

第1章

ネットワークの概要

学習目標

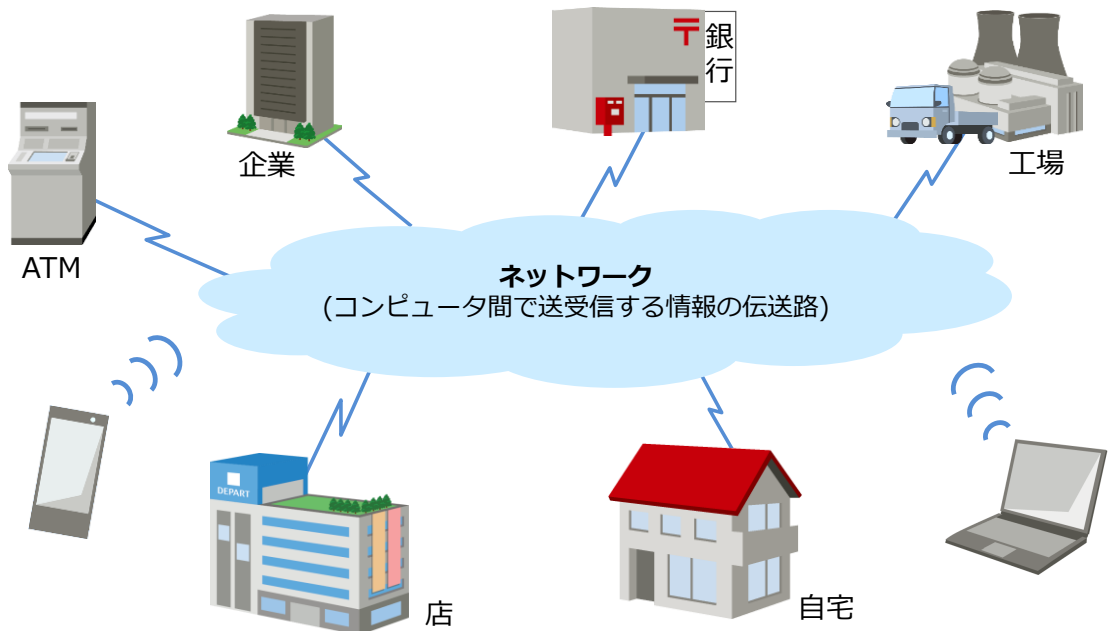
この章では、ネットワークの利点や基本的なネットワーク用語を学習します。

- ネットワークの利点を理解する。
- インターネット、イントラネット、LAN、WANなどの用語を理解する。

1.1 ネットワーク

1.1.1 ネットワークとは

地理的な制限を排除し、迅速な通信が可能

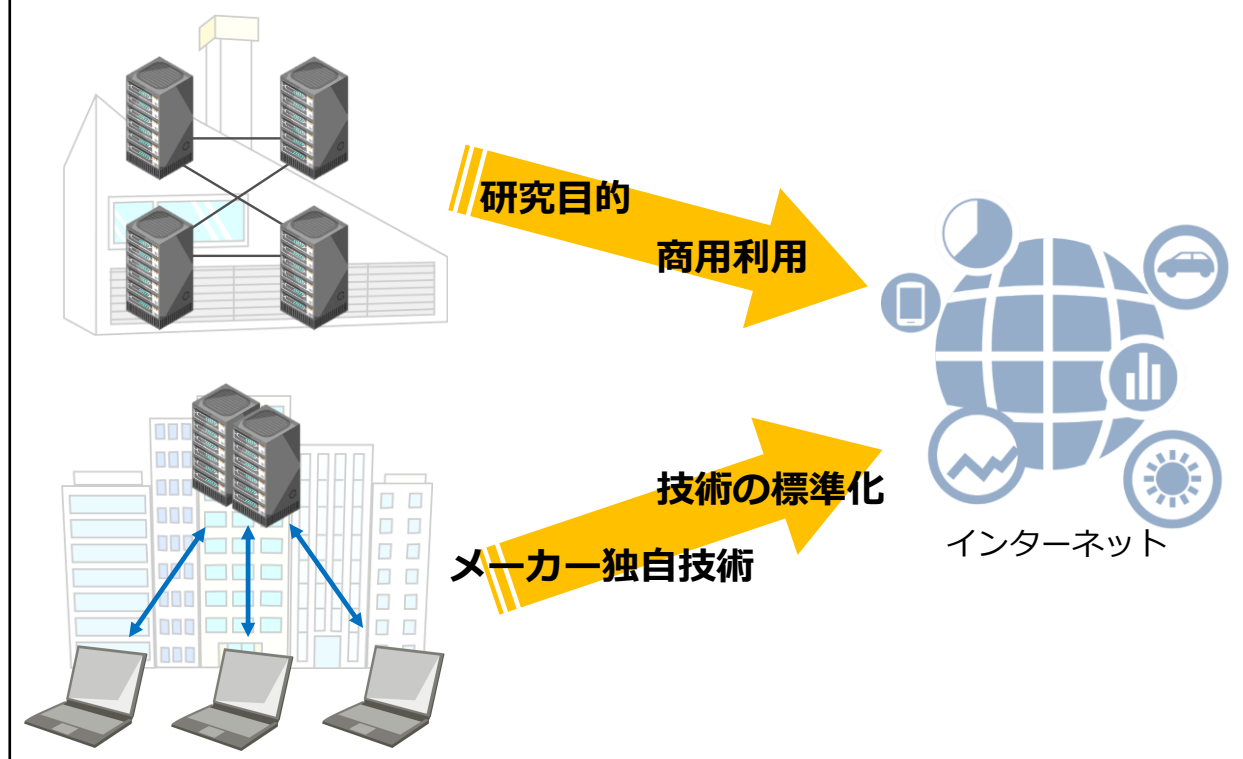


まずは、ネットワークの定義を確認します。

ネットワークとは、コンピュータ間で取り扱われるさまざまな情報を伝達し合うための伝送路の集合です。ここでのコンピュータとは「通信可能な機械」を意味します。たとえば、パソコンに限らず、汎用機、携帯電話、モバイル機器などです。

ネットワークを利用することで、企業や商店、一般家庭に存在するコンピュータを接続し、地理的、物理的に依存せず、情報のやり取りが可能です。あらゆる情報はネットワークを介して伝達されています。私たちにとって、ネットワークはなくてはならない存在です。

1.1.2 ネットワークの生い立ち



ここでは、ネットワークの生い立ちを確認します。

ネットワークは、コンピュータが開発された頃、コンピュータと周辺機器間で情報の伝達をするために登場しました。そして、複数台のコンピュータ間で通信するための技術として発展し、今では世界中のコンピュータを接続する巨大な通信網に成長しました。

周辺装置の接続、またはホストコンピュータと操作系端末との接続を主な用途として開発された通信技術は、コンピュータを製造したメーカーごとに存在し、異なるメーカー間での互換性はありませんでした。

一方で、1960年代に、DoD(米国国防総省)のARPA(高等研究計画局)がARPANETを構築し、パケット交換技術の開発・研究などを行いました。当初は、研究目的でしたが、1980年代後半には商用に転換され始め、今のインターネットの姿となります。インターネットで採用された通信技術は、コンピュータを製造する各メーカーで採用され、世界中に普及し、インターネット利用者也増加しました。

こうして、ネットワーク技術が普及し、ネットワーク通信は私たちの生活の身近なものとなりました。インターネットを取り巻く代表的な出来事にはこのような事がありました。

年	出来事
1967	ARPANET研究プロジェクト発足 (ARPANET運用開始は1969年)
1974	IBMがSNA（ネットワークアーキテクチャ）を公開
1980	Ethernet規格公開
1981	TCP/IP version 4（現在主流の規格）公開
1989	世界初のインターネットサービスプロバイダー（PSINet）登場

【用語解説】

ホストコンピュータ:

コンピュータネットワークの中で、データの処理や管理を一手に引き受けている大型コンピュータです。略して「ホスト」、または「メインフレーム」とも言います。

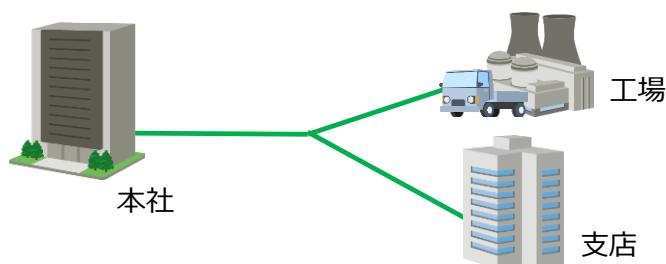
1.2 ネットワークの種類と特徴

1.2.1 インターネットとイントラネット

インターネット = 世界最大規模のネットワーク（利用者制限なし）



イントラネット = 企業/団体のネットワーク（関係者のみ利用可能）



ここでは、ネットワークの種類と特徴を確認します。

ネットワークを、利用者の特徴により2つの種類に分類できます。

インターネットと**イントラネット**です。

・インターネット

インターネットとは、世界中にあるネットワークが相互に接続された、世界で一番大きなネットワークの名前(固有名詞)です。利用者の制限はなく、インターネットへ接続することができれば、あらゆる情報へ自由にアクセスできます。WWW（World Wide Web）やMailを利用して、インターネット利用者間での情報交換が可能です。

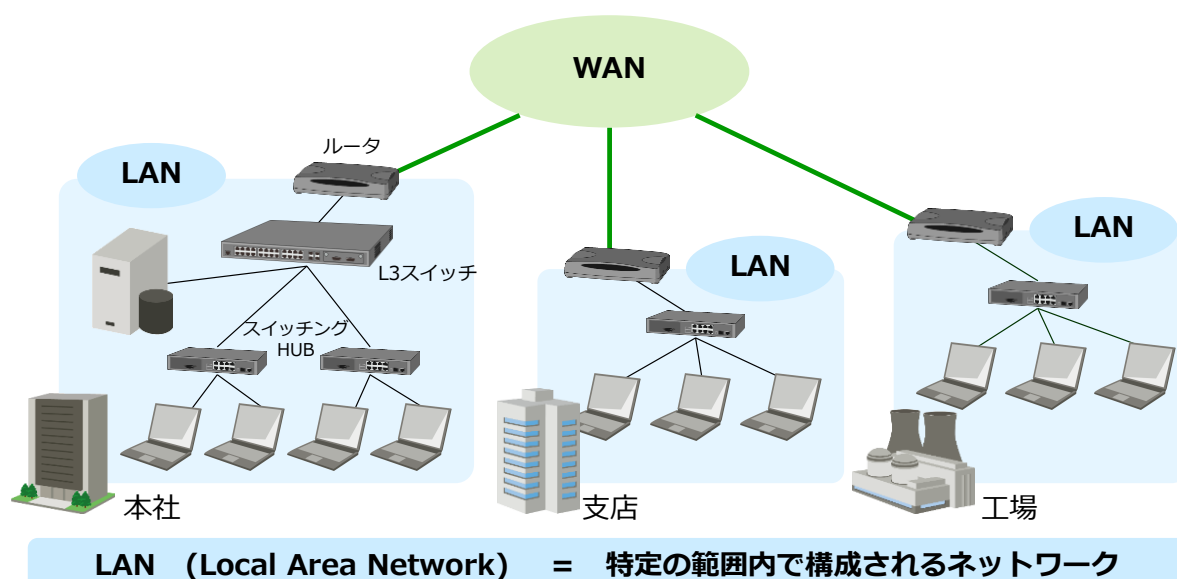
・イントラネット

イントラネットとは、企業や団体の資産（コンピュータやシステム）を接続したネットワークです。接続されている拠点内および拠点間で情報交換、情報共有することが可能であり、利用者也関係者のみに制限されます。インターネットで発展した技術を利用するため、インター「inter：対等な個々の関係」に対して、イントラ「intra：範囲内の～」と表現します。

1.2.2 LANとWAN

イントラネット

WAN (Wide Area Network) = 地理的に離れているLANを相互接続するネットワーク



次に、LANとWANを確認します。

イントラネットを、構築する場所により2つの種類に分類できます。**LAN**と**WAN**です。

•LAN (Local Area Network)

自敷地内、自構内に構築された自前のネットワークです。自己構築、自己運用が前提です。設備の手配や論理設計、ポリシー設計などは、すべて管理者が行います。

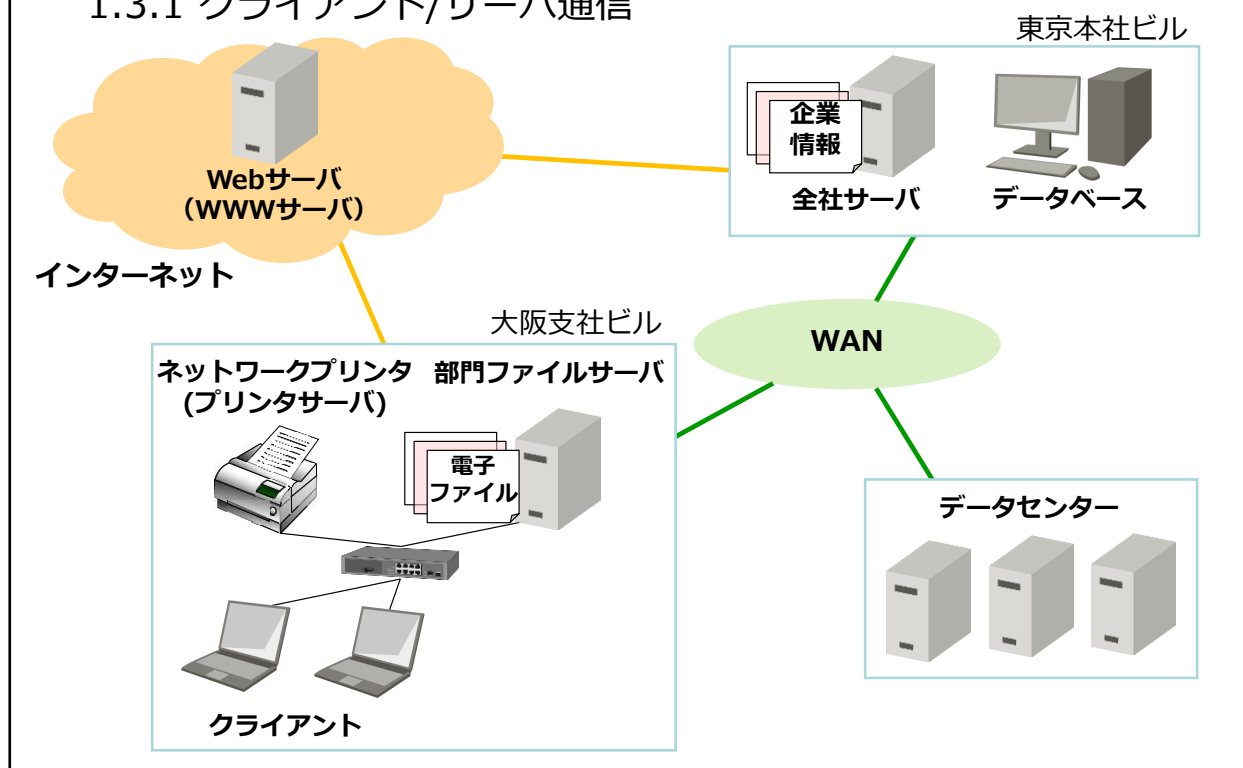
•WAN (Wide Area Network)

地理的に離れた地域間を結ぶためのネットワークです。通信キャリアからサービスとして提供され、契約し利用します。一般に、利用者が独自にWANを敷設することはできません。

通信キャリアにより管理されたネットワークなので、セキュリティが高いという特徴があります。また、契約時には通信速度を指定することもでき、高品質な回線を利用できます。

1.3 ネットワークの利用形態

1.3.1 クライアント/サーバ通信



ここでは、ネットワークの利用形態を確認します。

ネットワークには、さまざまな情報が保存されている**サーバ**と情報を閲覧/編集するための**クライアント**という2つの立場のコンピュータがあります。

•イントラネットの場合

イントラネットには、部署内の共有データを格納するファイルサーバやプリンタサーバがあります。従業員は自席にあるコンピュータ(クライアント)からサーバへ接続し、必要な情報を閲覧および取得できます。サーバは、クライアントと同じ事業所になければならないわけではなく、他の事業所やデータセンターに存在する場合があります。

•インターネットの場合

インターネットには無数のサーバが存在しています。その情報は、だれでも参照できるよう公開されており、WWWやMailを利用して膨大な情報を自由に取得できます。

このようにネットワークを利用することで、物理的な場所に制限されず、あらゆる場所に点在する資源(プリンタ、サーバ、システムなど)を共有できます。

また、企業内に資源や情報を保持せず、データセンターやインターネット上のサーバに情報を集約し、情報管理を外部業者へ委託する方法もあります。ネットワークの利用形態が変化しつつあります。

【用語解説】

サーバ:

各種資源 (プログラム、データなど)を提供するコンピュータ。サーバには高性能、高信頼性が求められるため、サーバ専用機と呼ばれる高性能のコンピュータ上にサーバOSを組み込む。サーバOSの例として、Windows Server、UNIX、Linux、BSDなどがある。

クライアント:

サーバが提供する資源を利用するコンピュータ。通常は、デスクトップPCやノートPC、スマートデバイスを利用する。クライアントOSの例として、Windows 10、Android、macOSなどがある。

1.4 章のまとめ

- ネットワークはコンピュータ間で送受信する情報の伝送路の集合とその仕組みです。
- ネットワークのメリットは地理的な制限を排除し、迅速に通信できることです。
- ネットワークは利用者の特徴により、インターネットとイントラネットの2種類に分類できます。
 - ✓ インターネット : 利用者の制限がなく、世界中のネットワークが相互に接続されている、世界で一番大きなネットワークの名前
 - ✓ イントラネット : 利用者は関係者に限られ、企業や団体の資産が接続されている、特定の範囲内のネットワーク
- ネットワークは構築する場所により、LANとWANの2種類に分類できます。
 - ✓ LAN : 自敷地内、自構内に構築された自前のネットワーク
 - ✓ WAN : 地理的に離れた拠点を接続するネットワーク
- クライアント/サーバ通信では、2つの立場があります。
 - ✓ サーバ : クライアントに資源（プログラム、データなど）を提供するコンピュータやソフトウェア
 - ✓ クライアント : サーバの提供する資源を利用するコンピュータやソフトウェア

第1章のまとめです。

- ネットワークはコンピュータ間で送受信する情報の伝送路の集合とその仕組みです。
- ネットワークのメリットは地理的な制限を排除し、迅速に通信できることです。
- ネットワークは利用者の特徴により、インターネットとイントラネットの2種類に分類できます。
 - ✓ インターネット :
利用者の制限がなく、世界中のネットワークが相互に接続されている、世界で一番大きなネットワークの名前
 - ✓ イントラネット :
利用者は関係者に限られ、企業や団体の資産が接続されている、特定の範囲内のネットワーク
- ネットワークは構築する場所により、LANとWANの2種類に分類できます。
 - ✓ LAN :
自敷地内、自構内に構築された自前のネットワーク
 - ✓ WAN :
地理的に離れた拠点を接続するネットワーク
- クライアント/サーバ通信では、2つの立場があります。
 - ✓ サーバ :
クライアントに資源（プログラム、データなど）を提供するコンピュータやソフトウェア
 - ✓ クライアント :
サーバの提供する資源を利用するコンピュータやソフトウェア

第2章

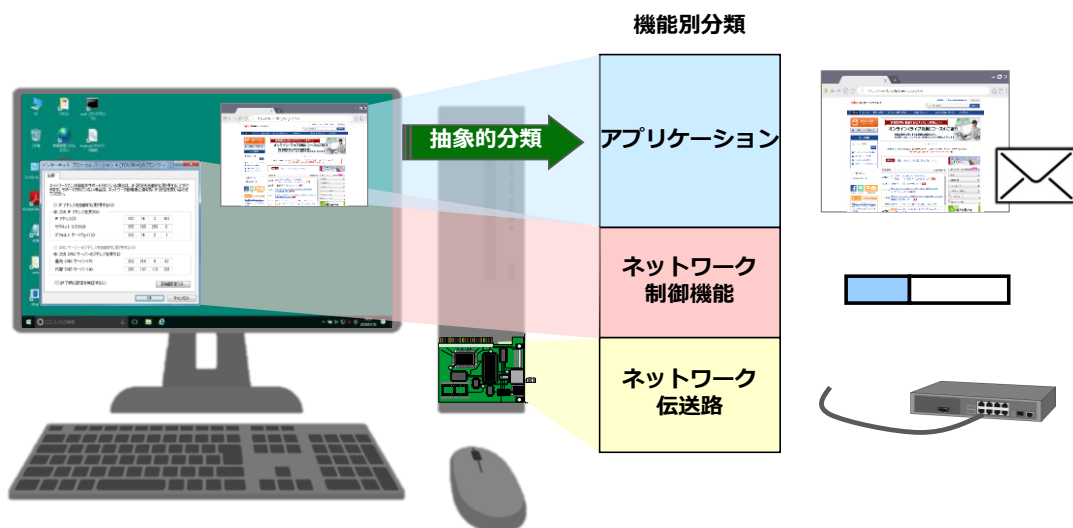
ネットワーク技術の全体像

学習目標

この章では、ネットワーク技術の全体像や技術モデルを学習します。

- OSI参照モデルについて理解する。
- TCP/IPについて理解する。
- ネットワークアーキテクチャ、プロトコルなどの用語を理解する。

2.1 ネットワーク技術の機能による分類



コンピュータネットワーク技術は、さまざまな技術が連携することにより通信を実現しています。機能別に大きく3つに分類できます。

•アプリケーション(ソフトウェア)

他のコンピュータと情報伝送を行うために必要となるソフトウェアです。このソフトウェアは、利用するサービスに応じて各種提供されています。

例)電子メールクライアントソフトウェア(メーラー)、Webブラウザ など

•ネットワーク制御機能(ソフトウェア)

コンピュータのOSがデータ伝送の制御をするために組み込むソフトウェアです。このソフトウェアは、他のコンピュータとの通信方法や伝送時のデータ制御の方法によって各種提供されています。

例) TCP/IP プロトコル、IPX/SPX プロトコル など

•ネットワーク伝送路(ハードウェア)

コンピュータをネットワークに接続するために必要となるハードウェアです。利用用途や価格に応じて、各種提供されています。

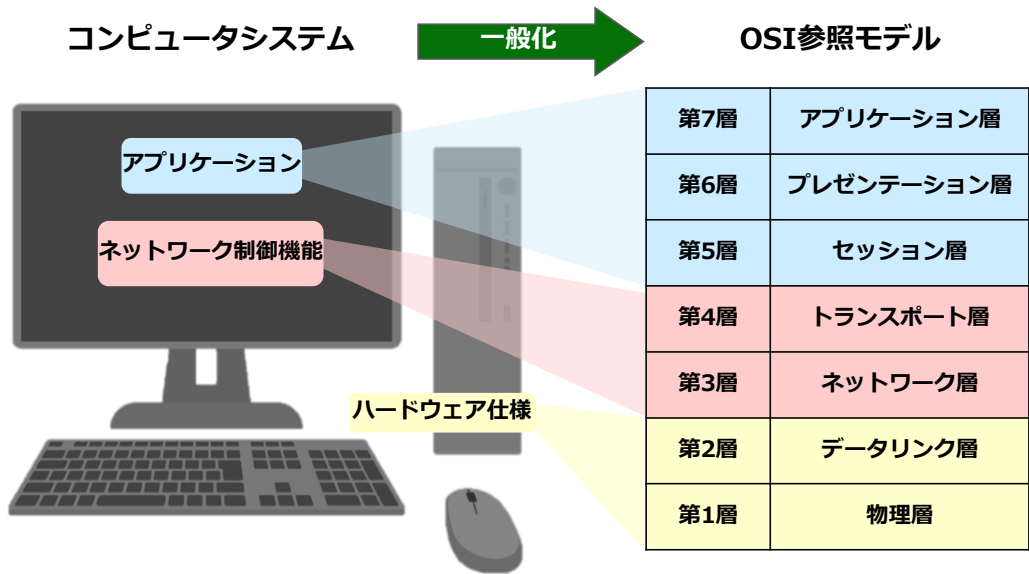
例) 100BASE-TX 用LAN カード、ツイストペアケーブルなど

ネットワーク技術は、上記の3つの機能のいずれか1つでも欠けると通信を実現することができません。また、複数の技術の中から連携が取れる組み合わせを選ぶ必要があります。特徴のあるネットワーク技術を体系的に整理し、個々の技術の位置づけを明確にとらえる必要があります。

次は、世界中で共通の概念として取り扱われるOSI参照モデルを解説します。

2.2 OSI参照モデル
2.2.1 OSI参照モデルとは

コンピュータネットワークの技術群を一般化した抽象モデル



OSI (Open Systems Interconnection)参照モデルとは、情報システムの一般化されたモデルシステムです。ISO (International Organization for Standardization)で検討された国際標準規格であり、世界中で共通の概念として取り扱われています。

OSI参照モデルでは、ネットワークに接続されるコンピュータ間でデータ交換のために必要とされる各種仕様を7つの階層に分類しています。ハードウェアの仕様である物理層から始まり、ユーザーインターフェースであるアプリケーション層まで規定しています。各層は1～7層まで順に積み重なって1つのシステムを構成しています。また、各階層の役割は独立して規定されています。

OSI参照モデルは、ネットワーク技術の全体像と個別技術の位置づけを関連付けることができるため、コンピュータネットワークを理解する際の大きな指針となっています。ネットワークの構築や障害発生時の対応、ネットワークシステムの開発などでは、この OSI 参照モデルの枠組みに沿って作業が行われています。

2.2.2 OSI参照モデルの各層の役割

第7層	アプリケーション層	アプリケーションの操作方法に関する仕様
第6層	プレゼンテーション層	データ形式の共通化に関する仕様
第5層	セッション層	通信の開始から終了までを制御する仕様
第4層	トランスポート層	アプリケーション間通信の独立性およびデータ転送制御に関する仕様
第3層	ネットワーク層	送信元から宛て先までの経路決定に関する仕様
第2層	データリンク層	ハードウェア上でのデータ伝送に関する仕様
第1層	物理層	システムに組み込むべきハードウェアの仕様

ここでは、OSI参照モデルの各層の役割について確認します。

•アプリケーション層

コンピュータ(OS)の種類によりファイルシステムや命令コマンドが異なります。ユーザーがこれらの違いを意識せずに共通操作できる仕様が規定されます。

•プレゼンテーション層

文字や数値の表現方法はOSやコンピュータの種類で異なります。標準的なデータ形式に変換する方法について規定されます。

•セッション層

アプリケーションの状態やユーザーからの操作に合わせて、セッションという単位で通信の開始・維持・終了を制御する方法について規定されます。

•トランスポート層

同一コンピュータ内から複数のアプリケーション間通信を実現するために、各通信の独立性の維持や宛先まで正しくデータ転送するための制御方法について規定されます。

•ネットワーク層

送信元から宛て先までの経路の決定方法に関する仕様が規定されます。コンピュータシステムでは、複数の端末間でデータの転送を繰り返し目的の端末へ到達します。目的の端末への到達可能な通信経路を判断する方法が規定されます。

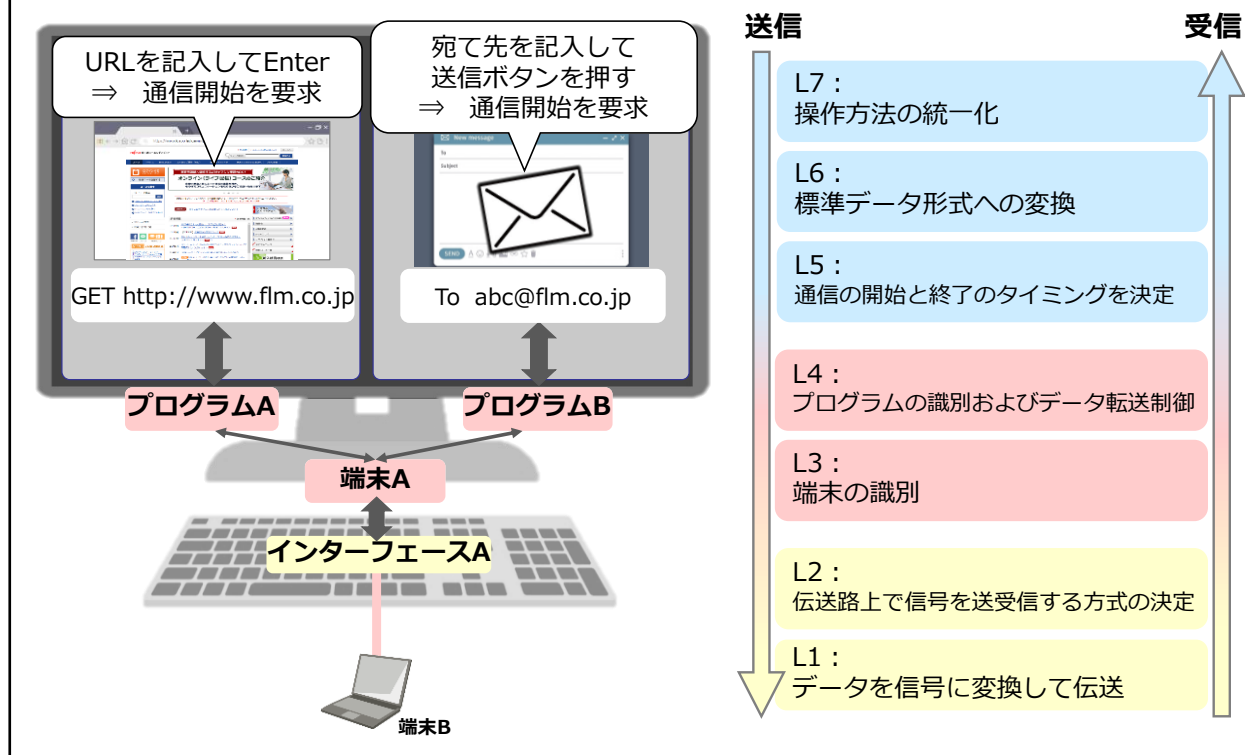
•データリンク層

ハードウェア上でのデータ伝送に関する仕様が規定されます。データの開始・終了を識別するフラグや誤り検出をするためのパラメーターなどが規定されます。また、伝送路へデータを送信するタイミングを規定し、複数の端末が同じタイミングでデータを送信した場合に発生する衝突を回避するための制御方法(アクセス制御)が規定されます。

•物理層

システムに組み込むべきハードウェアの仕様が規定されます。伝送路(銅線の数、コネクタの形状など)、信号(有線/無線、電気/光、電圧や周波数など)が規定されます。

2.2.3 OSI参照モデルと通信の流れ



ここでは、7階層に分類されたネットワーク技術の各役割を「通信を開始する端末」における通信を例に解説します。

- ①【アプリケーション層(第7層)】 WWWやメールを利用するためにユーザーインターフェースを操作します。
プログラムによりユーザーの操作に対して特定の命令コマンドが発行されます。ユーザーとコンピュータ間の情報の橋渡しをします。
- ②【プレゼンテーション層(第6層)】 標準データ形式へ変換されます。
コンピュータ(OSやハード)の違いによるデータ表現方法の差を吸収し、多様な環境でのアプリケーションが動作するよう調整します。
- ③【セッション層(第5層)】 アプリケーションからネットワーク制御機能にデータを渡すタイミングを取ります。
アプリケーションにおける通信の開始～終了を制御します。
- ④【トランスポート層(第4層)】 コンピュータ内の通信プログラムの識別およびデータ転送制御を行います。
適切なプログラム間でのデータの受け渡しができるよう制御します。
- ⑤【ネットワーク層(第3層)】 ネットワーク内で稼働している端末を識別します。
適切な端末間でのデータの受け渡しができるよう制御します。
- ⑥【データリンク層(第2層)】 伝送路上で信号を送受信するための方式を決定します。
物理的に隣り合うコンピュータ間のデータ送受信に関する方式を決定します。
- ⑦【物理層(第1層)】 データを信号に変換して伝送します。
物理的に他の端末までデータを届けます。

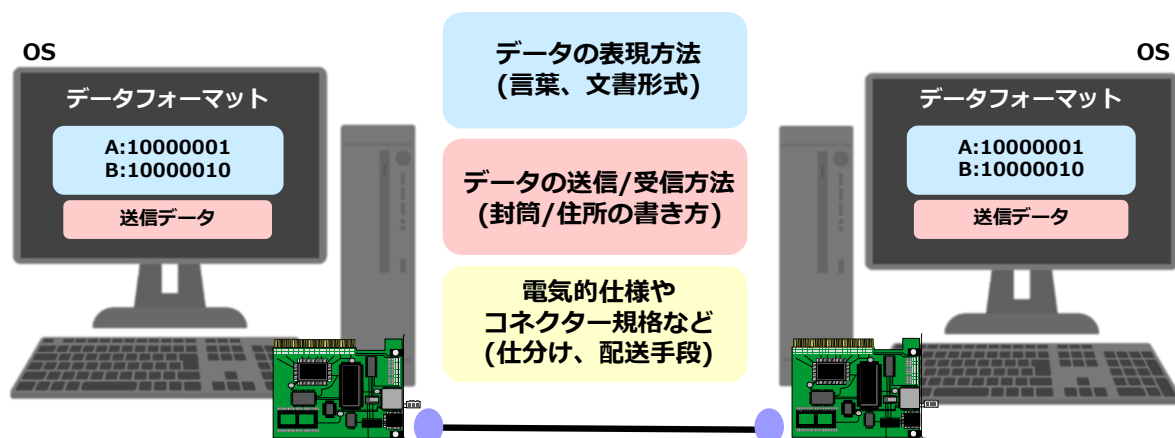
上記のように送信元端末における通信の流れは、上位層から下位層へと処理が行われます。一方、宛て先端末では、下位層から上位層へ処理が行われます。

次は、ネットワークアーキテクチャを解説します。

2.3 ネットワークアーキテクチャ

2.3.1 ネットワークアーキテクチャとは

ネットワーク技術(プロトコル)の組み合わせ



ネットワークアーキテクチャとは、ネットワーク技術の組み合わせパターンのことです。代表的なネットワーク技術とその周辺技術を組み合わせ、パターン化しています。

基本的に、通信を実現するためには通信をする機器間でネットワークアーキテクチャを同一とする必要があります。どのネットワークアーキテクチャを採用するかを通信相手とそろえる必要があります。

ネットワークアーキテクチャには、各メーカーが開発した「**メーカー独自規格**」とメーカー以外の組織・団体が開発した「**国際標準規格**」、「**業界標準規格**」があります。

●メーカー独自規格

ネットワークアーキテクチャ内の技術は、メーカーごとに開発が行われていますが、すべての製品が個々にまったく異なる仕様を持っていると統一性が取れません。メーカー内で各仕様を規格として制定し、その規格に準拠するように製品を開発しています。

●国際標準規格

異なるメーカー間で通信ができるように統一規格として発表された規格です。

●業界標準規格

多くのメーカーで採用され、異なるメーカーであっても通信ができるようになった規格です。

ネットワークアーキテクチャ内の技術規格をプロトコルと表現します。

通信を行う上での約束事や決まり事とも言われます。

データの表現方法やデータの送信/受信方法、電氣的仕様やコネクターの形状などに対する約束事、決まり事が組み合わさってネットワークアーキテクチャができています。

次は、ネットワークアーキテクチャの種類を解説します。

2.3.2 ネットワークアーキテクチャの種類

ネットワークアーキテクチャの種類 代表的なネットワークアーキテクチャ

メーカー独自規格	FNA (富士通)
	SNA (IBM)
業界標準規格	TCP/IP (IETF)
国際標準規格	OSI (ISO)

【参考】標準化組織

ISO	国際標準化機構
ISOC (IETF)	インターネット(TCP/IP)技術の規格

※他にもLANやWANの通信規格を定める組織があります。
(LANの通信規格は「IEEE802」、WANの通信規格は「ITU-T/R」)

基本的には、異なるアーキテクチャ(規格)同士は互換性が保証されません。そのため、ネットワークを構築する場合は、どのアーキテクチャ(規格)を採用するかを検討し、その規格に合った製品を選択することが必要です。

メーカー間の互換性を維持するため多くの標準化規格が存在します。

- FNA (Fujitsu Network Architecture) :
富士通が開発したネットワークシステム用の規格名称です。
- SNA (System Network Architecture) :
IBM社が開発したネットワークシステム用の規格名称です。
- TCP/IP (Transmission Control Protocol / Internet Protocol) :
IETFで開発・草案・規格化されているネットワークプロトコルです。多くの通信は、このプロトコルを採用しています。
- OSI (Open Systems Interconnection) :
ISO (国際標準化機構) で制定したプロトコルです。通信機能を7階層に分類したOSI参照モデルが有名です。

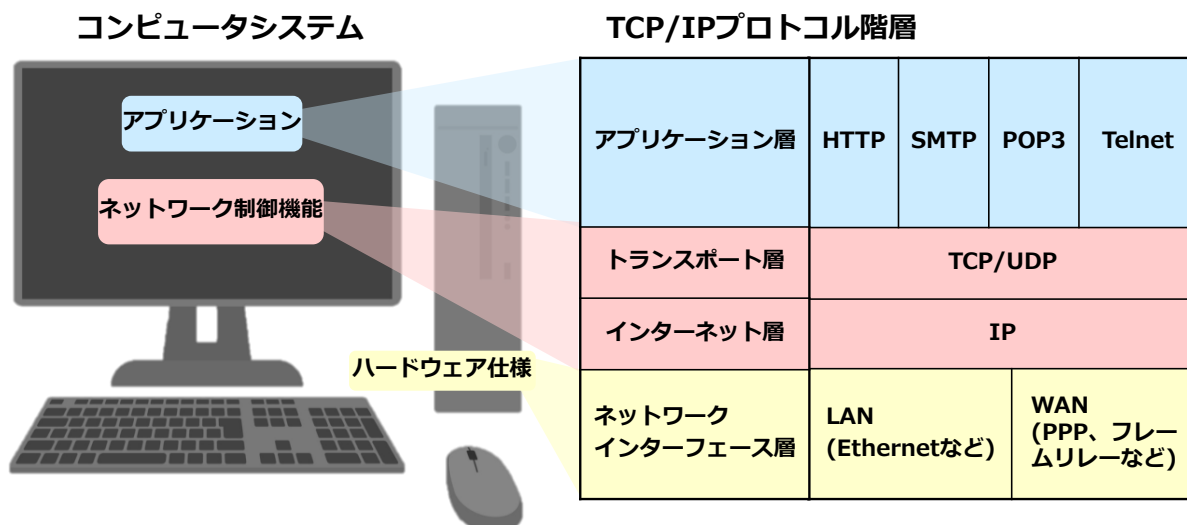
【参考】

以下は代表的な標準化規格を検討する組織です。

- ISO (International Organization for Standardization) :
国際標準化機構と呼ばれる組織です。世界的な標準仕様を策定する目的で設立されている団体です。
- ISOC (Internet SOCIety) :
インターネットにかかわるさまざまな研究グループや委員会を統括しています。
- IETF (Internet Engineering Task Force) :
ISOC配下に位置する技術研究活動グループの名称です。インターネットに関係するすべての技術仕様、規格の制定を行っており、その結果をRFCドキュメントとして発行しています。

2.4 TCP/IP

インターネットで利用されているネットワーク技術



ここでは、TCP/IPを確認します。

TCP/IPは、インターネットや多くのイントラネットで利用されているネットワーク技術です。IETF (Internet Engineering Task Force)で技術の標準化が行われており、ほとんどのコンピュータやネットワーク装置において、TCP/IPが実装されています。

TCP/IPでは、4つの階層に技術を分類しています。

- アプリケーション層**：HTTP、SMTP、POP3、Telnetなど
通信アプリケーションごとのデータの取り扱い方法や通信の流れを定義します。
アプリケーション層プロトコルには、数多くの種類が存在しています。
- トランスポート層**：TCP、UDP
コンピュータ内のアプリケーション間通信を識別したり、データの送信チェックや再送を行います。
- インターネット層**：IP
ネットワーク内のコンピュータを識別し、データを配送します。
- ネットワークインターフェース層**：Ethernetなど
通信用ハードウェア間でデータを受け渡します。なお、TCP/IPでは、製品の制限はありません。

【用語解説】

HTTP (Hypertext Transfer Protocol)：WWW (World Wide Web) を実現するプロトコル。

SMTP (Simple Mail Transfer Protocol)：電子メールサービスを実現するためのメール配送プロトコル。

Telnet：コンピュータや装置を遠隔操作するプロトコル。

TCP (Transmission Control Protocol)：コンピュータ間で信頼性の高い通信を実現するため、データの送信順序やデータ到達確認などを行うプロトコル。

IP (Internet Protocol)：相手を識別するためのアドレス情報(IP アドレス)や経路制御などを行うプロトコル。

Ethernet：主にLAN内で利用されている通信ハードウェアの規格。

次は、本章のまとめです。

2.5 章のまとめ

- ネットワークアーキテクチャとはネットワーク技術の組み合わせパターンのことです。以下の3つの種類に分類できます。
 - ✓ メーカー独自規格 : 各メーカーが開発した独自規格 (FNAなど)
 - ✓ OSI : 異なるメーカー間で通信ができるように統一規格として発表された国際標準規格
 - ✓ TCP/I IP : 多くのメーカーで採用され、異なるメーカーであっても通信ができるようになった業界標準規格
- アーキテクチャ内の技術規格をプロトコルと表現します。コンピュータが通信するのに使う手順をプロトコルが定めています。さまざまなプロトコルがあり、ネットワークアーキテクチャによって整理されています。
- TCP/IPはインターネットや多くのイントラネットで利用されているネットワーク技術です。TCPやIPというプロトコルを中心として、さまざまなプロトコルが規定されています。

第2章のまとめです。

- ネットワークアーキテクチャとはネットワーク技術の組み合わせパターンのことです。以下の3つの種類に分類できます。
 - ✓ メーカー独自規格 :
各メーカーが開発した独自規格 (FNAなど)
 - ✓ OSI :
異なるメーカー間で通信ができるように統一規格として発表された国際標準規格
 - ✓ TCP/IP :
多くのメーカーで採用され、異なるメーカーであっても通信ができるようになった業界標準規格
- アーキテクチャ内の技術規格をプロトコルと表現します。コンピュータが通信するのに使う手順をプロトコルが定めています。さまざまなプロトコルがあり、ネットワークアーキテクチャによって整理されています。
- TCP/IPはインターネットや多くのイントラネットで利用されているネットワーク技術です。TCPやIPというプロトコルを中心として、さまざまなプロトコルが規定されています。

第3章

ネットワークを利用したサービス (アプリケーション層)

学習目標

この章では、TCP/IPのアプリケーション層について学習します。

- FQDN、ドメインなどの用語を理解する。
- WWWやメールなどの代表的なアプリケーションサービスについて理解する。

3.1 アプリケーション層

通信アプリケーションごとのデータの取り扱い方法や通信の流れを定義する

コンピュータシステム



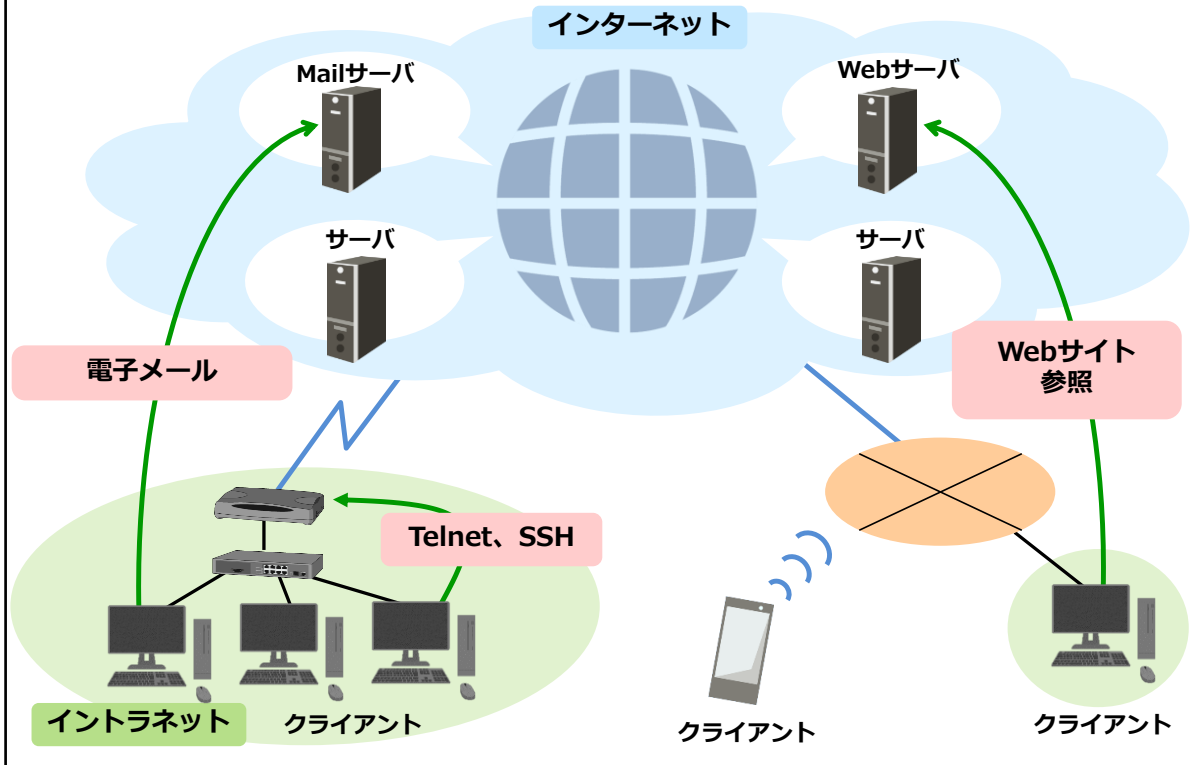
TCP/IPプロトコル階層

アプリケーション層	HTTP	SMTP	POP3	Telnet
トランスポート層	TCP/UDP			
インターネット層	IP			
ネットワーク インターフェース層	LAN (Ethernetなど)		WAN (PPP、フ レームリレーなど)	

TCP/IPの**アプリケーション層**では、HTTP、SMTP、POP3、Telnetなど、さまざまなプロトコルが存在しています。各プロトコルは、通信の目的に対応したデータの取り扱い方法や通信の流れを定義しています。

3.2 インターネットの通信サービス

3.2.1 代表的な通信サービス



インターネット上にはさまざまな通信サービスが存在しています。情報発信や交換のための各種サーバが世界各地に存在しており、クライアントとサーバ間で情報伝達を行います。通信の目的にあわせてサービスを選択し利用します。

• Webサイト参照

WWW (World Wide Web)を利用します。ユーザーはブラウザからインターネットにアクセスし、情報を入手できます。また、情報はリンク(関連付け)されており、クリックするだけで、文字・画像・動画・音声といった多様な形態で情報を入手できます。

• 電子メール

インターネットを利用しているユーザー間で情報のやり取りが行えます。ユーザーはメーラーを利用します。手紙と異なり電子的に配送するため、瞬時に情報交換ができます。

なお、インターネットの通信サービスは、利用者を限定してイントラネット(企業ネットワーク)においても活用されています。

【用語解説】

ブラウザ: Webページを閲覧するためのアプリケーション。HTMLを解析し表示する。代表的な製品として、Microsoft社の「Internet Explorer」、Mozilla社「Firefox」、Google社「Chrome」などがある。

メーラー: 電子メールの情報を閲覧するためのソフトウェア(Outlook、Thunderbirdなど)

【参考】

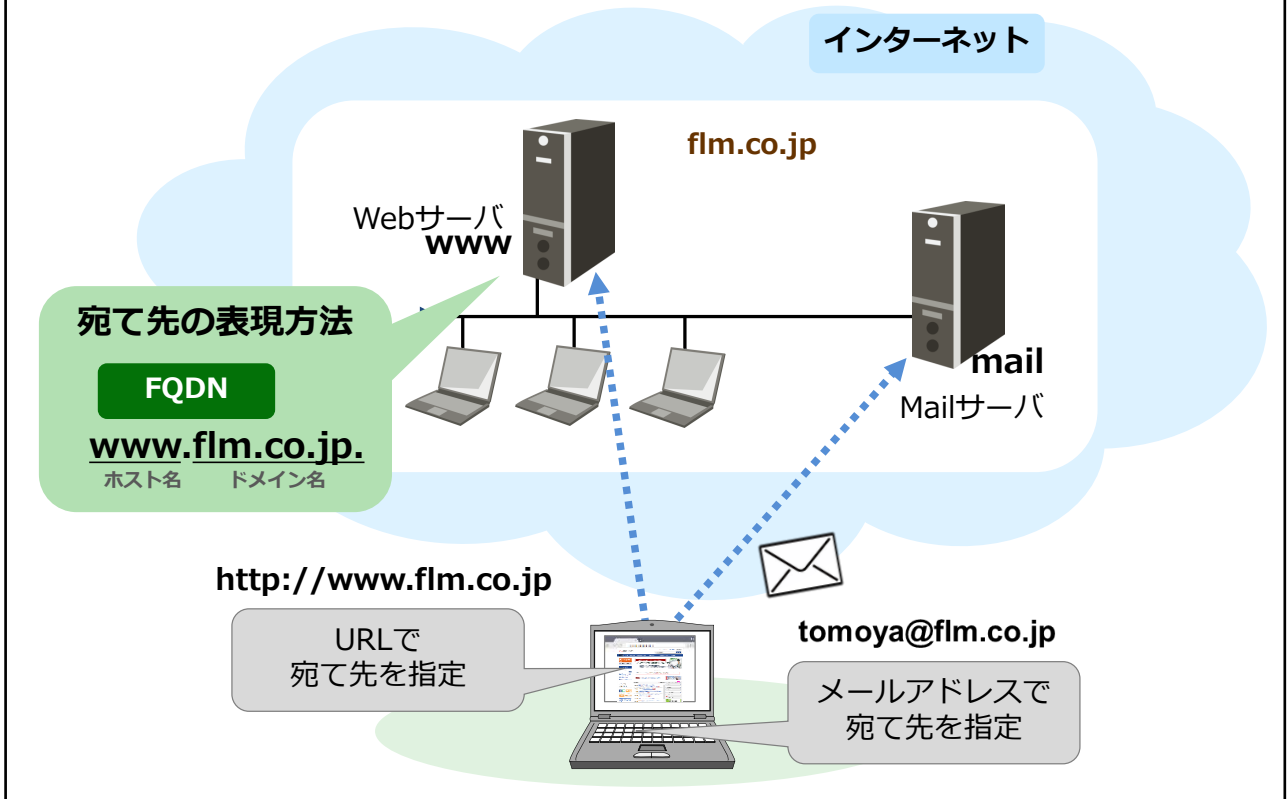
ファイル転送:

インターネット上のコンピュータ間でデータやプログラムのダウンロードとアップロードができます。インターネット上には、一般公開されているデータやプログラムが複数あります。

(有償のものや無償のものがあります。)

次は、通信サービスの宛て先の表現方法について解説します。

3.2.2 通信サービスの宛て先



通信サービスを利用するとき、通信相手(ユーザーやコンピュータ)を指定するには、アドレス(識別子)を指定します。インターネット上のユーザーやコンピュータは、**FQDN (Fully Qualified Domain Name)**と呼ばれる文字列形式で識別できます。

利用者にとっては、数値よりも文字列で表現できた方が意味付けが行え、覚えやすい・管理しやすいといったメリットがあります。たとえば、ネットワーク「flm.co.jp.」内のコンピュータ「www」は、FQDN形式で「www.flm.co.jp.」と表現されます。

各通信サービスでは、FQDNを活用し、宛て先を指定します。

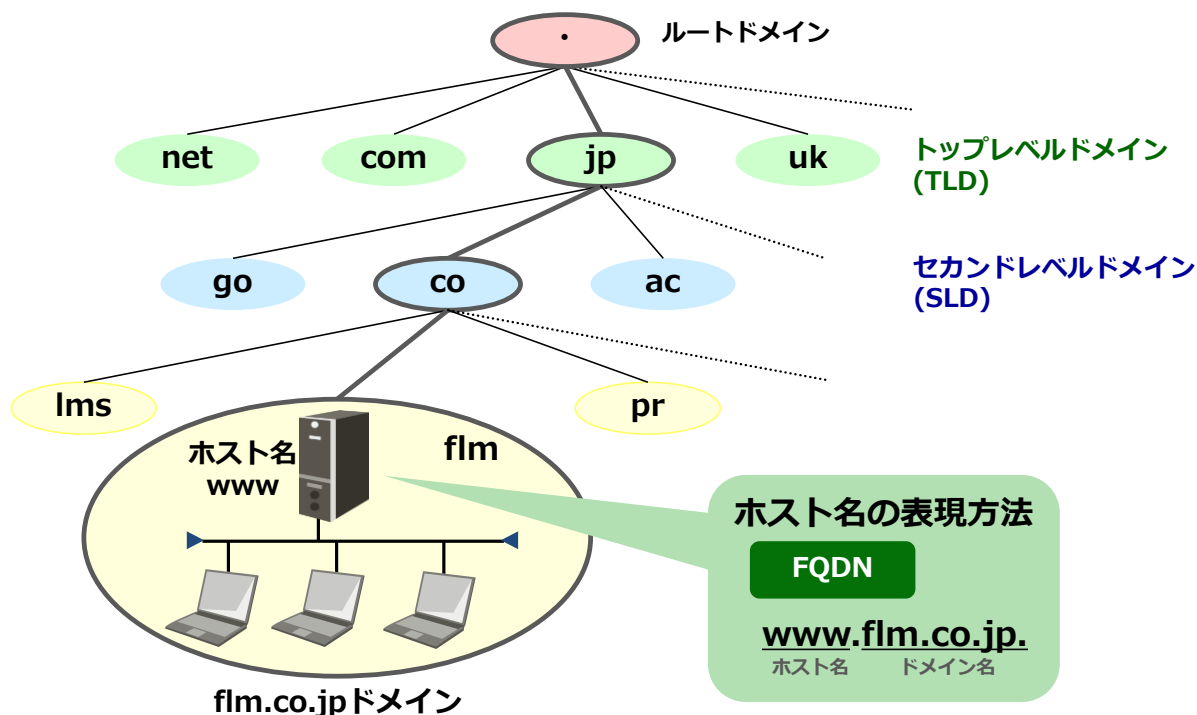
例)

- WWWで使用するアドレス : http://www.flm.co.jp/
- Mailで使用するアドレス : tomoya@flm.co.jp

FQDNで表現された文字列にはネットワークを示す「ドメイン名」とコンピュータを示す「ホスト名」があります。

次は、FQDNに含まれている「ドメイン名」について解説します。

3.2.3 ドメインとFQDN



インターネットでは、ネットワークを国別、組織別（企業、ネットワーク団体、教育機関など）、さらに会社別などの階層構造に分割して管理しています。この管理単位をドメインと呼びます。各ドメインには、文字列で名前（ドメイン名）が付与されます。ドメイン名は、インターネット上に公開するため、重複は許されません。ドメイン名の管理は、国際組織である ICANN（日本のドメインはJPRS）が行っており、新規にドメイン名を取得する場合は申請が必要です。

インターネット上のドメインは、ツリー構造で管理されており、頂点をルートドメインといいます。配下に、トップレベルドメイン(TLD)、セカンドレベルドメイン(SLD)と続き、個別のドメインが配置されます。

ドメイン内の各コンピュータを表現する場合には、自ドメインから最上位のルートドメインまでをピリオドで区切って表現します。最上位のルートドメインを表す末尾のピリオドは通常省略されます。

【用語解説】

ICANN (The Internet Corporation for Assigned Names and Numbers):

ドメイン登録業務やIPアドレス割り当て業務を行っている非営利団体です。

【参考】

- トップレベルドメイン(TLD)の例
 - netドメイン：network(ネットワーク事業者)のドメインであることを示す。
 - comドメイン：commercial(商業・商用)のドメインであることを示す。
 - jpドメイン：日本国で利用するドメインであることを示す。
 - ukドメイン：United Kingdom(イギリス)で利用するドメインであることを示す。
- セカンドレベルドメイン(SLD)の例
 - goドメイン：政府機関のドメインであることを示す。
 - coドメイン：company(企業)のドメインであることを示す。
 - acドメイン：academy(大学・教育機関)のドメインであることを示す。

3.3 WWW

3.3.1 URL

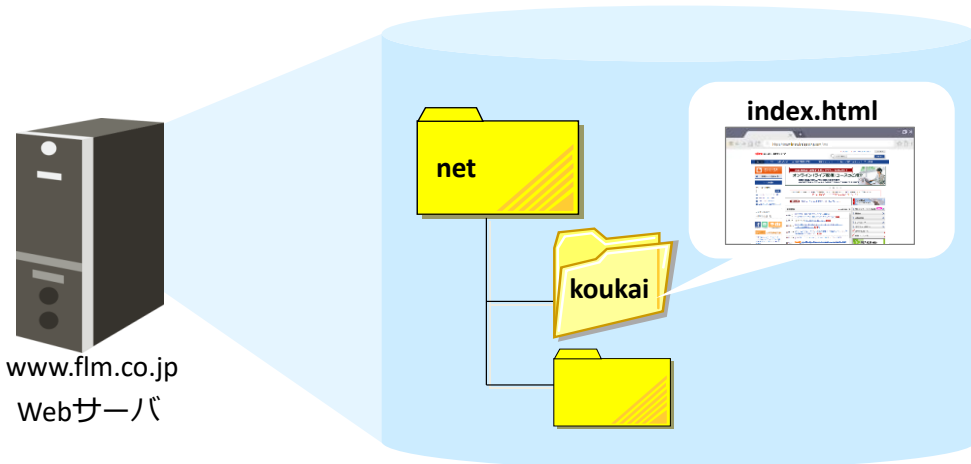
URL (Uniform Resource Locator)

`http://www.flm.co.jp/net/koukai/index.html`

プロトコル名

ホスト名・ドメイン名

ディレクトリ・ファイル名



以降では代表的な通信サービス（Webサイト参照、電子メール、Telnet）について解説します。まずはWebサイト参照にて使用するURL(Uniform Resource Locator)について解説します。URL (Uniform Resource Locator) は、WWW内の情報の所在場所を指定する仕組みです。利用者は、ブラウザでURLを入力することで、どのコンピュータのどの情報を取得したいのかを明示的に指定しています。Webサーバのデータであれば、URLに「`http://FQDN名/`」形式で指定します。

< URLのフォーマット >

- プロトコル名 : 使用するアプリケーションプロトコルを指定します。「http」は、Webサーバへアクセスするためのプロトコルです。
- ホスト名・ドメイン名 : サーバのアドレス(ホスト名・ドメイン名またはIPアドレス)を指定します。
- ディレクトリ・ファイル名 : 情報のパスを指定します。情報が保存されているディレクトリ(フォルダ)をツリー構造で指定します。

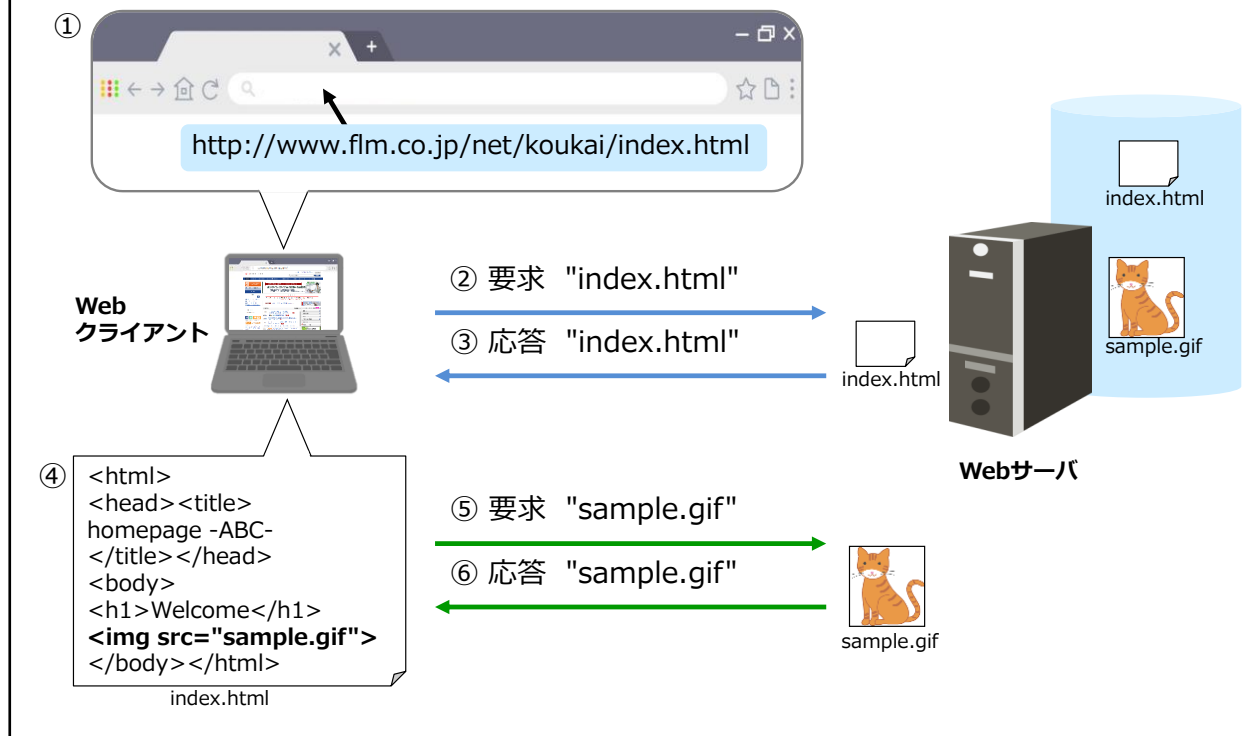
※URLのホスト名・ドメイン名の後ろに「: 8080」などの数値（ポート番号）を入力して、任意のアプリケーション（ポート番号）を、宛て先に指定することが可能です。たとえば、上図のURLを「`http://www.flm.co.jp : 8080/net/koukai/index.html`」に変更した場合は、Webサーバの通常の実行アプリケーション（ポート番号: 80）とは、異なるアプリケーション（ポート番号: 8080）に対してWWWの情報を取得しようと試みます。（「: 80」を入力した場合は、標準と同じ指定のため、「: 80」の表記は省略されます。）

※上記の「ポート番号」は第4章、「IPアドレス」は第5章にて詳しく説明します。

【参考】

ファイル転送を行うプロトコルには、http以外に、FTP(File Transfer Protocol)やCIFS(Common Internet File System)など多くのプロトコルがあります。

3.3.2 WWW の仕組み



WWW (World Wide Web) を閲覧するときに使用するプロトコルが**HTTP (Hypertext Transfer Protocol)**です。

WWWの情報は、**HTML (Hypertext Markup Language)**で構成されています。HTMLでは、情報の表示レイアウトを指定でき、画像や映像などを埋め込んだ効果的な情報表示を工夫することができます。

■ HTTP通信の流れ

- ① 利用者が、ブラウザにURLを入力します。
- ② クライアントは、URLに記載されているサーバに情報を要求します。
(まず、情報の全体像を示しているHTMLファイルを要求します。)
- ③ サーバは、要求された情報を送信します。
- ④ クライアントはHTMLファイルを解析し、HTML内に埋め込まれている画像データなどの有無を確認します。
- ⑤ 埋め込まれているデータ(画像データなど)が存在する場合、あらためてサーバに情報を要求します。
- ⑥ サーバは、要求された情報を送信します。

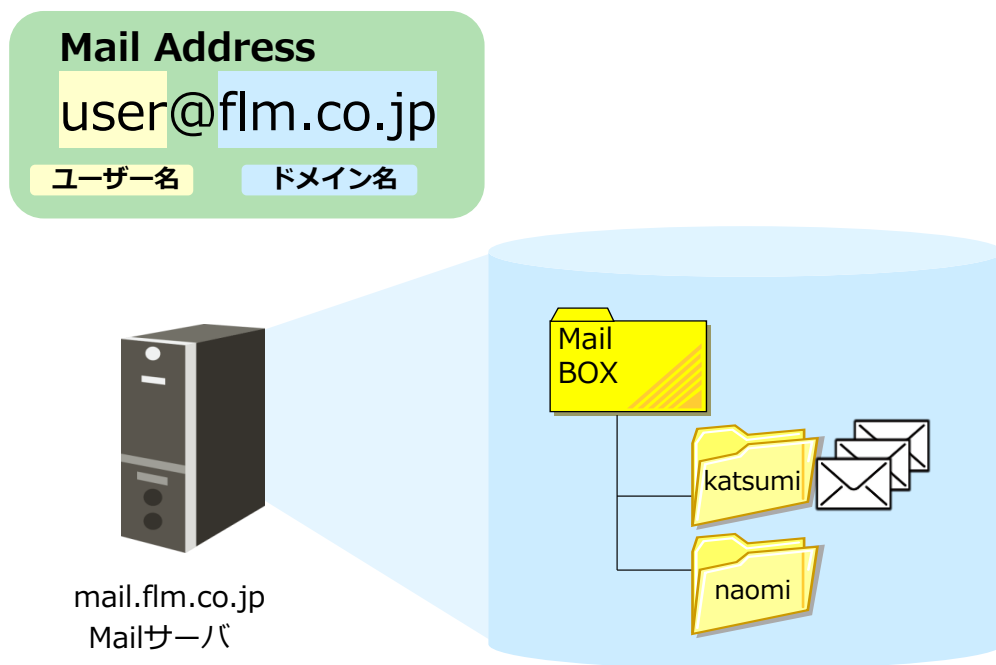
【参考】

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer):

SSL (Secure Sockets Layer) / TLS (Transport Layer Security) を用いて、データの暗号化、セッション管理を行い、セキュリティの脅威から通信内容を保護します。WWW上で個人情報を取り扱う場合など、広く利用されています。

3.4 電子メール

3.4.1 電子メールアドレス



ここでは、電子メールで使用する電子メールアドレスについて解説します。

電子メールアドレス は、電子メールの送信元/宛て先ユーザーを指定する仕組みです。利用者は、作成した電子メールに宛て先のメールアドレスを付与し、どのユーザーへ届けたいのかを明示的に指定します。

<メールアドレスのフォーマット>

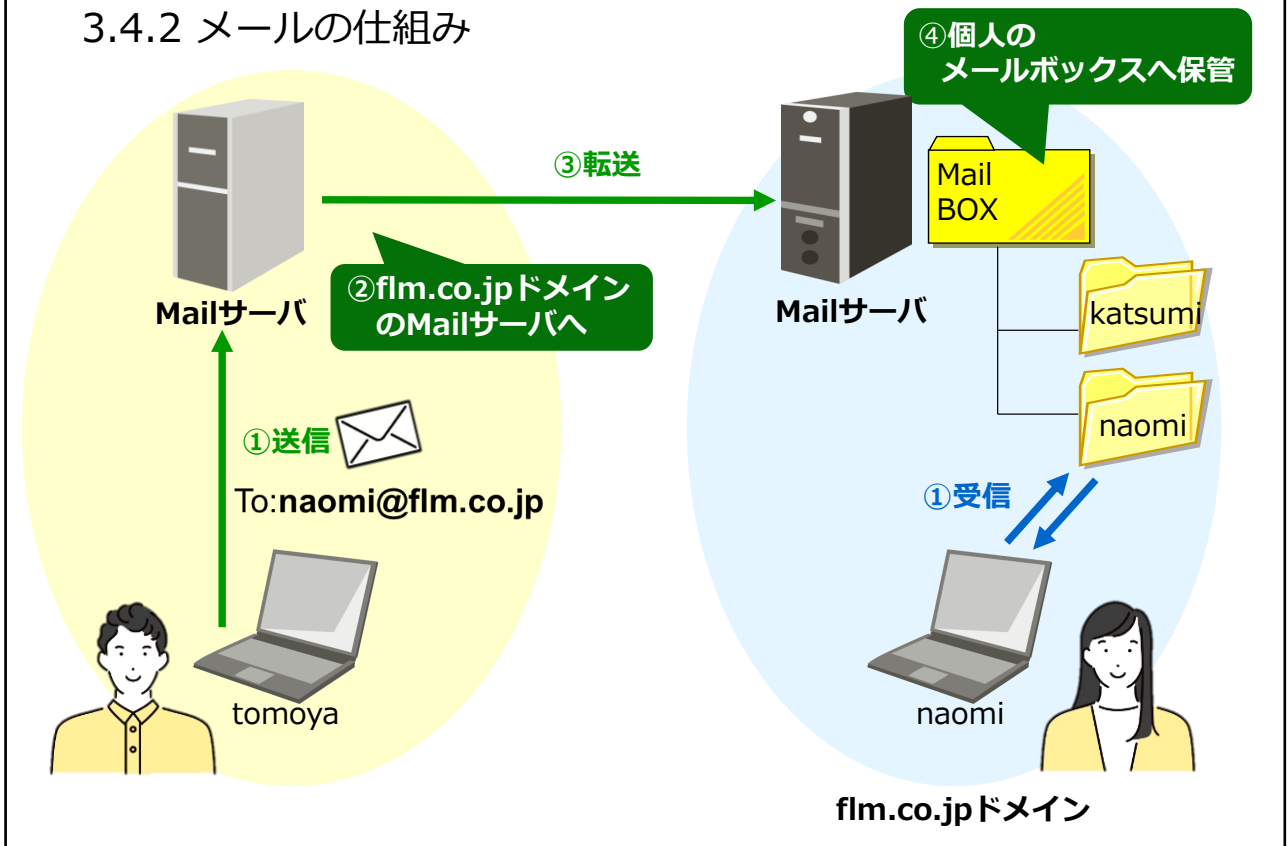
ユーザー名 : コンピュータ名ではなく、宛て先のユーザー名を指定します。

ドメイン名 : 宛て先ユーザーが登録されているMailサーバの所属ドメインを指定します。

【参考】

メーリングリスト: 複数のユーザーをグループ化し、そのグループに対してメールを一斉送信することができます。このようにユーザーを束ねたアドレスをメーリングリストといいます。

3.4.2 メールの仕組み



電子メールは、インターネットで利用できるサービスの中で最も基本的なサービスの1つです。一般的に、メールの送受信を行うには**SMTP (Simple Mail Transfer Protocol)**と**POP3 (Post Office Protocol version3)**、または**IMAP4**を使用します。メールを送信時にはSMTP、受信時にはPOP3、またはIMAP4を使用します。

■ 電子メールの通信の流れ(送信時：SMTP)

- ① メールの送信
相手先の電子メールアドレスを指定してメールを送信します。この際、メールは自ドメインのMailサーバに一度格納されます。
- ② メールの宛て先解析
自ドメイン内のMailサーバは、宛て先ドメインのMailサーバを調べます。
- ③ Mailサーバによる宛て先ドメインへの配送
自ドメイン内のMailサーバは、宛て先ドメインのMailサーバへメールを送信します。(宛て先が自ドメイン内であれば、Mailサーバ内の宛て先ユーザーのメールボックスに保管します。)
- ④ メールの受け取り・保管
メールを受信したMailサーバは、該当のユーザーのメールボックスにメールを保管します。

■ 電子メールの通信の流れ(受信時：POP3、IMAP4)

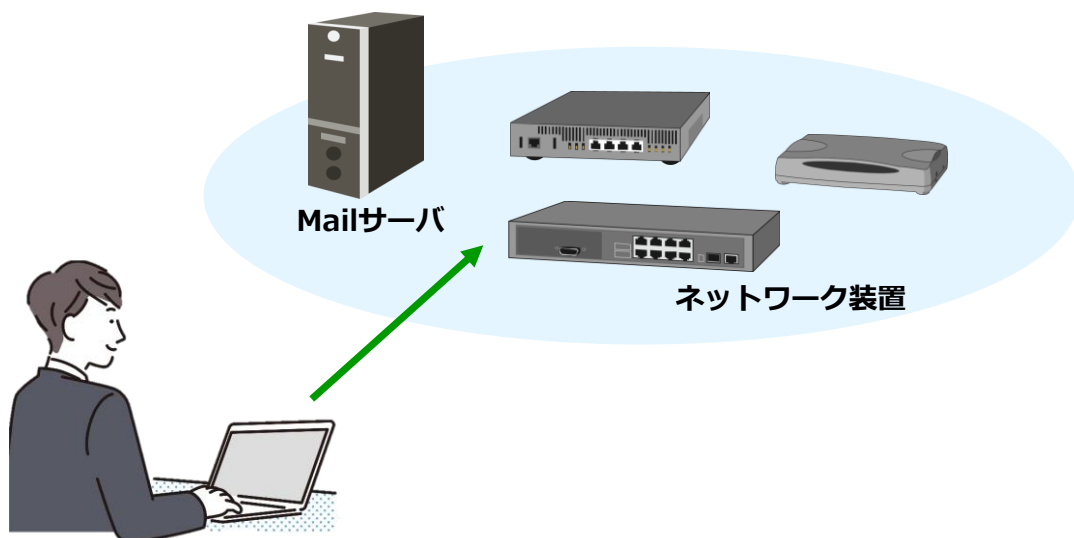
- ① メールの取り出し
ユーザーは、Mailサーバ内のメールボックスにメールが届いているかを確認します。メールが届いている場合には、自身のコンピュータに転送し、受信します。

【用語解説】

IMAP4(Internet Message Access Protocol 4):

POP3では、メールを受信するとサーバからデータが削除されます。その後はユーザーのコンピュータで情報を管理します。一方IMAP4では、受信してもサーバから削除はされません。Mailサーバ上で情報を管理します。この特長を利用し、メールのヘッダー情報のみをダウンロードして、必要なメールを選択するなど細かい操作が可能です。

3.5 管理系プロトコル (Telnet、SSH)



ここでは、TelnetやSSHについて確認します。

Telnetや**SSH**は、ネットワーク装置やサーバにネットワーク経由で接続し、状態確認や設定などの管理作業を行うためのプロトコルです。

利用者は、ターミナルソフトを用いて操作を行います。ターミナルソフトにより、目の前の端末のキーボードとディスプレイで、仮想的にネットワーク装置やサーバを遠隔操作することができます。

ネットワークを介して管理を行うため、管理者は装置やサーバが設置されている場所に赴かず、自席から作業ができ便利です。

Telnetの標準仕様はRFC854で規定されており、特徴としてすべての通信が平文（暗号化されない）であることが挙げられます。一方、SSH（Secure Shell）は、すべての通信が暗号化され、セキュアな通信を実現しています。SSHの仕様はRFC4253で規定されています。

【参考】

ターミナルソフト：

代表的なターミナルソフトにはフリーのソフトウェアである「Tera Term」があります。コンピュータに標準搭載されていない場合は、別途インストールが必要です。

<演習問題1> URLから読み取れる情報を確認してみよう

■ 演習問題1 ■

URL「<http://www.knowledgewing.com/kw/index.html>」の文字列を確認して、以下の設問に答えてください。

■ 設問1 ■ 上記URLの文字列から読み取ってみましょう。
「Webサイト閲覧のために使用したTCP/IPのアプリケーション層のプロトコルは？」

■ 設問2 ■ 上記URLの文字列から読み取ってみましょう。
「通信相手のWebサーバのホスト名・ドメイン名は？」

【解答例】 (※URLが以下の場合)

<http://www.knowledgewing.com/kw/index.html>

プロトコル名 ホスト名 ドメイン名 ディレクトリ・ファイル名

FQDN



上記URLの場合は以下が確認できます。

- TCP/IPのアプリケーション層のHTTPを使用
- 通信相手のホスト名・ドメイン名は「www.knowledgewing.com」

■ 演習問題1 ■

URL「<http://www.knowledgewing.com/kw/index.html>」の文字列を確認して、以下の設問に答えてください。

■ 設問1 ■

上記URLの文字列から読み取ってみよう。

「Webサイト閲覧のために使用したTCP/IPのアプリケーション層のプロトコルは？」

■ 設問2 ■

上記URLの文字列から読み取ってみよう。

「通信相手のWebサーバのホスト名・ドメイン名は？」

【解答例】

URL「<http://www.knowledgewing.com/kw/index.html>」の文字列から読み取った結果は、以下のとおりです。

- URLの先頭の「http」の文字列から、プロトコル名はHTTPと判断できる。
- URLの「http://」の後ろに続くFQDNの文字列から、ホスト名は「www」、ドメイン名は「[knowledgewing.com](http://www.knowledgewing.com)」と判断できる。

次は、本章のまとめです。

3.6 章のまとめ

- ネットワークを利用するアプリケーションは、FQDNの表現方法を利用し宛て先を示します。
- FQDNは、「ホスト名」、「ドメイン名」と表現し、所属するドメイン名が含まれます。FQDNに使われるドメイン名はツリー構造で管理されています。
- URLは、WWW内の情報の所在場所を指定する仕組みです。フォーマットにプロトコル名、ホスト名、ドメイン名、ディレクトリ、ファイル名が含まれます。
- 電子メールアドレスは、電子メールの送信元/宛て先ユーザーを指定する仕組みです。フォーマットにユーザー名、ドメイン名が含まれます。
- WWW（Webと省略可）の主な通信プロトコルはHTTPを使用し、Webサーバから提供されているWebページ情報を表示する仕組みです。
- メールの通信プロトコルは、送信用としてSMTPを利用し、受信用としてPOP3またはIMAP4を利用します。

第3章のまとめです。

- ネットワークを利用するアプリケーションは、FQDNの表現方法を利用し宛て先を示します。
- FQDNは、「ホスト名」、「ドメイン名」と表現し、所属するドメイン名が含まれます。FQDNに使われるドメイン名はツリー構造で管理されています。
- URLは、WWW内の情報の所在場所を指定する仕組みです。フォーマットにプロトコル名、ホスト名、ドメイン名、ディレクトリ、ファイル名が含まれます。
- 電子メールアドレスは、電子メールの送信元/宛て先ユーザーを指定する仕組みです。フォーマットにユーザー名、ドメイン名が含まれます。
- WWW（Webと省略可）の主な通信プロトコルはHTTPを使用し、Webサーバから提供されているWebページ情報を表示する仕組みです。
- メールの通信プロトコルは、送信用としてSMTPを利用し、受信用としてPOP3またはIMAP4を利用します。

第4章

通信を多重化する仕組み (トランスポート層)

学習目標

この章では、TCP/IPのトランスポート層について学習します。

- TCP、UDP、ポート番号などの用語について理解する。
- 通信を多重化する仕組みについて理解する。

4.1 トランスポート層

コンピュータ内のアプリケーション通信を識別する

コンピュータシステム

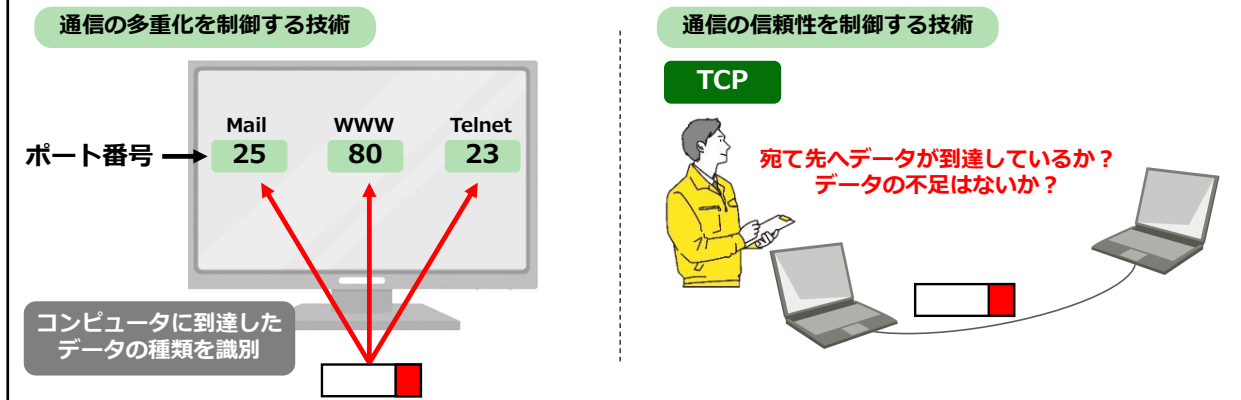
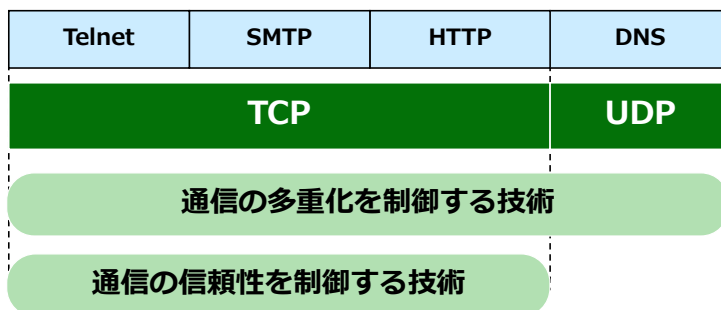


TCP/IPプロトコル階層

アプリケーション層	HTTP	SMTP	POP3	Telnet
トランスポート層	TCP/UDP			
インターネット層	IP			
ネットワーク インターフェース層	LAN (Ethernetなど)		WAN (PPP、フレームリレーなど)	

TCP/IPのトランスポート層では、TCPとUDPの2つのプロトコルが存在しています。この層では、コンピュータ内のアプリケーション通信を識別したり、データの送信チェックや再送を行います。

4.2 TCPとUDP



アプリケーションにより送受信されるデータを制御するプロトコルに、**TCP (Transmission Control Protocol)**と**UDP (User Datagram Protocol)**があります。

どちらのプロトコルにも、1台のコンピュータで複数の通信サービスを同時に稼働させるために、稼働している通信サービスを識別する仕組みがあります。通信サービスの識別は、**ポート番号**と呼ばれる識別子を利用します。

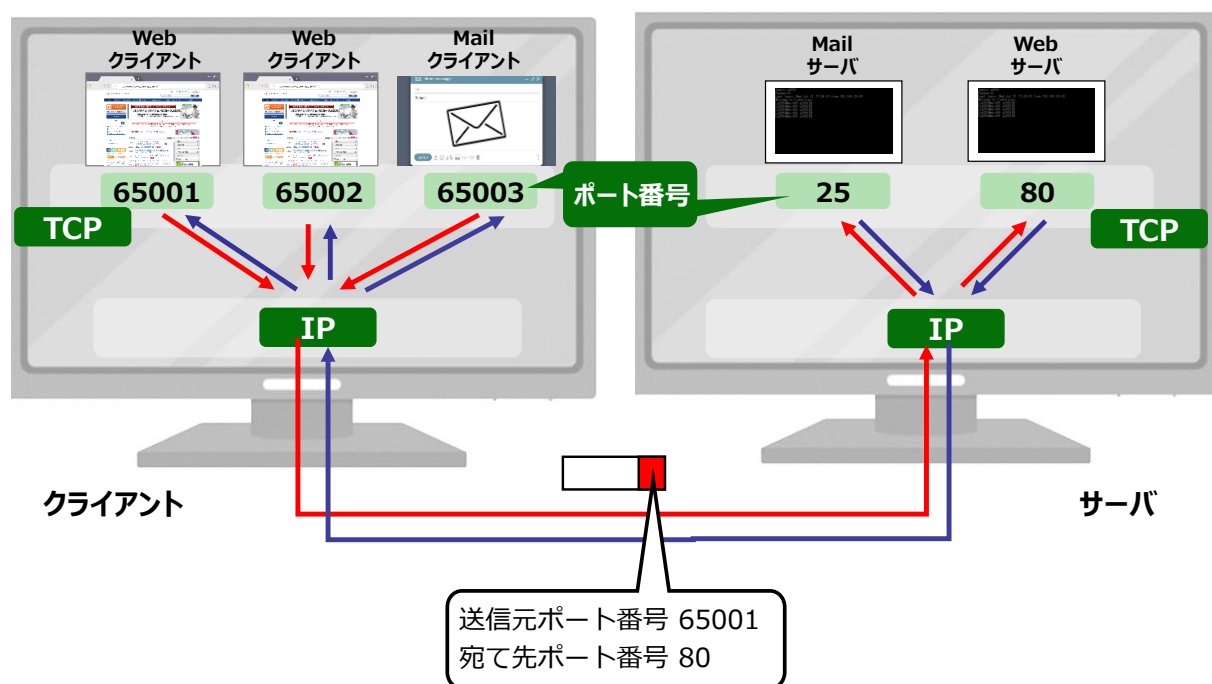
TCPには、データを確実に宛て先のコンピュータへ配送するために、通信の状態をチェックする機能があります。この機能はUDPにはありません。

このように、TCPとUDPでは制御の特徴が異なるため、アプリケーションサービスの特性に応じて、どちらか片方のプロトコルが利用されます。たとえば、WWW(HTTP)やMail(SMTP, POP3)は、TCPが活用されており、DNS(名前解決)では、UDPが活用されています。

次に、ポート番号について解説します。

4.3 ポート番号

4.3.1 ポート番号



※次のページにて通信の流れを解説します。

1台の端末上には複数のアプリケーションが存在し、同時に通信が可能です。これらの通信が混在しないように、アプリケーションを識別する識別子が必要です。これを**ポート番号**といいます。ポート番号は、0～65535 の数値で示されます。

サーバで用いられるポート番号とクライアントで用いられるポート番号の大きく2つの種類に分類できます。

- ・**サーバ用ポート番号 (ウェルknownポート) 範囲：0～1023**

サーバで稼働しているアプリケーションプロトコルを静的に識別します。代表的なプロトコルに対するポート番号は、国際的に取り決められています。(例：HTTP：80番、SMTP：25番、HTTPS：443番)

クライアントから、サーバ上のどのアプリケーションへ通信を行いたいかを指定できます。

- ・**クライアント用ポート番号 範囲：1024～65535**

クライアントで稼働しているアプリケーションプロトコルを識別します。プロトコルが起動したタイミングで重複しない値がランダム(動的)に割り当てられます。

クライアントのコンピュータで稼働しているアプリケーションの個別識別を行い、サーバからの返信データを発信アプリケーションへ間違いなく戻します。

【参考】

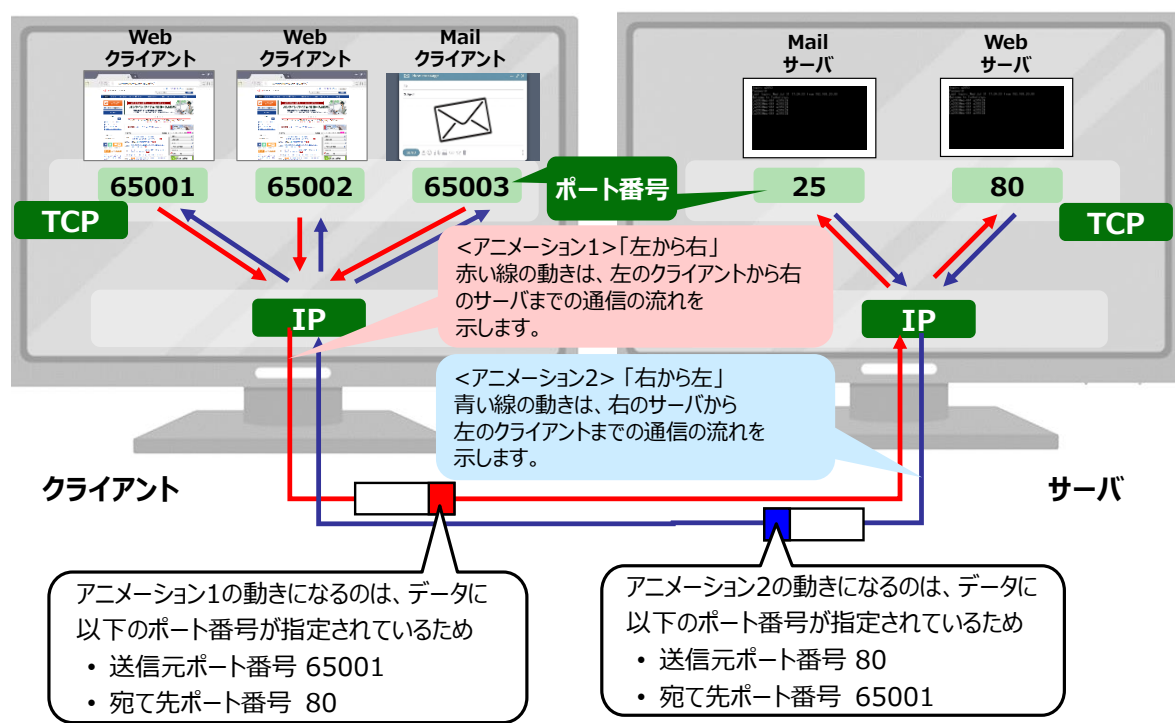
端末が使用するクライアント用ポート番号はOSによって異なります。たとえば、Windowsの初期値では「49152～65535」を使用します。

次は、ポート番号を用いた通信の流れをアニメーションを用いて解説します。

4.3.2 ポート番号（続き）



画面左下の▶にて、ポート番号を用いた通信の流れを確認しましょう。



<ポート番号を用いた通信の流れ>

- ① クライアントでブラウザを起動し、URLを入力してEnterキーを押すと、クライアント用ポート番号が動的に割り当たる。
- ② クライアントからサーバへの通信では、以下のポート番号が指定される。
送信元ポート番号：クライアント用ポート番号
宛て先ポート番号：アプリケーションプロトコルのポート番号
- ③ サーバからのクライアントへの返信の通信では、以下のポート番号が指定される。
送信元ポート番号：アプリケーションプロトコルのポート番号
宛て先ポート番号：クライアント用ポート番号
- ④ クライアント側の通信を発信したアプリケーションへサーバの返信データが到達する。

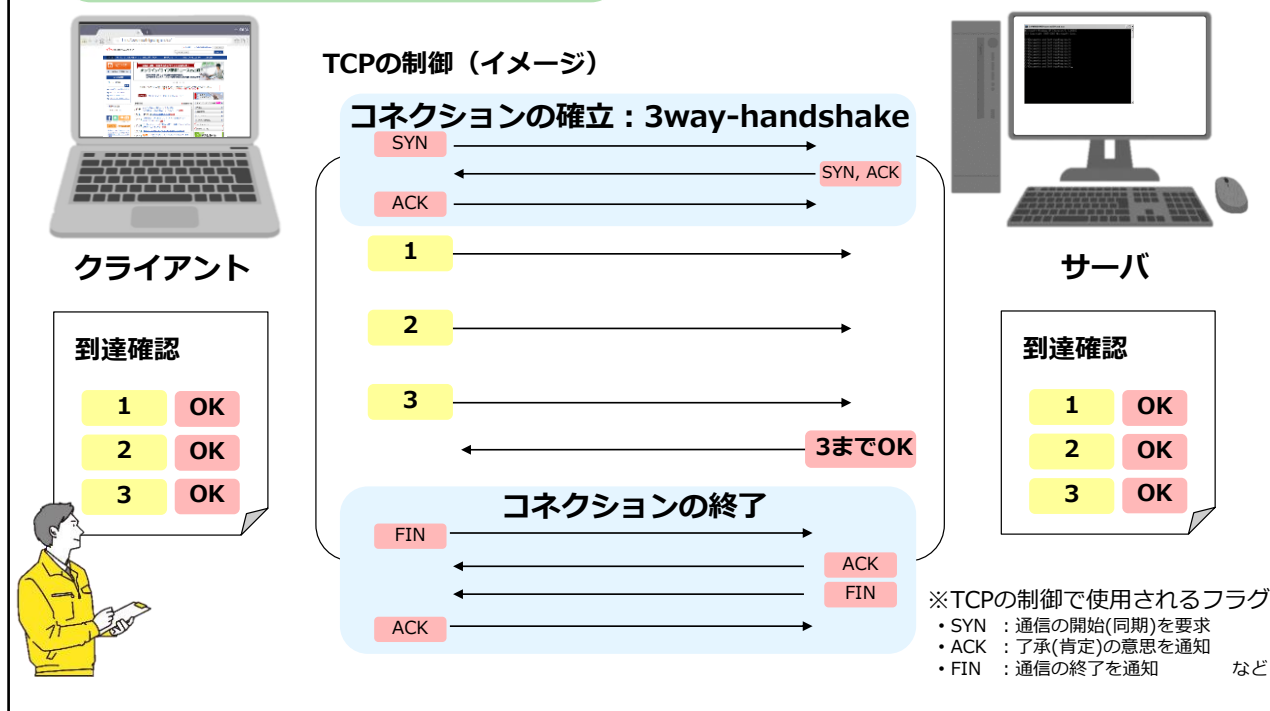
次は、TCPについて解説します。

4.4 TCPの機能



画面左下の▶にて、TCPを用いた通信の流れを確認しましょう。

通信の信頼性を制御する技術



TCPでは、ポート番号によるアプリケーションの識別に加え、通信状態の確認や再送制御を行い、通信の信頼性を確保します。そのため、TCPを使用した通信では、送信元が発信したデータが不足なく宛て先のコンピュータへ届きます。TCPを採用するアプリケーションでは、送信データが必ず宛て先に到達することを前提にプロトコルを開発することができます。

信頼性を確保するための仕組みとして、以下の3点があります。

・コネクション管理

通信に先立ち、コネクション(関係)を確立します。コネクション確立時(3way-handshake)には、通信に必要な各種情報が交換され、通信の準備がなされます。コネクションを確立したアプリケーション間での通信は、TCPによって制御されます。通信が終了したならば、コネクションも終了されます。なお、コネクションは同時に複数確立することができます。またコネクション確立時や終了時には、図のようにさまざまなフラグを使用した特徴的な通信が発生します。

・応答確認

すべての送信データが宛て先に到達しているかを確認します。宛て先側は、データを受信すると送信元側に応答を返信します。

・順序番号管理

データの送受信が成功しているかをチェックするために、データに番号を付与します。この情報は、応答確認時に通知されます。

応答確認に何番目のデータまでを受信したかを示す情報が入ります。送信元では、不足なくデータを伝達できているかが確認できます。もし、送信したが到達が確認できていないデータがある場合には、不足しているデータを再送し補完します。

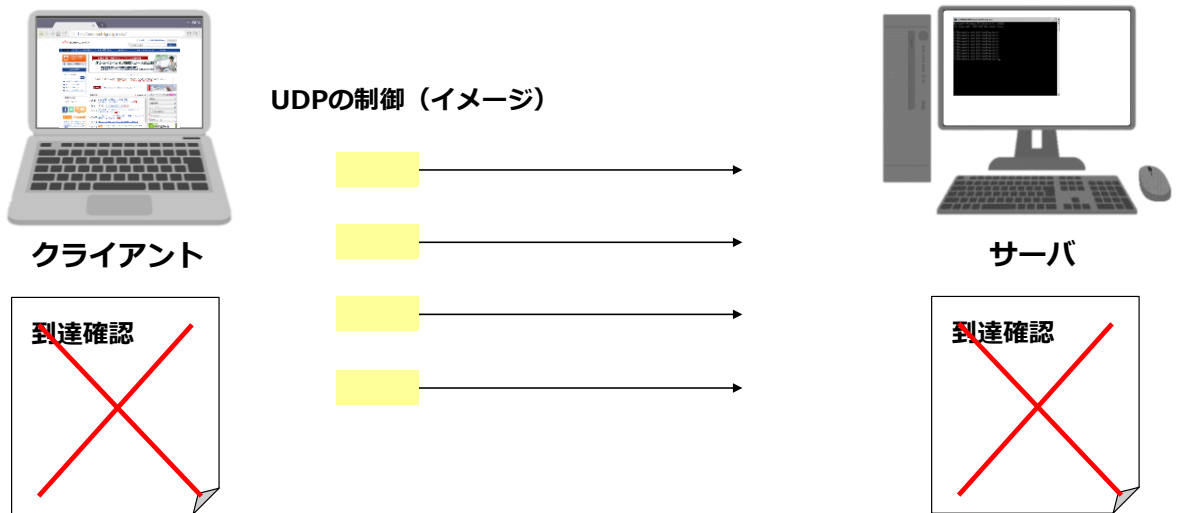
【参考】

フロー制御:

TCPの機能の1つです。宛て先コンピュータの処理性能や伝送路の状況により、データ伝送のスピードを調整します。フロー(通信の流れ)を制御し、適切なタイミングでデータを送信します。例) 宛て先コンピュータの処理性能が低い場合、一度に大量のデータを送信すると処理が追いつかないため、データ伝送のスピードを遅くする。

4.5 UDPの機能

効率重視のデータ転送



UDPでは、ポート番号によるアプリケーションの識別のみを行います。そのため、TCPを使用した通信と異なり、通信の信頼性は確保されません。

TCPでは、信頼性を確保するための制御をするため、データの到達タイミングが一定間隔にならない可能性があります。データの到達が一定の間隔になることが望まれるマルチメディア通信などでは、TCPの制御がデメリットとなります。

UDPを採用するアプリケーションでは、細かい制御がされない分、装置やネットワークに負荷をかけない効率の良い通信が可能です。（データの再送など制御が必要な場合は、アプリケーションプロトコルで実装する必要があります。）

<UDPに向いている通信の特徴>

- 一定の間隔でデータが到達することが望まれる通信
例) 音声や動画配信など、リアルタイム性が重視される通信。
- 通信で発生するデータ量が多く、TCPの処理負荷が過大になる通信
例) DNSなど、サーバへの同時接続数が多い通信。

<参考> Windows OSのコマンド操作方法

本コースでは、Windowsのコマンドプロンプトを用いたコマンド操作にて演習手順を解説します。端末の設定やネットワーク接続状況に応じて、実行結果が異なることをあらかじめご了承ください。



画面内にコマンドを入力し、[Enter]キーで実行します。入力したコマンドに応じて、コンピュータ設定の確認や変更が可能です。本コースでは、ネットワーク設定の確認に使用します。※コマンドの詳細は、「コマンド紹介ページ」にて解説します。（付録にもまとめています。）

コマンドプロンプトを起動 コマンドプロンプト画面（イメージ）

Windowsのコマンド操作方法

操作の流れ	手順詳細
手順1. 事前準備 （コマンドプロンプトを起動） ※起動手順は複数あります。	<ul style="list-style-type: none">・ [Windowsロゴ]キーと[R]キーを同時に入力する。・ [ファイル名を指定して実行]の画面で、「cmd」を入力し[OK]を選択する。・ コマンドプロンプト（cmd.exe）を起動する。
手順2. コマンド入力し実行	<ul style="list-style-type: none">・ 起動した[コマンドプロンプト]の画面の「>」（大なり表示）の後ろに、コマンド（例、「netstat -n」）を入力する・ [Enter]キーでコマンドを実行する
手順3. コマンド結果を確認	<ul style="list-style-type: none">・ コマンドの実行結果が表示される （例、netstatコマンドの場合は、端末のアクティブなTCP接続が表示される）

ここでは、今後の演習で使用するWindows端末のコマンド操作方法について解説します。Windows OSでは、「コマンドプロンプト」を起動し、画面内に入力したコマンドに応じて、コンピュータ設定の確認や変更が可能です。コマンドの詳細はコマンド紹介ページにて解説します。（付録にもまとめています。）

※注意

操作端末の設定やネットワーク接続状況に応じてコマンド実行結果が異なります。実行例が実際の結果とは異なる場合があることをご了承ください。

次は、端末のアクティブなTCP接続を確認するコマンドを紹介します。 netstat コマンドです。

<コマンド紹介> netstat コマンド

> " netstat -n "と入力

> netstat -n ※"netstat"と"-n"の間には、空白（ブランク）が必要

ポート番号は、コロン（:）の後ろに表示される

- ・[ローカルアドレス]側は 送信元情報
- ・[外部アドレス]側は 宛て先情報

アクティブな接続

プロトコル	ローカル アドレス	外部アドレス	状態
TCP	172.16.1.10:49181	172.200.1.10:80	TIME_WAIT
TCP	172.16.1.10:49198	172.16.1.100:80	ESTABLISHED
TCP	172.16.1.10:49209	172.20.20.20:21	ESTABLISHED
TCP	172.16.1.10:49212	172.100.1.10:1048	ESTABLISHED

アクティブなTCP接続が1行ずつ表示される

[プロトコル]、[ローカルアドレス]、[外部アドレス]、[状態]が、1行で表示され、接続情報が確認可能

表示される内容は以下の通りです。

- ・[プロトコル] → TCPかUDPか示す（基本はTCPと表示）
- ・[ローカルアドレス] → 送信元側（自側）IPとポート（詳細は5章）
- ・[外部アドレス] → 宛先側（対向側）IPとポート（詳細は5章）
- ・[状態] → 接続状態（表示内容はOSに依存）

コマンド紹介ページでは、Windowsコマンドプロンプト上の実行例を用いて各コマンドを紹介します。最後の付録にもコマンド紹介ページをまとめています。

ここでは、netstatコマンドを紹介します。

netstatコマンドは、TCP/IPのセッション情報を表示します。アクティブなTCP接続、コンピュータが待ち状態のポート、イーサネット統計情報、IPルーティングテーブル、TCP/IP統計情報を表示します。

<構文>

netstat 各オプション

<主なオプション>

- n : セッション中のローカルコンピュータと宛て先コンピュータのIPアドレスとポート番号を表示します。
- e : 送受信データの統計情報を表示します。
- s プロトコル名 : プロトコルごとの統計情報を表示します。デフォルトではTCP、UDP、ICMP、IPの統計情報が表示されます。
- r : ローカルコンピュータのルーティングテーブルを表示します。

【参考】

実行結果には、デスクトップに表示されていないアプリケーションの通信や、実際のWebサーバとは異なる別のサーバを経由した通信もアクティブなTCP接続として表示されます。

<演習問題2> ポート番号を確認してみよう

■ 演習問題2 ■

コマンドプロンプトを使用し、アクティブなTCP接続を一覧表示してください。

【実行例】

```
コマンドプロンプト
> netstat -n
アクティブな接続

プロトコル  ローカル アドレス  外部アドレス  状態
TCP  10.1.1.15:65000  10.1.2.100:80  ESTABLISHED
TCP  10.1.1.15:65011  10.1.2.100:8080 ESTABLISHED
TCP  10.1.1.15:65022  10.1.2.100:25  ESTABLISHED
>
```

コマンドプロンプトを起動し、
netstatコマンドを実行する

※ 図のコマンドの場合、
“netstat”と“-n”の間には、
空白（ブランク）が必要

「:」（コロン）の後ろがポート番号

まずは実行してみましょう。
結果は、状況に応じて異なります。
左図の実行結果の場合、
ポート番号は「:」（コロン）の後ろに表示されます。

1行で一つのTCP接続を示しています。
ポート番号は以下のように読み取れます。
・1行目の送信元ポート番号は、65000です。
・1行目の宛て先ポート番号は、80です。

※「10.1.1.15」の表記に関しては、次の第5章で解説します。

■ 演習問題2 ■

コマンドプロンプトを使用し、アクティブなTCP接続を一覧表示してみましょう。

【操作手順】

操作手順は以下のとおりです。

- 手順1. コマンドプロンプトにて“netstat -n”を入力しコマンドを実行する
- 手順2. 実行結果として表示されたアクティブなTCP接続の一覧を確認する
- 手順3. 各行の送信元ポート番号、宛て先ポート番号部分を読み取る

【実行例】

実行例は図の下段のとおりです。

実行結果のうち、下記の1行を実行例として解説します。

実行例（図の1行）：「TCP 10.1.1.15:65000 10.1.2.100:80 ESTABLISHED」

ポート番号は、実行例の「:」（コロン）の後ろに表示されるため、使用している送信元ポート番号は「65000」、宛て先ポート番号は「80」と読み取れます。

※コマンド操作については、Windows OSのコマンド操作方法（本資料P.36）を参照してください。

※netstatコマンドについては、コマンド紹介ページ（本資料P.37）を参照してください。

次は、本章のまとめです。

4.6 章のまとめ

- トランスポート層では、コンピュータ内のアプリケーション通信の識別やデータの送信チェック、再送を行います。TCPとUDPの2つのプロトコルが存在しています。
 - ✓ TCP : 送信側と受信側で、データの抜けや不達がなく、確実に受け渡しできるように制御する
 - ✓ UDP : 細かい制御がされない分、装置やネットワークに負荷をかけない効率の良い通信が可能である
- ポート番号は通信アプリケーションを識別するために使用されます。
- サーバ用のポート番号はクライアントからの要求を受け取るため、使用する番号があらかじめ規定されています。（ウェルノウンポート）

第4章のまとめです。

- トランスポート層では、コンピュータ内のアプリケーション通信の識別やデータの送信チェック、再送を行います。TCPとUDPの2つのプロトコルが存在しています。
 - ✓ TCP : 送信側と受信側で、データの抜けや不達がなく、確実に受け渡しできるように制御する
 - ✓ UDP : 細かい制御がされない分、装置やネットワークに負荷をかけない効率の良い通信が可能である
- ポート番号は通信アプリケーションを識別するために使用されます。
- サーバ用のポート番号はクライアントからの要求を受け取るため、使用する番号があらかじめ規定されています。（ウェルノウンポート）

第5章

端末を識別する仕組み (インターネット層)

学習目標

この章では、TCP/IPのインターネット層について学習します。

- IPアドレス、ルーティングなどの用語について理解する。
- 端末を識別する仕組みを理解する。
- データの伝送経路の決定の仕組みを理解する。

5.1 インターネット層

ネットワーク上のコンピュータを識別する

コンピュータシステム



TCP/IPプロトコル階層

アプリケーション層	HTTP	SMTP	POP3	Telnet
トランスポート層	TCP/UDP			
インターネット層	IP			
ネットワーク インターフェース層	LAN (Ethernetなど)		WAN (PPP、フ レームリレーなど)	

TCP/IPのインターネット層では、IPがあります。この層では、ネットワーク内のコンピュータを識別しデータを配送したり、データの伝送経路を決定したりします。

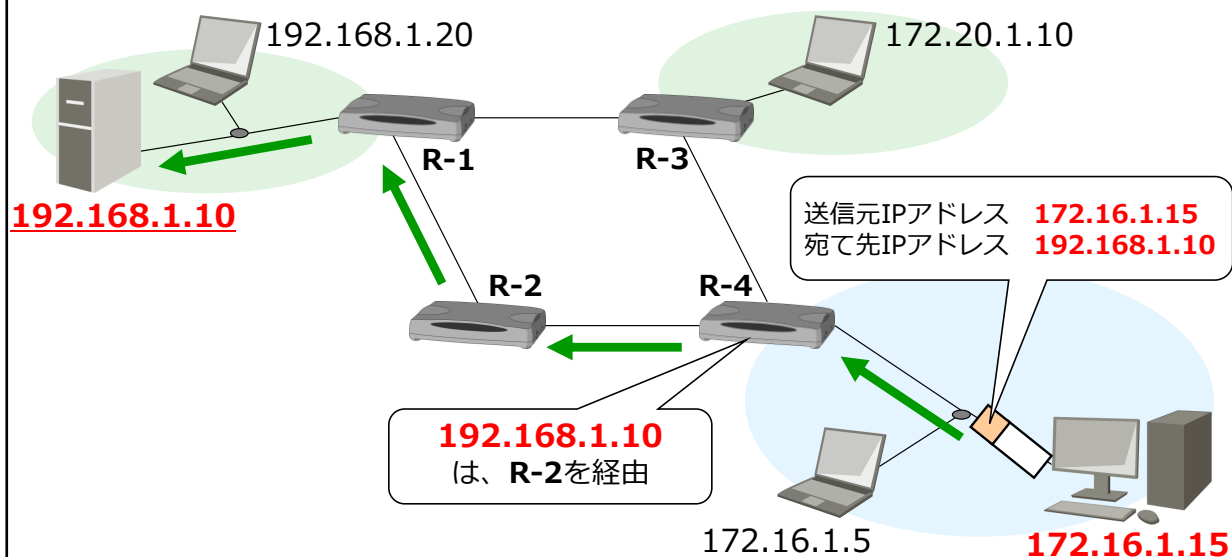
5.2 IPの役割

5.2.1 IPの役割

IPの役割は、データの配送を実現すること

端末の識別(アドレッシング): ネットワーク上の端末を識別する

経路の決定(ルーティング): データの転送方向を判断する



IPの役割は、送信元の端末から宛て先の端末へデータを届けることです。

ネットワーク上に存在する複数の端末から送信元と宛て先を特定し、到達可能な経路を判断することによって通信を実現します。

• 端末の識別(アドレッシング)

通信を実現するには、送信元と宛て先の端末を特定する必要があります。そのため、ネットワーク上の全端末に識別子を付与します。

IPでは、**IPアドレス**と呼ばれる識別子を用います。通信前に端末には他の端末と重複しないIPアドレスを設定しておく必要があります。

IPアドレスには、構造や割り当てルールが定義されています。

• 経路の決定(ルーティング)

通信を実現するには、送信元から宛て先までの到達可能な経路にデータを誘導する必要があります。そのため、相互接続しているネットワークへの到達可能な経路を事前に登録しておきます。経路情報は、ルータやPCなどの装置内にあるルーティングテーブルに登録します。

※利用者は、FQDNで宛て先を指定しますが、コンピュータ内部では、IPアドレスを用いて通信制御をしています。また、利用者は、FQDN名ではなくIPアドレスを指定し、通信することも可能です。

次は、アドレッシングについてアニメーションを用いて解説します。

5.2.2 IPの役割 (続き1)



画面左下の▶にて、
アドレッシングを確認しましょう。

IPの役割は、データの配送を実現すること

端末の識別(アドレッシング): ネットワーク上の端末を識別する

経路の決定(ルーティング): データの転送方向を判断する

アドレッシングにより、
配送されるデータの
始点と最終目的地を
識別できる

配送されるデータには、
送信元と宛て先を示す、
アドレスが含まれる

送信元IPアドレス **172.16.1.15**
宛て先IPアドレス **192.168.1.10**

送信元端末

宛て先端末



アドレッシングは、郵便物の宛て先を指定
するのに住所を使うことと似ています。
すべての通信端末に、異なるIPアドレスを
割り当てることで、ネットワーク上の
どの端末なのか、識別できるようにします。

172.16.1.5

172.16.1.15

アドレッシングは、郵便物の宛て先を指定するために住所を使うことと似ています。
すべての通信端末に、異なるIPアドレスを割り当てることで、ネットワーク上のどの端末なのか、
識別できるようにします。

・端末の識別(アドレッシング)

通信を実現するには、送信元と宛て先の端末を特定する必要があります。そのため、ネットワーク上の全端末に識別子を付与します。

IPでは、IPアドレスと呼ばれる識別子を用います。通信前に端末には他の端末と重複しないIPアドレスを設定しておく必要があります。

IPアドレスには、構造や割り当てルールが定義されています。

次は、ルーティングについてアニメーションを用いて解説します。

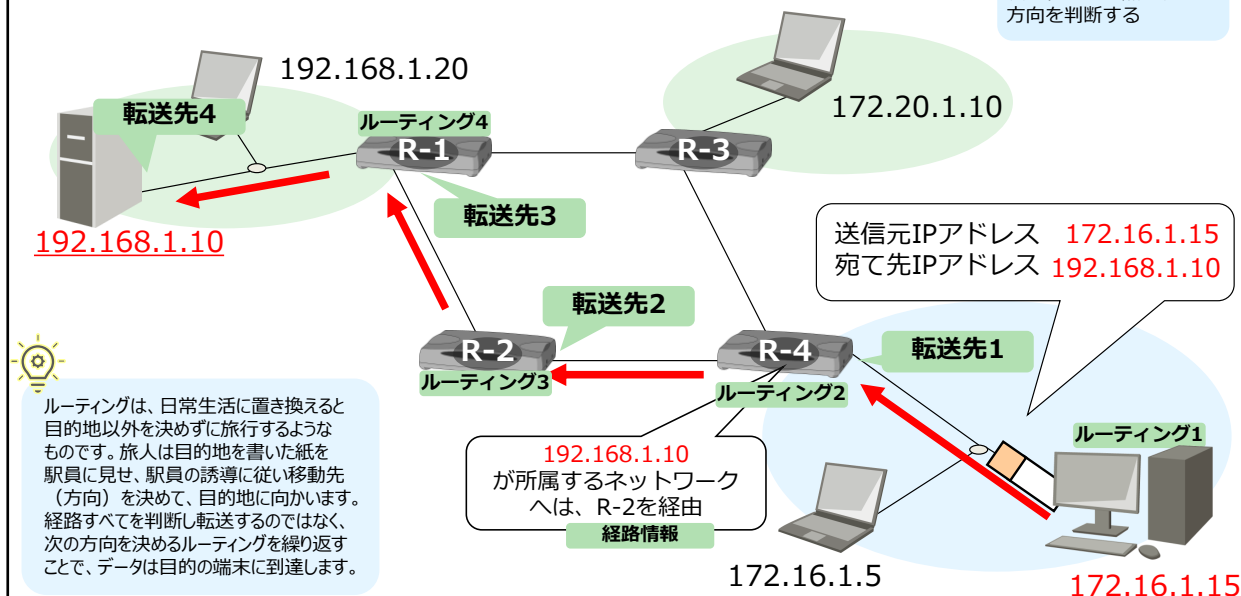
5.2.3 IPの役割 (続き2)



画面左下の▶にて、
ルーティングを確認しましょう。

IPの役割は、データの配送を実現すること
端末の識別(アドレッシング): ネットワーク上の端末を識別する
経路の決定(ルーティング): データの転送方向を判断する

ルーティングは、
次に経由する点を決めて
方向を判断する



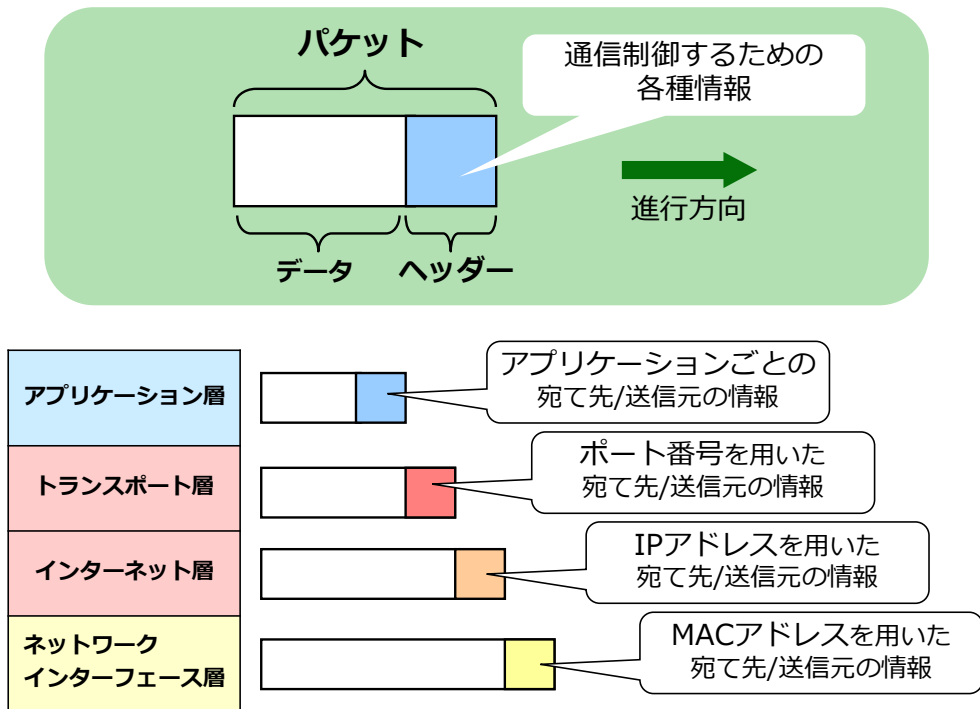
ルーティングは、日常生活に置き換えると、目的地以外を決めずに旅行するようなものです。旅人は目的地を書いた紙を駅員に見せ、駅員の誘導に従い移動先（方向）を決めて、目的地に向かいます。経路すべてを判断し転送するのではなく、次の方向を決めるルーティングを繰り返すことで、データは目的の端末に到達します。

• 経路の決定(ルーティング)

通信を実現するには、送信元から宛て先までの到達可能な経路にデータを誘導する必要があります。そのため、相互接続しているネットワークへの到達可能な経路を事前に登録しておきます。経路情報は、ルータやPCなどの装置内にあるルーティングテーブルに登録します。

次は、送信元端末から宛て先端末まで配送されるデータ（パケット）について解説します。

5.3 パケットとヘッダー



通信を実現するには、データを配送するための情報(宛て先情報など)が必要です。そのため各プロトコルには、データに必要な情報を付加する仕組みがあります。その情報は、通信の進行方向の先頭に付加されます。この領域を**ヘッダー**といいます。また、データにヘッダーを付加したものを**パケット**といいます。

ヘッダーは、各プロトコルがデータ処理をするタイミングで付加および削除されます。プロトコルごとに付加される情報はフォーマットで定義されています。

- アプリケーション層のヘッダー
各アプリケーションで必要とされる情報(SMTP/POP3の場合はメールアドレス、HTTPの場合はURLなど)が格納される。
- トランスポート層のヘッダー
TCPまたは、UDPの処理で必要な情報(ポート番号や順序番号など)が格納される。
- インターネット層のヘッダー
IPの処理で必要な情報(IPアドレスなど)が格納される。
- ネットワークインターフェース層のヘッダー
各ハードウェア規格で必要とされる情報(Ethernetの場合はMACアドレスなど)が格納される。

次からは、インターネット層のヘッダーであるIPアドレスについて詳しく解説します。

5.4 IPアドレス

5.4.1 表記方法

ビット表記

10101100 00010000 00000001 00001111

コンピュータ
向き



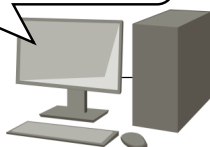
ドット表記

172 . 16 . 1 . 15

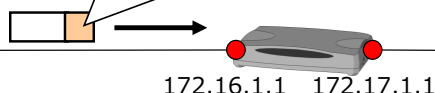
利用者
向き



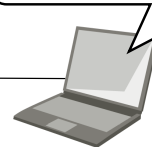
IPアドレス
172.16.1.15



送信元IPアドレス172.16.1.15
宛て先IPアドレス172.17.1.10



IPアドレス
172.17.1.10



現在、主に使用されているIPアドレスはバージョン4です。32bit(ビット)で表現され、約43億台の端末を識別することができます。IPアドレスの表記方法は2つあります。

・ビット表記

32個の0または1で表現される方法です。装置内部での処理は、デジタルな信号(0または1)で取り扱われるため、2進数の表記が適します。

例) 10101100000100000000000100001111

・ドット表記

0 または1の羅列は利用者(人)にとっては、不便さがあります。そのため、人にとって馴染みの深い10進数での表記が適します。

例) 172.16.1.15

<ビット表記からドット表記への変換>

8bit(1オクテット)単位で10進数へ変換し、ドット(.)で区切ります。逆変換を行うには、10進数から2進数へ変換しドットを削除します。8bit分の変換については[こちら](#)を参照してください。

例) 10101100 (2進数) ⇔ 172 (10進数)

$$1(2^7) + 0(2^6) + 1(2^5) + 0(2^4) + 1(2^3) + 1(2^2) + 0(2^1) + 0(2^0) \\ = 128 + 32 + 8 + 4 = 172_{(10)}$$

2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰
128	64	32	16	8	4	2	1
1	0	1	0	1	1	0	0

【用語解説】

オクテット:

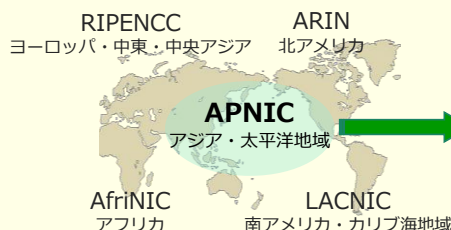
情報量を表す単位の1つで、1オクテットは8ビットに相当する。

5.4.2 管理方法

■インターネットで使用するアドレス(グローバルアドレス) 全IPアドレスを組織で分担して管理する

IANA : インターネットにおける世界中のIPアドレスを管理する組織

RIR : 管轄地域のIPアドレスを管理する組織



NIR : 国家や地域におけるIPアドレスを管理する組織



■イントラネットで使用するアドレス(プライベートアドレス)



FLM商事 : 10.*.*.*

東京本社 10.1.*.*	大阪支社 10.2.*.*	名古屋支社 10.3.*.*
営業部 10.1.1.*	営業部 10.2.1.*	営業部 10.3.1.*
開発部 10.1.2.*	開発部 10.2.2.*	開発部 10.3.2.*

IPアドレスは、端末を識別することが目的であるため重複することは許されません。ネットワークに接続されている全端末において、重複が発生しないように管理する必要があります。
アドレスを管理する組織やルールは、インターネットとイントラネットで異なります。

・インターネットでのIPアドレス管理

インターネットに接続する端末に割り当てるIPアドレスは、国際的な管理団体により管理されています。全体管理をする**IANA**、地域別の**RIR(地域インターネットレジストリ)**、国別の**NIR(国別インターネットレジストリ)**、IPアドレス管理指定事業者として指定された**LIR(ローカルインターネットレジストリ)**が階層構造で組織され、IPアドレスを分配・管理しています。アジア地域のRIRはAPNIC、日本のNIRは、JPNICです。

IANAにおいて、IPアドレスの特定の範囲がRIRに分配され、その一部が最終的にはLIRに分配されます。その範囲からユーザーにIPアドレスを割り当てているため、インターネット全体で、重複が発生しない仕組みとなっています。

・イントラネットでのIPアドレス管理

イントラネットに接続する端末に割り当てるIPアドレスは、組織内の情報システム部などが管理します。イントラネットと独立しているため、イントラネット内でのIPアドレス重複を避けることができ、IPアドレスの各オクテットに意味を付与するなど、IPアドレス割り当てルールを作成し、重複が発生しない仕組みを作ります。

例)2オクテット目：拠点識別コード、3オクテット目：部署識別コード、4オクテット目：ホスト識別アドレス

アドレスの管理元を明確化するために、**インターネットで使用するアドレス(グローバルアドレス)**と**イントラネットで使用されるアドレス(プライベートアドレス)**は、アドレス範囲が異なります。
プライベートアドレスの範囲は、[こちら](#)を参照してください。

プライベートアドレスの範囲

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

【参考】

日本国内では、JPNIC という団体がグローバルアドレスを統括管理しています。実際のアドレス割り当て管理業務は、JPNICからIPアドレス管理指定事業者の指定を受けた組織(プロバイダーなど)が代行しています。

JPNIC : <https://www.nic.ad.jp/ja/>

5.4.3 領域

ビット表記

10101100

00010000

00000001

00001111

ドット表記

172

.

16

.

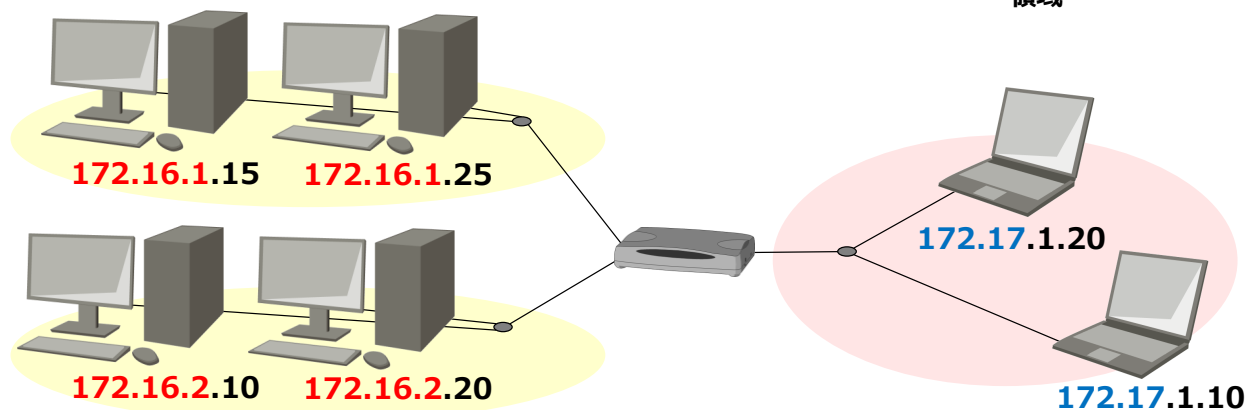
1

.

15

ネットワークアドレス領域

ホストアドレス
領域



IPアドレスは、端末同士で重複しないことが条件です。そのため、割り当てるアドレスを管理する必要があります。管理を簡素化するために、大きく2つの領域が存在します。

・ネットワークアドレス領域

端末が所属するネットワーク(※)を一意に識別するための情報を表す部分です。同一ネットワークに接続されている端末には、ネットワーク識別の領域に同じ数値が割り当たります。

・ホストアドレス領域

ネットワーク内にある端末を一意に識別するための情報を表す部分です。同一のネットワークに接続されている端末には、ホストアドレス領域に異なる数値が割り当たります。

<ネットワークアドレス領域と、ホストアドレス領域の境界線>

各領域の境界線は、**アドレスクラス**、**サブネットマスク**で定義します。

※「ネットワーク」の範囲について

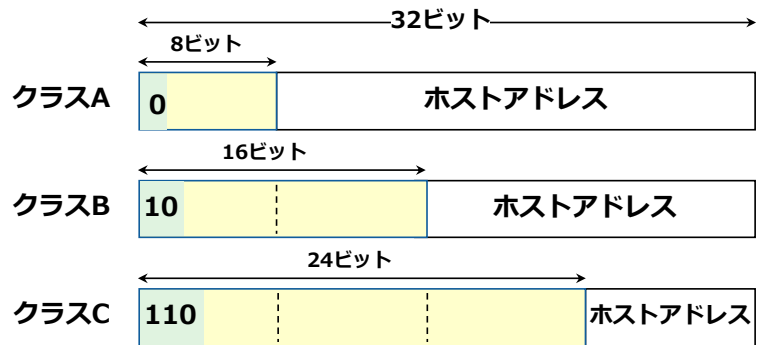
広義では、端末が相互接続されている様子のことです。狭義ではルーティング装置(ルータ、L3スイッチ)によって分割される範囲のことです。(狭義の範囲を正確には「**ブロードキャストドメイン**」と呼びます。)

本ページは、狭義で使用しています。

次は、各領域の境界線を定義しているアドレスクラスとサブネットマスクについて解説します。

5.4.4 アドレスクラス

IPアドレスのクラス



クラス体系

アドレス クラス	ネットワークアドレスの 大きさ	ホストアドレス の大きさ	ネットワークアドレスとして 利用できる値	ネットワーク アドレス の割り当て個数	ホストアドレス の割り当て個数
クラスA	8ビット (先頭は“0”固定)	24ビット	0.0.0.0 ~ 127.0.0.0	128	16,777,216
クラスB	16ビット (先頭は“10”固定)	16ビット	128.0.0.0 ~ 191.255.0.0	16,384	65,536
クラスC	24ビット (先頭は“110”固定)	8ビット	192.0.0.0 ~ 223.255.255.0	2,097,152	256

※ただし、127.0.0.0などは、規格上予約範囲とされており、一般のネットワークアドレスとして使用することはできません。
また、ネットワークアドレスの割り当て個数とホストアドレス割り当て個数の中には、端末に割り当て不可能なアドレスも含まれます。

アドレスクラスは、IPアドレスの領域長を定めるルールです。クラスは、A～Eまでの5種類があり、用途により分類されています。

次ページのサブネットマスクが利用される以前は、アドレスクラスに基づき、IPアドレスの領域を考えていました。アドレスクラスにより定義されたネットワーク識別の領域のことを、「ネットワークアドレス領域」と呼び、後半の端末を識別する領域を「ホストアドレス領域」と呼ぶ場合もありました。

現在、クラスA～CのIPアドレスは、サブネットマスクに従い領域を識別しています。

- ・1対1の通信(ユニキャスト)に使用するアドレス

クラスA ネットワークアドレス領域：8bit + ホストアドレス領域：24bit

1つのネットワークに約1700万台の端末を接続することができる大規模ネットワークを想定したクラス。ただし、ネットワークの数は、約100個を上限とする。

クラスB ネットワークアドレス領域：16bit + ホストアドレス領域：16bit

1つのネットワークに約6万5千台の端末を接続することができる中規模ネットワークを想定したクラス。ただし、ネットワークの数は、約1万6千個を上限とする。

クラスC ネットワークアドレス領域：24bit + ホストアドレス領域：8bit

1つのネットワークに約250台の端末を接続することができる小規模ネットワークを想定したクラス。ただし、ネットワークの数は、約200万個を上限とする。

- ・複数の端末への一斉送信(マルチキャスト)に使用するアドレス

クラスD

一定の条件を満たす端末へデータを一斉送信するためのアドレス。個別の端末へは割り当てません。

- ・実験用アドレス

クラスE

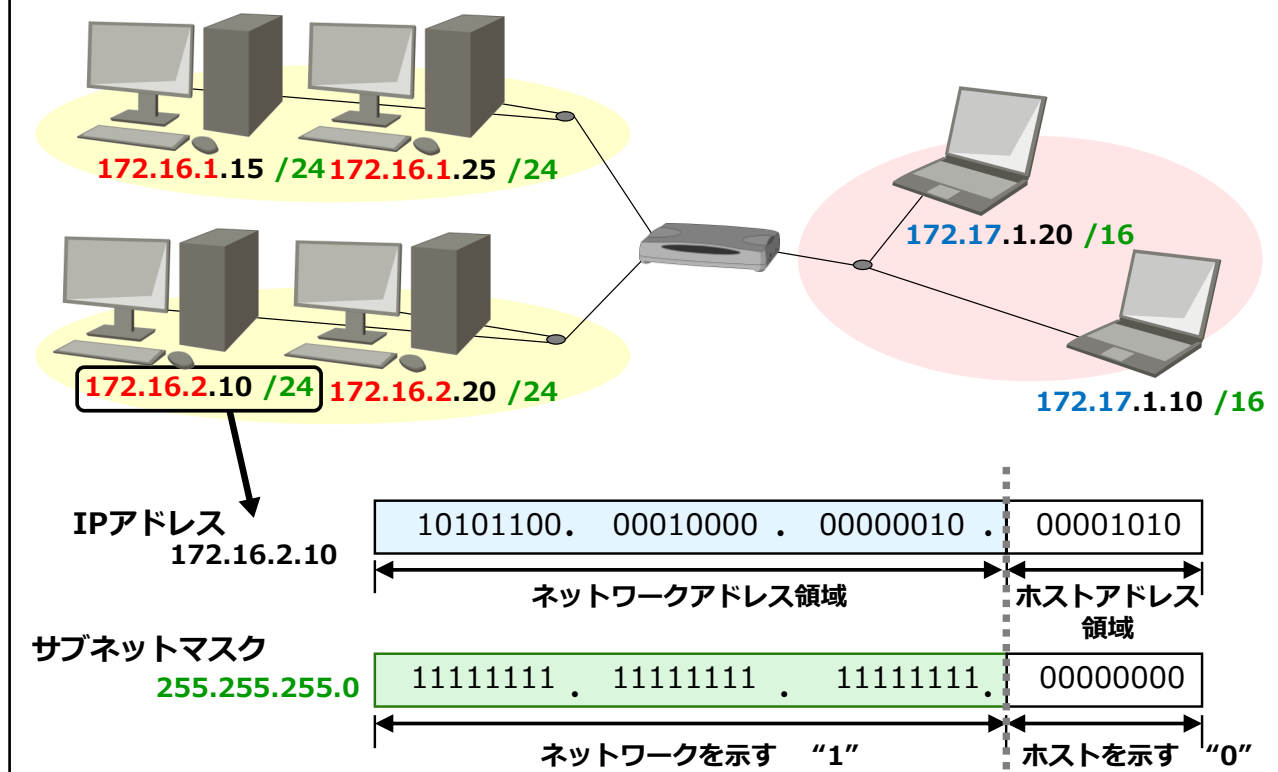
開発時から予約されている実験用のアドレス。通信で使用することはありません。

<アドレスの識別方法>

先頭のビットをチェックすることで、クラスを判断することができます。先頭1ビットが“0”であればクラスA、先頭2ビットが“10”であればクラスB、先頭3ビットが“110”であればクラスCです。
(ドット表記における範囲は図の表を参照)

次は、サブネットマスクについて解説します。

5.4.5 サブネットマスク



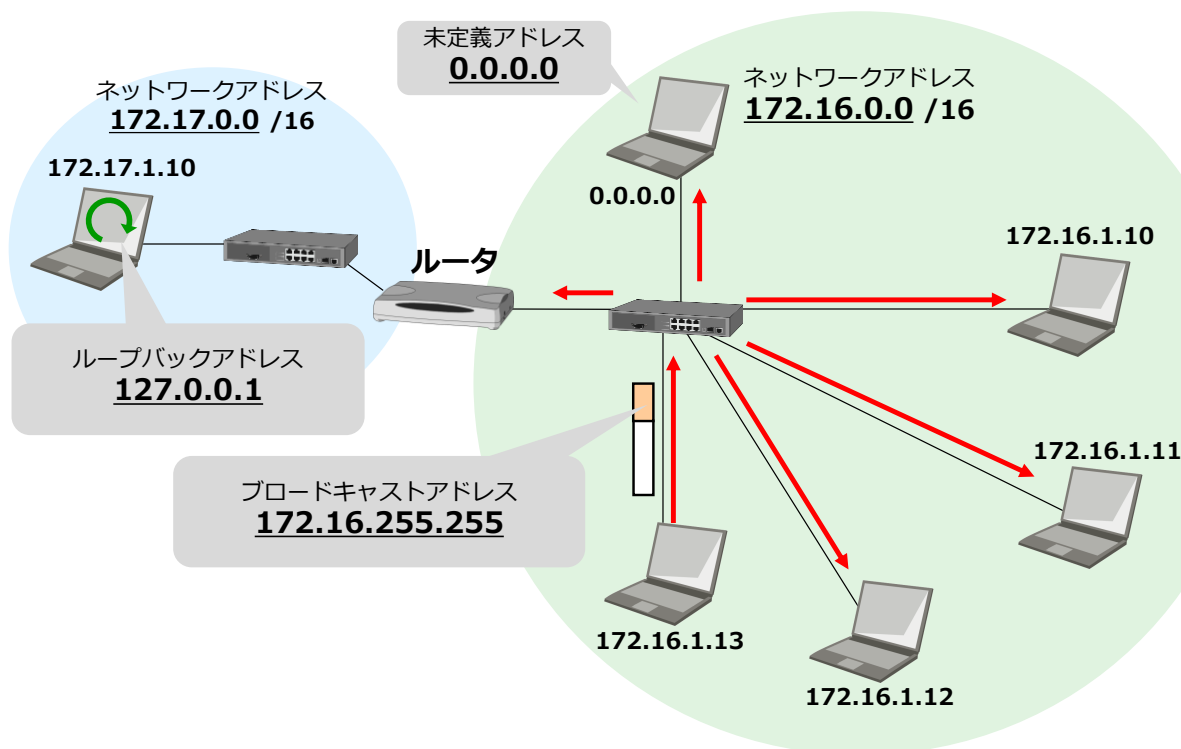
ネットワークアドレス領域長は任意に定義できます。ネットワーク管理者により設計された領域長は、**サブネットマスク**により示されます。

サブネットマスクは、IPアドレスと同様に32ビットで表現されます。

サブネットマスクの表記方法は3つあります。

- ① ネットワークアドレス領域を、先頭から2進数の「1」で表し、ホストアドレス領域を「0」で表す。
例) **11111111 11111111 11111111 00000000**
(ネットワークアドレス領域:先頭から24bit、ホストアドレス領域:末尾の8bit)
- ② ①の表記を10進数のドット表記へ変換して表す。
例) **255.255.255.0**
- ③ ①の表記において、先頭から連続する「1」の数をIPアドレスの後に、スラッシュ(/)を付けて表す。
例) 172.16.1.15 /24

5.4.6 特別な意味を持ったアドレス



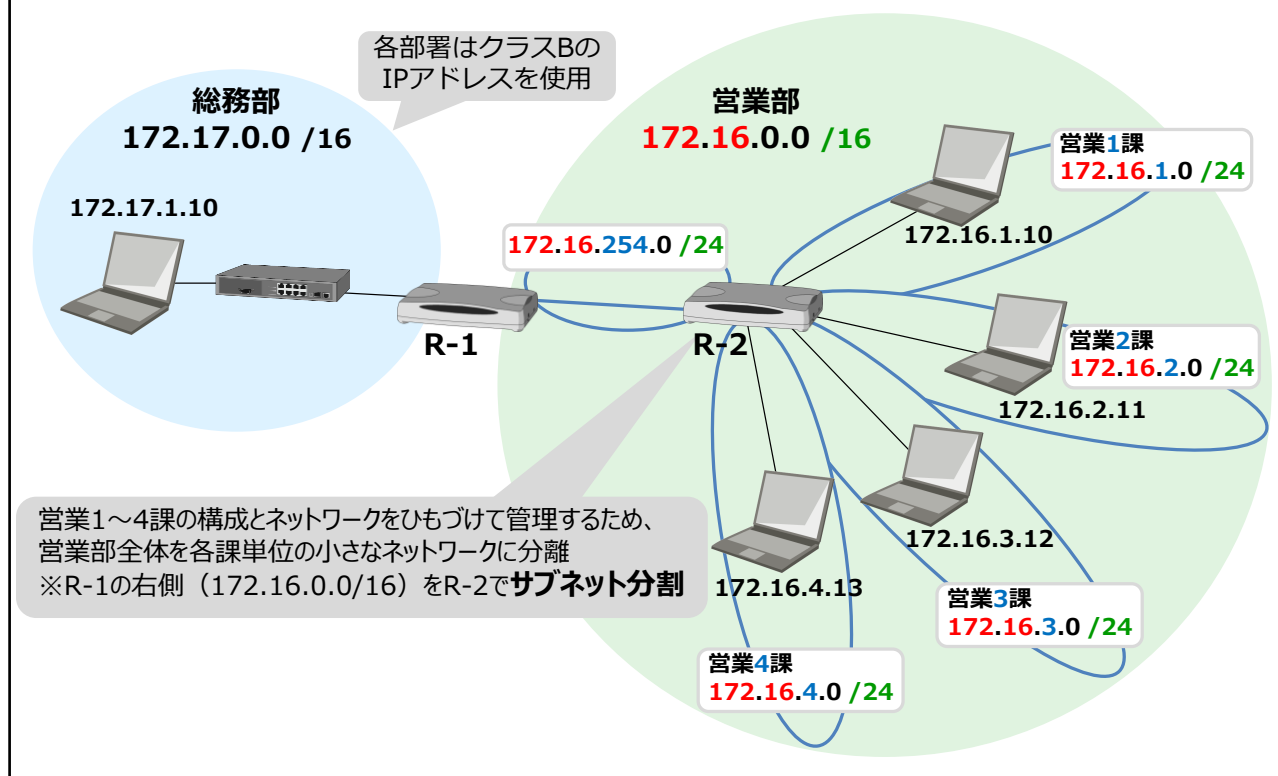
次は、特別な意味を持ったIPアドレスについて解説します。

端末にIPアドレスを割り当てる際、特別な意味を持ったIPアドレスを利用することはできません。

<特別な意味を持ったアドレス>

- **ネットワークアドレス**(例：172.16.0.0/16)
ホストアドレス領域の値が、すべて“0”となるアドレス。端末ではなくネットワーク全体を指し示す。
- **ブロードキャストアドレス**(例：172.16.255.255/16)
ホストアドレス領域の値が、すべて“1”となるアドレス。所属しているネットワーク内の全端末へデータを一斉送信する際に利用する。
- **未定義**(0.0.0.0)
32bitすべてが“0”となるアドレス。IPアドレスが割り当たっていない状態を示す。
- **ループバックアドレス**(例：127.0.0.1)
10進数表記で、「127」で始まるアドレス。IPネットワーク機能が稼働しているかを確認する際に使用する。

<参考> サブネット分割



組織内部が1つのネットワークで構成されている場合では、ネットワーク内の端末台数が過剰になり、多量の通信が飛び交う結果、通信効率下がります。また、組織構成とネットワークをひもづけて管理したいという要求から、部署単位や部署配下の各課単位で階層的にネットワークを小さく分割する場合もあります。

上記のように、必要に応じて組織内のネットワークを分割して、複数の小さなネットワークを構成することを**サブネット分割**と呼びます。また、サブネット分割後の小さなネットワークのことを、**サブネット**（または、**サブネットワーク**）と呼びます。

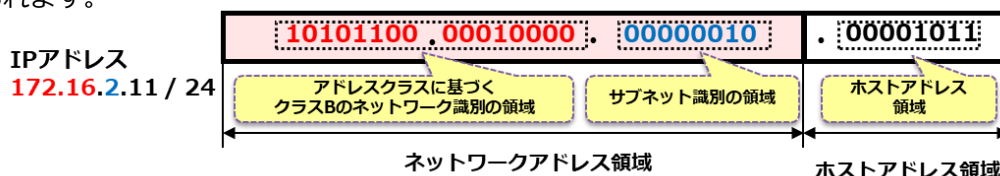
また、サブネットを構成する場合、アドレスクラスとサブネットマスクに従いIPアドレスを「3つの領域」で説明する場合もあります。

上図の172.16.2.11/24のIPアドレスを例に説明します。

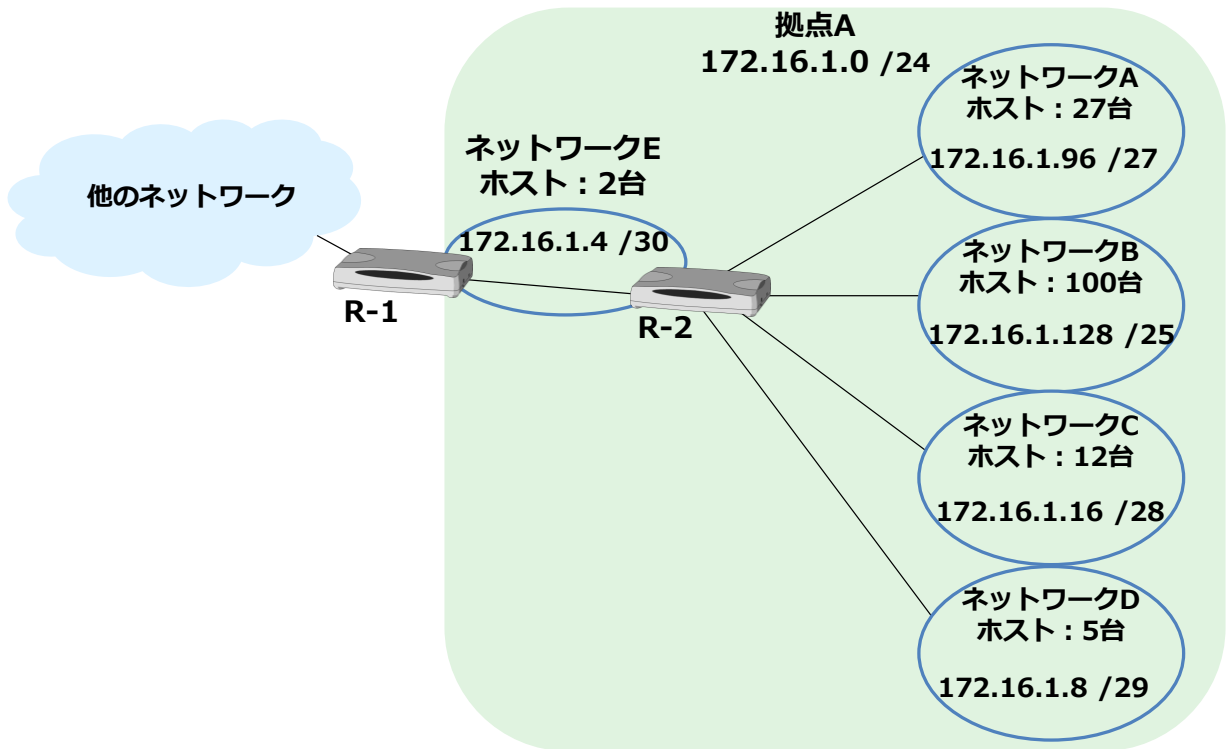
172.16.2.11/24の端末は、先頭16ビットが「172.16.*.*」のため、クラスBのIPアドレスを使用していることが確認できます。また、サブネットマスクから、先頭24ビット（3オクテット目）までが、ネットワークアドレス領域であることが確認できます。IPアドレスの先頭16ビット（先頭から2オクテット目まで）がアドレスクラスに基づく「クラスBのネットワーク識別の領域」となり、引き続き8ビット（3オクテット目）が「サブネット識別の領域」となります。末尾の残り8ビット（4オクテット目）がホストアドレス領域と判断できます。

結果として、172.16.2.11/24はクラスBのIPアドレスの範囲を使用し、「172.16.2.0/24」のサブネット（ブロードキャストドメイン）に所属していると説明できます。

172.16.2.11/24をアドレスクラスとサブネットマスクに従い「3つの領域」で説明する場合、こちらのとおりに考えられます。



<参考> ビットを意識したネットワーク分割



ここでは、可変長サブネットマスクについて解説します。

通常のサブネット分割の場合、ルータによって接続される各サブネットのマスク値は同一である必要があります。しかし、サブネット内のホスト数はすべて同じではないため、サブネットの規模によってはホストアドレスを無駄に浪費してしまうサブネットも出てきます。

そこで、サブネットのマスク値を可変にし、各サブネットの規模（必要なホスト数）に応じたアドレス分割をします。このようなネットワーク構成は**可変長サブネットマスク**または**VLSM (Variable Length Subnet Mask)**と呼ばれています。

こちらは、クラスCのアドレスをサブネット分割する際、サブネット数に対応した、ホスト数を示す表です。サブネット数および、ホスト数は、単純に数値化しています。そのため、実際に割り当てる場合は、各値から2（ネットワークアドレスとブロードキャストアドレス）を差し引いた値が、割り当て可能な数になります。

■ クラスCの場合

下表のホスト数は、ネットワークアドレスとブロードキャストアドレスを含む

ドット表記	マスク数	ビット表記	サブネット数	ホスト数
255.255.255.128	/25	<u>11111111.11111111.11111111.10000000</u>	2	128
255.255.255.192	/26	<u>11111111.11111111.11111111.11000000</u>	4	64
255.255.255.224	/27	<u>11111111.11111111.11111111.11100000</u>	8	32
255.255.255.240	/28	<u>11111111.11111111.11111111.11110000</u>	16	16
255.255.255.248	/29	<u>11111111.11111111.11111111.11111000</u>	32	8
255.255.255.252	/30	<u>11111111.11111111.11111111.11111100</u>	64	4
255.255.255.254	/31	<u>11111111.11111111.11111111.11111110</u>	128	2

クラスCのアドレスのため、
先頭24ビットは「1」に確定

先頭24ビットは「1」確定のため、
残りの4オクテット目にサブネット識別
の領域を、作成

<演習問題3> IPアドレス確認問題（問題）

■ 確認問題1 ■

下記のIPアドレスとサブネットマスクの情報から、「ネットワークアドレス領域」、「ホストアドレス領域」が、それぞれどこからどこまでか求めてください。

■ 設問1 ■

IPアドレス : 172 . 17 . 20 . 1
サブネットマスク : 255 . 255 . 255 . 0

■ 設問2 ■

IPアドレス : 10 . 1 . 1 . 128
サブネットマスク : 255 . 0 . 0 . 0

■ 確認問題2 ■

下記のような既存のネットワークに端末を一台追加したい。
端末で 사용할 수 있는 IP 주소로 올바른 것을 선택지 중에서 すべて 선택하시오.



192.168.0.0 /24

■ 選択肢 ■

- ① 172. 17. 1. 100 /24
- ② 192. 168. 10. 5 /24
- ③ 192. 168. 0. 1 /24
- ④ 192. 168. 0. 255 /24
- ⑤ 192. 168. 0. 254 /24

ここで、IPアドレスの確認問題を解いてみましょう。

■ 確認問題1

下記のIPアドレスとサブネットマスクの情報から、「ネットワークアドレス領域」、「ホストアドレス領域」が、それぞれどこからどこまでか求めてください。

■ 設問1

IPアドレス : 172. 17. 20. 1
サブネットマスク : 255. 255. 255. 0

■ 設問2

IPアドレス : 10. 1. 1. 128
サブネットマスク : 255. 0. 0. 0

■ 確認問題2

図の「192.168.0.0/24」のネットワークに端末を一台追加したい。
端末で 사용할 수 있는 IP 주소로 올바른 것을 선택지 중에서 すべて 선택하시오.
(ただし、アドレス重複は考慮しないものとして考えてください。)

■ 選択肢

- ① 172. 17. 1. 100 /24
- ② 192. 168. 10. 5 /24
- ③ 192. 168. 0. 1 /24
- ④ 192. 168. 0. 255 /24
- ⑤ 192. 168. 0. 254 /24

<演習問題3> IPアドレス確認問題（解答例）

■ 確認問題1 ■

下記のIPアドレスとサブネットマスクの情報から、「ネットワークアドレス領域」、「ホストアドレス領域」が、それぞれどこからどこまでか求めてください。

■ 設問1 ■

IPアドレス : 172 . 17 . 20 . 1
サブネットマスク : 255 . 255 . 255 . 0

■ 設問2 ■

IPアドレス : 10 . 1 . 1 . 128
サブネットマスク : 255 . 0 . 0 . 0

■ 設問1 ■

IPアドレス : 172 . 17 . 20 . 1
サブネットマスク : 255 . 255 . 255 . 0

■ 設問2 ■

IPアドレス : 10 . 1 . 1 . 128
サブネットマスク : 255 . 0 . 0 . 0

■ 確認問題2 ■

下記のような既存のネットワークに端末を一台追加したい。
端末で 사용할 수 있는 IP 주소として正しいものを選択肢の中から すべて 選びなさい。



192.168.0.0 /24

■ 選択肢 ■

- ① 172. 17. 1. 100 /24
- ② 192. 168. 10. 5 /24
- ③ 192. 168. 0. 1 /24
- ④ 192. 168. 0. 255 /24
- ⑤ 192. 168. 0. 254 /24

③と⑤が端末で使用可能。

図のネットワークアドレスと、サブネットマスクの値から、使用できるIPアドレスは、192.168.0.1～192.168.0.254の範囲が使用可能と判明するため。

■ 確認問題1（解答例）

【設問1】

サブネットマスクが「255.255.255.0」のため、先頭から3オクテット目までがネットワークアドレス領域です。残りの4オクテット目のみホストアドレス領域です。

【設問2】

サブネットマスクが「255.0.0.0」のため、先頭から1オクテット目がネットワークアドレス領域です。2オクテット目以降がホストアドレス領域です。

■ 確認問題2（解答例）

【確認問題2】

端末で使用可能なIPアドレスは選択肢の③と⑤です。

「192.168.0.0」と「/24」のサブネットマスクの値から、IPアドレスは「192.168.0.0～192.168.0.255」の範囲内である必要があります。

また、特別な意味を持ったアドレスとして、ネットワークアドレスやブロードキャストアドレスは端末に使用できないIPアドレスのため、「192.168.0.1～192.168.0.254」の範囲のIPアドレスが端末で使用可能です。

【参考】

確認問題1のアドレスを、アドレスクラスとサブネットマスクに従い「3つの領域」で説明すると、以下のとおりです。

■ 確認問題1（解答例）

【設問1】

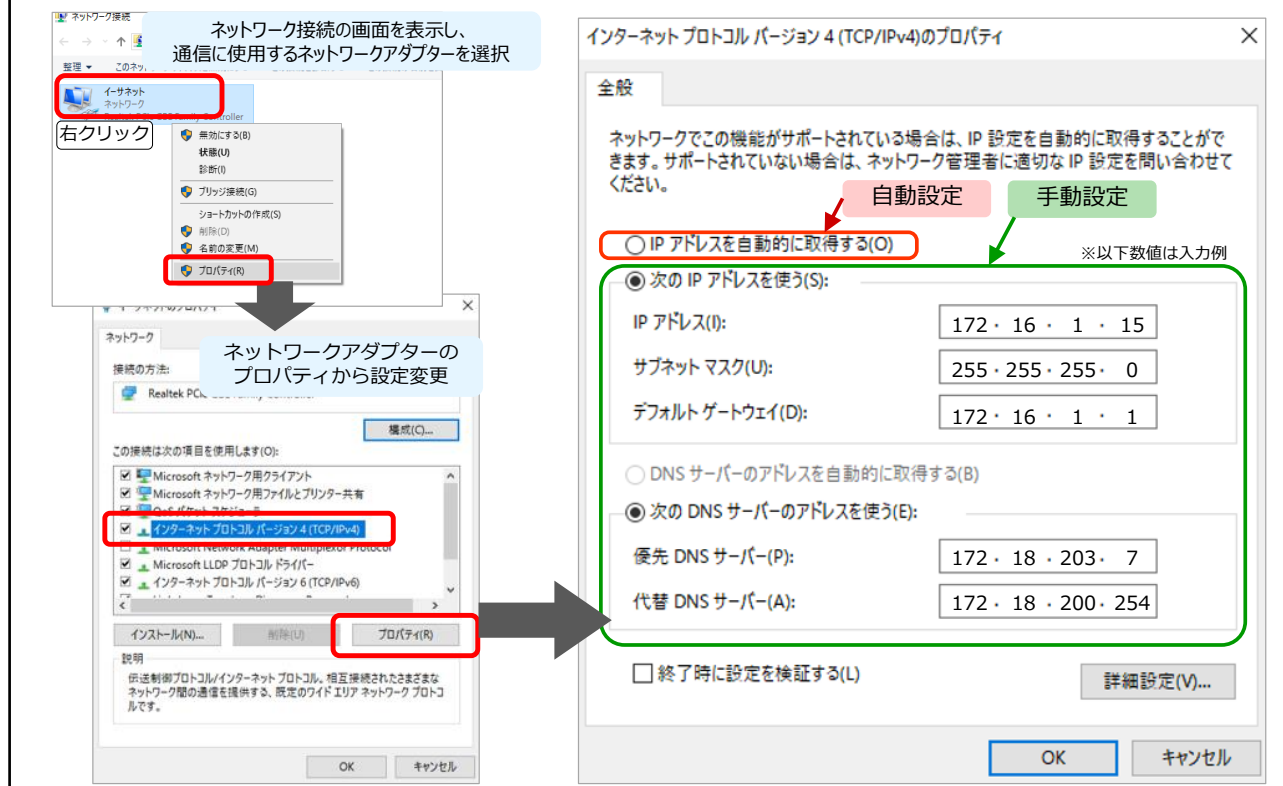
まずアドレスクラスを考えると、IPアドレスの先頭ビットが、「10101100」のため、設問1のIPアドレスはクラスBです。クラスBの場合は、先頭から16bitがネットワーク識別の領域となるため、先頭16bitがアドレスクラスに基づくネットワーク識別の領域です。また、サブネットマスクが「255.255.255.0」のため、先頭24bitと後半8bitの境界線が、ネットワークアドレス領域とホストアドレス領域の区切りと定義されています。

結果として、サブネット識別に3オクテット目の領域が使用されています。

【設問2】

まず、アドレスクラスを考えると、IPアドレスの先頭ビットが、「00001010」のため、設問2のIPアドレスはクラスAです。クラスAの場合は、先頭から8bitがネットワーク識別の領域となるため、先頭8bitがアドレスクラスに基づくネットワーク識別の領域です。また、サブネットマスクが「255.0.0.0」のため、先頭8bitと後半24bitの境界線が、ネットワークアドレス領域とホストアドレス領域の区切りと定義されています。結果として、サブネット識別の領域は定義されていないことになります。

5.5 端末のIPアドレス設定



コンピュータのIPアドレス設定方法について解説します。（Windows OSの場合）

Windows OSでは、ネットワークアダプターのプロパティで設定を変更します。

ネットワークアダプターの設定は、「ネットワーク接続」の画面を表示して操作します。

詳細な手順は、OSのバージョンにより異なるため、Microsoft社のサポート情報などを参照してください。

また、設定を変更するには管理者権限が必要です。変更する際には管理者の指示に従ってください。

端末のIPアドレス設定方法は、2種類あります。

●自動設定

DHCPを利用して、自動的にIPアドレスを割り当てる方法。

（設定画面にて「IPアドレスを自動的に取得する」を選択する）

●手動設定

ネットワーク管理者から設定すべきネットワーク情報を通知してもらい、端末ごとに手動で設定する方法。

（設定画面にて「次のIPアドレスを使う」を選択し、数値を設定する）

※注意

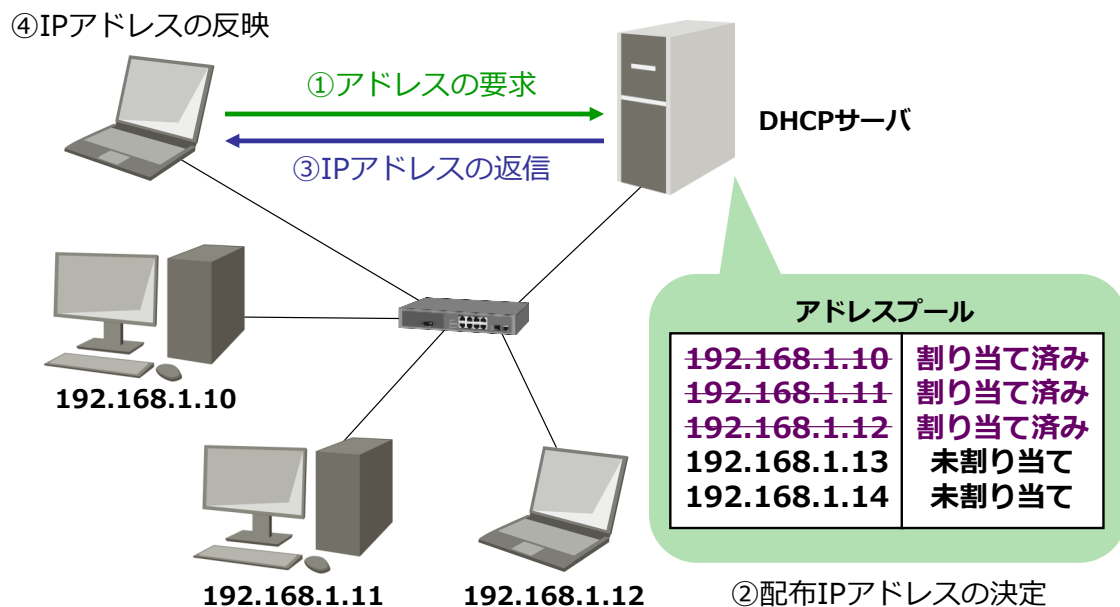
画面上には複数のネットワークアダプターが表示される場合があります。複数のアダプターが選択できる場合には、設定変更するアダプターを間違えないように注意してください。

【参考】（Windows OSの場合）

「ネットワーク接続」画面の呼び出し方法は複数あります。

例）[Windowsロゴ]キーと[R]キーを同時に入力し、「ファイル名を指定して実行」画面で [ncpa.cpl] と入力し[OK]

<参考> DHCPによるIPアドレスの配信



ここでは、DHCPによるIPアドレスの配信について解説します。

コンピュータ側でIPアドレスの自動取得が設定されている場合、ネットワーク内にあるDHCPサーバから端末ごとにIPアドレスが配布されます。

DHCPサーバでは、どのIPアドレスをどの端末に割り当てたかを記録しているため、IPアドレスの重複は発生しません。

また、複数台の端末に対し個別に設定する必要がないため、設定作業が簡素化できます。

<DHCPサーバからのIPアドレスの割り当て>

- ① 端末からDHCPサーバに、「IPアドレスの割り当て要求」が発信される。
- ② DHCPサーバ内のアドレス配布範囲から配布されるIPアドレスが決定される。
- ③ DHCPサーバから端末に「IPアドレス」を返信する。
- ④ 端末がアドレスを受信し、端末へ設定する。

【参考】

DHCPサーバへアドレス返却するコマンド [ipconfig /release]

DHCPサーバへアドレス要求するコマンド [ipconfig /renew]

【参考】リンクローカルアドレス(169.254.0.0/16)

IPアドレスが手動で設定されず、DHCPサーバからの割り当てもない場合、装置自身がIPアドレスを自動で割り当てる機能があります。IPv4では、169.254.0.0/16の範囲が利用され、ホストアドレスはランダムに選出されます。Windowsでは、APIPA (Automatic Private IP Addressing)と表現されます。

<コマンド紹介> ipconfigコマンド

```
> ipconfig /all
```

Windows IP 構成
(中略)

イーサネット アダプター ローカル エリア接続:

```
接続固有の DNS サフィックス . . . . :  
物理アドレス . . . . . : 00-00-0E-AA-BB-CC  
DHCP 有効 . . . . . : いいえ  
自動構成有効 . . . . . : はい  
リンクローカル IPv6 アドレス . . . : fe80::9855:abab:cddc:efef%10 (優先)  
IPv4 アドレス . . . . . : 172.16.1.15 (優先)  
サブネット マスク . . . . . : 255.255.255.0  
デフォルト ゲートウェイ . . . . . : 172.16.1.1  
DHCPv6 IAID . . . . . : 012345678  
DHCPv6 クライアント DUID . . . . . : 00-01-00-01-12-AB-CD-EF-00-12-3...  
DNS サーバー . . . . . : 172.16.200.2  
                        : 172.20.200.2  
  
NetBIOS over TCP/IP . . . . . : 有効  
(以下略)
```

複数のアダプター情報が表示されるため注意する必要がある

※図中の主な項目について

- | | |
|--------------|-----------------------------|
| ・物理アドレス | → MACアドレス (物理インターフェースを識別) |
| ・IPv4アドレス | → IPアドレスが表示 (IPv4とIPv6は後ほど) |
| ・サブネットマスク | → サブネットマスク |
| ・デフォルトゲートウェイ | → デフォルトゲートウェイ |
| ・DNSサーバ | → DNSサーバ (DNSについては後ほど) |

ここでは、ipconfigコマンドを紹介します。

ipconfigコマンドは現在のTCP/IP構成を表示します。このユーティリティを使うと、DHCPサーバにより割り当てられたTCP/IP構成を手動で開放および更新することもできます。オプションを指定せずに実行すると、すべてのアダプターのIPアドレス、サブネットマスク、デフォルトゲートウェイが表示されます。

<構文>

ipconfig

<主なオプション>

/all : すべてのアダプターの完全なTCP/IP構成を表示します。

/renew アダプター : アダプターが指定されていなければすべてのアダプターのDHCP構成を更新します。アダプターが指定されていれば指定されたアダプターのDHCP構成を更新します。

/release アダプター : DHCPRELEASEメッセージをDHCPサーバに送信して、アダプターが指定されていなければすべてのアダプターの、アダプターが指定されていれば指定されたアダプターのDHCP構成を開放し、IPアドレス構成を破棄します。

<使い方>

コマンド結果をテキストファイルとして保存するには、以下のコマンドを入力します。

コマンド > ディレクトリ¥ファイル名

例 : **ipconfig /all > C:¥Users¥FLM¥Desktop¥ipconfig.txt**

(「FLM」ユーザーのデスクトップにipconfig /allの結果をipconfig.txtという名前のテキストファイルで保存する)

<コマンド紹介> pingコマンド

疎通確認に成功する場合、図のような実行結果が表示される

```
> ping 172.16.1.1
```

※疎通確認に失敗した場合は以下が表示される

- ・タイムアウトの場合：「要求がタイムアウトしました。」
- ・到達不可の場合：「宛先ネットワークに到達できません。」

```
172.16.1.1 に ping を送信しています 32 バイトのデータ：
172.16.1.1 からの応答： バイト数 =32 時間 =1ms TTL=255
172.16.1.1 からの応答： バイト数 =32 時間 =1ms TTL=255
172.16.1.1 からの応答： バイト数 =32 時間 =1ms TTL=255
172.16.1.1 からの応答： バイト数 =32 時間 =1ms TTL=255
```

```
172.16.1.1 の ping 統計：
```

```
    パケット数：送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒)：
```

```
    最小 = 1ms、最大 = 9ms、平均 = 3ms
```

ここでは、pingコマンドを紹介します。

pingコマンドは、IP接続の構成を確認し、IP接続をテストします。ネットワーク上の別のコンピュータへのIPレベルの接続を確認します。IPv4かIPv6かはアドレスから自動的に判断します。

<構文>

ping 各オプション 宛て先アドレス(ホスト名)

<主なオプション>

- t** : 連続的に疎通確認を行います。強制終了するには、Ctrlキーを押しながらCキーを押します。
- a** : IPアドレスをホスト名に解決して、疎通確認を行います。
- n 数値** : 入力した数値分(要求の回数)のデータを送信します。
- l 数値** : 入力した数値の容量(単位：バイト)の データを送信します。(容量はpingのヘッダーを除く)

ホスト名 : ホスト名に対して疎通確認を行います。

※疎通確認の失敗例はこちらです。

```
> ping 172.16.1.100
```

```
172.16.1.100 に ping を送信しています 32 バイトのデータ：
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
```

```
172.16.1.100 の ping 統計：
```

```
    パケット数：送信 = 4、受信 = 0、損失 = 4 (100% の損失)、
```

```
> ping 172.17.1.100
```

```
172.17.1.100 に ping を送信しています 32 バイトのデータ：
172.16.1.1 からの応答： 宛先ネットワークに到達できません。
172.16.1.1 からの応答： 宛先ネットワークに到達できません。
172.16.1.1 からの応答： 宛先ネットワークに到達できません。
172.16.1.1 からの応答： 宛先ネットワークに到達できません。
```

```
172.17.1.100 の ping 統計：
```

```
    パケット数：送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
```

<演習問題4> 端末のTCP/IP設定を確認してみよう

■ 演習問題4 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

ipconfig /allコマンドを実行し、端末に設定されているIPアドレスを確認してください。

【実行例】

コマンドプロンプト

```
> ipconfig /all
Windows IP 構成
イーサネット アダプター ローカル エリア接続:
(~~~中略~~~)
物理アドレス.....: 00-00-0E-AA-BB-CC
DHCP 有効.....: いいえ
IPv4 アドレス.....: 172.16.1.15(優先)
サブネットマスク.....: 255.255.255.0
デフォルトゲートウェイ.....: 172.16.1.1
DNS サーバー.....: 172.16.200.2
(~~~以下略~~~)
>
```

※IPアドレス以外の表記に関しては、5章後半で解説します。

【解答例】

ipconfigコマンドを使用し、通信に使用するアダプターのIPv4アドレスの項目を確認する
【参考】"/all"のオプション追加により図は、詳細まで表示している

【参考】疎通確認(pingコマンド)は以下のように実行する
例えば、「ping」の後ろに疎通確認相手のIPアドレス「172.16.1.1」を指定し、実行すると結果が確認できる

コマンドプロンプト

```
> ping 172.16.1.1

172.16.1.1 に ping を送信しています 32 バイトのデータ:
172.16.1.1 からの応答: バイト数 =32 時間 =1ms TTL=255
172.16.1.1 からの応答: バイト数 =32 時間 =1ms TTL=255
172.16.1.1 からの応答: バイト数 =32 時間 =1ms TTL=255
172.16.1.1 からの応答: バイト数 =32 時間 =1ms TTL=255

172.16.1.1 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
    ラウンドトリップの概算時間 (ミリ秒):
        最小 = 1ms、最大 = 9ms、平均 = 3ms
```

※上図は、pingの疎通が成功した例です。失敗例はコマンド紹介ページ 参照。
セキュリティ的な理由からping通信が遮断されている場合もあります。

■ 演習問題4 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

ipconfig /allコマンドを実行し、端末に設定されているIPアドレスを確認してください。

【操作手順】

操作手順は以下のとおりです。

- 手順1. コマンドプロンプトにて“**ipconfig /all**”を実行する
- 手順2. 実行結果として表示されたIPv4アドレスの項目を確認する

【実行例】

実行例は図の下段のとおりです。

【解答例】

図の実行結果から以下のとおりに読み取れます。

端末のIPv4アドレス : 172.16.1.15

※コマンド操作については、Windows OSのコマンド操作方法（本資料P.36）を参照してください。

※ipconfigコマンドとpingコマンドについては、コマンド紹介ページ（本資料P.58,59）を参照してください。

次は、アドレッシングのまとめです。

5.6 アドレッシングのまとめ

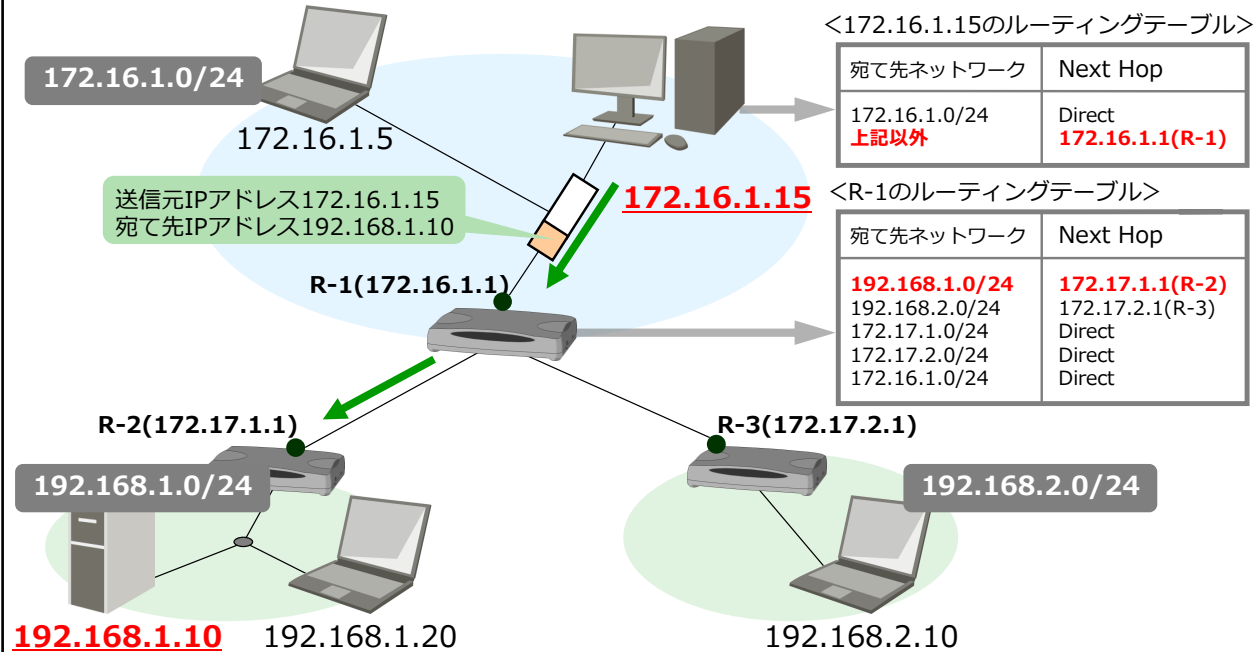
- IPアドレスはネットワーク内の端末を識別するために使用する32ビットの識別子で、表記方法は2進数の「ビット表記」と10進数の「ドット表記」があります。
- IPアドレスの管理方法が、インターネットとイントラネットによって異なります。
 - ✓ インターネット：IPアドレスをグローバルアドレスと呼び、アドレス管理組織によって分担管理される
 - ✓ イントラネット：主にプライベートアドレスを使い、各イントラネットのネットワーク管理者が重複が起きないようにアドレス割り当てルールを作成し、管理する
- 各領域の境界線は、アドレスクラスのクラスA・クラスB・クラスCと、サブネットマスクの仕組みによって定義されます。
- 特別な意味を持つアドレスは、端末に割り振ることができないアドレスです。

アドレッシングのまとめです。

- IPアドレスはネットワーク内の端末を識別するために使用する32ビットの識別子で、表記方法は2進数の「ビット表記」と10進数の「ドット表記」があります。
- IPアドレスの管理方法が、インターネットとイントラネットによって異なります。
 - ✓ インターネット：IPアドレスをグローバルアドレスと呼び、アドレス管理組織によって分担管理される
 - ✓ イントラネット：主にプライベートアドレスを使い、各イントラネットのネットワーク管理者が重複が起きないようにアドレス割り当てルールを作成し、管理する
- 各領域の境界線は、アドレスクラスのクラスA・クラスB・クラスCと、サブネットマスクの仕組みによって定義されます。
- 特別な意味を持つアドレスは、端末に割り振ることができないアドレスです。

5.7 ルーティング
5.7.1 ルーティングとは

宛て先に指定されたネットワークにデータを届けるため、
ルーティングテーブルを使用して転送方向を判断する



ここでは、ルーティングについて解説します。

ルーティングは、送信元から宛て先までの到達可能な経路を判断する機能です。データは自らが進むべき方向を判断できないため、データを中継する装置(端末やルータ)がデータの送信方向を決定します。ルーティングを行うためには、**ルーティングテーブル**が必要です。

ルーティングテーブルとは、「宛て先ネットワーク」と「そのネットワークに到達するための次のルータ(Next Hop)」を登録したリストです。すべてのデータは、パケットに含まれる宛て先IPアドレスとルーティングテーブル内の情報を比較し、転送方向が決定されるため、登録されていないネットワークへはデータを届けることはできません。また、誤ったNext Hopが登録されていると目的のネットワークに到達することができません。ルーティングテーブルには、必要な経路情報が過不足なく、正確に登録されていなければなりません。

次は、ルーティングテーブルへの情報の登録方法であるスタティックルーティングとダイナミックルーティングについて解説します。

5.7.2 スタティックルーティング

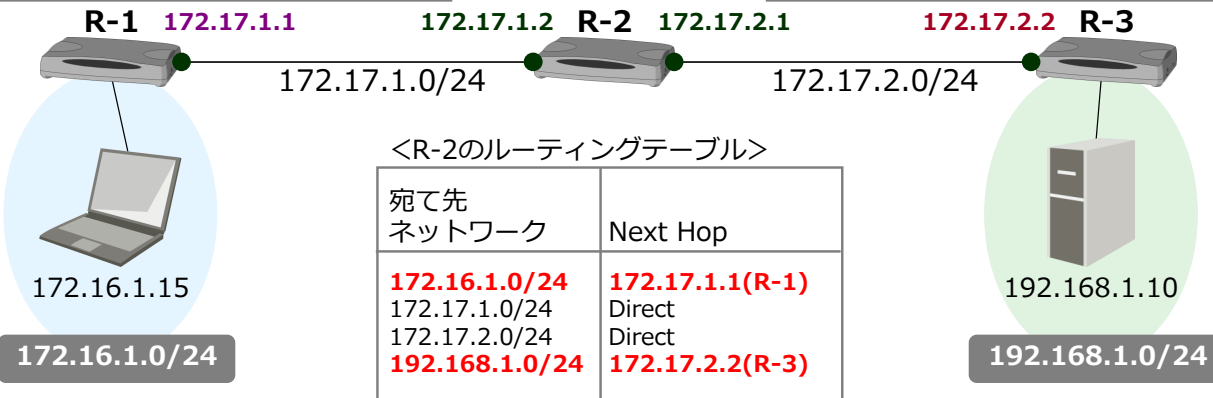
ネットワーク管理者が、
装置にログインし、経路情報を設定する。

<R-1のルーティングテーブル>

宛て先 ネットワーク	Next Hop
172.16.1.0/24	Direct
172.17.1.0/24	Direct
172.17.2.0/24	172.17.1.2(R-2)
192.168.1.0/24	172.17.1.2(R-2)

<R-3のルーティングテーブル>

宛て先 ネットワーク	Next Hop
172.16.1.0/24	172.17.2.1(R-2)
172.17.1.0/24	172.17.2.1(R-2)
172.17.2.0/24	Direct
192.168.1.0/24	Direct



ルーティングテーブルには、装置に直接接続されるネットワーク(Direct)は自動的に登録されます。しかし、他の装置を介して間接的に接続されるネットワークについては、自動的に登録されることはなく、意図的に登録する必要があります。

ルーティングテーブルへの情報の登録方法は、2つあります。**スタティックルーティング**と**ダイナミックルーティング**です。

・スタティックルーティング

スタティックルーティングとは、管理者がルーティングテーブルを設計し、各ホストやルータに手動で情報を登録する方法です。ネットワークやルータに経路情報更新の負荷がかからず、経路情報が固定であるため、処理が安定します。しかし、大規模ネットワークや構成変更が頻繁に発生する環境では、変更に伴う作業が多発し、管理が煩雑になります。

ネットワーク数や構成変更などが比較的少ない、小規模ネットワークに効果的です。

図では、R-1、R-2、R-3のルーティングテーブルを示しています。間接的に接続しているネットワークは、管理者が誤らないよう設定した情報です。

5.7.3 ダイナミックルーティング



画面左下の▶にて、ダイナミックルーティングを確認しましょう。

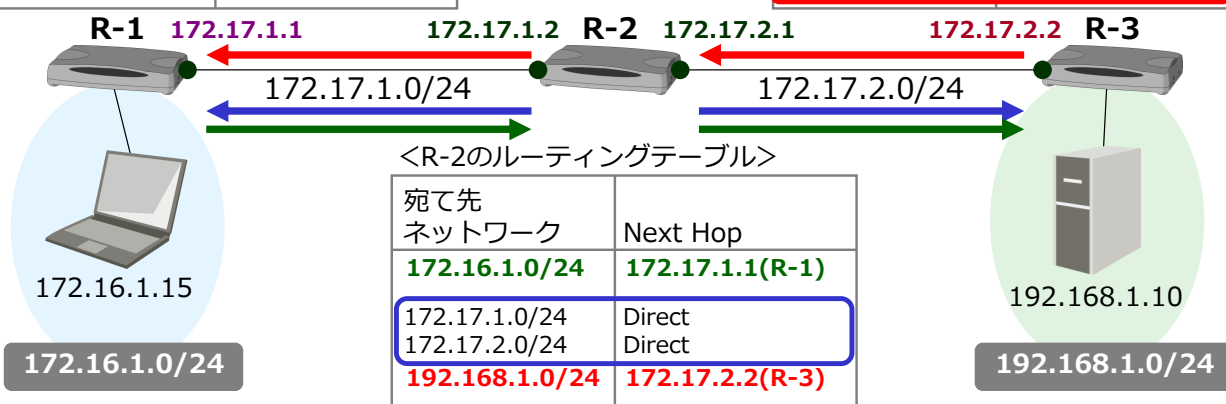
ルータ間で相互に経路情報を交換し、自動的に経路情報の設定がなされる。

<R-1のルーティングテーブル>

宛て先ネットワーク	Next Hop
172.16.1.0/24	Direct
172.17.1.0/24	Direct
172.17.2.0/24	172.17.1.2(R-2)
192.168.1.0/24	172.17.1.2(R-2)

<R-3のルーティングテーブル>

宛て先ネットワーク	Next Hop
172.16.1.0/24	172.17.2.1(R-2)
172.17.1.0/24	172.17.2.1(R-2)
172.17.2.0/24	Direct
192.168.1.0/24	Direct



・ダイナミックルーティング

ダイナミックルーティングは、ネットワークに接続されるルータ同士が**ルーティングプロトコル**を使用し、経路情報を交換する方法です。ルータが動的にルーティングテーブルを更新するため、管理者の設定作業負荷を軽減できます。

図では、R-3から [192.168.1.0/24] の経路情報を他のルータに伝達している様子を示しています。R-2は、R-3から [192.168.1.0/24] の経路情報を受け取り、ルーティングテーブルに登録します。また、R-2はR-1へ [192.168.1.0/24] の経路情報を転送します。

【用語解説】

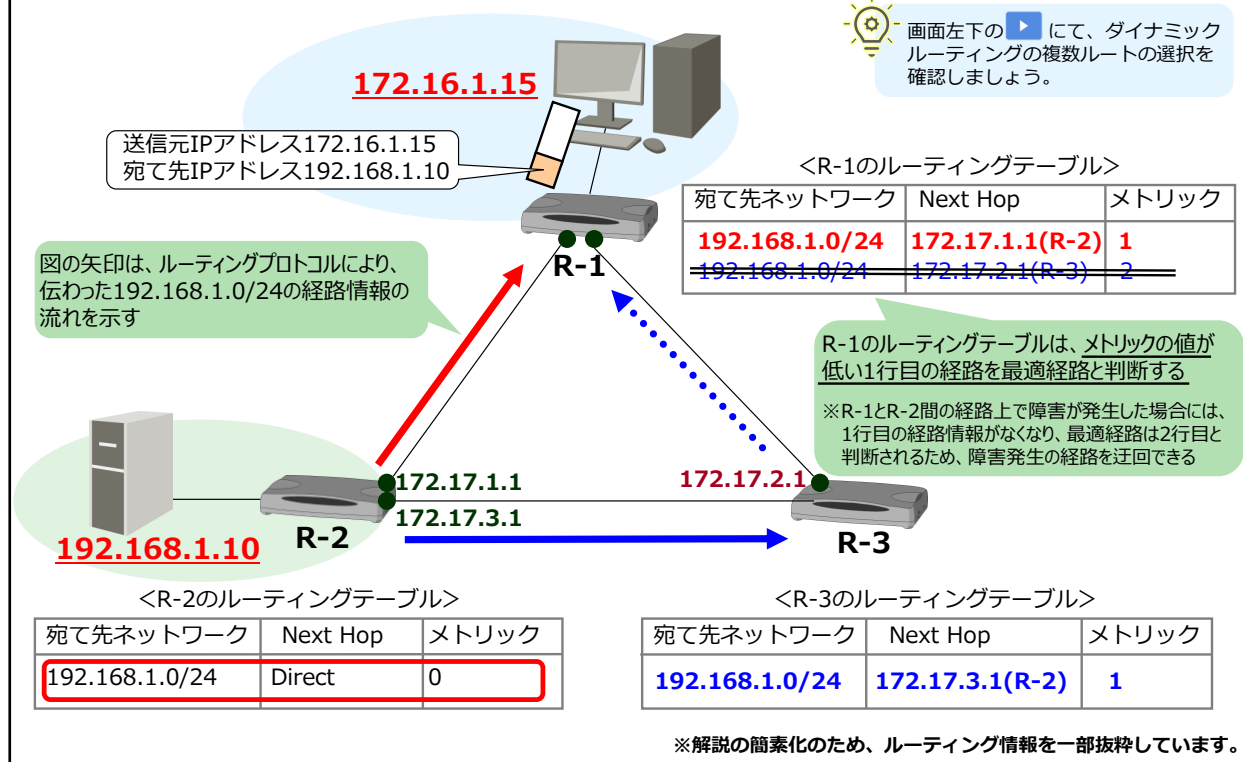
ルーティングプロトコル:

ルータ同士で経路情報を交換する方法を定めたプロトコル。RIPやOSPFなどさまざまな種類があり、ネットワークの規模や要件で選択する。

<参考> ダイナミックルーティングの複数ルートの選択



画面左下の▶にて、ダイナミックルーティングの複数ルートの選択を確認しましょう。



ここでは、ダイナミックルーティングの複数ルートの選択について解説します。

ダイナミックルーティングでは、目的のネットワークへの経路が複数ある場合には、**メトリック**を優先度として最適経路を判断します。また、ネットワーク上で障害が発生すると、自動的に予備経路(冗長経路)へ切り替わり、障害発生時に迅速な復旧が可能です。

図では、R-2から[192.168.1.0/24]の経路情報を他のルータに伝達している様子を示しています。R-1は、R-2およびR-3から[192.168.1.0/24]の経路情報を受け取りますが、メトリック値を比較し、R-2経由の経路情報を優先しています。

(図は、解説を簡素化するためにルーティングテーブル内の経路情報を一部のみを表記しています。)

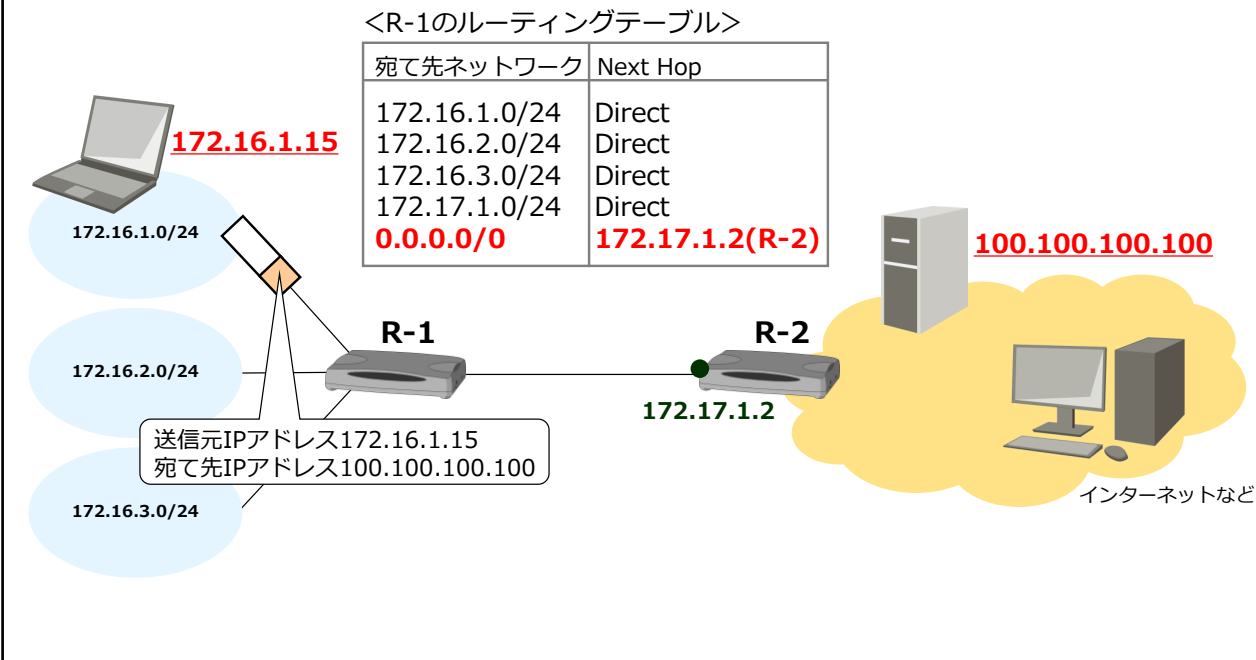
【用語解説】

メトリック:

経路の優先度を示す値。小さい値が優先される。ルータにおいて設定することができる。メトリック値の算出方法は、ルーティングプロトコルにより異なる。

5.7.4 デフォルトルート

明示的に登録されていないネットワークの転送方向を登録する



ここでは、デフォルトルートについて解説します。

ルーティングテーブルに未登録であるネットワークへの通信はできないため、接続される全ネットワークの経路を登録する必要があります。しかし、インターネット上のネットワークなどは膨大な数であるため、把握/管理することは現実的ではありません。

ルーティングテーブルへの情報の登録方法として、明示的に登録されていないネットワークへの経路を定義する手段があります。これを**デフォルトルート**といいます。

主に、インターネットへの経路を登録する方法として利用されます。管理者の登録作業の負荷が軽減されるだけでなく、ルーティングテーブルの情報量が削減できることもメリットです。

次は、デフォルトゲートウェイの設定について解説します。

5.8 端末のデフォルトゲートウェイ設定

インターネット プロトコル バージョン 4 (TCP/IPv4) のプロパティ

全般

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

☐ IP アドレスを自動的に取得する(O)

☒ 次の IP アドレスを使う(S):

IP アドレス(I): 172.16.1.15

サブネット マスク(U): 255.255.255.0

デフォルト ゲートウェイ(D): 172.16.1.1

☐ DNS サーバーのアドレスを自動的に取得する(B)

☒ 次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): 172.18.200.254

代替 DNS サーバー(A): . . .

☐ 終了時に設定を検証する(L)

詳細設定(M)

OK キャンセル

※数値は入力例

172.16.1.15

172.16.1.1

```
> route PRINT
(中略)

IPv4 ルート テーブル

アクティブ ルート:
ネットワーク宛先      ネットマスク      ゲートウェイ      インターフェイス      メトリック
0.0.0.0                0.0.0.0            172.16.1.1        172.16.1.15            291
127.0.0.0              255.0.0.0          リンク上          127.0.0.1              331
127.0.0.1              255.255.255.255    リンク上          127.0.0.1              331
127.255.255.255        255.255.255.255    リンク上          127.0.0.1              331
172.16.1.0             255.255.255.0      リンク上          172.16.1.15            291
172.16.1.15            255.255.255.255    リンク上          172.16.1.15            291
172.16.1.255           255.255.255.255    リンク上          172.16.1.15            291
224.0.0.0              240.0.0.0          リンク上          127.0.0.1              331
224.0.0.0              240.0.0.0          リンク上          172.16.1.15            291
255.255.255.255        255.255.255.255    リンク上          127.0.0.1              331
255.255.255.255        255.255.255.255    リンク上          172.16.1.15            291

固定ルート:
ネットワーク アドレス ネットマスク ゲートウェイ アドレス メトリック
0.0.0.0          0.0.0.0      172.16.1.1 既定
```

(以下略)

コンピュータのルーティング情報の登録方法にデフォルトゲートウェイの登録があります。デフォルトゲートウェイとは、コンピュータが所属しているネットワーク以外の経路を指定する方法です。(意味は、デフォルトルートと同じです。)

コンピュータのデフォルトゲートウェイ設定方法については、「5.5 端末のIPアドレス設定」(本資料P.56)を参照し、上図のプロパティ画面にて設定変更します。

上図のとおり、IPアドレスとサブネットマスクの下にある「デフォルトゲートウェイ」を設定します。

デフォルトゲートウェイを設定すると、ルーティングテーブル内に経路情報が追加され、他のネットワークへの到達性を確保することができます。

端末のルーティングテーブルは、コマンドプロンプトにおいて、「route PRINT」で確認可能です。(デフォルトゲートウェイは、IPv4ルートテーブル上の「ネットワーク宛先」が「0.0.0.0」の行において、ゲートウェイの項目に表示されます。)

【参考】

「route PRINT」の実行結果において、「ゲートウェイ」の列が「リンク上」と表示されている行は、端末と同一ネットワークの経路情報です。

<コマンド紹介> tracertコマンド

```
> tracert 192.168.1.10
```

192.168.1.10 へのルートをトレースしています。
経由するホップ数は最大 30 です

1	12 ms	1 ms	1 ms	172.16.1.1
2	1 ms	1 ms	1 ms	172.17.2.1
3	1 ms	1 ms	1 ms	192.168.1.10

トレースを完了しました。

コマンドで指定したIPアドレスまでの通信経路が調査できる
本図の場合では、以下を経由したことが判明する

・経由1つ目：172.16.1.1

・経由2つ目：172.17.2.1

※最後の行には目的端末との通信結果が表示される

※セキュリティ的に問題なく経路上から応答が届く場合、
表示される

ここでは、tracertコマンドを紹介します。

tracertコマンドは、データが宛て先に到達するまでに経由するルートを追跡します。送信元端末と宛て先端末の間にあるルータのアドレスが一覧表示されます。

<構文>

tracert 各オプション 宛て先アドレス

<主なオプション>

-d IPアドレス : ホスト名とIPアドレスの名前解決をしないように指定します。

ホスト名 : 宛て先ホスト名までの経路を判断します。このとき、ホスト名とIPアドレスの名前解決が行われ、IPアドレスも表示されます。

<演習問題5> 端末からの通信経路を確認してみよう

■ 演習問題5 ■

コマンドプロンプトを起動して、以下の設問に教えてください。

■ 設問 ■

tracertコマンドを実行し、端末からの通信経路を確認してください。

【実行例】

```
コマンドプロンプト
> tracert 192.168.1.10

192.168.1.10 へのルートをトレースしています。
経路するホップ数は最大 30 です

 1    12 ms    1 ms    1 ms    172.16.1.1
 2     1 ms    1 ms    1 ms    172.17.2.1
 3     1 ms    1 ms    1 ms    192.168.1.10

トレースを完了しました。
```

送信元端末に設定されている
デフォルトゲートウェイの値

※セキュリティ的な理由から、IPアドレスが表示されない場合もあります。

■ 演習問題5 ■

コマンドプロンプトを起動して、以下の設問に教えてください。

■ 設問 ■

tracertコマンドを実行し、端末からの通信経路を確認してください。

【操作手順】

操作手順は以下のとおりです。

- 手順1. コマンドプロンプトにて“**tracert**”を実行する
- 手順2. 実行結果として表示されたIPアドレスを確認する

【実行例】

実行例は図の下段のとおりです。

【解答例】

図の実行結果から以下のとおりに読み取れます。

送信元端末から宛先端末（192.168.1.10）まで、以下を経由したことが判明する

- ・ 経由1つ目：172.16.1.1（送信元端末に設定されているデフォルトゲートウェイの値）

※環境によっては設定値と異なる値が表示される場合があります。

- ・ 経由2つ目：172.17.2.1

※セキュリティ的に問題なく経路上から応答が届く場合、IPアドレスが表示される

※コマンド操作については、Windows OSのコマンド操作方法（本資料P.36）を参照してください。

※ tracertコマンドについては、コマンド紹介ページ（本資料P.68）を参照してください。

次は、ルーティングのまとめです。

5.9 ルーティングのまとめ

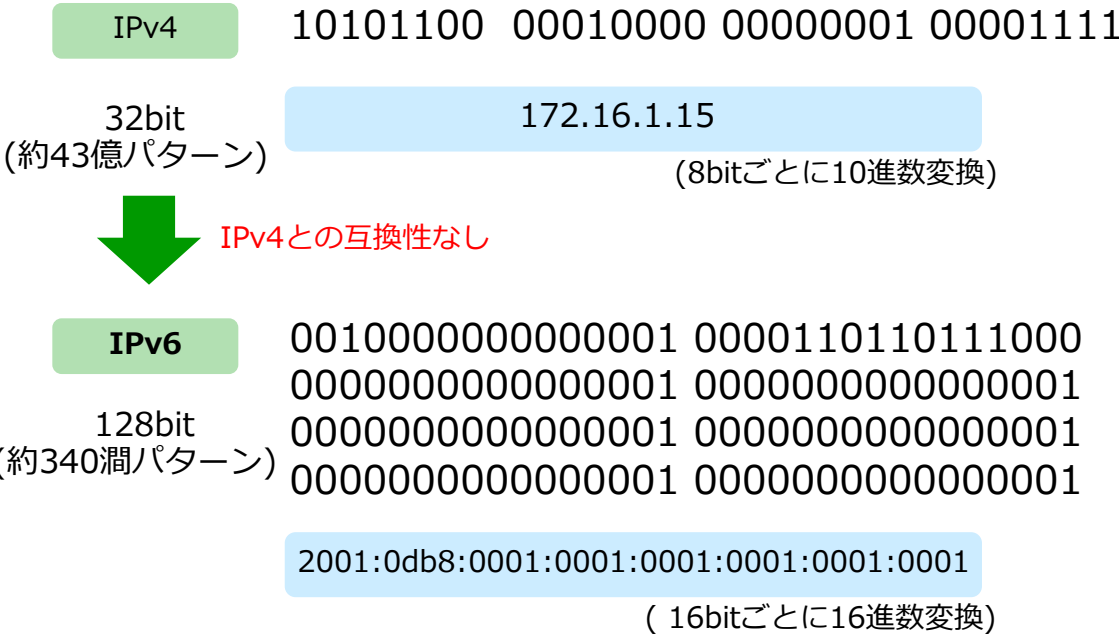
- ルーティングは、宛て先IPアドレスとルーティングテーブルを比較し、どの方向へ転送するか（どのNextHopを中継するか）を判断します。
具体的には、宛て先IPアドレスのネットワーク領域部分と、ルーティングテーブルの宛て先ネットワークを比較し、転送先（NextHop）を決めています。
- すべてのデータはルーティングテーブルの経路情報を基に転送されるため、ルーティングテーブルには経路情報が過不足なく正確に登録されている必要があります。
- ルータに直接接続されるネットワークに配送する場合には、経路情報の登録は不要ですが、間接的に接続されるネットワークに配送する場合には、経路情報の登録が必要です。
- ルーティングテーブルに経路情報を登録する方法は、以下の2つです。
 - ✓ スタティックルーティング : 管理者が手動で登録する方法
 - ✓ ダイナミックルーティング : ルータが経路情報を交換し自動登録する方法
- デフォルトルートは、未知の宛て先に対する経路情報としてルーティングテーブルに登録します。端末にも、未知の宛て先の転送先として、設定する必要があり、デフォルトゲートウェイ（デフォルトルートのNextHop）を登録すれば、端末のルーティングテーブルにデフォルトルートが加わります。

ルーティングのまとめです。

- ルーティングは、宛て先IPアドレスとルーティングテーブルを比較し、どの方向へ転送するか（どのNextHopを中継するか）を判断します。
具体的には、宛て先IPアドレスのネットワーク領域部分と、ルーティングテーブルの宛て先ネットワークを比較し、転送先（NextHop）を決めています。
- すべてのデータはルーティングテーブルの経路情報を基に転送されるため、ルーティングテーブルには経路情報が過不足なく正確に登録されている必要があります。
- ルータに直接接続されるネットワークに配送する場合には、経路情報の登録は不要ですが、間接的に接続されるネットワークに配送する場合には、経路情報の登録が必要です。
- ルーティングテーブルに経路情報を登録する方法は、以下の2つです。
 - ✓ スタティックルーティング : 管理者が手動で登録する方法
 - ✓ ダイナミックルーティング : ルータが経路情報を交換し自動登録する方法
- デフォルトルートは、未知の宛て先に対する経路情報としてルーティングテーブルに登録します。端末にも、未知の宛て先の転送先として、設定する必要があり、デフォルトゲートウェイ（デフォルトルートのNextHop）を登録すれば、端末のルーティングテーブルにデフォルトルートが加わります。

5.10 IPv4のアドレス枯渇

インターネット層の次世代のプロトコル



ここでは、IPv4の後に登場したIPv6について解説します。

IPv6 (IP version 6)は、IPv4 (IP version 4)を全面的に見直し、開発されたプロトコルです。(現在主に利用されているIPのバージョンは4です。)IPv4では、32bitのアドレス長のため、約43億パターンの表現ができます。しかし、ネットワークに接続する端末数は年々増えており、数が不足してきました。そこで、IPv4に変わるプロトコルとして、IPv6が開発されました。

IPv6で使用するIPアドレスは、128bitで表します。

340,282,366,920,938,463,374,607,431,768,211,456 (約340潤)パターンが表現できるため、実質無限大のアドレス空間といえます。この豊富なアドレス空間を実現することにより、将来に向けてネットワークの適用場面や用途が広がります。

IPv4アドレスは、32ビットを8ビットごとに10進数で表現し、“.”(ドット)で区切って表現しました。(例：192.168.0.1) それに対し、IPv6アドレスは、128ビットを16ビットごとに16進数で表現し、“:”(コロン)で区切って表現します。

なお、IPv4とIPv6には互換性がありません。移行作業には注意が必要です。

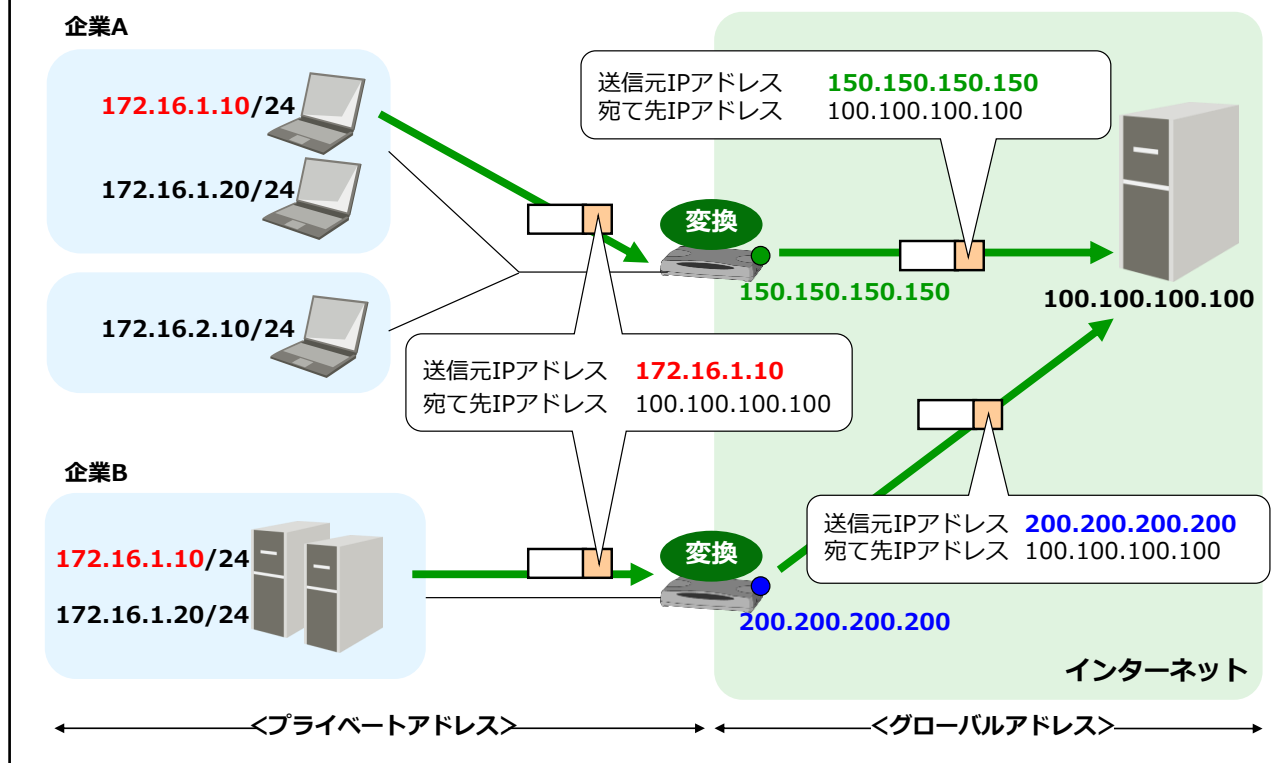
【参考】IPv6のリンクローカルアドレス(fe80::/10)

同一ネットワーク通信のアドレスとして、リンクローカルアドレスを利用します。アドレスの一部をランダムに生成する方式(匿名アドレス)や、MACアドレスを元に生成する方式(EUI-64)があります。

次は、IPv4のアドレス枯渇問題を先延ばしにするために導入されたアドレス変換について解説します。

5.11 アドレス変換

5.11.1 企業ネットワークとインターネット接続



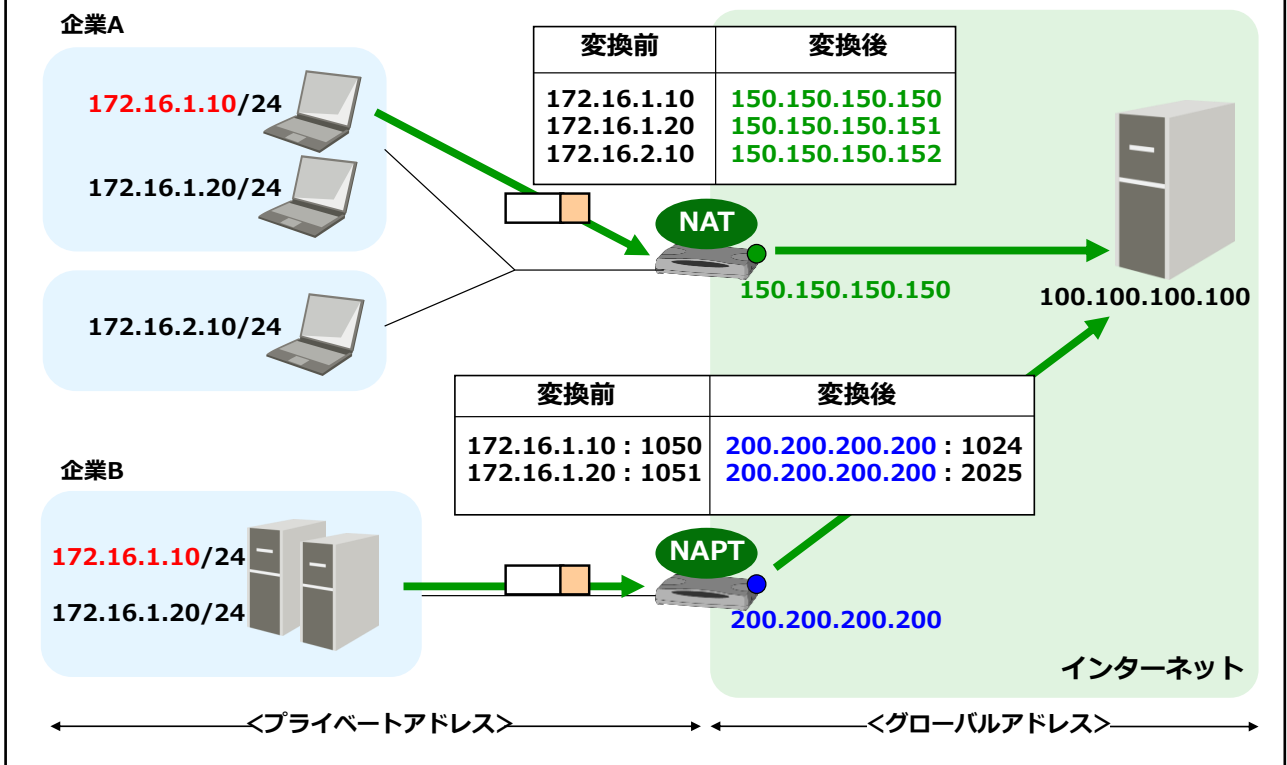
インターネットとイントラネットは、独立したIPアドレス体系と割り当てルールがあり、そのままでは相互接続することはできません。イントラネットからインターネット上の資源(コンピュータやシステム)にアクセスするには、通信で使用するアドレスを変換する必要があります。具体的には、インターネットへの接続点となる装置(ルータやファイアウォール)において、プライベートアドレスからグローバルアドレスへの変換を行います。

イントラネット内においてプライベートアドレスを利用する利点には、以下があります。

- アドレス枯渇への対応
イントラネット内で利用するプライベートアドレスは、組織が異なれば(ネットワークが独立していれば)同じアドレスが利用可能です。(グローバルアドレスのように唯一無二のアドレスではないため、アドレス枯渇に対し対応ができます。)
- イントラネットワークの隠ぺい
アドレス変換を行いインターネットへ接続するため、イントラネットワーク内のアドレス体系やルールを非公開にできます。アドレス体系やルールが第3者に公開されると、インターネット側からの攻撃の対象となることがあります。これを防ぐことが可能です。

次は、アドレス変換の種類としてNAT/NAPTについて解説します。


5.11.2 NAT/NAPT



プライベートアドレスとグローバルアドレスの相互変換を行う技術には、大きく分けて以下の2種類があります。


- NAT (Network Address Translation)
イントラネット内の端末に対し、異なるアドレスを割り当てる技術です。
インターネットへの同時接続端末台数分の変換後アドレス(グローバルアドレス)が必要です。
変換前と変換後のアドレスをあらかじめ登録して、1対1で変換を行う静的NATと、登録した範囲からn対nで変換を行う動的NATがあります。
- NAPT (Network Address Port Translation)
イントラネット内の端末に対し、同一のアドレスを割り当てる技術です。
端末の一意性は、ポート番号を用いることで通信の独立性を実現しています。
変換前と変換後のアドレスとポート番号をあらかじめ登録して、1対1で変換を行う静的NAPTと、登録した範囲からn対1で変換を行う動的NAPTがあります。

5.12 階層と識別子(FQDNとIPアドレス)

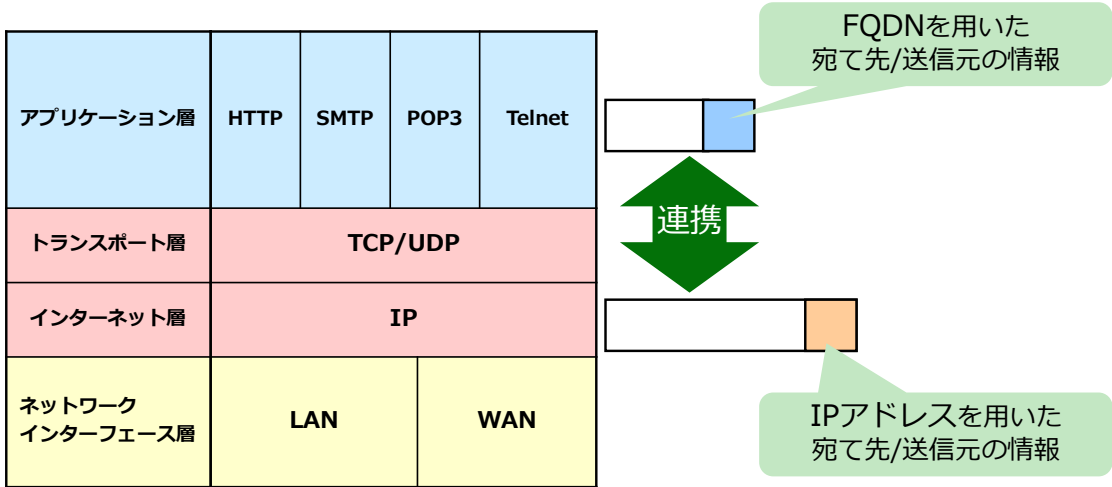


**FQDNとIPアドレスの
対応付けが必要**

www.flm.co.jp



172.16.1.15

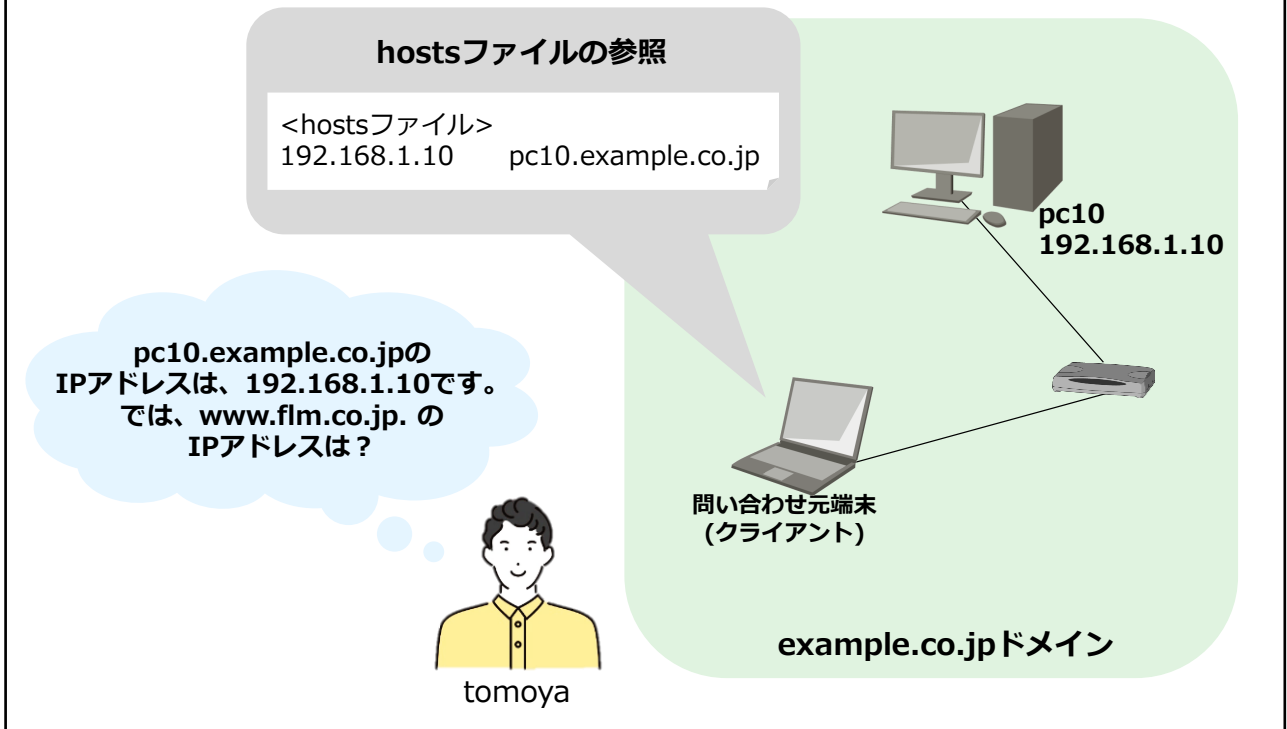


ここでは、FQDN形式の文字列とIPアドレスの対応付け（**名前解決**）について解説します。通信アプリケーションにおいて、宛て先を示すにはFQDN形式の文字列のアドレスを使用しています。ユーザーが直感で分かりやすい点が特徴です。一方、TCP/IPによるデータ通信を制御するには、IPアドレスを用います。

アプリケーションの通信制御機能とTCP/IPの通信制御機能を連携させるために、FQDNで表現されたホスト名・ドメインとIPアドレスを関連付ける必要があります。FQDN形式とIPアドレスの対応付けを解決する仕組みが**名前解決**です。

5.13 名前解決

5.13.1 hostsファイルを使用する名前解決



名前解決には、**hostsファイル**を使用する方法と**DNS (Domain Name System)**を使用する方法があります。

• **hostsファイル**による名前解決

hostsファイルは、各端末のOSに備わっているテキストファイルです。

FQDNとIPアドレスの対応付けをあらかじめhostsファイルに記載しておきます。

(Windows OSでは、C:¥WINDOWS¥system32¥drivers¥etcフォルダ内などシステムフォルダ内に格納されているため 編集するにはWindows OSの管理者権限が必要です。一般的にはセキュリティの観点から編集しません。)

<問い合わせ元端末の名前解決の流れ>

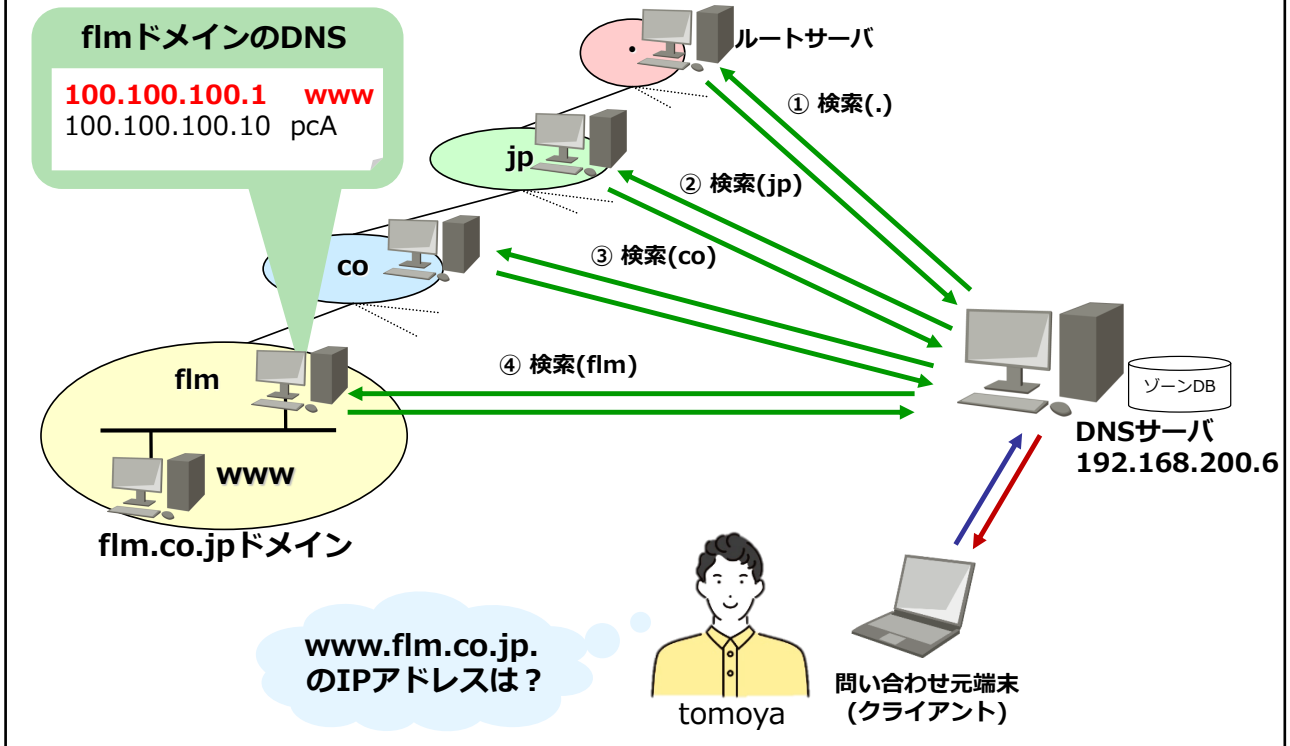
- 1.FQDNで宛て先が指定された通信が発生。
- 2.発信端末内のhostsファイルを参照する。

ファイルに記載されている端末の名前解決が可能です。

- 3.DNSサーバへ問い合わせる。

hostsファイルに情報が登録されていない場合は、DNSサーバへ問い合わせを行います。
(DNSサーバの事前登録が必要です。)

5.13.2 DNSサーバを使用する名前解決



DNSでは名前解決にDNSサーバを使用します。

• DNSによる名前解決

DNSを使用した名前解決は、サーバでFQDNとIPアドレスの対応付けを行う方法です。所属ドメイン内のホスト名とIPアドレスの対応付けを集中管理しています。

<DNSサーバの名前解決の流れ>

1. 問い合わせ元端末(クライアント)から名前解決の要求を受信する。
2. DNSサーバにて、名前解決を試みる。

DNSサーバが所属しているドメイン内にある端末の、名前解決に必要な情報が登録されています。しかし、異なるドメインにある端末の名前解決に必要な情報は保持していないため、他のDNSサーバへ問い合わせを行います。

3. 他のDNSサーバにて、名前解決を試みる。

解決したいFQDN名の上位ドメインから検索を行います。名前解決したい端末が所属しているドメインのDNSサーバにて名前解決できます。

- ① ルートサーバ：ルートドメイン内の端末の名前解決が行えます。ルートドメイン以外に所属している端末の名前解決は行えないため、その場合には、下位ドメインのDNSサーバのIPアドレスを通知します。
- ② 下位ドメインのDNSサーバ：そのDNSサーバが所属しているドメイン内の端末の名前解決が行えます。他のドメインに所属している端末の名前解決は行えないため、その場合には、さらに下位ドメインのDNSサーバのIPアドレスを通知します。
- ③ ②を繰り返し、解決したい端末が所属するドメインへ到達し、名前解決を実行します。

4. DNSサーバが問い合わせ元端末(クライアント)へ解決情報を送信する。

【用語解説】

ルートサーバ:

世界に13系統存在しているルートドメインのDNSサーバ。各ドメインのDNSサーバにあらかじめ登録されている。

5.14 端末のDNSサーバ設定

インターネット プロトコル バージョン 4 (TCP/IPv4) のプロパティ

全般

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

☐ IP アドレスを自動的に取得する(O)

☒ 次の IP アドレスを使う(S):

IP アドレス(I):

サブネット マスク(U):

デフォルト ゲートウェイ(D):

☐ DNS サーバーのアドレスを自動的に取得する(B)

☒ 次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P):

代替 DNS サーバー(A):

☐ 終了時に設定を検証する(L)

詳細設定(V)...

OK キャンセル

※数値は入力例

```
> ipconfig /all

Windows IP 構成
(略)

イーサネット アダプター イーサネット:

    接続固有の DNS サフィックス . . . . . :
    物理アドレス. . . . . : 00-00-0E-AA-BB-CC
    DHCP 有効. . . . . : いいえ
    自動構成有効. . . . . : はい
    リンクローカル IPv6 アドレス. . . . . : fe80::9855:e4a2:897b:
    IPv4 アドレス. . . . . : 172.16.1.15(優先)
    サブネット マスク. . . . . : 255.255.255.0
    デフォルト ゲートウェイ. . . . . : 172.16.1.1
    DHCPv6 IAID. . . . . :
    DHCPv6 クライアント DUID. . . . . :
    DNS サーバー. . . . . : 172.18.203.7
    172.18.200.254
    NetBIOS over TCP/IP. . . . . : 有効

(以下略)
```

ここでは、コンピュータのDNSサーバ設定について解説します。

コンピュータのDNSサーバ設定方法については、「5.5 端末のIPアドレス設定」（本資料P.56）を参照し、上図のプロパティ画面にて設定変更します。

プロパティ画面の下段にある「優先 DNSサーバー」を設定します。
(設定する値は、ネットワーク管理者から通知してもらいます。)

【参考】

組織内では、DNSサーバは2台以上で構成することが推奨されているため、「代替 DNSサーバー」の設定が行われることもあります。

<コマンド紹介> nslookupコマンド

```
> nslookup server1.flm.local ns1.flm.local
```

サーバー: ns1.flm.local

Address: 172.20.100.2

上段には使用した
DNSサーバアドレスが
表示される

権限のない回答:

名前: server1.flm.local

Address: 172.18.100.1

本コマンドにて、指定したDNSサーバに
名前解決した結果が表示される

※図の場合、DNSサーバ: ns1.flm.localを指定して、
server1.flm.localの名前解決を行っている

下段の実行結果から以下が読み取れる

・名前: server1.flm.local の名前解決を行い、
IPアドレス: 172.18.100.1が解決された



【参考】

実行環境に応じて、「権限のない回答」の
表示や、名前解決結果自体表示されない
場合もあります。

ここでは、nslookupコマンドを紹介します。

nslookupコマンドは、DNSクライアントの名前解決機能を手動実行します。ホスト名の後ろにDNSサーバ名を入力することで、問い合わせを行うDNSサーバを指定することもできます。オプションを指定せずに実行すると、コンピュータに設定されたDNSサーバに対し、入力されたホスト名(コンピュータ名、FQDN表記による文字列)の名前解決を行います。

<構文>

nslookup 各オプション ホスト名 (DNSサーバ)

<主なオプション>

なし : 指定されたホスト名の名前解決を行います。DNSサーバが指定されている場合には、指定されているDNSサーバに名前解決を行います。
ホスト名が未入力の場合には、対話モードにて動作します。

-type=タイプ : 名前解決するタイプを指定して名前解決を行い結果を表示します。

タイプ例) a=ホスト名のIPv4アドレス(Aレコード)

aaaa=ホスト名のIPv6アドレス(AAAAレコード)

mx=指定されたドメイン名のメールサーバのIPアドレス(MXレコード)

<演習問題6> 名前解決を確認してみよう

■ 演習問題4 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

FQDNで示された「www.knowledgewing.com」のホスト名・ドメイン名を名前解決してみましょう。
名前解決に使用したDNSサーバのIPアドレスや、名前解決結果を確認してください。
(環境によっては名前解決の結果が表示されない場合もあります。)

【実行例】

```
コマンドプロンプト
> nslookup www.knowledgewing.com

サーバー: ns1.flm.local
Address: 172.20.100.2

権限のない回答:
名前: www.knowledgewing.com
Address: 210.148.44.8

>
```

【解答例】

図の実行結果から以下が確認できる

- ・DNSサーバのIPアドレス：172.20.100.2
- ・「www.knowledgewing.com」の名前解決結果：210.148.44.8



名前解決に失敗しても、DNSサーバを使おうとする点を確認してください。端末に設定済みのDNSサーバを使用して、名前解決を試みている点がポイントです。
(「ipconfig /all」のコマンドでDNSサーバのアドレスを確認できます)

※本実行例は、名前解決に成功した場合です。DNSサーバのアドレスしか判明しない場合もあります。
※図はあくまでも実行例です。問題文のFQDNのサーバと必ずしも同じではないと考えてください。

■ 演習問題6 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

FQDNで示された「www.knowledgewing.com」のホスト名・ドメイン名を名前解決してみましょう。
名前解決に使用したDNSサーバのIPアドレスや、名前解決結果を確認してください。
(環境によっては名前解決の結果が表示されない場合もあります。)

【操作手順】

操作手順は以下のとおりです。

- 手順1. コマンドプロンプトにて“**nslookup www.knowledgewing.com**”を実行する
- 手順2. 実行結果として表示されたDNSサーバのIPアドレスと、名前解決結果を確認する

【実行例】

実行例は図の下段のとおりです。

【解答例】

図の実行結果から以下が確認できます。

- ・DNSサーバのIPアドレス：172.20.100.2
- ・「www.knowledgewing.com」の名前解決結果：210.148.44.8

※名前解決に失敗しても、DNSサーバを使おうとする点を確認してください。

※端末に設定済みのDNSサーバを使用して、名前解決を試みている点がポイントです。

※コマンド操作については、[Windows OSのコマンド操作方法](#)（本資料P.36）を参照してください。

※[nslookupコマンド](#)については、[コマンド紹介ページ](#)（本資料P.78）を参照してください。

次は、本章のまとめです。

5.15 章のまとめ

- IPはTCP/IPの重要なプロトコルの一つです。主な役割は送信元から宛て先までデータを配送することです。トランスポート層とネットワークインターフェース層の間にある、インターネット層のプロトコルです。
- IPは以下の2つの仕組みによってデータを配送します。
 - ✓ アドレッシング : IPアドレスにより、ネットワーク内の端末を識別する
 - ✓ ルーティング : 宛て先IPアドレスとルーティングテーブルを比較し、どの方向へ転送するか（どのNextHopを中継するか）を判断する
- イントラネットとインターネットの境界点の装置において、プライベートアドレスとグローバルアドレスの対応付け（アドレス変換）を行い、各ネットワークの相互通信を行っています。アドレス変換を行う技術には、大きく分けて「NAT」と「NAPT」があります。
- IPアドレスとFQDNを用いた宛て先の対応付けを名前解決と呼び、端末では、以下の方法で名前解決します。
 - ✓ 端末内のhostsファイルを利用した名前解決
 - ✓ 端末に設定されているDNSサーバを利用した名前解決

第5章のまとめです。

- IPはTCP/IPの重要なプロトコルの一つです。主な役割は送信元から宛て先までデータを配送することです。トランスポート層とネットワークインターフェース層の間にある、インターネット層のプロトコルです。
- IPは以下の2つの仕組みによってデータを配送します。
 - ✓ アドレッシング :
IPアドレスにより、ネットワーク内の端末を識別する
 - ✓ ルーティング :
宛て先IPアドレスとルーティングテーブルを比較し、どの方向へ転送するか（どのNextHopを中継するか）を判断する
- イントラネットとインターネットの境界点の装置において、プライベートアドレスとグローバルアドレスの対応付け（アドレス変換）を行い、各ネットワークの相互通信を行っています。アドレス変換を行う技術には、大きく分けて「NAT」と「NAPT」があります。
- IPアドレスとFQDNを用いた宛て先の対応付けを名前解決と呼び、端末では、以下の方法で名前解決します。
 - ✓ 端末内のhostsファイルを利用した名前解決
 - ✓ 端末に設定されているDNSサーバを利用した名前解決

第6章

イーサネット (ネットワークインターフェース層)

学習目標

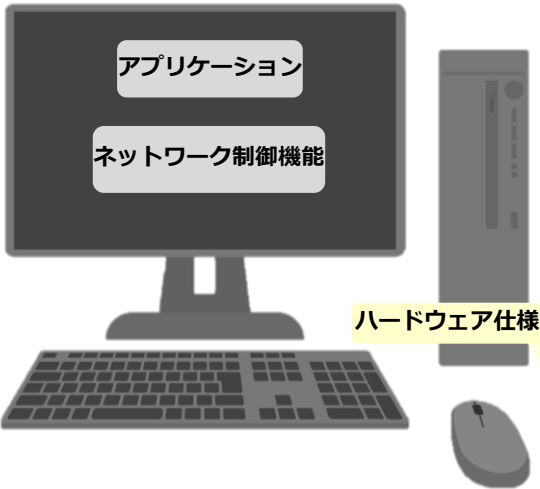
この章では、TCP/IPのネットワークインターフェース層について学習します。

- イーサネット、MACアドレス、ARPなどの用語について理解する。
- 通信用ハードウェア間の通信の仕組みを理解する。

6.1 ネットワークインターフェース層

通信用ハードウェア間でデータを受け渡す

コンピュータシステム



TCP/IPプロトコル階層

アプリケーション層	HTTP	SMTP	POP3	Telnet
トランスポート層	TCP/UDP			
インターネット層	IP			
ネットワーク インターフェース層	LAN (Ethernetなど)		WAN (PPP、フレームリレーなど)	

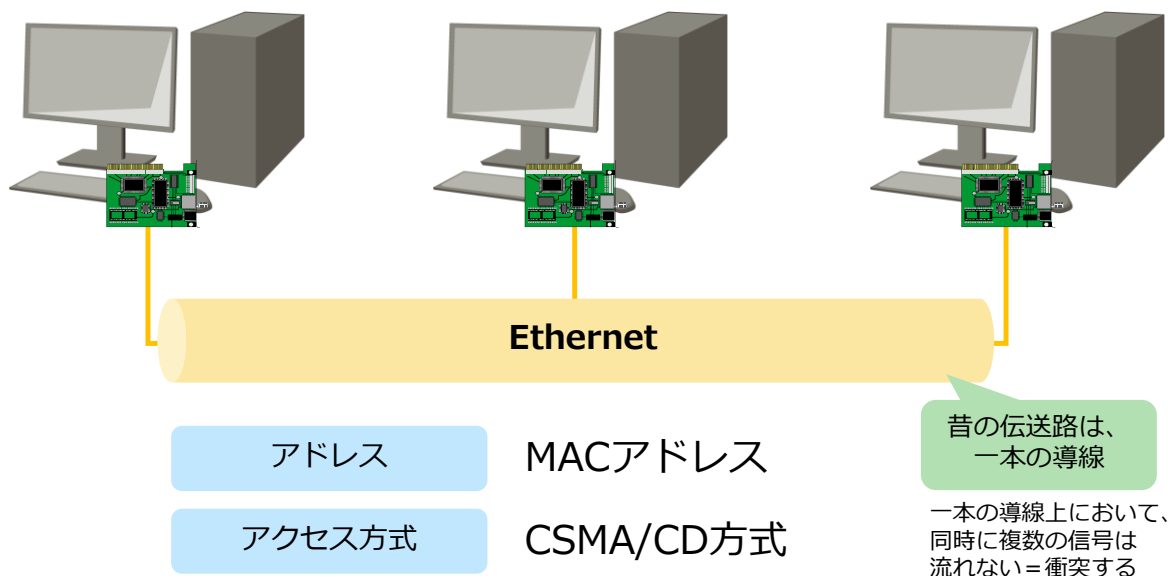
TCP/IPのネットワークインターフェース層では、通信用ハードウェアが位置づけられます。通信用ハードウェアは、LANやWANで採用されるさまざまな製品規格があります。この層では、伝送路で接続された通信用ハードウェアを識別しデータの送受信を制御します。

なお、企業ネットワークは、主にEthernet製品規格が採用されています。

6.2 イーサネット

6.2.1 イーサネットとは

LANで使用するネットワーク製品規格



ここでは、イーサネット (Ethernet)について解説します。

イーサネット (Ethernet)は、伝送路の規格や制御ルールを定めています。イーサネットは、LANで最も使用されているネットワーク製品の規格です。

イーサネットは、DEC、Intel、Xeroxの3社で共同開発され、これを基準に国際標準規格 (ISO8802-3/IEEE802.3)が制定され、世界中に広まりました。

イーサネットでは、伝送路上の通信用ハードウェア (ネットワークアダプタ) を識別するために、**MACアドレス**を使用します。また、伝送路上のデータが衝突しないように制御する方法(アクセス方式)に、**CSMA/CD方式(Carrier Sense Multiple Access with Collision Detection)**を活用しています。

【参考】

イーサネット以外のLANの製品規格として、トークンリングやFDDIなどがありましたが、現在ではあまり使用されていません。

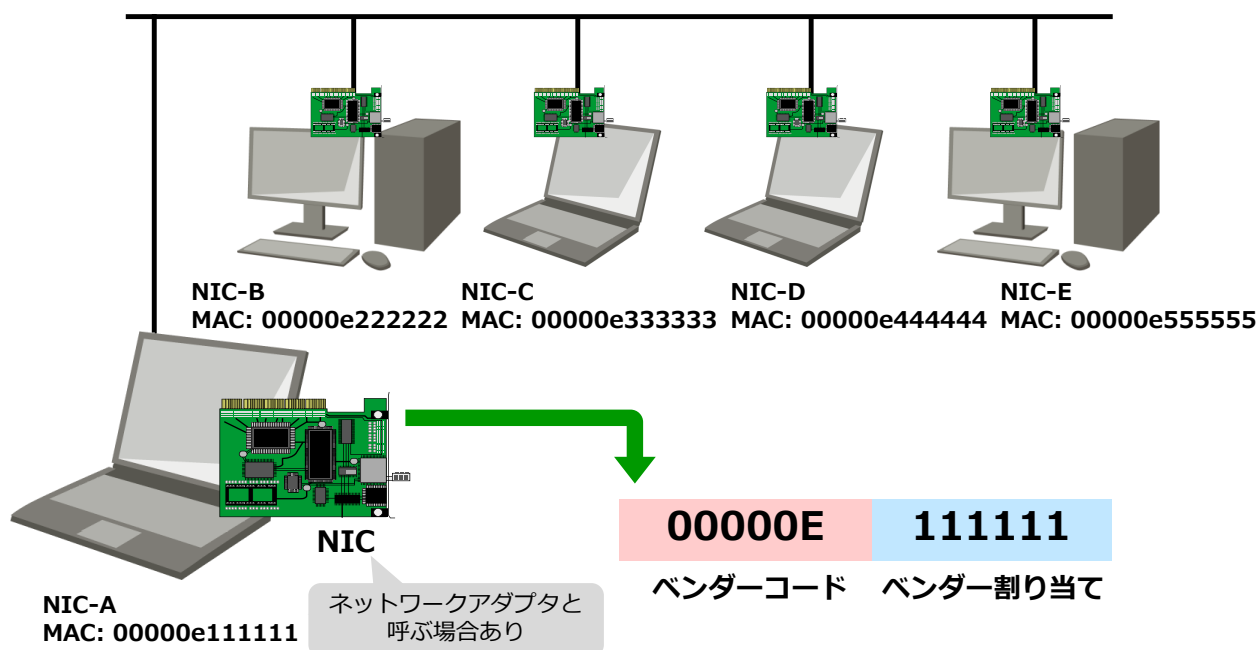
【用語解説】

アクセス方式：

伝送路内で、スムーズなデータの伝送を実現するための通信方式です。衝突の回避や再送制御が定義されており、製品規格が異なると、アクセス方式も異なります。(トークンリング、FDDIでは、トークンパッシング方式が採用されています。)

6.2.2 MACアドレス

イーサネットで使用される、ネットワークアダプタを識別するアドレス



ここでは、MACアドレスについて解説します。

イーサネットで利用される識別子は、**MACアドレス**です。伝送路は分岐し、複数の端末や装置を接続しているため、特定の端末や装置に対してデータを伝送する場合に宛て先の指定が必要となります。MACアドレスは、伝送路の始点または終点となるネットワークアダプタ(NIC)に設定されます。

MAC アドレスは、48bitで構成されており、前半24bitにはベンダーコードが記されています。この部分はNICを製造するベンダー固有のアドレスであり、IEEEが割り当てや管理を行っています。後半24bitは、ベンダーが個別に管理している部分で、NICごとに重複のない固有のアドレスが設定されています。基本的には、NICの出荷時に付加され、後から変更することはできません。

【用語解説】

NIC (Network Interface Card):

コンピュータや装置をLANに接続するための拡張部品(ハードウェア)のことです。

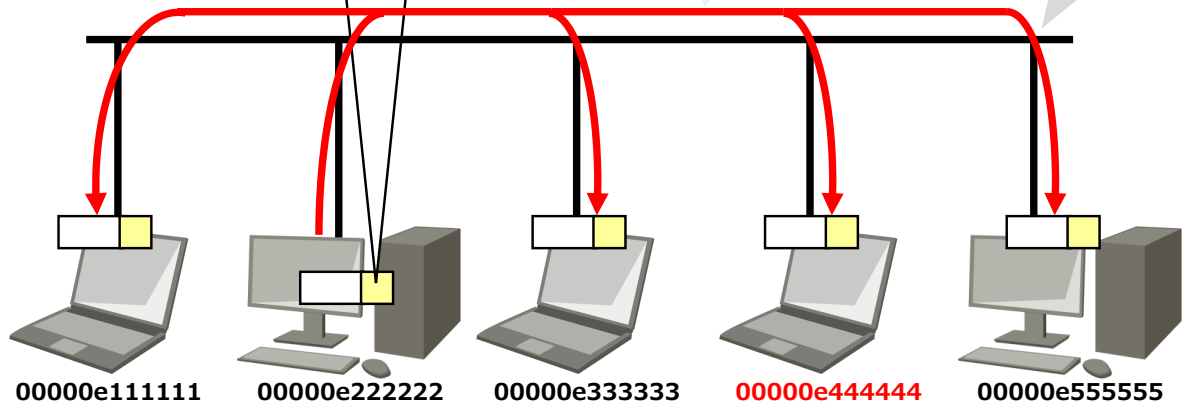
6.2.3 CSMA/CD方式

衝突を回避するアクセス方式としてCSMA/CD方式を採用

送信元MACアドレス 00000e222222
宛て先MACアドレス **00000e444444**

2. 伝送路にデータが流れる

一本の導線の場合、
衝突の可能性あり



1. 伝送路に他のデータが
流れていないことを確認し、
送信する

3. 流れてきたデータの
宛て先アドレスを確認し、
自身宛てであれば、受信する

自身宛てでなければ、
データを破棄する

ここでは、CSMA/CD方式 について解説します。

CSMA/CD方式 (Carrier Sense Multiple Access with Collision Detection)は、伝送路上でデータが衝突を起こさないよう制御する仕組みです。データが衝突すると再送しなければならず、通信効率が悪化するため、これを防ぎます。

<CSMA/CD方式>

1. データの送信に先立ち、端末は伝送路上に他のデータが流れていないことを確認します。他のデータが流れていれば、伝送路が空くまで送信を開始できません。
2. データを伝送路に送信します。
3. 各端末では、到達したデータの宛て先アドレスを参照し、自身宛てであれば受信します。自身宛てでなければ、そのデータを破棄します。

※同時に伝送路の空きを確認し、同時に伝送路へデータを送信した場合には、データが衝突する可能性があります。CSMA/CDでは、データの衝突が検出されると、通信が初期化され再送信される仕組みがあります。

次は、イーサネットの規格について解説します。

6.2.4 イーサネットの規格

呼称	規格名	伝送速度	ケーブルの種類
Ethernet	10BASE5	10Mbps	同軸ケーブル (Thickケーブル)
	10BASE2		軽量同軸ケーブル (Thinケーブル)
	10BASE-T		ツイストペアケーブル
Fast Ethernet	100BASE-TX	100Mbps	
	100BASE-FX		光ファイバーケーブル
Gigabit Ethernet	1000BASE-LX	1Gbps (=1000Mbps)	
	1000BASE-SX		
	1000BASE-T		
10 Gigabit Ethernet (10GbE、10GigE)	10GBASE-T	10Gbps (=10000Mbps)	光ファイバーケーブル
	10GBASE-SR		
	10GBASE-LR		

イーサネットには、伝送速度や使用するケーブルにより異なる規格が定義されています。
規格名の先頭の数字 (10/100/1000)が伝送速度 (単位: Mbps)を、末尾のアルファベットは伝送媒体を表しています。

- 例)100BASE-TX
100Mbpsの伝送速度を持つ規格。ツイストペアケーブルを使用する。
- 1000BASE-SX
1Gbpsの伝送速度を持つ規格。光ファイバーケーブルを使用する。
- 10GBASE-T
10Gbpsの伝送速度を持つ規格。ツイストペアケーブルを使用する。

最大通信速度に着目し、最大伝送速度が10Mbpsのイーサネットを「**Ethernet**」、最大伝送速度が100Mbpsのイーサネットを「**Fast Ethernet**」、最大伝送速度が1Gbpsのイーサネットを「**Gigabit Ethernet**」、最大伝送速度が10Gbpsのイーサネットを「**10 Gigabit Ethernet**」と表現することがあります。

<演習問題7> MACアドレスを確認してみよう

■ 演習問題5 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

MACアドレスを確認してみましょう。

ipconfig /allコマンドを実行し、MACアドレスを確認してください。

※通信に使用しているアダプターの物理アドレスの項目を確認してください。

【実行例】

```
コマンドプロンプト
> ipconfig /all
Windows IP 構成
イーサネット アダプター ローカル エリア接続:
(~~~中略~~~)
物理アドレス.....: 00-00-0E-AA-BB-CC
DHCP 有効.....: いいえ
IPv4 アドレス.....: 172.16.1.15(優先)
サブネット マスク.....: 255.255.255.0
デフォルト ゲートウェイ.....: 172.16.1.1
DNS サーバー.....: 172.16.200.2
(~~~以下略~~~)
>
```

【設問】（解答例）

“ipconfig /all”コマンドを実行し、通信に使用するアダプターの物理アドレスの項目を確認できる
物理アドレス.....: 00-00-0E-AA-BB-CC

実行結果から、
MACアドレスは「00-00-0E-AA-BB-CC」と読み取れる



ipconfigコマンドに、“/all”のオプションを指定することで端末のTCP/IP設定を詳細まで表示しています。

※実際には図とは異なる結果が表示されると考えてください。

■ 演習問題7 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

MACアドレスを確認してみましょう。

ipconfig /allコマンドを実行し、MACアドレスを確認してください。

※通信に使用しているアダプターの物理アドレスの項目を確認してください。

【操作手順】

操作手順は以下のとおりです。

手順1. コマンドプロンプトにて“**ipconfig /all**”を実行する

手順2. 実行結果として表示されたMACアドレスを確認する

【実行例】

実行例は図の下段のとおりです。

【解答例】

解答例は図のとおりです。

実行結果から、MACアドレスは「00-00-0E-AA-BB-CC」と読み取れます。

※MACアドレスの表記はOSによって異なります。大文字と小文字のどちらの表記でも同じMACアドレスです。

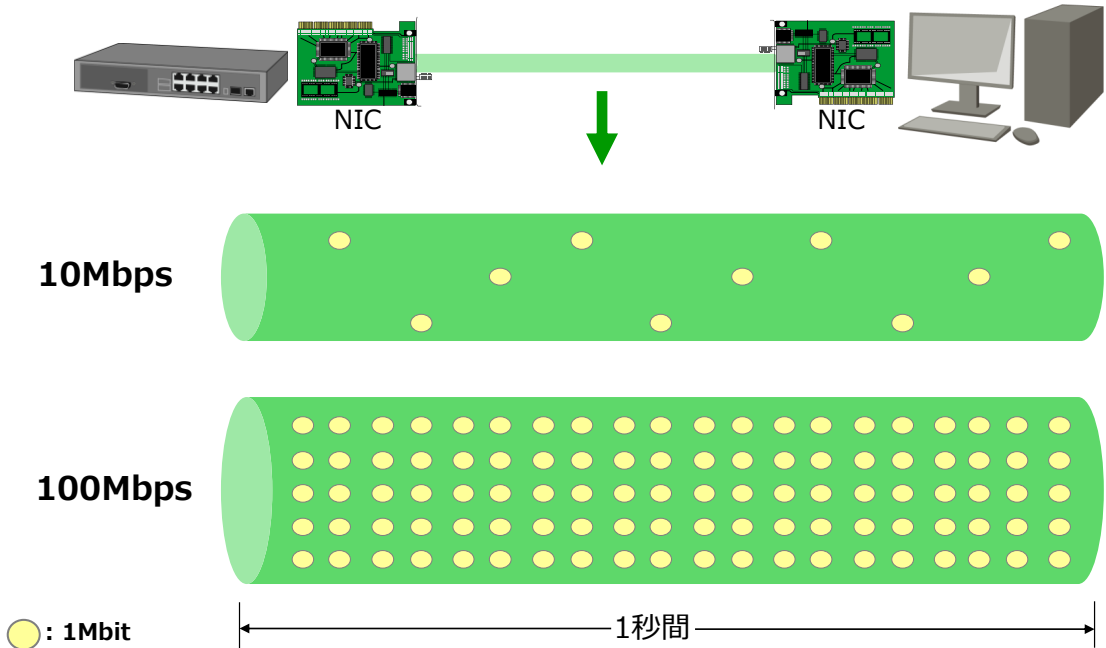
※コマンド操作については、[Windows OSのコマンド操作方法](#)（本資料P.36）を参照してください。

※[ipconfigコマンド](#)については、[コマンド紹介ページ](#)（本資料P.58）を参照してください。

次は、環境によって異なる情報の中から、伝送速度を解説します。

6.3 伝送速度と帯域幅

一定時間に伝送できるデータ量で表現する



通信の速さは、**伝送速度**で表現します。伝送速度により、伝送路(ケーブル)やNICの性能を表現することが可能です。

伝送速度は「1秒間に何bit伝送できるか」を表します。単位は、**bps (bit per second)**です。現在、LAN内では、100Mbps～1Gbpsが主流です。

1秒間に伝送できるデータ量を幅としてとらえ、その幅が「広い」または「狭い」で伝送速度を表現することがあります。これを**帯域幅(帯域)**といいます。

【参考】

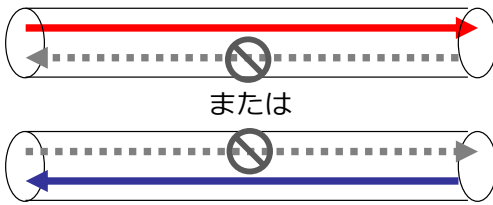
- 1000bps = 1K (キロ)bps
- 1000kbps = 1M (メガ)bps
- 1000Mbps = 1G (ギガ)bps

次は、ネットワークの通信方式と接続形態について解説します。

6.4 通信方式と接続形態

半二重通信

同時に両方向通信はできない



全二重通信

同時に両方向通信可能

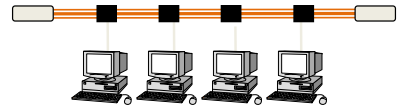


現在の伝送路は、
ケーブル内に導線が
複数存在する

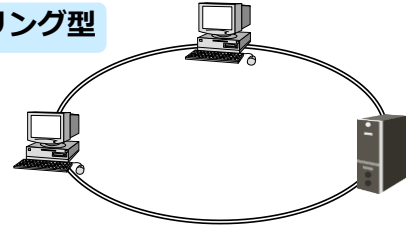
初期

現在

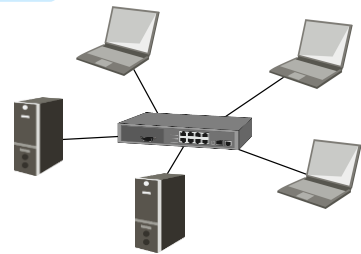
バス型



リング型



スター型



ネットワークの通信方式と接続形態は、技術の発展により変化してきました。

■ 通信方式

・半二重通信

半二重通信は、1本のケーブルを1つの伝送路として用い、送信と受信の順番を切り替えます。送受信を同時に行えません。初期のネットワーク(10BASE5、10BASE2)では、すべてが半二重通信方式でした。

・全二重通信

1本のケーブルの中に送信用と受信用の2つの伝送路を確保し、同時に送受信が可能です。送信と受信が同時に行えるので、半二重の2倍の伝送効率で通信が可能です。現在のネットワークは、ほぼすべて全二重通信方式です。

■ ネットワークの接続形態

・バス型

初期のイーサネットによる接続形態です。1本の共有ケーブルに、複数台の端末を接続する。安価に構築できますが、通信効率は悪いです。(10BASE5、10BASE2)

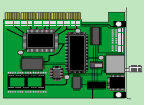

・リング型

共有ケーブルの端を接続し、伝送路が輪になる接続形態です。複数台の端末を接続しても伝送効率が維持できることが特徴です。(イーサネットではなく、トークンリング規格で実現されていた。)

・スター型

集線装置を使用し、周囲の端末を束ねる形態。集線装置において端末ごとに通信制御できることが特徴です。(10BASE-T、100BASE-TX、100BASE-FXなど)

6.5 階層と識別子(IPアドレスとMACアドレス)

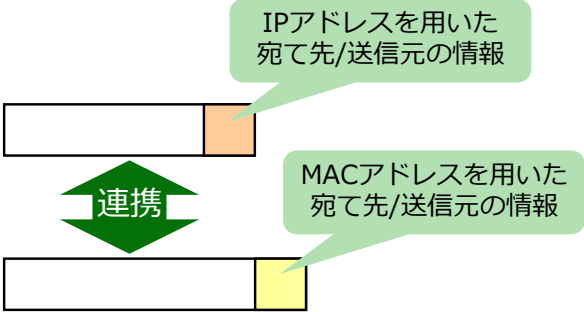


192.168.1.15

**IPアドレスとMACアドレスの
対応付けが必要**

00000E 111111

アプリケーション層	HTTP	SMTP	POP3	Telnet
トランスポート層	TCP/UDP			
インターネット層	IP			
ネットワーク インターフェース層	LAN (Ethernetなど)		WAN (PPP、フレイムリレーなど)	



ここでは、IPアドレスとMACアドレスの対応付け（**アドレス解決**）について解説します。

TCP/IPにおいて、宛て先を示すには、IPアドレスを使用しています。端末の所属しているネットワークを識別し、データを配送するためのアドレスです。一方、イーサネットによるデータ通信を制御するには、MACアドレスを用います。

TCP/IPの通信制御機能とイーサネットの通信制御機能を連携させるために、IPアドレスとMACアドレスを関連付ける必要があります。IPアドレスとMACアドレスの対応付けをする仕組みが**ARP (Address Resolution Protocol)**です。

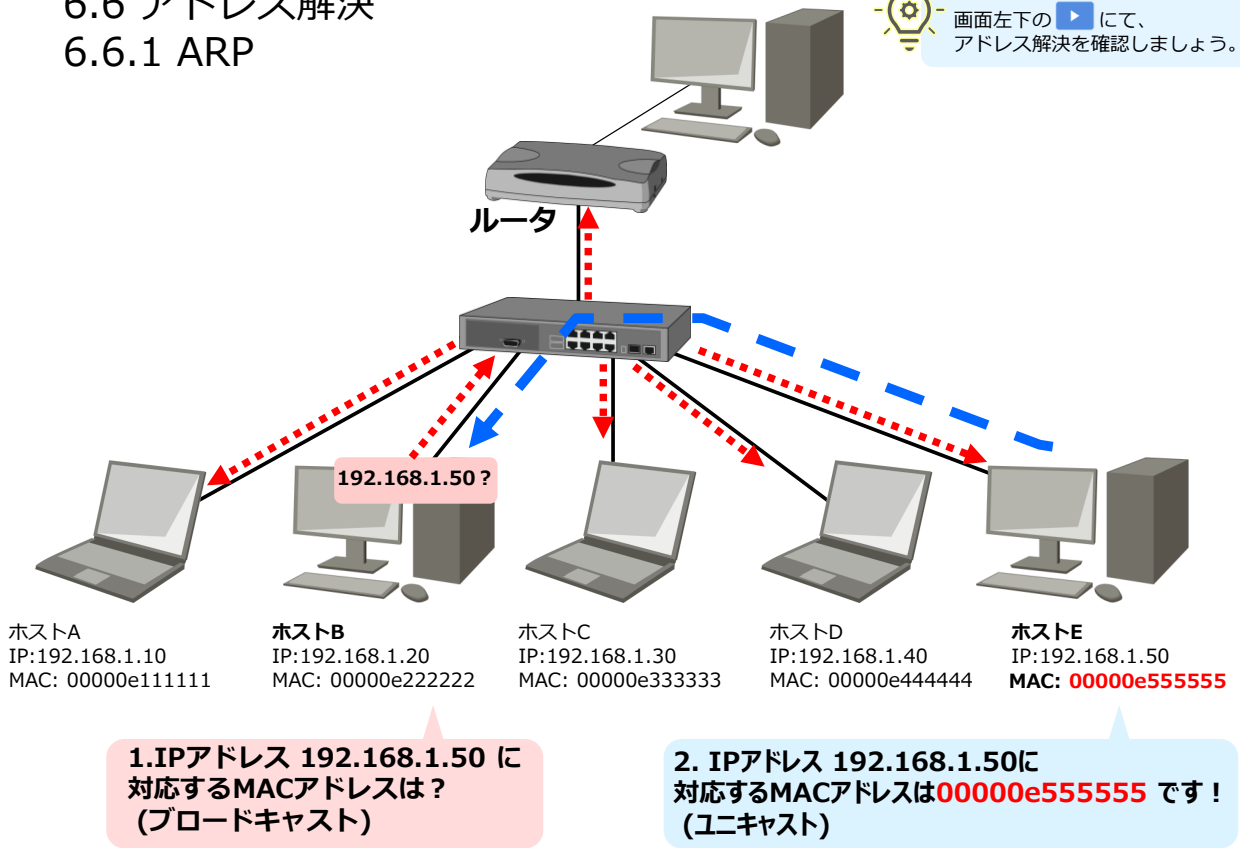
次は、ARPについて解説します。

6.6 アドレス解決

6.6.1 ARP



画面左下の▶にて、
アドレス解決を確認しましょう。



ARP(アドレス解決)は、宛て先端末のMACアドレスを検索する仕組みです。

宛て先端末のIPアドレスは既知であることが前提ですが、MACアドレスは分からない状態から通信が始まります。イーサネット上でデータを伝送するには宛て先MACアドレスが必要なため、通信に先立ち、宛て先のIPアドレスに対応するMACアドレスを解決します。

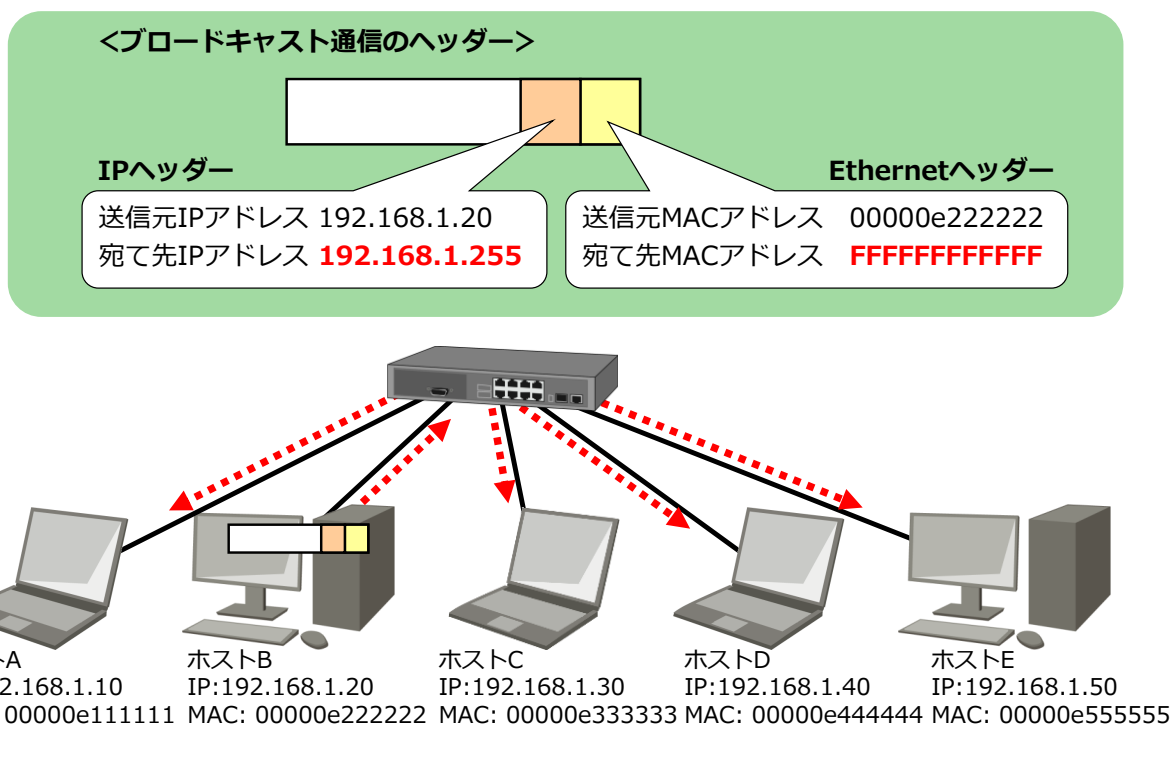
<ARPの仕組み>

1. 送信元は、データの送信に先立ち、宛て先端末の MAC アドレスを検索する。
「ARP要求」をブロードキャストで送信します。
(ブロードキャストで送信されたARP要求は、同一ネットワーク上のすべてのホストが受信します。)
2. 宛て先端末は、自身への問い合わせを受信した場合のみ、送信元に応答する。
「ARP応答」は送信元端末にのみユニキャストで送信します。

上記のように、宛て先端末のMACアドレスが解決できた送信元端末は、イーサネット上にデータを送信することができます。

なお、端末は一度調べたIPアドレスとMACアドレスの情報を一定時間保持します。(仕様はOSに依存します。)その時間内であれば、端末はARPによるアドレス解決は行わず、データを送信します。

6.7 ブロードキャスト通信



ここでは、ブロードキャストパケットについて解説します。

IPヘッダーの宛て先にブロードキャストアドレスが設定されると、自動的に宛て先MACアドレスには、FF:FF:FF:FF:FF:FFが設定されます。

スイッチングHUBでは、宛て先MACアドレスがFF:FF:FF:FF:FF:FFであるパケットを受信した以外のすべてのインターフェースへ無条件に転送します。そのため、ブロードキャストパケットは、すべての端末に到達します。なお、ルータでは、宛て先MACアドレスがFF:FF:FF:FF:FF:FFであるパケットを他のインターフェースへ転送しないため、ブロードキャストパケットの到達範囲は、同一ネットワーク内に限られます。

【参考】ブロードキャスト通信の負荷

ブロードキャストパケットは、同一ネットワーク内のすべての端末にデータを送信しますが、すべての端末にて必要な通信であるとは限りません。不必要なデータであっても、各端末ではネットワークインターフェース層、および、TCP/IP層での通信制御処理が行われます。最終的にはアプリケーション層にて不必要なデータは廃棄されますが、各端末の資源(CPU)を使用することとなるため、負荷がかかります。

<コマンド紹介> arpコマンド

```
> arp -a
```

```
インターフェイス: 172.16.1.10 --- 0xa
インターネット アドレス      物理アドレス      種類
172.16.1.1                  00-00-0e-ea-6a-cc    動的
172.16.1.15                 00-00-0e-ea-7a-ee    動的
```

本コマンドにてアドレス解決した履歴（ARPキャッシュ）が表示される図の場合、2行のアドレス解決情報が確認できる
表示内容は以下

- ・インターネットアドレス : IPアドレス
- ・物理アドレス : アドレス解決結果のMACアドレス



【参考】

OSの制御により、より多くの情報が表示される場合があります。

ここでは、arpコマンドについて紹介します。

arpコマンドは、ARPキャッシュの内容表示と変更を行います。ARPキャッシュには、IPアドレスと、その解決済みイーサネット物理アドレス(またはトークンリング物理アドレス)を格納するために使用する1つ以上のテーブルが含まれます。

<構文>

arp 各オプション

<主なオプション>

- a** : 現在のARPエントリーを表示します。IPアドレスを指定すると、指定したコンピュータのIPアドレスとMACアドレスを表示します。
- d** : すべてのエントリーを削除します。
- d IPアドレス** : IPアドレスで指定したエントリーを削除します。
- s IPアドレス MACアドレス** : ARPエントリーを追加します。MACアドレスはハイフンで区切った16進数で指定します。IPアドレスはドットで区切った10進数で指定します。ただし、コンピュータを再起動するとエントリーは削除されます。

<演習問題8> ARPの履歴を確認してみよう

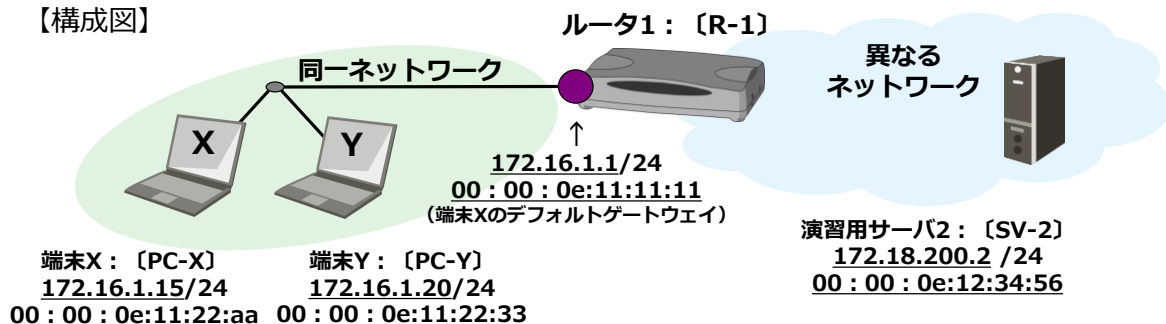
■ 演習問題6 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

arpコマンドを使用し、同一ネットワークの端末と異なるネットワークの端末に対して通信したときのARPのアドレス解決履歴を確認します。それぞれの宛て先端末に疎通確認した後、arp -aコマンドを実行し、アドレス解決結果を確認してください。

【構成図】



ARPのアドレス解決結果を確認
(端末と同一ネットワークのIPアドレスが
宛て先の場合)

ARPのアドレス解決結果を確認
(端末と異なるネットワークのIPアドレスが
宛て先の場合)

■ 演習問題8 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

arpコマンドを使用し、同一ネットワークの端末と異なるネットワークの端末に対して通信したときのARPのアドレス解決履歴を確認します。それぞれの宛て先端末に疎通確認した後、arp -aコマンドを実行し、アドレス解決結果を確認してください。

【操作手順】

操作手順は以下のとおりです。

- 手順1. コマンドプロンプトにてpingコマンドを使用し、宛て先端末を指定して疎通確認を行う
- 手順2. 疎通確認後、コマンドプロンプトにて“arp -a”を実行する
- 手順3. 実行結果として表示されたアドレス解決結果を確認する

※実行例と解答例は次のページです。

※MACアドレスの表記はOSによって異なります。大文字と小文字のどちらの表記でも同じMACアドレスです。

※コマンド操作については、Windows OSのコマンド操作方法（本資料P.36）を参照してください。

※arpコマンドについては、コマンド紹介ページ（本資料P.93）を参照してください。

次は、同一ネットワークの端末と異なるネットワークの端末に対して通信したときのアドレス解決履歴の実行例と解答例を確認します。

<演習問題8> ARPの履歴を確認してみよう（続き）

■ 演習問題6 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

arpコマンドを使用し、同一ネットワークの端末と異なるネットワークの端末に対して通信したときのARPのアドレス解決履歴を確認します。それぞれの宛て先端末に疎通確認した後、arp -aコマンドを実行し、アドレス解決結果を確認してください。

【実行例】

【端末と同一ネットワークのIPアドレスが宛て先の場合】
宛て先端末のIPアドレスに対してアドレス解決

```
コマンドプロンプト
> arp -a

インターフェイス: 172.16.1.10 --- 0xa
インターネット アドレス    物理アドレス    種類
172.16.1.20                00-00-0e-11-22-33  動的
172.16.1.15                00-00-0e-11-22-aa  動的
```

【端末と異なるネットワークのIPアドレスが宛て先の場合】
デフォルトゲートウェイのIPアドレスに対してアドレス解決

```
コマンドプロンプト
> arp -a

インターフェイス: 172.16.1.10 --- 0xa
インターネット アドレス    物理アドレス    種類
172.16.1.1                00-00-0e-11-11-11  動的
172.16.1.15                00-00-0e-11-22-aa  動的
```

※実際には図とは異なる結果が表示されると考えてください。

■ 演習問題8 ■

コマンドプロンプトを起動して、以下の設問に答えてください。

■ 設問 ■

arpコマンドを使用し、同一ネットワークの端末と異なるネットワークの端末に対して通信したときのARPのアドレス解決履歴を確認します。それぞれの宛て先端末に疎通確認した後、arp -aコマンドを実行し、アドレス解決結果を確認してください。

【操作手順】

操作手順は以下のとおりです。

- 手順1. コマンドプロンプトにてpingコマンドを使用し、宛て先端末を指定して疎通確認を行う
- 手順2. 疎通確認後、コマンドプロンプトにて“arp -a”を実行する
- 手順3. 実行結果として表示されたアドレス解決結果を確認する

【実行例】

実行例は図の下段のとおりです。

【解答例】

図の実行結果を読み取ると以下の内容が確認できます。

- ・ 端末と同一ネットワークのIPアドレスが宛て先の場合
172.16.1.20のアドレス解決結果： 00-00-0e-11-22-33
172.16.1.15のアドレス解決結果： 00-00-0e-11-22-aa
⇒宛て先端末のIPアドレスに対してアドレス解決を行う。

- ・ 端末と異なるネットワークのIPアドレスが宛て先の場合
172.16.1.1のアドレス解決結果： 00-00-0e-11-11-11
172.16.1.15のアドレス解決結果： 00-00-0e-11-22-aa
⇒送信元のルーティングテーブルによって判断された次の転送先（端末の場合、デフォルトゲートウェイ）のIPアドレスに対してアドレス解決を行う。

次は、本章のまとめです。

6.8 章のまとめ

- TCP/IPのネットワークインターフェース層は通信用ハードウェアが位置づけられ、通信用ハードウェアはLANやWANで採用されるさまざまな製品規格があります。
- イーサネット（Ethernet）はLANで最も使用されているネットワーク製品の規格です。
- イーサネットの特徴は以下のとおりです。
 - ✓ 伝送路上のハードウェア(NIC)を識別するためにMACアドレスを使う
 - ✓ 伝送路上のデータ衝突を検知するためにCSMA/CD方式を使う
- イーサネットの規格名の先頭の数字 (10/100/1000)が伝送速度を、末尾の文字は伝送媒体などを表しています。
- TCP/IPの通信制御機能とイーサネットの通信制御機能を連携させるために、IPアドレスとMACアドレスを関連付ける必要があります。IPアドレスとMACアドレスの対応付け（アドレス解決）をする仕組みがARPです。

第6章のまとめです。

- TCP/IPのネットワークインターフェース層は通信用ハードウェアが位置づけられ、通信用ハードウェアはLANやWANで採用されるさまざまな製品規格があります。
- イーサネット（Ethernet）はLANで最も使用されているネットワーク製品の規格です。
- イーサネットの特徴は以下のとおりです。
 - ✓ 伝送路上のハードウェア(NIC)を識別するためにMACアドレスを使う
 - ✓ 伝送路上のデータ衝突を検知するためにCSMA/CD方式を使う
- イーサネットの規格名の先頭の数字 (10/100/1000)が伝送速度を、末尾の文字は伝送媒体などを表しています。
- TCP/IPの通信制御機能とイーサネットの通信制御機能を連携させるために、IPアドレスとMACアドレスを関連付ける必要があります。IPアドレスとMACアドレスの対応付け（アドレス解決）をする仕組みがARPです。

第7章

端末の接続（LAN）

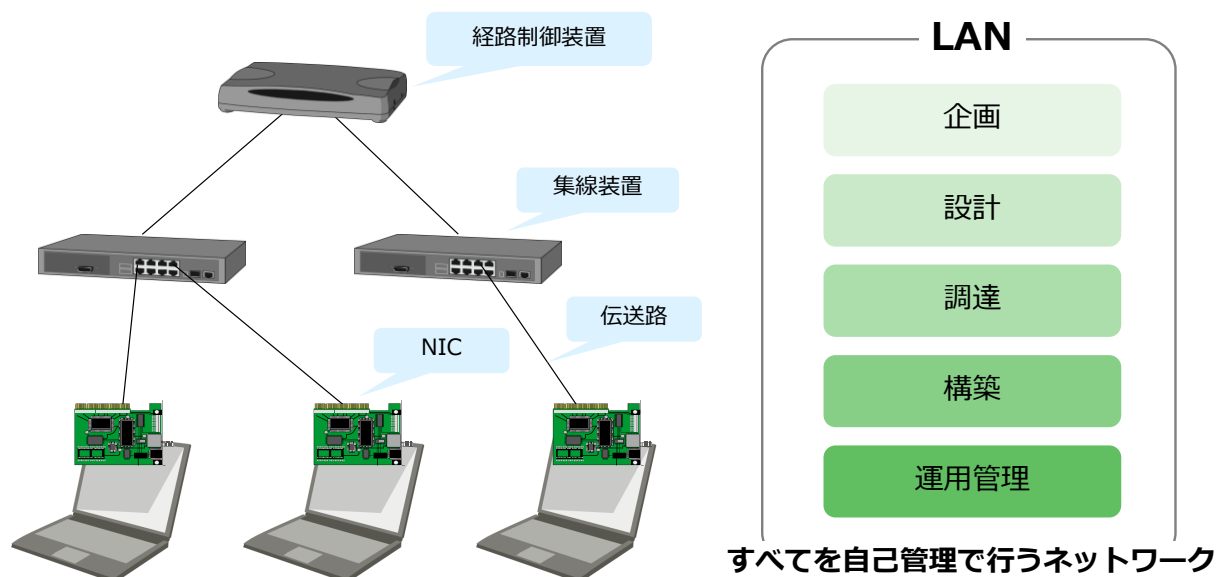
学習目標

この章では、ケーブルやネットワーク装置などのLANの要素について学習します。

- ケーブルやネットワーク装置の種類と特徴を理解する。

7.1 LANを構成する要素

ケーブル、ネットワーク装置を接続してLANを構成する



LANは限られた敷地内に敷設され、所有者が構築・運用・管理を行うネットワークです。LANは、NIC(インターフェース)、伝送路(ケーブル)、集線装置(リピータHUB、スイッチングHUB)、経路制御装置(ルータ、L3スイッチ)から構成されています。

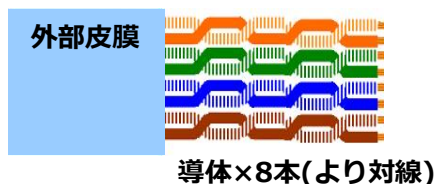
各装置の主な役割は、以下のとおりです。

- NIC
伝送路上のデータを送受信する部品です。装置と伝送路を接続する役割も担っています。
- 伝送路
装置間をケーブルで接続します。さまざまな伝送路の種類があります。
- 集線装置(リピータHUB、スイッチングHUB)
伝送路の延長や集線を行い、データを中継します。
- 経路制御装置(ルータ、L3スイッチ)
ネットワークを形成し、ブロードキャスト通信の範囲を制御します。

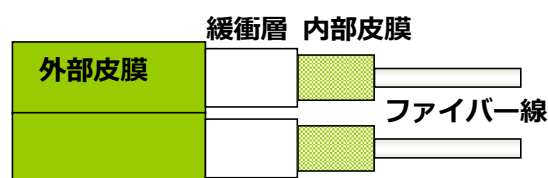
7.2 LANケーブルの種類と特徴

7.2.1 ツイストペアケーブルと光ファイバーケーブル

■ ツイストペアケーブル



■ 光ファイバーケーブル



ここでは、利用頻度が高いLANケーブルについて説明します。

■ ツイストペアケーブル

8本の信号線の各2本を対によっています。ケーブルの先端にはモジュージャックコネクタを採用しています。他ケーブルと比較するとノイズに対して弱いという欠点がありますが、ケーブルの敷設性に優れており、また低価格で手に入ることから、特にアクセスLANの構成に使用されています。ツイストペアケーブルの最大延長距離は、100mです。

・カテゴリ

許容伝送速度に応じて、カテゴリと呼ばれる区分に分けられています。

カテゴリ3	: 10Mbps
カテゴリ5	: 100Mbps
カテゴリ5e	: 1Gbps
カテゴリ6	: 1Gbps
カテゴリ7	: 10Gbps (専用NICが必要)

■ 光ファイバーケーブル

このケーブルは、ファイバー線内部 (コアと呼ばれる部分) に光信号を伝播するよう設計されており、他のケーブルよりも耐ノイズ性に優れています。他のケーブルよりも敷設コストが高くなります。主にバックボーンLANで使用されます。

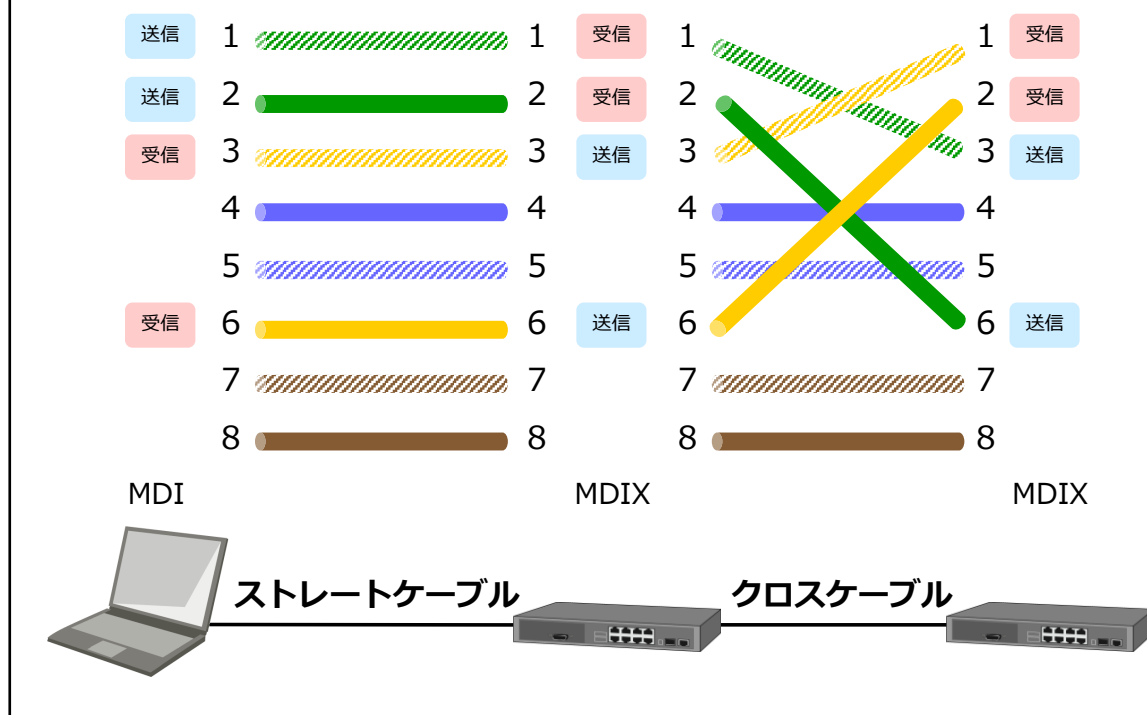
・モード

光ファイバーケーブルは、モードにより特徴が異なります。

シングルモード : ケーブル内を直進させて信号を伝送するため、減衰が少なく、長距離伝送 (5km程度) が可能です。極細のガラス素材のため、高価であり、ケーブルの折り曲げに弱いなど注意が必要です。

マルチモード : ケーブル内を反射させながら信号を伝送するため、信号が減衰しやすいです。そのため、最大延長距離は500m程度です。しかし、石英またはプラスチック素材のため安価で折り曲げに強く取り扱いやすいことが特徴です。

7.2.2 ストレートケーブルとクロスケーブル



ツイストペアケーブルには、**ストレートケーブル**と**クロスケーブル**の2種類があります。

ストレートケーブル : 送信経路と受信経路が交差していないケーブル
クロスケーブル : 送信経路と受信経路が1度交差しているケーブル

コンピュータのインターフェース(MDI)では、1,2番でデータの送信、3,6番でデータの受信を行います。集線装置であるHUBのインターフェース(MDIX)では、コンピュータとは逆に、1,2番でデータの受信、3,6番でデータの送信を行うため、コンピュータとHUB間はストレートケーブルで接続します。(カテゴリ5、カテゴリ5eのケーブルにおいて)

しかし、HUBとHUBを接続するときなど、インターフェースの仕組みが同じ装置同士(MDIとMDI、MDIXとMDIX)の場合は、ストレートケーブルでは送受信の整合性が取れず通信が実現できません。この場合は、伝送路が一度交差しているクロスケーブルを使用します。

【用語解説】

カスケード接続:

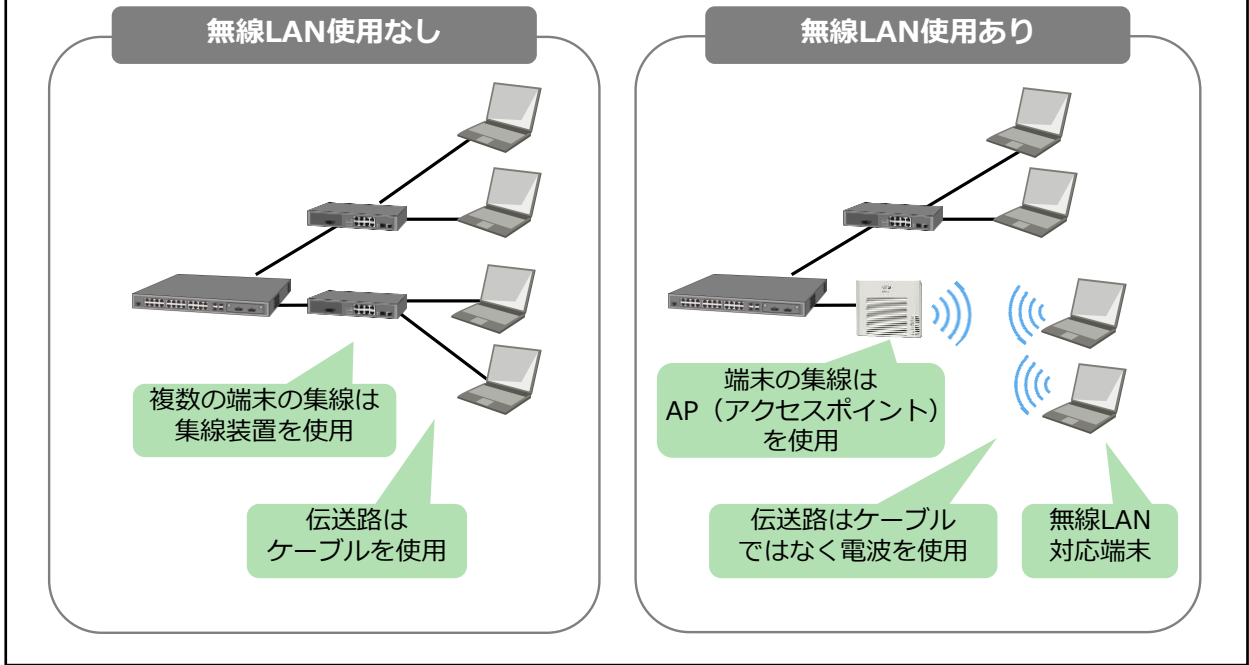
ネットワーク中継装置同士の多段接続のこと。クロスケーブルを使用して接続する必要がある。なお、カスケードとは「数珠繋ぎ」という意味。

カスケード専用ポート:

カスケード接続をする際に利用されるインターフェースのこと。通常HUBのインターフェースは、MDIXであるが、カスケード専用ポートは、MDIとなっているため、ストレートケーブルを用いて接続が可能である。**アップリンクポート**とも表現される。

7.3 無線LAN

集線装置をアクセスポイントへと置き換えます



ここでは、無線LANについて解説します。

無線LANは、ケーブルを使用せず、電波で端末を接続する形態のネットワークです。場所に限定されない柔軟なネットワークが構築できるため、企業内のさまざまな場面で活用されています。ただし、便利に利用できる反面、セキュリティや通信の不安定さなどマイナスの特徴もあります。

アクセスポイントと無線LAN対応端末との間で通信を行うには、双方で同一の規格を使用する必要があります。この規格には、通信規格や、セキュリティ規格があります。

異なる通信規格やセキュリティ規格同士では通信することができないため、無線LANの導入に際しては端末要件を考慮した上で、導入するネットワーク機器を選定する必要があります。

・通信規格

周波数帯や通信速度によって規格が分かれています。

通信規格名	周波数帯	通信速度(規格上の最大値)
IEEE802.11	2.4GHz	2Mbps
IEEE802.11b	2.4GHz	11Mbps
IEEE802.11g	2.4GHz	54Mbps
IEEE802.11a	5GHz	54Mbps
IEEE802.11n (Wi-Fi4)	2.4GHz/5GHz	600Mbps
IEEE802.11ac (Wi-Fi5)	5GHz	6.9Gbps
IEEE802.11ax (Wi-Fi6)	2.4GHz/5GHz	9.6Gbps

・セキュリティ規格

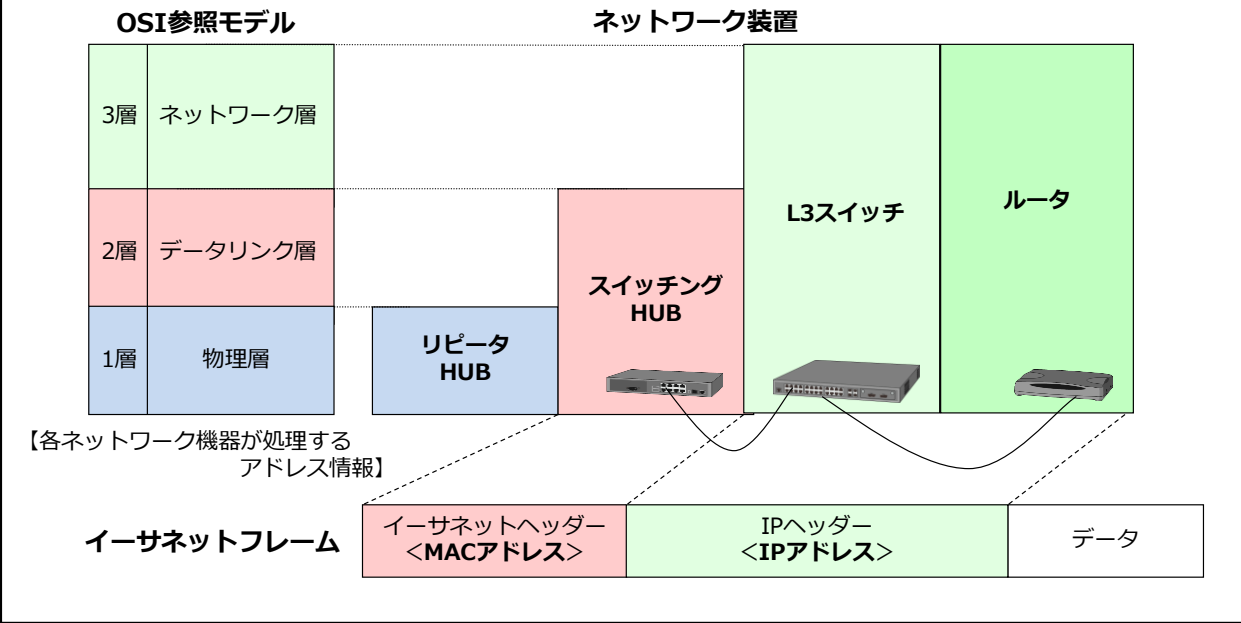
認証方式と暗号化方式の組み合わせの種類によって分かれています。

セキュリティ規格の例：WEP、WPA、WPA2、WPA3 等

7.4 ネットワーク装置の種類と特徴

7.4.1 集線装置と経路制御装置

機能や特徴が異なるため、導入効果が異なる



ここでは、ネットワーク装置について解説します。

ネットワーク装置は、ケーブルを束ねる集線装置(スイッチングHUB、リピータHUB)とデータ配送を制御する経路制御装置(L3スイッチ、ルータ)があります。それぞれの装置の役割は、OSI参照モデル (本資料P.10) の各層に対応付けることができます。

■ 集線装置

● リピータHUB

経路延長や集線を行います。中継するデータは無条件にすべてのインターフェースに送出します。現在では、主に使用されておらずスイッチングHUBに置き換えられています。

● L2スイッチ (スイッチングHUB)

中継するデータの宛て先MACアドレスによる転送制御を行います。スイッチ機能により、宛て先端末が接続されているインターフェースにのみデータが転送されます。

■ 経路制御装置

● L3スイッチ

中継するデータの宛て先IPアドレスによる転送制御を行います。ルーティング機能により、宛て先端末が所属しているネットワークまでの経路が選択されます。ルータよりも処理速度が速く、LAN内で使用されます。

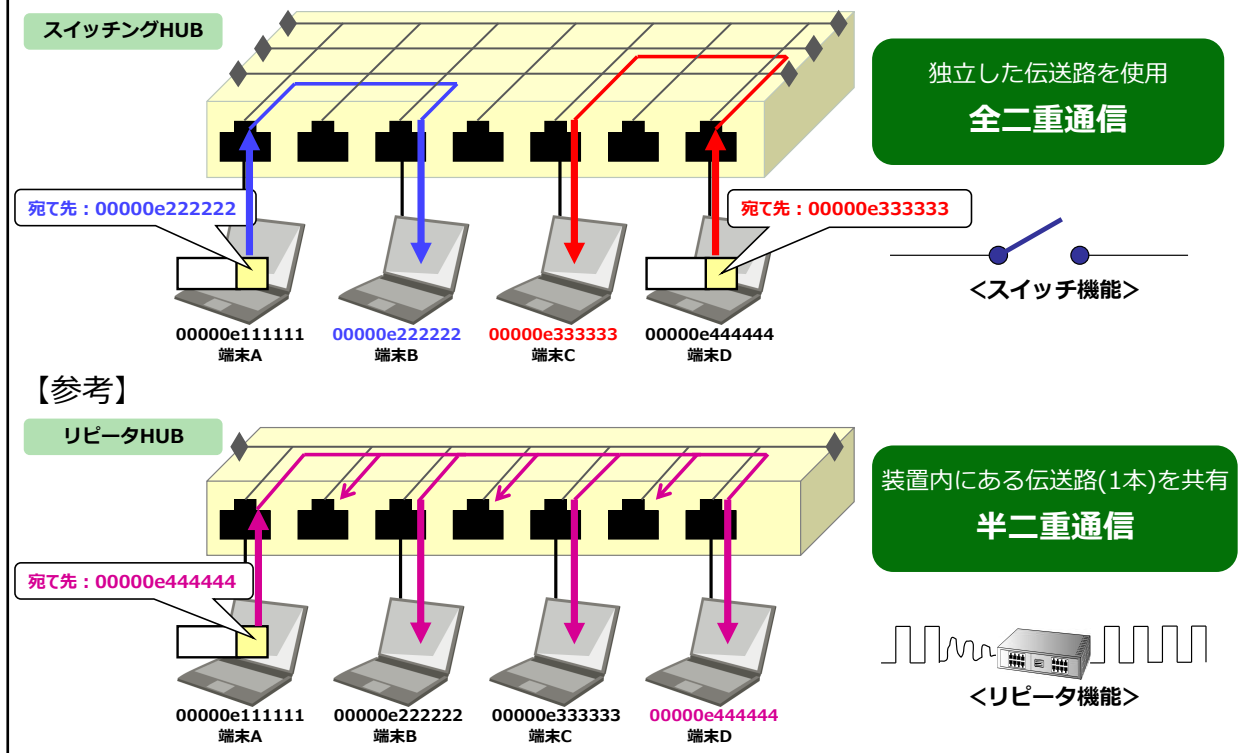
● ルータ

中継するデータの宛て先IPアドレスによる転送制御を行います。ルーティング機能により、宛て先端末が所属しているネットワークまでの経路が選択されます。LANとWANなど異なるネットワークを接続する際に使用されます。

7.4.2 スイッチングHUBとリピータHUB



画面左下の▶にて、
集線装置を確認しましょう。



まずは、集線装置について解説します。

●スイッチングHUB

スイッチとは、宛て先端末が接続されているインターフェースにのみデータを中継する機能です。データに含まれるMACアドレスを元に通信制御しています。

通信している端末のペアの間でのみ帯域が専有されるため、複数の端末が接続されている場合でも、通信効率が低下しません。

図の例では、端末Aが端末Bにデータを送信すると、スイッチングHUBは端末Bにのみデータを送信します。端末A-B間の経路のみが専有されるため、同時に端末Cから端末Dへの通信も可能です。つまり、複数の端末が同時にデータを送信することができます。

【参考】

●リピータHUB

リピータとは、伝送路から受ける抵抗で減衰し、弱まったり波形の乱れた電気信号を増幅、整形する機能です。伝送路を延長する場合やコンピュータからの伝送路を集線する目的で利用します。流れてきた電気信号をただ伝送しているだけで、通信制御は行っていません。

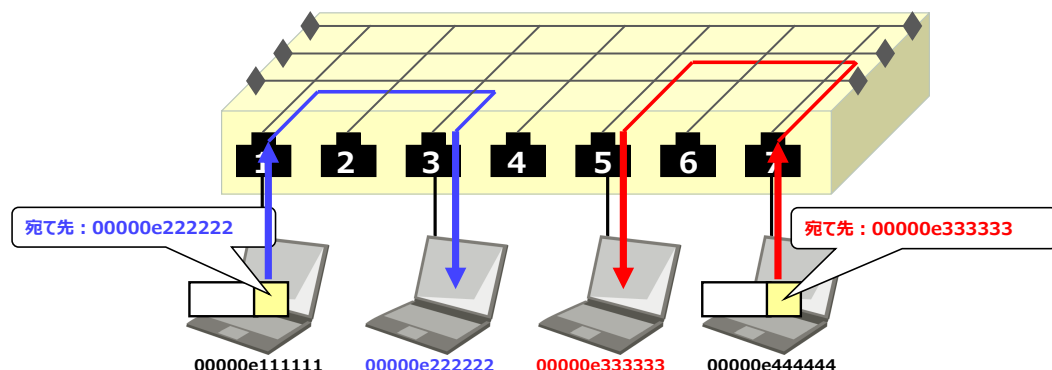
リピータHUBは内部に1本の伝送路があります。すべての端末からの通信が1本の伝送路を共有するため、1つの通信が発生している最中に、他の通信を行うことはできません。

図の例では、端末Aが端末D宛にデータを送信していますが、端末Bや端末Cにも同じデータが転送されています。もし、端末Bや端末Cが同時にデータを送信した場合、端末Aが送信したデータと衝突してしまいます。よって、複数の端末が同時に通信を行うことはできません。

7.4.3 MACアドレステーブル

MACアドレステーブル

インターフェース1	00000e111111	インターフェース5	00000e333333
インターフェース2		インターフェース6	
インターフェース3	00000e222222	インターフェース7	00000e444444
インターフェース4			



ここでは、スイッチングHUBが持つMACアドレステーブルについて解説します。

スイッチ機能の制御で使用する情報は、**MACアドレステーブル**です。MACアドレステーブルは、スイッチングHUBの装置内部にあり、どのインターフェースの先にどの端末が存在するかが登録されています。なお、MACアドレステーブルは、自動的に学習が行われます。

<スイッチングHUBによるデータ転送制御>

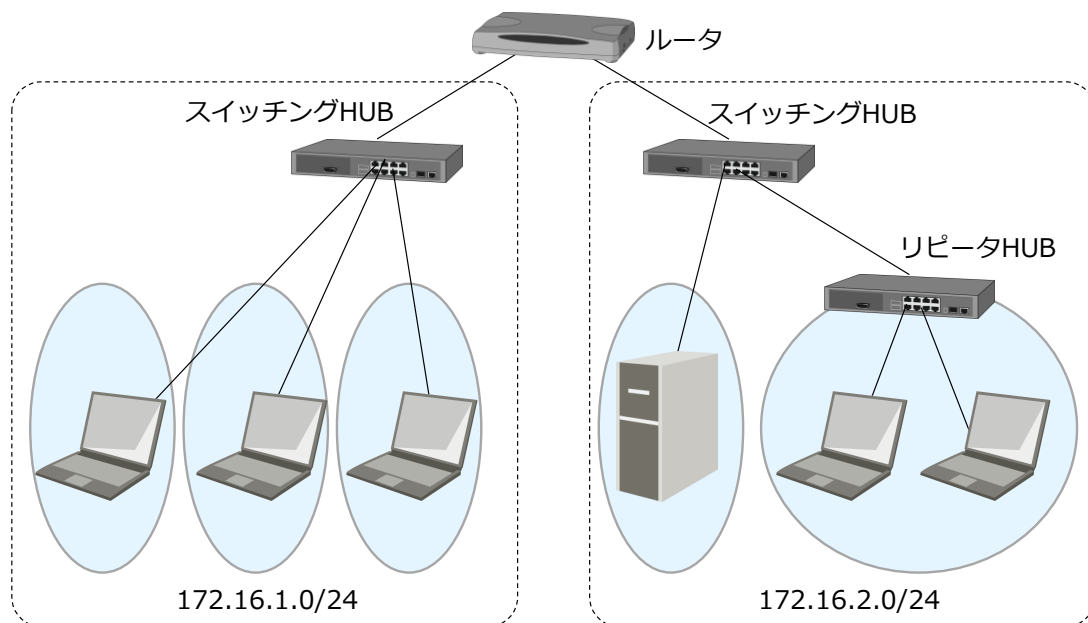
1. データがスイッチングHUBに到達すると、宛て先MACアドレスがMACアドレステーブルに登録されているかが確認される。
2. 登録されている場合には、該当のインターフェースにのみデータが転送される。
3. 登録されていない場合には、受信したインターフェース以外のすべてのインターフェースに転送される。

<MACアドレステーブル内の情報の構成>

1. スwitchングHUBに電源が投入された時点では、情報は登録されていない。
2. データがスイッチングHUBに到達すると、送信元MACアドレスが参照される。
3. MACアドレステーブルの受信インターフェース番号に送信元MACアドレスが登録される。
4. 一定時間以内に同じ送信元から通信が発信されなければ、登録情報が消去される。

7.4.4 コリジョンドメイン

データの衝突(コリジョン)が発生する範囲



ここでは、コリジョンドメインについて解説します。

コリジョンドメインを適切に構成することにより、ネットワークの通信効率を向上させることができます。リピータHUBとL2スイッチHUBとでは、導入効果が異なります。

コリジョンドメイン

コリジョンドメインとは、データの衝突(コリジョン)が発生する範囲のことです。リピータHUBで接続された範囲では、複数の端末が同時にデータを送信すると衝突が発生します。複数の通信が同時に発生した場合には、タイミングをずらしてデータを送信するため、通信効率下がります。

コリジョンドメイン内に接続された端末の台数が増えると、衝突が発生する確率が高くなり、通信効率が悪くなります。そのため、コリジョンドメイン内の端末数は、できるだけ少ない台数であることが望ましいです。(コリジョンドメインの推奨端末台数は、5台程度です。)

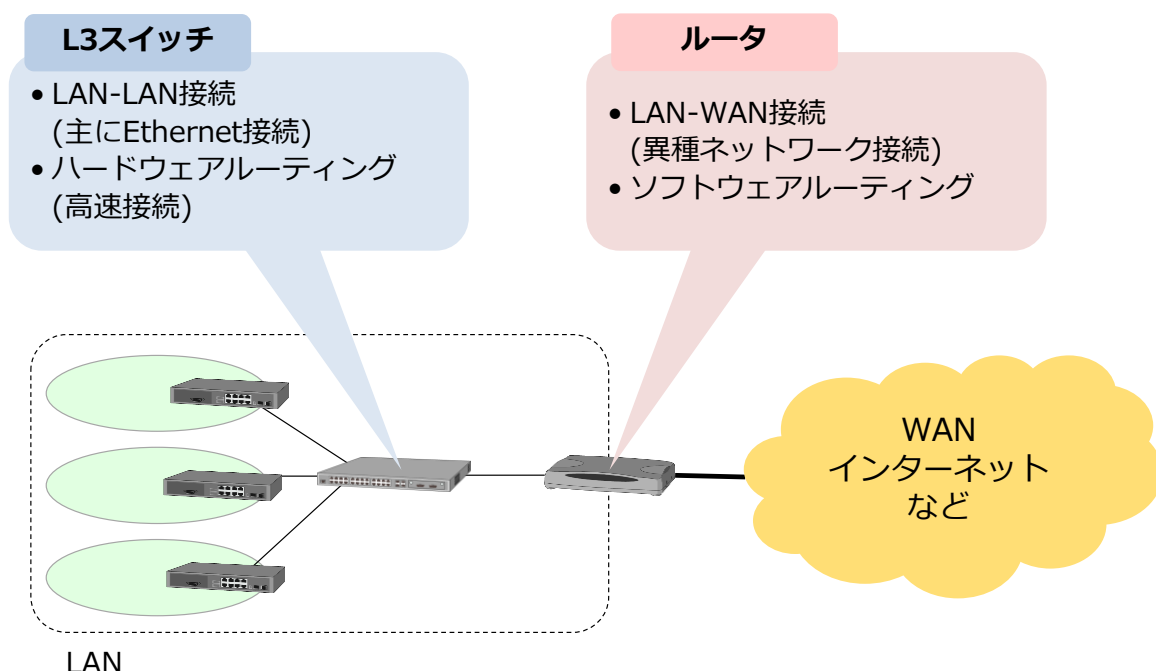
なお、スイッチングHUBは、インターフェースごとにコリジョンドメインを分割するため、通信効率の低下を防ぐことができます。

【用語解説】

コリジョン:

リピータHUBなどの半二重通信環境でおこるデータの衝突のこと。コリジョンが発生すると、一定時間通信ができなくなるため、多発すると通信速度が著しく低下する。

7.4.5 ルータとL3スイッチ



次は、経路制御装置について解説します。

•ルータ

ルータとは、目的のネットワークまでの経路を判断する機能を持った装置です。装置内部にあるルーティングテーブルを用いて、データの転送方向を決定します。データに含まれるIPアドレスを元にデータ制御しています。

ルータは、イーサネット以外のネットワーク規格を相互接続することができ、LANとWAN(インターネット)を接続することができます。

•L3スイッチ

L3スイッチは、スイッチングHUBにルーティング機能を付加した装置です。ルータと同じくIPアドレスを元にしてデータの転送方向を決定します。

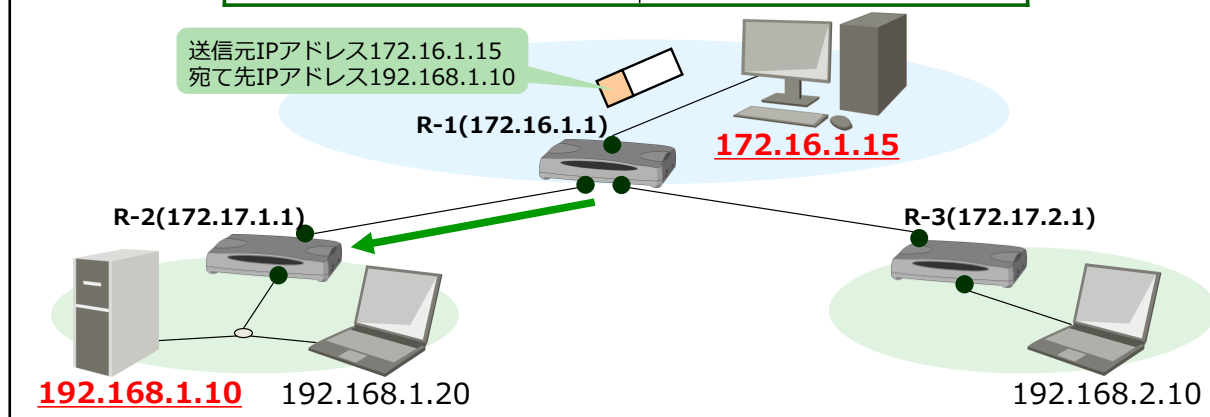
L3スイッチは、ルータとは異なり専用のハードウェアで転送処理を行うため、高速データ転送が可能です。ただし、ルーティング処理の高速化が図られるプロトコルは、通常IPのみです。また、L3スイッチの多くは、WAN インターフェースを持たないため、LAN間ルーティングで適用されます。

社内ネットワークを構成するときは、WANとの接続はルータを使用し、内部の高速化のためにL3スイッチを用いる構成が一般的です。

<参考> ルーティングテーブル

R-1のルーティングテーブル

ネットワーク	転送先
192.168.1.0/24	172.17.1.1(R-2)
192.168.2.0/24	172.17.2.1(R-3)
172.17.1.0/24	Direct
172.17.2.0/24	Direct
172.16.1.0/24	Direct



経路制御(ルーティング)機能で使用する情報は、ルーティングテーブルです。ルーティングテーブルは、ルータ・L3スイッチの装置内部にあり、どのルータに転送すれば、目的のネットワークに到達できるかが登録されています。なお、ルーティングテーブルは、管理者が情報を登録しなければいけません。

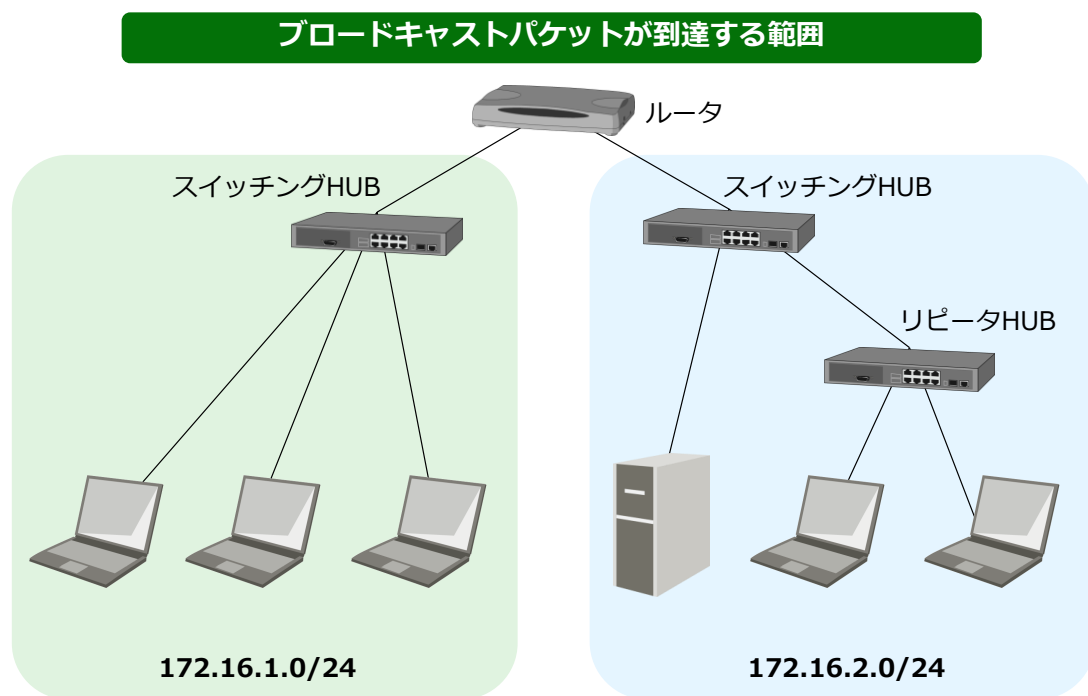
<ルータ・L3スイッチによるデータ転送制御>

1. データがルータ・L3スイッチに到達すると、宛て先端末の所属するネットワークがルーティングテーブルに登録されているかが確認される。
2. 登録されている場合には、登録されている転送先にデータが転送される。
3. 登録されていない場合には、データは破棄される。

<ルーティングテーブル内の情報の構成>

1. ルータ・L3スイッチに電源が入り、インターフェースにIPアドレスが設定された時点では、直接接続されているネットワーク情報(Direct)のみ登録されている。
2. 管理者が、手動(スタティックルーティング)または、動的(ダイナミックルーティング)により間接的に接続されているネットワークへの経路情報を登録する。

7.4.6 ブロードキャストドメイン



ここでは、ブロードキャストドメインについて解説します。

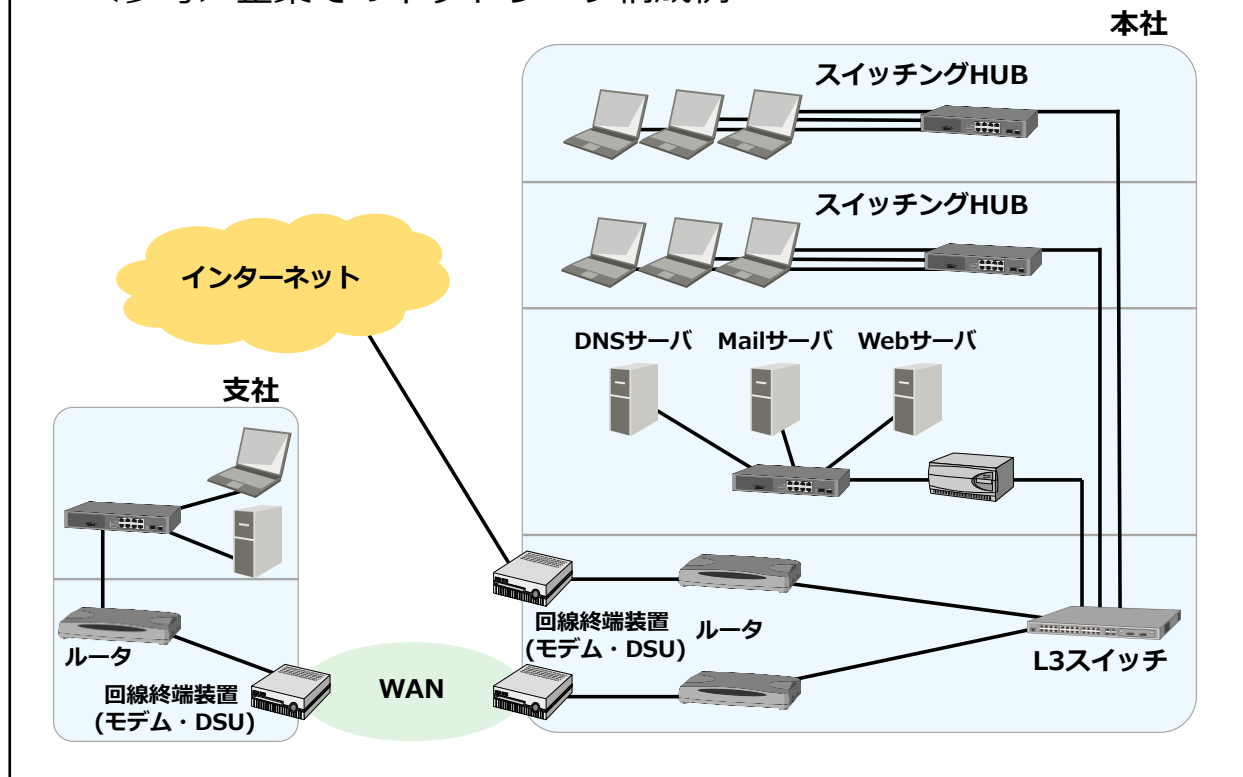
ブロードキャストドメインを適切に構成することにより、ネットワークの通信効率を向上させることができます。ルータおよびL3スイッチを導入することで効果が得られます。

ブロードキャストドメイン

ブロードキャスト通信は、同一ネットワーク内の全端末を宛て先とした通信です。ブロードキャストパケットが流れる範囲をブロードキャストドメインといいます。

ブロードキャストドメイン内に接続された端末の台数やブロードキャストパケットの発生率によっては、ネットワークに負荷がかかる場合があります。そのため、適する範囲でブロードキャストドメインを分割する必要があります。(ブロードキャストドメインの推奨端末台数は、100台～200台です。)

<参考> 企業でのネットワーク構成例



図は、企業のネットワークにおけるネットワーク装置の導入例です。通信するために必要なネットワーク装置（ルータ、L3スイッチ、スイッチングHUB）の配置を確認しましょう。

主な要件は以下のとおりです。

- 本社内のネットワークにはL3スイッチを導入し、データ転送処理を高速化
- 端末の接続にL2スイッチを使用し、コリジョンドメインを分割
- WAN回線で拠点間を接続
- 本社ネットワークからインターネット接続
- 本社ネットワーク内に、インターネット公開サーバ (Mailサーバ、Webサーバ)を設置

7.5 ネットワーク装置の基本機能と付加機能

	リピータHUB	スイッチングHUB	L3スイッチ	ルータ
基本機能			ルーティング	
		スイッチ		
	リピータ			
付加機能				
	10/100/1000Mbps対応			
	SNMPエージェント			
		VLAN		
		STP		
		リンクアグリゲーション		
			VRRP	

ネットワーク装置の機能を比較すると、図のようになります。

■基本機能

●リピータ

リピータとは、伝送路から受ける抵抗で減衰し、弱まったり波形の乱れた電気信号を元のように増幅、整形する機能です。リピータにより、経路を延長することができます。

●スイッチ:

受信したデータの宛て先 MAC アドレスを参照し、該当するインターフェースにのみデータの中継するよう装置内部の経路を切り替える(スイッチ)機能です。各インターフェースは、並行してデータの送受信ができるため、リピータ HUB に比べて効率良い通信が可能となります。

●ルーティング:

受信したデータの宛て先IPアドレスを参照し、データの転送方向を決定する機能です。

■付加機能

●10/100/1000Mbps対応:

10Mbps と 100Mbpsと1Gbps のスピードに対応したインターフェースを備え、速度の異なるコンピュータが混在する環境においても、それぞれのスピードでの通信を可能にする機能です。(デュアルスピードHUB)

●SNMPエージェント:

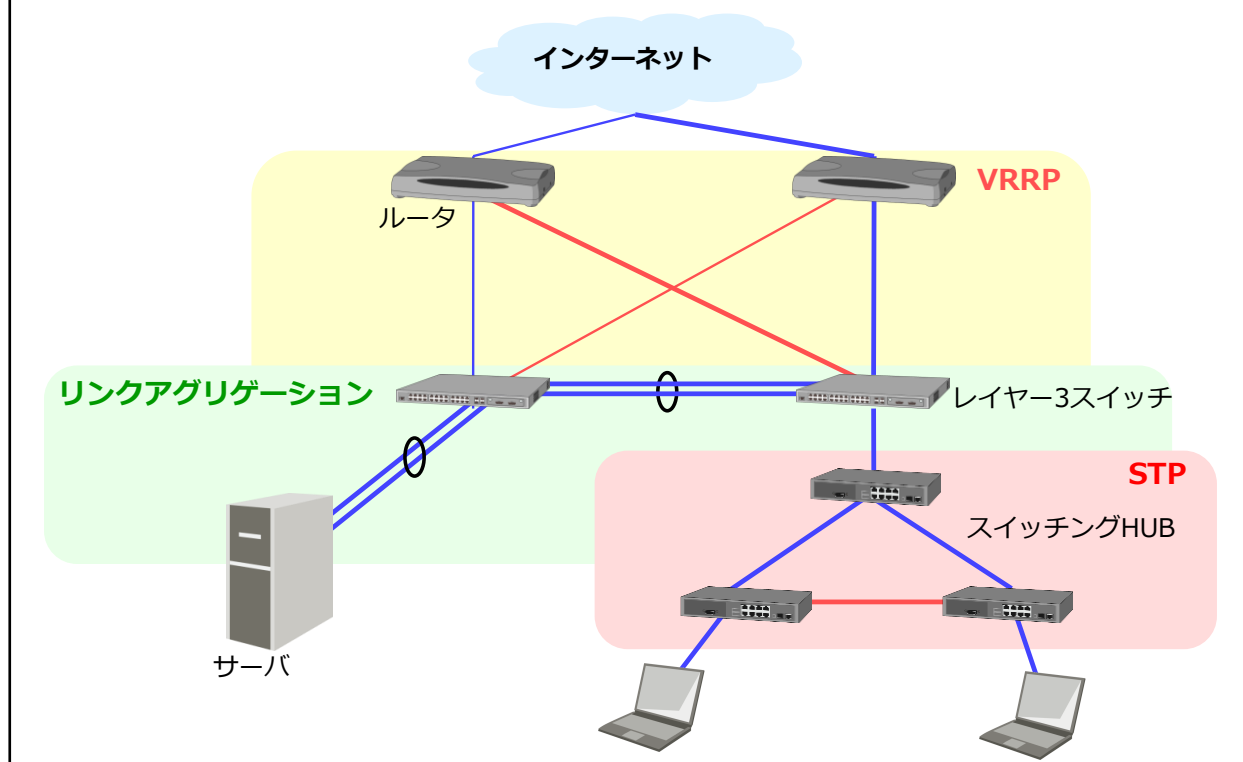
SNMP(Simple Network Management Protocol)を利用して、装置の状態監視ができる機能です。エージェント(被監視機能)とマネージャ(監視機能)間で連携して監視します。(インテリジェント HUB)

●VLAN:

本来は物理的な構成変更を必要とするようなネットワークの分割や統合を論理的に実現する機能です。組織変更などにより、1つのL2スイッチに接続されたネットワークを別のネットワークとして分割したり、逆に物理的に離れた場所のネットワークを同一のネットワークとして構成する場合に、時間とコストをかけずに論理的な設定変更のみでネットワーク構成を変更することができます。

※付加機能は、すべての装置にサポートされているわけではありません。

<参考> ネットワーク装置の付加機能



ここでは、付加機能の一種であるSTP、リンクアグリゲーション、VRRPについて解説します。

•STP (spanning tree protocol)

スイッチングHUBをループ構成にした場合のブロードキャストストームを防ぐ機能がSTPです。経路の冗長化のために、スイッチングHUBをループ構成にした場合、ブロードキャストフレームを各スイッチングHUBがお互いに転送し合うため、ネットワークが飽和状態になります (ブロードキャストストーム)。STPを構成することにより、物理的にループ構成になったネットワークにおいても、一部の経路を遮断し、問題なくデータ転送を行うことができます。

•リンクアグリゲーション

複数の伝送路を束ねることにより、帯域の拡張と信頼性の向上を実現する機能がリンクアグリゲーションです。

物理的に複数ある伝送路を、論理的に1本であるかのようにデータ転送を行うことができます。いずれかの伝送路が障害により使用できなくなった場合には、残っている伝送路で通信を継続することができるため、比較的低コストで拡張性と耐障害性の両面を実現できます。

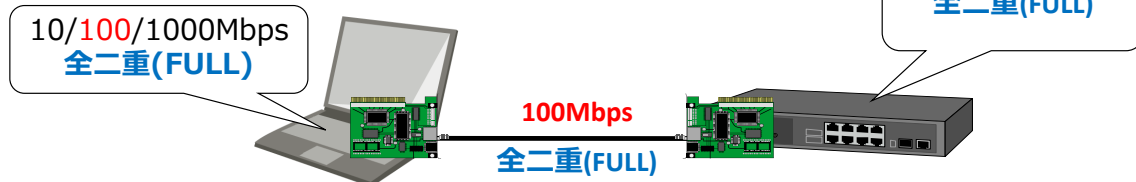
•VRRP (Virtual Router Redundancy Protocol)

ルータやL3スイッチの障害による運用停止を防ぐために、機器を二重化する機能がVRRPです。

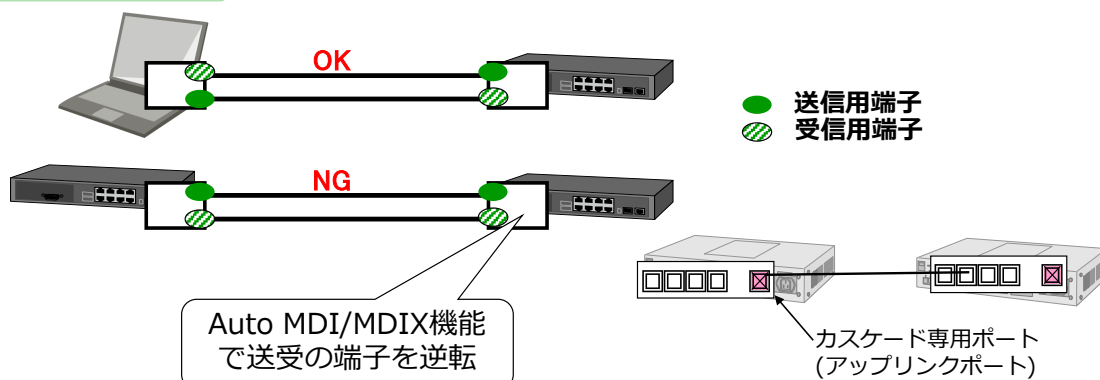
2台の同一機器のうち一方を現用系、他方を待機系と定義します。2台の装置間で同期を行い、通常の運用で使用している現用系に障害が発生した場合には、待機系に自動的に切り替えて運用を継続します。同一機器を2台導入しなければならないため、高コストですが、大変信頼性の高い耐障害性を実現することができます。

7.6 自動設定機能

オートネゴシエーション



Auto MDI/MDIX



ここでは、自動設定機能であるオートネゴシエーション機能、Auto MDI/MDIX機能について解説します。

装置を接続する際、対向装置と同一の通信速度、通信方式を設定し、MDI/MDI-Xの整合性を保つ必要があります。しかし、対向装置ごとに装置の性能や設定情報を確認するのは手間であるため、自動設定機能がサポートされています。

•オートネゴシエーション機能

インターフェース間で、伝送する相手により通信速度 (10/100/1000Mbps) と、通信方式 (全二重/半二重) を自動的に切り替える機能です。

•Auto MDI/MDIX機能

伝送路の種類(ストレートケーブル、クロスケーブル)を判断し、適切なインターフェースの種類(MDIまたはMDIX)に切り替える機能です。

Auto MDI/MDIX機能がサポートされていない装置では、カスケード専用ポートが用意されていることが多いです。

次は、本章のまとめです。

7.7 章のまとめ

- 利用頻度が高いLANケーブルに以下2つがあります。
 - ✓ ツイストペアケーブル : ケーブルの敷設性に優れており、低価格で手に入るが、ノイズに対して弱い
 - ✓ 光ファイバーケーブル : 光信号を伝播できるため他のケーブルよりも耐ノイズ性に優れるが敷設コストが高い
- 集線装置にリピータHUBやスイッチングHUB（L2スイッチ）があります。
 - ✓ リピータHUB : 経路延長や集線のために用いる
 - ✓ スwitchingHUB : MACアドレスを元に、宛て先端末が接続されているインターフェースにのみデータを中継するスイッチ機能を持つ
- 経路制御装置にルータやL3スイッチがあります。どちらもルーティング可能な装置です。
 - ✓ ルータ : イーサネット以外のネットワーク規格を相互接続することができ、LANとWAN(インターネット)を接続する
 - ✓ L3スイッチ : ルータとは異なり専用のハードウェアで転送処理を行うため、高速データ転送が可能である
- 異種のネットワークを接続するためにはルータを使用し、内部の高速化のために、L3スイッチを使うのが一般的な企業ネットワークです。

第7章のまとめです。

- 利用頻度が高いLANケーブルに以下2つがあります。
 - ✓ ツイストペアケーブル : ケーブルの敷設性に優れており、低価格で手に入るが、ノイズに対して弱い
 - ✓ 光ファイバーケーブル : 光信号を伝播できるため他のケーブルよりも耐ノイズ性に優れるが敷設コストが高い
- 集線装置にリピータHUBやスイッチングHUB（L2スイッチ）があります。
 - ✓ リピータHUB : 経路延長や集線のために用いる
 - ✓ スwitchingHUB : MACアドレスを元に、宛て先端末が接続されているインターフェースにのみデータを中継するスイッチ機能を持つ
- 経路制御装置にルータやL3スイッチがあります。どちらもルーティング可能な装置です。
 - ✓ ルータ : イーサネット以外のネットワーク規格を相互接続することができ、LANとWAN(インターネット)を接続する
 - ✓ L3スイッチ : ルータとは異なり専用のハードウェアで転送処理を行うため、高速データ転送が可能である
- 異種のネットワークを接続するためにはルータを使用し、内部の高速化のために、L3スイッチを使うのが一般的な企業ネットワークです。

第8章

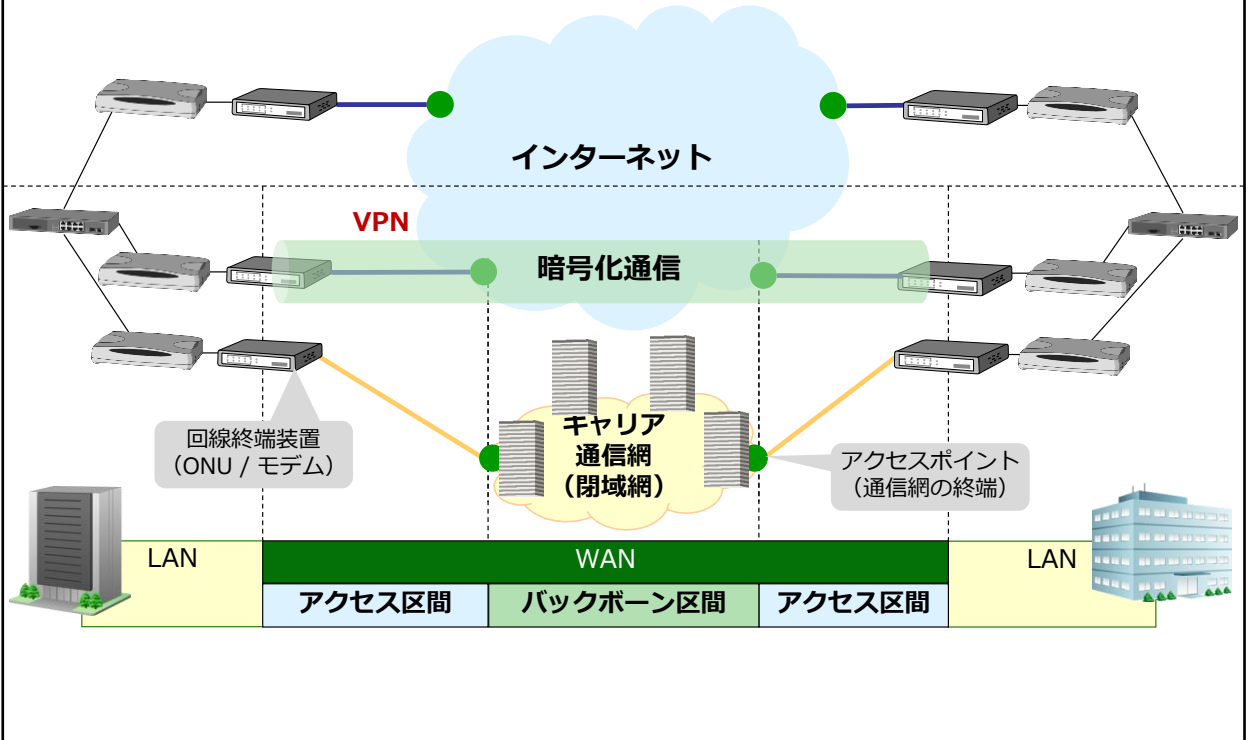
拠点間接続（WAN）

学習目標

この章では、拠点間を接続するWANサービスについて学習します。

- WANサービスの種類と特徴を理解する。

8.1 WANの構成要素



WANは物理的に離れている拠点間を結ぶネットワークです。個人が敷設することはできないため、電気通信事業者(キャリア)が回線の敷設工事を行い、サービスとしてユーザーに提供しています。WANは**アクセス区間**と**バックボーン区間**に区分されます。

・アクセス区間

アクセスポイントとユーザー拠点を結ぶ区間です。帯域保証型やベストエフォート型などのさまざまなサービスが用意されており、距離や料金、利用時間に応じて適するサービスを検討します。

サービス例)ADSL、光回線（FTTH）など

・バックボーン区間

WANの中核となる区間です。電気通信事業者が敷設した通信網やインターネットを介した通信サービスとして提供されています。電気通信事業者や地域により提供されるサービスが異なるため、適するサービスを検討します。

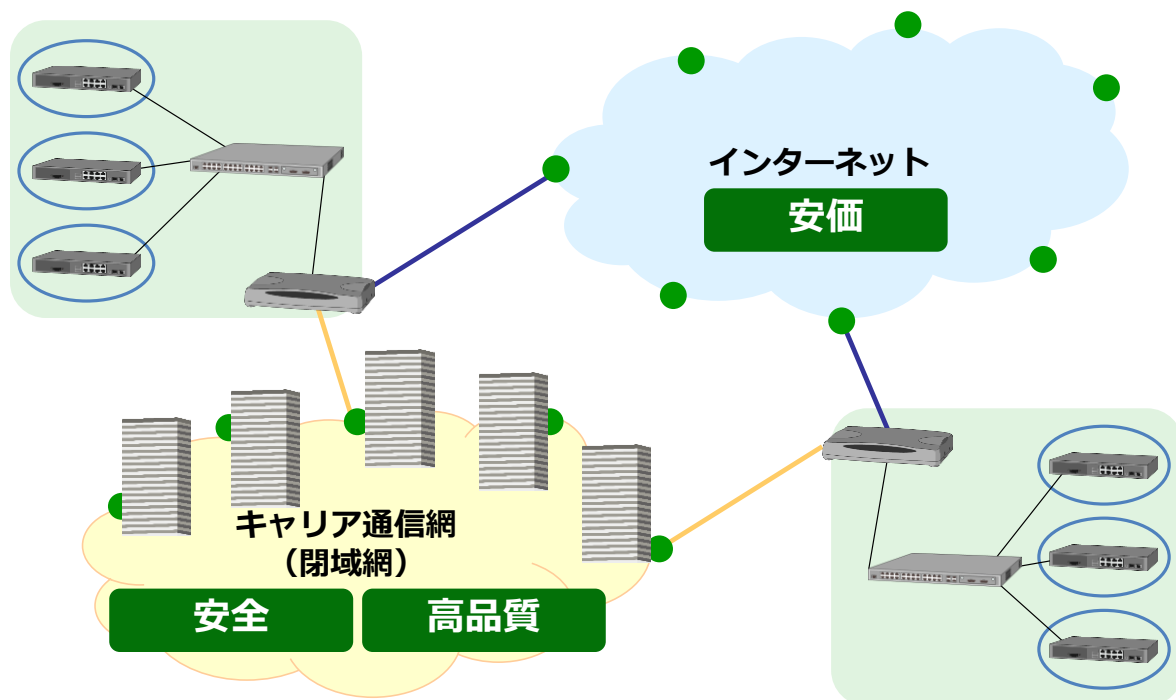
サービス例)インターネットVPN、IP-VPN、広域イーサネット

【参考】

電気通信事業者:

日本国内で電気通信事業を行うために総務省の認可を受けた事業者を指します。単に通信事業者、またはキャリアと呼ばれる場合もあります。

8.2 キャリア通信網とインターネット



ここでは、キャリア通信網とインターネットについて解説します。

WANサービスは、電気通信事業者が提供する通信網やインターネット上での通信を提供します。企業の拠点間でやり取りする通信内容には、機密情報を含むため安全で安定した通信が望まれます。

電気通信事業者が提供する通信網とインターネットの特徴を比較します。

- **キャリア通信網**(電気通信事業者が提供する通信網)

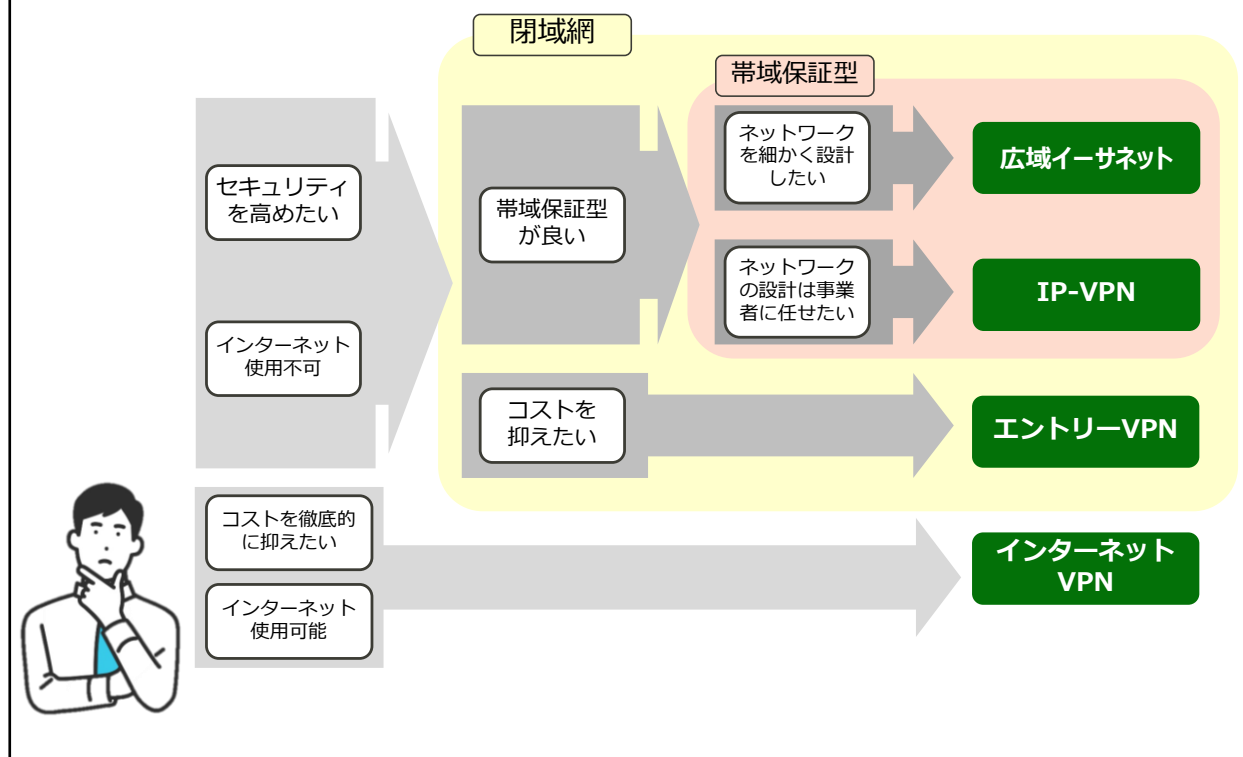
電気通信事業者がアクセスポイント(収容局)間で敷設している通信網です。電気通信事業者が利用者や通信量を制御しているため、安全で安定した通信が提供されますが、コストがかかります。閉域網と呼ぶ場合があります。

- **インターネット**

ベストエフォート型の通信網です。インターネットサービスプロバイダー(ISP)がアクセスポイントを提供しています。アクセスポイントの利用料金は発生しますが、通信網の使用料金はかからないため安価に使用できます。ただし、利用者や通信量の制御は行われないため、安全性や品質はキャリア通信網より劣ります。

次は、バックボーン区間のWANサービスの選定について解説します。

8.3 WANサービスの選定



WANサービスの選定では、要件を基に4つのバックボーン区間の中から選択します。

主に検討する項目としては下記項目があります。

・セキュリティ

セキュリティを高めたい通信かを検討します。セキュリティを高めたい場合は、電気通信事業者が管理している閉域網を使用します。セキュリティとコストはトレードオフの関係になっていることが多くあります。

・コスト

コストはイニシャルコストとランニングコストを合わせて検討します。WANはLANに比べ、コスト全体に占める、ランニングコストの比率が大きくなります。

コストを抑える場合にはインターネットVPNやエントリーVPNなどを使用します。ただし、インターネットVPNを使用するためには、社内ネットワークからインターネット接続が可能であることが必要です。

・通信品質

帯域保証すべき通信や、帯域制御を行うべき通信があるかを検討します。通信品質を高めたい場合には、帯域保証型のサービスを使用します。通信品質とコストはトレードオフの関係になっていることが多くあります。

・拠点数

拠点数が多いか、この先拠点数が増える予定があるのかを検討します。

拠点数が多い場合には、広域イーサネットやIP-VPNを使用します。エントリーVPNやインターネットVPNは最大接続数に上限が設けられているサービスがあるため、注意が必要です。広域イーサネットは自由度の高いネットワーク設計が可能な反面、拠点数増加によって、担当者の負荷が大きくなる場合があります。

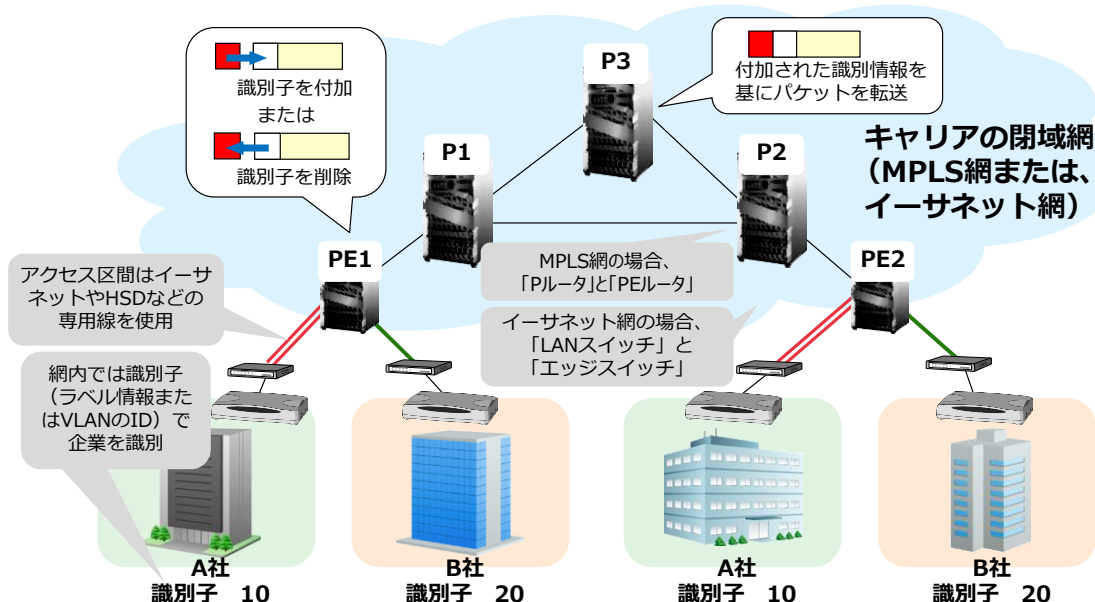
上記の内容にお客様からの要件を加え、総合的に検討します。

バックボーン区間選定後は、アクセス区間のサービスを選定します。アクセス区間では、使用できるサービスがバックボーン区間に依存するため、バックボーン区間の条件を確認します。

8.4 バックボーン区間

8.4.1 広域イーサネットとIP-VPN

- 電気通信事業者が利用者や通信量(帯域)を制御しているネットワーク
- WANのメイン回線として利用されることが多い
- 接続拠点数が多いネットワークで導入が多い



ここからは、バックボーン区間のWANサービスを解説します。

広域イーサネットとIP-VPNは、電気通信事業者が敷設した通信網(キャリア通信網)を利用するWANサービスです。一定の帯域を保証するなど高品質で安定した通信が可能です。

それぞれのサービス用の通信網を全国的に敷設しており、多数の拠点を接続する場合に向いています。アクセス区間は、帯域保証型のサービスを利用します。

■広域イーサネット

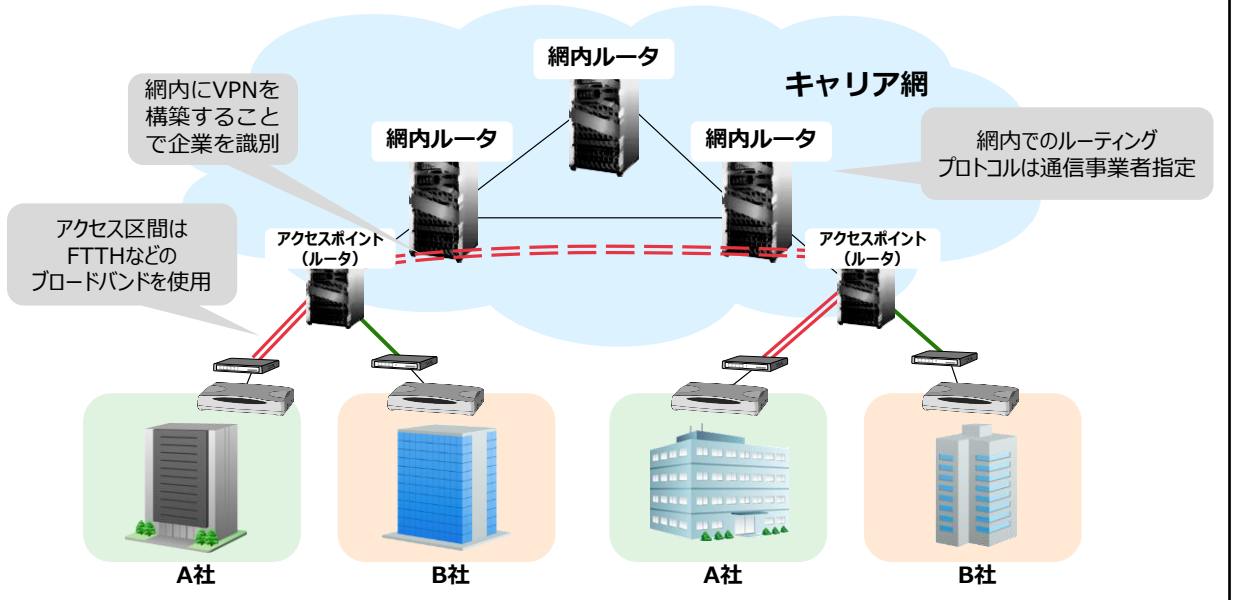
- イーサネット技術を用いたネットワーク
レイヤー2レベルで接続されるネットワークです。
- レイヤー3以上のプロトコルに制限がない。
IPとFNAなど複数のネットワークプロトコルを利用する場合に適しています。
- タグVLAN機能を利用して網内のユーザーを識別する。
拠点から流れてくるデータは、網内に入るとタグが付与され、独立した通信として扱われます。なお、タグの付け外しは電気通信事業者の機器で行うため、ユーザーは、特に意識する必要はありません。

■IP-VPN

- IP技術を用いたネットワーク
レイヤー3レベルで接続されるネットワークです。
- レイヤー3以上のプロトコルはTCP/IPに限定される。
IPとFNAなど複数のネットワークプロトコルを利用する場合は活用できません。
- MPLS (MultiProtocol Label Switching)を利用して網内のユーザーを識別する。
拠点から流れてくるデータは、網内に入るとラベルが付与され、転送先が制御されます。なお、ラベルの付け外しは電気通信事業者の機器で行うため、ユーザーは、特に意識する必要はありません。

8.4.2 エントリーVPN

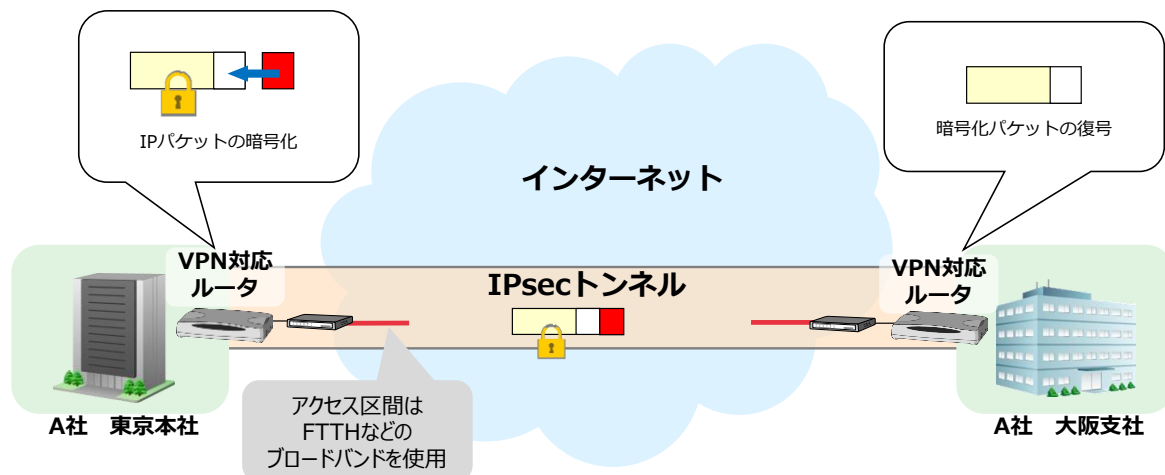
- キャリア通信網を利用し、拠点間接続するサービス
- インターネットVPNより安全性が確保される
- 料金が比較的安価
- 接続拠点数が少ないネットワークで導入が多い



エントリーVPNは、キャリア通信網を利用し、拠点間接続するサービスです。インターネットではなく、電気通信事業者が管理している通信網を利用するため、安全性(セキュリティ)が向上します。エントリーVPNで使用されている通信網はベストエフォート型であるため、比較的安価に拠点間接続を実現できます。また、アクセス区間には、ブロードバンド型のサービスを利用するため導入が容易です。

8.4.3 インターネットVPN

- インターネットを利用し、拠点間接続するサービス
- 安全性を確保するために、接続相手を認証し、通信データを暗号化する
- 料金が安価



インターネットVPNは、インターネットを利用し、拠点間接続するサービスです。インターネットの利用料金がかからないため、安価に拠点間接続を実現できます。ただし、インターネットには利用者制限や通信監視がされていないため、通信内容は、ユーザー側で保護する必要があります。インターネットVPNの多くは、**IPsec技術**を利用しています。

【用語解説】

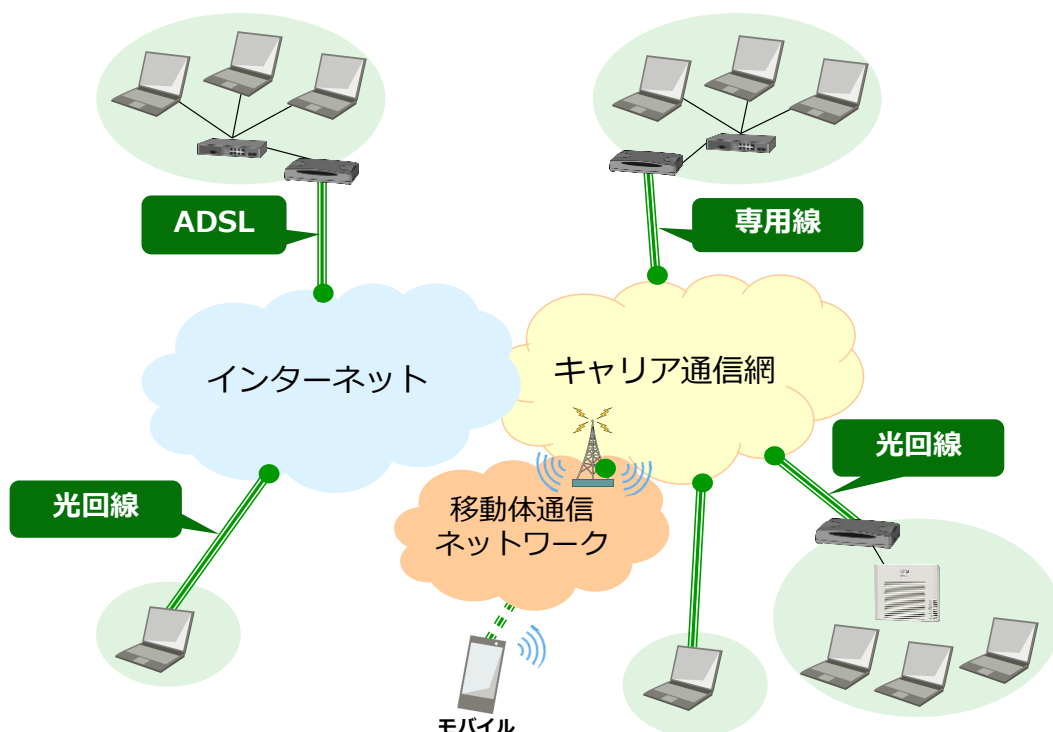
IPsec (Security Architecture for Internet Protocol):

IP通信を暗号化するプロトコル。通信を行う対向拠点が不正に偽装をしていないかを確認する「認証」。データが書き換わっていないか(改ざん)を調査する「改ざんチェック」、通信データを盗聴されないようにする「暗号化」がサポートされています。

次は、アクセス区間のWANサービスについて解説します。

8.5 アクセス区間

8.5.1 アクセス区間のサービスの種類



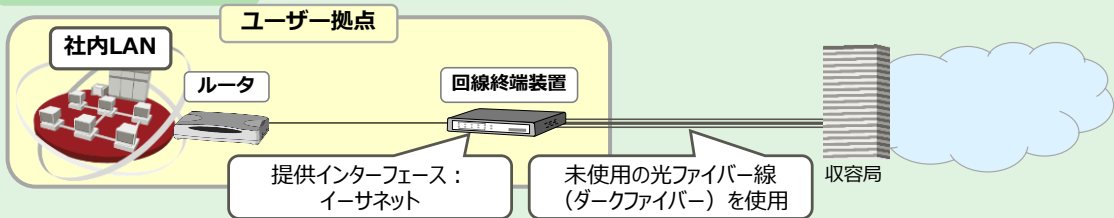
キャリア通信網(バックボーン区間)の終端である収容局、およびインターネットの終端であるアクセスポイントに接続するためには、拠点からの物理的な回線が必要です。これが**アクセス区間**です。

アクセス区間の通信品質を保証したい場合には**帯域保証型**のサービス、安価に通信を実現したい場合には**ブロードバンド型**のサービスを利用します。利用用途やネットワーク要件によって適するサービスを選択します。

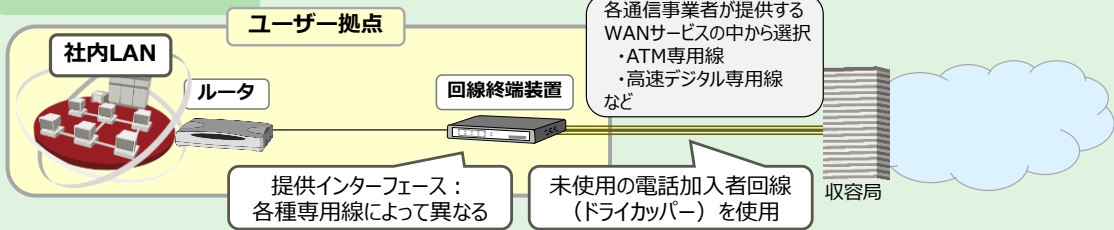
8.5.2 帯域保証型サービス

品質が保証されたサービスです

イーサネットタイプ



専用線タイプ



アクセス区間のサービスのうち、帯域保証型のサービスであるイーサネットタイプと専用線タイプについて説明します。

■ イーサネットタイプ

アクセスポイントとユーザー拠点の間にイーサネット専用線を設置し、回線上に直接イーサネットフレームを送出します。

物理回線には、一般的にダークファイバー（将来的な利用を見越して先行投資的に敷設されたものの、利用されていなかった光ファイバー）が活用されます。

帯域によって細かく料金が設定されています。専用線タイプの同等帯域のサービスに比べるとコストが低い場合が多いです。

提供事業者は、NTTグループ各社や電力系NCC各社があり、多くの選択肢があります。

■ 専用線タイプ

イーサネットフレームをWANの伝送単位にカプセル化して伝送します。

物理回線には、ドライカッパー（未使用の電話加入者回線）が活用されることが多いです。

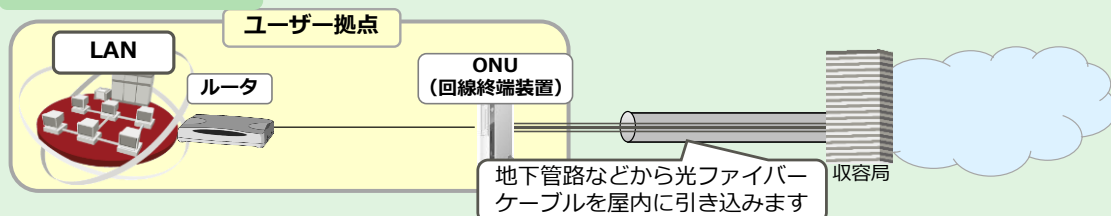
主なサービスとしてATM専用線や、デジタル専用線などがあります。

イーサネットタイプよりコストが高い場合が多いため、イーサネットタイプが利用できない地域で利用されます。

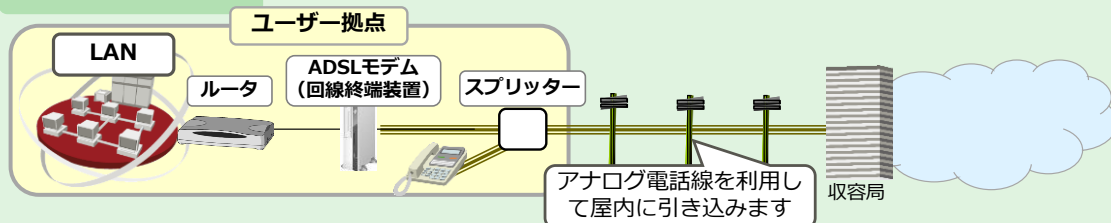
8.5.3 ブロードバンド型サービス

品質が保証されていないコスト重視のサービスです

光回線 (FTTH)



ADSL



ブロードバンドは、ベストエフォートかつ広帯域なアクセス区間のサービスに対する総称です。本来は個人利用者向けのサービスでしたが、回線速度の向上により企業の利用も広がっています。

■ FTTH (Fiber To The Home)

FTTHは光ファイバーを使ったデジタル通信サービスです。

最大10Gbpsのベストエフォート型通信ができます。そのため、元々は個人利用者向けのサービスでしたが、比較的高速でコストを抑えられるという点から企業のアクセス区間としても利用されることが多くなりました。

加入者宅から収容局までを光ファイバーで結ぶため、光ファイバーが敷設されていない地域ではサービスを利用できないという欠点があります。

企業向けサービスとして、グローバルIPアドレスの付与、24時間保守などのオプションがあるサービスもあります。

■ ADSL (Asynchronous Digital Subscriber Line)

ADSLはアナログ電話線を使ったデジタル通信サービスです。

FTTHと同様に元々は個人利用者向けのサービスでしたが、比較的高速でコストを抑えられるという点から企業のアクセス区間のサービスとしても利用されます。

既存の電話線を流用できるため、光ファイバーが敷設されていない地域でも、サービス利用が可能となっています。しかし、距離による信号の減衰が著しいため、収容局からの距離が長いと、通信速度は大きく低下します。

ADSLは上りと下りの帯域を非対称に設定し、下りの帯域を大きくしています。この特性は、情報を受動的に得る個人利用者や、中小規模組織の通信に適しています。

最近では、FTTHの普及や、無線系のインターネットの発達により、加入者は減少傾向にあります。

8.6 章のまとめ

- WANは、バックボーン区間とアクセス区間に区分されます。
- 主なバックボーン区間のWANサービスとして、広域イーサネット、IP-VPN、インターネットVPN、エントリーVPNがあります。
 - ✓ 広域イーサネット、IP-VPN : 高品質で安定した通信ができる
 - ✓ インターネットVPN、エントリーVPN : 安価に構築できる
- アクセス区間のWANサービスは、帯域保証型サービスとブロードバンド型サービスに分類できます。

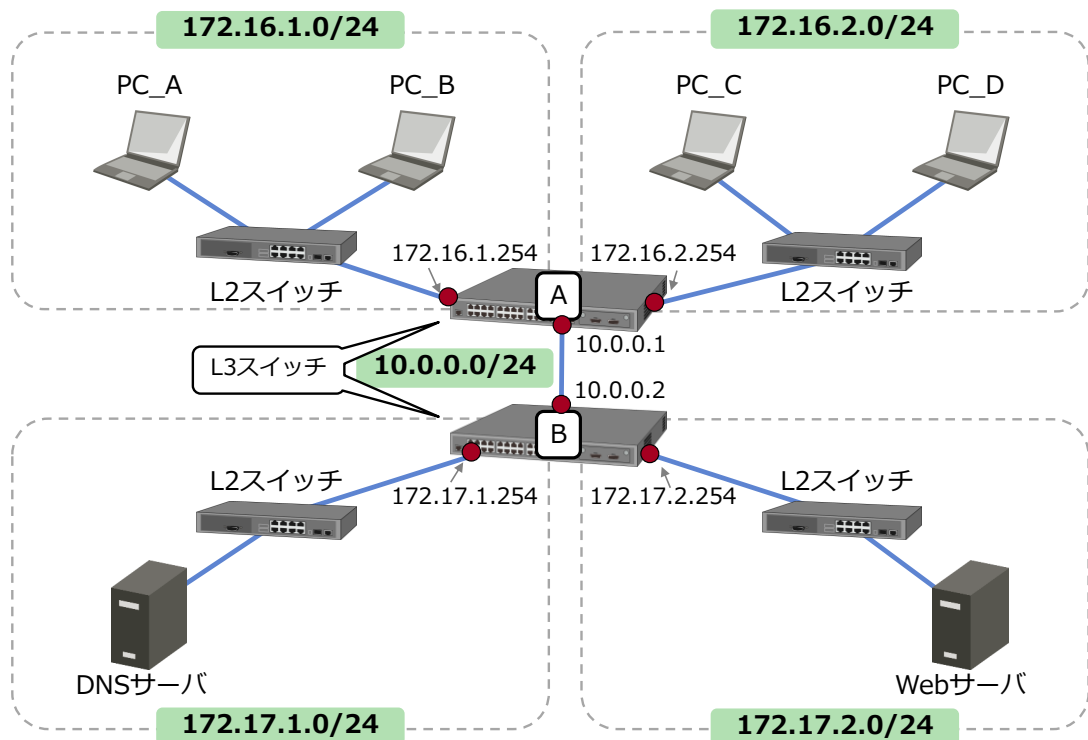
第8章のまとめです。

- WANは、バックボーン区間とアクセス区間に区分されます。
- 主なバックボーン区間のWANサービスとして、広域イーサネット、IP-VPN、インターネットVPN、エントリーVPNがあります。
 - ✓ 広域イーサネット、IP-VPN : 高品質で安定した通信ができる
 - ✓ インターネットVPN、エントリーVPN : 安価に構築できる
- アクセス区間のWANサービスは、帯域保証型サービスとブロードバンド型サービスに分類できます。

総合演習

学習したTCP/IP通信の総まとめです。
演習問題が解けるか力試ししてみましょう。
各問題に解答例があるので、参考にしてください。

【演習 1】 端末の設定値を考えよう



構成図に配置されている各端末からWebサーバへURLでアクセスする場合の各端末の設定値を考えてみましょう。なお、PC_A、PC_B、PC_C、PC_Dは、優先DNSサーバの設定値も考えてください。

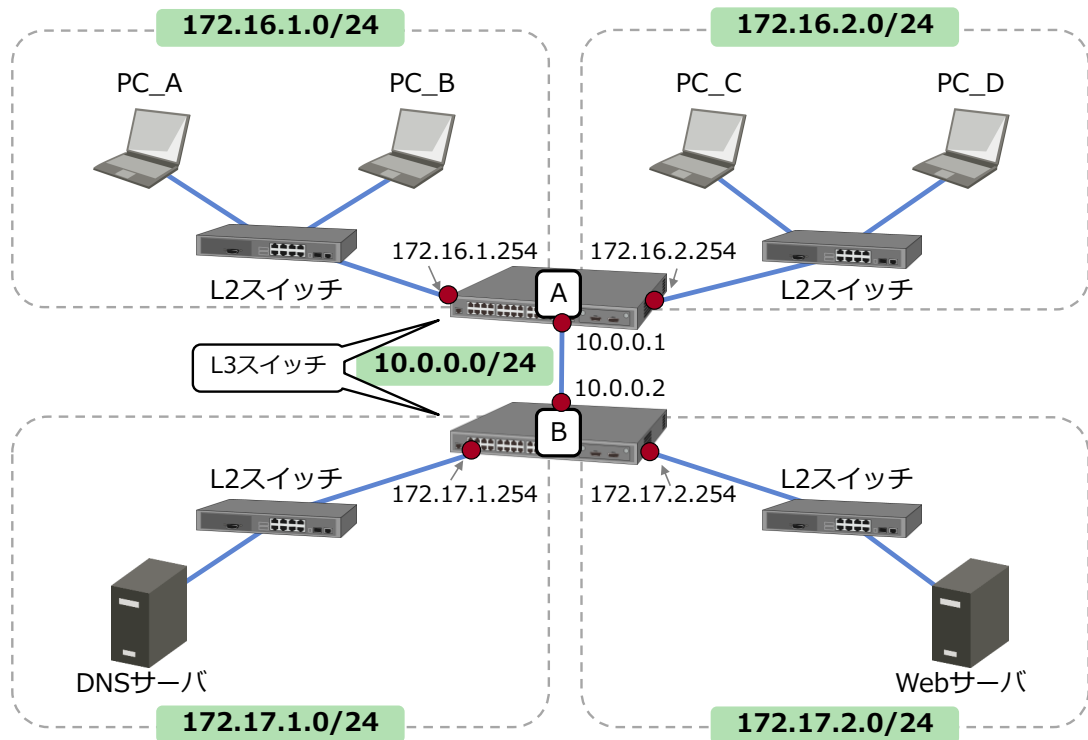
PC_A		PC_B	
IPアドレス		IPアドレス	
サブネットマスク		サブネットマスク	
デフォルトゲートウェイ		デフォルトゲートウェイ	
優先DNSサーバ		優先DNSサーバ	
PC_C		PC_D	
IPアドレス		IPアドレス	
サブネットマスク		サブネットマスク	
デフォルトゲートウェイ		デフォルトゲートウェイ	
優先DNSサーバ		優先DNSサーバ	
DNSサーバ		Webサーバ	
IPアドレス		IPアドレス	
サブネットマスク		サブネットマスク	
デフォルトゲートウェイ		デフォルトゲートウェイ	

【演習 1】 端末の設定値を考えよう（解答例）

PC_A		PC_B	
IPアドレス	172.16.1.101	IPアドレス	172.16.1.102
サブネットマスク	255.255.255.0	サブネットマスク	255.255.255.0
デフォルトゲートウェイ	172.16.1.254	デフォルトゲートウェイ	172.16.1.254
優先DNSサーバ	172.17.1.10	優先DNSサーバ	172.17.1.10
PC_C		PC_D	
IPアドレス	172.16.2.101	IPアドレス	172.16.2.102
サブネットマスク	255.255.255.0	サブネットマスク	255.255.255.0
デフォルトゲートウェイ	172.16.2.254	デフォルトゲートウェイ	172.16.2.254
優先DNSサーバ	172.17.1.10	優先DNSサーバ	172.17.1.10
DNSサーバ		Webサーバ	
IPアドレス	172.17.1.10	IPアドレス	172.17.2.10
サブネットマスク	255.255.255.0	サブネットマスク	255.255.255.0
デフォルトゲートウェイ	172.17.1.254	デフォルトゲートウェイ	172.17.2.254

【演習1】 の解答例です。

【演習 2】経路制御装置のルーティングテーブルを考えよう



構成図に配置されている経路制御装置（L3スイッチ）のルーティングテーブルの設定を考えます。ネットワーク上にあるすべてのコンピュータ同士で疎通確認が行えるよう、構成図内のL3スイッチAおよびL3スイッチBのルーティングテーブルについて必要な経路情報を考えてください。直接接続の場合は、Next Hopに「Direct」と記載してください。

	宛先ネットワーク	Next Hop
L3スイッチ_A		

	宛先ネットワーク	Next Hop
L3スイッチ_B		

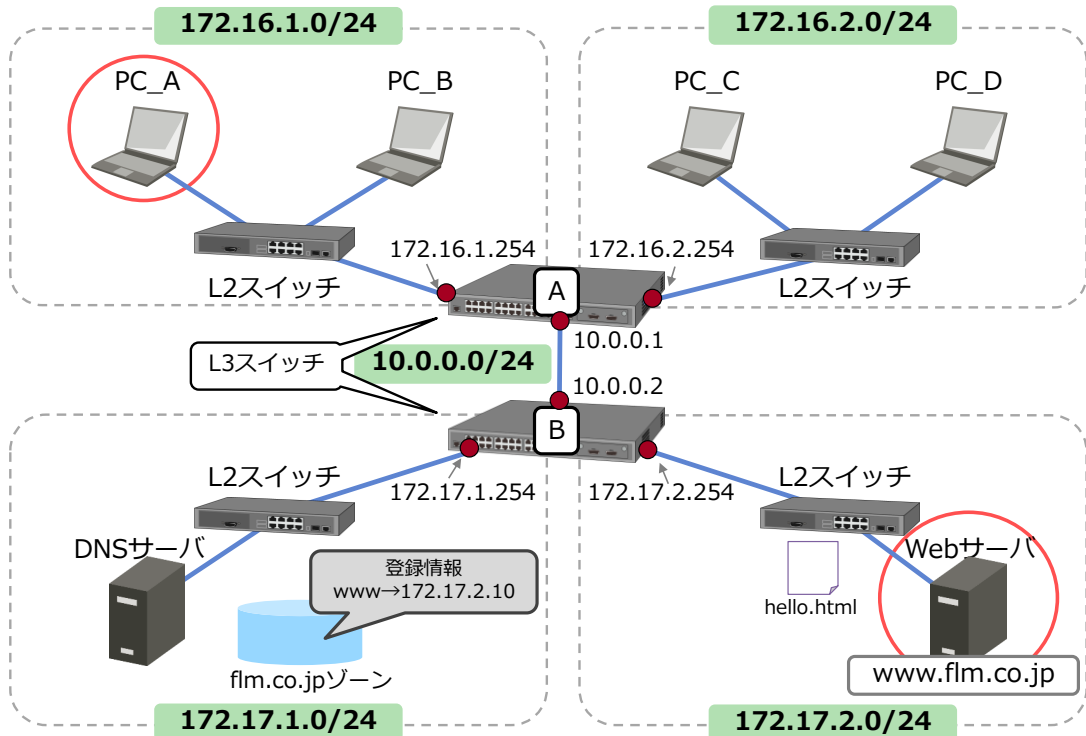
【演習 2】 経路制御装置のルーティングテーブルを考えよう（解答例）

L3スイッチ_A	宛先ネットワーク	Next Hop
	172.16.1.0/24	Direct
	172.16.2.0/24	Direct
	10.0.0.0/24	Direct
	172.17.1.0/24	10.0.0.2
	172.17.2.0/24	10.0.0.2

L3スイッチ_B	宛先ネットワーク	Next Hop
	172.17.1.0/24	Direct
	172.17.2.0/24	Direct
	10.0.0.0/24	Direct
	172.16.1.0/24	10.0.0.1
	172.16.2.0/24	10.0.0.1

【演習2】の解答例です。

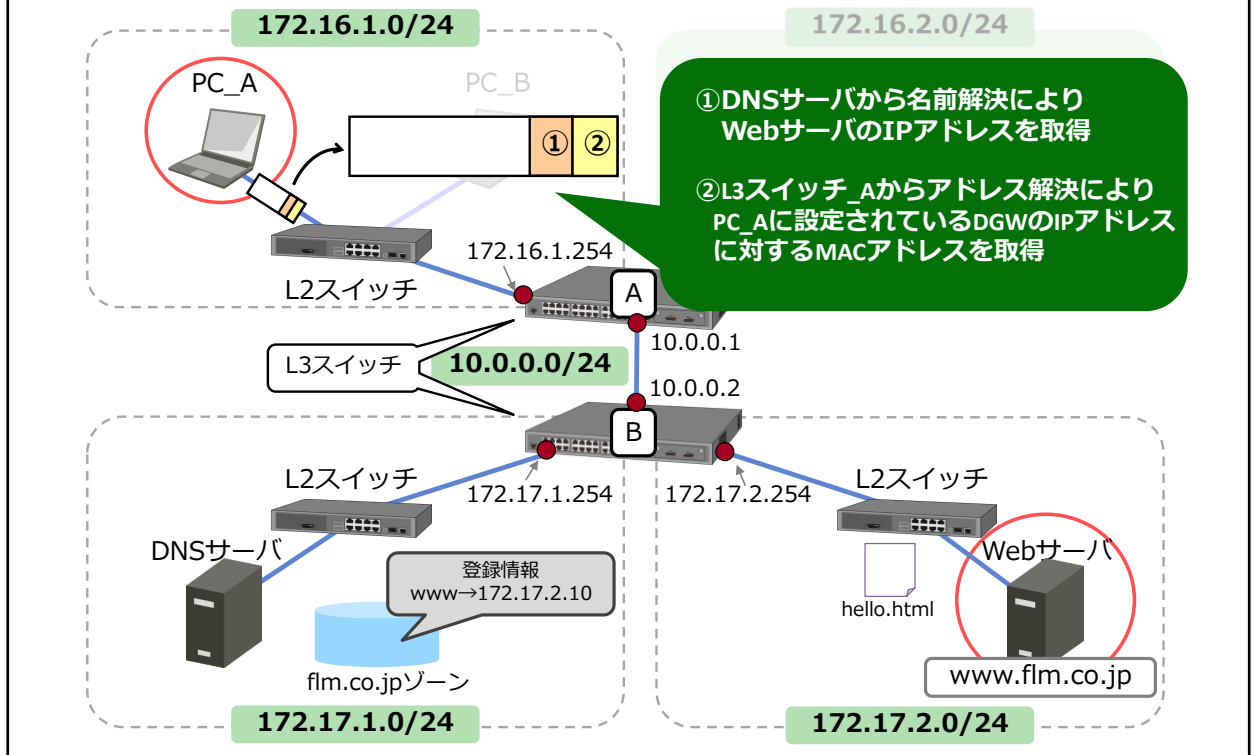
【演習3】Webサーバへの通信フローを考えよう



この構成図において、PC_AからWebサーバまでの通信フローを考えます。

- ① PC_AがWebサーバにHTTPアクセスを行います。httpリクエストに対する**インターネット層のヘッダー**を付与するために、PC_Aは事前にどの装置から何の情報を取得する必要がありますか？
- ② PC_AはWebサーバにhttpリクエストを送信します。**ネットワークインターフェース層のヘッダー**を付与するために、PC_Aは事前にどの装置から何の情報を取得する必要がありますか？

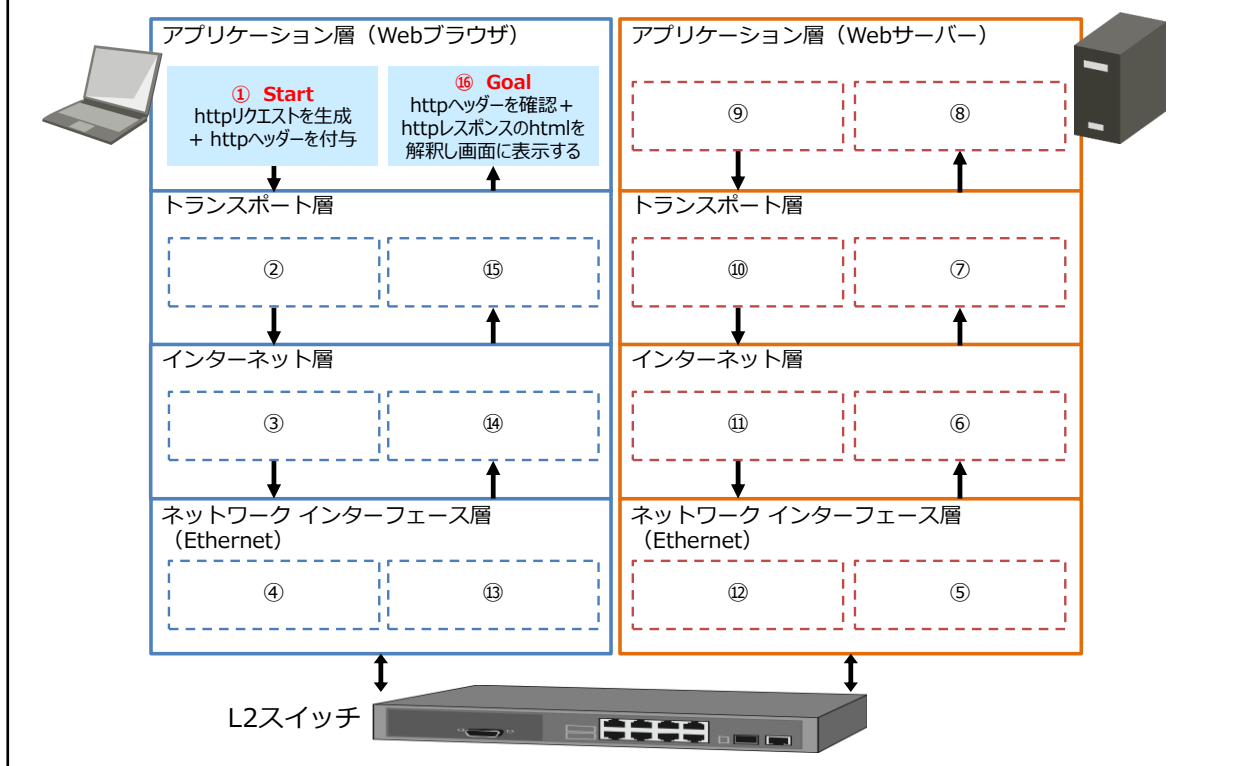
【演習3】Webサーバへの通信フローを考えよう（解答例）



【演習3】の解答例です。問題文を再掲します。
この構成図において、PC_AからWebサーバまでの通信フローを考えます。

- ① PC_AがWebサーバにHTTPアクセスを行います。httpリクエストに対する**インターネット層のヘッダー**を付与するために、PC_Aは事前にどの装置から何の情報を取得する必要がありますか？
- ② PC_AはWebサーバにhttpリクエストを送信します。**ネットワークインターフェース層のヘッダー**を付与するために、PC_Aは事前にどの装置から何の情報を取得する必要がありますか？

【演習 4 - 1】 TCP/IP通信の階層の流れを考えよう

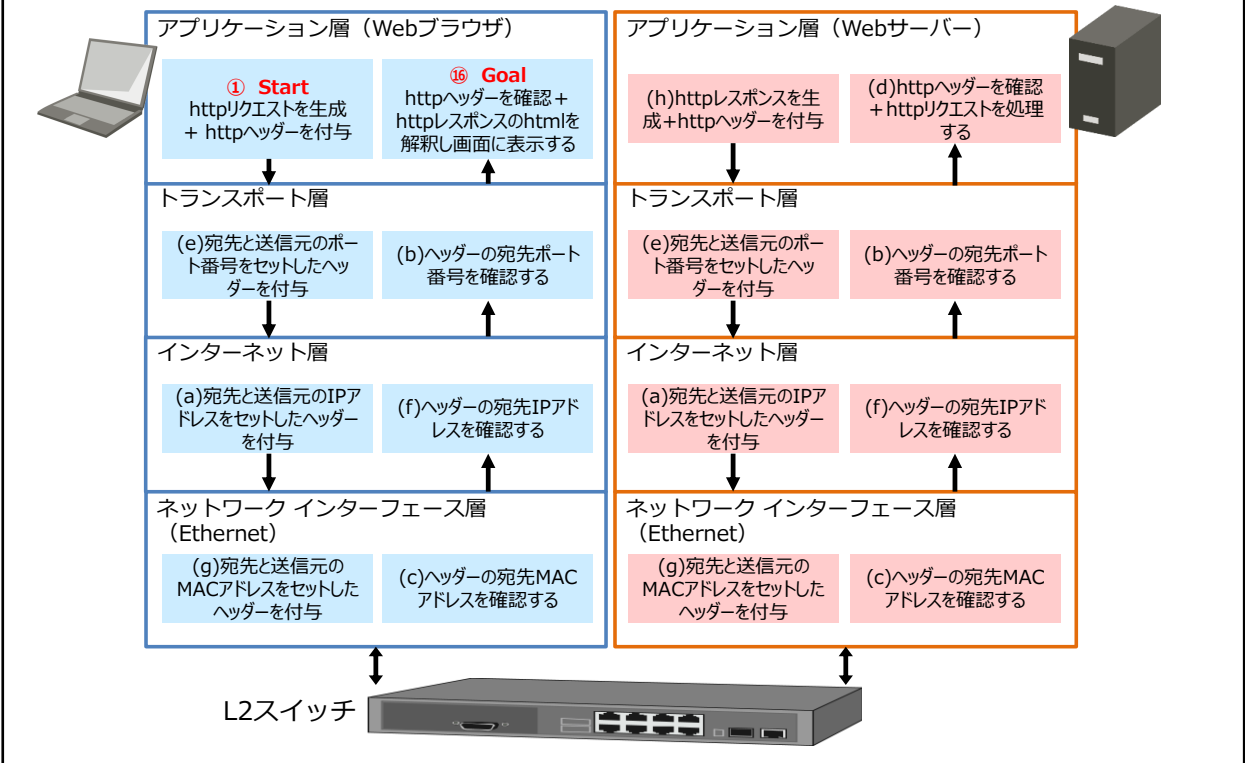


クライアントからWebサーバへのHTTP通信時におけるTCP/IPの階層の流れを考えます。
図の②～⑮に当てはまるものを下記の選択肢から選んでください。

<選択肢> ※選択肢の中には複数回使用するものもあります。

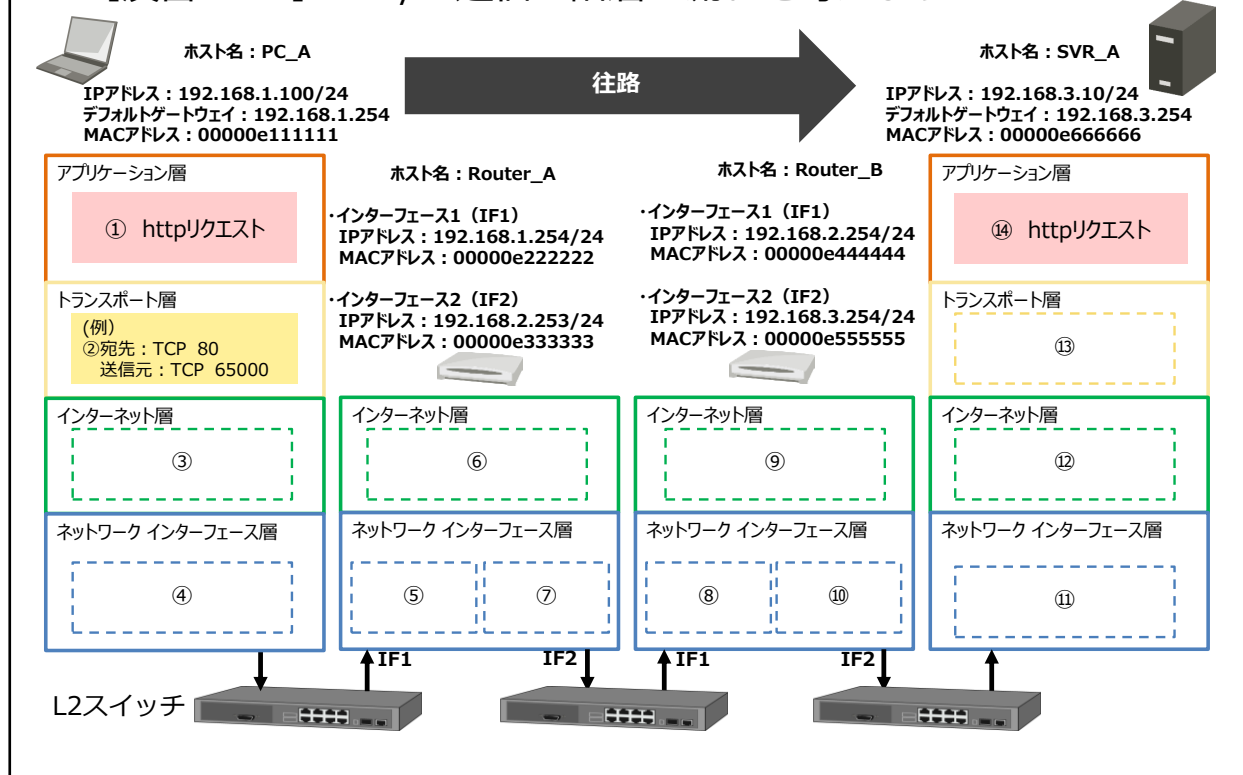
- (a) 宛先と送信元のIPアドレスをセットしたヘッダーを付与
- (b) ヘッダーの宛先ポート番号を確認する
- (c) ヘッダーの宛先MACアドレスを確認する
- (d) httpヘッダーを確認 + httpリクエストを処理する
- (e) 宛先と送信元のポート番号をセットしたヘッダーを付与
- (f) ヘッダーの宛先IPアドレスを確認する
- (g) 宛先と送信元のMACアドレスをセットしたヘッダーを付与
- (h) httpレスポンスを生成 + httpヘッダーを付与

【演習 4 - 1】 TCP/IP通信の階層の流れを考えよう（解答例）



【演習4-1】の解答例です。

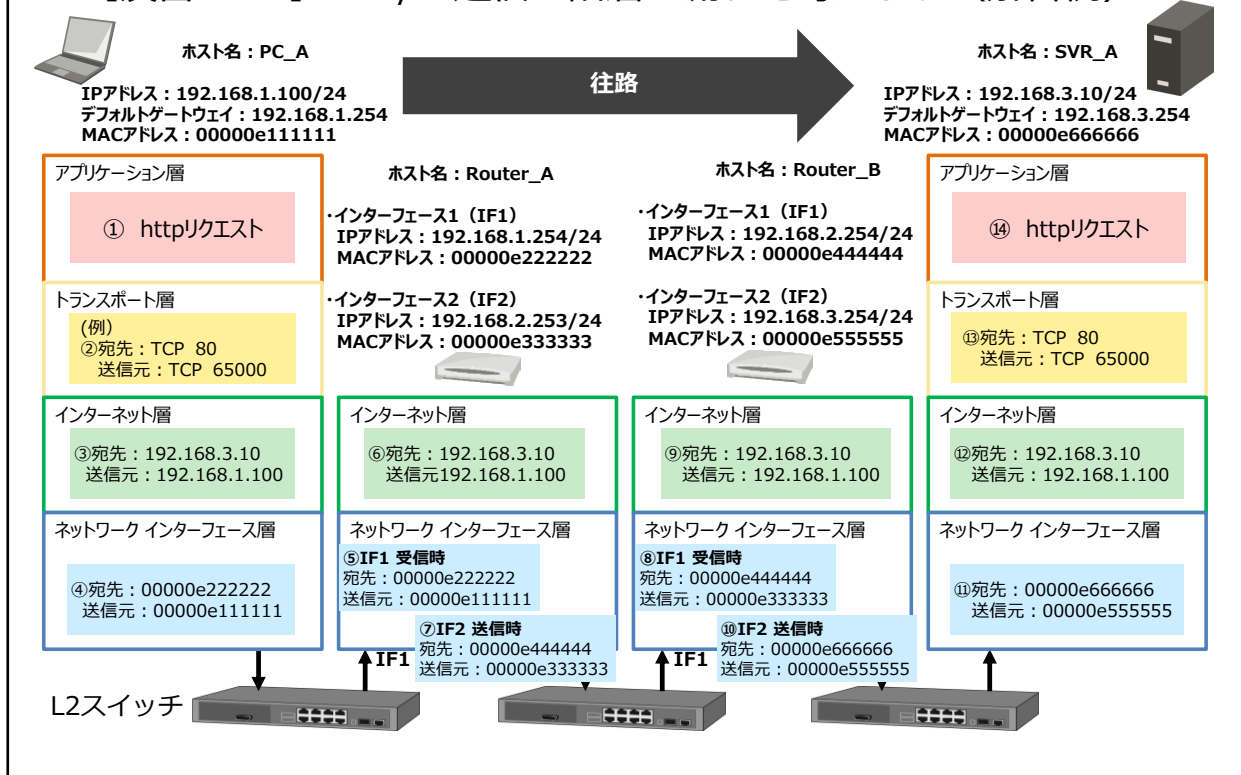
【演習 4 - 2】 TCP/IP通信の階層の流れを考えよう



図はクライアントからWebサーバへのHTTP通信時（往路）におけるTCP/IPの各階層のヘッダーを表しています。図の③～⑬に当てはまるものとして適切なヘッダー情報（宛先・送信元情報）を考えてください。

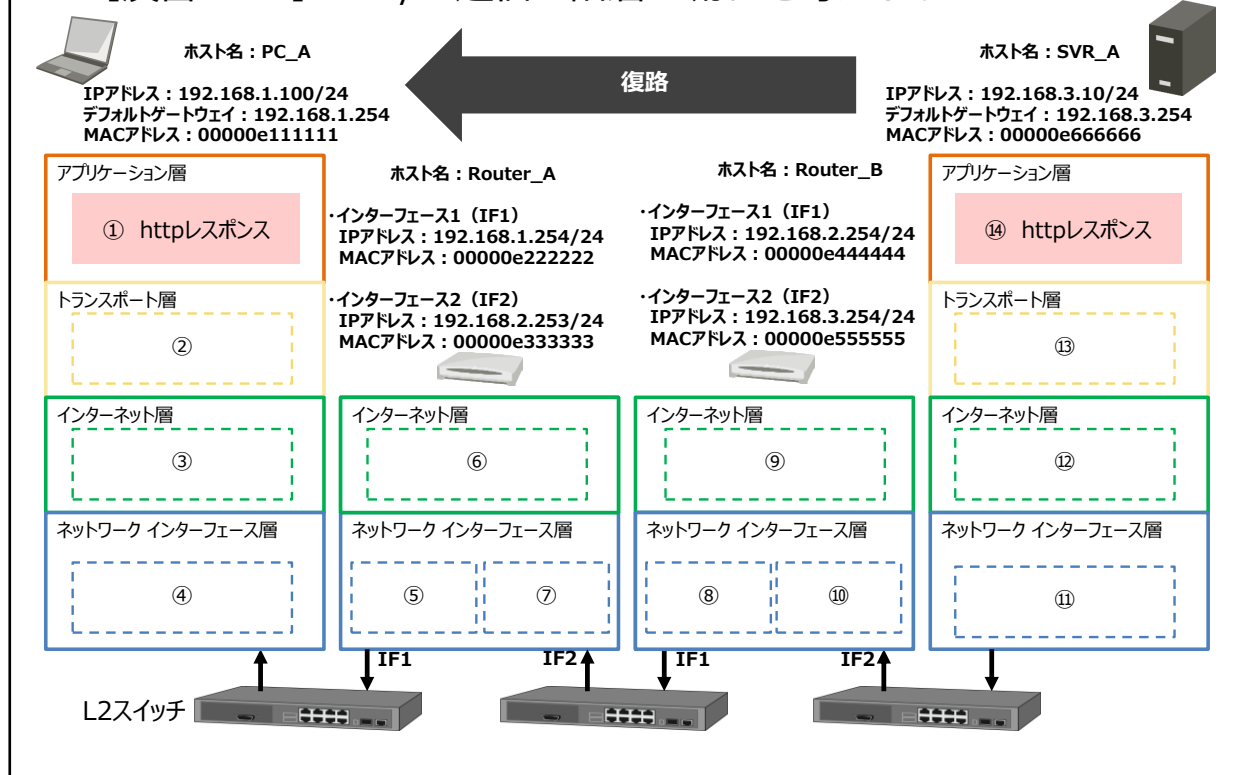
なお、PC_Aのブラウザのポート番号は65000とします。ルータは受信時と送信時それぞれのヘッダーを考えてください。

【演習 4 - 2】 TCP/IP通信の階層の流れを考えよう（解答例）



【演習4-2】の解答例です。

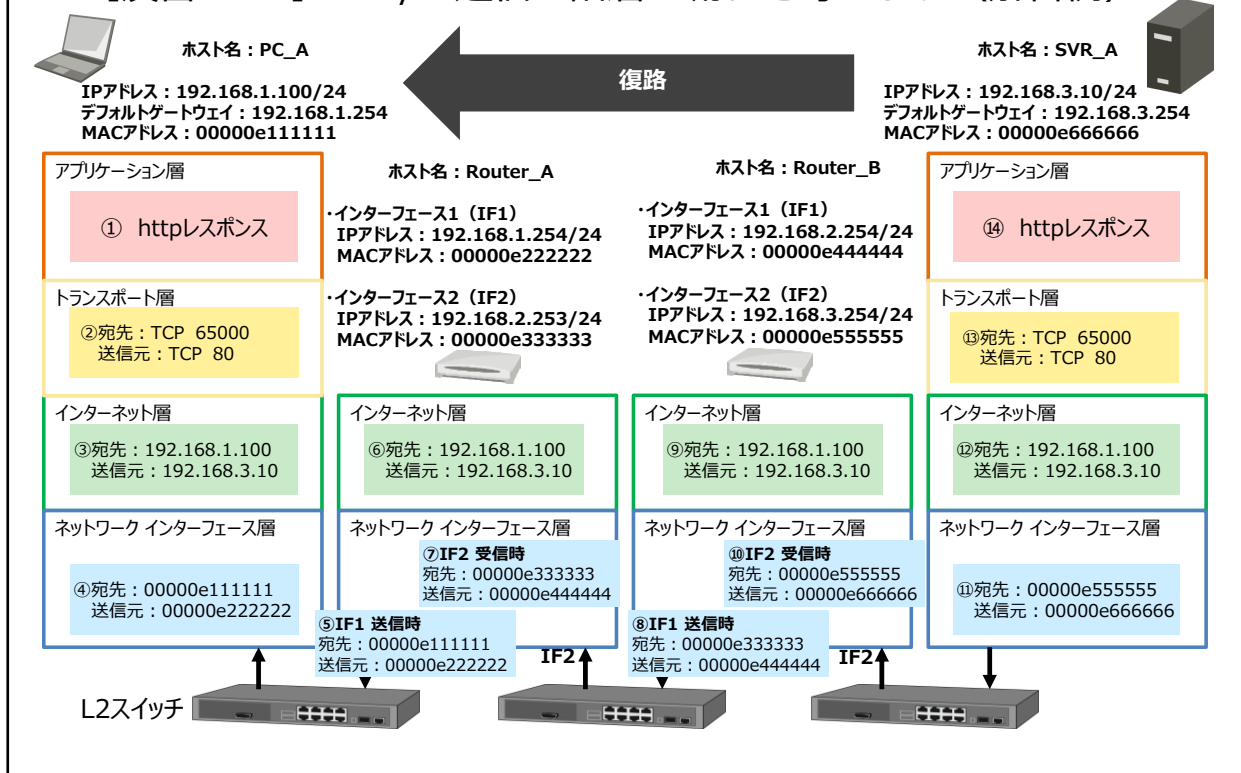
【演習 4 - 3】 TCP/IP通信の階層の流れを考えよう



図はクライアントからWebサーバへのHTTP通信時（復路）におけるTCP/IPの各階層のヘッダーを表しています。図の②～⑬に当てはまるものとして適切なヘッダー情報（宛先・送信元情報）を考えてください。

なお、PC_Aのブラウザのポート番号は65000とします。ルータは受信時と送信時それぞれのヘッダーを考えてください。

【演習 4 - 3】 TCP/IP通信の階層の流れを考えよう（解答例）



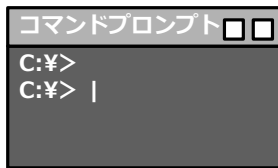
【演習4-3】の解答例です。

付録

コマンド (Windows コマンドプロンプト)

【付録1】 Windows OSのコマンド操作方法

本コースでは、Windowsのコマンドプロンプトを用いたコマンド操作にて演習手順を解説します。端末の設定やネットワーク接続状況に応じて、実行結果が異なることをあらかじめご了承ください。



画面内にコマンドを入力し、[Enter]キーで実行します。入力したコマンドに応じて、コンピュータ設定の確認や変更が可能です。本コースでは、ネットワーク設定の確認に使用します。※コマンドの詳細は、「コマンド紹介ページ」にて解説します。（付録にもまとめています。）

コマンドプロンプトを起動 コマンドプロンプト画面（イメージ）

Windowsのコマンド操作方法

操作の流れ	手順詳細
手順1. 事前準備 (コマンドプロンプトを起動) ※起動手順は複数あります。	<ul style="list-style-type: none">・ [Windowsロゴ]キーと[R]キーを同時に入力する。・ [ファイル名を指定して実行]の画面で、「cmd」を入力し[OK]を選択する。・ コマンドプロンプト (cmd.exe) を起動する。
手順2. コマンド入力し実行	<ul style="list-style-type: none">・ 起動した[コマンドプロンプト]の画面の「>」（大なり表示）の後ろに、コマンド（例. 「netstat -n」）を入力する・ [Enter]キーでコマンドを実行する
手順3. コマンド結果を確認	<ul style="list-style-type: none">・ コマンドの実行結果が表示される (例. netstatコマンドの場合は、端末のアクティブなTCP接続が表示される)

ここでは、Windows端末のコマンド操作方法について確認します。
Windows OSでは、「コマンドプロンプト」を起動し、画面内に入力したコマンドに応じて、コンピュータ設定の確認や変更が可能です。コマンドの詳細はコマンド紹介ページにて解説します。

※注意
操作端末の設定やネットワーク接続状況に応じてコマンド実行結果が異なります。実行例が実際の結果とは異なる場合があることをご了承ください。

【付録2】 <コマンド紹介> netstat コマンド

```
>  
> netstat -n
```

“ netstat -n ”と入力
※“netstat”と“-n”の間には、
空白（ブランク）が必要

ポート番号は、コロン（:）の後ろに表示される
・[ローカルアドレス]側は 送信元情報
・[外部アドレス]側は 宛て先情報

アクティブな接続

プロトコル	ローカル アドレス	外部アドレス	状態
TCP	172.16.1.10:49181	172.200.1.10:80	TIME_WAIT
TCP	172.16.1.10:49198	172.16.1.100:80	ESTABLISHED
TCP	172.16.1.10:49209	172.20.20.20:21	ESTABLISHED
TCP	172.16.1.10:49212	172.100.1.10:1048	ESTABLISHED

アクティブなTCP接続が1行ずつ表示される

[プロトコル]、[ローカルアドレス]、[外部アドレス]、
[状態]が、1行で表示され、接続情報が確認可能

表示される内容は以下の通りです。

- ・[プロトコル] → TCPかUDPか示す（基本はTCPと表示）
- ・[ローカルアドレス] → 送信元側（自側）IPとポート（詳細は5章）
- ・[外部アドレス] → 宛先側（対向側）IPとポート（詳細は5章）
- ・[状態] → 接続状態（表示内容はOSに依存）

ここでは、netstatコマンドを紹介します。

netstatコマンドは、TCP/IPのセッション情報を表示します。アクティブなTCP接続、コンピュータが待ち状態のポート、イーサネット統計情報、IPルーティングテーブル、TCP/IP統計情報を表示します。

<構文>

netstat 各オプション

<主なオプション>

- n : セッション中のローカルコンピュータと宛て先コンピュータのIPアドレスとポート番号を表示します。
- e : 送受信データの統計情報を表示します。
- s **プロトコル名** : プロトコルごとの統計情報を表示します。デフォルトではTCP、UDP、ICMP、IPの統計情報が表示されます。
- r : ローカルコンピュータのルーティングテーブルを表示します。

【参考】

実行結果には、デスクトップに表示されていないアプリケーションの通信や、実際のWebサーバとは異なる別のサーバを経由した通信もアクティブなTCP接続として表示されます。

【付録3】 <コマンド紹介> ipconfigコマンド

```
> ipconfig /all
```

Windows IP 構成
(中略)

イーサネット アダプター ローカル エリア接続:

```
接続固有の DNS サフィックス . . . . :  
物理アドレス . . . . . : 00-00-0E-AA-BB-CC  
DHCP 有効 . . . . . : いいえ  
自動構成有効 . . . . . : はい  
リンクローカル IPv6 アドレス . . . : fe80::9855:abab:cddc:efef%10 (優先)  
IPv4 アドレス . . . . . : 172.16.1.15 (優先)  
サブネット マスク . . . . . : 255.255.255.0  
デフォルト ゲートウェイ . . . . . : 172.16.1.1  
DHCPv6 IAID . . . . . : 012345678  
DHCPv6 クライアント DUID . . . . . : 00-01-00-01-12-AB-CD-EF-00-12-3...  
DNS サーバー . . . . . : 172.16.200.2  
                        172.20.200.2  
NetBIOS over TCP/IP . . . . . : 有効  
(以下略)
```

複数のアダプター情報が表示されるため注意する必要がある

※図中の主な項目について

- ・物理アドレス → MACアドレス (物理インターフェースを識別)
- ・IPv4アドレス → IPアドレスが表示 (IPv4とIPv6は後ほど)
- ・サブネットマスク → サブネットマスク
- ・デフォルトゲートウェイ → デフォルトゲートウェイ
- ・DNSサーバ → DNSサーバ (DNSについては後ほど)

ここでは、ipconfigコマンドを紹介します。

ipconfigコマンドは、現在のTCP/IP構成を表示します。このユーティリティを使うと、DHCPサーバにより割り当てられたTCP/IP構成を手動で開放および更新することもできます。オプションを指定せずに実行すると、すべてのアダプターのIPアドレス、サブネットマスク、デフォルトゲートウェイが表示されます。

<構文>

ipconfig

<主なオプション>

/all

: すべてのアダプターの完全なTCP/IP構成を表示します。

/renew アダプター

: アダプターが指定されていなければすべてのアダプターのDHCP構成を更新します。アダプターが指定されていれば指定されたアダプターのDHCP構成を更新します。

/release アダプター

: DHCPRELEASEメッセージをDHCPサーバに送信して、アダプターが指定されていなければすべてのアダプターの、アダプターが指定されていれば指定されたアダプターのDHCP構成を開放し、IPアドレス構成を破棄します。

<使い方>

コマンド結果をテキストファイルとして保存するには、以下のコマンドを入力します。

コマンド > ディレクトリ¥ファイル名

例: **ipconfig /all > C:¥Users¥FLM¥Desktop¥ipconfig.txt**

(「FLM」ユーザーのデスクトップにipconfig /allの結果をipconfig.txtという名前のテキストファイルで保存する)

【付録4】 <コマンド紹介> pingコマンド

疎通確認に成功する場合、図のような実行結果が表示される

```
> ping 172.16.1.1
```

※疎通確認に失敗した場合は以下が表示される

- ・タイムアウトの場合：「要求がタイムアウトしました。」
- ・到達不可の場合：「宛先ネットワークに到達できません。」

```
172.16.1.1 に ping を送信しています 32 バイトのデータ：
172.16.1.1 からの応答： バイト数 =32 時間 =1ms TTL=255
172.16.1.1 からの応答： バイト数 =32 時間 =1ms TTL=255
172.16.1.1 からの応答： バイト数 =32 時間 =1ms TTL=255
172.16.1.1 からの応答： バイト数 =32 時間 =1ms TTL=255
```

```
172.16.1.1 の ping 統計：
```

```
    パケット数：送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒)：
    最小 = 1ms、最大 = 9ms、平均 = 3ms
```

ここでは、pingコマンドを紹介します。

pingコマンドは、IP接続の構成を確認し、IP接続をテストします。ネットワーク上の別のコンピュータへのIPレベルの接続を確認します。IPv4かIPv6かはアドレスから自動的に判断します。

<構文>

ping 各オプション 宛て先アドレス(ホスト名)

<主なオプション>

- t** : 連続的に疎通確認を行います。強制終了するには、Ctrlキーを押しながらCキーを押します。
- a** : IPアドレスをホスト名に解決して、疎通確認を行います。
- n 数値** : 入力した数値分(要求の回数)のデータを送信します。
- l 数値** : 入力した数値の容量(単位：バイト)の データを送信します。(容量はpingのヘッダーを除く)

ホスト名 : ホスト名に対して疎通確認を行います。

※疎通確認の失敗例はこちらです。

```
> ping 172.16.1.100
```

```
172.16.1.100 に ping を送信しています 32 バイトのデータ：
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
```

```
172.16.1.100 の ping 統計：
```

```
    パケット数：送信 = 4、受信 = 0、損失 = 4 (100% の損失)、
```

```
> ping 172.17.1.100
```

```
172.17.1.100 に ping を送信しています 32 バイトのデータ：
172.16.1.1 からの応答： 宛先ネットワークに到達できません。
172.16.1.1 からの応答： 宛先ネットワークに到達できません。
172.16.1.1 からの応答： 宛先ネットワークに到達できません。
172.16.1.1 からの応答： 宛先ネットワークに到達できません。
```

```
172.17.1.100 の ping 統計：
```

```
    パケット数：送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
```

【付録5】 <コマンド紹介> routeコマンド

>route PRINT
(中略)
IPv4 ルート テーブル

※図中の主な項目について
・ネットワーク宛先 → 宛先ネットワーク
・ネットマスク → サブネットマスク
・ゲートウェイ → 宛て先ネットワークに到達するための
次のルータのIPアドレス

アクティブ ルート:

ネットワーク宛先	ネットマスク	ゲートウェイ	インターフェイス	メトリック
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.99	20
192.168.0.0	255.255.255.0	リンク上	192.168.0.99	276
192.168.0.99	255.255.255.255	リンク上	192.168.0.99	276
192.168.0.255	255.255.255.255	リンク上	192.168.0.99	276
127.0.0.0	255.0.0.0	リンク上	127.0.0.1	306
127.0.0.1	255.255.255.255	リンク上	127.0.0.1	306
127.255.255.255	255.255.255.255	リンク上	127.0.0.1	306
224.0.0.0	240.0.0.0	リンク上	127.0.0.1	306
224.0.0.0	240.0.0.0	リンク上	192.168.0.99	276
255.255.255.255	255.255.255.255	リンク上	127.0.0.1	306
255.255.255.255	255.255.255.255	リンク上	192.168.0.99	276

固定ルート:
なし

ここでは、routeコマンドを紹介します。

routeコマンドは、ルーティングテーブルの内容表示と変更を行います。ルーティングテーブルでは、宛て先IPアドレスやネットワークアドレスに応じた転送先の経路情報を管理します。「ゲートウェイ」の列が「リンク上」と表示される行は、端末と同一ネットワークの経路情報です。

<構文>

route 各オプション

<主なオプション>

print : ルーティングテーブルを表示します。

add 宛て先アドレス 転送先アドレス : 宛て先アドレス（または宛て先ネットワークアドレス）に対応する転送先の経路情報をルーティングテーブルに追加します。

deletet 宛て先アドレス 転送先アドレス : 宛て先アドレス（または宛て先ネットワークアドレス）に対応する転送先の経路情報をルーティングテーブルから削除します。

-4 : IPv4に対する操作を指定します。

-6 : IPv6に対する操作を指定します。

【付録6】 <コマンド紹介> tracertコマンド

```
> tracert 192.168.1.10
```

192.168.1.10 へのルートをトレースしています。
経由するホップ数は最大 30 です

1	12 ms	1 ms	1 ms	172.16.1.1
2	1 ms	1 ms	1 ms	172.17.2.1
3	1 ms	1 ms	1 ms	192.168.1.10

トレースを完了しました。

コマンドで指定したIPアドレスまでの通信経路が調査できる
本図の場合では、以下を経由したことが判明する

・経由1つ目：172.16.1.1

・経由2つ目：172.17.2.1

※最後の行には目的端末との通信結果が表示される

※セキュリティ的に問題なく経路上から応答が届く場合、
表示される

ここでは、tracertコマンドを紹介します。

tracertコマンドは、データが宛て先に到達するまでに経由するルートを追跡します。送信元端末と宛て先端末の間にあるルータのアドレスが一覧表示されます。

<構文>

tracert 各オプション 宛て先アドレス

<主なオプション>

-d IPアドレス : ホスト名とIPアドレスの名前解決をしないように指定します。

ホスト名 : 宛て先ホスト名までの経路を判断します。このとき、ホスト名とIPアドレスの名前解決が行われ、IPアドレスも表示されます。

【付録7】 <コマンド紹介> nslookupコマンド

```
> nslookup server1.flm.local ns1.flm.local
```

サーバー: ns1.flm.local

Address: 172.20.100.2

上段には使用した
DNSサーバアドレスが
表示される

権限のない回答:

名前: server1.flm.local

Address: 172.18.100.1

本コマンドにて、指定したDNSサーバに
名前解決した結果が表示される

※図の場合、DNSサーバ: ns1.flm.localを指定して、
server1.flm.localの名前解決を行っている

下段の実行結果から以下が読み取れる

- ・名前: server1.flm.local の名前解決を行い、
IPアドレス: 172.18.100.1が解決された



【参考】

実行環境に応じて、「権限のない回答」の
表示や、名前解決結果自体表示されない
場合もあります。

ここでは、nslookupコマンドを紹介します。

nslookupコマンドは、DNSクライアントの名前解決機能を手動実行します。ホスト名の後ろにDNSサーバ名を入力することで、問い合わせを行うDNSサーバを指定することもできます。オプションを指定せずに実行すると、コンピュータに設定されたDNSサーバに対し、入力されたホスト名(コンピュータ名、FQDN表記による文字列)の名前解決を行います。

<構文>

nslookup 各オプション ホスト名 (DNSサーバ)

<主なオプション>

なし : 指定されたホスト名の名前解決を行います。DNSサーバが指定されている場合には、指定されているDNSサーバに名前解決を行います。
ホスト名が未入力の場合には、対話モードにて動作します。

-type=タイプ : 名前解決するタイプを指定して名前解決を行い結果を表示します。

タイプ例) a=ホスト名のIPv4アドレス(Aレコード)

aaaa=ホスト名のIPv6アドレス(AAAAレコード)

mx=指定されたドメイン名のメールサーバのIPアドレス(MXレコード)

【付録8】 <コマンド紹介> arpコマンド

```
> arp -a
```

```
インターフェイス: 172.16.1.10 --- 0xa
インターネット アドレス      物理アドレス      種類
172.16.1.1                  00-00-0e-ea-6a-cc    動的
172.16.1.15                 00-00-0e-ea-7a-ee    動的
```

本コマンドにてアドレス解決した履歴（ARPキャッシュ）が表示される図の場合、2行のアドレス解決情報が確認できる
表示内容は以下

- ・インターネットアドレス : IPアドレス
- ・物理アドレス : アドレス解決結果のMACアドレス



【参考】

OSの制御により、より多くの情報が表示される場合もあります。

ここでは、arpコマンドについて紹介します。

arpコマンドは、ARPキャッシュの内容表示と変更を行います。ARPキャッシュには、IPアドレスと、その解決済みイーサネット物理アドレス(またはトークンリング物理アドレス)を格納するために使用する1つ以上のテーブルが含まれます。

<構文>

arp 各オプション

<主なオプション>

- a : 現在のARPエントリーを表示します。IPアドレスを指定すると、指定したコンピュータのIPアドレスとMACアドレスを表示します。
- d : すべてのエントリーを削除します。
- d IPアドレス : IPアドレスで指定したエントリーを削除します。
- s IPアドレス MACアドレス : ARPエントリーを追加します。MACアドレスはハイフンで区切った16進数で指定します。IPアドレスはドットで区切った10進数で指定します。ただし、コンピュータを再起動するとエントリーは削除されます。