Security Network Processor による低消費電力 IPSec ESP の実装と評価

下國　治、河合　純、陣崎　明、山澤　昌夫†

中村　修、村井　純‡

†富士通　株式会社　IP ネットワーク事業本部　システムフロント事業部
〒211-8588　川崎市中原区上小田中 4-1-1
E-mail: {osamus,jkawai,zinzin,yamasawa}@flab.fujitsu.co.jp
‡慶應義塾大学　環境情報学部
〒252-0816　神奈川県藤沢市遠藤 5322
E-mail: {osamu,jun}@sfc.keio.ac.jp

Implementation and Evaluation of Low Power IPSec ESP by Security Network Processor

Osamu Shimokuni, Jun Kawai, Akira Jinzaki, Masao Yamasawa †
Osamu Nakamura, Jun Murai ‡

† System Front Division,　Network Systems Group,　Fujitsu Limited
211-8588 Kamikodanaka 4-1-1, Nakahara-ku, Kawasaki, Kanagawa, Japan
E-mail: {osamus,jkawai,zinzin,yamasawa}@flab.fujitsu.co.jp
‡ Faculty of Environmental Information, Keio University
252-0816 Endou 5322, Fujisawa, Kanagawa, Japan
E-mail: {osamu,jun}@sfc.keio.ac.jp

本論文ではインターネットのネットワーク層においてセキュリティを実現する IPSec（IP Security）技術、特に ESP（Encapsulating Security Payload）の高速処理、低消費電力処理を課題とし、これを解決する手段として我々が開発した Security Network Processor である Comet NP を使用して IPv4 ならびに IPv6 の ESP を実装した Comet ESP を評価した結果をまとめる。次にこの結果をふまえて ESP 処理の低消費電力化を実現する Trusted Network Processor（TNP）の検討結果を述べる。TNP は 1Gbps の IPSec ESP 処理を 2W 以下の電力で処理可能と予測でき、クロック当たりの IPSec ESP 処理性能で比較してソフトウェア処理の約 130 倍、暗号回路を内蔵した一般的な Security Network Processor の約 30 倍の能力をもつと考えられる 。

1. はじめに

インターネットでセキュリティ通信を利用する局面が多くなってきた。すでに TLS/SSL を用いた web サービスは我々の生活になくてはならない仕組みとなっているし、VPN を用いて自宅や出先から組織内ネットワークに接続し、メール処理、資料作成、会議、ソフトウェア開発などの作業を組織内にいるのと同じように行える環境が整いつつある。今後は個人が仕事場、自宅、趣味、仲間など複数の「情報空間」を持ち、物理的に存在する場所がどこであってもインターネットに接続すれば必要な情報空間を安全に利用できる、文字どおりの「時空遍在する安全な情報システム＝ユビキタスシステム」が現実のものとなっていくだろう。

ユビキタスシステムの実現には様々な技術が必要であるが、中でも重要な基盤技術としてワイヤレスネットワーク技術とセキュリティ技術がある。ワイヤレスネットワーク技術は煩雑なケーブルから我々を解放し、真の「ユビキタス」を実現する。セキュリティ技術は使用者の情報を保護するネットワーク通信の安全性を実現する。実際問題としてセキュリティ技術は物理的な階層から使用者の意識にまでかかわる大きな問題であるが、インターネット基盤技術としてまず検討しなければならないのは通信路のセキュリティであろう。特にワイヤレス通信は常に傍受の危険を伴うため、通信の安全性を確保するのが必須であり、ネットワーク層でのセキュリティが望まれる。

本論文ではインターネットのネットワーク層においてセキュリティを実現する IPSec（IP Security）技術、特に ESP（Encapsulating Security Payload）の高速処理、低消費電力処理を課題とし、これを解決する手段として我々が開発した Security Network Processor である Comet NP を使用して IPv4 ならびに IPv6 の ESP を実装した Comet ESP を評価した結果をまとめる。次にこの結果をふまえて ESP 処理の低消費電力化を実現する Trusted Network Processor（TNP）の検討結果を述べる。TNP は 1Gbps の IPSec ESP 処理を 2W 以下の電力で処理可能と予測でき、クロック当たりの IPSec ESP 処理性能で比較してソフトウェア処理の約 130 倍、暗号回路を内蔵した一般的な Security Network Processor の約 30 倍の能力をもつと考えられる[1]。

2. IPSec ESP 処理の課題

2.1. IPSec とその課題

IPSec は大きく分けて認証と暗号化からなるネットワーク層のセキュリティ技術である。認証は送信側でパケットデータのハッシュ値をパケットに付加して送信し、受信側で検査することでパケットの改竄や偽造を検出可能とする。但しパケットは平文のまま転送されるため情報秘匿はできない。これに対して暗号化はパケットデータを暗号化して送信することによりパケットを傍受されても内容を解読できないようにする。IPSec では AH（Authentication Header）で認証を、ESP（Encapsulating Security Payload）で暗号化と認証を定義している。

IPSec の課題は種々あるが、基本的なのは認証に用いるハッシュ関数、暗号化、復号化に用いる暗号関数の計算量が大きいことである。例えば現在最も一般的に利用されている 3DES（Triple DES: Data Encryption Standard）のソフトウェア処理性能は最適化しても Pentium III 550MHz で 36.4Mbps の性能である（富士通研究所内部での実験性能）。

次に IPSec においては単に暗号計算性能だけでなく、パケット処理を含めた処理性能が重要である。 IPSec では純粋な計算処理だけでなくヘッダの解析や作成などプロトコル処理、ネットワーク送受信処理、Operating System のオーバヘッドがあり、性能は一層低下する。Pentium III 500MHz での ESP 3DES 性能は IPv4、IPv6 とも 10Mbps 程度と報告されている[1]。

このように IPSec の性能は決して高くないが、その一方でインターネットの性能は高速化が著しい。 ADSL 接続で 10Mbps、ワイヤレス LAN で 50Mbps、FTTH 接続で 100Mbps、サーバネットワークは 10Gbps になっている。このような速度に見合う IPSec 性能を実

[1] 本研究の一部は新エネルギー・産業技術総合開発機構（NEDO）基盤技術研究促進事業委託研究 02004216-0「トラステッドネットワークプロセッサ基盤技術の研究開発」によって行った。

現することが大きな課題となる。また、ユビキタスシステムの実現においては性能を実現するための消費電力がさらに大きな課題となる。電池駆動可能な携帯機器で 50Mbps のワイヤレス LAN を十分に使いこなすことができなければ真のユビキタスシステムは実現できないといえよう。

2.2. IPSec 高速化

IPSec を高速化するためにまず行われるのは暗号演算の高速化である。既存の暗号方式についてはプログラムチューニングでは劇的な改善はみこめないが、新しい暗号アルゴリズム開発ではソフトウェアでの実装を考慮することが一般的になっている。例えばこれから IPSec 暗号の主流になるとみられる AES（Advanced Encryption Standard）は Pentium III 550MHz を用いた実測性能で 258Mbps と 3DES の 7 倍以上の性能が可能である [2]。このような努力があるものの、ソフトウェアでの高速化は原理的に限界があるだけでなく、アプリケーションプログラムを含めたシステム性能を低下させるので、最近はハードウェアによる高速化が盛んに行われている。

ハードウェア面では暗号演算回路を用いるのが一般的で、3DES で 1Gbps 以上の処理性能を実現可能な暗号チップが開発されており、VPN ゲートウェイ装置やサーバ向けセキュリティ NIC（Network Interface Card）に用いられる。

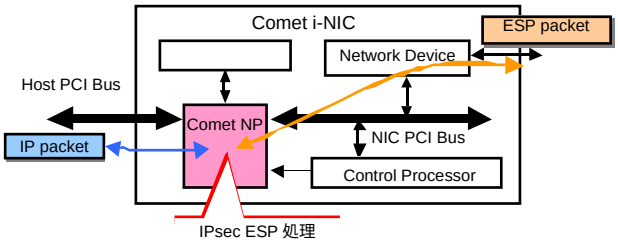
先に述べたように IPSec 処理では暗号計算だけでなくパケット処理も高速化する必要があるため、Network Processor に暗号演算回路を組み込んだ「Security Network Processor（以下 SNP と略す）」が開発されるようになってきた。例えばルネサスの SH7710 は 200MHz で動作する SH3-DSP プロセッサと「IPSec アクセラレータ」を内蔵した SNP で、IPv4 の IPSec ESP 3DES を 34.2Mbps と Pentium III 550MHz クラスの性能を実現している[3]。SNP は低消費電力な IPsec を実現するキーコンポネントとして期待される。

3. Comet ESP

3.1. 仕様

Comet ESP[4, 5]は Comet i-NIC（Intelligent NIC）を用いて IPv4 および IPv6 の IPSec ESP Tunnel モード[6] Gateway 機能を実現する。ESP 方式は DES/3DES CBC Explicit IV[7]である。

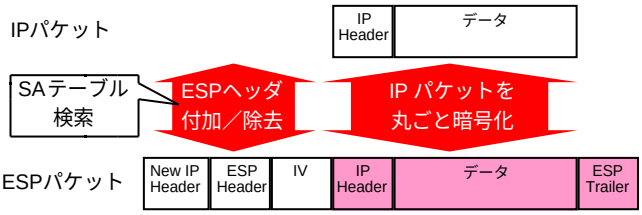
Comet ESP のパケットフローを図－１に示す。



図－１ Comet ESP のパケットの流れ

Comet i-NIC は PCI アダプタカードでホスト計算機からは単なる Ethernet NIC にみえる。ホスト計算機が IP 層までソフトウェアで処理し、Comet ESP に IP パケットを送信すると、Comet ESP がこの IP パケットを解析の上 ESP パケットに変換してネットワークに送信する。ネットワークから受信したパケットは Comet ESP か解析の上、必要ならば ESP から IP への変換を行いホスト計算機に転送する。Comet ESP を用いると、ホスト計算機は IPSec を全く意識せずに、ネットワーク上は ESP 通信を実現可能である。また、ホスト計算機に複数の Comet ESP を搭載することで、システム全体の ESP 性能を容易に向上させることができる。

図－２にパケット変換の概要を示す。IP から ESP への変換は平文の IP パケットをあらかじめ設定された SA（Security Association）テーブルに従って先頭の ESP ヘッダと末尾の ESP トレイラを付加し、暗号化を行う。逆変換は IP ヘッダ、ESP ヘッダを除去し、復号化し、ESP トレイラを除去する。



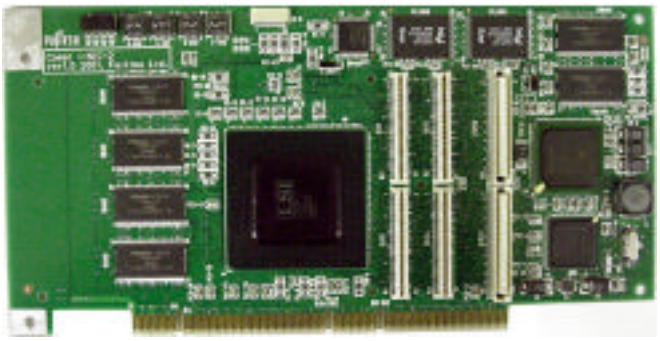
図－２ Comet ESP のパケット変換

鍵交換はホスト計算機が行い、SA テーブルを設定する。Comet ESP は与えられた SA テーブルを参照して

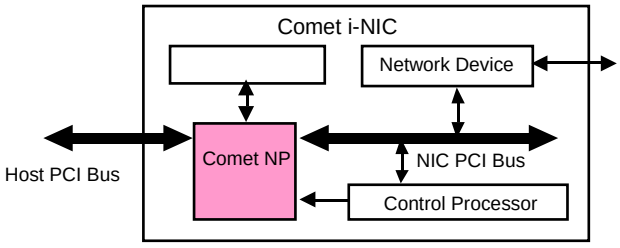
処理を行う。SA テーブルにマッチしないアドレスをもつパケットは ESP 処理せずそのまま転送する。エラーパケットは Comet ESP 内部で破棄する。

3.2. Comet i-NIC

図－３に Comet i-NIC の外形を、図－４に構成を示す。Comet i-NIC は PCI（Peripheral Component Interconnect）規格準拠のボードで Comet NP を搭載している[8]。PCI Bus は Host PCI Bus、NIC PCI Bus 共に 64/32bit、66/33MHz で、NIC PCI Bus に PMC（PCI Mezzanine Card）規格[9]の NIC をドータボードとして搭載できる。I_2O（Intelligent I/O）アーキテクチャを採用しており、アダプタ内部の制御は専用プロセッサ（Intel SA1110、200MHz）が行う。



図－３　Comet i-NIC



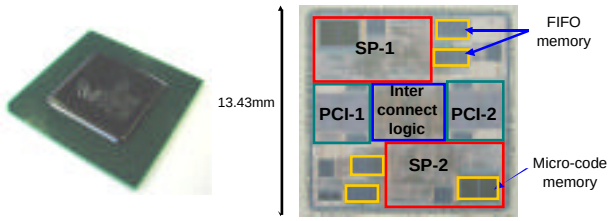
図－４　Comet i-NIC の構成

PMC 準拠の NIC を利用することにより、多種のネットワークに容易に対応可能である。Comet ESP の評価では 1000Base-T を用いた。1000Base-T デバイスの制御は SA1110 が行う。

3.3. Comet NP

Comet NP（Network Processor）はサーバ用に開発した SNP である（図－５）[10]。CMOS 0.35μm プロセス、90 万ゲート規模でパケット処理専用のプロセッサである「Stream Processor（SP）[11]」を 2 プロセッサ、PCI 64/32bit、66/33MHz を 2 チャネル持つ。

SP は DES/3DES、IP Checksum などパケット処理用の演算回路とテーブル検索機能を持つ SNP である。SP 一個あたりの回路規模は論理回路 100KGate、SP 用プログラムメモリ 70KGate と合わせて 200KGate 以下と小さい。Comet NP では送受信を独立に処理するため 2 個の SP を備えている。

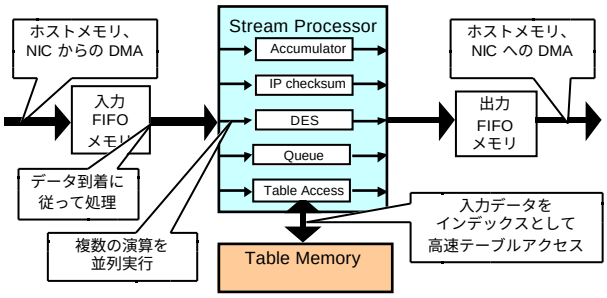


図－５　Comet NP

表－１　Comet NP 諸元

テクノロジ	CMOS 0.35μm（LSI Logic G10p）
動作周波数	Max. 70MHz
パッケージ	EPBGA 655pin
消費電力	6W@66MHz
外部バス	PCI 64/32bit、66/33MHz x 2
処理エンジン	Stream Processor (SP) x 2
付加機能	DES/3DES、Checksum、Table Lookup（全てSPに内蔵）

SP は一種のデータフロー型マイクロプログラムプロセッサであって、ホスト計算機やネットワークデバイスから転送されたデータを入力 FIFO メモリに受けると、パケット全体の転送完了を待たずにワード単位に処理を行い、結果を出力 FIFO メモリに出力する。内部演算器は並列動作可能であり、水平型マイクロプログラム命令により、入力データを同時に複数の演算器で処理させることができる。



図－６　SP 内部のデータフロー

SP の最大の特徴は Programmable Finite State Machine アーキテクチャによってプログラマブルでありながら

高速なパケット処理を実現可能な点にある。パケット処理は有限状態機械で記述できるが、 SP ではこの有限状態機械の状態遷移表を SP プログラムメモリに格納し、パケットデータを入力として 1 サイクル（2 クロック）に一回の状態遷移、演算、データ出力を行う（図－７）。

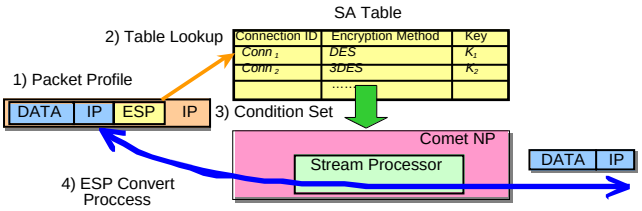
図－７　SP の状態遷移処理

2K 語のプログラムメモリにより最大 2048 状態遷移を定義可能である。

3.4.　ESP 実装

Comet ESP ではパケット解析と変換を SP が担当し、1000Base-T、ホスト計算機、 Comet NP 間の転送を SA1110 が担当する。Comet i-NIC のテーブルメモリに置く SA テーブルへの設定はホスト計算機が行う。SA テーブルには鍵データ、ESP ヘッダのプロトタイプ他の制御情報が格納されており、1 エントリあたりの大きさは受信側 88 バイト、送信側 184 バイトである。

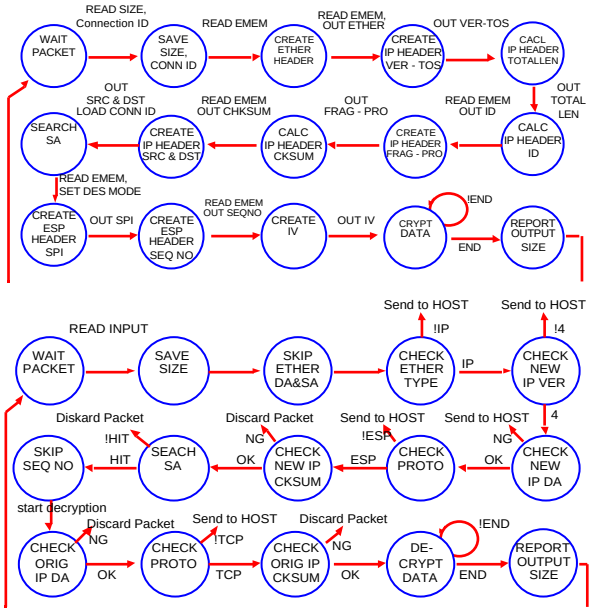
図－８に Comet ESP の処理フローを示す。



図－８　Comet ESP 処理フロー

まず ESP パケットを受信すると第一ステップで ESP パケットの解析を行い、第二ステップで SA テーブルを検索する。この処理は ESP パケットのヘッダ部データを転送した段階で行われる。第三ステップで SA テーブルの鍵データ等を Comet NP 内部の設定し、第四ステップでペイロードデータを復号化し、 IP パケットにして出力する。逆方向も似た流れとなる。

図－９に SP で実現する状態遷移図の概略を示す。



図－９　IP→ESP（上）、ESP→IP（下）状態遷移

IPv4 と IPv6 の識別は IP ヘッダによって行う。また SA テーブルにエントリのないパケットは変換せずに転送する。

IPv4 および IPv6 の IPsec ESP に対応する SP プログラムは送受信合わせて 721 語である。IPv4 のみの場合は 325 語[5]で IPv6 対応により約二倍強となったが、SP のプログラムメモリは 2048 語なのでさらなる機能増強が可能である。

4.　Comet ESP の評価

4.1.　評価環境

性能評価環境として Intel Architecture（IA）サーバを 2 組準備し 1000Base-T で対向接続した。基礎データとして IP 性能を表－２に示す。IA サーバは Fujitsu Primergy TS225 （ Pentium III Xeon 1GHz Dual Processor、表中プロセッサ種別として 1G と記述）と IBM eServer x345（Xeon 2.4GHz Dual Processor、同 2.4G）を使用し、シングルプロセッサ（ Single、表中 1G、2.4G）とデュアルプロセッサ（Dual、同 1G-D、2.4G-D）の場合について測定した。 Operating System は RedHat 9.0 kernel-2.4.20 、 IPSec は IPv4 で FreeS/Wan 2.01、IPv6 で USAGI Stable Release 4.1 を利用した。性能測定には netperf 2.2pl14 を使用し、単方向の TCP、UDP 性能を測定した。

TS225 はオンボードの 1000Base-T を持たないため、

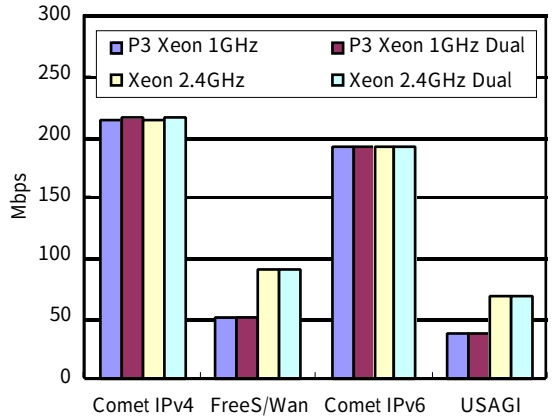
ソフトウェアスタックの測定では Comet i-NIC を単純な 1000Base-T NIC として用いた。x345 ではオンボードの 1000Base-T を用いた。いずれの場合も 1000Base-T 帯域の 90%以上の通信性能を実現していることがわかる。なお、IP 処理は SMP 対応していないため、Single/Dual の性能差はほとんどない。

表－２　IP 通信性能（Mbps）

	IPv4		IPv6	
	TCP	UDP	TCP	UDP
TS225+Comet i-NIC	938	946	929	954
x345	939	948	927	944

4.2.　ESP 評価結果

netperf による TCP の片方向転送性能の評価結果を図－10 に、TCP、UDP の数値データを表－３、表－４に示す。66MHz で動作する Comet ESP は IPv4、IPv6、プロセッサの違いに関わらず、200Mbps 前後の性能を実現していることがわかる。 Comet NP が内蔵する DES 演算器の 3DES 性能は 66MHz 動作ではで 220Mbps のため、DES 性能ネックとなっている。Comet ESP がプロセッサの違いに依存しない性能を実現しているのは ESP 処理を Comet i-NIC にオフロードした効果といえる。



図－10　IPSec ESP 3DES CBC Tunnel 性能

表－３　TCP/ESP 通信性能（Mbps）

TCP	Comet IPv4	FreeS/Wan	Comet IPv6	USAGI
1G	214.64	49.98	192.62	36.96
1G-D	215.12	51.23	191.85	37.62
2.4G	214.10	90.96	192.87	67.26
2.4G-D	215.23	91.52	192.60	67.82

表－４　UDP/ESP 通信性能（Mbps）

UDP	Comet IPv4	FreeS/Wan	Comet IPv6	USAGI
1G	214.00	53.16	195.88	40.65
1G-D	227.00	58.22	195.48	45.62
2.4G	219.82	99.40	196.76	76.15
2.4G-D	219.64	99.82	196.09	76.41

これに対して FreeS/Wan、USAGI は 2.4GHz Xeon でも UDP でも 100Mbps を下回る性能しかでていない。このことは 1Gbps の ESP 性能を実現するためには 24GHz 以上の Xeon が必要であることを意味する。

なお Comet ESP でも Xeon ソフトウェア処理でも Single/Dual で性能に大きな違いはなかった。これは IPSec ソフトウェアが SMP 対応していないためと考えられる。Xeon 2.4GHz では Hyper Threading Technology も試したが、ほとんど効果はなかった。

4.3.　Comet NP のパフォーマンス

以上の評価結果から 66MHz の Comet NP の SP は IPv4 TCP で 215Mbps の ESP 3DES 処理性能なので、処理バイト数／クロックは 3.26MB/MHz である。同様に Xeon 2.4GHz+FreeS/Wan は 38KB/MHz で Comet NP の 1/85 である。これらの値を基礎として IPv4 ESP 3DES 性能に対する Comet NP の所要クロックと消費電力を推測した。参考に Xeon ソフトウェア処理の予測クロックも示す。

表－５　Comet NP の性能と消費電力予測

IPv4 ESP 性能	Comet NP SP		Xeon Linux+FreeS/Wan
	clock	power	
1Gbps	307 MHz	27.9 W	26GHz
500Mbps	153 MHz	13.9 W	13GHz
200Mbps	61 MHz	5.6 W	5.2GHz
100Mbps	31 MHz	2.8 W	2.6GHz
50Mbps	15 MHz	1.4 W	1.3GHz
10Mbps	3 MHz	300mW	262MHz
性能比率	85		1

Comet NP の SP は 3MHz、300mW で 10Mbps の ESP 3DES 処理能力がある。現在は 0.35μm プロセスのためクロックが 70MHz 以下に限られるが、微細テクノロジで 300MHz 動作させればアーキテクチャを変更す

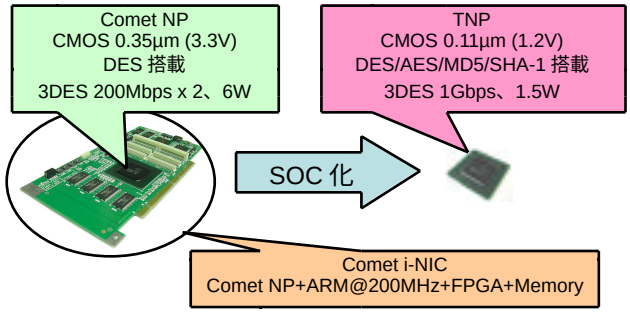
ることなく 1Gbps を実現可能であることがわかる。

また、Comet NP のパフォーマンス、すなわちクロック当りの ESP 3DES 処理性能は Xeon ソフトウェア処理に対して 85 倍、ルネサス SH7710 に対して 19 倍である。このことから SP アーキテクチャが優れていることがわかる。

5. Trusted Network Processor

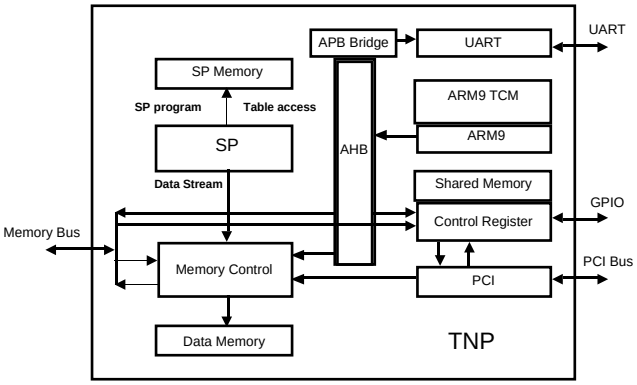
5.1. TNP

Comet ESP の評価結果に基づき、 TNP （Trusted Network Processor）[12]を検討した。TNP では Comet i-NIC をシステムチップ化すると共に、SP をさらに改善することで一層のパフォーマンス向上を狙う。Comet NP の回路を元に TNP の SP を試験的に設計し、シミュレーションで評価した結果を示す（図－11）。



図－11 TNP

図－12 に TNP の内部構成を示す。Comet NP では 2 個搭載していた SP 数を 1 個とし、各種アービタを簡略化することで SP 単体の処理能力を高めた。



図－12 TNP 内部構成

SP は機能および性能の向上を図った。まず演算器として DES/3DES の他に AES、MD5、SHA-1 を搭載した他、Comet NP では暗号演算中に SP の有限状態機械が停止していたのを改善して並列動作可能とした。その他命令セットの拡張を行った。

内蔵制御プロセッサとしては Comet i-NIC の SA1110 にほぼ匹敵する性能の ARM9（最高動作周波数 200MHz）を用いる。命令 128KB、 データ 128KB の大容量 TCM（Tightly Coupled Memory）を搭載し、SA1110 よりも実質的には高速に動作する。SP のプログラムメモリ、テーブルメモリ、データバッファメモリを全て TNP に内蔵し、200MHz 動作でノーウェイトメモリアクセスを実現する。

内蔵データメモリは 256KB の SRAM を 8 バイト幅で 200MHz 動作させ、SP、Memory Bus、PCI Bus からのデータ転送をこなす帯域を実現する。データ転送はそれぞれ専用の DMA エンジンを持ち、ARM9 の制御のもとに Gather/Scatter DMA、Multiple DMA を実現する。

Comet NP の RTL をベースに TNP の SP コアを作成した。表－6 に TNP の予想諸元を示す。

表－6 TNP 予想諸元

	TNP
テクノロジ	0.11µm、コア電源1.2V
ダイサイズ	6.2mm角
パッケージ	LBGA280（19mm角）
制御CPU	ARM9@200MHz
外部IF	32bit Memory Bus PCI 32bit, 33/66MHz
内蔵メモリ	600KB（4.8Mbit）
周波数／電力	10～200MHz/15mW～1.5W
暗号回路	DES/3DES、AES、MD5、SHA-1

プロセスとして LSI Logic 社 Gflx（0.11µm）を想定し、諸元を見積もった。消費電力はゲート動作率 20%で評価している。シミュレーションによる予想最高動作周波数は 200MHz であった。PCI 以外の部分について 10MHz から 200MHz まで動的に設定可能である。

ダイサイズを決定しているのは内蔵メモリ量である。内蔵メモリ量は Comet i-NIC で実現しているアプリケーションの一つである DVIPsec（Digital Video over IPSec）[8]プログラムがオンチップメモリで動作可能な最小限度の容量とした。

SP 部分のメモリを除くゲートサイズは 205KGate（SP

ロジック 70KGate、暗号 135KGate）であった。タイミング的に暗号回路がクリティカルパスになっているため、実配線遅延を考慮すると回路の並列化が必要とみられるが、その場合も 300KGate 以下で実現可能と考えられる。

5.2. TNP の ESP 性能

Comet ESP の性能から TNP による ESP 性能を見積もった（表－７）。基本的に TNP は Comet i-NIC より高速処理可能であるが、この効果は考慮せずあくまでクロックと消費電力で比較した。 TNP は携帯機器向けには 10MHz、75mW で 50Mbps のワイヤレス LAN を、サーバ向けには 200MHz、1.5W で 1Gbps ネットワークをフル ESP 可能と予測できる。このパフォーマンスは Xeon ソフトウェア処理の 131 倍、ルネサス SH7710 の 29 倍である。

表－７ TNP の性能と消費電力予測

IPv4 ESP性能	TNP		Xeon Linux+FreeS/Wan
	clock	power	
1Gbps	200MHz	1.5W	26GHz
500Mbps	100MHz	750mW	13GHz
200Mbps	40MHz	300mW	5.2GHz
100Mbps	20MHz	150mW	2.6GHz
50Mbps	10MHz	75mW	1.3GHz
10Mbps	2MHz	15mW	262MHz
性能比率	131		1

6. おわりに

我々が開発した Security Network Processor である Comet NP を使用して IPv4 ならびに IPv6 の ESP を実装した Comet ESP を評価した結果、66MHz の Comet NP を用いて 200Mbps の ESP 3DES 性能が得られることを確認した。

次にこの結果をふまえて ESP 処理の低消費電力化を実現する Trusted Network Processor（TNP）を検討し、RTL の試作ならびにシミュレーション評価を行った。TNP は 1Gbps の IPSec ESP 処理を 1.5W 以下の電力で処理可能と予測でき、クロック当たりの IPSec ESP 3DES 処理性能で比較してソフトウェア処理の約 131 倍、暗号回路を内蔵した一般的な Security Network Processor の 29 倍の能力をもつと考えられる。

SP は、パフォーマンスが高いこと、暗号回路を除くロジックが 70KGate と小さいことから携帯電話、各種携帯機器、情報家電、ブロードバンドルータ、サーバ向け NIC など様々な用途向けのシステム LSI に容易に組み込むことが期待できる。

今後は TNP をサーバや端末など実際のアプリケーションに応用していく予定である。

謝辞

TNP 見積もりのために情報を提供していただいた LSI Logic 株式会社、見積もりを担当していただいたイノテック株式会社、性能測定のための機材を提供していただいた東京大学情報理工学研究科平木教授に深く感謝します。

参考文献

[1] 有賀、南、江崎: IP Security ソフトウェア処理の性能評価, インターネットコンファレンス '99 論文集, pp. 61-66, Dec 15-16, 1999

[2] http://www.tcs.hut.fi/~helger/aes/rijndael.html

[3] http://www.renesas.com/jpn/edge/pdf/edge_vol02.pdf

[4] 陣崎: IPv6 マイクロチップの開発, WIDE 研究会 2001 年 12 月

[5] Masanori Naganuma, Akira Jinzaki: An IPsec ESP gateway on the "Comet NP" encryption network processor chip, Cool Chips 2002, April 2002

[6] RFC 2406, IP Encapsulating Security Payload (ESP)

[7] RFC 2405, The ESP DES-CBC Cipher Algorithm With Explicit IV

[8] http://www.comet-can.jp

[9] IEEE standard No. 1386-2001 and 1386.1-2001

[10] 陣崎: ネットワークプロセッサ, 第五回システム LSI ワークショップ, pp.139-148, 2001

[11] 陣崎: Stream Processor、並列処理シンポジウム JSPP2000, IPSJ symposium Series Vol. 2000, No.6, pp. 205-212, 2000

[12] 山澤: トラステッドネットワークプロセッサ , NEDO 電子・情報技術ワークショップ「次世代ヒューマンインターフェイス技術」, 2003