

IPsec高速処理エンジン MB86978

双方向毎秒100Mビットの高速通信と暗号処理の両立を可能にした、ネットワーク機器向けセキュリティLSI「MB86978」を開発しました。本稿では、その基本的なコンセプトと特長を解説します。

* IPsec : Internet Protocol Security

はじめに

当社では、VPN*¹におけるIPsec処理を、双方向100Mbpsフルワイヤスピードで実行するLSI「MB86978」を開発しました。本製品を利用することにより、安定した高速通信と高度なセキュリティの両立が求められる、光ファイバ通信(FTTH)用ルータなどのブロードバンドネットワーク機器を容易に実現できます。また、現在主流のルックアサイド*²型のIPsec処理LSIと比べて飛躍的な処理性能の向上が期待できます。本製品は、高速・低遅延・低揺らぎが求められる、これからのブロードバンドVPNルータに最適なLSIです。

IPsecとは

IPsecは、IPパケット単位でのセキュリティを実現する技術です。IPパケットを暗号化し、通信相手が本物であることや通信データが改ざんされていないことを保証してアクセス制御を行います。これまで、多くのセキュリティ機能はアプリケーション別に提供されてきましたが、IPsecの登場によってその必要がなくなります。

近年インターネットにおいて、拠点間を仮想的な専用線で相互接続し、安全な通信を可能にするVPNが注目を集めています。IPsecは、VPNを実現するためのキーテクノロジーの一つとして利用されています。

開発コンセプト

ブロードバンドネットワークの普及に伴い、VPN業界標準であるIPsecに対応したブロードバンドルータが利用される機会が増えています。IPsecの機能であるパケットの暗号化・認証を実行するには、高速かつ大量の計算処理が必要です。このため、通常はIPsec専用のLSIを使って計算処理を行います。現状のIPsec対応VPNルータでは、ルックアサイド型のIPsec処理用LSIが使用されており、PCIバス経由でCPUとデータのやり取りを行います。しかし、この

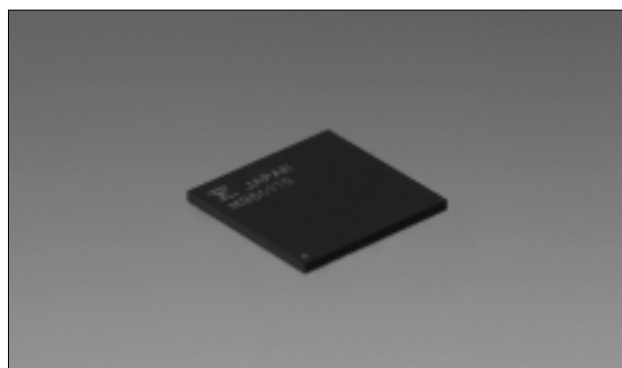
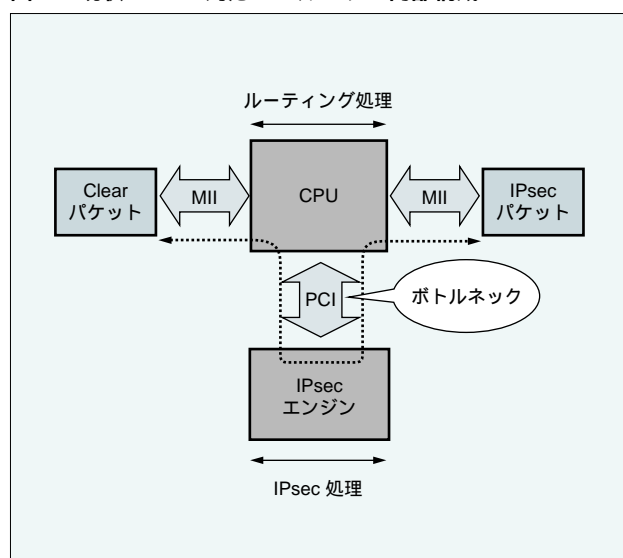


写真1 外観

図1 現状のIPsec対応VPNルータの内部構成



アーキテクチャではPCIバスにおけるボトルネックが存在し、IPsec処理のスループットに大きな影響を与えています。

図1に、現状のIPsec対応VPNルータの内部構成を示します。

本製品は、ホストCPUからSRAMインタフェース経由で必要なコンフィギュレーションを設定したあと、双方向100Mbpsフルワイヤスピードで暗号化/復号化の処理を実行します。IPsecパケットは、MII^{*3}インタフェース経由でルーティング処理を行うCPUとやり取りされるので、システムバス・ボトルネックの影響を受けません。

図2に、本製品を使用した場合のVPNルータの内部構成を示します。

図3に、現状のIPsec処理LSIと、本製品のパケットサイズに対するIPsec処理性能(3DES^{*4}使用時)の比較を示します。この図から分かるように、現状のルックアサイド型のIPsec処理LSIでは、十分な処理性能が得られていません。例えば、企業の拠点間をつなぐVPNなど、広帯域が必要な市場のニーズに応えるのは困難です。一方、本製品は、パケットサイズに関係なくフルワイヤスピードでIPsec処理が可能です。このため、高速ブロードバンド時代のVPN通信に欠かせないLSIソリューションになると考えられます。

図2 本製品を使用した場合のVPNルータの内部構成

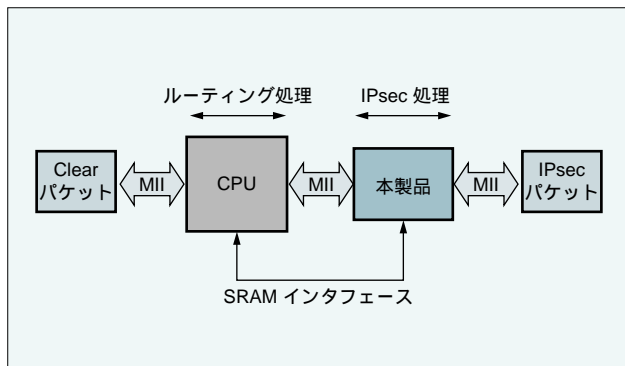
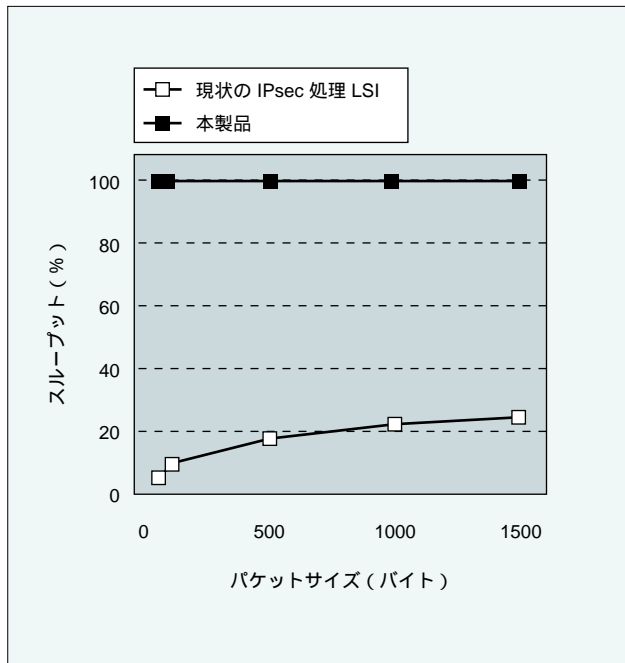


図3 パケットサイズに対するIPsec処理性能比較(3DES使用時)



特 長

●インラインIPsec処理

フルワイヤのIPsec処理を実行するために次の機能を搭載しています。

- ・フルワイヤ暗号エンジン：DES/3DES(CBCモード)，AES^{*5} (CBCモード，鍵長128/192/256ビット)
- ・フルワイヤ認証エンジン：HMAC-SHA-1^{*6}，HMAC-MD5^{*6}
- ・SA^{*7}(セキュリティアソシエーション)データベース：64件のSAが設定可能(エンコード側：64件，デコード側：64件) セレクタとして次のパラメータを指定可能
IPアドレス/ポート番号/セキュリティパラメータ・インデックス (SPI)/トランスポート層プロトコル/IPsecプロトコル

●IKE^{*8}サポート

IKEの計算処理を高速化するための機能ブロックを搭載しています。

●対応モード

トンネルモードとトランスポートモードに対応します。トンネルモードの場合はトンネルヘッダ処理も実行します。

- ・トランスポートモード(ESP^{*9}，AH^{*10}，ESP and AH)
- ・トンネルモード(ESP，AH)
- ・トランスポートoverトンネルモード

●対応パケット

- ・PPPoEパケット
- ・VLAN^{*11}パケット
- ・IPv4/IPv6両対応
- ・NAT-Traversal^{*12}対応

●2ポートのRMII/MIIインタフェースを搭載

インターネット側とルーティングファンクション側に、それぞれ1つの10/100BASE-T/TXインタフェースを搭載しています。

●SAデータベースの拡張

拡張クラシファイヤLSI「MB86979」を併せて使用することで、確立可能な暗号通信路(トンネル)の数を増やすことができるため、企業向けネットワーク機器にも適用できます。

仕様と構成

- 暗号化機能：DES/3DES，AES
- 認証機能：HMAC-SHA-1，HMAC-MD5
- IKEサポート：IKE Engine
- トンネル数：64件(暗号方向64，復号方向64)
- ホスト/F：16/32ビットSRAMインタフェース
- MACブロック：IEEE802.3(DIX形式)に準拠，WAN側/LAN側，各1ポートのMII/RMII I/F
- 電源電圧：1.8V/3.3V 2電源
- 動作周波数：最大66MHz
- パッケージ：FBGA337(13mm x 13mm x 1.15mm)
- プロセス：0.18 μm プロセス

図4に本製品のブロック図を示します。

拡張機能

本製品のESA I/Fに拡張クラシファイヤLSI「MB86979」を接続することで、トンネル数を大幅に拡張できます。拡張クラシファイヤLSIは1個で512件のトンネル数を提供し、最大8個まで接続できるので、トンネル数は4,096件になります。

図5に拡張クラシファイヤLSIの使用例を示します。

開発環境

当社では、本製品を使用した製品開発をサポートするため、評価/開発ボードをご用意しています。さらに、本製品とIPフォワードリングLSI「MB86977」を搭載し、VPNルータに組み込んだ評価/開発もご提供しています。本キットを利用することにより、高性能VPNルータを短期間で開発することができます。

図4 ブロック図

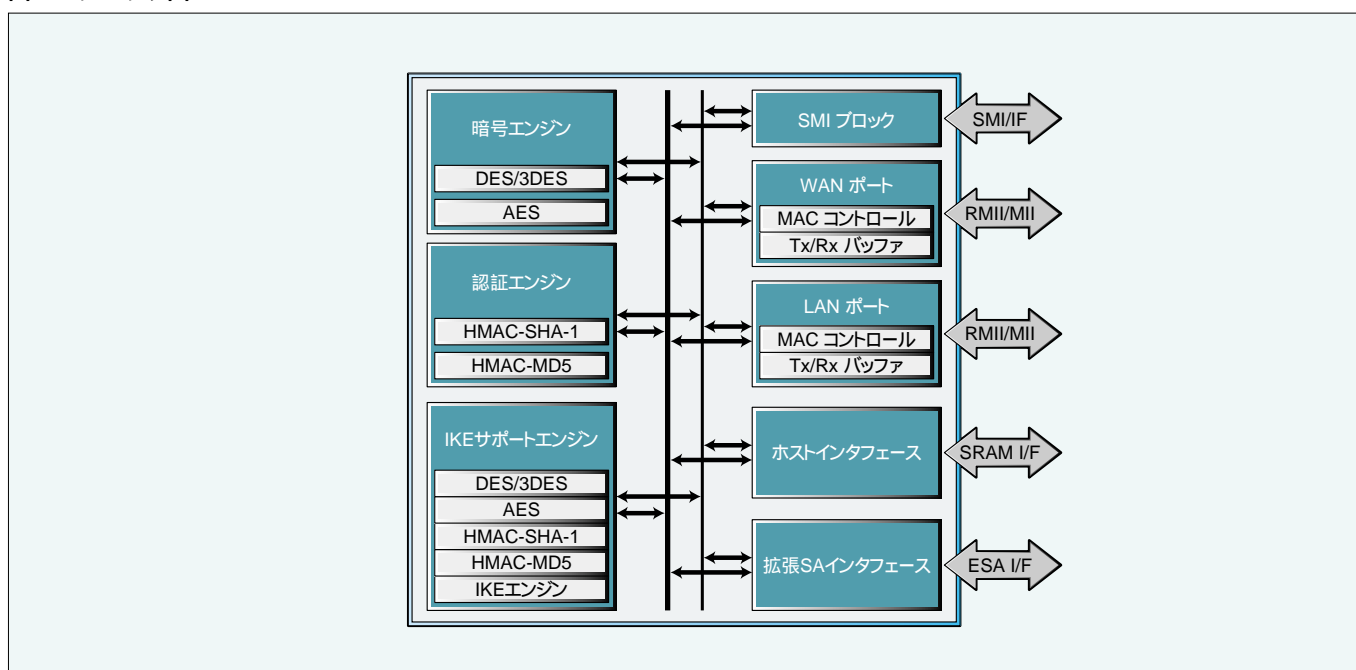
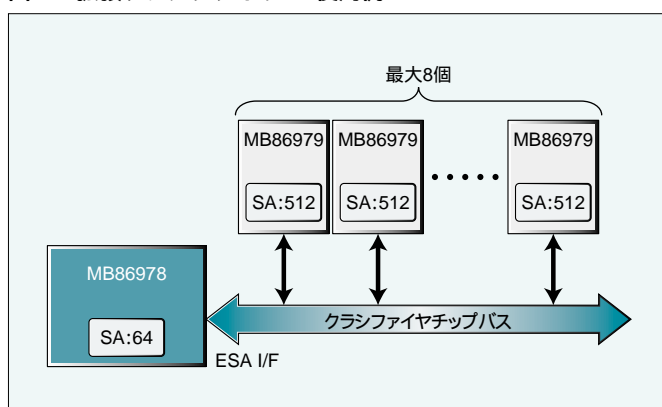


図5 拡張クラシファイヤLSI使用例



- * 1 : VPN (Virtual Private Network) : インターネットなどの公衆網を使用しながら、拠点間を専用線接続した場合と同等のセキュリティを確保し、安全な通信を実現する技術。
- * 2 : ルックアサイド : システムバス経由でCPUと接続する方式。
- * 3 : MII/RMII : PHY (物理層) とのインタフェース規格。
- * 4 : DES : 秘密鍵暗号化アルゴリズム。3DESは、DESを三重に適用したものの。
- * 5 : AES : DESに代わる次世代の秘密鍵暗号化アルゴリズム。
- * 6 : HMAC-SHA-1, HMAC-MD5 : 通信データの改ざんチェックを行う認証方式。
- * 7 : SA (Security Association) : 暗号通信を始める前に、暗号化方式や暗号鍵などの情報を交換・共有して確立された安全な暗号通信路。
- * 8 : IKE (Internet Key Exchange) : 通信相手の認証を行い、IPsecで使う秘密鍵の交換を行うプロトコル。
- * 9 : ESP (Encapsulating Security Payload) : 暗号化に用いられるセキュリティプロトコル。
- * 10 : AH (Authentication Header) : 認証に用いられるセキュリティプロトコル。
- * 11 : VLAN (Virtual LAN) : LANにおいて、物理的な接続形態に依存することなく、端末の仮想的なグループを構築する技術。
- * 12 : NAT-Traversal : NAT越しにIPsecを行うための技術。