

高速アクセスルータ 「UNIVERGE IX1000, 2000, 3000シリーズ」

High-Speed Access Router “UNIVERGE IX1000, 2000, 3000 Series”

鈴木 徹*
Toru Suzuki

歳田 隆一*
Ryuichi Toshida

松木 敦*
Atsushi Matsuki

立石 賀**
Tsuyoshi Tateishi

要 旨

近年、IP-VPNや広域イーサネット、インターネットVPNなどの新しいVPNサービスを活用して、IPベースの内線電話システムや基幹系システムをデータ系システムと統合して構築する企業が増えています。

そのため、中小規模拠点においても高速なスループットと信頼性の高いQoS処理、VPN実現のための高速な暗号処理能力を有するアクセスルータが求められています。

本稿では、キャッシュ方式によるパケット転送処理の高速化と、暗号LSIの採用によるVPN処理の高速化を低コストで実現した高速アクセスルータ(IX1000/IX2000/IX3000シリーズ)の実装技術について説明します。

Recently, increasing number of enterprises are utilizing new VPN services such as IP-VPN, Wide Area Ethernet and Internet VPN to integrate their IP based corporate telephone system and core transaction system onto the data network.

To support this integration, even at small to medium sized corporate sites, a high performance access router capable of handling large throughput, reliable QoS processing and high-speed encryption for VPN is on demand.

In this paper, technologies employed in the high-speed access router (IX1000/IX2000/IX3000 series router) to implement a low cost solution for fast packet forwarding using caching mechanism and high performance VPN processing using an encryption LSI are described.

1. まえがき

近年、IP-VPNや広域イーサネット、インターネットVPNなどのVPNサービスによるブロードバンド化に伴い、企業

ネットワークの中小規模拠点においても、情報インフラとなるネットワーク製品の機能の充実と、さらなる高速化および低価格化が求められています。特に、アプリケーションに依存せずにIPパケットを暗号化し、VPNを実現するための暗号通信プロトコルである、IPsecの暗号処理による性能劣化の少ない高速アクセスルータのニーズが高まっています。

NECでは、ルータの低価格化を実現するため、使用するデバイスを厳選して、ハードウェアを設計しています。特にIPsec処理に関しては市販のIPsecアクセラレータを搭載することで、高速化を実現したIX1000/IX2000/IX3000シリーズ(以下、IXシリーズと略す)を開発しました。

さらに、ソフトウェア技術として、フィルタ、NAT/NAPT、IPsecなどの各サービスで行われる検索処理を一元化するUFS(Unified Forwarding Service)キャッシュと呼ばれる独自機能の開発により、IPsec転送性能のさらなる高速化を実現した手法を紹介します。

2. ハードウェアアーキテクチャ

高速アクセスルータを開発するに当たって、高速なパケット転送性能と、VPNルータとして必須となるIPsec処理の高速化を低コストで実現することをコンセプトとしたハードウェアアーキテクチャを採用しました。

本章では、この施策検討結果をもとに製品化したIXシリーズのなかからIX2010を例に主要ハードウェア構成および、IPsec処理の高速化方式について説明します。

2.1 主要ハードウェア構成

IX2010では、CPUとして通信組み込みプロセッサ(Embedded CPU)を採用しています(図1参照)。

図1において、Embedded CPUには、レイヤ2処理を行う通信プロセッサ(Com Processor)とレイヤ3以上の処理を行うCPUコア(CPU Core)、およびブリッジ機能を有する汎用PCIコントローラ(PCI Controller)が内蔵され

* ビジネスネットワーク事業部
Business Networks Division

** NECエンジニアリング IPビジネス事業部
NEC Engineering, Ltd.

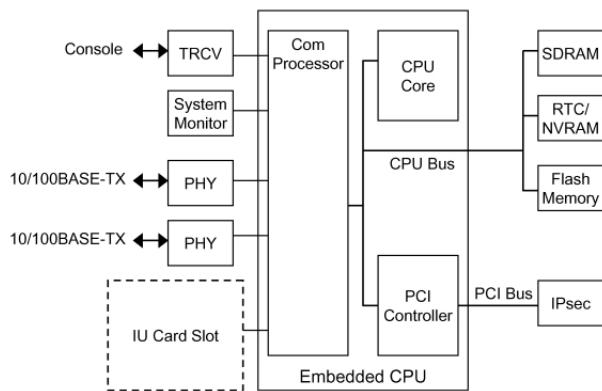


図1 IX2010の主要ハードウェア構成
Fig.1 IX2010 main hardware composition.

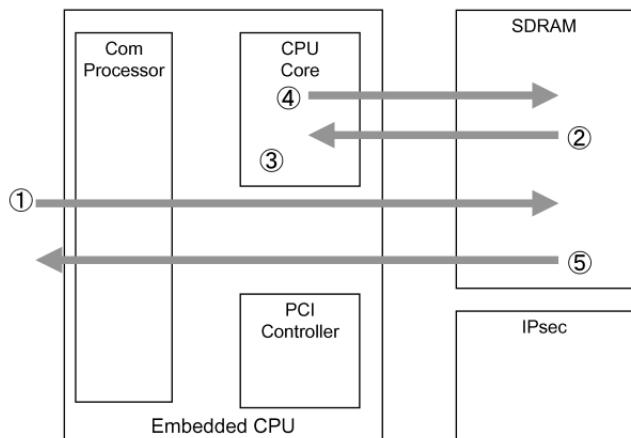


図2 IPsecソフトウェア処理フロー
Fig.2 IPsec software processing flow.

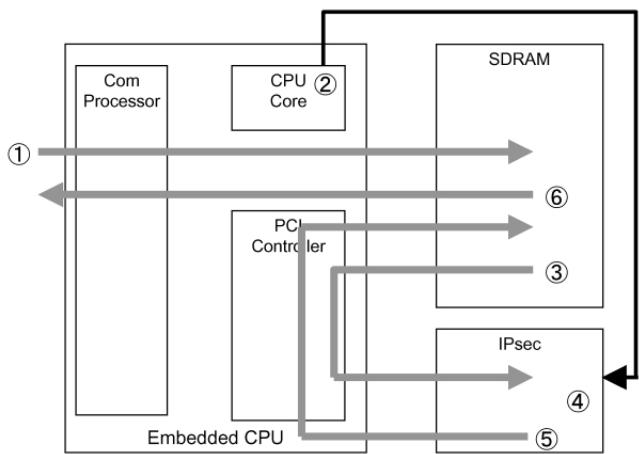


図3 IPsecハードアシスト処理フロー
Fig.3 IPsec hardware processing flow.

これに対して、ハードウェアアシスト処理では、IPsecに必要な演算やヘッダ処理などをすべてIPsecアクセラレータ内部で高速に行います。図3には、ハードウェアアシスト処理のフローが示されています。

- ① パケットの受信処理
- ② IPsecアクセラレータへの指示
- ③ パケットの読み出し
- ④ IPsec処理 (IPsecアクセラレータ内部)
- ⑤ IPsec処理完了パケットの書き込み
- ⑥ パケットの送信処理

このようにハードウェアアシスト処理では、IPsec処理にかかるほとんどの処理をIPsecアクセラレータで行うことにより、処理の高速化およびCPU Core負荷の軽減が可能となります。

ソフトウェア処理とハードウェアアシスト処理のIPsec使用時のパケット転送性能の実測値を図4に示します。ハードアシスト処理を用いることにより、ソフトウェア処理の最大約10倍の転送性能が実現できました。

ています。Embedded CPUの外部には、Ethernetフレームを送受する物理インターフェースデバイス（図中：PHY）、プログラムやルータのコンフィグレーションを格納するFlash Memory、プログラムのワークエリアおよびパケットバッファとして使用するSDRAM、IPsec処理を行うIPsecアクセラレータ（IPsec）とその他ペリフェラル部品により、構成されています。

また、Embedded CPUとIPsecアクセラレータ間は、PCIバスで接続することにより、チップ間の転送時間の高速化を図っています。

2.2 IPsec処理の高速化方式

IPsec通信を行うためには、以下の処理が必要です。

- (1) 共通秘密鍵を生成するためのDiffie-Hellman演算
- (2) ハッシュ計算アルゴリズムであるMD5, SHA
- (3) 暗号化処理であるDES, 3DES, AES
- (4) 認証ヘッダAH, ESP処理

これらの処理のうち、(1), (2), (3)の処理速度は、同時に確立できるIPsecのセッション数に影響し、(2), (3), (4)の処理速度は、IPsecセッション確立後のIPsecパケット転送性能に影響を及ぼします。したがって、(1)～(4)の処理時間を短縮することで、IPsec処理の高速化を実現することが可能となります。

以下に、IPsec処理をソフトウェア（以下、ソフトウェア処理）のみで行った場合、IPsecアクセラレータを使用した場合（以下、ハードウェアアシスト処理）のフローをそれぞれ図2、図3を使用して説明します。

図2には、ソフトウェア処理のフローが示されています。

- ① パケットの受信処理
- ② パケットの読み出し
- ③ IPsec処理 (CPU Core内部)
- ④ IPsec処理完了パケットの書き込み
- ⑤ パケットの送信処理

ソフトウェア処理では、通常のIPパケット転送処理に加え、IPsecに関するすべての処理をCPU Coreで実現しているため、CPU Coreに多くの負荷がかかります。

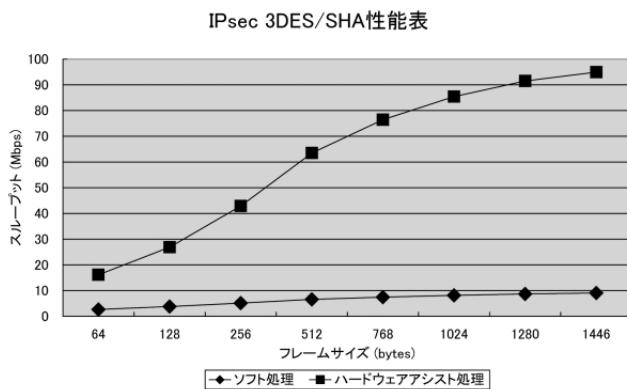


図4 処理の違いによる転送性能の比較

Fig.4 Throughput comparison by difference between software and hardware assisted processing.

3. パケット転送処理の高速化

IXシリーズは高速なパケット転送を行うために、NEC独自のソフトウェアプラットフォームを採用しています。

独自プラットフォームを扱う利点としては、ソフトウェアのメンテナンスが容易となります。さらに、OSの基本処理を調整することにより、ソフトウェアの格納メモリ、実行メモリを削減できます。そして、CPU処理負荷を最小限にすることにより、パケット転送処理に対して、ハードウェアのスペックを最大限引き出すことができます。その結果、IXシリーズでは高性能なフォワーディング処理を実現しています。

以下に、高速パケット転送処理における、独自の技術として、フォワーディングメカニズムの方式について説明します。

- UFS (Unified Forwarding Service) キャッシュ方式
パケット送受信時のフィルタやIPsecなどのサービスは、
パケットに応じてどの設定を有効にするかを決定するため
に、パケット検索処理やその結果を保持するためのキャッ
シュを持っています。各サービスはそれぞれ独立でキャッ
シュを保持し、その検索結果に基づいて処理が行われてい
ます。

通常では、フィルタ、IPsec、NATの設定がされている処理の流れを考えますと、図5左側のフローのように、それぞれのサービスにおいて、検索処理を行っています。そのため、1つのパケットに対して複数の処理負荷がかかっていました。

そこで、IXシリーズでは、パケット転送のさらなる高速化の実現のために、パケット転送の処理時に使用されるフォワーディングメカニズムとして、独自機能であるUFSキヤッショ方式を採用しています。

図5右側のフローにおいて、UFSキャッシュ方式は、パケットの受信から送信までの間に、フィルタ、NAT/NAPT、IPsecなどの各サービスで行われている検索処理を一元化

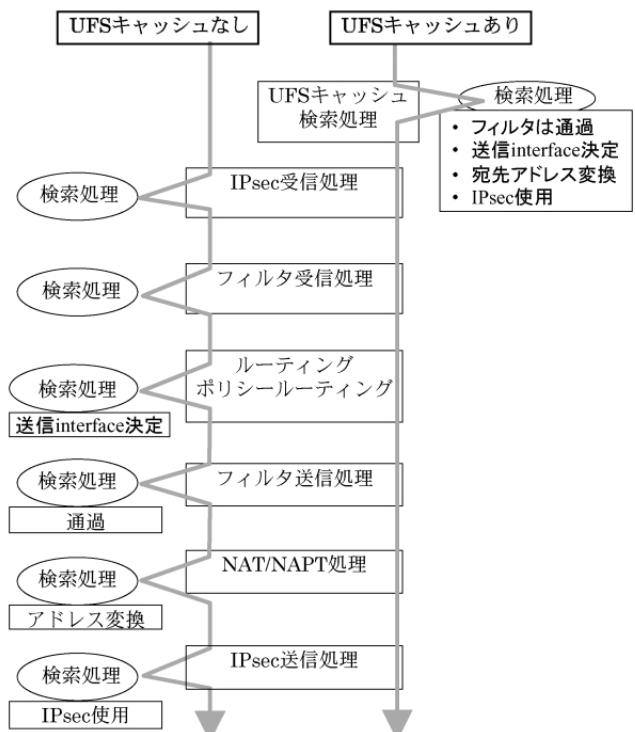


図5 UFS キャッシュパケット処理
Fig.5 UFS cache packet processing.

し、複数サービスの検索処理を1つの検索キャッシュに統合します。これにより、検索処理にかかる負荷、時間を軽減し高速化を実現しました。

図6では、UFSキャッシュ方式の有無、同価格帯のA社ルータと比較した性能結果を示します。UFSキャッシュありの場合、UFSキャッシュなしの場合と比べて10%程度の性能向上を実現しています。また、A社と比較しても性能差があることが分かります。

IX シリーズでは、UFS キャッシュの使用により、検索処理の軽減による性能の低下の抑制をすることにより、高速転送処理を実現しています。

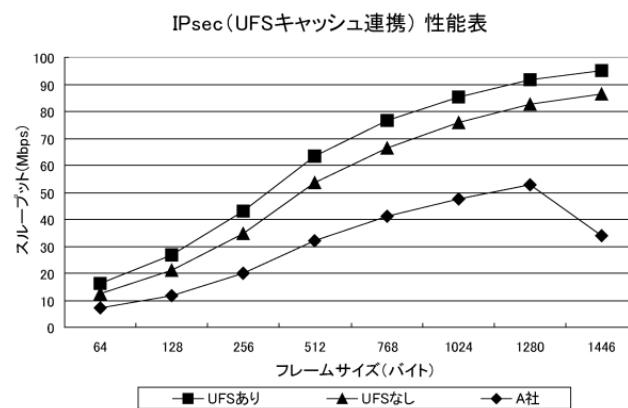


図6 IPsec性能表

4. むすび

IXシリーズでは、以上のような技術を適用し、同価格帯の他のルータと比較しても高負荷時での転送性能の劣化が小さく、実環境における高速なパケット転送を実現しています。

今後はIXシリーズの開発を通して培った技術をもとに、今後の市場ニーズに応えて、さらに高性能の製品開発を行う予定です。

* Ethernetは、米国XEROX社の登録商標です。

筆者紹介



Toru Suzuki
 鈴木 徹 1991年、NEC入社。現在、プロードバンドネットワーク事業本部ビジネスネットワーク事業部主任。



Ryuichi Toshida
 歳田 隆一 2002年、NEC入社。現在、プロードバンドネットワーク事業本部ビジネスネットワーク事業部勤務。



Atsushi Matsuki
 松木 敦 2003年、NEC入社。現在、プロードバンドネットワーク事業本部ビジネスネットワーク事業部勤務。



Tsuyoshi Tateishi
 立石 賢 1990年、NECエンジニアリング入社。現在、IPビジネス事業部主任。