新連載

VPN環境を構築する前に学んでおこう

ここが知りたいVPN

馬場達也

第1回

リモートアクセスVPNに必要となる機能

本連載では、リモートアクセスVPNの導入を検討している読者のために、リモートアクセスVPNにおいて利用されている技術、すなわちIPsecやPPTP、L2TP、SSLの技術的な特徴や違いをわかりやすく解説していく。

インフラの充実でリモートアクセスVPNへの期待と需要が高まっている

リモートアクセス**VPN**は、ADSLなどにより常時接続された自宅のPCや、出張先でインターネットサービスプロバイダー(ISP)にダイヤルアップ接続したノートブックPCなどから、インターネット経由で社内ネットワーク(イントラネット)などへ安全にアクセスするための仕組みである。

従来、社外から社内のネットワークにアクセスするには、社内ネットワーク上に設置したアクセスサーバへ直接ダイヤルアップ接続することが一般的だった。しかし、電話料金の負担が大きいという問題やセキュリティ上の問題があることから、現在では、インターネットを利用したリモートアクセスVPNが注目されるようになってきた。

駅や喫茶店などのさまざまな場所からインターネットへのアクセスが可能となったことや、各種OSや低価格のブロードバンドルータでもVPN機能をサポートするようになってきたことなどを背景として、実際に多くの企業がリモートアクセスVPNを導入している。読者の中にも、外部から自宅あるいは社内のネットワークへアクセスするために、すでにリモートアクセスVPNを利用している方がいるかもしれない。

今回は、連載第1回目ということで、**IPsec**、**PPTP**、**L2TP**、**SSL**といったリモートアクセスVPNを実現する技術には触れずに、リモートアクセスVPNに必要となる機能や、導入に関しての注意点を解説する。

VPN(Virtual Private Network)
インターネットなどの公衆回線を仮想的な専用回線として利用することでセキュアな通信路を確保するための技術。

IPsec(IP Security Protocol)
IPパケットレベルで認証や暗号化を行うことのできるセキュリティプロトコル群。

PPTP(Point-to-Point Tunneling Protocol)
マイクロソフトが提唱した、インターネットを利用したVPNを実現するためのプロトコル。PPPを拡張してデータの認証や暗号化機能を実装している。

L2TP(Layer2 Tunneling Protocol)
データリンク層のレベルでPPP通信をトンネリングするためのプロトコルで、PPTPとシスコシステムズのL2Fが統合されたものである。

SSL(Secure Sockets Layer)
ネットスケープコミュニケーションズが提唱した、HTTP暗号化通信のためのプロトコル。公開鍵暗号化方式やメッセージ認証によるデータ改ざんの確認、デジタル証明書を利用した相互認証などの機能を実装する。

リモートアクセスには注意しなければならないさまざまな脅威が伴う

リモートアクセスVPNを導入する前に、まず、インターネット経由で社内ネットワークへリモートアクセスする場合に、どのような脅威が存在するのかを知る必要があるだろう(図1)。一般にリモートアクセスを行う場合には、次のように脅威に対して備えなければならない。

インターネット上での機密データの盗聴

社内ネットワークへリモートアクセスして送受信するデータは、機密扱いであることも多いだろう。リモートアクセスを行う際には、このようなデータをインターネット上で第三

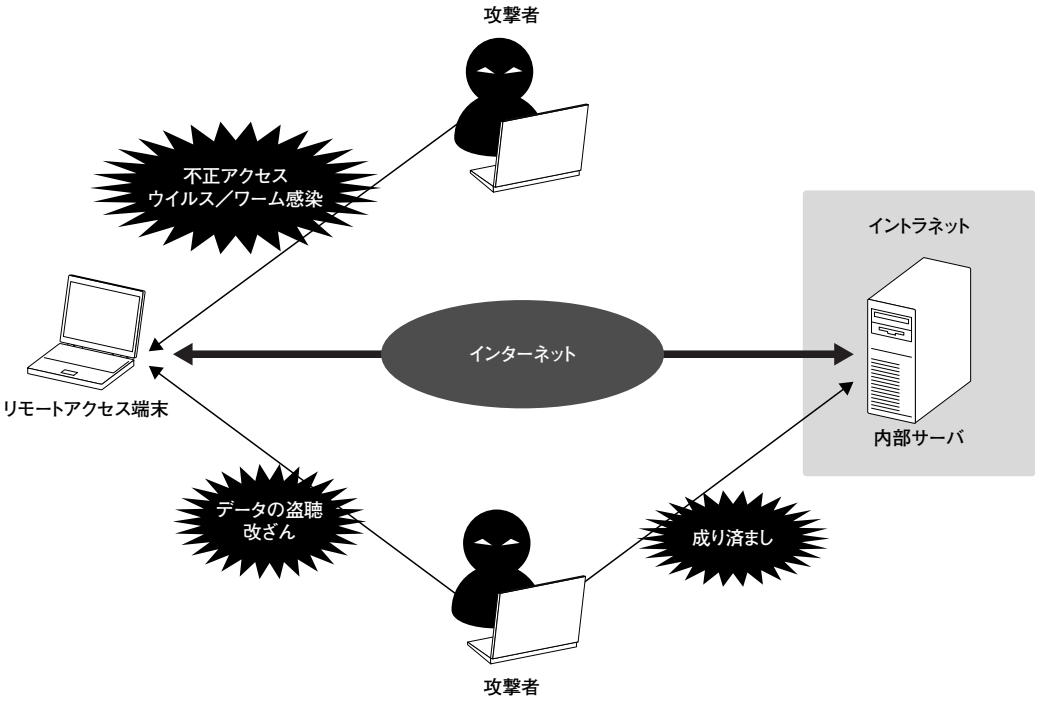

図1● リモートアクセス利用時にはさまざまな脅威がある

者に盗聴されないようにする仕組みが必要となる。

インターネット上での重要データの改ざん

インターネット上で第三者に重要なデータを改ざんされないようにする仕組みが必要となる。

正規リモートアクセスユーザーへの成り済まし

社内ネットワークへのリモートアクセスを許可する場合には、正規のユーザーからのアクセスのみを許可する必要がある。しかし、正規のユーザーの認証情報（パスワードなど）が漏えいすると、アクセスが許可されていない者が社内ネットワークへ侵入することが可能となってしまうため、強力なユーザー認証の仕組みが必要となる。

リモートアクセス端末への不正アクセス

リモートアクセスに使用する端末は、組織のファイアウォールで保護されていない場合が多いため、不正アクセスの被害にあいやすい。リモートアクセス端末が不正アクセスされると、そこを踏み台として社内ネットワークへ侵入されてしまう危険性がある。このため、リモートアクセス端末では、不正アクセス対策をしっかりと行っておく必要がある。

リモートアクセス端末のウイルスおよびワーム感染

リモートアクセスに使用する端末は、ふだんからウイルスやワームに感染しないように対策を講じておく必要がある。もし、ウイルスやワームに感染した端末を使用して社内ネットワークへリモートアクセスした場合、その端末から社内ネットワーク上のほかの端末へウイルスやワームの感染が拡大してしまう可能性があり、非常に危険である。

このように、インターネット経由でリモートアクセスを行う際にはさまざまな脅威が存在することがわかる。リモートアクセスVPNには、VPNを構築するための基本機能と、それらの脅威に対抗するための機能が必要となってくる。以下では、リモートアクセスVPNに必要な機能について述べる。

リモートアクセスVPNを実現するために必要となる基本機能

リモートアクセスVPNは、トンネリング機能や、ネットワーク情報自動設定機能、スプリットVPN機能といった基本的な機能が実装されることで実現可能となる。

トンネリング機能

トンネリング機能は、インターネット上に仮想的な通信トンネルを構築する機能であり、VPN技術には必須の機能である。これにより、リモートアクセス端末と社内ネットワークに設置されたVPN機器との間に仮想的な通信路（VPN）が構築される。

実際には、図2のようになる。最初に社内ネットワークあてのパケットに対して、社内ネットワークに設置されたVPN機器まで送信するための新しいヘッダを付加（これを「カプセル化」という）する。そのパケットを受信した社内ネットワークのVPN機器は、新しく付加されたヘッダを削除（これを「カプセル解放」という）したあとに、パケットを目的のホストに転送する。インターネット上では、新しく付加されたVPN機器あてのヘッダを使用してルーティングされるため、VPN機器にグローバルアドレスが付与されていれば、目的のホストでプライベートアドレスが使用されていても問題なくアクセスすることができる。

ネットワーク情報自動設定機能

リモートアクセスVPNを利用する端末には、社内ネットワークに存在する端末と同じ条件でアクセスできるように、社内ネットワークに存在する端末と同じネットワーク情報を設定する必要がある。

具体的には、リモートアクセスVPNの接続時に、VPN機器がリモートアクセス端末に対して割り当てる内部IPアドレス（社内ネットワークで使用しているアドレス）やネットマスク、DNSサーバのIPアドレスなどのネットワーク情報を通知しなくてはならない。リモートアクセス端末がVPN経由でアクセスする際は、その送信元IPアドレスとして、VPN機器から通知された内部IPアドレスを使用し、通知された社内ネットワーク上のDNSサーバを使用してアクセスを行う（図3）。

スプリットVPN機能

社内ネットワークあてのアクセスはVPN経由で行うが、インターネットあてのアクセスはVPN経由ではなく、端末から直接アクセス可能にする際には、スプリットVPN機能を利用する（図4）。また、スプリットVPN機能はリモートアクセスVPNに必須の機能ではない

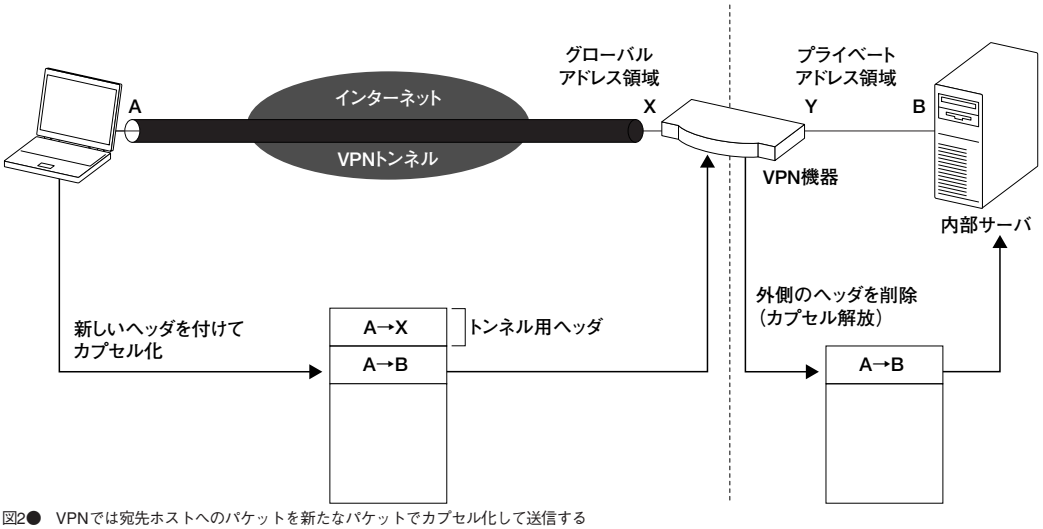

図2● VPNでは宛先ホストへのパケットを新たなパケットでカプセル化して送信する

が、この機能がない場合は、インターネットあてのアクセスでも必ずVPNを経由して社内ネットワーク経由でアクセスすることになってしまい、これがオーバヘッドとなってしまう。ただし、VPN接続において、リモートアクセス端末が組織のファイアウォールやプロキシによる適切なフィルタリングなしで直接インターネット上のサーバにアクセスする

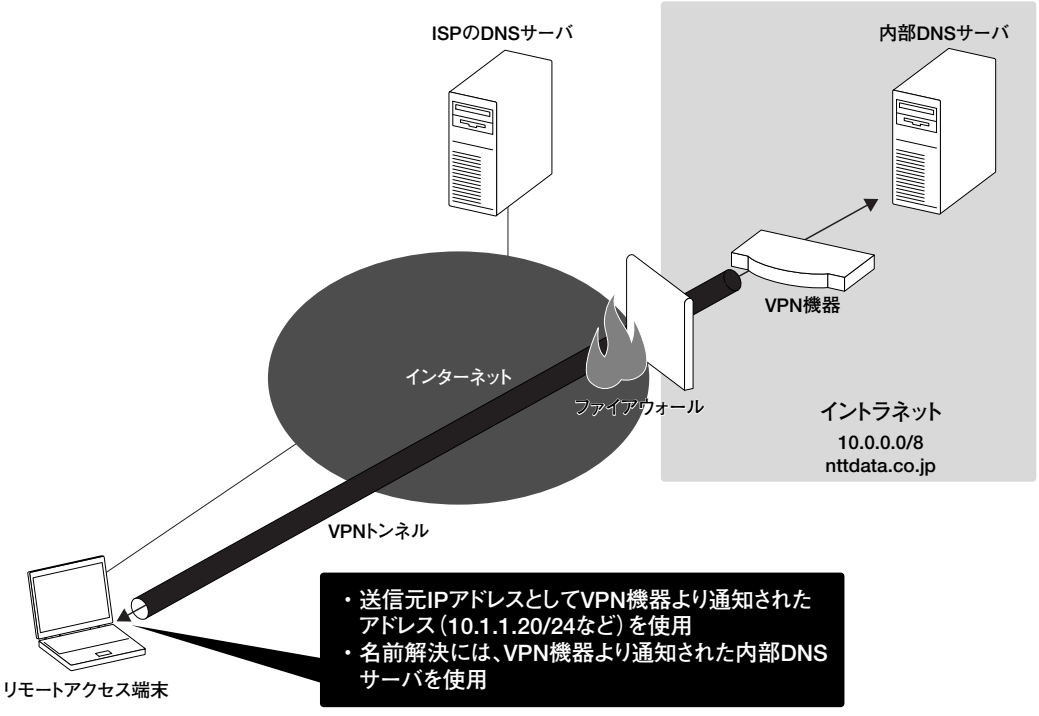

図3● リモートアクセス端末がVPN経由でアクセスする際には、VPN機器より通知されたIPアドレス、ネットマスク、DNSサーバのアドレスを使用する

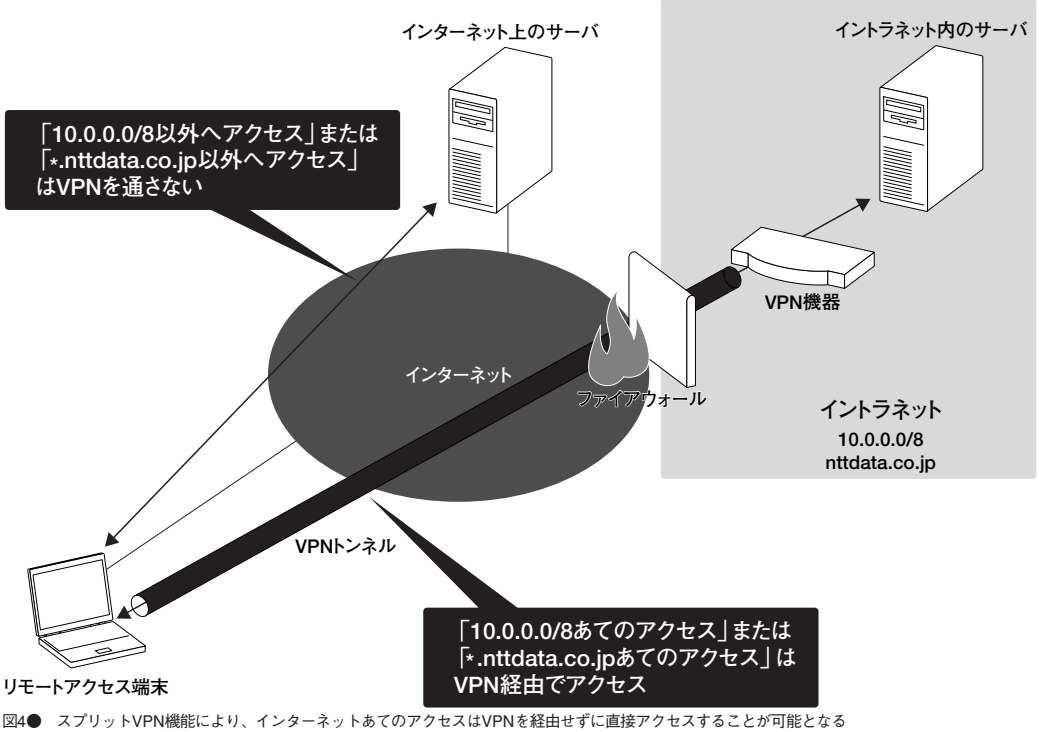

図4● スプリットVPN機能により、インターネットあてのアクセスはVPNを経由せずに直接アクセスすることが可能となる

と、ウイルスやワームに感染する可能性がある。また、感染後にVPN経由で社内ネットワークにアクセスして、被害を広げる可能性もある。このため、スプリットVPNの機能を使用するかどうかは慎重に検討する必要があるだろう。

インターネット上の脅威に対抗するためのセキュリティ機能

リモートアクセスを利用する場合に懸念されるセキュリティ上の問題として、データの盗聴や改ざん、正規リモートアクセスユーザーへの成り済ましなどがあげられるが、これらの問題は次の機能によって対策が講じられている。

暗号化機能

インターネット上での盗聴からデータを保護するために、カプセル化されたパケットを共通鍵暗号方式などで暗号化する機能が必要となる。パケットを暗号化することにより、インターネット上で通信を盗聴されても、その内容が第三者に漏えいすることを防ぐことが可能となる。ただし、パケットを暗号化しても、盗聴そのものを防ぐことはできないため、ぜい弱な暗号を使用していると、第三者に暗号化したパケットの内容を解読される可能性がある。このため、性能などを考慮しつつ、なるべく強力な暗号を使用する必要がある。

メッセージ認証機能

インターネット上でのデータの改ざんによる被害を避けるために、データの改ざんを検知するメッセージ認証機能が必要となる。メッセージ認証機能は、カプセル化されたパケットに、送信者（および受信者）のみが生成することが可能な署名（メッセージ認証コード）を付加し、その署名を受信側で検証することで、データの改ざんを検知することが可能となる。

鍵交換機能

リモートアクセス端末と社内ネットワークのVPN機器との間で暗号化処理やメッセージ認証処理を行うために必要な鍵をセットアップしたり、変更したりするための鍵交換機能が必要となる。鍵交換機能により、定期的に鍵を変更することが可能となるため、万が一、鍵が漏えいした場合でも、その被害はその鍵によって暗号化されたデータに関してのみにとどまることとなる。

ユーザー認証機能

拠点間VPNなどでは接続時に端末（VPN機器）を認証するが、リモートアクセスの場合は、ふだん持ち歩いているノートブックPCなどの端末そのものが盗まれる可能性があることや、インターネットカフェなどに設置されている共用端末からアクセスする場合もあるため、端末を認証するのではなく、リモートアクセスを行うユーザー自身を認証する機能が必要となる。

ユーザー認証の方式には、ダイヤルアップ接続などで用いられる**PAP**や**CHAP**、**MS-CHAP**を使用する方法や、米国RSAセキュリティの「SecurID」、米国セキュアコンピューティングの「SafeWord」などの認証トークンを使用する方法、ICカードやUSBトークンなどを使用する方法などがある。

これまでに説明した機能は、リモートアクセスVPNプロトコルによって提供される機能であるが、リモートアクセスVPNプロトコルでは、リモートアクセス端末への不正アクセスやウイルスおよびワームの感染などへの対策は講じられていない。そこで、これらの脅威に対抗するために次のことをあわせて行っておく必要がある。

最新のセキュリティパッチの適用

リモートアクセス端末には、使用しているOSやアプリケーションソフトウェアのベンダ

PAP（Password Authentication Protocol）
PPPにおいて利用される認証プロトコル。認証時に利用されるパスワードなどは通信経路上を平文のまま送信される。

CHAP（Challenge Handshake Authentication Protocol）
PPPにおいて利用される認証プロトコルのひとつで、PAPとは違い、認証情報をチャレンジと呼ばれる乱数文字列を使って暗号化して通信を行う。

MS-CHAP（Microsoft Challenge HandshakeAuthentication Protocol）
マイクロソフトがCHAPを拡張して作成した認証プロトコル。

ーから提供されている最新のセキュリティパッチを適用しておき、不正アクセスやワームなどの侵入口をふさいでおく必要がある。

アンチウイルスソフトの導入と、最新のウイルス定義ファイルの更新

最新のセキュリティパッチを適用していても、電子メールで送信されてきたウイルスプログラムを手動で実行してしまった場合などは、ウイルスの感染を防ぐことはできない。このため、リモートアクセス端末にはアンチウイルスソフトを導入しておき、ウイルスやワームの侵入をリアルタイムで検知できるようにしておく必要がある。また、アンチウイルスソフトのウイルス定義ファイルは常に最新の状態にしておく必要がある。

パーソナルIDS／ファイアウォールの導入

不正アクセスやワームの被害を受けないようにするため、リモートアクセス端末には、パーソナルIDSやパーソナルファイアウォールを導入しておくとよい。

リモートアクセスを受ける側では、これらのような仕組みがリモートアクセス端末に導入されているかどうかをチェックする機能があるとよいだろう。具体的には、クライアントからリモートアクセス要求があった場合に、リモートアクセス端末に対してセキュリティチェックを行い、チェック結果がOKだった場合のみVPN接続を許可するというような仕組みである。セキュリティチェックでは、次のような項目をチェックするとよい。

- **最新のセキュリティパッチが適用されているかどうか**
- **アンチウイルスソフトが動作しているかどうか**
- **アンチウイルスソフトのウイルス定義ファイルが最新であるかどうか**
- **パーソナルIDSソフトが動作しているかどうか**
- **パーソナルIDSのシグネチャファイルが最新であるかどうか**
- **パーソナルファイアウォールソフトが動作しているかどうか**

既存のネットワークへリモートアクセスVPNを導入する際の注意点

リモートアクセスVPNを既存のネットワーク環境へ導入する場合、事前に、次の項目の確認を行っておく必要があるだろう。

使用するVPNプロトコルのファイアウォールでの許可

リモートアクセス端末がファイアウォールで保護されたネットワークに接続されている場合、VPNプロトコルが、そのファイアウォールを越えてアクセスできなければならない。例えば、IPsecでは、500/UDP（IKE）および50/IP（ESP）などのプロトコルを使用するが、これらのプロトコルを使用した外部へのアクセスを、リモートアクセス端末が接続されているネットワークのファイアウォールで許可している必要がある。

使用するVPNプロトコルがNATを介する場合

リモートアクセス端末がプライベートアドレスを使用したネットワークに接続されており、外部へは**NAT**を介してアクセスするような環境から利用する場合は、使用しているVPNプロトコルがNATを通過できるものであるかどうかを確認しておく必要がある。

NAT（Network Address Translator）
グローバルアドレスとプライベートアドレスを相互に変換する機能。この機能により、プライベートアドレスが割り当てられたノードから透過的に、グローバルアドレスが用いられるインターネットへのアクセスが可能となる。

リモートアクセスVPNを実現する技術には、さまざまなものがあるが、現在、代表的なものとしてはIPsec、PPTP、L2TP、SSLなどがある。

次回からは、これらの技術を用いてリモートアクセスVPNを実現するための仕組みや運用方法について順に解説していく。

NTTデータ　馬場達也