdはこのセッティングを記憶するように設定されています。一度に複数のxinetd サービスを有効/無効にすることが可能で、終了した時点で変更を保存できます。

例えば、ユーザーがrsyncをランレベル3で有効にするためにチェックを入れて、変更を保存したと想定します。rsyncサービスはすぐに有効になります。次回にxinetdがスタートした時もrsyncはまだ有効のままです。

警告

xinetdサービスへの変更を保存すると、xinetdは再起動して、変更がすぐに反映されます。他のサービスへの変更を保存するとランレベルが再設定されますが、変更はすぐには反映されません。

現在選択しているランレベルでブート時にxinetd以外のサービスをスタート出来るようにするには、一覧内のサービスの名前の横のチェックボックスにチェックを入れます。ランレベルを設定した後、プルダウンメニューから**ファイル** => **変更を保存**を選択して、変更を適用します。ランレベルの設定は変わりますが、ランレベルは再起動されません。そのため、変更はすぐには反映されません。

例えば、ランレベル3の設定をしていると想定しましょう。anacronサービスの値を「チェック付き」から「チェックなし」に変更して、それから**変更を保存**を選択すると、ランレベル3の設定はブート時にanacronをスタートしないように変更されます。しかし、ランレベル3は再初期化されていないのでまだ作動中のままです。ここで以下のオプションの1つを選択します：

1. anacronサービスの停止— 一覧からそのサービスを選択して**停止**ボタンをクリックすることで停止します。サービスが停止されたことを伝えるメッセージが表示されます。
2. ランレベルの再初期化— シェルプロンプト（**XTerm**か**GNOME terminal**）に進んで、コマンドtelinit 3（3はランレベルの数字）を入力して、ランレベルを再初期化します。このオプションは、2つ以上のサービスの**起動時に開始**の値を変更して、その変更内容をただちに反映させたい場合に推奨されます。
3. 何もしない—anacronサービスを停止する必要はありません。サービスの停止には、システムが再起動するまで待ちます。次回システムが起動するとき、ランレベルはanacronサービスが実行されずに初期化されます。

14.4. ntsysv

ntsysv ユーティリティは、サービスを有効または無効にするための単純なインターフェイスを提供します。**ntsysv**を使用すれば、xinetdによって管理されるサービスのオン/オフを切り替えることができます。また、**ntsysv**を使用して、ランレベルの設定をすることも出来ます。デフォルトでは現在のランレベルのみが設定されています。別のランレベルを設定するには、--levelオプションで1つ又は複数のランレベルを指定します。例えば、ntsysv --level 345コマンドはランレベル3、4、5のを設定します。

ntsysvインターフェイスは、テキストモードのインストールプログラムのような動き方をします。上向き矢印や下向き矢印を使用して、一覧の中を移動します。スペースキーは、サービスの選択と選択解除を切り替える場合、または**OK**ボタンや**キャンセル**ボタンを「押す」場合にも使用します。サービスの一覧、**OK**ボタン、**キャンセル**ボタンの間を移動するには、[Tab]キーを使用します。*はサービスがオンになっていることを示します。[F1]キーを押すと、各サービスに関する簡単な説明が表示されます。

警告

xinetdで管理されているサービスはすぐに**ntsysv**に反応します。その他のサービスは全て、すぐには反映されません。コマンドservice *daemon* stopを使用して個々のサービスを開始したり停止する必要があります。今の例では、*daemon*を停止したいサービスの名前、例えばhttpdに入れ換えます。stopの代わりに、startやrestartを指定すると起動や再起動をすることができます。

14.5. chkconfig

chkconfigコマンドはサービスを有効または無効にするために使用することもできます。chkconfig --listコマンドを使用すると、システムサービスの一覧と、各サービスがどのランレベル（0〜6）で起動（on）し、また停止（off）したかが表示されます。一覧の末尾には、xinetdによって管理されるサービス用のセクションがあります。

chkconfig --listを使用して、xinetdが管理するサービス1つを照会すると、xinetdサービスが起動している（on）か、停止している（off）かが表示されます。たとえば、chkconfig --list fingerコマンドは以下の出力を表示してきます：

```
finger    on
```

上記で表示してあるように、fingerはxinetdサービスとして有効です。xinetdが稼動していれば、fingerは有効です。

chkconfig --listによって/etc/rc.dのサービス1つを照会する場合は、ランレベルごとのサービス設定が表示されます。例えば、chkconfig --list anacronコマンドは以下の出力を表示します：

```
anacron    0:off 1:off 2:on  3:on  4:on  5:on  6:off
```

chkconfigは、あるサービスを特定のランレベルで起動する(あるいは起動しない)ように設定するのにも使用されます。例えば、ランレベル3、4、5でnscdを停止するには、以下のコマンドを使用します：

```
chkconfig --level 345 nscd off
```

警告

xinetdで管理されているサービスは、すぐにchkconfigに反応します。たとえば、xinetdが実行中で、fingerが無効の場合にchkconfig finger onを実行すると、手動でxinetdを再起動しなくてもfingerはすぐに有効になります。chkconfigを使用しても、ほかのサービスへの変更がすぐに反映されるわけではありません。service *daemon* stop形式のコマンドを使って、各サービスの停止や起動を行う必要があります。今の例では、*daemon*に停止するサービスの名前（たとえばhttpd）を指定します。stopの代わりに、startやrestartを指定すると、サービスを起動または再起動することができます。

14.6. その他のリソース

詳しい情報は以下のリソースで参照して下さい。

14.6.1. インストールされているドキュメント

- ntsysv, chkconfig, xinetd, 及びxinetd.conf用のmanページ
- man 5 hosts_access — （manページのセクション5の）ホストアクセス制御ファイルの書式に関するmanページ

14.6.2. 役に立つWebサイト

- http://www.xinetd.org —xinetdのWebページ。詳細な機能一覧や設定ファイルのサンプルが含まれています。

14.6.3. 関連書籍

- *Red Hat Linux* 参照ガイド, Red Hat, Inc. — このコンパニオンマニュアルには、TCPラッパーとxinetdがアクセスを許可と拒否をする手段についての情報、それらを使用したネットワークアクセスの設定法に関する詳細情報、及びiptablesファイヤーウォール規則の作成法などが含まれています。

第15章

OpenSSH

OpenSSHは、公開され無料で提供されているSSH（*S*ecure *SH*ell）プロトコルのソース実装です。`telnet`、`ftp`、`rlogin`、`rsh`、`rcp`といったコマンドの代わりに使用できる、安全な暗号化ネットワーク接続ツールです。OpenSSHは、SSHプロトコルのバージョン1.3、1.5、2をサポートしています。OpenSSHバージョン2.9の発表以降、デフォルトプロトコルはバージョン2で、これはデフォルトでRSA鍵を使用しています。

15.1. なぜOpenSSHを使うのか

OpenSSHツールを使用すると、マシンのセキュリティを強化することができます。OpenSSHツールを使用する通信は、パスワードを含め、すべて暗号化されます。`Telnet`と`ftp`では、平文のパスワードを使用して、すべての情報を暗号化せずに送信します。情報が傍受され、パスワードが読み取られてしまう可能性もあります。つまり、アクセスを許可されていないユーザーが盗み取ったパスワードを使ってシステムへログインしてしまう可能性があります。このようなセキュリティ問題を回避したい場合は、必ずOpenSSHユーティリティセットを使用します。

OpenSSHを使用するもう1つの理由は、`DISPLAY`変数をクライアントマシンへ自動的に転送できるためです。つまり、ローカルマシンでX Window Systemを稼動している場合、`ssh`コマンドを使ってリモートマシンへログインしていれば、Xが必要なリモートマシン上のプログラムを実行したときに、ローカルマシン上に表示することができます。これは、ユーザーがグラフィカルなシステム管理ツールを好むが、いつでもサーバーの設置場所へ物理的にアクセスできるとは限らない場合などに便利です。

15.2. OpenSSHサーバーの設定

OpenSSHサーバーを実行するには、最初に適切なRPMパッケージがインストールされていることを確認する必要があります。`openssh-server`パッケージが必要であり、これは`openssh`パッケージに依存します。

OpenSSHデーモンは、設定ファイルとして`/etc/ssh/sshd_config`を使用します。Red Hat Linuxにインストールされているディフォルトの設定ファイルは、ほとんどの目的に十分なはずです。デフォルトの`sshd_config`が提供していない方法でデーモンを設定する場合は、`sshd`のmanページで、設定ファイル内に定義できるキーワードの一覧を御覧下さい。

OpenSSHサービスを起動するには、`/sbin/service sshd start`コマンドを使用します。OpenSSHサーバーを停止するには、`/sbin/service sshd stop`コマンドを使用します。ブート時にデーモンを自動的に起動する場合は、第14章でサービスの管理方法に関する情報を参照してください。

Red Hat Linuxシステムを再インストールするとき、その前にクライアントが何らかのOpenSSHツールでシステムに接続されていた場合は、再インストールの後でクライアントユーザーは次の様なメッセージを見ることになります：

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
```

再インストールされたシステムはシステム用に新しく識別キーのセットを作成します。それで、RSAホストキー変更の警告が出るわけです。システム用に生成されたホストキーを継続使用する場合は、`/etc/ssh/ssh_host*key*`ファイルをバックアップしておいて、再インストール後に

それを復元します。このプロセスでシステムの識別を保存しますので再インストール後にクライアントがシステムに接続をしても警告のメッセージを受ける事はありません。

15.3. OpenSSHクライアントの設定

クライアントマシンからOpenSSHサーバーへ接続するには、クライアントマシンにopenssh-clientsとopensshパッケージがインストールされている必要があります。

15.3.1. sshコマンドの使用

sshコマンドは、rlogin、rsh、telnetコマンドに代わる安全な手段です。これを使用してリモートマシンへログインし、リモートマシン上でコマンドを実行することができます。

sshコマンドを使ってリモートマシンにログインする方法はtelnetの場合と同様です。penguin.example.netという名前のリモートマシンへログインするには、シェルプロンプトで次のコマンドを入力します：

```
ssh penguin.example.net
```

初めてsshコマンドでリモートマシンへログインした場合には、次のようなメッセージが表示されます：

```
The authenticity of host 'penguin.example.net' can't be established.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

yesとタイプして続行します。これによって、次のメッセージのように、ユーザーの既知ホストの一覧にサーバーが追加されます：

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list of known hosts.
```

次に、リモートマシンのパスワードの入力を求めるプロンプトが表示されます。パスワードを入力すると、リモートマシンのシェルプロンプトが現れます。ユーザー名を指定しない場合は、ローカルクライアントマシンにログインしてあるユーザー名がリモートマシンに渡されます。別のユーザー名を指定したい場合は、次のコマンドを使用します：

```
ssh username@penguin.example.net
```

`ssh -l username penguin.example.net`という構文も使用できます。

sshコマンドを使用すると、シェルプロンプトへログインせずに、リモートマシン上でコマンドを実行できます。構文は、 `ssh hostname command`です。たとえば、リモートマシンpenguin.example.net上で`ls /usr/share/doc`というコマンドを実行する場合は、シェルプロンプトで次のコマンドを入力します：

```
ssh penguin.example.net ls /usr/share/doc
```

正しいパスワードを入力すると、リモートディレクトリ/usr/share/docの内容が表示され、その後ローカルのシェルプロンプトへ戻ります。

15.3.2. scpコマンドの使用

scpコマンドを使うと、安全な暗号化通信を介してマシン間でファイルを転送できます。これは、rcpコマンドによく似ています。

ローカルファイルをリモートシステムへ転送するための一般的な構文は次の様になります：

```
scp localfile username@tohostname:/newfilename
```

*localfile*が転送元を指定する部分で、*username@tohostname:/newfilename*が転送先を指定する部分となります。

shadowmanというローカルファイルをpenguin.example.net上のアカウントへ転送するには、シェルプロンプトで次のように入力します（*username*には自分のユーザー名を指定）：

```
scp shadowman username@penguin.example.net:/home/username
```

このコマンドにより、ローカルファイルshadowmanは、penguin.example.net上の/home/*username*/shadowmanへ転送されます。

リモートファイルをローカルシステムへ転送する一般的な構文は次の様になります：

```
scp username@tohostname:/remotefile /newlocalfile
```

*remotefile*が転送元を指定する部分で、*newlocalfile*が転送先を指定する部分になります。

転送元ファイルとして複数のファイルを指定できます。たとえば、/downloadsディレクトリの内容を、リモートマシンpenguin.example.net上のuploadsという既存ディレクトリへ転送するには、シェルプロンプトで次のように入力します：

```
scp /downloads/* username@penguin.example.net:/uploads/
```

15.3.3. sftpコマンドの使用

sftpユーティリティを使うと、安全な対話型FTPセッションを開くことができます。これは、安全な暗号化接続を使用する点以外は、ftpコマンドによく似ています。一般的な構文は、*sftp username@hostname.com*です。認証が完了すると、FTPの場合と同様のコマンドセットを使用できます。これらのコマンドの一覧については、sftpのmanページを参照してください。manページを表示するには、シェルプロンプトでman sftpコマンドを実行します。sftpユーティリティは、OpenSSHバージョン2.5.0p1以降にのみ対応しています。

15.3.4. 鍵ペアの生成

ssh、scp、sftpのいずれかを使用してリモートマシンに接続するたびにパスワードを入力したくない場合は、認証鍵ペアを生成できます。

鍵は、ユーザーごとに生成する必要があります。次の手順に従い、リモートマシンへの接続を要求するユーザーとしてユーザー鍵を生成します。rootとして以下の手順を完了した場合、鍵を使用できるのはrootだけです。

OpenSSHバージョン3.0始まった、~/.ssh/authorized_keys2、~/.ssh/known_hosts2、/etc/ssh_known_hos
古くなっています。SSH Protocol 1と2は、~/.ssh/authorized_keys、~/.ssh/known_hosts、/etc/ssh/ssh_kr
イルを共有しています。

Red Hat Linux 9はディフォルトでSSH Protocol 2 とRSA鍵を使用します。

ヒント

Red Hat Linuxを再インストールして、ユーザーの生成された鍵ペアを保存したい場合は、ユーザーのホームディレクトリの.sshディレクトリをバックアップします。再インストール後にこのディレクトリをホームディレクトリにコピーして戻します。このプロセスはrootも含めて、システム上のすべてのユーザー用に実行できます。

15.3.4.1. バージョン2対応のRSA鍵ペアの生成

次の手順で、SSHプロトコルバージョン2に対応するRSA鍵ペアを生成します。これはOpenSSH 2.9以降でのデフォルトです。

1. SSHプロトコルバージョン2で動作するRSA鍵ペアを生成するには、シェルプロンプトで次のコマンドを入力します：
   `ssh-keygen -t rsa`

   デフォルトファイルの場所として、`~/.ssh/id_rsa`を受け入れます。ユーザーアカウントのパスワードとは異なったパスフレーズを入力し、確定のためもう1度入力します。

   公開鍵は`~/.ssh/id_rsa.pub`に書き込まれます。秘密鍵は`~/.ssh/id_rsa`に書き込まれます。秘密鍵を他人に配布してはいけません。
2. `chmod 755 ~/.ssh`コマンドを使用して`.ssh`ディレクトリのパーミッションを変更します。
3. `~/.ssh/id_rsa.pub`の内容を接続したいマシン上の`~/.ssh/authorized_keys`にコピーします。`~/.ssh/authorized_keys`ファイルが存在しない場合でも、`~/.ssh/id_rsa.pub`ファイルをその相手マシン上の`~/.ssh/authorized_keys`ファイルへコピーできます。
4. GNOMEを稼動している場合は、項15.3.4.4へ進みます。X Window Systemを稼動していない場合は、項15.3.4.5へ進みます。

15.3.4.2. バージョン2対応のDSA鍵ペアの生成

次の手順で、SSHプロトコルバージョン2に対応するDSA鍵ペアを生成します。

1. SSHプロトコルバージョン2で動作するDSA鍵を生成するには、シェルプロンプトで次のコマンドを入力します：
   `ssh-keygen -t dsa`

   デフォルトファイルの場所として、`~/.ssh/id_dsa`を受け入れます。ユーザーアカウントパスワードとは異なるパスフレーズを入力し、確定のためもう1度入力します。

   ヒント

   パスフレーズとは、ユーザー認証に使用される一連の単語と文字です。パスフレーズは、スペースやタブを使用できる点でパスワードとは異なります。通常、パスフレーズでは、1つの単語の代わりに複数のフレーズを使用するため、パスワードより長くなります。

   公開鍵は、`~/.ssh/id_dsa.pub`に書き込まれます。秘密鍵は`~/.ssh/id_dsa`に書き込まれます。秘密鍵をほかの人に渡さないことが重要です。
2. `chmod 755 ~/.ssh`コマンドを使用して`.ssh`ディレクトリのパーミッションを変更します。
3. `~/.ssh/id_dsa.pub`の内容を接続したいマシン上の`~/.ssh/authorized_keys`にコピーします。`~/.ssh/authorized_keys`ファイルが存在しない場合でも、`~/.ssh/id_dsa.pub`ファイルをその相手マシン上の`~/.ssh/authorized_keys`ファイルへコピーできます。
4. GNOMEを稼動している場合は、項15.3.4.4へ進みます。X Window Systemを稼動していない場合は、項15.3.4.5へ進みます。

15.3.4.3. バージョン1.3と1.5に対応するRSA鍵ペアの生成

次の手順で、SSHプロトコルバージョン1が使用するRSA鍵ペアを生成します。DSAを使用するシステム同士を接続している場合は、RSAバージョン1.3またはRSAバージョン1.5鍵ペアは必要ありません。

1. RSA（バージョン1.3と1.5のプロトコルに対応）鍵ペアを生成するには、シェルプロンプトで次のコマンドを入力します：
   ```
   ssh-keygen -t rsa1
   ```
   デフォルトのファイルの場所（~/.ssh/identity）を受け入れます。アカウントパスワードとは異なるパスフレーズを入力します。確定のため、もう1度入力します。

   公開鍵は~/.ssh/identity.pubに書き込まれます。秘密鍵は~/.ssh/identityに書き込まれます。秘密鍵を他人に渡さないでください。
2. chmod 755 ~/.sshコマンドとchmod 644 ~/.ssh/identity.pubコマンドを使って、.sshディレクトリと鍵のパーミッションを変更します。
3. ~/.ssh/identity.pubの内容を接続したいマシン上の~/.ssh/authorized_keysファイルへコピーします。~/.ssh/authorized_keysファイルが存在しない場合でも、~/.ssh/identity.pubファイルをそのリモートマシン上の~/.ssh/authorized_keysファイルへコピー出来ます。
4. GNOMEを稼動している場合は、項15.3.4.4へ進みます。GNOMEを稼動していない場合は、項15.3.4.5へ進みます。

15.3.4.4. GNOMEを使ったssh-agentの設定

ssh-agentユーティリティを使用するとパスフレーズを保存できるため、sshやscp接続を開始するたびにパスフレーズを入力する必要はありません。GNOMEを使用している場合は、openssh-askpass-gnomeユーティリティを使用するとユーザーがGNOMEへログインするときにパスフレーズの入力が要求され、GNOMEからログアウトするまでパスフレーズを保存しておくことができます。つまり、GNOMEセッション中は、ssh接続またはscp接続を確立するたびに、パスワードやパスフレーズを入力する必要はありません。GNOMEを使用していない場合は、項15.3.4.5を参照してください。

GNOMEセッションが終了するまでパスフレーズを保存するための手順は次のとおりです：

1. openssh-askpass-gnomeパッケージがインストールされている必要があります。rpm -q openssh-askpass-gnomeコマンドを使用して、インストールされているかどうかを判別できます。インストールされていない場合は、Red Hat Linux CD-ROMセット、Red Hat FTPミラーサイト、Red Hat ネットワークのいずれかを使用してインストールします。
2. ~/.Xclientsファイルが存在しない場合は、switchdeskを実行して作成することができます。~/.Xclientsファイルの中に以下の行があります：
   ```
   exec $HOME/.Xclients-default
   ```
   次のように変更します：
   ```
   exec /usr/bin/ssh-agent $HOME/.Xclients-default
   ```
3. (パネル上の)**メインメニューボタン** => **個人設定** => **その他の設定** => **セッション**の順で選択して**自動起動プログラム**タブをクリックします。**追加**をクリックして、**自動起動コマンド**のテキスト欄に**/usr/bin/ssh-add**と入力します。必ず最後に実行されるように、優先順位を既存のコマンドより大きい数字に設定します。ssh-addには70以上の優先番号が適しています。優先順位の数字が大きいほど、優先順位は低くなります。他のプログラムが一覧にある場合は、このプログラムが最も低い優先順となる必要があります。**閉じる**ボタンをクリックしてプログラムを終了します。
4. ログアウトして、再びGNOMEにログインします。つまり、Xを再起動します。GNOMEが起動すると、パスフレーズの入力を求めるダイアログボックスが表示されます。要求されたパスフレーズを入力します。DSA鍵ペアとRSA鍵ペアの両方が設定されている場合は、両方の入力が求められます。この後は、ssh、scp、sftpのいずれかを実行したときにパスワードの入力が求められることはないはずです。

15.3.4.5. ssh-agentの設定

ssh-agentコマンドを使用してパスフレーズを保存すると、ssh接続またはscp接続を確立するたびにパスフレーズを入力する必要がなくなります。X Window Systemを稼動していない場合は、シェルプロンプトから次の手順を実行します。GNOMEを稼動しているが、ログイン時にパスフレーズの入力を求めないように設定する場合は（項15.3.4.4を参照）、以下の手順をxtermなどのターミナルウィンドウで実行します。Xは稼動しているが、GNOMEは稼動していない場合も、この手順をターミナルウィンドウで実行します。ただし、この場合、パスフレーズの設定はその使用するターミナルウィンドウにだけ保存され、グローバルな設定値とはなりません。

1. シェルプロンプトで、次のコマンドを入力します：
   `exec /usr/bin/ssh-agent $SHELL`
2. 次のコマンドを入力します：
   `ssh-add`

   次にパスフレーズを入力します。複数の鍵ペアが設定されている場合は、両方の入力が求められます。
3. ログアウトすると、保存されていたパスフレーズは消去されます。仮想コンソールへログインするたびに、あるいはターミナルウィンドウを開くたびに、この2つのコマンドを実行する必要があります。

15.4. その他のリソース

OpenSSHとOpenSSLプロジェクトの開発は常に進められているため、これらに関する最新情報は該当するWebサイトを参照してください。OpenSSHとOpenSSLツールのmanページでも詳細情報を参照することができます。

15.4.1. インストールされているドキュメント

- ssh, scp, sftp, sshd, 及びssh-keygenコマンドのman ページ— これらのmanページには、各コマンドの使用方法と指定できるすべてのパラメータに関する情報が記載されています。

15.4.2. 役に立つWebサイト

- http://www.openssh.com —OpenSSH FAQページ、バグレポート、メーリングリスト、プロジェクトの目標、セキュリティ機能に関する技術的な詳細情報を参照できます。
- http://www.openssl.org —OpenSSL FAQページ、メーリングリスト、プロジェクトの目標に関する説明を参照できます。
- http://www.freessh.org —その他のプラットフォームに対応するSSHクライアントソフトウェアを確認できます。

第16章

NFS（ネットワークファイルシステム）

NFS（ネットワークファイルシステム）は、ローカルのハードディスクドライブ上にあるかのように、ネットワーク上のマシン間でファイルを共有できるようにするための手段です。Red Hat Linuxは、NFSサーバーにもNFSクライアントにもなることができます。つまり、Red Hat Linuxはほかのシステムに対してファイルシステムをエクスポートすることも、ほかのマシンからエクスポートされたファイルシステムをマウントすることもできます。

16.1. NFSを使用する理由

NFSは、同じネットワーク上の複数のユーザー間でファイルのディレクトリを共有できる便利な手段です。たとえば、同じプロジェクトで仕事をしているユーザーのグループは、ディレクトリ/myprojectにマウントされているNFSファイルシステムの共有ディレクトリ(一般に「NFS共有」と呼びます)を使用して、そのプロジェクトのファイルへのアクセス権を取得することができます。共有ファイルにアクセスするには、ユーザーは自分のマシンの/myprojectディレクトリに移動します。パスワードを入力したり、特別なコマンドを覚えたりする必要はありません。ユーザーは、そのディレクトリがあたかも自分のローカルマシン上にあるかのように作業することができます。

16.2. NFS ファイルシステムのマウント

別のマシンからNFS共有ディレクトリをマウントするには、mountコマンドを使用します。

```
mountshadowman.example.com:/misc/export/misc/local
```

警告

ローカルマシン上にマウントポイントディレクトリ（上記の例では/misc/local）が存在していなければなりません。

このコマンドでは、shadowman.example.comはNFSファイルサーバーのホスト名であり、/misc/exportはshadowmanがエクスポートしているファイルシステムで、/misc/localはファイルシステムをマウントするローカルマシン上の場所です。mountコマンドを実行した後は、(shadowman.example.comNFSサーバーから適切な権限が与えられていれば)クライアントユーザーはls /misc/localを実行して、shadowman.example.com上の/misc/exportに含まれるファイルの一覧を表示させることができます。

16.2.1. /etc/fstabを使ったNFSファイルシステムのマウント

ほかのマシンからNFS共有をマウントするもう1つの方法は、/etc/fstabファイルに行を追加する方法です。この行では、NFSサーバーのホスト名、エクスポートするサーバー上のディレクトリ、NFS共有をマウントするローカルマシン上のディレクトリを指定します。/etc/fstabファイルを修正できるのはrootだけです。

/etc/fstab内のこの行の一般的な構文は次のとおりです：

```
server:/usr/local/pub  /pub  nfs  rsize=8192,wsize=8192,timeo=14,intr
```

クライアントマシン上にマウントポイント/pubが存在している必要があります。この行をクライアントシステムの/etc/fstabに追加した後、シェルプロンプトでコマンドmount /pubを入力すると、サーバーからマウントポイント/pubがマウントされます。

16.2.2. autofsを使ったNFS ファイルシステムのマウント

NFS共有をマウントする3つ目の方法は、autofsの使用です。autofsはautomountデーモンを使ってマウントポイントを管理し、マウントポイントがアクセスされる場合にのみ動的にマウントします。

autofsは、マスターマップ設定ファイル/etc/auto.masterを参照して、どのマウントポイントが定義されているかを判別します。そして、マウントポイントごとに適切なパラメータを指定して、automountプロセスを起動します。マスターマップ内の各行では、マウントポイントと、そのマウントポイント下にマウントするファイルシステムを定義する別のマップファイルが定義されています。たとえば、/etc/auto.miscファイルでは、/miscディレクトリ内のマウントポイントが定義されるかも知れません。このディレクトリとマウントポイント間の関係は、/etc/auto.masterファイルで定義されることになります。

auto.master内の各項目は、3つのフィールドで構成されます。1つ目のフィールドはマウントポイントです。2つ目のフィールドは、マップファイルの場所で、3つ目のフィールドはオプションフィールドです。3つ目のフィールドには、タイムアウト値などの情報を入力することができます。

たとえば、ユーザーマシンのマウントポイント/misc/myprojectにリモートマシンpenguin.host.netのディレクトリ/proj52をマウントするには、auto.masterに次の行を追加します：

```
/misc  /etc/auto.misc --timeout60
```

/etc/auto.miscに次の行を追加します：

```
myproject -rw,soft,intr,rsize=8192,wsize=8192 penguin.example.net:/proj52
```

/etc/auto.miscの1つ目のフィールドは、/miscサブディレクトリの名前です。このディレクトリは、automountによって動的に作成されます。実際にクライアントマシン上に存在してはなりません。2つ目のフィールドには、読み取りと書き込みのアクセスを表すrwなどのマウントオプションを指定します。3つ目のフィールドは、ホスト名とディレクトリを含む、NFSエクスポートの場所です。

注意

ローカルファイルシステムにディレクトリ/miscが存在していなければなりません。また、ローカルファイルシステムに/miscのサブディレクトリが存在してはなりません。

autofsはサービスです。このサービスを起動するには、シェルプロンプトで次のコマンドを入力します：

```
/sbin/service autofs restart
```

有効なマウントポイントを表示するには、シェルプロンプトで次のコマンドを入力します：

```
/sbin/service autofs status
```

autofsを実行しているときに/etc/auto.master設定ファイルを修正した場合は、シェルプロンプトで次のコマンドを入力して、リロードすることをautomountデーモンに伝える必要があります：

```
/sbin/service autofs reload
```

ブート時にautofsを起動するように設定する方法については、第14章でサービスの管理に関するトピックを参照してください。

16.3. NFS ファイルシステムのエクスポート

NFSサーバからのファイルを共有することは、ディレクトリのエクスポートとして知られています。**NFS サーバー設定ツール**は、システムをNFSサーバとして設定するために使用できます。

NFS サーバー設定ツールを使用するには、X Window Systemを起動している状態で、root権限で操作し、`redhat-config-nfs` RPMパッケージをインストールしておく必要があります。アプリケーションをスタートするには、パネル上から**メインメニューボタン**=> **システム設定** => **サーバ設定** => **NFS サーバ**と進みます。又はコマンド`redhat-config-nfs`を入力します。

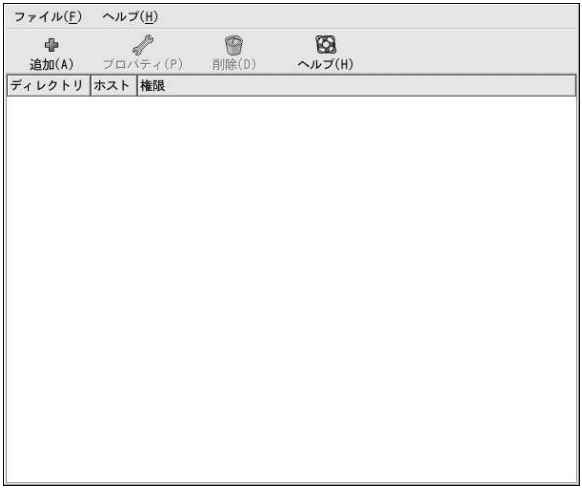


図16-1. NFS サーバー設定ツール

NFS共有を追加するには、**追加**ボタンをクリックします。図16-2に示すようなダイアログボックスが表示されます。

基本タブは次のような情報を必要とします：

- **ディレクトリ** — `/tmp`などの共有するディレクトリを指定。
- **ホスト** — ディレクトリを共有するホストを指定。可能なフォーマットについては項16.3.2を参照して下さい。
- **基本権限** — ディレクトリが読み込み専用か、或は読み込み/書き込み両方の権限を持つかどうか指定します。

図16-2. 共有の追加

一般的オプションタブでは、次のようなオプションが設定できます：

- **1024以上のポートからの接続を許可** — 1024以下のポートから開始したサービスはrootで開始開始する必要があります。root以外のユーザーからNFSサービスが開始出来るようにするにはこのオプションを選択します。このオプションは`insecure`コマンドに相当します。
- **安全でないファイルロックを許可** — ロック要求を必要としません。このオプションは`insecure_locks`コマンドに相当します。
- **サブツリーチェックを無効にする** — ファイルシステムのサブディレクトリがエクスポートされてファイルシステム全体はエクスポートされない場合、サーバはサブディレクトリの要求されたファイルがエクスポートされたかどうかチェックします。このチェックはサブツリーチェックと呼ばれます。このオプションを選択するとサブツリーチェックを無効にします。ファイルシステム全体がエクスポートされる場合、このサブツリーチェックを無効にすると、転送レートが向上します。このオプションは`no_subtree_check`コマンドに相当します。
- **要求時に書き込みを同期化** — デフォルトで有効になっており、このオプションでは、要求がディスクに書き込まれるまでサーバはこの要求への返事を許可されません。このオプションは`sync`コマンドに相当します。これが選択されない場合、`async` オプションが使用されます。
  - **すぐに書き込みの同期化を強制** — ディスクへの書き込み遅延がありません。このオプションは`no_wdelay`コマンドに相当します。

ユーザーアクセスタブでは、次のオプションが設定できます：

- **リモートのrootユーザーをローカルのrootとみなす** — デフォルトで、rootユーザーのユーザーIDとグループIDは両方とも0です。root 潰し(squashing)が、ユーザーID 0とグループID 0をanonymousのユーザーIDとグループIDにマップしてクライアント上のrootが、NFSサーバ上でroot権限を持てないようにします。このオプションが選択されると、rootはanonymousにマップされないのでクライアント上のrootは、root権限でディレクトリをエクスポート出来ます。このオプションを選択するとシステムのセキュリティを大幅に低減します。絶対に必要な場合以外は、これを選択しないで下さい。このオプションは`no_root_squash`コマンドに相当します。
- **全てのクライアントユーザーをanonymousユーザーとみなす** — このオプションが選択されると、すべてのユーザーIDとグループIDはanonymousユーザーにマップされます。このオプションは`all_squash` コマンドに相当します。
  - **anonymousユーザーにローカルユーザーIDを指定** — **全てのクライアントユーザーをanonymousユーザーとみなす**が選択されると、このオプションでanonymousユーザーの為のユーザーIDを指定できます。このオプションは`anonuid`コマンドに相当します。
  - **>anonymousユーザーにローカルグループIDを指定** — **全てのクライアントユーザーをanonymousユーザーとみなす**が選択されると、このオプションでanonymousユーザーの為のグループIDを指定できます。このオプションは`anongid`コマンドに相当します。

既存のNFS 共有を編集するには、一覧から共有を選択し、**プロパティ**ボタンをクリックします。既存のNFS 共有を削除するには、一覧から共有を選択し、**削除**ボタンをクリックします。

一覧からNFS共有を追加、編集、又は削除するために**OK**ボタンをクリックした後に、変更はすぐに反映されます。— サーバデーモンが再起動して古い設定ファイルは`/etc/exports.bak`として保存されます。新規の設定は`/etc/exports`に書き込まれます。

NFS サーバー設定ツールは、`/etc/exports` 設定ファイルに対し直接、読み込みと書き込みします。そのため、このファイルはこのツールを使用した後で手動で修正が可能で、また、このツールはファイルを手動で修正した後に使用できます。(ファイルが正しい構文で修正されている場合)。

16.3.1. コマンドラインで設定

設定ファイルをテキストエディタで編集することを好む場合、又はX Window Systemをインストールしていない場合、設定ファイルを直接修正することが出来ます。

`/etc/exports` ファイルはNFSサーバがどのディレクトリをエクスポートするかを制御します。その形式は以下のようになります：

```
directoryhostname(options)
```

指定すべき唯一のオプションはsyncか又はasyncの1つです(syncを推奨)。syncが指定されている場合は、要求による変更がディスクに書き込まれるまでは、サーバは要求に返事しません。

例えば：

```
/misc/export  speedy.example.com(sync)
```

これは、`speedy.example.com`からのユーザーが、デフォルトの読み込み専用権限で`/misc/export`をマウント出来るようにします。しかし：

```
/misc/export  speedy.example.com(rw,sync)
```

これは、`speedy.example.com`からのユーザーが読み込み/書き込みの両方の権限で`/misc/export`をマウントできるようにします。

可能なホスト名形式に付いての説明は項16.3.2を参照して下さい。

指定できるオプションの一覧に関しては、*Red Hat Linux* 参照ガイドを参照して下さい。

用心

`/etc/exports`ファイル内のスペースの使用に注意してください。ホスト名とかっこで囲んだオプションとの間にスペースがない場合、オプションはそのホスト名にのみ適用されます。ホスト名とオプションの間にスペースがある場合、オプションはほかのすべてのホストに適用されます。たとえば、次の例で確認してみます：

```
/misc/export speedy.example.com(rw,sync)
/misc/export speedy.example.com (rw,sync)
```

初めの行は、`speedy.example.com`のユーザーに読み取りと書き込みのアクセスを許可し、その他すべてのユーザーにはアクセスを禁止しています。2番目の行は、`speedy.example.com`のユーザーには読み取りアクセスのみを許可し（デフォルト）、その他のユーザーには読み取りと書き込みを許可しています。

`/etc/exports`を変更する度に、NFS デーモンに情報提供するか、あるいは、次のコマンドで設定ファイルをリロードする必要があります：

```
/sbin/service nfs reload
```

16.3.2. ホスト名の形式

ホストは以下のような形式になっています：

- 単独マシン— 完全修飾ドメイン名(サーバが解決出来る)、ホスト名(サーバが解決出来る)、或はIPアドレス
- ワイルドカードで指定されたマシン群—「*」か「?」記号を使用して文字列の合致を指定します。ワイルドカードはIPアドレスでは使用しません。しかし逆引きのDNS検索で失敗した場合、偶然にうまくできるかもしれません。完全修飾ドメイン名でワイルドカードを使用する場合は、ドット「.」はワイルドカードに含まれません。例えば、`*.example.com`はone.example.comを含みますが、one.two.example.comは含みません。
- IP ネットワーク— *`a.b.c.d/z`*を使います。ここで、*`a.b.c.d`*は、ネットワークであり、*`z`*は、ネットマスク内のビットの数字です。(例えば、192.168.0.0/24). もう1つの認識されている形式は*`a.b.c.d/netmask`*で、ここで*`a.b.c.d`*がネットワークで、*`netmask`*はネットマスクです。(例えば、192.168.100.8/255.255.255.0)。
- ネットグループ— *`@group-name`*の形をしており、ここで*`group-name`*はNISネットグループ名のことです。

16.3.3. サーバーの起動と停止

NFSファイルシステムをエクスポートするサーバー上では、`nfs`サービスが実行されている必要があります。

次のコマンドを使用してNFSデーモンの状態を表示します：

```
/sbin/service nfs status
```

次のコマンドを使用してNFSデーモンを起動します：

```
/sbin/service nfs start
```

次のコマンドを使用してNFSデーモンを停止します：

```
/sbin/service nfs stop
```

ブート時に`nfs`サービスを起動するには、次のコマンドを使用します：

```
/sbin/chkconfig --level 345 nfs on
```

`chkconfig`,**ntsysv** 或は**サービス設定ツール**を使用して、ブート時に起動するサービスを設定することもできます。詳細については第14章を参照してください。

16.4. その他のリソース

この章では、NFSの使用に関する基本的な項目についてのみ説明しています。詳細については、以下のリソースを参照してください。

16.4.1. インストールされているドキュメント

- `nfsd`、`mountd`、`exports`、`auto.master`、`autofs`のmanページ（マニュアルのセクション5と8）—これらのmanページには、NFSとautofsの設定ファイルの構文が記載されています。

16.4.2. 役に立つWebサイト

- http://www.tldp.org/HOWTO/NFS-HOWTO/index.html — Linux Documentation Projectからの*Linux NFS-HOWTO*です。

16.4.3. 関連書籍

- 「*Managing NFS and NIS Services*」（Hal Stern著、O’Reilly &アソシエイツ）

第17章
Samba

Sambaは、SMBプロトコルを使用して、ネットワーク接続全体でファイルとプリンタを共有します。このプロトコルをサポートするオペレーティングシステムには、Microsoft Windows **(隣接ネットワーク(Network Neighborhood)**を利用)、OS/2、Linuxがあります。

17.1. Sambaを使う理由

Sambaは、1つのネットワークにWindowsマシンとLinuxマシンの両方がある場合に役立ちます。Sambaを使えば、ネットワーク内のすべてのシステムでファイルとプリンタを共有することができます。ファイルの共有をRed Hat Linuxマシン間だけに制限したい場合は、第16章で説明してあるNFSを使用します。プリンタの共有をRed Hat Linuxマシン間だけに制限したい場合は、Sambaを使う必要はありません。第27章を参照してください。

17.2. Sambaサーバの設定

デフォルトの設定ファイル(`/etc/samba/smb.conf`)の使用で、ユーザーはRed Hat Linux ホームディレクトリをSamba共有として閲覧することができます。また、Red Hat Linuxシステムで設定されているどんなプリンタもSamba共有プリンタとして共有できます。すなわち、プリンタをRed Hat Linuxシステムに接続して、ネットワーク上のWindowsマシンから印刷することが出来ます。

17.2.1. グラフィカル設定

グラフィカルインターフェイスを使用してSambaを設定するには、**Samba サーバー設定ツール**を使用します。コマンド行の設定については、項17.2.2へ進んで下さい。

Samba サーバー設定ツールツールは、Samba共有、ユーザー、及び基本サーバ設定を管理する為のグラフィカルインターフェイスです。これは`/etc/samba/`ディレクトリの設定ファイルを修正します。これらのファイルに対する変更でこのアプリケーション以外から来るものは保存されます(上書きされません)。

このアプリケーションを使用するには、X Window Systemを起動していて、root権限を持っている必要があります。さらに`redhat-config-samba`RPM パッケージがインストールされていなければなりません。デスクトップから**Samba サーバー設定ツール**を開始するには、パネル上の**メインメニューボタン**=>**システム設定** => **サーバ設定** =>**Sambaサーバ**と進みます。又は、シェルプロンプト(例えば、XTerm やGNOMEターミナル)で`redhat-config-samba`と入力します。

図17-1. Samba サーバー設定ツール

注意

Samba サーバー設定ツールは、共有プリンタあるいは、Sambaサーバ上の自己のホームディレクトリをユーザーが表示できるようなデフォルトスタンザは表示しません。

17.2.1.1. サーバ設定の構成

Sambaサーバを設定する最初のステップは、サーバに基本設定とセキュリティオプションを構成することです。アプリケーションをスタートした後、プルダウンメニューから**ユーザー設定 =>サーバ設定**を選択します。**基本**タブは図17-2に示してあるようになります。

図17-2. 基本サーバー設定の構成

基本タブでは、コンピュータが属すべきワークグループ、及び簡単なコンピュータの説明を記入します。これらは、`smb.conf`内の`workgroup`と`server string`のオプションに相当します。

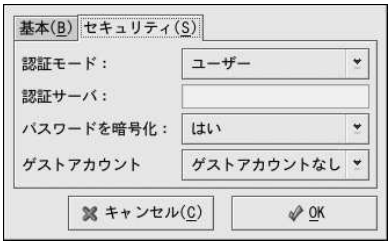


図17-3. セキュリティサーバ設定の構成

セキュリティタブには、次のオプションが含まれています：

- **認証モード** — これは、セキュリティ オプションに相当します。次の認証タイプの1つを選択します。
  - **ドメイン** — Samba サーバはユーザー名とパスワードの組合せをWindows NT プライマリ、又はバックアップドメインコントローラに渡します。**認証サーバ**フィールド内のプライマリか、バックアップドメインコントローラのNetBIOS名を指定します。

    暗号化パスワード選択されている場合、オプションは**Yes**にセットされる必要があります。
  - **サーバ** — Sambaサーバは、ユーザー名とパスワードの組合せを別のSamba サーバに渡してそれを確証しようとします。それが出来ない場合、サーバはユーザー認証モードを使用して確証しようとします。**認証サーバ** フィールド内に他のSambaサーバのNetBIOS名を指定して下さい。
  - **共有** — Sambaユーザーはユーザー名とパスワードの組合せをSambaサーバベース単位で入力する必要はありません。ユーザー名とパスワードは、Sambaサーバから特定の共有ディレクトリへ接続を試みるまでは、要求されません。
  - **ユーザー** — (デフォルト) Sambaユーザーは、有効なユーザー名とパスワードをSambaサーバベース単位で用意する必要があります。**Windowsユーザー名** オプションを有効にしたい場合、このオプションを選択します。詳細については項17.2.1.2を参照して下さい。

- **パスワードを暗号化する** — (デフォルト値は**Yes**)。クライアントがWindows 98, Windows NT 4.0 (サービスパック3付き)、あるいはより新しいバージョンのMicrosoft Windowsから接続をしている場合、このオプションを有効にする必要があります。パスワードは、傍受される可能性のあるプレインテキストではなく、暗号化された形式でサーバとクライアント間で転送されます。これは、`encrypted passwords` オプションに相当します。暗号化したSambaパスワードに関する詳細は項17.2.3を参照して下さい。
- **ゲストアカウント** — ユーザー又は、ゲストユーザーがSambaサーバにログインする時、彼らはサーバ上に有効なユーザーでマップされなければなりません。ゲストのSambaアカウントになるには、システム上の既存のユーザー名1つを選択します。ゲストがSambaサーバにログインする時、彼らはこの既存ユーザーと同じ権限を持ちます。これは`guest account`オプションに相当します。

OKボタンを押したあと、変更は設定ファイルに書き込まれてデーモンが再スタートします。これにより、変更はすぐに反映されます。

17.2.1.2. Sambaユーザーの管理

Samba サーバー設定ツールでは、既存のユーザーアカウント1つがRed Hat Linuxシステム上で有効になっており、Sambaユーザー1人が追加される前にSambaサーバとして動作していることを要求します。Sambaユーザーはこの既存のRed Hat Linuxユーザーアカウントに連携されます。

図17-4. Sambaユーザーの管理

Sambaユーザーを追加するには、プルダウンメニューから**ユーザー設定** => **Sambaユーザー**と進み、**ユーザーの追加**ボタンをクリックします。**新規のSambaユーザーを作成**ウィンドウ上で、ローカルシステムの既存ユーザー一覧から**Unixユーザー名**を選択します。

ユーザーがWindowsマシン上で別のユーザー名を持っていて、そのWindowsマシンからSambaサーバにログインしようとしている場合は、**Windowsユーザー名**フィールドにWindowsのユーザー名を指定します。**サーバ設定**内にあるユーザー設定の**セキュリティ** タブ上の**認証モード**は、このオプションを有効にするために**ユーザー** に設定しておく必要があります。

Sambaユーザー用の**Sambaパスワード**も設定して、確認の目的で再度、それを入力します。Samba用に暗号パスワードを選択したとしても、全てのユーザーのSambaパスワードはいつもRed Hat Linuxシステムのパスワードとは別の物にされることを推薦します。

既存のユーザーを編集するには、**ユーザーの編集**ボタンをクリックします。既存のSambaユーザーを削除するには、そのユーザーを選択して、**ユーザーの削除** ボタンをクリックします。Sambaユーザーを削除しても、関連したRed Hat Linuxユーザーアカウントを削除するものではありません。

OKボタンをクリックするとすぐにユーザーは変更されます。

17.2.1.3. 共有を追加

図17-5. 共有を追加

共有を追加するには、**追加**ボタンをクリックします。**基本**タブは以下のオプションを設定します：

- **ディレクトリ** — Samba経由で共有するディレクトリ。このディレクトリが存在している必要があります。
- **説明** — 共有の簡単な説明。

- **基本権限** — ユーザーが共有ディレクトリのファイルを読み込む権限だけか、あるいは共有ディレクトリの読み込みと書き込みの権限を持つか決定します。

アクセスタブ上で、指定したユーザーだけが共有にアクセスできるか、又は、全てのSambaユーザーが共有にアクセスを許可されるかを選択します。特定のユーザーにアクセスを許可する選択をする場合、利用できるSambaユーザーの一覧からユーザーを選択します。

OKボタンをクリックするとすぐに共有が追加されます。

17.2.2. コマンド行の設定

Sambaは、`/etc/samba/smb.conf`をその設定ファイルとして使用します。この設定ファイルを変更する場合は、その変更は`service smb restart`コマンドでSambaデーモンを再開始するまで反映されません。

Windowsのワークグループ とSambaサーバの簡単な説明を記入するには、`smb.conf`ファイルの中で次の行を編集します：

```
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
```

*`WORKGROUPNAME`*には、このマシンが属するWindowsワークグループの名前を指定します。*`BRIEF COMMENT ABOUT SERVER`*はオプションで、Sambaシステムに関するWindows用のコメントを入力できます。

Linuxシステム上にSamba共有ディレクトリを作成するには（ニーズやシステムに合わせてファイルを編集した後で）`smb.conf`ファイルに次のセクションを追加します：

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
writable = yes
printable = no
create mask = 0765
```

上記の例では、tfoxとcaroleというユーザーが、SambaクライアントからSambaサーバー上のディレクトリ`/home/share`に対し読み取りと書き込みを行うことができます。

17.2.3. 暗号化パスワード

Red Hat Linux 9では、暗号化されたパスワードがデフォルトで使用可能なため、より安全性が向上しています。暗号化パスワードを使用せず、プレインテキストパスワードを使用する場合、ネットワークパケットスニファを使用して誰かに傍受される可能性があります。したがって、暗号化パスワードを使用することをお勧めします。

Microsoft SMBプロトコルは、当初プレインテキストのパスワードを使用していました。しかし、Windows NT 4.0（サービスパック3以上付き）、Windows 98、Windows 2000、Windows ME、及びWindows XPでは、暗号化したSambaパスワードが必要です。Red Hat Linuxシステムとそれらのオペレーティングシステムの1つが動作しているシステム間でSambaを使用するには、Windowsのレジストリを編集してプレインテキストのパスワードを使用するか、又はLinuxシステムのSambaを設定して暗号化パスワードを使用するかのどちらかです。レジストリを修正する選択をした場合、全てのWindowsマシンでそれを実行する必要があります。—これはリスクを伴い、さらに衝突の原因にもなる可能性があります。より良いセキュリティの為に暗号化されたパスワードの使用が推薦されます。

暗号化したパスワードを使用するようにRed Hat Linuxシステム上のSambaを設定する場合は、次の手順に従ってください：

1. Samba用に個別のパスワードファイルを作成します。既存の/etc/passwdファイルに基づいてこのパスワードファイルを作成する場合は、次のコマンドを入力します。
   ```
   cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   システムがNISを使用する場合は、以下のように入力します。
   ```
   ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   mksmbpasswd.shスクリプトは、sambaパッケージと共に/usr/binディレクトリにインストールされます。
2. rootだけが読み取り/書き込みを行えるようにSambaパスワードファイルのアクセス権を変更します。次のコマンドを使用します。
   ```
   chmod 600 /etc/samba/smbpasswd
   ```
3. このスクリプトでは、ユーザーのパスワードは新しいファイルにコピーされません。そして、Sambaユーザーアカウントはその為のパスワードが設定されるまで有効ではありません。より高度なセキュリティの為に、ユーザーのSambaパスワードは、Red Hat Linuxのパスワードとは別のものを使用されることが推薦されます。各Sambaユーザーのパスワードを設定するには、次のコマンドを使用します（*username*には各ユーザーのユーザー名を指定します）：
   ```
   smbpasswd username
   ```
4. 暗号化パスワードはSamba設定ファイルで有効にする必要があります。ファイルsmb.confで、次の行がコメントアウトされていないことを確認します：
   ```
   encrypt password = yes
   smb passwd file = /etc/samba/smbpasswd
   ```
5. シェルプロンプトでコマンドservice smb restartを入力して、smbサービスが起動されていることを確認します。
6. smbサービスを自動的に起動させたい場合は、ntsysv、chkconfig、**サービス設定ツール**を使用して、ランタイム時にこのサービスを有効にします。詳細については第14章を参照してください。

ヒント

暗号化パスワードの詳細については、/usr/share/doc/samba-<*version*>/docs/htmldocs/ENCRYPTION.html を参照して下さい。(<*version*> をインストールしたSambaのバージョン番号に置き換えます)

passwdコマンドの使用時に、ユーザーのSambaパスワードとシステムパスワードを同期化するためにpam_smbpass PAMモジュールを使用することができます。ユーザーがpasswdコマンドを起動すると、Red Hat Linuxシステムへのログインに使用するパスワードとSamba共有への接続に使用するパスワードは変更されます。

この機能を有効にするには、以下の行をpam_cracklib.soの下の/etc/pam.d/system-authに追加します。

```
password required /lib/security/pam_smbpass.so nullok use_authtok try_first_pass
```

17.2.4. サーバの開始と停止

Samba経由でディレクトリを共有しているサーバ上では、smbサービスが実行されている必要があります。

Sambaデーモンのステータスを表示するには次のコマンドを使用します：

```
/sbin/service smb status
```

以下のコマンドでデーモンを開始します：

```
/sbin/service smb start
```

以下のコマンドでデーモンを停止します：

```
/sbin/service smb stop
```

ブート時にsmbサービスを開始するには以下のコマンドを使用します：

```
/sbin/chkconfig --level 345 smb on
```

また、chkconfig, **ntsysv**あるいは**サービス設定ツール**を使用して、ブート時にスタートするサービスを設定できます。詳細は第14章を御覧下さい。

17.3. Samba共有との接続

Microsoft WindowsマシンからLinuxのSamba共有に接続するには、**隣接ネットワーク(Network Neighborhood)**又は、グラフィカルファイルマネージャを使用します。

Linuxシステムから Samba共有に接続する場合は、シェルプロンプトで次のコマンドを入力します：

```
smbclient //hostname/sharename -U username
```

ここで、*hostname*には、接続したいSambaサーバーのホスト名またはIPアドレスを指定します。*sharename*には、ブラウズしたい共有ディレクトリの名前を指定します。*username*には、このシステムでのSambaユーザー名を指定します。正しいパスワードを入力します。ユーザーのパスワードが必要ない場合は[Enter]キーを押します。

smb:\>プロンプトが表示されれば、正しくログインできたことになります。ログインした後は、**help**と入力するとコマンドの一覧が表示されます。ホームディレクトリの内容を参照するには、*sharename*にユーザー名を指定します。-Uスイッチを指定しない場合は、現在のユーザーのユーザー名がSambaサーバーに渡されます。

smbclientを終了するには、smb:\>プロンプトで**exit**と入力します。

Nautilusを使用して、ネットワーク上の使用可能なSamba共有を表示することもできます。パネル上の**メインメニューボタン** =>**ネットワークサーバ**と進んで、ネットワークのSambaのワークグループの一覧を表示します。また、Nautilusの**場所:**のバーに**smb:**と入力してワークグループを表示することも出来ます。

図17-6に示してある様に、ネットワーク上のそれぞれの利用できるSMBワークグループのアイコンが現れます。

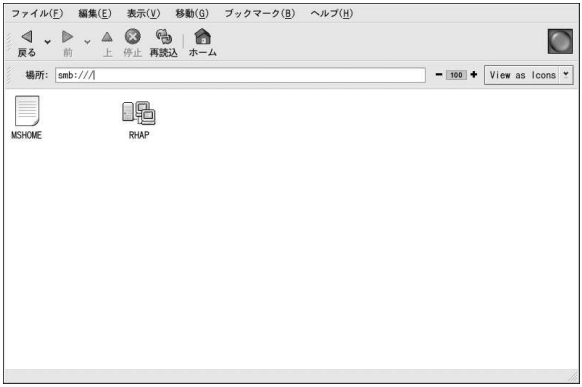


図17-6. Nautilus内のSMBワークグループ

これらのワークグループアイコンの1つをダブルクリックすると、そのワークグループ内のコンピュータの一覧を表示することが出来ます。

図17-7. Nautilus内のSMBマシン

図17-7で見ることが出来る様に、ワークグループ内の各マシン用にアイコンが1つずつあります。どれかアイコンをダブルクリックするとマシン上のSamba共有を表示することが出来ます。ユーザー名とパスワードが必要な場合は、その様に要求されます。

ユーザー名とパスワードを指定する別の方法として**場所:**バーに次の構文で指定してください。（*user*、*password*、*servername*、*sharename*は該当する値で置き換えます）：

```
smb://user:password@servername/sharename/
```

17.4. その他のリソース

ここで説明されていない設定オプションについては、次のリソースを参照してください。

17.4.1. インストールされているドキュメント

- `smb.conf`のmanページ— Samba設定ファイルの設定方法が説明されています。
- `smbd`のmanページ— Sambaデーモンの働きが説明されています。
- `/usr/share/doc/samba-<version-number>/docs/` — `samba`パッケージに組み込まれているHTML形式とテキスト形式のヘルプファイル

17.4.2. 役に立つWebサイト

- http://www.samba.org — SambaのWebページには、参考となるドキュメントや、メーリングリスト情報、GUIインターフェイスの一覧が掲載されています。

redhat.

第18章

DHCP（Dynamic Host Configuration Protocol）

DHCP（Dynamic Host Configuration Protocol）は、クライアントマシンに自動的にTCP/IP情報を割り当てるネットワークプロトコルです。各DHCPクライアントは、中央に配置されたDHCPサーバーに接続し、サーバーはIPアドレス、ゲートウェイ、DNSサーバーなどのクライアントのネットワーク設定情報を返します。

18.1. DHCPを使用する理由

DHCPを使用することにより、クライアントのネットワーク設定の受け渡しを簡単に行うことができます。クライアントシステムを設定するときDHCPを選択すれば、IPアドレス、ネットマスク、ゲートウェイ、DNSサーバーを入力する必要はありません。クライアントはこれらの情報をDHCPサーバーから受け取ります。また、管理者が多数のシステムのIPアドレスを変更する場合もDHCPは便利な機能です。すべてのシステムの再設定を行う代わりに、サーバー上のDHCP設定ファイルを編集することによって、新規のIPアドレスセットを設定できます。組織のDNSサーバーが変更された場合は、DHCPクライアントで変更を行うのではなく、DHCPサーバーで変更を行います。クライアントでネットワークが再起動（またはクライアントがリブート）されると、変更が反映されます。

また、ノートPCなどのモバイル用途のコンピュータがDHCPを使用するよう設定されている場合、各オフィスのDHCPサーバーがこのようなコンピュータをネットワークに接続できるよう設定されていれば、オフィス間を移動するたびにノートPCを再設定するという必要はありません。

18.2. DHCPサーバーの設定

DHCPサーバーを設定するには、設定ファイル`/etc/dhcpd.conf`を使用します。

また、DHCPはファイル`/var/lib/dhcp/dhcpd.leases`を使用してクライアントのリースデータベースを保存します。詳細については項18.2.2を参照してください。

18.2.1. 設定ファイル

DHCPサーバーを設定するには、まずクライアントのネットワーク情報を保存する設定ファイルを作成します。すべてのクライアントに対するグローバルオプションを宣言することも、クライアントシステムごとにオプションを宣言することもできます。

設定ファイルには、任意のタブや空白行を使用して書式をわかりやすく整えることができます。キーワードには大文字小文字の区別があり、先頭がシャープ記号（#）の行はコメントとみなされます。

2つのDNS更新スキームが現在実装されています。— ad-hoc DNS更新モードとinterim DHCP-DNSインターアクションドラフト更新(interaction draft update)モードです。これらの2つがIETF標準プロセスの一部として受理された場合、将来3番目のモード— 標準DNS更新モードが出来るでしょう。DHCPサーバは現在の2つのスキームの内の1つを使用するように設定する必要があります。バージョン3.0b2pl11と以前のバージョンはad-hocモードを使用しました。しかし、もう古くて使用されません。同じような動作を維持したい場合は、設定ファイルの上に次の行を追加します：

```
ddns-update-style ad-hoc;
```

推奨されるモードを使用するには、設定ファイルの上に次の行を追加します：

```
ddns-update-style interim;
```

これらのモード別の詳細を知るには`dhcpd.conf`のman ページをお読み下さい。

設定ファイルのステートメントには、次の2タイプがあります：

- パラメーター— タスクの実行方法、タスクを実行するかどうか、あるいはクライアントに送信するネットワーク設定オプションを表記します。
- 宣言—ネットワークのトポロジの記述、クライアントの記述、クライアントのアドレスの指定、あるいは宣言グループに対するパラメータグループの適用を行います。

一部のパラメータは、optionキーワードで開始する必要があります。オプションは、DHCPオプションを設定するものです。一方、パラメータは、オプションでない値を設定したり、DHCPサーバーの動作を制御したりするものです。

中かっこ（{ }）で囲まれたセクションの前に宣言されたパラメータとオプションは、グローバルパラメータとみなされます。グローバルパラメータは、それ以降のすべてのセクションに適用されます。

重要

設定ファイルを変更した場合、`service dhcpd restart`コマンドでDHCPデーモンを再起動するまでは変更内容は反映されません。

例18-1で は 、routers, subnet-mask、domain-name、domain-name-servers、 及びtime-offsetオプションは、その下で宣言されるhostステートメント用に使用されます。

例18-1に示すように、サブネットの宣言が可能です。サブネット宣言は、ネットワークのすべてのサブネットに対して記述する必要があります。宣言されていない場合、DHCPサーバーは起動できません。

この例では、サブネット内のすべてのDHCPクライアントに対するグローバルオプションが存在し、範囲が宣言されています。クライアントには、範囲内のIPアドレスが割り当てられます。

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  option routers             192.168.1.254;
  option subnet-mask         255.255.255.0;

  option domain-name         "example.com";
  option domain-name-servers    192.168.1.1;

  option time-offset         -18000;   #EasternStandardTime

  range 192.168.1.10 192.168.1.100;
}
```

例18-1. サブネット宣言

同じ物理ネットワークを共有するすべてのサブネットは、例18-2に示すように共有ネットワーク内で宣言する必要があります。共有ネットワーク内のパラメータでサブネット宣言の外にあるものは、グローバルパラメータとみなされます。共有ネットワークの名前は、たとえばテストラボ環境のすべてのサブネットを記述するtest-labのように、ネットワークの記述名にします。

```
shared-network name {
  option domain-name         "test.redhat.com";
  option domain-name-servers    ns1.redhat.com,ns2.redhat.com;
  option routers             192.168.1.254;
  more parameters for EXAMPLE shared-network
  subnet 192.168.1.0 netmask 255.255.255.0 {
     parameters for subnet
```

```
    range 192.168.1.11 92.168.1.31;
 }
 subnet 192.168.1.32 netmask 255.255.255.0 {
    parameters for subnet
    range 192.168.1.33 192.168.1.63;
 }
}
```

例18-2. 共有ネットワーク宣言

例18-3に示すように、グループ宣言を使用して宣言のグループにグローバルパラメータを適用できます。共有ネットワーク、サブネット、ホストやその他のグループをグループ化することができます。

```
group {
 option routers        192.168.1.254;
 option subnet-mask      255.255.255.0;

 option domain-name      "example.com";
 option domain-name-servers   192.168.1.1;

 option time-offset      -18000;   #Eastern Standard Time

 host apex {
  option host-name "apex.example.com";
  hardware ethernet 00:A0:78:8E:9E:AA;
  fixed-address 192.168.1.4;
 }

 host raleigh {
  option host-name "raleigh.example.com";
  hardware ethernet  00:A1:DD:74:C3:F2;
  fixed-address 192.168.1.6;
 }
}
```

例18-3. グループ宣言

サブネット内のシステムに動的IPアドレスをリースするDHCPサーバーを設定するには、例18-4を修正し、実際に使用する値を記述します。これにより、クライアントのデフォルトのリース期間、最大リース期間、ネットワークの設定値を宣言します。この例では、範囲192.168.1.10～192.168.1.100の範囲内のIPアドレスがクライアントシステムに割り当てられます。

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1,192.168.1.2;
option domain-name "example.com";

subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.10 192.168.1.100;
}
```

例18-4. 範囲パラメータ

ネットワークインターフェイスカードのMACアドレスを基にしてクライアントにIPアドレスを割り当てるには、ホスト宣言内のハードウェアイーサネットパラメータを使用します。例18-5の参考例では、ホ

ストアペックス宣言は、MACアドレス00:A0:78:8E:9E:AAのネットワークインターフェイスカードが常にIPアドレス192.168.1.4を受け取るように指定しています。

オプションパラメータホスト名を使用してクライアントにホスト名を割り当てることも可能です。

```
host apex {
 option host-name "apex.example.com";
 hardware ethernet 00:A0:78:8E:9E:AA;
 fixed-address 192.168.1.4;
}
```

例18-5. DHCPを使用した静的IPアドレス

ヒント

Red Hat Linux 9のサンプル設定ファイルを自分用の開始点として利用するのに、カスタム設定オプションを追加できます。次のコマンドでサンプルファイルを適当な場所にコピーします。

```
cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf
```

（<*version-number*>には使用しているDHCPのバージョンが入ります）

オプションのステートメントの全一覧とその機能については、dhcp-optionsのmanページを参照してください。

18.2.2. リースデータベース

DHCPサーバーでは、ファイル`/var/lib/dhcp/dhcpd.leases`を使用してクライアントのリースデータベースを保存します。このファイルは、手動で変更すべきではありません。リースデータベースには、最近割り当てられた各IPアドレスのDHCPリース情報が自動的に保存されます。この情報には、リース期間、IPアドレスの割り当て先、リースの開始/終了日、リースの取得に使用されたネットワークインターフェイスカードのMACアドレスが含まれます。

リースデータベースにおける時刻はすべて、ローカル時でなくグリニッジ標準時（GMT）を使用します。

リースデータベースは、サイズが大きくなり過ぎるのを避けるために、適宜再作成されます。最初に、すべての既知のリースが一時リースデータベースに保存されます。`dhcpd.leases`ファイルの名前が`dhcpd.leases~`に変更され、一時リースデータベースが`dhcpd.leases`に書き込まれます。

リースデータベースの名前がバックアップファイルの名前に変更された後、新規ファイルが書き込まれる前に、DHCPデーモンがkillされたりシステムがクラッシュしたりすることも考えられます。この場合、サービスの起動に必要な`dhcpd.leases`ファイルは存在しません。その際に新しいリースファイルを作成しないようにしてください。新しいファイルを作成すると、それまでのリースはすべて失われ、問題が発生します。これを解決するには、`dhcpd.leases~`バックアップファイルの名前を`dhcpd.leases`に変更して、デーモンを起動してください。

18.2.3. サーバーの起動と停止

重要

DHCPサーバーを初めて起動するとき、`dhcpd.leases`ファイルがなければサーバーは起動できません。このファイルが存在しない場合は、コマンド`touch /var/lib/dhcp/dhcpd.leases`を使用して作成してください。

DHCPサービスを起動するには、`/sbin/service dhcpd start`コマンドを使用します。DHCPサーバーを停止するには、`/sbin/service dhcpd stop`コマンドを使用します。ブート時にデーモンを自動的に起動する必要がある場合は、第14章で説明しているサービスの管理方法に関する情報を参照してください。

システムに複数のネットワークインターフェイスを組み込む場合、そのうちの1つのインターフェイスだけでDHCPサーバーを起動するには、そのデバイスだけでサービスを起動するようにDHCPサーバーを設定します。`/etc/sysconfig/dhcpd`にある`DHCPDARGS`のリストに次のインターフェイス名を追加します。

```
# Command line options here
DHCPDARGS=eth0
```

これは、ファイアウォールマシンにネットワークカードが2つある場合に便利な機能です。一方のネットワークカードをDHCPクライアントとして設定してインターネット用のIPアドレスを取得します。もう一方のネットワークカードは、ファイアウォール内の内部ネットワーク用のDHCPサーバーとして使用できます。内部ネットワークに接続されたネットワークカードだけを指定することにより、ユーザーがインターネット経由でデーモンに接続できなくなるので、システムがより安全になります。

`/etc/sysconfig/dhcpd`で指定できるその他のコマンドラインオプションには次のようなものがあります：

- `-p <portnum>` — dhcpdが監視するudpポート番号を指定します。デフォルトはポート67です。DHCPサーバーは、指定されたupdポートよりも1つ大きな番号のポートにあるDHCPクライアントに応答を送信します。たとえば、デフォルトポート67をそのまま使用する場合、サーバーはポート67に来る要求を監視し、ポート68にあるクライアントに応答します。ここにポートを指定し、DHCPリレーエージェントを使用した場合、DHCPリレーエージェントが監視すべきポートとして同じポートを指定する必要があります。詳細については項18.2.4を参照してください。
- `-f` — フォアグラウンドプロセスとしてデーモンを実行します。これはおもにデバッグに使用されます。
- `-d` — 標準エラー記述子にDCHPサーバーデーモンをログします。これはおもにデバッグに使用されます。このオプションを指定しなかった場合、ログは`/var/log/messages`に書きこまれます。
- `-cf filename` — 設定ファイルの場所を指定します。デフォルトの場所は`/etc/dhcpd.conf`です。
- `-lf filename` — リースデータベースファイルの場所を指定します。リースデータベースファイルがすでに存在する場合、DHCPサーバーを起動するたびに、同じファイルが使用されるようにすることが非常に重要です。このオプションは、生産に関係のないマシンで、デバッグのためだけに使用することを強くお勧めします。デフォルトの場所は`/var/lib/dhcp/dhcpd.leases`です。
- `-q` — デーモンを開始するときに、著作権に関するメッセージを表示しません。

18.2.4. DHCPリレーエージェント

DHCPリレーエージェント（dhcrelay）により、DHCPやBOOTPの要求を、DHCPサーバーを持たないサブネットからほかのサブネットのDHCPサーバーへと中継することができます。

DHCPクライアントが情報を要求すると、DHCPリレーエージェントは自身の起動時に指定された一覧に含まれるDHCPサーバーに要求を転送します。DHCPサーバーのいずれかから応答が返されると、その応答はオリジナルの要求を送信したネットワークにブロードキャストされたりユニキャストされたりします。

INTERFACESの指示文(directive)で/etc/sysconfig/dhcrelay内にインターフェイスが指定されている場合を除き、DHCPリレーエージェントは全てのインターフェイス上でDHCP要求を監視します。

DHCPリレーエージェントを開始するには、service dhcrelay startコマンドを使用します。

18.3. DHCPクライアントの設定

DHCPクライアントを設定する最初のステップは、カーネルがネットワークカードを認識することの確認です。ほとんどのカードはインストールのプロセス中に認識されシステムはそのカード用に正しいモジュールを使用するように設定されます。インストールの後でカードを取り込む場合、**Kudzu** [1] がそれを認識するはずで、対応するカーネルモジュールを設定するように要求してきます。以下のサイトでRed Hat Linuxハードウェア互換性リストを忘れずにチェックして下さい：http://hardware.redhat.com/hcl/。どのカーネルモジュールをロードするか判っているのに、ネットワークカードがインストールプログラム、あるいは**Kudzu**で設定できない場合は、カーネルモジュールのロードについての詳細を第31章で参照して下さい。

DHCPクライアントを手動で設定するには、/etc/sysconfig/networkファイルを修正して、/etc/sysconfig/network-scriptsディレクトリにある各ネットワークデバイスのネットワークと設定ファイルを有効にする必要があります。このディレクトリには、デバイスごとに設定ファイルifcfg-eth0（eth0はネットワークデバイス名）があります。

/etc/sysconfig/networkファイルには、次の行が必要です：

```
NETWORKING=yes
```

このファイルにはより多くの情報が記述されている可能性がありますが、ブート時にネットワークを起動するには、NETWORKING変数をyesに設定する必要があります。

/etc/sysconfig/network-scripts/ifcfg-eth0ファイルには、次の行が必要です：

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

DHCPを使用するよう設定するデバイスごとに設定ファイルが必要です。

DHCPクライアントの設定にグラフィカルインターフェイスを使用するには、第12章に記載されている**ネットワーク管理ツール**の使用法を参照して、DHCPを使用するネットワークインターフェイスを設定してください。

---

1. **Kudzu** はシステムブート時に実行されるハードウェア検出ツールでどのハードウェアが追加、又は削除されたかを判定します。

18.4. その他のリソース

ここで説明されなかった設定オプションについては、以下の資料を参考にして下さい。

18.4.1. インストールされているドキュメント

- dhcpdのmanページ— DHCPデーモンの動作を説明しています。
- dhcpd.confのmanページ—DHCP設定ファイルの設定方法の説明と、いくつかの例が含まれています。
- dhcpd.leasesのmanページ—DHCPリースファイルの設定方法の説明と、いくつかの例が含まれています。
- dhcp-optionsのmanページ—dhcpd.confのDHCPオプション宣言の構文の説明と、いくつかの例が含まれています。
- dhcrelayのmanページ—DHCPリレーエージェントとその設定オプションが説明されています。

第19章

Apache HTTP サーバーの設定

Red Hat Linux 8.0では、Apache HTTP サーバーはバージョン2.0に更新され、異なる設定オプションを使用します。また同じくRed Hat Linux 8.0から始まったもので、パッケージ名がhttpdに変更されています。既存の設定オプションファイルを手動で転換したい場合は、その詳細を*Red Hat Linux* 参照ガイド又は/usr/share/doc/httpd-*<ver>*/migration.htmlで御覧下さい。

Red Hat Linux の以前のバージョンで、**HTTP 設定ツール**を使用して、Apache HTTP サーバーを設定して、アップグレードをしている場合は、そのアプリケーションで設定ファイルを、バージョン2.0の新しい形式に転換できます。**HTTP 設定ツール**を開始して、設定へ必要な変更をして保存します。保存された設定ファイルはバージョン2.0との互換性があります。

HTTP 設定ツールを使用すると、Apache HTTP サーバー用の設定ファイルである/etc/httpd/conf/httpd.confを設定することが出来ます。古いsrm.confファイルやaccess.confファイルは使用しないで、空のままにしておきます。グラフィカルインターフェイスを通して、仮想ホスト、ログの属性、及び接続の最大数などのディレクティブが設定できます。

Red Hat Linux と一緒に出荷されている唯一のモジュールは**HTTP 設定ツール**で設定出来ます。追加のモジュールがインストールされている場合、このツールではそれらを設定できません。

HTTP 設定ツールを使用するには、httpdとredhat-config-httpd RPMパッケージのインストールが必要です。又、同じくX Window Systemとroot権限も必要です。このアプリケーションをスタートするには、**メインメニューボタン** =>**システム設定** =>**サーバ設定** =>**HTTP サーバ**と進みます。あるいは、シェルプロンプト(例えば、XTerm やGNOMEターミナルなど)でredhat-config-httpdと入力します。

用心

このツールを使用する場合は/etc/httpd/conf/httpd.conf設定ファイルを手動で編集しないで下さい。このファイルは、ユーザーが変更を保存してこのプログラムを終了した後で、**HTTP 設定ツール**によって生成されます。**HTTP 設定ツール**で提供されていない追加のモジュールや設定オプションを追加したい場合、このツールは使用できません。

HTTP 設定ツールを使用してApache HTTP サーバーを設定する一般的な手順は次のとおりです:

1. **メイン**タブで基本設定値を設定します。
2. **仮想ホスト**タブをクリックして、デフォルト設定を設定します。
3. **仮想ホスト**タブで、デフォルトの仮想ホストを設定します。
4. 複数のURLや仮想ホストを提供したい場合は、その分の仮想ホストを追加します。
5. **サーバ**タブでサーバー設定値を設定します。
6. **パフォーマンスの調整**タブで接続設定値を設定します。
7. 必要なファイルをすべてDocumentRootディレクトリとcgi-binディレクトリにコピーします。
8. アプリケーションを終了して、その設定を保存する選択します。

19.1. 基本設定

メインタブで、サーバーの基本設定値を設定します。

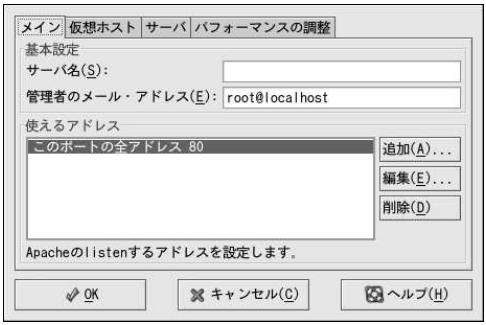


図19-1. 基本設定

サーバ名のテキストフィールドに、自分が使用権限をもっているドメインの完全修飾ドメイン名を入力します。このオプションは、`httpd.conf`の`ServerName`ディレクティブに相当します。`ServerName`ディレクティブは、Webサーバーのホスト名を設定します。このサーバー名は、URLへのリダイレクトを作成するときに使用されます。サーバー名を定義しなかった場合、Webサーバーはシステムの IPアドレスを元に名前解決を試みます。サーバー名は、サーバーのIPアドレスを元に解決されたドメイン名と一致している必要はありません。たとえば、サーバーの実際のDNS名がfoo.example.comであっても、サーバー名をwww.example.comと設定することができます。

管理者のメールアドレスのテキストフィールドには、Webサーバーの管理者の電子メールアドレスを入力します。このオプションは、`httpd.conf`の`ServerAdmin`ディレクティブに相当します。サーバーのエラーページに電子メールアドレスを表示するように設定すると、この電子メールアドレスが使用されます。したがって、ユーザーはサーバーの管理者に電子メールを送信して、問題を報告することができます。デフォルト値はroot@localhostです。

使えるアドレスエリアには、着信した要求を受け取るサーバ上のポートを定義します。このオプションは、`httpd. conf`の`Listen`ディレクティブに相当します。デフォルト設定では、Red HatはApache HTTP サーバーを設定してセキュリティのないWeb通信用のポート80を監視します。

追加ボタンをクリックすると、要求を受け入れる追加ポートを定義できます。図19-2 に示してあるようなウィンドウが表示されます。**全アドレスにListenする**オプションを選択して、ポートに定義してある全てのアドレスを監視するか、あるいはサーバが接続を許可する一意のIPアドレスを**アドレス**フィールドの中に指定します。IPアドレスは、ポート番号毎に1つだけ指定します。同一のポート番号に対して複数のIPアドレスを指定したい場合は、各IPアドレス用にエントリを1つ作成します。DNSルックアップ失敗を防ぐために、もし可能ならドメイン名の代わりにIPアドレスを使用して下さい。 *DNS* と*Apache*に関する事項についての詳細情報はhttp://httpd.apache.org/docs-2.0/dns-caveats.htmlで御覧下さい。

アドレスフィールドにアスタリスク(*)を挿入することは、**全アドレスにListenする**を選択したことになります。**使えるアドレス**のフレームの中の**編集**ボタンをクリックすると、選択済のエントリがフィールドにあること以外は、**追加**ボタンを押した時と同じ画面が表示されます。エントリを削除するには、それを選択して**削除**ボタンをクリックします。

ヒント

1,024より小さい番号のポートを監視するようにサーバを設定する場合は、rootとして起動しなければなりません。番号が1,024以上のポートの場合は、一般のユーザーとして`httpd`を起動できます。

図19-2. 使えるアドレス

19.2. デフォルト設定

サーバー名、**管理者のメールアドレス**、**使えるアドレス**を指定したら、**仮想ホスト**タブをクリックし、**デフォルト設定の編集**ボタンをクリックします。図19-3のようなウィンドウが表示されます。このウィンドウでWebサーバーのデフォルト設定値を設定します。仮想ホストを追加した場合は、その仮想ホスト用に設定した設定値が優先されます。仮想ホストの設定値内に定義されていないディレクティブの場合は、デフォルト値が使用されます。

19.2.1. サイト設定

ディレクトリページの検索リストと**エラーページ**のデフォルト値で殆どのサーバは十分に動作します。これらの設定値がはっきりわからない場合は、変更しないでください。

図19-3. サイト設定

ディレクトリページの検索リストのエントリの一覧は、`DirectoryIndex`ディレクティブを定義します。`DirectoryIndex`は、ユーザーがディレクトリ名の最後にスラッシュ（/）を指定して、ディレクトリのインデックスを要求したときに、サーバーによって表示されるデフォルトページです。

たとえば、ユーザーがhttp://*`www.example.com/this_directory`*/ページを要求すると、存在する場合は`DirectoryIndex`に指定されたページが、それ以外はサーバーが生成したディレクトリ一覧が表示されます。サーバーは、`DirectoryIndex`ディレクティブに一覧されているいずれかのファイルの検索を試み、最初に見つかったファイルを返します。 ファイルが見つからず、そのディレクトリに`Options Indexes`が設定されている場合は、サーバーはディレクトリ内のサブディレクトリとファイルの一覧をHTML形式で生成して返します。

エラーコードセクションでは、問題やエラーが発生したときにクライアントをローカルURLまたは外部URLへリダイレクトするように、Apache HTTP サーバーを設定できます。オプションは、`ErrorDocument`ディレクティブに相当します。クライアントがApache HTTP サーバーへ接続しようしている時に、問題やエラーが発生した場合に、、デフォルトアクションとして、**エラーコード**列に示すような簡潔なエラーメッセージが表示されます。このデフォルト設定を上書きするには、変更したいエラーコードをクリックして選択し、**編集**ボタンをクリックします。デフォルトの簡潔なエラーメッセージを表示するため、**デフォルト**を選択します。**URL**を選択すると、クライアントは外部URLへリダイレクトされます。リダイレクト先として、**場所**フィールドにhttp://を含む完全なURLを入力します。**ファイル**を選択すると、クライアントは内部URLへリダイレクトされ、ファイルの保存場所をWebサーバーのドキュメントルートに置きます。場所を指定する場合は、スラッシュ（/）で開始し、Document Rootからの相対位置を指定します。

例えば、404 Not Foundエラーコードが発生した時に、`404.html`という名前のファイル内のユーザーが作成したWebページへリダイレクトする場合は、`404.html`を*`DocumentRoot`*`/errors/404.html`にコピーします。この場合、*`DocumentRoot`*は、定義したDocument Rootディレクトリです（デフォルトは、`/var/www/html`）。次に、**404 - Not Found**エラーコードが発生したときの動作（Behavior）として**ファイル**を選択し、**場所**として`/errors/404.html`を入力します。

デフォルトのエラーページフッタメニューから、次のいずれかのオプションを選択できます：

- **フッタにメールアドレスを追加** —すべてのエラーページの下部に、デフォルトのフッターと、`ServerAdmin`ディレクティブで指定したWebサイト管理者の電子メールアドレスを表示します。`ServerAdmin`ディレクティブの設定については、項19.3.1.1を参照してください。
- **フッタを表示** — エラーページの下部に、デフォルトのフッターだけを表示します。
- **フッタなし** —エラーページの下部にフッターを表示しません。

19.2.2. ログ

デフォルトでは、サーバは`/var/log/httpd/access_log`ファイルに転送ログを書き込み、`/var/log/httpd/error_log`ファイルにエラーログを書き込みます。

Transfer Log（転送ログ）は、Webサーバーへのすべてのアクセス試行の一覧です。ログには、接続を試みたクライアントのIPアドレス、試行日時、検索対象となったWebサーバー上のファイルが記録されます。この情報の格納先となるパスとファイルの名前を入力します。パスとファイル名をスラッシュ（/）で開始しなかった場合、パスは設定されたServerRootディレクトリからの相対パスとみなされます。このオプションは、`TransferLog`ディレクティブに相当します。

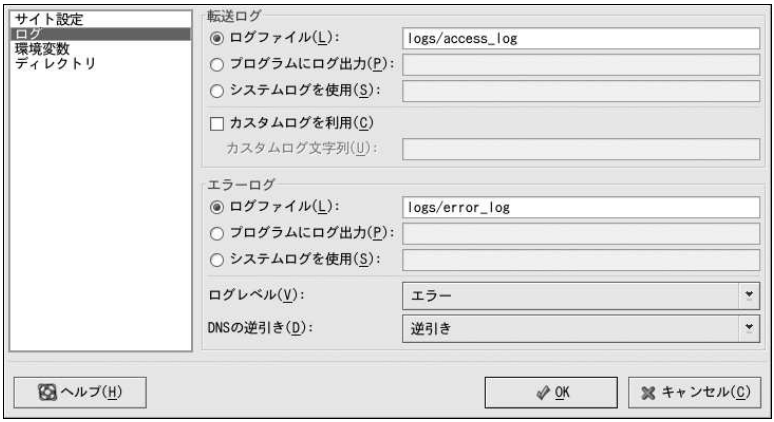


図19-4. ログ

カスタムログを利用をチェックし、**カスタムログ文字列**フィールドにカスタムログ文字列を入力すると、カスタムログ形式を設定できます。これによって、`LogFormat`ディレクティブが設定されます。このディレクティブの形式については、http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formatsを参照してください。

エラーログには、発生したサーバエラーすべての一覧が含まれます。この情報の格納先のパスとファイル名を入力します。パスとファイル名をスラッシュ（/）で開始しなかった場合、パスは設定されたServerRootディレクトリからの相対パスとみなされます。このオプションは、`ErrorLog`ディレクティブに相当します。

ログレベルメニューを使って、エラーログにどの程度詳細にエラーメッセージを記録するかを設定できます。（最も簡潔なレベルから最も詳細なレベルへの順）emerg、alert、crit、error、warn、notice、info、debugのいずれかを設定できます。このオプションは、`LogLevel`ディレクティブに相当します。

DNSの逆引きメニューで選択した値によって、`HostnameLookups` ディレクティブが定義されます。**逆引きなし**を選択すると、値はOffに設定されます。**逆引き**を選択すると、値はOnに設定されます。**二重の逆引き**を選択すると、値はDoubleに設定されます。

逆引きを選択した場合は、サーバーが自動的に、Webサーバーからのドキュメントを要求する各接続のIPアドレスを解決します。IPアドレスの解決とは、サーバーがDNSへ複数の接続を確立して特定のIPアドレスに相当するホスト名を検出することです。

二重の逆引きを選択すると、サーバーはDNSの二重逆引きを実行します。つまり、逆引きを実行した後に、その結果に基づいて正引きを実行します。正引き時には、少なくとも1つのIPアドレスが、最初に逆引きしたアドレスに合致しなければいけません。

DNS要求はサーバーの負荷を高めパフォーマンスを低下させるため、通常、このオプションは**逆引きしない**に設定したままにしておきます。サーバーの負荷が高い場合に、このような逆引きや二重逆引きを実行しようとすると、その影響はかなり顕著に現れます。

逆引きと二重逆引きも、インターネット全体から見ると問題の1つです。個々の接続が各ホスト名をルックアップすると負荷は増大します。個々のWebサーバーの利益は、インターネット全体の利益につながります。したがって、このオプションは、**逆引きしない**に設定しておくのがよいでしょう。

19.2.3. 環境変数

時には、CGIスクリプト、又はサーバサイドインクルード(SSI)ページの為に環境変数を変更する必要があります。Apache HTTP サーバーは、`mod_env`モジュールを使用して、CGIスクリプトやSSIペー

ジへ渡す環境変数を設定できます。**環境変数**ページを使用すると、このモジュールのディレクティブを設定できます。

図19-5. 環境変数

CGIスクリプトのために設定セクションで、CGIスクリプトやSSIページに渡す環境変数を設定します。たとえば、環境変数MAXNUMを50に設定するには、図19-5に示すように**CGIスクリプトのために設定**セクションの**追加**ボタンをクリックし、**環境変数**テキストボックスに**MAXNUM**、及び**設定する値**テキストボックスに**50**と入力します。**OK**ボタンをクリックして一覧に追加します。**CGIスクリプトのために設定**セクションが、SetEnvディレクティブを設定します。

CGIスクリプトに渡すセクションを使用して、サーバが最初に起動した時に環境変数の値をCGIスクリプトに渡すように設定できます。環境変数を確認するには、シェルプロンプトでコマンドenvを入力します。**CGIスクリプトに渡す**セクション内の**追加**ボタンをクリックして、出て来るダイアログボックスに環境変数の名前を入力します。**OK**ボタンをクリックします。**CGIスクリプトに渡す**セクションがPassEnv ディレクティブを設定します。

CGIスクリプトやSSIページへ値を渡さないようにするため環境変数を削除したい場合は、**CGIスクリプトのために解除** セクションを使用します。**CGIスクリプトのために解除**セクションの**追加**ボタンをクリックし、設定解除する環境変数の名前を入力します。これは、UnsetEnvディレクティブに相当します。

これらの環境変数のいずれかを編集するには、それを一覧から選択して、対応する**編集**ボタンをクリックします。一覧からエントリのいずれかを削除するには、それを選択して、対応する**削除**ボタンをクリックします。

Apache HTTP サーバー内の環境変数についてのさらなる情報は、以下のサイトで御覧下さい:

```
http://httpd.apache.org/docs-2.0/env.html
```

19.2.4. ディレクトリ

ディレクトリページを使って、特定のディレクトリのオプションを設定できます。これは、<Directory>ディレクティブに相当します。

図19-6. ディレクトリ

右上の**編集**ボタンをクリックすると、その下の**ディレクトリ** 一覧に指定されているものを除くすべてのディレクトリの**デフォルトのディレクトリオプション**を設定できます。選択したオプションは、<Directory>ディレクティブ内の Options ディレクティブとして一覧表示されます。以下のオプションを設定できます：

- **ExecCGI** —CGIスクリプトを実行できます。このオプションが選択されていないと、CGIスクリプトは実行されません。
- **FollowSymLinks** —シンボリックリンクに従います。
- **Includes** —サーバーサイドインクルードを許可します。
- **IncludesNOEXEC** —サーバーサイドインクルードを許可しますが、CGIスクリプト内の#execコマンドと#includeコマンドは使用できません。
- **Indexes** —DirectoryIndex（index.htmlなど）が要求されたディレクトリに存在しない場合、ディレクトリの内容を書式設定した一覧で表示します。
- **Multiviews** —コンテンツネゴシエート型のマルチビューをサポートします。このオプションはデフォルトでは無効です。
- **SymLinksIfOwnerMatch** —ターゲットファイルやディレクトリの所有者がリンクの所有者と同じ場合にだけ、シンボリックリンクに従います。

特定のディレクトリのオプションを指定するには、**ディレクトリ**一覧ボックスの横にある**追加**ボタンをクリックします。図19-7のウィンドウが表示されます。ウィンドウ下部の**ディレクトリ** テキストフィールドに設定対象のディレクトリを入力します。右側の一覧でオプションを選択し、左側のオプションを使ってOrderディレクティブを設定します。Orderディレクティブは、許可ディレクティブまたは拒否ディレクティブを評価する順序を指定します。**このホストを許可**テキストフィールドと**このホストを拒否**では、次のいずれかを指定できます：

- すべてのホストを許可—**all**と入力すると、すべてのホストへのアクセスを許可
- ドメイン名の一部—指定の文字列に一致する名前、または末尾がその文字列に一致する名前を持つすべてのホストを許可
- 完全なIPアドレス—特定のIPアドレスへのアクセスを許可
- サブネット—**192.168.1.0/255.255.255.0**など
- ネットワークのCIDR指定—**10.3.0.0/16**など

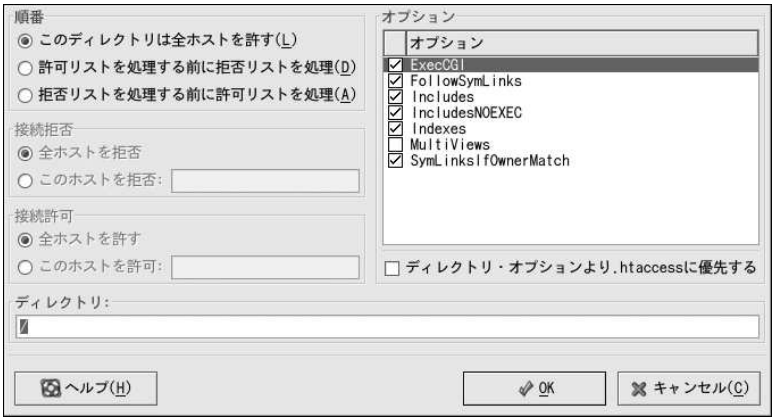


図19-7. ディレクトリの設定

ディレクトリオプションより.htaccessを優先するをチェックすると、.htaccessファイル内の設定ディレクティブが優先されます。

19.3. 仮想ホストの設定値

HTTP 設定ツールを使用して、仮想ホストを設定できます。仮想ホストがあると、異なるIPアドレス、異なるホスト名、または同じマシン上の異なるポートを使って、異なるサーバーを稼動させることができます。たとえば、仮想ホストを使用して、同じサーバ上で、http://www.example.com/やhttp://www.anotherexample.com/といったWebサイトを実行できます。このオプションは、デフォルト仮想ホストとIPベースの仮想ホストの場合は、<VirtualHost>ディレクティブに相当します。名前ベースの仮想ホストの場合は、<NameVirtualHost> ディレクティブに相当します。

仮想ホストのディレクティブ群は、特定の仮想ホストだけに適用されます。**デフォルト設定を編集**ボタンでサーバー全体に対して設定されているが、仮想ホスト設定値内に定義されていないディレクティブに関しては、デフォルト設定値が使用されます。たとえば、**メイン**タブの**管理者のメールアドレス**を定義することはできますが、各仮想ホストに個別の電子メールアドレスを定義することはできません。

HTTP 設定ツールには、図19-8に示してあるように、デフォルトの仮想ホストが含まれます。

図19-8. 仮想ホスト

http://httpd.apache.org/docs-2.0/vhosts/Webサイトや、コンピュータにインストールされているApache HTTP サーバードキュメントには仮想ホストに関する詳しい情報が記載されています。

19.3.1. 仮想ホストの追加と編集

仮想ホストを追加するには、**仮想ホスト**タブの**追加**ボタンをクリックします。一覧内の仮想ホストを選択して**編集**ボタンをクリックし、仮想ホストの設定を編集することもできます。

19.3.1.1. 一般のオプション

一般のオプション設定値は、設定中の仮想ホストだけに適用されます。**仮想ホスト名**テキストフィールドに仮想ホストの名前を設定します。この名前は、**HTTP 設定ツール**が仮想ホストを区別するために使用します。

ドキュメントのルートディレクトリの値は、仮想ホストのrootドキュメント（index.htmlなど）を含むディレクトリに対して設定します。このオプションは、`VirtualHost`ディレクティブ内の`DocumentRoot`ディレクティブに相当します。Red Hat Linux 7.0より前のRed Hat LinuxのApache HTTP サーバーでは、`/home/httpd/html`を`DocumentRoot` として使用していました。Red Hat Linux 9では、デフォルトの`DocumentRoot`は`/var/www/html` です。

管理者のメールアドレスは、`VirtualHost`ディレクティブ内の`ServerAdmin`ディレクティブに相当します。エラーページのフッタに電子メールアドレスを表示するように選択した場合は、フッタにこの電子メールアドレスが使用されます。

ホスト情報セクションでは、**デフォルトの仮想ホスト**、**IPベースの仮想ホスト**、**名前ベースの仮想ホスト**のいずれかを選択します。

デフォルト仮想ホスト

- 設定できるデフォルト仮想ホストは1つだけです。要求されたIPアドレスが別の仮想ホスト内に明示的に一覧されていない場合に、デフォルト仮想ホストの設定値が使用されます。デフォルト仮想ホストが定義されていない場合は、メインのサーバーの設定値が使用されます。

IPベースの仮想ホスト

- **IPベースの仮想ホスト**を選択すると、サーバーのIPアドレスに基づいて<VirtualHost> ディレクティブを設定するためのウィンドウが表示されます。**IP アドレス**フィールドでサーバーのIPアドレスを指定します。複数のIPアドレスを指定するには、各IPアドレスをスペースで区切ります。ポートを指定するときは、*`IP Address:Port`*という構文を使います。「:*」を使用すると、そのIPアドレスにすべてのポートを設定できます。**サーバのホスト名**フィールドに仮想ホストのホスト名を指定します。

名前ベースの仮想ホスト

‘ **名前ベースの仮想ホスト**を選択すると、サーバーのホスト名に基づいてNameVirtualHostディレクティブを設定するためのウィンドウが出てきます。**IPアドレス**フィールドにサーバーのIPアドレスを指定します。複数のIPアドレスを指定するには、各IPアドレスをスペースで区切ります。ポートを指定するときは、*IP Address:Port* という構文を使います。「:*」を使用すると、そのIPアドレスのすべてのポートを設定できます。**サーバのホスト名**フィールドに仮想ホストのホスト名を指定します。**エイリアス** セクションで、**追加**ボタンをクリックし、ホスト名の別名を追加します。ここで別名を追加すると、 NameVirtualHostディレクティブ内にServerAliasディレクティブが追加されます。

19.3.1.2. SSL

注意

SSLハンドシェイクは、該当する名前ベースの仮想ホストを識別するHTTP要求の前（ブラウザがセキュアWebサーバーの証明書を受け取ったとき）に実行されるため、名前ベースの仮想ホストとSSLを同時に使用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、セキュアでないWebサーバーでしか稼動できません。

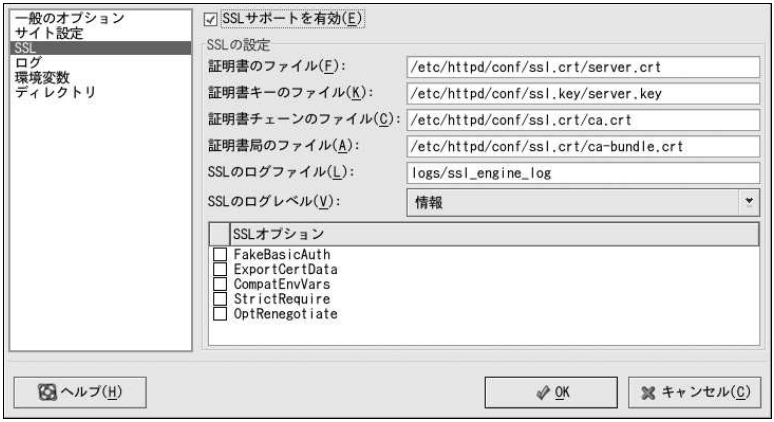


図19-9. SSLサポート

Apache HTTP サーバーにSSLサポートが設定されていないと、Apache HTTP サーバーとクライアント間の通信は暗号化されません。これは、ユーザー情報や機密情報を持たないWebサイトには適しています。たとえば、ソースが公開されたソフトウェアやドキュメントを配信するオープンなWebサイトには、セキュアな通信は必要ありません。ただし、クレジットカード情報が必要なEコマースWebサイトでは、ApacheのSSLサポートを使用して通信を暗号化する必要があります。Apache SSLサポートを有効にすると、mod_sslセキュリティモジュールを使用できるようになります。**HTTP 設定ツール**を使ってこれを有効にするには、**メイン**タブの**使えるアドレス**の一覧のアドレスを使い、ポート443を使用してアクセスできるように設定する必要があります。詳細については項19.1を参照してください。次に、**仮想ホスト**タブで仮想ホスト名を選択し、**編集**ボタンをクリックします。左側のメニューから**SSL**を選択し、**SSLサポートを有効**オプションをチェックします（図19-9参照）。**SSL**

設定セクションは、仮のデジタル証明書を使って事前設定されています。デジタル証明書は、セキュアWebサーバーの認証に使用され、クライアントWebブラウザに対してセキュアサーバーの身元を証明します。自分専用のデジタル証明書を購入する必要があります。自分のWebサイトでは、Red Hat Linuxに組み込まれている仮のデジタル証明書は使用しないでください。CAの承認を受けたデジタル証明書の購入については、第20章を参照してください。

19.3.1.3. その他の仮想ホストのオプション

仮想ホストの**サイト設定**、**環境変数**、**ディレクトリ** といったオプションは、これらのオプションが設定中の個々の仮想ホスト用に設定される点を除けば、**デフォルト設定の編集**ボタンをクリックしたときに設定したディレクティブと同じです。これらのオプションについての詳細は、項19.2を参照してください。

19.4. サーバーの設定

サーバータブでは、基本的なサーバーの設定値を設定できます。通常の環境では、これらのオプションにはデフォルト値を設定しておけば十分に動作します。

図19-10. サーバーの設定

ロックファイル値は、`LockFile`ディレクティブに相当します。このディレクティブは、サーバがUSE_FCNTL_SERIALIZED_ACCEPTまたはUSE_FLOCK_SERIALIZED_ACCEPTのどちらかでコンパイルされるときに使用するロックファイルへのパスを設定します。この値はローカルファイルに格納されている必要があります。`logs`ディレクトリがNFS共有に配置されている場合を除き、デフォルト値のままにしておいてください。このディレクトリがNFS共有に配置されている場合は、デフォルト値をローカルディスク上のrootだけが読み取り可能なディレクトリに変更します。

PIDファイル値は、`PidFile`ディレクティブに相当します。このディレクティブは、サーバーがプロセスID（PID）を記録するファイルを設定します。このファイルの読み取り権は、rootにだけ許可します。通常は、デフォルト値のままにしておきます。

コアをダンプするディレクトリ値は、`CoreDumpDirectory` ディレクティブに相当します。Apache HTTP サーバーは、コアをダンプする前にこのディレクトリへの切り替えを試みます。デフォルト値は、`ServerRoot`です。ただし、サーバーを稼動するユーザーがこのディレクトリへの書き込みを禁止されている場合、コアダンプを書き込むことはできません。デバッグ目的でコアダンプをディスクへ書き込みたい場合は、サーバーを稼動するユーザーが書き込み可能なディレクトリに値を変更します。

ユーザ-値は、`User`ディレクティブに相当します。これは、サーバーが要求に応答するために使用するユーザーIDを設定します。このユーザーの設定値によって、サーバーへのアクセス権が決ま

ります。このユーザーがアクセスできないファイルは、Webサイトのビジターもアクセスできません。Userのデフォルトは、apacheです。

このユーザーは、外部に公開することを前提としたファイルへのアクセス特権だけを持ちます。また、サーバーが引き起こしたCGIプロセスの所有者でもあります。このユーザーは、コードを実行したり、HTTP要求へ応答したりすることはできません。

警告

自分が現在何を実行しているか正確に理解していない限り、Userディレクティブをrootに設定しないでください。UserとしてrootをWebサーバーに大きなセキュリティホールを作り出すことになります。

通常の操作時には、親httpdプロセスは最初にrootとして実行されますが、すぐに、apacheユーザーに引き渡されます。サーバーは、番号が1,024未満のポートにバインドする必要があるため、rootとして起動しなければなりません。番号が1,024未満のポートはシステム用に予約されているため、root以外のユーザーが使用することはできません。サーバーは該当するポートへの接続が完了すると、接続要求を受け入れる前に、プロセスをapacheユーザーに引き渡します。

グループ値は、Groupディレクティブに相当します。GroupディレクティブはUserディレクティブと似ています。Groupは、サーバーがどのグループの配下で要求に応答するかを設定します。デフォルト値は、apacheです。

19.5. パフォーマンスの調整

パフォーマンスの調整タブでは、子サーバープロセスの最大数やクライアント接続のApache HTTPサーバーオプションを設定できます。通常の使用では、これらのオプションにはデフォルト値を設定しておけば十分に動作します。これらの設定値を変更すると、Webサーバー全体のパフォーマンスに影響が及びます。

図19-11. パフォーマンスの調整

接続の最大数は、サーバーが処理する同時クライアント要求の最大数に設定します。接続ごとに、子httpdプロセスが作成されます。プロセスが最大数に達すると、それ以降、子サーバープロセスが解放されるまでは、誰もWebサーバーへ接続することはできません。再コンパイルしない限り、この値を256より大きい数値に設定することはできません。このオプションは、MaxClientsディレクティブに相当します。

接続タイムアウトは、サーバーが通信時に受信と送信を待機する時間を秒単位で定義します。特に、**接続タイムアウト**ではサーバーがGET要求を受け取るまで待機する時間、POSTまたはPUT要求時にTCPパケットを受信するまで待機する時間、TCPパケットに応答するACKを受け取るまで待機する時間を定義します。**接続タイムアウト**は、デフォルトでは300秒に設定されています。通常の環

境では、デフォルト値で十分に動作します。このオプションは、TimeOutディレクティブに相当します。

接続ごとの最大リクエスト数は、1つの固定接続が許容する要求の最大数に設定します。デフォルト値は100です。通常の環境では、デフォルト値で十分に動作します。このオプションは、MaxRequestsPerChild ディレクティブに相当します。

接続ごとのリクエスト数を無制限にするオプションをチェックすると、MaxKeepAliveRequests ディレクティブは0に設定され、要求の許容数は無制限となります。

永続接続を有効オプションが未チェックの場合、KeepAliveディレクティブがfalseに設定されます。このオプションにチェックを付けると、KeepAliveディレクティブはtrueに設定され、KeepAliveTimeoutディレクティブは**次の接続のタイムアウト**値で選択した数値に設定されます。このディレクティブは、サーバーが要求を処理した後、接続を切断する前に、次の要求を待機する時間を秒数で設定します。要求を受け取ると、代わりに**接続タイムアウト**値が適用されます。

永続接続を大きな値に設定すると、サーバーへの接続を試みるユーザー数によっては、サーバーのパフォーマンスが低下することがあります。数値が大きいほど、最後のクライアントがサーバーへ接続した後に、別の接続が解放されるまで待機するサーバープロセス数が多くなります。

19.6. 設定値の保存

Apache HTTP サーバー設定ツールの設定値を保存しない場合は、**HTTP 設定ツール**ウィンドウの右下にある**キャンセル**ボタンをクリックします。保存しないことを確認するメッセージが表示されます。**はい**ボタンをクリックすると保存しないことが確定され、設定値は廃棄されます。

Apache HTTP サーバー設定ツールの設定値を保存する場合は、**HTTP 設定ツール**ウィンドウの下にある**OK**ボタンをクリックします。設定の保存を確認するダイアログウィンドウが開きます。**はい**ボタンをクリックすると、設定値は/etc/httpd/conf/httpd.confに保存されます。オリジナルの設定ファイルは上書きされてしまう点に注意してください。

初めて**HTTP 設定ツール**を使用した場合は、ダイアログウィンドウが開き、設定ファイルを手動で変更したことを示す警告が表示されます。**HTTP 設定ツール**は、httpd.conf設定ファイルが手動で変更されたことを検出すると、そのファイルを/etc/httpd/conf/httpd.conf.bakとして保存します。

重要

設定値を保存した後は、service httpd restartコマンドを使ってhttpdデーモンを再起動する必要があります。このコマンドを実行するには、rootとしてログインしていなければいけません。

19.7. その他のリソース

もっとApache HTTP サーバーについて情報を得るには、以下のリソースを参照して下さい。

19.7.1. インストールされているドキュメント

- Apache HTTP サーバードキュメント— httpd-manualパッケージがインストールしてあり、Apache HTTP サーバーデーモン(httpd)が実行中であれば、Apache HTTP サーバードキュメントを表示できます。Webブラウザを開き、Apache HTTP サーバーを実行しているサーバのhttp://localhostへ移動して、**Documentation**リンクをクリックします。

- `/usr/share/docs/httpd-<version>` — *Apache Migration HOWTO*ドキュメントには、バージョン1.3 からバージョン2.0への変更事項の一覧、及び設定ファイルを手動で転換する方法の情報が含まれています。

19.7.2. 役に立つWebサイト

- http://www.apache.org — *Apache Software Foundation*のWebサイトです。
- http://httpd.apache.org/docs-2.0/ — *Apache HTTP* サーバーバージョン*2.0* ユーザーズガイドを含むApache HTTP サーバーバージョン2上のApache Software Foundationのドキュメントです。
- http://localhost/manual/index.html — ローカルシステムでApache HTTP サーバーをスタートした後、このサイトでApache HTTP サーバーバージョン2.0 ドキュメントを見ることが出来ます。
- http://www.redhat.com/support/resources/web_ftp/apache.html — Red Hat サポートは、役に立つApache HTTP サーバーリンク一覧を管理しています。
- http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html —Red HatによるRed Hat Linux Apacheナレッジベースです。

19.7.3. 関連書籍

- *Apache: The Definitive Guide*ハンドブック第*2*版（Ben Laurie、Peter Laurie共著、オライリー・ジャパン刊）
- *Red Hat Linux* 参照ガイド; Red Hat, Inc. — このコンパニオンマニュアルには、Apache HTTP サーバーバージョン1.3からApache HTTP サーバーバージョン2.0に手動で移行する方法の案内、Apache HTTP サーバーディレクティブの詳細、及びApache HTTP サーバーにモジュールを追加する方法などが含まれています。

第20章

Apache HTTP セキュアサーバーの設定

20.1. はじめに

本章では、OpenSSLライブラリとツールキットを使用できる様に有効にされているmod_ssl セキュリティモジュールを持つApache HTTP サーバーの基本的な情報について説明します。Red Hat Linuxに含まれるこの3つのコンポーネントの組み合わせを本章ではセキュアWebサーバーあるいは単にセキュアサーバーと呼びます。

mod_sslモジュールは、Apache HTTP サーバー用のセキュリティモジュールです。mod_sslモジュールはOpenSSLプロジェクトによって提供されるツールを使用しており、これによって通信を暗号化するという非常に重要な機能がApache HTTP サーバーに追加されます。これとは対照的に、通常のHTTPを使用したブラウザとWebサーバー間の通信は暗号化されないため、ブラウザとサーバー間の経路で誰かに傍受され、読み取られるおそれがあります。

本章は、以上のプログラムのいずれについても、完全かつ唯一の文書となるものではありません。本ガイドでは、可能な限り、特定のテーマに関する詳しい資料が入手できる場所を案内します。

本章では、これらのプログラムのインストール方法について説明します。また、秘密鍵と証明書の要求を生成するために必要な手順や、自己署名証明書の生成方法、セキュアサーバーで使用するための証明書のインストール方法についても説明します。

mod_ssl設定ファイルは/etc/httpd/conf.d/ssl.confに配置されています。このファイルがロードされ、mod_sslが機能できるようにするには、/etc/httpd/conf/httpd.confの中にInclude conf.d/*.conf という記述を入れる必要があります。この記述はデフォルトで、Red Hat Linux 9内のデフォルトのApache HTTP サーバー設定ファイルに含まれています。

20.2. セキュリティ関連パッケージの概要

セキュアサーバーを有効にするには、少なくとも次のパッケージをインストールする必要があります:

httpd

- httpdパッケージには、httpdデーモンとその関連ユーティリティ、設定ファイル、アイコン、Apache HTTP サーバーモジュール、manページ及びApache HTTP サーバーに使用される他のファイルが含まれています。

mod_ssl

- mod_sslには、mod_sslモジュールが含まれています。これは、SSL（Secure Sockets Layer）プロトコルとTLS（Transport Layer Security）プロトコルを使用したApache HTTP サーバーの為の強力な暗号化手法を提供するモジュールです。

openssl

- opensslパッケージには、OpenSSLツールキットが含まれています。OpenSSLツールキットはSSLプロトコルとTLSプロトコルを実装するものです。また、汎用暗号化ライブラリも含まれています。

さらに、Red Hat Linuxに含まれるその他のソフトウェアパッケージにもセキュリティ機能が含まれています。(セキュアサーバーが機能するために必要となるものではありません)。

`httpd-devel`

‘ `httpd-devel`パッケージには、Apache HTTP サーバーinclude ファイル、ヘッダファイル、及びAPXS ユーティリティが含まれています。この製品で提供されているモジュールの他に、余分のモジュールをロードする予定がある場合、これらの全てが必要になります。Apache's DSO 機能を使用したセキュアサーバー上へのモジュールのロードに関する詳細は*Red Hat Linux* 参照ガイドで御覧下さい。

Apache HTTP サーバーにほかのモジュールをロードする予定がない場合は、このパッケージをインストールする必要はありません。

`httpd-manual`

‘ `apache-manual`パッケージには、Apacheプロジェクトの*Apache* ユーザーズガイドがHTML形式で含まれています。このマニュアルはhttp://httpd.apache.org/docs-2.0/ でも公開されています。

OpenSSHパッケージ

‘ OpenSSHパッケージは、リモートマシンにログインしてコマンドを実行するためのネットワーク接続ツールのセットです。OpenSSHツールは、すべてのトラフィック（パスワードを含む）を暗号化するので、ユーザーのマシンとリモートマシン間の通信に対する傍受や接続の乗っ取りなどの攻撃を回避できます。

`openssh`パッケージには、OpenSSHクライアントプログラムとOpenSSHサーバーの双方が必要とするコアファイルが含まれています。`openssh`パッケージには、`rcp`（マシン間でファイルをコピー）の安全な代替手段である`scp`も含まれています。

`openssh-askpass`パッケージは、OpenSSHエージェントの使用時にパスワードを要求するダイアログウィンドウの表示をサポートします。

`openssh-askpass-gnome`パッケージは、GNOMEデスクトップ環境と共に使用できる為、OpenSSHプログラムがパスワードの要求をした時にグラフィカルダイアログウィンドウを表示することが出来ます。GNOMEを実行していて、OpenSSHユーティリティを使用している場合は、このパッケージをインストールする必要があります。

`openssh-server`パッケージには、セキュアシェルデーモン`sshd`のファイルとその関連ファイルが含まれています。セキュアシェルデーモンはOpenSSHスイートのサーバーサイドであり、SSHクライアントをホストに接続させる場合は、それをホストにインストールする必要があります。

`openssh-clients`パッケージには、SSHサーバーとの通信を暗号化するために必要なクライアントプログラムが含まれています。パッケージに含まれるプログラムには、`rsh`の安全な代替手段としての`ssh`、`ftp`(マシン間でのファイル転送用)の安全な代替手段としての`sftp`、`rlogin`(リモートログイン用)の安全な代替手段としての`slogin`、及び`telnet`(Telnetプロトコルを介して別のホストと通信)があります。

OpenSSHの詳細については、第15章と、*Red Hat Linux* 参照ガイド、及びOpenSSHのWebサイトhttp://www.openssh.comを参照してください。

`openssl-devel`

‘ `openssl-devel`パッケージには、各種暗号化アルゴリズムとプロトコルをサポートするアプリケーションのコンパイルに必要な、静的ライブラリとインクルードファイルが含まれています。このパッケージをインストールする必要があるのは、SSLサポートを含むアプリケーションを開発する場合のみです。SSLを使用するだけであれば、このパッケージは必要ありません。

`stunnel`

‘ `stunnel`パッケージはStunnel SSLラッパーを提供します。StunnelはSSLによるTCP接続の暗号化をサポートしているため、デーモンのコードを変更することなく、非SSL対応のデーモンやプロトコル（POP、IMAP、LDAPなど）に暗号化機能を提供することができます。

表20-1では、セキュアサーバーパッケージの概要及び、セキュアサーバーをインストールする際に各パッケージがオプションであるかどうかを表示しています。

パッケージ名	オプション(?)
httpd	いいえ
mod_ssl	いいえ
openssl	いいえ
httpd-devel	はい
httpd-manual	はい
openssh	はい
openssh-askpass	はい
openssh-askpass-gnome	はい
openssh-clients	はい
openssh-server	はい
openssl-devel	はい
stunnel	はい

表20-1. セキュリティパッケージ

20.3. 証明書とセキュリティの概要

セキュアサーバーは、SSL（Security Sockets Layer）プロトコルと、多くの場合CA（認証局：Certificate Authority）が発行するデジタル証明書を組み合わせてセキュリティ機能を実現します。SSLは、ブラウザとの間で通信を暗号化し、ブラウザとセキュアサーバーとの相互認証を扱います。CAによって承認されたデジタル証明書は、セキュアWebサーバーに対する認証を与えるものです（CAは組織の身元を保証します）。ブラウザがSSL暗号化を使用して通信を行うときは、ナビゲーションバーのURLの先頭にhttps://という接頭辞が表示されます。

暗号化は鍵の使用によって決まります（鍵はデータ形式における秘密の符号化/復号化の輪と考えることができます）。従来の、つまり対称式の暗号法では、トランザクションの両端で同じ鍵を持ち、その鍵を使用して互いの伝送データを復号します。公開、つまり非対称の暗号法では、公開鍵と秘密鍵の2つの鍵が共存します。個人あるいは組織は秘密鍵を秘匿し、公開鍵を発行します。公開鍵によって暗号化されたデータは、秘密鍵を使用しないと復号できません。秘密鍵によって暗号化されたデータは、公開鍵を使用しないと復号できません。

セキュアサーバーをセットアップするには、公開暗号法を使用して公開鍵と秘密鍵の組を作成します。ほとんどの場合、証明書の要求（公開鍵を含む）、企業の身元を保証するもの、手数料をCAに送ります。CAは証明書の要求と身元を検証して、セキュアサーバーの証明書を返送します。

セキュアサーバーは、自分自身の身元をWebブラウザに対して明らかにするために、証明書を使用します。自分自身の証明書（「自己署名」証明書）を生成することも、CA（認証局）から証明書を取得することも可能です。信頼できるCAが発行する証明書により、Webサイトが特定の企業または組織に関連付けられていることが保証されます。

別の方法として、自分自身の自己署名証明書を作成することができます。ただし、自己署名証明書は、殆どの生産稼働環境では使用すべきではないことに注意してください。ユーザーのブラウザが、自己署名証明書を自動的に受け入れることはありません。— ブラウザは、証明書を受け入れて安全な接続を作成するかどうかをユーザーに問い合わせます。自己署名証明書とCA署名証明書の相違についての詳細は、項20.5を参照してください。

自己署名証明書を作成、またはCAからの署名済み証明書を取得したら、セキュアサーバーにインストールする必要があります。

20.4. 既存の鍵と証明書の使用

すでに鍵と証明書を保有している場合（たとえば、他社のセキュアWebサーバー製品に代えてセキュアサーバーをインストールする場合）、セキュアサーバーにおいてもおそらく既存の鍵と証明書を使用できます。ただし、次のような2つの状況では、既存の鍵と証明書を使用することはできません：

- 自分の*IP*アドレスまたはドメイン名を変更する場合— 証明書は特定のIPアドレスとドメイン名の組に対して発行されます。したがって、IPアドレスまたはドメイン名を変更する場合は、新しい証明書を取得する必要があります。
- *VeriSign*からの証明書を保有していて、サーバーソフトウェアを変更する場合 —VeriSignは広く使用されているCAです。別の目的ですでにVeriSign証明書を取得している場合、新しいセキュアサーバーにおいても既存のVeriSign証明書を使用することを考えるかもしれませんが、これは許されません。VeriSignの証明書は、特定のサーバーソフトウェアとIPアドレス/ドメイン名の組み合わせに対して発行されるものであるからです。

  これらのパラメータのいずれかを変更する場合(たとえば、過去に別のセキュアサーバー製品を使用したことがある場合)、以前の設定で使用するために取得したVeriSign証明書は、新しい設定では機能しません。新しい証明書を取得する必要があります。

既存の鍵と証明書が利用可能である場合は、新しい鍵を生成して新たに証明書を取得する必要はありません。ただし、鍵と証明書が含まれているファイルを移動し、名前を変更しなければならない場合があります。

既存の鍵ファイルは次の場所に移動します：

```
/etc/httpd/conf/ssl.key/server.key
```

既存の証明書ファイルは次の場所に移動します：

```
/etc/httpd/conf/ssl.crt/server.crt
```

鍵と証明書を移動した後は、項20.9へ進んで下さい。

Red Hatセキュアwebサーバーからアップグレードしている場合、古い鍵（`httpsd.key`）と証明書（`httpsd.crt`）は`/etc/httpd/conf/`に配置されます。鍵と証明書を移動して名前を変更して、セキュアサーバーがそれらを使用できるようにする必要があります。次の2つのコマンドを使用して鍵と証明書のファイルを移動し、名前を変更します：

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

それから次のコマンドでセキュアサーバーを開始します：

```
/sbin/service httpd start
```

セキュアサーバー用のパスワードを入力するよう指示するプロンプトが表示されます。パスワードを入力して[Enter]キーを押すと、サーバーが起動します。

20.5. 証明書の種類

Red Hat LinuxのRPMパッケージからセキュアサーバーをインストールすると、ランダム鍵とテスト証明書が生成され、適切なディレクトリに保存されます。ただし、セキュアサーバーの使用を開始する前に、独自の鍵を生成して、サーバーの身元を正しく示す証明書を取得する必要があります。

セキュアサーバーを稼動させるには鍵と証明書が必要です。— 自己署名証明書を作成するか、CA署名済みの証明書を購入するかのどちらかが必要です。では、この2つの相違は何でしょうか。

CA署名済み証明書によって得られるサーバーの重要な機能には、次のものがあります：

- 通常、ブラウザはユーザー操作を要求せずに自動的に証明書を認識し、安全な接続を許可します。
- CAが署名済み証明書を発行するとき、ブラウザに対してWebページを提供する組織の身元をCAが保証することになります。

セキュアサーバーを公衆アクセスの対象とする場合は、このサーバーがCA署名済みの証明書を保有していれば、Webサイトへの訪問者に対して、そのサイトを所有すると主張する組織の身元が保証されていることを示します。CAは、証明書に署名する前に、証明書を要求する組織が本当にその組織であることを確認します。

SSLをサポートするWebブラウザのほとんどは、自動的に受け入れる証明書の発行元であるCAの一覧を保持しています。この一覧にないCAからの証明書が検出された場合、ブラウザは、接続を受け入れるか、あるいは拒否するかをユーザーに確認します。

セキュアサーバーで使用する自己署名証明書を生成することもできますが、自己署名証明書の機能は、CAによって署名された証明書と同じではないことを認識しておいてください。自己署名証明書はユーザーのブラウザによって自動的に認識されることはなく、Webサイトを所有する組織の身元を保証するものでもありません。CAによって署名された証明書であれば、セキュアサーバーにとって重要なこの2つの機能を備えています。セキュアサーバーを生産稼働環境で使用する場合は、おそらくCAによって署名された証明書が必要になります。

CAから証明書を取得する手順は非常に簡単です。以下にその概要を示します：

1. 暗号化用の秘密鍵と公開鍵の組を作成します。
2. 公開鍵に基づいて証明書の要求を作成します。証明書の要求には、サーバーやサーバーを運用する企業に関する情報が含まれます。
3. 証明書の要求を、自社の身元を証明する文書と共にCAに送付します。どの認証局を選択すべきかは、おそらく過去の経験、または友人や同僚の経験、あるいは純粋に金銭的要因によって決められるでしょう。

   証明書を取得するCAを決定したら、各機関の証明書取得マニュアルに従ってください。
4. CAは、申請者の身元が主張どおりであることを確認すると、デジタル証明書を返送します。
5. この証明書をセキュアサーバーにインストールして、安全なトランザクションの処理を開始します。

CAから証明書を取得する場合も、自分自身の自己署名証明書を作成する場合でも、最初の手順として鍵を生成します。鍵の作成方法については、項20.6を参照してください。

20.6. 鍵の生成

鍵の生成にはrootで操作する必要があります。

最初に、cdコマンドを実行して/etc/httpd/confディレクトリに移動します。次の2つのコマンドを実行して、インストール時に生成された鍵と証明書を削除します。

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

次に、自分自身のランダム鍵を作成します。/usr/share/ssl/certsディレクトリに移動して、次のコマンドをタイプします。

```
make genkey
```

次のようなメッセージが表示されます：

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

ここでパスワードを入力します。安全のため、パスワードは8文字以上で、数字や句読点が含まれている必要があります。また、辞書にある単語は使用しないでください。また、パスワードは大文字/小文字を区別することを忘れないで下さい。

注意

セキュアサーバーを起動するたびにこのパスワードを入力する必要があります。パスワードは忘れないでください。

パスワードが正しいことを確認するために、再入力する必要があります。正しく入力すると、/etc/httpd/conf/ssl.key/server.keyというファイルが作成され、ここに鍵が含まれています。

セキュアWebサーバーを起動するたびにパスワードを入力しないようにするには、鍵を作成する場合にmake genkeyではなく、次の2つのコマンドを使用します。

コマンドを次のとおり実行して鍵を作成します：

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

そして、更に次のコマンドを使用して、このファイルの権限が正しく設定されていることを確認します：

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

上記のコマンドを使用して鍵を作成した場合は、セキュアサーバーを起動するときにパスワードを入力する必要はありません。

用心

セキュアWebサーバーのパスワード機能を無効にすると、セキュリティ上のリスクが発生します。セキュアWebサーバーのパスワード機能を無効にすることはお勧めできません。

パスワードを使用しない場合に発生する問題は、直接ホストマシンのセキュリティに影響します。たとえば、悪意のある人物がホストマシンの通常のUNIXセキュリティを突破した場合、その人物はシステムの秘密鍵（server.keyファイルの内容）を入手できるでしょう。この鍵を使用すれば、Webページを偽造できて、本来の所有者のサイトのように見せかけることもできるのです。

ホストコンピュータでUNIXセキュリティに関する作法が厳密に守られていれば（オペレーティングシステムのすべてのパッチとアップデートを公開と同時にインストールし、不要なサービスあるいは危険度が高いサービスは実行しない、など）、セキュアWebサーバーのパスワードは不要であるようにも思えます。ただし、セキュアサーバーは頻繁に再起動するものではないので、ほとんどの場合はパスワードを入力することによって得られる安全性に価値があるはずです。

server.keyファイルの所有者はシステムのrootユーザーとし、ほかのユーザーはアクセスできないようにしてください。このファイルのバックアップコピーを作成し、安全な場所に保存してください。バックアップコピーが必要となるのは、証明書の要求を作成するためにserver.keyファイルを使用した後、このファイルが失われると、証明書が無効になり、CAの支援を受けられなくなるためです。その場合、唯一のオプションは、新しい証明書を要求(そして支払)をすることになります。

CAから証明書を購入する場合は、項20.7に進みます。自己署名証明書を作成する場合は、項20.8に進みます。

20.7. 証明書要求の作成とCAへの送付

鍵を作成した後、次は選択したCAに送る必要のある証明書要求を生成します。/usr/share/ssl/certsディレクトリに居ることを確認して次のコマンドをタイプします:

```
make certreq
```

次のようなメッセージが表示されたら、パスワードを入力します(パスワードを無効にした場合を除く):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

鍵の生成時に選択したパスワードを入力します。指示に続いて一連の項目が表示されます。各項目への応答を入力してください。入力した情報は証明書の要求に組み込まれます。画面表示と応答の例を次に示します:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.example.com
Email Address []:admin@example.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

デフォルトの入力値は、入力項目の直後に角かっこ[]で囲んで表示されます。たとえば、最初に要求される情報は証明書が使用される国の名前であり、次のように表示されます:

```
Country Name (2 letter code) [GB]:
```

かっこ内のデフォルト値はGBです。デフォルト値をそのまま使用するには、[Enter]を押し、そうでない場合は、2文字の国コードを入力します。

残りの値は自分で入力する必要があります。これらの全ては自然に判る内容です。但し、次のようなガイドラインに従う必要があります：

- 市や州の名前は省略せず、正しく入力してください（たとえば、St.LouisではなくSaint Louis）。
- このCSRをCAに送信するときは、すべてのフィールド、特に`Organization Name`と`Common Name`が正しく入力されているよう注意してください。CAはCSRに記載された情報を調べ、`Common Name`として提供するものに対する責任の所在が申請者の組織にあるかどうかを確認します。CSRに記載されている情報が無効であるとCAが判断した場合、そのCSRは拒否されます。
- `Common Name`には、サーバーのエイリアス(別名)ではなく、セキュアサーバーの本当の名前（有効なDNS名）を入力してください。
- `Email Address`には、Webマスターやシステム管理者の電子メールアドレスを入力します。
- @、#、&、!などの特殊な文字は避けてください。CAの中には、特殊文字を含む証明書要求を拒否するものがあります。したがって、社名に「&」が含まれている場合は、「&」ではなく「and」と入力してください。
- 余分な属性（`A challenge password`と`An optional company name`）は使用しないでください。これらのフィールドに入力せずに続行するには、[Enter]キーを押して、デフォルト値である空白を受け入れます。

情報の入力を終了すると、`/etc/httpd/conf/ssl.csr/server.csr`という名前のファイルが作成されます。このファイルがCAに送付可能な状態の証明書要求です。

CAを決定したら、CAのWebサイトで指示されている手順に従います。証明書要求の提出方法、その他の必要事項、CAに対する支払い方法などを確認してください。

CAの要件を満たしていれば、CAから証明書が送付されます（通常は電子メール）。送付された証明書を、`/etc/httpd/conf/ssl.crt/server.crt`として（カット&ペーストしてください）保存します。このファイルのバックアップを忘れずに作成して保存して下さい。

20.8. 自己署名証明書の作成

自分自身の自己署名証明書を作成できます。自己署名証明書は、CAの署名済み証明書によるものと同等のセキュリティを保証するものではないことに注意してください。証明書の詳細については、項20.5を参照してください。

自己署名証明書を作成する場合は、最初に項20.6の説明に従ってランダム鍵を作成する必要があります。鍵を作成したら、`/usr/share/ssl/certs`のディレクトリに移動して次のコマンドをタイプします：

```
make testcert
```

次のメッセージが表示されたら、パスワードを入力します（パスワードなしで鍵を生成した場合を除く）：

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

パスワードを入力すると（パスワードなしで鍵を作成した場合、プロンプトは表示されません）、さらに情報を要求するメッセージが表示されます。表示される項目と入力の例を次に示します（特に組織とホストに関しては正しく情報を入力してください）：

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.example.com
Email Address []:myemail@example.com
```

情報を正しく入力すると、自己署名証明書が作成され、/etc/httpd/conf/ssl.crt/server.crtに保存されます。証明書を生成した後は、次のコマンドを使用してセキュアサーバーを再起動する必要があります。

```
/sbin/service httpd restart
```

20.9. 証明書のテスト

デフォルト設定でインストールされたテスト証明書、CA署名の証明書、及び自己署名証明書をテストするには、以下のホームページをWebブラウザで開きます(*server.example.com*は、使用するドメイン名で入れ換えます) :

```
https://server.example.com
```

注意

httpの後ろのsに注意して下さい。https:は、安全なHTTPのトランザクションの表示として使用される接頭辞です。

一般に知られているCAから取得したCA署名証明書を使用している場合、おそらくブラウザは自動的に証明書を受け入れ（ユーザーの介入なしに）、セキュア接続を作成します。テスト証明書と自己署名証明書はCAによって署名されていないので、ブラウザが自動的に認識することはありません。CAから取得した証明書を使用していない場合は、証明書を受け入れるにはブラウザに表示される指示に従います。

ブラウザが証明書を受け入れると、セキュアサーバーによって、デフォルトのホームページが表示されます。

20.10. セキュアサーバーへのアクセス

セキュアサーバーにアクセスするには、以下のようにURLを指定します：

```
https://server.example.com
```

セキュアサーバー以外のサーバーには以下の様なURLの指定を使います：

```
http://server.example.com
```

セキュアなWeb通信を行うための標準ポートはポート443です。セキュアでないWeb通信を行うための標準ポートはポート80です。セキュアサーバーのデフォルトの設定では、これらの標準ポートの両方を監視します。したがって、URLでポート番号を指定する必要はありません（ポート番号は指定されているものとみなされます）。

ただし、標準的ではないポート（つまり、80または443以外）を監視するようにサーバーを設定した場合は、その非標準ポートでサーバーに接続するURL全てにポート番号を指定する必要があります。

たとえば、ポート12331でセキュアでない仮想ホストが稼動するようにサーバーを設定してあるとします。その場合、仮想ホストに接続するためのURLには、ポート番号を指定しなければなりません。次のURLの例は、ポート12331で監視を行うセキュアでないWebサーバーへの接続を試みるものです：

```
http://server.example.com:12331
```

20.11. その他のリソース

Apache HTTP サーバーに関する参照文献については項19.7を御覧下さい。

20.11.1. インストールされているドキュメント

- `mod_ssl documentation` — Web ブラウザを開き、Apache HTTP サーバーを実行していて`httpd-manual`パッケージをインストールしてあるサーバー上でhttp://localhost/manual/mod/mod_ssl.html を開いて下さい。

20.11.2. 役に立つWebサイト

- http://www.redhat.com/mailing-lists/ — このURLでredhat-secure-serverのメールリストを購読することができます。

  また、redhat-secure-serverのメールリストの購読は、<`redhat-secure-server-request@redhat.com`>にEメールで、件名の中に*subscribe(*購読*)*と書いて送ることでも達成出来ます。
- http://www.modssl.org —`mod_ssl` Webサイトは、`mod_ssl`の最も信頼できる情報源です。このWebサイトには、http://www.modssl.org/docsの「*User Manual*」をはじめとする豊富なドキュメントがあります。

20.11.3. 関連書籍

- *Apache*ハンドブック第*2*版（Ben Laurie、Peter Laurie共著、オライリー・ジャパン刊）

第21章
BINDの設定

本章の説明は、読者がBINDとDNSについての基本を理解していることを前提としています。BINDとDNSの概念については説明していません。本章では、**Bind 設定ツール** (redhat-config-bind)を使用して、基本的なBINDサーバーのゾーンを設定する方法について説明します。**Bind 設定ツール**は毎回、変更を適用する度に/etc/named.conf設定ファイルと/var/namedディレクトリ内のゾーン設定ファイルを作成します。

重要

/etc/named.conf設定ファイルは編集しないでください。ユーザーが変更を適用した後で、**Bind 設定ツール**によりこのファイルが生成されます。**Bind 設定ツール** を使用して実行できない設定をする場合は、それを/etc/named.customに追加します。

Bind 設定ツールではrootの権限とX Window Systemが必要です。**Bind 設定ツール**を起動するには、パネル上から**メインメニューボタン** =>**システム設定** =>**サーバ設定** => **ドメインネームサービス**と進みます。又はシェルプロンプト(XTermやGNOMEターミナルなど)でコマンドredhat-config-bindを入力します。

図21-1. Bind 設定ツール

Bind 設定ツールはデフォルトのゾーンのディレクトリが/var/namedになるよう設定されます。すべてのゾーンファイルは、このディレクトリに関連付けて指定します。**Bind 設定ツール**は、また、値が入力された時に基本的な構文チェック機能も持ちます。例えば、有効なエントリがIPアドレスである場合、テキストエリアに入力できるのは数字とドット (.) だけです。

Bind 設定ツールを使用して、正引きマスターゾーン、逆引きマスターゾーン、スレーブゾーンを追加できます。図21-1に示すように、ゾーンの追加後、それをメインウィンドウから編集または削除することもできます。

ゾーンを追加、編集、あるいは削除したら、**保存**ボタンをクリックするか、又は**ファイル-保存**を選び/etc/named.conf 設定ファイルと/var/namedディレクトリ内の全ての個別ゾーンファイルに書き込む必要があります。また、変更を保存するとnamedサービスにより設定ファイルがリロードされます。**ファイル-終了**を選択して、変更を保存してからアプリケーションを終了します。

21.1. 正引きマスターゾーンの追加

正引きマスターゾーン（別名プライマリマスター）を追加するには、**新規**ボタンをクリックし、**正引きマスターゾーン**を選択して、**ドメイン名**のテキストエリアにマスターゾーンのドメイン名を入力します。

図21-2のような新しいウィンドウが、以下のオプションを表示して現れます：

- **名前** — 前のウィンドウで入力したドメイン名
- **ファイル名** — /var/namedを基準としたDNS データベースファイルの名前。ドメイン名に、付加してある.zoneとともにプリセットしてあります。
- **連絡先** — マスターゾーンのおもな連絡先の電子メールアドレス。
- **プライマリネームサーバ-（SOA）** — SOA（State of authority）レコード。これは、このドメインに関する最良の情報源であるネームサーバーを指定するものです。
- **シリアル番号** — DNSデータベースファイルのシリアル番号。この番号は、ゾーンのスレーブネームサーバーが最新のデータを取得できるようにするために、ファイルの変更のたびにインクリメントする必要があります。設定の変更のたびに、**>Bind 設定ツール**によって、この番号はインクリメントされます。**シリアル番号**の隣にある**設定** ボタンをクリックして、この番号を手動でインクリメントすることもできます。
- **時間設定** — DNSデータベースファイル内に保存される**更新**、**再試行**、**期限切れ**、**最小**（TTL：Time to Live、有効期限）の値。全ての値は秒単位です。
- **レコード** —**ホスト**、**エイリアス**、**ネームサーバー**の各種レコードリソースの追加、編集、削除。

図21-2. 正引きマスターゾーンの追加

プライマリネームサーバ(SOA)を指定する必要があります。**レコード**のセクションで**追加**ボタンをクリックして、少なくとも1つのネームサーバレコードが指定される必要があります。

正引きマスターゾーンの設定が終了したら、**OK**ボタンをクリックして図21-1に示したメインウィンドウに戻ります。プルダウンメニューから**保存**ボタンをクリックして、/etc/named.conf設定ファイルを書き込み、/var/namedディレクトリ内の個々のゾーンファイル全てを書き込み、デーモンに設定ファイルをリロードさせます。

この設定は、/etc/named.confの中に次に似たようなエントリを作成します：

```
zone "forward.example.com" {
```

```
type master;
file "forward.example.com.zone";
};
```

この設定では以下の情報を含むファイル/var/named/forward.example.com.zoneも作成されます。

```
$TTL 86400
@   IN   SOA  ns.example.com. root.localhost (
          2 ; serial
          28800 ; refresh
          7200 ; retry
          604800 ; expire
          86400 ; ttl
          )


   IN   NS   192.168.1.1.
```

21.2. 逆引きマスターゾーンの追加

逆引きマスターゾーンを追加するには、**新規**ボタンをクリックして、**逆引きマスターゾーン**を選択します。設定するIPアドレスの範囲の最初の3つのオクテットを入力します。たとえば192.168.10.0/255.255.255.0というIPアドレスの範囲の設定を行う場合、**IPアドレス(最初の3つのオクテット)**テキストエリアに192.168.10と入力します。

図21-3の新しいウィンドウが表示されます。このウィンドウには、以下のオプションが表示されます：

1. **IPアドレス** —以前のウィンドウに入力した最初の3つのオクテット
2. **逆引きIPアドレス** —編集不可。入力されたIPアドレスで充填されています。
3. **連絡先** —マスターゾーンの主な連絡先の電子メールアドレス
4. **ファイル名** —/var/namedディレクトリ内に置かれるDNSデータベースファイルのファイル名。
5. **プライマリネームサーバー-（SOA）** —SOA（State of authority）レコード。これは、このドメインに関する最良の情報源であるネームサーバーを指定するものです。
6. **シリアル番号** — DNSデータベースファイルのシリアル番号。この番号は、ゾーンのスレーブネームサーバーが最新のデータを取得できるようにするために、ファイルの変更のたびにインクリメントする必要があります。設定の変更のたびに、**>Bind 設定ツール**によって、この番号はインクリメントされます。**シリアル番号**の隣にある**設定** ボタンをクリックして、この番号を手動でインクリメントすることもできます。
7. **時間設定**— DNSデータベースファイル内に保存される**更新**、**再試行**、**期限切れ**、**最小**（TTL：Time to Live、有効期限）の値。
8. **ネームサーバー** — 逆引きマスターゾーンのネームサーバの追加、編集、削除。少なくともネームサーバが1つ必要です。
9. **逆引きアドレステーブル** — 逆引きマスターゾーン内のIPアドレスとそのホスト名の一覧。例えば、192.168.10と言う逆引きマスターゾーンについて**逆引きアドレステーブル**に192.168.10.1とホスト名one.example.comを追加することが出来ます。ホスト名の最後にはピリオド（.）を付加し、それがフルホスト名であることを指定する必要があります。

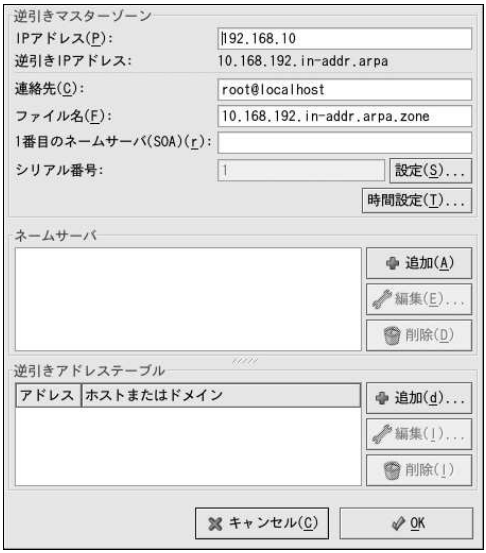


図21-3. 逆引きマスターゾーンの追加

プライマリ ネームサーバ(SOA)を指定する必要があります。そして**ネームサーバ**セクション内の**追加**ボタンをクリックして、少なくとも1つのネームサーバ記録を指定する必要があります。

逆引きマスターゾーンの設定が終了したら、**OK**ボタンをクリックして図21-1に示してあるようにメインウィンドウに戻ります。プルダウンメニューから**保存**ボタンをクリックして/etc/named.conf設定ファイルに書き込み、さらに/var/namedディレクトリ内の個々のゾーンファイルを全て書き込み、デーモンに設定ファイルをリロードさせます。

この設定は/etc/named.confの中に次と似たようなエントリを作成します：

```
zone "10.168.192.in-addr.arpa" {
    type master;
    file "10.168.192.in-addr.arpa.zone";
};
```

この設定で、以下の情報を含むファイル/var/named/10.168.192.in-addr.arpa.zoneも作成されます。

```
$TTL 86400
@   IN   SOA  ns.example.com. root.localhost (
          2 ; serial
          28800 ; refresh
          7200 ; retry
          604800 ; expire
          86400 ; ttk
          )


@   IN   NS   ns2.example.com.

1   IN   PTR  one.example.com.
2   IN   PTR  two.example.com.
```

21.3. スレーブゾーンの追加

スレーブゾーン（別名セカンダリマスター）を追加するには、**新規**ボタンをクリックし、**スレーブゾーン**を選択します。**ドメイン名**テキストエリアには、スレーブゾーンのドメイン名を入力します。

図21-4に示すような新しいウィンドウが表示されます。このウィンドウには以下のオプションが表示されています。

- **名前** — 以前のウィンドウで入力したドメイン名。
- **マスターリスト** — スレーブゾーンがデータを取得するネームサーバー。それぞれの値は有効なIPアドレスでなければなりません。テキストエリアに入力できるのは数字とドット（.）だけです。
- **ファイル名** —/var/namedに置かれるDNSデータベースファイルのファイル名。

図21-4. スレーブゾーンの追加

スレーブゾーンの設定が終了したら、**OK**ボタンをクリックして図21-1に示したメインウィンドウに戻ります。**保存**ボタンをクリックして、/etc/named.conf設定ファイルに書き込み、デーモンに設定ファイルをリロードさせます。

この設定は、/etc/named.confの中に次に似たようなエントリを作成します：

```
zone "slave.example.com" {
    type slave;
    file "slave.example.com.zone";
    masters {
        1.2.3.4;
        };
};
```

マスターサーバーからゾーンデータがダウンロードされるとき、namedサービスにより設定ファイル/var/named/slave.example.com.zoneが作成されます。

第22章
認証の設定

ユーザーがRed Hat Linuxにログインするとき、ユーザー名とパスワードの組み合わせが有効でアクティブなユーザーであることが確認、または認証されなければなりません。ときには、ユーザーを確認する情報がローカルシステム上にあったり、リモートシステム上にあるユーザーのデータベースに対する認証に時間がかかることもあります。

認証設定ツールは、ユーザーの情報を取り出すためのNIS、LDAP、Hesiodの設定用グラフィカルインターフェース、同様に認証プロトコルとしてのLDAP、Kerberos、SMBの設定用グラフィカルインターフェースを備えています。

注意

中または高のセキュリティレベル設定を、インストール中に、あるいは**セキュリティレベル設定ツール** を使用して、行なった場合(または、**GNOME Lokkit** プログラムを使用して高または低のセキュリティを選択した場合)、NIS及びLDAPなどのネットワーク認証方法はファイアウォールを通り抜けることが許可されません。

この章はそれぞれの異なった認証タイプの詳細については説明していません。代わりに、**認証設定ツール**を使用して認証を設定する方法を説明しています。

デスクトップから**認証設定ツール**のグラフィカルバージョンをスタートするには、**メインメニュー** (パネル上) => **システム設定** => **認証**の順で進むか、シェルプロンプト(例、**XTerm**または**GNOME terminal**内)で `authconfig-gtk`とコマンドを入力します。テキストベースのバージョンをスタートするには、シェルプロンプトで`authconfig` とコマンドを入力します。

重要

認証プログラムを終了すると直ちにその変更は有効となります。

22.1. ユーザー情報

ユーザー情報タブにはいくつかオプションがあります。オプションを有効にするには、横にある空のチェックボックスをクリックします。オプションを解除するには、横にあるチェックボックスをクリックしてチェックを消します。**OK**をクリックしてプログラムを終了し、変更を適用します。

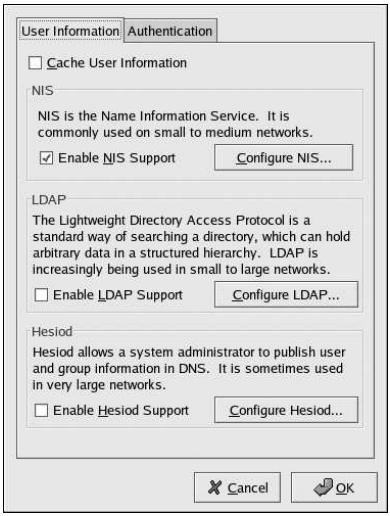


図22-1. ユーザー情報

以下の一覧は各オプションの説明です。

- **キャッシュユーザー情報** — このオプションを選択すると、ネームサービスのキャッシュデーモン(nscd)が有効になりブート時にスタートする設定になります。

  このオプションを作動させるには、`nscd` パッケージをインストールする必要があります。

- **NISサポートを有効にする** — このオプションを選ぶと、システムをNISクライアントとして設定します。NISクライアントはユーザーとパスワードの認証にNISサーバーへ接続します。**NISの設定**ボタンをクリックして、NISドメインとNISサーバーを指定します。NISサーバーが指定されないと、デーモンがブロードキャストを介して検出を試みます。

  このオプションを作動させるには`ypbind` パッケージをインストールする必要があります。NISサポートが有効になると、`portmap` サービスと`ypbind`サービスがスタートします。また、ブート時にも有効になりスタートします。

- **LDAPサポートを有効にする** — このオプションを選択すると、システムがLDAPを介してユーザー情報を取り出すよう設定します。**LDAPの設定**ボタンをクリックして**LDAP検索基本DN**と**LDAPサーバー**を指定します。**接続を暗号化するためにTLSを使用**を選択すると、LDAPサーバーに送信されるパスワードを暗号化するためにTransport Layer Security が使用されます。

  このオプションを作動させるには`openldap-clients`パッケージをインストールする必要があります。

  LDAPについての詳細は、*Red Hat Linux* 参照ガイド を参照してください。

- **Hesiodサポートを有効にする** — このオプションを選択すると、システムがユーザー情報などのリモートHesiodデータベースから情報を取り出すよう設定します。

  `hesiod`パッケージをインストールする必要があります。

22.2. 認証

認証タブでネットワーク認証方法の設定ができます。オプションを有効にするには、横にある空のチェックボックスをクリックします。オプションを解除するには、横にあるチェックボックスをクリックしてチェックを消します。

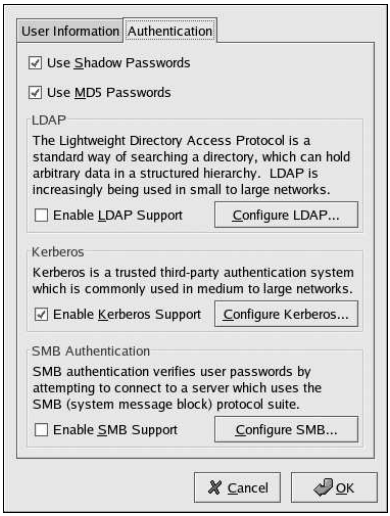


図22-2. 認証

以下は各オプション設定の説明です。

- **シャドウパスワードを使用** — このオプションを選択すると、パスワードをシャドウパスワード形式で`/etc/passwd`ファイルではなく`/etc/shadow`ファイルに格納します。シャドウパスワードはインストール中にデフォルトで有効になります。システムのセキュリティを増強するためにシャドウパスワードの使用を強くおすすめします。

  このオプションを作動させるには`shadow-utils` パッケージをインストールする必要があります。シャドウパスワードについての詳細は、*Red Hat Linux* 参照ガイドのユーザーとグループ の章を参照してください。

- **MD5パスワードを使用** — このオプションを選択するとMD5パスワードが有効になります。パスワードの制限が8文字以下から256文字まで広くなります。インストール中にデフォルトで選択されます。セキュリティを増強するためにMD5パスワードの使用を強くおすすめします。

- **LDAPサポートを有効にする** — このオプションを選択すると、認証にLDAPを使用する標準のPAM使用可能なアプリケーションを持たせます。**LDAPの設定**ボタンをクリックして以下を指定します。

  - **接続を暗号化するためにTLSを使用** — LDAPサーバーに送信されるパスワードを暗号化するためにTransport Layer Securityを使用します。
  - **LDAP検索基本DN** — 識別名(Distinguished Name-DN)でユーザー情報を取り出します。
  - **LDAPサーバー** — LDAPサーバーのIPアドレスを指定します。

  このオプションを作動させるには`openldap-clients`パッケージをインストールする必要があります。LDAPについての詳細は、*Red Hat Linux* 参照ガイドを参照してください。

- **Kerberosサポートを有効にする** — このオプションを選択するとKerberos認証が有効になります。**Kerberosの設定**ボタンをクリックして設定します。

  - **Realm** — Kerberosサーバー用のrealmを設定します。realmはKerberosを使用するネットワークで、ひとつ以上のKDCと場合によっては多数のクライアントから構成されます。
  - **KDC** — Kerberosチケットを発行するサーバーのKey Distribution Center (KDC)を定義します。
  - **管理サーバー** — `kadmind`を実行する管理サーバーを指定します。

このオプションを作動させるには`krb5-libs`と`krb5-workstation`パッケージをインストールする必要があります。Kerberosについての詳細は、*Red Hat Linux* 参照ガイドを参照してください。

- **SMBサポートを有効にする** — このオプションでは、PAMがSMBサーバーを使用してユーザーを認証するように設定します。**SMBの設定**ボタンをクリックして指定します。
  - **ワークグループ** — 使用するSMBワークグループを指定します。
  - **ドメインコントローラ** — 使用するSMBドメインコントローラを指定します。

22.3. コマンドラインバージョン

認証設定ツールはインターフェースなしのコマンドラインツールとしても実行できます。コマンドラインバージョンは設定スクリプトまたはキックスタートスクリプトで使用できます。表22-1は認証オプションの要約です。

オプション	詳細
`--enableshadow`	シャドウパスワードを有効にする
`--disableshadow`	シャドウパスワードを解除する
`--enablemd5`	MD5パスワードを有効にする
`--disablemd5`	MD5パスワードを解除する
`--enablenis`	NISを有効にする
`--disablenis`	NISを解除する
`--nisdomain=<domain>`	NISドメインを指定する
`--nisserver=<server>`	NISサーバーを指定する
`--enableldap`	ユーザー情報にLDAPを有効にする
`--disableldap`	ユーザー情報にLDAPを解除する
`--enableldaptls`	LDAPでTLSの使用を有効にする
`--disableldaptls`	LDAPでTLSの使用を解除する
`--enableldapauth`	認証にLDAPを有効にする
`--disableldapauth`	認証にLDAPを解除する
`--ldapserver=<server>`	LDAPサーバーを指定する
`--ldapbasedn=<dn>`	LDAP基本DNを指定する
`--enablekrb5`	Kerberosを有効にする
`--disablekrb5`	Kerberosを解除する
`--krb5kdc=<kdc>`	KerberosのKDCを指定する
`--krb5adminserver=<server>`	Kerberosの管理サーバーを指定する
`--krb5realm=<realm>`	Kerberosのrealmを指定する
`--enablesmbauth`	SMBを有効にする
`--disablesmbauth`	SMBを解除する

オプション	詳細
`--smbworkgroup=<workgroup>`	SMBのワークグループを指定する
`--smbservers=<server>`	SMBのサーバーを指定する
`--enablehesiod`	Hesiodを有効にする
`--disablehesiod`	Hesiodを解除する
`--hesiodlhs=<lhs>`	Hesiod LHSを指定する
`--hesiodrhs=<rhs>`	Hesiod RHSを指定する
`--enablecache`	`nscd`を有効にする
`--disablecache`	`nscd`を解除する
`--nostart`	たとえ設定されても、`portmap`、`ypbind`、`nscd` サービスをスタートしない、または停止しない
`--kickstart`	ユーザーインターフェースを表示しない
`--probe`	ネットワークデフォルトを調査して表示する

表22-1. コマンドラインのオプション

ヒント

これらのオプションは`authconfig`のmanページにもあります。また、シェルプロンプトで `authconfig --help`とタイプして見つけることもできます。

第23章

MTA（Mail Transport Agent）の設定

メール転送エージェント (MTA) は、Red Hat Linuxシステムから電子メールを送信するのに欠かせません。**Evolution**、**Mozilla Mail**、**Mutt**、などのMUA（メールユーザーエージェント）は、電子メールを読んだり書いたりするのに使用します。ユーザーがMUAから電子メールを送信する場合、メッセージはMTAに渡され、さらに一連のMTAに渡されてから送信先に届けられます。

ユーザーがシステムから電子メールを送信するつもりがない場合でも、自動化されたタスクやシステムプログラムで`/bin/mail`コマンドが使用されて、ログメッセージが記録された電子メールがローカルシステムのrootユーザーに送られることがあります。

Red Hat Linux 9には、SendmailとPostfixという2つのMTAがあります。両方のMTAがインストールされている場合、`sendmail`がデフォルトのMTAになります。**メール転送エージェント切替**を使用すると、システムのデフォルトのMTAとして`sendmail`と`postfix`のどちらかを選択することができます。

テキストベースで**メール転送エージェント切替**を使用したい場合は、`redhat-switch-mail` RPMパッケージがインストールしてある必要があります。グラフィックバージョンを使用する場合は、`redhat-switch-mail-gnome` パッケージがインストールされている必要があります。RPMパッケージのインストールについての詳細は、パートVを参照してください。

メール転送エージェント切替をスタートするには、パネル上の**メインニュー**ボタンを選択して**システムツール** => **その他のシステムツール** => **メール転送エージェント切替**と進みます。あるいは、シェルプロンプト(例えば、XTerm又はGNOMEターミナル)で`redhat-switch-mail`と入力します。

X Window Systemが実行されている場合は、プログラムが自動的に検出します。実行されている場合、図23-1に示すように、プログラムはグラフィカルモードで起動します。Xが検出されない場合、プログラムはテキストモードで起動します。**メール転送エージェント切替**を強制的にテキストモードで起動するには、`redhat-switchmail-nox` コマンドを使用します。

図23-1. メール転送エージェント切替

MTAの変更に**OK**を選択すると、その選択されたメールデーモンのブート時起動が有効になります。そして選択されていないメールデーモンは無効となり、ブート時に開始されません。選択したメールデーモンがスタートして、他のメールデーモンが止まることになります。このように変更はすぐに反映されます。

電子メールのプロトコルとMTAに関する詳細は、*Red Hat Linux* 参照ガイドを参照して下さい。MUAに関する情報は*Red Hat Linux* 入門ガイドを参照して下さい。

IV. システムの設定

このパートでは、コンソールへのアクセス及びRed Hat Linuxシステムからのハードウェアとソフトウェア情報の収集の仕方の説明、その後に、一般システムの設定についての作業を説明します。

目次

第24章

コンソールのアクセス

root以外の一般ユーザーがコンピュータにローカルからログインすると、2種類の特殊な権限が与えられます。

1. ユーザーは、他では実行できないような特定のプログラムを実行できます。
2. ユーザーは、他ではアクセスできないような特定のファイル（通常はディスケット、CD-ROMなどへのアクセスに使用される特別なデバイスファイル）にアクセスできます。

1つのコンピュータ上に複数のコンソールがある状態では、複数のユーザーが同時にローカルからコンピュータにログインできるため、ユーザーのうちの1人がファイルにアクセスする競争に「勝つ」必要があります。最初にコンソールにログインするユーザーがファイルの所有権を取得します。最初のユーザーがログアウトすると、ファイルはログインしている次のユーザーの権利となります。

逆に、コンソールからログインしているすべてのユーザーは、通常rootユーザーに制限されているタスクを行うプログラムを実行できます。Xが動作している場合、これらのアクションはグラフィカルユーザーインターフェイスのメニュー項目として取り込むことができます。コンソールからアクセスできるプログラムには、`halt`、`poweroff`、`reboot`などがあります。

24.1. Ctrl-Alt-Delキーを使ったシャットダウンの無効化

デフォルトでは、`/etc/inittab`によって、コンソールで[Ctrl]-[Alt]-[Del]キーの組み合わせを使用した場合にシステムのシャットダウンとリブートを行うよう指定されています。この機能を完全に無効にするには、`/etc/inittab`の次の行の先頭にシャープ記号（#）を付けてコメントアウトします：

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

あるいは、[Ctrl]-[Alt]-[Del]キーを使用してコンソールからシステムをシャットダウンする権利だけをrootでないユーザーに許可したい場合もあります。次の手順で、この権限を特定のユーザーに制限できます。

1. 上に示した`/etc/inittab`行に`-a`オプションを追加すると、次のように表示されます。
   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```
   `-a`フラグは、次の手順で作成する`/etc/shutdown.allow`ファイルを探すように`shutdown`に指示します。
2. `/etc`に`shutdown.allow`というファイルを作ります。`shutdown.allow`ファイルは、[Ctrl]-[Alt]-[Del]キーを使ってシステムをシャットダウンすることが許されているユーザーの一覧です。`/etc/shutdown.allow`ファイルのフォーマットは、次のようなユーザー名（1行に1名ずつ)のリストです：
   ```
   stephen
   jack
   sophie
   ```

この`shutdown.allow`ファイルの例では、stephen、jack、sophieは[Ctrl]-[Alt]-[Del]キーを使ってコンソールからシステムをシャットダウンすることが許可されています。このキーコンビネーションを使用すると、`/etc/shutdown.allow`内のユーザー（またはroot）が仮想コンソールにログインされているかどうかが`/etc/inittab`の`shutdown -a`で確認されます。ユーザーの誰かがログインしている場合は、システムのシャットダウンが続きます。ログインされていなければ、その代わりにシステムコンソールにエラーメッセージが書き込まれます。

`shutdown.allow`の詳細については、`shutdown`のmanページを参照してください。

24.2. コンソールプログラムアクセスの無効化

コンソールプログラムへのユーザーのアクセスを無効にするには、以下のコマンドをrootとして実行してください。

```
rm -f /etc/security/console.apps/*
```

コンソールの安全性がそれ以外の方法で保証されている環境（BIOSとブートローダーの各パスワードが設定されている環境、[Ctrl]-[Alt]-[Delete]キーが無効化されている環境、電源スイッチやリセットスイッチが無効化されている環境など）では、デフォルトでコンソールからアクセスできるpoweroff、halt、rebootを、コンソールにいるユーザーからは実行できないようにしたい場合があります。

これらの機能を解除するには、rootとして次のコマンドを実行します。

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

24.3. すべてのコンソールアクセスの無効化

PAMのpam_console.soモジュールは、コンソールファイルの権限と認証を管理します（PAMの設定の詳細については、「*Red Hat Linux* 参照ガイド」を参照してください）。プログラムアクセスやファイルアクセスなどのすべてのコンソールアクセスを無効化したい場合は、/etc/pam.dディレクトリ内のpam_console.soを参照するすべての行をコメントアウトします。これは、rootで次のスクリプトを実行します：

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

24.4. コンソールの定義

pam_console.soモジュールは、/etc/security/console.permsファイルを使ってシステムコンソールにいるユーザーの権限を決定します。このファイルの構文は非常に柔軟性があります。つまり、これらの指示が適用されないようにファイルを編集できます。ただし、デフォルトファイルには次のような行があります：

```
<console>=tty[0-9][0-9]*:[0-9]\.[0-9]:[0-9]
```

ユーザーがログインすると、特定の名前の付いたターミナル（:0やmymachine.example.com:1.0のような名前のXサーバー、または/dev/ttyS0や/dev/pts/2のようなデバイス）に接続されます。デフォルトでは、ローカルの仮想コンソールやローカルのXサーバーがローカルとみなされるように定義されますが、隣の/dev/ttyS1ポート上のシリアルターミナルをローカルとみなしたい場合は、次のようにその行を変更できます。

```
<console>=tty[0-9][0-9]*:[0-9]\.[0-9]:[0-9] /dev/ttyS1
```

24.5. コンソールからファイルにアクセスできるようにする方法

/etc/security/console.permsには、次のような行を持つセクションがあります：

```
<floppy>=/dev/fd[0-1]*\
/dev/floppy/*/mnt/floppy*
<sound>=/dev/dsp*/dev/audio*/dev/midi*\
/dev/mixer*/dev/sequencer\
/dev/sound/*/dev/beep
<cdrom>=/dev/cdrom*/dev/cdroms/*/dev/cdwriter*/mnt/cdrom*
```

必要であれば、このセクションに独自の行を追加できます。追加する行が対応するデバイスを参照するかどうかを確認してください。たとえば、次の行を追加できます。

```
<scanner>=/dev/scanner /dev/usb/scanner*
```

もちろん、/dev/scannerが、ハードディスクドライブなどでなく、実際にスキャナーであることを確認する必要があります。

これが最初のステップです。2番目は、これらのファイルで何をするかを定義します。/etc/security/console.perms内の最後のセクションで以下のような行を見付けて下さい：

```
<console> 0660<floppy> 0660root.floppy
<console> 0600<sound> 0640root
<console> 0600<cdrom> 0600root.disk
```

ここに、次のような行を追加します：

```
<console> 0600 <scanner> 0600 root
```

次に、コンソールからログインすると、/dev/scannerデバイスの所有権が与えられます。デバイスの権限は0600（自分だけが読み取り可能かつ書き込み可能）です。ログアウトすると、デバイスはrootのものになり、引き続き0600（今度はrootのみが読み取り可能かつ書き込み可能）の権限があります。

24.6. ほかのアプリケーションに対するコンソールアクセスの有効化

コンソールユーザーがほかのアプリケーションにアクセスできるようにしたい場合は、少し余計に作業をするだけで可能です。

まず、コンソールアクセスは/sbinと/usr/sbinのいずれかに存在するアプリケーションに対してのみ有効なので、実行したいアプリケーションがそこになければいけません。それを確認した後、次のステップを実行します：

1. アプリケーションの名前から/usr/bin/consolehelperアプリケーションへのリンクを作成します（ここの例としては*foo*プログラム）：
   ```
   cd /usr/bin
   ln -s consolehelper foo
   ```
2. /etc/security/console.apps/*foo*ファイルを作成します：
   ```
   touch /etc/security/console.apps/foo
   ```
3. /etc/pam.d/内に*foo*サービスのためのPAM設定ファイルを作成します。これを行う簡単な方法として、まずhaltサービスのPAM設定ファイルをコピーし、その後、その動作を変更したい場合はファイルを変更します。
   ```
   cp /etc/pam.d/halt /etc/pam.d/foo
   ```

これで、/usr/bin/*foo*を実行すると、consolehelperが呼び出されます。このコマンドは、/usr/sbin/userhelperを利用してユーザーを認証します。ユーザーを認証するため

に、/etc/pam.d/*foo*が/etc/pam.d/haltのコピーであれば、consolehelperはユーザーのパスワードを要求し（それ以外は/etc/pam.d/*foo*で指定されている内容を正確に実行します)、次にroot権限で/usr/sbin/*foo*を実行します。

PAM設定ファイルの中で、アプリケーションは成功した認証要請を記憶(キャッシュに入れる)する為に*pam_timestamp*モジュールを使用する設定が出来ます。アプリケーションがスタートして正式な認証(ルートのパスワード)が用意された時に、時間スタンプが生成されます。ディフォルトでは、成功した認証はキャッシュに5分間だけ記憶されます。この5分間はpam_timestampを使用して、同じセッションから実行するように設定されている他のアプリケーションはどれもそのユーザーの為に自動的に認証されます。—ユーザーは再度ルートパスワードを入力する必要がありません。

このモジュールはpamパッケージの中に含まれています。この機能を有効にするにはetc/pam.d/の中のPAM設定ファイルが以下の行を含む必要があります。

```
auth sufficient /lib/security/pam_timestamp.so
session optional /lib/security/pam_timestamp.so
```

authで始まる最初の行は、他のauth sufficientの行の後に来るようにし、sessionで始まる行は、他のsession optional行の後に来るようにしなければなりません。

pam_timestampを使用するように設定されているアプリケーションが**メインメニューボタン** (パネル上)から認証されると、GNOMEデスクトップ環境を使用している場合、パネル部分の通知区域にアイコン  が表示されます。認証が時間切れになると(ディフォルトでは5分間)、アイコンは無くなります。

ユーザーは、アイコンをクリックして、認証を無視するオプションを選択することによりキャッシュにある認証を無視できます。

24.7. floppyグループ

どのような理由であれ、コンソールアクセスが組織に適していないために、システムのフロッピーディスクドライブへのアクセス権をrootでないユーザーに与えなければならない場合は、floppyグループで行うことができます。選択したツールを使用してユーザーをfloppyグループに追加するだけで済みます。ここに、gpasswdを使用してユーザーfredをfloppyグループに追加する方法の例を示します：

```
[root@bigdog root]# gpasswd -a fred floppy
Adding user fred to group floppy
[root@bigdog root]#
```

これで、ユーザーfredはコンソールからシステムのフロッピーディスクドライブにアクセスできるようになります。

第25章

ユーザーとグループの設定

ユーザーマネージャを使用するとローカルのユーザーとグループを、表示、変更、追加、削除などすることが出来ます。

ユーザーマネージャを使用するには、`redhat-config-users` RPM パッケージがインストールされていて、X Window Systemを起動している状態で、rootの権限を使う必要があります。**ユーザーマネージャ**をデスクトップからスタートする場合は、(パネル上の) **メインメニューボタン** => **システム設定** => **ユーザーとグループ**と選択します。あるいは、シェルプロンプト(例えば、XTermやGNOMEターミナル)で`redhat-config-users`コマンドをタイプします。

図25-1. ユーザーマネージャ

システムのすべてのローカルユーザーの一覧を表示するには、**ユーザー**タブをクリックします。システムのすべてのローカルグループの一覧を表示するには、**グループ**タブをクリックします。

特定のユーザーやグループを検索する必要がある場合は、**検索フィルタ**フィールドに、名前の最初の数文字を入力します。[Enter]キーを押すか、**フィルタの適用**ボタンをクリックします。フィルタ処理後の一覧が表示されます。

ユーザーまたはグループを並べ替えるには、列名をクリックします。ユーザーまたはグループは、その列の値によって並べ替えられます。

Red Hat Linuxは、500までのユーザーIDをシステムユーザー用に予約しています。デフォルトでは、**ユーザーマネージャ**はシステムユーザーを表示しません。システムユーザーを含め、すべてのユーザーを表示するには、プルダウンメニューから**設定 - システムユーザーとグループをフィルタ**の順に進みチェックをはずします。

ユーザーとグループの詳細情報については、*Red Hat Linux* 参照ガイドと*Red Hat Linux* システムアドミニストレーションプレミアを御覧下さい。

25.1. 新しいユーザーの追加

新しいユーザーを追加するには、**ユーザの追加**ボタンをクリックします。図25-2に示すようなウィンドウが開くので、該当のフィールドに追加するユーザーのユーザー名とフルネームを入力します。**パスワード**と**パスワードの確認**フィールドに、ユーザーのパスワードを入力します。パスワードは6文字以上でなければなりません。

ヒント

ユーザーのパスワードは、長ければ長いほど、他人がそれを推定し、許可なしにユーザーのアカウントにログインすることが困難になります。1つの単語だけのパスワードは避け、文字、数字、特殊な文字を組み合わることをお勧めします。

ログインシェルを選択します。どのシェルを選んでよいのかわからない場合は、`/bin/bash`のデフォルト値を使用します。デフォルトのホームディレクトリは`/home/`ユーザー名です。ユーザーのために作られたホームディレクトリは変更でき、又、**ホームディレクトリの作成**の選択を解除して、ホームディレクトリを作成しないようにもできます。

ホームディレクトリを作成するように選択すると、デフォルトの設定ファイルが`/etc/skel`ディレクトリから新しいホームディレクトリへコピーされます。

Red Hat Linuxは*UPG*（User Private Group）スキームを使用します。UPGスキームは、UNIXの標準グループ取り扱い方法の追加や変更はしません。新しい取り決めを提供するだけです。新しいユーザーを作成すると、デフォルトでユーザーと同じ名前の独自のグループが作成されます。このグループの作成を望まない場合は、**ユーザー用にプライベートグループを作成**の選択を解除します。

ユーザーのユーザーIDを指定するには、**ユーザーIDを手動で指定**を選択します。このオプションが選択されていない場合、500の数字で始まる次に使用可能なユーザーIDが新しいユーザーに割り当てられます。500より下のユーザーIDは、Red Hat Linuxによりシステムユーザー用に予約されています。

OKボタンをクリックしてユーザーを作成します。

図25-2. 新規ユーザ

パスワードの失効のような、高度なユーザー特性を設定するには、ユーザーを追加した後にユーザーの特性を変更します。詳細については項25.2を参照してください。

他のユーザーグループにユーザーを追加するには、**ユーザー**タブをクリックし、ユーザーを選択し、**プロパティ**ボタンをクリックします。**ユーザープロパティ**ウィンドウで、**グループ**タブを選択します。ユーザーがそのメンバーとなるグループを選択します。ユーザー用のプライマリグループを選択し、**OK**をクリックします。

25.2. ユーザー特性の変更

既存のユーザーの特性を表示するには、**ユーザー**タブをクリックし、ユーザー一覧からユーザーを選択し、ボタンメニューから**プロパティ**ボタンをクリックします（または、プルダウンメニューから**ファイル-プロパティ**を選択します）。図25-3のようなウィンドウが表示されます。

図25-3. ユーザープロパティ

ユーザープロパティウィンドウは、複数タブの付いたページに分割されます。

- **ユーザーデータ**—ユーザーを追加したときに設定される基本的なユーザー情報を表示します。このタブを使用して、ユーザーのフルネーム、パスワード、ホームディレクトリ、ログインシェルなどを変更します。
- **アカウント情報**—アカウントが一定の日付に満了することを望む場合は、**アカウント失効を有効にする**を選択します。アカウント失効日時フィールドに日付を入力します。ユーザーがシステムにログインできなくなるように、ユーザーアカウントをロックするには、**ユーザアカウントがロックされています**を選択します。
- **パスワード情報**—このタブは、パスワードが最後に変更された日付を示します。一定の日数が経過した後にユーザーにパスワードを強制的に変更させるには、**パスワード失効を有効にする**を選択します。ユーザーがパスワードを変更できるようになるまでの日数、ユーザーがパスワードを変更するように警告されるまでの日数、アカウントが無効になるまでの日数も設定できます。
- **グループ**—ユーザーを追加したいグループとユーザーのプライマリグループを選択します。

25.3. 新しいグループの追加

新しいユーザーグループを追加するには、**グループを追加**ボタンをクリックします。図25-4のようなウィンドウが表示されます。作成する新しいグループの名前を入力します。新しいグループのグループIDを指定するには、**グループIDを手動で指定**を選択し、GIDを選択します。Red Hat Linuxは500未満のグループIDをシステムグループ用に予約しています。

OKボタンをクリックしてグループを作成します。新しいグループがグループ一覧に表示されます。

図25-4. 新規グループ

ユーザーをグループに追加するときは、項25.4を参照してください。

25.4. グループ特性の変更

既存グループの特性を表示するには、グループ一覧からグループを選択し、ボタンメニューから**プロパティ**ボタンをクリックします（または、プルダウンメニューから**ファイル-プロパティ**を選択します）。図25-5のようなウィンドウが表示されます。

図25-5. グループ特性

グループタブは、どのユーザーがグループのメンバーであるかを表示します。グループに追加するには、追加されるユーザーを選択し、又は、グループから削除するには、削除されるユーザーの選択を解除します。**OK**ボタンか**適用**ボタンをクリックして、グループのユーザーを変更します。

25.5. コマンドラインの設定

コマンドラインツールを好む場合や、又はX Window Systemがインストールされていない場合、この章の内容を使用してユーザーとグループの設定をして下さい。

25.5.1. ユーザーの追加

システムにユーザーを追加するには、以下のようにします：

1. `useradd`コマンドを発行してロックされたユーザーアカウントを作成します:
   `useradd <username>`
2. `passwd`コマンドでパスワードを入れ、パスワードの経年変化ガイドラインを設定して、アカウントをアンロックします：
   `passwd <username>`

`useradd`用のコマンドラインオプションは表25-1に示してあります。

オプション	説明
`-c` コメント	ユーザー用のコメント
`-d` ホームディレクトリ	デフォルトの`/home/`ユーザー名の代わりに使うホームディレクトリ
`-e` 日付	アカウントが無効になる日付をYYYY-MM-DD形式で設定

オプション	説明
-f 日数	パスワードが失効になってからアカウントが無効になるまでの日数。(**0**が指定されると、パスワードが失効になるとすぐにアカウントが無効になります。**-1**が指定されると、パスワード失効の後でもアカウントは無効になりません)。
-gグループ名	ユーザーのデフォルトグループ用のグループ名、又はグループ番号。(グループは指定できる前に存在する必要があります)。
-G グループリスト	ユーザーがメンバーである追加の(デフォルト以外の)グループ名、又はグループ番号が、コンマで区切られている一覧。(グループは指定できる前に存在する必要があります)。
-m	ホームディレクトリがない場合は、それを作成する。
-M	ホームディレクトリを作成しない。
-n	ユーザー用にユーザーのプライベートグループを作成しない。
-r	500以下のUIDで、ホームディレクトリのないシステムアカウントを作成する。
-p パスワード	cryptコマンドで暗号化されたパスワード。
-s	/bin/bashがデフォルトのユーザーログインシェル。
-u *uid*	ユーザー用のユーザーID、ユニークで499以上であることが必要。

表25-1. useraddのコマンドラインオプション

25.5.2. グループの追加

システムにグループを追加するには、groupaddコマンドを使用します：

groupadd <*group-name*>

groupadd用のコマンドラインオプションは表25-2に示してあります

オプション	説明
-g グループ*ID*	グループ用のグループID、ユニークで499以上であることが必要。
-r	500以下のGIDでシステムグループを作成する。
-f	グループが既に存在する場合は、エラーで終了。(グループは変更されません)。-g と -fが指定されて、グループが既にある場合には、-gオプションは無視されます。

表25-2. groupaddコマンドラインオプション

25.5.3. パスワードの経年変化

セキュリティの目的でユーザーが定期的にパスワードを変更するように要求することは良い対策です。これは**ユーザーマネージャ**の**パスワード情報**タブ上でユーザーの追加、又は編集することで達成されます。

シェルプロンプトからユーザーのパスワード失効日を設定するには、chage コマンドを使用し、続けて表25-3にあるオプションの1つとそのユーザーのユーザー名を入力します。

重要

chageコマンドを使用するには、シャドウパスワードが有効になっている必要があります。

オプション	説明
-m 日数	ユーザーがパスワードを変更する必要が出る最低期間を日数で指定。値が0の場合はパスワードは失効になりません。
-M 日数	パスワードが有効である最大期間を日数で指定。このオプションで指定した日数と-dオプションで指定したオプションの合計が現在の日より小さい場合、ユーザーはアカウントを使用する前に自己のパスワードを変更する必要があります。
-d 日数	パスワードが変更される時期を1970年1月1日からの日数で指定
-I 日数	パスワード失効からアカウントロックまでの無活動の期間を日数で指定。値が0の場合は、パスワード失効の後でもアカウントはロックされません。
-E 日付	YYYY-MM-DD形式で、アカウントがロックされる日付を指定。日付の代わりに1970年1月1日からの日数でも使用可能。
-W 日数	パスワードの失効日前にユーザーに警告する日数を指定。

表25-3. change コマンドラインオプション

ヒント

chageコマンドのすぐ後に、ユーザー名(オプションなし)があれば、現在のパスワード経年変化の値を表示し、変更を可能にします。

システム管理者はユーザーが最初のログインでパスワードを設定するようにしたい場合は、ユーザーのパスワードをすぐに失効させて、ユーザーに最初のログイン直後にパスワードを変更させるように設定できます。

最初のログイン後に、ユーザーにコンソールでパスワードを設定させる場合は、以下のステップに従って下さい。SSHプロトコルでユーザーがログインをしている場合は、このプロセスは実行できないことに注意して下さい。

1. ユーザーパスワードをロックする — ユーザーが存在しない場合、useraddコマンドを使用して、ユーザーアカウントを作成します。しかし、パスワードは与えないでロックされたままにしておきます。

   パスワードがすでに有効になっている場合は、次のコマンドでそれをロックします：
   ```
   usermod -L username
   ```

2. すぐにパスワード失効を強制する — 次のコマンドを入力します：
   ```
   chage -d 0 username
   ```

   このコマンドは最後にパスワードが変更された期日の値をエポック(1970年1月1日)にセットします。パスワードの経年変化ポリシーに関係なく、この値が即時にパスワードの失効を強制します。

3. アカウントをアンロック —2つのアプローチがこのステップにあります。管理者は、初期パスワードを割り当てるか、又は無効なパスワードを割り当てます。


警告

passwdコマンドは、設定したばかりのパスワード失効を無効にしますので、passwdコマンドを使用したパスワードの設定はしないで下さい。

初期パスワードを割り当てるには、以下のステップに従います：

- pythonコマンドでコマンドラインpython インタプリタを開始します。以下が表示されます：
```
Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
[GCC 3.2.1 20021207 (Red Hat Linux 8.0 3.2.1-2)] on linux2
Type "help", "copyright", "credits" or "license" for moreinformation.
>>>
```
- プロンプトで、以下を入力します(*password*には、暗号化するパスワードで入れ換え、そして*salt*にはabや12の様にちょうど2つの大文字、又は小文字の英文字、数字、ドット(.)記号、スラッシュ(/) 記号等の組合せで入れ換えます)：
```
import crypt; print crypt.crypt("password","salt")
```
その出力は、12CsGd8FRcMSMのような暗号化されたパスワードになります。
- [Ctrl]-[D]を押して、Pythonインタプリタを終了します。
- 前後に空白のない状態で、カットアンドペーストで暗号化したパスワード出力をそのまま次ぎのコマンドに張り付けます：
```
usermod -p "暗号化したパスワード" ユーザー名
```

初期パスワードを割り当てる代わりに、以下のコマンドで無効なパスワードを割り当てることもできます：
```
usermod -p "" ユーザー名
```


用心

無効なパスワードを使用するのは、ユーザーにとっても管理者にとっても便利なことですが、第三者が最初にログインしてシステムにアクセスすると言うリスクが少々あります。このような脅威を最小限に保つには、管理者はアカウントがアンロックされる時点でユーザーがログインの準備が出来ているかを確認することが推奨されます。

どちらの場合も、初期ログインでユーザーは新しいパスワードを要求されます。

25.6. プロセスの説明

次のステップは、シャドウパスワードが有効になっているシステムでuseradd juanコマンドが発行された場合に、起こる結果を説明しています：

1. /etc/passwdの中にjuan用の新しい行が作成されます。この行は、以下のような特徴を持っています：
   - ユーザー名juanで始まる。
   - パスワードフィールドに、システムがシャドウパスワードを使用していることを示す1つのxがある。
   - 500、又はそれ以上のUIDが作成される。(Red Hat Linuxでは、500以下のUIDとGIDはシステムの使用に予約済みです)。
   - 500、又はそれ以上のGIDが作成される。
   - オプションのGECOS情報は空白のまま残る。

- juanのホームディレクトリは/home/juan/にセットされる。
- デフォルトのシェルは、/bin/bashにセットされる。

2. /etc/shadowの中にjuanの新しい行が作成されて、以下の様な特徴を持ちます：
   - ユーザー名juanで始まる。
   - 2つの感嘆符(!!)が/etc/shadowファイルのパスワードフィールドに表示され、アカウントをロックする。

     注意

     暗号化されたパスワードが-pフラグを付けて渡されると/etc/shadowファイルのユーザー用の新しい行に置かれます。

   - パスワードは失効しないようにセットされる。

3. /etc/groupの中にjuanと言うグループ用の新しい行が出来る。ユーザーと同じ名前のグループはユーザープライベートグループと呼ばれます。ユーザープライベートグループに関する詳細は、項25.1を参照して下さい。

   /etc/group内に作成された行は、以下の特徴を持ちます：
   - グループ名juanで始まる。
   - パスワードフィールドの中に、システムがシャドウパスワードを使用していることを示す1つのxが表示される。
   - GIDは、/etc/passwdの中のユーザーjuan用のリストにあるものと同じ。

4. /etc/gshadowの中にjuanと言うグループ用の行が作成され、次のような特徴を持ちます：
   - グループ名juanで始まる。
   - 1つの感嘆符(!)が、/etc/gshadowファイルのパスワードフィールドに表示され、これがグループをロックする。
   - 他のフィールドは全て空白となる。

5. ユーザーjuan用のディレクトリは、/home/ ディレクトリの中に作成されます。このディレクトリは、ユーザーjuanとグループjuanに所有されます。しかし、ユーザーのjuanのみが書き込み、読み込み、及び実行の特権を持ちます。他の全ての権限は拒否されます。
6. /etc/skel/ディレクトリ内のファイル(デフォルトのユーザー設定を持つ)は、新しい/home/juan/ディレクトリにコピーされます。

この時点で、juanと言うロックされたアカウントがシステム上に存在します。それを活性化するには、管理者はpasswd コマンドを使用してアカウントへのパスワードを割り当てる必要があり、さらにはオプションとして、パスワードの経年変化ガイドラインも設定します。

第26章

システム情報の収集

システム設定の方法を考える前に、まず基本的なシステム情報を収集する方法を考えなければいけません。たとえば、未使用のメモリがどれだけ残っているか、ハードディスクドライブの使用可能なスペースの大きさはどの程度か、ハードディスクドライブのパーティションがどうなっているか、どんなプロセスが作動しているかといったことを知っておく必要があります。この章では、いくつかの簡単なコマンドやプログラムを使ってRed Hat Linuxシステムからこのような情報を収集する方法を説明します。

26.1. システムプロセス

ps axコマンドは、現在動いているシステムプロセスを、ほかのユーザーが所有するものも含めて一覧にして表示します。プロセスの所有者も表示したいときは、 ps auxコマンドを使います。この一覧は静的です。つまり、このコマンドを実行したときに作動しているものの状態を表しているだけです。実行プロセスの一覧を継続的に更新したい場合は、のちほど説明するtopコマンドを使います。

ps出力は長くなる可能性があります。画面外へスクロールするのを防ぐために、パイプを使用してlessで表示することができます。

```
ps aux | less
```

psコマンドとgrep コマンドを組み合わせて使用すると、あるプロセスが動いているかどうかを調べることができます。例えば、**emacs** が実行されているかを調べるには、次のコマンドを使用します。

```
ps ax | grep emacs
```

topコマンドは、現在動作中のプロセスを表示します。これには、メモリやCPU使用率などの重要な情報も含まれています。一覧はリアルタイムでインタラクティブです。次に示すのは、topの出力表示例です。

```
 00:53:01 up 6 days, 14:05, 3 users, load average: 0.92, 0.87, 0.71
71 processes: 68 sleeping, 2 running, 1 zombie, 0 stopped
CPU states: 18.0% user  0.1% system  16.0% nice  0.0% iowait 80.1% idle
Mem: 1030244k av, 985656k used,  44588k free,    0k shrd, 138692k buff
         424252k actv,  23220k in_d, 252356k in_c
Swap: 2040212k av, 330132k used, 1710080k free        521796k cached

 PID USER   PRI NI SIZE RSS SHARE STAT %CPU %MEM  TIME COMMAND
15775 joe    5  0 11028 10M 3192 S   1.5 4.2  0:46 emacs
14429 root   15  0 63620 62M 3284 R   0.5 24.7 63:33 X
17372 joe    11  0 1056 1056  840 R   0.5 0.4  0:00 top
17356 joe    2  0 4104 4104 3244 S   0.3 1.5  0:00 gnome-terminal
  1 root   0  0  544 544  476 S   0.0 0.2  0:06 init
  2 root   0  0   0   0    0 SW  0.0 0.0  0:00 kflushd
  3 root   1  0   0   0    0 SW  0.0 0.0  0:24 kupdate
  4 root   0  0   0   0    0 SW  0.0 0.0  0:00 kpiod
  5 root   0  0   0   0    0 SW  0.0 0.0  0:29 kswapd
347 root   0  0  556 556  460 S   0.0 0.2  0:00 syslogd
357 root   0  0  712 712  360 S   0.0 0.2  0:00 klogd
372 bin    0  0  692 692  584 S   0.0 0.2  0:00 portmap
388 root   0  0   0   0    0 SW  0.0 0.0  0:00 lockd
389 root   0  0   0   0    0 SW  0.0 0.0  0:00 rpciod
414 root   0  0 436 432  372 S   0.0 0.1  0:00 apmd
476 root   0  0 592 592  496 S   0.0 0.2  0:00 automount
```

topコマンドを終了するには、[q]キーを押します。

以下は、topコマンドの動作中に使える、便利なコマンドです。

コマンド	説明
[Space]	すぐに表示を更新します
[h]	ヘルプ画面を表示します
[k]	プロセスをkillします。プロセスIDとそれに送る信号を要求されます。
[n]	表示されるプロセスの数を変更します。数を入力するように要求されます。
[u]	ユーザーの順に並べます。
[M]	メモリ使用量の順に並べます。
[P]	CPU使用率の順に並べます。

表26-1. インタラクティブなtopのコマンド

ヒント

Mozillaや **Nautilus**などのアプリケーションは、スレッド認知します。— 複数のスレッドが複数のユーザーまたは複数の要求を取り扱うために作成され、各スレッドにはプロセスIDが与えられます。デフォルトでは、psとtopはメイン(初期) のスレッドのみ表示します。すべてのスレッドを表示するには、ps -mコマンドを使用するか、または topの中で[Shift]と[H] のキーの組み合わせを押します。

topをグラフィカルインターフェイスで使いたい場合は、**GNOME システムモニタ**を利用できます。デスクトップで起動するには、(パネル上の)**メインメニューボタン** => **システムツール** => **システムモニタ**と進むか、または、X Window System 内のシェルプロンプトでgnome-system-monitor とタイプします。そして、**プロセス一覧** タブを選択します。

GNOMEシステムモニタを使用すると、起動中のプロセス一覧でプロセスの検索ができ、また、すべてのプロセス、自分のプロセス、またはアクティブなプロセスを表示できます。

プロセスについての詳細を見るには、そのプロセスを選択して、**詳細情報**ボタンをクリックします。プロセスに関する詳細がウィンドウの底辺に表示されます。

プロセスを停止するには、それを選択して**プロセスの終了**をクリックします。この機能は、ユーザー入力に応答しなくなったプロセスに役に立ちます。

特定の欄で情報別に分類するには、その欄の名前をクリックします。情報が分類された欄が濃い灰色で提示されます。

デフォルトでは、**GNOMEシステムモニタ**はスレッドを表示しません。この設定を変更するには、**編集** => **Preferences** と選択して、**プロセス一覧** タブをクリックします。そして**スレッドを表示する**を選択します。また、Preferencesでは更新時間、デフォルトで各プロセスについて表示する情報のタイプ、システムモニタグラフの色などの設定もできます。

図26-1. GNOME システムモニタ

26.2. メモリ使用量

freeコマンドは、システムの物理メモリとスワップ領域の総量の他にも、使用中のメモリ、空きメモリ、共有メモリ、カーネルバッファのメモリ、キャッシュメモリの容量も表示します。

```
      total   used   free  shared  buffers  cached
Mem:   256812  240668   16144  105176   50520   81848
-/+ buffers/cache:  108300  148512
Swap:   265032   780  264252
```

free -mコマンドは、同じ情報をメガバイトで表示するので読みやすくなります。

```
      total   used   free  shared  buffers  cached
Mem:     250    235     15    102     49     79
-/+ buffers/cache:    105    145
Swap:    258     0    258
```

freeをグラフィカルインターフェイスで使用する場合も、**GNOMEシステムモニタ**を使うことができます。デスクトップから起動するには、(パネル上の) **メインメニューボタン** => **システムツール**=> **システムモニタ**の順で選択します。または、X Window System 内のシェルプロンプトでgnome-system-monitor と入力して、次に**システムモニタ**タブを選択します。

図26-2. GNOME システムモニタ

26.3. ファイルシステム

dfコマンドはシステムのディスク領域の使用状況を表示します。シェルプロンプトでdf コマンドを入力すると、次のような出力が表示されます。

```
Filesystem     1k-blocks   Used Available Use% Mounted on
/dev/hda2      10325716  2902060  6899140 30% /
/dev/hda1         15554   8656   6095 59% /boot
/dev/hda3      20722644  2664256 17005732 14% /home
none         256796    0  256796  0% /dev/shm
```

デフォルトでは、このユーティリティは、パーティションサイズを1キロバイトブロックの単位で表示し、使用中と未使用のディスク領域の大きさをキロバイト単位で表示します。メガバイトやギガバイトで表示するには、df -hコマンドを使用します。-hという引数は、「human-readable format：人間が読める形式」という意味です。その出力は次のようになります。

```
Filesystem      Size Used Avail Use% Mounted on
/dev/hda2      9.8G 2.8G 6.5G 30% /
/dev/hda1       15M 8.5M 5.9M 59% /boot
/dev/hda3       20G 2.6G  16G 14% /home
none        251M  0 250M  0% /dev/shm
```

パーティションの一覧の中に、/dev/shm という項目があります。この項目はシステムの仮想メモリーファイルシステムを示す名目です。

duコマンドは、ディレクトリにあるファイルが占めている領域の大きさを見積もって表示します。シェルプロンプトでduとタイプすると、サブディレクトリごとにディスク使用状況が一覧表示されます。一覧の最後の行には、現在のディレクトリとサブディレクトリの総合計も表示されます。すべてのサブディレクトリの合計を見る必要がない場合は、du -hsコマンドを使用すると、人間に読み

やすい形式でそのディレクトリの総計だけを見ることができます。他のオプションを見るには、du --helpコマンドを使ってください。

グラフィカルな形式でシステムのパーティションとディスク領域の使用量を表示するには、図26-2の底辺に示してあるように**システムモニタ**タブを使用します。

ヒント

ディスク容量制限の実践についての詳細は、第6章を参照してください。

26.3.1. ファイルシステムの監視

Red Hat Linuxには、システムの使用可能な空き領域の大きさを監視するdiskcheckというユーティリティがあります。設定ファイルを基づいて、ひとつまたは複数のドライブが指定の容量に到達した時にシステム管理者に電子メールを送信します。このユーティリティを使用するには、diskcheck RPMパッケージがインストールされている必要があります。

このユーティリティは毎時のcron[1]タスクとして実行されます。

以下の変数は、/etc/diskcheck.conf で定義できます。

- defaultCutoff — ディスクドライブがこのパーセント容量に達したときに報告されます。たとえば、defaultCutoff = 90なら、モニタされているディスクドライブが90%容量に達したときに電子メールが送信されます。
- cutoff[*/dev/partition*] — パーティションにdefaultCutoffを上書きします。たとえば、cutoff[’/dev/hda3’] = 50を指定した場合、パーティション/dev/hda3が50%容量に達すると、diskcheckコマンドがシステム管理者に警告します。
- cutoff[*/mountpoint*] — マウントポイントに defaultCutoffを上書きします。たとえば、 cutoff[’/home’] = 50を指定した場合、マウントポイント/homeが50%容量に達すると、 diskcheckがシステム管理者に警告します。
- exclude — diskcheckを無視するひとつまたは複数のパーティションを指定します。たとえば、exclude = "/dev/sda2 /dev/sda4"を指定した場合、/dev/sda2か/dev/sda4 が指定されたカットオフパーセントに達しても、diskcheckはシステム管理者に警告しません。
- ignore — 無視するひとつまたは複数のファイルシステムタイプを-x *filesystem-type*の形式で指定します。例えば、ignore = "-x nfs -x iso9660" を指定した場合、システム管理者は、nfsまたはiso9660 ファイルシステムが容量に達していることを警告されません。
- mailTo — パーティションやマウントポイントが指定された容量に達したときに、警告が送信されるシステム管理者の電子メールアドレス。たとえば、 mailTo = "webmaster@example.com"が指定された場合、webmaster@example.comに電子メール警告が送信されます。
- mailFrom — 電子メール送信者の身元を指定します。これは、システム管理者が diskcheckコマンドからのメールにフィルタをかける場合に便利です。たとえば、mailFrom = "Disk Usage Monitor"が指定された場合、送信者のDisk Usage Monitorを含む電子メールがシステム管理者に送信されます。
- mailProg — 電子メール警告の送信に使用されるメールプログラムを指定します。たとえば、mailProg = "/usr/sbin/sendmail"が指定された場合、メールプログラムとしてSendmailが使用されます。

cronタスクが実行されるたびに読み込まれるので、設定ファイルを変更する場合も、サービスを再開する必要はありません。cronタスクが処理されるためには、crond サービスが起動している必要があ

1. cronの詳細については第28章を参照してください。

ります。デーモンが稼働しているか判定するには、/sbin/service crond status コマンドを使います。起動時にサービスをスタートすることをお勧めします。起動時にcronサービスを自動的にスタートする方法の詳細については、第14章 を参照してください。

26.4. ハードウェア

ハードウェアの設定中にトラブルがあった場合、あるいは単純にシステムにあるハードウェアを知りたい場合は、**ハードウェアブラウザ** アプリケーションを使用して、検査できるハードウェアを表示することができます。デスクトップからプログラムを開始するには、**メインメニューボタン** => **システムツール** => **ハードウェアブラウザ**と選択して行きます。あるいは、シェルプロンプトでhwbrowserと入力します。図26-3に示してあるように、ご使用のCD-ROMデバイス、フロッピーディスク、ハードドライブとそのパーティション、ネットワークデバイス、ポインティングデバイス、システムデバイス、及びビデオカードが表示されます。左のメニューのカテゴリ名をクリックすると、情報が表示されます。

図26-3. ハードウェアブラウザ

lspciコマンドを使用してすべてのPCI デバイスを一覧表示できます。verbose情報の詳細は lspci -vコマンドを、very verbose出力についてはlspci -vvコマンドを使用します。

たとえば、lspciを使用して、システムのビデオカードのメーカー、モデル、メモリーサイズを判定することができます。

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04) (prog-if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max
Flags: medium devsel, IRQ 16
Memory at f4000000 (32-bit, prefetchable) [size=32M]
```

```
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

システム内のネットワークカードを判定するのに、製造元やモデル番号が判らない場合、lspciが役に立ちます。

26.5. その他のリソース

システム情報の収集については、次の資料も参考にしてください。

26.5.1. インストールされているドキュメント

- ps --help — ps と共に使用できるオプションの一覧を表示します。
- topのマニュアルページ— man topと入力すると、top コマンドとそのオプションについて、詳しい説明を読むことができます。
- freeのマニュアルページ— man freeと入力すると、free コマンドとそのオプションについて、詳しい説明を読むことができます。
- dfのマニュアルページ— man dfと入力すると、df コマンドとそのオプションについて、詳しい説明を読むことができます。
- duのマニュアルページ— man duと入力すると、du コマンドとそのオプションについて、詳しい説明を読むことができます。
- lspci マニュアルページ— man lspciと入力すると、lspci コマンドとそのオプションについて、詳しい説明を読むことができます。
- /proc — /procディレクトリの内容を使って、さらに詳しいシステム情報を集めることもできます。/procディレクトリの詳細については、*Red Hat Linux* 参照ガイドを参照してください。

26.5.2. 関連書籍

- *Red Hat Linux* システムアドミニストレーションプレミア; Red Hat, Inc. — リソースのモニタに関する章が記載されています。

第27章
プリンタ設定

プリンタ設定ツールを使用するとユーザーはRed Hat Linuxでプリンタを設定することができます。このツールは、プリンタ設定ファイル、印刷スプールディレクトリ、及び印刷フィルターの保全を手伝います。

バージョン9から開始されたRed Hat LinuxのデフォルトのCUPS印刷システム。以前のデフォルト印刷システムであるLPRngは、まだ提供されています。システムがLPRngを使用する以前のRed Hat Linuxバージョンからアップグレードされている場合、アップグレードプロセスはLPRngをCUPSに交換していません。システムはLPRngを使い続けます。

システムが、CUPSを使用していた以前のRed Hat Linuxバージョンからアップグレードされている場合、アップグレードプロセスは設定済みのキューを保存しており、システムはCUPSを使い続けます。

プリンタ設定ツールはCUPSとLPRngの両方の印刷システムを設定しますが、これはどちらのシステムが使用目的で設定されているかによります。変更を適用した時点で、使用する印刷システムが設定されます。

プリンタ設定ツールを使用するにはrootの権限が必要です。このアプリケーションを開始するには、パネル上から**メインメニューボタン** =>**システム設定** =>**プリンタ設定**と進みます。又は、コマンド`redhat-config-printer`を入力します。このコマンドは、それがグラフィカルX Windowシステム環境から、又はテキストベースのコンソールから実行されたかに応じて、自動的にグラフィカルバージョンかテキストベースバージョンの実行を決定します。

また、シェルプロンプトでコマンド`redhat-config-printer-tui`を使用すれば、**プリンタ設定ツール**をテキストベースのアプリケーションとして実行することが出来ます。

重要

`/etc/printcap`ファイル又は`/etc/cups/` ディレクトリ内のファイルを編集しないで下さい。プリンタデーモン(`lpd` 又は`cups`)が起動/再起動する度に、新しい設定ファイルが動的に生成されます。このファイルは**プリンタ設定ツール**に変更が適用された時にも動的に生成されます。

LPRngを使用している状態で、**プリンタ設定ツール**を使わないでプリンタを追加したい場合には、`/etc/printcap.local`を編集します。`/etc/printcap.local`内のエントリは**プリンタ設定ツール**内に表示されませんが、プリンタデーモンにより読み込まれます。以前のバージョンのRed Hat Linuxからシステムをアップグレードしている場合、既存の設定ファイルは、このアプリケーションで使用される新しい形式に変換されています。新しい設定ファイルが生成される度に、古いファイルは`/etc/printcap.old`に保存されます。

CUPSを使用している場合、**プリンタ設定ツール**は、**プリンタ設定ツール**を使用しないで設定されたキューや共有は表示しません。しかし、それらを設定ファイルから削除することもしません。

図27-1. プリンタ設定ツール

以下のようなタイプの印刷キューを設定できます：

- **ローカル接続のプリンタ** — パラレル又はUSBポート経由で直接コンピュータに接続されているプリンタ。
- **ネットワーク上のCUPS (IPP)** — IPPと呼ばれるインターネット印刷プロトコルを経由してTCP/IPネットワーク上でアクセスできるプリンタ(例えば、ネットワーク上でCUPSを実行している別のRed Hat Linuxシステムに接続されているプリンタ)。
- **ネットワーク上のUNIX (LPD)** — TCP/IPネットワーク上でアクセスできる別のUNIXシステムへ接続されたプリンタ。(例えば、ネットワーク上でLPDを実行している別のRed Hat Linuxへ接続されているプリンタ)。
- **ネットワーク上のWindows (SMB)** —SMBネットワーク上のプリンタを共有する別のシステムに接続されているプリンタ。(例えば、Microsoft Windows™マシンに接続されているプリンタ)。
- **ネットワーク上のNovell (NCP)** — NovellのNetWareネットワーク技術を使用した別のシステムに接続されているプリンタ。
- **ネットワーク上のJetDirect** — コンピュータにではなく、HP JetDirectを通してネットワークに直接接続されているプリンタ。

重要

新規の印刷キューを追加したり、又は既存のものを変更したりする場合、その変更を有効にするにはそれを「適用」する必要があります。

適用ボタンをクリックすると、変更した内容が保存されプリンタデーモンが再起動します。変更はプリンタデーモンが再起動すると設定ファイルに書き込まれます。別の方法として、**操作** => **適用**と選択することでも実行できます。

27.1. ローカルプリンタの追加

コンピュータのパラレルポート、あるいはUSBポートに接続されているローカルプリンタを追加するには、メインの**プリンタ設定ツール**ウィンドウ内で**新規**ボタンをクリックして図27-2に示すようなウィンドウを出します。そして**進む**ボタンをクリックして続けます。

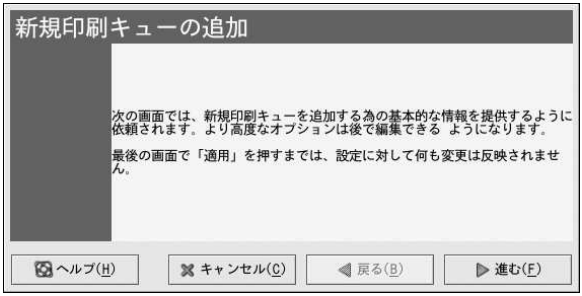


図27-2. プリンタの追加

図27-3の画面で示してあるように、**プリンタ名**のテキストフィールドにプリンタ用の独特の名前を入力します。プリンタ名は空白を含むことができず、文字で始まる必要があります。プリンタ名は文

字、数字、ハイフン(-)、下線(_)を含むことが出来ます。オプションとして、空白を含むことができるプリンタ用の短い説明を入力します。

図27-3. プリンタ名の選択

進むボタンをクリックすると、図27-4が表示されます。**プリンタタイプの選択**メニューから**ローカル接続のプリンタ**を選択します。デバイスは通常、パラレルプリンタ用には/dev/lp0であり、USBプリンタ用には/dev/usb/lp0です。一覧にデバイス名が表示されない場合は、**デバイスを再スキャン**ボタンをクリックしてコンピュータを再スキャンするか、又は**カスタムデバイス**ボタンをクリックして、手動でそれを指定します。**進む**ボタンをクリックして続けます。

図27-4. ローカルプリンタの追加

次のステップでプリンタのタイプを選択します。項27.7まで進んで続けて下さい。

27.2. IPPプリンタの追加

IPPプリンタとは、同じネットワーク上で別のLinuxシステムへ接続されたCUPSを実行しているプリンタ、又は、別のオペレーティングシステム上でIPPを使用するように設定されたプリンタです。デフォルト設定で、**プリンタ設定ツール**は共有のIPPプリンタを探してネットワークを閲覧します。(このオプションは、プルダウンメニューから**操作** => **共有**と選択して行き、変更することが出来ます)。ネットワーク上のIPPプリンタはいずれもメインウィンドウに、検索したプリンタとして表示されます。

プリンタサーバー上にファイアウォールを設定している場合、これは受信UDPポート631で接続を送信と受信できる必要があります。クライアント(印刷要求を送信するコンピュータ)上にファイアウォールを設定している場合、ポート631で接続の送信と受け付けを許可される必要があります。

自動の閲覧機能を無効にしている場合でも、メインの**プリンタ設定ツール** ウィンドウで**新規**ボタンをクリックすることによりネットワーク上のIPP プリンタを追加することができ、図27-2の中にあるウィンドウを表示します。**進む**ボタンをクリックして続けます。

図27-3の画面で示してあるように、**プリンタ名**のテキストフィールドにプリンタ用の独特の名前を入力します。プリンタ名は空白を含むことができず、文字で始まる必要があります。プリンタ名は文字、数字、ハイフン(-)、下線(_)を含むことが出来ます。オプションとして、空白を含むことができるプリンタ用の短い説明を入力します。

進むボタンをクリックした後に、図27-5が表示されます。**プリンタタイプの選択**から**ネットワーク上のCUPS (IPP)**を選択します。

図27-5. IPPプリンタの追加

次のオプションを持つテキストフィールドが表示されます：

- **サーバー** — プリンタが接続されているリモートマシンのホスト名、又はIPアドレス。
- **パス** — リモートマシン上の印刷キューへのパス。

進むボタンをクリックして続けます。

次のステップでプリンタのタイプを選択します。項27.7まで進んで続けて下さい。

重要

ネットワーク上のIPPプリンタサーバーはローカルシステムからの接続を許可する必要があります。詳細は項27.13で御覧下さい。

27.3. リモートUNIX (LPD)プリンタの追加

同一ネットワーク上の別のLinuxシステムに接続されているようなリモートのUNIXプリンタを追加するには、メインの**プリンタ設定ツール**ウィンドウで**新規**ボタンをクリックします。図27-2に示すウィンドウが現れます。**進む** ボタンをクリックして続けます。

図27-3の画面で示してあるように、**プリンタ名**のテキストフィールドにプリンタ用の独特の名前を入力します。プリンタ名は空白を含むことができず、文字で始まる必要があります。プリンタ名は文字、数字、ハイフン(-)、下線(_)を含むことが出来ます。オプションとして、空白を含むことができるプリンタ用の短い説明を入力します。

プリンタタイプの選択メニューの中から**ネットワーク上のUNIX (LPD)**を選択して**進む**ボタンをクリックします。

図27-6. リモートLPDプリンタの追加

次のオプションを持つテキストフィールドが表示されます：

- **サーバー** — プリンタが接続してあるリモートマシンのホスト名、又はIPアドレス。
- **プリンタ** — リモートのプリンタキュー。デフォルトのプリンタキューは通常lpです。

進むボタンをクリックして続けます。

次のステップでプリンタのタイプを選択します。項27.7まで進んで続けて下さい。

重要

リモートのプリントサーバーはローカルシステムからの印刷ジョブを受理する必要があります。詳細は項27.13.1を御覧下さい。

27.4. Samba (SMB)プリンタの追加

SMBプロトコルを使用してアクセスするプリンタ(Microsoft Windowsシステムに接続されているようなプリンタ)を追加するには、メインの**プリンタ設定ツール**ウィンドウで**新規** ボタンをクリックします。図27-2に示すようなウィンドウが現れます。**進む**ボタンをクリックして続けます。

図27-3の画面で示してあるように、**プリンタ名**のテキストフィールドにプリンタ用の独特の名前を入力します。プリンタ名は空白を含むことができず、文字で始まる必要があります。プリンタ名は文字、数字、ハイフン(-)、下線(_)を含むことが出来ます。オプションとして、空白を含むことができるプリンタ用の短い説明を入力します。

プリンタタイプの選択メニューから**ネットワーク上のWindows (SMB)**を選択して、**進む**ボタンをクリックします。Microsoft Windowsシステムにプリンタが接続してある場合は、このキュータイプを選択します。

図27-7. SMBプリンタの追加

図27-7で表示してあるように、SMB共有は自動的に検出され一覧表示されます。各共有名の横にある矢印をクリックしてその一覧を展開します。展開した一覧からプリンタを1つ選択します。

目的のプリンタが一覧にない場合は、右側にある**指定**ボタンをクリックします。すると以下のオプションを持つテキストフィールドが表示されます：

- **ワークグループ** — 共有プリンタ用のSambaワークグループの名前。
- **サーバー** — プリンタを共有しているサーバーの名前。
- **共有** — 印刷したい共有プリンタの名前。この名前は、リモートのWindowsマシン上のSambaプリンタとして定義されている物と同じである必要があります。
- **ユーザー名** — プリンタにアクセスする為にログインするユーザーの名前。このユーザーはWindowsシステム上でも存在する必要があり、プリンタにアクセスする権限を持っていなければなりません。デフォルトのユーザーは標準的にWindowsサーバー用には**guest**であり、Sambaサーバー用には**nobody**です。
- **パスワード** — **ユーザー**フィールドに指定してあるユーザーのパスワード(必要な場合)。

進むボタンをクリックして続けます。そこで**プリンタ設定ツール**は共有プリンタに接続しようと試みます。共有プリンタがユーザー名とパスワードを必要とする場合、ダイアログウィンドウが開いて共有プリンタの有効なユーザー名とパスワードの供給が要求されます。共有名を間違えて指定した場合、ここでも変更が出来ます。共有に接続するのにワークグループ名が要求される場合は、このダイアログボックスで指定できます。このダイアログウィンドウは**指定**ボタンをクリックする時に表示されるものと同じものです。

次のステップでプリンタのタイプを選択します。項27.7まで進んで続けて下さい。

警告

ユーザー名とパスワードを必要とする場合、それらは暗号化をしないままで、root とlpdだけが読み込み権利を持つファイルに保存されています。その為、第三者がrootアクセスを持つ場合、ユーザー名とパスワードを知られてしまいます。これを避けるには、プリンタにアクセスするためのユーザー名とパスワードは、ローカルRed Hat Linuxシステム上のユーザーアカウント用のユーザー名とパスワードとは別なものにする必要があります。それらが異なる場合は、唯一可能性のあるセキュリティ侵略は、プリンタの違反使用ということになります。サーバからのファイル共有がある場合、これもプリンタキューに設定してあるものとは別のパスワードを使用されることが推奨されます。

27.5. Novell NetWare (NCP)プリンタの追加

Novell NetWare (NCP)プリンタを追加するには、メイン**プリンタ設定ツール** ウィンドウ内の**新規**ボタンをクリックします。すると図27-1に示すようなウィンドウが現れます。**進む**ボタンをクリックして続けます。

図27-3の画面で示してあるように、**プリンタ名**のテキストフィールドにプリンタ用の独特の名前を入力します。プリンタ名は空白を含むことができず、文字で始まる必要があります。プリンタ名は文字、数字、ハイフン(-)、下線(_)を含むことが出来ます。オプションとして、空白を含むことができるプリンタ用の短い説明を入力します。

プリンタタイプの選択メニューから**ネットワーク上のNovell (NCP)**を選択します。

図27-8. NCPプリンタの追加

次のオプションを持つテキストフィールドが表示されます：

- **サーバー** — プリンタが接続してあるNCPシステムのホスト名、又はIPアドレス。
- **プリンタ** — NCPシステム上のプリンタのリモートキュー。
- **ユーザー** — プリンタにアクセスする為にログインするユーザー名。
- **パスワード** — 上記の**ユーザー**フィールドに指定したユーザー用のパスワード。

次のステップでプリンタのタイプを選択します。項27.7まで進んで続けて下さい。

警告

ユーザー名とパスワードを必要とする場合、それらは暗号化をしないままで、root とlpdだけが読み込み権利を持つファイルに保存されています。その為、第三者がrootアクセスを持つ場合、ユーザー名とパスワードを知られてしまいます。これを避けるには、プリンタにアクセスするためのユーザー名とパスワードは、ローカルRed Hat Linuxシステム上のユーザーアカウント用のユーザー名とパスワードとは別なものにする必要があります。それらが異なる場合は、唯一可能性のあるセキュリティ侵略は、プリンタの違反使用ということになります。サーバからのファイル共有がある場合、これもプリンタキューに設定してあるものとは別のパスワードを使用されることが推奨されます。

27.6. JetDirectプリンタの追加

JetDirectプリンタを追加するには、メインの**プリンタ設定ツール**ウィンドウ内の**新規**ボタンをクリックします。図27-1に示すようなウィンドウが表示されます。そこで**進む**ボタンをクリックして進みます。

図27-3の画面で示してあるように、**プリンタ名**のテキストフィールドにプリンタ用の独特の名前を入力します。プリンタ名は空白を含むことができず、文字で始まる必要があります。プリンタ名は文字、数字、ハイフン(-)、下線(_)を含むことが出来ます。オプションとして、空白を含むことができるプリンタ用の短い説明を入力します。

プリンタタイプの選択のメニューから**ネットワーク上のJetDirect**を選択します。そして**進む**ボタンをクリックします。

図27-9. JetDirectプリンタの追加

次のオプションを持つテキストフィールドが表示されます：

- **プリンタ** — JetDirectプリンタのホスト名、又はIPアドレスを入力します。
- **ポート** — 印刷ジョブを監視するJetDirectプリンタのポート。デフォルトでは9100になっています。

次のステップでプリンタのタイプを選択します。項27.7まで進んで続けて下さい。

27.7. プリンタモデルの選択と終了

プリンタタイプを選択した後、次のステップはプリンタモデルを選択することです。

図27-10と同様なウィンドウが表示されます。自動検出がされなかった場合、一覧からそのモデルを選択します。プリンタは製造元別に区分してあります。先ずプルダウンメニューから製造元を選択します。プリンタモデルは製造元が選択される度に更新されます。一覧からプリンタモデルを選択します。

図27-10. プリンタモデルの選択

推奨のプリンタドライバーは、選択したプリンタモデルを元にして選択されます。プリンタドライバーは、印刷したいデータをプリンタが理解できる形式に処理します。ローカルプリンタは直接コンピュータに接続されている為、プリンタに送られるデータを処理する為のプリンタドライバーが必要になります。

リモートプリンタ(IPP, LPD, SMB,又はNCP)を設定している場合、リモートプリンタサーバーは通常、それ自身のプリンタドライバーを持っています。ローカルマシンに追加のプリンタドライバーを選択した場合、データは複数回フィルターされてプリンタが理解できないような形式に変換されてしまいます。

データが1回以上フィルターされないようにするには、最初に製造元として**汎用**を選択し、プリンタモデルとして**直接印刷キュー**か、あるいは**Postscriptプリンタ**を選択してみます。変更を適用した後、テストページを印刷してこの新規設定を試します。もしテストが失敗すれば、リモートプリンタサー

バーが、プリンタドライバを設定していない可能性があります。その場合、リモートプリンタの製造元とモデルに応じてプリンタドライバーを選択して、変更を適用した後、テストページを印刷してみます。

ヒント

プリンタを追加した後は、**プリンタ設定ツール**をスタートして別のプリンタドライバーを選択することができます。一覧からプリンタを選択して、**編集**ボタンをクリックして**プリンタドライバー**タブをクリックします。別のドライバーを選択したあとは、変更を適用します。

27.7.1. プリンタ設定の確認

最後のステップはプリンタ設定の確認です。設定内容が正しければ**適用**ボタンをクリックして印刷キューを追加します。**戻る**ボタンをクリックするとプリンタ設定を修正できます。

メインウィンドウの**適用**ボタンをクリックするとそれまでの変更を保存して、プリンタデーモンを再起動します。変更を適用した後には、その設定が正しいかどうか確認する為にテストページを印刷して下さい。詳細は項27.8を御覧下さい。

基本的なASCIIセット以上の文字(日本語などで使用される文字も含む)が必要な場合は、ドライバーオプションを見直して、**Postscriptの再描画**を選択します。詳細は項27.9を参照して下さい。さらには印刷キューを追加した後に編集する場合は、紙面サイズなどのオプションも設定することができます。

27.8. テストページの印刷

プリンタを設定した後で、プリンタが適切に機能しているかどうかを確認する為にテストページを印刷すべきです。このテストページを印刷するには、プリンタの一覧から試したいプリンタを選択して、**テスト**プルダウンメニューから妥当なテストページを選択します。

プリンタドライバーを変更したり又は、ドライバーオプションを修正したりする場合、テストページを印刷して異なった設定をテストする必要があります。

図27-11. テストページオプション

27.9. 既存プリンタの変更

既存のプリンタを削除するには、そのプリンタを選択し、ツールバーの**削除**ボタンをクリックします。プリンタの一覧からそのプリンタが削除されますので、**適用** ボタンをクリックするとその変更を保存しプリンタデーモンが再起動します。

デフォルトのプリンタを設定するには、プリンタの一覧からそのプリンタを選択してツールバーにある**デフォルト**ボタンをクリックします。するとデフォルトのプリンタアイコン が、一覧のデフォルトプリンタの**デフォルト**列に表示されます。

プリンタを追加した後、その設定の編集をするにはプリンタの一覧からそのプリンタを選択して**編集**ボタンをクリックします。図27-12に示されたようなタブ付きのウィンドウが表示されます。このウィンドウには、選択したプリンタの現在の値が含まれます。必要な変更を加えて**OK**ボタンをクリックします。メインの**プリンタ設定ツール**ウィンドウ内の**適用** ボタンをクリックすると変更が保存され、プリンタデーモンが再起動します。

図27-12. プリンタの編集

27.9.1. プリンタ名

プリンタの名前やその短い説明を変更するには、**プリンタ名**タブ内の値を変更します。その後**OK**ボタンをクリックするとメインウィンドウに戻ります。プリンタの名前はプリンタの一覧で変更されているはずです。**適用** ボタンをクリックすると変更を保存しプリンタデーモンが再起動します。

27.9.2. プリンタ名

プリンタタイプタブでは、プリンタを追加してその設定をした時に選択したプリンタタイプが表示されます。プリンタのプリンタタイプ、又はその設定は変更できます。変更をした後は、**OK**ボタンをクリックするとメインのウィンドウに戻ります。**適用**をクリックして変更を保存しプリンタデーモンを再起動します。

どのキュータイプが選択されているかに応じて、各種のオプションが表示されます。オプションの説明については、プリンタの追加に関するセクションを参照して下さい。

27.9.3. プリンタドライバ

プリンタドライバタブでは、現在使用されているプリンタドライバを表示します。変更した場合は、その後**OK**ボタンをクリックしてメインウィンドウに戻ります。**適用**をクリックすることで変更を保存し、プリンタデーモンを再起動します。

27.9.4. ドライバオプション

ドライバオプションタブでは、高度なプリンターオプションを表示します。各プリンタドライバに応じてドライバは異なります。一般的なオプションには次の項目が含まれます：

- **Form-Feed (FF)を送る**は、印刷の最後のページがプリンタから排出されない(例：Form-Feedライトが点滅する)場合に選択すべきオプションです。これが機能しない場合は、**End-of-Transmission(EOT)を送る**を代わりに試します。幾つかのプリンタは最後のページを送出するのに**Form-Feed (FF)を送る**と**End-of-Transmission(EOT)を送る**の両方のオプションを必要とするものがあります。**Form-Feed (FF)を送る**オプションはLPRng印刷システムでのみ利用出来ます。
- **End-of-Transmission (EOT)を送る**は、「form-feedを送る」が機能しない場合、選択すべきオプションです。上記の**Form-Feed (FF)を送る**を参照して下さい。このオプションはLPRng印刷システムでのみ利用できます。
- **未知のデータをテキストとみなす**は、送られたデータをプリンタドライバが認識できない時に選択すべきオプションです。このオプションは印刷に問題がある時にのみ選択してください。このオプションが選択されると、プリンタドライバは認識できないデータは全てテキストとみなすことになり、どれもテキストで印刷しようとします。このオプションが**テキストをPostscriptに変換**オプションと一緒に選択された場合、プリンタドライバはまず、不明なデータはテキストだとみなし、それからポストスクリプトに変換します。このオプションはLPRng印刷システムでのみ利用できます。
- **PostScriptの再描画**は、基本的なASCIIセットの範囲外の文字(日本語の文字など)がプリンタに送られて来て正しく印刷できない場合に選択すべきオプションです。このオプションは標準PostScript以外のフォントを再描画して正しく印刷できるようにします。

  印刷しようとしているフォントをプリンタがサポートしていない場合、このオプションを選択してみて下さい。例えば、日本語用でないプリンタで日本語を印刷する場合にこのオプションを選択します。

  この機能を発揮するのに余分の時間が要求されます。正しいフォントを印刷するのに問題がなければ、このオプションは選択しないで下さい。

  また、プリンタがPostScriptレベル3を処理できない場合には、このオプションを選択して下さい。このオプションがそれをPostScriptレベル1に変換します。
- **GhostScript プレフィルタ** — この使用により、プリンタがポストスクリプトのいずれかのレベルを処理できない場合、**プレフィルタなし**、**PostScriptレベル1へ変換**、又は**PostScriptレベル2へ変換**を選択することが出来ます。このオプションはポストスクリプトのドライバがCUPS印刷システムと共に使用されている場合にのみ利用できます。
- **テキストをPostscriptに変換**はデフォルトで選択されています。プリンタがプレインテキスト(平文)を印刷できる場合は、このオプションを選択解除して印刷にかかる時間を節約して下さい。CUPS印刷システムを使用している場合、テキストは常にPostScriptに変換される為、これはオプションにはなりません。
- **ページサイズ**により、各種ページサイズを選択でます。オプションにはUS Letter、US Legal、A3、及びA4が含まれます。
- **フィルタで使うロケール**はデフォルトで**C**となります。日本語の文字が印刷されている場合、**ja_JP**を選択します。それ以外はデフォルトの**C**を使用します。
- **メディアの資料**は、デフォルトで**Printer default**です。別のトレイからペーパーを使用するには、このオプションを変更します。

ドライバオプションを変更するには、**OK**ボタンをクリックしてメインウィンドウに戻ります。**適用**ボタンをクリックするとその変更を保存してプリンタデーモンが再起動します。

27.10. 設定ファイルの保存

プリンタの設定が**プリンタ設定ツール**を使用して保存されると、このアプリケーションは自身の設定ファイルを作成し、それが/etc/cups ディレクトリ(又はlpdを読み込む/etc/printcapファイル)の中でファイルを作成する為に使用されます。**プリンタ設定ツール**ファイルを保存したり、復元したりするのにコマンドラインオプションを使用することが出来ます。もし/etc/cupsディレクトリ又は、/etc/printcapファイルが同じ場所で保存と復元がされる場合、プリンタデーモンが再起動する度にそれが特別な**プリンタ設定ツール**の設定ファイルから新規の/etc/printcap ファイルを生成する為、プリンタ設定は復元されません。システムの設定ファイルのバックアップを作成する時は、次の方法で、プリンタ設定ファイルを保存します。システムがLPRngを使用していて/etc/printcap.local ファイル内にカスタム設定が追加されている場合は、これもバックアップシステムの1部として保存されるべきです。

プリンタ設定を保存するには、rootとして以下のコマンドを入力します：

```
/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
```

これで、設定がsettings.xmlファイルに保存されます。

このファイルが保存されると、プリンタ設定の復元に使用できます。これは、プリンタ設定が削除された場合、Red Hat Linuxが再インストールされた場合、又は同じプリンタ設定が複数のシステムに必要な場合などに役に立ちます。このファイルは再インストールの前に別のシステムに保存しておく必要があります。設定を復元するにはrootとして次のコマンドを入力します：

```
/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
```

既に設定ファイルを所持しており(システム上で1つ又は複数のプリンタを設定している状態)で別の設定ファイルをインポート使用とした場合、その既存の設定ファイルは上書きされてしまいます。既存の設定を維持して、保存ファイル内に設定を追加する場合は、双方のファイルを次のコマンドで(rootで)マージ(融合)することが出来ます：

```
/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
```

プリンタの一覧はここで、システム上で設定したプリンタと更に保存された設定ファイルからインポートしたプリンタで構成されています。インポートした設定ファイルが、システム上の既存の印刷キューと同じ名前の印刷キューを持つ場合、インポートファイルの印刷キューが既存のプリンタを上書きします。

設定ファイルをインポートした後には(mergeコマンドの使用に関係なく)、プリンタデーモンを再起動する必要があります。CUPSを使用している場合、次のコマンドを発行します：

```
/sbin/service cups restart
```

LPRngを使用している場合は、次のコマンドを発行します：

```
/sbin/service lpd restart
```

27.11. コマンドラインで設定

Xをインストールしていない状態で、テキストベースのバージョンを使用したくない場合は、コマンドライン経由でプリンタを追加することが出来ます。スクリプトから、又はキックスタートインストールの%postセクション内で、プリンタを追加したい場合にこの方法が役に立ちます。

27.11.1. ローカルプリンタの追加

プリンタを追加するには次のコマンドを使用します：

```
redhat-config-printer-tui --Xadd-local options
```

オプションには次のようなものがあります：

--device=*node*

‘ (必須) 使用するデバイスノード。例えば、/dev/lp0。

--make=*make*

‘ (必須) IEEE 1284 MANUFACTURER 文字列、又は製造元の文字列がない場合は、foomaticデータベース内にあるようなプリンタの製造元の名前。

--model=*model*

‘ (必須) IEEE 1284 MODEL 文字列、又はモデルの文字列がない場合、foomaticデータベース内に一覧表示してあるプリンタモデル。

--name=*name*

‘ (選択可) 新しいプリンタへ与える名前。与えられない場合、デバイスノード(“lp0”など) を元にした名前が使用されます。

--as-default

‘ (選択可) デフォルトのプリンタとしてこれを設定。

CUPSを印刷システムとして使用している場合(デフォルト)、プリンタを追加した後に次のコマンドを使用してプリンタデーモンを起動/再起動させます：

```
service cups restart
```

LPRngを印刷システムとして使用している場合、プリンタを追加した後で、次のコマンドを使用してプリンタデーモンを起動/再起動します：

```
service lpd restart
```

27.11.2. ローカルプリンタの削除

印刷キューはコマンドライン経由で削除することが出来ます。

rootとして、印刷キューを削除するには次のコマンドを使用します：

```
redhat-config-printer-tui --Xremove-local options
```

オプションには次のようなものがあります：

--device=*node*

‘ (必須) /dev/lp0などとして使用されるデバイスノード

--make=*make*

‘ (必須) IEEE 1284 MANUFACTURER 文字列、又は(何もなければ) foomaticデータベース内にあるプリンタ製造元の名前。

--model=*model*

‘ (必須) IEEE 1284 MODEL 文字列、又は(何もなければ)、foomaticデータベースに一覧表示してあるようにプリンタのモデル。

CUPS印刷システム(デフォルト)を使用している場合、**プリンタ設定ツール**設定からプリンタを削除した後で、次のコマンドでプリンタデーモンを再起動するまでその変更は反映されません：

```
service cups restart
```

LPRng印刷システムを使用している場合、**プリンタ設定ツール**設定からプリンタを削除した後に、次のコマンドを使用してプリンタデーモンを再起動するまで、その変更は反映されません：

```
service lpd restart
```

CUPSを使用していて、プリンタを全て削除してプリンタデーモンをもう起動したくない場合は、次のコマンドを実行します：

```
service cups stop
```

LPRngを使用していて、プリンタを全て削除してプリンタデーモンをもう起動したくない場合は、次のコマンドを実行します：

```
service lpd stop
```

27.12. 印刷ジョブの管理

Emacsからのテキストファイル印刷や、**GIMP**からのイメージ印刷など、印刷ジョブをプリンタデーモンに送ると、ジョブはプリントスプールキューに追加されます。プリントスプールキューはプリンタに送られた印刷ジョブと各印刷要求の情報を持つ一覧です。この情報には要求のステータス、要求の送り主のユーザー名、要求を送ったシステムのホスト名、ジョブ番号、その他を含みます。

グラフィカルデスクトップ環境を実行している場合、パネル上で**印刷マネージャ** アイコンをクリックして、図27-13に示してあるように、**GNOME印刷マネージャ**を開きます。

図27-13. GNOME印刷マネージャ

また、これはパネル上の**メインメニューボタン** => **システムツール** =>**印刷マネージャ**と選択することでも開始できます。

プリンタ設定を変更するには、プリンタ用のアイコンを右クリックして**プロパティ**を選択します。そうすると**プリンタ設定ツール**が開始されます。

設定済みのプリンタをダブルクリックすると、図27-14で見えるようなプリントスプールキューが表示されます。

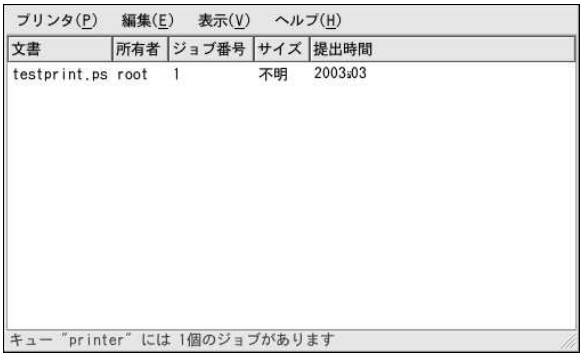


図27-14. 印刷ジョブの一覧

GNOME印刷マネージャに一覧表示してある特定の印刷ジョブを取り消すには、一覧からそれを選択して**編集**からプルダウンメニューの**文書をキャンセル**を選択します。

プリントスプールの中にアクティブな印刷ジョブがある場合、図27-15に示されるようにプリンタ通知アイコンがデスクトップパネルの**パネル通知エリア**に表示されることがあります。但し、アクティブ印刷ジョブの検出は5秒毎に実行されますので、短い印刷ジョブにはアイコンが表示されない可能性があります。

図27-15. プリンタ通知アイコン

プリンタ通知アイコンをクリックすると**GNOME印刷マネージャ**が開始され現在の印刷ジョブの一覧を表示します。

また、パネル上には**印刷マネージャ**アイコンもあります。**Nautilus**からファイルを印刷するには、そのファイルのある場所まで閲覧して、それをパネル上の**印刷マネージャ**アイコンにドラッグアンドドロップします。図27-16に示すようなウィンドウが表示されます。そこで**OK**ボタンをクリックするとファイルの印刷が開始されます。

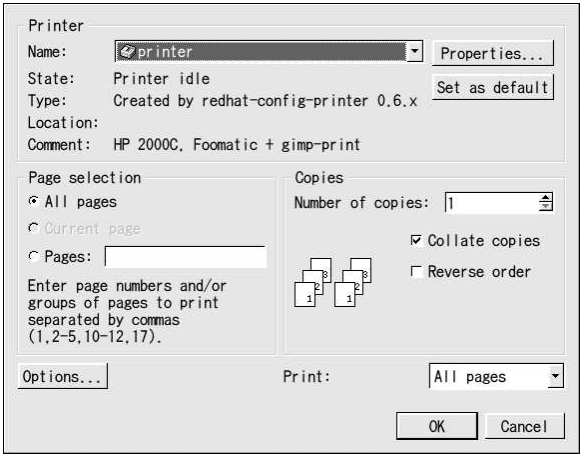


図27-16. 印刷確認のウィンドウ

シェルプロンプトでプリントスプールの印刷ジョブを表示するには、コマンド`lpq`を入力します。その表示の末尾の数行は以下のようになります：

```
Rank  Owner/ID      Class Job Files    Size Time
active user@localhost+902  A  902 sample.txt 2050 01:20:46
```

例27-1. `lpq`出力の例

印刷ジョブを取り消すには、`lpq`を使用して要求のジョブ番号を見付け、そしてコマンド`lprm` *`job number`*を使用します。例えば、`lprm 902`は例27-1に示すような印刷ジョブを取り消します。印刷ジョブを取り消すには正しい権限を持っている必要があります。プリンタが接続してあるマシン上でrootとしてログインしている場合以外は、他のユーザーが開始した印刷ジョブを取り消すことは出来ません。

シェルプロンプトから直接、ファイルを印刷することも出来ます。例えば、コマンド`lpr sample.txt`はテキストファイル`sample.txt`を印刷します。印刷フィルタがそれはどのタイプのファイルかを判断して、プリンタが理解できる形式に変換します。

27.13. プリンタの共有

プリンタ設定ツールの設定オプションを共有する機能は、CUPS印刷システムを使用している場合にのみ利用できます。LPRng用に共有を設定する方法は項27.13.1で御覧下さい。

ネットワーク上の別のコンピュータのユーザーに、自分のシステムで設定したプリンタの使用を許可することをプリンタの共有と呼びます。デフォルトでは**プリンタ設定ツール**で設定したプリンタは共有ではありません。

設定されたプリンタを共有するには、**プリンタ設定ツール**をスタートして、一覧からプリンタ1つを選択します。それから**操作** のプルダウンメニューから**共有**を選択します。

注意

プリンタが選択されていないと、**操作 => 共有**の選択は単に、通常**全般**タブに表示されるシステム全体の共有オプションを表示するだけです。

プリンタタブ上で、プリンタを他のコンピュータで利用出来るようにするオプションを選択します。

図27-17. プリンタオプション

プリンタを共有する選択をした後、デフォルトでは全てのホストが共有プリンタでの印刷を許可されます。ネットワーク上の全てのシステムにそのプリンタでの印刷を許可することは、特にシステムが直接インターネットに接続してある場合は危険です。**All hosts**のエントリを選択して**編集**ボタンをクリックします。図27-18に示すようなウィンドウが表示されますのでその中でこのオプションを変更することが推奨されます。

プリンタサーバーでファイアウォールを設定している場合、それは受信のUDPポート631で接続の送信と受信が出来る必要があります。クライアント(印刷要求を送るコンピュータ)でファイアウォールを設定している場合、ポート631で接続の送信と受信を許可される必要があります。

図27-18. 許可されたホスト

全般タブは、**プリンタ設定ツール**内で見えないものを含めて、全てのプリンタ用の設定を構成します。2つのオプションがあります:

図27-19. システム全体の共有オプション

- **自動的にリモートの共有プリンタを探す** — デフォルトで選択されています。このオプションはIPP閲覧を有効にします。これは、ネットワーク上の他のマシンが使用しているプリンタをブロー

ドキャストする時に、それらのプリンタは自動的に、システムで利用可能なプリンタの一覧に追加されるという意味になります。IPP閲覧で検出されたプリンタには追加の設定は必要ありません。但し、このオプションはローカルシステムで設定したプリンタを自動的に共有するものではありません。

- **LPDプロトコルを有効にする** — このオプションにより、プリンタはcups-lpdサービス(xinetdサービス)を利用してLPDプロトコルを使うように設定されたクライアントからの印刷ジョブを受け取ることが出来ます。


警告

このオプションが有効になっていると、印刷ジョブがLPDクライアントから来る場合は全てのホストの印刷ジョブを受け付けることになります。

27.13.1. LPRngでプリンタを共有

LPRng印刷システムを実行している場合、共有は手動で設定する必要があります。ネットワーク上のシステムにRed Hat Linuxシステムで設定したプリンタでの印刷を許可するには、次のステップを使用します：

1. /etc/accepthostファイルを作成します。このファイル内に印刷アクセスを許可するシステムのIPアドレス又はホスト名を、IPかホスト名毎に1行で追加します。
2. /etc/lpd.permsの中で以下の行をアンコメントします：
```
ACCEPT SERVICE=X REMOTEHOST=</etc/accepthost
```
3. デーモンを再起動して変更を有効にします：
```
service lpd restart
```

27.14. 印刷システムの切替え

印刷システムを切替えるには、**プリンタシステム切替**アプリケーションを実行します。開始するには、パネル上の**メインメニューボタン**=> **システム設定** =>**More System Settings** => **プリンタシステム切替**と選択していきます。又は、シェルプロンプト(例えば、XTerm やGNOMEターミナル)でコマンドredhat-switch-printerを入力します。

X Windowシステムが稼働していれば、プログラムが自動的に検出します。X Windowが実行中であると図27-20で示すように、プログラムがグラフィカルモードで開始されます。X Windowが検出されない場合は、テキストモードで開始されます。最初からテキストベースのアプリケーションとして実行する場合は、コマンド redhat-switch-printer-noxを使用します。

図27-20. プリンタシステム切替

LPRngか、又は**CUPS**の印刷システムを選択します。Red Hat Linux 9では、CUPSがデフォルトとなっています。印刷システムを1つしかインストールしていない場合は、それが唯一のオプションとして表示されます。

印刷システムを変更して**OK**ボタンを選択すると、選択したプリンタデーモンはブート時の開始が有効になります。そして、選択していないプリンタデーモンは無効になり、ブート時に開始されません。選択したプリンタデーモンが開始され、他のプリンタデーモンは停止されます。このように、切替えは素早く達成されます。

27.15. その他のリソース

Red Hat Linux上での印刷に関して詳細を学ぶには、以下のリソースを参照して下さい。

27.15.1. インストールされているドキュメント

- `man printcap` — `/etc/printcap` プリンタ設定ファイル用のマニュアルページです。
- `map lpr` — コマンドラインからファイルを印刷できる様にする`lpr`コマンド用のマニュアルページ。
- `man lpd` — LPRngプリンタデーモン用のマニュアルページ。
- `man lprm` — LPRngスプールキューから印刷ジョブを削除するコマンドラインユーティリティ用のマニュアルページ。
- `man mpage` — 1枚の紙面に複数ページを印刷するコマンドラインユーティリティ用のマニュアルページ。
- `man cupsd` — CUPSプリンタデーモン用のマニュアルページ。
- `man cupsd.conf` — CUPSプリンタデーモン設定ファイル用のマニュアルページ。
- `man classes.conf` — CUPSの為のクラス設定ファイル用のマニュアルページ。

27.15.2. 役に立つWebページ

- http://www.linuxprinting.org — *GNU/Linux Printing*には、Linuxでの印刷に関する大量の情報が含まれています。
- http://www.cups.org/ — CUPSに付いてのドキュメント、良く有る質問、ニュースグループなどです。

第28章

自動化タスク

Linuxのタスクは、指定された所定の時間内や、指定の日付に、又はシステムの平均負荷が指定した値以下の場合に自動的に実行するような設定が可能です。Red Hat Linuxは、システムを常に最新の状態に保つための重要なシステムタスクを実行するようにあらかじめ設定がされています。たとえば、locateコマンドにより使用されるslocateデータベースは毎日更新されます。システム管理者は自動化タスクによって、定期的なバックアップ、システムのモニタ、カスタムスクリプトの実行などが行えます。

Red Hat Linux には次の4種類の自動タスクユーティリティが用意されています。これらのユーティリティは、cron、anacron、at、batchです。

28.1. Cron

Cronは、繰り返し行われるタスクを実行するためのデーモンで、時刻、日付、月、曜日、週の組み合わせに従ってタスクを実行します。

Cronは、システムが継続して稼動していることを前提としています。タスクの実行予定時にシステムが稼動中でない場合、タスクは実行されません。特定の時刻ではなく、期間に基づきタスクを実行するよう構成する方法については、項28.2を参照してください。1回きりのタスクをスケジュールする方法については、項28.3を参照してください。

cronサービスを使用するには、vixie-cronRPMパッケージがインストールされ、crondサービスが実行されている必要があります。このパッケージがインストールされていることを確認するには、rpm -q vixie-cronコマンドを使用してください。このサービスが実行されていることを確認するには、/sbin/service crond statusコマンドを使用してください。

28.1.1. cronタスクの設定

cronのメイン設定ファイル/etc/crontabにある次の行を使用して設定を行います。

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

最初の4行は、cronタスクを実行する環境変数の設定に使用します。SHELL変数の値は、使用するシェル環境（この例ではbashシェル）を指定し、PATH変数はコマンドの実行に使用するパスを定義します。cronタスクの出力は、MAILTO変数に定義されたユーザー名に電子メール送信されます。MAILTO変数に空の文字列が定義されている場合（MAILTO=""）、電子メールは送信されません。HOME変数は、コマンドやスクリプトを実行する際に使用するホームディレクトリの設定に使用します。

/etc/crontabファイルの各行は1つのタスクを表し、次の形式をとります。

```
minute hour day month dayofweek command
```

- `minute` —0～59の整数
- `hour` —0～23の整数
- `day` —1～31の整数（月を指定した場合はその月にある日付）
- `month` —1～12の整数（またはjanやfebなど月の短縮名）
- `dayofweek` — 0～7の整数。0や7は日曜を表す（またはsunやmonなど曜日の短縮名）
- `command` — 実行するコマンド(コマンドは、`ls /proc >> /tmp/proc`のようなコマンドにするか、ユーザーが作成したカスタムスクリプトを実行するコマンドのいずれかにすることができます)

上記のいずれの値についても、アスタリスク（*）を使用すると、すべての有効な値が指定されます。たとえば、月の値にアスタリスクを使用すると、コマンドはその他の値による制約の範囲内で毎月実行されます。

整数間にハイフン（-）を使用すると、整数の範囲を指定できます。たとえば、**1-4**は、整数1、2、3、4を表します。

値をカンマ（,）で区切ると、値の一覧を指定できます。たとえば、**3, 4, 6, 8**はこれら4つの値を指定します。

スラッシュ（/）を使用すると、ステップ値を指定できます。範囲に***/<integer>***を付けると、範囲内でその整数の値をスキップできます。たとえば**0-59/2**とした場合、分フィールドにおける1分おきの間隔が定義されます。ステップ値は、アスタリスクと組み合わせることも可能です。たとえば、値***/3**を月フィールドで使用すると、3ヶ月ごとにタスクが実行されます。

先頭がシャープ記号（#）の行はコメント行で処理の対象外です。

`/etc/crontab`ファイルが示すように、これは`run-parts`スクリプトを使用して`/etc/cron.hourly`、`/etc/cron.daily`、`/etc/cron.weekly`、`/etc/cron.monthly`ディレクトリのスクリプトをそれぞれ毎時間、毎日、毎週、毎月実行します。これらディレクトリにあるファイルは、シェルスクリプトである必要があります。

cronタスクを毎時間、毎日、毎週、毎月設定以外の予定で実行する必要がある場合、それを`/etc/cron.d`ディレクトリに追加することが出来ます。このディレクトリ内のファイルは全て`/etc/crontab`と同じ構文を使用します。その例については、例28-1を参照して下さい。

```
# record the memory usage of the system every monday
# at 3:30AM in the file /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# run custom script the first day of every month at 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

例28-1. crontabの例

root以外のユーザーがcronタスクを設定するには、`crontab`ユーティリティを使用します。ユーザー定義のcrontabはいずれも`/var/spool/cron`ディレクトリに保存され、これを作成したユーザーのユーザー名を使用して実行されます。ユーザーとしてcrontabを作成するには、そのユーザーとしてログインし、`crontab -e`コマンドを入力してユーザー定義のcrontabを編集します。これには、`VISUAL`や`EDITOR`環境変数で指定したエディタを使用します。このファイルの形式は、`/etc/crontab`ファイルと同じです。crontabの変更が保存されると、crontabはユーザー名に従って保存され、ファイル`/var/spool/cron/`*`username`*に書き込まれます。

cronデーモンは、`etc/crontab`ファイル、`etc/cron.d/`ディレクトリ、`/var/spool/cron`ディレクトリを毎分チェックして変更がないかを確認します。変更が見付かれば、メモリにロードされます。したがってcrontabファイルを変更した場合でもデーモンを再起動する必要はありません。

28.1.2. Cronに対するアクセスの制御

/etc/cron.allowファイルや/etc/cron.denyファイルは、cronへのアクセスを制限するために使用されます。どちらのアクセスコントロールファイルも、1行にユーザー名を1つという形式で記述されています。また、どちらのファイルでも空白文字は使えません。これらのアクセスコントロールファイルを変更したときに、cronデーモン（crond）を再起動する必要はありません。アクセスコントロールファイルはユーザーがcronタスクを追加したり、削除したりしようとするたびに読み込まれます。

アクセスコントロールファイルにリストされているユーザー名に関係なく、rootユーザーはいつでもcronを使用できます。

ファイルcron.allowが存在する場合、このファイルに記載されているユーザーだけがcronを使用することができます。このとき、at.denyファイルは無視されます。

cron.allowが存在しない場合、cron.denyに記載されているユーザーはすべて、cronを使用できません。

28.1.3. サービスの起動と停止

cronサービスを起動するには、/sbin/service crond startコマンドを使用します。サービスを停止するには、/sbin/service crond stopコマンドを使用します。サービスの起動はブート時に行うことをお勧めします。ブート時に自動的にcronサービスを起動する方法については、第14章を参照してください。

28.2. Anacron

Anacronは、cronと同様のタスクスケジューラですが、これはシステムが継続的に稼動している必要はありません。これを使用して、通常はcronによって毎日、毎週、毎月実行するジョブの実行ができます。

Anacronサービスを使用するには、anacronRPMパッケージがインストールされ、anacronサービスが実行されている必要があります。このパッケージがインストールされていることを確認するには、rpm -q anacronコマンドを使用してください。このパッケージがインストールされていることを確認するには、/sbin/service anacron statusコマンドを使用してください。

28.2.1. Anacronタスクの設定

Anacronタスクの一覧は、設定ファイル/etc/anacrontab中にあります。設定ファイルの各行はタスクに対応し、次の形式をとります。

```
period delay job-identifier command
```

- period —コマンドの実行頻度（単位：日）
- delay —分単位の遅延時間
- job-identifier — ジョブのタイムスタンプファイルの名前であり、Anacronメッセージで使用するタスクの説明。空白以外の任意の文字を使用可能（スラッシュを除く）
- command —実行するコマンド

Anacronは各タスクごとに、そのタスクが設定ファイルのperiodフィールドに指定された期間内に実行されたかを確認します。タスクがその期間内に実行されていない場合は、delayフィールドに指定された遅延時間の後、commandフィールドに指定してあるコマンドを実行します。

タスクが完了すると、/var/spool/anacronディレクトリのタイムスタンプファイルに日付が記録されます。時刻ではなく日付のみが使用され、タイムスタンプファイルのファイル名にはjob-identifierの値が使用されます。

SHELLやPATHなどの環境変数は、cron設定ファイルと同様、/etc/anacrontabの先頭に定義が可能です。

デフォルトの設定ファイルは、およそ次のようになっています：

```
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# These entries are useful for a Red Hat Linux system.
1   5   cron.daily      run-parts /etc/cron.daily
7   10   cron.weekly      run-parts /etc/cron.weekly
30   15   cron.monthly      run-parts /etc/cron.monthly
```

図28-1. デフォルトのanacrontab

図28-1の説明のとおり、Red Hat Linuxのanacronを設定することにより、毎日、毎週、毎月のcronタスクを確実に実行することができます。

28.2.2. サービスの起動と停止

anacronサービスを起動するには、/sbin/service anacron startコマンドを使用します。サービスを停止するには、/sbin/service anacron stopコマンドを使用します。サービスの起動はブート時に行うことをお勧めします。ブート時に自動的にanacronサービスを起動する方法については、第14章を参照してください。

28.3. atコマンドとbatchコマンド

コマンドcronとanacronは繰り返し行われるタスクをスケジュールするために使用されますが、atコマンドは、指定した時刻に1度だけ行われるタスクをスケジュールするために使用されます。batchコマンドは、システムの平均負荷が0.8を下回ったときに実行される1度限りのタスクをスケジュールするために使用されます。

atやbatchを使用するには、at RPMパッケージをインストールし、atdサービスを実行しておく必要があります。このパッケージがインストールされていることを確認するには、rpm -q atコマンドを使用してください。このパッケージがインストールされていることを確認するには、/sbin/service atd statusコマンドを使用してください。

28.3.1. Atジョブの設定

指定した時刻に1度だけ実行されるジョブのスケジュールを設定するには、コマンドat *time*を入力します。ここで、*time*にはこのコマンドを実行する時刻を指定します。

引数*time*は次のいずれかを指定できます。

- HH:MM 形式—たとえば、04:00は午前4:00を表します。その時刻がすでに過ぎてしまっている場合、次の日のその時刻に実行されます。
- midnight—午後12:00を表します。

- noon—正午（午前12:00）を表します。
- teatime—午後4:00を表します。
- month-name day year形式—たとえば、「January 15 2002」は2002年1月15日を表します。年は省略できます。
- MMDDYY、MM/DD/YY、またはMM.DD.YY形式—たとえば、「011502」は2002年1月15日を表します。
- now + time—timeはminutes（分）、hours（時）、days（日）、weeks（週）単位で指定します。たとえば、「now + 5 days」はこのコマンドが5日後のこの時間に実行されることを表します。

最初に時刻を指定して、その次にオプションの日付を指定します。日付と時刻の書式については/usr/share/doc/at-<*version*>/timespec テキストファイルを参照してください。

atコマンドに引数timeを付けて実行すると、at>プロンプトが表示されます。実行するコマンドを入力し、[Enter]キーを押して、Ctrl-Dキーを押します。複数のコマンドを指定する場合は、コマンドを1つ入力するたびに[Enter]キーを押します。コマンドをすべて入力したら、[Enter]キーを押して、空白行を挿入し、Ctrl-Dキーを押します。また、プロンプトでシェルスクリプトを入力し、スクリプトで1行ごとに[Enter]キーを押し、空白行でCtrl-Dを押して終了することもできます。スクリプトを入力した場合、ユーザーのSHELL環境で設定されたシェル、ユーザーのログインシェル、または/bin/shのうち、最初に見つかったシェルが使用されます。

標準出力に情報を表示するコマンドやスクリプトを入力した場合、この出力はユーザーに電子メールで送信されます。

保留ジョブを表示するには、atqコマンドを使用します。詳細については項28.3.3を参照してください。

atコマンドの使用法を制限することができます。詳細については項28.3.5を参照してください。

28.3.2. batchジョブの設定

平均負荷が0.8を下回ったときに、1度きりのタスクを実行するには、batchコマンドを使用します。

batchコマンドを実行すると、at>プロンプトが表示されます。実行するコマンドを入力し、[Enter]キーを押して、Ctrl-Dキーを押します。複数のコマンドを指定する場合は、コマンドを1つ入力するたびに[Enter]キーを押します。コマンドをすべて入力したら、[Enter]キーを押して、空白行を挿入し、Ctrl-Dキーを押します。また、プロンプトでシェルスクリプトを入力し、スクリプトで1行ごとに[Enter]キーを押し、空白行でCtrl-Dを押して終了することもできます。スクリプトを入力した場合、ユーザーのSHELL環境で設定されたシェル、ユーザーのログインシェル、または/bin/shのうち、最初に見つかったシェルが使用されます。平均負荷が0.8を下回ると同時に、コマンドのセットやスクリプトが実行されます。

標準出力に情報を表示するコマンドやスクリプトを入力した場合、この出力はユーザーに電子メールで送信されます。

保留ジョブを表示するには、atqコマンドを使用します。詳細については項28.3.3を参照してください。

batchコマンドの使用法を制限することができます。詳細については項28.3.5を参照してください。

28.3.3. 保留ジョブの表示

保留されているatジョブやbatchジョブを表示するには、atqコマンドを使用します。この結果、保留になっているジョブが1行に1つずつ表示されます。各行は、ジョブ番号、日付、時間、ジョブのクラス、ユーザー名の形式をとります。ユーザーは自分のジョブしか見ることができません。ただし、rootユーザーがatqコマンドを実行した場合は、すべてのユーザーのすべてのジョブが表示されます。

28.3.4. その他のコマンドラインオプション

atやbatchには、その他にも次のようなコマンドラインオプションがあります。

オプション	説明
-f	コマンドやシェルスクリプトはプロンプトで指定するのではなく、ファイルから読み込む
-m	ジョブが完了したら、ユーザに電子メールを送信する
-v	ジョブが実行される時刻を表示する

表28-1. atとbatchのコマンドラインオプション

28.3.5. atとbatchへのアクセスの制御

/etc/at.allowファイルや/etc/at.denyファイルは、atコマンドやbatchコマンドへのアクセスを制限するために使用されます。どちらのアクセスコントロールファイルも、1行にユーザー名を1つという形式で記述されています。また、どちらのファイルでも空白文字は使えません。これらのアクセスコントロールファイルを変更したときに、atデーモン（atd）を再起動する必要はありません。アクセスコントロールファイルはユーザーがatコマンドやbatchコマンドを実行しようとするたびに読み込まれます。

アクセスコントロールファイルにリストされているユーザー名に関係なく、rootユーザーはいつでもatコマンドやbatchコマンドを使用できます。

ファイルat.allowが存在する場合、このファイルに記載されているユーザーだけがatコマンドやbatchコマンドを使用することができます。このとき、at.denyファイルは無視されます。

at.allowが存在しない場合、at.denyに記載されているユーザーはすべて、atコマンドやbatchコマンドを使用できません。

28.3.6. サービスの起動と停止

atサービスを開始するには、/sbin/service atd startコマンドを使用します。サービスを停止するには、/sbin/service atd stopコマンドを使用します。サービスの起動はブート時に行うことをお勧めします。ブート時に自動的にcronサービスを起動する方法については、第14章を参照してください。

28.4. その他のリソース

自動化タスクに関する詳細は、次のリソースを参照してください。

28.4.1. インストールされているドキュメント

- cron manページ—cronの概要
- セクション1と5のcrontab manページ—セクション1のmanページには、crontabファイルの概要が説明されています。セクション5のmanページには、ファイル形式といくつかのエントリの例が示されています。
- /usr/share/doc/at-<*version*>/timespecには、cronジョブで指定できる時刻に関する詳しい情報が含まれています。

- `anacron` manページ—anacronとコマンドラインオプションの説明
- `anacrontab` manページ—anacron設定ファイルの概要
- `/usr/share/doc/anacron-<version>/README` — Anacronの概要とそれが便利な理由を説明しています。
- `at` manページ—`at`コマンドと`batch`コマンド、およびこれらのコマンドラインオプションの説明

第29章

ログファイル

ログファイルは、システム上で動作しているカーネル、サービス、アプリケーションなどのシステムに関するメッセージが入っているファイルです。情報ごとに異なるログファイルがあります。例えば、デフォルトシステムログファイル、セキュリティメッセージだけのログファイル、cronタスク用のログファイルなどがあります。

ログファイルは、カーネルドライバをロードするなどで問題を解決しようとしているとき、システムに無許可のログインがあったかをさがすとき、などに大変役に立ちます。この章は、ログファイルの場所、ログファイルの見方、ログファイルで見るべき項目などについて説明します。

ログファイルのいくつかは`syslogd`と呼ばれるデーモンにより制御されています。 `syslogd`によって保管されているメッセージの一覧は`/etc/syslog.conf`設定ファイルで見ることができます。

29.1. ログファイルを探す

ほとんどのログファイルは`/var/log` ディレクトリ内に収まっています。`httpd`や`samba`などのいくつかのアプリケーションは`/var/log` の中に専用ログファイル用の個別ディレクトリを持っています。

ログファイルディレクトリにある複数のファイルの後ろに番号が付いているに注目してください。これらはログファイルが入れ換えられた時に生成されたものです。ログファイルは、ファイルサイズが大きくなり過ぎないように入れ換えられます。`logrotate` パッケージはcronタスクを含んでいて、それが`/etc/logrotate.conf`設定ファイルと`/etc/logrotate.d` ディレクトリにある設定ファイルに従ってログファイルを自動的に入れ換えます。デフォルトでは、毎週入れ換えて、過去4週間分のログファイルを保存するように設定されています。

29.2. ログファイルの表示

ほとんどのログファイルはプレーンテキスト形式です。**Vi**や**Emacs** など、どんなテキストエディタでも表示することができます。ログファイルのいくつかはシステムのすべてのユーザーが読み込めますが、ほとんどのログファイルは、読むためにはrootの権限が要求されます。

インテラクティブでリアルタイムのアプリケーションでシステムログファイルを表示するには、**ログビューア**を使います。このアプリケーションを開始するには、(パネル上の) **メインメニューボタン**=> **システムツール**=>**システムのログ**と進みます。または、シェルプロンプトで`redhat-logviewer`とコマンドを入力します。

図29-1. ログビューア

このアプリケーションは存在するログファイルしか表示しません。このため、図29-1 に示してあるものと異なるかもしれません。見ることができるログファイルの完全な一覧を表示するには、設定ファイル、`/etc/sysconfig/redhat-logviewer` を参照してください。

デフォルトでは、現在表示できるログファイルは30秒毎に更新されています。この更新レートを変更するには、プルダウンメニューから**編集** => **設定**と選択していきます。図29-2に示してあるウィンドウが出てきます。**ログファイル**タブで、更新レートの横にある上下の矢印をクリックして変更します。**閉じる** をクリックしてメインのウィンドウに戻ります。更新レートが直ちに変更になります。手動で現在表示できるファイルを更新するには、**ファイル** =>**今すぐ更新** と選択するか、または[Ctrl]と[R]キーを同時に押します。

キーワードでログファイルの内容をフィルタするには、**次の項目用のフィルター**のテキストフィールドにキーワードを入力して、**フィルター**ボタンをクリックします。**リセット**ボタンをクリックすると内容をリセットします。

ログファイルタブから、アプリケーションがログファイルを探す場所を変更することもできます。一覧からログファイルを選択して、**場所の変更**ボタンをクリックします。ログファイルの新しい場所を入力するか、または、**閲覧...**ボタンをクリックして、ファイル選択ダイアログを使ってファイルの場所を探します。**OK**をクリックして設定に戻り、**閉じる**をクリックしてメインウィンドウに戻ります。

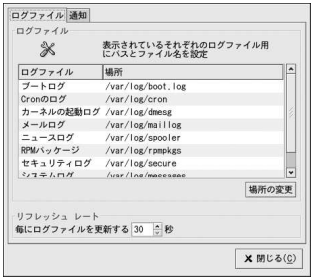


図29-2. ログファイルの場所

29.3. ログファイルの検証

ログビューアは、重要な通知用語がある行の横に通告アイコンを表示するよう設定できます。通知用語を追加するには、プルダウンメニューから **編集** => **設定**と進み、**通知**タブをクリックします。**追加**

ボタンをクリックして通知用語を追加します。通知用語を削除するには、一覧からその用語を選択して、**削除**をクリックします。

図29-3. 通知

第30章
カーネルのアップグレード

Red Hat Linuxカーネルは、Red Hatカーネルチームによってカスタマイズされ、サポートされるハードウェアとの統合性と互換性を確保しています。Red Hatはカーネルをリリースする前に、一連の厳しい品質保証テストに合格しなければなりません。

Red Hat Linuxのカーネルは RPM形式でパッケージされていますので、アップグレードと確認を容易に行うことができます。たとえば、Red Hat, Inc. 提供の`kernel` RPMパッケージをインストールするとき、`initrd`イメージが作成されます。したがって、別のカーネルをインストールした後で、`mkinitrd`コマンドを使用する必要はありません。また、GRUBまたはLILOをインストールした場合、ブートローダー設定ファイルに新規カーネルを含むように変更します。

本章では、x86システムでのみカーネルをアップグレードするために必要なステップについて説明します。


警告

ユーザーによるカスタムカーネルの構築は、Red Hat Linuxインストールサポートチームによってサポートされていません。ソースコードからのカスタムカーネルの構築に関する詳細については、付録Aを参照してください。

30.1. 2.4カーネル

Red Hat Linuxに附随するカスタム2.4カーネルには、次の特徴があります。

- カーネルソースのディレクトリは、`/usr/src/linux/`ではなく、`/usr/src/linux-2.4/` です。
- ext3ファイルシステムをサポートしています。
- マルチプロセッサ(SMP)をサポートしています。
- USBをサポートをサポートしています。
- 主としてIEEE 1394デバイスへのサポートは、FireWire™とも呼ばれています。

30.2. アップグレードの準備

カーネルをアップグレードする前に、あらかじめいくつかの準備作業をしてください。まず最初に、問題が発生した場合、システム用に作動するブートディスクがあることを確認します。ブートローダが正しく構成されていないために新規カーネルをブートできない場合は、作動するブートディスクなしにはRed Hat Linuxでシステムをブートできません。

ブートディスクを作成するには、シェルプロンプトでrootとしてログインして、以下のコマンドを実行します。

```
/sbin/mkbootdisk `uname -r`
```

ヒント

オプションの詳細についてはmkbootdiskのmanページを参照してください。

次へ進む前に、ブートディスクでマシンをリブートして、作動することを確認します。

ディスクを使用する必要がない方が望ましいのですが、万一のため安全な場所に保存してください。

インストールしてあるカーネルパッケージを確認するには、シェルプロンプトで次のコマンドを実行します。

```
rpm -qa | grep kernel
```

実行したインストールのタイプによって、以下のパッケージの一部、もしくはすべてが出力されます(バージョン番号とパッケージは異なる場合があります)。

```
kernel-2.4.20-2.47.1
kernel-debug-2.4.20-2.47.1
kernel-source-2.4.20-2.47.1
kernel-doc-2.4.20-2.47.1
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.20-2.47.1
```

出力から、カーネルのアップグレードにダウンロードする必要のあるパッケージを確認します。シングルプロセッサシステムの場合、唯一の必要なパッケージはkernelパッケージです。

複数のプロセッサを使用するコンピュータの場合、システムが複数のプロセッサを使用するために、マルチプロセッサに対応するkernel-smpパッケージが必要になります。システムでマルチプロセッサカーネルが正しく機能しない場合にkernelパッケージもインストールすることをお勧めします。

4ギガバイトを超えるメモリを備えたコンピュータの場合、システムが4ギガバイトを越えるメモリを使用するためにkernel-bigmemパッケージをインストールする必要があります。デバッグすることを目的としてkernel パッケージもインストールすることを強くお勧めします。kernel-bigmemパッケージは、i686アーキテクチャのみに対応して構築されています。

PCMCIAサポートが必要な場合(ノートブック型PCなど)、kernel-pcmcia-csパッケージが必要です。

kernel-sourceパッケージは、カーネルを再コンパイルする場合か、カーネルの開発を行う場合以外は必要ありません。

kernel-docパッケージには、カーネル開発ドキュメントが含まれているので必要ありません。システムがカーネル開発用に使用される場合におすすめします。

kernel-utilパッケージには、カーネルやシステムのハードウェアの制御に使用できるユーティリティが含まれています。必要とされません。

Red Hatは種々のx86バージョンに対応して最適化されたカーネルを構築します。オプションには、AMD Athlon™とAMD Duron™システム用のathlon、Intel® Pentium® II、Intel® Pentium® III、Intel® Pentium® 4 システム用のi686 、及びIntel® Pentium®とAMD K6™システム用のi586があります。使用しているx86システムのバージョンが不明な場合は、i386バージョン用に構築されたカーネルを使用します。このカーネルはすべてのx86ベースシステム用に構築されています。

RPMパッケージのx86バージョンはファイル名に含まれています。たとえば、kernel-2.4.20-2.47.1.athlon.rpm はAMD Athlon™とAMD Duron™システム用に最適化されています。また、kernel-2.4.20-2.47.1.i686.rpm はIntel® Pentium® II、Intel® Pentium® III、Intel® Pentium® 4 システム用に最適化されています。カーネルのアップグレードに必要なパッケージを確定したら、kernel、kernel-smp 、kernel-bigmemの各パッケージに対して適切なアーキテクチャを選択します。その他のパッケージのi386 バージョンを使用します。

30.3. アップグレードされたカーネルのダウンロード

システム用に更新されたカーネルあるか確認するには、いくつかの方法があります。

- http://www.redhat.com/apps/support/errata/にアクセスし、Red Hat Linuxの適切なバージョンを選択してそれのErrataを表示します。カーネルエラータは通常**Security Advisories** のセクションにあります。エラータの一覧から、カーネルエラータをクリックし、詳細なレポートを表示します。エラータレポートには、必要なRPMパッケージの一覧とRed Hat FTPミラーサイトからそれらをダウンロードするためのリンクがあります。RPMパッケージは、Red Hat FTPミラーサイトからダウンロードすることもできます。ミラーサイトの一覧はhttp://www.redhat.com/download/mirror.htmlで見ることができます。
- Red Hat ネットワークを使用してカーネルRPMパッケージをダウンロードし、そのパッケージをインストールします。Red Hat ネットワークはシステム上に最新カーネルのダウンロード、カーネルのアップグレードができ、必要であれば初期RAMディスクイメージを作成します。そして、ブートローダが新規カーネルをブートするよう設定します。詳細については、 http://www.redhat.com/docs/manuals/RHNetwork/で入手できる*Red Hat* ネットワークユーザー参照ガイドをご覧ください。

RPMパッケージをRed Hat Linuxエラータページからダウンロードした場合、または、パッケージをダウンロードするのにRed Hat ネットワークのみを使用した場合は、項30.4へ進んでください。更新されたカーネルをダウンロードしてインストールするのにRed Hat ネットワークを使用した場合は、項30.5または項30.6にある説明に従います。これ以外は、Red Hat ネットワークは自動的にデフォルトのカーネルを最新バージョンに変更するためデフォルトでカーネルをブートするよう変更しないでください。

30.4. アップグレードの実行

必要なカーネルRPMパッケージの準備ができたら、既存のカーネルをアップグレードします。rootとしてログインし、シェルプロンプトでカーネルRPMパッケージの入っているディレクトリに移動し、次のステップに従います。

重要

万一、新規カーネルに問題がある可能性に備えて、古いカーネルを保存しておくことを強くお薦めします。

古いカーネルを保存しておくには、`rpm`で引数`-i`を使います。`kernel` パッケージをアップグレードするためにオプション`-U` を使用すると、現在インストールされているカーネルを上書きしてしまいます(カーネルバージョンとx86バージョンが異なる場合があります)。

```
rpm -ivh kernel-2.4.20-2.47.1.i386.rpm
```

マルチプロセッサシステムの場合、`kernel-smp` パッケージもインストールします(カーネルバージョンとx86バージョンが異なる場合があります)。

```
rpm -ivh kernel-smp-2.4.20-2.47.1.i386.rpm
```

システムがi686ベースであり、4Gバイトを超えるRAMを備えている場合は、i686アーキテクチャ用に構築された`kernel-bigmem` パッケージもインストールします(カーネルバージョンが異なる場合があります)。

```
rpm -ivh kernel-bigmem-2.4.20-2.47.1.i686.rpm
```

kernel-sourceパッケージ、kernel-docsパッケージ、kernel-utilsパッケージなどをアップグレードする場合は、元のバージョンをバックアップしておく必要はないでしょう。次のコマンドを使用してこれらのパッケージをアップグレードします(バージョン番号が異なる場合があります)。

```
rpm -Uvh kernel-source-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-docs-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-utils-2.4.20-2.47.1.i386.rpm
```

PCMCIA(たとえばノートブック型PC)を使用している場合は、kernel-pcmcia-csファイルをインストールし、元のバージョンも保存しておきます。-iスイッチを使用する場合は、元のカーネルがPCMCIAサポートでブートするのにこのパッケージを必要とするため、通常、競合を起こしますこれを避けるには、次のように--forceスイッチを使用します(バージョンが異なる場合があります)。

```
rpm -ivh --force kernel-pcmcia-cs-3.1.24-2.i386.rpm
```

次のステップは初期RAMディスクイメージが作成されていることを確認します。詳細については項30.5を参照してください。

30.5. 初期RAMディスクイメージの確認

ext3ファイルシステムまたはSCSIコントローラを使用している場合は、初期RAMディスクが必要です。初期RAMディスクの目的は、通常はモジュールが常駐するデバイスにカーネルがアクセスする前に、そこからモジュラーカーネルがブートする必要があるモジュールにカーネルがアクセスできるようにすることです。

初期RAMディスクは、mkinitrd コマンドを使用して作成できます。ただし、Red Hat, Inc.提供のRPMパッケージからカーネルと関連パッケージがインストールされているまたはアップグレードされている場合は、このステップは自動的に実行されます。従って、手動で実行する必要はありません。ディスクが作成されたことを確認するには、 ls -l /bootコマンドを使用して initrd-2.4.20-2.47.1.imgファイルが作成されたことを確認します(バージョンはインストールしたカーネルのバージョンに対応しなければなりません)。

次のステップは、ブートローダが新しいカーネルをブートするよう設定されているか確認することです。詳細については、項30.6 を参照してください。

30.6. ブートローダの確認

GRUBまたはLILOのどちらかのブートローダーがインストールされていると、kernel RPMパッケージは新規にインストールされたカーネルをブートするようにGRUBまたはLILO ブートローダーを構成します。しかし、新規のカーネルをデフォルトとしてブートするようにブートローダーを構成するわけではありません。

常に、ブートローダーが正しく構成されていることを確認したほうがよいでしょう。これはたいへん重要なステップです。ブートローダーの構成が正しくない場合、システムをRed Hat Linuxで正常に起動できません。その場合、先に作成しているブートディスクでシステムを起動して、再度ブートローダーを設定し直します。

30.6.1. GRUB

ブートローダーとしてGRUBを選択した場合、 /boot/grub/grub.confファイルが、インストールしたkernelパッケージと同じバージョンのtitleセクションを含んでいることを確認してください(kernel-smpやkernel-bigmemパッケージをインストールした場合にも、このセクションが含まれています)。

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
```

```
#     all kernel and initrd paths are relative to /boot/, eg.
#     root (hd0,0)
#     kernel /vmlinuz-version ro root=/dev/hda2
#     initrd /initrd-version.img
#boot=/dev/hda
default=3
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-2.47.1)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-2.47.1 ro root=LABEL=/
    initrd /initrd-2.4.20-2.47.1.img
title Red Hat Linux (2.4.20-2.30)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-2.30 ro root=LABEL=/
    initrd /initrd-2.4.20-2.30.img
```

別の/bootパーティションを作成すると、カーネルやinitrdイメージへのパスは、/boot パーティションに関連してきます。

デフォルトは新しいカーネルに設定されていないので注意してください。GRUBがデフォルトで新しいカーネルをブートするよう設定するには、default変数の値を新規カーネルを含むタイトルセクションのタイトルセクション番号へ変更します。0からカウントが始まります。例えば、新規カーネルが2番目のタイトルセクションにあれば、defaultを**1**に設定します。

新規カーネルのテストを開始するには、コンピュータを再起動して、ハードウェアが正しく検出されることを確認するためにメッセージをよく見ます。

30.6.2. LILO

ブートローダーとしてLILOを選択した場合、/etc/lilo.confファイルが、インストールしたkernelパッケージと同じバージョンのimageを含んでいることを確認してください(kernel-smpパッケージまたはkernel-bigmemパッケージがインストールされた場合、セクションは同様にそのパッケージ用に存在します)。

```
prompt
timeout=50
default=2.4.20-2.30
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear

image=/boot/vmlinuz-2.4.20-2.47.1
    label=2.4.20-2.47.1
    initrd=/boot/initrd-2.4.20-2.47.1.img
    read-only
    append="root=LABEL=/"

image=/boot/vmlinuz-2.4.20-2.30
    label=2.4.20-2.30
    initrd=/boot/initrd-2.4.20-2.30.img
    read-only
    append="root=LABEL=/"
```

デフォルトは新規カーネルに設定されていないので注意してください。デフォルトで新規カーネルがブートするようにLILOを構成するには、default 変数を新規カーネルのimage セクション内

のlabelの値に設定します。rootとして/sbin/liloコマンドを実行し、変更を有効にします。実行後は次のような出力が表示されます。

```
Added 2.4.20-2.47.1 *
Added linux
```

ここで、2.4.20-2.47.1のあとにある*は、セクションがLILOのブートするデフォルトカーネルだということを表します。

新規カーネルのテストを開始するには、コンピュータを再起動して、ハードウェアが正しく検出されることを確認するためメッセージをよく見ます。

第31章

カーネルモジュール

Linuxカーネルはモジュール形式で設計されています。起動時に、最小限度の常駐カーネルだけがメモリにロードされます。したがって、ユーザーが常駐カーネルに存在しない機能を要求すると、時々ドライバと呼ばれる、カーネルモジュール、が動的にメモリにロードされます。

インストール中、システムのハードウェアはプローブされます。この調査とユーザーからの情報を基にして、インストールプログラムはブート時にロードする必要があるモジュールを決定します。インストールプログラムは透過的に動的ロードメカニズムが機能するようにセットアップします。

インストール後に、カーネルモジュールを必要とするハードウェアを新しく追加する場合は、新しいハードウェア用のカーネルモジュールがロードされるようシステムを設定する必要があります。新しいハードウェアを装着してブートすると、**Kudzu** プログラムが作動して対応するハードウェアであるか検出し、そのハードウェア用にモジュールを設定します。また、モジュールは、モジュール設定ファイル、`/etc/modules.conf` を編集して手動で指定することもできます。

注意

X Window Systemのインターフェースを表示するのに使用されるビデオカードモジュールは`XFree86`パッケージの一部であり、カーネルではありません。したがって、この章は適用しません。

例えば、システムがSMC EtherPower 10 PCI ネットワークアダプタを装着する場合、モジュールの設定ファイルには次の行があります。

```
alias eth0 tulip
```

2枚目のネットワークカードがシステムに追加され1枚目のカードと同一である場合、`/etc/modules.conf`に次の行を付け加えます。

```
alias eth1 tulip
```

カーネルモジュールとモジュールでサポートされるハードウェアのアルファベット順一覧は、*Red Hat Linux* 参照ガイドでご覧ください。

31.1. カーネルモジュールのユーティリティ

`modutils`パッケージがインストールされる場合、カーネルモジュールを管理するための一連のコマンドが利用できます。モジュールが正常にロードされているか確認したり、新しいハードウェア用に別のモジュールを試すとき、これらのコマンドを使用します。

コマンドの`/sbin/lsmod`は現在、ロードされているモジュールを表示します。例えば、

```
Module        Size Used by  Not tainted
iptable_filter    2412  0 (autoclean) (unused)
ip_tables      15864  1 [iptable_filter]
nfs         84632  1 (autoclean)
lockd        59536  1 (autoclean) [nfs]
sunrpc       87452  1 (autoclean) [nfs lockd]
soundcore       7044  0 (autoclean)
ide-cd       35836  0 (autoclean)
cdrom        34144  0 (autoclean) [ide-cd]
parport_pc      19204  1 (autoclean)
```

```
lp          9188  0 (autoclean)
parport       39072  1 (autoclean) [parport_pc lp]
autofs       13692  0 (autoclean) (unused)
e100         62148  1
microcode      5184  0 (autoclean)
keybdev       2976  0 (unused)
mousedev       5656  1
hid         22308  0 (unused)
input         6208  0 [keybdev mousedev hid]
usb-uhci      27468  0 (unused)
usbcore       82752  1 [hid usb-uhci]
ext3         91464  2
jbd         56336  2 [ext3]
```

各行は、最初のコラムがモジュールの名前、2番目のコラムがモジュールのサイズ、3番目のコラムが使用回数です。

使用回数の後の情報はモジュールごとに少しづつ異なります。モジュールの行に(unused) が表示された場合は、そのモジュールは現在使用されていません。モジュールの行に(autoclean)と表示された場合は、そのモジュールはrmmod -a コマンドでオートクリーンすることができます。このコマンドを実行すると、autocleanが付いたモジュール、前回のautoclean作動から使用されていないモジュールのすべてがアンロードされます。デフォルトでは、Red Hat Linux はこのオートクリーン実行を行ないません。

モジュール名が行末のカッコ内に表示された場合、カッコ内のそのモジュールは、その行の最初のコラムに表示されているモジュールに依存します。例えば、次の行で、

```
usbcore       82752  1 [hid usb-uhci]
```

hid とusb-uhci のカーネルモジュールはusbcore モジュールに依存します。

/sbin/lsmodの出力は/proc/modules表示からの出力と同じです。

カーネルモジュールをロードするには、 /sbin/modprobeコマンドを入力し、その後にカーネルモジュール名を続けます。デフォルトでは、modprobeで /lib/modules/<*kernel-version*>/kernel/drivers/ サブディレクトリからモジュールのロードが行なわれます。ネットワークインターフェースドライバ用のnet/サブディレクトリなどのように、各タイプのモジュールにサブディレクトリがあります。カーネルモジュールのなかには、別のモジュールに依存するものがあります。つまり、このようなモジュールがロードするために他のモジュールがさきにロードされなければならないということです。/sbin/modprobe コマンドはこれらの依存関係を確認し、指定されたモジュールをロードする前にモジュールの依存関係をロードします。

たとえば、以下のコマンドを入力したとします。

```
/sbin/modprobe hid
```

すべてのモジュール依存関係をロードし、それからhidモジュールをロードします。

/sbin/modprobeが実行するすべてのコマンドをスクリーンに表示するには、-vオプションを使用します。例えば、

```
/sbin/modprobe -v hid
```

次と似たような出力が表示されます。

```
/sbin/insmod /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Using /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'
```

/sbin/insmodコマンドもカーネルモジュールをロードするため存在しますがこれは依存関係を解決しません。したがって、/sbin/modprobeコマンドを使用することをおすすめします。

カーネルモジュールをアンロードするには、/sbin/rmmodコマンドを使用してその後にモジュール名を続けます。rmmodユーティリティは使用されていないモジュールと、使用中の他のモジュールが依存しないモジュールのみをアンロードします。

たとえば、以下のコマンドを入力したとします。

```
/sbin/rmmod hid
```

hidカーネルモジュールをアンロードします。

もう1つの便利なカーネルモジュールユーティリティはmodinfoです。/sbin/modinfo コマンドを使用して、カーネルモジュールに関する情報を表示できます。一般的なシンタックスは次のようになります。

```
/sbin/modinfo [options] <module>
```

オプションとして、モジュールの簡単な説明を表示する-dと、モジュールがサポートするパラメータを一覧表示する-pがあります。オプションの完全な一覧については、modinfo のman ページ(man modinfo)を参照してください。

31.2. その他のリソース

カーネルモジュールとそのユーティリティの詳細については、以下の資料を参照してください。

31.2.1. インストールされているドキュメント

- lsmod manページ—その出力の記述と説明
- insmod manページ—コマンドラインオプションの記述と一覧
- modprobe manページ—コマンドラインオプションの記述と一覧
- rmmod manページ—コマンドラインオプションの記述と一覧
- modinfo manページ—コマンドラインオプションの記述と一覧
- /usr/src/linux-2.4/Documentation/modules.txt —カーネルモジュールのコンパイルと使用の方法

31.2.2. 役に立つウェブサイト

- http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html — Linuxドキュメントプロジェクトからの*Linux Loadable Kernel Module HOWTO*

V. パッケージの管理

Red Hat Linuxシステム上のすべてのソフトウェアは、インストール、アップグレード、除去ができるRPMパッケージに別けられます。このパートでは、グラフィカルツールとコマンドラインツールを使用してRed Hat Linuxシステム上でのRPMパッケージの管理方法を説明します。

目次

redhat.

第32章

RPMによるパッケージ管理

Red Hat Package Manager(RPM)は、誰もが利用できるオープンパッケージングシステムで、Red Hat Linuxだけでなく他のLinuxやUNIXシステム上でも動作します。Red Hat, Inc.では、他のベンダーにもRPM を自社製品に使用するよう奨励しています。RPM はGPL契約に基づいて配布されます。

エンドユーザーはRPMによりシステムを簡単に更新することができます。RPM パッケージのインストール、アンインストール、アップグレードは短いコマンドで実行できます。RPM はインストールされているパッケージやそのファイル群に関するデータベースを維持しているので、システムで強力な問い合わせ/ 検証を実行することができます。グラフィカルインターフェイスで使用したい場合は、**パッケージ管理ツール** を使用して多くのRPM コマンドを実行することができます。詳細は第33章を参照してください。

アップグレード時に、RPM は設定ファイルを慎重に処理するためカスタマイズ情報が失われることはありません— 普通の`.tar.gz`ファイルなどを使用した場合は、このような機能を実現することができません。

開発者は、RPM を使用することにより、ソフトウェアのソースコードを取り出し、エンドユーザー用にソースとバイナリパッケージにパッケージ化することができます。このプロセスは極めて単純で、ひとつのファイルと作成するオプションのパッチから操作することができます。ソフトウェアの新しいバージョンがリリースされた場合でも、この「純粋な」ソースを明確に記述したファイル、パッチ、ビルド命令を使用することで容易にパッケージを保守することができます。

注意

RPM はシステムに変更を加えるため、RPM パッケージのインストール、削除、アップグレードはrootで実行します。

32.1. RPM の設計目標

RPM の使用方法を理解するために、RPM の設計目標を理解するとわかりやすいでしょう。

アップグレードの可能性

‘ RPM を使用すれば、コンポーネントを完全に再インストールすることなく、個別にコンポーネントをアップグレードすることができます。RPM に基づくオペレーティングシステム(Red Hat Linuxなど)の新しいバージョンを入手したときに、マシンに再インストールする必要がありません(他のパッケージングシステムに基づくオペレーティングシステムの場合はその必要があります)。RPM を使用すれば、賢く、完全に自動化された、適切なシステムのアップグレードを行うことができます。パッケージに含まれる設定ファイルはアップグレード後にも保持されるので、カスタマイズ情報が失われることはありません。システムへのパッケージのインストールとアップグレードでは同じRPM ファイルが使用されるため、パッケージをアップグレードするために特別なアップグレードファイルが必要になることはありません。

強力な問い合わせ

‘ RPM では、強力な問い合わせオプションが提供されています。データベース全体を通じてパッケージを検索したり、特定のファイル群のみを検索したりすることができます。あるファイルがどのパッケージに属し、パッケージがどこから来たのかをも簡単に検索することができます。RPM パッケージに含まれるファイルは圧縮アーカイブ形式であり、パッケージとその内容に関する有用な情報を含むカスタムバイナリヘッダーが付いているため、個別のパッケージをすばやく簡単に問い合わせすることができます。

システムの検証

‘ もう1つの強力な特徴は、パッケージの検証が可能であるということです。パッケージに関する重要ファイルを削除してしまったのではないかと心配になった場合には、パッケージを検証すればよいのです。何か矛盾があれば通知されます。その時点で必要であればそのパッケージを再インストールすることができます。再インストールを行っても、修正した設定ファイルは保持されます。

純粋なソース

‘ 最終的な設計目標は、ソフトウェアのオリジナル作者によって配布されたときのままの「純粋な」ソフトウェアソースをユーザーが利用できるようにすることでした。RPM を使用した場合、純粋なソースと適用済みのパッチ、完全なビルド命令群が入手できます。いくつかの理由から、これは大きなメリットとなります。たとえば、あるプログラムの新しいバージョンがリリースされた場合、それをコンパイルするために必ずしも最初から作業を始める必要はなくなります。パッチを見て、必要になるかもしれない作業を確かめることができます。この技術を使えば、組み込み済みのすべてのデフォルト設定と、ソフトウェアを適切に構築するために行われたすべての変更内容が、容易に目に見えるようになります。

ソースを純粋な状態に保持するという目標は、開発者にとってのみ重要なことのように思われるかもしれませんが、結果として、エンドユーザーにより高品質のソフトウェアが提供されることにもなります。純粋なソースのコンセプトを最初に考え出したBOGUSディストリビューションの皆様に感謝の意を表したいと思います。

32.2. RPMの使用法

RPM には、次の5つの基本的作動モードがあります(パッケージの構築はカウントしません)。インストール、アンインストール、アップグレード、照会、検証の5つです。このセクションでは、各モードの概要を説明します。詳細な説明やオプションについては`rpm --help`をご覧ください。RPM の詳細については項32.5を参照してください。

32.2.1. RPM パッケージの検索

RPM を使用する前に、それがどこにあるかを調べる必要があります。インターネットを検索すると数多くのRPM リポジトリが見つかりますが、Red Hat製のRPM パッケージは以下の場所にあります。

- Red Hat Linux CD-ROM
- Red HatのErrataページhttp://www.redhat.com/apps/support/errata/
- Red HatのFTPミラーサイトhttp://www.redhat.com/download/mirror.html
- Red Hat ネットワーク— Red Hat ネットワークの詳細については、第34章を参照してください。

32.2.2. インストール

RPM パッケージには概して`foo-1.0-1.i386.rpm` というようなファイル名が付けられています。このファイル名は、パッケージ名(`foo`)、バージョン(`1.0`)、リリース(`1`)、アーキテクチャ(`i386`)で構成されています。パッケージのインストールは、rootでログインするのと同様に簡単です。シェルプロンプトで以下のようにコマンドを入力します。

```
rpm -Uvh foo-1.0-1.i386.rpm
```

インストールが正常に進行すると、以下のような表示がでます。

```
Preparing...        ########################################### [100%]
```

```
 1:foo         ########################################### [100%]
```

RPMはパッケージ名を出力し、パッケージのインストール状況をシャープ記号を使って表示します。

RPMバージョン4.1から始まったことですが、パッケージの署名はパッケージのインストール時やアップグレード時にチェックされます。署名の検証が失敗に終れば、次のようなエラーが表示されます。

```
error: V3 DSA signature: BAD, key ID 0352860f
```

ヘッダのみの新しい署名なら、次のようなエラーメッセージが表示されます。

```
error: Header V3 DSA signature: BAD, key ID 0352860f
```

署名を検証するための適切なキーを持っていない場合は、メッセージは以下のような`NOKEY` を含みます。

```
warning: V3 DSA signature: NOKEY, key ID 0352860f
```

パッケージ署名のチェックに関する詳細情報は、項32.3で参照してください。

注意

カーネルパッケージをインストールしている場合は、代わりに`rpm -ivh`を使用する必要があります。詳細は第30章を参照してください。

パッケージのインストールは簡単にできるように設計されています。しかし、時にはエラーが出る可能性は否定できません。

32.2.2.1. すでにインストールされているパッケージ

同じバージョンのパッケージがすでにインストールされている場合は、以下のメッセージが表示されます。

```
Preparing...         ########################################### [100%]
package foo-1.0-1 is already installed
```

どうしてもパッケージをインストールする必要があり、それがインストールされているものと同じバージョンである場合は、`--replacepkgs`オプションを使用することができます。このオプションは、RPMに対しエラーを無視するよう指示するものです。

```
rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
```

このオプションは、RPM からインストールされたファイルが削除された場合や、RPM からオリジナルの設定ファイルをインストールしたい場合に便利です。

32.2.2.2. ファイルの競合

別のパッケージや同じパッケージの古いバージョンによってインストールされたファイルを含むパッケージをインストールしようとすると、以下のメッセージが表示されます。

```
Preparing...         ########################################### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package bar-2.0.20
```

RPM にこのエラーを無視するよう指示するには、`--replacefiles`オプションを使用します。

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

32.2.2.3. 未解決の依存

RPM パッケージは他のパッケージに「依存する」ことがあります。つまり、正しく動作するために他のパッケージのインストールが必要な場合があります。未解決の依存関係を持つパッケージをインストールしようとすると、以下のメッセージが表示されます。

```
Preparing...        ########################################### [100%]
error: Failed dependencies:
    bar.so.2 is needed by foo-1.0-1
  Suggested resolutions:
    bar-2.0.20-3.i386.rpm
```

Red Hat LinuxのCDセットからインストールしている場合は、通常、依存関係を解決するパッケージを提案してきます。このパッケージをRed Hat Linux CD-ROMから、または、Red Hat FTPサイト(またはミラー)から見つけて、それを次のようにコマンドに追加します。

```
rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
```

両方のパッケージのインストールが正常に行なわれると、以下の表示がでます。

```
Preparing...        ########################################### [100%]
   1:foo         ########################################### [ 50%]
   2:bar         ########################################### [100%]
```

もし、プログラムが依存関係を解消するパッケージを提案してこない場合は、`--redhatprovides`オプションを試して、どのパッケージが必要なファイルを含んでいるか判定します。このオプションを実行するには、`rpmdb-redhat` パッケージをインストールしている必要があります。

```
rpm -q --redhatprovides bar.so.2
```

`bar.so.2`を含むパッケージが`rpmdb-redhat`パッケージのインストール済みデータベースにある場合、そのパッケージ名が表示されます。

```
bar-2.0.20-3.i386.rpm
```

とにかくインストールをそのまま強制したい場合(恐らくパッケージは正常に作動しないので良くない方法)、`--nodeps`オプションを使用します。

32.2.3. アンインストール

パッケージのアンインストールは、インストールと同様、簡単に実行できます。シェルプロンプトで以下のコマンドを入力します。

```
rpm -e foo
```

注意

アンインストールするため先のコマンドで使用したのは、パッケージの名前である`foo`であって、オリジナルパッケージのファイル名、 `foo-1.0-1.i386.rpm`ではないことに注意してください。パッケージをアンインストールするには、`foo`の部分を実際のオリジナルパッケージのパッケージ名に置き換える必要があります。

削除しようとしているパッケージに別のインストールされているパッケージが依存している場合、アンインストール時に依存関係エラーが発生することがあります。たとえば、

```
Preparing...        ########################################### [100%]
error: removing these packages would break dependencies:
    foo is needed by bar-2.0.20-3.i386.rpm
```

RPM にこのエラーを無視させ、強制的にパッケージをアンインストールするには、(おそらく依存しているパッケージが正しく動作しなくなるのであまりお勧めできません)、--nodepsオプションを使用します。

32.2.4. アップグレード

パッケージのアップグレードはインストールと似ています。シェルプロンプトで以下のコマンドを入力します。

```
rpm -Uvh foo-2.0-1.i386.rpm
```

上記の内容には示されていませんが、古いバージョンのfooパッケージもすべてRPM により自動的にアンインストールされました。実際には、常に-Uを使用してパッケージをインストールすれば、古いバージョンのパッケージがインストールされていなくても正しく動作するため、その方が好ましいかもしれません。

RPM は設定ファイルを使用したパッケージのインテリジェントなアップグレードを行うので、以下のようなメッセージが表示されることもあります。

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

このメッセージは、設定ファイルに加えられた変更内容が、パッケージ内の新しい設定ファイルと「上位互換性」を持たない可能性があるため、RPM が元のファイルを保存してから新しいファイルをインストールしたことを意味しています。できる限り早期に2つのファイル間の違いを調査し、解決することで、引き続きシステムが正しく動作することを確認してください。

アップグレードは、実際にはアンインストールとインストールを組み合わせた作業になります。このため、RPM がアップグレードを実行している間、両方行のエラーが発生する可能性があります。そしてもう1つ別のエラーが発生します。RPM が古いバージョン番号のパッケージへアップグレードが行われようとしていると判断すると、以下のようなメッセージが表示されます。

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

RPM に「アップグレード」を強行させるには、--oldpackageオプションを使用します。

```
rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
```

32.2.5. freshenの実行

パッケージへのfreshenの実行はアップグレードと似ています。シェルプロンプトで以下のコマンドを入力します。

```
rpm -Fvh foo-1.2-1.i386.rpm
```

RPM のfreshenオプションにより、コマンドラインで指定されたパッケージのバージョンと、すでにシステムにインストールされているパッケージのバージョンが照合されます。インストールされているパッケージよりも新しいバージョンのパッケージに対してRPM のfreshen オプションが実行される

と、そのパッケージは新しいバージョンへアップグレードされます。ただし、同じ名前でインストールされているパッケージが存在しない場合は、RPM のfreshenオプションによるパッケージのインストールは実行されません。この点が、RPM のアップグレードオプションと異なります。アップグレードでは、古いバージョンのパッケージがインストールされているかどうかに関係なくパッケージが必ず インストールされます。

RPM のfreshenオプションは、単一のパッケージに対しても複数のパッケージに対しても使用できます。これは、多数のパッケージをダウンロードした後で、システムにインストールされているパッケージのみをアップグレードしたい場合に、freshenを実行します。freshenを使用する場合、RPMの使用前にダウンロードした複数のパッケージの中から不要なパッケージを削除する必要はありません。

この場合、以下のコマンドを発行することができます。

```
rpm -Fvh *.rpm
```

RPMはすでにインストールされているパッケージのみ自動的にアップグレードします。

32.2.6. queryの実行

インストール済みパッケージのデータベースに対するqueryを行うには、`rpm -q`コマンドを使用します。`rpm -q foo`コマンドは、インストール済みパッケージfooのパッケージ名、バージョン、リリース番号を出力します。

```
foo-2.0-1
```

注意

パッケージの名前 `foo`が使用されていることに注意してください。パッケージについてqueryを行うには、`foo` の部分を実際のパッケージ名に置き換える必要があります。

パッケージ名を指定する代わりに、`-q` コマンドに以下のオプションを使用してqueryを行うパッケージ(群)を指定することができます。これらのオプションをパッケージ指定オプションと呼びます。

- `-a`コマンドは、現時点でインストールされているすべてのパッケージについてqueryを実行します。
- `-f` <*`file`*>は、<*`file`*> が含まれるパッケージについてqueryを実行します。ファイルを指定するときは、そのファイルのフルパスを指定する必要があります(例、 `/usr/bin/ls`)。
- `-p` <*`packagefile`*> は、<*`packagefile`*> パッケージについてqueryを実行します。

queryを行なったパッケージに関して表示する情報を指定する方法がたくさんあります。検索を行う情報のタイプを選択するには、以下のオプションを使用します。これらのオプションを情報選択オプションと呼びます。

- `-i`コマンドは、パッケージ名、説明、リリース、サイズ、構築日、インストール日、ベンダーなど多様なパッケージ情報を表示します。
- `-l`コマンドは、パッケージに含まれるファイルの一覧を表示します。
- `-s`コマンドは、パッケージに含まれるすべてのファイルの状態を表示します。
- `-d`コマンドは、ドキュメント(manページ、infoページ、READMEなど)としてマークが付けられたファイルの一覧を表示します。

- `-c`は、設定ファイルとしてマークが付けられたファイルの一覧を表示します。これは、パッケージをシステムに適合させるために、ユーザーがインストール後に変更を加えるファイルです(例、`sendmail.cf`、`passwd`、`inittab` など)。

ファイルの一覧を表示するオプションについては、コマンドに`-v`を追加して、その一覧を使い慣れた`ls -l`形式で表示させることができます。

32.2.7. 検証

パッケージの検証では、パッケージからインストールされたファイルに関する情報と、元のパッケージに含まれるファイルに関する情報が同一かどうか調べます。検証により、各ファイルのサイズ、MD5チェックサム、権限、タイプ、所有者、グループを始め、さまざまなことが比較されます。

コマンド`rpm -V`は、パッケージの検証を行います。queryの説明で示したパッケージ選択オプションを使用して、検証したいパッケージを指定することができます。簡単な使用法としては`rpm -V foo`というものがあります。これを実行すると、パッケージfooに含まれるすべてのファイルが、それがインストールされたときの状態と同じであるかどうかが検証されます。例えば、

- 特定のファイルを含むパッケージを検証するには、
  `rpm -Vf /bin/vi`
- インストールされているすべてのパッケージを検証するには、
  `rpm -Va`
- インストールされているパッケージと、RPMパッケージファイルとを検証するには、
  `rpm -Vp foo-1.0-1.i386.rpm`

  RPMデータベースが破損した疑いがある場合に、このコマンドが役立ちます。

すべてが正常に検証された場合は何も出力されません。何らかの矛盾が見つかった場合はその内容が表示されます。出力フォーマットは、8個の文字列(`c` は設定ファイルを示す)とファイル名です。8個の各文字は、ファイルの1つの属性とRPMデータベースに記録されたその属性の値とを比較した結果を示します。`.`(ピリオド)がひとつは、テストに合格したことを示します。以下の文字はそれぞれ何らかのテストで不合格になったことを示しています。

- `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` —ファイル修正時刻
- `D` —デバイス
- `U` —ユーザー
- `G` —グループ
- `M` —モード(権限とファイルタイプを含む)
- `?` —読み込み不可ファイル

何らかが出力された場合は、パッケージを削除するのか、再インストールするのか、あるいは別の方法で問題を修正するのかを熟慮の上判断してください。

32.3. パッケージの署名のチェック

パッケージが破損したり不正に変更されたりしていないことを検査する場合、シェルプロンプトで以下のコマンドを入力してmd5sumを調べます(<*rpm-file*> の部分を実際の**RPM** パッケージのファイル名に置き換えてください)。

```
rpm -K --nogpg <rpm-file>
```

<*rpm-file*>: md5 OKと言うメッセージが表示されます。この短いメッセージはダウンロードによるメッセージの破損はないことを意味しています。詳細メッセージを表示するには、コマンド内の-Kを-Kvvに置き換えます。

一方、パッケージを作成した開発者はどの程度に信用できるでしょうか。パッケージが開発者の **GnuPG** キーで署名されていれば、開発者が誰なのか判断できます。

RPM パッケージはGnu Privacy Guard (GnuPG)を使用して署名を入れることができ、これによりユーザーはダウンロードしたパッケージが信頼できるものであることを確認するのに役立ちます。

GnuPG は安全な通信のためのツールで、PGPの暗号化技術である電子プライバシー保護プログラムを完全に無償で置き換えたものです。GnuPGを使用して、ドキュメントの正当性を認証し、他の受信者との間で送受信するデータを暗号化/解読することができます。GnuPG は、PGP 5.*x*のファイルについても同様に解読、認証を行うことが可能です。

Red Hat Linuxのインストール時に、GnuPG がデフォルトでインストールされます。このため、Red Hatから入手したパッケージの検査をGnuPG を使用してすぐに始めることができます。最初に、Red Hatの公開キーをインポートする必要があります。

32.3.1. キーのインポート

Red Hatパッケージを検証するには、Red Hat GPGキーをインポートする必要があります。これを実行するには、シェルプロンプトで次のコマンドを実行します。

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

RPM検証用にインストールされたすべてのキーの一覧を表示するには、次のコマンドを実行します。

```
rpm -qa gpg-pubkey*
```

Red Hatキー用には、出力が次を含んでいます。

```
gpg-pubkey-db42a60e-37ea5438
```

特定のキーの詳細を表示するには、rpm -qi コマンドの後に、先程のコマンドの出力を付けます。

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

32.3.2. パッケージ署名の検証

構築者のGnuPGキーをインポートした後で、RPMファイルのGnuPG署名をチェックするには、次のコマンドを使用します(<*rpm-file*>を実際のRPMパッケージのファイル名に置き換えます)。

```
rpm -K <rpm-file>
```

すべて問題がなければ、md5 gpg OK のメッセージが表示されます。これは、パッケージの署名が検証され、破損もしていないという意味です。


ヒント

GnuPGについての詳細情報は、付録Bをご覧ください。

32.4. RPMで友人を感心させよう

RPMはシステムの管理や問題の診断及び修正に役に立つツールです。これらのすべてのオプションを理解する最善の方法はいくつかの例を見ることでしょう。

- 誤って何らかのファイルを削除してしまったものの、何を削除したかがわからないとします。システム全体を検証して足りないものを調べたい場合は、以下のコマンドを試すことができます。
  ```
  rpm -Va
  ```
  足りないファイルがあるか、壊れているファイルがあるように見える場合は、おそらくパッケージを再インストールするか、いったんアンインストールして再インストールする必要があります。
- 所属先のわからないファイルを見つけたとします。そのファイルが含まれるパッケージを検索するには、以下のように入力します。
  ```
  rpm -qf /usr/X11R6/bin/ghostview
  ```
  出力は以下のようになります。
  ```
  gv-3.5.8-22
  ```
- 上記2つの例を組み合わせて、次のような方法を考えることができます。`/usr/bin/paste` に問題があるとします。このプログラムが含まれるパッケージを検証しようにも、`paste` がどのパッケージに含まれるかがわかりません。単純に次のコマンドを入力します。
  ```
  rpm -Vf /usr/bin/paste
  ```
  該当するパッケージが検証されます。
- 特定のプログラムに関して詳細な情報が必要なら、次のコマンドを入力して、そのプログラムの入ったパッケージに付随するドキュメントを検索することができます。
  ```
  rpm -qdf /usr/bin/free
  ```
  出力は以下のようになります。
  ```
  /usr/share/doc/procps-2.0.11/BUGS
  /usr/share/doc/procps-2.0.11/NEWS
  /usr/share/doc/procps-2.0.11/TODO
  /usr/share/man/man1/free.1.gz
  /usr/share/man/man1/oldps.1.gz
  /usr/share/man/man1/pgrep.1.gz
  /usr/share/man/man1/pkill.1.gz
  /usr/share/man/man1/ps.1.gz
  /usr/share/man/man1/skill.1.gz
  /usr/share/man/man1/snice.1.gz
  /usr/share/man/man1/tload.1.gz
  /usr/share/man/man1/top.1.gz
  /usr/share/man/man1/uptime.1.gz
  /usr/share/man/man1/w.1.gz
  /usr/share/man/man1/watch.1.gz
  /usr/share/man/man5/sysctl.conf.5.gz
  /usr/share/man/man8/sysctl.8.gz
  /usr/share/man/man8/vmstat.8.gz
  ```
- 新しい**RPM**パッケージが見つかったものの、それが何であるかがわからないとします。それに関する情報を検索するには、以下のコマンドを使用します。
  ```
  rpm -qip crontabs-1.10-5.noarch.rpm
  ```
  出力は以下のようになります。

```
Name    : crontabs          Relocations: (not relocateable)
Version : 1.10                Vendor: Red Hat, Inc.
Release : 5               Build Date: Fri 07 Feb 2003 04:07:32 PM EST
Install date: (not installed)       Build Host: porky.devel.redhat.com
Group   : System Environment/Base    Source RPM: crontabs-1.10-5.src.rpm
Size    : 1004              License: Public Domain
Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : Root crontab files used to schedule the execution of programs.
Description :
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

- RPMがインストールするcrontabs ファイルがどのようなものか見てみましょう。次のように入力します。

```
rpm -qlp crontabs-1.10-5.noarch.rpm
```

出力は以下のようになります。

```
Name    : crontabs          Relocations: (not relocateable)
Version : 1.10                Vendor: Red Hat, Inc.
Release : 5               Build Date: Fri 07 Feb 2003 04:07:32 PM EST
Install date: (not installed)       Build Host: porky.devel.redhat.com
Group   : System Environment/Base    Source RPM: crontabs-1.10-5.src.rpm
Size    : 1004              License: Public Domain
Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : Root crontab files used to schedule the execution of programs.
Description :
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

以上がいくつかの例です。使用するにつれて、たくさんのRPM の用途がわかってきます。

32.5. その他のリソース

RPM は、パッケージのquery、インストール、アップグレード、削除を実行するためのたくさんのオプションや方法がある非常に複雑なユーティリティです。RPM の詳細については、以下のリソースを参照してください。

32.5.1. インストールされているドキュメント

- rpm --help — このコマンドを実行すると、RPM のパラメータのクイックリファレンスが表示されます。
- man rpm — RPM のmanページでは、rpm --help コマンドよりも詳細なRPMのパラメータに関する情報が提供されています。

32.5.2. 役に立つWebサイト

- http://www.rpm.org/ —RPMのWebページ
- http://www.redhat.com/mailing-lists/rpm-list/ — RPMのメーリングリストがここにアーカイブされています。講読するには、件名の欄に`subscribe`という単語を記入してメールを`<rpm-list-request@redhat.com>` 宛に送信します。

32.5.3. 関連書籍

- *Maximum RPM*(Ed Bailey著、Red Hat Press) — この書籍(残念ながら日本語版はまだ発売されていません)のオンラインバージョンが http://www.rpm.org/と http://www.redhat.com/docs/books/ で入手できます。

第33章

パッケージ管理ツール

インストール中に、ユーザーは**ワークステーション**や**サーバ**などのインストールタイプを選択します。ソフトウェアパッケージはこの選択を基にしてインストールされます。使用者によりコンピュータはいろいろな方法で使用されますので、ユーザーはインストール後に、パッケージをインストール、または、削除したくなる場合があります。**パッケージ管理ツール**を使用すると、こうした操作をすることができます。

パッケージ管理ツールを実行するにはX Window Systemが必要となります。アプリケーションをスタートするには、(パネル上の)**メインメニュー** => **システム設定** => **アプリケーションの追加と削除**と進みます。または、シェルプロンプトで`redhat-config- packages`とコマンドを入力します。

コンピュータにRed Hat Linux CD-ROM #1 を挿入すると、同じインターフェースが表示されます。

図33-1. パッケージ管理ツール

このアプリケーションのインターフェースは、インストール中に使用したインターフェースに似ています。パッケージはパッケージグループに分かれており、共通の機能を共有できる標準パッケージと 追加パッケージを収納しています。例えば、**グラフィカルインターネット** グループには、Web ブラウザ、電子メールクライアント、その他インターネット接続で使用されるグラフィカルプログラムが入っています。標準パッケージは、グループ全体が削除されない限り、削除の対象として選択できません。追加パッケージは、グループが選択されている限り、インストールまたは削除の選択ができるオプションパッケージです。

メインウィンドウはパッケージグループの一覧を表示します。パッケージグループの横にあるチェックボックスにチェックマークがある場合は、そのグループのパッケージは現在インストールされています。グループの個々のパッケージ一覧を表示するには、横にある**詳細** ボタンをクリックします。横にチェックマークがあるそれぞれのパッケージは現在インストールされています。

33.1. パッケージのインストール

現在インストールされていないパッケージグループの中の標準パッケージをインストールするには、パッケージの横にあるチェックボックスにチェックを入れます。そのグループ内でインストールされるパッケージをカスタマイズするには、横にある**詳細**ボタンをクリックします。図33-2で示すように標準グループと追加グループの一覧が表示されます。パッケージ名をクリックすると、ウィンドウの下部にパッケージインストールに必要なディスク容量が表示されます。パッケージ名の横にあるチェックボックスにチェックを入れると、インストールとしてマークされます。

また、**詳細**ボタンをクリックして、まだインストールされていない追加パッケージのどれかをチェックすることにより、インストール済のパッケージグループから個々のパッケージを選択することができます。

図33-2. 個々のパッケージ選択

インストールするパッケージグループと個々のパッケージを選択したら、メインウィンドウの**更新**ボタンをクリックします。アプリケーションはここで、パッケージのインストールに必要なディスク容量やパッケージ依存関係を算出して概要を表示します。パッケージ依存関係がある場合は、インストールするパッケージ一覧の中へ自動的に追加します。**詳細を表示**ボタンをクリックしてインストールされるパッケージの完全一覧を表示します。

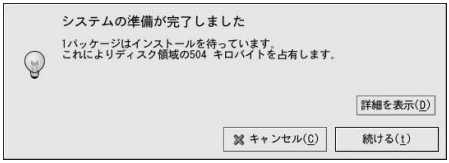


図33-3. パッケージインストールの概要

続行をクリックして、インストールプロセスを開始します。終了すると、**更新完了**のメッセージが表示されます。

ヒント

コンピュータでファイルやディレクトリをブラウズするのに**Nautilus**を使用する場合、それを使用してパッケージをインストールすることもできます。**Nautilus**で、RPMパッケージ(通常、`.rpm`でファイル名が終る

ファイル) があるディレクトリへ移動して、RPMアイコンをダブルクリックします。

33.2. パッケージの削除

パッケージグループ内のインストール済みの全パッケージを削除するには、その横にあるチェックボックスのチェックを外します。個々のパッケージを削除するには、パッケージグループの横にある**詳細**ボタンをクリックして、個々のパッケージからチェックを外します。

削除するパッケージを選択したら、メインウィンドウの**更新**ボタンをクリックします。アプリケーションは、解放されるディスク容量とソフトウェアパッケージ依存関係を算出します。他のパッケージが削除の選択をしたパッケージに依存している場合、それらも削除するパッケージの一覧に自動的に追加されます。**詳細を表示**ボタンをクリックして削除されるパッケージの一覧を表示します。

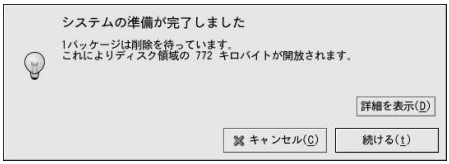


図33-4. パッケージ削除の概要

続行をクリックして削除のプロセスを開始します。終了すると、**更新完了**のメッセージが表示されます。

ヒント

インストールする/削除する、パッケージグループ/パッケージなどをまとめて選択して、**更新**ボタンをクリックすることにより、インストールと削除の作業を合わせて行なうことができます。**システムの準備完了**ウィンドウがインストールするパッケージと削除されるパッケージの数を表示します。

第34章

Red Hat ネットワーク

Red Hat ネットワークは単独、又は複数のRed Hat Linuxシステムを管理する為のインターネットソリューションです。セキュリティに関する通知、バグ修正に関する通知、追加機能に関する通知(Errata情報と総称)はすべて、スタンドアロンのアプリケーション**Red Hat 更新エージェント**を使用してRed Hatから直接ダウンロードするか、またはRHN Webサイト； http://rhn.redhat.com/からダウンロードすることができます。

図34-1. ユーザーの為のRHN

Red Hat ネットワークを利用すると、ユーザーは更新パッケージがリリースされた時に電子メールの連絡を受けますので時間の節約となります。最新のパッケージに関する情報やセキュリティに関する情報を求めてWebを検索する必要もなくなります。デフォルトでは、Red Hat ネットワークによってパッケージもインストールされます。ユーザーはRPM の使用方法を理解する必要もなく、ソフトウェアパッケージの依存関係の解決を気にする必要もありません。RHNがすべての作業を実行します。

各Red Hat ネットワークアカウントに付属しているものは、次のとおりです：

- Errata 通知— ネットワークにあるすべてのシステムに関するセキュリティに関する情報、バグフィックスに関する情報、追加機能に関する情報を基本インターフェイスを通じて知ることが出来ます。

図34-2. 適切なErrata

- 電子メールの自動通知— ユーザーのシステムに関するErrata 情報が発行されると、自動的に電子メールの通知を受け取ります。
- スケジュール設定のErrata更新— Errata更新の配信をスケジュールできます。
- パッケージインストール— ボタンをクリックするだけで、1つ、又は複数のシステムに対するパッケージのインストールのスケジュールを設定できます。
- **Red Hat 更新エージェント** — **Red Hat 更新エージェント**を使用すると、パッケージインストールのオプション付でユーザーのシステム用に最新のソフトウェアパッケージをダウンロードできます。
- Red Hat ネットワークwebサイト— どのコンピュータからでも安全なwebブラウザを通じて、複数のシステムや個別パッケージのダウンロードを管理し、Errata更新などの仕事をスケジュールします。

Red Hat ネットワークの使用を開始するには、以下の3つの基本的な手順を実行します：

1. 次の方法の1つを使用してシステムプロファイルを作成します：
   - インストール後の最初の起動で**セットアップエージェント**が出た時にRHNに対してシステムを登録します。
   - デスクトップ上で**メインメニューボタン** => **システムツール** => **Red Hat ネットワーク**と選択して行きます。
   - シェルプロンプトで`up2date`コマンドを実行します。

2. RHN（http://rhn.redhat.com/にログインし、システムのサービス権利を取得します。ユーザーは誰でも1システムにつきRed Hat ネットワークアカウントを1つ無料で利用できます。追加アカウントを購入することもできます。

3. RHN Webサイトからアップデートのスケジュール設定を開始するか、または**Red Hat 更新エージェント**でErrata 更新をダウンロードしてインストールします。

詳細については、 http://www.redhat.com/docs/manuals/RHNetwork/で入手可能な「*Red Hat* ネットワーク*User Reference Guide*」を参照してください。

ヒント

Red Hat Linux には、**Red Hat ネットワーク通知お知らせツール**と言う、便利なパネルアイコンがあり、ユーザーのRed Hat Linuxシステム用の更新がある場合には、視覚的に知らせてくれます。このアプレット(パネル上のアイコン)に関する説明は、 http://rhn.redhat.com/help/basic/applet.htmlで御覧下さい。

VI. 付録

このパートでは、Red Hat, Inc.提供のソースファイルからのカスタムカーネル構築法を説明します。
また、安全な通信のために使用できるツール、Gnu Privacy Guard の章についても含まれています。

目次

付録A.
カスタムカーネルの構築

Linuxは初めてという人は、「なぜ独自のカーネルを構築する必要があるのだろうか」という疑問をよく抱きます。現在ではカーネルモジュールが改善されているので、この疑問に対する最も正確な答えは次のようになるでしょう。「今、独自のカーネルを構築する必要性を感じていなければ、構築しなくてもよい。」

Red Hat Linuxと一緒に提供されたカーネル及びRed Hat Linuxエラータシステムを介して提供されたカーネルは、最近のハードウェアやカーネル機能のほとんどにサポートを提供します。ほとんどのユーザーにとって、再コンパイルの必要性はありません。この付録は、カーネルについてさらに知識を深めるために再コンパイルしたいユーザー、カーネルに試験的機能をコンパイルしたいユーザーなどのためのガイドです。

Red Hat, Inc.で配給されたカーネルパッケージを使用してアップグレードするには、第30章を参照してください。


警告

カスタムカーネルの構築はRed Hat Linuxインストールサポートチームによるサポートはありません。Red Hat, Inc.で配給されたRPMパッケージを使用してのカーネルのアップグレードについての詳細は、第30章を参照してください。

A.1. 構築の準備

カスタムカーネルを構築する前に、非常に重要なことがあります。まず、万一の場合に備えて作動する緊急ブートディスクが手元にあることを確認してください。現在実行中のカーネルを使ってブートするブートディスクを作成するには、以下のコマンドを実行します。

```
/sbin/mkbootdisk `uname -r`
```

ディスクを作成したら、確かにそのディスクがシステムをブートするか確認のためのテストをしてください。

カーネルを再コンパイルするには、 `kernel-source`パッケージをインストールする必要があります。次のコマンドを実行して

```
rpm -q kernel-source
```

インストールされているか確認します。インストールされていなければ、Red Hat LinuxのCD-ROM、Red HatのFTPサイトftp://ftp.redhat.com (ミラーの一覧は、 http://www.redhat.com/mirrors.html)、Red Hat ネットワークなどからインストールします。RPMパッケージのインストールについての詳細は、パートVを参照してください。

A.2. カーネルの構築

ここでは、モジュール形式カーネルの構築について解説します。モノリシックカーネルについては、項A.3を参照してください。モノリシックカーネルの構築とインストールについて、モジュール形式カーネルとは異なる点について説明してあります。

注意

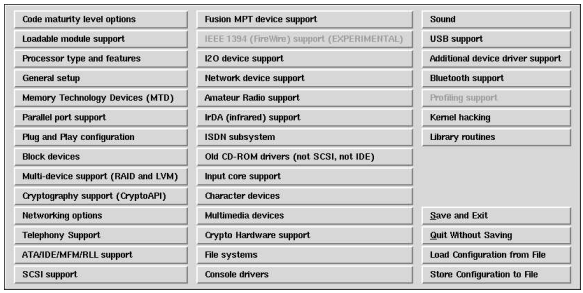
ここの例では、カーネルバージョンとして2.4.20-2.47.1を使っています(使用カーネルバージョンが異なる場合があります)。カーネルバージョンを確認するには、`uname -r` コマンドを入力します。2.4.20-2.47.1を返ってきた実際のバージョンに置き換えてください。

x86アーキテクチャ用のカスタムカーネルを構築するには(以下すべてのステップはrootとして行なうこと)、

1. シェルプロンプトを開き、`/usr/src/linux-2.4` ディレクトリに移動します。これ以降のコマンドは、すべてこのディレクトリで実行しなければなりません。
2. カーネルを構築するときは、ソースツリーをきれいな状態にしておくことが重要です。したがって、最初に、 `make mrproper`コマンドを発行して、ソースツリーに散らばっている可能性がある前回の構築作業の残りと共に設定ファイルを削除することをおすすめします。`/usr/src/linux-2.4/.config`ファイルとしてすでに設定ファイルが存在する場合は、このコマンドを実行する前に別のディレクトリへバックアップをとっておき、後でコピーして元にもどします。
3. スタート地点として、デフォルトのRed Hat Linuxカーネルの設定を使用することをおすすめします。これを行なうには、システムのアーキテクチャ用設定ファイルを `/usr/src/linux-2.4/configs/` ディレクトリから `/usr/src/linux-2.4/.config`にコピーします。システムに4ギガバイト以上のメモリがある場合は、 `bigmem`のキーワードを含むファイルをコピーします。
4. 次に、設定をカスタマイズします。X Window Systemが利用可能なら、推奨される方法として`make xconfig` コマンドを使い**Linux Kernel Configuration**を実行します。

注意

`make xconfig` コマンドで開始されるグラフィカルツールを使用するには、`wish`コマンドを提供する`tk`パッケージをインストールする必要があります。RPMパッケージのインストールについての詳細は、パートVを参照してください。



図A-1. カーネルコンポーネントのカテゴリ設定

図A-1で示すように、カテゴリをクリックして選択し、設定します。各カテゴリ内はコンポーネントです。コンポーネントの横にある**y** (yes)、**m**(module)、**n**(no)のいずれかを選択して、それぞれ、カーネルにコンパイルする、カーネルモジュールとしてコンパイルする、コンパイルしないなどを行ないます。コンポーネントについての詳細は、横にある**Help**ボタンをクリックします。

メインメニューをクリックしてカテゴリ一覧に戻ります。

設定が完了したら、メインメニューウィンドウにある**Save and Exit button**をクリックして設定ファイル `/usr/src/linux-2.4/.config`を作成し、**Linux Kernel Configuration** プログラムを終了します。

設定になにも変更を加えなかった場合にも、続行する前に`make xconfig`コマンドの実行(または、カーネル設定の他の方法のどれか)が要求されます。

カーネル設定のために利用できる他の方法と以下のような方法があります。

- `make config` — インテラクティブなテキストプログラム。コンポーネントはリニア形式で表示され、ひとつづつ答えていきます。この方法はX Window Systemを必要としません。前の質問に戻って答えを変更することはできません。
- `make menuconfig` — テキストモードのメニュー法式プログラム。コンポーネントはカテゴリのメニューで表示されます。Red Hat Linuxインストールプログラムのテキストモードで使用したのと同じ方法で、目的のコンポーネントを選択します。**[*]** (ビルトイン)、**[]**(除外)、<**M**>(モジュール)、< >(モジュール可能)などの含まれるべきアイテムに対応するタグを切り替えます。この方法はX Window Systemを必要としません。
- `make oldconfig` — これはノンインテラクティブなスクリプトで、設定ファイルがデフォルト設定を含むようセットアップします。システムがデフォルトのRed Hat Linuxカーネルを使用している場合は、アーキテクチャ用としてRed Hat Linuxと共に配給されたカーネルの設定ファイルを作成します。作動するデフォルトを確認し必要のない機能を停止するためのカーネルを設定するのに便利です。

注意

`kmod` とカーネルモジュールを使用するには、設定中に`kmod support` と`module version (CONFIG_MODVERSIONS) support`に**Yes**と答えます。

5. `/usr/src/linux-2.4/.config` ファイルを作成したら、`make dep`コマンドを使用して正しく依存関係をセットアップします。
6. `make clean`コマンドを実行し、構築用にソースツリーの準備をします。
7. 既存のカーネルが上書きされないようにカスタムカーネルのバージョン番号は修正したものをつけることをおすすめします。ここで説明している方法は、万一の場合、最も簡単なリカバリ方法です。その他の可能性については、 http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html、または、`/usr/src/linux-2.4`にある`Makefile`をご覧ください。

   デフォルトでは、`/usr/src/linux-2.4/Makefile` は、`EXTRAVERSION`で始まるラインの末尾に`custom`という単語があります。その文字列を加えることにより、システムが作動している古いカーネルと新しいカーネル(バージョン2.4.20-2.47.1カスタム)を同時に持つことができます。

   システムがひとつ以上のカスタムカーネルを含む場合は、最後に日付を加えるとよいでしょう(または、別の識別子)。
8. `make bzImage`を実行して、カーネルを構築します。
9. `make modules` で設定されたモジュールはすべて構築します。
10. `make modules_install` コマンドを使用してカーネルモジュールをインストールします(実際にはなにも構築されていない場合も)。コマンド内の下線(_)に注意してください。これでカーネルモジュールをディレクトリパスの`/lib/modules/ <`*`KERNELVERSION`*`> /kernel/drivers(` *`KERNELVERSION`* は、 `Makefile`で指定したバージョン)にインストールします。この例では、 `/lib/modules/2.4.20-2.47.1custom/kernel/drivers/` となります。

11. `make install`を使用して新しいカーネルと関連ファイルを該当ディレクトリにコピーします。

    `/boot`ディレクトリにカーネルをインストールすることに加えて、このコマンドは新しい`initrd`イメージを構築して、新しいエントリをブートローダー設定ファイルに追加する`/sbin/new-kernel-pkg`スクリプトの実行もします。

    システムにSCSIアダプタがあり、SCSIドライブがコンパイルされた場合、あるいは、カーネルがモジュール(Red Hat Linuxではデフォルト)としてext3サポートで構築された場合は、`initrd`イメージが必要となります。

12. `initrd`イメージ及びブートローダに修正が加えられるとしても、正しく行なわれたか確認して2.4.20-2.47.1の代わりにカスタムカーネルバージョンを使用することを確認してください。これらの修正の確認についての説明は、項30.5と項30.6を参照してください。

A.3. モノリシックカーネルの構築

例外はいくつかありますが、モノリシックカーネルを構築するには、モジュール形式カーネルの構築の場合と同じ手順です。

- カーネルを設定する場合、どの設定もモジュールとしてコンパイルしないでください。つまり、質問に対して、 **`Yes`**か、**`No`**のみで答えてください。そして、`kmod support` と`module version (CONFIG_MODVERSIONS) support`に対しては、**`No`**と答えます。
- 次の手順は省略します。
  `make modules`
  `make modules_install`
- `nomodules`で `grub.conf`に`kernel` ラインを加える、あるいは、`lilo.conf`を編集して `append=nomodules`ラインを含ませます。

A.4. その他のリソース

Linuxカーネルについての詳細は、以下のリソースを参照してください。resources.

A.4.1. インストールされているドキュメント

- `/usr/src/linux-2.4/Documentation` — Linuxカーネルとそのモジュールに関する上級ドキュメント。これらのドキュメントは、カーネルソースコードへの貢献、カーネルの動作法の理解などに興味を持つ方向けです。

A.4.2. 役に立つWebサイト

- http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html — Linux Documentation Projectの*The Linux Kernel HOWTO*
- http://www.kernel.org/pub/linux/docs/lkml/ — Linuxカーネルのメーリングリスト

付録B.

Gnu Privacy Guardの使用

電子メールは、送信してから相手が受信するまで両方向の通信中に読み取られることはないのでしょうか。残念なことに、第三者がそのメールを盗み見たり、改ざんしたりする可能性があります。

従来の郵便（いわゆる「郵政省メール」）では、内容は封筒に密封され、消印を押され、いくつかの郵便局を経由して受取人に配達されます。しかし、インターネットを使用したメールの送信は安全性が低く、電子メールは暗号化されていないテキストの形でサーバーからサーバーへ転送されます。他人による盗み見や改ざんから通信内容を保護する特別な処置は何も取られていません。

プライバシーを保護するために、Red Hat Linux 9には、GnuPG、（**GNU Privacy Guard**）が用意されており、通常のRed Hat Linuxインストール時にデフォルトでインストールされます。**GPG**と呼ばれることもあります。

GnuPGは安全な通信のためのツールで、PGP(Pretty Good Privacy というポピュラーな暗号アプリケーション)で使われている暗号技術への互換性を持つフリーのツールです。GnuPGを使えば、データや通信を暗号化するだけでなく、電子署名によって通信が本物であることを証明することも出来ます。GnuPGは、PGP 5.*x*の解読と検証もできます。

GnuPGはほかの暗号規格と互換性がありますので、これで暗号化した通信は、WindowsやMacintoshなどのほかのオペレーティングシステムの電子メールアプリケーションと互換性があります。

GnuPGは、公開鍵暗号方式を使用して、データの安全な交換を実現しています。公開鍵暗号方式では、公開鍵と秘密鍵の2つの鍵を作成します。公開鍵は通信相手またはキーサーバーと交換します。秘密鍵は絶対に公開してはいけません。

暗号は鍵の使用によって実現するものです。従来の、つまり対称式の暗号法では、トランザクションの両端で同じ鍵を持ち、その鍵を使用して互いの伝送データを復号します。公開鍵暗号方式では、公開鍵と秘密鍵の2つの鍵が共存します。個人あるいは組織は秘密鍵を秘匿し、公開鍵を公開します。公開鍵によって暗号化されたデータは、秘密鍵を使用しないと復号できません。秘密鍵によって暗号化されたデータは、公開鍵を使用しないと復号できません。

重要

重要な点は、公開鍵は安全な通信を行いたい相手の誰に渡してもかまいませんが、秘密鍵は決して誰にも渡さない、ということです。

暗号化については内容の大部分が本書の範囲を越えていますが、多くの書籍がこの課題で出版されております。この章では、GnuPGについて、暗号を使った通信を始められるだけの情報を提供します。GnuPG、PGP及び暗号化技術ついてもっと知識を得るには、項B.8を参照してください。

B.1. 設定ファイル

始めてGnuPGコマンドを実行する時に、ユーザーのホームディレクトリに`.gnupg`ディレクトリが生成されます。バージョン1.2からスタートした設定ファイル名は`.gnupg/options`から`.gnupg/gpg.conf`に変更されています。ホームディレクトリに`.gnupg/gpg.conf`がない場合は、`.gnupg/options`を使用して下さい。バージョン1.2又はそれ以降のみを使用する場合は、次のコマンドを使用して設定ファイル名の変更が推奨されます：

```
mv ~/.gnupg/options ~/.gnupg/gpg.conf
```

バージョン1.0.7以前の物からアップグレードしている場合、署名キャッシュをキーリングの中に作成してキーリングアクセス時間を短縮できます。この操作をするには、次のコマンドを1回実行します：

```
gpg --rebuild-keydb-caches
```

B.2. 警告メッセージ

GnuPGコマンドを実行するとき、以下のメッセージが出ることがあります：

```
gpg: Warning: using insecure memory!
```

この警告は、root以外のユーザーがメモリページをロックできない為、表示されます。もしユーザーがメモリページをロックできるのなら、メモリについてサービス妨害(DoS) 攻撃を実行できます。これはセキュリティ問題の可能性があります。詳細については以下のサイトを参照して下さい。http://www.gnupg.org/(en)/documentation/faqs.html#q6.1.

次のようなメッセージが出る可能性もあります：

```
gpg: WARNING: unsafe permissions on configuration file "/home/username/.gnupg/gpg.conf"
```

このメッセージは、設定ファイルのファイル権限が他の人に読み込みを許可する場合に表示されます。この警告が出た時は、次のコマンドを実行してファイルの権限を変更することが推奨されます：

```
chmod 600 ~/.gnupg/gpg.conf
```

他の一般的なメッセージには、次のようなものがあります：

```
gpg: WARNING: unsafe enclosing directory permissions on configuration file
"/home/username/.gnupg/gpg.conf"
```

このメッセージは、設定ファイルを含むディレクトリが他人にその内容の読み込みを許可している場合に、表示されます。この表示が出た時は、次のコマンドを実行してファイルの権限を変更することが推奨されます：

```
chmod 700 ~/.gnupg
```

GnuPGの以前のバージョンからアップグレードした場合は、以下のメッセージが出る可能性があります：

```
gpg: /home/username/.gnupg/gpg.conf:82: deprecated option "honor-http-proxy"
gpg: please use "keyserver-options honor-http-proxy" instead
```

この警告は~/.gnupg/gpg.conf ファイルが以下の行を含んでいる為です：

```
honor-http-proxy
```

バージョン1.0.7とそれ以降には、別の構文が適切です。この行を次のように変更して下さい：

```
keyserver-options honor-http-proxy
```

B.3. 鍵ペアの生成

GnuPGを使用するには、最初に新しい鍵ペア、つまり公開鍵と秘密鍵を生成しなければいけません。

鍵ペアを生成するには、シェルプロンプトに対して以下のコマンドを入力します：

```
gpg --gen-key
```

ユーザーは、自分のユーザーアカウントで作業することが最も多いので、この操作はユーザーアカウント（rootではなく）にログインしている間に行うようにします。

初期画面で、推奨オプション（デフォルト）を含む鍵オプションが以下の様に表示されます：

```
gpg (GnuPG) 1.2.1; Copyright (C) 1999 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
(1) DSA and ElGamal (default)
(2) DSA (sign only)
(5) RSA (sign only)
Your selection?
```

オプションの選択を必要とするほとんどの画面では、かっこの中にデフォルトのオプションを示しています。[Enter]キーを押すだけでデフォルトオプションをそのまま指定できます。

初期画面では、デフォルトオプションの`(1) DSA and ElGamal`をそのまま指定してください。このオプションを選択すると、2種類の方法でデジタル署名を作成したり暗号化（復号）したりすることができます。**1**と入力して[Enter]キーを押してください。

次に、キーサイズ、つまり鍵の長さを選択します。一般に、鍵の長さが長いほど攻撃に対する抵抗力が高くなります。デフォルトサイズの1,024ビットでほとんどのユーザーにとっては十分です。[Enter]キーを押します。

次のオプションでは、鍵の有効期間を指定します。通常、デフォルトの `0 = key does not expire`で問題ありません。有効期限を設定する場合は、公開鍵を交換する相手にも有効期限を通知する必要があり、失効したら新しい公開鍵を交付する必要があることに注意してください。有効期限を設定しない場合は、決定を確認するように依頼されます。[y]キーを押して確定します。

次の作業は、氏名、電子メールアドレス、そしてコメント（省略可）を含むユーザーのユーザーIDの入力です。入力を終えると、入力した情報の要約が表示されます。

選択内容を確認後、パスフレーズを入力する必要があります。

ヒント

アカウントのパスワードと同様に、GnuPGのセキュリティを最適にするためには、よいパスフレーズを使うことが重要です。たとえば、大文字と小文字を混合する、数値や句読点記号類を使用するなどの方法を取ります。

パスフレーズを入力し、確認すると、鍵が生成されます。次のようなメッセージが表示されます：

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++.+++++.++++++++....++++++++++..+++++.+++++.+++++++.+++++++
+++.++++++++++++++++++++++++++++++++++++++.........................++++
```

画面の動きが止まると、新しい鍵が作成され、ホームディレクトリの`.gnupg`に格納されます。キーの一覧を表示するには、次のコマンドを使用します：

```
gpg --list-keys
```

次のようなメッセージが表示されます。

```
/home/username/.gnupg/pubring.gpg
---------------------------------
pub 1024D/B7085C8A 2000-06-18 Your Name <you@example.com>
sub 1024g/E12AF9C4 2000-06-18
```

GnuPGキーをバージョン1.0.6又はそれ以前のもので生成した場合、秘密キーをエキスポートして、新しくそれをインポートし直したバージョン1.0.7又はそれ以降で署名する為に明確に自己のキーを信任する必要があります。自己のキーを信任するには次のコマンドを使用します(<*user-id*>を入れ換え):

```
gpg --edit-key <user-id>
```

Command>プロンプトで、**trust**とタイプして5 = I trust ultimatelyを選択して自己のキーへの信任を示します。

B.4. 失効証明の生成

鍵ペアを生成したら、公開鍵に対して失効証明を生成する必要があります。パスフレーズを忘れたり、パスフレーズが漏洩したりした場合は、ユーザーにその公開鍵がもはや使用できないことを通知するために、この証明を発行します。

注意

失効証明を生成するといっても、生成したばかりの鍵を失効させるわけではありません。その代わり、パスフレーズを忘れたり、ISP（アドレス）が変わったり、ハードディスクがクラッシュした場合に、公開した鍵の使用を取り消す安全な方法を確立します。失効証明を使用して、公開鍵を無効にすることができます。

あなたの署名は、公開鍵が失効するまでは通信内容を読む相手にとって有効となり、逆にあなたは鍵が失効する前に受け取ったメッセージを解読することができます。失効証明を生成するには、--gen-revokeオプションを使用します：

```
gpg --output revoke.asc --gen-revoke <you@example.com>
```

上記の--output revoke.ascオプションを省略すると、失効証明は標準出力としてモニタ画面に表示されることに注意してください。テキストエディタを使って、出力の内容をコピーして任意のファイルに貼り付けることができますが、出力をログインディレクトリ内のファイルにリダイレクトする方が簡単です。こうすると、保管した失効証明を後で利用したり、あるいはフロッピーディスクに移して安全な場所に保管できます。

その出力は以下のようになります：

```
sec 1024D/823D25A9 2000-04-26 Your Name <you@example.com>

このキーの失効証明を生成しますか？
```

[Y]キーを押してリストしてあるキーの失効証明を生成します。次に、失効の理由を選択する場面でオプションの記述を選びます。その理由を確認した後は、キー生成に使用したパスフレーズを入力します。

失効証明が生成されると（revoke.asc）、ログインディレクトリに格納されます。失効証明は、フロッピーディスクにコピーして安全な場所に保管します（Red Hat Linuxでファイルをフロッピーディスクにコピーする方法がわからない場合は、「*Red Hat Linux* 入門ガイド」を参照してください）。

B.5. 公開鍵のエクスポート

公開鍵暗号方式を使用するには、相手が公開鍵のコピーを持っている必要があります。通信相手やキーサーバーに鍵を送信するには、鍵をエクスポート しなければいけません。

以下のコマンドを入力して鍵をエクスポートすれば、鍵をWebページで表示したり、電子メールに貼り付けることができます。

```
gpg --armor --export <you@example.com> > mykey.asc
```

公開鍵はエクスポートされ、この例ではmykey.ascファイルに出力がリダイレクトされるため、画面には何も表示されません。（>mykey.ascを省略すると、鍵は標準出力のディスプレイ画面に表示されます）。

これで、mykey.ascファイルを電子メールに挿入したり、キーサーバーにエキスポートしたりできるようになりました。鍵を表示するには、シェルプロンプトでless mykey.ascと入力して、ページャでファイルを開きます（ページャを閉じるには、[q]キーを入力します）。以下のようになります：

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDkHP3URBACkWGsYh43pkXU9wj/X1G67K8/DSrl85r7dNtHNfLL/ewil10k2
q8saWJn26QZPsDVqdUJMOdHfJ6kQTAt9NzQbgcVrxLYNfgeBsvkHF/POtnYcZRgL
tZ6syBBWs8JB4xt5V09iJSGAMPUQE8Jpdn2aRXPApdoDw179LM8Rq6r+gwCg5ZZa
pGNlkgFu24WM5wC1zg4QTbMD/3MJCSxfL99Ek5HXcB3yhj+o0LmIrGAVBgoWdrRd
BIGjQQFhV1NSwC8YhN/4nGHWpaTxgEtnb4CI1wI/G3DK9olYMyRJinkGJ6XYfP3b
cCQmqATDF5ugIAmdditnw7deXqn/eavaMxRXJM/RQSgJJyVpbAO2OqKe6L6Inb5H
kjcZA/9obTm499dDMRQ/CNR92fA5pr0zriy/ziLUow+cqI59nt+bEb9nY1mfmUN6
SW0jCH+pIQH5lerV+EookyOyq3ocUdjeRYF/d2jl9xmeSyL2H3tDvnuE6vgqFU/N
sdvby4B2Iku7S/h06W6GPQAe+pzdyX9vS+Pnf8osu7W3j60WprQkUGF1bCBHYWxs
YWdoZXIgPHBhdWxnYWxsQHJlZGhhdC5jb20+iFYEExECABYFAjkHP3UECwoEAwMV
AwIDFgIBAheAAAoJEJECmvGCPSWpMjQAoNF2zvRgdR/8or9pBhu95zeSnkb7AKCm
/uXVS0a5KoN7J61/1vEwx11poLkBDQQ5Bz+MEAQA8ztcWRJjW8cHCgLaE402jyqQ
37gDT/n4VS66nU+YItzDFScVmgMuFRzhibLblfO9TpZzxEbSF3T6p9hLLnHCQ1bD
HRsKfh0eJYMMqB3+HyUpNeqCMEEd9AnWD9P4rQtO7Pes38sV0lX0OSvsTyMG9wEB
vSNZk+Rl+phA55r1s8cAAwUEAJjqazvk0bgFrw1OPG9m7fEeDlvPSV6HSA0fvz4w
c7ckfpuxg/URQNf3TJA00Acprk8Gg8J2CtebAyR/sP5IsrK5l1luGdk+l0M85FpT
/cen2OdJtToAF/6fGnIkeCeP1O5aWTbDgdAUHBRykpdWU3GJ7NS6923fVg5khQWg
uwrAiEYEGBECAAYFAjkHP4wACgkQkQKa8YI9JamliwCfXox/HjlorMKnQRJkeBcZ
iLyPH1QAoI33Ft/0HBqLtqdtP4vWYQRbibjW
=BMEc
-----END PGP PUBLIC KEY BLOCK-----
```

B.5.1. キーサーバーへのエクスポート

通信相手が少数であれば、公開鍵をエクスポートした後で個別に送信するとよいでしょう。しかし、通信相手が大勢の場合は、公開鍵の配布に時間がかかります。その場合は、キーサーバーを使うと便利です。

キーサーバーとは、インターネット上の保管所であり、ここで公開鍵を保管したり、要求する人に対して公開鍵を配布したりすることができます。多くのキーサーバーが利用できますが、そのほとんどは互いに同期を取るようにしているので、1つのキーサーバーに公開鍵を送れば、すべてのキーサーバーに配布できます。通信相手は、キーサーバーに対して公開鍵を要求し、取得した鍵をキーリングにインポートすることができます。これで安全な通信のための準備は完了です。

ヒント

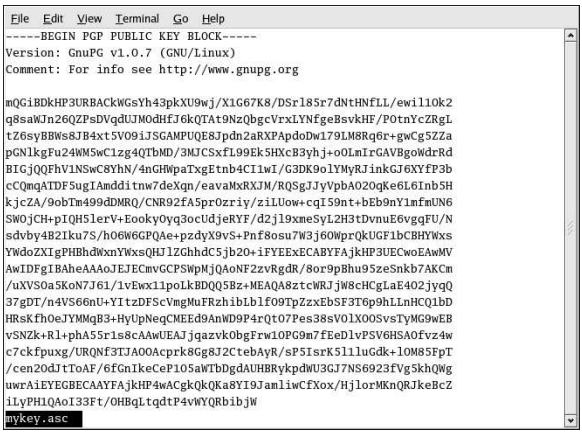
ほとんどのキーサーバーは互いに同期を取っており、1つのキーサーバーに送れば、通常すべてのキーサーバーに配布できます。しかし、別のキーサーバーを検索することはできます。キーサーバーと関連情報を検索する場所として、「*Keyserver.Net*」（http://www.keyserver.net）があります。

シェルプロンプトかWebブラウザのどちらを使用しても公開鍵を送ることができますが、キーサーバーを利用して鍵を送受信するには、インターネットに接続している必要があります。

- シェルプロンプトで以下のように入力します：
  `gpg --keyserver search.keyserver.net --send-key` *`you@example.com`*
- ブラウザからKeyserver.Net（http://www.keyserver.net）にアクセスし、PGP公開鍵を追加する為のオプションを選択します。

  そして、公開鍵をWeb ページの適切な場所にコピーして貼り付けます。この方法についての説明が必要な場合は以下を使用して下さい：

  - エクスポートした公開鍵ファイル（たとえば項B.5で作成した*`mykey.asc`*）を、ページャを使って開きます。— シェルプロンプトで、コマンド`less mykey.asc`を入力します。
  - マウスを使って、`BEGIN PGP`から`END PGP`までのすべての行を強調表示(図B-1を参照)してコピーします。
  - コピーした*`mykey.asc`*の内容を、Keyserver.Netのページの適切な場所に、マウスの中央ボタンをクリックして貼り付けます（2ボタンのマウスの場合は、両方のボタンを同時に押します）。キーサーバーページで**Submit**ボタンをクリックします（間違えた場合は、**Reset**ボタンをクリックして、貼り付けた鍵を削除します）。



図B-1. 公開鍵のコピー

別のWebベースのキーサーバーに公開鍵を登録する場合でも基本的に上記と同様にして行えます。

必要な作業は以上でおしまいです。鍵が正しく登録されたことを知らせるメッセージが、シェルプロンプトの場合はシェルプロンプトに、Webの場合はキーサーバーのWebページに表示されます。これで、安全な通信を希望する通信相手は、キーサーバーに登録された公開鍵をインポートして、キーリングに追加できるようになりました。

B.6. 公開鍵のインポート

通信相手の公開鍵をキーリングにインポートすることは、エクスポートする場合と同じくらい簡単です。通信相手の公開鍵をインポートすれば、キーリングに含まれる相手の公開鍵を使用することによって、メールを解読したり電子署名を確認したりできます。

一番簡単なインポートは、Webサイトから鍵をダウンロードして保存することです。

鍵をダウンロードしてから、*key.asc*ファイルに保存します。シェルプロンプトで次のコマンドを実行してキーリングに追加します。

```
gpg --import key.asc
```

鍵を保存する別の方法として、ブラウザの**名前を付けて保存**機能を使う方法があります。**Mozilla**などのブラウザを使用していて、かつ鍵をキーサーバーに置いている場合は、そのページをテキストファイルとして保存できます（**ファイル-名前を付けて保存**）。文書を保存するときは、**ファイルの種類**を選択して、**テキストのみのファイル(*.txt)**を選択します。これで鍵をインポートできますが、保存したファイルの名前を覚えておいてください。たとえば、鍵を*newkey.txt*というテキストファイルとして保存した場合、ファイルをインポートするには、以下をシェルプロンプトに入力します：

```
gpg --import newkey.txt
```

出力は、次のようになります：

```
gpg: key F78FFE84: public key imported
gpg: Total number processed: 1
gpg:       imported: 1
```

インポートが成功したかどうかをチェックするには、`gpg --list-keys`コマンドを入力します。新たにインポートされた鍵がキーリングに表示されます。

公開キーをインポートする時には、そのキーを自分の*keyring*(公開及び秘密キーが保存されているファイル)に追加します。そしてドキュメントやファイルを相手先からダウンロードする時点に、キーリングに追加したキーを使用してドキュメントの信頼度をチェック出来ます。

B.7. デジタル署名とは

デジタル署名は、サインにたとえられるものです。署名を改ざんできる可能性があった従来の通信文とは異なり、デジタル署名は偽造できません。デジタル署名は一意の秘密鍵によって作成され、通信の受取人は相手の公開鍵を使ってその署名を検証できます。

デジタル署名は、文書にタイムスタンプを添付します。つまり、文書に署名した時刻は署名の一部になります。このため、だれかが文書を修正しようとすると、署名の検証が失敗することになります。**Exmh**やKDEの**KMail**などの一部の電子メールアプリケーションではアプリケーションのインターフェイスから**GnuPG**を使って文書に署名する機能を利用できます。

デジタル署名の便利な2タイプは、*clearsigned*文書と*detached signatures*です。どちらの認証も安全性は同程度であり、受信者はメッセージ全体を解読する必要はありません。

clearsignedメッセージでは、署名は文面にテキストブロックとして表示され、detached signatureは別のファイルとして文面といっしょに送信されます。

B.8. その他のリソース

暗号化技術については、ここでGnuPGについて説明したことよりはるかに多くの事柄があります。より詳しく知るためには、以下を参照してください。

B.8.1. インストールされているドキュメント

- `man gpg`と`info gpg` —**GnuPG**コマンドとオプションのクリックリファレンス。

B.8.2. 役に立つWebサイト

- http://www.gnupg.org — GnuPGのWebサイトには、GnuPGリリース、詳細なユーザーズガイド、その他の暗号情報のリンクがあります。
- http://hotwired.lycos.com/webmonkey/backend/security/tutorials/tutorial1.html —Webmonkeyの「*Encryption Tutorial*」には、暗号に関する情報とその応用に関する情報があります。
- http://www.eff.org/pub/Privacy —The Electronic Frontier Foundationの「Privacy, Security, Crypto, & Surveillance」アーカイブ。

B.8.3. 関連資料

- *The Official PGP User's Guide*（Philip R. Zimmermann著、MIT Press刊）
- *PGP: Pretty Good Privacy*（Simson Garfinkel著、オライリー・ジャパン刊）
- *E-Mail Security: How to Keep Your Electronic Messages Private*（Bruce Schneier著、John Wiley & Sons刊）

索引

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

あとがき

Red Hat Linux マニュアルはDocBook SGML v4.1形式で書かれています。HTML版とPDF版はカスタムDSSSLスタイルシートとカスタムjade wrapperスクリプトを使用して作成されています。DocBook SGMLファイルは、PSGMLモードの支持を使用して、**Emacs**で書かれています。

Garrett LeSageがアドモーショングラフィクスを製作しました(注意、ヒント、重要、用心、警告など)。これらは自由にRed Hatのドキュメントと一緒に使用することができます。

Red Hat Linux製品ドキュメントチームは以下のメンバーから構成されています。:

Sandra A. Moore — *Red Hat Linux x86* インストールガイドの主任ライター/管理人; *Red Hat Linux* 入門ガイドの支援ライター。

Tammy Fox — *Red Hat Linux* カスタマイズガイドの主任ライター/管理人; *Red Hat Linux* 入門ガイドの支援ライター; カスタムDocBook スタイルシートとスクリプトのライター/管理人

Edward C. Bailey — *Red Hat Linux* システムアドミニストレーションプレミアの主任ライター/管理人; *Red Hat Linux x86* インストールガイドの支援ライター

Johnray Fuller — *Red Hat Linux* 参照ガイドの主任ライター/管理人; *Red Hat Linux* セキュリティガイドの共同ライター/共同管理人; *Red Hat Linux* システムアドミニストレーションプレミアの支援ライター

John Ha — *Red Hat Linux* 入門ガイドの主任ライター/管理人; *Red Hat Linux* セキュリティガイドの共同ライター/共同管理人; *Red Hat Linux* システムアドミニストレーションプレミアの支援ライター

James Kiyoko Hashida — *Red Hat Linux* カスタマイズガイド及び*Red Hat Linux* 参照ガイドの翻訳者：橋田喜代人 ; Noriko Mizumoto — *Red Hat Linux x86* インストールガイド及び*Red Hat Linux* 入門ガイドの翻訳者：水本紀子