5Q-09 動的経路変更に対応した暗号化通信中継方式の提案

日下 貴義　　田中 俊介　　吉谷 文徳　　松田 栄之
株式会社ＮＴＴデータ　情報科学研究所
E-mail：{kusaka,shun,yositani,matu}@rd.nttdata.co.jp

1. はじめに

企業間や組織内の情報通信基盤となるTCP/IPをベースとしたネットワークにおいて、他組織や他人が容易にその通信内容を解読できないことが望まれているとき、通信の暗号化を図る方法が一般的である。代表例として、中継装置（以下、ノードと呼ぶ）によるIPSec[1]を使ったVPN(Virtual Private Network)と呼ばれる暗号通信がある。また、ミッションクリティカルなイントラネットなどでは、冗長な通信経路を設定し、通信経路障害から回復するための動的通信経路変更方式（以下、経路制御プロトコルと呼ぶ）が使われる。以上のような通信暗号化と経路制御を、現状の方式のままで組み合せて使用する場合、経路障害による動的経路変更が起こると、暗号化通信ができない問題がある。本稿では、動的経路変更が発生した場合、暗号通信が不可能になることを説明し、その解決策を提案する。

2. 動的暗号化通信経路制御方式の提案

2.1. 従来方式の問題点

動的経路制御プロトコル[i]と暗号鍵生成方式(IKEなど)[ii]を併用する場合、復号化装置の障害などで動的に通信経路の変更を行ったとき、暗号通信内容の復号化ができなくなるという問題が存在する。その原因は、図1でわかるように経路制御プロトコルと暗号鍵生成の連携ができていないため、復号化装置（復号鍵）の変更があっても、それに対応した適切な暗号鍵を送信側で選択できないことである。

2.2. 提案方式の概要

前述の問題を解決するために、経路制御プロトコルに暗号鍵情報を付加する動的暗号化通信中継方式を提案する。提案方式は、経路制御プロトコルで通常やりとりする経路情報に加え、どのノード（またはネットワーク）と暗号通信ができる状態にあるか（暗号通信を希望している、または暗号通信を受信できる）の情報もやりとりする。具体的には、以下のような動作をノードが実施することによる。

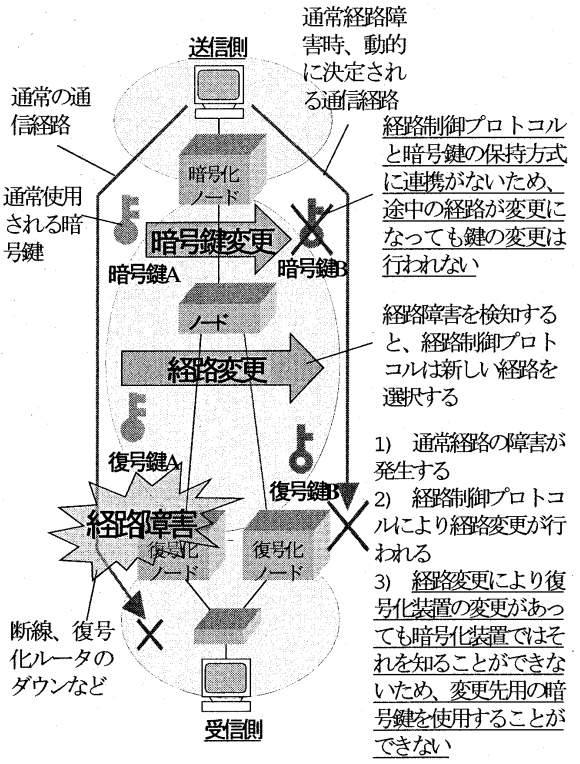

図１　従来方式の問題

1) 通常時、ノード同志が経路制御プロトコルで定期的に交換される情報に、ノードが持つ暗号通信用情報として以下の2つの情報も交換する。
   a. 暗号化通信を実施できる（暗号化/復号化できる）ノードの識別子（またはネットワークの識別子）
   b. 暗号通信を受け持つことのできるノードの識別子（またはネットワークの識別子）

   以上の情報により、暗号化通信ができるノード（またはネットワーク）を決定できる。
2) 経路障害発生時、経路制御プロトコルにより新経路に、いままで経由していた復号化装置が含まれないことを知る。
3) 2)の後、1)により他の暗号通信ができる中継装置を知り、対応する暗号鍵を予め鍵生成したあった中から選択するかIKEなどで再生成する。

Encrypted Communication System Adapted Dynamic Routing Protocol
Takayoshi Kusaka, Shunsuke Tanaka, Fuminori Yoshinani, Shigeyuki Matsuda
Labortory for Information Technology, NTT DATA

[i] OSPF、RIP、EIGRP など
[ii] 一般にIKE (Internet Key Exchange)[2]を使用

以上から、動的に新経路が作成された後も適切な暗号鍵/復号鍵の組合せにより通信が再開できる。

2. 3. 実装例

TCP/IP 上の代表的な経路制御プロトコルの例として、OSPF(Open Shortest Path First)[3]に提案方式を適応した場合は以下のようになる。

1) OSPF のリンク状態広告パケット (LSA[iii]) のタイプ 1 ルータリンクに、暗号化通信の存在を示す情報（リンクタイプ 5）の追加を行う。この情報は前述の 3.2 項 1) a、b の情報が記述される。OSPF としては表 1 のような意味を持つことになる。
2) 図 2 を例に、動作は以下のようになる。
   ① net α→net β の通信は、通常時ノード A-B 間で暗号鍵 A により暗号通信が行われる。
   ② ノード B に障害が発生すると、経路制御プロトコルにより新経路が作成される。新経路からはノード B が消え、ノード C が出現する。
   ③ ノード C から OSPF によって送られてくる LSA で、ノード A は net α→net β の暗号通信にノード C 用の暗号鍵 B を選択すべきことを知る。

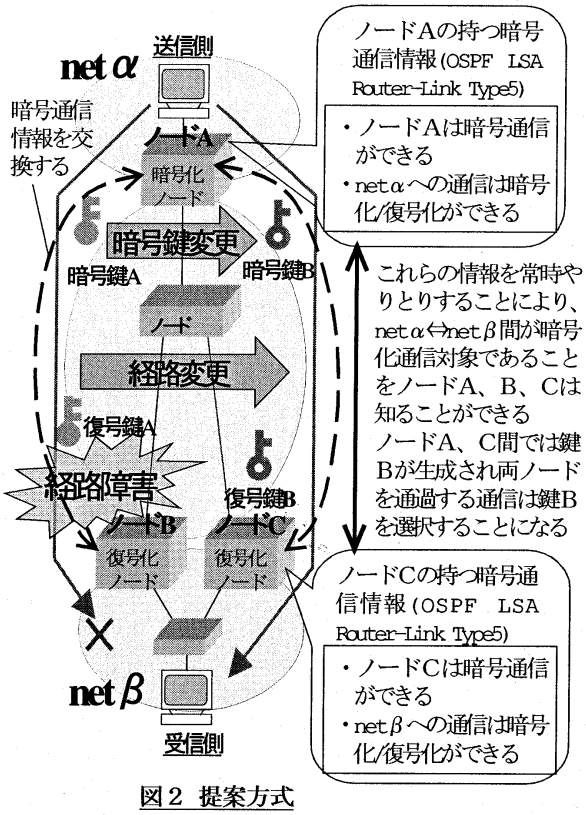

図 2 提案方式

[iii] Link State Advertisement ノード間でやりとりされる経路情報

以上から、経路変更にあわせて適切な暗号鍵の変更も行われるようになる。

表 1 LSA(ルータリンクタイプ)の内容

タイプ番号	内容	リンク ID (情報 a に相当)	リンクデータ (情報 b に相当)
5 (追加タイプ)	暗号通信	暗号通信ができる自ノードの IP アドレスや ID、インタフェース番号、インタフェースアドレス	暗号通信を受け持つことができるネットワークアドレス、ホストアドレスノードの IP アドレス (Null の場合は，まだ決定されていないどこかと暗号通信ができることを示す)

※ タイプ番号 1～4 までは既存

3. 考察

本提案方式は、経路制御プロトコルの使用が前提となるため、経路制御プロトコルを中継しないネットワークでは適用できない。したがって、主な適用場所は、比較的規模が大きく可用性とセキュリティが求められる閉域網であり、組織間のイントラネット/エクストラネットにおいて有効である。

さらに、本方式のメリットとして、移動ネットワークのように、通常時でも通信経路が動的に変更されるような場合や通信先が固定的でない場合でも、送信元が受信先に合わせて動的に暗号鍵を変更し、通信の自動継続を可能にする点がある。

なお、個人を対象とした暗号通信技術の主流は SSL であり、これはエンド-エンドの暗号化通信を可能としている。この場合、動的経路変更によっても復号鍵の変更は起こり得ず、本提案方式は不要である。しかし、端末のパフォーマンスや実装の容易さという点、VPN といった利用形態がある限り、ネットワーク機器による暗号化も必要であり続けると考えられ、本提案方式が適応できる。

4. まとめ

以上、従来の動的経路制御方式と暗号鍵生成方式を併用するとき発生する問題点を、本提案方式が解決し、動的経路変更後も暗号通信が自動的に継続できることを説明した。

【参考文献】

[1] S.Kent," Security Architecture for the Internet Protocol"(RFC 2401),
[2] D.Harkins, D.Carrel , "The Internet Key Exchange"(RFC 2409)
[3] J.Moy , "OSPF Version 2" (RFC2328)
[4] C.Huitema ,"Routing In The Internet"
[5] W.R.Stevens,"TCP/IP Illustrated, Volume1"