コンピュータセキュリティ　18－10
(2002. 7. 18)

IPマルチキャスト経路制御プロトコル向けセキュリティ方式の提案

渡辺 義則† 笠井 真理子† オノ元 義貴‡

†(株)日立製作所システム開発研究所 〒244-0817 横浜市戸塚区吉田町292
‡(株)日立製作所エンタープライズサーバ事業部 〒259-1392 神奈川県秦野市堀山下1
E-mail: †{y-watana, boh}@sdl.hitachi.co.jp, ‡yoshitaka.sainomoto@itg.hitachi.co.jp

あらまし 一般家庭でのインターネットへのブロードバンド接続普及に伴い，今後増加が見込まれるマルチキャストによる放送型コンテンツ配信サービスへの適用を目的に，IPマルチキャスト経路制御プロトコルの安全を確保するセキュリティ方式を提案する。IPsecで利用されているデータ認証方式を基にしながら，マルチキャスト配信システムに適した認証鍵管理方式を新たに提案し，IPマルチキャスト経路制御プロトコルに対する盗聴や偽造パケット，リプレイパケットによる攻撃を防御できる見込みが得られた。現在，本提案の有効性検証のため，提案方式による鍵管理プロトコルの詳細設計とプロトタイプ作成を進めている。

キーワード インターネット，マルチキャスト経路制御，認証，鍵管理

Proposal of Security Architecture for IP Multicast Routing Protocol

Yoshinori WATANABE† Mariko KASAI† and Yoshitaka SAINOMOTO‡

† Systems Development Laboratory, Hitachi, Ltd. 292 Yoshida-cho, Totsuka-ku, Yokohama-shi, 244-0817 Japan
‡ Enterprise Server Division, Hitachi, Ltd. 1 Horiyamashita, Hadano-shi, Kanagawa, 259-1392 Japan
E-mail: †{y-watana, boh}@sdl.hitachi.co.jp, ‡yoshitaka.sainomoto@itg.hitachi.co.jp

Abstract The broadband internet connection from homes has come into wide use, and the services of broadcasting contents via the Internet will be expected to increase. So we propose a security architecture for IP multicast routing protocol for broadcasting contents more securely. It is based on a data authentication method used by IPsec protocol and a new key management method studied by us to avoid wire tapping, IP spoofing and replay attacks. Now we are trying to design a new key management protocol based on our architecture and implementing it to evaluate its effectiveness.

Keyword Internet, Multicast Routing, Authentication, Key Management

1. はじめに

一般家庭でのインターネット広帯域接続，常時接続が進む中，家庭や個人をターゲットとした映画クラスの高品質なデジタルコンテンツの配信など，いわゆるブロードバンドアプリケーションの提供がビジネスとして急速に立ち上がろうとしている。

しかし，このようなブロードバンドアプリケーション提供を実際にビジネスとして成立させていくためには，いくつかの課題を解決しなければならない。その中で最も重要なものの一つが，顧客に安心して対価を支払ってもらえる信頼性とセキュリティの確保である。デジタルコンテンツ配信サービスにおいては，DoS(Denial of Services)攻撃などの不正行為に影響されない安定したサービス品質の確保とコンテンツ盗聴の防止が特に重要な課題となる。

これらを実現するための基本技術としては，たとえばIP (Internet Protocol) ネットワークレベルでデータの秘匿や認証を行うIPsec (IP security) 技術[1]などがすでに実用段階にある。しかし，コンテンツの配信方法によっては既存の技術をそのまま適用できない場合がある。特にIPマルチキャスト技術を利用している場合が問題となる。IPsecなどの既存の技術はほとんどがユニキャスト通信を前提として考えられたものであり，そのままではIPマルチキャスト通信に適用できない。この問題は，インターネットプロトコルの標準化団体IETF (Internet Engineering Task Force) でも認識されており，IPマルチキャストに特化したセキュリティ技術の標準化に向けて動きだしている。しかし，IPマルチキャスト通信技術自体が未だ標準化途中ということもあり，特にIPマルチキャスト通信の基盤となるIPマルチキャスト経路制御プロトコルに対するセキュリティ機能の検討が開始されたばかりである[2]。

本研究では，IPマルチキャスト経路制御プロトコルにおいて，種々の不正行為からマルチキャスト配信システムを保護するためのセキュリティ方式の一つを提案する。

表 1 IPマルチキャスト配信システムへの不正行為の手法と対策

不正行為	コンテンツ盗聴		サービス妨害
具体的手法	回線モニタリング等によるパケット盗聴	不正な経路制御メッセージをルータに送信し，盗聴者宛のマルチキャスト経路を不正に作成	不正な経路制御メッセージをルータに送信し，サービス中のマルチキャスト経路を削除
対策	・IPマルチキャストパケットの暗号化 ・アプリケーションレベルによるコンテンツの暗号化		経路制御メッセージに認証機能を設け，ルータが不正な経路制御パケットを破棄できるようにする → IPマルチキャスト経路制御プロトコル向けセキュリティ方式

2. IPマルチキャストへの不正行為と対策

IP マルチキャストをコンテンツ配信サービスに適用する場合，特に以下のような不正行為への対策を施しておかないと，サービスがビジネスとして成り立たなくなる。

(1) 非契約者による不正なコンテンツ盗聴
(2) IPマルチキャスト配信システムへの攻撃によるサービス妨害

これらの可能性は，IPマルチキャスト通信，および，IPマルチキャスト経路制御プロトコル自身に，セキュリティを確保するための仕掛けが現状作り込まれていないことが原因の一つである。そのため，第三者がたとえば不正な経路制御パケットをルータに向けて送信することで，ルータ内のマルチキャスト経路情報を狂わせることも不可能ではない。

表1にIPマルチキャスト通信システムに対する不正行為の具体的手法と，その対策方法を整理する。

IP マルチキャストパケットの暗号化とそれに必要な鍵管理方式についてはすでに具体的な提案も行われているため[3][4]，本研究ではIPマルチキャスト経路制御プロトコルをターゲットとしたセキュリティ方式を検討した。

3. 検討方針

IP マルチキャスト経路制御プロトコルに対する不正行為を防止するためのセキュリティ機能を検討するにあたり，IPマルチキャスト経路制御プロトコルの標準化状況や最終的なシステムの運用性などを考え，今回は以下のような方針に従うことにした。

(1) マルチキャスト経路制御プロトコルには手を加えず，IP層で実現する方式とする。

マルチキャスト経路制御プロトコルには種類がいくつかある。その中で広範囲へのコンテンツ配信に適している PIM-SM (Protocol Independent Multicast -Sparse Mode) プロトコルも標準化作業段階にあり，今後変更が加えられる可能性もある。

したがって，セキュリティ機能を経路制御プロトコルの拡張として実現することは柔軟性や汎用性の面で得策ではなく，IPsec のように IP 層に実装する方向で考える。ただし，今回はマルチキャスト経路制御プロトコルとしては PIM-SM を第一のターゲットとして検討する。

(2) IP マルチキャスト配信システム構築の柔軟性をなるべく損なわないような方式とする。

PIM-SM プロトコルは，ネットワーク構成の変化に対して柔軟に対応できる機能を持っている。たとえば，ルータの追加やダウンなどは各ルータが自動的に検出し，特定の役割を持ったルータの変更なども各ルータが自動的に認識できるようになっている。つまり，システム構築時に個々のルータにあらかじめ設定しておく情報は比較的少ない。システム構築・運用面での柔軟性を保つため，セキュリティ機能の追加によって必要となるシステム構成依存の設定情報がなるべく増えないよう配慮する。

4. 経路制御パケット認証方式

マルチキャスト経路制御プロトコルに対する第三者からの不正行為を防ぐためには，経路制御パケットが以下の条件を満足するパケットであることを検証できるようにすればよい。

(1) 信頼されたルータから送信されたパケットであること
(2) パケットの送信元が詐称されていないこと
(3) パケットの改ざんが行われていないこと
(4) リプレイ攻撃によるパケットでないこと

これらの検証は，「パケットの認証値」と「シーケンス番号」を使った認証方式により実現できる。パケットの認証値とは，パケットの送信側と受信側のみが知る秘密鍵とパケットそのものを組み合わせて作った

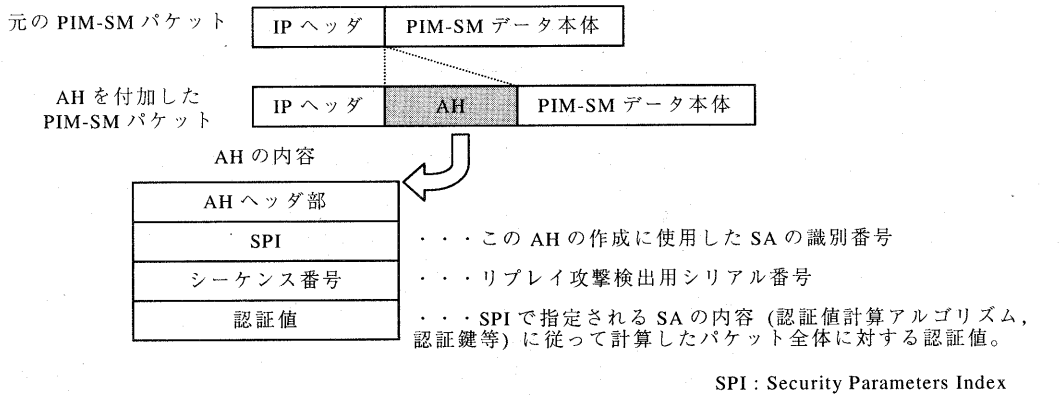

図 1　AH を付加した PIM-SM パケットフォーマット

データにハッシュ関数を適用して得られる値である。この値は秘密鍵を知らない限り正しく生成することが困難なため，パケットの改ざんや送信元認証に利用することができる。また，シーケンス番号は送信するパケットに付加する単調増加のシリアル番号で，パケットの受信側が過去に受信したパケットのシーケンス番号を管理することで第三者によって送信されたリプレイパケットを検出するものである。

前述の検討方針に従えば，これらの情報は PIM-SM メッセージの一部として付け加えるのではなく，IP 層で拡張ヘッダとして付け加える方が適している。これには認証ヘッダ (AH : Authentication Header) という仕様がすでに標準化されており[5]，マルチキャスト経路制御パケットの認証もこれで行うことができる。

AH を付加した PIM-SM パケットのフォーマットを図 1 に示す。AH は，IP ヘッダと PIM-SM データ本体の間に挿入し，IP ヘッダまで含めたパケット全体に対する認証値と，1 パケット送信毎に増加していくシーケンス番号を AH に含めることで上記四つの検証を行えるようになる。

5. 認証鍵管理方式

経路制御パケットに AH という形で認証情報を加えることは比較的容易である。一番の課題は，マルチキャスト配信システムを構成するルータの間でパケットの認証情報の作成に必要な認証鍵をどのように共有するかということである。

ここで，鍵共有方式を検討する前に，ターゲットとしている PIM-SM プロトコルがどのような経路制御情報を交換しているかを簡単に説明しておく。

PIM-SM では，隣接するルータ間で“All PIM Routers”というマルチキャストグループ宛にリンクローカルマルチキャストパケットを送信して経路情報を受け渡しを行うのが基本となっている。あるルータは，隣接ルータからリンクローカルマルチキャストにより経路情報を受け取ると，そのルータが接続される別のネットワークに対してさらにリンクローカルマルチキャストによりその経路情報を転送する。こうして，経路情報がルータ間を順次伝搬していく。また，隣接ルータ同士での生死確認もリンクローカルマルチキャストパケットにより定期的に実施される。さらに，特定の機能を割り当てられたルータ同士では，ユニキャストパケットにより情報転送を行う場合もある。

詳細なプロトコルの説明は割愛するが，認証されるべき PIM-SM プロトコルのパケットは，結局次の二種類となる。

(1) 隣接ルータ間でのリンクローカルマルチキャストパケット
(2) 特定ルータ間でのユニキャストパケット

5.1. 一括鍵設定方式

PIM-SM プロトコルでは，あるルータが経路制御情報を交換する可能性があるルータは固定的ではない。これは次の理由による。

(1) ルータが途中で参加・離脱可能なプロトコルになっている
(2) ユニキャスト通信が必要な場合，その相手はプロトコルにより動的に決まる

したがって，IPsec で一般に行われているような，各ルータが通信相手毎に鍵を設定・管理するという方法では，検討方針に示した「システム構築の柔軟性を損なわない」を満足することが難しくなってしまう。

ここで，個々の PIM-SM パケットについて何を認証すればよいかを再度検討する。上の理由に示したような PIM-SM の性質から考えると，PIM-SM パケットの

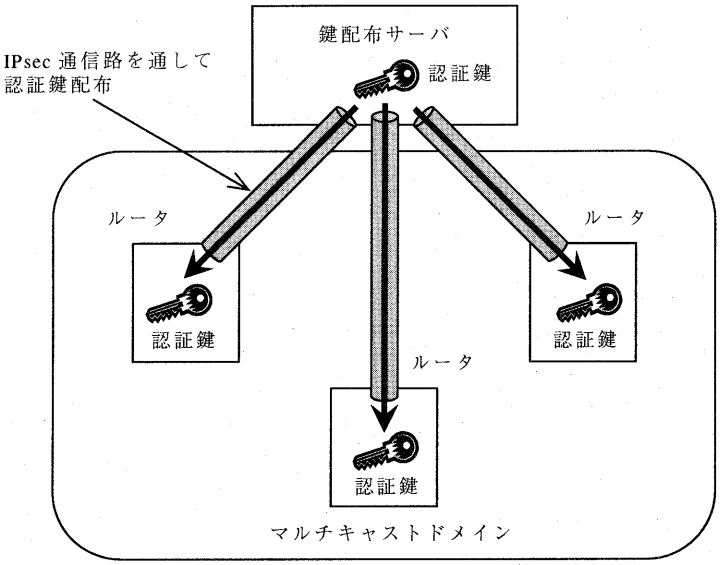

図 2　一括鍵設定方式

送信元となるルータの IP アドレスを各ルータが事前にすべて把握しておくことは困難である。最低限必要なことは，あるルータが PIM-SM パケットを受信したとき，そのパケットの送信元が同じマルチキャストドメインに属するルータであるかどうかを認証することである。

これを実現する最も簡単な方法は，同じマルチキャストドメインに属するルータが秘密情報を事前に共有し，これを認証鍵として利用する方法である。そこで，鍵共有方式の一つの案として図 2 に示すような一括鍵設定方式をまず検討した。

一括鍵設定方式は，マルチキャストドメインに対して一つの鍵配布サーバを設け，AH 作成に必要な認証鍵をその鍵配布サーバが乱数等により生成し，マルチキャストドメイン内のすべてのルータに配布する方式である。配布にあたっては，各ルータと鍵配布サーバとの間に通常のユニキャストによる IPsec 通信路を設定し，ここを通して認証鍵を盗聴されない形で配布する。また，IPsec 通信路を確立するための IPsec 鍵交換プロトコルである IKE (Internet Key Exchange) [6]は，証明書等を用いた鍵交換相手の認証機能を持っている。これにより鍵配布サーバは IPsec 通信路を確立する段階で相手ルータがマルチキャストドメイン内の正しいルータかどうかを確認するができる。すなわち，IKE がルータの装置認証の機能も兼ねる。

本方式のメリットは，簡単な設定のみで全ルータに認証鍵を安全に配布できることである。各ルータには，鍵配布サーバと IKE により IPsec 通信路を確立するための情報のみを設定しておけばよく，同じマルチキャストドメイン内に存在する他のルータに関する情報は設定しておく必要がない。つまり，検討方針(2)を満足できる。

ところが，この方式ではシーケンス番号によるリプレイ攻撃のチェックに関し，PIM-SM パケットの送信側と受信側でシーケンス番号の初期値の同期が取れないという問題点を持っている。鍵配布サーバから認証鍵と同時にシーケンス番号の初期値も配布するという方法も考えられるが，PIM-SM ではルータが途中から参加することも認めており，このルータはシーケンス番号がある程度進んだところからマルチキャストの PIM-SM パケットを受け取り始めることになる。途中から参加したルータは鍵配布サーバから認証鍵を受け取ることはできても，既に稼働中の他のルータとの間で途中まで進んだシーケンス番号の値を知ることができない。

リプレイ攻撃の防御は，ここで検討しているセキュリティ方式の重要な目的の一つであり，これに対応可能な鍵共有方式が必要である。

5.2. 個別鍵設定方式

上記の検討を踏まえ，PIM-SM プロトコルのパケット認証に必要な鍵共有方式に求められる条件を再度整理すると次のようになる。

(1) 鍵共有のための設定は最小限でマルチキャスト

ドメイン内の構成になるべく依存しないものであること (検討方針(2))

(2) PIM-SM パケットの送信側と受信側の間で，リプレイ攻撃検出に必要なシーケンス番号の同期が行えること

これを満足する方式として，図3に示すような個別鍵設定方式を考えた。

個別鍵設定方式は，鍵配布サーバが直接認証鍵を生成するのではなく，その元となるマスタ鍵を生成・配布し，ルータ同士がそのマスタ鍵を利用しながら個別に情報交換を行って実際の認証鍵を生成するという方式である。すなわち，次の2ステップで認証鍵配布が完了する。

(1) 鍵配布サーバからのマスタ鍵配布
(2) ルータ同士による認証鍵配布

シーケンス番号は認証鍵と対応づけて管理される番号なので，認証鍵を配布する際にシーケンス番号の同期も行うようにすればよい。以下，各ステップ毎にその概要を説明する。

5.2.1. マスタ鍵配布ステップ

マスタ鍵と言っても実体は認証鍵と同様の乱数値であり，マスタ鍵配布の動作は一括鍵設定方式における認証鍵配布と全く同じにできる。IPsec 通信路を事前に設定し，そこを通して配布することでセキュリティを確保する。鍵配布サーバが行うルータの認証もこのIPsec 通信路設定時に IKE の中で行われる。

5.2.2. 認証鍵配布ステップ

各ルータは，配布されたマスタ鍵を用いて隣接ルータとの間で情報交換を行い，そこで使用する認証鍵の配布とシーケンス番号の初期値の通知を相互に行う。この時，隣接ルータのアドレスはお互いに認識していないが，情報交換の最初のメッセージを”All PIM Routers” 宛のマルチキャストデータグラムとして送信することで処理を開始できる。PIM-SM プロトコルの中で特定のルータとの間でユニキャスト通信が必要となった場合は，そのルータとの間で同様の情報交換を行って認証鍵を生成する。

5.2.3. 認証鍵配布ステップのセキュリティ

ところで，ルータ間で認証鍵配布のための情報交換する際，PIM-SM プロトコルを開始する前の状態では

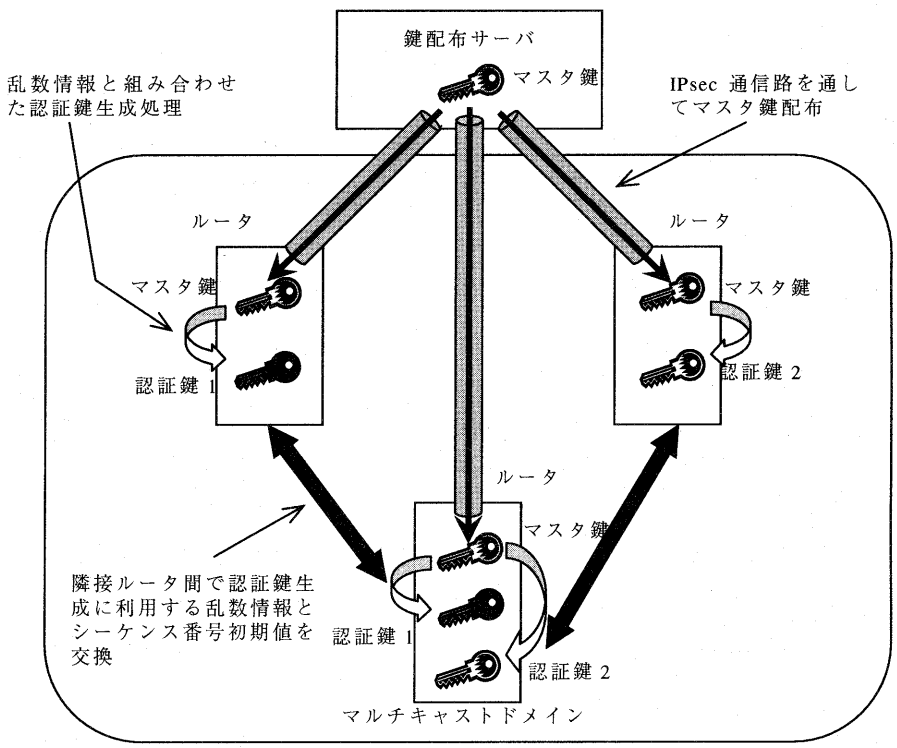

図 3 個別鍵設定方式

お互いに相手ルータの IP アドレス等の情報を持っていないことや，この情報自身がマルチキャストで配布されるなどの理由により，ルータ間でのセキュリティ確保に IPsec が使えない。そのため，この情報交換プロトコル自体に盗聴，改ざん等に対応するためのセキュリティ機能が必要となる。しかし，これは，マルチキャストドメインに属するルータしか知らない秘密のマスタ鍵が存在するという前提により，次のような方法で実現可能である。

(1) 盗聴対策

ルータ間で交換する情報の中で秘匿が必要なのは認証鍵である。ここではマスタ鍵が存在することを利用し，任意の乱数とマスタ鍵を連結したデータのハッシュ値を認証鍵として利用する方法が考えられる。これにより，上記の乱数を第三者に見られてもマスタ鍵を知らない限り，そこから生成される認証鍵を推測することは困難になり，情報を特に暗号化することなく送信することができるようになる。

(2) 改ざん・偽造パケット対策

ルータ間で交換する情報に対してマスタ鍵を認証鍵として計算した認証値を付加する方法で対策可能である。

(3) リプレイ攻撃対策

ここではシーケンス番号によるリプレイパケット検出を利用できないので，任意の乱数データ (Nonce データ) を情報交換の一連のシーケンス識別子として利用する。同様の方法はたとえば IKE でも用いられている。情報交換を行う両側のルータがシーケンス中の最初のメッセージ送信時に乱数を生成して付加し，以後シーケンスが完了するまで同じシーケンス番号を付加し続けることで，リプレイ攻撃により不正にシーケンスを実行してしまうことを防ぐことができる。

6. プロトコルエンティティ構成案

以上の議論から，IP マルチキャスト経路制御プロトコル向けのセキュリティ方式としては，

(1) IPsec AH に準拠したパケット認証方式
(2) 個別鍵設定方式による認証鍵管理

を併用した方式を提案する。

現在，上記の個別鍵設定方式に準拠した認証鍵管理プロトコルを詳細設計中である。プロトコルとして実装する際のエンティティ構成は図 4 のような形を考え

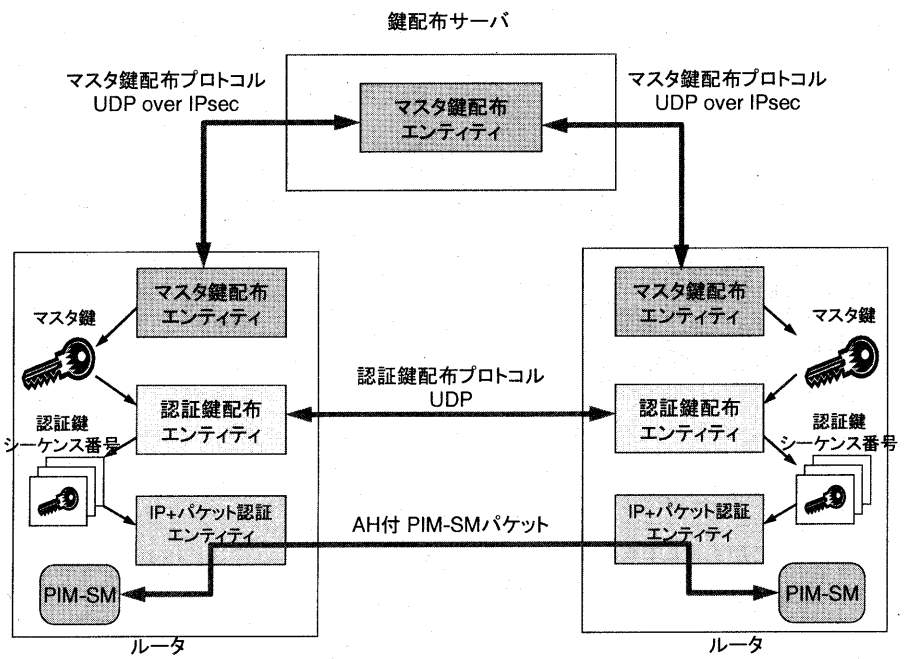

図 4　プロトコルエンティティ構成案

ており，各エンティティ間で交換するメッセージ内容やその手順の詳細を検討中である。

7. まとめと今後の課題

インターネット上でのデジタルコンテンツ配信サービスの普及に伴い，特に放送型コンテンツ配信で重要性が増すと見込まれる IP マルチキャスト通信システムに関し，そのサービスとしての品質確保に必要なマルチキャスト経路制御プロトコル向けセキュリティ方式を検討し，以下のような提案を行った。

(1) 種々のマルチキャスト経路制御プロトコルへの柔軟に対応するため，IPsec の AH と同一の形式で認証情報を IP 層で付加する。
(2) 各ルータが認証情報の作成に利用する認証鍵の配布方式として，シーケンス番号によるリプレイ攻撃検出に対応可能な個別鍵設定方式を採用する。

今後は，このセキュリティ方式を実装したプロトコルの設計とプロトタイプ開発を行い，マルチキャストデータ配信を行う実験システムに適用して，セキュリティ上の脆弱性の有無や問題点の検証を進めることが課題である。

文　献

[1] S. Kent, R. Atkinson, “Security Architecture for IP”, RFC 2401, November 1998.

[2] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, “Protocol Independent Multicast - Sparse Mode (PIM-SM)”, IETF, draft-ietf-pim-sm-v2-new-05.txt, pp.129-133, March 2002.

[3] M. Baugher, T. Hardjono, H. Harney, B. Weis, “The Group Domain of Interpretation”, IETF, draft-ietf-msec-gdoi-04.txt, February 2002.

[4] M. Baugher, R. Canetti, L. R. Dondeti, F. Lindholm, “Group Key Management Architecture”, IETF, draft-ietf-msec-gkmarch-02.txt, February 2002.

[5] S. Kent, R. Atkinson, “IP Authentication Header”, RFC 2402, November 1998.

[6] D. Harkins, D. Carrel, “The Internet Key Exchange (IKE)”, RFC 2409, November 1998.