■3 群（コンピュータネットワーク）－ 3 編 ネットワーク層

5 章 IP Multicast

■概要■

IP Multicast は，IP パケット（データグラム）を複数のホストに送るための技術である．アドレス体系からサブネット内での制御方式，広域ネットワークにおける経路制御まで，幅広い技術を含む．

【本章の構成】

本章では，IP Multicast の概要（5-1 節），及び IGMP（5-2 節）について述べる．

■3群 - 3編 - 5章

5-1 IP Multicast

（執筆者：井上　武）［2008年6月 受領］

本来，IP ネットワークは，一対一の通信であるユニキャストをサポートするために開発された．ユニキャストを用いて複数ホストに IP パケットを送るためには，同じパケットを繰り返し送出する必要がある．これは，送信ホストと経路上のネットワークにとって大きな負荷となる．また，すべてのホストを宛先とするブロードキャストという通信方法がある．スイッチなどのネットワーク装置は，受信したパケットをすべてのインタフェースにコピーして送出する．このため，パケットはネットワーク全域に行き渡る．ブロードキャストは，サブネットに限定して利用されることが多い．

IP Multicast [1] は，ユニキャストとブロードキャストの中間に位置し，受信を希望する複数のホスト（ホストグループ）に IP パケットを送信する技術である．ホストグループはマルチキャストアドレス(グループアドレス)によって区別される．224.0.0.0 から 239.255.255.255 までのアドレス領域をクラスD と呼び，IP Multicast のために用いられる．ホストが参加するグループ数は任意である．

図 5・1 に示すように，IP Multicast では送信ホスト（サーバ）と受信ホスト（クライアント）をいくつかのルータによって接続する．ルータは IGMP（Internet Group Management Protocol）と呼ばれるプロトコルによってクライアントを制御する．IGMP については次節で紹介する．ルータ間の経路制御プロトコルは次章で述べる．

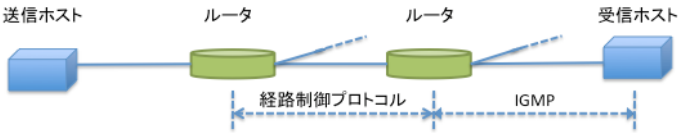

図 5・1　IP Multicast 概要

ユニキャストでは TCP を用いて信頼性のある通信を行うことが一般的である．しかし，TCP は送受信ホスト間で受信確認を行うため，複数の受信ホストが存在する IP Multicast では利用できない．このため，トランスポート層プロトコルには UDP が用いられる．また，リアルタイム通信では RTP （Real-time Transport Protocol）[2] によって順序やタイミングが制御されることが多い．

IP Multicast の開発は，1988 年に発表されたディアリング（Deering）の論文[2] によって開始された．その後，1990 年代には MBone（Multicast Bone）[3] と呼ばれる実験ネットワークが構築され，世界規模で研究開発が進められた．MBone は，トンネリング技術によって論理的に接続された仮想ネットワークであった．並行して，経路制御アルゴリズム[4,5] やネットワーク利用効率[6] について多くの学術的研究が行われた．

IETFではIP Multicastに関連した標準が熱心に議論されてきた．ホストの振る舞いやアドレス体系に言及した文献[1] に始まり，クライアントを制御するIGMPを定義した文献[8] ，経路制御を定義した文献[9] などが代表的である．これら以外にも，アドレス配布や信頼性マルチ

キャストなど，多岐にわたる標準が策定された．

このように多くの労力が注がれたにもかかわらず，IP Multicast の利用は企業内ネットワークなど限定されたものとなっている．広域展開を妨げた理由として，オペレーションが煩雑であったことや，経済的な成功に結びつかなかったことが挙げられる．

5-1-1 マルチキャストアドレス

IP Multicastでは，クラスDと呼ばれるアドレス領域を用いる．クラスDは 224.0.0.0 から 239.255.255.255 までの範囲である．いくつかのアドレス領域はすでに割り当てられている[9]．代表的なものを紹介する．

224.0.0.0/24 はリンクローカルに限定されている．このアドレスを宛先とするパケットを異なるサブネットに転送してはいけない．このアドレス領域は，主にプロトコル制御に用いられる．いくつかのアドレスは特定のホストグループに割り当てられている．例えば，224.0.0.1 はサブネット上の全システムを表し，224.0.0.2 はサブネット上の全ルータを表す．これら以外にも，224.0.0.0/8 のアドレス領域は多くの用途のために予約されている．

232.0.0.0/8 はSSM（Source Specific Multicast）[10] と呼ばれる拡張方式のために予約されている．SSMはホストグループを区別するために，マルチキャストアドレスだけではなくサーバのアドレスを用いる．このため，サーバ管理者はこの領域のマルチキャストアドレスを自由に利用することができる．SSMについては後述する．

233.0.0.0/8 は GLOP ブロックと呼ばれる．このアドレスは，アドレスの第 2 バイトと第 3 バイトが AS 番号に合致する AS に配布される．各 AS は，第 4 バイトを自由に設定し，利用することができる．

239.0.0.0/8 はローカルな用途に限定されたアドレス領域である．いわゆるプライベートアドレスに相当し，ドメイン内で自由に使うことができる[11]．

これら以外のアドレス領域は IANA に予約されている．

一方で，アドレスを動的に割り当てる方式も議論された．MASC（Multicast Address-Set Claim Protocol）[12] は AS 単位でアドレス割当てを行い，AS 内では AAP（Address Allocation Protocol）及び MADCAP（Multicast Address Dynamic Client Allocation Protocol）[13] により割当てを行う．しかし，これらの方式は普及していない．

Ethernet あるいは IEEE 802.3 標準などのデータリンク層はマルチキャストをサポートする．IANA は，01:00:5E から始まる MAC アドレスをマルチキャストのために割り当てている．マルチキャストアドレスを MAC アドレスに変換するには，マルチキャストアドレスの下位 23 ビットを MAC アドレスにコピーする．ただし，マルチキャストは 28 ビットのアドレス領域を持つため，複数のマルチキャストアドレスが同一の MAC アドレスに対応づけられる．このため，データリンク層のマルチキャスト機能が利用可能であっても，ネットワーク層でホストグループを判定する必要がある．

5-1-2 マルチキャストルータ及びホストの振る舞い

ホストは，いつでもマルチキャストパケットを送出することができる．受信を希望するときは，IGMP レポートと呼ばれるパケットを送出し，ルータに対してマルチキャストパケットの転送を要求する．IGMP については次節で述べる．IGMP レポートを受信したルータは，

マルチキャスト経路制御プロトコルによって経路を確立し，パケットを転送する．経路制御については次章で解説する．

マルチキャストパケットを転送するルータは，マルチキャストアドレスに対応した経路表を持つ．ユニキャスト経路表と同様に，宛先アドレスと出力インタフェースが記載される．ただし，マルチキャストにおいては，送信元アドレスと宛先アドレスのペアごとに出力インタフェースを決定することがある．

一般に，宛先となるマルチキャストアドレスのみで出力インタフェースを決定する転送方式を ASM（Any Source Multicast）と呼び，送信元アドレスとのペアで決定する方式を SSM[10] と呼ぶ（**図 5･2**）．送信元アドレスと宛先アドレスのペアをチャネルと呼ぶ．ASMではマルチキャストアドレスの一意性が要求されるが，SSMではペアとして一意であればよいため，サーバがマルチキャストアドレスを決定することができる．また，送信元が一つになるため，経路制御が簡易になる．SSMは次節で述べるIGMPバージョン 3 とともに用いられる．

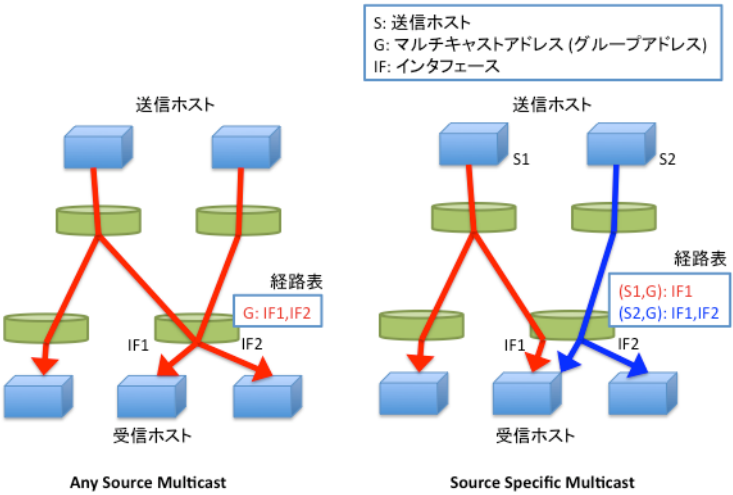

図 5･2　ASM と SSM

マルチキャストアドレスに対応した経路表をもたないルータは，マルチキャストパケットを転送することができない．経路上にこのようなルータが存在するときには，トンネリングと呼ばれる技術を用いてルータでの転送処理をスキップする（**図 5･3**）．トンネリングでは，トンネルの両端となるルータを事前に定めておく．トンネルの始点となるルータはマルチキャストパケットを受信すると，トンネル終端に宛てたユニキャストパケットに格納し，送出する．終端ルータまでの経路上のルータは，このパケットを通常のユニキャストパケットとして処理する．終端ルータはマルチキャストパケットを取り出すと，マルチキャスト経路表に従って送出する．

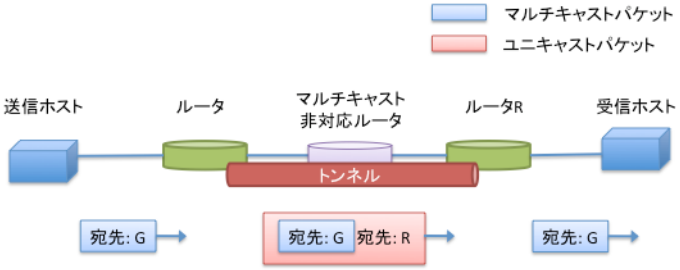
マルチキャストパケット
ユニキャストパケット
送信ホスト
ルータ
マルチキャスト
非対応ルータ
ルータR
受信ホスト
トンネル
宛先: G
宛先: G
宛先: R
宛先: G

図 5・3　トンネリング

■3群 － 3編 － 5章

5-2 IGMP

（執筆者：井上　武）［2008年6月 受領］

IGMP（Internet Group Management Protocol）は，受信ホスト（クライアント）の有無をマルチキャストルータに通知するために定義されたプロトコルである．最初のバージョンは1989年に標準となっている．現在の最新バージョンは3である．

5-2-1 IGMP バージョン1

バージョン1は文献[1]で定められている．マルチキャストルータがクライアントに問合せを行うためのメッセージをクエリ（Membership Query）と呼ぶ．全ホストアドレス 224.0.0.1 を宛先として送出される．また，クライアントがマルチキャストルータに報告を行うメッセージをレポート（Membership Report）と呼ぶ．レポートの宛先は，報告対象となるグループアドレスである．

バージョン1 のメッセージフォーマットを**図 5・4** に示す．バージョン番号フィールドは 1 とする．タイプフィールドは，クエリを表す1か，レポートを表す2のいずれかとなる．チェックサムフィールドには，IGMP フォーマットに対して計算したチェックサム値が入る．チェックサム値はこのフィールドを 0 として計算される．グループアドレスフィールドはレポートにおいてのみ意味をもつ．

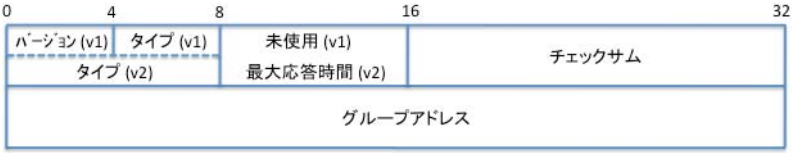

図 5・4　IGMP バージョン 1 及び 2 のメッセージヘッダ

図 5・5 に動作概要を示す．マルチキャストルータは，定期的にクエリを送出する．レポートを受信すると，経路表にそのグループアドレスを追加する．クエリに対して何回か連続してレポートを受信しなかったグループアドレスは，経路表から削除する．

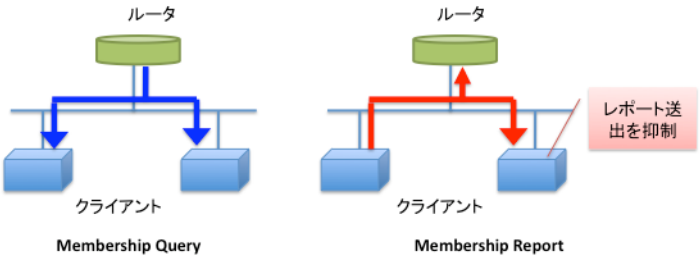

図 5・5　IGMP 動作概要

クライアントは，クエリを受信したインタフェースからレポートを送出する．このとき，複数のクライアントが同時にレポートを送出することを避けるために，クライアントは送出するまでに 10 秒以下のランダムな時間だけ待機する．待機中に，同じグループアドレスに対するレポートがほかのクライアントから送出されたときには，レポートの送出を省略することができる．マルチキャストルータにとって，クライアントの有無がわかればよく，台数を知る必要はないためである．

起動直後のクライアントは，待機せずに，数回連続してレポートを送出する．

バージョン 1 では，受信を停止するためのメッセージは定義されていない．いずれルータがクエリを送出し，レポートが返されなければ，そのグループアドレスの転送は停止される．

5-2-2 IGMP バージョン 2

バージョン 2 は文献[14] に定められている．バージョン 2 は，バージョン 1 からいくつかの機能が追加されている．バージョン 2 は後方互換性をもつ．

バージョン 2 では，バージョンフィールドとタイプフィールドを一つと考える．クエリは 0x11 となる．バージョン 1 レポートは 0x12 であり，バージョン 2 レポートは 0x16 となる．また，バージョン 2 で新たに導入されたリーブ（Leave）は 0x17 である．

バージョン 1 で未使用とされていたフィールドは，最大応答時間（Max Response Time）として使われる．バージョン 1 では，クエリに対するクライアントの応答時間は 10 秒以下とされていた．バージョン 2 では，この時間をクエリで指定することができる．

バージョン 1 では，受信を停止するにはタイムアウトを待つ必要があったが，バージョン 2 ではリーブによって明示的に停止することができる．クライアントは受信を停止する前にリーブを送信する．リーブを受信したマルチキャストルータは，そのグループアドレスを宛先とするクエリを送出する．これは Group Specific Query と呼ばれる．同じグループアドレスを受信するクライアントがいれば，通常のクエリと同様にレポートを返す．このクエリの最大応答時間は 1 秒と短く設定されるため，迅速に停止することができる．

同じサブネットに複数のルータが存在するときに，マルチキャストルータとしてクエリを送出するルータを選択することができる．マルチキャストルータは，自分より小さなアドレスをもつルータがクエリを送出していたら，クエリの送出を停止する．また，一定時間クエリの送出がなければ，他のルータがマルチキャストルータとしてクエリの送出を開始する．複数のルータを設置することで，フェイルオーバを実現できる．

5-2-3 IGMP バージョン 3

バージョン 3 は文献[7] に定められている．バージョン 3 は大幅に機能が追加され，とても複雑なプロトコルとなっている．ここでは主な機能を解説する．バージョン 3 は後方互換性をもつ．

バージョン 2 まではグループを単位として転送制御を行っていたが，バージョン 3 では送信元アドレスとグループアドレスの組合せを指定することができる．送信元アドレスを列挙するために，メッセージフォーマットは大きく拡張された．詳細は省略するが，一つのグループアドレスと，対応する複数の送信元アドレスを記述することができるようになっている．ある送信元アドレスを含める場合を INCLUDE モードと呼び，排除する場合を EXCLUDE モ

ードと呼ぶ．クライアントは，レポートによって INCLUD モードと EXCLUDE モードを指定することができる．

送信元アドレスを EXCLUDE モードに指定すると，その送信元からのパケットは転送されなくなる．例えば，あるグループアドレスに対して攻撃パケットが送られてきているときに，攻撃元を排除するために指定する．指定されたアドレス以外を送信元とするパケットは，通常どおり転送される．

送信元アドレスを INCLUDE モードに指定すると，その送信元からのパケットのみが転送されるようになる．これは，前節で解説した SSM などで用いられる．SSM では，送信元アドレスと宛先アドレスのペアをチャネルと呼び，チャネルを単位として経路制御を行う．

受信停止には INCLUDE モードが用いられる．INCLUDE モードを指定し，送信元アドレスを一つも指定しないことで，すべての送信元からのパケットを受信しないことを表すことができる．これによって，バージョン 2 のリーブと同様の機能を実現している．

バージョン 3 のレポートはグループへの参加離脱だけでなく，INCLUDE/EXCLUDE モードの変更や送信元アドレスの追加削除に対応するために，多くのメッセージタイプが定義されている．

5-2-4 IGMP Snooping

IGMP は IP 層で動作するプロトコルである．このため，データリンク層でのマルチキャストパケット転送を制御することはできない．つまり，サブネット内に受信ホストが存在する場合，そのマルチキャストパケットはサブネット全体に行き渡ることになる．

IGMP Snooping はこの問題を解決するために開発された技術である．IGMP Snooping に対応したスイッチは，通過するパケットの IGMP メッセージを覗き見する．スイッチのポートごとにクライアントの有無を判断し，クライアントが存在しないポートへのマルチキャストパケット転送を停止する．

■参考文献

1) S. Deering, “Host Extensions for IP Multicasting,” IETF RFC 1112, Aug. 1989.
2) H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications,” IETF RFC 3550, Jul. 2003.
3) S. Deering, “Multicast routing in internetworks and extended LANs,” Proc. of SIGCOMM’88, Aug. 1988.
4) H. Eriksson, “MBONE: the multicast backbone,” Communications of ACM, Vol.37, No.8, pp.54–60, Aug. 1994.
5) T. Ballardie, P. Francis, and J. Crowcroft, “Core based trees (CBT),” Proc. of SIGCOMM’93, pp.13-17, Sep. 1993.
6) S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C.-G. Liu, and L. Wei, “An Architecture for Wide-Area Multicast Routing,” Proc. of SIGCOMM’94, pp.126-135, Aug. 1994.
7) G. Phillips, S. Shenker, and H. Tangmunarunkit, “Scaling of Multicast Trees: Comments on the Chuang-Sirbu scaling law,” Proc. of SIGCOMM’99, Aug. 1999.
8) B. Cain, S. Deering, B. Fenner, I. Kouvelas, and A. Thyagarajan, “Internet Group Management Protocol, Version 3,” IETF RFC 3376, Oct. 2002.
9) B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised),” IETF RFC 4601, Aug. 2006.

10) Z. Albanna, K. Almeroth, D. Meyer, and M. Schipper, “IANA Guidelines for IPv4 Multicast Address Assignments,” IETF RFC 3171, Aug. 2001.
11) S. Bhattacharyya, “An Overview of Source-Specific Multicast (SSM),” IETF RFC 3569, July 2003.
12) D. Meyer, “Administratively Scoped IP Multicast,” IETF RFC 2365, Jul. 1998.
13) P. Radoslavov, D. Estrin, R. Govindan, M. Handley, S. Kumar, and D. Thaler, “The Multicast Address-Set Claim (MASC) Protocol,” IETF RFC 2909, Sep. 2000.
14) S. Hanna, B. Patel, and M. Shah, “Multicast Address Dynamic Client Allocation Protocol (MADCAP),” IETF RFC 2730, Dec. 1999.
15) W.C. Fenner, “Internet Group Management Protocol, Version 2,” IETF RFC 2236, Nov. 1997.