VPN(Virtual Private Network)装置における IPSEC の実装方法の検討

4G−2

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)が普及しつつあり、業界標準である IPSEC(Internet Protocol Security)規格が用いられている。IETF(Internet Engineering Task Force)は、RFC2401〜2412 を IPSEC の規格として定めている。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している。SA の確立／解放に関する実装上の問題点について検討したので報告する。

2．IPSEC／IKE の仕組みと問題点

IPSEC 装置間では、DES などの秘密鍵暗号通信に用いる暗号鍵や、SHA-1(Secure Hash Algorithm)などの鍵付きハッシュ関数に用いる認証鍵を IKE(Internet Key Exchange)プロトコル[1]で共有する。

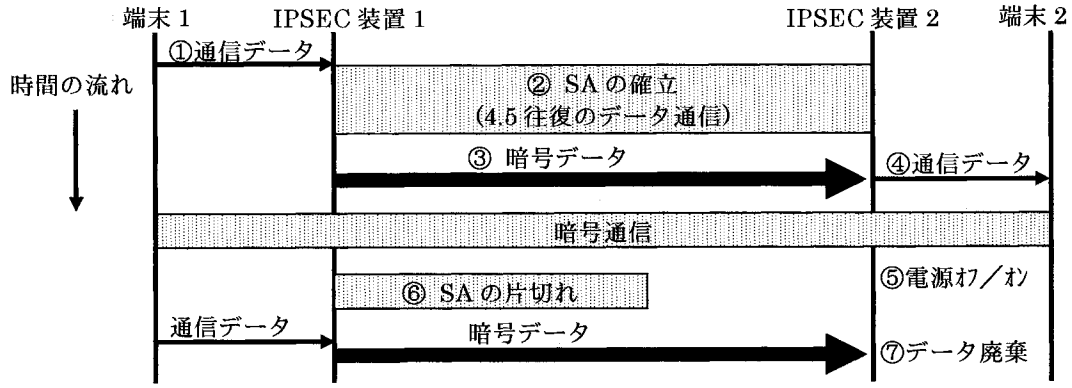

図 1　IKE の動作概要と SA の片切れ

図 1 は IPSEC の動作概要であり、①端末 1 から端末 2 へのデータを送信し、②IPSEC 装置 1 と IPSEC 装置 2 間で IKE により SA を確立し、③SA 確立し共有した鍵を用いて暗号／認証したデータを IPSEC 装置 1 から IPSEC 装置 2 へ送り、④IPSEC 装置 2 で復号したデータを端末 2 へ送信し端末 2 はデータを受信する。また、図 1 において、⑤IPSEC 装置 2 を電源オフ／オンにより立ち上げると、⑥通常は IPSEC 装置 2 において確立した SA の鍵を消失してしまい、⑦IPSEC 装置 1 で暗号したデータを廃棄してしまう。一方、装置 1 側は相手側の SA が消失したことを認識できないためデータを送り続ける。この状態を SA の片切れと呼ぶ。SA の片切れは、IKE プロトコルの状態遷移が明確に規定されていないために起こる。

3．SA 片切れの回避策

本状態を回避するために以下の５つの方法について検討した(図２〜図６)。これらの検討結果は、他社製品との相互接続試験で得られた結果を参考にしている。

(1)SA の life time(寿命)を短く設定し SA 片切れの期間を短縮する。lifetime 満了時、該 SA は解放され、次の通信発生時に再確立される。

(2)装置を立ち上げ後、SPD(Security Policy Database)に設定されている情報に従って、全ての IPSEC 装置に対して SA を確立する。装置 1 側では装置 2 宛の同じ SA が二個できることになるが最新の SA の情報(鍵)

A Study on IPSEC Implementation in virtual private networks equipment.
Yasuhisa TOKINIWA, Toru INADA, Akiko Miyagawa, Shinobu USHIROZAWA
Information Technology R&D Center, Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, 247 Japan

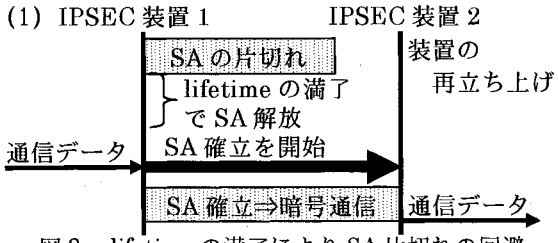

図２．lifetime の満了により SA 片切れの回避

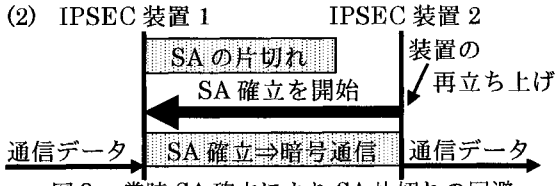

図３．常時 SA 確立により SA 片切れの回避

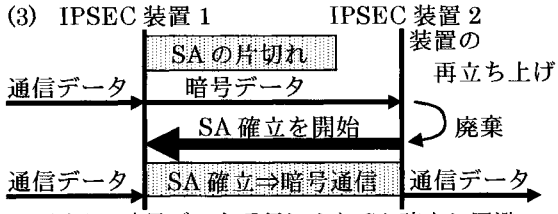

図４．暗号データ受信により SA 確立し回避

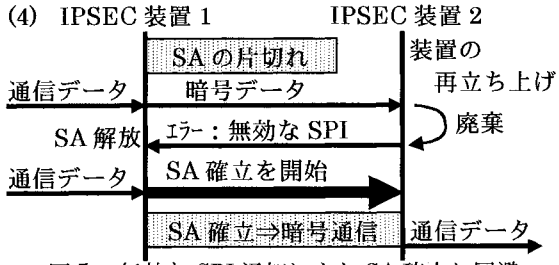

図５．無効な SPI 通知により SA 確立し回避

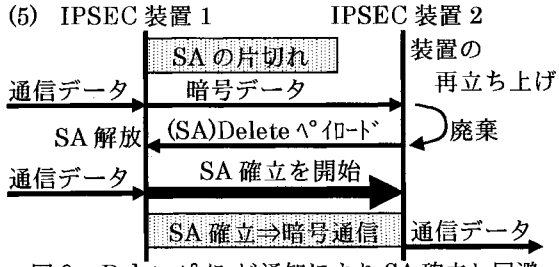

図６．Delete ﾍﾟｲﾛｰﾄﾞ通知により SA 確立し回避

を用いて暗号通信する。

(3)SA を未確立にも関わらず、暗号されているデータを受信したならば、initiator になって SA を確立する。SA を確立後は、二者間で確立した最新の SA の情報によって暗号通信する。

(4)SA を未確立にも関わらず、暗号されているデータを受信したならば、ISAKMP Information Exchange(エラーコード INVALID-SPI)と呼ばれるエラー通知を通信相手に送り、相手側からの SA 確立を促す。

(5)立ち上げを実施した装置は、立ち上げ前に確立している SA の状態を不揮発性メモリ(ハードディスクやフラッシュメモリなど)に記憶しておき該 SA 宛のデータを受信した場合、ISAKMP Information Exchange に Delete ペイロードを付加して送信し、これを受信した IPSEC 装置は、Delete ペイロードで指定された SA を解放する。

各方法の評価 ：

(1)～(3)については、通信相手の実装状況によらず、実現可能である。(4)～(5)については、ISAKMP Information Exchange 受信後の動作は規約として定められていないので他社製品との接続においては必ずしも通信相手がこちら側の意図する動作をしないため、実使用には向かない。(1)については、SA の片切れの時間が短くはなるが完全に問題を解消しない。(2)については、通信が無いにもかかわらず SA を確立しリソースを消費してしまう問題はあるが re-keying と呼ばれる SA 再確立の動作をほとんどの IPSEC 装置が実装していることから一番良い解決方法である。(3)については、暗号データを送り込むことにより、SA 確立動作処理のためのリソース消費攻撃が可能である。

IPSEC 機能を内蔵したモバイル端末との通信では、モバイル端末は IPSEC の responder 機能を実装していない場合も多いので、サーバ側が電源オフ／オン後 initiator になった場合、(2)と(3)では動作しないので、(1)の方法が最良である。

４．まとめと今後の展望

IPSEC の SA の片切れについての実運用上での解決方法を検討した。今後の課題として IKE、SPD、AH/ESP の高速処理のための実装方法の検討、認証局やディレクトリサーバと連携させた SPD の高機能化が挙げられる。

参考文献　[1] RFC2409 : The Internet Key Exchange (IKE)