IPsec 相互接続実証実験報告書

日本ネットワークセキュリティ協会

2001 年 2 月 28 日

1. 実験の概要

1.1. 背景と目的

近年、コンピュータのネットワークことにインターネット環境におけるセキュリティの重要性が求められ始めている。企業間をはじめ行政のサービスをインターネット上で行う為には様々なセキュリティを確保する技術の開発は重要かつ急を要する課題である。

IPsec は多くのインターネットアプリケーションの通信プロトコルを扱うことのできるネットワーク層のセキュリティ機構として有力な地位を占めている。インターネット上で様々なタイプの情報を通信する際のセキュリティ機構として広い範囲に IPsec を適用することが期待できる。企業間やその他の組織の間での通信ではアプリケーションを限定することなく接続ができることが求められる。外部との接続のために新たなアプリケーションを開発することなく接続できることが望ましい。またネットワーク層でセキュリティ保護を実現するため上層のアプリケーションやユーザーがセキュリティを意識することなく利用が可能である。

様々な組織がそれぞれの環境から通信を行う環境では IPsec 機器はそれぞれの組織によって選択されることが予想され、異なる製品間での接続を前提条件としなければならない。しかし、現在の IPsec 機器は多くの標準化しきれない技術をそれぞれのメーカが実装していることが判っている。単一の製品を採用した場合は問題になることは無いが、異機種の相互接続では採用された技術や手順の差が問題になることは明白である。

時間とともにこれらは標準化が進むと考えられているが、段階的な導入を考えると現時点で市販されている製品から相互接続を実現していかなければならない。

本実験では組織間で異機種の IPsec 機器が採用されておりその組織間で相互接続を行うことを想定して実証実験を実施し、相互接続の可否と運用時における操作手順作成のガイドラインを作成することを目的とした。

1.2. IPsec の相互接続における問題概要

IPsec はその通信経路をインターネット上に設定して暗号化によって通信のセキュリティを守る技術である。現時点での主な使用用途は同一組織内の地方拠点との接続である。

IPsec は ITEF の発行する RFC によってすでに標準的な実装を示されている。IPsec は通信のデータを暗号化する技術と暗号化に必要な鍵を生成する技術からなる。通信データを暗号化復号化する手順は定められた演算の繰り返しである。この部分は同じ暗号復号方式を指定することができるかどうかが問題となる。よって、暗号方式の DES はほとんどの機器が採用しているため機相互接続可能と判断できる。しかし実際には暗号化復号化の鍵の生成と管理が相互接続の可否、運用の実用性を支配する。

暗号化復号化鍵は事前に定めずにそれぞれの機器で同時に生成される。暗号による保護は絶対的なものではなく常に破られる(第三者に解読される)可能性がある。盗聴を困難にしデータの改ざんや内部ネットワークへの侵入を防ぐためには、第三者の解読が完了する前に鍵は更新しつづけなければならない。

随時、鍵を交換するためには接続するそれぞれの機器で鍵を共有する手段を作らなくてはならない。一方が定めた鍵を他方に通知すれば鍵を盗聴される恐れがある。これらの理由から IKE、ISAKMP が採用されてそれぞれの機器で同じ鍵を同時に生成・管理する。鍵の生成･管理は機種ごとに解釈、拡張されて問題発生時の解決手順が異なっている。この違いが相互接続の際に不具合を生じる。

さらにもう一つ、長期にわたって通信経路のインフラとして使うためには考慮しておかなければならないことがある。電源異常や機器の故障によって機器自身を交換した場合の状況である。この場合、正常に動作していた側には鍵が残っているが、異常から回復した側では鍵を喪失してしまっている。鍵は機器同士の ID,暗号化トンネルを通過するネットワークの情報と対にして管理されているために、機器同士の情報を整合させなければ通信できない。このような状況に陥った場合に回復する手順は標準化されていない。ここでも機器ごとに異常な状況の検出やその解決方法はまちまちである。異機種を組み合わせた場合の動作は実際に試験する以外に確定させることは難しい。

2. 実験環境

2.1. 実験対象

試験対象となる IPsec 製品はすでに市販され使用実績のあり、公募に応じて供給元から試験参加の意思表明があったものとする。

以下の表は実際に参加表明が行なわれ実験が行なわれたもののリストである。開発・製造元、参加企業の名称については略称で記載した。

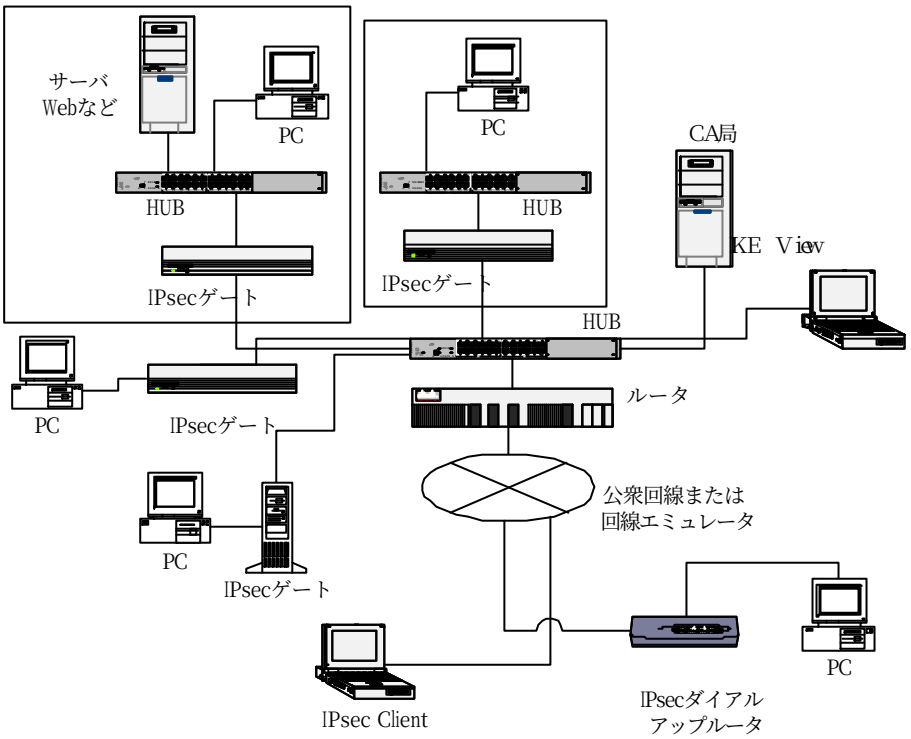
また作業の一部は工学院大学の有志学生にお手伝いいただいた。

製品名	Version	開発／製造	参加企業
Contivity Extranet Switch	2.62	Nortel Networks	ネットワンシステムズ
PERMIT Gate	3.10.010 Entrust	Alcatel	ディアイティ CRC 総合研究所
VPN-1 Solaris	4.1 sp2	Checkpoint	ENICOM フォーバルクリエーティブ
VPN-1 WindowsNT	4.1 sp2	Checkpoint	VPN-1 Solaris に同じ
VPN-1 Linux	4.1 sp3	Checkpoint	VPN-1 Solaris に同じ
Nokia IP	4.1 sp2	Nokia	ネットマークス ENICOM
AR720	2.0.2-01	アライドテレシス	アライドテレシス
Windows2000 Server		Microsoft	IRI Microsoft
FireboxII	4.5	WatchGuard	ヒューコム
Shiva VPN Gateway	6.8p3	Intel	ヒューコム
VPN3005	2.5.2	Cisco Systems	Cisco Systems ネットワンシステムズ
IOS (Cisco7100)	12.1	Cisco Systems	Cisco Systems
INFONET-VP100	02.01	古河電工	古河電工
VSU	3.0.52	VPNet	ネットマークス
IPSEC Express Toolkit	4.0	SSH	SSH
CIPro	4.47	RadGuard	東陽テクニカ
PowerVPN	6.5	Symantec	Symantec 日新電機
RAVLIN	3.4	RedCreek	日新電機
FNX0531	2.1.03	フジクラ	フジクラ
NetShelter/FW	E11L10	富士通	PFU 富士通北陸システム

2.2. ネットワーク構成

相互接続の実験を行うには多くの機器が要求される。今回の実験では実際の運用に耐えうるシステムを構築するのに最低限度必要な技術およびノウハウを収集できるような構成を目標とした。すべての資材は実験に参加するベンダーやメーカが提供できる範囲が原則であり、目標に対して不十分な点もあり今後の課題とされる点も多いものになった。

基本の実験環境は以下の図のとおり。



IKE の過程を記録、観察できるよう各 IPsec の外側を結ぶネットワークはシェアード HUB で構成した。IKE の過程は”IKEview”を用いてデコードし確認する。

3. 検証項目概要

相互接続性と運用性を検証評価するための条件を列挙し、実験の手順を考察した。試験項目を4つのカテゴリに分類した

1. 相互接続性確認 基本試験
   基本的な接続性を確認。
2. 運用性確認 基本試験
   運用をはじめる前に必要とされる確認
3. 相互説性確認 オプション試験
   デジタル証明書による機器の認証など、RFC では実装必須とされない機能を使った接続性の確認。
4. 運用性確認 オプション試験
   IPsec 機器を運用する際に有益な情報取得のための試験

今回の試験では相互接続性と運用性の基本試験を必須の試験項目とした。オプション試験については各ベンダーで任意の試験項目とし、そのつど確認項目や試験手順を評価するものとした。

試験項目の実際の実験に用いた手順および記入書式については添付資料に含めた。

3.1. サポートパラメータ確認

実験を行うにあたり事前にサポートする機能を調査した。

3.2. 接続性の評価

基本接続性

IPsec では暗号化ペイロードで通信が行なわれる前に鍵の交換が行なわれる。試験の条件として指定したパラメータに基づき鍵交換を行い、IPsec の接続で最初に行われる認証と暗号鍵の自動生成が相互接続の環境で行われることを確認する。

フェーズ 2 における ID ペイロードタイプ

Ph2 において IPsec による通信保護の対象となるネットワークの情報を交換する。VPN として用いられているのはサブネットであることが多い。ゲートの実装によってはサブネットのほかにホストアドレスや IP アドレスレンジを指定できるものが在る。この ID ペイロードタイプをサブネット以外に設定した際にも接続可能かどうか確認する。

Re-Key 動作

Re-key は SA を更新し鍵も更新する。Re-key 動作は IKE のネゴシエーションにより行なわれるため接続初期と同様に問題を起こす可能性の在る動作である。

Re-key はそれぞれの機器に設定された SA の寿命か、ネゴシエーションによって Peer より引き渡された時間が基準で行なわれる。タイミングは以下のようにして決まっている。

Re-key の行なわれるか否か
1:SA が存在するとき
2:SA が存在し、トラフィックがあるとき
re-key が行なわれる場合のタイミング
1:SA の寿命に対して特定の割合の時間を経過したとき
2:SA の寿命までの残り時間が規定の秒数に達したとき

また、イニシエータ、レスポンダの関係からその後の動作を変化させるものもある。このためにはじめに接続ができたとしても re-key に失敗して通信不能になる可能性が在る。これらを想定して re-key を発生させ通信を継続することができることを確認する。

3.3. 運用性評価

実際の運用段階に入って問題となる可能性がある点について確認する。

IP フラグメント処理

平文のデータグラムを暗号化された ESP に変換する際、新たに付加する IP ヘッダや ESP ヘッダなどによりパケットのデータ容量が増加する。ネットワークのメディアによってパケットの最大容量が定まっている。これらの理由からセキュリティゲートウェイはフラグメントの処理を行わなくてはならない。単純なフラグメント処理に加え、DF フラグの取り扱いの問題も存在する。通常、DF フラグは経路のルータに対してデータの分割を禁止するものである。DF に対する各セキュリティゲートウェイの処理の違いを確認する。

SA 消失時の回復手順問題

長期にわたる継続運用では機器自身や電源などの定期点検や異常などにより接続が一方的に切断される事態が発生する。SA 情報は各々の機器が内部に生成して保持するために、peer の喪失を容易に確認することはできない。機器が停止状態から回復し SA を再度構成する場合、動作を継続していた側の残っている SA を破棄し新たに SA を構築しなければならない。この手順について標準化されていない。現状各機器が行っている処理で対応できる範囲の見極めと、手動で回復する手順確立に必要な情報を収集する。

End to End の通信確認

具体的に相互接続の動作を確認する。TCP/IP のプロトコルで動作するアプリケーションの実際に起動し、その通信の完遂を確認する。

本実験では比較的容易に準備できる ftp と tftp を TCP、UDP それぞれの代表として採用しファイル転送で検証する。