9. ネットワークサーバ管理に関する知識 II

1. 科目の概要

OSS が動作するネットワークサーバについて、比較的高度なサーバについて紹介する。さらにサーバ運用管理の概要と具体的な手順、ログの管理やセキュリティ対策など実際のサーバ運用に求められる知識を解説する。

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-9-1. スーパーサーバの仕組みと構築・設定方法	リクエストに応じてサービスを割り振るために用意されたスーパーサーバの仕組みについて概説する。さらにスーパーサーバの構築例として、xinetdの導入と設定の手順を示す。telnetやftpによる接続を例として、スーパーサーバの具体的な動作について述べる。	6
II-9-2. プロキシサーバの仕組みと構築・設定方法	Linuxで動作するプロキシサーバであるsquidを導入、構築し、設定を行う手順を解説する。プロキシサーバ運用のメリットを示し、プロキシサーバが実際に動作する状況について解説する。	7
II-9-3. その他の様々なネットワークサーバ	実際のネットワークで様々に利用されているネットワークサーバを解説する。インターネット向けにはNTPサーバとニュースサーバ、イントラネット向けにはLDAPサーバ、NISサーバ、NFSサーバ、Netatlkサーバ、プリントサーバといった各種サーバの機能を説明する。	8
II-9-4. ルーティングとパケットフィルタリング	ネットワークサーバにおけるルーティングとフィルタリングの処理を理解させる。ルーティングにおいては静的なルーティングの設定を示し、フィルタリングにおいてはパケットフィルタリングの概念とNetfilterやiptablesにおける設定方法を示す。	9
II-9-5. インターネット接続の設定方法	インターネットにサービスを提供するために必要な知識、行うべき作業と設定方法を解説する。ドメインとIPアドレスの取得、インターネットに接続するための設定、信頼性とセキュリティを確保するための運用管理方法などについて説明する。	10
II-9-6. サーバ運用管理の目的と内容	ネットワークサーバを運用管理する作業の内容と、管理対象とする項目、運用管理自体の重要性などについて述べる。運用管理業務の目的としてシステムやサービスの品質を維持することとそのために構成管理、ログ管理、セキュリティ管理、障害管理等の様々な管理が必要であることを示す。	11
II-9-7. サーバにおけるログ管理	ネットワークサーバの管理業務を構成する重要な作業であるログ管理について解説する。syslogの導入と管理の説明に加え、logwatch、logrotate、swatchといった様々なログ管理ツールの導入と設定方法を説明する。	12
II-9-8. セキュリティ対策と運用方法	Linuxサーバを運用する上で必須であるセキュリティ確保について説明する。そもそもセキュリティとは何か、セキュリティの定義について触れ、サーバ運用においてサーバをセキュアに保つための設定方法や診断ツールなどを紹介する。	13
II-9-9. サービスセキュリティの仕組みと設定方法	Linuxサーバが提供する各種のサービスについてセキュリティを確保するための仕組みを解説する。Linuxサーバにおける具体的な構築事例として、tcp_wrappersの機能や設定方法、xinetdによるアクセス制御など具体的な手順を示す。	14
II-9-10. セキュアOSの特徴	セキュリティを強化したOSであるセキュアOSについて、その必要性や特性、セキュアOSが満たすべき要件は何かなど、セキュアOSの特徴を解説する。セキュアOSの具体例としてTrusted Solaris、SELinux、LIDSを紹介する。	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

「9. ネットワークサーバ管理に関する知識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
9. ネットワークサーバ管理に関するスキル	<ネットワークサーバの機能と特徴>	<サーバシステムの導入>	<ネームサーバの導入>	<Webサーバの導入>	<メールサーバ導入の内容と作業手順>	<スーパーサーバの導入>	<プロキシサーバの導入>	<その他のネットワークサーバ導入の作業内容と手順>	<ネットワークサーバによるルーティング処理、フィルタリング処理の実装>	<ネットワークサーバによるインターネット接続>	<サーバの運用管理業務>	<ログ管理の内容と手順>	<Linuxサーバセキュリティ>	<Linuxのサービスセキュリティ>	<セキュアOSの機能と実装>

[シラバス：http://www.ipa.go.jp/software/open/ossc/download/Model_Curriculum_05_09.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
組織間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	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		
			[9-I3]		[9-I3]	[9-I3]									
	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	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							
						[9-I3]									
	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	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
					[9-3, 4]		[9-1]	[9-4]						[9-10, 11]	
			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		
								[9-I5]							
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 上で動作するサービスの管理が挙げられる。サービスにはスーパーサーバ、プロキシサーバ、ログ管理などが含まれる。ここでは、OSS 実装を通してインターネットで利用されるサービス管理手法について習得する。

科目名	第6回	第7回	第8回	第9回	第10回	第11回	第12回	第13回	第14回	第15回
9.ネットワークサーバ管理に関する知識Ⅱ	(1)スーパーサーバとは (2)スーパーサーバの導入と設定手順	(1)プロキシサーバの仕組みと作業概要 (2)Squid の導入と設定	(1)インターネット向けサービス (2)イントラネット向けサービス	(1)静的ルートの設定 (2)パケットフィルタリング	(1)作業の概要 (2)サーバのインターネット接続設定	(1)運用管理業務の目的 (2)運用管理業務の種類と特徴	(1)syslog の管理 (2)ログの集中管理 (3)logwatch (4)logrotate (5)swatch	(1)セキュリティ上の問題とポリシー (2)セキュリティの定義 (3)診断用ユーティリティ	(1)サービスセキュリティの概要 (2)サービスセキュリティの設定内容とその (3)xinetd	(1)セキュアOS の機能概要 (2)セキュアOS の種類と特徴

（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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-1. スーパーサーバの仕組みと構築･設定方法	
対応するコースウェア	第 6 回 スーパーサーバの導入	

II-9-1. スーパーサーバの仕組みと構築･設定方法

リクエストに応じてサービスを割り振るために用意されたスーパーサーバの仕組みについて概説する。さらにスーパーサーバの構築例として、xinetd の導入と設定の手順を示す。telnet や ftp による接続を例として、スーパーサーバの具体的な動作について述べる。

【学習の要点】

* スーパーサーバは、クライアントからの要求に応じて、対応するサービスプログラムに対して起動をかけるプログラムである。
* 代表的なスーパーサーバである xinetd の設定を行う。
* xinetd ではアクセス可能なホストの制限をかける等、セキュリティを考慮した設定を行うことができる。
* telnet や ftp による接続を例にしてスーパーサーバの具体的な動作を理解する。

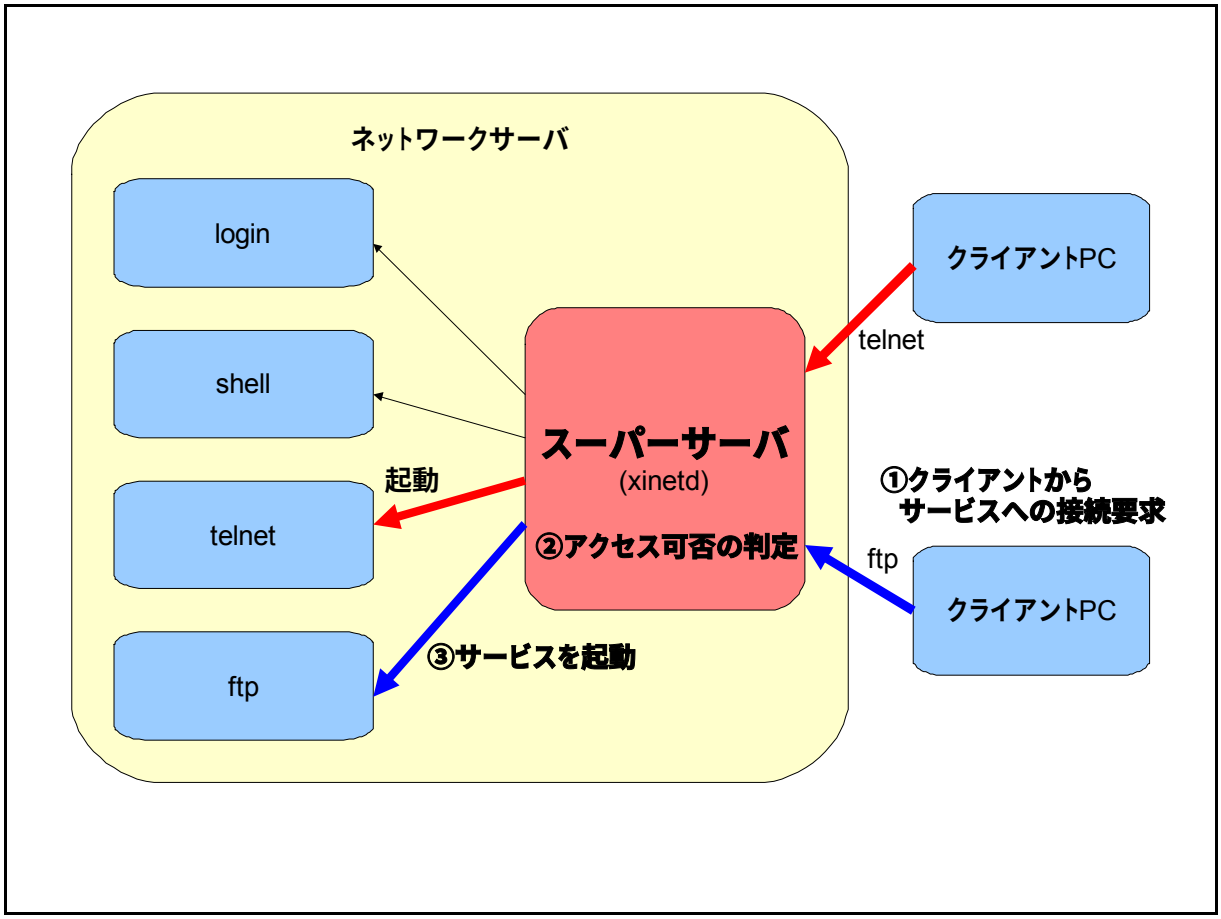

図 II-9-1.　スーパーサーバの役割

【解説】

1) スーパーサーバとは

ネットワークサーバにて各種サービスを提供するには、クライアントからの要求に応答するためサービスごとにプログラムを起動し常駐させておく必要がある。提供するサービスが増えると常駐するプログラムも増え、常に CPU やメモリが消費された状態となってしまう。

スーパーサーバは、ネットワークサービスへの要求を代表して受け付け、サービスの種類によって対応するサービスのプログラムを起動することで、CPU やメモリの消費を抑えるためのプログラムである。

2) xinetd とは

代表的なスーパーサーバとしては inetd が利用されていたが、現在では inetd にセキュリティ機能などの機能拡張を行った、xinetd が利用されている。

xinetd の特徴的な機能としては以下のような点があげられる。

* アクセス可能なクライアントの制御
  ホスト名、IP アドレスやネットワークアドレスを指定することにより、アクセスを許可または不許可とするクライアントの指定を行う。
* アクセス可能時間の設定
  ネットワークサービスの提供可能な時間帯を設定する。
* 接続回数の制限
  同時に起動できるサーバプログラムの数や、1 秒あたりの接続数の制限を設定する。
* 独自のログ出力
  syslog に出力する他、出力する項目や出力方法をを指定して独自のファイルへの出力を設定する。

3) xinetd の設定

xinetd の設定は、/etc/xinetd.confg と/etc/xinetd.d/以下にあるサービスごとの設定ファイルにて行う。/etc/xinetd.conf では xinetd から実行されるプログラム全体に適用する基本的な設定を行い、/etc/xinetd.d/以下にある設定ファイルはプログラムごとに設定を行う。

各ファイルの書式は以下のように記述する。

```
service サービス名(または「default」)
{
        属性名  代入演算子  設定値
}
```

属性として指定できる項目としては、「プログラム（デーモン）の動作タイプ」「ソケットタイプ」「サービスを実行するユーザ／グループ」「サーバプログラムのパス」「サービスの有効／無効」などがある。

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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-2. プロキシサーバの仕組みと構築･設定方法	
対応する コースウェア	第 7 回 プロキシサーバの導入	

II-9-2. プロキシサーバの仕組みと構築･設定方法

Linux で動作するプロキシサーバである Squid を導入、構築し、設定を行う手順を解説する。プロキシサーバ運用のメリットを示し、プロキシサーバが実際に動作する状況について解説する。

【学習の要点】

* プロキシサーバは外部ネットワークが提供するサービスを、内部ネットワークに存在するクライアントへ提供するための代理サーバとして利用される。
* プロキシサーバにてキャッシュを行うことにより内部ネットワークから外部ネットワークへのトラフィックを低減することができる。
* 内部ネットワークへの不正侵入などを防ぎながら、内部ネットワークから外部ネットワークへのアクセスができる。
* 代表的なプロキシサーバである Squid の設定を行いプロキシサーバの実際の動作を確認する。

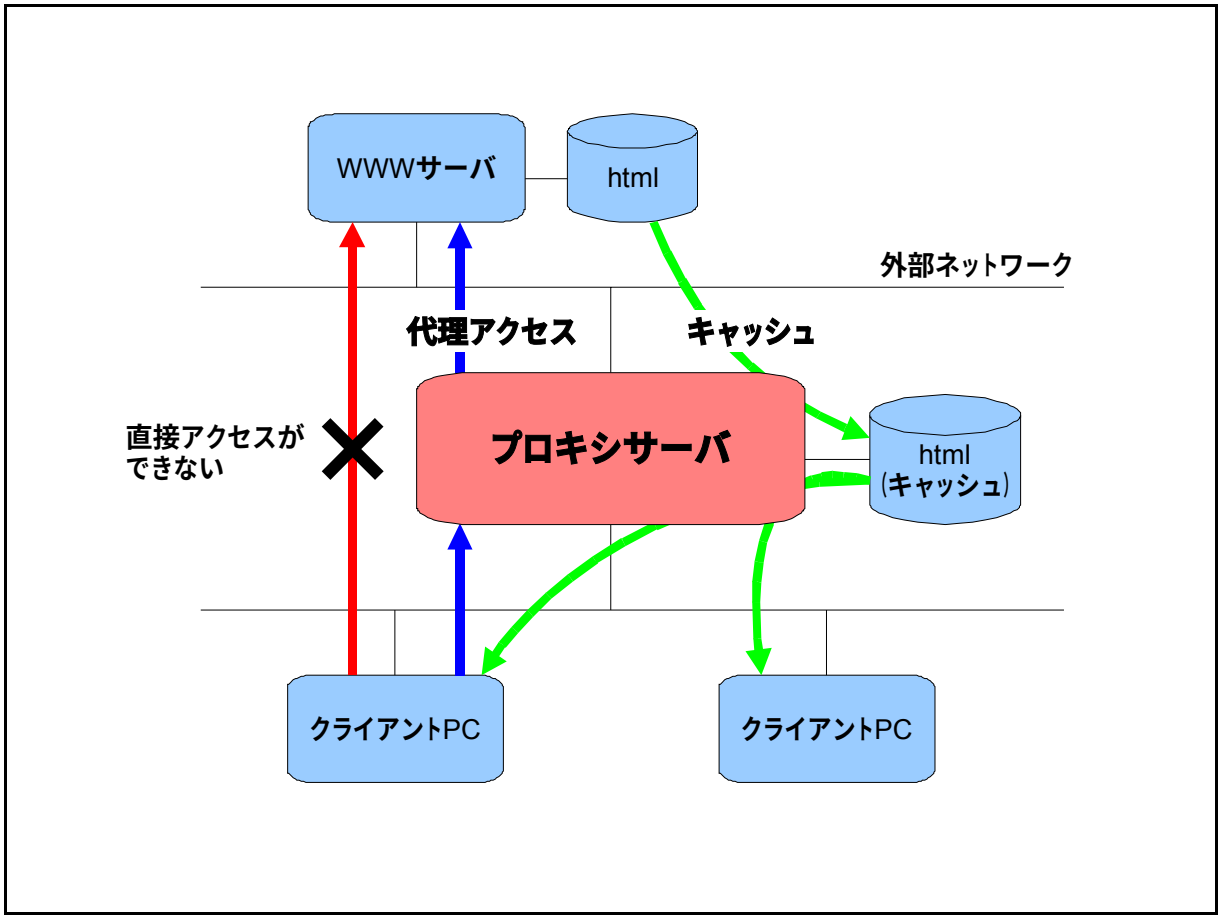

図 II-9-2.　プロキシサーバの動作

【解説】

1) プロキシサーバとは

ファイアウォールなどを設置して外部のネットワークと切り離している場合、プロキシサーバの機能としては大きく以下の 2 つに分けられる。

* 代理アクセス
  ファイアウォールなどによって直接外部のネットワークと通信することが出来ない場合、ネットワーク内のコンピュータの代わりに外部のネットワークと通信を行う。
  また、外部のネットワークとの通信をプロキシサーバだけに制限することで通信の管理が容易となり、セキュリティを向上することができる。

* キャッシング
  ネットワーク内のコンピュータが外部のネットワークと通信を行った結果を保存することにより、他のコンピュータが同じサーバと通信を行う際に保存されているデータを利用する。これにより、外部のネットワークとの通信量を減らし、見かけ上のデータ転送速度を向上することができる。

2) Squid とは

プロキシサーバの 1 つで、主に HTTP を利用した通信に対してプロキシサービスを提供するプログラム。

ネットワーク内のコンピュータが外部のネットワークにある Web サーバへデータを要求する際、Squid によって Web サーバのデータがキャッシングされていない場合には、Squid が Web サーバと通信しデータを取得後、要求のあったコンピュータへ送信する。

要求のあった Web サーバのデータが Squid にキャッシュされていた場合、Web サーバへキャッシュされているデータが更新されていないか確認を行い、更新されていなければキャッシュの内容を要求のあったコンピュータへ送信する。

Squid の特徴的な機能としては以下のようなものがある。

* 分散キャッシュ
  同一ネットワーク内に複数のプロキシサーバを設置し、あるプロキシサーバのキャッシュに要求するデータが存在しない場合、他のプロキシサーバのキャッシュを利用してデータの送信を行うことにより、外部のネットワークからデータを取得するよりも速くデータの送信を行うことができる。

* httpd アクセラレータ
  Squid が存在するネットワーク内にある Web サーバの内容をキャッシングし、外部のネットワークからの要求に対してデータの送信を行うことにより、Web サーバの負荷を低減することができる。

* 透過型プロキシ
  プロキシサーバを利用するためには、ネットワークに接続されたコンピュータに設定をする必要があるが、外部のネットワークへ通信があった場合、デフォルトゲートウェイにてプロキシサーバへ直接転送することにより、各コンピュータで設定を行わずにプロキシサーバを利用するようにできる。

4) Squid の設定

Squid の設定は、/etc/squid/squid.conf によって行い、キャッシュ、アクセスコントロール、パケットフィルタリング、ログなどに関する設定を行う。

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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-3. その他の様々なネットワークサーバ	
対応するコースウェア	第 8 回 その他のネットワークサーバ導入の作業内容と手順	

II-9-3. その他の様々なネットワークサーバ

実際のネットワークで様々に利用されているネットワークサーバを解説する。インターネット向けには NTP サーバとニュースサーバ、イントラネット向けには LDAP サーバ、NIS サーバ、Netatalk サーバ、NFS サーバ、プリントサーバといった各種サーバの機能を説明する。

【学習の要点】

* インターネット向けのサーバとしては、NTP、ニュースサーバ等がある。
* NTP はネットワーク上に存在するホストのシステムクロックを同期するために使用する。
* ニュースサーバはネットニュースの蓄積と他のニュースサーバへの伝播を行う。
* イントラネット向けのサーバとしては、LDAP、NIS、Netatalk 等がある。
* LDAP サーバはネットワークを利用するユーザ情報や、利用可能なサーバと提供しているサービス、プリンタなどの利用可能な機器などを一括管理するために使用する。
* NIS はネットワークに接続しているホスト間でパスワードファイルを一括管理したり、 hosts ファイル等の共有行う時に使用する。
* Netatalk は Linux と Macintosh との間でファイルやプリンタの共有を行う時に使用する。

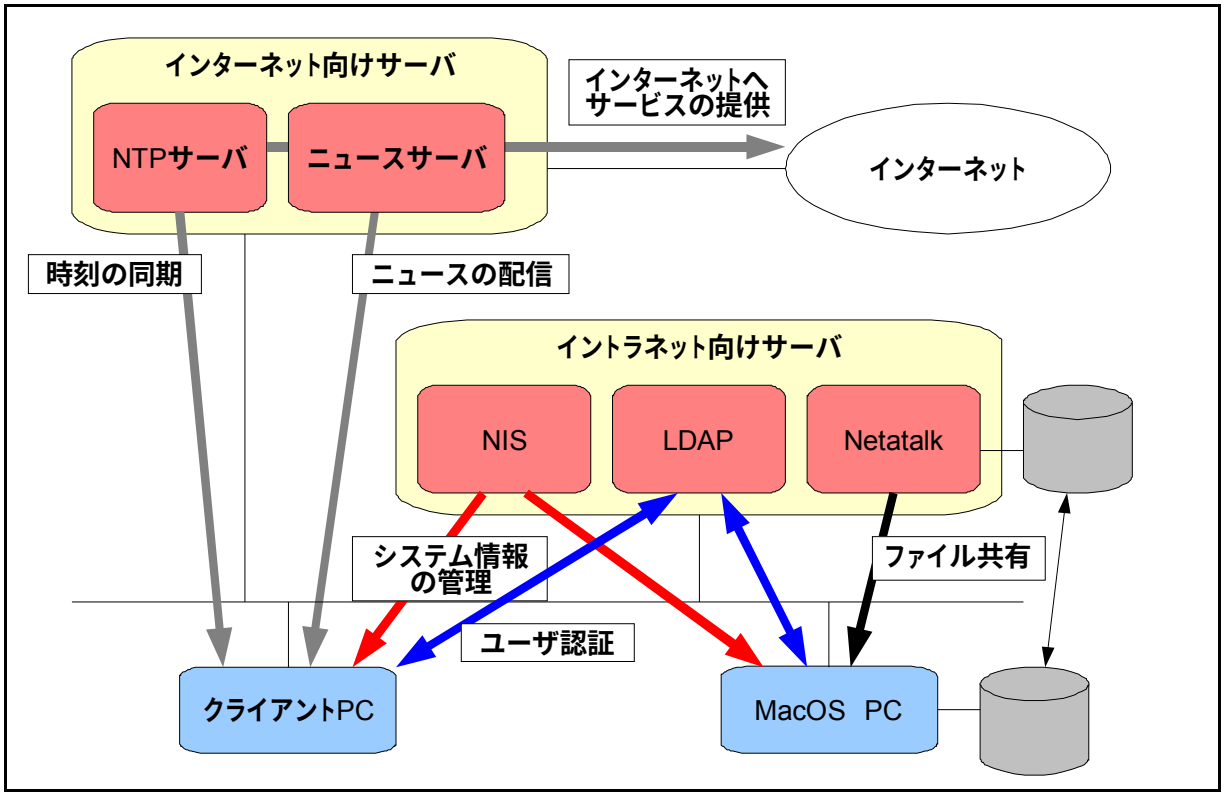

図 II-9-3. その他のネットワークサーバ

【解説】

ネットワークサービスを提供するサーバプログラムとしては、主に外部のネットワークへサービスを行うものと、内部のネットワークにて利用するものに大別することができる。

1) インターネット向けサービス

主に外部のネットワークへサービスを行うサーバとしては以下のようなものがある。

* NTP サーバ

ネットワークを介してクライアントがサーバへ時刻の問合せを行うときに利用する NTP (Network Time Protcol) を利用するためのサーバで、サーバとクライアント間で時刻の同期を行うために使用する。クライアントから時刻の問合せがあると、NTP サーバで管理している時刻をクライアントへ提供することにより、時刻の同期を行う。

NTP サーバは、ntp パッケージを導入し、ntpd サービスを起動することにより使用できる。

* ニュースサーバ

NNTP (Network News Transfer Protocol) を利用してネットニュースの投稿や配信を行うためのサーバである。ネットニュースはテーマごとに階層化されたニュースグループ (掲示板) の集合で、管理しているニュースグループへのニュースの投稿の受付やクライアントへの配信のほか、他のニュースサーバへからのニュースの受信や他のサーバへの配信を行う。

ニュースサーバとしては INN (InterNetNews) があり、inn および inews の 2 つのパッケージをインストールし、innd サービスを起動することにより使用できる。

2) イントラネット向けサービス

内部のネットワークにて利用する主なサーバとしては以下のようなものがある。

* LDAP サーバ

LDAP (Lightweight Directory Access Protocol) はネットワークを介して、ユーザ ID、パスワードやメールアドレス等のユーザ情報を管理・提供する「ディレクトリサービス」を行う時に利用するプロトコルである。LDAP サーバはこのプロトコルを利用してユーザ認証やクライアントへユーザ情報の提供を行う。

LDAP のプログラムとしては OpenLDAP があり、openldap-server および openldap-clients をインストールすることにより使用できる。

* NIS サーバ

NIS (Network Information Service) はネットワーク内のユーザ情報やコンピュータ情報などのシステム情報を管理するためのサービスある。NIS サーバでシステム情報を一元管理することにより、各コンピュータにて同じユーザ名とパスワードでログインすることが可能となり、またネットワーク内に接続されているコンピュータの名前解決を行うことができる。

NIS サーバは ypserv、yppasswdd、ypxfrd サービスで構成され、これらをインストールすることにより使用できる。

* Netatalk サーバ

Netatalk は Linux へ AppleTalk Network の機能を組み込むためのソフトウェアである。Netatalk を利用すると Linux を Mac OS クライアントに対するファイルサーバとして利用することが可能となり、Mac OS クライアントから Linux 上のファイルシステムの共有や、プリンタを利用することができる。

Netatalk パッケージをインストールし、atak サービスを起動することにより使用できる。

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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-4. ルーティングとパケットフィルタリング	
対応するコースウェア	第 9 回ネットワークによるルーティング処理、フィルタリング処理の実装	

II-9-4. ルーティングとパケットフィルタリング

ネットワークサーバにおけるルーティングとフィルタリングの処理を理解させる。ルーティングにおいては静的なルーティングの設定を示し、フィルタリングにおいてはパケットフィルタリングの概念と Netfilter や iptables における設定方法を示す。

【学習の要点】

* サーバからデータを送信する通信経路を見つけ出す方法のことをルーティングと呼ぶ。ルーティングは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。
* 静的ルートはルーティング設定ファイル(/etc/sysconfig/static-routes) 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ことができる。
* サーバに送られてきたパケットのヘッダにはプロトコルや送信元アドレス、送信先アドレスやポート番号などの情報が含まれており、これを参照して通過するかどうかを決定することをパケットフィルタリングという。
* Netfileter のパッケージとして iptables があり、iptables コマンドで設定するか、フィルタリングのルールを/etc/sysconfig/iptables に記述することにより設定する。

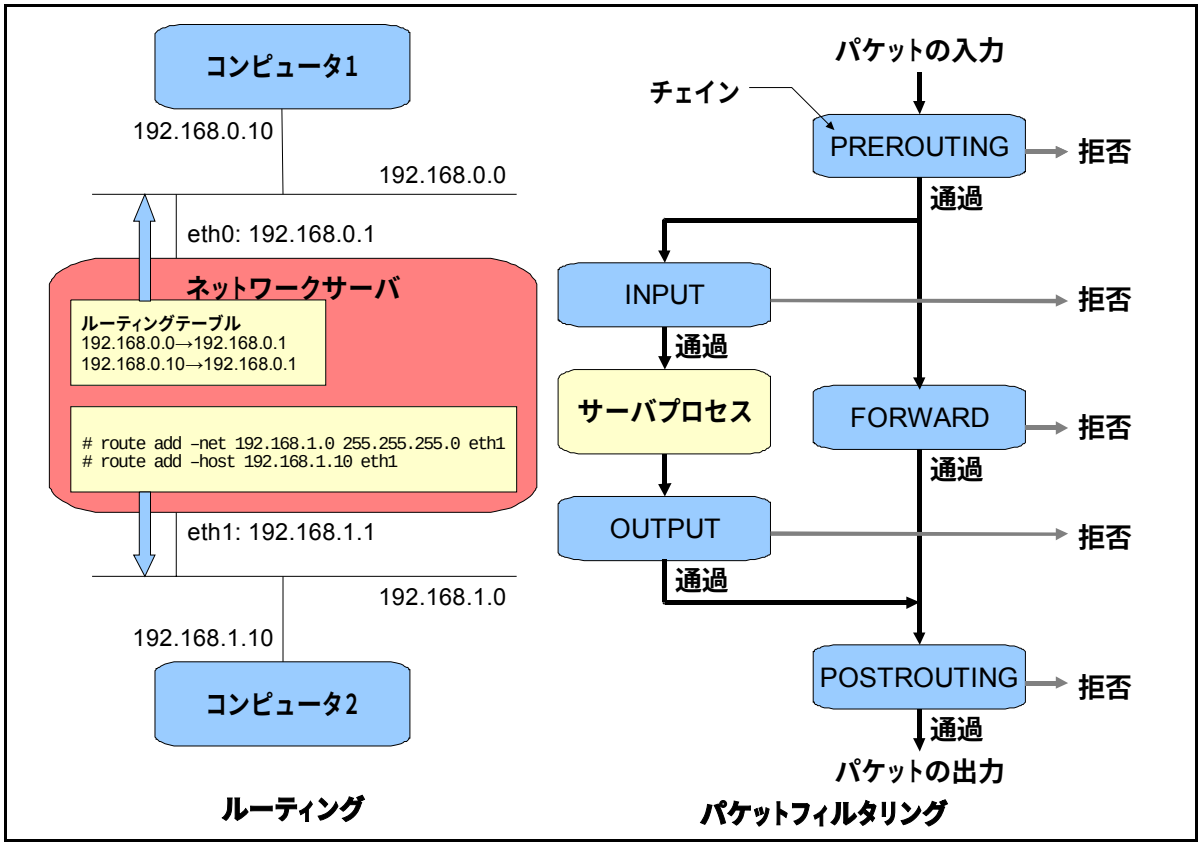

図 II-9-4.　静的ルートとパケットフィルタリング

【解説】

1) ネットワークサーバのルーティング

ネットワークサーバにて内部のネットワークと外部のネットワークへ同時にサービスを提供する場合など、要求のあったコンピュータへ返信を行うためには、要求元のコンピュータがどちら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くてはいけない。

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。

経路情報としては、静的ルーティングと動的ルーティングがあるが、ネットワークサーバでは主に静的ルーティングにて経路情報の設定を行う。

2) 静的ルーティングの設定

設定ファイルまたは route コマンドにて、宛先のネットワークアドレスまたはホストアドレスがどのゲートウェイを経由してデータを送出するのかを設定する。

* 設定ファイルによる設定の例

/ etc/sysconfig/static-routes

```
any net 192.168.0.0 netmask 255.255.255.0 gw 192.168.0.1
any host 192.168.0.10 gw 192.168.0.1
```

* route コマンドによる設定の例

```
# route add -net 192.168.1.0 255.255.255.0 eth1
# route add -host 192.168.1.10 eth1
```

3) パケットフィルタリング

パケットフィルタリングはネットワークインタフェースを通過するデータ（パケット）のプロトコルや送信元アドレス、送信先アドレスやポート番号などを参照し、データを通過させるかどうか決定することで、ネットワークサーバおよびネットワーク内のセキュリティを高めるために使用する。

パケットフィルタリングはデータの入力、出力や転送などが行われるタイミングごとにチェインと呼ばれるルールセットによりフィルタリングを行う。

5) パケットフィルタリングの設定

Linux では主として Netfilter を利用してパケットフィルタリングを行い、iptables サービスを起動することにより使用することができる。

Netfilter は、PREROUTING、FORWARD、INOUT、OUTPUT および POSTROUTING の 5 つのチェインによってパケットフィルタリングを行う。

Netfilter で設定する項目は、ルールを設定する場所を設定する「テーブル」、ルールに一致したデータの扱いを設定する「ターゲット」、各チェインのデフォルトのターゲットを設定する「ポリシー」がある。

フィルタリングのルールは iptables コマンドを使い、各チェインで使用するルールを追加することにより設定を行う。また、/etc/sysconfig/iptables へ記述しておくことによりサービスの起動した時に自動的にパケットフィルタリングのルールを設定することができる。

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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-5. インターネット接続の設定方法	
対応するコースウェア	第 10 回 ネットワークサーバによるインターネット接続	

II-9-5. インターネット接続の設定方法

インターネットにサービスを提供するために必要な知識、行うべき作業と設定方法を解説する。ドメインと IP アドレスの取得、インターネットに接続するための設定、信頼性とセキュリティを確保するための運用管理方法などについて説明する。

【学習の要点】

* 独自の Linux サーバをインターネットに接続してサービスを行う場合、ドメインおよびグローバル IP を取得しておく必要がある。
* インターネットへ接続したサーバを公開するためには、取得したドメイン名を外部ネットワークで管理している DNS サーバへ登録する必要がある。また、外部ネットワークとの通信を行うためには DNS サーバの設定を行い、ドメイン情報を取得できるようにする。
* インターネットへ接続する方法としては、モデムとサーバを直接接続する方法と、モデムとサーバをファイアウォールを介して接続する方法がある。モデムとサーバを直接接続する場合、サーバに PPPoE クライアントにて接続方法の設定を行う。
* ネットワークサーバをインターネットへ公開することで不正アクセスなどの脅威にさらされることになる。TCP Wrapper などでサーバへのアクセス制限を設定することが必須である。

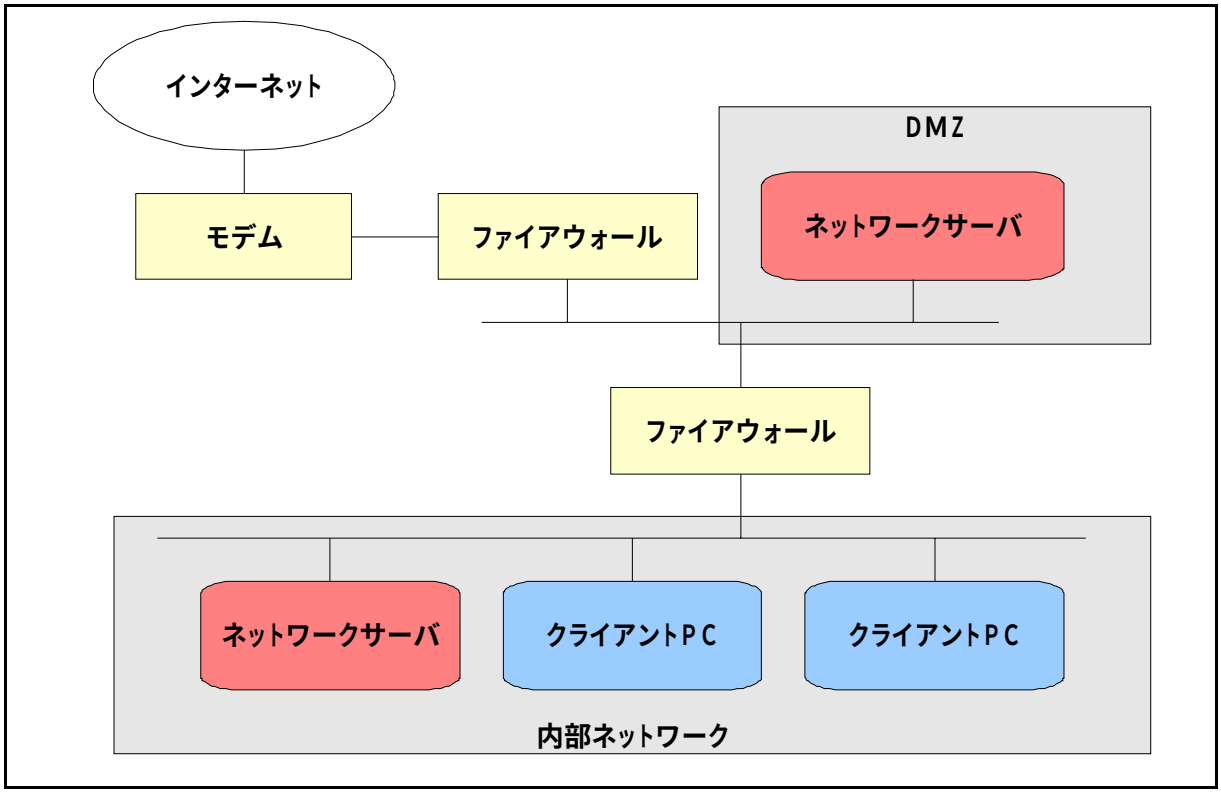

図 II-9-5.　インターネットへの接続

【解説】

1) インターネット接続に必要な情報

ネットワークサーバをインターネットへ接続してサービスを提供する場合、ネットワークサーバの所属を識別する「ドメイン名」とインターネット上で利用可能な「グローバル IP アドレス」を取得しておく必要がある。

取得したドメイン名とグローバル IP アドレスで他のネットワークからアクセスできるようにするには ISP などで管理している DNS サーバへドメイン情報を登録する必要がある。

2) 接続方法

インターネットへ接続する方法としては、モデムとサーバを直接接続する方法と、ファイアウォールを介してモデムとサーバを接続する方法がある。

* モデムとサーバを直接接続

モデムを介してネットワークサーバを直接インターネットへ接続する方法で、不正アクセスなどを内部ネットワークのセキュリティを確保するため、サーバに必ずファイアウォールを設定する。

インターネットとの接続は、サーバに PPPoE クライアントをインストールし、ISP などからグローバル IP アドレスを取得できるようにする。

* ファイアウォールを介してモデムとサーバを接続

インターネットとの接続はファイアウォールが行い、インターネットへ公開するサーバは DMZ (DeMilitarized Zone) へ配置する。内部のネットワークは、更に DMZ とファイアウォールを介して接続することにより、内部ネットワークのセキュリティを確保する。

ファイアウォールの PPPoE クライアント機能を使用して、ファイアウォールにグローバル IP アドレスが取得し、公開するネットワークサーバは DMZ のプライベート IP アドレスを設定する。公開するネットワークサーバはファイアウォールの IP マスカレード (内部の複数の IP アドレスを外部に対しては 1 つだけに見えるようにする方法) を利用して外部との通信を行う。

3) サーバの設定

ネットワークサーバをインターネットへ接続する場合、以下のような設定を行う必要がある。

* グローバル DNS の設定

外部の DNS サーバへ公開するサーバ自身の DNS 情報の設定と、DNS 情報の転送を許可する DNS サーバやクライアントの設定を行う。

* アクセス制限

外部へ提供するサービスごとにアクセス制限を設定する。スーパーサーバから起動されるサービスはスーパーサーバのアクセス制限を利用し、それ以外のサービス単体でアクセス制限を実行することが出来ないサービスについては TCP Wrapper を利用してアクセス制限を行う。

また不要なサービスを停止することにより、無用なアクセスを受け付けないようにする。

* 外部からのアクセス手段

ネットワークに所属するユーザが外部のネットワークからアクセスを行う必要がある場合、SSH や SSL によるアクセスやクライアント証明書を利用することにより、よりセキュアな方法でアクセスを行うように設定を行う。

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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-6. サーバ運用管理の目的と内容	
対応する コースウェア	第 11 回 サーバの運用管理業務	

II-9-6. サーバ運用管理の目的と内容

ネットワークサーバを運用管理する作業の内容と、管理対象とする項目、運用管理自体の重要性などについて述べる。運用管理業務の目的としてシステムやサービスの品質を維持することとそのために構成管理、ログ管理、セキュリティ管理、障害管理等の様々な管理が必要であることを示す。

【学習の要点】

* サーバ運用管理の業務としては、サーバが正常に動作しているかを確認する業務、サーバで定期的に実行される管理操作を実行する業務が挙げられる。
* ログ監視、ネットワーク監視、サービス監視やパフォーマンス／リソース監視などを行い、サーバが正常に動作していることを確認する。
* システムのバックアップやログ収集、設定変更、パッチの適用、ソフトウェアインストールなど定期的に作業を行いサーバの維持を行う。

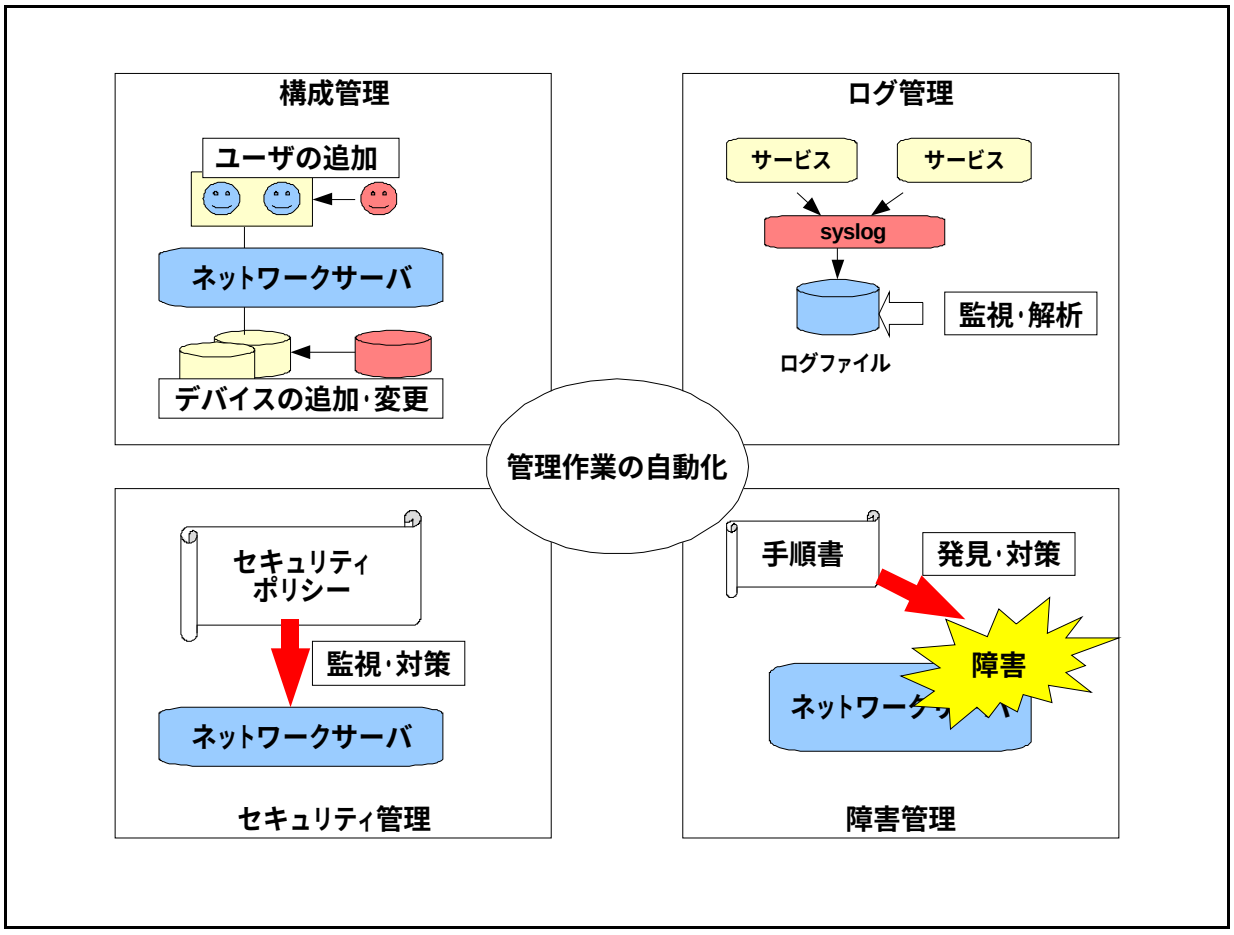

図 II-9-6.　サーバの運用管理

【解説】

1) ネットワークサーバの運用管理

ネットワークサーバは安定して継続したサービスを提供することが求められているが、ハードウェアやネットワーク障害、不正アクセスなどの発生を完全に防ぐことは困難である。

このため、ネットワークサーバ運用を円滑に行い、問題の発生した場合には迅速に発見し、問題解決を行うために以下のような管作業を行う必要がある。

2) 構成管理

ハードウェアやソフトウェアの構成・設定・登録・変更を管理する業務でサーバの設計から導入、運用中の作業が必要となる。

運用中の主な作業としては、利用するユーザやサーバアプリケーションの追加・変更や OS やアプリケーションのアップグレードが行われた場合の更新作業がある。

また、パフォーマンスやリソースの監視を行い、これらが不足していた場合、最適なシステム構成を設計し変更作業を行う。

3) ログ管理

ネットワークサーバでは運用中に発生する様々な事象をログへ出力される。出力されるログを監視することにより、障害や不正アクセスなどを発見することが可能となる。

ログ監視では、主に「ログ取得対象の設定」「ログの取得」「ログローテーションの設定」「ログのスケジューリングの設定」「ログの解析」などの作業を実施する。

4) セキュリティ管理

セキュリティ管理を行うためには、どのようなサービスを誰に提供するかなどを設定した「セキュリティポリシー」を作成しておく必要がある。セキュリティ管理では、ログやネットワーク、サービスの監視を行い、セキュリティポリシーに沿って運用がされているか確認を行う。

セキュリティポリシーに沿っていない状態が発見された場合は、ネットワークの設定変更やサービスの停止などを行う。

5) 障害管理

ネットワークサーバでは障害が必ず発生することを前提とし、発生を早期発見し被害を最小限に抑え、早く復旧することが必要である。

障害を早期発見するには、障害を検出するための処理を自動化して定期的に実行し、異常があった場合速やかに通知を行う仕組みを構築することが有効である。

障害の解決には、障害発生時の状況や対応方法などの手順やツールをまとめておき、障害が発見された時は、この手順に従って速やかに障害解決の作業を行うことで被害を最小限に抑え、復旧までの時間を短く抑えることが必要である。

6) 管理作業の自動化

管理作業で頻繁に使用する監視用のコマンドやデータのバックアップ処理などはスクリプトを作成し、確実にコマンドが実行するようにすることが必要である。

また定期的に実行する管理作業は crontab でスケジューリングしておき、指定した日時にコマンドが実行されるようにする。

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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-7. サーバにおけるログ管理	
対応するコースウェア	第 12 回 ログ管理の内容と手順	

II-9-7. サーバにおけるログ管理

ネットワークサーバの管理業務を構成する重要な作業であるログ管理について解説する。syslog の導入と管理の説明に加え、logwatch、logrotate、swatch といった様々なログ管理ツールの導入と設定方法を説明する。

【学習の要点】

* サーバで出力されるログには、サーバの異常を示すログ、ユーザのログイン履歴や認証時のログ、プログラムの動作ログなど、さまざまな種類が存在し、多くはログ制御システム（syslog）を介して出力される。
* syslog はサーバのプログラム syslogd で出力し、出力する内容は設定ファイル（syslog.conf）により決定する。
* syslog により出力されるログから異常値を発見することは困難であり、logwatch 等で特定の情報が出力された時に自動的に通知を行うことが有効である。
* syslog により作成されるログファイルには膨大な量のログが出力される。cron で logrotate を実行すログファイルを何世代かに分割し肥大化を防ぐ。

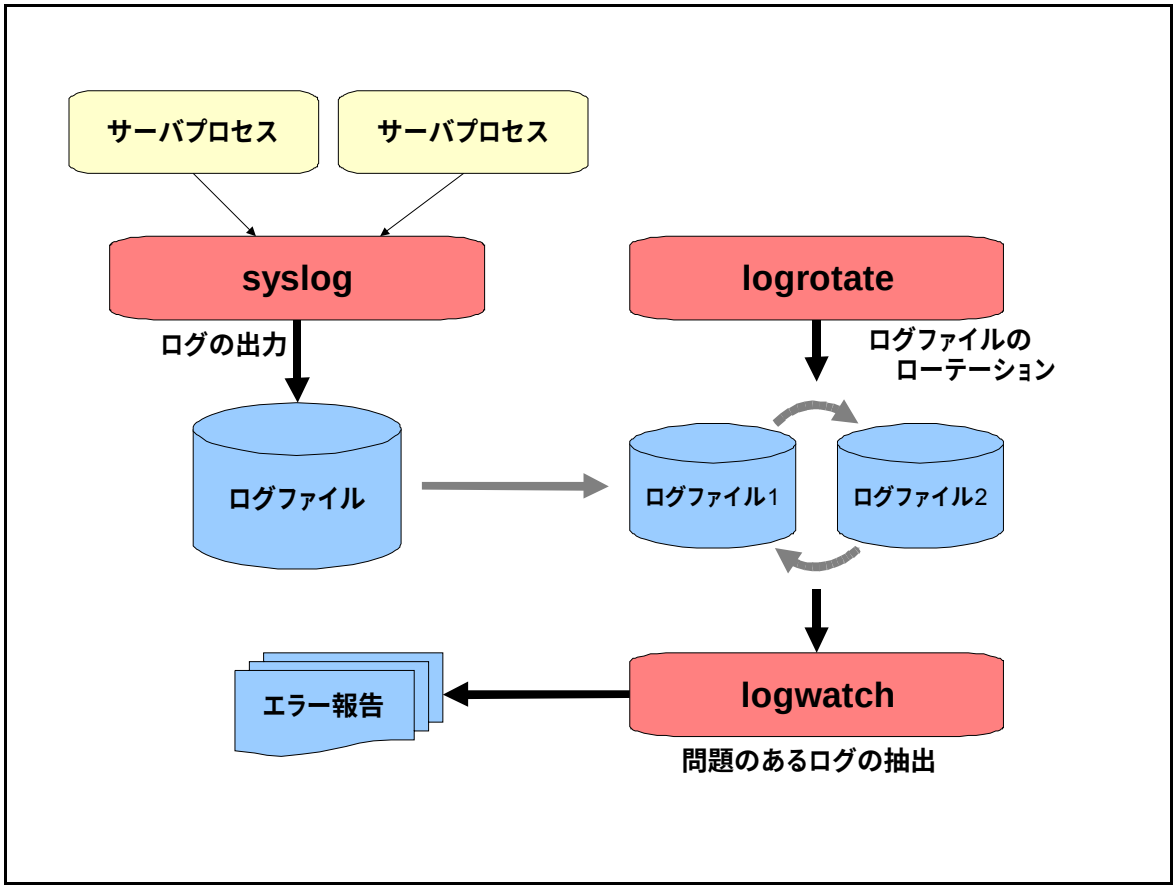

図 II-9-7.　syslog によるログ管理

【解説】

1) サーバで出力するログ

ネットワークサーバの各サービスプログラムではサーバの異常を示すログ、ユーザのログイン履歴や認証時のログ、プログラムの動作ログなどをログとして記録している。

このログを検証することにより、サービスが問題なく提供されているか、また不正なアクセスが行われていないかなどの検収が可能となる。

出力するログの多くはsyslogサービスを使用して出力される。またログを管理し検証を行うツールとして logwatch コマンドや logrotate コマンドなどがある。

2) syslog

syslog を使用してログを出力することにより、ログの出力方法をシステム内で統一することが可能となり、ログの解析や問題の発見などが容易となる。

syslog は Linux に標準で導入されているサービスで、システム起動時に自動的に起動するようになっている。動作の設定は/etc/syslog.conf にて行い、以下のように設定を行う。

<ファシリティ>.<レベル>　<アクション>

* ファシリティ

syslog で出力するログをどのカテゴリで出力するかを指定する。

auth（認証時）、cron（クーロン）、daemonm（デーモン）、user（ユーザ）などがある。

* レベル

出力するログの重要度や緊急度を指定する。

emerg（システム不能）、crit（致命的）、err（一般エラー）、warning（警告）などがある。

* アクション

ファシリティとレベルで指定したログのアクションを指定する。

出力するファイル名やメッセージを送信するホスト名、ユーザ名などがある。

syslog は UDP を用いたクライアント･サーバ方式で動作しているため、アクションに送信先ホスト名を指定することにより、特定のサーバでログを集中管理することが可能となる。

3) logwatch コマンド

ログファイルには様々な情報が膨大に出力されるため、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 コマンドを利用することにより、問題のあるログを容易に抜き出すことが可能となる。logwatch ではサービスごとに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だけを抽出し、指定したメールアドレスへ送信する。

問題を迅速に発見するためには、cron にて定期的にコマンドを実行する必要がある。

4) 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検証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 コマンドを利用することにより、ログファイルを分割して管理することが可能となる。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ことでログ管理が容易となる。

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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-8. セキュリティ対策と運用方法	
対応する コースウェア	第 13 回 Linux サーバセキュリティ	

II-9-8. セキュリティ対策と運用方法

Linux サーバを運用する上で必須であるセキュリティ確保について説明する。そもそもセキュリティとは何か、セキュリティの定義について触れ、サーバ運用においてサーバをセキュアに保つための設定方法や診断ツールなどを紹介する。

【学習の要点】

* ネットワークサーバを管理する上で、「コンピュータへの不正進入」「コンピュータの不正使用」「情報の漏洩」「コンピュータウィルスへの感染」などセキュリティ上の問題が発生することを認識する。
* ネットワークサーバにおけるセキュリティとは「機密性」「完全性」および「可用性」の維持である。提供するサービスや対象とするユーザを明確にしセキュリティを確保しなくてはいけない。
* セキュリティの確保のためには、セキュリティポリシーにより系統だった対策を策定し、これを実行する必要がある。
* セキュリティ対策としては、各種診断ユーティリティを使用し、サービスの実行状況の確認と設定、システムログのチェック、ネットワークの監視、システムのアップデート、システムパスワードのチェック、システムパスワードの保護などを実施する。

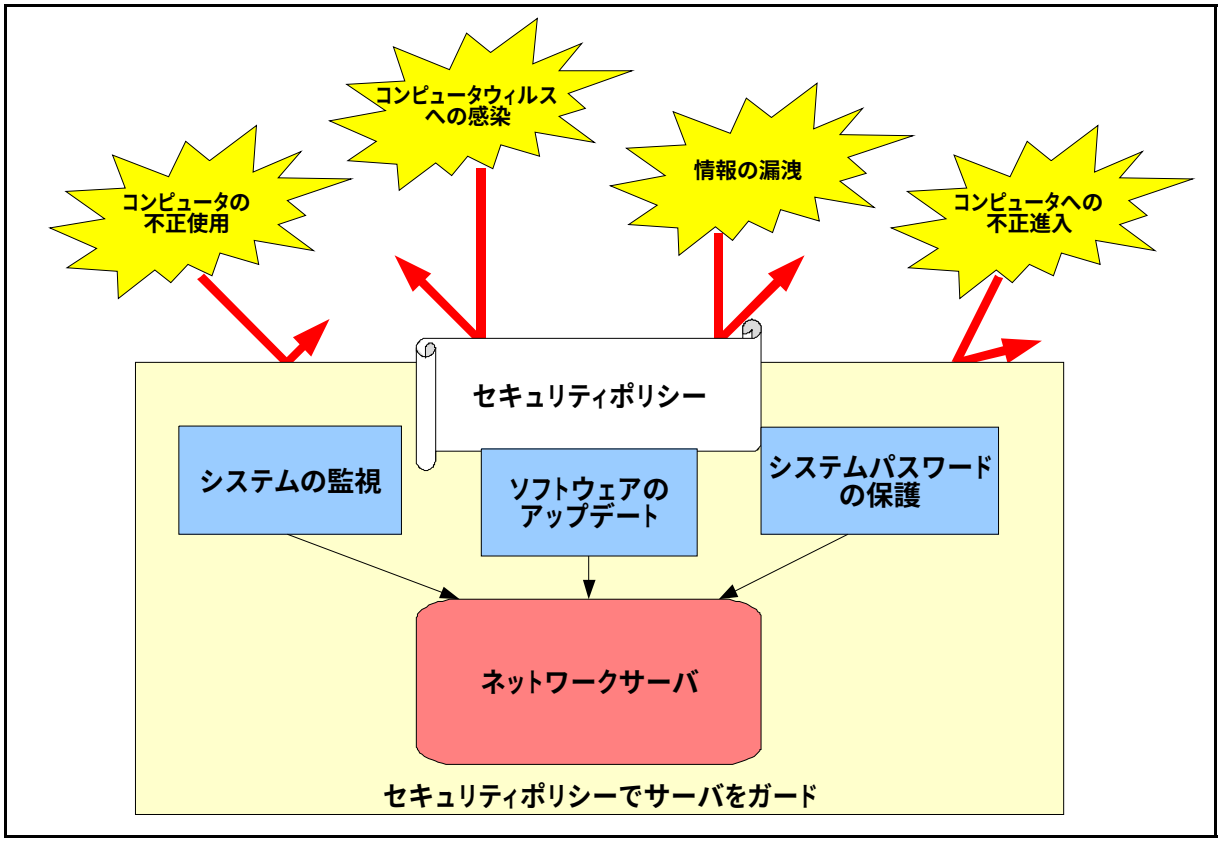

図 II-9-8.　サーバセキュリティ

【解説】

1) ネットワークサーバのセキュリティ

様々な情報を扱うネットワークサーバにおいて、セキュリティとは「機密性」「完全性」および「可用性」の維持である。

* 機密性 ： アクセスを認可された者だけが情報にアクセスできること。
* 安全性 ： 情報および処理方法が、正確であることおよび完全であること。
* 可用性 ： 許可された利用者が、必要なときに、情報にアクセスできること。

ネットワークサーバにてセキュリティの対策を行うためには、セキュリティ上の問題は必ず発生することを前提とし、どのような問題があるのかを知る必要がある。以下の項目は最低限知っておく必要がある問題である。

* コンピュータへの不正進入
* コンピュータの不正使用
* 情報の漏洩
* コンピュータウィルスへの感染

2) セキュリティポリシーの策定

セキュリティの確保のためには、ネットワークサーバにて提供するサービスの種類や提供のするユーザ、運用方法などを系統立てて策定したセキュリティポリシーを作成することが重要である。

実際のサーバ設計、構築および運用はセキュリティポリシーに沿って作業を実施する必要がある。

3) セキュリティ対策

セキュリティ対策として以下のような管理作業を行う必要がある。

* 各種診断ユーティリティを使用したシステムの監視

  Linux にて提供されている各種診断ユーティリティを使用し、サービスの実行状況の確認、システムログのチェック、ネットワークの監視などを行い問題の早期発見を行う。

  サービスの実行状況は、chkconfig コマンドによるサービスの自動起動の確認や、service コマンドによるサービスの稼動状態の確認により行うことができる。

  ネットワークやサーバ全体の稼動状況は、SNMP や MRTG により監視することができる。

* ソフトウェアのアップデート

  Linux カーネルやサービスプログラムなどにセキュリティ上の問題が発見された場合、できるだけ早く対策を行う必要がある。

* システムパスワードの保護

  パスワードは設定するだけではなく、ある程度の強度を持たせる必要がある。強度の高いパスワードの条件としては以下のようなものがあげられる。

  - 文字数が 8 文字以上
  - アルファベット大文字、小文字、数字、記号のうち 3 種類以上を含む

  また、パスワードの解析を防ぐためにはパスワードに有効期限を設定し定期的にパスワードを変更することが必要である。

  パスワードの文字数や有効期限は/etc/login.defs で設定することができる。

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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-9. サービスセキュリティの仕組みと設定方法	
対応する コースウェア	第 14 回 Linux のサービスセキュリティ	

II-9-9. サービスセキュリティの仕組みと設定方法

Linux サーバが提供する各種のサービスについてセキュリティを確保するための仕組みを解説する。Linux サーバにおける具体的な構築事例として、tcp_wrappers の機能や設定方法、xinetd によるアクセス制御など具体的な手順を示す。

【学習の要点】

* Linux ではシステム起動時に rc スクリプトを使用してサービスの起動を行う。rc スクリプトはサービス毎に作成されるシェルスクリプトで、システムのモード（ランレベル）によって起動するサービスを設定することができる。
* ネットワークサーバにてサービスすることはセキュリティ上の問題に直結するため、提供するサービスの種類や利用するユーザの制限･監視を行い安全の利用できる環境を構築する必要がある。
* スーパーサーバ(xinetd)によって起動されるサービスのセキュリティ強化の方法としては、設定ファイルにアクセス可能なホスト、アクセス可能時間、接続数を指定することによるアクセス制御がある。
* スーパーサーバによって起動されるサービス以外（デーモンなど）は、TCP Wrapper によってアクセス制御を行う。TCP Wrapper ではサービス（デーモン）毎にアクセスを拒否または許可するするホストやユーザを設定することによりアクセスの制御行う。

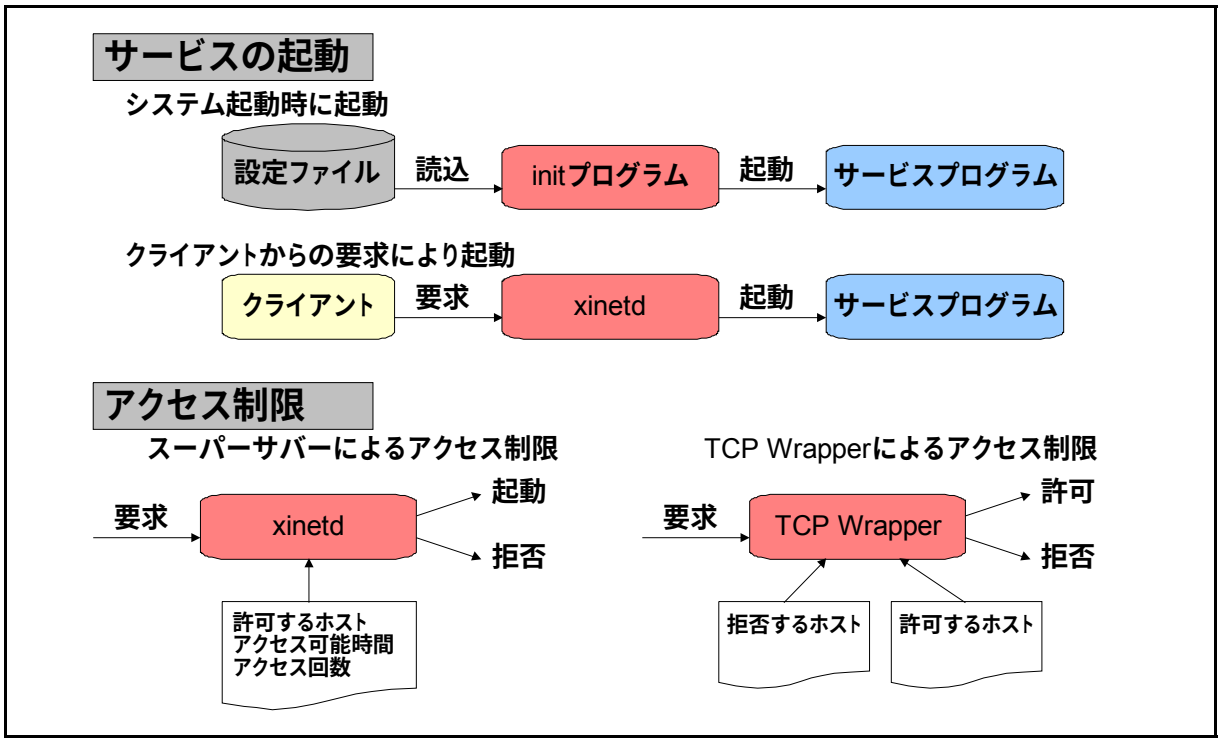

図 II-9-9. サービスセキュリティ

【解説】

1) サービスのセキュリティ

ネットワークサーバとして運用するには提供するサービスごとにサービスプログラムを起動する必要があるが、サービスが増えるほどサーバへアクセスする方法が増えるため、セキュリティ上の危険も増える。サービスによって発生する問題を回避するには、必要なサービスのみを利用し、必要のないサービスを停止することが最も基本的な対策となる。

また提供するサービスは、利用を許可するコンピュータやユーザなどを制限することによりセキュリティの強化を行う。

2) サービスの起動

Linux ではサービスプログラムを起動する方法としては以下のようなものがある。

* システム起動時に同時に起動
  ネットワークの設定を行うデーモンなど、システム起動に必要なサービスや、WWW サーバなどクライアントへのレスポンスの速さが要求されるサービスの起動を行う。
* スーパーサーバ(xinetd)による起動
  ユーザに提供するサービスで TELNET や FTP などクライアントクライアントからの要求によりサービスの起動を行う。

3) システム起動時のサービスプログラムの起動

Linux では init プログラムによってシステム起動時にサービスプログラムを実行する。各サービスプログラムの起動は rc スクリプトによって行い、システムの起動モード（ランレベル）によって実行するrcスクリプトを設定することができる。

必要なサービスのみ起動するためには、ランレベルごとに必要なサービスを起動するように設定を行うことが必要となる。起動するrcスクリプトの設定は chkconfig コマンドによって行う。

また、サーバ起動後は service コマンドにてサービスの稼動状態を確認し、必要のないサービスが起動されていた場合、サービスの停止を行う。

4) スーパーサーバによるアクセス制限

スーパーサーバでは起動するサービスを必要なサービスのみに制限することが必要である。

また、スーパーサーバには、アクセス可能なホストやネットワークの設定、アクセス可能時間の設定、接続数の制限の設定などにより、セキュリティを強化する機能が実装されている。

サービスごとアクセス制限の内容を設定ファイルに記述することによりサービスのセキュリティを強化することが可能となる。

5) TCP Wrapper によるアクセス制限

デーモンなどスーパーサーバによって起動されるサービス以外のサービスプログラムは TCP Wrapper によってアクセス制御を行うことができる。

TCP Wrapper は各サービスのアクセス制限を一元管理することができる。設定ファイルに、アクセス制限を行うサービスプログラムと、アクセスを拒否するホストおよび許可するホストを記述することにより、サービスのアクセス制限を行いセキュリティを強化することが可能となる。

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	9 ネットワークサーバ管理に関する知識 II	応用
習得ポイント	II-9-10. セキュア OS の特徴	
対応する コースウェア	第 15 回 セキュア OS の機能と実装	

II-9-10. セキュア OS の特徴

セキュリティを強化した OS であるセキュア OS について、その必要性や特性、セキュア OS が満たすべき要件は何かなど、セキュア OS の特徴を解説する。セキュア OS の具体例として Trusted Solaris、SELinux、LIDS を紹介する。

【学習の要点】

* 従来のセキュリティ対策には限界があり、OS そのものを強化することにより不正侵入などへの耐性を根本的に高められるセキュア OS が求められている。
* セキュア OS とは「強制アクセス制御」と「最小特権」の機能を満たしている OS を指している。
* セキュア OS としては「Trusted Solaris」や「SELinux」等がある。
* Trusted Solaris は米国家安全保障局で策定されたセキュリティ評価基準に定義されている規約を満たした Trusted OS を実装した OS である。
* SELinux は米国の NSA が中心になって開発した, Linux カーネルの セキュリティ拡張モジュールで、多くの Linux ディストリビューションに組み込まれている。

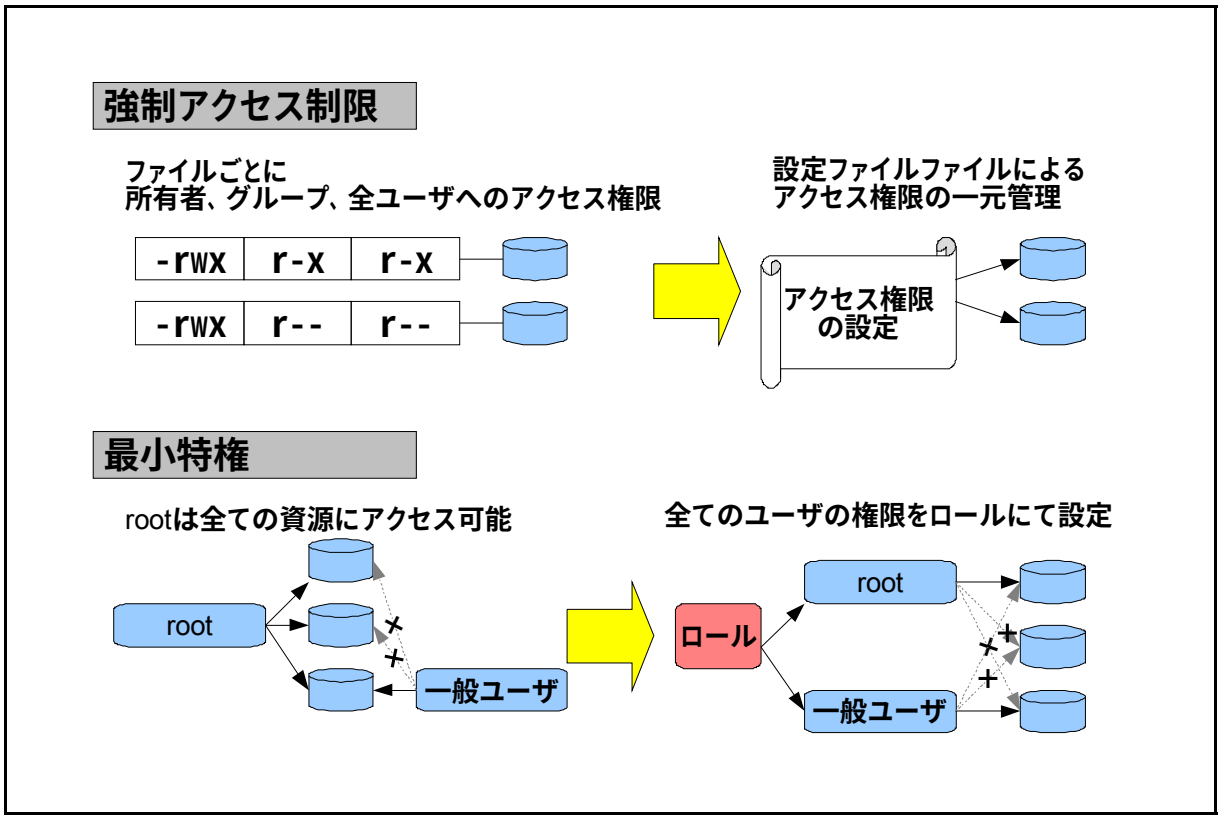

図 II-9-10.　セキュア OS の特徴

【解説】

1) セキュア OS とは

Linux はネットワークやサービスの設定や運用を適切に行うことにより、セキュリティを強化することが可能であるが、セキュリィホールや利用者に依存するパスワードの管理など、従来の OS では防ぐことが出来ない問題が存在する。
セキュア OS は通常の OS と比べ最低限以下のような点が強化がされているものを指す。

* 強制アクセス制御
  Linux では、ファイルやディレクトリに対するアクセス権として所有者、グループおよび全てのユーザの 3 種類の設定を行う。また所有者によってアクセス権が自由に設定できる。
  セキュア OS では、アクセス権の設定をファイルやディレクトリの所有者が行うのではなく、設定ファイルで一元管理することにより、システム管理者がシステム全体のアクセス権の設定状態を把握し管理することができる。

* 最小特権
  Linux では root ユーザがシステムに関する全ての権限を所有しているため、root 権限を不正なユーザに取られた場合、システム全体を自由に操作することが可能となってしまう。
  セキュア OS では、root 権限を廃止し複数のユーザに権限を分割して割り当てることにより、アカウントやサービスには最低限の権限が付与されるため、ユーザ権限を不正なユーザに取られた場合でも、システムへの影響を少なくすることができる。

2) Trusted Solaris

Trusted Solaris は米国家安全保障局で策定されたセキュリティ評価基準に定義されている規約を満たした Trusted OS を実装した OS で、主に以下のような特徴がある。

* MLS (Multi-Level Security)
  システム内の各情報に機密レベルを設定し上位レベルから下位のレベル、または下位のレベルから上位のレベルへのアクセス制御を行うことで強制アクセス制御を実現している。

* RBAC (Role-Based Access Control)
  全てのユーザに対してロール呼ばれる役割を結びつけることにより、管理者権限の分割、root 特権の細分化を行い最小特権実現している。

3) SELinux

SELinux は米国の NSA が中心になって開発した, Linux カーネルの セキュリティ拡張モジュールで、多くの Linux ディストリビューションに組み込まれている。

セキュア OSとして、セキュリティポリシーファイルによる強制アクセス制御、RBAC による最初権限の他、以下のような特徴がある。

* Type Enforcement
  システムの資源に対して「タイプ」と呼ばれる属性情報を割り当て、タイプごとにアクセス権限を割り当てることによりアクセス制御を行う。プロセスなど他の資源へアクセスするものについては「ドメイン」と呼ぶ。

* ドメイン遷移
  親プロセスによって起動された子プロセスに対して、親プロセスよりもアクセス権限が小さいドメインを割り当てることにより、アクセス権限を制限する。