

第7回

VPN

VPNの利用形態を知る

VPN(Virtual Private Network)とは、インターネットなどのオープンなネットワーク上で、安全な通信を可能にする仮想的なプライベート・ネットワークである。本連載では、今号から3回にわたり、VPNについて解説していく。その第1回目となる今回は、VPN技術の種類や利用形態について説明する。

内藤正規
ネットワークシステムズ

VPNのコア技術
IPsecとSSL

VPNは元来、インターネットのような公衆回線を介した通信において、専用線と同等の安全性を確保することを目的としたセキュリティ技術であり、IPによる通信にさえ対応していれば、接続環境は問われない。とはいえ、VPN製品が市場に出回りだした当初は、セキュリティを高めるための手段ではなく、専用線の代替手段として注目を集めていた。というのも、セキュリティの向上よりも、専用線をVPNに置き換えることで得られるコスト効果のほうが、市場に対する訴求力としては大きかったからである。

VPNを実現する技術はいくつかあるが、その中で主流と言えるのはIPsecだろう。また、近年、SSLベースのVPN製品もリリースされ、注目を集めている。そこで、まずは、これら2つの技術の機能や特徴について説明する。

IPsec

IPsecは、IPパケットを安全に通信相手となるマシンに搬送するセキュリティ・プロトコルである。当初、同プロトコルは拡張性と汎用性に欠けていた。その例として、リモート・アクセスVPNやLAN間VPN(詳しくは後述)において、接続元のマシンのIPアドレスが動的に変化することが考慮されていなかったり、通信を行うマシンの認証機能は備えるが、ユーザーの認証はRADIUSやLDAPといった技術を利用しなければならなかったりしたことが挙げられる。しかしながら、IPsecは、IETF(Internet Engineering Task Force)で標準化された技術であること、また、数学的に保証された暗号強度と、LANよりも強力な通信

の秘匿性を備えていたことなどにより、セキュリティ技術として確固たる地位を確立した。

なお、ベンダー各社は、上述したようなIPsecに内在する拡張性と汎用性に関する課題を実装で補うことで、IPsecをベースとするVPN製品の機能向上を図っている。

SSL

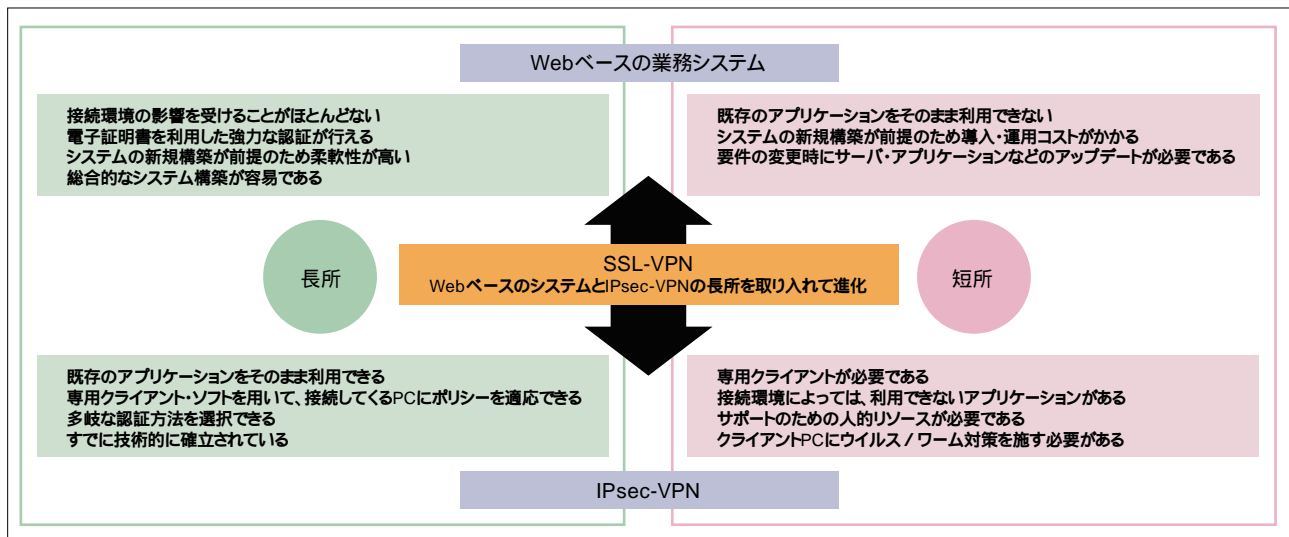
SSLはそもそも、サーバとWebブラウザとの間で送受されるデータを暗号化したり、通信相手を認証したりするための技術である。これまでもSSLは暗号化通信などに利用されていたが、それほどメジャーな技術ではなかった。しかし、SSLを利用したVPN製品が2002年辺りからリリースされ始めたことで、SSLの知名度は急上昇した。そして、昨年後半から現在にかけて、SSLベースのVPN製品市場は一気に成長した。

IPsec-VPNと
SSL-VPNの違い

IPsecによるVPN(以下、IPsec-VPN)と、SSLによるVPN(以下、SSL-VPN)は、VPNを実現する技術という意味では同類だが、原理的にはまったく異なる。具体的には、IPsec-VPNでは専用のクライアント・ソフトウェアを用意する必要があるのに対して、SSL-VPNでは、クライアント・ソフトを別途用意する必要がない(詳しくは後述する)。

SSL-VPNではHTTPS(注1)を用いて暗号化や認証を行うため、クライアントとなるデバイスにはHTTPSに対応した多機能なWebブラウザを用意すればよい。SSL-VPN製品によっては、PCだけではなく、

図1：SSL-VPNの位置づけ



HTTPSに対応したWebブラウザを装備したPDAなどでも、VPNを利用できる可能性がある。こうした特徴を備えるSSL-VPNは、ユビキタスというキーワードの浸透とともに、「どこからでも使えるVPN」といった触れ込みで利用が広がっている。

IPsec-VPNとSSL-VPNは、進化の方向も異なっていくと予想される。IPsec-VPNが専用クライアントソフトの機能強化により、「利用環境は限定されるものの多機能さ」へ向かっていくのに対して、HTTPSによるWebベースの業務システムとIPsec-VPNの中間に位置づけられるSSL-VPNは、安全性とユビキタスのバランスが取られた技術として発展していくものと考えられる(図1)。

リモート・アクセスVPNの仕組みと利用時の注意点

次に、VPNの利用形態について解説しよう。その種類は複数あるが、ここでは「リモート・アクセスVPN」という形態の説明から始めることにする。

リモート・アクセスVPNは、リモートのホスト(自宅や

外出先など遠隔地にあるマシン)と、拠点に設置されたVPN機器との間の通信を可能にするというものである(116ページの図2)。接続形態には、モバイル・ユーザー向けの定額制パケット通信や、ブロードバンド接続が用いられることが多いため、リモート・アクセスVPNはダイヤルアップ接続の置き換えとして定着しつつある。

リモート・アクセスVPNは、IPsecやSSLによって実現することが可能だが、この2つの技術では、クライアントソフトの取り扱い方法が大きく異なり、いくつか注意すべき点がある。以下、クライアントソフトに焦点を当て、リモート・アクセスVPNにおける注意事項を説明する。

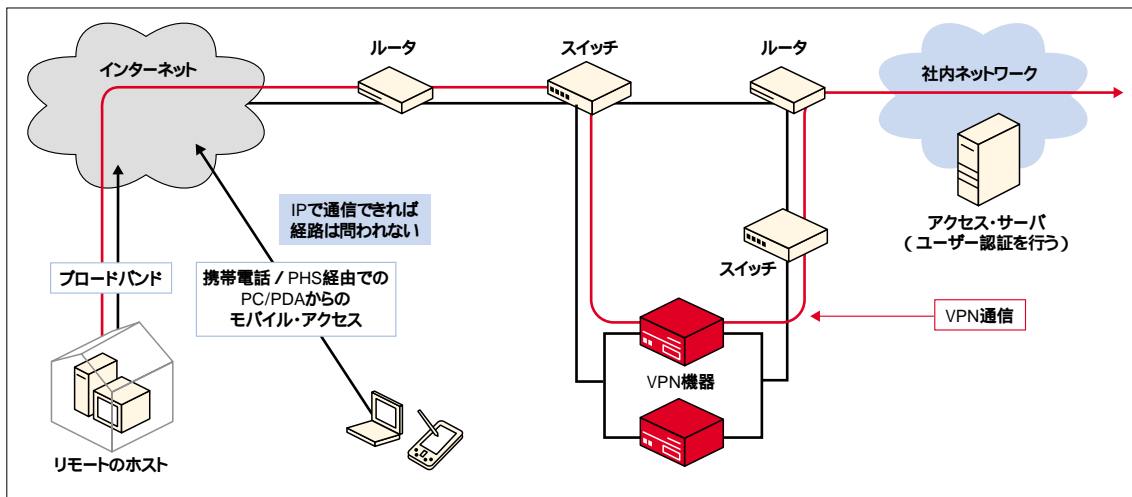
IPsec-VPNの場合

IPsecによるリモート・アクセスVPNでは、VPN機器にアクセスするリモートのホストに専用のクライアントソフトを導入しておく必要があるが、このソフトの配布、運用にはさまざまな障壁がある。以下、具体

注1：HTTPS(HyperText Transfer Protocol Security)は、HTTPにSSLの暗号機能を付加したプロトコル



図2：典型的なリモート・アクセスVPNの構成例



的な問題点を説明する。

輸出入の制限

VPNクライアント・ソフトを配付、利用するうえでの最も大きな問題は、輸出入の制限である。というのも、VPNのクライアント・ソフトは戦略物資として取り扱われるため、一般的には無条件で国外に持ち出すことができないのだ。他国にVPNクライアント・ソフトを持ち込みたい場合は、搬出元と搬出先の双方の輸出入規制をクリアしなければならない。そのためには、VPNクライアント・ソフトを利用するユーザーは法律で定められた関係当局に届け出る必要があるが、国によっては、該当する機関が周知されていないなどの理由から手続きに時間がかかったり、ソフトの輸出/輸入が実質不可能だったりする。よって、海外からの接続を受け付ける場合は、クライアント・ソフトの現地調達も視野に入れてVPN導入を検討されたい。なお、VPN機器本体を国外に持ち出す際も、クライアント・ソフトと同様の対応が必要となる。

現在日本で主に流通しているVPN製品については、ベンダーに問い合わせれば、海外での入手方

法がわかるため、日本国内から送付するよりも、現地で入手したほうが手間がかからないと言える。ただし、筆者の経験上、現地のベンダーに導入などを依頼して、スキル不足が原因で作業に手間取ったことがあるため、その点には注意していただきたい。

リモートのホストにおけるセキュリティ対策

通信経路としてインターネットを用いた場合、リモートのホストは外部からの脅威にさらされることになるため、セキュリティ対策を施す必要がある。さまざまなセキュリティ・リスクからリモートのホストを守るには、ウイルス/ワーム対策や、外部からの攻撃に対する防御策として、クライアントPC用のファイアウォール・ソフト(パーソナル・ファイアウォール製品など)を導入するのが望ましい。ただし、ファイアウォール・ソフトの導入に際しては、VPNクライアント・ソフトとの相性を考慮する必要がある。

これまで、こうしたリモートのホストにおけるセキュリティ対策はユーザーの自主性に任せられており、VPN機器は、各ホストのセキュリティ対策の実施状況に関係なく、すべてのアクセスを受け付けるような設定になっていた。だが、昨年辺りからは、リモー

VPNクライアント・ソフトが引き起こす問題

IPsecによるリモート・アクセスVPNでは、リモートのホストに専用のクライアント・ソフトウェアを導入する必要があるが、このソフトがさまざまな問題を引き起こす。というのも、こうしたクライアント・ソフトを導入する際には、VPN通信用の仮想ネットワーク・アダプタが実装されるなど、OSに含まれるネットワーク機能の部分にまで大きな影響を及ぼし、ハードウェアの追加と同等のリスクを伴うからだ。

具体的なトラブルの例としては、次のようなものがある。1つは、デバイス・ドライバに関連した障害で、この場合、深刻な事態(Windowsであれば、ブルー・スクリーンの発生など)に発展することがある。

また、他のアプリケーションとの相性問題から、あるPCでのみトラブルが生じることもある。このような場合は、他の障害発生の際に則した問題の切り分け方法が適用できないため解決が難しく、ベンダーやメーカーにサポートを依頼しても、よほど明確な問題でなければ対応は期待できない。なぜなら、固有のPCに由来する障害は他のPCでは再現でき

ないため、検証によってその原因を見つけることは不可能であり、問題の要因がクライアント・ソフト以外にあることも少なくないからである。

なお、クライアント・ソフトの仕様によっては、どのソフトに非があるのかを明らかにできないケースもある。最終的には、“最悪なサポートの典型”としてしばしば例に出されるように、「OSを再インストールしてください」と言われてしまう可能性もありうる。

ならば、専用のクライアント・ソフトが不要なSSL-VPNであれば、上述したようなトラブルと無縁かという、必ずしもそうとは言いきれない。SSL-VPNでは、利用環境(デバイスやWebブラウザの種類など)を限定することができないだけに、「原因不明の障害」がもっとも多くなる可能性が高い。つまり、SSL-VPNは、クライアント・ソフトに起因したトラブルからはフリーであるにすぎないのだ。なおSSL-VPNは、本文でも述べたように、“間口が広い”ゆえに、情報漏洩などのセキュリティ・リスクが多く待ち受けていることを認識しておかなければならない。

ト・ホストが接続した際にセキュリティ対策の実施状況をチェックすることが可能なVPN機器が出始めている。それを利用すればリモートのホストにインストールされたウイルス対策ソフトのパターン・ファイルのバージョンや、ファイアウォール・ソフト導入の有無などをチェックしたうえで、セキュリティ対策が十分に施されていないホストからの接続を拒否できるようになる。

SSL-VPNの場合

SSL-VPNでは、アプリケーションに依存する通信の仕組みとセキュリティに注意する必要がある。以下、それらについて説明する。

通信の仕組み

IPsec-VPNでは専用のクライアント・ソフトによって、どのようなアプリケーションでも同一の仕組みで通信できるのに対して、SSL-VPNでは、利用するアプリケーションによって通信の仕組みが異なる(118ページの図3)。

HTTPSをサポートしているアプリケーションは、

Webブラウザから利用することができる。また、Webブラウザからアクセスできない、HTTPS以外のプロトコルで通信するアプリケーションは、Webブラウザ上でJavaアプレットやActiveXコントロールを動作させたり、ポート・フォワーディング機能(注2)を用いたりすることで、利用することが可能になる(118ページの図4)。なお、Windowsのファイル共有機能や、上記の方法では対応しきれない機能は、専用のポータル・サイトを構築し、それをゲートウェイとして用いることで、SSL-VPN経由で利用できる。

なお、こうした機能は各SSL-VPN製品の実装方法に依存するので、必ずしもすべての機能を使用するわけではない点に注意されたい。また、SSL-VPN製品のベンダーはほとんどが海外ベンダーなので、日本語対応についても確認しておく必要がある。

セキュリティ

SSL-VPNは、IPsec-VPNと比べて、デバイスやそ

注2：ポート・フォワーディングは、ローカル・マシンの特定のポートに送られてきたパケットを、リモート・マシンの別のポートあてに送信する機能



図3：IPsec-VPNとSSL-VPNの仕組みの違い

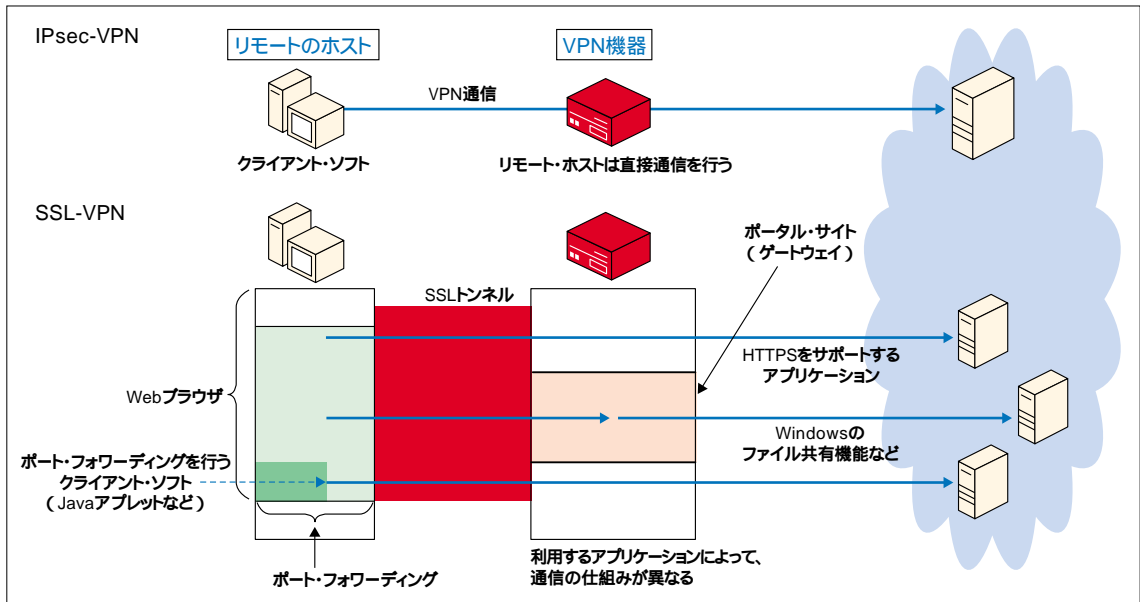
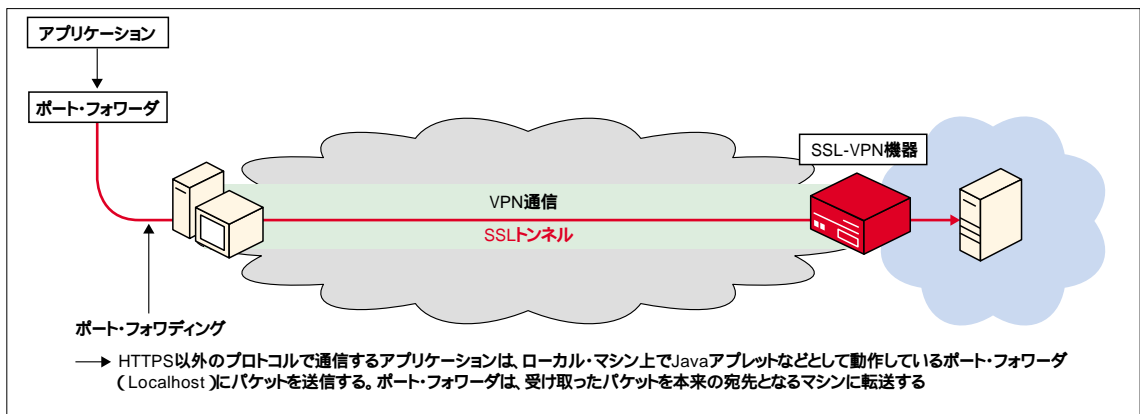


図4：ポート・フォワーディングの仕組み



のデバイスの設置場所を問わないユビキタ性が特徴であることは先に述べたが、セキュリティを要する機密情報とユビキタスという概念が本来は相いれない可能性があるということ忘れてはならない。実際、インターネット・カフェなども含めて、どこからでも使えるということは「利用を制限できない」とこと同義であり、SSL-VPNでは、利用者の専有物ではないPCや安全ではない場所からのアクセスにより、

情報漏洩などのリスクが常に伴うのだ。こうしたリスクに対して防御策が施されている製品もあるが、まだ実績は少ないので、利用の際は注意していただきたい。

なお、PCからVPN経由でアプリケーションを利用し終わったあと、その通信のデータを削除するというSSL-VPNサービスを提供しているベンダーもある。このサービスでは、USBデバイスのような着脱式の

メディアに、VPN通信に必要な情報などを格納しておく仕組みが採用されている。



ワイヤレスLANを利用したVPN

ユビキタスというキーワードに関連したVPNの利用形態としては、ワイヤレスLANを用いたものがある。ワイヤレスLANは利用エリアの拡大や通信速度の向上などにより、その利用者は増す一方だが、利用上の問題として、セキュリティリスクを抱えていることが挙げられている。

VPNを用いることで、ワイヤレスLANにありがちな情報漏洩に対するリスク(不安感も含め)を考慮することなく、外出先でブロードバンド環境から安全に社内ネットワークへの接続を行うことができる。ワイヤレスLANは利用する暗号方式によっては盗聴される可能性があるが、こうした状態でも、VPNにより安全な通信が行えるということは、先に述べたような、「IPによって通信可能な環境であれば、どこでもセキュアな通信が行える」というVPNのメリットを象徴する好例だと言える。

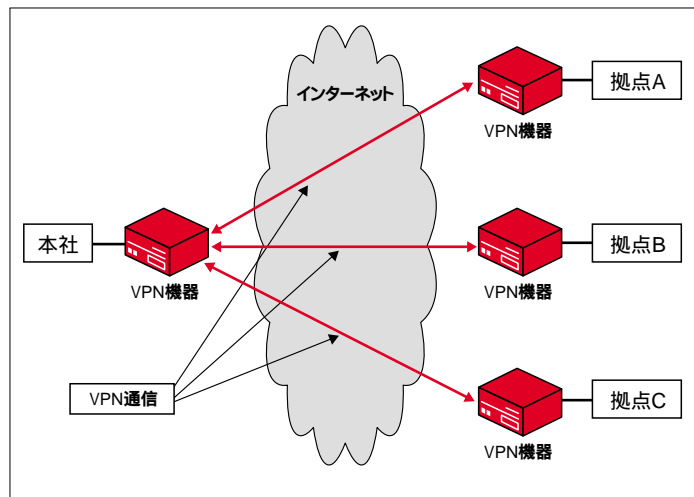
また、モバイル・デバイスからのリモート・アクセスにワイヤレスLANとVPNを用いれば、高速で安全な通信環境を実現できるだけでなく、通信コストも抑えられる。第3世代携帯電話の回線を利用しても、高速な通信は可能だが、その場合、本稿執筆時点では、従量制サービスしか提供されていないため、送受されるデータ量が増加すればするほど、通信料が高額になってしまう。したがって、その方法は、あまり現実的ではないというのが実情である。



コスト削減と通信の秘匿性を 実現するLAN間VPN

リモート・アクセスVPNと並ぶVPNの利用形態とし

図5：LAN間VPNの構成例



ては、離れた拠点間を接続する「LAN間VPN」がある(図5)。これは、IPsecによって構築されることが多い。LAN間VPNには、コスト削減の効果があるほか、導入時は途中経路のみを変更すればよいため、ユーザーに影響を与えることなくVPN環境を構築でき、既存環境との親和性も高い。こういった点から、LAN間VPNは“安価でセキュアな通信”を実現するネットワークとして、多くの企業においてすでに定着している。

ただし、LAN間VPNでは、通信回線コストの低下に伴い、回線の信頼性も低下するため、特に安全性が求められる用途に用いることは推奨できない。むしろ、機器や経路の冗長化によって信頼性の低下を補うことも可能だが、専用線レベルの信頼性に到達することは難しく、コスト削減効果は低くなってしまふ。

とはいえ、近年は、コスト削減効果ではなく、暗号化通信によるデータの秘匿性に主眼を置いたLAN間VPNの需要が大きく伸び始めている。また、金融機関などでは、専用線を用いて離れた拠点間を接続しながら、通信の暗号化を目的としてIPsecを利用するケースもあるようだ。

CW