マルチメディア通信と分散処理　101－12
コンピュータセキュリティ　12－12
（2001．2．21）

IPsec処理の高速化方式の検討

笠井真理子[†]　渡辺義則[†]　中野喜之[*]
(株) 日立製作所 システム開発研究所[†]
(株) 日立システムアンドサービス[*]

あらまし: インターネット上にVPNを構築するための標準的な暗号プロトコルとしてIPsecが注目されている。IPsec では複雑な暗号/認証処理を行うので、高速なネットワーク環境に VPN を構築するためには、IPsec 処理速度の向上が重要課題となる。そこで、本稿では、IPsec 処理性能を向上させるために、暗号処理ハードウェアを用いた IPsec 処理の高速化方式を提案する。そして、ハードウエア構成要素毎に要求される性能条件の定量的な評価を行い、100Mbps の通信環境で十分なスループットを得るために必要な各構成要素の性能条件を求めた結果を報告する。

A High-performance Method for IPsec Processing

Mariko Kasai[†] ,Yoshinori Watanabe[†] ,Yoshiyuki Nakano[*]
Systems Development Laboratory, Hitachi, Ltd.[†]
Hitachi Systems & Services, Ltd.[*]

abstract: IPsec technology is noticed as one of the standard secure communication protocols to construct VPN on the Internet. IPsec's cryptographic functions are highly computer-intensive and use complex mathematical instructions. So, when building VPN in the high speed network environment, it is very important to consider the performance of IPsec processing. We propose to use encryption hardware-based high speed IPsec processing method to get high performance. Then, we describe the performance required of each component which constitutes the proposed method in order to obtain enough throughput in 100Mbps network environment as a result of our quantitative analysis.

1. はじめに

近年、社内拠点間等のデータ通信にインターネットを利用して通信コストを低く押さえたいというニーズが高まっている。その際、インターネット上での通信における機密性や完全性の保証といったセキュリティの確保が重要課題となる。これを実現する方法の一つとして、VPN (Virtual Private Network) と呼ばれる方法が注目されている。VPN 構築に適用できる技術としては種々のものが提案されているが、その 1 つに IPsec(IP security)と呼ばれる技術がある。この IPsec の規定が、インターネット標準化組織 IETF (Internet Engineering Task Force)で進んだことにより、VPN 製品市場は急速な立ち上がりを見せている[1]。

今後は、VPN を使用するネットワークシステムの増加や通信回線速度の向上に伴い、VPN の通信速度の向上が要求されるようになることが予想される。そこで、本稿では、VPN 製品の IPsec 処理性能を向上させるために、専用ハードウェアを用いて IPsec 処理を高速化することを検討した。具体的には、IPsec 処理に必要なハードウエア構成の考案と、現在、企業内ネットワークで一般に使われている 100Mbps の回線に対して十分な性能が得られる各構成要素の性能の検討を行う。

なお、検討に際しては、コストとシステム構築の簡易性に配慮することにし、低コストで構成可能な PC アーキテクチャを用いて

VPN 製品を実現することを前提とする。

2. ソフトウェアによる IPsec 処理性能

IPsec 処理を全て CPU で行った場合、即ち、ソフトウェアで IPsec 処理を実施した場合の処理性能（スループット）を図 1 の測定環境で測定した。測定では、動作周波数 500MHz の CPU を搭載した 2 台の PC を用いて IPsec トンネルを構築し、これにルータ性能測定装置を接続する構成とした。表 1 が、パケットサイズ 1280Mbyte の場合の測定結果である。測定では、暗号/認証アルゴリズム処理の IPsec 処理性能に対する影響を評価するために、暗号化アルゴリズム無、認証値計算アルゴリズム無の設定でも測定を行った。通信回線として 10Mbps のイーサネットを使用した場合は、暗号アルゴリズムの種類によらず、回線速度である 10Mbps のほぼ限界までの伝送速度が得られている。しかしながら、100Mbps の通信回線を使用した場合は、暗号アルゴリズムによって性能の差が生じ、特に、3DES を使用した場合は約 13Mbps、3DES と SHA1 の両方を使用した場合は約 10Mbps と回線速度に対して非常に低い伝送速度となった。これは、3DES のような CPU 負荷の大きいアルゴリズムを使用すると、500MHz クラスの CPU を使用したシステムでは IPsec 処理がボトルネックとなり、結果的に 100Mbps のイーサネット帯域幅を使い切れていないことを示している。

一方、暗号化アルゴリズムも認証値アルゴリズムも無で設定した場合は、100Mbps の帯域上限までの伝送速度が得られている。これは、(a)IPsec ポリシチェック、(b) IPsec パケット処理、(c)暗号化/認証値計算処理からなる一連の IPsec 処理のうち、(c)暗号化/認証値計算処理を行わない設定である。(c)暗号化/認証値計算処理を行わない設定では十分な伝送速度が出ていることから、IPsec 処理全体の中で、特に(c)暗号化/認証値計算処理がボトルネックの大きな要因になっていると考えられる。DES よりも 3DES、3DES よりも 3DES と SHA1 の設定の方が伝送速度が低いのは、暗号化/認証値計算処理がより複雑になるためである。

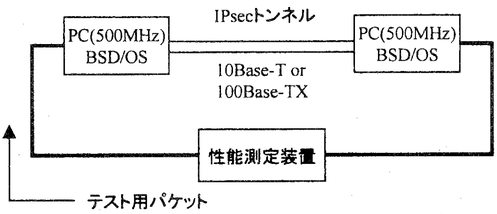

図 1 性能測定方法

表 1 性能測定結果（ソフトウェア処理）[Mbps]

アルゴリズムの設定		通信回線	
		10Base-T	100Base-TX
暗号化	認証値	(10Mbps)	(100Mbps)
3DES	SHA1	9.3	9.9
3DES	無	9.5	12.6
DES	SHA1	9.5	-
DES	無	9.5	29.3
無	無	9.5	93.1
IPsec を使用しない		9.8	95.9

表 1 の結果によれば、100Mbps イーサネットの帯域幅を十分に活用できるようにするためには、約 8 倍（3DES 使用時を想定）の高速化が必要である。CPU の動作周波数に比例して処理速度が向上すると仮定すると、約 4GHz(500MHz×8)の CPU が必要となるが、PC アーキテクチャにおいて現時点で一般的に入手可能な CPU の動作周波数は 1GHz 程度であり、CPU の動作周波数が向上するだけでは 100Mbps の通信回線に対しては依然として性能が不足することになる。

そこで、暗号化/認証値計算処理を専用ハードウェア（以下 IPsec ボードと記す）によって実施することにした。CPU による処理では CPU の汎用命令セットで処理プログラムを記述し実行させることになるので、プログラムステップも多くなり処理時間が長くなってしまう。暗号化/認証値計算処理を専用に実行するハードウェアを用いることで、

CPU 負荷が最も重く実行に時間がかかっていた暗号化/認証値計算処理を、より短時間で効率よく実行できるようになる。

3. IPsec ボード方式の検討

本章では、IPsec ボードを使用する場合の IPsec 処理方式を検討した結果について述べる。

図 2 は、IPsec 処理をソフトウェアで行った場合の処理モジュールの関係と IP パケットの流れを示したものである。

ネットワークインターフェースドライバ経由で届いた IP パケットは、IPsec ポリシ処理モジュールに送られる。IPsec ポリシ処理モジュールでは、IPsec 処理対象パケットを定義してあるテーブル[2]を参照しながら、入力パケットが IPsec 処理対象パケットであるかを判定し、IPsec 処理対象パケットでない場合はネットワークインターフェースドライバへ、パケットが IPsec 処理対象パケットである場合は、IPsec パケット処理モジュールへパケットを送る。IPsec パケット処理モジュールは、使用する暗号アルゴリズムや暗号鍵の情報が管理されているテーブル[2]を参照しながら、平文の IP パケットを暗号化して IPsec パケットにしたり、逆に IPsec パケットを復号化して平文の IP パケットに戻す処理を行う。IPsec 処理済パケットは、ネットワークインターフェースドライバに渡される。

以上が IPsec 処理をソフトウェアで実施した場合の一連の流れとなるが、IPsec ボード方式では、前章で述べたように IPsec 処理のボトルネックの大きな要因となっている図 2 の「暗号化/復号化」処理と「認証値計算」処理の双方の処理を専用ハードウェアで実行するようにした。また、CPU－IPsec ボード間のインターフェースオーバヘッドを最小化することに配慮し、CPU－IPsec ボード間のデータ転送を IP パケット形式で行うことにした。これに伴い、IPsec パケット処理も IPsec ボードで実行することにした。なお、ここで述べたオーバヘッドの要因としては、CPU－IPsec ボード間の同期処理、割り込みハンドラ処理、CPU が IPsec ボードへ送ったパケットに関する状態管理が挙げられる。

IPsec ボード方式における IPsec 処理の一連の流れを図 3 に示す。

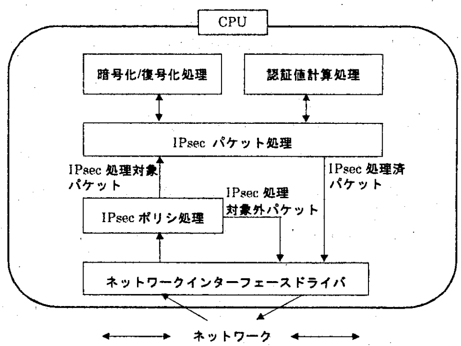

図 2 IPsec 処理関連モジュール図 (ソフトウェア処理方式)

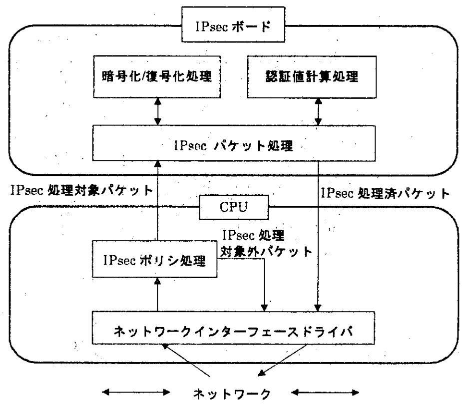

図 3 IPsec 処理関連モジュール図 (IPsec ボード方式)

4. IPsec ボードのハードウェア仕様検討

4.1. ハードウェア構成

前章で述べた IPsec ボード方式を実現するために、図 4 に示すハードウエア構成を考案した。IPsec ボードには、IPsec パケット処理を行うマイコンと、暗号化/復号化/認証

値計算処理を行う暗号モジュールを搭載する。

マイコンは IPsec パケット処理の他、IPsec ボード全体の制御と暗号モジュールのシーケンス制御も行う。

暗号モジュールは、暗号化/復号化/認証値計算処理を行うコプロセッサであり、数種類の暗号/認証アルゴリズム（DES、3DES、SHA-1 など）を扱うことができる。また、各暗号アルゴリズムごとに入出力バッファを設けることで、暗号処理時間とデータ転送時間をオーバラップさせ、暗号モジュールの利用効率を高めるように配慮する。

ワークメモリは、マイコンの作業領域として使用される。パケットデータの一時格納やマイコンのマイクロコード格納などが主な用途となる。

PCI/IF は、PC 本体－IPsec ボード間のデータ入出力を制御する。

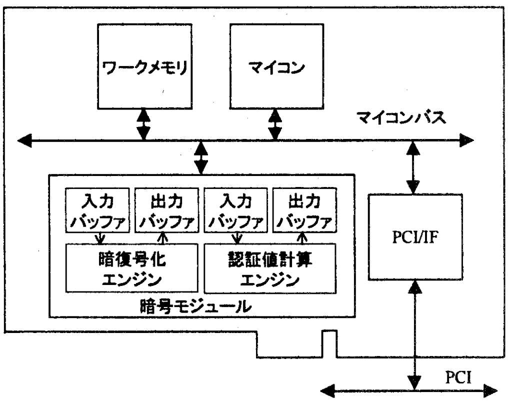

図 4　IPsec ボードのブロック図

4.2. データフロー

平文の IP パケットを暗号化して IPsec パケットにする場合 (暗号化/認証)の IPsec ボード内部のデータフローを、図 5 を用いて説明する。図 5 に示したデータの流れの矢印は、便宜上、各構成要素間に描かれているが、実際のデータはマイコンバスを経由して行き来する。

PC 本体から送られた IP パケットは、一時、PCI/IF の入力用バッファに置かれる。これをマイコンが読み出し、ワークメモリへ転送する①②。ワークメモリでは、マイコンが IPsec パケット処理を行う。暗号化の対象になるデータは、暗号モジュールへ転送され③④、暗号化される。暗号化されたデータは、マイコンにより再びワークメモリに転送される⑤⑥。その後、認証データ計算の対象となるデータが再び暗号モジュールへ転送され⑦⑧、認証データが計算される。計算終了後、認証データはワークメモリに転送される⑨⑩。マイコンは、ワークメモリでヘッダの組み立て処理を実施し、IPsec パケットの形式で PCI/IF の出力用バッファに転送する⑪⑫。最後にこの出力用バッファから PC 本体へ転送される。

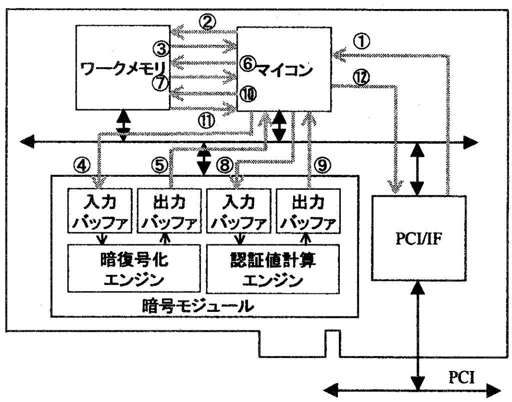

図 5　データフロー
(IP パケット→IPsec パケットの場合)

4.3. 各構成要素の性能検討

図 4 に示す構成の IPsec ボードで IPsec 処理を行う場合、暗号モジュールとワークメモリ間のデータ転送を繰り返し行う必要がある。このため、暗号モジュールとワークメモリ間のデータ転送時間と、暗号モジュールの暗号処理/認証値計算時間とのバランスが悪いとボード全体としての処理性能は向上しない。

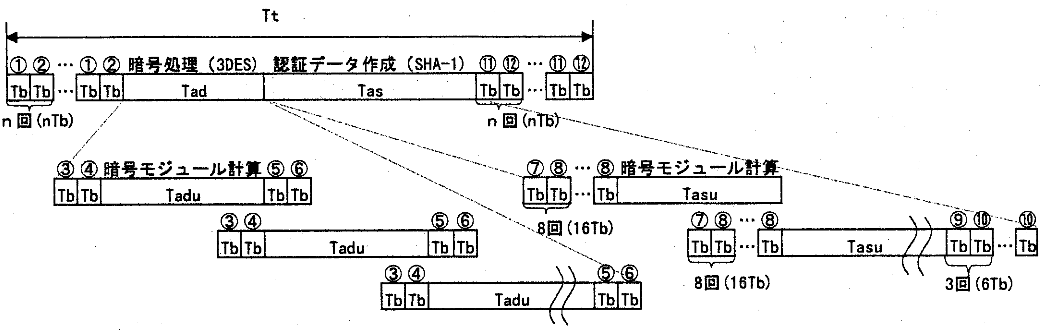

図 6　処理時間の内訳

本稿では、図５のデータフローをもとにして、IPsec ボードのバスに流れるデータの転送時間と暗号モジュールの処理時間とを、バスの利用効率に配慮しながら積み上げた。そして、IPsec ボードが IPsec 処理に所要する時間の合計を求める計算式を導いた。また、100Mbps のスループットを得るために必要な各構成要素の性能を算出した。

図６は、図５のデータフローモデルをもとに、暗号処理のアルゴリズムに 3DES、認証データ生成のアルゴリズムに SHA-1 を用いた場合のバスのデータ転送時間と暗号化モジュールでの処理時間とを時系列で表現したものである。3DES は、64bit のデータ単位で暗号化し 64bit のデータを出力するアルゴリズムである。SHA-1 は、512bit 単位で計算を繰り返して 160bit の認証値を出力するアルゴリズムである。

なお、本稿では、マイコンで実施する IPsec パケット処理の時間が暗号化/認証値計算時間と比較して十分に短いと考え、性能条件の検討ではこの時間を省略することにした。

ここで、

n：処理するデータのブロック数(64bit 単位)
Tb：1 ブロック(64bit)のデータ転送にかかる時間
Tad：暗号化処理時間
Tas：認証データ作成時間
Tadu：64bit のデータの計算(3DES)にかかる時間
Tasu：512bit のデータの計算(SHA-1)にかかる時間
Tt：全体の処理時間

である。

全体の処理時間(Tt)は、図６から

$$Tt = n*2Tb + Tad + Tas + n*2Tb \qquad (1)$$

で表せる。

また、暗号モジュール実行中に次のデータの書き込みと前のデータの読み出しを完了させるためには、

$$Tadu > 4Tb \quad Tasu > 16Tb \qquad (2)$$

を満足する必要がある。

式(2)を満たせば、暗号化処理時間(Tad)と認証データ作成時間(Tas)は、図６から以下の式(3)式(4)で表せる。

$$Tad = 4Tb + n*Tadu \qquad (3)$$

$$Tas = 22Tb + n/8*Tasu \qquad (4)$$

式(3) 式(4)を式(1)に代入して、

$$Tt = n(4Tb + Tadu + Tasu/8) + 26Tb \qquad (5)$$

式(5)が、IPsec 処理に所要する時間の合計を求める計算式となる。

さて、n ブロックのデータを 100Mbps 以上で処理するためには、

$$Tt < (64*n/100)\ [\mu s] \qquad (6)$$

n>>26 の場合、式(5)を式(6)に代入して整理すると、

$$4Tb + Tadu + Tasu/8 < 640\ [ns] \qquad (7)$$

ここで、バスのデータ幅＝64bit、バスの周波数＝133MHz、モジュール間データ転送所要クロック数を 4clk とすると、

$$Tb = 4/133 = 30\ [ns] \qquad (8)$$

また、64bit データ計算(3DES) と 512bit のデータ計算(SHA-1)の所要クロック数は、暗号モジュールの内部構成によって異なるが、実際の暗号モジュールの一構成例から、64bit のデータ計算(3DES) の所要クロック数を 36clk、512bit のデータ計算(SHA-1)の所要クロック数を 162clk と仮定すると、

$$Tadu : Tasu = 36 : 162 \qquad (9)$$

という関係が成立する。

式(7)に式(8)式(9)を代入して、

$$Tadu < 332.8\ [ns] \qquad (10)$$

暗号モジュールの内部動作周波数

$$= 1/(Tadu/36) = 108MHz \qquad (11)$$

となる。

以上の計算から、バス性能 133MHz/64bit、暗号モジュールの内部動作周波数 108MHz で IPsec ボードを構成すれば、100Mbps のスループットが期待できる。この仕様は、最新のマイコンを用いれば、満足できる範囲である。なお、ワークメモリと PCI/IF も、133MHz で動作可能なデバイスを選択する必要がある。

4.4. CPU－IPsec ボード間のデータ転送性能

本稿では、IPsec ボード内部の IP パケット処理性能を考察した。IPsec ボードを用いた場合のシステムトータル性能には、CPU－IPsec ボード間のデータ転送性能も関係する。CPU－IPsec ボード間のデータ転送性能は、IPsec ボードのインターフェースである PCI バスの転送速度に大きく依存する。PCI バスの仕様上の最高転送速度は、132MB/s（バースト転送）である[3]。実際のシステムでは、PCI バスは、NIC(Network Interface Card)などの他の PCI デバイスにも使われるため、IPsec ボードが使用できる帯域はこれよりさらに低くなるが、IPsec ボードが PCI バスマスタ機能を搭載し、バースト転送をサポートしていれば、100Mbps（約 12MB/s）は十分に満足できると考える。

5. まとめと今後の課題

本稿では、専用のハードウエアを用いた IPsec 処理の高速化方式を検討した結果を報告した。

10Mbps 以下の通信回線に対しては、CPU によるソフトウェア処理で十分である。しかしながら、100Mbps の通信回線に対しては、ソフトウェアによる処理では性能不足であり、IPsec ボードが必要となる。バス性能 133MHz/64bit、暗号モジュールの内部動作周波数 108MHz 程度の IPsec ボードを使用すれば、100Mbps のスループットが期待できる。この仕様は、最新のマイコンを用いれば、満足できる範囲である。

一方、さらに高速な通信回線に対しては、PC アーキテクチャでは、PCI バスの転送速度を考慮する必要が出てくる。IPsec 処理では、IPsec ボードへの送信データ、受信データ、NIC への送信データ、受信データと、少なくとも、4 種類のデータが流れる。これらが、PCI バスの帯域を全て使うと仮定しても、理論的には、132MB/s÷4＝33MB/s (254Mbps) が限界となる。このため、200Mbps 以上の高速な通信回線に対しては、64bit/66MHz での PCI バス接続など、NIC、CPU、IPsec ボード間のデータ転送の高速化を検討していく必要がある。

参考文献

[1] 渡辺義則,大浦哲生：IPsec の相互接続性に関する現状と課題,情報処理学会コンピュータセキュリティ研究報告 99-CSEC-6 pp31-36

[2] RFC2401, http//www.ietf.org/rfc.html

[3] Solari 他(株)インフォ・クリエイツ出版事業部訳：PCI ハードウェアとソフトウェア　アーキテクチャ&デザイン,(株)インフォ・クリエイツ出版事業部,1998.9