7. Linux のシステム管理に関する知識 I

1. 科目の概要

Linux のシステム管理に関する基本的な手順を解説する。システム管理者の役割を示し、システムのインストールから各種サービスの設定、システムの起動・停止とシステムの運用など、実際に Linux システムを運用するために必要なノウハウを具体的に説明する。

2. 習得ポイント

本科目の学習により習得することが期待されるポイントは以下の通り。

習得ポイント	説　明	シラバスの対応コマ
I-7-1. システム管理者の役割と管理業務	システム管理業務の概要と、目的、必要性、システム管理作業の種類と内容などについて解説する。またシステム管理者の役割と管理者権限について説明し、システム管理者として心がけるべき事項についても言及する。	1,2
I-7-2. Linuxシステムのインストール	Linuxのインストール作業について解説する。インストールの具体的な手順を示し、各種項目の設定方法やアプリケーションパッケージの導入方法、パッケージ管理、インストール作業を行う際に気をつけることなどについて説明する。	3
I-7-3. Linuxシステムの起動と停止	Linuxシステムの起動と終了の手順、起動時および終了時の動作内容を説明する。またサービスの起動と停止の基本について述べ、提供するサービスの選択方法やサービスの起動停止を設定する各種のツールについて解説を加える。	2,3
I-7-4. 各種サービスの設定方法	Linuxシステムが提供する各種のサービスについて、多くのサービスでは /etc 以下に設定ファイルが集められていることを示し、さらに代表的なサービスの設定方法や設定ツールについて解説する。	2
I-7-5. ファイルシステムとディスクの管理	Linuxにおけるファイルシステムについて説明し、ファイルシステムを管理する方法を紹介する。また、ハードディスク、フロッピーディスク、CD、DVD、その他の周辺機器など様々な形態のディスク装置について、その利用方法を解説する。	6
I-7-6. ユーザの登録・削除とユーザ環境の整備	Linuxにおけるユーザの登録・削除等のユーザ管理について、その基本と作業手順、ユーザ環境の設定方法、グループの作成方針、ユーザごとのセキュリティ管理など、実際の作業に必要な項目を解説する。	4
I-7-7 システムのバックアップとリストア	Linuxシステムにおけるデータやアプリケーションリソースに関して、不慮の事故に備えたバックアップの運用管理方法について説明する。さらに事故が生じた場合のリストア方法や運用コストを考慮したバックアップ方針についても説明する。	5
I-7-8. ログの取得、管理と解析	システムが正常に動作しているかどうかを監視する手段としてのログ管理について解説する。ログの種類、ログの取得方法、ログの分散管理といった話題や、ログ取得のタイミング、ログの解析方法といったログ運用にまつわる話題についても触れる。	5
I-7-9. カーネルの運用・管理とカーネル再構築	カーネルの位置づけと機能についてカーネル管理の側面から説明し、カーネルの設定を管理する運用の重要性を示す。また実際にカーネルを更新する方法やカーネルパラメータの調整、カーネルモジュールの取扱い方法などについて説明する。	7
I-7-10. ネットワークの基本的な設定	Linuxにおけるネットワークの管理運用方法について解説する。イーサネットやWifiといった各種のネットワークの設定方法や設定ファイル、稼働状況の確認方法、ネットワーク全体の設定ファイルなど、ネットワーク運用に関わる基本的な項目を確認する。	8

【学習ガイダンスの使い方】

1. 「習得ポイント」により、当該科目で習得することが期待される概念・知識の全体像を把握する。
2. 「シラバス」、「IT 知識体系との対応関係」、「OSS モデルカリキュラム固有知識」をもとに、必要に応じて、従来の IT 教育プログラム等との相違を把握した上で、具体的な講義計画を考案する。
3. 習得ポイント毎の「学習の要点」と「解説」を参考にして、講義で使用する教材等を準備する。

3. IT 知識体系との対応関係

「7. Linux のシステム管理に関する知識Ⅰ」と IT 知識体系との対応関係は以下の通り。

科目名	基本レベル（Ⅰ）								応用レベル（Ⅱ）						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
7. Linuxのシステム管理に関する知識	<Linuxシステム管理の作業概要>	<Linuxシステム管理・サーバ管理>	<Linuxシステム管理・ファイル／ディスク管理>	<Linuxシステム管理・ユーザ管理>	<Linuxシステム管理・バックアップとログ運用管理>	<Linuxシステム管理・リソース管理>	<Linuxシステム管理・カーネルの管理>	<Linuxシステム管理・ネットワーク管理>	<Linuxシステム管理・ルーティング管理>	<Linuxシステム管理・DHCPの構築と運用>	<Linuxシステム管理・FTPの構築と運用>	<Linuxシステム管理・NFSの構築と運用>	<Linuxシステム管理・Sambaの構築と運用>	<Linuxシステム管理・基本運用作業のトラブルシューティング>	<Linuxシステム管理・ネットワークのトラブルシューティング>

[シラバス：http://www.ipa.go.jp/software/open/ossc/download/Model_Curriculum_05_07.pdf]

<IT 知識体系上の関連部分>

分野		科目名	1	2	3	4	5	6	7	8	9	10	11	12	13
組織関連事項と情報システム	1	IT-IAS 情報保証と情報セキュリティ	IT-IAS1. 基礎的な問題	IT-IAS2. 情報セキュリティの仕組み（対策）	IT-IAS3. 運用上の問題	IT-IAS4. ポリシー	IT-IAS5. 攻撃	IT-IAS6. 情報セキュリティ分野 [7-1-1]	IT-IAS7. フォレンジック（情報証拠）	IT-IAS8. 情報の状態	IT-IAS9. 情報セキュリティサービス	IT-IAS10. 脅威分析モデル	IT-IAS11. 脆弱性		
	2	IT-SP 社会的な観点とプロフェッショナルとしての課題	IT-SP1. プロフェッショナルとしてのコミュニケーション	IT-SP2. コンピュータの歴史	IT-SP3. コンピュータを取り巻く社会環境	IT-SP4. チームワーク	IT-SP5. 知的財産権	IT-SP6. コンピュータの法的問題	IT-SP7. 組織の中のIT	IT-SP8. プロフェッショナルとしての倫理的な問題と責任	IT-SP9. プライバシーと個人の自由				
応用技術	3	IT-IM 情報管理	IT-IM1. 情報管理の概念と基礎	IT-IM2. データベース問合わせ言語	IT-IM3. データアーキテクチャ	IT-IM4. データモデリングとデータベース設計	IT-IM5. データと情報の管理	IT-IM6. データベースの応用分野							
	4	IT-WS Webシステムとその技術	IT-WS1. Web技術	IT-WS2. 情報アーキテクチャ	IT-WS3. デジタルメディア	IT-WS4. Web開発	IT-WS5. 脆弱性	IT-WS6. ソーシャルソフトウェア							
ソフトウェアの方法と技術	5	IT-PF プログラミング基礎	IT-PF1. 基本データ構造	IT-PF2. プログラミングの基本的構成要素	IT-PF3. オブジェクト指向プログラミング	IT-PF4. アルゴリズムと問題解決	IT-PF5. イベント駆動プログラミング	IT-PF6. 再帰							
	6	IT-IPT 技術を統合するためのプログラミング	IT-IPT1. システム間通信	IT-IPT2. データ割り当てと交換	IT-IPT3. 統合的コーディング	IT-IPT4. スクリプティング手法	IT-IPT5. ソフトウェアセキュリティの実現	IT-IPT6. 種々の問題	IT-IPT7. プログラミング言語の概要						
	7	CE-SWE ソフトウェア工学	CE-SWE0. 歴史と概要	CE-SWE1. ソフトウェアプロセス	CE-SWE2. ソフトウェアの要求と仕様	CE-SWE3. ソフトウェアの設計	CE-SWE4. ソフトウェアのテストと検証	CE-SWE5. ソフトウェアの保守	CE-SWE6. ソフトウェア開発・保守ツールと環境	CE-SWE7. ソフトウェアプロジェクト管理	CE-SWE8. 言語翻訳	CE-SWE9. ソフトウェアのフォールトトレランス	CE-SWE10. ソフトウェアの構成管理 [7-1-1]	CE-SWE11. ソフトエアの標準化	
	8	IT-SIA システムインテグレーションとアーキテクチャ	IT-SIA1. 要求仕様	IT-SIA2. 調達/手配	IT-SIA3. インテグレーション	IT-SIA4. プロジェクト管理	IT-SIA5. テストと品質保証	IT-SIA6. 組織の特性	IT-SIA7. アーキテクチャ						
システム基盤	9	IT-NET ネットワーク	IT-NET1. ネットワークの基礎	IT-NET2. ルーティングとスイッチング	IT-NET3. 物理層	IT-NET4. セキュリティ	IT-NET5. アプリケーション分野	IT-NET6. ネットワーク管理							
	10	CE-NWK テレコミュニケーション	CE-NWK0. 歴史と概要	CE-NWK1. 通信ネットワークのアーキテクチャ	CE-NWK2. 通信ネットワークのプロトコル [7-1-8]	CE-NWK3. LANとWAN	CE-NWK4. クライアントサーバコンピューティング	CE-NWK5. データのセキュリティと整合性	CE-NWK6. ワイヤレスコンピューティングとモバイルコンピューティング	CE-NWK7. データ通信	CE-NWK8. 組込み機器向けネットワーク	CE-NWK9. 通信技術とネットワーク概要	CE-NWK10. 性能評価	CE-NWK11. ネットワーク管理	CE-NWK12. 圧縮と伸張
			CE-NWK13. クラスタシステム	CE-NWK14. インターネットアプリケーション	CE-NWK15. 次世代インターネット	CE-NWK16. 放送									
	11	IT-PT プラットフォーム技術	IT-PT1. オペレーティングシステム	IT-PT2. アーキテクチャと機構	IT-PT3. コンピュータインフラストラクチャ	IT-PT4. デプロイメントソフトウェア	IT-PT5. ファームウェア	IT-PT6. ハードウェア							
	12	CE-OPS オペレーティングシステム	CE-OPS0. 歴史と概要	CE-OPS1. 並行性	CE-OPS2. スケジューリングとディスパッチ	CE-OPS3. メモリ管理	CE-OPS4. セキュリティと保護	CE-OPS5. ファイル管理	CE-OPS6. リアルタイムOS	CE-OPS7. OSの概要	CE-OPS8. 設計の原則	CE-OPS9. デバイス管理	CE-OPS10. システム性能評価		
コンピュータアーキテクチャとハードウェア	13	CE-CA0 コンピュータのアーキテクチャと構成	CE-CA00. 歴史と概要	CE-CA01. コンピュータアーキテクチャの基礎	CE-CA02. メモリシステムの構成とアーキテクチャ	CE-CA03. インタフェースと通信	CE-CA04. デバイスサブシステム	CE-CA05. CPUアーキテクチャ	CE-CA06. 性能・コスト評価	CE-CA07. 分散・並列処理	CE-CA08. コンピュータによる計算	CE-CA09. 性能向上			
複数領域にまたがるもの	14	IT-ITF IT基礎	IT-ITF1. ITの一般的なテーマ	IT-ITF2. 組織の問題	IT-ITF3. ITの歴史	IT-ITF4. IT分野（学科）とそれに関連のある分野（学科）	IT-ITF5. 応用領域	IT-ITF6. IT分野における数学と統計学の活用							
	15	CE-ESY 組込みシステム	CE-ESY0. 歴史と概要	CE-ESY1. 低電力コンピューティング	CE-ESY2. 高信頼性システムの設計	CE-ESY3. 組込み用アーキテクチャ	CE-ESY4. 開発環境	CE-ESY5. ライフサイクル	CE-ESY6. 要件分析	CE-ESY7. 仕様定義	CE-ESY8. 構造設計	CE-ESY9. テスト	CE-ESY10. プロジェクト管理	CE-ESY11. 並行設計（ハードウェア、ソフトウェア	CE-ESY12. 実装
			CE-ESY13. リアルタイムシステム設計	CE-ESY14. 組込みマイクロコントローラ	CE-ESY15. 組込みプログラム	CE-ESY16. 設計手法	CE-ESY17. ツールによるサポート	CE-ESY18. ネットワーク型組込みシステム	CE-ESY19. インタフェースシステムと混合信号システム	CE-ESY20. センサ技術	CE-ESY21. デバイスドライバ	CE-ESY22. メンテナンス	CE-ESY23. 専門システム	CE-ESY24. 信頼性とフォールトトレランス	

4. OSS モデルカリキュラム固有の知識

OSS モデルカリキュラム固有の知識として、Linux という具体的なシステムを通した運用に関する知識がある。Linux の管理者の主要な作業であるサービス管理、パッケージ管理、ユーザ管理、バックアップ、ログ管理、カーネルの運用管理などが含まれる。

科目名	第1回	第2回	第3回	第4回	第5回	第6回	第7回	第8回
7.Linux のシステム管理に関する知識Ⅰ	(1)システム管理業務の概要 (2)システム管理者の作業	(1)管理者権限とは (2)Linux のインストール (3)システムの起動とサービス制御 (4)RPM パッケージ	(1)ファイルシステム管理 (2)ディスクの利用	(1)ユーザ管理 (2)ユーザごとのセキュリティパーミッ	(1)バックアップ (2)ログ管理	(1)システム運用	(1)カーネルとは (2)カーネルの運用管理	(1)Linux とTCP/IP プロトコル

（網掛け部分は IT 知識体系で学習できる知識を示し、それ以外は OSS モデルカリキュラム固有の知識を示している）

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-1. システム管理者の役割と管理業務	
対応する コースウェア	第1回（Linux システム管理の作業概要） 第2回（Linux システム管理・サーバ管理）	

I-7-1. システム管理者の役割と管理業務

システム管理業務の概要と、目的、必要性、システム管理作業の種類と内容などについて解説する。またシステム管理者の役割と管理者権限について説明し、システム管理者として心がけるべき事項についても言及する。

【学習の要点】

* システム管理業務には、ユーザのアカウントの管理やパーティションの増設、バグ・セキュリティ対策、データ管理などがある。
* システム管理を適切に行うには、事前に手順・ルールを文書化し、定期的に見直さなければならない。
* システム管理者としてログインした場合は、誤操作の被害が大きいので、慎重に操作を行う。

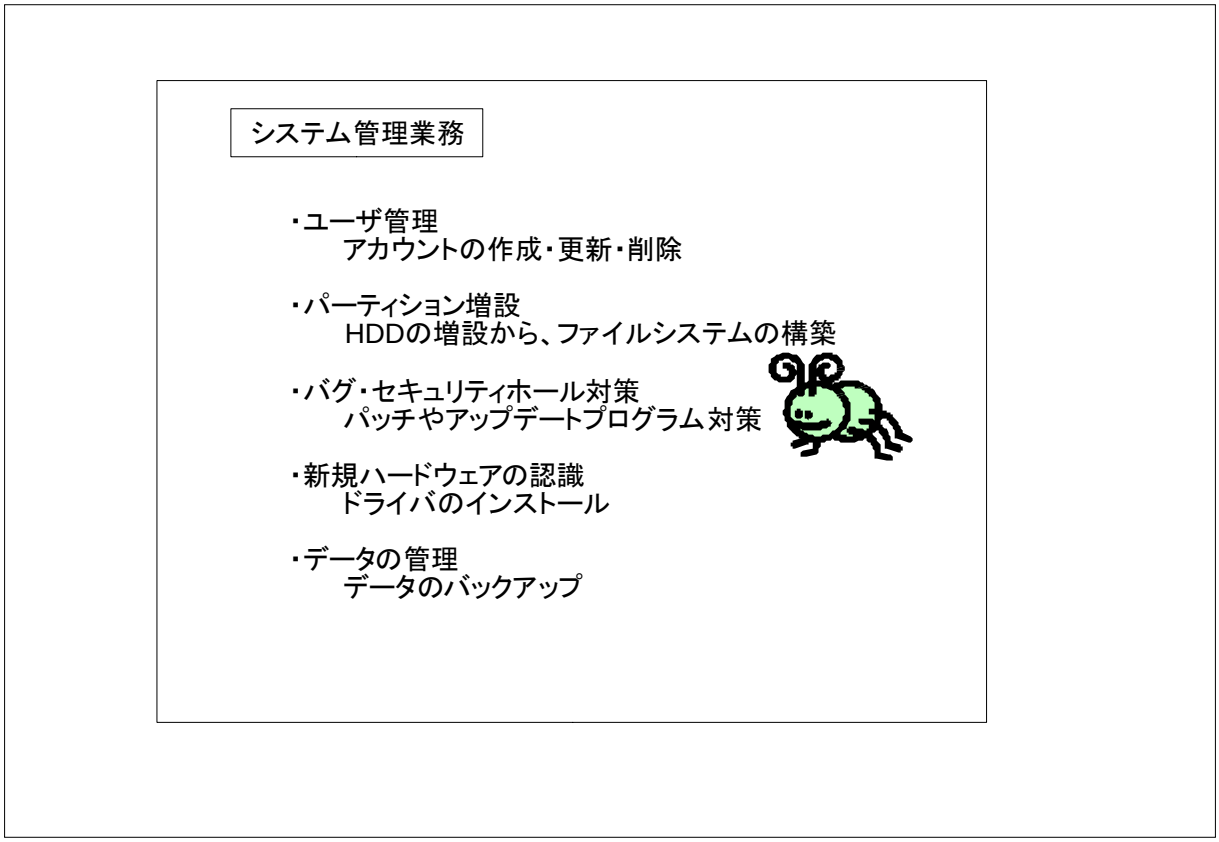

図 I-7-1.　システム管理業務

【解説】

1) システム管理業務の概要

システム管理者は、当該システムもしくはサービスを利用するユーザに対して、安全で信頼できるシステムを維持できるようにルールを定めて運用・管理を行う必要がある。具体的な作業は以下の通り。

＊ ユーザ管理
一般ユーザのためのアカウントの作成・更新・削除を実施する。

＊ パーティション増設
HDD の増設からパーティションの構築、ファイルシステムの構築を行う。

＊ バグ・セキュリティホール対策
パッチやアップデートプログラム対策を行う。

＊ 新規ハードウェアの認識
ハードウェアの増設に伴うドライバのインストール処理

＊ データの管理
重要なデータは、定期的にバックアップを取得し維持保管に努める。

2) システム管理者の役割と管理者権限

基本的に管理業務を行うユーザは、常に管理者権限を持つシステム管理者（root ユーザ）である。ただし、都度システム管理者としてログインして操作を行うことは、あまり推奨されていない。

＊ 一般ユーザからシステム管理者へスイッチする。
一般ユーザとしてログインしてから、su などのコマンドを使用することで、システム管理者にスイッチすることが可能である。ただし、この場合はシステム管理者のパスワードを事前に入手しておかなければならない。

＊ 一般ユーザにシステム管理者専用のコマンドが使用できる権限を与えておく。
sudo コマンドを使用することで、一般ユーザであっても管理者コマンドの使用が可能となる。

3) システム管理者として心がけるべき事項

システム管理者はすべてのファイルへのアクセスが可能であり、ふとした不注意で重要なファイルを壊してしまう可能性もある。システム管理者として操作を行う場合は、十分に注意しながら操作を行う必要がある。

＊ パッチやアップデートプログラムを入手した場合。
最新のパッチやアップデートプログラムを入手した場合であっても、それが本当に必要なプログラムとは限らない。必要なプログラムはどれなのかを、管理者は注意して監視していかなければならない。

＊ ユーザの削除
不要となったアカウントを削除したことにより、何らかの不具合が発生する可能性もある。削除する場合は、事前にルールを決めておき、そのルールに従って削除すべきである。

＊ ハードディスク上の空き領域の管理
定期的にバックアップを取得したりしながら、同時に空き容量の管理も行わなければならない。

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-2. Linux システムのインストール	
対応する コースウェア	第3回（Linux システム管理・ファイル/ディスク管理）	

I-7-2. Linux システムのインストール

Linux のインストール作業に関して解説する。インストールの具体的な手順を示し、各種項目の設定方法やアプリケーションパッケージの導入方法、パッケージ管理、インストール作業を行う際に気をつけることなどについて説明する。

【学習の要点】

＊ Linux のインストールには、anaconda を採用しているディストリビューションが多い。

＊ anaconda を利用すれば、パーティショニングなども簡単に行える。

＊ インストール時に HDD を多くのパーティションに分割すると、安全な運用が可能となる。

＊ アプリケーションパッケージの導入は、ディストリビューションに含まれているものを利用するか、コミュニティの Web サイトからソースコードをダウンロードしてから利用する方法の2通りがある。

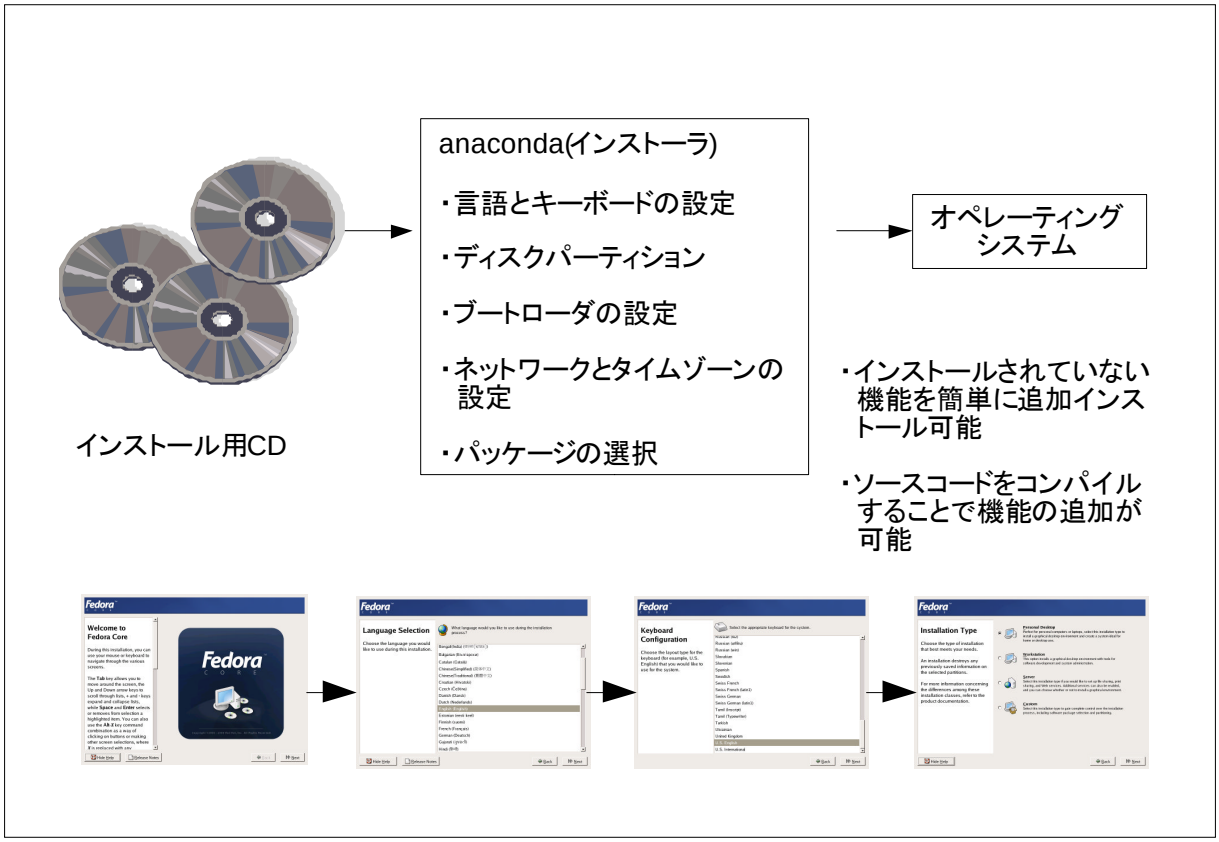

図 I-7-2.　Linux システムのインストール

【解説】

1) anaconda とは

Linux のインストールには、OSS として提供されている anaconda を利用しているディストリビューションが多い。anaconda の特徴は以下の通りである。

＊ レスキューモードでトラブルシューティングが可能である
何らかの設定ミス、もしくはファイルシステムの損傷等によりシステムが起動しなくなった場合には、レスキューモードという状態で起動することによりトラブル対処が可能となる。

＊ Kickstart によりインストールの自動化が可能である
インストール時の操作を一切省いて、テキストファイルの指示でインストールを自動的に行う。

2) anaconda の操作方法

anaconda を利用してのインストールは、非常に簡単でわかりやすい。インストール操作は以下に示す項目に関して、もっとも適切と思われるものを選択しながら進める。なお、ディストリビューションによっては、anaconda から間接的に呼び出されるツールが異なっているので注意が必要である。

＊ 言語とキーボード
＊ ディスクパーティショニング
＊ ブートローダの設定
＊ ネットワークとタイムゾーンの設定
＊ パッケージの選択

パーティションは、なるべく多く作成した方がよいとされている。その理由は、障害が発生した場合に、被害のおよぶ範囲をその小さなパーティション内にとどめることが可能だからである。典型的なマウントポイントを以下に示す。

- /boot　サイズの目安としては、ディスクの先頭に 100MB 程度
- /　必須。サイズの目安としては数百 MB 程度
- /usr　インストールする機能に数にもよるが、1GB～5GB 程度
- /var　頻繁に変更されるファイルが保存される。1GB 程度
- SWAP　一般的に物理メモリーの2倍
- その他　/home など

3) アプリケーションパッケージの導入方法

アプリケーションの導入方法に関しては、以下に示す2つの方法がある。

＊ ディストリビューションに添付されているものを利用する方法
オペレーティングシステムのインストール時に導入することが可能。インストール時に導入しなくても、ツールの利用により追加インストールは簡単に行える。ただし、製品 CD 作成時に最新であったバージョンが組み込まれるため、利用時の最新バージョンではない場合が多い。

＊ ソースコードをダウンロードして、コンパイルする方法
アプリケーションのソースコードをダウンロードして、コンパイルを行ってから利用する方法。常に最新のバージョンを利用することが可能だが、ソースコードからビルドする手間がかかり、環境の違いからうまく動作しない可能性もある。

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-3. Linux システムの起動と停止	
対応する コースウェア	第2回（Linux システム管理・サーバ管理） 第3回（Linux システム管理・ファイル/ディスク管理）	

I-7-3. Linux システムの起動と停止

Linux システムの起動と終了の手順、起動時および終了時の動作内容を説明する。またサービスの起動と停止の基本について述べ、提供するサービスの選択方法やサービスの起動停止を設定する各種のツールについて解説を加える。

【学習の要点】

＊ 起動時のログを参照することで、認識されたハードウェアを確認することが可能である。

＊ 個々のサービスの起動方法は、ディストリビューションによって異なる。

＊ システムを停止させる場合は、データの書き込み速度も考えて、安全にシステムを停止させるコマンドを利用する。

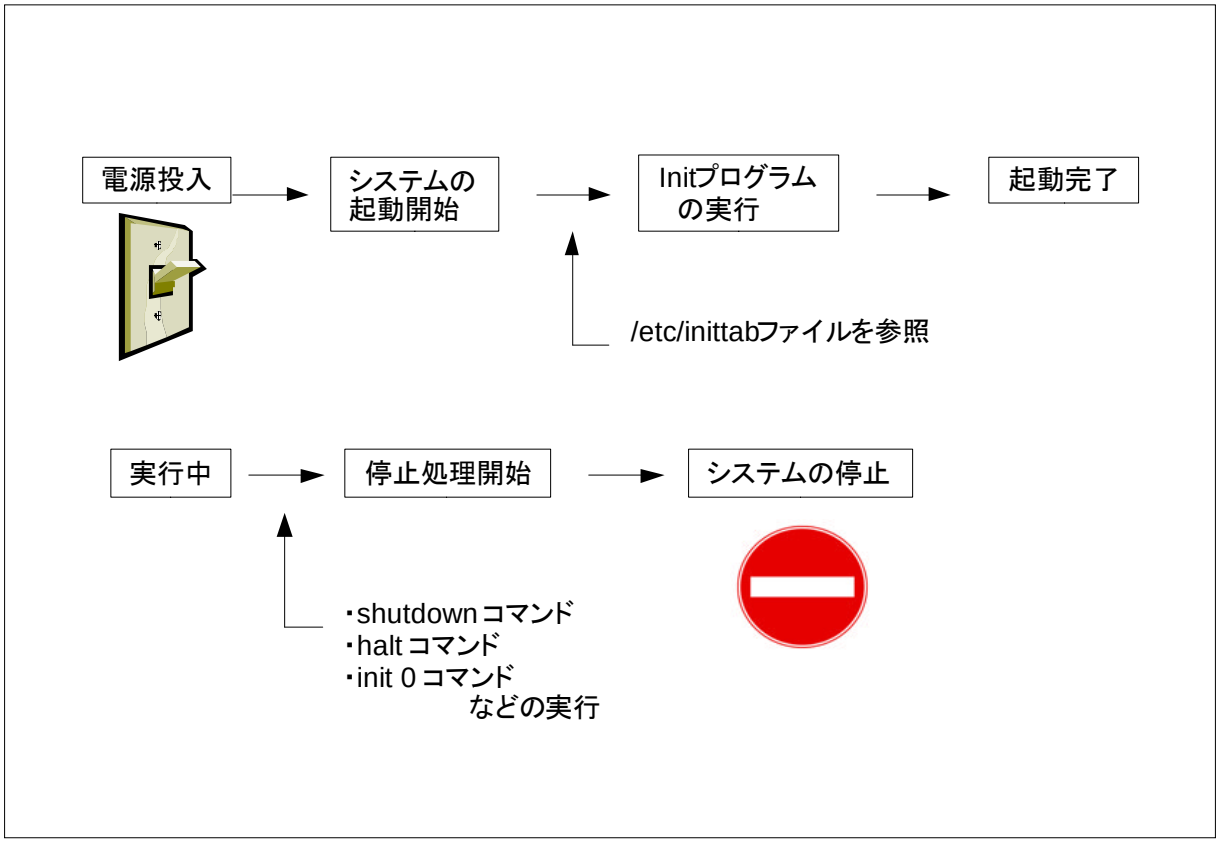

図 I-7-3.　起動と停止

【解説】

1) 起動時のログ

コンピュータの電源を投入することで、Linux システムが起動される。新しいハードウェアが正しく認識されたかを確認したい場合には、起動時のログをチェックする必要がある。

＊ 起動時のログは dmesg コマンドで参照可能である。
起動時の画面には、ドライバの初期化とハードウェアチェックの結果が表示される。この起動時の画面から問題発生が確認できたとしても、その時点で該当するハードウェアにアクセスすることは不可能である。実際には正常に起動したあとで、ログを参照して問題解決を図る。起動時のログは dmesg コマンドで確認することができる。

- dmesg： カーネルの（ログ用）リングバッファの表示と制御

2) サービスの起動

Linux の起動時、カーネルが読み込まれて必要な初期化処理が行われたあと、最初のプログラムである init が実行される。init は/etc/inittab の記述に従い、様々なサービスの起動を行う。

＊ init プログラム
初期ランレベルを取得後、そのランレベル専用のディレクトリ内のスクリプトを順次実行する。このスクリプトから個々のサービスが起動するため、init プログラムはほとんどのサービスの親プロセスとなる。

- ランレベル
起動時のモードや状態などを、0から6までの数値などを使って表す。通常、ランレベルは3（マルチユーザ）もしくは5（マルチユーザとグラフィカル環境）が使用される。
- ランレベル専用のディレクトリ
/etc/rc.d ディレクトリ配下には、rc0.d, rc1.d～rc6.d というディレクトリが用意されている。ランレベル5で起動する場合には、/etc/rc.d/rc5.d 以下のスクリプトが順番に実行される。
- サービス起動のためのスクリプト
Linux 起動時には、あらかじめ指定したサービスを提供するプログラムのみが起動する。この設定、すなわちLinuxの起動と同時に立ち上げるサービスの選択には、GUI で提供されるサービス設定用ツールや、chkconfig などのコマンドを利用する。

3) システムの停止

システムを停止させるためのコマンドとして様々なコマンドが用意されている。書き込みキャッシュに残ったデータを確定させたり、アンマウント処理を確実に実施したりという配慮が必要なため、安全にシステムを停止させるコマンドを利用すべきである。代表的なコマンドを以下に示す。

- shutdown コマンド
システムを安全に停止させるコマンド。オプションや引数の設定によって、振る舞いが異なってくる。
- halt コマンド
短縮形のコマンド。即座にシステムの停止処理を開始させる。
- init 0 コマンド
halt コマンドと同様。

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-4. 各種サービスの設定方法	
対応する コースウェア	第2回（Linux システム管理・サーバ管理）	

I-7-4. 各種サービスの設定方法

Linux システムが提供する各種のサービスについて、多くのサービスでは/etc 以下に設定ファイルが集められていることを示し、さらに代表的なサービスの設定方法や設定ツールについて理解する。

【学習の要点】

* 各種サービスの設定ファイルは、/etc ディレクトリ配下に置かれていることが多い。
* ディストリビューション毎にサービスの設定ファイルを保存したディレクトリが異なるので注意を要する。
* インストール直後のデフォルト設定のままで最低限のサービス提供が可能なものもあるが、デフォルト設定ではサービスの提供先が限定されていることがある。

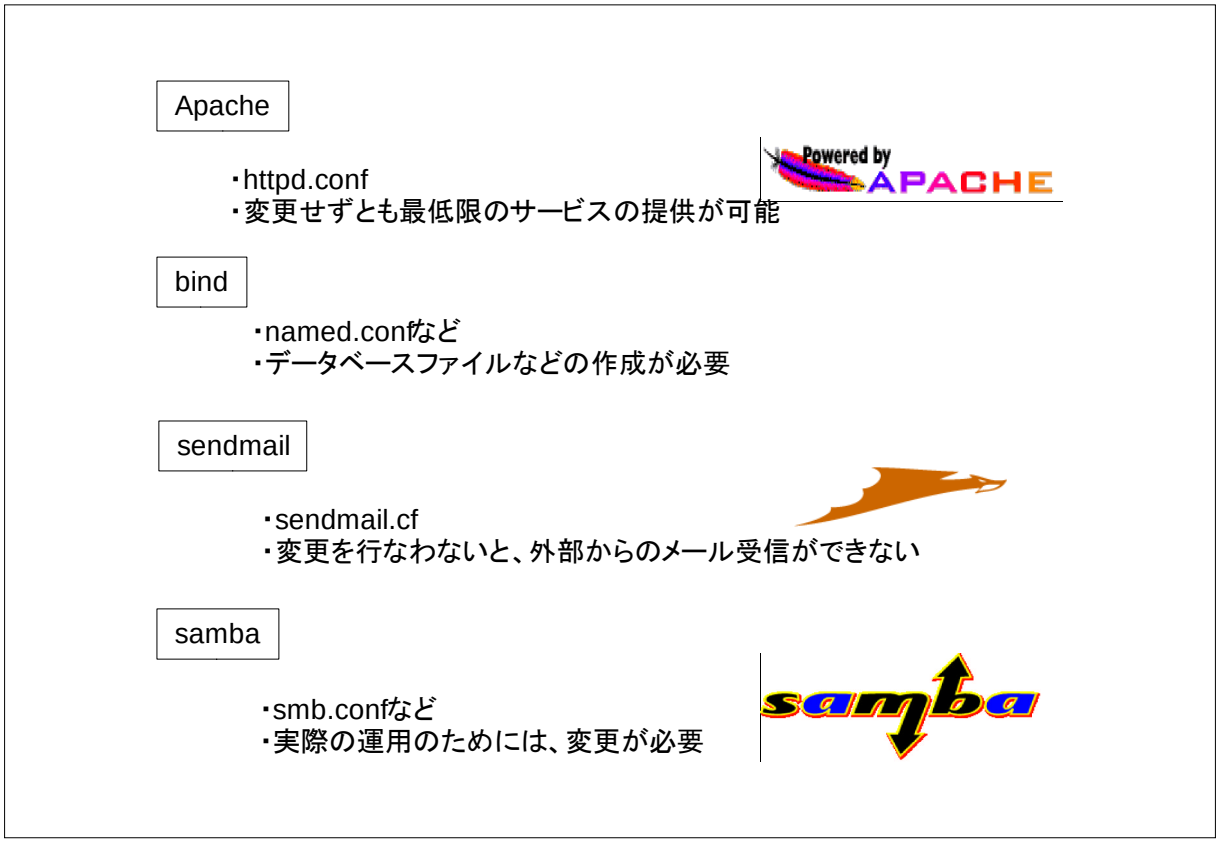

図 I-7-4.　代表的なサービスの設定ファイル

【解説】

1) コンフィグレーションファイルの置き場所

Linux システムが提供する各種のサービスには、個別のチューニングを行うためのコンフィグレーションファイルが用意されている。コンフィグレーションファイルの置き場所は、ディストリビューションごとに異なる。代表的なサービスのコンフィグレーションファイルの置き場所を、以下に示す。

* Domain Name Services（bind）
  - chroot 未実行時：/etc/named.conf
  - chroot 実行時：/var/named/chroot/etc/named.conf
* Apache Web Server
  - Red Hat 系：/etc/httpd.conf
  - SUSE 系：/etc/apache2
  - ソースコードからのインストール：/usr/local/apache2/conf
* sendmail
  - /etc/mail/sendmail.cf
  - 過去のバーションでは /etc/sendmail.cf
* Samba
  - /etc/samba/smb.conf
  - 過去のバージョンでは /etc/smb.conf

2) サービスの設定方法と設定ツール

サービスによっては、インストールを行うだけで最低限のサービスを提供することが可能なものもあれば、コンフィグファイルに何らかの追記を行わないと、サービスの提供先が限定されているものもある。

* Domain Name Services（bind）
  - 名前解決を行うためのデータベースファイルを作成しないと、十分な名前解決は行えない。ディストリビューションにより、bindconf や system-config-bind などのツールを提供している。
* Apache Web Server
  - コンフィグレーションファイルを書き換えなくても、最低限のサービス提供は可能である。ディストリビューションによっては、redhat-config-httpd といったツールを提供している。
* sendmail
  - コンフィグレーションファイルの書き換えを行わないと、外部から送られてきたメールを受信することができない。手動でコンフィグレーションファイルを書き換えることは推奨されていないため、m4 というツールを使って設定すべきである。
* Samba
  - 実際の運用を考えると、コンフィグレーションファイルの書き換えを実施すべきである。SWAT や system-config-smb などの便利な設定ツールも豊富に用意されている。

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-5. ファイルシステムとディスクの管理	
対応する コースウェア	第6回 (Linux システム管理・リソース管理)	

I-7-5. ファイルシステムとディスクの管理

Linux におけるファイルシステムについて説明し、ファイルシステムを管理する方法を紹介する。また、ハードディスク、フロッピーディスク、CD、DVD、その他の周辺機器など様々な形態のディスク装置について、その利用方法を解説する。

【学習の要点】

* Linux は ext2 や ext3 といったファイルシステムを主にサポートしている。
* このファイルシステム上で利用可能な ACL (Access Control List)といった機能は、特に Enterprise 系のセキュリティ管理で重要である。
* ネットワークを使わずにデータを移動するために利用できるデバイス(リムーバブルメディア)は、ほとんどのものがサポートされている。

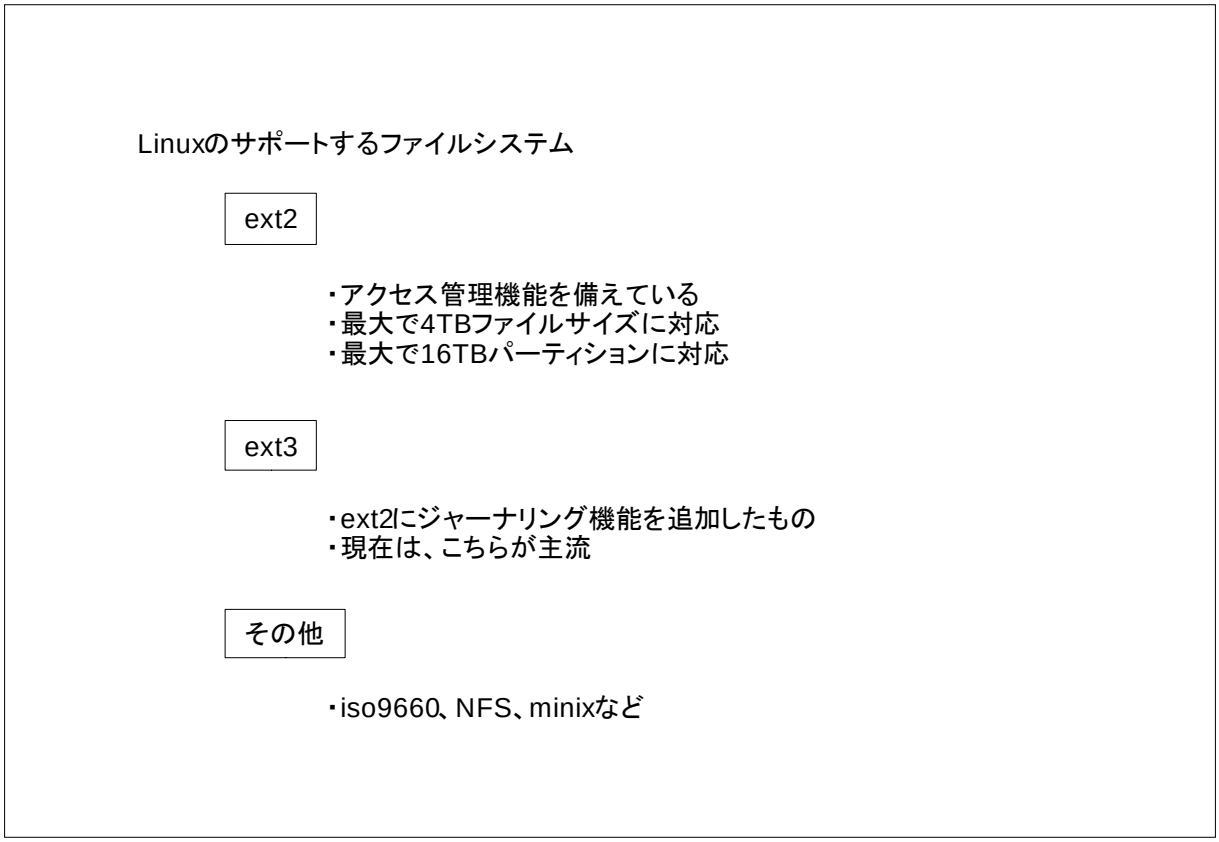

図 I-7-5.　Linux のサポートするファイルシステム

【解説】

1) Linux におけるファイルシステム

Linux が採用しているファイルシステムには ext2 ファイルシステムや ext3 ファイルシステムなどがある。また、バージョン 2.6 系のカーネルでは、XFS や JFS といった商用ファイルシステムもサポートされている。

＊ ext2 ファイルシステムとは
以前のディストリビューションにおいて採用されていたファイルシステムである。拡張属性や POSIX Access Control List（ACL）という高度な機能を備えている。

＊ ext3 ファイルシステムとは
現在主流のファイルシステム。ext2 ファイルシステムにジャーナリング機能(ディスクへの書込みをトランザクションデータとして管理する機能)を追加したファイルシステムである。

＊ その他のファイルシステムに関して
その他、Windows が採用している FAT や VFAT というファイルシステムに関しても、Linux はサポートを行っている。したがって、これらのファイルシステム上のディレクトリやファイルへ Linux からアクセスすることもできる。以下はその他対応済みのファイルシステムである。

- NFS
- iso9660
- minix

2) ファイルシステムの構築

ハードディスクを増設するなどにより新たにパーティションを作成した場合は、そのパーティション上にファイルシステムを構築する。ファイルシステムの構築には、mke2fs コマンドを使用する。
なお 2.6 系のカーネルから採用されている ACL（Access Control List）などの拡張属性（商用 UNIX では一般に利用されている機能）を ext2 ファイルシステムや ext3 ファイルシステムにおいても使用することができる。

3) 周辺機器などの利用方法

ハードディスクや USB メモリーなどは、そのデバイス上にファイルシステムを構築することで、データ書き込み・読み込み等のアクセスが可能となる。

＊ ハードディスク
一般的な方法でパーティションを作成し、その上にファイルシステムを構築することで、アクセスが可能となる。

＊ USB メモリー
ハードディスクと同様。アクセスを行う場合は、SCSI デバイスとして認識される。

＊ フロッピーディスク
基本的にハードディスクと同様に利用することが可能だが、最近はフロッピディスクドライブを内蔵していない PC が主流となっている。

＊ CD・DVD
iso9660 というファイルシステムで構築されているが、Linux としてサポート済みであるため問題なくデータを読み込むことが可能である。

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-6. ユーザの登録・削除とユーザ環境の整備	
対応する コースウェア	第4回（Linux システム管理・ユーザ管理）	

I-7-6. ユーザの登録・削除とユーザ環境の整備

Linux におけるユーザの登録・削除等のユーザ管理について、その基本と作業手順、ユーザ環境の設定方法、グループの作成方針、ユーザごとのセキュリティ管理など、実際の作業に必要な項目を解説する。

【学習の要点】

＊ ユーザ管理は、「ユーザ管理ポリシー」を制定してから実施すべきである。

＊ ユーザのパスワードは、システム管理者であっても知っていてはいけない。

＊ ユーザ・アカウントの作成・削除は、コマンド操作で簡単にできるが、トラブルを避けるため、「ユーザ管理ポリシー」に定められた手続きを守って実施すべきである。

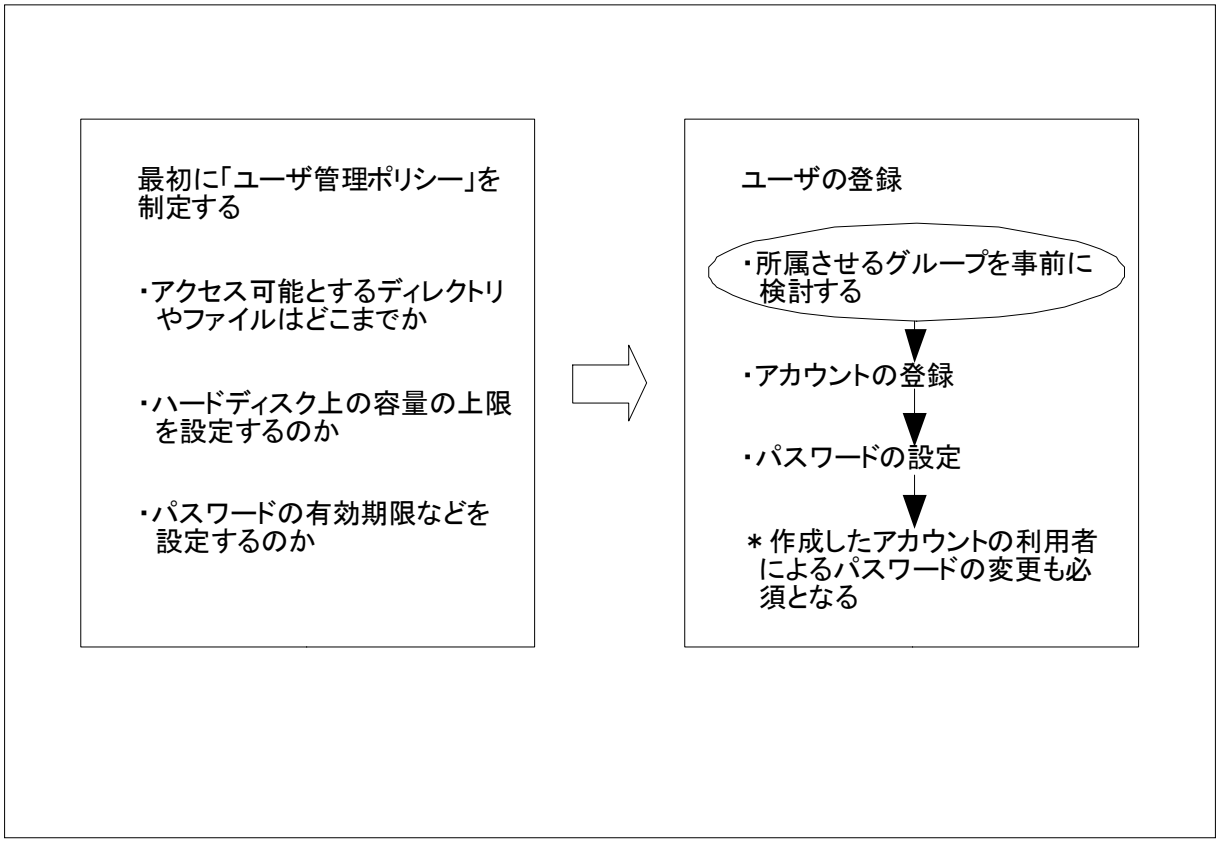

図 I-7-6.　ユーザの登録

【解説】

1) ユーザ管理はポリシーを制定してから実施すること

一般アカウントの作成は、コマンドで簡単に作成できる。アカウントの削除に関しても同様である。ユーザ管理をどのように行うのかを、ユーザ管理ポリシーとして事前に制定しておくことが重要である。

* ディレクトリやファイルをユーザがどこまでアクセス可能と設定するか。
  所属するグループにおけるパーミッションの設定や、ACL などの設定により実装が可能。
* 個々のユーザが使用することが可能な、ハードディスク上の容量に上限値を持たせるか否か。
  quota の設定により実装が可能。
* パスワードの有効期限に関する設定を行うか否か。
  chage コマンドによりユーザ・アカウントの有効期限を設定することが可能。

2) ユーザの登録方法

ユーザの登録(一般アカウントの作成)は、以下に示す操作で行う。

* 所属させるグループを事前に検討する
  既存のグループに登録させるのか、新規のグループに登録するのかを検討しておく。新規のグループへの登録であり、かつアカウント名とは異なる名称のグループとする場合は、事前にグループを作成しておく必要がある。
* アカウントの登録
  新しいアカウントはuseraddなどのコマンドで作成される。このアカウントの情報は/etc/passwdファイルに登録される。同時に、このアカウント用のホームディレクトリも作成される。
* パスワードの設定
  システム管理者であっても一般ユーザのパスワードを知っている必要はない。ただし、初期設定値はわかりやすいものに設定されていると思われるので、各個人でパスワードを自主的に変更するように教育すべきである。パスワードの変更はpasswdコマンドで行う。パスワードが記録されるのは、以下に示すファイルである。
  - /etc/passwd ファイル
  - /etc/shadow ファイル(シャドウパスワード機能が有効な場合)
* ユーザの削除
  アカウント利用者の退職等により、ユーザ(アカウント)を削除する場合にはuserdelなどのコマンドを使用する。この時、削除対象となるユーザのホームディレクトリも同時に削除するか否かは、事前に定めておいたポリシーに従って操作することが望ましい。

3) 特記事項

アカウントの作成に伴い、ユーザのホームディレクトリは自動的に作成される。このホームディレクトリには、必ずコピーされるファイルが存在する。これらは/etc/skel ディレクトリに保管されているファイルがコピーされる。

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-7. システムのバックアップとリストア	
対応する コースウェア	第5回（Linux システム管理・バックアップとログ運用管理）	

I-7-7. システムのバックアップとリストア

Linux システムにおけるデータやアプリケーションリソースに関して、不慮の事故に備えたバックアップの運用管理方法について説明する。さらに事故が生じた場合のリストア方法や運用コストを考えたバックアップ方針についても説明する。

【学習の要点】

＊ バックアップは、万が一の障害を想定して、リストア方法、全体と差分、周期（月次、周次、日次など）を考慮して、計画的に実施する必要がある。

＊ バックアップメディアにはデータ容量・信頼性の点で長所・短所があるので、正しく理解して使用する必要がある。

＊ バックアップ方針は、システムを運用する顧客毎に異なる。バックアップについてどんな方針を定めるべきか、事前に十分な協議を行う必要がある。

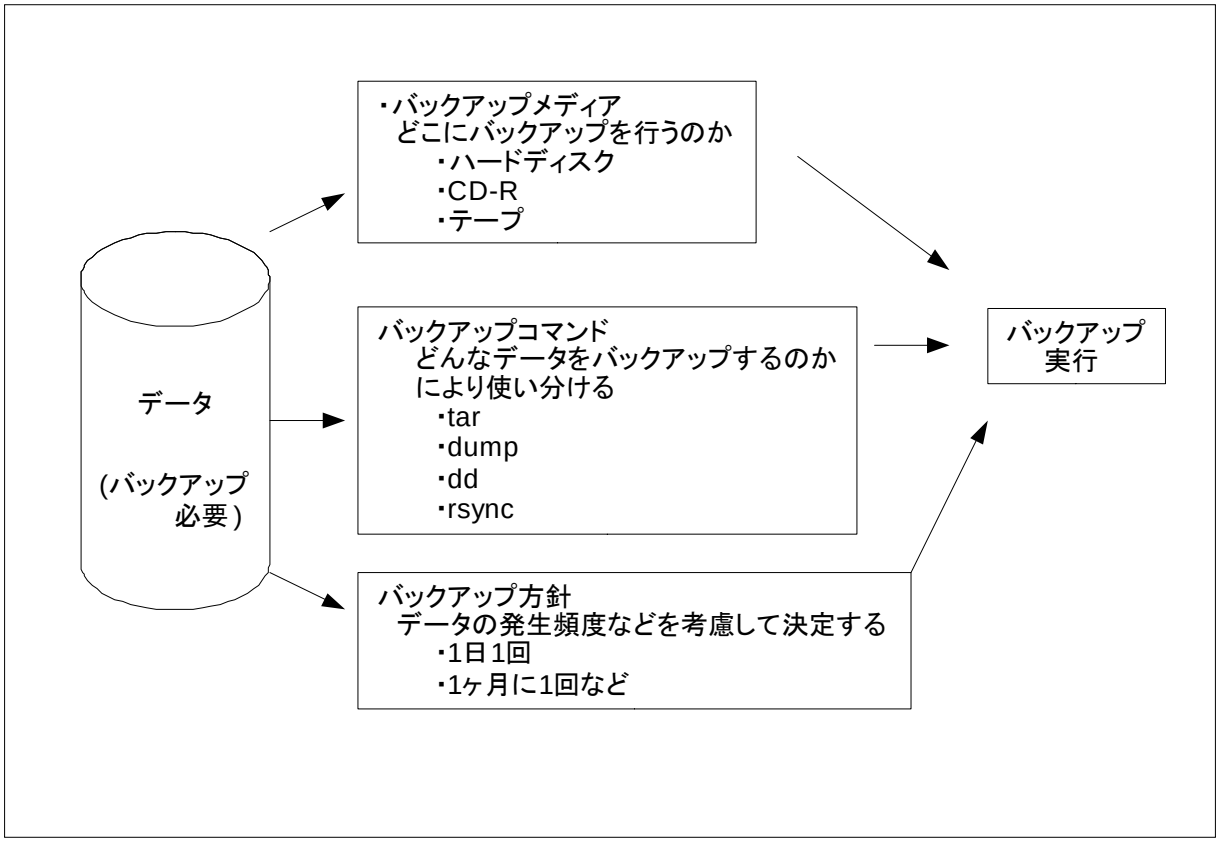

図 I-7-7.　システムのバックアップ

【解説】

1) バックアップメディア

システムやデータのバックアップを取得する際には、バックアップ対象となるデータの容量、バックアップメディアの信頼性、メディアの可搬性、コストと言ったものを事前に認識しておくことが重要である。

以下にバックアップを取得する際に利用可能なバックアップメディアを紹介する。

＊ ハードディスク
大容量データのバックアップ時に有効。信頼性も高く、コスト面でも低く抑えることが可能だが、可搬性に問題がある。

＊ CD-R、DVD などの光メディア
メディアがコンパクトで劣化が少ない。ただし、メディア1枚あたりの容量が少ないため、単価が高い。

＊ テープ
容量が多く単価も安いのだが、初期導入コストが高いことと環境によっては劣化が発生しやすい。Linux/UNIX システムでは主流となっている。

2) バックアップコマンドの操作

バックアップを行う際に使用するコマンドは、どんなデータを対象にバックアップするのかを考慮して、使い分けることが望ましい。

＊ tar コマンド
ディレクトリ単位や個々のデータ単位でバックアップを行いたい場合に利用。アプリケーションが出力したデータのバックアップ時に有効。tar コマンドでリストアも可能。

＊ dump コマンド
パーティション単位でバックアップを行いたい場合に利用。システム全体のバックアップ時に有効。restore コマンドでリストアが可能。

＊ dd コマンド
ハードディスク全体のバックアップを行いたい場合に利用。データがバックアップされハードディスクに交換することで、データのリストアとなる。

＊ rsync コマンド
常に同期を取りながらデータのバックアップを残したい場合に利用。

3) バックアップ方針

バックアップは、データの容量のほかにも、そのデータがどのくらいの期間に、どの程度発生するのかといったことも考慮して、その方針を決めていかなければならない。

＊ データは毎日発生し、その容量も多いシステムの場合。
1日に1回程度、テープメディアなどにバックアップする。

＊ 必要なのはデータのバックアップではなく、システムのバックアップである。
1月に1回程度、CD-R もしくはテープメディアにバックアップする。

＊ アプライアンスサーバなので、簡単に復旧できるようにしたい。
ハードディスクを2個設置し、dd コマンドなどで1日に1回程度バックアップする。

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-8. ログの取得、管理と解析	
対応する コースウェア	第5回（Linux システム管理・バックアップとログ運用管理）	

I-7-8. ログの取得、管理と解析

システムが正常に動作しているかどうかを監視する手段としてのログ管理について解説する。ログの種類、ログの取得方法、ログの分散管理といった話題や、ログ取得のタイミング、ログの解析方法といったログ運用にまつわる話題についても触れる。

【学習の要点】

＊ カーネルが出力するログデータは、klogd や syslogd デーモンにより記録される。

＊ ログが記録されるファイルの種類とその内容に関しては、正しく認識する必要がある。

＊ ログを管理するプログラムは、crond デーモンによって実行されるように設定されている。

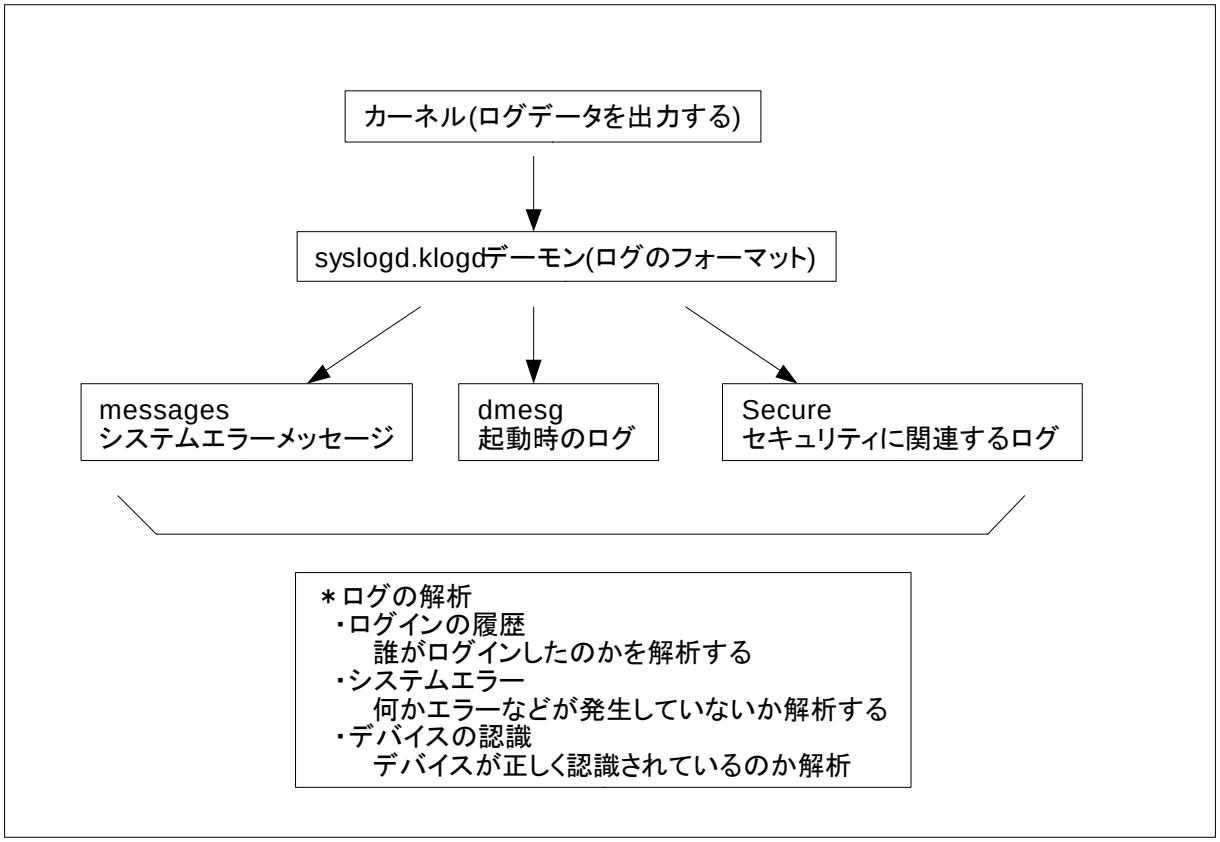

図 I-7-8.　ログの取得と解析

【解説】

1) ログの種類

カーネルが出力するログデータは、klogd や syslog というデーモンにより、管理者が参照しやすい形式に整形される。その結果は以下に示すファイルに書き込まれる。また、各アプリケーションから出力されるログデータは、アプリケーションごとのファイルの中に記録される。

* /var/log/dmesg
  起動時のログデータが記録される。
* /var/log/messages
  一般的なシステムエラーメッセージが記録される。
* /var/log/secure
  セキュリティに関連するログデータが記録される。

2) ログの管理

ログデータが書き込まれるファイルは、システムの運用が続く限り永久に出力され続ける。従って各ファイルのサイズも拡大し続けるが、ログを格納する領域が溢れないように定期的にログファイルの圧縮・保存が行われる。なおその処理は cron によって実行される以下のプログラムで実施される。

* logrotate
  各ログファイルを、他の名前のファイルに変更(xxx.log を xxx.log.1 とするなど)して保存する。そのようなファイルが増えてきた場合には、アーカイブ化を行い圧縮する。
* logwatch
  ログファイルの中に不正なログが残っていた場合に、その旨を root ユーザ宛にメールで通知する。

3) ログの解析方法

/var/log/secure ファイルには、リモート環境から誰がいつログインしたのかなどの情報が記録される。不正なログインの記録が残っていないかを、定期的にチェックすべきである。

* リモート環境からのログインの履歴
  許可を与えているユーザがログインしたのかどうか、許可を与えている環境からログインしたのかどうかといった事項に関する情報を解析する。
* システムエラーが発生していないかどうかの解析
  /var/log/messages ファイルには、システムエラーが記録されている。個々のサービスの起動時に、何らかのエラーが発生していないかをチェックすべきである。
* デバイスが認識されているのかを解析
  デバイスが認識されているかどうかに関する情報は、/var/log/dmesg ファイルに記録されている。デバイスの利用に問題が発生した場合に、まずは認識されているかどうかをチェックする。

なお、悪意を持つものが不正ログインしたような場合、この記録が残らないようにログファイルを書き換えてしまう場合がある。これに対処するためには、ログデータをサーバ内に残しておくだけでなく、他のリモートサーバの内部にも記録しておくことが望ましい。

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-9. カーネルの運用・管理とカーネルの再構築	
対応する コースウェア	第7回（Linux システム管理・カーネルの管理）	

I-7-9. カーネルの運用・管理とカーネルの再構築

カーネルの位置づけと機能についてカーネル管理の側面から説明し、カーネルの設定を管理する運用の重要性を示す。また実際にカーネルを更新する方法やカーネルパラメータの調整、カーネルモジュールの取扱い方法などについて説明する。

【学習の要点】

* カーネルとは、OS の基本機能を実装したソフトウェアである。
* 最新バーションのカーネルが公開された際は、セキュリティ強化のために最新バージョンに更新すべきである。
* 最新バージョンのソースコードが入手できればカーネルの再構築は可能であるが、ディストリビューションを利用すれば煩雑な操作を軽減できる。
* 新しいハードウェアデバイスを追加した場合には、ドライバ（カーネルモジュール）の追加が必要となる。

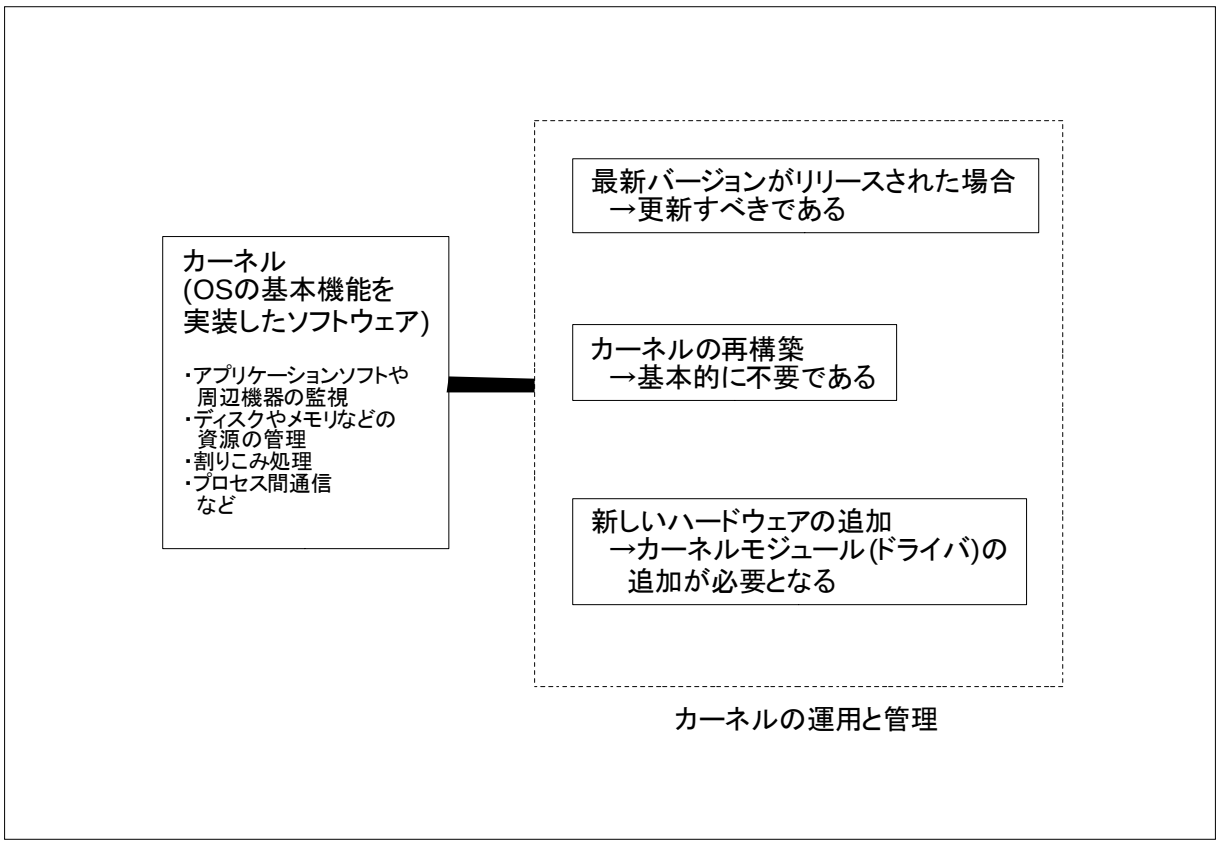

図 I-7-9.　カーネルの運用と管理

【解説】

1) カーネルとは

OS の中核部分となるプログラムであり、プログラム監視、周辺機器監視、資源管理、割りこみ管理、プロセス間通信の管理といった機能を提供する。Linux という言葉の本当の意味は、このカーネルを示している。

* カーネルモジュール
  周辺機器にアクセスする場合に必要となるドライバなど新たに組み込まれる機能は、必要なドライバだけをモジュールとして取り込んで使用している。
* セキュリティ機能の実装
  パケットベースでのフィルタリング機能を提供している。
* データの書き込み容量に関して、上限値の設定・監視を行う。
  ユーザごと、もしくはグループごとに、情報の書き込み容量に関して上限値の設定と監視を行っている。
* カーネルは積極的に更新が行われている
  カーネルは他のソフトウェアと比較しても、積極的に更新が行われている。セキュリティの側面からも、更新バージョンが提供された場合は、早々に最新バージョンに更新すべきである。Red Hat 系のディストリビューションであれば、最新バージョンのカーネルがパッケージファイルとして提供されるので、yum コマンドや rpm コマンドで簡単に更新することが可能である。

2) カーネルパラメータの調整と引数として設定する方法

カーネルに一時的な引数を与えて起動させることができる。Linux の多くのディストリビューションでは、起動時のブートローダ画面において起動パラメータを指定することができる。
また、以下に示す理由によりカーネルの再構築を行うこともある。ただし、各ディストリビュータは「カーネルの再構築」作業は基本的に不要であると宣言している。

* 不要な機能が組み込まれているため、取り除きたい場合
* 必要な機能が組み込まれていないため、カーネルにその機能を追加したい場合
* カーネル全体のサイズを縮小した場合

3) カーネルモジュールの取扱方法

新しいハードウェアを増設した場合には、ドライバ（カーネルモジュール）の追加が必要となる場合がある。情報を追記する必要のあるファイルは、ディストリビューションやバージョンごとに異なるが、基本的な流れは以下の通りとなる。

* ドライバ（カーネルモジュール）を用意する。
  ソースコードをコンパイルすることで、カーネルモジュールの作成が可能となる場合もある。
* 定められたディレクトリに、カーネルモジュールをコピーする。
  Red Hat 系 Linux の場合は、/lib/modules/配下のディレクトリとなる。
* どのデバイスがそのカーネルモジュールを使用するのかを宣言する。
  例えば Red Hat Enterprise Linux 5 の場合は、/etc/modprobe.conf ファイルに必要な命令を追記する。
* modprobe、insmod などのコマンドを使用して、カーネルにそのモジュールを認識させる。

スキル区分	OSS モデルカリキュラムの科目	レベル
システム分野	7　Linux システム管理に関する知識 I	基本
習得ポイント	I-7-10. ネットワークの基本的な設定	
対応する コースウェア	第8回（Linux システム管理・ネットワーク管理）	

I-7-10. ネットワークの基本的な設定

Linux におけるネットワークの管理運用方法について解説する。イーサネットや Wifi といった各種ネットワークの設定方法や設定ファイル、稼動状況の確認方法、ネットワーク全体の設定ファイルなど、ネットワーク運用に関わる基本的な項目を確認する。

【学習の要点】

* IP アドレスなどを設定するためのコマンドやツールの使い方を理解する。
* 設定ファイルを直接書き換えることでも、設定変更を行うことができる。
* サーバの死活監視など稼動状況をネットワーク上で監視するには、物理的なネットワーク接続、監視コンソールの設定、DNS サーバの動作が正常かを事前に確認する。

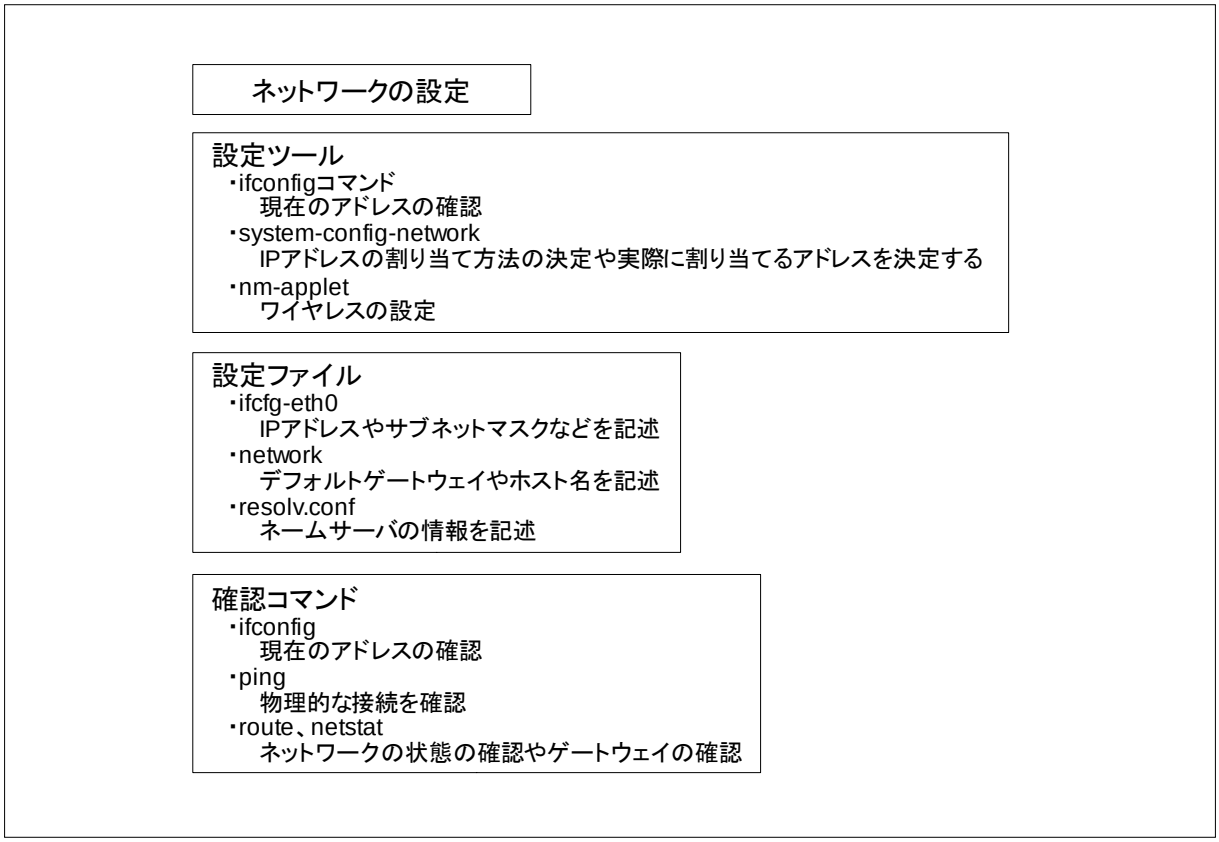

図 I-7-10.　ネットワークの設定

【解説】

1) ネットワーク設定ツール

ネットワークに接続する場合には、IP アドレスが割り当てられていなければならない。アドレスの割り当て方法には、静的に割り当てる方法と動的に割り当てる方法がある。どちらに設定するか、どんなアドレスを設定するのかなどは、コマンドやツールを利用することで可能となる。

* ifconfig コマンド
  割り当てられているアドレスを確認したり、静的にアドレス割り当てたりという場合に利用する。
* system-config-network ユーティリティ(Red Hat 系ディストリビューションで使用可)
  ifconfig と同じ機能を持つ。環境に合わせて GUI 画面やテキスト画面での設定が可能となる。
* nm-applet ユーティリティ(Red Hat 系ディストリビューションで使用可)
  ワイヤレスネットワークにおける設定を行う。

2) ネットワークに関連する設定ファイル

ネットワークを使用する場合には、IP アドレス・ネットマスク・デフォルトゲートウェイ・ネームサーバアドレスなどの情報が必要となる。これらの情報は、以下に示すファイルの中に格納されている。なお、以下に示すファイルを直接書き換えることで、IP アドレスなどの情報を変更することも可能である。

* /etc/sysconfig/network-scripts/ifcfg-eth0
  IP アドレスとネットマスクと言った情報が記述されている。ただし、DHCP などのサービスを利用している場合には、これらの情報は記述されない。
* /etc/sysconfig/network
  デフォルトゲートウェイの情報やホスト名などが記述されている。
* /etc/resolv.conf
  ネームサーバのアドレスが記述されている。

3) 稼動状況の確認方法

ネットワークに関して、設定ファイルの記述が正しくても、プログラムが起動していなければ正しく接続することはできない。同様に各種のサービスが実行されていなければ、サーバとして正しく動作する状態にならない。以下に稼動状況を確認するためのコマンドを明記する。

* IP アドレスやネットマスクの設定の確認方法
  ifconfig コマンドなどで、確認を行う。
* ネームサーバが正常に動作していることの確認方法
  以下に示すファイルや、コマンドの結果を見て確認を行う。
  - /etc/resolv.conf
  - host、dig、nslookup
* 物理的に接続されているかどうかの確認方法
  ping コマンドなどで、物理的に接続されているか確認を行う。
* ルーティングやデフォルトゲートウェイの確認方法
  以下に示すコマンドの結果を見て確認を行う。
  - route、netstat