2009-IOT-4（2）
2009 / 3 / 5

マルチコア CPU による IPsec の実装検討

辻村 達徳† 竹内 清史†

†三菱電機（株）情報技術総合研究所 〒247-8501 神奈川県鎌倉市大船 5-1-1

E-mail: †Tsujimura.Tatsunori@da.MitsubishiElectric.co.jp, Takeuchi.Kiyofumi@bp.MitsubishiElectric.co.jp

あらまし 次世代のインターネットプロトコルである IPv6 で必須とされる IPsec (IP Security Protocol)を用いた暗号通信では、通信の高速化に伴い、暗号認証処理の負荷増大が問題となりつつある。そして、暗号認証処理で使用する暗号アルゴリズムとしてはブロック暗号が知られているが、伝送効率の高さからストリーム暗号が用いられる場合がある。一方で組み込み機器の分野では、シングルコア CPU の性能向上限界に伴い、複数コアを用いた分散処理により処理性能を向上させるマルチコア CPU の普及が進んでいる。本稿では、スループット 1Gbps を実現する IPv6／ストリーム暗号に対応した IPsec のマルチコア CPU への実装方式の紹介と、実機での評価結果を報告する。

キーワード IPsec，マルチコア，暗号通信，VPN

A Study on Implementation of IPsec for Multi-Core CPU

Tatsunori TSUJIMURA† Kiyofumi TAKEUCHI†

†Information Technology R&D Center, Mitsubishi Electric Corporation

5-1-1 Ohfuna, Kamakura-shi, Kanagawa, 247-8501 Japan

E-mail: †Tsujimura.Tatsunori@da.MitsubishiElectric.co.jp, Takeuchi.Kiyofumi@bp.MitsubishiElectric.co.jp

Abstract In this paper, we introduce an implementation of IPsec with IPv6/stream cipher that achieves throughput 1Gbps for Multi-Core CPU, and we reports on the evaluation. In the evaluation, it was implemented for the CPU that had 16 MIPS64 cores (500MHz), and it achieved throughput 1Gbps when the packets that the frame length was over 1024 bytes were processed.

Keyword IPsec, Multi-Core, Encrypt Communication, Virtual Private Network

1. はじめに

次世代のインターネットプロトコルである IPv6 で必須とされる IPsec (IP Security Protocol)を用いた暗号通信では、ギガビットイーサネットの普及による通信の高速化に伴い、暗号認証処理の負荷増大が問題となりつつある。暗号認証処理で使用する暗号アルゴリズムにはブロック暗号が知られているが、ブロックサイズを一致させるためのパディングが必要であるため、暗号化データが平文データより大きい。これに対してストリーム暗号を使用した場合は、パディングが不要であるため伝送効率が高いという利点がある。また他方では、発熱や消費電力の問題によりシングルコア CPU の性能向上は限界であるため、複数コアを用いた分散処理により処理性能を向上させるマルチコア CPU の普及が進んでいる。

本稿では、スループット 1Gbps を実現する IPv6／ストリーム暗号に対応した IPsec のマルチコア CPU への実装方式を紹介し、実機での評価を報告する。

以下、まず背景技術として IPsec の概要を説明し、次に実装方式とその実機評価について説明する。

2. IPsec の概要

本稿の背景技術となる IPsec による暗号中継処理を説明する。

まず、IPsec とはインターネットワーキングの標準団体 IETF(Internet Engineering Task Force)において、IP の上位層プロトコルのセキュリティを確保するために標準化されたプロトコルである。インターネット上に安全で仮想的な通信路を構築する技術である VPN(Virtual Private Network)において、データの暗号化によりセキュリティを確保したパケットの中継を実現するプロトコルとして使われている。

次に IPsec による暗号中継処理について下図を用いて説明する。尚、図中の縦軸はプロトコルスタックを表している。

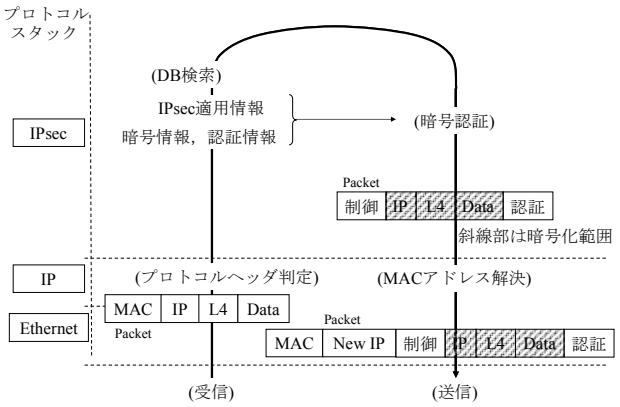

図 1　IPsec による暗号中継処理フロー

まず、平文パケットを受信すると、Ethernet と IP の各プロトコルにより、MAC アドレスと IP アドレスをチェックする(受信、プロトコルヘッダ判別)。MAC アドレスが他局宛の場合は中継処理を行い、自局宛の場合はパケットで指定されている上位層プロトコルの処理をする。また IP アドレスは次のデータベース検索で検索キーとして使用する。

次に、IPsec プロトコルにより、IP アドレスを検索キーとしてデータベースの検索が行われる(DB 検索)。検索するデータベースは、暗号中継と透過中継(暗号化をしないで中継)、廃棄のいずれでパケットを処理するかを指定する SP(Security Policy)が登録されている SPD(Security Policy Database)と、暗号認証処理で適用する暗号認証アルゴリズムや鍵の値を指定する SA(Security Association)が登録されている SAD(Security Association Database)の 2 つである。

次に、検索の結果得た SP と SA に従って暗号認証処理が行われる。暗号認証処理では、制御ヘッダ(シーケンス番号等)の付加と IP ヘッダから Data までの暗号化、認証ダイジェストの付加がパケットに対して行われる(暗号認証)。

そして最後に送信のため、MAC アドレスとトンネリングのための IP ヘッダ(図 1 では New IP と表している)がパケットに付加され送信される(MAC アドレス解決、送信)。

3. 実装方式の検討

本章では、スループット 1Gbps を実現する IPv6／ストリーム暗号に対応した IPsec のマルチコア CPU への実装方式を示す。

実装方式を決定するに当たり、暗号通信処理を分割し、分割して得た各処理を複数コアによるパイプラインまたは多重化(図 2)で行うことで高速化を実現することを志向した。

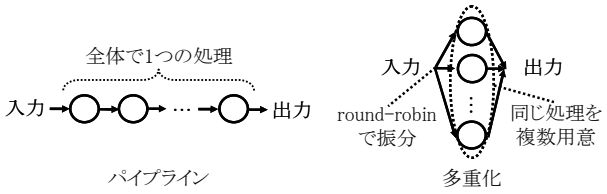

図 2 パイプラインと多重化処理

以下、まずマルチコア CPU のアーキテクチャ(コア間の接続形態、コア数)に依存しない汎用的な実装方式を説明する。そして、事例として、実装対象となる CPU を設定し、前述の実装方式を適用した場合の実装例を説明する。

3.1. 実装方式

まずマルチコア CPU への IPsec の汎用的な実装方式を説明する。

実装方式の決定に当たり、IPsec の処理の内容や機能に着目して処理を分割することと、分割して得た各処理がパイプラインと多重化のどちらに適しているかを決定することを考えた。以下、実装方式の導出手順と、それにより得られた実装方式を説明する。尚、IPsec でボトルネックとなる暗号認証処理を外部 H/W で処理する場合が考えられるので、以下の説明では H/W 送受信の処理を含んで説明している。

(手順 1-1)

処理全体を処理の内容や機能に着目して、受信、プロトコルヘッダ判定、DB 検索、H/W 送信、暗号認証、H/W 受信、MAC アドレス解決、送信の 8 つの処理に分割

(手順 1-2)

8 つの処理に対して、再帰処理を行う場合は多重化、共有リソースを使用する場合はパイプライン、とアーキテクチャを決定

(手順 1-3)

手順 1-2 で決定したアーキテクチャが同種の処理で順序が連続するものを 1 つにまとめ、それをコアの割り当てる対象に決定

以上より、マルチコア CPU への IPsec の汎用的な実装方式として、受信とプロトコルヘッダ判定、DB 検索、H/W 送信で 1 つのパイプライン、暗号認証は多重化、H/W 受信と MAC アドレス解決、送信で 1 つのパイプラインという実装方式を得た(表 1)。

表 1 マルチコア CPU への IPsec の
汎用的な実装方式

IPsec の処理部	実装アーキテクチャ
受信 プロコトルヘッダ判定 DB 検索 H/W 送信	パイプライン
暗号認証	多重化
H/W 受信 MAC アドレス解決 送信	パイプライン

3.2. 実装例

次に実装対象 CPU を設定し、前節で得られた実装方式で、実装アーキテクチャごとの 3 つの処理に対して割り当てるコア数の決定により得た実装例について説明する。

我々はこれまでにマルチコア CPU のみで IPsec の処理をする場合について、IPv4／ブロック暗号でロングパケットに対してスループット 1Gbps を実現する実装を確立している。そこで、これを基にして、暗号認証処理を外部 H/W で処理することにより IPv6／ストリーム暗号でロングパケットに対してスループット 1Gbps を実現する実装例を考えた。

本節では、実装対象 CPU の設定と IPv4／ブロック暗号の実装をまず説明し、その実装を基にした IPv6／ストリーム暗号の実装方式について説明する。

3.2.1. 実装対象となるマルチコア CPU の設定

まず実装対象 CPU として、十分な数のコアを有していることから、Cavium Network 社製 Octeon CN3860 (MIPS64 コア 500MHz×16 個)を選択した。そして 16 個のコアのうち 14 個を暗号処理及び復号処理でそれぞれ 7 個ずつ使用することとした(残りの 2 個は IPsec 以外のプロトコル処理、暗号認証処理で使用する鍵を交換する処理にそれぞれ割り当てた)。この条件は IPv4／ブロック暗号の実装も同様である。

3.2.2. IPv4/ブロック暗号の実装

次に IPv4／ブロック暗号の実装について説明する。

IPv4／ブロック暗号の実装はマルチコア CPU のみで IPsec の処理をする場合の実装例である。この場合、前節で説明した実装方式(表 1)と比較すると、H/W との送受信が無くなるので、受信とプロトコルヘッダ判定、DB 検索で 1 つのパイプライン、暗号認証は多重化、MAC アドレス解決と送信で 1 つのパイプラインという 3 つの処理の実装となる。

IPv4／ブロック暗号の実装を決定するに当たり、3 つの処理に対して割り当てるコア数を決定するため、以下の手順を実施した。

(手順 2-1)
処理速度の変動要因である入力パケット長ごとの処理時間を実機を用いて測定

(手順 2-2)
各処理単位の処理時間実測結果の比率を算出し、その比率に応じてパケット長ごとのコア割当数を決定

(手順 2-3)
手順 2-2 で決定したコア割当について、パケット長が最短から最長までの区間でスループットの積分をとり、その値が最大となるコア割当を最適なコア割当として決定

以上より、暗号化処理、復号処理ともコア割当は、受信＋プロトコルヘッダ判定＋DB 検索に 1 個、暗号認証に 4 個、MAC アドレス解決＋送信に 2 個と決定した(表 2)。

表 2　IPv4／ブロック暗号の実装

IPsec の処理部	実装アーキテクチャ	コア割当数	
		暗号	復号
受信 プロコトルヘッダ判定 DB 検索	パイプライン	1	1
暗号認証	多重化	4	4
MAC アドレス解決 送信	パイプライン	2	2

3.2.3. IPv6/ストリーム暗号の実装

最後に、前述した IPv4／ブロック暗号の実装を基にした IPv6／ストリーム暗号の実装方式について説明する。

IPv6／ストリーム暗号の実装を決定するには、表 1 に示した実装アーキテクチャごとの 3 つの処理に対してコアの割り当てを決定する必要がある。そこで、IPv6／ストリーム暗号の実装方式を得るため、暗号認証処理のうちの暗号処理と認証処理の割り振りを決め、ロングパケットに対して 1Gbps を実現する IPv4／ブロック暗号の実装の処理時間を基にして、目標性能 1Gbps を実現するコア割当を決定した。

まず暗号認証処理のうちの暗号処理と認証処理の割り振りとして、暗号処理は外部 H/W、認証処理はマルチコア CPU で処理することとした。

次に IPv4／ブロック暗号の実装の処理時間を基にして、目標性能 1Gbps を実現するコア割当を検討した。尚、外部 H/W での暗号処理のスループットはフレーム長によらず 1Gbps であることを仮定して検討した。検討に当たっては、まず IPv4／ブロック暗号においてフレーム長によらずに各処理で最長の処理時間を選び、

そこから1Gbpsを実現するために上限となる処理時間を決定した。そしてその処理時間以下となるようにしてコア割当を決定した。

まずIPv4／ブロック暗号の実装において、フレーム長によらず各3つの処理で最長の処理時間はそれぞれ以下の通りである。

・受信＋プロトコルヘッダ判定＋DB検索：6.64μs
・暗号認証：10.205μs／コア数
・MACアドレス解決(ARP)＋送信：5.58μs／コア数

以上より、1Gbpsを実現するIPv4／ブロック暗号の実装では、1コア当たりで最長の処理時間は暗号認証の10.205μsであり、この処理時間をIPv6／ストリーム暗号の実装で1Gbpsを実現するコア割当を決定する際の基準値とした。

次に1コア当たりの処理時間が基準値以下となるようにして、IPv6／ストリーム暗号の実装のコア割当を各処理で検討した。

① 受信＋プロトコルヘッダ判定＋DB検索

IPv4／ブロック暗号の実装を基にして考えた場合、IPv6／ストリーム暗号の実装と異なるのは、IPアドレスがIPv4の場合は32 bit、IPv6の場合が128 bitである点である。これが影響するのはIPアドレス値を検索キーとするDB検索である。そこで本処理の処理時間として、IPv4／ブロック暗号の実装の場合の処理時間に、IPv6に変わった場合のIPアドレス長の増分によるオーバーヘッドが加算された時間を考えた。そしてこの処理時間をIPv4／ブロック暗号の実装の場合の少なくとも2割増しと見積もったところ、処理時間は6.64×1.2 = 7.968μsであった。従って、1コア当たりの処理時間10.205μs以下を満たすため、コアを1個割り当てることとした。

② H/W送信、H/W受信

それぞれの処理は設計段階であったため処理時間を測定することができなかった。そこで処理内容から1Gbpsの性能を実現するために必要なコア数を予想し、それぞれの処理にコアを1個割り当て、暗号化処理、復号処理で共通に使用することとした。

③ 暗号認証

前述の通り、暗号処理は外部H/W、認証処理はマルチコアCPUで処理することとした。従って、1コア当たりの認証処理の処理時間を10.205μs以下とするコア割当を求めるため、認証処理の処理時間を測定した。入力パケットは、目標性能を実現する場合に想定しているロングパケットとした。測定の結果、フレーム長1280 byteのパケットに対して処理時間は35.3μsであった。従って、1コア当たりの処理時間を10.205μs以下とするために、暗号認証処理にはコアを4個割り当てることとした。

④ MACアドレス解決＋送信

IPv4／ブロック暗号の実装の場合に本処理をコア1個で処理した場合の処理時間の測定値は11.16μs（5.58μs／コア数×2コア）であり、1コア当たりの処理時間10.205μs以下を満たさない。しかし、IPv4／ブロック暗号の実装を解析したところ、MACアドレス解決処理ではOS提供の関数を使用しており、ルーティングテーブル検索と連動する余分な処理を行っていた。そこで、MACアドレス解決の処理時間を測定し、MACアドレス解決処理からルーティングテーブル検索と連動する余分な処理を省くことで、処理時間を約1μs短縮して1コア当たりの処理時間10.205μs以下とできるかを見積もった。

まずMACアドレス解決の処理時間を測定したところ、6.68μsであった。従って、本処理の処理時間11.16μsから6.68μsを引くことで送信の処理時間が4.48μsとわかる。次に、ルーティングテーブル検索と連動する処理の処理時間を測定したところ、検索処理のため処理時間に変動があるものの、1μs以上ではあることがわかった。従ってIPv6／ストリーム暗号の実装では、OS提供の関数から余分な処理を省くことで1コア当たりの処理時間を(6.68 - 1) + 4.48 = 10.16μsと見積もった。

以上より1コア当たりの処理時間を1Gbps実現の際の基準値10.205μs以下とできる見込みのため、本処理にはコアを1個割り当てることとした。

以上より、暗号化処理、復号処理で1Gbpsを実現できるコア割当として、受信＋プロトコルヘッダ判定＋DB検索に1個、暗号認証に4個、MACアドレス解決＋送信に1個と決定し、暗号化処理、復号処理で共通のH/W送信とH/W受信にはそれぞれ1個と決定した(表3)。

表3　IPv6／ストリーム暗号の実装

IPsecの処理部	実装アーキテクチャ	コア割当数	
		暗号	復号
受信 プロコトルヘッダ判定 DB検索	パイプライン	1	1
H/W送信	パイプライン	1	
暗号認証(認証のみ)	多重化	4	4
H/W受信	パイプライン	1	
MACアドレス解決 送信	パイプライン	1	1

4. 性能評価

前章で確立した実装方式に対して、スループット 1Gbps を達成することを確認するため実施した性能評価について説明する。

4.1. 評価環境

性能評価として、RFC1242/2544 に基づいたベンチマークテストによりスループットを測定するため、マルチコア CPU を搭載した CPU ボードと暗号処理を行う FPGA ボード(FPGA ボードにおける暗号処理の実装については文献[1]を参照のこと)、ネットワークの性能測定機器である SmartBits を使用し、図 3 のように評価環境を構成した。図 3 のような評価環境により、SmartBits から固定長パケットを一定時間送信し、暗号化及び復号側の CPU ボードと FPGA ボードを経由して戻ってきたパケットをカウントすることでスループットを測定できる。

また IPsec の設定として、IPsec プロトコルと暗号化アルゴリズム、認証アルゴリズムをそれぞれ ESP+認証あり、ストリーム暗号、HMAC-SHA256 と設定した。

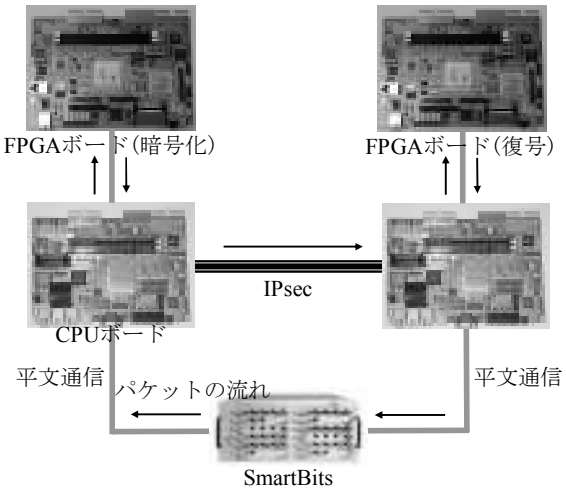

図 3　評価環境のシステム構成

4.2. 評価方法

スループット測定では SmartBits のアプリケーションソフト SmartFlow のスループット測定機能を使用した。これを使用すると、ある特定のフレーム長のパケットを一定時間送信した数と SmartBits で受信した数からスループットを測定することができる。測定の際に設定の必要がある主な項目としては、送信するパケットのフレーム長、送信時間、負荷をかける通信方向があり、表 4 のように決定した。

まず入力するパケットのフレーム長は、スループット測定に関することを規定している RFC1242/2544 に記載のフレーム長とした。但し、最大フレーム長については、IPv6 ではフラグメントの発生が許可されないので、フラグメントが発生しない場合の最大フレーム長 1452 byte とした。また最小フレーム長については、IPv6 の場合に SmartFlow で設定できる最小フレーム長 76 byte とした。また送信時間と通信方向は、それぞれ 10 秒、片方向とした。

表 4　スループット測定における設定

設定項目	設定内容
フレーム長 (byte)	76/128/256/512/1024/1280/1452
測定時間 (秒)	10
通信方向	片方向

4.3. 評価結果

各フレーム長に対するスループットの測定結果とそれをグラフ化したものを以下に示す。

表 5　スループット測定結果

	フレーム長 (byte)						
	76	128	256	512	1024	1280	1452
スループット (Mbps)	114.0	177.3	332.0	627.3	943.8	957.8	964.8

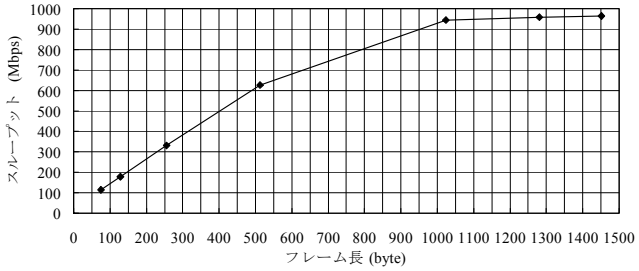

図 4　スループット測定結果

スループット 1Gbps を実現する実装として設計できたかを確認するため、測定結果を IPv6/IPsec を適用したパケットに対する GbE のワイヤスピードと図 5 を用いて比較した。比較の結果、フレーム長が 1024 byte 以上のパケットに対して今回の実装のスループット性能はワイヤスピードを達成したことがわかった。従って、設計した実装の性能目標達成を確認できた。

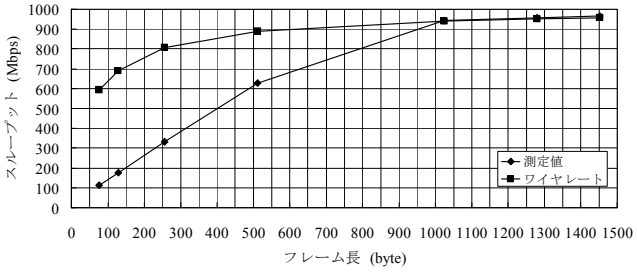

図 5 測定値と GbE ワイヤレートの比較

5. おわりに

本稿では、スループット 1Gbps を実現する IPv6／ストリーム暗号に対応した IPsec のマルチコア CPU への実装方式を紹介し、実機での評価を報告した。実機評価では、16 個の MIPS64 コア(500MHz)を有する CPU に対して実装をし、パケットのフレーム長が 1024 byte 以上の場合にスループット 1Gbps を達成した。

今後は、H/W 送受信の処理時間を測定し、それを基に各コアの処理時間を均一とした実装方式を検討して、更なる性能向上に取り組む予定である。

文　献

[1] 竹内清史，辻村達徳，“ストリーム暗号を用いたパケット中継装置の実装評価，”インターネットアーキテクチャ研究会，Mar.2009.

[2] 辻村達徳，時庭康久，“マルチコア CPU による IPsec プロトコルの実装検討，”2009 信学全大，Mar.2009.

[3] 時庭康久，辻村達徳，“マルチコア CPU を用いた IPsec 装置の実装方式の検討，”2009 信学全大，Mar.2009.

[4] 馬場達也，マスタリング IPsec 第 2 版，（株）オライリー・ジャパン，2006.