VPN環境を構築する前に学んでおこう

ここが知りたいVPN

本連載では、これからリモートアクセス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に利用されている技術、すなわちIPsecやPPTP、L2TP、SSL-VPNについて、それらの技術的な特徴や違いをわかりやすく解説していく。今回は、PPTPを使用したリモートアクセスVPNについて説明する。　馬場達也

第4回　PPTPを使用したリモートアクセスVPNの仕組み

Supplement

■PPTP（Point-to-Point Tunneling Protocol）
マイクロソフトなどが提唱した、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（Point-to-Point Protocol）
電話回線などを使用して、コンピュータをインターネットなどのネットワークへダイヤルアップ接続するのに一般的に使われるデータリンク層プロトコル。上位プロトコルとして、TCP/IPなどさまざまなネットワーク層プロトコルを運ぶことができる。

■IETF（Internet Engineering Task Force）
インターネットで利用される、プロトコルなどの技術を標準化する団体。標準化された技術仕様は、RFC（Request For Comments）として公開される。

■L2F（Layer 2 Forwarding）
シスコシステムズが開発した、インターネットを利用したリモートアクセスVPNを実現するためのプロトコル。

■L2TP（Layer 2 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。

PPTPはPPPをトンネリングするためのプロトコル

PPTPは、マイクロソフトを中心として、アセンド・コミュニケーションズ（現ルーセント・テクノロジー）、USロボティックス（現スリーコム）などが開発した、**PPP**フレームをIPネットワーク上で交換できるようにするためのプロトコルである。PPTPは**IETF**標準のプロトコルではなく、シスコシステムズが提案した**L2F**と統合されて**L2TP**として標準化されたが、Windows標準のクライアントを利用して手軽にVPNを構築できることから、現在でも多くのVPN製品で採用されている。PPTPの仕様は、RFC 2637に記述されている。

PPTPでは、PPTPトンネルを制御するための「PPTP制御コネクションプロトコル」と、PPPフレームをIPネットワーク上でやり取りするための「PPTPトンネルプロトコル」の2種類のプロトコルを使用する（表1）。

PPTPはインターネット経由でのPPP接続を提供する

ここでは、PPTPが提供する主な機能について解説する。

プロトコル名称	プロトコル番号など
PPTP制御コネクションプロトコル	1723/TCP
PPTPトンネルプロトコル	プロトコル番号47

表1●　PPTPで使用されるプロトコルの種類

■トンネリング機能

PPTPのトンネリング機能を利用すると、インターネット経由でPPP接続を行うことが可能となり、VPNを構築することができる。では、PPTPのトンネリング機能とは具体的にどのようなものだろう。

PPTPは、PPPフレームを**GRE**でカプセル化する（図1）。PPPは、ダイヤルアップ接続などの際に使用されるデータリンク層のプロトコルであり、PPP上ではIPを含むさまざまなネットワーク層のプロトコルを使用することができる。

GREの仕様は、RFC 1701および2784に記述されているが、PPTPでは、このGREを修正したものを使用している。オリジナルのGREのバージョン番号は「0」であるが、PPTPで使用するものはバージョン番号が「1」となっているため、これ以降はPPTP用に修正されたものを「GREv1」と呼ぶ。GREv1ヘッダは、図2のようなフォーマットになっており、バージョンフィールドにはGREのバージョンである「1」が、プロトコル番号フィールドにはカプセル化するPPPのプロトコル番号である「0x880b」が入る。

また、ペイロード長フィールドには、カプセル化する「PPPフレームのサイズ（バイト数）」が入り、コールIDフィールドには、PPTP制御コネクションの確立時に決定された「コールID」が入る。このコールIDは、PPTPクラ

図1● PPTPではPPPフレームをGREでカプセル化する

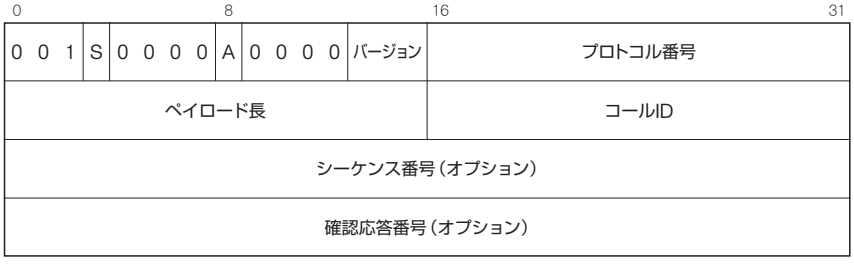

図2● PPTPで使用されるGREv1ヘッダのフォーマット

イアントからPPTPサーバに送信する場合と、PPTPサーバからPPTPクライアントに送信する場合とでそれぞれ異なるものが使用される。また、図2の中の「S」ビットが「1」のときにはシーケンス番号フィールドが存在し、送信するPPTPトンネルパケットの「シーケンス番号」が入る。そして、図2の中の「A」ビットが「1」のときには確認応答番号フィールドが存在し、これまでに受信したPPTPトンネルパケットの「シーケンス番号の最大値」が入る。

■ネットワーク情報自動設定機能

PPTPでは、PPPの**IPCP**によって提供されるネットワーク情報自動設定機能を使用する。IPCPにより、PPTPクライアントは、PPTPサーバからクライアントが使用する内部IPアドレスや内部DNSサーバのアドレス、内部WINSサーバのアドレスを取得することができる。

■暗号化機能

PPTPには仕様として暗号化機能が備わっていない。したがって、通常は暗号化プロトコルとして**MPPE**を使用する。MPPEの仕様はRFC 3078に記述されている。MPPEでは、PPPのデータ部分、つまり、PPP上でIPを使用するのであればIPパケット全体を**RC4**で暗号化する。

また、MPPEはIPパケット全体を暗号化するため、送信するデータだけでなく、TCPヘッダやUDPヘッダなどのトランスポート層プロトコルのヘッダも隠すことが可能となる。そのため、どのようなプロトコル（サービス）を利用しているかを第三者から隠すことができる。

■鍵交換機能

MPPEで使用される暗号化用の秘密鍵は、PPPのユーザー認証プロトコルである**MS-CHAP**、**MS-CHAP v2**、**EAP-TLS**によって自動的にセットアップされる。また、MPPEでステートレスモードを選択した場合は、PPTPトンネルパケットを1パケット送信するごとに鍵が変更され、ステートフルモードを選択した場合は、256パケット送信するごとに鍵が変更される。

■ユーザー認証機能

PPTPでは、PPPのユーザー認証機能を使用する。ユーザー認証方式としては、**PAP**、**CHAP**、MS-CHAP、MS-CHAP v2、EAP-TLSなどが利用できるが、MPPEによる暗号化を行う場合には、MS-CHAP、MS-CHAP v2、EAP-TLSのいずれかを使用する必要がある。MS-CHAPおよびMS-CHAP v2は、ユーザー名とパスワードを使用して、チャレンジレスポンス方式でユーザーを認証する。一方、EAP-TLSは証明書を使用してユーザーを認証する。

なお、MS-CHAPには、ユーザー側の認証のみを行いサーバ側の認証は行わないという問題や、MPPEで使用する暗号化鍵が毎回同じになるという問題があるため、MS-CHAP

Supplement

■GRE（Generic Routing Encapsulation）
シスコシステムズが開発した、ほかのプロトコルのパケットをIPパケットにカプセル化するためのフォーマット。

■IPCP（Internet Protocol Control Protocol）
PPPにてTCP/IPを利用する際に用いられるIP制御プロトコル。IPアドレスやヘッダなどの圧縮方法の設定を行う。

■MPPE（Microsoft Point-To-Point Encryption）
マイクロソフトが開発した、PPPフレームのデータ部分を暗号化するプロトコル。

■RC4（Rivest's Cipher 4）
RSAセキュリティのRivest氏が開発した、ストリーム暗号化アルゴリズム。

■MS-CHAP（Microsoft Challenge Authentication Protocol）
マイクロソフトがCHAP（次ページSupplementを参照）を拡張して作成した認証プロトコル。

■MS-CHAP v2（MS-CHAP version 2）
MS-CHAPの新しいバージョン。MS-CHAP v2では、相互認証やより強力な初期データ暗号化キーが利用可能となっている。

■EAP-TLS（Extensible Authentication Protocol-Transport Layer Security）
PPPを拡張した認証プロトコルの1つで、認証方式としてTLSを使用する。電子証明書を利用してサーバとクライアントで相互認証を行うことができる。

■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。

Supplement

■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、サーバから送信されたチャレンジと呼ばれる乱数文字列とパスワードを組み合わせたものにハッシュを適用することによってレスポンスを生成し、その結果をサーバに送信する。レスポンスが盗聴されても、その内容から実際のパスワードは知ることはできない。

v2またはEAP-TLSを使用することが推奨されている。

PPTPでは提供されない機能

次にあげる機能は、PPTPによっては提供されない。

■メッセージ認証機能

PPTPには、悪意のある第三者によってメッセージが作成されたり、改ざんされたりしたことを検知するためのメッセージ認証機能は備わっていない。

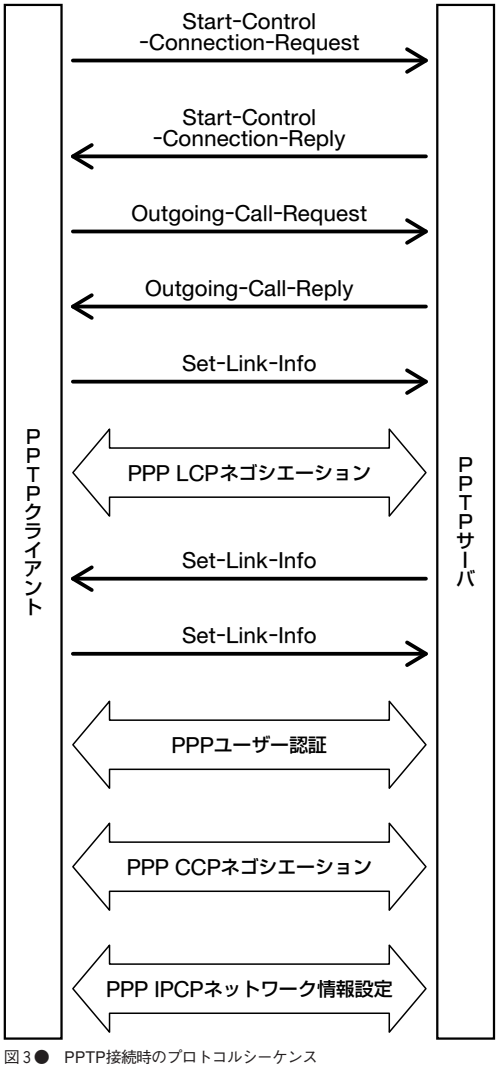

図3● PPTP接続時のプロトコルシーケンス

■リプレイ防御機能

PPTPには、悪意のある第三者が、正規のユーザーが送信したPPTPトンネルパケットを盗聴し、それを再び利用する「リプレイ攻撃」から防御する機能は備わっていない。

■スプリットVPN機能

PPTPでは、スプリットVPN機能は提供されない。このため、インターネットあてのアクセスであっても、すべてのアクセスはVPN経由で行われる。

PPTP接続ではPPTPトンネル構築や認証プロトコル／暗号化などのネゴシエーションが行われる

それでは、PPTP接続時の処理について具体的に見ていこう。基本的な処理の流れは次のようになる（図3）。

まず、PPTPクライアントはPPTPサーバの1723/TCPポートに接続し、PPTP制御コネクションプロトコルの「Start-Control-Connection-Request」メッセージを発行して、PPTP制御コネクションの開始を要求する。この要求に対して、PPTPサーバは「Start-Control-Connection-Reply」メッセージを返答し、PPTP制御コネクションが確立される。続いてPPTPクライアントは、PPTPクライアントからPPTPサーバに送信するPPTPトンネルパケットに付与するコールIDを含んだ「Outgoing-Call-Request」メッセージを発行する。これに対して、PPTPサーバは、PPTPサーバからPPTPクライアントに送信するPPTPトンネルパケットに付与するコールIDを含んだ「Outgoing-Call-Reply」メッセージを返答する。さらに、PPTPクライアントは「Set-Link-Info」メッセージをPPTPサーバに送信する。これにより、PPTPクライアントとPPTPサーバの間でPPTPトンネルが構築され、PPPフレームを送信することが可能となる。

このPPTPトンネルでは、PPPフレームが、

図4● PPTPにおけるPPPネゴシエーション時のフォーマット

図5● PPTPにおけるIPパケット送信時のフォーマット（網掛け部は暗号化されている）

GREv1を使用してカプセル化される。具体的には、PPPフレームにGREv1ヘッダと、PPTPトンネルのエンドポイント間（PPTPクライアントからPPTPサーバ）を運ぶためのトンネル用IPヘッダが付加される。なお、PPPネゴシエーション時のフォーマットは図4のようになる。

PPTPトンネルが構築されたら、PPPのリンク制御プロトコル（**LCP**）により、使用する認証プロトコルなどのPPPパラメータのネゴシエーションを行う。使用する認証プロトコルがネゴシエーションされると、その認証プロトコルを使用してユーザー認証が行われる。認証プロトコルとしては、PPTPでデータを暗号化する場合は、MS-CHAP、MS-CHAP v2またはEAP-TLSのいずれかを使用する必要がある。

さらに、PPPの圧縮制御プロトコル（**CCP**）により、PPTPで使用する暗号化鍵の鍵長や、ステートレスモードまたはステートフルモードのどちらを使うか、**MPPC**による圧縮を行うかどうかのネゴシエーションを行う。PPTPトンネルにおけるデータの暗号化にはMPPEが使用されるが、MPPEではデータの暗号化に40ビットまたは128ビットのRC4を使用する。使用するRC4の鍵長は、PPTPクライアントから1つ以上の値を提案し、PPTPサーバがその中から1つを選択することで決定される。両者とも128ビットのRC4が利用可能であれば、128ビットのRC4の使用が決定される。またCCPのネゴシエーションと並行して、PPTPクライアントはPPPのIPCPを使用し、PPTPサーバから内部IPアドレスの割り当てや、内部DNSサーバ、内部WINSサーバのアドレスの通知を受ける。

ここで注意したいのは、このフェーズまではデータが暗号化されていないため、MS-CHAPで送信するアカウント名や、割り当てられた内部IPアドレス、内部DNSサーバ、内部WINSサーバのアドレス、さらに使用している暗号化アルゴリズムの鍵長などが平文で流れてしまうことである（暗号化アルゴリズムは盗聴するまでもなくRC4とわかってしまう）。例えばIPsecでは、これらの内容をIKEフェーズ1で確立するISAKMP SAで暗号化するが、PPTPにはこのような機能はない。

PPTPトンネルではPPPフレーム中のIPパケットをRC4で暗号化

PPTP接続が完了すると、IPパケットなどのデータを含むPPPフレームが送信可能となる。IPパケットをPPTPトンネル経由で送信する場合は、まずIPパケットの直前に、4バイトのMPPEヘッダの後半2バイトぶんを構成するプロトコルフィールド（IPの場合は「0x0021」）が付加される。続いて、このプロトコルフィールドが付加されたIPパケット全体がRC4で暗号化される。ただし、MPPCによる圧縮を行う場合は、暗号化の前に圧縮が行われる。

次に、その暗号化されたデータにMPPEヘッダの残りの前半2バイトぶんとPPPヘッダが付加され、PPPフレームが作成される。このPPPヘッダのプロトコルフィールドには、MPPEを使用する場合は必ず「0x00fd（Compressed Datagram）」が入る。さらに、GREv1ヘッダと、PPTPトンネルのエンドポイント間を運ぶためのトンネルIPヘッダが付加され、PPPフレームがカプセル化される（図5）。

Supplement

■LCP（Link Control Protocol）
PPPにおけるコネクションの確立や切断、さらに認証プロトコルやパケット情報の設定などを行うプロトコル。

■CCP（Compression Control Protocol）
PPP接続時におけるデータ圧縮や、データ圧縮のネゴシエーション方法を規定するプロトコル。

■MPPC（Microsoft Point-to-Point Compression）
マイクロソフトが提唱する、PPPにおけるデータ圧縮方式。

Supplement

■NAPT（Network Address Port Translation）
NATと同様に、IPパケット中のIPアドレスを変換する機能。IPマスカレードとも呼ばれる。NATと異なるのはIPアドレスに加えポート番号も変換される点である。これにより1つのグローバルアドレスを複数のプライベートネットワーク内のホストで共有できる。

■NAT（Network Address Translator）
IPパケット中のIPアドレスを変換する機能。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。

PPP接続の切断とPPTP制御コネクションの切断によりPPTPは終了する

PPTP終了時の処理の流れは次のようになる（図6）。

PPTPクライアントは、PPTP制御コネクションを使用して、PPTPサーバに対して「Set-Link-Info」メッセージを送信する。さらに、PPTPトンネルを使用して、PPPのLCPの「Terminate-Request」メッセージを送信し、PPP接続の切断を要求する。これに対して、PPTPサーバはPPTP制御コネクションを使用して、PPTPクライアントに「Set-Link-Info」メッセージを送信する。さらに、PPTPトンネルを使用して、さきほどの「Terminate-Request」メッセージの返答として、LCPの「Terminate-Ack」メッセージをPPTPクライアントへ送信し、PPTPトンネルプロトコルによるPPP接続を切断する。

次に、PPTPクライアントは、PPTP制御コネクションを使用して、PPTPサーバに対して「Call-Clear-Request」メッセージを送信する。これに対して、PPTPサーバは「Call-Disconnect-Notify」メッセージをPPTPクライアントに返答する。さらに、PPTPクライアントは「Stop-Control-Connection-Request」メッセージを送信して、PPTP制御コネクションの切断を要求する。これを受けて、PPTPサーバは「Stop-Control-Connection-Reply」メッセージをPPTPクライアントに送信し、PPTP制御コネクションを切断する。ここまでの処理でPPTP接続は終了することになる。

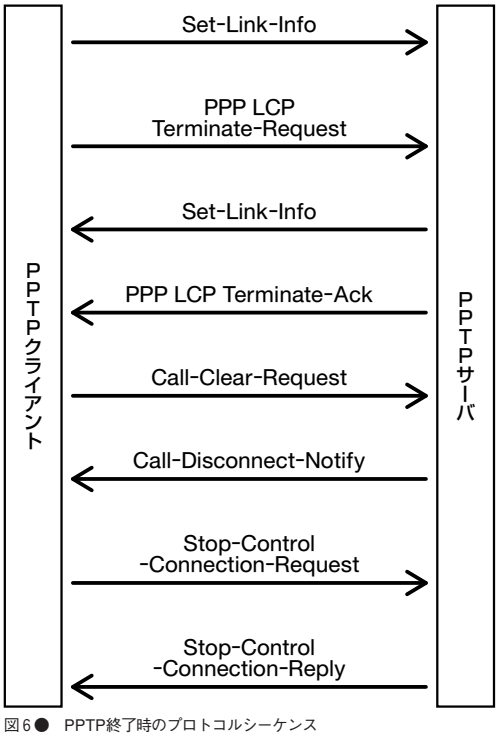

図6● PPTP終了時のプロトコルシーケンス

NATを介してPPTPを使うにはPPTPパススルー機能などが必要

PPTPでは、1723/TCPを使用するPPTP制御コネクションプロトコルと、IPプロトコル番号47（GRE）を使用するPPTPトンネルプロトコルを使用する。TCPを使用したPPTP制御コネクションプロトコルは、**NAPT**を含む**NAT**を問題なく通過することができるが、GREを使用するPPTPトンネルプロトコルにはTCPヘッダやUDPヘッダが存在しないため、通常はNAPTを通過させることができない。

しかし、最近のブロードバンドルータなどには、NAPTにPPTPパススルー機能が備わっており、これにより問題の解決が図られている。PPTPパススルー機能は、PPTPクライアントから送信されるPPTPトンネルパケットの送信元IPアドレスのみを変更して送信する一方で、外部から受け取ったPPTPトンネルパケットは、受け取る直前にそのPPTPサーバあてにパケットを送信したPPTPクライアントへ転送するというものだ。

ただし、NAPTの背後に存在する複数のPPTPクライアントが特定のPPTPサーバに対して同じタイミングでパケットを送信した場合には、PPTPサーバは外部から受け取ったパケットをどのPPTPクライアントへ転送すればよいのか判断できないという問題が生じる。このため、NAPTにおいては、複数のPPTPクライアントが付与するコールIDが、同一のPPTPサーバに対して重複しないように変換し、さらに、PPTPサーバから送信さ

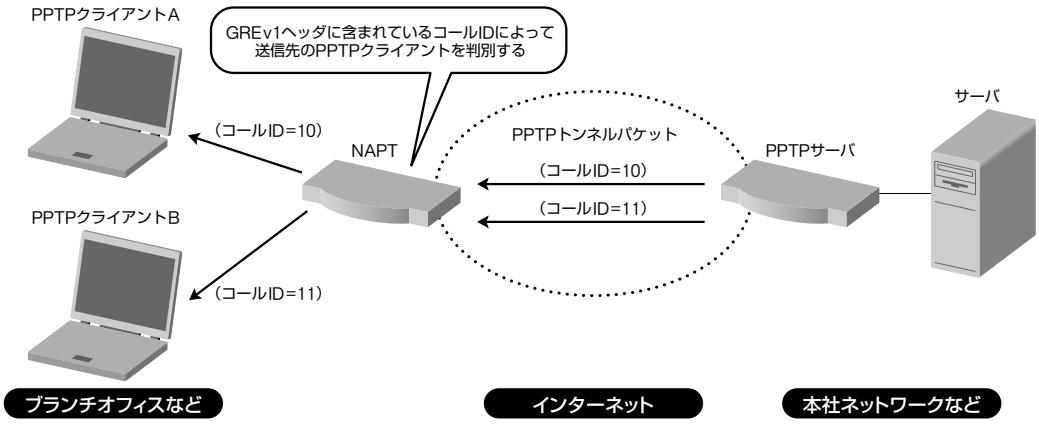

図7● NAPTではコールIDによって送信先PPTPクライアントを判別する

れたPPTPトンネルパケットのGREv1ヘッダに含まれるコールIDを参照し、送信先のPPTPクライアントを判別できる機能が必要となる(図7)。

PPTPによるリモートアクセスVPNを導入する際の注意点

PPTPを使用したリモートアクセスVPNを導入する場合は、企業ネットワーク側に、PPTP-VPNを確立するための「PPTPサーバ」、ユーザー認証を行うための「**RADIUS**サーバ」が必要となる(次ページの図8)。ただし、PPTPサーバ製品にはRADIUSサーバと同等の機能が組み込まれているものも多いので、導入する製品の機能を事前にチェックしておくとよいだろう。またPPTP-VPNの場合は、Windows付属のPPTPクライアントソフトウェアを利用できるため、クライアントがWindowsの場合は特別なソフトウェアをインストールする必要はない。もし、クライアントにLinuxなどを使用している場合には、「http://pptpclient.sourceforge .net/」で提供されているPPTPクライアントなどを利用することができる。

さらにファイアウォールにおいて、PPTPクライアントからPPTPサーバへのPPTP制御コネクションプロトコル（1723/TCP）および両方向のPPTPトンネルプロトコル（IPプロトコル番号47）の通過を許可するように設定する必要がある。また、NAPTを使用する場合は、PPTPパススルー機能のあるものを選択する必要がある。

PPTPの設定では、認証プロトコルとしてMS-CHAP v2またはEAP-TLSを選択する。MS-CHAPは、サーバ側の認証を行わないという問題や、最初に生成される暗号化鍵が毎回同じになるという問題があるため、利用しないほうがよい。また、暗号化鍵の鍵長は128ビットのみを使用し、強度の弱い40ビットは選択しないようにする。さらに、MPPEのモードは1パケットごとに鍵を変更するステートレスモードを選択するとよいだろう。なおWindowsでは、デフォルトでステートレスモードをネゴシエーションするようになっている。

多くのプロトコルをカバーするがセキュリティ面が弱点

これまで、PPTPのリモートアクセスVPN機能について述べてきたが、最後にPPTPを使用したリモートアクセスVPNの長所と短所についてまとめてみる。

■長所

- **PPPレベルでセキュリティが確保できるので、IPを使用するアプリケーションはもちろん、IPXやAppleTalkなどのプロトコルを使用したアプリケーションの通信データ**

Supplement

■RADIUS（Remote Authentication Dial In User Service）
米国リビングストンが開発した、ダイヤルアップユーザー認証方式。RFC 2138/2139にて標準化されている。ユーザー情報をデータベースで管理する。

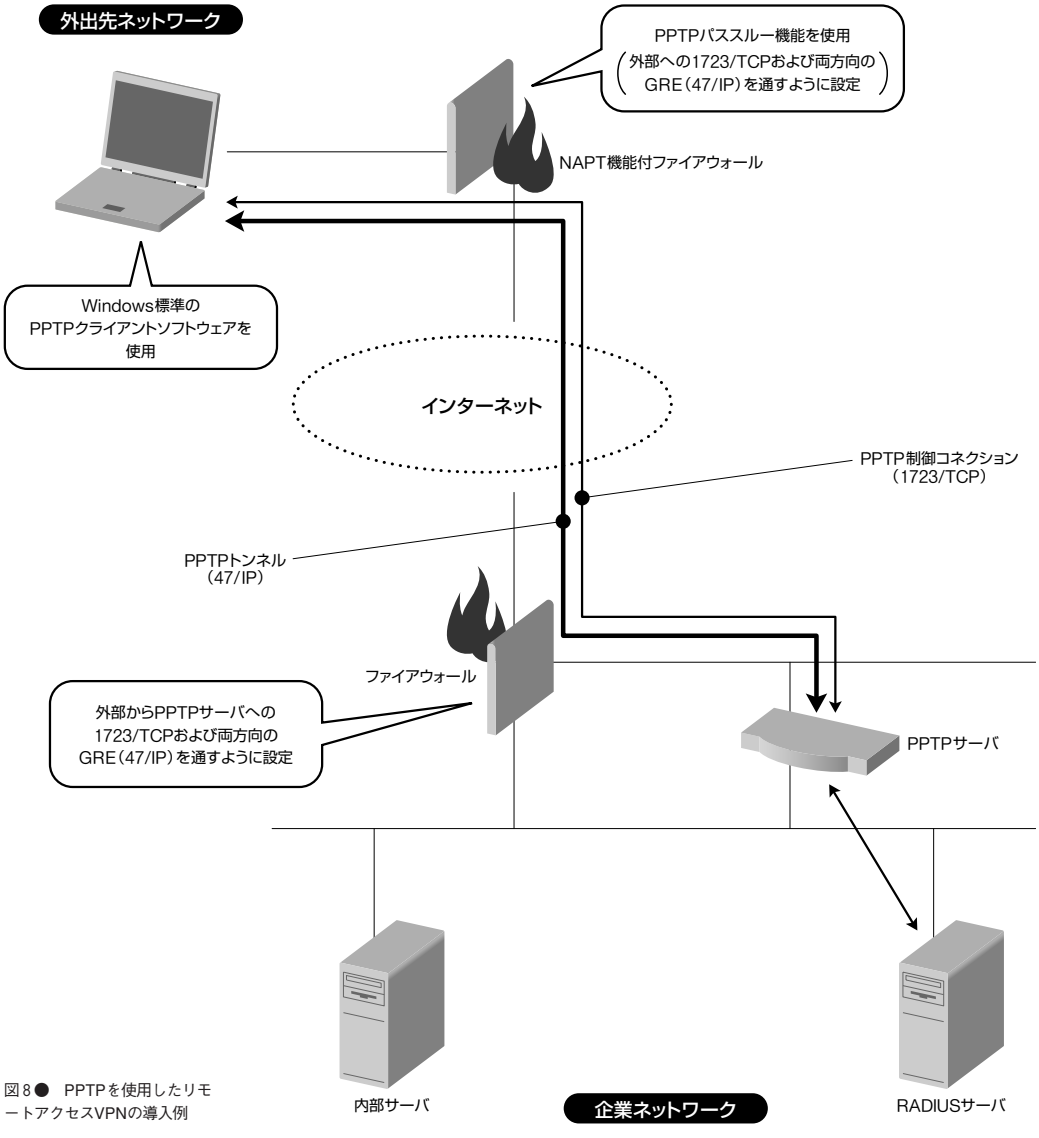

図8● PPTPを使用したリモートアクセスVPNの導入例

も保護することができる。

・Windows標準のクライアントソフトウェアが利用できるため、クライアントソフトウェアのインストールに手間がかからない。

■短所

・PPTPには、メッセージ認証機能が備わっていない、暗号化アルゴリズムがRC4しか利用できない、最初のセットアップの内容が暗号化されないなど、ほかのVPNプロトコルと比較してセキュリティ面で不安がある。

・ファイアウォールを介する場合は、PPTP制御コネクションプロトコル（1723/TCP）およびPPTPトンネルプロトコル（IPプロトコル番号47）の通過を許可するように設定しておかなければならない。このため、リモートアクセスユーザーは、自分で設定する権限のない外部のファイアウォールで保護されたネットワークからは通常はVPN接続することができない。

以上、PPTPを用いたリモートアクセスVPNについて述べた。次回は、L2TP-VPNについて解説する。

NTTデータ　馬場達也