7F－1

ネットワークセキュリティのための パケット暗号化方式に関する一考察

妹尾　尚一郎，馬場　義昌，渡辺　晃，厚井　裕司
三菱電機(株) 情報技術総合研究所

1．はじめに

ネットワークセキュリティの実現手段としてパケット暗号化方式を取り上げ，ルーティングとの対応づけや暗号データのエンカプセルにおける選択肢を評価する．特にエンカプセルにIPトンネルを用いる場合を検討し，端末アドレスとIPトンネルの端点アドレスのマッピングを動的に実行するためDNS(Domain Name System)[2, 3]を利用することを提案する．

なお，本稿では以下の定義を用いる．

［セキュアネットワーク］.パケットを暗号化することで実現される，機密性を持ったネットワーク内の領域．一般には機密性を持たないネットワーク内に分散し，秘密鍵を共有する端末の集まりとして構成される．

［平文ネットワーク］セキュアネットワーク以外の領域．

2．ルーティングとの対応

セキュアネットワークとデータリンク層ないしネットワーク層におけるルーティングの対応づけには，次の方法が考えられる．これらの比較を表1に示す．

(方法1) セキュアネットワークIDを各パケットに付加する(tagging)．

(方法2) セキュアネットワークをMACアドレスの集合と対応づける．

(方法3) セキュアネットワークを個別ネットワークアドレスの集合と対応づける．

(方法4) セキュアネットワークをサブネットワーク(IPならサブネット，IPXならネットワーク番号)と対応づける．

上記の中では，ルータを介した暗号通信が可能であり管理上の負荷の少ない(方法1)の有効性が高いが，実際にはセキュアネットワークの適用対象によって使い分るべきものと考えられる．

3．暗号プロトコル

セキュアネットワークの暗号プロトコルとして規定すべきことは，①暗号化したデータのエンカプセル形式，②暗号ヘッダ，③その他の付加的プロトコル，に分類される．

3.1 暗号データのエンカプセル形式

次の2つがあるが，より汎用的な②の方法を検討する．

① ネットワーク層プロトコルのユーザデータ部分を平文から暗号文へ入れ換える（図1a）．

② 上記に加え，暗号化方法，暗号アルゴリズムや鍵識別子を含む暗号ヘッダを暗号データの前に挿入する（図1b）．

A Study on Packet Encryption Schemes for Network Security
Shoichiro SENO, Yoshimasa BABA, Akira WATANABE and Yuuji KOUI
Information Technology R&D Center, Mitsubishi Electric Corporation , 5-1-1 Ofuna, Kamakura, 247 JAPAN

表1　セキュアネットワークとルーティングの関係

	長所	短所
方法1	ルーティングと独立にセキュアネットワークを定義できる。データリンク層だとIEEE 802.10[1]で規定されるタグが使用可能。復号時に暗号鍵の決定が容易。	タグの付加によりMTUを越えた場合の対策が必要。暗号装置の処理が大きい。
方法2	自由なMACアドレス単位のグルーピングが可能。	ルータを介したリモート通信には適用できないためブリッジネットワークの範囲内でしか使えない。
方法3	自由な個別ネットワークアドレス単位のグルーピングが可能。ルータを介した暗号通信にも適用可能。	セキュアネットワークとルーティングの単位が独立であるため、管理情報の設定／保守の負荷が大きい。暗号化／復号に際しアドレス比較の負荷が大きい。
方法4	セキュアネットワークがルーティングの単位と対応するため、管理情報の設定／保守の負荷が軽減される。ルータを介した暗号通信にも適用可能。	セキュアネットワークをサブネットワークの集合として定義する必要がある。

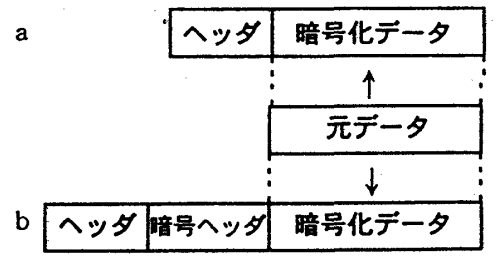

図1　エンカプセル方式

(1) 暗号ヘッダ内の情報

次の情報の搭載が考えられる．

(a) 暗号プロトコルの識別子／版番号

拡張性を確保するためにはあった方が良い．

(b) 暗号アルゴリズム識別子／初期値など暗号パラメータ

暗号アルゴリズムや暗号モードの選択が可能になる．

(c) 鍵識別子

同一の暗号アルゴリズムでも，鍵を複数用いることにより端末をグループ分けできる．鍵はアドレスに対応づけても良いが，鍵識別子があれば復号時の処理が容易になる．

(d) セキュアネットワーク識別子

セキュアネットワーク毎のアクセス制御などに利用できる．アドレスに対応づけても良いが，本識別子があれば復号時の処理が容易になる．

(e) 認証情報

暗号ヘッダ内の情報の正当性を保証し改竄を防止するため，ディジタル署名などの認証情報を設ける．

(2) エンカプセルフォーマット

次の両者があり，比較を表２に示す．本稿では，以下(b)の場合を検討する．

(a) ネイティブエンカプセル: 暗号ヘッダと暗号データを，ネットワーク層プロトコルのデータフィールドにそのまま入れる．

(b) IPエンカプセル: 暗号ヘッダと暗号データをIPパケットでエンカプセルし，IPトンネル方式で転送する．

表２　エンカプセルフォーマットの比較

	長所	短所
(a)	IPエンカプセルに比べ処理負荷が小さい。暗号化時のデータ長の増加が最小限である。	ネットワーク層プロトコル毎に（ルータなど中継ノードで透過的に）暗号データが中継できることを保証する必要がある。
(b)	暗号データの中継網がIPをサポートすれば、暗号化対象のすべてのネットワーク層プロトコルが中継できる。	処理負荷が大きい。3.2に述べる課題の解決が必要。暗号ヘッダに加えエンカプセル用の情報を付加するため、データ長が長くなる。

3.2 IPトンネルによる実現の課題

(a) アドレスのマッピング

IPトンネルにおいては，エンカプセルされるプロトコルのネットワークアドレスとIPトンネル終端を収容する装置のIPアドレスを対応付ける必要がある（例えばNetWare/IPではIPXのネットワーク番号をサーバに登録し検索するようにしている）．この対応付けはアドレスマッピングテーブルを各装置に持たせることで可能であるが，装置数が増えるとマッピングテーブルの保守コストが膨大なものになる．解決策としては，４に示すDNSを用いたマッピング情報の配布が考えられる．

(b) エンカプセルフォーマット

転送データをSNAP，PPP，GME，ESP[5]あるいは独自形式でエンカプセルしIPデータとして運ぶ方法が考えられる．標準として確立されたものはまだない．

(c) ICMPパケット

暗号データをエンカプセルしたIPパケットに中継途中で障害が検出されICMPパケットが返送された場合への対処が課題である[4].

(d) MTU超過時のフラグメント

暗号ヘッダ等の挿入により暗号パケットがMTUを越える場合，そのままではLAN上へ送出できない．IPトンネルではフラグメントによりパケットを分割して送出することが可能であるが，暗号化／復号に加え分割／組み立てのオーバヘッドが加わることで，性能面や輻輳の対策が必要になると予想される．

４．DNSによるアドレスマッピング

本稿では，新たなDNSレコードを定義し，これを宛先端末アドレスからIPトンネル端点アドレスを導出するため用いることを提案する．

セキュアネットワーク構築のためDNSを用いる場合，DNSのセキュリティ確保が前提となる．一例として，暗号ルータには使用するDNSサーバのIPアドレスを登録しておき，DNSのリクエスト先を限定する，またアドレス導出に用いるDNSレコードにはディジタル署名による認証情報を含ませ，レコードの改竄／偽造を防止する，といった対策が考えられる．

図２にDNSを用いた通信シーケンス例を示す．

① 暗号ルータは端末Aからの平文パケットを受信すると，宛先（端末Bのアドレス）をDNSサーバに問い合わせる．
② DNSサーバは端末Bが用いる復号ルータのアドレスを応答として返す．この時，共用鍵やセキュリティラベルに関する情報も返して良い．
③ 暗号ルータは復号ルータ宛に暗号パケットを送信する．
④ 復号ルータは暗号パケット内の暗号ヘッダを見て共用鍵を決定し，パケットを復号した後端末Bへ送信する．
⑤ 暗号ルータはDNSサーバから得た情報をキャッシュに蓄えるので，端末Aからの2番目以降のパケットは，DNSサーバへの問い合わせ無しに暗号化され送信される．

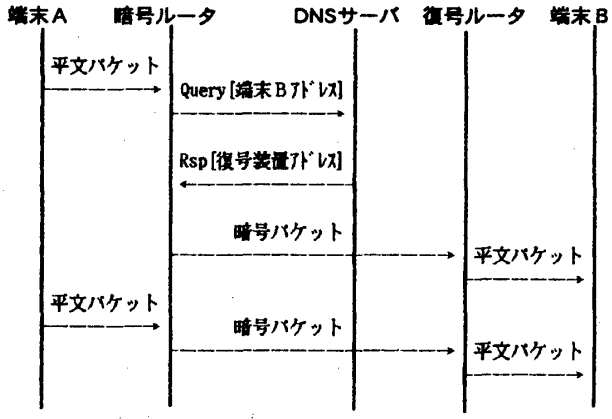

図２　DNSを用いた暗号通信のシーケンス

５．まとめ

パケット暗号化方式とルーティングとの対応づけや暗号データのエンカプセルにおける選択肢を評価し，特にIPエンカプセル方式を検討した．この時端末アドレスとIPトンネル端点アドレスのマッピングを動的に実行するため，DNSの利用を提案し，通信シーケンス例を示した．

今後はDNSが持つセキュリティ上の弱点の解決方法を検討し，さらに実装／評価を行う予定である．

参考文献

1. IEEE 802.10, "Interoperable LAN/WAN Security (SILS), 1992, 1993.
2. RFC 1034, "Domain Names - Concepts and Facilities", 1987-11.
3. RFC 1035, "Domain Names - Implementation and Specification", 1987-11.
4. RFC 1241, "A Scheme for an Internet Encapsulation Protocol: Version 1", 1991-7.
5. Internet Draft, "IP Encapsulating Security Payload (ESP)", draft-ietf-ipsec-esp-01.txt, 1995-4.