ネットワーク入門 version 2.10

Contents

第1章

知ってる？インターネット

今では、多くの人にとって身近な存在となっているインターネット。
この章では、インターネットで提供されているサービスについて振り返った上で、インターネットの概要について学習します。

1.1 インターネットのサービス

1.1.1 ホームページ

インターネット上のホームページを見るためのサービスは、World Wide Web（www、または Web）と呼ばれるシステムによって提供されています。

ホームページを見るためには、『ブラウザ』と呼ばれるアプリケーションが必要です。

ブラウザで表示するホームページのデータは、HTML（Hyper Text Markup Language）と呼ばれる言語で記述されたテキストデータです。HTML で記述されたテキストデータは、『リンク』をクリックすると指定したデータに移動することができます。

ブラウザを起動すると、上部に
http://www.linuxacademy.ne.jp/network/index.html
といった文字列が表示されます。

この記述は、ブラウザが現在表示しているデータの保存場所と名前を示しています。

http（Hyper Text Transfer Protocol）：データをやり取りする際の方式
www　：コンピュータ名
linuxacademy.ne.jp　：ネットワーク名
network　：フォルダ名
index.html　：ファイル名

つまり、『linuxacademy.ne.jp』というネットワーク内の『www』というコンピュータ内の『network』というフォルダ内の『index.html』というファイルを、『http』という方式でやり取りする、ということを示しているのです。

この記述方法は、URL（Uniform Resource Locator）といいます。

また、インターネットの世界では、コンピュータ名を『ホスト名』、ネットワーク名を『ドメイン名』と呼んでいます。また、ホスト名とドメイン名を組み合わせたものを、FQDN（Fully Qualified Domain name：完全修飾ドメイン名）といいます。

[参考] 主なブラウザ

名称	補足
Internet Explorer(IE)	Windows に標準でインストール
Firefox	
Opera	
Safari	Mac OS に標準でインストール

1.1.2 電子メール

手紙やハガキによる連絡も、現在では電子メールで行うことの方が多くなっています。自宅のコンピュータから送信して電子メールは、どのようにして相手のコンピュータに届くのでしょうか。

自宅のコンピュータをインターネットに接続するためには、ISP（Internet Service Provider）と呼ばれる、インターネットへの接続を提供している電気通信事業社と契約する必要があります。

ISP は、契約しているユーザが電子メールを送受信するために必要な設定を行い、ユーザにメールアドレスやパスワードを交付します。

電子メールを送受信するためには、『メーラー』と呼ばれるアプリケーションが必要です。

自宅のコンピュータから送信した電子メールは、契約している ISP の『送信用メールサーバ』に到着します。そして、ISP の『送信用メールサーバ』が、電子メールの宛先メールアドレスを見て、相手のコンピュータが所属しているネットワークに電子メールを転送します。

また、自分宛の電子メールは、ISP の『受信用メールサーバ』に格納されています。格納されている電子メールは、ユーザがメーラーで受信の操作を行った時に、『受信用メールサーバ』から自宅のコンピュータに転送されます。

ここで、『サーバ』という言葉が出てきました。『サーバ』とは、サービスを提供するコンピュータ、またはアプリケーションを指します。そして、『サーバ』のサービスを利用するコンピュータやアプリケーションが、『クライアント』です。

現在のインターネットのサービスは、『サーバ』と『クライアント』によって成り立っています。この、『クライアント』が『サーバ』のサービスを利用する通信の方式を、『クライアントサーバモデル』といいます。

ISP では、ISP 内のコンピュータに必要な設定を行います。
多くの場合、ユーザ側のコンピュータに必要な設定は、ユーザ自ら行う必要があります。

最近は、ブラウザを使用した電子メールの送受信をサポートしている ISP も存在します。

[参考] 主なメーラー

名称	補足
Windows メール	Windows に標準でインストール
Microsoft Outlook	Microsoft Office に付属
Thunderbird	

1.2 クライアントサーバモデル

1.2.1 サーバ

サーバは、それぞれの用途に特化した機能を使えるようにした上で、クライアントからの要求に応えるため待機しています。そして、クライアントからの要求データが到着すると、その要求に応答するための処理を行った上で、応答データをクライアントに返します。

電子メールを送受信するためにはメールサーバが必要なように、ホームページを見るためにも専用のサーバが必要です。ブラウザから要求されたホームページのデータを提供するサーバが、『Web サーバ』です。

インターネットでは、Web サーバ、メールサーバ以外に、どのようなサーバが利用されているのでしょうか。

種類	機能	主なアプリケーション
Web サーバ	ホームページのデータを提供する。	Apache Internet Information Service
メールサーバ	電子メールの送受信を提供する。	sendmail qmail postfix
DNS サーバ	FQDN と IP アドレスを対応づける。	BIND
FTP サーバ	ファイルの転送サービスを提供する。	vsftpd ProFTPD

DNS（Domain Name System）サーバは、私たちがサーバを指定する時に使用する FQDN と、インターネット上で実際にコンピュータを識別するために使用されている『IP アドレス』を対応づける機能を提供します。

FTP（File Transfer Protocol）サーバは、ファイルの転送サービスを提供します。具体的には、FTP クライアントから FTP サーバへファイルを転送（＝アップロード）したり、FTP サーバから FTP クライアントへファイルを転送（＝ダウンロード）することができます。

1.2.2 クライアント

サーバのサービスを利用するためには、まずクライアント側で操作します。例えば、Web サーバのサービスを利用するためには、まずブラウザで URL を指定し、Web サーバにデータを要求します。

図 1-1：クライアントサーバ

ここで、サーバ用とクライアント用のアプリケーションの対応を確認しておきましょう。

クライアント用アプリケーション	サーバ用アプリケーション
ブラウザ	Web サーバ
メーラー	メールサーバ
リゾルバ	DNS サーバ
FTP クライアント	FTP サーバ

1.3 インターネットとは

1.3.1 インターネットのはじまり

私たちが利用しているインターネットと呼ばれるネットワークは、どのような経緯で生まれたのでしょうか。

インターネットの前身である ARPAnet は、アメリカ合衆国国防総省の研究機関である ARPA（Advanced Research Projects Agency）の意向により構築されました。

ARPAnet は、ソビエト連邦とアメリカ合衆国を中心とした冷戦時代の最中である 1967 年 12 月に誕生しました。この時に誕生した ARPAnet は、UCLA（University of California, LosAngeles1：カルフォルニア大学ロサンゼルス校）、UCSB（University of California, Santa Barbara：カルフォルニア大学サンダバーバラ校）、SRI（Stanford Research Institute：スタンフォード研究所）、ユタ大学のコンピュータを電話回線で接続したネットワークでした。

ARPAnet は、主に大学や研究機関のコンピュータを接続しながら発展していきました。発展していく中で、コンピュータ同士でデータをやり取りするためのルールが決まっていきました。

1972 年、国際的な会議の場で世界中の研究者たちの注目を集めた ARPAnet は、『インターネット』と名前を変えて世界中の大学や研究機関のコンピュータを接続しながら発展し、現在に至ります。

1.3.2 インターネットの構成

現在のインターネットは、どのような構成になっているのでしょうか。

現在のインターネットは、世界中の国や自治体、大学や研究機関、そしてユーザに接続を提供する ISP のネットワークによって構成されています。

この、インターネットを構成している組織のネットワークひとつひとつを、AS（Autonomous System：自律システム）と呼んでいます。つまり、インターネットは、それぞれの組織が運営するネットワーク（＝ AS）の集合体です。

AS は、他の AS と直接接続することもあれば、IX（Internet eXchange）と呼ばれる中継ポイントによって、複数の AS と接続することもあります。

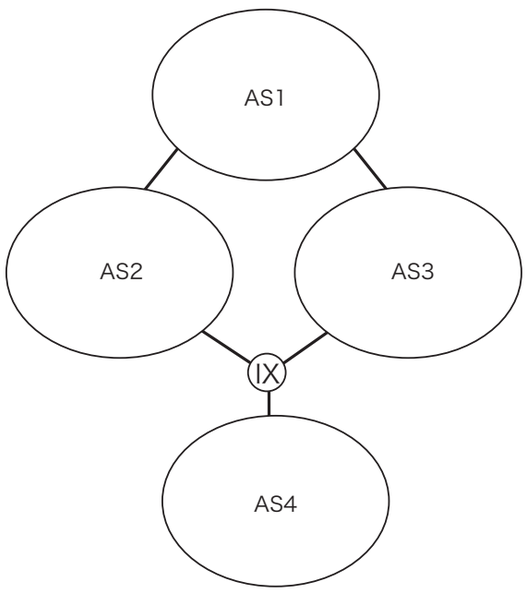

図 1-2： AS

1.4 ネットワークに接続するには

1.4.1 まずは接続

最近は、ケーブルを使用せずに接続する『無線 LAN』も一般的になってきました。無線 LAN については後述します。

現在、一般的に販売されているパーソナルコンピュータには、最初から NIC が内蔵されています。

NIC は、LAN カード、LAN ボードと呼ばれることもあります。

UTP ケーブルは、LAN ケーブルを呼ばれることもあります。

LAN（Local Area Network）とは、使用者が自分でケーブルやネットワーク機器を購入して構築するネットワークを指します。会社内や家庭内のネットワークが、LAN に相当します。

コンピュータをネットワークに参加させるためには、物理的にケーブルで接続する必要があります。

コンピュータにケーブルを接続するためには、ケーブルを接続するためのインタフェースが必要です。そのインタフェースを提供するためのハードウェアが、NIC（Network Interface Card）です。

NIC には、UTP（Unshielded Twist Pair）ケーブルを接続します。

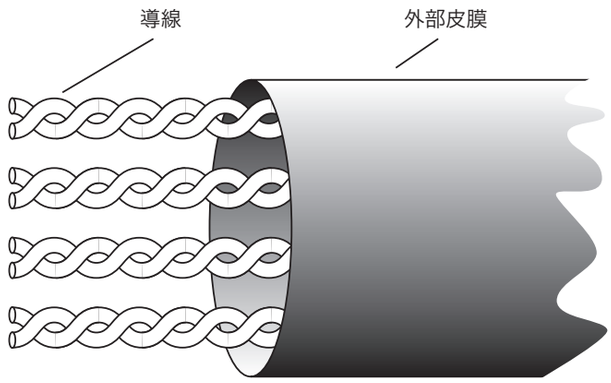

図 1-3： UTP

家庭向けのスイッチは、一般的に『スイッチングハブ』と呼ばれています。

同じネットワーク内のコンピュータを接続するためには、『ハブ』や『スイッチ』を使用します。
異なるネットワーク同士を接続するためには、『ルータ』を使用します。一般家庭向けの製品は『ブロードバンドルータ』、企業向けの製品は『ルータ』と呼ばれています。

1.4.2 決まり事

コンピュータ同士でデータをやり取りするためには、それぞれのコンピュータが同じルールで動作している必要があります。このコンピュータ同士でデータをやり取りするためのルールが、『プロトコル』です。

コンピュータ同士でデータをやり取りするには、どのようなルールが必要でしょうか。

例えば、ケーブルの素材や形状、ケーブル上に流す信号、ケーブルと機器を接続するコネクタの形状、といった物理的な部分に関するルールが必要です。

また、宛先のコンピュータを識別し、そのコンピュータまでデータを届けるためのルールも必要でしょう。

確実にデータを届けるためには、エラーが発生したら通知し、データを再送するといったことも必要です。

そして、ホームページを見るため、電子メールを送受信するため、といったそれぞれのアプリケーション独自の機能を実現するためのルールも必要です。

これらのルールを、ひとつのプロトコルで決めるのは困難なため、実際には、複数のプロトコルを組み合わせて使用しています。

例えば、宛先のコンピュータを識別し、そのコンピュータまでデータを届けるために IP（Internet Protocol）、確実にデータを届けるために TCP（Transmission Control Protocol）を使用します。

また、ホームページを見るために HTTP（Hyper Text Transfer Protocol）、電子メールを送信するために SMTP（Simple Mail Transfer Protocol）、受信するために POP（Post Office Protocol）、FQDN と IP アドレスを関連づけるために DNS（Domain Name System）、ファイルを転送するために FTP（File Transfer Protocl）を使用します。

第2章

自分を表す『IPアドレス』

電話網で電話を識別するために電話番号を使用するように、インターネットではコンピュータを識別するために『IP アドレス』を使用しています。
この章では、『IP アドレス』について学習します。

2.1 IPアドレス

2.1.1 IP アドレスによる通信

インターネットに接続しているコンピュータには、ユニークな（他のコンピュータと重複しない）『IP アドレス』を設定する必要があります。IP アドレスは、インターネット内におけるコンピュータの住所です。インターネットに接続しているコンピュータ間でデータを送受信するときは、IP アドレスを使って宛先のコンピュータを識別します。

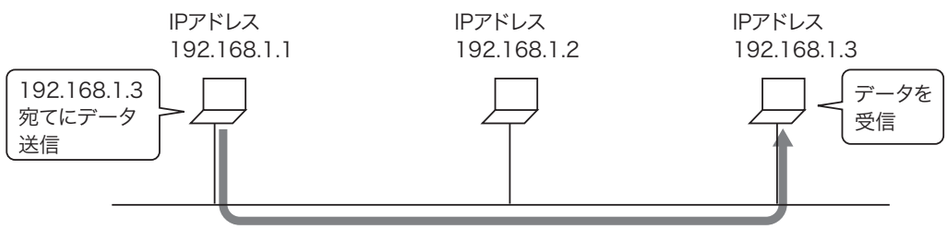

図 2-1：IP アドレスによる通信

2.1.2 IP アドレスの表記

コンピュータは、全ての情報を『0』か『1』で表現しています。このように、『0』と『1』だけで全ての数値を表す数え方を『2 進数』といいます。また、コンピュータが取り扱う情報の最小単位を『ビット』といいます。

IP アドレスは、32 桁の『0』または『1』で構成されます。つまり、IP アドレスは 32 ビットの 2 進数です。

コンピュータ内では 2 進数で処理されていますが、人間が扱うときには分かりやすいように 10 進数で表記します。

次のように、2 進数表記の IP アドレスを 8 ビット(1 オクテット)ずつに分け、それぞれを 10 進数に変換した上で、ドットで区切って表記します。

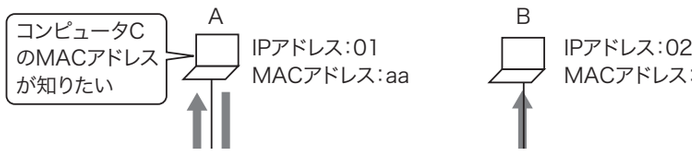

図 2-2：2 進数と 10 進数での IP アドレス表記

2.1.3 2進数、10進数の変換

IPアドレスを表記するためには、2進数を10進数に変換する必要があります。ここでは、2進数を10進数に変換する方法について説明します。

◆2進数→10進数

例として、2進数「10100110」を10進数に変換します。

2進数の各ビットは、以下の重みを持ちます。

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

① 各桁の重みの下に2進数を記述します。

128	64	**32**	16	8	**4**	**2**	1
1	0	**1**	0	0	**1**	**1**	0

② 1になっている桁の値を合計します。

```
128 + 32 + 4 + 2 = 166
```

逆に、10進数で表記したIPアドレスをコンピュータが取り扱う値に直すためには10進数を2進数に変換する必要があります。ここでは、10進数を2進数に変換する方法について説明します。

◆10進数→2進数

例として、10進数「166」を2進数に変換します。

2進数の各ビットは、以下の重みを持ちます。

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

① 10進数から、各桁の重みを引き算していきます。

```
  166
- 128   ←まず128を引き算する
-----
   38
-  32   ←64は引けないので、次の32を引き算する
-----
    6
-   4   ←16と8は引けないので、次の4を引き算する
-----
    2
-   2   ←2を引き算する
-----
    0
```

② 引き算できた箇所は1になり、引き算できなかった箇所は0になります。

128	64	**32**	16	8	**4**	**2**	1
1	0	**1**	0	0	**1**	**1**	0

2.1.4 サブネットマスク

◆ネットワーク部とホスト部

IP アドレスは、ネットワークを識別するための『ネットワーク部』と、ネットワーク内のコンピュータを識別するための『ホスト部』から構成されます。

これは、電話番号の構造とよく似ています。電話番号は市外局番と加入者番号に分かれており、市外局番で都道府県や地域を特定し、その中から加入者番号を特定しています。

IP アドレスも同様に、ネットワーク部の情報をもとにネットワークを特定し、ホスト部の情報をもとに、そのネットワーク内のコンピュータを特定します。

◆サブネットマスク

『サブネットマスク』は、ネットワーク部とホスト部の境界を示すものです。ネットワーク部を『1』で、ホスト部を『0』で表現します。つまり、サブネットマスクを２進数で表記したときの１と０の境目が、ネットワーク部とホスト部の境界です。

サブネットマスクも IP アドレスと同様に、人間が扱うときには８ビットずつ 10 進数に変換し、ドットで区切って表記します。

例えば、サブネットマスクが『255.255.255.0』の場合は、第３オクテットと第４オクテットの間が境界であることが分かります。

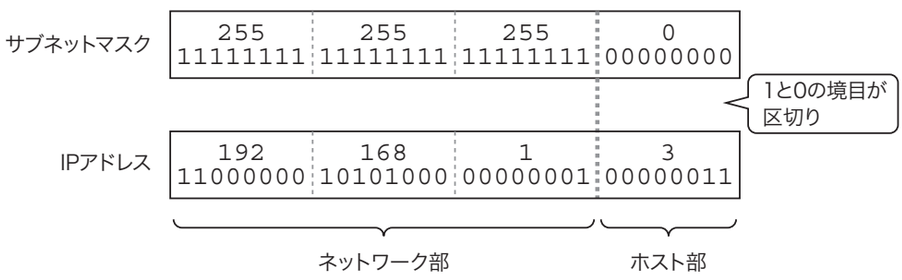

図 2-3：サブネットマスク

サブネットマスクは、『192.168.1.3 255.255.255.0』のように IP アドレスと一緒に表記します。

『192.168.1.3/24』のように、IP アドレスの後ろに『/』を付け、更にネットワーク部のビット数を記載する方法でネットワーク部とホスト部の区切りを示す方法もあります。この表記を『プレフィックス表記』といいます。

2.1.5 ネットワークアドレスとブロードキャストアドレス

各ネットワーク内の最初と最後の IP アドレスは、特別な用途のために使用されるため、コンピュータに設定することはできません。

◆ネットワークアドレス

各ネットワーク内の最初の IP アドレスは『ネットワークアドレス』と呼ばれ、ネットワーク全体を表す IP アドレスとして使用します。ネットワークアドレスは、そのネットワーク内で一番小さな IP アドレス、つまり、ホスト部が全て 0 になっているアドレスです。

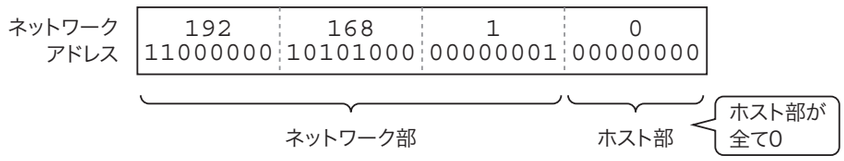

図 2-4：ネットワークアドレス

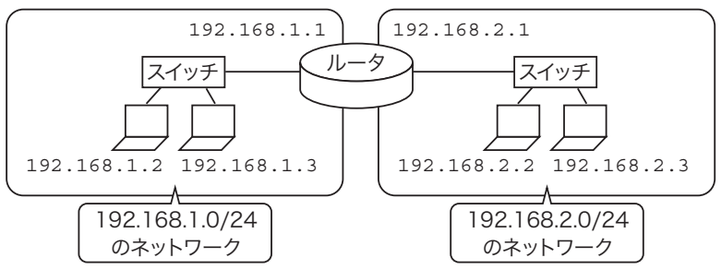

図 2-5： ネットワーク全体を表すときに使う

◆ブロードキャストアドレス

各ネットワーク内の最後の IP アドレスは、『ブロードキャストアドレス』と呼ばれ、ネットワーク内の全てのコンピュータ宛てにデータを送信するための IP アドレスとして使用します。宛先をブロードキャストアドレスにすると、ネットワーク内の全てのコンピュータが受信します。ブロードキャストアドレスは、そのネットワーク内で一番大きな IP アドレス、つまり、ホスト部が全て 1 になっているアドレスです。

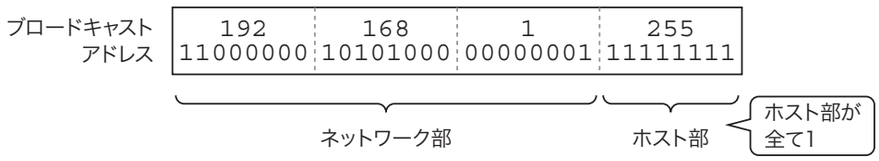

図 2-6：ブロードキャストアドレス

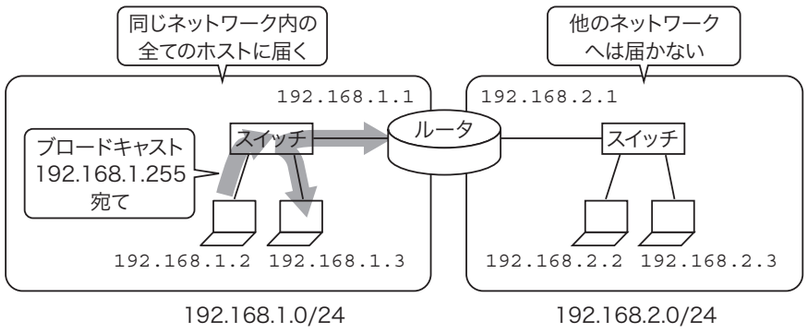

図 2-7：ブロードキャスト通信

◆IP アドレス数

ネットワーク 192.168.1.0/24 の IP アドレスの範囲は、192.168.1.0 ～ 192.168.1.255 となります。ホスト部が 8 ビットあるので、IP アドレスの個数は、2^8=256 個と計算することができます。

このうち、ネットワークアドレスとブロードキャストアドレスはコンピュータに設定することはできないので、実際に使える IP アドレスはここから 2 を引いた 254 個となります。

サブネットマスク	IP アドレス数	設定可能な IP アドレス数
255.0.0.0 (/8)	16777216 (2^{24})	16777214
255.255.0.0 (/16)	65536 (2^{16})	65534
255.255.255.0 (/24)	256 (2^8)	254

2.1.6 クラス

◆IP アドレスのクラス

IP アドレスは、5 つのクラスに分類されており、クラスごとに IP アドレスの範囲が決められています。

このうちコンピュータに設定できるのは、クラス A ～ C の IP アドレスです。クラス D は『マルチキャスト通信』という特別な通信用のアドレスとして使用します。

コンピュータに設定可能なクラス A ～ C は、クラスごとにサブネットマスクが決められています。

クラス	IP アドレスの範囲	サブネットマスク	1 ネットワークあたりの IP アドレス数（有効アドレス数）	用途
A	先頭が「0」で始まる IP アドレス （2 進数） 0.0.0.0 ～ 127.255.255.255 （10 進数）	255.0.0.0 （/8）	16777216 （16777214）	大規模ネットワーク
B	先頭が「10」で始まる IP アドレス （2 進数） 128.0.0.0 ～ 191.255.255.255 （10 進数）	255.255.0.0 （/16）	65536 （65534）	中規模ネットワーク
C	先頭が「110」で始まる IP アドレス （2 進数） 192.0.0.0 ～ 223.255.255.255 （10 進数）	255.255.255.0 （/24）	256 （254）	小規模ネットワーク
D	先頭が「1110」で始まる IP アドレス （2 進数） 224.0.0.0 ～ 239.255.255.255 （10 進数）			マルチキャストアドレス

◆ネットワークをサブネットに分ける

クラスで決められたサブネットマスクを使用していると、状況によってはコンピュータに設定されない IP アドレスが存在するケースが出てきます。

例えば、300 台のコンピュータが存在しているネットワークにクラス B を割り当てると、65534 – 300 ＝ 65234 個の IP アドレスは使用されず余ってしまいます。

一方、インターネットは世界中に広まり、IP アドレスの数は足りなくなっています。そこで、ネットワークを『サブネット』に分割する、という考え方が生まれました。

◆サブネット分割の例

クラスレスネットワークの例を見てみます。

ネットワーク 172.16.0.0 はクラス B アドレスです。クラス B 規定のサブネットマスク /16 を使った場合、IP アドレスの範囲は次のようになります。

ネットワーク	IP アドレスの範囲	IP アドレス数（有効アドレス数）
172.16.0.0/16	172.16.0.0 ～ 172.16.255.255	65536（65534）

/24 を使用すると IP アドレスの範囲は次のようになります。/24 のネットワークは /16 のネットワークを 256 に分割（サブネット化）できることが分かります。

ネットワーク	IP アドレスの範囲	IP アドレス数（有効アドレス数）
172.16.0.0/24	172.16.0.0 ～ 172.16.0.255	256（254）
172.16.1.0/24	172.16.1.0 ～ 172.16.1.255	256（254）
～		
172.16.254.0/24	172.16.254.0 ～ 172.16.254.255	256（254）
172.16.255.0/24	172.16.255.0 ～ 172.16.255.255	256（254）

クラス C の場合も考えてみましょう。

ネットワーク 192.168.1.0 はクラス C アドレスです。クラス C 規定のサブネットマスク /24 を使った場合、IP アドレスの範囲は次のようになります。

ネットワーク	IP アドレスの範囲	IP アドレス数（有効アドレス数）
192.168.1.0/24	192.168.1.0 ～ 192.168.1.255	256（254）

/26 を使用すると IP アドレスの範囲は次のようになります。/26 のネットワークは /24 のネットワークを 4 つに分割（サブネット化）していることが分かります。

ネットワーク	IP アドレスの範囲	IP アドレス数（有効アドレス数）
192.168.1.0/26	192.168.1.0 ～ 192.168.1.63	64（62）
192.168.1.64/26	192.168.1.64 ～ 192.168.1.127	64（62）
192.168.1.128/26	192.168.1.128 ～ 192.168.1.191	64（62）
192.168.1.192/26	192.168.1.192 ～ 192.168.1.255	64（62）

2.1.7 グローバルアドレスとプライベートアドレス

IP アドレスの数が不足しているため、ネットワークをサブネットに分割することで対応してきましたが、インターネットに接続するコンピュータの数が増加するにつれ、それだけでは対応しきれなくなりました。

そこで、組織内部のネットワークで自由に使用することができる『プライベートアドレス』という考え方が導入されました。

プライベートアドレスは、このようにインターネットに直接接続しないホストに割り当てるための IP アドレスです。

プライベートアドレスの範囲は次のように決められています。

プライベートアドレスの範囲

クラス	アドレス範囲	プレフィックス表記
A	10.0.0.0～10.255.255.255	10.0.0.0/8
B	172.16.0.0～172.31.255.255	172.16.0.0/12
C	192.168.0.0～192.168.255.255	192.168.0.0/16

プライベートアドレスは組織内で自由に使用することができます。しかし、インターネットではプライベートアドレスは使用できません。

インターネットと接続するためには、プライベートアドレス以外のアドレスを使用する必要があります。これが、『グローバルアドレス』です。

実際にグローバルアドレスを管理しているのは ICANN 配下の組織です。アジア太平洋地域のグローバルアドレスは APNIC（Asia Pacific Network Information Centre）が管理し、更に日本国内のグローバルアドレスは APNIC 配下の JPNIC（Japan Network Information Centre）が管理しています。

グローバルアドレスはインターネット内でユニークな値である必要があるため、ICANN（Internet Corporation for Assigned Names and Numbers）が管理しています。

インターネットにサーバを公開するためにはグローバルアドレスが必要です。その場合は、契約している ISP にグローバルアドレスを割り当ててもらいます。

クライアントのコンピュータにはプライベートアドレスを使用するのが一般的です。しかし、プライベートアドレスを使用しているコンピュータは、そのままではインターネットに接続することができません。そこで利用されるのが、NAT（Network Adress Translation）です。

2.1.8 NATとNAPT

◆ NAT

NATを使用すると、プライベートアドレスをグローバルアドレスに変換した上で、インターネットと通信することができます。

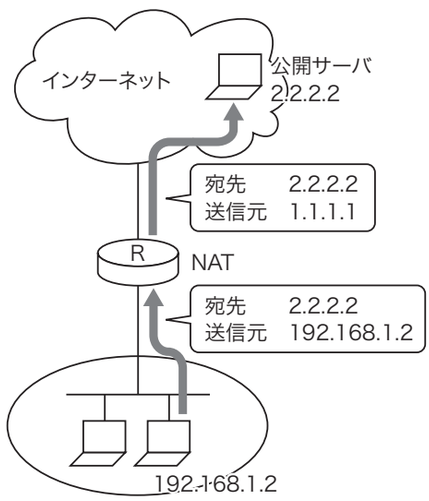

図 2-9：NAT

◆ NAPT（Network Address Port Translation）

NATはプライベートアドレスとグローバルアドレスを1対1で変換するため、インターネットに同時に接続するホストの数だけグローバルアドレスが必要です。

NAPTでは、IPアドレスだけでなく、アプリケーションを識別するために使用している『ポート番号』も一緒に変換することで、複数のプライベートアドレスを1つのグローバルアドレスに変換することができます。

正式名称は「NAPT（Network Address Port Translation）」ですが、メーカーによっては「IPマスカレード」と呼んでいます。

ポート番号については後述します。

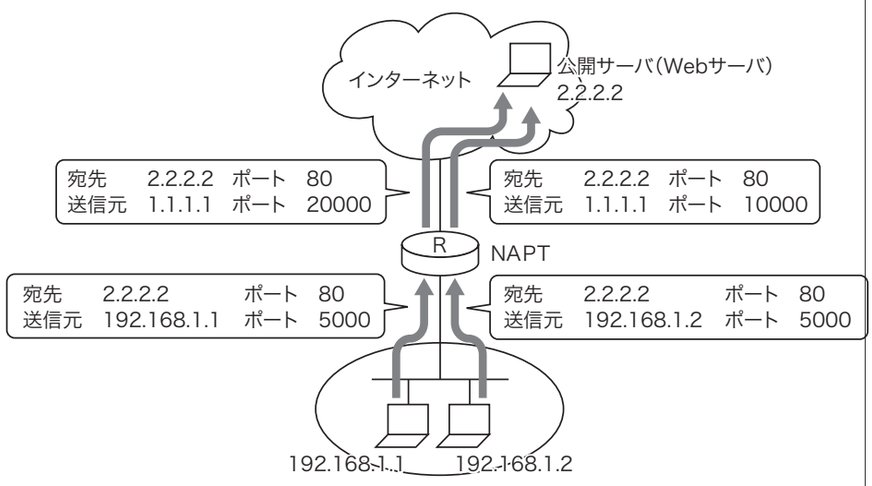

図 2-10：NAPT

第2章 確認問題

問題 1

以下の IP アドレスを 10 進数で表記してみましょう。

1-1.　11001100　10101010　10010010　01001001

1-2.　11000000　01111000　00111000　01111010

1-3.　01111111　00001111　11110000　10111111

問題 2

コマンドプロンプトを起動し、『ipconfig』コマンドを実行して、コンピュータに設定されている IP アドレスを確認してみましょう。

問題 3

『問題 1』で調べた IP アドレスを 2 進数で表記してみましょう。

問題 4

隣の席の人と IP アドレスを教え合い、教えてもらった IP アドレスを 2 進数で表記してみましょう。

問題 5

以下の IP アドレスを 2 進数で表記してみましょう。

5-1.　10.20.40.80

5-2.　150.75.37.15

5-3.　210.168.63.30

第3章

IPアドレスの計算

ネットワークのアドレス設計やトラブルシューティングの際には、各ネットワークやサブネットで使用できるIPアドレスの範囲、有効なホストアドレス数、ネットワークアドレス、ブロードキャストアドレスを把握する必要があります。

そのため、IPアドレスに関する計算問題は、どの資格試験においても出題されます。

この章では、IPアドレスの計算問題に対処できるよう、問題を解いてみましょう。

3.1 IPアドレスの計算

3.1.1 基本に忠実に

IP アドレスとサブネットマスクを２進数に変換すれば、どんな問題にも対応することができます。早速、試してみましょう。

◆『192.168.0.60　255.255.255.0』の場合

1. IP アドレス、サブネットマスクを２進数に変換する

192.168.0.60　　→　11000000　10101000　00000000　00111100
255.255.255.0　　→　11111111　11111111　11111111　00000000

2. IP アドレスのホスト部を『0』にし、ネットワークアドレスを求める

11000000　10101000　00000000　00000000　　→ 192.168.0.0

3. IP アドレスのホスト部を『1』にし、ブロードキャストアドレスを求める

11000000　10101000　00000000　11111111　　→ 192.168.0.255

4.『2』と『3』の間の値を求め、有効なホストアドレスの範囲を確認する

192.168.0.1　～　192.168.0.254

5. ホスト部のビット数から、有効なホストアドレスの個数を求める

$2^8 - 2 = 254$

◆『192.168.0.60　255.255.255.240』の場合

1. IP アドレス、サブネットマスクを２進数に変換する

192.168.0.60　　→　11000000　10101000　00000000　00111100
255.255.255.240　→　11111111　11111111　11111111　11110000

2. IP アドレスのホスト部を『0』にし、ネットワークアドレスを求める

11000000　10101000　00000000　00110000　　→ 192.168.0.48

3. IP アドレスのホスト部を『1』にし、ブロードキャストアドレスを求める

11000000　10101000　00000000　00111111　　→ 192.168.0.63

4.『2』と『3』の間の値を求め、有効なホストアドレスの範囲を確認する

192.168.0.49　～　192.168.0.62

5. ホスト部のビット数から、有効なホストアドレスの個数を求める

$2^4 - 2 = 14$

3.1.2 公式が使えれば

下の表をよく見てください。クラスCをサブネット化する場合、以下の公式が成り立つことが分かります。

クラスCのサブネット化

サブネットマスク	IPアドレス数（有効ホスト数）
/25　255.255.255.128	128（126）
/26　255.255.255.192	64（62）
/27　255.255.255.224	32（30）
/28　255.255.255.240	16（14）
/29　255.255.255.248	8（6）
/30　255.255.255.252	4（2）

256　－　第4オクテットのマスク値　＝　サブネット内のIPアドレス数

この公式を使って、前ページの例について考えてみましょう。

◆『192.168.0.60　255.255.255.240』の場合

1. サブネット化する前のネットワークアドレスを確認する

192.168.0.0

2. 公式より、サブネット内のIPアドレス数、有効なホストアドレス数を求める

IPアドレス数　→　256　－　240　＝　16
有効なホストアドレス数　→　16　－　2　＝　14

3.『1』と『2』より、各サブネットのネットワークアドレスを確認する

192.168.0.0
192.168.0.16
192.168.0.32
192.168.0.48
192.168.0.64

4.『3』より、『192.168.0.60　255.255.255.0』が所属するサブネットのネットワークアドレス、ブロードキャストアドレス、有効なホストアドレスの範囲を確認する

ネットワークアドレス　→　192.168.0.48
有効なホストアドレスの範囲　→　192.168.0.49　～　192.168.0.62
ブロードキャストアドレス　→　192.168.0.63

第3章　確認問題

問題 1

以下の IP アドレスとサブネットマスク、又はプレフィックス値を持つ IP アドレスが属するネットワークの、ネットワークアドレス、ブロードキャストアドレス、設定可能な IP アドレス数を求めてください。

1-1.　172.16.0.65　255.255.255.224

1-2.　192.168.0.129/30

1-3.　100.11.10.190/27

1-4.　10.10.10.129/28

1-5.　172.20.16.110　255.255.255.248

1-6.　192.168.201.60/29

1-7.　172.16.64.92　255.255.255.192

1-8.　192.168.153.190　255.255.255.224

1-9.　10.10.10.17　255.255.255.240

1-10.　192.168.17.17/26

1-11.　172.31.32.33/26

1-12.　10.10.10.225　255.255.255.252

1-13.　192.168.0.150　255.255.255.240

1-14.　10.10.10.110/27

1-15.　192.168.201.50/30

1-16.　10.10.10.17/26

1-17.　172.16.0.65/30

1-18.　192.168.0.129　255.255.255.224

1-19.　100.11.10.190/28

1-20.　10.10.10.129　255.255.255.248

1-21.　172.20.16.110/30

1-22.　192.168.201.60　255.255.255.240

1-23.　10.10.100.50/26

1-24.　172.18.62.92　255.255.255.224

1-25.　192.168.153.190/28

1-26.　192.168.17.17　255.255.255.248

1-27.　172.16.24.17/28

1-28.　192.168.0.150　255.255.255.224

1-29.　10.10.10.110　255.255.255.252

1-30.　172.16.16.17/26

1-31.　192.168.0.3　255.255.255.240

問題 2

以下の IP アドレスとサブネットマスク、又はプレフィックス値を持つ IP アドレスが属するネットワークの、ネットワークアドレス、ブロードキャストアドレスを求めてください。

2-1.　10.10.10.17　255.255.192.0

2-2.　10.10.100.50/22

2-3.　172.16.24.17/23

2-4.　172.16.16.17/22

2-5.　192.168.0.3　255.255.252.0

2-6.　10.10.10.17/20

2-7.　172.31.32.33/23

2-8.　10.10.10.225/18

2-9.　192.168.201.50　255.255.254.0

第4章

データが届くためには(1)

コンピュータ同士でデータのやり取りを行うためには、同じルール、つまり同じプロトコルで動作している必要があります。
この章では、プロトコルの概要と、同じネットワークのコンピュータにデータを届けるためのプロトコルについて学習します。

4.1 プロトコルの階層モデル

4.1.1 OSI 基本参照モデル

プロトコル開発のガイドラインとなるのが、ISO（国際標準化機構）によって制定された OSI 参照モデルです。OSI 参照モデルは、通信機能を 7 階層（レイヤ）に分割して定義しています。

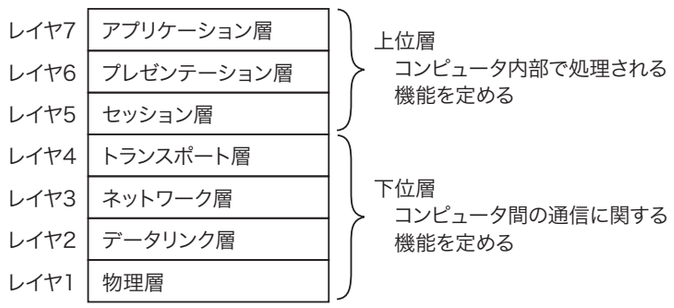

図 4-1： OSI 参照モデル

レイヤ５～７（上位層）は、コンピュータ内部で処理される機能を定めています。レイヤ１～４（下位層）は、コンピュータ間の通信に関する機能を定めています。

・アプリケーション層（レイヤ 7）
アプリケーション層は、ネットワークを利用するアプリケーションのうち、アプリケーションの機能について定めています。

・プレゼンテーション層（レイヤ 6）
プレゼンテーション層は、データの表現形式を定めています。データをネットワークで通信できる形式に変換したり、逆にネットワーク経由で受信したデータをアプリケーションが認識できる形式に復元したりします。

・セッション層（レイヤ 5）
セッション層は、アプリケーション間での通信方式を定めています。アプリケーション間でのセッションの確立・制御・終了を管理します。

・トランスポート層（レイヤ 4）
トランスポート層は、コンピュータ間での通信方法を定めています。コンピュータ間でのコネクションの確立・制御・終了を管理し、エラー回復、フロー制御などで信頼性を確保します。データの分割と再組み立てや上位層のアプリケーションを識別する機能も提供します。

・ネットワーク層（レイヤ 3）
ネットワーク層は、異なるネットワークのコンピュータ間での通信方式を定めています。論理アドレスを使って相手を特定し、相手に行くまでの伝送経路を選択します。

・データリンク層（レイヤ 2）
データリンク層は、同じネットワークのコンピュータ間での通信方式を定めています。物理アドレスを使って相手を特定し、データフレームを転送します。

・物理層（レイヤ 1）
物理層は、ケーブルの材質やコネクタ形状、および電気信号の変換方式など、物理的な仕様を定めています。

4.1.2 TCP/IP の階層モデル

◆ TCP/IP の 4 階層モデル

インターネットでは、4 階層のモデルを使って通信機能を定義しています。これを TCP/IP の階層モデルといいます。

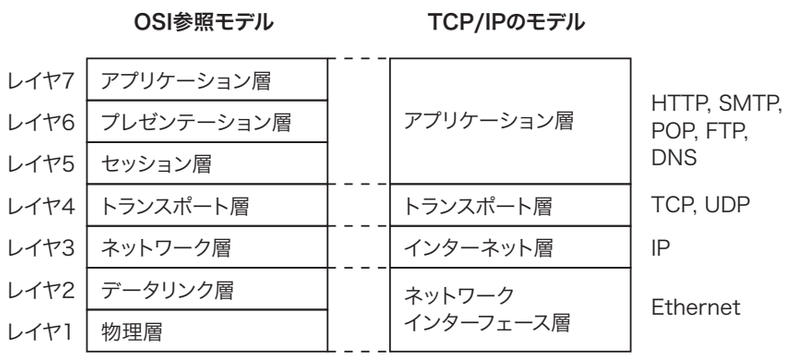

図 4-2：TCP/IP の階層モデル

ネットワークインターフェース層のプロトコルは、厳密にいうと TCP/IP プロトコル群には含まれません。

インターネットでは、非常に多くのプロトコルが使われていますが、その中でも代表的なものが TCP と IP です。そこで、インターネットで使われるプロトコルを総称して、『TCP/IP プロトコル群』と呼んでいます。単純に『TCP/IP』ともいいます。

◆ TCP/IP の標準化

RFC はインターネットに公開されています。

TCP/IP で使われているプロトコルは、IETF（Internet Engineering Task Force）で標準化が行われており、RFC（Request for Comment）というタイトルの文書に纏められています。

4.1.3 カプセル化と PDU

◆カプセル化

ネットワーク経由でデータを送信するには、データの内容に加えて、宛先アドレスや送信元アドレスなど、データを送るための制御情報が必要です。

制御情報は、データの前に付加されます。これを『ヘッダ』といいます。データリンク層ではデータの後ろにも付加されます。後ろに付く場合は『トレーラ』といいます。データに対してヘッダやトレーラを付加することを『カプセル化』といいます。

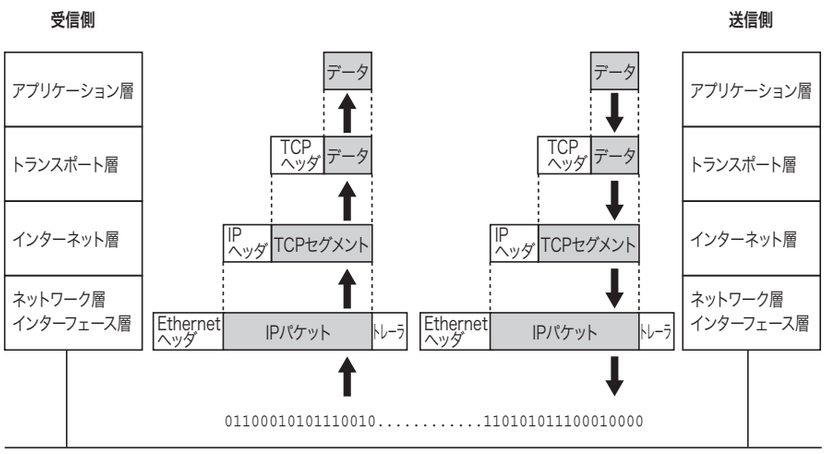

図 4-3：カプセル化

送信側では、それぞれの階層でデータをカプセル化して下位層に渡します。受信側では、各階層でヘッダの内容をチェックし、逆カプセル化を行って上位層に渡します。

◆ PDU

それぞれの階層で扱うデータの単位を、PDU（Protocol Data Unit）といいます。PDU の名称は各階層で異なっています。

階層	PDU の名称
トランスポート層	セグメント
ネットワーク層	パケット
データリンク層	フレーム
物理層	ビット

4.2 イーサネット

4.2.1 イーサネット

イーサネット（Ethernet）は、ネットワークインターフェース層（OSI 参照モデルの物理層とデータリンク層）のプロトコルで、同じネットワークのコンピュータ間での通信方式を定めています。

イーサネットの物理層では、次のような物理的な規格を定めています。

・ケーブルの種類
・コネクタの形状
・信号の変換方式

データリンク層では、次のような規格を定めています。

・メディアアクセス制御方式（誰がデータを送信するか）
・アドレッシング（誰にデータを送信するか）
・フレームフォーマット
・エラーチェック

4.2.2 イーサネットの規格

イーサネットには、使用する伝送メディア（ケーブル）や帯域幅（通信速度）によって、次のような規格があります。

規格		伝送メディア（ケーブル）	帯域幅	最大ケーブル長
Ethernet	10Base5	同軸（太）	10Mbps	500m
	10Base2	同軸（細）	10Mbps	185m
	10Base-T	UTP（カテゴリ 3 以上）	10Mbps	100m
FastEthernet	100Base-TX	UTP（カテゴリ 5 以上）	100Mbps	100m
GigabitEthernet	1000Base-T	UTP（カテゴリ 5e 以上）	1Gbps	100m

規格の名称には、次のような規則性があります。

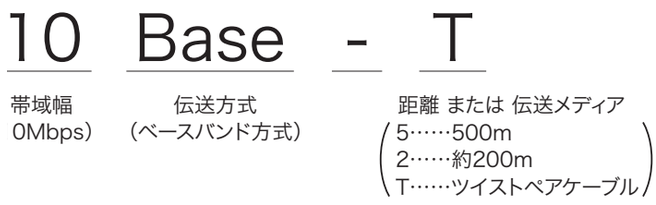

図 4-4： 命名規則

4.2.3 ケーブル

◆同軸ケーブル

当初のイーサネットは、同軸ケーブルを使用し、同軸ケーブルに複数のコンピュータを接続していました。

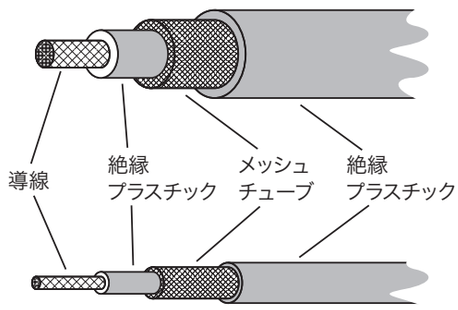

図 4-5： 同軸ケーブル

◆ UTP ケーブル

現在は、同軸ケーブルではなく、UTP ケーブルを使用しています。

・カテゴリ

UTP ケーブルは、ケーブルの品質によってカテゴリ分けされています。

UTP ケーブルのカテゴリ

カテゴリ	最大周波数	主な用途
1	-	電話線
2	1MHz	低速なデータ通信
3	16MHz	10Base-T
4	20MHz	カテゴリ 3 までの用途 TokenRing（16Mbps）、ATM（25Mbps）
5	100MHz	カテゴリ 4 までの用途 100Base-TX、ATM（156Mbps）、CDDI
5e	100MHz	カテゴリ 5 までの用途 1000Base-T
6	250MHz	カテゴリ 5e までの用途 ATM（622Mbps）、ATM（1.2Gbps）
7	600MHz	カテゴリ 6 までの用途 10GBASE-T

・ストレートケーブルとクロスケーブル

UTP ケーブルには、ストレートケーブルとクロスケーブルの 2 種類があります。

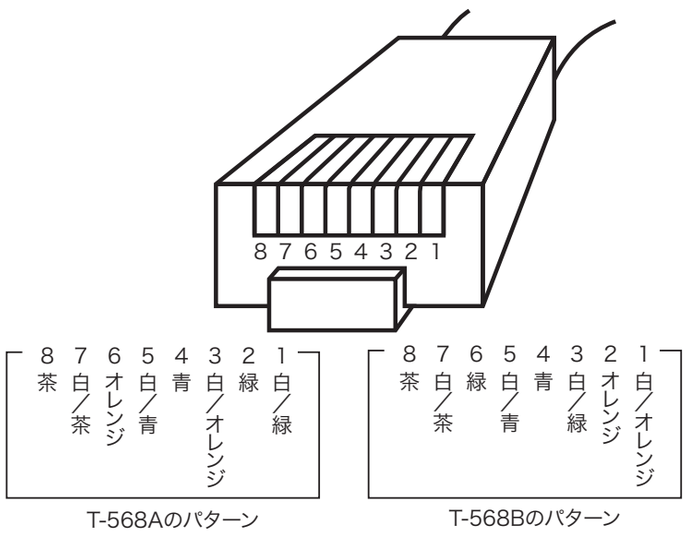

図 4-6： 芯線の色と順番

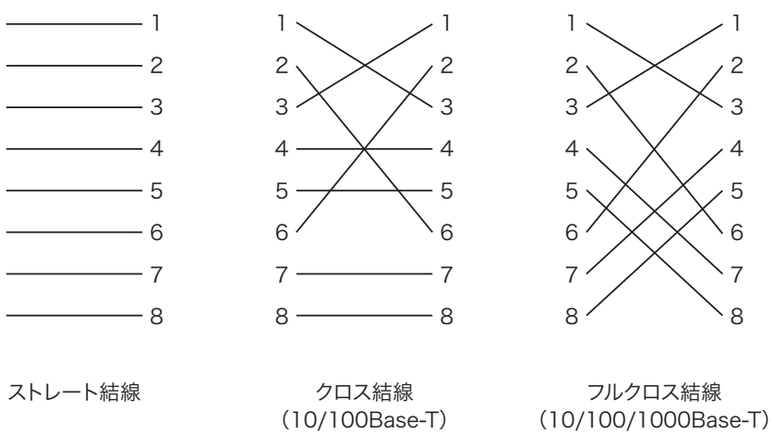

図 4-7：ストレート結線とクロス結線

イーサネットの規格によって、送信と受信に 1 対ずつ使用するものと、送信と受信に 2 対ずつ使用するものがあります。

ストレートケーブルとクロスケーブルは、どの機器とつなぐかによって使い分けます。同一機器同士を接続する場合にはクロスケーブル、同一機器同士でない場合はストレートケーブルを使用します。

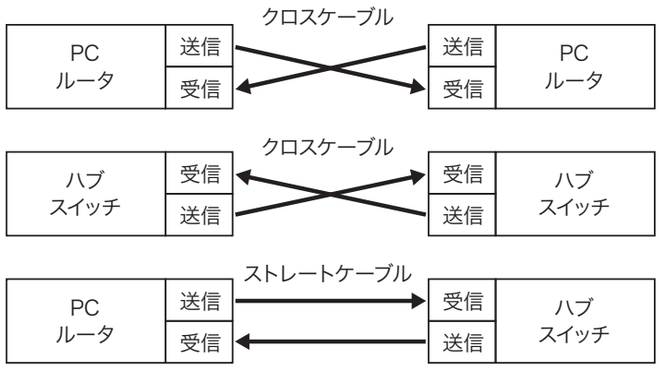

図 4-8：ケーブルの使い分け

4.2.4 CSMA/CD

イーサネットの通信方式には、CSMA/CD（Carrier Sense Multiple Access with Collision Detection）が使われています。

・Carrier Sense（搬送波感知）
フレームを送信したいコンピュータは、ケーブル上に信号が流れているかどうかをチェックします。信号が流れている場合は待機します。

・Collision Detection（衝突検出）
複数のコンピュータが同時にフレームを送信すると、衝突（collision）が発生します。
イーサネットでは、フレームの送信中にコリジョンの発生を検出すると、送信を中断し、コリジョンの発生を伝えるための JAM 信号を送信し、ランダムな時間待機してからフレームを再送します。

次のような状況になると、コリジョンが発生します。

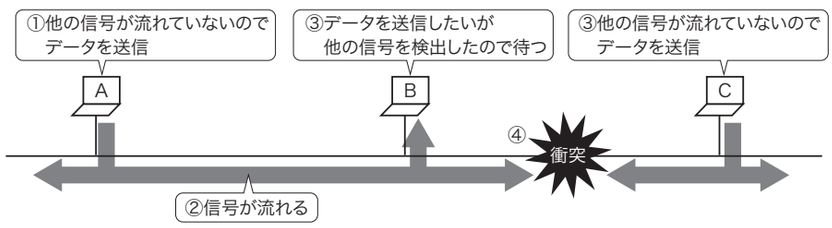

図 4-9： コリジョンの発生

①コンピュータ A は、Carrier Sense を行って、他の信号を検出しなければフレームの送信を開始する。

②ケーブル上を信号が流れていく。

③コンピュータ B は、データを送信しようとして Carrier Sense を行うと、他の信号が検出されたので待つ。コンピュータ C が、データを送信しようとして Carrier Sense を行うとコンピュータ A からの信号がまだ届いていない状態なので検出されず、フレームの送信を開始してしまう。

④コリジョンが発生する。

◆ UTP ケーブルとハブを使用する場合

現在は、同軸ケーブルではなく UTP ケーブルを使用しています。UTP ケーブルをハブと接続した場合の CSMA/CD の動作について考えてみましょう。

ハブは、あるポートで受信した信号を、他の全てのポートから送信します。そのため、ハブに接続している複数のコンピュータが同時にフレームを送信した場合、同軸ケーブルを使用している時と同様に、コリジョンが発生してしまいます。

フレームの送信中にコリジョンを検出したコンピュータが、JAM 信号を送信するのと同様に、コリジョンを検出したハブは、すべてのポートから JAM 信号を送信します。

4.2.5 MAC アドレス

イーサネットでは、『MAC アドレス』によって通信相手を特定します。MAC アドレスは、物理アドレスやハードウエアアドレスとよばれることもあります。

MAC アドレスは、世界中でユニークな（重複しない）アドレスが割り当てられ、製造時に NIC（Network Interface Card）に書き込まれます。

MAC アドレスは 48 ビットの情報で構成されているアドレスです。通常は 16 進数で表記されます。前半 24 ビットは IEEE（Institute of Electrical and Electronic Engineers：電気電子学会）がベンダに割り当てている OUI（Organizational Unique Identifier）という番号です。後半 24 ビットはシリアル番号で、ベンダ内で重複しない数字が割り当てられます。

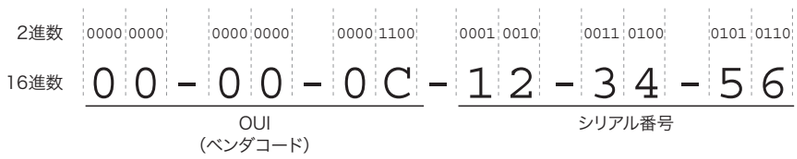

図 4-10： MAC アドレスの構成

4.2.6 フレームフォーマット

イーサネットで通信を行うときに必要な制御情報は、ヘッダとトレーラに格納されます。イーサネットのフレームフォーマットは次のようになっています。

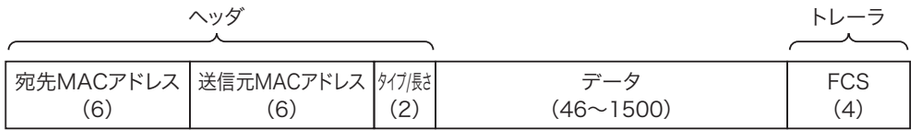

図 4-11：イーサネットのフレームフォーマット

・宛先 MAC アドレス
宛先の MAC アドレスが入ります。

・送信元 MAC アドレス
送信元の MAC アドレスが入ります。

・タイプ / 長さ
タイプの場合は、上位層でどのプロトコルを使用しているかを識別する番号が入ります。長さの場合は、後ろに続くデータの長さが入ります。

・データ
データの大きさによって 46 〜 1500 バイトのサイズになります。

・FCS
エラーチェックを行うための値が入ります。フレームを受信したコンピュータは FCS（Frame Check Sequence）を使ってエラーチェックを行います。

4.3 無線LAN

4.3.1 無線 LAN

最近は、イーサネットの代わりに電波などを使って通信を行う『無線 LAN』を使用するケースも多くなっています。ケーブルを使わずにネットワークに接続できるため、配線のコストや手間がなくなり、オフィスのレイアウト変更にも柔軟に対応できます。

一般的に、コンピュータを無線 LAN で接続する場合は、アクセスポイントを使用します。この場合、アクセスポイントと無線 LAN 用の NIC を搭載したコンピュータ間で、電波によってフレームを送受信します。

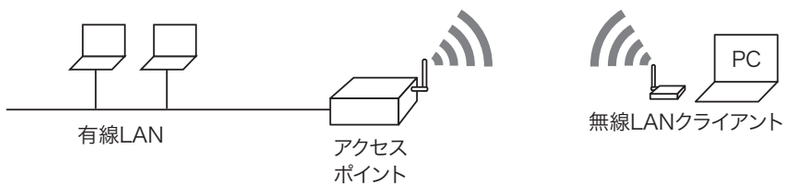

図 4-12： 無線 LAN

フロア内や建物内など、地理的に狭い範囲で構築されるネットワークのことを LAN（Local Area Network）といいます。

4.3.2 無線 LAN の規格

◆ IEEE802.11

無線 LAN のプロトコルは IEEE によって定められています。

表のチャネル数は米国での数です。日本国内では 802.11b/g は 14 チャネル（オーバーラップなしは 4 チャネル）、802.11a は、W52（4 チャネル）、W53（4 チャネル）、W56（14 チャネル）の合計 19 チャネルが、オーバーラップなしで利用可能です。

実際のスループットは、制御情報などを勘案すると、最大速度のおよそ半分程度になります。

規格名	周波数帯	DSSS 使用時の最大速度	OFDM 使用時の最大速度	チャネル数（オーバーラップなし）
802.11a	5GHz	-	54Mbps	23（12）
802.11b	2.4GHz	11Mbps	-	11（3）
802.11g	2.4GHz	11Mbps	54Mbps	11（3）

・周波数帯

周波数とは、1 秒間に電波の波形が振幅する数のことで、単位は Hz（ヘルツ）で表されます。2.4GHz 帯は、Bluetooth やコードレス電話などの家電製品でも使用されているため、家電製品との電波干渉が問題になることもあります。

・符号化方式

デジタル信号を電波に乗せる際の方式として、DSSS（Direct Sequence Spread Spectrum： ダイレクトシーケンススペクトラム拡散方式）と OFDM（Orthogonal Frequency Division Multiplexing： 直交周波数分割多重）を使用しています。

・チャネル

実際には、5GHz、または 2.4GHz の周波数帯を複数のチャネルに分けて使用します。

2.4GHz 帯は、2.402GHz ～ 2.483GHz の範囲を 11 チャネルに分けていますが、それぞれのチャネルの範囲は互いにオーバーラップしています。

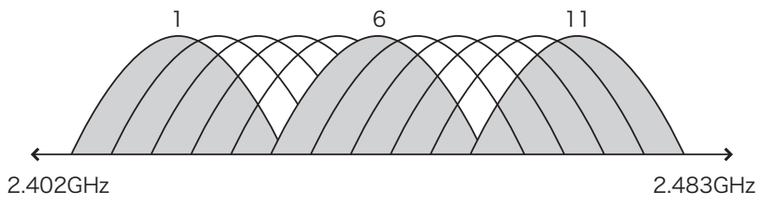

図 4-13： チャネル

複数のアクセスポイントの電波の届く範囲では、オーバーラップしているチャネルを利用すると電波の干渉が発生してしまうので、アクセスポイントはオーバラップしないチャネルを使用しなければなりません。例えば、1、6、11 チャネルを使用すれば、ほぼオーバーラップが発生せずに通信することができます。

◆ Wi-Fi アライアンス

ユーザーが安心して無線 LAN 製品を購入できるよう、無線 LAN 製品を製造しているメーカーが『Wi-Fi アライアンス』という団体を組織し、異なるメーカーの無線 LAN 製品の接続試験を行っています。相互接続試験にパスした製品には、『Wi-Fi』、『WPA』、『WPA2』マークを付けて販売しています。

マークの違いは、後述するセキュリティの実装の違いを表しています。

4.3.4 無線 LAN のセキュリティ

ここで説明しているセキュリティ規格の他に、ESSID を隠蔽する機能や MAC アドレス認証を行う機能もあります。

無線 LAN 通信では、電波の届く範囲にいれば誰でもフレームを受信することができてしまいます。そのため認証やデータの暗号化によってセキュリティを確保する必要があります。

◆ WEP（IEEE802.11）

WEP（Wired Equivalent Privacy）は､IEEE802.11 で定められているセキュリティ規格です。WEP キーとよばれる鍵を使ってデータを暗号化した上で送信することで、セキュリティを高めます。暗号化には共通鍵暗号の RC4 という方式が採用されています。しかし、この RC4 による暗号化は解読可能という問題点があります。

◆ WPA

WEP の脆弱性を補強し、セキュリティ強度を高めるために、Wi-Fi アライアンスが策定した規格が WPA（Wi-Fi Protected Access）です。Wi-Fi アライアンスによるセキュリティ試験にパスした製品には『WPA』マークが付与されます。

WPA は次のような機能でセキュリティを高めています。

- **TKIP（Temporal Key Integrity Protocol）**
  WEP キーの長さを増やし、さらに定期的に WEP キーを変更することによってセキュリティを向上させる。

IEEE802,1x は、無線 LAN だけではなく、イーサネットでも使用することができます。

個人で無線 LAN を利用する場合は、IEEE802.1x による認証はほとんど利用されていません。代わり に、PSK（Pre-Shared Key：事前共有鍵）による認証を行います。

- **IEEE802.1x**
  コンピュータがアクセスポイントに接続したときに、認証サーバによってコンピュータを使用しているユーザを認証する。

- **MIC（Message Integrity Code）**
  データの改ざんを検出する。

◆ WPA2（IEEE802.11i）

WEP の脆弱性を補強し、セキュリティ強度を高めるために、2004 年 7 月に IEEE802.11i という規格が策定されています。Wi-Fi アライアンスでは、IEEE802.11i に準拠した製品に『WPA2』マークを付与しています。

WPA2（IEEE802.11i）は、WPA のセキュリティ機能に加えて、暗号化の方式として、RC4 ではなく、AES（Advanced Excryption Standard）を採用しています。

第4章 確認問題

問題 1

コマンドプロンプトを起動し、『ipconfig /all』コマンドを実行して、コンピュータに設定されている MAC アドレスを確認しましょう。

問題 2

『問題 1』で調べた MAC アドレスのベンダーコードを確認し、どこのベンダーの NIC が搭載されているのか調べましょう。

第5章

データが届くためには(2)

同じネットワークのコンピュータにフレームを送信するためのプロトコルがイーサネットです。
しかし、イーサネットだけでは異なるネットワークのコンピュータと通信することができません。
この章では、異なるネットワークのコンピュータと通信するためのプロトコルなど、TCP/IP プロトコル群の各プロトコルについて学習します。

5.1 インターネット層

5.1.1 インターネット層のプロトコル

TCP/IP プロトコル階層モデルのインターネット層は、OSI 参照モデルのネットワーク層と同じ役割の階層です。つまり、異なるネットワークのコンピュータにデータを届けるための階層です。

ここでは、インターネット層のプロトコルについて紹介します。

・ IP（ Internet Protocol ）
インターネット層の役割を担っているのが IP です。IP によって、異なるネットワークのコンピュータと通信することができます。
IP は、IP アドレスによってコンピュータを識別します。

現在使われている IP は IPv4 (IP version 4) です。しかし、IPv4 のグローバルアドレスが残り少なくなっているため、新しいバージョンである IPv6 (IP version 6) が既に標準化され、徐々にリプレースが進んでいます。

・ ICMP（ Internet Control Message Protocol ）
IP によって、異なるネットワークのコンピュータにデータを届けることができますが、IP には、データが届いたかどうか確認する機能がありません。

そこで、IP によってデータを届けることができるかどうか確認したり、データを転送できなかった場合に、パケットの送信元に異常を知らせるために使われるプロトコルが ICMP です。

ICMP には、診断を行うためのメッセージと、エラーを通知するためのメッセージがあります。

・ ARP（ Address Resolution Protocol ）
インターネット層とネットワークインターフェイス層の中間に位置して IP アドレスと MAC アドレスの変換を行います。

5.1.2 ルータの役割（パケットのバケツリレー）

IP を使用すると、異なるネットワークコンピュータと通信することができます。

実際には、どのようにして異なるネットワークのコンピュータにデータを届けているのでしょうか。

ネットワークとネットワークの境界には、ルータが存在します。それぞれのルータは、宛先ネットワークへ到達するためには、次のどのルータにパケットを転送すれば良いのか、という情報を持っています。

また、コンピュータには、IP アドレス、サブネットマスクと共に『デフォルトゲートウェイ』という値が設定されています。この値は、ネットワークの出口に存在するルータの IP アドレスです。

コンピュータは、宛先 IP アドレスが異なるネットワークである場合、デフォルトゲートウェイとして設定されているルータに IP パケットを転送します。

パケットを転送されたルータは、宛先 IP アドレスの情報を元に、パケットを次のルータに転送します。

このようにして、コンピュータやルータがパケットを転送することで、異なるネットワークのコンピュータまでパケットを届けます。

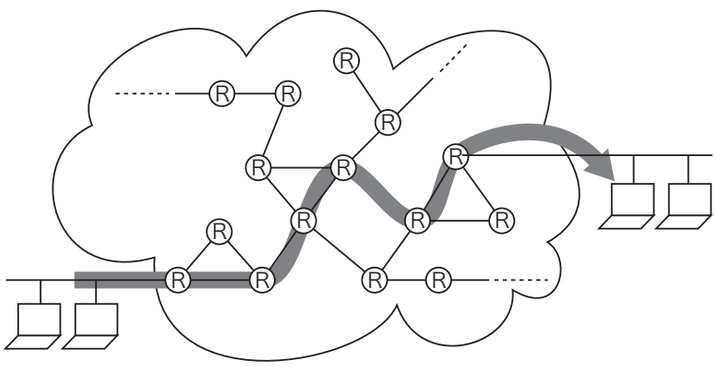

図 5-1：ルーティング

5.1.3 ICMP を利用した便利なコマンド

◆ ping

ping コマンドを使用すると、指摘した IP アドレスを持つコンピュータまで、IP パケットを転送できるかどうかを診断することができます。

ping を実行すると、ICMP Echo Request を相手に送信します。ICMP Echo Request を受け取ったコンピュータは ICMP Echo Reply を返します。

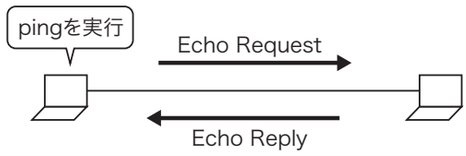

図 5-2：ping

以下は、Windows で ping を実行したときの例です。

相手から ICMP Echo Reply が返ってきた場合

ping コマンドでは、IP アドレスの代わりに FQDN を指定することもできます。

```
C:¥WINDOWS>ping 192.168.1.3

192.168.1.3 に Ping を送信しています  32 バイトのデータ：

192.168.1.3 からの応答： バイト数 =32 時間 =1ms TTL=64
192.168.1.3 からの応答： バイト数 =32 時間 =1ms TTL=64
192.168.1.3 からの応答： バイト数 =32 時間 =1ms TTL=64
192.168.1.3 からの応答： バイト数 =32 時間 =1ms TTL=64
192.168.1.3 の Ping 統計：
    パケット数： 送信 = 4, 受信 = 4, 損失 = 0(0% の損失),
ラウンドトリップの概算時間：
    最小 = 1ms, 最大 = 1ms, 平均 = 1ms
```

相手からの応答がない場合

```
C:¥WINDOWS>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
192.168.1.3 の Ping 統計：
    パケット数： 送信 = 4, 受信 = 0, 損失 = 4(100% の損失),
```

◆ tracert

tracert は、パケットが宛先に到達するまでに通ったルータを調べるコマンドです。tracert コマンドは、どのような仕組みで経由するルータを調べているのでしょうか。

Windows 以外の多くの OS では、tracert ではなく traceroute コマンドを使用します。

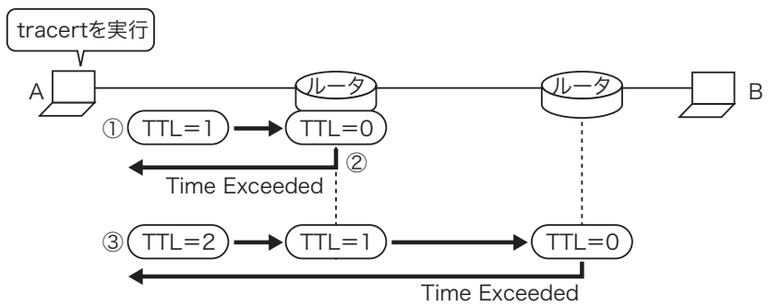

図 5-3：traceroute

① tracert を実行したコンピュータ（A）から､宛先のコンピュータ（B）に、IP ヘッダ内の TTL（Time To Live：生存時間）を 1 にセットしてパケットを送信します。

TTL は IP ヘッダに含まれる値で、ルータを通過するたびに 1 ずつ減っていき、0 になるとパケットは廃棄されます。

②パケットがデフォルトゲートウェイに到達すると、ルータは TTL を 1 から 0 に変更してパケットを破棄します。その後、パケットの送信元であるコンピュータ A に ICMP Time Exceeded を送信してパケットが破棄されたことを知らせます。コンピュータ A は、ICMP Time Exceeded を送信したルータの IP アドレスを画面に表示します。

③コンピュータ A は TTL を 2 にセットしてコンピュータ B にパケットを送信します。すると、パケットが 2 つ目のルータに到達した時点で TTL が 0 となり、2 つ目のルータから ICMP Time Exceeded が返ってきます。コンピュータ A は 2 つ目のルータの IP アドレスを画面に表示します。

5.1.4 ARP

◆ ARP とは

ARP は、IP アドレスから MAC アドレスを調べるためのプロトコルです。

パケットを送信するときには、宛先のコンピュータを IP アドレスによって指定します。しかし、実際にケーブル上に信号を送信し、同じネットワーク内のコンピュータにフレームを届けるのはイーサネットの役割です。つまり、コンピュータ間でデータをやり取りするためには、IP アドレスと MAC アドレス両方の情報が必要です。

ところが、私たちがデータを送信するときは、IP アドレス、または FQDN で相手のコンピュータを指定するだけで、MAC アドレスは指定しません。そこで、MAC アドレスを調べるために ARP を使用します。

ARP は、どのように MAC アドレスを調べているのでしょうか。

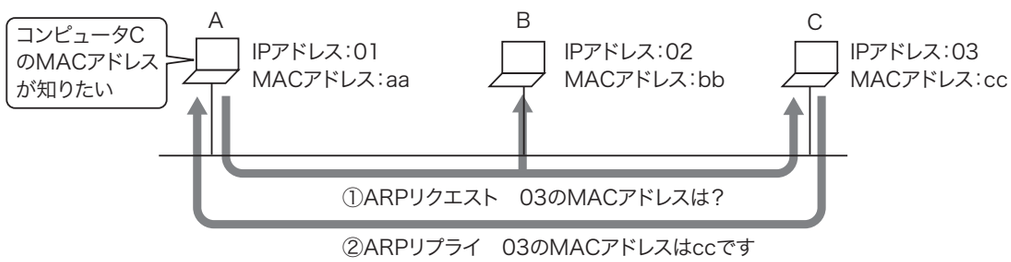

図 5-4 : ARP

①コンピュータ A は、ブロードキャスト宛てに ARP リクエストを送信し、IP アドレス 03 を持つホストに対して MAC アドレスを応答として返すように要求します。

②コンピュータ C は、ARP リプライをコンピュータ A に返し、自分の MAC アドレスをコンピュータ A に知らせます。

ARP で調べた情報は、しばらく保存されています。Windows で IP アドレスと MAC アドレスの一覧を確認するには、arp -a コマンドを実行します。

```
C:¥WINDOWS>arp -a

Interface: 172.16.0.79 --- 0x4
  Internet Address      Physical Address      Type
  172.16.0.1            00-00-e2-38-68-ba     dynamic
  172.16.0.6            00-90-cc-c2-2f-dd     dynamic
```

◆MAC アドレスと IP アドレス

ここで、同じネットワークのコンピュータにパケットを送信するときの IP アドレスと MAC アドレスについて、確認しておきましょう。

次の構成において、コンピュータ A かコンピュータ D にパケットを送信するときの送信元 IP アドレスは 01、宛先 IP アドレスが 04、送信元 MAC アドレスが aa、宛先 MAC アドレスが dd となります。

図 5-5：同じネットワーク内の通信

次に、異なるネットワークと通信するときの動作について考えてみましょう。

cc

コンピュータは、宛先 IP アドレスが異なるネットワーク宛であると判断すると、デフォルトゲートウェイに指定されているルータにパケットを転送しよう、と判断します。

そこで、ARP を使ってデフォルトゲートウェイの MAC アドレスを調べます。そして、調べた MAC アドレス宛にフレームを送信します。

この時の送信元 IP アドレスは 01、宛先 IP アドレスが 04、送信元 MAC アドレスが aa、宛先 MAC アドレスが bb となります。

ルータは、到着したパケットの宛先 IP アドレスを見て、コンピュータ B にパケットを転送しよう、と判断します。

そして、ARP を使ってコンピュータ B の MAC アドレスを調べ、調べた MAC アドレス宛にフレームを送信します。

この時の送信元 IP アドレスは 01、宛先 IP アドレスが 04、送信元 MAC アドレスが cc、宛先 MAC アドレスが dd となります。

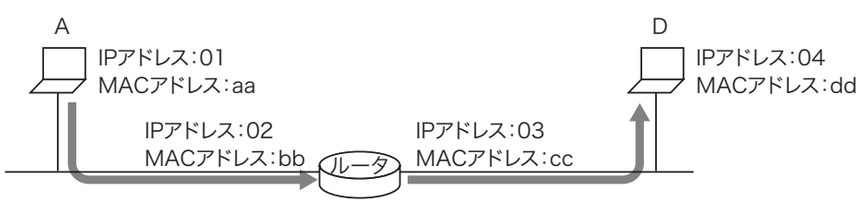

図 5-6：異なるネットワークとの通信

5.2 トランスポート層

5.2.1 トランスポート層のプロトコル

TCP/IP プロトコル階層モデルのトランスポート層では、上位のアプリケーションを識別しています。

TCP/IP のトランスポート層で動作するプロトコルには TCP（Transmission Control Protocol）や UDP（User Datagram Protocol）があります。

TCP は、上位のアプリケーションを識別するだけではなく、通信に信頼性を確保するための機能を持っています。UDP には信頼性の機能はありませんが、信頼性を確保するための手続きを省略しているため、高速な通信が可能です。

5.2.2 ポート番号

コンピュータ上では、同時に複数のアプリケーションが動作し、複数のコンピュータとデータをやり取りすることがあります。その場合、それぞれのコンピュータは、IP によって届けられたパケットが、どのアプリケーション宛てなのかを識別する必要があります。そこで、『ポート番号』を使ってアプリケーションを識別します。

ポート番号には 0 ～ 65535 の値が使われており、その番号によって 3 つに分類されています。

ポート番号	名前と用途
0 ～ 1023	ウェルノウンポート
1024 ～ 49151	登録ポート
49152 ～ 65535	プライベートポート

◆ウェルノウンポート / 登録ポート

サーバは、80 番なら Web サーバ宛て、25 番ならメールサーバ宛てというように、あらかじめ予約されているポート番号を使用します。

古くから使用されているサーバは、ウェルノウンポート（well-known port）を使用します。比較的新しいサーバは、登録ポートを使用します。

主なウェルノウンポート

ポート番号	TCP/UDP	プロトコル	用途
20	TCP	ftp-data	ファイル転送（データ本体）
21	TCP	ftp	ファイル転送（コントロール）
25	TCP	smtp	メール送信
53	TCP/UDP	domain	DNS（名前解決は UDP、ゾーン転送は TCP）
80	TCP	http	WWW
110	TCP	pop3	メール受信
123	UDP	NTP	時刻合わせ

◆プライベートポート

クライアントからサーバ宛にデータを送信すると、今度はサーバからクライアントにデータが返ってきます。

クライアント側でも、どのアプリケーション宛てのデータなのかを識別する必要があるため、サーバ側と同じように、ポート番号を使用してアプリケーションを識別しています。

クライアント側は、49152 ～ 65535 の内、使っていない番号をダイナミックに使用します。例えば、クライアントでポート 6000 番が空いているとき、Web サーバと通信するために、「宛先ポート 80 番、送信元ポート 6000 番」を使用します。この場合、Web サーバがクライアントにデータを送信する時は、「宛先ポート 6000 番、送信元ポート 80 番」を使用します。

現在、ダイナミックに割り当てることができるポートの範囲は、49152 ～ 65535 となっていますが、古い OS の場合は 1024 ～ 65535 を使用することがあります。

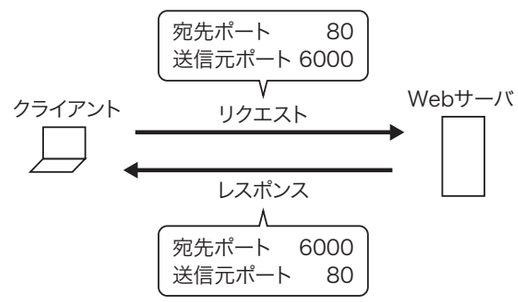

図 5-7：ポート番号

5.4 アプリケーション層

5.4.1 アプリケーション層のプロトコル

TCP/IP 階層モデルのアプリケーション層では、各アプリケーションの機能について定めています。

ここでは、主なアプリケーション層のプロトコルについて紹介します。

- **HTTP（Hyper Text Transfer Protocol）：TCP/80**
  Web サーバとクライアント間で通信するためのプロトコルです。HTTP は、Web ブラウザと Web サーバ間の通信方式を定めています。

- **SMTP（Sinple Mail Transfer Protocol）：TCP/25**
  電子メールを送信するためのプロトコルです。クライアントが送信した電子メールがサーバに届けられるときや、サーバ間でメールが転送されるときに使われます。

- **POP3（Post Office Protocol version 3）：TCP/110**
  クライアントが電子メールを受信するために使用するプロトコルです。

- **FTP（File Transfer Protocol）：TCP/20、21**
  ネットワークに接続しているコンピュータ間でファイルを転送するためのプロトコルです。ファイル転送にはポート 20、制御データの送受信にはポート 21 を使用します。

PASV モードで使用する場合は、ファイル転送時に 20 番以外のポートを使用します。

- **DNS（Domain Name System）TCP、UDP/53**
  FQDN と IP アドレスの名前解決を行うサービスです。DNS サーバ、クライアント間のやりとりには UDP を使用し、DNS サーバ間でデータを同期する際には TCP を使用します。

第5章 確認問題

問題 1

『ipconfig』コマンドを実行して、コンピュータに設定されている IP アドレスを確認しましょう。

問題 2

『問題 1』で調べた IP アドレスに対して ping を実行し、その結果を確認しましょう。

問題 3

『www.google.co.jp』に対して ping を実行し、その結果を確認しましょう。

問題 4

『www.google.co.jp』に対して tracert を実行し、その結果を確認しましょう。

問題 5

『arp -a』コマンドを実行して、コンピュータに一時保存されている IP アドレスと MAC アドレスを確認しましょう。

問題 6

『netstat -n』コマンドを実行し、結果を確認しましょう。

第6章

安全にインターネットを利用するために

世界規模のネットワークであるインターネットには、悪いことをたくらむユーザも存在します。インターネットを安全に利用するためには、どのような対策が必要なのでしょうか。

この章では、安全にインターネットを利用するための方法ついて学習しましょう。

6.1 セキュリティ

6.1.1 セキュリティとは

インターネットには、様々なユーザが接続しています。その中には、インターネットを利用して悪さをしようと企んでいるユーザも存在します。

セキュリティ（security）とは、『安全保障』という意味です。つまり、コンピュータにおけるセキュリティとは、コンピュータを安全に利用することを指します。

インターネットに接続するコンピュータを安全に利用するために、まずは、どのような脅威が存在するのか、について確認しましょう。

6.1.2 インターネットに存在する脅威

インターネット上で悪さをしようと企むユーザは、まず、ターゲットとするコンピュータの情報を入手しようとします。ここでは、情報を収集する方法について紹介します。

◆情報収集手法

・アドレススキャン

インターネットに接続しているコンピュータの IP アドレスを調べる行為を指します。
具体的には、特定の範囲を指定して ping を行う ping sweep などの方法を用います。

・ポートスキャン

インターネットに接続しているコンピュータの IP アドレスが判明したら、次は、そのコンピュータで動いているアプリケーションを特定しようと試みます。
具体的には、何番ポートで接続を受け付けるのかを調査することによって、そのコンピュータで動作しているアプリケーションのプロトコルを特定します。例えば、80 番ポートで接続を受け付けるのであれば、Web サーバ用のアプリケーションである Apache や IIS が動作していると推測することができます。

・盗聴

インターネット上を流れるパケットの内容を盗み見ることによって、情報を収集することもできます。
具体的には、『パケットキャプチャ』、『パケットスニファ』と呼ばれるツールを使用し、パケットのヘッダの内容、データの内容を読み取ります。

・フィッシング（phishing）

偽の Web サイトに誘導してパスワードなどの情報を入手します。
具体的には、金融機関などの Web サイトと精巧に再現した偽サイトを構築し、ID、パスワード、暗証番号、クレジットカード番号などを入力させ、その情報を収集します。
場合によっては、金融機関を装った電子メールを送信し、偽サイトにユーザを誘導します。この行為を、特に『ファーミング（pharming)』といいます。

・スパイウェア

コンピュータ内に保存されている情報を攻撃者のもとへ送信するプログラムです。特に、キーボードに入力した情報を収集して攻撃者に送信するスパイウェアのことを、『キーロガー』といいます。

・パスワードクラック

パスワードを破ることを、『パスワードクラック』といいます。推測、盗聴、フィッシング、スパイウェア、または文字列を総当りで試してパスワードを破ります。最後の方法は、『ブルートフォース攻撃』といいます。

ターゲットとなるコンピュータの情報を収集したら、いよいよ攻撃や侵入を企てます。ここでは、攻撃や侵入の方法について紹介します。

◆侵入・攻撃手法

・DoS 攻撃 /DDoS 攻撃

インターネットに公開されているサーバは、攻撃に備えてセキュリティを実装しているため、侵入するのは困難です。
そこで、侵入せずに、単純にサーバのサービスを停止させようと企む攻撃が頻繁に行われています。この攻撃を、『DoS（Denial of Service）攻撃』といいます。
DoS 攻撃では、サーバに大量のパケットを送りつけるなどして負荷をかけることにより、本来のサービスを提供できないようにします。
また、攻撃用のプログラムを複数のコンピュータで動かすことによって、複数のコンピュータから同時に DoS 攻撃を行う行為を、DDoS（Destributed DoS）攻撃といいます。

・脆弱性に対する攻撃

OS やアプリケーションに存在する脆弱性（セキュリティホール）を突く攻撃を行うことで、対象のコンピュータをダウンさせたり、侵入したりする攻撃です。
多くのアプリケーションに存在する脆弱性として、『バッファオーバーフロー』と呼ばれるものがあります。これは、プログラムが確保したメモリサイズを越える容量のデータが入力されると、予期しない動作が起こる、という現象です。
この現象を利用した攻撃が多数確認されたため、現在は、バッファオーバーフローを防ぐ機能が搭載されている CPU や OS が登場しています。

・バックドア

脆弱性を利用してコンピュータへの侵入が成功すると、次は容易に侵入できるように、裏口を用意しておきます。この裏口を『バックドア』といいます。

・ウィルス、ワーム、トロイの木馬

データの改ざん、破壊、情報漏洩など、様々な不正行為を行うプログラムを総称して、『不正プログラム』といいます。最近では、不正プログラム全般を指して『コンピュータウィルス』と呼ぶことがありますが、厳密には、感染対象となるファイルがあるものを『ウィルス』、そうでないものを『ワーム』といいます。
また、プログラムと一緒に、こっそりインストールされている不正プログラムのことを、特に『トロイの木馬』といいます。

6.1.2 セキュリティの実装

様々な脅威から身を守り、安全にインターネットを利用するためには、様々な対策を施す必要があります。ここでは、セキュリティ対策のための手法をいくつか紹介します。

・ファイアウォール

ファイアウォールとは、元々は『防火壁』のことです。IT の世界で『ファイアウォール』と言った場合は、組織内のネットワークと、インターネットとの間に設置して、外部からの不正なアクセスを防ぐための装置やプログラムを指します。

ファイアウォールは、ネットワークを出入りするパケットを検査して、必要なパケットは通し、不必要なパケットは破棄することによってセキュリティを確保します。

具体的には、宛先 IP アドレスや送信元 IP アドレス、ポート番号などの情報を元に、破棄するパケットを識別します。

・IDS/IPS

ファイアウォールを設置しただけでは、DoS 攻撃、DDoS 攻撃を防ぐことは出来ません。

ファイアウォールだけでは防ぐことができない攻撃を検知する装置やプログラムを IDS（Intrusion Detection System： 侵入検知システム）といいます。また、不正侵入を検知するだけではなく、攻撃パケットを破棄する機能を持つ装置は、IPS（Intrusion Prevention System： 侵入防御システム）といいます。

・IPsec

インターネットを流れるパケットは、攻撃者によって盗聴されたり、改ざんされる可能性があります。これらの攻撃から身を守るためには、パケットを暗号化し、データの改ざんを検出する必要があります。

IPsec（Security Architecture for Internet Protocol）を利用すると、パケットを暗号化し、データの改ざんを検出するだけではなく、通信相手の認証も行うことができます。インターネット上にパケットを送信する際、IPsec を利用すると、安全にパケットを送受信することができます。そこで、IPsec によって、安全にインターネットを利用することを、『インターネット VPN（Virtual Private Network）』又は『IPsec VPN』といいます。IPsec を利用するには、専用のルータやアプリケーションが必要です。

・SSL（Secure Socket Layer）

Web サーバとブラウザとの間で、安全にデータのやり取りを行うためのプロトコルとして、SSL があります。SSL にも、IPsec と同じく、暗号化、改ざんの検出、認証の機能が備わっています。SSL はブラウザに実装されているため、専用のアプリケーションを導入しなくても利用することができます。

・アンチウィルスソフト

ウィルス対策を行う専用のアプリケーションを、『アンチウィルスソフト』、『ワクチンソフト』といいます。

第7章

IPv6

IPv6（IP バージョン 6）は、新しいバージョンの IP で、使用できる IP アドレスの数が大幅に増えるほか、さまざまな機能が追加されています。
この章では、IPv6 の概要について学習しましょう。

7.1 IPv6の概要

7.1.1 IPv4 から IPv6 へ

これまでは、IPv4（IP バージョン 4）について説明を行ってきました。IPv4 アドレスは、32 ビットのアドレス空間を使用しているので、アドレスの数は約 43 億個です。インターネットの初期の頃はアドレスの数はこれで十分に足りていましたが、インターネットが世界中に普及してホスト数が増大すると、アドレスの不足が深刻な問題となってきました。

そこで、IPv4 では、クラスレス、プライベート IP アドレス、NAT などの技術を利用して IP アドレスを効率よく使う手法が用いられています。しかし、根本的な解決のためにはアドレスの数を増やすしかありません。

IPv6 アドレスは、128 ビットのアドレス空間を使用することによって、IP アドレスの数を大幅に増やしています。また、IP アドレス数以外にも様々な機能が追加されています。

7.1.2 IPv6 の特徴

◆ 128 ビットのアドレス空間

IPv6 は、128 ビットのアドレス空間を使用します。

IPv4	2^{32}=4,294,967,296 （約 43 億）
IPv6	2^{128}=340,282,366,920,938,463,463,374,607,431,768,211,456 （約 340 澗）

地球の人口を 60 億とすると、IPv4 では 1 人あたり 1 個行き渡りませんが、IPv6 では 56,713,727,820,156,410,577,229,101,238 個（約 5.7×10^{28}）ものアドレスを割り当てることが可能となり、事実上は無限とみなすことができます。

IP アドレスの数が十分にあれば、コンピュータだけでなく家電などのあらゆる機器に IP アドレスを割り当てることができます。

◆セキュリティ、モビリティ

IPv6 には、IPsec と Mobile IP の機能が標準で組み込まれています。

Mobile IP とは、ノート PC などが接続中に移動しても、同じ IP アドレスを使って途切れることなく通信を行う仕組みです。

7.2 IPv6アドレス

7.2.1 IPv6 アドレスの表記

IPv4 は、32 ビットのアドレスを 8 ビットずつに区切り 10 進数で表記します。IPv6 は、128 ビットのアドレスを 16 ビットずつに区切り 16 進数で表記します。また、表記を短くするために次のような省略の決まりがあります。

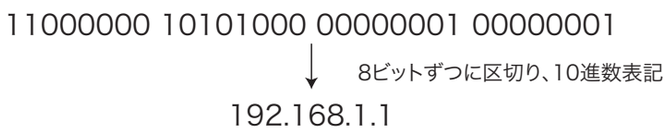

図 7-1：IPv4 の表記

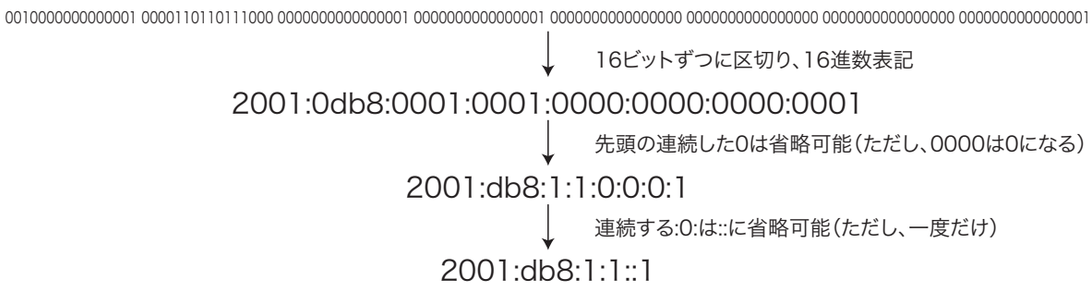

図 7-2：IPv6 の表記

7.2.2 IPv6 アドレスの種類

IPv6 には次の 3 種類のタイプがあります。

・ユニキャストアドレス
・マルチキャストアドレス
・エニーキャストアドレス

IPv4 には、ユニキャスト、ブロードキャスト、マルチキャストがありますが、IPv6 では、ブロードキャストはマルチキャストに統合され、新しくエニーキャストが追加されています。

◆ユニキャストアドレス

IPv4 と同様に、1 対 1 通信を行うためにホストを識別するアドレスです。次の 3 つに分類されます。

・グローバルユニキャストアドレス（2000::/3）
グローバルユニキャストアドレスは、2 進数「001」で始まるアドレスで、16 進数では「2000::/3」と表記されます。インターネットにおいてホストを一意に識別するためのアドレスです。

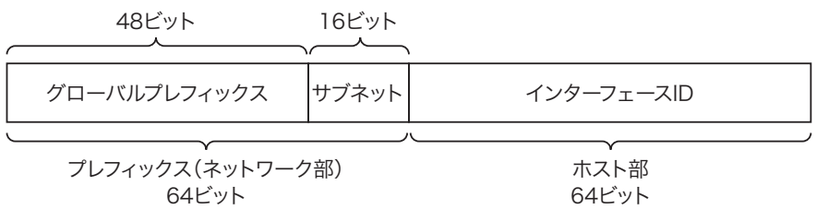

図 7-3： グローバルユニキャストアドレス

グローバルルーティングプレフィックスは、ISP から割り当てを受ける部分です。サブネットは、組織内部においてサブネット分割するときに使われる部分です。これらを合わせた前半 64 ビットがプレフィックスとよばれ、IPv4 のネットワーク部にあたります。後半 64 ビットはインターフェース ID とよばれます。サブネット内でホストを識別するための部分です。IPv4 のホスト部にあたります。

・リンクローカルアドレス（fe80::/10）
リンクローカルアドレスは、2 進数「1111 1110 10」で始まるアドレスで、16 進数では「fe80::/10」と表記されます。同一ネットワーク内で通信するときに使用される IP アドレスで、同一ネットワーク内において一意のアドレスです。このアドレスはルータによって転送されることはありません。

各インターフェースは必ずリンクローカルアドレスを持ちます。通常は、グローバルユニキャストアドレスを設定してインターフェースを有効にすると、リンクローカルアドレスは自動生成されます。

・ユニークローカルアドレス（fc00::/7）

ユニークローカルアドレスは２進数「1111 110」で始まるアドレスで、16 進数では「fc00::/7」と表記されます。IPv4 のプライベートアドレスと同様のアドレスです。

以前はサイトローカルアドレスというものがありましたが、これが廃止され、その代替として用意されたのがユニークローカルアドレスです。自由に使えるローカルアドレスでありながら、広域での一意性をなるべく担保するようになっているのが特徴です。

◆マルチキャストアドレス（ff00::/8）

マルチキャストアドレスは、２進数「1111 1111」で始まるアドレスで、16 進数では「ff00::/8」と表記されます。IPv4 と同様に、ホストのグループを識別するアドレスです。あるマルチキャストアドレスに送られたパケットは、そのマルチキャストグループに属するすべてのホストが受け取ります。

予約済みマルチキャストアドレスの例

マルチキャストアドレス	説明
ff02::1	サブネット内の全ホスト
ff02::2	サブネット内の全ルータ

◆エニーキャストアドレス

マルチキャストと同様に、ホストのグループを識別するアドレスですが、送られたパケットはグループに属するすべてのホストに届くのではなく、もっとも近いホストにのみ届きます。

同一の機能を持つサーバに同じエニーキャストアドレスを設定し、クライアントからエニーキャストアドレス宛に通信があったときに、もっとも近いサーバへ接続させるような場合に利用します。

7.3 IPv4とIPv6の共存

7.3.1 デュアルスタック

IPv4 から IPv6 へは段階的に移行していくことになります。そのため、IPv4 と IPv6 の混在環境で通信を行うための方法が用意されています。

デュアルスタックは、IPv4 と IPv6 両方のプロトコルを実装し、通信相手によってどちらを使うかを切り替える方法です。設定は、IPv4 と IPv6 のアドレスを両方設定するだけです。現在、使用されている OS は、既に IPv4 と IPv6 に対応しています。

7.3.2 トンネリング

トンネリングは、既存の IPv4 ネットワークを経由して IPv6 通信を行うときに利用される方法です。IPv6 パケットを IPv4 でカプセル化（トンネリング）することによって通信を行います。

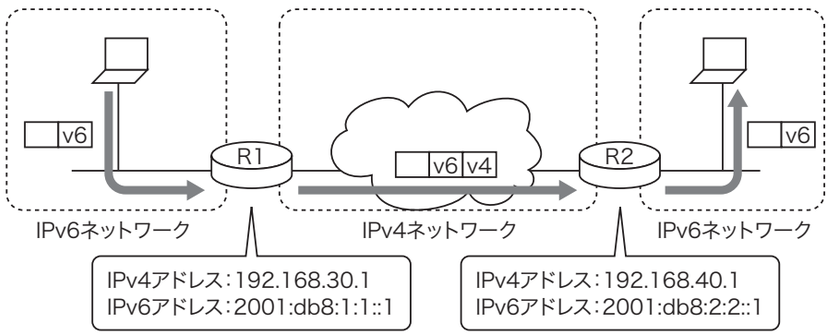

図 7-4：トンネリング

7.3.3 トランスレータ

トランスレータは、通信元や通信先がIPv6、IPv4の差異を意識しなくてすむ仕組みを提供します。

（1）Proxy方式

Proxy方式は、IPv4で利用されるProxyと同様に、アプリケーション毎に送信元の代理となって送信先へ通信を行う方式です。

（2）NAT-PT方式

NAT-PT(Network Address Translation / Protocol Translation) は、IPv6とIPv4のアドレス変換（プロトコル変換）を行います。

確認問題 解答

第3章

問題 1

1-1.　172.16.0.65　255.255.255.224

ネットワークアドレス：172.16.0.64
ブロードキャストアドレス：172.16.0.95
有効なホスト数：30

1-2.　192.168.0.129/30

ネットワークアドレス：192.168.0.128
ブロードキャストアドレス：192.168.0.131
有効なホスト数：2

1-3.　100.11.10.190/27

ネットワークアドレス：100.11.10.160
ブロードキャストアドレス：100.11.10.191
有効なホスト数：30

1-4.　10.10.10.129/28

ネットワークアドレス：10.10.10.128
ブロードキャストアドレス：10.10.10.143
有効なホスト数：14

1-5.　172.20.16.110　255.255.255.248

ネットワークアドレス：172.20.16.104
ブロードキャストアドレス：172.20.16.111
有効なホスト数：6

1-6.　192.168.201.60/29

ネットワークアドレス：192.168.201.56
ブロードキャストアドレス：192.168.201.63
有効なホスト数：6

1-7.　172.16.64.92　255.255.255.192

ネットワークアドレス：172.16.64.64
ブロードキャストアドレス：172.16.64.127
有効なホスト数：62

1-8.　192.168.153.190　255.255.255.224

ネットワークアドレス：192.168.153.160
ブロードキャストアドレス：192.168.153.191
有効なホスト数：30

1-9.　10.10.10.17　255.255.255.240

ネットワークアドレス：10.10.10.16
ブロードキャストアドレス：10.10.10.31
有効なホスト数：14

1-10.　192.168.17.17/26

ネットワークアドレス：192.168.17.0
ブロードキャストアドレス：192.168.17.63
有効なホスト数：62

1-11.　172.31.32.33/26

ネットワークアドレス：172.31.32.0
ブロードキャストアドレス：172.31.32.63
有効なホスト数：62

1-12.　10.10.10.225　255.255.255.252

ネットワークアドレス：10.10.10.224
ブロードキャストアドレス：10.10.10.227
有効なホスト数：2

1-13.　192.168.0.150　255.255.255.240

ネットワークアドレス：192.168.0.144
ブロードキャストアドレス：192.168.0.159
有効なホスト数：14

1-14.　10.10.10.110/27

ネットワークアドレス：10.10.10.96
ブロードキャストアドレス：10.10.10.127
有効なホスト数：30

1-15.　192.168.201.50/30

ネットワークアドレス：192.168.201.48
ブロードキャストアドレス：192.168.201.51
有効なホスト数：2

1-16.　10.10.10.17/26

ネットワークアドレス：10.10.10.0
ブロードキャストアドレス：10.10.10.63
有効なホスト数：62

1-17.　172.16.0.65/30

ネットワークアドレス：172.16.0.64
ブロードキャストアドレス：172.16.0.67
有効なホスト数：2

1-18.　192.168.0.129　255.255.255.224

ネットワークアドレス：192.168.0.128
ブロードキャストアドレス：192.168.0.159
有効なホスト数：30

1-19.　100.11.10.190/28

ネットワークアドレス：100.11.10.176
ブロードキャストアドレス：100.11.10.191
有効なホスト数：14

1-20.　10.10.10.129　255.255.255.248

ネットワークアドレス：10.10.10.128
ブロードキャストアドレス：10.10.10.135
有効なホスト数：6

1-21.　172.20.16.110/30

ネットワークアドレス：172.20.16.108
ブロードキャストアドレス：172.20.16.111
有効なホスト数：2

1-22.　192.168.201.60　255.255.255.240

ネットワークアドレス：192.168.201.48
ブロードキャストアドレス：192.168.201.63
有効なホスト数：14

1-23.　10.10.100.50/26

ネットワークアドレス：10.10.100.0
ブロードキャストアドレス：10.10.100.63
有効なホスト数：62

1-24.　172.18.62.92　255.255.255.224

ネットワークアドレス：172.18.62.64
ブロードキャストアドレス：172.18.62.95
有効なホスト数：30

1-25.　192.168.153.190/28

ネットワークアドレス：192.168.153.176
ブロードキャストアドレス：192.168.153.191
有効なホスト数：14

1-26.　192.168.17.17　255.255.255.248

ネットワークアドレス：192.168.17.16
ブロードキャストアドレス：192.168.17.23
有効なホスト数：6

1-27.　172.16.24.17/28

ネットワークアドレス：172.16.24.16
ブロードキャストアドレス：172.16.24.31
有効なホスト数：14

1-28.　192.168.0.150　255.255.255.224

ネットワークアドレス：192.168.0.128
ブロードキャストアドレス：192.168.0.159
有効なホスト数：30

1-29.　10.10.10.110　255.255.255.252

ネットワークアドレス：10.10.10.108
ブロードキャストアドレス：10.10.10.111
有効なホスト数：2

1-30.　172.16.16.17/26

ネットワークアドレス：172.16.16.0
ブロードキャストアドレス：172.16.16.63
有効なホスト数：62

1-31.　192.168.0.3　255.255.255.240

ネットワークアドレス：192.168.0.0
ブロードキャストアドレス：192.168.0.15
有効なホスト数：14

問題 2

2-1.　10.10.10.17　255.255.192.0

ネットワークアドレス：10.10.0.0
ブロードキャストアドレス：10.10.63.255

2-2.　10.10.100.50/22

ネットワークアドレス：10.10.100.0
ブロードキャストアドレス：10.10.103.255

2-3.　172.16.24.17/23

ネットワークアドレス：172.16.24.0
ブロードキャストアドレス：172.16.25.255

2-4.　172.16.16.17/22

ネットワークアドレス：172.16.16.0
ブロードキャストアドレス：172.16.19.255

2-5.　192.168.0.3　255.255.252.0

ネットワークアドレス：192.168.0.0
ブロードキャストアドレス：192.168.3.255

2-6.　10.10.10.17/20

ネットワークアドレス：10.10.0.0
ブロードキャストアドレス：10.10.15.255

2-7.　172.31.32.33/23

ネットワークアドレス：172.31.32.0
ブロードキャストアドレス：172.31.33.255

2-8.　10.10.10.225/18

ネットワークアドレス：10.10.0.0
ブロードキャストアドレス：10.10.63.255

2-9.　192.168.201.50　255.255.254.0

ネットワークアドレス：192.168.200.0
ブロードキャストアドレス：192.168.201.255

索引

索引

数字

アルファベット

索引

かな