特集2

費用対効果を高める最新＆適切なサービス選び

まるごとわかるVPN導入術

text：大澤文孝

VPNは、離れた拠点を仮想的に直結したように見せかける技術だ。VPNを利用すると、低コストで拠点間のLANを接続したり、社内のLANにインターネットで接続して社内のサーバーを遠隔操作で利用したりできるようになる。近年は、回線事業者やプロバイダーがVPNの導入や保守も含めたサービスを提供しているので、導入は容易だ。むしろサービスが多品種にわたるため、目的に合ったVPNサービスを選ぶのが活用のポイントとなる。

ブロードバンドの普及で一層拡大するVPN利用の背景

支社がいくつかある企業では、各支社に構築したLAN同士をつなぎ、全国どこでもLANと同様にセキュアーで閉じたネットワークを構成したいという要望がある。支社間を接続するネットワークは「WAN」(Wide Area Network)と呼ばれる。そして、WANを構成するのに使われるのが、NTTが提供する「ディジタルアクセス」やパケット通信方式のフレームリレー、ATM(非同期転送モード)を使った専用線だ。

また近年は、かならずしも社内で仕事をするという形態ではなく、外出先や自宅から社内のサーバーに接続したいという場面も多い。その要望を叶えるのが、リモートアクセスだ。リモートアクセスを提供するには、社内にPPP(Point to Point Protocol)サーバーとモデムやターミナルアダプター(TA)を設置し、社外からPPP接続ができるようにすればいい。

しかしこれらの方法は、コストが高くつ

VPNの役割その❶

本社と支社や拠点間を結ぶ「事業所間VPN」

事業所間VPNは、サービス事業者が用意したVPN網を使って拠点間を結ぶものだ。接続した拠点同士が、あたかも同一のLANに接続されているように見える。

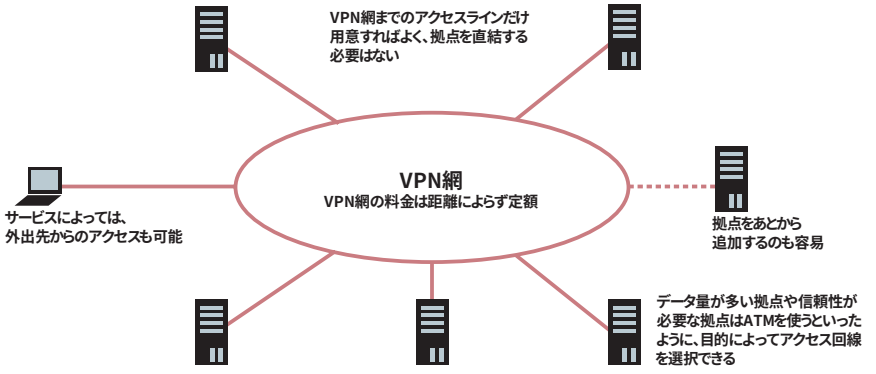
通信途中では、同じ網内を複数の企業が利用するため、他企業のデータと混在するが、データの振り分けや暗号化によって機密は守られるので、盗聴の心配はない。

事業所間VPNを構築するには、VPN網と各拠点とを適当なアクセスラインで接続する。多くの場合、VPN網内は距離を問わず、通信速度(帯域)で料金(初期費用・月額費用)が決定する。このため、拠点間が遠くても、月々の料金は「VPN網の利用料＋VPN網と拠点とを接続するアクセスラインの利用料」となる(詳細は124ページ参照)。

アクセスラインは自由に選べることが多いため、信頼性が必要な場合にはATMで、価格を重視する場合にはFTTHやADSLでといったように、用途によってアクセスラインを選択できるのも魅力だ。サービスによっては、電話回線やPHS網などを使ったモバイル環境からの接続もサポートする。

事業所間VPNでは、拠点間をそのまま接続するため、各拠点が安全であるということが前提だ。たとえば拠点の1か所に不正な侵入やウイルスの感染があると、すべての拠点が危険な状態となる。事業所間VPNを導入する場合には、各拠点のLANのセキュリティーに注意し、より安全に運用するには、VPNへの接続の直前にファイアーウォールを導入すべきだ。

■事業所間VPNによるネットワークの構築

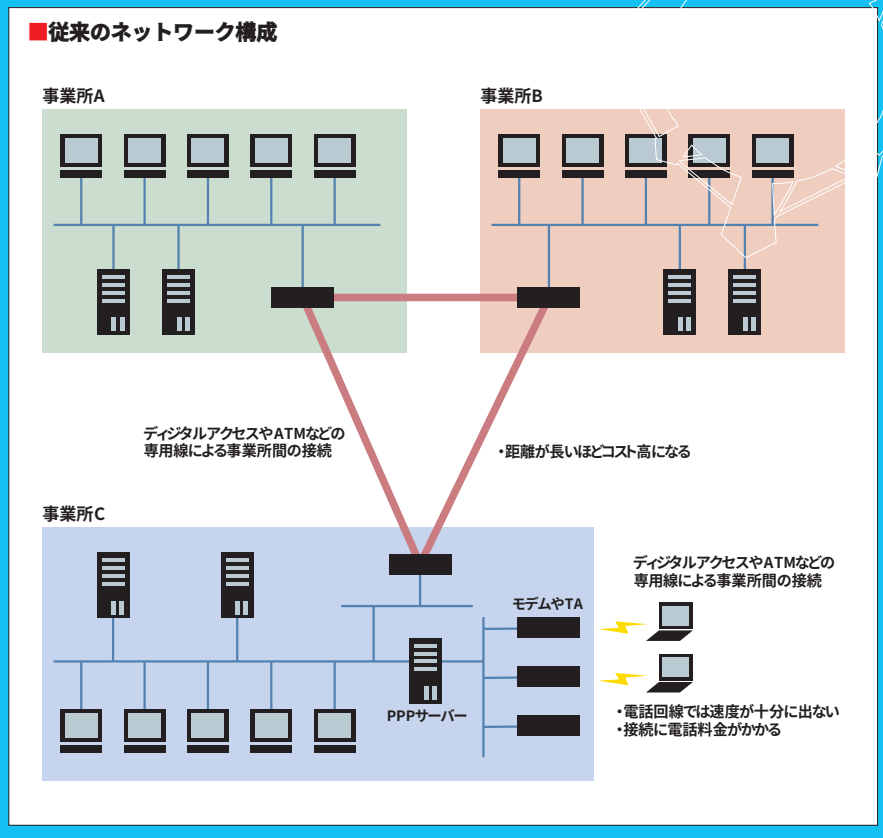


くものが多く、十分な速度が出ない点が問題だ。たとえば専用線は、速度はもちろん、距離によって価格が大きく異なる。このため、拠点間の距離が遠いほど、コスト高となってしまう。さらに、近年はリモートアクセスでも扱うデータ量が多いため、モデム(最大56kbps)やTA(最大128kbps)の通信速度では十分とは言えない。そこで専用線や電話回線に替わって使われるのがVPN(Virtual Private Network)だ。

VPNは、サービス事業者が用意する複数の企業で共有する回線やインターネットを利用し、暗号化して通信することで、あたかもLAN同士や、LANとクライアントが直結しているように見せかける技術だ。

VPNの最大のメリットは、拠点間を専用線で直結したり外出先からダイアルアップで接続したりするのに比べて低コストで実現できる点にある。特にインターネットを利用したVPNの場合、ADSLやFTTHなどの安価なインターネット回線を使うことで、低価格で高速な接続を実現できる。

■従来のネットワーク構成



VPNの役割その❷

社外から会社のLANに接続する「リモートアクセスVPN」

リモートアクセスVPNは、社外からインターネットを通じて社内LANに入り込めるようにするVPNだ。リモートアクセスVPNは、事業所間VPNと違い、ネットワークと1台のクライアントとを接続する。

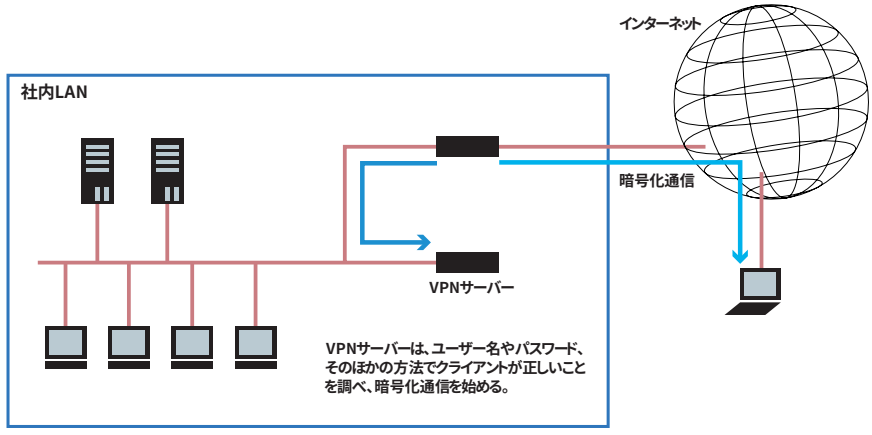
当然、インターネットからは不正なアクセスもあるので、正しいクライアントであるかどうかを認証する必要がある。クライアントの認証方式は、ユーザー名とパスワードを使う簡単なものから、ワンタイムパスワードやICカード、クライアント証明書を使うものまで、方法はさまざまだ。

もちろんインターネットではデータの盗聴の可能性もあるので、通信の暗号化も欠かせない。

リモートアクセスVPNを使う場合は、社内にVPNサーバー(またはVPNルーター)を用意する。VPNサーバーは、クライアントを認証し、不正なクライアントでなければ、暗号化通信を始める。

リモートアクセスVPNは、正しいクライアントであると識別されれば、どこからでも社内LANに入り込めるため、セキュリティーの確保も課題となる。クライアントのパスワードが漏洩すると、誰でも社内LANに入ることができてしまう。このためリモートアクセスVPNを導入する場合には、VPNサーバーのログを定期的に監査するなど、適切な保守運用が不可欠だ。

■リモートアクセスVPNによるネットワークの構築



専用線より速くて安い！

IP-VPNと広域イーサネット

拠点間を接続するVPN網には、通信事業者が提供するIP-VPNや広域イーサネットがある。専用線に比べて安価なうえに、インターネットとは別のネットワーク網のため、帯域を細かく設定でき、経路上の切断などのトラブルも少ない。

専用線に取って代わるVPNは価格・帯域・信頼性で選ぶ

拠点間をネットワークで接続するときには、VPNの利用を検討したい。

VPNの最大のメリットは、何と言ってもコストの削減効果だ。VPNを使えば、拠点間を専用線で直結する必要がないため、拠点間が長距離なほど、コスト削減のメリットが大きくなる。近年は企業のインフラに対するコスト削減の意識が高く、専用線からVPNに変更する事例が増えている。

しかしながら、専用線が必要となる場面では、重要なデータを運ぶことも多く、単に価格の安さを求めてVPNにするわけにもいかない。

VPNは、「IP-VPN」「広域イーサネット」「インターネットVPN」の3つに分類できる。それぞれ特徴があり、価格、帯域、信頼性が異なる。このため、VPNを選ぶ場合には、目的に合ったサービスを選ぶのが重要だ。

TCP/IPネットワークで他のLANとも相互接続がしやすい「IP-VPN」

IP-VPNは、サービス事業者によって構築された、仮想的なTCP/IPネットワークだ。IP-VPNでは、一般的なIPルーターを使ってVPN網に接続する（VPN対応ルーターである必要はない）。利用するIPアドレスは任意のもので構わない。

IP-VPN網へのアクセスラインは、ATMのほか、ADSLやFTTH、イーサネットなどの回線網を利用でき、これら多様なプランをサービス事業者は提供している。もちろん、複数を組み合わせる方法もあり、たとえば本社にはATMを使い、支社にはADSLを使うといったことも可能だ。

IP-VPNの料金体系（月額利用料）は、「アクセスラインの利用料＋IP-VPN網の利用料」となる。

このうち、アクセスラインの利用料は、IP-VPN網に接続するためにNTT東西などのラストワンマイルを提供する事業者に支払う料金だ。そして、IP-VPN網の利用料は、IP-VPNを提供する事業者に支払う料金で、アクセスラインの種類と速度によってのみ決定する。このため、拠点が近い場合も遠い場合も、アクセスラインの種類や速度が同じであれば、同一料金だ。

IP-VPNの初期費用は、ほとんどがアクセスライン敷設のための費用だ。たとえば、ATMの場合には数十万円の費用がかかるが、ADSLの場合には数千円から数万円で済む。なお、アクセスラインの種類によっては、契約期間が1年以上などと決められており、途中で解約できないこともあるので事前によく調査したい。

≫事業所間VPNに求められるもの

- 安定性
- 速度（スループット）
- 価格の安さ

■事業所間VPNサービスの比較

	IP-VPN	広域イーサネット	インターネットVPN
利用範囲・対象	拠点が全国各地にまばらに分散しており、拠点ごとに必要な通信速度や信頼性がまちまち	遠距離でMbps単位の通信が必要な拠点間の接続。同一都道府県での通信料が多い	既存のインターネットへの接続回線を利用して安価に拠点間を接続したい
メリット	距離にかかわらずVPN網内の料金は一定。VoIPなどのTCP/IPの付加サービスを提供するものもある	高速な通信が可能。高速な帯域を必要とする場合には、他のサービスに比べて安価。ゾーン分けされた料金体系により同一ゾーン内の通信が安価	安価。インターネットにさえ接続できれば、国内国外問わず、どこでも接続可能
デメリット	やや高価。TCP/IPでの通信のみ	速度が低い場合には割高	帯域保証や品質確保が難しい
通信プロトコル	TCP/IPのみ	TCP/IP以外もOK	TCP/IPのみ
セキュリティー	高い	高い	機器を正しく設定すれば高い
イニシャルコスト	アクセスラインの敷設料	アクセスラインの敷設料	—
	IP-VPN網の初期費用	広域イーサネットの初期費用	プロバイダーのVPNサービスの場合には、初期設定導入費用およびコンサルティング費用
	IPルーターの購入費用（レンタルの場合は不要）	メディアコンバーターの費用	VPNルーターの購入費用（レンタルの場合は不要）
運用コスト*1	アクセスラインの利用料	アクセスラインの利用料	アクセスラインの利用料
	IP-VPN網の利用料	ゾーン内通信利用料	インターネット接続料金
	—	ゾーン間通信利用料	機器レンタル費を含む月額料金
導入方法	IPルーターで接続	イーサネットで直結	VPNルーターにより接続
主なサービス	KDDI IP-VPN（KDDI）	KDDI Ether-VPN（KDDI）	126ページ参照
	Arcstar IP-VPN（NTTコミュニケーションズ）	e-VLAN（NTTコミュニケーションズ）	
	Powered-IP MPLS（パワードコム）	Powered-Ethernet（パワードコム）	

*1 別途、配線設備使用料と回線接続装置使用料、イーサ終端装置使用料などがかかる

オプションとしてVoIPによるIP電話サービスを提供しているIP-VPNサービスもある。このため、事業所間の通話を安くするために段階を踏んでIP電話を導入したい場合にも構築が容易だ。拠点間の通話を無料に(または内線化)するだけでなく、社外に電話を掛けるときも相手先からもっとも近い拠点を経由して発信できる。

またIP-VPNはIPプロトコルによる接続のため、事業所間だけでなく他の企業のLANとも相互接続しやすく、エクストラネットを構成する基幹網としても活用できる。

通信プロトコルを問わず高速な通信に適す「広域イーサネット」

広域イーサネットは、イーサネットを社内に引き込んで拠点間を接続するサービスだ。TCP/IPだけでなく、NetBEUIやAppleTalkなどのプロトコルも通せる。

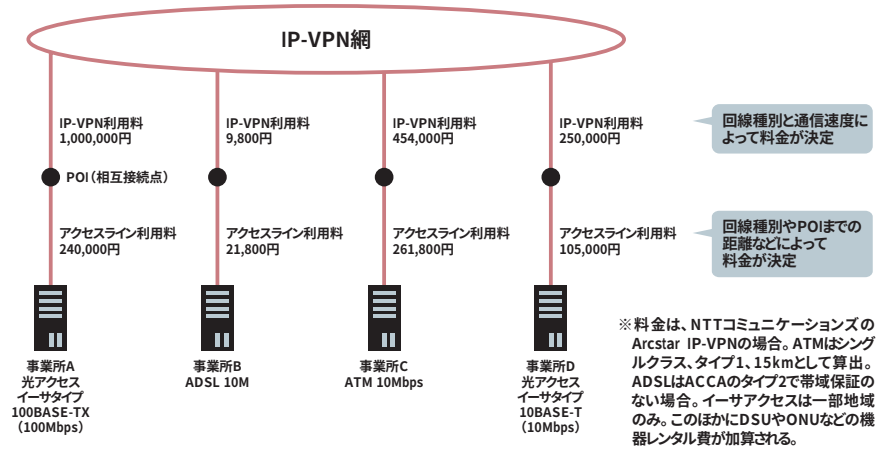
アクセスラインは光ケーブルを用いて直接引き込むのが主流だ。しかしサービスによっては、ATMやADSLなども利用できる。いずれのアクセスラインでも、メディアコンバーターによって最終的にイーサネットに変換されて提供される。このため、イーサネットケーブルを差し込むだけで拠点を接続でき、拠点間はまさにLAN感覚だ。

広域イーサネットの料金体系は、サービス事業者によって異なるが、多くの場合、都道府県などでゾーン分けされ、「ゾーン内通信」と「ゾーン間通信」とで料金が分類される。

月額料金の総額は、「アクセスラインの利用料＋ゾーン内通信の利用料＋ゾーン間通信の利用料」となる。このうち、アクセスラインの料金は、あくまで足回りに利用するため、IP-VPNの場合と同じ額だ。初期費用もIP-VPNと同様だが、メディアコンバーターが必要なため、その設置費用が数万円かかる。

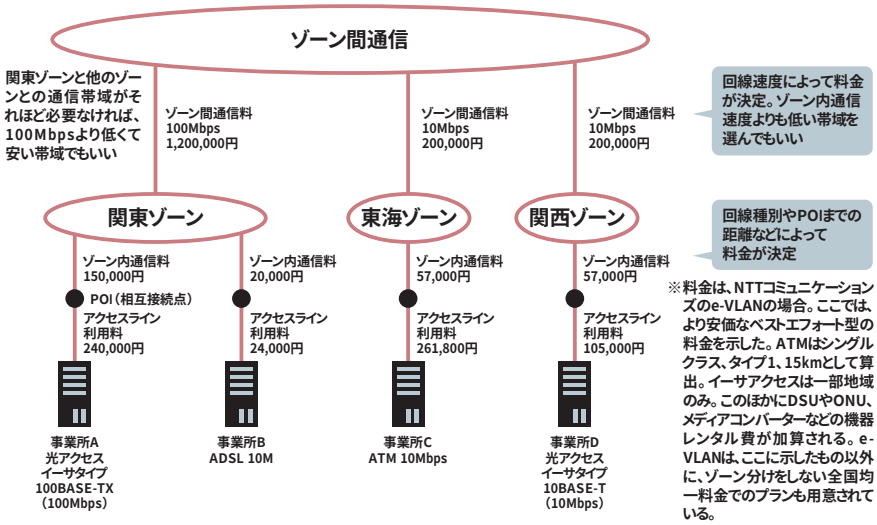
特徴的なのは、ゾーン内通信がゾーン間通信に比べて安価に設定されているという点だ。また、ゾーン間料金はアクセスラインがいくつあっても各ゾーンごとの料金は帯域によって固定で変わらないため、同一ゾーン内に多数の拠点がある場合には得になる。

■IP-VPNサービスの料金設定(ランニングコスト)



※料金は、NTTコミュニケーションズのArcstar IP-VPNの場合。ATMはシングルクラス、タイプ1、15kmとして算出。ADSLはACCAのタイプ2で帯域保証のない場合。イーサアクセスは一部地域のみ。このほかにDSUやONUなどの機器レンタル費が加算される。

■広域イーサネットサービスの料金設定(ランニングコスト)



※料金は、NTTコミュニケーションズのe-VLANの場合。ここでは、より安価なベストエフォート型の料金を示した。ATMはシングルクラス、タイプ1、15kmとして算出。イーサアクセスは一部地域のみ。このほかにDSUやONU、メディアコンバーターなどの機器レンタル費が加算される。e-VLANは、ここに示したもの以外に、ゾーン分けをしない全国均一料金でのプランも用意されている。

IP-VPNと広域イーサネットの違いと導入のポイント

IP-VPNと広域イーサネットの違いは、IPで通信するのか、イーサネットで通信するのかの違いだ。品質や速度の差はほとんどないので、どちらを利用してもいい。ただし、速度ではなく遅延で考えた場合、巨大なIP-VPN網だと内部のルーティングによって遅延が生じやすくなる可能性があり、VoIPなどリアルタイム性を必要とする場面では、広域イーサネットのほうがやや有利だ。

それ以外の機能では、広域イーサネットを使ってTCP/IPで通信すれば、結果はIP-VPNと同じであるから、コストの差によってどちらを使うかを決めることになるだろう。

IP-VPNは拠点の場所によらず料金が一定なのに対し、広域イーサネットにはゾーンによる料金設定がある。よって、接続したい拠点の位置関係や要求する速度によって、どちらが適するのかが異なってくる。

ちなみにIP-VPNや広域イーサネットには、帯域保証型のサービスとベストエフォート型のサービスの2種類があり、用途に応じて選ぶことになる。一般に長距離で高速な通信が必要な場合には広域イーサネットが安く、そうでない場合にはIP-VPNが安いと言われる。しかし、サービス事業者によっても価格体系がかなり異なるので、一概にそうとも言えず、いくつかの見積もりを取り寄せることが重要だ。また、広域イーサネットが提供される地域は、現在は都心部に限られているため、地域によってはIP-VPNしか選択肢がないケースもある。

なお、広域イーサネットサービスの中には、オプションでIP-VPNとの相互接続をサポートしているものもある。よって、必要があれば、IP-VPNと広域イーサネットを併用したネットワーク構築も可能だ。

VPNルーターさえあれば自前も可能

インターネットVPN

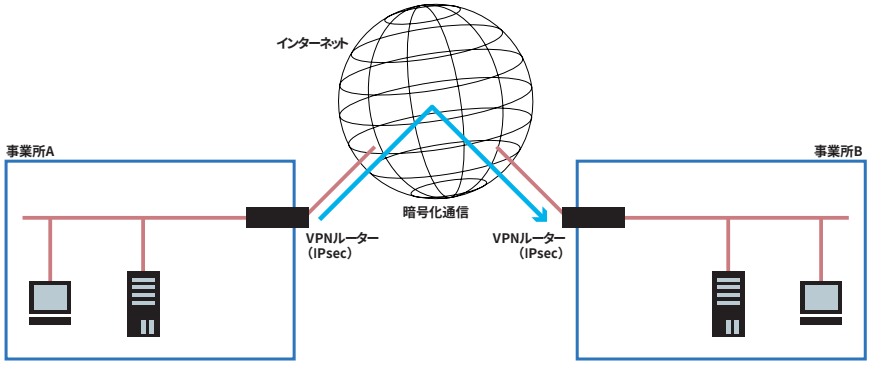
インターネットVPNは、インターネット内を暗号化して通信することでVPNを構築する技術だ。安価に構築できるだけでなく新たな回線の敷設が容易なため、取引先の社内や社員の自宅、モバイル環境など、VPNを柔軟に構成できる。

インターネット回線を利用して導入が容易な「インターネットVPN」

インターネットVPNは、拠点間の接続にインターネットを利用する。このため、既存のインターネット回線を使って、安価にVPNを構築できる。宅内工事も不要で、導入も手軽だ。インターネットに接続さえされていればよく、国内国外問わず、どことでもVPN接続できる。

インターネットVPNを構成するには、各拠点にVPNルーターを設置する。すると、VPNルーター同士が暗号化通信を始め、仮想的な回線網ができる。暗号化された回線網の中を送受信するデータが通ることで、盗聴の危険なく安全にデータを届けられる。暗号化の方式は、いくつかあるが、もっともよく使われているのはIPsecだ。

■インターネットVPNの概要



拠点同士を暗号化して接続する。拠点はインターネットと接続されていれば、どこでもいい。
接続した拠点同士は、あたかも同一ネットワークに存在するかのように見える。

≫インターネットVPN導入に必要な要素

- VPNルーターの相互接続性、速度、ファイアーウォール機能、管理機能
- インターネットへのアクセス回線の障害への対処
- 保守運用まで含めた担当者の選定

■インターネットVPNサービスを提供する主なプロバイダー・通信事業者

プロバイダー・通信事業者／サービス名 URL	初期費用 *1 月額費用 *1 提供するVPNルーター	レンタル	売切	センドバック *2	オンサイト保守	リモートアクセスVPN対応	24時間監視
bit-drive「DigitalGate VPNプラス」 http://www.bit-drive.ne.jp/vpn/	別途見積 5,800円～ DigitalGate、Century Systems（XR-410）	○	-	-	○	○	-
DTI「M-plus！ VPN」 http://magic.dti.ad.jp/vpn/	150,000円～ 7,900円～ NetScreen（5GT/5XT/25/50/204/208）	○	○	-	○	○	○
InfoSphere「InfoSphere IP インターネットVPNソリューション」 http://www.sphere.ne.jp/i-vpn/	55,000円～ 3,500円～ FutureNet（XR-1000/XR-440/XR-410）	○	-	-	○	-	-
KCOM「インターネットVPNサービス」 http://security.kcom.ne.jp/vpn.html	170,000円～ 90,000円～ NetScreen（5XP/5XT/25/50/204）	○	-	-	○	-	○
KDDI「インターネットVPNパッケージ」 http://www.kddi.com/business/internet/internet_vpn/	別途見積 別途見積 FITELnet、NetScreen、ヤマハ（RTX1000/RTX2000）	○	○	○	○	-	○
NTT東日本「インターネットVPNソリューション」 http://www.ntt-east.co.jp/ced/solution/plan/vpn/	別途見積 別途見積 Webport BR410VPN	応相談	○	-	○	-	-
NTT西日本「VPNextインターネットVPNソリューション」 http://www.ntt-west.co.jp/collection/solution/management/vpnext.html	別途見積 別途見積 相談のうえで決定	応相談	○	-	○	○	-
OCN「OCNビジネスパックVPN」 http://www.ocn.ne.jp/business/vpn/biz/	別途見積 5,900円～ ヤマハ（RTX1000）、NetScreen（5XT/25/50/204）、MUCHO-EV/PK	○	-	○	○	○	-
ODN「ODN-Biz マネージドVPN」 http://www.japan-telecom.co.jp/business/odn/vpn/	別途見積 別途見積 ノーテルネットワークスContivity	○	-	-	○	応相談	-
パワードコム「Powered VPN-I」 http://www.poweredcom.net/service/vpn-i/	別途見積 別途見積 NetScreen（5GT/5XT/25/50/204）	○	-	-	○	○	○
So-net「インターネットVPNサービス」 http://www.so-net.ne.jp/business/access/vpn/	50,000円～ 7,600円～ NetScreen（5GT/5XT）	○	-	○	応相談	○	○
SANNET「インターネットVPNサービス」 http://www.sannet.ne.jp/biz/VPN/	別途見積 8,500円～ NetScreen（5GT/5XT/25/50/204）	○	-	○	○	-	-
VECTANT「インターネットVPN type-R」 http://www.vectant.co.jp/svc_c/prv/prv_vpn_r01.html	36,000円～ 6,000円～ ヤマハ（RT105e/RTX1000/RTX2000）	○	○	○	○	-	○
XePhion「インターネットVPNサービス」 http://wakwak.com/evpn/	71,500円 12,800円～ NetScreen（5XP）	○	-	○	-	-	-

*1 費用は基本的に機器レンタルの場合
*2 機器先出し保守

固定IPアドレスを持つ環境なら インターネットVPNを構築できる

IPsecを使う場合には、インターネットとの接続で固定IPアドレスが割り当てられているのが望ましい。少なくとも、相互に接続する拠点の一方が固定IPアドレスでないと、割り当てられるIPアドレスが変化するたびにルーターの設定を変更しなければならなくなる。

固定IPアドレスを持つ環境なら、VPNルーターを導入することで、すぐにでもVPNを構築できる。また、LinuxやFreeBSD、Windows Server 2003などのサーバーOSは、IPsecで通信できる機能を備えているので、これらのOSがインストールされたサーバーを使ってVPNで接続することも可能だ。

なお、IPsecにはいくつかの暗号化および認証方式があるため、VPNルーターのメーカーが違うと相互に接続できないことがある。同じメーカー製のルーターにするか相互接続が確認されている製品を選ぶかすると安心だ。

よく使われるVPNルーターとしては、NetScreenがある。NetScreenは事業所間VPNを構築するだけでなく、クライアントにNetScreen Remoteというソフトウェアを導入し、リモートアクセスVPNとしても接続できる。

インターネットVPNのデメリットは 帯域確保と安定性の欠如

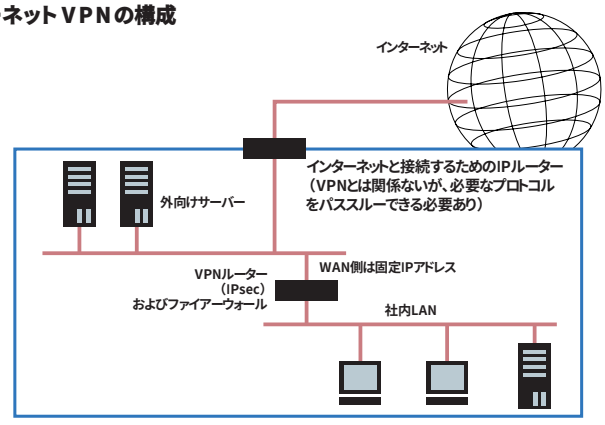
インターネットVPNは安価にどこでも構築できるというメリットがある反面、デメリットも多い。デメリットの最たるものは、帯域確保と安定性だ。

インターネットVPNでは、データがインターネットを通るため、あくまでベストエフォート型の回線であり、帯域の保証はできない。それに途中の回線断などでデータが失われてしまう可能性もある。

したがってインターネットVPNは、リアルタイム性が要求されるデータの送信や確実に相手に届けなければならないデータの送信には向かない。つまりインターネットVPNは、24時間常時接続が保証されているわけではないので、現状の専用線と同等の品質を求めてはいけない。

インターネットでのトラブルがあれば、拠点間との接続が数分～1時間程度停止することもありうる。よって、安価なのだから、ある程度の障害は許容するという寛容な使い方が求められる。

■インターネットVPNの構成



■インターネットVPNに適したIPsec対応ルーター

	NetScreen-5GT	RTX1000	IX3010
メーカー名	NetScreen	ヤマハ	NEC
価格	114,000円（10ユーザー版）	118,000円	338,000円
VPNセッション数	10	30	512
VPN時の通信速度	20Mbps	55Mbps	100Mbps
備考	VPNのほか、ファイアーウォール機能も備えた総合ルーター。DMZ機能も備え、サーバー公開環境にも向く。プロバイダーが提供するインターネットVPNで、レンタルVPNルーターとして採用される例も多い	中規模なインターネット接続に向く。障害時のISDN迂回に対応。通常のルーター機能も豊富であるため、既存のルーターを置き換えてVPNに対応させる場合に適す。IPv6にも対応する	大規模なセンター側の利用に向く。電源の冗長化、障害時のISDN迂回に対応。IPv6にも対応。拡張スロットによって、専用線、ISDN-PRIなどのさまざまなアクセス回線にも対応する

機器設置から保守運用まで一括提供のインターネットVPNサービス

VPNルーターを使ってインターネットVPNを構築するには、それぞれのVPNルーターに対して、「接続先のVPNルーターのIPアドレス」「接続したときのVPN網で通信に利用するIPアドレス（プライベートIPアドレス）」を設定するだけでいい。

ただし、2か所を相互に接続するのではなく、複数拠点を接続する場合には、ルーティングの設定をする必要がある。またVPNルーターのほとんどは、QoS（Quality of Service）機能によって帯域制限をかけることができる。しかし、帯域制限などの高度な機能を使う場合には、設定が難しくなりがちだ。また、接続したLAN同士は何も制限しなければすべての通信が透過するので、安全を保つためにいくつかの通信を制限するファイアーウォールを構築したほうがいい場面もある。

もちろん、VPNは相手先と常時接続することを目的とするものだから、回線断が発生したときに迅速に復帰できるトラブル対策や不正侵入の防御を確認する保守運用も必要だ。

近年は、プロバイダーや通信事業者が設定済みのVPNルーターを貸し出したり、インターネットVPNのコンサルティングを行うメニューを用意したりしている。

複数の拠点を接続する場合や、基幹としてVPNを導入する場合には、プロバイダーや通信事業者が提供するインターネットVPNサービスを利用したほうがいい。というのは、拠点のどこにデータが集中するのかによって、アクセスラインのどこを増速しなければならないのか、どこに帯域制限をかける必要があるのかなど、いくつかのノウハウを持つためだ。もちろん、これらのインターネットVPNサービスでは、導入時の面倒がなくなるだけでなく保守運用まで任せてしまえるため（サービスプランにより保守内容は異なる）、トラブルが発生したときの対処の安心感も強い。

外出先でも仕事をこなせる

IPsec-VPNとSSL-VPN

リモートアクセスVPNを使うと、インターネットから社内LANにアクセスできるようになる。リモートアクセスVPNは便利な反面、インターネットからのアクセスを許すことになるので、万全なセキュリティーの管理体制が求められる。

リモートアクセスVPNで どこでも仕事のできる環境作り

社員が外出先や自宅などから会社のサーバーにアクセスしたいという要求は多い。このような場合、従来はモデムを使って接続していた。これがRAS（Remote Access Service）接続だ。しかしモデムは最大通信速度が56kbpsと低速なのが難点だ。また、社内にも電話回線とモデムを用意する必要があり、維持運用コストもかかる。

そこでモデムに取って代わって利用されるのが、インターネットを通じて社内のサーバーに接続するリモートアクセスVPNだ。リモートアクセスVPNを構築すれば、社員（クライアント）はいつも使っているインターネット回線を使って社内にアクセスでき、ADSLやFTTHなどであれば高速かつ安価なリモート接続を実現できる。リモートアクセスは、下記の表のようにいくつかの方式がある。クライアントの種類と接続形態によって、適したものを選ぶのがポイントだ。

仮想ネットワーク型と 代理アクセス型の違い

リモートアクセスVPNは、仮想ネットワークを構成するものと、代理でアクセスをするものの2種類に分かれる。

仮想ネットワーク型では、社内で使われているIPアドレスをクライアントに割り当て、そのIPアドレスを使ってアクセスさせる。この方式をとる通信プロトコルには、IPsec、PPTP、L2TPなどがある。

仮想ネットワーク型では、接続してきたクライアントが、まるで社内にいるかのように見える。またアプリケーションの種類を問わず、すべてのTCP/IPデータが通る。

一方の代理アクセス型では、クライアントからの通信をVPNサーバーが受け取り、VPNサーバーが実際の相手先に代理でアクセスし、その結果をクライアントに届ける。この方式をとるものには、後述するSSL-VPNや、SSHの暗号化技術を使って特定のポートに送られたデータを相手先のコンピュータの特定ポートに転送するポートフォワードなどがある。

代理アクセス型では、接続先はクライアントが接続してきたのではなく、VPNサーバーが接続してきたかのように見える。また、すべてのデータが通るわけではなく、VPNサーバーが通信を代理できるものだけに限られる。

≫リモートアクセスVPNに求められるもの

- 安全性
- クライアント側の設定の容易さ
- 通信の透過性
- クライアントOSの非依存性

リモートアクセスVPN構築の 注意点

リモートアクセスVPNは、クライアントがアクセスするので、クライアント側の設定が簡単でないと導入や保守が難しくなる。たとえば、IPsecでVPNを構築する場合には、クライアントとなる社員宅にそれぞれ適切に設定したVPNルーターを設置する必要

■リモートアクセスVPNの比較

	RAS	PPTP	IPsec-VPN	SSL-VPN
接続方式	仮想ネットワーク型	仮想ネットワーク型	仮想ネットワーク型	代理アクセス型
メリット	インターネットではなくモデムを使うので、第三者が侵入する余地が少ない。さらに安全にしたいならば、着信後にコールバックすることで、拠点の確認もできる	ウィンドウズの場合、標準でサポートされているため、導入が容易	インターネットVPNと同じ方式をとれるので混在が容易	必要なデータだけを中継でき、不正なデータの排除が容易。ユーザーの識別方法として多様なものが用意されている。ブラウザーさえあればアクセスできる
デメリット	電話代がかかる。モデムが必要。低速	ウィンドウズ以外からのアクセスが困難	機器の設定が複雑。固定IPアドレスでない場合には、運用が難しい	通らないデータがある
認証方式	ユーザーを認証	ユーザーを認証	接続元の機器を認証	ユーザーを認証
通信の制限	ファイアーウォールで設定	ファイアーウォールで設定	ファイアーウォールで設定	どのデータを通すかをプロトコル単位で設定。特定のプロトコルのみの通過許可やデータの監視、データの一部除去などにも対応
ファイアーウォールの透過性	電話回線で直結するためファイアーウォールは関係ない	PPTPパススルーに対応していることが必要	IPsecパススルーに対応していることが必要	SSL（ポート443）が通ればよい
利用できるアプリケーション	すべて	すべて	すべて	ウェブが中心。その他アプリケーションの対応は、製品次第。UDPを用いるアプリケーションはほぼ不可能
主な製品、サービス	Windows Server 2003に付属のサービス。集合モデム	Windows Server 2003の標準機能。LinuxやFreeBSDでの構成も可能。一部のルーター製品もサポート	VPN対応ルーター。Windows Server 2003やLinux、FreeBSDでの構成も可能	各種のSSL-VPNアプライアンス。「FirePassリモートアクセスコントローラ」（F5ネットワークス）など

があり、導入が面倒だ。

またクライアントは、インターネットの接続経路のどこかにファイアーウォール機能を持つルーターなどを設置していることが多く、ファイアーウォールの透過性も問題だ。たとえばIPsecは、1つのグローバルIPアドレスを複数のローカルIPアドレスに変換するNAT環境では利用できない。そしてPPTPは、クライアント側のルーターがPPTPパススルーに対応してVPNのパケットを送出しないと接続できない問題がある。このため、たとえば、内部がNAT化されているCATV回線やインターネットカフェからの接続ができないこともある。

そこで近年注目を集めているのがSSL-VPNだ。SSL-VPNは、ウェブの暗号化で使われるSSL暗号化を用いたものだ。簡単に言えば、企業内にブラウザーでアクセスできるポータルサイトがあり、そのポータルサイトにSSLを使ってクライアントがアクセスするというイメージだ。

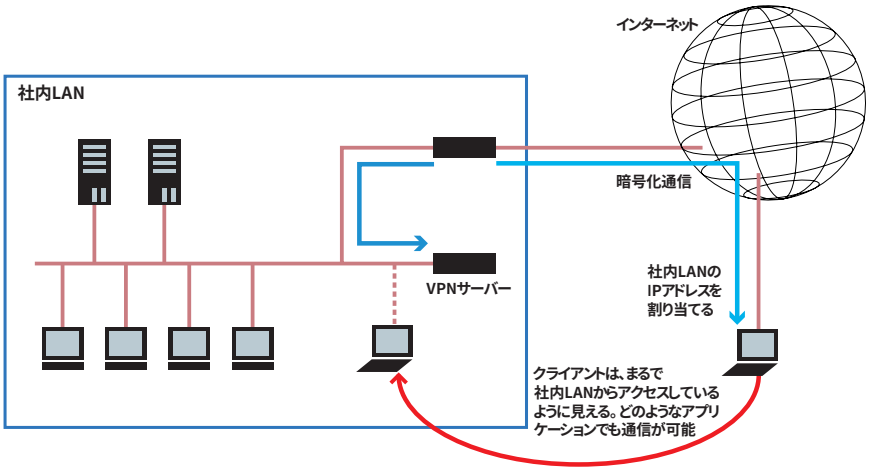
SSL-VPNでは、クライアント側には、インターネットエクスプローラ6.0などのSSL対応ブラウザーさえあればよく、設定やインストール作業が不要だ。接続経路にあるルーターなどのファイアーウォールで、SSLが用いるポート443さえ通すように設定されていれば、VPNパケットが通過できるメリットもある。

またSSL-VPNでは、JavaアプレットやActiveXコントロールを通すことで、ウェブ以外のプロトコルもサポートする。この仕組みでは、TCP接続ならばほとんどの通信が通るため、メールソフトを使ったメールの送受信やファイル転送などもできる。

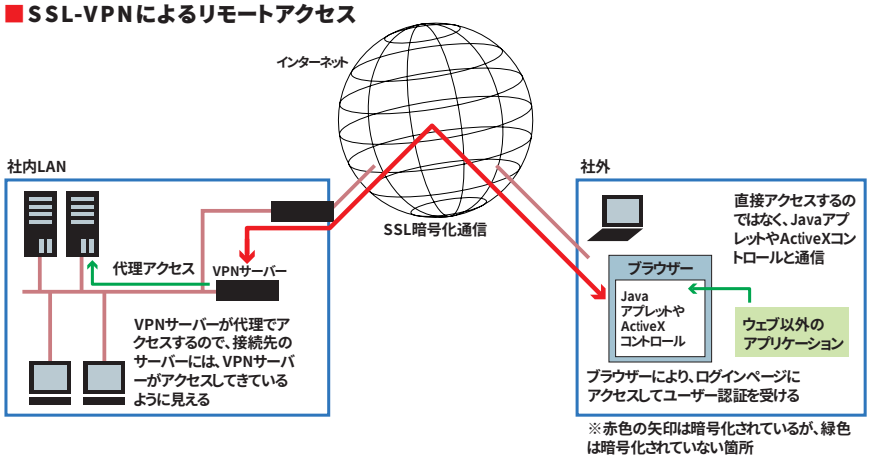
ただしどのような通信に対応するのかは、SSL-VPNサーバー機器やその設定に依存する。つまり、SSL-VPNはIPsecやPPTPと異なり、かならずしもすべての通信をサポートするわけではない。しかし逆に言えば、通信の許可／不許可を設定できることを意味し、安全面では優れる。

さらにSSL-VPNは、さまざまなユーザー認証方式を使えるのも利点の1つだ。たとえば、ワンタイムパスワードを使う方法やクライアント証明書を使った強固なセキュリティーの確保も可能だ。

■IPsec-VPNによるリモートアクセス



■SSL-VPNによるリモートアクセス



「フレッツ・グループアクセス」を使って手軽にVPNを導入

安価かつ簡単にVPNを構築するには、NTT東日本が提供するフレッツ・グループアクセスを利用する方法もある。フレッツ・グループアクセスは、Bフレッツ、フレッツ・ADSL、フレッツ・ISDNにプライベートなIPアドレスを割り当て、拠点間での接続を可能とするものだ。

フレッツ・グループアクセスには、拠点に複数のIPアドレスを割り当てる「フレッツ・グループアクセス プロ」（最大30か所で複数IP可能）と1つのIPアドレスを割り当てる「フレッツ・グループアクセス ライト」（最大10か所でIPアドレスはNTT東日本より割り当て）の2種類がある。前者は事業所間VPNの構築に、後者はリモートアクセスVPNの構築に利用できる。

フレッツ・グループアクセスでは、1つの拠点が管理者となり、ユーザー名やパスワードを事前に設定する（ライトの場合ユーザー名は固定で変更不可）。各拠点では、PPPoEルーターなどで、その接続ユーザー名とパスワードを入力すると、IPアドレスが割り当てられ、拠点間の通信が可能となる仕組みだ。つまり加入者は、いつも使っているプロバイダーのユーザー名を入力すればインターネットへ、フレッツ・グループアクセスのユーザー名を入力すればVPNへと接続先を切り替えて利用する。近年は2セッション同時接続が可能なルーターもあり、そのような機器を使えば、切り替えることなく同時利用も可能だ。

フレッツ・グループアクセスの月額料金は、プロの場合4,500円、ライトの場合700円と安価だ（初期費用は2,000円）。宅内工事は必要ない。契約は回線ごとのため、外出先で利用することはできないが、SOHO環境で互いにネットワークで接続したい場合には便利なサービスだろう。

SOHO・小規模企業から導入できる使い勝手のいいIP-VPNが登場！

SuperEBN

NTTPCコミュニケーションズ URL http://www.nttpc.co.jp/

NTT地域IP網を活用してインターネットVPN並みの価格を実現するIP-VPNが「SuperEBN Multi IP-VPN」だ。株式会社NTTPCコミュニケーションズ ネットワーク事業部 VPNソリューション推進室 室長の齋藤壽勝氏に、その特徴と運用面におけるメリットについて伺った。

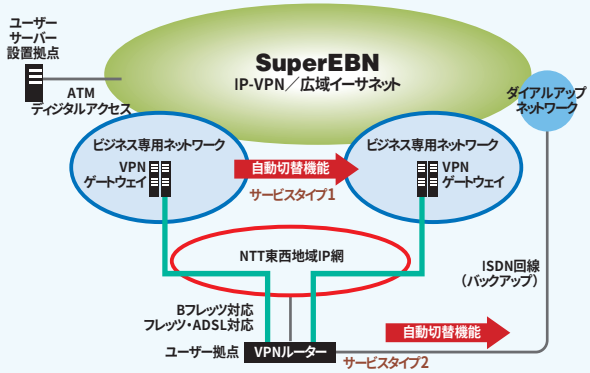
専用線並みの信頼性をブロードバンド回線並みの価格で提供

価格面で気軽に導入できるインターネットVPNは、コスト削減が叫ばれるなかで魅力的なものと映るが、インターネットに接続するとなるとセキュリティーが心配だ。実際、企業のネットワークサーバーに対して「毎日5000回以上のDoS攻撃に加えて何らかの侵入が試みられるケースもある」と齋藤氏は語る。「これだけのDoS攻撃があるとネットワークのパフォーマンスにも影響する」とリスク以外のマイナス面も指摘する。

一方、IP-VPNはこうしたマイナス面を排除してはいるが、割高なことが多い。しかしながら、インターネットVPN並みの低価格でIP-VPNを提供するのが「SuperEBN Multi IP-VPN」だ。

SuperEBN Multi IP-VPNでは、「フレッツ・オフィス網」と「フレッツ・オフィスワイド網」を複数ユーザーで利用し、地域IP網からインターネットを経由せず、SuperEBNに接続している。IPsecの暗号化方式により複数のユーザーがこの網を共用する形をとることで、インターネットVPN並みの低コストと専用線と同等のセキュリティーを持つ閉じたブロードバンドネットワークを実現する。アクセスラインには、専用線やATM技術を利用したメガデータネッツのほかに、ダイアルアップやモバイル環境（@FreeDやFOMA、Air H"、bモバイル）に加え、ADSL（アッカ・ネットワークスやフレッツ・ADSL）やFTTH（Bフレッツ）などが利用できる。モバイル接続では、パケットの圧縮・最適化によって通信速度を約3倍向上できる「ブロードバンドモバイル」と呼ばれるオプションサービスを用意。キャリアに依存することなく利用でき、速度向上に加えてパケット従量制サービスのFOMAなどでは通信コストの削減も同時に実現できる。

■BBBサービス構成図



NTTの地域IP網からインターネットを経由せず、SuperEBNに接続するため専用線同様のセキュリティーを確保する。この構成図は、フレッツ・ADSLとBフレッツを利用する「ビジネス専用ブロードバンド（BBB）サービス」の例。ネットワークは二重化されて障害時に自動で通信経路を切り替えられるほか、さらにフレッツ接続回線を物理的に二重化するオプションも用意する。

強力なバックアップ体制とワンストップビリングで運用も万全

VPN網と拠点間は2つの通信経路を確保しているほか、オプションでフレッツ回線を物理的にも二重化するサービスやダイヤルアップ網を加えて三重化するサービスも用意され、信頼性の高いネットワークを構築できる。これら冗長化への対応は、レンタルで提供される専用のIPsecルーターにより自動的に行われる。障害発生時も、ユーザー側でIP-VPNサービスやアクセスラインの提供事業者にそれぞれ連絡するような煩わしさはなく、SuperEBNのサポートセンターにさえ連絡すれば、問題点の切り分けから障害復旧まで一括でサポートする。

同様に、運用面で手間になるのが回線利用料の支払い方法だ。通常は、IP-VPN網とアクセスラインの利用料を、各社個別に支払う必要がある。しかしSuperEBN Multi IP-VPNでは、「ワンストップビリング」で月々の利用料をすべて1つにまとめて請求書を発行する。全国各地に事業所がある場合でも、各地域別に発行されるNTTのフレッツ網の請求をまとめて受け取れるほか、各拠点ごとに明細も提示され、経理担当者の作業効率もアップする。

ちなみに、NTTPCコミュニケーションズでは、SuperEBN Multi IP-VPNを3月末までに契約すると、初期費用が最大で0円となるキャンペーンを実施している。

NTTPCコミュニケーションズ
ネットワーク事業部
VPNソリューション推進室
室長 齋藤壽勝氏

■SuperEBN Multi IP-VPN（ビジネス専用ブロードバンドサービス）利用料金

サービスタイプ	アクセス回線種類	月額固定料金	初期契約料
サービスタイプ1（ISDNバックアップなし）	フレッツ・ADSL	11,500円	10,000円
	Bフレッツ	19,000円	
サービスタイプ2（ISDNバックアップあり）	フレッツ・ADSL	12,000円	
	Bフレッツ	19,500円	

導入事例：杏林製薬株式会社

杏林製薬株式会社は、3種類のネットワークが混在する複雑な環境にある。各ネットワーク間を接続するための回線が必要なものの、それぞれコストを抑えようとすると帯域不足になる傾向にあった。そこで、SuperEBN Multi IP-VPNでネットワークを統合し、アクセスラインには安価なブロードバンド回線を利用することで、従来に比べて高速かつ約3分の1のコスト削減を実現した。

複雑なネットワークのため速度アップにコストの壁

杏林製薬では従来、各拠点からセンターへの接続にIP-VPN、ATMシェアリンク（ベストエフォート＆ギャランティー型のATM専用サービス）、リモートアクセス用ネットワーク（リモートLAN）の3種類のネットワークを使っていて、各ネットワークを接続するためには広帯域の回線が必要になる問題があった。また、専用線やATMシェアリンク（最高でも10Mbpsまで）で接続していた部署では帯域が不足していたが、それを高速化するためにはコストアップが避けられず、安価なブロードバンド回線では安定性や信頼性の面で不安があった。さらに、医療情報担当者が利用するリモートLANは従量課金のため、コストの予測が難しいという問題もあった。

ネットワーク再編でコスト1/3カット 帯域にも余裕

そこで、SuperEBN Multi IP-VPNを導入してネットワークを1つに統合し、VPNから各拠点にはそれぞれ最適なアクセスラインを使うように変更した。

まず、異なるネットワーク間の接続回線が不要となり、各拠点とVPNとの接続には、アッカ・ネットワークスのADSLやNTT東日本・西日本のフレッツ・ADSL、Bフレッツなどのブロードバンド回線を使用できるようになった。一部本社や都内支店など特にスループットに対する要望の強い拠点間は100Mbpsのメトロイーサを導入するなどして最適化しながらコストを削減。モバイル環境では定額制のPHS通信網（bモバイル）を採用することで通信費を減らし、さらに利用する認証方式（ワンタイムパスワード）は自前で運用していたものをサービス事業者に委託することで省力化を実現した。

このようなネットワークの切り替えにより、運用コストは以前の3分の2まで抑えられた。加えて帯域は3～10倍と大幅に高速化した。切り替えに際し、初期費用など追加でかかるコストもあったが、それでも半年くらいで回収できる計算だ。杏林製薬の例にかぎらず、初期費用は一般に半年から長くても1年で回収できるという。

安心のセキュリティー対策でインターネット接続を開放

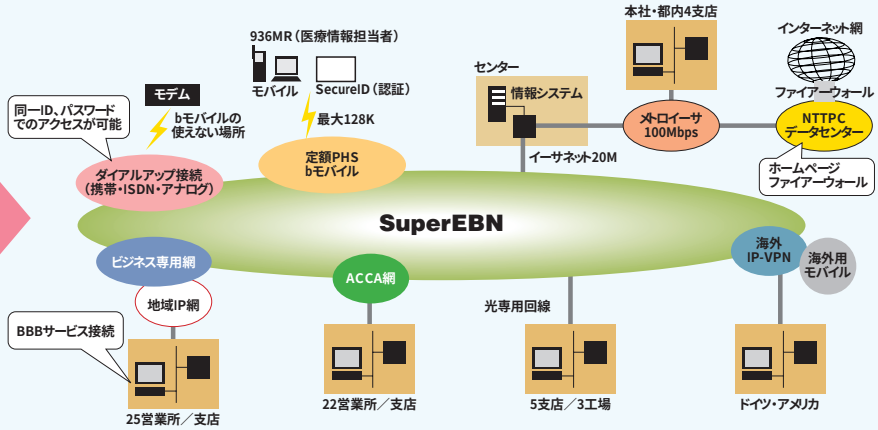
杏林製薬ではこれまでセキュリティーや回線速度の都合上、外回りの医薬情報担当者にインターネットを開放していなかった。しかし、このたびの回線変更のおかげで帯域に余裕ができたため、インターネットへの接続を可能とした。また、すべてのマシンにプライベートIPアドレスを割り当て、インターネットへの出口を1か所に限定することで、不正な操作をすると即座にマシンが特定できる万全のセキュリティー体制をとっている。このため、昨今のウイルス被害などの影響も皆無だという。ネットワーク再編のメリットは費用対効果が大きく、多方面にまでその効果は及んでいるようだ。

■SuperEBN導入前の問題点

- センターと支店・工場の一部(IP-VPN)、センターと本社・支店の一部(ATM網)、リモートLANは、それぞれ別のネットワークで構成3つのネットワークが存在)。このネットワークを相互に接続するために広帯域の回線が必要になる。
- ディジタルアクセスやATMで接続されていた一部の本社、支店・工場の帯域が不十分。帯域を太くするにはコストがかかり、安価なブロードバンド回線に変更すれば安定性や信頼性の面で不安がある。
- リモートLANに接続するモバイル端末は従量課金。このため、運用コストの予測が難しい。

運用コスト1/3削減

■SuperEBN導入後のネットワーク構成



ネットワークの統合により、ネットワーク間の接続回線が不要となった。セキュリティーが確保されたSuperEBNへの接続でアクセスラインに安価なブロードバンド回線が利用できるようになり、速度の向上とコスト削減を実現。モバイル環境には定額のbモバイルを導入した。これに併せて、ウェブサーバーもNTTPCのデータセンターにアウトソーシングした。

問い合わせ先　株式会社NTTPCコミュニケーションズ　VPNソリューション推進室　小西／大隅
TEL：03-5212-1380　FAX：03-5275-6576
E-mail：nwvpn@nttpc.co.jp

［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