IPv6インターネットにおけるIPSec通信路の集約方式に関する検討

唐澤 圭† 原 知†† 藤崎 智宏† 三上 博英†

†NTT 情報流通プラットフォーム研究所
††NTT 東日本 研究開発センタ

現在、IPv6 (IP version 6) インターネットへの接続性提供サービスが数多く発表され、IPv6技術を活用した付加価値サービスが強く求められている。本稿では、IPv6技術の特徴の一つであるセキュリティ機能に注目し、IPSec (IP security) を用いたインターネットVPN (Virtual Private Network) を容易に構築するための技術を検討した。IPv6インターネットでは、必須のIPSec機能と豊富なグローバルアドレスを利用して、VPNに参加するホストを柔軟に指定できる特徴がある。しかし、エンドホスト毎に設定を行うと、認証に必要な事前の交渉とIPSecポリシ設定のコストが大きくなる。特に、VPNを電子商取引などに応用して、頻繁にVPNを切替える場合には、各ホストのIPSec設定コストの低減が重要な課題となる。我々は、IPSecトンネルを利用してIPSec通信路を集約するルータを用意することにより、各ホストの設定コストを低減する方式を提案する。最後に、本方式の実用性を評価するため、試験的VPN上でのラウンドトリップ時間の測定結果を報告する。

An Aggregation Method of IPSec Paths on the IPv6 Internet

Kei KARASAWA† Satoshi HARA†† Tomohiro FUJISAKI† Hirohide MIKAMI†

†NTT Information Sharing Platform Laboratories
††NTT-East R&D center

IPv6 (IP version 6) Internet has been available more easily. Many Internet service providers will provide IPv6 connectivity in 2000. It is eager to develop IPv6-specific applications and services. This paper focuses on IPv6 security function, IPSec (IP security). In the IPv6 Internet, it is easier to join an Internet VPN (Virtual Private Network), because each host can securely communicate to another host by using IPSec mandatory function. However, it will be arduous task to negotiate pre-shared information and set up IPSec policy information on each host. We propose an aggregation method of IPSec paths by using IPSec tunnel to reduce setup cost. The applicability of the method is evaluated by measuring round trip time on a VPN.

1 はじめに

インターネットは、ISDNやADSLよる常時接続、IP接続サービス等の出現により、家庭などの小規模なエンドサイトでも常に利用可能な情報通信のプラットフォームとなっている。このようなインターネット利用の拡大に対応するため、広大なアドレス空間をもつIPv6が提案されている [1]。IPv6インターネットでは、現在主流であるパソコン等の情報端末に加えて、携帯電話や家電、自動車、センサーなど、あらゆる電気電子機器を相互に接続し、情報を交換することが可能となる。

IPv6インターネットではネットワーク基盤を再構築する必要があるため、そのノードには、現行の機器には必ずしも含まれていない、1) アドレス自動設定、2) セキュリティ(IPSec)、3) マルチキャスト等の重要な機能の実装が新たに標準化されている。現在、IPv6対応のルータとホストは、これらの機能を持つ

実装が既に用意されている。今後は、インターネット利用者がIPv6技術の利点を享受できるよう、上記の機能を活用するサービスが求められている。

ここでは、上記3機能のうち、IPSec[2]技術に注目する。IPSecプロトコルは、現行のインターネットが持つセキュリティ上の欠陥を防御するために提案された[4]。IPSecを用いたインターネットVPN (Virtual Private Network)は、インターネット上の任意のユーザグループに対して、クローズド・ネットワークを提供でき、かつ、専用線を用いた場合などに比べて導入コストが低いという特徴がある。そのため、VPNを利用した電子商取引など、多様なサービスが提案されている[5]。

特にIPv6インターネットでは、個人の携帯端末だけでもインターネット全体へアクセスできるようになるため、逆に個人端末をグローバル・ネットワークからの攻撃から保護できるよう、IPSecを用いたインターネットVPNの活用が重要となる。

本稿では、IPv6端末が標準装備するIPSec機能を活用し、インターネットVPNの構築および変更を容易に行う方式を検討する。2章では、IPv6 IPSecを用いてVPNを構築する際の課題を整理する。3章では、IPv6 IPSec通信路の集約による解決法を提案する。4章では、IPv6 IPSec通信路の集約ネットワークの評価を行う。

2 IPv6 IPSecによるVPN構築の課題

IPv6インターネットでは、全端末が双方向に通信でき、かつ、IPSec機能を装備することが必須であるため、端末単位でVPNに参加するメンバを指定できるという特徴がある。この特徴を活用するためには、参加するVPNに合わせて、端末の設定を容易に切替えられる必要がある。

一般に、各IPSec通信ノードにおける処理手順は、図1のようになる。SPDには、IPSec通信開始を決定するために必要な、送信元/宛先IPアドレス/プレフィックス、IPSecモード、IPSecレベルなどの情報が保存される。SADには、IPSec通信を確立するために必要な送信元/宛先IPアドレス、暗号/認証アルゴリズム、鍵、IDなどの情報が保存される。拡張フィルタでは、IPパケットのヘッダを調べ、対応するSPDエントリに応じて、適用するIPSecのモードを決定する。次に、IPSecエンジンでは、再びIPパケットのヘッダを調べ、対応するSADエントリに応じて、IPパケットに暗号化や認証処理を施す。

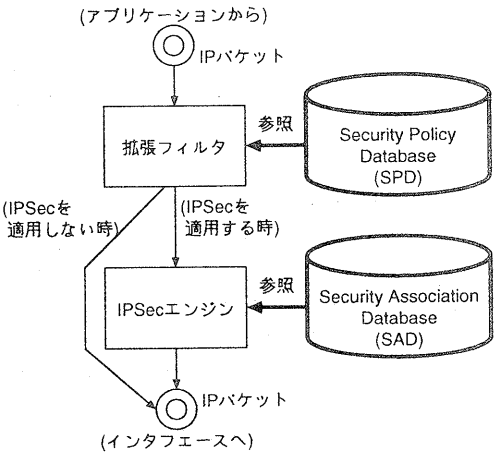

図1: IPSecの出力処理構造

エンドノードがIPSecを用いたVPNを切替えて利用するには、図1のSPDとSADの2つを適切に変更する必要がある。ただし、多数の参加者がいるVPNに参加するには、以下の課題がある。

- データベースの設定コストの増加
- データベースの検索コストの増加

以下では、各課題について議論する。

2.1 データベースの設定コスト

一般的に、VPNの形態は以下の2種類に分類される。

- コンセントレータ型
  1つのIPSec機器が中心となり、残りのIPSecクライアントからのIPSecパスを終端する集中構造をとる。一対多通信となり、主に、モバイル端末とセキュリティ・ゲートウェイの間で使用される。コンセントレータ側でアクセス可能なクライアントリストを管理する手法を採るので、クライアント側のIPSec設定はサーバへの通信路のみである。

- フルメッシュ型
  全てのIPSecノードがお互いにIPSecパスを終

端する自律分散構造をとる。多対多通信となり、主に、複数のセキュリティ・ゲートウェイの間で使用される。設定対象となるIPSecノードが分散しており、設定コストは大きくなる。

フルメッシュ型VPNの場合、接続ノードが増減する、または接続ノードの設定が変更される度に、残りの全ノードのSPDとSADの設定を更新する必要がある。n個のノードで構成されるVPNに1つのノードが追加される場合、各ノードで入力側と出力側の動作を定義する必要があるため、全体で$2n$個のセキュリティポリシ(SP)とセキュリティアソシエーション(SA)の追加が必要となる。また、新規にVPNに加入するノードにも、$2n$個のSPとSAを設定する必要がある。

また、SAは、暗号強度を高めるため、ある程度の周期で交換する必要がある。この作業については、SADを自動設定するための鍵交換プロトコル(IKE[3])が提案されている。IKEアプリケーションを用いれば、SADエントリの交換作業を自動化できるが、現在のIKE実装では、認証処理にIPアドレス、FQDN、電子メールアドレスなどを用いるため、SADの設定と同程度の初期設定が必要となる。また、SPDは、現在のところ、手動で設定する実装しか存在しない。

2.2 データベースの検索コスト

IPSecとユニキャストプロトコルを用いた場合、1つの端末が複数の相手と暗号化通信するには、全てのIPSec通信路に対する個別のSAが設定される。IPSecとマルチキャストプロトコルを利用すれば、SAの数を削減できるが、IKEによるSA交換手法やマルチキャストグループの構成方法などに課題が残されているため、本稿では対象としない。一方、SPは、ネットワーク単位でも設定可能であるため、必ずしも全てのIPSec通信路に対して、個別のSPを設定しなくてもよい。よって、以下では、SAについて検索コストを議論する。

全てのIPSec通信路に対する個別のSAを管理する場合、通信相手が増えると、SAを検索する負荷が大きくなる問題がある。実際に、大規模ネットワーク専用のセキュリティ・ゲートウェイなどは、1000以上のSAを管理できるが、SOHO用ダイヤルアップルータなどでは、カーネル上に保存可能なSAの数は数十程度である。

予備実験として、KAMEを用いた2台のIPv6端末を用いて、SA数を変化させた場合のRTT (Round-Trip Time)を測定した。図2は、SAの数を2個から8192個まで増やした際に、64バイトと8KバイトのICMP ECHO_REQUESTパケットを送受信した際のRTTを示している。また、比較のため、IPSecを行わない時のRTTも示されている。図2は、パケットサイズに関わらず、SAの数に比例して、RTTが線形に増加することを示している。

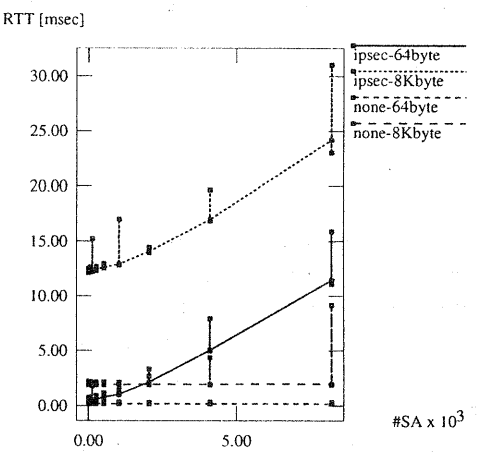

図 2: SAが増加した際のRTT測定結果

3 IPSec通信路の集約方式

フルメッシュ型のVPNにおいて、各IPSec通信ノードのSPDとSADのエントリを減らすには、前章で述べたコンセントレータ型のVPN構造を採ればよい。そのためには、まず、トンネルモードのIPSec通信を用いて、1つの端末の持つ複数のIPSec通信路をコンセントレータへ一旦集約し、次に、コンセントレータがIPSecパケットを宛先のIPSecトンネルへ転送することによって、エンド-エンド間のIPSec通信路を確立する方式が考えられる。本稿では、この転送機能を持つルータをIPSecリダイレクタと呼ぶ。

例えば、4サイト間でVPNを構築した際のネットワーク構成を図3に示す。図3左の構成では、サイト間にフルメッシュでIPSec通信路が張られており、各サイトが3つのIPSec通信路を制御している。一方、図3右の構成では、IPSecリダイレクタにより一旦通信路が集約されるため、サイト2,3,4は、1つのIPSec

通信路を制御すればよい。

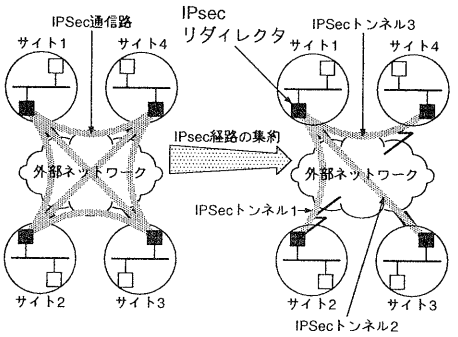

図 3: リダイレクタを介した 4サイト間の VPN 構成

このような構成を採る場合、IPSec リダイレクタのスループットが VPN 全体のボトルネックとなるが、DES や 3DES など普及した暗号化アルゴリズムに対しては、専用ハードウェアも製品化されており、全パケットを暗号化しても高いレスポンスを得られる環境が整ってきている。

本章では、まず、IPSec リダイレクタの設定方法について述べ、さらに、IPSec リダイレクタの導入による SPD と SAD の削減効果と、経路制御プロトコルへの影響を検証する。

3.1 IPSec リダイレクタの設定方法

フルメッシュ型の IPSec 通信路を集約して管理するには、あるノードから送信された IPSec パケットを、IPSec リダイレクタが適切に、宛先ノードへ転送する必要がある。この制御機能は、SP を適切に設定することにより実現できる。すなわち、IPSec 処理を行うパケットを決定するために利用される送信元と宛先の情報を、VPN に参加する全ノードの組合せについて用意し、各々に対して利用する IPSec トンネルを定義すれば良い。

例えば、図 3の例では、サイト 1のルータにおいて、(送信元サイト, 宛先サイト) $= (4,3),(4,2),\cdots,(1,2)$ に対応する IPSec 通信路を (入力側 $IPSec$ トンネル, 出力側 $IPSec$ トンネル) $= (3,2),(3,1),\cdots,(1,1)$ のように指定する。なお、その他のサイトは、全パケットをサイト 1へ送るようにすれば良い。

3.2 IPSec リダイレクタによる設定コスト削減量の算出

IPSec リダイレクタにより、各ノードの IPSec 通信路は削減できるが、全節で述べたように、IPSec リダイレクタの SPD 設定は増加する。本節では、VPN 全体での、設定コストを算出する。

IPSec 通信ノード数を n とした時、IPSec リダイレクタがある/ない場合の、IPSec 通信ノード (IN) と IPSec リダイレタ (IR) における SPD と SAD のエントリ数を表 1に示す。

表 1: SPD と SAD のエントリ数

	IPSec リダクレクタ	
	あり	なし
IN (SPD)	2	$2(n-1)$
IR (SPD)	$2n(n-1)$	—
小計	$2n^2$	$2n^2-2n$
IN (SAD)	2	$2(n-1)$
IR (SAD)	n	—
小計	$3n$	$2n(n-1)$
合計	$2n^2+3n$	$4n^2-4n$

IPSec リダイレクタを用いた場合、定量的な SPD 設定作業の総量は大きくなっている。しかし、定性的に見れば、作業が 1箇所に集中しているため、n 箇所に分散した場合より小さくなると考えられる。また、SPD と SAD の合計では、IPSec リダイレクタを入れた場合の方が、$2n^2-7n$ 小さくなる。すなわち、4つ以上のノードから構成される VPN では、本方式により、設定コストを軽減できることが分かる。

3.3 経路制御プロトコルへの影響

トンネルモードの IPSec 通信を利用したパケット転送を行う場合、実際のリンクと対応しない経路をパケットが通るため、経路制御プロトコルが隣接リンクを間違って保存し、誤動作する可能性がある。ここで対象とする IPv6 の内部経路制御プロトコルは、経路情報を受け取るために、リンクローカル・マルチキャストを受け取るインタフェースを使っている。したがって、IPSec トンネルがグローバルアドレスを指定する場合は、経路情報が IPSec トンネルを通ることはない。すなわち、本方式は、経路制御プロトコルへ影響しない範囲で利用可能である。

4 IPv6 VPN ネットワークの評価

前章で提案した IPSec リダイレクタを用いたネットワークを構築し、実用性を評価するため、RTT の測定実験を行った。実験に用いたルータは、暗号化処理性能を考慮し、ルータ専用機器ではなく、UNIX PC を用いた。具体的には、IPv6 スタックとして KAME を組み込んだ FreeBSD を OS とし、400,450,500MHz の x86 系プロセッサを持つ PC を用いた。各ルータは、リンクデバイスのボトルネックをなくすため、クロスの 100M イーサケーブルで直接接続した。今回は、鍵交換プロトコルよる通信遅延が影響しないように、SA のライフタイムを十分に長く設定した。

実験ネットワークの構成は、性能評価が簡単になるよう、2 台の IPSec ルータと 1 台の IPSec リダイレクタを使い、図 4のような構成とした。

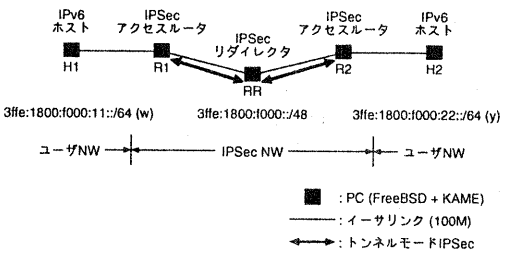

図 4: 実験ネットワーク

4.1 IPSec 通信路集約ネットワークの性能測定

IPSec リダイレクタを用いたネットワークと、図 4 の IPv6 アクセスルータ R1,R2 間で直接 IPSec 通信を行うネットワークを構築し、左端 IPv6 ホスト H1 から H2 へ ICMP ECHO_REQUEST (ping6) パケットを送受信し、RTT を測定した。その際、暗号化処理の負荷を変化させるため、パケットサイズを 64, 128, 256, 512, 1024, 2048, 4096, 8196 バイトに変更して測定した。ここでは、暗号アルゴリズムに DES を用い、認証処理は行っていない。結果を図 5に示す。

この結果、特に、パケット分割が生じない 1024 バイトまでのパケットは、143〜161%程度の増加であった。この性能は、インタラクティブなアプリケーションや短期のネットワーク利用には耐えられる範囲と考えられる。ただし、8196 バイトの場合は、RTT が 1020%増加する。また、この時 19%のパケットロスが生じていた。そのため、大容量のデータを送受信する際には、非常に応答が悪くなる可能性がある。

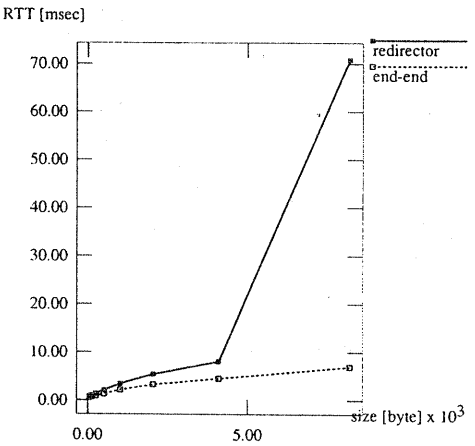

図 5: IPSec リダイレクタを利用した際の RTT

4.2 IPSec アルゴリズムに応じた性能測定

IPSec アルゴリズム毎の実用性を評価するため、IPSec リダイレクタを用いたネットワークにおいて、暗号と認証のアルゴリズムを変更して、前節と同様に、RTT を測定した。

まず、暗号アルゴリズムに、des-cbc, 3des-cbc, des-deriv, blowfish-cbc, cast128-cbc, rc5-cbc を用いた結果を図 6に示す。ここでは、比較のため、暗号処理を行わない simple アルゴリズムを用いて、IPSec 通信を行った際の RTT 測定結果も合わせて示してある。

この結果、パケット分割が生じない 1024 バイトまでのパケットは、全ての暗号アルゴリズムで安定的な応答が得られることが分かった。また、3des-cbc, blowfish-cbc など処理の重いアルゴリズムは、パケットサイズが大きくなると RTT が大きくなってしまうが、cast128-cbc は、安定性が高いことが分かった。

次に、暗号アルゴリズムを simple に設定し、認証アルゴリズムに hmac-md5 hmac-sha1 keyed-md5 keyed-sha1 を用いた結果を図 7に示す。

この結果、パケット分割が生じない 1024 バイトまでのパケットは、全ての認証アルゴリズムで安定的な応答が得られ、hmac-md5 と keyed-md5 では、安定性が高いことが分かった。

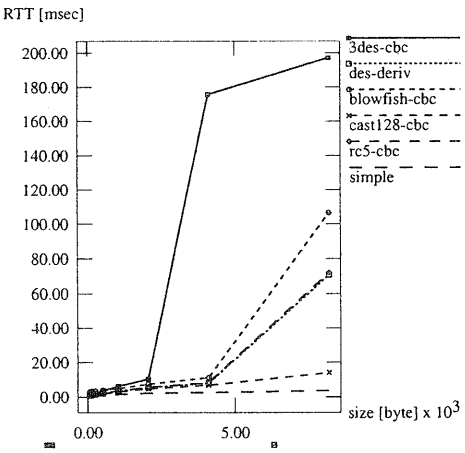

図 6: 暗号アリゴリズム毎の RTT

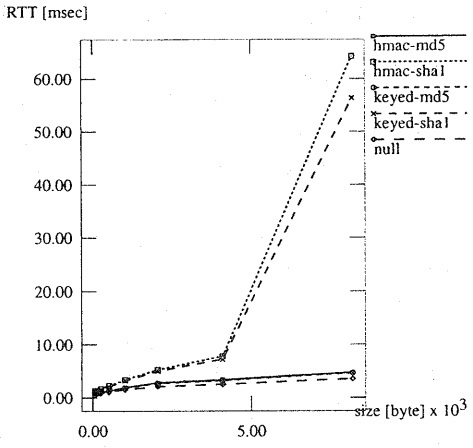

図 7: 認証アリゴリズム毎の RTT

また、全測定結果で共通に、急激に RTT 値が大きくなる現象については、パケット分割と暗号化処理の動作を詳細に検証し、ソースコードを検査した上で、実装を見直すなどの対応を取る必要がある。

5 結論

IPv6 インターネットは、いわゆるユビキタスネットワークとして、どこでも使える通信基盤となる可能性がある。その際、情報端末に保持される情報だけでなく、情報端末自体を守るために VPN を柔軟かつ用意に構築できることが望まれる。本稿では、ホストやネットワークが多数の VPN を頻繁に切替えながら接続する場合に、設定の変更コストを低減する IPSec 通信路の集約方式を提案した。そして、実績のある KAME の実装を用いて、提案方式の動作を検証し、小規模な試験的 VPN において、実用に耐えうる性能を得られることを確認した。また、パケット分割送信時の異常動作など、実装上の問題点を指摘した。

現在、IETF の IP secrity policy charter では、ポリシの設定プロトコルを検討中である [6]。ここでは、コンセントレータ型の VPN において、サーバ側から自動的にポリシを生成してクライアント側に設定する方式が提案されているが、フルメッシュ型の VPN におけるポリシの自動設定法は提案されていない。

謝辞

本研究にご援助頂いた、NTT サイバーソリューション研究所 茂木一男氏、また、本方式についてご議論頂いたインターネット総合研究所 許先明氏、小谷厚友氏に感謝の意を表します。

参考文献

[1] S. Deering and R. Hinden: "Internet Protocol, Version 6 (IPv6) Specification," RFC2460, p.39 (1998).

[2] S. Kent and R. Atkinson: "Security Architecture for the Internet Protocol," RFC2401, p.66 (1998).

[3] D. Harkins and D. Carrel: "The Internet Key Exchange (IKE)," RFC2409, p.41 (1998).

[4] E. Kaufman and A. Newman: "IPsec 導入の手引き," 翔泳社, p.247 (2000).

[5] 是友春樹: "VPN/VLAN 教科書," アスキー出版局, p.430 (1999).

[6] M. Blaze, A. Keromytis, M. Richardson and L. Sanchez: "IPsec Policy Architectur," draft-ietf-ipsp-arch-00 (2000).