VPNサービス

コストエフェクティブなオフィス間ネットワーク

このコーナーは、注目の製品やサービスについて、それを支える技術や市場動向の解説(セミナー)と具体的な商品を紹介(展示)する、バーチャル展示会。今回のテーマは、機能、価格ともに多彩な選択肢がそろっているVPNサービスだ。基本的なVPNの種類と技術を理解して、最適なサービスを選択してほしい。

text：大神企画

VPNは専用線を使わないプライベートネットワーク

オフィスが1か所だけの企業の場合、社内にイーサネットによるLANを敷設すれば、それだけで全社ネットワークを構築したことになる。だが、大企業のほとんどは、全国に複数の支社、営業所、工場などを持っており、それらの拠点間を接続する専用回線がなければ、全社ネットワークを構築することはできない。しかし、専用回線は利用料が非常に高く、すべての拠点を専用回線で結んでいるような企業は、大企業の中でも非常に少ないのが現状だ。

このような専用回線の敷居の高さを解決し、中小企業でも拠点間を接続したプライベートなネットワークを構築できるのが、「VPN（仮想プライベートネットワーク）」だ。

社外であることを意識せず社内ネットワークへアクセス

VPNは、公衆回線を利用してプライベートネットワークを構築するための技術であり、大きく分けて2つの種類がある。1つはリモートアクセス型、もう1つは専用線型だ。

VPNが登場する以前、遠隔地の支社や営業所から本社のネットワークにアクセスするために用いられていたのがリモートアクセスだ。リモートアクセスでは、アナログ電話回線、ISDN、PHSなどを利用し、ダイヤルアップで社内ネットワークに接続する（図1）。しかし、リモートアクセスには、いくつかの課題がある。中でも最も問題になるのが通信費だ。ダイヤルアップでリモートアクセスサーバーにつなぐ場合、距離に応じた電話料金がかかる。特に拠点間の場合、その多くは高額な

図1　従来のリモートアクセス環境

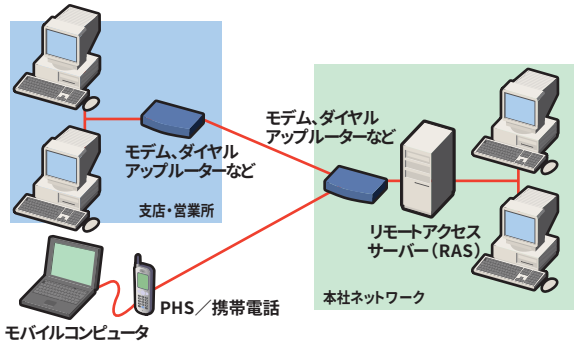
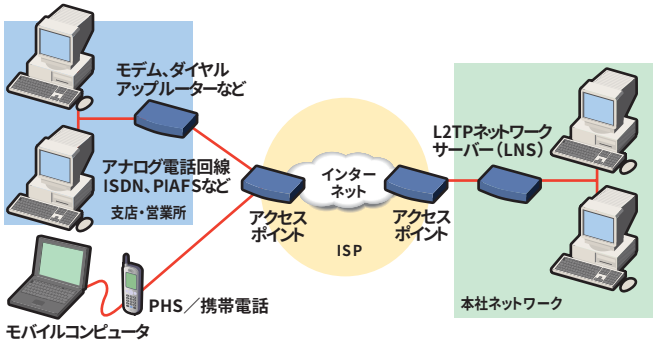


図2　リモートアクセス型のVPN



従来は、「ネットワークの物理的な距離＝コスト」であったが、その中継部分をインターネットで代用することで、低コスト化が実現した

つながるものが端末自体なのかネットワークなのかによる違いだけで、構造はリモートアクセス型VPNと同じ

図3　従来の専用線環境

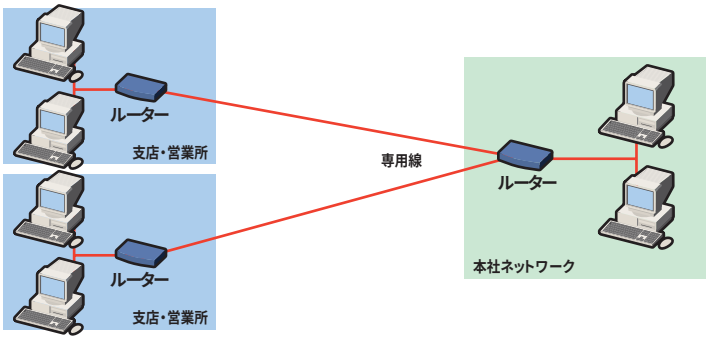
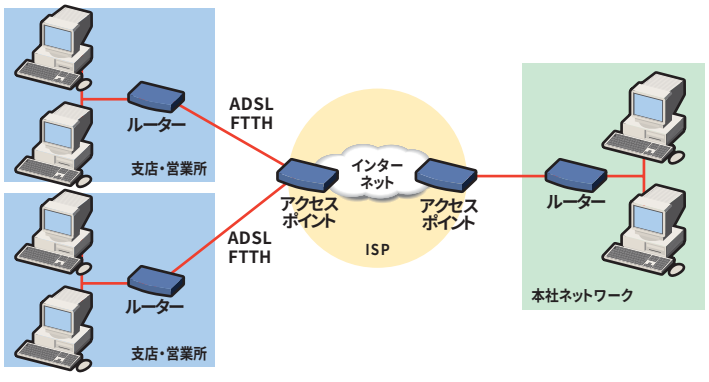


図4　専用線型VPN



市外通話料金であり、使用頻度が多ければ、専用線を敷設するのと同等かそれ以上のコストになる。また、リモートアクセスサーバーを立てた場合、同時接続数を多くすればするほど、導入と運用管理に関する手間やコストが膨れ上がるという問題もある。

この問題を避けるため、最も低料金の市内通話料金の区域内にあるISPのアクセスポイントにダイヤルアップし、社内ネットワーク側にはISPのアクセスポイントと結ぶルーターを設置して、アクセスポイント間はISPが提供するパブリックなネットワークを利用するのが「リモートアクセス型VPN」だ。遠隔地へ直接ダイヤルアップしないので、通信費を大幅にカットできることが最大の特徴になる（図2）。ISP側の設備を利用するので、同時接続数が増えても導入・運用管理コストに大きな影響はない。

専用線と同等のネットワーク環境を低コストで実現

これまで、拠点間のネットワークを常時接続するために利用されてきたのが専用線である（図3）。また、専用線よりも安価なフレームリレーというパケット通信網が用いられることもある。ただし、専用線は導入・運用コストが非常に高い。フレームリレーも登場した当初は専用線と比較して安くて速いものだったが、現在のブロードバンド環境と比べると帯域は狭く、決して安価とはいえない。そのため、多数の拠点間を専用線やフレームリレーで接続できるのは、一部の大企業に限られる。ただし、そういう大企業でも地方の数人規模の営業所にまで専用線を敷設することはまずない。

こうした専用線のコスト面の課題を解決するのが「専用線型VPN」である。専用線型VPNでは、一般のインターネット接続のようにネットワークからISPのアクセスポイントに常時接続するだけ（図4）。料金も、インターネットVPNを利用すると、ADSLやFTTHと変わらない。しかも、専用線では基本的に1対1の接続だが、VPNでは1対多の接続も容易だ。

ただし、ほとんどのVPNはIPベースで動作する。そのため、IP以外のプロトコルを利用する通信の場合、VPNではデータをやり取りできない。その場合は、広域イーサネットといった別の選択が必要になる。

機能とコストで異なる多様なVPNサービス

拠点間を結ぶのに公衆回線を利用するVPNは、通信事業者のクローズドなネットワークを利用する「IP-VPN」と、インターネットを利用する「インターネットVPN」に大別できる。

IP-VPNは、ISPがオールインワンのパッケージとしてVPNサービスを提供するもの。VPNルーターなどの機器構成がシンプルで、導入や運用管理が非常に容易だ（図5）。また、インターネットVPNと比べて無防備なインターネット回線に重要な情報を流

図5　IP-VPN

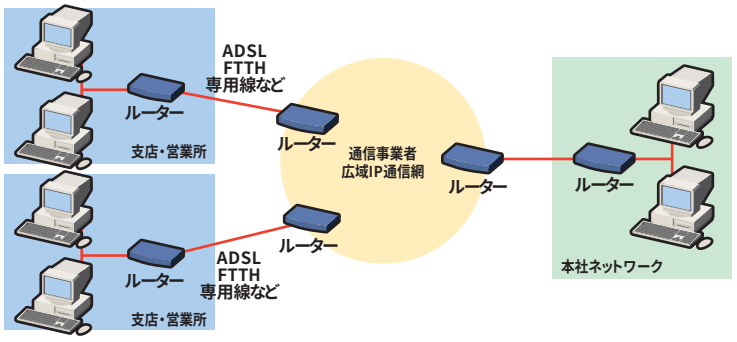
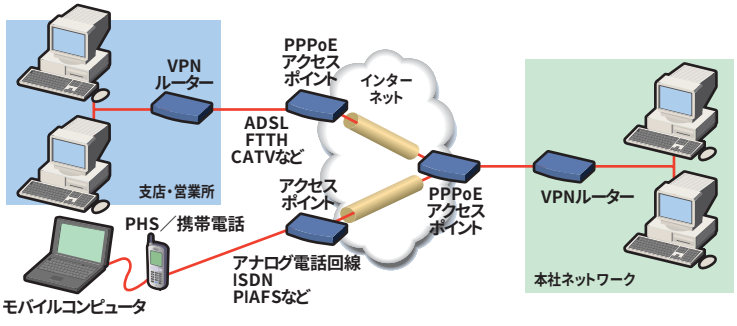


図6　インターネットVPN



IP-VPNとインターネットVPNの大きな違いは、経路が公衆網か閉域網かという点。コストの差もこの違いから生まれる

すことがないので、安全性も高いといえる。ただし、コスト的には専用線に比べると格段に安価だが、インターネット接続に比べると高い。さらに、IP-VPNを構築できるのは、ISPがカバーするエリアに限定されるという点も注意が必要だ。

一方、ブロードバンドの時代を迎えて回線料金が非常に廉価になったインターネットを中継回線に利用するのが「インターネットVPN」だ（図6）。IP-VPNで利用される広域IPネットワークよりもはるかに低料金のインターネット回線を利用するため、きわめて安価な料金になる。インターネットにつながるなら、あらゆる場所でVPNが構築できるのも特徴だ。

ただし、インターネットVPNには課題も多い。第一に、無防備なインターネットでは、社内ネットワークの通信をそのまま流してしまうと、データの盗聴や改ざんのおそれがある。また、インターネットVPNは機器構成が条件によって異なるので、導入や運用管理は容易ではない。しかし、そうしたデメリットは、インターネットVPNを実現するさまざまな技術によって克服され、現在ではVPNの主流になろうとしている。

また、この他にもTCP/IP以外のプロトコルを利用する場合の選択肢として考えられるのが「広域イーサネット」と呼ばれるもの。他のVPNがTCP/IPベースのネットワークであるのに対し、広域イーサネットでは名前のとおりイーサネットベースであるため、TCP/IPも含めてさまざまな通信プロトコルが利用できる。QoSが比較的高いといったメリットもある反面コストは高めで、利用できる地域も限定されている。ブリッジ技術などを使って接続にインターネット回線をうまく組み合わせるサービスも登場している。

インターネットVPNを支えるトンネリング技術

インターネットVPNを実現するネットワーク技術には、いくつかの種類がある。その中でも現在主流になっているのが、「L2TP」や「PPTP」、「IPsec」そして「SSL-VPN」などだ。L2TPやPPTPは、OSI参照モデルの第2層にあたるデータリンクレイヤーのパケットを、第3層にあたるネットワークレイヤーのIPプロトコルでカプセル化する。つまり、NetWareのIPXやウィンドウズネットワークのNetBEUIなど、IP以外のプロトコルもカプセル化して通信できる。これらは、主にリモートアクセス型VPNで利用されることが多い。

IPsecは、ネットワークレイヤーのIPプロトコルでセキュリティーを確保できるもの。認証ヘッダー（AH）や暗号ペイロード（ESP）をIPパケットに付加することで、高いセキュリティーを実現している。専用線型VPNではほとんどの場合、IPsecが用いられている。

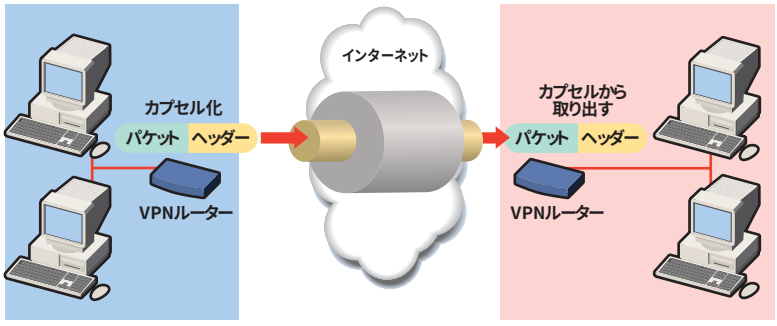
SSL-VPNは、主にウェブブラウザベースのリモートアクセスなどで用いられる。これは、第5層のセッションレイヤーに実装されるもので、IPsecがすべてのIPプロトコルをサポートするのに対し、HTTP、FTP、Telnet、POP3、SMTPなどトランスポートレイヤーでTCPを利用するアプリケーションのみがサポートされる（図7）。基本的に内部ネットワーク側にSSL-

図7　OSI参照モデルとVPNプロトコル

OSI参照モデル	VPNプロトコル
第7層　アプリケーションレイヤー	
第6層　プレゼンテーションレイヤー	
第5層　セッションレイヤー	SSL-VPN
第4層　トレンスポートレイヤー	
第3層　ネットワークレイヤー	IPsec
第2層　データリンクレイヤー	L2TP、PPTP、L2F
第1層　物理レイヤー	

どのプロトコルを使うかによって、利用できるアプリケーションが限定される。第3層にあるSSL-VPNでは第4層はTCPに限定される（UDPを使うアプリケーションは利用できない）。逆に第2層にあるL2TPなどでは、第3層以上であればIP以外も利用できる

図8　トンネリングのイメージ



トンネリングのイメージは、土管のような専用の道を作り出して、その中で通信を行うというもの

VPN装置があれば、クライアント側にはウェブブラウザがあればよく、運用管理の手間はかからない。そのため、限られたアプリケーションのみをやりとりする場合は、この方法が用いられることも多い。その手軽さから、ASPとして提供するサービスもあり、用途が合えば導入しやすいVPNサービスだといえる。

強固な暗号化と認証技術で構成されるIPsec

インターネットVPNを実現するいくつかの方法の中で、ネットワーク間の距離を意識せずにプライベートネットワークを構築できるのが、IPsecを利用するものだ。そのIPsecは、トンネリングと暗号化技術、認証技術によって構成される。

トンネリングは、IPパケットに新しいヘッダーを付加し、通信すること（図8）。新しいヘッダーを付けることをカプセル化という。そのカプセル化を行うのが、VPNルーターだ。データの送信元ネットワークにあるVPNルーターは、IPパケットを受け取るとそれを暗号化するとともに受信先ネットワークにあるVPNルーターを宛先とするヘッダーを付けて送信する。受け取ったVPNルーター側では、IPパケットを復号化するとともに本来の受信先コンピュータに向けてデータを送るという仕組みだ。

暗号化は、IPパケットのカプセル化の際に行われる。一般的には、共通鍵暗号方式と公開鍵暗号方式を組み合わせた方法が使われる。さらに、この鍵交換を行う際のVPNルーターの「なりすまし」を防止するために、認証技術が用いられる。認証は、PKI（Public Key Infrastructure）を利用したデジタル署名方式が使われることが多い。

インターネットVPNを利用するには

インターネットVPNを利用する場合、インターネット接続回線の種類は問わない。固定IPサービスを契約することで、一般家庭向けのADSLやFTTHを利用することも可能だ。ただし、IPsecによるインターネットVPN機能を持ったルーターなどの装置が必要になる。インターネットVPNで用いるVPNルーターは、設定の面でやや複雑な部分もあるが、最近ではVPNルーターの導入・保守・サポートとインターネット接続サービスをセットで提供する「マネージドVPN」と呼ばれるサービスも登場しているので、そうしたサービスを利用すると運用管理は楽になる。ただし、社内で運用管理が可能なら、自分でルーターを導入するほうが、低コストで高機能なネットワークを構築できる。どちらにするかは、VPNの利用目的によって考えるとよいだろう。

インターネットVPNは、1対多のセッションを張ることも自由自在にできる。価格面の優位性と複数拠点間を結べるメリットを活かすことで、これまで専用線を利用できなかった他店舗チェーン店展開を行っている企業、全国各地に小規模な支社、営業所を抱える企業などでも、内部ネットワークに容易にアクセスできるプライベートネットワークを構築できる。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp