



# Red Hat Enterprise Linux 4

## システム管理ガイド

For Red Hat Enterprise Linux 4



# Red Hat Enterprise Linux 4 システム管理ガイド

---

For Red Hat Enterprise Linux 4

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

## 法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/System\_Administration\_Guide.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 概要

システム管理者のガイドでは、Red Hat Enterprise Linux 4 のデプロイメント、設定、および管理に関する関連情報を説明します。本書は、システムに関する基本的な理解があるシステム管理者を対象としています。

## 目次

はじめに .....	11
1. この手動の変更 .....	11
2. 本書の表記慣例 .....	12
2.1. 誤字規則 .....	12
2.2. 引用規則 .....	13
2.3. 注記および警告 .....	14
3. 詳細情報 .....	15
3.1. フィードバックをお寄せください .....	15
パート I. インストール関連情報 .....	16
第1章 キックスタートを使ったインストール .....	17
1.1. キックスタートを使ったインストールとは .....	17
1.2. キックスタートを使ったインストールの実行方法 .....	17
1.3. キックスタートファイルの作成 .....	17
1.4. キックスタートオプション .....	18
1.4.1. 高度なパーティション設定の例 .....	45
1.5. パッケージの選択 .....	46
1.6. インストール前のスクリプト .....	48
1.6.1. 例 .....	48
1.7. インストール後のスクリプト .....	49
1.7.1. 例 .....	50
1.8. キックスタートファイルの準備 .....	51
1.8.1. キックスタートブートメディアの作成 .....	51
1.8.2. ネットワーク上でキックスタートファイルの準備 .....	52
1.9. インストールツリーを利用可能にする .....	53
1.10. キックスタートインストールの開始 .....	54
第2章 KICKSTART CONFIGURATOR .....	57
2.1. 基本設定 .....	57
2.2. インストール方法 .....	59
2.3. ブートローダーのオプション .....	61
2.4. パーティション情報 .....	63
2.4.1. パーティションの作成 .....	64
2.4.1.1. ソフトウェア RAID パーティションの作成 .....	65
2.5. NETWORK CONFIGURATION .....	67
2.6. 認証 .....	68
2.7. ファイアウォールの設定 .....	70
2.7.1. SELinux の設定 .....	71
2.8. 設定の表示 .....	71
2.8.1. 全般 .....	71
2.8.2. ビデオカード .....	72
2.8.3. Monitor .....	73
2.9. パッケージの選択 .....	74
2.10. インストール前のスクリプト .....	75
2.11. インストール後のスクリプト .....	77
2.11.1. chroot 環境 .....	78
2.11.2. インタープリターの使用 .....	78
2.12. ファイルの保存 .....	78
第3章 PXE ネットワークインストール .....	80
3.1. ネットワークサーバーの設定 .....	80

3.2. PXE ブート設定	81
3.2.1. コマンドラインからの設定	83
3.3. PXE ホストの追加	84
3.3.1. コマンドラインからの設定	86
3.4. カスタムブートメッセージの追加	87
3.5. PXE インストールの実行	87
<b>第4章 ディスクレス環境</b>	<b>88</b>
4.1. NFS サーバーの設定	89
4.2. ディスクレス環境の設定の完了	90
4.3. ホストの追加	90
4.4. ホストの起動	92
<b>第5章 基本的なシステムの復元</b>	<b>93</b>
5.1. 一般的な問題	93
5.1.1. Red Hat Enterprise Linux で起動できない	93
5.1.2. ハードウェア/ソフトウェアの問題	93
5.1.3. root パスワード	94
5.2. レスキューモードでの起動	94
5.2.1. ブートローダーの再インストール	97
5.3. シングルユーザーモードで起動	98
5.4. 緊急モードでのブート	98
<b>パート II. ファイルシステム</b>	<b>100</b>
<b>第6章 EXT3 ファイルシステム。</b>	<b>101</b>
6.1. EXT3 の機能	101
6.2. EXT3 ファイルシステムの作成	102
6.3. EXT3 ファイルシステムへの変換	102
6.4. EXT2 ファイルシステムに戻す	104
<b>第7章 論理ボリュームマネージャー (LVM)</b>	<b>106</b>
7.1. LVM とは	106
7.2. LVM2 とは	107
7.3. 関連情報	107
7.3.1. インストールされているドキュメント	108
7.3.2. 便利な Web サイト	108
<b>第8章 LVM の設定</b>	<b>109</b>
8.1. 自動パーティション設定	109
8.2. 手動での LVM パーティション設定	111
8.2.1. /boot/ パーティションの作成	111
8.2.2. LVM 物理ボリュームの作成	114
8.2.3. LVM ボリュームグループの作成	116
8.2.4. LVM 論理ボリュームの作成	118
<b>第9章 RAID (REDUNDANT ARRAY OF INDEPENDENT DISKS)</b>	<b>121</b>
9.1. RAID とは	121
9.2. RAID を使用するユーザー	121
9.3. ハードウェア RAID とソフトウェア RAID の比較	121
9.3.1. ハードウェア RAID	121
9.3.2. ソフトウェア RAID	122
9.4. RAID レベルとリニアサポート	123
<b>第10章 ソフトウェア RAID の設定</b>	<b>125</b>

10.1. RAID パーティションの作成	126
10.2. RAID デバイスとマウントポイントの作成	129
<b>第11章 SWAP 領域</b>	<b>135</b>
11.1. 変動スペースとは	135
11.2. スワップ領域の追加	135
11.2.1. LVM2 論理ボリュームでのスワップ領域の拡張	136
11.2.2. スワップの LVM2 論理ボリュームの作成	136
11.2.3. スワップファイルの作成	137
11.3. スワップ領域の削除	138
11.3.1. LVM2 論理ボリュームでのスワップ領域の縮小	138
11.3.2. スワップの LVM2 論理ボリュームの削除	139
11.3.3. スワップファイルの削除	140
11.4. SWAP 領域の移動	140
<b>第12章 ディスクストレージの管理</b>	<b>141</b>
12.1. PARTEDで標準パーティション	141
12.1.1. パーティションテーブルの表示	143
12.1.2. パーティションの作成	144
12.1.2.1. パーティションの作成	144
12.1.2.2. パーティションのフォーマット	145
12.1.2.3. パーティションのラベル付け	146
12.1.2.4. マウントポイントの作成	146
12.1.2.5. /etc/fstab への追加	146
12.1.3. パーティションの削除	146
12.1.4. パーティションのサイズ変更	148
12.2. LVM パーティション管理	149
<b>第13章 ディスククォータの実装</b>	<b>152</b>
13.1. ディスククォータの設定	152
13.1.1. クォータの有効化	152
13.1.2. ファイルシステムの再マウント	153
13.1.3. クォータデータベースファイルの作成	153
13.1.4. ユーザーごとのクォータ割り当て	155
13.1.5. グループごとのクォータ割り当て	156
13.1.6. ファイルシステムごとのクォータの割り当て	156
13.2. ディスククォータの管理	157
13.2.1. 有効化と無効化	157
13.2.2. ディスククォータに関するレポート	158
13.2.3. クォータの精度維持	158
13.3. 関連情報	159
13.3.1. インストールされているドキュメント	159
13.3.2. 関連書籍	159
<b>第14章 アクセス制御リスト</b>	<b>160</b>
14.1. ファイルシステムのマウント	160
14.1.1. NFS	161
14.2. アクセス ACL の設定	161
14.3. デフォルト ACL の設定	163
14.4. ACL の取り込み	163
14.5. ACL が設定されているファイルシステムのアーカイブ作成	164
14.6. 旧システムとの互換性	165
14.7. 関連情報	165
14.7.1. インストールされているドキュメント	165

14.7.2. 便利な Web サイト	166
<b>パート III. パッケージ管理</b>	<b>167</b>
<b>第15章 RPM でのパッケージ管理</b>	<b>168</b>
15.1. RPM 設計ゴール	168
15.2. RPM の使用	169
15.2.1. RPM パッケージの検索	169
15.2.2. インストール	170
15.2.2.1. インストールされているパッケージ	171
15.2.2.2. 競合するファイル	171
15.2.2.3. 解決できない依存関係	172
15.2.3. アンインストール	173
15.2.4. アップグレード	173
15.2.5. Freshening	174
15.2.6. クエリ	175
15.2.7. 検証	176
15.3. パッケージの署名の確認	178
15.3.1. キーのインポート	179
15.3.2. パッケージの署名の確認	179
15.4. RPM で金を抑制する	179
15.5. 関連情報	182
15.5.1. インストールされているドキュメント	182
15.5.2. 便利な Web サイト	182
15.5.3. 関連書籍	182
<b>第16章 RED HAT NETWORK</b>	<b>183</b>
<b>パート IV. ネットワーク関連の設定</b>	<b>188</b>
<b>第17章 NETWORK CONFIGURATION</b>	<b>189</b>
17.1. 概要	190
17.2. イーサネット接続の確立	191
17.3. ISDN 接続の確立	193
17.4. モード接続の確立	196
17.5. XDSL 接続の確立	199
17.6. トークンリング接続の確立	201
17.7. ワイヤレス接続の確立	204
17.8. DNS 設定の管理	207
17.9. ホストの管理	209
17.10. プロファイルの使用	210
17.11. デバイスエイリアス	214
17.12. ネットワーク設定の保存および復元	216
<b>第18章 ファイアウォール</b>	<b>217</b>
18.1. ALLINONES および IPTABLES	220
18.1.1. iptables の概要	221
18.2. 基本的なファイアウォール設定	221
18.2.1. Security Level Configuration Tool	221
18.2.2. ファイアウォールの有効化および無効化	222
18.2.3. 信頼できるサービス	223
18.2.4. 他のポート	224
18.2.5. 設定の保存	225
18.2.6. IPTables サービスのアクティブ化	225
18.3. IPTABLES の使用	226



---

18.3.1. iptables コマンド構文	226
18.3.2. 基本的なファイアウォールポリシー	227
18.3.3. IPTables ルールの保存および復元	227
18.4. 一般的な IPTABLES フィルタリング	228
18.5. FORWARD および NAT ルール	230
18.5.1. POSTROUTING and IP Masquerading	231
18.5.2. PREROUTING	232
18.5.3. DMZ および IPTables	232
18.6. 悪意のあるソフトウェアおよび SPOOFED IP アドレス	233
18.7. IPTABLES および接続の追跡	234
18.8. IPV6	235
18.9. 関連情報	235
18.9.1. インストールされているドキュメント	235
18.9.2. 便利な Web サイト	235
18.9.3. 関連するドキュメント	236
<b>第19章</b> .....	<b>237</b>
19.1.	237
19.2.	238
19.2.1. xinetd	238
19.3.	239
19.4. NTSYSV	241
19.5. CHKCONFIG	242
19.6. 関連情報	242
19.6.1. インストールされているドキュメント	242
19.6.2. 便利な Web サイト	243
19.6.3. 関連書籍	243
<b>第20章 OPENSSSH</b> .....	<b>244</b>
20.1.	244
20.2.	244
20.3.	244
20.3.1.	244
20.3.2.	245
20.3.3.	246
20.3.4. 鍵ペアの生成	246
20.3.4.1.	247
20.3.4.2.	247
20.3.4.3.	248
20.3.4.4.	249
20.3.4.5.	249
20.4. 関連情報	250
20.4.1. インストールされているドキュメント	250
20.4.2. 便利な Web サイト	250
20.4.3. 関連書籍	250
<b>第21章 NETWORK FILE SYSTEM (NFS)</b> .....	<b>251</b>
21.1.	251
21.2.	251
21.2.1. /etc/fstab を使用した NFS ファイルシステムのマウント	251
21.2.2.	252
21.2.3.	253
21.2.4. ACL の維持	254
21.3. NFS ファイルシステムのエクスポート	254

---

21.3.1. コマンドラインからの設定	257
21.3.2. ホスト名の形式	259
21.3.3. サーバーの起動と停止	260
21.4. 関連情報	260
21.4.1. インストールされているドキュメント	260
21.4.2. 便利な Web サイト	261
21.4.3. 関連書籍	261
<b>第22章 SAMBA</b>	<b>262</b>
22.1. SAMBA を使用する理由	262
22.2. SAMBA サーバーの設定	262
22.2.1. グラフィカル設定	262
22.2.1.1. サーバーの設定	263
22.2.1.2. Samba ユーザーの管理	265
22.2.1.3. 共有の追加	267
22.2.2. コマンドラインからの設定	268
22.2.3. 暗号化パスワード	268
22.2.4. サーバーの起動と停止	270
22.3. SAMBA 共有への接続	271
22.3.1. コマンドライン	273
22.3.2. 共有のマウント	274
22.4. 関連情報	274
22.4.1. インストールされているドキュメント	274
22.4.2. 便利な Web サイト	275
<b>第23章 DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP)</b>	<b>276</b>
23.1. DHCP を使用する理由	276
23.2. DHCP サーバーの設定	276
23.2.1. 設定ファイル	276
23.2.2. リースデータベース	280
23.2.3. サーバーの起動と停止	281
23.2.4. DHCP リレーエージェント	283
23.3. DHCP クライアントの設定	283
23.4. 関連情報	285
23.4.1. インストールされているドキュメント	285
<b>第24章 APACHE HTTP サーバーの設定</b>	<b>286</b>
24.1. 基本設定	287
24.2. デフォルトの設定	289
24.2.1. サイトの設定	289
24.2.2. ログイン	291
24.2.3. 環境変数	293
24.2.4. ディレクトリー	295
24.3. 仮想ホストの設定	297
24.3.1. 仮想ホストの追加と編集	298
24.3.1.1. 一般的なオプション	298
24.3.1.2. SSL	299
24.3.1.3. 仮想ホストの追加オプション	301
24.4. サーバー設定	301
24.5. パフォーマンスチューニング	303
24.6. 設定の保存	304
24.7. 関連情報	305
24.7.1. インストールされているドキュメント	305
24.7.2. 便利な Web サイト	305

24.7.3. 関連書籍	305
<b>第25章 APACHE HTTP セキュアサーバー設定</b>	<b>306</b>
25.1. はじめに	306
25.2. セキュリティー関連パッケージの概要	306
25.3. 証明書およびセキュリティーの概要	309
25.4. 事前検証キーおよび証明書の使用	310
25.5. 証明書の種類	311
25.6. キーの生成	313
25.7. CA に送信する証明書要求の生成	315
25.8. 自己署名証明書の作成	317
25.9. 証明書のテスト	318
25.10. サーバーへのアクセス	318
25.11. 関連情報	319
25.11.1. 便利な Web サイト	319
25.11.2. 関連書籍	319
<b>第26章 認証設定</b>	<b>320</b>
26.1. ユーザー情報	320
26.2. 認証	322
26.3. コマンドラインのバージョン	324
<b>パート V. システム設定</b>	<b>329</b>
<b>第27章 コンソールアクセス</b>	<b>330</b>
27.1. SHUTDOWN VIA CTRL+ALT+DELの無効化	330
27.2. コンソールプログラムアクセスの無効化	331
27.3. コンソールの定義	331
27.4. コンソールからのファイルへのアクセス許可	332
27.5. 他のアプリケーションのコンソールアクセスの有効化	333
27.6. フロッピー グループ	334
<b>第28章 日付と時刻の設定</b>	<b>335</b>
28.1. 日付と時刻のプロパティー	335
28.2. NETWORK TIME PROTOCOL(NTP)プロパティー	336
28.3. タイムゾーンの設定	338
<b>第29章 キーボードの設定</b>	<b>339</b>
<b>第30章 マウス設定</b>	<b>340</b>
<b>第31章 X WINDOW SYSTEM の設定</b>	<b>342</b>
31.1. 表示設定	342
31.2. ハードウェア設定の表示	343
31.3. デュアルビューリスティックディスプレイの設定	344
<b>第32章 ユーザーとグループ</b>	<b>346</b>
32.1. ユーザーおよびグループの設定	346
32.1.1. 新規ユーザーの追加	347
32.1.2. ユーザープロパティーの変更	349
32.1.3. 新規グループの追加	350
32.1.4. グループプロパティーの変更	351
32.2. ユーザーおよびグループ管理ツール	352
32.2.1. コマンドラインからの設定	353
32.2.2. ユーザーの追加	353
32.2.3.	354

32.2.4.	355
32.2.5. プロセスの説明	358
32.3.	359
32.4.	362
32.5. ユーザープライベートグループ	365
32.5.1. グループディレクトリー	366
32.6. シャドウパスワード	367
32.7. 関連情報	368
32.7.1. インストールされているドキュメント	368
<b>第33章 プリンターの設定</b>	<b>370</b>
33.1. ローカルプリンターの追加	371
33.2. IPP プリンターの追加	373
33.3. SAMBA(SMB)プリンターの追加	374
33.4. JETDIRECT プリンターの追加	376
33.5. プリンターモデルの選択と完了	377
33.5.1. プリンター設定の確認	378
33.6. テストページの印刷	379
33.7. 既存プリンターの修正	379
33.7.1. 設定 タブ	379
33.7.2. ポリシー タブ	380
33.7.3. アクセス制御 タブ	381
33.7.4. プリンター および ジョブオプションタブ	382
33.8. 印刷ジョブの管理	384
33.9. 関連情報	385
33.9.1. インストールされているドキュメント	385
33.9.2. 便利な Web サイト	385
<b>第34章 自動タスク</b>	<b>387</b>
34.1. CRON	387
34.1.1. cron タスクの設定	387
34.1.2. cron へのアクセスの制御	389
34.1.3. サービスの起動と停止	390
34.2. AT および BATCH	390
34.2.1. at ジョブの設定	390
34.2.2. batch ジョブの設定	392
34.2.3. 保留中のジョブの表示	392
34.2.4. 追加のコマンドラインオプション	392
34.2.5. at と batch へのアクセスの制御	393
34.2.6. サービスの起動と停止	393
34.3. 関連情報	393
34.3.1. インストールされているドキュメント	393
<b>第35章 ログファイル</b>	<b>395</b>
35.1. ログファイルの場所の特定	395
35.2. ログファイルの表示	395
35.3. ログファイルの追加	397
35.4. ログファイルの検証	398
<b>第36章 カーネルの手動によるアップグレード</b>	<b>401</b>
36.1. カーネルパッケージの概要	401
36.2. アップグレードの準備	403
36.3. アップグレードされたカーネルのダウンロード	405
36.4. アップグレードの実行	406

36.5. 初期 RAM ディスクイメージの確認	406
36.6. ブートローダーの確認	407
36.6.1. x86 システム	407
36.6.1.1. GRUB	407
36.6.2. pidgin Systems	408
36.6.3. IBM S/390 および IBM eServer zSeries Systems	409
36.6.4. IBM eServer iSeries Systems	409
36.6.5. IBM eServer pSeries Systems	410
<b>第37章 カーネルモジュール</b> .....	<b>412</b>
37.1. カーネルモジュールユーティリティ	412
37.2. 永続的なモジュールの読み込み	415
37.3. 関連情報	415
37.3.1. インストールされているドキュメント	415
37.3.2. 便利な Web サイト	416
<b>第38章 メール転送エージェント (MTA) の設定</b> .....	<b>417</b>
<b>パート VI. システムモニタリング</b> .....	<b>419</b>
<b>第39章 システム情報の収集</b> .....	<b>420</b>
39.1. システムプロセス	420
39.2. MEMORY USAGE	423
39.3. ファイルシステム	425
39.4. ハードウェア	427
39.5. 関連情報	429
39.5.1. インストールされているドキュメント	429
<b>第40章 OPROFILE</b> .....	<b>431</b>
40.1. ツールの概要	432
40.2. OPROFILE の設定	433
40.2.1. カーネルの指定	433
40.2.2. 監視するイベントの設定	434
40.2.2.1. サンプリングレート	437
40.2.2.2. ユニットマスク	437
40.2.3. カーネルとユーザー空間プロファイルの分離	437
40.3. OPROFILE の起動および停止	439
40.4. データの保存	439
40.5. データの分析	440
40.5.1. opreportの使用	441
40.5.2. 単一の実行可能ファイルでの opreport の使用	441
40.5.3. opannotateの使用	444
40.6. /DEV/OPROFILE/について	444
40.7. 使用例	445
40.8. グラフィカルインターフェース	446
40.9. 関連情報	450
40.9.1. Installed Docs	450
40.9.2. 便利な Web サイト	450
<b>パート VII. 付録</b> .....	<b>451</b>
<b>付録A 改訂履歴</b> .....	<b>452</b>
<b>索引</b> .....	<b>452</b>



## はじめに

『『システム管理者のガイド』』 によろこそ。

『システム 『管理者ガイド』』 には、必要に応じて Red Hat Enterprise Linux システムをカスタマイズする方法が記載されています。ステップバイステップの、システムの設定およびカスタマイズのためのタスク指向のガイドが必要な場合には、これは手動で行います。このマニュアルでは、以下のような中間トピックを多数説明します。

- ネットワークインターフェースカード(NIC)の設定
- キックスタートインストールの実行
- Samba 共有の設定
- RPM を使用したソフトウェアの管理
- システムに関する情報の決定
- カーネルのアップグレード

このマニュアルは、以下の主要なカテゴリーに分類されます。

- インストール関連のリファレンス
- ファイルシステムのリファレンス
- パッケージ管理
- Network Configuration
- システム設定
- システムモニタリング

本書は、Red Hat Enterprise Linux システムに関する基本的な理解があることを前提としています。Red Hat Enterprise Linux のインストールに関するヘルプが必要な場合は、『インストール 『ガイド』』 を参照してください。システム管理に関する一般的な情報は、『システム管理者の 『概要』』 を参照してください。ファイルシステムの概要など、より高度なドキュメントが必要な場合は、『『リファレンスガイド』』 を参照してください。セキュリティ情報が必要な場合は『セキュリティ 『ガイド』』 を参照してください。

## 1. この手動の変更

このマニュアルは明確にするために変更されており、Red Hat Enterprise Linux 4 の最新機能で更新されています。変更には以下が含まれます。

### 『カーネルモジュール』の更新および『カーネルの』章の手動更新

カーネル 『モジュールおよびカーネル』 の 『手動アップグレード』 には、2.6 カーネルに関して更新された情報が含まれています。本章を完了するのに役立つハード作業のために **Arjan van de Ven** に特化しました。

### 更新され 『たネットワークファイルシステム(NFS)』の章

『ネットワークファイルシステム(NFS)』の章が修正され、NFSv4 を組み込むように再編成されました。本章を完了するのに役立つハード作業のために **Steve Dickson** に特化しました。

## Update Update 『OProfile』の章

『OProfile』の章が修正され、2.6 カーネルに関して更新された情報を組み込むように修正および再編成されました。本章を完了するのに役立つハード作業についての **Will Cohen** に特化しました。

## Update Update 『X Window System』の章

『X Window System の』章が修正され、X.Org チームが開発した X11R6.8 リリースに関する情報が追加されています。

本ガイドを読む前に、インストールの問題、基本的な管理概念のための『システム管理の概要』、一般的なカスタマイズ手順のための『システム管理者ガイド』、セキュリティー関連の手順については『『』セキュリティーガイド』を参照してください。『』本ガイドでは、上級ユーザーのトピックについて説明します。

## 2. 本書の表記慣例

本ガイドでは、いくつかの規則を使用して特定の単語やフレーズを強調表示し、特定の情報への注意を促しています。

### 2.1. 誤字規則

特定の単語や句への注意を促すために4つの表記慣習を使用しています。これらの規則や、これらが適用される状況は以下のとおりです。

#### 等幅ボールド

シェルコマンド、ファイル名、パスなど、システム入力を強調表示するために使用されます。キーとキーの組み合わせを強調表示するためにも使用されます。以下に例を示します。

現在の作業ディレクトリーのファイル **my\_next\_bestselling\_novel** の内容を表示するには、シェルプロンプトで **cat my\_next\_bestselling\_novel** コマンドを入力し、**Enter** を押してコマンドを実行します。

上記には、ファイル名、シェルコマンドおよびキーが含まれます。これはすべて等幅ボールドで表示され、コンテキストにより区別可能なものになります。

キーの組み合わせは、キーの組み合わせの各パーツをつなげるプラス記号によって個別のキーと区別できます。以下に例を示します。

**Enter** を押してコマンドを実行します。

**Ctrl+Alt+F2** を押して、仮想ターミナルに切り替えます。

最初の例では、押す特定のキーを強調表示しています。2つ目の例は、同時に押す3つのキーのセットというキーの組み合わせを強調表示しています。

ソースコードの場合、段落内で記述されるクラス名、メソッド、関数、変数名、および戻り値は、上記のように **等幅ボールド** で示されます。以下に例を示します。

ファイル関連のクラスには、ファイルシステムの **filesystem**、ファイルの **file**、ディレクトリーの **dir** が含まれます。各クラスには、独自の関連付けられたパーミッションセットがあります。

#### プロポーショナルボールド



これは、アプリケーション名、ダイアログボックステキスト、ラベルが付いたボタン、チェックボックスおよびラジオボタン、メニュータイトルおよびサブメニュータイトルなど、システムで発生した単語またはフレーズを示します。以下に例を示します。

メインメニューバーから **System** → **Preferences** → **Mouse** を選択し、**Mouse Preferences** を起動します。**Buttons** タブで、**Left-handed mouse** チェックボックスを選択し、**Close** をクリックしてメインのマウスボタンを左から右に切り替えます (マウスを左手で使い易くします)。

特殊文字を **gedit** ファイルに挿入するには、メインメニューバーから **Applications** → **Accessories** → **Character Map** を選択します。次に、**Character Map** メニューバーから **Search** → **Find...** を選択し、**Search** フィールドに文字の名前を入力して **Next** をクリックします。目的の文字が **Character Table** で強調表示されます。この強調表示した文字をダブルクリックして **Text to copy** フィールドに配置し、**Copy** ボタンをクリックします。ここでドキュメントに戻り、**gedit** メニューバーから **Edit** → **Paste** を選択します。

上記のテキストにはアプリケーション名、システム全体のメニュー名および項目、アプリケーション固有のメニュー名、GUI インターフェース内のボタンおよびテキストなどがあります。すべては proportional bold で示され、コンテキストと区別できます。

### 等幅ボールドイタリックまたは プロポーショナルボールドイタリック

等幅ボールドまたはプロポーショナルボールドのいずれでも、イタリックが追加されると、置換または変数テキストを意味します。イタリックは、状況に応じて変化するテキストや、文字を入力しないテキストを表します。以下に例を示します。

ssh を使用してリモートマシンに接続するには、シェルプロンプトで **ssh** **username@domain.name** を入力します。リモートマシンが **example.com** で、そのマシンのユーザー名が **john** の場合は、**ssh john@example.com** と入力します。

**mount -o remount file-system** コマンドは、指定したファイルシステムを再マウントします。たとえば、**/home** ファイルシステムを再マウントする場合には、コマンドは **mount -o remount /home** です。

現在インストールされているパッケージのバージョンを表示するには、**rpm -q** **package** コマンドを使用します。その結果が **package-version-release** のように返されます。

上記の太字のイタリック体の用語、username、domain.name、file-system、package、version、および release に注意してください。各単語はプレースホルダーで、コマンドの発行時に入力するテキストまたはシステムによって表示されるテキストのどちらかになります。

作業のタイトルを示す標準的な使用法のほかに、イタリックは新用語と重要な用語の最初の使用を示します。以下に例を示します。

Publican は *DocBook* 公開システムです。

## 2.2. 引用規則

端末の出力およびソースコードの一覧は、周りのテキストから視覚的に表示されます。

端末に送信される出力は、**mono-spaced roman** に設定され、次のように表示されます。

```
books Desktop documentation drafts mss photos stuff svn
books_tests Desktop1 downloads images notes scripts svgs
```

ソースコードの一覧も **mono-spaced roman** に設定されますが、構文強調表示を以下のように追加します。

```
static int kvm_vm_ioctl_deassign_device(struct kvm *kvm,
                                       struct kvm_assigned_pci_dev *assigned_dev)
{
    int r = 0;
    struct kvm_assigned_dev_kernel *match;

    mutex_lock(&kvm->lock);

    match = kvm_find_assigned_dev(&kvm->arch.assigned_dev_head,
                                  assigned_dev->assigned_dev_id);
    if (!match) {
        printk(KERN_INFO "%s: device hasn't been assigned before, "
               "so cannot be deassigned\n", __func__);
        r = -EINVAL;
        goto out;
    }

    kvm_deassign_device(kvm, match);

    kvm_free_assigned_device(kvm, match);

out:
    mutex_unlock(&kvm->lock);
    return r;
}
```

### 2.3. 注記および警告

最後に、3つの視覚的スタイルを使用して、見落とす可能性のある情報に注意を促します。



#### 注記

注記とは、タスクへのヒント、ショートカット、または代替アプローチです。注意を無視しても悪い結果を招くことはありませんが、便利なヒントを見逃してしまう可能性があります。



#### 重要

見落としやすい詳細のある重要なボックス: 現行セッションにのみ適用される設定変更や、更新を適用する前に再起動が必要なサービスなどです。「Important」というラベルが付いたボックスを無視しても、データが失われることはありませんが、スムーズな操作が行えないことがあります。



#### 警告

警告は無視すべきではありません。警告を無視すると、データが失われる可能性があります。

## 3. 詳細情報

『『システム管理者ガイド』』は、Red Hat Enterprise Linux ユーザーに有用で時間上のサポートを提供するために、Red Hat, Inc's 増加の取り組みの一部です。新しいツールおよびアプリケーションがリリースされると、本書は拡張され、それを組み込むように拡張されます。

### 3.1. フィードバックをお寄せください

『『システム管理者ガイド』』にエラーが見つかった場合や、このマニュアルを改善する方法を検討している場合は、ご連絡ください。コンポーネント **rh-sag** に対して Bugzilla(<http://bugzilla.redhat.com/bugzilla/>)でレポートを送信してください。

手動識別子を必ず言及してください。

rh-sag

このマニュアルの識別子について言及することで、どのバージョンのガイドがどのバージョンのものかを正確に知っています。

本ガイドを改善するためのご意見やご提案をお寄せいただく場合は、できるだけ具体的にご説明ください。エラーが見つかった場合は、簡単に確認できるように、セクション番号と前後のテキストを含めてください。

## パート I. インストール関連情報

『インストール 『ガイド』』では、Red Hat Enterprise Linux のインストールと、インストール後の基本的なトラブルシューティングについて説明します。ただし、高度なインストールオプションは本ガイドで説明しています。ここでは、キックスタート（自動インストール技術）とすべての関連ツールの手順を説明します。この部分は『インストール 『ガイド』』と共に使用し、これらの通常インストール』（Advanced installation）タスクのいずれかを実行します。

# 第1章 キックスタートを使ったインストール

## 1.1. キックスタートを使ったインストールとは

多くのシステム管理者は、マシンに Red Hat Enterprise Linux をインストールするための自動インストール方法を使用することが推奨されます。このニーズに対応するために、Red Hat, Inc ではキックスタートインストールの方法を作成しました。キックスタートを使用すると、システム管理者は、典型的なインストール時に通常尋ねられるすべての質問への回答を含む1つのファイルを作成できます。

キックスタートファイルを1つのサーバーに置くことで、インストール時に各コンピューターが読み込むことができます。このインストール方法は、1つのキックスタートファイルを使用して複数のマシンに Red Hat Enterprise Linux をインストールすることをサポートすることができるため、ネットワークおよびシステム管理者に適しています。

キックスタートは、Red Hat Enterprise Linux のインストールを自動化する方法を提供します。

## 1.2. キックスタートを使ったインストールの実行方法

キックスタートインストールでは、ローカルの CD-ROM、ローカルのハードドライブ、または NFS、FTP、または HTTP を使用して実行できます。

キックスタートを使用するには、以下を行う必要があります。

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を使用してブートメディアを作成するか、キックスタートファイルをネットワーク上で利用できるようにします。
3. インストールツリーを利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、これらの手順について詳しく見ていきます。

## 1.3. 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、それぞれキーワードで識別される項目の一覧を含むシンプルなテキストファイルです。Red Hat Enterprise Linux ドキュメント CD の **RH-DOCS** ディレクトリーにある **sample.ks** ファイルのコピーを編集し、**Kickstart Configurator** アプリケーションを使用するか、ゼロから作成することで作成できます。Red Hat Enterprise Linux インストールプログラムは、インストール時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。ファイルを ASCII テキストとして保存できるテキストエディターまたは単語プロセッサで編集できるはずです。

まず、キックスタートファイルを作成する場合に以下の問題に注意してください。

- 各セクションは**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については、特に指定がない限り順序は関係ありません。セクションの順序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については、「[キックスタートオプション](#)」を参照してください。必須のオプションを使用する必要があります。
  - **%packages** セクション：詳細は「[パッケージの選択](#)」を参照してください。

- **%pre** セクションおよび **%post** セクション - この2つのセクションは任意の順序で指定でき、必須ではありません。詳細は、「[インストール前のスクリプト](#)」および「[インストール後のスクリプト](#)」を参照してください。
- 必須項目以外は省略しても構いません。
- 必須項目が省略されている場合は、通常のインストール中のプロンプトと同様、インストールプログラムにより、その関連項目についての回答が求められます。回答を入力すると、インストールが自動的に続行されます (他にも省略されている部分があればその部分まで)。
- サウンド (またはハッシュ) 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。
- キックスタートの **アップグレード** には、以下の項目が必要です。
  - 言語
  - 言語サポート
  - インストール方法
  - デバイスの仕様 (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
  - ブートローダーの設定

アップグレードに他の項目を指定すると、これらのアイテムは無視されます (これにはパッケージの選択が含まれることに注意してください)。

## 1.4. キックスタートオプション

次のオプションは、キックスタートファイルに置くことができます。キックスタートファイルの作成にグラフィカルインターフェースを使用する場合は、**Kickstart Configurator** アプリケーションを使用します。詳細は、[2章 Kickstart Configurator](#) を参照してください。



### 備考

オプションの後に等号(=)が続く場合は、値を指定してから指定する必要があります。上記のコマンド例では、括弧([])内のオプションはオプションの引数です。

### autopart (オプション)

自動的にパーティションを作成する -1GB 以上の root(/)パーティション、swap パーティション、アーキテクチャーに適したブートパーティションデフォルトのパーティションサイズは、**part** ディレクティブで再定義できます。

### ignoredisk (任意)

インストーラーが、指定したディスクを無視するようにします。これは、自動パーティションを使用し、一部のディスクを無視したい場合に便利です。たとえば、**ignoredisk** を使用せずに SAN クラスタでデプロイしようとする、インストーラーが SAN へのパッシブパスを検出し、パーティションテーブルは返さないため、キックスタートが失敗します。

**ignoredisk** オプションは、ディスクへのパスが複数ある場合に便利です。

構文は以下のようになります。

```
ignoredisk --drives=drive1,drive2,...
```

*driveN* は、**sda**、**sdb** などのいずれかになります。

### autostep (オプション)

**interactive** と似ていますが、次の画面に移動します。これは主にデバッグに使用されます。

### auth または authconfig (必須)

システムの認証オプションを設定します。これは **authconfig** コマンドと似ていますが、インストール後に実行できます。デフォルトでは、パスワードは通常暗号化され、シャドウ化されません。

#### **--enablemd5**

ユーザーパスワードには **md5** 暗号化を使用します。

#### **--enablenis**

NIS サポートを有効にします。デフォルトでは、**--enablenis** はネットワーク上で検出したドメインを使用します。ほぼ常に **--nisdomain=** オプションで手動でドメインを設定する必要があります。

#### **--nisdomain=**

NIS サービスに使用する NIS ドメイン名。

#### **--nisserver=**

NIS サービスに使用するサーバー（デフォルトでは**broadcasts**）。

#### **--useshadow** または **--enableshadow**

シャドウパスワードを使用します。

**--enableldap**

`/etc/nsswitch.conf` の LDAP サポートをオンにし、システムで LDAP ディレクトリーからユーザー（UID、ホームディレクトリー、シェルなど）に関する情報を取得できるようにします。このオプションを使用するには、`nss_ldap` パッケージをインストールする必要があります。--ldapserver= および --ldapbasedn= で、サーバーとベース DN（識別名）も指定する必要があります。

**--enableldapauth**

LDAP を認証方法として使用します。これにより、認証に `pam_ldap` モジュールが有効になり、LDAP ディレクトリーを使用してパスワードを変更できます。このオプションを使用するには、`nss_ldap` パッケージがインストールされている必要があります。--ldapserver= および --ldapbasedn= でサーバーとクライアント DN も指定する必要があります。

**--ldapserver=**

--enableldap または --enableldapauth のいずれかを指定した場合は、このオプションを使用して使用する LDAP サーバーの名前を指定します。このオプションは `/etc/ldap.conf` ファイルに設定されます。

**--ldapbasedn=**

--enableldap または --enableldap auth のいずれかを指定した場合は、このオプションを使用してユーザー情報が保存される LDAP ディレクトリーツリーに DN を指定します。このオプションは `/etc/ldap.conf` ファイルに設定されます。

**--enableldaptls**

TLS(Transport Layer Security)ルックアップを使用します。このオプションを使用すると、認証前に LDAP が暗号化され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**

ユーザーの認証に Kerberos 5 を使用します。Kerberos 自体はホームディレクトリー、UID、シェルなどを認識しません。Kerberos を有効にする場合、LDAP、NIS、または Hesiod を有効にするか、`/usr/sbin/useradd` コマンドを使用してアカウントをこのワークステーションで認識させることで、ユーザーのアカウントをこのワークステーションを認識させる必要があります。このオプションを使用する場合は、`pam_krb5` パッケージがインストールされている必要があります。



**--krb5realm=**

ワークステーションが属する Kerberos 5 レルム。

**--krb5kdc=**

レルムの要求を処理する KDC (または KDC) レルムに複数の KDC がある場合は、名前をコンマ(,)で区切ります。

**--krb5adminserver=**

kadmind も実行しているレルムの KDC。このサーバーでパスワードの変更やその他の管理要求を処理します。複数の KDC を設置する場合、このサーバーはマスターの KDC で実行する必要があります。

**--enablehesiod**

ユーザーのホームディレクトリー、UID、およびシェルを検索するために Hesiod サポートを有効にします。ネットワーク上で Hesiod を設定および使用する方法は、glibc パッケージに含まれる /usr/share/doc/glibc-2.x.x/README.hesiod を参照してください。Hesiod は DNS の拡張機能になります。DNS レコードを使ってユーザー、グループ、その他の情報を格納します。

**--hesiodlhs**

Hesiod LHS("left-hand side")オプションは、/etc/hesiod.conf で設定します。このオプションは、LDAP がベース DN の使用と同様に、情報検索時に DNS を検索する名前を決定するために Hesiod ライブラリーによって使用されます。

**--hesiodrhs**

/etc/hesiod.conf で設定される Hesiod RHS(right-hand side)オプション。このオプションは、LDAP がベース DN の使用と同様に、情報検索時に DNS を検索する名前を決定するために Hesiod ライブラリーによって使用されます。



## ヒント

ユーザー情報を "jim" で検索するには、Hesiod ライブラリーが `jim.passwd<LHS><RHS>` を検索し、`passwd` エントリーがどのように見えるかを示す TXT レコードに解決されます (`jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`)。グループの場合、`jim.group<LHS><RHS>`; 以外は同じになります。

ユーザーおよびグループを番号で検索するには、「501.uid」を「jim.passwd」の CNAME に、「501.gid」を「jim.group」に設定します。LHS と RHS にはピリオドがないため、ライブラリーの前に検索する名前を決定すると、LHS と RHS は通常ピリオドで始まります。

### --enablesmbauth

SMB サーバー（通常は 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 認証サポートでは、ホームディレクトリ、UID、シェルなどは認識しません。SMB を有効にする場合、LDAP、NIS、または Hesiod を有効にするか、`/usr/sbin/useradd` コマンドを使用してアカウントをワークステーションに認識させることで、ユーザーアカウントがワークステーションを認識できるようにする必要があります。このオプションを使用するには、`pam_smb` パッケージがインストールされている必要があります。

### --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、名前をコンマ(,)で区切ります。

### --smbworkgroup=

SMB サーバーのワークグループの名前。

### --enablecache

`nscd` サービスを有効にします。`nscd` サービスは、ユーザー、グループ、およびその他の種類の情報に関する情報をキャッシュします。NIS、LDAP、または `hesiod` を使用してネットワーク上でユーザーおよびグループに関する情報を配信する場合、キャッシュは特に便利です。

**bootloader (必須)**

**GRUB** ブートローダーをインストールする方法を指定します。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、**GRUB** が現在のブートローダーではない場合は、ブートローダーが **GRUB** に変更になります。その他のブートローダーを保持するには、`bootloader --upgrade` を使用します。

#### **--append=**

カーネルパラメーターを指定します。複数のパラメーターを指定する場合は空白で区切ります。以下に例を示します。

```
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
```

#### **--driveorder**

**BIOS** ブート順で、どのドライブを最初に指定してください。以下に例を示します。

```
bootloader --driveorder=sda,hda
```

#### **--location=**

ブートレコードの書き込み先を指定します。有効な値は、`mbr`（デフォルト）、`partition`（カーネルを含むパーティションの最初のセクター）、または `none`（ブートローダーをインストールしません）です。

#### **--password=**

**GRUB** ブートローダーのパスワードを、このオプションで指定したパスワードに設定します。任意のカーネルオプションが渡される可能性のある **GRUB** シェルへのアクセスを制限する場合に使用できます。

#### **--md5pass=**

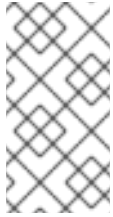
`--password=` と同様に、パスワードがすでに暗号化されているはずですが。

#### **--upgrade**

既存のブートローダー設定をアップグレードして、古いエントリーを保持します。このオプションは、アップグレード時にのみ利用できます。

## clearpart (オプション)

新しいパーティションを作成する前に、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。



備考

`clearpart` コマンドを使用する場合は、`--onpart` コマンドを論理パーティションで使用できません。

### `--all`

システムからすべてのパーティションを消去します。

### `--drives=`

パーティションを消去するドライブを指定します。次の例では、プライマリー IDE コントローラーの 1 番目と 2 番目のドライブにあるパーティションをすべて消去することになります。

```
clearpart --drives=hda,hdb --all
```

### `--initlabel`

アーキテクチャーのデフォルトにディスクラベルを初期化します（例：x86 の場合は `msdos`、`pidt` の場合は `gpt`）。ブランドの新しいハードドライブにインストールする場合に、インストールプログラムがディスクラベルを初期化するかどうかを要求しないと便利です。

### `--linux`

すべての Linux パーティションを消去します。

### `--none` (デフォルト)

パーティションは削除しないでください。

## cmdline (任意)

完全に非対話式のコマンドラインモードでインストールを実行します。対話プロンプトがあるとインストールは停止します。このモードは、x3270 コンソールを使用する S/390 システムに便利です。

### device (任意)

ほとんどの PCI システムでは、イーサネットカードおよび SCSI カード用のインストールプログラムの `autoprobe` が適切に行われます。しかし、以前のシステムと一部の PCI システムでは、適切なデバイスを見つけるためにキックスタートにヒントが必要です。追加モジュールをインストールするようにインストールプログラムに指示する `device` コマンドは以下の形式になります。

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

<type>

`scsi` または `eth` に置き換えます。

<moduleName>

インストールするカーネルモジュールの名前に置き換えます。

--opts=

NFS エクスポートのマウントに使用するマウントオプション。NFS マウントの `/etc/fstab` で指定できるオプションはすべて許可されます。オプションは、`man` ページの `nfs(5)` に記載されています。複数のオプションはカンマで区切られます。

### driverdisk (任意)

キックスタートインストール中にドライバーのディスクを使用できます。ドライバーディスクのコンテンツを、システムのハードドライブにあるパーティションのルートディレクトリーにコピーする必要があります。次に、`driverdisk` コマンドを使用して、ドライバーディスクを検索する場所をインストールプログラムに通知する必要があります。

```
driverdisk <partition> [--type=<fstype>]
```

ドライバーディスク用にネットワークの場所を指定することもできます。

```
driverdisk --source=ftp://path/to/dd.imgdriverdisk --source=http://path/to/dd.imgdriverdisk --source=nfs:host:/path/to/img
```

**<partition>**

ドライバードискを含むパーティション。

**--type=**

ファイルシステムのタイプ (vfat または ext2)。

## ファイアウォール (任意)

このオプションは、インストールプログラムの Firewall Configuration 画面に対応します。

```
firewall --enabled|--disabled [--trust=] <device> [--port=]
```

**--enabled**

DNS 応答や DHCP 要求など、送信要求に応答しない受信接続を拒否します。このマシンで実行中のサービスへのアクセスが必要な場合は、特定サービスに対してファイアウォールの通過許可を選択できます。

**--disabled**

iptables ルールは設定しないでください。

**--trust=**

eth0 などのデバイスを一覧表示すると、そのデバイスから送信されるすべてのトラフィックがファイアウォールを通過できるようになります。複数のデバイスを一覧表示するには、`--trust eth0 --trust eth1` を使用します。`--trust eth0`、`eth1` などのカンマ区切りの形式を使用しないでください。

**<incoming>**

指定したサービスがファイアウォールを通過できるように、以下のいずれかに置き換えます。

- `--ssh`

- `--telnet`
- `--smtp`
- `--http`
- `--ftp`

#### `--port=`

`port:protocol` 形式を使用して、ファイアウォールでポートが許可されるように指定できます。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` を指定します。数値ポートは明示的に指定することもできます。たとえば、ポート 1234 の UDP パケットを許可するには、`1234:udp` を指定します。複数のポートを指定する場合は、コンマで区切って指定します。

#### `firstboot` (オプション)

システムの初回起動時に セットアップエージェント が起動するかどうかを決定します。有効な場合は、`firstboot` パッケージをインストールする必要があります。何も指定しないとデフォルトで無効になるオプションです。

#### `--enable`

Setup Agent は、システムの初回起動時に起動します。

#### `--disable`

Setup Agent は、システムの初回起動時に開始されません。

#### `--reconfig`

設定エージェントが 起動時 に再設定モードで起動するようにします。このモードでは、デフォルトのオプションに加えて、言語、マウス、キーボード、`root` パスワード、セキュリティレベル、タイムゾーン、ネットワーク設定オプションを使用できます。

## halt (任意)

インストールが正常に完了するとシステムを一時停止します。手動インストールと類似しており、`anaconda` にはメッセージが表示され、ユーザーがキーを押すのを待ってから再起動が行われます。キックスタートインストール中に、完了方法が指定されていない場合には、`reboot` オプションがデフォルトで使用されます。

`halt` オプションは `shutdown -h` コマンドとほぼ同じです。

その他の完了方法は、電源オフ、再起動、およびシャットダウンのキックスタートオプションを参照してください。

## インストール (任意)

既存システムをアップグレードするのではなく、システムに新規システムをインストールするように指示します。これがデフォルトのモードです。インストールには、`cdrom`、`harddrive`、`nfs`、または `url` (FTP または HTTP のインストール用) からインストールのタイプを指定する必要があります。`install` コマンド自体とインストール方法を指定するコマンドは別々の行で指定してください。

### 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

ローカルドライブの Red Hat インストールツリーからインストールします。これは `vfat` または `ext2` のいずれかでなければなりません。

- `--partition=`  
  
インストール元となるパーティション (`sdb2` など)。
- `--dir=`



インストールツリーの RedHat ディレクトリーを含むディレクトリー。

以下に例を示します。

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

## nfs

指定した NFS サーバーからインストールします。

- `--server=`

インストール元となるサーバー（ホスト名または IP）。

- `--dir=`

インストールツリーの RedHat ディレクトリーを含むディレクトリー。

以下に例を示します。

```
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ーのインストールツリーからインストールします。

以下に例を示します。

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

または

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

### interactive (任意)

インストール時にキックスタートファイルで提供された情報を使用しますが、指定した値を検証および変更できます。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。Next をクリックして値を使用するか、値を変更して Next をクリックして続行します。autostep コマンドを参照してください。

### keyboard (必須)

システムのキーボードタイプを設定します。以下は、i386、Warehouse、および Alpha マシンで利用可能なキーボードの一覧です。

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-noddeadkeys, 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, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querly, slovene, trq, ua,
uk, us, us-acentos
```

/usr/lib/python2.2/site-packages/rhpl/keyboard\_models.py ファイルにはこの一覧が含まれ、rhpl パッケージに含まれています。

### 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、言語を英語に設定するには、キックスタートファイルに以下の行が含まれている必要があります。

```
lang en_US
```

/usr/share/system-config-language/locale-list ファイルには、各行の最初の列に有効な言語コードの一覧があり、system-config-language パッケージに含まれています。

### 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 で使用されるものと同じ言語コードは langsupport と合わせて使用できます。

1つの言語をインストールするには、それを指定します。たとえば、フランス語の言語 `fr_FR` をインストールして使用するには、次のコマンドを実行します。

```
langsupport fr_FR
```

#### **--default=**

複数の言語の言語サポートが指定されている場合は、デフォルトを指定する必要があります。

たとえば、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、以下を実行します。

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

1つの言語でのみ **--default** を使用すると、すべての言語がデフォルトに設定された指定の言語でインストールされます。

## **logvol (任意)**

構文で論理ボリューム管理(LVM)に論理ボリュームを作成します。

```
logvol <mntpoint> --vgname=<name> --size=<size> --name=<name><options>
```

オプションは次のとおりです。

#### **--noformat**

既存の論理ボリュームを使用し、フォーマットは行いません。

#### **--useexisting**

既存の論理ボリュームを使用し、再フォーマットします。

#### **--pesize**

物理エクステンツのサイズを設定します。

まずパーティションを作成します。次に論理ボリュームグループを作成して、論理ボリュームを作成します。以下に例を示します。

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

logvol in アクションの詳細な説明は、「[高度なパーティション設定の例](#)」を参照してください。

### mouse (必須)

GUI モードとテキストモードの両方で、システムのマウスを設定します。オプションは以下のとおりです。

**--device=**

マウスが置かれるデバイス (例: `--device=ttyS0`) 。

**--emulthree**

存在する場合は、左および右のマウスボタンの同時クリックは、X Window System によって中間マウスボタンとして認識されます。2つのボタンボタンがある場合は、このオプションを使用する必要があります。

オプション後、マウスタイプは以下のいずれかとして指定できます。

```
alpsps/2, ascii, asciips/2, atibm, generic, generic3, genericps/2,
generic3ps/2, genericwheels/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 パッケージに含まれる `/usr/lib/python2.2/site-packages/rhpl/mouse.py` ファイルでも確認することができます。

`mouse` コマンドを引数なしで指定するか、省略すると、インストールプログラムはマウスを自動的に検出しようとします。この手順は、最新のマウスで動作します。

## ネットワーク (任意)

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が必要ない場合（つまり、NFS、HTTP、または FTP でインストールされていない場合）、ネットワークがシステム用に設定されていません。インストールにネットワークが必要で、ネットワーク情報が指定されていない場合には、インストールプログラムは動的 IP アドレス(BOOTP/DHCP)で `eth0` でインストールを行う必要があり、最後にインストールされたシステムを設定して IP アドレスを動的に判断します。`network` オプションは、ネットワークおよびインストール済みシステムを使用して、キックスタートインストールのネットワーク情報を設定します。

### --bootproto=

`dhcp`、`bootp`、または `static` のいずれか。

デフォルトは `dhcp` です。BOOTP と `dhcp` は同じように処理されます。

DHCP メソッドでは、DHCP サーバーシステムを使用してネットワーク構成を取得します。分かるように、BOOTP メソッドも同様に、BOOTP サーバーがネットワーク設定を提供する必要があります。システムが DHCP を使用するようになる場合は、以下のように指定します。

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

BOOTP を使用してネットワーク構成を取得する場合は、キックスタートファイルで次の行を使用します。

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

`static` メソッドでは、キックスタートファイルに必要なすべてのネットワーク情報を入力する必要があります。この名前が示すように、この情報は静的で、インストール時およびインストール後に使用されます。1 行にすべてのネットワーク設定情報を含める必要があるため、静的ネットワークの行は複雑になります。IP アドレス、ネットマスク、ゲートウェイ、およびネームサーバーを指定する必要があります。たとえば、"`"` はこれを 1 つの連続行として読み取る必要があることを示します。

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

**static** メソッドを使用する場合は、以下の 2 つの制限に注意してください。

- 静的ネットワーク設定情報はすべて 1 行で指定する必要があります。バックslash ラッシュなどを使用して行をラップすることはできません。
- ここでは、複数のネームサーバーを設定することもできます。これを行うには、コマンドラインでコンマ区切りリストで指定します。以下に例を示します。

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 \  
--gateway=10.0.2.254 --nameserver 192.168.2.1,192.168.3.1
```

#### **--device=**

インストール用の特定のイーサネットデバイスを選択するために使用されます。インストールプログラムがキックスタートファイルを検索するようにネットワークを設定するため、**--device=** の使用は有効ではありません（**ks=floppy** など）。以下に例を示します。

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

#### **--ip=**

インストールするマシンの IP アドレス。

#### **--gateway=**

IP アドレスとしてのデフォルトゲートウェイ。

#### **--nameserver=**

プライマリーネームサーバー（IP アドレス）

#### **--nodns**

DNS サーバーは設定しないでください。

**--netmask=**

インストール済みシステムのネットマスク。

**--hostname=**

インストール済みシステムのホスト名

**--nostorage**

ISCSI、IDE、RAID などの自動プローブストレージデバイスを使用しないでください。

**part** または **partition** (インストールに必要。アップグレードで無視)

システムにパーティションを作成します。

異なるパーティションのシステムに複数の Red Hat Enterprise Linux インストールが存在する場合は、インストールプログラムにより、アップグレードを尋ねるよう求められます。



#### WARNING

--noformat および --onpart が使用されていない限り、作成されたパーティションはすべてインストールプロセスの一部としてフォーマットされます。

アクションの一部の詳細な例は、「[高度なパーティション設定の例](#)」を参照してください。

**<mntpoint>**

**<mntpoint>** は、パーティションをマウントする場所です。次のいずれかの形式になります。

- `<path>`

例： `/, /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。

自動的に `swap` パーティションのサイズを確認するには、`--recommended` オプションを使用します。

```
swap --recommended
```

自動生成されたスワップパーティションの最小サイズは、システムの RAM 容量よりも小さく、システム内の RAM 容量よりも大きくなります。

推奨 オプションを使用すると、`swap` パーティションに 8GB に制限されます。より大きな `swap` パーティションを作成する場合は、キックスタートファイルに正しいサイズを指定するか、パーティションを手動で作成します。

- `RAID. <id>`

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

- `pv.<id>`

このパーティションは LVM に使用されます（`logvol`を参照）。

`--size=`

パーティションの最小サイズをメガバイト単位で指定します。500 などの整数値を指定します。数値には `MB` を追記しないでください。



**--grow**

利用可能な領域（存在する場合）を埋めるか、最大サイズ設定まで埋めるためにパーティションに指示します。

**--maxsize=**

パーティションが **grow** に設定されている場合の最大サイズ（メガバイト単位）。ここで整数値を指定し、**MB** で数値を追加しないでください。

**--noformat**

インストールプログラムがパーティションをフォーマットしないように、**--onpart** コマンドで使用するよう指示します。

**--onpart= または --usepart=**

既存のデバイスにパーティションを配置します。以下に例を示します。

```
partition /home --onpart=hda1
```

**/home** を **/dev/hda1** に配置しますが、これは存在している必要があります。

**--ondisk= or --ondrive=**

特定のディスクに強制的にパーティションを作成します。たとえば、**--ondisk=sdb** は、2番目の SCSI ディスクにパーティションを配置します。

**--asprimary**

プライマリーパーティションとしてパーティションの自動割り当てを強制しないと、パーティション設定は失敗します。

**--type=**（**fstype**に置換）

このオプションは利用できなくなりました。fstype を使用します。

#### --fstype=

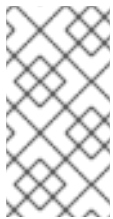
パーティションのファイルシステムタイプを設定します。有効な値は、ext2、ext3、swap、および vfat です。

#### --start=

パーティションの最初の周期を指定します。ドライブに --ondisk= または ondrive= を指定する必要があります。また、--end= で終わるシリンダーを指定するか、--size= でパーティションサイズを指定する必要があります。

#### --end=

パーティションの終わるシリンダーを指定します。開始したシリア語は --start= で指定する必要があります。



#### 備考

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 に表示されます。

#### 電源オフ (任意)

インストールが正常に完了したら、システムをシャットダウンして電源を切ります。通常、手動インストール時に anaconda はメッセージが表示され、ユーザーがキーを押すのを待ってから再起動します。キックスタートインストール中に、完了方法が指定されていない場合には、reboot オプションがデフォルトで使用されます。

poweroff オプションは shutdown -p コマンドにほぼ同等です。



## 備考

poweroff オプションは、使用中のシステムハードウェアに大きく依存します。特に、BIOS、APM (advanced power management)、ACPI (advanced configuration and power interface) などの特定ハードウェアコンポーネントは、システムカーネルと対話できる状態にする必要があります。お使いのシステムの APM/ACPI 機能の詳細については、製造元にお問い合わせください。

その他の完了方法は、halt、reboot、shutdown などのキックスタートオプションを参照してください。

## RAID (任意)

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 ファイルシステムがマウントされている場所。/ にマウントする場合、boot パーティション (/boot) がなければ RAID レベルは 1 にする必要があります。boot パーティションがある場合は、/boot パーティションをレベル 1 にしてください。ルート (/) パーティションのタイプはどれでも構いません。< ;partitions\* > (複数のパーティションを表示できることを示し) は、RAID アレイに追加する RAID 識別子を一覧表示します。

### --level=

使用する RAID レベル (1、または 5)

### --device=

使用する RAID デバイスの名前 (md0、md1 など)。RAID デバイスの範囲は md0 から md7 までで、それぞれを 1 回しか使用することができません。

### --spares=

RAID アレイに割り当てられるスペアドライブの数を指定します。スペアドライブは、ドライブに障害が発生した場合にアレイの再構成に使用されます。

**--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`、および `vfat` です。

**--noformat**

既存の RAID デバイスを使用し、RAID アレイをフォーマットしないでください。

**--useexisting**

既存の RAID デバイスを使用して再フォーマットします。

以下の例では、`/` に RAID レベル 1 のパーティションを作成し、`/usr` に RAID レベル 5 を作成します。ここでは、システムには SCSI ディスクが 3 つあることが前提です。各ドライブに 1 つずつ、3 つの `swap` パーティションを作成します。

```
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
```

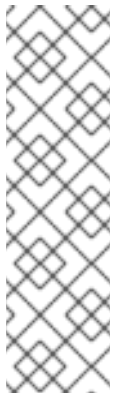
```
raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

`raid` の動作の詳細な説明は、[「高度なパーティション設定の例」](#) を参照してください。

**reboot (任意)**

インストールが正常に完了したら再起動します (引数なし)。通常、手動インストール時に `anaconda` はメッセージが表示され、ユーザーがキーを押すのを待ってから再起動します。

reboot オプションは shutdown -r コマンドとほぼ同じです。



#### 備考

インストールメディアや方法によっては、reboot オプションを使用すると、無限のインストールループが発生することがあります。

キックスタートファイルに他の方法が明示的に指定されていない場合は、reboot オプションがデフォルトの完了方法になります。

その他の完了方法は、halt、poweroff、shutdown などのキックスタートオプションをご覧ください。

#### rootpw (必須)

システムの root パスワードを `<password>` 引数に設定します。

```
rootpw [--iscrypted] <password>
```

#### --iscrypted

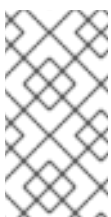
これが存在する場合は、パスワードの引数がすでに暗号化されていると見なされます。

#### SELinux (任意)

システムの SELinux モードを、次のいずれかの引数に設定します。

#### --enforcing

SELinux を、強制するデフォルトのターゲットポリシーで有効にします。



#### 備考

selinux オプションがキックスタートファイルに存在しない場合は、SELinux が有効になり、デフォルトで --enforcing に設定されます。

**--permissive**

SELinux ポリシーに基づいてのみ警告を出力しますが、実際にはポリシーを強制しません。

**--disabled**

システムで SELinux を完全に無効にします。

Red Hat Enterprise Linux の SELinux に関する詳細は、『Red Hat, Inc』を参照してください。

**shutdown (任意)**

インストールが正常に完了したらシステムをシャットダウンします。キックスタートインストール中に、完了方法が指定されていない場合には、reboot オプションがデフォルトで使用されません。

shutdown オプションは shutdown コマンドにほぼ同等です。

その他の完了方法は、halt、poweroff、および reboot のキックスタートオプションを参照してください。

**skipx (任意)**

存在する場合は、インストール済みシステムで X が設定されていません。

**text (任意)**

テキストモードでキックスタートインストールを実行します。キックスタートインストールは、デフォルトでグラフィカルモードで実行します。

**timezone (必須)**

システムのタイムゾーンを < timezone > に設定します。これは、timeconfig で一覧表示されるタイムゾーンのいずれかになります。

```
timezone [--utc] <timezone>
```

■

**--utc**

ハードウェアクロックが存在する場合は、ハードウェアクロックが UTC (グリニッジ標準) 時間に設定されていることを前提としています。

**upgrade (オプション)**

システムに、新規システムをインストールするのではなく、既存の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`、`harddrive`、`nfs`、または `url` (FTP および HTTP 用) のいずれかを指定する必要があります。詳細は、`install` を参照してください。

**xconfig (任意)**

X Window System を設定します。このオプションを指定しないと、X がインストールされている場合は、インストール時に X を手動で設定する必要があります。X が最終システムにインストールされていない場合は、このオプションを使用しないでください。

**--noprobe**

モニターをプローブしないでください。

**--card=**

指定したカードを使用します。このカード名は、`hwdata` パッケージの `/usr/share/hwdata/Cards` 内のカード一覧から取得する必要があります。カードの一覧は、Kickstart Configurator の X Configuration 画面でも見つけることができます。この引数を指定しないと、インストールプログラムはカードの PCI バスをプローブします。AGP は PCI バスの一部であるため、サポートされている場合は AGP カードが検出されます。プローブの順序は、マザーボードの PCI スキャン順序により決定されます。

**--videoram=**

ビデオカードのビデオ RAM の容量を指定します。

**--monitor=**

指定したモニターを使用します。モニター名は、`hwdata` パッケージの `/usr/share/hwdata/MonitorsDB` の監視一覧にある必要があります。モニターの一覧は、Kickstart Configurator の X 設定画面で確認できます。--hsync または --vsync が指定され

ている場合は無視されます。モニター情報が指定されていない場合には、インストールプログラムはこのモニター情報を自動的にプローブしようとします。

**--hsync=**

モニターの水平の同期頻度を指定します。

**--vsync=**

モニターの垂直の同期頻度を指定します。

**--defaultdesktop=**

GNOME または KDE のいずれかを指定して、デフォルトのデスクトップを設定します (GNOME デスクトップ環境または KDE Desktop Environment が %packages でインストールされていることを前提とします)。

**--startxonboot**

インストール済みシステムでグラフィカルログインを使用します。

**--resolution=**

インストール済みシステムの X Window System のデフォルトの解像度を指定します。有効な値は 640x480、800x600、1024x768、1152x864、1280x1024、1400x1050、1600x1200 です。ビデオカードおよびモニターと互換性のある解決を必ず指定してください。

**--depth=**

インストール済みシステムの X Window System のデフォルトの色深度を指定します。有効な値は 8、16、24、および 32 です。ビデオカードおよびモニターと互換性のある色深度を指定してください。

**volgroup (任意)**

構文で論理ボリューム管理(LVM)グループを作成します。



```
volgroup <name><partition><options>
```

オプションは次のとおりです。

#### **--noformat**

既存のボリュームグループを使用し、フォーマットは行いません。

#### **--useexisting**

既存のボリュームグループを使用して、ボリュームグループを再フォーマットします。

まずパーティションを作成します。次に論理ボリュームグループを作成して、論理ボリュームを作成します。以下に例を示します。

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

**volgroup** の動作の詳細な説明は、[「高度なパーティション設定の例」](#) を参照してください。

#### **zerombr (任意)**

**zerombr** を指定し、**yes** がその唯一の引数である場合は、ディスクにある無効なパーティションテーブルが初期化されます。これにより無効なパーティションテーブルが含まれるディスクの内容がすべて破棄されます。このコマンドは、以下の形式でなければなりません。

```
zerombr yes
```

他の形式は有効ではありません。

#### **%include**

**%include /path/to/file** コマンドを使用して、キックスタートファイル内の別のファイルのコンテンツが、キックスタートファイルの **%include** コマンドの場所にあるかのように組み込みます。

#### 1.4.1. 高度なパーティション設定の例

以下は、`clearpart`、`raid`、`part`、`volgroup`、および `logvol` キックスタートのオプションの動作を示す単一の統合例です。

```
clearpart --drives=hda,hdc --initlabel

# Raid 1 IDE config
part raid.11 --size 1000 --asprimary --ondrive=hda
part raid.12 --size 1000 --asprimary --ondrive=hda
part raid.13 --size 2000 --asprimary --ondrive=hda
part raid.14 --size 8000 --ondrive=hda
part raid.15 --size 1 --grow --ondrive=hda

part raid.21 --size 1000 --asprimary --ondrive=hdc
part raid.22 --size 1000 --asprimary --ondrive=hdc
part raid.23 --size 2000 --asprimary --ondrive=hdc
part raid.24 --size 8000 --ondrive=hdc
part raid.25 --size 1 --grow --ondrive=hdc

# You can add --spares=x
raid / --fstype ext3 --device md0 --level=RAID1 raid.11 raid.21
raid /safe --fstype ext3 --device md1 --level=RAID1 raid.12 raid.22
raid swap --fstype swap --device md2 --level=RAID1 raid.13 raid.23
raid /usr --fstype ext3 --device md3 --level=RAID1 raid.14 raid.24
raid pv.01 --fstype ext3 --device md4 --level=RAID1 raid.15 raid.25

# LVM configuration so that we can resize /var and /usr/local later
volgroup sysvg pv.01
logvol /var --vgname=sysvg --size=8000 --name=var
logvol /var/freespace --vgname=sysvg --size=8000 --name=freespacetouse
logvol /usr/local --vgname=sysvg --size=1 --grow --name=usrlocal
```

この高度な例では、RAID を使用した LVM や、将来的なデータの増加に応じてさまざまなディレクトリーのサイズを変更できる機能が実装されています。

## 1.5. パッケージの選択

`%packages` コマンドを使用して、インストールするパッケージを一覧表示するキックスタートファイルセクションを開始します（アップグレード時のパッケージの選択はサポートされていないため、これはインストール専用です）。

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できます。インストールプログラムは、関連パッケージを含む複数のグループを定義します。グループの一覧は、最初の Red Hat Enterprise Linux CD-ROM の `RedHat/base/comps.xml` ファイルを参照してください。各グループには、`id`、`user visibility value`、`name`、`description`、および `package list` があります。パッケージリストでは、グループが選択された場合に `mandatory` とマークされたパッケージが常にインストールされ、グループが選択された場合に `default` とマークされたパッケージがデフォルトで選択され、`optional` と

マークされたパッケージは、グループをインストールするように選択された場合でも、特に `optional` とマークされたパッケージを選択する必要があります。

多くの場合、個々のパッケージではなく、必要なグループのみを一覧表示する必要があります。Core グループおよび Base グループは常にデフォルトで選択されるため、`%packages` セクションで指定する必要はありません。

`%packages` 選択例を以下に示します。

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

ご覧のとおり、グループを指定すると行に1つ、`@` 記号、スペース、および `comps.xml` ファイルで指定した完全なグループ名から始まります。グループは、`gnome-desktop` などのグループの `id` を使用して指定することもできます。追加文字なしで個々のパッケージを指定します（上記の例の `dhcp` 行は、個別パッケージです）。

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。

```
-autofs
```

`%packages` オプションでは、以下のオプションを使用できます。

```
--resolvedeps
```

一覧表示されたパッケージをインストールして、パッケージの依存関係を自動的に解決します。このオプションが指定されておらず、パッケージの依存関係がある場合は、自動インストールが一時停止し、ユーザーにプロンプトが表示されます。以下に例を示します。

```
%packages --resolvedeps
```

```
--ignoredeps
```

解決できない依存関係を無視し、依存関係なしでリストされたパッケージをインストールします。以下に例を示します。

```
%packages --ignoredeps
```

**--ignoremissing**

インストールを停止する代わりに、足りないパッケージとグループを無視して、インストールを中断するか、または継続するかを確認してください。以下に例を示します。

```
%packages --ignoremissing
```

## 1.6. インストール前のスクリプト

`ks.cfg` が解析された直後に、システムで実行するコマンドを追加できます。このセクションは、キックスタートファイルの最後（コマンド後）にある必要があり、`%pre` コマンドで開始する必要があります。`%pre` セクションでネットワークにアクセスできますが、`name` サービスはこの時点では設定されていないため、IP アドレスのみが機能します。



## 備考

`pre-install` スクリプトは、`root` 環境では実行されないことに注意してください。

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

Python などの別のスクリプト言語を指定できます。`/usr/bin/python` は、任意のスクリプト言語に置き換えます。

## 1.6.1. 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
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-include
  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数を判定して、ドライブ数が1台または2台に合わせて、異なるパーティション設定スキー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を設定する代わりに、以下の行を追加します。

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

スクリプトで選択したパーティション設定コマンドが使用されます。



#### 備考

キックスタートの事前インストールスクリプトセクションは、複数のインストールツリーやソースメディアを管理できません。インストールプロセスの2番目の段階でインストールスクリプトが行われるため、作成した `ks.cfg` ファイルごとにこの情報を含める必要があります。

### 1.7. インストール後のスクリプト

インストールが完了したら、システムで実行するコマンドを追加するオプションがあります。このセクションは、キックスタートファイルの最後にあり、`%post` コマンドで開始する必要があります。本

セクションは、追加のソフトウェアのインストールや、追加のネームサーバーの設定などの機能に便利です。



#### 備考

ネットワークにネームサーバーを含む静的 IP 情報を設定した場合は、ネットワークにアクセスして、`%post` セクションで IP アドレスを解決できます。ネットワークを DHCP 用に設定している場合、インストールが `%post` セクションを実行すると、`/etc/resolv.conf` ファイルは完了しません。ネットワークにはアクセスできますが、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は、`%post` セクションに IP アドレスを指定する必要があります。



#### 備考

インストール後のスクリプトは `chroot` 環境で実行するため、インストールメディアからスクリプトや RPM をコピーするなどのタスクを実行することはできません。

#### `--nochroot`

`chroot` 環境外で実行するコマンドを指定できます。

以下の例では、ファイル `/etc/resolv.conf` をインストールされたばかり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 などの別のスクリプト言語を指定できます。`/usr/bin/python` は、任意のスクリプト言語に置き換えます。

### 1.7.1. 例

サービスのオンとオフを切り替えます。

```
/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` という名前のスクリプトを実行します。

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



#### 備考

NFS ファイルのロックはキックスタートモードでは対応していないため、NFS マウントをマウントする際に `-o nolock` が必要です。

ユーザーをシステムに追加します。

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

## 1.8. キックスタートファイルの準備

キックスタートファイルは、以下のいずれかの場所に配置する必要があります。

- ブートディスクチット
- ブート CD-ROM の場合
- 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またはネットワーク上で利用可能にされます。ほとんどのキックスタートインストールは、ネットワーク化されたコンピュータで実行する傾向があるため、ネットワークベースのアプローチが最も一般的です。

キックスタートファイルを配置する場所をより詳細に見てみましょう。

### 1.8.1. キックスタートブートメディアの作成

Red Hat Enterprise Linux では、ディスクベースの起動はサポートされなくなりました。インストールは、起動に CD-ROM またはフラッシュメモリ製品を使用する必要があります。ただし、キッ

クスタートファイルはディスクの最上位ディレクトリーに留まる可能性があり、`ks.cfg` という名前にする必要があります。

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に `ks.cfg` という名前を付け、ブート CD-ROM の最上位ディレクトリーに置く必要があります。CD-ROM は読み取り専用であるため、ファイルを CD-ROM に書き込むイメージの作成に使用するディレクトリーに追加する必要があります。起動用メディアの作成方法については、『『インストールガイド』』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、キックスタートファイル `ks.cfg` を `isolinux/` ディレクトリーにコピーします。

キックスタートによるペンベースのフラッシュメモリーインストールを実行するには、キックスタートファイルに `ks.cfg` という名前を付け、フラッシュメモリーの最上位ディレクトリーに置く必要があります。最初にブートイメージを作成してから、`ks.cfg` ファイルをコピーします。

たとえば、以下は、`dd` コマンドを使用して、ブートイメージを `pen` ドライブ (`/dev/sda`) に転送します。

```
dd if=diskboot.img of=/dev/sda bs=1M
```



#### 備考

起動用の USB フラッシュメモリーペンドライブの作成は可能ですが、システムハードウェアの BIOS 設定には大きく依存します。お使いのシステムが別のデバイスの起動に対応しているかどうかを確認します。

### 1.8.2. ネットワーク上でキックスタートファイルの準備

キックスタートを使用したネットワークインストールは非常に一般的です。システム管理者は、多くのネットワーク化されたコンピューターで簡単にインストールを自動化できるため、非常に一般的です。通常、最も一般的に使用される方法は、管理者がローカルネットワーク上の BOOTP/DHCP サーバーと NFS サーバーの両方を持つ方法です。BOOTP/DHCP サーバーは、クライアントシステムのネットワーク情報を提供するのに使用されますが、インストール時に使用される実際のファイルは NFS サーバーによって提供されます。多くの場合、これら 2 つのサーバーは同じ物理マシンで実行されますが、必須ではありません。

ネットワー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、ネットワーク上に BOOTP/DHCP サーバーが必要で、Red Hat Enterprise Linux のインストールしようとしているマシンの設定情報を含める必要があります。BOOTP/DHCP サーバーは、クライアントにネットワーク情報とキックスタートファイルの場所を提供します。

BOOTP/DHCP サーバーでキックスタートファイルを指定すると、クライアントシステムはファイ



ルのパスの NFS マウントを試行し、キックスタートファイルとして使用して、指定したファイルをクライアントにコピーします。必要な設定は、使用する BOOTP/DHCP サーバーによって異なります。

以下は、DHCP サーバーの `dhcpd.conf` ファイルからの行の例です。

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

`filename` の後の値は、キックスタートファイルの名前（またはキックスタートファイルが存在するディレクトリー）に置き換え、`next-server` の後の値を NFS サーバー名に置き換えます。

BOOTP/DHCP サーバーで返されるファイル名がスラッシュ("/")で終了する場合、パスとしてのみ解釈されます。この場合、クライアントシステムはそのパスを NFS を使用してマウントし、特定のファイルを検索します。クライアントが検索するファイル名は次のとおりです。

```
<ip-addr>-kickstart
```

ファイル名の `< ip-addr >` セクションは、ドット付き 10 進数表記のクライアントの IP アドレスに置き換える必要があります。たとえば、IP アドレスが 10.10.0.1 のコンピューターのファイル名は 10.10.0.1-kickstart になります。

サーバー名を指定しないと、クライアントシステムは、BOOTP/DHCP 要求を NFS サーバーとして回答したサーバーの使用を試みることに注意してください。パスまたはファイル名を指定しないと、クライアントシステムは BOOTP/DHCP サーバーから /kickstart をマウントし、上記のように同じ `< ip-addr > -kickstart` ファイル名を使用してキックスタート ファイルの検索を試行します。

## 1.9. インストールツリーを利用可能にする

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は、同じディレクトリー構造を持つバイナリー Red Hat Enterprise Linux CD-ROM のコピーです。

CD ベースのインストールを実行している場合は、キックスタートインストールを開始する前に Red Hat Enterprise Linux CD-ROM #1 をコンピューターに挿入します。

ハードドライブのインストールを実行している場合は、バイナリー Red Hat Enterprise Linux CD-ROM の ISO イメージがコンピューターのハードドライブ上にあることを確認してください。

ネットワークベースの (NFS、FTP、または HTTP) のインストールを実行している場合は、ネットワーク経由でインストールツリーを使用できるようにする必要があります。詳細は、『『』 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。

## 1.10. 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、作成した起動用メディアまたは Red Hat Enterprise Linux CD-ROM #1 からシステムを起動し、ブートプロンプトで特別な起動コマンドを入力する必要があります。ks コマンドライン引数がカーネルに渡されると、インストールプログラムはキックスタートファイルを検索します。

### CD-ROM #1 および Diskette

また、`linux ks=floppy` コマンドは、ディスク上の `vfat` または `ext2` ファイルシステムにあり、Red Hat Enterprise Linux CD-ROM #1 から起動する場合にも機能します。

別の起動コマンドは、Red Hat Enterprise Linux CD-ROM #1 から起動し、ディスク上の `vfat` または `ext2` ファイルシステムにキックスタートファイルを用意することです。これを行うには、`boot:` プロンプトで以下のコマンドを入力します。

```
linux ks=hd:fd0:/ks.cfg
```

### Driver ディスクの使用

キックスタートでドライバー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。たとえば、ブートディスクから起動し、ドライバーディスクを使用するには、`boot:` プロンプトで以下のコマンドを入力します。

```
linux ks=floppy dd
```

### Boot CD-ROM

「[キックスタートブートメディアの作成](#)」の説明に従って、キックスタートファイルがブート CD-ROM 上にある場合は、システムに CD-ROM を挿入して、`boot:` プロンプトで以下のコマンドを入力します (`ks.cfg` はキックスタートファイルの名前に置き換えます)。

```
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とおりです。

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

インストールプログラムは、NFS サーバー < server > のキックスタートファイルをファイル < path > として検索します。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 /mydir/ks.cfg にある場合は、正しい起動コマンド ks=nfs:server.example.com:/mydir/ks.cfg になります。

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

インストールプログラムは、ファイル < path > として HTTP サーバー < server > のキックスタート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 ディレクトリー /mydir/ks.cfg にある場合、正しい起動コマンドは ks=http://server.example.com/mydir/ks.cfg になります。

**ks=floppy**

インストールプログラムは、/dev/fd0 内のディスク上の vfat または ext2 ファイルシステムのファイル ks.cfg を検索します。

**ks=floppy:/<path>**

インストールプログラムは、/dev/fd0 内のディスク上のキックスタートファイルをファイル < path > で検索します。

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

インストールプログラムは、ファイルシステムを < device > (vfat または ext2) にマウントし、そのファイルシステムで < file > としてキックスタートファイルを検索します (例: ks=hd:sda3:/mydir/ks.cfg)。

**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ファイル < file > を読み取ろうとします。マウントは行われません。これは通常、キックスタートファイルが initrd イメージ上にある場合に使用されます。

**ks=cdrom: /<path>**

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

**ks**

ks のみを使用する場合、インストールプログラムは DHCP を使用するようにイーサネットカードを設定します。キックスタートファイルは、キックスタートファイルを共有する NFS サーバーであるかのように、DHCP 応答から「bootServer」から読み込まれます。デフォルトでは、bootServer 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以下のいずれかです。

- DHCP を指定し、ブートファイルが / で開始すると、DHCP が提供するブートファイルは NFS サーバーで検索されます。
- DHCP を指定し、ブートファイルが他のもので始まる場合は、DHCP が提供するブートファイルが NFS サーバーの /kickstart ディレクトリーで検索されます。
- DHCP がブートファイルを指定しなかった場合、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 はインストールされるマシンの数値の IP アドレスになります。

**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用してネットワークに接続します。たとえば、eth1 デバイスを介してシステムに接続されている NFS サーバーのキックスタートファイルを使用して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 **ks=nfs: <server> :/ <path> ksdevice=eth1** を使用します。

## 第2章 KICKSTART CONFIGURATOR

Kickstart Configurator を使用すると、グラフィカルユーザーインターフェースを使用してキックスタートファイルを作成または変更できるため、ファイルの正しい構文を覚えておく必要はありません。

キックスタート Configurator を使用するには、X Window System を実行する必要があります。Kickstart Configurator を起動するには、Applications（パネルのメインメニュー）⇒ System Tools ⇒ Kickstart を選択するか、コマンド `/usr/sbin/system-config-kickstart` を入力します。

キックスタートファイルを作成する際に、いつでも File ⇒ プレビュー を選択して現在の選択を確認できます。

既存のキックスタートファイルから開始するには、File ⇒ Open を選択して既存のファイルを選択します。

### 2.1. 基本設定

図2.1 基本設定

File Help

Basic Configuration (required)

Default Language: English (USA) ▼

Keyboard: U.S. English ▼

Mouse: Generic - Wheel Mouse (PS/2) ▼

Emulate 3 Buttons

Time Zone: America/New\_York ▼

Use UTC clock

Root Password:

Confirm Password:

Encrypt root password

Language Support:  Lao (Laos)  
 Latvian (Latvia)  
 Lithuanian

Target Architecture: x86, AMD64, or Intel EM64T ▼

Reboot system after installation

Perform installation in text mode (graphical is default)

Perform installation in interactive mode

[D]

インストール時に使用する言語と、**Default Language** メニューからインストール後に使用するデフォルト言語を選択します。

キーボードメニューからシステムキーボードタイプを選択します。

**Mouse** メニューからシステムのマウスを選択します。**No Mouse** を選択した場合、マウスは設定されません。**Mouse** の **Probe** が選択されている場合、インストールプログラムはマウスを自動的に検出しようとします。**probing** は最新のマウスで機能します。

システムに2ボタンのマウスがある場合、**Emulate 3 Buttons** を選択して、3つのボタンのマウスをエミュレートできます。このオプションを選択すると、左および右のマウスボタンを同時にクリックすると、マウスボタンがクリックされます。

タイムゾーンメニューから、システムに使用する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、**Use UTC clock** を選択します。

**Root Password** テキストボックスに、システムの **root** パスワードを入力します。パスワードの確認テキストボックスに、同じパスワードを入力します。2 つ目のフィールドは、パスワードを誤入力しないようにし、インストールの完了後に何であるかを知らないことです。パスワードを暗号化されたパスワードとしてファイルに保存するには、**Encrypt root password** を選択します。暗号化オプションが選択された場合は、ファイルが保存されると、入力したプレーンテキストのパスワードは暗号化され、キックスタートファイルに書き込まれます。暗号化されたパスワードを入力せず、暗号化する場合は選択しないでください。キックスタートファイルは簡単に読み取ることのできるプレーンテキストファイルであるため、暗号化されたパスワードを使用することが推奨されます。

**Default Language** プルダウンメニューから選択した言語に加えて言語をインストールするには、**言語 サポート** の一覧でそれらを確認します。**Default Language** 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で使用されますが、インストール後にデフォルトを **Language Configuration Tool (system-config-language)** で変更できます。

**ターゲットアーキテクチャー** を選択すると、インストール時に使用される特定のハードウェアアーキテクチャーディストリビューションを指定します。

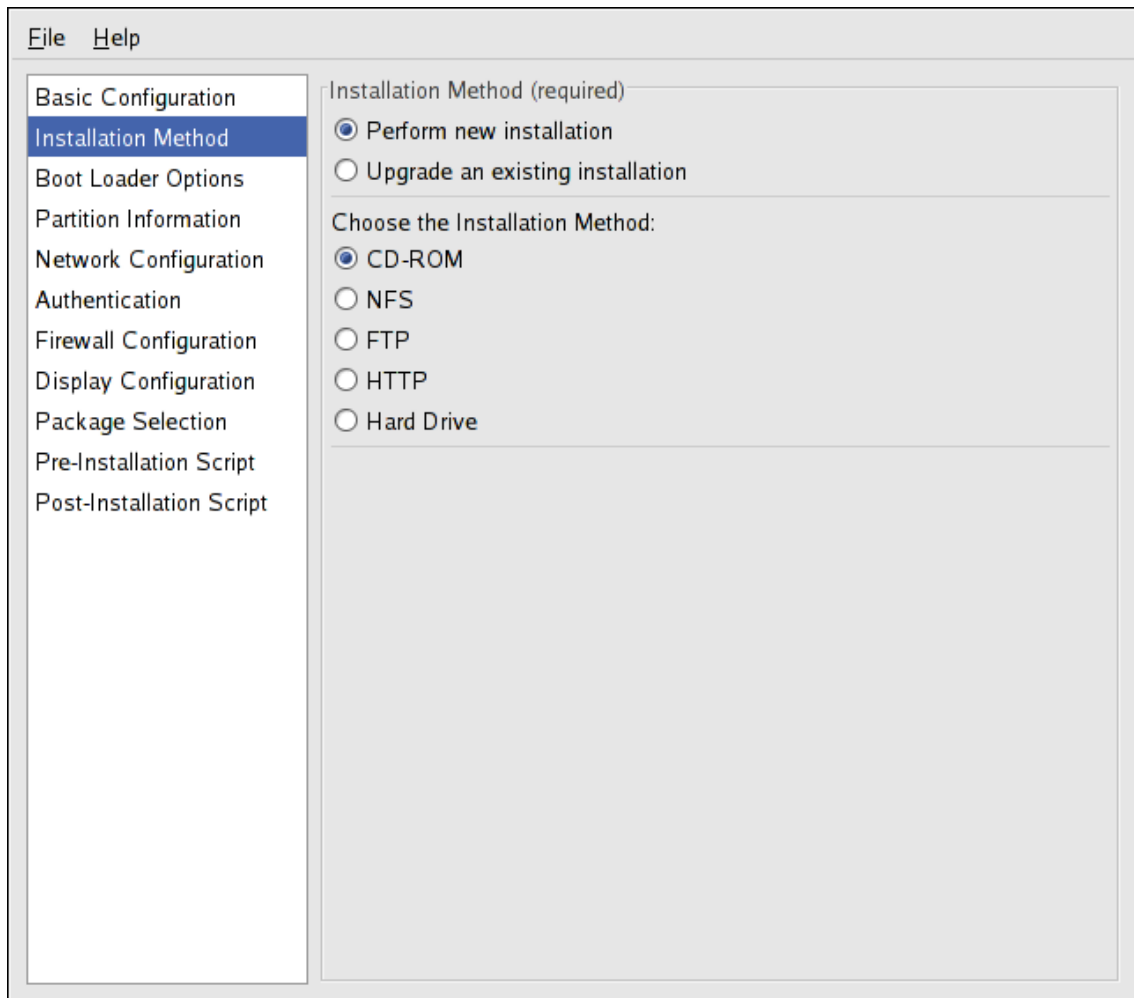
インストール後に **Reboot system** を選択し、インストールの完了後にシステムを自動的に再起動します。

キックスタートインストールは、デフォルトでグラフィカルモードで実行します。このデフォルトを上書きし、代わりにテキストモードを使用するには、**Per Installation in text mode** オプションを選択します。

インタラクティブモードでキックスタートインストールを実行できます。これは、インストールプログラムがキックスタートファイルで事前に設定されたすべてのオプションを使用することを意味しますが、次の画面に進む前に、各画面でオプションのプレビューを行うことができます。次の画面に進むには、設定を承認した後、または設定を変更してから **Next** ボタンをクリックしてからインストールを続行します。この種のインストールを選択するには、**Perform installation in interactive mode** オプションを選択します。

## 2.2. インストール方法

図2.2 インストール方法



[D]

インストール方法 画面では、新規インストールまたはアップグレードのいずれかを選択できます。アップグレードを選択すると、パーティション情報 オプションおよび パッケージ の選択 オプションが無効になります。キックスタートのアップグレードではサポートされません。

以下のオプションからキックスタートインストールまたはアップグレード画面を選択します。

- **CD-ROM** - このオプションを選択して、Red Hat Enterprise Linux CD-ROM からインストールまたはアップグレードします。
- **NFS** - NFS 共有ディレクトリーからインストールまたはアップグレードするには、このオプションを選択します。NFS サーバーのテキストフィールドで、完全修飾ドメイン名または IP アドレスを入力します。NFS ディレクトリーに、インストールツリーの RedHat ディレクトリーを含む NFS ディレクトリーの名前を入力します。たとえば、NFS サーバーに /mirrors/redhat/i386/RedHat/ ディレクトリーが含まれている場合は、NFS ディレクトリーに /mirrors/redhat/i386/ を入力します。



- **FTP** - FTP サーバーからインストールまたはアップグレードするには、このオプションを選択します。FTP server テキストフィールドに、完全修飾ドメイン名または IP アドレスを入力します。FTP ディレクトリーに、RedHat ディレクトリーを含む FTP ディレクトリーの名前を入力します。たとえば、FTP サーバーに /mirrors/redhat/i386/RedHat/ ディレクトリーが含まれている場合は、FTP ディレクトリーに /mirrors/redhat/i386/ を入力します。FTP サーバーにユーザー名とパスワードが必要な場合は、それらも指定します。
- **HTTP** - HTTP サーバーからインストールまたはアップグレードするには、このオプションを選択します。HTTP サーバーのテキストフィールドで、完全修飾ドメイン名または IP アドレスを入力します。HTTP ディレクトリーに、RedHat ディレクトリーを含む HTTP ディレクトリーの名前を入力します。たとえば、HTTP サーバーに /mirrors/redhat/i386/RedHat/ ディレクトリーが含まれている場合は、HTTP ディレクトリーに /mirrors/redhat/i386/ を入力します。
- **ハードドライブ** - ハードドライブからインストールまたはアップグレードする場合は、このオプションを選択します。ハードドライブのインストールには、ISO（または CD-ROM）イメージを使用する必要があります。インストールを開始する前に、ISO イメージが無効であることを確認してください。これを確認するには、『『インストールガイド』』で説明されているように、md5sum プログラムと linux mediacheck 起動オプションを使用します。ハードドライブパーティションのテキストボックスに、ISO イメージ（例： /dev/hda1）が含まれるハードドライブパーティションを入力します。ハードドライブの Directory テキストボックスに、ISO イメージが含まれるディレクトリーを入力します。

### 2.3. ブートローダーのオプション

図2.3 ブートローダーのオプション

The screenshot shows a window titled 'File Help' with a menu on the left containing the following items: Basic Configuration, Installation Method, **Boot Loader Options**, Partition Information, Network Configuration, Authentication, Firewall Configuration, Display Configuration, Package Selection, Pre-Installation Script, and Post-Installation Script. The main content area is divided into three sections:

- Boot Loader Options (required):**
  - Install new boot loader
  - Do not install a boot loader
  - Upgrade existing boot loader
- GRUB Options:**
  - Use GRUB password
    - Password:
    - Confirm Password:
    - Encrypt GRUB password
  - Install boot loader on Master Boot Record (MBR)
  - Install boot loader on first sector of the boot partition
- Kernel parameters:**

[D]

**GRUB** は、Red Hat Enterprise Linux のデフォルトのブートローダーです。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ません。ブートローダーをインストールしない場合は、ブートディスクを作成するか、サードパーティーのブートローダーなどのシステムを起動する方法を確認してください。

ブートローダー（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ー）をインストールする場所を選択する必要があります。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。

システムの起動時に使用されるカーネルに特別なパラメーターを渡すには、カーネルパラメーターのテキストフィールドに入力します。たとえば、**IDE CD-ROM Writer** がある場合は、`hdd=ide-scsi` をカーネルパラメーターとして設定します（`hdd` は **CD-ROM** デバイスである場合）、`cdrecord` を使用する前に読み込む必要がある **SCSI** エミュレーションドライバを使用するようにカーネルに指示します。

**GRUB** パスワードを設定すると、**GRUB** ブートローダーをパスワードで保護できます。**Use GRUB password** を選択し、**Password** フィールドにパスワードを入力します。パスワードの確認のテキス

トフィールドに同じパスワードを入力します。パスワードを暗号化されたパスワードとしてファイルに保存するには、暗号化 GRUB パスワードの暗号化 を選択します。暗号化オプションが選択された場合は、ファイルが保存されると、入力したプレーンテキストのパスワードは暗号化され、キックスタートファイルに書き込まれます。暗号化されたパスワードを入力する場合は、選択を解除して暗号化を解除します。

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する場合は、Upgrade existing boot loader を選択して、古いエントリーを保持しつつ、既存のブートローダー設定をアップグレードします。

## 2.4. パーティション情報

図2.4 パーティション情報

File Help

Basic Configuration  
Installation Method  
Boot Loader Options  
**Partition Information**  
Network Configuration  
Authentication  
Firewall Configuration  
Display Configuration  
Package Selection  
Pre-Installation Script  
Post-Installation Script

Partition Information (required)

Clear Master Boot Record  
 Do not clear Master Boot Record

Remove all existing partitions  
 Remove existing Linux partitions  
 Preserve existing partitions

Initialize the disk label  
 Do not initialize the disk label

Device/ Partition Number	Mount Point/ RAID	Type	Format	Size (MB)

Add Edit Delete RAID

[D]

Master Boot Record(MBR)を消去するかどうかを選択します。既存のパーティションをすべて削除するか、既存の Linux パーティションをすべて削除するか、既存のパーティションを保持します。

システムのアーキテクチャーのデフォルトにディスクラベルを初期化するには（例：x86 の場合は msdos、gp (x86 の場合は gpt)）、ブランドの新しいハードドライブにインストールしている場合

は、ディスクラベルの初期化を選択します。

### 2.4.1. 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2.5「パーティションの作成」に表示される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、およびパーティションサイズを選択します。必要に応じて、以下から選択することもできます。

- **Additional Size Options** セクションで、パーティションに固定サイズ、選択したサイズまで設定するか、ハードドライブの残りの領域を埋めるかを選択します。swap をファイルシステムタイプとして選択した場合は、インストールプログラムがサイズを指定するのではなく、推奨されるサイズで swap パーティションを作成するように選択できます。
- パーティションがプライマリーパーティションとして作成されるように強制します。
- 特定のハードドライブにパーティションを作成します。たとえば、最初の IDE ハードディスク(/dev/hda)のパーティションを作成するには、hda をドライブとして指定します。ドライブ名に /dev を含めないでください。
- 既存のパーティションを使用します。たとえば、最初の IDE ハードディスク(/dev/hda1)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、hda1 をパーティションとして指定します。パーティション名に /dev を含めないでください。
- パーティションを、選択し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2.5 パーティションの作成

Mount Point:

File System Type:

Size (MB):

Additional Size Options

Fixed size

Grow to maximum of (MB):

Fill all unused space on disk

Use recommended swap size

Force to be a primary partition (asprimary)

Make partition on specific drive (ondisk)

Drive :  (for example: hda or sdc)

Use existing partition (onpart)

Partition :  (for example: hda1 or sdc3)

Format partition

[D]

既存のパーティションを編集するには、リスト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。選択したパーティションの値を反映している場合を除き、パーティションの追加を選択したときと同じパーティションオプションウィンドウが表示されます。図2.5「パーティションの作成」パーティション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。

#### 2.4.1.1. ソフトウェア RAID パーティションの作成

ソフトウェア RAID パーティションを作成するには、以下の手順を行います。

1. **RAID ボタンをクリックします。**
2. **Create a software RAID partition を選択します。**
3. 前述のようにパーティションを設定します。ただし、ファイルシステムタイプとして **Software RAID** を選択します。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、使用する既存のパーティションを指定する必要があります。

図2.6 ソフトウェア RAID パーティションの作成

Mount Point:

File System Type: software RAID

Size (MB): 2048

Additional Size Options

Fixed size

Grow to maximum of (MB):

Fill all unused space on disk

Use recommended swap size

Force to be a primary partition (asprimary)

Make partition on specific drive (ondisk)

Drive :  (for example: hda or sdc)

Use existing partition (onpart)

Partition :  (for example: hda1 or sdc3)

Format partition

[D]

この手順を繰り返して、RAID 設定に必要なパーティションを多数作成します。すべてのパーティションを RAID パーティションにする必要はありません。

RAID デバイスの形成に必要なすべてのパーティションを作成したら、以下の手順に従います。

1. RAID ボタンをクリックします。
2. Create a RAID device 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 デバイスの予備数、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2.7 ソフトウェア RAID デバイスの作成

The screenshot shows a configuration window for creating a software RAID device. The fields are as follows:

- Mount Point: /home
- File System Type: ext3
- RAID Device: md0
- RAID Level: 0
- Raid Members: A list containing 'raid.01' and 'raid.02', both with checked checkboxes. 'raid.02' is highlighted in blue.
- Number of spares: 1
- Format RAID device

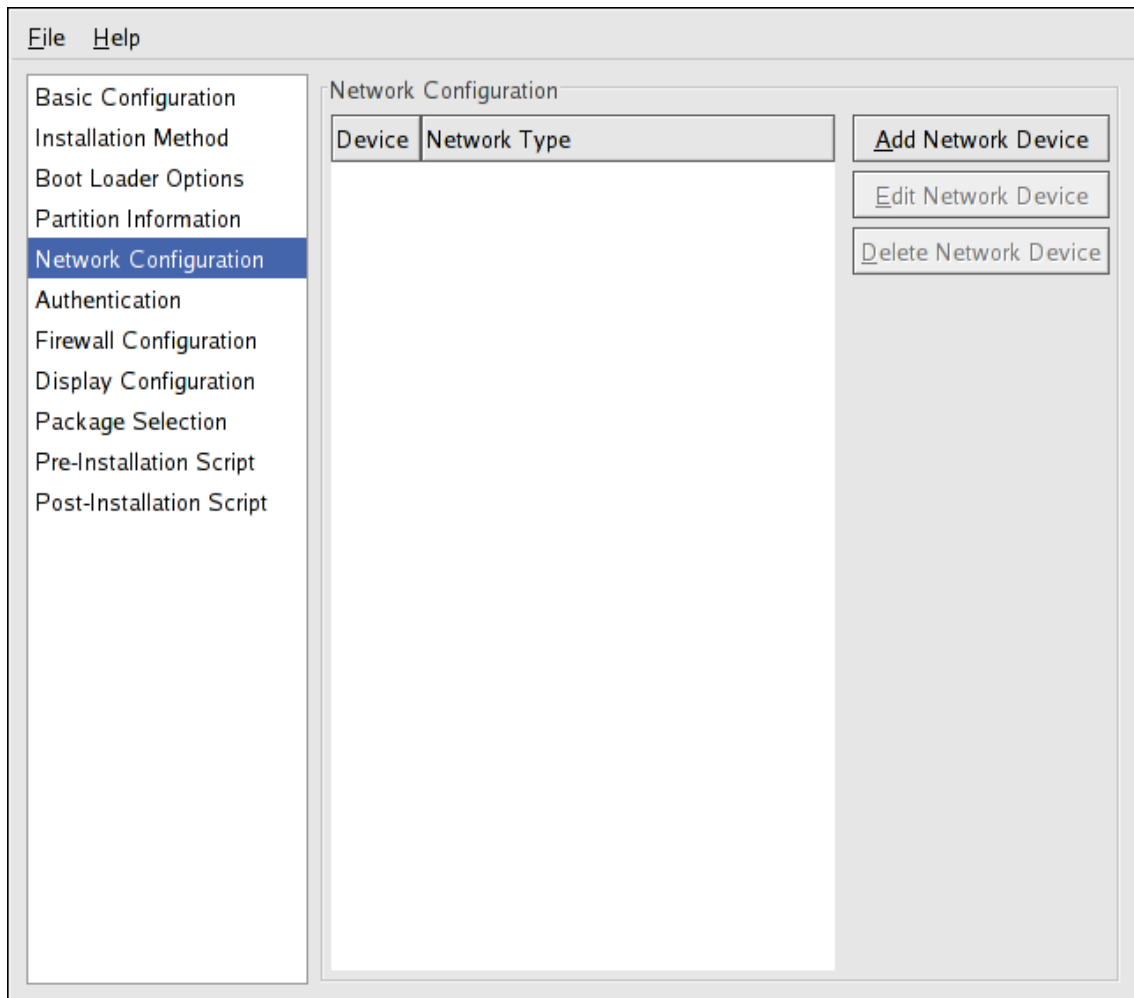
Buttons at the bottom: Cancel (with a red X icon) and OK (with a green arrow icon).

[D]

4. OK をクリックして、一覧にデバイスを追加します。

## 2.5. NETWORK CONFIGURATION

図2.8 Network Configuration



[D]

キックスタートを介してインストールするシステムにイーサネットカードがない場合は、ネットワーク 設定 のページで設定しないでください。

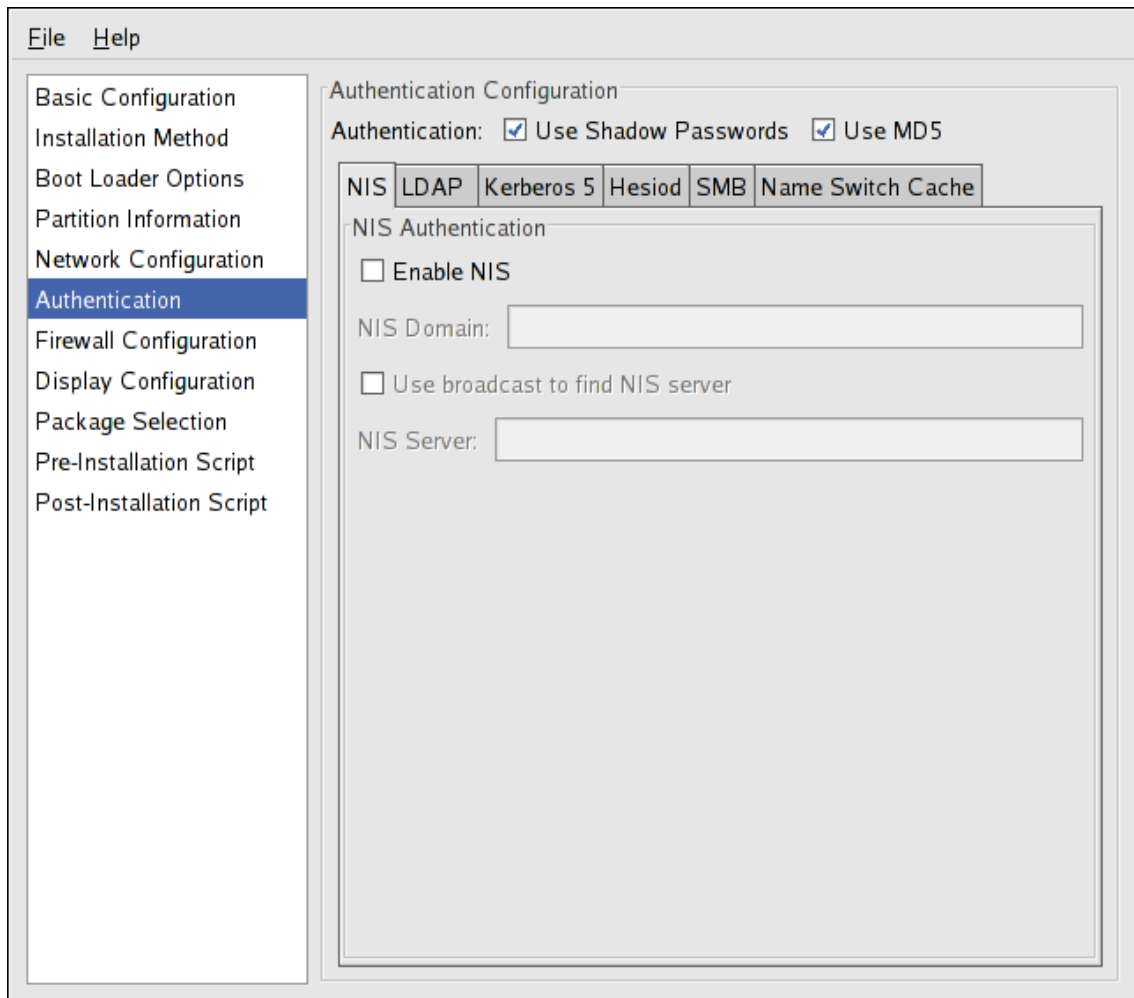
ネットワークは、ネットワークベースのインストール方法（NFS、FTP、または HTTP）を選択する場合のみ必要です。ネットワークは、ネットワーク 管理ツール (`system-config-network`)を使用してインストール後に常に設定できます。詳細は、[17章 Network Configuration](#) を参照してください。

システムのイーサネットカードごとに、ネットワークデバイスの 追加 をクリックし、デバイスのネットワークデバイスおよびネットワークタイプを選択します。eth0 を選択して、最初のイーサネットカードを設定し、2つ目のイーサネットカードに eth1 を設定します。

## 2.6. 認証



図2.9 認証



[D]

**Authentication** セクションで、ユーザーパスワードに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は強く推奨され、デフォルトで選択されます。

**Authentication Configuration** オプションでは、以下の認証方法を設定できます。

- **NIS**
- **LDAP**
- **Kerberos 5**
- **hesiod**

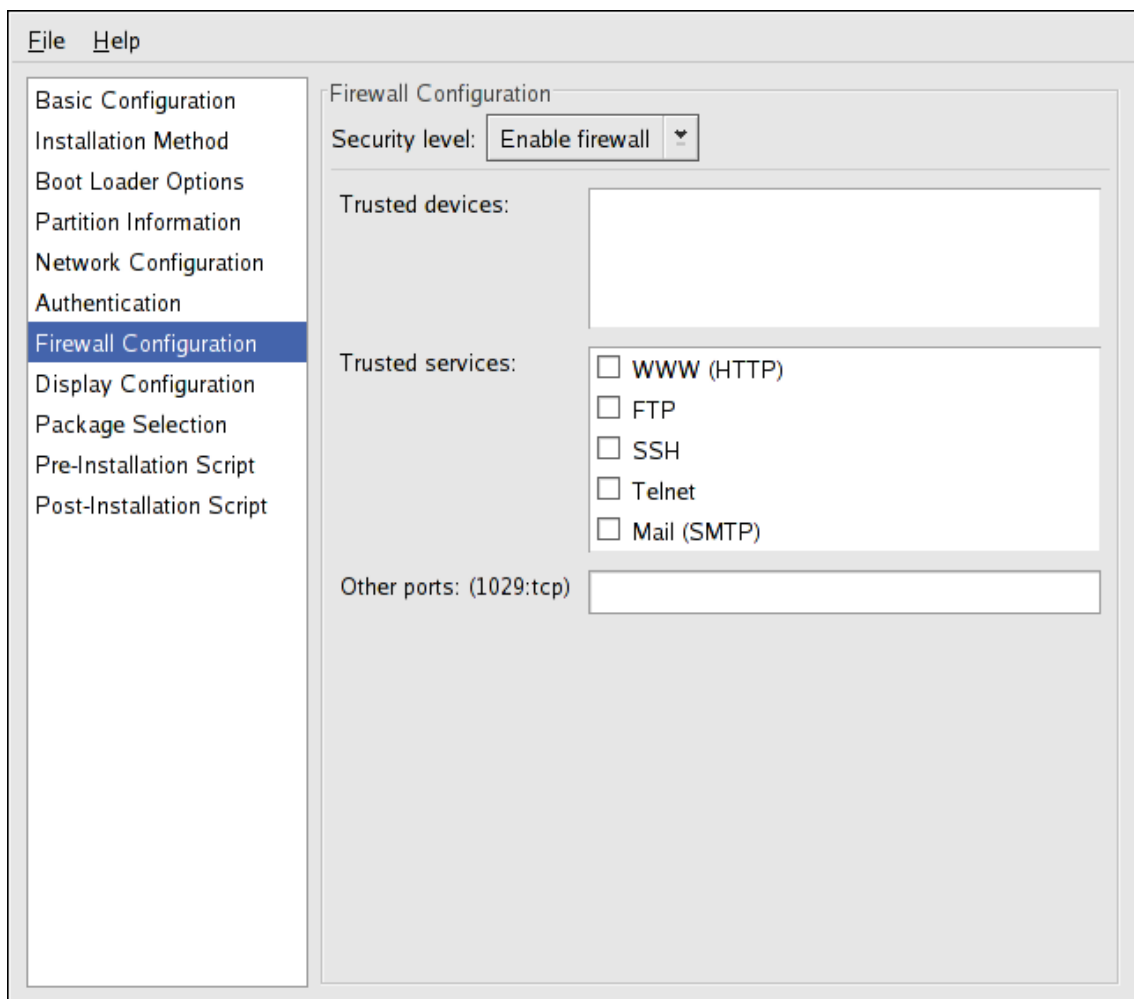
- **SMB**
- **名前スイッチキャッシュ**

これらのメソッドは、デフォルトでは有効になっていません。これらのメソッドを1つ以上有効にするには、該当するタブをクリックして **Enable** の横にあるチェックボックスをクリックし、認証方法の適切な情報を入力します。オプションの詳細は、[26章 認証設定](#) を参照してください。

## 2.7. ファイアウォールの設定

**Firewall Configuration** ウィンドウは、インストールプログラムおよび **Security Level Configuration Tool** の画面と似ています。

図2.10 ファイアウォールの設定



[D]

ファイアウォールを無効にすると、システムはアクティブなサービスおよびポートへの完全なアクセスを許可します。システムへの接続が拒否されたり拒否されたりすることはありません。

**Enable firewall** を選択すると、DNS 応答や DHCP 要求など、送信要求に対応しない受信接続を拒否するように設定します。このマシンで実行中のサービスへのアクセスが必要な場合は、特定のサービスがファイアウォールを通過するのを許可することを選択できます。

ネットワーク設定 セクションで設定したデバイスのみが、利用可能な **Trusted** デバイスとして一覧表示されます。リストで選択したデバイスからの接続がシステムにより受け入れられます。たとえば、eth1 が内部システムからの接続のみを受信する場合、その接続を許可する場合があります。

**Trusted services** 一覧でサービスが選択されている場合、サービスの接続はシステムが許可および処理します。

**Other ports** テキストフィールドに、リモートアクセス用に開く必要のある追加のポートの一覧を表示します。port:protocol の形式を使用します。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 を指定します。数値ポートを指定することもできます。ファイアウォールを介してポート 1234 の UDP パケットを許可するには、1234:udp を入力します。複数のポートを指定するには、コンマで区切ります。

### 2.7.1. SELinux の設定

SELinux の設定は Kickstart Configurator で指定されていませんが、キックスタートファイルから selinux パラメーターを省略すると、キックスタートはデフォルトで Enforcing モードで SELinux を有効にします。

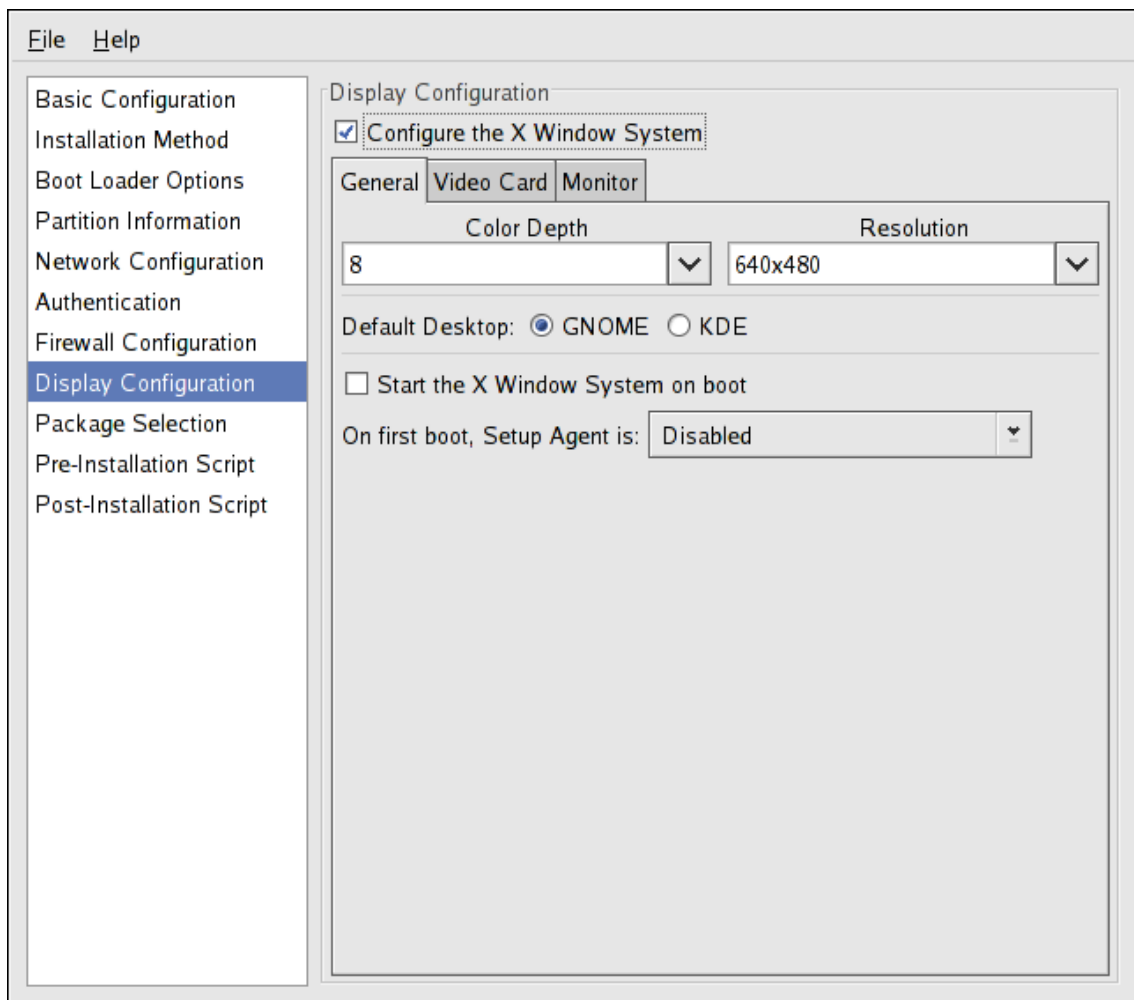
## 2.8. 設定の表示

X Window System をインストールしている場合は、[図2.11「X 設定 - 全般」](#) に示されているように Display Configuration ウィンドウで **Configure the X Window System** オプションを選択すると、キックスタートインストール時に設定できます。このオプションを選択しないと、X 設定オプションが無効になり、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。

### 2.8.1. 全般

X の設定の最初の手順は、デフォルトの色深度と解像度を選択することです。各プルダウンメニューからそれらを選択します。ビデオカードと互換性のある色深度と解決策を指定し、システムを監視するようにしてください。

図2.11 X 設定 - 全般



[D]

GNOME と KDE desktop の両方をインストールする場合は、デフォルトとするデスクトップを選択する必要があります。1つのデスクトップのみをインストールする場合は必ず選択してください。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とするデスクトップを選択できます。

次に、システムの起動時に X Window System を開始するかどうかを選択します。このオプションは、グラフィカルログイン画面を使用して、ランレベル 5 でシステムを起動します。システムのインストール後に、`/etc/inittab` 設定ファイルを変更すると変更できます。

また、システムの初回再起動時に Setup Agent を起動するかどうかを選択します。これはデフォルトで無効になっていますが、設定は再設定モードで有効または無効にできます。再設定モードでは、言語、マウス、キーボード、root パスワード、セキュリティーレベル、タイムゾーン、ネットワーク設定オプションもデフォルトの設定オプションになります。

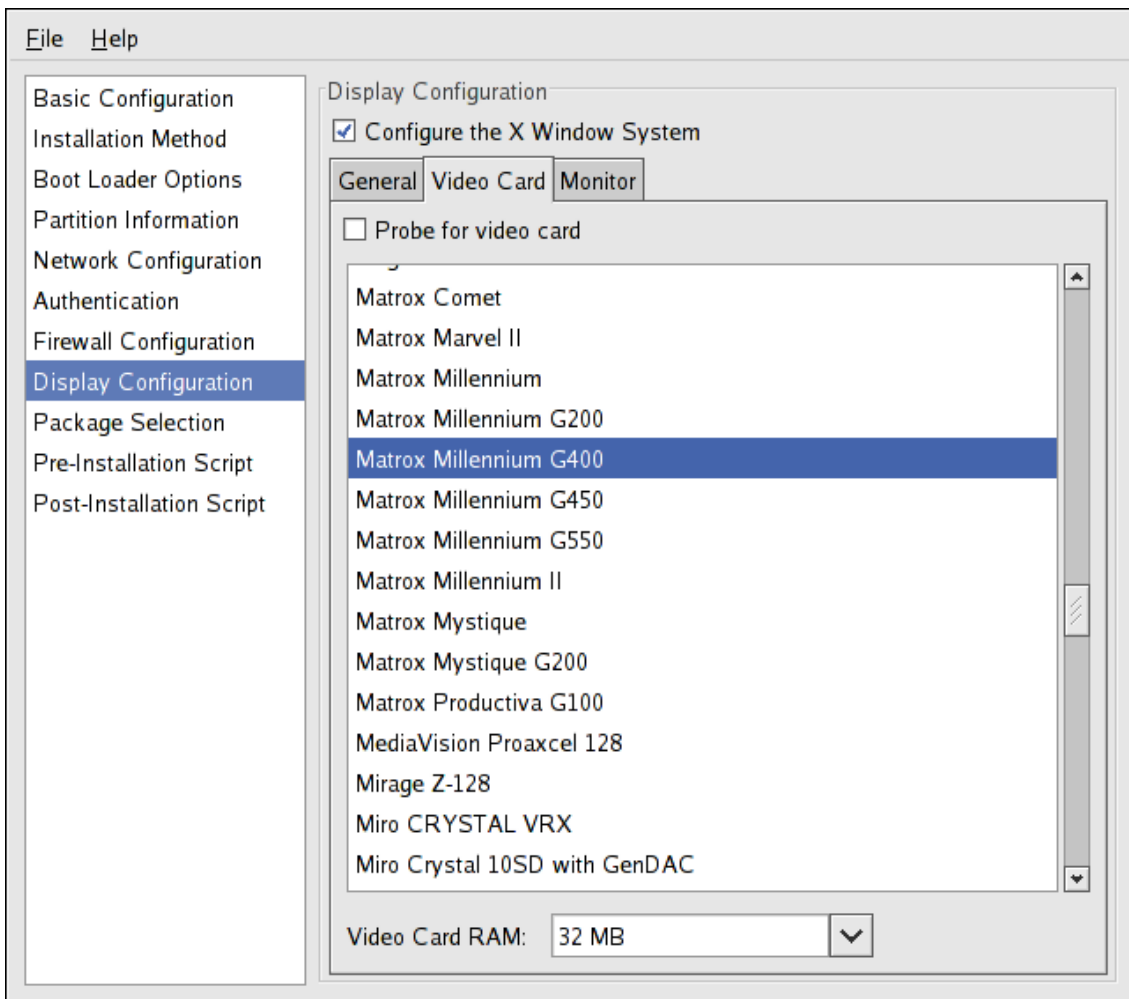
## 2.8.2. ビデオカード

ビデオカードのプロープは、デフォルトで選択されます。このデフォルトを使用して、インストール時にビデオカードのインストールプログラムプロープを使用します。プロービングは最新のビデオ

カードで機能します。このオプションが選択され、インストールプログラムがビデオカードを正常にブロードできない場合は、ビデオカード設定画面でインストールプログラムを停止します。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て **Next** をクリックします。

また、[図2.12 「X 設定 - ビデオカード」](#) に示されるように、**Video Card** タブの一覧からビデオカードを選択できます。**Video Card RAM** プルダウンメニューから選択したビデオカードの容量を指定します。これらの値は、インストールプログラムが **X Window System** を設定するために使用されます。

図2.12 X 設定 - ビデオカード

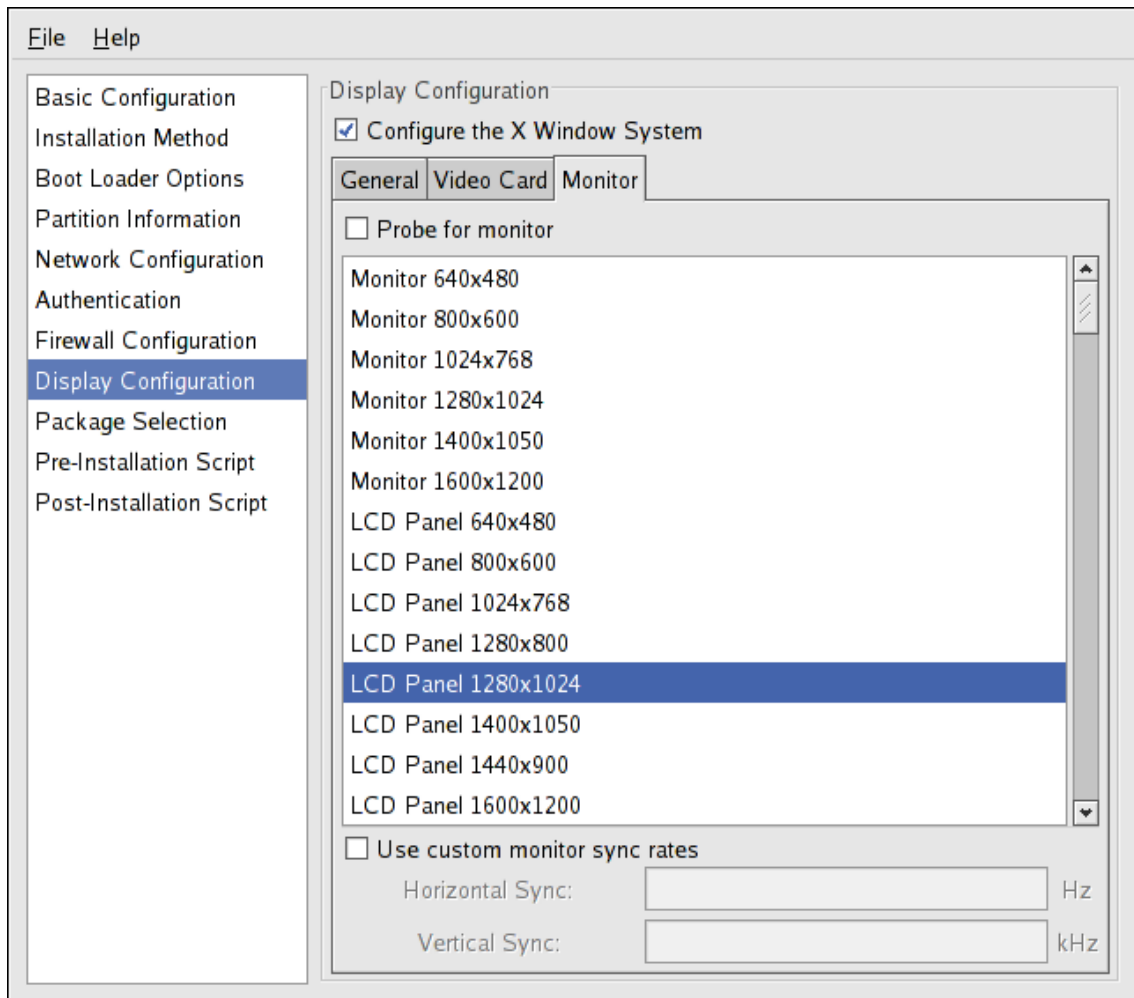


[D]

### 2.8.3. Monitor

ビデオカードを設定したら、[図2.13 「X 設定 - 監視」](#) に示されるように **Monitor** タブをクリックします。

図2.13 X 設定 - 監視



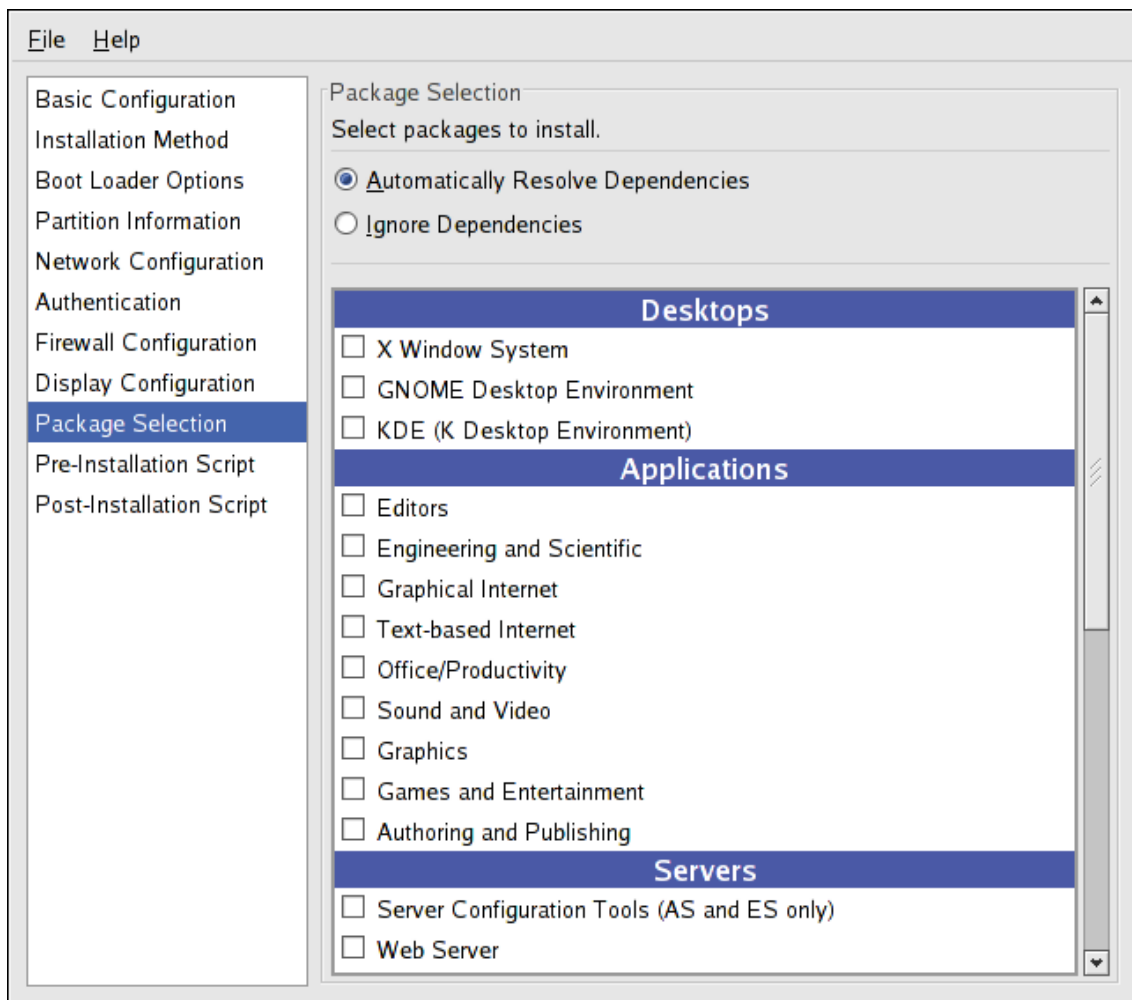
[D]

**monitor** のプローブは、デフォルトで選択されます。このデフォルトを使用して、インストール時にモニターのインストールプログラムプローブを設定します。**probing** は最新のモニターで機能します。このオプションが選択され、インストールプログラムがモニターをプローブできない場合、インストールプログラムはモニター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、一覧からモニターを選択して **Next** をクリックします。

または、一覧からモニターを選択できます。また、**monitor** オプションの代わりに **hysnc** および **vsync** をチェックして、特定のモニターを選択するのではなく、水平および垂直の同期速度を指定することもできます。このオプションは、システムのモニターが一覧にない場合に役に立ちます。このオプションを有効にすると、監視リストが無効になります。

## 2.9. パッケージの選択

図2.14 パッケージの選択



[D]

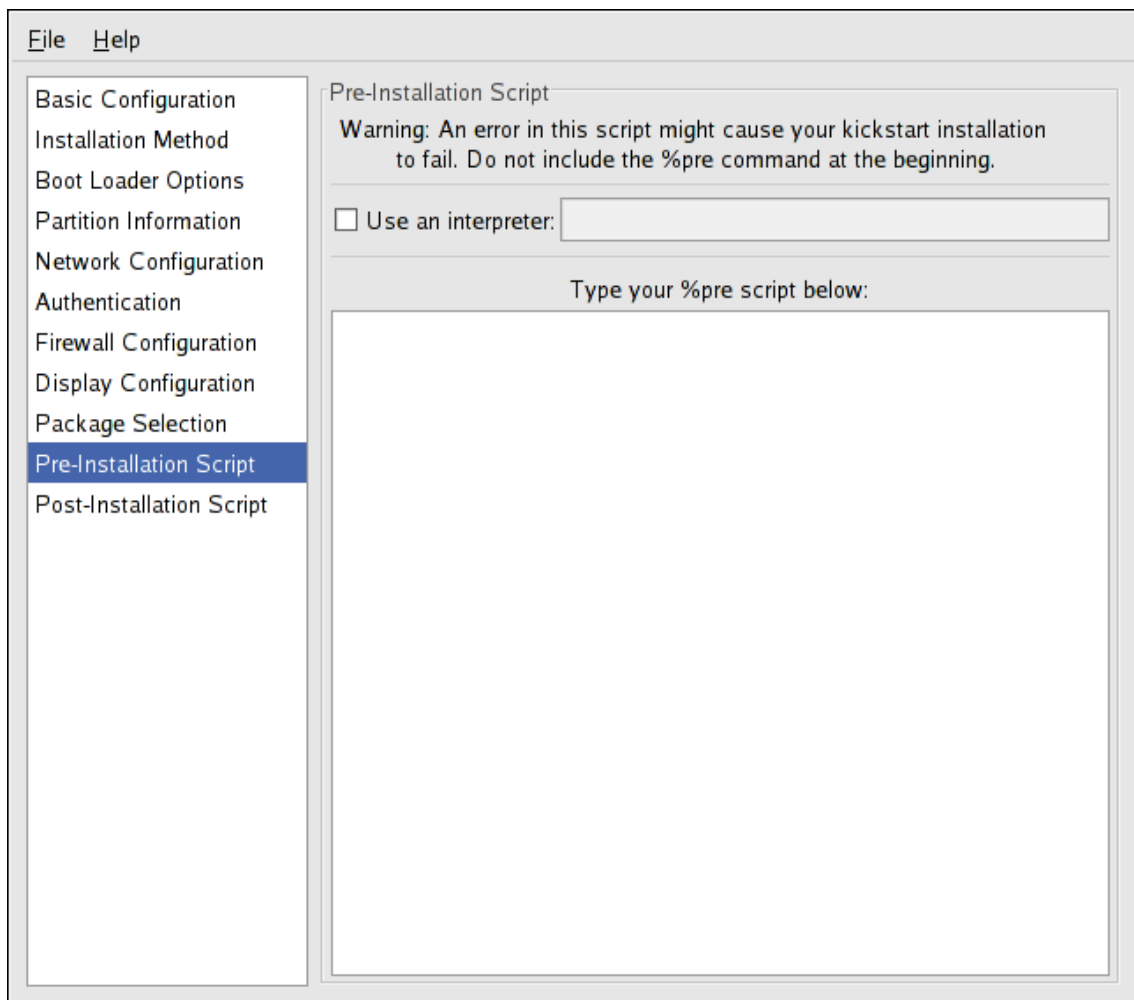
パッケージの選択 ウィンドウでは、インストールするパッケージを選択できます。

パッケージの依存関係を自動的に解決して無視するオプションもあります。

現在、Kickstart Configurator 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、保存した後にキックスタートファイルの `%packages` セクションを変更します。詳細は、「[パッケージの選択](#)」を参照してください。

## 2.10. インストール前のスクリプト

図2.15 インストール前のスクリプト



[D]

キックスタートファイルが解析され、インストールを開始する前に、システムで実行す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は、このセクションが処理される前にネットワークが有効になります。インストールスクリプトを追加するには、テキストエリアに入力します。

スクリプトの実行に使用するスクリプト言語を指定するには、**Use an interpreter** オプションを選択し、その隣のテキストボックスにインタープリターを入力します。たとえば、Python スクリプトに `/usr/bin/python2.2` を指定できます。このオプションは、キックスタートファイルで `%pre --interpreter /usr/bin/python2.2` の使用に対応します。

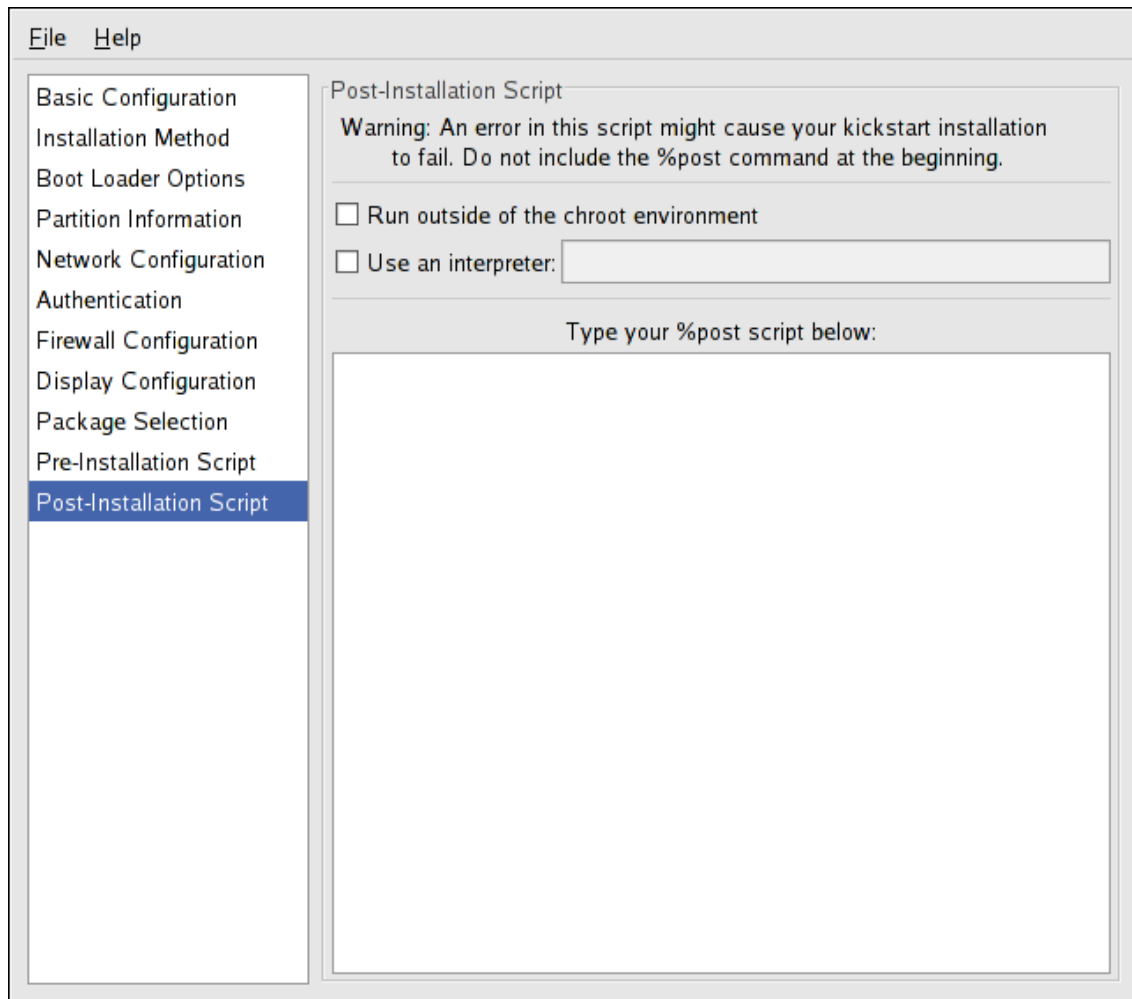
**WARNING**

`%pre` コマンドは指定しないでください。これは追加されています。



## 2.11. インストール後のスクリプト

図2.16 インストール後のスクリプト



[D]

インストールの完了後に、システムで実行するコマンドを追加することもできます。ネットワークがkickstartファイルで適切に設定されている場合、ネットワークが有効化され、スクリプトにネットワーク上のリソースにアクセスするためのコマンドを含めることができます。インストール後のスクリプトを含めるには、テキストエリアに入力します。



### WARNING

%post コマンドは含めないでください。これは追加されています。

たとえば、新たにインストールしたシステムの日付のメッセージを変更するには、以下のコマンドを %post セクションに追加します。

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



#### ヒント

その他の例は、「例」を参照してください。

### 2.11.1. chroot 環境

chroot 環境外でインストール後のスクリプトを実行するには、インストール後のウィンドウの上部にあるこのオプションの横にあるチェックボックスをクリックします。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。

新規にインストールしたファイルシステムを変更するには、インストール後のセクションで、chroot 環境外にあるディレクトリー名の前に /mnt/sysimage/ を追加する必要があります。

たとえば、chroot 環境外で Run を選択した場合は、前の例を以下のように変更します。

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

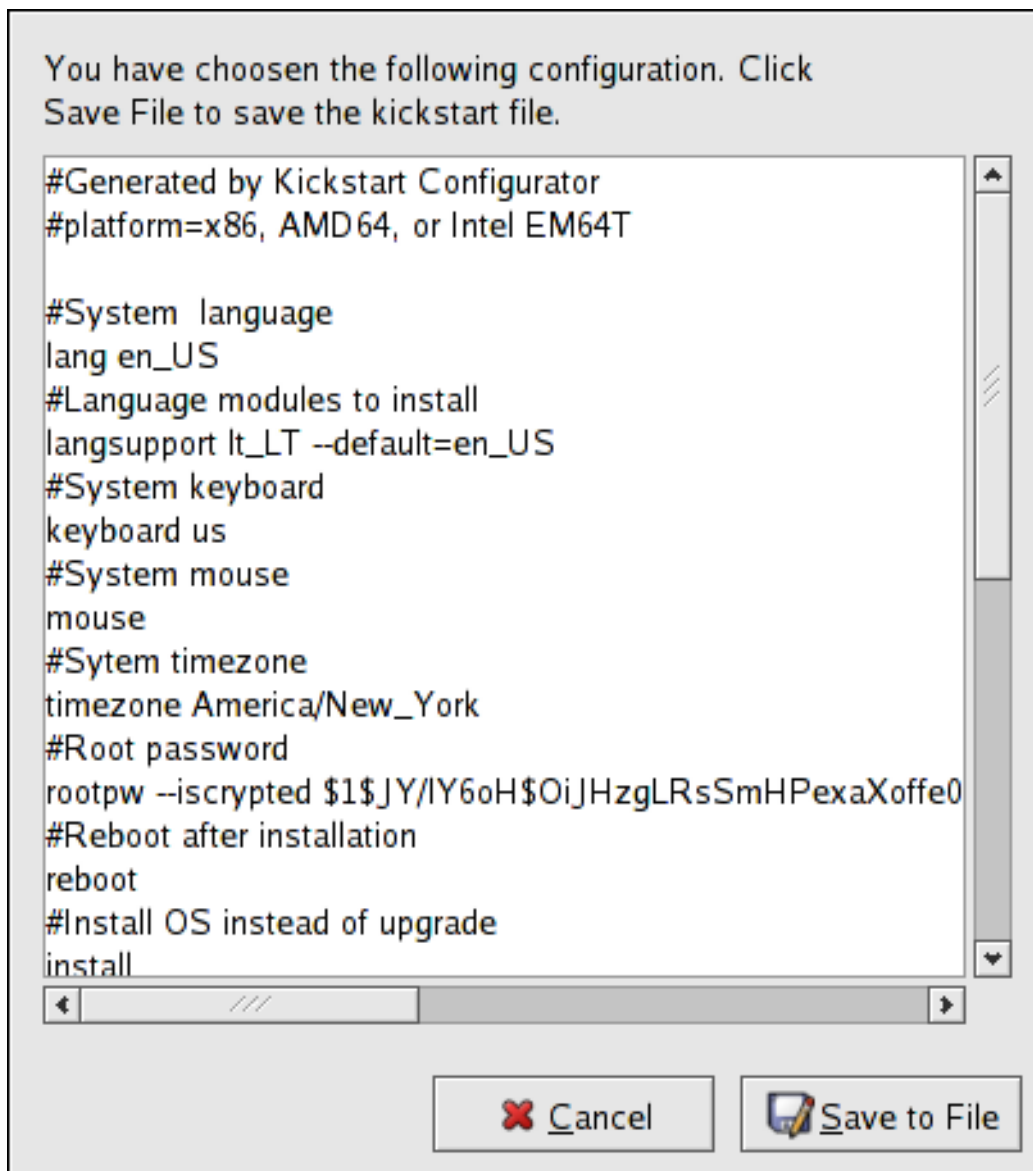
### 2.11.2. インタープリターの使用

スクリプトの実行に使用するスクリプト言語を指定するには、Use an interpreter オプションを選択し、その隣のテキストボックスにインタープリターを入力します。たとえば、Python スクリプトに /usr/bin/python2.2 を指定できます。このオプションは、キックスタートファイルで %post --interpreter /usr/bin/python2.2 の使用に対応します。

## 2.12. ファイルの保存

キックスタートオプションの選択後に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 File => Preview を選択します。

図2.17 プレビュー



[D]

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 **Save to File** ボタンをクリックします。ファイルをプレビューせずに保存するには、**File => Save File** を選択するか、**Ctrl+S** を押します。ダイアログボックスが表示されます。ファイルを保存する場所を選択します。

ファイルを保存すると、キックスタートインストールを開始する方法は「[キックスタートインストールの開始](#)」を参照してください。

## 第3章 PXE ネットワークインストール

Red Hat Enterprise Linux では、NFS、FTP、または HTTP プロトコルを使用したネットワーク上でインストールできます。ネットワークインストールは、ブート CD-ROM、起動可能なフラッシュメモリードライブ、または Red Hat Enterprise Linux CD #1 と共に askmethod ブートオプションを使用して起動できます。または、インストールするシステムに PXE(Pre-Execution Environment)に対応するネットワークインターフェースカード(NIC)が含まれている場合は、CD-ROM などのローカルメディアではなく、別のネットワークシステムでファイルから起動するように設定できます。

PXE ネットワークインストールでは、PXE 対応のクライアントの NIC は、DHCP 情報のブロードキャスト要求を送信します。DHCP サーバーは、クライアントに IP アドレス、ネームサーバー、tftp サーバーの IP アドレス、tftp サーバーの IP アドレスやホスト名（インストールプログラムを起動するために必要なファイルを提供する）、tftp サーバーのファイルの場所をクライアントに提供します。これは、`syslinux` パッケージの一部である `PXELINUX` が原因で可能です。

PXE インストールを準備するには、以下の手順を実行する必要があります。

1. インストールツリーをエクスポートするように、ネットワーク（NFS、FTP、HTTP）サーバーを設定します。
2. PXE ブートに必要な tftp サーバーでファイルを設定します。
3. PXE 設定から起動できるホストを設定します。
4. tftp サービスを起動します。
5. DHCP を設定している。
6. クライアントを起動して、インストールを開始します。

### 3.1. ネットワークサーバーの設定

まず、インストールする Red Hat Enterprise Linux のバージョンとバリエーションのインストールツリー全体をエクスポートするように、NFS サーバー、FTP サーバー、または HTTP サーバーを設定します。詳細な手順については、『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。

## 3.2. PXE ブート設定

次の手順では、クライアントが要求した時に検索できるように、インストールを開始するのに必要なファイルを tftp サーバーにコピーすることです。tftp サーバーは通常、インストールツリーをエクスポートするネットワークサーバーと同じサーバーです。

これらのファイルをコピーするには、NFS サーバー、FTP サーバー、または HTTP サーバーで Network Booting Tool を実行します。別の PXE サーバーは必要ありません。

これらの手順のコマンドラインバージョンは、「[コマンドラインからの設定](#)」を参照してください。

グラフィカルバージョンの Network Booting Tool を使用するには、X Window System を実行し、root 権限で、system-config-netboot 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。デスクトップから Network Booting Tool を起動するには、Applications（パネルのメインメニュー）=> System Settings => Server Settings => Network Booting Service に移動します。または、シェルプロンプトで system-config-netboot コマンド（XTerm や GNOME ターミナルなど）を入力します。

Network Booting Tool を初めて開始する場合は、First Time Druid から Network Install を選択します。それ以外の場合は、プルダウンメニューから Configure => Network Installation を選択し、Add をクリックします。[図3.1「ネットワークインストールの設定](#)」のダイアログが表示されます。

図3.1 ネットワークインストールの設定

Operating system identifier	rhel-4-as
Description:	RHEL 4 AS
Select protocol for installation:	NFS
Kickstart:	http://www.example.com/ks/ks.cfg
Software:	
Server:	server.example.com
Location:	/misc/RHEL-4/AS/i386/tree/
<input checked="" type="checkbox"/> Anonymous FTP	
User:	<input type="text"/>
Password:	<input type="text"/>
<input type="button" value="Cancel"/> <input type="button" value="OK"/>	

[D]

- オペレーティングシステム識別子 - Red Hat Enterprise Linux のバージョンとバリエーションを識別するため、1つの単語を使用して一意の名前を指定します。これは、`/tftpboot/linux-install/` ディレクトリーのディレクトリー名として使用されます。
- Description: Red Hat Enterprise Linux のバージョンとバリエーションの簡単な説明を表示します。
- インストールにプロトコルを選択します。以前に設定したものに依りて、ネットワークインストールタイプとして NFS、FTP、または HTTP を選択します。FTP が選択されていて、匿名の FTP が使用されていない場合は、Anonymous FTP の選択を解除し、有効なユーザー名とパスワードの組み合わせを提供します。
- キックスタート - キックスタートファイルの場所を指定します。ファイルは、URL またはローカルに保存されているファイル（ディスク）にすることができます。キックスタートファイルは、Kickstart Configurator で作成できます。詳細は、[2章 Kickstart Configurator](#) を参照してください。
- サーバー - NFS、FTP、または HTTP サーバーの IP アドレスまたはドメイン名を指定します。
- location: ネットワークサーバーで共有されるディレクトリーを指定します。FTP または

HTTP を選択した場合、ディレクトリーは FTP サーバーのデフォルトディレクトリーまたは HTTP サーバーのドキュメントルートに対して相対的である必要があります。すべてのネットワークインストールの場合、提供されるディレクトリーにはインストールツリーの RedHat/ディレクトリーが含まれている必要があります。

OK をクリックすると、インストールプログラムを起動するのに必要な `initrd.img` ファイルおよび `vmlinuz` ファイルが、指定したインストールツリーの `images/pxeboot/` から、tftp サーバーの `/tftpboot/linux-install/<os-identifier>/` ( Network Booting Tool を実行しているもの) に転送されます。

### 3.2.1. コマンドラインからの設定

ネットワークサーバーが X を実行していない場合は、`system-config-netboot` パッケージに含まれる `pxeos` コマンドラインユーティリティーを使用して、tftp サーバーファイル を設定できます。

```
pxeos -a -i "<description>" -p <NFS|HTTP|FTP> -D 0 -s client.example.com \ -L <net-location> -k <kernel> -K <kickstart><os-identifer>
```

以下の一覧で、オプションについて説明します。

- **-a:** OS インスタンスが PXE 設定に追加されるように指定します。
- **-i " &lt;description> ; "** - Replace "*<description>*" with a description of the OS instance.これは、[図3.1「ネットワークインストールの設定」](#) の Description フィールドに対応します。
- **-p <NFS|HTTP|FTP>** - インストールに使用する NFS プロトコル、FTP、または HTTP プロトコルを指定します。指定できるのは 1 つのみです。これは、[図3.1「ネットワークインストールの設定」](#) のインストールメニューの Select protocol に対応します。
- **-d &lt;0|1>: "0"** を指定します。これは、pxeos を使用してディスクレス環境を設定することができるため、ディスクレス設定ではないことを示します。
- **-s client.example.com** - -s オプションの後に NFS サーバー、FTP サーバー、または HTTP サーバーの名前を指定します。これは、[図3.1「ネットワークインストールの設定」](#) の Server フィールドに対応します。
- **-l &lt;net-location> ; - -L** オプションの後に、そのサーバー上にインストールツリーの

場所を指定します。これは、[図3.1「ネットワークインストールの設定」](#) の Location フィールドに対応します。

- `-k <kernel>` - 起動に使用するサーバーインストールツリーの特定のカーネルバージョンを指定します。
- `-k <kickstart>` - キックスタートファイルの場所を指定します（ある場合）。
- `<os-identifier>: /tftpboot/linux-install/` ディレクトリーのディレクトリー名として使用する OS 識別子を指定します。これは、[図3.1「ネットワークインストールの設定」](#) のオペレーティングシステム識別子 フィールドに対応します。

FTP がインストールプロトコルとして選択され、匿名ログインが利用できない場合は、直前のコマンドで `<os-identifier>` の前に以下のオプションを指定して、ログインのユーザー名とパスワードを指定します。

```
-A 0 -u <username> -p <password>
```

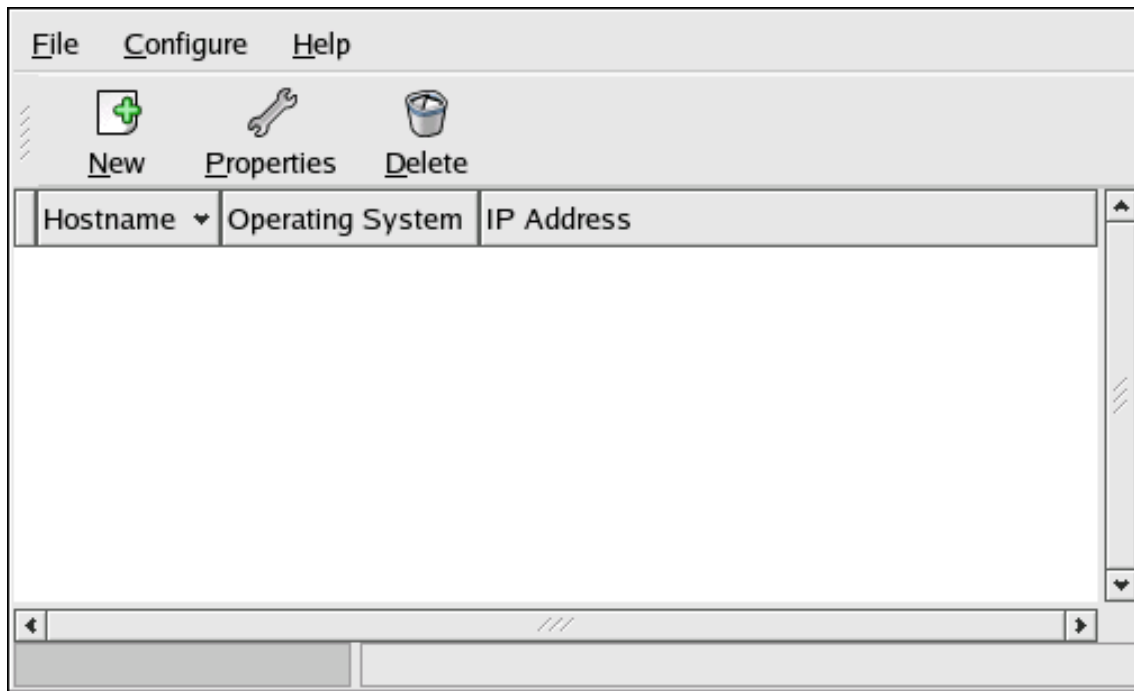
`pxeos` コマンドで使用できるコマンドラインオプションの詳細は、`pxeos` の `man` ページを参照してください。

### 3.3. PXE ホストの追加

ネットワークサーバーを設定すると、[図3.2「ホストの追加」](#) に示されるようにインターフェースが表示されます。



図3.2 ホストの追加



[D]

次の手順では、PXE ブートサーバーに接続できるホストを設定します。このステップのコマンドラインバージョンは、「[コマンドラインからの設定](#)」を参照してください。

ホストを追加するには、新規 ボタンをクリックします。

図3.3 ホストの追加

 A screenshot of a configuration dialog box for adding a host. The dialog has several input fields and a checkbox. 
 - 'Hostname or IP Address/Subnet': text input field containing 'client.example.com'.
 - 'Operating System': dropdown menu showing 'rhel-4-as'.
 - 'Serial Console': checkbox, currently unchecked.
 - 'Diskless OS' section: 'Snapshot name' text input field.
 - 'Network OS Install' section: 'Kickstart File' text input field.
 - 'Ethernet': dropdown menu showing 'eth0'.
 - At the bottom right, there are two buttons: 'Cancel' (with a red X icon) and 'OK' (with a green checkmark icon).

[D]

以下の情報を入力します。

- ホスト名または IP アドレス/ サブネット：インストール用に PXE サーバーに接続できる

必要のある IP アドレス、完全修飾ホスト名、またはシステムのサブネット。

- オペレーティングシステム - このクライアントにインストールするオペレーティングシステムの識別子この一覧は、ネットワークインストールダイアログで作成したネットワークインストールインスタンスから入力されます。
- シリアルコンソール - このオプションではシリアルコンソールを使用できます。
- キックスタート ファイル - `http://server.example.com/kickstart/ks.cfg` など、使用するキックスタートファイルの場所このファイルは、Kickstart Configurator で作成できます。詳細は、[2章 Kickstart Configurator](#) を参照してください。

Snapshot name および Ethernet オプションを無視します。これらはディスクレス環境にのみ使用されます。ディスクレス環境の設定に関する詳細は、[4章 ディスクレス環境](#) を参照してください。

### 3.3.1. コマンドラインからの設定

ネットワークサーバーが X を実行していない場合は、pxeboot ユーティリティー (system-config-netboot パッケージの一部) を使用して、PXE サーバーに接続できるホストを追加することができます。

```
pxeboot -a -K <kickstart> -O <os-identifier> -r <value><host>
```

以下の一覧で、オプションについて説明します。

- **-a:** ホストを追加するように指定します。
- **-k<kickstart>** - キックスタートファイルの場所 (ある場合)。
- **-o <os-identifier>** - 「[PXE ブート設定](#)」で定義されているオペレーティングシステムの識別子を指定します。
- **-r<value>** - ram ディスクのサイズを指定します。

- **<host>**: 追加するホストの IP アドレスまたはホスト名を指定します。

pxeboot コマンドで使用できるコマンドラインオプションの詳細は、pxeboot の man ページを参照してください。

### 3.4. カスタムブートメッセージの追加

必要に応じて、/tftpboot/linux-install/messages/boot.msg を変更して、カスタムブートメッセージを使用します。

### 3.5. PXE インストールの実行

ネットワークから起動する PXE サポートでネットワークインターフェースカードを設定する方法は、NIC のドキュメントを参照してください。カードごとに若干異なります。

インストールプログラムを起動したら、『インストール 『ガイド』』を参照してください。

## 第4章 ディスクレス環境

一部のネットワークには、同じ設定を持つ複数のシステムが必要です。また、これらのシステムの再起動、アップグレード、および管理を簡単に行う必要があります。1つの解決策として、ほとんどのオペレーティングシステムが読み取り専用である **ディスクレス環境** を使用することが、クライアント間の中央サーバーから共有されるという点です。各クライアントには、その他のオペレーティングシステムに対して中央サーバー上に独自のディレクトリーがあります。このディレクトリーは、読み取り/書き込みである必要があります。クライアントを起動するたびに、NFS サーバーからほとんどの OS を読み取り専用としてマウントし、別のディレクトリーを読み取り/書き込みとしてマウントします。各クライアントには独自の読み書きディレクトリーがあるため、あるクライアントが他のクライアントに影響を与えないようにします。

ディスクレスクライアントで実行するように Red Hat Enterprise Linux を設定するには、以下の手順が必要です。

1. ファイルを NFS サーバーにコピーできるように、システムに Red Hat Enterprise Linux をインストールします。（詳細は『『インストールガイド』』を参照してください。）クライアントで使用されるソフトウェアをすべてこのシステムにインストールし、`busybox-anaconda` パッケージがインストールされている必要があります。
2. NFS サーバーにディレクトリーを作成して、ディスクレス環境（`/diskless/i386/RHEL4-AS/` など）を追加します。以下に例を示します。

```
mkdir -p /diskless/i386/RHEL4-AS/
```

このディレクトリーは、**diskless ディレクトリー** と呼ばれます。

3. `root/` という名前のこのディレクトリーのサブディレクトリーを作成します。

```
mkdir -p /diskless/i386/RHEL4-AS/root/
```

4. `rsync` を使用して、クライアントシステムからサーバーに Red Hat Enterprise Linux をコピーします。以下に例を示します。

```
rsync -a -e ssh installed-system.example.com:/diskless/i386/RHEL4-AS/root/
```

この操作の長さは、ネットワーク接続の速度とインストール済みシステムのファイルシステムのサイズによって異なります。これらの要因によっては、この操作に時間がかかる場合があ

ります。

5. **tftp サーバーの起動**
6. **DHCP サーバーの設定**
7. **「ディスクレス環境の設定の完了」**の説明に従って、ディスクレス環境の作成を終了します。
8. **「ホストの追加」**の説明に従って、ディスクレスクライアントを設定します。
9. **各ディスクレスクライアントが PXE 経由で起動し、起動するように設定します。**

#### 4.1. NFS サーバーの設定

オペレーティングシステムの共有専用部分は、NFS 経由で共有されます。

`/etc/exports` に `root/` ディレクトリーおよび `snapshot/` ディレクトリーを追加して、NFS がエクスポートされるように設定します。以下に例を示します。

```
/diskless/i386/RHEL4-AS/root/ *(ro,sync,no_root_squash)
/diskless/i386/RHEL4-AS/snapshot/ *(rw,sync,no_root_squash)
```

\*を「**ホスト名の形式**」で説明されているホスト名形式のいずれかに置き換えます。`hostname` 宣言を可能な限り具体的なものにし、不要なシステムが NFS マウントにアクセスできないようにします。

NFS サービスが実行していない場合は、起動します。

```
service nfs start
```

NFS サービスがすでに実行中の場合は、設定ファイルを再読み込みします。

```
service nfs reload
```

## 4.2. ディスクレス環境の設定の完了

グラフィカルバージョンの Network Booting Tool を使用するには、X Window System を実行し、root 権限で、system-config-netboot 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。デスクトップから Network Booting Tool を起動するには、Applications (パネルのメインメニュー) => System Settings => Server Settings => Network Booting Service に移動します。または、シェルプロンプトで system-config-netboot コマンド (XTerm や GNOME ターミナルなど) を入力します。

Network Booting Tool を初めて開始する場合は、First Time Druid から Diskless を選択します。それ以外の場合は、プルダウンメニューから Configure => Diskless を選択し、Add をクリックします。

プロセスをステップするためのウィザードが表示されます。

1. 最初のページで **Forward** をクリックします。
2. **Diskless Identifier** ページで、ディスクレス環境の **Name** および **Description** を入力します。Forward をクリックします。
3. **「NFS サーバーの設定」** で設定した NFS サーバーの IP アドレスまたはドメイン名、およびディスクレス環境としてエクスポートしたディレクトリーを入力します。Forward をクリックします。
4. ディスクレス環境にインストールされたカーネルバージョンが一覧表示されます。ディスクレスシステムで起動するカーネルバージョンを選択します。
5. **Apply** をクリックして設定を終了します。

Apply をクリックすると、選択したカーネルに基づいてディスクレスカーネルとイメージファイルが作成されます。これらは、PXE ブートディレクトリー /tftpboot/linux-install/ <os-identifier> / にコピーされます。ディレクトリー snapshot/ は、root/ ディレクトリー (例: /diskless/i386/RHEL4-AS/snapshot/) と同じディレクトリーに、そのファイル内の files と呼ばれるファイルを使って作成されます。このファイルには、各ディスクレスシステムに読み書きする必要のあるファイルおよびディレクトリーの一覧が含まれます。このファイルは変更しないでください。追加のエントリーを一覧に追加する必要がある場合には、ファイルと同じディレクトリーに files.custom ファイルを作成し、各行に各ファイルまたはディレクトリーを追加します。

## 4.3. ホストの追加

各ディスクレスクライアントには、読み取り/書き込みファイルシステムとして使用される NFS サーバーに独自の スナップショットディレクトリーが必要です。Network Booting Tool を使用すると、これらのスナップショットディレクトリーを作成できます。

「ディスクレス環境の設定の完了」の手順の実行後に、ディスクレス環境用のホストを追加できるウィンドウが表示されます。New ボタンをクリックします。図4.1「ディスクレスホストの追加」に表示されるダイアログで、以下の情報を入力します。

- ホスト名または IP アドレス/サブネット: ディスクレス環境のホストとして追加するシステムのホスト名または IP アドレスを指定します。システムのグループを指定するためにサブネットを入力します。
- オペレーティングシステム: ホストの、またはホストのサブネット用にディスクレス環境を選択します。
- Serial Console: このチェックボックスを選択し、順次インストールを実行します。
- スナップショット名: ホストの読み取り/書き込みコンテンツすべてを保存するために使用されるサブディレクトリー名を指定します。
- イーサネット - ディスクレス環境をマウントするために使用するホストでイーサネットデバイスを選択します。ホストにイーサネットカードが1つしかない場合は、eth0 を選択します。

キックスタートファイル オプションを無視します。これは PXE インストールにのみ使用されます。

図4.1 ディスクレスホストの追加

Hostname or IP Address/Subnet:	192.168.1.1
Operating System:	rhel-4-as
<input type="checkbox"/> Serial Console	
<b>Diskless OS</b>	<b>Network OS Install</b>
Snapshot name: test1	Kickstart File:
Ethernet: eth0	
<input type="button" value="Cancel"/> <input type="button" value="OK"/>	

[D]

ディスクレスディレクトリーの既存の **snapshot/** ディレクトリーに、ファイル名として指定されたスナップショット名でサブディレクトリーが作成されます。次に、**snapshot/files** および **snapshot/files.custom** にリストされているすべてのファイルは、**root/** ディレクトリーからこの新規ディレクトリーにコピーされます。

#### 4.4. ホストの起動

PXE カードが PXE 経由で起動するようにホストを設定する方法については、ドキュメントを参照してください。

ディスクレスクライアントの起動時に、リモート **root/** ディレクトリーをディスクレスディレクトリーに読み取り専用としてマウントします。また、個別のスナップショットディレクトリーを読み取り/書き込みとしてマウントします。次に、ファイルおよびファイル内のすべてのファイルおよびディレクトリーは、**read-only** のディスクレスディレクトリーで **mount -o** をバインドして、必要に応じてアプリケーションがディスクレス環境の **root** ディレクトリーに書き込みできるようにします。



## 第5章 基本的なシステムの復元

問題が発生しても、それを解決する方法はあります。しかし、それらの方法を実行するには、システムを十分に理解している必要があります。本章では、レスキューモード、シングルユーザーモード、および緊急モードで起動する方法を説明します。このモードでは、独自の知識を使用してシステムを修復できます。

### 5.1. 一般的な問題

以下のいずれかの理由で、これらのリカバリーモードの1つで起動する必要がある場合があります。

- 通常、Red Hat Enterprise Linux で起動することはできません（ランレベル 3 または 5）。
- ハードウェアおよびソフトウェアの問題があり、システムのハード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とします。
- root パスワードを忘れてしまった。

#### 5.1.1. Red Hat Enterprise Linux で起動できない

この問題は多くの場合、Red Hat Enterprise Linux のインストール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によって生じます。他のオペレーティングシステムの中には、コンピューターに他のオペレーティングシステムがないものとみなします。マスターブートレコード(MBR)は、最初に GRUB ブートローダーが含まれているので上書きされます。このようにブートローダーを上書きする場合は、レスキューモードに切り替え、ブートローダーを再設定しない限り、Red Hat Enterprise Linux を起動することはできません。

もう1つの一般的な問題は、パーティションツールを使用してパーティションのサイズを調整したり、インストール後に空き領域から新しいパーティションを作成したりするときに発生します。これにより、パーティションの順番が変更されてしまいます。パーティションの数を変更すると、ブートローダーがパーティションをマウントすることができない可能性があります。この問題を修正するには、レスキューモードで起動し、`/boot/grub/grub.conf` ファイルを変更します。

レスキュー環境から GRUB ブートローダーを再インストールする方法は、「[ブートローダーの再インストール](#)」を参照してください。

#### 5.1.2. ハードウェア/ソフトウェアの問題

このカテゴリにはさまざまな状況が含まれます。例として、ハードドライブが機能しない場合と、ブートローダーの設定ファイル内に無効なルートデバイスまたはカーネルを指定する場合を挙げることができます。これらのいずれかが発生した場合は、Red Hat Enterprise Linux で再起動できない可能性があります。ただし、システムリカバリーモードのいずれかを起動する場合は、問題を解決したり、少なくとも最も重要なファイルのコピーを取得したりできます。

### 5.1.3. root パスワード

root パスワードを忘れた場合はどうしたらよいでしょうか。別のパスワードにリセットするには、レスキューモードまた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 パスワードをリセットします。

## 5.2. レスキューモードでの起動

レスキューモードでは、システムのハードドライブではなく、CD-ROM またはその他の起動方法で、小さな Red Hat Enterprise Linux 環境全体を起動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何かからレスキューします。通常の操作時に、Red Hat Enterprise Linux システムはシステムのハードドライブにあるファイルを使用して、プログラムの実行、ファイルの保存などを行います。

ただし、Red Hat Enterprise Linux を完全に実行できず、システムのハードドライブのファイルにアクセスするだけで十分な場合もあります。レスキューモードを使用すると、ハードドライブから Red Hat Enterprise Linux を実行できない場合でも、システムのハードドライブに保存されているファイルにアクセスできます。

レスキューモードで起動するには、以下のいずれかの方法でシステムを起動する必要があります。[1]:

- インストールブート CD-ROM からシステムを起動する。
- USB フラッシュデバイスなどの他のインストールメディアからシステムを起動する。
- Red Hat Enterprise Linux CD-ROM #1 からシステムを起動する。

上記の方法のいずれかを使用してシステムを起動したら、キーワード `rescue` をカーネルパラメーターとして追加します。たとえば、x86 システムの場合は、インストール起動プロンプトに以下のコマ

ンドを入力します。

```
linux rescue
```

使用する言語など、いくつかの基本的な質問に回答するように求められます。また、有効なレスキューイメージがある場所を選択するように求められます。Local CD-ROM、Hard Drive、NFS イメージ、FTP、または HTTP から選択します。選択したロケーションには有効なインストールツリーが含まれている必要があり、インストールツリーは、ブートした Red Hat Enterprise Linux ディスクと同じバージョンの Red Hat Enterprise Linux である必要があります。ブート CD-ROM またはその他のメディアを使用してレスキューモードを開始している場合、インストールツリーは、メディアが作成されたのと同じツリーからなければなりません。ハードドライブ、NFS サーバー、FTP サーバー、または HTTP サーバーにインストールツリーを設定する方法は、本ガイドの前の項を参照してください。

ネットワーク接続を必要としないレスキューイメージを選択すると、ネットワーク接続を確立するかどうか尋ねられます。ネットワーク接続は、ファイルを別のコンピューターにバックアップする必要がある場合や、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する必要がある場合などに便利です。

以下のメッセージが表示されます。

これで、レスキュー環境は Linux インストールの検索を試行し、`/mnt/sysimage` ディレクトリーにマウントします。その後、システムに必要な変更を加えることができます。この手順を進める場合は、「Continue」を選択します。「Read-only」を選択して、読み取り/書き込みの代わりにファイルシステムを読み取り専用でマウントすることを選択することもできます。何らかの理由でこのプロセスに失敗した場合は「Skip」を選択すると、この手順が省略され、コマンドシェルに直接移動します。

Continue を選択すると、ファイルシステムを `/mnt/sysimage/` ディレクトリーにマウントしようとします。パーティションのマウントに失敗すると、通知されます。Read-Only を選択すると、ファイルシステムを `/mnt/sysimage/` ディレクトリーにマウントしようとしますが、読み取り専用モードになります。スキップを選択すると、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、スキップを選択します。

レスキューモードでシステムを選択すると、VC (仮想コンソール) 1 および VC 2 にプロンプトが表示されます (Ctrl-Alt-F1 キーの組み合わせを使用して VC 1 にアクセスし、Ctrl-Alt-F2 を使用して VC 2 にアクセスします)。

```
sh-3.00b#
```

「Continue」を選択してパーティションを自動的にマウントし、正常にマウントされた場合は、シングルユーザーモードになります。

ファイルシステムがマウントされている場合でも、レスキューモードではデフォルトの `root` パーティションは一時的な `root` パーティションで、通常のユーザーモードで使用されるファイルシステムの `root` パーティションではありません (runlevel 3 または 5)。ファイルシステムのマウントを選択し、正常にマウントされた場合は、次のコマンドを実行してレスキューモード環境の `root` パーティションを、ファイルシステムの `root` パーティションに変更できます。

```
chroot /mnt/sysimage
```

これは、`root` パーティションが `/` としてマウントされる必要がある `rpm` などのコマンドを実行する必要がある場合に便利です。`chroot` 環境を終了するには、`exit` と入力してプロンプトに戻ります。

`Skip` を選択した場合でも、`/foo` などのディレクトリーを作成し、次のコマンドを入力すると、レスキューモード内でパーティションまたは LVM2 論理ボリュームを手動でマウントできます。

```
mount -t ext3 /dev/mapper/VolGroup00-LogVol02 /foo
```

上記のコマンドでは、`/foo` は作成したディレクトリーで、`/dev/mapper/VolGroup00-LogVol02` はマウントする LVM2 論理ボリュームです。パーティションのタイプが `ext2` の場合は、`ext3` を `ext2` に置き換えます。

すべての物理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ると一覧が表示されま

```
fdisk -l
```

LVM2 物理ボリューム、ボリュームグループ、または論理ボリュームの名前がすべて不明な場合は、以下のコマンドを使用して一覧を表示します。

```
pvdisplay
```

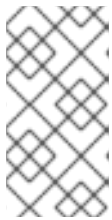
```
vgdisplay
```

```
lvdisplay
```

プロンプトから、以下のような多くの便利なコマンドが実行できます。

- ネットワークが開始されている場合、`ssh`、`scp`、`ping`

- テープドライブのユーザー用に `dump` と `restore`
- パーティションの管理に `parted` と `fdisk`
- ソフトウェアのインストールまたはアップグレードを行うための `RPM`
- 設定ファイルを編集するための `joe`



#### 備考

`emacs`、`pico`、`vi` などの他の一般的なエディターを開始しようとする  
と、`joe` エディターが起動します。

### 5.2.1. ブートローダーの再インストール

多くの場合、`GRUB` ブートローダーが誤って削除、破損したり、他のオペレーティングシステムによって置き換えられることがあります。

以下の手順は、マスターブートレコードに `GRUB` を再インストールするプロセスについて詳述しています。

- インストールメディアからシステムを起動します。
- インストール起動プロンプトで `linux rescue` と入力して、レスキュー環境を入力します。
- `chroot /mnt/sysimage` と入力し、`root` パーティションをマウントします。
- `/sbin/grub-install /dev/hda` と入力して、`GRUB` ブートローダーを再インストールします。`/dev/hda` はブートパーティションに置き換えます。
- `GRUB` が追加のオペレーティングシステムを制御するために追加エントリーが必要になる可能性があるため、`/boot/grub/grub.conf` ファイルを確認してください。

- システムを再起動します。

### 5.3. シングルユーザーモードで起動

シングルユーザーモードの利点の1つは、ブート CD-ROM を必要としないことです。ただし、ファイルシステムを読み取り専用としてマウントするオプションや、ファイルシステムをマウントしない選択肢はありません。

システムが起動していても、起動が完了したとき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てください。

シングルユーザーモードでは、コンピューターがランレベル 1 で起動します。ローカルファイルシステムはマウントされますが、ネットワークがアクティブになっていません。利用可能なシステムメンテナンスシェルがある。レスキューモードとは異なり、シングルユーザーモードは、ファイルシステムのマウントを自動的に試みます。ファイルシステムを正常にマウントできない場合は、シングルユーザーモードを使用しないでください。システムのランレベル 1 設定が破損している場合は、シングルユーザーモードは使用できません。

GRUB を使用する x86 システムで、以下の手順を使用してシングルユーザーモードで起動します。

1. システムの起動時に GRUB スプラッシュ画面で、任意のキーを押して GRUB 対話メニューに入ります。
2. 起動するカーネルバージョンを指定して Red Hat Enterprise Linux を選択し、行を追加する **a** を入力します。
3. 行の最後に移動し、別の単語として **single** を入力します（**Spacebar** を削除してから、**single** を入力します）。**Enter** を押して編集モードを終了します。

### 5.4. 緊急モードでのブート

緊急モードでは、可能な限り最小限の環境で起動します。root ファイルシステムが読み取り専用でマウントされ、ほとんど何も設定されていません。シングルユーザーモードにおける緊急モードの主な利点は、init ファイルが読み込まれないことです。init が破損しているか、または機能していない場合は、再インストール中に失われた可能性のあるデータを回復するためにファイルシステムをマウントできます。

緊急モードで起動するには、「[シングルユーザーモードで起動](#)」のシングルユーザーモードで説明されているのと同じ方法を使用し、キーワード `single` を `emergency` キーワードに置き換えます。

- 
- [1] 詳細は、本ガイドのこれまでの項を参照してください。

## パート II. ファイルシステム

ファイルシステムは、コンピューターに保存されているファイルおよびディレクトリーを参照します。ファイルシステムには、ファイルシステムタイプと呼ばれる形式が異なる場合があります。これらの形式は、情報がファイルおよびディレクトリーとして保存される方法を決定します。ファイルシステムタイプによっては、データの冗長コピーが格納されているものもありますが、ファイルシステムタイプによってはハードドライブへのアクセスが速くなります。ここでは、`ext3`、`swap`、`RAID`、`LVM` ファイルシステムの種類を説明します。また、パーティションおよびアクセス制御リスト(ACL)を管理し、ファイルパーミッションをカスタマイズする `parted` ユーティリティーについても説明します。



## 第6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ジャーナリング ext3 ファイルシステムです。

### 6.1. EXT3 の機能

ext3 ファイルシステムは、基本的に、ext2 ファイルシステムが拡張されたバージョンです。さまざまな改善点により、以下のような利点が提供されます。

#### 可用性

予期しない停電やシステムクラッシュ (クリーンでないシステムシャットダウンとも言われる) が発生すると、マシンにマウントしている各 ext2 ファイルシステムは、e2fsck プログラムで整合性をチェックする必要があります。これは時間を浪費するプロセスであり、大量のファイルを含む大型ボリュームでは、システムの起動時間を著しく遅らせます。このプロセスの間、そのボリュームにあるデータは使用できません。

ext3 ファイルシステムで提供されるジャーナリングは、クリーンでないシステムシャットダウンが発生してもこの種のファイルシステムのチェックが不要であることを意味します。ext3 の使用していても整合性チェックが必要になる唯一の場面は、ハードドライブの障害が発生した場合など、ごく稀なハードウェア障害のケースのみです。クリーンでないシャットダウンの発生後に ext3 ファイルシステムを復元する時間は、ファイルシステムのサイズやファイルの数量ではなく、一貫性を維持するために使用される ジャーナルのサイズに依存します。デフォルトのジャーナルサイズは、ハードウェアの速度に応じて、復旧するのに約 1 秒かかります

#### データの整合性

ext3 ファイルシステムは、クリーンでないシステムのシャットダウンが発生した場合に、より強力なデータ整合性を提供します。ext3 ファイルシステムにより、データが受けることのできる保護のタイプとレベルを選択できるようになります。デフォルトでは、ext3 ボリュームは、ファイルシステムの状態に関して、高いレベルのデータの整合性を維持するように設定されています。

#### 速度

一部のデータを複数回書き込みますが、ext3 のジャーナリングにより、ハードドライブのヘッドモーションが最適化されるため、ほとんどの場合、ext3 のスループットは ext2 よりも高くなります。3 つのジャーナリングモードを選択して速度を最適化できますが、データの整合性に関してトレードオフが生じます。

#### 簡単なトランジション

`ext2` から `ext3` に簡単に移行でき、再フォーマットをせずに、堅牢なジャーナリングファイルシステムの恩恵を受けることができます。このタスクの実行方法は、「[ext3 ファイルシステムへの変換](#)」を参照してください。

以下のセクションでは、`ext3` パーティションの作成およびチューニングの手順を説明します。`ext2` パーティションの場合は、以下のパーティションパーティションおよびフォーマットセクションを省略し、「[ext3 ファイルシステムへの変換](#)」に直接移動します。

## 6.2. EXT3 ファイルシステムの作成

インストール後、`ext3` ファイルシステムを新たに作成しないといけない場合があります。たとえば、システムに新しいディスクドライブを追加する場合は、ドライブを分割して `ext3` ファイルシステムを使用できます。

`ext3` ファイルシステムを作成する手順は次のとおりです。

1. `parted` または `netstat` を使用してパーティションを作成します。
2. `mkfs` を使用して、`ext3` ファイルシステムでパーティションを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. `/etc/fstab` ファイルにパーティションを追加します。

## 6.3. EXT3 ファイルシステムへの変換

`tune2fs` プログラムは、パーティション上にあるデータを変更せずに、既存の `ext2` ファイルシステムにジャーナルを追加できます。ファイルシステムが移行中にすでにマウントされている場合は、ジャーナルがファイルシステムのルートディレクトリーにある `.journal` ファイルとして表示されます。ファイルシステムがマウントされていない場合、ジャーナルは非表示になり、ファイルシステムには全く表示されません。



## 備考

Red Hat Enterprise Linux のデフォルトのインストールでは、すべてのファイルシステムに `ext3` を使用します。

`ext2` ファイルシステムを `ext3` に変換するには、`root` としてログインし、以下を入力します。

```
/sbin/tune2fs -j <file_system>
```

ここで、`<file_system>` は適切な LVM2 ファイルシステムです。

有効な LVM2 ファイルシステムは、以下の 2 つのタイプのエントリーのいずれかになります。

- マップされたデバイス - ボリュームグループの論理ボリューム（例：`/dev/mapper/VolGroup00-LogVol02`）。
- 静的デバイス - 従来のストレージボリューム（例：`/dev/hdbX`）。`hdb` はストレージデバイス名に、`X` はパーティション番号になります。

`df` コマンドを実行して、マウントされたファイルシステムを表示します。LVM ファイルシステムの詳細は、[8章 LVM の設定](#) を参照してください。

これ以降の例では、サンプルコマンドは以下の値を使用します。

```
/dev/mapper/VolGroup00-LogVol02
```

これを行ったら、`/etc/fstab` ファイルでパーティションの種類を `ext2` から `ext3` に変更してください。

`root` ファイルシステムを移行する場合は、`initrd` イメージ（または RAM ディスク）を使用して起動する必要があります。これを作成するには、`mkinitrd` プログラムを実行します。`mkinitrd` コマンドの使用方法は、`man mkinitrd` と入力します。また、`GRUB` 設定が `initrd` を読み込むことを確認します。

この変更を加えても、システムは起動したままですが、ファイルシステムが `ext3` ではなく `ext2` としてマウントされます。

## 6.4. EXT2 ファイルシステムに戻す

`ext3` は比較的新しいため、一部のディスクユーティリティーはまだサポートされていません。たとえば、`resize2fs` でパーティションを縮小する必要がありますが、`ext3` はまだサポートされていません。このような状況では、ファイルシステムを一時的に `ext2` に戻す必要がある場合があります。

パーティションを復元するには、まず `root` としてログインしてパーティションをアンマウントします。

```
umount /dev/mapper/VolGroup00-LogVol02
```

次に、`root` で以下のコマンドを入力して、ファイルシステムタイプを `ext2` に変更します。

```
/sbin/tune2fs -O ^has_journal /dev/mapper/VolGroup00-LogVol02
```

`root` で以下のコマンドを入力して、パーティションにエラーの有無を確認します。

```
/sbin/e2fsck -y /dev/mapper/VolGroup00-LogVol02
```

次に、以下を入力して `ext2` ファイルシステムとしてパーティションを再度マウントします。

```
mount -t ext2 /dev/mapper/VolGroup00-LogVol02/mount/point
```

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

次に、マウントしたディレクトリーに移動して、パーティションのルートレベルで `.journal` ファイルを削除します。

```
rm -f .journal
```

これで、`ext2` パーティションが作成されます。

パーティションを `ext2` に永続的に変更する場合は、必ず `/etc/fstab` ファイルを更新するようにしてください。



## ヒント

`ext2online` を使用して、`ext3` ファイルシステムのサイズを増やすことができます。`ext2online` を使用すると、`ext3` ファイルシステムのマウント（オンライン）およびリズル可能な論理ボリュームで、`ext3` ファイルシステムのサイズを拡大できます。`root` ファイルシステムは、インストール時に LVM2 論理ボリュームにデフォルトで設定されます。

`ext2online` は、`ext3` ファイルシステムでのみ機能することに注意してください。詳細は、`man ext2online` を参照してください。

## 第7章 論理ボリュームマネージャー (LVM)

## 7.1. LVM とは

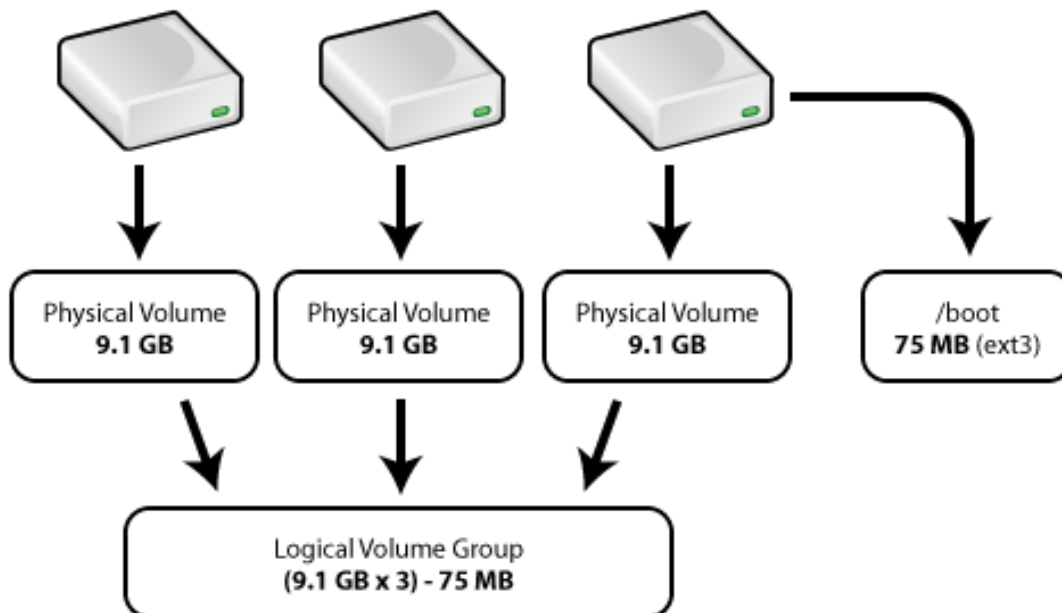
LVM は、ハードドライブの領域を論理ボリュームに割り当て、パーティションの代わりに簡単にサイズ変更できる方法です。

LVM では、ハードドライブまたはハードドライブのセットが 1 つ以上の *物理ボリューム* に割り当てられます。物理ボリュームは、複数のドライブにまたがることはできません。

物理ボリュームは、`/boot/` パーティションを除く *論理ボリュームグループ* に統合されます。`/boot/` パーティションは、ブートローダーが読み取ることができないため、論理ボリュームグループ上に存在できません。`root (/)` パーティションが論理ボリューム上にある場合、ボリュームグループに属さない別の `/boot/` パーティションを作成します。

物理ボリュームは複数のドライブにまたがることはできないため、複数のドライブにまたがるには、ドライブごとに 1 つ以上の物理ボリュームを作成します。

図7.1 論理ボリュームグループ

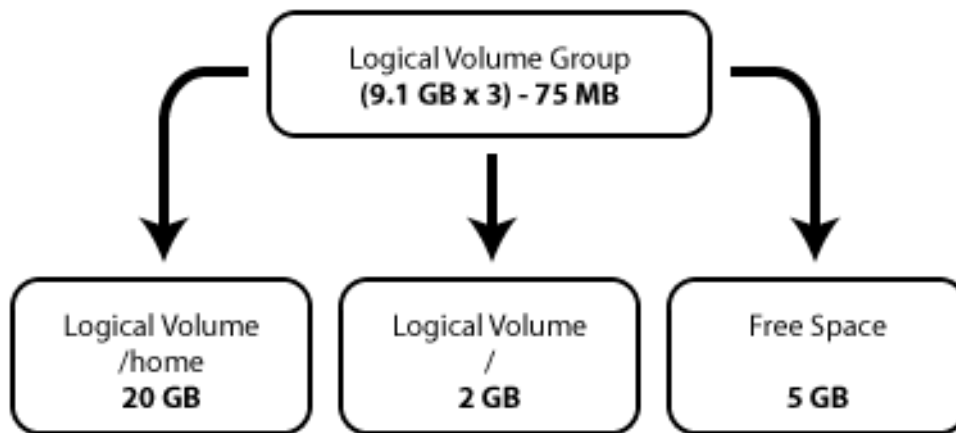


[D]

論理ボリュームグループは、*論理ボリューム*に分割されます。このボリュームには、`/home`、`/m`、ファイルシステムタイプ (`ext2`、`ext3` など) が割り当てられます。「パーティション」がフル容量に到達すると、論理ボリュームグループの空き容量を追加して、パーティションのサイズを増やすことがで

きます。システムに新しいハードドライブを追加すると、そのドライブを論理ボリュームグループに追加できます。また、論理ボリュームであるパーティションを拡張することができます。

図7.2 論理ボリューム



[D]

一方、システムが ext3 ファイルシステムでパーティション設定されている場合、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割されます。パーティションがいっぱいになると、パーティションのサイズを拡張するのは簡単ではありません。パーティションを別のハードドライブに移動した場合でも、元のハードドライブのスペースを別のパーティションとして再割り当てするか、使用しないようにする必要があります。

LVM サポートはカーネルにコンパイルする必要があり、デフォルトの Red Hat カーネルは LVM サポートでコンパイルされます。

インストールプロセス中に LVM を設定する方法は、[8章 LVM の設定](#) を参照してください。

## 7.2. LVM2 とは

LVM バージョン 2 または LVM2 は、2.6 カーネルに含まれるデバイスマッパードライバーを使用する Red Hat Enterprise Linux のデフォルトです。LVM2 は、以前の LVM1 バージョンとほぼ完全に互換性があり、2.4 カーネルを実行する Red Hat Enterprise Linux のバージョンからアップグレードできます。

通常、LVM1 から LVM2 へのアップグレードはシームレスに行われますが、より複雑な要件とアップグレードのシナリオの詳細については、「[関連情報](#)」を参照してください。

## 7.3. 関連情報

これらのソースを使用して、LVM の詳細を確認してください。

### 7.3.1. インストールされているドキュメント

- `rpm -qd lvm` - このコマンドは、man ページなど、lvm パッケージで利用可能なすべてのドキュメントを表示します。
- `lvm help` —このコマンドは、使用可能なすべての LVM コマンドを表示します。

### 7.3.2. 便利な Web サイト

- <http://sourceware.org/lvm2>: 概要やメーリングリストへのリンクを含む LVM2 web ページ。
- <http://tldp.org/HOWTO/LVM-HOWTO/>: Linux ドキュメントプロジェクトの『LVM HOWTO』



## 第8章 LVM の設定

LVM は、グラフィカルインストールプロセス、テキストベースのインストールプロセス、またはキックスタートインストール中に設定できます。lvm パッケージのユーティリティーを使用して、インストール後に独自の LVM 設定を作成できますが、この手順では、インストール時に ディスク Druid を使用してこのタスクを完了できます。

LVM について理解するには、まず [7章論理ボリュームマネージャー \(LVM\)](#) を参照してください。LVM の設定に必要な手順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 ボリュームからのボリュームグループの作成*
- ボリュームグループから *論理ボリューム* を作成し、論理ボリュームのマウントポイントを割り当てます。



### 備考

以下の手順は、GUI のインストール時に示していますが、テキストベースのインストールで同じことができます。

2 9.1 GB の SCSI ドライブ (/dev/sda および /dev/sdb) が以下の例で使用されています。インストール時に、1 つの LVM ボリュームグループと関連する論理ボリュームを使用して、単純な設定を作成する方法が詳細に説明されています。

### 8.1. 自動パーティション設定

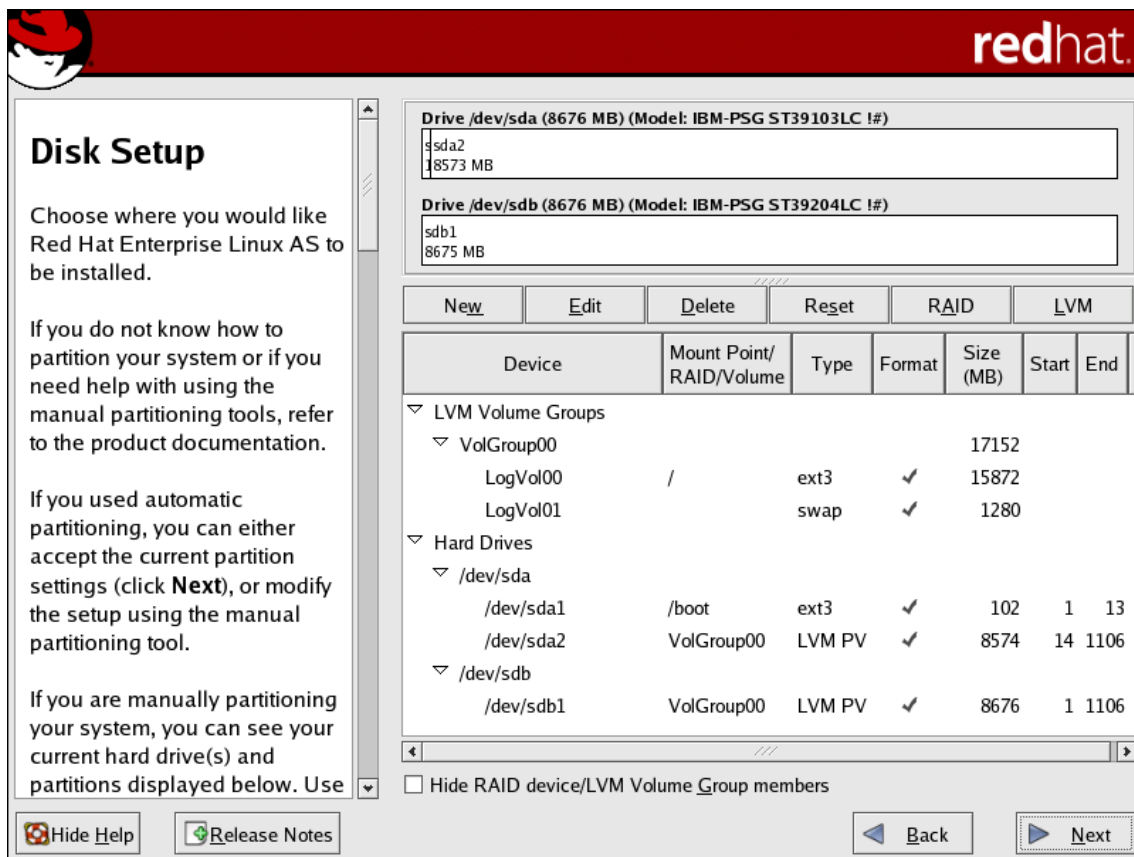
ディスクパーティションセットアップ画面で、*自動パーティション* を選択します。

Red Hat Enterprise Linux の場合は、LVM がディスクパーティション化のデフォルト方法です。LVM を実装しない、または RAID のパーティション設定が必要な場合は、disk Druid で手動でディスクパーティションを設定する必要があります。

以下のプロパティーは、自動作成された設定を構成します。

- `/boot/` パーティションは、独自の非 LVM パーティションにあります。以下の例では、最初のドライブ(`/dev/sda1`)の最初のパーティションです。起動可能なパーティションは LVM 論理ボリュームには存在できません。
- 1 つの LVM ボリュームグループ(VolGroup00)が作成され、選択されたすべてのドライブと利用可能な残りのすべての領域を分割します。以下の例では、最初のドライブ(`/dev/sda2`)の残りのドライブと、2 番目のドライブ全体(`/dev/sdb1`)がボリュームグループに割り当てられます。
- 新規作成したボリュームグループから、LVM 論理ボリューム (LogVol00 および LogVol01) が作成されます。以下の例では、推奨されるスワップ領域は自動的に計算され、LogVol01 に割り当てられ、残りのスワップ領域は root ファイルシステム LogVol00 に割り当てられます。

図8.1 2つの SCSI ドライブを使用した LVM の自動設定



[D]



## 備考

クォータを有効にする場合は、`/home/` や `/var/` などの他のマウントポイントを含めるように自動設定を変更することが推奨されます。これにより、各ファイルシステムに独自の独立したクォータ設定制限を持たせることができます。

多くの場合、デフォルトの LVM パーティションの自動パーティションで十分ですが、高度な実装では LVM パーティションテーブルの変更や手動の設定が必要となる可能性があります。



## 備考

将来のメモリーアップグレードを想定している場合は、ボリュームグループに空き領域の一部を残すことで、システム上のスワップ領域の論理ボリュームを簡単に拡張できます。この場合、LVM の自動設定を変更して、将来の拡張のために利用可能な領域を確保する必要があります。

## 8.2. 手動での LVM パーティション設定

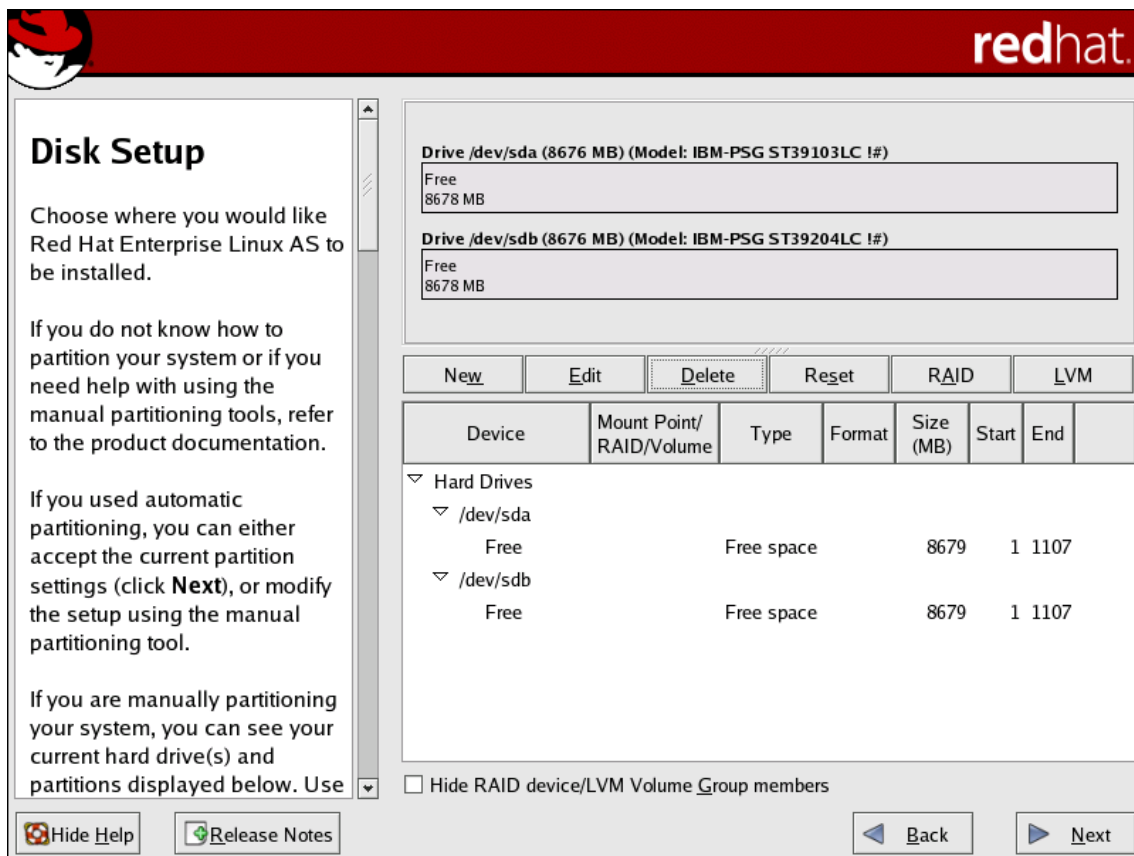
次のセクションでは、Red Hat Enterprise Linux 用に LVM を手動で設定する方法を説明します。LVM でシステムを手動で設定する方法は多数ありますが、以下の例では「[自動パーティション設定](#)」で行ったデフォルト設定と似ています。

ディスクパーティションセットアップ画面で、ディスク Druid を使用した手動パーティションを選択します。

### 8.2.1. `/boot/` パーティションの作成

一般的な状況では、ディスクドライブが新しく、またはフォーマットされたクリーニングです。以下の図の [図8.2 「2つの Blank Drives \(構成に Ready\)」](#) は、パーティションが設定されていない raw デバイスとして、両方のドライブを示しています。

図8.2 2つの Blank Drives (構成に Ready)



[D]

**WARNING**

GRUB ブートローダーは読み取れないため、/boot/ パーティションを LVM ボリュームグループに置くことはできません。

1. **New** を選択します。
2. マウントポイント プルダウンメニューから /boot を選択します。
3. **File System Type** プルダウンメニューから ext3 を選択します。
4. **Allowable Drives** エリアから sda チェックボックスを選択します。

5. Size(MB) メニューの 100 (デフォルト) のままにします。
6. Additional Size Options エリアで Fixed size (デフォルト) ラジオボタンを選択したままにします。
7. Force to a primary partition を選択して、パーティションをプライマリパーティションにします。プライマリパーティションは、ハードドライブの最初の 4 つのパーティションの 1 つです。選択しないと、パーティションが論理パーティションとして作成されます。他のオペレーティングシステムがすでにシステムにインストールされている場合は、このオプションの選択を解除することを検討する必要があります。プライマリパーティションと論理的/拡張パーティションの詳細は、『『インストールガイド』』の付録セクションを参照してください。

入力した値を確認するには、[図8.3「ブートパーティションの作成」](#)を参照してください。

図8.3 ブートパーティションの作成

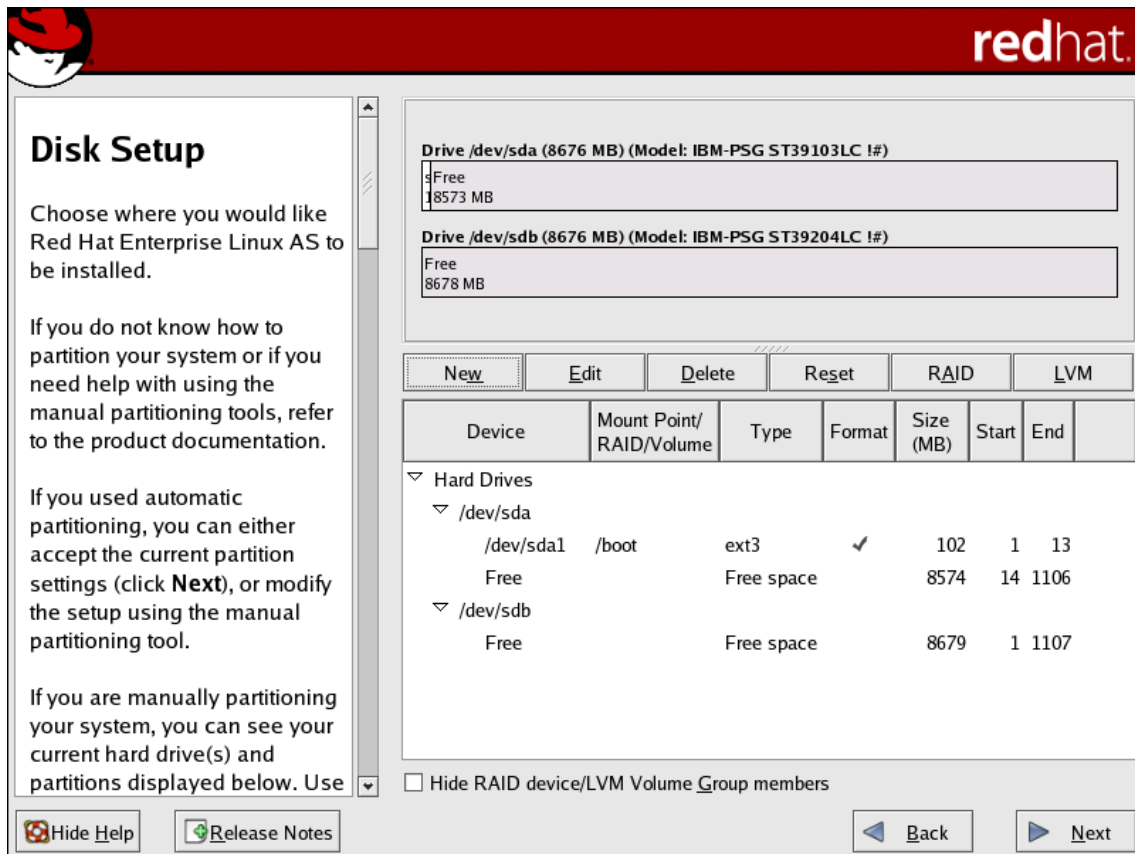
The screenshot shows the 'Add Partition' dialog box with the following configuration:

- Mount Point: /boot
- File System Type: ext3
- Allowable Drives:  sda 8676 MB IBM-PSG ST39103LC !#  
 sdb 8676 MB IBM-PSG ST39204LC !#
- Size (MB): 100
- Additional Size Options:
  - Fixed size
  - Fill all space up to (MB): 1
  - Fill to maximum allowable size
- Force to be a primary partition

[D]

OK をクリックしてメイン画面に戻ります。以下の図は、ブートパーティションが正しく設定されていることを確認します。

図8.4 /boot/ パーティションの表示



[D]

## 8.2.2. LVM 物理ボリュームの作成

ブートパーティションを作成したら、残りのディスク領域を LVM パーティションに割り当てることができます。LVM の実装を正常に作成するための最初の手順は、物理ボリュームの作成です。

1. **New** を選択します。
2. 図8.5「物理ボリュームの作成」に示されるように、File System Type 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8.5 物理ボリュームの作成

[D]

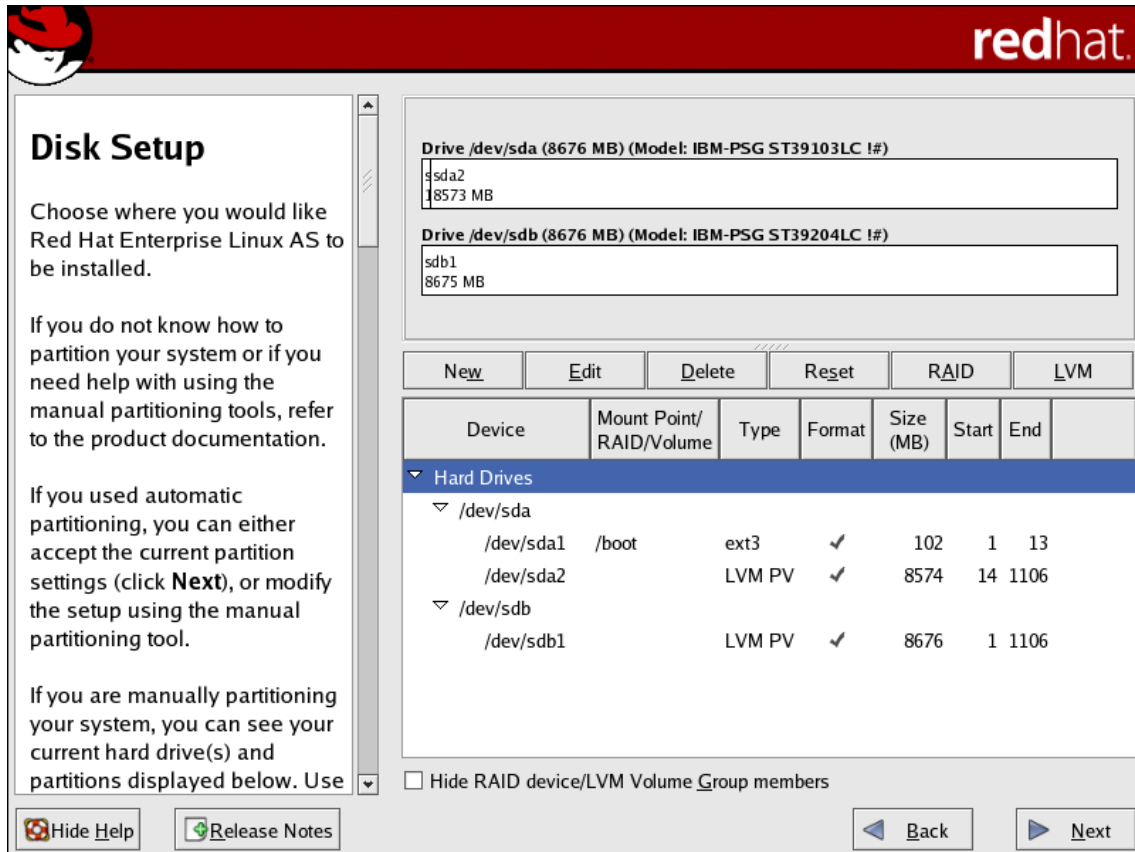
3. マウントポイントは、まだ入力できません（すべての物理ボリュームを作成した後にすべてのボリュームグループを作成すると可能になります）。
4. 物理ボリュームは、1つのドライブに制限する必要があります。Allowable Drives には、物理ボリュームを作成するドライブを選択します。複数のドライブがある場合は、すべてのドライブが選択され、1つのドライブからすべての選択を解除する必要があります。
5. 物理ボリュームのサイズを入力します。
6. Fixed size を選択して、指定したサイズに物理ボリュームを作成し、Fill all space up to(MB) を選択し、物理ボリュームサイズの範囲を MB 単位で入力するか、最大許容サイズを選択してハードディスク上の利用可能な領域をすべて埋めます。複数の拡張を可能にすると、ディスクの空き容量を共有します。
7. パーティションをプライマリーパーティションにするには、Force to a primary partition を選択します。

## 8.

OK をクリックしてメイン画面に戻ります。

これらの手順を繰り返して、LVM 設定に必要な物理ボリュームをいくつでも作成します。たとえば、ボリュームグループを複数のドライブにまたがるようにするには、ドライブごとに物理ボリュームを作成します。以下の図は、反復プロセス後に完了した両方のドライブを示しています。

図8.6 2つの物理ボリュームが作成される



[D]

### 8.2.3. LVM ボリュームグループの作成

すべての物理ボリュームを作成したら、ボリュームグループを作成できます。

## 1.

LVM ボタンをクリックして、物理ボリュームをボリュームグループに収集します。ボリュームグループは、基本的には物理ボリュームの集合です。複数の論理ボリュームグループを設定できますが、物理ボリュームは1つのボリュームグループにしか存在できません。





## 備考

論理ボリュームグループに、オーバーヘッドのディスク領域が予約されています。物理ボリュームの合計はボリュームグループのサイズと同じではない場合がありますが、表示される論理ボリュームのサイズは正しくありません。

図8.7 LVM ボリュームグループの作成

**Make LVM Volume Group**

Volume Group Name:

Physical Extent:

Physical Volumes to Use:

<input checked="" type="checkbox"/>	sda2	8512.00 MB
<input checked="" type="checkbox"/>	sdb1	8640.00 MB

Used Space: 0.00 MB (0.0 %)  
 Free Space: 17152.00 MB (100.0 %)  
 Total Space: 17152.00 MB

Logical Volumes

Logical Volume Name	Mount Point	Size (MB)

Buttons: Add, Edit, Delete, Cancel, OK

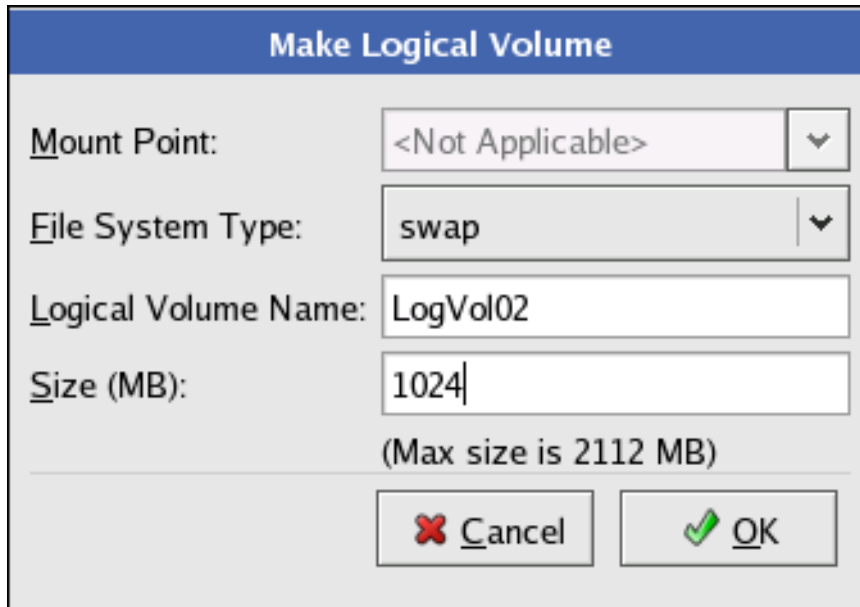
[D]

2. 必要に応じて ボリュームグループ名 を変更します。
3. ボリュームグループ内の論理ボリュームはすべて、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 32 MB に設定されています。そのため、論理ボリュームのサイズは 32 MB で除算する必要があります。32 MB の単位ではないサイズを入力すると、インストールプログラムは、32 MB の単位で最も近いサイズを自動的に選択します。この設定を変更することは推奨されません。
4. ボリュームグループに使用する物理ボリュームを選択します。

## 8.2.4. LVM 論理ボリュームの作成

、`/home/`、`swap` 領域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することはできないことに注意してください。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。図8.8「論理ボリュームの作成」に示されているようにダイアログウィンドウが表示されます。

図8.8 論理ボリュームの作成



Make Logical Volume

Mount Point: <Not Applicable>

File System Type: swap

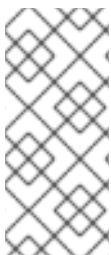
Logical Volume Name: LogVol02

Size (MB): 1024  
(Max size is 2112 MB)

Cancel OK

[D]

作成するボリュームグループごとに、この手順を繰り返します。



### ヒント

論理ボリュームを後で拡張できるように、論理ボリュームグループに空き領域の一部を残すこともできます。デフォルトの自動設定はこれを行いませんが、この手動設定の例は今後の拡張用に約 1 GB の空き領域として残されます。

図8.9 保留中の論理ボリューム

Make LVM Volume Group

**Volume Group Name:**

**Physical Extent:**

**Physical Volumes to Use:**

<input checked="" type="checkbox"/>	sda2	8512.00 MB
<input checked="" type="checkbox"/>	sdb1	8640.00 MB

Used Space: 16064.00 MB (93.7 %)  
 Free Space: 1088.00 MB ( 6.3 %)  
 Total Space: 17152.00 MB

**Logical Volumes**

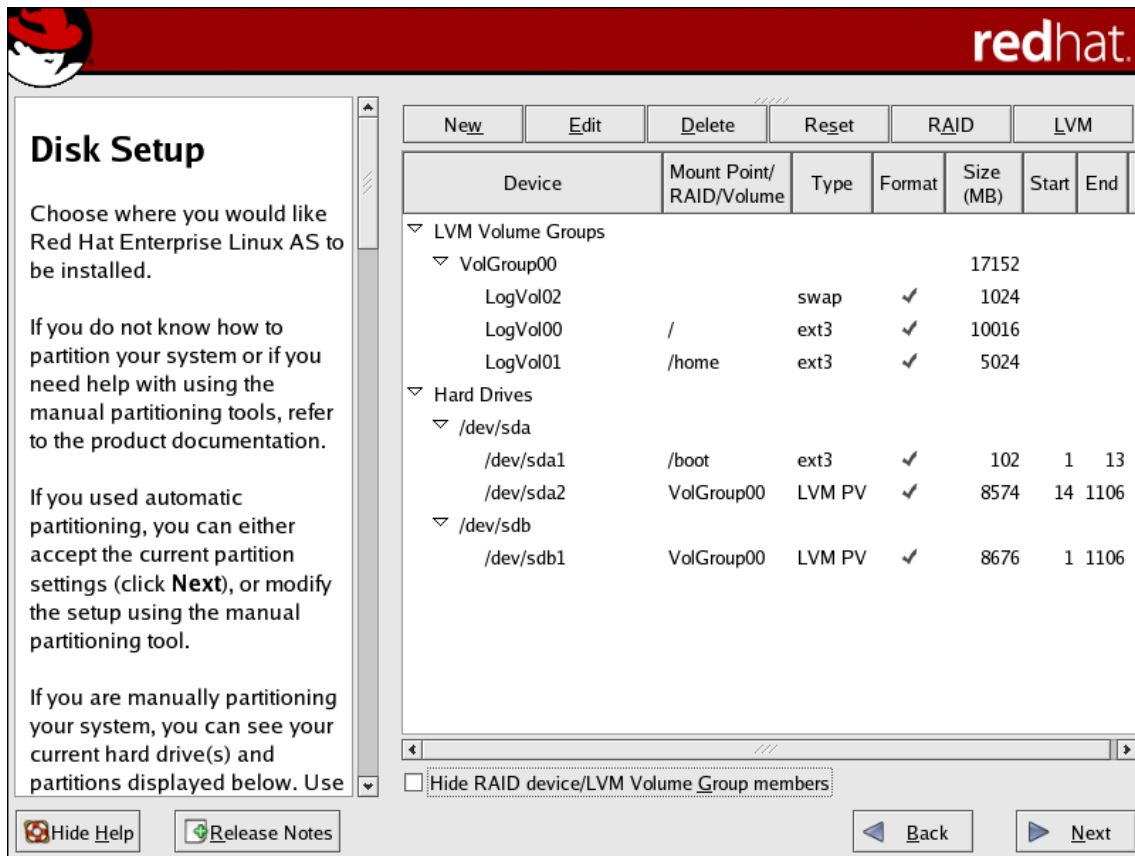
Logical Volume Name	Mount Point	Size (MB)
LogVol00	/	10016
LogVol01	/home	5024
LogVol02	N/A	1024

[D]

OK をクリックして、ボリュームグループと、関連するすべての論理ボリュームを適用します。

以下の図は、最終的な手動設定を示しています。

図8.10 最終の手動設定



[D]

## 第9章 RAID (REDUNDANT ARRAY OF INDEPENDENT DISKS)

### 9.1. RAID とは

RAID の登場した背景には、容量が小さく手頃なディスクドライブを複数集めてアレイに結合させ、容量が大きく高価なドライブに負けないパフォーマンスと冗長性を実現しようとする動きがありました。この複数のデバイスからなるアレイは、コンピューター上では単一の論理ストレージユニットまたはドライブとして表されます。

RAID は、情報が複数のディスクに分散される方法です。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)、および パリティ (RAID レベル 5) でのディスクストライピングなどの技術を使用して、冗長性、レイテンシーの短縮、ディスクの読み取りや書き込みのための帯域幅の向上、ハードディスクのクラッシュから復旧する機能を最大化します。

RAID の基本的な概念は、アレイ内の各ドライブにデータを一貫した方法で分散できることです。これを実行するには、データを最初に一貫して使用する チャンクに分割する必要があります (サイズが 32K または 64K のサイズは異なります)。各チャンクは、使用される RAID レベルに従って、RAID アレイのハードドライブに書き込まれます。データを読み取る場合、プロセスは逆になり、アレイ内の複数のドライブが実際には 1 つの大きなドライブであることを確認できます。

### 9.2. RAID を使用するユーザー

大量のデータを維持する必要がある場合 (システム管理者など) は、RAID テクノロジーを使用して利点があります。RAID を使用する主な理由は次のとおりです。

- 改善された速度
- 1 つの仮想ディスクを使用したストレージ容量の拡張
- ディスク障害の影響を軽減

### 9.3. ハードウェア RAID とソフトウェア RAID の比較

考えられる RAID 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。

#### 9.3.1. ハードウェア RAID

ハードウェアベースのアレイは、ホストから RAID サブシステムを管理し、RAID アレイごとに 1

つのディスクのみを提示します。

ハードウェア RAID デバイスの例は、SCSI コントローラーに接続し、RAID アレイを 1 つの SCSI ドライブとして表示するものです。外部 RAID システムは、「intelligence」のすべての RAID 処理を、外部ディスクサブシステムにあるコントローラーに移動します。サブシステム全体が通常の SCSI コントローラーを介してホストに接続され、1 つのディスクとしてホストに表示されます。

RAID コントローラーは、オペレーティングシステムへの SCSI コントローラーのように動作し、実際のドライブ通信自体すべてを処理するカードの形式にも提供されます。このような場合は、SCSI コントローラーと同様にドライブを RAID コントローラーにプラグインしますが、RAID コントローラーの設定に追加し、オペレーティングシステムは違いを認識しません。

### 9.3.2. ソフトウェア RAID

ソフトウェア RAID では、カーネルディスク (ブロックデバイス) コード内に各種の RAID レベルを実装しています。高価ディスクコントローラーカードやホットスワップシャーシなど、最優先的な解決策を提供します。[2] 必須ではありません。ソフトウェア RAID は、SCSI ディスクだけでなく安価な IDE ディスクでも機能します。現在高速な CPU により、ソフトウェア RAID のパフォーマンスは、ハードウェア RAID に対して調査できます。

Linux カーネルの MD ドライバーは、完全にハードウェアに依存しない RAID ソリューションの例です。ソフトウェアベースのアレイのパフォーマンスは、サーバーの CPU パフォーマンスと負荷によって異なります。

インストール時にソフトウェア RAID を設定する方法は、[10章ソフトウェア RAID の設定](#)を参照してください。

ソフトウェア RAID が提供する詳細を知るには、以下に最も重要な機能を紹介します。

- スレッド再構築プロセス
- カーネルベースの設定
- 再構築なしで Linux マシン間でのアレイの移植性

- アイドルシステムリソースを使用したバックグラウンドのアレイ再構築
- ホットスワップ可能なドライブのサポート
- 特定の CPU 最適化を利用する自動 CPU 検出

#### 9.4. RAID レベルとリニアサポート

RAID は、レベル 0、1、4、5、リニアなどのさまざまな設定に対応します。これらの RAID タイプは以下のように定義されます。

- レベル 0: RAID レベル 0 は、多くの場合「ストライプ化」と呼ばれ、パフォーマンス指向のストライプ化データマッピング技術です。これは、アレイに書き込まれるデータがストライプに分割され、アレイのメンバーディスク全体に書き込まれることを意味します。これにより低い固有コストで高い I/O パフォーマンスを実現できますが、冗長性は提供されません。レベル 0 アレイのストレージ容量は、ハードウェア RAID 内のメンバーディスクの合計容量、またはソフトウェア RAID 内のメンバーパーティションの合計容量と同じになります。
- レベル 1: RAID レベル 1 または「ミラーリング」は、他の RAID 形式よりも長く使用されています。レベル 1 は、アレイ内の各メンバーディスクに同一データを書き込むことで冗長性を提供し、各ディスクに対して「ミラーリング」コピーをそのまま残します。ミラーリングは、データの可用性の単純化と高レベルにより、いまでも人気があります。レベル 1 は、2 つ以上のディスクで動作します。このディスクは、読み取り時に、データ転送率が高いのに並列アクセスを使用できるものの、一般的には独立して動作し、高い I/O トランザクションレートを提供します。レベル 1 は、非常に優れたデータの信頼性を提供し、読み取り集中型アプリケーションのパフォーマンスを向上しますが、比較的成本が高くなります。<sup>[3]</sup> レベル 1 アレイのストレージ容量は、ハードウェア RAID でミラーリングされたハードディスクのいずれかの容量と同じか、またはソフトウェア RAID にミラーリングされたパーティションの 1 つと等しくなります。
- レベル 4: レベル 4 でパリティを使用<sup>[4]</sup> データを保護するため、1 つのディスクドライブで連結します。これは、大きなファイル転送ではなく、トランザクション I/O に適しています。専用のパリティディスクは固有のボトルネックを表すため、レベル 4 は、ライトバックキャッシングなどの付随するテクノロジーを使用せずに使用されます。RAID レベル 4 は、一部の RAID パーティションスキームではオプションですが、Red Hat Enterprise Linux RAID インストールではオプションは使用できません。<sup>[5]</sup> ハードウェア RAID レベル 4 のストレージ容量はメンバーディスクの容量と同じで、1 つのメンバーディスクの容量を引いたことができます。ソフトウェア RAID レベル 4 のストレージ容量は、メンバーパーティションの容量と同じで、パーティションのサイズを等しい場合は、パーティションの 1 つを減算します。
- レベル 5: これは RAID の最も一般的なタイプです。RAID レベル 5 は、アレイのメンバー

ディスクドライブの一部またはすべてにパリティを分散することで、レベル 4 に固有の書き込みボトルネックを排除します。パリティ計算プロセスのみがパフォーマンスのボトルネックです。最新の CPU とソフトウェア RAID では、通常非常に大きな問題ではありません。レベル 4 と同様に、読み取りは書き込みを大幅に上回ります。レベル 5 は、多くの場合、ライトバックキャッシングで使用され、アクレトリーを削減します。ハードウェア RAID レベル 5 のストレージ容量はメンバーディスクの容量と同じで、1 つのメンバーディスクの容量を引いたことができます。ソフトウェア RAID レベル 5 のストレージ容量は、メンバーパーティションの容量と同じで、パーティションのサイズを等しい場合は、パーティションの 1 つを減算します。

- リニア RAID - リニア RAID は、より大きな仮想ドライブを作成するためのドライブを簡単にグループ化したものです。リニア RAID では、あるメンバードライブからチャンクが順次割り当てられます。最初のドライブが完全に満杯になったときにのみ次のドライブに移動します。これにより、メンバードライブ間の I/O 操作が分割される可能性はないため、パフォーマンスの向上は見られません。リニア RAID には冗長性がなく、実際に、信頼性は低下します。いずれかのメンバードライブに障害が発生した場合は、アレイ全体を使用することができません。容量はすべてのメンバーディスクの合計になります。

---

[2]

ホットスワップシャーシを使用すると、システムの電源を切らずにハードドライブを削除できます。

[3]

RAID レベル 1 は、ドライブ領域を無駄にするアレイ内のすべてのディスクに同じ情報を書き込むため、高価になります。たとえば、`root(/)`パーティションが 2 つの 40G ドライブに存在するように RAID レベル 1 が設定されている場合は、合計 80G があり、その 80G の 40G のみにアクセスできます。他の 40G は最初の 40G のミラーのように動作します。

[4]

パリティ情報は、アレイ内の残りのメンバーディスクのコンテンツに基づいて計算されます。この情報は、アレイ内のいずれかのディスクに障害が発生した場合にデータの再構築に使用できます。その後、再構築されたデータを使用して、交換前に失敗したディスクに I/O 要求に対応でき、交換後に失敗したディスクを接続します。

[5]

RAID レベル 4 は、RAID レベル 5 と同じ領域を使用しますが、レベル 5 の方が利点があります。このため、レベル 4 はサポートされません。



## 第10章 ソフトウェア RAID の設定

ソフトウェア RAID は、グラフィカルインストールプロセス、テキストベースのインストールプロセス、またはキックスタートインストール中に設定できます。本章では、ディスク Druid インターフェースを使用して、インストール時にソフトウェア RAID を設定する方法を説明します。

**9章 RAID (Redundant Array of Independent Disks)** は、最初に RAID、ハードウェアおよびソフトウェア RAID の相違点、および RAID 0、1、および 5 の相違点を参照してください。RAID の設定に必要な手順の概要を以下に示します。

- ソフトウェア RAID パーティションを物理ハードドライブに適用する。  
  
起動パーティション(/boot/)が RAID 分割に存在する場合は、RAID 1 パーティション上にある必要があります。
- ソフトウェア RAID パーティションから RAID デバイスを作成する。
- 必要に応じて、RAID デバイスから LVM を設定します。RAID の設定後に LVM を設定する方法は、**8章 LVM の設定** を参照してください。
- RAID デバイスから ファイルシステムを作成する。



### 備考

以下の手順は、GUI のインストール時に示していますが、テキストベースのインストールで同じことができます。

ソフトウェア RAID の設定は、インストールプロセス時に ディスク Druid で手動で行う必要があります。

2 9.1 GB の SCSI ドライブ (/dev/sda および /dev/sdb) が以下の例で使用されています。複数の RAID デバイスを実装して、シンプルな RAID 1 設定を作成する方法について詳しく説明します。

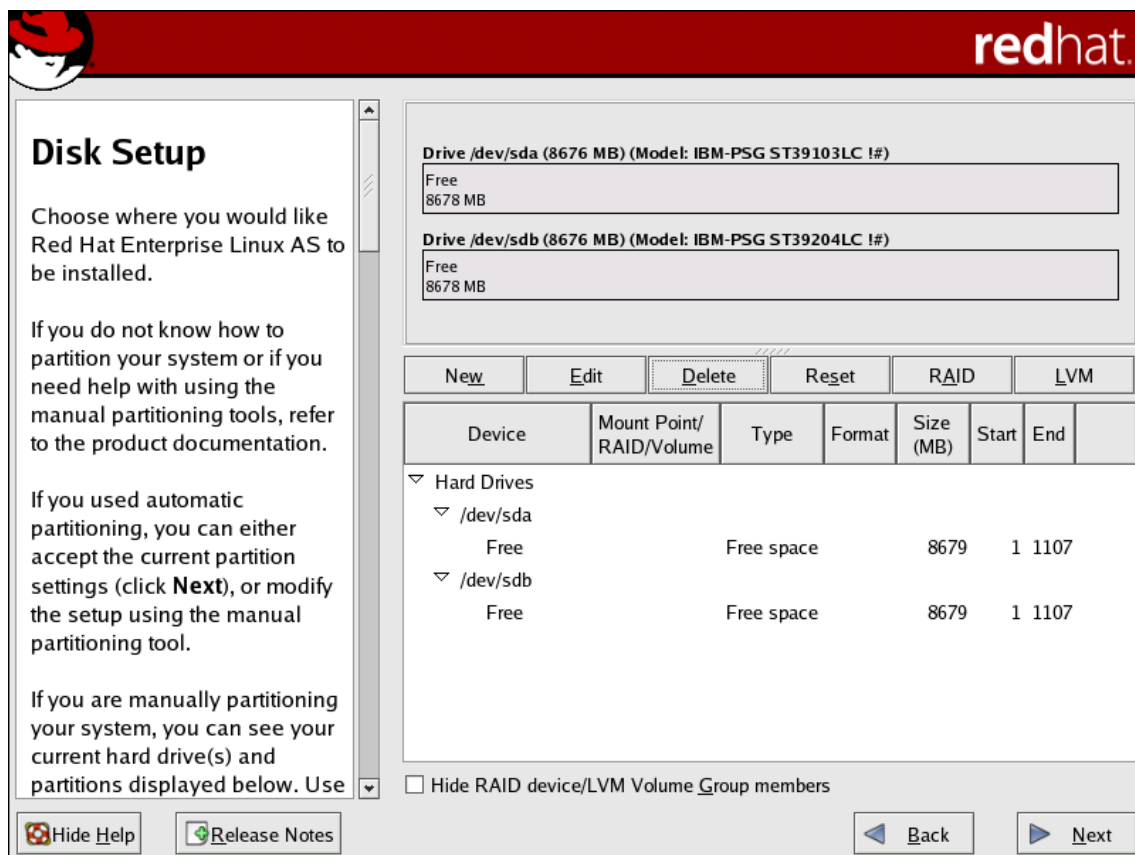
ディスクパーティションセットアップ画面で、ディスク Druid を使用した手動パーティション を 選

択します。

## 10.1. RAID パーティションの作成

一般的な状況では、ディスクドライブが新規またはフォーマットされます。両方のドライブは、[図 10.1 「2つの Blank Drives \(構成に Ready\)」](#) にパーティション設定のない raw デバイスとして表示されます。

図10.1 2つの Blank Drives (構成に Ready)

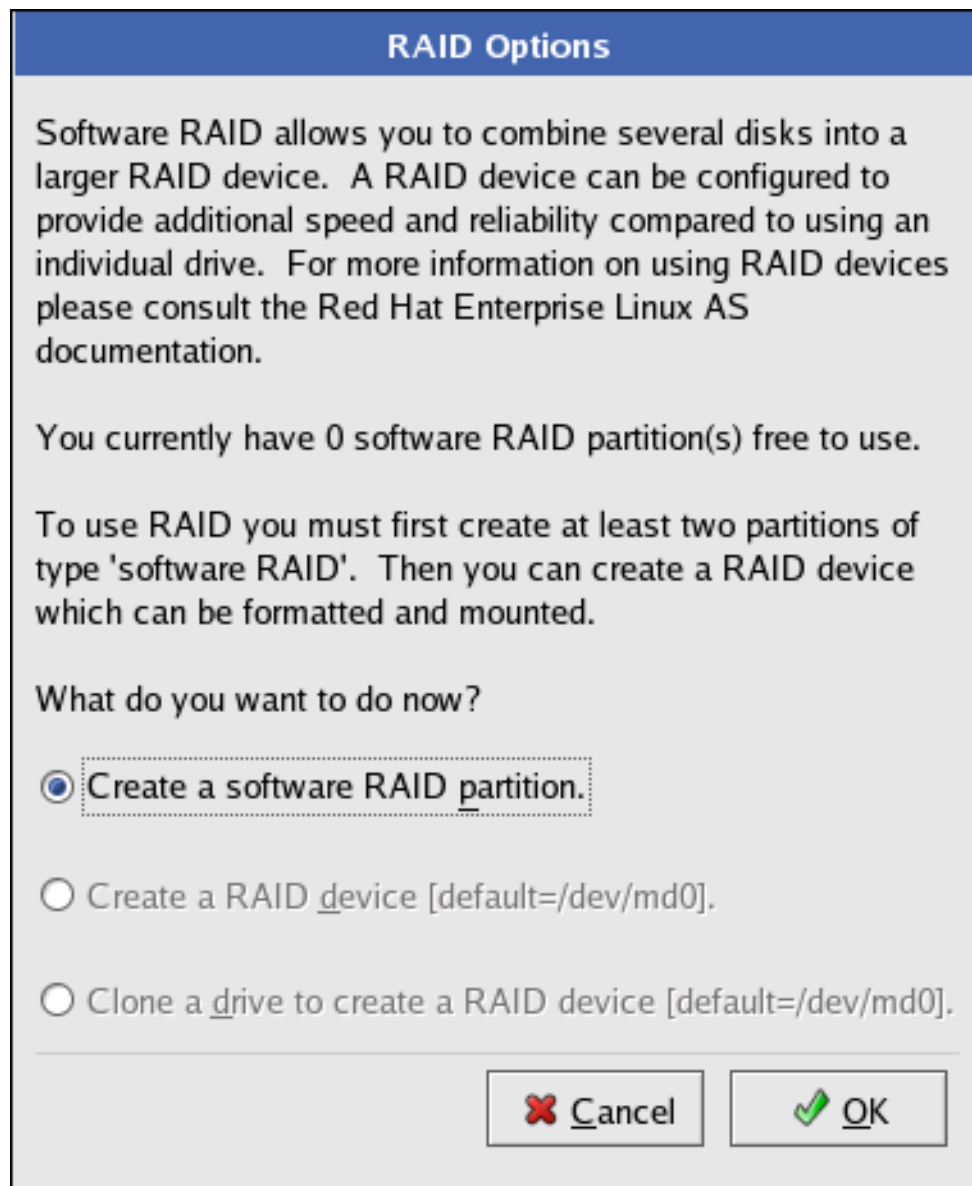


[D]

1. Disk Druid で RAID を選択し、ソフトウェア RAID の作成画面を入力します。

2. [図10.2 「RAID パーティションオプション」](#) にあるように、ソフトウェア RAID パーティションの作成を選択して、RAID パーティションを作成します。RAID パーティションと RAID デバイスが作成されるまで、その他の RAID オプション（マウントポイントの入力など）はできません。

図10.2 RAID パーティションオプション



[D]

3.

ソフトウェア RAID パーティションは、1つのドライブに制限する必要がありません。Allowable Drives 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、すべてのドライブが選択され、1つのドライブからすべての選択を解除する必要があります。

図10.3 RAID パーティションの追加

**Add Partition**

Mount Point: <Not Applicable>

File System Type: software RAID

Allowable Drives:

<input checked="" type="checkbox"/>	sda	8676 MB	IBM-PSG ST39103LC !#
<input type="checkbox"/>	sdb	8676 MB	IBM-PSG ST39204LC !#

Size (MB): 100

Additional Size Options

Fixed size

Fill all space up to (MB): 1

Fill to maximum allowable size

Force to be a primary partition

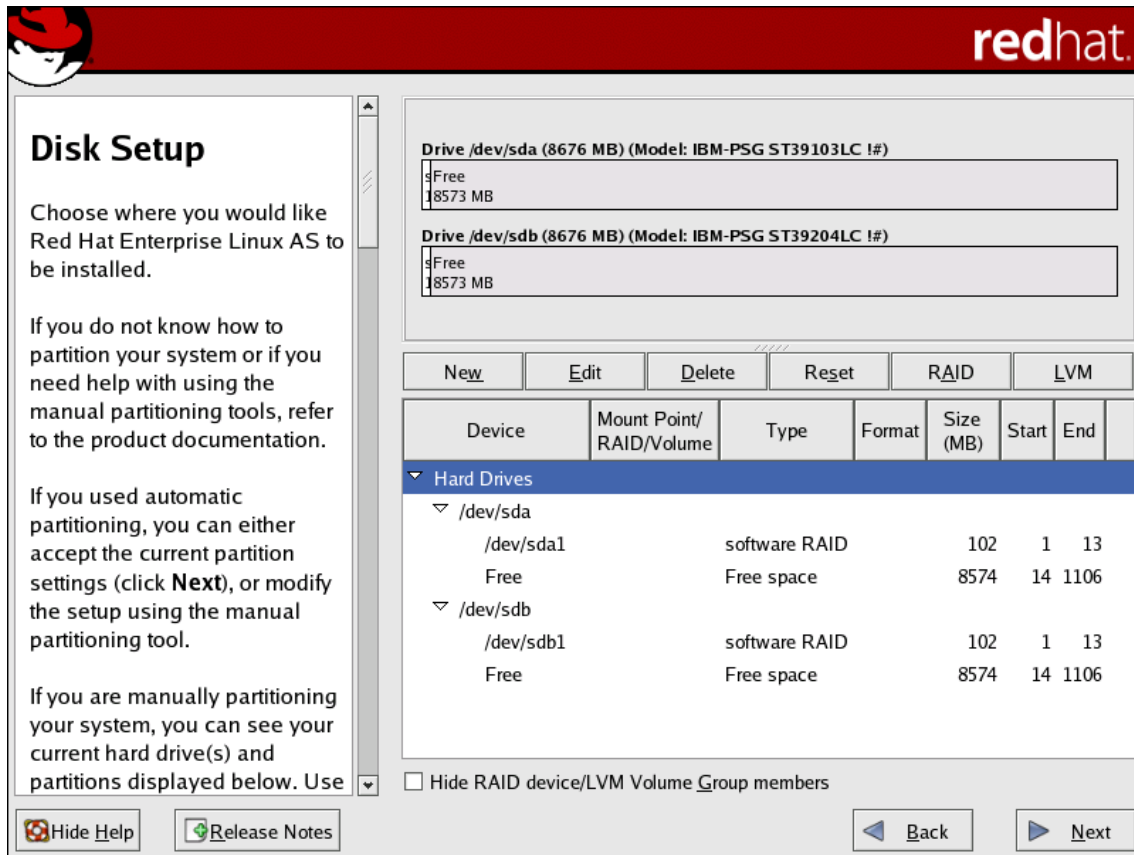
Cancel OK

[D]

4. パーティションを設定するサイズを入力します。
5. **Fixed size** を選択してパーティションの指定サイズを作成し、**Fill all space up to(MB)** を選択し、パーティションサイズの範囲を **MB** 単位で入力するか、**Fill** を選択して、ハードディスクで利用可能な領域をすべて埋めます。複数のパーティションを拡大できる場合は、ディスクで利用可能な空き領域を共有します。
6. パーティションをプライマリーパーティションにするには、**Force to a primary partition** を選択します。プライマリーパーティションは、ハードドライブの最初の 4 つのパーティションの 1 つです。選択しないと、パーティションが論理パーティションとして作成されます。他のオペレーティングシステムがすでにシステムにインストールされている場合は、このオプションの選択を解除することを検討する必要があります。プライマリーパーティションと論理的/拡張パーティションの詳細は、『『インストールガイド』』の付録セクションを参照してください。
7. **OK** をクリックしてメイン画面に戻ります。

この手順を繰り返して、RAID 設定に必要なパーティションを多数作成します。すべてのパーティションを RAID パーティションにする必要はありません。たとえば、/boot/ パーティションのみをソフトウェア RAID デバイスとして設定し、root パーティション(/)、/home/、および swap を通常のファイルシステムとして残すことができます。図10.4「RAID 1 パーティションが Ready、Pre-Device、および Mount Point の作成」 RAID 1 設定 (/boot/の場合) に正常に割り当てられた領域が表示されます。これは、RAID デバイスとマウントポイントの作成の準備が整いました。

図10.4 RAID 1 パーティションが Ready、Pre-Device、および Mount Point の作成



[D]

## 10.2. RAID デバイスとマウントポイントの作成

ソフトウェア RAID パーティションとしてパーティションをすべて作成したら、以下の手順で RAID デバイスとマウントポイントを作成します。

1. Disk Druid main partitioning 画面で RAID ボタンを選択します ( 図10.5 「RAID オプション」 を参照) 。
2. 図10.5 「RAID オプション」 が表示されます。Create a RAID device を選択します。

図10.5 RAID オプション



[D]

3.

次に 図10.6 「RAID デバイスの作成およびマウントポイントの割り当て」が表示されます。ここでは、RAID デバイスを作成してマウントポイントを割り当てることができます。

図10.6 RAID デバイスの作成およびマウントポイントの割り当て

The screenshot shows a dialog box titled "Make RAID Device". It contains the following fields and options:

- Mount Point:** /boot
- File System Type:** ext3
- RAID Device:** md0
- RAID Level:** RAID0
- RAID Members:** A list with two entries:  sda1 102 MB and  sdb1 102 MB.
- Number of spares:** 0

At the bottom right, there are two buttons: "Cancel" (with a red X icon) and "OK" (with a green checkmark icon).

[D]

4. マウントポイントを入力します。
5. パーティションのファイルシステムタイプを選択します。この時点で、動的 LVM ファイルシステム、または従来の静的 ext2/ext3 ファイルシステムを設定できます。RAID デバイスに LVM を設定する方法は、物理ボリューム(LVM) を選択してから [8章 LVM の設定](#) を参照してください。LVM が必要ない場合は、以下の手順に進んでください。
6. RAID デバイスの md0 などのデバイス名を選択します。
7. RAID レベルを選択します。RAID 0、RAID 1、および RAID 5 から選択できます。実装する RAID レベルの決定にサポートが必要な場合は、[9章 RAID \(Redundant Array of Independent Disks\)](#) を参照してください。

## 備考

`/boot/` の RAID パーティションを作成する場合は、RAID レベル 1 を選択する必要があります。また、最初の 2 つのドライブ (IDE 1、SCSI 2) のいずれかを使用する必要があります。`/boot/` の RAID パーティションを作成しておらず、`root` ファイルシステム(/)用に RAID パーティションを作成している場合は、RAID レベル 1 にする必要があります。また、最初の 2 つのドライブ (IDE 1、SCSI 2) のいずれかを使用する必要があります。

図10.7 /boot/ マウントエラー



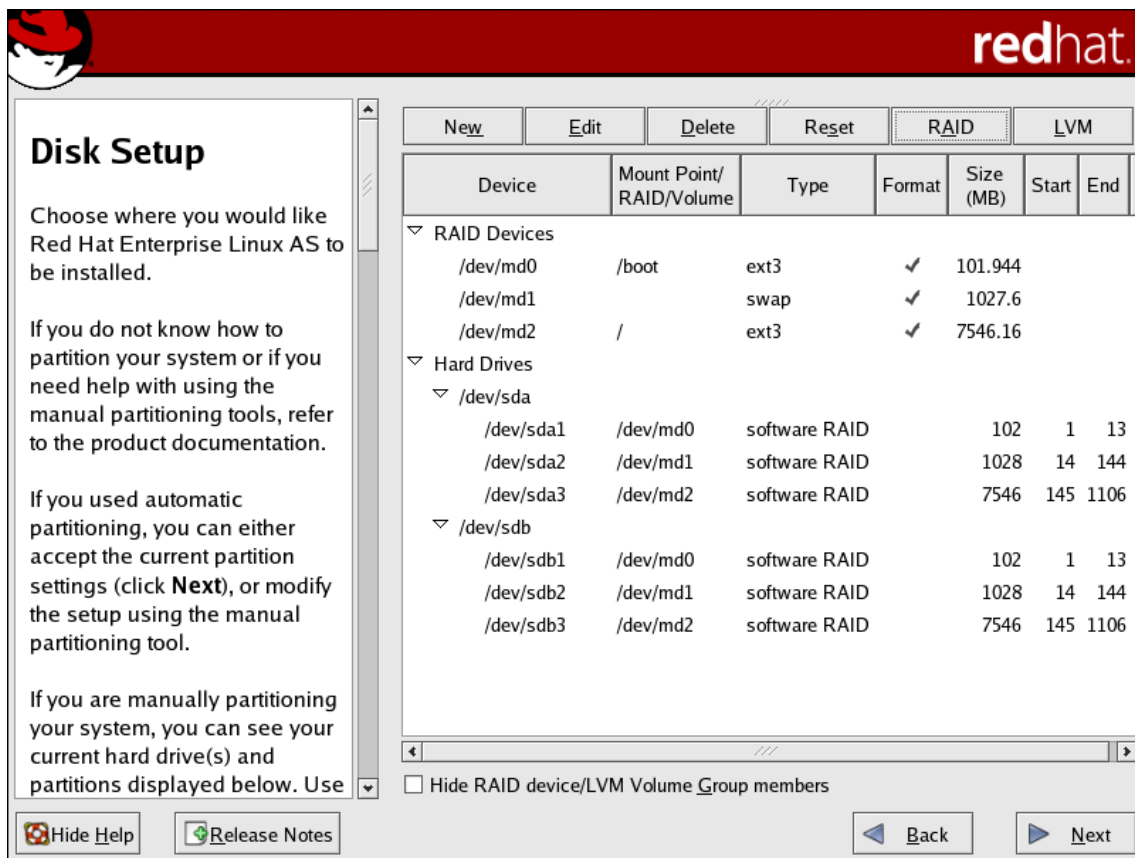
[D]

8. 作成した RAID パーティションが RAID メンバー の一覧に表示されます。RAID デバイスの作成に使用するパーティションを選択します。
9. RAID 1 または RAID 5 を設定する場合は、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、スペアは代替として自動的に使用されます。指定する各ペアについて、(RAID デバイスのパーティションに加えて) 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と、予備のパーティションを選択します。
10. OK をクリックすると、RAID デバイスがドライブの 概要一覧に表示 されます。
11. この章では、`root` パーティション(/)、`/home/`、`swap` など、追加のパーティション、デバイス、マウントポイントを設定するプロセス全体を繰り返します。

設定全体が終わると、[図10.8 「RAID 設定のサンプル」](#) に示される図は、RAID の使用を除きデフォルト設定のようになります。



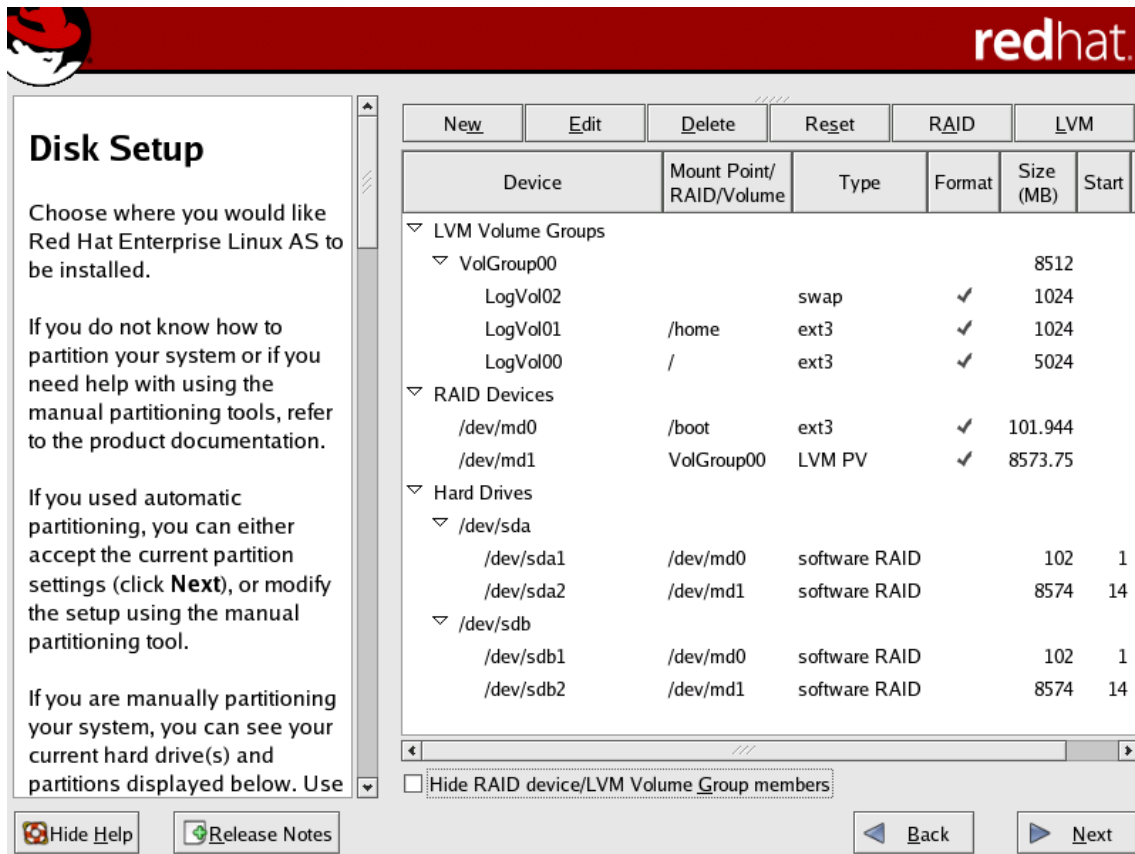
図10.8 RAID 設定のサンプル



[D]

図10.9 「LVM 設定を使用した RAID の最終的なサンプル」 に示されている図は、RAID および LVM の設定例です。

図10.9 LVM 設定を使用した RAID の最終的なサンプル



[D]

インストールプロセスを続行できます。その他の手順については、『『インストールガイド』』を参照してください。

## 第11章 SWAP 領域

### 11.1. 変動スペースとは

Linux の **スワップ領域** は、物理メモリー (RAM) が不足すると使用されます。システムに多くのメモリーリソースが必要で、RAM が不足すると、メモリーの非アクティブなページがスワップ領域に移動します。スワップ領域は、RAM が少ないマシンで役に立ちますが、RAM の代わりに使用しないようにしてください。スワップ領域はハードドライブにあり、そのアクセス速度は物理メモリーに比べると遅くなります。

スワップ領域の構成は、専用のスワップパーティション (推奨)、スワップファイル、またはスワップパーティションとスワップファイルの組み合わせが考えられます。

swap のサイズは、最大 2 GB の物理メモリーに対して、コンピューターの物理メモリーの 2 倍以上である必要があります。物理 RAM が 2 GB を超える場合、スワップのサイズは 2 GB を超える物理メモリーの容量と同じである必要があります。swap のサイズは、32 MB 未満にしないでください。

この基本的な式を使用すると、2 GB の物理メモリーを持つシステムには 4 GB の swap が設定されます。また、3 GB の物理メモリーを持つシステムの swap は 5 GB です。



#### 備考

ただし、Red Hat Enterprise Linux に割り当てるスワップ量を決定することは、人数よりも多くあるため、ハードルールはできません。スワップサイズを決定するときは、各システムの最も使用されているアプリケーションを考慮する必要があります。



#### 重要な影響

スワップ領域として割り当てたファイルシステムおよび LVM2 ボリュームは、変更時に使用できません。たとえば、システムプロセスに swap 領域が割り当てられず、カーネルにより割り当てて使用するスワップはできません。free コマンドおよび cat /proc/swaps コマンドを使用して、スワップの使用量と、使用中の場所を確認します。

スワップ領域の変更を実現する最適な方法は、システムをレスキューモードで起動してから、本章の残りの手順 (各シナリオ用) に従うことです。レスキューモードで起動する方法は、[5章 基本的なシステムの復元](#) を参照してください。ファイルシステムをマウントするように指示されたら、スキップを選択します。

### 11.2. スワップ領域の追加

場合によっては、インストールした後にさらに swap 領域の追加が必要になることもあります。たとえば、システムの RAM 容量を 128 MB から 256 MB にアップグレードできますが、swap 領域は 256 MB のみになります。メモリーを大幅に消費する操作を実行している場合や、大量のメモリーを必要とするアプリケーションを実行する場合には、スワップ領域を 512 MB に増やすと有益となる可能性があります。

選択肢が3つあります: 新規の swap パーティションの作成、新規の swap ファイルの作成、あるいは既存の LVM2 論理ボリューム上で swap の拡張。この中では、既存論理ボリュームを拡張することが推奨されます。

### 11.2.1. LVM2 論理ボリュームでのスワップ領域の拡張

LVM2 スワップ論理ボリュームを拡張するには ( /dev/VolGroup00/LogVol01 が拡張するボリュームと想定します)。

1. 関連付けられている論理ボリュームのスワップ機能を無効にします。

```
# swapoff -v /dev/VolGroup00/LogVol01
```

2. LVM2 論理ボリュームのサイズを 256 MB に変更します。

```
# lvm lvresize /dev/VolGroup00/LogVol01 -L +256M
```

3. 新しいスワップ領域をフォーマットします。

```
# mkswap /dev/VolGroup00/LogVol01
```

4. 拡張論理ボリュームを有効にします。

```
# swapon -va
```

5. 論理ボリュームが適切に拡張されていることを確認します。

```
# cat /proc/swaps # free
```

### 11.2.2. スワップの LVM2 論理ボリュームの作成

スワップボリュームグループを追加するには (/dev/VolGroup00/LogVol02 が追加するスワップボリュームであると想定)、以下を実行します。

1. サイズが 256 MB の LVM2 論理ボリュームを作成します。

```
# lvm lvcreate VolGroup00 -n LogVol02 -L 256M
```

2. 新しいスワップ領域をフォーマットします。

```
# mkswap /dev/VolGroup00/LogVol02
```

3. 次のエントリを /etc/fstab ファイルに追加します。

```
/dev/VolGroup00/LogVol02 swap swap defaults 0 0
```

4. 拡張論理ボリュームを有効にします。

```
# swapon -va
```

5. 論理ボリュームが適切に拡張されていることを確認します。

```
# cat /proc/swaps # free
```

### 11.2.3. スワップファイルの作成

swap ファイルを追加します。

1. 新しいスワップファイルのサイズをメガバイト単位で指定してから、そのサイズに 1024 をかけてブロック数を指定します。たとえばスワップファイルのサイズが 64 MB の場合は、ブロック数が 65536 になります。
2. root としてシェルプロンプトで、必要なブロックサイズと同じ カウント を持つ以下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セットアップします。

```
mkswap /swapfile
```

4.

スワップファイルを起動時に自動的にではなく、すぐに有効にする場合は、以下を実行します。

```
swapon /swapfile
```

5.

起動時に有効にするには、`/etc/fstab` を編集して以下のエントリーを含めます。

```
/swapfile      swap          swap defaults    0 0
```

次にシステムが起動すると、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ら、`cat /proc/swaps` または `free` のコマンドの出力を表示してこれが有効であることを確認します。

### 11.3. スワップ領域の削除

インストールの後に `swap` 領域を減らすことが賢明な場合もあります。たとえば、システムの RAM 容量を 1 GB から 512 MB にダウングレードするとします。しかし、依然として 2 GB のスワップスペースが割り当てられています。ディスク領域が大きくなる (2 GB など) と無駄になる可能性があるため、スワップ領域を 1 GB に減らすことでメリットを得られることがあります。

ここでも選択肢が 3 つあります: `swap` 用に使用していた LVM2 論理ボリューム全体を削除、`swap` ファイルの削除、あるいは既存の LVM2 論理ボリューム上の `swap` 領域の低減。

#### 11.3.1. LVM2 論理ボリュームでのスワップ領域の縮小

LVM2 スワップ論理ボリュームを減らします (`/dev/VolGroup00/LogVol01` が拡張するボリュームを想定)。

1.

関連付けられている論理ボリュームのスワップ機能を無効にします。

```
# swapoff -v /dev/VolGroup00/LogVol01
```

2. LVM2 論理ボリュームのサイズを変更して 512 MB 削減します。

```
# lvm lvreduce /dev/VolGroup00/LogVol01 -L -512M
```

3. 新しいスワップ領域をフォーマットします。

```
# mkswap /dev/VolGroup00/LogVol01
```

4. 拡張論理ボリュームを有効にします。

```
# swapon -va
```

5. 論理ボリュームが適切に縮小されたことをテストします。

```
# cat /proc/swaps # free
```

### 11.3.2. スワップの LVM2 論理ボリュームの削除

swap 論理ボリュームは使用できません（ボリュームのシステムロックやプロセスはありません）。最も簡単にこれを実現する方法は、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は、[5章 基本的なシステムの復元](#) を参照してください。ファイルシステムをマウントするように指示されたら、スキップを選択します。

swap ボリュームグループを削除します (/dev/VolGroup00/LogVol02 が削除するボリュームであるとして)。

1. 関連付けられている論理ボリュームのスワップ機能を無効にします。

```
# swapoff -v /dev/VolGroup00/LogVol02
```

2. サイズ 512MB の LVM2 論理ボリュームを削除します。

```
# lvm lvremove /dev/VolGroup00/LogVol02
```

3. /etc/fstab ファイルから次のエントリを削除します。

```
| /dev/VolGroup00/LogVol02 swap swap defaults 0 0
```

4. 論理ボリュームが適切に拡張されていることを確認します。

```
| # cat /proc/swaps # free
```

### 11.3.3. スワップファイルの削除

swap ファイルを削除します。

1. root としてシェルプロンプトで以下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（/swapfile はスワップファイル）。

```
| # swapoff -v /swapfile
```

2. /etc/fstab ファイルから該当するエントリーを削除します。

3. 実際のファイルを削除します。

```
| # rm /swapfile
```

### 11.4. SWAP 領域の移動

スワップスペースをある場所から別の場所に移動するには、スワップスペースを削除する手順を実行してから、スワップスペースを追加する手順を実行します。



## 第12章 ディスクストレージの管理

さまざまなメソッドの概要...

## 12.1. PARTEDで標準パーティション

多くのユーザーは、既存のパーティションテーブルの表示、パーティションのサイズの変更、パーティションの削除、空き領域からのパーティションの追加、またはハードドライブの追加が必要になります。ユーティリティー `parted` を使用すると、ユーザーはこれらのタスクを実行することができます。本章では、`parted` を使用してファイルシステムタスクを実行する方法を説明します。

システムのディスク領域の使用状況を表示したり、ディスク領域の使用量を監視する場合は、「[ファイルシステム](#)」を参照してください。

`parted` ユティリティーを使用するには、`parted` パッケージがインストールされている。`parted` を起動するには、`root` としてシェルプロンプトで `parted /dev/sda` コマンドを入力します。`/dev/sda` は、設定する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。利用可能なコマンドの一覧を表示するには、`help` と入力します。

パーティションを作成、削除、またはサイズ変更する場合は、デバイスを使用できなくなります (パーティションをマウントできず、`swap` 領域を有効化できません)。カーネルが変更を適切に認識しないため、パーティションテーブルは使用中の間変更しないでください。データは、パーティションテーブルとマウントされたパーティションが一致しないため、誤ったパーティションに書き込むことで上書きされる可能性があります。最も簡単にこれを実現する方法は、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は、[5章 基本的なシステムの復元](#) を参照してください。ファイルシステムをマウントするように指示されたら、`スキップ` を選択します。

または、ドライブに使用中のパーティション (ファイルシステムがアンマウントされないように使用またはロックしているシステムプロセス) がない場合、`umount` コマンドでパーティションをアンマウントし、`swapoff` コマンドで、ハードドライブのすべてのスワップ領域を無効にできます。

[表12.1 「parted コマンド」](#) 一般的に使用される `parted` コマンドの一覧が含まれています。以下のセクションでは、その一部について詳細に説明します。

表12.1 `parted` コマンド

コマンド	説明
<code>check minor-num</code>	ファイルシステムの簡単なチェックを実行します。

コマンド	説明
<b>cp <i>from to</i></b>	ファイルシステムをあるパーティションから別のパーティションにコピーします。 <i>from</i> と <i>to</i> はパーティションのマイナー番号です。
<b>help</b>	利用可能なコマンドの一覧を表示します。
<b>mklabel <i>label</i></b>	パーティションテーブル用のディスクラベルを作成します。
<b>mkfs <i>minor-num file-system-type</i></b>	タイプ <i>file-system-type</i> のファイルシステムを作成します。
<b>mkpart <i>part-type fs-type start-mb end-mb</i></b>	新しいファイルシステムを作成せずに、パーティションを作成します。
<b>mkpartfs <i>part-type fs-type start-mb end-mb</i></b>	パーティションを作成し、指定されたファイルシステムを作成します。
<b>move <i>minor-num start-mb end-mb</i></b>	パーティションを移動します。
<b>name <i>minor-num name</i></b>	Mac と PC98 のディスクラベル用のみのパーティションに名前を付けます。
<b>print</b>	パーティションテーブルを表示します。
<b>quit</b>	<b>parted</b> を終了します。
<b>rescue <i>start-mb end-mb</i></b>	<i>start-mb</i> から <i>end-mb</i> へ、消失したパーティションを復旧します。
<b>resize <i>minor-num start-mb end-mb</i></b>	パーティションのサイズを <i>start-mb</i> から <i>end-mb</i> に変更します。
<b>rm <i>minor-num</i></b>	パーティションを削除します。
<b>select <i>device</i></b>	設定する別のデバイスを選択します。
<b>set <i>minor-num flag state</i></b>	パーティションにフラグを設定します。 <i>state</i> はオンまたはオフのいずれかになります。

### 12.1.1. パーティションテーブルの表示

`parted` を起動したら、以下のコマンドを入力してパーティションテーブルを表示します。

```
print
```

以下のようなテーブルが表示されます。

```
Disk geometry for /dev/sda: 0.000-8678.789 megabytes
```

```
Disk label type: msdos
```

Minor	Start	End	Type	Filesystem	Flags
1	0.031	101.975	primary	ext3	boot
2	101.975	5098.754	primary	ext3	
3	5098.755	6361.677	primary	linux-swap	
4	6361.677	8675.727	extended		
5	6361.708	7357.895	logical	ext3	

```
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	

最初の行はディスクのサイズを表示し、2番目の行にはディスクラベルのタイプが表示され、残りの出力にはパーティションテーブルが表示されます。

パーティションテーブルでは、最小番号がパーティション番号になります。たとえば、マイナー番号1のパーティションは、`/dev/sda1`に対応します。StartおよびEndの値はメガバイト単位です。Typeはprimary、extended、またはlogicalのいずれかです。Filesystemはファイルシステムタイプで、ext2、ext3、fat16、fat32、hfs、jfs、linux-swap、ntfs、reiserfs、hp-ufs、sun-ufs、またはxfsのいずれかです。Flagsは、パーティションに設定したフラグを一覧表示しています。利用可能なフラグは、boot、root、swap、hidden、raid、lvm、またはlbaです。

この例では、マイナー番号1は/boot/ファイルシステムを指し、マイナー番号2はrootファイルシステム(/)を指し、マイナー番号3はスワップを参照し、マイナー番号5は/home/ファイルシステムを指します。



## 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** コマンドで、**/dev/sda** などのデバイス名を指定します。次に、パーティションテーブルを表示したり、設定できます。

### 12.1.2. パーティションの作成



#### 警告

使用中のデバイスに、パーティションを作成しないようにしてください。

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 (または、デバイス上のパーティションをアンマウントして、デバイス上の **swap** 領域をすべてオフにします)。

**parted** を起動します。 **/dev/sda** は、パーティションを作成するデバイスです。

```
parted /dev/sda
```

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

```
print
```

十分な空き容量がない場合は、既存のパーティションのサイズを変更できます。詳細は、[「パーティションのサイズ変更」](#) を参照してください。

#### 12.1.2.1. パーティションの作成

パーティションテーブルから、新しいパーティションの開始点と終了点、およびパーティションのタイプを決定します。プライマリーパーティションは、1つのデバイス上に4つまで保有できます (この場合は拡張パーティションは含みません)。パーティションが5つ以上必要な場合は、プライマリーパーティションを3つ、拡張パーティションを1つにし、その拡張パーティションの中に複数の論理パーティションを追加します。ディスクパーティションの概要『は、『『インストールガイド』』の付録「ディスクパーティションの概要」を』参照してください。

たとえば、ハードドライブの 1024 メガバイトから 2048 メガバイトに ext3 ファイルシステムのプライマリパーティションを作成するには、以下のコマンドを入力します。

```
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てからファイルシステムが作成されます。ただし、`parted` では、ext3 ファイルシステムの作成に対応していません。そのため、ext3 ファイルシステムを作成する場合は、`mkpart` を使用して、後述のように `mkfs` コマンドを実行してファイルシステムを作成します。`mkpartfs` は、ファイルシステムタイプ `linux-swap` で動作します。

Enter を押すと変更が反映されるため、押す前に再度確認してください。

パーティションを作成したら、`print` コマンドを使用して、パーティションが正しいパーティションタイプ、ファイルシステムタイプ、およびサイズでパーティションテーブルにあることを確認します。また、ラベル付けできるように、新しいパーティションのマイナー番号も覚えておいてください。以下の出力も表示されるはずですが。

```
cat /proc/partitions
```

カーネルが新しいパーティションを認識していることを確認します。

#### 12.1.2.2. パーティションのフォーマット

パーティションにはまだファイルシステムがありません。ファイルシステムを作成します。

```
/sbin/mkfs -t ext3 /dev/sda6
```



#### WARNING

パーティションをフォーマットすると、そのパーティションに現存するすべてのデータが永久に抹消されます。

### 12.1.2.3. パーティションのラベル付け

次に、パーティションにラベルを指定します。たとえば、新しいパーティションが `/dev/sda6` で、`/work` にラベルを付ける場合は、次のコマンドを実行します。

```
e2label /dev/sda6 /work
```

デフォルトでは、インストールプログラムは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て、ラベルが固有なものとなるようにします。ユーザーは使用するラベルを選択できます。

### 12.1.2.4. マウントポイントの作成

`root` でマウントポイントを作成します。

```
mkdir /work
```

### 12.1.2.5. `/etc/fstab` への追加

`root` で `/etc/fstab` ファイルを編集して、新しいパーティションを追加します。新しい行は以下のようになります。

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

最初の列には、`LABEL=` の後にパーティションを付けたラベルが含まれるはずですが、2 番目の列には、新しいパーティションのマウントポイントが含まれている必要があります。その次の列はファイルシステムタイプ (たとえば、`ext3` または `swap`) である必要があります。フォーマットの詳細が必要な場合は、コマンド `man fstab` を使用して `man` ページを参照してください。

4 列目がデフォルトである場合、パーティションは起動時にマウントされます。再起動せずにパーティションをマウントするには、`root` で次のコマンドを入力します。

```
mount /work
```

### 12.1.3. パーティションの削除

**警告**

パーティションが設定されているデバイスが使用中の場合は、削除しないでください。

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 (または、デバイス上のパーティションをアンマウントして、デバイス上の `swap` 領域をすべてオフにします)。

`parted` を起動します。 `/dev/sda` は、パーティションを削除するデバイスです。

```
parted /dev/sda
```

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確認します。

```
print
```

`rm` コマンドで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のは以下のコマンドです。

```
rm 3
```

変更は `Enter` を押すと変更が反映されるため、押す前にコマンドを再度確認してください。

パーティションを削除したら、`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。以下の出力も表示されるはずです。

```
cat /proc/partitions
```

カーネルがパーティションが削除されていることを確認します。

最後の手順は、`/etc/fstab` ファイルからそれを削除することです。削除したパーティションを宣言している行を見つけ、ファイルから削除します。

#### 12.1.4. パーティションのサイズ変更



##### 警告

パーティションが設定されているデバイスが使用中の場合は、サイズを変更しないでください。

パーティションのサイズを変更する前に、レスキューモードで起動します (または、デバイス上のパーティションをアンマウントして、デバイス上の `swap` 領域をすべてオフにします)。

`parted` を起動します。 `/dev/sda` は、パーティションのサイズを変更するデバイスです。

```
parted /dev/sda
```

現在のパーティションテーブルを表示して、サイズを変更するパーティションのマイナー番号と、パーティションの開始点と終了点を決定します。

```
print
```



##### WARNING

サイズを変更するパーティションに使用される領域は、新しいサイズよりも大きくすることはできません。

パーティションのサイズを変更するには、`resize` コマンドの後に、パーティションのマイナー番号、開始位置 (メガバイト単位)、終了位置 (メガバイト単位) を使用します。以下に例を示します。

```
resize 3 1024 2048
```



パーティションのサイズを変更した後、`print` コマンドを使用して、パーティションのサイズが正しく変更され、正しいパーティションタイプであり、正しいファイルシステムタイプであることを確認します。

システムを通常モードに再起動した後、`df` コマンドを使用して、パーティションがマウントされ、新しいサイズで認識されていることを確認します。

## 12.2. LVM パーティション管理

以下のコマンドを確認するには、コマンドプロンプトで `lvm help` を実行します。

表12.2 lvm コマンド

コマンド	Description
<code>dumpconfig</code>	アクティブな設定をダンプします。
<code>formats</code>	利用可能なメタデータ形式を一覧表示します。
<code>help</code>	ヘルプコマンドの表示
<code>lvchange</code>	論理ボリュームの属性の変更
<code>lvcreate</code>	論理ボリュームを作成します。
<code>lvdisplay</code>	論理ボリュームに関する情報を表示します。
<code>lvextend</code>	論理ボリュームに領域を追加する
<code>lvmchange</code>	デバイスマッパーの使用により、このコマンドは非推奨になっています。
<code>lvmdiskscan</code>	物理ボリュームとして使用できるデバイスを一覧表示します。
<code>lvmsadc</code>	アクティビティーデータの収集
<code>lvmsar</code>	Create activity report
<code>lvreduce</code>	論理ボリュームのサイズ縮小

コマンド	Description
<b>lvremove</b>	システムから論理ボリュームを削除する
<b>lvrename</b>	論理ボリュームの名前変更
<b>lvresize</b>	論理ボリュームのサイズ変更
<b>lvs</b>	論理ボリュームに関する情報を表示する
<b>lvscan</b>	すべてのボリュームグループの論理ボリュームを一覧表示します。
<b>pvchange</b>	物理ボリュームの属性の変更
<b>pvcreate</b>	LVM で使用する物理ボリュームの初期化
<b>pvdata</b>	物理ボリュームのディスク上のメタデータを表示します。
<b>pvdisplay</b>	物理ボリュームの各種属性の表示
<b>pvmove</b>	エクステントをある物理ボリュームから別の物理ボリュームに移動する
<b>pvremove</b>	物理ボリュームから LVM ラベルを削除する
<b>pvresize</b>	ボリュームグループにより使用されている物理ボリュームのサイズ変更
<b>pvs</b>	物理ボリュームに関する情報の表示
<b>pvscan</b>	物理ボリュームの一覧を表示します。
<b>segtypes</b>	利用可能なセグメントタイプの一覧を表示します。
<b>vgcfgbackup</b>	バックアップのボリュームグループの設定
<b>vgcfgrestore</b>	ボリュームグループ設定の復元
<b>vgchange</b>	ボリュームグループ属性の変更

コマンド	Description
vgck	ボリュームグループの一貫性の確認
vgconvert	ボリュームグループのメタデータ形式の変更
vgcreate	ボリュームグループの作成
vgdisplay	ボリュームグループ情報の表示
vgexport	システムからボリュームグループの登録解除
vgextend	ボリュームグループへの物理ボリュームの追加
vgimport	エクスポートしたボリュームグループをシステムに登録します。
vgmerge	ボリュームグループのマージ
vgmknodes	ボリュームグループデバイス用の特殊ファイルを /dev/ に作成します。
vgreduce	ボリュームグループから物理ボリュームの削除
vgremove	ボリュームグループの削除
vgrename	ボリュームグループの名前変更
vgs	ボリュームグループに関する情報を表示します。
vgscan	すべてのボリュームグループの検索
vgsplit	物理ボリュームを新しいボリュームグループに移動
version	ソフトウェアとドライバーのバージョン情報を表示します。

## 第13章 ディスククォータの実装

ディスク領域はディスククォータによって制限できます。ディスククォータは、ユーザーが過度のディスク領域を消費するか、パーティションが満杯になる前にシステム管理者に警告をします。

ディスククォータは、ユーザーグループにも個別のユーザーにも設定できます。このような柔軟性により、各ユーザーに小規模のクォータを指定して（電子メールやレポートなどの）「成り」ファイル（電子メールやレポートなど）を処理し、作業するプロジェクトにより多くのサイジング可能なクォータを持たせることができます（プロジェクトに独自のグループが割り当てられていることを前提とします）。

さらにクォータは、消費されるディスクブロックの数の制御だけでなく、inode (UNIX ファイルシステム内のファイルに関する情報を含むデータ構造) の数も制御するように設定できます。inode はファイル関連の情報を組み込むように使用されるため、これが作成されるファイルの数を制御することも可能にします。

ディスククォータを実装するには、`quota RPM` をインストールしておく必要があります。

### 13.1. ディスククォータの設定

ディスククォータを実装するには、以下の手順を行います。

1. `/etc/fstab` を修正することで、ファイルシステムごとのクォータを有効にします。
2. ファイルシステムを再マウントします。
3. クォータデータベースファイルを作成して、ディスク使用状況テーブルを生成します。
4. クォータポリシーを割り当てます。

この各手順は、以下のセクションで詳しく説明します。

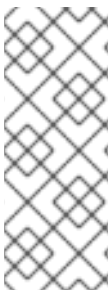
#### 13.1.1. クォータの有効化

`root` として、テキストエディターを使用して、`/etc/fstab` ファイルを編集します。クォータを必要

とするファイルシステムに `usrquota` オプションや `grpquota` オプションを追加します。

```
/dev/VolGroup00/LogVol00 /      ext3 defaults    1 1
LABEL=/boot              /boot ext3 defaults    1 2
none                     /dev/pts devpts gid=5,mode=620 0 0
none                     /dev/shm tmpfs defaults    0 0
none                     /proc  proc  defaults    0 0
none                     /sys   sysfs defaults    0 0
/dev/VolGroup00/LogVol02 /home ext3 defaults,usrquota,grpquota 1 2
/dev/VolGroup00/LogVol01 swap  swap  defaults    0 0
.
.
.
```

この例では、`/home` ファイルシステムがユーザーとグループの両方のクォータを有効にしています。



#### 備考

以下の例では、Red Hat Enterprise Linux のインストール時に別の `/home` パーティションが作成されたことを前提としています。理想的ではありませんが、`root(/)` パーティション（インストールのデフォルト作成されたパーティション）は、`/etc/fstab` ファイルでクォータポリシーを設定するのに使用できます。

### 13.1.2. ファイルシステムの再マウント

`usrquota` オプションや `grpquota` オプションを追加した後、`fstab` エントリーが変更された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どのプロセスでも使用されていない場合は、以下のいずれかの方法を使用します。

- `umount` コマンドを実行してから `mount` コマンドを実行し、ファイルシステムを再マウントします。
- `mount -o remount /home` コマンドを実行して、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の場合、そのファイルシステムを再マウントする最も簡単な方法は、システムを再起動することです。

### 13.1.3. クォータデータベースファイルの作成

クォータが有効な各ファイルシステムを再マウントすると、システムはディスククォータを操作で

きます。ただし、ファイルシステム自体がクォータに対応するには、追加の設定が必要です。次のステップとして、`quotacheck` コマンドを実行します。

`quotacheck` コマンドは、クォータが有効なファイルシステムを検証し、現在のディスク使用状況のテーブルをファイルシステムごとに構築します。このテーブルは、ディスク使用状況のオペレーティングシステム用コピーを更新するのに使用されます。また、ファイルシステムのディスククォータが更新されます。

ファイルシステムにクォータファイル (`aquota.user` および `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。たとえば、`/home` ファイルシステムでユーザーとグループのクォータが有効になっている場合は、`/home` ディレクトリーにファイルを作成します。

```
quotacheck -cug /home
```

`-c` オプションは、クォータが有効になっているファイルシステムごとにクォータファイルを作成することを指定し、`-u` オプションは、ユーザークォータをチェックすることを指定し、`-g` オプションは、グループクォータをチェックすることを指定します。

`-u` オプションまたは `-g` オプションのいずれも指定しない場合は、ユーザークォータファイルのみが作成されます。`-g` のみを指定すると、グループクォータファイルのみが作成されます。

ファイルの作成後、以下のコマンドを実行し、クォータを有効にしたファイルシステムごとの現在のディスク使用量のテーブルを生成します。

```
quotacheck -avug
```

使用されるオプションは次のとおりです。

- **a:** クォータが有効になっているすべてのファイルシステムを確認し、ローカルにマウントされたファイルシステムを確認します。
- **v:** クォータチェックが進む際に詳細なステータス情報を表示します。
- **u:** ユーザーディスククォータ情報の確認

## ● g: グループのディスククォータ情報の確認

quotacheck の実行が終了すると、有効なクォータ (ユーザーやグループ) に対応するクォータファイルに、/home などの、クォータが有効になっているローカルにマウントされた各ファイルシステムのデータが取り込まれます。

### 13.1.4. ユーザーごとのクォータ割り当て

最後の手順は、edquota コマンドを使用したディスククォータ割り当てです。

ユーザーにクォータを設定するには、シェルプロンプトで、root で次のコマンドを実行します。

```
edquota username
```

クォータが必要な各ユーザーに対して、この手順を実行します。たとえば、クォータが /etc/fstab で /home パーティション(/dev/VolGroup00/LogVol02)で有効になり、edquota testuser コマンドを実行すると、システムのデフォルトとして設定されたエディターに以下が表示されます。

```
Disk quotas for user testuser (uid 501):
```

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/VolGroup00/LogVol02	440436	0	0	0	37418	0 0

#### 備考

EDITOR 環境変数により定義されたテキストエディターは、edquota により使用されます。エディターを変更するには、~/.bash\_profile ファイルの EDITOR 環境変数を、使用するエディターのフルパスに設定します。

最初の列は、クォータが有効になっているファイルシステムの名前です。2 列目には、ユーザーが現在使用しているブロック数が示されます。その次の 2 列は、ファイルシステム上のユーザーのソフトブロック制限およびハードブロック制限を設定するのに使用されます。inodes 列は、ユーザーが現在使用している inode の数を示します。最後の 2 列は、ファイルシステムのユーザーに対するソフトおよびハードの inode 制限を設定するのに使用されます。

ハード制限は、ユーザーまたはグループが使用できる最大ディスク容量 (絶対量) です。この制限に達すると、それ以上のディスク領域は使用できなくなります。

ソフト制限は、使用可能な最大ディスク容量を定義します。ただし、ハード制限とは異なり、ソフト制限は一定時間超過する可能性があります。この時間は *猶予期間* として知られています。猶予期間の単位は、秒、分、時間、日、週、または月で表されます。

いずれかの値が 0 に設定されていると、その制限は設定されません。テキストエディターで必要な制限に変更します。以下に例を示します。

```
Disk quotas for user testuser (uid 501):
```

```
Filesystem      blocks  soft  hard inodes soft  hard
/dev/VolGroup00/LogVol02 440436 500000 550000 550000 37418 0 0
```

ユーザーのクォータが設定されていることを確認するには、以下のコマンドを使用します。

```
quota testuser
```

### 13.1.5. グループごとのクォータ割り当て

クォータは、グループごとに割り当てることもできます。たとえば、`devel` グループのグループクォータを設定するには（グループはグループクォータを設定する前に存在している必要があります）、以下のコマンドを使用します。

```
edquota -g devel
```

このコマンドにより、グループの既存クォータがテキストエディターに表示されます。

```
Disk quotas for group devel (gid 505):
```

```
Filesystem      blocks  soft  hard inodes soft  hard
/dev/VolGroup00/LogVol02 440400 0 0 0 37418 0 0
```

制限を変更し、ファイルを保存してからクォータを設定します。

グループクォータが設定されたことを確認するには、次のコマンドを使用します。

```
quota -g devel
```

### 13.1.6. ファイルシステムごとのクォータの割り当て

クォータに有効な各ファイルシステムに基づいてクォータを割り当てるには、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、これにより、テキストエディターでファイルシステムの現在のクォータが開きます。

```
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/mapper/VolGroup00-LogVol02  7days              7days
```

ブロックの猶予期間または inode の猶予期間を変更し、変更をファイルに保存してテキストエディターを終了します。

## 13.2. ディスククォータの管理

クォータが実装されている場合には、若干の保守が必要となります。大半は、クォータの超過監視および精度確認という形となります。当然ながら、ユーザーが繰り返しクォータを超過したり、常にソフト制限に到達すると、システム管理者には、ユーザーのタイプや作業に影響を与えるディスク領域のサイズに応じていくつかの選択肢があります。管理者は、ユーザーがディスク容量を少なくなるか、または必要に応じてユーザーのディスククォータを増やす方法を判別するのに役立ちます。

### 13.2.1. 有効化と無効化

クォータは、0 に設定しなくても無効にできます。すべてのユーザーとグループのクォータをオフにするには、以下のコマンドを使用します。

```
quotaoff -vaug
```

`-u` オプションまたは `-g` オプションのいずれも指定しない場合は、ユーザークォータのみが無効になります。`-g` のみを指定すると、グループクォータのみが無効になります。

クォータを再度有効にするには、同じオプションを指定して `quotaon` コマンドを使用します。

たとえば、すべてのファイルシステムに対してユーザーとグループのクォータを有効にするには、次のコマンドを使用します。

```
quotaon -vaug
```

/home などの特定のファイルシステムにクォータを有効にするには、以下のコマンドを使用します。

```
quotaon -vug /home
```

-u オプションまたは -g オプションのいずれも指定しない場合は、ユーザクォータのみが有効になります。-g のみが指定されている場合は、グループのクォータのみが有効になります。

### 13.2.2. ディスククォータに関するレポート

ディスク使用状況のレポートを作成するには、repquota ユーティリティーの実行が必要になります。たとえば、コマンド repquota /home により、以下のような出力が表示されます。

```
*** Report for user quotas on device /dev/mapper/VolGroup00-LogVol02
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
kristin --  540   0   0       125   0   0
testuser -- 440400 500000 550000   37418   0   0
```

クォータが有効なすべてのファイルシステム (オプション -a) のディスク使用状況レポートを表示するには、次のコマンドを使用します。

```
repquota -a
```

レポートは読みやすいですが、いくつか説明しておくべき点があります。各ユーザーの後に表示される--を利用すると、ブロック制限または inode 制限を超えたかどうかをすばやく判断できます。いずれかのソフト制限を超えると、対応する - の代わりに + が表示されます。最初の - はブロックの制限を表し、2 つ目は inode の制限を表します。

grace 列は通常空白です。ソフト制限が超過した場合、その列には猶予期間に残り時間量に相当する時間指定が含まれます。猶予期間が過ぎると、代わりに none が表示されます。

### 13.2.3. クォータの精度維持

(システムクラッシュなどにより) ファイルシステムのマウントが正しく解除されない場合は、quotacheck を実行する必要があります。ただし、システムがクラッシュしていないとしても、quotacheck は定期的に行うことができます。以下のコマンドを定期的に行うと、クォータがより正確になります (使用するオプションは「クォータの有効化」で説明されています)。

## quotacheck -avug

これを定期的に行う最も簡単な方法は、`cron` を使用することです。`root` で `crontab -e` コマンドを使用して定期的なクォータチェックをスケジュールするか、以下のディレクトリーのいずれかで `quotacheck` を実行するスクリプトを配置します（任意に最も適した間隔を使用します）。

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

ファイルシステムがアクティブで使用されていない場合は、最も正確なクォータ統計を取得できません。そのため、ファイルシステムが最も少ない時間に `cron` タスクをスケジュールする必要があります。この時間がクォータを含む異なるファイルシステムで異なる場合は、複数の `cron` タスクを指定して、各ファイルシステムのクォータチェックを異なるタイミングで実行します。

`cron` の設定に関する詳細は、[34章 自動タスク](#) を参照してください。

### 13.3. 関連情報

ディスククォータの詳細は、以下のリソースを参照してください。

#### 13.3.1. インストールされているドキュメント

- `quotacheck`、`edquota`、`repquota`、`quota`、`quotaon`、および `quotaoff` の man ページ

#### 13.3.2. 関連書籍

- システム 『管理の概要』 : Red Hat, Inc - <http://www.redhat.com/docs/> およびドキュメント CD で利用可能です。このマニュアルには、新しい Red Hat Enterprise Linux システム管理者向けのストレージ管理（ディスククォータを含む）に関する背景情報が記載されています。

## 第14章 アクセス制御リスト

ファイルとディレクトリーには、ファイルの所有者、そのファイルに関連したグループ、およびシステムを使用する他のすべてのユーザーの権限セットが設定されます。しかし、これらの権限には制限があります。たとえば、ユーザーごとに異なる権限を設定することはできません。そのため **アクセス制御リスト (ACL)** が実装されています。

Red Hat Enterprise Linux 4 カーネルは、**ext3** ファイルシステムと **NFS** エクスポートのファイルシステムに対する **ACL** サポートを提供します。**ACL** は、**Samba** 経由でアクセスする **ext3** ファイルシステムでも認識されます。

**ACL** の実装には、カーネルでのサポートと **acl** パッケージが必要になります。このパッケージには、**ACL** 情報の追加、修正、削除および、取得のためのユーティリティーが同梱されています。

**cp** コマンドと **mv** コマンドは、ファイルとディレクトリーに関連するすべての **ACL** のコピーまたは移動を実行します。

### 14.1. ファイルシステムのマウント

ファイルやディレクトリー用に **ACL** を使用する前に、そのファイルまたはディレクトリーのパーティションを **ACL** サポートでマウントする必要があります。ローカルの **ext3** ファイルシステムの場合は、以下のコマンドでマウントできます。

```
mount -t ext3 -o acl <device-name><partition>
```

以下に例を示します。

```
mount -t ext3 -o acl /dev/VolGroup00/LogVol02 /work
```

パーティションが **/etc/fstab** ファイルにリストされている場合は、パーティションのエントリーに **acl** オプションを含めることができます。

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

**Samba** 経由で **ext3** ファイルシステムにアクセスし、そのアクセスに対して **ACL** が有効になっている場合は、**ACL** が認識されます。これは、**--with-acl-support** オプションでコンパイルされているためです。**Samba** 共有のアクセス時またはマウント時に特別なフラグは必要ありません。

### 14.1.1. NFS

デフォルトでは、NFS サーバーでエクスポートされているファイルシステムが ACL をサポートし、NFS クライアントが ACL を読み込める場合は、クライアントシステムで ACL が使用されています。

サーバーを設定する際に NFS 共有上の ACL を無効にするには、`/etc/exports` ファイルに `no_acl` オプションを追加します。クライアントに NFS 共有をマウントする際に ACL を無効にするには、コマンドラインまたは `/etc/fstab` ファイルに `no_acl` オプションを指定してマウントします。

## 14.2. アクセス ACL の設定

ACL には、アクセス ACL と デフォルト ACL と 2つのタイプがあります。アクセス ACL は、特定のファイルまたはディレクトリーに対するアクセス制御リストです。デフォルト ACL は、ディレクトリーにのみ適用されます。ディレクトリー内のファイルにアクセス ACL が設定されていない場合は、そのディレクトリーにデフォルト ACL のルールが適用されます。デフォルト ACL は任意です。

ACL は以下のように設定できます。

1. 各ユーザー
2. 各グループ
3. 実効権マスクを使用して
4. ファイルのユーザーグループに属さないユーザーに対して

`setfacl` ユーティリティーは、ファイルとディレクトリー用の ACL を設定します。-m オプションを使用して、ファイルまたはディレクトリーの ACL を追加または変更します。

```
setfacl -m <rules><files>
```

ルール(<rules>)は、以下の形式で指定する必要があります。複数のルールをコンマで区切って同じコマンドに指定することもできます。

**U:** <uid>: &lt;perms>

ユーザーにアクセス ACL を設定します。ユーザー名または UID を指定できます。システムで有効な任意のユーザーを指定できます。

`g:<gid>:<perms>`

グループにアクセス ACL を設定します。グループ名または GID を指定できます。システムで有効な任意のグループを指定できます。

`m:<perms>`

実効権マスクを設定します。このマスクは、所有グループの全権限と、ユーザーおよびグループの全エントリーを結合したものです。

`o:<perms>`

ファイルのグループに属さないユーザーにアクセス ACL を設定します。

空白は無視されます。パーミッション(<perms>)は、読み取り、書き込み、および実行を表す r、w、および x の文字の組み合わせである必要があります。

ファイルまたはディレクトリーにすでに ACL が設定されている状態で、setfacl コマンドを使用した場合は、設定するルールが既存の ACL に追加されるか、既存のルールが修正されます。

たとえば、ユーザー「andrius」に読み取りと書き込みの権限を付与するには以下を実行します。

```
setfacl -m u:andrius:rw /project/somefile
```

ユーザー、グループ、またはその他のユーザーからすべての権限を削除するには、-x オプションにいずれの権限も指定せずに指定します。

```
setfacl -x <rules><files>
```

たとえば、UID 500 のユーザーからすべての権限を削除するには以下を実行します。

■

```
setfacl -x u:500 /project/somefile
```

### 14.3. デフォルト ACL の設定

デフォルトの ACL を設定するには、**d:** をルールの前に追加してから、ファイル名ではなくディレクトリーを指定します。

たとえば、`/share/` ディレクトリーにデフォルト ACL を設定し、ユーザーグループに属さないユーザーの読み取りと実行を設定するには、以下のコマンドを実行します (これにより、個別ファイルのアクセス ACL が上書きされます)。

```
setfacl -m d:o:rx /share
```

### 14.4. ACL の取り込み

ファイルまたはディレクトリーに設定されている ACL を確認するには、`getfacl` コマンドを使用します。

```
getfacl <filename>
```

以下のような出力を返します。

```
# file: file
# owner: andrius
# group: andrius
user::rw-
user:smoore:r--
group::r--
mask::r--
other::r--
```

ディレクトリーが指定され、デフォルトの ACL がある場合は、以下のようにデフォルトの ACL も表示されます。

```
# file: file
# owner: andrius
# group: andrius
user::rw-
user:smoore:r--
group::r--
mask::r--
other::r--
default:user::rwx
default:user:andrius:rwx
```

```
default:group::r-x
default:mask::rwx
default:other::r-x
```

#### 14.5. ACL が設定されているファイルシステムのアーカイブ作成



#### WARNING

tar コマンドおよび dump コマンドは ACL をバックアップしません。

star ユーティリティーは、ファイルのアーカイブ生成に使用される点で tar ユーティリティーと似ています。しかし、一部のオプションは異なります。より一般的に使用されるオプションの一覧は、[表 14.1 「star のコマンドラインオプション」](#) を参照してください。利用可能なすべてのオプションは star の man ページを参照してください。このユーティリティーを使用するには star パッケージが必要になります。

表14.1 star のコマンドラインオプション

オプション	説明
-c	アーカイブファイルを作成します。
-n	ファイルを抽出しません。-x と併用すると、ファイルが行う抽出を表示します。
-r	アーカイブ内のファイルを入れ替えます。パスとファイル名が同じファイルが置き換えられ、アーカイブファイルの末尾に書き込まれます。
-t	アーカイブファイルのコンテンツを表示します。
-u	アーカイブファイルを更新します。アーカイブにファイルが存在しない場合や、アーカイブ内の同じ名前のファイルよりも新しい場合は、そのファイルがアーカイブの末尾に書き込まれます。このオプションは、アーカイブがファイルであるか、またはバックスペース可能な非ブロックテープの場合にのみ機能します。



オプション	説明
-x	アーカイブからファイルを抽出します。-U と併用すると、アーカイブ内のファイルがファイルシステムにあるファイルよりも古い場合、そのファイルは抽出されません。
-help	最も重要なオプションを表示します。
-xhelp	最も重要ではないオプションを表示します。
-/	アーカイブからファイルを抽出する際に、ファイル名から先頭のスラッシュを削除します。デフォルトでは、ファイルの抽出時にストライプ化されます。
-acl	作成時または抽出時に、ファイルおよびディレクトリーに関連付けられた ACL をアーカイブまたは復元します。

#### 14.6. 旧システムとの互換性

指定したファイルシステムのいずれかのファイルに ACL が設定されている場合、そのファイルシステムには `ext_attr` 属性があります。この属性は、以下のコマンドを使用すると確認できます。

```
tune2fs -l <filesystem-device>
```

`ext_attr` 属性を持つファイルシステムは古いカーネルでマウントできますが、それらのカーネルは設定されている ACL を強制しません。

バージョン 1.22 以降の `e2fsprogs` パッケージ (Red Hat Enterprise Linux 2.1 および 4 のバージョンも含む) に含まれている `e2fsck` ユーティリティのバージョンは、`ext_attr` 属性を使用してファイルシステムを確認できます。古いバージョンではこの確認が拒否されます。

#### 14.7. 関連情報

詳細は、以下のリソースを参照してください。

##### 14.7.1. インストールされているドキュメント

- [ACL man ページ](#) : ACL の説明

- **man ページ - ファイルアクセス制御リストの取得方法**
- **man ページ - ファイルアクセス制御リストの設定方法**
- **star man ページ : star ユーティリティーとそのオプションの詳細**

#### 14.7.2. 便利な Web サイト

- **<http://acl.bestbits.at/> — Website for ACLs**

---

## パート III. パッケージ管理

**Red Hat Enterprise Linux** システムのすべてのソフトウェアは、**RPM** パッケージに分類されます。このパッケージは、インストール、アップグレード、または削除が可能です。ここでは、グラフィカルおよびコマンドラインツールを使用して、**Red Hat Enterprise Linux** システムで **RPM** パッケージを管理する方法を説明します。

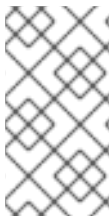
## 第15章 RPM でのパッケージ管理

RPM Package Manager(RPM)は、誰でも使用できるオープンパッケージシステムであり、Red Hat Enterprise Linux や他の Linux システムや UNIX システムで実行できます。Red Hat, Inc は、他のベンダーが独自の製品に RPM を使用することを推奨しています。RPM は、GPL の用語で配布可能です。

RPM を使用すると、エンドユーザーはシステムの更新を簡素化します。RPM パッケージのインストール、アンインストール、およびアップグレードは、短いコマンドで実行できます。RPM はインストールされたパッケージとそのファイルのデータベースを維持するため、システムで強力なクエリーと検証を呼び出すことができます。グラフィカルインターフェースを使用する場合は、Package Management Tool を使用して多くの RPM コマンドを実行できます。

アップグレード中、RPM は設定ファイルを誤って処理するため、カスタマイズを失うことはありません。通常の .tar.gz ファイルで実行できません。

開発者は、RPM を使用して、ソフトウェアソースコードを取り、エンドユーザー向けのソースパッケージとバイナリーパッケージにパッケージ化できます。このプロセスは非常にシンプルで、単一のファイルと作成するオプションのパッチから実行されます。ビルド命令とともに、元のソースとパッチの区別が明確になり、新しいバージョンのソフトウェアがリリースされると、パッケージのメンテナンスが容易になります。



### 備考

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、またはアップグレードを行う root でなければなりません。

### 15.1. RPM 設計ゴール

RPM の使用方法を理解するには、RPM の設計目標を理解すると便利です。

#### アップグレード可能性

RPM を使用すると、完全に再インストールせずにシステムの個々のコンポーネントをアップグレードできます。RPM (Red Hat Enterprise Linux など) をベースとしたオペレーティングシステムの新しいリリースを取得する場合は、マシンに再インストールする必要はありません (他のパッケージシステムに基づいたオペレーティングシステムと同様)。RPM は、システムのインテリジェントな完全自動インプレースアップグレードを可能にします。パッケージの設定ファイルはアップグレード後も保持されるため、カスタマイズは失われません。パッケージのアップグレードに必要な特別なアップグレードファイルはありません。システムのパッケージのインストールとアップグレードに同じ RPM ファイルが使用されるためです。

## 強力なクエリ

RPM は、強力なクエリーオプションを提供するように設計されています。パッケージや特定のファイルのみをデータベース全体で検索できます。また、ファイルが属するパッケージや、パッケージの出所を簡単に見つけることもできます。RPM パッケージに含まれるファイルは圧縮アーカイブにあり、カスタムバイナリーヘッダーにはパッケージとそのコンテンツに関する有用な情報が含まれており、個々のパッケージを素早く簡単にクエリーできます。

## システムの検証

別の強力な機能は、パッケージを検証する機能です。一部のパッケージで重要なファイルを削除した場合には、パッケージを検証します。異常が通知されます。この時点で、必要に応じてパッケージを再インストールできます。変更した設定ファイルは再インストール時に保持されます。

## 純粋なソース

重要な設計目的は、ソフトウェアの元の作成者によって配布される「元の」ソフトウェアソースを使用できるようにしたことでした。RPM では、元のソースと、使用されたパッチ、完全なビルド命令があります。これは、いくつかの理由で重要な利点です。たとえば、新しいバージョンのプログラムが除外している場合には、コンパイルを行うために必ずしもゼロから開始する必要はありません。パッチを確認して、必要な内容を確認できます。コンパイルされたすべてのデフォルトと、ソフトウェアが適切にビルドできるように加えられたすべての変更は、この手法を使用して簡単に表示できます。

ソースを純粋に保つことの目的は開発者にとってのみ重要だと思われませんが、エンドユーザーにとっても品質の高いソフトウェアになります。

## 15.2. RPM の使用

RPM には基本的な動作モードが 5 つあります（パッケージの構築をカウントしません）：インストール、アンインストール、アップグレード、クエリー、および検証を行います。このセクションでは、各モードの概要について説明します。完全な詳細情報およびオプションについては、`rpm --help` を試行するか、RPM に関する詳細情報は「[関連情報](#)」を参照してください。

### 15.2.1. RPM パッケージの検索

RPM を使用する前に、その RPM を見つける場所を知っている必要があります。インターネット検索は多くの RPM リポジトリを返しますが、Red Hat, Inc が構築した RPM パッケージを探す場合は、以下の場所にあります。

- **The Red Hat Enterprise Linux CD-ROMs**
- <http://www.redhat.com/apps/support/errata/>から入手できる Red Hat エラーページ
- <http://www.redhat.com/download/mirror.html>で利用可能な Red Hat FTP ミラーサイト
- **Red Hat Network: Red Hat Network** に関する詳細情報は、[16章 Red Hat Network](#) を参照してください。

### 15.2.2. インストール

RPM パッケージには、通常 `foo-1.0-1.i386.rpm` などのファイル名があります。ファイル名には、パッケージ名(`foo`)、バージョン(`1.0`)、リリース(`1`)、アーキテクチャー(`i386`)が含まれます。パッケージをインストールするには、`root` としてログインし、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-1.0-1.i386.rpm
```

インストールに成功すると、以下の出力が表示されます。

```
Preparing...          ##### [100%]
 1:foo                ##### [100%]
```

ご覧のとおり、RPM はパッケージ名を出力し、パッケージが進捗メーターとしてインストールされているため、ハッシュマークの連続して出力します。

パッケージのインストールまたはアップグレード時に、パッケージの署名が自動的にチェックされます。署名は、パッケージが承認されたパーティーによって署名されていることを確認します。たとえば、署名の検証に失敗した場合、以下のようなエラーメッセージが表示されます。

```
error: V3 DSA signature: BAD, key ID 0352860f
```

新しいヘッダーのみの署名の場合は、以下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に適切なキーがインストールされていない場合、メッセージには以下のように

NOKEY という単語が含まれます。

```
warning: V3 DSA signature: NOKEY, key ID 0352860f
```

パッケージの署名の確認に関する詳細は、「[パッケージの署名の確認](#)」を参照してください。



#### WARNING

カーネルパッケージをインストールする場合は、代わりに `rpm -ivh` を使用する必要があります。詳細は、[36章カーネルの手動によるアップグレード](#)を参照してください。

パッケージのインストールはシンプルとなるように設計されていますが、エラーが発生することがあります。

#### 15.2.2.1. 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、以下が表示されます。

```
Preparing... ##### [100%]
package foo-1.0-1 is already installed
```

インストールしようとしているバージョンと同じバージョンがすでにインストールされ、パッケージをインストールする場合は、`--replacepkgs` オプションを使用できます。これにより、RPM にエラーを無視するように指示します。

```
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 から元の設定ファイルをインストールする場合に便利です。

#### 15.2.2.2. 競合するファイル

別のパッケージまたはそれ以前のバージョンですでにインストールされているファイルを含むパッケージのインストールを試みると、以下が表示されます。

```
Preparing... ##### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package bar-2.0.20
```

RPM がこのエラーを無視するには、`--replacefiles` オプションを使用します。

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

### 15.2.2.3. 解決できない依存関係

RPM パッケージは基本的に、他のパッケージに依存します。つまり、適切に実行するために他のパッケージをインストールする必要があります。未解決の依存関係があるパッケージをインストールしようとすると、以下のような出力が表示されます。

```
error: Failed dependencies:
  bar.so.2 is needed by foo-1.0-1
Suggested resolutions:
  bar-2.0.20-3.i386.rpm
```

Red Hat Enterprise Linux CD-ROM セットからパッケージをインストールする場合は、通常、依存関係の解決に必要なパッケージを提案します。Red Hat Enterprise Linux CD-ROM または Red Hat FTP サイト（またはミラー）で推奨されるパッケージを見つけ、これを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に成功すると、以下のような出力が表示されます。

```
Preparing... ##### [100%]
1:foo          ##### [ 50%]
2:bar          ##### [100%]
```

依存関係を解決するパッケージを提案していない場合は、`--redhatprovides` オプションを試して、必要なファイルを含むパッケージを判断してください。このオプションを使用するには、`rpmdb-redhat` 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 --redhatprovides bar.so.2
```

`bar.so.2` が含まれるパッケージが、`rpmdb-redhat` パッケージからインストールされたデータベースにある場合は、パッケージ名が表示されます。



```
bar-2.0.20-3.i386.rpm
```

(パッケージが正しく実行されない可能性があるため) インストールを強制的に実行するには、`--nodeps` オプションを使用します。

### 15.2.3. アンインストール

パッケージのアンインストールは、パッケージのインストールと同様に簡単です。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
```



#### 備考

元のパッケージ ファイル `foo -1.0-1.i386.rpm` の名前ではなく、パッケージ名 `foo` を使用していました。パッケージをアンインストールするには、`foo` を元のパッケージの実際のパッケージ名に置き換えます。

別のインストール済みパッケージが削除しようとしているパッケージに依存する場合は、パッケージをアンインストールする際に依存関係エラーが発生する可能性があります。以下に例を示します。

```
error: Failed dependencies:
    foo is needed by (installed) bar-2.0.20-3.i386.rpm
```

RPM がこのエラーを無視し、パッケージの依存関係を中断する可能性があるパッケージをアンインストールする場合は、`--nodeps` オプションを使用します。

### 15.2.4. アップグレード

パッケージのアップグレードは、パッケージのインストールに似ています。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
```

パッケージのアップグレードの一環として、RPM は古いバージョンの `foo` パッケージを自動的にアンインストールします。実際、以前のバージョンがインストールされていない場合でも、`-U` を使用して、機能するパッケージをインストールしたい場合があります。



## ヒント

RPM は以前のカーネルパッケージに置き換わるため、カーネルパッケージのインストールに `-U` オプションを使用したくありません。これは実行中のシステムには影響しませんが、次の再起動時に新しいカーネルが起動できない場合は、代わりに他のカーネルが起動できません。

`-i` オプションを使用すると、カーネルを GRUB 起動メニュー(`/etc/grub.conf`)に追加します。同様に、不要な古いカーネルを削除すると、GRUB からカーネルが削除されます。

RPM は設定ファイルを使ってパッケージのインテリジェントなアップグレードを実行するので、以下のようなメッセージが表示されることがあります。

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

このメッセージは、設定ファイルへの変更が、パッケージ内の新しい設定ファイルと後方互換性がない可能性があります。そのため、RPM は元のファイルを保存し、新しいファイルをインストールしてください。システムが適切に機能し続けるようにするには、2つの設定ファイル間の違いを調べ、できるだけ早く解決する必要があります。

アップグレードはアンインストールとインストールの組み合わせであるため、RPM のアップグレード時に、アンインストールおよびインストールエラーが発生し、さらにエラーが1つ以上発生する可能性があります。RPM が古いバージョン番号のパッケージにアップグレードしようとしていると考える場合、出力は以下のようになります。

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

RPM を強制的にアップグレードするには、`--oldpackage` オプションを使用します。

```
rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
```

### 15.2.5. Freshening

パッケージの追加は、パッケージのアップグレードに似ています。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 の新規オプションは、コマンドラインで指定したパッケージのバージョンと、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を確認します。すでにインストールされているパッケージの新規バージョンが RPM の新規オプションで処理されると、そのパッケージが新しいバージョンにアップグレードされます。ただし、同じ名前のパッケージが存在しない場合、RPM の `newen` オプションはパッケージをインストールしません。これは、以前の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かどうかにかかわらず、アップグレードによってパッケージがインストールされるため、RPM のアップグレードオプションとは異なります。

RPM の新規オプションは、1つのパッケージまたはパッケージグループで機能します。多数の異なるパッケージをダウンロードし、システムにすで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する場合は、新たにジョブを行います。新しいパッケージを使用する場合は、RPM を使用する前にダウンロードしたグループから不要なパッケージを削除する必要はありません。

この場合は、以下のコマンドを実行します。

```
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を自動的にアップグレードします。

### 15.2.6. クエリ

`rpm -q` コマンドを使用して、インストール済みパッケージのデータベースにクエリーします。`rpm -q foo` コマンドは、インストール済みパッケージのパッケージ名、バージョン、リリース番号を表示します。

```
foo-2.0-1
```



備考

パッケージをクエリーするには、`foo` を実際のパッケージ名に置き換えます。

パッケージ名を指定する代わりに、`-q` で以下のオプションを使用して、問い合わせるパッケージを指定します。これらはパッケージの選択オプションと呼ばれます。

- `-a` は、現在インストールされているすべてのパッケージをクエリーします。
- `-f <file>` は、`<file>` を所有するパッケージをクエリーします。ファイルを指定する場合は、ファイルの完全パスを指定する必要があります (例: `/bin/lis`)。

- `-p &lt;packagefile>` は パッケージ `<packagefile>` をクエリーします。

クエリーされたパッケージに関する情報を表示する方法は複数あります。以下のオプションは、検索する情報のタイプを選択するために使用されます。これらは Information Query Options と呼ばれます。

- `-i` は、名前、説明、リリース、サイズ、ビルド日、インストール日、ベンダー、その他のその他の情報など、パッケージ情報を表示します。
- `-l` 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` は、パッケージ内の全ファイルの状態を表示します。
- `-d` は、ドキュメントとしてマークされているファイルの一覧を表示します (man ページ、情報ページ、README など)。
- `-c` は、設定ファイルとしてマークされているファイルの一覧を表示します。これは、パッケージのインストール後に変更するファイルです (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、一般的な `ls -l` 形式でリストを表示します。

### 15.2.7. 検証

パッケージの検証は、パッケージからインストールしたファイルに関する情報と、元のパッケージからの同じ情報を比較します。また、検証により、各ファイルのサイズ、MD5 合計、パーミッション、タイプ、所有者、およびグループを比較します。

コマンド `rpm -V` はパッケージを検証します。クエリーに一覧表示されるパッケージ検証 オプションのいずれかを使用して、検証するパッケージを指定できます。検証の簡単な使用法は `rpm -V foo` です。これは、`foo` パッケージ内のすべてのファイルが、最初にインストールした時と同じであることを検証します。以下に例を示します。

- 特定のファイルを含むパッケージを確認するには、次のコマンドを実行します。

```
rpm -Vf /usr/bin/vim
```

- インストールされているすべてのパッケージを確認するには、次のコマンドを実行します。

```
rpm -Va
```

- RPM パッケージファイルに対してインストール済みのパッケージを確認するには、次のコマンドを実行します。

```
rpm -Vp foo-1.0-1.i386.rpm
```

このコマンドは、RPM データベースが破損していると思われる場合に便利です。

すべてが適切に検証された場合、出力はありません。不一致がある場合は、それらが表示されます。出力の形式は、8文字の文字列（cは設定ファイルを示します）、ファイル名です。8文字はそれぞれ、ファイルの1つの属性とRPMデータベースに記録された属性の値を比較した結果を示します。1つのピリオド(.)は、テストに合格したことを意味します。以下の文字は、特定のテストの失敗を示しています。

- 5 - MD5 checksum
- s - ファイルサイズ
- l - シンボリックリンク
- T - ファイル変更時間
- d - device
- u - user

- **g - group**
- **m: モード (パーミッションおよびファイルタイプを含む)**
- **? - 読み取り不可能なファイル**

出力が表示された場合は、最善の判断を使用して、パッケージを削除または再インストールする必要があるかを判断するか、別の方法で問題を修正します。

### 15.3. パッケージの署名の確認

パッケージが破損していないか、改ざんされていないことを確認する場合は、シェルプロンプトで以下のコマンドを入力して `md5sum` のみを確認します (RPM パッケージのファイル名は `<rpm-file>` です)。

```
rpm -K --nosignature <rpm-file>
```

`<rpm-file>` : `md 5 OK` というメッセージが表示されます。この簡単なメッセージは、ファイルのダウンロードによって破損されなかったことを意味します。より詳細なメッセージを表示するには、コマンドの `-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だけに信頼する方法。パッケージが開発者の GnuPG キーで署名されている場合、開発者がそれらが本人であることがわかっていることが分かります。

RPM パッケージは、ダウンロードしたパッケージに信頼できるものにするために、Gnu Privacy Guard (または GnuPG) を使用して署名できます。

GnuPG は、安全な通信を行うためのツールです。これは、電子プライバシープログラムである PGP の暗号化テクノロジーの完全な置換です。GnuPG を使用すると、ドキュメントの有効性を認証し、他の受信者との間でデータを暗号化/復号化できます。GnuPG は PGP 5.x ファイルを復号および検証することもできます。

インストール時に、ART はデフォルトでインストールされます。これにより、Red Hat から受け取るパッケージを確認できるようにするために GnuPG の使用をすぐに開始できます。まず、Red Hat の公開鍵をインポートする必要があります。

### 15.3.1. 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。これを行うには、シェルプロンプトで以下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鍵の一覧を表示するには、以下のコマンドを実行します。

```
rpm -qa gpg-pubkey*
```

Red Hat キーの出力には、以下が含まれます。

```
gpg-pubkey-db42a60e-37ea5438
```

特定のキーの詳細を表示するには、rpm -qi の後に直前のコマンドの出力を使用します。

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

### 15.3.2. パッケージの署名の確認

ビルダーの GnuPG キーのインポート後に RPM ファイルの GnuPG 署名を確認するには、以下のコマンドを使用します (<rpm-file> を RPM パッケージのファイル名に置き換えます)。

```
rpm -K <rpm-file>
```

すべてが正常に行われると、md5 gpg OK メッセージが表示されます。つまり、パッケージの署名を検証し、破損していないことを意味します。

## 15.4. RPM で金を抑制する

RPM は、システムの管理と問題の診断と修正の両方に役立ちます。すべてのオプションを把握する最適な方法は、いくつかの例を参照してください。

- 場合によっては、誤って一部のファイルを削除しましたが、削除内容を把握しているわけではありません。システム全体を検証し、足りないものを確認するには、以下のコマンドを実行します。

■

```
rpm -Va
```

一部のファイルが欠落しているか、破損している場合、パッケージを再インストールするか、またはアンインストールしてからパッケージを再インストールします。

- 場合によっては、認識しないファイルが表示される場合があります。パッケージを所有するパッケージを確認するには、次のコマンドを実行します。

```
rpm -qf /usr/bin/ggv
```

出力は以下のようになります。

```
ggv-2.6.0-2
```

- 以下のシナリオにおいて、上記の2つの例を組み合わせることができます。/usr/bin/paste に問題があるとします。そのプログラムを所有するパッケージを確認しますが、どのパッケージが貼り付けるかは分かりません。以下のコマンドを入力します。

```
rpm -Vf /usr/bin/paste
```

また、適切なパッケージが検証されています。

- 特定のプログラムに関する詳細情報を見つけてもよろしいですか？以下のコマンドを試し、そのプログラムを所有するパッケージに含まれるドキュメントを確認できます。

```
rpm -qdf /usr/bin/free
```

出力は以下のようになります。

```
/usr/share/doc/procps-3.2.3/BUGS  
/usr/share/doc/procps-3.2.3/FAQ  
/usr/share/doc/procps-3.2.3/NEWS  
/usr/share/doc/procps-3.2.3/TODO  
/usr/share/man/man1/free.1.gz  
/usr/share/man/man1/pgrep.1.gz  
/usr/share/man/man1/pkill.1.gz  
/usr/share/man/man1/pmap.1.gz  
/usr/share/man/man1/ps.1.gz  
/usr/share/man/man1/skill.1.gz  
/usr/share/man/man1/slabtop.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 が見つかるかもしれませんが、何ができるのかは分かりません。情報を確認するには、以下のコマンドを使用します。

```
rpm -qip crontabs-1.10-7.noarch.rpm
```

出力は以下のようになります。

```

Name       : crontabs                Relocations: (not relocatable)
Version    : 1.10                   Vendor: Red Hat, Inc
Release    : 7                     Build Date: Mon 20 Sep 2004 05:58:10 PM EDT
Install Date: (not installed)      Build Host: tweety.build.redhat.com
Group      : System Environment/Base Source RPM: crontabs-1.10-7.src.rpm
Size       : 1004                  License: Public Domain
Signature  : DSA/SHA1, Wed 05 Jan 2005 06:05:25 PM EST, Key ID 219180cddb42a60e
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.

```

- 場合によっては、crontabs RPM がどのファイルをインストールするかを見てください。以下を入力します。

```
rpm -qlp crontabs-1.10-5.noarch.rpm
```

出力は以下の例のようになります。

```

/etc/cron.daily
/etc/cron.hourly
/etc/cron.monthly
/etc/cron.weekly
/etc/crontab
/usr/bin/run-parts

```

これらはいくつかの例です。RPM に使用することが多くあります。

## 15.5. 関連情報

RPM は、パッケージのクエリー、インストール、アップグレード、および削除を行う数多くのオプションと、非常に複雑なユーティリティーです。RPM の詳細は、以下の資料を参照してください。

### 15.5.1. インストールされているドキュメント

- `rpm --help` - このコマンドは、RPM パラメーターのクイックリファレンスを表示します。
- `man rpm` - RPM の man ページには、`rpm --help` コマンドよりも RPM パラメーターに関する詳細が記載されています。

### 15.5.2. 便利な Web サイト

- <http://www.rpm.org/>: RPM の Web サイト
- <http://www.redhat.com/mailman/listinfo/rpm-list/>: RPM メーリングリストは、ここにアーカイブされます。サブスクライブするには、単語で [rpm-list-request@redhat.com](mailto:rpm-list-request@redhat.com) にメールを送信し、サブジェクトの行にサブスクライブします。

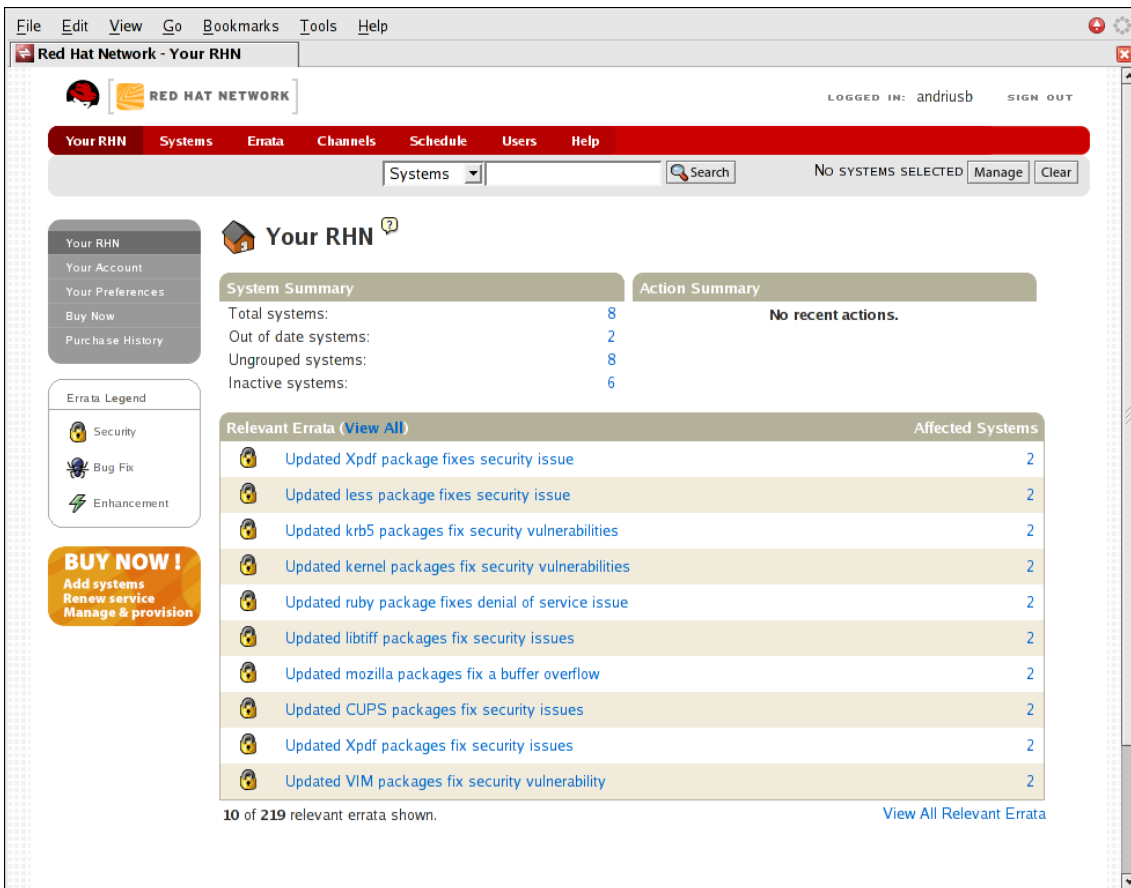
### 15.5.3. 関連書籍

- 『Red Hat RPM Guide』 (Eric Foster-Johnson; Wiley, John & Sons, Incorporated)- 本ガイドでは、パッケージのインストールから RPM の構築まで、RPM に対する包括的なガイドです。

## 第16章 RED HAT NETWORK

Red Hat Network は、1 つ以上の Red Hat Enterprise Linux システムを管理するためのインターネットソリューションです。すべてのセキュリティーアラート、バグ修正アラート（エラータアラートと総称される）は、Package Updater スタンドオンアプリケーションを使用するか、<https://rhn.redhat.com/> の RHN Web サイトを使用して Red Hat から直接ダウンロードできます。

図16.1 RHN



[D]

Red Hat Network は、更新されたパッケージがリリースされるとメールを受け取るので、時間を節約できます。Web で更新されたパッケージやセキュリティーアラートを検索する必要はありません。デフォルトでは、Red Hat Network はパッケージもインストールします。RPM の使用方法や、ソフトウェアパッケージの依存関係の解決について把握する必要はありません。RHN がこれらすべてを行います。

Red Hat Network の機能は以下のとおりです。

- エラータアラート：ネットワーク内のすべてのシステムについて、セキュリティーアラート、バグ修正アラート、および機能拡張アラートが発行されるタイミングを確認します。

図16.2 関連エラータ

The screenshot shows the Red Hat Network web interface. The main heading is "Errata Relevant to Your Systems". Below this is a table with columns: Type, Advisory, Synopsis, Systems, and Updated. The table lists 16 errata entries, including Rhsas and Rhbas with their respective descriptions and update dates. On the left side, there is a sidebar with "Errata Legend" (Security, Bug Fix, Enhancement) and a "BUY NOW!" button.

Type	Advisory	Synopsis	Systems	Updated
Security	RHSA-2005:059	Updated Xpdf package fixes security issue	2	2005-01-26
Security	RHSA-2005:068	Updated less package fixes security issue	2	2005-01-26
Security	RHSA-2005:012	Updated krb5 packages fix security vulnerabilities	2	2005-01-19
Security	RHSA-2005:043	Updated kernel packages fix security vulnerabilities	2	2005-01-18
Security	RHSA-2004:635	Updated ruby package fixes denial of service issue	2	2005-01-17
Security	RHSA-2005:019	Updated libtiff packages fix security issues	2	2005-01-13
Security	RHSA-2005:038	Updated mozilla packages fix a buffer overflow	2	2005-01-13
Security	RHSA-2005:018	Updated Xpdf packages fix security issues	2	2005-01-12
Security	RHSA-2005:013	Updated CUPS packages fix security issues	2	2005-01-12
Security	RHSA-2005:010	Updated VIM packages fix security vulnerability	2	2005-01-05
Bug Fix	RHBA-2004:699	Updated samba packages	2	2005-01-04
Bug Fix	RHBA-2004:700	Updated aspell packages	2	2005-01-04
Security	RHSA-2004:651	Updated imlib packages fix security vulnerabilities	2	2004-12-23
Security	RHSA-2004:654	Updated SquirrelMail package fixes security vulnerability	2	2004-12-23
Bug Fix	RHBA-2004:696	Updated BIND packages	2	2004-12-23
Security	RHSA-2004:680	Updated kernel packages fix security vulnerabilities	2	2004-12-23

[D]

- **自動メール通知**：システムに対してエラータ通知が発行されたときにメール通知を受け取ります。
- **スケジュールされたエラータ更新 - エラータ更新のスケジュール**
- **パッケージのインストール** - ボタンをクリックする、1つ以上のシステムへのパッケージインストールのスケジュール
- **Package Updater - Package Updater** を使用して、システムの最新ソフトウェアパッケージをダウンロードします（オプションのパッケージインストールを使用）。
- **Red Hat Network Web サイト**：複数のシステムの管理、個々のパッケージのダウンロード、およびコンピューターからの安全な Web ブラウザー接続によるエラータ更新などのスケジュールアクション

**WARNING**

**Red Hat Network** にシステムを登録する前に、**Red Hat Enterprise Linux** 製品をアクティベートして、お使いのシステムが正しいサービスに割り当てられていることを確認してください。プロダクトを有効にするには、以下に移動します。

<http://www.redhat.com/apps/activate/>

製品をアクティベートしたら、**Red Hat Network** に登録してエラー更新を受け取ります。登録プロセスは、更新の通知に必要なシステムに関する情報を収集します。たとえば、システムにインストールされているパッケージの一覧はコンパイルされるため、システムに関連する更新のみが通知されません。

システムを初めて起動すると、**Software Update Setup Assistant** により登録が求められます。登録していない場合は、デスクトップで **Applications** (パネルのメインメニュー) => **System Tools** => **Package Updater** を選択して登録プロセスを開始します。または、シェルプロンプトから **yum update** コマンドを実行します。

図16.3 RHN への登録

**Step 3: Register a System Profile - Packages**

RPM information is important to determine what updated software packages are relevant to this system.

Include RPM packages installed on this system in my System Profile

Below is a list of packages present on your system that RPM knows about:

	Package Name	Version	Release
<input checked="" type="checkbox"/>	4Suite	0.11.1	14
<input checked="" type="checkbox"/>	GConf	1.0.9	12
<input checked="" type="checkbox"/>	GConf2	2.2.1	1
<input checked="" type="checkbox"/>	Glide3	2001052	25
<input checked="" type="checkbox"/>	MAKEDEV	3.3.6	1
<input checked="" type="checkbox"/>	ORBit	0.5.17	10.4
<input checked="" type="checkbox"/>	ORBit2	2.6.2	1

By default, all packages that RPM knows about will be included in your System Profile. Uncheck any packages which you do not want to be included.

[D]

登録後は、以下のいずれかの方法を使用して更新の受信を開始します。

- デスクトップで **Applications** (パネルのメインメニュー) => **System Tools** => **Package Updater** を選択します。
- シェルプロンプトから `yum` コマンドを実行します。
- RHN の Web サイト(<https://rhn.redhat.com/>)を使用します。
- パネルにパッケージアイコンをクリックして、**Package Updater** を起動します。

詳細については、以下のドキュメントを参照してください。

<http://www.redhat.com/docs/manuals/RHNetwork/>



## ヒント

**Red Hat Enterprise Linux** には、**Red Hat Enterprise Linux** システムの更新がある場合に表示されるアラートを表示する便利なパネルアイコンが含まれています。利用可能な更新がない場合は、このパネルアイコンは表示されません。

## パート IV. ネットワーク関連の設定

ネットワークの設定方法の説明後、このパートでは、リモートログイン、ネットワーク経由でのファイル共有、Web サーバーの設定などのネットワーク関連のトピックについて説明します。



## 第17章 NETWORK CONFIGURATION

相互に通信するには、コンピューターにネットワーク接続が必要です。これは、オペレーティングシステムがインターフェースカード (Ethernet、ISDN モデム、トークンリングなど) を認識し、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することで実行できます。

**Network Administration Tool** を使用すると、以下のタイプのネットワークインターフェースを設定できます。

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

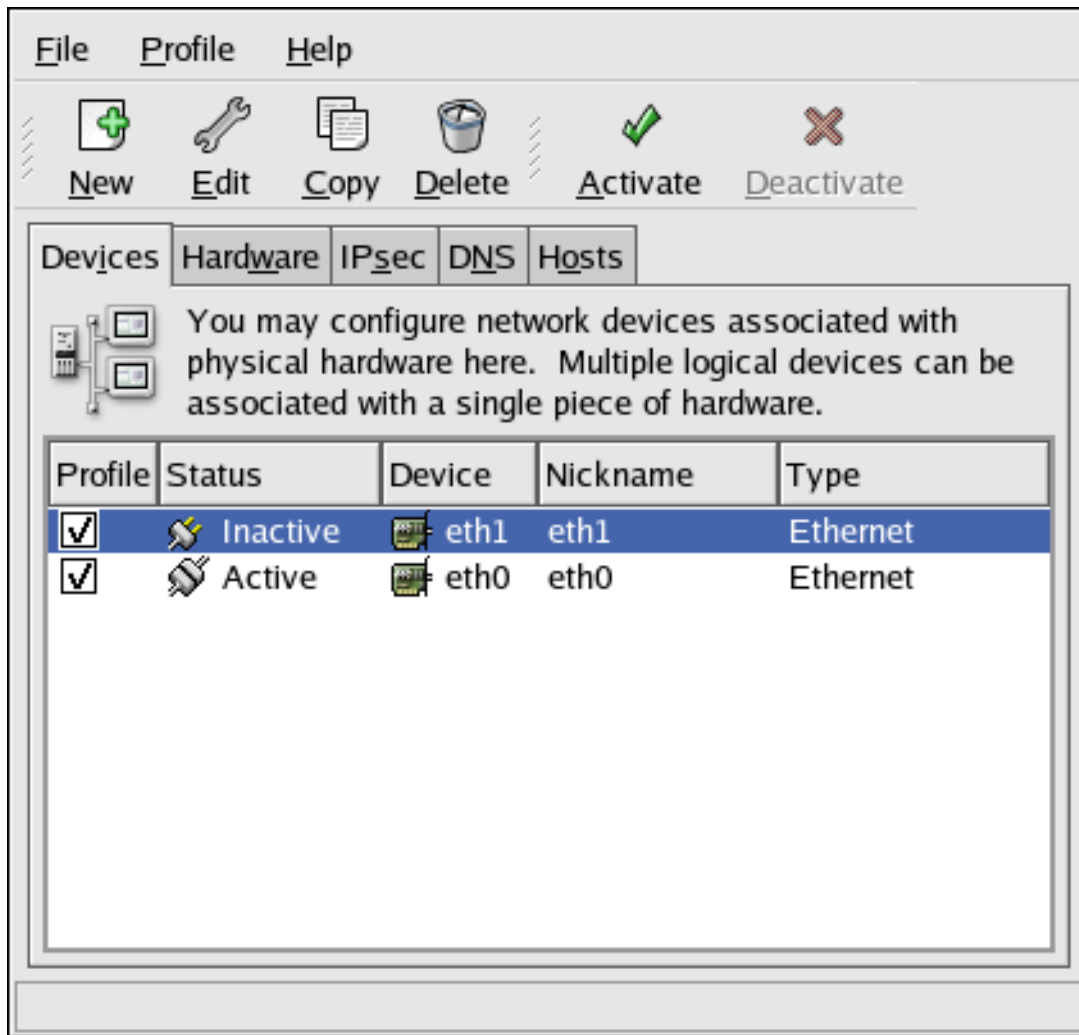
IPsec 接続の設定、DNS 設定の管理、および追加のホスト名と IP アドレスの組み合わせの保存に使用する `/etc/hosts` ファイルの管理にも使用できます。

ネットワーク管理ツールを使用するには、`root` 権限が必要になります。アプリケーションを起動するには、**Applications** (パネルのメインメニュー) => **System Settings** => **Network** に移動するか、シェルプロンプトで `system-config-network` コマンド (`XTerm` や `GNOME` ターミナルなど) を入力します。コマンドを入力すると、`X` が実行されているとグラフィカルバージョンが表示されます。それ以外の場合は、テキストベースのバージョンが表示されます。

コマンドラインのバージョンを使用するには、`root` でコマンド `system-config-network-cmd --help`

を実行して、すべてのオプションを表示します。

図17.1 ネットワーク管理ツール



[D]



#### ヒント

Red Hat Hardware Compatibility List(<http://hardware.redhat.com/hcl/>)を使用して、Red Hat Enterprise Linux がハードウェアデバイスに対応しているかどうかを確認します。

### 17.1. 概要

Network Administration Tool を使用したネットワーク接続を設定するには、以下の手順を実行します。

1. 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。

2. ハードウェア一覧に物理ハードウェアデバイスが存在しない場合は追加します。
3. ホスト名および DNS 設定を構成します。
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各タイプの手順を説明します。

## 17.2. 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、ネットワークインターフェースカード(NIC)、ネットワークケーブル（通常は CAT5 ケーブル）、および接続先のネットワークが必要です。異なるネットワークが異なるネットワーク速度を使用するように設定されています。NIC が接続するネットワークと互換性があることを確認してください。

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 New 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、forward をクリックします。
4. ネットワークインターフェースカードをハードウェア一覧にすでに追加している場合は、イーサネットカード一覧からこれを選択します。それ以外の場合は、その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。



### 備考

インストールプログラムは、対応しているイーサネットデバイスを検出し、その設定を求めるプロンプトを出します。インストール時にイーサネットデバイスを設定すると、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.

**Other Ethernet Card** を選択した場合は、**Select Ethernet Adapter** ウィンドウが表示されます。イーサネットカードの製造元およびモデルを選択します。デバイス名を選択します。システムの最初のイーサネットカードの場合は、デバイス名として `eth0` を選択します。2 番目のイーサネットカードの場合は、`eth1` (など) を選択します。**Network Administration Tool** を使用すると、NIC のリソースを設定することもできます。**進む** をクリックして続けます。

6. のネットワーク設定ウィンドウで、**DHCP** と静的 IP アドレスのいずれかを選択します。[図17.2 「イーサネットの設定」](#) ネットワークの開始時にデバイスに別の IP アドレスを受信する場合は、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. **Create Ethernet Device** ページで **Apply** をクリックします。

図17.2 イーサネットの設定

**Configure Network Settings**

Automatically obtain IP address settings with: **dhcp**

DHCP Settings

Hostname (optional):

Automatically obtain DNS information from provider

Statically set IP addresses:

Manual IP Address Settings

Address:

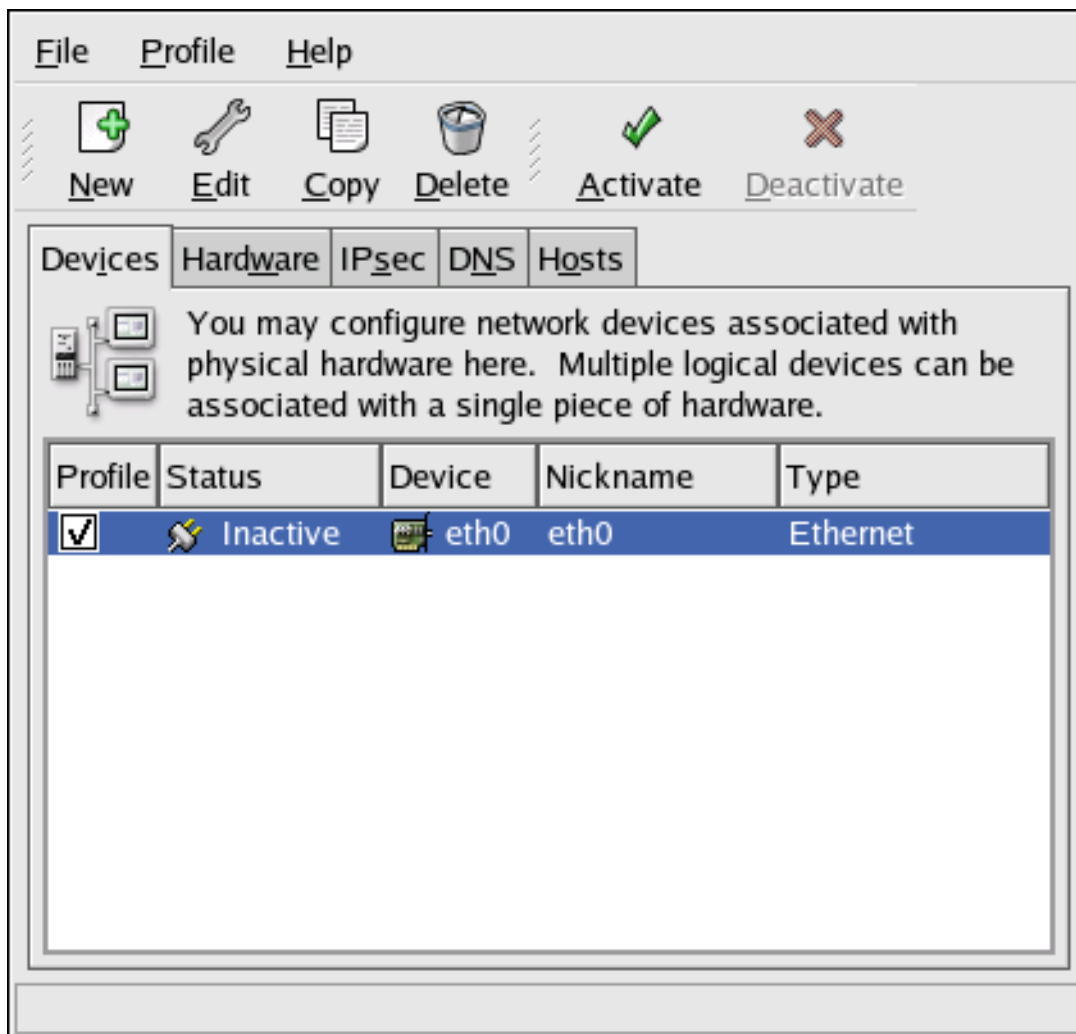
Subnet Mask:

Default Gateway Address:

[D]

イーサネットデバイスを設定すると、[図17.3 「イーサネットデバイス」](#) に示されるようにデバイス一覧に表示されます。

図17.3 イーサネットデバイス



[D]

イーサネット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** をクリックして、設定を **編集** できます。たとえば、デバイスが追加されると、デフォルトで起動時に開始するように設定されています。この設定を変更するには、デバイスの **編集** を選択し、コンピューターの起動時に **Activate device** を変更し、変更を保存します。

複数のデバイスをイーサネットカードに関連付けると、後続のデバイスはデバイスのエイリアスになります。デバイスエイリアスを使用すると、1つの物理デバイスに複数の仮想デバイスを設定できるため、1つの物理デバイスに複数のIPアドレスを指定できます。たとえば、eth1 デバイスと eth1:1 デバイスを設定できます。詳細は、「[デバイスエイリアス](#)」を参照してください。

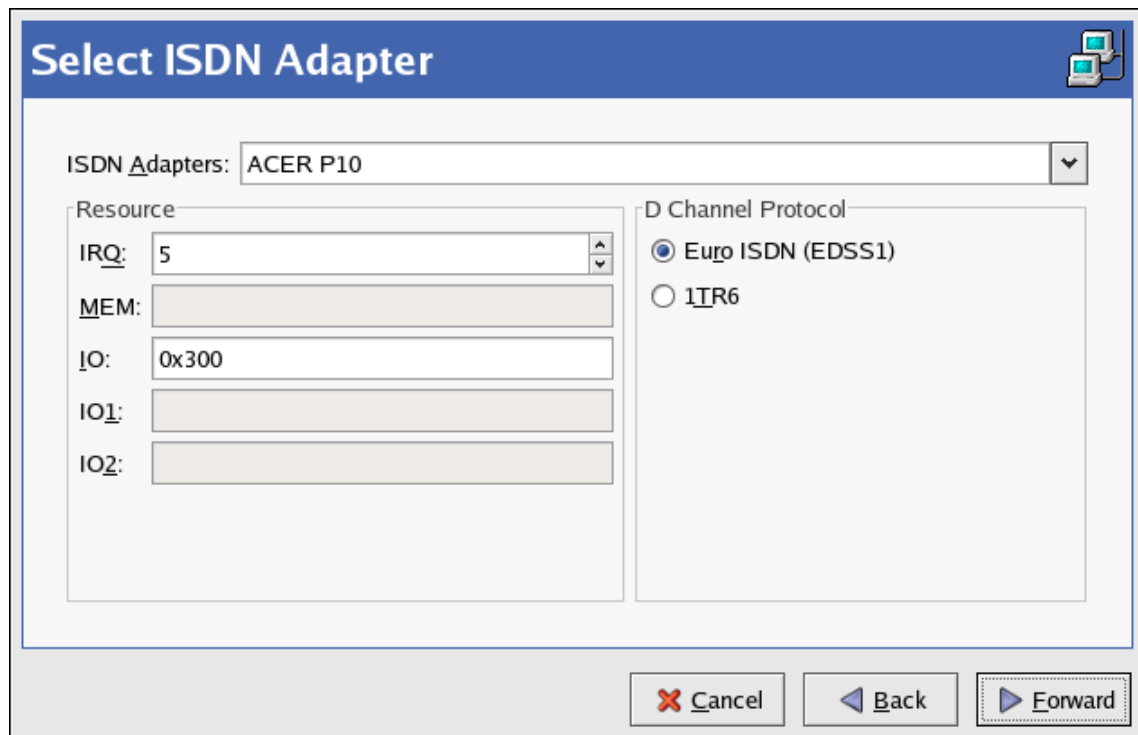
### 17.3. ISDN 接続の確立

ISDN 接続は、電話会社によって特別な phone 行がインストールされている ISDN モードm カードで確立されたインターネット接続です。ISDN 接続は欧州で人気があります。

ISDN 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 **New** 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、**forward** をクリックします。
4. プルダウンメニューから **ISDN アダプター** を選択します。次に、アダプターのリソースおよび **D** チャンネルプロトコルを設定します。進む をクリックして続けます。

図17.4 ISDN の設定



[D]

5. **Internet Service Provider(ISP)**が事前に設定された一覧にある場合は、これを選択します。それ以外の場合は、**ISP アカウント**に関する必要な情報を入力します。値が分からない場合は、**ISP**にお問い合わせください。**Forward** をクリックします。
6. **IP** 設定ウィンドウで、**Encapsulation Mode** を選択し、**IP アドレス**を自動的に取得するか、**静的 IP** を設定するかどうかを選択します。終了したら **Forward** をクリックします。

## 7.

**Create Dialup Connection** ページで **Apply** をクリックします。

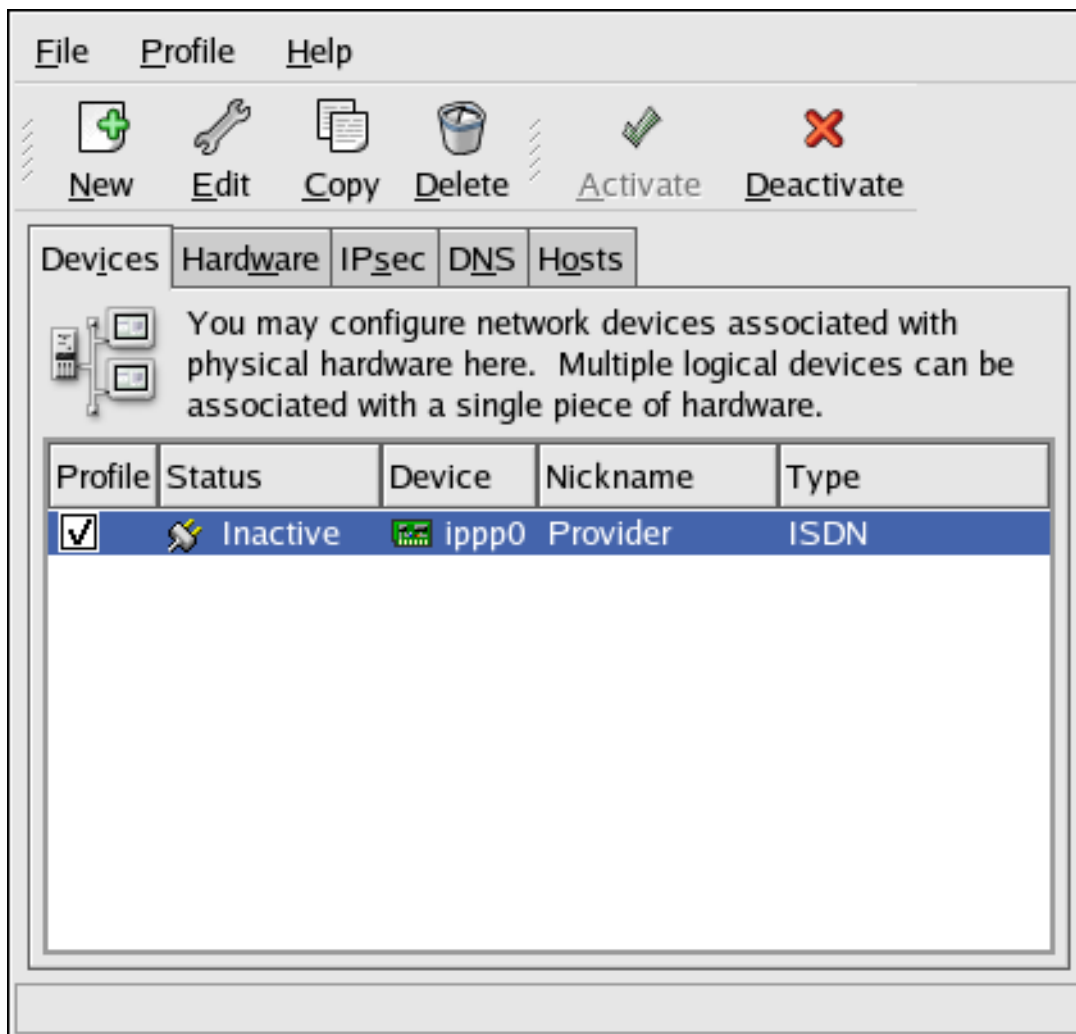
ISDN デバイスを設定したら、[図17.5 「ISDN デバイス」](#) に示されるように、それが ISDN タイプのデバイスとしてデバイス一覧に表示されます。

必ず **File => Save** を選択して変更を保存します。

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** をクリックして設定を編集できます。たとえば、デバイスが追加されると、デフォルトでシステムの起動時には開始しないように設定されています。設定を編集してこの設定を変更します。圧縮、PPP オプション、ログイン名、パスワードなどを変更することができます。

デバイスが追加されると、**Inactive** ステータスにあるように、すぐにアクティブになりません。デバイスを有効にするには、デバイス一覧から選択し、**Activate** ボタンをクリックします。コンピューターの起動時にシステムをアクティベートするように構成されている場合（デフォルト）、この手順を再度実行する必要があります。

図17.5 ISDN デバイス



[D]

#### 17.4. モード接続の確立

モデムを使用して、アクティブな電話番号でインターネット接続を設定できます。インターネットサービスプロバイダー(ISP)アカウント（ダイヤルアップアカウントとも呼ばれます）が必要です。

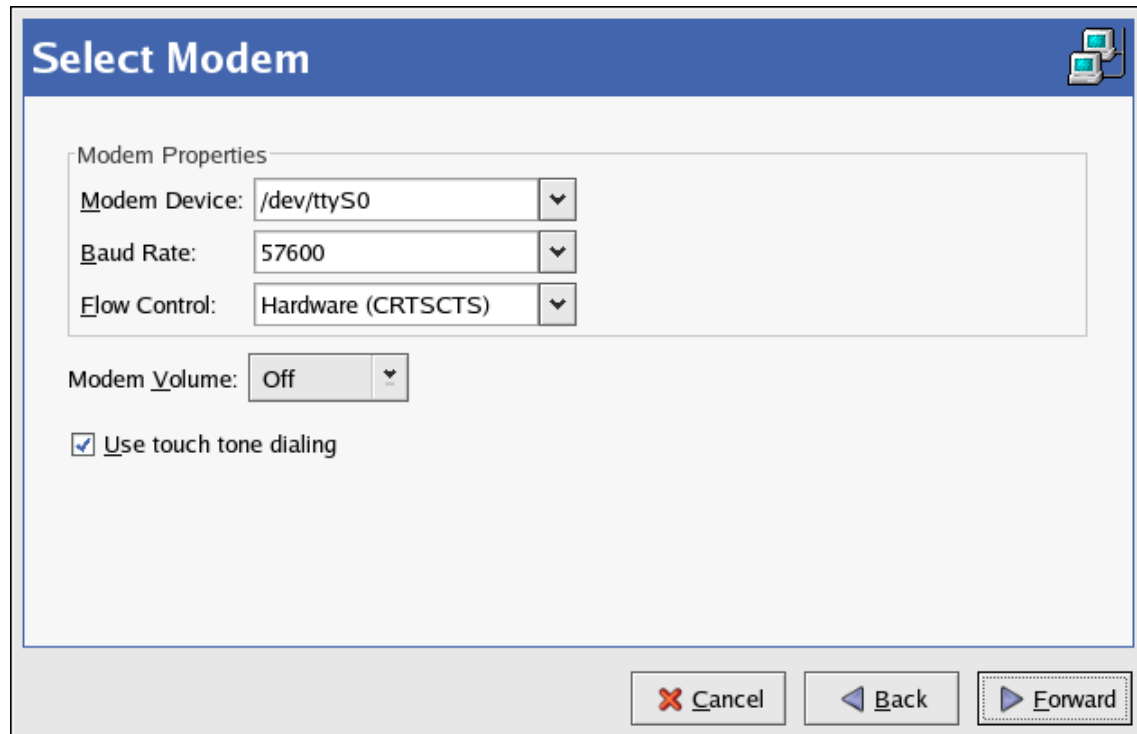
モード接続を追加するには、以下の手順に従います。

1. デバイス タブをクリックします。
2. ツールバーの *New* ボタンをクリックします。
3. *Device Type* リストから *Modem connection* を選択し、*forward* をクリックします。



4. ハードウェア一覧にモードがすでに設定されている場合は、**Network Administration Tool** がそれを使用してモード接続を確立することを想定します。すでに **modems** が設定されていない場合は、システムのいずれのモードも検出しようとしています。このプローブには時間がかかる場合があります。モデムが見つからない場合は、表示される設定がプローブから見つかった値がないことを警告するメッセージが表示されます。
5. プロービングすると、[図17.6 「モード設定」](#) にウィンドウが表示されます。

図17.6 モード設定



[D]

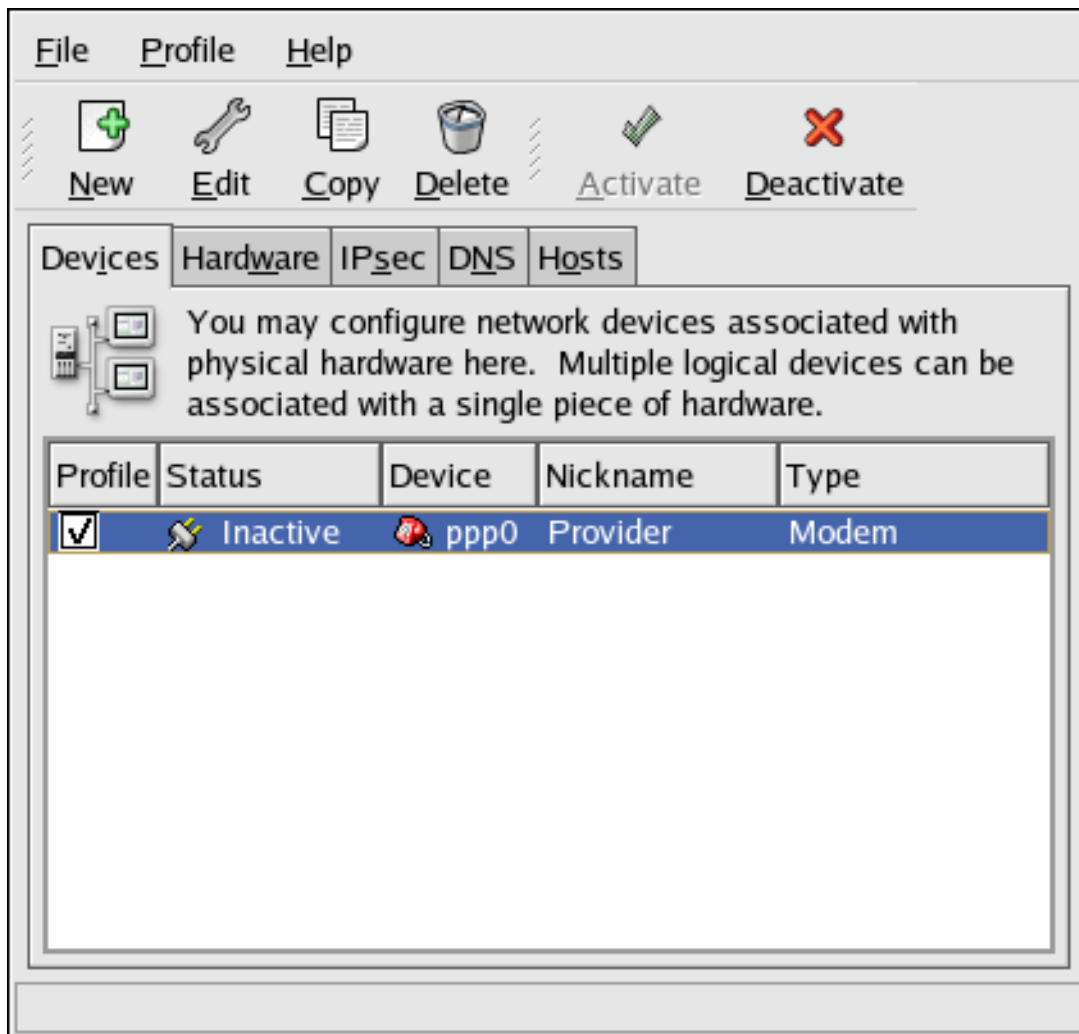
6. **modem** デバイス、ボーレート、フロー制御、および **modem** ボリュームを設定します。これらの値が分からない場合は、モードがプローブされたかどうかについてデフォルト値を受け入れます。手間が入らない場合は、該当するチェックボックスにチェックを入れてください。**Forward** をクリックします。
7. **ISP** が事前に設定された一覧にある場合は、これを選択します。それ以外の場合は、**ISP** アカウントに関する必要な情報を入力します。これらの値が分からない場合は、**ISP** にお問い合わせください。**Forward** をクリックします。
8. **IP** 設定 ページで、**IP** アドレスを自動的に取得するか、または静的に設定するかどうかを選択します。終了したら **Forward** をクリックします。

## 9.

**Create Dialup Connection** ページで **Apply** をクリックします。

**modem** デバイスを設定すると、[図17.7 「モデムデバイス」](#) に示すように、タイプが **Modem** のデバイス一覧に表示されます。

図17.7 モデムデバイス



[D]

必ず **File => Save** を選択して変更を保存します。

**modem** 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** できます。たとえば、デバイスが追加されると、デフォルトでシステムの起動時には開始しないように設定されています。設定を編集してこの設定を変更します。圧縮、PPP オプション、ログイン名、パスワードなどを変更することもできます。

デバイスが追加されると、**Inactive** ステータスにあるように、すぐにアクティブになりません。デバイスを有効にするには、デバイス一覧から選択し、**Activate** ボタンをクリックします。コンピュー

ターの起動時にシステムをアクティベートするように構成されている場合（デフォルト）、この手順を再度実行する必要があります。

### 17.5. XDSL 接続の確立

DSL は、**Digital Subscriber Lines** を表します。DSL には、**ADSL**、**IDSL**、**SDSL** などのさまざまなタイプがあります。Network Administration Tool は **xDSL** という用語を使用して、すべてのタイプの DSL 接続を意味します。

DSL プロバイダーによっては、イーサネットカードを使用して DHCP で IP アドレスを取得するようシステムを設定する必要があります。DSL プロバイダーによっては、イーサネットカードで PPPoE(Point-to-Point Protocol over Ethernet)接続を設定する必要があります。使用する DSL プロバイダーに尋ねます。

DHCP を使用する必要がある場合は、「[イーサネット接続の確立](#)」を参照して、イーサネットカードを設定します。

PPPoE を使用する必要がある場合は、以下の手順に従います。

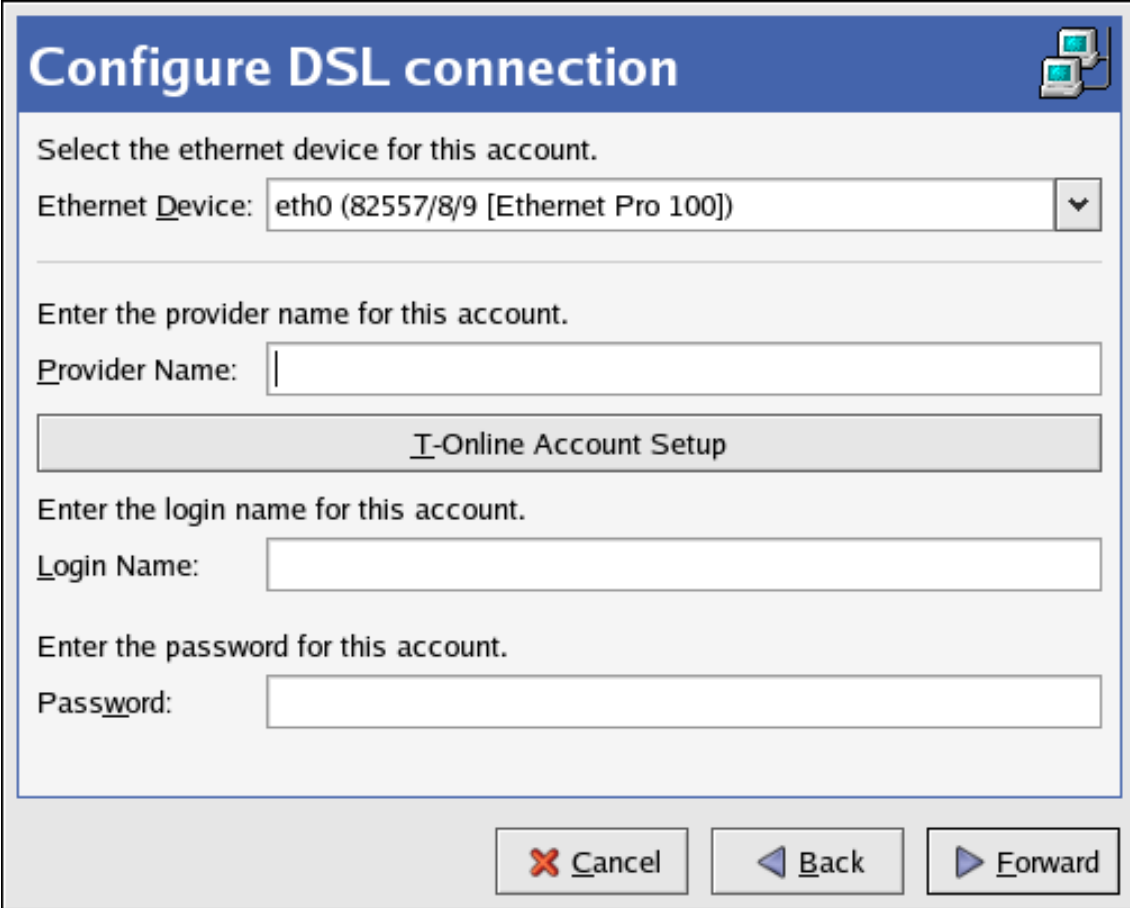
1. デバイス タブをクリックします。
2. New ボタンをクリックします。
3. デバイスタイプリストから **xDSL 接続** を選択し、**forward** をクリックします。
4. イーサネットカードがハードウェア一覧にある場合は、[図17.8 「xDSL 設定」](#) に表示されるページから、プルダウンメニューから **Ethernet Device** を選択します。それ以外の場合は、**Select Ethernet Adapter** ウィンドウが表示されます。



#### 備考

インストールプログラムは、対応しているイーサネットデバイスを検出し、その設定を求めるプロンプトを出します。インストール時にイーサネットデバイスを設定すると、ハードウェア タブのハードウェア一覧に表示されます。

図17.8 xDSL 設定



[D]

5.

**Select Ethernet Adapter** ウィンドウが表示されたら、イーサネットカードの製造元およびモデルを選択します。デバイス名を選択します。システムの最初のイーサネットカードの場合は、デバイス名として `eth0` を選択します。2 番目のイーサネットカードの場合は、`eth1`（など）を選択します。**Network Administration Tool** を使用すると、NIC のリソースを設定することもできます。**進む** をクリックして続けます。

6.

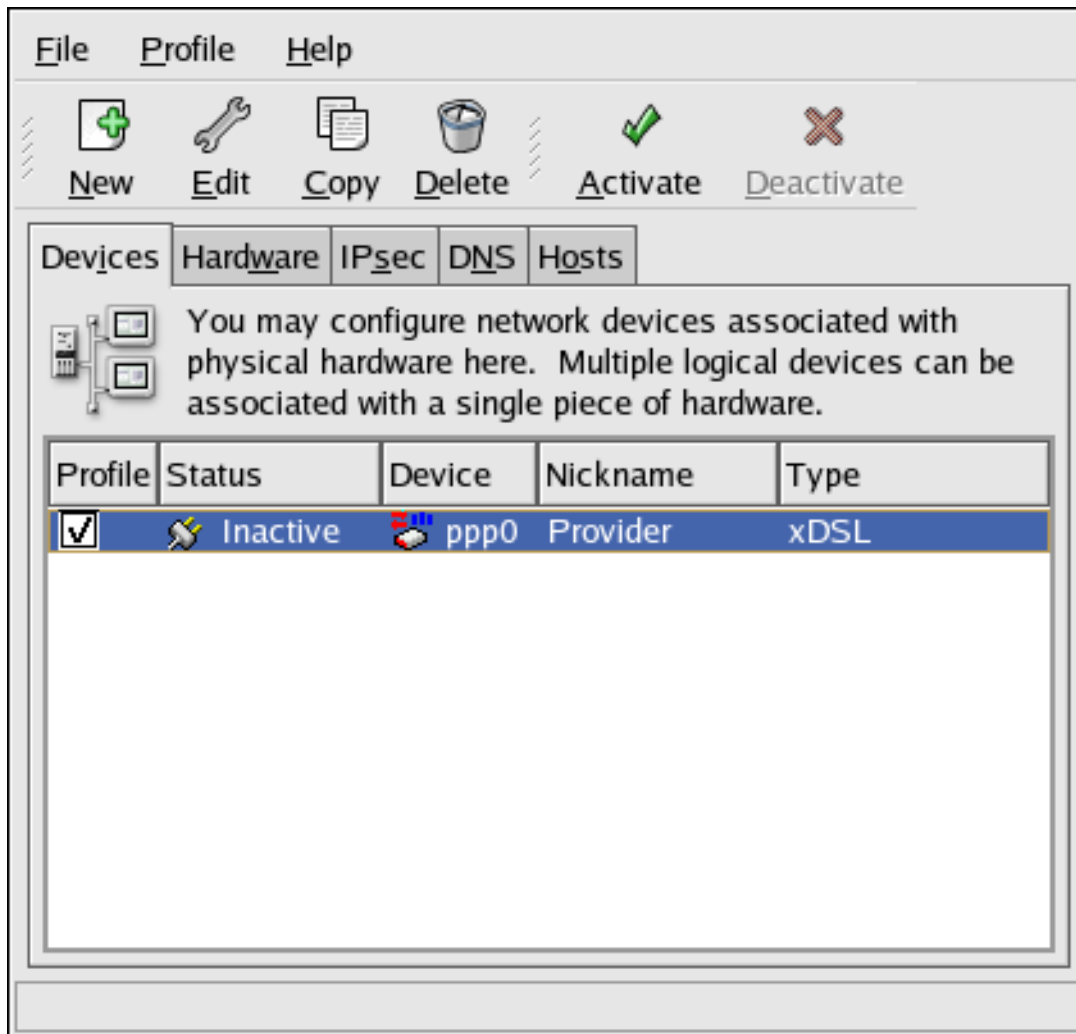
**Provider Name**、**Login Name**、および **Password** を入力します。**T-Online** アカウントがある場合は、デフォルトのウィンドウで **Login Name** および **Password** を入力せずに、**T-Online Account Setup** ボタンをクリックし、必要な情報を入力します。**進む** をクリックして続けます。

7.

**Create DSL Connection** ページで **Apply** をクリックします。

DSL コネクションの設定後、[図17.7 「モムデバイス」](#) に示されるようにデバイス一覧に表示されません。

図17.9 xDSL Device



[D]

必ず **File => Save** を選択して変更を保存します。

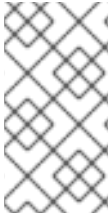
xDSL 接続を追加したら、デバイスリストからデバイスを選択して **編集** をクリックして設定を編集できます。たとえば、デバイスが追加されると、デフォルトでシステムの起動時には開始しないように設定されています。設定を編集してこの設定を変更します。

デバイスが追加されると、**Inactive** ステータスにあるように、すぐにアクティブになりません。デバイスを有効にするには、デバイス一覧から選択し、**Activate** ボタンをクリックします。コンピューターの起動時にシステムをアクティベートするように構成されている場合（デフォルト）、この手順を再度実行する必要があります。

## 17.6. 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は、すべてのコンピューターが円形のパターンで接続されるネットワークです。トークンまたは特別なネットワークパケットは、トークンリングを通過し、コンピューター

ターが情報を相互に送信できるようにします。



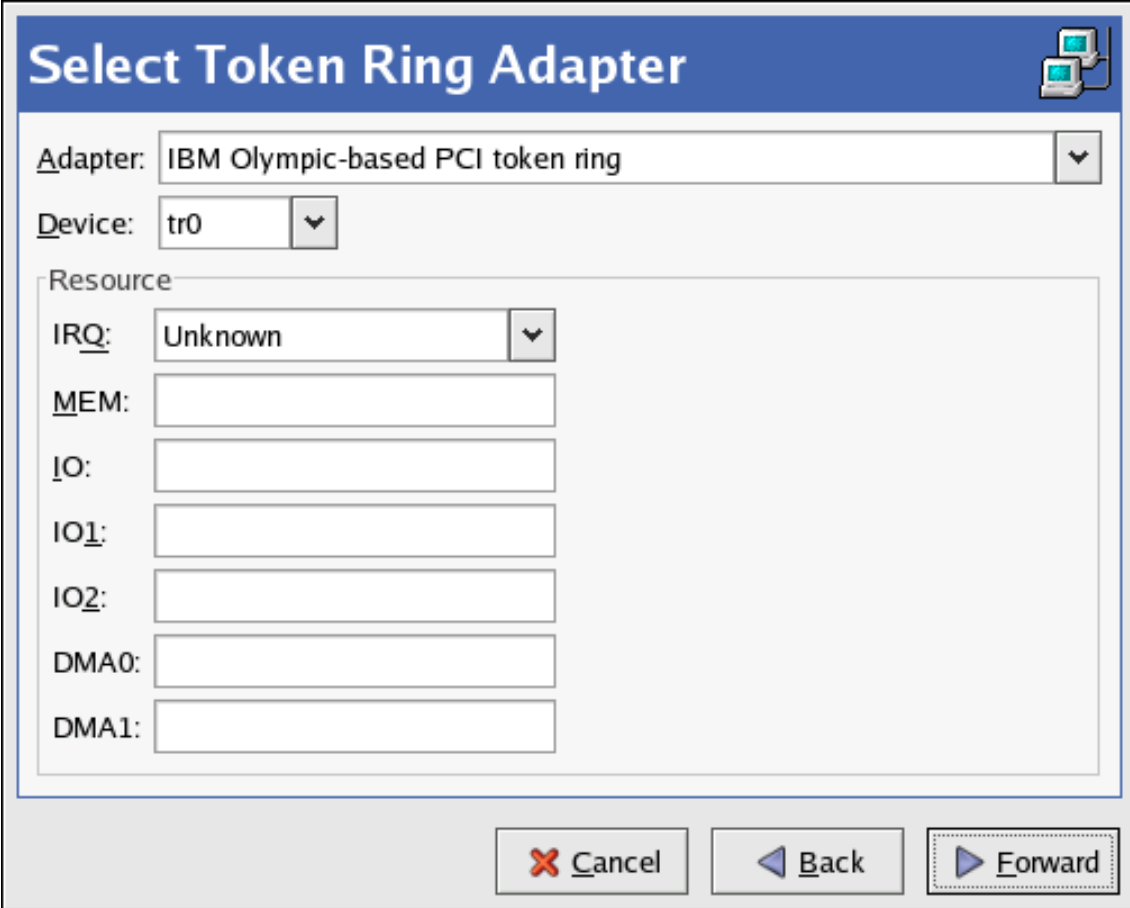
#### ヒント

Linux でのトークンリングの使用に関する詳細は、<http://www.linuxtr.net/> の『Linux Token Ring Project』の Web サイト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、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 **New** ボタンをクリックします。
3. **Device Type** 一覧から **Token Ring connection** を選択し、**forward** をクリックします。
4. トークンリングカードをハードウェア一覧にすでに追加している場合は、**Tokenring** カード一覧からトークンリングカードを選択します。それ以外の場合は、**Other Tokenring Card** を選択してハードウェアデバイスを追加します。
5. **Other Tokenring Card** を選択した場合、**図17.10 「トークンリング設定」** に示されるように **Select Token Ring Adapter** ウィンドウが表示されます。アダプターの製造元およびモデルを選択します。デバイス名を選択します。システムの最初のトークンリングカードの場合は、**tr0** を選択します。これが 2 番目のトークンリングカードの場合は、**tr1** (など) を選択します。また、**Network Administration Tool** を使用すると、ユーザーはアダプターのリソースを設定することもできます。**進む** をクリックして続けます。

図17.10 トークンリング設定



**Select Token Ring Adapter**

Adapter: IBM Olympic-based PCI token ring

Device: tr0

Resource

IRQ: Unknown

MEM:

IO:

IO1:

IO2:

DMA0:

DMA1:

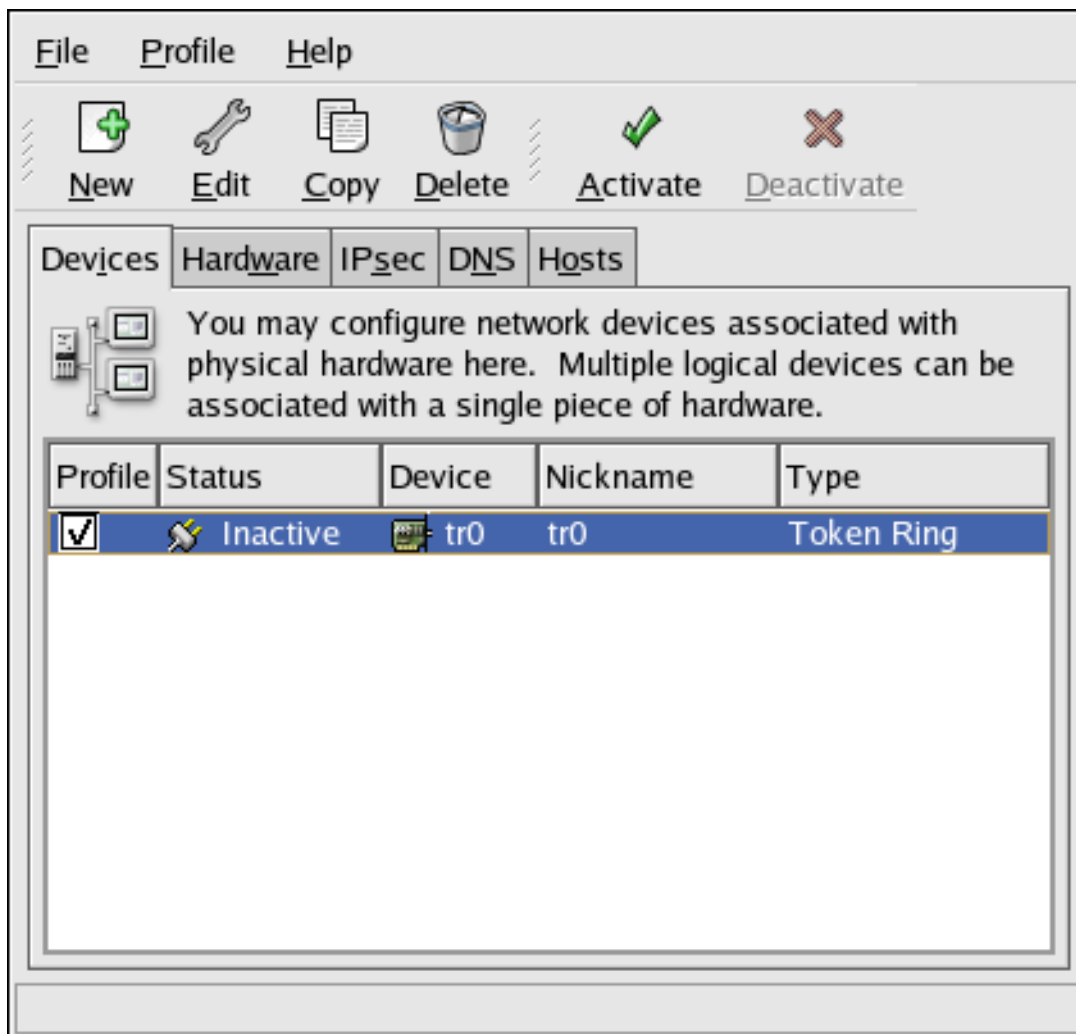
Cancel Back Forward

[D]

6. ネットワーク設定 ページで、**DHCP** と静的 IP アドレスのいずれかを選択します。デバイスのホスト名を指定できます。ネットワークの開始時にデバイスが動的 IP アドレスを受信した場合は、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. **Create Tokenring Device** ページで **Apply** をクリックします。

トークンリングデバイスを設定すると、図17.11 「トークンリングデバイス」 に示されるようにデバイス一覧に表示されます。

図17.11 トークンリングデバイス



[D]

必ず **File => Save** を選択して変更を保存します。

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** をクリックします。たとえば、システムの起動時にデバイスを起動するかどうかを設定できます。

デバイスが追加されると、**Inactive** ステータスにあるように、すぐにアクティブになりません。デバイスを有効にするには、デバイス一覧から選択し、**Activate** ボタンをクリックします。コンピューターの起動時にシステムをアクティベートするように構成されている場合（デフォルト）、この手順を再度実行する必要があります。

### 17.7. 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人気があります。設定はイーサネット設定と似ていますが、ワイヤレスデバイスの **SSID** やキーなどの設定を構成できます。



ワイヤレス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 **New** 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、**forward** をクリックします。
4. ワイヤレスネットワークインターフェースカードをハードウェア一覧にすでに追加している場合は、ワイヤレスカード一覧からこれを選択します。それ以外の場合は、**Other Wireless Card** を選択して、ハードウェアデバイスを追加します。

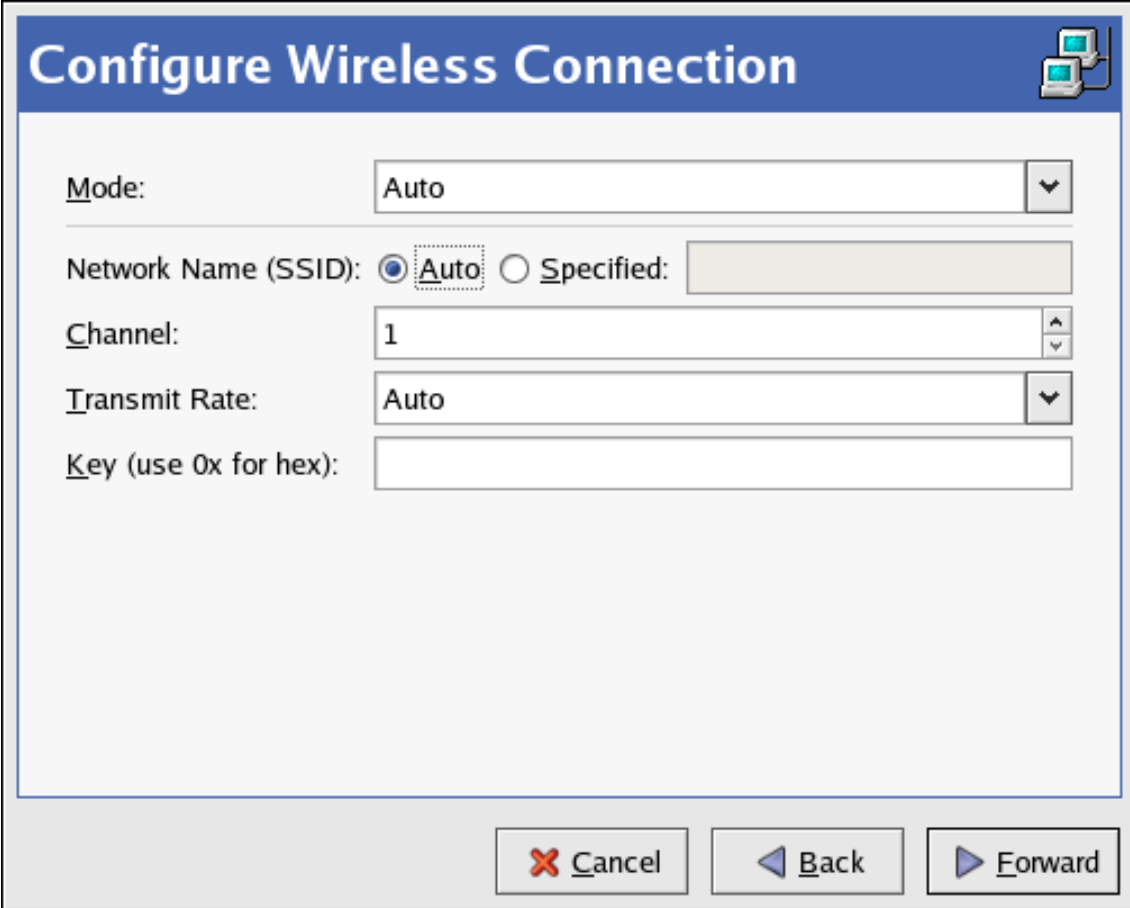


#### 備考

インストールプログラムは通常、対応しているワイヤレスイーサネットデバイスを検出し、その設定を求めるプロンプトを出します。インストール時に設定した場合には、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. **Other Wireless Card** を選択した場合は、**Select Ethernet Adapter** ウィンドウが表示されます。イーサネットカードとデバイスの製造元およびモデルを選択します。これがシステムの最初のイーサネットカードである場合は、**eth0** を選択します。これがシステムの2番目のイーサネットカードである場合は、**eth1** (など) を選択します。また、**Network Administration Tool** を使用すると、ユーザーは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設定できません。**進む** をクリックして続けます。
6. [図17.12 「ワイヤレス設定」](#) にあるように、**Configure Wireless Connection** ページで、ワイヤレスデバイスの設定を行います。

図17.12 ワイヤレス設定



**Configure Wireless Connection**

Mode: Auto

Network Name (SSID):  Auto  Specified:

Channel: 1

Transmit Rate: Auto

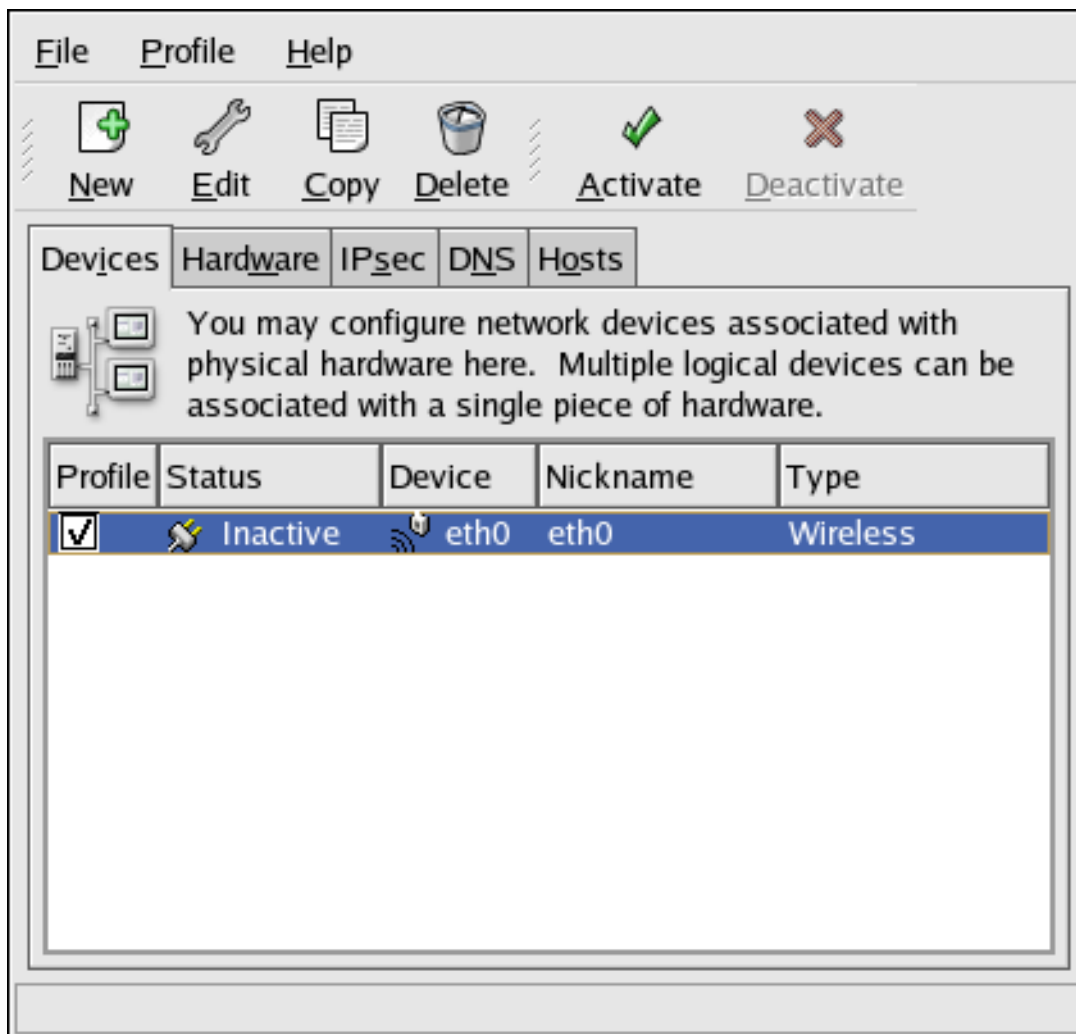
Key (use 0x for hex):

[D]

7. ネットワーク設定 ページで、**DHCP** と静的 IP アドレスのいずれかを選択します。デバイスのホスト名を指定できます。ネットワークの開始時にデバイスが動的 IP アドレスを受信した場合は、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。
8. **Create Wireless Device** ページで **Apply** をクリックします。

ワイヤレスデバイスを設定すると、[図17.13 「ワイヤレスデバイス」](#) に示されるようにデバイス一覧に表示されます。

図17.13 ワイヤレスデバイス



[D]

必ず **File => Save** を選択して変更を保存します。

ワイヤレス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** をクリックして設定を編集できます。たとえば、システムの起動時にデバイスをアクティベートするように設定できます。

デバイスが追加されると、**Inactive** ステータスにあるように、すぐにアクティブになりません。デバイスを有効にするには、デバイス一覧から選択し、**Activate** ボタンをクリックします。コンピューターの起動時にシステムをアクティベートするように構成されている場合（デフォルト）、この手順を再度実行する必要があります。

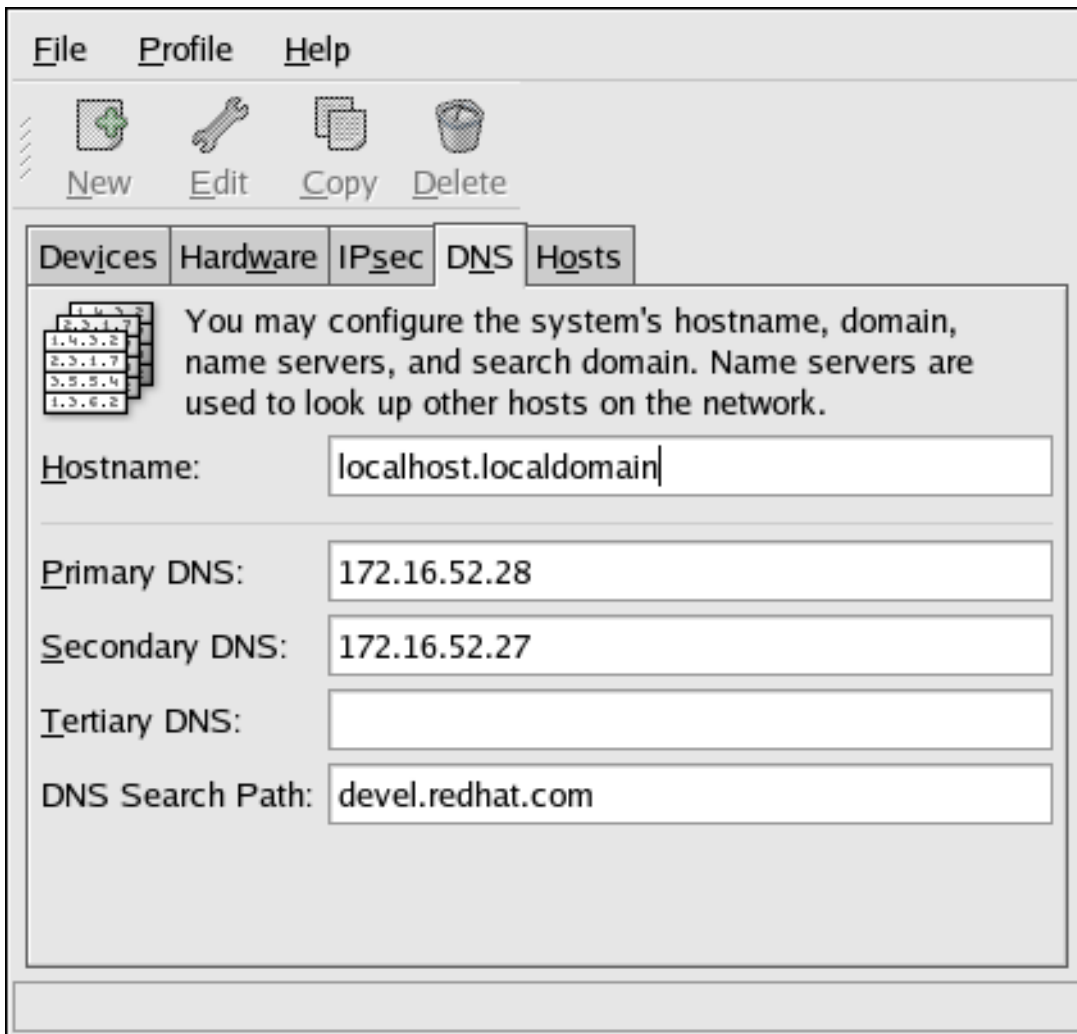
### 17.8. DNS 設定の管理

**DNS** タブを使用すると、システムのホスト名、ドメイン、ネームサーバー、および検索ドメインを設定できます。ネームサーバーは、ネットワーク上の他のホストを検索するために使用されます。

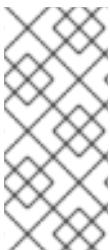
DNS サーバー名が DHCP または PPPoE (または ISP から取得) から取得した場合は、プライマリ、セカンダリ、または 3 つ目の DNS サーバーを追加しないでください。

ホスト名が DHCP または PPPoE (または ISP から取得) から動的に取得される場合、これを変更しないでください。

図17.14 DNS 設定



[D]



#### 備考

ネームサーバーのセクションは、システムをネームサーバーとして設定しません。代わりに、IP アドレスをホスト名に解決する際に使用するネームサーバーを設定し、その逆も同様です。

**WARNING**

ホスト名が変更され、ローカルホストで `system-config-network` が開始されている場合は、別の X11 アプリケーションを起動できない可能性があります。そのため、新しいデスクトップセッションに再度ログインする必要がある場合があります。

## 17.9. ホストの管理

ホストタブでは、`/etc/hosts` ファイルにホストを追加、編集、または削除できます。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ます。

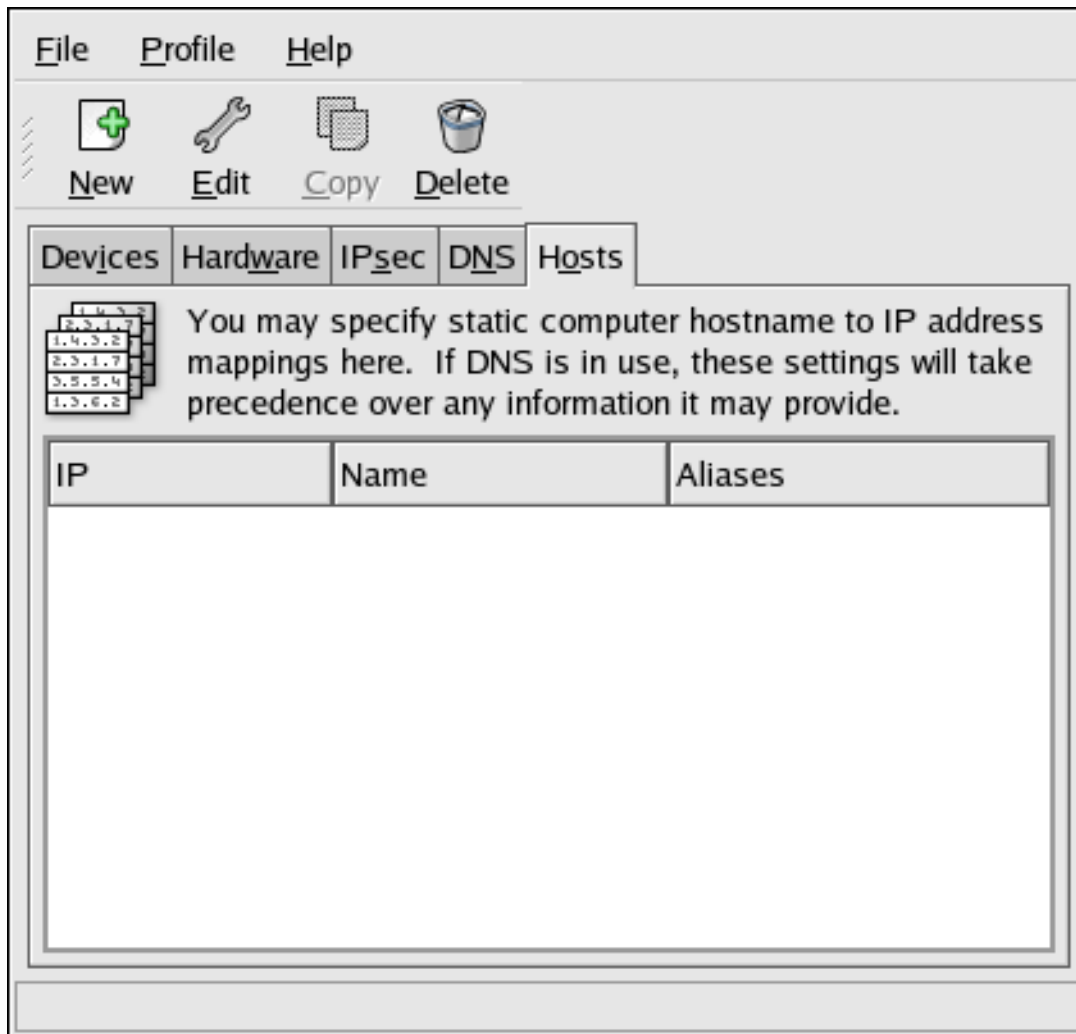
システムが IP アドレスにホスト名を解決したり、IP アドレスのホスト名を判別したりしようとする時、ネームサーバーを使用する前に `/etc/hosts` ファイルを参照します（デフォルトの Red Hat Enterprise Linux 設定を使用している場合）。`/etc/hosts` ファイルに IP アドレスが記載されている場合は、ネームサーバーは使用されません。ネットワークに IP アドレスが DNS に記載されていないコンピュータが含まれている場合は、`/etc/hosts` ファイルに追加することが推奨されます。

`/etc/hosts` ファイルにエントリーを追加するには、Hosts タブに移動し、ツールバーの New ボタンをクリックして要求された情報を指定して、OK をクリックします。File => Save を選択するか、Ctrl+S を押して、`/etc/hosts` ファイルへの変更を保存します。ファイルの現行バージョンは、アドレスが解決されるたびに参照されているため、ネットワークサービスまたはネットワークサービスを再起動する必要はありません。

**WARNING**

`localhost` エントリー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や、ネットワーク接続が常に実行している場合でも、一部のプログラムは `localhost` ループバックインターフェースを介してシステムに接続する必要があります。

図17.15 ホストの設定



[D]



### ヒント

ルックアップ順序を変更するには、`/etc/host.conf` ファイルを編集します。行の順序  
 ホストでは、`bind` は `/etc/hosts` がネームサーバーよりも優先されます。行を `order bind`  
 に変更すると、ホストは最初にネームサーバーを使用してホスト名と IP アドレスを解決  
 するようにシステムを設定します。IP アドレスをネームサーバーで解決できない場合、  
 システムは `/etc/hosts` ファイルで IP アドレスを検索します。

## 17.10. プロファイルの使用

物理ハードウェアデバイスごとに、複数の論理ネットワークデバイスを作成できます。たとえば、  
 システムに1つのイーサネットカードがある場合、別のニックネームと設定オプションを持つ論理ネッ  
 トワークデバイスを作成できます。これらはすべて `eth0` にとくに関連付けられます。

論理ネットワークデバイスは、デバイスのエイリアスとは異なります。同じ物理デバイスに関連付  
 けられた論理ネットワークデバイスは、異なるプロファイルに存在し、同時にアクティブにすることは  
 できません。デバイスエイリアスは同じ物理ハードウェアデバイスに関連付けられますが、同じ物理

ハードウェアに関連付けられたデバイスエイリアスを同時にアクティブにできます。デバイスのエイリアスの作成に関する詳細は、「[デバイスエイリアス](#)」を参照してください。

プロファイルを使用すると、異なるネットワーク用に複数の設定セットを作成することができます。設定セットには、論理デバイスとホストと DNS 設定を含めることができます。プロファイルの設定後に、**Network Administration Tool** を使用して、プロファイル間の切り替えを行うことができます。

デフォルトでは、**Common** という名前のプロファイルが1つあります。新規プロファイルを作成するには、プルダウンメニューから **Profile => New** を選択して、プロファイルに一意の名前を入力します。

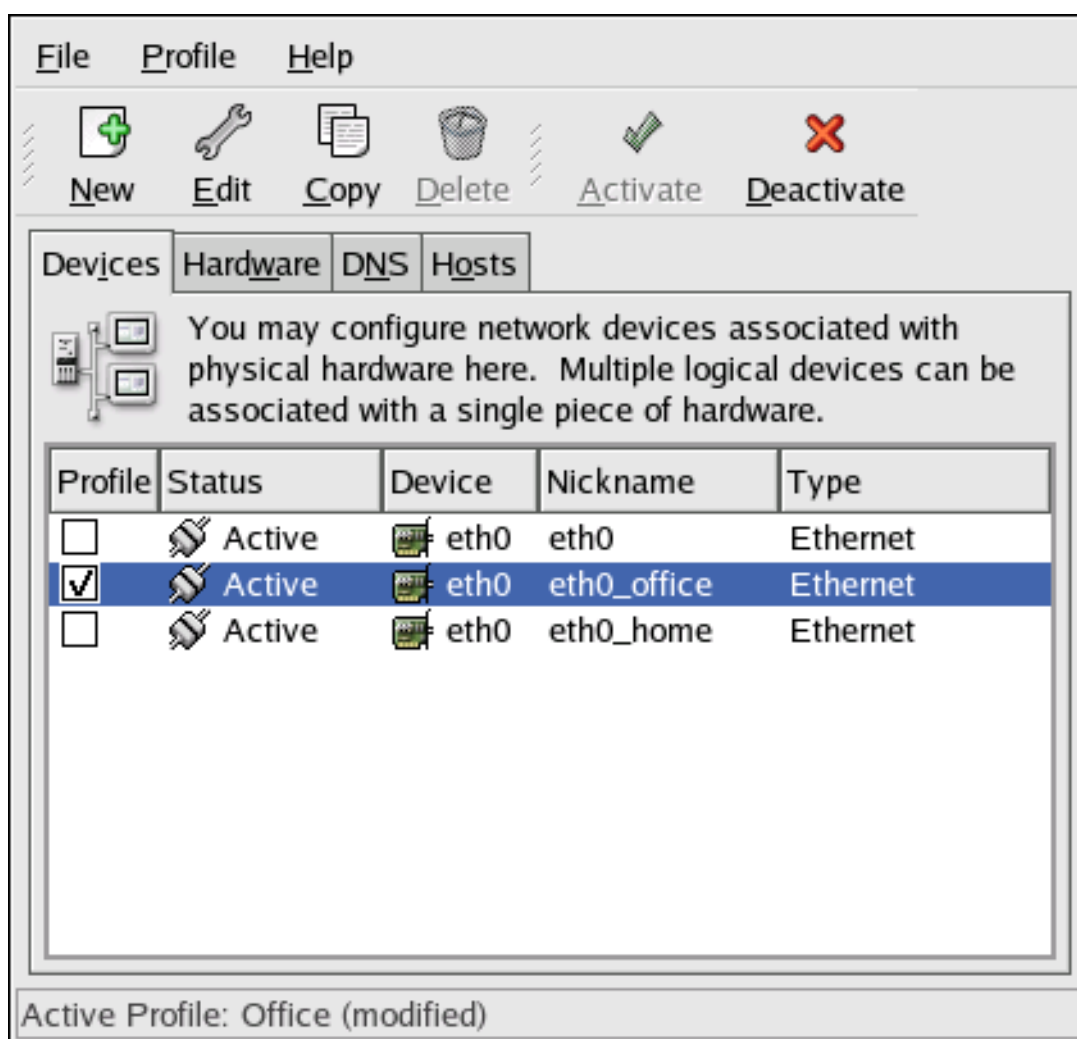
これで、メインのウィンドウの下部にあるステータスバーで示される新しいプロファイルを変更します。

一覧にある既存のデバイスをクリックし、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。New ボタンを使用すると、ネットワークエイリアスが作成されますが、これは正しくありません。論理デバイスのプロパティを変更するには、一覧から選択し、編集 をクリックします。たとえば、ニックネームを **eth0\_office** などのより分かりやすい名前に変更して、より簡単に認識できるようにすることができます。

デバイスの一覧には、Profile とラベルが付いたチェックボックスがあります。各プロファイルについて、デバイスの確認または確認解除を行うことができます。現在選択されているプロファイルには、チェックしたデバイスのみが含まれます。たとえば、**eth0\_office** という名前のプロファイルに **Office** という名前の論理デバイスを作成し、プロファイルが選択されている場合は論理デバイスをアクティベートする場合は、**eth0** デバイスの選択を解除して、**eth0\_office** デバイスを確認します。

たとえば、[図17.16 「オフィスプロファイル」](#) は、論理デバイス **eth0\_office** を持つ **Office** というプロファイルを表示します。DHCP を使用して最初のイーサネットカードをアクティベートするように設定されています。

図17.16 オフィスプロファイル

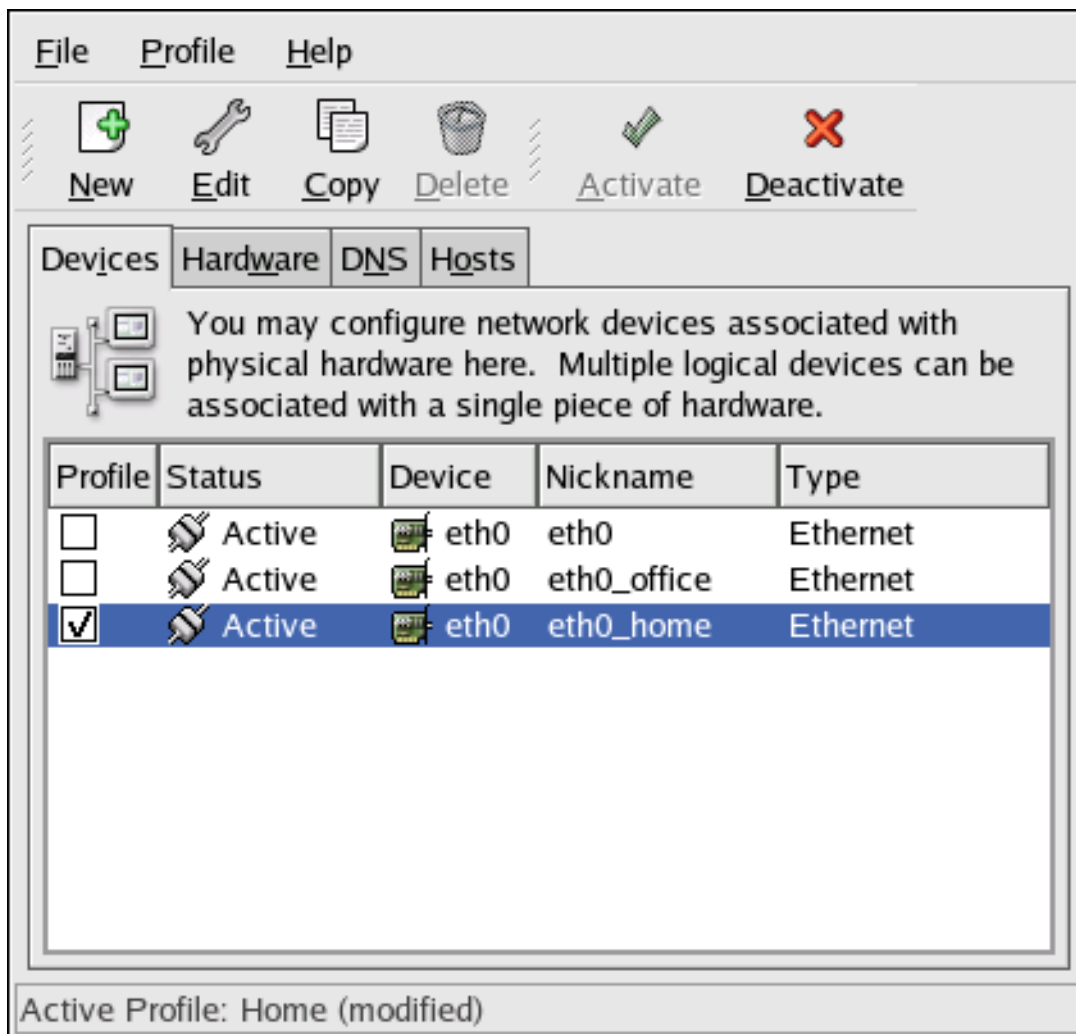


[D]

図17.17 「Home Profile」にあるように Home プロファイルは、eth0 に関連付けられた eth0\_home 論理デバイスをアクティブにします。



図17.17 Home Profile



[D]

また、Office プロファイルでのみアクティブにするように eth0 を設定し、Home プロファイルでのみ PP(modem)デバイスを有効にすることもできます。別の例として、Common プロファイルが eth0 をアクティブにし、Away プロファイルは、移動中に PPP デバイスをアクティベートします。

起動時にプロファイルをアクティベートするには、ブートローダー設定ファイルを変更して `netprofile= <profilename>` オプションを含めます。たとえば、システムが GRUB をブートローダーとして使用し、`/boot/grub/grub.conf` には以下が含まれます。

```
title Red Hat Enterprise Linux (2.6.9-5.EL)
  root (hd0,0)
  kernel /vmlinuz-2.6.9-5.EL ro root=/dev/VolGroup00/LogVol00 rhgb quiet
  initrd /initrd-2.6.9-5.EL.img
```

それを以下のように変更します（`<profilename>` は、起動時にアクティベートされるプロファイルの名前です）。

```

title Red Hat Enterprise Linux (2.6.9-5.EL)
  root (hd0,0)
  kernel /vmlinuz-2.6.9-5.EL ro root=/dev/VolGroup00/LogVol00 \
  netprofile=<profilename> \ rhgb quiet
  initrd /initrd-2.6.9-5.EL.img

```

システムの起動後にプロファイルを切り替えるには、**Applications**（パネルのメインメニュー）⇒ **System Tools** ⇒ **Network Device Control**（またはコマンド `system-control-network`）に移動してプロファイルを選択し、アクティベートします。activate profile セクションは、デフォルトの **Common** インターフェースが存在する場合に **Network Device Control** インターフェースにのみ表示されます。

または、以下のコマンドを実行してプロファイルを有効にします（`<profilename>` をプロファイルの名前に置き換えます）。

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

### 17.11. デバイスイエリアス

デバイスエイリアスは、同じ物理ハードウェアに関連付けられる仮想デバイスですが、同時にアクティブにして異なる IP アドレスを指定することができます。通常、デバイス名の後にコロンと数字（例：eth0:1）が続きます。これらは、1つのネットワークカードしか持たないシステムに複数の IP アドレスがある場合に便利です。

eth0 などのイーサネットデバイスを設定したら（例：eth0 -静的 IP アドレス（DHCP がエイリアスでは機能しません））、**Device** タブで、**New** をクリックします。エイリアスで設定するイーサネットカードを選択し、エイリアスの静的 IP アドレスを設定し、**Apply** をクリックして作成します。イーサネットカード用にデバイスが存在するため、作成したデバイスは eth0:1 などのエイリアスになります。



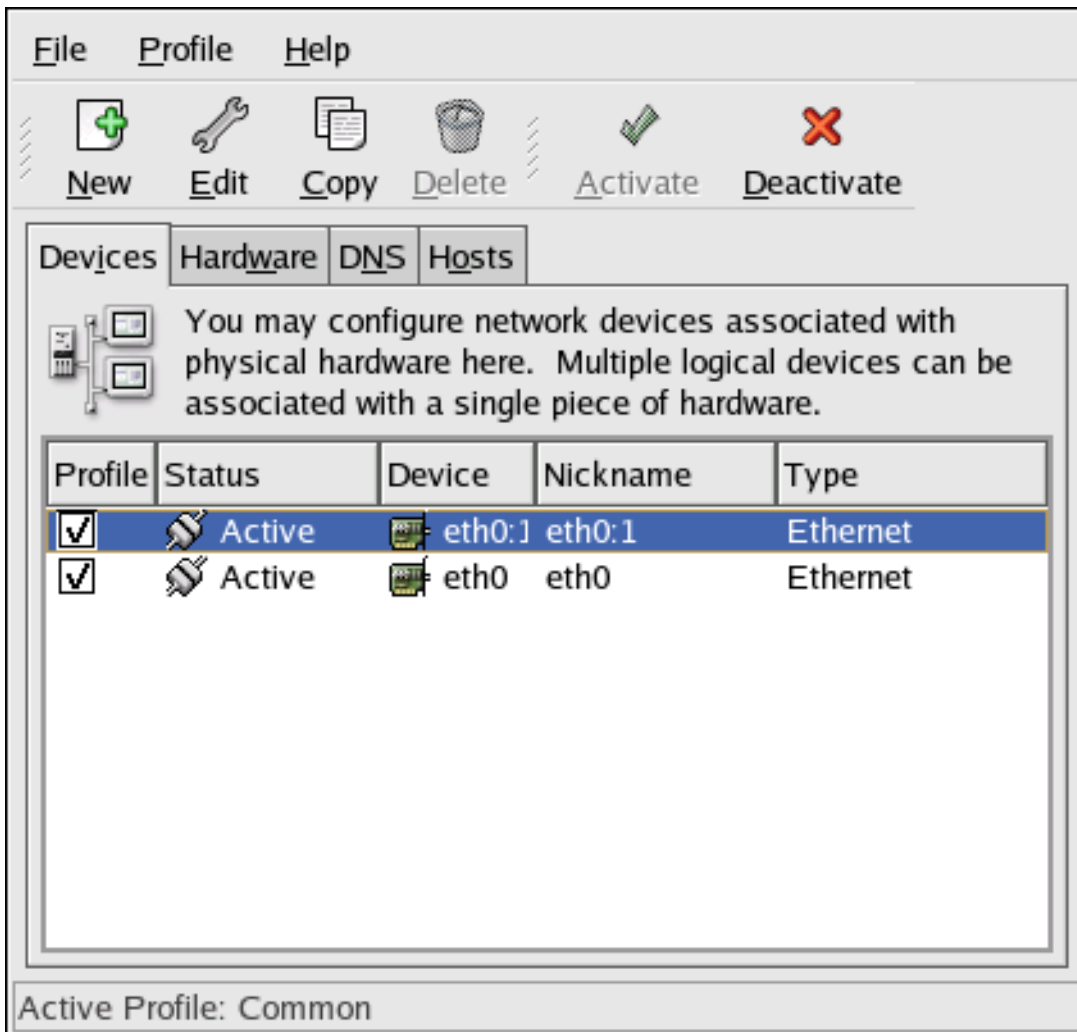
#### WARNING

エイリアスを持つようにイーサネットデバイスを設定する場合は、デバイスやエイリアスを DHCP を使用するように設定することはできません。IP アドレスは手動で設定する必要があります。

図17.18「ネットワークデバイスのエイリアスの例」は、eth0 デバイスのエイリアス1つの例を示しています。eth0 :1 デバイス - eth0 の最初のエイリアスに注目してください。eth0 の2つ目のエイリアスにはデバイス名 eth0:2 があります。システムの起動時にアクティブにするかどうかやエイリア

ス番号など、デバイスエイリアスの設定を変更するには、一覧から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17.18 ネットワークデバイスのエイリアスの例



[D]

エイリアスを選択し、**Activate** ボタンをクリックしてエイリアスを有効にします。複数のプロファイルを設定している場合は、それを含めるプロファイルを選択します。

エイリアスがアクティブであることを確認するには、コマンド `/sbin/ifconfig` を使用します。出力には、デバイスと、異なる IP アドレスを持つデバイスエイリアスが表示されます。

```
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)
```

## 17.12. ネットワーク設定の保存および復元

**Network Administration Tool** のコマンドラインバージョンを使用すると、システムのネットワーク設定をファイルに保存できます。このファイルを使用して、Red Hat Enterprise Linux システムにネットワーク設定を復元できます。

この機能は、自動バックアップスクリプトの一部として使用したり、アップグレードまたは再インストールの前に設定を保存したり、設定を別の Red Hat Enterprise Linux システムにコピーすることもできます。

システムのネットワーク設定を `/tmp/network-config` ファイルに保存またはエクスポートするには、`root` で以下のコマンドを実行します。

```
system-config-network-cmd -e > /tmp/network-config
```

直前のコマンドで作成したファイルからネットワーク設定を復元またはインポートするには、`root` で以下のコマンドを実行します。

```
system-config-network-cmd -i -c -f /tmp/network-config
```

`-i` オプションは、データをインポートすることを意味します。`-c` オプションはインポート前に既存の設定を消去することを意味します。`-f` オプションはインポートするファイルは以下のようになりません。

## 第18章 ファイアウォール

情報セキュリティは、一般的に製品ではなくプロセスとして考慮されます。ただし、標準的なセキュリティ実装は、通常、アクセス権限を制御し、許可、識別可能な、およびトレース可能なユーザーにネットワークリソースを制限するための専用のメカニズムを使用します。Red Hat Enterprise Linux には、ネットワークレベルのアクセス制御問題に関する管理者およびセキュリティエンジニアを支援するツールが複数含まれています。

ファイアウォールは、ネットワークセキュリティ実装の中核となるコンポーネントの1つです。複数のベンダーの市場ファイアウォールソリューションは、すべてのレベルの市場に分類されています。つまり、1つのPCをデータセンターソリューションに対して保護し、重要なエンタープライズ情報を保護します。ファイアウォールは、Cisco、Nokia、Sonicwall によるファイアウォールアプライアンスなどのスタンドアロンのハードウェアソリューションです。Checkpoint、McAfee、IaaS などのベンダーは、ホームおよびビジネス市場向けのプロプライエタリーソフトウェアファイアウォールソリューションも開発しました。

ハードウェアおよびソフトウェアファイアウォールの違い以外に、ファイアウォールが互いにソリューションを分離する方法にも違いがあります。表18.1「ファイアウォールの種類」ファイアウォールの一般的な3つのタイプと、その仕組みを説明します。

表18.1 ファイアウォールの種類

メ ソッ ド	Description	メリット	デメリット

メ ソ ッ ド	Description	メリット	デメリット
NAT	<p><b>Network Address Translation (NAT)</b>は、プライベート IP サブネットワークを一つまたは一つまたは小さなプールに配置し、複数のソースではなく、一つのソースにすべての要求をマスカレードします。Linux カーネルには、<b>getfacl</b> カーネルサブシステムを介した NAT 機能がビルトインされています。</p>	<p>LAN のマシンに対して透過的に設定することができます。</p> <p>一つ以上の外部 IP アドレスの背後で多数のマシンおよびサービスを保護することで管理作業が容易になります。</p> <p>NAT ファイアウォール/ゲートウェイでポートを開くと閉じることで、LAN へのユーザーアクセスの制限を設定できます。</p>	<p>ユーザーがファイアウォール外のサービスに接続すると、悪意のあるアクティビティーが阻止できない</p>

メソッド	Description	メリット	デメリット
パケットフィルター	<p>パケットフィルタリングのファイアウォールは、LANを通過する各データパケットを読み取ります。ヘッダー情報でパケットを読み取りおよび処理し、ファイアウォール管理者が実装するプログラム可能なルールセットに基づいてパケットをフィルターできます。Linuxカーネルには、<b>getfacl</b> カーネルサブシステムを介して、パケットフィルタリング機能が組み込まれています。</p>	<p><b>iptables</b> フロントエンドユーティリティーを使用したカスタマイズ可能</p> <p>すべてのネットワークアクティビティーはアプリケーションレベルではなくルーターレベルでフィルタリングされるため、クライアント側でのカスタマイズは必要ありません。</p> <p>パケットがプロキシを介して送信されないため、クライアントからリモートホストへ直接接続することでネットワークのパフォーマンスが速くなります。</p>	<p>プロキシファイアウォールなど、コンテンツの packets をフィルターできない</p> <p><b>pidgin</b> はプロトコル層でパケットを処理しますが、アプリケーション層でパケットをフィルターできない</p> <p><b>IP</b> マスカレードまたはローカルサブネットワークと組み合わせる場合など、パケットのフィルタリングルールの確立が困難になる場合があります。</p>

メソッド	Description	メリット	デメリット
Proxy	<p>プロキシファイアウォールは、LAN クライアントからプロキシマシンに特定のプロトコルやタイプのリクエストをすべてフィルタリングし、ローカルクライアントの代わりにインターネットにそれらの要求を行います。プロキシマシンは、悪意のあるリモートユーザーと内部ネットワーククライアントマシンとの間のバッファとして機能します。</p>	<p>管理者は、LAN 外でのアプリケーションとプロトコルが機能するかを制御することができます。</p> <p>一部のプロキシサーバーは、インターネット接続を使用して要求する必要なく、頻繁にアクセスされるデータをキャッシュできます。これは、帯域幅の消費を減らすのに役立ちます。</p> <p>pidgin プロキシサービスは、厳密にログに記録および監視でき、ネットワーク上のリソース使用率をより詳細に制御できます。</p>	<p>多くの場合、プロキシはアプリケーション固有 (HTTP、Telnet など)、またはプロトコルの制限付きサービス (ほとんどのプロキシは TCP 接続済みサービスでのみ機能します) です。</p> <p>アプリケーションサーバーは、別の形式のネットワークセキュリティを使用する必要があります。</p> <p>すべてのリクエストと送信がクライアントからリモートサービスに直接渡されるのではなく、1つのソースを介して渡されるので、これらのプロキシはネットワークのボトルネックになることがあります。</p>

### 18.1. ALLINONES および IPTABLES

Linux カーネルは、`CtrlC` と呼ばれる強力なネットワークサブシステムを特長としています。ステートフルまたはステートレスのパケットフィルタリングと、NAT および IP マスカレードサービスを提供します。また、高度なルーティングおよび接続状態管理のための IP ヘッダー情報を `man` する機能があります。`allfacel` は、`iptables` ツールを使用して制御されます。



### 18.1.1. iptables の概要

**iptables** 管理ツール (**predecessor**、**ipchains**) の構文に似たコマンドラインツールである **iptables** 管理ツールを使用して、電力と柔軟性が実装されます。

ただし、同様の構文は同様の実装ではありません。**ipchains** には、ソースパスのフィルタリング、宛先パスのフィルタリング、および送信元と宛先接続ポートの両方をフィルタリングするためのルールセットが必要です。

対照的に、**iptables** は、ネットワーク接続、検査、および処理を強化するために、**getfacl** サブシステムを使用してネットワーク接続、検査、および処理を強化します。**iptables** は、1つのコマンドラインインターフェースで、高度なロギング、事前およびルーティング後のアクション、ネットワークアドレス変換、およびポート転送を特長としています。

このセクションでは、**iptables** の概要を説明します。

## 18.2. 基本的なファイアウォール設定

構築におけるファイアウォールとして、コンピューターファイアウォールは悪意のあるソフトウェアがコンピューターに分散されないようにします。また、承認されていないユーザーがコンピューターにアクセスできないようにするのに役立ちます。

デフォルトの **Red Hat Enterprise Linux** インストールでは、コンピューターまたはネットワークと信頼できないネットワーク (インターネットなど) 間でファイアウォールが存在します。お使いのコンピューターのリモートユーザーがアクセス可能なサービスを決定します。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ーが大幅に向上する可能性があります。インターネット接続のある **Red Hat Enterprise Linux** システムのファイアウォールを設定することが推奨されます。

### 18.2.1. Security Level Configuration Tool

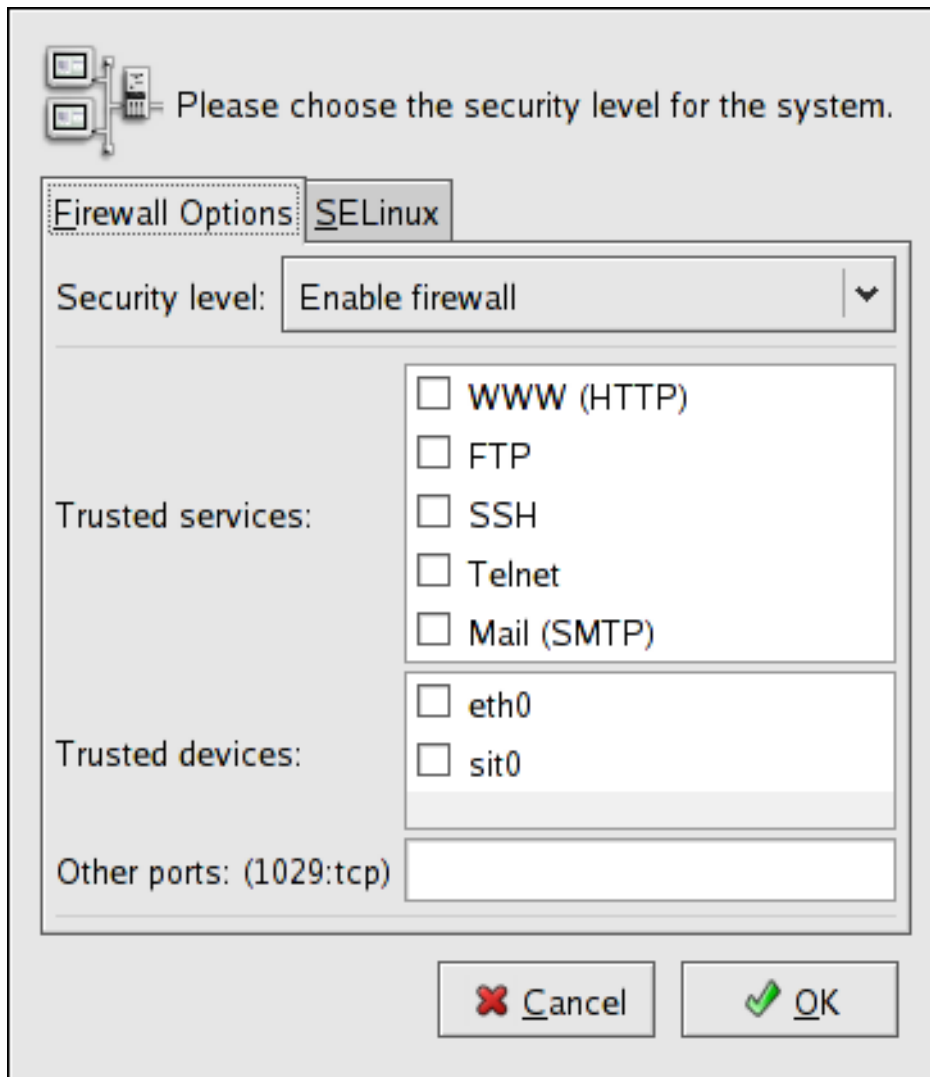
**Red Hat Enterprise Linux** インストールの **Firewall Configuration** 画面では、基本的なファイアウォールを有効にし、特定のデバイス、受信サービス、およびポートを許可するオプションを選択できます。

インストール後に、**Security Level Configuration Tool** を使用してこの設定を変更できます。

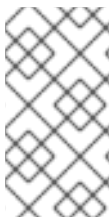
このアプリケーションを起動するには、次のコマンドを使用します。

```
[root@myServer ~] # system-config-selinux
```

図18.1 Security Level Configuration Tool



[D]



備考

**Security Level Configuration Tool** は基本的なファイアウォールのみを設定します。

### 18.2.2. ファイアウォールの有効化および無効化

ファイアウォールに以下のいずれかのオプションを選択します。

- disabled:** ファイアウォールを無効にすると、システムに完全なアクセスが可能になり、セキュリティーチェックは行われません。これは、信頼できるネットワーク（インターネット

ではない) で実行している場合や、`iptables` コマンドラインツールを使用してカスタムファイアウォールを設定する必要がある場合にのみ選択する必要があります。



#### WARNING

ファイアウォール設定とカスタマイズされたファイアウォールルールは、`/etc/sysconfig/iptables` ファイルに保存されます。**Disabled** を選択し、**OK** をクリックすると、これらの設定およびファイアウォールルールが失われます。

- **enabled:** このオプションは、DNS 応答や DHCP 要求など、送信要求に応答しない受信接続を拒否するように設定します。このマシンで実行中のサービスへのアクセスが必要な場合は、特定サービスに対してファイアウォールの通過許可を選択できます。

システムをインターネットに接続しているが、サーバーを実行する予定がない場合は、最も安全な選択肢になります。

### 18.2.3. 信頼できるサービス

**Trusted services** リストでオプションを有効にすると、指定したサービスがファイアウォールを通過できるようになります。

#### WWW (HTTP)

HTTP プロトコルは、Apache (およびその他の Web サーバー) が Web ページを提供するために使用されます。Web サーバーを公開されている場合は、このチェックボックスを選択します。このオプションは、ローカルでページを表示したり、Web ページを開発する場合には必要ありません。このサービスは、`httpd` パッケージをインストールする必要があります。

WWW(HTTP) を有効にしても、HTTPS (HTTP の SSL バージョン) のポートが開かない。このサービスが必要な場合は、**Secure WWW(HTTPS)** チェックボックスを選択します。

#### FTP

FTP プロトコルは、ネットワーク上のマシン間でファイルを転送するために使用されます。FTP サーバーを一般に公開されている場合は、このチェックボックスを選択します。このサービス

は、**vsftpd** パッケージをインストールする必要があります。

## SSH

**Secure Shell(SSH)**は、リモートマシンでコマンドにログインして実行するツールセットです。**ssh** 経由でマシンにリモートアクセスできるようにするには、このチェックボックスを選択します。このサービスは、**openssh-server** パッケージをインストールする必要があります。

## 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。**telnet** 通信は暗号化されず、ネットワークスヌーピングからセキュリティを提供しません。着信 **Telnet** アクセスを許可することは推奨されません。**telnet** 経由でマシンにリモートアクセスできるようにするには、このチェックボックスを選択します。このサービスは、**telnet-server** パッケージをインストールする必要があります。

## mail(SMTP)

**SMTP** は、リモートホストがマシンに直接接続してメールを配信できるようにするプロトコルです。**POP3** または **IMAP** を使用して **ISP** のサーバーからメールを収集する場合や、**fetchmail** などのツールを使用する場合は、このサービスを有効にする必要はありません。マシンにメールを配信できるようにするには、このチェックボックスを選択します。**SMTP** サーバーが適切に設定されていないと、リモートマシンがサーバーを使用してスパムを送信する可能性があることに注意してください。

## NFS4

**Network File System(NFS)**は、\***NIX** システムで一般的に使用されるファイル共有プロトコルです。このプロトコルのバージョン 4 は、先行するものよりも安全です。システムのファイルまたはディレクトリーを他のネットワークユーザーと共有する場合は、このチェックボックスを選択します。

## Samba

**Samba** は、**Microsoft** のプロプライエタリー **SMB** ネットワークプロトコルの実装です。**Microsoft Windows** マシンを使用して、ファイル、ディレクトリー、またはローカルで接続されたプリンターを共有する必要がある場合は、このチェックボックスを選択します。

### 18.2.4. 他のポート

Security Level Configuration Tool には、`iptables` によって信頼されるカスタム IP ポートを指定するその他のポートセクションが含まれます。たとえば、IRC およびインターネット印刷プロトコル (IPP) がファイアウォールを通過するのを許可するには、他のポート セクションに以下を追加します。

```
194:tcp,631:tcp
```

### 18.2.5. 設定の保存

OK をクリックして変更を保存し、ファイアウォールを有効または無効にします。Enable firewall が選択されている場合、選択されたオプションは `iptables` コマンドに変換され、`/etc/sysconfig/iptables` ファイルに書き込まれます。`iptables` サービスも起動し、選択したオプションの保存直後にファイアウォールがアクティベートされるようにします。ファイアウォールを無効にすると、`/etc/sysconfig/iptables` ファイルが削除され、`iptables` サービスはすぐに停止します。

選択したオプションも `/etc/sysconfig/system-config-selinux` ファイルに書き込まれます。これにより、アプリケーションの次回起動時に設定が復元できます。このファイルは手動で編集しないでください。

ファイアウォールがすぐにアクティブであっても、`iptables` サービスは起動時に自動的に起動するように設定されていません。詳細は、[「IPTables サービスのアクティブ化」](#) を参照してください。

### 18.2.6. IPTables サービスのアクティブ化

ファイアウォールルールは、`iptables` サービスが実行されている場合にのみアクティブになります。サービスを手動で起動するには、以下のコマンドを使用します。

```
[root@myServer ~] # service iptables restart
```

システムの起動時に `iptables` が起動していることを確認するには、以下のコマンドを使用します。

```
[root@myServer ~] # chkconfig --level 345 iptables on
```

`ipchains` サービスは、Red Hat Enterprise Linux に含まれていません。ただし、`ipchains` がインストールされている場合は（アップグレードが実行され、システムに `ipchains` 以前がインストールされている場合など）、`ipchains` サービスおよび `iptables` サービスを同時にアクティブにすることはできません。`ipchains` サービスが無効になり、システムの起動時に起動しないようにするには、以下の 2 つのコマンドを使用します。

```
[root@myServer ~] # service ipchains stop
[root@myServer ~] # chkconfig --level 345 ipchains off
```

### 18.3. IPTABLES の使用

`iptables` を使用する最初の手順は、`iptables` サービスを起動することです。以下のコマンドを使用して `iptables` サービスを起動します。

```
[root@myServer ~] # service iptables start
```

#### 備考

`iptables` サービスのみを使用する場合には、`ip6tables` サービスをオフにすることができます。`ip6tables` サービスを非アクティブにした場合は、IPv6 ネットワークを必ず非アクティブにしてください。一致するファイアウォールなしでネットワークデバイスをアクティブな状態にしないでください。

システムの起動時に `iptables` を強制的に起動するには、次のコマンドを使用します。

```
[root@myServer ~] # chkconfig --level 345 iptables on
```

これにより、システムがランレベル 3、4、または 5 で起動されるたびに `iptables` を強制的に起動します。

#### 18.3.1. iptables コマンド構文

以下の `iptables` コマンドの例は、基本的なコマンド構文を示しています。

```
[root@myServer ~] # iptables -A <chain> -j <target>
```

`-A` オプションは、ルールを `<chain>` に追加するように指定します。各チェーンは 1 つ以上のルールで構成されており、ルール セットとも呼ばれます。

3 つの組み込みチェーンは `INPUT`、`OUTPUT`、および `FORWARD` です。これらのチェーンは永続的であるため、削除できません。チェーンは、パケットが操作されるポイントを指定します。

`-j <target>` オプションは、ルールのターゲットを指定します。ビルトインターゲットの例は `ACCEPT`、`DROP`、および `REJECT` です。

利用可能なチェーン、オプション、およびターゲットの詳細は、`iptables` の `man` ページを参照してください。

### 18.3.2. 基本的なファイアウォールポリシー

基本的なファイアウォールポリシーを確立することで、より詳細にわたるユーザー定義ルールを構築する基盤が作成されます。

各 `iptables` チェーンはデフォルトポリシーと、ファイアウォールの全体的なルールセットを定義するデフォルトポリシーと組み合わせるゼロ以上のルールで構成されています。

チェーンのデフォルトポリシーは `DROP` または `ACCEPT` のいずれかになります。セキュリティーが付与された管理者は、通常 `DROP` のデフォルトポリシーを実装し、ケースごとに特定の packets のみを許可します。たとえば、以下のポリシーは、ネットワークゲートウェイの着信 packet および送信 packet をすべてブロックします。

```
[root@myServer ~] # iptables -P INPUT DROP
[root@myServer ~] # iptables -P OUTPUT DROP
```

また、転送された packet (ファイアウォールから宛先ノードへルーティングされるネットワークトラフィック) も拒否され、内部クライアントがインターネットへの誤った公開を制限することが推奨されます。これを行うには、以下のルールを使用します。

```
[root@myServer ~] # iptables -P FORWARD DROP
```

各チェーンにデフォルトのポリシーを確立したら、特定のネットワークおよびセキュリティー要件に関する追加のルールを作成して保存することができます。

以下のセクションでは、`iptables` ルールを保存する方法と、`iptables` ファイアウォールを構築するのに役立つルールの一部を説明します。

### 18.3.3. IPTables ルールの保存および復元

`iptables` への変更は推移的です。システムが再起動した場合や、`iptables` サービスが再起動した場合、ルールは自動的にフラッシュされ、リセットされます。`iptables` サービスの起動時に読み込まれるようにルールを保存するには、以下のコマンドを使用します。

```
[root@myServer ~] # service iptables save
```

ルールは `/etc/sysconfig/iptables` ファイルに保存され、サービスが起動したり、マシンが再起動されたりするたびに適用されます。

#### 18.4. 一般的な IPTABLES フィルタリング

リモート攻撃者が LAN にアクセスできないのは、ネットワークセキュリティーの最も重要な要素の 1 つです。LAN の整合性は、意図的なファイアウォールルールを使用して悪意のあるリモートユーザーから保護する必要があります。

ただし、デフォルトのポリシーでは、受信、送信、転送パケットをすべてブロックするように設定されていれば、ファイアウォール/ゲートウェイと内部 LAN ユーザーが相互に通信したり、外部リソースと通信したりすることはできません。

ユーザーがネットワーク関連の機能を実行し、ネットワークアプリケーションを使用できるようにするには、管理者は通信用に特定のポートを開く必要があります。

たとえば、ファイアウォールのポート 80 へのアクセスを許可するには、以下のルールを追加します。

```
[root@myServer ~] # iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
```

これにより、ユーザーは標準ポート 80 を使用して通信する Web サイトを閲覧できます。Web サイト (例: <https://www.example.com/>) をセキュアにできるようにするには、以下のようにポート 443 へのアクセスを提供する必要があります。

```
[root@myServer ~] # iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
```



## 重要な影響

iptables ルールセットを作成する場合、順序は重要です。

ルールで 192.168.100.0/24 サブネットからのパケットが削除され、その後に 192.168.100.13 (ドロップされたサブネット内にある) からのパケットを許可するルールを指定すると、2 番目のルールは無視されます。

192.168.100.13 からのパケットを許可するルールは、残りのサブネットをドロップするルールの前に付ける必要があります。

既存のチェーンに特定の場所にルールを挿入するには、`-I` オプションを使用します。以下に例を示します。

```
[root@myServer ~] # iptables -I INPUT 1 -i lo -p all -j ACCEPT
```

このルールは、ローカルループバックデバイストラフィックを許可するために INPUT チェーンの最初のルールとして挿入されます。

LAN へのリモートアクセスが必要になる場合があります。SSH などのセキュアなサービスは、LAN サービスへの暗号化されたリモート接続に使用できます。

PP ベースのリソース (モード銀行、一括 ISP アカウントなど) を持つ管理者は、ファイアウォールバリアを安全に行うためにダイアルアップアクセスを使用できます。直接接続されているため、モード接続は通常、ファイアウォール/ゲートウェイの背後になります。

ただし、ブロードバンド接続を持つリモートユーザーの場合は、特別なケースを行うことができます。iptables を、リモート SSH クライアントからの接続を受け入れるように設定できます。たとえば、以下のルールではリモートの SSH アクセスを許可します。

```
[root@myServer ~] # iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
[root@myServer ~] # iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
```

これらのルールにより、インターネットまたはファイアウォール/ゲートウェイに直接接続された単一の PC など、個別システムの送受信アクセスが可能になります。ただし、ファイアウォール/ゲートウェイの背後にあるノードがこれらのサービスにアクセスするのを許可しません。これらのサービスへ

の LAN アクセスを許可するには、`iptables` フィルタリングルールと共に ネットワークアドレス変換 (NAT) を使用できます。

## 18.5. FORWARD および NAT ルール

ほとんどの ISP は、サービスを提供する組織に公開されているルーティング可能な IP アドレスのみを提供します。

管理者は、LAN 上の全ノードにパブリック IP アドレスを指定せずにインターネットサービスへのアクセスを共有する代替方法を見つける必要があります。プライベート IP アドレスの使用は、LAN 上の全ノードが内部および外部のネットワークサービスに適切にアクセスできるようにする最も一般的な方法です。

エッジルーター (ファイアウォールなど) は、インターネットから着信送信を受け取り、パケットを目的の LAN ノードにルーティングすることができます。同時に、ファイアウォール/ゲートウェイは、LAN ノードからリモートインターネットサービスに送信要求をルーティングすることもできます。

ネットワークトラフィックの転送により、特に内部 IP アドレスのなりすまみや、リモート攻撃者のマシンが LAN のノードとして機能する可能性がある最新のクラッキングツールが利用可能になると、危険にさらされる可能性があります。

これを防ぐために、`iptables` は、ネットワークリソースの異常な使用を防ぐために実装可能なルーティングおよび転送ポリシーを提供します。

管理者は、FORWARD チェーンを使用して、LAN 内でパケットをルーティングできる場所を制御できます。たとえば、(firewall/gateway に `eth1` の内部 IP アドレスが割り当てられていることを前提とします)、以下のルールを使用します。

```
[root@myServer ~] # iptables -A FORWARD -i eth1 -j ACCEPT
[root@myServer ~] # iptables -A FORWARD -o eth1 -j ACCEPT
```

このルールは、ファイアウォールの背後にあるシステムに内部ネットワークへのアクセスを付与します。ゲートウェイは、1つの LAN ノードから目的の宛先ノードにパケットをルーティングし、`eth1` デバイスを介してすべてのパケットを渡します。

## 備考

デフォルトでは、Red Hat Enterprise Linux カーネルの IPv4 ポリシーは IP 転送のサポートを無効にします。これにより、Red Hat Enterprise Linux を実行するマシンが専用の edge ルーターとして機能しなくなります。IP 転送を有効にするには、以下のコマンドを使用します。

```
[root@myServer ~] # sysctl -w net.ipv4.ip_forward=1
```

この設定変更は、現行セッションでのみ有効で、再起動またはネットワークサービスの再起動後も維持されません。IP 転送を永続的に設定するには、以下のように `/etc/sysctl.conf` ファイルを編集します。

以下の行を見つけます。

```
net.ipv4.ip_forward = 0
```

この設定を以下のように編集します。

```
net.ipv4.ip_forward = 1
```

以下のコマンドを使用して `sysctl.conf` ファイルへの変更を有効にします。

```
[root@myServer ~] # sysctl -p /etc/sysctl.conf
```

### 18.5.1. POSTROUTING and IP Masquerading

ファイアウォールの内部 IP デバイスを介して転送されたパケットを受け取ると、LAN ノードは相互に通信できますが、インターネットに外部で通信することはできません。

プライベート IP アドレスを持つ LAN ノードが外部のパブリックネットワークと通信できるようにするには、IP マスカレードのファイアウォールを設定します。これにより、LAN ノードの要求をファイアウォールの外部デバイスの IP アドレスでマスクします（この場合は `eth0`）。

```
[root@myServer ~] # iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

このルールは NAT パケットマッチングテーブル(-t nat)を使用し、ファイアウォールの外部ネットワークデバイス(-o eth0)上の NAT(-A POSTROUTING)の組み込み POSTROUTING チェーンを指定し

ます。

**POSTROUTING** により、パケットの変更はファイアウォールの外部デバイスから出る際に変更できません。

**-j MASQUERADE** ターゲットを指定して、ファイアウォール/ゲートウェイの外部 IP アドレスでノードのプライベート IP アドレスをマスクします。

### 18.5.2. PREROUTING

内部ネットワーク上に、外部から利用できるようにするサーバーがある場合は、**NAT** の **PREROUTING** チェーンの **-j DNAT** ターゲットを使用して、内部サービスへの接続を要求する着信パケットを転送できる宛先 IP アドレスとポートを指定できます。

たとえば、受信した **HTTP** 要求を専用の **Apache HTTP Server 172.31.0.23** に転送する場合は、次のコマンドを使用します。

```
[root@myServer ~] # iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 172.31.0.23:80
```

このルールは、**nat** テーブルが組み込みの **PREROUTING** チェーンを使用して、一覧表示される宛先 IP アドレス **172.31.0.23** のみに受信 **HTTP** 要求を転送するように指定します。

#### 備考

**FORWARD** チェーンにデフォルトのポリシーが **DROP** の場合には、宛先 **NAT** ルーティングが可能になるように、受信 **HTTP** 要求をすべて転送するルールを追加する必要があります。これを行うには、以下のコマンドを使用します。

```
[root@myServer ~] # iptables -A FORWARD -i eth0 -p tcp --dport 80 -d 172.31.0.23 -j ACCEPT
```

このルールは、ファイアウォールから受信する **HTTP** 要求をすべて、ファイアウォールの背後にある **Apache HTTP Server** に転送します。

### 18.5.3. DMZ および IPTables

**iptables** ルールを作成して、トラフィックを専用の **HTTP** サーバーや **FTP** サーバーなど特定のマシンにルーティングできます。**DMZ** は、インターネットなどのパブリックテーライザーでサービスを

提供する専用の特別なローカルサブネットワークです。

たとえば、受信 HTTP 要求を 10.0.4.2 の専用 HTTP サーバーにルーティングするルールを設定するには、NAT は PREROUTING テーブルを使用してパケットを適切な宛先に転送します。

```
[root@myServer ~] # iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 10.0.4.2:80
```

このコマンドを使用すると、LAN の外部からポート 80 への HTTP 接続はすべて、残りの内部ネットワークとは別にネットワーク上の HTTP サーバーにルーティングされます。この形式のネットワークセグメンテーションを使用すると、ネットワーク上のマシンへの HTTP 接続が許可されるよりも安全を確保できます。

HTTP サーバーがセキュアな接続を受け入れるように設定されている場合は、ポート 443 も転送する必要があります。

## 18.6. 悪意のあるソフトウェアおよび SPOOFED IP アドレス

より詳細なルールを作成して、LAN 内の特定のサブネット、または特定のノードへのアクセスを制御することができます。また、trojans、worms、その他のクライアント/サーバーのワイルドカードなどの特定のアプリケーションまたはプログラムを制限することもできます。

たとえば、31337 から 31340（クラッキング用語の elite ポートと呼ばれる）のポートのサービス用にネットワークをスキャンするものもあります。

標準以外のポートを介して通信する正当なサービスがないため、それらのブロックにより、ネットワーク上のノードに個別にリモートマスターサーバーと通信する可能性を効果的に軽減できます。

以下のルールは、ポート 31337 の使用を試行する TCP トラフィックをすべてドロップします。

```
[root@myServer ~] # iptables -A OUTPUT -o eth0 -p tcp --dport 31337 --sport 31337 -j DROP  
[root@myServer ~] # iptables -A FORWARD -o eth0 -p tcp --dport 31337 --sport 31337 -j DROP
```

また、なりすましのプライベート IP アドレス範囲を試行する外部接続をブロックして、LAN をインフォレンジットすることもできます。

たとえば、LAN が 192.168.1.0/24 範囲を使用する場合、インターネット向けネットワークデバイス

(例: `eth0`) に指示するルールを設計して、LAN IP 範囲のアドレスを持つそのデバイスにパケットをドロップすることができます。

転送されたパケットをデフォルトポリシーとして拒否することが推奨されます。そのため、外部向けデバイス(`eth0`)への他のなりすましの IP アドレスは自動的に拒否されます。

```
[root@myServer ~] # iptables -A FORWARD -s 192.168.1.0/24 -i eth0 -j DROP
```

#### 備考

追加されたルールを扱う際に、`DROP` と `REJECT` ターゲットには区別があります。

`REJECT` ターゲットはアクセスを拒否し、サービスへの接続を試行するユーザーに接続拒否エラーを返します。`DROP` ターゲットは名前が示すように、警告なしにパケットを破棄します。

管理者は、これらのターゲットを使用する際に独自の判断を使用できます。ただし、ユーザーの混乱を回避し、接続の続行を試みるには、`REJECT` ターゲットが推奨されます。

## 18.7. IPTABLES および接続の追跡

接続状態に基づいてサービスへの接続を検査したり、制限したりすることができます。`iptables` 内のモジュールは、接続追跡と呼ばれる方法を使用して、受信接続に関する情報を保存します。以下の接続状態に基づいて、アクセスを許可または拒否できます。

- **NEW:** HTTP 要求などの新しい接続を要求するパケット。
- **ESTABLISHED:** 既存の接続の一部であるパケット。
- **RELATED:** 新しい接続を要求するパケットは、既存の接続の一部です。たとえば、FTP はポート 21 を使用して接続を確立しますが、データは別のポート (通常はポート 20) に転送されます。
- **INVALID:** コネクション追跡テーブルの接続の一部ではないパケット。

プロトコル自体がステートレスである場合でも、`iptables` 接続追跡のステートフル機能を使用できます (UDP など)。以下の例は、接続追跡を使用して、確立された接続に関連するパケットのみを転送するルールを示しています。

```
[root@myServer ~] # iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

## 18.8. IPV6

IPv6 と呼ばれる次の世代のインターネットプロトコルの導入は、IPv4 (または IP) の 32 ビットアドレス制限を超えています。IPv6 は 128 ビットアドレスに対応しており、IPv6 に対応している代理ネットワークは、IPv4 よりも大量のルーティング可能なアドレスに対応できます。

Red Hat Enterprise Linux は、`getfacl 6` サブシステムと `ip6tables` コマンドを使用して、IPv6 ファイアウォールルールをサポートします。Red Hat Enterprise Linux 5 では、IPv4 サービスおよび IPv6 サービスの両方がデフォルトで有効になっています。

`ip6tables` コマンド構文は、128 ビットアドレスをサポートすることを除き、すべての要素で `iptables` と同じです。たとえば、以下のコマンドを使用して、IPv6 対応ネットワークサーバーで SSH 接続を有効にします。

```
[root@myServer ~] # ip6tables -A INPUT -i eth0 -p tcp -s 3ffe:ffff:100::1/128 --dport 22 -j ACCEPT
```

IPv6 ネットワークの詳細は、<http://www.ipv6.org/> の IPv6 情報ページを参照してください。

## 18.9. 関連情報

ファイアウォールと、本章ではカバーできない Linux サブシステムにはいくつかの側面があります。詳細は、以下のリソースを参照してください。

### 18.9.1. インストールされているドキュメント

- `man` ページの `iptables` には、さまざまなオプションの概要が記載されています。

### 18.9.2. 便利な Web サイト

- <http://www.netfilter.org/>: 公式のホームページおよび `iptables` プロジェクトのホームページです。

- <http://www.tldp.org/>: Linux ドキュメントプロジェクトには、ファイアウォールの作成や管理に関する役立つガイドが複数含まれています。
- <http://www.iana.org/assignments/port-numbers>: インターネット割り当て番号機関が割り当てた登録済みおよび共通のサービスポートの公式リスト。

### 18.9.3. 関連するドキュメント

- 
-



## 第19章

•

•

•

19.1.

- 

- 

- 

- 

- 

- 

- 

***id:5:initdefault:***

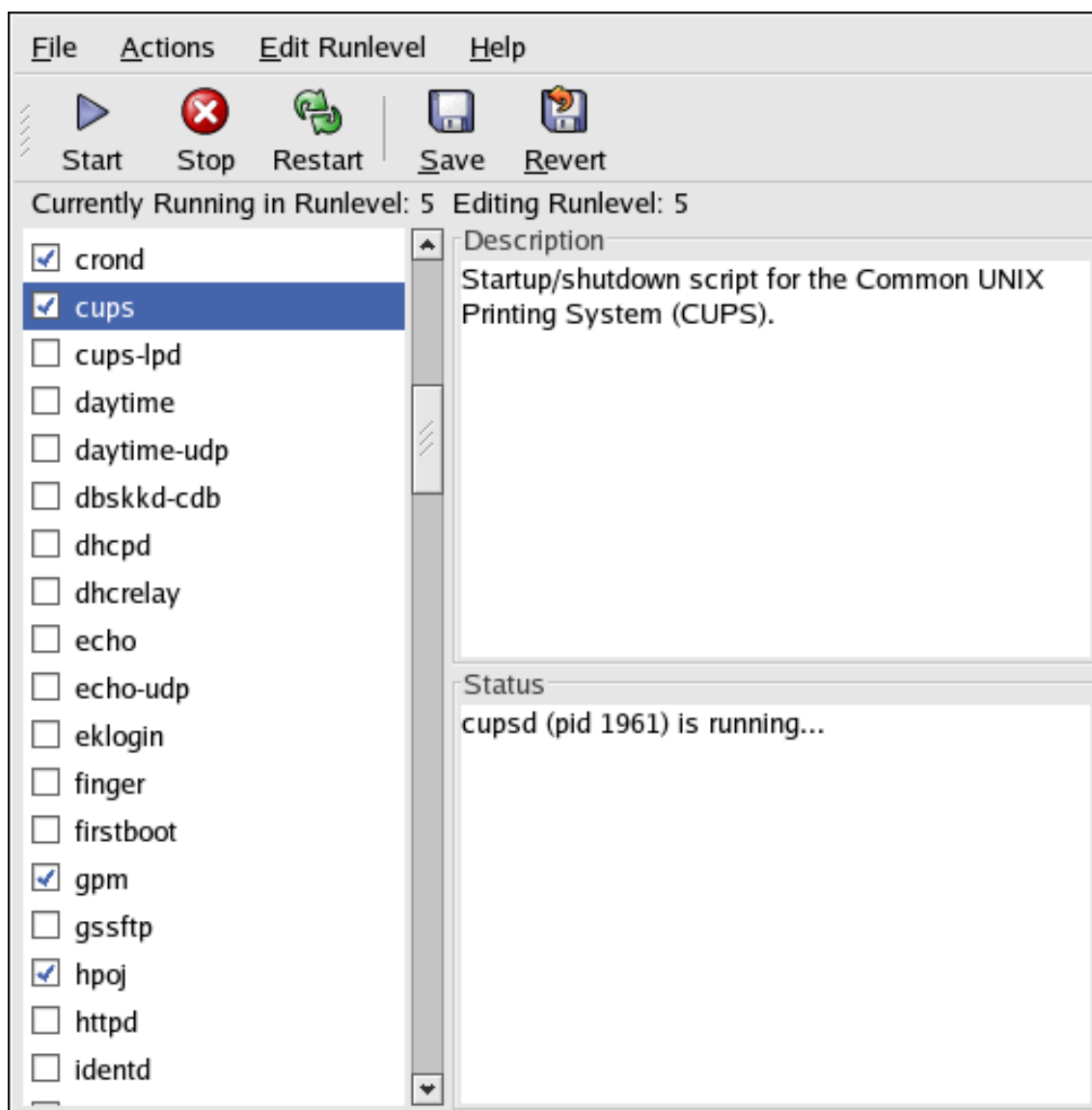
## **19.2.**

### **19.2.1. xinetd**

---

**19.3.**

図19.1



[D]



**WARNING**

**1.**

**2.**

**3.**

#### **19.4. NTSYSV**



**WARNING**

## 19.5. CHKCONFIG

```
finger    on
```

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

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



**WARNING**

## 19.6. 関連情報

### 19.6.1. インストールされているドキュメント

- 
-

---

### 19.6.2. 便利な Web サイト

- 

### 19.6.3. 関連書籍

- 

-

## 第20章 OPENSSSH

### 20.1.

### 20.2.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@
@  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.
```

### 20.3.

#### 20.3.1.



`ssh penguin.example.net`

***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)?***

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

`ssh username@penguin.example.net`

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

### 20.3.2.

```
scp <localfile>username@tohostname:<remotefile>
```

```
scp shadowman username@penguin.example.net:shadowman
```

```
scp username@tohostname:<remotefile><newlocalfile>
```

```
scp downloads/* username@penguin.example.net:uploads/
```

### **20.3.3.**

#### **20.3.4. 鍵ペアの生成**



#### 20.3.4.1.

1.

```
ssh-keygen -t rsa
```

2.

```
chmod 755 ~/.ssh
```

3.

4.

```
chmod 644 ~/.ssh/authorized_keys
```

5.

#### 20.3.4.2.



1.

```
ssh-keygen -t dsa
```



2.

```
chmod 755 ~/.ssh
```

3.

4.

```
chmod 644 ~/.ssh/authorized_keys
```

5.

#### 20.3.4.3.

1.

```
ssh-keygen -t rsa1
```



2.

3.

4.

#### 20.3.4.4.

1.

2.

3.

#### 20.3.4.5.

1.

`exec /usr/bin/ssh-agent $SHELL`

2.

`ssh-add`



3.

## 20.4. 関連情報

### 20.4.1. インストールされているドキュメント

- 

### 20.4.2. 便利な Web サイト

- 

- 

- 

### 20.4.3. 関連書籍

-

## 第21章 NETWORK FILE SYSTEM (NFS)

21.1.

21.2.

```
mount shadowman.example.com:/misc/export/misc/local
```

**WARNING****21.2.1. /etc/fstab を使用した NFS ファイルシステムのマウント**

別のマシンから NFS 共有をマウントする別の方法は、`/etc/fstab` ファイルに行を追加することです。その行には、NFS サーバーのホスト名、エクスポートされるサーバーディレクトリー、および NFS 共有がマウントされるローカルマシンディレクトリーを記述する必要があります。`/etc/fstab` ファイルを変更するには、`root` でなければなりません。

`/etc/fstab` の行の一般的な構文は以下の通りです。

```
server:/usr/local/pub /pub nfs rsize=8192,wszsize=8192,timeo=14,intr
```

このコマンドを実行する前に、マウントポイント `/pub` がクライアントマシンに存在している必要があります。

## 21.2.2.

```
/misc /etc/auto.misc --timeout 60
```

```
myproject -rw,soft,intr,rsize=8192,wspace=8192 penguin.example.net:/proj52
```



備考

```
/sbin/service autofs restart
```

```
/sbin/service autofs status
```

```
/sbin/service autofs reload
```



## 21.2.3.

```
mount -o udp shadowman.example.com:/misc/export /misc/local
```

```
server:/usr/local/pub /pub nfs rsize=8192,wsiz=8192,timeo=14,intr,udp
```

NFS マウントが NIS サーバーの `autofs` 設定ファイルで指定されている場合には、NIS 対応のワークステーションに利用できます。

```
myproject -rw,soft,intr,rsize=8192,wsiz=8192,udp penguin.example.net:/proj52
```

デフォルトは TCP であるため、`-o udp` オプションが指定されていない場合、NFS でエクスポートされるファイルシステムは TCP 経由でアクセスされます。

TCP を使用する利点は次のとおりです。

- 接続の持続性が改善され、NFS 古いファイルがメッセージを処理します。
- TCP は、完了のみを確認する UDP とは異なり、負荷の高いネットワークのパフォーマンスが発生します。
- TCP は UDP(none)よりも優れた輻輳制御を持ちます。非常に輻輳のネットワークでは、UDP パケットはドロップされる最初のパケットになります。つまり、NFS が (8K チャンク内

に) データを書き込む場合は、その 8K がすべて UDP で再送信される必要があります。TCP の信頼性により、8K データの一部のみが一度に送信されます。

- エラー検出。TCP 接続が破損した場合 (サーバーが利用できないことを原因に)、クライアントはサーバーが利用可能になると接続プロセスを再開します。UDP では接続を使用しないため、クライアントはサーバーが接続を再確立するまで、データでネットワークを固定します。

主な欠点は、TCP プロトコルに関連するオーバーヘッドにより、パフォーマンスに非常に少ないヒットがあることです。

#### 21.2.4. ACL の維持

Red Hat Enterprise Linux 4 カーネルは、NFS プロトコルまたは Samba プロトコルでマウントされた ext3 ファイルシステムおよび ext3 ファイルシステムの ACL サポートを提供します。したがって、ext3 ファイルシステムで ACL が有効になり、NFS エクスポートされている場合、NFS クライアントが ACL を読み取れる場合は、NFS クライアントでも使用されます。

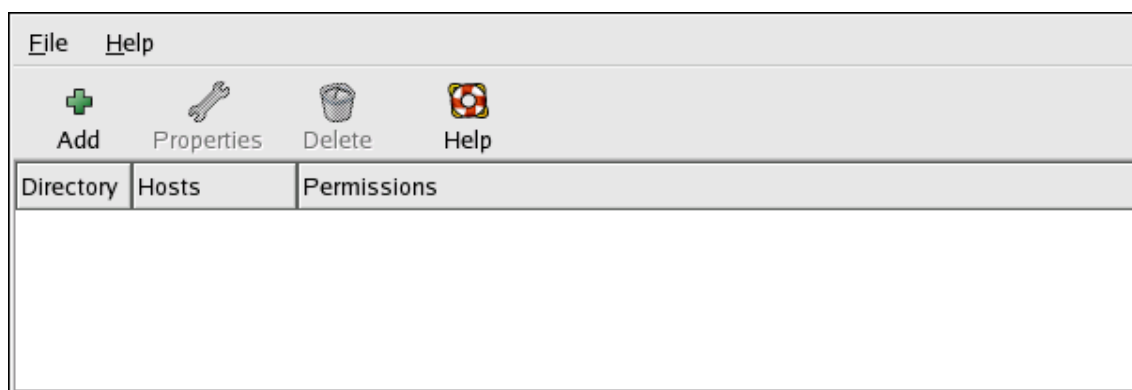
ACL で NFS ファイルシステムのマウントに関する詳細は、[14章アクセス制御リスト](#) を参照してください。

#### 21.3. NFS ファイルシステムのエクスポート

NFS サーバーからのファイルの共有または提供は、ディレクトリーのエクスポート と呼ばれます。NFS サーバー設定ツールを使用すると、システムを NFS サーバーとして設定できます。

NFS Server Configuration Tool を使用するには、X Window System を実行し、root 権限があり、system-config-nfs 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。アプリケーションを起動するには、(Panel)=> System Settings => Server Settings => NFS の Main Menu Button を選択するか、コマンド system-config-nfs を入力します。

図21.1 NFS サーバー設定ツール



[D]

NFS 共有を追加するには、追加 ボタンをクリックします。図21.2「共有の追加」に表示されるダイアログボックスが表示されます。

Basic タブには、以下の情報が必要です。

- **directory:** /tmp など、共有するディレクトリーを指定します。
- **host(s):** ディレクトリーを共有するホストを指定します。使用できる形式の説明は、「[ホスト名の形式](#)」を参照してください。
- **Basic permissions:** ディレクトリーに読み取り専用パーミッションか、読み取り/書き込み権限を指定するかどうかを指定します。

図21.2 共有の追加

The image shows a dialog box for adding an NFS share. It has three tabs: 'Basic', 'General Options', and 'User Access'. The 'General Options' tab is active. The 'Directory' field is set to '/tmp' with a 'Browse...' button. The 'Host(s)' field is set to '\*.example.com'. Under 'Basic permissions', the 'Read-only' option is selected. At the bottom, there are 'Cancel' and 'OK' buttons.

[D]

**General Options** タブでは、以下のオプションを設定できます。

- ポート 1024 以上からの接続を許可します (1024 未満のポート番号で開始するサービスは root として起動する必要があります)。このオプションを選択すると、root 以外のユーザーが NFS サービスを起動できます。このオプションは `insecure` に対応します。
- **Allow insecure file locking** - ロックの要求は必要ありません。このオプションは `insecure_locks` に対応します。
- **サブツリーの確認の無効化** - ファイルシステムのサブディレクトリーがエクスポートされていて、ファイルシステム全体がエクスポートされていない場合、サーバーは、要求されたファイルがエクスポートされたサブディレクトリーにあるかどうかを確認します。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して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ている場合は、サブツリーの確認を無効にして転送率を増やすことができます。このオプションは `no_subtree_check` に対応します。
- **要求時の同期書き込み操作** : デフォルトでは有効で、リクエストによって加えられた変更がディスクに書き込まれる前に、サーバーが要求に回答できません。このオプションは `sync` に対応します。これを選択しないと `async` オプションが使用されます。
  - **書き込み操作の即時同期を強制** - ディスクへの書き込みを遅延させないでください。このオプションは `no_wdelay` に対応します。

User Access タブでは以下のオプションを設定できます。

- リモート root ユーザーとしてリモートの root として処理：デフォルトでは、root ユーザーのユーザー ID とグループ ID はいずれも 0 です。root squashing は、ユーザー ID 0 とグループ ID 0 を匿名のユーザーおよびグループ ID にマッピングし、クライアントの root 権限が NFS サーバー上の root 権限を持たないようにします。このオプションが選択された場合は、root は匿名にマッピングされず、クライアントの root 権限はエクスポートされるディレクトリーへの root 権限を持ちます。このオプションを選択すると、システムのセキュリティーが大幅に低下します。絶対に必要な場合を除き、選択しないでください。このオプションは no\_root\_squash に対応します。
- すべてのクライアントユーザーを匿名ユーザーとして扱います。このオプションを選択すると、ユーザー ID とグループ ID はすべて匿名ユーザーにマッピングされます。このオプションは all\_squash に対応します。
  - 匿名ユーザーのローカルユーザー ID の指定 - 匿名ユーザーとして全クライアントユーザーを選択すると、匿名ユーザーのユーザー ID を指定できます。このオプションは anonuid に対応します。
  - 匿名ユーザーのローカルグループ ID の指定 - 匿名ユーザーとして全クライアントユーザーを選択すると、匿名ユーザーのグループ ID を指定できます。このオプションは anongid に対応します。

既存の NFS 共有を編集するには、一覧から共有を選択し、Properties 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て削除 ボタンをクリックします。

OK をクリックして、一覧から NFS 共有を追加、編集、または削除すると、サーバーデーモンが再起動され、古い設定ファイルは /etc/exports.bak として保存されます。新しい設定は /etc/exports に書き込まれます。

NFS Server Configuration Tool は、/etc/exports 設定ファイルに直接読み書きします。そのため、ツールを使用して手動で変更でき、ファイルを手動で変更した後にこのツールを使用できます（ファイルが正しい構文で変更されている場合）。

### 21.3.1. コマンドラインからの設定

テキストエディターを使用して設定ファイルを編集する場合や、X Window System がインストールされていない場合は、設定ファイルを直接変更できます。

`/etc/exports` ファイルは、NFS サーバーがエクスポートするディレクトリーを制御します。形式は以下ようになります。

```
directoryhostname(options)
```

指定する必要があるオプションは `sync` または `async (sync)` のいずれかです。 `sync` が指定されている場合、サーバーは要求による変更がディスクに書き込まれる前に要求に応答しません。

以下に例を示します。

```
/misc/export speedy.example.com(sync)
```

ユーザーは `speedy.example.com` のユーザーが、デフォルトの読み取り専用パーミッションで `/misc/export` をマウントすることを許可しましたが、

```
/misc/export speedy.example.com(rw,sync)
```

これにより、ユーザーは `speedy.example.com` のユーザーが読み取り/書き込み権限で `/misc/export` をマウントできるようになります。

可能なホスト名の形式の説明は、「[ホスト名の形式](#)」を参照してください。

指定できるオプションの一覧については、『[リファレンスガイド](#)』を参照してください。



## WARNING

`/etc/exports` ファイルのスペースを注意して行ってください。ホスト名とオプションを括弧で囲んでいけない場合には、オプションは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は、オプションは残りの世界に適用されます。たとえば、以下の行を調べます。

```
/misc/export speedy.example.com(rw,sync)
/misc/export speedy.example.com (rw,sync)
```

最初の行は `speedy.example.com` の読み取り/書き込みアクセスからユーザーに付与され、他のすべてのユーザーを拒否します。2番目の行は `speedy.example.com` の読み取り専用アクセス（デフォルト）からユーザーに付与され、残りのユーザーに読み書きアクセスを許可します。

`/etc/exports` を変更するたびに、NFS デーモンに変更を通知するか、以下のコマンドで設定ファイルを再読み込みする必要があります。

```
/sbin/service nfs reload
```

### 21.3.2. ホスト名の形式

ホストは以下の形式にすることができます。

- 単一マシン：完全修飾ドメイン名（サーバーにより解決）、ホスト名（サーバーによって解決可能）、または IP アドレス。
- ワイルドカードで指定された一連のマシン - 文字列の一致を指定するには、\* または ? 文字を使用します。ワイルドカードは IP アドレスでは使用しないことになっていますが、逆引き DNS ルックアップが失敗した場合には誤って動作する可能性があります。完全修飾ドメイン名でワイルドカードを指定する場合、ドット(.)はワイルドカードに含まれません。たとえば、`*.example.com` には `one.example.com` が含まれますが、`1.two.example.com` は含まれません。
- IP ネットワーク：`a.b.c.d/z` を使用します。a.b.c.d はネットワークに、z はネットマスクのビット数（例：pidt）です。もう 1 つの許容形式として `a.b.c.d/ netmask` を使用すること

ができます。ここで、`a.b.c.d` はネットワークとネットマスク（例：`192.168.100.8/255.255.255.0`）になります。

- `netgroups: @group-name` 形式。 `group-name` は NIS `netgroup` 名です。

### 21.3.3. 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で、`nfs` サービスが実行している必要があります。

以下のコマンドを使用して、NFS デーモンのステータスを表示します。

```
/sbin/service nfs status
```

以下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
```

以下のコマンドで NFS デーモンを停止します。

```
/sbin/service nfs stop
```

システムの起動時に `nfs` サービスを起動するには、以下のコマンドを使用します。

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

`chkconfig`、`ntsysv`、または `Services Configuration Tool` を使用して、システムの起動時に開始するサービスを設定することもできます。詳細は、[19章](#) を参照してください。

## 21.4. 関連情報

本章では、NFS を使用する基本を説明します。詳細は、以下のリソースを参照してください。

### 21.4.1. インストールされているドキュメント

- `nfsd` の `man` ページ、`mountd`、`export`、`auto.master`、および `autofs` (`man` セクション



5 および 8) の man ページです。これらの man ページは、NFS および autofs 設定ファイルの正しい構文を示しています。

#### 21.4.2. 便利な Web サイト

- <http://nfs.sourceforge.net/>: NFS の Web ページには、メーリングリストおよび FAQ へのリンクが含まれています。
- <http://www.tldp.org/HOWTO/NFS-HOWTO/index.html>: Linux ドキュメントプロジェクトからの『Linux NFS-HOWTO』

#### 21.4.3. 関連書籍

- Hal Stern; O'Reilly & Associates, Inc に『よる NFS サービスおよび NIS サービス』の管理

## 第22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ーを共有します。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、OS/2、および Linux が含まれます。

Red Hat Enterprise Linux 4 カーネルには、ext3 ファイルシステムの アクセス制御リスト (ACL) サポートが含まれています。Samba サーバーが、ACL が有効になっている状態で ext3 ファイルシステムを共有し、クライアントシステムのカーネルが ext3 ファイルシステムからの ACL の読み取りに対応する場合、クライアントは ACL を自動的に認識し、使用します。ACL の詳細は、[14章アクセス制御リスト](#) を参照してください。

### 22.1. SAMBA を使用する理由

Samba は、Windows マシンと Linux マシンの両方のネットワークがある場合に役立ちます。Samba は、ネットワーク内のすべてのシステムでファイルおよびプリンターを共有できるようにします。Linux マシン間でのみファイルを共有するには、[21章Network File System \(NFS\)](#) で説明されているように NFS を使用します。Linux マシン間でプリンターを共有する場合は、Samba を使用する必要はありません。[33章プリンターの設定](#) を参照してください。

### 22.2. SAMBA サーバーの設定

デフォルトの設定ファイル(/etc/samba/smb.conf)を使用すると、ユーザーはホームディレクトリーを Samba 共有として表示できます。また、システムに設定されたすべてのプリンターを Samba 共有プリンターとして共有します。つまり、システムにプリンターを割り当て、ネットワーク上の Windows マシンから印刷できます。

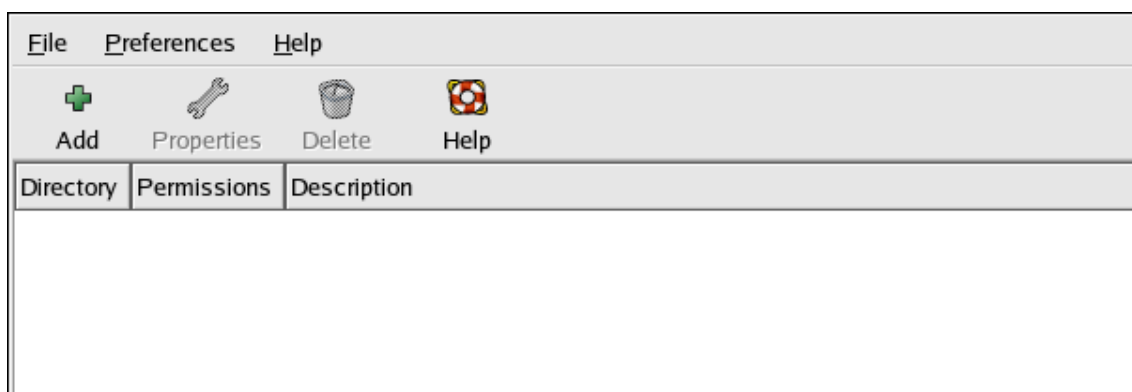
#### 22.2.1. グラフィカル設定

グラフィカルインターフェースを使用して Samba を設定するには、Samba Server Configuration Tool を使用します。コマンドラインの設定の場合は、[「コマンドラインからの設定」](#)に進みます。

Samba Server Configuration Tool は、Samba 共有、ユーザー、および基本的なサーバー設定を管理するグラフィカルインターフェースです。/etc/samba/ ディレクトリーの設定ファイルを変更します。アプリケーションを使用していないこれらのファイルに加えた変更は保持されます。

このアプリケーションを使用するには、X Window System を実行し、root 権限があり、system-config-samba 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。デスクトップから Samba Server Configuration Tool を起動するには、(Panel)=> System Settings => Server Settings => Samba に移動するか、シェルプロンプトで system-config-samba コマンド (XTerm や GNOME ターミナルなど) を入力します。

図22.1 Samba サーバー設定ツール



[D]



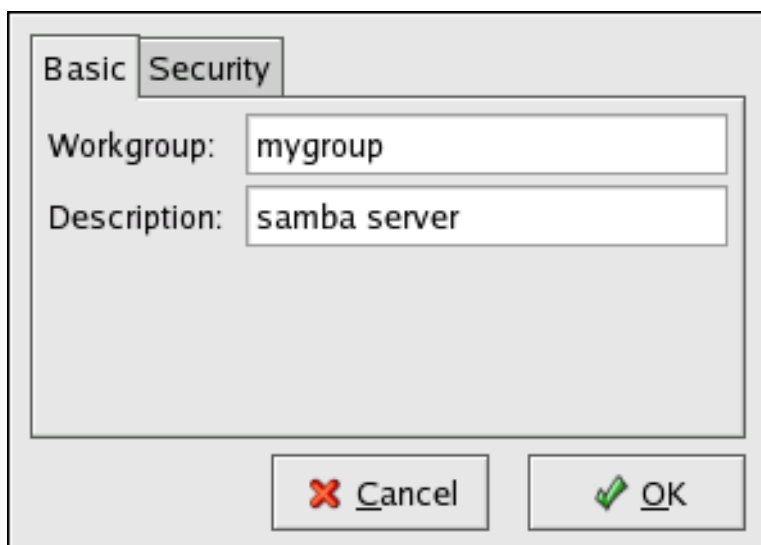
## 備考

**Samba Server Configuration Tool** は、**Samba** サーバーで独自のホームディレクトリを表示できるようにする共有プリンターまたはデフォルトのスタンザを表示できません。

## 22.2.1.1. サーバーの設定

**Samba** サーバーを設定する最初の手順は、サーバーの基本設定といくつかのセキュリティーオプションを設定することです。アプリケーションの起動後に、プルダウンメニューから **Preferences => Server Settings** を選択します。**Basic** タブは、[図22.2「基本的なサーバーの設定」](#) に示すように表示されます。

図22.2 基本的なサーバーの設定



[D]

**Basic** タブで、コンピューターが置かれるワークグループと、コンピューターの簡単な説明を指定します。これらは、`smb.conf` の `workgroup` オプションおよび `サーバー文字列` オプションに対応しま

す。

図22.3 セキュリティーサーバーの設定

[D]

セキュリティー タブには以下のオプションが含まれます。

- **Authentication Mode:** これは セキュリティー オプションに対応します。以下の認証のタイプのいずれかを選択します。
- **ADS:** Samba サーバーは、Active Directory Domain(ADS)レルムのドメインメンバーとして機能します。このオプションでは、Kerberos がサーバーにインストールおよび設定され、Samba は samba-client パッケージに含まれる net ユーティリティーを使用して ADS レルムのメンバーである必要があります。詳細は、net の man ページを参照してください。このオプションでは、Samba を ADS コントローラーとして設定することはありません。Kerberos Realm フィールドに Kerberos サーバーのレルムを指定します。



#### 備考

Kerberos Realm フィールドは、EXAMPLE.COM など、すべての大文字で指定する必要があります。

ADS レルムで Samba サーバーをドメインメンバーとして使用する場合は、/etc/krb5.conf ファイルなど、Kerberos の適切な設定を想定します。

- **ドメイン:** Samba サーバーは、Windows NT Primary または Backup Domain Controller に依存してユーザーを検証します。サーバーはユーザー名とパスワードをコントローラーに渡して、戻るまで待機します。Authentication Server フィールドに Primary または Backup Domain Controller の NetBIOS 名を指定します。

これを選択した場合、Encrypted Passwords オプションを Yes に設定する必要があります。

- **server:** Samba サーバーは、別の Samba サーバーに渡すことで、ユーザー名とパスワードの組み合わせを検証しようとします。そうでない場合、サーバーはユーザー認証モードを使用して検証を試みます。Authentication Server フィールドに他の Samba サーバーの NetBIOS 名を指定します。

- **共有 - Samba ユーザー:** Samba サーバーごとにユーザー名とパスワードの組み合わせを入力する必要はありません。Samba サーバーから特定の共有ディレクトリーへの接続を試みるまで、ユーザー名とパスワードの入力は要求されません。

- **user:** (デフォルト) Samba ユーザーは、Samba サーバーごとに有効なユーザー名とパスワードを提供する必要があります。Windows のユーザー名 オプションを機能させる場合は、このオプションを選択します。詳細は、「[Samba ユーザーの管理](#)」を参照してください。

- **暗号化パスワード:** このオプションは、クライアントが Windows 98、Windows NT 4.0 と Service Pack 3 などの新しいバージョンの Microsoft Windows に接続している場合は有効にする必要があります。パスワードは、傍受できるプレーンテキストの単語ではなく、暗号化された形式でサーバーとクライアント間で転送されます。これは、暗号化されたパスワード オプションに対応します。暗号化された Samba パスワードの詳細は、「[暗号化パスワード](#)」を参照してください。

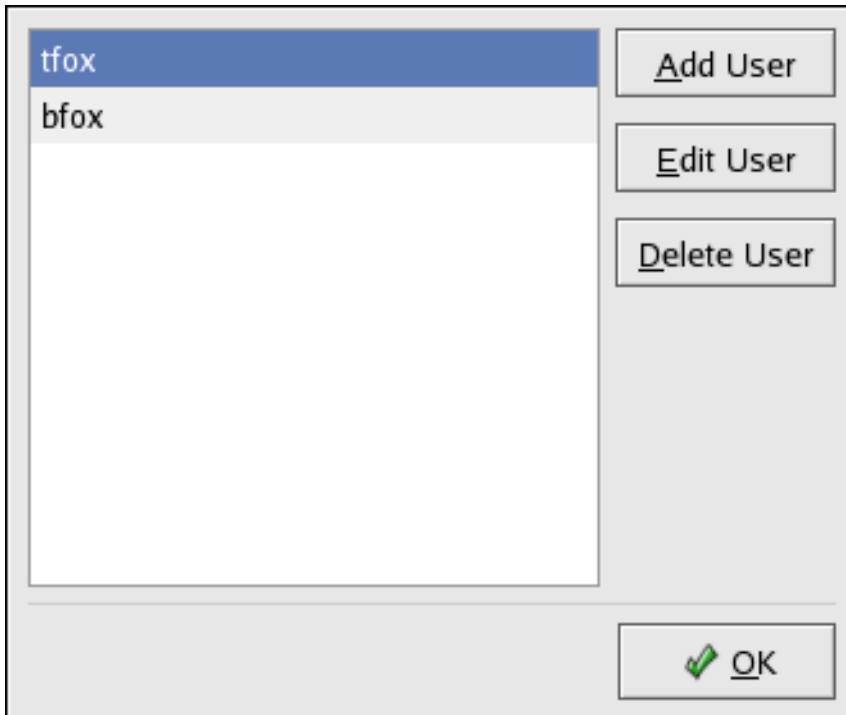
- **ゲストアカウント:** ユーザーまたはゲストユーザーが Samba サーバーにログインする場合は、サーバーの有効なユーザーにマップされる必要があります。ゲスト Samba アカウントとなるシステムの既存のユーザー名を 1 つ選択します。ゲストが Samba サーバーにログインすると、このユーザーと同じ特権を持ちます。これは、ゲストアカウント オプションに対応します。

OK をクリックすると、変更は設定ファイルに書き込まれ、デーモンが再起動され、変更はすぐに有効になります。

### 22.2.1.2. Samba ユーザーの管理

**Samba Server Configuration Tool** では、**Samba ユーザーを追加する前に、Samba サーバーとして機能するシステムで既存のユーザーアカウントがアクティブである必要があります。Samba ユーザーは、既存のユーザーアカウントに関連付けられます。**

図22.4 Samba ユーザーの管理



[D]

**Samba ユーザーを追加するには、プルダウンメニューから Preferences => Samba Users を選択して Add User ボタンをクリックします。「Create New Samba User」ウィンドウで、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 マシンに異なるユーザー名を持ち、Windows マシンから Samba サーバーにログインする必要がある場合は、Windows ユーザー名 フィールドに Windows ユーザー名を指定します。このオプションが機能するには、Server Settings 設定の Security タブの Authentication Mode を User に設定する必要があります。**

**また、Samba User の Samba パスワードを設定し、再度入力して確認します。Samba に暗号化されたパスワードを使用することを選択した場合でも、すべてのユーザーに対して Samba パスワードはシステムパスワードとは異なることが推奨されます。**

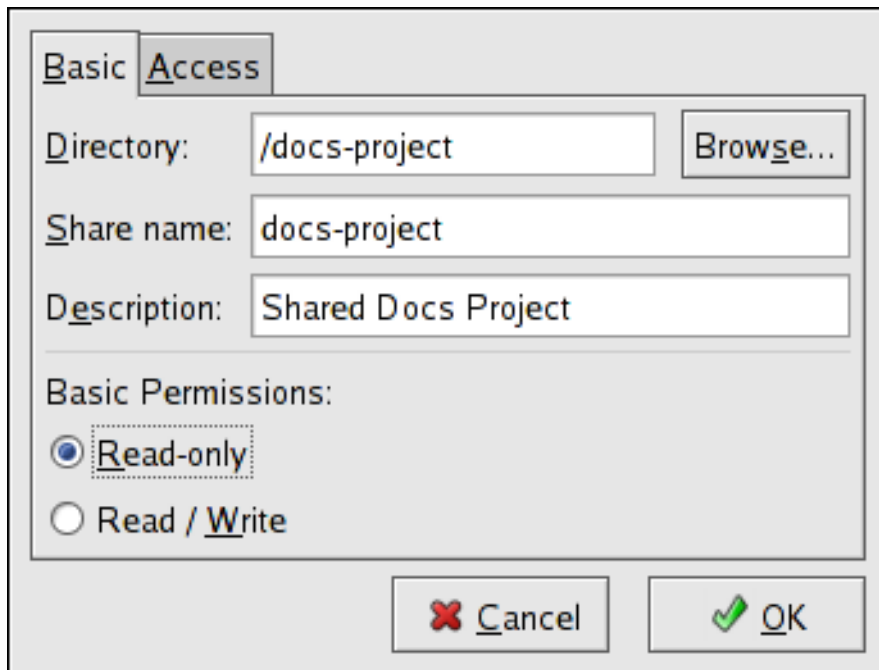
**既存のユーザーを編集するには、一覧からユーザーを選択し、Edit User をクリックします。既存の Samba ユーザーを削除するには、ユーザーを選択し、Delete User ボタンをクリックします。Samba ユーザーを削除しても、関連付けられたシステムユーザーアカウントは削除されません。**

OK ボタンをクリックすると、すぐにユーザーが変更されます。

### 22.2.1.3. 共有の追加

Samba 共有を作成するには、メインの Samba 設定ウィンドウの Add ボタンをクリックします。

図22.5 共有の追加



The screenshot shows a dialog box with two tabs: 'Basic' and 'Access'. The 'Access' tab is selected. It contains the following fields and options:

- Directory:** A text box containing '/docs-project' and a 'Browse...' button to its right.
- Share name:** A text box containing 'docs-project'.
- Description:** A text box containing 'Shared Docs Project'.
- Basic Permissions:** A section with two radio button options:
  - Read-only
  - Read / Write
- At the bottom, there are two buttons: 'Cancel' (with a red X icon) and 'OK' (with a green checkmark icon).

[D]

Basic タブでは、以下のオプションを設定します。

- ディレクトリー - Samba で共有するディレクトリー。ディレクトリーは、ここに入力する前に存在している必要があります。
- 共有名 : リモートマシンから表示される共有の実際の名前。デフォルトでは、Directory と同じ値ですが、設定できます。
- 説明 - ファイル共有の簡単な説明
- 基本的なパーミッション - ユーザーが共有ディレクトリー内のファイルのみを読み取ることができるかどうか、または共有ディレクトリーへの読み書きが可能かどうか。

**Access** タブで、指定したユーザーのみが共有にアクセスできるようにするか、すべての Samba ユーザーが共有にアクセスできるようにするかを選択します。特定のユーザーへのアクセスを許可する場合は、利用可能な Samba ユーザー一覧からユーザーを選択します。

ファイル共有は、OK をクリックした後すぐに追加されます。

### 22.2.2. コマンドラインからの設定

Samba は、`/etc/samba/smb.conf` を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と、コマンド `service smb restart` で Samba デーモンを再起動するまで変更は反映されません。

Windows のワークグループと Samba サーバーの簡単な説明を指定するには、`smb.conf` ファイルで以下の行を編集します。

```
workgroup = WORKGROUPNAME  
server string = BRIEF COMMENT ABOUT SERVER
```

**WORKGROUPNAME** は、このマシンが属する Windows ワークグループ名に置き換えま  
す。**BRIEF COMMENT ABOUT SERVER** はオプションで、Samba システムに関する Windows コメ  
ントとして使用されます。

Linux システムに Samba 共有ディレクトリーを作成するには、必要に応じて変更してか  
ら、`smb.conf` ファイルに以下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、Samba クライアントからユーザー `tfox` および `carole` が Samba サーバーの  
`/home/share` ディレクトリーの読み取りと書き込みを許可します。

### 22.2.3. 暗号化パスワード

暗号化パスワードはより安全であるため、デフォルトで有効になっています。暗号化したパスワー  
ドが使用されていない場合は、プレーンテキストのパスワードが使用されます。これは、ネットワーク



パケットスニファーを使用して傍受できます。暗号化されたパスワードを使用することが推奨されま  
す。

Microsoft SMB Protocol は、当初はプレーンテキストのパスワードを使用していました。ただし、Windows NT 4.0 と Service Pack 3 以降、Windows 98、Windows 2000、Windows ME、および Windows XP には暗号化された Samba パスワードが必要です。Linux システムと、これらの Windows オペレーティングシステムのいずれかを実行しているシステム間で Samba を使用するに  
は、Windows レジストリーを編集してプレーンテキストのパスワードを使用するか、暗号化されたパ  
スワードを使用するように Linux システムで Samba を設定します。レジストリーの変更を選択した場  
合は、すべての Windows マシンについてこれを実行する必要があります。これはリスクであり、さら  
に競合が生じる可能性があります。セキュリティの強化には、暗号化されたパスワードを使用するこ  
とが推奨されます。

Samba が暗号化パスワードを使用するように設定するには、以下の手順に従います。

1.

Samba 用に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  
いてシェルプロンプトでこれを作成するには、以下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、以下のコマンドを入力します。

```
ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
```

mksmbpasswd.sh スクリプトは、samba パッケージで /usr/bin ディレクトリーにイン  
ストールされます。

2.

root のみに読み取りおよび書き込み権限が割り当てられるように、Samba パスワード  
ファイルのパーミッションを変更します。

```
chmod 600 /etc/samba/smbpasswd
```

3.

このスクリプトは、ユーザーパスワードを新しいファイルにはコピーされず、Samba  
ユーザーアカウントはパスワードが設定されるまでアクティブになりません。セキュリティ  
を強化する場合は、ユーザーの Samba パスワードをユーザーのシステムパスワードとは異なる  
ことが推奨されます。各 Samba ユーザーのパスワードを設定するには、以下のコマンドを  
使用します (username を各ユーザーのユーザー名に置き換えます)。

```
smbpasswd username
```

4.

暗号化パスワードを有効にする必要があります。これらはデフォルトで有効にされているので、設定ファイルで明示的に有効にする必要はありません。ただし、設定ファイルで無効にすることはできません。/etc/samba/smb.conf ファイルで、以下の行が存在しないことを確認します。

```
encrypt passwords = no
```

行の先頭にあるセミコロン(;)でコメントアウトされていても、その行は無視され、暗号化されたパスワードが有効になります。この行が存在していてもコメントアウトされていない場合は、削除するか、コメントアウトします。

設定ファイルで暗号化されたパスワードを有効にするには、以下の行を/etc/samba/smb.conf に追加します。

```
encrypt passwords = yes  
smb passwd file = /etc/samba/smbpasswd
```

5.

シェルプロンプトで `command service smb restart` を入力し、`smb` サービスが起動していることを確認します。

6.

`smb` サービスが自動的に起動するようにするには、`ntsysv`、`chkconfig`、または `Services Configuration Tool` を使用してランタイム時に有効にします。詳細は、[19章](#) を参照してください。

`pam_smbpass` PAM モジュールを使用して、`passwd` コマンドの使用時に、ユーザーの Samba パスワードをシステムパスワードと同期できます。ユーザーが `passwd` コマンドを呼び出すと、Red Hat Enterprise Linux システムへのログインに使用するパスワードと、Samba 共有への接続に必要なパスワードが変更されます。

この機能を有効にするには、`pam_cracklib.so` 呼び出しの下にある /etc/pam.d/system-auth に次の行を追加します。

```
password required /lib/security/pam_smbpass.so nullok use_authok try_first_pass
```

#### 22.2.4. サーバーの起動と停止

Samba 経由でディレクトリーを共有するサーバーで、`smb` サービスが実行している必要があります。

以下のコマンドを使用して Samba デーモンのステータスを表示します。

```
/sbin/service smb status
```

以下のコマンドを使用してデーモンを起動します。

```
/sbin/service smb start
```

次のコマンドでデーモンを停止します。

```
/sbin/service smb stop
```

システムの起動時に smb サービスを起動するには、以下のコマンドを使用します。

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

chkconfig、ntsysv、または Services Configuration Tool を使用して、システムの起動時に開始するサービスを設定することもできます。詳細は、[19章](#) を参照してください。



#### ヒント

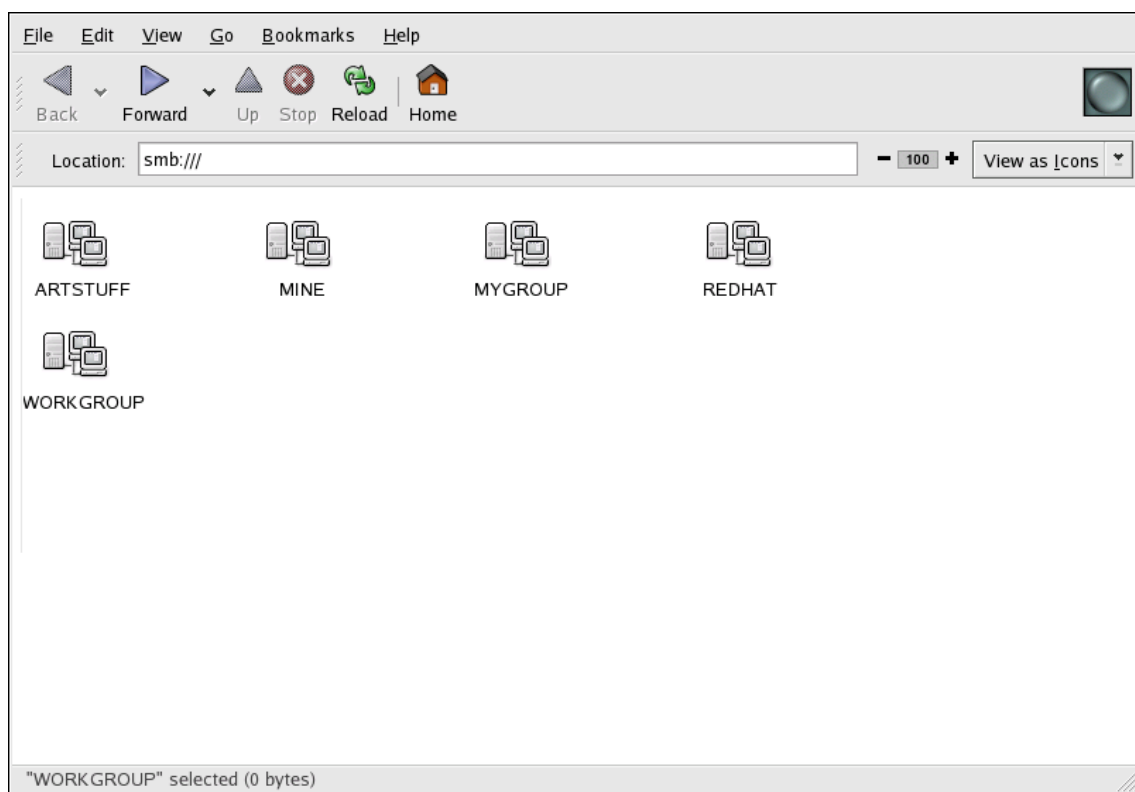
システムへのアクティブな接続を表示するには、`smbstatus` コマンドを実行します。

### 22.3. SAMBA 共有への接続

ネットワーク上で利用可能な Samba 共有を表示するには、Nautilus を使用できます。Main Menu Button (Panel) => Network Servers を選択して、ネットワーク上の Samba ワークグループの一覧を表示します。また、Nautilus の Location: バーに smb: と入力して作業グループを表示することもできます。

[図22.6 「nautilus の SMB Workgroups」](#) に示されているように、ネットワーク上の利用可能な SMB ワークグループごとにアイコンが表示されます。

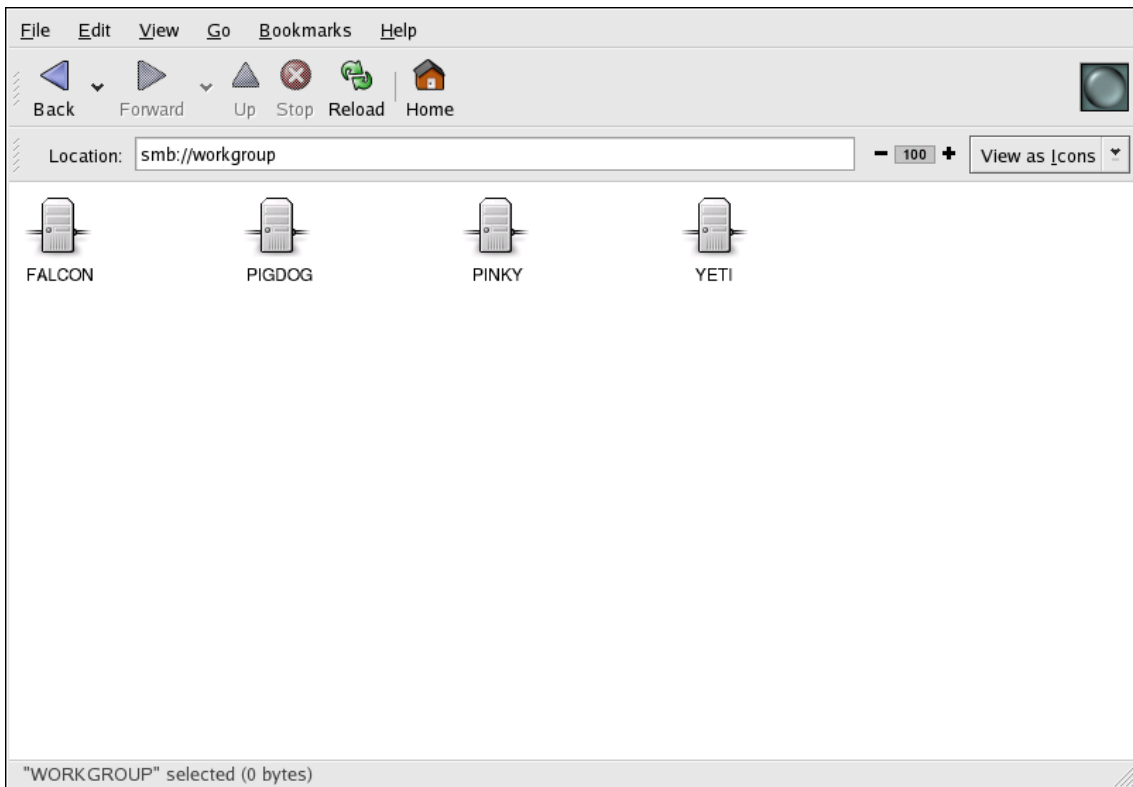
図22.6 nautilus の SMB Workgroups



[D]

ワークグループアイコンのいずれかをダブルクリックして、ワークグループ内のコンピューターの一覧を表示します。

図22.7 nautilus の SMB マシン



[D]

図22.7 「nautilus の SMB マシン」 から分かるように、ワークグループ内の各マシンのアイコンがあります。アイコンをダブルクリックして、マシン上で Samba 共有を表示します。ユーザー名とパスワードの組み合わせが必要な場合は、そのユーザー名とパスワードの入力が求められます。

または、次の構文を使用して、Nautilus の Location: bar で Samba サーバーおよび sharename を指定することもできます (<servername> と <sharename> を適切な値に置き換えます)。

```
smb://<servername>/<sharename>/
```

### 22.3.1. コマンドライン

Samba サーバーのネットワークをクエリーするには、findsmb コマンドを使用します。見つかった各サーバーに対して、IP アドレス、NetBIOS 名、ワークグループ名、オペレーティングシステム、および SMB サーバーバージョンが表示されます。

シェルプロンプトから Samba 共有に接続するには、以下のコマンドを入力します。

```
smbclient //<hostname>/<sharename> -U <username>
```

& It;hostname > は、接続する Samba サーバーのホスト名または IP アドレスに、< sharename >

は参照する共有ディレクトリーの名前に、`<username>` は、システムの Samba ユーザー名に置き換えます。正しいパスワードを入力するか、ユーザーにパスワードが必要ない場合は `Enter` を押します。

`smb:|>` プロンプトが表示された場合には、正常にログインしています。ログインしたら、コマンドのリストとして `help` と入力します。ホームディレクトリーの内容を閲覧する場合は、`sharename` をユーザー名に置き換えます。`-U` スイッチを使用しない場合、現行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、`exit` プロンプトで `smb:|>` と入力します。

### 22.3.2. 共有のマウント

Samba 共有をディレクトリーにマウントして、ディレクトリー内のファイルをローカルファイルシステムの一部であるかのように処理できるように、Samba 共有をマウントすると便利な場合があります。

Samba 共有をディレクトリーにマウントするには、ディレクトリーがない場合はディレクトリーを作成し、`root` で以下のコマンドを実行します。

```
mount -t smbfs -o username=<username> //<servername>/<sharename>/mnt/point/
```

このコマンドは、ローカルディレクトリー `/mnt/point/` の `<servername>` から `<sharename>` をマウントします。

## 22.4. 関連情報

ここで説明されていない設定オプションについては、以下のリソースを参照してください。

### 22.4.1. インストールされているドキュメント

- `man` ページの `SMB .conf - Samba 設定ファイル` の設定方法が説明されています。
- `smbd man` ページ: Samba デーモンがどのように機能するかを説明します。
- `smbclient` および `findsmb man` ページ: これらのクライアントツールの詳細について確認してください。

- `/usr/share/doc/samba- &lt;version-number&gt; /docs/ - samba` パッケージに含まれるヘルプファイル

#### 22.4.2. 便利な Web サイト

- <http://www.samba.org/>: Samba の Web ページには、便利なドキュメント、メーリングリスト、GUI インターフェースの一覧が含まれます。
- [http://www.samba.org/samba/docs/using\\_samba/toc.html](http://www.samba.org/samba/docs/using_samba/toc.html): 『Samba のオンラインバージョン、2nd Edition』 by Jay Ts, Robert Eckstein, および David Collier-Brown; O'Reilly & Associates

## 第23章 DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP)

Dynamic Host Configuration Protocol(DHCP)は、クライアントマシンに TCP/IP 情報を自動的に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、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を返す集中管理された DHCP サーバーに接続します。

### 23.1. DHCP を使用する理由

DHCP は、クライアントネットワークインターフェースの自動設定に役立ちます。管理者は、クライアントシステムを設定する際に、IP アドレス、ネットマスク、ゲートウェイ、または DNS サーバーを入力せずに DHCP を選択できます。クライアントはこの情報を DHCP サーバーから取得します。DHCP は、管理者が多数のシステムの IP アドレスを変更する必要がある場合にも便利です。すべてのシステムを再設定する代わりに、サーバー上の 1 つの DHCP 設定ファイルを編集して新しい IP アドレスを設定できます。組織の DNS サーバーが変更されると、DHCP クライアントではなく、DHCP サーバーで変更が行われます。クライアント（またはクライアントを再起動する）でネットワークを再起動すると、変更が反映されます。

さらに、ラップトップまたは何らかのタイプのモバイルコンピューターが DHCP 用に設定されている場合は、各オフィスにネットワークへの接続を許可する DHCP サーバーがある限り、オフィスからオフィスに移動できます。

### 23.2. DHCP サーバーの設定

DHCP サーバーを設定するには、`/etc/dhcpd.conf` 設定ファイルを作成する必要があります。サンプルファイルは、`/usr/share/doc/dhcp-<バージョン>/dhcpd.conf.sample` にあります。

DHCP は `/var/lib/dhcp/dhcpd.leases` ファイルを使用してクライアントリースデータベースを保存します。詳細は、「[リースデータベース](#)」を参照してください。

#### 23.2.1. 設定ファイル

DHCP サーバーを設定する最初のステップは、クライアントのネットワーク情報を格納する設定ファイルを作成することです。グローバルオプションはすべてのクライアントに宣言できますが、他のオプションは各クライアントシステムに宣言できます。

設定ファイルには追加のタブや空白行が含まれているため、簡単に書式を整えることができます。キーワードは大文字と小文字を区別せず、ハッシュ記号(#)で始まる行はコメントとみなされます。

現在、2 つの DNS 更新スキームが実装されています。アドホックの DNS 更新モードと、Interim



DHCP-DNS の対話ドラフト更新モードが使用されます。この2つがインターネットエンジニアリングタスクの強制(IETF)標準プロセスの一部として許可される場合、3番目のモード（標準のDNS更新方法）があります。DHCP サーバーは、現在の2つのスキームのいずれか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 以前のバージョンでは ad-hoc モードを使用していましたが、非推奨となっています。同じ動作を維持するには、設定ファイルの最上部に以下の行を追加します。

```
ddns-update-style ad-hoc;
```

推奨されるモードを使用するには、以下の行を設定ファイルの一番上に追加します。

```
ddns-update-style interim;
```

異なるモードの詳細は、`dhcpcd.conf` の `man` ページを参照してください。

設定ファイルのステートメントには、次のような2つのタイプがあります。

- **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、クライアントに送信するネットワーク設定のオプションを規定します。
- **宣言 - ネットワークトポロジの記述、クライアントの記述、クライアントのアドレス指定、宣言グループへのパラメーターグループの適用を行います。**

一部のパラメーターは `option keyword` で開始する必要があり、オプションと呼ばれます。オプションは DHCP オプションを設定します。一方、パラメーターはオプションでないか、または DHCP サーバーの動作を制御する値を設定します。

中括弧({ }) で囲まれたセクションの前に宣言されたパラメーター（オプションを含む）はグローバルパラメーターとみなされます。グローバルパラメーターは、これ以降のすべてのセクションに適用されます。

#### 重要な影響

設定ファイルを変更すると、コマンド `service dhcpcd restart` で DHCP デーモンを再起動するまで変更は反映されません。



## ヒント

DHCP 設定ファイルを変更し、毎回サービスを再起動する代わりに、omshell コマンドを使用して、DHCP サーバーへの接続、クエリー、および設定を変更するインタラクティブな方法を提供します。omshell を使用すると、DHCP サーバーの実行中でも変更を行うことができます。omshell の詳細は、omshell の man ページを参照してください。

**例23.1 「サブネットの宣言」** では、ルーター、subnet-mask、domain-name、domain-name-servers、および time-offset オプションは、以下に宣言された ホスト ステートメントに使用されます。

また、サブネットを宣言することもできます。サブネットは、ネットワーク内のすべてのサブネットに含める必要があります。そうでない場合には、DHCP サーバーは起動できません。

以下の例では、サブネットの DHCP クライアントごとにグローバルオプションがあり、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。

### 例23.1 サブネットの宣言

```
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; # Eastern Standard Time

    range 192.168.1.10 192.168.1.100;
}
```

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23.2 「Shared-network 宣言」** に示されるように shared-network 宣言内で宣言する必要があります。shared-network 内のパラメーターですが、囲まれた subnet 宣言以外は、グローバルパラメーターとみなされます。shared-network の名前は、テストラボ環境内のすべてのサブネットを記述するために「test-lab」というタイトルを使用するなど、ネットワークの説明的なタイトルになります。

### 例23.2 Shared-network 宣言

```
shared-network name {
    option domain-name      "test.redhat.com";
    option domain-name-servers ns1.redhat.com, ns2.redhat.com;
    option routers          192.168.0.254;
```

```

more parameters for EXAMPLE shared-network
subnet 192.168.1.0 netmask 255.255.252.0 {
    parameters for subnet
    range 192.168.1.1 192.168.1.254;
}
subnet 192.168.2.0 netmask 255.255.252.0 {
    parameters for subnet
    range 192.168.2.1 192.168.2.254;
}
}

```

例23.3 「Group 宣言」で説明されているように、**group** 宣言を使用してグローバルパラメーターを宣言のグループに適用することができます。たとえば、共有ネットワーク、サブネット、ホストをグループ化することができます。

### 例23.3 Group 宣言

```

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;
    }
}

```

動的 IP アドレスをサブネット内のシステムにリースする DHCP サーバーを設定するには、例 23.4 「Range パラメーター」を実際の値で変更します。これにより、クライアントのデフォルトのリース時間、最大リース時間、ネットワークの設定値を宣言します。この例では、192.168.1.10 および 192.168.1.100 の範囲の IP アドレスをクライアントシステムに割り当てます。

### 例23.4 Range パラメーター

```

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;
}

```

ネットワークインターフェースカードの MAC アドレスに基づいて IP アドレスをクライアントに割り当てるには、`host` 宣言内の `hardware ethernet` パラメーターを使用します。例23.5「DHCP を使用する静的 IP アドレス」で説明されているように、ホスト `apex` 宣言は、MAC アドレス `00:A0:78:8E:9E:AA` が常に IP アドレス `192.168.1.4` を受信するように指定します。

オプションのパラメーター `host-name` 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できます。

### 例23.5 DHCP を使用する静的 IP アドレス

```

host apex {
    option host-name "apex.example.com";
    hardware ethernet 00:A0:78:8E:9E:AA;
    fixed-address 192.168.1.4;
}

```

#### ヒント

提供される設定ファイルのサンプルは開始点として使用し、カスタム設定オプションを追加できます。これを適切な場所にコピーするには、次のコマンドを使用します。

```
cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf
```

(<version-number> は DHCP バージョン番号)

オプションの説明の一覧と、それらの実行内容については、`dhcp-options` の `man` ページを参照してください。

### 23.2.2. 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` が DHCP クライアントのリースデータ

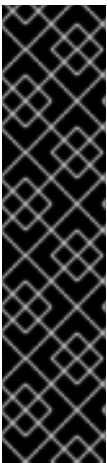
ベースを保存します。このファイルは手動で変更しないでください。最近割り当てられた各 IP アドレスの DHCP リース情報は、リースデータベースに自動的に保存されます。情報には、リースの長さ、IP アドレスの割り当て、リースの開始日と終了日、リースの取得に使用されたネットワークインターフェースカードの MAC アドレスが含まれます。

リースデータベースの毎回、ローカル時間ではなくグリニッジ標準時(GMT)にあります。

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は一時的なリースデータベースに保存されます。dhcpd.leases ファイルの名前は dhcpd.leases~ に変更され、一時的なリースデータベースが dhcpd.leases に書き込まれます。

DHCP デモンを強制終了したり、リースデータベースがバックアップファイルに変更した後に、新規ファイルを書き込む前にシステムをクラッシュさせる可能性があります。この場合、dhcpd.leases ファイルは存在しませんが、サービスを起動する必要があります。この際、新規のリースファイルを作成しないでください。作成すると、それまでのリースはすべて失われ、多くの問題が発生します。これを解決する方法は、dhcpd.leases~ バックアップファイルの名前を dhcpd.leases に変更して、デーモンを起動することです。

### 23.2.3. サーバーの起動と停止



#### 重要な影響

DHCP サーバーを初めて起動すると、dhcpd.leases ファイルがなければ失敗します。ファイルがない場合は、`touch /var/lib/dhcp/dhcpd.leases` コマンドを使用して作成します。

同じサーバーが DNS サーバーとして BIND を実行している場合でも、named サービスを開始すると dhcpd.leases ファイルが自動的にチェックされるため、この手順は必要ありません。

DHCP サービスを起動するには、コマンド `/sbin/service dhcpd start` 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。

デフォルトでは、DHCP サービスは起動時に起動しません。システムの起動時にデーモンが自動的に起動するように設定するには、サービスの管理方法に関する情報は [19章](#) を参照してください。

複数のネットワークインターフェースがシステムにアタッチされていて、DHCP サーバーをいずれかのインターフェースで起動する必要がある場合は、DHCP サーバーがそのデバイスでのみ起動するよ

うに設定します。/etc/sysconfig/dhcpd で、インターフェース名を DHCPDARGS の一覧に追加します。

```
# Command line options here
DHCPDARGS=eth0
```

これは、ネットワークカードが2つあるファイアウォールマシンで役立ちます。1つのネットワークカードを DHCP クライアントとして設定すると、インターネットに IP アドレスを取得できます。他のネットワークカードは、ファイアウォールの内側にある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のみを指定すると、ユーザーがインターネットを介してデーモンに接続できないので、システムの安全性が向上します。

/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、以下が含まれます。

- **-p <portnum>** - dhcpd がリッスンする UDP ポート番号を指定します。デフォルト値はポート 67 です。DHCP サーバーは、指定された UDP ポートよりも大きいポート番号で DHCP クライアントに応答を送信します。たとえば、デフォルトのポート 67 を使用すると、サーバーはポート 67 でリッスンし、ポート 68 のクライアントへのリクエストと応答をリッスンします。ポートを指定して DHCP リレーエージェントを使用する場合は、DHCP リレーエージェントがリッスンするポートと同じポートを指定する必要があります。詳細は、「[DHCP リレーエージェント](#)」を参照してください。
- **-f** - デーモンをフォアグラウンドプロセスとして実行します。これは主にデバッグ用に使用されます。
- **-d** - DHCP サーバーデーモンを標準のエラー記述子に記録します。これは主にデバッグ用に使用されます。このオプションを指定しないと、ログは /var/log/messages に書き込まれます。
- **-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は、DHCP サーバーを起動するたびに同じファイルを使用することが非常に重要になります。このオプションは、実稼働環境以外のマシンでデバッグする目的にのみ使用することが強く推奨されます。デフォルトの場所は /var/lib/dhcp/dhcpd.leases です。
- **-q** - デーモンの起動時に著作権に関するメッセージ全体を表示しません。



### 23.2.4. DHCP リレーエージェント

DHCP リレーエージェント(dhcrelay)では、DHCP サーバーを使用しないサブネットから、他のサブネット上の1つ以上のDHCP サーバーに、DHCP および BOOTP 要求のリレーを行うことができます。

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、DHCP リレーエージェントの起動時に指定したDHCP サーバーの一覧に要求を転送します。DHCP サーバーが応答を返すと、応答は元の要求を送信したネットワーク上でブロードキャストまたはユニキャストになります。

DHCP リレーエージェントは、インターフェースが `INTERFACES` ディレクティブで `/etc/sysconfig/dhcrelay` に指定されていない限り、すべてのインターフェースのDHCP 要求をリッスンします。

DHCP リレーエージェントを起動するには、コマンド `service dhcrelay start` を使用します。

### 23.3. 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手順は、カーネルがネットワークインターフェースカードを認識していることを確認することです。ほとんどのカードはインストールプロセス時に認識され、システムはカードに正しいカーネルモジュールを使用するように設定されます。インストール後にカードが追加される場合、Kudzu<sup>[6]</sup> これを認識し、対応するカーネルモジュールの設定を求めるプロンプトを出す必要があります。<http://hardware.redhat.com/hcl/> で利用可能なハードウェア互換性一覧を確認してください。ネットワークカードがインストールプログラムまたは Kudzu によって設定されていない場合で、読み込むカーネルモジュールが分かっている場合は、カーネルモジュールの読み込みの詳細は、[37章カーネルモジュール](#) を参照してください。

DHCP クライアントを手動で設定するには、`/etc/sysconfig/network` ファイルを変更して、`/etc/sysconfig/network-scripts` ディレクトリー内の各ネットワークデバイスのネットワークおよび設定ファイルを有効にします。このディレクトリーでは、各デバイスに `ifcfg-eth0` という名前の設定ファイルがなければなりません。ここで、`eth0` はネットワークデバイス名です。

`/etc/sysconfig/network` ファイルには、以下の行が含まれている必要があります。

```
NETWORKING=yes
```

ネットワークがブート時に起動するようにするには、`NETWORKING` 変数は `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、以下の行が含まれているはずですが。

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

各デバイスが DHCP を使用するように設定するには、設定ファイルが必要です。

ネットワークスクリプトの他のオプションには以下が含まれます。

- **DHCP\_HOSTNAME:** DHCP サーバーが IP アドレスを受信する前にクライアントがホスト名を指定する必要がある場合にのみこのオプションを使用します。(Red Hat Enterprise Linux の DHCP サーバーデーモンはこの機能をサポートしません。)
- **PEERDNS= <answer>.** ここで、&lt ;answer&gt; は以下のいずれかになります。
  - はい: サーバーの情報を使用して `/etc/resolv.conf` を変更します。DHCP を使用している場合は、`yes` がデフォルトになります。
  - **No:** `/etc/resolv.conf` は変更しないでください。
- **SRCADDR= <address>.** ここで、&lt ;address&gt; は送信パケットの指定されたソース IP アドレスになります。
- **USERCTL= <answer>.** ここで、&lt ;answer&gt; は以下のいずれかになります。
  - はい - `root` 以外のユーザーはこのデバイスを制御できます。
  - **No** - `root` 以外のユーザーはこのデバイスを制御することはできません。

グラフィカルインターフェースを使用する場合は、**Network Administration Tool** を使用して DHCP を使用するようにネットワークインターフェースを設定する方法の詳細は、[17章Network](#)



**Configuration** を参照してください。



#### ヒント

プロトコルタイミング、リース要件、要求、動的 DNS サポート、エイリアス、クライアント側の設定の上書き、追加、または追加するさまざまな値など、クライアント DHCP オプションの高度な設定は、man ページの `dhclient` および `dhclient.conf` を参照してください。

### 23.4. 関連情報

ここで説明されていない設定オプションについては、以下のリソースを参照してください。

#### 23.4.1. インストールされているドキュメント

- `dhcpcd man` ページ - DHCP デーモンの動作が説明されています。
- `man` ページの `dhcpcd.conf` - DHCP 設定ファイルの設定方法を検討し、いくつかの例が含まれています。
- `dhcpcd.leases man` ページ - DHCP リースファイルの設定方法を確認してください。例が含まれています。
- `man` ページの `dhcp-options` - `dhcpcd.conf` で DHCP オプションを宣言する構文には、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およびその設定オプションを説明します。
- `/usr/share/doc/dhcp-<バージョン>/:` DHCP サービスの特定バージョンのサンプルファイル、`README` ファイル、およびリリースノートが含まれています。

#### [6]

`kudzu` は、システムの起動時にハードウェアプロービングツールを実行し、システムから追加または削除されたハードウェアを判断します。

## 第24章 APACHE HTTP サーバーの設定

Red Hat Enterprise Linux は、Apache HTTP Server のバージョン 2.0 を提供します。既存の設定ファイルを手動で移行する場合は、`/usr/share/doc/httpd- <ver> /migration.html` または『リファレンスガイド』を参照してください。

以前のバージョンの Red Hat Enterprise Linux で HTTP 設定ツールで Apache HTTP Server を設定し、アップグレードを実行している場合は、HTTP Configuration Tool を使用して設定ファイルをバージョン 2.0 の新しい形式に移行できます。HTTP Configuration Tool を起動し、設定に変更を加えて保存します。保存される設定ファイルは、バージョン 2.0 と互換性があります。

HTTP 設定ツールを使用するには、`httpd` パッケージおよび `system-config-httpd RPM` パッケージをインストールする必要があります。また、X Window System と root アクセスも必要です。アプリケーションを起動するには、Main Menu Button => System Settings => Server Settings => HTTP に移動するか、シェルプロンプトで `system-config-httpd` コマンド (XTerm や GNOME ターミナルなど) を入力します。

HTTP Configuration Tool を使用すると、Apache HTTP Server の `/etc/httpd/conf/httpd.conf` 設定ファイルを設定できます。古い `srm.conf` または `access.conf` 設定ファイルを使用せず、空白のままにします。グラフィカルインターフェースでは、仮想ホスト、ロギング属性、および最大接続数などのディレクティブを設定できます。

Red Hat Enterprise Linux で提供されるモジュールのみが、HTTP Configuration Tool で設定できます。追加のモジュールがインストールされている場合は、このツールを使用して設定できません。



### WARNING

このツールを使用する場合は、手動で `/etc/httpd/conf/httpd.conf` 設定ファイルを編集しないでください。HTTP Configuration Tool は、変更を保存し、プログラムを終了するとこのファイルを生成します。HTTP Configuration Tool で利用できないモジュールまたは設定オプションを追加する場合は、このツールは使用できません。

HTTP Configuration Tool を使用して Apache HTTP Server を設定する一般的な手順は次のとおりです。

1. **Main** タブで基本的な設定を行います。
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 または仮想ホストを提供するには、仮想ホストを追加します。
5. **Server** タブでサーバー設定を行います。
6. **Performance Tuning** タブで接続設定を行います。
7. 必要なすべてのファイルを **DocumentRoot** と **cgi-bin** ディレクトリーにコピーします。
8. アプリケーションを終了し、選択して設定を保存します。

### 24.1. 基本設定

**Main** タブを使用して、基本的なサーバー設定を構成します。

図24.1 基本設定

The screenshot shows a dialog box with four tabs: Main, Virtual Hosts, Server, and Performance Tuning. The 'Main' tab is selected. Under 'Basic Setup', there is a 'Server Name' text field (empty) and a 'Webmaster email address' text field containing 'root@localhost'. Below this is an 'Available Addresses' section with a list box containing 'All available addresses on port 80'. To the right of the list box are three buttons: 'Add...', 'Edit...', and 'Delete'. At the bottom of the dialog are three buttons: 'OK' (with a green checkmark icon), 'Cancel' (with a red X icon), and 'Help' (with a question mark icon). A note at the bottom of the dialog reads 'Set addresses for Apache to listen for requests on.'

[D]

**Server Name** テキスト領域で使用する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` ディレクティブに対応します。`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。これはリダイレクト URL の作成時に使用されます。サーバー名を定義しない場合、Web サーバーはシステムの IP アドレスから解決しようとしています。サーバー名は、サーバーの IP アドレスから解決したドメイン名であ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` の場合に、サーバー名を `www.example.com` に設定します。

**Web master** のメールアドレステキストエリアで Web サーバーを維持するユーザーの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` ディレクティブに対応します。サーバーのエラーページにメールアドレスが含まれる場合、ユーザーがサーバーの管理者に問題を報告できるようにこのメールアドレスが使用されます。デフォルト値は `root@localhost` です。

**利用可能なアドレス** エリアを使用して、サーバーが受信要求を受け入れるポートを定義します。このオプションは、`httpd.conf` の `Listen` ディレクティブに対応します。デフォルトでは、Red Hat は Apache HTTP Server が、セキュアでない Web 通信に対してポート 80 をリッスンするように設定します。

**追加** ボタンをクリックして、要求を受け入れる追加のポートを定義します。図24.2「利用可能なアドレス」に示されているウィンドウが表示されます。定義されたポートの全 IP アドレスをリッスンするには、`Listen to all addresses` オプションを選択するか、サーバーが `Address` フィールドで接続を受け入れる特定の IP アドレスを指定します。ポート番号ごとに 1 つの IP アドレスのみを指定します。

同じポート番号を持つ複数の IP アドレスを指定するには、各 IP アドレスのエントリーを作成します。可能な限り、ドメイン名の代わりに IP アドレスを使用し、DNS ルックアップの失敗を防ぎます。

『DNS および Apache の問題』の詳細は、<http://httpd.apache.org/docs-2.0/dns-caveats.html> を参照してください。

**Address** フィールドにアスタリスク(\*)を入力することは、すべてのアドレスに対して **Listen** を選択する場合と同じです。利用可能なアドレス フレームの **編集** ボタンをクリックすると、選択したエントリーにフィールドが入力された以外の **Add** ボタンと同じウィンドウが表示されます。エントリーを削除するには、エントリーを選択して **削除** ボタンをクリックします。



#### ヒント

サーバーが 1024 未満のポートをリッスンするように設定する場合は、起動するには **root** にする必要があります。ポート 1024 以上では、**httpd** を一般ユーザーとして起動できます。

図24.2 利用可能なアドレス

The dialog box contains the following elements:

- A question mark icon on the left.
- Radio button:  Listen to all addresses
- Radio button:  Address: 192.168.1.4
- Text field: Port: 80
- Buttons:  and

[D]

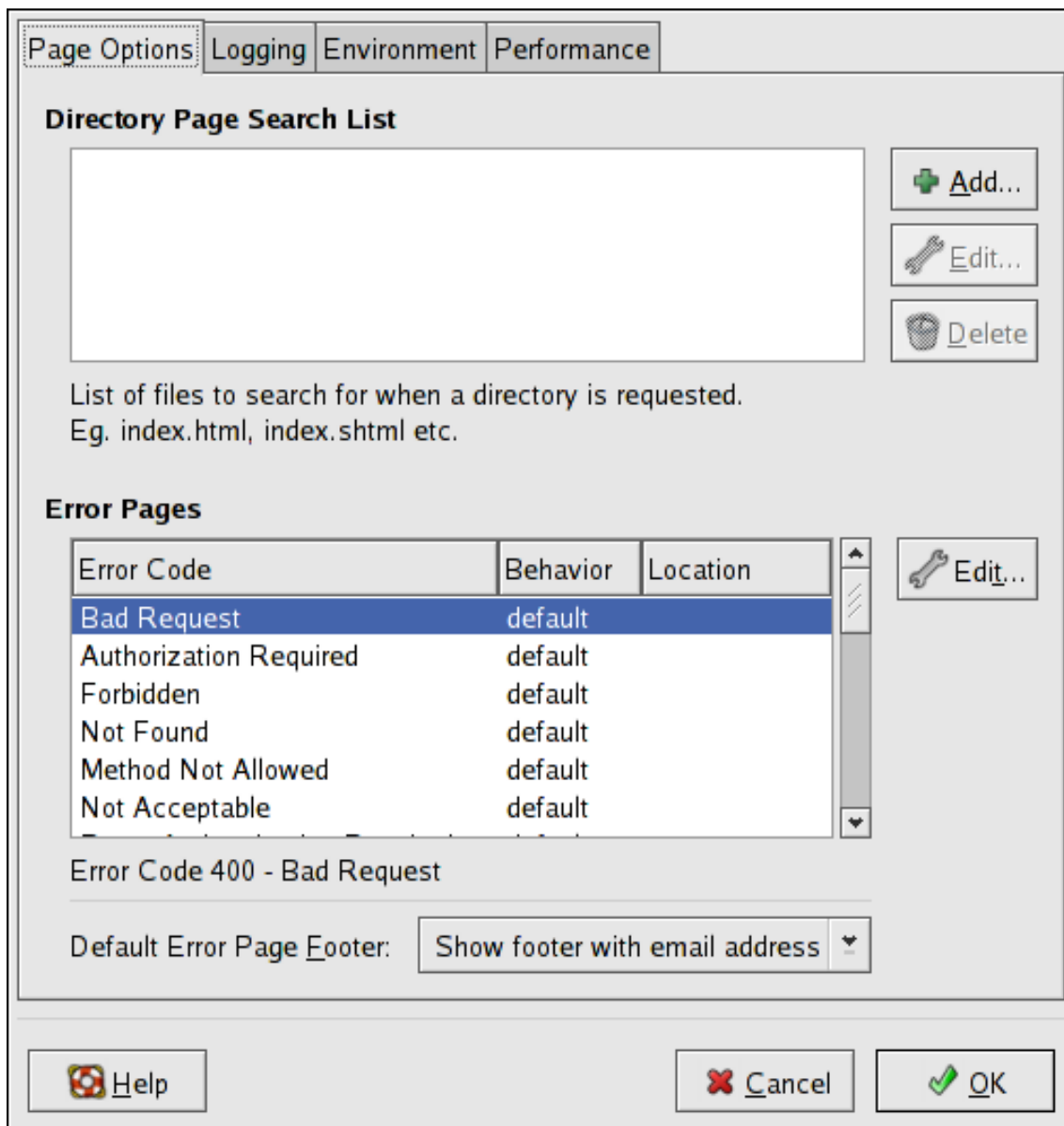
## 24.2. デフォルトの設定

**Server Name**、**Webmaster** のメールアドレス、および **利用可能なアドレス** を定義したら、**仮想ホスト** タブをクリックして、**デフォルト設定の編集** ボタンをクリックします。図24.3「**サイトの設定**」に示されている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を設定します。仮想ホストを追加する場合、仮想ホストに設定した設定がその仮想ホストに優先されます。仮想ホスト設定内に定義されていないディレクティブについては、デフォルト値が使用されます。

### 24.2.1. サイトの設定

**Directory Page Search List** および **Error Pages** のデフォルト値は、ほとんどのサーバーで機能します。これらの設定が分からない場合は、変更しないでください。

図24.3 サイトの設定



[D]

**Directory Page Search List** に一覧表示されているエントリは **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ー名の最後にスラッシュ(/)を指定してディレクトリーのインデックスを要求する際にサーバーによって提供されるデフォルトページです。

たとえば、ユーザーがページ `http://www.example.com/this_directory/` をリクエストすると、**DirectoryIndex** ページ（存在する場合）またはサーバー生成ディレクトリーリストのいずれかが取得されます。サーバーは **DirectoryIndex** ディレクティブにリストされているファイルの1つを見つけ、最初に見つかったファイルを返します。このファイルが見つからない場合や、そのディレクトリーに **Options Indexes** が設定されている場合、サーバーはディレクトリー内のサブディレクトリーおよびファイルの **HTML** 形式でリストを生成し、返します。

**Error Code** セクションを使用して、問題やエラーが発生した場合にクライアントをローカルまたはリモートの URL にリダイレクトするように **Apache HTTP Server** を設定します。このオプションは

**ErrorDocument** ディレクティブに対応します。クライアントが Apache HTTP Server に接続しようとする際に問題が発生した場合に、デフォルトのアクションは **Error Code** 列に表示される短いエラーメッセージを表示します。このデフォルト設定を上書きするには、エラーコードを選択し、**Edit** ボタンをクリックします。**Default** を選択して、デフォルトの短いエラーメッセージを表示します。クライアントを外部 URL にリダイレクトする URL を選択し、**http://** を含む完全な URL を **Location** フィールドに入力します。**File** を選択して、クライアントを内部 URL にリダイレクトし、Web サーバーのドキュメントルートの下にファイルの場所を入力します。場所はスラッシュ(/)を開始し、**Document Root** と相対的である必要があります。

たとえば、404 Not Found エラーコードを 404.html ファイルで作成した Web ページにリダイレクトするには、404.html を **DocumentRoot/./error/404.html** にコピーします。この場合、**DocumentRoot** は定義した **Document** ルートディレクトリーです（デフォルトは **/var/www/html/** です）。**Document Root** がデフォルトの場所に残っている場合は、そのファイルを **/var/www/error/404.html** にコピーする必要があります。404 - Not Found エラーコードとして **File** を選択し、**Location** に **/error/404.html** を入力します。

デフォルトの **Error Page Footer** メニューから、以下のオプションのいずれかを選択できます。

- メールアドレスと共にフッターを表示 - すべてのエラーページの下部にあるデフォルトのフッターと、**ServerAdmin** ディレクティブで指定された Web サイトメンテナの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関する情報は、「**一般的なオプション**」を参照してください。
- **show footer** - エラーページの下部にデフォルトのフッターのみを表示します。
- フッターなし - エラーページ下部にフッターは表示されません。

### 24.2.2. ロギング

**Logging** タブを使用して、特定の転送およびエラーログのオプションを設定します。

デフォルトでは、サーバーは転送ログを **/var/log/httpd/access\_log** ファイルに書き込みます。エラーログは **/var/log/httpd/error\_log** ファイルに記録されます。

転送ログには、Web サーバーへのアクセス試行の一覧が含まれます。接続しようとしているクライアントの IP アドレス、試行の日時、および取得しようとしている Web サーバーのファイルを記録します。この情報を保存するパスおよびファイルの名前を入力します。パスとファイル名がスラッシュ(/)で開始されない場合、パスは設定済みのサーバールートディレクトリーに対する相対パスになります。このオプションは **TransferLog** ディレクティブに対応します。



図24.4 ログイン

Page Options	<b>Logging</b>	Environment	Performance
<b>Transfer Log</b>			
<input checked="" type="radio"/> Log to File:	<input type="text" value="logs/access_log"/>		
<input type="radio"/> Log to Program:	<input type="text"/>		
<input type="radio"/> Use System Log:	<input type="text"/>		
<input type="checkbox"/> Use custom logging facilities			
Custom Log String:	<input type="text"/>		
<b>Error Log</b>			
<input checked="" type="radio"/> Log to File:	<input type="text" value="logs/error_log"/>		
<input type="radio"/> Log to Program:	<input type="text"/>		
<input type="radio"/> Use System Log:	<input type="text"/>		
Log Level:	<input type="text" value="Error"/>		▼
Reverse DNS Lookup:	<input type="text" value="Reverse Lookup"/>		▼
<input type="button" value="Help"/> <input type="button" value="Cancel"/> <input type="button" value="OK"/>			

[D]

**Use custom logging facility** を確認し、**Custom Log String** フィールドにカスタム ログ文字列を入力して、カスタムログ形式を設定できます。これにより、**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関する詳細は、[http://httpd.apache.org/docs-2.0/mod/mod\\_log\\_config.html#formats](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、発生したサーバーエラーの一覧が含まれます。この情報を保存するパスおよびファイルの名前を入力します。パスとファイル名がスラッシュ(/)で開始されない場合、パスは設定済みのサーバールートディレクトリーに対する相対パスになります。このオプションは **ErrorLog** ディレクティブに対応します。

**Log Level** メニューを使用して、エラーログでエラーメッセージの詳細レベルを設定します。これは (詳細度の低いものから) **emerg**、**alert**、**crit**、**error**、**warn**、**notice**、**info**、または **debug** に設定



できます。このオプションは **LogLevel** ディレクティブに対応します。

**Reverse DNS Lookup** メニューで選択する値は **HostnameLookups** ディレクティブを定義します。No Reverse Lookup を選択すると、値を off に設定します。Reverse Lookup を選択すると、値が on に設定されます。Double Reverse Lookup を選択すると、値が double に設定されます。

**Reverse Lookup** を選択すると、サーバーは Web サーバーからドキュメントを要求する各接続の IP アドレスを自動的に解決します。IP アドレスを解決すると、特定の IP アドレスに対応するホスト名を確認するために、お使いのサーバーが DNS への接続を行うことを意味します。

**Double Reverse Lookup** を選択すると、サーバーは二重の逆引き DNS を実行します。つまり、逆引きルックアップが実行された後に、結果にフォワードルックアップが実行されます。正引きルックアップの IP アドレスが少なくとも 1 つと、最初の逆引きルックアップのアドレスと一致する必要があります。

DNS 要求がサーバーに負荷を追加し、停止する可能性があるため、通常はこのオプションを No Reverse Lookup に設定したままにする必要があります。サーバーがビジー状態になると、これらの逆引きルックアップの実行や二重の逆ルックアップの影響は非常に気づかる可能性があります。

逆引きルックアップと二重の逆引き検索も、インターネット全体の問題です。各ホスト名を検索するために作成された各接続が加算されます。そのため、独自の Web サーバーやインターネットの利点のために、このオプションは No Reverse Lookup に設定されたままにする必要があります。

### 24.2.3. 環境変数

**Environment** タブを使用して、CGI スクリプトの設定、パス、または未設定を行う特定の変数のオプションを設定します。

CGI スクリプトまたはサーバー側の include(SSI)ページの環境変数を変更する必要がある場合があります。Apache HTTP Server は mod\_env モジュールを使用して、CGI スクリプトおよび SSI ページに渡される環境変数を設定できます。環境変数 ページを使用して、このモジュールのディレクティブを設定します。

**Set for CGI scripts** セクションを使用して、CGI スクリプトおよび SSI ページに渡される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24.5 「環境変数」](#) に示されるように **Set for CGI Script** セクションの **Add** ボタンをクリックしてから、「**Environment Variable text**」フィールドに MAXNUM を入力し、Value に 50 と入力してテキストフィールドを設定します。OK をクリックして一覧に追加します。**Set for CGI scripts** セクションで、**SetEnv** ディレクティブを設定します。

**Pass to CGI scripts** セクションを使用して、サーバーが最初に CGI スクリプト を起動するときに環境変数の値を渡します。この環境変数を表示するには、シェルプロンプトでコマンド `env` を入力します。**Pass to CGI Scripts** セクション内の **Add** ボタンをクリックし、結果として表示され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 をクリックして一覧に追加します。**Pass to CGI scripts** セクションで、**PassEnv** ディレクティブを設定します。

図24.5 環境変数

[D]

値が CGI スクリプトおよび SSI ページに渡されないように環境変数を削除するには、**Unset for CGI scripts** セクションを使用します。**Unset for CGI Scripts** セクションで **Add** 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。OK をクリックして一覧に追加します。これは **UnsetEnv** ディレクティブに対応します。

これらの環境値のいずれかを編集するには、一覧から選択し、対応する **Edit** ボタンをクリックします。一覧からエントリーを削除するには、エントリーを選択して、対応する **Delete** ボタンをクリック

します。

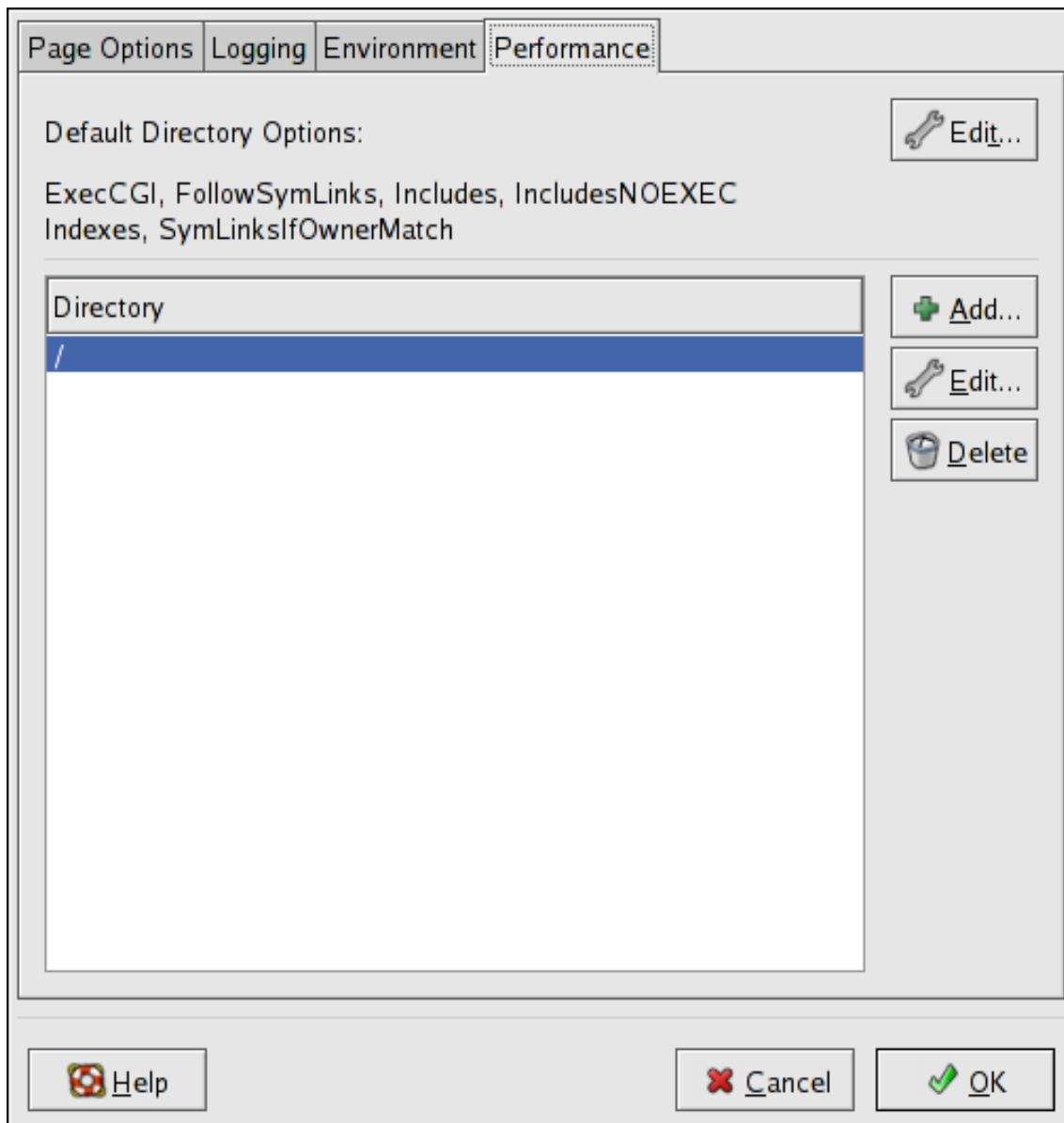
Apache HTTP Server の環境変数の詳細は、以下を参照してください。

<http://httpd.apache.org/docs-2.0/env.html>

#### 24.2.4. ディレクトリー

Performance タブの *directories* ページを使用して、特定のディレクトリーのオプションを設定します。これは < *Directory* > ディレクティブに対応します。

図24.6 ディレクトリー



[D]

右上隅の **Edit** ボタンをクリックして、その下の **Directory** 一覧に指定されていないすべてのディレクトリーに **Default Directory Options** を設定します。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することができます。

- **ExecCGI** - CGI スクリプトの実行を許可します。このオプションが選択されていない場合は、CGI スクリプトは実行されません。
- **FollowSymLinks** - シンボリックリンクのフォローを許可します。
- **includes**: サーバー側の インクルード を許可します。
- **IncludesNOEXEC** - サーバー側のインクルードを許可しますが、CGI スクリプトで **#exec** コマンドおよび **#include** コマンドを無効にします。
- **Index**: ( **index.html** などの ) **DirectoryIndex** が要求されたディレクトリーに存在しない場合は、ディレクトリーの内容のフォーマットされた一覧を表示します。
- **Multiview** - コンテンツをネゴシエートした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無効になっています。
- **SymLinksIfOwnerMatch**: ターゲットファイルまたはディレクトリーがリンクと同じ所有者を持つ場合に限り、シンボリックリンクをたどります。

特定のディレクトリーのオプションを指定するには、**Directory** リストボックスの横にある **Add** ボタンをクリックします。図24.7「ディレクトリー設定」に示されているウィンドウが表示されます。ウィンドウ下部の **Directory** テキストフィールドに、設定するディレクトリーを入力します。右側のオプションを選択し、左側のオプションで **Order** ディレクティブを設定します。**Order** ディレクティブは、**allow** ディレクティブおよび **deny** ディレクティブが評価される順序を制御します。**Allow hosts from text** フィールドで、以下の1つを指定できます。

- **Allow all hosts**: **all** と入力して、すべてのホストへのアクセスを許可します。
- **部分的なドメイン名**: 指定の文字列に一致する名前または終了ホスト名を持つすべてのホストを許可します。

- 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します。
- サブネット : Such 192.168.1.0/255.255.255.0
- ネットワークの CIDR 仕様 (例 : ) 10.3.0.0/16

図24.7 ディレクトリー設定

The screenshot shows the Apache Directory Settings dialog box. It is divided into several sections:

- Order:** Three radio buttons are present. The first is 'Let all hosts access this directory'. The second is 'Process Deny list before Allow list'. The third, 'Process Allow list before Deny list', is selected.
- Deny List:** Two radio buttons are present. The first, 'Deny access from all hosts', is selected. The second is 'Deny hosts from:' followed by an empty text box.
- Allow List:** Two radio buttons are present. The first is 'Allow access from all hosts'. The second, 'Allow hosts from:', is selected and followed by a text box containing '192.168.1.0/255.255.255.0'.
- Options:** A list of options with checkboxes. 'ExecCGI', 'FollowSymLinks', 'Includes', 'IncludesNOEXEC', 'Indexes', and 'SymLinksIfOwnerMatch' are checked. 'MultiViews' is unchecked. Below this list is a checkbox for 'Let .htaccess files override directory options', which is also unchecked.
- Directory:** A text box containing the path '/var/www/html/testing'.
- Buttons:** At the bottom, there are three buttons: 'Help' (with a question mark icon), 'OK' (with a green checkmark icon), and 'Cancel' (with a red X icon).

[D]

Let .htaccess ファイルがディレクトリーオプションを上書きすると、.htaccess ファイルの設定ディレクティブが優先されます。

### 24.3. 仮想ホストの設定

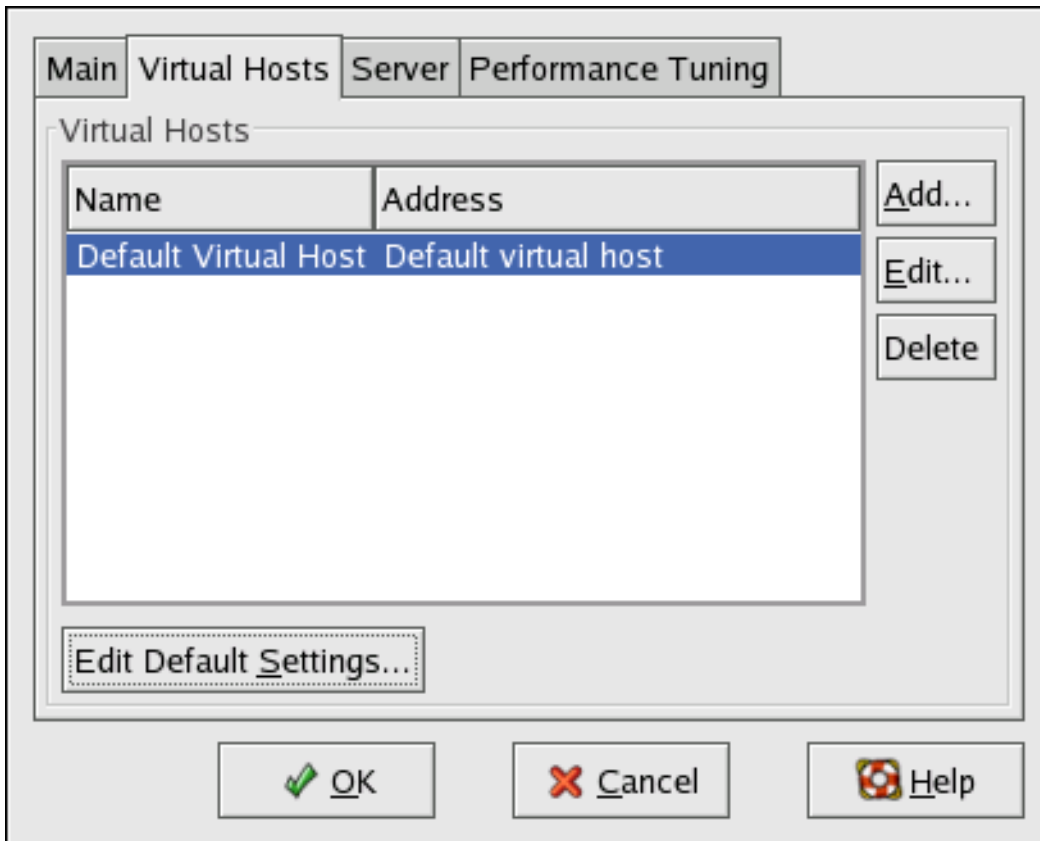
仮想ホストを使用すると、同じマシン上で異なる IP アドレス、異なるホスト名、または異なるポートに対して異なるサーバーを実行できます。たとえば、仮想ホストを使用して、同じ Web サーバーで `http://www.example.com` と `http://www.anotherexample.com` の Web サイトを実行することができます。このオプションは、デフォルトの仮想ホストおよび IP ベースの仮想ホストの `<VirtualHost>` ディレクティブに対応します。名前ベースの仮想ホストの `<NameVirtualHost>` ディレクティブに対応します。

仮想ホストに設定されたディレクティブは、その特定の仮想ホストにのみ適用されます。ディレクティブが `Edit Default Settings` ボタンを使用してサーバー全体で設定され、仮想ホスト設定内で定義さ

れていないと、デフォルト設定が使用されます。たとえば、Main タブで Webmaster のメールアドレスを定義し、各仮想ホストに個別のメールアドレスを定義することはできません。

HTTP Configuration Tool には、[図24.8「仮想ホスト」](#)に示されるようにデフォルトの仮想ホストが含まれます。

図24.8 仮想ホスト



[D]

<http://httpd.apache.org/docs-2.0/vhosts/> およびマシンの Apache HTTP Server ドキュメントでは、仮想ホストに関する詳細情報が提供されています。

### 24.3.1. 仮想ホストの追加と編集

仮想ホストを追加するには、仮想ホストタブをクリックしてから追加ボタンをクリックします。また、仮想ホストを選択して編集ボタンをクリックして編集することもできます。

#### 24.3.1.1. 一般的なオプション

General Options 設定は、設定する仮想ホストにのみ適用されます。仮想ホスト名のテキストエリアに仮想ホストの名前を設定します。この名前は、仮想ホストを区別するために HTTP Configuration Tool によって使用されます。

**Document Root Directory** の値を、仮想ホストのルートドキュメント (`index.html` など) が含まれるディレクトリーに設定します。このオプションは、`< VirtualHost >` ディレクティブ内の **DocumentRoot** ディレクティブに対応します。デフォルトの **DocumentRoot** は `/var/www/html` です。

**Webmaster** のメールアドレスは、**VirtualHost** ディレクティブ内の **ServerAdmin** ディレクティブに対応します。エラーページにメールアドレスのあるフッターを表示する場合は、このメールアドレスはエラーページのフッターで使用されます。

**Host Information** セクションで、**Default Virtual Host**、**IP ベースの仮想ホスト**、または **Name based Virtual Host** を選択します。

### デフォルトの仮想ホスト

デフォルトの仮想ホストは 1 つのみ設定する必要があります (デフォルトでは設定が 1 つあることに注意してください)。デフォルトの仮想ホスト設定は、要求された IP アドレスが別の仮想ホストに明示的に一覧表示されない場合に使用されます。デフォルトの仮想ホストが定義されていない場合は、メインのサーバー設定が使用されます。

### 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ウィンドウが表示されます。この IP アドレスを **IP address** フィールドに指定します。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。ポートを指定するには、構文 `IP Address:Port` を使用します。「colon, asterisk」(:\*)を使用して、IP アドレスの全ポートを設定します。**Server Host Name** 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

**Name based Virtual Host** 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ウィンドウが表示されます。IP アドレス フィールドに 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。ポートを指定するには、構文 `IP Address:Port` を使用します。「colon, asterisk」(:\*)を使用して、IP アドレスの全ポートを設定します。**Server Host Name** フィールドに仮想ホストのホスト名を指定します。**Aliases** セクションで、**Add** をクリックしてホスト名のエイリアスを追加します。エイリアスを追加すると、**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。

#### 24.3.1.2. SSL





## 備考

SSL ハンドシェイク（ブラウザがセキュアな Web サーバーの証明書を受け入れる場合）は、適切な名前ベースの仮想ホストを識別する HTTP 要求の前に行われるため、SSL で名前ベースの仮想ホストを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 サーバーでのみ機能することに注意してください。

図24.9 SSL サポート

General Options	Page Options	SSL	Logging	Environment	Performance						
<input checked="" type="checkbox"/> Enable SSL support											
<b>SSL Configuration</b>											
Certificate File:		/etc/httpd/conf/ssl.crt/server.crt									
Certificate Key File:		/etc/httpd/conf/ssl.key/server.key									
Certificate Chain File:		/etc/httpd/conf/ssl.crt/ca.crt									
Certificate Authority File:		/etc/httpd/conf/ssl.crt/ca-bundle.crt									
<table border="1"> <thead> <tr> <th>SSL Options</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> FakeBasicAuth</td> </tr> <tr> <td><input type="checkbox"/> ExportCertData</td> </tr> <tr> <td><input type="checkbox"/> CompatEnvVars</td> </tr> <tr> <td><input type="checkbox"/> StrictRequire</td> </tr> <tr> <td><input type="checkbox"/> OptRenegotiate</td> </tr> </tbody> </table>						SSL Options	<input type="checkbox"/> FakeBasicAuth	<input type="checkbox"/> ExportCertData	<input type="checkbox"/> CompatEnvVars	<input type="checkbox"/> StrictRequire	<input type="checkbox"/> OptRenegotiate
SSL Options											
<input type="checkbox"/> FakeBasicAuth											
<input type="checkbox"/> ExportCertData											
<input type="checkbox"/> CompatEnvVars											
<input type="checkbox"/> StrictRequire											
<input type="checkbox"/> OptRenegotiate											
<input type="button" value="Help"/>		<input type="button" value="Cancel"/>		<input type="button" value="OK"/>							

[D]

Apache HTTP Server が SSL サポートで設定されていない場合、Apache HTTP Server とそのクライアント間の通信は暗号化されません。これは、個人情報や機密情報のない Web サイトに適しています。たとえば、オープンソースソフトウェアとドキュメントを配信するオープンソースの Web サイトでは、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を必要とする ecommerce の Web サイトでは、Apache 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 セキュリティーモジュールの使用が可能になります。HTTP Configuration Tool でこれを有効にするには、Main タブ => 利用可能なアドレスのポート 443 経由で



アクセスを許可する必要があります。詳細は、「[基本設定](#)」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て、左側のメニューから SSL を選択し、[図 24.9 「SSL サポート」](#) に示されるように SSL サポートの有効化 オプションを選択します。SSL Configuration セクションは、ダミーのデジタル証明書で事前設定されています。デジタル証明書はセキュアな Web サーバーの認証を提供し、クライアント Web ブラウザーへのセキュアなサーバーを特定します。独自のデジタル証明書を購入する必要があります。Web サイトに提供されるダミーは使用しないでください。CA が承認したデジタル証明書を購入する方法は、[25章Apache HTTP セキュアサーバー設定](#) を参照してください。

### 24.3.1.3. 仮想ホストの追加オプション

仮想ホストのサイト設定、環境変数、およびディレクトリー オプションは、設定する個々の仮想ホストのオプションを除き、デフォルト設定の編集 ボタンをクリックする際に設定したのと同じディレクティブです。これらのオプションの詳細については、「[デフォルトの設定](#)」を参照してください。

## 24.4. サーバー設定

Server タブでは、基本的なサーバー設定を設定できます。これらのオプションのデフォルト設定は、ほとんどの状況に適しています。

図24.10 サーバー設定

Main	Virtual Hosts	Server	Performance Tuning
Lock File: <input type="text" value="/var/lock/httpd.lock"/> <input type="button" value="Browse..."/>			
PID File: <input type="text" value="/var/run/httpd.pid"/> <input type="button" value="Browse..."/>			
Core Dump Directory: <input type="text" value="/etc/httpd"/> <input type="button" value="Browse..."/>			
User: <input type="text" value="apache"/>			
Group: <input type="text" value="apache"/>			
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>			

[D]

Lock File の値は `LockFile` ディレクティブに対応します。このディレクティブは、`USE_FCNTL_SERIALIZED_ACCEPT` または `USE_FLOCK_SERIALIZED_ACCEPT` のいずれかでサー

バーをコンパイルする際に使用するロックファイルへのパスを設定します。ローカルディスクに保存されている必要があります。logs ディレクトリーが NFS 共有にある場合を除き、デフォルト値のままにする必要があります。この場合、デフォルト値はローカルディスクの場所と、root でのみ読み取り可能なディレクトリーに変更する必要があります。

PID File の値は **PidFile** ディレクティブに対応します。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。このファイルは root でのみ読み取りできる必要があります。ほとんどの場合、デフォルト値のままにする必要があります。

Core Dump Directory の値は **CoreDumpDirectory** ディレクティブに対応します。Apache HTTP Server は、コアダンプを実行する前にこのディレクトリーに切り替えようとします。デフォルト値は ServerRoot です。ただし、サーバーが実行されるユーザーがこのディレクトリーへの書き込みができない場合、コアダンプは書き込みできません。デバッグ目的でコアダンプをディスクに書き込む場合は、この値を、サーバーが実行するユーザーが書き込み可能なディレクトリーに変更します。

User の値は **User** ディレクティブに対応します。要求に応答するためにサーバーが使用するユーザー ID を設定します。このユーザー設定は、サーバーへのアクセスを決定します。このユーザーがアクセスできないファイルは、Web サイトにもアクセスできません。User のデフォルト値は apache です。

ユーザーは、外部に表示される予定のファイルにアクセスできるように特権のみを持っている必要があります。ユーザーは、サーバーが生成する CGI プロセスの所有者でもあります。ユーザーは、HTTP リクエストへの応答として意図されていないコードの実行を許可しないでください。



#### WARNING

実行内容を正確に把握していない場合は、User ディレクティブを root に設定しないでください。ユーザーとして root を使用すると、Web サーバー用の大規模なセキュリティーホールが作成されます。

親 httpd プロセスは、最初に通常の操作中に root として実行しますが、続いて apache ユーザーに直ちに渡されます。サーバーは、1024 未満のポートにバインドする必要があるため、root で起動する必要があります。1024 未満のポートはシステムで使用するために予約されているため、root 以外でも使用できません。ただし、サーバー自体がそのポートにアタッチされると、接続要求を受け入れる前に、Apache ユーザーにプロセスを切断します。

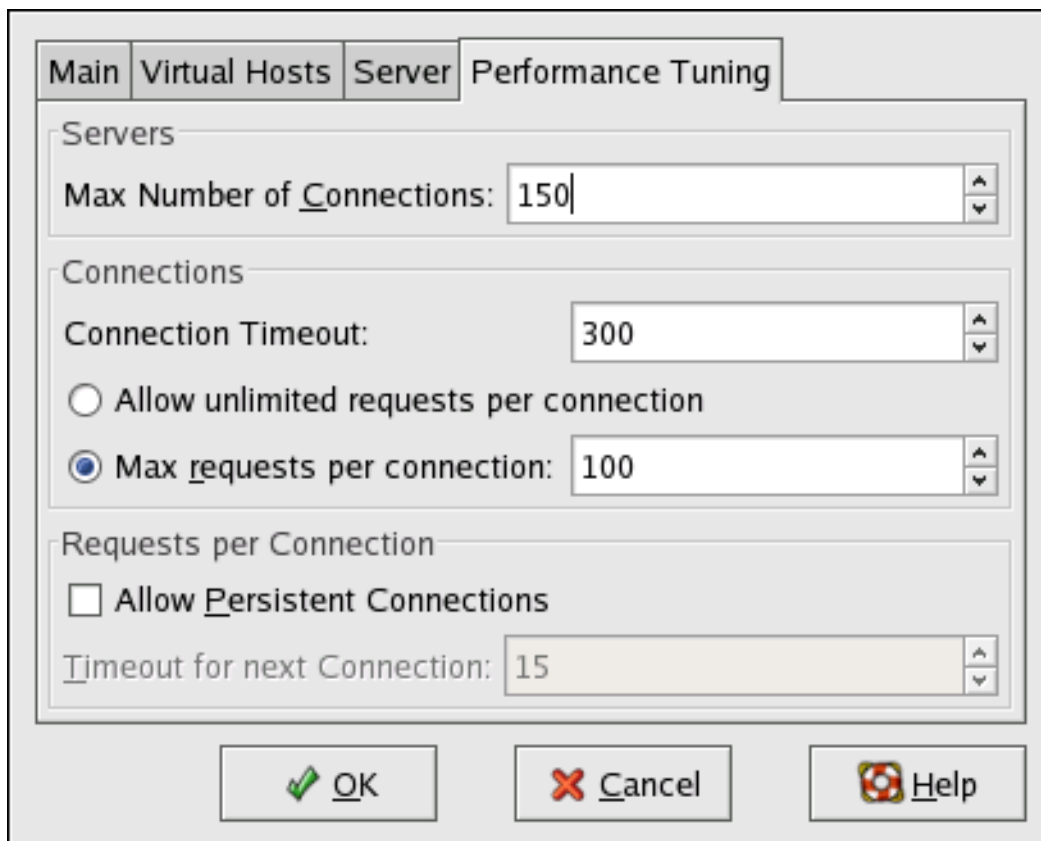
Group の値は **Group** ディレクティブに対応します。Group ディレクティブは User ディレクティブ

に似ています。group は、サーバーが要求に回答するグループを設定します。デフォルトのグループも apache です。

## 24.5. パフォーマンスチューニング

Performance Tuning タブをクリックし、必要な子サーバープロセスの最大数を設定し、クライアント接続に Apache HTTP Server オプションを設定します。これらのオプションのデフォルト設定は、ほとんどの状況に適しています。これらの設定を変更すると、Web サーバーの全体的なパフォーマンスに影響する可能性があります。

図24.11 パフォーマンスチューニング



[D]

**Max Number of Connections** を、サーバーが処理でき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。この最大プロセス数に達すると、子サーバープロセスが解放されるまで、Web サーバーに接続できません。この値は、再コンパイルせずに 256 を超える値に設定することはできません。このオプションは `MaxClients` ディレクティブに対応します。

接続タイムアウトは、通信中にサーバーが受信と送信を待つ時間（秒単位）を定義します。具体的には、接続タイムアウトはサーバーが GET リクエストを受信するのを待つ時間、POST または PUT リクエストで TCP パケットを受信するのを待つ時間、TCP パケットに回答する確認応答の間隔を定義します。デフォルトでは、接続タイムアウトは 300 秒に設定されています。これは、ほとんどの状況に適しています。このオプションは `TimeOut` ディレクティブに対応します。

接続ごとの **Max requests** を、永続接続ごとに許可される最大リクエスト数に設定します。デフォルト値は 100 で、ほとんどの状況で適しています。このオプションは **MaxRequestsPerChild** ディレクティブに対応します。

**Allow unlimited requests per connection** オプションを選択すると、**MaxKeepAliveRequests** ディレクティブは 0 に設定され、無制限の要求が許可されます。

**Allow Persistent Connections** オプションの選択を解除すると、**KeepAlive** ディレクティブが **false** に設定されます。これを確認すると、**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 **Connection** 値の **Timeout** として選択される数字に設定されます。このディレクティブは、リクエストが提供されると、サーバーが接続を閉じるまでサーバーが後続のリクエストを待機する秒数を設定します。リクエストが受信されると、代わりに **Connection Timeout** の値が適用されます。

永続的な接続を高い値に設定すると、接続しようとしているユーザーの数によってはサーバーの速度が遅くなる可能性があります。数値が大きいほど、サーバープロセスは、接続した最後のクライアントからの別の接続を待機しています。

## 24.6. 設定の保存

**Apache HTTP Server** 設定を保存しない場合は、**HTTP Configuration Tool** ウィンドウの右下隅にある **Cancel** ボタンをクリックします。この決定を確認するよう求められます。Yes をクリックしてこの選択を確認すると、設定は保存されません。

**Apache HTTP Server** 設定を保存する場合は、**HTTP Configuration Tool** ウィンドウの右下隅にある **OK** ボタンをクリックします。ダイアログウィンドウが表示されます。Yes と回答すると、設定は `/etc/httpd/conf/httpd.conf` に保存されます。元の設定ファイルは新しい設定で上書きされる点に注意してください。

**HTTP Configuration Tool** を初めて使用した場合には、ダイアログウィンドウが表示され、設定ファイルを手動で変更したことを警告します。**HTTP Configuration Tool** が `httpd.conf` 設定ファイルが手動で変更されたことを検知すると、手動で変更したファイルを `/etc/httpd/conf/httpd.conf.bak` として保存します。



### 重要な影響

設定を保存したら、コマンド `service httpd restart` で `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` でログインしている必要があります。

## 24.7. 関連情報

Apache HTTP Server の詳細は、以下のリソースを参照してください。

### 24.7.1. インストールされているドキュメント

- `/usr/share/docs/httpd- <version> /migration.html`: 『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 への変更の一覧と、設定ファイルを手動で移行する方法を説明します。

### 24.7.2. 便利な Web サイト

- <http://www.apache.org/>: 『Apache Software Foundation』
- <http://httpd.apache.org/docs-2.0/> - Apache HTTP Server バージョン 2.0 向け Apache Software Foundation's ドキュメント ( 『Apache HTTP Server Version 2.0 User's Guide』を含む)

### 24.7.3. 関連書籍

- 『apache:』 Ben Laurie および pid Laurie; O'Reilly & Associates, Inc.
- 『リファレンスガイド』 ; Red Hat, Inc - このコンパニオンマニュアルには、Apache HTTP Server バージョン 1.3 から Apache HTTP Server バージョン 2.0 に手動で移行する手順、Apache HTTP Server ディレクティブの詳細、および Apache HTTP Server へのモジュールの追加手順が含まれています。

## 第25章 APACHE HTTP セキュアサーバー設定

### 25.1. はじめに

本章では、OpenSSL ライブラリーおよびツールキットを使用できるように `mod_ssl` セキュリティーモジュールが有効になっている Apache HTTP Server に関する基本的な情報を提供します。これらの 3 つのコンポーネントの組み合わせは、本章ではセキュアな Web サーバー、またはセキュアサーバーとして参照されます。

`mod_ssl` モジュールは Apache HTTP Server のセキュリティーモジュールです。 `mod_ssl` モジュールは、OpenSSL プロジェクトが提供するツールを使用して、Apache HTTP Server に非常に重要な機能を追加します。これは、通信を暗号化する機能です。一方、ブラウザと Web サーバー間の通常の HTTP 通信はプレーンテキストで送信されます。これは、ブラウザとサーバー間のルートを傍受および読み取りできます。

本章は、これらのプログラムの完全なドキュメントおよび排他的なドキュメントではありません。可能な場合には、本書では特定の対象についてより詳細なドキュメントを見つけることができる適切な場所を参照します。

本章では、これらのプログラムをインストールする方法を説明します。秘密鍵と証明書要求の生成に必要な手順、独自の自己署名証明書の生成方法、およびセキュアなサーバーで使用する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` にあります。このファイルを読み込むには、`mod_ssl` を機能させるには、`/etc/httpd/conf/httpd.conf` ファイルに `Include conf.d/*.conf` ステートメントが必要です。このステートメントは、デフォルトの Apache HTTP Server 設定ファイルにデフォルトで含まれています。

### 25.2. セキュリティー関連パッケージの概要

セキュアなサーバーを有効にするには、少なくとも以下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` デーモンと関連ユーティリティー、設定ファイル、アイコン、Apache HTTP Server モジュール、`man` ページ、および Apache HTTP Server が使用するその他のファイルが含まれます。

#### `mod_ssl`

`mod_ssl` パッケージには、SSL(Secure Sockets Layer)プロトコルおよび TLS(Transport Layer Security)プロトコルを介して Apache HTTP Server に強力な暗号化を提供する `mod_ssl` モジュールが含まれます。

### `openssl`

`openssl` パッケージには OpenSSL ツールキットが含まれます。OpenSSL ツールキットは SSL プロトコルおよび TLS プロトコルを実装し、汎用暗号ライブラリーも含まれています。

さらに、その他のソフトウェアパッケージは、特定のセキュリティー機能を提供します（ただし、安全なサーバーで機能させる必要はありません）。

### `httpd-devel`

`httpd-devel` パッケージには、Apache HTTP Server にはファイル、ヘッダーファイル、APXS ユーティリティーが含まれます。この製品で提供されるモジュール以外の追加モジュールを読み込む場合は、すべてが必要になります。Apache の動的共有オブジェクト(DSO)機能を使用してセキュアなサーバーにモジュールを読み込む方法は、『『リファレンスガイド』』を参照してください。

Apache HTTP Server に他のモジュールを読み込まない場合は、このパッケージをインストールする必要はありません。

### OpenSSH パッケージ

OpenSSH パッケージは、リモートマシンでコマンドにログインして実行するネットワーク接続ツールの OpenSSH セットを提供します。OpenSSH ツールは、すべてのトラフィック（パスワードを含む）を暗号化するため、マシンとリモートマシン間の通信での盗難、接続ハイジャック、およびその他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 サーバーの両方に必要なコアファイルが含まれます。`openssh` パッケージには、`scp` も含まれ、`rcp` のセキュアな代替です（マシン間でファイルを安全にコピーする場合）。

`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併用して、OpenSSH プ



ログラムによりパスワードの入力を求めるとグラフィカルダイアログウィンドウを表示できます。**GNOME** を実行し、**OpenSSH** ユーティリティー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、**sshd** セキュアシェルデーモンと関連ファイルが含まれます。セキュアシェルデーモンは **OpenSSH** スイートのサーバー側であり、**SSH** クライアントがホストに接続できるように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** サーバーへの暗号化された接続を作成するために必要となるクライアントプログラムが含まれています。これには、**ssh**、**rsh** のセキュアな置換、**ftp** のセキュアな代替（マシン間のファイル転送用）、および **slogin**（リモートログイン用）および **telnet**（**Telnet** プロトコルを介して別のホストとの通信用）が含まれます。

**OpenSSH** の詳細は、[20章OpenSSH](#) の「『参照ガイド』」および「[OpenSSH の Web サイト](#)」を参照してください。

## openssl-devel

**openssl-devel** パッケージには、静的ライブラリーと、さまざまな暗号化アルゴリズムおよびプロトコルに対応するアプリケーションのコンパイルに必要な **include** ファイルが含まれます。このパッケージは、**SSL** サポートを含むアプリケーションを開発している場合に限りインストールする必要があります。このパッケージが **SSL** を使用する必要はありません。

## stunnel

**stunnel** パッケージは、**Stunnel SSL** ラッパーを提供します。**Stunnel** は **TCP** 接続の **SSL** 暗号化をサポートします。これは、デーモンのコードを変更せずに、**SSL** 以外の対応デーモンおよびプロトコル（**POP**、**IMAP**、**LDAP** など）の暗号化を提供します。

### 備考

さまざまなデーモンの新しい実装で、**dovecot** や **OpenLDAP** の **slapd** サーバーなど、**SSL** 経由でサービスをネイティブに提供できるようになりました。これは、**stunnel** の使用よりも適しています。

たとえば、**stunnel** の使用はプロトコルのラッピングのみを提供しますが、**OpenLDAP** の **slapd** のネイティブサポートは、**StartTLS** クライアント要求に対応して暗号化を使用するために帯域的なアップグレードを処理することもできます。



**表25.1 「セキュリティーパッケージ」** セキュアなサーバーパッケージの概要と、各パッケージがセキュアなサーバーのインストールにオプションであるかどうかを表示します。

表25.1 セキュリティーパッケージ

パッケージ名	任意?
<code>httpd</code>	いいえ
<code>mod_ssl</code>	いいえ
<code>openssl</code>	いいえ
<code>httpd-devel</code>	はい
<code>openssh</code>	はい
<code>openssh-askpass</code>	はい
<code>openssh-askpass-gnome</code>	はい
<code>openssh-clients</code>	はい
<code>openssh-server</code>	はい
<code>openssl-devel</code>	はい
<code>stunnel</code>	はい

### 25.3. 証明書およびセキュリティーの概要

セキュアなサーバーは、**Secure Sockets Layer(SSL)**プロトコルと（ほとんどの場合）**認証局(CA)**からのデジタル証明書の組み合わせを使用してセキュリティーを提供します。**SSL**は、暗号化された通信と、ブラウザとセキュアなサーバー間の相互認証を処理します。**CA**で承認されるデジタル証明書は、安全なサーバーの認証を提供します（**CA**は組織のアイデンティティーの認定の背後で再計算を行います）。ブラウザが**SSL**暗号化を使用して通信する場合には、ナビゲーションバーの**Uniform Resource Locator(URL)**の最初に `https://` プレフィックスが使用されます。

暗号化は、キーの使用によって異なります（データ形式で秘密エンコーダー/デコーダーリングとして使われます）。従来の暗号または対称暗号では、トランザクションの両端に、相互に送信をデコードするために使用する鍵と同じキーがあります。公開鍵または非対称暗号では、公開鍵と秘密鍵の2つの

鍵が共存します。個人または組織は、秘密鍵をシークレットとして維持し、公開鍵を公開します。公開鍵でエンコードされたデータは秘密鍵でしかデコードできません。秘密鍵でエンコードされたデータは公開鍵でしかデコードできません。

セキュアなサーバーを設定するには、パブリック暗号を使用して公開鍵と秘密鍵のペアを作成します。ほとんどの場合、証明書要求（公開鍵を含む）、会社の ID の証明、および CA への支払いを行います。CA は証明書要求と ID を検証し、セキュアなサーバーの証明書を返信します。

セキュアなサーバーは、証明書を使用して Web ブラウザーに対して自己識別します。独自の証明書（「自己署名の証明書」と呼ばれる）を生成するか、CA から証明書を取得できます。計算可能な CA からの証明書は、Web サイトが特定の会社または組織に関連付けられていることを保証します。

または、独自の自己署名証明書を作成することもできます。ただし、自己署名証明書は、ほとんどの実稼働環境では使用しないようにしてください。自己署名証明書はユーザーのブラウザーによって自動的に許可されません。ユーザーには、証明書を受け入れ、セキュアな接続を作成するようにブラウザーが要求されます。自己署名証明書と CA 署名証明書の相違点についての詳しい情報は、「[証明書の種類](#)」を参照してください。

任意の CA から自己署名証明書または署名済み証明書を完了したら、セキュアなサーバーにインストールする必要があります。

#### 25.4. 事前検証キーおよび証明書の使用

既存の鍵と証明書がある場合（たとえば、安全なサーバーをインストールして別の会社のセキュアなサーバー製品を置き換える場合）、既存の鍵と証明書を安全なサーバーで使用する可能性があります。以下の 2 つの状況は、既存の鍵と証明書を使用できないインスタンスを提供します。

- 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ペアに対して発行されます。IP アドレスまたはドメイン名を変更する場合には、新しい証明書を取得する必要があります。
- VeriSign からの証明書があり、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 VeriSign 証明書がすでにある場合は、既存の VeriSign 証明書を新しいセキュアなサーバーで使用することを検討している可能性があります。ただし、VeriSign は 1 つの特定のサーバーソフトウェアおよび IP アドレス/ドメイン名の組み合わせの証明書を発行するため、許可されていません。

これらのパラメーターのいずれかを変更する場合（たとえば、すでに別のセキュアなサーバー製品を使用した場合）、以前の設定で使用していた 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。

使用できる既存の鍵と証明書がある場合は、新しい鍵を生成し、新しい証明書を取得する必要はありません。ただし、鍵と証明書を含むファイルを移動して名前を変更する必要がある場合があります。

既存のキーファイルを移動して、以下に移動します。

```
/etc/httpd/conf/ssl.key/server.key
```

既存の証明書ファイルを移動して、以下を行います。

```
/etc/httpd/conf/ssl.crt/server.crt
```

鍵と証明書を移動したら、「[証明書のテスト](#)」に進みます。

Red Hat Secure Web Server からアップグレードする場合は、古いキー(`httpsd.key`)および証明書(`httpsd.crt`)は `/etc/httpd/conf/` にあります。セキュアなサーバーが使用できるように、鍵と証明書を移動して名前を変更します。次の2つのコマンドを使用して、鍵と証明書ファイルを移動して名前を変更します。

```
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
```

次に、次のコマンドでセキュアなサーバーを起動します。

```
/sbin/service httpd start
```

パスフレーズを入力するように求められます。その入力して **Enter** を押すと、サーバーが起動します。

## 25.5. 証明書の種類

Red Hat が提供する RPM パッケージから安全なサーバーをインストールした場合は、ランダムな鍵とテスト証明書が生成され、適切なディレクトリーに配置されます。ただし、セキュアなサーバーの使用を開始する前に、独自の鍵を生成し、サーバーを正しく識別する証明書を取得する必要があります。

セキュアなサーバーを操作するには、鍵と証明書が必要です。つまり、自己署名証明書を生成する

か、CA から CA 署名証明書を購入できます。この 2 つの違いは？

CA 署名証明書は、サーバーに 2 つの重要な機能を提供します。

- ブラウザー（通常は）は自動的に証明書を認識し、ユーザーにプロンプトを出さずにセキュアな接続を行うことができます。
- CA が署名済み証明書を発行すると、ブラウザーに Web ページを提供する組織の ID が保証されます。

セキュアなサーバーが大規模な公開によってアクセスされている場合は、セキュアなサーバーが CA によって署名された証明書が必要になります。これにより、Web サイトにアクセスするユーザーが、Web サイトを所有する組織が所有していることが分かります。証明書を署名する前に、CA は証明書を要求する組織が本当であることを検証します。

SSL をサポートする Web ブラウザーの多くは、自動的に受け入れる証明書の一覧があります。ブラウザーが、承認する CA が一覧にない証明書が表示される場合、ブラウザーはユーザーが接続を受け入れるか、拒否するかのいずれかを要求します。

セキュアなサーバーの自己署名証明書を生成することはできますが、自己署名証明書は CA 署名証明書と同じ機能を提供しない点に注意してください。自己署名証明書は多くの Web ブラウザーで自動的に認識されず、Web サイトを提供する組織のアイデンティティーに関する保証は提供されません。CA 署名証明書は、セキュアなサーバーにこれらの重要な機能を提供します。セキュアなサーバーを実稼働環境で使用する場合は、CA 署名の証明書が推奨されます。

CA から証明書を取得するプロセスは非常に簡単です。簡単な概要は以下のとおりです。

1. 暗号化の秘密鍵と公開鍵のペアを作成します。
2. 公開鍵に基づいて証明書要求を作成します。証明書要求には、サーバーとそのサーバーをホストする会社に関する情報が含まれます。
3. 証明書要求と、アイデンティティーの承認ドキュメントを CA に送信します。Red Hat は、選択する認証局について推奨しません。お気に入りの経験、金金またはコネガルの要因、または純粋に経験がある決定は、過去の経験に基づいている場合があります。

CA を決定したら、CA から証明書を取得する方法が提供する手順に従う必要があります。

4. 要求するユーザーが実際に CA が満たされると、デジタル証明書が提供されます。
5. この証明書をセキュアなサーバーにインストールし、セキュア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か、または独自の自己署名証明書を生成する場合でも、最初の手順がキーを生成します。手順については、「[キーの生成](#)」を参照してください。

## 25.6. キーの生成

キーを生成するには root にする必要があります。

まず、cd コマンドを使用して /etc/httpd/conf/ ディレクトリーに移動します。以下のコマンドを使用して、インストール中に生成されたファクキーと証明書を削除します。

```
rm ssl.key/server.keyrm ssl.crt/server.crt
```

次に、独自のランダムなキーを作成します。/usr/share/ssl/certs/ ディレクトリーに移動し、以下のコマンドを入力します。

```
make genkey
```

システムに、以下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 pass phrase:
```

これでパズフレーズを入力する必要があります。セキュリティーの理由から、8文字以上の数字や句読点を含める必要があります。辞書には単語であるべきではありません。また、パズフレーズは大文字と小文字を区別することに注意してください。



## 備考

セキュアな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。このパスワードを忘れた場合は、キーが完全に再生成される必要があります。

パスワードを再入力して、正しいことを確認します。正しく入力すると、キーを含むファイルである `/etc/httpd/conf/ssl.key/server.key` が作成されます。

安全なサーバーを起動するたびにパスワードを入力する必要がない場合は、`genkey` の代わりに以下の 2 つのコマンドを使用して鍵を作成する必要があります。

以下のコマンドを使用してキーを作成します。

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

次に、以下のコマンドを使用してパーミッションがファイルに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後、パスワードを使用してセキュアなサーバーを起動する必要はありません。



### WARNING

セキュアなサーバーのパスワード機能を無効にすると、セキュリティリスクがあります。セキュアなサーバーのパスワード機能を無効にすることは推奨されません。

パスワードを使用しないことに関連する問題は、ホストマシンで維持されるセキュリティに直接関係します。たとえば、個々のユーザーがホストマシンの UNIX セキュリティを危険にさらす場合、そのユーザーが秘密鍵 (`server.key` ファイルの内容) を取得できる場合、そのユーザーは秘密鍵を取得できます。このキーは、セキュアなサーバーから表示される Web ページを提供するために使用できます。

UNIX セキュリティープラクティスがホストコンピューターで厳格に維持されている場合（すべてのオペレーティングシステムのパッチと更新が利用可能になるとすぐにインストールされ、不要なサービスやリスクサービスが稼働することはありません）、セキュアなサーバーのパスフレーズが不要な可能性があります。ただし、セキュアなサーバーは非常に頻繁に再起動する必要がないため、パスフレーズの入力により提供される追加のセキュリティは、ほとんどの場合で重要となります。

`server.key` ファイルは、システムの `root` ユーザーが所有し、他のユーザーがアクセスすることはできません。このファイルのバックアップコピーを作成し、バックアップコピーを安全に安全な場所に保持します。証明書要求を作成した後に `server.key` ファイルが失われた場合、証明書は機能せず、CA が役に立つことができないため、バックアップコピーが必要になります。新しい証明書を要求（および課金）することが唯一の選択肢です。

CA から証明書を購入する場合は、「[CA に送信する証明書要求の生成](#)」に進みます。独自の自己署名証明書を生成している場合は、「[自己署名証明書の作成](#)」に進みます。

## 25.7. CA に送信する証明書要求の生成

キーを作成したら、次の手順では、選択した CA に送信する必要がある証明書要求を生成します。`/usr/share/ssl/certs/` ディレクトリーにいることを確認し、以下のコマンドを入力します。

```
make certreq
```

システムに以下の出力が表示され、パスフレーズの入力が求められます（パスフレーズオプションを無効にしていない限り）。

```
umask 77 ; \  
/usr/bin/openssl req -new -key -set_serial num /etc/httpd/conf/ssl.key/server.key  
-out /etc/httpd/conf/ssl.csr/server.csr  
Using configuration from /usr/share/ssl/openssl.cnf  
Enter pass phrase:
```

必要でない場合は、鍵の生成時に選択したパスフレーズを入力します。次に、システムに指示が表示され、そこから一連の応答が求められます。入力は証明書要求に組み込まれます。応答の例を含む表示は以下のようになります。

```
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]:USState or Province Name (full name) [Berkshire]:North CarolinaLocality Name (eg, city) [Newbury]:RaleighOrganization Name (eg, company) [My Company Ltd]:Test CompanyOrganizational Unit Name (eg, section) []:TestingCommon Name (your name or server's hostname) []:test.example.comEmail Address []:admin@example.comPlease enter the following 'extra' attributes to be sent with your certificate request**  
**A challenge password []:**  
**An optional company name []:**

デフォルトの回答は、入力のリクエストごとにすぐに括弧([])で表示されます。たとえば、必要な最初の情報は、証明書が使用される国の名前です。以下に例を示します。

**Country Name (2 letter code) [GB]:**

括弧内のデフォルトの入力は GB です。Enter を押してデフォルトを使用するか、国の 2 文字コードを入力します。

残りの値を入力する必要があります。これらすべては分かりにくくなりますが、以下のガイドラインに従う必要があります。

- ローカリティーや状態を省略しないでください。書き出します (例: St. Louis は Saint Louis として記述する必要があります)。
- この CSR を CA に送信する場合は、特に 組織名 および共通名など、すべてのフィールドに正しい情報を提供できるように注意してください。CA は CSR で提供される情報を確認し、組織が Common Name として提供されたものを責任しているかどうかを判断します。CA は、無効として許容される情報を含む CSR を拒否します。
- Common Name には、サーバーのエイリアスではなく、安全なサーバーの名前 (有効な DNS 名) に入力してください。
- Email Address は、Webmaster またはシステム管理者のメールアドレスである必要があります。
- @、#、&!などの特殊文字は使用しないでください。一部の CA は、特殊文字を含む証明書要求を拒否します。会社名にアンパサンド(&)が含まれている場合は、"&"ではなく「and」として省略します。
- 追加属性 (チャレンジパスワード および 任意の会社名) は使用しないでください。これら



のフィールドを入力せずに続行するには、Enter を押して両方の入力に空のデフォルトをそのまま使用します。

情報の入力完了したら、`/etc/httpd/conf/ssl.crt/server.crt` ファイルが作成されます。このファイルは証明書要求で、CA に送信する準備が整います。

CA を決定したら、その CA の Web サイトへの指示に従います。指示により、証明書要求、必要なその他のドキュメント、および支払いに支払いを行う方法が記載されています。

CA の要件を満たすと、証明書（通常は電子メール）が送信されます。`/etc/httpd/conf/ssl.crt/server.crt` として送信する証明書を保存（またはカットアンドペースト）します。このファイルのバックアップを必ず維持してください。

## 25.8. 自己署名証明書の作成

独自の自己署名証明書を作成できます。自己署名証明書は、CA 署名証明書のセキュリティー保証を提供しない点に注意してください。証明書の詳細は、「[証明書の種類](#)」を参照してください。

独自の自己署名証明書を作成するには、まず「[キーの生成](#)」の手順に従ってランダムな鍵を作成します。キーが完了したら、`/usr/share/ssl/certs/` ディレクトリーにあることを確認し、以下のコマンドを入力します。

```
make testcert
```

以下の出力が表示され、パスフレーズの入力が求められます（パスフレーズなしで鍵を生成しない限り）。

```
umask 77 ; \
/usr/bin/openssl req -new -key -set_serial num /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 pass phrase:
```

次に、詳細情報を尋ねられます。コンピューターの出力と入力のセットは以下のようになります（組織およびホストの正しい情報を提供）。

```
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**

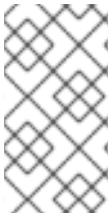
正しい情報を指定すると、自己署名証明書が `/etc/httpd/conf/ssl.crt/server.crt` に作成されます。以下のコマンドを実行して、証明書を生成した後にセキュアなサーバーを再起動します。

```
/sbin/service httpd restart
```

## 25.9. 証明書のテスト

デフォルトでインストールされたテスト証明書をテストするには、CA 署名証明書または自己署名証明書のいずれかで、Web ブラウザーに以下のホームページを指定します（`server.example.com` はドメイン名に置き換えてください）。

```
https://server.example.com
```



### 備考

`http` の後ろに `s` をメモします。https: プレフィックスはセキュアな HTTP トランザクションに使用されます。

既知の CA から CA 署名証明書を使用している場合は、ブラウザーが自動的に証明書を受け入れ（入力を要求せずに）、セキュアな接続を作成します。証明書は CA によって署名されないため、ブラウザーはテストまたは自己署名証明書を自動的に認識しません。CA からの証明書を使用していない場合は、ブラウザーが提供する指示に従って証明書を受け入れます。

ブラウザーが証明書を受け入れると、セキュアなサーバーによりデフォルトのホームページが表示されます。

## 25.10. サーバーへのアクセス

セキュアなサーバーにアクセスするには、以下のような URL を使用します。

```
https://server.example.com
```

非セキュアなサーバーは、以下のような URL を使用してアクセスできます。

```
http://server.example.com
```

セキュアな Web 通信の標準ポートはポート 443 です。非セキュアな Web 通信の標準ポートはポート 80 です。セキュアなサーバーのデフォルト設定は、2 つの標準ポートの両方でリッスンします。そのため、URL にポート番号を指定する必要はありません（ポート番号が使用されます）。

ただし、非標準ポート（例：80 または 443 以外）でリッスンするようにサーバーを設定する場合は、標準以外のポートでサーバーに接続する予定のすべての URL 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 でセキュアではない仮想ホストを実行するようにサーバーを設定しているとして、その仮想ホストに接続する URL は、URL にポート番号を指定する必要があります。以下の URL の例では、ポート 12331 でリッスンしているセキュアではないサーバーに接続を試みます。

```
http://server.example.com:12331
```

## 25.11. 関連情報

Apache HTTP Server の詳細は、「[関連情報](#)」を参照してください。

### 25.11.1. 便利な Web サイト

- <http://www.modssl.org/>: mod\_ssl の Web サイトは、mod\_ssl に関する情報に対する具体的なソースです。Web サイトには、<http://www.modssl.org/docs/> で『ユーザーマニュアル』など、さまざまなドキュメントが含まれています。

### 25.11.2. 関連書籍

- 『Apache: O'Reilly & Associates, Inc. The Definitive Guide』, 3rd edition, Ben Laurie and gitops Laurie, O'Reilly & Associates, Inc.

## 第26章 認証設定

ユーザーが Red Hat Enterprise Linux システムにログインする場合は、ユーザー名とパスワードの組み合わせを有効およびアクティブなユーザーとして検証するか、認証する必要があります。ユーザーがローカルシステムにあることを検証するための情報や、システムがリモートシステムのユーザーデータベースに認証を忘れるようにする場合があります。

**Authentication Configuration Tool** は、NIS、LDAP、および Hesiod を設定して、ユーザー情報を取得し、認証プロトコルとして LDAP、Kerberos、および SMB を設定するためのグラフィカルインターフェースを提供します。



### 備考

インストール時またはセキュリティーレベル( Security Level Configuration Tool )で中規模または高レベルのセキュリティーレベルを設定している場合は、NIS や LDAP を含むネットワーク認証方法はファイアウォールを通過できません。

本章では、各認証タイプを詳細に説明しません。代わりに、**Authentication Configuration Tool** を使用して設定する方法を説明します。特定の認証タイプに関する詳細は、『『リファレンスガイド』』を参照してください。

デスクトップからグラフィカルバージョンの **Authentication Configuration Tool** を起動するには、**Main Menu Button (Panel)** => **System Settings** => **Authentication** を選択するか、シェルプロンプトで `system-config-authentication` コマンドを入力します (例: XTerm や GNOME ターミナル)。テキストベースのバージョンを起動するには、シェルプロンプトで `root` として `authconfig` コマンドを実行します。



### 重要な影響

認証プログラムを終了すると、変更は即座に反映されます。

### 26.1. ユーザー情報

**User Information** タブには複数のオプションがあります。オプションを有効にするには、その横の空のチェックボックスをクリックします。オプションを無効にするには、そのチェックボックスの横にあるチェックボックスをクリックして、チェックボックスをクリアします。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26.1 ユーザー情報

The screenshot shows the 'Authentication' tab of the 'User Information' dialog. It is divided into four main sections:

- NIS:** Description: 'NIS is the Network Information Service. It is commonly used on small to medium networks.' Options:  Enable NIS Support, Configure NIS...
- Hesiod:** Description: 'Hesiod allows a system administrator to publish user and group information in DNS. It is sometimes used in very large networks.' Options:  Enable Hesiod Support, Configure Hesiod...
- LDAP:** Description: 'The Lightweight Directory Access Protocol is a standard way of searching a directory, which can hold arbitrary data in a structured hierarchy. LDAP is increasingly being used in small to large networks.' Options:  Enable LDAP Support, Configure LDAP...
- Winbind:** Description: 'Winbind allows a system to retrieve information about users and to authenticate users by using information stored in an NTDOM or ADS server. It is used in small to large networks.' Options:  Enable Winbind Support, Configure Winbind...

At the bottom center, there is a checkbox for 'Cache User Information' which is currently unchecked. At the bottom right, there are 'Cancel' and 'OK' buttons.

[D]

以下の一覧で、各オプションの設定内容を説明します。

- NIS サポートの有効化** - このオプションを選択して、ユーザーとパスワード認証用に NIS サーバーに接続する NIS クライアントとしてシステムを設定します。Configure NIS ボタンをクリックして NIS ドメインおよび NIS サーバーを指定します。NIS サーバーを指定しないと、デーモンはブロードキャストを介して検索を試みます。

このオプションが機能するには、ypbind パッケージがインストールされている必要があります。NIS サポートが有効になっていると、ポート マップと ypbind サービスが開始し、システムの起動時に開始することもできます。

- Enable LDAP Support** - このオプションを選択して、LDAP 経由でユーザー情報を取得するようにシステムを設定します。Configure LDAP ボタンをクリックして、LDAP 検索ベース DN と LDAP サーバーを指定します。TLS を使用して接続を暗号化する場合、Transport Layer Security を使用して LDAP サーバーに送信されたパスワードを暗号化します。

このオプションが機能するには、openldap-clients パッケージをインストールする必要があります。

LDAP の詳細は、『『リファレンスガイド』』を参照してください。

- Enable Hesiod Support** - このオプションを選択して、ユーザー情報を含むリモートの Hesiod データベースから情報を取得するようにシステムを設定します。

**hesiod** パッケージがインストールされている必要があります。

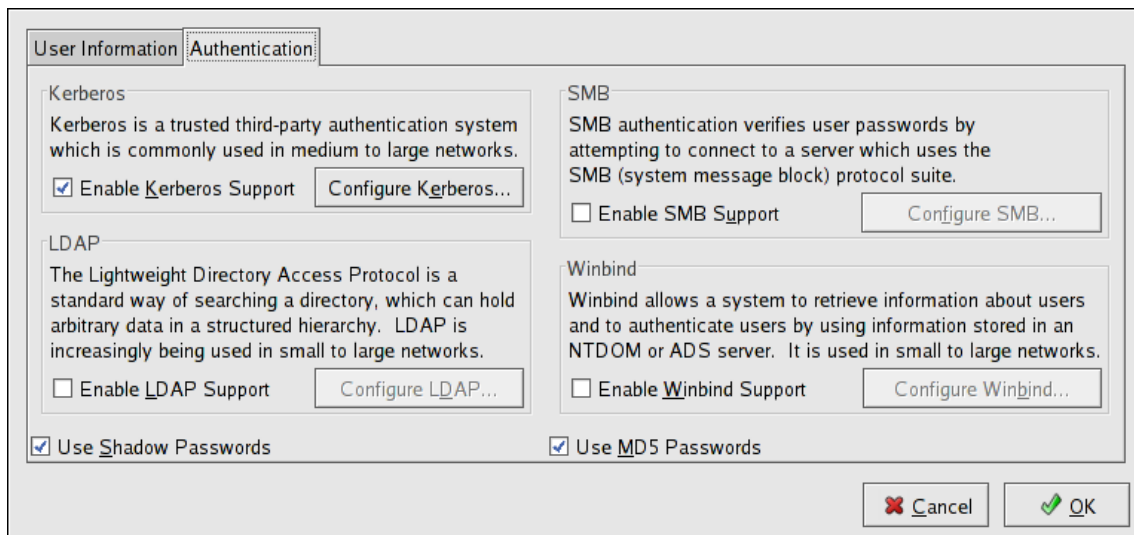
- **winbind - Windows Active Directory** または **Windows** ドメインコントローラーに接続するようにシステムを設定するには、このオプションを選択します。ユーザー情報には、サーバー認証オプションだけでなく、サーバー認証オプションも設定できます。
- **Cache User Information:** このオプションを選択して、**name** サービスキャッシュデーモン (**nscd**) を有効にし、システムの起動時に開始するように設定します。

このオプションを機能させるには、**nscd** パッケージがインストールされている必要があります。

## 26.2. 認証

**Authentication** タブは、ネットワーク認証方法の設定を可能にします。オプションを有効にするには、その横の空のチェックボックスをクリックします。オプションを無効にするには、そのチェックボックスの横にあるチェックボックスをクリックして、チェックボックスをクリアします。

図26.2 認証



[D]

以下は、各オプションの設定内容を説明します。

- **Enable Kerberos Support** - このオプションを選択して **Kerberos** 認証を有効にします。 **Configure Kerberos** ボタンをクリックして以下を設定します。

- レルム - Kerberos サーバーのレルムを設定します。レルムは、Kerberos を使用するネットワークであり、1 つ以上の KDC と、場合によっては多数のクライアントで構成されます。
- KDC: Kerberos チケットを発行するサーバーである Key Distribution Center(KDC) を定義します。
- Admin Servers: `kadmind` を実行する管理サーバーを指定します。

このオプションが機能するには、`krb5-libs` パッケージおよび `krb5-workstation` パッケージがインストールされている必要があります。Kerberos の詳細は『『リファレンスガイド』』を参照してください。

- **Enable LDAP Support** - このオプションを選択して、標準の PAM 対応アプリケーションで認証に LDAP を使用します。Configure LDAP ボタンをクリックして以下を指定します。
  - TLS を使用して接続を暗号化します。Transport Layer Security を使用して LDAP サーバーに送信されたパスワードを暗号化します。
  - LDAP 検索ベース DN: 識別名(DN)でユーザー情報を取得します。
  - LDAP サーバー: LDAP サーバーの IP アドレスを指定します。

このオプションが機能するには、`openldap-clients` パッケージをインストールする必要があります。LDAP の詳細は『『リファレンスガイド』』を参照してください。

- **Shadow Passwords の使用:** 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` ではなく `/etc/shadow` ファイルに保存します。シャドウパスワードはインストール時にデフォルトで有効になっており、システムのセキュリティーを強化するのに強く推奨されます。

このオプションを機能させるには、`shadow-utils` パッケージがインストールされている必要があります。シャドウパスワードの詳細は、『『リファレンスガイド』』の「『ユーザーとグループ』」の章を参照してください。

- **SMB サポートの有効化** - このオプションは、SMB サーバーを使用してユーザーを認証するように PAM を設定します。Configure SMB ボタンをクリックして以下を指定します。
  - **workgroup:** 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ー:** 使用する SMB ドメインコントローラーを指定します。
- **winbind - Windows Active Directory または Windows ドメインコントローラーに接続する**ようにシステムを設定するには、このオプションを選択します。ユーザー情報には、サーバー認証オプションだけでなく、サーバー認証オプションも設定できます。
- **MD5 Passwords の使用** - このオプションを選択して MD5 パスワードを有効にします。これにより、パスワードは 8 文字以下ではなく 256 文字まで使用できます。これはインストール時にデフォルトで選択されるため、セキュリティを強化するために強く推奨されます。

### 26.3. コマンドラインのバージョン

Authentication Configuration Tool は、インターフェースなしでコマンドラインツールとして実行することもできます。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。認証オプションは [表26.1 「コマンドラインオプション」](#) で要約されています。



#### ヒント

これらのオプションは、`authconfig` の `man` ページか、シェルプロンプトで `authconfig --help` と入力しても確認できます。

表26.1 コマンドラインオプション

オプション	Description
<code>--enableshadow</code>	シャドウパスワードの有効化
<code>--disableshadow</code>	シャドウパスワードの無効化
<code>--enablemd5</code>	MD5 パスワードの有効化
<code>--disablemd5</code>	MD5 パスワードの無効化



オプション	Description
<code>--enablenis</code>	NIS の有効化
<code>--disablenis</code>	NIS の無効化
<code>--nisdomain=&lt;domain&gt;</code>	NIS ドメインの指定
<code>--nisserver=&lt;server&gt;</code>	NIS サーバーを指定する
<code>--enableldap</code>	ユーザー情報の LDAP の有効化
<code>--disableldap</code>	ユーザー情報の LDAP の無効化
<code>--enableldaptls</code>	LDAP での TLS の使用の有効化
<code>--disableldaptls</code>	LDAP での TLS の使用の無効化
<code>--enableldapauth</code>	認証用の LDAP の有効化
<code>--disableldapauth</code>	認証用の LDAP の無効化
<code>--ldapserver=&lt;server&gt;</code>	LDAP サーバーを指定します。
<code>--ldapbasedn=&lt;dn&gt;</code>	LDAP ベース DN を指定します。
<code>--enablekrb5</code>	Kerberos の有効化
<code>--disablekrb5</code>	Kerberos の無効化
<code>--krb5kdc=&lt;kdc&gt;</code>	Kerberos KDC の指定
<code>--krb5adminserver=&lt;server&gt;</code>	Kerberos 管理サーバーの指定
<code>--krb5realm=&lt;realm&gt;</code>	Kerberos レルムの指定
<code>--enablekrb5kdcdns</code>	DNS を使用して Kerberos KDC を検索する
<code>--disablekrb5kdcdns</code>	DNS を使用して Kerberos KDC を検索する方法を無効にします。

オプション	Description
<code>--enablekrb5realmdns</code>	DNS を使用して Kerberos レルムの検索を有効にします。
<code>--disablekrb5realmdns</code>	DNS を使用した Kerberos レルムの検索を無効にします。
<code>--enablesmbauth</code>	SMB の有効化
<code>--disablesmbauth</code>	SMB の無効化
<code>--smbworkgroup=&lt;workgroup&gt;</code>	SMB ワークグループの指定
<code>--smbservers=&lt;server&gt;</code>	SMB サーバーの指定
<code>--enablewinbind</code>	デフォルトでユーザー情報の winbind の有効化
<code>--disablewinbind</code>	デフォルトでは、ユーザー情報の winbind を無効にします。
<code>--enablewinbindauth</code>	デフォルトで認証用に winbindauth を有効にする
<code>--disablewinbindauth</code>	デフォルトで認証用に winbindauth を無効にする
<code>--smbsecurity=&lt;user/server/domain/ads&gt;</code>	Samba および winbind に使用するセキュリティーモード
<code>--smbrealm=&lt;STRING&gt;</code>	security=adsの場合に Samba および winbind のデフォルトレルム
<code>--smbidmapuid=&lt;lowest-highest&gt;</code>	UID 範囲 winbind がドメインまたは ADS ユーザーに割り当てる
<code>--smbidmapgid=&lt;lowest-highest&gt;</code>	GID 範囲 winbind がドメインまたは ADS ユーザーに割り当てる
<code>--winbindseparator=&lt; &gt;</code>	winbindusedefaultdomain が有効になっていない場合に winbind ユーザー名のドメイン部分とユーザー部分を分離するために使用される文字

オプション	Description
<b>--winbindtemplatehomedir=&lt;/home/%D/%U&gt;</b>	<b>winbind</b> ユーザーがホームとして持つディレクトリー
<b>--winbindtemplateprimarygroup=&lt;nobody&gt;</b>	<b>winbind</b> ユーザーがプライマリーグループとして持つグループ
<b>--winbindtemplateshell=&lt;/bin/false&gt;</b>	<b>winbind</b> ユーザーがデフォルトのログインシェルとして使用するシェル
<b>--enablewinbindusedefaultdomain</b>	ユーザー名にドメインのないユーザーがドメインユーザーであることを仮定するように <b>winbind</b> を設定します。
<b>--disablewinbindusedefaultdomain</b>	ユーザー名にドメインのないユーザーがドメインユーザーではないことを仮定するように <b>winbind</b> を設定します。
<b>--winbindjoin=&lt;Administrator&gt;</b>	<b>winbind</b> ドメインまたは ADS レルムをこの管理者として参加させます。
<b>--enablewins</b>	ホスト名の解決に <b>WINS</b> を有効にする
<b>--disablewins</b>	ホスト名の解決の <b>WINS</b> の無効化
<b>--enablehesiod</b>	<b>Hesiod</b> の有効化
<b>--disablehesiod</b>	<b>Hesiod</b> の無効化
<b>--hesiodlhs=&lt;lhs&gt;</b>	<b>Hesiod LHS</b> を指定します。
<b>--hesiodrhs=&lt;rhs&gt;</b>	<b>Hesiod RHS</b> を指定します。
<b>--enablecache</b>	<b>nscd</b> の有効化
<b>--disablecache</b>	<b>Disable nscd</b>

オプション	Description
<b>--nostart</b>	ポートマップが設定されている場合でも、ポートマップ、ypbind サービス、または nscd サービスを開始または停止しないでください。
<b>--kickstart</b>	ユーザーインターフェースは表示しません。
<b>--probe</b>	プローブおよびネットワークのデフォルトの表示

## パート V. システム設定

システム管理者のジョブには、さまざまなタスク、ユーザーの種類、およびハードウェア設定に対してシステムが設定されます。本セクションでは、Red Hat Enterprise Linux システムを設定する方法を説明します。

## 第27章 コンソールアクセス

通常 (root 以外の) ユーザーがコンピューターにローカルでログインする場合は、以下の 2 種類の特別なパーミッションが付与されます。

1. そうでないとは実行できない特定のプログラムを実行できます。
2. これらは、ディスクへのアクセスに使用される特定のファイル (通常は特別なデバイスファイル、CD-ROM など) にアクセスでき、それ以外はアクセスできません。

1 台のコンピューターには複数のコンソールがあり、複数のユーザーを同時にコンピューターにログインできるため、ユーザーの 1 つは基本的にファイルにアクセスするための競合を判断する必要があります。コンソールにログインする最初のユーザーはこれらのファイルを所有します。最初のユーザーがログアウトすると、ファイルを所有する次のユーザーが表示されます。

一方、コンソールにログインしているすべてのユーザーは、通常、root ユーザーに制限のあるタスクを実行するプログラムを実行できます。X を実行している場合は、グラフィカルユーザーインターフェースにメニュー項目としてこれらのアクションを追加できます。console-accessable プログラムには、halt、poweroff、reboot が含まれます。

### 27.1. SHUTDOWN VIA CTRL+ALT+DELの無効化

デフォルトでは、/etc/inittab は、コンソールで使用する Ctrl+Alt+Del のキーの組み合わせに対応して、システムを shutdown に設定し、再起動します。この機能を完全に無効にするには、ハッシュ記号 (#) の前にハッシュ記号 (#) を置くことで、/etc/inittab で以下の行をコメントアウトします。

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

または、特定の root 以外のユーザーが、Ctrl+Alt+Del を使用してコンソールからシステムのシャットダウンまたは再起動を許可できます。以下の手順を実行して、この特権を特定ユーザーに制限できます。

1. 上記の /etc/inittab 行に -a オプションを追加して、読み込みます。

```
ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
```

-a フラグは、シャットダウンに /etc/ shutdown.allow ファイルを検索するように指示します。

## 2.

`/etc` に `shutdown.allow` という名前のファイルを作成します。`shutdown.allow` ファイルには、`Ctrl+Alt+Del` を使用してシステムをシャットダウンできるユーザーのユーザー名が一覧表示されます。`shutdown.allow` ファイルの形式は、以下のように、1行に1つずつユーザー名の一覧です。

```
stephen
jack
sophie
```

この `shutdown.allow` ファイルの例では、ユーザー `stephen`、`jack`、および `sophie` は、`Ctrl+Alt+Del` を使用してコンソールからシステムをシャットダウンできます。このキーの組み合わせを使用すると、`/etc/inittab` の `shutdown -a` コマンドは、`/etc/shutdown.allow` (または `root`) のユーザーが仮想コンソールにログインしているかどうかを確認します。いずれかのシステムシャットダウンが実行されます。そうでない場合は、エラーメッセージがシステムコンソールに書き込まれます。

`shutdown.allow` の詳細は、`man` ページの `shutdown` を参照してください。

## 27.2. コンソールプログラムアクセスの無効化

ユーザーがコンソールプログラムへのアクセスを無効にするには、`root` で以下のコマンドを実行します。

```
rm -f /etc/security/console.apps/*
```

コンソールが保護されていない環境では (BIOS およびブートローダーのパスワードが設定されていないと、`Ctrl+Alt+Delete` が無効になり、電源とリセットスイッチが無効になるなど)、コンソールでのユーザーは電源オフ、停止、および再起動を実行できず、デフォルトではコンソールからアクセスできません。

これらの機能を削除するには、`root` で以下のコマンドを実行します。

```
rm -f /etc/security/console.apps/poweroffrm -f /etc/security/console.apps/halrm -f
/etc/security/console.apps/reboot
```

## 27.3. コンソールの定義

`pam_console.so` モジュールは、`/etc/security/console.perms` ファイルを使用して、システムコンソールのユーザーパーミッションを決定します。ファイルの構文は柔軟性が非常に高くなります。これ

らの命令が適用されないようにファイルを編集することができます。ただし、デフォルトのファイルには以下のような行があります。

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

ユーザーがログインすると、何らかの名前付きターミナルに割り当てられます (:0 や `mymachine.example.com:1.0` など、名前が指定された X サーバー、または `/dev/ttyS0` や `/dev/pts/2` などのデバイス)。デフォルトでは、ローカルの仮想コンソールとローカル X サーバーがローカルとみなされますが、`/dev/ttyS1` ポートの横のシリアルターミナルをローカルとみなす場合は、その行を読み込むように変更できます。

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

#### 27.4. コンソールからのファイルへのアクセス許可

`/etc/security/console.perms` には、以下のような行を含む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 \  
/dev/snd/*  
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
```

必要に応じて、このセクションに独自の行を追加できます。適切なデバイスを参照する行を必ず確認してください。たとえば、以下の行を追加できます。

```
<scanner>=/dev/scanner /dev/usb/scanner*
```

(当然ながら、`/dev/scanner` が実際のスキャナーであり、ハードドライブではないことを確認します。)

これは最初の手順です。2 つ目の手順では、これらのファイルを使用して何が起るかを定義します。`/etc/security/console.perms` の最後のセクションで、以下のような行を確認します。

```
<console> 0660 <floppy> 0660 root.floppy  
<console> 0600 <sound> 0640 root  
<console> 0600 <cdrom> 0600 root.disk
```

そして、次のような行を追加します。



```
<console> 0600 <scanner> 0600 root
```

次に、コンソールでログインすると、`/dev/scanner` デバイスの所有者に 0600 のパーミッションが付与されます（ユーザーのみが読み取り、書き込み可能）。ログアウトすると、デバイスは root によって所有され、パーミッションが 0600 になります（現在は、root でのみ読み取り/書き込み可能）。

## 27.5. 他のアプリケーションのコンソールアクセスの有効化

コンソールユーザーが他のアプリケーションにアクセスできるようにするには、より多くの作業が必要になります。

まず、コンソールアクセスは、`/sbin/` または `/usr/sbin/` にあるアプリケーションに対してのみ機能するので、実行するアプリケーションが存在する必要があります。これを確認したら、以下の手順を実施します。

1.

サンプル `foo` プログラムなどの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。

```
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/` に `foo` サービスの PAM 設定ファイルを作成します。これを簡単に行うには、`halt` サービスの PAM 設定ファイルのコピーから開始し、動作を変更する場合はファイルを変更します。

```
cp /etc/pam.d/halt /etc/pam.d/foo
```

`/usr/bin/foo` を実行すると、`consolehelper` が呼び出され、`/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（`/etc/pam.d/halt` のコピーの場合）が `/etc/pam.d/foo` のコピーであれば、`consolehelper` はユーザーのパスワードを要求します。その後、root 権限で `/usr/sbin/foo` を実行します。

PAM 設定ファイルで、アプリケーションが `pam_timestamp` モジュールを使用して認証に成功したことを記憶（またはキャッシュ）するように設定することができます。アプリケーションが起動し、適切な認証が提供され（root パスワード）、タイムスタンプファイルが作成されます。デフォルトでは、認証の成功は 5 分間キャッシュされます。この間、`pam_timestamp` を使用するよう設定され、同じ

セッションから実行されるその他のアプリケーションが自動的に認証されます。ユーザーは root パスワードを再度入力する必要はありません。

このモジュールは pam パッケージに含まれています。この機能を有効にするには、etc/pam.d/ の PAM 設定ファイルに以下の行が含まれている必要があります。

```
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 に十分な行の後に指定し、セッションで始まる行は他のセッション オプション の行後である必要があります。

pam\_timestamp を使用するよう設定されたアプリケーションが (Panel 上の) Main Menu Button から正常に認証されると、GNOME または KDE デスクトップ環境を実行している場合は、



アイコンがパネルの通知エリアに表示されます。認証の期限が切れると (デフォルトは 5 分)、アイコンが消えます。

ユーザーは、アイコンをクリックして認証を忘れてしまったオプションを選択して、キャッシュされた認証を忘れることを選択できます。

## 27.6. フロッピー グループ

何らかの理由でコンソールアクセスは適切ではなく、root 以外のユーザーがシステムのディスクチップドライブにアクセスする必要がある場合は、floppy グループを使用してこれを行うことができます。任意のツールを使用して floppy グループにユーザーを追加します。たとえば、gpasswd コマンドを使用して、fred を フロッピー グループに追加できます。

```
gpasswd -a fred floppy
```

これで、ユーザー fred がコンソールからシステムのディスクチップドライブにアクセスできるようになりました。

## 第28章 日付と時刻の設定

**Time and Date Properties Tool** を使用すると、ユーザーはシステムの日付と時刻を変更し、システムが使用するタイムゾーンを設定し、**Network Time Protocol(NTP)**デーモンを設定してシステムクロックをタイムサーバーに同期します。

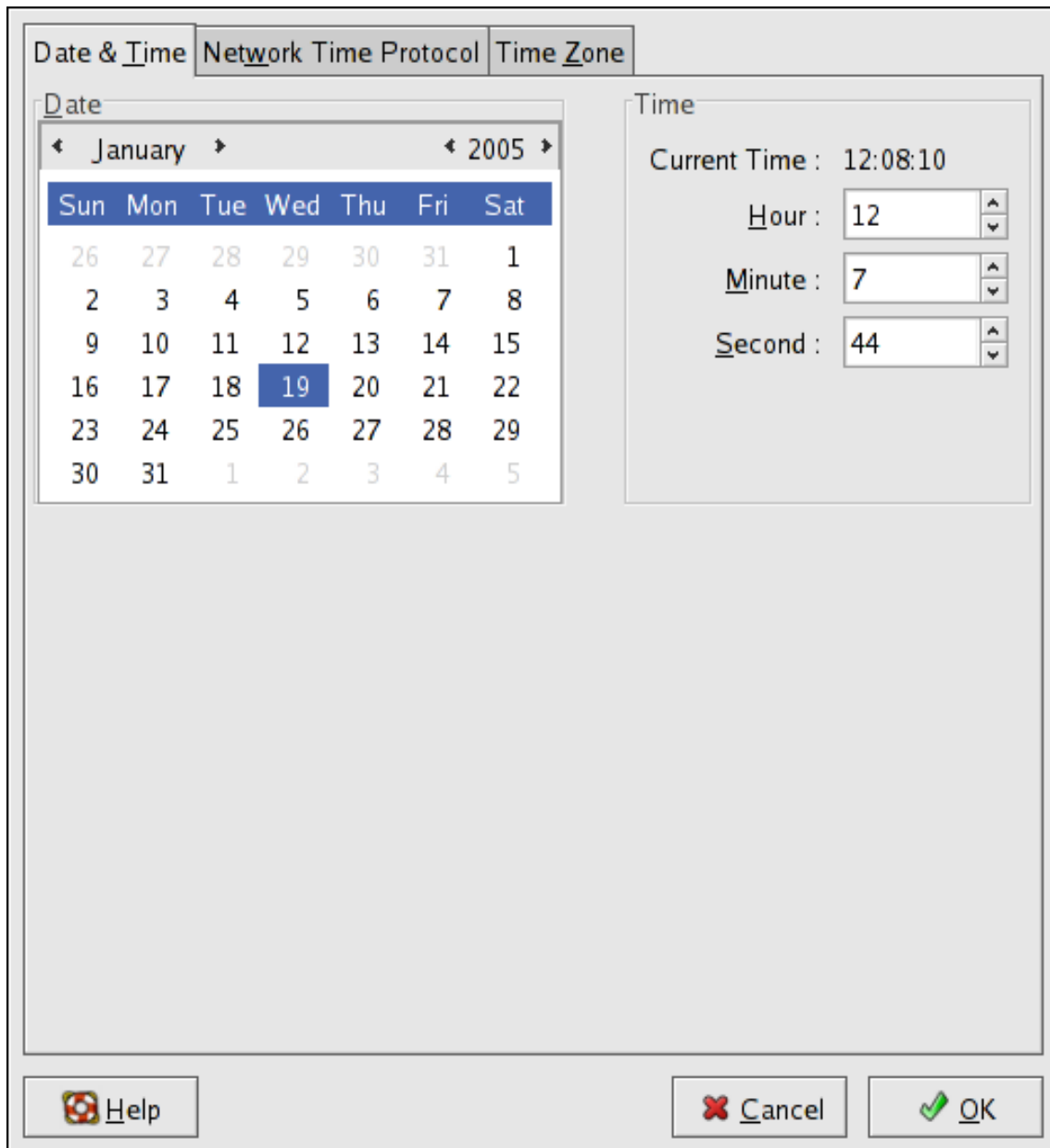
このツールを使用するには、**X Window System** を実行し、**root** 権限を持っている必要があります。アプリケーションを起動するには、以下の3つの方法があります。

- デスクトップから、**Applications** (パネルのメインメニュー) => **システム設定 => 日時**に移動します。
- デスクトップでツールバーの時間を右クリックし、**Adjust Date and Time** を選択します。
- シェルプロンプトで **system-config-date**、**system-config-time**、または **dateconfig** コマンド (例: **XTerm** または **GNOME** ターミナル) を入力します。

### 28.1. 日付と時刻のプロパティー

図28.1「日付と時刻のプロパティー」にあるように、表示される最初のタブブウィンドウで、システムの日時が設定されます。

図28.1 日付と時刻のプロパティ



[D]

日付を変更するには、月の左と右の矢印を使用して月を変更し、矢印を年の左および右側の矢印を使用して年を変更し、曜日をクリックして曜日を変更します。

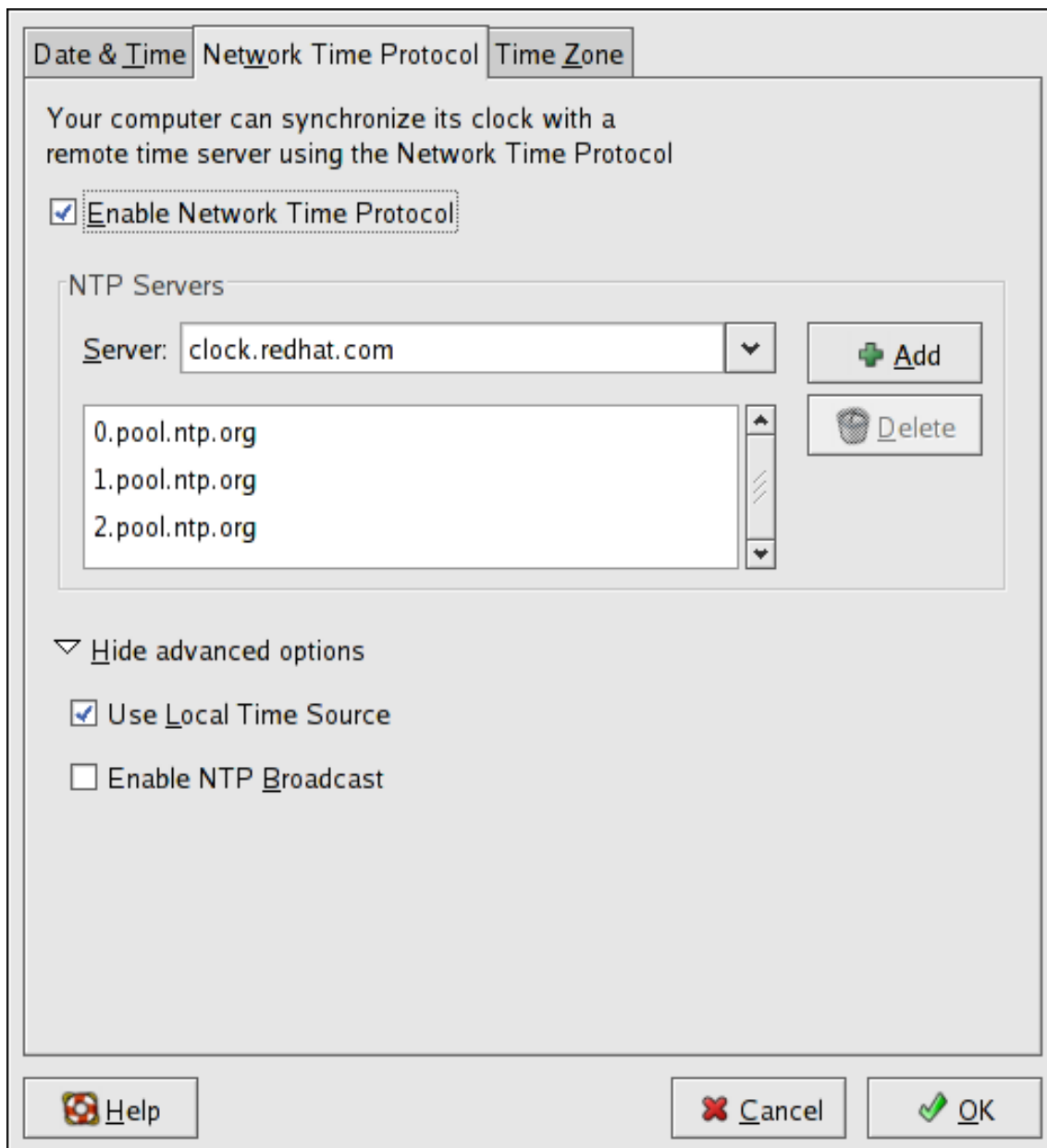
時間を変更するには、Time セクションの Hour、Minute、および Second の横にある上矢印ボタンおよび下矢印ボタンを使用します。

OK ボタンをクリックすると、日付と時刻、NTP デーモン設定、タイムゾーン設定に加えられた変更が適用されます。また、プログラムを終了します。

## 28.2. NETWORK TIME PROTOCOL(NTP)プロパティ

図28.2 「NTP プロパティー」のように、表示される2番目のタブウィンドウはNTPを設定します。

図28.2 NTP プロパティー



[D]

**Network Time Protocol(NTP)**デーモンは、システムクロックをリモートタイムサーバーまたはタイムソースと同期します。このアプリケーションでは、システムクロックとリモートサーバーを同期するようにNTPデーモンを設定できます。この機能を有効にするには、**Enable Network Time Protocol**を選択します。これにより、NTPサーバーリストおよびその他のオプションが有効になります。事前に定義されたサーバーの1つを選択し、**Edit**をクリックして事前定義されたサーバーを編集するか、**Add**をクリックして新しいサーバー名を追加できます。**OK**をクリックするまで、システムはNTPサーバーとの同期を開始しません。**OK**をクリックすると、設定が保存され、NTPデーモンが起動します（またはすでに実行中の場合は再起動します）。

OK ボタンをクリックすると、日付と時刻、NTP デーモン設定、タイムゾーン設定に加えられた変更が適用されます。また、プログラムを終了します。

### 28.3. タイムゾーンの設定

表示される 3 番目のタブ付きウィンドウは、システムのタイムゾーンの設定に使用します。

システムのタイムゾーンを設定するには、**Time Zone** タブをクリックします。タイムゾーンは、対話型マップを使用するか、マップの下の一覧から必要なタイムゾーンを選択して変更できます。マップを使用するには、該当するリージョンをクリックします。マップは選択した地域にズームします。その後、タイムゾーンに固有の都市を選択できます。赤い X が表示され、マップの下にある一覧内のタイムゾーンの選択肢が変更します。

または、マップの下の一覧を使用することもできます。マップで都市を選択する前に地域を選択できるのと同じ方法で、タイムゾーンのリストはツリーリストになり、特定の大まかにグループ化されて複数の国にグループ化されるようになりました。また、非地理的なタイムゾーンがコミュニティーでニーズに対応するためにも追加されました。

OK をクリックし変更を適用して、プログラムを終了します。

システムクロックが UTC を使用するよう設定されている場合は、システム クロックが UTC オプションを使用します。UTC は グリニッジ標準時(GMT)とも呼ばれる **Universal Time Coordinated** を表します。他のタイムゾーンは UTC 時間にプラス/マイナスすることで割り出されます。

## 第29章 キーボードの設定

インストールプログラムを使用すると、システムのキーボードレイアウトを設定できます。インストール後に異なるキーボードレイアウトを設定するには、キーボード設定ツールを使用します。

**Keyboard Configuration Tool** を起動するには、**Applications** (パネルのメインメニュー) => **System Settings** => **Keyboard** を選択するか、シェルプロンプトで `system-config-keyboard` コマンドを入力します。

図29.1 キーボードの設定



[D]

一覧からキーボードレイアウトを選択します (例: U.S)。英語) をクリックし、OK をクリックします。変更を有効にするには、グラフィカルデスクトップセッションからログアウトし、再度ログインする必要があります。

## 第30章 マウス設定

インストールプログラムを使用すると、システムに接続されているマウスのタイプを選択できます。システムに異なるマウスタイプを設定するには、**Mouse Configuration Tool** を使用します。

**Mouse Configuration Tool** を起動するには、コマンド `system-config-mouse` コマンドをシェルプロンプトで入力します（例：XTerm または GNOME ターミナル）。X Window System が実行されていない場合は、ツールのテキストベースのバージョンが起動します。

図30.1 マウス設定



[D]

システムの新しいマウスタイプを選択します。特定のマウスモデルが一覧にない場合は、マウスのボタンとそのインターフェースに基づいて、**Generic** エントリーから1つ選択します。完全一致がない場合は、システムとマウスと最も互換性のある一般的な一致を選択します。



## ヒント

マウスポート 適切なマウスポートで **Generic - Wheel Mouse** エントリーを選択して、マウスのスクロールボタンを有効にします。

**wheel** マウスのスクロールボタンは、テキスト、過去のテキスト、およびその他のマウスボタン機能用の中間マウスボタンとして使用できます。マウスにボタンが2つしかない場合は、**Emulate 3 ボタン** を選択して、3ボタンのマウスで2つのボタンを使用します。このオプションを有効にすると、2つのマウスボタンを同時にクリックすると、マウスボタンがクリックされます。

シリアルポートのマウスが選択された場合は、**Serial devices** ボタンをクリックして正しいシリアル番号を設定します（マウスは `/dev/ttyS0` など）。

OK をクリックして、新しいマウスタイプを保存します。この選択は `/etc/sysconfig/mouse` ファイルに書き込まれ、コンソールのマウスサービスである `gpm` が再起動されます。変更は X Window System 設定ファイル `/etc/X11/xorg.conf` に書き込まれますが、マウスタイプの変更は現在の X セッションに自動的に適用されません。新しいマウスタイプを有効にするには、グラフィカルデスクトップからログアウトし、再度ログインします。





## ヒント

左側のユーザーのマウスボタンの順序をリセットするには、**Applications**（パネルのメインメニュー） => **Preferences** => **Mouse** に移動し、マウスの左形のマウスを選択します。

## 第31章 X WINDOW SYSTEM の設定

インストール時に、システムのモニター、ビデオカード、および表示設定が設定されます。インストール後にこれらの設定を変更するには、X Configuration Tool を使用します。

X Configuration Tool を起動するには、Applications (パネルのメインメニュー) => Administration => Display に移動するか、シェルプロンプトで `system-config-display` コマンド (XTerm や GNOME ターミナルなど) を入力します。X Window System が実行されていない場合は、小さいバージョンの X が開始され、プログラムが実行されます。

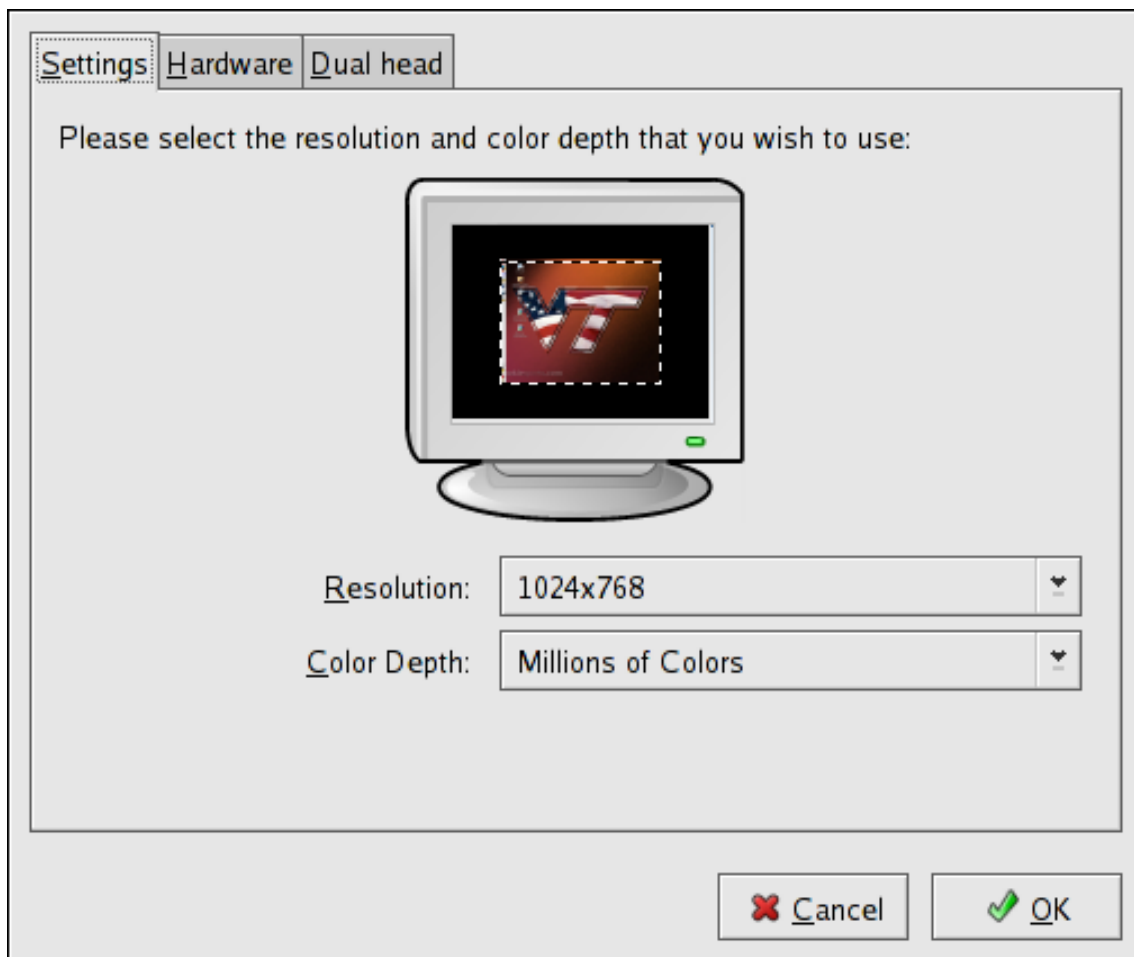
設定を変更したら、グラフィカルデスクトップからログアウトし、ログインし直して変更を有効にします。

### 31.1. 表示設定

Settings タブを使用すると、ユーザーは 解像度 および 色深度 を変更できます。モニターの表示は、ピクセルと呼ばれる小さなドットで構成されています。一度に表示されるピクセルの数は、解像度と呼ばれます。たとえば、解像度 1024x768 は、1024 水平ピクセルと 768 の垂直ピクセルが使用されることを意味します。解像度の値が高いと、モニターが一度に表示できる複数のイメージがあります。

表示の色深度により、表示される色の数が決まります。色深度が高いことは、色間の対比を意味します。

図31.1 表示設定

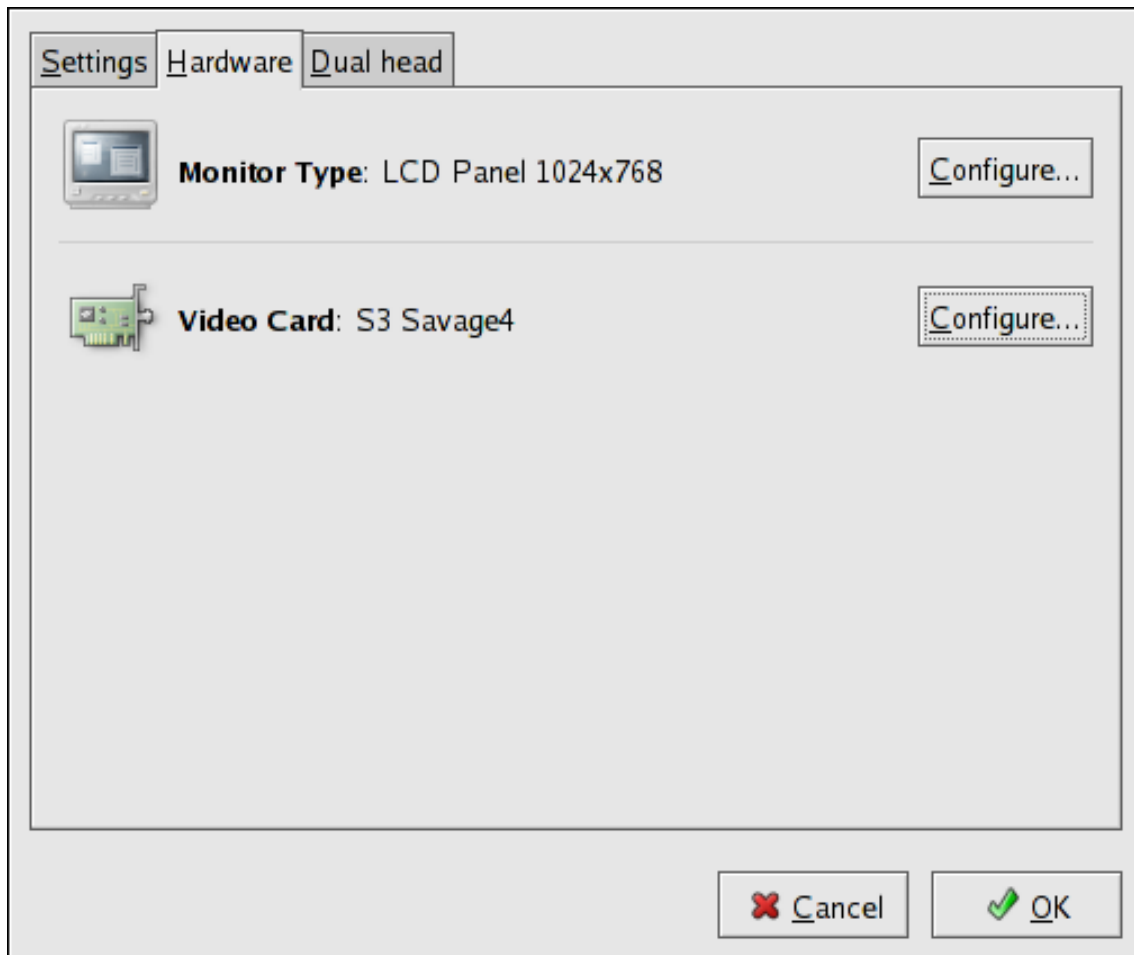


[D]

### 31.2. ハードウェア設定の表示

*X Configuration Tool* が起動すると、モニターとビデオカードがプローブされます。ハードウェアが適切にプローブされている場合は、[図31.2 「ハードウェア設定の表示」](#) に示されるように **Hardware** タブにその情報が表示されます。

図31.2 ハードウェア設定の表示



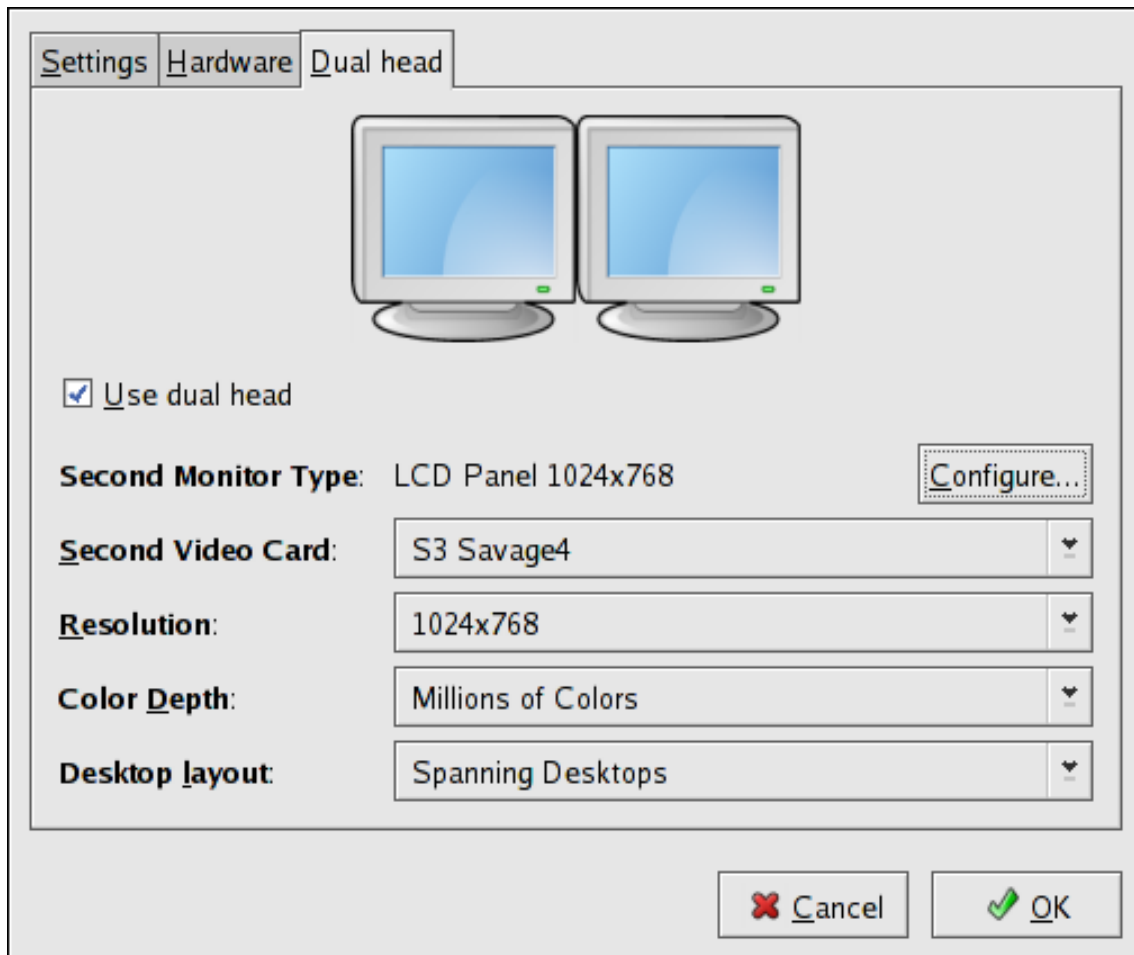
[D]

監視タイプまたはその設定のいずれかを変更するには、該当する **Configure** ボタンをクリックします。ビデオカードの種類やその設定を変更するには、設定の横にある **Configure** ボタンをクリックします。

### 31.3. デュアルヒューリスティックディスプレイの設定

システムに複数のビデオカードがインストールされている場合は、デュアルヘッドモニターのサポートが利用可能になり、[図31.3 「デュアルヒューリスティックディスプレイの設定」](#) に示されているように **Dual head** タブで設定されます。

図31.3 デュアルヒューリスティックディスプレイの設定



[D]

*Dual head* の使用を有効にするには、*Use dual head* チェックボックスを選択します。

2 つ目の監視タイプを設定するには、該当する *Configure* ボタンをクリックします。対応するドロップダウンリストを使用して、他の *Dual head* 設定を設定することもできます。

*Desktop layout* オプションの場合は、*Spanning* を選択すると、両方のモニターで使用可能なワークスペースが拡大されます。個別選択を選択すると、ディスプレイ間でマウスとキーボードが共有されますが、ウィンドウを1つのディスプレイに制限します。

## 第32章 ユーザーとグループ

ユーザー および グループ の制御は、Red Hat Enterprise Linux システム管理の中核となる要素です。

ユーザー は、ユーザー（物理システムに関連するアカウント）または、使用する特定のアプリケーションに存在するアカウントのいずれかを指定できます。

グループ は組織の論理式で、共通の目的でユーザーをグループ化します。グループ内のユーザーは、そのグループが所有するファイルの読み取り、書き込み、実行が可能です。

各ユーザーおよびグループには、userid (UID)と groupid (GID)と呼ばれる一意の数值 ID 番号があります。

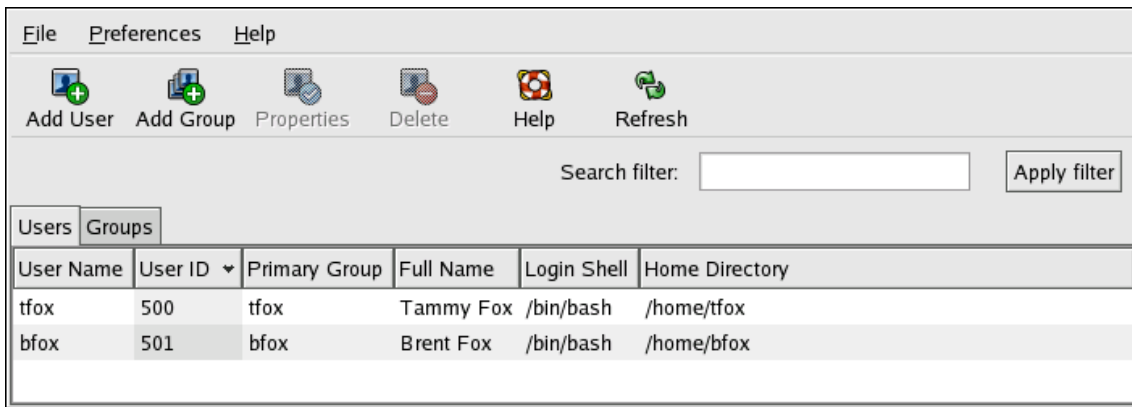
ファイルを作成するユーザーは、そのファイルの所有者であり、グループ所有者でもあります。ファイルには、所有者、グループ、その他に対して読み取り、書き込み、実行のパーミッションが別々に割り当てられます。ファイルの所有者は root ユーザーのみが変更できます。アクセスパーミッションは、root ユーザーとファイル所有者の両方が変更できます。

### 32.1. ユーザーおよびグループの設定

User Manager では、ローカルユーザーおよびグループの表示、変更、追加、削除が可能です。

ユーザー マネージャー を使用するには、X Window System を実行し、root 権限があり、system-config-users 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。デスクトップから User Manager を起動するには、Applications（パネルのメインメニュー）=> Administration => Users & Groups の順に移動します。シェルプロンプトで system-config-users コマンドを入力することもできます（例：XTerm や GNOME ターミナル）。

図32.1 User Manager



[D]

システムでローカルユーザーの一覧を表示するには、**Users** タブをクリックします。システムでローカルグループの一覧を表示するには、**Groups** タブをクリックします。

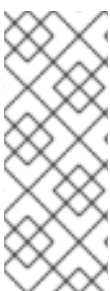
特定のユーザーまたはグループを検索するには、**Search filter** フィールドに名前の最初の数文字を入力します。**Enter** を押すか、**Apply filter** ボタンをクリックします。フィルターされたリストが表示されます。

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、その列の値に従ってソートされます。

**Red Hat Enterprise Linux** は、システムユーザー用に 500 以下のユーザー ID を確保します。デフォルトでは、**User Manager** 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むすべてのユーザーを表示するには、**Edit => Preferences** の順に移動し、ダイアログボックスから **Hide system users and groups** の選択を解除します。

### 32.1.1. 新規ユーザーの追加

新規ユーザーを追加するには、ユーザーの **追加** ボタンをクリックします。図32.2「新規ユーザー」に示されているウィンドウが表示されます。適切なフィールドに、新規ユーザーのユーザー名およびフル名を入力します。**Password** フィールドおよび **Confirm Password** 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

これにより、侵入者が推測し、パーミッションなしでアカウントにアクセスするのがより困難になるため、より長いパスワードを使用することが推奨されます。また、辞書用語にベースではないパスワードも推奨し、文字、数字、および特殊文字の組み合わせを使用します。

ログインシェルを選択します。選択するシェルが不明な場合は、デフォルト値の `/bin/bash` を受け入れます。デフォルトのホームディレクトリーは `/home/<username>/` です。ユーザー用に作成したホームディレクトリーを変更するか、`Create home directory` の選択を解除してホームディレクトリーを作成しないよう選択することもできます。

ホームディレクトリーの作成を選択すると、デフォルトの設定ファイルが `/etc/skel/` ディレクトリーから新しいホームディレクトリーにコピーされます。

Red Hat Enterprise Linux は、ユーザープライベートグループ (UPG) スキームを使用します。UPG スキームは、グループを処理する標準の UNIX 方法で追加または変更されません。新しい規則が提供されています。デフォルトでは、新規ユーザーを作成するたびに、そのユーザーと同じ名前を持つ一意のグループが作成されます。このグループを作成したくない場合は、そのユーザー用に「`Create a private group`」を選択します。

ユーザーのユーザー ID を指定するには、ユーザー ID を手動で指定するを選択します。このオプションが選択されていない場合は、次に 500 を超える利用可能なユーザー ID が新規ユーザーに割り当てられます。Red Hat Enterprise Linux は、システムユーザー用に 500 未満のユーザー ID を確保するため、ユーザー ID 1 ~ 499 を手動で割り当てることは推奨されません。

OK をクリックしてユーザーを作成します。



図32.2 新規ユーザー

User Name: tfox

Full Name: Tammy Fox

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Login Shell: /bin/bash

Create home directory

Home Directory: /home/tfox

Create a private group for the user

Specify user ID manually

UID: 500

Cancel OK

[D]

パスワードの有効期限などの高度なユーザープロパティを設定するには、ユーザーを追加した後にユーザーのプロパティを変更します。詳細は、「[ユーザープロパティの変更](#)」を参照してください。

### 32.1.2. ユーザープロパティの変更

既存のユーザーのプロパティを表示するには、**Users** タブをクリックして、ユーザーリストからユーザーを選択し、メニューから **Properties** をクリックします（または、プルダウンメニューから **File => Properties** と選択します）。[図32.3 「ユーザープロパティ」](#) のようなウィンドウが表示されます。

図32.3 ユーザープロパティ

User Data	Account Info	Password Info	Groups
User Name:	tfox		
Full Name:	Tammy Fox		
Password:	*****		
Confirm Password:	*****		
Home Directory:	/home/tfox		
Login Shell:	/bin/bash		

Cancel OK

[D]

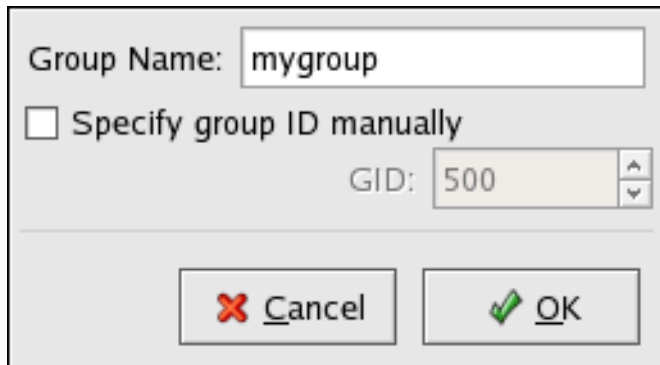
ユーザープロパティウィンドウは、複数のタブ化されたページに分割されます。

- **User Data:** ユーザーの追加時に設定された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ー、またはログインシェルを変更します。
- **アカウント情報 -** 特定の日付でアカウントの有効期限が切れるようにするには、**Enable account expiration** を選択します。指定のフィールドに日付を入力します。**Local password is locked** を選択して、ユーザーアカウントをロックし、ユーザーがシステムにログインできないようにします。
- **Password Info:** ユーザーのパスワードが最後に変更した日付を表示します。特定の日後にパスワードを変更するように強制するには、**Enable password expiration** を選択し、**required:** フィールドを変更する前に **Days** に必要な値を入力します。ユーザーのパスワードが期限切れになるまでの日数、パスワードの変更をユーザーに警告する日数、アカウントが非アクティブになる前の日数も変更可能です。
- **Groups:** ユーザーのプライマリーグループと、ユーザーを所属させる他のグループを表示および設定できます。

### 32.1.3. 新規グループの追加

新規ユーザーグループを追加するには、グループの追加 ボタンをクリックします。図32.4「新規グループ」のようなウィンドウが表示されます。作成する新規グループの名前を入力します。新規グループのグループIDを指定するには、グループIDを手動で選択し、GIDを選択します。Red Hat Enterprise Linux は、システムグループ用に500未満のグループIDを確保することに注意してください。

図32.4 新規グループ



[D]

OK 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。

#### 32.1.4. グループプロパティーの変更

既存のグループのプロパティーを表示するには、グループリストからグループを選択し、メニューから **Properties** をクリックします（または、プルダウンメニューから **File => Properties** を選択します）。図32.5「グループプロパティー」のようなウィンドウが表示されます。

図32.5 グループプロパティ



[D]

**Group Users** タブには、グループのメンバーであるユーザーが表示されます。このタブを使用してグループに対してユーザーを追加または削除します。OK をクリックして変更を保存します。

## 32.2. ユーザーおよびグループ管理ツール

ユーザーおよびグループの管理は、多重なタスクになります。そのため、Red Hat Enterprise Linux はそれらを管理しやすくするためのツールおよび規則を提供しています。

ユーザーおよびグループを管理する最も簡単な方法は、グラフィカルアプリケーションの **User Manager (system-config-users)** を使用して行います。ユーザー マネージャーの詳細は、「[ユーザーおよびグループの設定](#)」を参照してください。

以下のコマンドラインツールを使用して、ユーザーおよびグループを管理することもできます。

- **useradd**、**usermod**、および **userdel**: ユーザーアカウントを追加、削除、および変更するための業界標準の手法
- **groupadd**、**groupmod**、および **groupdel**: ユーザーグループを追加、削除、変更するための業界標準の手法

- **gpasswd: /etc/group ファイルを管理する方法の業界標準**
- **pwck, grpck - パスワード、グループ、および関連するシャドウファイルの検証に使用されるツール**
- **pwconv, pwunconv - シャドウパスワードへの変換および標準パスワードに戻るツール**

### 32.2.1. コマンドラインからの設定

コマンドラインツールを使用する場合や、X Window System がインストールされていない場合は、本セクションを使用してユーザーとグループを設定します。

### 32.2.2. ユーザーの追加

システムをユーザーを追加するには、以下を実行します。

1. **useradd** コマンドを実行して、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** コマンドを実行してパスワードを割り当て、パスワードのページガイドラインを設定してアカウントのロックを解除します。

```
passwd <username>
```

**useradd** のコマンドラインオプションの詳細は、[表32.1 「useradd コマンドラインオプション」](#) を参照してください。

表32.1 useradd コマンドラインオプション

オプション	Description
-c '<comment>'	& lt;comment&gt; は任意の文字列に置き換えることができます。このオプションは、通常、ユーザーの氏名を指定するのに使用されません。

オプション	Description
<b>-d &lt;home-dir&gt;</b>	デフォルトの /home/<username> / の代わりに使用するホームディレクトリー
<b>-e &lt;date&gt;</b>	YYYY-MM-DD 形式でアカウントを無効にする日付
<b>-f &lt;days&gt;</b>	パスワードが失効してからアカウントが無効になるまでの日数です。0 を指定すると、パスワードが失効した直後にアカウントが無効になります。-1 を指定すると、パスワードが失効してもアカウントは無効になりません。
<b>-g &lt;group-name&gt;</b>	ユーザーのデフォルトグループ用のグループ名またはグループ番号。グループは、ここで指定するよりも前に作成されている必要があります。
<b>-G &lt;group-list&gt;</b>	ユーザーがメンバーとなっている追加（デフォルト）のグループ名またはグループ番号の一覧（コンマで区切られた）。グループは、ここで指定する前に作成しておく必要があります。
<b>-m</b>	ホームディレクトリーがない場合は、これを作成します。
<b>-M</b>	ホームディレクトリーを作成しません。
<b>-n</b>	ユーザー用のユーザープライベートグループを作成しません。
<b>-r</b>	
<b>-p &lt;password&gt;</b>	
<b>-s</b>	
<b>-u &lt;uid&gt;</b>	

### 32.2.3.

```
groupadd <group-name>
```

表32.2

オプション	Description
<code>-g &lt;gid&gt;</code>	
<code>-r</code>	
<code>-f</code>	

## 32.2.4.



## 重要な影響

表32.3

オプション	Description
<code>-M &lt;days&gt;</code>	このオプションで指定した日数と、 <code>-d</code> オプションで指定した日数を足した日数が、現在の日数より少ない場合、ユーザーはアカウントを使用する前にパスワードを変更する必要があります。
<code>-d &lt;days&gt;</code>	
<code>-l &lt;days&gt;</code>	パスワードの有効期限後、アカウントをロックするまでの非アクティブ日数を指定します。
<code>-E &lt;date&gt;</code>	アカウントがロックされる日付を YYYY-MM-DD のフォーマットで指定します。日付の代わりに、1970年1月1日からの日数を使うこともできます。
<code>-W &lt;days&gt;</code>	パスワードの有効期限の何日前にユーザーに警告を発するかを指定します。

ユーザーが初めてログインしたときにパスワードが失効するように設定することができます。



#### 備考

1.

```
usermod -L username
```

2.

```
chage -d 0 username
```

このコマンドは、パスワードが最後に変更された日付の値をエポック (1970年1月1日) に設定します。この値は、パスワードエージングポリシーがある場合、それに関係なく、パスワードの即時期限切れを強制します。

3.



#### WARNING



- 

```
Python 2.4.3 (#1, Jul 21 2006, 08:46:09)
[GCC 4.1.1 20060718 (Red Hat 4.1.1-9)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

- 

```
import crypt; print crypt("<password>", "<salt>")
```

- 

- 

```
usermod -p "<encrypted-password>" <username>
```

これを行うには、以下のコマンドを使用します。

```
usermod -p "" username
```



**WARNING**

### 32.2.5. プロセスの説明

1.

この行には以下の特徴があります。

- 

- 

- 

- 

- 

- 

- 

2.

この行には以下の特徴があります。

- 

- 



備考

- パスワードは有効期限なしで設定されています。

3.

- 

- 

- 

4.

この行には以下の特徴があります。

- 

- 

- 

その他のフィールドはすべて空白です。

5.

その他のパーミッションは拒否されます。

6.

32.3.

表32.4

<i>User</i>	<i>UID</i>	<i>GID</i>		<i>シェル</i>
<i>root</i>	<i>0</i>	<i>0</i>	<i>/root</i>	<i>/bin/bash</i>
	<i>1</i>	<i>1</i>	<i>/bin</i>	<i>/sbin/nologin</i>
<i>daemon</i>	<i>2</i>	<i>2</i>	<i>/sbin</i>	<i>/sbin/nologin</i>
<i>adm</i>	<i>3</i>	<i>4</i>	<i>/var/adm</i>	<i>/sbin/nologin</i>
<i>lp</i>	<i>4</i>	<i>7</i>	<i>/var/spool/lpd</i>	<i>/sbin/nologin</i>
<i>sync</i>	<i>5</i>	<i>0</i>	<i>/sbin</i>	<i>/bin/sync</i>
<i>shutdown</i>	<i>6</i>	<i>0</i>	<i>/sbin</i>	<i>/sbin/shutdown</i>
<i>halt</i>	<i>7</i>	<i>0</i>	<i>/sbin</i>	<i>/sbin/halt</i>
<i>mail</i>	<i>8</i>	<i>12</i>	<i>/var/spool/mail</i>	<i>/sbin/nologin</i>
<i>news</i>	<i>9</i>	<i>13</i>	<i>/etc/news</i>	
<i>uucp</i>	<i>10</i>	<i>14</i>	<i>/var/spool/uucp</i>	<i>/sbin/nologin</i>
<i>operator</i>	<i>11</i>	<i>0</i>	<i>/root</i>	<i>/sbin/nologin</i>
	<i>12</i>	<i>100</i>	<i>/usr/games</i>	<i>/sbin/nologin</i>
	<i>13</i>	<i>30</i>	<i>/var/gopher</i>	<i>/sbin/nologin</i>
<i>ftp</i>	<i>14</i>	<i>50</i>	<i>/var/ftp</i>	<i>/sbin/nologin</i>
<i>nobody</i>	<i>99</i>	<i>99</i>	<i>/</i>	<i>/sbin/nologin</i>
<i>rpm</i>	<i>37</i>	<i>37</i>	<i>/var/lib/rpm</i>	<i>/sbin/nologin</i>
<i>vcsa</i>	<i>69</i>	<i>69</i>	<i>/dev</i>	<i>/sbin/nologin</i>
<i>dbus</i>	<i>81</i>	<i>81</i>	<i>/</i>	<i>/sbin/nologin</i>

<i>User</i>	<i>UID</i>	<i>GID</i>		<i>シェル</i>
<i>ntp</i>	<b>38</b>	<b>38</b>	<i>/etc/ntp</i>	<i>/sbin/nologin</i>
	<b>39</b>	<b>39</b>	<i>/var/lib/canna</i>	<i>/sbin/nologin</i>
<i>nscd</i>	<b>28</b>	<b>28</b>	<i>/</i>	<i>/sbin/nologin</i>
<i>rpc</i>	<b>32</b>	<b>32</b>	<i>/</i>	<i>/sbin/nologin</i>
<i>postfix</i>	<b>89</b>	<b>89</b>	<i>/var/spool/postfix</i>	<i>/sbin/nologin</i>
<i>mailman</i>	<b>41</b>	<b>41</b>	<i>/var/mailman</i>	<i>/sbin/nologin</i>
<i>named</i>	<b>25</b>	<b>25</b>	<i>/var/named</i>	<i>/bin/false</i>
<i>amanda</i>	<b>33</b>	<b>6</b>	<i>var/lib/amanda/</i>	<i>/bin/bash</i>
<i>postgres</i>	<b>26</b>	<b>26</b>	<i>/var/lib/pgsql</i>	<i>/bin/bash</i>
<i>exim</i>	<b>93</b>	<b>93</b>	<i>/var/spool/exim</i>	<i>/sbin/nologin</i>
<i>sshd</i>	<b>74</b>	<b>74</b>	<i>/var/empty/sshd</i>	<i>/sbin/nologin</i>
<i>rpcuser</i>	<b>29</b>	<b>29</b>	<i>/var/lib/nfs</i>	<i>/sbin/nologin</i>
<i>nfsnobody</i>	<b>6553 4</b>	<b>6553 4</b>	<i>/var/lib/nfs</i>	<i>/sbin/nologin</i>
<i>pvm</i>	<b>24</b>	<b>24</b>	<i>/usr/share/pvm3</i>	<i>/bin/bash</i>
<i>apache</i>	<b>48</b>	<b>48</b>	<i>/var/www</i>	<i>/sbin/nologin</i>
<i>xfst</i>	<b>43</b>	<b>43</b>	<i>/etc/X11/fs</i>	<i>/sbin/nologin</i>
<i>gdm</i>	<b>42</b>	<b>42</b>	<i>/var/gdm</i>	<i>/sbin/nologin</i>
<i>htt</i>	<b>100</b>	<b>101</b>	<i>/usr/lib/im</i>	<i>/sbin/nologin</i>
<i>mysql</i>	<b>27</b>	<b>27</b>	<i>/var/lib/mysql</i>	<i>/bin/bash</i>
<i>webalizer</i>	<b>67</b>	<b>67</b>	<i>/var/www/usage</i>	<i>/sbin/nologin</i>

<i>User</i>	<i>UID</i>	<i>GID</i>		<i>シェル</i>
	<b>47</b>	<b>47</b>	<b><i>/var/spool/mqueue</i></b>	<b><i>/sbin/nologin</i></b>
<b><i>smmsp</i></b>	<b>51</b>	<b>51</b>	<b><i>/var/spool/mqueue</i></b>	<b><i>/sbin/nologin</i></b>
<b><i>squid</i></b>	<b>23</b>	<b>23</b>	<b><i>/var/spool/squid</i></b>	<b><i>/sbin/nologin</i></b>
<b><i>ldap</i></b>	<b>55</b>	<b>55</b>	<b><i>/var/lib/ldap</i></b>	<b><i>/bin/false</i></b>
<b><i>netdump</i></b>	<b>34</b>	<b>34</b>	<b><i>/var/crash/</i></b>	<b><i>/bin/bash</i></b>
<b><i>pcap</i></b>	<b>77</b>	<b>77</b>	<b><i>/var/arpwatch</i></b>	<b><i>/sbin/nologin</i></b>
	<b>95</b>	<b>95</b>	<b><i>/</i></b>	<b><i>/bin/false</i></b>
<b><i>radvd</i></b>	<b>75</b>	<b>75</b>	<b><i>/</i></b>	<b><i>/sbin/nologin</i></b>
<b><i>quagga</i></b>	<b>92</b>	<b>92</b>	<b><i>/var/run/quagga</i></b>	<b><i>/sbin/login</i></b>
	<b>49</b>	<b>49</b>	<b><i>/var/lib/wnn</i></b>	<b><i>/sbin/nologin</i></b>
<b><i>dovecot</i></b>	<b>97</b>	<b>97</b>	<b><i>/usr/libexec/dovecot</i></b>	<b><i>/sbin/nologin</i></b>

## 32.4.

表32.5

<i>Group</i>	<i>GID</i>	<i>Members</i>
<b><i>root</i></b>	<b>0</b>	<b><i>root</i></b>
	<b>1</b>	
<b><i>daemon</i></b>	<b>2</b>	
<b><i>sys</i></b>	<b>3</b>	
<b><i>adm</i></b>	<b>4</b>	

<i>Group</i>	<i>GID</i>	<i>Members</i>
	5	
<i>disk</i>	6	<i>root</i>
<i>lp</i>	7	
<i>mem</i>	8	
	9	
ホイール	10	<i>root</i>
<i>mail</i>	12	
<i>news</i>	13	<i>news</i>
<i>uucp</i>	14	<i>uucp</i>
<i>man</i>	15	
	20	
	30	
	40	
<i>ftp</i>	50	
<i>lock</i>	54	
<i>nobody</i>	99	
<i>users</i>	100	
<i>rpm</i>	37	
<i>utmp</i>	22	
<i>floppy</i>	19	

<i>Group</i>	<i>GID</i>	<i>Members</i>
<i>vcsa</i>	<i>69</i>	
<i>dbus</i>	<i>81</i>	
<i>ntp</i>	<i>38</i>	
	<i>39</i>	
<i>nscd</i>	<i>28</i>	
<i>rpc</i>	<i>32</i>	
<i>postdrop</i>	<i>90</i>	
<i>postfix</i>	<i>89</i>	
<i>mailman</i>	<i>41</i>	
<i>exim</i>	<i>93</i>	
<i>named</i>	<i>25</i>	
<i>postgres</i>	<i>26</i>	
<i>sshd</i>	<i>74</i>	
<i>rpcuser</i>	<i>29</i>	
<i>nfsnobody</i>	<i>65534</i>	
<i>pvm</i>	<i>24</i>	
<i>apache</i>	<i>48</i>	
<i>xfx</i>	<i>43</i>	
<i>gdm</i>	<i>42</i>	
<i>htt</i>	<i>101</i>	



<i>Group</i>	<i>GID</i>	<i>Members</i>
<i>mysql</i>	<i>27</i>	
<i>webalizer</i>	<i>67</i>	
<i>mailnull</i>	<i>47</i>	
<i>smmsp</i>	<i>51</i>	
<i>squid</i>	<i>23</i>	
<i>ldap</i>	<i>55</i>	
<i>netdump</i>	<i>34</i>	
<i>pcap</i>	<i>77</i>	
<i>quaggavt</i>	<i>102</i>	
<i>quagga</i>	<i>92</i>	
<i>radvd</i>	<i>75</i>	
<i>Slocate</i>	<i>21</i>	
<i>wnn</i>	<i>49</i>	
<i>dovecot</i>	<i>97</i>	
<i>radiusd</i>	<i>95</i>	

### 32.5. ユーザープライベートグループ

**Red Hat Enterprise Linux** では ユーザープライベートグループ (UPG) スキームが使用されているため、UNIX グループの管理が容易になります。

UPG は、新規ユーザーがシステムに追加されるたびに作成されます。UPG は、作成したユーザーと同じ名前で、そのユーザーが UPG の唯一のメンバーになります。

UPG を使用すると、新規に作成したファイルまたはディレクトリーに対して確実にデフォルトのパーミッションを設定できます。これにより、ユーザーとそのユーザーのグループの両方がファイルまたはディレクトリーを修正できるようになります。

新規に作成するファイルまたはディレクトリーに適用される権限を決定する設定は `umask` と呼ばれ、`/etc/bashrc` ファイルで設定します。従来の UNIX システムでは、`umask` は `022` に設定されており、ファイルまたはディレクトリーを作成したユーザーしか変更できませんでした。このスキームでは、作成者のグループのメンバーなど、他のユーザーは変更できません。ただし、UPG スキームでは、すべてのユーザーがそれぞれプライベートグループを持つため、この「グループ保護」は必須ではなくなりました。

### 32.5.1. グループディレクトリー

多くの IT 組織では、主要なプロジェクトに対してグループを作成し、そのプロジェクトのファイルにアクセスする必要がある場合に、そのユーザーをグループに割り当てます。この従来のスキームを使用すると、ファイルの管理は困難でした。ユーザーがファイルを作成すると、そのファイルが属するプライマリグループに関連付けられます。1人のユーザーが複数のプロジェクトで作業を行う場合は、正しいファイルを適切なグループに関連付けることは困難です。ただし、UPG スキームを使用すると、グループは `setgid` ビットセットを持つディレクトリーに作成されたファイルに自動的に割り当てられます。`setgid` ビットを使用すると、共通ディレクトリーを共有するグループプロジェクトを非常に簡単に管理できます。これは、ユーザーがディレクトリー内で作成するすべてのファイルは、そのディレクトリーを所有するグループによって所有されるためです。

たとえば、あるグループが `/usr/share/emacs/site-lisp/` ディレクトリーのファイルで作業する必要があるとします。ディレクトリーの修正を信頼できる人もありますが、誰もが信頼されているわけではありません。まず、以下のコマンドのように `emacs` グループを作成します。

```
/usr/sbin/groupadd emacs
```

ディレクトリーの内容を `emacs` グループに関連付けるには、以下を入力します。

```
chown -R root.emacs /usr/share/emacs/site-lisp
```

`gpasswd` コマンドを使用して、適切なユーザーをグループに追加できるようになりました。

```
/usr/bin/gpasswd -a <username> emacs
```

ユーザーがディレクトリーにファイルを作成できるようにするには、次のコマンドを使用します。

```
chmod 775 /usr/share/emacs/site-lisp
```

ユーザーが新しいファイルを作成すると、そのユーザーのデフォルトプライベートグループのグループが割り当てられます。次に `setgid` ビットを設定します。このビットは、ディレクトリー自体と同じグループパーミッション(`emac`s)に作成されたものをすべて割り当てます。以下のコマンドを使用します。

```
chmod 2775 /usr/share/emacs/site-lisp
```

この時点で、各ユーザーのデフォルトの `umask` は `002` であるため、`emac`s グループのすべてのメンバーは、ユーザーが新しいファイルを書き込むたびにファイルを変更しなくても、`/usr/share/emacs/site-lisp/` ディレクトリーにファイルを作成および編集できます。

## 32.6. シャドウパスワード

マルチユーザー環境では、シャドウパスワードを使用することが非常に重要です (`shadow-utils` パッケージで提供されます)。これにより、システム認証ファイルのセキュリティを強化します。このため、インストールプログラムでは、デフォルト設定でシャドウパスワードを有効にしています。

以下は、UNIX ベースのシステムにパスワードを格納する従来の方法と比較して、`pf`d シャドウパスワードの利点を示しています。

- 暗号化されたパスワードハッシュを、あらゆるユーザーが読み取り可能な `/etc/passwd` ファイルから、`root` ユーザーのみが読み取り可能な `/etc/shadow` に移動して、システムセキュリティを向上させます。
- パスワードのマージに関する情報を保存します。
- `/etc/login.defs` ファイルを使用してセキュリティポリシーを強制できるようにします。

`shadow-utils` パッケージが提供するほとんどのユーティリティーは、シャドウパスワードが有効かどうかに関わらず適切に機能します。ただし、パスワードの変更情報は `/etc/shadow` ファイルにのみ格納されるため、パスワードの変更情報を作成または変更するコマンドは機能しません。

シャドウパスワードを有効にしなくても機能しないコマンドのリストを以下に示します。

- `chage`

- **`gpasswd`**
- **`/usr/sbin/usermod -e` オプションまたは `-f` オプション**
- **`/usr/sbin/useradd -e` オプションまたは `-f` オプション**

## 32.7. 関連情報

ユーザーおよびグループ、およびそれらを管理するツールの詳細は、以下のリソースを参照してください。

### 32.7.1. インストールされているドキュメント

- **関連する man ページ:** ユーザーおよびグループの管理に関連するさまざまなアプリケーションや設定ファイルの man ページが多数あります。その他重要な man ページは、以下に挙げています。

#### ユーザーおよびグループ管理アプリケーション

- **`mangitops`:** パスワードのマージポリシーおよびアカウントの有効期限を変更するコマンド。
- **`man gpasswd - /etc/group`** ファイルを管理するコマンドです。
- **`man groupadd`** - グループを追加するコマンド
- **`man grpck - /etc/group`** ファイルを確認するコマンド。
- **`man groupdel`:** グループを削除するコマンド。
- **`man groupmod`** - グループメンバーシップを変更するコマンド。
- **`man pwck - /etc/passwd`** ファイルおよび `/etc/shadow` ファイルを検証するコマンド。

- **man pwconv**: 標準パスワードをシャドウパスワードに変換するツール。
- **man pwunconv**: シャドウパスワードを標準パスワードに変換するツール。
- **man useradd** - ユーザーを追加するコマンド。
- **man userdel**: ユーザーを削除するコマンド。
- **man usermod**: ユーザーを変更するコマンド。

#### 設定ファイル

- **man 5 グループ**: システムのグループ情報が含まれるファイル。
- **man 5 passwd** - システムのユーザー情報を含むファイル。
- **man 5 shadow**: システムのパスワードおよびアカウントの有効期限情報が含まれるファイル。

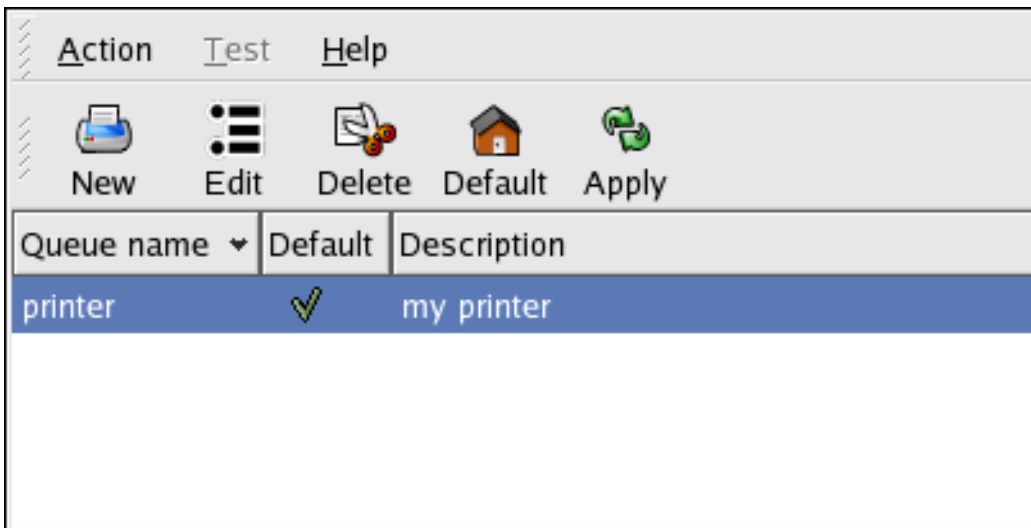
## 第33章 プリンターの設定

**Printer Configuration Tool** を使用すると、ユーザーはプリンターを設定できます。このツールは、プリンター設定ファイル、印刷プールディレクトリー、印刷フィルター、プリンタークラスの維持に役立ちます。

**Red Hat Enterprise Linux 4** は、**Common Unix Printing System(CUPS)**を使用します。**CUPS** を使用した以前の **Red Hat Enterprise Linux** バージョンからシステムをアップグレードすると、アップグレードプロセスにより、設定したキューが保持されます。

**Printer Configuration Tool** を使用するには、**root** 権限が必要です。アプリケーションを起動するには、**Applications** (パネルのメインメニュー) => **Administration** => **Printing** を選択するか、シェルプロンプトで **system-config-printer** コマンドを入力します。

図33.1 プリンター設定ツール



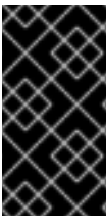
[D]

以下のタイプの印刷キューを設定できます。

- **AppSocket/HP JetDirect** - コンピューターの代わりに **HP JetDirect** インターフェースまたは **Appsocket** インターフェースを介してネットワークに直接接続されたプリンター。
- **IPP(Internet Printing Protocol)** - **Internet Printing Protocol** を介して **TCP/IP** ネットワーク経由でアクセス可能なプリンター (たとえば、ネットワーク上の **CUPS** を実行している別の **Red Hat Enterprise Linux** システムに接続されているプリンターなど)。
- **LPD/LPR Host or Printer: TCP/IP** ネットワーク上でアクセス可能な別の **UNIX** システムに

接続されているプリンター（たとえば、ネットワーク上で LPD を実行している別の Red Hat Enterprise Linux システムに接続されているプリンターなど）。

- ネットワーク Windows(SMB): SMB ネットワークでプリンターを共有する別のシステム (Microsoft Windows™ マシンに接続されているプリンターなど) に接続されているプリンター。
- Networked JetDirect - コンピューターの代わりに HP JetDirect を介してネットワークに直接接続されたプリンター。



#### 重要な影響

新しい印刷キューを追加するか、または既存のキューを変更する場合は、変更を適用する必要があります。

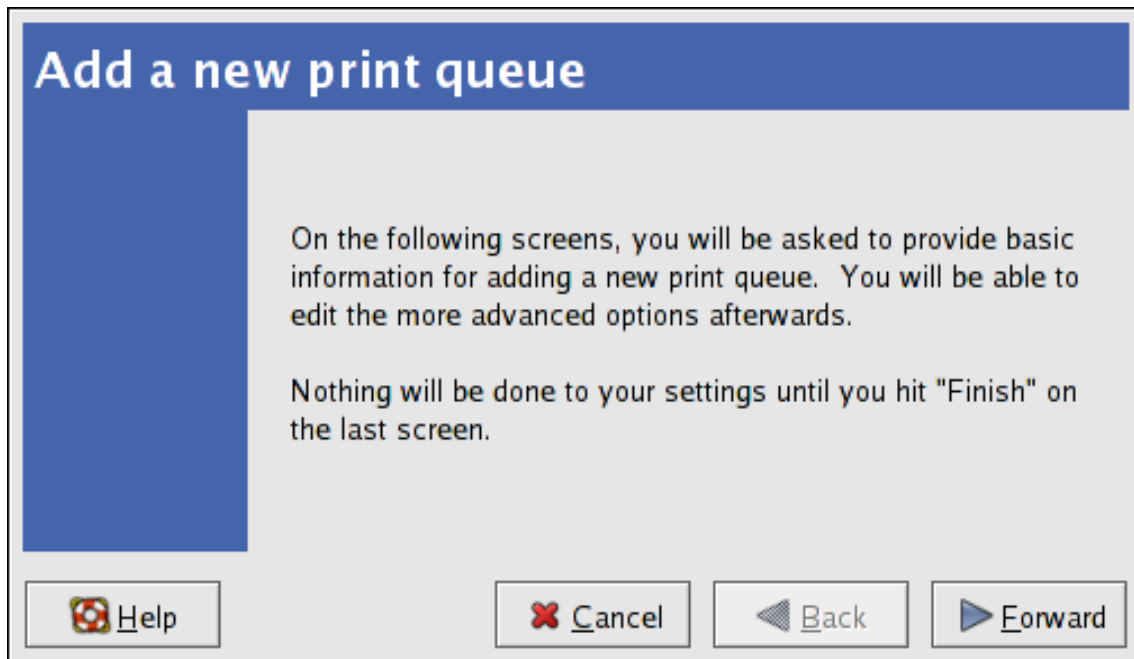
Apply ボタンをクリックすると、設定した変更でプリンターデーモンが再起動するように求められます。

戻す ボタンをクリックすると、適用されていない変更は破棄されます。

### 33.1. ローカルプリンターの追加

並列ポート、コンピューターの USB ポートなどを介して接続しているローカルプリンターを追加するには、メインの Printer Configuration Tool ウィンドウで New Printer ボタンをクリックして、[図 33.2 「プリンターの追加」](#) にウィンドウを表示します。

図33.2 プリンターの追加



[D]

**Forward** をクリックして先に進みます。

**Printer Name** フィールドにプリンターの一意的名前を入力します。プリンター名には、文字、数字、ダッシュ(-)、およびアンダースコア(\_)を使用できます。スペースを含めることはできません。

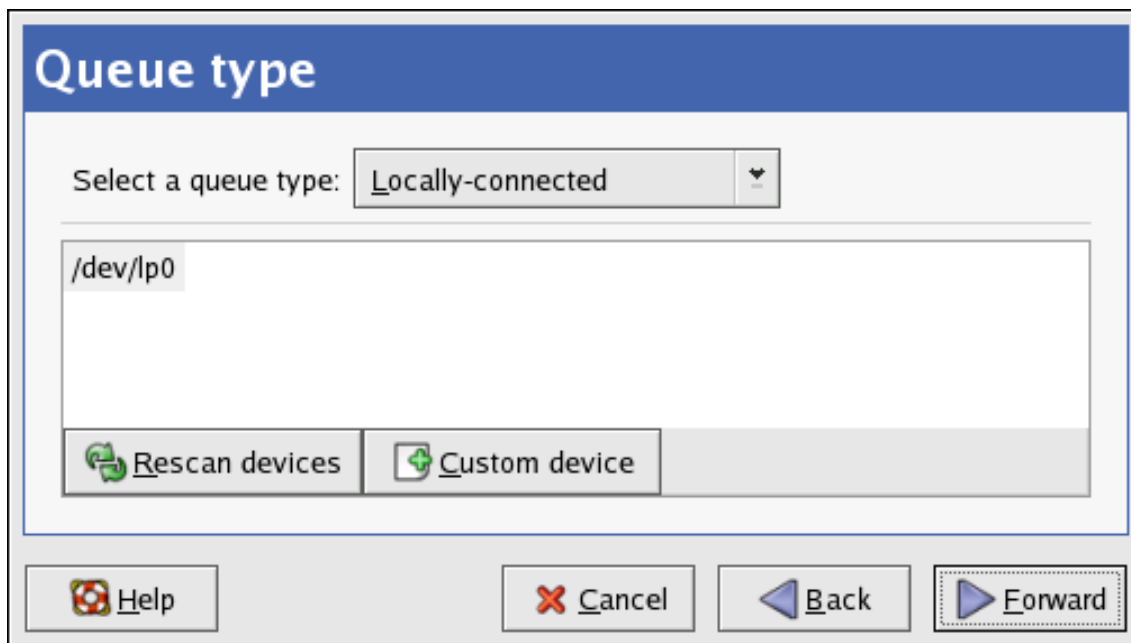
また、**説明** フィールドおよび **Location** フィールドを使用して、このプリンターと、システムに設定した可能性のある他のプリンターをさらに区別することもできます。これらのフィールドはいずれも任意で、スペースを含めることができます。

**Forward** をクリックして **New Printer** ダイアログを開きます（[図33.3「ローカルプリンターの追加」](#)を参照）。プリンターが自動的に検出されると、プリンターのモデルが **接続の選択** に表示されます。プリンターモデルを選択し、**進む** をクリックして続行します。

デバイスが自動的に表示されない場合は、**接続の選択** でプリンターを接続するデバイスを選択します（**LPT # 1** や **Serial Port #1** など）。



図33.3 ローカルプリンターの追加



[D]

次に、プリンタータイプを選択します。詳細は、「[プリンターモデルの選択と完了](#)」を参照してください。

### 33.2. IPP プリンターの追加

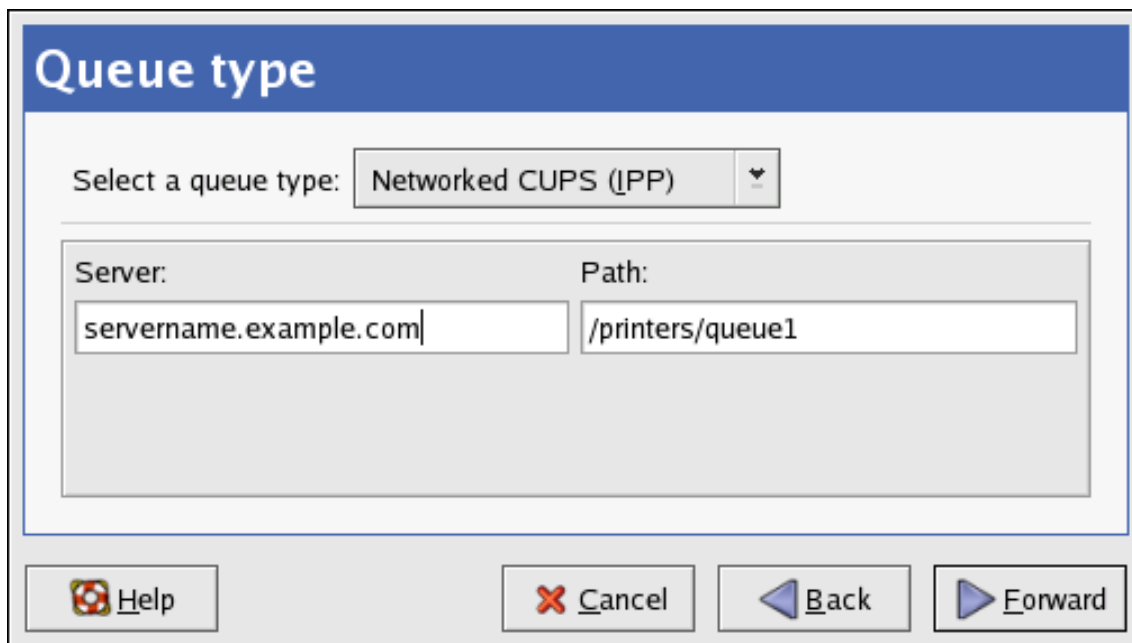
IPP プリンターは同じ TCP/IP ネットワークにある別のシステムに接続されているプリンターです。このプリンターがアタッチされているシステムは CUPS を実行しているか、または単に IPP を使用するように設定されているだけです。

プリンターサーバーでファイアウォールが有効な場合は、受信 UDP ポート 631 での送受信接続を許可するようにファイアウォールを設定する必要があります。クライアントでファイアウォールが有効になっている場合（出力要求を送信するシステム）、ファイアウォールがポート 631 を介して接続を許可および作成できるようにする必要があります。

メインの **Printer Configuration Tool** ウィンドウで **New Printer** ボタンをクリックして、[図 33.2 「プリンターの追加」](#) にウィンドウを表示して、ネットワーク IPP プリンターを追加できます。プリンター名（printer 名にはスペースを含めることができません）、文字、数字、ダッシュ(-)、アンダースコア(\_)、説明（場所）を入力して、このプリンターをシステムで設定できる他の人と区別することができます。Forward をクリックして先に進みます。

[図33.4 「IPP プリンターの追加」](#) に表示されるウィンドウで、**Hostname** フィールドに IPP プリンターのホスト名と、**Prinтерname** フィールドにプリンターの一意名を入力します。

図33.4 IPP プリンターの追加



[D]

進む をクリックして続けます。

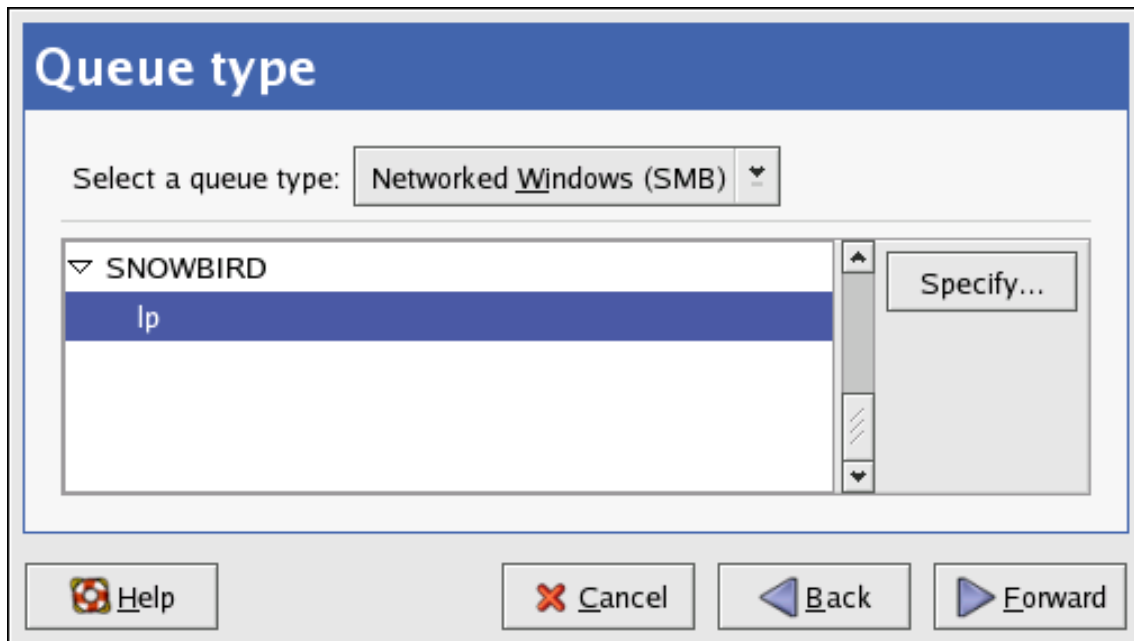
次に、プリンタータイプを選択します。詳細は、「[プリンターモデルの選択と完了](#)」を参照してください。

### 33.3. SAMBA(SMB)プリンターの追加


メインの **Printer Configuration Tool** ウィンドウで **New Printer** ボタンをクリックして、[図 33.2 「プリンターの追加」](#) にウィンドウを表示して、Samba(SMB)ベースのプリンター共有を追加できます。**Printer Name** フィールドにプリンターの一意の名前を入力します。プリンター名には、文字、数字、ダッシュ(-)、およびアンダースコア(\_)を使用できます。スペースを含めることはできません。

また、説明フィールドおよび **Location** フィールドを使用して、このプリンターと、システムに設定した可能性のある他のプリンターをさらに区別することもできます。これらのフィールドはいずれも任意で、スペースを含めることができます。

図33.5 SMB プリンターの追加



[D]

図33.5「SMB プリンターの追加」で示されているように、利用可能な SMB 共有は自動的に検出され、Share 列に表示されます。Workgroup の横にある矢印( )をクリックして展開します。拡張されたリストからプリンターを選択します。

検索するプリンターが一覧に表示されない場合は、`smb://` フィールドに SMB アドレスを入力します。`computer name/printer share` の形式を使用します。図33.5「SMB プリンターの追加」では、プリンター共有は `r2` で、コンピューター名は `dellbox` になります。

ユーザー名フィールドには、プリンターにアクセスするユーザー名を入力します。このユーザーは、SMB システムで存在している必要があり、ユーザーはプリンターへのアクセス権を持っている必要があります。デフォルトのユーザー名は通常、Windows サーバーでは `guest`、または Samba サーバーの場合は `nobody` です。

ユーザー名フィールドに指定したユーザーのパスワード（必要な場合）を入力します。

確認をクリックすると、接続をテストできます。確認が成功すると、ダイアログボックスが表示され、プリンター共有のアクセスを確認します。

次に、プリンタータイプを選択します。詳細は、「プリンターモデルの選択と完了」を参照してください。

**WARNING**

Samba プリンターのユーザー名およびパスワードは、root および lpd が読み取り可能な暗号化されていないファイルとしてプリンターサーバーに保存されます。そのため、プリンターサーバーに root アクセスを持つ他のユーザーは、Samba プリンターへのアクセスに使用するユーザー名とパスワードを表示できません。

そのため、Samba プリンターにアクセスするためのユーザー名とパスワードを選択する場合は、ローカルの Red Hat Enterprise Linux システムへのアクセスに使用するパスワードとは異なるパスワードを選択することが推奨されます。

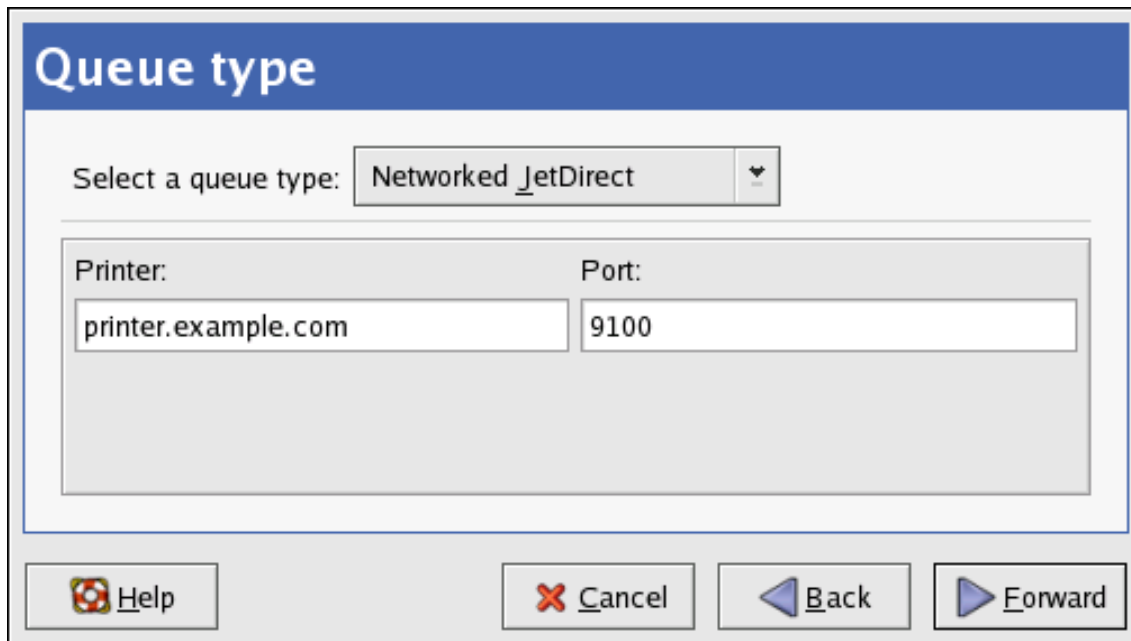
Samba プリンターサーバーで共有するファイルがある場合も、印刷キューで使用されるパスワードとは異なるパスワードを使用することが推奨されます。

### 33.4. JETDIRECT プリンターの追加

JetDirect または AppSocket の接続プリンター共有を追加するには、メインの **Printer Configuration Tool** ウィンドウで **New Printer** ボタンをクリックして、[図33.2 「プリンターの追加」](#) でウィンドウを表示します。Printer Name フィールドにプリンターの一意の名前を入力します。プリンター名には、文字、数字、ダッシュ(-)、およびアンダースコア(\_)を使用できます。スペースを含めることはできません。

また、説明フィールドおよび Location フィールドを使用して、このプリンターと、システムに設定した可能性のある他のプリンターをさらに区別することもできます。これらのフィールドはいずれも任意で、スペースを含めることができます。

図33.6 JetDirect プリンターの追加



[D]

進む をクリックして続けます。

以下のオプションのテキストフィールドが表示されます。

- **hostname** - JetDirect プリンターのホスト名または IP アドレス。
- **ポート 番号** - 印刷ジョブをリッスンする JetDirect プリンターのポートデフォルトのポートは 9100 です。

次に、プリンタータイプを選択します。詳細は、「[プリンターモデルの選択と完了](#)」を参照してください。

### 33.5. プリンターモデルの選択と完了

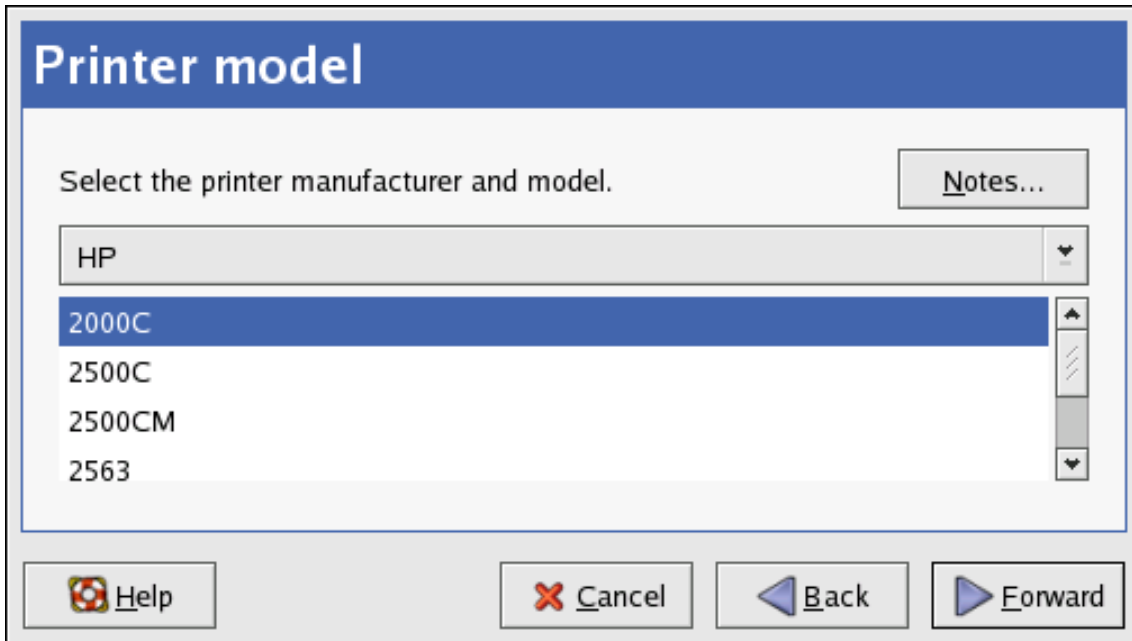
プリンターキュータイプを適切に選択したら、以下のいずれかのオプションを選択できます。

- **データベースからプリンターを選択** - このオプションを選択すると、製造元の一覧からプリンターの製造元を選択します。ご使用のプリンターの製造が一覧にない場合は、**Generic** を選択します。

- **PPD ファイルの提供**： PPD(PPD)ファイルはプリンターでも指定できます。このファイルは、通常製造元によって提供されます。 PPD ファイルで提供される場合は、このオプションを選択し、オプションの詳細の下にあるブラウザーを使用して PPD ファイルを選択できます。

図33.7「プリンターモデルの選択」を参照してください。

図33.7 プリンターモデルの選択



[D]

オプションの選択後に **Forward** をクリックして続行します。図33.7「プリンターモデルの選択」が表示されます。プリンターの対応するモデルとドライバーを選択する必要があります。

推奨される印刷ドライバーは、選択したプリンターモデルに基づいて自動的に選択されます。ただし、別の利用可能なドライバーを選ぶことも可能です。ローカルプリンターはコンピューターに直接接続されているため、プリンターに送信されるデータを処理するにはプリンタードライバーが必要です。

デバイスの PPD ファイル（通常は製造元提供）がある場合は、**Provide PPD file** を選択して選択できます。その後、**Browse** をクリックして PPD ファイルのファイルシステムを参照できます。

### 33.5.1. プリンター設定の確認

最後の手順では、プリンター設定を確認します。設定が正しい場合は **Apply** をクリックし、印刷ジョブを追加します。戻る (**Back**) をクリックすると、プリンター設定を変更できます。

変更を適用した後、テストページを出力して設定が正しいことを確認します。詳細は、「[テストページの印刷](#)」を参照してください。

### 33.6. テストページの印刷

プリンターを設定したら、テストページを印刷して、プリンターが適切に機能していることを確認する必要があります。テストページを印刷するには、プリンターの一覧から試行するプリンターを選択し、プリンターの **Settings** タブから **テストページの印刷** をクリックします。

印刷ドライバーを変更したりドライバーオプションを変更する場合は、テストページを印刷して別の設定をテストする必要があります。

### 33.7. 既存プリンターの修正

既存のプリンターを削除するには、プリンターを選択し、ツールバーの **Delete** ボタンをクリックします。プリンター設定の削除を確認すると、プリンターの一覧からプリンターが削除されます。

デフォルトのプリンターを設定するには、プリンターの一覧からプリンターを選択し、設定タブの **Make Default Printer** ボタンをクリックします。

#### 33.7.1. 設定タブ

プリンターのドライバー設定を変更するには、プリンター リストで該当する名前をクリックして、設定タブをクリックします。

製造元やモデルなどのプリンター設定を変更し、プリンターのデフォルトやテストページの印刷、デバイスの場所(URI)の変更などが可能です。

図33.8 Settings タブ

The screenshot shows a window titled "Settings" with a sidebar on the left containing the following menu items: Settings (highlighted), Policies, Access Control, Printer Options, Job Options, and Ink/Toner Levels. The main content area is divided into two sections: "Settings" and "Tests and Maintenance".

**Settings**

Description: Generic PCL 5e LF Printer

Location: lab1

Device URI: socket://localhost:9100

Make and Model: Generic PCL 5e Printer -...

Printer State: Idle

**Tests and Maintenance**

At the bottom of the window are three buttons: , , and .

[D]

### 33.7.2. ポリシー タブ

印刷出力の設定を変更するには、**Policies** タブをクリックします。

たとえば、バナーページ（送信元プリンター、ジョブを開始したユーザー名、印刷中のドキュメントのセキュリティステータスなど）を説明するページを作成するには、**Starting Banner** ドロップまたは **Ending Banner** ドロップメニューをクリックし、印刷ジョブの性質に最適なオプションを選択します（トップシークレット、分類された機密など）。



図33.9 Policies タブ

**Settings**

**Policies**

Access Control

Printer Options

Job Options

Ink/Toner Levels

**State**

Enabled

Accepting jobs

Shared

*Not published*  
*See server settings*

**Policies**

Error Policy: Stop printer

Operation Policy: Default behavior

**Banner**

Starting Banner: Classified

Ending Banner: Classified

Apply Cancel OK

[D]

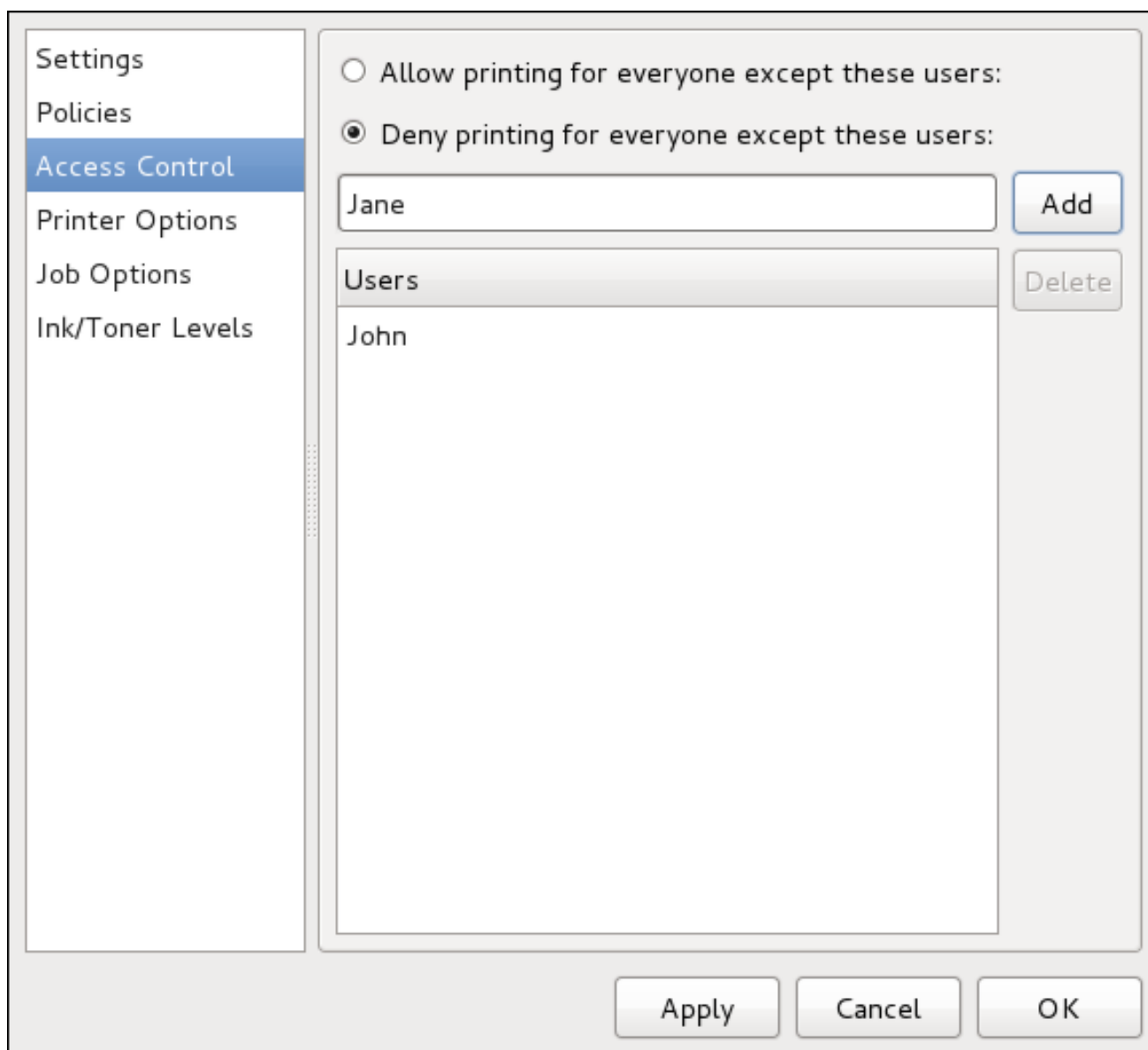
ドロップダウンメニューからオプションを選択して、プリンターのエラーポリシーを設定することもできます。印刷ジョブを中止、再試行、または停止することを選択できます。

### 33.7.3. アクセス制御 タブ

アクセス 制御 タブをクリックして、設定したプリンターへのユーザーレベルのアクセスを変更できます。

テキストボックスを使用してユーザーを追加し、その横の Add ボタンをクリックします。その後、そのユーザーのサブセットへのプリンターの使用のみを許可したり、それらのユーザーに使用を拒否するかを選択できます。

図33.10 アクセス制御タブ

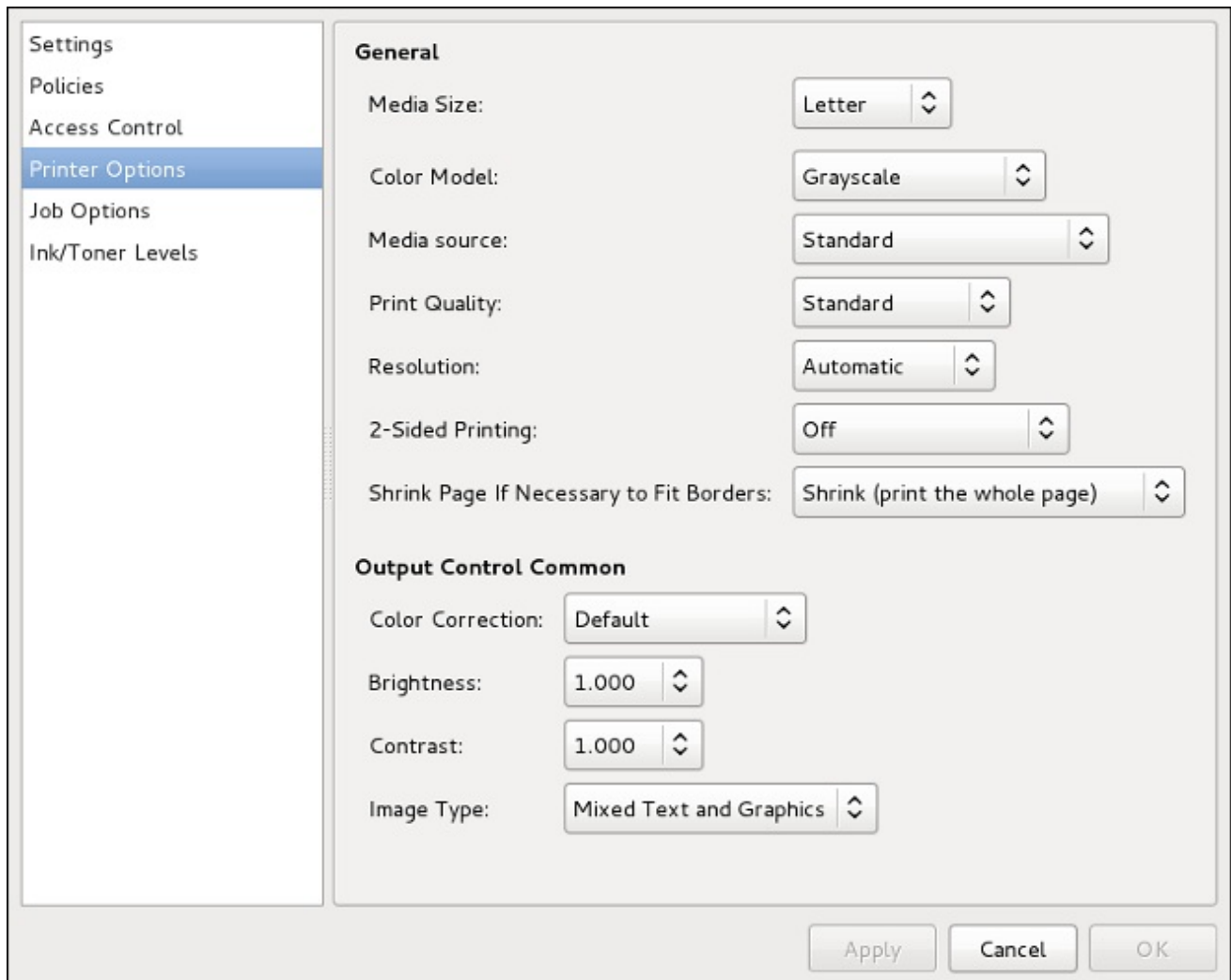


[D]

#### 33.7.4. プリンター および ジョブオプションタブ

プリンターオプションタブには、プリンターのメディアと出力のさまざまな設定オプションが含まれます。

図33.11 プリンターオプションタブ



[D]

- ページサイズ: ビデオサイズを選択できます。オプションには、US Letter、米国、A3、およびA4が含まれます。
- メディアソース: デフォルトで Automatic に設定されます。このオプションを変更して、別のトレイからのビデオを使用します。
- メディアタイプ: ビデオタイプを変更できます。オプションには Plain、thick、bond、および透過性があります。
- Resolution: printout の品質および詳細を設定します (デフォルトは、inch(dpi)ごとに 300 のドットです)。
- Toner saving - リソースを節約するためにプリンターが短いトナーを使用するかどうかを選択します。

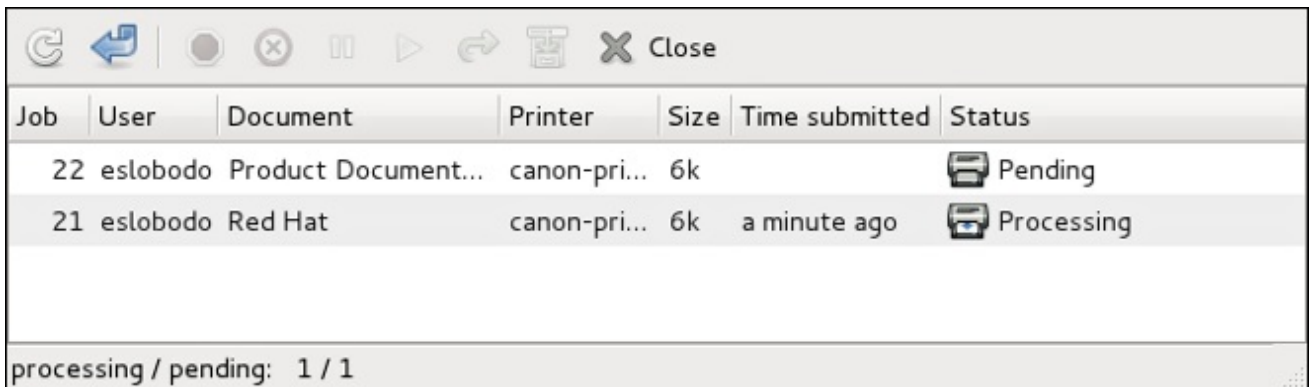
ジョブオプション タブを使用してプリンタージョブのオプションを設定することもできます。ドロップダウンメニューを使用して、Landscape モード (horizontal または vertical printout)、コピー、スケーリング (印刷可能領域のサイズを拡大または縮小) など、使用するジョブオプションを選択します。

### 33.8. 印刷ジョブの管理

Emacs からのテキストファイルの印刷、GIMP からの画像の印刷など、プリンターデーモンに印刷ジョブを送信すると、印刷ジョブは印刷スプールキューに追加されます。印刷スプールキューはプリンターに送信された印刷ジョブの一覧であり、リクエストの状態、ジョブ番号など、各印刷要求に関する情報です。

印刷プロセス中に、Printer Status アイコンがパネルの Notification Area に表示されます。印刷ジョブのステータスを確認するには、[図33.12 「GNOME 印刷の状態」](#) のようなウィンドウを表示する Printer Status をダブルクリックします。

図33.12 GNOME 印刷の状態



Job	User	Document	Printer	Size	Time submitted	Status
22	eslobodo	Product Document...	canon-pri...	6k		Pending
21	eslobodo	Red Hat	canon-pri...	6k	a minute ago	Processing

processing / pending: 1 / 1

[D]

GNOME Print Status に記載されている特定の印刷ジョブをキャンセルするには、一覧から選択し、プルダウンメニューから Edit => Cancel Documents を選択します。

シェルプロンプトから印刷スプールの印刷ジョブの一覧を表示するには、lpq コマンドを入力します。最後の数行は以下のようになります。

#### 例33.1 lpq 出力例

```
Rank Owner/ID          Class Job Files   Size Time
active user@localhost+902 A    902 sample.txt 2050 01:20:46
```

印刷ジョブをキャンセルするには、`lpq` コマンドで要求のジョブ番号を見つけ、`lprm job number` コマンドを使用します。たとえば、`lprm 902` は [例33.1 「lpq 出力例」](#) で印刷ジョブをキャンセルします。印刷ジョブをキャンセルするには、適切なパーミッションが必要です。プリンターが接続しているマシンに `root` としてログインしていない限り、他のユーザーが開始された印刷ジョブはキャンセルできません。

シェルプロンプトから直接ファイルを印刷することもできます。たとえば、`lpr sample.txt` コマンドはテキストファイル `sample.txt` を出力します。印刷フィルターはファイルのタイプを決定し、プリンターが理解できる形式に変換します。

### 33.9. 関連情報

`Red Hat Enterprise Linux` での印刷の詳細は、以下の資料を参照してください。

#### 33.9.1. インストールされているドキュメント

- `man lpr`: コマンドラインからのファイルの印刷を可能にする `lpr` コマンドの `man` ページです。
- `man lprm`: 印刷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ーの `man` ページです。
- `man mpage`: 1 枚の用紙に複数ページを印刷するためのコマンドラインユーティリティーの `man` ページです。
- `man cupsd`: `CUPS` プリンターデーモンの `man` ページです。
- `man cupsd.conf`: `CUPS` プリンターデーモンの設定ファイルの `man` ページです。
- `man classes.conf`: `CUPS` のクラス設定ファイルの `man` ページです。

#### 33.9.2. 便利な Web サイト

- <http://www.linuxprinting.org>: 『GNU/Linux 印刷には、』 `Linux` での印刷に関する多くの情報が含まれています。

- <http://www.cups.org/>: CUPS に関するドキュメント、FAQ、および newsgroups。

## 第34章 自動タスク

Linux では、タスクは、指定期間、指定された日付、またはシステムの負荷平均が指定された数を下回る場合に、自動的に実行するように設定できます。Red Hat Enterprise Linux は、システムの更新を維持するために重要なシステムタスクを実行するように事前設定されています。たとえば、locate コマンドで使用される slocate データベースが毎日更新されます。システム管理者は、自動化されたタスクを使用して定期的なバックアップの実行、システムの監視、カスタムスクリプトの実行などを実行できます。

Red Hat Enterprise Linux には、cron、at、batch などの自動タスクユーティリティーが複数含まれています。

### 34.1. CRON

Cron は、時間、月、曜日の組み合わせ、タスクの繰り返し実行をスケジュールするために使用できるデーモンです。

crons は、システムが継続的にあることを前提としています。タスクがスケジュールされている時にシステムがオンになっていない場合は、実行されません。1 回限りのタスクをスケジュールするには、[「at および Batch」](#) を参照してください。

cron サービスを使用するには、vixie-cron RPM パッケージがインストールされ、crond サービスが実行している必要があります。パッケージがインストールされているかどうかを確認するには、rpm -q vixie-cron コマンドを使用します。サービスが実行中かどうかを確認するには、/sbin/service crond status コマンドを使用します。

#### 34.1.1. cron タスクの設定

cron(/etc/crontab)の主な設定ファイルには、以下の行が含まれます。

```
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 タスクが実行される環境を設定するために使用される変数です。SHELL 変数

は、使用するシェル環境（この例では `bash` シェル）をシステムに指示しますが、`PATH` 変数はコマンドの実行に使用されるパスを定義します。`cron` タスクの出力は、`MAILTO` 変数で定義したユーザー名にメールで送信されます。`MAILTO` 変数が空の文字列（`MAILTO=""`として定義されている場合）の場合、メールは送信されません。`HOME` 変数を使用すると、コマンドまたはスクリプトの実行時に使用するホームディレクトリーを設定できます。

`/etc/crontab` ファイルの各行はタスクを表し、以下の形式となっています。

`minute hour day month dayofweek command`

- `minute`: 0 から 59 までの任意の整数
- `hour`: 0 から 23 までの任意の整数
- `day`: 1 から 31 までの整数（月を指定する場合は有効な日付である必要があります）
- `month`: 1 から 12 までの任意の整数（または `jan` や `feb` などの月の省略名）
- `dayOfWeek`: 0 から 7 までの任意の整数。0 または 7 は日曜日を表します（または `sun` または `mon` などの曜日の短縮名）。
- `command` - 実行するコマンド（コマンドは `ls /proc >> /tmp/proc` などのコマンドか、またはカスタムスクリプトを実行するコマンドになります）。

上記のいずれの値でも、アスタリスク(\*)を使用して有効な値をすべて指定できます。たとえば、`month` 値のアスタリスクは、他の値の制約内で毎回コマンドを実行します。

整数間のハイフン(-)は整数の範囲を指定します。たとえば、`1-4` は整数の 1、2、3、および 4 を意味します。

コンマで区切られた値の一覧(,)はリストを指定します。たとえば、`3,4,6,8` は 4 つの特定の整数を示します。

スラッシュ(/)を使用して `step` の値を指定できます。整数の値は、`<integer>` の範囲に従って範囲内



をスキップできます。たとえば、`0-59/2` を使用すると、1分ごとの分を1分単位で定義できます。ステップ値はアスタリスクでも使用することができます。たとえば、`*/3` の値を月フィールドで使用することで、3カ月ごとにタスクを実行できます。

ハッシュマーク(#)で始まる行はすべてコメントで、処理されません。

`/etc/crontab` ファイルにあるように、`run-parts` スクリプトは、`/etc/cron.hourly/`、`/etc/cron.daily/`、`/etc/cron.weekly/`、および `/etc/cron.monthly/` ディレクトリーのスクリプトを実行します。これらのディレクトリーの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 `hourly`、`daily`、`weekly`、または `monthly` 以外のスケジュールで実行する必要がある場合は、`/etc/cron.d/` ディレクトリーに追加できます。このディレクトリー内のすべてのファイルは、`/etc/crontab` と同じ構文を使用します。例については、[例34.1 「crontab の例」](#) を参照してください。

#### 例34.1 crontab の例

```
# 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
```

`root` 以外のユーザーは、`crontab` ユーティリティーを使用して `cron` タスクを設定できます。ユーザー定義の `crontabs` は `/var/spool/cron/` ディレクトリーに保存され、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、そのユーザーにログインし、`crontab -e` コマンドを入力して、`VISUAL` または `EDITOR` 環境変数が指定したエディターを使用してユーザーの `crontab` を編集します。このファイルは、`/etc/crontab` と同じ形式を使用します。`crontab` へ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、`/var/spool/cron/` ユーザー名に書き込まれます。

`cron` デーモンは、`/etc/crontab` ファイル、`/etc/cron.d/` ディレクトリー、および `/var/spool/cron/` ディレクトリーごとに変更の有無を確認します。変更が見つかった場合は、メモリーに読み込まれます。そのため、`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。

#### 34.1.2. cron へのアクセスの制御

`cron` へのアクセスを制限するには、`/etc/cron.allow` ファイルおよび `/etc/cron.deny` ファイルが使用されます。両方のアクセス制御ファイルの形式は、1行に1つのユーザー名です。いずれのファイルでも空白は許可されません。アクセス制御ファイルを変更した場合、`cron` デーモン(`crond`)を再起動す

る必要はありません。アクセス制御ファイルは、ユーザーが cron タスクの追加または削除を試みるたびに読み込まれます。

root ユーザーは、アクセス制御ファイルに記載されているユーザー名に関係なく、常に cron を使用できます。

cron.allow ファイルが存在する場合は、それに一覧表示されているユーザーのみが cron を使用でき、cron.deny ファイルは無視されます。

cron.allow が存在しない場合は、cron.deny に一覧表示されているユーザーは cron を使用することができません。

### 34.1.3. 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` の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。システムの起動時にサービスを開始することが推奨されます。起動時に cron サービスを自動的に起動する方法は、[19章](#) を参照してください。

## 34.2. AT および BATCH

cron は繰り返しの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 1 回限りのタスクを特定の時間にスケジュールするために使用されます。batch コマンドは、システムが 0.8 未満のシステムの平均ドロップ時に 1 回限りのタスクが実行されるようスケジュールするために使用されます。

at または batch を使用するには、at RPM パッケージがインストールされ、atd サービスが実行している必要があります。パッケージがインストールされているかどうかを確認するには、`rpm -q` コマンドを使用します。サービスが実行中かどうかを確認するには、`/sbin/service atd status` コマンドを使用します。

### 34.2.1. at ジョブの設定

特定の時間に 1 回限りのジョブをスケジュールするには、一度にコマンドを入力してください。time はコマンドを実行する時間になります。

引数の時間 は以下のいずれかになります。

- 

HH:MM 形式 - たとえば、04:00 は 4:00 を指定します。時間がすでに過去の場合は、その

時刻が次の日に指定のタイミングで実行されます。

- `midnight: 12:00 a.m` を指定します。
- `noon - 12:00 p.m` を指定します。
- `teatime - 4:00 p.m` を指定します。
- 月 1 日の年号の形式：たとえば、2002 年 1 月 15 日に 2002 年 1 月 15 日と指定していません。年はオプションです。
- `MMDDYY`、`MM/DD/YY`、または `MM.DD.YY` 形式。たとえば、2002 年 1 月 15 日の場合は `011502` です。
- `now + time - 時間` は分、時間、日、または週です。たとえば、現在は `+ 5 days` はコマンドを同時に 5 日に実行するように指定しています。

最初に時間を指定し、その後にオプションの日付を指定する必要があります。時間形式の詳細は、`/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 `time` 引数を入力すると、`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` を押し、`Ctrl+D` と入力します。各コマンドの後に `Enter` キーを押し、複数のコマンドを指定できます。すべてのコマンドを入力したら、`Enter` を押し、空白行に移動し、`Ctrl+D` と入力します。または、プロンプトでシェルスクリプトを入力し、スクリプトの各行の後に `Enter` を押し、空白行に `Ctrl+D` を入力して終了します。スクリプトを入力すると、使用するシェルは、ユーザーの `SHELL` 環境、ユーザーのログインシェル、または `/bin/sh`（最初に見つかったもの）に設定されるシェルになります。

コマンドまたはスクリプトセットが標準出力に情報を表示しようとする場合、出力はユーザーに電子メールで送信されます。

`atq` コマンドを使用して、保留中のジョブを表示します。詳細は、「[保留中のジョブの表示](#)」を参照してください。

`at` コマンドの使用は制限できます。詳細は、「[at と batch へのアクセスの制御](#)」を参照してくだ

さい。

### 34.2.2. batch ジョブの設定

負荷平均が 0.8 未満のときに 1 回限りのタスクを実行するには、`batch` コマンドを使用します。

`batch` コマンドを入力すると、`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` を押して、`Ctrl+D` と入力します。各コマンドの後に `Enter` キーを押し、複数のコマンドを指定できます。すべてのコマンドを入力したら、`Enter` を押して空白行に移動し、`Ctrl+D` と入力します。または、プロンプトでシェルスクリプトを入力し、スクリプトの各行の後に `Enter` を押して、空白行に `Ctrl+D` を入力して終了します。スクリプトを入力すると、使用するシェルは、ユーザーの `SHELL` 環境、ユーザーのログインシェル、または `/bin/sh`（最初に見つかったもの）に設定されるシェルになります。負荷平均が 0.8 未満になると、コマンドまたはスクリプトのセットが実行されます。

コマンドまたはスクリプトセットが標準出力に情報を表示しようとする場合、出力はユーザーに電子メールで送信されます。

`atq` コマンドを使用して、保留中のジョブを表示します。詳細は、[「保留中のジョブの表示」](#) を参照してください。

`batch` コマンドの使用は制限できます。詳細は、[「at と batch へのアクセスの制御」](#) を参照してください。

### 34.2.3. 保留中のジョブの表示

保留中の `at` および `batch` ジョブを表示するには、`atq` コマンドを使用します。`atq` コマンドは、保留中のジョブ一覧と、各ジョブが行に表示されます。各行は、ジョブ番号、日付、時間、ジョブクラス、ユーザー名形式に従います。ユーザーは独自のジョブのみを表示できます。`root` ユーザーが `atq` コマンドを実行すると、全ユーザーのジョブがすべて表示されます。

### 34.2.4. 追加のコマンドラインオプション

`at` および `batch` の追加コマンドラインオプションには以下が含まれます。

表34.1 `at` および `batch` のコマンドラインオプション

オプション	Description
-------	-------------

オプション	Description
-f	プロンプトで指定する代わりに、ファイルからコマンドまたはシェルスクリプトを読み取ります。
-m	ジョブが完了したらユーザーにメールを送信します。
-v	ジョブが実行される時間を表示します。

#### 34.2.5. at と batch へのアクセスの制御

`/etc/at.allow` ファイルおよび `/etc/at.deny` ファイルを使用して、`at` コマンドおよび `batch` コマンドへのアクセスを制限できます。両方のアクセス制御ファイルの形式は、1行に1つのユーザー名です。いずれのファイルでも空白は許可されません。アクセス制御ファイルを変更した場合でも、`at` デーモン (`atd`) を再起動する必要はありません。アクセス制御ファイルは、ユーザーが `at` または `batch` のコマンドの実行を試みるたびに読み込まれます。

`root` ユーザーは、アクセス制御ファイルに関係なく、常に `at` コマンドと `batch` コマンドを実行できます。

`at.allow` ファイルが存在する場合は、リストされているユーザーのみが `at` または `batch` を使用でき、`at.deny` ファイルは無視されます。

`at.allow` が存在しない場合は、`at.deny` に一覧表示されているユーザーは `at` または `batch` を使用できません。

#### 34.2.6. サービスの起動と停止

`at` サービスを起動するには、起動時に `/sbin/service` 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。システムの起動時にサービスを開始することが推奨されます。起動時に `cron` サービスを自動的に起動する方法は、[19章](#) を参照してください。

### 34.3. 関連情報

自動タスクの設定に関する詳細は、以下のリソースを参照してください。

#### 34.3.1. インストールされているドキュメント

- **cron の man ページ：cron の概要**
- **セクション 1 および 5 の crontab man ページ：セクション 1 の man ページには、crontab ファイルの概要が記載されています。セクション 5 の man ページには、ファイルの形式とエントリーの例が記載されています。**
- **/usr/share/doc/at- <version> /timespec には、cron ジョブに指定できる時間に関する詳細情報が含まれています。**
- **man ページ：at および batch の説明とそのコマンドラインオプション**

## 第35章 ログファイル

ログファイルは、システム（カーネル、サービス、および実行中のアプリケーションなど）に関するメッセージが含まれるファイルです。各情報にはそれぞれ異なるログファイルがあります。例えば、デフォルトのシステムログファイル、セキュリティメッセージ専用のログファイル、cron タスク用のログファイルなどです。

ログファイルは、カーネルドライバーのロードを試みるシステムや、システムへの不正ログインを探す場合など、システムの問題のトラブルシューティングを行う場合に非常に便利です。本章では、ログファイルの場所、ログファイルの閲覧方法、ログファイルの注意すべき項目を説明します。

一部のログファイルは、`syslogd` と呼ばれるデーモンによって制御されます。`syslogd` が維持するログメッセージの一覧は、`/etc/syslog.conf` 設定ファイルにあります。

### 35.1. ログファイルの場所の特定

ほとんどのログファイルは `/var/log/` ディレクトリーにあります。`httpd` や `samba` などの一部のアプリケーションでは、ログファイル用のディレクトリーが `/var/log/` 内にあります。

ログファイルディレクトリーの複数のファイルの後に番号が付いたファイルがあることに気付くかもしれません。これらはログファイルがローテーションされる際に作成されます。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ローテーションが行われます。`logrotate` パッケージには cron タスクが含まれており、`/etc/logrotate.conf` 設定ファイルと `/etc/logrotate.d/` ディレクトリー内の設定ファイルに従って自動的にログファイルをローテーションします。デフォルトでは、週ごとにローテーションするように設定され、以前のログファイルの 4 週間分のままにします。

### 35.2. 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 などのテキストエディターで表示できます。一部のログファイルは、システム上のすべてのユーザーが読み取り可能ですが、ほとんどのログファイルを読み取るには root 権限が必要になります。

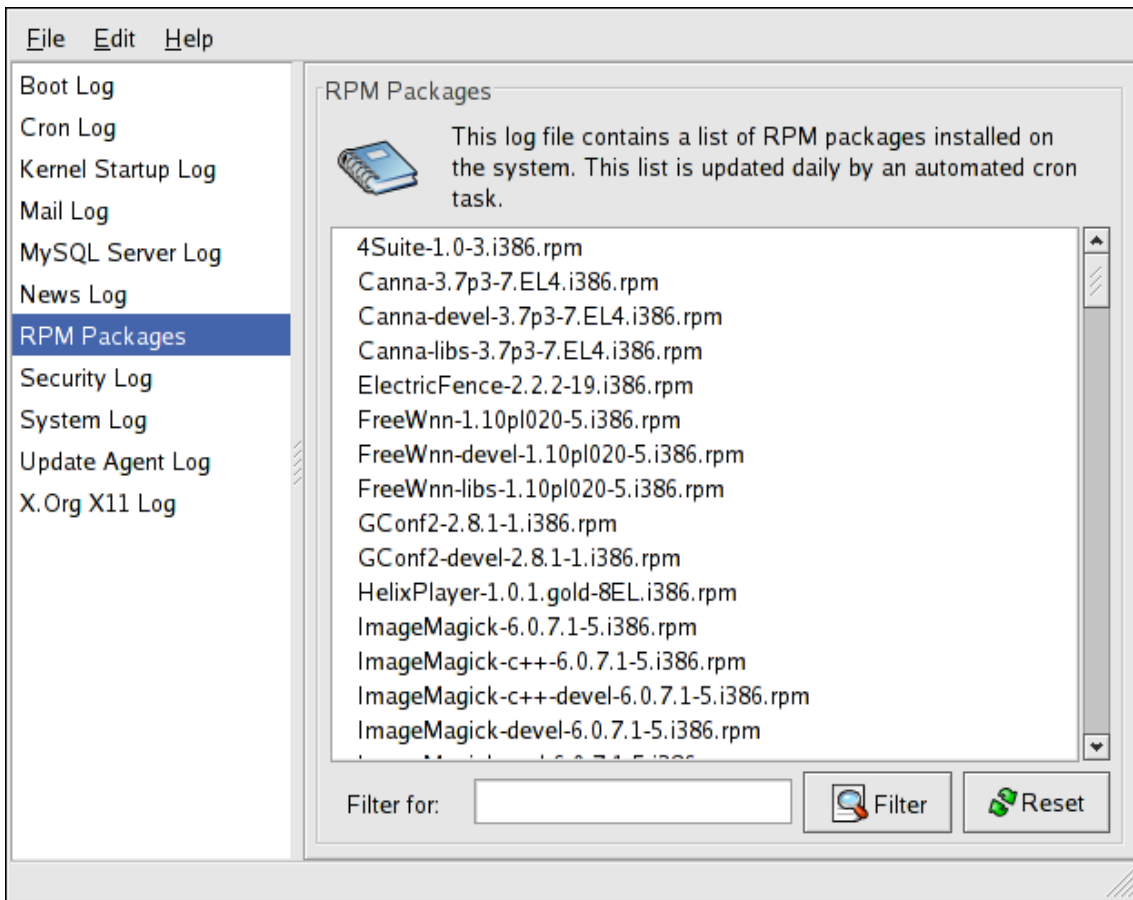
インタラクティブなリアルタイムアプリケーションでシステムのログファイルを表示するには、Log Viewer を使用します。アプリケーションを起動するには、Applications（パネルのメインメニュー） => System Tools => System Logs に移動するか、シェルプロンプトで `system-logviewer` コマンドを入力します。

アプリケーションは、存在するログファイルのみを表示します。そのため、[図35.1「ログビューアー」](#) に記載されている一覧とは異なる場合があります。



キーワードのログファイルの内容をフィルタリングするには、**Filter for text** フィールドにキーワードを入力し、**Filter** をクリックします。**Reset** をクリックして、コンテンツをリセットします。

図35.1 ログビューアー



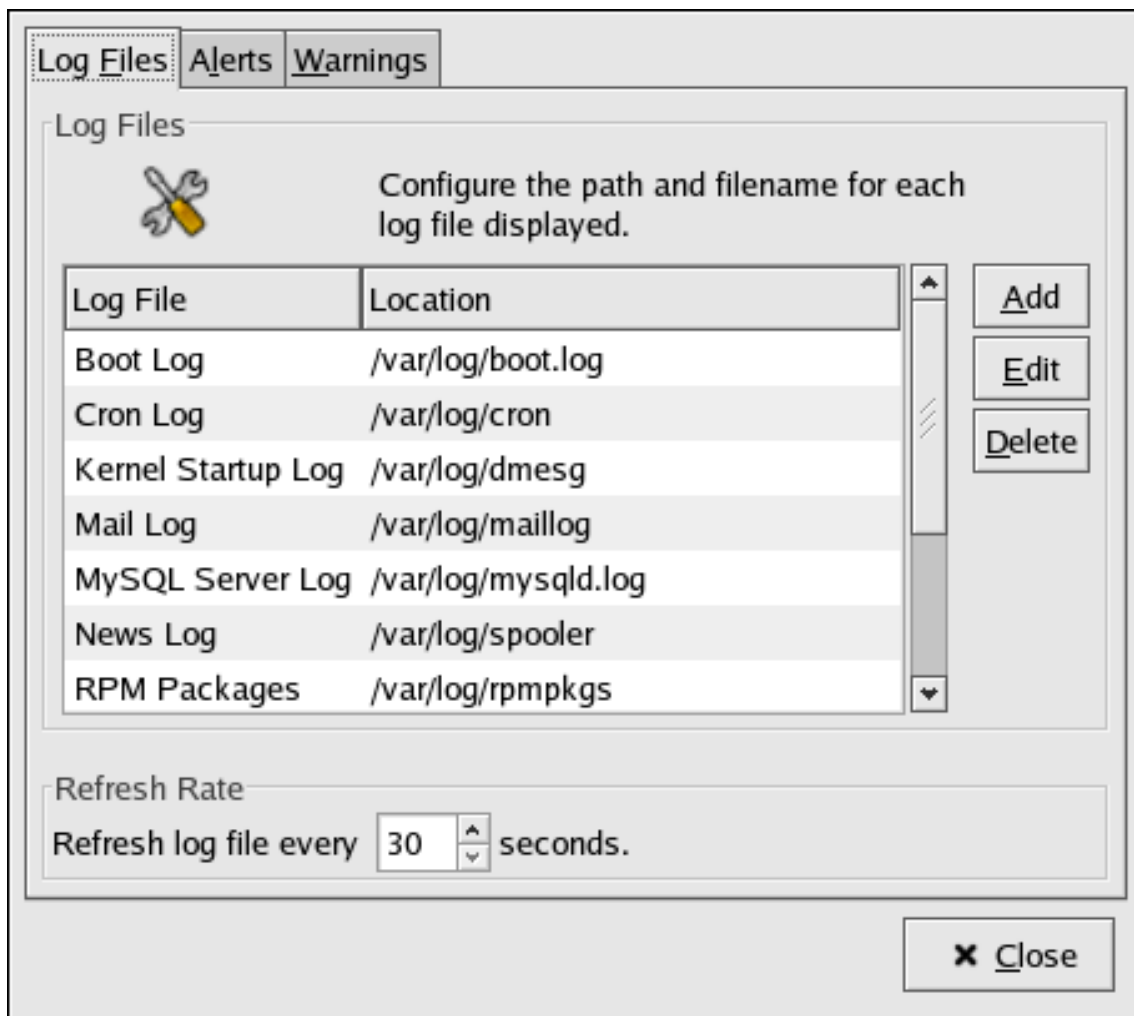
[D]

デフォルトでは、現在表示可能なログファイルは 30 秒ごとに更新されます。更新レートを変更するには、プルダウンメニューから **Edit => Preferences** を選択します。図35.2「ログファイルの場所」に表示されるウィンドウが表示されます。ログファイルタブで、更新レートの横にある上矢印および下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。更新レートはすぐに変更されます。現在表示可能なファイルを手動で更新するには、**File => Refresh Now** を選択するか、**Ctrl+R** を押します。

**Preferences** のログファイルタブで、ログファイルの場所を変更できます。一覧からログファイルを選択し、編集 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、参照 ボタンをクリックして、ファイル選択ダイアログを使用してファイルの場所を特定します。OK をクリックして設定に戻り、Close をクリックしてメインウィンドウに戻ります。



図35.2 ログファイルの場所

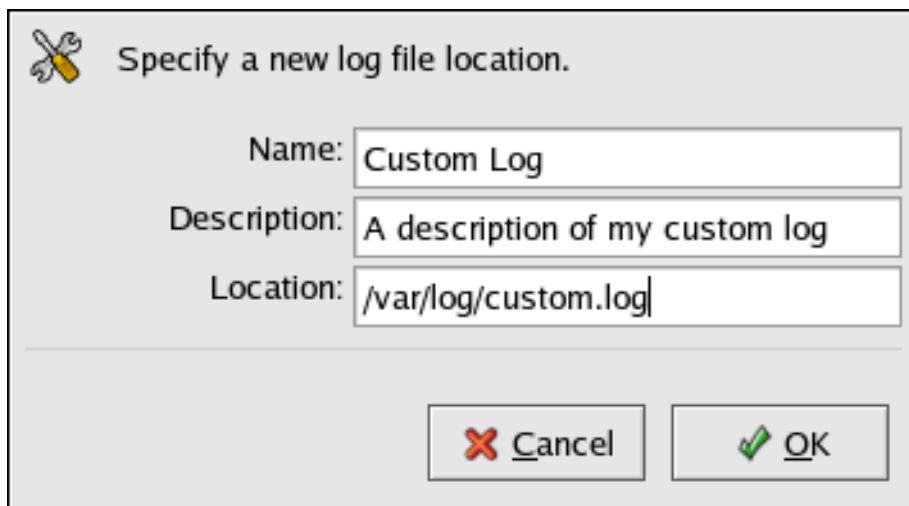


[D]

### 35.3. ログファイルの追加

ログファイルをリストに追加するには、*Edit => Preferences* の順に選択し、*Log Files* タブの *Add* ボタンをクリックします。

図35.3 ログファイルの追加



The image shows a dialog box with a wrench icon and the title "Specify a new log file location." It contains three text input fields: "Name:" with the value "Custom Log", "Description:" with the value "A description of my custom log", and "Location:" with the value "/var/log/custom.log". At the bottom, there are two buttons: "Cancel" with a red 'X' icon and "OK" with a green checkmark icon.

[D]

追加するログファイルの名前、説明、および場所を指定します。OK をクリックすると、ファイルが存在する場合は、表示領域にファイルがすぐに追加されます。

#### 35.4. ログファイルの検証

ログビューアーは、主要なアラート単語を含む行の横にあるアラートアイコンと、キーの警告単語を含む行の横にある警告アイコンを表示するように設定できます。

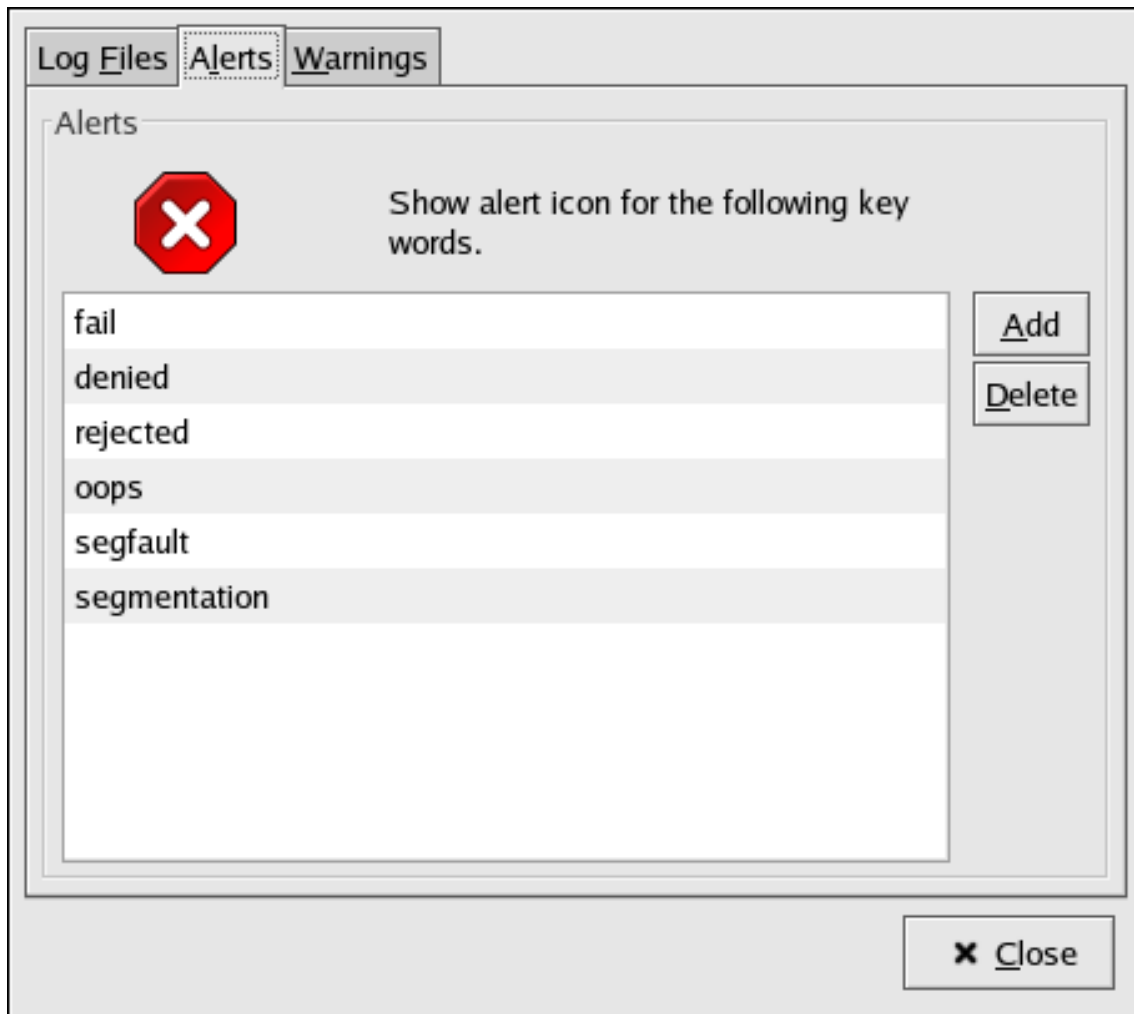
アラートの単語を追加するには、プルダウンメニューから **Edit => Preferences** を選択し、**Alerts** タブをクリックします。Add ボタンをクリックしてアラート単語を追加します。アラート単語を削除するには、一覧から単語を選択して **Delete** をクリックします。

##### アラートアイコン



は、アラート単語が含まれる行の左側に表示されます。

図35.4 アラート



[D]

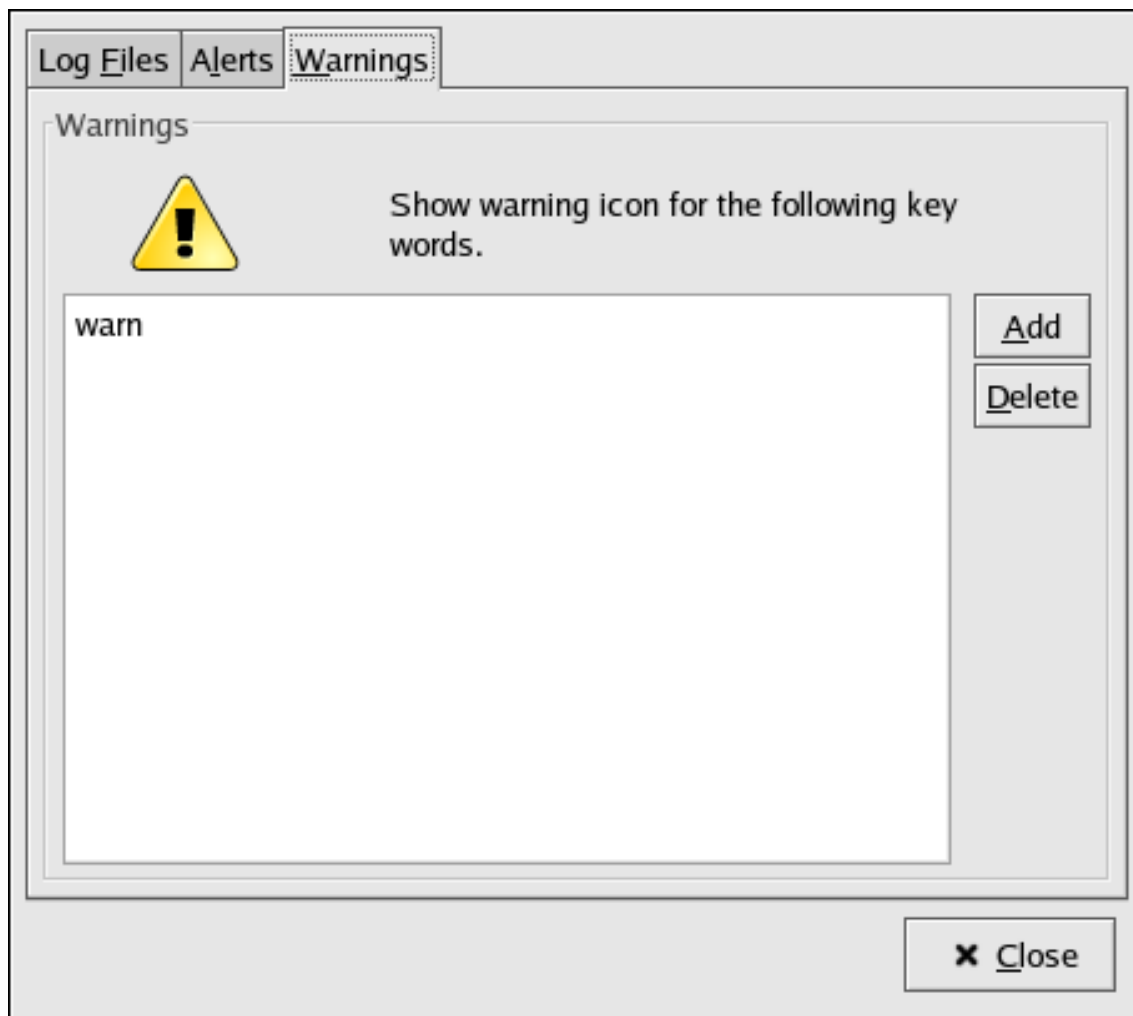
警告の単語を追加するには、プルダウンメニューから **Edit => Preferences** を選択し、**Warnings** タブをクリックします。Add ボタンをクリックして警告単語を追加します。警告単語を削除するには、一覧から単語を選択して **Delete** をクリックします。

#### 警告アイコン



は、警告単語が含まれる行の左側に表示されます。

図35.5 Warning

[\[D\]](#)

## 第36章 カーネルの手動によるアップグレード

Red Hat Enterprise Linux カーネルは、サポートしているハードウェアとの整合性と互換性を確保するために、Red Hat カーネルチームがカスタムを構築します。リリースする前に、カーネルは Red Hat が定める厳格な品質保証テストセットをパスしなければなりません。

Red Hat Enterprise Linux カーネルは RPM 形式でパッケージ化されるため、Red Hat User Agent または `up2date` コマンドを使用したアップグレードと検証が容易になります。Red Hat User Agent は Red Hat Network サーバーを自動的にクエリーし、カーネルを含むマシンで更新する必要のあるパッケージを決定します。本章では、`up2date` コマンドを使用せずに、カーネルパッケージを手動で更新する必要がある個人にのみ 役立ちます。



### WARNING

カスタムカーネルの構築は Red Hat グローバルサービスサポートチームではサポートされていないため、このマニュアルでは検討されていません。



### ヒント


Red Hat は、アップグレードしたカーネルをインストールする場合に、`up2date` の使用を強く 推奨します。

Red Hat Network、Red Hat User Agent、および `up2date` の詳細は、[16章 Red Hat Network](#) を参照してください。

### 36.1. カーネルパッケージの概要

Red Hat Enterprise Linux には、以下のカーネルパッケージが含まれています（アーキテクチャーに適用されないものもあります）。

- **kernel:** カーネルと、以下の主な機能が含まれます。
  - x86 および Athlon システムの Uniprocessor サポート（マルチプロセッサシステムで実行できますが、1つのプロセッサのみが使用される）

- その他のすべてのアーキテクチャーのマルチプロセッササポート
  - x86 システムの場合は、最初の 4 GB の RAM のみを使用され、RAM が 4 GB を超える x86 システムに `kernel-hugemem` パッケージを使用します。
  - `kernel-devel`: `kernel` パッケージに対してモジュールを構築するのに十分なカーネルヘッダーと `makefiles` が含まれます。
  - `kernel-hugemem`: (i686 システムのみ) カーネルパッケージに有効なオプションに加え、主な設定オプションは以下のとおりです。
    - 4 GB を超える RAM (x86 用最大 64 GB) のサポート
-  備考
- `kernel-hugemem` は、16 GB を超えるメモリー設定に必要です。
- PAE (物理アドレス拡張) または、PAE に対応する x86 プロセッサに 3 レベルのページング
  - 複数のプロセッサのサポート
  - 4GB/4GB の分割 - カーネル用の仮想アドレス空間および x86 システムのユーザープロセスごとに 4GB の仮想アドレス空間
  - `kernel-hugemem-devel`: `kernel-hugemem` パッケージに対してモジュールを構築するのに十分なカーネルヘッダーと `makefiles` が含まれます。
  - `kernel-smp`: マルチプロセッサシステムのカーネルが含まれます。主な特長を以下に示します。
    - マルチプロセッサのサポート

- 4 GB を超える RAM のサポート (x86 用最大 16 GB)
- PAE (物理アドレス拡張) または、PAE に対応する x86 プロセッサに 3 レベルのページング
- **kernel-smp-devel:** kernel-smp パッケージに対してモジュールを構築するのに十分なカーネルヘッダーと makefiles が含まれます。
- **kernel-utils:** カーネルまたはシステムハードウェアを制御するのに使用できるユーティリティが含まれます。
- **kernel-doc:** カーネルソースからのドキュメントファイルが含まれます。これらのファイルには、同梱で配布される Linux カーネルとデバイスドライバーのさまざまな部分が文書化されています。このパッケージをインストールすると、オプションへの参照が提供され、読み込み時に Linux カーネルモジュールに渡すことができます。

デフォルトでは、これらのファイルは `/usr/share/doc/kernel-doc- <version> /` ディレクトリに配置されます。

#### 備考

**kernel-source** パッケージが削除され、Red Hat Network からしか取得できない RPM に置き換えられています。\*.src.rpm は、rpmbuild コマンドを使用してローカルに再構築する必要があります。カーネルソースパッケージの取得およびインストールに関する詳細は、すべての更新を含む最新のディストリビューションリリースノート(<https://www.redhat.com/docs/manuals/enterprise/>)を参照してください。

## 36.2. 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、いくつかの予防的な手順を行います。最初のステップでは、問題が発生した場合にシステムに作業用メディアが存在することを確認します。ブートローダーが新しいカーネルを起動するように適切に設定されていない場合、起動用メディアを動作せずにシステムを Red Hat Enterprise Linux で起動できません。

たとえば、ブートディスクを作成し、root としてログインして、シェルプロンプトで以下のコマンドを入力します。

```
/sbin/mkbootdisk `uname -r`
```



## ヒント

その他のオプションについては、`man` ページの `mkbootdisk` を参照してください。CD-R、CD-RWs、および USB フラッシュドライブを介した起動可能なメディアの作成も、システム BIOS がサポートしていることが前提となります。

ブートメディアでマシンを再起動し、それが機能することを確認してから続行します。

理想的には、メディアは不要ですが、単にケースで安全な場所に保存してください。

どのカーネルパッケージがインストールされているかを確認するには、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
```

出力には、システムのアーキテクチャーに応じて以下のパッケージの一部またはすべてが含まれます (バージョン番号とパッケージが異なる場合があります)。

```
kernel-2.6.9-5.EL kernel-devel-2.6.9-5.EL kernel-utils-2.6.9-5.EL kernel-doc-2.6.9-5.EL kernel-smp-2.6.9-5.EL kernel-smp-devel-2.6.9-5.EL kernel-hugemem-devel-2.6.9-5.EL
```

この出力から、カーネルのアップグレード用にダウンロードする必要のあるパッケージを判断します。単一のプロセッサシステムの場合、必要なパッケージは `kernel` パッケージのみです。異なるパッケージの説明は、[「カーネルパッケージの概要」](#) を参照してください。

ファイル名で、各カーネルパッケージには、パッケージがビルドされたアーキテクチャーが含まれます。形式は `kernel- <variant> - <version> . <arch> .rpm` です。< variant > は `smp`、`utils` などです。< arch > は以下のいずれかです。

- **AMD64** アーキテクチャー : `x86_64`
- **Intel®Warehouse** アーキテクチャー : `ia64™`
- **IBM®eServer™pSeries™** アーキテクチャー : `ppc64`



- **IBM®eServer™iSeries™ アーキテクチャー : ppc64**
- **IBM®S® 390 アーキテクチャー : s390**
- **IBM®eServer™zSeries® アーキテクチャー : s390x**
- **x86 バリエーション : x86 カーネルは、異なる x86 バージョンに対して最適化されています。オプションは次のとおりです。**
  - **Intel Pentium II, Intel®Pentium® II, Intel®®Pentium®® 4, AMD Athlon®, および AMD Duron® システムの i686**

### 36.3. 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が利用可能かを判定する手段は数種類あります。

- **セキュリティエラー - セキュリティ問題を修正するカーネルのアップグレードなど、セキュリティエラーに関する情報は、以下の場所に移動します。**

<http://www.redhat.com/apps/support/errata/>

- **Quarterly Updates - 詳細は、以下の場所を参照してください。**

[http://www.redhat.com/apps/support/errata/rhlas\\_errata\\_policy.html](http://www.redhat.com/apps/support/errata/rhlas_errata_policy.html)

- **Red Hat Network 経由 : カーネル RPM パッケージをダウンロードしてインストールします。Red Hat Network は最新のカーネルをダウンロードし、システム上のカーネルをアップグレードし、必要に応じて初期 RAM ディスクイメージを作成し、ブートローダーを設定して新しいカーネルを起動できます。詳細は、<http://www.redhat.com/docs/manuals/RHNetwork/>を参照してください。**

更新されたカーネルのダウンロードとインストールに Red Hat Network を使用している場合は、「初期 RAM ディスクイメージの確認」および「ブートローダーの確認」の指示に従い、カーネルをデフォルトで起動するだけです。Red Hat Network は、デフォルトのカーネルを最新バージョンに変更します。カーネルを手動でインストールするには、「アップグレードの実行」に進みます。

## 36.4. アップグレードの実行

必要なパッケージをすべて取り込んだ後は、既存カーネルをアップグレードします。シェルプロンプトで、`root` でカーネル RPM パッケージが含まれるディレクトリーに切り替え、以下の手順を実行します。



### 重要な影響

新しいカーネルに問題がある場合は、古いカーネルを保持することが強く推奨されま  
す。

`rpm` コマンドに `-i` 引数を使用して古いカーネルを残します。`-U` オプションは、現在インストールされているカーネルを上書きして、ブートローダーの問題を作成するため、使用しないでください。以下のコマンドを実行します（カーネルバージョンは異なる場合があります）。

```
rpm -ivh kernel-2.6.9-5.EL.<arch>.rpm
```

システムがマルチプロセッサシステムである場合は、`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は異なる場合があります）。

```
rpm -ivh kernel-smp-2.6.9-5.EL.<arch>.rpm
```

システムが `i686-based` で、4 GB 以上の RAM が含まれている場合には、`i686` アーキテクチャー用  
に構築された `kernel-hugemem` パッケージをインストールします（カーネルバージョンは異なる場合  
があります）。

```
rpm -ivh kernel-hugemem-2.6.9-5.EL.i686.rpm
```

次の手順では、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。詳細は、[「初期 RAM ディスクイメージの確認」](#) を参照してください。

## 36.5. 初期 RAM ディスクイメージの確認

システムで `ext3` ファイルシステム、SCSI コントローラー、またはラベルを使用して `/etc/fstab` の  
パーティションを参照する場合は、初期 RAM ディスクが必要になります。初期 RAM ディスクによ  
り、モジュールカーネルが、モジュールが通常存在するデバイスにアクセスする前に起動する必要があ  
る場合があります。

IBM eServer iSeries 以外の Red Hat Enterprise Linux アーキテクチャーでは、`mkinitrd` コマンド

で初期 RAM ディスクを作成できます。ただし、カーネルとその関連パッケージが Red Hat, Inc に同梱される RPM パッケージからインストールまたはアップグレードされると、このステップは自動的に実行されるので、手動で実行する必要はありません。これ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- <version > .img` ファイルが作成されていることを確認します（バージョンはインストールされたカーネルのバージョンと一致する必要があります）。

iSeries システムでは、初期 RAM ディスクファイルと `vmlinux` ファイルが 1 つのファイルに統合され、このファイルは `addRamDisk` コマンドで作成されます。カーネルとその関連パッケージが Red Hat, Inc により配布される RPM パッケージからインストールまたはアップグレードされると、このステップは自動的に実行されるので、手動で実行する必要はありません。作成したことを確認するには、`ls -l /boot` コマンドを使用して、`/boot/vmlinitrd- <kernel-version >` ファイルが作成されていることを確認します（バージョンはインストールされたカーネルのバージョンと一致する必要があります）。

次の手順では、ブートローダーが新しいカーネルを起動するように設定されていることを確認します。詳細は、「[ブートローダーの確認](#)」を参照してください。

## 36.6. ブートローダーの確認

カーネル RPM パッケージは、新たにインストールしたカーネルを起動するようにブートローダーを設定します（IBM eServer iSeries システムを除く）。ただし、デフォルトで新しいカーネルを起動するようにブートローダーを設定しません。

ブートローダーが正しく設定されていることを確認するとよいでしょう。これは重要なステップです。ブートローダーが正しく設定されていない場合には、システムは Red Hat Enterprise Linux で適切に起動しません。この場合は、先に作成したブートメディアでシステムを起動し、ブートローダーを再び設定してみてください。

### 36.6.1. x86 システム

すべての x86 システムはブートローダーとして GRUB を使用します。これには、すべての AMD64 システムが含まれます。

#### 36.6.1.1. GRUB

`/boot/grub/grub.conf` ファイルに、インストールした kernel パッケージと同じバージョンの `title` セクションが含まれていることを確認します（`kernel-smp` または `kernel-hugemem` パッケージがインストールされている場合は、このセクションも存在します）。

```
# 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=1
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Enterprise Linux (2.6.9-5.EL)
    root (hd0,0)
    kernel /vmlinuz-2.6.9-5.EL ro root=LABEL=/
    initrd /initrd-2.6.9-5.EL.img
title Red Hat Enterprise Linux (2.6.9-1.906_EL)
    root (hd0,0)
    kernel /vmlinuz-2.6.9-1.906_EL ro root=LABEL=/
    initrd /initrd-2.6.9-1.906_EL.img
```

個別の `/boot/` パーティションが作成されると、カーネルと `initrd` イメージへのパスは `/boot/` との相対パスになります。

デフォルトでは新しいカーネルが設定されていないことに注意してください。デフォルトで新しいカーネルを起動するように `GRUB` を設定するには、新しいカーネルを含むタイトルセクションの `title` セクション番号にデフォルト変数の値を変更します。数は 0 で始まります。たとえば、新しいカーネルが最初の `title` セクションである場合は、`default` を 0 に設定します。

コンピューターを再起動して新しいカーネルのテストを開始し、メッセージを監視してハードウェアが適切に検出されるようにします。

### 36.6.2. pidgin Systems

`faillock` システムは、設定ファイルとして `/boot/efi/EFI/redhat/elilo.conf` を使用するブートローダーとして `ELILO` を使用します。このファイルには、インストールした `kernel` パッケージと同じバージョンの `image` セクションが含まれていることを確認します。

```
prompt
timeout=50
default=old

image=vmlinuz-2.6.9-5.EL
    label=linux
    initrd=initrd-2.6.9-5.EL.img
    read-only
    append="root=LABEL=/"
image=vmlinuz-2.6.9-1.906_EL
    label=old
    initrd=initrd-2.6.9-1.906.img
    read-only
    append="root=LABEL=/"
```

デフォルトでは新しいカーネルが設定されていないことに注意してください。ELILO が新規カーネルを起動するように設定するには、デフォルト 変数の値を新規カーネルが含まれる image セクションのラベルの値に変更します。

コンピューターを再起動して新しいカーネルのテストを開始し、メッセージを監視してハードウェアが適切に検出されるようにします。

### 36.6.3. IBM S/390 および IBM eServer zSeries Systems

IBM S/390 および IBM eServer zSeries システムは z/IPL をブートローダーとして使用します。このブートローダーは /etc/zipl.conf を設定ファイルとして使用します。ファイルに、インストールした kernel パッケージと同じバージョンのセクションが含まれていることを確認します。

```
[defaultboot]
default=old
target=/boot/
[[linux]
  image=/boot/vmlinuz-2.6.9-5.EL
  ramdisk=/boot/initrd-2.6.9-5.EL.img
  parameters="root=LABEL=/"
[old]
  image=/boot/vmlinuz-2.6.9-1.906_EL
  ramdisk=/boot/initrd-2.6.9-1.906_EL.img
  parameters="root=LABEL=/"
```

デフォルトでは新しいカーネルが設定されていないことに注意してください。z/IPL を、デフォルトで新しいカーネルを起動するように設定するには、デフォルト 変数の値を新しいカーネルを含むセクションの名前に変更します。各セクションの最初の行には括弧内に名前が含まれています。

設定ファイルを変更したら、root で以下のコマンドを実行して、変更を有効にします。

```
/sbin/zipl
```

コンピューターを再起動して新しいカーネルのテストを開始し、メッセージを監視してハードウェアが適切に検出されるようにします。

### 36.6.4. IBM eServer iSeries Systems

/boot/vmlinitrd- <kernel-version> ファイルは、カーネルのアップグレード時にインストールされます。ただし、dd コマンドを使用して、新しいカーネルを起動するように設定する必要があります。

1. `root` として、`cat /proc/iSeries/mf/side` コマンドを実行してデフォルトのサイドを確認します (A、B、または C のいずれか)。
2. `root` で、以下のコマンドを実行します。ここで、`< kernel-version >` は新しいカーネルのバージョンで、`< side >` は直前のコマンド側になります。

```
dd if=/boot/vmlinitrd-<kernel-version> of=/proc/iSeries/mf/<side>/vmlinux bs=8k
```

コンピューターを再起動して新しいカーネルのテストを開始し、メッセージを監視してハードウェアが適切に検出されるようにします。

### 36.6.5. IBM eServer pSeries Systems

IBM eServer pSeries システムは、設定ファイルとして `/etc/aboot.conf` を使用するブートローダーとして YABOOT を使用します。ファイルに、インストールした kernel パッケージと同じバージョンの `image` セクションが含まれていることを確認します。

```
boot=/dev/sda1
init-message=Welcome to Red Hat Enterprise Linux!
Hit <TAB> for boot options

partition=2
timeout=30
install=/usr/lib/yaboot/yaboot
delay=10
nonvram

image=/vmlinux--2.6.9-5.EL
    label=old
    read-only
    initrd=/initrd--2.6.9-5.EL.img
    append="root=LABEL=/"

image=/vmlinux-2.6.9-5.EL
    label=linux
    read-only
    initrd=/initrd-2.6.9-5.EL.img
    append="root=LABEL=/"
```

デフォルトでは新しいカーネルが設定されていないことに注意してください。最初のイメージ内のカーネルは、デフォルトで起動します。デフォルトのカーネルを変更して、そのイメージスタンプが一覧表示された最初のものになるように変更するか、ディレクティブのデフォルトを追加して、新しいカーネルを含むイメージスタンプのラベルに設定します。

コンピューターを再起動して新しいカーネルのテストを開始し、メッセージを監視してハードウェアが適切に検出されるようにします。

## 第37章 カーネルモジュール

Linux カーネルにはモジュール設計があります。システムの起動時に、最小の常駐カーネルのみがメモリーに読み込まれます。その後、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、ドライバーと呼ばれるカーネルモジュールは動的にメモリーに読み込まれます。

インストール時に、システムのハードウェアがプローブされます。このプローブとユーザーが提供する情報に基づいて、インストールプログラムは起動時に読み込む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、透過的に動作する動的ロードメカニズムを設定します。

インストール後に新しいハードウェアを追加し、ハードウェアにカーネルモジュールが必要な場合は、新しいハードウェア用に適切なカーネルモジュールを読み込むようにシステムを設定する必要があります。システムが新しいハードウェアで起動すると、Kudu プログラムは実行され、サポートされている場合は新しいハードウェアを検出し、そのハードウェアに対するモジュールを設定します。モジュールは、モジュール設定ファイル `/etc/modprobe.conf` を編集して手動で指定することもできます。



### 備考

X Window System インターフェースの表示に使用されるビデオカードモジュールは、カーネルではなく `xorg-X11` パッケージの一部であるため、本章は適用されません。

たとえば、システムに SMC EtherPower 10 PCI ネットワークアダプターが含まれている場合、モジュール設定ファイルには以下の行が含まれます。

```
alias eth0 tulip
```

2 つ目のネットワークカードがシステムに追加され、1 番目のカードと同じ場合は、以下の行を `/etc/modprobe.conf` に追加します。

```
alias eth1 tulip
```

カーネルモジュールのアルファベット順と、これらのモジュールでサポートされるハードウェアの一覧は、『『リファレンスガイド』』を参照してください。

### 37.1. カーネルモジュールユーティリティー

`module-init-tools` パッケージがインストールされている場合は、カーネルモジュールを管理するた



めのコマンドのグループを利用できます。これらのコマンドを使用して、モジュールが正常に読み込まれているかどうか、または新しいハードウェアの一部で異なるモジュールを試行するかどうかを決定します。

`/sbin/lsmmod` コマンドは、現在読み込まれているモジュールの一覧を表示します。以下に例を示します。

```

Module          Size Used by
nfs              218437 1
lockd            63977 2 nfs
parport_pc      24705 1
lp              12077 0
parport          37129 2 parport_pc,lp
autofs4         23237 2
i2c_dev         11329 0
i2c_core        22081 1 i2c_dev
sunrpc          157093 5 nfs,lockd
button          6481 0
battery         8901 0
ac              4805 0
md5             4033 1
ipv6            232833 16
ohci_hcd        21713 0
e100            39493 0
mii             4673 1 e100
floppy          58481 0
sg              33377 0
dm_snapshot     17029 0
dm_zero         2369 0
dm_mirror       22957 2
ext3            116809 2
jbd             71257 1 ext3
dm_mod          54741 6 dm_snapshot,dm_zero,dm_mirror
ips            46173 2
aic7xxx        148121 0
sd_mod         17217 3
scsi_mod        121421 4 sg,ips,aic7xxx,sd_mod

```

行ごとに 1 列目がモジュールの名前、2 列目はモジュールのサイズ、3 列目は使用カウントです。

`/sbin/lsmmod` 出力は、`/proc/modules` の表示出力よりも詳細ではなく、読みやすくなります。

カーネルモジュールを読み込むには、`/sbin/modprobe` コマンドの後にカーネルモジュール名を使用します。デフォルトでは、`modprobe` は `/lib/modules/<kernel-version>/kernel/drivers/` サブディレクトリーからモジュールを読み込もうとします。各タイプのモジュールには、ネットワークインターフェースドライバの `net/` サブディレクトリーなど、各タイプのモジュールにサブディレクトリーがあります。一部のカーネルモジュールにはモジュールの依存関係があります。つまり、ロードするため

に他のモジュールを最初に読み込む必要があります。/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読み込む前にモジュールの依存関係を読み込みます。

たとえば、コマンドは以下のようになります。

```
/sbin/modprobe e100
```

モジュール依存関係を読み込み、次に e100 モジュールを読み込みます。

/sbin/modprobe が実行したコマンドをすべて画面に表示するには、-v オプションを使用します。以下に例を示します。

```
/sbin/modprobe -v e100
```

以下のような出力が表示されます。

```
/sbin/insmod /lib/modules/2.6.9-5.EL/kernel/drivers/net/e100.ko Using /lib/modules/2.6.9-5.EL/kernel/drivers/net/e100.ko Symbol version prefix 'smp_'
```

/sbin/insmod コマンドもカーネルモジュールを読み込むため存在しますが、依存関係は解決されません。したがって、/sbin/modprobe コマンドの使用が推奨されます。

カーネルモジュールをアンロードするには、/sbin/rmmod コマンドの後にモジュール名を使用します。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の依存関係ではないモジュールのみをアンロードします。

たとえば、コマンドは以下のようになります。

```
/sbin/rmmod e100
```

e100 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します。一般的な構文は以下のとおりです。

```
/sbin/modinfo [options]<module>
```

オプションには `-d` が含まれます。これにより、モジュールの簡単な説明が表示されます。`-p` は、モジュールがサポートするパラメーターを一覧表示します。オプションの完全なリストは、`modinfo` の `man` ページ(`man modinfo`)を参照してください。

## 37.2. 永続的なモジュールの読み込み

カーネルモジュールは通常、`/etc/modprobe.conf` ファイルに正しい設定が提供されるように、必要なファシリティーによって直接読み込まれます。ただし、システムの起動時にモジュールを明示的に読み込む必要がある場合があります。

Red Hat Enterprise Linux は、起動時に `/etc/rc.modules` ファイルが存在するかどうかをチェックします。これには、モジュールを読み込むさまざまなコマンドが含まれます。`rc.modules` は起動プロセスの早い段階で実行されるため、`rc.local` ではなく `rc.modules` を使用する必要があります。

たとえば、次のコマンドは、システムの起動時に `foo` モジュールの読み込みを設定します (root として)。

```
# echo modprobe foo >> /etc/rc.modules
# chmod +x /etc/rc.modules
```



### ヒント

ネットワークや SCSI インターフェースには独自のメカニズムがあるため、このアプローチは必要ありません。

## 37.3. 関連情報

カーネルモジュールとそのユーティリティーの詳細は、以下のリソースを参照してください。

### 37.3.1. インストールされているドキュメント

- `lsmod` `man` ページ: 出力の説明および説明
- `insmod` `man` ページ - コマンドラインオプションの説明および一覧
- `modprobe` の `man` ページ - コマンドラインオプションの説明および一覧

- ***rmmod man*** ページ: コマンドラインオプションの説明および一覧。
- ***modinfo の man*** ページ - コマンドラインオプションの説明および一覧
- ***/usr/share/doc/kernel-doc- &lt;version&gt; /Documentation/kbuild/modules.txt***: カーネルモジュールをコンパイルし、使用方法。

### 37.3.2. 便利な Web サイト

- **<http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html>**: 『Linux ドキュメントのプロジェクトからの Linux 読み込み可能カーネルモジュール HOWTO』

## 第38章 メール転送エージェント (MTA) の設定

メール転送エージェント (MTA) は電子メールの送信に不可欠です。メールユーザーエージェント (MUA) ( Evolution、Mozilla Mail、pidC)、および Mutt などのメールユーザーエージェント (MUA) は、電子メールの読み取りと構成に使用されます。ユーザーが MUA から電子メールを送信すると、メッセージは MTA に渡されます。MTA は一連の MTA を通じて、メッセージが送信先に届くまで送信します。

ユーザーがシステムから電子メールを送信する予定でなくても、一部の自動化されたタスクまたはシステムプログラムは、`/bin/mail` コマンドを使用して、ログメッセージを含む電子メールをローカルシステムの root ユーザーに送信する場合があります。

Red Hat Enterprise Linux 4 は、Sendmail、Postfix、および Exim の 3 つの MTA を提供します。3 つがすべてインストールされている場合は、sendmail がデフォルトの MTA になります。Mail Transport Agent Switcher を使用すると、sendmail、postfix、またはシステムのデフォルト MTA を選択できます。

Mail Transport Agent Switcher プログラムのテキストベースのバージョンを使用するには、system-switch-mail RPM パッケージをインストールする必要があります。グラフィカルバージョンを使用する場合は、system-switch-mail-gnome パッケージもインストールされている必要があります。

Mail Transport Agent Switcher を起動するには、Applications (パネルのメインメニュー) => Preferences => More Preferences => Mail Transport Agent Switcher を選択するか、シェルプロンプトで system-switch-mail コマンド (XTerm や GNOME ターミナルなど) を入力します。

プログラムは、X Window System が実行しているかどうかを自動的に検出します。実行中である場合、プログラムは [図38.1 「メール転送エージェントスイッチ」](#) に示されるようにグラフィカルモードで起動します。X が検出されないと、text-mode で起動します。Mail Transport Agent Switcher を text-mode で強制的に実行するには、system-switch-mail-nox コマンドを使用します。

図38.1 メール転送エージェントスイッチ



[D]

OK を選択して MTA を変更する場合、選択したメールデーモンは起動時に起動し、選択されていないメールデーモンは無効にされ、起動時に起動されないようにします。選択したメールデーモンが起動し、その他のメールデーモンは停止されるため、変更は即座に行われます。

メールプロトコルおよび MTA の詳細は、『『リファレンスガイド』』を参照してください。

## パート VI. システムモニタリング

システム管理者は、システムパフォーマンスも監視します。Red Hat Enterprise Linux には、管理者がこれらの作業を支援するツールが含まれています。

## 第39章 システム情報の収集

システムの設定方法を学習する前に、重要なシステム情報を収集する方法を学ぶ必要があります。たとえば、空きメモリー容量、利用可能なハードドライブの領域、ハードドライブのパーティション設定方法、実行中のプロセスを見つける方法を知っておく必要があります。本章では、簡単なコマンドと簡単なプログラムを使用して、この種類の情報を Red Hat Enterprise Linux システムから取得する方法を説明します。

### 39.1. システムプロセス

`ps ax` コマンドは、他のユーザーが所有しているプロセスを含め、現在のシステムプロセスの一覧を表示します。各プロセスと共に所有者を表示するには、`ps aux` コマンドを使用します。このリストは静的リストです。つまり、コマンドを呼び出したときに実行したもののスナップショットです。実行中のプロセスの一覧を常に更新する必要がある場合は、以下のように `top` を使用します。

`ps` 出力は長い可能性があります。画面をスクロールしてしまうのを防ぐために、パイプは少なくなります。

```
ps aux | less
```

`ps` コマンドを `grep` コマンドと組み合わせて使用して、プロセスが実行中かどうかを確認することができます。たとえば、Emacs が実行しているかどうかを確認するには、以下のコマンドを使用します。

```
ps ax | grep emacs
```

`top` コマンドは、現在実行中のプロセスと、メモリーや CPU の使用状況に関する重要な情報を表示します。この一覧は、リアルタイムとインタラクティブの両方になります。`top` コマンドの出力例を以下に示します。

```
top - 15:02:46 up 35 min, 4 users, load average: 0.17, 0.65, 1.00
Tasks: 110 total, 1 running, 107 sleeping, 0 stopped, 2 zombie
Cpu(s): 41.1% us, 2.0% sy, 0.0% ni, 56.6% id, 0.0% wa, 0.3% hi, 0.0% si
Mem: 775024k total, 772028k used, 2996k free, 68468k buffers
Swap: 1048568k total, 176k used, 1048392k free, 441172k cached

  PID USER   PR  NI  VIRT  RES  SHR  S %CPU %MEM  TIME+  COMMAND
 4624 root    15   0 40192 18m 7228 S 28.4  2.4  1:23.21 X
 4926 mhideo  15   0 55564 33m 9784 S 13.5  4.4  0:25.96 gnome-terminal
 6475 mhideo  16   0 3612  968 760 R  0.7  0.1  0:00.11 top
 4920 mhideo  15   0 20872 10m 7808 S  0.3  1.4  0:01.61 wnck-applet
    1 root    16   0 1732  548 472 S  0.0  0.1  0:00.23 init
    2 root    34  19   0    0  0 S  0.0  0.0  0:00.00 ksoftirqd/0
    3 root     5 -10   0    0  0 S  0.0  0.0  0:00.03 events/0
```



```

4 root    6-10    0  0  0 S  0.0  0.0  0:00.02 khelper
5 root    5-10    0  0  0 S  0.0  0.0  0:00.00 kacpid
29 root   5-10    0  0  0 S  0.0  0.0  0:00.00 kblockd/0
47 root   16  0    0  0  0 S  0.0  0.0  0:01.74 pdflush
50 root   11-10   0  0  0 S  0.0  0.0  0:00.00 aio/0
30 root   15  0    0  0  0 S  0.0  0.0  0:00.05 khubd
49 root   16  0    0  0  0 S  0.0  0.0  0:01.44 kswapd0

```

`top` を終了するには、`q` キーを押します。

表39.1「対話型の `top` コマンド」には、`top` で使用できる便利な対話型のコマンドが含まれています。詳細は、`top(1)` の `man` ページを参照してください。

表39.1 対話型の `top` コマンド

コマンド	Description
スペース	表示を即時にリフレッシュします。
<code>h</code>	ヘルプ画面の表示
<code>k</code>	プロセスを強制終了します。プロセス ID およびプロセスに送信するシグナルがプロンプトされます。
<code>-n</code>	表示されるプロセス数を変更します。番号を入力するようプロンプトされます。
<code>u</code>	ユーザー別に並べ替えます。
<code>M</code>	メモリー使用量で並べ替えます。
<code>%P</code>	CPU 使用率で並べ替えます。

上部のグラフィカルインターフェースを使用する場合は、GNOME システムモニターを使用できます。デスクトップから起動するには、`System => Administration => System Monitor` を選択するか、シェルプロンプトで `gnome-system-monitor` を入力します (XTerm など)。Process Listing タブを選択します。

GNOME System Monitor を使用すると、実行中のプロセスの一覧でプロセスを検索できます。Gnome System Monitor を使用して、すべてのプロセス、プロセス、またはアクティブなプロセスを確認することもできます。

**Edit** メニュー項目を使用すると、以下が可能になります。

- プロセスを停止します。
- プロセスを続行または開始します。
- プロセスを終了します。
- プロセスを強制終了します。
- 選択したプロセスの優先度を変更します。
- システムモニターの設定を編集します。これには、一覧を更新する間隔（秒単位）の変更や、システムモニターウィンドウに表示されるプロセスフィールドの選択が含まれます。

**View** メニュー項目では、以下を行うことができます。

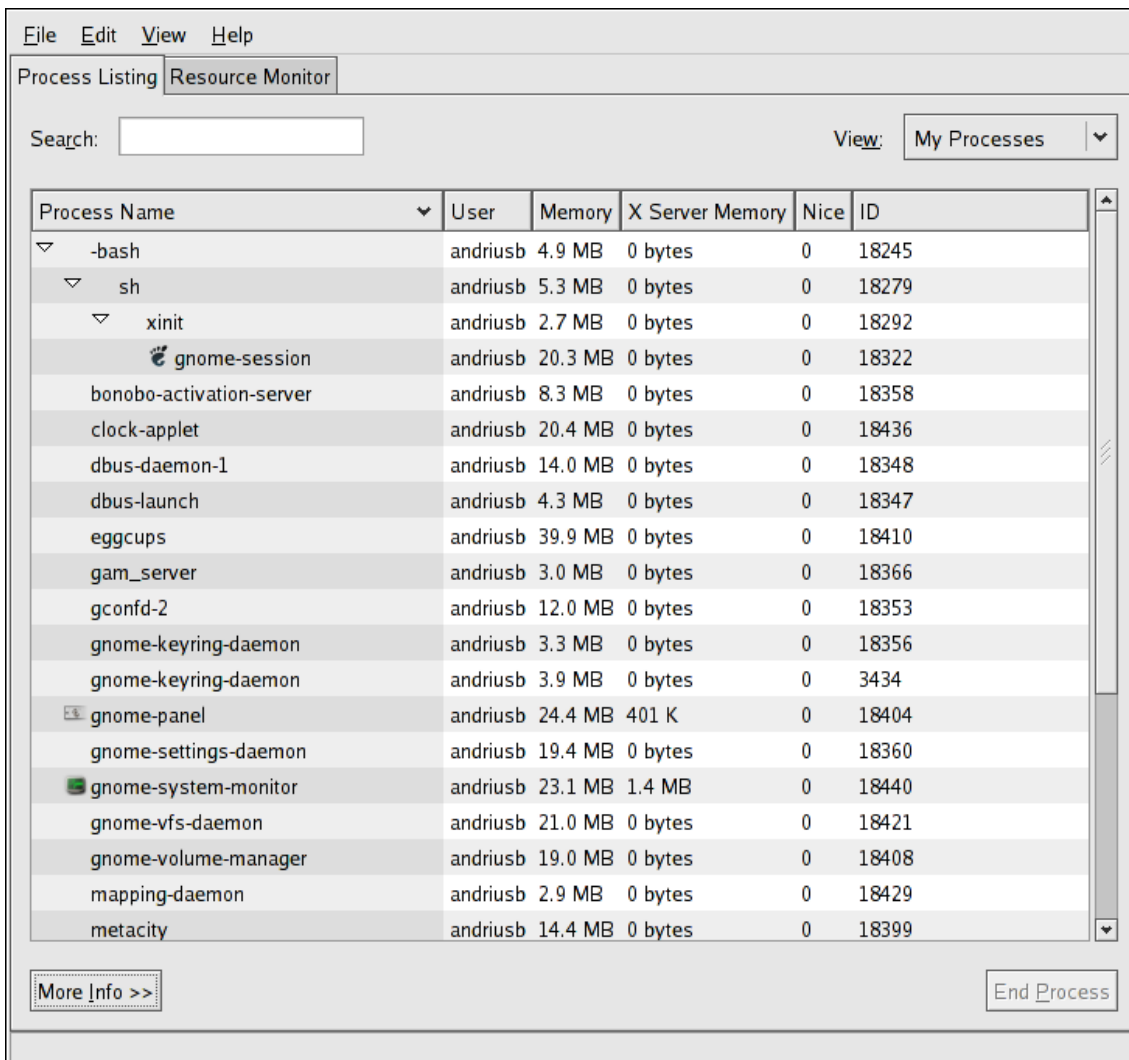
- アクティブなプロセスのみを表示します。
- すべてのプロセスを表示します。
- プロセスを表示します。
- プロセスの依存関係を表示します。
- プロセスを非表示にします。
- 非表示のプロセスを表示します。

- メモリーマップを表示します。
- 選択したプロセスで開いているファイルを表示します。

プロセスを停止するには、プロセスを選択し、プロセスの終了をクリックします。または、メニューから **Edit** をクリックし、**Stop Process** を選択してプロセスを停止することもできます。

特定の列で情報を並べ替えるには、列の名前をクリックします。これにより、選択した列で情報を昇順でソートできます。列の名前を再度クリックして、昇順と降順のソートを切り替えます。

図39.1 GNOME システムモニター



[D]

## 39.2. MEMORY USAGE

`free` コマンドは、システムの物理メモリーおよびスワップ領域の合計量と、カーネルバッファ内

で使用、解放、共有、およびキャッシュされているメモリー量を表示します。

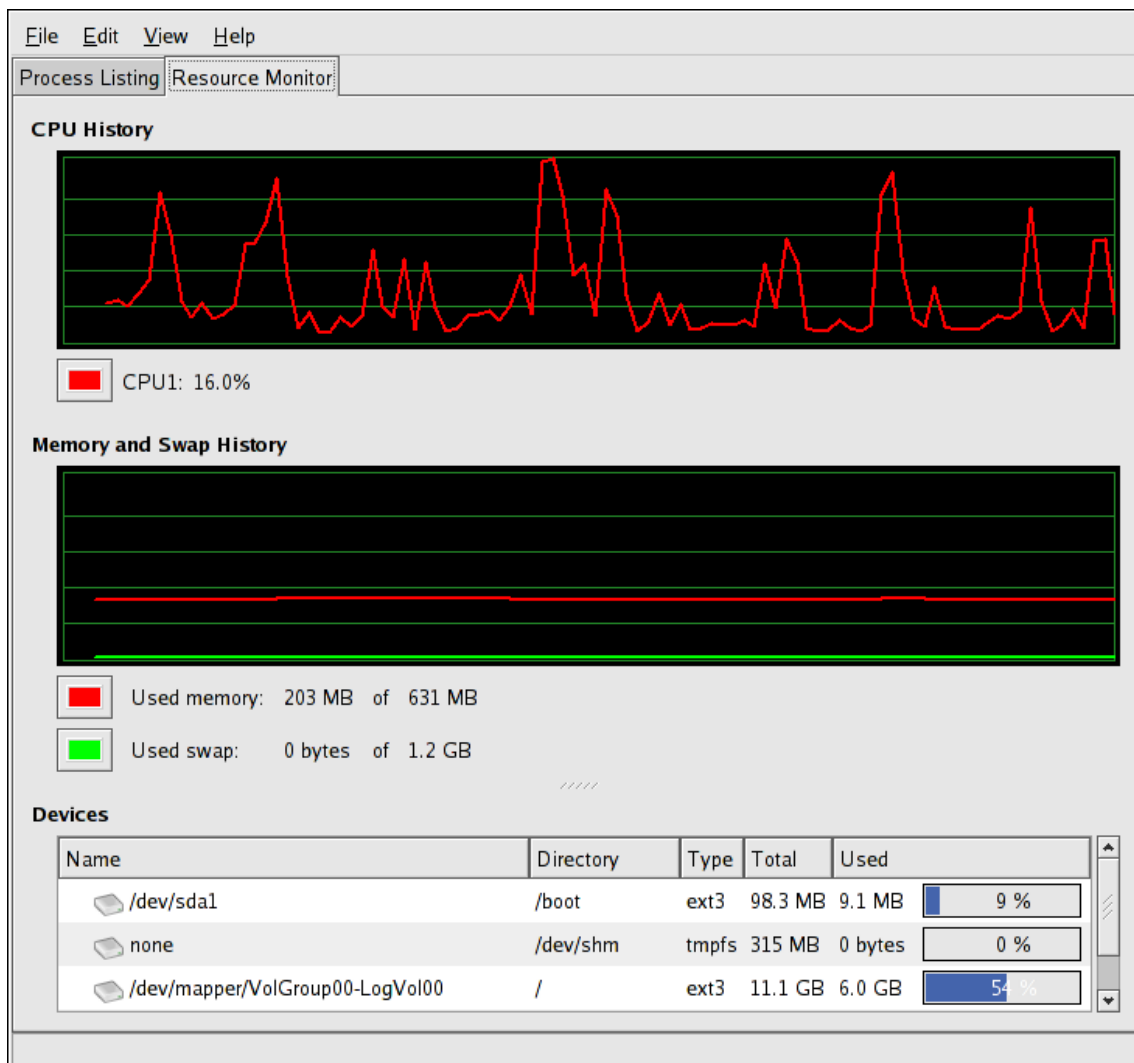
```
      total    used    free  shared  buffers  cached
Mem:    645712  549720   95992     0    176248  224452
-/+ buffers/cache:  149020  496692
Swap:   1310712     0   1310712
```

`free -m` コマンドは、同じ情報をメガバイトで表示しますが、これは読みやすくなります。

```
      total    used    free  shared  buffers  cached
Mem:     630     536     93     0     172     219
-/+ buffers/cache:    145     485
Swap:    1279     0    1279
```

フリーのグラフィカルインターフェースを使用する場合は、GNOME システムモニターを使用できます。デスクトップから起動するには、**System => Administration => System Monitor** に移動するか、シェルプロンプトで `gnome-system-monitor` を入力します (XTerm など)。Resources タブをクリックします。

図39.2 GNOME システムモニター - リソースタブ



[D]

### 39.3. 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量を報告します。シェルプロンプトで `df` コマンドを入力すると、出力は以下のようになります。

```
Filesystem      1K-blocks  Used Available Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
 11675568 6272120 4810348 57% //dev/sda1
 100691   9281   86211 10% /boot
none        322856    0 322856 0% /dev/shm
```

デフォルトでは、このユーティリティーは、1 キロバイトブロック単位でパーティションのサイズを、キロバイト単位で使用中および利用可能なディスク領域の容量を表示します。メガバイトおよびギガバイトで情報を表示するには、`df -h` コマンドを使用します。`-h` 引数は人間が判読できる形式を表します。出力は以下の例のようになります。

```
Filesystem      Size Used Avail Use% Mounted on
```

```

/dev/mapper/VolGroup00-LogVol00
    12G 6.0G 4.6G 57% //dev/sda1
    99M 9.1M 85M 10% /boot
    none 316M 0 316M 0% /dev/shm

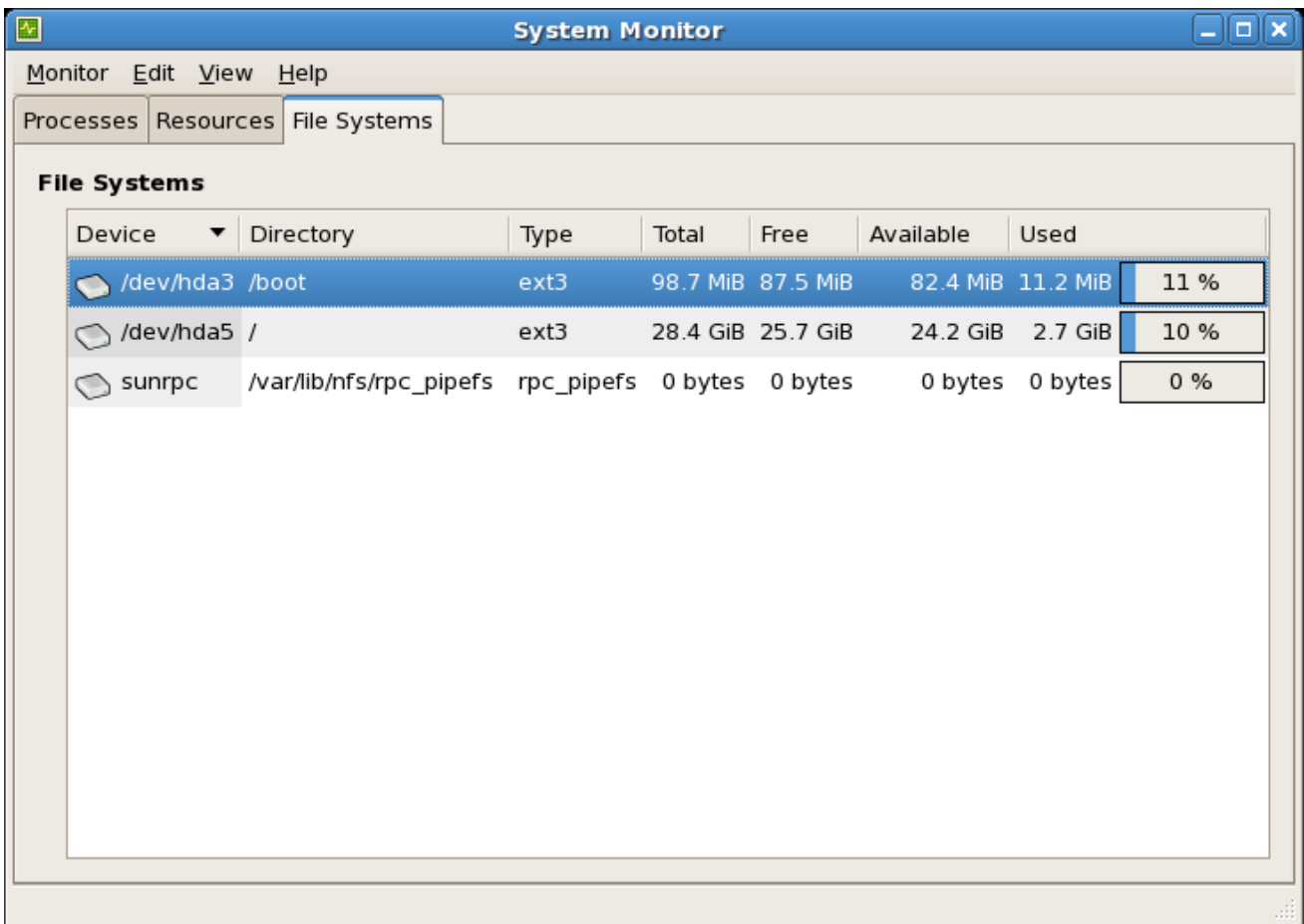
```

マウントされたパーティションの一覧には、`/dev/shm` のエントリーがあります。このエントリーは、システムの仮想メモリーファイルシステムを表します。

`du` コマンドはディレクトリー内のファイルが使用している領域を表示します。シェルプロンプトで `du` と入力しても、各サブディレクトリーのディスク使用量が一覧に表示されます。現在のディレクトリーおよびサブディレクトリーの合計量も、一覧の最後の行として表示されます。すべてのサブディレクトリーの合計を表示したくない場合は、`du -hs` コマンドを使用して、人間が判読可能な形式でディレクトリーの合計のみを表示します。その他のオプションを表示するには、`du --help` コマンドを使用します。

システムのパーティションとディスク領域の使用量をグラフィカル形式で表示するには、**System => Administration => System Monitor** をクリックして **Gnome System Monitor** を使用し、シェルプロンプトで `gnome-system-monitor` を入力します (XTerm など)。ファイルシステム タブを選択して、システムのパーティションを表示します。以下の図は、ファイルシステム タブを示しています。

図39.3 GNOME システムモニター - ファイルシステム

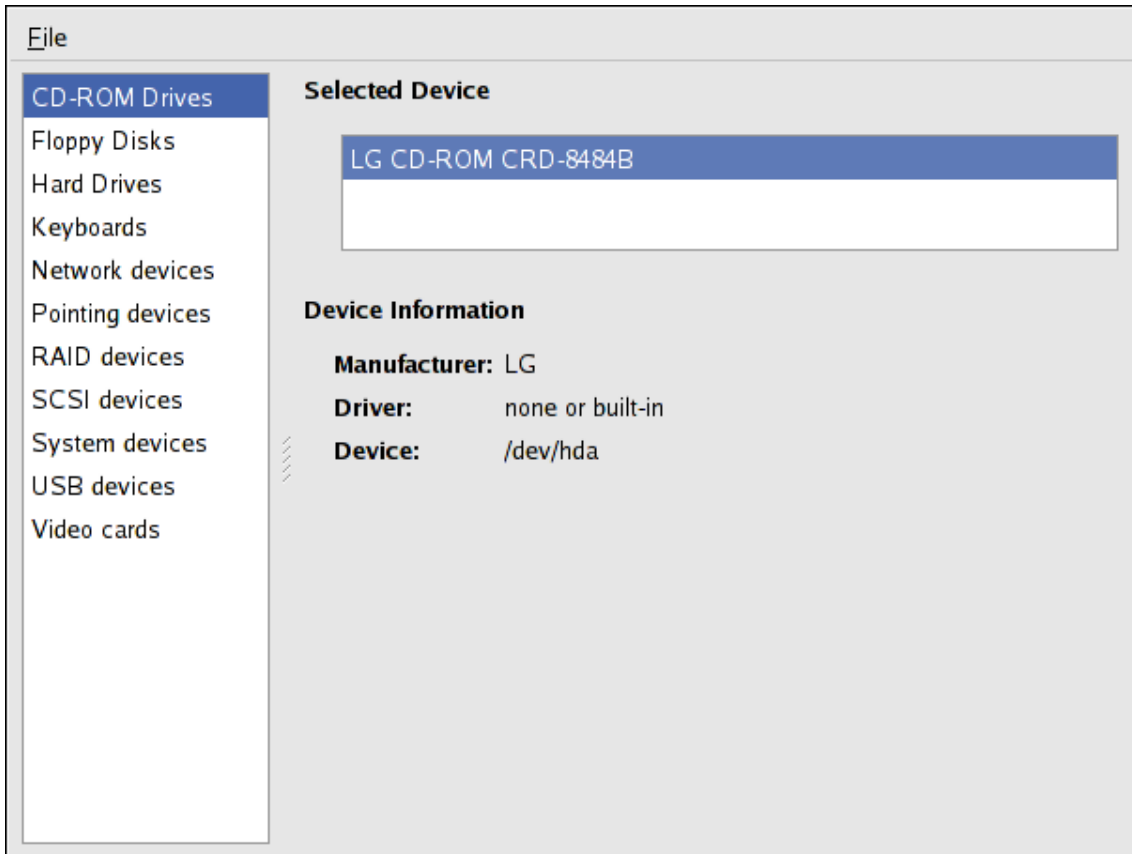


[D]

### 39.4. ハードウェア

ハードウェアの設定に問題がある場合や、システムにあるハードウェアを把握する必要がある場合は、**Hardware Browser** アプリケーションを使用してプローブできるハードウェアを表示できます。デスクトップからプログラムを起動するには、**System**（パネルのメインメニュー）⇒ **Administration** ⇒ **Hardware** を選択するか、またはシェルプロンプトで `hwbrowser` と入力します。図39.4「ハードウェアブラウザー」で示されているように、**CD-ROM** デバイス、ディスクドライブ、ハードドライブ、パーティション、ネットワークデバイス、ポイントデバイス、システムデバイス、ビデオカードが表示されます。左側のメニューでカテゴリ名をクリックすると、情報が表示されます。

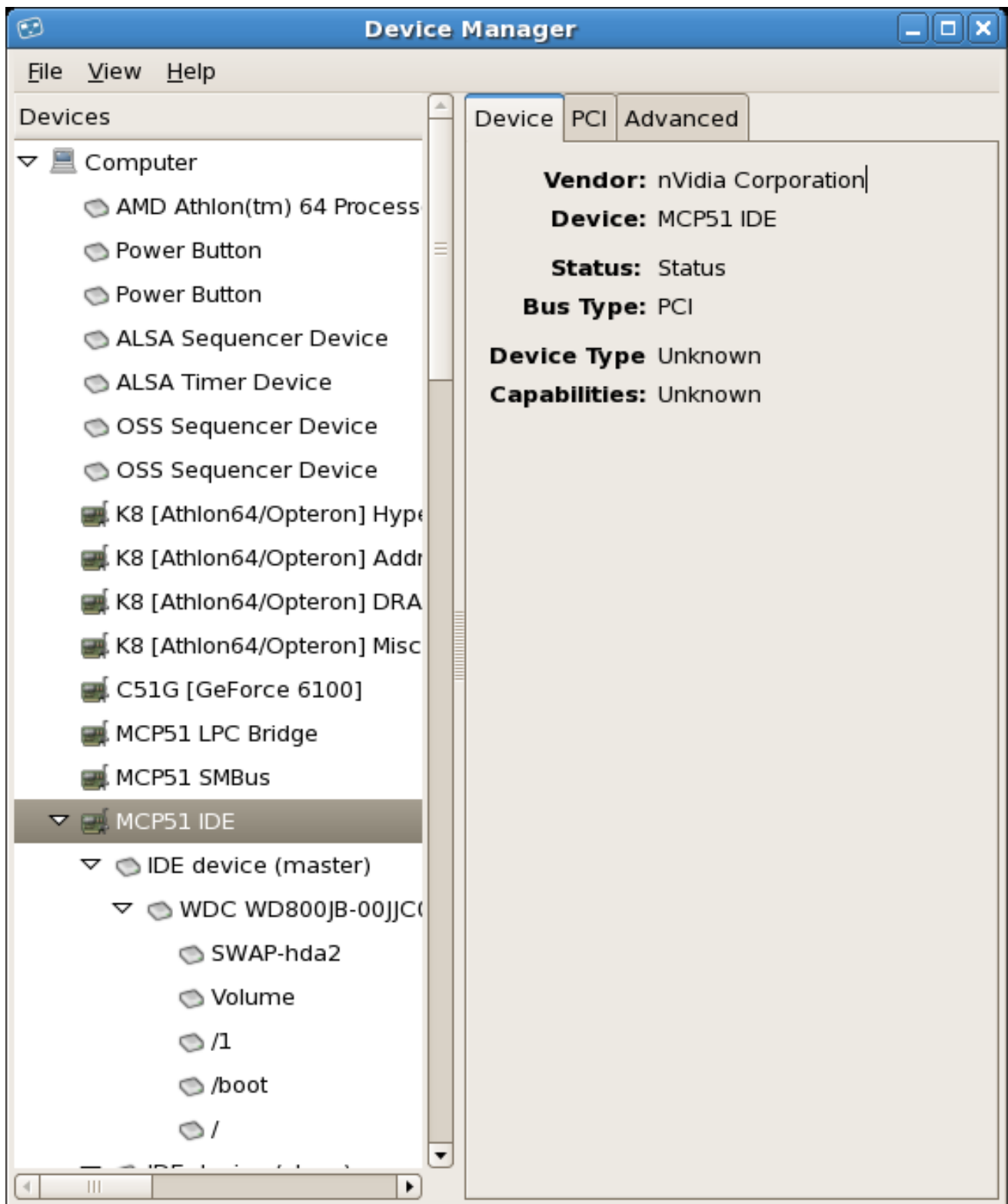
図39.4 ハードウェアブラウザー



[D]

**Device Manager** アプリケーションを使用して、システムハードウェアを表示することもできます。このアプリケーションを起動するには、**System**（パネルのメインメニュー）⇒ **Administration** ⇒ **Hardware Browser** のようなハードウェアを選択します。ターミナルからアプリケーションを起動するには、`hal-device-manager` と入力します。インストールの設定によっては、上記のグラフィカルメニューがこのアプリケーションを起動したり、クリックするとハードウェアブラウザーを起動することがあります。以下の図は、**Device Manager** ウィンドウを示しています。

図39.5 デバイスマネージャー



[D]

*lspci* コマンドを使用して、すべての PCI デバイスを一覧表示することもできます。詳細情報については *lspci -v* コマンド、または非常に詳細な出力には *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製造元、モデル、およびメモリーサイズを判断できます。



```
00:00.0 Host bridge: ServerWorks CNB20LE Host Bridge (rev 06)
00:00.1 Host bridge: ServerWorks CNB20LE Host Bridge (rev 06)
00:01.0 VGA compatible controller: S3 Inc. Savage 4 (rev 04)
00:02.0 Ethernet controller: Intel Corp. 82557/8/9 [Ethernet Pro 100] (rev 08)
00:0f.0 ISA bridge: ServerWorks OSB4 South Bridge (rev 50)
00:0f.1 IDE interface: ServerWorks OSB4 IDE Controller
00:0f.2 USB Controller: ServerWorks OSB4/CSB5 OHCI USB Controller (rev 04)
01:03.0 SCSI storage controller: Adaptec AIC-7892P U160/m (rev 02)
01:05.0 RAID bus controller: IBM ServeRAID Controller
```

`lspci` は、製造元またはモデル番号が分からない場合に、システムのネットワークカードを確認する際に役立ちます。

## 39.5. 関連情報

システム情報の収集の詳細は、以下のリソースを参照してください。

### 39.5.1. インストールされているドキュメント

- `ps --help - ps` で使用できるオプションの一覧を表示します。
- トップ `man` ページ: `top` およびそのオプションに関する詳細は、`man top` を参照してください。
- フリー `man` ページ - `man free` と入力し、フリーオプションとその多くのオプションの詳細を確認してください。
- `df man` ページ - `man df` と入力して、`df` コマンドとその多くのオプションの詳細を確認します。
- `du` の `man` ページ - `man du` と入力して、`du` コマンドとその多くのオプションの詳細を確認します。
- `lspci man` ページ: `lspci` コマンドとそのオプションの詳細を確認するには、`man lspci` と入力します。
- `/proc/` ディレクトリー: `/proc/` ディレクトリーのコンテンツを使用して、より詳細なシ

システム情報を収集することもできます。

## 第40章 OPROFILE

OProfile は、オーバーヘッドが低い、システム全体のパフォーマンス監視ツールです。これはプロセッサ上のパフォーマンス監視ハードウェアを使用して、メモリーの参照時、L2 キャッシュ要求の数、受信したハードウェア割り込みの数など、システムのカーネルと実行可能ファイルに関する情報を取得します。Red Hat Enterprise Linux システムでは、このツールを使用するには `oprofile 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。

多くのプロセッサには、専用のパフォーマンス監視ハードウェアが含まれます。このハードウェアを使用すると、特定のイベントの発生時（要求されたデータがキャッシュにないなど）を検出できます。ハードウェアは通常、イベントが実行されるたびにインクリメントされる 1 つ以上のカウンターの形式を取ります。カウンターの値が基本的にロールオーバーされると割り込みが生成され、パフォーマンス監視で生成される詳細（つまりオーバーヘッド）の量を制御できます。

OProfile はこのハードウェア（またはパフォーマンス監視ハードウェアが存在しない場合）を使用して、カウンターが割り込みを生成するたびにパフォーマンス関連のデータのサンプルを収集します。これらのサンプルは定期的にディスクに書き込まれます。その後、これらのサンプルに含まれるデータを使用して、システムレベルのパフォーマンスおよびアプリケーションレベルのパフォーマンスに関するレポートを生成できます。

OProfile は便利なツールですが、これを使用する場合にはいくつかの制限に注意してください。

- 共有ライブラリーの使用：共有ライブラリーのコードの Samples は、`--separate=library` オプションが使用されていない限り、特定のアプリケーションに属性されません。
- パフォーマンス監視サンプルは正確に行われません。パフォーマンス監視レジスターがサンプルをトリガーすると、割り込み処理はゼロ例外による分割のように正確ではありません。プロセッサによる命令の順不同な実行により、サンプルはほぼ近い命令に記録される場合があります。
- `opreport` は、インライン関数のサンプルを適切に関連付けません。`opreport` は単純なアドレス範囲メカニズムを使用して、アドレスがどの関数にあるかを判断します。インライン関数のサンプルは、インライン関数には属性ではなく、インライン関数が挿入された関数に対して属性されません。
- OProfile は複数の実行からのデータを累積します。OProfile はシステム全体のプロファイラーであり、プロセスが複数回起動し、シャットダウンすることを想定します。そのため、複数の実行のサンプルが累積されました。`opcontrol --reset` コマンドを使用して、直前の実行からサンプルを消去します。

- CPU の制限のないパフォーマンスの問題: OProfile は、CPU の制限のあるプロセスの問題を見つけるために使用されます。OProfile は、ロックを待機するか、または他のイベントが発生するため、`sleep` であるプロセスを特定しません (例: I/O デバイスで操作を終了するなど)。

#### 40.1. ツールの概要

表40.1 「OProfile コマンド」では、`oprofile` パッケージで提供されるツールの概要を説明します。

表40.1 OProfile コマンド

コマンド	Description
<code>op_help</code>	システムプロセッサで使用可能なイベントとその簡単な説明を表示します。
<code>op_import</code>	サンプルデータベースファイルをシステム用に外部のバイナリー形式からネイティブの形式に変換します。異なるアーキテクチャーからのサンプルデータベースを解析する場合にのみこのオプションを使用してください。
<code>opannotate</code>	アプリケーションがデバッグシンボルでコンパイルされている場合は、実行可能ファイルのアノテーション付きソースを作成します。詳細は、「 <a href="#">opannotateの使用</a> 」を参照してください。
<code>opcontrol</code>	収集されるデータを設定します。詳細は、「 <a href="#">OProfile の設定</a> 」を参照してください。

コマンド	Description
<b>opreport</b>	プロファイリングデータを取得します。詳細は、 <a href="#">「opreportの使用」</a> を参照してください。
<b>oprofiled</b>	デーモンとして実行して定期的にサンプルデータをディスクに書き込みます。

## 40.2. OPROFILE の設定

OProfile を実行する前に、設定する必要があります。少なくとも、カーネルの監視（またはカーネルを監視しない選択）を選択することが必要です。次のセクションでは、`opcontrol` ユーティリティーを使用して OProfile を設定する方法を説明します。`opcontrol` コマンドを実行すると、設定オプションが `/root/.oprofile/daemonrc` ファイルに保存されます。

### 40.2.1. カーネルの指定

まず、OProfile がカーネルを監視するかどうかを設定します。これは、OProfile を起動する前に必要となる唯一の設定オプションです。その他はすべてオプションです。

カーネルを監視するには、`root` で以下のコマンドを実行します。

```
opcontrol --setup --vmlinux=/usr/lib/debug/lib/modules/`uname -r`/vmlinux
```



#### 備考

カーネルを監視するために、`debuginfo` パッケージがインストールされている（非圧縮カーネルを含む）。

カーネルを監視しないように OProfile を設定するには、`root` で以下のコマンドを実行します。

```
opcontrol --setup --no-vmlinux
```

このコマンドは、oprofile カーネルモジュールもロードされていない場合は読み込み、/dev/oprofile/ ディレクトリーが存在しない場合は作成します。このディレクトリーの詳細は、「[/dev/oprofile/について](#)」を参照してください。



#### 備考

OProfile がカーネルのプロファイル用に設定されていない場合でも、oprofile モジュールをファイルからロードできるように SMP カーネルを実行する必要があります。

カーネル内でサンプルを収集するべきかどうかを設定することにより、収集されるデータのみが変更され、収集したデータが保存される方法や場所は変更されません。カーネルライブラリーおよびアプリケーションライブラリーのさまざまなサンプルファイルを生成するには、「[カーネルとユーザー空間プロファイルの分離](#)」を参照してください。

#### 40.2.2. 監視するイベントの設定

ほとんどのプロセッサにはカウンターが含まれており、これは特定のイベントを監視するために OProfile によって使用されます。表40.2「[OProfile Processors and Counters](#)」で示されているように、利用可能なカウンターの数はプロセッサによって異なります。

表40.2 OProfile Processors and Counters

プロセッサ	cpu_type	カウンターの数
Pentium Pro	i386/ppro	2
Pentium II	i386/pii	2
Pentium336	i386/piii	2
Pentium 4(hy-hyper- thread)	i386/p4	8
Pentium 4 (ハイパースレッド)	i386/p4-ht	4
Athlon	i386/athlon	4
AMD64	x86-64/hammer	4
pidgin	ia64/itanium	4

プロセッサ	cpu_type	カウンターの数
Itanium 2	ia64/itanium2	4
TIMER_INT	timer	1
IBM eServer iSeries and pSeries	timer	1
	ppc64/power4	8
	ppc64/power5	6
	ppc64/970	8
IBM eServer S/390 および S/390x	timer	1
IBM eServer zSeries	timer	1

**表40.2 「OProfile Processors and Counters」** を使用して、正しいプロセッサタイプが検出され、同時に監視できるイベントの数を判断します。プロセッサでパフォーマンス監視ハードウェアがサポートされていない場合は、タイマーがプロセッサタイプとして使用されます。

タイマーを使用する場合は、ハードウェアのパフォーマンスカウンターに対応していないため、どのプロセッサにもイベントも設定できません。代わりに、タイマー割り込みがプロファイリングに使用されます。

タイマーがプロセッサタイプとして使用されていない場合は、監視されるイベントを変更し、プロセッサのカウンター0はデフォルトで時間ベースのイベントに設定されます。プロセッサに複数のカウンターが存在する場合は、カウンター0以外のカウンターはデフォルトでイベントには設定されません。監視されるデフォルトイベントは、**表40.3 「デフォルトイベント」** に表示されます。

表40.3 デフォルトイベント

プロセッサ	カウンターのデフォルトイベント	Description
Pentium Pro, Pentium II, Pentium III, Athlon, AMD64	CPU_CLK_UNHALTED	プロセッサのクロックが停止されていない

プロセッサ	カウンターのデフォルトイベント	Description
Pentium 4 (HT および非 HT)	GLOBAL_POWER_EVENTS	プロセッサが停止していない時間
Itanium 2	CPU_CYCLES	CPU ライフサイクル
TIMER_INT	(なし)	各タイマー割り込みの例
ppc64/power4	サイクル	プロセッササイクル
ppc64/power5	サイクル	プロセッササイクル
ppc64/970	サイクル	プロセッササイクル

一度に監視できるイベントの数は、プロセッサのカウンター数によって決定されます。ただし、1対1の相関ではありません。一部のプロセッサでは、特定のイベントを特定のカウンターにマップする必要があります。利用可能なカウンターの数を確認するには、以下のコマンドを実行します。

```
cat /dev/oprofile/cpu_type
```

利用可能なイベントはプロセッサのタイプによって異なります。プロファイリングに使用できるイベントを確認するには、`root` で以下のコマンドを実行します（一覧はシステムのプロセッサタイプに固有のものです）。

```
op_help
```

各カウンターのイベントは、コマンドラインまたはグラフィカルインターフェースで設定できます。グラフィカルインターフェースの詳細は、「[グラフィカルインターフェース](#)」を参照してください。カウンターを特定のイベントに設定しない場合は、エラーメッセージが表示されます。

コマンドラインで設定可能な各カウンターのイベントを設定するには、`opcontrol` を使用します。

```
opcontrol --event=<event-name>:<sample-rate>
```

<event-name> を `op_help` のイベントの正確な名前に置き換え、<sample-rate> をサンプル間のイベント数に置き換えます。



### 40.2.2.1. サンプリングレート

デフォルトでは、時間ベースのイベントセットが選択されます。プロセッサごとに 100,000 クロックサイクルごとにサンプルを作成します。タイマー割り込みを使用する場合は、タイマーは jiffy レートがどれでも設定され、ユーザー設定のテーブルではありません。cpu\_type がタイマーでない場合、各イベントにはサンプリングレートを設定できます。サンプリングレートは、各サンプルスナップショット間のイベント数です。

カウンターのイベントを設定する場合、サンプルレートを指定することもできます。

```
opcontrol --event=<event-name>:<sample-rate>
```

<sample-rate> を、再度サンプリングする前に待機するイベントの数に置き換えます。数値が小さいほど、サンプルが頻繁に使用されます。頻繁に発生しないイベントの場合、イベントインスタンスをキャプチャーするためにカウントが低くなる可能性があります。



#### WARNING

サンプリングレートを設定する場合は十分に注意してください。サンプリングが頻繁にシステムをオーバーロードする可能性があります。これにより、システムがフリーズするか、システムが実際にフリーズするかのようにシステムが表示されます。

### 40.2.2.2. ユニットマスク

cpu\_type がタイマーでない場合、イベントをさらに定義するためにユニットマスクが必要になる場合もあります。

各イベントのユニットマスクは、op\_help コマンドで一覧表示されます。各ユニットマスクの値は 16 進数形式で一覧表示されます。複数のユニットマスクを指定するには、ビット単位の操作または操作を使用して 16 進数の値を組み合わせる必要があります。

```
opcontrol --event=<event-name>:<sample-rate>:<unit-mask>
```

### 40.2.3. カーネルとユーザー空間プロファイルの分離

デフォルトでは、カーネルモードおよびユーザーモード情報は、各イベントについて収集されま

す。特定のカウンターのカーネルモードでイベントをカウントしないように OProfile を設定するには、以下のコマンドを実行します。

```
opcontrol --event=<event-name>:<sample-rate>:<unit-mask>:0
```

次のコマンドを実行して、カウンターのカーネルモードのプロファイリングを開始します。

```
opcontrol --event=<event-name>:<sample-rate>:<unit-mask>:1
```

特定のカウンターのユーザーモードでイベントをカウントしないように OProfile を設定するには、以下のコマンドを実行します。

```
opcontrol --event=<event-name>:<sample-rate>:<unit-mask>:<kernel>:0
```

次のコマンドを実行して、カウンターのユーザーモードを再度プロファイリングします。

```
opcontrol --event=<event-name>:<sample-rate>:<unit-mask>:<kernel>:1
```

OProfile デーモンがプロファイルデータをサンプルファイルに書き込むと、カーネルとライブラリープロファイルデータをサンプルファイルに分割できます。デーモンがサンプルファイルに書き込む方法を設定するには、`root` で以下のコマンドを実行します。

```
opcontrol --separate=<choice>
```

&lt;choice&gt; は以下のいずれかになります。

- `none`: プロファイルを分離しません (デフォルト)。
- `library-library`: ライブラリー - ライブラリー のアプリケーションごとのプロファイルを生成します。
- `kernel`: カーネルおよびカーネルモジュール用のアプリケーションごとのプロファイルを生成します。
- `all`: カーネルおよびカーネルモジュールのライブラリーおよびアプリケーションごとのプロファイルを生成します。

`--separate=library` が使用される場合、サンプルファイル名には実行可能ファイルの名前およびライブラリーの名前が含まれます。

### 40.3. OPROFILE の起動および停止

OProfile を使用してシステムのモニタリングを開始するには、`root` で以下のコマンドを実行します。

```
opcontrol --start
```

以下のような出力が表示されます。

```
Using log file /var/lib/oprofile/oprofiled.log
Daemon started.
Profiler running.
```

`/root/.oprofile/daemonrc` の設定が使用されます。

OProfile デーモン `oprofiled` が起動し、定期的にサンプルデータを `/var/lib/oprofile/samples/` ディレクトリーに書き込みます。デーモンのログファイルは `/var/lib/oprofile/oprofiled.log` にあります。

プロファイラーを停止するには、`root` で以下のコマンドを実行します。

```
opcontrol --shutdown
```

### 40.4. データの保存

特定の時間にサンプルを保存すると便利な場合もあります。たとえば、実行可能ファイルをプロファイリングする場合、異なる入力データセットに基づいて異なるサンプルを収集すると便利です。監視するイベントの数がプロセッサで利用可能なカウンター数を超える場合は、OProfile の複数の実行を使用してデータを収集し、常にサンプルデータを異なるファイルに保存します。

サンプルファイルの現在のセットを保存するには、以下のコマンドを実行します。`< name >` は、現行セッションの一意記述名に置き換えてください。

```
opcontrol --save=<name>
```

`/var/lib/oprofile/samples/` ディレクトリーが作成され、現在のサンプルファイルがコピーされま  
す。

#### 40.5. データの分析

OProfile デーモン `oprofiled` は定期的にサンプルを収集し、それらを `/var/lib/oprofile/samples/`  
ディレクトリーに書き込みます。データを読み取る前に、`root` で以下のコマンドを実行して、すべての  
データがこのディレクトリーに書き込まれていることを確認します。

```
opcontrol --dump
```

各サンプルファイル名は、実行可能ファイルの名前に基づいています。たとえば、`/bin/bash` の  
Pentiumでのデフォルトイベントのサンプルは以下のようになります。

```
\{root\}/bin/bash/\{dep\}/\{root\}/bin/bash/CPU_CLK_UNHALTED.100000
```

以下のツールは、サンプルデータの収集後にサンプルデータのプロファイルに使用できます。

- `opreport`
- `opannotate`

これらのツールとバイナリープロファイルを使用して、さらに分析できるレポートを生成します。



#### WARNING

プロファイルされる実行可能ファイルは、データを分析するためにこのツール  
と共に使用する必要があります。データの収集後に変更する必要がある場合は、サ  
ンプルファイルおよびサンプルファイルの作成に使用する実行ファイルをバック  
アップします。

各実行可能ファイルのサンプルは、1つのサンプルファイルに書き込まれます。動的にリンクされた  
各ライブラリーからのサンプルも、1つのサンプルファイルに書き込まれます。OProfile が実行中に、  
変更がモニタリングされ、実行可能ファイルのサンプルファイルが存在する場合、既存のサンプルファ

イルが自動的に削除されます。したがって、既存のサンプルファイルが必要な場合は、実行ファイルを新バージョンに置き換える前に、作成に使用する実行ファイルと共にバックアップする必要があります。サンプルファイルのバックアップ方法は、「データの保存」を参照してください。

#### 40.5.1. oprofileの使用

oprofile ツールは、プロファイルされるすべての実行可能ファイルの概要を提供します。

以下は出力例の一部です。

```
Profiling through timer interrupt
  TIMER:0|
samples|  %|
-----
25926 97.5212 no-vmlinux
 359  1.3504 pi
  65  0.2445 Xorg
  62  0.2332 libvte.so.4.4.0
  56  0.2106 libc-2.3.4.so
  34  0.1279 libglib-2.0.so.0.400.7
  19  0.0715 libXft.so.2.1.2
  17  0.0639 bash
   8  0.0301 ld-2.3.4.so
   8  0.0301 libgdk-x11-2.0.so.0.400.13
   6  0.0226 libgobject-2.0.so.0.400.7
   5  0.0188 oprofiled
   4  0.0150 libpthread-2.3.4.so
   4  0.0150 libgtk-x11-2.0.so.0.400.13
   3  0.0113 libXrender.so.1.2.2
   3  0.0113 du
   1  0.0038 libcrypto.so.0.9.7a
   1  0.0038 libpam.so.0.77
   1  0.0038 libtermcap.so.2.0.8
   1  0.0038 libX11.so.6.2
   1  0.0038 libgthread-2.0.so.0.400.7
   1  0.0038 libwnck-1.so.4.9.0
```

各実行可能ファイルは各行に一覧表示されます。最初の列は、実行ファイル用に記録されたサンプル数です。2列目は、サンプルの合計数に対するサンプルの割合です。3列目は実行可能ファイルの名前です。

利用可能なコマンドラインオプションの一覧は、man ページの `oprofile` を参照してください。たとえば、`-r` オプションでは、サンプルの最大数が最も少ない実行可能ファイルから、最大数のサンプルを持つ実行ファイルから出力をソートします。

#### 40.5.2. 単一の実行可能ファイルでの oprofile の使用

特定の実行ファイルに関するより詳細なプロファイル情報を取得するには、`opreport` を使用しません。

```
opreport <mode><executable>
```

分析する実行可能ファイルへの完全パスである `<executable>` 必要があります。 `&lt;mode>` は以下のいずれかでなければなりません。

`-l`

シンボルによるサンプルデータを一覧表示します。たとえば、以下は、`opreport -l /lib/tls/libc- <version> .so` コマンドを実行する際の出力の一部です。

```

samples %    symbol name
12   21.4286 __gconv_transform_utf8_internal
5    8.9286  _int_malloc
4    7.1429  malloc
3    5.3571  __i686.get_pc_thunk.bx
3    5.3571  _dl_mcount_wrapper_check
3    5.3571  mbrtowc
3    5.3571  memcpy
2    3.5714  _int_realloc
2    3.5714  _nl_intern_locale_data
2    3.5714  free
2    3.5714  strcmp
1    1.7857  __ctype_get_mb_cur_max
1    1.7857  __unregister_atfork
1    1.7857  __write_nocancel
1    1.7857  _dl_addr
1    1.7857  _int_free
1    1.7857  _itoa_word
1    1.7857  calc_eclosure_iter
1    1.7857  fopen@@GLIBC_2.1
1    1.7857  getpid
1    1.7857  memmove
1    1.7857  msort_with_tmp
1    1.7857  strcpy
1    1.7857  strlen
1    1.7857  vfprintf
1    1.7857  write

```

最初の列は、シンボルのサンプル数で、2番目のコラムは、実行可能なサンプルに対するこのシンボルのサンプルの割合で、3番目のコラムは記号名になります。

最大数のサンプルから最小（リバース順序）に出力を並べ替えるには、`-l` オプションとともに `-r` を使用します。

**-i <symbol-name>**

シンボル名に固有のサンプルデータを一覧表示します。たとえば、以下の出力では `opreport -i __gconv_transform_utf8_internal /lib/tls/libc- <version> .so` コマンドです。

```

samples %    symbol name
12   100.000  __gconv_transform_utf8_internal

```

最初の行は、シンボル/実行可能ファイルの組み合わせの概要です。

最初の列は、メモリーシンボルのサンプル数です。2列目は、シンボルのサンプルの合計数と相対的に、メモリーアドレスのサンプルの割合（パーセント）です。3列はシンボル名です。

**-d**

-i よりも多くの詳細を含むシンボルによるサンプルデータを一覧表示します。たとえば、以下の出力は、`opreport -i -d __gconv_transform_utf8_internal /lib/tls/libc- <version> .so` コマンドです。

```

vma  samples %    symbol name
00a98640 12   100.000  __gconv_transform_utf8_internal
00a98640 1     8.3333
00a9868c 2    16.6667
00a9869a 1     8.3333
00a986c1 1     8.3333
00a98720 1     8.3333
00a98749 1     8.3333
00a98753 1     8.3333
00a98789 1     8.3333
00a98864 1     8.3333
00a98869 1     8.3333
00a98b08 1     8.3333

```

データは -i オプションと同じですが、各シンボルで、使用される各仮想メモリーアドレスが表示されます。各仮想メモリーアドレスについて、シンボルのサンプル数と基準に対するサンプル数とパーセンテージが表示されます。

**-x <symbol-name>**

出力からシンボルのコンマ区切りリストを除外します。

セッション: &lt;name>

`/var/lib/oprofile/samples/` ディレクトリーに対するセッションまたはディレクトリーへの完全パスを指定します。

### 40.5.3. `opannotate`の使用

`opannotate` ツールは、特定の手順のサンプルをソースコードの対応する行と照合しようとします。生成されたファイルには、左側の行のサンプルが必要です。また、関数の合計サンプルを一覧表示する各関数の最初のコメントに配置します。

このユーティリティーを機能させるには、実行ファイルを GCC の `-g` オプションでコンパイルする必要があります。デフォルトでは、Red Hat Enterprise Linux パッケージは、このオプションでコンパイルされません。

`opannotate` の一般的な構文は以下のとおりです。

```
opannotate --search-dirs <src-dir> --source <executable>
```

ソースコードと分析対象の実行可能ファイルを含むディレクトリーを指定する必要があります。追加のコマンドラインオプションの一覧は、`man` ページの `opannotate` を参照してください。

### 40.6. `/DEV/OPROFILE/`について

`/dev/oprofile/` ディレクトリーには、OProfile のファイルシステムが含まれます。`cat` コマンドを使用して、このファイルシステムの仮想ファイルの値を表示します。たとえば、以下のコマンドは検出されたプロセッサ OProfile のタイプを表示します。

```
cat /dev/oprofile/cpu_type
```

カウンターごとにディレクトリーが `/dev/oprofile/` に存在する。たとえば、カウンターが 2 つある場合は、`/dev/oprofile/0/` ディレクトリーと `dev/oprofile/1/` ディレクトリーが存在します。

カウンターの各ディレクトリーには、以下のファイルが含まれます。



- **count:** サンプルの間隔
- **enabled:** 0 の場合、カウンターはオフになり、そのカウンターは収集されません。1 の場合は、カウンターがオンになり、サンプルが収集されます。
- **event:** 監視するイベント。
- **kernel:** 0 の場合は、プロセッサがカーネル空間にあるときにこのカウンターイベントのサンプルが収集されません。1 の場合は、プロセッサがカーネル空間にある場合でもサンプルが収集されます。
- **unit\_mask:** カウンターに対して有効なユニットマスクを定義します。
- **User:** 0 の場合は、プロセッサがユーザー空間にあるときにカウンターイベントのサンプルが収集されません。1 の場合は、プロセッサがユーザー空間にある場合でもサンプルが収集されます。

このファイルの値は、`cat` コマンドで取得できます。以下に例を示します。

```
cat /dev/oprofile/0/count
```

## 40.7. 使用例

OProfile は開発者がアプリケーションのパフォーマンスを分析するのに使用できますが、システム管理者がシステム分析を実行するのに使用することもできます。以下に例を示します。

- システムで使用されるアプリケーションとサービスを判別します。`opreport` を使用して、アプリケーションやサービスが使用するプロセッサ時間を判別できます。システムが複数のサービスに使用されていても、実行中である場合は、最もプロセッサ時間を消費するサービスを専用のシステムに移動できます。
- プロセッサの使用量の決定: `CPU_CLK_UNHALTED` イベントを監視して、一定期間におけるプロセッサの負荷を判断できます。このデータを使用して、追加のプロセッサが追加または高速のプロセッサがシステムパフォーマンスを向上させるかどうかを判断できます。

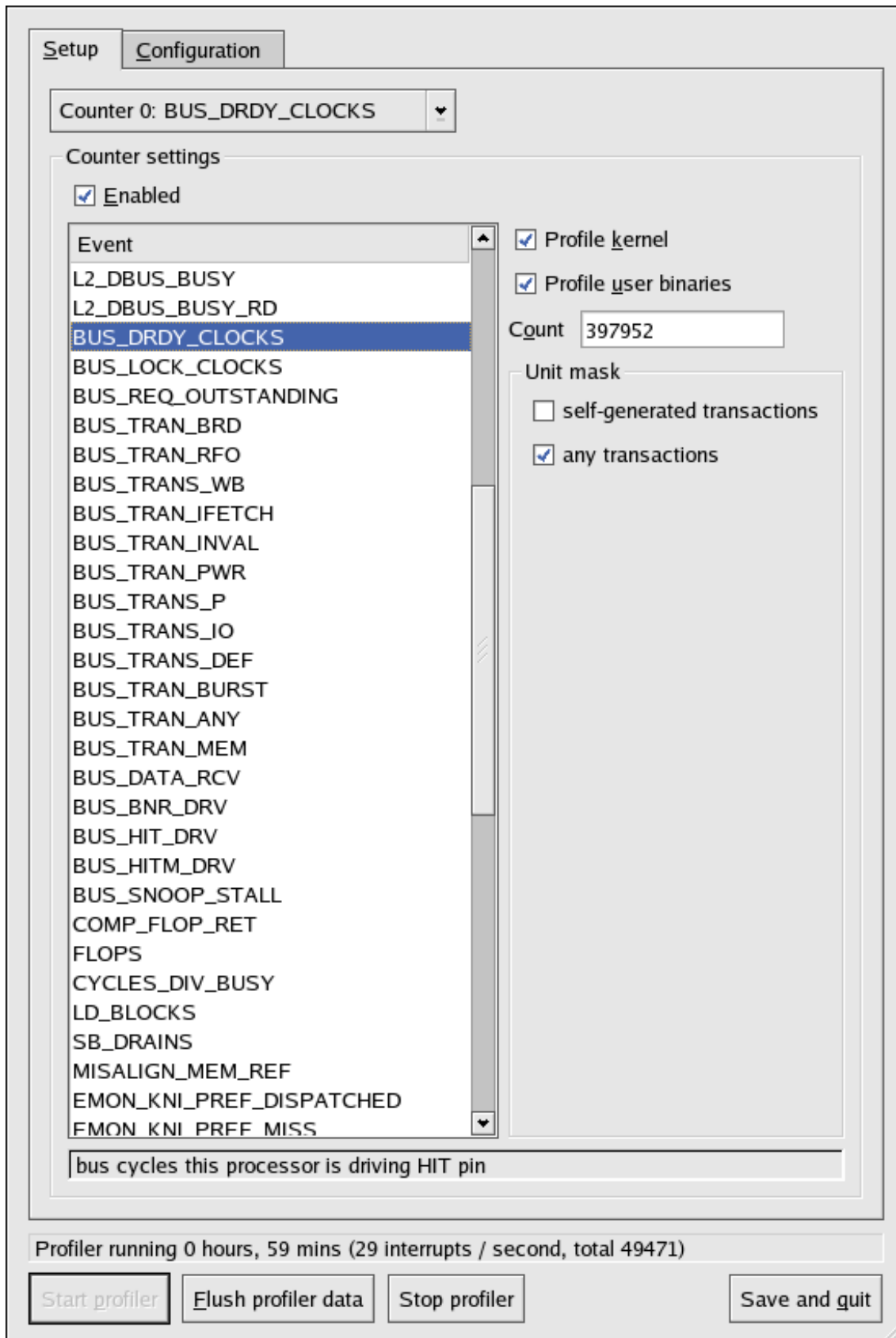
## 40.8. グラフィカルインターフェース

一部の OProfile 設定は、グラフィカルインターフェースで設定できます。これを起動するには、シェルプロンプトで root で `oprof_start` コマンドを実行します。

オプションのいずれかを変更したら、**Save and quit** ボタンをクリックして保存します。設定は `/root/.oprofile/daemonrc` に書き込まれ、アプリケーションが終了します。アプリケーションを終了しても OProfile がサンプリングから削除されません。

**Setup** タブでプロセッサカウンターのイベントを設定するには、**「監視するイベントの設定」** プルダウンメニューからカウンターを選択し、一覧からイベントを選択します。イベントの簡単な説明が、リストの下にあるテキストボックスに表示されます。特定のカウンターと特定のアーキテクチャーで利用可能なイベントのみが表示されます。また、このインターフェースは、プロファイラーが実行されているかどうかと、それに関する簡単な統計も表示します。

図40.1 OProfile のセットアップ



[D]

タブの右側にある **Profile kernel** オプションを選択して、現在選択されているイベントのカーネルモードでイベントをカウントします。「[カーネルとユーザー空間プロファイルの分離](#)」で説明されてい

るように、カーネルモードでイベントをカウントします。このオプションが選択されていない場合、カーネルのサンプルは収集されません。

「[カーネルとユーザー空間プロファイルの分離](#)」で説明されているように、**Profile user binaries** オプションを選択して、現在選択されているイベントのイベントをユーザーモードでカウントします。このオプションが選択されていない場合、ユーザーアプリケーションのサンプルは収集されません。

**Count** テキストフィールドを使用して、「[サンプリングレート](#)」で説明されているように、現在選択されているイベントのサンプリングレートを設定します。

「[ユニットマスク](#)」で説明されているように、現在選択されているイベントでユニットマスクが利用可能な場合は、**Setup** タブの右側の **Unit Masks** エリアに表示されます。ユニットマスクの横にあるチェックボックスを選択してイベントで有効にします。

設定 タブでカーネルのプロファイルを行うには、カーネル イメージ ファイルのテキストフィールドで監視するカーネルの **vmlinux** ファイルの名前と場所を入力します。**OProfile** がカーネルを監視しないように設定するには、**No kernel image** を選択します。

図40.2 OProfile の設定



[D]

**Verbose** オプションを選択すると、`oprofiled` デーモンログにより多くの情報が含まれます。

アプリケーション別のカーネルサンプルファイルが選択されている場合、OProfile は「[カーネルとユーザー空間プロファイルの分離](#)」で説明されているように、カーネルおよびカーネルモジュールのアプリケーションごとのプロファイルを生成します。これは `opcontrol --separate=kernel` コマンドと同じです。アプリケーション別の共有 `libs` サンプルファイルが選択されている場合、OProfile はライブ

ラリーのアプリケーションごとのプロファイルを生成します。これは `opcontrol --separate=library` コマンドと同じです。

「データの分析」で説明されているように、データがサンプルファイルに書き込まれるように強制するには、`Flush profiler data` ボタンをクリックします。これは `opcontrol --dump` コマンドと同じです。

グラフィカルインターフェースから OProfile を起動するには、`Start profiler` をクリックします。プロファイラーを停止するには、`Stop profiler` をクリックします。アプリケーションを終了しても OProfile がサンプリングから削除されません。

## 40.9. 関連情報

本章では、OProfile と設定、使用方法のみを取り上げています。詳細は、以下のリソースを参照してください。

### 40.9.1. Installed Docs

- `/usr/share/doc/oprofile- &lt;version> /oprofile.html` - 『OProfile Manual』
- OProfile man ページ : `opcontrol`、`opreport`、`opannotate`、および `op_help`

### 40.9.2. 便利な Web サイト

<http://oprofile.sourceforge.net/> - 最新のドキュメント、メーリングリスト、IRC チャンネルなどが含まれます。

パート VII. 付録

## 付録A 改訂履歴

改訂 1.0-1.33.402 Publican 4.0.0 用にリビルド	Fri Oct 25 2013	Rüdiger Landmann
改訂 1.0-1.33 Publican 3.0 の再ビルド	July 24 2012	Ruediger Landmann
改訂 1.0-1 新しい自動ビルドシステムに移行	Thu Sep 18 2008	Don Domingo

## 索引

## シンボル

[/dev/oprofile/, /dev/oprofile/について](#)

[/dev/shm, ファイルシステム](#)

[/etc/auto.master,](#)

[/etc/exports, NFS ファイルシステムのエクスポート](#)

[/etc/fstab, ext3 ファイルシステムへの変換, /etc/fstab を使用した NFS ファイルシステムのマウント](#)

[/etc/fstab ファイル](#)

[ディスククォータの有効化, クォータの有効化](#)

[/etc/hosts, ホストの管理](#)

[/etc/httpd/conf/httpd.conf, Apache HTTP サーバーの設定](#)

[/etc/sysconfig/dhcpd, サーバーの起動と停止](#)

[/proc/ ディレクトリー, インストールされているドキュメント](#)

[/var/spool/cron, cron タスクの設定](#)

[アクセス制御リスト \(参照 ACL\)](#)

## インストール

[kickstart \(参照 キックスタートインストール\)](#)

[LVM, LVM の設定](#)

[PXE \(参照 PXE インストール\)](#)

[ソフトウェア RAID, ソフトウェア RAID の設定](#)



インターネット接続 (参照 ネットワーク設定)

イーサネット接続 (参照 ネットワーク設定)

カーネルモジュール

`/etc/rc.modules`, 永続的なモジュールの読み込み

アンロード, カーネルモジュールユーティリティー

リスト, カーネルモジュールユーティリティー

ロード中, カーネルモジュールユーティリティー

永続的なロード, 永続的なモジュールの読み込み

カーネルモジュールの読み込み, カーネルモジュール

キックスタートインストール, キックスタートを使ったインストール

CD-ROM ベース, キックスタートブートメディアの作成

`diskette-based`, キックスタートブートメディアの作成

`flash-based`, キックスタートブートメディアの作成

LVM, キックスタートオプション

インストールツリー, インストールツリーを利用可能にする

ネットワークベース, ネットワーク上でキックスタートファイルの準備, インストールツリーを利用可能にする

ファイルの場所, キックスタートファイルの準備

ファイルフォーマット, キックスタートファイルの作成

起動, キックスタートインストールの開始

From CD-ROM #1 with a diskette, キックスタートインストールの開始

ブート CD-ROM から, キックスタートインストールの開始

キックスタートファイル

`%include`, キックスタートオプション

`%post`, インストール後のスクリプト

`%pre`, インストール前のスクリプト

`auth`, キックスタートオプション

`authconfig`, キックスタートオプション

`autopart`, キックスタートオプション

`autostep`, キックスタートオプション

`bootloader`, キックスタートオプション

CD-ROM ベース, キックスタートブートメディアの作成

`clearpart`, キックスタートオプション

**cmdline**, キックスタートオプション

**device**, キックスタートオプション

**diskette-based**, キックスタートブートメディアの作成

**driverdisk**, キックスタートオプション

**firewall**, キックスタートオプション

**firstboot**, キックスタートオプション

**flash-based**, キックスタートブートメディアの作成

**halt**, キックスタートオプション

**ignoredisk**, キックスタートオプション

**install**, キックスタートオプション

**interactive**, キックスタートオプション

**lang**, キックスタートオプション

**langsupport**, キックスタートオプション

**logvol**, キックスタートオプション

**mouse**, キックスタートオプション

**network**, キックスタートオプション

**options**, キックスタートオプション

パーティショニングの例, 高度なパーティション設定の例

**part**, キックスタートオプション

**poweroff**, キックスタートオプション

**raid**, キックスタートオプション

**reboot**, キックスタートオプション

**rootpw**, キックスタートオプション

**selinux**, キックスタートオプション

**shutdown**, キックスタートオプション

**skipx**, キックスタートオプション

**text**, キックスタートオプション

**timezone**, キックスタートオプション

**upgrade**, キックスタートオプション

**volgroup**, キックスタートオプション

**xconfig**, キックスタートオプション

**zerombr**, キックスタートオプション

インストール前の設定, インストール前のスクリプト

インストール後の設定, インストール後のスクリプト

インストール方法, キックスタートオプション

キーボード, キックスタートオプション

ネットワークベース, ネットワーク上でキックスタートファイルの準備, インストールツリーを利用可能にする

パッケージ選択の指定, パッケージの選択

パーティション, キックスタートオプション

フォーマット, キックスタートファイルの作成

作成, キックスタートオプション

例, キックスタートファイルの作成

別のファイルのコンテンツを含める, キックスタートオプション

キーボード, キーボードの設定

設定, キーボードの設定

キーボード設定ツール, キーボードの設定

グループ設定

グループのユーザーの変更, グループプロパティの変更

グループの追加, 新規グループの追加

グループプロパティの変更, グループプロパティの変更

グループ一覧のフィルタリング, ユーザーおよびグループの設定

グループ一覧の表示, ユーザーおよびグループの設定

コマンドラインオプション

印刷元, 印刷ジョブの管理

システムの復元, 基本的なシステムの復元

一般的な問題, 一般的な問題

Red Hat Enterprise Linux で起動できない, Red Hat Enterprise Linux で起動できない

root パスワードを取得する場合, root パスワード

ハードウェア/ソフトウェアの問題, ハードウェア/ソフトウェアの問題

ブートローダーの再インストール, ブートローダーの再インストール

システム分析

OProfile (参照 OProfile)

システム情報

gathering, システム情報の収集

**processes**, [システムプロセス](#)

[現在実行中の](#), [システムプロセス](#)

[ハードウェア](#), [ハードウェア](#)

[ファイルシステム](#), [ファイルシステム](#)

[/dev/shm](#), [ファイルシステム](#)

[メモリー使用量](#), [Memory Usage](#)

[シャドウパスワード](#), [認証](#)

[概要](#), [シャドウパスワード](#)

[シングルユーザーモード](#), [シングルユーザーモードで起動](#)

[ストライピング](#)

[RAID の基礎](#), [RAID とは](#)

[スワップ領域](#), [swap 領域](#)

[expanding](#), [スワップ領域の追加](#)

[file](#)

[作成](#), [スワップファイルの作成](#), [スワップファイルの削除](#)

[LVM2](#)

[作成](#), [スワップの LVM2 論理ボリュームの作成](#)

[削除中](#), [スワップの LVM2 論理ボリュームの削除](#)

[拡張](#), [LVM2 論理ボリュームでのスワップ領域の拡張](#)

[縮小](#), [LVM2 論理ボリュームでのスワップ領域の縮小](#)

[作成](#), [スワップ領域の追加](#)

[削除中](#), [スワップ領域の削除](#)

[推奨サイズ](#), [変動スペースとは](#)

[移動](#), [Swap 領域の移動](#)

[説明:](#), [変動スペースとは](#)

[セキュアなサーバー](#)

[certificate](#)

[authorities](#), [証明書の種類](#)

[CA の選択](#), [証明書の種類](#)

[アップグレード後の移動](#), [事前検証キーおよび証明書の使用](#)

[テスト](#), [証明書のテスト](#)

テスト vs 自己署名型, 証明書の種類

リクエストの作成, CA に送信する証明書要求の生成

既存の機能, 事前検証キーおよび証明書の使用

自己署名, 自己署名証明書の作成

installing, Apache HTTP セキュアサーバー設定

key

生成, キーの生成

security

説明:, 証明書およびセキュリティの概要

URL, サーバーへのアクセス

Web サイト, 便利な Web サイト

アクセス, サーバーへのアクセス

アップグレード元, 事前検証キーおよび証明書の使用

セキュリティの説明, 証明書およびセキュリティの概要

パッケージ, セキュリティ関連パッケージの概要

ポート番号, サーバーへのアクセス

接続先, サーバーへのアクセス

本, 関連書籍

証明書の指定, 証明書およびセキュリティの概要

セキュリティレベル (参照 Security Level Configuration Tool)

ソフトウェア RAID (参照 RAID)

タイムゾーンの設定, タイムゾーンの設定

ディスククォータ, ディスククォータの実装

グループごとに割り当て, グループごとのクォータ割り当て

ソフト制限, ユーザーごとのクォータ割り当て

ハード制限, ユーザーごとのクォータ割り当て

ファイルシステムごとの割り当て, ファイルシステムごとのクォータの割り当て

ユーザーごとに割り当て, ユーザーごとのクォータ割り当て

有効化, ディスククォータの設定, 有効化と無効化

/etc/fstab, 変更, クォータの有効化

quotacheck, 実行中, クォータデータベースファイルの作成

クォータファイルの作成, クォータデータベースファイルの作成

無効化, [有効化と無効化](#)

猶予期間, [ユーザーごとのクォータ割り当て](#)

管理, [ディスククォータの管理](#)

[quotacheck コマンド](#), [確認](#), [クォータの精度維持](#)

[レポート](#), [ディスククォータに関するレポート](#)

[関連情報](#), [関連情報](#)

[ディスクストレージ \(参照 ディスククォータ\)](#)

[parted \(参照 parted\)](#)

[ディスクレス環境](#), [ディスクレス環境](#)

[NFS の設定](#), [NFS サーバーの設定](#)

[ネットワーク起動ツール](#), [ディスクレス環境の設定の完了](#)

[ホストの追加](#), [ホストの追加](#)

[概要](#), [ディスクレス環境](#)

[デミライズされたゾーン](#), [DMZ および IPTables](#)

[トークンリング接続 \(参照 ネットワーク設定\)](#)

[ドキュメント](#)

[インストール済みの検索](#), [RPM で金を抑制する](#)

[ネットワークアドレス変換](#), [FORWARD および NAT ルール](#)

[iptablesの使用](#), [FORWARD および NAT ルール](#)

[ネットワークタイムプロトコル \(参照 NTP\)](#)

[ネットワークデバイスの制御](#), [プロファイルの使用](#)

[ネットワークファイルシステム \(参照 NFS\)](#)

[ネットワーク管理ツール \(参照 ネットワーク設定\)](#)

[ネットワーク設定](#)

[DHCP](#), [イーサネット接続の確立](#)

[DNS 設定の管理](#), [DNS 設定の管理](#)

[ISDN 接続](#), [ISDN 接続の確立](#)

[アクティベート中](#), [ISDN 接続の確立](#)

[managing /etc/hosts](#), [ホストの管理](#)

[PPoE 接続](#), [xDSL 接続の確立](#)

[xDSL 接続](#), [xDSL 接続の確立](#)

アクティベート中, [xDSL 接続の確立](#)

[イーサネット接続](#), [イーサネット接続の確立](#)

アクティベート中, [イーサネット接続の確立](#)

[デバイスのエイリアス](#), [デバイスエイリアス](#)

[トークンリング接続](#), [トークンリング接続の確立](#)

アクティベート中, [トークンリング接続の確立](#)

[ファイルからの復元](#), [ネットワーク設定の保存および復元](#)

[ファイルへの保存](#), [ネットワーク設定の保存および復元](#)

[プロファイル](#), [プロファイルの使用](#)

アクティベート中, [プロファイルの使用](#)

[ホストの管理](#), [ホストの管理](#)

[モデム接続](#), [モード接続の確立](#)

アクティベート中, [モード接続の確立](#)

[ワイヤレス接続](#), [ワイヤレス接続の確立](#)

アクティベート中, [ワイヤレス接続の確立](#)

[概要](#), [概要](#)

[論理ネットワークデバイス](#), [プロファイルの使用](#)

[静的 IP](#), [イーサネット接続の確立](#)

[ネットワーク起動ツール](#), [PXE ブート設定](#)

[PXE インストールでの使用](#), [PXE ブート設定](#)

[pxeboot](#), [コマンドラインからの設定](#)

[pxeos](#), [コマンドラインからの設定](#)

[ディスクレス環境の使用](#), [ディスクレス環境の設定の完了](#)

[ハードウェア](#)

表示する, [ハードウェア](#)

[ハードウェア RAID \(参照 RAID\)](#)

[ハードウェアブラウザー](#), [ハードウェア](#)

[パスワード](#)

[shadow](#), [シャドウパスワード](#)

[パッケージ](#)

**dependencies**, [解決できない依存関係](#)

**installing**, [インストール](#)

**RPM** でのリミネーション, [Freshening](#)

を使用したファイル所有権の決定, [RPM](#) で金を抑制する

[アップグレード](#), [アップグレード](#)

アンインストールされたクエリー, [RPM](#) で金を抑制する

[クエリー](#), [クエリ](#)

ドキュメントの検索, [RPM](#) で金を抑制する

[ヒント](#), [RPM](#) で金を抑制する

[ファイル一覧の取得](#), [RPM](#) で金を抑制する

[削除されたファイルの検索](#), [RPM](#) で金を抑制する

[削除中](#), [アンインストール](#)

[検証](#), [検証](#)

[設定ファイルの保存](#), [アップグレード](#)

## パーティション

[サイズ変更](#), [パーティションのサイズ変更](#)

[一覧表示](#), [パーティションテーブルの表示](#)

[作成](#), [パーティションの作成](#)

[mkpart](#), [パーティションの作成](#)

[削除中](#), [パーティションの削除](#)

## パーティションテーブル

[表示する](#), [パーティションテーブルの表示](#)

## ビデオカード

[X の設定](#), [ハードウェア設定の表示](#)

[デュアルヘッドの設定](#), [デュアルヒューリスティックディスプレイの設定](#)

## ピクセル, [表示設定](#)

[ファイアウォール](#), [ファイアウォール](#)

[iptables](#), [allInOnes](#) および [IPTables](#)

[policies](#), [基本的なファイアウォールポリシー](#)

[stateful](#), [iptables](#) および [接続の追跡](#)

[コネクションの追跡](#), [iptables](#) および [接続の追跡](#)

[タイプ](#), [ファイアウォール](#)



悪意のあるソフトウェア, 悪意のあるソフトウェアおよび Spoofed IP アドレス

関連情報, 関連情報

ファイアウォールの種類, ファイアウォール

proxy, ファイアウォール

ネットワークアドレス変換(NAT), ファイアウォール

パケットフィルター, ファイアウォール

ファイアウォールの設定 (参照 Security Level Configuration Tool)

ファイルシステム, ファイルシステム

ext2 (参照 ext2)

ext3 (参照 ext3)

LVM (参照 LVM)

NFS (参照 NFS)

フィードバック, フィードバックをお寄せください

ブートメディア, アップグレードの準備

プリンターの設定, プリンターの設定

CUPS, プリンターの設定

IPP プリンター, IPP プリンターの追加

JetDirect プリンター, JetDirect プリンターの追加

Networked CUPS(IPP)プリンター, IPP プリンターの追加

Samba(SMB)プリンター, Samba(SMB)プリンターの追加

コマンドラインからの印刷, 印刷ジョブの管理

テストページ, テストページの印刷

デフォルトのプリンター, 既存プリンターの修正

ローカルプリンター, ローカルプリンターの追加

印刷ジョブの管理, 印刷ジョブの管理

印刷ジョブをキャンセルする, 印刷ジョブの管理

印刷スプール, コマンドラインの表示, 印刷ジョブの管理

既存のプリンターの削除, 既存プリンターの修正

追加

cups(IPP)プリンター, IPP プリンターの追加

IPP プリンター, IPP プリンターの追加

JetDirect プリンター, JetDirect プリンターの追加

[Samba\(SMB\)プリンター](#), [Samba\(SMB\)プリンターの追加](#)

[ローカルプリンター](#), [ローカルプリンターの追加](#)

[プリンター設定ツール](#) (参照 [プリンターの設定](#))

[ボリュームグループ](#), [LVM とは](#), [LVM ボリュームグループの作成](#)

[マウントする](#)

,

[マスターブートレコード](#), [Red Hat Enterprise Linux で起動できない](#)

[再インストール](#), [ブートローダーの再インストール](#)

[メモリー使用量](#), [Memory Usage](#)

[メールユーザーエージェント](#), [メール転送エージェント \(MTA\) の設定](#)

[メール転送エージェント \(Mail Transport Agent\)](#) (参照 [MTA](#))

[メール転送エージェントスイッチ](#), [メール転送エージェント \(MTA\) の設定](#)

[テキストモードで起動](#), [メール転送エージェント \(MTA\) の設定](#)

[モデム接続](#) (参照 [ネットワーク設定](#))

[ユーザープライベートグループ](#) (参照 [groups](#))

[共有ディレクトリー](#), [グループディレクトリー](#)

[ユーザー設定](#)

[グループへのユーザーの追加](#), [ユーザープロパティーの変更](#)

[コマンドラインの設定](#), [コマンドラインからの設定](#)

[passwd](#), [ユーザーの追加](#)

[useradd](#), [ユーザーの追加](#)

[パスワードの変更](#), [ユーザープロパティーの変更](#)

[パスワードの有効期限](#), [ユーザープロパティーの変更](#)

[フルネームの変更](#), [ユーザープロパティーの変更](#)

[ホームディレクトリーの変更](#), [ユーザープロパティーの変更](#)

[ユーザーのグループの変更](#), [ユーザープロパティーの変更](#)

[ユーザーの変更](#), [ユーザープロパティーの変更](#)

[ユーザーの追加](#), [新規ユーザーの追加](#)

[ユーザーアカウントのロック](#), [ユーザープロパティーの変更](#)

[ユーザーアカウントの有効期限の設定](#), [ユーザープロパティーの変更](#)

[ユーザー一覧のフィルタリング](#), [ユーザーおよびグループの設定](#)

ユーザー一覧の表示, ユーザーおよびグループの設定

ログインシェルの変更, ユーザープロパティの変更

ランレベル 1, シングルユーザーモードで起動

レスキューモード

利用可能なユーティリティー, レスキューモードでの起動

定義, レスキューモードでの起動

ログビューアー

alerts, ログファイルの検証

フィルタリング, ログファイルの表示

ログファイルの場所, ログファイルの表示

更新レート, ログファイルの表示

検索, ログファイルの表示

ログファイル, ログファイル

(参照 ログビューアー)

description, ログファイル

rotating, ログファイルの場所の特定

syslogd, ログファイル

検索, ログファイルの場所の特定

検証, ログファイルの検証

表示する, ログファイルの表示

動的ホスト設定プロトコル(Du Dynamic Host Configuration Protocol) (参照 DHCP)

実行環境, PXE ネットワークインストーラ

情報

システムについて, システム情報の収集

日付の設定, 日付と時刻のプロパティ

時間設定, 日付と時刻のプロパティ

NTP サーバーとの同期, Network Time Protocol(NTP)プロパティ

概要, はじめに

物理エクステンツ, LVM ボリュームグループの作成

物理ボリューム, LVM とは, LVM 物理ボリュームの作成

緊急モード, 緊急モードでのブート

自動タスク, [自動タスク](#)

色深度, [表示設定](#)

解決方法, [表示設定](#)

設定

`console access`, [コンソールアクセス](#)

`NFS`, [Network File System \(NFS\)](#)

論理ボリューム, [LVM とは](#), [LVM 論理ボリュームの作成](#)

論理ボリュームグループ, [LVM とは](#)

論理ボリュームマネージャー (参照 [LVM](#))

起動

シングルユーザーモード, [シングルユーザーモードで起動](#)

レスキューモード, [レスキューモードでの起動](#)

緊急モード, [緊急モードでのブート](#)

起動パーティション, [/boot/ パーティションの作成](#)

追加

`group`,

`user`, [コマンドラインからの設定](#)

, , , ,

`groupadd`,

`password`

,

生成, , ,

[関連情報](#), [関連情報](#)

A

ACL

`ext3` ファイルシステム上, [アクセス制御リスト](#)

`getfacl`, [ACL の取り込み](#)

`NFS` 共有のマウント:, [NFS](#)

`setfacl`, [アクセス ACL の設定](#)

with Samba, [アクセス制御リスト](#)

[アクセス ACL](#), [アクセス ACL の設定](#)

[アーカイブ](#); [ACL が設定されているファイルシステムのアーカイブ作成](#)

[デフォルト ACL](#), [デフォルト ACL の設定](#)

[ファイルシステムのマウント](#); [ファイルシステムのマウント](#)

[取得](#), [ACL の取り込み](#)

[設定](#)

[アクセス ACL](#), [アクセス ACL の設定](#)

[関連情報](#), [関連情報](#)

**Apache HTTP サーバー (参照 [HTTP 設定ツール](#))**

[保護](#), [証明書およびセキュリティーの概要](#)

[関連情報](#), [関連情報](#)

[関連書籍](#), [関連書籍](#)

**APXS, [セキュリティー関連パッケージの概要](#)**

**at, [at](#) および [Batch](#)**

[関連資料](#), [関連情報](#)

**authconfig (参照 [Authentication Configuration Tool](#))**

**authentication, [認証設定](#)**

**Authentication Configuration Tool, [認証設定](#)**

**authentication, [認証](#)**

[Kerberos サポート](#), [認証](#)

[LDAP サポート](#), [認証](#)

[MD5 パスワード](#), [認証](#)

[SMB サポート](#), [認証](#)

[Winbind](#), [認証](#)

[シャドウパスワード](#), [認証](#)

**コマンドラインのバージョン, [コマンドラインのバージョン](#)**

**ユーザー情報, [ユーザー情報](#)**

[cache](#), [ユーザー情報](#)

[hesiod](#), [ユーザー情報](#)

[LDAP](#), [ユーザー情報](#)

[NIS](#), [ユーザー情報](#)

## Winbind, [ユーザー情報](#)

**autofs,**

[/etc/auto.master,](#)

## B

**batch, at および Batch**

[関連情報,](#) [関連情報](#)

## C

**CA (参照 [セキュアなサーバー](#))**

**chkconfig, [chkconfig](#)**

**console**

[ファイルへのアクセス権限,](#) [コンソールからのファイルへのアクセス許可](#)

**console access**

[定義,](#) [コンソールの定義](#)

[有効化,](#) [他のアプリケーションのコンソールアクセスの有効化](#)

[無効化,](#) [コンソールプログラムアクセスの無効化](#)

[設定,](#) [コンソールアクセス](#)

**Cron, [自動タスク](#)**

**cron**

[crontab の例,](#) [cron タスクの設定](#)

[ユーザー定義のタスク,](#) [cron タスクの設定](#)

[設定ファイル,](#) [cron タスクの設定](#)

[関連資料,](#) [関連情報](#)

**crontab, [cron タスクの設定](#)**

**CtrlAltDel**

[shutdown,](#) [disabling,](#) [Shutdown Via Ctrl+Alt+Delの無効化](#)

**CUPS, [プリンターの設定](#)**

## D

**dateconfig (参照 [日付と時刻のプロパティーツール](#))**

**devel パッケージ, [セキュリティ関連パッケージの概要](#)**

**df**, [ファイルシステム](#)

**DHCP**, [Dynamic Host Configuration Protocol\(DHCP\)](#)

[dhcpd.conf](#), [設定ファイル](#)

[dhcpd.leases](#), [サーバーの起動と停止](#)

[dhcrelay](#), [DHCP リレーエージェント](#)

[group](#), [設定ファイル](#)

[options](#), [設定ファイル](#)

[shared-network](#), [設定ファイル](#)

[subnet](#), [設定ファイル](#)

[クライアント設定](#), [DHCP クライアントの設定](#)

[グローバルパラメーター](#), [設定ファイル](#)

[コマンドラインオプション](#), [サーバーの起動と停止](#)

[サーバーの停止](#), [サーバーの起動と停止](#)

[サーバーの起動](#), [サーバーの起動と停止](#)

[サーバー設定](#), [DHCP サーバーの設定](#)

[リレーエージェント](#), [DHCP リレーエージェント](#)

[使用する理由](#), [DHCP を使用する理由](#)

[接続先](#), [DHCP クライアントの設定](#)

[関連情報](#), [関連情報](#)

[dhcpd.conf](#), [設定ファイル](#)

[dhcpd.leases](#), [サーバーの起動と停止](#)

[dhcrelay](#), [DHCP リレーエージェント](#)

[display](#)

[X の設定](#), [表示設定](#)

[DMZ](#) ([参照](#) [デミライズされたゾーン](#))

[DSOs](#)

[ロード中](#), [セキュリティ関連パッケージの概要](#)

**du**, [ファイルシステム](#)

**E**

[e2fsck](#), [ext2 ファイルシステムに戻す](#)

[e2label](#), [パーティションのラベル付け](#)

[exim](#), [メール転送エージェント \(MTA\) の設定](#)

**exports**, [NFS ファイルシステムのエクスポート](#)

**ext2**

[ext3 からの復元](#), [ext2 ファイルシステムに戻す](#)

**ext2online**, [ext2 ファイルシステムに戻す](#)

**ext3**

[ext2 からの変換](#), [ext3 ファイルシステムへの変換](#)

**features**, [ext3 の機能](#)

[作成](#), [Ext3 ファイルシステムの作成](#)

**ext3 ファイルシステム**

[サイズ変更](#), [ext2 ファイルシステムに戻す](#)

**F**

**findsmb**, [コマンドライン](#)

**floppy グループ** (以下を使用) , [フロッピー グループ](#)

**free**, [Memory Usage](#)

**ftp**,

**G**

**getfacl**, [ACL の取り込み](#)

**GNOME システムモニター**, [システムプロセス](#)

**gnome-system-monitor**, [システムプロセス](#)

**GnuPG**

[RPM パッケージ署名の確認](#), [パッケージの署名の確認](#)

**groups** (参照 [グループ設定](#))

[floppy \(使用\)](#) , [フロッピー グループ](#)

**GID**, [ユーザーとグループ](#)

**standard**,

[ユーザープライベート](#), [ユーザープライベートグループ](#)

[共有ディレクトリー](#), [グループディレクトリー](#)

[概要](#), [ユーザーとグループ](#)

**管理するツール**

[groupadd](#), [ユーザーおよびグループ管理ツール](#), [ユーザープライベートグループ](#)

[system-config-users](#), [ユーザープライベートグループ](#)



**User Manager**, [ユーザーおよびグループ管理ツール](#)

[関連資料](#), [関連情報](#)

[インストールされているドキュメント](#), [インストールされているドキュメント](#)

## H

**hesiod**, [ユーザー情報](#)

**HTTP ディレクティブ**

**DirectoryIndex**, [サイトの設定](#)

**ErrorDocument**, [サイトの設定](#)

**ErrorLog**, [ロギング](#)

**Group**, [サーバー設定](#)

**HostnameLookups**, [ロギング](#)

**KeepAlive**, [パフォーマンスチューニング](#)

**KeepAliveTimeout**, [パフォーマンスチューニング](#)

**listen**, [基本設定](#)

**LogFormat**, [ロギング](#)

**LogLevel**, [ロギング](#)

**MaxClients**, [パフォーマンスチューニング](#)

**MaxKeepAliveRequests**, [パフォーマンスチューニング](#)

**ServerAdmin**, [基本設定](#)

**ServerName**, [基本設定](#)

**TimeOut**, [パフォーマンスチューニング](#)

**TransferLog**, [ロギング](#)

**User**, [サーバー設定](#)

**オプション**, [サイトの設定](#)

**HTTP 設定ツール**

**modules**, [Apache HTTP サーバーの設定](#)

**エラーログ**, [ロギング](#)

**ディレクティブ** (参照 [HTTP ディレクティブ](#))

**転送ログ**, [ロギング](#)

**httpd**, [Apache HTTP サーバーの設定](#)

**hwbrowser**, [ハードウェア](#)

## I

[insmod](#), [カーネルモジュールユーティリティー](#)

[ip6tables](#), [IPv6](#)

[iptables](#), [allInOnes](#) および [IPTables](#), [IPTables](#) サービスのアクティブ化

[policies](#), [基本的なファイアウォールポリシー](#)

[rules](#), [IPTables](#) ルールの保存および復元

[common](#), [一般的な IPTables フィルタリング](#)

[NAT](#), [POSTROUTING and IP Masquerading](#), [DMZ](#) および [IPTables](#)

[保存中](#), [IPTables](#) ルールの保存および復元

[復元](#), [IPTables](#) ルールの保存および復元

[転送](#), [FORWARD](#) および [NAT](#) ルール

および [DMZ](#), [DMZ](#) および [IPTables](#)

[コネクションの追跡](#), [iptables](#) および [接続の追跡](#)

[状態](#), [iptables](#) および [接続の追跡](#)

[ステートフル検査](#), [iptables](#) および [接続の追跡](#)

[状態](#), [iptables](#) および [接続の追跡](#)

[チェーン](#), [iptables](#) コマンド構文

[FORWARD](#), [FORWARD](#) および [NAT](#) ルール

[INPUT](#), [一般的な IPTables フィルタリング](#)

[OUTPUT](#), [一般的な IPTables フィルタリング](#)

[POSTROUTING](#), [POSTROUTING and IP Masquerading](#)

[PREROUTING](#), [PREROUTING](#), [DMZ](#) および [IPTables](#)

[使用](#), [IPTables](#) の使用

[悪意のあるソフトウェア](#), [悪意のあるソフトウェア](#) および [Spoofed IP](#) アドレス

[関連情報](#), [関連情報](#)

[ISDN 接続](#) (参照 [ネットワーク設定](#))

## K

[Kerberos](#), [認証](#)

[kernel](#)

[modules](#), [カーネルモジュール](#)

[アップグレード](#), [カーネルの手動によるアップグレード](#)

ダウンロード中, [アップグレードされたカーネルのダウンロード](#)

大規模なメモリのサポート, [カーネルパッケージの概要](#)

複数のプロセッサのサポート, [カーネルパッケージの概要](#)

## kickstart

[ファイルの表示方法](#), [キックスタートインストールの開始](#)

## Kickstart Configurator, [Kickstart Configurator](#)

[%post スクリプト](#), [インストール後のスクリプト](#)

[%pre スクリプト](#), [インストール前のスクリプト](#)

[interactive](#), [基本設定](#)

[mouse](#), [基本設定](#)

[preview](#), [Kickstart Configurator](#)

[reboot](#), [基本設定](#)

[root パスワード](#), [基本設定](#)

[encrypt](#), [基本設定](#)

[SELinux の設定](#), [SELinux の設定](#)

[インストール方法の選択](#), [インストール方法](#)

[キーボード](#), [基本設定](#)

[タイムゾーン](#), [基本設定](#)

[テキストモードのインストール](#), [基本設定](#)

[ネットワーク設定](#), [Network Configuration](#)

[パッケージの選択](#), [パッケージの選択](#)

[パーティション設定](#), [パーティション情報](#)

[ソフトウェア RAID](#), [ソフトウェア RAID パーティションの作成](#)

[ファイアウォールの設定](#), [ファイアウォールの設定](#)

[ブートローダー](#), [ブートローダーのオプション](#)

[ブートローダーのオプション](#), [ブートローダーのオプション](#)

保存中, [ファイルの保存](#)

[基本オプション](#), [基本設定](#)

[言語](#), [基本設定](#)

[言語サポート](#), [基本設定](#)

[設定の表示](#), [設定の表示](#)

[認証オプション](#), [認証](#)

## L

[LDAP, ユーザー情報, 認証](#)

[logrotate, ログファイルの場所の特定](#)

[lpd, プリンターの設定](#)

[lsmod, カーネルモジュールユーティリティー](#)

[lspci, ハードウェア](#)

[LVM, 論理ボリュームマネージャー \(LVM\)](#)

### installing

[ブートパーティションの作成, /boot/ パーティションの作成](#)

[ボリュームグループの作成, LVM ボリュームグループの作成](#)

[物理ボリュームの作成, LVM 物理ボリュームの作成](#)

[自動パーティション設定, 自動パーティション設定, 手動での LVM パーティション設定](#)

[論理ボリュームの作成, LVM 論理ボリュームの作成](#)

[インストール時の LVM の設定, LVM の設定](#)

[キックスタートの使用, キックスタートオプション](#)

[ボリュームグループ, LVM ボリュームグループの作成](#)

[物理エクステンツ, LVM ボリュームグループの作成](#)

[物理ボリューム, LVM とは, LVM 物理ボリュームの作成](#)

[説明:, LVM とは](#)

[論理ボリューム, LVM とは, LVM 論理ボリュームの作成](#)

[論理ボリュームグループ, LVM とは](#)

[関連資料, 関連情報](#)

### lvm

[LVM ツールおよびユーティリティー, LVM パーティション管理](#)

### LVM2

[説明:, LVM2 とは](#)

## M

[MD5 パスワード, 認証](#)

[mkfs, パーティションのフォーマット](#)

[mkpart, パーティションの作成](#)

[modprobe, カーネルモジュールユーティリティー](#)

**modprobe.conf**, [カーネルモジュール](#)

**monitor**

[X の設定](#), [ハードウェア設定の表示](#)

[デュアルヘッドの設定](#), [デュアルヒューリスティックディスプレイの設定](#)

**MTA**

[デフォルトの設定](#), [メール転送エージェント \(MTA\) の設定](#)

[メール転送エージェントスイッチスイッチによる切り替え](#), [メール転送エージェント \(MTA\) の設定](#)

**MUA**, [メール転送エージェント \(MTA\) の設定](#)

**N**

**NAT** ([参照 ネットワークアドレス変換](#))

**neat** ([参照 ネットワーク設定](#))

**NFS**

,

[/etc/fstab](#), [/etc/fstab](#) を使用した **NFS** ファイルシステムのマウント

**autofs** ([参照 autofs](#))

[エクスポート](#), [NFS ファイルシステムのエクスポート](#)

[コマンドラインの設定](#), [コマンドラインからの設定](#)

[サーバーのステータス](#), [サーバーの起動と停止](#)

[サーバーの停止](#), [サーバーの起動と停止](#)

[サーバーの起動](#), [サーバーの起動と停止](#)

[ディスクレス環境](#), [設定](#), [NFS サーバーの設定](#)

[ホスト名の形式](#), [ホスト名の形式](#)

[マウントする](#),

[設定](#), [Network File System \(NFS\)](#)

[関連情報](#), [関連情報](#)

**NFS** サーバー設定ツール, [NFS ファイルシステムのエクスポート](#)

**NFS** ファイルシステムのエクスポート, [NFS ファイルシステムのエクスポート](#)

**NIS**, [ユーザー情報](#)

**NTP**

[ntpd](#), [Network Time Protocol\(NTP\)プロパティー](#)

[設定](#), [Network Time Protocol\(NTP\)プロパティー](#)

**ntpd**, [Network Time Protocol\(NTP\)プロパティ](#)ー

**ntsysv**, [ntsysv](#)

O

**O'Reilly & Associates, Inc.**, [関連書籍](#)

**O'Reilly & Associates, Inc.**, [関連書籍](#)

**opannotate** ([参照 OProfile](#))

**opcontrol** ([参照 OProfile](#))

**OpenLDAP**, [ユーザー情報](#), [認証](#)

**openldap-clients**, [ユーザー情報](#)

**OpenSSH**, [OpenSSH](#)

**client**,

[scp](#),

[sftp](#),

[ssh](#),

**server**,

[/etc/ssh/sshd\\_config](#),

**ssh-add**,

**ssh-agent**,

, ,

**ssh-keygen**

,

[DSA](#),

[RSA](#),

[関連資料](#), [関連情報](#)

**OpenSSL**

[関連情報](#), [関連情報](#)

**opreport** ([参照 OProfile](#))

**OProfile**, [OProfile](#)

[/dev/oprofile/](#), [/dev/oprofile/](#)について

**events**

[サンプリングレート](#), [サンプリングレート](#)

設定, [監視するイベントの設定](#)

[opannotate](#), [opannotateの使用](#)

[opcontrol](#), [OProfile の設定](#)

[--no-vmlinux](#), [カーネルの指定](#)

[--start](#), [OProfile の起動および停止](#)

[--vmlinux=](#), [カーネルの指定](#)

[opreport](#), [opreportの使用](#)

1 つの実行可能ファイルで, [単一の実行可能ファイルでの opreport の使用](#)

[oprofiled](#), [OProfile の起動および停止](#)

[ログファイル](#), [OProfile の起動および停止](#)

[op\\_help](#), [監視するイベントの設定](#)

[カーネルの監視](#), [カーネルの指定](#)

[ツールの概要](#), [ツールの概要](#)

[データの保存](#), [データの保存](#)

[データの読み取り](#), [データの分析](#)

[ユニットマスク](#), [ユニットマスク](#)

設定, [OProfile の設定](#)

[プロファイルの分離](#), [カーネルとユーザー空間プロファイルの分離](#)

起動, [OProfile の起動および停止](#)

[関連資料](#), [関連情報](#)

[oprofiled](#) ([参照 OProfile](#))

[oprof\\_start](#), [グラフィカルインターフェース](#)

[op\\_help](#), [監視するイベントの設定](#)

## P

[Package Updater](#), [Red Hat Network](#)

[pam\\_smbpass](#), [暗号化パスワード](#)

[pam\\_timestamp](#), [他のアプリケーションのコンソールアクセスの有効化](#)

[parted](#), [partedで標準パーティション](#)

[コマンドの表](#), [partedで標準パーティション](#)

[デバイスの選択](#), [パーティションテーブルの表示](#)

[パーティションのサイズ変更](#), [パーティションのサイズ変更](#)

[パーティションの削除](#), [パーティションの削除](#)

[パーティションを作成する](#), [パーティションの作成](#)

[パーティションテーブルの表示](#), [パーティションテーブルの表示](#)

[概要](#), [partedで標準パーティション](#)

## **partitions**

[フォーマット](#)

[mkfs](#), [パーティションのフォーマット](#)

[ラベル付け](#)

[e2label](#), [パーティションのラベル付け](#)

## **password**

,

## **PCI デバイス**

[リスト](#), [ハードウェア](#)

[pidgin](#), [allInOnes](#) および [IPTables](#)

[pidgin 6](#), [IPv6](#)

[postfix](#), [メール転送エージェント \(MTA\) の設定](#)

[PPPoE](#), [xDSL 接続の確立](#)

[printconf](#) (参照 [プリンターの設定](#))

[printtool](#) (参照 [プリンターの設定](#))

[processes](#), [システムプロセス](#)

[ps](#), [システムプロセス](#)

[PXE](#), [PXE ネットワークインストール](#)

[PXE インストール](#), [PXE ネットワークインストール](#)

[ネットワークサーバーの設定](#), [ネットワークサーバーの設定](#)

[ネットワーク起動ツール](#), [PXE ブート設定](#)

[ブートメッセージ](#), [カスタム](#), [カスタムブートメッセージの追加](#)

[ホストの追加](#), [PXE ホストの追加](#)

[実行中](#), [PXE インストールの実行](#)

[概要](#), [PXE ネットワークインストール](#)

[設定](#), [PXE ブート設定](#)

[pxeboot](#), [コマンドラインからの設定](#)



[pxeos](#), コマンドラインからの設定

## Q

[quotacheck](#), クォータデータベースファイルの作成

[quotacheck](#) コマンド

によるクォータ正確性の確認, クォータの精度維持

[quotaoff](#), 有効化と無効化

[quotaon](#), 有効化と無効化

## R

[RAID](#), [RAID \(Redundant Array of Independent Disks\)](#)

[installing](#)

[RAID デバイスの作成](#), [RAID デバイスとマウントポイントの作成](#)

[RAID パーティションの作成](#), [RAID パーティションの作成](#)

[ブートパーティションの作成](#), [RAID パーティションの作成](#)

[マウントポイントの作成](#), [RAID デバイスとマウントポイントの作成](#)

[インストール時のソフトウェア RAID の設定](#), [ソフトウェア RAID の設定](#)

[ソフトウェア RAID](#), [ハードウェア RAID とソフトウェア RAID の比較](#)

[ハードウェア RAID](#), [ハードウェア RAID とソフトウェア RAID の比較](#)

[レベル](#), [RAID レベルとリニアサポート](#)

[レベル 0](#), [RAID レベルとリニアサポート](#)

[レベル 1](#), [RAID レベルとリニアサポート](#)

[レベル 4](#), [RAID レベルとリニアサポート](#)

[レベル 5](#), [RAID レベルとリニアサポート](#)

[使用理由](#), [RAID を使用するユーザー](#)

[説明](#):, [RAID とは](#)

[RAM](#), [Memory Usage](#)

[rcp](#),

[Red Hat Network](#), [Red Hat Network](#)

[Red Hat Package Manager](#) (参照 [RPM](#))

[Red Hat RPM ガイド](#), [関連書籍](#)

[resize2fs](#), [ext2 ファイルシステムに戻す](#)

[RHN](#) (参照 [Red Hat Network](#))

**rmmod**, [カーネルモジュールユーティリティ](#)

**RPM**, [RPM](#) でのパッケージ管理

**dependencies**, [解決できない依存関係](#)

**freshen**, [Freshening](#)

**GnuPG**, [パッケージの署名の確認](#)

**installing**, [インストール](#)

**md5sum**, [パッケージの署名の確認](#)

**website**, [便利な Web サイト](#)

[で削除されたファイルの検索](#), [RPM](#) で金を抑制する

[を使用したファイル所有権の決定](#), [RPM](#) で金を抑制する

[アップグレード](#), [アップグレード](#)

[アンインストール](#), [アンインストール](#)

[アンインストールされたパッケージのクエリー](#), [RPM](#) で金を抑制する

[クエリー](#), [クエリ](#)

[パッケージの新規化](#), [Freshening](#)

[パッケージ署名の確認](#), [パッケージの署名の確認](#)

[ヒント](#), [RPM](#) で金を抑制する

[ファイルの競合](#)

**resolving**, [競合するファイル](#)

[ファイル一覧のクエリー](#), [RPM](#) で金を抑制する

[使用](#), [RPM](#) の使用

[本ガイド](#), [関連書籍](#)

[検証](#), [検証](#)

[設定ファイルの保存](#), [アップグレード](#)

[設計ゴール](#), [RPM](#) 設計ゴール

[関連ドキュメント](#), [RPM](#) で金を抑制する

[関連資料](#), [関連情報](#)

## S

**Samba**, [Samba](#)

**findsmb**, [コマンドライン](#)

**pam\_smbpass**, [暗号化パスワード](#)

**share**

[nautilus](#) を使用した接続, [Samba 共有への接続](#)

コマンドラインでの接続, [コマンドライン](#)

マウントする, [共有のマウント](#)

[smbclient](#), [コマンドライン](#)

Windows NT 4.0、2000、ME、および XP を使用する場合, [暗号化パスワード](#)

アクティブな接続の一覧, [サーバーの起動と停止](#)

グラフィカル設定, [グラフィカル設定](#)

[Samba ユーザーの管理](#), [Samba ユーザーの管理](#)

[サーバー設定の構成](#), [サーバーの設定](#)

[共有の追加](#), [共有の追加](#)

[サーバーのステータス](#), [サーバーの起動と停止](#)

[サーバーの停止](#), [サーバーの起動と停止](#)

[サーバーの起動](#), [サーバーの起動と停止](#)

[パスワードとパスワードの同期](#), [暗号化パスワード](#)

[使用する理由](#), [Samba を使用する理由](#)

[暗号化されたパスワード](#), [暗号化パスワード](#)

[設定](#), [Samba サーバーの設定](#), [コマンドラインからの設定](#)

[default](#), [Samba サーバーの設定](#)

[smb.conf](#), [Samba](#)

[関連情報](#), [関連情報](#)

[scp](#) (参照 [OpenSSH](#))

[security](#),

[Security Level Configuration Tool](#)

[iptables サービス](#), [IPTables サービスのアクティブ化](#)

[カスタムポートの設定](#), [他のポート](#)

[保存中](#), [設定の保存](#)

[信頼できるサービス](#), [信頼できるサービス](#)

[有効化および無効化](#), [ファイアウォールの有効化および無効化](#)

[sendmail](#), [メール転送エージェント \(MTA\) の設定](#)

[services](#)

,

[setfacl](#), [アクセス ACL の設定](#)

**Setup Agent**

[キックスタート経由](#), [キックスタートオプション](#)

**sftp** ([参照 OpenSSH](#))

**shutdown**

[CtrlAltDelの無効化](#), [Shutdown Via Ctrl+Alt+Delの無効化](#)

**SMB**, [Samba](#), [認証](#)

**smb.conf**, [Samba](#)

**smbclient**, [コマンドライン](#)

**smbstatus**, [サーバーの起動と停止](#)

**ssh** ([参照 OpenSSH](#))

**ssh-add**,

**ssh-agent**,

’ ’

**star**, [ACL が設定されているファイルシステムのアーカイブ作成](#)

**syslogd**, [ログファイル](#)

**system-config-authentication** ([参照 Authentication Configuration Tool](#))

**system-config-date** ([参照 日付と時刻のプロパティーツール](#))

**system-config-display** ([参照 X 設定ツール](#))

**system-config-httpd** ([参照 HTTP 設定ツール](#))

**system-config-keyboard**, [キーボードの設定](#)

**system-config-kickstart** ([参照 Kickstart Configurator](#))

**system-config-mouse** ([参照 mouse Configuration Tool](#))

**system-config-netboot**, [PXE ブート設定](#)

**system-config-network** ([参照 ネットワーク設定](#))

**system-config-network-cmd**, [Network Configuration](#), [プロファイルの使用](#), [ネットワーク設定の保存および復元](#)

**system-config-printer** ([参照 プリンターの設定](#))

**system-config-selinux** ([参照 Security Level Configuration Tool](#))

**system-config-time** ([参照 日付と時刻のプロパティーツール](#))

**system-config-users** ([参照 ユーザー設定およびグループの設定](#))

**system-logviewer** ([参照 ログビューアー](#))

**system-switch-mail** ([参照 メール転送エージェントスイッチ](#))

**system-switch-mail-nox** (参照 [メール転送エージェントスイッチ](#))

## T

**telinit**,

**telnet**,

**fttp**, [PXE ネットワークインストール](#)

**timetool** (参照 [日付と時刻のプロパティーツール](#))

**top**, [システムプロセス](#)

**tune2fs**

[ext2 への復元](#), [ext2 ファイルシステムに戻す](#)

[ext3 への変換](#), [ext3 ファイルシステムへの変換](#)

## U

**User Manager** (参照 [ユーザー設定](#))

**useradd** コマンド

[を使用したユーザーアカウントの作成](#), [コマンドラインからの設定](#)

**users** (参照 [ユーザー設定](#))

[/etc/passwd](#),

[standard](#),

[UID, ユーザーとグループ](#)

[概要, ユーザーとグループ](#)

[管理するツール](#)

[User Manager, ユーザーおよびグループ管理ツール](#)

[useradd, ユーザーおよびグループ管理ツール](#)

[関連情報, 関連情報](#)

[関連資料](#)

[インストールされているドキュメント](#), [インストールされているドキュメント](#)

## V

**VeriSign**

[既存の証明書の使用](#), [事前検証キーおよび証明書の使用](#)

## W

## Windows

ファイルと印刷の共有, [Samba](#)

## Windows 2000

[Samba](#) を使用した共有への接続, [暗号化パスワード](#)

## Windows 98

[Samba](#) を使用した共有への接続, [暗号化パスワード](#)

## Windows ME

[Samba](#) を使用した共有への接続, [暗号化パスワード](#)

## Windows NT 4.0

[Samba](#) を使用した共有への接続, [暗号化パスワード](#)

## Windows XP

[Samba](#) を使用した共有への接続, [暗号化パスワード](#)

## X

### X Window System

設定, [X Window System の設定](#)

### X 設定ツール

[デュアルヘッド表示の設定](#), [デュアルヒューリスティックディスプレイの設定](#)

[ハードウェア設定](#), [ハードウェア設定の表示](#)

[設定の表示](#), [表示設定](#)

[xDSL 接続 \(参照 ネットワーク設定\)](#)

[xinetd](#), [xinetd](#)

## Y

[ypbind](#), [ユーザー情報](#)