4G－3

VPN(Virtual Private Network)構築技術の検討・PKI対応システム

時庭康久　永嶋規充　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にPKI(Public Key Infrastructure)を導入し、企業等の大規模／中規模システムに適用する方法を検討したので報告する。

2．IPSEC／IKEの仕組み

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。IKEにおけるIPSEC装置間での認証方法には、秘密情報を事前に共有する方法、RSAの公開鍵を事前に共有する方法、PKIに対応し認証局[2]が発行したX.509の認証書を利用する方法が規定されている。秘密情報をニ者間で事前に共有する方法は、小規模のシステムに向いているが大規模なネットワークでは、秘密情報の管理が複雑になる。RSAの公開鍵を事前に共有しRSA演算をする方法は、システム上で公開鍵を管理する仕組みが必要である。認証書(PKI)を利用する方法は、CA局を構築すると初期コストが増大するが、IPSEC装置の台数が増えるほど認証書の管理運用をCA局に任せられるため運用が容易になる。

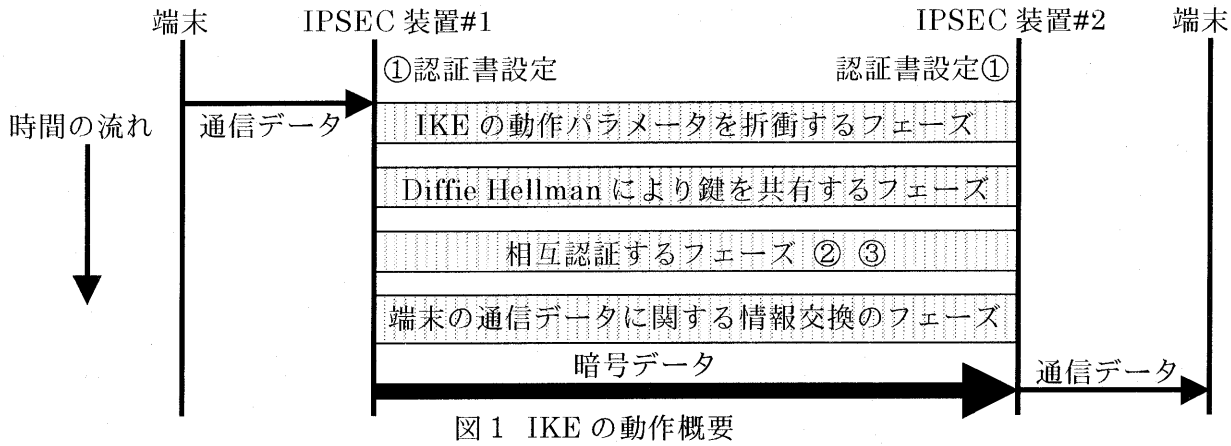


図1　IKEの動作概要

図1はIKEの動作概要であり、PKI導入時の認証書の運用手順を以下に示す。①CAが発行した認証書をIPSEC装置に設定する。②IPSEC装置は、認証書を交換する(図1の相互認証するフェーズ)。③IPSEC装置は、受け取った認証書を検証しデジタル署名を使用し互いに認証する(図1の相互認証するフェーズ)。

3．PKIの実装について

PKIの実現には、ASN.1、PKCS等のデータ変換処理やRSA演算等の暗号アルゴリズムを実装する必要があり、これらはメモリとCPU時間を大量に必要とする。特に使用する鍵を共有するIKEのプロトコルが終了するまで(図1に示した各フェーズが終了するまで)先頭の通信データが一時的に内部に保留されるため通信遅延が発生する。そこでSA(Security Association)と呼ばれる暗号通信論理パスを事前に確立しておくことにより通信遅延を小さくすることとした。

Construct of virtual private networks by public key infrastructure.
Yasuhisa TOKINIWA, Norimitsu NAGASHIMA, Toru INADA, Akiko Miyagawa, Shinobu USHIROZAWA
Information Technology R&D Center, Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, 247 Japan　(E-mail：toki@isl.melco.co.jp)

IPSEC 装置が通信相手の認証書を取得する方法には、予め配布しておく方法と IKE のオプションである認証書を交換する方法が定義されている。また、IPSEC の動作設定パラメータの概念を SPD(Security Policy Database)と定義している。SPD のパラメータとして IPSEC 装置を識別する識別子は、通常は IP アドレスであり、X.509 の認証書を識別するものは識別名(Distinguish Name)である。

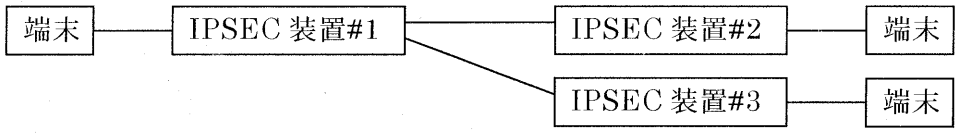
通信相手の認証に関して、以下の 4 つの方法を検討した。（図 2 参照）

案 1. 通信相手の IP アドレスごとに認証書を予め SPD として装置に設定しておく。鍵共有時、設定してある認証書内の通信相手の公開鍵を使用し相互認証し鍵を共有する。

案 2. 認証書を交換し、通信相手から受け取った認証書を通信相手の IP アドレスに無関係に処理する。認証書の正当性を確認した場合、相互認証し鍵を共有する。

案 3. IP アドレスと認証書の識別名を組みにして SPD に設定する。認証書を交換し IP アドレスと組を成す識別名と通信相手から受け取った認証書の識別名が一致した場合、相互認証し鍵を共有する。

案 4. 予め認証書の属性値や識別名に認証書の持ち主の IP アドレスを設定しておく。認証書を交換し、通信相手の IP アドレスと認証書内の IP アドレスが一致した場合、相互認証し鍵を共有する。



案 1.

装置#2 の IP ｱﾄﾞﾚｽ ⇒ IPSEC 装置#2 の認証書（予め設定されている）
装置#3 の IP ｱﾄﾞﾚｽ ⇒ IPSEC 装置#3 の認証書（予め設定されている）

案 2.

装置#2 の IP ｱﾄﾞﾚｽ ⇒ 受信した全ての正当な認証書の装置と通信可能
装置#3 の IP ｱﾄﾞﾚｽ ⇒ 受信した全ての正当な認証書の装置と通信可能

案 3.

装置#2 の IP ｱﾄﾞﾚｽ，装置#2 の識別名 ⇒ 受信した認証書内の識別名が一致すれば通信可
装置#3 の IP ｱﾄﾞﾚｽ，装置#3 の識別名 ⇒ 受信した認証書内の識別名が一致すれば通信可

案 4.

装置#2 の IP ｱﾄﾞﾚｽ ⇒ 受信した認証書の属性値に装置#2 の IP ｱﾄﾞﾚｽがあれば通信可
装置#3 の IP ｱﾄﾞﾚｽ ⇒ 受信した認証書の属性値に装置#3 の IP ｱﾄﾞﾚｽがあれば通信可

図 2. IPSEC 装置#1 内でのデータの保持方法の概念

案 1 は、認証書の管理方法が複雑になる。通信相手の認証書を設定するには、ローカルコンソールからの入力や FTP 等により管理装置／DAP サーバから認証書をダウンロードにより可能である。案 2～4 は、セキュリテイ強度の強い順に案 4＞案 3＞案 2 であり、運用の容易さの順に案 2＞案 3＞案 4 であり、トレードオフの関係にある。案 4 は、IP アドレスを変更するたびに認証書を再発行する必要があり運用コストが大きいと判断し不採用とした。認証書を交換した方が運用が容易であるため、案 2 と案 3 が望ましいと考える。

4．まとめと今後の展望

PKI 対応にする場合の IPSEC での認証書の運用管理方法についてまとめた。PKI 対応にした利点として IPSEC 装置は課金情報や各種統計情報などにデジタル署名をすることが可能になる。今後の課題として LDAP(Lightweight Directory Access Protocol)とシステム運用管理との最適な方式検討や認証局と連携させた SPD の高機能化が上げられる。

参考文献

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

[2] 佐伯他：”公開鍵インフラストラクチャ構築技術”，三菱電機技報 Vol72 No5 ’98 5