R&D ホットコーナー ソリューション

ベストエフォート型L2-VPNシステムの実用化

NTTアクセスサービスシステム研究所

斎藤（さいとう）　玲（あきら）※ /宮本（みやもと）　正和（まさかず） /首藤（すとう）　晃一（こういち）

中小企業/SOHOユーザをターゲットに，既存フレッツ網上でL2-VPN（Layer2 Virtual Private Network）サービスを実現するためのエッジルータ（ER）と設定サーバを開発しました．本サービスは，ユーザ宅内に小型ERを，サービス提供事業会社の網内に設定サーバを設置することにより容易に提供することができます．従来の広域イーサネットサービスが大企業向けであったのに対して，中小企業/SOHOユーザ向けに安価なL2-VPNサービスを提供することが可能です．

VPNとは

VPN（Virtual Private Network）は，仮想的な専用線環境を提供するための技術です．以前は，ユーザ拠点間をATM（Asynchronous Transfer Mode）やFR（Frame Relay）技術による仮想的なパスで接続するオーバーレイモデル方式が主流でした．

この方式は，データリンク層で冗長化できて信頼性も高く，細かな品質（QoS: Quality of Service）制御が可能であるということが利点です．しかし，各拠点にルータを設置する必要があり，装置コストが上昇し，設定の際に高度な知識と経験が必要であること，拠点間が１対１接続で結ばれるため，拠点数の増加で網が大規模化すると，パスの維持管理が複雑になること，通信キャリア網のコア側に負荷が集中することが課題でした．

こうした中，IPやVLAN（Virtual LAN）通信技術を用いた新しいVPN技術が出現しました．これらの技術は，網内のパケット転送方法の違いから，L3-VPNとL2-VPN方式に大別されます．

L3-VPN方式

L3-VPN（Layer3-VPN）方式は，IPパケットのヘッダ情報に基づいてVPNを制御します．BGP（Border Gateway Protocol）とMPLS（Multi Protocol Label Switching）技術の組み合わせや，VR（Virtual Router）技術を用いたIP-VPNサービスが代表的な例です．

この方式は，各VPN拠点からの経路制御を通信キャリア網内のエッジルータでいったん終端するため，拠点ルータの設定や負荷が軽減されることや，各ユーザ拠点からの経路制御情報が網内に流入しないため，網内ルータの負荷が軽減すること，動的な経路制御プロトコルにより網内の転送経路を柔軟に冗長化できることが利点です．しかし，エッジルータに負荷が集中することや，IPプロトコルしか利用できないことが課題です．

L2-VPN方式

L2-VPN（Layer2-VPN）方式は，イーサネットフレームのヘッダ情報に基づいてVPNを制御します．VLAN-VPN技術を用いた広域イーサネットサービスが代表的な例です．

この方式は，通信キャリア網全体をLayer2スイッチで構成し，各スイッチはVLANタグ値によりVPNを識別します．

すなわち，ユーザ拠点側からは，網全体が１つのスイッチングハブのように見えるため，IP以外のプロトコル（WindowsのNetBIOS やMacintoshのAppleTalk等）が利用できることや，ユーザ拠点にルータを設置する必要がないため，運用設定に関する高度な知識や経験が不要であることが利点です．しかしながら，階層化されていないMAC（Media Access Control）アドレスにより転送経路が制御されるため，各スイッチの転送テーブルが巨大化することや，MAC層には転送ホップ数の制限がないため，スイッチの経路制御の設定に注意が必要なこと，VLANタグのスタックを行っても，識別できるVPN数に限りがあるため，大規模な網を構築することが難しいこと，QoS制御機能が乏しいことが課題です．

開発したベストエフォート型L2-VPNシステム

本システムは，ベストエフォート型のIP-VPN上でイーサネットの接続性を提供するEther/IP-VPN（Ethernet over IP-VPN）方式により動作します．

Ether/IP-VPN方式は，IP-VPNとVLAN-VPNの長所を兼ね備えています．

すなわち，ユーザ拠点側からは，通信キャリア網が１つのスイッチングハブと

※現，NTT東日本

して見えますが，実際には網内でIP経路制御を実行します．この特徴により，ユーザ拠点にルータを設置する必要がなくなり，運用設定が容易であることや，IP以外のプロトコルも利用できること，網内をイーサネットで構成する必要がないため，既存のIP網を利用できることが利点として挙げられます．

またL2-VPNの制御に必要なユーザ端末のMACアドレスは，ユーザ拠点に設置されるL2-VPN用ERにより自動学習され，学習したアドレスは，ERごとに分散管理されるため，ERの運用管理が容易であり，網内ルータへの負荷も軽減されるため，網の規模拡張性に優れていることも利点として挙げられます．

パケット転送方式

Ether/IP-VPN方式のパケット転送の流れとERのパケット転送フォーマットを図１に示します．本方式は，ER間の転送網として通常のIP網を用いており，イーサネットトラヒックをIP上でトンネル接続*1します．まず入口ERは，端末側からイーサネットフレームが届くと，VPNを識別するためのVPNヘッダと出口ER宛のIPヘッダを付加して網内へ転送します．網内のIPルータは，ユーザ拠点内と独立したIP経路制御を行い，出口ERまでパケットを転送します．出口ERは，付加されたVPNヘッダとIPヘッダを除去した後，イーサネットフレームを自拠点側の端末へ転送します．

ERにおけるMACアドレス自動学習

各ERは，どのER拠点にどの端末が存在するかを自動学習します．これにより，同一VPN内の適切な拠点にしかトラヒックを転送しないため，網内の帯域消費量やERの処理負荷を軽減する効果があります．またユーザ拠点からは，網全体を１つのスイッチングハブのように取り扱えます．

MACアドレスの自動学習の方法を図２に示します．図２(a)は自拠点からの上りパケットにより，下りパケット用の転送テーブルを自動学習する様子を，図２(b)は網側からの下りパケットにより上りパケット用の転送テーブルを自動学習する手順をそれぞれ示しています．

まず入口ERは，LAN側の自拠点端末AからWAN側の対向拠点端末B宛の上りパケットが到着すると，下り用の転送テーブルにパケットの送元（端末A）MACアドレスのエントリーを追加します．この学習により，WAN側の対向拠点から端末A宛のパケットが入口ERに到着した場合，ERは自拠点に端末Aが存在することを認識できるので，VPN-IDを検査した後，網内転送用に付加されたIPヘッダを除去してLAN側に転送します．

一方，出口ERは，WAN側の対向拠点端末AからLAN側端末B宛の下りパケットが到着すると，パケットヘッダ内のVPN-IDを検査した後，上り用の転送テーブルにパケットの送元（端末A）MACアドレスと，送元（入口）ERのIPアドレスをエントリーに追加します．この学習により，出口ERの自拠点側から端末A宛のパケットが到着した場合，出口ERは端末Aが入口ERの拠点に存在することを認識できるので，網内転送用のIPヘッダを付加してWAN側に転送します．

なお転送テーブルを自動学習した後は，ER間でユニキャスト転送*2が行われます．しかし，宛先端末のIPアドレスは分かっているが，どのERの配下に属しているか不明であるような場合は，IPアドレスからMACアドレスを解決するためのARP（Address Resolution Protocol）パケット等が，端末からERに届きます．この場合は，ERが同一VPNに属する対向拠点の数だけパケットをコピー

*1　トンネル接続：転送方式の異なる２つの網がある場合にエンドエンドでパケットを転送するために，網境界上で経路制御ヘッダを挿入削除する技術．例えば，IPv4網に挟まれたIPv6網がある場合，IPv6網内ではIPv4パケットをIPv6パケットで包んで転送します．

*2　ユニキャスト転送：特定のある１つのノードだけを対象とした通信方式．マルチキャストの反対語．

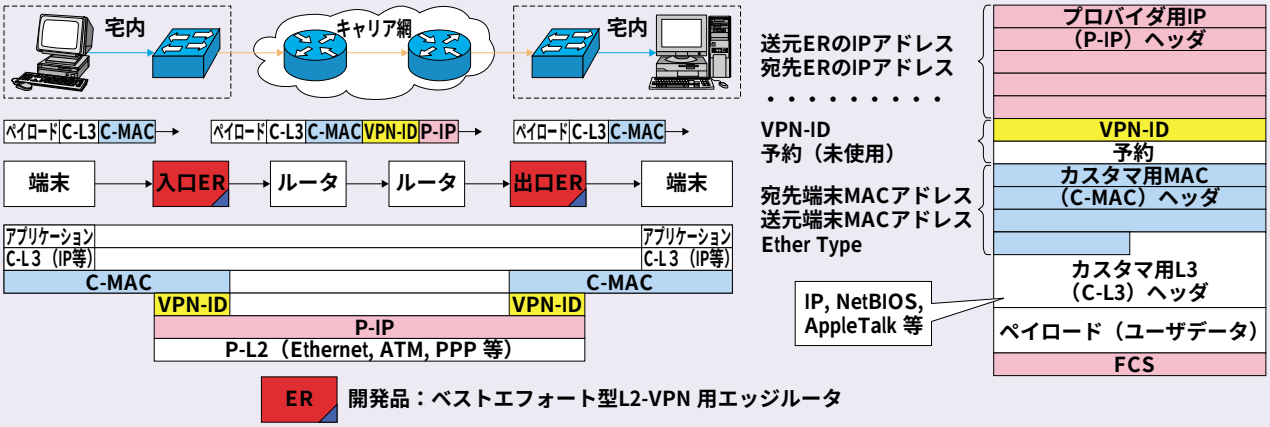

図１　Ether/IP-VPN方式のパケット転送の流れとERのパケット転送フォーマット

し，全ユーザ拠点へブロードキャスト転送します．

またER間を端末が移動することも考慮して，転送テーブルにすでにエントリーが存在する場合は，そのエントリーを新しい到着パケットのヘッダ情報に基づいて上書き更新します．さらに実装上，保持できるエントリー数にも限りがあるため，エージングタイム*3を設け，無通信状態が長いエントリーは削除します．

サービス提供形態

既存フレッツ網上に本L2-VPNシステムを適用する場合のサービス提供形態を図３に示します．図３(a)は，NTT事業会社とVPN事業者が連携して実施するサービス形態，図３(b)は，NTT事業会社が単独で実施するサービス提供形態です．

VPN事業者とNTT事業会社が提携してサービスを提供する場合，VPN事業者は一般的なISPが有するフレッツ網との接続設備と，ERを管理する設定サーバ等を備え，ユーザ間をVPN接続することで収入を得ます．一方，NTT事業会社はフレッツ網内の通信料金で収入を得ます．

NTT事業会社が単独でサービスを提供する場合，フレッツグループアクセスで異種VPN間のセキュリティを確保したうえで，イーサネット層でのLAN間接続サービスを展開します．東西事業会社は，フレッツ網の利用料金，フレッツグループアクセスの利用料金が収入となります．

インターネット接続との同時利用

開発したERは，２本のPPPoE（Point-to-Point Protocol over Ethernet）セッションを使い分けることにより，VPNとインターネットに同時接続できます．図４に導入例を示します．VPNを

*3 エージングタイム：学習したMACアドレスは，永久に保持されるわけではなく，学習後一定の時間がたつと学習前（忘れた）の状態になります．このMACアドレスの保持時間のこと．

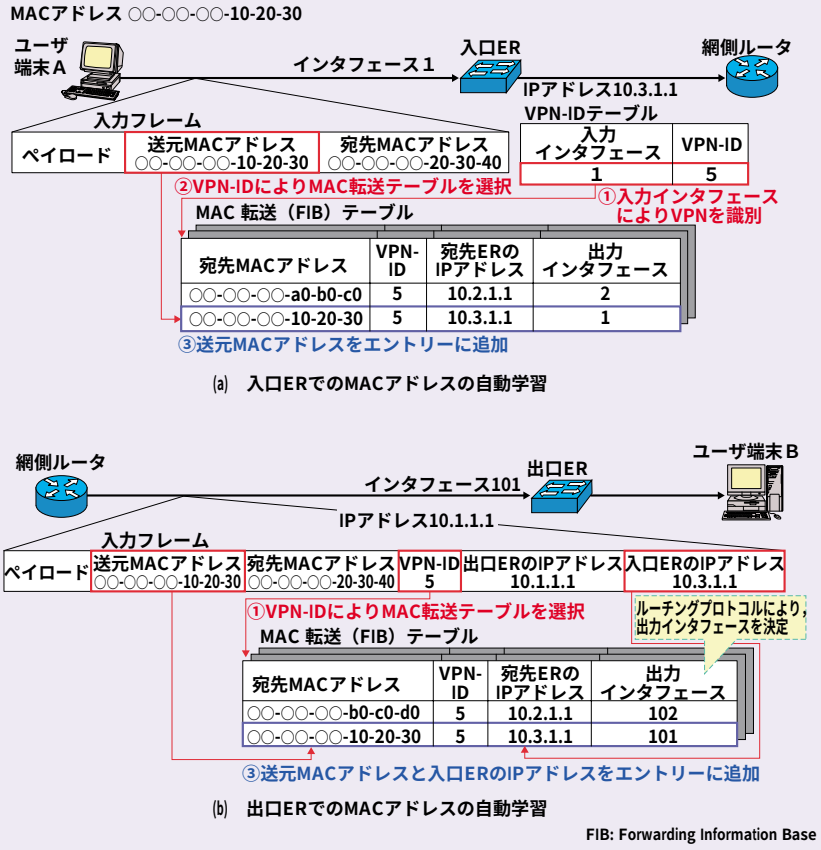

図２　MACアドレス自動学習の手順

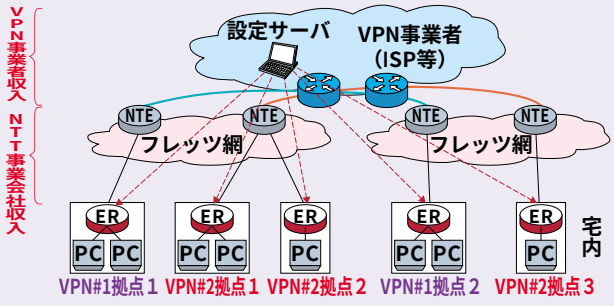

図３　フレッツ網上でのL2-VPNシステム適用時のサービス提供形態

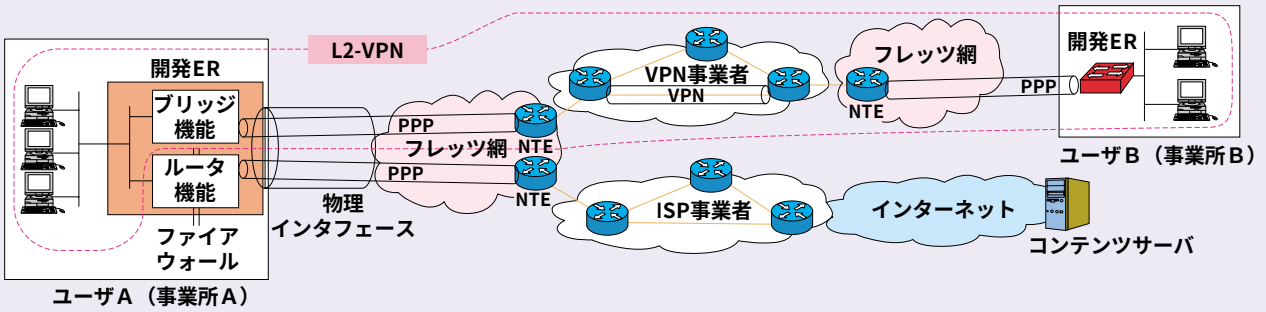

図4　L2-VPNとインターネットの同時接続の導入例

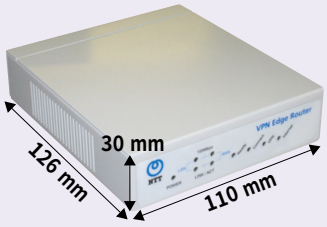

図5　ERの外観

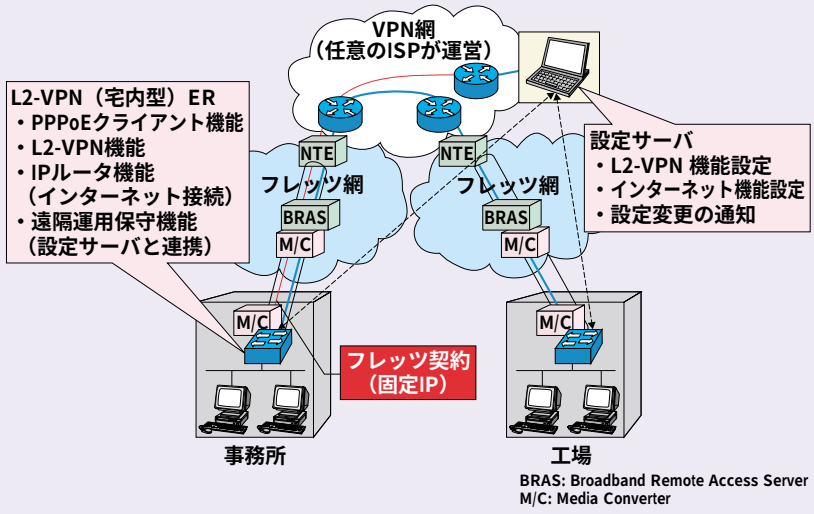

図6　サーバ設定方式の運用例

活用すると，一拠点だけインターネット接続を契約すれば，VPNを経由して他拠点のユーザもインターネットに接続することが可能となります．

なおインターネット接続を行うためにルータ機能とファイアウォール機能を内蔵し，インターネットからVPNへの不正アクセスに対するセキュリティを確保しています．

ERと設定サーバ

ERの外観を図5に示します．通常のブロードバンドルータと比較してもコンパクトで，宅内装置として適しています．設定サーバは，市販PC上に開発したアプリケーションソフトをインストールすることにより実現します．

ERの設定方法としては，直接設定方式とサーバ設定方式があります．直接設定方式は，LAN側の端末からTELNET接続によりERを設定します．サーバ設定方式は，設定サーバ上にERの設定条件を記述しておき，ERが起動時に設定サーバから設定データをダウンロードします．必要に応じ，設定サーバ側から強制的にダウンロードさせることも可能です．サーバ設定方式の運用例を図6に示します．サーバ設定方式を利用すれば，ユーザ設定や各種切り分け試験が，遠隔から一元的に実施可能となります．

今後の展開

IP-VPN上でイーサネット接続を提供することができる宅内用の小型ERおよび，ER設定を遠隔から一元管理できる設定サーバを開発しました．

これにより，中小企業/SOHO向けの安価なベストエフォート型広域イーサネットサービスを実現することができます．

実用化システムとしての開発は終了しましたが，運用性の向上やユーザインタフェースの改善等を図る事が残されている課題であると考えています．

（左から）斎藤　玲/ 宮本　正和/
首藤　晃一

従来のIP-VPNより設定が容易でアプリケーションの利用制限も少なく，VLAN-VPNよりも安価で多くのユーザを収容できるVPNシステムを実現したことにより，これまでVPNを利用されなかったユーザの市場開拓につながるものと期待しています．

◆問い合わせ先
NTTアクセスサービスシステム研究所
アクセスサービスネットワーク
アーキテクチャプロジェクト
TEL　043-211-2074
FAX　043-211-4577
E-mail　miyamoto@ansl.ntt.co.jp