社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＳＬＤＭ－119（１）
2005／3／17

# Gigabit ネットワーク向け低消費電力セキュリティ LSI の開発

陣崎　明[†]　都筑 俊秀[‡]　鈴木 英好[†††]

†株式会社富士通研究所 〒211-8588 川崎市中原区上小田中 4-1-1
‡株式会社富士通コンピュータテクノロジーズ 〒211-8588 川崎市中原区上小田中 4-1-1
†††富士通株式会社 〒211-8588 川崎市中原区上小田中 4-1-1
E-mail: †zinzin@labs.fujitsu.com, ‡tsuzuki@ctec.fujitsu.com, †††suzuki@jp.fujitsu.com

**あらまし**　130nm プロセス、8.6mm ダイ、FBGA 584 ピン 18mm 角パッケージに Security Network Processor, GbE MAC 2 port, ARM9 を組込み、1Gbps の IPsec ESP 処理（AES 128bit, HMAC-MD5）を 2.3W-typical の消費電力で実現する TNP（Trusted Network Processor）を紹介する.

**キーワード**　SoC, GbE, Security Network Processor, ARM9, IPsec

# Development of a Low-power Security LSI for Gigabit Networks

Akira JINZAKI[†]　Toshihide TSUZUKI[‡]　and　Hidetaka SUZUKI[†††]

†Fujitsu Laboratories LTD., 4-1-1 Kami-odanaka, Nakahara-ku, Kawasaki, 211-8588 Japan
‡Fujitsu Computer Technologies Limited, 4-1-1 Kami-odanaka, Nakahara-ku, Kawasaki, 211-8588 Japan
†††Fujitsu Limited, 4-1-1 Kami-odanaka, Nakahara-ku, Kawasaki, 211-8588 Japan
E-mail: †zinzin@labs.fujitsu.com, ‡tsuzuki@ctec.fujitsu.com, †††suzuki@jp.fujitsu.com

**Abstract**　This paper describes the Trusted Network Processor (TNP), that integrates a Security Network Processor, 2 ports GbE MAC and an ARM9 into a 130nm, 8.6mm square die chip in an 18mm square FBGA 584pin package. TNP simulation confirmed 1Gbps IPsec ESP (AES 128bit, HMAC-MD5) performance with 2.3W-typical power.

**Keyword**　SoC, GbE, Security Network Processor, ARM9, IPsec

## 1. はじめに

2004 年 12 月，総務省は「u-Japan 政策」の工程表[1]を発表し，2010 年までに国民の 100%が高速あるいは超高速ネットワークを利用できる環境を実現する計画を示した．これからの数年間で全ての国民が平等に利用できる全国規模の「安心で安全な情報流通」基盤を実現するためには，物理ネットワークのみならず情報処理技術，プライバシー保護，著作権保護など非常に幅広い分野において多くの課題を解決していく必要があるが，中でもネットワーク基盤の高速性，安全性の確立は直近の課題と考えられる．

ネットワーク性能についてみると，日本では 2004 年 9 月で ADSL，FTTH あわせて 1763 万回線が契約中で，なお 200 万回線／半年の割合で増加している[2]．通信速度も FTTH は 100Mbps から 1Gbps へ，無線ネットワークは 10Mbps から 100Mbps へ高速化しており，着実に超高速ネットワーク基盤が整備されつつあるといえよう．

これに対して安全性についてはこれからである．現状，Gigabit クラスのセキュリティ通信は高価で消費電力低減は十分ではない．特に今後拡大する無線ネットワークを用いる携帯機器ではセキュリティ通信における性能対電力効率の向上が大きな課題である．

そこで，我々は Gigabit 性能のセキュリティ通信を低消費電力で実現することを目標とした Trusted Network Processor（TNP）を開発している．TNP はチップ単体で複雑なネットワーク処理を高速かつ省電力に実装可能なセキュリティ LSI であって，プログラム可能な点に特徴がある．開発はレイアウトをほぼ完了し，シミュレーションによる性能評価の結果，IPsec ESP（AES-128bit）および ESP-auth（HMAC-MD5）と IP の変換処理を 1Gbps, 2.3W-Typical で実現する見通しを得た．さらに TNP を 90nm プロセスで実装すれば同じ処理を携帯機器適用可能な 200Mbps-450mW, 50Mbps-250mW で実現可能と考えられる．本論文は TNP の仕様，内部構成，評価結果を報告する．

## 2. セキュリティ通信

安全な通信を実現するためには暗号による秘匿，認証による改竄防御が不可欠である．インターネットにおけるセキュリティ通信としてはネットワーク層で IP Security（IPsec），トランスポート層で Transport Layer Security（TLS），Secure Socket Layer（SSL）が多く用いられるが，これらの通信を実現した時の性能と消費電力が大きな課題である．ここでは IPsec の一部である Encapsulating Security Payload（ESP）トンネルゲートウェイ処理（ESP 処理）を具体例として，セキュリティ通信の実現方式と課題を述べる．

### 2.1. IPsec ESP

IPsec ESP は IP パケットを暗号化し，新たな ESP パケットにカプセル化（図 1）する規格で，本来の IP パケットは DES（Data Encryption Standard）/3DES や AES（Advanced Encryption Standard）などのブロック暗号によって秘匿される．ESP-auth を用いると MD5（Message Digest 5），SHA-1（Secure Hash Algorithm-1）などによるハッシュ値を用いてパケットの改竄を検出可能である．

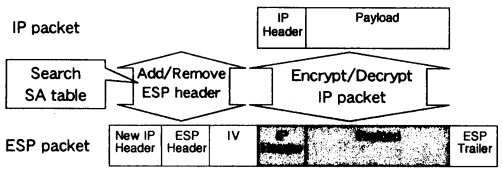


図 1　IPsec ESP（トンネルモード）処理

ESP 処理の実現においては，まず暗号や認証の計算コスト，次にパケットをカプセリングする処理コストが問題となる．

### 2.2. ソフトウェアによる実現

ESP 処理を実現する自然な方法はソフトウェアによる実装であるが，実装の柔軟性では優れるものの性能や消費電力の面では問題が多い．例えば Linux 及び FreeS/Wan の ESP（3DES）通信性能を実測すると Xeon 2.4GHz を用いて 99.4Mbps[3]で，Gigabit 性能を実現するためには 24GHz 程度の Xeon を必要とする．AES は DES の 7 倍程度のパフォーマンスが得られる[4]が，それでも 1Gbps を達成するには 3.2GHz 以上の Xeon 能力を 100%必要とする．

### 2.3. Network Processor による実現

本来暗号，認証計算をソフトウェアで行うのは無理があるので，プロセッサに専用演算回路を付加して，高速化を狙うアプローチがある．例えば，通信処理専用プロセッサである Network Processor[5,6]ではチップ内に暗号回路やハッシュ演算回路を内蔵するものが多く存在する．性能を公表している例ではルネサスの SH7710 が 200MHz の SH3-DSP プロセッサと「IP アクセラレータ」を用い，ESP 3DES を 34.2Mbps で処理する[7]．

### 2.4. 専用ハードウェアによる実現

さらに徹底して IPsec 処理を全てハードウェア化するアプローチもある．例えば Hifn HIPP は Gigabit Ethernet 対応，富士通 MB86978 は Fast Ethernet 対応で，共にワイヤスピードの ESP 処理を低消費電力で処理できる．但し，ハードウェア化してしまうと仕様を変更できない点が問題である．インターネットプロトコルは常に改善や新機能追加により変更され，様々なレベルで実装された機器間の相互接続性が要求される．実装の柔軟性は大きな課題である．

### 2.5. Comet NP

我々は処理の柔軟性を失うことなく高速なネットワーク処理を実現することを目標に Programmable Finite State Machine アーキテクチャを特徴とする Stream Processor（SP）方式を 1999 年に開発した[8]．2000 年には暗号回路として DES/3DES 機能を搭載した SP を 2 個内蔵する Comet NP を開発し，1 SP あたり 200Mbps の ESP（3DES）処理性能を実現した[5,9,10]．

## 3. TNP

Trusted Network Processor（TNP）は Comet NP の結果をもとに，最新のテクノロジーを用いて高速性，省電力性を追求したシステム LSI である．

### 3.1. ブロックダイアグラム

パケット処理を担当する専用プロセッサとして我々が開発した Stream Processor（SP），組込みプロセッサとして 32bit RISC プロセッサの ARM9，ネットワークインタフェースとして 10/100/1000Mbps Ethernet Media Access Controller（MAC）を 2 ポート，汎用の高速パラレルインタフェースを 2 ポート，データバッファ用メモリとして最大 512MB を接続可能な DDR SDRAM インタフェースを搭載した（図 2）．

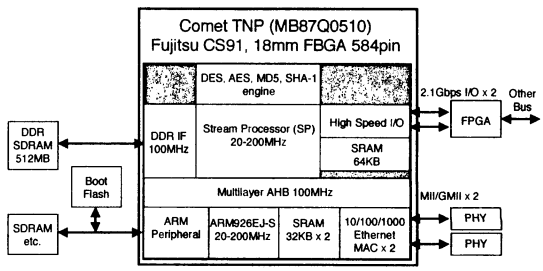


図 2　TNP 構成

### 3.2. ストリーム処理

TNP はパケットデーター連のデータ（これをストリームという）を入力ポートから読み込んで処理し，出力ポートに結果を書き出すパイプライン処理を行うプロセッサである．TNP には二つの高速通信ポートと外付けバッファメモリとのストリームデータ入出力 DMA 機能を設け，SP はこれら三組のストリームを自由に切り替えながら処理する．Gigabit Ethernet MAC（GMAC）とのデータのやりとりは組込みプロセッサの制御により，バッファメモリを介して行う（図 3）．

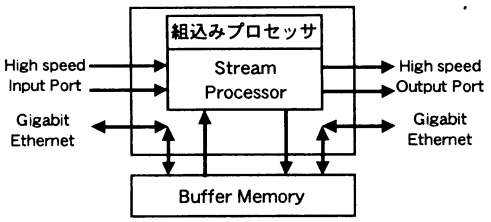


図 3　TNP のデータフロー

### 3.3. Stream Processor

TNP SP は Comet NP SP を踏襲し AES, MD5, SHA-1 機能の追加や各種機能の改善を行った．

表 1　Stream Processor 部仕様

| ブロック | 仕様 | 数量 |
|---|---|---|
| ネットワークプロセッサ | 64bit Stream Processor | 1 |
| ブロック暗号エンジン | AES 128/192/256bit Key | 1 |
| | DES/3DES | 1 |
| ハッシュエンジン | HMAC-MD5 | 1 |
| | HMAC-SHA-1 | 1 |
| 高速 I/O | 16bit Parallel w/ Clock I/O | 2 I/O |
| 内蔵メモリ | 8KW (64KB) SRAM | 1 |
| 外付けメモリ | DDR SDRAM max 512MB w/ Parity | 1 |

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，ストリームデータを入力 FIFO メモリに受けると，データ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．

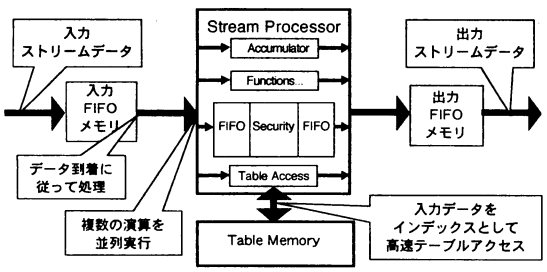


図 4　SP 処理

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ストリームデータ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 5）．セキュリティ演算はクロック数を要するので，データ入出力 FIFO メモリを設け，SP はセキュリティ演算中も他の処理を行えるようにした．

| Programmable Finite State Machine | |
|---|---|
| 最大 8 バイトのパケットデータ読み込み<br>処理データ部分の切り出し<br>最大 256 エントリの状態遷移表検索<br>複数演算（セキュリティ入出力他）を並列実行<br>パケットデータ出力<br>状態遷移（jump 命令） | 1 サイクル<br>(2 クロック)<br>で処理 |

図 5　SP 処理の特徴

内蔵メモリは SP 専用でプログラムとデータを配置し，高速にアクセス可能である．SP プログラムは 64bit 幅の水平型マイクロコードであり，最大 8KW のプログラムを格納できる．ESP 処理（暗号化／復号化，認証）を例にとると，SP プログラムサイズは 1KW，IPsec のデータベースである Security Association（SA）を 200 個程度置くことができる．

### 3.4. 組込みプロセッサ

組込みプロセッサとして ARM926EJ-S を採用した．MMU を持ち，Linux などの Operating System を動作可能である．高速な組込みソフトウェアをオンチップで動作させるために，キャッシュを命令，データそれぞれ 32KB，AHB 上に合計 64KB の RAM を設けた．ARM は TNP 内部の全ての資源にアクセス可能で，DDR SDRAM にプログラムを置くこともできる．ARM 周辺回路として DMAC, IRC, UART を備える．

内部バスとして Multilayer AHB を使用し，ARM, DMAC，GMAC が最高 400MB/sec の専用バスを用いてターゲットにアクセス可能である．GMAC は 10/100/1000Mbps 対応で MII/GMII に外付け PHY チップを選択可能である．

表 2　組込みプロセッサ部仕様

| ブロック | 仕様 |
|---|---|
| 組込みプロセッサ | ARM926EJ-S (I$ 32KB, D$ 32KB) |
| 内部バス、資源 | AMBA Multilayer AHB<br>64KB SRAM, UART, IRC, DMAC |
| Stream Processor 制御 | AHB Memory Mapped Register |
| データバッファ転送 | AHB DDR SDRAM DMAC |
| ネットワーク | AHB 10/100/1000Mbit<br>Ethernet MAC (MII/GMII) |
| 外付け ARM メモリ | AHB SDRAM 16bit max 64MB,<br>Flash Memory |

### 3.5. チップ仕様

表 3 に TNP のチップ仕様を示す.

表 3　TNP チップ仕様

| チップ仕様 | |
|---|---|
| プロセス | Fujitsu CS91 (130nm), |
| 規模 | Die size 8.6mm x 8.6mm, 2.6M Gates |
| パッケージ | FBGA-584, 18mm x 18mm, 0.5mm pin pitch |
| 消費電力 | 2.3W Typical (1.2 V core) |
| 内蔵機能 | ARM9, Stream Processor, Security, GMAC x 2 |
| 外部 IF | SDRAM, DDR SDRAM, Parallel I/O x 4, MII/GMII x 2, Serial, ETM, JTAG |

### 3.6. クロック

処理内容によって最適な処理性能を実現するため, 動作中にクロックを 10MHz から 200MHz まで機能ブロック毎に変更可能とした (表 4).

表 4　クロック

| ブロック | 動作周波数 |
|---|---|
| Stream Processor | 10-100MHz |
| 組込みプロセッサ | 20-200MHz |
| 内部バス、資源 | 10-100MHz |
| データバッファ転送 | 10-100MHz |
| 外付け ARM メモリ | 10-100MHz |

### 3.7. 回路規模

TNP の回路規模は全体で 2.6M Gates, ロジック部分は 1.4M Gates, RAM 部分は 1.2M Gates である (表 5). この内セキュリティ回路を含む SP のロジックは 0.5M Gates と小さい.

表 5　TNP 回路規模

| TNP 回路規模 | | |
|---|---|---|
| Stream Processor | Stream Processor Logic (including AES, DES, MD5, SHA-1) | 0.5M Gates |
| | Program Memory | 0.3M Gates |
| | Stream FIFO Memory | 0.3M Gates |
| ARM 他 | ARM9 core, Cache, SRAM, I/O | 1.5M Gates |
| 合計 | | 2.6M Gates |

### 3.8. パッケージ

TNP の消費電力は worst で 3W 程度になると予想される. この消費電力に耐え, 必要ピン数を満足するパッケージを新規開発した. FBGA-584 は Fine-pitch Ball Grid Array プラスチックパッケージ 18mm 角, ピンピッチ 0.5mm, 584 ピンである. 放熱のため Thermal BGA 構成とし, Thermal Pin 169 ピンを配置した.

### 3.9. ソフトウェア

TNP のソフトウェアは TNP 全体を制御する ARM ソフトウェアとパケット処理を担当する SP ソフトウェアからなる. アプリケーションに依存して「組込みソフトウェアモデル (図 6)」と ARM に Linux を搭載し, デバイスドライバで SP を制御する「Linux モデル (図 7)」がある.

組込みソフトウェアモデルは高速かつ実時間性を必要とする用途に有効で, 組込みソフトウェアは基本的にキャッシュ及びオンチップメモリで動作する.

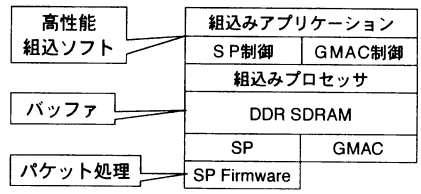


図 6　組込みソフトウェアモデル

一方, Linux モデルは高速性よりも Linux 上で動作するソフトウェアを活用し, 多彩な機能を実現する. いずれのモデルでも SP Firmware は同じであり, Linux モデルでは SP ドライバが Linux アプリケーションと SP との仲介を担当する.

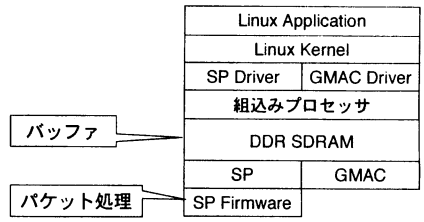


図 7　Linux モデル

ESP 処理では SP がパケット毎の高速処理が要求される IP-ESP 変換を行い, 組込みプロセッサが SA 管理, IKE (Internet Key Exchange) 処理を実行する. Linux モデルでは Linux で実装されている IKE ソフトウェアをそのまま利用可能である.

### 3.10. アプリケーション

TNP のアプリケーションは表 6 にあげるように多彩である. これらのいくつかはすでに Comet プロジェクトの中で Comet NP, 組込みプロセッサ, FPGA ハードウェアを用いて実装しており, それらのソフトウェアを TNP に移植する予定である.

表 6　TNP アプリケーション

| 分野 | アプリケーション | 概要 |
|---|---|---|
| サーバ ネットワーク | GbE NIC | Shaping NIC |
| | TCP | TCP 通信高速化装置 |
| インターネット | Delay | IP ネットワーク遅延シミュレータ |
| | Regulator | IP パケット平滑化装置 |
| | 1Gbps Home Router | 1Gbps WAN-LAN VPN Router |
| | Streaming Shaper | 1Gbps Streaming Shaper |
| 画像通信 | DVIP | Digital Video over IP |
| | DVIPsec | Digital Video over IPsec |
| | FWIP | IEEE1394/Firewire over IP<br>HDV, IIDC 等の IP 中継 |
| | SXGA/IP | SXGA over IP |
| | HDTV/IP | 非圧縮 HDTV over IP |
| | デジタル STB | MPEG2-TS over IP<br>地上デジタル放送端末 |

## 4. 評価

TNP の性能を論理シミュレーションツール(Cadence NC-Verilog, Mentor ModelSim) 及び消費電力評価ツール（富士通 PScope）を用いて評価した．シミュレータ上に試験環境を構築し，ARM プログラム，SP プログラム，GMAC を動作させた．ARM プログラムは GMAC の制御と DDR SDRAM と SP 間の DMA の起動，SP プログラムは DMA されたデータに対して ESP（AES-128bit, HMAC-MD5）処理を行う．

### 4.1. TNP 性能

表 7 に TNP のブロック毎の最高性能を示す．AES は 1.5Gbps，HMAC-MD5 は 1Gbps である．SP は 64bit 処理時に 4.2Gbps の性能なのでセキュリティ通信性能はセキュリティ回路の性能に制限される．

表 7　TNP 処理性能

| フロック | 仕様 | 最高性能 |
|---|---|---|
| ネットワークプロセッサ | 64bit Stream Processor | 4.2Gbps |
| ブロック暗号エンジン | AES 128/192/256bit Key | 1.5Gbps |
| | 3DES | 600Mbps |
| ハッシュエンジン | HMAC-MD5 | 1Gbps |
| | HMAC-SHA-1 | 600Mbps |
| 高速 I/O | 16bit Parallel w/ Clock I/O | 2.1Gbps |
| 外付けメモリ | DDR SDRAM max 512MB w/ Parity | 6.4Gbps |

### 4.2. 消費電力

SP で ESP（AES-128bit, HMAC-MD5）処理を行った場合の Typical 消費電力を PScope によって試算した．ESP 処理は全て SP が担当し，ARM は SP と DDR SDRAM の間の DMA 管理のみを行う．

試算の結果 SP 部の消費電力は 1Gbps で 464mW，100Mbps で 55mW となり，SP の性能対消費電力効率の良さが確認できた．一方，最も電力を消費するのは最高 100MHz で動作する DDR SDRAM である．リーク電流はチップ全体で 23mW と小さく押さえることができた．すでに述べたようにクロックを動的にブロック毎に変更可能なので，処理内容，要求性能によって消費電力を最適化できる．

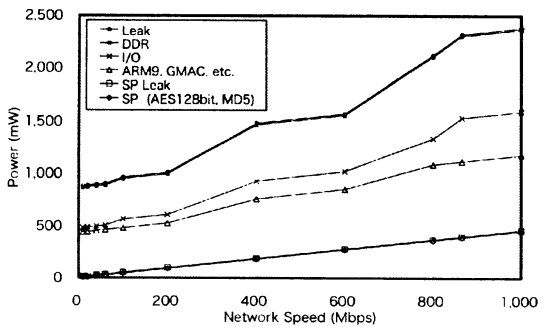


図 8　TNP 消費電力

### 4.3. 比較

表 8 に Comet NP と TNP の仕様比較を示す．ESP 性能は同じ 3DES で 3 倍，消費電力は 1/3 で，性能対電力効率は 9 倍である．AES では 22 倍になる．

表 8　Comet NP と TNP の比較

| | Comet NP | TNP |
|---|---|---|
| ES 完成 | 2000 年 3 月 | 2005 年 5 月 |
| プロセス | LSI Logic G10p (350nm) | 富士通 CS91 (130nm) |
| ダイサイズ | 13.43mm | 8.6mm |
| ゲート数 | 90 万ゲート | 260 万ゲート |
| 消費電力 Typical | 7W | 2.3W |
| パッケージ | 35mm 角 EPBGA-655 | 18mm 角 FBGA-584 |
| Stream Processor | 2 | 1 |
| セキュリティ回路 | DES/3DES | DES/3DES, AES, MD5, SHA-1 |
| 組込みプロセッサ | - | ARM9 (200MHz) |
| 外部インタフェース | PCI x 2, SRAM | GbE GMII x 2, Parallel I/O x 2, DDR SDRAM, ARM Bus |
| IPsec ESP 性能/SP | 200Mbps (3DES) | 600Mbps (3DES) 1.5Gbps (AES) |

表 9 に現時点で発表されている GMAC をもつチップをまとめる．TNP と同じ分野を狙ったチップが多数存在することがわかる．TNP と同程度の小面積，省電力チップは少ないと考えられる．

表 9　GMAC 搭載システム LSI

| Chip | Processor | GMAC | Security | Power | Package |
|---|---|---|---|---|---|
| AMCC nP3705 | uPcore 700MHz | 2 | × | ?? | ?? |
| AMCC PPC 440SPe | PPC 667MHz | 1 | × | 10W | FC-PBGA 675 |
| PMC-sierra RM9222 | MIPS64 1GHzx2 | 2 | × | 12W | FC-BGA 672 |
| CAVIUM NETWORKS CN3430 | OCTEON cnMIPS x4 | 4 | ○ | ?? | ?? |
| freescale MPC8545E | PPC 1.3GHz | 2 | ○ | ?? | FC-BGA 783 |
| freescale MPC8555 | PPC 533MHz | 2 | ○ | 5.4W | FC-BGA 783 |
| Vitesse VSC2202 | RISC 400MHz | 2 | × | 4W | FC-BGA 673 |
| Mindspeed M27483 | RISC 400MHzx2 | 4 | × | 5W | CBGA 1156 |
| Fujitsu TNP MB87Q0510 | ARM9 200MHz SP 133MHz | 2 | ○ | 2.3W | FBGA 584 |

## 5. TNP Mobile

携帯機器向けに 200Mbps 以下の性能に最適化した TNP Mobile を検討し，消費電力を評価した．200Mbps 以下の性能を実現するための SP の動作周波数は 50MHz 以下で十分である．ARM も 100MHz 以下でよい．大量のデータバッファは不要なので内蔵メモリとし，高速パラレルインタフェースを削除することで I/O 消費電力を大幅に低減できる．

図 9 に TNP Mobile の構成を示す．ネットワークを Compact Flash インタフェースに，DDR SDRAM を内蔵メモリに変更した．評価においては TNP と同じく ARM は組込みソフトウェアを実行することを想定し，100Mbps 以上では動作周波数を 100MHz，100Mbps 以下では 50MHz とした．SP は TNP 評価と同じプログラムを実行する．

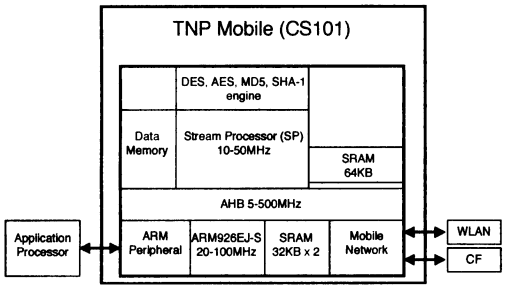


図 9　TNP Mobile の構成

表 10 に予測消費電力を示す．200Mbps 処理時においても 450mW-Typical 以下，SP 部分は 65mW-Typical であった．チップ全体のリーク電力は 2.3mA と TNP の 1/10 と考えられる．

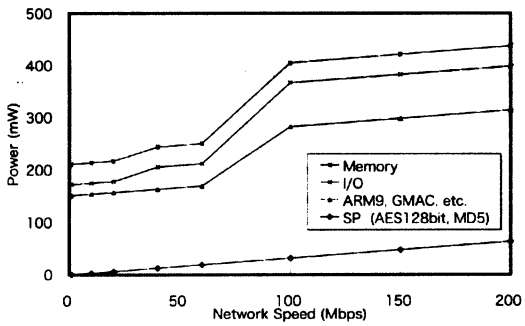


図 10　TNP Mobile の消費電力予測

## 6. おわりに

Trusted Network Processor(TNP)は 130nm プロセス、8.6mm ダイ、FBGA 584 ピン 18mm 角パッケージに Stream Processor, GMAC 2 port, ARM9 を組込み、1Gbps の IPsec ESP（AES-128bit, HMAC-MD5）処理を 2.3W-Typical で実現するセキュリティ LSI である．SP コアは 1Gbps に対して 464mW-Typical で動作する．開発はレイアウトをほぼ完了しており，2005 年 5 月に ES 完成を予定している．

次に TNP の評価結果に基づいて 200Mbps 以下の性能に最適化した TNP Mobile の消費電力予測を行った．この結果，90nm プロセスを用いればチップ全体で 200Mbps に対して 450mW-Typical，SP コアは 65mW-Typical と予想され，IP 携帯機器に十分適用可能な性能対電力効率を達成できることがわかった．

今後は TNP ES を評価するとともに，TNP アプリケーションソフトウェアの開発を進め，家庭向けネットワーク機器を中心に実用化していく予定である．

## 謝　辞

TNP の開発に関し，以下の技術者の尽力に厚く感謝する．富士通コンピュータテクノロジーズ第三統括部の彦坂貴弘氏，奥村嘉樹氏，山口隆明氏，根木秀幸氏，古川英治氏，加藤義則氏は SP 部の開発およびチップレベルシミュレーションを担当した．富士通デバイス株式会社 SoC ソリューション部の斉藤正氏，平田昭氏は組込みプロセッサ部および全体のレイアウトを担当した．富士通関西中部ネットテック株式会社システム開発統括部田中淳介氏は Stream Processor ファームウェアおよび開発ツールを担当した．

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。

## 文　献

[1] http://www.soumu.go.jp/s-news/2004/041217_7_bt2.html

[2] 大橋，“総務省の電気通信市場調査”，日経コミュニケーション 2005.2.15，pp. 91-103，2005 年 2 月

[3] 下國，河合，陣崎，山澤，中村，村井，"Security Network Processor による低消費電力 IPSec ESP の実装と評価"，インターネットコンファレンス 2003, pp. 51-58, 2003 年 10 月．

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

[5] 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.

[6] 陣崎，“ネットワークプロセッサの最近の動向”，電子情報通信学会誌，Vol. 86, No. 9 pp. 697-702, 2003 年 9 月．

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

[8] 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.

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

[10] 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 年 3 月．