リピータ型IPSEC暗号装置の冗長化方法の検討

時庭康久† 稲田徹† 宮川明子† 後沢忍†
三菱電機(株)情報技術総合研究所†

１．はじめに

近年、暗号を用いたインターネットVPN(Virtual Private Network)が普及し、業界標準であるIPSEC(Internet Protocol Security)規格が用いられている。中継装置でIPSEC機能を実現する場合、IPSECルータをネットワークに設置する場合が多い。一般的にルータには、冗長化プロトコルとして、VRRP(Virtual Router Redundancy Protocol)が実装され、故障時などに容易に切り替えられる仕組みを備えている。

一方、我々はネットワークアドレスに依存せずに導入可能なリピータ型のIPSEC装置を提案[1][2]しており、IPSECルータと異なる方法で冗長化を実現する必要がある。本稿では、リピータ型IPSEC中継装置に適した冗長化方式について提案する。

２．課題

(1)リピータ型暗号装置の特性による課題

通常、中継装置の冗長化方法では、自装置が動作していることを通知するVRRPや、装置間を通信回線とは別の管理用回線で接続して監視し、異常検出と同時に中継装置を切り替える。また、図１に示す暗号装置＃１から暗号装置＃２に切り替わった時、システム全体の冗長性を維持するため、左右のスイッチの転送動作も同時に切り替える必要がある。しかし、リピータ型のIPSEC装置の場合、暗号装置はMACアドレスを付け替えずにそのまま中継するため、暗号装置が切り替わったことをスイッチが中継データのMACアドレスから識別することができない。

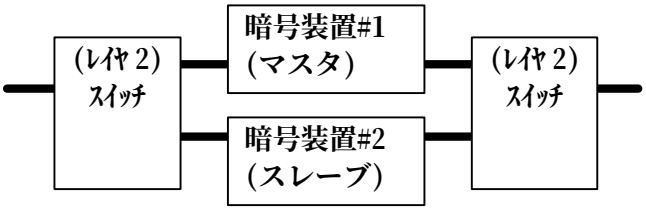

図1. 暗号装置の冗長化構成

(2) SAの引継ぎに関する課題

IPSECでは、SA(Security Association)と呼ばれる論理的な暗号通信路上でデータを送受信する。暗号装置が切り替わった時、新たに一からSAを確立し暗号用鍵や認証用鍵を生成すれば良いが、Diffie-Hellmanの多倍長演算などでリソースを必要とし処理時間が掛かる。アプリケーションの特徴やネットワーク構成によっては、通信が中断されることを避けるため瞬時に切り替える仕組みが必要である。

３．提案方式

(1)経路切り替えの対処方法

回線を分岐させる方法（図２）や専用の切り替え装置を導入する方法(図３)がある。前者は、信号の分岐による物理層の様々な問題があり、後者は、製造コストが掛かる。

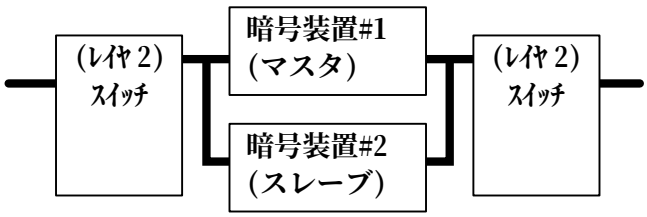

図２．回線分岐による冗長化構成

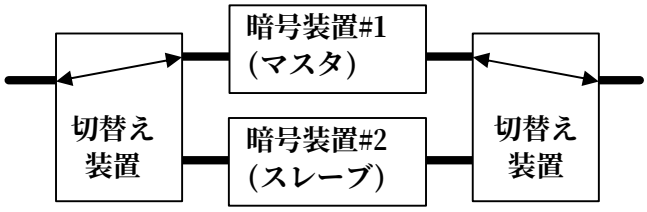

図３．切り替え装置による冗長化構成

そこで、暗号装置が平文で中継するデータのMACアドレスを学習し、学習したMACアドレスを送信元アドレスとするデータを送信することによって、スイッチの転送動作を切り替える方式を考案した(図４)。

A Study of Redundancy on IPSEC Encryption Equipment.
Yasuhisa TOKINIWA, Toru INADA, Akiko MIYAGAWA, Shinobu USHIROZAWA
Information Technology R&D Center, Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, 247-8501 Japan

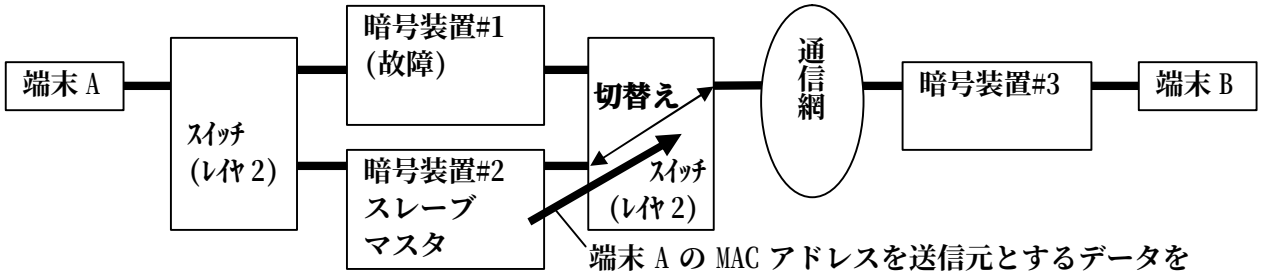

図４．スイッチの経路切り替え

(2)切り替え時の SA 確立と SA 引継ぎ

IPSEC では、SA ごとに暗号用鍵や認証用鍵を生成し暗号装置間で維持している。暗号装置を瞬時に切り替えるためには、これらの鍵情報を瞬時に引き継ぐ必要がある。これに対し、冗長化構成を成す複数の暗号装置の IP アドレスを同一に設定し、SA の鍵情報を共有する方法がある。例えば、マスタの暗号装置からスレーブの暗号装置に SA 情報をコピーする（図５）。しかし、ESP(Encapsulating Security Payload)のシーケンス番号などの動的に変わるパラメータを引き継いで(コピーして)SA を継続して暗号通信させるのが難しい。

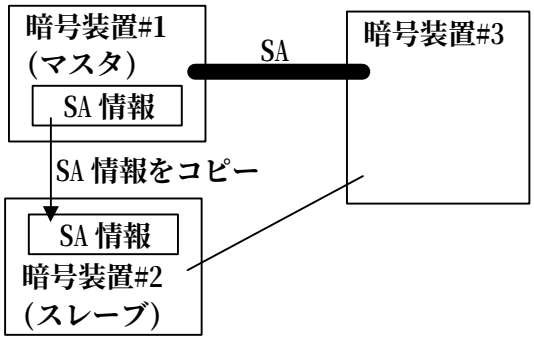

図５．SA 情報のコピーによる切り替え動作

提案方式では、冗長化構成を成す複数の暗号装置に異なる IP アドレスを割り振る。冗長化構成の暗号装置と暗号通信する対向の暗号装置の SPD(Security Policy Database)には、マスタ/スレーブの種別を区別すること無く複数登録する。IKE の Initiator 側(発呼側)になった場合は、登録してある全ての SA を確立する。SA を確立すると同時にマスタの暗号装置は、マスタ通知を対向の暗号装置へ通知する。マスタ通知を受信した暗号装置はマスタ通知を受けた暗号装置との間で確立した SA を用いて暗号通信する。マスタ通知を受けなかった SA を保持して、いつでも切り替えられるように待機する。IKE の Responder 側(着呼側)になった場合も、マスタ通知を受信した SA のみを利用して暗号通信し、マスタ通知を受けなかった SA を保持し、切り替えられるように待機する。図６では、暗号装置＃２がスレーブからマスタに遷移した場合の動作を示している。図６の暗号装置＃１が故障などから復帰した場合は、暗号装置＃１側から SA を確立しマスタ通知を送信し、暗号装置＃３の動作を切り替えて元の状態に戻る。

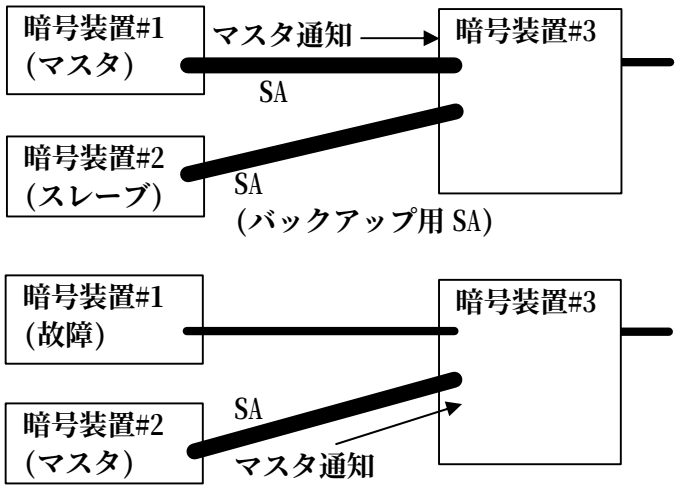

図６．マスタ通知による SA 切り替え動作

４．まとめ

リピータ型の IPSEC 暗号装置の冗長化について検討結果を述べた。実際に作成し検討結果を評価していく所存である。今後は、IPSEC の NAT 対応や大規模なシステム構成時の処理方式を検討する予定である。

参考文献

[1]稲田他“VPN(Virtual Private Network)構築技術の検討・リピータアーキテクチャ”，情報処理学会第 61 回(平成 12 年後期)全国大会
[2]後沢他“暗号による VPN(Virtual Private Network)方式の検討と実現”，信学技法 NS2003-114