インターネット最新テクノロジー：第４回

インターネット経由で離れたLANに接続する PPTP（Point-to-Point Tunneling Protocol）

インターネットはTCP/IPでデータをやり取りするが、実はほかのプロトコルもやりとりする方法がある。インターネット上でTCP/IP以外のプロトコルがやり取りできれば、プロバイダーにダイアルアップ接続して会社のファイルサーバーに置いてあるファイルを共有できて大変便利だ。これはPPTPという技術を使った方法で、96年12月に発売されたウィンドウズNT4.0でもサポートされている。今回はこのPPTPについて解説しよう。

池田 健二（インプレスグループ・ラボ）
ikeda@impress.co.jp

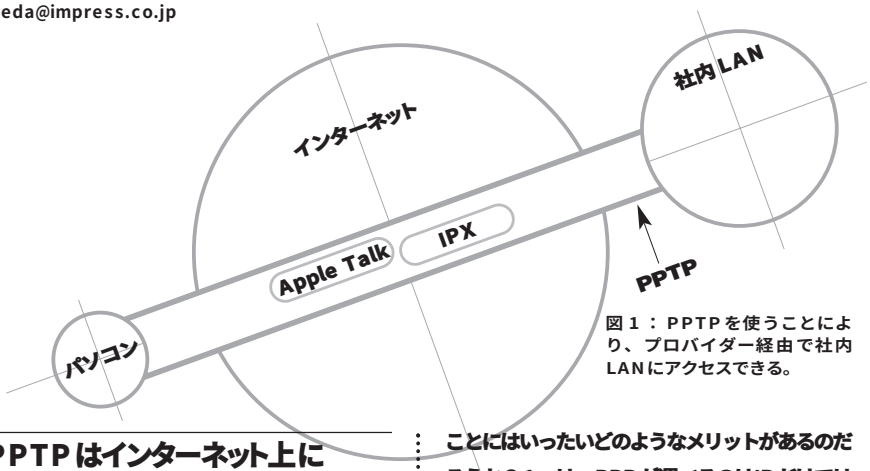


図１：PPTPを使うことにより、プロバイダー経由で社内LANにアクセスできる。

PPTPはインターネット上に仮想的なトンネルを作る技術

PPTPはPoint-to-Point Tunneling Protocol（ポイント・ツー・ポイント・トンネリング・プロトコル）の略で、IPしか中継しない現在のインターネット上に仮想的なトンネルを作り、PPPパケットをそのまま送るプロトコルだ。

ダイアルアップでおなじみのPPPはTCP/IPをやり取りするのに使われている。当然、モデムに送られているパケットはPPPパケットで、その中身はIPだ。つまり、PPPパケットそのものはIPではないので、PPPパケットそのものをインターネットで中継するにはトンネリングが必要となる。

PPPパケットをトンネリングで遠隔地に運ぶことにはいったいどのようなメリットがあるのだろうか？1つは、PPPが運べるのはIPだけではなく、パソコンで使われているファイル共有やプリンター共有のプロトコルであるIPX、AppleTalkといったプロトコルもインターネットを経由して送れることを意味している。

もう1つは、企業などでファイアーウォールがある場合、インターネットから企業内のネットワーク（イントラネット）に入るのは不可能である。このような場合には企業内にTAやモデムを設置し、長距離電話の料金を覚悟すれば、安全にイントラネットにアクセスできる。ところがPPTPを使えばインターネットからでも安全にアクセスでき、用意すべきモデムや電話回線、電話料金およびそれらのメンテナンスコストを抑えることができる（図1）。

PPPとPPTPの関係

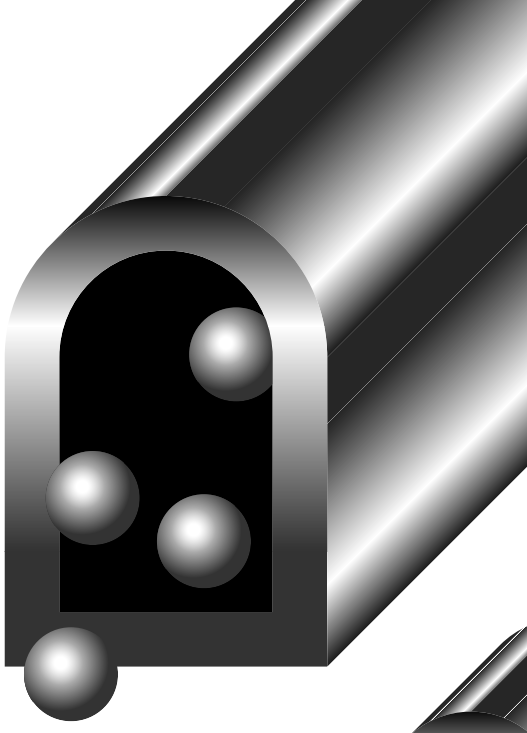
ダイアルアップ接続するときに使うプロトコルはPPPがすでに標準である。この点から、PPPはダイアルアップ用のプロトコルだと誤解されていることがあるが、PPPはPoint-to-Point Protocolの略であることを思い出してほしい。このPoint-to-Pointとは、2つの機材をシリアル回線で接続した形態を指す。いつも使っているパソコンとプロバイダー側の機材の接続だけではなく、デジタル専用線を使った2台の専用ルーター間の接続もPoint-to-Pointと呼ばれ、これらのルーター間の接続プロトコルも実はPPPが使われている（図2）。つまり、シリアル回線で接続された対向2台の間で使われる通信プロトコルがPPPで、その2台間のパケットをそのままるごと遠隔地に送るためのプロトコルがPPTPだ。

トンネリングはIPの中に違うプロトコルを入れて送る技術

パソコンで主に使用されているファイル共有やプリンター共有などのプロトコルはTCP/IPではないため、インターネットを越えて使用することができない。最近はパソコンのOSがTCP/IPに対応してこれらの共有プロトコルそのものが拡張され、直接TCP/IPを使ってファイル共有やプリンター共有ができるようになってきている。しかし古くからあるソフトウェアも有効に活用するためには、インターネットを経由した場合でもIP以外のプロトコルが扱えたほうが便利だと言える。

こうした要望を実現するのがトンネリングの技術で、IPしか中継しないインターネット上に仮想的なトンネルを作り、そのトンネルを通してIP以外のプロトコルを送る。受け手では、IPのパケットから元のデータを取り出すことで、最終的なプロトコルをやり取りできるのである。

こうした方法は古くからあり、RFC 1234の「Tunneling IPX Traffic through IP Networks」



[9]などでその具体的なプロトコルが公開されている。これ以外にもさまざまなトンネリングプロトコルが考案されてきたが、1996年6月13日付でPPTPのドラフト「Point-to-Point Tunneling Protocol--PPTP」[9]が公開されている。従来のトンネリングプロトコルと同様、PPTPもいろいろなプロトコルをインターネット経由で送ることを目的としており、さまざまな点でこれまでのトンネリングプロトコルより優れている。

PPTPはほかのプロトコルをカプセル化して送出する

IPでないパケットをインターネットで中継してもらうためにはどのような方法があるだろうか？必然的な条件がIPのパケットであることなので、IPが運ぶデータとして目的のパケットをまるごと入れてしまえばとりあえずは送ることができる。別の表現を使えば、目的のパケットをIPで包んで送ればよい。こうした包んで送る方法はカプセル化と呼ばれる。

カプセル化すれば中にどのようなプロトコルのパケットが入っていようと問題なく送れる。しかしカプセル化することはIPのヘッダーなどを付加することであり、中継されるパケットが大きくなる。たとえば、目的のパケットが1,500オクテットだった場合、当然これよりも大きなIPのパケットができ、もしその機器がイーサネットに接続されていた場合は、イーサネットの上限である1,500オクテットを超えているので2パケットに分割せざるをえなくなり、結果的にはパケット数が増えデメリットとなる。

カプセル化以外の方法としては、IPに備わっているソースルートを使う方法もあるが、送りたいプロトコルがIPに限定されることもあって、現在の主流はカプセル化方式である。PPTPは当然カプセル化方式を採用している。

PPTPでは拡張GREを使用

これまでの多くのトンネリングプロトコルは、主にUDPで実際のデータの転送を行っていたが、PPTPでは図3に示すようにRFC1701のGRE（Generic Routing Encapsulation）[8]を拡張してデータ転送に使用している。この拡張GREではフロー制御と輻輳制御が実現されており、これまでのUDPを使った搬送と比べて、混雑したインターネットをより有効に使える。

トンネル以外にも通信している

PPTPでは前述した拡張GREでユーザーデータを運ぶ。そのトンネルを制御するために実はもう1つ別のコネクションが使用される。この制御コネクションにはTCPが使われ、サービスポート番号は5678である。ダイアルアップ用の電話回線が接続されているPAC（PPTP Access Concentrator）から、企業内に設置されているPNS（PPTP Network Server）に向かってこの制御コネクションが張られ、ここを通して行われる操作は大きく分けて4つある（表1）。

その中の「9.Incoming-Call-Request」は、実際にPACにダイアルアップ接続されたときにPNSに送られるコントロールメッセージで、ダイアルアップしてきた発信者の電話番号（ISDNの場合）が含まれている。また、ダイア

表1：PPTPのコントロールメッセージ・コード

Control Connection Management	
1	Start-Control-Connection-Request
2	Start-Control-Connection-Reply
3	Stop-Control-Connection-Request
4	Stop-Control-Connection-Reply
5	Echo-Request
6	Echo-Reply
Call Management	
7	Outgoing-Call-Request
8	Outgoing-Call-Reply
9	Incoming-Call-Request
10	Incoming-Call-Reply
11	Incoming-Call-Connected
12	Call-Clear-Request
13	Call-Disconnect-Notify
Error Reporting	
14	WAN-Error-Notify
PPP Session Control	
15	Set-Link-Info

●PPTP　draft-ietf-pppext-pptp-00.txtから抜粋

図2：専用線による常時接続でも、ルーター間の接続にはダイアルアップと同じようにPPPで接続する。

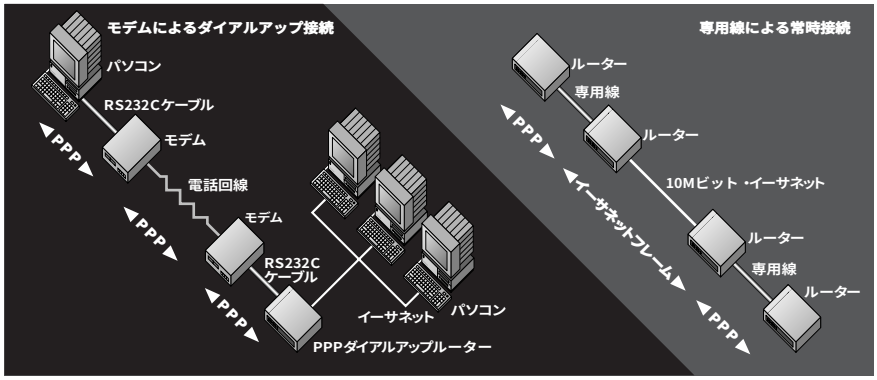
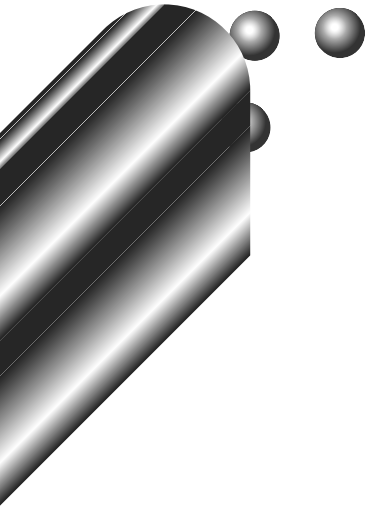


図3：PPTPパケットの構造／PPTPはPPPパケットを転送するために拡張したGREを使う。

Mediaヘッダー	IPヘッダー	GREヘッダー	PPPヘッダー	PPP Payload（転送するデータ）



ルアップしてきたクライアントとPACとの間のコネクションが切れた場合にPNSに通知する機能（13.Call-Disconnect-Notify）もある。これらの点から、PPTPはダイアルアップPPPをトンネリングすることを強く意識したプロトコルであると言える。

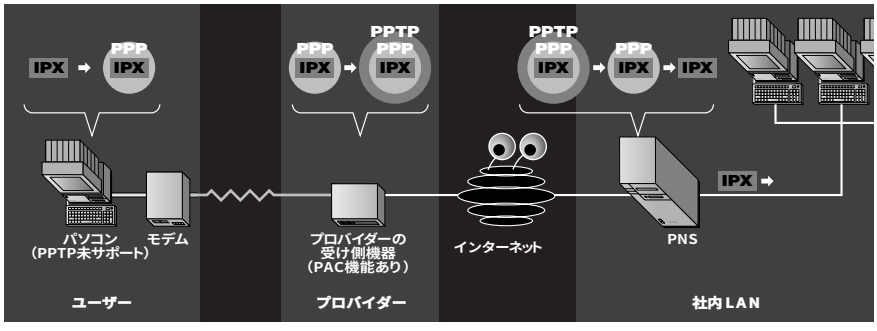
多くのプロトコルに対応

PPTPはカプセル化したデータをトンネリングで送る。このカプセル化するという点から、扱いたいプロトコルの数が増えればその数だけカプセルの形式を定義しなければならず、その開発に時間がかかる。しかし複数のプロトコルをカプセル化する標準的な方法はすでに開発されている。そう、PPPだ。

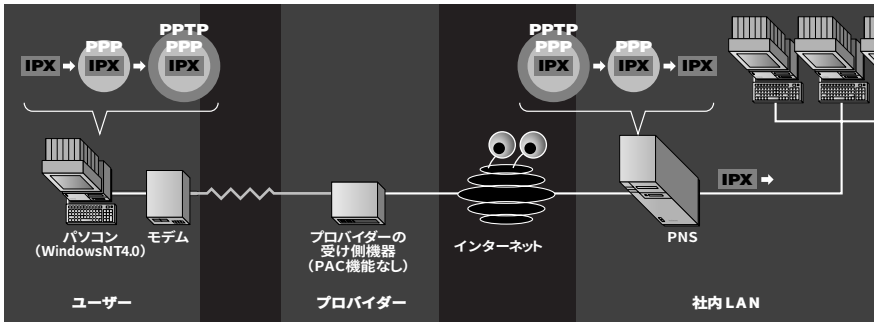
PPPは「扱えないプロトコルはない」と言えるほど、ほとんどすべてのプロトコルを転送できる。つまりPPPをトンネリングすれば、新規開発の苦労なしにあらゆるプロトコルを送ることができる。また、今後も新しいプロトコルを扱うためにPPPは拡張され続けると予測でき、将来性を考えても申し分ない。こうした点からPPTPではPPPをトンネリングしており、PPTPのマルチプロトコル機能は実はすべてPPPの機能だ。PPTPで新たに規定しているのは、PPPパケットを送る通信路（トンネル）とその制御に関してだけだ。

図3：PPTPではさまざまなプロトコルのデータ（図の場合はIPX）をカプセル化して送出する。PNSでは、受け取ったパケットから元のプロトコルに戻す。ウィンドウズNT4.0をクライアントにすれば、プロバイダーがPPTPをサポートしていなくてもPPTPが使える。

●PPTPをサポートしないクライアントパソコンを使う場合



●クライアントパソコンにウィンドウズNT4.0を使う場合



認証と暗号化のしくみ

PPTPのマルチプロトコル対応と同じく、PPTPのユーザー認証とデータ暗号化もPPPの機能だ。ユーザー認証においては、クライアントから送られたPPPパケットをPACでPPTPに変換してPNSに送る。PNSではPPTPパケットをPPPに戻し、ユーザーの認証が行われる。認証がPACを越えて行われるが、クライアントから見れば通常のPPPとまったく同様であり、いつものPAPやCHAP、場合によってはRFC 1915の「Variance for The PPP Connection Control Protocol and The PPP Encryption Control Protocol」[9]が使われることもあるだろう。

通信するデータの暗号化に関してもPPTP自体は何も規定しておらず、すべてPPPの機能を使うことになる。PPPのデータ暗号化に関しては RFC 1968の「The PPP Encryption ControlProtocol（ECP）」[8]とRFC 1969の「The PPP DES Encryption Protocol（DESE）」[8]がプトロコルとして公開されてはいるが、後者のRFC 1969では56bitのDESが使われているため日本国内では使用できない。また、米国内でも実際にはそれぞれのシステムに依存した方法で暗号化が行われている場合が多い。

こうした暗号化の実装で現在最も簡単に入手できるものとしてはウィンドウズNT4.0が挙げられる。マイクロソフトが公開している技術資料[7][8][8]では、40bitのRC4が使われているとの記述がある。

ウィンドウズNT4.0のPPTP

PPTPはPPPをそのままトンネリングするので、PPPパケットを受け取る機器、つまりプロバイダー側のルーター機材がPACになるのが最も自然だと考えられる。この方法ならPPTPをサポートしていない従来のダイアルアップクライアントでもPPTPが利用できるメリットがあるが、プロバイダーに設置してある機材がPPTP対応であることが条件となり、普及していない現在では簡単に利用できない。しかしもう1つ方法がある。ダイアルアップするクライアント自身でPPTPを扱えるようにする方法だ。この場合、クライアントマシンがPPTPを送出する。

PPTPが扱えて最も入手が簡単なのはウィンドウズNT4.0である。現行ではウィンドウズNT4.0がPPTP対応クライアントになれる。つまり、ウィンドウズNT4.0自体が、内部から発生したPPPパケットをPPTPパケットに変換する機能を持っているのである（図4）。ウィンドウズNT4.0はPNSとしても、またPPTPクライアントとしても機能する。ただ、クライアントOSとしてのウィンドウズNTはそれほど普及していないのが実状で、エンドユーザーとしてはウィンドウズ95も対応してほしいものである。ウィンドウズ95をPPTP対応とするモジュールはマイクロソフトによると提供する予定はあるがいつごろ公開するかはまだ未定とのことだ。

PNSとPPTPクライアントになれるウィンドウズNT4.0だが、PACとはしては機能しないようだ。ウィンドウズ95で今すぐPPTPを使う場合は、プロバイダー側でのPPTP対応が必要だ。

マイクロソフトが提唱するVPN

企業内LANにインターネットからアクセスできるようにするにはセキュリティー上問題があり、多くの企業でファイアーウォールを設置して社内と社外を分離している。こうした制限はインターネット経由でアクセスするユーザーの認証、たとえばパケット単位でできれば解決するが、効率が劣り、またそうしたプロトコルを新規開発して普及を図らねばならず、現実的ではない。現実的な方法として、マイクロソフトが提唱しているVPN（Virtual Private Network）では、PPTPを使ってインターネット上に仮想のネットワークを作ることを狙いとしている。

ここで、PPTPではPNSにおいてPPPレベルのユーザー認証を行うことを思い出してほしい。つまり、パケットのルーティングを開始する前にユーザー認証を行うので、認証したトンネルからのパケットは無条件にルーティングしても基本的には問題ない。もう1つのセキュリティー上の問題は通信途中での盗聴や改竄、偽造だが、データの暗号化はPPPの機能やウィンドウズNTのRASで提供される機能などを使えばよく、またPPPでのユーザー認証はCHAPを使えばよいだろう。PPTPはこのようなインターネットを利用した企業ネットワーク作りに有効だと言える。

他のトンネリングプロトコル

PPTP以外で現在ドラフトになっているものとしては、L2F（Layer 2 Forwarding Protocol）[q]がある。L2FはPPTPとはかなり考え方が異なるが目的は同じである。L2FはシスコL2社のルーターなどに実装されているが、UDPでのトンネリングなど、PPTPよりも古いやり方である。しかし、L2Fを発展させたL2TP（Layer 2 Tunneling Protocol）[w]が現在ドラフトとして公開されており、PPTPと似たコントロールメッセージを使っているなどの点から、最終的にはPPTPと統合されると予測できる。

専用線への応用に期待

これまで見てきたように、現在のPPTPはダイアルアップでの利用を強く意識しているが、専用線での利用でも現在のプロトコルで十分と思える。しかし、イーサネットからパケットを受け取りPPTPに変換してイーサネットから送出するという実装は、時間切れで見つけられなかった。今後の開発・製品に期待したい。

●

参考文献
[❶] RFC 1234, Tunneling IPX Traffic through IP Networks
[❷] <draft-ietf-pppext-pptp-00.txt>, Point-to-Point Tunneling Protocol--PPTP
[❸] RFC 1701, Generic Routing Encapsulation (GRE)
[❹] RFC 1915, Variance for The PPP Connection Control Protocol and The PPP Encryption Control Protoco
[❺] RFC 1968, The PPP Encryption Control Protocol (ECP)
[❻] RFC 1969, The PPP DES Encryption Protocol (DESE)
[❼] <http://www.microsoft.co.jp/products/ntserver/ver40/tech/vpn_pptp.exe> (Word Document), PPTPによる仮想プライベートネットワーク
[❽] <http://www.microsoft.com/ntserver/pptpwp.exe> (Word Document), Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol
[❾] <http://www.microsoft.com/windows/common/nrpptp.htm>, PPTP and Implementation of Microsoft Virtual Private Networking
[❿] <draft-ietf-pppext-l2f-03.txt>, Layer Two Forwarding (Protocol) "L2F"
[⓫] <draft-ietf-pppext-l2tp-01.txt>, Layer Two Tunneling Protocol "L2TP"

［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