

PacketiX VPNってどんなソフト？



あのSoftEtherの後継版 新機能を追加し使い勝手も向上

ルーターがなくても、Windowsパソコンが2台あれば手軽にイーサネットVPNを構築できる「SoftEther」。そのSoftEtherの後継ソフト「PacketiX VPN 2.0」が2005年12月末に正式公開された。およそ2年ぶりの新版ということで、数多くの機能追加や強化が施されているという。いったい何が変わったのかを調査した。

「ねえねえ、このPacketiX VPN2.0ってどんなVPNソフトなのかな?『2005年12月28日から正式版の提供を開始』と書いてあるんだけど」——。編集部に送られてきた新製品リリースの山を整理していると、通りかかったデスクがその中の1枚をひょいと拾い上げて尋ねてきた。

「あの筑波大学の学生起業家・登大遊氏が開発したSoftEtherの後継ソフトだそうですよ」と私。

「へえ、そうなんだ。SoftEther1.0が出たのは、たしか2004年春だったから、ほぼ2年ぶりのバージョン・アップか。機能的にもかなり変わっているんだろうな」とデスクが話を振ってくる。

「そうですね」と話を合わせた私に、すかさずデスクがたたみかけてきた。「せっかくの機会だから詳しく調べて記事にしようよ。SoftEtherの後継版が出たということで気になっている読者も多いだろうからね」。

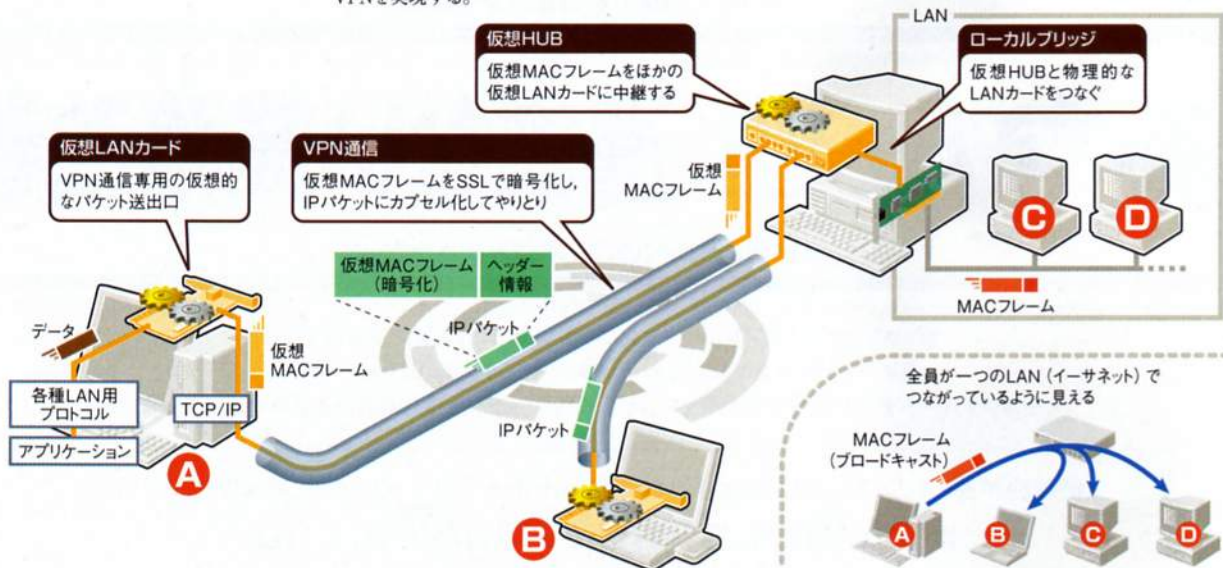
イーサネットLANを仮想的に実現

ADSLやFTTHなどブロードバンド・サービスの普及によって、インターネット経由で会社や家庭のLANにリモート・アクセスしたり、LAN同士をつなぐ「インターネットVPN」のニーズが高まっている。2004年に登場したSoftEtherとは、そうしたインターネットVPNの構築に使えるパソコン用のVPNソフトだった(図1)。

SoftEtherは、「仮想LANカード」とい

図1 SoftEther/PacketiX VPNの概要

インターネットなどのIPネットワーク上でイーサネットLANのしくみを仮想的に実現するVPNソフト。パソコンにインストールした仮想LANカードを専用サーバー上で動く仮想HUBにつなぐという、実際のLAN接続を模した形でVPN通信を行う。仮想HUBと物理的なLANカードをブリッジ接続することでリモート・アクセスやLAN間接続VPNを実現する。





VPN

virtual private networkの略。暗号技術を使って公衆ネットワーク上に仮想的な専用網を構築する技術の総称。

ほぼ2年ぶりのバージョン・アップ

その間もなかったわけではなく、2004年12月からSoftEther VPN2.0という名前で新版のベータ・テストが始まり、約1年をかけてさまざまな機能追加や改良が施されてきた。

MACフレーム

LANでデータをやりとりする単位となるデータの固まりのこと。イーサネットの場合、最大1500バイトまでのデータ一つのMACフレームで運べる。

構築するわけだ

このようにイーサネット・レベルでVPNを構築するタイプを「イーサネットVPN」などと呼ぶことが多い。

うVPNクライアント機能と「仮想HUB」というVPNサーバー機能を併せ持つソフトウェアを使いVPNを構築する。

仮想LANカードと仮想HUB間では、LANで使うMACフレームを丸ごと埋め込んだIPパケットをやりとりする。こうすることで、同じ仮想HUBにつながるパソコン同士をあたかも一つのLANにつながっているように扱える。つまり、IPネットワーク上に仮想的なイーサネットLANを構築するわけだ。

IPパケット中のMACフレームは暗号化されるので、インターネット経由でも安全に通信できる。また、SoftEtherの仮想LANを実際のLANとつなぐことで、インターネットから家庭や職場のLANへリモート・アクセスしたり、拠点のLAN同士のVPN接続も実現する。

基本は同じだが中身は大きく変化

PacketiX VPN2.0は、このSoftEtherの後継版として開発されたソフト

である。両者とも、仮想的にイーサネットLANを構築するという基本は同じ。ただし、PacketiX VPNは、①通信効率の向上、②セキュリティや安定性の強化、③使い勝手の向上、④新機能の追加、⑤対応OSの増加——といった改良によって、ほとんど別物といえるソフトに仕上がっている(図2)。

例えば、セキュリティを強化するための認証機能一つとっても、新たにRADIUSや電子証明書、ICカードなどを使う方式が選べるようになった。VPN通信に使う暗号化アルゴリズムの選択肢も増えた。

導入時のソフト構成も変わった。SoftEther1.0では一つのソフトから必要に応じて仮想LANカードと仮想HUBを導入する方式だった。それに対してPacketiX VPNでは、仮想LANカードによるVPNクライアント機能を提供する「PacketiX VPN Client」、仮想HUBによるVPNサーバー機能を提供

する「PacketiX VPN Server」、さらにローカルブリッジ機能だけを提供する「PacketiX VPN Bridge」と、役割ごとに三つのソフトに分かれた(図2)。

PacketiX VPNで追加/強化された機能をすべて解説するのは難しいので、今回はこの中でもとくに大きく変わった五つのポイントに注目して調べてみた。具体的には、図2に示した新機能/強化点のうち、①「仮想レイヤ3スイッチ」機能の搭載、②「SecureNAT」機能の搭載、③専用サーバー管理ツールの追加、④TCP最適化ツールの追加、⑤ライセンス方式の変更——について見ていく。

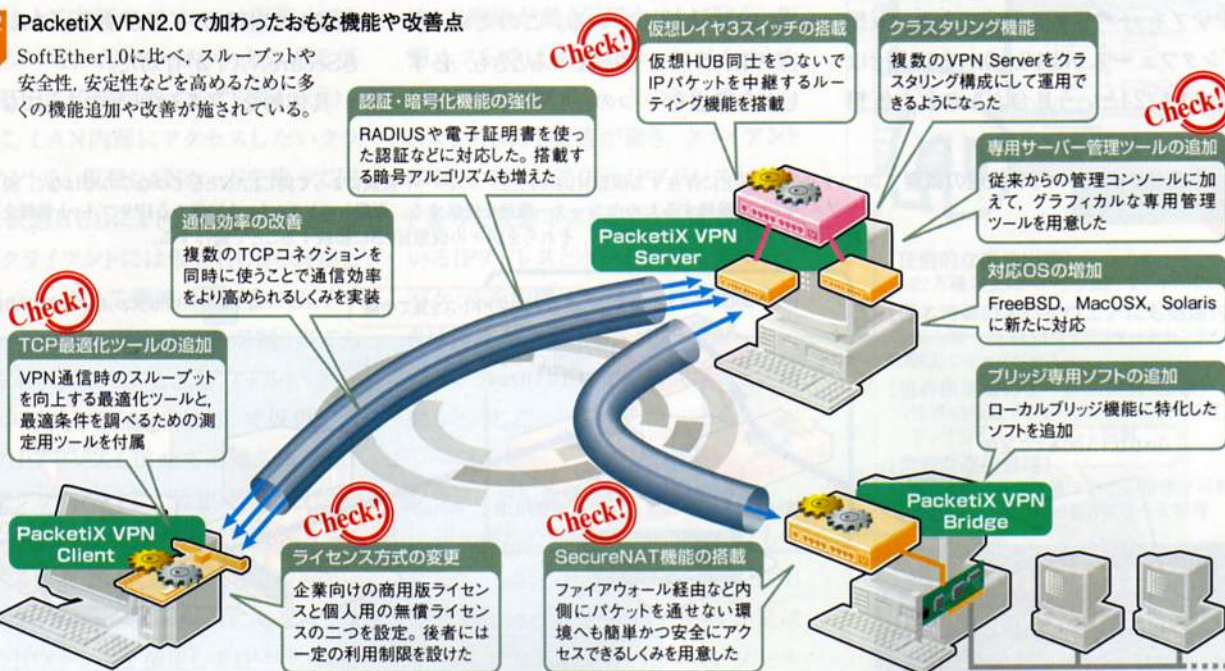
仮想HUBを仮想的にルーターでつなぐ

まずは①の仮想レイヤ3スイッチ(以下、仮想L3スイッチと表記)機能から見ていこう。

PacketiX VPNやSoftEtherは、1台のサーバー上で複数台の仮想HUBを

図2 PacketiX VPN2.0で加わったおもな機能や改善点

SoftEther1.0に比べ、スループットや安全性、安定性などを高めるために多くの機能追加や改善が施されている。



RADIUS

remote authentication dial-in user serviceの略。ユーザーを認証し、パスワードや課金情報などをやりとりするためのしくみ。プロバイダがユーザー管理のために使うほか、最近ではLANのセキュリティ確保のために社内ネットワークで使うケースもある。

通信できない

それぞれの仮想HUBは、物理的には同じ機器につながっていて通信可能だけれども論理的には異なるLANに属しているため通信できないというVLAN (バーチャルLAN) を構成しているイメージになる。

ルーター機能

一般に、レイヤー3スイッチとはルーターの機能をハードウェア化した機器を指す言葉である。PacketIX VPNの仮想L3スイッチ機能は、ソフトウェアでルーティング処理しているので本記事ではルーター機能と呼んでいる。

IPサブネット

IPネットワークを構成する最小単位。ネットワーク・アドレスとサブネット・マスクによって範囲を示す。IPサブネット同士を接続するにはルーターが必要になる。

運用できる。これらの仮想HUBは、初期状態では独立して動く。つまり、仮想HUB1につないだパソコンAと、仮想HUB2につないだパソコンBは別々のLANに属するので通信できない。

この別々の仮想HUBにつながるパソコンAとBを通信させる一つの手段が、従来からあった「カスケード接続」だ。カスケード接続とは、仮想HUB同士を仮想的なLANケーブルでつなぐ機能のこと。複数の仮想HUBが一つのLANに收容されるイメージになる。

それに対して、PacketIX VPNでは、仮想L3スイッチを使って仮想HUB同士を接続する方法を新たに用意した。こちらの接続方法では、カスケード接続時と異なり仮想HUB同士は別々のLANとして分かれたまま。それぞれは、仮想L3スイッチが実現するルーター機能を介して通信する(図3)。

仮想L3スイッチは「仮想インタフェース」を複数持つことができ、それぞれのインタフェースにはユーザーが任意のIPサブネット情報を設定できる。仮想インタフェース1は10.0.0.1/24、同2は10.0.1.1/24という具合だ。これら仮想

インタフェースに仮想HUBを接続すれば、それぞれの仮想HUBにIPサブネットを割り当てられる。そして、仮想L3スイッチの仲介によってIPサブネット間でIPパケットをルーティングできるというわけだ。

外付けのルーターが不要になる

でも、SoftEtherはそもそもイーサネットLAN同士をそのままVPNで接続できることがウリだったはず。それなのに、どうしてわざわざIPしか通せないルーター機能を追加したのだろうか。

追加した理由は開発した本人に教えてもらえない。そこで、ソフトイサ社を訪ねて登大遊社長に直接聞いた。すると、「SoftEther1.0のときから仮想HUB同士を別々のIPサブネットとしてつなぎたいという要望が多くあったので入れたんです」という答えが返ってきた。

イーサネットVPNといっても、実際はほとんどのユーザーがプロトコルにTCP/IPを使っている。このため、拠点のLAN同士を接続するとき、必ずしも全拠点を一つのLANとしてつなぐ

必要はない。それどころか、すべてを同じLANとしてカスケード接続してしまうと、ブロードキャスト・フレームが隅々まで流れてしまい帯域が無駄になるうえ、IPアドレスも管理しにくい。

SoftEther1.0では、IPサブネットを区切るには仮想HUB同士を外付けのルーターでつなぐしか手がなかった。今回PacketIX VPNに仮想L3スイッチ機能が加わったことで、ようやく追加の外付けルーターが不要になった。

アドレス変換してLAN側に中継

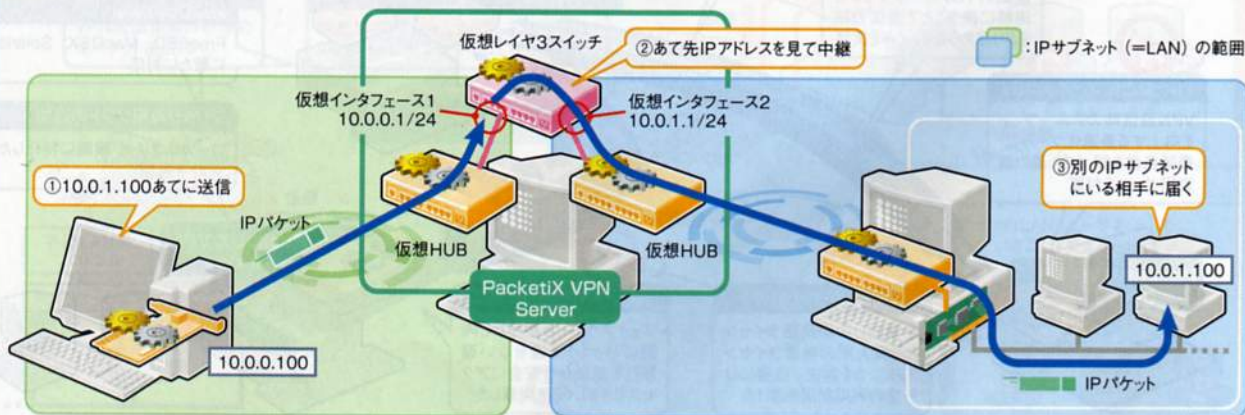
次は②のSecureNAT機能を見ていこう。SecureNAT機能とは、ひと言で表すと「アドレス変換(NAT)機能を持つブロードバンド・ルーターを仮想的に実現する」機能である。先ほどの仮想L3スイッチと似ている機能かと想像する人がいるかもしれないが、その利用目的やしきみは異なる。

例えば、LAN同士をつなぐとき、お互いが使っているIPアドレスの範囲が重複して困るケースがある。こんなときSecureNATが有効だ。

具体的なしきみは以下のようになる。

図3 仮想レイヤ3スイッチ機能の概要

同じVPN Server上に存在する仮想HUB同士を、カスケード接続によって同じLANとしてつなぐのではなく、別々のIPサブネットとして接続するためのルーター機能を提供する。仮想レイヤ3スイッチに異なるIPサブネット情報を持たせた仮想インタフェースを複数個作り、それらを別々の仮想HUBに接続することで動作する。



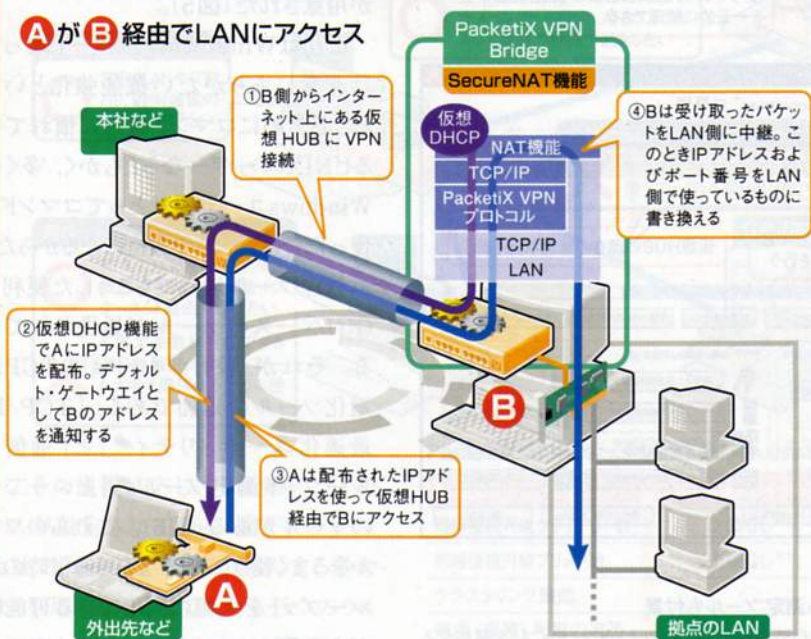
ブロードキャスト・フレーム
LANで全員に同報する際に使うMACフレームのこと。あて先アドレスとしてFF:FF:FF:FF:FF:FFというMACアドレスを使う。このブロードキャスト・フレームが届く範囲が一つのLANとなる。

SecureNAT機能
SoftEther VPN2.0ベータ版ではUser-mode Routerという名前で呼ばれていたものだ。

NAT
network address translationの略。ルーターやファイアウォールなどが搭載するIPアドレスやポート番号を変換するしくみを指す言葉。「IPマスカレード」や「NAPT」などの呼び方もある。

図4 SecureNATのしくみ PacketiX VPNネットワーク上で、アドレス変換 (NAT) 機能を備えたブロードバンド・ルーターと同じしくみを実現する。中継用ソフトが「LAN側からインターネット上の仮想HUBに接続する形をとれるので、NAT越えを容易に実現できファイアウォールに穴を開けたりせずに済む。管理者権限が不要な一般のアプリケーションとして動作できるので、ソフトのバグによって不正アクセスを受ける危険も減らせる。

AがB経由でLANにアクセス



まず、SecureNAT機能が動いているLAN内部のパソコン（仮想ホストと呼ぶ）を、インターネット上にある仮想HUBにVPN接続する（図4の①）。次に、LAN内部にアクセスしたいクライアントを、仮想LANカードを使って同じく仮想HUBにVPN接続する。すると、クライアントには仮想HUBを経由してSecureNAT機能の「仮想DHCPサーバー」からIPアドレスが割り当てられる（同②）。このとき、デフォルト・ゲートウェイのIPアドレスとして仮想ホストのIPアドレスも併せて通知される。これでクライアントは、仮想HUBと仮想ホストを経由してLAN内部にIPパケットを送る準備ができたことになる。

クライアントが、LAN内にあるパソコンのIPアドレスを指定してIPパケットを

送信すると（同③）、パケットはSecureNAT機能が動く仮想ホストに届く。仮想ホストでは、受け取ったパケットをLAN側に中継する。このとき、SecureNATのNAT機能が働き、クライアントが使っていた送信元IPアドレスとポート番号を仮想ホストがLAN側で使っているIPアドレスとポート番号に変換してパケットを中継する（同④）。通信の向きは逆だが、ブロードバンド・ルーターでインターネットにアクセスするときの動きと同じだ。

グラフィカルな管理ツールが付属

追加された管理ツールはどんなものだろう。SoftEther1.0では、仮想HUBの管理といったサーバー側の設定はすべてテキスト・ベースのコンソール

動いている
SecureNAT機能を使うのは、VPN ServerあるいはVPN Bridgeが稼働するパソコンである。

VPN接続する
このようにLANの内側から外部に向けてVPNセッションを張ることで、ファイアウォールに穴を開けずにLANにアクセスさせられるのがSecureNATのメリットの一つとなる。

DHCP
dynamic host configuration protocol。IPアドレスなどの情報を動的に割り当てるためのプロトコル。

デフォルト・ゲートウェイ
経路情報(IPパケットの送信先)がわからないときに、決め打ちで送る先機器(IPアドレス)のこと。通常はルーターがデフォルト・ゲートウェイになる。

図5 グラフィカルなユーザー・インタフェース(GUI)を備えた専用の管理ツールが付属

SoftEther1.0に付属していたテキスト・ベースの管理ツールと比べて使い勝手が大幅に向上した。ただし、使えるのはWindows版のみ。それ以外のOSユーザーや上級者には従来同様のテキスト・ベースの管理ツールも用意している。



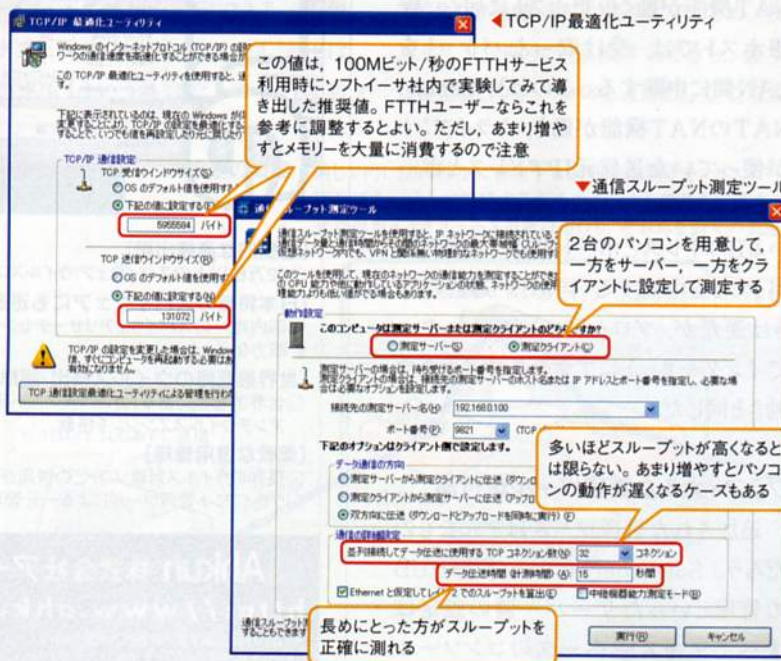
画面から操作する必要があった。それに対してPacketiX VPNでは、グラフィカルなユーザー・インタフェース(GUI)を備えた専用のサーバー管理ツールが用意された(図5)。

これはWindowsユーザーにとっては非常にありがたい機能強化といえる。日常的にコマンド入力に慣れているUNIXユーザーならともかく、多くのWindowsユーザーにとってコマンドを使った管理は大きな負担になるからだ。

管理ツール以外でもこうした便利なGUIベースのツールが提供されている。それが、注目ポイント④のTCP最適化ツールの追加である。「TCP/IP最適化ユーティリティ」と「通信スループット測定ツール」という二つのツールがある(図6)。これらのツールをうまく使うことで、VPN通信時のスループットを大幅に向上できる可能性がある。

図6 TCP通信設定の最適化ツールとスループット測定ツールも付属

「TCP/IP最適化ユーティリティ」を使ってTCP通信時のパラメータ(ウィンドウ・サイズ)を調整することで、環境によってはスループットを大幅に向上できる可能性がある。具体的にどういった値を設定すればいいかは、回線速度やパソコンのハードウェア環境などにもよるため一概には決められない。このため、「通信スループット測定ツール」を添付してユーザーが自分の環境での最適値を探せるようにしている。



無償版は60日ごとの更新が必要

PacketiX VPNは、新機能によって実際の企業ネットワークに近い環境をVPN上で実現しやすくなり、付属するGUIベースのツールによって使い勝手も大きく向上した。では、これですべてのユーザーが万々歳かというところでもない。若干使いづらくなった部分もあったりする。それが⑤のライセンス方式の変更だ。最後にこの部分について見ていく。

ライセンス方式に関しては、押さえておきたいことが二つある。一つは、有償の商用版と無償版(Free Edition)の2種類のライセンスがあること。そしてもう一つは、無償版には利用に際して制約事項がある点だ。

商用版には、対象とする企業やネット

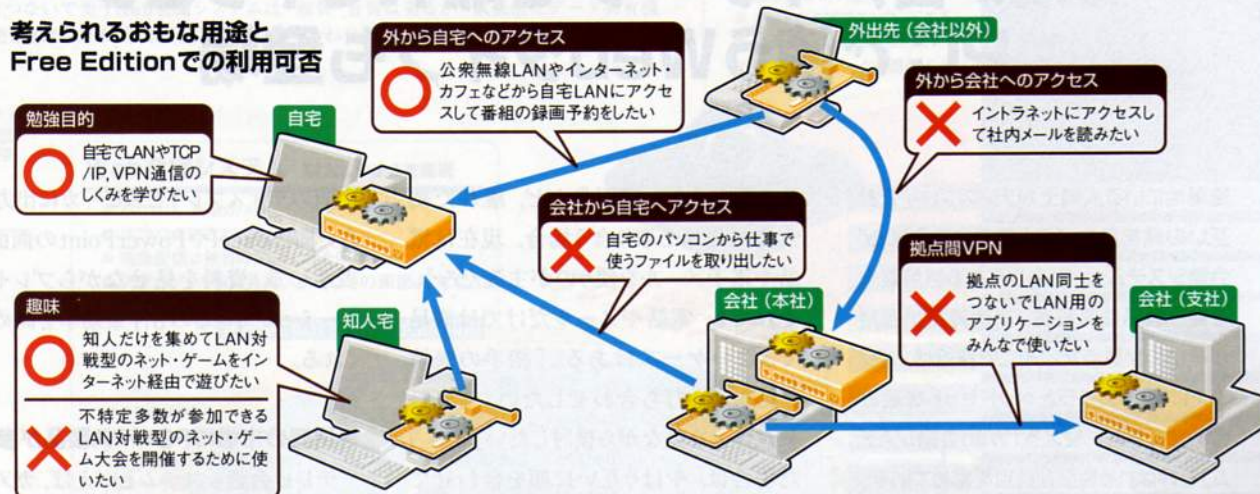
TCP/IP最適化ユーティリティ
このツールを使うことで、WindowsがTCP通信時に使うウィンドウ・サイズというパラメータを調整できる。TCPのオプション機能を使ってウィンドウ・サイズを64Kバイトを超える値に設定することもできるようになっている。

通信スループット測定ツール
最適なウィンドウ・サイズはユーザー環境ごとに異なるので、本ツールなどを使ってユーザーが自分で最適値を見つける作業が必要になる。転送に使うTCPコネクションの数を調整できるなど、一般的なTCPスループット測定ツールにはない特徴も備えている。

可能性がある
ただし、「利用している機器によっては64Kバイトを超える設定にするとうまく通信できなくなるケースがある」(ソフトウェアの登社長)ので注意が必要だ。このためPacketiX VPNでは、初期状態ではOSのTCP関連の設定はいじらないようになっている。

図7 ライセンスの種類とおもな用途 商用版と無償版の2種類がある。SoftEther1.0では個人が会社から自宅のパソコンにアクセスする使い方が認められていた。しかし、PacketiX VPNではこうした業務用途には無償版の利用はできなくなった。また無償版は、使う際に同社のWebページ経由でのライセンス取得作業が必要で、60日ごとに更新する必要がある。

考えられるおもな用途と Free Editionでの利用可否



トワーク規模に応じて3種類のライセンスが設定されている(図7下の表)。会社でPacketiX VPNを導入する場合は、利用目的に応じてこれら三つのライセンスから選んで購入すればよい。

多くの読者が気になるのはFree Editionだろう。こちらは、誰でも自由にダウンロードして無償で使えるという基本はSoftEther1.0と同じ。ただし、利用に際してはほぼ制約がなかったSoft Ether1.0と異なり、PacketiX VPNのFree Editionでは制約事項が二つ加わった。一つは、仕事(業務)で使ってはいけないという使用目的の制限。もう一つは、60日おきにライセンス延長のための更新作業が義務付けられたことだ。

後者に関しては、更新作業はWebページ経由であつという間に終わるため、60日に一度ならさほど苦にならないという人も多いただろう。

一方、前者の使用条件の制限は、既存のSoftEtherユーザーの中には困る人が出てくるかもしれない。「業務」と

PacketiX VPNのライセンス体系 これ以外に最大60日間試用できる体験版ライセンスも用意されている。

製品エディション名	Enterprise Edition	Standard Edition	SOHO Edition	Free Edition
同時接続可能クライアント数	上限なし ^{※1}	上限なし ^{※1}	3	無制限
同時接続可能ブリッジ数	上限なし ^{※1}	上限なし ^{※1}	0	無制限
クラスタリング機能	○	×	×	○
商用(業務)利用の可否	○	○	○	×
価格	9万円(VPN Server 1台あたり) + 接続ライセンス料金 ^{※2}	5万円(VPN Server 1台あたり) + 接続ライセンス料金 ^{※2}	1万9000円 ^{※3}	無償

※1 実際に同時接続できるのは購入したクライアント/ブリッジ接続ライセンス数まで
※2 クラスタリング機能は3ライセンス分が含まれる(追加はできない)
※3 クラスタリング機能は3ライセンス分が含まれる(追加はできない)

※2 クラスタリング機能は1接続8000円(ボリューム・ディスカウントあり)、ブリッジ接続ライセンスは1ブリッジあたり10万円

みなされる範囲が比較的広めに定義されているからだ(図7)。

このようにSoftEther1.0と比べて無償版を使う際に若干窮屈になったイメージがあるPacketiX VPNだが、実際には制約に引っかかるような使い方をしてきたユーザーは少ないはず。多くの機能追加や強化が施され、単純にイーサネットVPNソフトとしての実力もSoftEtherより優れる。そういう意味で企業ユーザーはもちろん、Soft Ether1.0を使っていたユーザーを含め、個人ユーザーも導入する価値は十分あるといえそうだ。(斉藤 栄太郎)

調査報告

- 仮想レイヤ3スイッチやSecure NATといった新機能を使うことで、旧版のSoftEther1.0よりも柔軟にVPNを組めるようになった
- 旧版と比べて使い勝手も大きく向上した。GUIベースのサーバー管理ツールの付属などにより運用・管理が楽になった
- ライセンス形式および利用条件が変わり、無償版の利用には一定の制約が付いた

NETWORK調査部