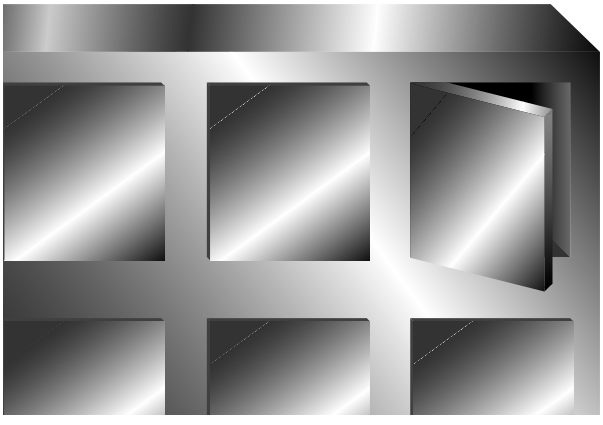
インターネット最新テクノロジー：第15回

インターネットを企業ネットワークの一部として利用できる

VPN（Virtual Private Network）

企業ネットワークとインターネットとの連携が不可欠なものになるに伴って、逆にインターネットを使って企業ネットワークのコストを削減しようという動きが出てきた。インターネット電話によって電話代を安く抑えるのと同様にVPN（Virtual Private Network：仮想私設網）と呼ばれる技術によってインターネットを専用線のように使い、企業ネットワーク（イントラネットやエクストラネット）の通信コストを安くあげることが可能である。VPNを実現するためにはデータを安全にやり取りするための暗号通信やトンネリングといった技術が使われている。今回はVPNを実現する技術と仕組みについて解説する。

長原 宏治　有限会社NSプランニング



自前の専用線からインターネットへ

オフィスワークの効率化を成し遂げて企業成長を維持するために企業内のネットワークがますます重要となっている。同時にインターネットは企業にとって不可欠のコミュニケーション手段となりつつある。最近のイントラネットの流行によって、企業ネットワークとインターネットの違いはファイアーウォールの内側か外側かということだけになりつつあることが重要である。企業内ネットワークで使われているプロトコルやアプリケーションとインターネットで使われているそれとの間に違いがなくなりつつあると言ってもいいだろう。

インターネットが普及する以前の企業ネットワークはすべての回線を自前で調達するものであった（図1-1）。今でも数多くの大企業がこのような自営ネットワークを維持しているが、専用線を維持するコストを考えると中小企業にはなかなか手が出せないのも事実である。そこで企業ネットワークもTCP/IPベースとなりつつあることと、全国規模のプロバイダーがいくつもあることを利用して、図1-2のように企業ネットワークの長距離部分にインターネットを利用することが考えられた。これがVPNの基本概念である。企業のプライベートネットワークをインターネット上に仮想的に作り上げることからこのように呼ばれる。特定の通信だけをインターネット経由で行うではなく、ある拠点のネットワークから別の拠点のネットワークに向かうすべての通信をインターネット経由で行うことが重要である。

必要なのは「いつでも」繋がり「すべて」を暗号化できること

インターネットを使って企業の拠点間で重要な情報をやり取りするには、常にネットワークが使えるという信頼性やデータが盗まれないようなセキュリティーの問題を慎重に考慮することが必要である。

ある程度のセキュリティーで構わないならば、特定の信頼できるプロバイダーを選び、そのプロバイダーをバックボーンとして利用するという方法も考えられる。実際にそのような方法で専用線のコストを削減している企業も存在する。しかしプロバイダーの管理体制を厳密にチェックすることはできないのが現実である。また複数のプロバイダーと契約してインターネットへの接続にバックアップの回線を用意する必要もあるだろう。

さらなるセキュリティーを確保するためには、拠点間のデータがインターネットを通るときに、それを暗号化する必要がある。現在ではVPNといった場合には「インターネット上で暗号を使い、企業ネットワークを（仮想的に）拡張すること」を指すと言っても過言ではないであろう。ただし拠点をまたいで利用するようなアプリケーションレベルで暗号化する方法（SSLなどがその代表と言えるだろう）はVPNとは言えない。VPNを実現するにはネッ

トワークをまたぐすべてのトラフィックを暗号化する必要がある。そのために暗号化をIPパケット単位で行うのである。

遮断ではなく安全にやり取りする

具体的な例を見ながらVPNの仕組みを見ていこう。図2はある企業の拠点にあるネットワークAと別の拠点にあるネットワークBをVPNで結んでいる例である。ホストAからホストBに向かうデータはVPN装置Aで暗号化されて送り出される。インターネットを通ってVPN装置Bに到着したデータはそこで復号されてホストBに至る。ホストAとホストBではデータがインターネットを経由してきたことも、その途中で暗号化されていたことも知る必要がない。またホストAからインターネットに向かうデータ、あるいは逆にインターネットからホストAにやってきたデータはそのまま暗号化されることなくやり取りされる。つまりVPN装置が発信元と宛先によってデータを選択して必要なものを暗号化および復号するので、企業ネットワーク内では通信の暗号化を気にする必要がない。

図2ではVPNの仕組みを実現するものを独立した装置として示したが、実際にはファイアーウォールやルーターのオプション機能として実現されている場合が多い。暗号化が必要となるのはファイアーウォールの外側だけであり、アドレスによってデータを選択するという動作はファイアーウォールに類似したものである。しかし、ファイアーウォールは外部からの不正なアクセスを遮断することが目的であるのに対して、VPNは内部のデータを安全に外に送り出す、あるいは正当なデータを安全に取り込むことが目的である。

パケットのカプセル化によってトンネリングを実現

VPNを実現しようとする場合、現在多くの企業ネットワークで使用しているプライベートアドレスが問題となる。プライベートアドレスをインターネット上で利用することはできないのでアドレスの付け替えが必要となるのだ。プライベートアドレスを使っていない場合であっ

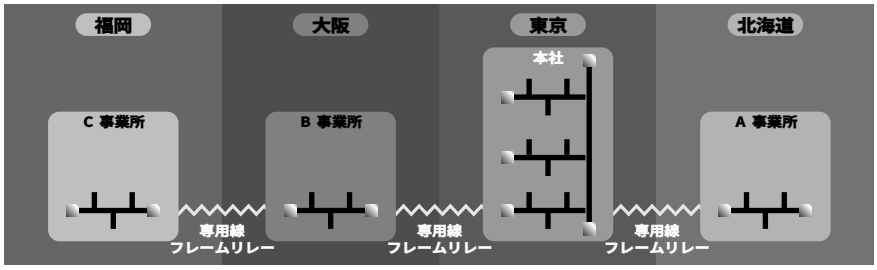


図1-1 広域企業ネットワーク

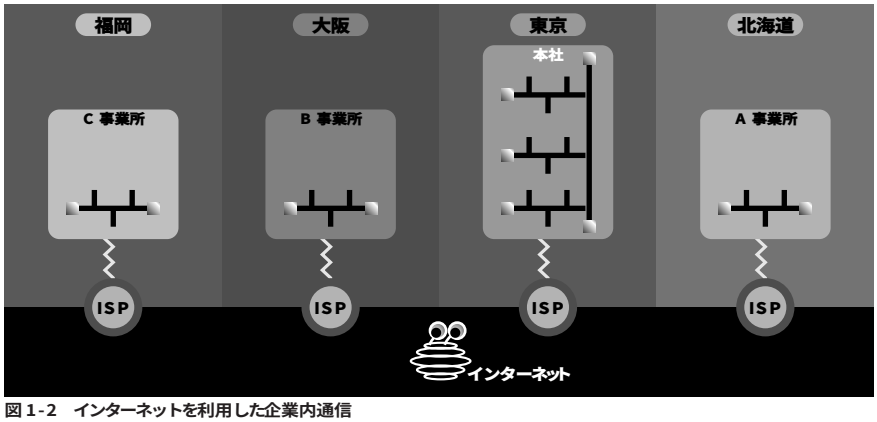


図1-2 インターネットを利用した企業内通信

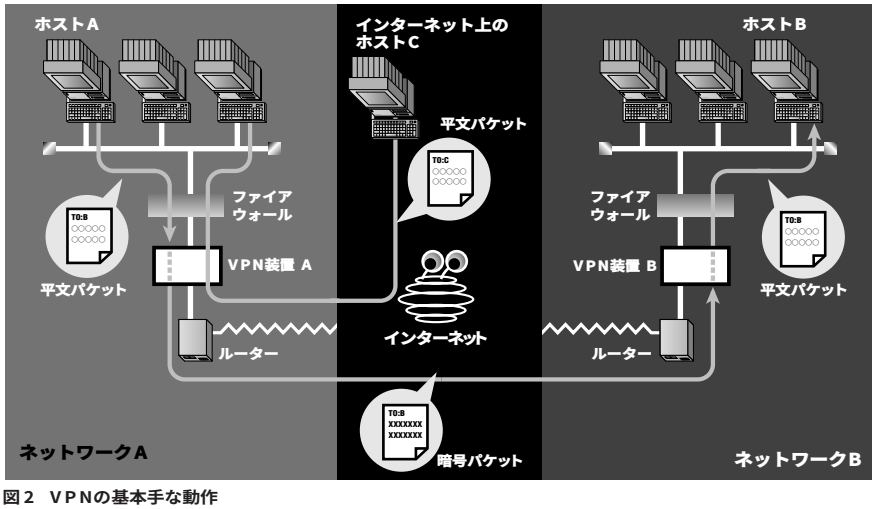
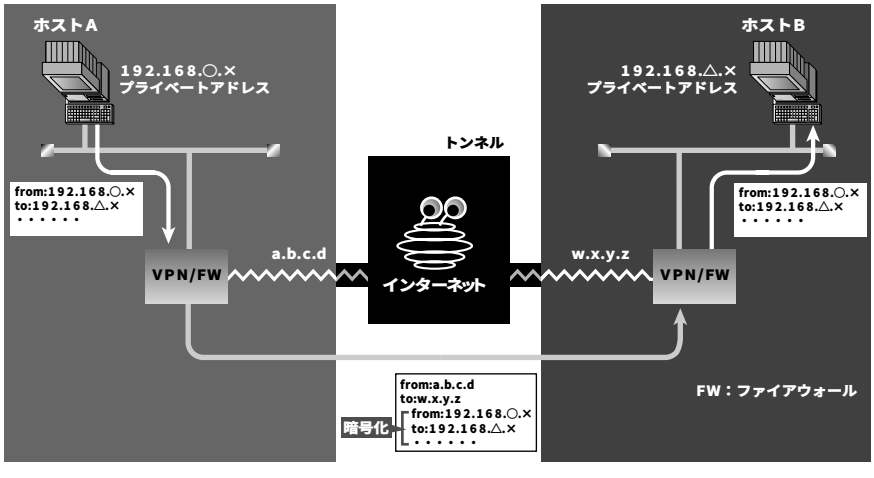


図2 VPNの基本手な動作

ても、クラスBアドレスを2分割して経路情報をほかのネットワークに伝えることはできないので、同様にアドレスの付け替えが必要となることが多いだろう。単に企業ネットワークからインターネットに出て行くだけならばNAT（Network Address Translation）によって問題を解決できるが、VPNではいったんインターネットに出たデータを再度企業ネットワークに取り込まねばならないため、特別な仕組みが必要となる。

このようなアドレスの問題に対応するために、トンネリング技術が利用されている。例を挙げながら考えよう。図3においてホストAからホストBに向かうパケットは、ネットワークAの出口で全体が暗号化されて、ネットワークBの入り口に宛てたパケットにカプセル化される。インターネットを通ってネットワークBに到達したパケットはその入り口でカプセル化が解かれ、復号されたうえでホストBに向かう。ネットワークAならびにBで通用する形のパケットは、インターネット上を流れるときはカプセル化によって「単なるデータ」となっているため、トンネルから抜けてきたように見えるのである。これによりファイアーウォール内部のネットワーク構造を知られたくないというニーズも満たすことができる。

図3 トンネリングによるアドレス変換



標準化の鍵はIPsec

VPNとは前述のとおりIPパケットをそのまま（パケットを単位で）暗号化して特定の宛先に送り込む技術であるとも言えるだろう。IPパケット自体の暗号化と言えばIPv6での実装が必須となった「IPsec（IP SECurityの意：RFC1825-1828）」が重要である。実際のところVPN製品のいくつかはすでにIPsecへの対応を完了または予定しており、IPsecに基づく形での相互運用性が今後は期待されることから、IPsecについて簡単に紹介しておこう。

IPsecは設計段階からIPv6とIPv4の双方で利用できるようにデザインされている。IPv4ではオプション機能であるが、IPv6では必須機能であるため、IPv6を利用する場合は特別な機器やソフトウェアを導入しなくても安全な通信が実現できるようになるはずである。IPsecでは最低限必要な暗号化方式と認証方式が規定されたうえで、送信側と受信側の双方でネゴシエーションを行って具体的な通信方法が決定される仕組みとなっている。実装が必須とされているのは、暗号化ならびに認証のアルゴリズムが「DES-CBC」と「鍵付きMD5」のものである。それぞれの詳細についてはIPv6について詳説された文献を見るといいだろう。なお暗号通信では鍵を管理および配布するための方法（プロトコル）が必要であるが、このIPsecでは定義されていない。鍵管理プロトコルとしては標準とされているSKIP（Simple Key-Management for Internet Protocols）やISAKMP（Internet Security Association And Key Management Protocol）がある。今後はIPv6のベースとして採用される見込みのISAKMPが標準的に利用されていくであろう。

IPv6では標準の機能

VPNとはパケットレベルでの暗号化を用いて「安全に」通信する技術である。ここで言

う「安全」とはやり取りしている情報の中身を他人に知られることがないということであり、プライバシーを気にすることなくどのような情報も自由に送受信できる。したがって企業ネットワークにおいて拠点間を結ぶだけではなく、取引先との重要な情報のやり取り（エクストラネット）やモバイルコンピュータからインターネットを経由して企業のネットワークにアクセスする（モバイルアクセス）などへの応用も期待されることが明らかだろう。さらに一歩進んで、IPv6によってプロトコルレベルでの安全性がどの機器にも標準装備されるようになればVPNを利用する必要はなくなり、単に「通常のネットワーク接続において暗号オプションを利用する」だけのこととなる。これはVPNが過渡的な技術であるということではなく、未来の安全な通信方法を前もって取り込み、開発と検証を行っていると捉えるべきであろう。

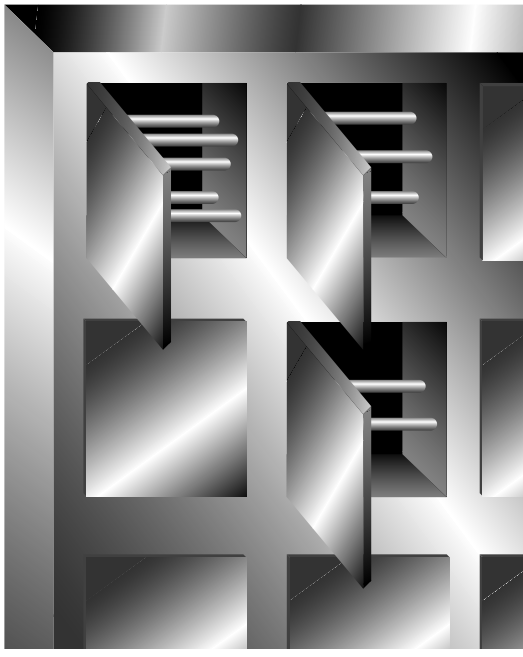
着目すべきは相互運用性

ここで現在のVPN製品について簡単に見ていこう。セキュリティー意識の高まりからかいくつもの製品が市場で入手可能となっているが、形態によって大まかに3種類に分けられる。

代表的な形態はファイアーウォールのソフトウェアと一体になったもの（ファイアーウォールの機能としてVPNを提供するもの）でCheckpoint社のFirewall-1やTIS社のGantletなどが有名である。さらにすぐに使える製品としてVPN機能を専用ハードウェアに納めたもの（TimeStep社のPermitなど）やルーターのオプション機能として組み込むもの（Cisco社やAscend社など）がある。いずれの製品も積極的に標準化に対応しようとしており、先に述べた標準となりつつある仕様に沿った製品同士であれば、相互運用性も得られるようになっているようだ。

VPNはその性格上、企業単位で機材やソフトウェアが導入されることが多いと思われるため、相互運用性が重視されることが少ないのかもしれないが、今後はIPsecやISAKMPといった標準仕様に沿った製品が増え、十分な相互運用性が確保されるものと期待される。

商品として販売されているものの常として、簡単にVPNを実現できるようにうたわれている製品が多いが、実際には暗号や鍵管理に関する十分な理解が必要となる。あたりまえのことだが、ドキュメントが充実していて、サポートのしっかりとしたベンダー製品を選ぶように心がけるべきだろう。



ファイアーウォールとの一括管理が現実的

セキュリティー機能を一括して提供するために、VPN製品の多くはファイアーウォールと一体となって販売されているし、別の製品として販売されている場合であってもファイアーウォールと同時に管理されることが多い。ファイアーウォール周辺の技術と設定項目は非常に多岐にわたっており、それぞれを互いに関連付けながら理解して設定するためには、すべての技術に対する十分な理解と経験が必要である。さらにこれらの機能を個別に設定していくことはかなり骨の折れる作業となってしまう。できるならばファイアーウォール、VPN、アドレス変換などをまとめて簡単に設定できる機能が欲しいものである。さらに今後普及が見込まれている帯域保証や負荷バランスなど技術に対しても同様の統合化されたソリューションが求められる。今後の製品の進化に期待したい。

●

［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