暗号によるネットワーク隠蔽方式

2T－3

永島　規充　後沢　忍　時庭　康久　稲田　徹　田口　卓哉
三菱電機（株）情報技術総合研究所

１．はじめに

インターネット、イントラネットの普及により、ネットワークを流れるデータの重要性も高まってきており、ネットワークセキュリティへの配慮が急務となっている。筆者らは、ネットワークセキュリティの実現手段として、経路情報など中継装置間でやり取りされる情報を暗号化する方式を検討した。本稿では、この方式における実現方法について述べる。

２．経路情報の暗号化

２．１　課題

中継装置（ルータ）により複数のネットワークが相互接続されるインターネットワーキングでは、各中継装置は、ネットワークがどのように接続され、どのネットワークを経由すれば目的のネットワークに到達できるかという経路情報をやり取りする。特に、インターネットプロトコル（IP）では、RIP（Routing Information Protocol)やOSPF（Open Shortest-Path First）のような経路情報プロトコルに従い、経路情報を交換する。

インターネットは、全世界の端末と通信できるオープンな環境であるのが利点であるが、このため、これらの経路情報もオープンとなり、悪意のあるユーザに対してネットワークのアドレスなどの情報、存在及び到達経路が漏れ、不正行為の手掛かりとなる可能性がある。また、不正ユーザが誤った経路情報を通知すると正規の通信経路に影響を与え、通信妨害や中継経路変更によるデータ盗聴などの危険がある。上記課題を解決するため、中継装置間でやり取りされる経路情報を暗号化する方法を提案する。なお、今回は経路情報プロトコルとしてRIPが使用されている場合について検討した。

２．２　隠蔽するネットワークの指定

中継装置の経路情報テーブルの中から、隠蔽したいネットワークを指定する。中継装置は、隠蔽指定されたネットワークに関する経路情報をMISTY、DES等の暗号アルゴリズムを用いて暗号化して送信する。この暗号化／復号処理では、予め、共通の暗号鍵を中継装置間で共有しておく必要がある。隠蔽指定されなかったネットワーク（公開ネットワーク）に関する経路情報は、従来と同じように暗号化せずに隣接する中継装置に送信する。図２に一般的なネットワーク接続におけるネットワーク隠蔽の例を示す。

２．３　データ暗号化

隠蔽指定されたネットワークの経路情報は下記のようなフォーマットで隣接する中継装置に通知する。データは、宛先アドレス（DA）、送信元アドレス（SA）、フレームタイプ、ヘッダ（IP、UDP）を除いた部分を暗号化する。図１にデータフォーマットを示す。

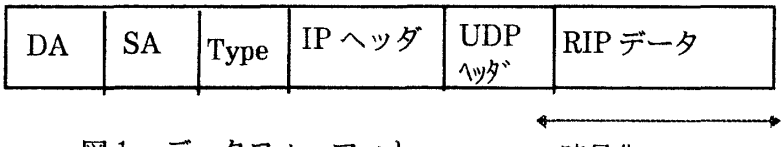

図１　データフォーマット

２．４　経路情報テーブル

中継装置は、隣接する中継装置から通知される経路情報を基に経路情報テーブルを作成する。中継装置によるデータフォワードは、この経路情報テーブルに従って行われる。経路情報テーブルには、終点のネットワークアドレス、次のホップルータのアドレス及びホップ数の情報が含まれている。本稿で提案する方式では、経路情報テーブルに属性のフィールドを追加する。隣接する中継装置から通知された経路情報が暗号化されている場合は、復号後、情報を経路情報テーブルに登録する。この時、属性は隠蔽とする。暗号化されていない通常の経路情報が通知された場合は、属性を公開として登録する。

Encryption of the Routing Information to prevent traffic analysis

Norimitsu NAGASHIMA, Shinobu USHIROZAWA, Yasuhisa TOKINIWA, Toru INADA, Takuya TAGUCHI
Information Technology R&D Center, Mitsubishi Electric Corporation 5-1-1 Ofuna Kamakura,247 JAPAN

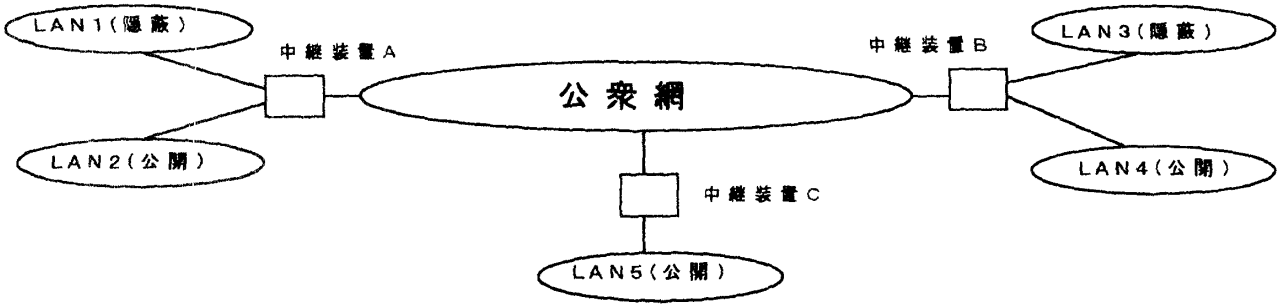

図2　ネットワークの隠蔽

表1に中継装置Bにおける経路情報テーブルの例を示す。

表1　中継装置Bの経路情報テーブル

終点ネットワーク	次のホップ	ホップ数	属性
LAN1	中継装置A	2	隠蔽
LAN2	中継装置A	2	公開
LAN3	直接接続	1	隠蔽
LAN4	直接接続	1	公開
LAN5	中継装置C	2	公開

2．5　経路情報の更新

中継装置では、隣接する中継装置から通知された経路情報に対し、その情報が未登録であれば、経路情報テーブルに登録する。登録済であれば、該当する経路情報テーブルのホップ数と比較する。ホップ数が小さければ、経路情報を更新する。

経路情報テーブルの属性が隠蔽となっている場合は、たとえホップ数の少ない経路が通知されたとしても、セキュリティが低下するのを防ぐため、原則として属性が公開の情報には更新しない。ネットワーク管理者が属性を変更する場合（図1のLAN1の属性を隠蔽→公開に変更）、各中継装置では通知された経路情報を基に経路情報テーブルの属性を更新する。この更新は、経路情報を通知してきた中継装置が正しく認証された場合のみ行うこととする。属性を公開→隠蔽と変更する場合も同様である。

2．6　経路情報の削除

中継装置では、経路情報テーブルに載っている情報をエージングタイマを用いて管理する。中継装置の保守などでネットワークへの中継経路が途絶えた場合、つまり一定期間、ある中継装置から通知されなくなった経路情報は、ホップ数を16（到達不能）とし、隣接する中継装置に通知する。属性が公開の情報については、ホップ数が16となった後、一定期間この経路に関する情報が通知されない場合は、経路情報テーブルから削除する。属性が隠蔽の情報については、削除後、不正に属性公開で登録されるのを防ぐため、一定期間情報が通知されない場合も、経路情報テーブルからは削除しない。

3．まとめ

ネットワークセキュリティの実現方法として、中継装置間でやり取りされる経路情報を暗号化する方法を検討した。今後は、大規模なシステムへの適用、当社ネットワークセキュリティシリーズMELWALLとの連携、既存ルータとの共存及びOSPFを用いたケースについてを検討していく予定である。

参考文献

[1]Brijesh Kumar 他："Integrating Security in Inter-Domain Routing Protocols"，Computer Communication Review,1994

[2]馬場他："ネットワークセキュリティ（盗聴防止）とセキュリティドメインに関する一考察"，情報処理学会第51回全国大会，1995

[3]横山他："LAN暗号装置の実現方式"，電子情報通信学会総合大会,1997