コンピュータセキュリティ　6－6
（1999．7．9）

IPsecの相互接続性に関する現状と課題

渡辺 義則† 大浦哲生‡

(株)日立製作所 システム開発研究所†
(株)日立製作所 エンタープライズサーバ事業部‡

要旨

インターネット上にVPNを構築するための標準的な暗号通信プロトコルとしてIPsecが注目されている。IPsecは，1998年11月には自動鍵交換プロトコル(IKE)も含めた仕様がIETFでの検討を経てRFCとして公開され，それに対応した製品もリリースされ始めている。そして，異なるIPsec実装間で相互接続性を検証する動きもそれに伴って活発化してきた。その結果，現状では特にIKEにて相互接続上の問題が多く発生することが明らかになった。本稿では，最近行われている相互接続実験の実施状況と，実際に我々が開発したIPsec実装のプロトタイプを相互接続実験に持ち寄って得られた実験結果から分析，整理した相互接続上の課題について報告する。

The status and problems related with interoperability of IPsec

Yoshinori WATANABE† Tetsuo OURA‡

Systems Development Laboratory, Hitachi, Ltd.†
Enterprise Server Division, Hitachi, Ltd.‡

Abstract

IPsec technology is noticed as one of standard secure communication protocols to construct VPN on the Internet. IPsec specification including Internet Key Exchange (IKE) protocol is published by RFCs in November 1998, and some products which implements IPsec have been released now. So some events to test interoperability between the various IPsec implementations have been held in each place, and it is cleared there are many interoperability problems especially related with IKE. We describe the status of the interoperability testing events and interoperability problems found by analyzing the results of interoperability test using our prototype of IPsec implementation.

1. はじめに

企業におけるインターネット利用は近年急速に普及し，その用途は単なるWWWのアクセスやメールの利用のみならず，VPN (Virtual Private Network) 技術を利用した企業の拠点間，あるいは企業間の通信インフラへ拡大しようとしている。

インターネット上でのVPN構築に適用できる技術には種々のものが提案されているが，その一つにIPsec(IPセキュリティ)と呼ばれる技術があ

る。IPsecは，TCP/IPプロトコルスタックのIP層でパケット単位の暗号化，認証を実現するプロトコルである。TCP/UDPを利用する上位アプリケーションに変更を加えることなく，その通信内容を保護することができる特徴を持っている。また，このプロトコルはインターネット技術の標準化団体にて標準化が進められており，相互接続性のある標準の通信路暗号技術としても注目されている。

IPsecは，標準化の進行に合わせて多くの研究機関や企業で実装が進められ，1998年頃からはIPsecに対応したネットワーク製品もリリースされ始めている。

それに伴い，IPsecの特徴の一つである異なる実装間での相互接続性に関する検証作業も実施されるようになってきた。その結果，その相互接続性は必ずしも十分ではないということが明らかになり，プロトコルとして不十分な点についての議論と見直しが続けられているのが現在の状態である。

本稿では，このようなIPsecに関して行われている相互接続性検証の現状と，我々が開発したIPsecのプロトタイプ実装を実際に相互接続検証の場に持ち込み，その結果から整理した現時点での相互接続性に関する課題について報告する。

2. IPsecの標準化動向

まず，IPsec仕様の標準化の流れについて説明する。なお，IPsecの仕様はインターネットプロトコルの標準化団体であるIETFのipsecワーキンググループで検討され，その上位組織であるIESGの承認を経てRFCとして公開されている。

2.1 第1バージョン仕様

IPsecの最初の仕様がRFCとして公開されたのは1995年である[1]。この仕様は，IPsec仕様の最も基本的な部分として，IPパケットの暗号化・復号化方法とパケットの送信元認証・改ざんチェック用の認証データの付加方法を定義したものである。

暗号化や認証で使用する鍵情報は，IPsecによる通信を行うノードにあらかじめ手動で設定しておくことが前提となっている。これをマニュアル鍵設定と呼ぶ。

2.2 第2バージョン仕様

第1バージョン仕様がRFCとして公開された後，その仕様に対するさまざまな見直しや機能追加が検討された。それらの仕様はインターネットドラフトとして公開され，標準化団体のミーティングやメーリングリストにおける議論を経て1998年11月に第2バージョン仕様がRFCとして公開された[2]。第1バージョン仕様からの主な変更点は以下の通りである。

(a) リプレイ攻撃に対する対策
(b) 暗号・認証アルゴリズムの追加
(c) 自動鍵交換プロトコル (IKE) の追加

IKE (Internet Key Exchange) は，IPsecによる通信を行うノード間で，そこで使用する暗号鍵，認証鍵を自動生成して交換するプロトコルで，UDPを使用する。このプロトコルは，あらかじめ両ノードに設定しておいた共有鍵またはお互いの公開鍵を使用して相手ノードを認証するフェーズ (認証フェーズ) と，IPsecで使用する鍵を生成・交換するフェーズ (鍵生成フェーズ) からなる。鍵交換に関しては，Diffie-Hellman法をベースとして交換中の鍵を保護する仕組みを備えており，第三者がそれを盗聴することが困難になっている。また，IPsecによる通信をしている最中に，そこで使う鍵を定期的に更新する機能も持ち，前述のマニュアル鍵設定と比べて鍵管理が容易になるという利点を持っている。

現在，製品としてリリースされている実装のほとんどは，この第2バージョン仕様に準拠したものである。

なお，特にIKEを中心に現在でも仕様の見直し，検討は続けられており，改訂版仕様がインターネットドラフトを経てRFCとして今後公開されるものと思われる。

3. 相互接続性検証の状況

IPsec/IKE の相互接続性検証は，相互接続実験という形で各所で実施されるようになってきている。ここでは，まず相互接続実験の種類について分類を行った後，米国および日本国内における相互接続実験の実施状況について述べる。

3.1 相互接続実験の分類

現在行われている相互接続実験は，その目的の違いから次の2種類に分類することができる。

(1) 開発者主体の相互接続実験

前述のように，IPsec/IKE の仕様は RFC 化されたとは言っても，まだまだ開発途上にあるプロトコルである。

この実験は，IPsec プロトコルの仕様や実装上の問題点を抽出し，それについて議論することを目的としたものであり，主に IPsec/IKE 実装の開発者が中心となって実施されるものである。

この実験の場合，デバッグのために開発途中の実装も多く持ち寄られる傾向にあり，この時点でどの実装間で接続に成功したかという結果にはそれほど意味がない場合もある。

(2) ユーザ主体の相互接続実験

この実験は，すでに製品またはフリーソフトウェアといった形態でリリースされている実装を集め，それらの間での接続性の有無を調査することを目的とするものであり，主にネットワークを構築・運用するユーザが中心となって実施されるものでる。

その結果は，実装間での接続が成功したかどうかをマトリクスにしてまとめられることが多い。この情報は，ネットワークの構築・運用管理者にとっては有用なものである。

3.2 米国での実施状況

米国では，VPN 技術の関連団体の主催で 1997 年頃から IPsec 対応製品の相互接続実験を開始している。その内容は開発者が直接実装を持ち寄って実験を行うもので，前述の「開発者主体の相互接続実験」に属するものである。

この実験は，年に2回程度のペースで定期的に開催されている。最近では 1999 年5月にカリフォルニア州サンタバーバラで開催され，60 以上の組織から約 150 名の開発者が参加するという大規模なものであった。ここでは，各組織が接続相手を探して実験を進める中で発生した種々の問題点が収拾され，それについてのミーティングも実施される。さらに，この結果は定期的に開催されている標準化団体のミーティングの場にも報告され，さらなる議論を経てインターネットドラフト，RFC へ反映されていくというのが通例である。

また，相互接続実験とは異なるが，米国には IPsec 対応製品の認定作業を行っている企業もある。これは開発者がその企業に依頼して標準仕様への準拠の度合いなどを検証するもので，1999 年5月現在で 12 製品がこの認定を受けている。ユーザグループによっては，グループ内で使用する IPsec 対応製品をこの認定を受けたものに限定しているところも存在する。

3.3 日本国内での実施状況

日本国内でも，インターネット関連の研究団体による「開発者主体の相互接続実験」が実施されており，数実装程度が持ち寄られて開発者自身による実験が行われている。

さらに 1998 年頃からは，国内でも IPsec 対応製品が増えてきたことを受け，ネットワークの構築・運用管理者等を中心とするユーザグループによる「ユーザ主体の相互接続実験」も行われるようになってきている。

これらの実験は，米国で行われているものほど大規模ではない。

4. 相互接続性に関する現状の課題

上記のように国内外で IPsec/IKE の相互接続性を検証していく動きが活発になり，その結果，特に IKE には既存の仕様，実装にはいくつかの問題があり，異なる実装間での相互接続性は決して高いとは言えない状態にあることが明らかになって

いる。

IPsec の基本的な暗号，認証機能については，第2バージョン仕様が固まってからは特に大きな問題点は指摘されていない。そこで，以下ではIKE に関して現在発生している相互接続上の問題点について分析，整理した結果について述べる。

4.1 現象の分類

実際に IPsec プロトタイプ実装を持参して相互接続実験に参加し，そこで発生した相互接続上の各種の不具合をまず現象面から整理した。その結果，ほとんどの不具合は次の3種類に振り分けられることが分かった。

(1) 接続条件折衝の失敗による通信不可

IKE では，鍵の生成・交換に先立ち，まず接続条件の折衝を行い，これに失敗した場合はIKE プロトコルを中断することになっている。ここで折衝する項目は，適用する IPsec 機能(暗号，認証)，使用する暗号・認証アルゴリズム，鍵の寿命などである。

本来，両ノードの仕様サポート範囲，設定内容から考えて成功するはずの折衝が失敗してしまうという現象は，実際の相互接続実験の場では最も多く発生しているものである。

(2) 生成・交換した鍵の不一致

これは，接続条件の折衝には成功するが，その後に生成される鍵が両者で不一致となり，IPsec による通信が失敗するという現象である。しかし，この現象は実際の接続実験の場ではそれほど多く発生しない。

(3) 鍵更新時の一時的な通信不可状態

この現象は，最初の IKE による鍵交換には成功して IPsec による通信も正常に行えるが，鍵の寿命が尽きて IKE で新たな鍵の生成・交換を行うときに，一時的に IPsec による通信ができなくなってしまうというものである。通常，IKE では鍵の寿命が尽きる少し前から鍵更新を開始し，鍵の存在しない状態が発生しないようにすることが求められている。

IPsec 通信不可となる時間は鍵の寿命の設定値や IPsec を必要としているトラフィックの状態に依存する。これは数秒程度で済む場合もあれば，場合によっては数十分から数時間におよぶ可能性もある。

4.2 原因分析

前節に示した現象が発生した原因を，過去の相互接続実験でまとめられた問題点や，我々が開発した IPsec/IKE の実装を持って実際に相互接続実験へ参加した時の結果を基に検討した。

4.2.1 RFC の仕様記述不足

これは，前節の(1)，(2)の原因として最も多かったものである。1998 年 10 月に米国ニューヨーク州で開催された相互接続実験の時に報告された問題点・意見の一覧表を調べても，そこに挙げられている報告(36 項目)のうち，約 7 割が RFC の記述や定義が曖昧で，いく様にも解釈された結果発生した不具合の報告であった。

4.2.2 実装間での鍵管理ポリシの相違

これは，前節(3)の直接的原因の一つと考えているものである。ここで言う鍵管理ポリシとは，鍵の状態管理と IKE の実行に関するポリシのことであり，現状ではその詳細は実装依存となっている。

ここで，前節(3)に分類されるの現象の一例として，我々のプロトタイプ実装と他の実装との相互接続実験で実際に発生した現象の一つを示す。

IKE では，折衝によって決められた IPsec 鍵の寿命にしたがって IPsec 鍵の更新(鍵生成フェーズの再実行)を行うことになっている。また，IKE の最初に行われる認証フェーズは，相手ノードの認証と同時に鍵生成フェーズで使われるマスタ鍵も生成する。そのため，マスタ鍵の寿命にしたがって認証フェーズも再実行することになっている。このマスタ鍵の寿命は IPsec 鍵の寿命に比べて長く設定されるのが普通である。

このような各フェーズの再実行に関して，今回実験を行った二つの実装は，それぞれ次のような

異なる鍵管理ポリシに従っていた

[実装 A] (我々のプロトタイプ実装)
認証フェーズの再実行と鍵生成フェーズの再実行は，非同期にそれぞれの鍵の寿命に従って独立に起動する。

[実装 B]
認証フェーズの再実行を開始すると，同時にそれまで同じ相手ノードとの間に確立していた IPsec 鍵，マスタ鍵をすべて解放する。認証フェーズ再実行直後は鍵生成フェーズも続けて実行する。

これらの実装を相互に接続し，最初の鍵交換が完了したとする。その後，IPsec 鍵の寿命が尽きて鍵生成フェーズを再実行する場合は特に問題は起こらないが，実装 A から認証フェーズの再実行を開始した場合に問題が発生する。認証フェーズを開始すると実装 B 側で使用中の IPsec 鍵を解放してしまうため，次に実装 A が鍵生成フェーズの再実行するまで IPsec の通信が不可能となってしまう。この様子を次の図に示す。

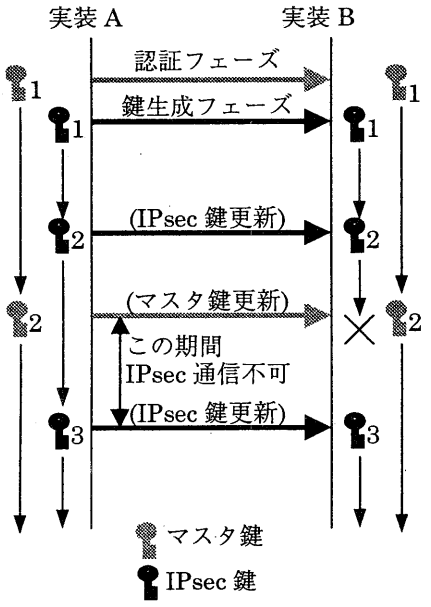

図 1　ポリシの異なる実装間での鍵交換例

この実験を行った二つの実装は，どちらも RFC で定義されている仕様を大きく逸脱しているわけではなく，そういう意味ではどちらも間違った実装ではない。ところが上記のような不具合を引き起こすような鍵管理ポリシの違いが発生してしまうところに問題がある。

このような鍵管理ポリシの違いが発生する原因を検討した結果，その一つとして，IKE プロトコルが現在持っている状態通知メカニズムをはじめとする IKE プロトコルの不完全さが影響していると考えた。この不完全さとは，具体的には次の 2 点である。

(a) 状態通知に関する応答確認手段の欠如
(b) サービス不能(DoS)攻撃に対する弱さ[3]

このような問題点がある中で，各実装者は少しでも安定的な通信を確保するため，独自に鍵管理ポリシを策定して実装している。そして，このポリシの違いが，特に鍵の更新や異常状態からの回復時における問題に繋がっていると考えている。

例えば，前述の実装 B の「認証フェーズ実行時に IPsec 鍵，，マスタ鍵を解放する」というポリシは，認証フェーズの開始を「相手ノードがリブート等によりリセットされた可能性がある」と考え，いち早く鍵の状態を復旧させるために自ノード側の鍵を解放し，新たな鍵交換を即開始できるよう準備するものである。このポリシは，同じ実装同士では有効に働くと考えるが，相手ノード側の鍵管理ポリシによっては問題を引き起こす可能性もあるというのが上の例である。

4.3　課題

以上から，IPsec/IKE の相互接続性を高めるための課題は以下の 2 点にまとめられる。

(a) RFC の仕様記述不足の改善
(b) IKE プロトコルの状態通知メカニズム等の改善とそれに伴う鍵管理ポリシの明確化

この中で，特に(b)の課題の解決が重要である。最近，相手ノードとの間で応答確認を伴う状態通知の手順に関する仕様なども提案されている[4]。しかし，サービス不能攻撃に対する対策といった

観点でのプロトコルの改善にはまだまだ研究の余地があり，重要な課題の一つである。

5. まとめと今後の課題

本稿では，IPsec 技術に関して，その相互接続性を検証するために国内外で行われている相互接続実験の状況と，実際にそこに参加して得た実験結果を分析，整理した結果を報告した。そして，相互接続性の課題として，特に IKE プロトコルについて状態通知メカニズムの改善とサービス不能攻撃への対策，および鍵管理ポリシの明確化が重要であることを述べた。

今後は，この課題に対する有効なプロトコル改善の研究と相互接続実験による検証を行っていく必要がある。

参考文献

[1] RFC 1825-1829, http://www.ietf.org/rfc.html
[2] RFC 2401-2412, http://www.ietf.org/rfc.html
[3] Kanta Matsuura, Hideki Imai : "Resolution of ISAKMP/Oakley Key-Agreement Protocol Resistant against Denial-of-Service Attack", Internet Workshop '99, 1999
[4] Dan Harkins, Dave Carrel : The Internet Key Exchange, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ike-01.txt, 1999