IPマルチキャスト通信のユーザ認証機能の提案と実装

石川憲洋[†] 山内長承[††] 高橋修[†]

近年，IPマルチキャスト通信のためのプロトコルが幅広いプラットフォーム上でサポートされるようになり，インターネット上の仮想的なマルチキャスト通信ネットワークであるMBone上で，様々なマルチメディアツールを用いたマルチメディア通信実験が実施されている．しかしながら，IPマルチキャスト通信は今のところ実験段階にあり，商用サービスとして提供するためには，セキュリティ，課金，QOS制御，IPマルチキャストアドレス付与などのいくつかの課題を解決する必要がある．その中で，最も重要な課題の1つがIPマルチキャスト通信のセキュリティ機能である．IPマルチキャスト通信が必要とするセキュリティ機能は，ユーザ認証機能，IPマルチキャストデータグラムの暗号化，暗号化のための鍵管理など多岐にわたるが，今のところ研究段階にあり，実用化には至っていない．本論文では，IPマルチキャスト通信のセキュリティ機能の中で最も基本となる，不正なユーザがIPマルチキャストデータグラムを送受信することを防ぐためのアクセス制御に適用することを主な狙いとしたIPマルチキャスト通信のユーザ認証機能のためのアーキテクチャとプロトコルについて提案する．我々はIPマルチキャスト通信のユーザ認証機能のためにIGMPを拡張し，認証サーバとしてRADIUSを使用した．本アーキテクチャに基づくFreeBSD上でのプロトタイプシステムの実装についても述べる．

An Architecture for User Authentication of IP Multicast and Its Implementation

NORIHIRO ISHIKAWA,[†] NAGATSUGU YAMANOUCHI[††] and OSAMU TAKAHASHI[†]

Protocols for IP multicast have been widely implemented on various platforms over the past few years. Various multimedia tools have been tested on MBone, virtual multicast network on the Internet. However, IP multicast is now at the experimental stage. In order to deploy IP multicast over the Internet as a commercial service, several issues on IP multicast must be resolved. Such issues include security, accounting, QOS and IP multicast address allocation. Among them, one of the most important issues on IP multicast is security for IP multicast. There are no security functions for IP multicast at this time. IP multicast requires many security functions that include user authentication function of IP multicast, encryption of IP multicast datagrams and key management protocols for IP multicast. In this paper, we propose an architecture for the user authentication function of IP multicast, which prevents an unauthorized user from sending and receiving IP multicast datagrams, which is considered one of the most important security functions of IP multicast. We extend IGMPv2 for the user authentication function of IP multicast and use RADIUS as the authentication server. We have implemented a prototype system based on our architecture on FreeBSD. Implementation results are also described.

1. はじめに

インターネット上の仮想的なマルチキャスト通信ネットワークであるMBone上で，様々なマルチメディアツールを用いたマルチメディア通信実験が実施されている．その経験は，IPマルチキャスト通信が，インターネット上でのマルチメディアアプリケーションのための基盤技術であることを示している．また，最近では，IPマルチキャスト通信の新しいアプリケーションとして，電子ニュース，ソフトウェアなどのデジタル情報を同時に誤りなく多数のユーザに分配する高信頼マルチキャストが注目を集めている[1)]．

しかしながら，IPマルチキャスト通信は今のところ実験段階にあり，商用サービスとして提供するためには，セキュリティ，課金，QOS制御，IPマルチキャ

† NTT移動通信網株式会社マルチメディア研究所
Multimedia Laboratories, NTT Mobile Communications Network Inc.
†† 日本IBM東京基礎研究所
IBM Research, Tokyo Research Laboratory

ストアドレス付与などの課題を解決する必要がある．その中で，最も重要な課題の1つがIPマルチキャスト通信のセキュリティ機能である．現在のIPマルチキャスト通信は，セキュリティ機能を提供していない．IPマルチキャスト通信のためのセキュリティ機能は，ユーザ認証機能，IPマルチキャストデータグラムの暗号化，暗号化のための鍵管理と鍵配送など多岐にわたるが，その大部分は未解決であり，今後の研究課題として残されている．

本論文では，IPマルチキャスト通信のセキュリティ機能の中で最も基本となる，不正なユーザがIPマルチキャスト通信ネットワークに侵入することを防ぐためのアクセス制御に適用することを主な狙いとしたユーザ認証機能のためのアーキテクチャとプロトコルについて提案する．本アーキテクチャに基づくFreeBSD上でのプロトタイプシステムの実装実験についても述べる．

本論文の構成は，以下のとおりである．2章では，IPマルチキャスト通信のセキュリティ機能におけるユーザ認証機能の位置づけについて述べる．3章では，IPマルチキャスト通信のユーザ認証機能に対する要求条件について述べる．4章では，提案するIPマルチキャスト通信のユーザ認証機能のためのアーキテクチャとプロトコルについて述べる．5章では，本アーキテクチャの実装実験とその中で明らかになった課題について述べる．6章では，関連する研究に言及する．

2. 背景と位置づけ

IPマルチキャスト通信のセキュリティに関する主な要求条件を以下に示す．

- **アクセス制御**：不正なユーザを排除し，正当なユーザのみが，送信ユーザまたは受信ユーザとしてIPマルチキャスト通信に参加することが要求される．
- **データの秘匿**：データが正当な受信ユーザ以外の第3者に盗み見されることを防ぐ必要ある．データの秘匿は，限られたメンバで機密性の高いビデオ会議等行う場合，課金をともなうコンテンツをマルチキャスト配信する場合などに要求される．
- **送信ユーザの認証**：不正なユーザが送信ユーザになりすましてデータを送信することを防ぐために，データが正当な送信ユーザから送信されたことを確認することが要求される．
- **データの完全性**：データが，送信ユーザから改ざんされることなくすべての受信ユーザに配信されたことを確認できることが要求される．

上記の要求条件を満足するためにIPマルチキャスト通信に要求されるセキュリティ機能として，下記をあげることができる．

(1) ユーザ認証機能
(2) IPマルチキャストデータグラムの暗号化
(3) 鍵管理プロトコル
(4) データ認証機能

上記のセキュリティ機能は，まずIPユニキャスト通信を対象として研究および標準化が進められ，基本的な部分に関してはほぼ標準化を完了し，実装およびインターネットへの導入が進展している[2)~5)]．したがって，IPマルチキャスト通信への適用を図る場合，実装の容易さおよびインターネットへの導入コストなどを考慮すると，IPユニキャスト通信のために開発されたセキュリティ機能とできる限り整合性を保つことが望ましい．しかしながら，「データの秘匿」を実現するために要求されるIPマルチキャストデータグラムの暗号化と鍵管理プロトコルについては，下記のIPマルチキャスト通信固有の要求条件が存在する[6)]．

- IPユニキャスト通信の場合と異なり，鍵管理プロトコルに対しては，暗号化のためのグループ鍵（すなわち，共通鍵）を多数の受信ユーザに対してスケーラブルに配信する機能が要求される．
- IPマルチキャスト通信に参加しているメンバは動的に変動するため，IPマルチキャスト通信に新しいメンバが参加した場合，IPマルチキャスト通信から既存メンバが離脱した場合などに，暗号化のための新しいグループ鍵をIPマルチキャスト通信に参加しているすべてのメンバに配信できる機能が要求される．

上記の要求条件を満足するためには，長期的な課題として，新規にプロトコルなどを開発する必要があり，IPユニキャスト通信のために開発されたセキュリティ機能と整合性を保持し，その拡張として開発することは困難である．

また，「送信ユーザの認証」および「データの完全性」を実現するためのデータ認証機能に関しても，IPユニキャスト通信の場合，2者間で共有している共通鍵を使用することを前提としているため，単純にIPマルチキャスト通信に拡張することは困難である．

一方，不正な送信ユーザおよび受信ユーザを排除するための「アクセス制御」については，従来，マルチキャストルータにあらかじめアクセス制御のためのデータベースを保持し，その内容に基づいて不正な送信ホストおよび受信ホストを排除する方式がとられてきた．しかしながら，本方式には下記の問題点が

あった．

- 個々のグループアドレスごとに，あらかじめアクセス制御のためのデータベースをマニュアルで設定する必要があり，スケーラビリティが実現できない．
- IETF（malloc-WGなど）では，IPマルチキャスト通信のインスタンスに対して，グループアドレスを動的に付与する方式が検討されている[7]．マルチキャストルータにあらかじめアクセス制御のためのデータベースを保持する方式では，この場合に適用することが困難である．
- 送信ユーザおよび受信ユーザごとのアクセス制御が実現できない．

上記の問題点を解決してアクセス制御を実現するためには，ユーザ認証機能が必要となる．ユーザ認証機能については，IPマルチキャスト通信固有の要求条件は少なく，IPユニキャスト通信のためのユーザ認証機能の自然な拡張として提供することが可能である．加えて，ユーザ認証機能は，正当なメンバにグループ鍵を配信するために鍵管理プロトコルからも要求される機能であり，IPマルチキャスト通信のための最も基本となるセキュリティ機能の1つととらえることができる．

上記の考察に基づき，本論文では，IPマルチキャスト通信のセキュリティ機能の実現に向けた最初のステップとして，主にアクセス制御に適用することを狙いとしたユーザ認証機能のためのアーキテクチャとプロトコルを提案する[8]．

3. 要求条件

IPマルチキャスト通信のユーザ認証機能に対する要求条件を以下に示す．

- **IPユニキャスト通信のセキュリティ機能との整合性**：実装の容易さ，インターネットへの導入コストなどを考慮すると，IPマルチキャスト通信のためのセキュリティ機能は，おおむね標準化が完了しインターネットへの導入が進展しているIPユニキャスト通信のためのセキュリティ機能と，できる限り整合性を保持することが望ましい．
- **スケーラビリティ**：インターネットは急速な発展を続けているため，スケーラビリティは非常に重要である．IPマルチキャスト通信のユーザ認証機能に関しても，小規模なイントラネットから大規模なサービスプロバイダまでに適用できるスケーラビリティが要求される．
- **ルーティングプロトコルからの独立性**：IPマルチキャスト通信のために，DVMRP[9]，PIM[10]，CBT[11]などのIPマルチキャストルーティングプロトコルが開発されている．IPマルチキャスト通信のユーザ認証機能は，これらのIPマルチキャストルーティングプロトコルから独立であり，特定のIPマルチキャストルーティングプロトコルに依存してはならない．
- **送信ユーザのアクセス制御**：ユニキャスト通信と異なり，IPマルチキャスト通信の場合，送信ユーザが送信したIPマルチキャストデータグラムは，ネットワーク上の多数の受信ユーザに同時に配信される．だれでも送信できるため，ユーザが誤ってまたは悪意を持って送信すると，1）このトラヒックは受信ユーザのいるところへあまねく配信されるため，ネットワークの負荷になる，2）受信ユーザは正当な送信ユーザから配信されたデータであると信じ，その内容を信頼してしまうなどの問題が生じる．したがって，認証されたユーザのみがIPマルチキャストデータグラムを送信できるように制限することは重要である．
- **受信ユーザのアクセス制御**：現在のIPマルチキャスト通信では，受信ユーザは認証されることなくだれでもIPマルチキャストデータグラムを受信することが可能である．これに対して，2つの問題がある．第1に，課金をともなうコンテンツを配信する場合，最終的にはコンテンツを暗号化するなどの手段を講じるにしても，まずそのコンテンツが対象外のユーザに配信されないことが望ましく，現在のIPマルチキャスト通信のように，だれでも受信できる状況は望ましくない．第2に，対象外のユーザが受信するために生じるトラヒックは，無駄な負荷になるうえ，その発生をネットワーク側で制御できない．それはサービスプロバイダにとって望ましくない．

4. プロトコルの提案

4.1 アーキテクチャ

3章で述べた要求条件を満足する，IPマルチキャスト通信のユーザ認証機能のためのアーキテクチャについて提案する（図1）．

送信ホストが接続されているマルチキャストルータを入ルータ（Ingress Router），受信ホストが接続されているマルチキャストルータを出ルータ（Egress Router）と呼ぶ．

送信ホストがIPマルチキャストデータグラムの送信を開始するとき，入ルータは，オプションとして，

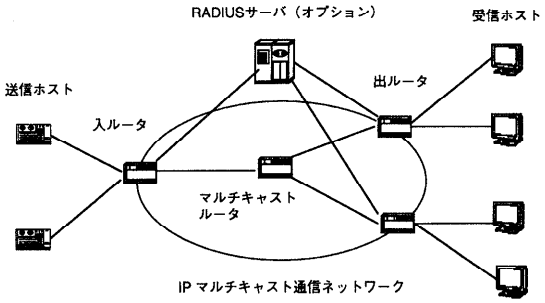


図1 IPマルチキャスト通信のユーザ認証のためのアーキテクチャ
Fig. 1 Architecture for user authentication of IP multicast.

送信ホスト上のユーザを認証可能とする．以下のシステム設計では，ユーザ認証はCHAP[12]と同様にチャレンジ・レスポンス方式により行う．入ルータは，認証サーバとしてRADIUS[13]を使用してもよい．ネットワーク上のすべての入ルータで，送信ユーザの認証を行うかまたはIPマルチキャストのルーティングを禁止するように設定すれば，ネットワークから不正な送信ユーザを排除できる．

認証に成功した場合，入ルータは，送信ホストから受信したIPマルチキャストデータグラムを出ルータまでルーティングする．ルーティングは，DVMRP，PIMなどの既存のIPマルチキャストルーティングプロトコルにより制御される．認証に失敗した場合，入ルータは，送信ホストから受信したIPマルチキャストデータグラムを廃棄する．

受信ホストは，IGMP[14]を使用して，出ルータにIPマルチキャストデータグラムの受信開始を要求する．受信ホストがIPマルチキャストデータグラムの受信を開始するとき，出ルータは，オプションとして，受信ホスト上のユーザを認証可能とする．以下のシステム設計では，ユーザ認証は送信ホストの場合と同様にチャレンジ・レスポンス方式により行う．

認証に成功した場合，出ルータは，送信ホストからマルチキャストルータを経由してルーティングされたIPマルチキャストデータグラムを受信ホストに送信する．認証に失敗した場合，出ルータは，IPマルチキャストデータグラムを受信ホストに送信しない．

本アーキテクチャにより，3章で述べた要求条件を満足することができる．本アーキテクチャは，IPユニキャスト通信のユーザ認証で広く利用されているチャレンジ・レスポンス方式を採用しているため，IPユニキャスト通信のセキュリティ機能との整合性が高い．本アーキテクチャは，IGMPを拡張して実現しているため，IPマルチキャストルーティングプロトコルとは独立である．個々の入ルータ，出ルータでユーザ認証のためのデータベースを管理する方式ではスケーラビリティを実現できないが，ユーザデータベースをネットワーク内の認証サーバで管理することにより，メンテナンスが容易になり，本アーキテクチャの大規模ネットワークへの適用が可能となる．我々は，認証サーバとしてダイアルアップユーザの認証に用いられているRADIUSを拡張して使用したが，本アーキテクチャでは，RADIUSに限定されることなく他の認証サーバを利用することも可能である．

表1 IGMPv2に追加した新メッセージ
Table 1 New messages added to IGMPv2.

メッセージ	主なパラメータ
Sender Start	Group-Address, User-ID
Challenge	User-ID, Challenge-Value
Response	User-ID, Response-Value
Success	Validity-Period
Failure	–

4.2 プロトコル

4.1節で提案したアーキテクチャを実現するために，IGMPおよびRADIUSに対して以下の拡張を行った．

4.2.1 IGMPの拡張

広く実装されているIGMP第2版（IGMPv2）[14]に対して，**表1**に示すメッセージを新たに追加した．

Sender Startは，送信ホストがIPマルチキャストデータグラムの送信開始を入ルータに通知するためのメッセージである．Sender Startメッセージを受信した入ルータは，送信ホスト上のユーザの認証を開始する．Challenge, Response, Success, Failureは，チャレンジ・レスポンス方式によるユーザ認証を実現するために追加したメッセージである．

4.2.2 RADIUSの拡張

我々は，認証サーバとして，ダイアルアップユーザの認証に用いられているRADIUSを拡張して使用した．RADIUSでは，ダイアルアップルータ–RADIUSサーバ間のプロトコルを規定している．

RADIUSサーバをIPマルチキャスト通信のユーザ認証に使用するために，RADIUSに対して，2つのサービスタイプ（“マルチキャスト送信ユーザ認証”と“マルチキャスト受信ユーザ認証”）およびそのパラメータとして**表2**に示す属性を新たに追加した．RADIUSに対しては，新しいメッセージの追加は行っていない．

4.3 方式概要

4.3.1 送信ホストのユーザ認証（図2）

IPマルチキャストデータグラムの送信を開始するとき，送信ホストは入ルータに対して，Sender Start

表2 RADIUSに追加した新属性
Table 2 New attributes added to RADIUS.

属性	説明
Group-Address	マルチキャストルータからRADIUSサーバに対して，認証の対象となるグループアドレスを通知する．
Validity-Period	RADIUSサーバからマルチキャストルータに対して，認証の有効期間を通知する．

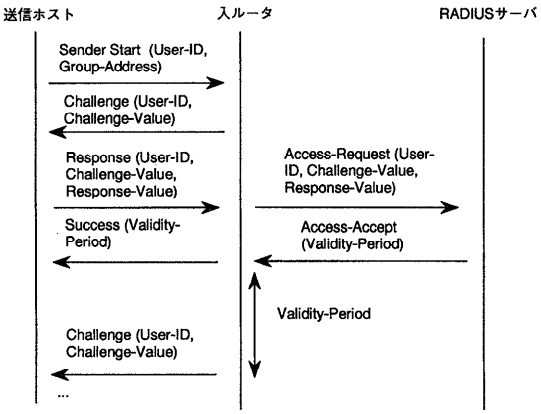


図2 送信ユーザの認証手順
Fig. 2 Procedure for authentication of IP multicast sender.

メッセージを送信する．Sender Start メッセージのGroup-Address パラメータには，IP マルチキャストデータグラムを送信する宛先のグループアドレス（クラスDのIPアドレス）を設定する．

Sender Start メッセージを受信した入ルータは，送信ユーザの認証を行うために，まず送信ホストに対して Challenge-Value パラメータに乱数を設定したChallenge メッセージを送信する．

Challenge メッセージを受信した送信ホストは，Response メッセージで入ルータに応答する．Response メッセージの Response-Value パラメータには，下記の値を設定する．

MD5（“乱数” + “送信ユーザのパスワード”）[15]

Response メッセージを受信した入ルータは，RADIUS サーバに Access-Request メッセージを送信して，送信ユーザの認証を依頼する．

Access-Request メッセージを受信したRADIUSサーバは，受信した“乱数”と自身が保持している“送信ユーザのパスワード”に対してMD5を適用し，その値と受信したResponse-Value パラメータを照合する．値が一致した場合は，入ルータに Access-Accept メッセージを送信して，認証の成功を通知する．値が一致しない場合は，入ルータに Access-Reject メッセージ

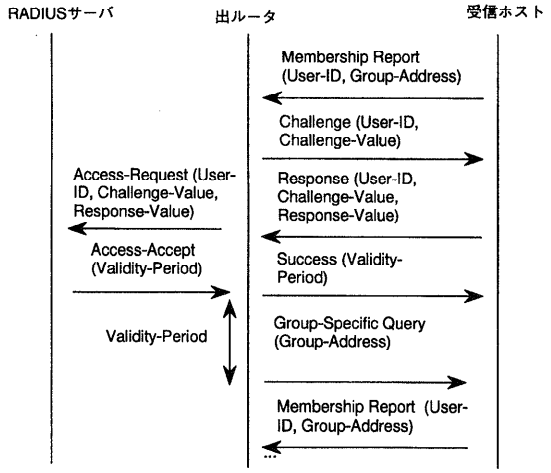


図3 受信ユーザの認証手順
Fig. 3 Procedure for authentication of IP multicast receiver.

を送信して，認証の失敗を通知する．

Access-Accept メッセージを受信した入ルータは，送信ホストに Success メッセージを送信して，認証の成功を通知する．Access-Reject メッセージを受信した入ルータは，送信ホストに Failure メッセージを送信して，認証の失敗を通知する．

認証に成功した場合，入ルータはその送信ホストが送信したIPマルチキャストデータグラムをルーティングする．認証に失敗した場合，入ルータはその送信ホストが送信したIPマルチキャストデータグラムを廃棄する．

ユーザ認証の有効期間（Validity-Period）を設けた．有効期間が切れた場合，入ルータは，送信ユーザの再認証を行う．

CHAP の場合と同様に，Challenge-Value パラメータに毎回異なる乱数を設定するため，Challenge-Value パラメータと Response-Value パラメータを不正なユーザに傍受されても，値を再利用されてネットワークに侵入される心配はない．

4.3.2 受信ホストのユーザ認証（図3）

IP マルチキャストデータグラムの受信を開始するとき，受信ホストは出ルータに対して，Membership Report メッセージを送信する．Membership Report メッセージの Group-Address パラメータには，受信ホストが参加するホストグループのグループアドレス（クラスDのIPアドレス）を設定する．

Membership Report メッセージを受信した出ルータは，受信ユーザの認証を行うために，まず受信ホストに対して Challenge-Value パラメータに乱数を設定

したChallengeメッセージを送信する．

以降，4.3.1項で述べた送信ユーザの認証と同様の手順で受信ユーザの認証を行う．

認証に成功した場合，出ルータは受信したIPマルチキャストデータグラムをその受信ホストにルーティングする．認証に失敗した場合，出ルータは受信したIPマルチキャストデータグラムをその受信ホストにルーティングしない．

送信ユーザの認証の場合と同様に，ユーザ認証の有効期間（Validity-Period）を設けた．有効期間が切れた場合，出ルータは受信ユーザの再認証を行う．

IPマルチキャスト通信では，イーサネットなどの共有メディアLANの場合，出ルータのルーティングのオン/オフは，LAN上に受信ホストが存在するか否かに基づいて行う．したがって，LAN上に1台以上の認証された受信ホストが存在すれば，出ルータはIPマルチキャストデータグラムをそのLANにルーティングすることとした．受信ホストの再認証を行う場合，出ルータは，LAN上のすべての認証された受信ホストに対しGroup-Specific Queryメッセージを送信し，Membership Reportメッセージで応答した1台の受信ホストが正しく認証されれば，IPマルチキャストデータグラムのルーティングを継続することとした．

4.4 IPマルチキャストデータグラムの暗号化への適用

提案した方式は，ISDNなどのポイント・ツー・ポイントネットワーク上では問題なく動作する．しかしながら，イーサネットなどの共有メディアLANの場合，LAN上に1台以上の認証された受信ホストが存在すれば，認証されていない受信ホストがIPマルチキャストデータグラムを傍受することが可能となる．

この課題を解決するためには，IPマルチキャストデータグラムの暗号化が必要となる．提案したユーザ認証方式を適用して実現されるIPマルチキャストデータグラムの暗号化の1方式を以下に提案する．

送信ユーザの認証が成功したとき，入ルータはグループ鍵管理サーバにアクセスして，グループアドレス（すなわち，クラスDのIPアドレス）に付与されたグループ鍵（すなわち，共通鍵）を取得する．その後，入ルータはSuccessメッセージのパラメータとして送信ユーザに受信したグループ鍵を送信する．グループ鍵は送信ユーザの公開鍵で暗号化して送信する．送信ユーザは，受信したグループ鍵で暗号化した後，IPマルチキャストデータグラムを入ルータに送信する．ユーザ認証の有効期間が切れた場合，入ルータは送信ユーザの再認証を行う．再認証に失敗した場合，入ルータは送信ユーザが離脱したと見なし，グループ鍵管理サーバに通知する．グループ鍵管理サーバは，離脱した送信ユーザが不正にIPマルチキャストデータグラムを送受信することを防ぐために，新しいグループ鍵を生成し，すべての入ルータおよび出ルータに配信する．スケーラビリティを確保するため，新しいグループ鍵の配信はIPマルチキャストを利用して行う．入ルータは，受信した新しいグループ鍵を送信ユーザに送信する．

同様に，受信ユーザの認証が成功したとき，出ルータは，グループ鍵管理サーバにアクセスして，グループアドレスに付与されたグループ鍵を取得する．その後，出ルータはSuccessメッセージのパラメータとして受信ユーザにグループ鍵を送信する．グループ鍵は受信ユーザの公開鍵で暗号化して送信する．受信ユーザは，暗号化されたIPマルチキャストデータグラムを，受信したグループ鍵で復号化する．ユーザ認証の有効期間が切れた場合，出ルータは受信ユーザの再認証を行う．再認証に失敗した場合，出ルータは受信ユーザが離脱したと見なし，グループ鍵管理サーバに通知する．グループ鍵管理サーバは，送信ユーザの離脱の場合と同様の手順で，新しいグループ鍵の配信を行う．

本方式では，グループアドレスがホストグループに割り当てられたときに，グループ鍵管理サーバがそのホストグループのためのグループ鍵を生成することを前提としている．スケーラビリティを実現するためのグループ鍵管理サーバの分散化については，今後の研究課題である．本方式に基づく，グループ鍵管理プロトコルの設計と実装についても今後の研究課題である．

5. 実装と評価

5.1 実装実験

我々は，**図4**に示す環境で，IPマルチキャスト通信のユーザ認証機能の実装実験を行った．

送信ホスト，受信ホストについては，FreeBSDのIGMPコードを拡張して実装した．送信ホスト上のIPマルチキャストアプリケーションが，ユーザ認証機能を利用可能とするために，新たに以下のソケットオプションを定義した．

- setsockopt (IP_MULTICAST_SENDER-START, User-ID, Passward)
- setsockopt (IP_MULTICAST_SENDER-END, User-ID, Passward)

受信ホスト上のIPマルチキャストアプリケーションが，ユーザ認証機能を利用可能とするために，既存

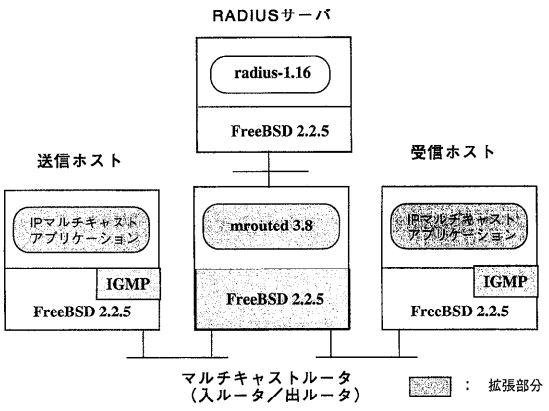


図4 IPマルチキャスト通信のユーザ認証機能の実装
Fig. 4 Implementation of prototype systems for user authentication of IP multicast.

のIPマルチキャスト通信のためのソケットオプションに，以下のとおりUser-IDパラメータとPasswardパラメータを追加した．

- setsockopt (IP_ADD_MEMBERSHIP, User-ID, Passward)
- setsockopt (IP_DROP_MEMBERSHIP, User-ID, Passward)

マルチキャストルータについては，mroutedとFreeBSDのIGMPコードを拡張して実装した．mroutedは，インターネット上の仮想的なIPマルチキャスト通信ネットワークであるMBone上で広く利用されているソフトウェアルータである．IGMPの認証プロトコルおよびRADIUSプロトコルの処理を行う機能は，mroutedに組み込んだ．FreeBSDに対しては，認証結果に基づいて，IPマルチキャストルーティングのオン/オフを行う機能を追加した．

RADIUSサーバについては，RADIUSプロトコル自身の拡張は行っていないため，Ascend社から提供されているRADIUSサーバのソフトウェア（radius-1.16）を拡張することなく使用した．

さらに，IPマルチキャストアプリケーションが，IPマルチキャスト通信のユーザ認証機能を利用できることを確認した．IPマルチキャストアプリケーションとしては，NTT情報通信研究所とIBM東京基礎研究所が共同開発した高信頼マルチキャスト通信プロトコルであるRMTP[1]を対象とした．RMTPを実装したソフトウェアを改造して，我々がFreeBSD上で開発したプロトタイプシステム上でユーザ認証機能を実行できることを確認した．

5.2 残された課題

4章で提案した方式では，入ルータは，送信元IPアドレスと宛先IPアドレス（すなわち，グループアドレス）の組に基づいて，送信ユーザから受信したIPマルチキャストデータグラムのフィルタリングを行う．本方式は，RTP[16]と組み合わせて使用する場合，以下の問題を引き起こす．RTPはIETFで標準化されたリアルタイムアプリケーションのためのトランスポートプロトコルである．

RTPを利用したアプリケーションとして，遠隔教育を例として問題を説明する．先生はIPマルチキャスト通信を利用して，同時に複数の生徒に対して遠隔教育を行う．この場合，正当な先生だけが遠隔教育をできるように，先生を送信ユーザとして認証する必要がある．送信ユーザとして認証された先生がRTPを使用して遠隔教育を行う場合，以下の問題が起こる．

生徒は，RTPを使用してはならないが，遠隔教育の品質を報告するために，RTCPを使用する必要がある．しかしながら，RTCPはRTPと同じ宛先アドレスを使用するため，生徒はRTCPパケットを送信することができない．

RTCPはRTPと異なった宛先ポート番号を使用するため，この課題は以下の方式により解決することが可能である．

先生の認証は，宛先IPアドレスとRTPが使用する宛先ポート番号の組に基づいて行う．したがって，認証された先生だけがRTPパケットを送信することができる．一方，生徒の認証は，宛先IPアドレスとRTCPが使用する宛先ポート番号の組に基づいて行う．結果として，生徒は，RTPパケットは送信できないが，RTCPパケットを送信することが可能となる．入ルータは，送信元IPアドレスと，宛先IPアドレスおよび宛先ポート番号の組に基づいて，送信ユーザから受信したIPマルチキャストデータグラムのフィルタリングを行う．

6. 関連研究

Ballardieは，IPマルチキャストルーティングプロトコルの1つであるCBTを利用したユーザ認証とグループ鍵配信方式を提案している[17]．Ballardieの方式では，受信ユーザは，IPマルチキャストデータグラムの受信を開始するときに，出ルータに対してユーザ認証を要求する．認証要求は，CBTを利用して，CBTのコアルータまで伝播される．受信ユーザの認証は，最終的にはコアルータが行う．ユーザ認証に成功した場合は，CBTを利用して暗号化のためのグループ鍵が受信ユーザまで配信される．グループ鍵配信方式のスケーラビリティはCBTを利用することにより実現さ

れる．しかしながら，Ballardieの方式は，CBTに依存しているため汎用性に乏しく，3章で述べた「ルーティングプロトコルからの独立性」の要求条件を満足できない．

Mittraは，ユーザ認証とグループ鍵管理方式のスケーラビリティを実現するために，サブグループの概念を導入している[6]．Mittraの方式では，IPマルチキャスト通信ネットワークを階層的なサブグループに分割し，各サブグループで独立にユーザおよび暗号化のためのグループ鍵を管理することによりスケーラビリティを実現している．しかしながら，各サブグループで異なるグループ鍵を使用するため，サブグループを越えて暗号化されたIPマルチキャストデータグラムを送信する場合，復合化と暗号化を繰り返す必要があり，性能面から見た場合，実用性に乏しいと考えられる．

7. まとめ

本論文では，IPマルチキャスト通信のセキュリティ機能の中で最も基本となる，不正なユーザがIPマルチキャスト通信ネットワークに侵入することを防ぐためのアクセス制御に適用することを主な狙いとしたIPマルチキャスト通信のユーザ認証機能のためのアーキテクチャとプロトコルを提案した．本アーキテクチャに基づくFreeBSD上でのプロトタイプシステムの実装実験を行い，IPマルチキャストアプリケーションが本機能を正しく利用できることを確認した．今後，本アーキテクチャの標準化を目指して，IETFなどに提案する予定である．

また，4.4節で提案したIPマルチキャストデータグラムの暗号化方式のためのグループ鍵管理プロトコルの設計と実装についても研究を進める予定である．

参考文献

1) 山内長承，城下輝治，佐野哲央，高橋 修：高信頼同報バルク転送機構，情報処理学会論文誌，Vol.39, No.6, pp.2009–2019 (1998).
2) Simpson, W.: PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994 (1996).
3) Kent, S. and Atkinson, R.: IP Encapsulating Security Payload (ESP), RFC 2406 (1998).
4) Kent, S. and Atkinson, R.: IP Authentication Header, RFC 2402 (1998).
5) Maughan, D., Schertler, M., Schneider, M. and Turner, J.: Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408 (1998).
6) Mittra, S.: Iolus: A Framework for Scalable Secure Multicasting, *ACM SIGCOMM '97* (1997).
7) Kumar, S., Radoslavov, P., Thaler, D., Alaettinoglu, C., Estrin, D. and Handley, M.: The MASC/BGM Architecture for Interdomain Multicast Routing, *ACM SIGCOMM '98* (1998).
8) Ishikawa, N., Yamanouchi, N. and Takahashi, O.: An Architecture for User Authentication of IP Multicast and Its Implementation, *Internet Workshop '99* (1999).
9) Waitzman, D., Partridge, C. and Deering, S.: Distance Vector Multicast Routing Protocol, RFC 1075 (1988).
10) Deering, S., Estrin, D., Farinacci, D., Jacobson, V., Liu, C. and Wei, L.: An Architecture for Wide-Area Multicast Routing, *ACM SIGCOMM '94* (1994).
11) Ballardie, T., Francis, P. and Crowcroft, J.: Core Based Tree (CBT), *ACM SIGCOMM '93* (1993).
12) Simpson, W.: PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994 (1996).
13) Rigney, C., Rubens, A., Simpson, W. and Willens, S.: Remote Authentication Dial In User Service, RFC 2138 (1997).
14) Fenner, W.: Internet Group Management Protocol, Version 2, RFC 2236 (1997).
15) Rivest, R. and Dusse, S.: The MD5 Message-Digest Algorithm, RFC 1321 (1992).
16) Schulzrine, H., Casner, S., Frederick, R. and Jacobson, V.: RTP: A Transport Protocol for Real-Time Applications, RFC 1889 (1996).
17) Ballardie, A.: Scalable Multicast Key Distribution, RFC 1949 (1996).

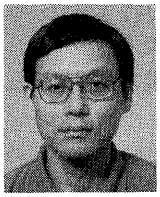
(平成11年1月22日受付)
(平成11年9月 2 日採録)

石川 憲洋（正会員）

1978年京都大学工学部情報工学科卒業．1980年同大学院工学研究科情報工学専攻修士課程修了．同年日本電信電話公社（現NTT）入社．1999年から，NTT移動通信網株式会社（NTTドコモ）マルチメディア研究所に所属．ATM，インターネットプロトコル，マルチメディア通信，モバイルインターネット等の研究開発に従事．

山内 長承（正会員）

1953年生．1975年東京大学工学部電子工学科卒業．1983年同大学院情報工学専門課程博士課程中退．1978～1984年スタンフォード大学大学院在学．1984年日本アイビーエム（株）入社．現在，東京基礎研究所勤務．東京都立大学工学研究科に客員教授として出向．主としてOS，並列プログラムの検証，計算機ネットワークの応用の研究開発に従事．工学博士．ACM，IEEE，日本ソフトウェア科学会各会員．



高橋 修（正会員）

1975年北海道大学大学院情報工学専攻修士課程修了．同年，日本電信電話公社入社．1999年より，NTT移動通信網株式会社（NTTドコモ）マルチメディア研究所主幹研究員．主としてモバイルマルチメディア通信サービスとプロトコルの研究開発に従事．電子情報通信学会会員．