# IPネットワークによる有料放送型配信の検討と実現 —ユーザ認証機能を付加したIPマルチキャスト映像配信実験報告—

北村 雅一† 押海 卓志† 小田 孝和‡ 西尾 修一† 本野 智治†
†NTT西日本研究開発センタ ‡NTT西日本技術部

**概要**

本論文では、IPマルチキャスト技術を用いて有料放送型配信を実現する方法について述べる。現行のIPマルチキャスト技術を有料放送型の通信に適応した場合、有料チャネルの受信者制限の実現、不正受信要求の抑制の実現、隣接受信者への漏洩の防止の実現などが課題となる。これらの課題を解決する方法を比較検討し、それらの解決案のうち、汎用OSを搭載した受信端末を利用できる方法について実験を行い、実験で得られた結果を報告する。

# Investigation and Realization of pay-TV System on IP Network -Experiment on TV Broadcasting System over IP Multicast with User Authentication-

Masakazu Kitamura † Takashi Oshiumi † Yoshikazu Oda ‡ Shuichi Nishio † Tomoharu Motono †
† NTT-West Research & Development Center ‡ NTT-West Technology Department

**Abstract**

This paper describes how to realize toll TV systems utilizing IP multicast technology. When applying the current IP multicast technology to the chargeable broadcasting system, there still exist several problems. We compared various methods for solving these problems. Among these, we performed an experiment on the method that does not require charge on user terminals. Through the experiment, we could confirm a certain amount of validity and some problems.

## 1. はじめに

家庭への通信設備の広帯域化／光化に伴い、映像などの広帯域コンテンツをIPネットワーク上で送受信することへの期待が高まってきている。総務省では、放送と通信の融合化が議論されている。

放送と通信の融合を実現する一つの技術として、1対n通信に適したIPマルチキャスト技術がある。IPマルチキャスト技術を利用して放送型配信の実現は、ユニキャスト技術で実現する場合に比べて、配信サーバのデータ送出負荷を軽減できる上に、ネットワークリソースを効率的に使用できる面で優位性を持つ。これらの優位性は、受信端末の増加に伴ってより顕著となる。IPマルチキャストを実現する技術は、ルーティング情報を処理するDVMRP[1]、PIM-DM[2]、PIM-SM[3]や、グループメンバシップを処理するIGMP[4]などが標準化されてきている。

しかしながら、これらの現行のIPマルチキャスト技術を用いてペイパーチャネルのような有料コンテンツを含む放送ネットワークの実現を考えた場合、複数の技術的な課題が存在する。

そこで、本論文ではそれらの課題を整理し、課題を解決する案を比較検討する。さらに解決案の中で汎用OSを搭載したPCを受信端末に利用できる方法について検証実験を行い、その結果を報告する。本論文が想定する環境は、一つの事業者がサーバから受信端末までのネットワークを管理／提供することを前提としている。

## 2. IPネットワークによる有料放送型配信の課題

IPマルチキャスト技術を利用して有料チャネルを含む放送サービスネットワークを実現する際の課題を以下に説明する。

○有料チャネルの受信者制限

契約者が自由に有料チャネルを選択契

約できるサービス形態において、有料チャネルは、契約した受信者にのみ提供される。つまり、契約していない有料チャネルを視聴できないように制限する仕組みが必要となる。

○不正受信要求の抑制

公衆の放送サービスネットワークでは、様々なユーザの接続が想定されるため、悪意をもったユーザの存在も考慮する必要がある。現行のIPマルチキャスト技術では、少なくとも以下の2つの点においてユーザから攻撃受ける可能性がある。

一つは、存在しないマルチキャストグループへの受信要求も含めた多量の新規受信要求をエッジルータへ送出する攻撃である。ルータは新規受信要求を受信すると、受信プロセスを動作させ上流ルータへと要求を伝える。必要以上の受信要求は、他の受信者の受信要求処理を遅らせたり、廃棄させたりする可能性もある。そのため、不正な受信要求による処理負荷の影響範囲を小さくする仕組みが必要となる。

もう一つは、受信者が割当て帯域以上のトラヒックを要求してトラヒックを受信することによる帯域の圧迫である。コスト面からネットワーク帯域は、複数受信端末で共有させて用意する場合がある。ある契約者が割当て帯域以上のトラヒックを受信すれば、そのネットワーク帯域を共有している他の契約者の帯域が足りなくなる可能性がある。そのため、1つの契約が同時に受信できるチャネル数を制限したり、受信できる最大帯域を制御したりするなどの仕組みが必要となる。

○隣接ユーザへの情報漏洩の防止

IPマルチキャストトラヒックは、Ethernetのような共有メディアでは、ブロードキャストトラヒックと同様に取り扱われる。そのため、同一ブロードキャストドメインに接続している端末は、隣接端末が受信しているトラヒックのグループアドレスを知ることができる上に、通信履歴も取得することができる。このような問題を防ぐために、隣接受信者にマルチキャストトラヒック情報が漏洩しないようにする仕組みが必要となる。

○マルチキャストトラヒック送信者の制限

現行のIPマルチキャストルーティングプロトコルは、ネットワークに流入するトラヒックからルーティング情報を計算する。例えば、ある配信サーバに割当てたマルチキャストIPアドレスを使用して他の配信サーバがIPマルチキャストトラヒックを送出するとルータは、そのIPマルチキャストトラヒックからルーティング情報を計算する。その結果、受信者は要求していないIPマルチキャストトラヒックを受信する可能性がある。この問題を解決するために、IPマルチキャストトラヒック送信サーバを制限する仕組みが必要となる。

以上の課題を解決する方法を3章で述べる。

## 3. 有料放送型の映像配信実現方法

### 3.1 有料チャネルの受信者制限を実現する方法

IPマルチキャストネットワーク上で有料チャネルの受信者を制限する方法としては、これまでいくつかの方法が提案されている。現状、提案されている方法は、以下の2つに分類することができる。

- コンテンツを暗号化し、契約者のみ復号化を可能にする方法
- IPマルチキャスト受信要求を利用してアクセス制御する方法

以下に上記のそれぞれの方法の説明をする。

#### 3.1.1 コンテンツを暗号化し、契約者のみ復号化を可能にする方法

この方法は、IP技術を使用していない衛星放送やCATVでも採用されている方法であり、受信端末に配布した鍵やチャネル毎の鍵など複数の暗号鍵を使用してデータを暗号化し、正当な鍵を持った受信者端末だけが復号できる方法である。例えば、契約した契約端末が使用する鍵を使用って暗号化することで、契約した受信端末のみが

複合できるようになる。この方法の特徴としては、アプリケーションレイヤで暗号化するため、アプリケーションの実装でコピー防止機能を盛り込むこともできる。ただし、暗号化/複合化に対応したサーバ、受信端末アプリケーションを用意する必要がある。

### 3.1.2 IP マルチキャスト受信要求を利用してアクセス制御する方法

この方法は、現在さまざまな案が提案されている。いずれの方法も図 1 に示すように受信端末と受信端末を接続するエッジルータとの間で交換される受信要求メッセージ(IGMP Host Membership Report)を制御することで実現する方法である。代表的な

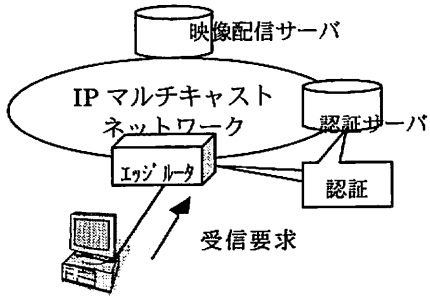


図 1　基本構成例

3 つの案を以下に説明する。

(1)　IGMPv2 を利用した端末認証方法

この方法は、受信端末から送出される受信要求をエッジルータが受信すると、上流ルータに受信要求を送信する前に受信要求パケットに含まれる IP マルチキャストアドレスと送信元 IP アドレス情報とをキーとして RADIUS 等の認証機能をもつ契約管理サーバに受信可否判断を仰ぎ、事前に登録されているもののみに送信を許容する方法[6]である。この方法は、ネットワークのエッジルータに機能を具備することで実現できる（古川電気工業の FITELnet-G シリーズに実装されている)。

また受信端末は、汎用 OS に実装されている IGMP をそのまま利用することが可能であることが大きな特徴である。詳細については、後述する。

(2)　拡張 IGMPv2 を利用した個人認証方法

(1)の方法では、例えば家庭の親子のような、同一端末を使用する複数のユーザを識別することができない。そこで、この課題を解決するため、ユーザ ID とパスワードを IGMP に付加する方法が IETF に提案されている[7]。しかし、現状この機能を実装する装置は、存在しない。さらに、受信端末は、汎用 OS に変更を加える必要がある。

(3)　IPsec を併用した認証方法

この方法は、IPsec AH(Authentication Header)を使用して、受信要求の正常性を確認して送受信する方法である。認証鍵の保持方法としては、LAN または IP マルチキャストグループ毎に 1 つの鍵を持つ方法と、システム全体で一つの public 鍵を保持する方法の 2 つの方法が提案されている[8]。しかしながら、現状 IPsec は、デジタル署名をサポートしていない等の問題があり、IGMP や IPsec の拡張も必要となる。また、多量の鍵を管理しなければならないという課題もある。

IPsec を利用する方法は、議論がなされ始めたところであり、実現には時間を要すると予想される。

### 3.2 不正受信要求の抑制を実現する方法

存在しないマルチキャストアドレスへの受信要求といった不正な要求を抑制することは、前述した 3.1.1 章の方法では解決できないが、3.1.2 章のいずれの方法でも、不正要求の処理をエッジルータまでの影響に留めることができ、上流ルータに影響を及ぼさない。

また、同時アクセス数を制限する方法も 3.1.1 章の方法では解決できないが、3.1.2 章のいずれの方法でも契約者毎または、契約端末毎に現在の使用帯域を管理し、受信要求時に割当て帯域と使用帯域を照合して受信可否を判断することで解決できる。ただ、この方法は、事前に手動等の方法によりマルチキャストグループ毎の使用帯域を判断機能に与えておく必要がある。

### 3.3 隣接ユーザへの情報漏洩を防止する方法

この課題は、受信端末と受信端末を接続するエッジルータとの間のネットワークのブロードキャストドメインをユーザ毎（契約者毎）に分割することで解決できる。グループメンバシップ処理が分割されるため、自端末が受信しているマルチキャストアドレスを隣接ユーザに知られなくすることができる。これは、3.1.1 章や 3.1.2 章のいずれの方法とも併用することが可能である。ブロードキャストドメインをユーザ毎に分割できない環境では、コンテンツを暗号化することでコンテンツ情報の漏洩を防ぐことはできるが、受信状態やマルチキャストアドレス情報の漏洩を防ぐことはできない。

### 3.4 マルチキャストトラヒック送信者を制限する仕組みの実現

この課題は、マルチキャストアドレスを管理し、サーバに割当てたアドレスを他のサーバが使用できないように、端末やサーバと接続しているルータにおいてフィルタリングすることで解決できる。これは、3.1.1 章や 3.1.2 章のいずれの方法とも併用することが可能である。

もう一つの解決策としては、PIM-SSM[9]を使用する方法がある。これは、マルチキャストグループアドレスと送信元 IP アドレスのペアでルーティングテーブルを管理するため、同一のマルチキャストアドレスを使用した配信サーバが存在しても、受信者は、要求するマルチキャストトラヒックを受信することができる。しかし、マルチキャストアドレス管理や、ネットアークリソース管理面で複雑となり、運用方法が課題となる。

以上より、有料放送型の映像配信を実現する方法を整理したものを表 1 に示す。同一契約者内の情報漏洩を問題としない場合は、3.1.1 章の方法を除いて、3.1.2 章のいずれの方法においても問題なく実現できる。また、同一契約者内の情報漏洩を問題とする場合は、(3)で実現するか、コンテンツの暗号化と、(1)または(2)を組み合わせることで、実現することは可能である。

表 1　各方法の比較

| | コンテンツの暗号化による方法 (3.1.1 章) | 受信要求を利用したアクセス制御(3.1.2 章) | | |
|---|---|---|---|---|
| | | (1) 端末アドレス認証 | (2) 個人認証 | (3) IPsec 認証 |
| 受信者制限 | ○ | ○ | ○ | ○ |
| 不正受信要求抑制 | × | ○ | ○ | ○ |
| 情報漏洩 | ○ | ○ | ○ | ○ |
| 暗号化 | ○ | − | − | ○ |
| 送信者制限 | ○ | ○ | ○ | ○ |
| 受信端末 | 専用アプリ | 汎用 OS | 専用アプリ | 専用アプリ |

そこで今回は、汎用 OS を搭載した PC を受信端末に利用でき、より現実的な(1)の方法を選択して検証実験を行なった。

## 4. 実験構成

本実験ネットワークは、図 2 に示すように映像を配信する配信サーバ、トラヒックを中継する中継ネットワーク、IGMP`v2 を利用した端末認証機能を実装したエッジルータ（古河電工製 FITELnet-G12）、認証を実行する RADIUS サーバ、汎用 OS である Windows2000/XP を搭載した受信端末とで構成される。

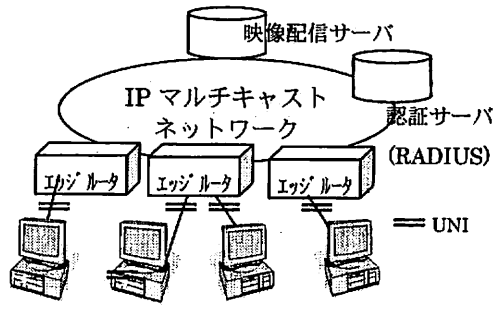


図 2　実験構成図

隣接契約者による盗聴防止のため、エッジルータと端末間のネットワークは、端

末毎にブロードキャストドメインを分割する構成とした。また、マルチキャストトラヒック送信サーバを限定するため、サーバに割当てたマルチキャストアドレスを他のサーバや受信端末が使用できないようにサーバを接続しているルータや端末を接続しているエッジルータにフィルタリングを設定した。

受信要求から IP マルチキャストトラヒックを受信するまでの動作シーケンスの概要を図 3 に示す。エッジルータは、受信端末から受信要求パケットを受信すると受信要求パケット情報に含まれる IP マルチキャストアドレスと送信元 IP アドレス情報をキーとして RADIUS サーバに送信可否を問い合わせる。RADIUS サーバは事前に登録された契約情報を照合して、送信可否結果をエッジルータに通知する。エッジルータは、その結果が許可通知であれば、上流ルータに受信要求を出す。拒否通知であれば、プロセスを終了する。エッジルータは、Leave Group Message を受信するか、IGMP Query に対する端末応答時間がタイムアウトするとトラヒック送信を止め、送信終了メッセージを RADIUS サーバに通知して終了する。RADIUS サーバは、アカウンティング情報として端末認証処理時刻、視聴開始時刻、視聴終了時刻を蓄積する。

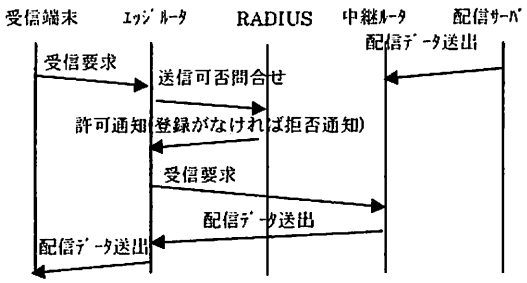


図 3　端末認証シーケンスの概要

## 5. 実験結果

○　有料チャネルの受信者制限

今回評価に用いた端末アドレス認証による方法は、受信要求パケットに含まれる送信元 IP アドレス情報をキーとして契約情報を照合する方法であるため、他の受信端末が同じ送信元 IP アドレスを使用して受信要求を送出できないようにする必要がある。

これを解決する方法は、契約者毎に IP サブネットを割当ててそれ以外のサブネットのアドレスを使用することができないように制限するか、RFC3069 で記述されている技術を利用して VLAN 単位に送信元 IP アドレスをチェックする[10]ことで解決できる。契約者毎に IP サブネットを割当てる方法も、参考文献[10]の方法も実験において評価した結果、なりすまし防止するために有効な方法であることを確認した。

次に本方法は、現行の IP マルチキャスト受信処理に認証処理を追加していることから、受信要求からマルチキャストトラヒック受信までの応答時間に影響を及ぼす。そこで、応答時間の確認を行なった。その結果を表 2 に示す。この測定は、認証機能を動作させた場合と動作させない場合のそれぞれにおいて、受信要求を送出してから IP マルチキャストトラヒックを受信するまでに要した時間を受信端末で測定したものである。認証機能を動作させた場合については、認証サーバの認証エントリ数の影響度を調べるため、約 160000 エントリ登録し、最初の行に記述した場合と、最後に記述した場合の条件の測定を行なった。測定値は、3 回測定した平均値である。表 2 の結果の通り、RADIUS サーバの応答時間は登録行数に影響を受ける。アプリケーションに影響しない範囲に遅延時間を抑える必要がある。処理時間が問題となる場合は、RADIUS サーバでの処理の効率化または、処理の分散化が必要となる。例えば、収容設計パラメータからルータ 1 台に対して収容する端末数をある程度見積もることができることから、認証サーバ 1 台に対して対応するルータの台数を決定し、何台かに 1 台の割合で認証サーバを設置することで分散処理させることができる。このことから

表 2 受信要求から映像受信までの時間

| | 受信要求から映像受信までの時間 |
|---|---|
| 認証なし | 98msec |
| 認証あり | 487msec（1 行目登録）<br>1066msec（160000 行目登録） |

RADIUS サーバの応答時間は、契約者が増加してもアプリケーションに対して問題ない範囲に抑えることは、可能であると言える。

○不正受信要求の抑制

端末アドレス認証処理をすることで不正受信要求による影響範囲をエッジルータまでに留めることができることから、認証しない場合に比べ、不正受信要求処理負荷を軽減できることの有効性は確認できた。

一方、契約者が同時にアクセスできるチャンネル数の制限や上限帯域の制限に関しては、今回用いたエッジルータに実装されている VLAN 毎の上限帯域の制限機能を利用した。このような機能は、割当て帯域以上の受信を抑制する手段として有効に働くことが実験を通して確認できた。

○情報漏洩の防止

本実験では、契約者単位にブロードキャストドメインを分割することで解決することとした。これにより、隣接契約者へのトラヒック情報の漏洩を防止することができた。詳細については、参考文献[10]を参照されたい。

○実験から得られた課題

RADIUS サーバには、課金情報として利用できる視聴開始/終了時刻のアカウンティング情報が蓄積される。ところが、実験において有料チャネル視聴中に不具合によりエッジルータが停止、再起動した場合、受信者へのトラヒックは停止したにもかかわらず、停止情報は RADIUS サーバに送信されず、アカウンティング情報は、視聴が継続している状態のままになるという事象が見られた。これは、もし RADIUS のアカウンティング情報を課金情報に利用すれば、ルータが停止して受信者が視聴できていないにもかかわらず課金されることになる。この問題は、エッジルータの起動／停止情報を RADIUS サーバに伝えることで解決できる。課金等で停止時刻の精度を必要とする場合は、さらなる検討が必要となる。

## 6. まとめ

本論文では、現行の IP ネットワーク技術を有料放送型の配信に適応した場合の課題である有料チャネル受信者制限、不正受信要求の抑制、隣接ユーザへの情報漏洩の防止、マルチキャストトラヒック送信サーバの制限を解決する方法の比較検討を行なった。さらに、受信端末に汎用 OS を搭載した PC を使用できる方法について検証実験を行なった。その結果、IGMP を利用してユーザ端末アドレス認証する方法の有効性を確認し、有料放送型の配信サービスが実現可能であることがわかった。

## 謝辞

本実験の実施にあたりご協力をいただいた安田圭一様、福富昌司様を始めとする古河電気工業株式会社の皆様に感謝します。

## 参考文献

[1] D.Waitzmman, et al., “Distance Vector Multicast Routing Protocol”, RFC1075, IETF, 1988

[2]Steven Deering,et al., “Protocol Independent Multicast version 2 Dense Mode Specification” , draft-ietf-idmr-pim-dm-06.txt, IETF, 1997

[3] D.Estrin, et al., “Protocol Independent Multicast-Sparse Mode (PIM-SM) Protocol Specification”, RFC2117, IETF, 1997

[4] W.Fenner, “Internet Group Management Protocol Version 2”, RFC2236, IETF, 1997

[5] M. Christense, et al., “IGMP and MLD snooping switches”, draft-ietf-magma-snoop-01, IETF, 2002

[6] 雑誌 ”月刊 Business Communication”, vol39 P66～P67, ビジネスコミュニケーション株式会社, 2002

[7]D.Andou, et al., ”IGMP for user Authentication Protocol (IGAP)”, draft-andou-igmp-auth-01.txt, IETF, 2002

[8]A.Van Moffaert, ”Security issues in Internet Group Management Protocol version 3 (IGMPv3)”, draft-irtf-gsec-igmpv3- security-issues-01, IETF, 2002

[9]S.Bhattacharyya, “An Overview of Source-Specific Multicast(SSM)”, draft-ietf-ssm-overview-03.txt, IETF, 2002

[10]押海,北村,他, “IP ネットワークシステムにおけるセキュアかつスケーラブルなユーザ収容方式の検討”, 第 10 回 DPS 研究会予稿集, 情報処理学会, 2002