4G-4 VPN(Virtual Private Network)構築技術の検討・暗号処理の高速化

永嶋 規充　　円城 雅之　　後沢 忍　　時庭 康久　　稲田 徹　　宮川 明子

三菱電機株式会社 情報技術総合研究所

1．はじめに

インターネットなどのオープンネットワークを利用して、従来の専用線よりも安価にイントラネットやエクストラネットを構築するケースが増えている。これらのネットワークに対して、専用線と同等の安全性を確保するための技術として、暗号による VPN(Virtual Private Network)があり、IPSEC がデファクトスタンダードとして定着している。

一方、社会のニーズからネットワーク上をマルチメディア情報のような高トラフィックな情報が流れるようになると、ネットワーク機器もそれに対応したより高速処理が可能な機器へと移り変わり、ネットワークは高速化の一途をたどることは必至である。また、VPN で用いる暗号に関しても、より高速で強固な新しい暗号アルゴリズムの登場が予想される。したがって、VPN 装置としてこれら 2 つの課題に対応可能なプラットフォームを形成しておくことが必要である。

2．暗号処理速度の分析

現状の分析のため、弊社にて開発した WAN ルータを IPSEC VPN 装置のサンプルとして、暗号処理の性能測定を実施した。暗号処理を行わない場合(none)と、暗号アルゴリズムとして IPSEC VPN 装置で一般的に用いられている DES,3DES を使用した場合について、測定を実施した。

測定結果を表 1-a に示す。表中の Frame size, Maximum Rate, FPS Passed Rate, Percentage はそれぞれイーサネットのパケット長，10Mbps ワイヤーレート理論値，1 秒間に中継したパケット数，10Mbps ワイヤーレート理論値に対する中継したパケット数の割合（FPS Passed Rate／Maximum Rate×100）を表わす。

表 1-a　測定結果（none, DES, 3DES）

	Frame size(Bytes)	64	128	256	512	1024	1280	1418
	Maximum Rate(Packets)	14881	8446	4529	2350	1197	962	869
none	FPS Passed Rate(Packets)	1953	1847	1782	1615	1152	931	841
	Percentage(%)	13.12	21.87	39.35	68.72	96.24	96.78	96.78
DES	FPS Passed Rate(Packets)	1116	791	508	307	164	132	118
	Percentage(%)	7.50	9.37	11.22	13.06	13.70	13.72	13.58
3DES	FPS Passed Rate(Packets)	744	422	254	146	66	54	48
	Percentage(%)	5.00	5.00	5.61	6.21	5.51	5.61	5.52

暗号処理を行わない場合の結果に着目すると、パケット長が大きくなるにつれて中継率がワイヤーレート理論値に近づいているのがわかる。これは、短パケットの場合は送受信処理に比べて IPSEC フレーム処理が極端に長いことが性能を劣化させる原因となっており、パケット長が十分大きくなれば送受信処理とフレーム処理とのパイプライン動作のバランスが良くなるため、ワイヤーレート理論値に近づくものと考察できる。

次に DES および 3DES で暗号処理を行った場合の結果に着目すると、パケット長が小さい場合の結果は

A Study of Fast Encryption in VPN Equipment

Norimitsu NAGASHIMA , Masayuki ENJO, Shinobu USHIROZAWA, Yasuhisa TOKINIWA, Toru INADA and Akiko MIYAGAWA

Information Technology R&D Center, Mitsubishi Electric Corporation

5-1-1 Ofuna, Kamakura, Kanagawa, 247 Japan

前述と同様の理由で性能劣化は当然であるが、パケット長が十分に大きくなった場合でも性能改善は見られない。これは、DES および 3DES はソフトウェアで実現されており、ソフトウェアによる暗号処理がボトルネックとなり、性能劣化を招いているものと考察できる。

以上の考察から、MISTY-LSI による暗号処理のハードウェア化を実現し、同様の性能測定を実施した。測定結果を表 1-b に示す。

表 1-b　測定結果（MISTY-LSI）

	Frame size(Bytes)	64	128	256	512	1024	1280	1418
	Maximum Rate(Packets)	14881	8446	4529	2350	1197	962	869
MISTY	FPS Passed Rate(Packets)	1674	1530	1471	1336	1144	931	841
	Percentage(%)	11.25	18.12	32.48	56.85	95.57	96.78	96.78

パケット長が小さい場合は前述と同様の理由で性能劣化は当然であるが、パケット長が十分に大きくなると、暗号処理を行わない場合と同等の性能となり、暗号処理によるボトルネックを回避できたことがわかる。

3．暗号処理部分離の提案

以上の比較検討から、図 1 に示すように、暗号処理部をフレーム処理部に依存しない独立した別ハードウェアに分離すれば、暗号処理のパイプライン効果が期待され、パケット中継率をワイヤーレート理論値へさらに近づけることが可能となり、さらに速い伝送路上では特にその効果が期待できると考察できる。また、この方式を採用することにより、暗号処理部をそれぞれの暗号アルゴリズムに対応したハードウェアに交換することで、任意の暗号アルゴリズムにも対応可能となる。

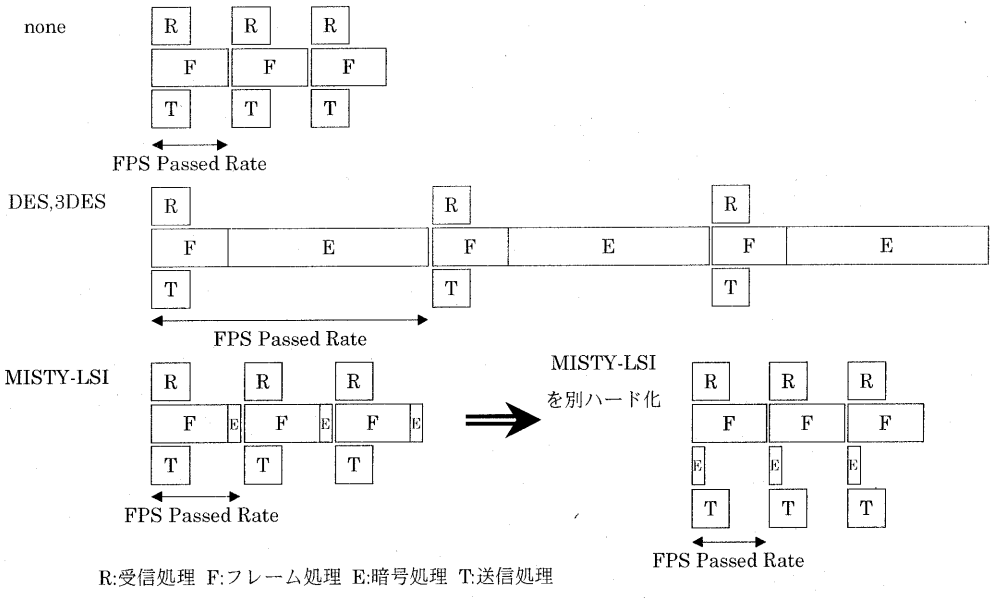

図 1　パイプライン処理

4．まとめと今後の課題

本稿では、IPSEC VPN の暗号アルゴリズムとして MISTY-LSI の性能測定を行い、その優位性を実証した。さらに、暗号処理部を別ハードウェアとして実現する方式を提案し、その方式ではパイプライン処理効果により IPSEC VPN 装置全体の性能改善が見込まれ、さらに任意の暗号アルゴリズムにも対応可能となることを述べた。今後、上記提案に基づくハードウェアを試作し、性能測定を実施する予定である。

参考文献

[1] 横山他“LAN 暗号装置の実現方式”，電子情報通信学会総合大会，1997