9. ネットワークサーバ管理に関する知識 I

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、その基本的な役割と構成、種類、特徴を解説する。さらに代表的なネットワークサーバを紹介し、各サーバの仕組みや実装について説明する。

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-9-1. サーバの役割と通信プロトコル	ネットワークにおいてサーバが担う役割やその基本的な仕組み、ネットワークサーバの機能、特徴を説明する。さらに通信プロトコルについて言及し、クライアントとサーバの通信によるサービスの提供方法について説明する。	1
I-9-2. ネットワークアドレス、ドメイン名やホスト名の意味	インターネットを構成する各ノードを識別する方式として、ネットワークのアドレス(IPアドレス)とドメイン名、ホスト名の構成を概説する。さらにネットワークバイトオーダやURI (Uniform Resource Identifier)など、関連するトピックを紹介する。	1
I-9-3. サーバの導入と設定方法	一般的なネットワークサーバ導入作業の概要と手順を、OSや必要なソフトウェアパッケージの入手、インストール、起動環境設定、ネットワーク設定、サービス提供内容の設定、サーバシステムの起動と停止など、順をおって具体的に示す。	2
I-9-4. 名前解決の仕組みとDNS	DNS (Domain Name System)の概要を説明し、DNSサービスを提供するDNSサーバの仕組みとDNSプロトコルについて解説する。またOSSによるDNSサーバ実装の歴史と背景など関連する情報も紹介する。	3
I-9-5. DNSサーバの構築・設定方法	Linuxで動作するネームサーバを導入、構築し、設定を行う手順を解説する。設定ファイルの各項目について、その意味と書き方を紹介し、実際に設定ファイルを作成する手順を示す。またネームサーバが実際に動作する状況について解説する。	3
I-9-6. Webサーバの仕組み	WWWの発展とWebサーバの機能や役割、CGIによるアプリケーション実行や拡張について説明する。OSSによるWebサーバ実装の歴史と背景、代表的なサーバの特徴についても述べる。また、HTTP (HyperText Transport Protocol)の概要と通信方式を解説する。	4
I-9-7. Webサーバの構築・設定方法	Linuxで動作するWebサーバを導入、構築し、設定を行う手順を解説する。設定ファイルの各項目について、その意味と書き方を紹介し、実際に設定ファイルを作成する手順を示す。またWebサーバが実際に動作する状況について解説する。	4
I-9-8. メールサーバの仕組み	ネットワークでメールをやりとりするために用意されるメールサーバの基本的な構成を解説する。メールを送信するSMTP (Simple Message Transfer Protocol)、受信したメールをクライアントにダウンロードするPOP (Post Office Protocol)など、関連するプロトコルを紹介する。	5
I-9-9. SMTPサーバの構築・設定方法	Linuxで動作するSMTPサーバを導入、構築し、設定を行う手順を解説する。また設定ファイルを作成する手順を示す。またメールサーバが実際に動作する状況について解説する。	5
I-9-10. POPサーバの構築・設定方法	Linuxで動作するPOPサーバを導入、構築し、設定を行う手順を解説する。また設定ファイルを作成する手順を示す。またメールサーバが実際に動作する状況について解説する。	5

【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 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
9. ネットワークサーバ管理に関する知識	<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	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	CE-SWE11. ソフトェアの標準化	
	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 [9-I-3,4]	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 [9-I-1]	CE-NWK5. データのセキュリティと整合性 [9-I-4]	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ネットワーク	13	CE-CAO コンピュータのアーキテクチャと構成	CE-CAO0. 歴史と概要	CE-CAO1. コンピュータアーキテクチャの基礎	CE-CAO2. メモリシステムの構成とアーキテクチャ	CE-CAO3. インタフェースと通信	CE-CAO4. デバイスサブシステム	CE-CAO5. CPUアーキテクチャ	CE-CAO6. 性能・コスト評価	CE-CAO7. 分散・並列処理	CE-CAO8. コンピュータによる計算	CE-CAO9. 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。サービスには一般的なインターネットプロトコルを扱う DNS、Web サーバ、メールサーバが含まれる。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学ぶこととなる。

科目名	第1回	第2回	第3回	第4回	第5回
9.ネットワークサーバ管理に関する知識 I	(1)クライアント/サーバ通信の仕組み (2)サーバの識別子	(1)サーバ構築に必要な環境と作業 (2)サーバ導入	(1)ネームサーバの特徴 (2)DNS サーバ構築	(1)Web サーバ導入の内容と手順 (2)Web サーバの仕組みと作業手順	(1)メールサーバの仕組みと構成 (2)メールサーバの仕組みと作業手順
	(3)JMX の概要	(3)インストール後の設定作		(3)セキュリサなサーバ	

（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 I	基本
習得ポイント	I-9-1. サーバの役割と通信プロトコル	
対応する コースウェア	第 1 回（ネットワークサーバの機能と特徴）	

I-9-1. サーバの役割と通信プロトコル

ネットワークにおいてサーバが担う役割やその基本的なしくみ、ネットワークサーバの機能、特徴を説明する。さらに通信プロトコルについて言及し、クライアントとサーバの通信によるサービスの提供方法について説明する。

【学習の要点】

- ＊ サーバを使うことで情報の管理や処理を集中的に行うことができ、ネットワーク利用を効率化し、情報伝達の手間を省力化できる。
- ＊ インターネットもイントラネットも TCP/IP という通信プロトコルに従って情報のやりとりがされており、OS が通信を担当している。
- ＊ 国際標準化機構によって制定された 7 階層に分割したモデルを OSI 参照モデルと呼び、TCP/IP もモデルで説明できる。
- ＊ サーバソフトウェアは、OSI 参照モデルのプレゼンテーション層やトランスポート層の機能を担当している。

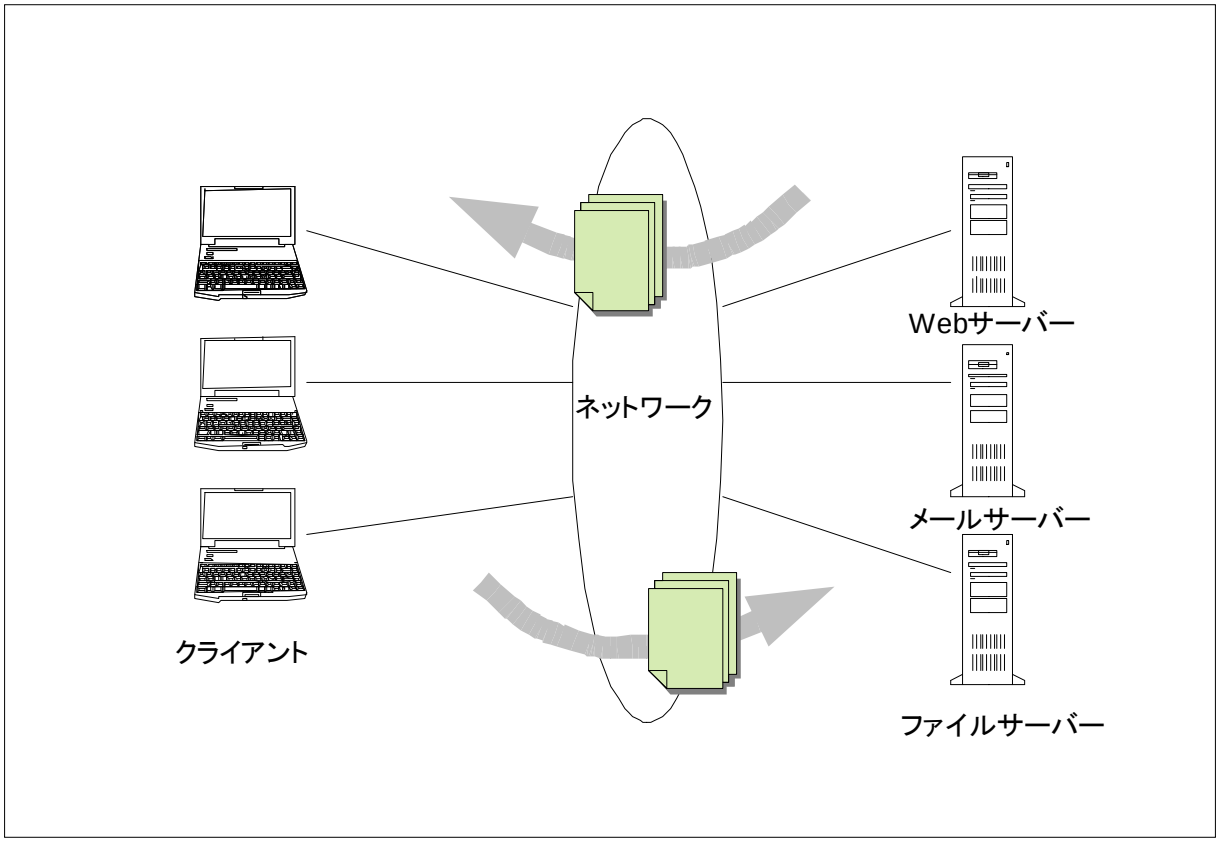

図 I-9-1.　サーバー・クライアント概念図

【解説】

1) サーバの役割

＊ サーバの役割

- ネットワークを介して、クライアントに対するサービス機能提供を行なう。
- 特定の業務やアプリケーションを処理するサーバが情報の管理や処理を集中的に行うことで、情報管理や処理を効率的にできるようになる。
- 企業内や組織内のイントラネットで提供されるイントラネットサーバと、インターネットで提供されるインターネットサーバに大きく分けることができる。

＊ イントラネットサーバ

- インターネットでの技術やプロトコルを利用する LAN(ローカルエリアネットワーク)のことをイントラネットと呼ぶ。
- イントラネットで使用するサーバは LAN に接続したクライアントへの機能提供を行う。
- プリンタサーバ、ファイルサーバが代表的なイントラネットサーバであるが、人事管理システム、勤怠管理システム、情報共有システムなど、その用途が拡大しつつある。

＊ インターネットサーバ

- インターネット上でサービスを提供しているサーバをインターネットサーバと呼ぶ。
- 利用対象者が特定できず利用時間も特定できないため、一般的なサービスでは 24 時間インターネットに接続し、稼動できることが必要条件となる。
- 代表的な例としては Web サーバ、メールサーバ、DNS サーバがある。

2) 通信プロトコル

＊ 機器同士が情報をやりとりするために、送信されるデータが送られる状況や順番する通信プロトコル(約束事)が定められている。

＊ インターネットもイントラネットも通信プロトコルには TCP/IP を利用している。

＊ TCP(Transmission Control Protocol)
OSI 参照モデルのトランスポート層に相当する。IP の上位プロトコルで、セッションによる 1 対 1 の通信を実現している。また、エラー訂正機能をもっているため、信頼性が高い。

＊ IP(Internet Protocol)
OSI 参照モデルのネットワーク層に相当する。異なるネットワークセグメントに属するクライアントとの通信を実現する。

3) OSI 参照モデル

- 国際標準化機構によって制定されている。
- 通信機能を 7 階層に分割し、異なるシステム間の通信を実現するためのモデルである。

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	9　ネットワークサーバ管理に関する知識 I	基本
習得ポイント	I-9-2. ネットワークアドレス、ドメイン名やホスト名の意味	
対応する コースウェア	第 1 回（ネットワークサーバの機能と特徴）	

I-9-2. ネットワークアドレス、ドメイン名やホスト名の意味

インターネットを構成する各ノードを識別する方式として、ネットワークのアドレス(IP アドレス)とドメイン名、ホスト名の構成を概説する。さらにネットワークバイトオーダや URI（Uniform Resource Identifier)など、関連するトピックを紹介する。

【学習の要点】

＊ TCP/IP プロトコルでは、ネットワーク上にある機器を区別するため IP アドレスという番号を使っており、通信機器や OS は IP アドレスで通信の制御を行っている。

＊ IP アドレスは桁の大きい数字で表記され分かりにくい。そのため人間が理解しやすい形から機器の扱いやすい数値に変換する仕組みが存在する。

＊ IP アドレスは、原則として一つの機器に対して一意に定められることで、世界中の通信したい相手に到達できる仕組みになっている。

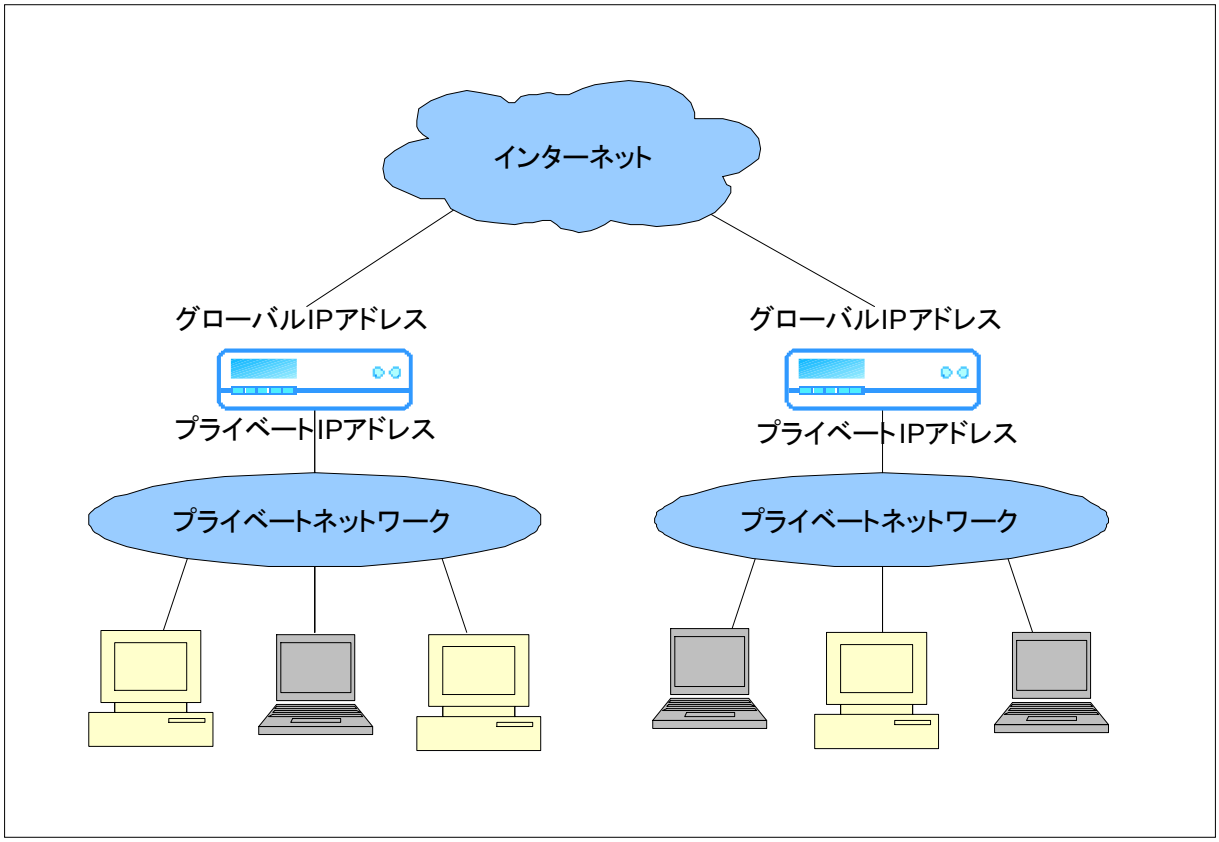

図 I-9-2.　ルーティングのイメージ図

【解説】

1) ネットワークアドレス

＊ IP アドレス

- TCP/IP では、ネットワーク上にある機器を一意に特定するため IP アドレスという番号を使用する。各機器は同じネットワークでの特定を可能にするため、すべて異なる IP アドレスをもつ。
- IP アドレスは 0～255 までの範囲の 4 つの数値を「.」で区切った形式で与えられる。

＊ グローバル IP アドレスとプライベート IP アドレス

IP アドレスは大きく 2 つに区分される。インターネット上からアクセスできる「グローバル IP アドレス」とイントラネットの IP アドレスである「プライベート IP アドレス」である。

- グローバル IP アドレス
  インターネット上からアクセスができる。割り当てはプロバイダが行う。
- プライベート IP アドレス
  イントラネット上からだけアクセスができる。イントラネット管理者が管理する。

＊ ネットワークアドレス

IP アドレスのうち各イントラネットやインターネットが管理するネットワークを識別するための部分のこと。

＊ ネットマスク

ネットワークアドレスと組み合わせて管理する IP アドレスの範囲を識別するためのもの。

＊ ルーティング

別々のネットワークに所属する機器が情報をやりとりするために、TCP/IP ではルーティングという手法を用いられる。ルーティングを行う装置としてはルータやレイヤ 3 スイッチがある。

＊ ネットワークバイトオーダ

複数バイトで構成されるデータを転送する場合には、転送する順番を決めておく必要がある。TCP では、ヘッダにビッグエンディアン(最上位のバイトから順番)で記録/送信することを決めている。

2) ドメイン名とホスト名

IP アドレスは数字で表記されて管理されているが、人間にとってわかりやすい名称(文字)との対応を管理する仕組みが存在する。

＊ ドメイン名

ネットワーク内にあるコンピュータや機器が属するグループを表すもの。www.example.com の example.com 部分を示す。

＊ ホスト名

ドメインに属するコンピュータ等に名前を与えてドメイン名と組み合わせて使うもの。

＊ URI(Uniform Resource Identifier)

ドメイン名とホスト名をあわせて、インターネットでの「住所」を示したもの。http や ftp といったプロトコル名をつけて、プロトコルごとに定義された書式で全体の住所を示す。

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 I	基本
習得ポイント	I-9-3. サーバの導入と設定方法	
対応する コースウェア	第 2 回（サーバシステムの導入）	

I-9-3. サーバの導入と設定方法

一般的なネットワークサーバ導入作業の概要と手順を、OS や必要なソフトウェアパッケージの入手、インストール、起動環境設定、ネットワーク設定、サービス提供内容の設定、サーバシステムの起動と停止など、順をおって具体的に示す。

【学習の要点】

＊ ネットワークサーバのインストールは GUI インタフェイスでも行うことができる。

＊ インストール後にはネットワーク接続確認を行い、ネットワークに参加できていることを確認する。

＊ セキュリティ向上のため、不要なサービスを導入しないことが望ましい。

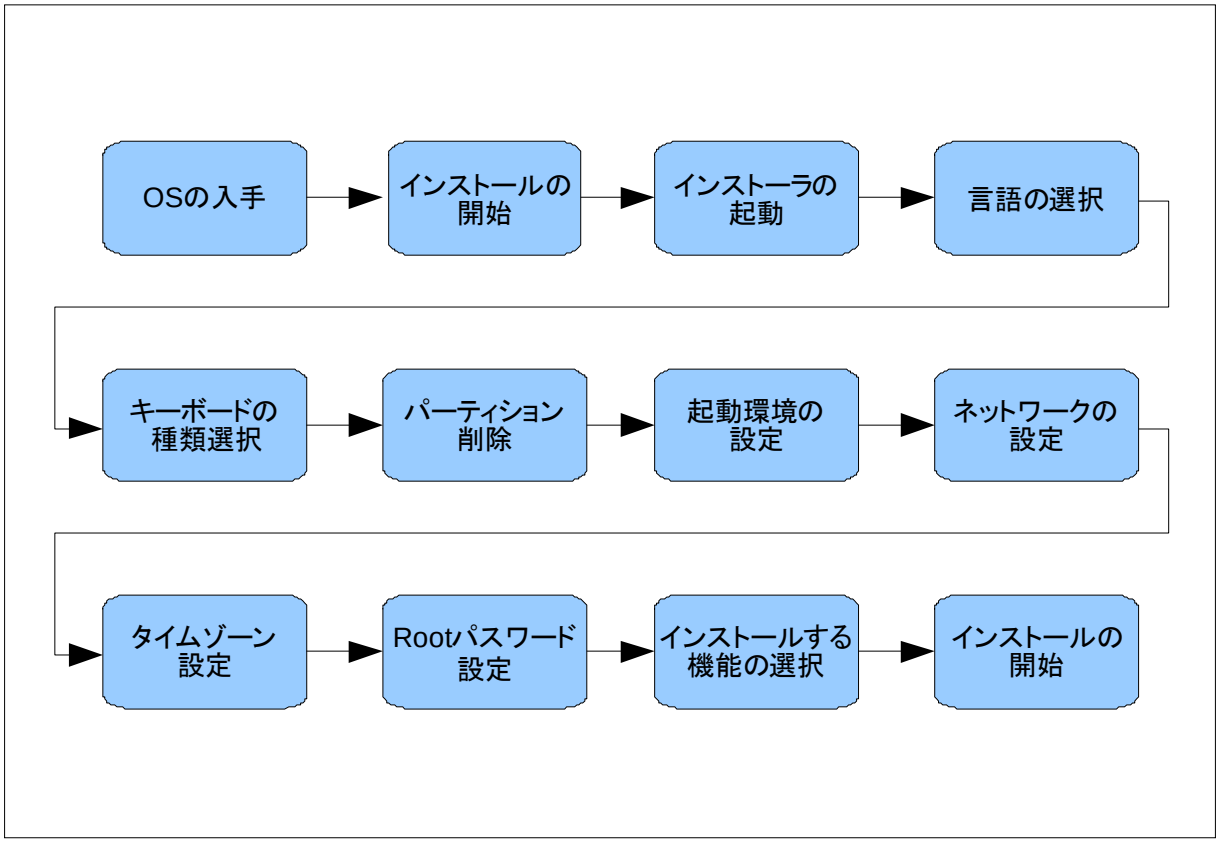

図 I-9-3.　インストールフロー

【解説】

1) ネットワークサーバの導入と設定

本文書では、ネットワークサーバ導入の例として Fedora Core 5 を使用した例を説明する。

＊ OS の入手
OS その他パッケージは以下の URL から最新版を入手する。
ftp://ftp.riken.jp/Linux/fedora/core/5/i386/iso/

＊ インストール
インストールを行うサーバを準備する。サーバの CD-ROMドライブにインストールする OS の CD を入れて、サーバを起動する。

＊ インストーラの起動
インストーラが起動したら、「Enter」キーを押してグラフィカルモードのインストーラが起動する。

＊ 言語の選択
言語の選択画面で English を選択する。

＊ キーボードの種類の選択
通常は日本で使われる 109 や 106 配列を選択する。

＊ パーティションを削除
すでにパーティションがあればパーティションの削除を行う。

＊ パーティションの設定
設定されたパーティションの情報が表示されるので次へ進む。

＊ 起動環境の設定
"Fedora Core /dev/volGroup00/LogVol00"にチェックが入っていることを確認して次へ進む。

＊ ネットワークの設置を行う
"Edit"ボタンをクリックし、ネットワーク管理者に確認した上で割り当てられたネットワーク情報を設定する。

＊ タイムゾーンの設定をする
Asia/Tokyo を選択する。

＊ root パスワードの設定をする
root のパスワード設定をする。

＊ インストールする機能を選択する
チェックのついている項目がインストールされるので、必要な項目を選択する。

＊ インストールの開始
インストールが開始する。

2) インストール後の設定

インストール後には以下の確認を行う。

＊ ネットワーク接続
ゲートウェイに ping 疎通確認を行い、応答があることを確認する。

＊ サーバシステムの起動・再起動
サーバシステムの停止・再起動は"shutdown"コマンドで行う。

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 I	基本
習得ポイント	I-9-4. 名前解決のしくみと DNS	
対応する コースウェア	第 3 回（ネームサーバの導入）	

I-9-4. 名前解決のしくみと DNS

DNS (Domain Name System)の概要を説明し、DNS サービスを提供する DNS サーバのしくみと DNS プロトコルについて解説する。また OSS による DNS サーバ実装の歴史と背景など関連する情報も紹介する。

【学習の要点】

* ホスト名でアクセスした場合に IP アドレスに変換する処理を名前解決とよび、名前解決を提供するのが DNS サーバである。
* DNS はインターネットにおける基本的なサービスであるため、システムの可用性が求められる。
* DNS サーバで最も多く使われているのは OSS の BIND である。

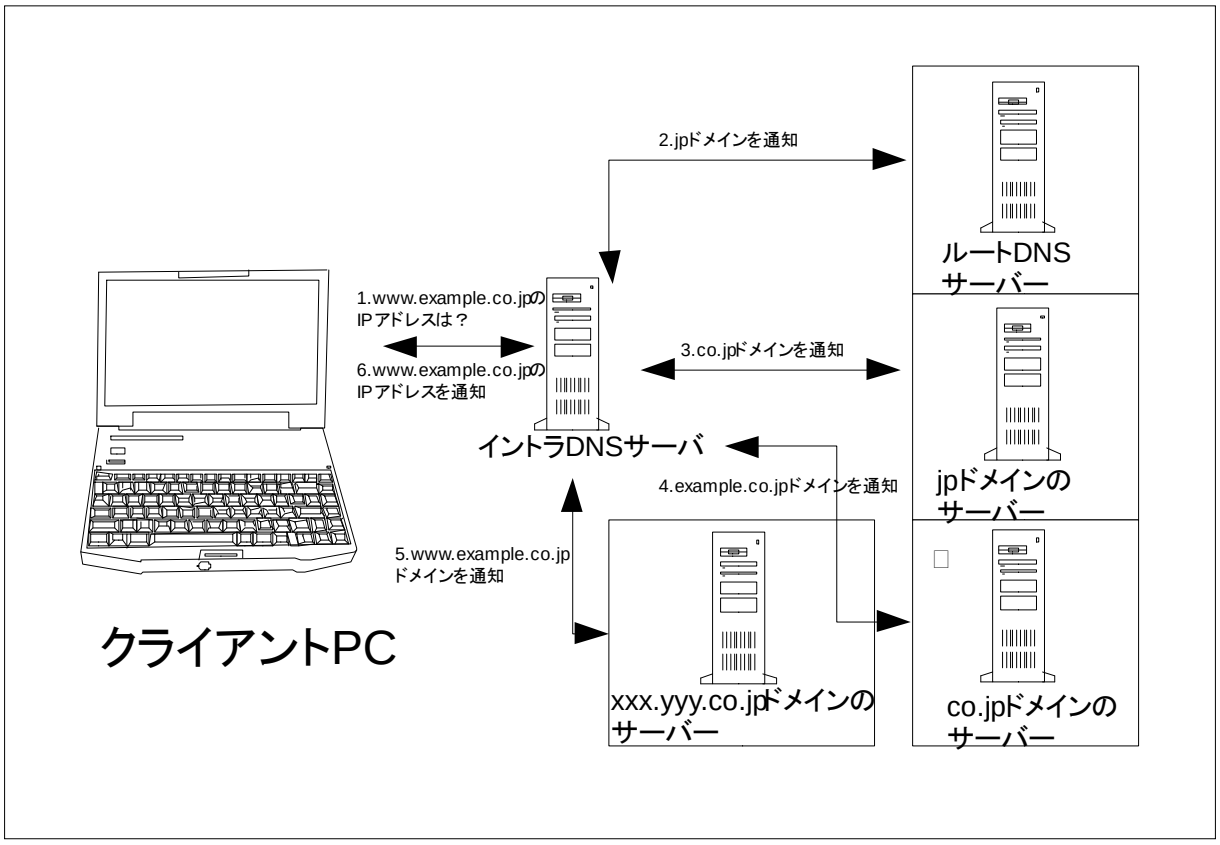

図 I-9-4.　DNS による名前解決

【解説】

1）DNS の役割

＊ インターネットでの実際のアクセスは、すべて IP アドレスに基づいて行う。

＊ ホスト名でのアクセスを IP アドレスに変換する処理を名前解決とよび、この機能を提供するのが DNS サーバである。

＊ DNS サーバの概念
インターネット上のホスト名と IP アドレスの組み合わせは膨大であり、かつ頻繁に追加・変更が発生するため、これらの情報を一カ所で管理することは現実的ではない。このため、ドメインごとに提供される DNS サーバが相互に情報を交換し合うことで名前の解決を行っている。

＊ 再帰問い合わせ
イントラネットでの名前解決を提供する DNS サーバは、クライアントからの問い合わせに対してその回答がキャッシュにないか確認する。キャッシュに存在しない場合は外部の DNS サーバに問い合わせを繰り返し行い名前解決を行う。これを再帰問い合わせと呼ぶ。

＊ DNS コンテンツサーバ
管理するドメインをもつ DNS サーバは、問い合わせを受けたホスト名が自らの管理ドメインである場合に、ホスト名に該当する IP アドレスを応答する。

＊ DNS プロトコル
DNS の問い合わせは UDP プロトコルで実装されている。

＊ プライマリ DNS とセカンダリ DNS
DNS サービスは、アクセスする実際の IP アドレス情報を提供するサービスであり、インターネットにおいて基幹となるものである。サービスの可用性を考慮し、プライマリ DNS とセカンダリ DNS の 2 つのサーバで構成されるのが一般的である。プライマリ DNS で更新された情報は自動的にセカンダリ DNS にコピーされる。

＊ 正引きと逆引き
正引きとは、ホスト名から IP アドレスを解決することで、逆引きとは IP アドレスからホスト名を解決することをいう。

2）OSS の DNS

OSS で DNS サーバのデファクトスタンダードは BIND（Berkeley Internet Name Domain）である。

＊ BIND の歴史

- 80 年代初期に DARPA の資金で開発される。
- 2000 年に現在の主流バージョンである BIND9 がリリースされる。
- 現在 BIND は ISC(Internet Systems Consortium)によって管理されている。

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	9　ネットワークサーバ管理に関する知識 I	基本
習得ポイント	I-9-5. DNS サーバの構築・設定方法	
対応する コースウェア	第 3 回（ネームサーバの導入）	

I-9-5. DNS サーバの構築・設定方法

Linux で動作するネームサーバを導入、構築し、設定を行う手順を解説する。設定ファイルの各項目について、その意味と書き方を紹介し、実際に設定ファイルを作成する手順を示す。またネーム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】

* BIND の設定は全体的な named.conf ファイルで行う。
* 各ドメインごとのホストの設定はゾーンファイルで行う。ゾーンファイルのレコードにはいくつかの種類がある。

named.confの例

```
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

zone "." IN {
        type hint;
        file "named.ca";
};

 zone "example.com" IN {
        type master;
        file "example.com.zone";
};

zone "10.168.192.in-addr.arpa" IN {
        type master;
        file "10.168.192.in-addr.arpa.zone";
};
```

図 I-9-5.　/etc/named.conf の設定

【解説】

1）BIND の設定

BIND の設定は以下のファイルで行う。

＊ named.conf

全体的な設定を行う。編集後には、BIND の再起動を行う。

- options ディレクティブ
  全体的な設定を記述する。
- diretory
  ゾーンファイルの設置してあるディレクトリを指定する。
- allow-transfer{}
  options ディレクティブに記述する。セカンダリ DNS サーバの IP アドレスを記述する。
- recursion
  options ディレクティブに記述する。再帰問い合わせを許可する場合は yes、しない場合は no を記述する。
- zone ディレクティブ
  自サーバで管理するドメイン名を記述する。
- type
  zone ディレクティブに記述する。プライマリ DNS の場合は master、セカンダリ DNS の場合は slave と記述する。
- file
  zone ディレクティブに記述する。ゾーンファイル名を指定する。

＊ ゾーンファイル

各 zone のホストやドメインの情報を記入する。1 行に 1 つのレコードが記述される。

- TTL
  他のネームサーバでキャッシュが保持される期間を設定する。単位は秒。
- SOA
  ドメイン自体に関する情報を記述する。Serial no の数を変更することでゾーン情報がセカンダリ DNS サーバに転送される。
- NS
  自分のドメインの DNS サーバのホスト名を記述する。セカンダリ DNS サーバについても記述する。
- A
  正引きのためのレコード情報。ホスト名から IP アドレスを調べるためのレコード。
- MX
  メールサーバのアドレスと優先順位を指定する。
- CNAME
  ホストの別名を記述する。
- PTR
  逆引きのためのレコード情報。

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 I	基本
習得ポイント	I-9-6. Web サーバのしくみ	
対応する コースウェア	第 4 回（Web サーバの導入）	

I-9-6. Web サーバのしくみ

WWW の発展と Web サーバの機能や役割、CGI によるアプリケーション実行や拡張について説明する。OSS による Web サーバ実装の歴史と背景、代表的なサーバの特徴についても述べる。また、HTTP (HyperText Transport Protocol)の概要と通信方式を解説する。

【学習の要点】

* WWW は個人や法人の情報交換を行うツールとして広く普及した。
* Web サーバは HTML ドキュメントに処理を組み込んだり、CGI アプリケーションなどで Web 画面に連動した動的処理を行ったりできる。
* OSS の代表的な Web サーバは Apache である。

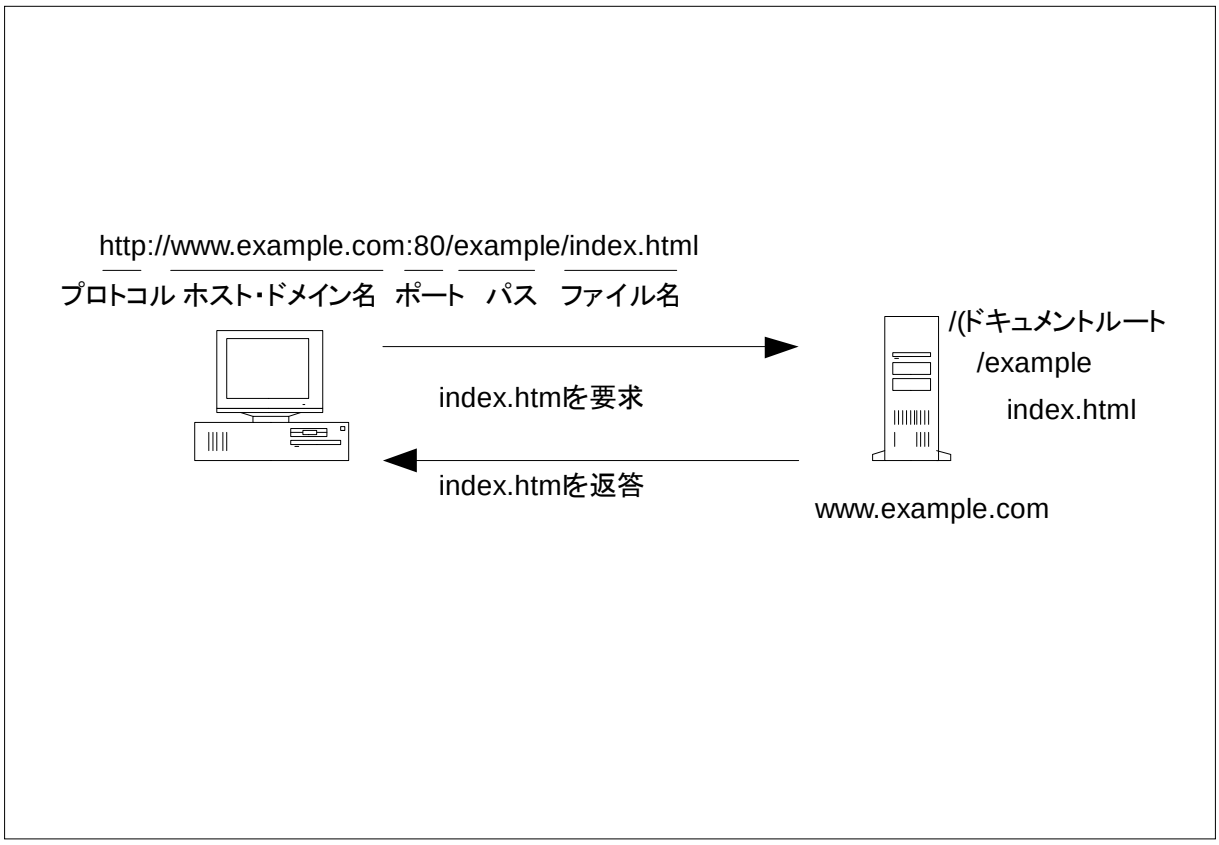

図 I-9-6.　HTTP のアクセス概念図

【解説】

1) WWW (World Wide Web)

1990 年代はじめに欧州原子核研究機構 (CERN)のメンバーが開発し、普及した。

＊ Web サーバの機能

- 機能
- HTTP プロトコルを介して HTML ドキュメントや画像などのコンテンツを送信する。ユーザの要求に対して、動的なコンテンツを都度生成し送信されることも多い。ユーザの要求ごとにコンテンツを生成する方法としては、HTML ドキュメントに処理を組み込む手法や、CGI アプリケーションなどを利用する方法がある。
- HTML(Hyper Text Markup Language)
  Web 上のドキュメントをクライアントのブラウザで表示するために、タグ付けされた言語(マークアップランゲージ)。Web の基幹的役割をもつ技術である。
- CGI(Common Gateway Interface)アプリケーション
  クライアントからの要求によって、Web サーバ上のプログラムを実行するための仕組みのこと。CGI アプリケーションの実装には Perl、 Ruby といったスクリプト言語や C 言語などが利用されることが多い。
- HTML 組み込みサーバサイドスクリプト
  Web サーバ上で要求されるたびに文書に記述されたプログラムをサーバ側で実行し、結果をブラウザに返すスクリプトのこと。PHP など。
- クライアントサイド・スクリプト
  Web サーバではなく、クライアントのブラウザ上で動作するスクリプトのこと。JavaScript など。Ajax によるリッチクライアントアプリケーション等に利用される。

2) OSS による Web サーバ実装

- Apache
  Web サーバのデファクトスタンダードとなっている。NCSA の開発した Web サーバをベースに作られている。
- lighttpd
  近年台頭してきた Web サーバ。高速な動作を目的に作成されている。

3) HTTP プロトコル

リクエスト-レスポンス型のプロトコルで、レスポンスメッセージの送信後にサーバは状態を保持しない。通常、80 番ポートを使用する。Web サーバは HTTP プロトコルに基づき、クライアントから要求されたサーバ上の HTML データを、HTTP コネクションに送信する。

- HTTPS
  SSL によって暗号化された HTTP プロトコル。通常、443 番ポートを使用する。
- WebDAV
  HTTP の拡張プロトコル。クライアントからファイルやフォルダを管理できるようにしたもの。

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 I	基本
習得ポイント	I-9-7. Web サーバの構築・設定方法	
対応する コースウェア	第 4 回（Web サーバの導入）	

I-9-7. Web サーバの構築・設定方法

Linux で動作する Web サーバを導入、構築し、設定を行う手順を解説する。設定ファイルの各項目について、その意味と書き方を紹介し、実際に設定ファイルを作成する手順を示す。また Web 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】

＊ Apache HTTP Server の設定は httpd.conf ファイルを編集して行う。httpd.conf ファイルは全体的な設定のほかに一つのサーバで複数のドメイン名を持つことの出来る VirtualHost の設定なども行うことができる。

＊ ユーザ領域で CGI を許可するためには、明示的に設定を行う必要がある。

Apacheの設定例 (httpd.conf)

```
Listen 80
ServerRoot "/etc/httpd"
DocumentRoot "/var/www/html/"

User  nobody
Group nobody

<Directory />
   Options FollowSymLinks
   AllowOverride None
</Directory>

<VirtualHost 192.168.10.0>
 ServerName example.com
 DocumentRoot /var/www/example.com
 ServerAdmin admin@example.com
</VirtualHost>
```

図 I-9-7.　httpd.conf 設定例

【解説】

1) Apache (Apache HTTP Server) の設定

Apache の設定は以下のファイルを編集して行う。設定後には Apache の再起動もしくは、設定ファイルの再読込を行う。

＊ httpd.conf
全体の設定を行う。

- DocumentRoot
Web サーバ上のルートディレクトリ。http://xxxx.xxxx.com/で示されるファイルが配置されたサーバ上のディレクトリ。

- Alias
特定のディレクトリをドキュメントルートのサブディレクトリに割り当てる

- DirectoryIndex
URL でファイル名が指定されない場合に表示されるファイル名を指定する。

＊ VirtualHost
httpd.conf ファイル内で設定を行う。DNS で設定した CNAME などで同じサーバ上で複数の Web サーバを運用する。VirtualHost ディレクティブ内で指定した対応ディレクティブは VirtualHost 外で指定されたディレクティブに上書きされる。

2) 設定の例

＊ CGI 設定
httpd.conf ファイル内で設定を行う。http://xxxx.xxxx.com/test.cgi が動作するようにする。

- AddHandler
.cgi という拡張子がついたファイルを CGI として処理するようにするため、.cgi を追加する。

- Options
CGI を実行できるように ExecCGI を追加する。

＊ アクセス制限(ユーザ)
特定ページへのアクセス時にパスワードを求める。

- httpd.conf
以下の設定を行う。
〈Directory {パスワードを求めたいディレクトリ}〉
AuthUserFile 〈パスワードファイル保存ディレクトリ〉
AuthType Basic
AuthName ByPassword
require user 〈パスワード認証時のユーザ名〉
〈/Directory〉

- パスワードファイルの作成
httpasswsd コマンドを実行する。
httppasswd -c 〈パスワードファイル保存ディレクトリ〉 〈パスワード認証時のユーザ名〉

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 I	基本
習得ポイント	I-9-8. メールサーバのしくみ	
対応する コースウェア	第 5 回（メールサーバ導入の内容と作業手順）	

I-9-8. メールサーバのしくみ

ネットワークでメールをやりとりするために用意されるメールサーバの基本的な構成を解説する。メールを送信する SMTP (Simple Message Transfer Protocol)、受信したメールをクライアントにダウンロードする POP (Post Office Protocol)など、関連するプロトコルを紹介する。

【学習の要点】

* 電子メールが送信されて配信されるまでの役割は MTA、MUA、MDA といった機能に分類される。
* クライアントから送信されたメールは SMTP プロトコルをリレーして目的のメールサーバに送信される。クライアントはサーバに届いたメールを POP プロトコルや IMAP プロトコルを介して読み出す。

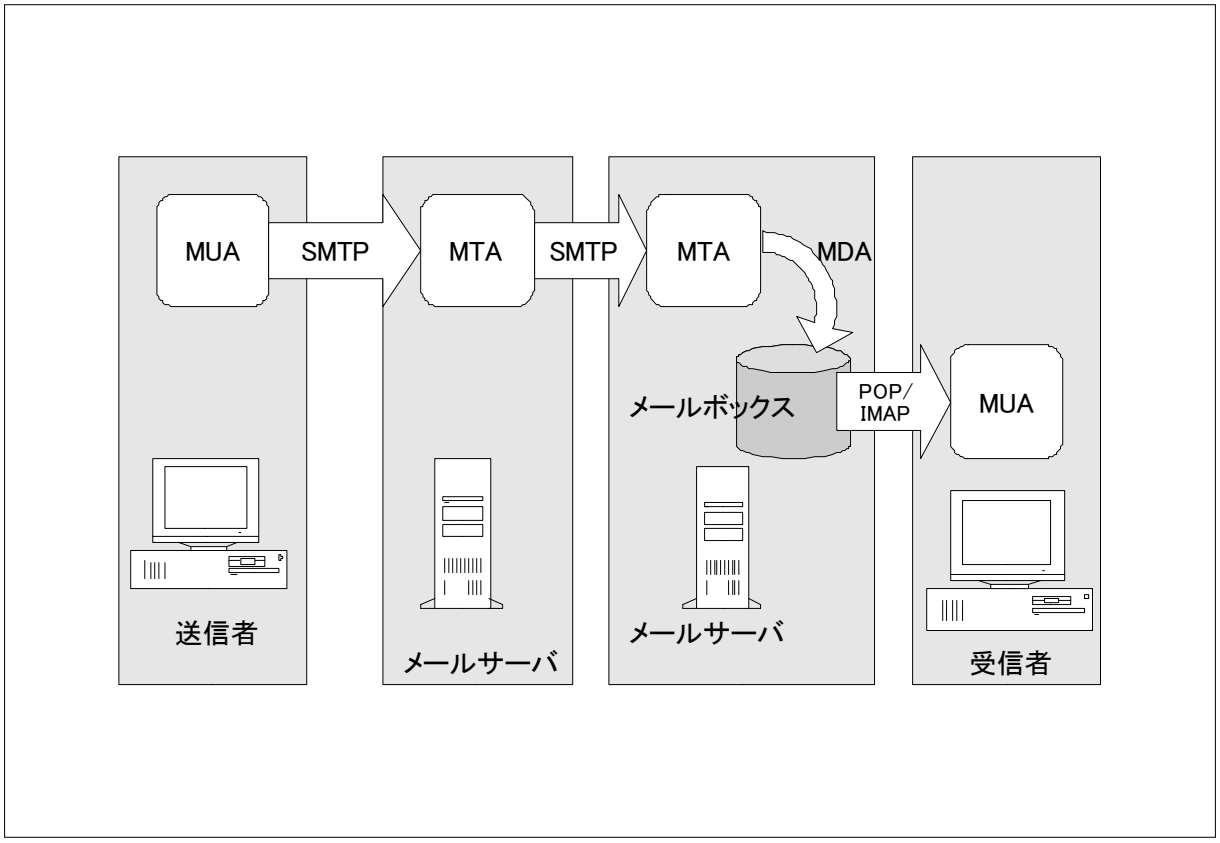

図 I-9-8.　メール概念図

【解説】

1) 電子メール

電子メールはインターネットにおけるコミュニケーションツールを代表するものである。

＊ MTA(Mail Transfer Agent)
クライアントからのメールを受信したり、MTA 間で転送したり MDA に配送する機能のこと。

＊ MDA（Mail Delivery Agent）
MTA によって配送されたメールを受信者ごとに配送する機能のこと。

＊ MUA(Mail User Agent)
電子メールを送受信し管理するためのアプリケーションソフトウェアのこと。

2) プロトコル

クライアントから送信されたメールはSMTPプロトコルをリレーして目的のメールサーバに送信される。クライアントはサーバに届いたメールを POP プロトコルや IMAP プロトコルを介して読み出す。

＊ SMTP(Simple Mail Transfer Protocol)
メールサーバの MTA 間の転送や、MUA から MTA へのメール送信に使われるプロトコル。電子メールを転送するプロトコルである。通常 TCP のポート番号 25 を利用する。OSS の代表的な STMP に sendmail、postfix がある。

- SMTP Auth
MUA から MTA へメール送信するときに認証を設ける必要があるため SASL メカニズムを利用した認証機構。

- SMTPs（SMTP over SSL）
SMTP と TLS/SSL を組み合わせて安全なメールの送信を実現するプロトコル。通常 TCP のポート番号 465 番を利用する。

＊ POP3（Post Office Protocol）
ユーザが MTA から MUA に自分のメールを読み出す際に使用する、メール受信用プロトコル。現在は、POP3（POP Version 3）が使用され、TCP のポート番号 110 番を利用する。

- POPs（POP over SSL）
POP3 と TLS/SSL を組み合わせて安全なメールの送信を実現するプロトコル。通常 TCP のポート番号995 番を利用する。

＊ IMAP（Internet Message Access Protocol）
MTA 上のメールにアクセスし操作するためのプロトコル。POP では MUA を使用して自分のメールをダウンロードするが、IMAP ではサーバ上にメールを保存したまま操作を行う。通常、IMAP4 は IMAP Version 4 revision 1(IMAP4rev1) のことを示し、TCP のポート番号 143 番を利用する。

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 I	基本
習得ポイント	I-9-9. SMTP サーバの構築・設定方法	
対応する コースウェア	第 5 回（メールサーバ導入の内容と作業手順）	

I-9-9. SMTP サーバの構築・設定方法

Linux で動作する SMTP サーバを導入、構築し、設定を行う手順を解説する。また設定ファイルを作成する手順を示す。またメール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】

* sendmail の設定ファイルは sendmail.cf で行うが、通常 sendmail.mc という定義ファイルを使用して自動生成を行う。
* パスワード認証などによるメール投稿のアクセス制限を実現するためには、メールサーバの他にセキュリティ認証ソフトウェア(SASL)の設定を行う必要がある。
* sendmail のほかに代表的な MTA として Postfix がある。

Sendmailcfの設定テスト例

外部へのメール配送を自身のサーバで行う場合の設定

```
# /usr/lib/sendmail -C/etc/mail/sendmail.cf -bt
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>

> 3,0 admin@example.com
rewrite: ruleset   3   input: admin @ example . com
rewrite: ruleset  96   input: admin < @ example . com >
rewrite: ruleset  96 returns: admin < @ example . com >
rewrite: ruleset   3 returns: admin < @ example . com >
rewrite: ruleset   0   input: admin < @ example . com >
rewrite: ruleset  88   input: < smtp : example . com > . admin < @ example . com >
rewrite: ruleset  88 returns: $# smtp $@ example . com . $: admin < @ example .
com >
rewrite: ruleset   0 returns: $# smtp $@ example . com . $: admin < @ example .
com >
>
```

図 I-9-9.　sendmail の設定テスト例

【解説】

1) sendmail 設定

sendmail の設定ファイルは sendmail.cf で行うが通常 sendmail.mc という定義ファイルを使用して自動生成を行う。sendmail.mc は変更後 make することで sendmail.cf ファイルが生成される。

＊ ドメイン設定
local－host－names ファイルに管理するドメイン名を記述する。

＊ クライアントのアクセス制限
MUA から送信される MTA サーバでは MUA のアクセス制限を行う。access ファイルに MUA の IP アドレスを記述する。

2) SASL 設定

SMTP Auth によるアクセス制限を実現するため SASL の設定を行う。設定の際には、cyrus－sasl パッケージをインストールしておく。

＊ sendmail.cf 設定
sendmail.mc で以下の箇所のコメントをはずし、sendmail.cf ファイルを生成する。

dnl TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl

＊ パスワードの設定
認証用のユーザを作成する。
saslpasswd2 -c 〈認証用ユーザ名〉

＊ semdmail の再起動
sendmail を再起動する。

3) Postfix 設定

sendmail とは別の SMTP ソフトである postfix の設定について説明する。

＊ main.cf
postfix の設定は main.cf で行う。

- mydestination
  sendmail のlocal－host－names の設定と同じ。自分が管理するドメインを記述する。
- mynetworks
  sendmail の access ファイルと同じ。信頼できる MUA の IP アドレスやホスト名、ドメイン名を記述する。
- myhostname
  自分自身のホスト名を記述する。

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 I	基本
習得ポイント	I-9-10. POP サーバの構築・設定方法	
対応する コースウェア	第 5 回（メールサーバ導入の内容と作業手順）	

I-9-10. POP サーバの構築・設定方法

Linux で動作する POP サーバを導入、構築し、設定を行う手順を解説する。また設定ファイルを作成する手順を示す。またメール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】

- POP サーバは、メールを利用者が PC 等で利用しているメールクライアント(MTA)に転送するサービスを提供する。
- 標準的な POP サーバの例としては pop3d がある。
- POP のプロトコルとして認証方式の違いから POP3 や APOP などがある。

dovecotの設定

/etc/dovecot.conf

* pop3のみを利用する場合

```
protocols = imap imaps pop3 pop3s
```

* pop3とpop over sslを利用する場合

```
protocols = pop3 pop3s
```

* pop3とimap4を利用する場合

```
protocols = imap pop3 pop3s
```

* apopの設定

```
auth default {
  mechanisms = plain apop
}
```

図 I-9-10.　Pop のテスト例

【解説】

1）POP3 プロトコル

POP3 プロトコルはユーザエージェントと POP サーバをつなぐプロトコルである。

＊ 代表的な POP サーバ

- ipop3d
  xinetd で動く pop3 デーモン。xinetd で起動して使用する。
- dovecot
  dovecot の設定は、dovecot.conf で行う。使用するプロトコルを記述する。pop3 のみを使う場合は pop3 と記述する。Dovecot では IMAP やPOP3s も利用することができるので利用する場合はスペースを空けて記述する。設定したら、dovecot の再起動を行う。

2）POP3 に関連するプロトコル

＊ APOP
POP3 では、ユーザ認証のためのパスワードも暗号化されずに送信されるため、APOP ではパスワードを暗号化して、安全性の向上を行う。

＊ POP3 over SSL

POP では、メールのメッセージが暗号化されずにやりとりされるため、HTTP で使用される SSL 暗号化を使用してメール自体の暗号化を行うためのプロトコルである。通常、995 番ポートを利用する。

3）IMAP

PO3P のほかにメール受信用のプロトコルとして IMAP4 があげられる。

＊ IMAP4
POP3 がクライアント側にメッセージをダウンロードして、メッセージの管理を行うのに対し、IMAP はサーバ側でメッセージの管理を行う。クライアントはサーバ上にあるメッセージの操作を行うプロトコルである。通常 143 番ポートを利用する。