

インターネット情報論の基礎(1)

-ネットワークのしくみと TCP/IP 入門-

土橋 喜

愛知大学現代中国学部

Introduction to Internet (1)

-Network and Basic TCP/IP-

Konomu DOBASHI

Aichi University

目 次

はじめに

1. ネットワークの基礎

1. 1. 通信のデジタル化

1. 2. 情報通信基盤

1. 3. コンピュータネットワーク

1. 4. ネットワークの目的

1. 5. リンクと放送

1. 6. LAN と WAN

1. 7. 通信媒体

1. 8. コンピュータネットワークの基本形態

1. 9. LAN の通信方式

1. 10. 回線交換とパケット交換

1. 11. ネットワークの相互接続

》》》 演習 1 《《《

2. インターネット入門

2. 1. ネットワークと通信

2. 2. インターネットの歴史

2. 3. 日本のインターネットの始まり

- 2. 4. インターネットの構成
- 2. 5. 学術研究ネットワークと商用ネットワーク
- 2. 6. インターネット関連組織
- 2. 7. インターネットの可能性

》》》 演習 2 《《《

3. インターネットのしくみ

- 3. 1. プロトコルとは
- 3. 2. 会話とプロトコル
- 3. 3. データ通信とプロトコルの特徴
- 3. 4. プロトコルの開発と標準化
- 3. 5. OSI 参照モデル
- 3. 6. OSI 参照モデルとデータ送信

》》》 演習 3 《《《

4. TCP/IP

- 4. 1. TCP/IP プロトコル
- 4. 3. OSI 参照モデルと TCP/IP
- 4. 3. データの単位と名称
- 4. 4. インターネット層
- 4. 5. トランスポート層
- 4. 6. アプリケーション層
- 4. 7. LAN と TCP のヘッダ形式
- 4. 7. 1. イーサネットヘッダ
- 4. 7. 2. TCP のヘッダ形式
- 4. 7. 3. UDP のヘッダ形式
- 4. 7. 4. LAN とパケットの送受信
- 4. 8. ヘッダの処理とデータ送受信

》》》 演習 4 《《《

5. IP プロトコル

- 5. 1. インターネット層とアドレス
- 5. 2. IP アドレス
- 5. 3. IP アドレスの管理

- 5. 4. IP アドレスと 3 つのクラス
- 5. 5. クラス A
- 5. 6. クラス B
- 5. 7. クラス C
- 5. 8. IP アドレスの不足
- 5. 9. サブネット
- 5. 10. サブネットマスク
- 5. 11. DHCP
- 5. 12. プライベート IP アドレス
- 5. 13. CIDR
- 5. 14. IPv6

》》》 演習 5 《《《

6. IP の経路制御

- 6. 1. IP ヘッダのしくみ
 - 6. 1. 2. IPv4 のヘッダ形式
 - 6. 1. 2. IPv6 のヘッダ形式
 - 6. 1. 3. IPv4 と IPv6 のヘッダ形式の違い
- 6. 2. 経路制御
- 6. 3. ICMP プロトコル
- 6. 4. ARP プロトコル
- 6. 5. ARP のしくみ
- 6. 6. ARP とハードウェアアドレスの取得
- 6. 7. RARP プロトコル
- 6. 8. ポート番号
- 6. 9. ドメインネームシステム
 - 6. 9. 1. ホスト名の管理と DNS
 - 6. 9. 2. DNS の役割としくみ
 - 6. 9. 3. ネームサーバとリゾルバ
 - 6. 9. 4. ドメイン名の多様化

》》》 演習 6 《《《

引用文献

はじめに

本稿はインターネットを中心にした情報ネットワークの基礎的なしくみやサービスについて、情報リテラシーの学習を終えた文科系または社会科学系の学生を対象に、講義内容をまとめたものです。

これからの情報化社会では、インターネットの普及に見られるように、情報ネットワークが果たす役割はますます重要になり、社会基盤として不可欠のものになっています。現代人は今後益々発展する情報化社会の中で、日常生活の中においても情報ネットワークと関わりを深めるようになります。そのためそれらのしくみや基本的な使い方を理解して上手に活用することが必要になります。

本稿ではインターネットを理解するための基礎的な理論について学びながら、パソコンを使って関連した演習を行うことによって、ネットワークの使い方やしくみを体験し、理解を深める工夫をしています。

講義資料として授業で活用するため、全体は12章で構成しています。本稿はそのうち前半部分にあたる第1章から第6章までをまとめたものです。全体構成および各章の概要については次のとおりです。第7章から第12章までの後半部分は次回に投稿します。

1. ネットワークの基礎

現在コンピュータと通信機器は、人間同士のコミュニケーションの道具として社会に広く普及しており、人々の日常生活において情報伝達を支える基盤となっています。高度に発達した情報通信を基盤とする社会を情報化社会と呼ぶことがあります。第1章では今後も社会を支える重要な基盤である情報ネットワークの基礎を取り上げます。

2. インターネット入門

現在では世界中の多くのコンピュータがインターネットに接続し、いまや世界中と情報のやりとりができるようになっています。現代社会においてインターネットに代表されるコンピュータネットワークは、重要な社会基盤のひとつとして不可欠の存在となっています。そのため第2章ではインターネットのしくみを学ぶ前提として、インターネットが発展してきた歴史的な経緯を取り上げます。

3. インターネットのしくみ

インターネットを上手に活用し、そのしくみや社会的な影響などを考えるためには、インターネットを成り立たせている基本的な技術を理解しておくことが必要です。インターネットの情報交換を支えている主要な技術を理解するために、第3章ではプロトコルの基本的なしくみを取り上げます。

4. TCP/IP

現在のインターネットにおいては、TCP/IP プロトコルが広く使われており、信頼性の高いデータ通信を実現しています。第4章ではTCP/IP プロトコルのしくみについて取り上げます。

5. IP プロトコル

インターネットでは主に TCP/IP によるデータ通信が利用され、その通信を成り立たせるために多くのプロトコルが使われています。なかでも IP プロトコル(Internet Protocol)は、インターネット上で行われる通信の宛先を指定する役割を果たしており、最も重要なものになっています。第5章では IP プロトコルのしくみと役割について取り上げます。

6. IP の経路制御

インターネットでは IP アドレスを使って経路制御を行い、相手先にデータが送り届けられ、それによって通信が成り立っています。第6章では IP の経路制御について取り上げます。

(以降は次回投稿します)

7. インターネットのサービス

各種のインターネットサービスは、そのサービスに応じたプロトコルに従って、コンピュータ同士で情報のやり取りを行うことによって実現されています。インターネットを利用する場合には、そのサービスの意味とサービスを受けるために用意されたソフトウェアの機能や使い方を知る必要があります。第7章では telnet や ftp によるサービスを取り上げます。

8. 電子メールのしくみ

電子メール(e-mail, electronic mail)サービスはインターネットで広く利用され、WWW とともにインターネットの中心的なサービスのひとつとして重要な存在であり、ユーザにとっても親しみのある通信サービスといえます。第8章では電子メールのしくみについて取り上げます。

9. World Wide Web

これまでのインターネットの発展の中で、最も注目を集めたもののひとつが World Wide Web です。現在ではインターネットだけでなく組織内のネットワークでも、文書の閲覧などに標準的に用いられるシステムになっています。第9章では World Wide Web のしくみについて取り上げます。

10. システム管理の基礎

システム管理では、インストールしてシステムを動かすだけではなく、その後の運用を確実にするため、セキュリティを保つことが極めて重要になっています。第10章ではインターネットへの接続を前提にして、

システムを管理する上での心構えや管理の概要を紹介していきます。

1 1. 情報化社会の問題とセキュリティ

情報技術の発展によってさまざまな情報通信基盤が整備された現代社会では、誰もがどこからでも必要な情報を手軽に手に入れることが可能になります。他方、情報化社会にはさまざまな問題も存在することが明らかになっています。第 11 章では望ましい情報化社会を実現するため、セキュリティ対策のあり方を中心に、解決すべきさまざまな課題を取り上げます。

1 2. セキュリティ対策の方法

インターネット上では、毎日のように新しいサイバー犯罪の手法が生まれていると言っても過言ではありません。さまざまな不正アクセスや犯罪が頻繁に起きており、それらからネットワークやシステムを守る必要があります。第 12 章では不正が起こりうるさまざまな観点から、セキュリティ対策の方法について取り上げます。

1. ネットワークの基礎

日本の携帯電話は、NTT が東京都区内で 1979 年に自動車電話サービスとして営業を開始したのがその発端です。その後小型軽量化と高機能化が進み、1990 年代の中ごろから一般庶民へ急速に普及しました。さらに 1999 年には携帯電話からインターネットへの接続（携帯インターネット）サービスが開始され、それを契機として携帯電話のほとんどがインターネットに接続するようになっていきます。

このようにコンピュータ技術と通信技術は、これまで以上に密接に融合されるようになって来ました。音声や画像などのさまざまな情報が、コンピュータではデジタル化されて扱われるように、通信（communication）で扱われるデータもデジタル化されています。

現在コンピュータと通信機器は、人間同士のコミュニケーションの道具として社会に広く普及しており、人々の日常生活において情報伝達を支える基盤となっています。高度に発達した情報通信を基盤とする社会を情報化社会(information society)あるいはネットワーク社会(network society)と呼ぶことがあります。ここでは今後の社会を支える重要な基盤である情報ネットワークの基礎を取り上げます。

1. 1. 通信のデジタル化

デジタル化された通信のことを、データ通信（data communication）あるいはデジタル通信(digital communication)と呼んでいます。データ通信という用語はコンピュータ分野で主に用いられ、これに対してデジタル通信という用語は通信分野で多く用いられるものです。多くの場合は、コンピュータと通信が融合したものを指しており、通信回線(communication line)の両側で少なくともどちらか一方はコンピュータが使われている形態です。

銀行の預貯金を扱うオンラインシステムや鉄道の座席予約システムあるいはコンビニの商品販売管理を行う POS(Point of Sale)システムなどはデータ通信システムの一例です。これらにおいては大型コンピュータに通信回線を通して端末装置を接続し、日常的な仕事に利用するという形態になっています。インターネット(Internet)やコンピュータネットワーク(computer network)での通信もデジタル化されたデータ通信が利用されています。

しかし事務室や一般的な家庭にも広く普及しているファクシミリは、デジタル方式を採用していても、その送受信をデータ通信と呼ぶことはほとんどありません。データ通信はコンピュータ分野の概念として発展してきたものです。数値データや文章のテキストなどを間違いなく送受信するために、そのデータをコンピュータで処理するというのが当初の考え方でした [引用文献 6]。

しかし最近ではインターネットにビデオを公開したり、遠隔地を結んでテレビ会議を行ったり、IP 電話による通話サービスが行われるようになっており、動画や音声などのマルチメディアデータの通信をより発展させるために、情報通信技術の研究開発と実用化が盛んに行われています。

さらにテレビ放送のデジタル化が進んでおり、当初は通信衛星(communication satellite)を使ったデジタル放送が主体でしたが、日本でも 2003 年から地上デジタル放送への移行が始まっています。

このように画像や音声などあらゆる情報がデジタル化して扱われるようになっており、データ通信においてもコンピュータ以外の情報機器と統合した活用方法に重要性が高まっています。

1. 2. 情報通信基盤

データ通信をより便利なものにするため、国際的な立場から情報通信の社会基盤の構築が進められています。地球全体をカバーするネットワーク網が構築されつつあり、情報通信基盤 (information infrastructure) となりつつあります。これは米国では情報スーパーハイウェイ (information superhighway) と呼ばれることもあります。米国以外にも日本など多くの国々で基幹となる情報通信基盤の整備計画が進んでいます。

情報通信基盤の構築は、通信のためのネットワーク (network) だけでなく、放送 (broadcast) のためのネットワークも含んでいます。今後もコンピュータと通信と放送の3つの融合が進み、さらにすべての通信がデジタル化され、個人のパソコンなどから世界中に瞬時に情報が行き届く時代になっています。デジタル革命 (digital revolution) という言葉はまさにこのような状況を指しており、各国政府は情報通信基盤を活用した各種の情報産業の育成に力を入れており、そのためのさまざまな IT (Information Technology) 国家戦略を策定しています。

情報通信基盤とは、電話などで使われる銅線のケーブルや光ファイバ (optical fiber) を用いた有線通信 (wired communication) のネットワークだけを意味するものではありません。最近のパソコンでも赤外線通信が使われているように、無線通信 (wireless communication) の技術がさらに重要になっており、ネットワークにも無線通信が使われるようになっていきます。無線には、自動車のナビゲーションシステム (navigation system) や船舶の誘導などで使われている衛星通信 (satellite communication) も含まれます。

今後は家庭の中まで高速通信網が広く普及し、家電製品がインターネットに接続するようになり、社会に大きな変化をもたらすことが予測されています。今世紀すなわち 21 世紀のあいだには、驚くほどの速さで世界の情報通信網が変わると予想されています。

最近の情報技術の普及は世界の未来に計り知れない影響を与え始めており、先進国だけでなく発展途上国にも大きな影響を与えます。このような変化は我々の生活や仕事など、身近なものごとにも起こり始めています。

1. 3. コンピュータネットワーク

情報通信基盤を構成する代表的なものに、コンピュータネットワーク (computer network) があります。コンピュータネットワークの物理的な形態は、複数あるいは多数のコンピュータが、お互いに通信できるようにつながったものであり、さまざまなデータのやり取りが可能になっています。しかしコンピュータネットワークという場合は、接続されたそれぞれのコンピュータが独立して動作し、また接続された他のコンピュータとお互いに協力しながら仕事を進めることができるようになっていきます。

またコンピュータ上で動作するシステムがネットワークに接続しているかどうかは、パソコン本体とプリンタのようにケーブルでつながっているという物理的な形態だけでなく、ソフトを含めてどのように運用されているかまで見ておく必要があります[引用文献10]。

例えばパソコンにビデオカメラやデジタルカメラなど各種の周辺機器を接続してデータのやり取りを行います。そのままではコンピュータネットワークというには不十分です。しかしパソコン上でインターネットを閲覧するブラウザなどのソフトを動かしており、接続先のコンピュータとホームページのデータの送受信をとおして、お互いに協力しあって仕事をするようなシステムになっていけば、コンピュータネットワークに接続しているといえます。インターネットサービスプロバイダ(ISP : Internet Service Provider)との接続はまさにこのようになっています。

またネットワークを構成しているコンピュータやケーブルなどのさまざまな情報通信機器およびそれらの上で動作するソフトウェアも含めて、ネットワークシステム(network system)ということがあります。この場合はコンピュータネットワークとほぼ同じ意味として使われます。

ところでもっとも単純で初歩的なネットワークの形態は、パソコンとプリンタを接続したような簡単なものから始まりました。またネットワークに接続しないで運用することをスタンドアロン (stand-alone) といいます (図 1.1) 。スタンドアロンの利用形態では基本的に全て個別に用意するため、導入や運用の費用が高くなり、また有益な情報の共同利用がやりにくいなどの欠点があります。

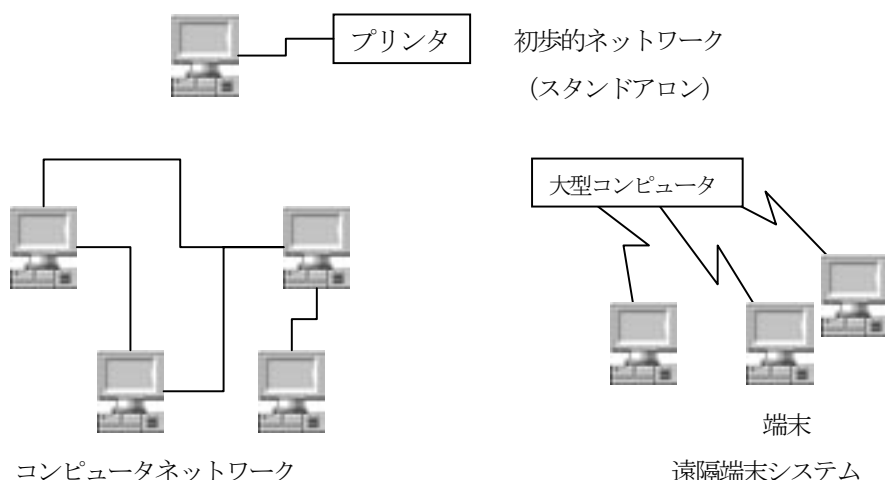


図 1.1 コンピュータネットワークと遠隔端末システム(概念図)

1960 年代には、タイムシェアリングシステム(TSS : Time Sharing System)やオンラインリアルタイムシステムなどと呼ばれるデータ通信が実用化されました。このような初期のデータ通信では、1 台の大型コンピュータに多数の利用者の端末が、通信回線を使って接続されていました。これは遠隔端末システムの一つであり、大型コンピュータの処理時間を分割し、利用者ごとに処理プログラムの切り替えを行い、それぞれの遠隔端末から複数の利用者で共同利用することを目的にしたネットワークです。座席予約システムなどは、

数多くの遠隔端末から入出力を行いながら座席の予約業務を処理するもので、遠隔端末システムの形態になっています。

1. 4. ネットワークの目的

コンピュータを中心とする情報機器は、利用形態をネットワーク化することによって活用範囲を広げ、人々の日常業務や生活にとって不可欠の存在となりました。

多くのコンピュータをつなげてネットワークを構成する目的には、資源共有、信頼性向上、より優れた経済性、システムの段階的な拡張、通信媒体としての活用などがあげられます[引用文献10]。

(1) 資源共有

例えばあるコンピュータに入っているデータを、そのコンピュータで使うだけでなく、別なコンピュータで使うときにも利用できるようになります。また大きな処理を行うとき、1台ではコンピュータの処理能力が足りなくなるときがあり、そのようなときにデータの一部を別のコンピュータで処理することができます。プリンタなどの周辺機器やデータベースなどを利用者間で共用させたり、通信回線を共用させたりもできます。

(2) 信頼性向上

1台のコンピュータだけで処理を行っていると、そのコンピュータが故障などで止まってしまうと処理ができなくなります。しかし複数のコンピュータがネットワークでつながっていると、1台が壊れても残りの処理を別なコンピュータで進めることができます。資源分散の観点から、地震などの災害時にコンピュータやデータが集中していると、被害が大きくなることがあるので、その対策を取ることができます。

(3) 経済性

スーパーコンピュータのような高価な1台で全部処理するより、複数のパソコンをネットワークで連結したほうがシステムのコストが安くなります。そのために個々のコンピュータに処理を分散させる分散処理を行わせます。

(4) 段階的拡張

1台のコンピュータで処理能力が不足したら、より高性能なコンピュータにリプレースする以外にありません。しかしネットワークシステムなら、コンピュータを何台か追加する形で処理を分散しながら拡張できます。

(5) 通信媒体としての活用

距離的に離れたシステムをお互いに接続することによってデータ通信が行えるので、新しいタイプの応用が可能になります。電子メールやWWWなどのほか遠隔テレビ会議システムなどが代表的な応用例といえます。

1. 5. リンクと放送

我々の最も身近にあるネットワークとして、電話網やテレビ放送網があります。この2つはかなり形態が異なっています(図1.2)[引用文献10]。

電話の場合は、特定の相手と一対一で通信路を確保して通信します。このような接続方法は2点間リンク（point-to-point link）と呼ばれます。従来のアナログテレビ放送やラジオの場合は、放送局から多数の受信機に一对多の形で送信され、一方向の通信を行います。このような接続形態は放送（broadcasting）と呼ばれています。

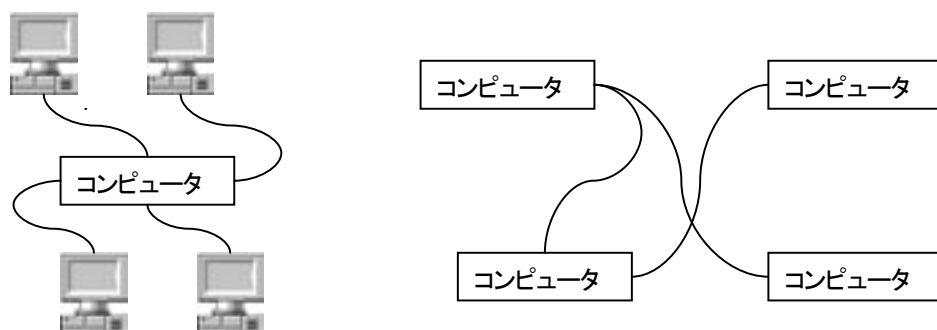


図 1.2 放送型リンク(左)と2点間リンク(右)[引用文献 10, p.166 より作成]

コンピュータネットワークの場合には、物理的には伝送媒体によって2点間リンクか放送型のどちらかの接続形態が使われることになります。しかし従来の放送が一方向なのに対して、コンピュータネットワークは放送型の接続形態でも、データの送受信はソフトウェアによって双方向に行うことができます。

また今後主流となる地上デジタル放送では、双方向のデータ通信が可能であるため、視聴者のデータを放送局側で受け取ることもできるようになり、コンピュータネットワークと放送とが融合した形態になっているといえます。

1. 6. LAN と WAN

ネットワークの活用目的をどのようなものにするかということによって、ネットワークの形態は大幅に異なります。例えば信頼性や経済性のために1台のコンピュータの代わりにネットワークを活用したシステムを構成するときは、それらのコンピュータ間の距離は比較的短いもの（10km程度）になります。そしてそれらの間は高速な通信方式で結ばれることになります。

建物と建物のように距離的に近いネットワークをローカルエリアネットワーク（Local Area Network）と呼び、略して LAN といいます。

また地域的に離れたところにあるデータの共有や個人間の通信が主な目的のときは、そのネットワークは比較的長い距離にならざるを得ません。このように比較的長い距離を結ぶネットワークをワイドエリアネットワークと呼び、略して WAN（Wide Area Network）といいます。

なお LAN の場合には、ケーブルの敷設工事を業者に発注などして自分達で確保するのが一般的です。しかし WAN の場合には自前で長距離のケーブルを敷設したり、衛星を確保したりすることは難しいので、NTT などの通信事業会社から回線の使用権を買って使うのが普通です[引用文献 10]。

この場合回線の使用権を買うということは、2 点間にケーブルを張ることと同じことになります。衛星の場合はパラボナアンテナを立てて、チャンネルの使用権を買うことになります。コンピュータネットワークではソフトウェアによって自由に通信の制御ができるので、2 点間型の媒体を利用しても中継によって全員に同じデータを放送することができます。

また逆に放送型の媒体でも、指定した宛先以外のアドレスについてはデータの配信を行わないことができるので、論理的には両方の形態を利用することができます。このようにデータ通信において柔軟な制御が可能であることが、コンピュータネットワークの特徴となっています。

1. 7. 通信媒体

ネットワーク上においてさまざまな情報は電気信号や光信号として送受信されます。ネットワークを構築するためにはこれらの電気信号や光信号を伝送するために、ケーブルなどの物理的な回線や接続機器が必要になり、これらをまとめて通信媒体あるいはメディア(media)と呼びます。

データ通信またはデジタル通信においては、データはすべて 0 か 1 による 2 進数で表現されています。0 または 1 のいずれか片方をビット(bit, binary unit)と呼び、この複数形がバイト(byte)になり、8 ビットが 1 バイトとして扱われます。通信における伝送速度は、1 秒間に送信できるビット数で表され、bps(bits per second)またはb/s と表示します。

現在市販されているイーサネットの伝送速度としては、10Mbps (1 秒間に 10Mb), 100Mbps (1 秒間に 100Mb), 1Gbps (1 秒間に 1Gb) の製品があり、なかでも 100Mbps のものはファーストイーサネット(Fast Ethernet)と呼ばれ、1Gbps のものはギガビットイーサネットと呼ばれています。

なお 1024b (ビット) は 1000 に近いので 1Kb (キロビット) と呼び、これを 1000 倍した 1024Kb (キロビット) は 1Mb (メガビット) , さらに 1000 倍した 1024Mb (メガビット) は 1Gb (ギガビット) , さらに 1000 倍した 1024Gb は 1Tb (テラビット) であり、これらは伝送速度の単位としてしばしば使われます。

またファイルの大きさの単位にはバイト (8 ビット=1 バイト) が使われ、1024B(バイト)は 1KB (キロバイト) , 1024KB は 1MB (メガバイト) , 1024MB は 1GB (ギガバイト) , 1024GB は 1TB (テラバイト) となります。小文字のbのときはビットを、大文字のBのときは複数形のバイトを表して区別することがあります。

ネットワーク構築に使われる通信媒体と通信技術としては次のようなものがあります。

(1) 銅線や光ファイバー

銅線や光ファイバー(fiber optics)の媒体には、ネットワークを構築するときに広く使われる標準規格のケーブル類が多数あります。また ADSL などのように既設の電話線などを利用することもできます。コストと速度に応じて多くの製品があり、選択肢が複数あります。光ファイバーは銅線よりも高速な 2 点間リンクを張ることができるので、今後コストの低下に伴い一般家庭への普及が見込まれています。2 点間リンクの媒体として使用するときは、これらの媒体を使ってコンピュータなどの機器同士を直接つなげます。

銅線は放送型の媒体にも同じように使われます。しかし大きな違いは、接続形態が異なることにあります。

ハブ(HUB)と呼ぶ集線装置を使ってケーブルと多数のコンピュータをスター型につなぎます。

家庭の電話の引き込みには2本の銅線を撚り合わせたツイストペア線が使われます。このツイストペア線をさらに複数本束ねたものがツイストペアケーブル(twisted pair cable)または「より対線」と呼ばれ広く使われています。このケーブルを使用したネットワークにイーサネット(Ethernet)があり、建物内などにおけるネットワークの標準的な媒体になっています。

建物と建物の間などネットワークの幹線にあたる部分は、光ファイバーが使われます。

(2) 赤外線やマイクロ波

赤外線(infra-red radiation)はノートパソコンなどのデータ通信にも採用されており、同室内など近距離の2点間リンクに多く用いられます。

またマイクロ波(micro wave)は2点間リンクとしても使われることがあります。マイクロ波は家庭用の電子レンジやテレビのUHF放送などにも使われ、比較的波長の短い(1mm~10cm)周波数帯の電波であり、建物が異なる場合や敷地が遠隔地にある場合などに、アンテナを立てて使われます。これらは近距離でもケーブルの敷設をしたくないときや、遠隔地のためにケーブルの敷設が困難なときに効果的といえます。

(3) 通信衛星

通信衛星(communication satellite)は放送型の媒体として使われます。通信衛星を利用する場合は、パラボラアンテナを立てて衛星を介して通信します。通信容量が多く、海外との通信や僻地との通信に適しているといえますが、これらの用途に限定されるものではありません。

(4) 公衆回線と専用線

また広域ネットワークのWANでは、公衆回線を利用したものと、専用線を用いたものがあります。銀行などのネットワークでは、安全性を高めるために専用線が用いられ、一般家庭からISPを経由したインターネットへの接続などは、電話などの公衆回線を使って手軽に接続できるようになっています。

公衆回線には、ISDN(Integrated Services Digital Network)あるいは統合デジタル通信回線と呼ばれるデジタル回線もあります。最近ではADSLに代表されるように既設の電話回線を使って高速にデジタルデータを送受信するXDSL(またはDSL:Digital Subscriber Line)と呼ばれる技術や、これよりもさらに高速な光ファイバーが、回線使用料の低価格化によって、一般家庭まで普及し始めています。

専用線は特定の地点間をつなげるデータ通信専用の回線です。専用線では電話回線のようにいろいろな場所とは通信することができません。専用線の多くは企業などの組織内で、支店間を結ぶネットワークの構築に使われたり、高速にインターネットに接続したりするときに使われます。

また光ファイバー網を使った広帯域ISDN(broad-band ISDN)すなわちB-ISDNでは、155Mbpsから622Mbpsという高速な伝送速度が得られるようになります。

(5) イーサネット

現在では特別な用途を除いて、ほとんどの LAN はイーサネットで構成されています。最近では 100BASE-TX などのように通信速度が 100Mbps のファーストイーサネットの普及が進んでいます。またギガビットイーサネットではより高速な 1Gbps の通信が可能になっており、既存のイーサネットと互換性を持つため、1000BASE-T を中心に普及が始まっています。

1000BASE-T などの意味は、最初の数字の 1000 が伝送速度を表しており、この場合は伝送速度が 1000Mbps (1Gbps) であることを示しています。また BASE の部分は LAN における電気信号の伝送方式がベースバンド(base band)と呼ばれる方式であることを示しています。

T の部分はケーブルの種類を示しており、T はツイストペアケーブルを示しています。ツイストペアケーブルでも銅線の周囲に外皮のほかには特別な絶縁体などのシールド（遮蔽体）を使っていない非シールド型のツイストペアケーブルを UTP (Unshielded Twisted Pair) ケーブルといい、LAN では最も一般的に使われます。このケーブルの両端には、RJ-45 と呼ばれる 8 極 8 芯のコネクタが取り付けられており、そのコネクタの形状は電話用のものに似ており、一回り大きめです[引用文献 15]。

さらにネットワークケーブルとして利用される場合は、信号の伝送品質などの基準によってカテゴリが定義されており、どのネットワークの規格に使用するかによって区分が行われます。主なものとしてカテゴリ 5 は 100BASE-TX で、エンハンスドカテゴリ 5 は 1000BASE-T においてそれぞれ使用されます。

なお Ethernet という表現は元々 10Mbps タイプの LAN 規格の名称として使われていました。現在は Fast Ethernet/Gigabit Ethernet を含んだ総称として使われることが多くなっています。

(6) ベースバンド伝送とブロードバンド伝送

ベースバンド伝送方式では、ケーブルなどの 1 本の媒体内に、チャンネル(channel)と呼ばれる通信路を 1 つだけ確立して、デジタル信号を送信します。そのため同時に複数の通信はできないしくみになっています。

これに対してブロードバンド(broadband)伝送方式では、ADSL が従来の電話を使いながら同時にパソコンによるデータ通信が可能なように、データを運ぶ搬送波(carrier)の周波数(frequency)を変えることで、1 本の媒体内で複数の通信路を確立し、同時に複数のデータ通信が可能になっています。ブロードバンドは広帯域通信ともいわれます。

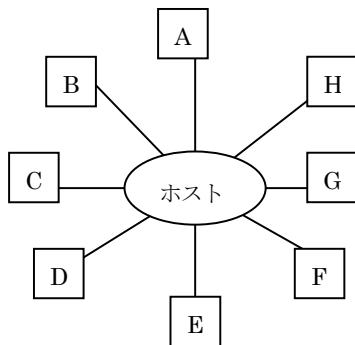
1. 8. コンピュータネットワークの基本形態

コンピュータネットワークの接続の基本形態を、ネットワークトポロジー (network topology) と呼びます。ネットワークトポロジーには複数の形態があり、代表的な形態はスター型ネットワーク (star network)、分散型ネットワーク (distributed network)、バス型ネットワーク (bus network)、リング型ネットワーク (ring network) があります (図 1.3)。

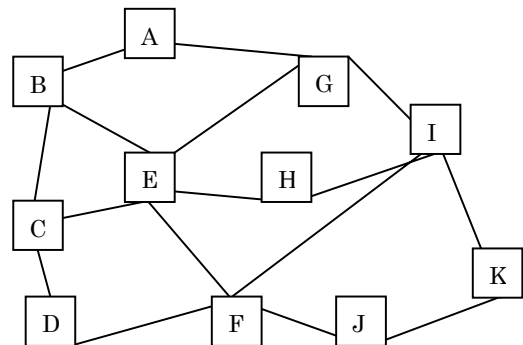
(1) スター型ネットワーク

スター型ネットワークでは、集中処理（centralized processing）の考え方が使われています。中央に 1 台のホストコンピュータ（host computer）が置かれており、他のコンピュータはそれに接続しています。

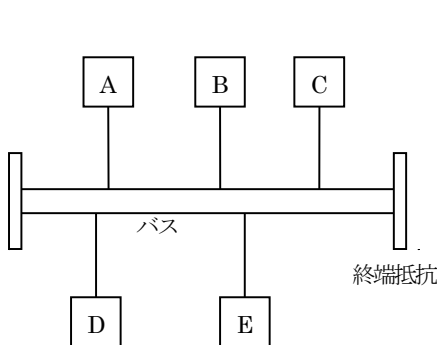
スター型を基本にしているネットワークでは、中央のホストコンピュータが故障したとき、ネットワーク全体が動かなくなるという欠点があります。他方ではすべてのデータを中央で管理するしくみにしておけば、ネットワーク全体を統一した運営がしやすいという利点もあります。銀行のオンラインシステムなどでは、このスター型ネットワークを基本にしています。



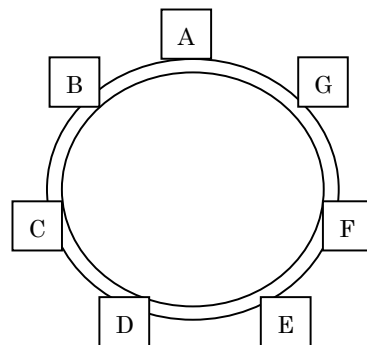
(1) スター型ネットワーク



(2) 分散型ネットワーク



(3) バス型ネットワーク



(4) リング型ネットワーク

図 1.3 ネットワークポロジの例(概念図)

(2) 分散型ネットワーク

分散型ネットワークでは、分散処理（distributed processing）の考え方に基づいた接続形態になっています。分散型ネットワークの利点としては、どれか 1 台のコンピュータが故障しても、全体としてのネットワークが動かなくなるのを避けられることがあります。ネットワークソフトウェアには故障したコンピュータを迂回するルートを探して、通信を続ける機能が備わっています。

分散型ネットワークは、あちこちでコンピュータをつないで、自己増殖的に拡大する傾向があります。そのため、ネットワークの統一した管理ができなくなるなどの問題が発生することがあります。インターネットはこの形態を取っており、世界中で拡大を続けています。

(3) バス型ネットワーク

バス型ネットワークでは、バスと呼ばれる直線状の1本のケーブルに端末を接続する方式です。端末からはバス上に左右両方向にデータが送り出され、受信側の端末が自分あてのデータを取り込みます。ケーブルの端には信号が反射して雑音になるのを防ぐため、終端抵抗が取り付けられています。

バス型ではケーブルの配線が容易であり、通信の信頼性も高いという特徴があります。しかし障害が発生したときに、端末の特定が難しいなどの短所もあります。

(4) リング型ネットワーク

リング型ネットワークでも、バスと呼ばれるリング状の1本のケーブルが使われ、それに端末を接続する方式です。トークンリング(token ring)やFDDI (Fiber Distributed Data Interface)などの通信方法がこの形態を取ります。トークンリングも標準化されたLAN規格の一つで、ツイストペアケーブルによって、通信を行う機器をリング状に接続したもので、通信速度は4Mbpsから16Mbpsです。FDDIは光ファイバーを利用したもので、100Mbpsの通信可能な規格の一つであり、主にイーサネットを相互に接続する基幹LANなどに使われていました。しかし最近ではイーサネットの機器がより低価格化し、かつ高速化する改良が行われたため、FDDIは使われなくなっています。

リング型は他の方式に比べると、ケーブルの総延長を長くすることが比較的容易であるという長所があります。しかし一箇所障害が起きると、全体が停止してしまうという欠点があります。

1. 9. LANの通信方式

(1) CSMA/CD

代表的なLANの通信技術にはイーサネットやトークンリングなどがあります。ネットワークの伝送路には、複数のコンピュータやさまざまな機器が接続しており、ネットワークに接続しているコンピュータやルータなどの通信機器をはじめ、それらの上で動作しているソフトウェアなども含めてノード(node)と呼ぶことができます。

LAN上においてこれらのノードは、さまざまな形態で伝送路に接続し、それらの間でデータ通信が行われ、接続しているノードはいつでも伝送路にデータを送出することができます。

ここでは伝送路とノード間におけるデータの送信を分かりやすくするため、イーサネットケーブルによる1本の通信媒体を同時に共有している場合で考えます。複数のコンピュータから同じ通信媒体の伝送路上に、ほぼ同時にデータが送出されることもあります。このようなときはイーサネットがベースバンド方式のため、データ同士が衝突(collision)してしまい、通信がうまくいかないことが起こります(図1.4)。

このように複数のコンピュータが同じ伝送路上でリンクしているときは、どのコンピュータがリンクを使用してデータを送出するかという制御を行う必要があります。これをメディアアクセス制御(media access control)あるいは単にアクセス制御(access control)と呼ぶことがあります。

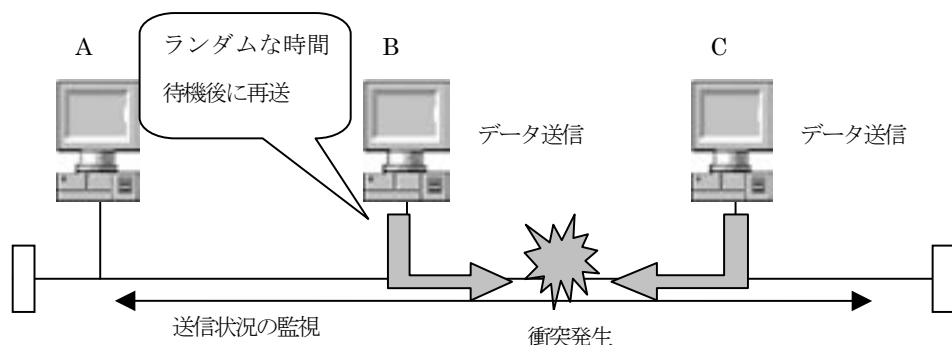


図 1.4 イーサネットにおける CSMA/CD

これらのアクセス制御には、イーサネットなどで用いられる CSMA/CD (Carrier Sense Multiple Access with Collision Detection) と呼ばれる代表的な方式があります。これは搬送波感知多重アクセス/衝突検出方式の英語名を略したもので、情報回路における同時発信処理を感知し、信号の衝突を検出するしくみのことです。

この方式においてそれぞれのコンピュータは、リンクしている伝送路上にデータ（キャリアと呼ぶ信号のこと）が流れていないかどうかを監視 (Carrier Sense) しています。どのコンピュータも通信していないときは伝送路が空いため、そのときだけデータを送り出すことができます。

しかしほぼ同時に複数のコンピュータからデータが送信されると、伝送路上でデータ同士が衝突して破壊されるため、通信が正常に行われません。そのためデータの衝突が起きるのを監視 (Collision Detection) し、衝突が起きると原因となった両方のコンピュータは、即座にデータの送信を停止します。そして衝突を回避するためにランダムな時間待機し、その後に再びデータを送り出します。

この方式を利用すれば、1 本のケーブルを複数のコンピュータなどで共有し、あたかも同時に複数の通信が行われているようにデータの送受信を行うことができるので、双方向に通信する (Multiple Access) ことが可能になります。

しかし接続しているコンピュータが多くなればなるほど衝突の発生が多くなり、伝送効率は低下することになります。この原因はイーサネットがベースバンド方式の伝送方式を取っているため、実際には 1 本のケーブルに対して 1 つの通信路しか確立できないためです。

(2) トークンパッシング

トークンパッシング (token passing) 方式は、トークンリングで用いられるアクセス制御方式です。トークンリングは、リング上でトークンと呼ばれる小さなデータ（送信権またはアクセス権）を常時巡回させています。このフリーな状態のトークンはアクセス権（または送信権）を持ち、トークンビットと呼ばれる値が 0 になっており、フリートークンと呼びます。

コンピュータがフリートークンを受け取った場合、送信したいデータがないときは、そのまま通過させま

す。送信したいデータがあるときは、トークンビットの値を1に変えてトークンをビジー状態に変更し、宛先と送信したいデータを付加して送り出します。データを搬送している最中のトークンはビジートークンと呼ばれます。

伝送路上のコンピュータは、ビジートークンを受信するとまず宛先を調べます。宛先が自分宛の場合はデータを受信し、受信完了の印を付加して送信します。宛先が自分宛ではないときは、そのまま通過させます。

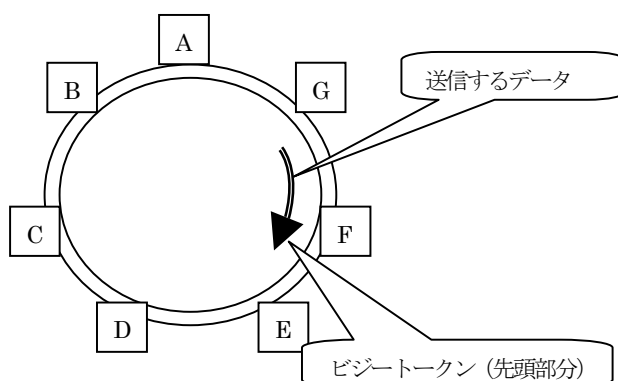


図 1.5 トークンリングとトークンパッシング (概念図)

ビジートークンが送信元のコンピュータに戻ってきたときは、ビジー状態からフリー状態にトークンビットの値を変更して送信し、フリートークンをネットワーク上に巡回させます (図 1.5)。

このような方法によって、伝送路上には常に1台のコンピュータのデータだけが流れ、他のコンピュータのデータと衝突しないしくみになっており、CSMA/CD よりも性能のよい伝送効率を実現しています。しかしトークンリングは管理面で複雑になり、またコストも高いため、一般的にはイーサネットが多く使われています。

1. 10. 回線交換とパケット交換

電話やテレビ放送などのネットワークとコンピュータのネットワークとでは大きな違いがあります。例えば従来の固定電話では、通話を開始するときのはじめに通信回線を設定し、通話中その回線は専有されたままになっています。また通話中に何かの用事で一時受話器を別なところに置くなどして中断すると、音声のデータは回線を流れないので、その回線はしばらくの間使われない状態となります。しかしその回線は他の人が利用できるわけではなく、専有されたままになっておりいつでも会話を再開できる状態になっています。テレビ放送も受信している間は、その電波を他の人が相乗りして使うようなことはなく、受信者が専有しています。

このように固定電話に代表されるネットワークの接続形態は、回線交換(circuit switching)と呼ばれる方式が採用されています。回線交換方式では、通信の開始時に回線を設定し、通信中は回線を専有し、通信が終われば回線を切断します。ファクシミリの通信方法なども同じやり方です。



図 1.6 パケットのしくみ(概念図)

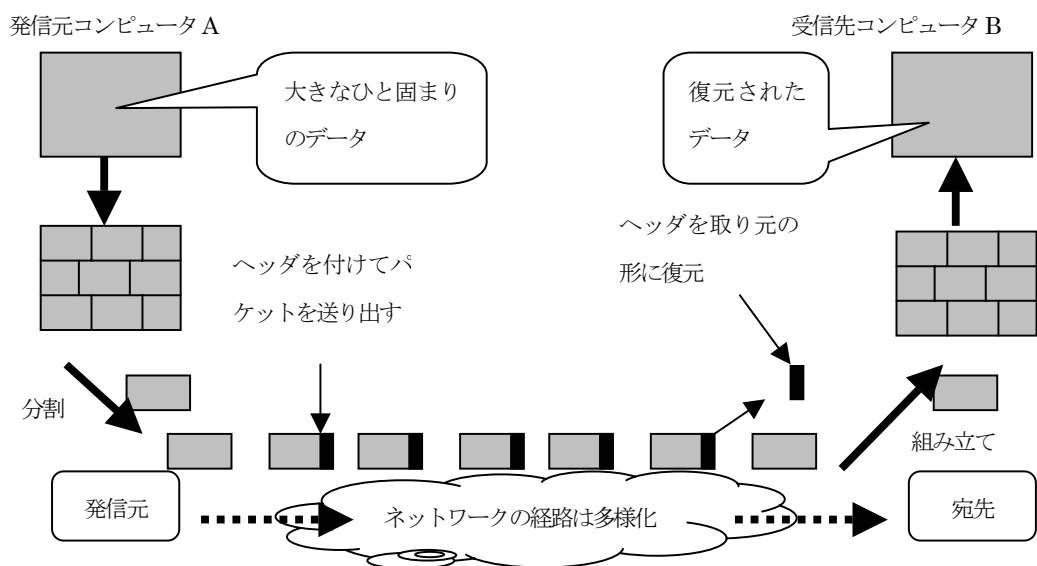


図 1.7 パケット交換方式(概念図)[引用文献 18, p.7 より作成]

これに対してコンピュータネットワークでは、多くの場合パケット交換(packet switching)という方式を採用しています。パケット(packet)というのは小さな小包という意味で、小包を送るときと同じようなやり方で、データの送受信をしているわけです。パケットのひとつひとつにヘッダ(header)と呼ばれる情報が付加され、それには発信元や宛先などパケットを送り届けるために必要な情報が記録されており、その後のペイロード(payload)に届けたいデータが格納されています(図 1.6 および図 1.7)。

パケット交換方式において送信されるデータは、ある決められたサイズ以内の大きさのパケットに分割され、それにヘッダが付けられています。ヘッダというのは、発信元アドレスと宛先アドレスなど、パケットの送受信に必要な情報を格納したもので、ちょうど宅配便や郵便局などで小包に張る宛名シールのようなものとなっています(図 1.7)。インターネットなどの分散型ネットワークでは、このパケットが空いている経路を選びながら送信されます。伝送の誤りを検出したり、訂正したりして、間違っているときには、再度伝送を要求したりする機能が備わっています。

パケットは発信した順番とは異なる順番で宛先に届くこともあります。そのためメッセージの順番も書き

込まれています。宛先に到着した後、元のメッセージに組み立てなおすようになっています。

パケット交換の最大の利点は、回線を有効利用できることにあります。通信を行うといっても、電話のように話しているあいだ回線を専有したままにしているわけではありません。実際に回線が使われるのは、ファイル転送などデータの送受信を行っている時間だけであり、これは接続している時間のごく一部にすぎません。

そのため回線の空きを活用して、データをパケットという小さな単位に分割し、多くの人たちのメッセージを1本の回線に相乗りさせることにより、回線を安いコストで有効利用できるように考え出されたものです。このようなわけでこのパケット交換方式というのは、データ通信における重要な発明のひとつと見なされています。

これ以外に、ATM (Asynchronous Transfer Mode) すなわち非同期転送モードという交換方式も注目されています。ATM は動画画像などのデータも短時間で送れるように、高速かつ簡略化した方式になっており、マルチメディア時代に適した交換方式であるといわれています。

またこの方式では、ATM 交換機と呼ばれる非同期多重化装置によって交換する方式になっており、これらは超高速光ファイバー網によって連結されており、毎秒ギガビット以上の通信ができるように考案されたものです。セル (cell) と呼ばれる固定長で比較的短い単位 of データ (規格では 53 バイト) に、簡略化したヘッダをつけています。伝送経路上で空いている時間があるときは、非同期的なタイミングでセルを詰め込み、利用効率を上げるようになっています (図 1.8)。

ATM は広帯域 ISDN を実現するための技術として、1980 年代の後半から共通の規格が検討され、標準化が行われました。現在では大学キャンパスや ISP などにおける LAN の幹線部分に ATM を利用する場合があります。また伝送が高品質なことから、遠隔テレビ会議システムの構築や運用にも使われることがあります [引用文献 11]。

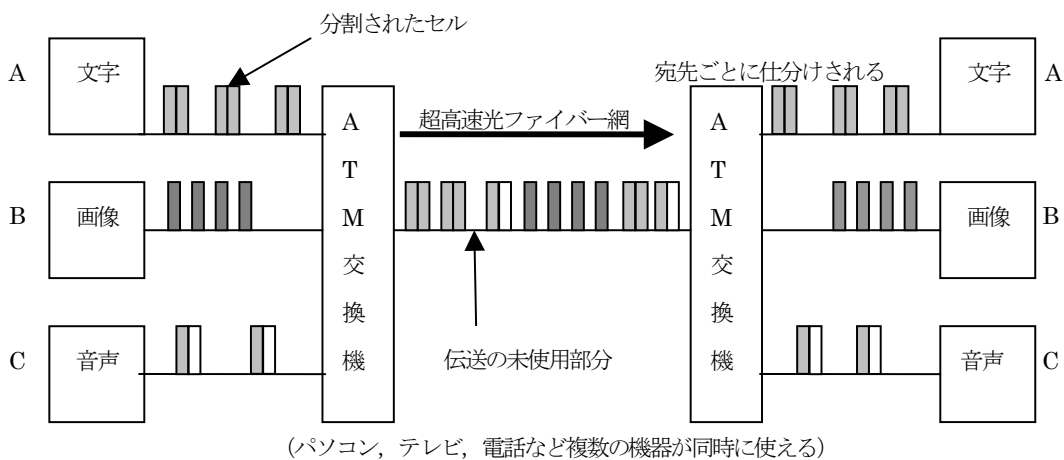


図 1.8 ATM 交換方式

1. 11. ネットワークの相互接続

LAN が普及している背景には、コンピュータのダウンサイジング（downsizing）すなわち小型化と高機能化に加えて低価格化があります。ダウンサイジングと高機能化がますます進行するとともに、オフィスの事務処理や工場の生産管理などにも多数のコンピュータが導入され、ネットワークシステムが構築されています。多くの LAN はこのような環境の中で敷設されています。LAN の運営には、普通は組織内に管理者を置いているので、接続については管理者に問い合わせることになります。

ほとんどの場合、LAN はクライアントサーバシステム（client server system）で構成されています。正確にはサービスを受ける方がクライアント（依頼する人という意味）で、逆にサービスを提供する方がサーバ（召使の意味）となります。サービスの関係が複雑になっているときは、お互いにクライアントとサーバの関係になっていることもあります。

加えて最近では、コンピュータの性能が向上したことにより、ネットワークに接続しているコンピュータが、それぞれ独立してサービスを提供することが可能になっています。そのためそれぞれのコンピュータにおいてサーバの機能を動作させ、互いにサービスを提供し合うことができます。これをピアツーピア（peer to peer）型のネットワークと呼ぶことがあり、益々重要になっています。

遠隔地のコンピュータネットワーク同士を相互に接続して、自由に通信できるとより広範囲にデータ通信ができるようになります。イーサネット同士といったように、同じ種類のネットワーク同士のときは、接続しやすいのは素人目に見ても分かります。しかし異なったタイプのネットワークを接続しなければならないときは、専用の機器が必要になります。

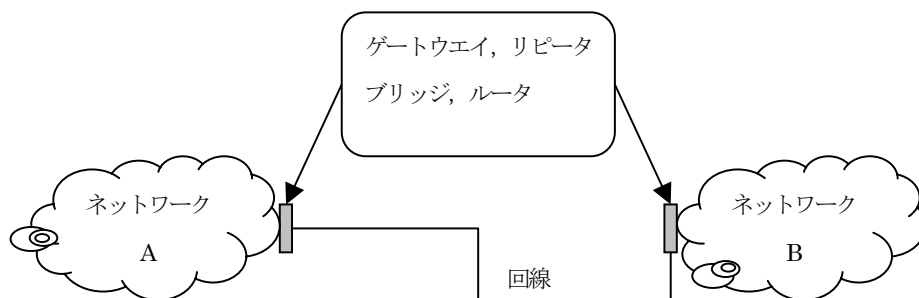


図 1.9 ネットワークとゲートウェイ

ネットワーク間の接続を行う中継システムを、一般的な名称としてゲートウェイ（gateway）と呼び、多くは LAN と WAN の間における中継システムのことを指します。イーサネット同士のときは、リピータ（repeater）やブリッジ（bridge）という簡単な装置で中継できるようになっています。異なるタイプのネットワークの間では、コンピュータ自体がゲートウェイとして用いられることも多く行われています（図 1.9）。

このような中継が可能になるためには、多くのネットワークに共通した通信方法が厳密に定められている

必要があります。例えばイーサネットとトークンリングでは、通信方法の一部が異なるためそのままでは通信することはできません。しかし異なるネットワーク同士を相互接続するためのルータという装置を使って中継すれば、お互いの LAN 同士で通信することができるようになります。

またネットワークの相互接続には、TCP/IP (Transport Control Protocol/Internet Protocol) という通信の決まりがよく使われます。これは現在では世界中をつなぐインターネットにおける標準の通信の規約となっており、元々は UNIX オペレーティングシステムでデータ通信を行うために開発されたものです。インターネット (Internet) という言葉を固有名詞ではなく、普通名詞として使うときには、「ネットワークのネットワーク」という意味であり、ネットワーク間の相互接続のことを指しているのです。

》》》 演習 1 《《《

次の演習を行ってみよ。

1. Web ページの閲覧

自分が住んでいる地方自治体や、自分の大学や学部、いろいろな大学や企業、政府の各省庁などのホームページを見てみよう。それぞれのホームページにはどのような情報が公開されているか調べてみよ。

またどこかの Web ページで、HTML で記述されたソースファイルを表示させ、ブラウザからそのソースファイルを見ることができるので、Web ページがどのように実現されているか考えてみよ。

2. 学内のネットワークがどのようなになっているか、教室のコンピュータから確認してみよ。

》》》 本章の復習 《《《

1. データ通信とはどのようなものか。
2. コンピュータネットワークとはどのようなものか。
3. 遠隔端末システムとはどのようなものか。
4. ネットワークを構築する目的をあげてみよ。
5. 通信媒体にはどのようなものがあるか。
6. コンピュータネットワークの基本形態にはどのようなものがあるか。
7. 情報通信におけるパケットとは何か。
8. 回線交換とパケット交換の違いは何か。
9. ATM 交換方式とはどのようなものか。
10. ネットワークを相互に接続する機器にはどのようなものがあるか。

2. インターネット入門

インターネット(Internet)とは、数多くのネットワークがつながったもので、地域ごとに構築された小規模なネットワークを地球規模で連結したものです。現在では世界中の多くのコンピュータがインターネットに接続し、いまや世界中と情報のやりとりができるようになっています。現代社会においてインターネットに代表されるコンピュータネットワークは、重要な社会基盤のひとつとして不可欠の存在となっています。そのためネットワークのしくみやその上で提供されるサービスについて理解しておくことは、現代人の日常生活にとって極めて重要なことになっています。

2. 1. ネットワークと通信

最近ではインターネットという言葉は日常的に使われるようになり、コンピュータにあまり関わりのない人々にも、何らかの形でインターネットの存在が知られるようになりました。

現在のインターネットは世界中の国々に普及しており、その利用者数や接続しているコンピュータの数を正確に把握することが困難なほど利用されています。しかもインターネットの利用者は現在でも増加を続けており、今後もこれまで以上の勢いで増加していくものと思われます。また接続する機器もコンピュータだけではなく携帯電話なども接続しており、将来的には一般の家電製品もインターネットに接続して利用されるようになるものと見られています。

インターネットという言葉は、ネットワーク同士が相互に接続することにより形成されたネットワークのことで、「ネットワークのネットワーク」ということを意味しています。

つまりインターネットは、コンピュータ技術と通信技術が基盤となって、世界中のコンピュータがネットワークに相互接続し、情報交換が可能になった世界規模の巨大なネットワークであるといえます。

このインターネット上で通信を行うために必要となる約束事が取り決められおり、それを通信規約といいます。例えばその主なものにTCP/IP プロトコルというものがあります。TCP/IP というのはプロトコルに付けられた名前のことで、プロトコル(protocol)というのは通信規約という意味です。

現在のインターネットは、TCP/IP を基盤としたデータ通信によって成り立っています。インターネットの技術的な基盤をより詳しく理解するためには、通信規約のTCP/IP についても知る必要があります。

図 2.1 にインターネットの概念図を示します。自宅のコンピュータが日本のネットワークである B に接続しているとします。そうすると自宅のコンピュータはネットワーク B をはじめとして、ネットワークの A, C, D に接続しているどのコンピュータとも、直接にネットワークを通して情報の送受信ができるようになります。ネットワーク C を中国のものと仮定し、ネットワーク F を米国のものでと仮定すれば、それらの国々の人々と情報交換を行うことができるようになるわけです。

インターネットに接続するためには、お互いに接続するネットワーク同士が、共通の通信規約を定めておく必要があります。この規約がないと言葉の通じない外国人同士の会話のようになってしまいます。イ

インターネットを構築できる通信規約には、TCP/IP のほかに Apple 社が提供している AppleTalk などもあります。

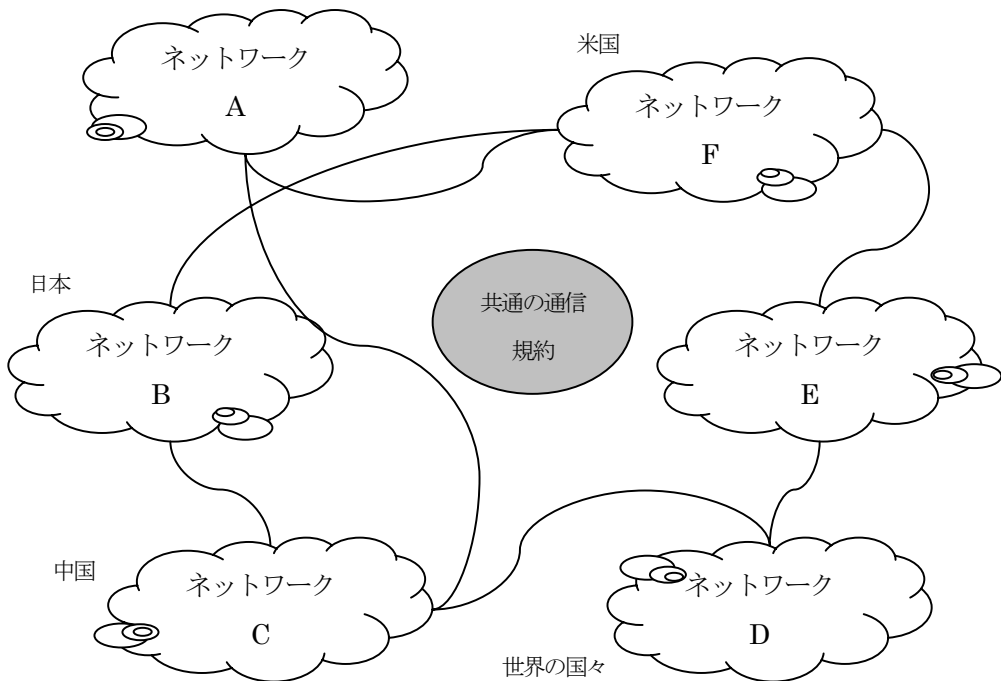


図 2.1 インターネット(概念図)

ネットワークでは TCP/IP を使ったものを、TCP/IP ネットワークということがありますが、これがインターネットで世界を結び付けている基盤となっています。

コンピュータネットワークの通信技術は、初期の大型コンピュータと端末による接続の形態から、現在のパケット交換による分散処理のコンピュータネットワークに至るまで、多くの技術的な試行錯誤を繰り返しながら、さまざまな分野で発展してきました。

コンピュータの機能や性能だけでなく、通信回線や相互接続のための約束である通信規約(プロトコル)にいたるまで、多くの面で改良が加えられたため、通信技術の発展にもつながりました。なかでも TCP/IP による通信は、1980 年代からコンピュータネットワークを利用する立場の人々のあいだに急速に広まりました。

現在では、ほとんどのコンピュータのハードウェアメーカーや基本ソフトを開発している OS (Operating System) のメーカーは、自社の独自プロトコルのほかに、TCP/IP も利用できるようにしており、他社システムと機種が異なっても接続できる異機種間接続を可能にしています。これによってコンピュータの種類やメーカーが異なっても TCP/IP によって通信ができるようになっているわけです。

2. 2. インターネットの歴史

1960 年代の後半、米国では国防総省が研究機関に資金援助を行い、通信技術の研究開発や実験が行われていました。そこではパケットという概念を用いたデータ通信の実験が行われ、これが現在のコンピュータネットワークの基礎となり、同時にインターネットが登場する基礎になったといえます[引用文献 17]。

パケットによるデータ通信のしくみが考案されるまでは、モデム(modem)回線などを用いて、一方的にデータを送るいわゆる垂れ流しの方法で、データの受け渡しが行われていました。この方法では回線が 1 組のユーザに専有されてしまうためさまざまな問題がありました。例えば送りたいデータをそのまま回線に流し込むので、複数のユーザがデータを 1 つの回線に同時に送った場合、どこからどこまでがその人のデータかを区別することができませんでした。

パケット通信では、データを特定の大きさに区切り、それぞれのパケットに宛先のアドレスと自分のアドレスをつけて、通信回線に送り出します。これにより複数のユーザが同時に 1 つの回線やネットワークを利用していても、それぞれのパケットが誰から発信されたもので、誰宛にそのデータを送信しているものかを識別することができるので、通信回線の共有による有効利用が可能になりました。

このパケット交換技術の実験を行うために、1969 年に米国の国防総省は ARPANET (Advanced Research Projects Agency Network) と呼ばれるネットワークを構築しました。これは西海岸にある 3 つの大学 (カルフォルニア大学ロサンゼルス校、カルフォルニア大学サンタバーバラ校、ユタ大学) と 1 つの研究所 (スタンフォード研究所) を接続したパケット交換ネットワークでした。

そこでは軍事的な研究が本来の目的であり、核攻撃などを受けてネットワークの一部が破損しても、部分的には機能し続け、全体が停止することのない冗長性を備えたネットワーク技術の開発が目標でした。

ARPANET で開発された技術は、インターネットの基盤技術となるもので、現在のインターネットの発展はすべてここから始まっているといえます。

ARPANET ではパケット交換技術の実験を行うと同時に、コンピュータとコンピュータの間において正確で信頼性の高い通信方法を提供するための通信規約を実現するためのソフトウェアの開発も行いました。TCP/IP は ARPANET で行われた研究の一環として開発されました。

ARPANET では通信規約としての TCP/IP を開発したほか、イーサネットによる LAN の通信技術の開発も進められ、BSD UNIX (Berkeley Software Distribution から配布される UNIX) オペレーティングシステムによるネットワークの構築が推進され、これによってパケット交換技術による大規模なコンピュータネットワークとして成長し、これがインターネットに発展してきました。

ARPANET が TCP/IP プロトコルを採用すると、UNIX から TCP/IP が利用できるようになり、UNIX ワークステーションの普及とともに、ネットワークの利用が大きく広まることになりました。

このようにして現在のインターネットの原型が、大学を中心としたネットワークとして運用が始まり、1985 年ごろにはコンピュータ関係の研究者だけでなく、一般の研究者もネットワークを利用するようになってきました。インターネットの発展と TCP/IP の開発は極めて密接な関係にあり、この関係は現在も続い

ています。

表 2.1 インターネット発展の歴史[引用文献 9, p.18 および引用文献 18, p.8 より作成]

1957 年	米国国防総省によって ARPA（高等研究計画局）が設立される
1961 年	Leonard Kleinrock（米国）がパケット交換方式の論文を発表
1964 年	Paul Baran（米国）がパケット交換ネットワークの論文を発表
1965 年	Ted Nelson（米国）ハイパーテキストの論文を発表
1969 年	ARPANET の運用開始(4 組織の接続)．ベル研究所が UNIX を開発
1971 年	Ray Tomlinson（米国）による電子メールの開発
1973 年	ARPANET がイギリスやノルウェーと国際接続．イーサネットの発明
1974 年	米国の Bob Kahn と Vinton Cerf が TCP/IP を開発
1976 年	AT&T ベル研究所がネットワーク接続ソフトウェアの UUCP を開発
1982 年	TCP/IP の仕様決定, BSD UNIX に TCP/IP が組み込まれる
1983 年	ARPANET が接続手順に TCP/IP を採用する
1984 年	日本で JUNET が設立される．DNS が開発される．
1986 年	全米科学財団が NSFNET を運用開始
1988 年	日本の WIDE プロジェクトが発足
1989 年	日本から NFSNET に接続可能となる．Tim Bernerds-Lee が WWW を考案
1990 年	NFSNET が ARPANET を吸収
1992 年	Internet Society が設立される
1993 年	米国ゴア副大統領が「情報スーパーハイウェイ構想」を提唱．Mosaic の開発
1995 年	NSFNET の解散
1997 年	米国で Internet2 プロジェクトが開始
1998 年	ICANN が設立される

1989 年に ARPANET は、米国政府の全米科学財団(NFS: National Science Foundation)が 1986 年に発足させた NSFNET に吸収されました。もともと NFSNET は米国 5 箇所のスーパーコンピュータを接続するためのネットワークとして始まりました。

全米科学財団はさらに米国の基幹通信網であるバックボーン(backbone)と、各地域のネットワークの整備を進め、これらを順次民間の経営に移し、1995 年に NFSNET は解散しました。このようにして学術研究を行うために構築されてきたインターネットの基幹通信網は、完全に民営化されてきました。

この間にネットワークを商用利用する道が模索され、1989 年に設立された CIX(Commercial Internet eXchange)というインターネット接続サービスを提供する商用プロバイダの共同組織は、商用利用のための基幹通信網を管理し、そこに接続するそれぞれのプロバイダ同士の情報交換を行うことによって、企業が

インターネット上で広告や販売活動を行う道を開きました。

他方で NFSNET 自体は、NREN(National Research and Education Network)として、全米情報基盤(NII : National Information Infrastructure)の一部を分担するものとして再編されました。またこの全米情報基盤を実現するものとして、1993 年には「情報スーパーハイウェイ (Information Super Highway) 構想」が提唱されています。これは全米をつなぐ高速なコミュニケーションを実現するための情報通信ネットワークの構築を目標としたものです。

2. 3. 日本のインターネットの始まり

日本のインターネットの歴史は、ボランティア活動を中心に進められてきました。1984 年に研究者レベルの研究用コンピュータネットワークの実験として、主要な大学間で UNIX が搭載されたコンピュータを接続する JUNET (Japan University UNIX NETwork) が始まりました[引用文献 7]。

当初は 3 つの大学 (東京大学, 東京工業大学, 慶応義塾大学) を結ぶネットワークとして実験が開始され、これが日本におけるインターネットの始まりとなり、最終的には約 700 の機関を結ぶネットワークに成長しました。

JUNET の接続形態は、現在インターネットで行われている TCP/IP による接続とは異なるものでした。このネットワークでは、モデムと電話回線を使って UUCP (Unix to Unix CoPy) という接続方法が使われ、電話をかけて電子メールやファイルなどを自分のコンピュータに転送していました。これはアメリカの学術ネットワークであった USENET を手本にしたといわれています。

JUNET は日本のインターネットの発展において先駆的な役割を果たしました。その後 1988 年には WIDE プロジェクト (Widely Integrated Distributed Environments) が設立されたことなどにより、実験ネットワークとしての役割を終え 1994 年に解散しました。

WIDE プロジェクトでは、TCP/IP に基づいたネットネットワークの運用が始まりました。またパソコン用の TCP/IP ソフトが数多く提供されるようになり、1993 年にはパソコン通信との電子メールの交換が始まりました。

また 1992 年に AT&T 社および IIJ (Internet Initiative Japan) が商用プロバイダとしてインターネット接続サービスを始め、さらにこれら国内の商用プロバイダと WIDE プロジェクトの相互接続が実現しました。

近年、日本でもインターネットサービスプロバイダが数多く設立され、インターネットの利用は急激に広がりました。

2. 4. インターネットの構成

インターネットは階層型 (ツリー型) の構造になっています。最下層には個人レベルで利用しているコンピュータがあります。ユーザはこの最下層からインターネットの世界に入っていきます。

これらのコンピュータは、大学や研究機関、企業、官公庁などのさまざまな組織のネットワーク、あるいはプロバイダなどの商用サービスのネットワークに接続されています。

さらにこれらは、地域ごとにまとまった地域のネットワークを構成しています。そして地域のネットワークは、全国的な基幹通信網に接続されており、この基幹通信網を通じて、海外のネットワークに接続しています。

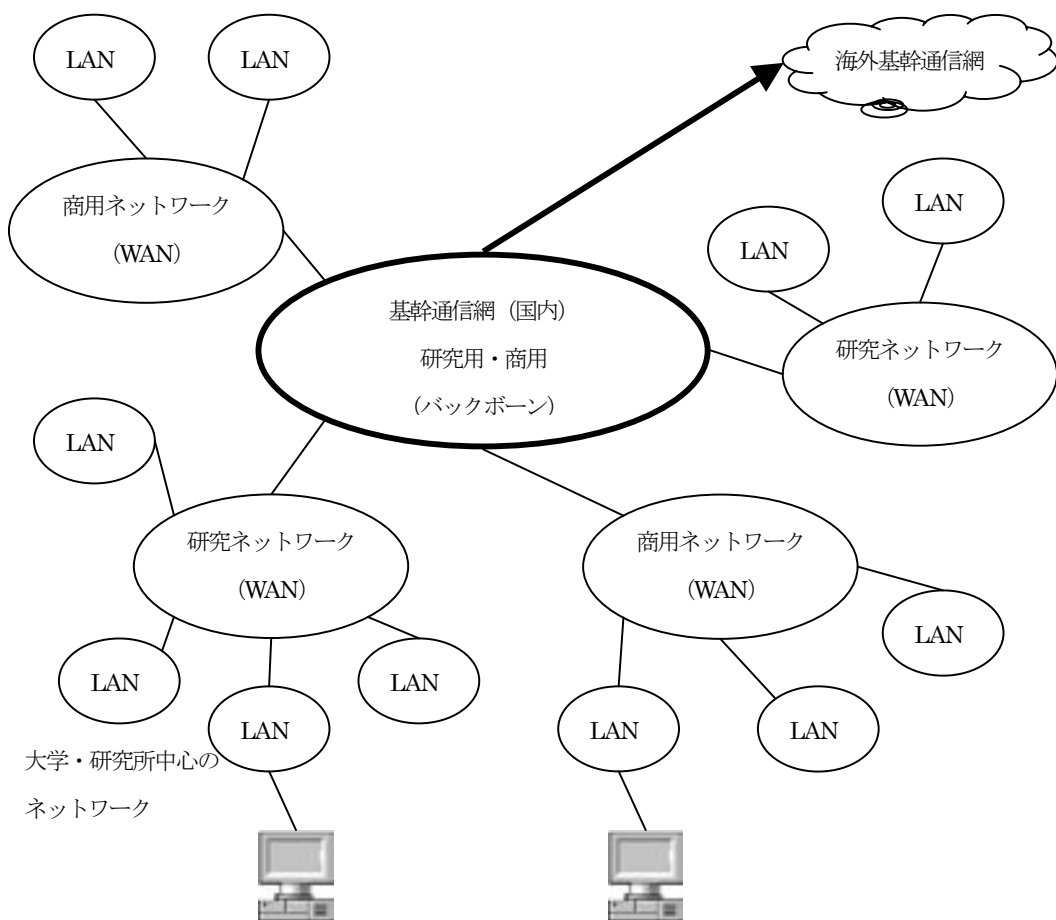


図 2.2 国内インターネットの構成(概念図)

2. 5. 学術研究ネットワークと商用ネットワーク

インターネットを構築しているネットワークは、その成立基盤や経済的な基盤から大きく 2 つに分けられます。ひとつは学術研究を目的とした非営利のネットワークであり、あとひとつは営利を目的とした商用ネットワークになります。

前者は大学や研究機関などが研究を目的として構築しているネットワークのことで、ここでは学術研究を目的とした通信の利用となっています。

後者の商用ネットワークは、営利事業としてネットワークサービスが提供されるもので、ユーザも営利目的の通信が可能になります。

従って、営利を目的とした一般企業は、通常は商用ネットワークへ接続することになりますが、企業の研究所などは、学術研究用のネットワークへ接続する場合があります。またどちらのネットワークに接続しても、お互いに情報交換ができるようになっています。

商用ネットワークは、営利事業としてインターネットへの接続サービスを行っています。米国では政府が企業のビジネス妨害をしてはならないという考え方があり、これが NSFNET の終了につながっています。

NSFNET が終了してからは、米国では大学や研究機関などの非営利組織も商用ネットワークに加入するようになっています。大学などは営利目的の通信をするわけではありません。しかし通信費用がかかるため、対価を払ってネットワークサービスを受けることになっています。日本の大学などもほぼ同じような傾向にあります。学術情報ネットワークなど研究用ネットワークと併用している大学や非営利組織もあります。

2. 6. インターネット関連組織

インターネットは世界中の国々に構築されたさまざまなネットワークの集合体として成り立っています。インターネットの運営を円滑に行い、統括するためのいくつかの組織があります[引用文献 18]。

(1) IETE(Internet Engineering Task Force)

IETE はインターネットに関する技術の研究開発や提案を行う組織です。インターネットのすべての技術がここで議論されます。

(2) IANA(Internet Assigned Number Authority)

IP アドレスやドメイン名などに代表されるインターネットの運用や、サービスのために必要な情報資源の調整と管理を行い、最終的な責任を負う組織です。

(3) ICANN(Internet Corporation for Assigned Names and Numbers)

1998 年にインターネットに関するドメイン名、IP アドレス、ポート番号などの各種資源を、全世界的に調整して管理することを目的に、IANA の業務を引き継いで設立された民間の非営利法人です。最近ではインターネットの商業利用が活発に行われているため、それに伴い商標名とドメイン名の利用において紛争が起きており、このような紛争処理のしくみを定めることも ICANN の役割と考えられています[引用文献 5, 7, 15]。

(4) NIC(Network Information Center)

上で述べた IANA によって決定されたことを具体的に運用管理する組織です。現在はインターネットの急速な発展と変化にすみやかに対応するため、各国で分散して管理を行っています。そのため我が国においても日本ネットワークインフォメーションセンター（JPNIC）設立されており、国内の IP アドレスやドメイン名の割り当てや管理を行っています[引用文献 12]。

（５）IAB(Internet Architecture Board)

インターネットのすべての技術に関する最終決定権を持っている組織であり、技術的なアドバイスなども行います。

（６）ISOC(Internet Society)

インターネットを国際的に代表し、技術開発や運用管理の面からも統括する組織です。この Internet Society は 1992 年より活動を開始し、関連組織を統括しています。またインターネットの相互接続、応用技術の開発、研究、管理、加えて教育研究などの文化的な事業まで幅広く活動を行っています。

（７）IRTF(Internet Research Task Force)

インターネットの方向性や技術開発の方針を長期的な観点から研究する組織です。

2. 7. インターネットの可能性

急速なネットワーク技術の発展を背景に、近年米国をはじめとした先進諸国はあいついで情報技術に関する国家戦略を策定し、国の政策として情報通信技術の発展と情報産業の育成に努めています。

すでに米国では 1993 年には情報スーパーハイウェイ構想が提唱され、その後も新たな情報技術の発展を目指した国家戦略の策定や従来の戦略の見直しが行われ、2000 年には情報通信技術分野の長期的な研究開発を行うために、「Networking IT R&D Program」を策定しています。

これはコンピュータネットワークの発展をより政策的に進めようとするものであり、米国が今後の情報化社会に対応しながら、情報先進国としての地位を築き上げるためといえます。

また日本政府は 2001 年に「e-Japan 戦略」を策定し、各種の情報通信に関連した国家戦略を実施しており、このような政策を策定している国は他にもいくつもあります[引用文献 16]。

これらは情報通信産業が国家の基幹産業として最も重要なものに成長していることを示しており、このような政策が多く の国々において大々的に提唱されるということは、すでにコンピュータネットワークあるいはインターネットが、今後の世界を考える上で、極めて重要な存在になっていることを示しています。

インターネットは、これまでの電話や FAX のような通信手段と統合されはじめています。コンピュータと通信が一体化したものであるため、それらが個別に持つ利点を合わせたもの以上の効果を発揮する可能性があります。

インターネットは、新しいコミュニケーション手段として期待されています。それはインターネットの技術を使えば、世界的な規模でさまざまなコミュニケーションに使える可能性が明らかになったためです。

現在インターネットの上では、電子メールや WWW (World Wide Web) などさまざまな種類のサービスが利用できるようになっています。これらのサービスは主に人と人とのコミュニケーションあるいは情報交換に使われています。

しばらく前まで、この役割を電話や FAX あるいは郵便などで行っていました。これからの情報化社会では、これらすべてのコミュニケーションがコンピュータネットワーク上で可能になりつつあるといわれています。さらに最近のマルチメディア技術の進展は、音声や動画を使った新しいコミュニケーション手段を誕生させています。

》》》 演習 2 《《《

次の演習を行ってみよ。

1. 検索エンジンの使い方と検索結果の検討

「プロトコル」という言葉で次の3つの検索エンジンを使い、検索結果を比較し、どのようなことがわかったかを簡潔にまとめよ。また同じように自分の関心のある言葉で3つの検索エンジンを試し、結果を比較検討せよ。

(1) <http://www.msn.co.jp/>

(2) <http://www.google.ne.jp/>

(3) <http://www.goo.ne.jp/>

》》》 本章の復習 《《《

1. インターネットの起源になったネットワークは何か。
2. インターネットの意味は何か。
3. プロトコルとは何か。
4. 通信でバックボーンとは何か。

3. インターネットのしくみ

インターネットを上手に活用し、そのしくみや社会的な影響などを考えるためには、インターネットを成り立たせている基本的な技術を理解しておく必要があります。

インターネットでは接続しているコンピュータ間で、お互いに1対1または1対多の双方向の通信を直接行うことができます。このようなことを可能にするためには、身近にある自分のコンピュータから発信した情報が、世界中で使われているコンピュータに到達するしくみが必要です。また世界中にあるコンピュータからどのコンピュータに情報を届ければよいのか、目的とするコンピュータを識別するためのしくみも必要となります。

さらにインターネットに接続されているいろいろな種類のコンピュータからは、Web ページの情報をはじめさまざまなサービスが提供されています。これらのサービスを実現し、インターネットの情報交換を支えている主要な技術は、通信規約である TCP/IP プロトコルや、DNS と略称されるドメインネームシステム (Domain Name System)、およびクライアントサーバ型のコンピュータネットワークなどであるといえます。ここではこのようなインターネットのサービスを背後で支える通信の規約について取り上げます。

3. 1. プロトコルとは

一般のデータ通信においては、データのやり取りに先立って、双方の間でデータの送受信に関する規約を定めておく必要があります。この規約のことをプロトコル(protocol)といいます。プロトコルとは転送するデータの形式とその送受信の手続きを定めたデータ通信の規約のことをいいます。

定められたプロトコルに従ってデータを送信すれば、それがどのような機器から送られたとしても、そのプロトコルを理解できるあらゆる機器の間で、正確な通信を行うことができますようになります。

ネットワークに接続されているコンピュータ同士が情報を交換しあう場合にも、お互いのコンピュータに共通のプロトコルを使って、通信することが必要です。あらかじめ定められたプロトコルに従って、情報をやり取りすることにすれば、ネットワークを構成しているコンピュータの機種やオペレーティングシステムが異なっても、データをやり取りすることが可能になります。

3. 2. 会話とプロトコル

プロトコルとはどういうものか、言葉の異なる外国人同士が会話する場合を例にとりて考えてみましょう。人間同士が向かい合った場合の単純な会話の例をあげます。例えばここに日本語しか話すことのできない N さんと、韓国語しか話すことのできない K さん、また日本語と韓国語の両方を話すことができる NK さんがいたとします。そして N, K, NK の3人で話し合いをすることにします[引用文献 18]。

ここでは会話でコミュニケーションを試みることにしますが、このときの日本語や韓国語を「プロト

コル」、会話によってコミュニケーションを試みることを「通信」、そして話の内容を「データ」と考える
とわかりやすくなります。

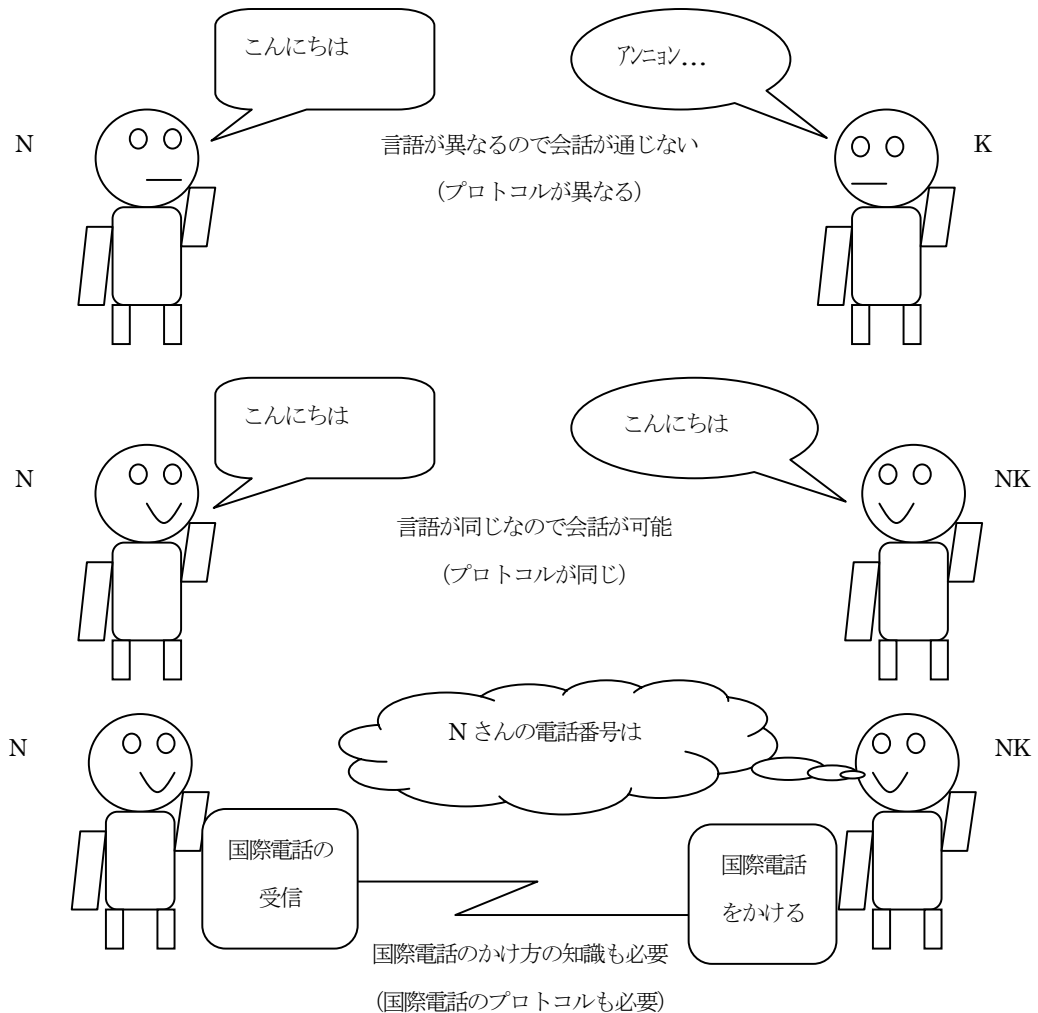


図 3.1 会話と電話におけるプロトコルの考え方[引用文献 9, p.11 より作成]

このような状況のもとで、NさんとKさんが会話をしようと試みても、Nさんは日本語、Kさんは韓国語しか話せないので、そのままではお互いに話している言葉が理解できません。NさんとKさんでは、お互いの言葉が異なるので、NさんとKさんはコミュニケーションすることができません。NさんとKさんとは言語というプロトコルが異なるので、お互いに自分の話の内容(データ)を相手に伝えることができません。

しかし、NさんとNKさんが同じように会話をする場合、NさんとNKさんは共に日本語を話すので、日本語という共通のプロトコルを使って会話をすれば、お互いの話の内容を理解できます。NさんとNKさんは

プロトコルが同じなため、コミュニケーションを行うことができ、その結果データ(話の内容)を相手に理解してもらうことができます。

次にNさん、Kさん、NKさんが国際電話によって会話する場合を考えてみます。NさんとKさんとは先ほどと同じように、日本語と韓国語では言葉のプロトコルがことなるので、国際電話を使ってもコミュニケーションはとれません。

これに対してNさんとNKさんの場合は、日本語というプロトコルはお互いに共通ですが、国際電話による会話を行うときに、日本語という約束事以外にも別な約束事、つまり別なプロトコルが必要になることがわかります。

それは国際電話の使い方や電話機の間での音声の伝え方など、国際電話を使って話し始めるまでの手順やきまりです。どちらか一方が国際電話を使えなかったり、回線がつながらなかったりすれば、コミュニケーションはできないわけです。これらのこともプロトコルと考える必要があります。

3. 3. データ通信とプロトコルの特徴

我々人間は知能や理解力を持っているので、ある程度あいまいな会話でも、お互いに推測したり補ったりして、意思の疎通を正常に保ち、コミュニケーションを行うことができます。しかしコンピュータでのデータ通信は、ケーブルなどのコネクタの形状のような物理的なレベルから、ソフトウェアなどのアプリケーションのレベルまで、多くの部分で明確な処理手順を定め、それに従ったデータの送受信を行わないとコミュニケーションは成り立ちません[引用文献 18]。

コンピュータでデータ通信を行う場合は、両方のコンピュータに、通信に必要なすべてのプログラムを用意しておく必要があります。

我々の場合はほとんど無意識のうちに言葉を発し、伝えたい内容を相手に伝えることができます。コンピュータの場合は、まずお互いが理解できる通信方法を決めておくと同時に、それをどのように相手のコンピュータに伝えるかを決める必要があります。

我々は言葉の途中が一部抜けたりしても、前後の会話から意味を推測することができます。コンピュータの場合は、途中に何らかの障害があつてデータの一部分が届かなかったときはどうするかなど、コミュニケーションを行う上でのありとあらゆることを考慮し、それらを通信するコンピュータ同士が理解できるしくみが必要です。

またプロトコルという用語自体は、通信する上での約束事すべてを意味します。コンピュータの通信には、約束事が数多く定められており、そのため一般のユーザには見えない部分にも、数多くのプロトコルが存在しています。

プロトコルというのは単純に考えれば、お互いにコミュニケーションするために必要なすべての約束事というように考えておくことができます。

3. 4. プロトコルの開発と標準化

コンピュータでデータ通信を行う場合は、お互いの通信のしかたを取り決めたプロトコルすなわち通信規約が重要な意味を持っています。インターネットでTCP/IP プロトコルを使った通信が行われるようになるためには、多くの機器を支障なく接続するための標準化した規格を作成することが必要でした。

標準化(standardization)というのは、自由に放置しておく多様化や複雑化によって無秩序化し、社会的な混乱の原因となりそうなものに対して、それらを少数化や単純化によって秩序化することを言います。多くは製品の性能、品質、安全性、大きさなどについて取り決めを定めて規格化し、それに従って製品を開発して生産します。コンピュータによる通信の場合には、通信機器を連結するための通信媒体の標準化のほかに、媒体を流れるデータを送受信する手続きの標準化も必要になります。

コンピュータを利用したデータ通信のことを、コンピュータ通信ということがあります。1960年代の後半にコンピュータ通信の研究が開始されたころには、当然ながら標準化はまったく考えられていませんでした。

その後もそれぞれのコンピュータメーカーは、独自の考え方に基づいてネットワークの体系を作っていました。そしてその中で各プロトコルの役割と機能を決め、独自のプロトコルを複数使用して、コンピュータ通信を実現していました。

コンピュータによるデータ通信は、ひとつのプロトコルだけで実現しているわけではありません。複数のプロトコルの連携プレーによって成り立っています。いわば複数のプロトコルがそれぞれの役割に応じ、段階的に機能することによってデータの送受信を行い、コンピュータ通信が可能になっています。

これらの通信を行うための体系のことを、ネットワークアーキテクチャ(network architecture)といいます。この体系を実現するためには複数のプロトコルが必要です。標準化が行われる前は、それぞれのメーカーが独自のネットワークアーキテクチャを持ち、各メーカー単位でコンピュータ通信を行っており、これらは当然ながら他社との互換性のないものでした。

しかしネットワークの重要性や便利さが理解されるようになると、ネットワークを利用して通信を行えば、さらにさまざまな可能性が開けることが明らかになってきました。

そして異なるメーカーのコンピュータ同士でも、ネットワークを通して通信を行いたいという要望が強くなり、コンピュータ通信の国際的な標準化が検討されるようになってきました。こういった経緯のなかで OSI (Open System Interconnection) 参照モデルが考案され、ネットワーク体系の標準化が実現されました。この OSI 参照モデルは、1977 年に国際標準化機構 (ISO: International Standard Organization) が作成したネットワークアーキテクチャの標準化モデルであり、開放型システム間相互接続と訳されています。

ネットワーク体系の標準化という場合、異なるメーカーの機器の間でも、お互いに通信が可能になり、コミュニケーションをとることができる基準を作ることを意味します。

標準化作業によって国際標準 (international standard) が作られ、すべての機器がそれを採用するようになれば、共通の通信手順が使えるようになり、世界中のコンピュータとコミュニケーションができるよ

うになります。

情報通信は世界的な規模で行われるので、プロトコルの標準化も世界規模で検討が行われます。いろいろな公的な標準化機関があり、そこで標準化の検討が行われ、国際標準が決まることもあります。あるいは民間企業が集まって団体を組織し、標準となるプロトコルを作成することもあります。

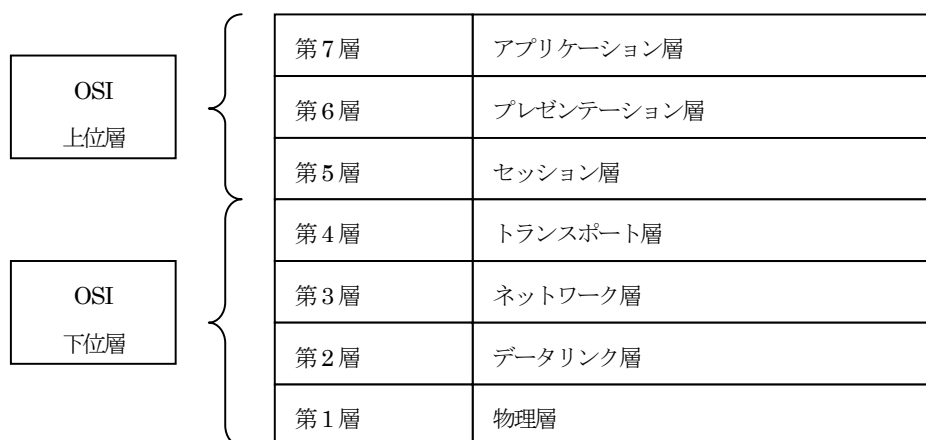
また、先んじて開発に成功した企業などが使い始めたプロトコルや製品などが、その業界における事実上の標準(de facto standard あるいは実質標準) となって広まることもあります。

現実の世界では、技術的に優れているものが必ずしも国際標準となるわけではなく、優れた技術が普及しなかった例は、通信やコンピュータ関係だけでなく、家電製品などをはじめ他の分野でもしばしば見られることです。また標準化されると、社会的にも非常に大きな影響を世界中に与えることが少なくありません。

ISO では OSI 参照モデルに基づき、コンピュータネットワークの世界標準をめざして OSI プロトコルを開発しましたが、TCP/IP が先に普及してしまったため、使われないものになってしまいました。しかしネットワークの仕様などについて記述する場合には、OSI 参照モデルに定義されている用語のほうが便利のため、しばしば使われます。TCP/IP は開発後 OSI 参照モデルに基づいたさまざまな改良が行われ、現在も続いています。

3. 5. OSI 参照モデル

OSI 参照モデルは、コンピュータ通信を実現するための考え方や、体系のモデルを示したもので、各メー



カーで共通に使用するため、ネットワークアーキテクチャを標準化したものです (図 3. 2)。

図 3.2 OSI 参照モデルのプロトコル階層

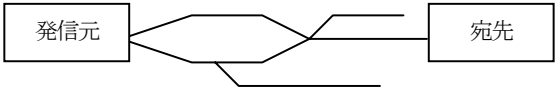
OSI 参照モデルは、下から順番に第1層から第7層までの層(layer)に分けられています。それらは階層構

造(layered architecture)となっており、それぞれ物理層、データリンク層、ネットワーク層、トランスポート層、セッション層、プレゼンテーション層、アプリケーション層と呼ばれ、各層ごとに役割が明確に決められています。このような階層構造になっていることから、プロトコルスタック(protocol stack)と呼ばれこともあります。

ネットワークアーキテクチャを構築しているプロトコルは、この OSI 参照モデルにおける各層のいずれかに属するようにその役割が定められており、各層で行われることをサービス(service)と呼んでいます。

OSI 参照モデルでは、各層でどのような役割を行うかということを定めたもので、そこでの具体的なプロトコルの機能を定めたり、それらの使用を強要したりするものではありません。しかし、各プロトコルはこの OSI 参照モデルの 7 層のうち、いずれかに該当するようになっています (表 3.1)。

表 3.1 OSI 参照モデルの各層の役割

上位	7	アプリケーション層	<p>ユーザにメールや WWW などのさまざまなサービスを提供する。</p> <p>ユーザにサービス提供 → メール・WWW</p>
	6	プレゼンテーション層	<p>上位層から来たデータは 0 と 1 のビット列に変換し、逆に下位層から来たデータはユーザに読めるように変換する。</p> <p>上位層からの入力データ → 変換 → 通信形式</p> <p>下位層からの入力データ → 変換 → ユーザが読める形式</p>
	5	セッション層	<p>宛先にデータを送信するための経路の確立や開放を行う。</p> <p>発信元 → 経路確立要求 → 宛先</p> <p>発信元 ← 確立 OK ← 宛先</p> <p>発信元 → 経路開放要求 → 宛先</p> <p>発信元 ← 開放 OK ← 宛先</p>
下位	4	トランスポート層	<p>データに落ちがないかどうかの確認を行い、宛先に確実にデータを届ける役割をする。</p>
	3	ネットワーク層	<p>宛先にデータを届けるため、宛先の確認や通信の経路選択を行う。</p> 
	2	データリンク層	<p>宛先との物理的な通信路を確立し、通過しているデータのチェックとエラーの検出を行う。(通信技術)</p>
	1	物理層	<p>データ(ビット列)をケーブルなどの回線に送り出すため、電気信号に変換して送出を行う。(通信媒体)</p>

3. 6. OSI 参照モデルとデータ送信

メッセージを送信する例で、具体的に OSI 参照モデルにおけるデータ送信のしかたを説明します。

X さんは発信元コンピュータ PC-X から、宛先コンピュータ PC-Y の Y さんにメッセージを送ることにし、ここでは X さんから Y さんに向けて、「こんにちは」という言葉を送ることにしておきます。なお以下で単に通信という場合は、デジタル化されたデータ通信のことを意味します[引用文献 18]。

(1) アプリケーション層

X さんは最初にコンピュータ PC-X の上で、メッセージ送信ソフトを使い、「こんにちは」とキーボードから入力します。このときにメッセージ送信ソフトを、通信に関係する機能と関係のない機能に分けて考えます。

「こんにちは」と言葉を入力することは、通信と関係なく行われます。書き込みが終わり、これを送信するところから通信と関係してきます。この通信と関わる部分が、アプリケーション層の主要な役割となります。

ここではメッセージ送信ソフトが言葉を書くサービスを提供し、そこで書かれたデータを、送信するためのプログラムに引き渡します。

(2) プレゼンテーション層

上で入力した「こんにちは」という言葉を、プレゼンテーション層で 0 と 1 を使って、ビット列に変換します。

(3) セッション層

この層では「こんにちは」という符号化されたデータを送信するために、発信元コンピュータ PC-X から宛先コンピュータ PC-Y への通信路であるコネクション(connection)を確保します。

(ここまでの上位層の処理になり、以下からトランスポート層より下の処理となります。)

(4) トランスポート層

この層はデータを確実に相手に届ける役割をはたします。発信元コンピュータ PC-X と宛先コンピュータ PC-Y の両方のトランスポート層では、データ送信に誤りがないかどうか確認をします。

例えば送信データがどこかで欠落し「こんにちは」ではなく、「こんに」としか相手に届かない場合も起こりえます。

宛先コンピュータ PC-Y は、発信元 PC-X に受け取った部分が「こんに」であることを知らせ、「ちは」の部分が届いていないことを知らせます。これによって PC-X は届いていない部分のデータを知ることができ、足りない部分である「ちは」を再び送信してきます。

(5) ネットワーク層

相手にデータを送信したり、通信路を確保(これをコネクションを張るという)したりするためには、相手先のアドレスを知る必要があります。ネットワーク層では送信相手のアドレスを目標にして、どこを通じて通信するかという経路選択を行います。

(6) データリンク層および物理層

実際につながっているケーブルなどの通信媒体を使って、これらのデータの伝送が行われます。データリンク層では、イーサネットなどの通信技術を使って通信路の確立を行います。物理層では電気信号に変換し、光ファイバーなどの通信媒体を通して、相手先まで送信されます。データリンク層には、イーサネットなどのような物理層の上で行われるデータ通信技術が該当します。物理層は銅線の同軸ケーブルあるいは光ファイバーなど、通信を行うための物理的な通信媒体のことです。

(7) 受信側コンピュータ PC-Y 側の処理

発信元コンピュータ PC-X からのメッセージを受け取った宛先コンピュータ PC-Y は、これらと逆の動作を行い、物理層から上位層にデータを引き渡していきます。最終的に Y さんは、コンピュータ PC-Y のメッセージ送信ソフトで、X さんからの「こんにちは」を読むことができます。

表 3.2 OSI 参照モデルとデータ送信の例

上位	7	アプリケーション層	「こんにちは」とキーボードから入力。データを送信するためのプログラムに引き渡す。
	6	プレゼンテーション層	上で入力した「こんにちは」を、0 と 1 を使ってビット列に変換。
	5	セッション層	データを送信するために、コンピュータ PC-X からコンピュータ PC-Y への通信路を確保。
下位	4	トランスポート層	コンピュータ PC-X とコンピュータ PC-Y の間でデータ送信に誤りがな いかどうか確認。
	3	ネットワーク層	宛先のアドレスを目標にして経路選択を行う。
	2	データリンク層	宛先との物理的な通信路の確立とエラーの検出。
	1	物理層	ビット列を電気信号に変換して宛先まで送信。

》》》 演習 3 《《《

ネットワークを活用したグループウェアのソフトをインストールし、どのように動作するかを体験してみよう。利用するソフトは「IP Messenger」というソフトで、LAN につながったパソコンのユーザにメッセ

ージを送ることができる。

1. ソフトの準備

IP Messenger のソフトを入れたフォルダを用意してあるので、そのフォルダをマイドキュメントにコピーしてソフトを準備する。フォルダ内には解凍した4つのファイル(IPMSG.EXE, OPENLAB.TXT, README.TXT, SETUP.EXE)が用意してある。

[フォルダのあるところ]

¥¥マイコンピュータ¥nftea の home\$¥dobashi¥lecture¥windows

[フォルダ名]

ipmsg32_142

(1) インストールとセットアップ

教室の設定では一般の学生にソフトのインストールを許可していない場合が多い。しかし IP Messenger はインストールしなくてもそのままで動作可能である。

教室以外でインストールが可能な場合は、次のようにしてインストールを行えばよい。

ipmsg32_142 というフォルダをマイドキュメントに作成(あるいはコピー)したあと、そのフォルダの中にある SETUP.EXE を左ボタンでダブルクリックし、セットアップを起動する(図 4.12)。



図 4.12 IP Messenger のセットアップ画面

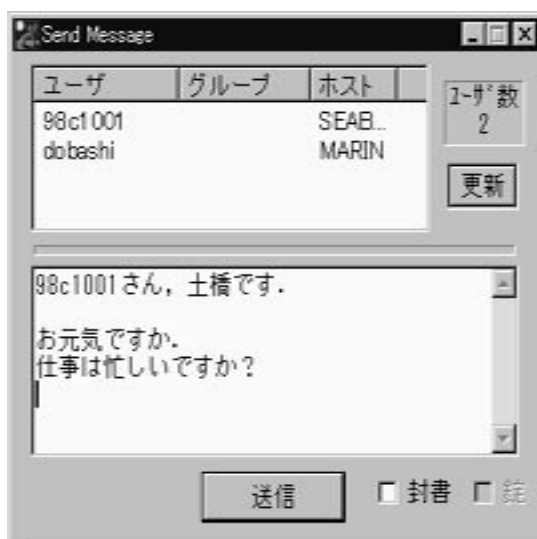


図 4.13 IP Messenger の起動画面

セットアップのダイアログボックスが開いたら、指定したフォルダにインストールするか、あるいはセ

ットアップと同じ場所の IPMSG (IP Messenger) をそのまま使うかのいずれかをチェックする。

(2) アンインストール

不要になってソフトを削除したいときは、アンインストールをクリックして実行する。なお教室ではアンインストールしたいときは、IP Messenger のフォルダを削除する。

(3) 詳細設定

この詳細設定では、プログラムの起動用アイコンやメニューを出すかどうかを指定する。教室ではセットアップが起動しないので詳細設定ができないが、しなくても特に問題なく動作する。

(4) 起動の仕方

IP Messenger プログラムのアイコンをダブルクリックして起動する (図 4. 12)。

2. 次の演習を行ってみよ。

- (1) README. TXT を読んで、使い方を調べよ。
- (2) 誰かログインしている人にメッセージを送ってみよ。
- (3) 届いたメッセージに返事を書いてみよ。
- (4) 複数の人に同時に送れるかどうか試してみよ。
- (5) 不在モードを使ってみよ。それはどのようなときに使えそうか。

3. 次の点について考えてみよ。

- (1) 電子メールとどのような違いがあるか。
- (2) どのようにしてユーザを探してくるか、そのしくみはどうなっているか。
- (3) どのようにして相手にメッセージが送られるか、そのしくみはどうなっているか。

》》》 本章の復習 《《《

1. 標準化とはどういうことか。
2. OSI 参照モデルとはどういうものか。
3. ネットワークアーキテクチャとはどのようなことか。
4. OSI 参照モデルの物理層というのは、実際には何のことか。

4. TCP/IP

1969 年から始まった ARPANET の研究において、米国国防総省はコンピュータネットワークを構築するため、通信技術の研究開発や実験を積極的に行いました。

この実験の中で、大学と研究機関を結ぶ幹線上で行われるパケット交換だけでなく、ネットワークの最下層に位置するコンピュータとコンピュータ（または端末と端末）の間を結ぶようなエンドノード間においても、確実にコミュニケーションができる方法を実現するため、通信プロトコルの開発実験が行われました。

1970 年代には TCP/IP (Transmission Control Protocol/Internet Protocol) プロトコルの開発が進められ、試作したソフトウェアが実際にコンピュータ上で動作するようになりました。その結果 1975 年に TCP/IP が開発されました。そして TCP/IP は 1982 年ごろまでかかって細部の仕様が決められていきました。

1980 年代には大学や研究所などでは、コンピュータのオペレーティングシステムとして BSD (Berkeley Software Distribution) が開発した UNIX というソフトウェアが用いられるようになり、この中に TCP/IP が組み込まれました[引用文献 17]。

1983 年には ARPANET の正式な接続方式として TCP/IP が採用されることになり、同じ年に米国のサン・マイクロシステムズ社が、一般ユーザ向けのオペレーティングシステムとして、TCP/IP を組み込んだ UNIX ワークステーションの提供を開始しました。

このようにして LAN の発達と UNIX を搭載したワークステーションの普及が急速に進み、これに伴って TCP/IP も広く使われるようになりました。ここでは TCP/IP の基本的なしくみを取り上げます。

4. 1. TCP/IP プロトコル

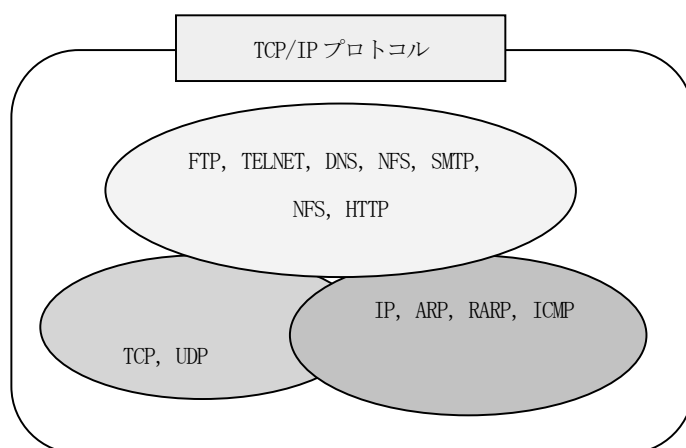


図 4.1 TCP/IP 通信のプロトコル[引用文献 18, p.46 より作成]

TCP/IP プロトコルは、主に TCP と IP という 2 つのプロトコルから成り立っています。また実際に TCP/IP という用語を使う場合は、これら 2 つのプロトコルだけではなく、TCP/IP 通信に関わっているいくつかのプロトコルも含めて使うことがあります [引用文献 18]。

どのプロトコルが TCP/IP に含まれるかという明確な定義はありません。関連した主なプロトコルには HTTP(Hyper Text Transfer Protocol), TELNET(Telnet Protocol), FTP(File Transfer Protocol), SMTP(Simple Mail Transfer Protocol)など、インターネット上で通信を行うアプリケーションソフトに広く利用されているものが多数あります(図 4. 1)。

4. 3. OSI 参照モデルと TCP/IP

TCP/IP に含まれるさまざまなプロトコルも、OSI 参照モデルのプロトコル階層に対応させて考えることができます。それぞれのプロトコルが行う基本的な役割は、OSI 参照モデルの各層ごとの役割と基本的にはあてはめることができます。

TCP/IP には下位層から順番に、物理層、データリンク層、インターネット層、トランスポート層、アプリケーション層があります。ここでは TCP/IP プロトコルが OSI 参照モデルのどの層に該当するか、またそれぞれのプロトコルがどのような役割を果たしているかなどについてまとめておきます (表 4. 1)。

表 4.1 OSI 参照モデルの各層の役割と TCP/IP の対応関係

	層	OSI	TCP/IP	対応する主なプロトコル
上位	7	アプリケーション層	アプリケーション層	TELNET, FTP, SNMP, SMTP, NIS, NFS, DNS, HTTP
	6	プレゼンテーション層		
	5	セッション層		
下位	4	トランスポート層	トランスポート層	TCP, UDP
	3	ネットワーク層	インターネット層	IP, ARP, RARP, ICMP
	2	データリンク層	データリンク層	イーサネット, FDDI, ISDN, X. 25 (通信技術)
	1	物理層	物理層	同軸ケーブル, UTP, 光ファイバー (通信媒体)

TCP/IP プロトコルは主に、インターネット層から上位の層でそれらの役割を果たします。データリンク層と物理層の下位 2 層は、OSI 参照モデルでは明確に分けて定義されています。しかし TCP/IP ではこの下位 2 層に該当するプロトコルについて明確に定義されていません。そのため TCP/IP ではこれらの下位 2 層をひとつの層として扱う場合もあります。

しかしここでは OSI 参照モデルに対応させたほうがわかりやすいため、データリンク層と物理層に分け

で示しています。なおデータリンク層には、イーサネットのような物理層の上で行われるデータ通信の技術が該当し、物理層は銅線あるいは光ファイバーなど、通信を行うための物理的な通信媒体のことです。

それぞれのプロトコルが OSI 参照モデルのどの層に該当するかがわかれば、そのプロトコルがどのような役割のためのものかが理解しやすくなります。さらにその役割を実現するために、技術的にどのようなになっているかを理解すればよいわけです。

詳しいことは TCP/IP の仕様を定義している RFC(Request For Comments) という文書に説明があります。RFC はインターネットのプロトコルについて定義した文書です。インターネットで使われるプロトコルなどの仕様はこの文書で提案されます。しかしこの文書の全てがインターネットの標準となっているわけではありません。RFC の文書はインターネットに公開されています[引用文献 13, 14]。

4. 3. データの単位と名称

インターネットにおけるデータ通信では、データは一塊のパケットとして伝送されます。パケットはヘッダとペイロードから構成されています。ペイロードには宛先に送りたい情報が格納され、パケットにはペイロードを宛先に届けるために必要な制御情報が格納されます。

インターネットではデータがプロトコル階層におけるさまざまな段階を経由して処理されます。そのためパケットという呼び名は、データの単位を表す一般的な総称として使われており、それぞれのプロトコル階層において、パケットには別々な名称が付けられています(表 4. 2) [引用文献 15]。

表 4. 2 TCP/IP におけるデータの名称[引用文献 15, p. 83 より作成]

TCP/IP	データの名称
アプリケーション層	データ □□□□
トランスポート層	セグメント ■□□□□
インターネット層	データグラム ■■□□□□
データリンク層	フレーム ■■■□□□□■
物理層	(ビット伝送) 100101100****1100011

LAN ではイーサネットによる通信をおこなうためパケットを生成します。このパケットはデータリンク層のプロトコルによって生成され、多くの場合これをフレーム(frame)と呼びます。イーサネット上ではフレームが送受信されます。

また LAN にパケットを流すためにはホスト上で TCP プロトコルもパケットを生成します。このパケットはセグメント(segment)と呼ばれます。

さらにインターネットでは後述する IP プロトコルがデータ通信の役割を担い、パケットの送受信を行います。このパケットは IP データグラム(IP Datagram)またはデータグラムと呼ばれており、インターネット

ト上で送受信されるパケットは IP データグラムになります。

なお表 4.2 の中の■は、それぞれの階層で付加されるヘッダがあることを示したものです。

これらはいずれもデータの一塊を表しています。フレーム、パケット、データグラムの3つの用語は、データを表す基本的な単位であり、意味はほぼ同じと考えて差し支えありません。

4. 4. インターネット層

インターネット層のプロトコルは、ネットワークに接続したホストとホストの通信を行うもので、そのためにインターネットプロトコル (Internet Protocol) が利用されています。略して IP プロトコルあるいは単に IP ということがしばしばあります。現在は IPv4 (Internet Protocol Version 4) が多く使われていますが、今後はより新しい IPv6 へ移行しつつあります。

ネットワーク層では、アドレッシング (addressing) およびルーティング (routing) を行います。データを送信する場合に、どこに送ればよいかという宛先の決定のことをアドレッシングといいます。

またどこを通して送ればよいかという経路の選択を決定することがルーティングになります。これらがうまく機能して宛先の決定を行っています。IP プロトコルはこれらのインターネット層に与えられた機能を具体化したもので、詳しくは第5章で触れます。

4. 5. トランスポート層

トランスポート層では、2進数の0または1のビット列に変換されたデータの流れを制御しています。この層では TCP と UDP というプロトコルが該当します。TCP プロトコルは、伝送速度は多少遅くても、伝送間違いを少なくするために信頼性を高めた仕様となっています。UDP プロトコルは TCP プロトコルとは逆に、信頼性は低くても、伝送速度を速めるための仕様を取り入れているという特徴があります。

アプリケーションソフトウェアは、その目的に応じてトランスポート層のいずれかのプロトコルを選択し、データの送受信を依頼します。

(1) TCP プロトコル

TCP (Transmission Control Protocol) は伝送を制御する通信規約という意味であり、コンピュータとコンピュータの間において、確実な通信を行うために開発されたものです。通信の途中でデータが消滅したり、パケットの順番がばらばらになって届いたときも、TCP プロトコルが元の順番どおりに再び組み立ててくれるなど、うまく解決するしくみを取り入れられています。

TCP はコネクション型のプロトコルといわれます。コネクションとは、ネットワークの中で通信を行う2つのアプリケーションあるいは通信機器などが、パケットの送受信を行うために、専有して使用できるように、仮想的な通信路を確立することです。またコネクションによって確立した仮想回線をバーチャルサ

ーキット(virtual circuit)と呼んでいます。

コネクション型のプロトコルは、相手とデータの送受信を行う場合に、1つのデータが届くたびに、決められた方法で返事を送り返すしくみを持っています。返事が来るかどうかによって、データが正確に届いたか否かの確認を行っているわけで、これによってデータを間違いなく届けるための信頼性をより高める工夫をしています。TCP プロトコルは文字を含むような Web ページのテキスト部分やメールなど文字データのファイルの送受信に使われます。

(2) UDP プロトコル

UDP (User Datagram Protocol) は TCP とは逆に、コネクションレス型のプロトコルになっています。コネクションレス型というのは、データ通信の際に相手からの受信確認を行わないものです。自分で送信したデータが相手に届いているかどうかなどは確認しないでデータの送信を行います。

そのため受信先に届かない場合も発生します。しかしコンピュータのデータ通信では接続端末の全部と通信を行うこともあり、そのようなときに役立ちます。インターネット上で音声や動画などマルチメディア情報を配信するのに使われます。画像などは全部のデータが届かなくても、届いた部分から再生できるので、UDP のようなプロトコルも必要です。

4. 6. アプリケーション層

TCP/IP では最上位のアプリケーション層が、ユーザへのサービスを提供しています。一般のユーザがアプリケーションソフトを使う場合に用いるプロトコルや通信サービスが、最上位のアプリケーション層に多数あります。それらは TCP/IP の開発時に用意されたものから、その後一般ユーザが独自に開発したものも含んでおり、このアプリケーション層の部分が最も一般的なユーザに近いところで動作しています。

この層のプロトコルには、HTTP、TELNET、FTP、SMTP、NNTP、SNMP、DNS などがあります。これらのプロトコルはサーバとクライアントとの間において、さまざまな目的を達成するためのデータの送受信を行うプロトコルとなっています。ここではこれらのプロトコルとしての機能の概要をまとめておくことにし、詳しくは第7章インターネットのサービスで触れます。

(1) HTTP プロトコル

HTML (Hyper Text Markup Language) で作成したハイパーテキストによってホームページを公開する WWW (World Wide Web) サービスでは、HTTP (Hyper Text Transfer Protocol) プロトコルが使われています。HTTP プロトコルは、Web ページを送り出す役割を担う WWW サーバとブラウザとの間で、データをやり取りするために決められたものです[引用文献1]。



図 4.2 HTTP と Web ページ

(2) TELNET プロトコル

TELNET (Telnet Protocol, Telecommunication Network Protocol) プロトコルは、ネットワークをとおして仮想端末機能を提供する機能で、遠隔地にあるコンピュータをあたかも自分の目で使うかのごとく使用することができます。この機能によって遠隔地の端末からホストコンピュータを操作して、遠隔地に居ながらさまざまなデータ処理を行うための通信を行うことができます。ネットワークに接続しており、TCP/IP が用意されているすべてのコンピュータに接続することができます。

TELNET プロトコルを用いたコマンドとして telnet (小文字) が用意されており、相手先のコンピュータに TELNET で接続することをログイン (login) するといいます。

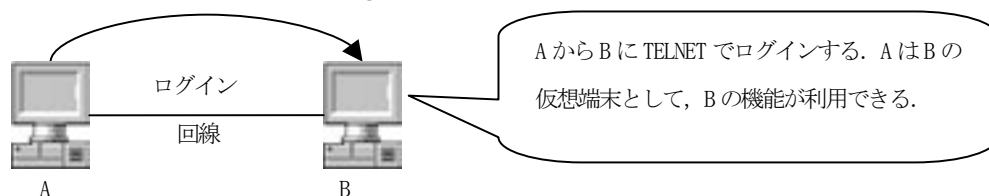


図 4.3 TELNET とログイン

(3) FTP プロトコル

FTP (File Transfer Protocol) は、コンピュータ間でファイルの転送を行うときのプロトコルです。FTP も TCP/IP 通信のなかでは頻繁に使われるサービスになっています。

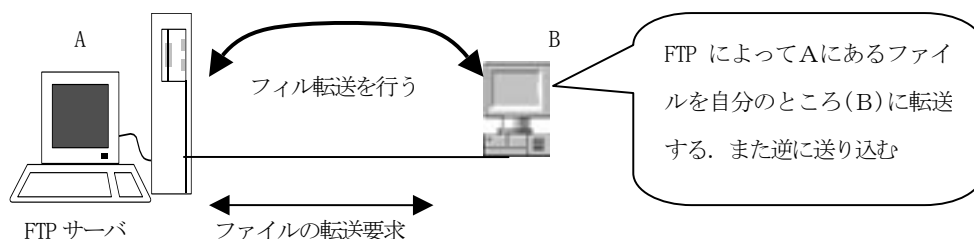


図 4.4 FTP とファイル転送

ファイル転送というのは、別なコンピュータ上においてあるファイルを、自分のコンピュータ上に持つ

できたり，自分のコンピュータ上にあるファイルを別なコンピュータ上に送り込んだりすることです。

(4) SMTP プロトコル

インターネットには，いろいろな組織のコンピュータが接続しており，その上では電子メールを交換するメールサーバが動いています。インターネットで電子メールをやり取りするためのプロトコルがSMTP(Simple Mail Transfer Protocol)プロトコルです。

電子メールはネットワーク上の郵便であり，自分のメッセージをネットワークをとおして，簡単に相手に伝えることができ，TCP/IP 通信の重要なサービスのひとつになっています。

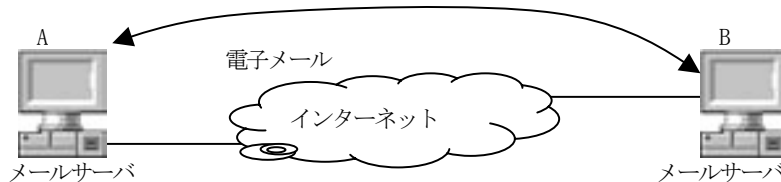


図 4.5 SMTP と電子メール

(5) NNTP プロトコル

NNTP(Network News Transfer Protocol)プロトコルは，電子ニュースを転送するときのプロトコルです。電子ニュースは，Web ページで行われている掲示板と同じようなもので，不特定多数の読者を対象に情報を発信します。

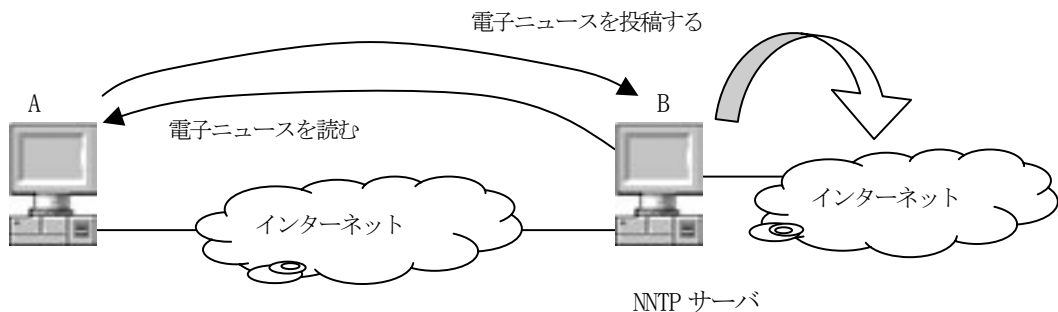


図 4.6 NNTP と電子ニュース

電子ニュースにはさまざまな仕事や，趣味，スポーツなど多種多様の分野があります。また組織内だけのニュースを運営したり，地域内，国内，そして世界中に向けて公開するために運営されるものなど，ニュースをさまざまなグループによって分けることができます。

(6) SNMP プロトコル

SNMP(Simple Network Management Protocol)プロトコルは，ネットワーク管理機能を提供するものです。

SNMP を使用すると、接続する端末を定期的にチェックして管理することができます。何らかの異常が生じたときには、それらに障害が発生したことを知ることができます。

SNMP プロトコルでは、サーバ上でネットワークを管理する SNMP マネージャを運用し、クライアントの上では SNMP エージェントを動作させます。ネットワークを構成する機器は、マネージャを運用するためのサーバと、管理の対象となるコンピュータやルータおよびハブなどの通信機器に分けられます。

SNMP エージェントは、自らの機器に何らかの異常が発生したときに、トラップ(trap)と呼ばれる信号をマネージャに送ります。それを受け取ったマネージャは、機器に障害が発生したことを知ることができます。

またマネージャは、エージェントになっている機器が正常に動作しているか否かを定期的に確認します。動作確認のために送った信号に対して、エージェントから何も返答がないときは、何らかの障害が起きていると考えられ、ネットワーク管理者に通知します。

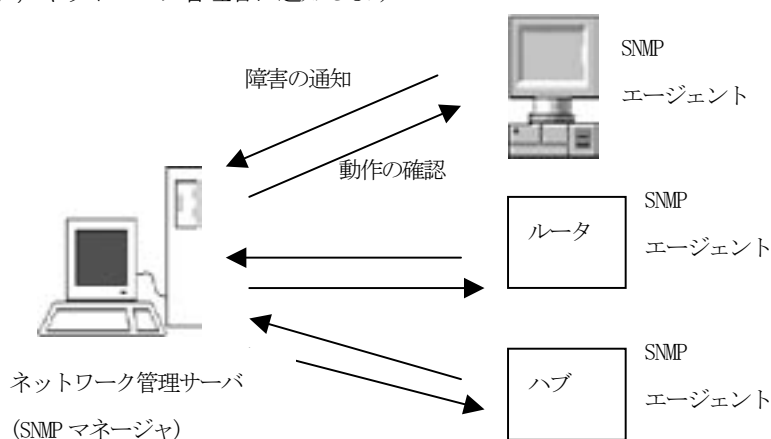


図 4.7 SNMP とネットワーク管理

4. 7. LAN と TCP のヘッダ形式

TCP/IP は、LAN と LAN の接続を可能にするプロトコルでもあります。LAN 上の通信技術には、イーサネット、トークンリング、FDDI などがあります。LAN などのネットワークではこれらの通信技術が使われ、TCP/IP プロトコルによってコミュニケーションが行われています。

最近の多くの LAN ではイーサネットが通信技術として使われ、イーサネットは通信技術なので、TCP/IP のプロトコル階層ではデータリンク層に該当します。ここではデータリンク層から物理層にデータが渡され、さらに宛先のコンピュータにパケットが届くまで、どのようなしくみでデータが処理されるか、IEEE802.3 の例で説明します。IEEE802.3 というのはイーサネットをもとに標準化された通信技術の規格です。ここでは IEEE802.3 (イーサネット) の例を使いますが、他の通信技術でも流れは基本的に同じようになっています。

4. 7. 1. イーサネットヘッダ

イーサネットにおいてパケットの送受信が行われると、TCP/IP のデータリンク層では、上位層にあたるネットワーク層から送られてきたパケットを下位層に伝送するために、ヘッダと呼ばれるパケットの管理情報が付加されます。

このヘッダの後ろにペイロードがあり、そこには実際に送受信される元のデータが入っています。つまり送受信されるパケットのひとつひとつには、伝送に必要な情報がヘッダとして自動的に生成されて付加され、そのヘッダは実際の送信内容の情報が格納されたペイロードの先頭に添付された形となって、下位層に送られます。

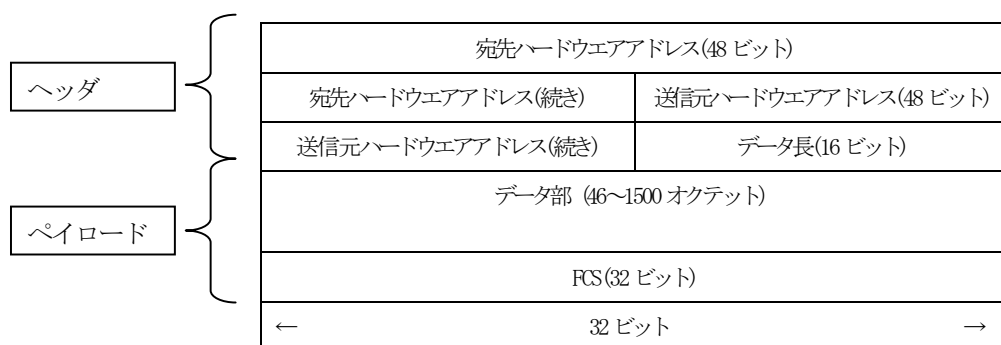


図 4.8 イーサネットヘッダ(ペイロードの部分の単位がオクテットであることに注意)

[引用文献 15, p.110 より作成]

イーサネットのヘッダ部は、宛先ハードウェアアドレス(destination hardware address)と送信元ハードウェアアドレス(source hardware address)のそれぞれのフィールドが 48 ビットずつあります。これらの後ろには、データ長を格納するフィールドが 16 ビットあります。これらの合計 112 ビットでヘッダが構成されています[引用文献 15, 18]。

またハードウェアアドレスというのは、MAC(Media Access Contorol)アドレスや物理アドレス(Physical Address)と呼ぶこともあり、通信に使う機器自体を識別する番号のことです。その番号はネットワークカードなどネットワーク接続機器に、メーカーによってあらかじめ記録されており、変更することができないようになっています。

データ長のフィールドは、データフィールドの有効データ長をオクテット (1 オクテット=8 ビット) 単位で指定します。

ペイロード (データ部) はデータ長の次のフィールドから始まり、その中に上位層から伝送された元の情報が組み込まれています。この場合のペイロードには、データリンク層より上位層の情報が入ります。

データリンク層から見れば、上位層から受け取るものは全部一塊のデータとして認識することになります。逆に言えば IP プロトコルなどの上位層のパケットは、図 4.8 に示したパケットのヘッダを除いたペイ

ロードの先頭から始まることがわかります。

パケットの長さはネットワークの伝送容量によって変化します。高速なネットワークでは、比較的長いパケットの伝送が可能となります。これに対して低速のネットワークでは、短めのパケットだけ伝送を許すようにしています。10Mbps の伝送速度の LAN においては、イーサネットのペイロードの長さは 1,500 バイトまでとなっており、現在のインターネットでもパケットの伝送は多くの場合 1,500 バイトに制限されています。

またペイロードの最後の部分には、FCS(Frame Check Sequence)フィールドが付いています。データ通信においては、1 ビットの誤りでも重大な問題を引き起こす危険性があります。そのため FCS フィールドでは伝送中に起こるビット誤りを検出するために、巡回符号(Cyclic Redundancy Check Code)と呼ばれるビット誤り検出機能が使われています。

イーサネットの場合は下位の 2 層に該当するプロトコルなので、ペイロードの最初に入っているのは 3 層にあるインターネット層のプロトコルである IP プロトコルになります。

IP プロトコルにも IP ヘッダがあります。これは IP プロトコルで必要な情報が組み込まれています。そしてヘッダの後ろには同様にペイロードが結合されており、IP プロトコルよりさらに上位のトランスポート層の TCP プロトコルが入ることになります。

ヘッダはそれぞれのプロトコルが、実際にパケットになった形として考えればわかりやすくなります。どのプロトコルにもこのヘッダという概念があります。このヘッダの情報と実際のデータが格納されるペイロードの部分に合わせて 1 つのパケットができあがり、これらを解析してコミュニケーションが行われるしくみになっています。

4. 7. 2. TCP のヘッダ形式

上ではデータリンク層のイーサネットヘッダで通信の例を示しましたが、ヘッダファイルは他にもあります。トランスポート層では TCP ヘッダや UDP ヘッダが使われ、送信するときは付加され、受信するときには解析されて取り除かれます。ここでは TCP ヘッダを取り上げて説明します。(図 4.9)。

アプリケーションソフトは、その目的に応じたデータ通信を行うため、トランスポートプロトコルである TCP または UDP プロトコルを選択して通信を依頼します。トランスポートプロトコルの役割は、アプリケーション間の通信を行うことにあります。

以下に TCP ヘッダの主なフィールドについて簡単にまとめます[引用文献 7, 15]。

(1) 発信元ポート番号(Source Port)と宛先ポート番号(Destination Port)

この層で付加されるヘッダには、宛先のアプリケーションサービスを識別する番号が記載され、指定されたプログラムにデータが届くしくみが提供されています。また返信のための通信を行うために、発信元のアプリケーションプログラムを識別するための番号も記載されています。

これらの番号はポート番号と呼ばれ、16 ビットで表現されます。宛先のアプリケーションサービスを識別する番号が宛先ポート番号で、発信元のアプリケーションプログラムを識別する番号が発信元ポート番号となります。ポート番号については第6章で詳しく述べます。

発信元ポート番号 (16 ビット)						宛先ポート番号 (16 ビット)						
シーケンス番号 (32 ビット)												
確認応答番号 (32 ビット)												
ヘッダ長 (4 ビット)	予約 (6 ビット)	コードビット (フラグ) (各1 ビット)						ウィンドウサイズ (16 ビット)				
		U	A	P	P	S	F					
		R	C	S	S	Y	I					
		G	K	H	T	N	N					
チェックサム (16 ビット)						緊急ポインタ (16 ビット)						
(オプション)												
データ												
←						32 ビット						→

図 4.9 TCP のヘッダ形式[引用文献 7, p.190 より作成]

(2) シーケンス番号(Sequence Number)

TCP はコネクション型のプロトコルであるため、通信を行うときに双方向の通信路としてコネクション(connection)を設定します。このコネクションの上でパケット(トランスポート層ではセグメントと呼ぶ)の送信を行うために、それぞれのパケットには順番を示す番号が付けられています。この番号をシーケンス番号(sequence number)と呼び、ヘッダに記載されています。この番号によって通信の途中でパケットの到着順番が狂っても、元の順番がわかるようになっています。

(3) 確認応答番号(Acknowledgement Number)

確認応答(Acknowledgement, ACK)とは、送信されたパケットが宛先に到着したときに、到着したことを発信元に送って知らせることです。発信元はパケットを送信した後、宛先からの確認応答が送られてくるまで、次のデータを発信しないで待ちます。このようにすることで、データ通信の信頼性を高めることができます。しかし通信障害などによってパケットが破棄されることもあり、そのようなときは確認応答が返されてこないことがあります。そのため一定時間が経過すると、自動的にパケットが届かなかったものと判断され再送信します。

宛先からはパケットを正しく受信すると、受信したことを知らせるために確認応答を返してきます。確認応答番号が有効であるときにはACK フラグに1がセットされ、ヘッダに確認番号を記載します。

宛先では受け取ったパケットのヘッダに記載されているシーケンス番号に、そのパケット長を加えて確

認応答番号を作成します。このように作成した確認応答番号を発信元に送信することによって、次に受け取る予定のパケットのシーケンス番号を知らせます。

(4) ヘッダ長(TCP Header Length)

TCP プロトコルのヘッダ長を表しています。オプションが付加されていない通常のパケットは、このフィールドの値は5であり、ヘッダ長は20 バイト (32 ビット×5÷8) です。

(5) 予約 (未使用のフィールド)

(6) コードビット(Code Bit)

コードビットのそれぞれのフラグ(Flag)は1 ビットで表現されており、0 か1 によって2 つの状態を示し、これによってパケット (トランスポート層ではセグメント) の種別を表しています。

◆URG 緊急に処理すべきデータかどうかを示します。

◆ACK 確認応答番号が有効であるかどうかを示します。

◆PSH(Push Flag)

TCP では効率のよい通信を行うため、ある程度のデータが蓄積された後に、パケットを生成して送信します。しかし対話的なアプリケーションの場合、PSH フラグに1 が設定されていると、このような蓄積を行わずに、パケットがすぐに上位のアプリケーションに送信され、宛先ホストにおいても、速やかにアプリケーションに届けられるようになります。0 が指定されている場合は、宛先の判断によって、パケットを送信します。

◆RST(Rest Flag)

何らかの障害によって、パケットの再送を行ってもコネクションを維持できなくなった場合には、仮想回線を切断してリセットすることになります。このフラグに1 が指定されると、通信障害によって制御不能に陥ったことを示し、仮想回線を強制的にリセットします。

◆SYN(Synchronize Flag)

値が1 のときは、コネクションを確立する際に、シーケンス番号を同期化させるために使われます。

◆FIN(Fin Flag)

このフラグに1 が指定されていたときは、発信側が送り出すパケットが終了したことを示し、コネクションの終了を表します。

(7) ウインドウサイズ(Window Size)

TCP ではパケットの送信を調整するために、ウインドウフロー制御方式と呼ばれるフロー制御が用いられます。宛先からは受信可能なパケット数を、ウインドウサイズとして発信元に伝えられます。発信元ではそのウインドウサイズを超えたパケットを送信しないようにして、宛先の受信可能範囲に収まるようにします。ウインドウサイズの値は、連続して送信可能な最大値となります。

(8) チェックサム(Checksum)

ビット誤りが発生しているかどうかを判断するために使われます。

(9) 緊急ポインタ(Urgent Pointer)

緊急ポインタの数值は、優先して送信したい緊急を要するデータがあるとき、そのデータの格納場所を示すポインタとして扱われます。

(10) データ(Data)

データの部分には上位のアプリケーション層から伝送された元のデータが入ります。

4. 7. 3. UDP のヘッダ形式

UDP プロトコルのヘッダ形式は次のようになっています(図4.10)。発信元と宛先のポート番号以外は、パケット(データグラム)の長さ、その送信誤りを検出するためのチェックサムのフィールドだけの構成になっています。

発信元ポート番号 (16 ビット)	宛先ポート番号 (16 ビット)
UDP データ長 (16 ビット)	チェックサム (16 ビット)
データ	
← 32 ビット →	

図 4.10 TCP のヘッダ形式[引用文献 7, p.200 より作成]

UDP は TCP のようにパケットの送信誤りを検出するような機能は備えていません。また UDP はコネクションレス型のプロトコルのため、通信に先立って論理的な通信路の設定なども行いません。そのためプログラムの処理途中でも、いきなりデータを送ることができます。またパケットに分割されて送られる場合でも、それらのパケットの順番は考慮されず、正確性や効率性なども考慮されません。

しかしコネクションの確立や切断などの処理を行わずに済むため、処理速度が要求される場合に利用されます。UDP はドメインネームシステム(DNS:Domain Name System)やUNIX のファイル共有システムである NFS(Network File System)などのアプリケーションソフトウェアで使用されています。これらにおいてデータの消滅などが起きた場合には、そのつどアプリケーション側が再送することで補っています。

また音声や映像などのマルチメディアデータの送信においては、若干のデータが途中で消滅しても音声や映像の再生が可能なものがあります。UDP は TCP よりもデータ送信が速く負荷も軽いため、このようなマルチメディアデータの送信に優れた効果を発揮します。

4. 7. 4. LAN とパケットの送受信

イーサネットによって LAN 上をパケットが流れ、ヘッダの情報を解析することによって、宛先のコンピュータに届けられます。これはデータを受け取ったコンピュータが、ヘッダを解析することを考えれば理解しやすくなります。例えばコンピュータ A から C にデータを送信するとします。C というノードのコンピュータがパケットを受信し、それを取

り込むためには以下のような手順を踏みます (図4.11)。

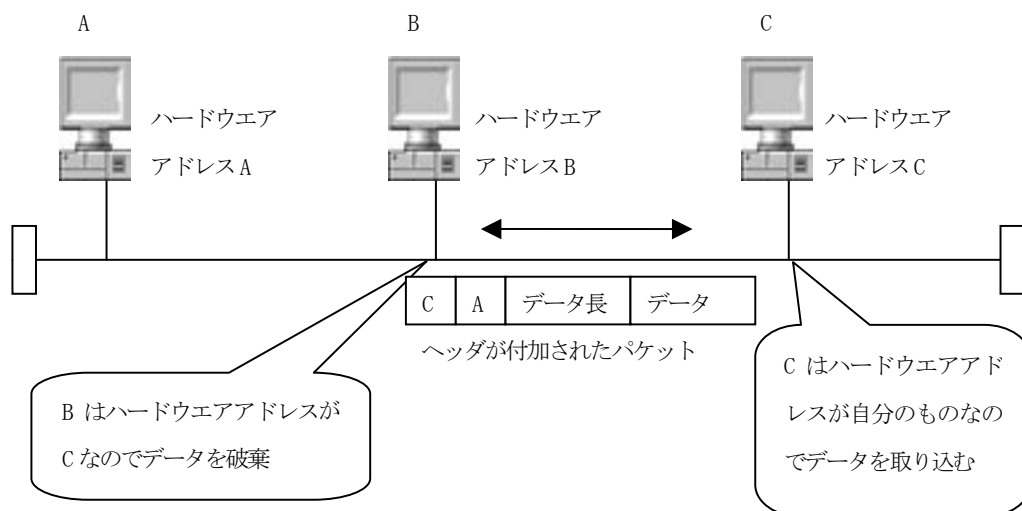


図 4.11 ノード C がパケットを受信するしくみ[引用文献 18, p.53 より作成]

(1) A からイーサネット上にデータが流れると、そのデータは同じネットワークに接続している B にも C にも届きます。しかしヘッダの宛先ハードウェアアドレスを見ると C となっているので、B はそれが自分のものではない判断し、データを取り込まずに破棄します。

(2) C にパケットが届くと C は宛先ハードウェアアドレスが自分のものなので、パケットを取り込みます。

(3) C は取り込んだパケットのヘッダを解析し、送信元ハードウェアアドレスが A であることがわかります。

(4) C は IP プロトコルを解析するためヘッダを取り除き、上位のインターネット層へパケットを伝送し、次に IP ヘッダの解析を行います。

(5) インターネット層での解析が終わると、より上位のトランスポート層にパケットが伝送され、ここでは TCP ヘッダの解析が行われ、さらに上位のアプリケーション層にパケットが伝送されると、A から送信された元の情報に復元され、C のユーザが読めるようになります。

4. 8. ヘッダの処理とデータ送受信

例えばメッセージ送信ソフトなどで「お元気ですか」という言葉を、TCP/IP を用いて送信するときのヘッダの処理を考えてみましょう。ここでは同じネットワークに接続している発信元コンピュータ A から宛先コンピュータ C に送信することになります。メッセージ送信ソフトによるデータの作成から、TCP/IP のヘッダの付加と解析を繰り返して、相手が受信して読めるようになるまでの経過を示すと次のようになります。

す(図 4.12) [引用文献 18].

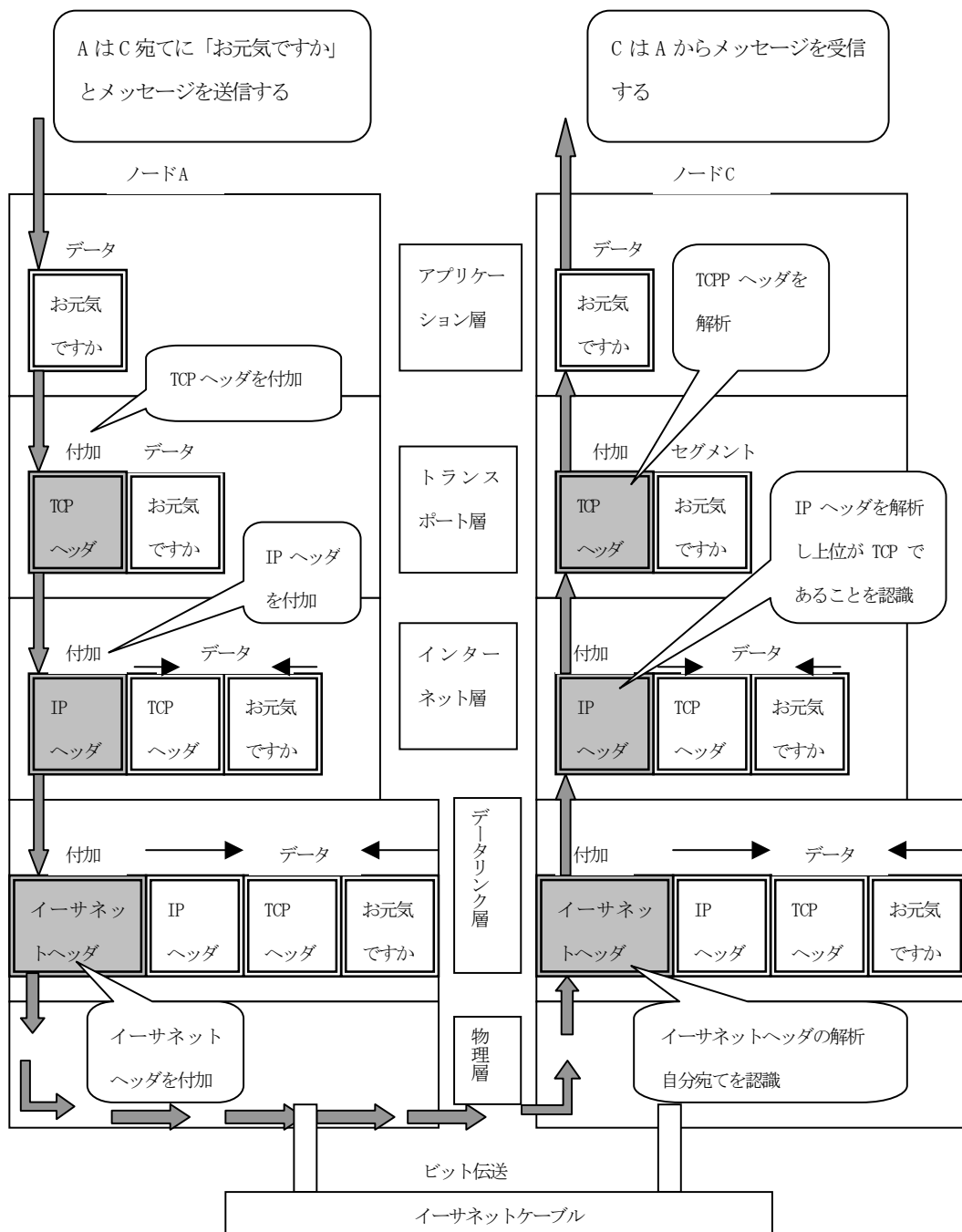


図 4.12 ヘッダの処理とデータ送受信[引用文献 18, p.56 より作成]

(1) アプリケーション層の処理

最初はAのキーボードから「お元気ですか」と入力してデータを作成しなければなりません。入力されたデータは、符号化されるなどの処理が行われ、下位のトランスポート層に下りてきます。

(2) トランスポート層の処理

トランスポート層のTCPプロトコルでは、上位層からきた情報を一塊のデータとして扱い、このデータの先頭にTCPヘッダを付け、下位のインターネット層に引き渡します。

(3) インターネット層の処理

インターネット層では上位層から降りてきたTCPヘッダを含むデータの塊を、やはり一塊のデータとして扱います。そしてTCPヘッダの先頭にIPヘッダを付け加え、下位のデータリンク層へ伝送します。

このIPヘッダの中には、どの宛先に送信するかという識別子(ここでは宛先Cの識別子)が組み込まれます。この識別子はIPアドレスと呼ばれるものです。

(4) データリンク層の処理

データリンク層では、上位のインターネット層からIPヘッダの付いたデータの塊が伝送され、ここではイーサネットヘッダが先頭に付加され、同様に一塊のデータとして扱われます。これから先は物理層(ここではイーサネットケーブル)によって宛先のCに運ばれます。

(5) コンピュータCの受信処理

宛先Cでは、発信元Aとは全く逆の順番にヘッダが解析されて取り除かれ、元のデータが復元されます。まず電気信号で物理層にデータが伝送されてきますが、物理層からデータリンク層に伝送されると、パケットはビット列に戻されます。

ヘッダの宛先ハードウェアアドレスがCになっているので、Cは自分宛てのパケットであると認識します。また送信元ハードウェアアドレスがAになっているため、このパケットはAから送信されたものと認識します。データリンク層でヘッダの解析を行い、上位のインターネット層へパケットを伝送します。

インターネット層ではIPヘッダの解析を行います。IPヘッダの中からは発信元であるAのIPアドレスも認識することができます。

トランスポート層ではTCPヘッダの解析を行い、上位層の適切なアプリケーションにデータを渡します。

このようにして受信したCでは、ひとつひとつのフィールドを解析し、それによって誰から送られてきたパケットで、どのような情報が入っているかを認識していきます。最終的にはCのディスプレイ上で、Aにおいて入力された「お元気ですか」が出力されます。

TCP/IPプロトコルでは、ヘッダの内容は細かい部分まで厳密に仕様が決められており、それによってプロトコルの構造を作っています。例えば上位プロトコルを識別するフィールドはTCP/IPではETYPEであり、それはどこに位置し、フィールドの長さは何バイトであるか、さらにそこに入ってくる番号がいくつであつたらどのプロトコルかというようなことが細かく決められており、それによってコンピュータ間の通信が成り立っています。

》》》 演習 4 《《《

ネットワークを利用してFTPによるファイル転送を行ってみよう。ソフトウェアを公開しているWebページからダウンロードし、自分のマイドキュメントでソフトウェアが動作するように試みる。

前準備として前回使用したIP Messengerは削除してから以下の作業を行う。

1. 必要なソフトウェア

ここでもIP Messengerを使用する。このソフトは前回一度使用しているので動作の確認が各自でできる。なおこのソフトは圧縮形式で提供されているので、圧縮ファイルを解凍するソフトも必要になる。

圧縮解凍ソフトはセキュリティ対策のため、教室にはインストールできても使用させない設定になっている。そのため圧縮ファイルの解凍は、各自のフロッピィを使用して行う。

必要なソフトは以下のURLで公開されている。

(1) IP Messenger

<http://www.asahi-net.or.jp/~VZ4H-SRUZ/ipmsg.html>

Win 版 IP Messenger ver2.04 (106KB) by H.Shirouzu (2003/10/01)

Download: from 窓の杜 from Vector (窓の杜またはVectorから最新版をダウンロードする)

(2) Lhaca (圧縮解凍ソフト)

<http://park8.wakwak.com/~app/Lhaca/>

Lhaca072.EXE

1. 2. ダウンロードのしかた



図 5.8 ファイルのダウンロード画面

上記の URL を Internet Explore で開き、「from 窓の杜 from Vector」のいずれかの上で左のボタンでクリックする。そうすると「ファイルのダウンロード」の画面が開くので、ここでは各自のフロッピーで処理をするため、フロッピーに保存する(図 5. 8)。「Lhaca072. EXE」のダウンロードも同様である。

2. 圧縮解凍ソフトのインストール

今回の作業に必要な 2 つのファイルを上の手順で自分のフロッピーにダウンロードしてくる。

最近の配布されるソフトは圧縮してあるものが一般的である。そのため圧縮されたファイルを解凍(元に戻す)するソフトを用意する必要がある。Lhaca072. exe をフロッピーにあることを確認し、左ボタンでダブルクリックすると、解凍したファイルのインストール先を入力する画面がでる(図 5. 9)。

参照ボタンを使ってインストール先をフロッピーにすると A:¥ と表示される。OK ボタンを押すと Lhaca のファイルが自動的に解凍されて作成される。

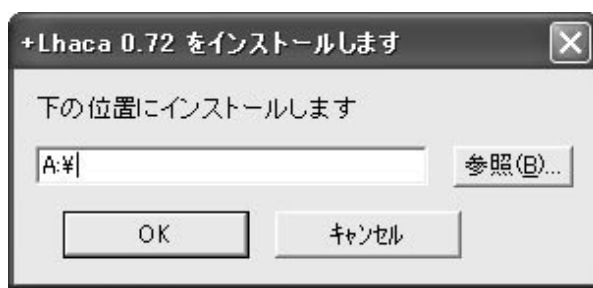


図 5.9 Lhaca のインストール画面

2. 1. 解凍先の指定

Lhaca をダブルクリックして、解凍についてのオプションを指定する。

ここでは解凍先を「ファイルと同じ」と「フォルダを作ってその中に解凍」をチェックしておく。これらを指定しておくと、元のファイルはフロッピーにあるので、フロッピーにフォルダが作成され、その中に解凍されたファイルが入る。

2. 2. IP Messenger の解凍

IP Messenger は, ipmsg204. lzh という名前で圧縮されている。Lhaca を使ってこのファイルを解凍する。解凍するときは, ipmsg147. lzh のアイコンを Lhaca. exe ファイルのアイコンの上にドラッグして重ねる(図 5. 10 の上に重ねる)。そうすると Lhaca. exe が起動して、圧縮してあるファイルを解凍してくれる。解凍先は「ファイルと同じ場所」を指定する。うまく解凍できれば ipmsg204 というフォルダができる。

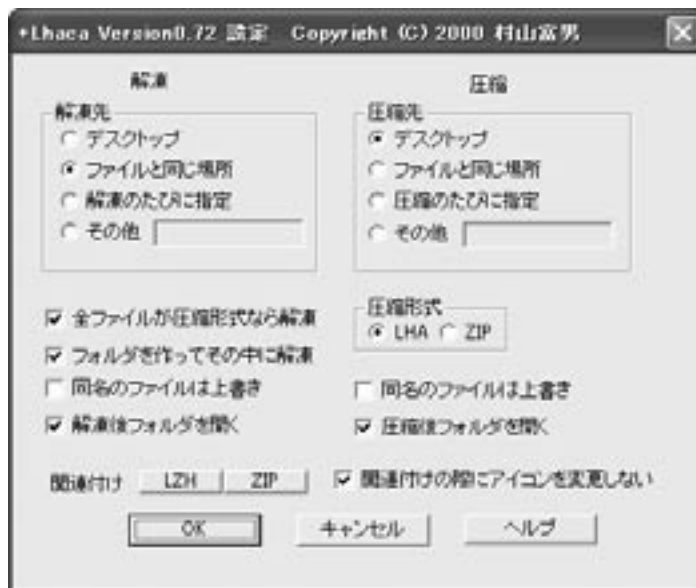


図 5.10 解凍先の指定

3. インストールとセットアップ

インストールとセットアップについては、前章（第3章）の演習を参照のこと。

4. アンインストール

アンインストールについても、前章（第3章）の演習を参照のこと。

》》》 本章の復習 《《《

- (1) TCP/IP のTCPは何の略か、またどのような意味か。
- (2) プロトコルのヘッダとは何か。
- (3) TELNET プロトコルはどんな機能を実現しているか。
- (4) FTP プロトコルはどんな機能を実現しているか。
- (5) HTTP プロトコルはどんな機能を実現しているか。

5. IP プロトコル

インターネットでは主に TCP/IP によるデータ通信が利用され、その通信を成り立たせるために多くのプロトコルが使われています。なかでも IP プロトコル(Internet Protocol)は、インターネット上で行われる通信の宛先を指定する役割を果たしており、最も重要なものになっています。ここでは IP プロトコルのしくみと役割について取り上げます。

現在 IP アドレスの不足が問題になっており、緊急の課題となっています。現在は主に IP バージョン 4(Internet Protocol Version 4, IPv4)が使われていますが、より多くの機器をインターネットにつなげるため、徐々に IP バージョン 6(Internet Protocol Version 6, IPv6)に移行しつつあります。

5. 1. インターネット層とアドレス

IP プロトコルは、TCP/IP では第 3 層のインターネット層に該当するプロトコルで、ネットワークにパケットを送り出すときの宛先と、送り出したパケットがどこを通るかという経路の決定をしています。IP プロトコルの主な役割は OSI 参照モデルでは、ネットワーク層が提供しているものと同じもので、パケットの宛先や送信経路の決定を行っています。

我々が電話や郵便などを使って相手と連絡を取り合うときは、相手の電話番号や住所を明確に把握しておく必要があります。コンピュータによるデータ通信もこれと同じことがいえ、通信をする相手のコンピュータがどこのどれかをはっきりさせておかなければ通信することができません。

そのためネットワーク上でデータを送る場合にも宛先を指定することが必要になります。この宛先を指定するための情報をネットワークアドレス(network address)あるいはアドレス(address)といいます。

ネットワークでは、ネットワークを構成しているケーブルや、各種の接続機器などの接点(結節点)のことをノードといいます。このような接続しているノードを識別するためには、アドレスを指定しておく必要があります。ノードにはコンピュータやプリンタなどのほかに、ネットワークを構成する各種の機器が接続されるので、それらへのアドレスの割り当て方式がどのようなメディアやネットワークの形態でも使えるものでなければなりません。

そのためどのような方法でネットワークに接続されていても、インターネット層で決められたアドレスの形式は同じである必要があります。

TCP/IP では、このアドレスのことを IP アドレス(IP address)と呼びます。実際にネットワーク上で通信を行う場合は、この IP アドレスがネットワークに接続しているそれぞれのコンピュータや、ネットワーク機器などに割り当てられ、送り先を決定するための識別子として使われます。

5. 2. IP アドレス

TCP/IP で通信を行う場合、ネットワークに接続されているノードには、必ず定められた IP アドレスを割り当てておく必要があります。この IP アドレスは、他のノードと区別するために、重複しないアドレスを割り当てることになり、ネットワークを構築する上で絶対を守る必要があります。

同じ IP アドレスがネットワーク上に存在するという事は、同じ送り先が複数存在するという事になってしまいます。そのため発信元では、どこ宛てにデータを送り出してよいのか分からなくなってしまい、通信ができない状態に陥ってしまいます。

5. 3. IP アドレスの管理

IP アドレスは、世界的に NIC(Network Information Center)が一元的に管理しています。国内では JPNIC(Japan Network Information Center)が IP アドレスの割り当て組織として活躍しています。

IP アドレスを使ったネットワークを IP ネットワークと呼ぶことがあります。IP ネットワークを構築する場合は、正式な IP アドレスを JPNIC または NIC から取得し、組織ごとに割り当てる必要があります。このようにして IP アドレスを取得した場合は、そのネットワークアドレスの範囲内において、機器を識別するためのホストアドレス(host address)が重複しないように、それぞれのコンピュータなどに割り当てることになります。

このようにすれば世界中において、同一の IP アドレスが存在しないように管理されます。したがって IP プロトコルを使っていれば、インターネットを通じて世界中どこからでも、どのコンピュータかを識別することができます。しかし世界中から誰でも直接アクセスできるかどうかは、セキュリティ対策を考慮して組織ごとにアクセスの管理方針を定めているため、その方針で定めたアクセス許可の内容によります。

5. 4. IP アドレスと 3 つのクラス

ここではコンピュータや各種の通信機器などにおいて、現在最も広く使われている IPv4 の IP アドレスの例で説明していきます。この IP アドレスは 32 ビットの数値によるバイナリーデータ(binary data)を使って表されています。この 32 ビットの数値の表し方では、組み合わせの数を計算すると 2 の 32 乗なので、4, 294, 967, 296(およそ 43 億)までの数を扱うことができます。よってそれだけのアドレスを機器に割り当てできる計算になります。

$$2^{32} = 4, 294, 967, 296$$

IP アドレスは 32 桁の 2 進数で表現されますが、これをそのまま用いると人間には見にくいので、32 ビットを 8 ビット(1 バイト)ずつ 4 つの部分に分けています。さらに 4 つに分けたそれぞれの部分を、10 進数に直し、ピリオドで区切った表記法が用いられます。

(32 ビットの 2 進数)	11001010000100000111110000001100
(8 ビットずつ 4 分割)	11001010. 00010000. 01111100. 00001100

IP アドレスの表記例 (IPv4)

(10 進数とピリオド)	202.	16.	124.	12.
--------------	------	-----	------	-----

この 32 ビットの数値は、ネットワークを識別するためのネットワークアドレス(network address)と、ホスト(host)を識別するためのホストアドレス(host address)から構成されています。ここでホストというのは、ネットワークに接続しているコンピュータや通信機器のことをいいます。

またこれらはネットワークの規模や接続するコンピュータ数の構成などから、アドレス体系を選択できるようになっています。それらの体系はクラス A, クラス B, クラス C の 3 つであり、これらが一般に利用されています。

なおクラス D, クラス E という 2 つの特別なクラスもありますが、これらのクラスは、他の 3 つのクラスと異なり、クラス D は IP マルチキャスト(IP multicast)用として、クラス E は実験用として特別に扱われ、他に転用して使われないように用途が限定されています。そのため一般に使われるのは、クラス A からクラス C までの 3 つとなります。

IP アドレスのどの部分がネットワークアドレスを表し、どの部分がホストアドレスを表すかは、A, B, C の 3 つのクラスで異なっています。

5. 5. クラス A

クラス A の IP アドレスの場合は、ネットワークアドレスは先頭から 8 ビット(1 バイト)までが使われ、ホストアドレスは残りの 24 ビット(3 バイト)が使われるしくみになっています。クラス A はホストアドレスは最も長いクラスであり、多くのコンピュータや通信機器を接続できるので、大規模な組織において構築されるネットワークのための IP アドレスとして考えられています。

(1) ネットワークアドレス

クラス A は、ネットワークアドレスを示す先頭の 1 ビット目は 0 で始まります。10 進数では 0 から 127 までが、クラス A のネットワークアドレスを表す数値となります。

これらのうちネットワークアドレスが 0.0.0.0 のように先頭が 0 で始まるものは、全てのネットワークを表すものとして、特殊な使い方のために予約されたアドレスのため使うことができません。

また先頭が 127 で始まる 127.0.0.0~127.255.255.255 はネットワーク上での通信には用いられません。これらは同一のコンピュータ上において、機器が正常に動作しているかを確認するために、試験的に自分

自身にテストデータを送るループバックテスト(loopback test)などに用いられるために予約されています。ループバックとは、自分自身にデータを送信することを意味しています。これらのアドレスはネットワークカードなどの機器において、自分自身を示すループバックアドレスを設定するために使われ、ループバックアドレス宛に送信されたデータは同じ機器内で受信されます。そのため同じコンピュータの上で動作しているプログラム間でデータのやり取りを行うプロセス間通信(interprocess communication)にも使われます。

このように0から127までの128個のネットワークアドレスのうち、0と127は他で使用されるので予約されており、利用できるネットワークアドレスの数は、128から2を引いた126個となります。

(2) ホストアドレス

ホストアドレスは、ネットワークアドレスの後ろの部分にあり、9ビットから32ビットまでの24ビットとなります。

この24ビットのホストアドレスは、2の24乗すなわち16,777,216通りになります。しかしこのうちすべて0のものとすべて1のもの、つまり10進数でいえば0と255のものは、他で使用されるため予約されています。そのためホストアドレスとして、1つのネットワークのなかで、クラスAで割り当てることのできるホストアドレスは、16,777,216から2を引いて16,777,214個になります。

クラスA

ネットワークアドレス	ホストアドレス(24ビット)		
0～127	0～255	0～255	0～255
(先頭0で8ビット)	(8ビット)	(8ビット)	(8ビット)

図 5.1 クラス A の IP アドレス

予約された0と255のホストアドレスには特別な意味があります。0を指定するとそのネットワーク自身のアドレスとして使用されます。例えば202.2.1.0は、202.2.1.というネットワークアドレスとなり、ホストアドレスは認識しません。

また255はブロードキャストアドレス(broadcast address)として使われます。このブロードキャストアドレスは、ネットワーク全体へ同時にパケットを送信するための宛先アドレスであり、2進数ではホストアドレスがすべて1のため、ホスト1のブロードキャストアドレスと呼ぶこともあります。

ブロードキャストアドレスを用いてパケットを送信すると、1つのパケットを全部のノードに送信することができます。このように予約された特別なホストアドレスは、クラスBやクラスCなど他のクラスでも同じように存在します。

それぞれのクラスともネットワークアドレス、ホストアドレスともにすべて 0 またはすべて 1 のものは、通常のアドレスとして割り当てることはできません。

このため、計算上で存在するアドレスから 2 を引いた数が、実際に使用可能なネットワークアドレスの数とホストアドレスの数になります。

5. 6. クラス B

クラス B のアドレスでは、最初の 2 ビットが 2 進法の 10 で始まり、14 ビット目までを使ってネットワークアドレスを表します。そして残りの 16 ビットがホストアドレスを表すというしくみになっています。

従ってネットワークアドレスは 128.1 から 191.254 まで、2 の 14 乗から 2 を引いた 16,382 個になります。また 1 つのネットワーク内のホスト数の最大は、2 の 16 乗から 2 を引いた 65,534 個になります。

ホスト数は組織の大きさや組織内で使われるコンピュータや通信機器などの数と深く関係があるため、クラス B は利用の要求が最も多いクラスになっています。

クラス B

ネットワークアドレス(16 ビット)	ホストアドレス(16 ビット)	
128.1~191.254	0~255	0~255
(先頭 10 で 16 ビット)	(8 ビット)	(8 ビット)

図 5.2 クラス B の IP アドレス

5. 7. クラス C

クラス C のアドレスでは、最初の 3 ビットが 2 進法の 110 で始まり、その後の 21 ビット目までを使ってネットワークアドレスを表し、残りの 8 ビットがホストアドレスを表すというしくみになります。

クラス C

ネットワークアドレス(24 ビット)	ホストアドレス
192.0.1~223.255.254	0~255
(先頭 110 で 24 ビット)	(8 ビット)

図 5.3 クラス C の IP アドレス

従って、ネットワークアドレスは 192. 0. 1 から 223. 255. 254 まで、2 の 21 乗から 2 を引いた 2, 097, 150 個が使用できます。また 1 つのネットワーク内ではホストアドレスは、2 の 8 乗から 2 を引いた 254 個まで使用することができます。そのため中小規模の組織などのように少ないホスト数でも間に合うような、比較的小規模ネットワーク向けの IP アドレスとして使われています。

5. 8. IP アドレスの不足

このように現在ではクラス A からクラス C までは IP アドレスとして使用しているわけです。また割り当てる組織の規模をあらかじめ想定した IP アドレスにおけるクラス分けの考え方は、1980 年代に作成されたものです。そのためインターネットへの参加組織がそれほど多くない時代には、ほとんど問題はありませんでした。しかし最近のインターネットの発展は、接続する機器を増加させる一方であり、これまでの IPv4 で定められた IP アドレスでは不足しているのが現状です。

実は IP アドレスが不足する問題の根底には、IP アドレスの体系自体にも次のようないくつかの問題があります。また今後は家電製品などがインターネットに接続すると見られており、そうすると現在使われている IP アドレスの数では需要を満たせる見込みがほとんどありません。

(1) クラス A の未使用

割り当て可能な IP アドレスのうち、クラス A がその 50% を占めています。クラス A は 1 つのネットワークで接続ホスト数が最大で 16, 777, 214 個になりますが、現実にはこれだけ多くのホストを持つ組織はありません。そのためクラス A の IP アドレスの多くは使われないままになってしまいます。

(2) クラス B の不足

一般の組織が実際に入手するアドレス体系は、組織で必要とされる接続可能ホスト数との関係から、クラス B またはクラス C が多くなります。クラス B のアドレス体系自体は、全アドレス体系の 25% 程度にあたります。クラス B は 1 つのネットワークあたりの最大ホスト数が 65, 534 個のため、中規模以上の組織で使うネットワークに向いています。

1 つのクラス B のネットワークは、さらに内部でサブネット化して分割することが可能なため、組織の大きさに適合したアドレス体系を構築しやすくなります。このためクラス B の IP アドレスの取得要望が大変多くなり、このクラスの IP アドレスが不足する事態になっています。

(3) クラス C の不足

クラス C の場合は、1 つのネットワークあたりの最大ホスト数が 254 個のため、小規模な組織のネットワークに向いていますが、これよりホスト数の多い組織では、このクラス C の IP アドレスが 1 つだけでは不足する場合があります。そのため複数のクラス C を取得する必要が発生してしまいます。クラス C が持つアドレス体系自体は、全アドレス体系の

12.5%程度にしかならないため、いずれにしてもこのクラスのIPアドレスも不足します。

5. 9. サブネット

IP を使ったネットワークでは、それぞれのネットワークに重複しないようにネットワークアドレスを割り当てる必要があります。しかし、ひとつの組織で建物が異なる場合などは、ルータ (router) という機器を使って、ネットワークとネットワークをつなげることがしばしばあります。このように複数のネットワークに分ける場合にも新たなネットワークアドレスを取得すると、限られたネットワークアドレスを無駄に使ってしまいます。

またクラス A やクラス B のネットワークアドレスは、1 つのネットワークに多数のホストを収容すること (A クラスでは 16, 777, 214 台、B クラスでは 65, 534 台のホスト) ができますが、現実にはこれだけの数のホストがひとつの物理的なネットワークに接続されることはないといえます。仮にあったとしてもホスト数の多さから、ネットワークの管理が極めて困難になります。そのため大きなネットワークは敷地や建物ごとに、クラス C のようにより小さなネットワークに分割されて管理されるのが適切といえます。

しかし、小さなネットワークごとにネットワークアドレスを割り当てていると、限りのあるネットワークアドレスが足りなくなります。

そこで 1 つのネットワークアドレスを複数のより小さなネットワークから構成されるように、サブネット (subnet) に分割し、アドレスを有効利用する方法が行われており、これをサブネット化といいます。

例えば、クラス B のネットワークでホストアドレスの上位 4 ビットを、サブネットを表すビットつまりサブネットアドレス (subnet address) として分割して使用することができます。この分割によってこのネットワークは 2 の 4 乗から 2 を引いた 14 のサブネットを収容することができます。

そしてそれぞれのサブネットには、2 の 12 乗から 2 を引いた 4, 094 台のホストを収容することができ、大きなネットワークアドレスを小さなサブネットに分割して有効利用することができます。この例のネットワーク全体では $14 \times 4, 094 = 57, 316$ 台のホストを収容できるようになります (図 5. 4)。

5. 10. サブネットマスク

サブネットに分割して利用する場合には、ホストアドレスの一部をサブネット用のフィールドとして使用することを示す必要があります。そのためにサブネットマスク (subnet mask) が定義されており、IP アドレスは以下の 3 つの要素から構成されることになります。

ネットワークアドレス + サブネットアドレス + ホストアドレス

これによってネットワークに階層的な構造を導入することができるようになります。サブネットを構成

しない場合、クラス A のサブネットマスクは 255. 0. 0. 0、クラス B のサブネットマスクは 255. 255. 0. 0、クラス C のサブネットマスクは 255. 255. 255. 0 と指定する場合があります。従って例えばクラス B の IP アドレスが指定されていて、サブネットマスクが 255. 255. 0. 0 のときはサブネット化は行われていないことを示します。

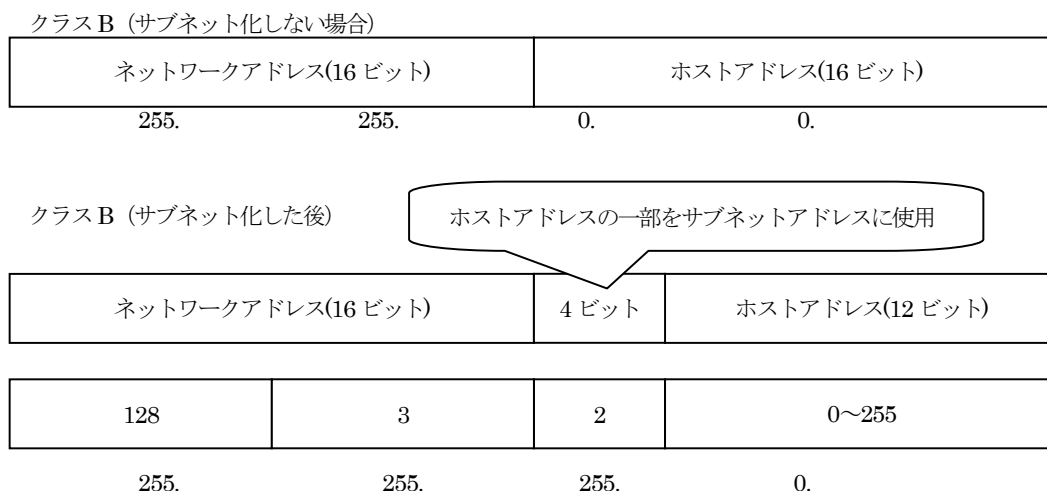


図 5.4 サブネットアドレスとネットワークの階層化の例

しかしクラス B の IP アドレスが割り当てられているにもかかわらず、サブネットマスクが 255. 255. 255. 0 のようになっているときは、IP アドレスがクラス C と同じ規模の IP アドレスとして用いられ、サブネット化されていることがわかります(図 5. 4)。

また例えばクラス B のネットワーク 128. 3. 2. 1 があり、これはサブネットに分割されていない場合、サブネットは 255. 255. 0. 0 となっています。この場合のネットワークアドレスの部分は 128. 3 であり、ホストアドレスの部分は 2. 1 となります。

これをサブネットに分割して、クラス C のネットワークと同じように扱いたい場合は、サブネットを 255. 255. 255. 0 のように指定します。これによってネットワークアドレスの部分は 128. 3. 2 となり、ホストアドレスの部分は 1 となります。以下にこの例を示します。

IP アドレス(サブネットマスク)

分割前	128. 3. 2. 1 (255. 255. 0. 0)	← ネットワークアドレス部分 : 128. 3	ホスト部分 : 2. 1
分割後	128. 3. 2. 1 (255. 255. 255. 0)	← ネットワークアドレス部分 : 128. 3. 2	ホスト部分 : 1

5. 11. DHCP

DHCP(Dynamic Host Configuration Protocol)というプロトコルは、インターネット接続サービスを提供している ISP や、学校のパソコン教室などでしばしば使われます。このサービスも IP アドレスの不足を解決する役割をはたしています。

従来の IP アドレスの割り当て方法では、個別の機器ごとに固定して付与していました。IP アドレスはコンピュータの電源を入れたときに、ネットワークに接続してはじめて使われるようになります。そのため電源を入れていないときは、IP アドレスが割り当てられていても使われないことになります。

そこで DHCP では、IP アドレスを個別の機器に固定的に割り当ててのではなく、DHCP サーバで一括管理を行います。そしてコンピュータの電源投入時や、電話回線で ISP に接続したときなど、実際に IP アドレスが必要な時に、DHCP サーバとやり取りを行い、その場で IP アドレスを自動的に割り当ててもらい、限られた時間だけ利用できるようにします。従って IP アドレスは使われない場合は回収され、接続のたびに変更になるのが一般的です。

この方法はインターネットへの接続を、短時間ながら何度も繰り返し使用するユーザをたくさん抱えているような場合に極めて有効といえます。固定的に IP アドレスを割り当てた場合は、それを管理者に返納するまで同じ IP アドレスを使うのが普通です。

組織の構成員が自宅などのような外部から LAN にリモートアクセス(remote access)で接続する場合や、ISP などへの接続では、全員が同時に接続することはほとんどないため、この DHCP なら少ない IP アドレスでも繰り返し有効に使いまわすことができます。

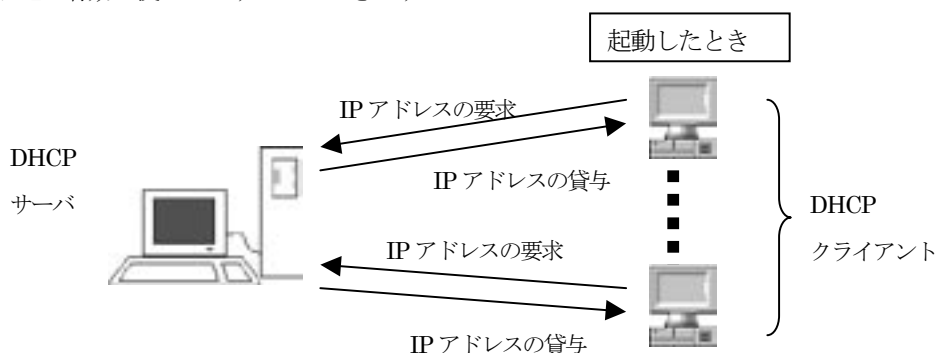


図 5.5 DHCP サービスと IP の貸与

5. 12. プライベート IP アドレス

IP アドレスは、グローバル IP アドレス(global IP address)とプライベート IP アドレス(private IP address)に分けることがあります。IP アドレスは、実際に一般ユーザが使えるものは A, B, C の 3 つのク

ラスに分けられており、インターネット接続時には、全世界で重複しないアドレスを使用しなければなりません。これは JPNIC に申請して取得することになりますが、これをグローバル IP アドレスと表現することがあります。

これに対して、IP アドレスの節約と有効利用を行うため、インターネットには直接公開しなくてもよい部分に、プライベート IP アドレスと呼ばれるものを割り当てて使用することができます。

プライベート IP アドレスは、あらかじめインターネット管理組織の文書である RFC によって決められており、次のネットワークアドレスが指定されています。

表 5.1 プライベート IP アドレス

クラス A	10. 0. 0. 0	1 個
クラス B	172. 16. 0. 0 ～ 172. 31. 0. 0	16 個
クラス C	192. 168. 0. 0 ～ 192. 168. 255. 0	256 個

プライベート IP アドレスは、そのままでは直接インターネットに接続することができないようになっています。そのためインターネットに接続させたいときは、プライベート IP アドレスからグローバル IP アドレスに変換する NAT (Network Address Translator) というしくみを導入する必要があります(図 5. 6)。

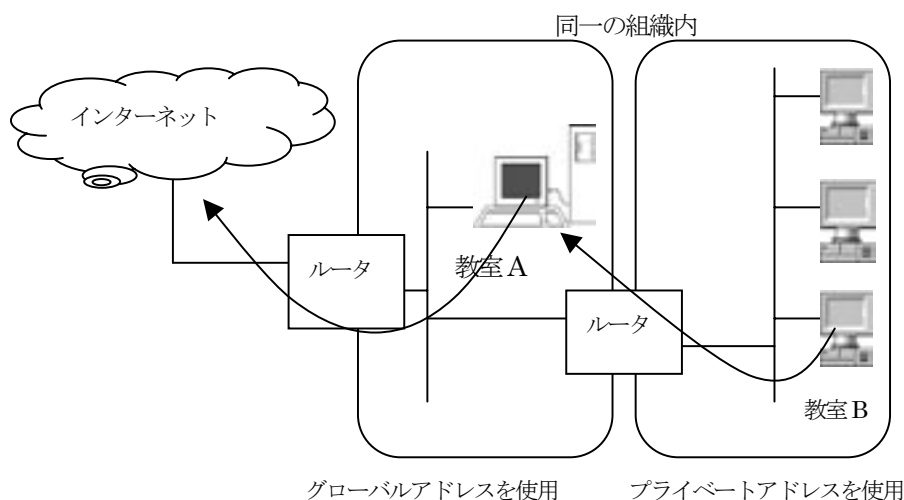


図 5.6 プライベートアドレスの使用例

例えば図 5. 6 のような場合を想定して考えると、A のコンピュータが属するネットワークにはグローバル IP アドレスが割り当てられ、インターネットに直接接続します。しかし教室などのように直接インターネットに接続しなくても何とかなる場合は、B のコンピュータが属しているネットワークのようにプライベート IP アドレスを割り当てることがあります。

そしてBのコンピュータからインターネットにアクセスしたいときは、いったんグローバルIPアドレスが割り当ててあるAのコンピュータに入り、そこからアクセスする場合があります。NATはこの機能を自動化するもので、ローカルIPアドレスをグローバルIPアドレスに変換し、ローカルIPアドレスからインターネットに接続することを可能にする機能です。

5. 13. CIDR

CIDR(Classless Inter-Domain Routing)という方法は、アドレス不足の問題を現在のIPv4における32ビットのアドレス体系のなかで解決するものとして、1993年から使われるようになってきました。IPアドレスを無駄なく利用し、同時にネットワークを流れる経路情報を削減するために開発されたものです。

クラスBのIPアドレスの枯渇によって、現在では中規模以上の組織に対して、複数のクラスCのIPアドレスの割り当てが行われています。同一の組織内に対してクラスCのIPアドレスの割り当てを続けていくと、ネットワークを中継するルータにおいて、パケットを転送するための経路情報が爆発的に増加し、設定や管理が極めて厄介になります。さらにトラフィック(traffic)と呼ばれるネットワークを流れるデータ量も増大させることになり、ネットワークが混雑する輻輳(congestion)と呼ばれる現象を引き起こす原因となります。

CIDRには、既存のネットワークアドレスのクラスをなくす(classless)考え方が取り入れられています。つまりクラスA、B、Cというこれまでの既存のネットワークアドレス部とホストアドレス部の8ビット単位での区別をなくすもので、クラスを使わないIPアドレスの割り当てを行い、加えて経路情報の集約を行う技術といえます。

以下の例のようにCIDRでは、どの位置でも自由にネットワークアドレスとホストアドレスを区別することが可能になっています(図5.7)。

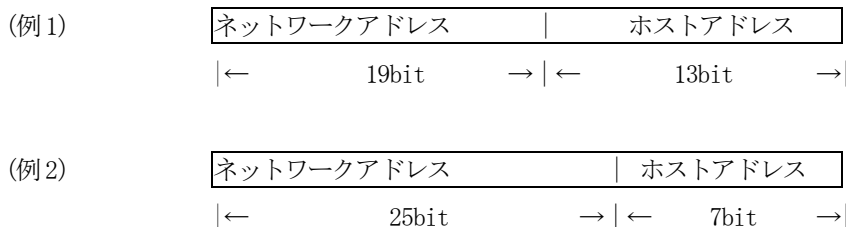


図5.7 IPアドレスのクラスレスの概念

このようにホストアドレス部とネットワークアドレス部を、任意のビット数によって区別することができるようになるため、ルータにおける経路情報を簡略化することができます。

例えば、192.64.0.1から192.64.255.255までの間には、256のネットワークアドレスがあります。これ

を 1 つのネットワークアドレスととらえれば、そのなかでホストアドレスを無駄なく割り当てることができます。

1 つに束ねるときは、192. 64. 0. 0/16 のように表現し、192. 64. 0. 0 の部分はネットワークアドレスを表し、/16 の部分はそのネットワークアドレスに使われるビット列の桁数を示しています。つまりネットワークアドレスは $8 \text{ 桁} + 8 \text{ 桁} = 16 \text{ 桁}$ となり、残りの 16 桁がホストアドレスとなります。

到着したデータは宛先 IP アドレスの上位 16 ビットが上記と同じもの(192. 64)は、すべて同じところに転送されます。これはもともと 192 で始まるクラス C の IP アドレスであるので、本来のネットワークアドレスの長さは 24 ビットのはずですが、その 24 ビットのうち上位 16 ビットが等しいクラス C の IP アドレスが一つにまとめられたことになります。これを集約化(aggregation)と呼んでいます(図 5. 8)。

この場合には 256 個のクラス C の IP アドレスが一つのネットワークとしてまとめられていることになります。そこではネットワークアドレスの長さは 16 ビットとなり、残りの 16 ビットをホストアドレスとして利用できるので、クラス B の規模の IP アドレスを割り当てることと同じようになります。このようにすればある組織に対して、254 個のクラス C を連続して割り当てることが可能になります。

このようにクラス C のアドレスでは足りない組織に対して、クラス B を割り当てず、CIDR を使って複数のクラス C を割り当てるような形で運用されています。これによってネットワークアドレスを集約し、かつ経路制御情報も少なくてすみます。さらに全体としてネットワーク上を流れるデータ量すなわちトラフィックを軽減する有効な手段といえます。

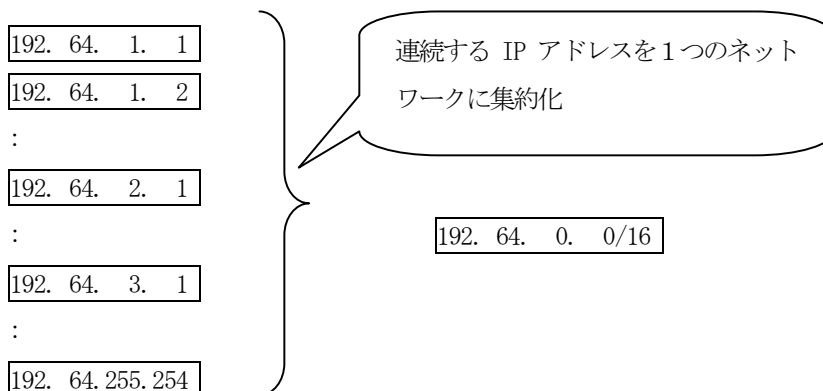


図 5. 8 CIDR によるアドレスの集約化の例

5. 14. IPv6

しかしサブネットなどを使っても、今後は家庭電化製品などを含めたコンピュータ以外の多くの機器も、インターネットに接続することが考えられているため、IPv4 ではアドレスの数が不足してしまいます。

そのため 1994 年ごろから IPv6 の開発が始められ、より多くの機器をインターネットに接続させること

を目標にしています。現在は IPv6 による実験的なネットワークが構築されており、IPv4 のアドレスと共存できるように設計されており、実際に使われ始めています[引用文献 4]。

IPv6 では、IP アドレスが 128 ビットの数値で表されます。この場合は、2 の 128 乗の数までの IP アドレスを扱うことができます。

$$2^{128} = 3.4028236692093846346337460743177e+38 \quad \text{すなわち } 3.4 \text{ 億} \times 1000 \text{ 兆} \times 1000 \text{ 兆}$$

また IPv6 ではアドレス表記の方法も 10 進数ではなく 16 進数が使われます。

表記方法は 128 ビットを 8 個の 16 ビットのグループに(8 個×16 ビット=128 ビット)に分け、それらを“:”(コロン)で区切り、そして 4 ビットをひとつの単位としてそれを 16 進数で表示します。例えば次のように表示します。

(例) 3060 : 14DE : 20AC : 0000 : 0000 : 0000 : 0BD0 : 208C

上の例のように途中で連続して 0 が出現する場合もあるため、その場合には 16 ビットに相当する 4 個の 0 をひとつの 0 で置き換えて、次のように簡略化して表記することもできます。

(例) 3060 : 14DE : 20AC : 0 : 0 : 0 : 0BD0 : 208C

IPv4 の場合には、アドレスがネットワークアドレスとホストアドレスに分かれていることはすでに述べました。これに対して IPv6 では上位 64 ビットはプレフィックス(prefix)であり、下位 64 ビットがホストアドレスとなります。プレフィックスの部分はネットワークアドレスの識別に使われます。プレフィックスは、IPv4 のような IP のクラス分けをなくし、集約化して効率よく利用するために工夫されています。

》》》 演習 5 《《《

Windows では IP アドレスがどのように設定されているかを紹介する。IP アドレスの設定や閲覧は、セキュリティ対策上 Windows では一般のユーザには許されていない。これは教室などにおいても同様である。そのため以下の IP アドレスの設定画面を見るためには、管理者でログインする必要がある。また教室などでは試すことができないため、自分のパソコンを使うか、貸し出し用など管理者でログインすることが許可されているパソコンで試すようにしていただきたい。

1. IP アドレスの設定画面

以下の順にクリックして進み、ローカルエリア接続のプロパティからインターネットプロトコル(TCP/IP)を選択し、プロパティボタンを押して、インターネットプロトコル(TCP/IP)のプロパティを開く。

スタートボタン→コントロールパネル→ネットワークとインターネット接続→ネットワーク接続→ロー

カルエリア接続を右ボタンでクリック→プロパティ→インターネットプロトコル(TCP/IP)→プロパティボタンをクリック。



図 5.9 ローカルエリア接続のプロパティ画面

インターネットプロトコル(TCP/IP)のプロパティ画面を開くと、IP アドレスの設定を行うことができる。「IP アドレスを自動的に取得する」をチェックすると、DHCP サーバーから IP アドレスの自動貸与が行われるようになり、IP アドレス、サブネットマスク、デフォルトゲートウェイの設定は行えないようになる(図 5.9)。

図 5.10 では IP アドレスとして 192.168.1.30 が設定されており、プライベート IP アドレスが使われている。またサブネットマスクが 255.255.255.0 となっており、クラス C のプライベート IP アドレスがそのまま使われていることがわかる。

デフォルトゲートウェイ(default gateway)は、別なネットワークにデータを送る場合に使われる。ネットワークにおいて同じ LAN 以外のノードにデータを転送するときは、ゲートウェイ(gateway)というノードを経由して行われる。しかしどのゲートウェイへ送ってよいかわからないときは、デフォルトゲートウェイと呼ばれる最も身近なノードへ転送する。デフォルトゲートウェイの設定をしておけば、通常のネットワークではそのデフォルトゲートウェイを経由して、目的のノードへ自動的に転送されていく。

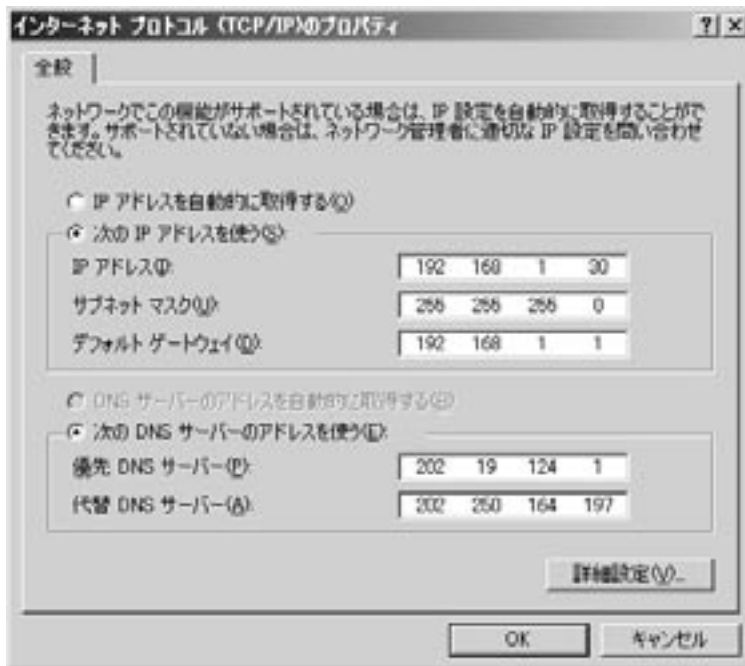


図 5.10 インターネットプロトコル(TCP/IP)のプロパティ画面

「次の DNS サーバーのアドレスを使う」というところには、DNS サーバーの IP アドレスを指定する。DNS サーバーはグローバル IP アドレスが使えるときは自分で運用することもできるが、通常はネットワークの管理者から指定されたアドレスを指定する。代替 DNS サーバーは、優先 DNS サーバーが何らかの理由で使用できないときに代わりに使われる。

なお図 5.10 における DNS サーバーなどの IP アドレスは、セキュリティ対策上架空のものを使っており、実際に設定するときは管理者から指定されたものを使う必要がある。

》》》 本章の復習 《《《

- (1) IP アドレスはどのような役割をするか。
- (2) IP アドレスのクラスとはどのようなものがあるか。
- (3) IPv4 ではアドレスはいくつぐらいまで使えるか。
- (4) サブネットとは何か。
- (5) DHCP とはどのような機能か。
- (6) プライベート IP アドレスはどのようなときに使えばよいか。

6. IP の経路制御

TCP/IP プロトコルを使って、コンピュータをインターネットに接続する場合や、コンピュータネットワーク同士を接続する場合に、IP 接続ということがあります。また自宅から ISP を経由してインターネットに接続する場合などにもしばしば使われます。IP 接続では IP アドレスを使って、相手先にデータが送り届けられ、それによって通信を行っています。

6. 1. IP ヘッダのしくみ

IP プロトコルでは、送信するデータの塊であるパケットごとに、その先頭部分にあるヘッダに、パケットの発信元 IP アドレス(Source IP Address)や宛先 IP アドレス(Destination IP Address)などの制御情報が自動的に付加されています。

現在広く使われている IPv4 は、アドレスの枯渇が憂慮されています。そのため IPv6 は、IPv4 と互換性を保ちながら、利用できるアドレス数を飛躍的に増大させ、セキュリティ機能を付加したものになっており、次世代のインターネットプロトコルといわれています。しかし今のところはまだ実験的なネットワークで使われている段階にあり、IPv4 から IPv6 への移行は急激には進まず、穏やかに進むものとみられています。

6. 1. 2. IPv4 のヘッダ形式

以下の図は IPv4 のプロトコルにおけるヘッダ形式を示したものです (図 6. 1)。

バージョン (4 ビット)	ヘッダ長 (4 ビット)	サービスタイプ(TOS) (8 ビット)	全データ長(バイト単位) (16 ビット)	
識別子(16 ビット)			フラグ (3 ビット)	フラグメントオフセット (13 ビット)
生存時間(TTL) (8 ビット)	上位プロトコル ID (8 ビット)		ヘッダチェックサム (16 ビット)	
発信元 IP アドレス(32 ビット)				
宛先 IP アドレス(32 ビット)				
オプション(不定長)			パディング	
データ				
← 32 ビット →				

図 6.1 IPv4 ヘッダの形式[引用文献7, p. 156 より作成]

IPv4 のヘッダの基本的な構成は次のようになっています[引用文献 7, 15].

(1) バージョン(Version)

IP プロトコルのバージョンが格納されています. IPv4 では 4 が格納されます.

(2) ヘッダ長(Heder Length)

パケットのヘッダの長さを表しています. ヘッダは 32 ビットを 1 単位としており, 通常のパケットはほとんどオプションが使われておらず, ヘッダ長は 20 バイト ($32 \text{ ビット} \times 5 \div 8$) です. ヘッダの最長は 60 バイト ($32 \text{ ビット} \times 15 \div 8$) になります.

(3) サービスタイプ(Service Type)

パケット (ここではデータグラム) がインターネット上でどのように扱われるかを表しています.

(4) 全データ長(Total Length)

パケットの全長を表しています. IPv4 では, 最大のパケット長は 65,535 バイトです.

(5) 識別子(Identifier)

データリンク層ではパケットの最大転送単位(MTU:Maximum Tranfer Unit)が定められており, イーサネットの場合は 1,500 バイトです. その大きさを超えるパケットは, 自動的にルータにおいてより小さな単位に細分化されます.

このときの分割される単位をフラグメント(fragment)といい, パケットを分割する処理のことをフラグメンテーション(fragmentation)と呼んでいます. 途中のルータでこの処理が行われると, この識別子フィールドに値が格納され, パケットの分割が行われたことすなわちフラグメンテーションが行われたことを示し, 宛先にパケットが届くとこの識別子フィールドの値を元にして順番に組み立てます.

(6) フラグ(Flag)

パケットのフラグメンテーションを禁止するかどうかなどの制御情報を表しています.

(7) フラグメントオフセット(Fragment Offset)

細分化されたパケットが, 元のパケットのどの位置にあったかを表します.

(8) 生存時間(Time To Live)

生存時間はそのパケットがネットワーク内に留まることができる最大の時間を示します. これは実際の時間とは異なり, 生存可能なホップ数を示します. ホップ数というのはルータの通過数のことです. ルータを経由するたびに 255 から 1 ずつ減少し, 0 になるとそのパケットは自動的に破棄されます. この生存時間の機能によって, ネットワークの中で永遠に転送され続けるパケットが発生しないように保証しています.

(9) 上位プロトコルID

パケットのデータ部が, どのような上位プロトコルかを識別するために用いられます. このフィールドによって, そのパケットが運んでいるデータはどのようなプロトコルのデータであるかを表しています. ICMP は 1, TCP は 6, UDP は 17 などの値がパケットごとに与えられています.

(1 0) ヘッダチェックサム(Header Checksum)

パケットのヘッダ部分にビットエラーが発生していないかどうか、誤り検査のために使われます。

(1 1) 発信元 IP アドレス(Source IP Address)

パケットの発信元の IP アドレスを表しています。

(1 2) 宛先 IP アドレス(Destination IP Address)

パケットの宛先の IP アドレスを表しています。

(1 3) オプション(Option)

IPv4 では通常のパケットはほとんどオプションが使われていません。しかし利用可能なものとして始点経路制御オプション、タイムスタンプオプション、経路記録オプションがあります。始点経路制御オプションは、通常の経路制御を行わないもので、パケットの発信者があらかじめ通過するルータを順番に記述するために使われます。タイムスタンプオプションは、経路上のルータまでの所用時間をオプションフィールドに記録します。経路記憶オプションは、経路上のルータのアドレスをオプションフィールドに記録します。

(1 4) パディング(Padding)

ヘッダ長を 32 ビットに揃えるために付加される調整用のビットを表しています。

(1 5) データ(Data)

転送するデータが格納されます。

6. 1. 2. IPv6 のヘッダ形式

IPv6 のヘッダ形式は次のようになっています[引用文献7, 15]。

バージョン (4 ビット)	優先順立 (8 ビット)	フローラベル (20 ビット)	
ペイロード長(16 ビット)		次ヘッダ(8 ビット)	ホップ制限(8 ビット)
発信元 IP アドレス(128 ビット)			
宛先 IP アドレス(128 ビット)			
拡張ヘッダ(可変長)			
データ			
← 32 ビット →			

図 6.2 IPv6 ヘッダの形式[引用文献7, p. 176 より作成]

IPv6 のヘッダの基本的な構成は次のようになっています[引用文献 7, 15].

(1) バージョン(Version)

IP プロトコルのバージョンが格納されています. IPv6 では 6 が格納されます.

(2) 優先度

トラフィッククラス(Traffic Class)ともいいます. トラフィックの種類などによって, 通過するルータが優先制御を行います.

(3) フローラベル(Flow Label)

音声などのリアルタイムが必要とされる特定のトラフィックフローを認識し, フローラベルの付いたパケットの優先順位を高く変更することができます.

(4) ペイロード長(Payload Length)

IPv6 のパケットの基本ヘッダ以降のデータ長を表します.

(5) 次ヘッダ(Next Header)

基本ヘッダの次にくるヘッダを示します. IPv6 の拡張ヘッダなどがきます.

(6) ホップ制限(Hop Limit)

ルータを経由する(ホップする)たびにホップ制限が 1 ずつ減少し, 0 になった場合はそのパケットは破棄されます. IPv4 では TTL に対応するフィールドです.

(7) 発信元 IP アドレスと宛先 IP アドレス

それぞれ IP パケットの発信元 IP アドレス(Source IP Address)と宛先 IP アドレス(Destination IP Address)を表しています. IPv4 と異なり, 128 ビットが使われます.

(8) 拡張ヘッダ(extension headers)

IPv6 では IPv4 のオプションフィールドを削除し, その代わりに IPv6 のさまざまな機能を実現するために使われるフィールドです. 使用可能な拡張ヘッダには次のようなものがあります.

◆経路制御ヘッダ(routing header)

パケットが宛先に到着するまでの送信途中において, 経由させたいルータを指定します.

◆フラグメントヘッダ(fragment header)

パケットのフラグメントすなわち断片化を扱うために使われます. IPv6 では途中のルータでのフラグメントは行わず, 送信ホストで行うようになっています.

◆認証ヘッダ(authentication header)

送信者自身がそのパケットを送ったことを証明するために使われます. ハッシュ関数を用いて送信パケットから認証情報を計算し, 認証ヘッダに格納します. 宛先では受け取ったパケットから同様にハッシュ関数を用いて認証情報を計算して, 今度は認証ヘッダの値と比較します. このような操作により, 発信元が信頼できる相手かどうか, 加えてパケットの内容が変更されていないかどうかを検証することができます.

◆暗号化セキュリティペイロードヘッダ(encrypted security payload header)

ネットワークに流れるパケットは、そのままでは盗聴される危険性があります。暗号化セキュリティペイロードヘッダは、この拡張ヘッダより後のペイロードを暗号化したいときに付加されます。つまり拡張ヘッダから後ろのパケットの内容が暗号化され、読み取られなくなります。

6. 1. 3. IPv4 と IPv6 のヘッダ形式の違い

IPv4 と IPv6 との違いは次のような点にあります[引用文献 15]。

◆アドレス長が 128 ビットとなり、アドレス空間が飛躍的に増大しています。

◆IPv4 においてあまり使われなかったフィールドを削除しています。また伝送上におけるビット誤りは極めて少ないと考えられ、ヘッダチェックサムも削除されています。

◆ 優先度とフローラベルという新たなフィールドを追加しました。

IPv6 は IPv4 とは異なり、通常のデータのほかに音声や映像などのマルチメディアデータを配送するために、伝送中の優先度を示すことができるように、新たに優先度フィールドとフローラベルフィールドを設けています。

◆IPv4 のオプションフィールドを削除し、機能別に拡張ヘッダを作り、必要に応じてそれらを連結します。

◆ホップごとのフラグメンテーションを禁止することになりました。これによって伝送途上で通過するルータによって、パケットが分割されなくなります。

6. 2. 経路制御

TCP/IP のインターネット層では、パケットを宛先のホストに届ける通信をコントロールするために、経路制御に関するプロトコルが用意されています。

インターネットではそれぞれのネットワークは、パケットの送受信を制御するルータ(router)と呼ばれる特殊な用途のコンピュータを経由して接続しています。

それぞれのルータには、そこに接続されている複数の回線が、どのネットワークに接続されているかという情報が設定されており、これを経路情報(routing information)と呼び、この情報はルーティングテーブル(routing table)に格納されています。ルーティングテーブルは経路制御表(経路表)あるいは転送表と呼ぶこともあります。

経路情報には、ルーティングプロトコル(routing protocol)によって自動的に生成される動的経路制御(dynamic routing)と、管理者によって手作業で設定される静的経路制御(static routing)があります。

経路情報を管理しているルータが IP パケットを受け取ると、そこに付加されている宛先 IP アドレスを調べ、ルータに設定されている経路情報を参照しながら、正しい宛先のネットワークアドレスにパケットを送り出します。

ルータのこのような機能をルーティング(routing)または経路制御と呼びます。このルーティングの機能によってインターネット層では、ホストとホストを結びつける通信を担当しています。インターネット層で送受信されるパケットは IP データグラムと呼ばれ、データグラム方式と呼ばれる経路制御方式によって転送されています。

インターネットに送り出される IP パケットは、ホストやルータの間でバケツリレーのように転送が繰り返され、IP アドレスを頼りに最終的に宛先のホストに届けられます。

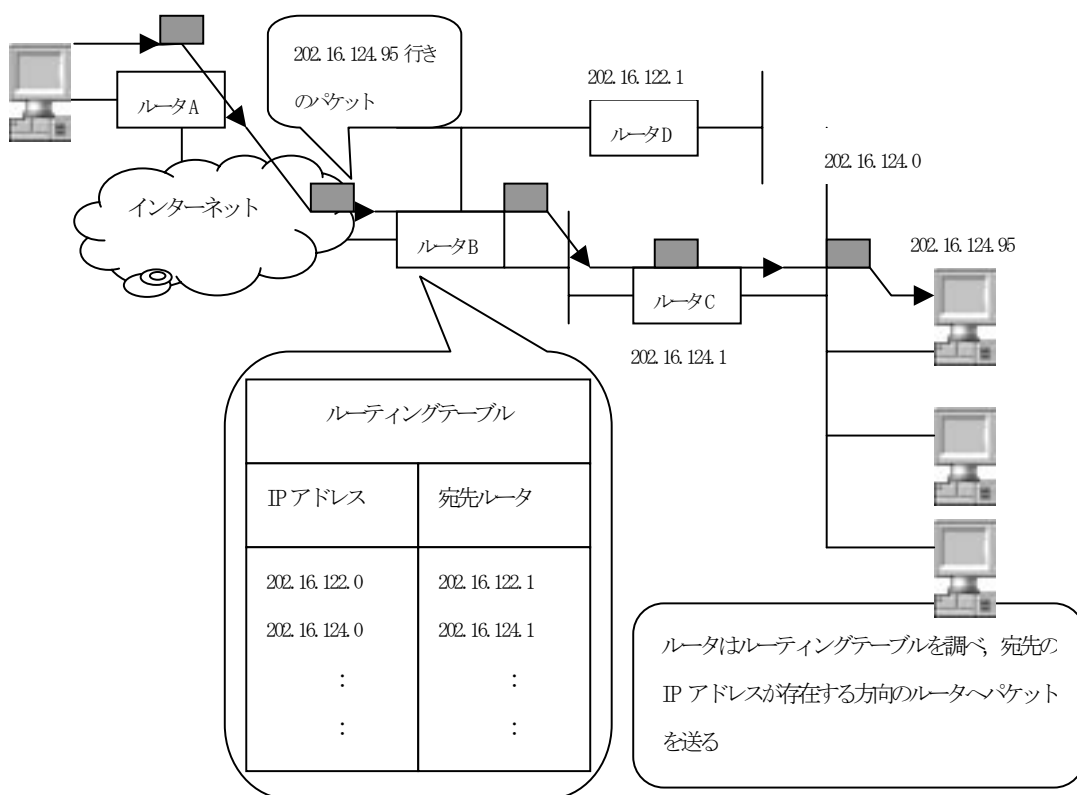


図62 IP の経路制御(ルーティング)の概念図

例えば図6.2のようにあるルータBにIPパケットが送られてきたとします。このパケットの宛先をみると202.16.124.95となっていたとします。

このIPアドレスからパケットのネットワークアドレスは202.16.124.ということが分かります。ここでは分かりやすくするため、仮にこのルータには2つのネットワークが接続されており、そのなかにルータCがあり、そのIPアドレスは202.16.124.1であるとします。

そうすればこのルータは202.16.124.のネットワークにつながっているので、このネットワークへパケットを送り出せば、目的のネットワークに接続したコンピュータに届くはずですが、

このようにどのネットワークアドレスならこのネットワークへ送ればよいのかということを、ルーティングテーブル

に設定された情報を参照することで判断しています。

6. 3. ICMP プロトコル

IP プロトコルはコネクションレス型のプロトコルのため、パケットを送信する際に順番どおりでなかったり、途中で失われることもあり、必ずしもその到着や順番が保障されているわけではありません。例えばルータの混雑などによってパケットがネットワークの何処かで消滅していないか、あるいはネットワーク機器のいずれかに障害が起きていないかなど、通信の混雑状況やネットワークの状態には関わらないようになっていきます。

つまり元々 IP プロトコルだけでは、信頼性の高いデータ通信を行うことは想定されていません。そのためこの欠点を補うために、IP プロトコルと相補って機能する ICMP (Internet Control Message Protocol) と呼ばれるプロトコルが用意されています。

ICMP は TCP/IP においては、IP プロトコルと同じインターネット層に該当するプロトコルです。IP には必ず ICMP が必要であり、ICMP は IP の上で動作するしくみになっています。

ICMP は、IP のパケットが届かないなどネットワークの障害が発生したときに、エコー要求 (echo request) とエコー応答 (echo reply) によってメッセージを生成し、送信元にパケットの到着状況を知らせます。また遠隔地の宛先ホストやルータなどにパケットを送ることによって、ネットワークがつながっているかどうかの問い合わせを行う機能を持っています。

つまり ICMP は、インターネット層の管理と制御の機能を提供しているプロトコルであり、パケットの転送途中に起きる障害を繰り返し発生させないように、エラーメッセージや制御メッセージを送信して知らせ、障害の診断を行う役割を担っているといえます。

ICMP の機能を利用したネットワーク管理ツールとして、ping, traceroute などのプログラムのほか Router Discovery (ルータ検出) などがあります。ping は宛先のコンピュータに接続できるかどうかを調べるために使われます。traceroute (Windows では tracert) はパケットがどこを経由して届くかを確認するために、転送経路を走査するために使われます。Router Discovery (ルータ検出) は、隣り合ったルータの IP アドレスを見出すための機能です [引用文献 13]。

6. 4. ARP プロトコル

図 6.2 に示したルーティング (経路制御) の概念図では、主に目的のコンピュータが接続しているネットワークに届くまでを説明していますが、図 6.2 の右端のコンピュータ (202.16.124.95) にパケットが届くまでには、IP アドレスに対応したハードウェアアドレスを知る必要があります。

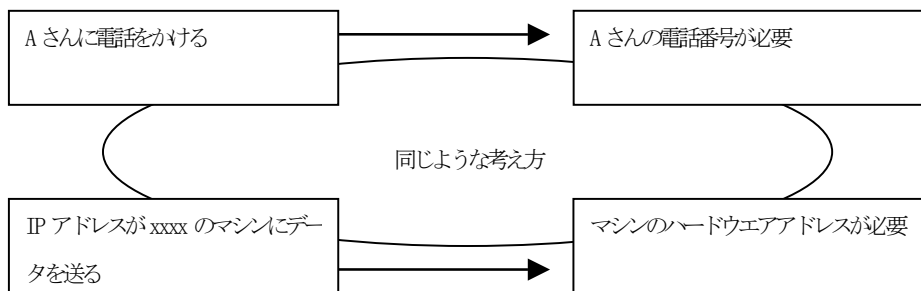


図6.3 IPアドレスとハードウェアアドレスの関係

宛先のIPアドレスが分かっているとしても、ハードウェアアドレスがわからないと通信することはできません。例えば誰かに電話をかける場合、相手の名前だけでは電話をかけることはできません。相手の名前に対応した電話番号が必要になります(図6.3)。

コンピュータにおけるデータ通信では、IPアドレスは電話の場合では相手の名前に相当し、電話番号がハードウェアアドレスに相当します。宛先のIPアドレスを頼りに通信を行いますが、同時に宛先のハードウェアアドレスを得なければ、宛先にデータを送ることはできません。

通常のネットワークに接続したホストコンピュータにおいても、各自のハードウェアアドレスは自分自身の機器の上に記載されているので、それを容易に知ることができますが、宛先のハードウェアアドレスについての情報を持ってはいません。そのため宛先のハードウェアアドレスを知るために、ARP(Address Resolution Protocol)というプロトコルが用意されています。

6. 5. ARP のしくみ

ARPプロトコルはIPアドレスからハードウェアアドレスを知るためのもので、宛先のIPアドレスを手がかりとして、それから宛先のハードウェアアドレスを入手します。通信を行う場合に途中で他のコンピュータやルータなどを経由する場合もあり、そのときは経由する機器のハードウェアアドレスを入手してさらに次の機器へパケットを送っていきます。

この際に発信元IPアドレスと宛先IPアドレスは、途中でどのような機器を経由しても変わることなく保持されています。しかしハードウェアアドレスは、物理的なネットワーク構成(物理セグメントという)ごとに、ルータなどの機器を経由するため変わっていきます。

ARPにはARPリクエストパケット(request packet)とARPレスポンスパケット(response packet)の2つがあり、前者は宛先IPアドレスなどの情報をブロードキャストするために使われ、後者は物理アドレスの送信に使われます。ハードウェアアドレスはイーサネットの場合、00-e0-16-8d-22-85のように48ビットを6つに分け、16進数で表示されます。

6. 6. ARP とハードウェアアドレスの取得

例えば、A のコンピュータが C のコンピュータに同じネットワーク上で通信するとします。A の IP アドレスは 202.16.124.1 とし、C の IP アドレスは 202.16.124.95 とします。

(1) A は C のハードウェアアドレスを入手するために、ARP リクエストパケットをブロードキャストしてネットワークに流します。このパケットのヘッダには宛先 IP アドレスが付加されています。

(2) 同じネットワーク上の全てのコンピュータには、ブロードキャストによって ARP リクエストパケットが送信されてくるので、それぞれパケットを受信してヘッダを調べます。

(3) C は宛先 IP アドレスが自分のものに該当するので、ARP レスポンスパケットによってハードウェアアドレスを A 宛に送信します。

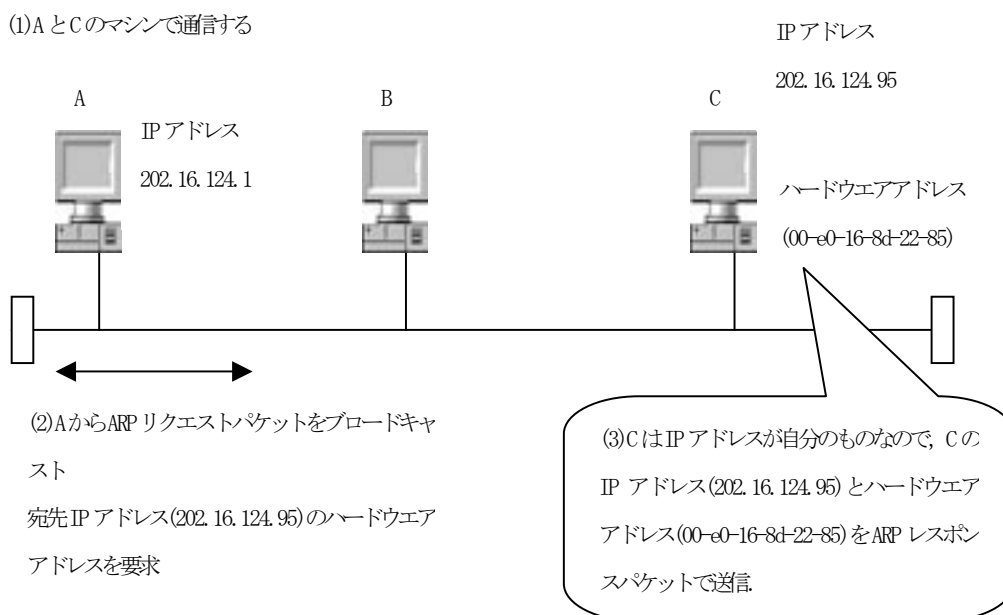


図6.4 ARP のハードウェアアドレス取得のしくみ[引用文献18, p.86 より作成]

このようにして A は C のハードウェアアドレスを入手し、通信を行うことができます(図 6.4)。ARP プロトコルを用いて入手されたハードウェアアドレスと IP アドレスの情報は、ネットワークが混雑しないようにするため、ARP キャッシュとして最長 20 分間記憶され、ARP 手続きが頻繁に発生しないようにしています[引用文献9]。

これらハードウェアアドレスや IP アドレスなどの情報は、ARP テーブルと呼ばれる対応表に、そのつど書き込まれて管理されています。arp コマンドはこの ARP テーブルの表示や設定を行うもので、これを使うと IP アドレスとハードウェアアドレスを確認することができます。

6. 7. RARP プロトコル

またARPとは逆に、ハードウェアアドレスからIPアドレスを知るプロトコルがあり、これをRARP (Reverse ARP) プロトコルといいます[引用文献 18]。

通常のコンピュータは自分のハードディスクなどに保存されるローカルなデータから、自らIPアドレスやハードウェアアドレスを認識します。しかしハードディスクを装備していないコンピュータもあり、これはIPアドレスなどの情報を保存することができません。このようなときにもハードウェアアドレスは自分の機器上に記載されているので知ることができるため、それを頼りにサーバからIPアドレスを入手する方法です。このときはRARPサーバが必要になります。

例えばIPアドレスの設定が行われていないパソコンが通信をする場合、自分のハードウェアアドレスを入れたパケットをネットワーク上に送信すると、RARPサーバがそれに応答し、これによってIPアドレスを受け取るしくみになっています。

6. 8. ポート番号

これまでの説明において、インターネットを経由してパケットが、宛先のコンピュータにどのようにして届けられるかを概説しました。しかしコンピュータの運用形態にはさまざまな方法があり、その上で使われているソフトウェアにも多種多様なものがあり、パケットを発信するコンピュータと宛先のコンピュータとでは、決して同じ状態で運用されているとはいえません。

例えば一人のユーザが、1つのアプリケーションだけを使いながら、コンピュータを専有する場合や、あるいは複数のユーザが同時に複数のアプリケーションを実行しているコンピュータもあるなど、いろいろな利用要求に合わせて運用されています。

2台以上のコンピュータでお互いに通信を行う場合、どのコンピュータまでデータを転送すべきかは、IPアドレスによって決まります。これらのコンピュータでパケットの送受信処理を行うとき、一人でコンピュータを専有している場合はほとんど問題になることはありません。

しかし、複数のユーザで1つのコンピュータを利用している場合は、どのユーザのどのプログラムにパケットを渡せばよいかを決めなければなりません。このような状態を解決する工夫が行われており、ポート番号はこの識別のために使われます。つまりネットワーク上において、同時に複数の相手と通信を行うために、IPアドレスの下に設定された補助のアドレスの役割を担っています。

どのプログラムがデータを発信したかは、発信元ポート番号をヘッダに記載することによって示されます。そしてデータの受信先のコンピュータにおいて、どのプログラムが受信すべきかを認識するために、宛先ポート番号が使われます。

TCP/IPでは実際に通信を行うためには、それぞれのコンピュータはポート番号を決定した上で通信を行

う必要があります。ポート番号は16ビットで表され、0から65535までの数値が使われます。このポート番号の機能を提供することも、TCP/IPの重要な役割になっています。

ポート番号には、公的な機関によってあらかじめサービスの種類によって決められているものがあり、これらは周知のポート(well-known port)と呼ばれています。加えてプログラムを動かしていて必要になったときに、不整合が起きないように適切にポート番号を生成して使用方法があります。

あらかじめ決められているポート番号の情報はオペレーティングシステムのファイルに格納されているので見るができます。Windows XPの場合はC:\WINDOWS\system32\drivers\etc\services (Windows2000の場合C:\WINNT\system32\drivers\etc\services) に、Linux (UNIX)の場合は/etc/services にそれぞれ格納されています。

以下にWindowsでよく使われるポート番号の例を示しますが、これらは事実上の標準となっています。

またポート番号1~1023のwell-known portは、IANA (Internet Assigned Numbers Authority) という機関によって一括して管理されています。

表6.1 Windowsにおける周知のポート番号の例

Copyright (c) 1993-1999 Microsoft Corp.

This file contains port numbers for well-known services defined by IANA Format:

<service name> <port number>/<protocol> [aliases...] [#<comment>]

#(サービス名) (ポート番号)/(プロトコル) [別名...] [説明]の順に記載

ftp-data	20/tcp		#FTP, data(ファイル転送, データ転送)
ftp	21/tcp		#FTP. Control(ファイル転送, コネクション設定)
telnet	23/tcp		
smtp	25/tcp	mail	#Simple Mail Transfer Protocol(電子メール転送)
nicname	43/tcp	whois	
domain	53/tcp		#Domain Name Server(DNS ネームサーバ)
gopher	70/tcp		
finger	79/tcp		
http	80/tcp	www www-http	#World Wide Web(ハイパーテキスト転送用)
<hr/>			
domain	53/udp		#Domain Name Server(DNS ネームサーバ)
tftp	69/udp		#Trivial File Transfer(簡易ファイル転送)
snmp	161/udp		#SNMP(ネットワーク管理)

またポート番号は、使用されるプロトコルごとに決められるため、異なるプロトコルで同じポート番号

を使用することが可能です。逆に同じコンピュータ上で同じプロトコルで動作するプロセスが複数あったときは、1つのプロセスだけでポート番号を使うことができ、他のプロセスは同一プロトコルである限り、別なポート番号を使う必要があります(図6.5)。

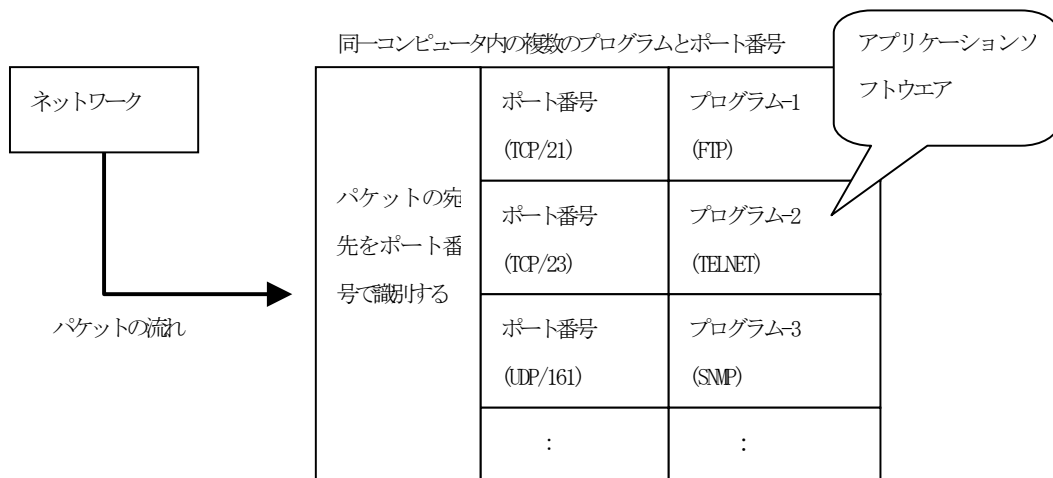


図6.5 ポート番号によるパケットの識別

6. 9. ドメインネームシステム

現在、我々はインターネットに接続することによって、さまざまなサービスの提供を受けることができます。インターネットではTCP/IPで提供される通信サービスによって、さまざまなサービスを受けることが可能になっています。

ここでのサービスはTCP/IPの通信を使って提供される通信サービスのことで、一般的にはネットワークソフトウェアによるアプリケーションサービスにあたります。

TCP/IPではアプリケーション層でこれらの多くのサービスを提供しています。しかしどの通信サービスも、第4層のTCP、UDPさらに第3層のIPプロトコルは必ず使うことになっています。

ここではインターネットを支えるために重要な役割を担っているドメインネームシステム(DNS:Domain Name System)の主なサービスについて紹介します。

6. 9. 1. ホスト名の管理とDNS

DNS(Domain Name System)は、IPアドレスとホスト名との対応づけを行うためのシステムです(図6.6の左)。ここでのホスト名は、TCP/IPによってネットワークに接続しているコンピュータに付けた名前でした。

TCP/IPを使った通信では、ネットワークに接続されているコンピュータを識別するために、必ずIPアドレスを使って、コンピュータに重複しない番号を割り当てており、そのIPアドレスに基づいてパケット

の送受信が行われ、通信が成り立つしくみになっています。

しかし IP アドレスは数字の羅列なため、相手先をよく覚えていないと使うのがなかなか大変であり、数が増えると管理するためのツールが必要になってきます。DNS が登場するまでは、それぞれのコンピュータごとに名前を付け、その名前と IP アドレスを対応させた表形式のデータを作成していました。そしてコンピュータの名前を入力すると、対応している IP アドレスが入力されたときと同じように、相手先コンピュータと通信ができるようにしていました。

Windows や Linux (UNIX) などのオペレーティングシステムでは、このようなホスト名と IP アドレスの対応表を、hosts ファイルという簡単なテキストファイルのデータベースにして管理していました。

この hosts ファイルは、Windows XP の場合は C:\WINDOWS\system32\drivers\etc\hosts (Windows2000 の場合 C:\WINNT\system32\drivers\etc\hosts に格納され)、Linux (UNIX) の場合は /etc/hosts に格納されています。

以下に Windows で使われている hosts ファイルの例を示します。このファイルに入力すれば現在でも利用することができるため、自宅などの小規模ネットワークでは手軽に使うことができます。

表 6.2 Windows の hosts ファイルの例

```
# Copyright (c) 1993-1999 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host

127.0.0.1      localhost

202.16.124.10   mc_srv.aichi-u.ac.jp   mc_srv
202.16.124.8    nwmail.aichi-u.ac.jp    nwmail
202.250.164.46  mpc-26.aichi-u.ac.jp    mpc-26
202.250.164.47  mpc-27.aichi-u.ac.jp    mpc-27
```


202. 250. 164. 52 mpc-32.aichi-u.ac.jp mpc-32
202. 250. 164. 53 mpc-33.aichi-u.ac.jp mpc-33

上の hosts ファイルの最後の部分には、IP アドレス、ホスト名、エイリアス（別名）が 1 行ごとにスペースで区切られ、表形式になって対応するように記述されています。なおここではエイリアスとはホスト名の別名のことで、これを指定しておくともアドレスを長々と入力しなくても、ホスト名だけを使うことができます。例えば同一のネットワーク内では、mc_srv.aichi-u.ac.jp と入力する代わりに、mc_srv とエイリアスだけ書けば済むようになります。

6. 9. 2. DNS の役割としくみ

インターネットの発達により、ネットワークの規模が大きくなり、接続するコンピュータの数が増加することにより、hosts ファイルのデータベースも大きくなり、IP アドレスとホスト名の登録や変更などを、集中管理によって維持しようとする考え方には限界がありました。そこでこれらの運用管理を効率よく行うために考案されたのが DNS です。

DNS は IP アドレスとホスト名の管理を、それぞれ所属する組織単位で行うことができるように分散型の管理システムになっています。従って組織内のホスト名や IP アドレスに関する変更は、その組織内で行うことができます。

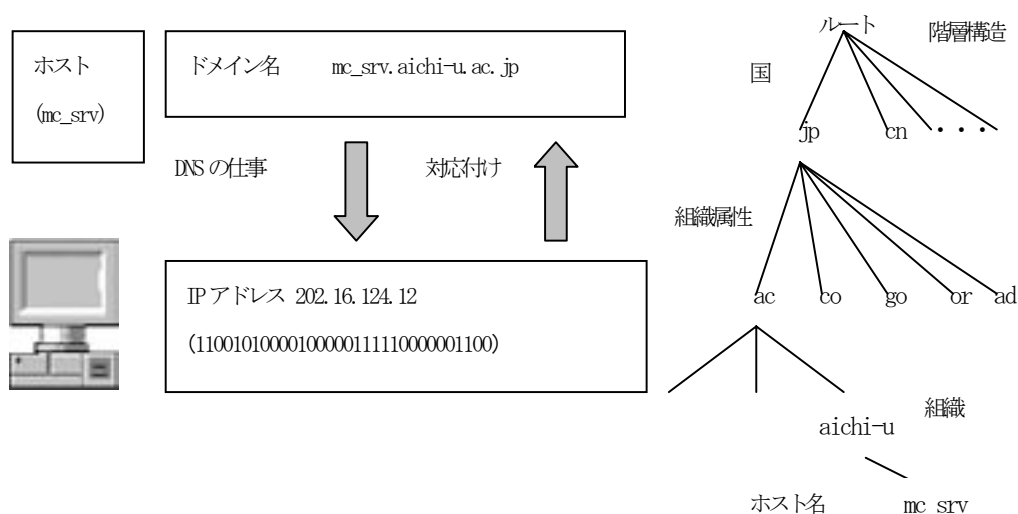


図66 ドメイン名の階層構造

DNS は階層型の名前の管理構造になっており、そのひとつの名前をドメインと呼びます。従来のドメイン

ン名は組織を表す場合が多く、同じ組織の場合は同一のドメイン名を使うのが普通です。

例えば愛知大学のドメイン名は aichi-u. ac. jp となっていますが、これで愛知大学というひとつの組織のドメイン名となっており、愛知大学の教員や学生は全員この名前を使います。

このドメインに属するある 1 台のコンピュータのホスト名に mc_srv と名前が付けられているとします。この mc_srv をインターネット上で識別するためには、mc_srv. aichi-u. ac. jp のようにドメイン名の先頭にホスト名を書きます。これによって日本を意味する jp ドメインの中の、アカデミックを意味する ac ドメインの中の、愛知大学を意味する aichi-u ドメインの中にある mc_srv と指定することができます。この階層構造の関係を図示すると、図 6.6 の右側のように表現することができます。

ドメイン名が国内の教育機関の組織のときは ac. jp が割り当てられ、政府機関であれば go. jp、一般の営利企業には co. jp のように割り当てています。

これらのドメイン名は、右側から第 1 レベル、次が第 2 レベルというようにドットで区切り、第 3 レベルの部分がそれぞれの組織を表す部分として使われています。一般的には次のような形式になっています。

組織名称. 組織の属性. 国名

このドメイン名の中にさまざまなホスト名を持つコンピュータが存在します。例えば aichi-u. ac. jp に mc_srv というホストや empc-05 というホストがあるということです。これらのコンピュータは DNS から識別するときは、mc_srv. aichi-u. ac. jp や empc-05. aichi-u. ac. jp というように先頭にホスト名を加えて表現されます。つまりホスト名を先頭に加えた場合には「ホスト名. 組織名称. 組織の属性. 国名」のように書くことができます。この書き方によってどのコンピュータかを世界中から指定することができます。

6. 9. 3. ネームサーバとリゾルバ

DNS はドメイン名の階層構造を基本として、ネームサーバ(name server)とリゾルバ(resolver)から成り立っています。ネームサーバはドメイン名を管理しているソフトウェアです。ドメイン内のホスト名と IP アドレスの情報、また他のネームサーバがどのコンピュータで動いているかという情報が設定されています。

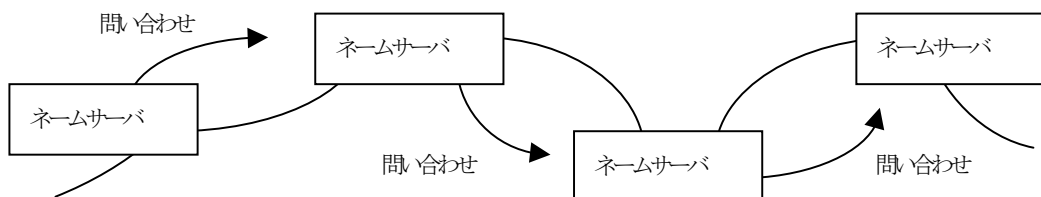


図6.7 ネームサーバと問い合わせ[引用文献18,p.172より作成]

ネームサーバが働いていることによって、どのホスト名にどのような IP アドレスが割り当ててあるかを知

ることができます。もし自分の組織外のドメイン名であるときは、他のネームサーバに問い合わせを行います(図 6. 7)。

リゾルバは、クライアントからの IP アドレスやホスト名の問い合わせを受け、その要求をネームサーバに問い合わせする機能を持つソフトウェアです。クライアントはリゾルバをとおして、ネームサーバからホスト名や IP アドレスなどの参照すべき情報をもらいます。

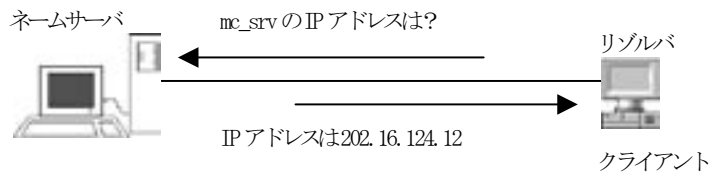


図6.8 ネームサーバとリゾルバ

従ってリゾルバは少なくとも 1 つのネームサーバにアクセスできるようになっている必要があり、コンピュータのネットワークを設定するときに、DNS が動作しているサーバの IP アドレスを指定しておく、DNS の機能を使うことができます(図 6. 8)。

6. 9. 4. ドメイン名の多様化

現在ドメイン名は、インターネット管理組織のひとつである ICANN(Internet Corporation for Assigned Names and Numbers) によって管理されています。ICANN は、ドメインネームと IP アドレスの割り当てに関するインターネット法人です。ICANN はインターネットにおけるトップの組織として、IP アドレスの割り当てを行うとともに、ドメインネームに関する調整を主な任務として行っています。

最近になって ICANN を中心にドメイン名の多様化が進められ、さまざまなドメイン名が使用できるようになっています。現在では日本でも jp ドメインのほかに、[.com] [.net] [.org] [.tv] [.info] [.biz] [.fm] [.mu] などのドメイン名が使えるようになっています。またドメイン名の一部にローマ字以外に、日本語も使えるようになりつつあり、維持費を払えば個人でドメイン名を取得することもできます[引用文献3, 5]。

》》》 演習 6 《《《

ネットワークを管理するソフトなどを使い次の演習を行ってみよ。

1. ping

ping(packet internetnetwork groper)は、ネットワークがつながっているかどうかを確認するために使われるネットワーク管理ツールの 1 つである。パケットが相手に届いたかどうかの確認に使われ、自分のコ

ンピュータから相手のコンピュータに接続できるかの診断テストに使われる。ping は ICMP (Internet Control Message Protocol) プロトコルを利用したものである。

次の例は Windows のコマンドプロンプトを起動し、mc_srv というコンピュータに ping コマンドを入力したものである。mc_srv は授業用のサーバであり、Linux が動いている。

以下の例では4つのパケットをmc_srv に向けて送信し、mc_srv からは4つのパケットを受信したので、パケットロスがなく通信は正常に行われていることを示している。もし何らかの異常が発生すると、タイムアウトになって通信が行われなかったり、パケットロスが発生したりする場合がある。

例えばtelnet やftpを利用しているアプリケーションを使おうとしてうまくいかないときなどにpingを使って調べることができる。ping コマンドを実行してパケットが正常に送受信できれば、ネットワークの接続に関しては問題がなく、アプリケーションで何らかの問題が発生していることが考えられる。

```
C:¥>ping mc_srv
```

```
Pinging mc_srv.aichi-u.ac.jp [202.16.124.8] with 32 bytes of data:
```

```
Reply from 202.16.124.8: bytes=32 time<1ms TTL=254
```

```
Reply from 202.16.124.8: bytes=32 time<1ms TTL=254
```

```
Reply from 202.16.124.8: bytes=32 time<1ms TTL=254
```

```
Reply from 202.16.124.8: bytes=32 time<1ms TTL=254
```

```
Ping statistics for 202.16.124.8:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:¥>
```

(1) 上の例を参考に、教室内で誰かが使っているコンピュータと電源が入っていないコンピュータに対して、ping コマンドを試し、結果を確認せよ。

2. arp

ARP (Address Resolution Protocol) プロトコルは、IP アドレスとハードウェアアドレス (物理アドレス、MAC アドレス) との対応付けに利用されているもので、この情報は ARP テーブルと呼ばれる対応表に格納されている。arp コマンドはこの ARP テーブルの表示や設定を行うもので、これを使うと IP アドレスとハー

ドウェアアドレスを確認することができる。

ARP テーブルには、他のコンピュータと通信を行うと、相手先の IP アドレスやハードウェアアドレスなどが一定期間保持されるようになっている。また IP アドレスが重複していると通信できなくなるが、このようにときに arp コマンドを使って調べることができる。以下の例は Windows の例であり、対応表の見方は次のようになっている。

Interface:	自分自身の IP アドレス
Internet Address	IP アドレス (ディフォルトゲートウェイと通信先のアドレス)
Physical Address	物理アドレス
Type	一定期間通信先の IP アドレスが利用されないとき自動的に削除される。

C:¥>arp -a

Interface: 202.250.164.189 — 0x2

Internet Address	Physical Address	Type
202.250.164.254	00-e0-16-8d-22-85	dynamic

(他のコンピュータと通信すると一定期間記録が保持され、ここに表示される)

(1) 自分のコンピュータの IP アドレスとハードウェアアドレスを確認してみよ。

3. ipconfig コマンド

ipconfig は、ネットワーク装置のチェックや設定に使われるコマンドである。このコマンドを使うと IP アドレスやサブネットマスク、ディフォルトゲートウェイなどの設定状況を見ることができるので、実際に試してみよ。以下の Windows の例では、IP アドレス、サブネットマスク、ディフォルトゲートウェイなどが表示されている。

C:¥>ipconfig

Windows IP Configuration

Ethernet adapter ローカル エリア接続:

Connection-specific DNS Suffix . :	(設定していないので表示されない)
IP Address. :	202.250.164.189
Subnet Mask :	255.255.255.0
Default Gateway :	202.250.164.254

4. DNS の動作

インターネットのネームサービスである DNS がどのように動作するか、Windows のコマンドプロンプトで nslookup コマンドを使って調べてみよう。

nslookup(name server lookup)は、DNS への問い合わせに利用されるネットワーク管理ツールである。DNS はコンピュータのホスト名を IP アドレスに変換するためのシステムである。なお nslookup コマンドは Linux でも使うことができる。次の例を実際に試してみよ。

(1) 教室で自分が使っている DNS サーバの IP アドレスを調べる。コマンドを次のように入力する。empc-02 の部分は自分が使っているコンピュータ名を入れる。

```
C:\>nslookup empc-02
```

(2) 愛知大学のネームサーバの名前と IP アドレスを調べる。

```
C:\>nslookup aichi-u.ac.jp
```

(3) 愛知大学の名古屋ドメインのネームサーバと IP アドレスを調べる

```
C:\>nslookup nagoya.aichi-u.ac.jp
```

(4) 上で調べた IP アドレスのひとつを使い ping コマンドを使って、通信できるかどうか確認せよ。また nslookup コマンドの後に IP アドレスを指定してコンピュータの名前と IP アドレスを調べてみよ。

```
C:\>nslookup 192.168.7.100 (例)
```

(5) Google のネームサーバの IP アドレスを調べる。Google のドメイン名は google.co.jp である。

(6) 上で調べた IP アドレスを使って、nslookup コマンドの後に IP アドレスを指定してコンピュータの名前と IP アドレスを調べてみよ。なお ping コマンドを終了させるときは Ctrl+c を押す。

5. tracert コマンド

tracert コマンドは相手先までの経路を調べて表示くれる機能を持つ。次のようにしてコマンドを試してみよ。

Windows では次のように入力する。

```
C:\>tracert google.co.jp
```

》》》 本章の復習 《《《

- (1) DNS は何の略か？ その機能はどのようなものか？
- (2) プライベート IP アドレスとグローバル IP アドレスの違いは何か？
- (3) ルータとはどのような役割をする機器のことか？
- (4) 経路制御(ルーティング)とはどういうことか？
- (5) ARP とはどのようなプロトコルか？
- (6) MAC アドレスとは何か？
- (7) ポート番号とはどのような役割をするか？

引用文献

- (1) CERN の URL には Web 誕生の経緯が紹介されている(2004.3.3).
<http://public.web.cern.ch/public/about/achievements/www/www.html>
- (2) ドメイン名の取得サービス(2004.3.3). <http://www.onamae.com/>
- (3) 遠藤薫著：システムリテラシー 2 マルチメディアとネットワーク，実教出版，pp.243，1996.
- (4) Hagen, Silvia：IPv6 エッセンシャルズ，p.357，2003.
- (5) ICANN の URL(2004.3.3). <http://icann.nic.ad.jp/>
- (6) 稲垣耕作著：コンピュータ科学の基礎，コロナ社，pp.216，1996.
- (7) 石田晴久監修：要点チェック式インターネット教科書（上），IE インスティテュート，p.381，2000.
- (8) 石田晴久監修：要点チェック式インターネット教科書（下），IE インスティテュート，p.389，2000.
- (9) 小林浩，江崎浩著：インターネット総論，共立出版，284p，2002.
- (10) 久野靖著：UNIX による計算機科学入門，丸善，pp.347，1997.
- (11) 村田正幸ほか著：社会基盤としてのインターネット，岩波書店，pp.291，2001(岩波講座インターネット6).
- (12) 日本ネットワークインフォメーションセンター(JPNIC)(2004.3.3). <http://www.nic.ad.jp/ja/>
- (13) RFC (英文) の URL(2004.3.3). <http://www.ietf.org/rfc.html>
- (14) RFC (日本語) の URL(2004.3.3). <http://rfc-jp.nic.ad.jp/>
- (15) 尾家祐二ほか著：インターネット入門，岩波書店，222p，2001(岩波講座インターネット1).
- (16) 総務省：情報通信白書，ぎょうせい，平成15年度版，Web 版は以下の URL (2004.3.3).
<http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm>
- (17) 竹下隆史ほか著：マスタリングTCP/IP—インターネットワーク編—，オーム社，p.260，1995.
- (18) 竹下隆史ほか著：マスタリングTCP/IP—入門編—，オーム社，p.336，2002.