VPN(Virtual Private Network)構築技術の検討・暗号装置におけるハイブリット暗号化

3G－6　稲田 徹　後沢 忍　時庭 康久

三菱電機株式会社 情報技術総合研究所

1．はじめに

企業活動などにおいてネットワークの活用は必要不可欠であり、それに流れるデータの重要度が増してきている現在、インタネット上のデータ秘匿だけではなく、LAN 上を流れるデータの秘匿も非常に重要になってきている。現在、LAN の主流は 100Mbps のイーサネットであり、我々は 100Mbps 対応の IPSEC VPN 装置を開発した。本装置では、高速 IPSEC 処理を実現するために、H/W 暗号と S/W 暗号を使い分けるハイブリット暗号方式を採用している。本稿では、ハイブリット暗号方式の性能評価結果を報告する。

2．VPN 装置の構成

VPN 装置の構成を図1に示す。VPN 装置は、S/W 処理を主に行うメインボードと暗号 LSI を搭載した暗号ボードから構成される。

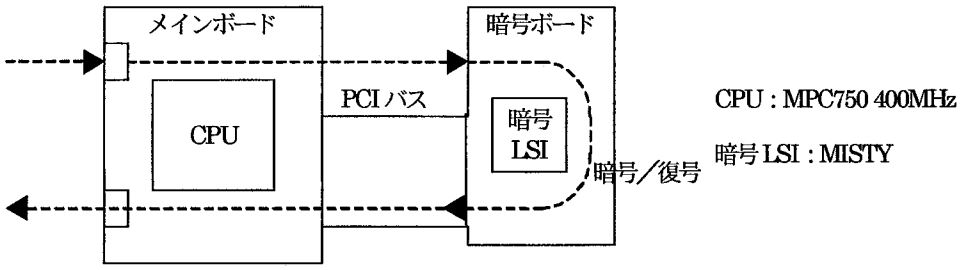

図1 VPN 装置の構成

メインボードは、CPU として MPC750 400MHz を持ち、受信パケットの精査処理、IPSEC 処理を主に実施する。暗号ボードは、暗号 LSI として、100Mbps 強の処理能力を持つ MISTY LSI を搭載している。メインボード－暗号ボード間の暗号データのやり取りは PCI バスを介した DMA 転送で実施される。メインボードでは、受信パケットの精査を実施し、暗号ボードに暗号データを転送した後は、次のパケットの精査処理、あるいは、前のパケットの IPSEC 処理を行うなど、パイプライン動作が期待できる構成となっている。

3．VPN 装置における H/W 暗号と S/W 暗号の特性

開発した VPN 装置で全てのパケットを H/W 暗号で処理した場合と S/W 暗号で処理した場合の評価データを図2、図3に示す。H/W 暗号の場合、暗号レングス(実際のパケットで暗号化される領域のレングス)が短い場合、DMA 転送およびその制御処理の起動回数が多くなるため、処理効率が悪くなる特性がある。S/W 暗号では、暗号レングスが短い場合、非常に高速処理できるが、パケット長に比例して処理時間が長くなる特性がある。

A Study on VPN(Virtual Private Network) Hybrid Encryption

Toru INADA, Shinobu USHIROZAWA, Yasuhisa TOKINIWA

Information Technology R&D Center, Mitsubishi Electric Corporation

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

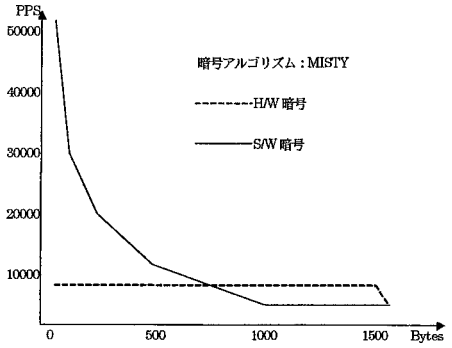

図２ スループット(PPS:Packet Per Second)

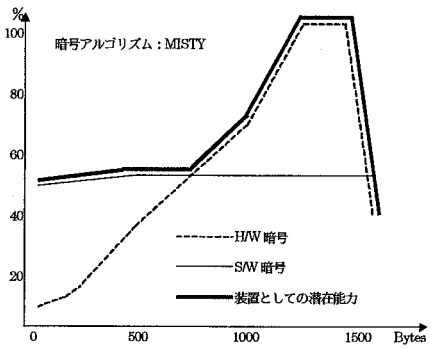

図３ スループット(論理限界に対する割合)

図中、1500 バイト以上のパケットにおいてスループットが低下するのは、IPSEC ヘッダの追加により IP フラグメント処理が発生するためである。

４．VPN 装置のハイブリット化および評価

上記の評価結果から、S/W 暗号、H/W 暗号それぞれに得意とする暗号レングスが存在することがわかった。このことから、暗号レングスによって S/W 暗号と H/W 暗号を使い分けるハイブリット化についての検討を行った。ハイブリット化した際の処理ブロック図を図４に示す。

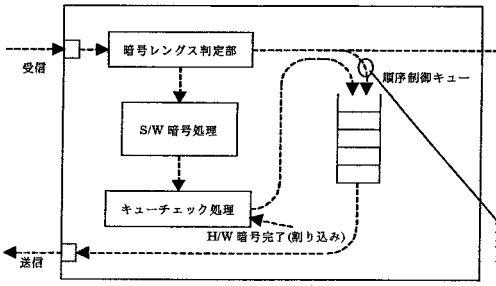

図４ S/W 構成図

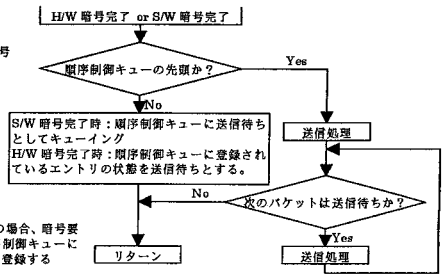

図５ キューチェック処理概略フロー

受信パケットは、暗号レングス判定部で S/W 暗号か H/W 暗号化振り分けする。このとき、パケットの受信順所の維持のために、順序制御キューを設け、S/W 暗号完了および H/W 暗号完了時にキューチェック処理によって、順序制御キューのチェックを実施する。キューチェック処理の概略フローを図５に示す。

本検討結果よりハイブリット VPN 装置を試作し、性能評価を実施した結果、図３太線と同等の特性が得られた。

５．まとめ

S/W 暗号と H/W 暗号を適宜使い分けるハイブリット VPN 装置の検討・性能評価を実施した。今回は、スループット向上をターゲットとしたが、今後、装置内部での遅延を削減する検討を行い、評価していきたい。

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

[2] 永嶋他“VPN 構築技術の検討・暗号処理の高速化”，情報処理学会第６１回全国大会，2000