

情報基礎シリーズ6

# ネットワークとセキュリティ

# ネットワークと セキュリティ

電子開発学園出版局

\* 本書に掲載した会社名・製品名等は、一般にそれぞれ各社の商号・登録商標または商標です。

## はじめに

コンピュータが開発されて以来、コンピュータは多くの分野で利用されてきました。現在では例えば、旅券を発行する、ご飯を炊く、ゲームをする、ニュースを知る、電話をするなど私たちの生活の中に根付いた分野で利用され、なくてはならない物として、また身近な物として存在しています。また現在のネットワーク社会はコンピュータなくして成り立ちません。

コンピュータはこれらの多くの分野で実現する様々な事柄を実現するために、“情報”を取扱い、制御し、処理しています。コンピュータで取り扱い、処理する“情報”とはいったいどのようなもので、それを取扱い、処理するためにどのような技術が使用されているのでしょうか。本書を含む「情報基礎シリーズ」では、このような知識、技術を“インフォメーションテクノロジー (IT)”と総称しております。

この“インフォメーションテクノロジー”を学ぶことは、様々な情報とそれを取り扱うコンピュータを学ぶことであり、それにより現代社会の基盤となるコンピュータについて理解を深めることとなり、そしてその社会についても知るようになります。

本書は、多くの分野から成立している“インフォメーションテクノロジー”のうち、ネットワークとセキュリティについて、基礎から学ぶためのテキストであります。

本書によって、情報とはなにか、情報技術とはなにか、コンピュータはどのようなものを学び、理解を深め、情報処理技術者試験の取得に役立てていただければ幸いです。

編著者

# 目次

## はじめに

<b>第1章 データ通信と制御</b> .....	1
1.1 ネットワークの種類と方式.....	1
1.1.1 データ伝送と回線方式.....	1
1.1.2 LANとWAN.....	5
1.1.3 回線の計算.....	13
1.2 ネットワークアーキテクチャ.....	16
1.2.1 OSI参照モデル.....	16
1.2.2 データの伝送制御.....	25
1.2.3 メディアアクセス制御.....	30
<b>第2章 TCP/IP</b> .....	33
2.1 TCP/IP.....	33
2.1.1 TCP/IPプロトコル群.....	33
2.2 TCP/IPプロトコル.....	36
2.2.1 ネットワークインタフェース層.....	36
2.2.2 インターネット層.....	49
2.2.3 トランスポート層.....	62
2.2.4 アプリケーション層.....	66
<b>第3章 ネットワークの応用と管理</b> .....	77
3.1 ネットワーク応用.....	77
3.1.1 インターネット.....	77
3.2 ネットワーク管理.....	85
3.2.1 ネットワーク運用管理.....	85
3.2.2 ネットワーク管理プロトコル.....	89
3.2.3 ネットワーク仮想化 (SDN、NFV等).....	91
<b>第4章 情報セキュリティ</b> .....	93
4.1 情報セキュリティの基礎.....	93
4.1.1 情報セキュリティの概念.....	93
4.1.2 情報セキュリティの技術.....	95

<b>第5章 情報セキュリティ管理</b> .....	111
5.1 情報セキュリティ管理 .....	111
5.1.1 情報セキュリティの範囲 .....	111
5.1.2 リスク分析と評価 .....	116
5.2 情報セキュリティポリシー .....	120
5.2.1 情報セキュリティポリシーとは .....	120
5.2.2 情報セキュリティマネジメントシステム .....	122
5.2.3 情報セキュリティ機関 .....	125
5.2.4 情報セキュリティ評価基準 .....	126
5.3 情報セキュリティ対策技術 .....	127
5.3.1 情報セキュリティ対策 .....	127
5.3.2 情報セキュリティ実装技術 .....	129
<b>【練習問題】ダウンロードのご案内</b> .....	137
<b>索引</b> .....	139

# ネットワークと セキュリティ

# 第1章 データ通信と制御

コンピュータから別のコンピュータへ持っているデータを伝送路を伝って伝送する。これが**データ通信**と呼ばれる情報通信の仕組みである。現在ではデータ通信はインターネットの急激な普及により、コンピュータシステムでは必要不可欠なものとなっている。

インターネットを含む現代の情報通信の内容も視野に入れ、まずデータ通信の基礎的な知識から説明していく。

## 1. 1 ネットワークの種類と方式

一口にネットワークと言っても、その使用環境、使用機器など環境によりいくつかの種類に分けられ、またその方式も環境によっても異なる。ネットワークの種類と方式についてまず説明をする。

### 1. 1. 1 データ伝送と回線方式

#### (1) 交換方式

ネットワークでは、コンピュータから別のコンピュータへ伝送路を使用して、データを運ぶ。特にネットワークではコンピュータの数が多く、それらのコンピュータが相互に任意のコンピュータとデータがやりとりできる事が特徴である。

よって、ネットワークでは、あるコンピュータが多くのコンピュータの中から任意に選んだ1台と通信するための道である“**伝送路**”が必要となる。もちろん、コンピュータがすべてのコンピュータと直接伝送路が引かれていれば問題はない。これを**専用回線方式**と呼ぶ。だが、コンピュータ数が多くなればそれだけ伝送路の数が必要となるため現実的ではない。

そのために”**交換**”によって伝送路を利用する。**交換方式**には**回線交換方式**と**パケット交換方式**が存在する。

#### (a) 専用回線方式

専用回線方式は、コンピュータや通信機器が1対1で直接1本の回線で接続する方式である。通信相手は固定されており、それ以外の相手との通信はできない。



(b) 交換方式

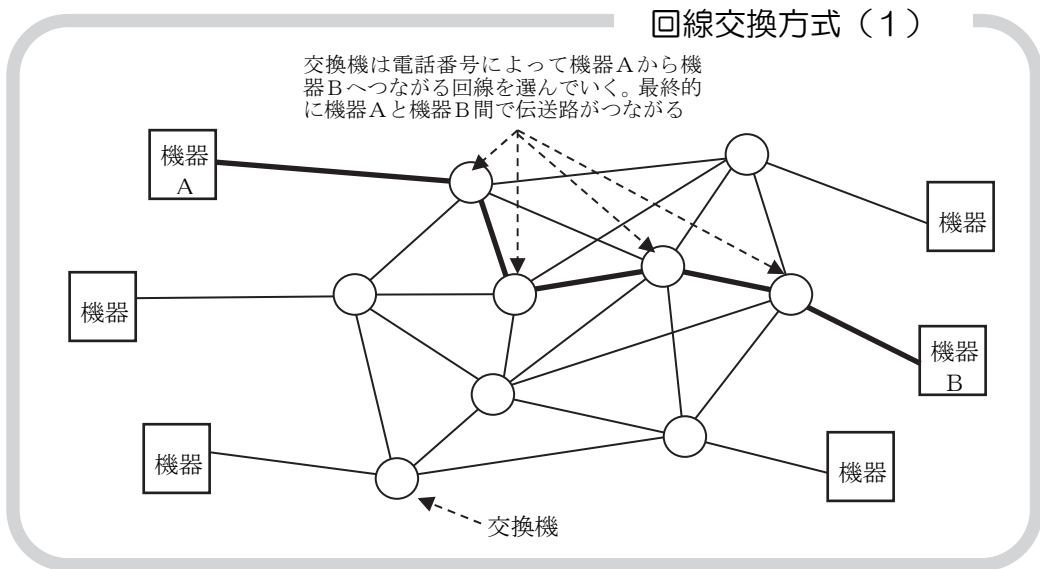
**交換方式**は交換機によって多くのコンピュータ・通信機器が接続されている方式である。そのため、あて先を指定することで任意のコンピュータへのデータ伝送が可能になる。多くのコンピュータの中からあて先を選んで届けることが必要なため、交換機による回線の選択が必要となる。

交換方式を利用することで、コンピュータ・通信機器は複数の相手とデータのやりとりを行いたい場合でも、必要とする回線は1つでよくなり、コストダウンになる。

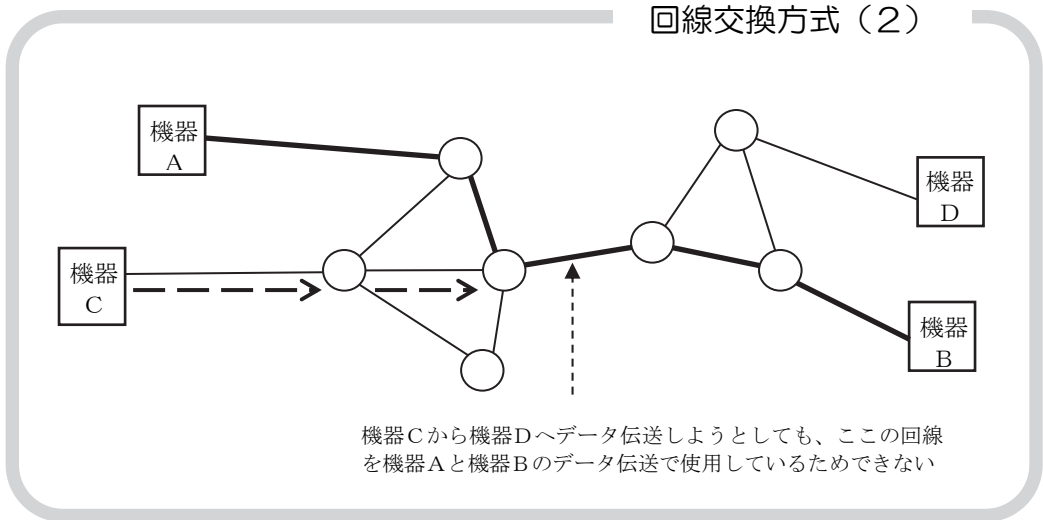
(ア) 回線交換方式

回線交換方式は、一般的には公衆電話網が代表的な方式である。データを送信するコンピュータから、あて先のコンピュータまでの回線を交換機が選び、データの伝送中はその回線のつながりを固定する。これを回線の確立、公衆電話網ではコールセットアップと呼ぶ。

回線交換方式は、電話のように一定時間、一定したデータ量を送信することに向いている。



回線交換方式では、データ伝送中は選ばれた回線はそれを使用している機器たち以外には利用できなくなる。そのため、交換機と交換機をつなぐ回線数により同時にデータ通信が可能になる機器のペア数が決まり、またデータ通信中に他の機器からデータを送ることができない。



#### （イ）パケット交換方式

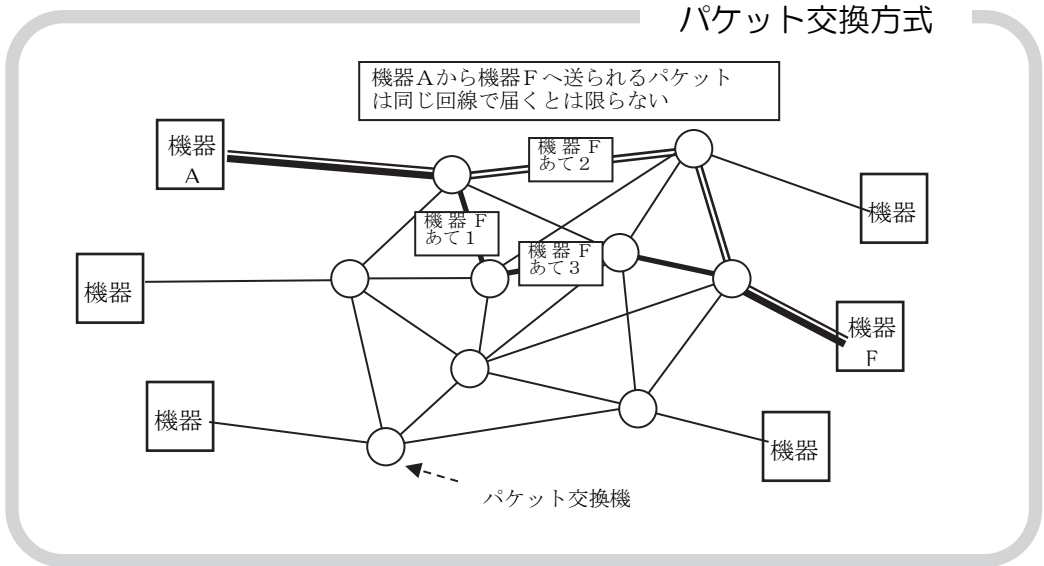
パケット交換方式は伝送するデータを**パケット**（packet：小包）という単位に分割し、それぞれにあて先を示すデータを付加して伝送する。交換機（パケット交換機）はパケットを受け取ると、付加されているあて先データを確認し、あて先への回線でそれを伝送する。

パケットという小さい単位でのやりとりのため回線を長時間使用せず、さらにもし同じ回線を使用するパケットが来たとしても、交換機に回線が空くまで交換機内で待機（蓄積）させることができる。そのため、**蓄積交換方式**とも呼ばれる。

ただし、パケットが必ずしも順番通り、おなじ時間間隔で届かないという欠点がある。さらに伝送路を迂回したり、蓄積されたりすることによりパケットの到着が遅れる（遅延する）ことがある。

パケット交換方式は、データが散発的に発生する場合に向いており、コンピュータによるデータ通信に適している。

現代のインターネットを含むデータ通信ネットワークは、パケット交換機とパケット交換機を結ぶ回線として専用線方式や回線交換方式が使用されている場所はあるものの、ネットワーク全体としてはパケット交換方式が使用されている。



## 1. 1. 2 LANとWAN

回線によって結ばれたネットワークは、その範囲と特性からLANとWANの2種類に大別される。

### (1) 有線LANと無線LAN

LAN (Local Area Network) とは、部屋、フロア、ビル、敷地内などの限られた範囲内で、コンピュータを接続したネットワークである。一般的には、多数のコンピュータをお互いにデータの通信が可能にしたネットワークである。

LANで使用される技術としては、伝送路に使用するものを**伝送媒体** (ネットワークメディア) と呼ぶが、この伝送媒体の違いによって種類が異なる。

#### (a) 有線LAN

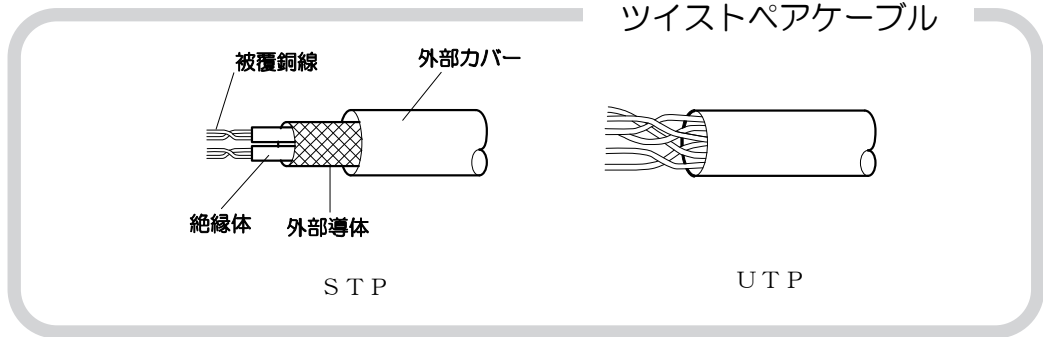
**有線LAN**は伝送媒体として、銅線または光ファイバを利用したケーブルを使用したLANである。最も一般的なネットワークの形態であり、家庭、企業など多くの場所で使用されている。

#### (ア) 伝送媒体

有線LANで使用される伝送媒体は、電気信号を運ぶための銅線ケーブルであるツイストペアケーブル・同軸ケーブルと、光信号を運ぶための光ファイバケーブルがある。

#### 【ツイストペアケーブル】

有線LANを構築する際に一般的に使用される伝送媒体が**ツイストペアケーブル**である。ツイストペアケーブルは、1本の伝送媒体の中に4対8本の導体が入っており、対毎に撚(よ)り合わせたものであり、そのため“撚り対線ケーブル”とも呼ばれる。最大伝送距離は100mとされており、低コストかつ、小径、柔軟なため、取り扱いが容易であるという利点があるが、他の伝送媒体に比べて雑音に弱いという欠点もある。また、金属被服の有無により、シールド型ツイストペアケーブル (STP : Shielded Twisted-Pair cable) と、非シールド型ツイストペアケーブル (UTP : Unshielded Twisted-Pair cable) の2種類に細分される。

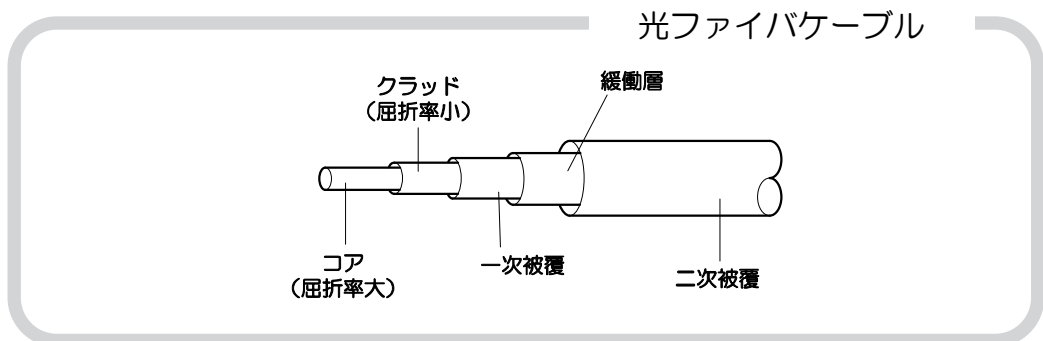


【同軸ケーブル】

ツイストペア・ケーブルの登場以前に使用されていた伝送媒体が同軸ケーブルである。1本の導体の周囲が絶縁体や金属メッシュで覆われた構造となっている。ツイストペア・ケーブルに比べ、雑音に強いという利点があるが、いずれも重く、硬いため取り扱いが困難である。TVのアンテナ線などでは使用されているが、LANのケーブルとしては現在はあまり使用されていない。

【光ファイバケーブル】

光ファイバケーブルは、極細のガラス、もしくはプラスチック製のコアと呼ばれる管を、屈折率の異なるガラスのクラッドで包み、さらにその外をジェルやプラスチックでの被膜で包んだ構造となっている。ツイストペアケーブルや同軸ケーブルは、導体に電気信号を流してデータを届けるのに対し、光ファイバ・ケーブルは管の中に光信号を流す。このため、電気的な雑音の影響をほとんど受けることなく、信号を届けることが可能である。このため、雑音が多い屋外に使用する場合が一般的である。最大伝送距離は数百m～数kmに及ぶ。長距離を高速に伝送できるという利点はあるが、高価な上に非常に破損しやすく、取り扱いが注意が必要である。



光ファイバでは、複数のLED光を使用してデータを伝送する**マルチモード**と、レーザ光を使用する**シングルモード**がある。シングルモードの方がマルチモードよりも高速であり、長距離の伝送が可能である。

#### (イ) 構成要素

有線LANを構成するものは、大別すると3つである。コンピュータまたは通信機器、ケーブル、LAN間接続装置の3つとなる。コンピュータは、クライアントやサーバなどの役割となる。ケーブルとLAN間接続装置で、コンピュータ間またはLANとLANを接続する。

コンピュータとLAN間接続装置はケーブルとの接続のためのインタフェースとして、**ネットワークインタフェースカード (NIC : Network Interface Card)**を持つ。

LAN間接続装置については後述する。

#### (ウ) 特徴

有線LANは現代のネットワークの基本となるネットワークで、多くの場所で使用されている。他のネットワーク技術よりも通信速度が高速で、またスループットも高いため大サイズのデータ転送などに向いている。

さらに、有線LANの技術を利用したWAN技術も登場しており、今後はより多くの場所で利用が見込まれている技術でもある。

### (b) 無線LAN

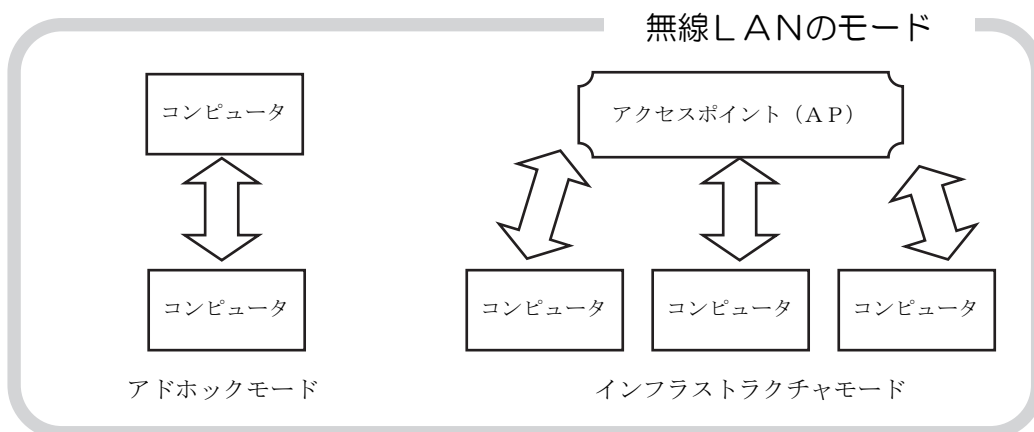
**無線LAN**は伝送媒体として電波や赤外線などを用い、名前の通り無線通信によるデータ通信を行うLANである。ケーブルを必要としないため自由に機器を配置でき、そのため携帯(モバイル)機器での使用に向いている。

#### (ア) 構成要素

無線LANを構成するものとして、コンピュータとそれに接続される無線LAN用のインタフェースがある。無線LAN用のインタフェースは無線LANカードなどと呼ばれる。無線LAN用のインタフェースは電波や赤外線の発信、受信ができるようになっている。

無線LANの代表的な規格である**IEEE 802.11**規格では、コンピュータと無線LANインタフェースの組み合わせで、2台のコンピュータが直接データ通信を行うことができる。これを**アドホックモード**と呼ぶ。基本的にはこのモードでは2台が互いに通信することしかできない。

一方、**アクセスポイント (AP : Access Point)**を電波の中継として利用すれば、複数台でのデータ通信が可能になる。これを**インフラストラクチャモード**と呼ぶ。



インフラストラクチャモードではアクセスポイントは有線LANでのハブの役割を果たし、他のコンピュータへのデータ伝送は、アクセスポイントを必ず中継して届くことになる。

#### (イ) 特徴

無線LANの最大の特徴は、ケーブルが必要ないためにコンピュータを自由に配置できるという点である。そのため、狭い場所や離れた場所などケーブルを通しにくい場所での利用に向いている。また、ケーブルがないため移動しながらでも使用することができ、携帯機器での利用にも向いている。

ただし、電波の強弱が通信速度に影響するため、電波が通りにくい場所や障害物があると極端にスループットが低下する場合がある。また、有線LANに比べてスループットが低いという欠点もある。

## (2) WAN

WAN (Wide Area Network) とは、LANを超えた範囲であるビルとビル、支店と本店のように地域的に離れた場所にあるコンピュータ、またはコンピュータ群 (LAN) を相互につないだネットワークである。WANにより地域や国といった離れた場所にあるLANとLANをつなぎ、大きなネットワークを構成できる。

### (a) 電気通信事業者

WANを構成する場合でも、コンピュータやLAN同士をつなぐためには伝送路が必要となる。LANで使用する伝送路として使用する伝送媒体 (ケーブル) は、自社のビル内・敷地内であるため独自にケーブルを敷設することは可能であった。

だが、WANの場合、市町村や県、国という単位をまたいでつながるため、公共の場所を

通ってケーブルを敷設する必要がある。これを行うことができるのは国の認可を受けた組織だけであり、このような組織を**電気通信事業者**と呼ぶ。

#### (ア) 電気通信事業法

明治時代に電報サービスが始まって以来、通信事業は鉄道や郵便と並んで国の重要事業とされてきた。当時、日本電信電話公社（現在NTTグループ）が国内通信を、国際電信電話株式会社（現KDDI）が国際通信を運営する唯一の通信ネットワークサービス機関として運営されてきた。しかし、さまざまな通信ネットワークに対する需要・要求にこたえるため、1985年、通信事業への民間企業参入が自由に認められるようになった。このとき発効した法律が電気通信事業法である。

#### 【電気通信事業者の区分】

電気通信事業者は条件によって届出電気通信事業者と登録電気通信事業者の2つの種類に分けられる。

### 電気通信事業者の分類

電気通信事業者の種類	条 件
届出電気通信事業者	①電気通信回線設備を設置する事業者のうち、以下の2つの要件を満たす事業者 <ul style="list-style-type: none"> <li>・ 端末系伝送路設備が一の市町村(※)の区域に留まること</li> <li>・ 中継系伝送路設備が一の都道府県の区域に留まること</li> </ul> ※特別区・政令指定都市にあつては「区」とする。           ②電気通信回線設備を設置しない事業者
登録電気通信事業者	上記の①の要件を超える回線設備を設置して電気通信事業を営む事業者

つまり、電気通信事業者は自前でケーブルを敷設している電気通信事業者（登録電気通信事業者と届出電気通信事業者の①）と、ケーブルを敷設している電気通信事業者に使用料を払うことでケーブルを利用している電気通信事業者(届出電気通信事業者の②)がある。



(b) WANサービス

電気通信事業者はケーブルを含むその保有している設備により、WANに必要な伝送路とその設備を他者にサービスとして提供している。これをWANサービスと呼ぶ。

WANサービスを利用することにより、利用者側は離れた地域のLANやコンピュータをつなぐことができ、WANを構築できる。

(ア) WANサービスの費用

WANサービスを利用するためには費用が必要となる。そのWANサービスの利用費としては2種類に分けられる。

**【従量制】**

使用した分だけ費用が発生する方式が**従量制**である。パケット交換を利用した場合は送受信したパケット数で、回線交換を利用した場合は使用した時間とあて先との距離を掛け合わせたものにより金額を算出する。

従量制の使用料と合わせて契約費などの固定費用が発生する場合は定額従量制、固定費用なしの従量制だけの場合は完全従量制などとも呼ばれる。また、従量制でも使用量に応じて徐々に費用が下がっていく、例えば100分までは1分3円、100分以上200分以内は1分2円50銭のように減っていく費用方式を逓減（ていげん）課金方式と呼ぶ。

**【定額制】**

定額制は、回線の利用費として決められた期間（多くの場合は月単位）で、利用によって変動しない費用を払う。パケット交換を使用するWANサービスによく使用されている。

(イ) WANサービスの種類

WANサービスは電気通信事業者が提供しており、前述のとおり電気通信事業者はケーブルを持つ事業者、持たない事業者がある。電気通信事業者はその規模や設備により様々なサービスを実施しており、利用者は自身の要求にあったサービスを選択することで、WANを構築できる。代表的なサービスは次の通りとなる。

**【専用線サービス】**

利用者の拠点と拠点を専用線で結ぶサービスである。定額制ではあるが距離によって費用が決まり、他のサービスに比べて高額である。その分スループットが高く、セキュリティも高い。

**【回線交換サービス】**

電気通信事業者が保有する回線交換を利用したネットワーク（回線交換網）を利用できるサービスである。費用としては従量制なものが多い。代表的なサービスとしては次のようなものがある。

## 1) 公衆交換電話網

一般的な電話のネットワークのことである。電話網を利用してデータ通信を行う。ダイヤルしてあて先へ接続を行う**ダイヤルアップ接続**を行う。

## 2) I S D N

I S D N (Integrated Services Digital Network : 統合サービスデジタル網) はデジタル化された電話、F A X、データ通信を行うことができるネットワークサービスである。電話とF A Xのサービスは回線交換で、データ通信はパケット交換で行う。

**【パケット交換サービス】**

電気通信事業者が保有するパケット交換を利用したネットワーク（パケット交換網）を利用できるサービスである。費用としては定額制なものが多い。代表的なサービスとしては次のようなものがある。

## 1) A T Mサービス

セルと呼ばれるパケットよりも小さいサイズでデータ通信を行うA T M (Asynchronous Transfer Mode : 非同期転送モード) を使用したネットワークサービスである。A T Mはセルリレー、セル交換とも呼ばれる。様々なデータを高速で運ぶことができる。

## 2) フレームリレーサービス

フレームと呼ばれる単位に区切られたデータでデータ通信を行う技術であるフレームリレーを利用したネットワークサービスである。共有回線を使いながらも高速で利用できる。

## 3) 広域イーサネットサービス

もともとはLANの技術であるイーサネットを利用したネットワークサービスである。LANの技術であるため、LANとWANのシームレスな接続が可能となる。

(ウ) インターネットサービスプロバイダ

インターネットへの接続、つまりインターネットを利用したデータ通信を行うために、インターネットへの接続のWANサービスを実施している電子通信事業者を**インターネットサービスプロバイダ** (ISP: Internet Service Provider) と呼ぶ。単にプロバイダと呼んだ場合はこのISPを指すことが多い。

インターネットへの接続を希望する利用者は、ISPの設備までWANによりデータの送受信を可能にする必要がある。そのため、通常はISPまでのWANサービスと、ISPが行うインターネットへの接続サービスをセットで利用することになる。

### 1. 1. 3 回線の計算

#### (1) 転送速度

転送速度とは伝送媒体を使って単位時間あたりに送信することが可能な情報量を意味しており、データ転送速度、回線利用率、転送データ量から転送にかかる時間を見積もりする。

##### (a) データ転送速度

**データ転送速度**は単位時間あたりに伝送可能な情報量である。一般的には1秒間に伝送可能なビット数で表され、単位として**b p s** (bit per second) かビット/秒を使用する。**回線容量**と呼ばれる場合もある。

##### (b) 回線利用率・伝送効率

**回線利用率**とは、実際に回線を利用してデータを伝送している割合を表す。回線使用率とも呼ぶ。回線利用率は実際に転送されているデータ量をデータ転送速度で割ったものになる。

また、一般的にデータ転送速度というものは、その回線の能力をすべて引き出した場合の値であり、現実はずべてを利用することはできない。この実際に回線で使われる割合も回線利用率と呼ぶ場合もある。または**伝送効率**と呼ぶ。

実際に使われる転送速度、これを**実効転送速度**と呼ぶが、**実効転送速度**の計算はデータ転送速度に伝送効率をかけたものになる。

##### (c) データ転送時間

データを転送するために必要な時間が**データ転送時間**である。データのサイズと実効速度、伝送効率、また必要な付加データの転送時間から求める。

## 例題

## 【問題】

設置場所の異なるクライアントとサーバ間で、次の条件で通信を行う場合の応答時間は何か。ここで、クライアントの送信処理の始まりから受信処理が終了するまでを応答時間とし、距離による遅延は考慮しないものとする。

[条件]

クライアントとサーバ間の回線速度	8 Mビット/秒
伝送効率	60%
電文長	上り 1 Mバイト、下り 2 Mバイト
クライアントの処理時間	送信、受信を合わせて 0.4 秒
サーバの処理時間	送信、受信を合わせて 0.4 秒

## 【解答】

まず、実効転送速度は回線速度に伝送効率をかけて、

$$8 \text{ M (ビット)} \times 0.6 = 4.8 \text{ M (ビット/秒)}$$

となる。データ転送時間を上りと下りで計算すると、

$$\text{上り} : (1 \text{ M (バイト)} \times 8 \text{ (ビット)}) \div 4.8 \text{ M (ビット/秒)} \approx 1.7 \text{ 秒}$$

$$\text{下り} : (2 \text{ M (バイト)} \times 8 \text{ (ビット)}) \div 4.8 \text{ M (ビット/秒)} \approx 3.3 \text{ 秒}$$

データはクライアント送信、サーバ受信、サーバ送信、クライアント受信の順番で動作し、そのための処理時間がサーバ、クライアントで 0.4 秒ずつなので、

$$1.7 + 3.3 + 0.4 + 0.4 = \underline{5.8 \text{ 秒}}$$

## (2) ビット誤り率

ビットは伝送路上を伝送している間に、ビットを示す信号が崩れ正しく読み取れなくなることがある。これをビット誤りと呼び、これが発生する確率が**ビット誤り率**である。

例えば、ビット誤り率が  $\frac{1}{100}$  ならば、100 ビットを送信すると、平均で 1 ビットが誤りという意味になる。

### (3) 呼量

サポートセンタやチケットセンタなどに電話をした場合、電話が混み合っていてつながらないことがある。このようなことを防ぐために、サポートセンタなどの設計時に、“どのぐらい電話がかかってくるか”“1回でどのぐらい話すのか”を計算し、そのために必要な“電話回線の回線数”を見積もる必要がある。コンピュータ通信でも、ダイヤルアップ接続を受ける場合や、IP電話を使う場合などで回線数を見積もる必要がある。その時に使用するものが**呼量**である。

#### (a) 呼と呼量

呼は1回の電話で使用した時間、つまり電話を受けてから終わるまでの時間を示す。これを単位時間（たとえば1時間など）での全体の呼の合計を**呼量（アーラン）**と呼ぶ。

一方、“電話がつながらなかった割合”をいくつにするかを定める。これを**呼損率**と呼ぶ。呼損率は電話がかかってきた中で、通話中などになり話すことができなくなる度合いである。

例えば、呼損率1%で、1時間あたり100本の電話がかかってくるとするならば、 $100 \times 0.01 = 1$ で、100本中1本の電話が話し中になってしまい受け取れないことになる。

#### (b) 回線数

アーランと呼損率から必要な回線数を導き出すことができる。計算には複雑な公式を使うため、通常はアーランB式と呼ばれる表を使い、換算することで回線数を求める。