IPSECの鍵管理方式に関する考察

1T－1

堤 俊之　鮫島 吉喜
日立ソフトウェアエンジニアリング(株)

1.はじめに

インターネットの商業利用が本格化している昨今その安全性を確保するために、多くのセキュリティ技術が研究･開発されている。なかでも、インターネット基盤を構成する上で欠かすことのできない IP (Internet Protocol) に認証機能や暗号機能を組み込んだ IPSEC[1] (IP SECurity) は、今後必要となる金銭情報や組織内機密情報、プライバシィ情報などを安全に交換できる標準プロトコルとして注目を集めている。

しかし、この IPSEC を組織内ネットワークに単純に適応した場合、組織内ネットワークの管理者は監視できない通信を許可することになり、組織内機密情報の漏洩や組織内ネットワーク不適切な利用を管理できなくなるという問題が発生する。

そこで、本稿では IPSEC を組織内ネットワークで運用する場合に、管理者が暗号通信を監視できる方式を提案する。

2.IPSECによる暗号通信の前提

IPSEC は、通信データを暗号化するセッション鍵や暗号方式などの SA (Security Assocication) が送受信者間で共有されている前提で、認証機能や暗号機能を実現している。そして、送受信者間の SA の共有は現在標準化されつつある鍵交換プロトコル(ISAKMP や SKIP など)で行われる。

本稿では、この SA の交換が予め設定された時間間隔毎に更新される場合を考える。

A Study of Key Management for IPSEC
Toshiyuki Tsutsumi, Yoshiki Sameshime
Hitachi Software Engineering Co., Ltd.
6-81 Onoe-cho, Yokohama, Kanagawa 231 Japan

3.提案方式

従来の暗号鍵回復方式はファイルやメッセージを対象にしていたが、ここでは、IPSEC に適応する鍵管理方式を示す。

3.1 構成

図１は、本提案方式の構成を示したものである。それぞれの要素は、自身の公開鍵と個人鍵を保持している。

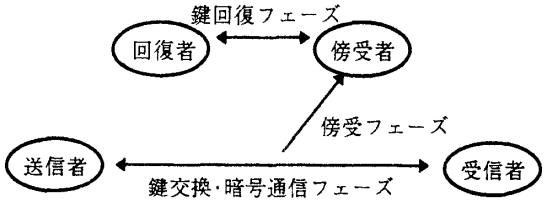

図１

送信者･受信者：セッション鍵の共有を行い、暗号通信を行う。通信端末やユーザなどである。
傍受者：送信者と受信者の間の通信を監視する。
回復者：正当な傍受者からの要求により暗号化セッション鍵データを復号する。

3.2 手順

3.2.1 鍵交換･暗号通信フェーズ

本提案方式の鍵交換･暗号通信フェーズの手順を図２に示す。

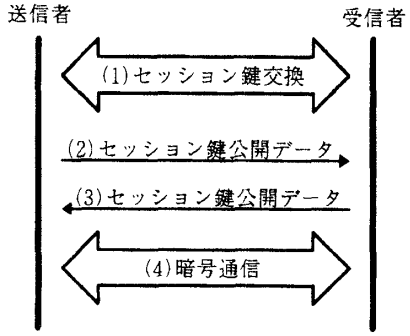

図２

(1)送信者と受信者が鍵交換プロトコルによりSAを交換･共有する。

(2)送信者が送信者から受信者へのセッション鍵公開データを転送する。このデータは、傍受している第三者に公開する目的で送信しているので、受信者は保持しない。セッション鍵公開データを以下に示す。

|送信者識別子、受信者識別子、暗号化セッション鍵$_{回復者}$、デジタル署名$_{送信者}$|

*暗号化セッション鍵*は回復者の公開鍵により暗号化されている。したがって、復号できるのは回復者だけとなる。*デジタル署名$_{送信者}$*はセッション鍵公開データの作成者である送信者の署名である。

(3)同様に、受信者が受信者から送信者へのセッション鍵公開データを転送する。

(4)送信者と受信者間が暗号通信を開始する。

(5)セッション鍵の有効期限が切れると、送信者と受信者は、鍵交換プロトコルによりSAの更新を行う。

(6)(2)から(4)の手順を実行し、(5)へ。

3.2.2 傍受フェーズ

(1)傍受者が特定の送信者と受信者の鍵交換･暗号通信フェーズでの交換データを傍受する。

(2)傍受者は、傍受データがセッション鍵公開データならば、鍵回復フェーズへ進み、暗号通信データを復号するためのセッション鍵を取得する。

(3)傍受者は、傍受した暗号通信データを回復用セッション鍵で復号する。

3.2.3 鍵回復フェーズ

(1)傍受者はセッション鍵回復要求データを送信する。セッション鍵回復要求データを、以下に示す。

|傍受者識別子、セッション鍵公開データ、デジタル署名$_{傍受者}$|

*デジタル署名$_{傍受者}$*は傍受者の署名である。

(2)回復者は*デジタル署名$_{傍受者}$*を検証しセッション鍵回復要求データの作成者を認証し、正しい、要求であることを確認する。

(3)回復者は*セッション鍵公開データ*のデジタル署名$_{送信者}$を検証し、傍受者が監視を許可されている通信であるか検証する。

(4)回復者は、*暗号化セッション鍵$_{回復者}$*を自身の個人鍵で復号する。

(5)回復者は回復用セッション鍵データを傍受者に返送する。回復用セッション鍵データを、以下に示す。

|セッション鍵、送信者識別子、受信者識別子、デジタル署名$_{回復者}$|

4.考察

従来までの鍵回復システムは、ファイルやメッセージなど順序のあるデータ単位に対する暗号化を回復するために、それらデータに暗号鍵回復用のデータを付加してきた。こうした方法を IPSEC に適応した場合、IPSEC パケット毎にセッション鍵回復データを付加しなければならなくなり、通信効率を悪化させる結果となる。

本稿での提案方式では、IPSEC のセッション鍵が交換される時にだけ、セッション鍵回復データを公開しているので通信効率がよい。

5.おわりに

本稿では、ＩＰＳＥＣを運用する組織内ネットワークで、暗号通信を監視できる方式を提案した。

今後は、ＩＰＳＥＣによる暗号通信システムを実装して、本稿で提案した方式を組み込んで実用性を検証する。

参考文献

[1]R. Atkinson, “Security Architecture for the Internet Protocol”, RFC1825, Auguest 1995