コンピュータセキュリティ 9－5
（2000．5．10）

グループ暗号通信の鍵供託方式に関する一考察

朴 美娘，井上 徹
（株）高度移動通信セキュリティ技術研究所（AMSL）

インターネット上でECを始め国際間の金融取引等様々なビジネスが盛んに行われつつあることによって，これらのサービスを利用するユーザを守るために法律的に定められた監視システムなどが必要になってきている．本研究では，インターネット上で多地点における多数のユーザにデータ転送サービスを行うグループ暗号通信において，鍵供託サービスを提供可能にする鍵供託スキームについて検討する．特に，大規模のグループ通信において，ネットワークリソースを効率よく利用できるIPマルチキャスト通信フラットフォームを利用した鍵供託システムの構築に関する考察を行う．ここでは，捜査機関が捜査対象のグループ通信メンバの一員になることによってリアルタイムにアクセス可能になり，グループ暗号通信のセッション鍵がダイナミックに更新しても鍵を供託できると共に，裁判所から許可された傍受期間が終わると自動的にグループから削除されることによって，無制限な盗聴を防ぐことができプライバシー保護ができるグループ暗号通信鍵供託モデルを提案する．

A Study of a Key Escrow System to Group Communications

Mirang PARK, Toru INOUE
Advanced Mobile Telecommunications
Security Technology Research Laboratories Co., Ltd

If the Internet and other public networks, such as mobile telecommunications networks, are to be used for commerce, then in many cases privacy for confidential user information is required. Typically a certain legal agency wishing to intercept the communications of a suspected criminal can do so if granted a warrant from a judicial authority. In this paper, we discuss about a key escrow scheme for a secure communication group, which is satisfied with the requirements for legal interception. The idea of such a scheme is that an interception agency becomes an inner member of a suspected group, when an agency is given authorization to intercept a particular group communications. Therefore, interception agency can escrow a session key near-real-time access when a warrant is held.

1. はじめに

今までの暗号システムというのは，ある特定の機関の秘密情報を守るための特定の暗号アルゴリズムに基づいた非公開のものであった．しかし，現在，インターネットが世界各国に普及することによって，EC を始め国際間の金融取引等様々なビジネスが盛んに行われつつあり，暗号通信システムというのは一般的になって行くと考えられる．

また，モバイル端末の普及に伴い，インターネット上で多地点における多数のユーザによるグループ暗号通信が注目を集めている．特に，ユーザが移動しても同じグループ暗号通信が可能になることは，グループ暗号通信の大きな魅力になっている．このようなグループ暗号通信を善良の一般ユーザだけではなく，麻薬取引などの犯罪グループが利用する可能性は大きい．従って，これらのサービスを利用するユーザの利益を守るために法律的に定められた監視システムなどが必要になってきている．本研究では，モバイル端末などを含むインターネット上で多数のユーザにデータ転送サービスを行うグループ暗号通信において，鍵供託サービスを提供可能にする鍵供託スキームについて検討する．特に，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ことができる IP マルチキャスト通信フラットフォームを利用した鍵供託方式に関する考察を行

う．

従来の鍵供託システム[7,8,11,12]は，主にユーザ間通信を対象にしている．これらの研究では，鍵の生成と保管機関の分散化[7,8]，捜査機関の無制限な盗聴を防ぐための方式[11]やユーザのプライバシーを考慮した方式[12]が提案されている．これらの方式においては，暗号アルゴリズムの安全性に関する考察は行われているが，通信フラットフォームを考慮したシステムの実現性や実際のネットワーク上で盗聴効率性については具体的に述べられてない．

一方，グループ暗号通信においては，外部からのセキュリティを確保するためグループ内で使われている暗号鍵の更新を頻繁に行う必要がある．また，グループメンバ構成がダイナミックに変更可能なダイナミックグループ暗号通信においては，鍵のスケーラビリティ問題を解決する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[3,4,5,10]．

本報告は，このような鍵更新が頻繁に行われるダイナミックグループ暗号通信における鍵供託方式について考察した結果をまとめたものである．そこで，インターネット上で暗号通信サービスを提供するサービス提供者（SP：Service Provider）と同様に信頼される第三者機関（TTP：Trusted Third Parties）でグループ暗号通信の鍵管理および鍵供託サービスを提供可能にする鍵供託スキームを提案する．このスキームに基づいた鍵供託システムでは，捜査機関がグループメンバに知れずにグループの一員になることによって，グループ暗号通信システムのグループ暗号鍵がダイナミックに変わっても鍵を供託でき，通信傍受が可能になると共に裁判所から許可された盗聴期間が終わると自動的にグループから削除されることによって無制限な盗聴を防ぐことができプライバシー保護ができる．

以下，2章ではマルチキャストグループ暗号通信の構築法と問題点について述べる．そして，3章でグループ暗号通信における鍵供託方式およびそれに基づいたシステム構築法について議論する．

2. マルチキャストグループ通信

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[1]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[2]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．

本研究では，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に既存の 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すると仮定する．そして，そのマルチキャストグループ暗号通信を悪用するものから守るサービスを提供するための，グループ暗号鍵供託方式について検討する．

2.2 グループ暗号通信構築法

暗号によりグループ通信を構築する手法としては，パス定義方式とエリア定義方式がある[9]．パス定義方式においては，グループメンバの対毎に異なるセッション鍵を保持し，グループ管理者がそれらをすべて管理する．セッション鍵は通信セッションの開始時に通信を行うグループメンバ間でやり取りされるのが一般的である．この方式では，すべての通信パスが異なる鍵を持つより柔軟なシステムの構築が可能であるが，セッション鍵の管理の負荷が大きく，小規模なシステムに適用が限定される．一方，エリア定義方式においては，グループメ

ンバ間で共通のセッション鍵を共有する．セッション鍵はあらかじめ（通信セッションとは独立のタイミングで）配布しておく．この方式は，セッション鍵の管理が容易で，大規模なシステムにも適用できる．従って，本稿では，エリア定義方式によるグループ暗号通信を鍵供託の対象として考える．エリア定義方式によるグループ通信においては，セキュリティの観点からセッション鍵を定期的に更新する必要がある．また，グループの構成が変化する際にもセッション鍵の更新が必要になる．

3．グループ暗号通信の鍵供託システム

以下では，グループ暗号通信における鍵供託システムを構築するための要求仕様をまとめ，その要求を満たすための鍵供託モデルおよびシステムを提案する．

3.1 鍵供託システム要求仕様

鍵供託システムの主な機能は，次のようになる．

(1) 傍受の許可：
捜査機関などがある通信を傍受するためには，国から定められた裁判所から傍受許可証を受け取らなければならない．

(2) データ回復：
暗号鍵を用いて暗号文から平文への復号を行わなければならない．

(3) プライバシー保護：
ユーザのプライバシーを保護するために，捜査機関の無制限な盗聴を防がなければならない．

現在，このような機能を実現するための１対１通信を対象にした鍵供託方式について研究が行われいくつかの提案がなされている[7,8, 11, 12]．これらの方式においては，結託防止のための鍵保管機関の分散化，無制限な盗聴を防ぐために鍵を捜査機関に直接渡さないなど鍵を供託する際の暗号アルゴリズムの安全性に関する考察が行われているが，通信フラットフォームを考慮したシステムの実現性，データ回復法およびリアルタイムな盗聴効率性などについては具体的に述べられていない．

本稿では，特にマルチキャスト通信プラットフォームの上でグループ鍵供託サービスを提供するためのシステムの実現性について考察する．グループ暗号通信における鍵供託を実現するための要求仕様を，UK の DTI(Department of Trade and Industry)のドラフト[6]を参照して表１にまとめる．

このような要求仕様を満たすためのグループ暗号通信の鍵供託モデル(KSM: Key Escrow System Model)を以下のように定義する．

【定義１】KSM＝（TTPs，IA，CGs）

・**TTPs(Trusted Third Parties)**：要求に応じて鍵供託サービスを提供する信頼される鍵管理サーバ．これは，グループメンバを管理するグループ管理センター（GM: Group Management Center）と，メンバの個人情報とは無関係に各グループへのセッション鍵を配布し，定期的に鍵を更新する鍵管理センター（KM: Key Management Center）で構成される．

・**IA（Interception Agency）**：傍受した暗号文を復号するための傍受許可を得て，TTPs から鍵を得る捜査機関．

・**CGs(secure Communication Groups)**：IP マルチキャスト通信フラットフォーム上でグループ暗号通信を希望するユーザで構成されたグ

表 1．鍵供託システムの要求仕様

(1)	鍵供託フレームワークは合法のユーザに利益を与えなければならない．
(2)	鍵供託サービスは，国内はもちろん国際間においても提供可能にしなければならない．
(3)	公共で公開された信頼される第三者機関（TTPs: Trusted Third Parties）を置く．
(4)	TTPs の実現にはよく知られている技術を使わなければならない．
(5)	特定の通信形態に限定されず，すべての電気通信形態をサポートしなければならない．
(6)	捜査機関は傍受許可が得られたら，リアルタイムにアクセス可能にしなければならない
(7)	鍵が使われる時間に制限を与えなければならない．
(8)	実現においてはハードウェアであろうがソフトウェアであるが，ある特定の暗号アルゴリズムに依存してはならない．
(9)	捜査機関が偽の傍受許可書を製作不可能にしなければならない．

ループ.

3.2 グループ暗号通信の鍵供託システム

上記の要求仕様を満たすための鍵供託システムについて考察する.

3.2.1 システム構成

本稿では,図1で示すようにグループ暗号通信の鍵供託システムを提案する.本システムの構成は,以下のようになる.各機関はそれぞれ公開鍵・秘密鍵を持ち,P_x, S_x と表す(但し,x=U, GM, KM, I, J).グループのユーザ間の通信は共通鍵暗号方式で行われるものとする.

(1) ユーザ(U:User)

鍵供託システムに加入して暗号通信を行うユーザ.各ユーザはユーザ名とホスト名を持つ.

(2) 通信グループ(CGs:secure Communication Group)

グループ暗号通信を希望するユーザで構成されるグループとして複数存在し得る.なお,ユーザは移動可能であり,複数のグループ間での暗号通信に参加可能である.

(3) グループ管理センター(GM:Group Management Center)

グループ暗号通信を希望するユーザの個人情報を管理するセンター.ここでは,各グループメンバの登録を行う.また,捜査機関(I)からあるグループへの裁判所(J)からの盗聴許可書を提示したら,そのグループメンバへのメンバ追加許可を得なくて,捜査機関(I)を隠されたグループメンバとして登録し,鍵管理センター(KM)へ鍵配布依頼をする.

(4) 鍵管理センター(KM:Key Management Center)

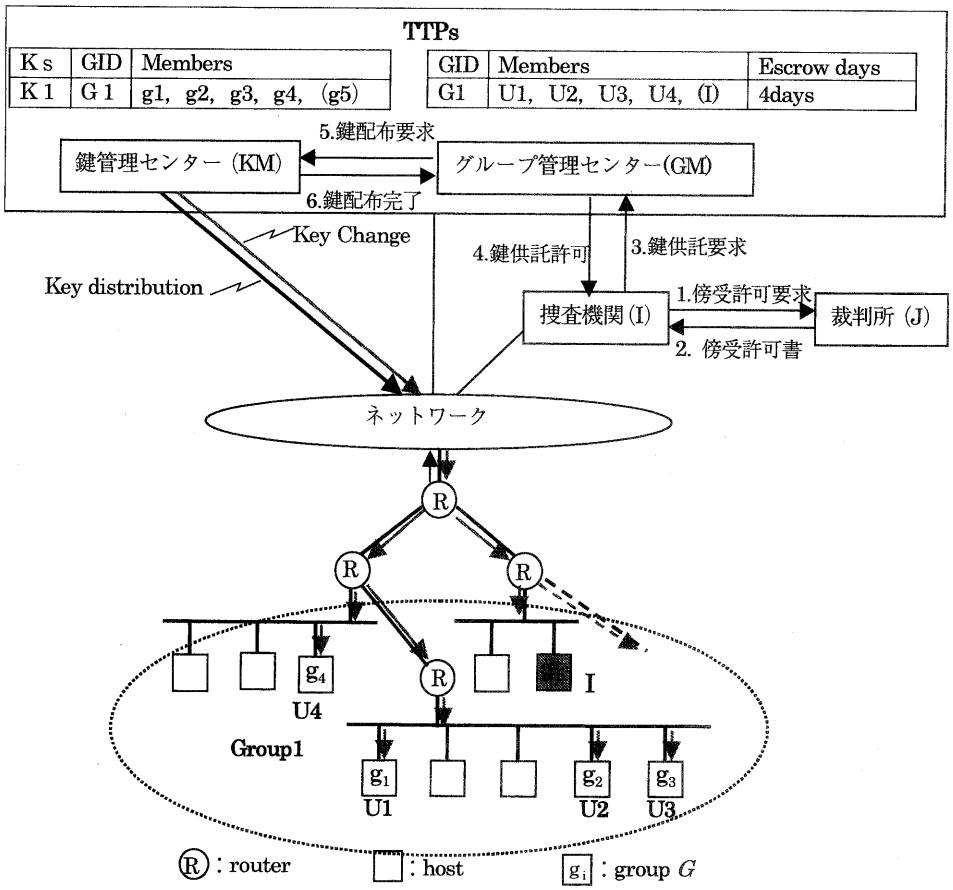

図1. グループ暗号通信の鍵供託システム

グループ暗号通信で使用するセッション鍵を生成し，グループ管理センターからメンバへの鍵配布要求に応じて，定期的に鍵配布・更新を行う．ここでは， GM から依頼される各ユーザのホスト名しか分からない．従って，捜査機関がグループに入るときも捜査機関の存在は知らないまま，鍵を配布するようになる．

(5) 捜査機関（I：Interception Agency）

犯罪捜査目的で，グループ通信の傍受と傍受した暗号文の復号化を行う機関．

(6) 裁判所（J：Court of Justice）

国から法的に定められて信頼できるものとして，捜査機関を認証し，通信傍受許可書を出す機関．ユーザのプライバシーを保護するために，盗聴期間を定めた傍受許可書を発行する．

3.2.2 グループセッション鍵共有手順

本システムでグループ暗号通信を行うためのセッション鍵共有手順は，以下のようにグループ登録，グループメンバへの鍵配布と定期的なセッション鍵更新によって行われる．

▪STEP1：グループ登録

グループの登録方法は次のようになる．

(1-1) グループ暗号通信を希望するユーザ同士がグループメンバリスト(G)を作成し，TTPsのグループ管理センター（GM）に各メンバの秘密鍵と公開鍵に関する情報を送信することによってグループ登録を依頼する．

(1-2) グループ管理センター（GM）は，そのグループメンバリストにグループ識別子（GID）を割り当て，メンバ登録を行い，ユーザのホスト名(g_i)と秘密鍵情報(S_{gi})を鍵管理センター（KM）に送信する．

(1-3) 鍵管理センター（KM）は，GM から受け取ったグループメンバリストに関してマルチキャストアドレス（MA）を割り当てる．

▪STEP2：セッション鍵配布

(2-1) g_i →GM ： *DIS_REQ*(GID)

GMにグループ登録を行った暗号通信グループのメンバ（g_i)は，GM にグループ ID と共にセッション鍵配布を依頼する．

(2-2) GM →KM ： *DIS_REQ*(GID,G)

GM は KM 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．

(2-3) KM→G: *KEY_DIS*[GID, *Ks*,time-exp]S_{gi}

KMは登録GIDとグループGの確認を行い，メンバそれぞれに有効期限付きのセッション鍵 Ks を各ユーザの秘密鍵によって暗号化してユニキャストで配布する．この鍵は有効期限が過ぎると使用しないものとする．

(2-4) g_i → KM：*K_ACK*(g_i)

自分の秘密鍵で復号することにより有効期限付きのセッション鍵（K_s）を受け取ったグループの各メンバ（g_i）は，KM にセッション鍵受信応答を返す．

(2-5) KM → GM ： *DIS_ACK*(GID,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，KM は GM にセッション鍵配布完了通知を送る．

▪STEP3：セッション鍵更新

グループのセッション鍵更新は，以下の手順

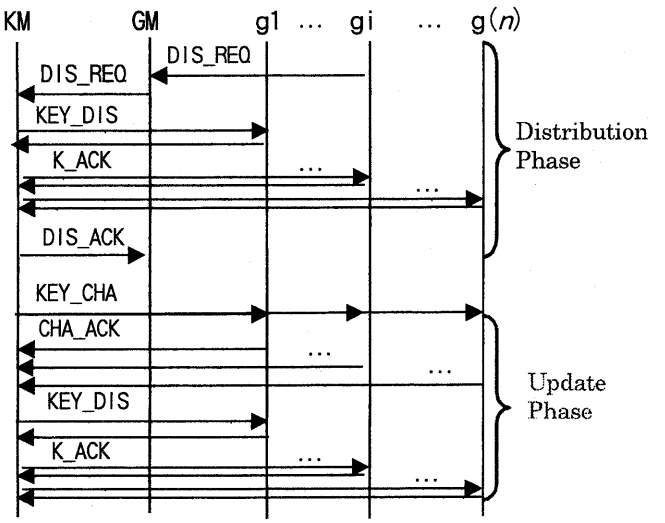

図２．セッション鍵共有シーケンス

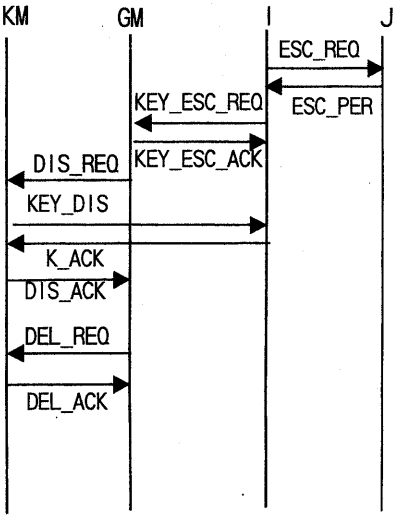

図３．鍵供託シーケンス

を定期的に行う．

(3-1) KM → G ： $[KEY\_CHA]K_s$

KMは，グループGのMA宛にセッション鍵更新メッセージ（*KEY_CHA*）を現在使用しているセッション鍵 K_s により暗号化して一斉に送信する．

(3-2) g_i **→ KM ：** $CHA\_ACK(g_i)$

各メンバ（g_i）はKMにセッション鍵更新確認応答メッセージを送る．

(3-3) KMはグループGへの新しいセッション鍵をSTEP 2の**(2-3), (2-4)**に従い再配布する．

これらに基づいたグループセッション鍵共有シーケンスを図2に表す．

3.2.3 鍵供託手順

捜査機関がある犯罪の疑いのあるメンバが属するグループの暗号通信を盗聴したい場合，まず裁判所に盗聴許可書を発行してもらわなければならない．捜査機関がグループ暗号通信を傍受するための鍵供託手順について述べる．ただし，裁判所には捜査機関を認証するために，捜査できる捜査機関を前もって登録しておくものとする．

・STEP1：傍受許可要求

1. I →J： ESC_REQ**(ID, GID)**

捜査機関（I）は自分のIDと盗聴したい犯罪グループの名前であるGIDと共に，裁判所（J）に盗聴許可書発行を要求する．

・STEP2：傍受許可書発行

2. J →I： $ESC\_PER([K_{I,GM}, [L_J]_{KGM}]_{KI})$

裁判所（J）は，捜査機関（I）の認証を行い，正しい捜査機関であったら盗聴有効期間(Days)とグループIDを定めた証明書付きの盗聴許可書（L_J）を発行する．この許可書はグループ管理センター（GM）との共通鍵 K_{GM} で暗号化しておく．また，IとGM間で使用できる共通鍵 $K_{I,GM}$ も用意する．これを最後にIとの共通鍵 K_I で暗号化して捜査機関（I）へ送る．

・STEP3：鍵供託要求

3. I →GM： $KEY\_ESC\_REQ([A_I]_{KI,GM}, [L_J]_{KGM})$

捜査機関（I）は，裁判所から送られてきた暗号化情報を復号して，GMとの共通鍵と傍受許可書を取り出す．そして，自分のID（I），秘密鍵，ホストアドレス（g5），メッセージ作成時のタイムスタンプを記した自分の認証情報 A_I を作成し，これをグループ管理センター（GM）との共通鍵で暗号化してGMに送る．

・STEP4：鍵供託許可

4. GM→I： KEY_ESC_ACK**(GID, Days)**

GMは，裁判所が発行した傍受許可書（L_J）と捜査機関の認証情報を確認した後，捜査機関（I）をグループGIDのグループメンバに追加し，盗聴有効期限をタイマー装置で設定し捜査機関（I）に盗聴期間中の盗聴可能である確認応答を示す．

・STEP5：グループセッション鍵配布要求

5. GM →KM： DIS_REQ**(GID, g5)**

GMは鍵管理センタ（KM）にグループIDとグループメンバIのホストアドレス（g5）を知らせると共に，そのホストへのセッション鍵配布を依頼する．

・STEP6：グループセッション鍵配布

6. KM→ g5： $KEY\_DIS[GID, K_s, \text{time-exp}]S_I$

KMは，ホストg5をグループGIDに追加しそのグループのMAを与える．そして，そのグループで現在使っているセッション鍵をIの秘密鍵によって暗号化し配布する．

セッション鍵を配布してもらった捜査機関はグループの一員となり，マルチキャスト通信パケットを受け取ることにより，グループ暗号通信にリアルタイムにアクセス可能になり盗聴することができる．また，KMでグループの鍵更新を行う際には，捜査機関（g5）を加えたGIDのメンバ宛に新しい鍵配布を行う．

・STEP7：捜査機関排除

7. GM →KM ： DEL_REQ**(GID, g5)**

GMのタイマー設定により，盗聴期間が終わると，GMからKMへ捜査機関の登録ホストg5をグループGIDのメンバから外すように要求する．

・STEP8：捜査機関排除確認

8. KM →GM ： DEL_ACK**(GID, g5)**

KMは，g5をグループGIDのメンバから外した後，GMに排除確認を送る．このようにして，捜査機関のグループ通信の無制限な盗聴を防ぐことが出きる．

これらをまとめた鍵供託シーケンスは，図3のようになる．

4. 提案方式の考察

まず，提案方式におけるユーザ情報の秘匿性について考察する．

・ユーザの個人情報に関するユーザ名やグループ名と端末ホスト名や秘密鍵情報を分離して保管しているので，TTPs 以外には利用者の情

報をしることが出来ない.
・裁判所が捜査機関を認証し，盗聴期間付き傍受許可書を裁判所とグループ管理センターとの共通鍵で暗号化して渡すので，捜査機関はそれを操作できない.
・GM が操作機関を認証し，KM に操作機関のホスト名だけを知らせているので，GM と KM が結託しない限り，KM は操作機関の存在をしることができない.
次に，提案方式の実用性について考察する.
・ユーザにおいて TTPs は信頼されるサービス提供サーバであるので，安心してグループ登録を行うことができる.
・傍受許可を得た操作機関はグループの一員になり，KM からダイナミックに更新されるグループセッション鍵を同時に配布してもらうことによって，グループ通信にリアルタイムにアクセス可能になり盗聴効率性がよい.

最後に，本システムが３．１での要求仕様を満たしているかを確認してみることによって，提案方式の考察を行う．従来の方式との比較をまとめて表２に示す.

表 2. 提案方式の考察

要求仕様	従来方式[8, 11, 12]	本提案方式
(1)	○	○
(2)	X	今後の課題
(3)	X	○
(4)	X	今後の課題
(5)	△	△
(6)	X	◎
(7)	○	◎
(8)	X	○
(9)	△	○

5．まとめ

本稿では，インターネット上でグループ暗号通信を対象にした鍵供託方式について検討した．そこで，特に IP マルチキャスト通信フラットフォームを考慮し，マルチキャストグループ管理プロトコルの性質を利用し，捜査機関がグループの一員になることによって，ダイナミックに鍵更新が行われるグループ暗号通信にリアルタイムにアクセス可能であることを示した．本方式を実現することによって，インターネットを利用するユーザを悪用するものからいつも監視し守ることができ，ユーザは安心して様々なサービスを享受できるようになると考える.

今後は，上記表２でまとめたように本方式に基づいたTTPsの具体的な実現方式および国際間の鍵供託サービスを提供可能にするための各国間のTTPsの相互接続性を考慮・検討しなければならない．また，鍵配送の安全性の向上およびグループの大規模化に伴う効率的な鍵管理などについて検討を行う予定である.

参考文献

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

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

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

[4] 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.

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

[6] M.P.Hoyle, C.J.Mitchell, "On Solutions to the Key Escrow Problem," *Commun. LNCS*, no.1528, pp.277 -306, 1998.

[7] B.C.Neuman, T.Ts'o "Kerberos : An Authentication Service for Computer Networks," *IEEE Communications*, Sep.1994.

[8] R.Ganesan: "Yaksha : Augmenting Kerberos with Public Key Cryptography," *Proc. ISOC Symp.on Network and Distributed System Security*, Feb.1995.

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

[10] 朴 美娘，岡崎 直宣，井手口 哲夫：マルチキャスト通信上で効率的な鍵配布方式に関する検討，DPS ワークショップ，pp.309-315, 1999.

[11] 山根 義則，櫻井幸一：無制限な盗聴を防ぐ鍵供託方式，*Proc. SCIS*96, Feb, 1996.

[12] 高谷和伯，尾形わかは，坂上仁志，高橋豊：プライバシーを保護する鍵供託方式，*Proc. SCIS*99, pp. 905-910, Feb, 1999.