

製品/プラットフォーム

高速アクセスルータ「UNIVERGE IX2000/3000シリーズ」

High-Speed Access Router “ UNIVERGE IX2000/3000 Series ”

高井道久*
Michihisa Takai

中村吾郎*
Goro Nakamura

中段信博*
Nobuhiro Nakadai

土屋幸一**
Koichi Tsuchiya

要旨

近年のIP-VPN、インターネットVPNの普及によって、より広帯域でセキュアなネットワークを安価に構築することが可能となっていました。

このようなVPNではIPデータ通信に限らず、音声通信の統合あるいはIP以外のプロトコルも使用可能なLAN間通信などへの利用に対する需要も高まってきています。

本稿ではこれら市場からの要求を実現するために、UNIVERGE IXシリーズ(IX2000/3000)に新たに実装した技術を紹介します。

Recently, the IP-VPN and Internet VPN have widely spread. It makes us possible to establish the network more extensively for cheap price.

Those VPN technologies not only support data communication but also are used for integrating voice communication system and LAN communication except for IP protocol, and these demands are getting higher day by day.

This paper introduces UNIVERGE IX series, (IX2000/3000) new technology which makes us satisfy those market demands.

1. まえがき

UNIVERGE IXシリーズ(以下、IXルータ)では市場からの要求を実現するために、SIP-NAT機能とEthernet over IP機能を新たに実装しました。

SIP-NAT機能により、従来のNAT/NAPT機能では不可能であったSIP(Session Initiation Protocol)パケットのアドレス変換が行え、インターネットを介したSIP端末間での通信が可能となります。

一方、Ethernet over IP機能では、EthernetフレームをIPパケットにカプセル化することにより、インターネットVPNを使用しての擬似的な広域LANネットワークの構築や非

IP端末による通信が可能となります。

本稿では新たにIXルータに実装したSIP-NAT機能とEthernet over IP機能の紹介をするとともに、IPsec機能を利用したインターネットVPNの構築例を紹介します。

2. SIP-NAT機能

IX2000/3000では、UNIVERGE SV7000(SIPサーバ)、UNIVERGE PS1000(プレゼンスサーバ)、およびNEterm50/60、DtermSP30といった多機能SIP電話機(SIP端末)に対応する、SIP-NAT機能を実装しました。図1のようなIPセントレックス形態での使用を想定しており、IXルータを拠点側に設置し、SIP端末を収容します。

従来、NAT/NAPT環境ではSIPを利用できませんでしたが、本機能を用いることで可能になります。

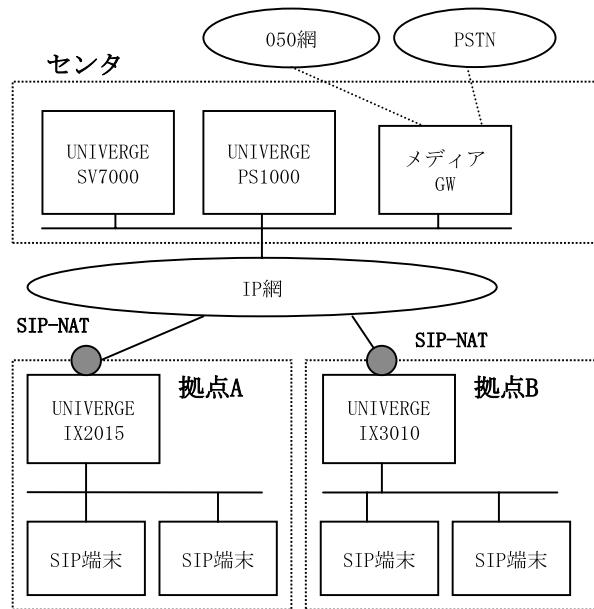


図1 ネットワーク構成
Fig.1 Network composition.

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

** IPネットワーク事業部
IP Networks Division

2.1 動作概要

(1) 機能ブロック

SIP-NATは以下のようにNAT/NAPTブロックとSIP-NATブロックが連携して、動作します。NAT/NAPTブロックはIPヘッダのIPアドレスおよびポート番号を変換する役割を持ち、IPアドレスおよびポート番号の変換情報（以下、NAPTキャッシュ）を持ちます。またSIPのデフォルトポート番号である5060ポートを監視しており、該当するパケットをNAPTキャッシュ情報とともに、SIP-NATブロックに渡します。

SIP-NATブロックは、SIPパケットのペイロードに含まれるSIPヘッダやSDP（Session Description Protocol）を解析し、それらに記述されているIPアドレスおよびポート番号を変換する役割を持ちます。またその解析結果からトランザクション・ダイアログの状態管理（SIP状態管理）、SDPの管理、SIP端末の管理を行います。SIP端末の状態やSDPにより記述される端末間のRTPセッション情報から、必要に応じてそれらのためのNAPTキャッシュの生成・削除をNAT/NAPTブロックに対して指示します。

(2) SIP端末の学習

SIP-NATは、プライベート空間内に存在するSIP端末からグローバル空間に存在するUNIVERGE SV7000へのREGISTERリクエストによって、SIP端末の存在を学習します。REGISTERリクエストを受信すると短時間のSIP端末情報を生成し、またUNIVERGE PS1000（プレゼンスサーバ）などREGISTERを行ったUNIVERGE SV7000以外の装置からのSIPパケットを受信するためのNAPTキャッシュを生成します。REGISTERリクエストが成功レスポンスを受信すると、それに記述されたExpires時間の間、そのSIP端末を有効なものとし、学習します（図2）。またSIPで規定されたREGISTERのリフレッシュの仕組みを利用して、不要な端末情報の削除を行います。

学習していないSIP端末からのSIPパケット、およびそのSIP端末へのSIPパケットは廃棄します。

(3) 通話制御

SIPではINVITEリクエストのシーケンス内でネゴシエートされるSDPにより、音声用RTPが使用するIPアドレスおよびポート番号が決定します。そのためSIPシーケンスを監視し、各セッション用にNAT/NAPT変換テーブルを生成・削除します。ただし、同一拠点内のSIP端末間での通話に関しては直接端末間で通信を行わせるため、NAPTキャッシュの生成は行いません。

各RTP用のNAPTキャッシュはBYEリクエスト（終話）を受信すると削除します（図2）。

2.2 成 果

本機能により、SIPのNAT/NAPT越えを実現しました。これにより、従来SIPを使用できなかったNAT/NAPT環境においてもSIP端末を使用することが可能になります。またNAPTと組み合わせて使用することで、拠点外に対し

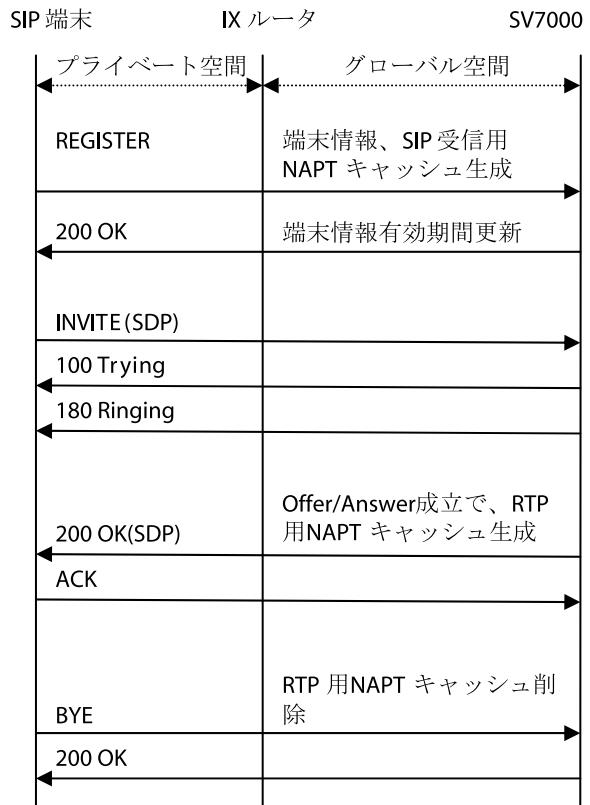


図2 動作例

Fig.2 Operation example.

て開いているポートをSIPと通話中のRTPのみに抑えることができるため、VoIP環境のセキュリティ向上が期待できます。

3. Ethernet over IP機能

IX2000/3000では、インターネット網上に広域Ethernetサービスと同様の環境を容易に実現することが可能となるEthernet over IPの機能として、EtherIP (RFC3378) を実装しました。たとえば図3のようなネットワークで本社内と営業所をEtherIPで結び、すべて同一LANのネットワークを構築できます。

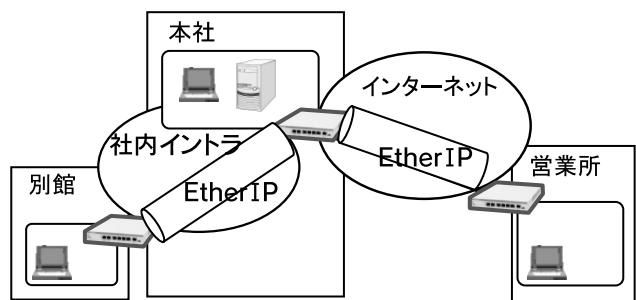


図3 Ethernet over IPによるネットワーク

Fig.3 Image of Ethernet over IP network.

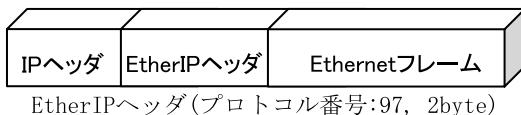


図4 パケットフォーマット

Fig.4 Packet format.

3.1 機能概要

EtherIPはRFC3378に定義されたカプセル化によるトンネリング技術です。図4のように、任意のEthernetフレームをIPヘッダとEtherIPヘッダでカプセル化することで実現します。

EtherIPでカプセル化したパケットは、IPの機能が利用できるため、IPsecと組み合わせて暗号化することや、経路を冗長化することも可能です。また、ブリッジ機能により、カプセル化するプロトコルを選択することも可能となります。

3.2 成果

このEtherIP機能により、従来よりも柔軟に多様なネットワーク構築が可能になりました。複数の拠点を同一LANセグメントに見せることができ、また非IPパケット通信のみをEtherIPでカプセル化することで、すでに構築済みのIPネットワークを崩すことなく、非IPプロトコルの通信を可能とすることも容易に実現できます。

4. インターネットVPN構築例

IX2000/3000では、大規模なネットワークを構築する際に、ミドルレンジルータのIX5000シリーズと連携することで、安全で信頼性の高いインターネットVPNネットワークを構築することができます。

ユーザデータをインターネット上で送受信すると、盗聴や改ざん、なりすましなどによる攻撃を受ける可能性があります。IXルータで実装しているIPsec機能を用いると、ユーザデータの暗号化、データ認証を行うことにより、攻撃を防ぐことが可能となるため、インターネットVPNをより安全に構築できます。さらに、ネットワーク冗長化、装置冗長化を行うことにより、ネットワーク障害、装置故障などから高速に復旧し、信頼性の高いネットワークを構築することができます。

図5に、IXルータを使用したインターネットVPNの構築例を示します。IXルータ間においてICMP Echo Request/Replyを利用し、到達性の監視を行い、到達性が確認できない場合、Main IPsec TunnelからBackup IPsec Tunnelへ切り替えることによりIPsecトンネルの冗長構成を構築し、また、センタ装置ではVRRP機能による装置冗長化を行うことにより、システムの信頼性を向上させています。

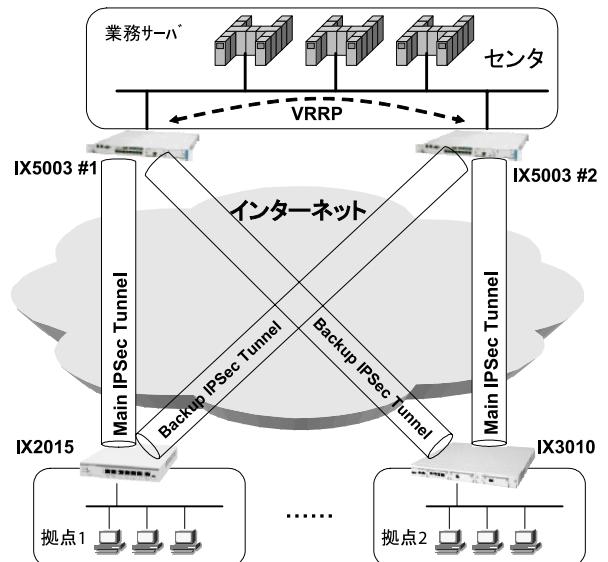


図5 インターネットVPNネットワーク構築例
Fig.5 Construction case of Internet-VPN network.

5. まくらび

IX ルータでは、以上のような機能を実装することにより、さらに幅広い範囲で適用することが可能となります。

今後はIXルータの開発を通して培った技術をもとに、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



Michihisa Takai
たか い みちひさ
高井 道久 1992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



Goro Nakamura
なかむら ごろう
中村 吾郎 1997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



Nobuhiro Nakadani
なかだん のぶひろ
中段 信博 2001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。



Koichi Tsuchiya
つち や こういち
土屋 幸一 2002年、NEC入社。現在、プロ
ードバンドネットワーク事業本部IPネットワーク
事業部勘定課