ＩＰ通信拡散法を用いた広帯域高セキュリティＶＰＮ装置の研究開発（第２報）

～ＩＰ通信拡散法を用いたＶＰＮ装置の実用性評価～

森田俊英*　新井尚機*　木村隆則**[1]　加納益子**[1]
東精司**[1]　成山紘一**[2]　天野正明**[2]
横山雄一***　有泉徹也***　寺西貴***　桧垣博章***

Development of Broadband Secure VPN Equipment Based on Dynamic Multiple-Route IP Transmissions (2nd Report)

－ Performance Evaluation of Dynamic Multiple-Route IP Transmissions －

MORITA Toshihide*, ARAI Naoki*, KIMURA Takanori**[1],KANO Masuko**[1],
HIGASHI Seiji**[1], NARIYAMA Koichi**[2], AMANO Masaaki**[2],
YOKOYAMA Yuichi***, ARIIZUMI Tetsuya***,TERANISHI Takashi***, HIGAKI Hiroaki***

抄録

ＩＰ通信拡散手法では中継ルータに対してＩＣＭＰエコー処理のオーバーヘッドがかかる。ＩＰ通信拡散手法にＩＰＳｅｃによる暗号通信とアドレス変換を実装した試作品による通信が中継点ルータにおいて従来のＩＰデータグラムに与える影響を測定した。その結果、ＩＰデータグラムスループットへの影響はほとんどないことが明らかとなった。

キーワード：ＩＰ通信拡散法，セキュリティ，ＶＰＮ，スループット

１．はじめに

平成１４年度は IP 通信拡散手法 [1)]における中継点ルータへのオーバーヘッドを評価し、ルータへの負荷の面で実用的なレベルであることを明らかにした [2)]。今回は IP 通信拡散手法に IPSec による暗号通信とアドレス変換を実装した試作品を用いて、本装置による通信が WAN などで用いられる高性能なスイッチ（ルータ）において、従来の IP 通信へ与える影響を測定し、その実用性を評価した。

２．IP 拡散通信への VPN 機能の実装

IP 通信拡散法は図１の Cs から Cd への通信を行う場合において、データグラムが複数の中継ル

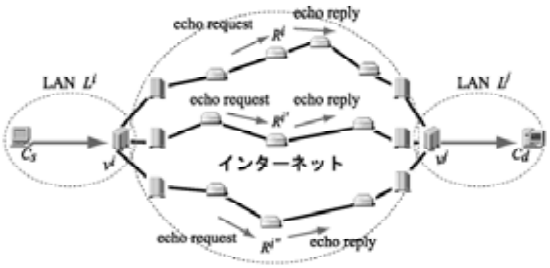

図１　ＩＰ通信拡散法を用いたＶＰＮ環境

*　電子情報技術部
**[1]　株式会社エルウィング
**[2]　不二エレクトロニクス株式会社
***　東京電機大学理工学部

ータ $R^i, R^{i'}, R^{i''}$を通るようランダムに拡散させて通信し、セキュリティを確保する方式である。この IP 通信拡散手法は暗号通信と対立するものではなく、暗号通信の欠点の１つを補完するものであるため、拡散通信と暗号通信を組み合わせて使用することとした。VPN 装置間の暗号通信を実現するものとして IPSec[3]がある。IPSec には、公開鍵暗号を用いたデータ配送のための秘密鍵の配送機能(IKE)と、この鍵を用いた秘密鍵通信(3DES)によるデータ配送機能とが含まれている。IPSec の Linux への実装としては FreeS/WAN プロジェクト [4]によるものがあるが、ここでは IPSec の機能はカーネルモジュールとして実現されている。

一方、拡散通信機能はアプリケーションプログラムとして実装されている。ここで、送信側の VPN 装置における処理を考えると、LAN に接続するインターフェイスから受信した IP データグラムの IP ヘッダを拡散通信プログラムが読み取る必要があることから、拡散通信プログラムによる処理の前に IPSec による処理を行うことは出来ない。また、拡散通信プログラムが作成した ICMP エコー要求の送信先は VPN 装置ではなく中継ルータであることから、拡散通信プログラムによる処理の後に IPSec による処理を行うこともできない。受信側の VPN 装置においても同様のことが成り立つことから暗号通信はカーネルの機能を流用するのではなく、拡散通信プログラムの一部として実現する必要がある。また、プライベートアドレスとグローバルアドレスの変換（NAT,IP マスカレード）は、Linux のカーネルモジュールとして実装されている iptables を使用した。

以上をまとめると、VPN に属する LAN 間の暗号通信はアプリケーションによって実現し、LAN とインターネットとの間の通信は、カーネルの機能によって実現する。したがって、LAN に接続するインターフェイスから受信した IP データグラムについては、その送信先がインターネット上のサーバコンピュータであるか VPN に含まれる他の LAN 上のコンピュータであるかによって、その処理をカーネルで行うかアプリケーションで行うかが異なる。同様に、インターネットに接続するインターフェイスから受信した IP データグラムについても、その送信元がインターネット上のサーバコンピュータであるか、VPN に含まれる他の LAN 上のコンピュータであるかによって、その処理をカーネルで行うかアプリケーションで行うかが異なる。

２．１　LAN から受信したパケットの処理

LAN から受信した IP データグラムは、Raw ソケットを通した受信によってコピーされる。この IP データグラムが VPN に含まれる LAN を送信先とする場合、アプリケーションプログラムによって ICMP エコーカプセル化とデータ部の暗号化が行われ、送信される。OS カーネルでは、iptables によって IP データグラムが破棄される。受信した IP データグラムがインターネット上のサーバを送信先とする場合、アプリケーションプログラムでは IP データグラムは破棄される。カーネルでは、iptables によって IP マスカレードの処理が施された IP データグラムが送信される。

２．２　インターネットから受信したパケットの処理

インターネットから受信した IP データグラムは、Raw ソケットを通した受信によってコピーされる。この IP データグラムが VPN に含まれる LAN を送信元とする場合、アプリケーションプログラムによって暗号化されたデータ部の復号化が行われ、送信される。OSカーネルでは、iptablesによってIPデータグラムが破棄される。受信したIPデータグラムがインターネット上のサーバを送信元とする場合、アプリケーションプログラムではIPデータグラムは破棄される。カーネルでは、iptablesのアドレス変換テーブルに従ってIPマスカレードの処理が施されたIPデータグラムが送信される。

以上のVPN機能を実装し、昨年度の結果を受け

てIP通信拡散法によるVPN装置を試作した。

３　評価

IP 通信拡散手法とそれを利用した VPN 装置では､経路の拡散に用いる中継点のルータにおいて、ICMP エコーの処理が必要となる。具体的には、受信した IP データグラムのデータ部に格納された ICMP エコー要求メッセージに対応する ICMP エコー応答メッセージが作成され、これをデータ部に格納した IP データグラムが送出される。

このとき、ICMP エコー要求メッセージのデータ部にカプセル化された IP データグラムが ICMP エコー応答メッセージのデータ部にコピーされることで、中継点を経由した IP データグラムの配送およびこれを利用した LAN 間の VPN 通信を実現している。

したがって、通常の IP データグラムを処理する場合と比較して、ICMP エコーの処理を必要とする分だけ、中継ルータの負担が増えることになる。 そこで図２のようなネットワーク構成にて、通常の IP データグラムと IP 通信拡散法でのデータグラムをそれぞれ単独で配送した場合のスループットの違いをフリーの測定ソフトである netperf を用いて測定した。

図２　中継ルータのスループット測定環境

表１　単独でのスループット測定結果

ルータ	IP 拡散	IP 通信
PC(Celeron 700MHz)	94.10	95.83
HP ProCurve5304 (PowerPC200MHz)	8.09	95.76
Cisco 7206VXR (MPE300 262MHz)	38.52	95.98
Cisco 2651MX (MPC860 80MHz)	12.66	57.95
Cisco 2621 (NPC860 50MHz)	9.10	67.24

表１の結果から ICMP エコーカプセル化されたパケットのスループットが IP データグラムのスループットよりも低くなっていることが分かる。しかし、その差異はルータの性能そのものとは直接的な関係がない。ICMP エコーの処理は前述したようなデータのコピーが伴う処理である一方、通常の IP データグラムの処理はこのようなコピーをできるだけ行わないようなチューニングが施されている。そのため、コピーを伴う ICMP エコーの処理に対してプロセッシング能力をどの程度割り当てるかは、ルータの実装法と設定によるものであると考えられる。

次に、HP　ProCurve5304を用いて、ICMP エコーカプセル化されたパケットの処理による他の IP データグラムのスループットの低下を測定した。図３に実験環境の概略を示す。ルータを中継点とした ICMP エコーカプセル化パケットのスループットを変化させた場合の IP パケットの最大スループットの変化を図４、図５に示す。

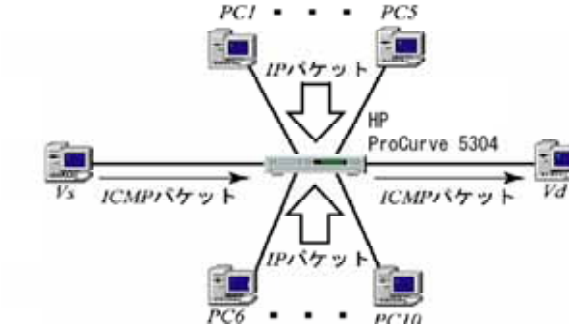

図３　IP通信スループットへの影響測定環境

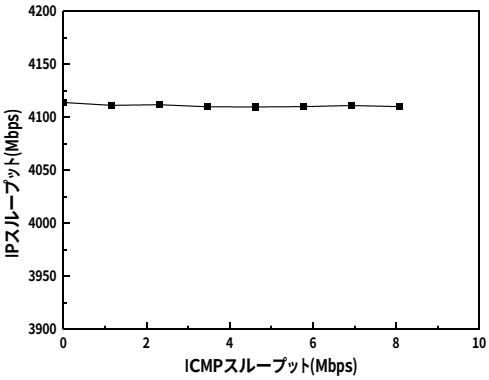

図４　IPデータグラムのスループット

この結果から、ICMPのスループットを変化させても、このルータを同時に通過するIPデータグラ

ムのスループットはほとんど変化しないことが分かる。これによって以下のような考察を行うことができる。

（１）現在のルータの設定、実装においては、ICMPエコーパケットに対するプロセッシング能力の割り当ては制限されたものになっており、この制限の範囲内ICMPエコーパケットの処理によって中継ルータの他のIPデータグラムに対する処理能力がほとんど低下することがない。

（２）表１のPCでの測定結果から、IPデータグラムの処理とICMPエコーカプセル化パケットの処理とに要するプロセッシング能力との間の差は大きなものではない。

４　まとめ

ＩＰ通信拡散法を実装したVPN装置の性能評価実験を行った結果、中継ルータには通常のIPデータグラムに比べて大きなオーバーヘッドを要するが、必ずしもCPUの能力によるものではなく、プロセッシング能力の割り当てによることが分かった。

また、IP通信拡散手法による通信が他のIPデータグラムの配送スループットには大きな影響を与えないことを明らかにした。

謝辞

本研究を進めるにあたり、様々な面から御指導くださった東京電機大学桧垣研究室の皆様へ深く感謝の意を表します。

参考文献

１）寺西貴、有泉徹也、横山雄一、桧垣博章、遠山宏明：暗号通信を用いたIP通信拡散手法，情報処理学会 分散システム／インターネット運用技術研究報告，No.031(2003)8

２）森田俊英、齊藤弘美、木村隆則、加納益子、東精司、成山紘一、駒形正則、齊藤孝紀、堀池唯人、桧垣博章：ＩＰ通信拡散法を用いた広帯域高セキュリティＶＰＮ装置の開発，埼玉県産業技術総合センター研究報告，第１巻，(2003)98

３）Kent,S. and Atkinson,R.: "Security Architecture for the Internet Protocol" RFC2401(1998)

４）http://www.freeswan.org.