10-A ネットワークの基本用語

10-A-1 通信の基礎

通信とは、物理的に離れた人やコンピュータ同士が情報をやり取りすることです。電話によって離れた人と会話をしたり、Webブラウザによりホームページを閲覧することができています。通信手段はさまざまですが、共通していることとして、通信を行うためには仕様や手順等の決まりが必要です。決まりがなければ通信は成り立ちません。この決まりのことを「プロトコル」と呼びます。

プロトコルは、協約、協定、規約といった意味です。通信では「通信規約」を意味します。通信を行うコンピュータ同士で、同じプロトコルを使用していれば、たとえ異なるベンダー（メーカー）のコンピュータであっても問題なく通信できます。

コンピュータによる通信が開始された当初は、ベンダー独自のプロトコルが使用されていましたが、プロトコル開発は非常に手間とコストがかかります。また、他社のシステムとの接続が多くなってきたという背景から、プロトコルの標準化作業が行われるようになりました。

OSI参照モデル

プロトコルの標準化作業は、「ISO」（International Organization for Standardization：国際標準化機構）や「CCITT」（Consultative Committee for International Telephony and Telegraphy：国際電信電話諮問委員会（ITU：International Telecommunication Union）の前身）によって進められました。この結果、策定されたのが、「OSI参照モデル」（Open Systems Interconnection：開放型システム間相互接続）です。OSI参照モデルはさまざまなベンダーから提供されたコンピュータ間で通信を実現するための仕組みを取り決めているものです。

OSI参照モデルを使用するメリットは、以下の通りです。

- マルチベンダー環境で通信が可能
- それぞれの層が独立して機能することにより、各層単位での開発や拡張が用意

OSI参照モデルでは、通信機能を7つの階層に分けて表現しています。各層の基本的な役割を以下に示します。

表10-A-1 OSI参照モデルの7つの階層

層	説明
アプリケーション層	ユーザアプリケーションにネットワークサービスを提供する
プレゼンテーション層	通信するうえで異なる情報の表現形式を共通の転送形式に変換する
セッション層	伝送するデータの形式に合わせて、通信形態を決定する
トランスポート層	データの分割と再組み立てを行う
ネットワーク層	通信相手とどのような経路でデータをやり取りするのか、経路の決定を行う
データリンク層	媒体を通して物理的な伝送を提供する。この層では、隣接したデバイス間での通信を制御する
物理層	電圧、コネクタの形状、大きさ、ピン配列、電気信号のタイミング等を規定する

OSI参照モデルとTCP/IP

TCP/IPは、米国国防総省が中心となって1982年に開発され、1983年に米国国防総省の標準プロトコル群として規定されました。その後、Unixマシンに組み込まれ、多機能でありながら、使いやすいことから広く普及し、現在ではインターネットにおいて事実上の標準プロトコルとなっています。OSIも国際標準のプロトコルとして認知されていますが、TCP/IPはインターネット等で直接利用しているものでもあり、より身近に感じられるプロトコルです。

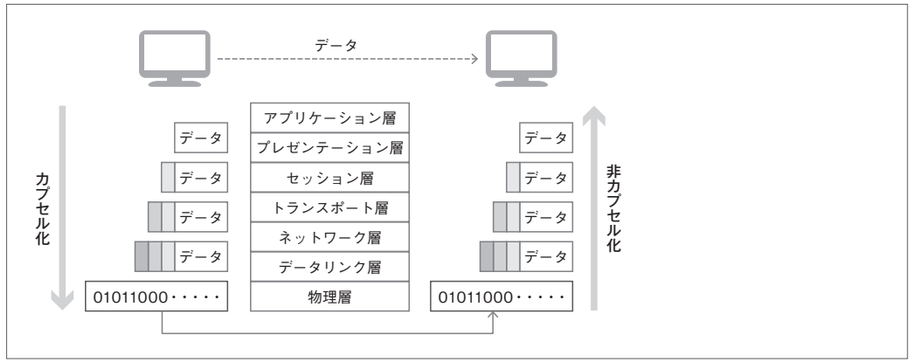
表10-A-2 OSI参照モデルとTCP/IP

OSI参照モデル		TCP/IP	
7層	アプリケーション層	アプリケーション層	HTTP、FTP、SMTP、DNS、…
6層	プレゼンテーション層		
5層	セッション層		
4層	トランスポート層	トランスポート層	TCP、UDP、…
3層	ネットワーク層	インターネット層	IP、ICMP、ARP、…
2層	データリンク層	ネットワーク インターフェイス層	Ethernet、PPP、…
1層	物理層		

データのカプセル化/非カプセル化

実際にコンピュータ同士が通信を行う場合に、どのような処理が行われていくか確認します。

図10-A-1 カプセル化/非カプセル化



Webブラウザ等のクライアントソフトウェアは、サーバに処理要求を送信する場合、自分が送りたいデータの他に、アプリケーション層のプロトコルに準拠した制御情報をデータの先頭に付加してOSにデータを渡します。OSには、TCP/UDPとIPの機能が組み込まれているので、レイヤ毎の制御情報を付加してハードウェアに渡します。ハードウェアでは、ネットワークインターフェイス層で必要な制御情報を付加して、ケーブルに電気信号を送信します。

このように、送信側のコンピュータではアプリケーションが宛先に送るデータを作成し、そのデ

ータが通信機能に渡されます。その後、OSIの各層で以下の処理が行われます。

①上位層からデータを受け取る
②その層で使用するヘッダ（制御情報）を付加する
③ヘッダ＋上位層データを下位層に渡す

データにヘッダ情報を付加しながら何重にも包み込んでいくため、送信時の処理を「カプセル化」と呼びます。
また、データを受信したコンピュータでは、以下の処理が行われます。

①下位層からデータを受け取る
②その層で使用するヘッダを読み取る
③ヘッダを取り除き、残りのデータを上位層に渡す

データ送信時とは逆に、ヘッダを次々に取り除いていくため、受信時の処理を「非カプセル化」と呼びます。
なお、このカプセル化と非カプセル化の処理で、各層が扱うデータの単位を「PDU」（Protocol Data Unit）と呼びます。PDUは基本的に「ヘッダ情報＋上位層データ」を表し、下位4層のPDUは以下のように呼ばれます。

表10-A-3　下位4層のPDU

層	呼び名
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

通信のタイプ

通信は1対1の他、複数のタイプがあります。主な通信のタイプは以下の通りです。

▷ユニキャスト
1台のコンピュータを指定してデータを通信するタイプです。通常のコンピュータ通信は、ユニキャストがほとんどです。

▷マルチキャスト
複数台の端末から成るグループを指定してデータを通信するタイプです。マルチキャストは動画配信等に使用されます。

▷ブロードキャスト
同じネットワークに属する全コンピュータ宛てにデータを通信するタイプです。ブロードキャストは、コンピュータ自身が自分の存在をネットワークの他のコンピュータに通知したり、情報の検索等に使用されることが多いです。

図10-A-2　ユニキャスト

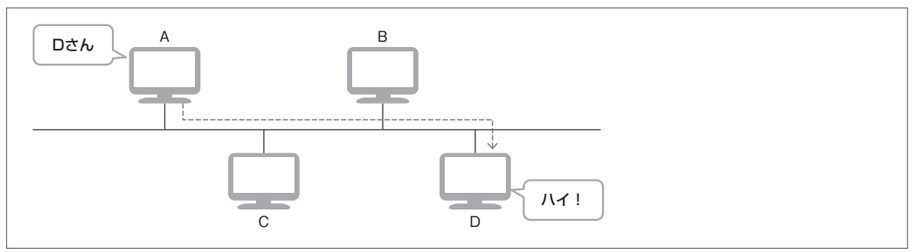


図10-A-3　マルチキャスト

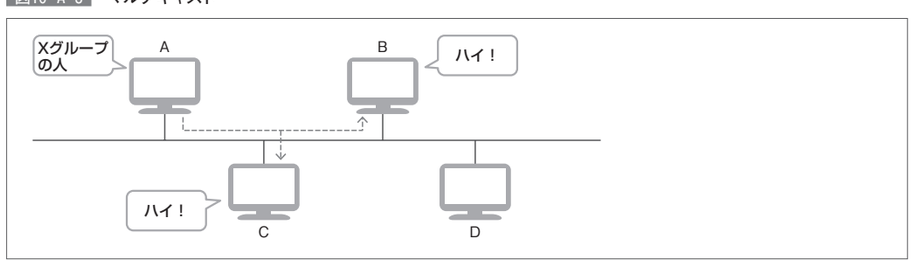
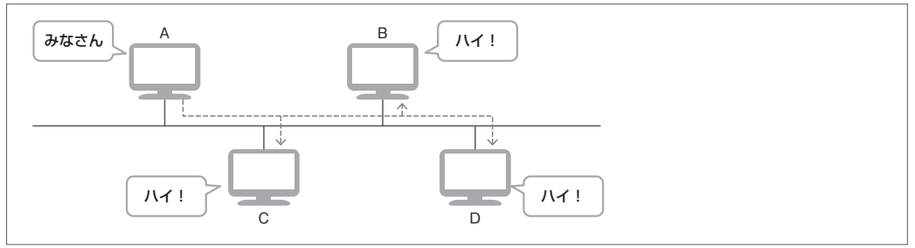


図10-A-4　ブロードキャスト



ネットワークの種類と特徴

ネットワークには、さまざまな種類があります。そのなかから、LAN、WAN、インターネット、イントラネットについて説明します。

▷LAN（Local Area Network）
限られた敷地内で作られたネットワークのことです。つまり、オフィス、学校、家庭のネットワークがLANとなります。

▷WAN（Wide Area Network）
離れた地域にあるLANとLANを接続するネットワークのことで、ISP（Internet Service Provider）の通信ケーブル等を利用して構築されます。ISPのことを、通信事業者やキャリアと呼ぶこともあります。

▷インターネット

誰でも自由に参加することができるオープンなネットワークです。ISPを経由することで接続します。そしてISP同士が繋がることによって、世界中に広がる大きなネットワークになっています。

▷イントラネット

企業内のネットワークのことで、インターネットの対称語として使われます。したがって限られた人しかアクセスできません。また、LANだけでなく、拠点間を結ぶWANでも構成されています。

10-A-2 LAN（Local Area Network）

LANは前述の通り、ある特定の建物や敷地内のネットワークを指します。このようなネットワークは、自営のネットワークなので、LANの敷地内ではISPは関連しません。このため、LANの運営やネットワークポリシー（運営方針）は全てLAN管理者の責任範囲となります。

同軸ケーブルや光ファイバー等の通信ケーブルで端末を接続するものを「有線LAN」（wired LAN）、無線通信で接続するものを「無線LAN」（wireless LAN）と呼びます。そして、有線LANの通信方式としては「Ethernet」（イーサネット/IEEE 802.3）系諸規格が、無線LANの通信方式としては「Wi-Fi」（ワイファイ/IEEE 802.11）系諸規格がそれぞれ標準として普及しています。

イーサネット

イーサネットは有線のLANで最も使用されている技術規格です。主に、OSI参照モデル（➡ p.1）の下位2つの層である物理層とデータリンク層に関して規定しています。

データリンク層では、扱うデータの単位を「フレーム」と呼びます。フレームの構成は以下の通りです。

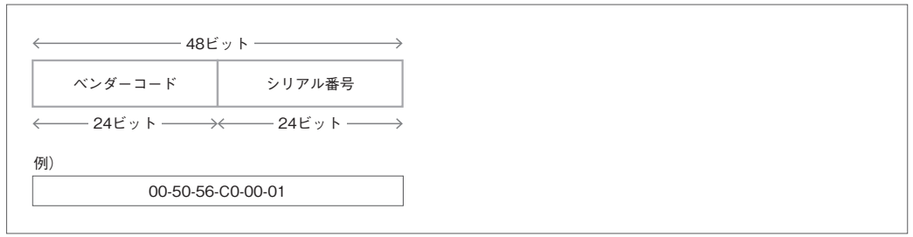
図10-A-5　フレームの構成

表10-A-4　フレームのフィールド

フィールド	説明
宛先MACアドレス	フレームの宛先となる機器のMACアドレスが格納
送信元MACアドレス	フレームの送信元となる機器のMACアドレスが格納
タイプ	上位層のプロトコルを識別するための番号が格納
データ	上位層のヘッダとユーザデータが格納
FCS	フレームエラーを検出するためのフィールド

MACアドレス（Media Access Controlアドレス）は、NIC（Network Interface Card）毎に割り当てられる固有のアドレスです。MACアドレスは全長が48ビットのアドレスであり、上位24ビットはベンダーコード、下位24ビットはベンダー内のシリアル番号が割り当てられています。

図10-A-6　MACアドレス



MACアドレスは機器（端末）を識別するためのアドレスであり、ネットワークの構成には依存しない物理アドレスです。

10-A-3 IPv4/IPv6

IP（Internet Protocol）はインターネットおよびローカルネットワークでのホスト間の通信プロトコルです。IPにより異なったネットワーク上にあるホスト間での通信を行うことができます。

現在広く使われているのが「IPv4」（Internet Protocol version 4）で、32ビットのIPアドレスを持ちます。その後継として普及しつつある「IPv6」（InternetProtocol version 6）は128ビットのIPアドレスを持ちます。

IPv4の32ビットのIPアドレスは、ネットワーク部とホスト部から構成されます。ネットワーク部とホスト部の構成により次のA、B、C、Dのクラスがあります。IPアドレスは1バイト毎に「.」で区切って10進数で表記します。

表10-A-5　ネットワークのクラス

クラス	アドレス	ネットワーク部（N）とホスト部（H）の構成	備考
A	0.0.0.0 - 127.255.255.255	N.H.H.H	ネットワーク部1バイト、ホスト部3バイトの大規模ネットワーク
B	128.0.0.0 - 191.255.255.255	N.N.H.H	ネットワーク部2バイト、ホスト部2バイトの中規模ネットワーク
C	192.0.0.0 - 223.255.255.255	N.N.N.H	ネットワーク部3バイト、ホスト部1バイトの小規模ネットワーク
D	224.0.0.0 - 239.255.255.255	-	マルチキャスト用
E	240.0.0.0 - 255.255.255.255	-	予約

1バイト目の値でクラスを分類します。以下はアドレスの例です。

- **Aクラスの例**：10.0.0.1（1バイト目の値が0-127の範囲内なのでAクラス）
- **Bクラスの例**：172.16.0.1（1バイト目の値が128-191の範囲内なのでBクラス）
- **Cクラスの例**：192.168.1.1（1バイト目の値が192-223の範囲内なのでCクラス）

しかし、IPアドレスのクラスを使用すると、アドレスに無駄が生じることがあります。したがって、ホスト部の一部を「サブネットワーク」として扱うことで、1つのネットワークをさらに細かな

ネットワークに分割し、ホスト部を小さくすることができます。

この時、どこまでをネットワーク部とするかを指定するのが「ネットマスク」です。ネットマスクは10進数あるいは16進数で表記します。また、ネットワーク部はプレフィックスで表すこともできます。プレフィックスはIPアドレスの後ろに「/ネットワーク部のビット数」を指定します。

以下は、Bクラスのネットワークを、3バイト目までをネットワーク部とするサブネットに分割する例です。

表10-A-6　**サブネット化**

	1バイト目（ネットワーク部）	2バイト目（ネットワーク部）	3バイト目（ホスト部）	4バイト目（ホスト部）	プレフィックス
IPアドレス1	172	16	1	1	/16
IPアドレス2	172	16	2	1	/16
ネットマスク	255	255	0	0	
	↑❶	↑❶	↑❷	↑❷	

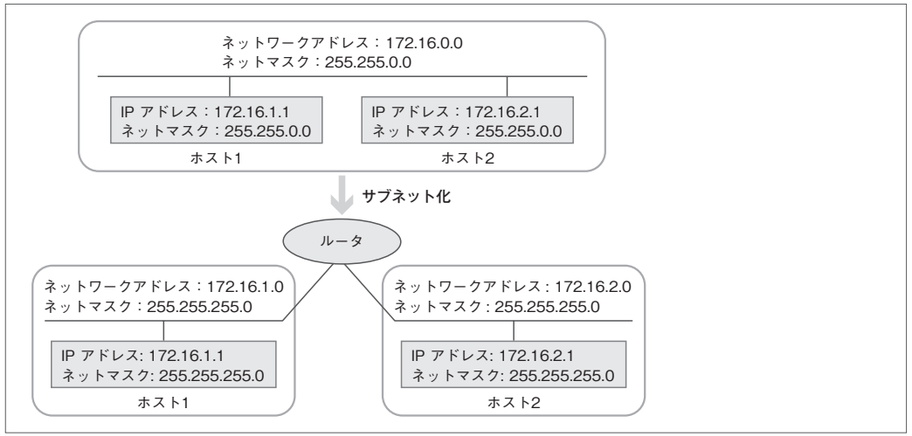
上記をサブネット化した例

	1バイト目（ネットワーク部）	2バイト目（ネットワーク部）	3バイト目（ホスト部）	4バイト目（ホスト部）	プレフィックス
IPアドレス1	172	16	1	1	/24
IPアドレス2	172	16	2	1	/24
ネットマスク	255	255	255	0	
	↑❶	↑❶	↑❸	↑❷	

❶ネットワーク部のビットは「1」。オールビット1なので「255」
❷ホスト部は「0」
❸このバイトをネットワーク部で使用。オールビット1なので「255」

サブネット化することで、ネットワークのトラフィックが分散し、管理単位も小さくなります（図10-A-7）。

図10-A-7　**サブネット化**



ネットマスクあるいはプレフィックスはビット単位で設定できます。例えば、表10-A-7のようなIPアドレスの構成があったとします。

表10-A-7　**IPアドレス32ビットの構成**

ネットワーク	ホスト部
26ビット	6ビット

32ビット～26ビット（ネットワーク部）でホスト部は6ビットになります。2の6乗＝64で64個のホストアドレスが使えます。ただし、ホスト部の全てのビットが「0」のアドレスはネットワーク自身を表すアドレス、ホスト部の全てのビットが「1」のアドレスはネットワーク内の全てのホストを宛先とするブロードキャストアドレスとして使用されます。

この2つのアドレスはホストアドレスとして使用できないため、残りの個数は64－2＝62ですが、さらにルータ分を1つ引くと61個となります。

同一ネットワーク上にあるホストのMACアドレスは、相手ホストのIPアドレスを指定したARPブロードキャストにより取得します。ネットマスクにより異なったネットワーク上にあると判定された相手ホストの場合は、ルータのIPアドレスを指定したARPブロードキャストによりルータのMACアドレスを取得します。

プライベートアドレス

プライベートアドレスとは、ファイアウォール内部（組織の内部ネットワーク）で使うアドレスのことです。それに対して、インターネット上で使うのがグローバルアドレスです。

プライベートアドレスはIANAによって予約され、RFC1918で以下の通り規定されています。

表10-A-8　**プライベートアドレス**

クラス	アドレス
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

グローバルアドレスは、NIC（Network Information Center）によって管理される重複のないアドレスですが、プライベートアドレスは内部ネットワークで自由に割り当てて使うことができます。内部ネットワークからインターネットに出ていく時は、プライベートアドレスはグローバルアドレスに変換され、インターネットから内部ネットワークに入ってくる時は、グローバルアドレスからプライベートアドレスに変換されます。

IANA（Internet Assigned Numbers Authority）はインターネットプロトコルに関連した番号やシンボルの割り当てを管理している組織です。プライベートアドレスや「WELL KNOWN PORT NUMBERS」と呼ばれるサービスに対応して予約されたポート番号の割り当て等を行っています。IANAについてはRFC1700で記述されています。

IPv6

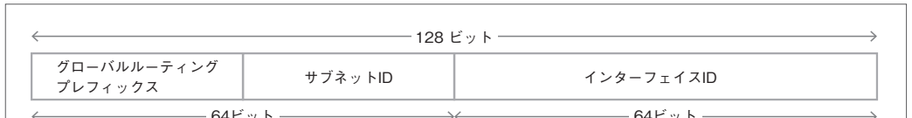
IPv6は、インターネットの普及に伴うIPv4の32ビットアドレスの不足を解決するために開発された、128ビットのアドレス空間を持つプロトコルです。Linuxカーネルは2.2からIPv6に対応しています。またDNS、メール、Web等の主要なネットワークアプリケーションの多くもIPv6に対応しています。

IPv6のアドレスには複数の種類とスコープ（有効範囲）があり、通常はグローバルユニキャストアドレス（GUA）とリンクローカルアドレス（LLA）が使われます。グローバルユニキャストアドレスはインターネット上で使用するアドレスです。リンクローカルアドレスは同一リンク上でのみ有効なアドレスです。

また2005年には、RFC4193によりIPv4のプライベートアドレスに相当する、サイト内で使用するローカルなアドレスとして、ユニークローカルユニキャストアドレス（ULA）が定義されました。アドレス中に一部ランダムな値を取り入れることで、他サイトのULAとのアドレス重複を回避するよう意図されています。

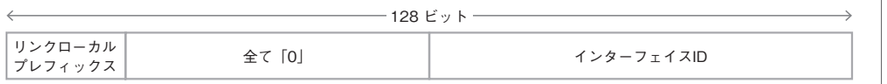
アドレスフォーマットは、GUAはRFC3587、LLAはRFC4291、ULAはRFC4193にて、それぞれ次のように規定されています。

図10-A-8　IPv6アドレスフォーマット（グローバルユニキャストアドレス）



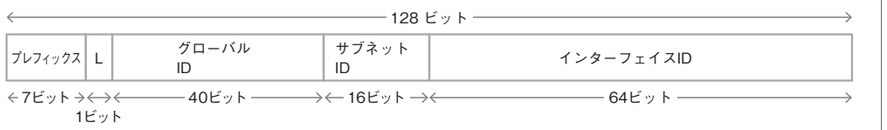
先頭の3ビットが「001」、プレフィックスは「2000::/3」

図10-A-9　IPv6アドレスフォーマット（リンクローカルアドレス）



先頭の10ビットが「1111111010」、その後の54 ビットが「0」
プレフィックスは「fe80::/64」

図10-A-10　IPv6アドレスフォーマット（ユニークローカルユニキャストアドレス）



先頭の7 ビットが「1111110」、プレフィックスは「fc00/7」
続く1ビット（L）が「1」→ローカルに定義、「0」→未定義（将来用）
グローバルID は乱数で生成

64ビットのインターフェイスIDはIPv4のホスト部に該当します。インターフェイスIDは、イーサネットの場合は通常、48ビットのイーサネットアドレスから64ビットのインターフェイスIDを生成します。

IPv6のアドレスは128ビットを16ビット毎にコロン「:」で区切り、8つのフィールドに分けて16進数で表記します。次の場合は表記の省略ができます。

- フィールドの先頭に0が連続する場合は省略できる
  例）0225→225
- 0のみが連続するフィールドで全体で一箇所だけ「::」と省略できる
  例）fe80:0000:0000:0000:0225:64ff:fe49:ee2f→fe80::225:64ff:fe49:ee2f

ISPからはGUA（グローバルユニキャストアドレス）が割り当てられます。例えば、ISPから割り当てられたIPv6アドレスが「2001:db8:0:100::/56」の場合、割り当てられたサブネットの個数は「64-56=8」で8ビット分の2^8=256個となります。

サブネットアドレスは「2001:db8:0:100::/64」から「2001:db8:0:1ff::/64」までとなります。ネットワークのトラフィックやホストの管理等の問題を別にすれば、論理的には各サブネットごとに2^64個のホストを接続できます。

JPNIC（日本ネットワークインフォメーションセンター）では、ISPからエンドユーザへのIPv6割り当てアドレス空間のサイズとして、最小/64、最大/48をポリシーとしています。

> **JPNIC（日本ネットワークインフォメーションセンター）**
> **https://www.nic.ad.jp/doc/jpnic-01167.html**

ISPでは、/48、/56、/64をユーザへの選択肢として提供し、/56を標準としているところが多いようです。したがって、IPv4のように内部サブネットをプライベートアドレスで構成し、それをNAT（Network Address Translation）によって、インターネットに接続するという形態はIPv6では通常は必要なくなります。

ただし、インターネットと内部ネットワーク間にファイアウォールを構築し、内部ネットワークへのトラフィックを制限する必要があります。また、GUAによる1個のサブネットと、ULAによる複数の内部ネットワークを、NATによって接続することも可能です。

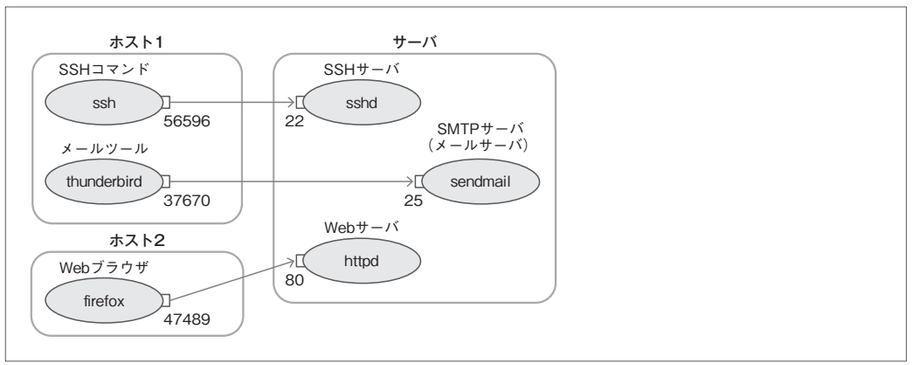
10-A-4 TCP/UDP/ポート番号

ネットワークを介したプロセス間の通信は、プロセスが生成したTCPポートあるいはUDPポート同士を接続することにより行われます。

サーバ（プロセス）は、提供するサービス毎に決められているTCPポートあるいはUDPポートの番号のポートを生成して、クライアントからのリクエストを受け付けます。

サービスを受けるクライアント（プロセス）は、サービスを提供するサーバ（プロセス）が待ち受けているTCPポートあるいはUDPポートの番号を指定してリクエストを送信します。

図10-A-11　ポートの概要



クライアント側のポート番号は、OSにより空きポート番号が自動的に割り当てられます。Linuxでは、/etc/servicesファイルにはサービス名とポート番号の対応が記述されています。なお、ポート番号の範囲は0から65535です。

よく使われるサービス名とポート番号は、「Well Known Ports」と呼ばれ、RFC1700で規定された0～1023番の範囲のポートを使用します。また、「System Ports」とも呼ばれ、特権ユーザのみアクセス可能とされています。

「Registered Ports」はRFC1700に掲載されている1024～49151番の範囲のポートで、IANAによってサービスに対応するポート番号がコミュニティの便宜に供する目的で掲載されています。ただし「Well Known Ports」と異なり、IANAがポート番号の割り当てを管理しているわけではありません。

TCPとUDP

IPと共に使用されるIPの上位のプロトコルには、TCP（Transmission Control Protocol）とUDP（User Datagram Protocol）があります。

TCPの特徴は、次の通りです。

・コネクションを確立し、確立した通信路で転送を行う（コネクション型）
・受信側でパケットの喪失を検知すると、送信側は喪失パケットの再送を行う
・受信パケットを正しい順番で並べ替える（パケットのシーケンス制御）
・受信データのエラー訂正機能がある
・上記の機能のためのオーバーヘッドが生じる

UDPの特徴は、次の通りです。

・コネクションを確立しない（コネクションレス型）
・TCPのような、喪失パケットの再送、シーケンス制御、エラー訂正機能はない
・上記によりオーバーヘッドがない

代表的なプロトコル

アプリケーション層は、ユーザに対してネットワークを利用したサービスを提供するためのインターフェースとして機能します。アプリケーション層のプロトコルにはさまざまなものがあります。

▷FTP

FTP（File Transfer Protocol）は、ファイルを転送するためのプロトコルです。FTPは制御用に21番、データ転送用に20番のポートを使用します。

FTPの詳細は、本書の「13-5 FTPサーバ、TFTPサーバ」を参照してください。

▷SMTP/POP/IMAP

SMTP（Simple Mail Transfer Protocol）は、電子メールを送信するプロトコルです。ユーザは電子メールを送信する際、メールサーバに向けてメールを送信します。メールサーバは、電子メール内の宛先アドレスをもとに宛先ユーザが利用しているメールサーバに電子メールを届けます。

宛先のユーザはいつでも自分が利用しているサーバにアクセスし、電子メールを受信することができます。なお、ユーザがメールサーバにアクセスして電子メールを受信する場合には、POP（Post Office Protocol）やIMAP（Internet Message Access Protocol）を使用します。

SMTP/POP/IMAPの詳細は、本書の「13-6 メールサーバ」を参照してください。

▷HTTP

HTTP（Hypertext Transfer Protocol）は、ブラウザでWebサーバにアクセスしてホームページを参照する際に使用します。HTTPは、クライアント（例：Webブラウザ）がサーバ（例：Webサーバ）にリクエスト（要求）を送信します。サーバはこれにレスポンス（応答）を返し、通信は終了します。

HTTPの詳細は、本書の「13-2 Webサーバ」を参照してください。

▷DHCP

DHCP（Dynamic Host Configuration Protocol）は、IPアドレス、サブネットマスク、デフォルトゲートウェイ等のネットワークの設定情報を自動的に設定するプロトコルです。このサービスを提供するDHCPサーバを使用するクライアントは、ネットワークに接続するだけで、必要な設定情報を自動的に取得することができます。

DHCPの詳細は、本書の「14-4 DHCPサーバ」を参照してください。