マルチキャスト通信上での効率的な鍵配布方式に関する検討

朴 美娘†, 岡崎 直宣†, 井手口 哲夫††
†三菱電機(株)情報技術総合研究所 ††愛知県立大学情報科学部

インターネット上で多地点における多数のユーザに同時に同じ情報を配信するサービスを実現するための手段として，IPマルチキャスト通信が利用されている．しかし，IPマルチキャスト通信では，特定のグループ内の安全なグループ通信を実現するためのセキュリティ確保が重要な課題になっている．本稿では，ネットワーク上でダイナミックグループ暗号通信を実現する際のセッション鍵の共有方式について検討し，鍵配送センタの処理負荷を減らすと共に通信ネットワークの通信量を減らし，さらに鍵配送時のセキュリティを高める鍵配布方式を提案する．本方式では，広域ネットワークのトポロジーに注目してネットワークのLANセグメントごとに任意の代表者を選んで，鍵配布・更新依頼に対する応答メッセージをまとめて鍵配送センタへ送ることによって，大規模システムの鍵配布・更新時間が短くなり，データ通信への影響を少なくすることができることを示す．さらに，グループ通信のメンバ構成を変更したり，グループ通信中，新たなユーザが新規に参加したり，途中で抜け出したりすることができるダイナミックセキュア通信グループを実現可能にするためのグループ暗号鍵管理モデルを定義する．

An Efficient Key Distribution Method for a Secure Communication Groups

Mirang PARK†, Naonobu OKAZAKI† and Tetsuo IDEGUCHI††
†Information Technology R&D Center, Mitsubishi Electric Corporation
††Faculty of Information Science and Technology, Aichi Prefectural Univ.

IP multicasting played an important role to realize multi-point multi-user applications on the Internet. Many enterprise networks require flexible group communications on the Internet. When we develop these systems on IP multicast networks, the various types of security threats will be occurred. As a result, the constructions of secure communication group that protect users from intrusion and eavesdropping are very important matters. In this paper, we discuss an efficient key distribution method for a secure communication group over the multicasting protocol.

1. はじめに

インターネット上で多地点における多数のユーザに同時に同じ情報を配信するサービスを実現するための手段として，グループ管理を行うプロトコル[1]（IGMP : Internet Group Management Protocol）と，グループ全員へマルチキャストパケットを効率的に配信するマルチキャストルーティングプロトコル[2]が提案されている．IGMPでは，情報の受け手がそのマルチキャストグループに加わるかどうかを選択する．すなわち，配信されてくる情報を受け入れるか廃棄するかを受け手が自由に選択できるようになっている．このことは，誰もがグループアドレスに加わるだけで，マルチキャストパケットを受信できてしまうというセキュリティ上の問題がある．また，正規の情報配信者になりすまし，マルチキャストグループ宛てに偽の情報を配信する危険性がある．従って，マルチキャストグループ通信を行う場合には，セキュリティの問題が大きな課題になっている．そこで，特定のグループメンバだけがマルチキャストグループ通信にアクセス可能にする暗号通信を実現する技術が求められている．そのためのマルチキャスト通信では，グループ暗号通信のための鍵管理の問題が重要な課題になっており，現在研究が進められている[3-9]．IETFなどでは，OFT(One-way Function Tree)に基づいたグループ暗号鍵管理方法および管理プ

ロトコルを提案している[3-7]. これらのアルゴリズムは，小規模のグループ暗号通信には簡単に適用できるが，大規模のグループへの適用には課題がある．また，論理的な鍵の階層構造(LHC: Logical Key Hierarchy)を導入し，大規模システムにおけり鍵のスケーラビリティ問題を解決するための議論もなされている[8,9]. このうち[8]では，全体のグループをいくつかのサブグループに分け，そのサブグループ内で鍵を共有するような構造を提案している．従って，グループへのユーザのjoin/leaveに伴う鍵更新は，そのユーザが属するサブグループだけに再配布する．また[9]では，[8]のグループ構造に基き，各ユーザが持つ鍵をユーザの固有鍵，ユーザが所属するサブグループ鍵および全体のグループ鍵とに階層構造化している．ユーザのjoin/leaveに伴う鍵更新時は，そのユーザが属するサブグループ鍵と新たなユーザへのユーザ固有鍵だけを配布する．これらの方式においては，階層構造を用いることによって，ユーザのjoin/leaveに伴うグループへの鍵配布のスケーラビリティ問題における性能の向上を図っているのが共通点である．しかし，鍵配布に伴う鍵更新時のシステムの動作，UDPプロトコルを用いるマルチキャスト通信の不到達性，複数グループの存在については考慮してない．

筆者らは複数グループが存在するグループ暗号通信における，鍵更新時のシステムのデータ通信への影響を考慮した鍵配布方式を提案した[10]. ここでは，鍵の混在に伴うシステムの誤動作を避けるためにシステムを一時停止している．そこで，システム動作の一時停止時間を短くし，データ通信への影響を少なくするためのマルチキャスト鍵配布方式を提案した[11,12]. ここでは，複数グループへの鍵配布の通信トラヒック問題を避けるために，各端末への鍵配布はユニーキャストで確実に行い，鍵更新通知をマルチキャストで行うようにしている．しかし，IPマルチキャストでは，ネットワークのエラー等によって各メッセージが定められた時間内に届かなかった場合には，メンバ宛てに再送処理を行う必要があるので，鍵の更新に時間がかかることや，通信トラヒックの集中が課題となっていた．

本研究では，このような問題を解決するために，広域ネットワークのトポロジーに注目し，隣接したホスト同士をまとめたLANセグメント上にプロキシサーバの役割をする代表メンバを決め，そのLANセグメント上の各応答メッセージをまとめて鍵管理サーバへ返す方式を提案する．さらに，ＩＰマルチキャスト上のセキュリティ問題を解決するために，配布鍵をそれぞれのメンバのマスター鍵で暗号化して配布している．

以下，２．ではマルチキャスト通信のセキュリティの課題と，解決策について述べる．そして，３．ではセキュアマルチキャスト通信での鍵管理方法について議論し，マルチキャスト鍵配布方式を提案する．４．はまとめである．

2. セキュアマルチキャスト通信

ここでは，マルチキャスト通信におけるセキュリティの問題点と解決策について述べる．

2.1 IP マルチキャスト通信の課題

現在，マルチキャストルーティングプロトコル[2]が実装されているマルチキャストルータが実現されつつある．マルチキャストルータによって構築されているインターネット上で，ホスト-ルータ間のグループ管理を行うプロトコルとして定められているIGMP[1]の動作は，次のような特徴を持つ：

・各グループは，一つのIPアドレスによって識別される．
・グループの規模は任意である．
・グループのメンバは，インターネット上の任意の場所にあってよい．
・グループのメンバは，いつでもグループへの参加やグループからの離脱ができる(receiver-oriented).

これらは，大規模なネットワークシステムにおいて，グループ通信を効率よく行うために非常に都合がよい．但し，最後のreceiver-orientedなプロトコルであるという点については，誰もがグループアドレスに加わるだけで，マルチキャストパケットを受信できてしまうというセキュリティ上の観点からの大きな課題になっている．例えば，課金を伴うコンテンツ配信サービスなどにおいて登録メンバ以外にコンテンツを無料で盗み見される可能性がある．また，グループのメンバ以外の者がマルチキャストパケットを送信することができるという問題もある．

2.2 解決策

上記のIPマルチキャスト通信上でのセキュリティ問題を解決し，安全なグループ通信を実現するための解決策として以下のものが考えられる．

（１）アクセス制御

登録されたマルチキャストグループのメンバだけがマルチキャストグループ通信にアクセス可能にする．

（2）ソース情報認証

受け取ったマルチキャストパケットが正規のソース情報を偽造したものでないことを検証する．

本研究では，既存のIPマルチキャストのネットワーク構造をそのまま用いて，端末側に暗号機能を持たせることによって，マルチキャストグループ暗号通信を実現させる方法について検討する．特に，上記（1）のアクセス制御を実現させるために，登録されたメンバだけが共通の暗号鍵を用いて暗号通信を可能にするための鍵配布方式について検討する．

2.3 マルチキャストグループ暗号通信における鍵配布方式

筆者らは，図1で示すようにマルチキャストグループ暗号通信における鍵配布方式を提案した[11,12]．本方式は，グループ全員に共有するセッション鍵を更新する際のシステム動作の一時停止時間[10]を短くし，データ通信への影響を少なくするために検討したものである．しかし，IPマルチキャストでは，各端末に鍵配布・鍵更新依頼メッセージ（key change）が届く保証がないので，確認応答メッセージ（acknowledge）をグループメンバそれぞれ個別にグループ管理者にユニキャストで送信する．ここで，ネットワークのエラー等によって各応答メッセージが定められた時間内に届かなかった場合には，メンバ宛てに再送処理を行う必要があるので，鍵の更新に時間がかかることや，通信トラヒックの集中が課題となっていた．

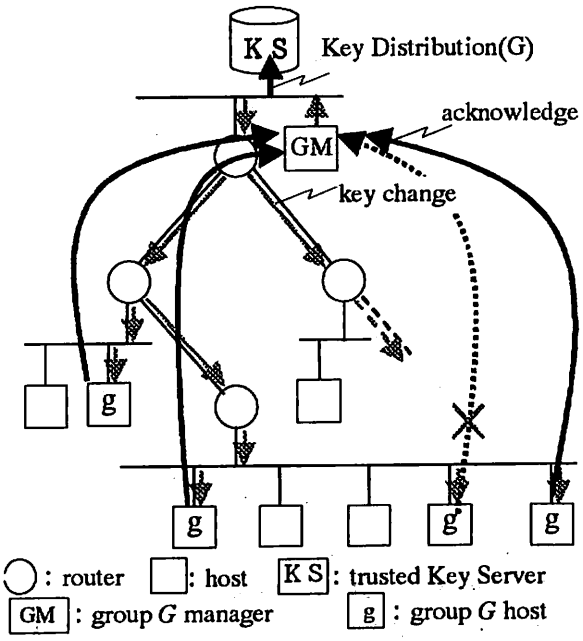

図1　従来の鍵配布方式

本研究では，このような問題を解決するために，隣接したホスト同士をまとめたLANセグメント上にプロキシサーバの役割をする代表メンバを決め，そのLANセグメント上の各応答メッセージをまとめて鍵管理サーバへ返す方式を提案する．さらに，各グループごとのセッション鍵を管理し配布する鍵管理サーバと，ユーザのjoin/leaveに伴うダイナミック鍵更新要求や各応答メッセージのやりとりはグループ管理者がまとめて行うようなグループ鍵管理モデルを定義する．

3.マルチキャストグループ暗号通信の鍵管理方式

マルチキャスト通信が可能な広域ネットワーク上で複数のグループに対する鍵配布・更新を安全かつ迅速に行うための，グループ暗号鍵管理モデルを定義し，そのモデルに基づきデータ通信への影響を少なくするための効率的な鍵配布方式を提案する．

3.1 グループ暗号鍵管理モデル

複数の暗号通信グループが存在するネットワーク上で，各通信グループへの鍵配布・更新を行うための，グループ暗号鍵管理モデル（GKM: Group Key Management model）を以下のように定義する．

【定義1】GKM＝（KS，CGs）

KS(trusted Key Server)：信頼される鍵管理サーバとして，グループ暗号通信を希望するユーザに鍵を配送する．KSは安全な場所に設置してあるものとする．

CG(secure Communication Group)：マルチキャスト暗号通信を希望するメンバで構成される通信グループ．

【定義2】KS＝（GID，U，G，K_s）

GID：通信グループを識別するためのグループ識別子．

U＝ $\{u_1, u_2, \cdots u_n\}$ ：マルチキャストパケットを受け取り可能なすべてのホストユーザ，

G＝ $\{g_1, g_2, \cdots g_m\}$ ：ホストユーザの中でマルチキャストグループに属するメンバ（$G \subseteq U$），

K_s：グループGのセッション鍵．

【定義3】CG＝（GID，G，GM）

GID：通信グループを識別するためのグループ

識別子．ここでは，グループ識別子とマルチキャストアドレス(MA)を一対一に対応付ける．
G：ホストユーザの中でマルチキャストグループに属するメンバ，
GM:マルチキャストグループメンバへの鍵配送を鍵管理サーバ（ＫＳ）に要求したり，鍵更新要求を出すグループ管理者（GM∈G）．□

以上の定義に基づき，マルチキャスト暗号通信グループを生成する方法を次のように定める．

【マルチキャスト暗号通信グループ生成法】

(1)鍵管理サーバKSにマルチキャスト暗号通信を希望するメンバのグループリスト（G）を作成し，グループ識別子(GID)とマルチキャストアドレス(MA)を割り当てる．

(2)グループメンバの中にグループ管理者(GM)をおく．グループメンバはそれぞれ異なるマスター鍵を持ち，自分が属しているグループ識別子とマルチキャストアドレスを知っているものとする．□

3.2 効率的なマルチキャスト鍵配布方式

図２に提案する鍵配布方式の概要を示し，図３に鍵配布シーケンスを示す．本方式では，安全で確実な鍵配布を行うために，配布する鍵は暗号化して各メンバにユニキャストで配布する．配布時の暗号方式としては，公開鍵暗号と秘密鍵暗号どちらでもよいが，以下では秘密鍵暗号を用いた方式を示す．また，ダイナミックな鍵更新に伴うネットワークの通信トラヒックの集中を減らすために，各暗号通信グループの管理者(GM)が鍵更新依頼メッセージをグループ全員へマルチキャストで出している．従って，鍵管理サーバへの通信トラヒックの集中問題を改善している．

【効率的なマルチキャスト鍵配布方式】

<u>・STEP１：セッション鍵配送</u>

(1-1) GM→ KS： *DIS_REQ*（GID,G）

GKMで定義されている暗号通信グループCGのグループ管理者(GM)は，鍵管理サーバ(KS)にグループIDとグループメンバリストGへのセッション鍵配布を依頼する．

(1-2) KS→G：*KEY_DIS*（GID, $[K_s]_{Egi}$）

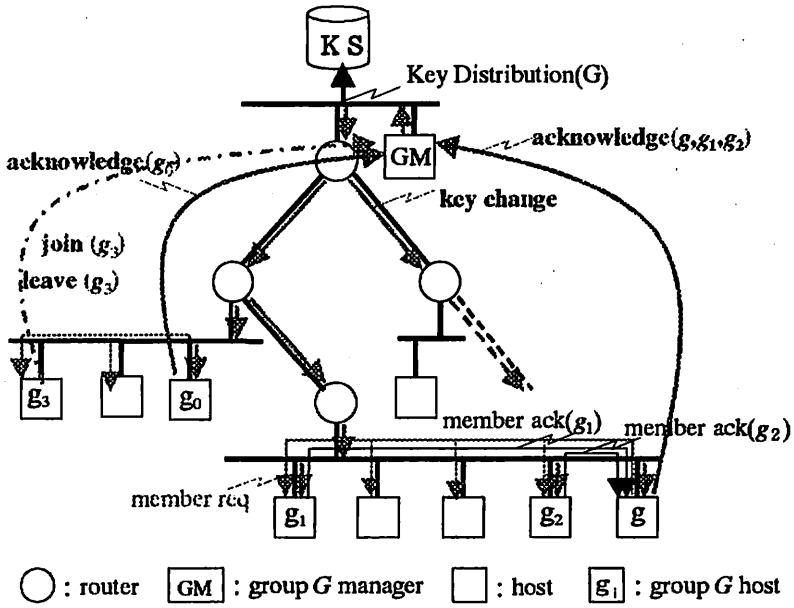

図2　提案する鍵配布方式

KSは，登録GIDとグループGとの確認を行い，グループGの各メンバ(g_i)の持っているマスター鍵でセッション鍵（K_s）を暗号化して各メンバにユニキャストで配布する．

(1-3) G→ KS: *K_ACK*（g_i）

セッション鍵（K_s）を受け取ったグループの各メンバ（g_i）は自分のマスター鍵で復号し，KSにセッション鍵受信応答を返す．

(1-4) KS→ GM：*DIS_ACK*（G）

すべてのメンバからセッション鍵受信応答を受け取ると，KSはGMにセッション鍵配布完了通知を送る．

<u>・STEP２：セッション鍵の更新</u>

(2-1) GM→G：[*C_REQ*（G）]E_{Ks}

GMは，グループGのMA宛に鍵更新要求メッセージ（*C_REQ*）をセッション鍵K_sにより暗号化してIPマルチキャストにより一斉に送信する．従って，STEP１でKSからセッション鍵K_sを配布されたグループメンバ以外のユーザが不正にアクセスすることを防ぐことができる．

(2-2) g∈G：（*C_REQ*（G））

グループGはGMから送信された鍵更新要求メッセージを受け取ると，同セッション鍵により復号する．上記の鍵更新要求メッセージの応答メッセージを迅速に返すために，ネットワークの各LANセグメント上のグループメンバから代表メンバgを選ぶ．

(2-3) g→ g_i：[*MEM_REQ*]E_{Ks}

代表メンバgは同セグメントのメンバに対する鍵更新依頼メッセージの確認応答メッセー

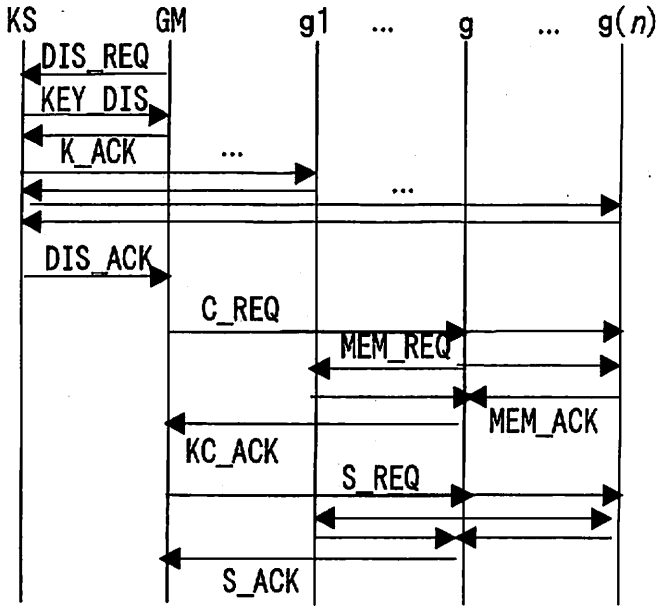

図3　マルチキャスト鍵配布シーケンス

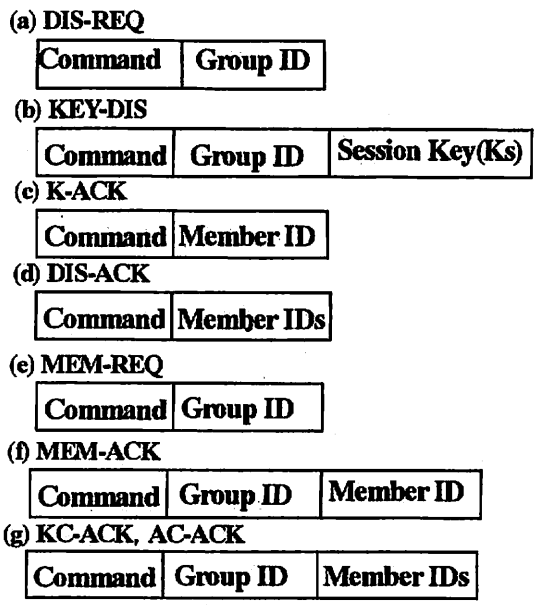

図4　鍵配布コマンドフォマット

ジの送信要求（member req）をセッション鍵K_sにより暗号化してLANセグメント上に送信する．

(2-4) $g_i \rightarrow g$: $[MEM\_ACK(g_i)]E_{Ks}$

各セグメント上の各グループメンバg_iは，暗号化された鍵更新依頼メッセージの確認応答メッセージの送信要求を受け取ると，同セッション鍵により復号する．そして，自分のメンバ識別子と共に確認応答メッセージ（member ack(g_i)）をセッション鍵K_sにより暗号化して代表メンバgに送る．

(2-5) $g \rightarrow$ GM : $[KC\_ACK]E_g$

各セグメント上の代表メンバgが一定時間内にセグメント上のGの各メンバからの確認応答メッセージを受信したら，その応答メッセージに含まれるメンバ識別子（g_i）と自分のメンバ識別子(g)を含む確認応答メッセージ（acknowledge(g, g_i, g_j)）をgの持つ秘密鍵により暗号化してGMに送信する．

(2-6) GM$\rightarrow g_i$: $[C\_REQ\ (g_i)]E_{Ks}$

各セグメントの代表メンバから鍵更新確認応答メッセージを受け取ったGMは，応答メッセージが来なかったグループメンバ(g_i)へユニキャストで鍵更新要求メッセージ（C_REQ）をセッション鍵K_sにより暗号化して再送信する．

この再送要求に対する応答メッセージが来なかった場合は，グループからの離脱として見直し，そのメンバをグループから外すことにする．GMは，グループメンバリストを再作成し，KSにメンバ更新登録を依頼する．

(2-7) GM$\rightarrow$G : S_REQ (G)

GMはすべてのグループメンバからの確認応答メッセージ(KC_ACK)を受け取ると，配布した新しいセッション鍵によるデータ転送開始要求（S_REQ）をIPマルチキャストで送信する．

(2-8) $g \rightarrow$GM : $S\_ACK\ (g_i)$

グループメンバは，S_REQを受け取ると，新しいセッション鍵を用いてデータ転送を再開し，KC_ACKの返し方と同様にセグメント上の応答を代表がまとめてGMにデータ転送開始応答（S_ACK）を送る．□

以上で示した鍵配布プロトコルにおける各コマンドパケットフォマットを図4に示す．

3.3 ダイナミックグループ鍵配布方式

次に，グループ通信のメンバ構成を変更できるダイナミックセキュア通信グループを実現可能にするためのグループ暗号鍵配布方式について検討する．ここでは，グループ通信中に，新たなメンバがグループGへ参加する場合と，通信途中グループからメンバが離脱する場合のセッション鍵配布方式について述べる．

(1)メンバの追加(join)時の鍵配布方式

ユーザmがグループGに新たに加わる場合，グループ暗号鍵配布方式は次のようになる．

・mはGMにグループへのjoinを要求する．

・GMがメンバの追加を承認する場合は，ユーザmに追加承認応答をし，KSにグループの追加メンバmを登録し，mに対するマスター鍵と現

在のセッション鍵配布を依頼する．
・KSは，メンバmにユニキャストでセッション鍵K_sを送る．

(2)メンバの脱退(leave)時の鍵配布方式

グループGのメンバkがグループから脱退する場合の鍵配布方式は，次のようになる．
・kはGMにグループからの脱退を要求する．
・GMはKSにkを除いたグループのメンバを登録し，セッション鍵更新を依頼する．
・以降は提案の鍵更新方式と同様に新しいセッション鍵の配布，更新を行う． □

3.4 提案方式の評価

本論文で提案した方式による通信トラヒックについて簡単な評価を行う．ここでは特に，セッション鍵の更新の手順に要するGMに対する送受信に関して考察する．

あるグループについて，グループのメンバを有するLANセグメントの数をm，各LANセグメントにおけるグループのメンバの数をn，GMから各メンバへのメッセージの不達率をkとする．ただし，ここでは広域ネットワーク上の各グループメンバ宛のメッセージについて一様な確率で不達が発生するものとする．従来の手法（図１）ではセッション鍵の更新の手順に要するGMに対する送受信の回数は$1+mn+2kmn$である．一方，提案手法（図２）では各グループの代表メンバが一括して応答を送信するため，GMに対する送受信の回数は $1+m+2kmn$となる．ただし，ここでは両手法とも再送時にはユニキャストによる送受信をするものとする．ここで，不達率kが十分小さい（$1/k \cong 0$）と仮定すると，従来の手法に対する提案手法のトラヒックの比は$O((1+m+2kmn)/(1+mn+2kmn)) \cong O(1/n)$となる．

この結果より，提案した手法は，企業ネットワークのような，一つのLANセグメント上に多数のノードが存在するような構成のネットワークに対して有効であると考えられる．

4. まとめ

本稿では，暗号通信グループに所属する暗号機能を持った端末を利用するグループメンバや暗号ゲートウェイ間で暗号に用いるセッション鍵を容易な手順で共有することを目的とし，鍵配送センタの処理負荷を減らすと共に通信ネットワークの通信量を減らし，さらに鍵配送時のセキュリティを高める鍵配布方式を提案した．また，グループ通信中，ユーザが自由にそのグループに参加したり，途中で脱け出したりすることができるダイナミック性を実現するセッション鍵配布方式を提案した．本方式を実現することによって，鍵更新におけるスケーラビリティを改善し，迅速かつ安全な鍵配布・更新を行うことが出来ることを示した．

本方式に基づいたグループ暗号通信システムを構築することによって，ネットワーク側の負荷が軽くなり，ユーザはより柔軟なサービスを授受できるようになると期待される．

参考文献

[1] B.Cain, S.Deering, "Internet Group Management Protocol, Version 3,"IETF, Internet Draft, Feb. 1999.

[2] J.Moy, "Multicast Routing Extensions for OSPF," *Commun. ACM*, vol.37, no.8, pp.61-66, Aug.1994.

[3] T.Hardjono, B.Cain, N .Doraswamy, "A Framework for Group Key Management for Multicast Security," IETF, Internet Draft, Aug. 1999.

[4] D.M.Wallner, E.J.Harder and R.C.Agee, "Key Management for Multicast: Issues and Architectures," IETF, Internet Draft, Sep. 1998.

[5] D.Balenson, D.McGrew and A.Sherman, "Key Management for Large Dynamic Groups:One-Way Function Trees and Amortized Initialization," IETF, Internet Draft, Feb. 1999.

[6] H.Harney and C.Muckenhirn, "Group Key Management Protocol(GKMP) Architecture" RFC 2094, July 1997.

[7] H.Harney and C.Muckenhirn, "Group Key Management Protocol(GKMP) Specification" RFC 2093, July 1997.

[8] Suvo Mittra, "Iolus: A Framework for Scalable Secure Multicasting" In *Proceedings of ACM SIGCOMM'97*, 1997

[9] Chung Kei Wong, Mohamed Gouda, and Simon S.Lam, "Secure Group Communication Using Key Graphs" In *Proceedings of ACM SIGCOMM'98*, 1998

[10] M.Park, et al, "Proposal of a Key Sharing Method for Secure Communication Systems," TJCOM98, p113-118, 1998.

[11] 朴 美娘，渡邊 晃，岡崎 直宣，井手口 哲夫：セキュアマルチキャスト通信方式に関する検討，DICOMOシンポジウム, p309-315, 1998.

[12] 朴 美娘，渡邊 晃，岡崎 直宣，井手口 哲夫：セキュアマルチキャスト鍵配布方式に関する検討，電子情報通信学会 ソサイエティ大会,B-7-107, 1998.