■3 群（コンピュータネットワーク）- 3 編（ネットワーク層）

1 章 IP

【本章の構成】

本章では，IP 技術（3-1 節），IPv6 技術（3-2 節），IGP（Interior Gateway Protocol）（3-3 節），EGP（Exterior Gateway Protocol）（3-4 節），IP Multicast（3-5 節），Multicast Routing（3-6 節）について述べる．

■3 群 - 3 編 - 1 章

1-1 IP

（執筆者：石田賢治）

1-1-1 IP 技術の背景

Internet Protocol は，略して IP と呼ばれることが多い．この IP を中心とする様々な技術が，IP 技術である．IP 技術の基礎となるパケット交換の概念は，1960 年初めに米国の RAND Corporation の Paul Baran によって提案された[1), 2)]．当初，Baran は，パケットのことをメッセージブロックと呼んでいた．ほぼ同時期の 1965 年頃，英国国立物理学研究所（NPL: National Physical Laboratory）の Donald W. Davies は，Baran とは独立に同じ基本概念を考案した．Davies は，メッセージの断片を表すためにパケットという用語を用いた．このパケットという用語は，それ以降定着し今日においても使われている．1969 年には，パケット交換方式のコンピュータネットワークである ARPANET が運用され始めた．ARPANET は，現在のインターネットの元となったネットワークである．1981 年には，プロトコルである IP（Internet Protocol）が，アメリカ国防総省 (DoD: Department of Defense) の標準インターネットプロトコル[3)]に規定され，ARPANET やその後のインターネットでも用いられるようになり，現在に至っている．

代表的なプロトコル体系として，インターネットプロトコル体系と開放型システム間相互接続（Open System Interconnection）がある．インターネットプロトコル体系は，IETF（Internet Engineering Task Force）における多くの RFC（Request for Comments）として規程されている．一方，開放型システム間相互接続は，OSI 参照モデルとも呼ばれ，ISO（国際標準化機構）と ITU-T（国際電気通信連合電気通信標準化部門）により規程されたものである．一方，インターネットプロトコル体系（インターネットプロトコルスイート）[4)]は，上位層からアプリケーション層，トランスポート層，インターネット層，リンク層の４階層と規程されている．最下位のリンク層は詳細に説明されることが少なく，自由度の大きなものとなっている．これらは，多くのプロトコルから構成されるが，TCP と IP は，代表的なプロトコルである．この体系において，TCP はトランスポート層に，IP はインターネット層に属する（図 1･1 参照）．TCP/IP は，TCP と IP の二つのプロトコルを指す場合もあるが，IP を利用する複数のプロトコルの総称を意味することもある．1974 年には，初期の TCP/IP のモデル[5)]が発表されている．また，1980 年代にはその概要[6)]や設計哲学[7)]もまとめられている．

インターネットプロトコル体系におけるアプリケーション層やトランスポート層のプロトコルは，データを送信元から送信先に運ぶために下位層のプロトコルとして，常に IP を利用する．そこで，Everything over IP と呼ばれる．また，IP が動作するプロトコル階層より下では，有線や無線 LAN などに関する数々のプロトコルが動作する．これは，IP over Everything と呼ばれる．そのため，IP の位置づけを砂時計モデル（hourglass model）に対応付ける場合もある．IP は砂時計のくびれた部分に相当する．つまり，IP はこの体系の要である．また，インターネットをはじめとする多くの情報通信システムで用いられており，現在，インターネットプロトコル体系は事実上の標準となっている．

一方，OSI 参照モデルは，上から，アプリケーション層，プレゼンテーション層，セッション層，トランスポート層，ネットワーク層，データリンク層，物理層となっている．インター

ネットプロトコル体系の階層モデルと OSI 参照モデルは若干異なる．しかしながら，インターネットプロトコル体系のインターネット層は機能的に OSI 参照モデルのネットワーク層によく似ている．例えば，OSI 参照モデルのネットワーク層に属する CLNP（Connectionless Network Protocol）は，基本的に IP とほぼ同等な機能をもつ．そのため，プロトコルが動作する階層を正確かつ簡潔に表したり，プロトコルの動作や階層構造の理解を助ける上で有用なため，IP をこのネットワーク層に位置づけたり[8) 9)]，対応付けて整理されること[10) 11) 12) 13) 14)]がある．ここでも，インターネット層を OSI 参照モデルのネットワーク層に対応付けて説明する．このネットワーク層の機能は，送信元からネットワーク的に接続してはいるが直接接続されていない送信先に対し，IP パケットを配送することである．このため，送信元と送信先間の経路を決定する経路制御（ルーチング）が，ネットワーク層における最も重要な課題となる．

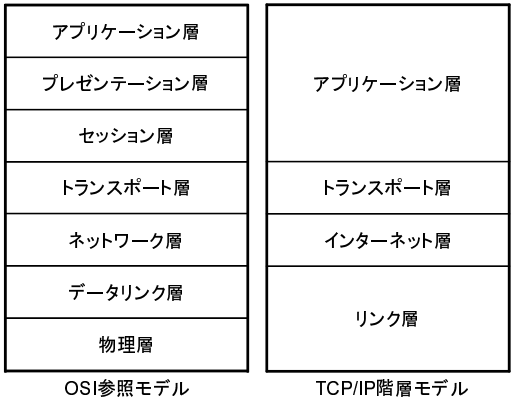

図 1･1　OSI 参照モデルと TCP/IP の階層モデル

1-1-2 コネクションレス型転送と最善努力方式

IP は，コネクションレス型のパケット伝送プロトコルである．つまり，送信元は送信先に対し，データ送信に先立ってコネクションを確立せず，一連のデータ転送後にコネクションの開放も行わない．データの送信要求が生じると直ちに，送信先に対しデータを送信する．このため，パケットが途中で失われたり，送信した順序と受信した順序が異なることもあり得る．信頼性は，必要に応じて，IP が動作する層より上のトランスポート層以上で確保される．このように，IP はパケットを送信先まで送り届けようと熱心に努力はするものの，実際に届いたか否かの確認はせずパケット配送の保証はしない．そのため，最善努力方式（Best Effort Delivery）あるいはベストエフォート方式と呼ばれる．

1-1-3 IP の機能

ネットワーク層の主な目的は，送信元から送信先に IP データグラム*を送り届けることである．この送信元と送信先との通信は，エンドツーエンド間の通信と呼ばれる．ネットワーク層の下に位置するデータリンク層は，直接接続された機器間の通信を提供する．ネットワーク層の IP はネットワーク的には連結であるが直接的には繋がっていない機器間に対し通信サービスを提供する．

この目的達成のため，ネットワーク層では，三つの機能が提供される．第 1 は，アドレス付け（addressing）である．アドレス付けにより，送信元，送信先，途中のルータの識別が可能となる．このネットワーク層レベルの識別子を IP アドレスという．また，このようなアドレス付けに基づく IP データグラムのフォーマットが規程されており，ネットワーク層内で動作するプロトコルにより利用される．ネットワーク層（インターネット層）で利用される標準プロトコル[4]として，IP，ICMP (Internet Control Message Protocol)[15]，IGMP (Internet Group Management Protocol) [16]がある．第 2 は，経路制御（ルーチング）である．経路制御とは，あるネットワークとそのネットワーク上の送信元と送信先が与えられたとき，その間の経路を選択することである．第 3 は，IP データグラムの分割（Fragmentation）と再構築（Reassembly）である．ネットワーク層より下位の層で具体的に利用されるデータリンクの種類ごとに，データの最大転送単位（MTU: Maximum Transmission Unit）は異なる．このため，利用するデータリンクの種類によっては，IP データグラムのサイズがこの MTU を越える場合があり，必要に応じて IP データグラムをより細かに分割して転送する必要がある．

以降，1-1-4 では，第 1 の機能であるアドレス付けについて述べる．次に，1-1-5 で，ネットワーク層（インターネット層）の標準プロトコルについて説明する．次に，1-1-6 で，第 2 の機能であるルーチングについて簡単にまとめる．ルーチングの詳しい説明は 3 章以降で行われる．最後に，1-1-7 で，第 3 の機能である IP データグラムの分割と再構築について述べる．

1-1-4 IP アドレス

IP アドレスは，インターネット上のホストを一意に識別するためのアドレスであり，IPv4（IP version 4）は，4 オクテット（32 ビット）* の固定長の識別子を持つ．これは，8 ビットごとに 10 進数で表されドットで区切られている．例えば，202.12.30.30 のように記述される．構造的には，インターネット内におけるネットワークを表すネットワーク部とそのネットワーク内に存在するホストを表すホスト部よりなる．原則的に，経路制御には IP アドレスのネットワーク部が利用される．これを意識した記法として，IP アドレスの後ろに「/」を付けて，先頭から何ビット目までネットワークアドレス（ネットワーク部）であるかを示すプレフィックス表記がある．例えば，202.12.30.30/24 のように記述される．また，この記法では最後の 0 を省略可能であり，165.242.0.0/16 は 165.242/16 と記述可能である．

IP アドレスは，先頭から 4 ビット目までのパターンにより，クラスA，B，C，D，Eのに分類される．このように分類されたアドレスをクラスフル（Classfull）ともいう．しかし

* IP（Internet Protocol）で送信されるデータの一塊を表す．一方，パケットはより広範囲で利用される用語である．

* 1 オクテットは 8 ビットを表す．1 バイトが 8 ビット以外を表すこともあるため，オクテットが使われる．

ながら，クラスフルなアドレス割当の非効率性が認識されるようになった．このような背景により，IP アドレスの利用効率を上げるために，いくつかの技術が導入されている．

（1）クラスフルなアドレス割当

IP アドレスの当初の割当法である．後に，クラスレスなアドレス割当法が出て来たので区別するために，クラスフルなアドレス割当と呼ばれることもある．図 1･2 に，クラスフルな IP アドレスのフォーマットを示す．

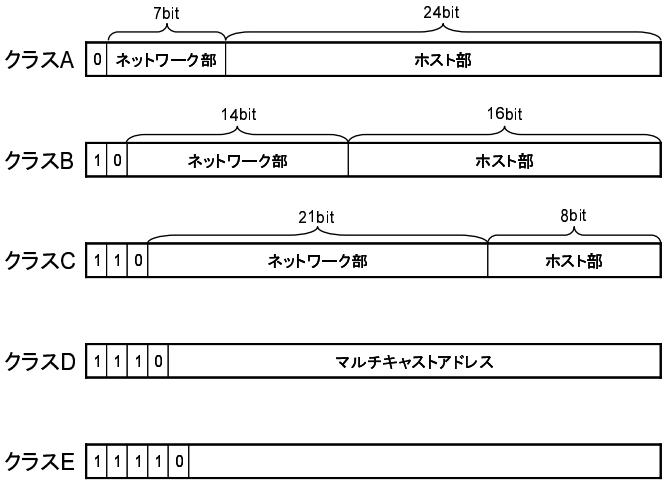

図 1･2　IP アドレスのフォーマット

クラス A は，IP アドレスの先頭 1 ビットが 0 である．同時に，これがクラス A の識別子となっている．クラス A の識別子 0 を除く，先頭 7 ビットでネットワークを表し，残りの 24 ビットで，そのネットワーク内のホストを表す．プレフィックス長（ネットワーク部の長さ）は 8 オクテットである．2^7=128 であるが，識別子 0 以降が全て 0 の $(00000000)_2 = (0)_{10}$ と識別子 0 以降が全て 1 の $(01111111)_2=(127)_{10}$ は，特別な意味を持つため，クラス A として割当可能なネットワーク数は，126（128-2）個である．また，ホスト部に関しては，2^{24}=16777216 であるが，全て 0 と全て 1 は特別な意味を持つため，ホストアドレスとして割当可能な数は，16777214（16777216-2）個である．

クラス B は，IP アドレスの先頭 2 ビットが 10 である．同時に，これがクラス B の識別子となっている．クラス B の識別子 10 を除く，先頭 14 ビットでネットワークを表し，残りの 16 ビットで，そのネットワーク内のホストを表す．プレフィックス長は 16 オクテットである．2^{14}-2=16382 のため，クラス B として割当可能なネットワーク数は，16382 個である．また，2^{16}-2=65534 のため，ホストアドレスとして割当可能な数は，65534 個である．

クラス C は，IP アドレスの先頭 3 ビットが 110 である．同時に，これがクラス C の識別子となっている．クラス C の識別子 110 を除く，先頭 21 ビットでネットワークを表し，残

りの 8 ビットで，そのネットワーク内のホストを表す．プレフィックス長は 24 オクテットである．2^{21}-2=2097150 のため，クラス C として割当可能なネットワーク数は，2097150 個である．また，2^{8}-2=254 のため，ホストアドレスとして割当可能な数は，254 個である．

クラス D は，IP アドレスの先頭 4 ビットが 1110 である．同時に，これがクラス D の識別子となっている．クラス D の識別子 1110 を除く，28 ビット全てがネットワーク部となる．また，ホストアドレスの部分はない．この 28 ビットは，IP マルチキャストで使われるアドレスである．

クラス E は，先頭 5 ビットが 11110 である．同時に，これがクラス E の識別子となっている．クラス E のアドレスは，実験目的のため予約されており割当てられていない．

1990 年代の始めまで，A，B，C のクラス単位で IP アドレスの割当が，各組織において行われていたが，以下の三つの問題が認識されるようになった．

（I）クラス B のアドレス空間の枯渇

組織が IP アドレスの割当を受けようとするとき，254 台のホストしか収容できないクラス C では不十分であり，多くの組織がクラス B の割当を望むようになった．その結果，クラス B のアドレス空間の枯渇が問題になってきた．また，割当てられたクラス B において収容可能な 65534 個のホストアドレスが十分利用されないこともあり，アドレス利用の非効率性が認識されるに至った．

（II）ルーチング表に含まれるエントリ数の増大とルーチング表更新メッセージ量の増大

IP データグラムを転送するホストやルータは，経路制御を行うため送信先への経路情報を含むルーチング表を持つ．また，ルーチング表はネットワークの状況に応じて動的に書き換えられる．多くの組織への IP アドレスの割当に従い経路情報は増え，結果としてそれらの経路に対応するデータを含むルーチング表は巨大化していった．加えて，IP アドレスの割当が当初地理的に行われなかったため，経路情報の集約が困難になったこともルーチング表の巨大化を促進した．結果として，ルーチング表自身のエントリ数の増加，および，ルーチング表を更新するメッセージの増大が大きな問題*になってきた．

（III）IP アドレスの枯渇の問題

インターネットに接続されるホスト数の爆発的な増加により，この 32 ビットのアドレス空間自体が枯渇する可能性が出てきた．一例として図 1･3 に，最近のホスト数の統計データ推移[17]を示す．

これらの問題に対処する技術として，地理に依存したアドレス割当の導入，組織内で閉じて使用されるプライベートアドレス（private address）[18]の導入や CIDR (Classless Inter–Domain Routing)[19]などがある．

まず，プライベートアドレスについて説明する．機器に対し全世界で一意に割付けられる IP アドレスのことをグローバルアドレス（global address）という．一方，プライベートな組織内で自由に利用可能な IP アドレスをプライベートアドレスという．このアドレスを持つホストは，そのままではインターネットへのアクセスが†できない．そこで，インターネットへ接続するためには，外部へのアクセスが可能なゲートウェイ（アプリケーション層ゲート

* ルーチング表の爆発と呼ばれることもある．

† プライベート IP アドレスを持った IP セグメントはインターネット内で転送されない．

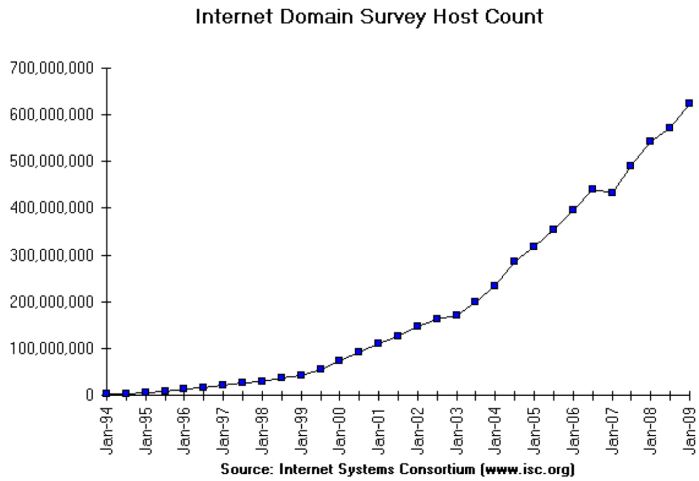

図 1·3　ホスト数の統計データの推移

ウェイ，NAT [20]，NAPT [21]など）を経由する必要がある．次の 3 種類の IP アドレス空間が，プライベート IP アドレスのために予約されている．

10.0.0.0 － 10.255.255.255(10/8)

172.16.0.0 － 172.31.255.255(172.16/12)

192.168.0.0 － 192.168.255.255(192.168/16)

(2) クラスレスなアドレス割当

上述した問題を克服することを目指して，クラスレスなアドレス割当が導入された．クラスレスなアドレス割当は，クラスフルなアドレス割当の拡張となっている．クラス A，B，C の IP アドレスの割当てにおいては，プレフィックス長が 3 通りに限定されていた．1993 年に導入された CIDR とは，プレフィックス長を 0 から 32 まで取れるようにした IP アドレスの利用規程である．CIDR によりプレフィックス長の指定の自由度が上がり，その結果，アドレス割当の自由度が飛躍的に拡大した．

また，CIDR により複数の IP アドレス的に連続する複数のネットワークを一つのネットワークにまとめることが可能となった．例えば，203.183.224.0/24 と 203.183.225.0/24 の連続する二つのクラス C のネットワークは，二つのクラス C に相当する一つのネットワーク 203.183.224.0/23 として記述可能となる．

このように，クラス B を用いなくとも，複数の連続するクラス C をまとめることにより，問題（I）の一部に対処可能となる．また，複数のネットワークを一つにまとめることにより，複数の経路情報を一つに集約 (aggregate) 可能となる．結果として，ルーチング表のエントリ数減少につながり，問題（II）を考慮したことになる．しかしながら，ルーチング表のエン

トリ数の増大，および，更新問題に対する対症療法にすぎない．

従来，クラス A，B，C のクラスフルな IP アドレスが組織の規模に従い，ネットワークインフォメーションセンター（NIC: Network Information Center）から順不同に割当てられていた．CIDR の技術が導入されてから，NIC は多量のクラス C の IP アドレスをインターネットサービスプロバイダーに割当てるようになった．組織は，インターネットサービスプロバイダーから，必要に応じて連続したクラス C のアドレスを割当ててもらうこととなった．このような割当は，地理に依存したアドレス割当の導入とも考えられ，経路集約の効率をあげて，ルーチング表のエントリ数の増大を抑制する効果がある．

一方，問題（III）は，プライベートアドレスの導入で緩和されるが，本質的には解決されない．そこで，IP アドレス長を 32 ビットから 128 ビットに拡張してアドレス空間を大幅に広げる IPv6（IP version 6）[22) 23) 24)] の導入が進みつつある．IPv6 は，2 章で説明される．

前述のクラスフルやクラスレスによる IP アドレス，プライベートアドレスの他に特別な意味を持つ IP アドレスが存在 [25) 26)] する．原則として，1 が並ぶフィールドを「全部」と解釈し，0 が並ぶフィールドを「ここ」と解釈する．

- IP アドレスが全て 0（あるいは，0.0.0.0 と記す）：このネットワークのこのホストを意味する．システムの立ち上げ時に自分自身の IP アドレスが不明なホストが，自分自身を表す場合に用いる．送信元アドレスとしてのみ使用される．
- IP アドレスが全て 1：限定ブロードキャストと呼ばれる．このアドレスをもつ IP データグラムは，送信元が属するネットワーク外には転送されない．送信先アドレスとしてのみ使用される．
- IP アドレスのホスト部が全て 1：指定ブロードキャストと呼ばれる．ネットワーク部で指定されたネットワークに対するブロードキャストを意味する．送信先アドレスとしてのみ使用される．
- IP アドレスのネットワーク部が全て 0：このネットワーク内において，ホスト部が示すホスト自身を指す．当該ホストが属するネットワーク部の番号が不明な際，送信元アドレスとしてのみ使用される．
- 127.0.0.0/8（あるいは，127.0.0.1 と記す）：このホスト自身を表すアドレスであり，ループバックアドレスとも呼ばれる．プロトコルのテストや同一ホスト内のプロセス間通信などで使われる．

1-1-5 ネットワーク層で利用される標準プロトコル

ネットワーク層（インターネット層）の標準プロトコルとして，IP，ICMP，IGMP がある．また，ネットワーク層と直下の層を結びつけるプロトコルとして，ARP (Address Resolution Protocol) [27)]がある．ARP を利用することにより，ホストは次にパケットを転送すべき機器の物理アドレス（MAC アドレス *）を取得できる．つまり，ARP はネットワーク機器の物理

* データリンク層おける，その機器の識別子であり，物理アドレスと呼ばれることもある．

アドレスを隠ぺい可能な下位レベルプロトコルであり，ネットワーク層（インターネット層）の標準プロトコルではない．この機構により，各ホストや各ネットワーク機器に対し，MAC アドレスに縛られない IP アドレスの割当が可能となっている．

IP データグラムは，まず送信元から最寄りのルータへ送られる．次に，経路制御により，ルータから送信先に至るべく次のルータへ転送される．最後に，最終のルータから送信先へ転送される．送信元から最寄りのルータへの転送は，同一 LAN 内で行われることが多い．LAN 内の転送においては，ネットワーク層より下のデータリンク層のアドレスである，最寄りのルータの MAC アドレスが必要となる．送信元がこのルータの IP アドレスはわかるものの，MAC アドレスが不明な場合，ARP を利用して，その MAC アドレスを得ることができる．ネットワーク層の下のデータリンク層では，この MAC アドレスに基づきデータが転送される．

以降，まず，IP データグラムのフォーマットについて述べる．3 章以降で詳細に説明される経路制御に加え，この IP データグラムのフォーマットそのものが IP の機能を具体的に示しているといえる．次に，IP を補助するプロトコルである ICMP について説明する．更に，マルチキャストの際に重要となる IGMP について述べる．

(1) IP データグラム

IP を用いて通信を行う際には，この IP ヘッダがデータの先頭につけられる．IP ヘッダには，IP 関係の制御情報が全て含まれる．図 1･4 に，IP ヘッダを含む IP データグラムのフォーマットを示す．

<table>
<tr><td>Version</td><td>HL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td>Time to Live</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="5">Options</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

図 1･4　IP データグラムのフォーマット

- Version：4 ビットのサイズで，IP プロトコルのバージョン番号が入る．IPv4 の場合は 4 が入り，IPv6 の場合は 6 となる．
- HL (Internet Header Lenght)：4 ビットのサイズで，IP ヘッダ自身の大きさを表す．4 オクテットが 1 単位である．オプションフィールドがない IP ヘッダサイズは 20 オクテットなので，HL=5 と記述される．

- Type of Service (TOS)：8 ビットのサイズである．Diffserv とよばれる通信品質制御や ECN (Explicit Congestion Notification) という輻輳制御に利用されることがあるが，現在，一般的には，ほとんど利用されていない．TOS とも呼ばれる．

- Total Length：16 ビットのサイズで，IP ヘッダを含む IP データグラム全体のサイズを表す．単位はオクテットである．

- Identification：16 ビットのサイズである．フラグメントを復元する際の識別子として用いられる．この Identification が同じであっても，送信元 IP アドレス，送信先 IP アドレスやプロトコルの組のどれかが異なる場合には，別のフラグメントとして扱われる．

- Flags：3 ビットのサイズで，パケット分割に関する制御のために用いられる．

- Fragment Offset：13 ビットのサイズである．分割したフラグメントが元データのどこに位置していたかを示す．単位は 8 オクテットである．

- Time to Live (TTL)：8 ビットのサイズである．TTL とも呼ばれる．元の意味は，IP データグラムがネットワーク内に存在してもよい時間で，単位は秒であった．しかしながら現在では，通過できる最大のルータ数を表す．IP データグラムがルータを通過するごとにこの値が 1 づつ減らされ，TTL が 0 になったルータで当該 IP データグラムは破棄される．TTL を適切に設定することで，IP データグラムが転送される範囲を限定できる．

- Protocol：8 ビットのサイズである．IP データグラムで転送される，ネットワーク層の一つ上のトランスポート層で動作するプロトコルの識別子（プロトコル番号）* が格納される．

- Header Checksum：16 ビットのサイズである．IP ヘッダに関するチェックサムを表す．IP ヘッダが壊れていないか否かを判定するために用いられる．

- Source Address：32 ビットのサイズである．送信元 IP アドレスを表す．

- Destination Address：32 ビットのサイズである．送信先 IP アドレスを表す．

- Options：4 オクテットが 1 単位で可変長である．一般的には，あまり使用されない．送信元が，IP データグラムが転送される送信先までの経路を予め指定する場合†，経由すべき，各ルータの IP アドレスを格納する．他にルートレコードやタイムスタンプなどで使われる．

- Padding：IP ヘッダの長さを整える詰め物である．Options フィールドなどを使った場合，IP ヘッダ長が，32 ビット（4 オクテット）の整数倍にならないことがある．その場合，0 を詰め込んで，32 ビットの整数倍に IP ヘッダ長を整える．

* 次の URL から最新のプロトコル番号が得られる．http://www.iana.org/assignments/protocol-numbers/
† ソースルーチングと呼ばれる．

- Data：IP が配送すべき，トランスポート層から受け取ったセグメントがデータとして入る．

（2）ICMP

IP は，最善努力方式のプロトコルであり，IP データグラム転送のため努力はするが，転送の保証はしない．そこで，IP データグラムが送信先に到達できない場合には，そのエラーが送信元に報告される．種々の制御情報を運ぶ ICMP は，このようなエラーなどが生じた場合に利用されるプロトコルである．ICMP は TCP や UDP 等のトランスポートプロトコルと同様に，自分自身を IP データグラムのデータ部に埋め込むことにより，IP を利用する．しかしながら， ICMP は，すべての IP モジュールが実装しなければならないと規定されており，IP の重要な一部分であるとみなされる．このことから，ICMP は，IP と同様にネットワーク層（インターネット層）のプロトコルであるといえる．

ICMP が扱うメッセージの種類は大きく二つに分けられる．一つはエラー通知のメッセージ群であり，もう一つはネットワークの診断等を行う問い合わせのメッセージ群である．エラー通知メッセージの代表的なものに，ICMP 到達不能メッセージ（ICMP Destination Unreachable Message）がある．これは，途中のルータが IP データグラムを送信先に転送できない場合に，そのルータから送信元に対して，通知される．際限がなくなるため，ICMP メッセージのエラーに対する ICMP メッセージは送信されない．ネットワークの診断メッセージの代表的なものに，ICMP エコーリクエストメッセージ（ICMP Echo Request Destination Message）がある．送信元からあるホストまでの到達可能性を調べるプログラムである ping は，この型のメッセージを利用している．また，送信元からあるホストまでの経路を調べるプログラムである traceroute は，ICMP 時間経過メッセージ（ICMP Time Exceeded Message）を用いている．

（3）IGMP

IGMP は，IP マルチキャストで動的なホストグループを管理するネットワーク層のプロトコルである．IGMP は，同じセグメント内のホストと隣接するマルチキャストルータ間で用いられる，マルチキャストグループの管理を行うプロトコルである．マルチキャストルータは，ホストからのマルチキャストグループ登録，離脱メッセージを受け取るばかりではなく定期的にホストに対して問合せを行い，グループ内のホストが活性状態か否かを調べる．IPv6 では，IGMP の機能は ICMPv6 (Internet Control Message Protocol v6)[28]に組み込まれている．

1-1-6 ルーチング

ルーチングは，3 章以降で主に説明されるため，ここでは，簡単にその準備をしておく．ルーチングとは，あるネットワークとそのネットワーク上の送信元と送信先が与えられたとき，その間の経路を選択することである．インターネットにおいては，ソースルーチングや固定ルーチング等のルーチング[29] も存在するが，インターネットの頑健性を支えているのは適応ルーチングである．

（1）インターネットの構成要素

インターネットは，基本的にネットワークノードとネットワークリンクから構成される．ネットワークノードは，更にデータの送受信を行うホストとデータの中継を行うルータに分

類される．インターネットはパケット交換ネットワークであり，交換されるデータの単位は，IP データグラムである．また，基本的にコネクションレスな通信を行う．つまり，IP データグラムに含まれる送信先アドレス等により，独立した配送が行われる．

（2）自律システム AS

インターネットのルーチングは，自律システム AS（Autonomous System）を単位として行われている．AS は，従来一つの組織によって管理され，通常単一経路制御プロトコルが動いているネットワークの一部分と定義[30]されていた．しかしながら，一つの AS が内部で複数の経路制御プロトコルを使う事例が出てきた．そのため，現在では，明確に定義された一つのルーチングポリシーによって運用される，単一の管理権限下にあるネットワークの範囲としてとらえられている．AS においては，内部のネットワークの構造をある程度自由に管理権限により決定できるが，この AS の外部に対しては一つのネットワークとして機能[31]することが要請される．IP のコミュニティにおける AS の概念は，OSI 用語の経路制御ドメイン (routing domain) に対応する．

（3）IGP と EGP

インターネットのルーチングは，AS を単位として行われ，AS 内，および，AS 間のルーチングからなる．AS 内のルーチングプロトコルをインテリアゲートウェイプロトコル IGP（Interior Gateway Protocol），AS 間のルーチングプロトコルをエクステリアゲートウェイプロトコル EGP（Exterior Gateway Protocol）と呼ぶ．IGP の要件としては，AS 内の経路計算を効率的に行えること，AS 内のネットワーク変化に対して素早く対応できることがある．EGP の要件としては，AS 間のルーチングポリシー[32]の交換，および，経路情報の集約がある．

1-1-7 IP データグラムの分割と再構築

IP データグラムは，送信元から送信先に至るまで，経路制御により，ルータからルータへ転送される．このルータ間では，様々なデータリンクが利用される可能性がある．ネットワーク層の下位層のデータリンク層のプロトコルにおいては，様々な最大転送単位（MTU）をもつメディアが使われることがある．例えば，FDDI（Fiber-distributed data interface）の MTU は，4352 オクテットであり，イーサネットの MTU は 1500 オクテットである．IP データグラムが，この一つの MTU に載せきれない場合には，IP データグラムの分割が行われる．一旦，分割された IP データグラムは，そのまま送信先に届けられ，送信先ホスト内のネットワーク層において，分割前の IP データグラムに再構築される．このように，IP は様々な種類のデータリンクに対応可能となっている．IP データグラムの分割と再構築は，ルーチングに加えて IP の重要な機能である．

■参考文献

1) P. Baran, et al.: *“On Distributed Communications,”* RM3420, 3103, 3578, 3638, 3097, 3762-7, The RAND Corp. (1964).
2) P. Baran: *“The beginnings of packet switching: some underlying concepts,”* IEEE Communication Magazine, vol.40, no.7, pp.42-48 (2002).
3) J. Postel (editor): *“Internet Protocol,”* RFC 791 (1981).
4) R. Braden (editor): *“Requirements for Internet hosts - communication layers,”* RFC 1122 (1989).
5) V. Cerf and R. Kahn: *“A protocol for packet network intercommunication,”* IEEE Trans on Commun., vol.Com-22, no.5, pp.637-648 (1974).

6) B. Leiner, R. Cole, J. Postel, and D. Mills: *“The DARPA internet protocol suite”* IEEE Communications Magazine, vol.23, no.3, pp.29-34 (1985).
7) D. D. Clark: “*The design philosophy of the DARPA Internet protocols*,” Proc. SIGCOMM ’88, Computer Communication Review, vol.18, no.4, pp.106-114 (1988).
8) 竹下隆史，村上公保，荒井透，苅田幸雄: “**マスタリング** *TCP/IP* **入門編 第４版**,” オーム社 (2007).
9) 堀 世彰，池永全志，門林雄基，後藤滋樹: “**ネットワークの相互接続**,” 岩波講座　インターネット第２巻，岩波書店 (2001).
10) 池田博昌，山本 幹: “**情報ネットワーク工学**,” オーム社 (2009).
11) 笠野英松 (監修), マルチメディア通信研究会編: “**インターネット** *RFC* **事典**,” アスキー出版局 (1998).
12) 村田正幸: “**マルチメディア情報ネットワーク –コンピュータネットワークの構成学–**,” 共立出版 (1999).
13) 小林 浩，江崎 浩: “**インターネット総論**,” 共立出版 (2002).
14) A.S. Tanenbaum（水野忠則，相田仁，東野輝夫，太田賢，西垣正勝　訳）: “**コンピュータネットワーク　第４版**,” 日経 BP 社 (2003).
15) J. Postel: *“Internet control message protocol,”* RFC 792 (1981).
16) W. Fenner: *“Internet group management protocol, version 2,”* RFC 2236 (1997).
17) Internet Systems Consortium: https: //www. isc. org/ ops/ solutions/ survey (2009).
18) Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot and E. Lear: *“Address allocation for private Internets,”* RFC 1918, February (1996).
19) V. Fuller and T. Li: *“Classless inter-domain routing (CIDR): the Internet address assignment and aggregation plan,”* RFC 4632 (2006).
20) K. Egevang and P. Francis: *“The IP network address translator (NAT),”* RFC 1631 (1994).
21) P. Srisuresh and M. Holdrege: *“IP network address translator (NAT) terminology and considerations,”* RFC 2663 (1999).
22) S. Deering and R. Hinden: *“Internet protocol, version 6 (IPv6) specification,”* RFC 2460 (1998).
23) C. Huitema: *“IP v6 – The New Internet Protocol– 2nd ed.,”* Prentice-Hall, Englewood Cliffs, NJ (1998).
24) D.E. Comer（村井純，楠本博之　訳）: “*TCP/IP* **によるネットワーク構築** *Vol. I*　**原理・プロトコル・アーキテクチャ第４版**,” 共立出版 (2002).
25) J. Reynolds and J. Postel: *“Assigned numbers,”* RFC 1700 (1994).
26) J. Reynolds (editor): *“Assigned numbers: RFC 1700 is replaced by an on-line database,”* RFC 3232 (2002).
27) D.C. Plummer *“Ethernet Address resolution protocol: or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware,”* RFC 826 (1982).
28) A. Conta and S. Deering: *“Internet control message protocol (ICMPv6) for the Internet protocol version 6 (IPv6) Specification,”* RFC 2463 (1998).
29) M.E. Streenstrup (editor): *“Routing in Communications Networks,”* Prentice-Hall (1995).
30) D.L. Mills: *“Autonomous confederations,”* RFC 975 (1986).
31) J. Hawkinson: *“Guidelines for creation, selection, and registration of an Autonomous System (AS),”* RFC 1930 (1996).
32) R. Govindan, et al.: *“An architecture for stable, analyzable internet routing,”* IEEE Network, vol.13, no.1, pp.29-35 (1999).