7. Linux のシステム管理に関する知識 II

1. 科目の概要

Linux のシステム管理に関する手順のうち、やや高度なサービスの設定に関する手順を解説する。サーバとして利用する際の基本的な設定と、DHCP、FTP、ファイル共有など様々なサービスについて具体的な設定方法を示し、運用のノウハウを紹介する。

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
II-7-1. ルーティングの設定	ルーティングの概念を簡単に示したうえで、Linuxにおけるネットワークルーティングの設定方法を説明する。ルーティングの設定手順を示し、さらにそのルーティング設定が正しく動作しているかどうかの検証方法についても述べる。	9
II-7-2. DHCP環境の構築	ネットワークの環境を動的に設定するためのプロトコルであるDHCPの仕組みについて解説する。さらにLinuxにおけるDHCPの利用方法と、DHCPサーバの設定方法およびDHCPサーバの運用管理方法についても説明する。	10
II-7-3. FTPサーバの設定	FTPの概要を説明し、FTPサーバへのアクセスとサーバの動作について解説する。さらにLinuxで動作する代表的なFTPサーバを紹介する。FTPサーバのインストールと設定、運用管理の手順について解説する。	11
II-7-4. ファイル共有	ネットワーク上におけるファイル共有の考え方について述べる。ファイル共有には様々な方法があることを示し、それぞれのファイル共有手法の特徴と歴史、代表的なサーバ、利用例などを紹介する。	12,13
II-7-5. NFSの設定と運用	UNIXで利用されてきた代表的なファイル共有の手法であるNFSについて解説する。NFSとは何か、LinuxサーバにおけるNFSの設定手順、NFSクライアントの設定といった具体的な設定方法を説明し、NFSの運用管理に必要なノウハウについても触れる。	12
II-7-6. Sambaの設定と運用	LinuxとWindowsでデータを共有するためのSambaについて説明する。Sambaとは何か、Sambaのインストール方法、Sambaサーバの設定方法、Sambaクライアントの利用法など、Sambaの導入から運用に至るまでに必要な知識を紹介する。	13
II-7-7. Linuxサーバの運用手順	Linuxサーバの起動・停止から日常的な管理項目まで、Linuxサーバの運用に関する手順を説明する。とくにユーザの管理やディスク使用量の管理など、日常的に気を配る必要がある項目に焦点をあてて運用管理のノウハウを紹介する。	14
II-7-8. 日常運用におけるトラブルシューティング	日常の運用管理に必要となるログの取り扱いや、ログを用いたトラブルシューティング方法を紹介する。またパッケージ管理システムを利用したアプリケーションの導入など、日常運用で求められがちな作業手順についても説明する。	14
II-7-9. ネットワークのトラブルシューティング	ネットワークサービスの制御コマンドやネットワーク管理診断コマンド、ネットワークプリンタの設定やファイル共有に関する診断コマンドなど、ネットワークのトラブルシューティングに必要な知識について説明する。	15
II-7-10. ありがちなトラブルとその対策	Linuxサーバの運用を行う際に、サーバ自体の運用管理およびネットワークの設定や環境設定に関して、ありがちなトラブル事例を紹介し、その対策について解説する。	14,15

【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Ⅱ」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スキル	<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]	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. データ割り当てと変換	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]	CE-SWE11. ソフトウェアの標準化	
	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 [7-8] [7-9]	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	13	CE-CAO 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ネットワークサービス管理やサーバやネットワークのトラブルシューティングが含まれる。

科目名	第9回	第10回	第11回	第12回	第13回	第14回	第15回
7.Linux のシステム管理に関する知識Ⅱ	(1)ルーティングの仕様と設定 (2)ルーティングの仕様と設定	(1)Linux におけるDHCP の環境 (2)DHCP サーバ設定 (3)DHCP サーバ運用管理	(1)Linux におけるFTP サーバとは	(1)NFS とは (2)NFS の運用	(1)Samba とは (2)Samba サーバの設定(v3.0) (3)Samba クライアント (4)Samba のログ (5)Samba と NFS の共存	(1)サーバのトラブルシューティング(実 (2)日常運用のトラブルシューティング(実習)	(1)ネットワークのトラブルシューティング (2)よく起こるトラブルとその原因

(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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-1. ルーティングの設定	
対応する コースウェア	第 9 回 Linux システム管理･ルーティング管理	

II-7-1. ルーティングの設定

ルーティングの概念を簡単に示したうえで、Linux におけるネットワークルーティングの設定方法を説明する。ルーティングの設定手順を示し、さらにそのルーティング設定が正しく動作しているかどうかの検証方法についても述べる。

【学習の要点】

* ネットワーク通信を行うためには、目的地へ到達するための経路情報（ルーティング）を設定する必要がある。
* ルーティングには静的ルートと動的ルートがあり、通信先がどこに接続されているかを定義する「ルーティングテーブル」で管理を行う。
* ルータなど複数のネットワークインタフェースを持つ場合、IP アドレスにより送出するネットワークインタフェースを設定する。また、設定に合致しない場合の送出先としてデフォルトゲートウェイを設定する必要がある。
* 静的ルートはルーティング設定ファイルへ経路情報を記述する他、route コマンドにて経路情報の追加や削除を行う。
* route、traceroute コマンド等により、実際に設定されているルーティングの確認することができる。

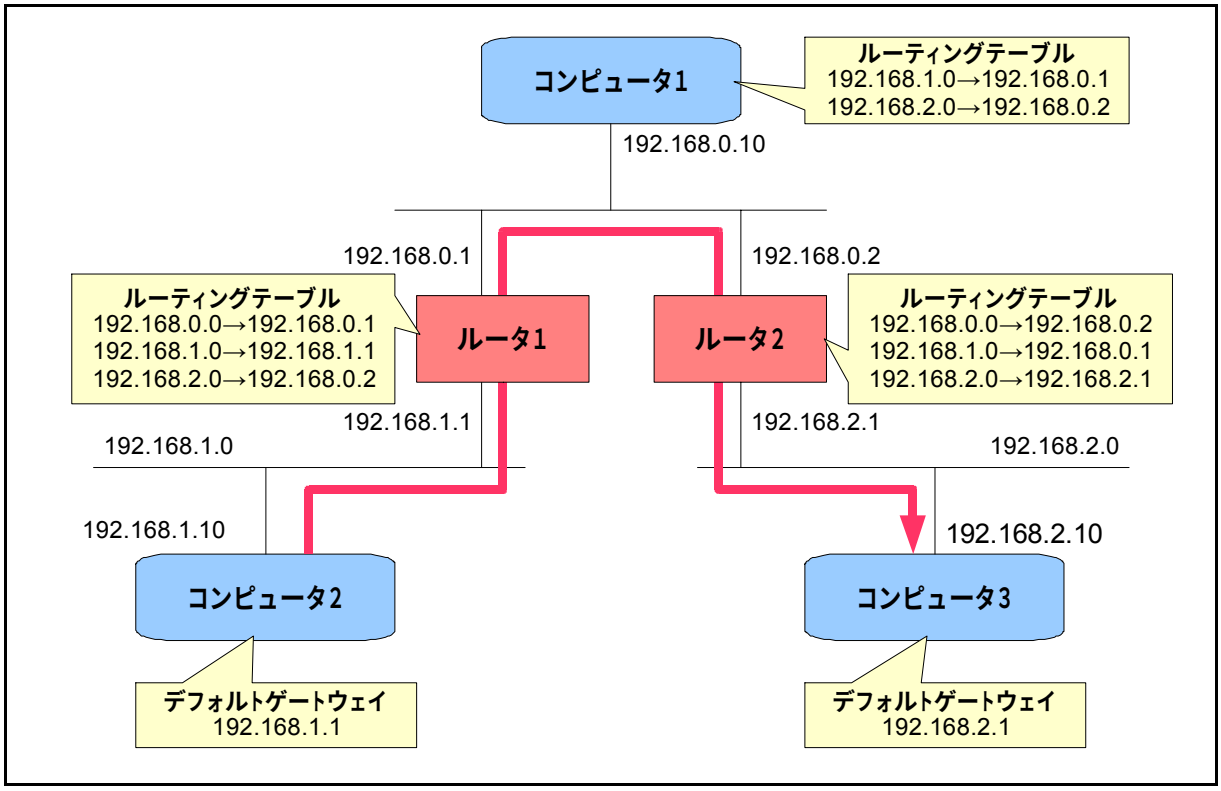

図 II-7-1.　ネットワークのルーティング

【解説】

1) ネットワークのルーティング

コンピュータに複数のネットワークインタフェースが接続されている場合や、複数のネットワークを経由して他のネットワークへ接続されているコンピュータと通信を行う場合、通信先がどのネットワークに接続されているか経路情報がわからなければ通信することができない。
この経路情報を見つけ出す方法のことを「ルーティング」と呼び、「ルーティングテーブル」によって管理されている経路情報を使用して通信経路を決定する。ルーティングテーブルは宛先となるネットワークアドレスと使用するネットワークインタフェースなどの情報を設定する。
宛先がルーティングテーブルに設定されているネットワークアドレスに一致すると、指定されたネットワークインタフェースへデータを送出する。どの情報にも一致しない場合は、デフォルトゲートウェイとして設定されているネットワークインタフェースへデータを送出する。
ルーティングには静的ルーティングと動的ルーティングがある。

* 静的ルーティング
  予め最適な経路を固定的に定義する。ルートが固定化されるためトラブルが発生した時に追跡が容易になるなどのメリットはあるが、ネットワークが変更されるたびにルーティングテーブルの設定を変更する必要がある。
* 動的ルーティング
  隣接したルータ間で経路情報を交換しあうことによって、自動的に最適な経路を取得する。ネットワークの変更があった場合でも設定のルーティングテーブルの設定を変更する必要はないが、ルートを探すためにブロードキャストを行うため、ルート探索がネットワークの混雑を引き起こすことがある。

2) 静的ルーティングの設定

* 設定ファイルによる設定
  ルーティング設定ファイルに経路情報を記述しておくと、ネットワークインタフェースの実行時にファイルに記述された経路情報を設定することができる。
  / etc/sysconfig/static-routes

```
any net 192.168.1.0 netmask 255.255.255.0 gw 192.168.0.1
any host 192.168.1.10 gw 192.168.0.1
```

* route コマンドによる設定
  route コマンドを使用すると、システムを起動後に静的ルーティングの追加や削除を行うことができる。また route コマンドはルーティングテーブルの状態を確認するためにも使用する。
  静的ルーティングの追加

```
# route add -net 192.168.1.0 255.255.255.0 eth0
# route add -host 192.168.1.10 eth0
```

3) ルーティングの確認

traceroute コマンドを使用すると、宛先となるコンピュータまでの経路の確認を行うことができる。

```
# traceroute computer3
```

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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-2. DHCP 環境の構築	
対応する コースウェア	第 10 回 Linux システム管理･DHCP の構築と運用	

II-7-2. DHCP 環境の構築

ネットワークの環境を動的に設定するためのプロトコルである DHCP の仕組みについて解説する。さらに Linux における DHCP の利用方法と、DHCP サーバの設定方法および DHCP サーバの運用管理方法についても説明する。

【学習の要点】

* DHCP はネットワークに接続するコンピュータに IP アドレスなど必要な情報の割り当てを自動的に行うプロトコルである。
* Linux では dhcpd と呼ばれるデーモンを利用してサービスの提供を行う。
* 設定ファイル (dhcpd.conf) によって、割り当てる IP アドレス、割り当てを行うコンピュータの制限などの設定を行う。
* DHCP による IP アドレスの割り当て状況等は syslog やリースファイルに記録される。割り当てを行う IP アドレスの過不足、不正アクセス等がないか定期的に確認を行う必要がある。

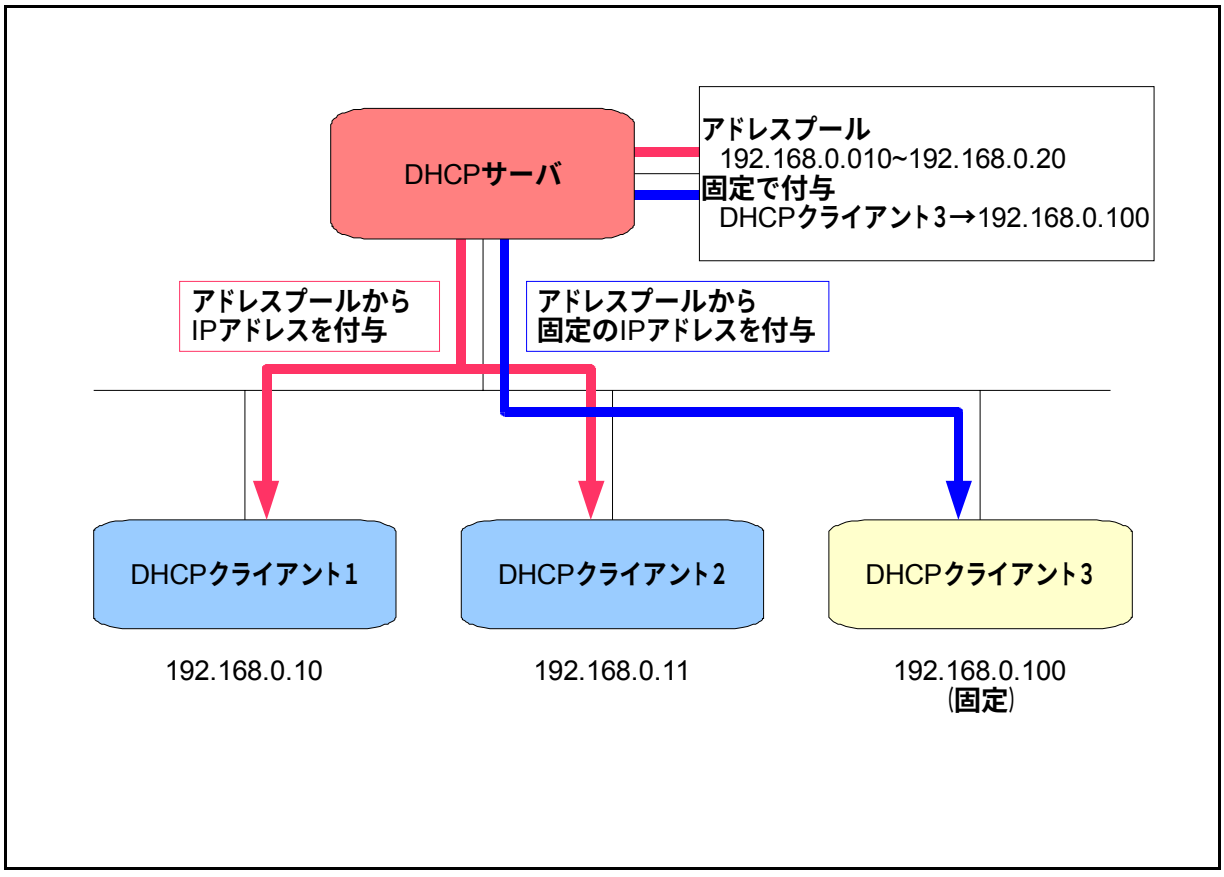

図 II-7-2.　DHCP の概要

【解説】

1) DHCP とは

DHCP（Dynamic Host Configuration Protocol）とは、コンピュータがネットワーク接続する際に、IP アドレス、ネットマスク、デフォルトゲートウェイ、DNS サーバアドレス等の情報を自動的に割り当てるためのプロトコルである。

DHCP サーバは予めクライアントへ割り当てるための IP アドレスのリスト（アドレスプール）を用意しておく。ネットワークへ DHCP クライアントのコンピュータを接続すると、DHCP クライアントは IP アドレスが 255.255.255.255 の UDP の要求メッセージを送信する。

メッセージを受信した DHCP サーバはアドレスプールから他のコンピュータで使用されていない IP アドレスを割り当て、DHCP クライアントへ通知を行う。

DHCP を利用する利点としては以下のような点が挙げられる。

* IP アドレス管理の省力化
  IP アドレスを固定で割り当てた場合、クライアントの追加やネットワークアドレスの変更の度に各クライアントへ IP アドレス等を正確に設定する必要がある。
  DHCP にて動的に IP アドレスを割り当てることにより、これらの設定作業が不要となる。

* IP アドレスの有効活用
  接続が必要なクライアントに対して、同時に接続するクライアント数が限られている場合、DHCP を利用することにより用意しておく IP アドレスを少なくすることができる。

DHCP サーバで動的に割り当てられる IP アドレスは同じコンピュータに対して常に同じ IP アドレスが割り当てられるとは限らない。

サーバなど他のコンピュータから IP アドレスでアクセスされるコンピュータの場合、固定の IP アドレスを割り当てる設定にしておく。これにより、該当するコンピュータから要求メッセージがあった場合、常に同じ IP アドレスを割り当てることができる。

2) DHCP サーバの設定方法

Linux では dhcpd サービスにより DHCP サーバを利用することができる。
dhcpd の設定は/etc/dhcpd.conf によって行い、主な設定項目は以下の通り。

- ダイナミック DNS の更新方法
- サブネットワークの情報
- アドレスプールの指定
- リリース時間の指定
- 固定で IP アドレスを割り当てるコンピュータの指定

3) DHCP のセキュリティ

DHCP はブロードキャスト型のサービスであり、ネットワークへ要求メッセージを送信できるコンピュータであれば、サーバ情報などを容易に取得することができる。これはセキュリティ上のリスクを抱えていることになる。

そのため、IP アドレスを割り当てるコンピュータの MAC アドレスなどの情報を事前に DHCP サーバへ登録しておき、登録されているコンピュータ以外への割り当ては行わないようにする。

また、DHCP では要求メッセージを受信したことと、割り当てた IP アドレスの情報を syslog にてログへ出力しており、不正な要求が無いか定期的に確認する。

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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-3. FTP サーバの設定	
対応する コースウェア	第 11 回 Linux システム管理･FTP の構築と運用	

II-7-3. FTP サーバの設定

FTP の概要を説明し、FTP サーバへのアクセスとサーバの動作について解説する。さらに Linux で動作する代表的な FTP サーバを紹介する。FTP サーバのインストールと設定、運用管理の手順について解説する。

【学習の要点】

* FTP(File Transfer Protocol)サーバはネットワークに接続しているコンピュータ間でファイルの送受信を行うためのサーバである。
* FTP は制御ポートとデータポートの 2 つのポートにより接続を行い、データポートは FTP サーバが設定するが、「Passive モード」を利用するとクライアントから設定することもできる。
* 一般的な FTP サーバとして、vsftpd のインストールおよび設定を行う。
* FTP の使用状況の確認や不正アクセスの監視を行うため、定期的にログファイル等の確認を行う必要がある。

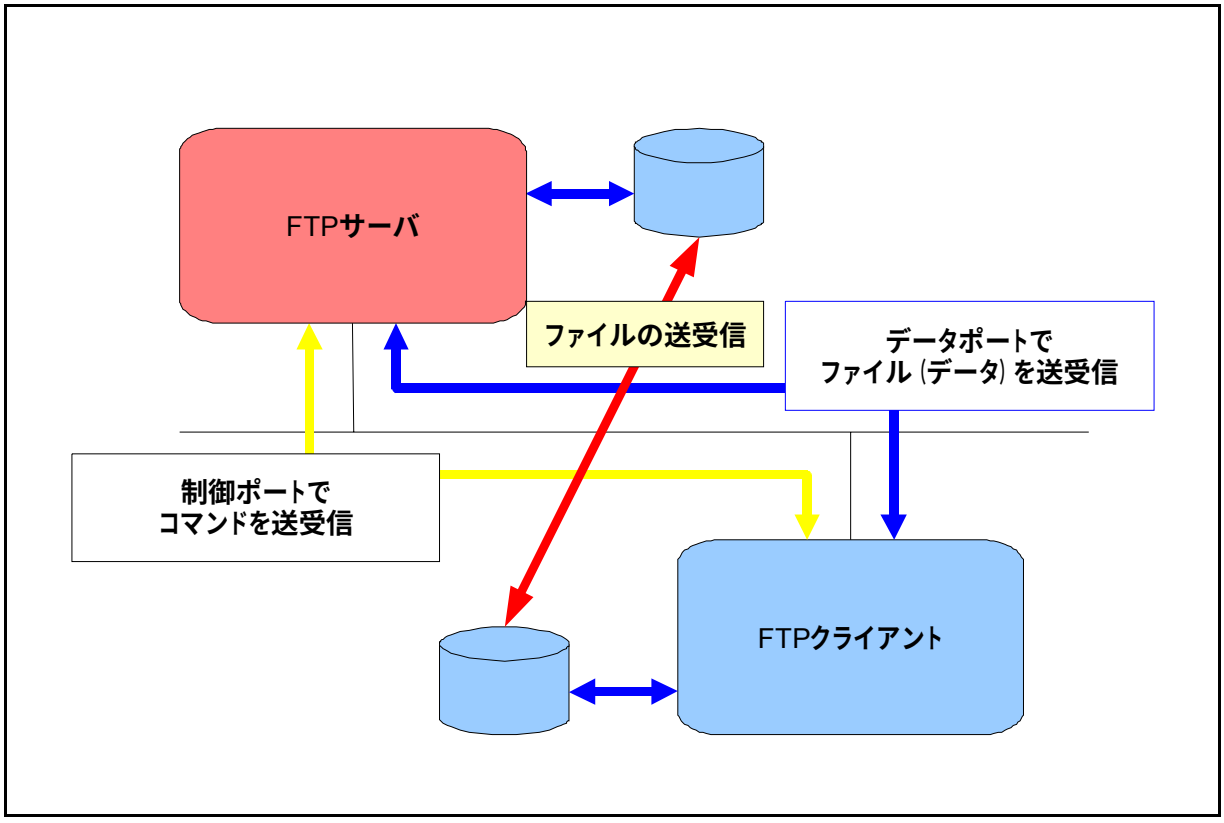

図 II-7-3.　FTP の概要

【解説】

1) FTP とは

FTP (File Transfer Protocol) はコンピュータ間で明示的にファイルを指定して転送するプロトコルである。

FTP の特徴としては以下のような点が挙げられる。

* 異機種間接続機能
  Linux と Windows など異なるファイルシステムの間でファイルの転送ができる。
* 匿名による認証のサポート
  不特定多数のユーザにファイル転送サービスを提供できる。

2) ＦＴＰによるファイル転送

FTP は制御ポートとデータポートの 2 つのポートを利用して接続を確立する。

クライアントからＦＴＰの接続要求が来ると、制御ポートにて接続および認証を行う。その後制御ポートにてコマンドの送信と応答が行われ、データの転送が必要になるとデータポートの接続を行いデータポートにてデータの送信を行う。

データポートの接続では、サーバからクライアントへ使用するポート番号を通知し、クライアントがこのポート番号でサーバへ接続を行う。ファイアウォールなど制限されたネットワークではサーバが通知したポート番号が使用できない場合がある。この場合はクライアントから接続するポート番号の候補を通知し、その中から使用するポート番号をサーバから通知を行う「Passive モード」にて接続を行う。

FTP で転送するデータタイプとしては、ASCII コード、EBCDIC コード、バイナリデータなどがあり、転送モードとしてはストリームモード、ブロックモード、圧縮モードが指定できる。

3) FTP サーバの設定

Linux では vsftpd サービスにより FTP サーバを利用することができる。
vsftpd の設定は「/etc/vsftpd/vsftp.conf」、「/etc/vsftpd/ftpusers」によって行い、主な設定項目は以下の通り。

- 匿名 FTP サーバの設定
- ユーザログインの設定
- FTP コマンドでのデータの書き込みの設定
- 転送ログ出力の設定
- ユーザの UMASK の設定
- アクセス拒否ユーザの設定
- tcp_wrappers 利用の設定

4) FTP のセキュリティ

匿名 FTP サーバとして設定した場合、不特定多数のユーザからのアクセスが行われるため、オプションの設定により十分なセキュリティを確保する必要ある。

FTP では認証時のログ、ファイル転送に関するログ、vsftpd の動作に関するログを出力する。これらのログを定期的に解析し統計情報を作成することにより、不正なアクセスの有無の調査や使用状況の確認を行う必要がある。

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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-4. ファイル共有	
対応する コースウェア	第 12 回 Linux システム管理･NFS の構築と運用 第 13 回 Linux システム管理･Samba の構築と運用	

II-7-4. ファイル共有

ネットワーク上におけるファイル共有の考え方について述べる。ファイル共有には様々な方法があることを示し、それぞれのファイル共有手法の特徴と歴史、代表的なサーバ、利用例などを紹介する。

【学習の要点】

* コンピュータ上にあるファイルを、ネットワークを経由して複数人でアクセスできる状態におくことをファイル共有という。
* ファイル共有の方法としてはクライアント･サーバ方式、P2P 方式などがあるが、これらはファイルの内容が非同期である。
* クライアント･サーバ方式は、HTTP や FTP など共有するファイルをサーバへアップロードまたはダウンロードすることによりファイルの共有を行う。
* P2P 方式はサーバを持たず、ファイルを共有するコンピュータ間でファイルの転送を行うことによりファイルの共有を行う。
* ファイルの内容が同期する方法としては、Linux では NFS、Windows では SMB(CIFS)、Mac OS では AppleShare という方式が使用されている。

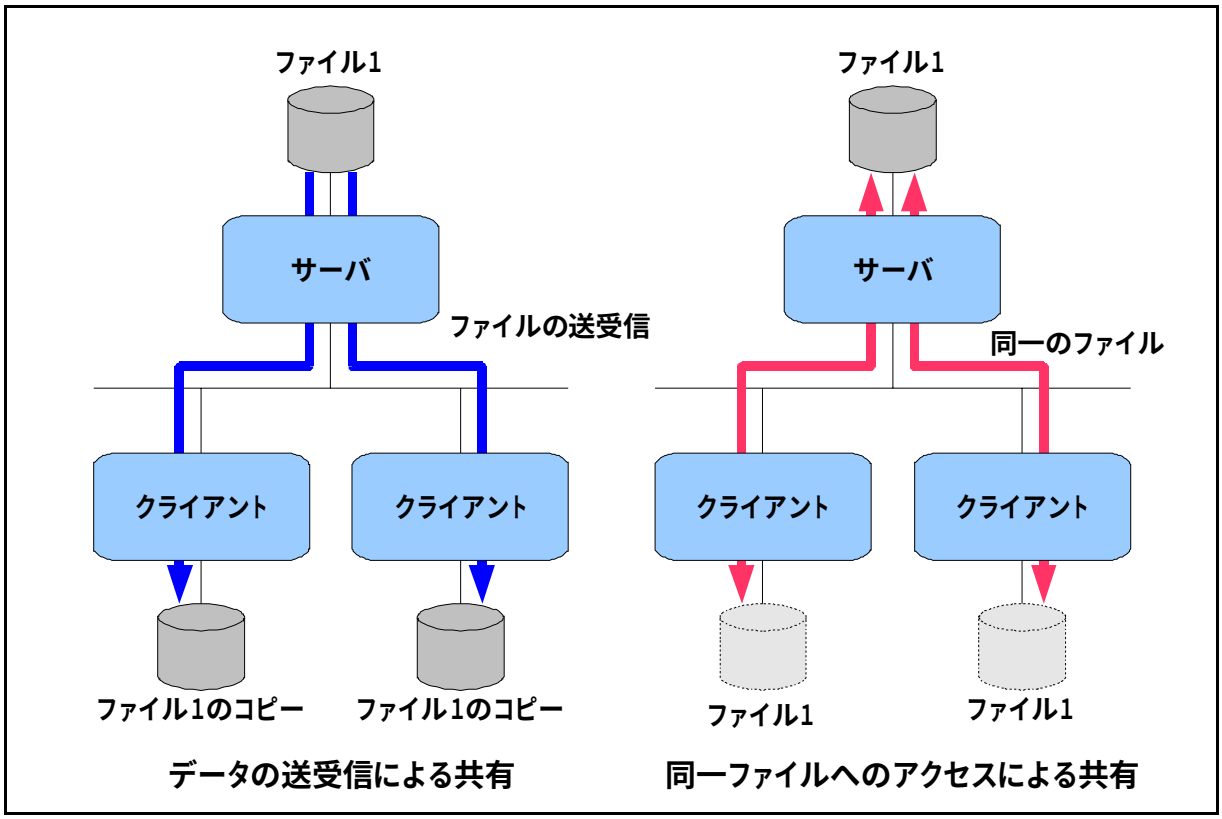

図 II-7-4.　ファイル共有

【解説】

1) ネットワーク上のファイル共有とは

情報の公開や、共同で作業をする際にデータの同期を図る場合など、あるコンピュータ上にあるファイルを、ネットワーク経由で他のコンピュータから複数の人がアクセスできる状態におくことをファイル共有という。通常、ファイル共有ではデータの同期性が保障されているものを指すが、広義ではファイルの送受信によりデータの同期性が保障されていないものも含まれる。

2) データが非同期のファイル共有

ファイルの送受信により同じファイルを取得することによりファイル共有を行う。受信側では送信側のファイルのコピーを保持しているため、送信側でファイルの変更があった場合でも受信側のファイルには変更が反映されない。

このファイル共有の方法は、クライアント・サーバ方式と P2P 方式の2つに大きく分けられる。

* クライアント・サーバ方式

共有を行うファイルを全てサーバ上で管理をし、クライアントからファイルのダウンロードやアップロードを行う。HTTP や FTP などを利用したファイル共有がこれにあたる。

共有の元となるファイルが一元管理されているため、変更があった場合でも即座に反映される。

* P2P 方式

ファイルの送受信がサーバを介さずにコンピュータ間で行われる。BitTorrent や Cabos などを利用したファイル共有がこれにあたる。

共有するファイルを持っている複数のコンピュータ（ノード）から最適なコンピュータを選択しファイルのダウンロードを行うため、ファイルダウンロードの効率は良くなるが、元となるファイルに変更があった場合でも、ダウンロード先のファイル反映されているとは限らない。

3) ファイルが同期しているファイル共有

1つのファイルに同時にアクセスできるようにファイル共有を行う。送信側と受信側では同じファイルにアクセスを行っているため、送信側でファイルの変更があった場合、受信側でも変更が即時に反映される。

このファイル共有の方法は、サーバとなるコンピュータでファイルを共有するファイルシステムまたはディレクトリなどの領域を提供し、これをクライアントとなるコンピュータから使用することにより、サーバとクライアント間、クライアントとクライアント間でファイルの共有を行う。

Linux で利用されるファイル共有としては、主に Linux 間で使用する「NFS」や、Linux と Windows 間で使用する「Samba」などがこれにあたる。

Windows では SMB（Server Message Block）プロトコルを利用した、ファイルやプリンタの共有がこれにあたる。

Mac OS では AppleTalk プロトコルを利用した AppleShare によるファイルやプリンタの共有がこれにあたる。

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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-5. NFS の設定と運用	
対応する コースウェア	第 12 回 Linux システム管理･NFS の構築と運用	

II-7-5. NFS の設定と運用

UNIX で利用されてきた代表的なファイル共有の手法である NFS について解説する。NFS とは何か、Linux サーバにおける NFS の設定手順、 NFS クライアントの設定といった具体的な設定方法を説明し、NFS の運用管理に必要なノウハウについても触れる。

【学習の要点】

* NFS(Network File System)はネットワークに接続された Linux 間でファイルシステムを共有するためのシステムである。
* NFS サーバでは設定ファイル (/etc/exports) により共有するディレクトリやアクセスするユーザおよびコンピュータの設定等を行う。
* NFS クライアントは、mount コマンドによる手動、または fstab へ設定することで起動時に自動で NFS サーバのファイルシステムを共有することができる。
* NFS サーバーログ機能により NFS の読み取りと書き込み、および対象とするファイルシステムを変更する操作の記録を行う。

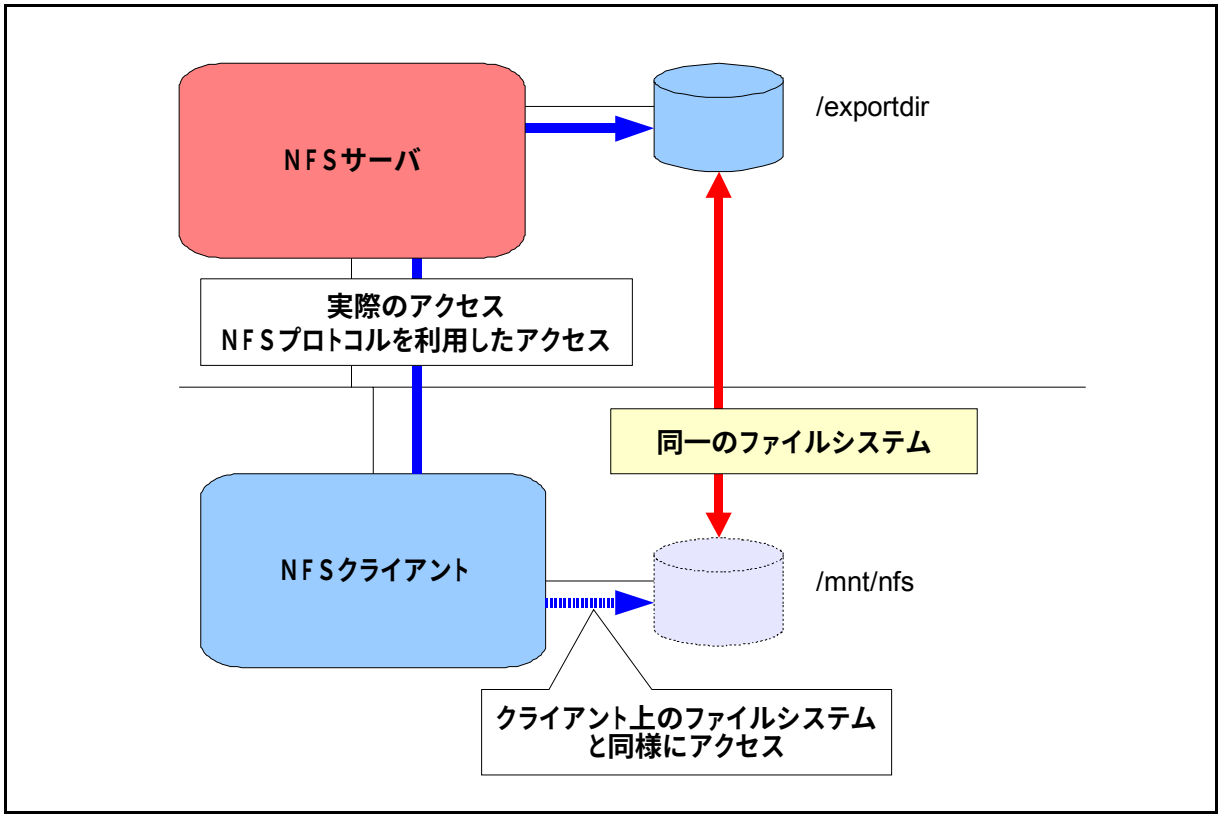

図 II-7-5. NFS の概要

【解説】

1) NFS とは

ＮＦＳ（Network File System）はサーバ上にあるファイルシステムを、クライアントでマウントすることにより、クライアント上にあるファイルシステムと同様に使用できるサービスを提供するものである。

このサービスを利用することにより、サーバにあるファイルもクライアントにあるファイルと区別することなく同様に操作を行うことが可能となる。

また、ＦＴＰと同様にファイルシステムの違いを吸収できる異機種間接続機能を持っているため、Linux と Windows などＯＳの違うコンピュータ間でもサービスを利用することができる。

NFS クライアントへ共有の許可を出すことを「エクスポート」と呼ぶ。

NFS では複数のポート番号を利用して接続を行う。NFS サーバが NFS クライアントから接続の要求を受け取ると、ポート番号を保管しているポートマッパーから接続を行うポート番号を取得して接続を行う。

2) NFS サーバの設定

Linux では nfsd サービスにより NFS サーバを利用することができる。

nfsd は/etc/exports により、NFS サーバ上のどのファイルシステムを他のコンピュータが共有してよいのか設定を行う。さらに、オプションとして、ディレクトリに対するアクセス制限などのファイル属性や、サーバとクライアントのユーザ ID やグループ ID の対応方法を設定する「ユーザ属性」を指定することができる。

/etc/exports の設定例

```
/exportdir      192.168.0.0/255.255.255.0(rw,no_route_squash)
```

/etc/exports に設定した内容を有効にするためには、exportfs コマンドを使用する。

showmount コマンドにて、NFS マウントしているクライアントの情報を確認することができる。

3) NFS クライアントの設定

NFS サーバにて提供されている共有ファイルを使用するためには、他のファイルシステムと同様に mount コマンドにて NFS マウントを行う。

```
# mount -t nfs -o nfsvers=3 nfsserver:/exportdir /mnt/nfs
```

/etc/fstab へマウント情報を記述することにより netfs サービスを利用してシステムを起動した時に自動的にマウントを行うことができる。

また、automount コマンドを使用することにより、ファイルシステムの利用に応じて自動的にマウント／アンマウントを行うことができる。

4) NFS のセキュリティ

NFS で読み書き込み可能な状態でマウントした場合、クライアント側のユーザ権限にてファイルへのアクセスが可能となる。これによりクライアントにて root 権限を持ったユーザで利用すると NFS で共有されたファイル全てにアクセス可能な状態になる。これを防ぐためには、/etc/exports にて root でアクセスがあった場合匿名ユーザとしてアクセスを行うように設定を行っておく必要がある。

NFS サーバでは、クライアントの認証結果やサーバから呼出しや書き込みを行ったファイルの情報を syslog へ出力する。このログから NFS の利用状況や不正なアクセスが行われていないか定期的に確認する必要がある。

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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-6. Samba の設定と運用	
対応する コースウェア	第 13 回 Linux システム管理･Samba の構築と運用	

II-7-6. Samba の設定と運用

Linux と Windows でデータを共有するための Samba について説明する。Samba とは何か、Samba のインストール方法、Samba サーバの設定方法、Samba クライアントの利用法など、Samba の導入から運用に至るまでに必要な知識を紹介する。

【学習の要点】

* Samba は Linux と Microsoft Windows との間でファイルやプリンタといった資源を共有するためのソフトウェアである。
* Samba は Linux のサービスとして起動され、smbd および nmbd の 2 つのプログラムで構成される。
* Samba サーバでは設定ファイル (smb.conf) により参加するワークグループ、共有するディレクトリやアクセスするユーザおよびコンピュータの設定等を行う。
* Microsoft Windows からはネットワークコンピュータとしてアクセスすることが可能であり、Linux からは samba-client を使用してアクセスを行う。
* Linux と Microsoft Windows が混在しているネットワーク環境では、NFS と共存させることも可能であるが、ファイル名に日本語を使用する場合には注意が必要となる。
* Samba ではサービスの起動状態を出力するログファイルと、Samba サーバへ接続したクライアントの状況を出力するログファイルを作成する。

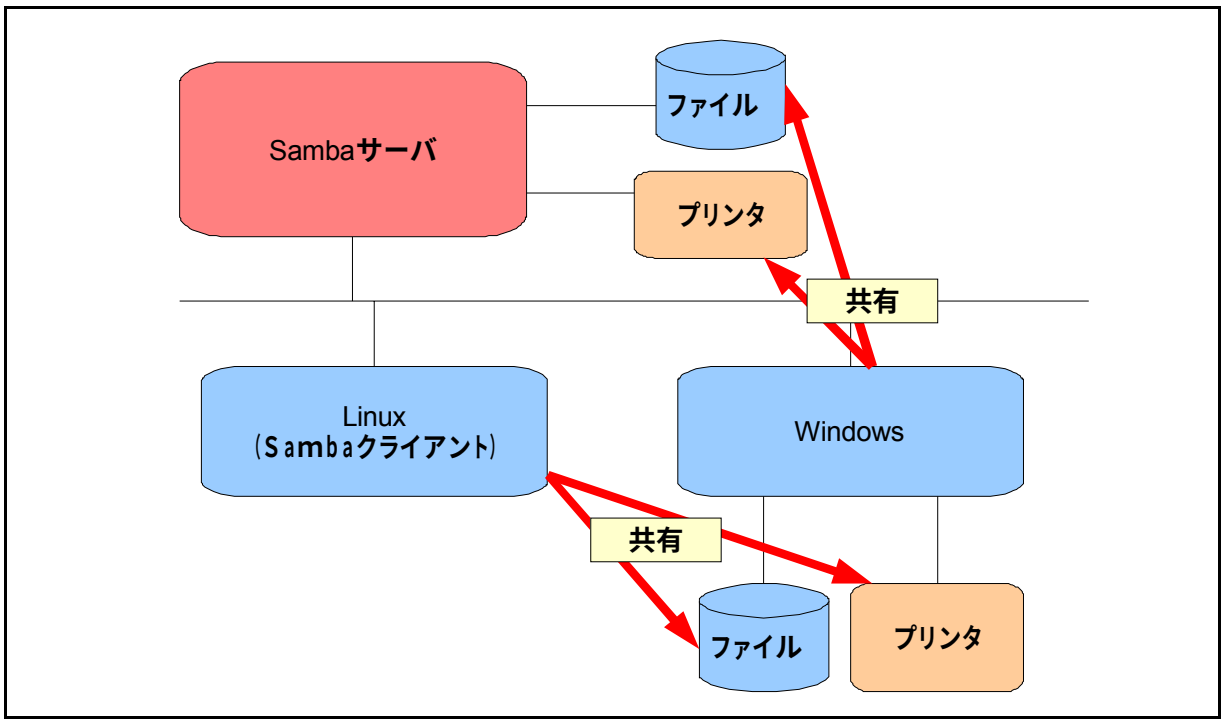

図 II-7-6.　Samba の概要

【解説】

1) Samba とは

Samba は Windows の NetBEUI (NetBIOS Extended User Interface) を Linux 上で実現するもので、Linux と Windows との間でファイル共有や印刷などの機能を提供するものである。

Samba はファイル共有だけでなく、Windowsドメインコントローラの仕組みも提供しているため、Linux サーバで Windows サーバと同様のサービスを提供することができる。

Samba は TCP/IP 上でネットワークの処理を行う NetBIOS と、ファイルや印刷を共有するサービスを提供する SMB (Server Message Block) の2つのプロトコルを使用している。

Samba サーバの共有ファイルへアクセスする際の認証としては大きく分けて Windows ワークグループで実装されている「共有レベルのセキュリティ認証」と Windows ドメインネットワークで実装されている「ユーザレベルのセキュリティ認証」の2つがあるが、現在では「ユーザレベルのセキュリティ認証」が標準となっている。

日本語ファイル名については、Linux と Windows では使用している文字コードの違いがあるため、各々の環境で使用する文字コードの設定をする必要がある。また、Windows では大文字と小文字の区別をしていないため、大文字と小文字が混在しているファイル名の扱いについても予め設定する必要がある。

2) Samba サーバの設定

Samba は SMB の機能を提供するsmbdと、NetBIOS の通信を行う nmbd で構成されている。

Samba の設定は「/etc/samba/smb.conf」、「/etc/lmhosts」によって行い、主な設定項目は以下の通りである。

- ワークグループ名の設定
- アクセスを許可する IP アドレスの設定
- パスワードファイルの設定
- プリンタ共有の設定
- 文字コードの設定
- 共有するディレクトリの設定
- NetBIOS 名と IP アドレスの関係情報の設定

Windows クライアントから Samba サーバへアクセスする際に使用するユーザ ID やパスワードは smbpasswd コマンドを使用してパスワードファイルを作成し管理を行う。

3) クライアントからの利用方法

Windows クライアントから Samba サーバへ接続する場合は、Windows ファイル共有機能を利用し、「マイネットワーク」で共有ディレクトリを検索して共有を行う。

Linux から Windows 環境のファイル共有へ接続する場合は smbclient コマンド (samba-client) を使用し、コンピュータ名と共有名を指定してファイルの共有を行う。

4) Samba のセキュリティ

「ネットワークインタフェースによるアクセス制限」、「IP アドレスによるアクセス制限」および「ユーザ名によるアクセス制限」を設定することにより、セキュリティを確保することができる。

Samba では、smbdおよび nmbd の動作状態に関するログの他、接続したクライアント毎にアクセルログを出力する。これらから不正なアクセスが無いか、定期的に確認する必要がある。

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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-7. Linux サーバの運用手順	
対応するコースウェア	第 14 回 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	

II-7-7. Linux サーバの運用手順

Linux サーバの起動･停止から日常的な管理項目まで、Linux サーバの運用に関する手順を説明する。とくにユーザの管理やディスク使用量の管理など、日常的に気を配る必要がある項目に焦点をあてて運用管理のノウハウを紹介する。

【学習の要点】

* Linux サーバの運用に必要な管理手順を実際に Linux を操作しながら理解する。
* サーバの起動と停止を行う。
* ユーザ管理ポリシーに準拠しユーザの追加･変更･削除を行う。
* デバイスの追加･交換などによるパーティションの作成やマウントを行う。
* サーバ管理コマンドによるサーバの負荷情報（CPU、メモリ、ディスクの使用量など）の確認を行う。

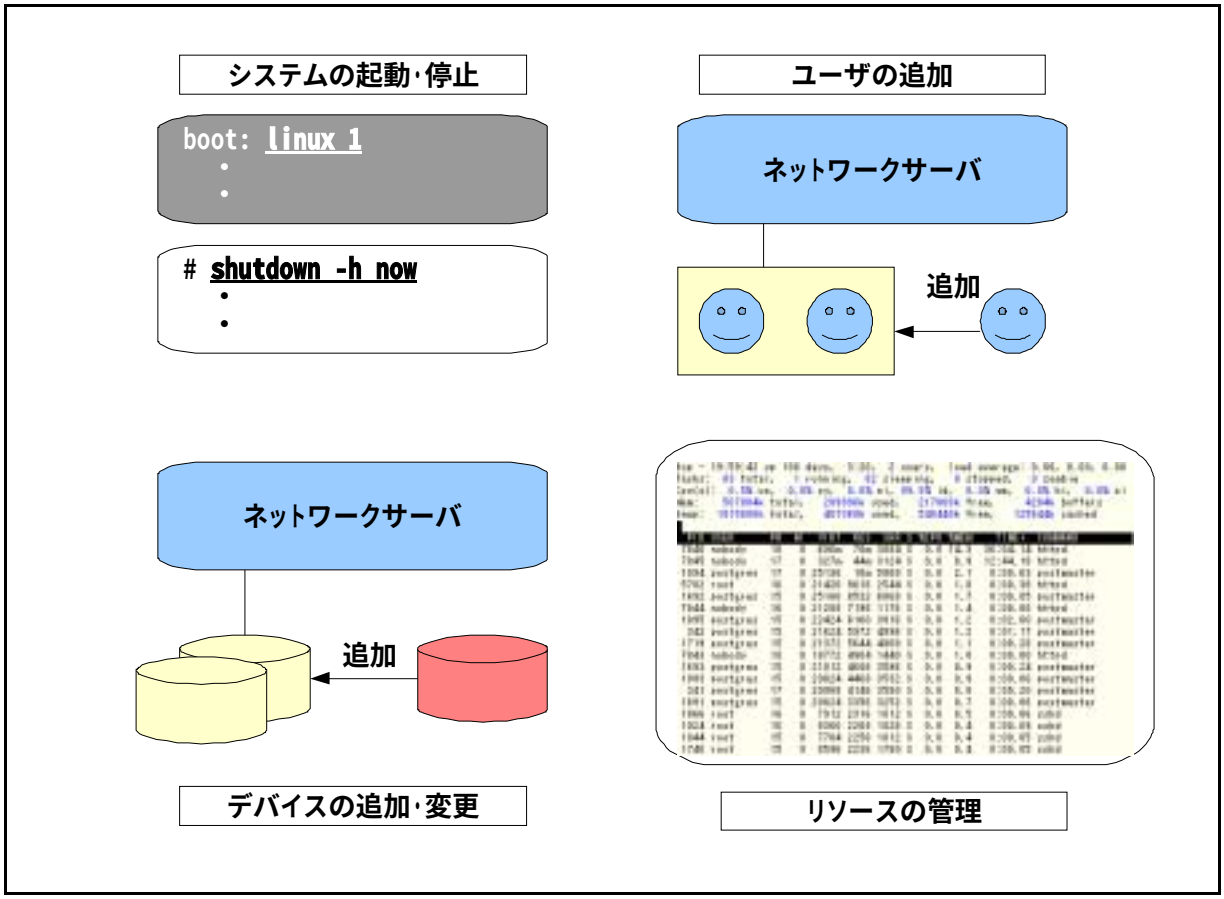

図 II-7-7.　運用管理作業の例

【解説】

1) 起動と停止

Linux を起動すると、init プログラムが実行される。Init プログラムではシステムの実行状態を表す「ランレベル」を指定することができる。ランレベルは0から6までの数値で指定する。
ランレベルはディストリビューションにより異なるが、代表的な実行状態を以下に示す。

* ランレベル0、6　：ランレベル0はシステムの停止、ランレベル6はシステムの再起動。
* ランレベル1　：ランレベル1はシングルユーザモードの状態で、root によるログインが出来なくなった場合や、通常の起動が出来なくなった場合に使用する。システムのバックアップの際にも使用する。
* ランレベル3、5　：ランレベル3、5は通常のシステム起動に使用し、ランレベル3はテキストモード、ランレベル5は GUI モードで起動する。

システム実行中でも、上記のランレベルを指定してinitコマンドを実行することにより、指定した状態へ移行することができる。また、システムの停止、再起動は shutdown コマンドでも行える。

2) ユーザの追加

システムの利用者の変さらに伴い、一般ユーザの追加、変更および削除の作業が必要になる。
ユーザを管理する際には、システムの利用範囲や組織構成を明確にしたユーザ管理ポリシーを作成し、これに沿って行う必要がある。以下のようなコマンドでユーザの管理を行う。

* useradd　：ユーザの新規作成。
* userdel　：ユーザの削除。
* passwd　：パスワードの変更

3) デバイスの追加、変更

障害が発生したハードディスクの交換や、新規に追加したデバイスを使用可能な状態にするには、パーティションの作成およびマウントが必要となる。以下のようなコマンドでデバイスを使用可能な状態にする。

* fdisk コマンド　：デバイスにパーティションを作成し、ファイルシステムの設定を行う。
* mount コマンド　：作成したパーティションをマウントし使用可能な状態にする。起動時に自動的にマウントするには/etc/fstab に設定を記述する。

4) リソースの管理

サーバ管理においては CPU、メモリ、ハードディスク、ネットワークなどのリソースを監視し、負荷状況を管理する必要がある。以下のようなコマンドでリソースの状態を確認することができる。

* ps コマンド　：起動中のプロセスの実行状態や CPU、メモリの使用状況を表示。
* vmstat コマンド　：CPU やメモリ、SWAP ファイルなどの使用状況を表示。
* free コマンド　：物理メモリおよび仮想メモリの使用状況など、メモリの詳細情報を表示。
* df コマンド　：各ハードディスクのパーティション情報として、パーティションのサイズや使用状況を表示。
* top コマンド　：CPU の使用率、プロセス数、待ちプロセス数、優先度、SWAP の使用量, 空きメモリ量など、様々な情報を表示する。

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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-8. 日常運用におけるトラブルシューティング	
対応するコースウェア	第 14 回 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	

II-7-8. 日常運用におけるトラブルシューティング

日常の運用管理に必要となるログの取り扱いや、ログを用いたトラブルシューティング方法を紹介する。またパッケージ管理システムを利用したアプリケーションの導入など、日常運用で求められがちな作業手順についても説明する。

【学習の要点】

* システム運用におけるトラブルの防止や早期発見を行うためにはシステムログの確認やソフトウェアのアップデート等を行う必要がある。
* 不正アクセス等があった場合、痕跡など重要な情報はシステムログに記録されるため、日常的に確認を行うことで異常値の発見がしやすくなる。
* システムログは膨大になるため、問題を迅速に発見するために、cron などを用いて解析ツールを定期的に起動するようにしておくべきである。
* トラブル発生に備え、tar コマンドや dump コマンドを用いて定期的にシステムのバックアップを行う。
* セキュリティ強化のため、セキュリティパッチ等がリリースされた場合はパッケージ管理にてシステムのアップデートを行う。

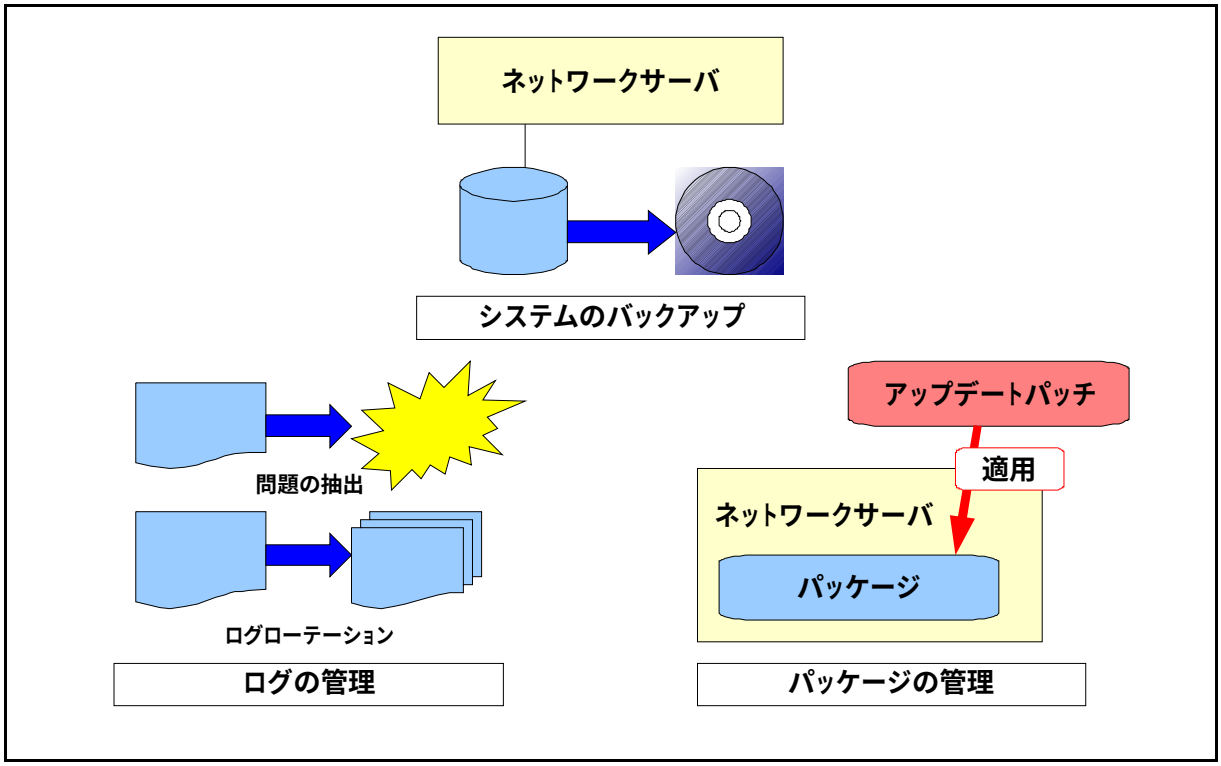

図 II-7-8.　日常的な運用操作

【解説】

1) ログの収集／解析

ネットワークサーバの運用では、提供するサービスが問題なく提供されているか監視を行う必要がある。また、問題が発生した場合原因がどこにあるのかを迅速に確認する必要がある。

Linux では syslog によってサーバのログを記録し、定期的にログの確認を行うことにより、サービスの監視および問題が発生した時の原因の究明を行うことができる。

syslog によって記録されるログは膨大な量となるため、以下のようなツールを導入し問題のあるログを容易に発見できるようにする。

* logwatch コマンド

ログファイルには様々な情報が出力されるため、その中から問題のある情報を抜き出す作業は大変である。logwatch は予め問題として判定するログの条件を設定しておき、条件に一致したログを抽出し表示を行う。

問題を迅速に発見するため、cron にて 1 日に 1 回は実行する。

* logrotate コマンド

ログファイルを出力したログファイルをそのまま使用していると、サイズが大きくなりすぎて記憶領域を圧迫したり、確認を行う際に範囲が広すぎて時間が掛かるなど問題が発生する可能性がある。logrotate コマンドを実行すると、現在のログファイルのファイル名を変更し、新規に空のログファイルを作成し、ログファイルのローテーションを行う。

ログファイルのローテーションは cron にて定期的に実行する。

2) システムのバックアップ

トラブルの発生によりシステムが破壊された場合、システムを破壊前の状態に復旧する必要がある。システムの設定ファイルや、ユーザが保存したデータなど復旧に必要なデータは定期的にバックアップを行う必要がある。全てのデータのバックアップや、前回のバックアップからの差分をバックアップする方法がある。

バックアップのためのコマンドとしては、tar コマンドや dump コマンドがある。

3) パッケージ管理

システムやネットワークサービスのプログラムへセキュリティ上の脆弱性が発見された場合など、アップデート用のプログラムやパッチが提供される。サーバのセキュリティを維持するには、パッチの提供を随時確認し、提供後は速やかにアップデートを適用する必要がある。

システムやネットワークサービスのアップデートを行う方法としては、yum(Yellow dog Updater Modified)や apt-get コマンドなどがある。

アップデートを迅速に適用するため、定期的に実行し常に最新の状態にしておくことが望ましいが、プログラムの依存関係によってはアップデート後にプログラムが動作しなくなる場合もあるため、注意が必要となる。

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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-9. ネットワークのトラブルシューティング	
対応するコースウェア	第 15 回 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	

II-7-9. ネットワークのトラブルシューティング

ネットワークサービスの制御コマンドやネットワーク管理診断コマンド、ネットワークプリンタの設定やファイル共有に関する診断コマンドなど、ネットワークのトラブルシューティングに必要な知識について説明する。

【学習の要点】

* ネットワークにおけるトラブルの防止や早期発見を行うためには、各種管理コマンドを使用した定期的な監視を行う必要がある。
* chkconfig コマンド等を使用して、サーバにインストールされているネットワークサービスの一覧や起動方法を確認し、不要なサービスが無いか確認し設定の変更を行う。
* ネットワーク管理診断コマンド(ping,netstat,traceroute 等)を使用して、サーバのネットワーク状況に問題がないか、また問題が発生した時の原因の究明を行う。

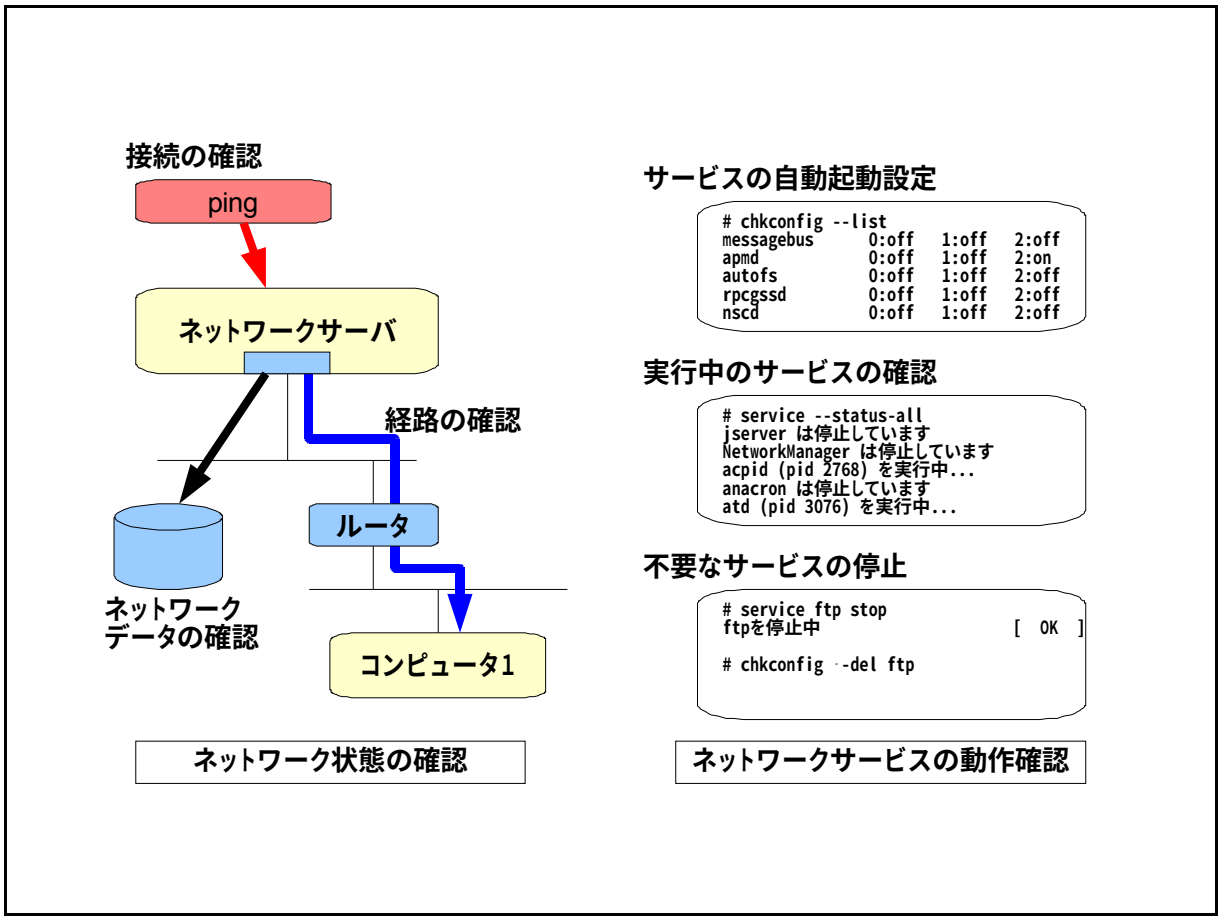

図 II-7-9.　ネットワークの監視

【解説】

ネットワーク内の通信が混雑していたり、一部の機器が異常な動作をしていないかなどを日常的に確認することは、トラブルを未然に防いだりセキュリティを保持するために重要な作業である。

以下のようなコマンドを使用し定期的に状態を確認、検証することにより、異常値の早期発見が可能となる。

1) ネットワーク状態の確認

以下のようなコマンドを使用することにより、ネットワークの状態を確認することができる。

* ping コマンド

ping コマンドは、宛先として指定したコンピュータとの接続がされているか確認するもので、ネットワークに接続されている機器に対して ping コマンドを定期的に実行し応答の有無や応答が返ってくる時間により、障害の発生やネットワークの混雑状態を把握することができる。

* tracetoute コマンド

traceroute は宛先として指定したコンピュータまでの通信経路情報を確認するもので、ルーティングの設定が正しく行われているのか確認を行い、ping コマンドにて応答が返ってこない場合、どこで通信経路が切断されているかなどを確認することができる。

* netstat コマンド

netstat コマンドはネットワークに対する総合的な情報を取得し出力を行うもので、実行中のネットワークサービスの状態や接続しているクライアントの情報などを確認することができる。

* tcpdump コマンド

tcpdump コマンドは、ネットワーク上のデータを調査するもので、ネットワークインタフェースに到着するパケットを全て取り込んで出力を行う。この出力結果を解析することにより、不正な使用が行われていないか、データが流れていないかなどを確認することができる。

その他、SNMP(Simple Network Management Protocol)を利用して、ネットワークに接続されている機器の状態をネットワーク経由で管理を行い、MRTG（Multi Router Traffic Grapher）を利用してネットワークの負荷を監視することができる。

2) ネットワークサービスの動作確認

ネットワークサーバで稼動するネットワークサービスが増えるほど、セキュリティ上の危険も増加する。セキュリティ上のリスクを最小限に抑えるためには、必要なサービスのみを利用し、不必要なサービスは停止しておく。

以下のようなコマンドを使用することにより、ネットワークサービスの管理を行うことができる。

* chkconfig コマンド

chkconfig コマンドは、システム起動時に自動的に起動するネットワークサービスなどの追加、変更、削除を行うものである。

システム起動時に不要なサービスまで起動することになっていないか確認を行い、不要なサービスがあれば起動しないように設定を行う。

* service コマンド

service コマンドは、実行中のネットワークサービスの確認、起動、停止などを行うものである。

必要なサービスの停止や、不要なサービスが実行されていないか監視を行い、必要に応じてサービスの再起動や停止を行う。

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 のシステム管理に関する知識 II	応用
習得ポイント	II-7-10. ありがちなトラブルとその対策	
対応する コースウェア	第 14 回 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 第 15 回 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	

II-7-10. ありがちなトラブルとその対策

Linux サーバの運用を行う際に、サーバ自体の運用管理およびネットワークの設定や環境設定に関して、ありがちなトラブル事例を紹介し、その対策について解説する。

【学習の要点】

* 発生するトラブルはパスワード忘れなど運用のミスに起因するもの、ハードウェア障害などサーバ自体に起因するもの、ネットワークの遮断など外部要因に起因するものなどがある。
* 日常運用でよく発生するトラブルの把握とその対応方法を理解する。

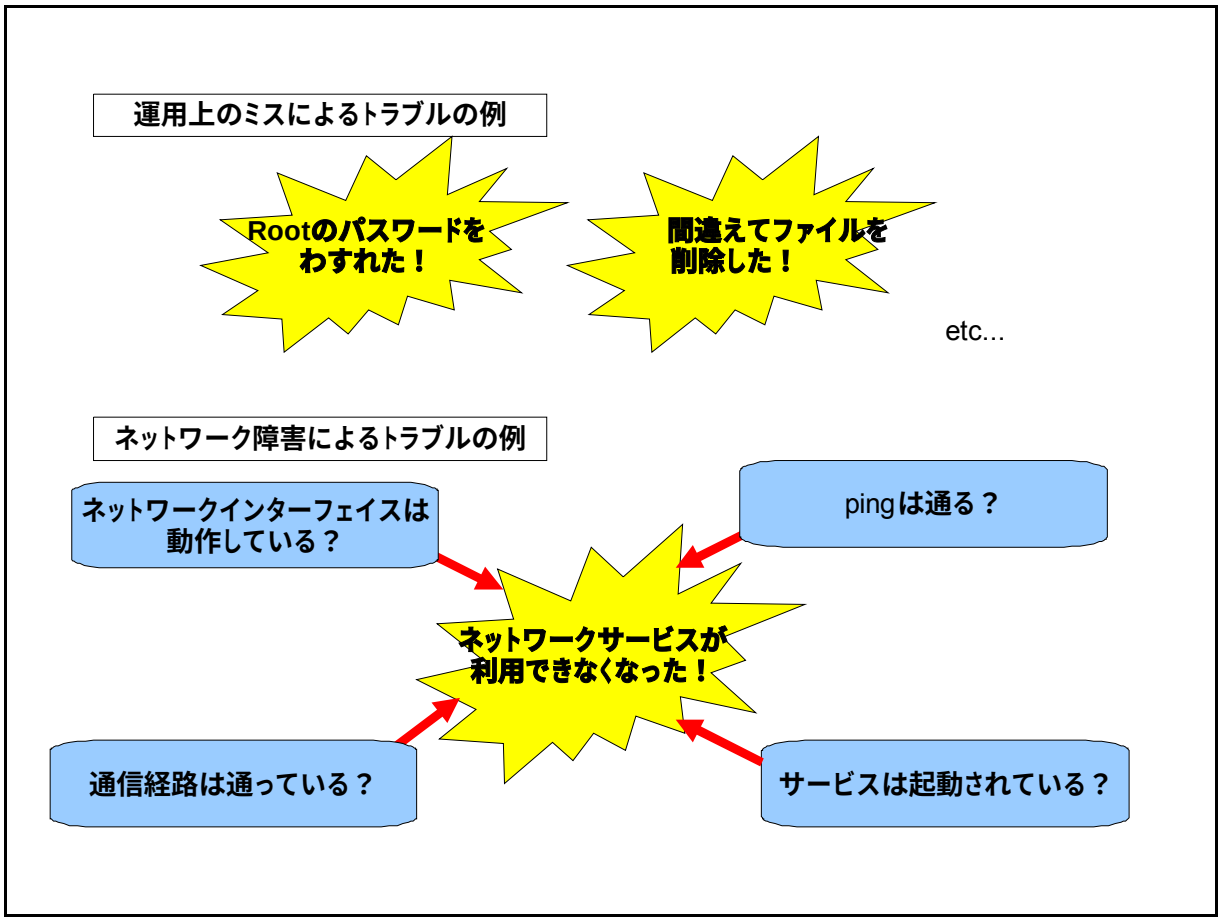

図 II-7-10.　ありがちなトラブルの例

【解説】

Linux サーバ運用中に発生するトラブルについて、その対応方法を確認する。特にネットワーク障害などは様々な要因により発生するため、いくつかのコマンドを組み合わせて原因の追究を行い、的確な対応を行う必要がある。

1) 運用上のミスによるトラブルの例

* root のパスワードを忘れた

root のパスワードを忘れてしまった場合、以下の手順でパスワードの再設定を行う。

i) システムをシングルユーザモードで起動する。

boot: Linux 1

ii) プロンプトが表示されたら passwd コマンドで root のパスワードを設定する。

passwd root

* 誤ってファイルを削除した

Linux では rm コマンドでファイルを削除した場合、標準のコマンドで復活することが困難である。ファイルのバックアップを定期的に行っている場合、バックアップファイルから該当するファイルをリストアすることにより、ファイルの復旧を行うことができる。

2) ネットワーク障害によるトラブルの例

* ネットワークサービスが利用できなくなった

ネットワークサービスが利用できなくなった、様々な原因が考えられる。代表的な原因の確認手順は以下の通り。

i) ifconfig コマンドでネットワークインタフェースの確認

コンピュータに接続されているネットワークインタフェースが正常に動作し、ネットワークの設定が正しく行われているか確認を行う。

ネットワークが正しく設定されていない場合、ネットワークインタフェースが動作していないか、DHCP サーバからネットワーク情報が取得できなかったなどの原因が考えられる。

ii) ping コマンドで接続の確認

宛先となるサーバがネットワークに接続されている状態か確認を行う。

サーバからの応答がなかった場合、サーバがネットワークに接続されていない、サーバが起動されていない、もしくはサーバまでの経路で障害が発生しているなどの原因が考えられる。

iii) traceroute で経路情報の確認

宛先となるサーバまでの経路情報が正しく設定されているか確認を行う。途中で経路が途絶えてしまう場合、途絶えたところでネットワークの障害が発生している可能性がある。

この場合、途絶えた機器に対して ping コマンドを実行し、機器がネットワークに接続されている状態か確認を行う。

iv) telnet でサービスの起動確認

利用するサービスがサーバにて起動されているか確認を行う。telnet でサーバへ接続する際に、オプションとしてサービスのポート番号を指定することにより、サービスが起動されていることが確認できる。