

双方向1Gbpsフルワイヤスピード IPsec処理エンジン

当社では現在、IPsec処理を双方向100Mbpsフルワイヤスピードで実行する「MB86978」を量産しています。本稿では、そのスループットを10倍の双方向1Gbpsに高速化した、次期LSIの基本的なコンセプトと特長を解説します。

はじめに

当社では、IPsec処理を双方向1Gbpsフルワイヤスピードで実行するLSIの開発を進めています。本製品をIPsec処理に特化させたことにより、現在主流のロックアサイド型*1の暗号処理LSIと比べて飛躍的な処理性能の向上と、CPU処理負荷の軽減が期待できます。

本製品は、セキュアで高速・低遅延・低揺らぎが求められる、今後のインターネット接続、LAN環境に最適なLSIを目指します。

IPsecとは

IPsecは、IPパケット単位で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、高速かつセキュアな通信経路を確保できるようになりました。

近年インターネットにおいて、拠点間を仮想的な私設網として相互接続し、安全な通信を可能にするVPNが注目を集めています。そのVPNを実現するプロトコルの一つがIPsecです。IPv4通信ではオプションとされていましたが、次世代プロトコルのIPv6通信では必須のプロトコルとなっています。このようにIPsecは、今後のネットワークのキーテクノロジーの一つとして、幅広く利用されていくと予想されます。

市場背景と開発コンセプト

本製品はネットワーク市況、オフィス環境の変化を考慮して開発を進めています。

ブロードバンドネットワークの普及と、SOHO環境下に設置されるIPsec対応VPNルータの高速化に伴い、センタ側の装置にはギガビットクラスのIPsec処理能力が求められています。またオフィス環

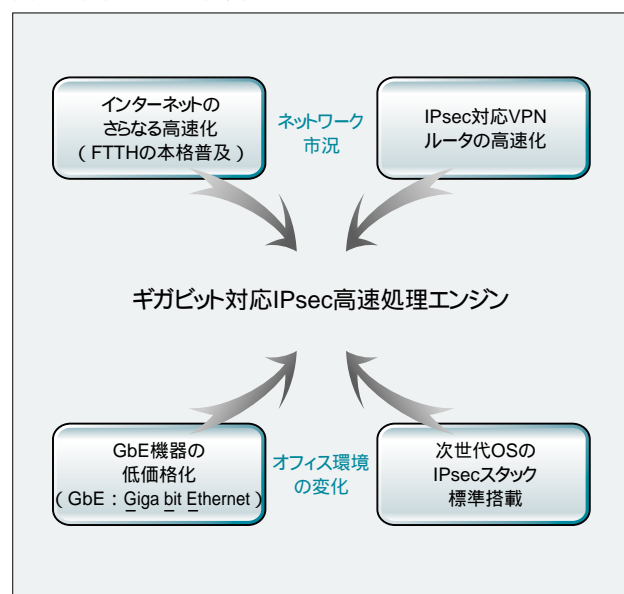
境では、ギガビット イーサネットポートを搭載したパソコンの登場や、ギガビット イーサネット対応NICとHUBの低価格化に伴い、近い将来にはLANのスピードがギガビットになると考えられます。

加えて、2006年後半からの発売が予定される、Microsoftの次世代OSにIPsecスタックが標準搭載される予定であり、本格的なIPv6時代の幕開けが予想されます。次世代OSを搭載したパソコンが増えれば、LAN内のIPv6パケット率は上がり、LANに接続されるプリンタやMFP(複合機)もIPv6対応が求められます。しかし、それらの機器とパソコンはCPU性能が異なり、超高速のIPsec処理にはIPsecアクセラレータ(エンジン)の搭載が不可欠になります。

以上のような要因により、当社はギガビット対応のIPsec高速処理エンジンの開発が急務と考えました。

図1に開発に至る市場背景を示します。

図1 開発に至る市場背景



当社では本製品に先立ち、双方向100Mbpsフルワイヤスピードを実現できるLSIを過去に開発しています。当時はロックアサイド型の暗号エンジンが市場を席捲していましたが、IPsec処理のスループットを上げるためには、CPU性能を上げるしかないと分かっていました。そのため当社では、LSIにインライン型アーキテクチャを採用し、CPU負荷を軽減するとともに双方向100Mbpsフルワイヤスピードを実現しました。本製品も、それと同じインライン型アーキテクチャを採用すると同時に、1チップでIPsec処理終端できるようにIKE*2をはじめ、プロトコル処理をサポートする専用コントローラ

を内蔵します。なお、専用コントローラを使用せず、メインCPUでIKEを実行できるIKEエンジンインタフェース(PCIバス)も有します。

図2に、本製品を使用した場合のシステム構成例(Security BOX)を示します。

図3に、本製品を使用した場合のシステム構成例(ミドルレンジVPNルータ)を示します。

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、高速ブロードバンド時代のVPN通信、また超高速LANのIPv6通信に欠かせないLSIソリューションを目指します。

図2 本製品を使用した場合のシステム構成例 (Security BOX)

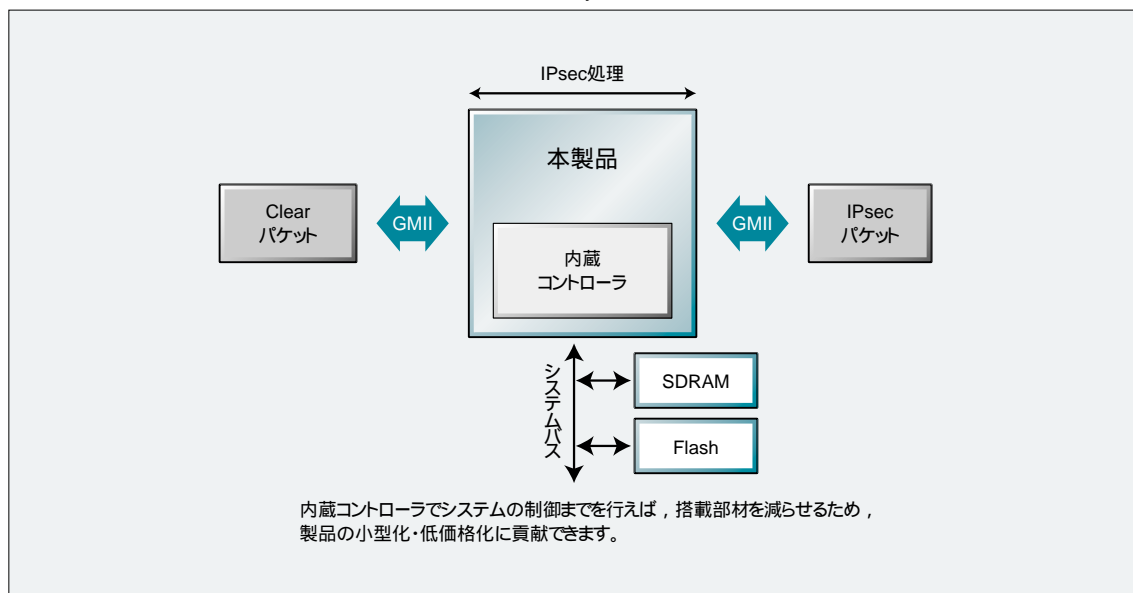
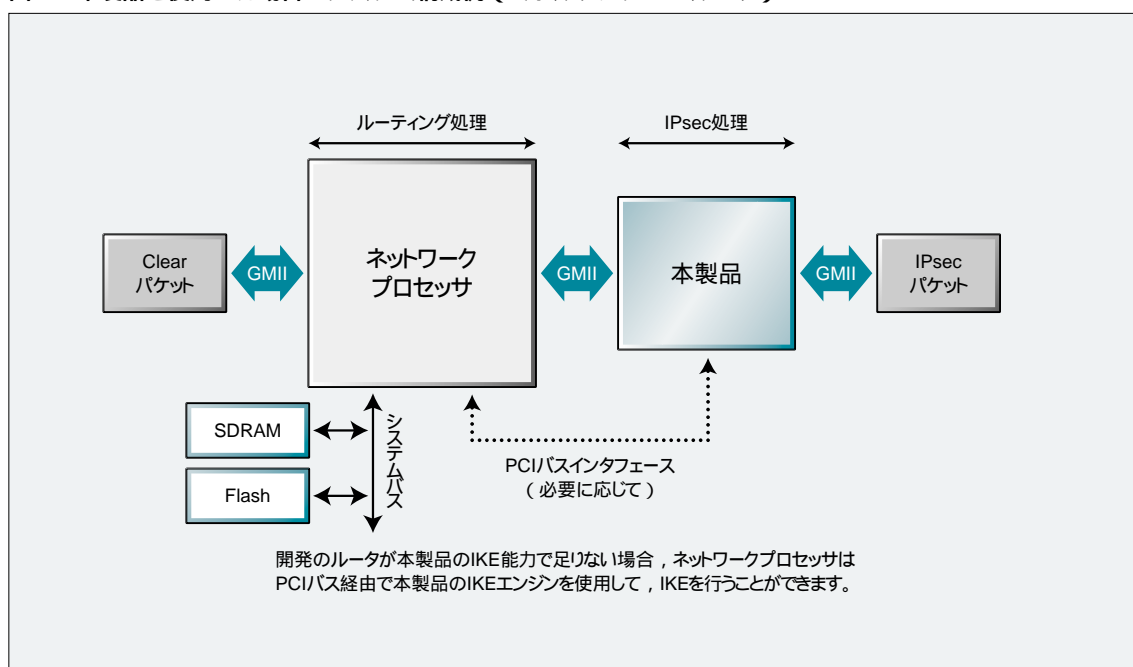


図3 本製品を使用した場合のシステム構成例 (ミドルレンジVPNルータ)



特 長

● GMII/RMII/MII*³ インタフェース搭載

- ・ WAN側 1ポート, LAN側 1ポート(計 2ポート)
- ・ GMII/RMII/MIIモードの設定可能
- ・ PHYデバイスの制御用SMIインタフェース搭載

● IKE専用コントローラとIKEエンジン搭載

IKEをフルサポートできる専用コントローラを搭載します。また, IKEの計算処理を高速化するために演算サポート用エンジンを搭載します。インタフェースは32ビット PCIバスです。

● IPsec処理エンジン搭載

フルワイヤスピードでIPsec処理を実行するため, 次の機能を搭載します。

- ・ フルワイヤ暗号エンジン :
 - DES/3DES*⁴(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
AES-XCBC*⁷
- ・ SA*⁸データベース : 512件のSAを設定可能
(暗号方向 : 512件, 復号方向 : 512件)

● 対応パケット

- ・ PPPoEパケット
- ・ VLAN*⁹パケット
- ・ IPv4/IPv6両対応
- ・ NAT-Traversal*¹⁰対応

● 対応モード

- ・ トランスポートモード(ESP*¹¹, AH*¹², ESP&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

● オートフラグメント, リアセンブル機能

IPsec処理後, パケット長がMTUサイズを超えるパケットを自動的に2分割できます。またフラグメントされたIPsecパケットを再構築できます。

● Jumbo Frame*¹³対応(~9Kバイト)

開発環境

当社では, お客様のスピーディな製品開発をサポートするため, 評価用プラットフォームの開発も進めています。なお, OSにはITRON, Linuxを採用する予定です。

- * 1 : ルックアサイド : システムバス経由でCPUと接続する方式。
- * 2 : 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。
- * 3 : GMII/RMII/MII : PHY(物理層)デバイス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を三重に適応したものの。
- * 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用認証アルゴリズム。
- * 7 : AES-XCBC : メッセージ認証コード(MAC)として, AESを使用する方法。
- * 8 : SA(Security Association) : 送信元, 送信先, セキュリティプロトコルなどを定義した論理的な通信路。
- * 9 : 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。
- * 10 : NAT-Traversal : NAT越しにIPsec通信を行うための技術。
- * 11 : ESP(Encapsulation Security Payload) : 暗号化に用いられるセキュリティプロトコル。
- * 12 : AH(Authentication Header) : 認証に用いられるセキュリティプロトコル。
- * 13 : Jumbo Frame : ギガビットイーサネットにおいて, パケットサイズを大きくし, データ転送効率を上げた技術。