IP マルチキャストの配送制御とそのセキュリティへの応用

山内長承[†] 石川憲洋[††] 高橋修[††]

近年，インターネットにおける効率の良い大規模情報配布技術として IP マルチキャスト（同報）による通信が注目されている．特にミッションクリティカルな情報を配布するために，配布の信頼性を確保する高信頼同報が検討されているが，他方同時に，配布情報の秘匿や送信者の認証，配布サービスの保全などのセキュリティ機能が必要であり，その方式を検討する必要がある．情報秘匿・認証については，1 対 1 通信で使われている暗号による秘匿では，大規模配送において鍵更新のオーバヘッドが大きくなるために問題を生じることが指摘されている．他方，システム保全については，現状の IP マルチキャストでは対策がとられていないが，アクセス・配送制御機構の導入を考えることができ，筆者らによる出入口（egress と ingress）ルータによる制御方式とマルチキャスト経路制御による方法が提案されているが，後者は利用できる経路制御方式が限定されているので，インターネットにおいては前者を主とした方式が望ましい．ところで，システム保全の手段として導入する配送制御が，許されていない所へ配送しないことによって，情報秘匿の手段としても有効である．配送制御は制御オーバヘッドが配送規模に依存しないため，大規模情報配送では暗号による秘匿に代わる秘匿手段であり得るが，他方秘匿性に弱い面があるので，秘匿性の実現手段としての暗号と配送制御を使い分ける必要がある．そのとき，秘匿性の要求と配送規模が相反する場合が多いという仮説を立て，暗号と配送制御を使い分けることにより，多くの場合で，必要な秘匿性が妥当なコストで実現できることを主張する．すなわち，秘匿性と配送規模がともに大きいことは少なく，秘匿性の要求が高く配送規模が小さい場合には暗号を使い，配送規模が大きく秘匿性が小さい場合には配送制御に依ることができる．

IP Multicast Delivery Control and Its Application to Security

Nagatsugu Yamanouchi,[†] Norihiro Ishikawa[††]
and Osamu Takahashi[††]

IP multicast has recently been studied as a medium for large scale information distribution. In order to distribute mission-critical information, reliable multicast technologies for delivery reliability have been studied. At the same time, security such as information secrecy, sender authentication, and security of delivery services need to be studied. Extension of 1-to-1 communication-based information secrecy and authentication based on encryption fails to scale to a large distribution due to the key update delivery overhead increase. On the other hand delivery service will be maintained by the delivery control mechanisms for IP multicast. We have two control methods, one that controls delivery at egress and ingress routers which the authors proposed, and the other to control delivery at intermediate routers. We point out now that the delivery control for maintaining service security is also effective for achieving information secrecy. As the overhead of delivery control does not increase in large delivery networks, it can be used as an alternative for encryption-based security. However, as the delivery control has weaker capability of maintaining information secrecy compared to encryption, appropriate use of the two methods need to be discussed. In discussing the appropriate use, we propose a hypothesis that large size deliveries do not require high degree of information secrecy and vice versa in most cases, and the combination of large delivery and high secrecy is rather scarse. If this hypothesis holds, we can implement required secrecy at a reasonable cost, namely, we use encryption if high secrecy and small delivery size are required, and delivery control if lower secrecy and large delivery size are required.

† 東京都立大学工学部電子情報工学科
Department of Electronics and Information Engineering, Tokyo Metropolitan University
†† NTT ドコモマルチメディア研究所
NTT Docomo Multimedia Laboratories

1. はじめに

近年，インターネットの新しい使い方として，IP マルチキャスト（同報）が注目されてきている．IP マルチキャストは，同一のデータを，多数の受信者に届け

ることができる．そのとき，1 対 1 通信による配送に比べて，送信サーバやネットワークの負担の軽減，並行転送による同時性，転送時間の短縮などのメリットが得られる技術である．

このような IP マルチキャストは，今まではネットワーク制御機構の一部，たとえば経路制御の実装などの動作のあらかじめよく知られている環境で使われているほか，エンドユーザにかかわる分野では転送の確実性を要求されない応用，たとえばラジオやテレビをまねた音声や画像の単方向の放送や，多人数会議システムで音声や画像，共有白板への書き込みなどを多人数の受信者に配送する場合に使われてきた．また最近では，ミッションクリティカルなデータの多地点同時配送やソフトウェアの多地点への短時間配布などの要求が大きくなっており，確実な転送を実現する高信頼同報技術も徐々に作られてきている．そこでは，今までのマルチキャストの応用を高品質化するだけでなく，営業情報や POS 価格表などの最新情報の営業店への配布，PC ソフトウェアの支店・営業所への配布などが現実の応用としてあげられている[1]．

このようなミッションクリティカルな情報の多地点への同時配送のために，一方ではネットワークの安定した運用を図るための IP マルチキャスト経路制御技術[2)~6)]や，確実なデータ転送を行うための高信頼同報技術[1),7)~12)]などが研究されているが，他方ではセキュリティに関しても 1 対 1 通信と同様にユーザ要求を満たすための十分な配慮が必要である．

IP マルチキャストのセキュリティに対する要件は，IP マルチキャストの応用が確立していないため，必ずしも体系的な分類が行われていないが，利用例に基づく Canetti ら[13)]の整理を参考にすると，以下の 3 点に大別できる．

- 情報の秘匿：情報を，許されていないアクセスから守る．用途としては，秘密情報に対するグループ外からのアクセスの制限や，課金をともなうサービスに対するアクセス制御がある．情報の秘匿には一般に受信者の認証をともなう．
- 情報の認証：届けられた情報が信用できることを保証する．具体的には想定している送信者からの情報であり，かつ改竄されていないという保証．
- サービスの保全：サービスを安定して供給するために，サーバ，受信端末，ネットワークなどを事故，悪意の攻撃から守る．情報処理システムについて一般にいわれているシステムの保全やサービス否定型の攻撃に対する防御の他，IP マルチキャストについては後で述べるようなサービス量の制御を含めて考える必要がある．受信者や送信者にサービスを許可するためには，受信者，送信者の認証をともなう．

なお，同文献はその他に耐監査性をあげているが，これは異質であるので別途考えることとする．

情報秘匿は 1 対 1 通信においては暗号を用いて，すなわち送信側で暗号化し受信側で復号することによって実現する場合が多い．IP マルチキャストを用いた 1 対多通信においても，この方法は情報秘匿に有効であるが，受信者数の多い環境では鍵の管理，配送に問題を生ずることが指摘されている[14)]．具体的には，受信者グループから退出した受信者が復号できないようにするためには鍵を変更する必要があるが，

- 変更後の鍵は，退出前のグループにマルチキャストすることはできないので，基本的には各受信者に個別に配送せざるをえない．この手間は受信者数に比例して大きくなる．
- 受信者数が多いと，受信者の入退出の頻度が比例して多くなる場合が想定され，退出のたびに鍵を更新するとその時間あたりの頻度は受信者数に比例して高くなる．

したがって，暗号を利用した情報秘匿はインターネット上の大規模な情報配送においてはコストの高いものとなる．

また，IP マルチキャストのサービス保全は，ネットワークに過大な負荷をかけて他のトラフィックを妨害するような事態を防ぐ，サービス量の制御機能を考える必要がある．現行の IP マルチキャストが次のような仕組みを持っているため，過失・悪意を問わず容易にトラフィックを生むことができる．

- IP マルチキャストにおいては，情報はトリー状の経路に沿って配送される．1 つのリンク上にはその下流で複数の受信者に分岐していても情報は 1 コピーしか流れない．分岐する時点で初めて，各々のリンクに 1 コピーだけ複製され配送される．またその下流に受信端末が存在しない物理的なリンクには情報は流れない．この IP マルチキャストの仕組みによると，今まで情報が流れていなかったリンクの下流に新たに受信端末が生まれれば，そのリンクに新たなトラフィックが発生する．既存の IP マルチキャストでは，任意の端末は任意のグループに何の制限もなく参加することができるので，送信者やネットワーク管理者の意図にかかわらずリンク上のトラフィックが増えていく．
- 送信者についても，送信参加は制限されていないので，任意の端末が新しいマルチキャストグルー

プを作成し，情報を発信することができる．このときは，ネットワークの管理者の意図にかかわらず，新しいトラフィックが追加されていく．

TCP/IP の枠組みでは，ユニキャストの場合でも，誰でも送信受信することによってネットワークへトラフィックを発生させることが許されている．その点ではマルチキャストも同じ程度の制約なのであるが，マルチキャストの場合，受信者の参加については予定していない受信者でも次々と参加してトラフィック負荷を増すことができる点で，また送信者の参加については新たに大きな配送グループを作る点で，ユニキャストに比較すると影響が予期できず，かつ大きい．

このような環境ではネットワークを安定に運用することに不安があり，現在のインターネットでは多くのサービスプロバイダーがマルチキャストを中継していない．この問題に対して，我々はマルチキャストに転送制約を課することを提案している[15)~17)]．

本論文では，サービス保全を第一義的な目的として提案されているマルチキャストアクセス・配送制御技術が，サービス保全に有効なだけでなく，情報秘匿に対しても一定の役割を果たしうることを検討する．配送制御は配布規模に依らずほとんど同じコストで適用可能であるが，その情報秘匿能力には不完全な面があり強度がつねに十分とはいえない．ここで我々は，多くの場合，配布の規模と秘匿性に対する要求は相反するという仮説のもとに，高機密情報の小規模な配布には暗号による秘匿を，低機密情報の大規模な配布には配送制御による秘匿を用いることを提案する．

2. システム保全のためのマルチキャスト転送制御

本章では，システム保全を主たる目的として提案されている，IP マルチキャスト転送制御技術の概要を整理する．

2.1 IP マルチキャスト配送の現状[18)]

IP マルチキャストでは，受信端末をグループとして扱い，グループに対して 1 つの IP アドレスを割り当てる．送信端末はグループのアドレスに宛てて情報を送出する．ネットワークは，中継ノードのルータにおいて，宛先グループアドレスに属する受信端末がどの出力リンクの下流にあるかを管理しており，必要なリンクに情報を複製して送出する．

ネットワーク内の中継ルータがその出力リンクに複製を送り出すかどうかの情報は，次のように作られる．

受信端末が LAN に接続されている構成の場合，その LAN が外部，具体的には同一組織内の上位の LAN もしくはインターネットに接続されている点に，ルータが設置されている．このルータをここでは出入口（egress または ingress）ルータと呼ぶことにする．このルータが，外部から到着するマルチキャストのグループ宛のパケットを内部 LAN へ転送する．LAN 上では，転送は LAN 媒体の持つマルチキャストまたはブロードキャスト機能を用いて実現される．

受信端末が，グループに宛てたパケットの配送を受けるためには，

- 外部ネットワークでは，そのグループアドレスに宛てたパケットを，受信端末を収容する LAN の出入口ルータまで転送する．この転送ができるように，途中に存在する中継ルータの経路制御情報を設定する必要がある．
- 出入口ルータまで到達したマルチキャストパケットを，LAN 内に転送する．LAN 内では LAN 媒体の持つマルチキャストまたはブロードキャスト機能を用いて転送する．
- 受信端末においては，グループアドレス宛のパケットを取り込み，アプリケーションへ渡す．

の 3 つの設定が必要になる．

これを行う手順は，

- 受信端末は自ら LAN からのグループ宛てパケット取り込みを設定すると同時に，IGMP（Internet Group Management Protocol[19)]）の Membership Report 制御パケットを出入口ルータに対して送る．Membership Report パケットは受信端末のユニキャストアドレス，受信したいグループのアドレスを含む．Membership Report の発信は，たとえばソケットインタフェースを使っている場合は setsockopt ルーチンを呼び出すことにより行われている．
- 出入口ルータでは，IGMP Membership Report を受信すると，受信転送設定を要求されたグループアドレスの通信をすでに LAN 内の他の端末に転送していればそれを継続し，していなければ新たに転送するように設定する．同時にインターネットからこの出入口ルータまでのマルチキャスト転送経路を設定するよう，ネットワークの他のルータに対して要求する．このルータ・ルータ間の要求はマルチキャスト経路制御プロトコルによって行われ，たとえば DVMRP[2)]，MSOPF[3)]，PIM[4),5)]，CBT[6)]などが提案，利用されている．
- 経路がすべて設定されると，当該のグループアドレス宛のパケットが出入口ルータに届くようになり，LAN 側に転送されるようになる．

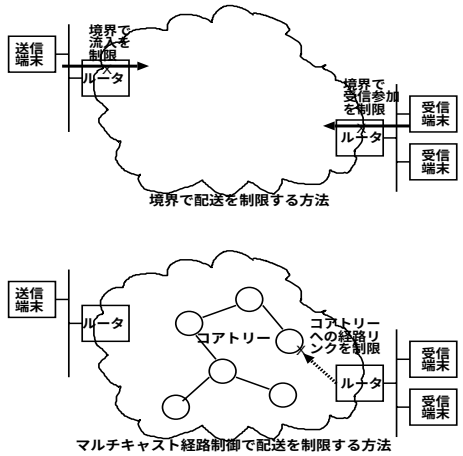

図 1 出入口ルータでの制御と経路制御による配送制御
Fig. 1 Control on boundary vs. control within the Internet.

現状では IGMP Membership Report による出入口ルータの設定，ルータ間マルチキャスト経路設定のいずれも，配送の制約やそれに必要な受信者の認証は行われていない．ルータ間経路設定に使われる CBT プロトコルにおいてその可能性が提案されている[20]だけである．他方，送信者の認証についても，マルチキャストパケットの配送上は制約が設けられておらず，誰でもグループに対して送信できる．

2.2 マルチキャスト配送の制約の導入

マルチキャスト受信，送信とも，マルチキャストグループと受信者・送信者の対に対して認証するように考える．つまり，端末についてマルチキャストすべてを許可・拒否するのではなく，マルチキャストグループによって許可・拒否する．これはサービスの受信を許可・拒否することにあたる．

マルチキャストの転送経路制御へ，配送に対する制約を導入する場合，2 つの要素が考えられる（**図 1**）．

- LAN とインターネットの境界（出入口ルータ）で制限する．
- インターネット内のマルチキャスト経路制御で制限する．

各々について考えられる手法は次のとおりである．

2.2.1 境界（出入口ルータ）で配送を制限する方法

受信者の配送制約，送信者の認証ともに利用できる．具体例として著者のグループが開発した IP マルチキャストユーザの認証[15)~17)]をあげておく☆．

受信者に対する配送制約は，出入口ルータが IGMP Membership Report を出してマルチキャスト参加を要求している受信者（受信端末）を認証することによって行う．その受信者のマルチキャストグループへの参加を許可しない場合は，その端末に対する出入口ルータ内での転送の設定を行わず，また外部インターネットに対するマルチキャスト経路設定要求の送出も行わない．受信者の認証は（参加を要求するグループアドレス，受信者）の対に対して行うことが考えられる．

具体的には，文献 15)~17) では

- 従来の枠組みでは，受信者の参加要求は IGMP Membership Report を介して行われるので，この要求メッセージを認証する．そのために，Membership Report メッセージに User-ID を添付し，その User-ID に対して，次のステップで送られるパスワードを利用して認証する．認証されたら，当該受信端末に対するマルチキャスト配送を設定する．
- 前項の端末認証のために，認証パスワードを送る手順を IGMP に追加する．認証はパスワードの安全性を確保する観点から Challenge 方式[21)]を用いる．具体的には，従来の IGMP メッセージのタイプに**表 1** のタイプを追加する．これにより，出入口ルータから端末へ Challenge 情報を送り，それに対して端末が返答を計算して送り返すことにより，認証される．
- 認証結果は Success および Failure メッセージタイプを用いて，出入口ルータから端末へ返される．Success 時には出入口ルータはこの認証の有効期間 Validity Period を指定し，端末は有効期間が過ぎる前に再認証を受けなければならない．
- 出入口ルータでは，認証が成功すればこの端末の参加のために，ルータ内の転送の設定をすると同時に，インターネットに対する経路設定要求を出す．

ユーザを認証し許可するためのデータベースは各々の出入口ルータの内部に持たせることもできるが，一元管理するために，出入口ルータからネットワーク内の認証データベースサーバへ問い合わせて認証を受け

表 1 IGMP[19)] メッセージに新しく追加されたタイプ
Table 1 New types added to IGMP[19)] messages.

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

☆ この機構は，送受信端末は FreeBSD 上のソケットコードに対する変更として，また出入口ルータは FreeBSD 上の mrouted に対する変更として実装されており，試用に供されている．

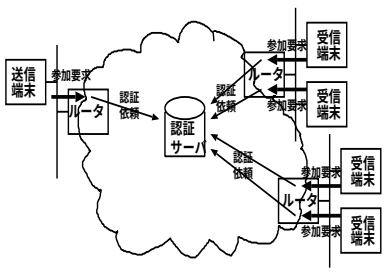

図 2 認証サーバーによる認証情報の一元管理
Fig. 2 Authentication server for centralized authentication data management.

ることも可能である（**図 2**）．認証サーバの例として文献 16) では従来ダイヤルアップルータに対するユーザ認証サーバ機構として使われている RADIUS を拡張する方法[22)]を提案しているが，必ずしもこれに限定されるものではない．受信者数の増加にともなう対応の観点からは，データベースサーバへアクセスが集中することが隘路になる可能性があるが，アクセスの頻度がそれほど高くないこと，必要であれば複数のサーバによる負荷分散も可能であることなどから，ある程度スケーラブルにできるものと考えられる．

この方法の長所は，ネットワーク全体の規模に対しては制約がないこと，グループに属する受信端末数の増加に対して対応できるスケーラビリティがあることがあげられる．なぜなら，認証の仕事は各出入口ルータに分散しており，1 つの出入口ルータで受け持つ端末数は一般に限定されているからである．

他方，問題点としては，受信端末と同じ LAN 上にある他の端末が同じマルチキャストサービス（グループアドレス）を許可されて利用している場合，ブロードキャスト型の LAN ではそのグループアドレスに対するデータが LAN 上を流れており，認証されない端末がパケットを受信できる可能性がある．受信するために必要なセキュリティ上の障壁は，媒体アクセス（MAC）レベルでのマルチキャスト機能の実装状況に依存するが，一般には端末のネットワークソフトウェアを改変することにより受信できてしまう．具体的には，認証拒否時に当該グループアドレス宛のデータの取り込みをプロトコルソフトウェアで禁じるのであるが，個人利用を想定した PC OS のようにシステムソフトウェアがまったく保護されていない場合や，UNIX でも特権ユーザになれる場合は，ネットワークソフトウェアを書き替えることにより，データの取り込みが可能になる．その点で情報の秘匿が十分に強いとはいえない．

またインターネットとユーザ収容 LAN との境界で制約するため，この制約を課していない出入口ルータがあるとその部分で破綻することになる．受信制約の場合，その出入口ルータの下流にある端末は制約なしにマルチキャストグループに参加できるし，送信制約の場合任意のマルチキャストパケットを送出することができる．幸いなことに，現状からの移行を考えると現在大半のルータがいっさいのマルチキャスト転送を禁じているので，マルチキャストをサービスするときに制約付きで徐々に解放していくことができれば，上記の問題は発生しない．

送信者に対する配送制約については，従来の IGMP の枠組みでは参加の制約がなく，送信者がマルチキャスト参加を要求したり認証・許可を受けたりする仕組みが存在しない．文献 16) では，マルチキャスト送信を原則として禁止し，送信端末として認証・許可された端末のみが送信できるように設定する．具体的にはマルチキャスト送信を希望する端末について，受信者と対称になるように IGMP Membership Report に相当する要求を表 1 の Sender-Start メッセージとして用意している．このメッセージを使って端末がマルチキャスト送信への参加要求を出入口ルータに対して出すこととし，送信者の ID とグループアドレスの組に対してアクセス許可を与えるようにしている．受信者の認証と同様に Challenge の認証パスワードを添えて認証を行う．転送データの流れに対する制御は，受信者の場合と違って出入口ルータでの転送設定によって制御することができないので，新たに出入口ルータにパケットをフィルタリングする機構を設ける．具体的には，外部から流入するマルチキャストパケットについて，そのパケットの持つ（宛先グループアドレス，送信アドレス）の対に対して，送信者が認証されていない場合はパケットのネットワークへの送出を行わないことによって制御している．

この場合，パケットフィルタの転送能力が性能上の問題になるが，出入口ルータが対応しなければならないフローはバックボーンルータのように大きくなることはないので，それほど問題にならないと考えられる．

受信と同様，送信もグループアドレスと端末の対に対してマルチキャストを許可する．これにより，送信サーバはグループアドレスごとに送信許可を受けることになる．

また受信と同様，送信の認証はインターネットの出入口境界で流れを制限しているので，この機能を装備していない出入口ルータからのデータの流入は起こりうる．この点についても受信の許可と同じように，現状ではインターネット内のルーターの大半がマルチキャ

ストの転送を禁じているので，それらがマルチキャストのサービスを始めるときに，そのルーターにつながる出入口ルーターがこの送信許可機能を持つことを条件にして開始する，という手順を踏むことにより，回避することができる．

ネットワークの過大トラフィックからの保全の観点からは，ネットワークに入る境界で許可されないトラフィックの発生や流入を防ぐことは，予想されないトラフィックがネットワーク内部にいっさい入らないので，高い効果が期待できる．

受信・送信を問わず出入口ルーターで制約する手法は，境界上のすべての出入口ルーターで制約されないと，洩れが生ずる可能性があり，洩れたものはネットワークの中を通過してしまう．次項の経路制御による配送制限と組み合わせればより確実なものになるが，経路制御による方法は適用範囲が極度に限定されている．さらに，上に述べた共有媒体 LAN での制約の困難さを考え合わせると，完璧な制約は期待できない．むしろ，大半の一般ユーザに対して乗り越えにくい障壁を提供する技術と考える方が適当である．

2.2.2 マルチキャスト経路制御で配送を制限する方法

文献 20) はマルチキャスト経路制御プロトコルの 1 つである CBT を用いた配送経路の制約と，その制約を用いた暗号鍵配送を提案している．

CBT ではマルチキャスト配送経路を，あらかじめ定めたいくつかのコアルータを中心にした共有配送トリーに，新しい受信端末が加わる形で作っていく．受信端末を収容する出入口ルータは IGMP Membership Report を受けると 1 つのコアルータに対して経路を設定する．この出入口ルータとコアルータの間の接続は出入口ルータが明示的に確立するものなので，確立の段階で共有コアトリーへの参加を許可するか否かの認証をすることができる．不許可の場合は当該の出入口ルータへの配送経路が作られない．

この技術は CBT が出入口ルータからコアルータまでのリンクをハードリンクとして扱っているために可能になっている．他のマルチキャスト経路制御プロトコルではソフトリンクとなっているため，認証は難しい．つまり CBT においてしか利用できない技術である．また，この方法でコアルータが参照する認証データを上述の境界での制限と同様に認証サーバに置くことにすれば，ネットワークの規模に対して制約がない，受信端末数の増加に対してもかなりスケールできるという長所がある程度成り立つだろう．境界での制限と異なる点は，境界での制限では出入口ルータでの認証は受信も送信ももっぱら LAN 内の端末に対して行うので，認証データは局所的に持っていればよい．それに対して CBT の場合はネットワーク全体に対して管理する必要があるのですべてのユーザの認証データを参照できる必要がある．

欠点は，コアトリーから出入口ルータに到達するまでの経路を制御するのであるから，上述の境界での制約と同じように，すでに許可された受信者があるとデータは LAN 上を流れてしまい，他の端末は読むことができる．特に CBT の制御だけを行った場合は LAN 内でのアクセスの制限は起こらないので，すべての端末が合法的に受信することができる．LAN 内でのアクセス制限，すなわち受信端末のプロトコルプログラム内でのグループアドレスによる取り込み制約を併用する必要がある．

また，CBT 以外の経路制御プロトコルでは，経路リンクをソフトリンクとして扱っているためこの機能は実現しにくく，ただちに実用化することは難しい．

ネットワーク保全の観点からは，CBT の手法は出入口ルータからコアトリーへの経路を制約するものであるから，出入口ルータでの制約と同じ効果を持つ．

3. マルチキャスト配送の情報秘匿の問題

前章ではシステム保全を目的とした配送制御の導入を議論したが，本章では，セキュリティのもう 1 つの課題である情報秘匿について，マルチキャスト時の問題を検討する．

3.1 暗号による情報技術の問題点

暗号による情報秘匿は 1 対 1 通信において広く用いられているが，1 対多通信に適用する場合，単純な拡張では配送規模の拡大にともなって次の 2 点で破綻する[14]．

- 鍵の変更時に必要な鍵の配送の手間が，受信者数にともなって増加するので破綻する．まず，マルチキャストを用いて 1 対多配送を行う場合は，送信情報は 1 つの鍵で暗号化される．受信者ごとに異なる鍵を使うのでは，同じ情報をマルチキャストすることができない．1 つの鍵をグループで共有する結果，受信者がグループを離脱したときに，その離脱した受信者に対して秘匿するためには，鍵の変更が必要になる．新しい鍵は離脱後のグループの全員に配布しなければならない（一斉更新）が，離脱した受信者に届いてはならないので，離脱前のグループへのマルチキャスト用の鍵を利用することができない．基本的には個々の受信者の個別の鍵を用いて鍵を送らなければならず，

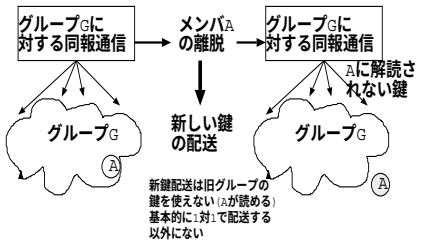

図 3 受信者の離脱と鍵の更新
Fig. 3 Delivery of group common key whenever a member leaves.

その方法としてはすべての受信者に対して 1 対 1 通信を用いて送るか，または受信者個別の鍵でグループの共通の鍵を暗号化したものをならべたデータをマルチキャストすることになる（**図 3**）．いずれにせよ，単純な方法ではグループの受信者数に比例する手間がかかる．また，グループをサブグループに分ける方法を用いて，受信者数 n に対して $\log\ n$ の手間で鍵を配送することが考えられるが，いずれにせよ，受信者数の増大にともなって手間が増える．

- 受信者のグループ離脱にともなう鍵更新が発生する頻度は，受信者数にともなって増加する場合がありうる[14]．これは受信者の離脱のパターンと，鍵更新に対する要求の程度に依存するが，たとえば次のような場合が考えられる．
  - 受信者が単位時間内に一定の確率で離脱し，かつ受信者が離脱すると必ず鍵を更新する必要がある場合は，受信者数の増加にともなって更新の頻度も増加する．たとえば，一般消費者を対象とした配布では受信者は一定の確率で離脱すると考えられるが，1 人が離脱するごとに鍵を更新するとすれば，鍵の更新頻度は受信者数に比例して増加する．
  - 受信者は一定確率で離脱するが，受信者が離脱してもすぐには鍵を更新せず，一定時間ごとに鍵を更新するシステムも考えられる．一般消費者を対象とした配布であるが，1 日に 1 回まとめて鍵を更新するといった設定があてはまる．この場合は鍵の更新頻度は固定されており，受信者数の増加とは関係しない．
  - 受信者数の変動が一定時期に起こる場合．たとえば企業内で用いる場合，人事移動の時点でまとめて離脱するので，その直後に鍵の変更を行えば済む．この場合も受信者数の増加と更新頻度は関係しない．

  第 1 の場合には，受信者の増加に対して，変更の頻度が比例して増加し，かつ 1 回の変更に要する手間が比例して増加するので，全体としては受信者数の 2 乗に比例することになる．

たとえば受信者が 100 万人，離脱の確率は 1 年に 1 回とすると約 31.5 秒に 1 回離脱が発生することになるが，離脱が発生するごとに長さ 64 ビットの鍵を 100 万人に対して更新すると，その鍵の配送量は毎秒平均 2.03 メガビットとなる．これは前述の 2 乗の効果が大きい場合であり，実用的にはほとんど鍵の更新をすることができない．

3.2 配送制約による情報秘匿

情報の秘匿機能は，配送の制約によってもある程度まで実現できる．すなわち，暗号を用いた方法では，許可されていない人が情報を読んだり作成したりすることができないことにより，秘匿や認証を実現する．他方，配送制約は，許可されていない人が情報を受信したり送信したりできないようにする．受信を許可されていない人に情報が配送されなければデータを秘匿でき，送信を許可されていない人が発信できなければ送信者の認証と同じ効果がある．

この 2 つの方法は，その能力と実現費用の観点から相補的に用いられてきた．たとえば，通信業者の提供する専用線を利用する場合，配送制御を信頼し，格段の暗号機構などを用いずに社外秘の情報を転送している場合も多い．他方，無線通信などのように配送を制御できない場合や，有線通信でも盗聴のコストに比べてデータの価値が高い場合，また配送だけでなくデータの生成から配送，保管まですべての段階でのセキュリティを保ちたいという要求がある場合などに，暗号利用が有用であると考えられてきた．マルチキャストにおいても同様に，エンド・エンド間の暗号化と転送制限によるアクセス制御は相補的にとらえ，実現コストによって使い分けることが考えられる．マルチキャストにおいては各々の技術の実現コストが 1 対 1 通信の場合と異なるため，使い分けの方法も異なってくる．

3.3 大規模マルチキャスト時の暗号化と配送制約の比較

前節で論じたように，情報の秘匿を実現する手段として，暗号を用いた方法と配送制約による方法が考えられる．両者を比較すると**表 2** のようになる．

これを要約すると，暗号化による秘匿は強いが，大規模な配布に対してコストが高く，配送制御による秘匿は秘匿性に問題がある場合があるが，大規模配布にも対応できる．この観察に従って，両者の使い分けを考える．

表 2 暗号による秘匿と配送制約による秘匿の比較
Table 2 Comparison between encryption and delivery control for information secrecy.

	暗号化による秘匿	配送制御による秘匿
秘匿の強度	エンド・エンドで秘匿される． 暗号強度が十分ならば配送途中で漏洩することはない．	理想的に動作すれば，情報そのものが配送されない． 共有媒体リンクでは，ほかに受信端末があると情報は端末入口まで流れるので，特権ユーザは盗聴できる．
受信者の離脱のコスト	鍵変更のたびにグループ内の受信者に異なる鍵情報を送らなければならない． 配布規模にともなって増加．	離脱する受信者の属する出入口ルータが配送を停止する．この処理は分散しており，配布規模に依存しない．

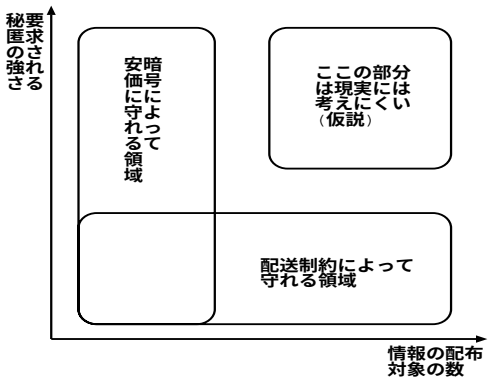

図 4 配布規模と情報価値は相反するという仮説と暗号・配送制御の使い分け
Fig. 4 A hypthesis that the security requirement is smaller for mass-distributed data.

3.4 配布規模と情報価値に関する仮説と，秘匿機構選択への適用

暗号と配送制御による秘匿の使い分けを考えるとき，配送規模のスケーラビリティと情報の間に，次のような仮説を考えることができる．すなわち一般に，情報の配布規模が大きいほど，その秘匿に関する要求レベルは低くなる．

従来，機密管理の面から一般に重大な機密事項はなるべく限定した少数の人にのみ知らせるのがよく，より多くの人に知らせればそれだけ漏洩する確率が高くなると考えられている．具体的には，たとえば国家の重大機密は数人の政府要人が知るだけであり，すべての閣僚に知らせればそれだけ機密保持のレベルは低下する．企業においても，機密度の高い情報ほど少数の人にのみ知らせるのであり，大勢に知られるようになればグループ外に漏洩する確率は高くなる．

もしこの仮説が，我々の対象とする情報配布においても広範囲に成立するのであれば，機密要求度の高い情報を大量に配布することはあまりなく，大規模配布時には高い機密度は必要ないということになる．

有料情報配布について適用してみると，秘匿の要求はもっぱら代金を払っていない人による無料受信を防ぐことにある．このとき要求される機密性はせいぜい情報の持つ価値の程度であり，実際に数千人から数万人に配布する情報であれば新聞のように数百円から有料レポートのようにせいぜい数万円程度に値付けされており，1 件で 100 万円の値がつくことはまずほとんどないだろう．一方，もしその情報が 100 万円の価値がある，たとえば企業内の機密情報であれば，その企業内のごく限られた人数だけに共有されるだろう．

さらに，情報配布だけでなく，電子会議をマルチキャストによって行う場合でも同じような傾向が成り立つに違いない．機密の会議であれば参加者はごく少数であり，他方，社員全員に対する放送であればその情報の機密性はかなり低いと考えられる．

ソフトウェアの配布についても同様の傾向が成り立つ部分があるだろう．高額なソフトウェアの配布は限定された少数の計算機に行い，多量の計算機に配布するソフトウェアは一般にそれほど高価なものではない場合が多い．ただし，この場合の理由は，多くの人に知られると機密漏洩の確率が高くなるという理由ではなく，単純に全体の購入費用が大きくなるからという理由かもしれず，この仮説の成り立たない場合もありうる．

以上検討したように，配布規模と情報価値は相反するという仮説はある程度広い範囲で成り立ちそうである．もし成り立つとすれば，配布機構の情報秘匿機能については，多くの場合，必ずしも高い秘匿性を保ったまま大きな配布規模を実現しなくてもよいといえる．両立する必要はなく，いずれか一方が大きい．

この考えに従うと，暗号による情報秘匿の効率が，配布規模が大きくなると低下する問題について，機密性が高い情報を少数の宛先に配布する場合には暗号による秘匿を用いるとし，それほどの秘匿性を要求されない情報を大規模に配布する場合は配送制約による秘匿を用いる，という使い分けによって解決することができる．

この状況を**図 4** に示す．配布規模を横軸に，機密要求度を縦軸にとるとき，配送制約は配送規模に依らず適用可能だが秘匿性に限界があり，暗号による方法は秘匿性は高いが配送規模の拡大に対応できない．図の右上隅に相当する部分は，機密性が高くかつ配布規模

が大きい場合であるが，配布規模と情報価値は相反するという仮説によってこの部分に該当する場合は多くないと考えられる．

4. 結　　論

IP マルチキャストにおける情報の秘匿と送信者認証，サービス保全の要求と実現手法を考えるとき，従来の 1 対 1 通信で使われている技術を 1 対多通信に拡張するとネットワーク規模や配布規模の増大に対応できない面がある．1 対 1 通信とは異なる，マルチキャストに適した手法や手法の使い分けを考える必要がある．

IP マルチキャストにおけるサービス保全の側面としてトラフィックの発生に対する規制機能があり，これを実現するために，受信者の認証とアクセス制限，送信者の認証とアクセス制限を設ける必要がある．その実現手法として著者らのグループが文献 15)〜17) で提案している出入口ルータにおける配送制御と，ネットワーク内でのマルチキャスト経路制御機構に対する認証の追加があるが，後者は限られた経路制御機構のみでしか利用できず，インターネットにおいては前者が望ましい．

情報の秘匿・送信者の認証については，暗号による秘匿と配送制御による秘匿が考えられるが，暗号による秘匿は配布規模の拡大に対応できず，他方配送制御による秘匿は秘匿性が不十分な場合があり，要求によって使い分ける必要があるとともに，高機密性かつ大規模な配布は難しい．そのとき，配布規模と情報価値が相反するという仮説がかなりの範囲で成り立つとすれば，高秘匿性と配布規模を同時に要求する場合は少なく，大半の場合は暗号と配送制御を使い分けることによって対応できるはずである．

さらに，サービス保全の要求から配送制御がすでに導入されている場合，大規模配送における一定の情報秘匿機能を代償なしに得ることができることにもなる．

今後の課題としては，

- 配布規模と情報価値は相反するという仮説のさらなる吟味が必要である．IP マルチキャストを用いる具体的な情報配布の例を多数取り上げて，この仮説をどの程度満たすか，どのような反例があるかを検討しなければならない．
- この仮説が受け入れられるものであれば，文献 15)〜17) の機構の試験実装は完了・実験済みであるので，これと暗号による機構との併用，切替えの可能性，配布制御と経路制御との併用など，他の機構との融合を検討する必要がある．

などがあげられる．

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 (1997).
2) Waitzman, D., Partridge, C. and Deering, S.: Distance Vector Multicast Routing Protocol, IETF RFC 1075 (Nov. 1988).
3) Moy, J.: Multicast Extensions to OSPF, IETF RFC 1584 (Mar. 1994).
4) Deering, S., Estrin, D., Farinacci, D., Jacobson, V., Helmy, A. and Wei, L.: Protocol Independent Multicast Version 2, Dense Mode Specification, IETF Draft ⟨draft-ietf-idmr-pim-sm-specv2-00.txt⟩ (May 1997).
5) Estrin, D., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, M., Jacobson, V., Liu, C., Sharma, P. and Wei, L.: Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, IETF RFC 2117 (June 1997).
6) Ballardie, A.: Core Based Tree (CBT version 2) Multicast Routing, IETF RFC 2189 (Sept. 1997).
7) Deering, S.: Host extension for IP multicasting, IETF RFC 1112 (Aug. 1989).
8) Miller, K.: StarBurst Multicast File Transfer Protocol (MFTP) Specification, IETF Draft ⟨draft-miller-mftp-spec-02.txt⟩ (1999).
9) Lin, J.C. and Paul, S.: RMTP: A Reliable Multicast Transport Protocol, *Proc. IEEE Infocom'96*, pp.1414–1424 (Apr. 1996).
10) Vicisano, L. and Crowcroft, J.: One to Many Reliable Bulk-Data Transfer in the MBone, *HIPPARCH 1997* (June 1997). Available as http://www.cs.ucl.ac.uk/external/L.Vicisano/pubb/hipparch97.ps.gz
11) McCane, S. and Jacobson, V.: Receiver-driven Layered Multicast, *Proc. ACM Sigcomm'96*, pp.117–130 (Aug. 1996).
12) Sano, T., Shiroshita, T., Takahashi, O. and Yamashita, M.: Monitor-based Flow Control for Reliable Multicast Protocol and Its Evaluation, *Proc. IEEE IPCCC'97*, pp.403–409 (Feb. 1997).
13) Canetti, R. and Pinkas, B.: A taxonomy of multicast security issues, IETF Draft ⟨draft-canetti-secure-multicast-taxonomy-00.txt⟩ (May 1998).
14) Mittra, S.: Iolus: A Framework for Scalable Secure Multicast, *Proc. ACM Sigcomm'98*, pp.277–288 (Aug. 1998).
15) 石川憲洋，山内長承，高橋　修：IP マルチキャスト通信へのユーザ認証機能の導入，情報処理学会マルチメディア通信と分散処理研究会 DPS

89-6, pp.31–36 (June 1998).
16) 石川憲洋，山内長承，高橋　修：IP マルチキャスト通信のユーザ認証機能の提案と実装，情報処理学会論文誌，Vol.40, No.10, pp.3728–3736 (1999).
17) Ishikawa, N., Yamanouchi, N. and Takahashi, O.: IGMP Extension for Authentication, IETF Draft ⟨draft-ietf-idmr-igmp-auth-00.txt⟩ (Mar. 1998).
18) Comer, D.E.: *Internetworking With TCP/IP, vol.1: Principles, Protocols and Architecture*, Prentice-Hall (1995).
19) Fenner, W.: Internet Group Management Protocol, Version 2, IETF RFC 2236 (Nov. 1997).
20) Ballardie, A.: Scalable Multicast Key Distribution, IETF RFC 1949 (May 1996).
21) Simpson, W.: PPP Challenge Handshake Authentication Protocol (CHAP), IETF RFC 1994 (1996).
22) Yamanouchi, N., Ishikawa, N. and Takahashi, O.: RADIUS Extension for Multicast Router Authentication, IETF Draft ⟨draft-yamanouchi-radius-ext-00.txt⟩ (Mar. 1998).
23) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, IETF Draft ⟨draft-ietf-ipsec-arch-sec-06.txt⟩ (July 1998).

(平成 11 年 3 月 2 日受付)
(平成 11 年 11 月 4 日採録)

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．

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．

高橋　　修（正会員）

1975 年北海道大学大学院工学研究科情報工学専攻修士課程修了．同年，日本電信電話公社入社．現在，NTT 移動通信網（株）マルチメディア研究所勤務．主としてモバイルインターネットサービスと通信プロトコルの研究開発に従事．電子情報通信学会会員．