VPN

稲西 克弥，寺井 大地
Katsuya AKINISHI，Daichi TERAI

1　はじめに

現在，多くの企業や家庭で LAN が構築されており，情報資産や周辺機器の共有，インターネット接続する際に一つの回線で複数端末からアクセスすることが可能となっている．しかし，遠隔地に複数拠点をもつ企業の場合，企業自身でネットワークを構築することは容易ではない．従来，企業の LAN 間に電気通信事業者が提供する専用線を導入する形態が一般的であったが，通信距離が長い場合には，コストが大きくかかってしまっていた．そこで設備投資を抑えるために，複数のユーザが共用するネットワークを仮想的に専用線のように利用する VPN（Virtual Private Network）という技術が用いられるようになった．本稿では VPN について述べる．

2　VPN

2.1　概要

VPN は拠点間を，電気通信事業者の閉域網やインターネット網を専用線のように，仮想化した中継網を介して行う通信である．中継網は物理的に他のユーザと共有しているために回線には他のデータが混在しているが，暗号化と認証，トンネリングを行うことで，理論的には専用線同様に秘匿な通信が可能である．暗号化により通信パケットの盗聴を防ぎ，認証によって接続相手を確認する．トンネリングによってパケットをカプセル化して，二拠点に回線を確立する．VPN は LAN 間の接続や，遠隔地の端末からリモートアクセスを行い，接続先の LAN 内にいるように振る舞える機能の実現に用いられる．なお，中継網として，電気通信事業者の閉域網を用いるものには IP-VPN があり，インターネットを用いるものはインターネット VPN と呼ばれる．

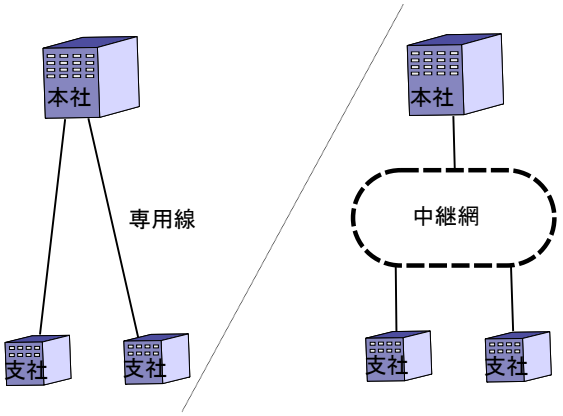

Fig.1　専用線と VPN

2.2　IP-VPN

電気通信事業者が持つ回線の内，IP 通信を行いインターネットから独立している閉域網を中継網に用いる VPN を IP-VPN という．IP-VPN は MPLS（Multi-Protocol Label Switching）技術をベースとして利用することで，中継網（MPLS 網）を構築する．MPLS はルーティングを IP ヘッダではなく，ラベルと呼ばれるもので行う手法である．顧客のルータ（CE）から，MPLS 網を構成するルータであるエッジルータ（LER）へと IP パケットを送信して，LER にて転送経路の情報をラベルに付加して，ラベルスイッチルータ（LSR）においてラベルを付け替え，パケットを転送していく．この際にラベルのみを見てルーティングを行うことが特徴である．このとき，CE は MPLS に関する仕組みを持つ必要はなく，通常のルータである．一例として，異なる CE がそれぞれ構成するネットワーク内に，同様の IP アドレスを持っていて，MPLS 網を介して重複している IP アドレス宛にパケット送信があった場合でも，MPLS では IP よりも下のレイヤであるために，他の CE のパケットと混線しない．なお，MPLS は暗号化の仕組みを持たないために，データ部分を暗号化する必要があり，通信の品質を維持するためにはルータの伝送速度と回線の使用率，中継するルータ数を適切にする必要がある．

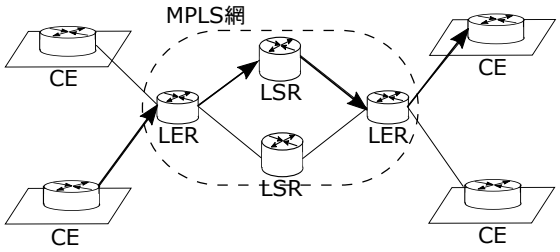

Fig.2　MPLS

2.3　インターネット VPN

中継網としてインターネット網を用いるインターネット VPN が普及している．実現手段の主要なものとして IPsec というプロトコルが用いられている．

IPsec は IP パケットを暗号化するカプセル化セキュリティペイロード（ESP）の機能を持つ．ESP は二つのモードを切り替えることができ，IP パケット全体を暗号化するトンネルモードと，データ部分だけを暗号化するトランスポートモードがある．トンネルモードは元の IP ヘッダを含むデータを IPsec で覆って暗号化し，新たにヘッダをつけるため，通信の内容が盗聴されることを

防ぐことが可能である．一方で，トランスポートモードは IP ヘッダをそのまま用いる．そのために通常，トンネルモードはゲートウェイ間の接続に利用して，トランスポートモードはホスト間の接続に利用する．

トランスポートモードを用いるプロトコルに L2TP/IPSec がある．L2TP（Layer 2 Tunneling Protocol）はリモートアクセスするために，トンネリングを行うプロトコルであり，それ自体が暗号化の仕組みを持っていないので，送信するデータを保護するために IPsec を用いている．

インターネットは不特定多数が利用して，かつ全体の管理者がいないために，セキュリティリスクが高く，さらに通信の帯域を明確に割り当てられているわけではないために，通信の品質の保証もされていないベストエフォート型のネットワークである．しかし，回線のコストが IP-VPN と比べても格段に安くなる，というメリットのために広く使用されている．

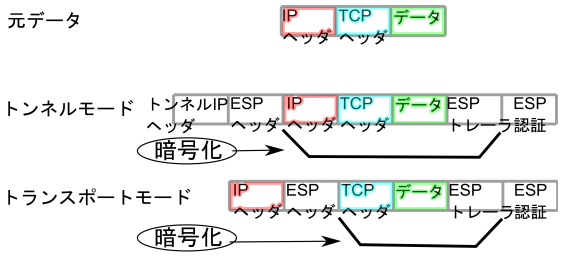

Fig.3　IPsec

3　導入における利点

専用線が拠点間の一対一の通信であるのに対して，VPN を用いた拠点間の通信は中継網を介して行われるために，ネットワークが簡単な構成になる．一例として福岡，大阪および東京との三つの拠点での通信を挙げる．専用線を利用する場合，福岡と大阪間，大阪と東京間に専用線を設置する必要がある．VPN を構築することにより福岡と東京間を大阪の拠点を介すことなく通信できる．つまり，中継網を中心としたフラットな構成になるために，耐障害性が向上する．さらに中継網を介すことで，広域ネットワークを構成するときに接続可能拠点を大幅に増やすことができる．

専用線を引くには距離が長いほどコストがかかるが，共用の回線を使用しているために距離に依存しない料金体系も実現できる．それによって広域なネットワークを構築する際には大幅なコストダウンが見込まれる．

4　導入事例

富士産業株式会社では本社と配送拠点，および営業所の間のデータ共有が可能となるように環境を整備し，通信コストを軽減するためにフレッツ・VPN ワイドという VPN の利用環境を 2009 年に導入した．専用線を利用していた従来のネットワークは月額利用料 174 万円（税別）ものコストがかかっていたのに対し，VPN を導入したことにより月額利用料 10 万 6,200 円（税別）と大きくコストが削減された．

5　今後の展望

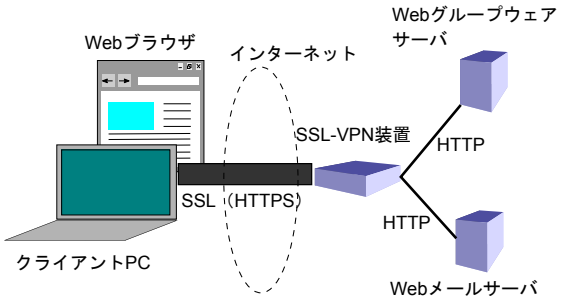

Fig.4　SSL-VPN

広域ネットワークの構築に関して，専用線から VPN へと需要が移る中，多くの LAN を結びつけたり，リモートアクセスをする機会が増えている．家庭用の無線ルータに VPN サーバ機能がついているものがすでにあり，さらに通信端末には VPN のクライアントとしての環境が整えられ，リモート操作できるものが増えると考えられる．VPN を実現するプロトコルが数多くある中，暗号化に SSL を活用した SSL-VPN がある．SSL-VPN は，インターネットでクライアントの使用しているアプリケーションが，HTTPS や POP over SSL といった SSL を利用している技術に対応している必要があるが，主な Web ブラウザやグループウェアはあらかじめ対応している．そのためにサーバが SSL-VPN 装置を用意すれば，クライアントとサーバの間に容易に VPN を構築できる．また，筑波大学大学院研究プロジェクトで SoftEther VPN という複数の VPN のプロトコルに対応している利用無料のオープンソースが配布されている．これにより高価なライセンス費用を支払う必要もない．以上より，VPN を使用するのにできるだけ専門的な知識を必要とせず，かつ費用も抑えられるようになってきていて、利用者を増やしていくと考えられる．

参考文献

1) 村嶋修一，ベテランが丁寧に教えてくれるネットワークの知識と実務，株式会社翔泳社，2007
2) 高田伸彦，南俊博，情報セキュリティ教科書，東京電機大学出版局，2008
3) NTT 東日本 導入事例 富士産業株式会社様 http://www.ntt-east.co.jp/business/case/2010/002/
4) 富士通 SSL-VPN 入門 http://fenics.fujitsu.com/products/ipcom/catalog/data/2/2.html
5) 筑波大学大学院研究プロジェクト SoftEther VPN https://ja.softether.org/