CUTTING EDGE TECHNOLOGY

話題のテクノロジーを読み解く

簡単VPNを実現するSoftEtherの衝撃

“SoftEther”はインターネット上に仮想的なネットワークをつくり、ネットワーク上のさまざまな障壁を越えて、離れた場所にあるコンピュータ同士、コンピュータとネットワークの間、ネットワークとネットワークの間を接続するソフトウェアである。その若き開発者が開発の経緯と仕組みについて解説する。

text：登大遊（DaiyuuNobori）
筑波大学第三学群情報学類1年。2001年（高校1年）以降、合計3冊の書籍を執筆・出版。平成15年度IPA未踏ソフトウェア創造事業未踏ユース部門にてSoftEtherを開発。現在SoftEther 2.0の開発中。2004年4月、株式会社を設立予定。

●IP
Internet Protocolの略。インターネットの通信のベースになるプロトコル（通信手順）のこと。

●IPパケット
IPの通信では、データを細かく区切って送信する。その区切ったデータに送信先などの付加情報を付け加えたものがパケット。IPでやり取りされる最小単位のデータ。

●グローバルIPアドレス
IPの通信ではIPアドレスという番号を使って、通信先を特定する。その中でインターネット上で使われる世界で唯一無二のIPアドレスがグローバルIPアドレス。これに対して、社内などの閉じられた環境で自由に使えるIPアドレスをプライベートIPアドレスという。

●ファイアーウォール
企業や家庭などの内部ネットワークとインターネットの間に設置し、インターネットから内部ネットワークへの不正な侵入を防ぐルーターやコンピュータに実装されるソフトウェア。

セキュリティーを確保するために自由な通信ができなくなっている

PCやインターネットが普及する過程において、さまざまな通信ソフトウェアが開発され、利用されてきました。これらの通信ソフトウェアやプロトコルのほとんどはIPをベースとしています。IPを利用したプロトコルを使って通信する場合、接続元コンピュータと接続先コンピュータの間はIPパケットが透過的に流れる必要があり、またインターネットを経由する場合は少なくともどちらか一方はグローバルIPアドレスを持っている必要があります。

さて、現在ほとんどの社内LANにはインターネットと接続する間にファイアーウォールやプロキシーサーバーなどのセキュリティー装置が置かれています。家庭でもインターネット側からの攻撃を避けるためにセキュリティー機能の付いたブロードバンドルーターを設置することが多くなっています。

これらのファイアーウォール、プロキシー、NATなどはインターネット側からの攻撃を防止するうえで大変有益なものですが、逆に従来開発されてきたIPベースのアプリケーションが正しく通信できないという問題を引き起こしています。

身近な例では、NATの内側にあるコンピュータ同士は ウィンドウズメッセンジャーのビデオチャットを利用できなかったり、VoIPによる通話ができなかったりします。また、社員が会社側から自宅のPCに接続したくても、社内LANとインターネットとの間にプロキシーやファイアーウォールなどが存在しているために接続できないことがよくあります。

守るべきか？　設定を変更すべきか？システム管理者の悩み

社内LANで一定数以上のコンピュータがある場合、システム管理者はこれらのコンピュータを使用する社員が誤って情報を外部に流出してしまうような通信ソフトウェアやプロトコルの使用を防ぐためにファイアーウォールに厳しい制限を設けています。また、インターネットとの間の通信はすべて1台のHTTPプロキシーサーバーを経由させるウェブアクセスのみに限定させ、外部マシンと直接接続することを禁止するような構成の社内LANもあります。

しかし、社員の業務内容によっては外部のコンピュータや他社のネットワークと接続してファイルを転送したり特殊な通信アプリケーションを利用したりしなければならない状況があります。このような場合、システム管理者はファイアーウォールの設定をその都度変更し、例外を設けなければなりません。しかしながら、最初から安全に設定されているファイアーウォールの構成を変更することは危険が伴います。設定ミスや、正しく設定したつもりでも思わぬ落とし穴があり、ネットワークの外からの攻撃対象になってしまうかもしれません。

このような状況でもインターネットを経由して離れた場所にあるコンピュータやネットワークと相互に通信できる技術として、VPN（Virtual Private Network; 仮想プライベートネットワーク）が最近注目されています。

VPNにもいろいろと問題があるたとえばプロキシーとの相性は悪い

VPNとはインターネットを利用して離れた2拠点

(あるいは複数拠点)間の安全な通信を実現しようという技術です。通信するホスト間やネットワーク間にソフトウェアによって仮想的な通信セッション(トンネル)を構成することにより、インターネットを仮想的な自分専用のネットワークとして利用できるようになります。

ウィンドウズ98/NT4.0にはPPTPのクライアント/サーバー機能が標準で搭載され、特殊なハードウェアなしでVPNを利用できるようになったほか(下図)、大手通信事業者やISPなども顧客のネットワークをVPN技術によって接続するIP-VPNなどのサービスを提供し始めました(122ページ参照)。

しかしながら、既存のVPNプロトコルには一長一短があり、現状の社内LANの構成では適切に利用できないといった声が多くあります。たとえば、もっとも普及しているVPNプロトコルであるPPTPはGREパケットを使用してトンネル通信を行いますが、GREパケットを転送できるNATルーターはごく一部に限られます。また、ファイアーウォール製品の種類によってはGREパケットを通過するように設定できないものもあります。L2TP/IPsecについても同様で、IPsecを適切に通過させられない環境では用いることができません。

また、インターネットと社内LANとの間の通信がHTTPプロキシーサーバーを経由しなければならないような構成になっている場合は、既存のVPNプロトコルを利用することは絶望的です。既存のVPNプロトコルはVPNクライアント側からVPNサーバーに対してIPパケットが直接届くことを前提としているため、プロキシーサーバーを経由してVPNを構成することができないのです。

大学のネットワークの不便さがSoftEther開発のきっかけに

筆者は2003年に筑波大学の情報学類に入学しました。筑波大学の学内ネットワークはインターネットに高速回線で接続されており、ネットワークを自由に利用できるという恵まれた環境です。

筑波大学には学内ネットワークの一部として「無線LANアクセスポイント」があります。これは一般的な無線LANカードを装着したノートPCがあれば、学内の無線LANの基地局に接続してインターネットにアクセスできるサービスで、筑波大学の学生であれば誰でも利用できます。

しかし、この無線LANを利用するには必ずブラウザーでプロキシーサーバーを設定する必要がありました。無線LANのネットワークとインターネットとの間はNATで接続されているのではなく、プロキシーサーバーによってのみ接続できる形式になっていたためです。その理由は学内の計算機システムのアカウントを持っている学生だけに無線LANの利用を限定し、部外者による無断使用を防止する必要があったためであり、インターネットへのアクセスの際に使用するプロキシーサーバーによってユーザー認証を行っていました。つまり、筑波大学の無線LANシステムは、学生がアクセスするウェブサイトをチェックしたりアプリケーションの利用を制限したりするためではなく、純粋に利用者の認証のためだけにHTTPプロキシーサーバーを導入していたのです。

したがって、この無線LANを利用するとHTTPを利用するウェブは見られますが、POP3/SMTPを利用するメールの送受信や、あるいはウィンドウズのリモートデスクトップ接続といった便利なプロトコルを一切利用できず、せっかくの高速学内ネットワークを十分に活用できませんでした。

そこで、筆者は従来のVPNプロトコルを応用してインターネット側に設置したVPNサーバーと無線LAN内のノートパソコンを接続し、VPNセッションの中で通信アプリケーションを利用できるかどうかを調べてみました。しかし、従来のVPNプロトコルは前述のような理由により、HTTPプロキシーサーバーの経由を前提とする無線LANシステムでは利用できないことがわかりました。

●プロキシーサーバー
ファイアーウォールが置かれる内部ネットワークから外部のコンピュータと通信するときに、外部と直接通信をしてくれる代理のサーバー。

●NAT
Network Address Translation。インターネットで通信するコンピュータはすべてグローバルIPアドレスが必要となるが、社内や家庭などの内部ネットワークでは、プライベートIPアドレスが使われることが多い。そこで、内部と外部の通信する際に、IPパケットのプライベートIPアドレスとグローバルIPアドレスの付け替えをして、うまく通信できるようにする。ルーターに実装されていることが多い。

●VoIP
Voice over IP。IPの通信で音声をデータとしてやり取りすること。最近話題のIP電話はVoIPのこと。

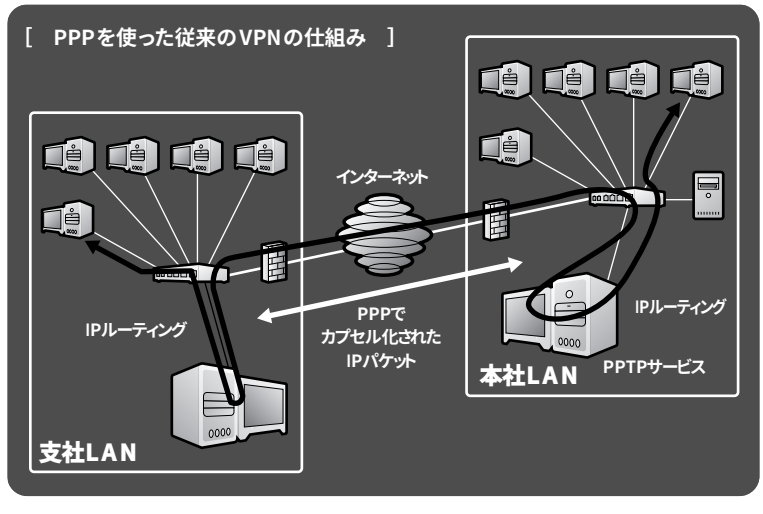
●PPTP
Point to Point Tunnelling Protocol。一対一の仮想通信ネットワークを実現する通信方式。ウィンドウズに標準で実装されている。

●GREパケット
PPTPで通信するために、IPパケットを暗号化などGREという方法で包んだもの(カプセル化)。

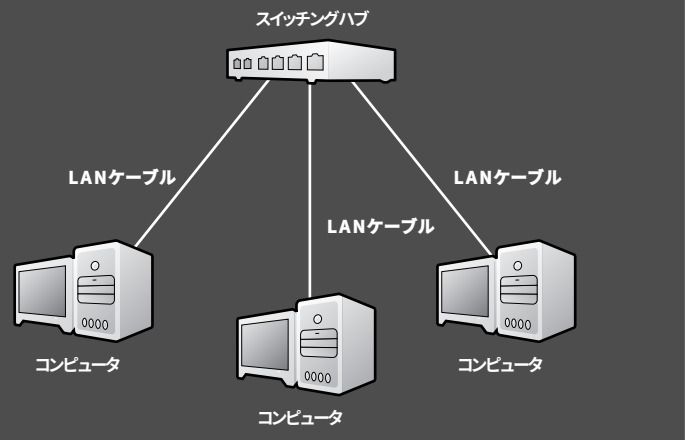
●L2TP/IPsec
L2TPは Layer 2 Tunnelling Protocol。L2TPもIPsecもVPNの方式の1つ。

●POP3/SMTP
POP3(Post Office Protocol version 3)はメールソフトがメールサーバーからメールを読み出すための通信手順。SMTP(Simple Mail Transfer Protocol)はメールを送るための通信手順。

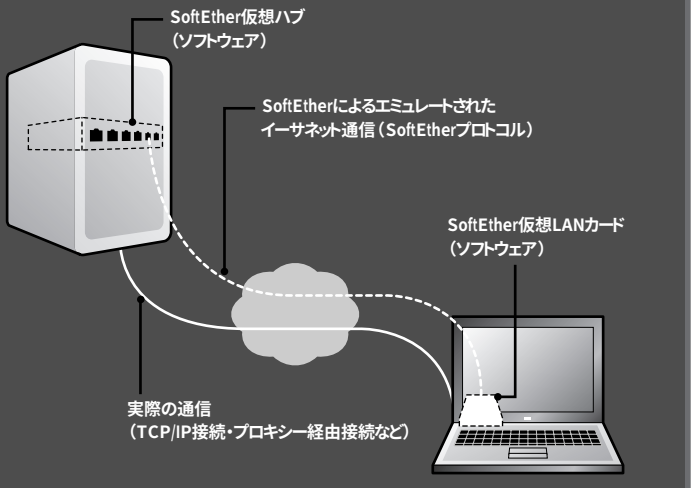
[PPPを使った従来のVPNの仕組み]



[物理的なイーサネットのLANの構成]



[仮想ハブと仮想LANカードで実現するSoftEther]



プロジェクトがついに発足！「未踏ソフトウェア創造事業」に

従来のVPNプロトコルのもう1つの欠点として、ほとんどのVPNプロトコルはトンネリングする対象がレイヤー3のIPパケットに限定されるという点があります。つまりVPNセッションを流せるパケットはレイヤー2のMACフレームではなくレイヤー3のIPパケットということになります。この場合、両拠点のIPネットワークに流れるルーティングテーブルの変更が必要となります。また、2拠点のイーサネットのセグメントは分断されたままとなります。

筆者は以前からPPTPなどのVPNを利用していて、トンネリング通信の対象がレイヤー3ではなくレイヤー2であればとても便利になるはずだと考えていました。そこで、「ほとんどのネットワーク上の障壁を通過でき、簡単で安全で柔軟に仮想ネットワークで通信できるまったく新しいVPNソフトウェア」を開発しようと思い立ちました。

このソフトウェアの開発プロジェクトは「平成15年度 未踏ソフトウェア創造事業未踏ユース部門」に採択され、2003年7月より開発を開始しました。また、名称は「SoftEther」に決定しました。

SoftEtherはウィンドウズで動く「仮想」LANカードと「仮想」ハブ

SoftEtherを一文で説明すると、「仮想的なLANカードとハブの間でイーサネットパケットを送受信するソフトウェア」ということになります。ここでSoftEtherの詳しい説明をする前に、普段われわれが利用しているイーサネット（LAN）の仕組みを見てみましょう。

イーサネットは、ノード（コンピュータ）間でMACフレームと呼ばれるパケット（最大1514バイト）を交換することによって相互通信を可能とする仕組みです。複数のコンピュータを1つのLANに接続する場合、1台以上のハブを設置して各コンピュータとハブとの間をLANケーブルで接続することになります。その結果、ハブがパケット交換機の役割を果たし、複数台のコンピュータ間で通信が可能になります（左上図）。ここで、各コンピュータの物理的なLANカードと物理的なハブとの間に流れるMACフレームは、実際には物理的な電気信号であるということに注目してください。3つのキーワード、「物理的なLANカード」「物理的なハブ」「物理的な電気信号」をソフトウェアによってそのまま「仮想的」に実現したものが、SoftEtherなのです（左下図）。

SoftEtherは大きく分けて「仮想LANカード」と「仮想ハブ」の2つのソフトウェアから構成されています。仮想LANカードは一般的なLANカードをソフトウェア的にエミュレーションします。同様に仮想ハブは一般的な100Base-TXスイッチングハブをエミュレーションします。そして、仮想LANカードと仮想ハブの間をTCP/IPベースのSoftEtherプロトコルによって接続し、仮想的なMACフレームパケットを交換します。この仕組みにより、仮想ハブを中心とした「SoftEther仮想LAN」が構成され、同一の仮想

●レイヤー3
ネットワークの通信手順はOSI参照モデルという7つの階層に分けて考えられる。レイヤー3はその下から3番目の階層で、インターネットの通信のベースであるIPがそれにあたる。

●レイヤー2
OSI参照モデルの下から2番目の階層。イーサネットなどがレイヤー2になる。

●MACフレーム
イーサネットでやり取りされるデータ単位。

LANに接続しているコンピュータ同士は自由に通信できます。

SoftEtherだからできること 接続方法からその機能・性能まで

仮想LANカードをインストールしたコンピュータから仮想ハブをインストールしたコンピュータに接続する方法には4種類あります。

①直接TCP/IP接続――直接、TCP/IPプロトコルによって両者を接続できます。
②HTTPプロキシー経由接続――HTTPプロキシーサーバーを経由して仮想ハブに接続します。多くの社内LANなどで利用できます。
③SOCKS経由接続――SOCKS v4サーバーを経由して仮想ハブに接続します。
④SSH経由接続――SSHサーバーが動作しているコンピュータを経由して仮想ハブに接続します。

上記のように多様な通信方法でクライアント側からサーバー側までの接続を確立できることが、従来のVPNにはなかった最大の特徴と言えます。特にほとんどのファイアーウォールやNAT、プロキシーを通過できるため、システム管理者はSoftEtherを導入するにあたってファイアーウォールの設定を変更する必要がほとんどありません。これ以外にもSoftEtherは次のような特徴を持っています。

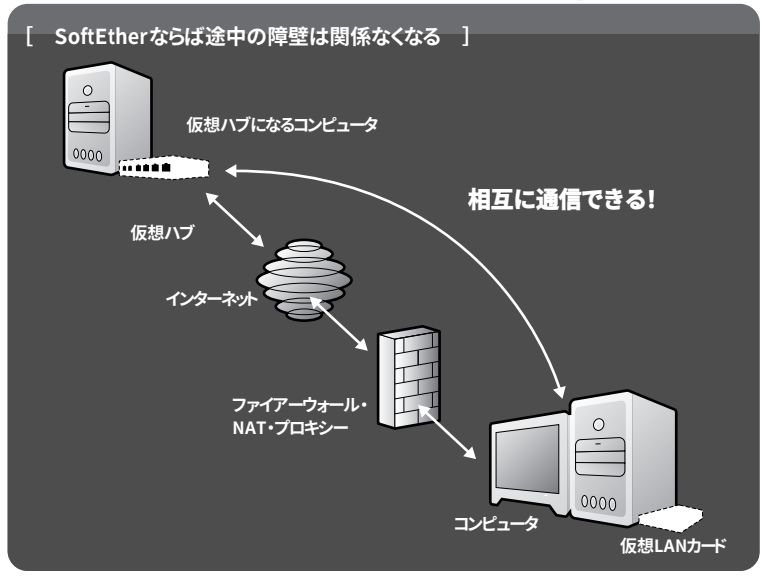
●Ethernet over TCP/IP

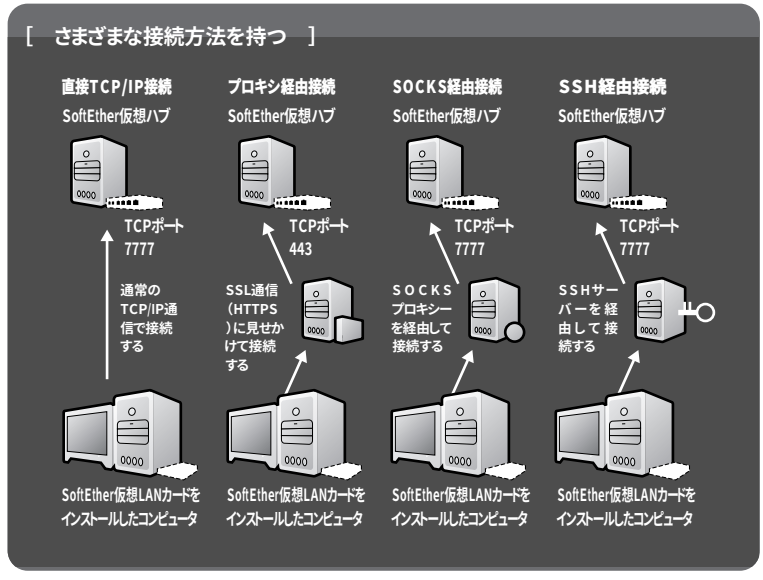
SoftEtherの通信形態はEthernet over TCP/IPということになります。従来、Ethernet over TCP(TCP over TCP)を利用した場合は非常に効率が悪化し、まともな通信ができなくなるという意見が多くありました。

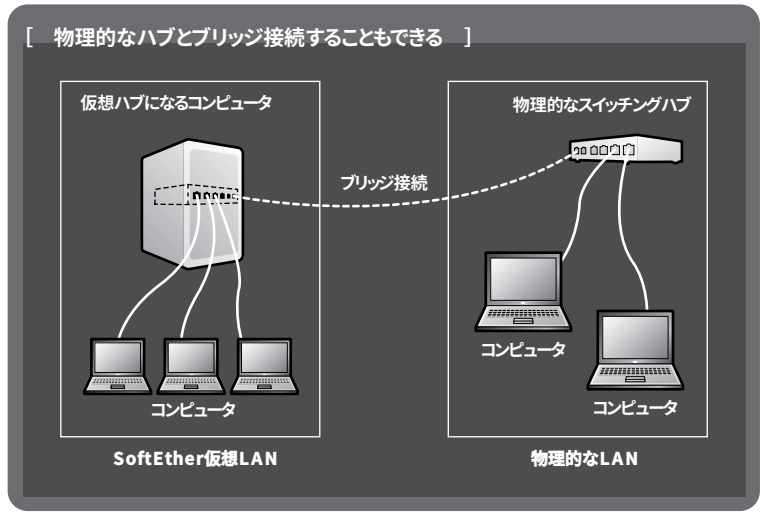
SoftEtherでは仮想ハブ側でリアルタイムトラフィック分析と輻輳制御を行うことにより、TCP over TCPによる問題を解決しました。たとえば、インターネットから直接ファイルをダウンロードする場合とSoftEther経由でダウンロードする場合、環境によっては速度低下は20%以下になります。

●ブリッジ接続

仮想LANカードはOSからは本物のLANカードのように見えます。そのため、物理的なLANと仮想的







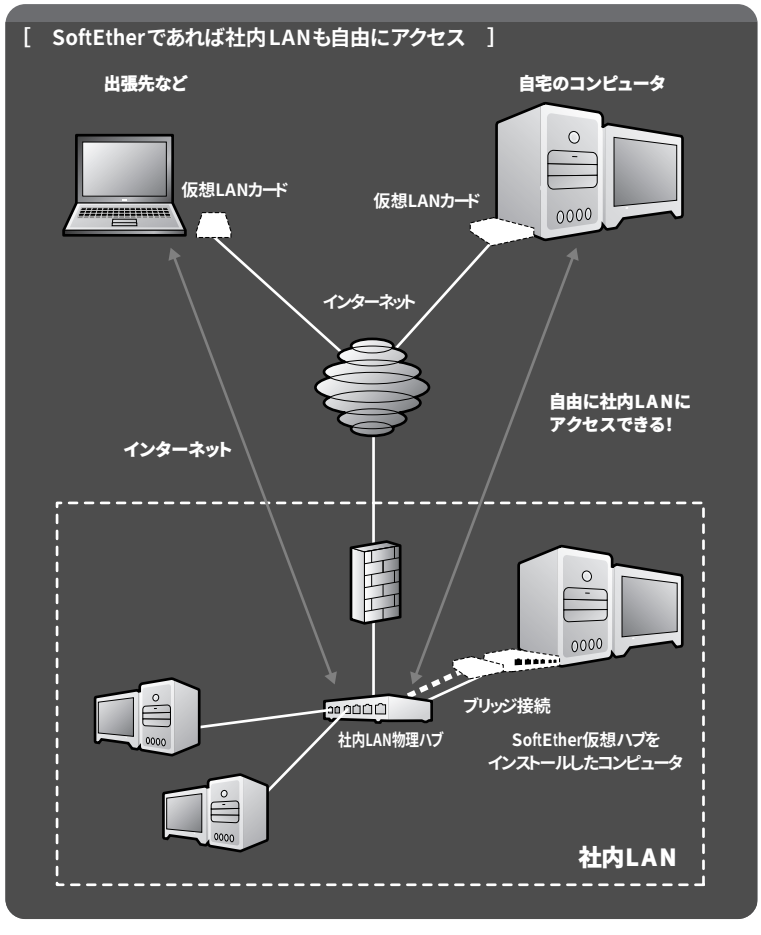
●SSL
Secure Socket Layer。暗号化のための通信方式。もともとブラウザーとウェブサーバーとの通信のためのものであったが、最近は用途が広がっている。

●ブロードキャスト
ネットワークにつながるすべてのコンピュータにデータをいっせいに送信すること。どんなコンピュータがつながっているかを調べるときなどに使われる。

なLANとの間で「ブリッジ接続」ができます。これは、物理LANと仮想LANが1つのセグメントとして認識され、完全に1つのLANとして動作することを意味します。従来のレイヤー3をトンネリングするVPNプロトコルでは実現できない機能の1つです。

●どこにでも設置できる仮想ハブ

仮想ハブは、接続しようとする各仮想LANカードからIP通信上で認識できる場所（たとえば、グローバルIPアドレスを持つなど）に設置しさえすれば、どこに設置してあっても構いません。従来のVPNでは、VPNサーバーとなるコンピュータがVPN接続したいネットワーク内に存在する必要がありましたが、SoftEtherではサーバー（仮想ハブ）は必ずしもVPN接続を構成したい拠点のLAN内に設置する必要はなく、インターネット上であればどこに設置してもいいということになります。SoftEtherでは一度クライアント側からサーバー側へSoftEtherプロトコルによるコネクションが確立した後は、そのトンネルの中を仮想MACフレームが自由に流れることになり、方向性はまったく意識しなくてもよくなります。



セキュリティー対策も万全 ユーザーの制御もできるから安心

ところで、家庭内や会社内専用の仮想ハブを設置した場合、誰でも接続できてしまうと大変危険です。そこで、SoftEther仮想ハブと仮想LANカードとの間の通信は、すべてSSLによる暗号化セッションとして確立するように解決しています。また、ユーザー認証も備えていて、ユーザー名とパスワードによる認証をサポートするほか、今後RADIUS/Active Directory認証に対応する予定です。

仮想ハブに登録されたユーザーごとにセキュリティーポリシーを設定できます。仮想ハブは一般的なスイッチングハブのように動作しますが、DHCPによってIPアドレスを割り当てる仕組みを仮想LAN内で運用している場合、おかしな設定のDHCPサーバーを悪意を持ったユーザーが意図的に仮想LANに接続したときは仮想LAN内のクライアントの状態が異常になります。また、既存のIPアドレスやMACアドレスと意図的に重複させて通信を妨害したり傍受したりする攻撃も可能になってしまいます。

このような攻撃や誤った設定による通信障害を防止するため、ユーザーのセッションごとに「セキュリティーポリシーオプション」を設定できます。

どんなアプリケーションでも 仮想ネットワークで通信できる

SoftEtherを使うと、離れた場所にある2台以上のコンピュータ同士の間で1つの仮想LANを構築できます。仮想LANはソフトウェアやOSから見れば一般的なイーサネットネットワークなので、既存のアプリケーションの設定を一切変更することなく通信できます。

社内LANなどに自宅や出張先からアクセスしたい場合、従来のVPNプロトコルが利用できないような環境でもSoftEtherを使用すると接続できるようになります。

インターネットから直接接続できるネットワーク上の場所に仮想ハブをインストールしたサーバーを設置し、社内LANのコンピュータに仮想LANカードをインストールして仮想ハブに接続します。その状態

で社内PCの仮想LANカードと物理的なLANカードとの間でブリッジ接続を構成することにより、別の場所から接続したコンピュータは自動的に社内LANに直接接続したのと同等の状態になります。

ブリッジ接続（2つのネットワーク間を直接接続する方法）を応用すると、離れた場所にあるLAN同士を1つの大きなLANとして接続できます。つまり、2つのLANが同一セグメントとして接続され、内部にあるコンピュータ同士は一切設定を変更することなく相互に通信できるようになります。

従来のレイヤー3ベースのVPNプロトコルを使用して拠点間を接続するには、各拠点でルーティングテーブルの設定を変更しなければなりませんでした。また、両方のネットワークは同一セグメントではないため、ウィンドウズのファイル共有などで使用されるブロードキャストパケットは届かないことになります。ですが、SoftEther仮想LAN技術を利用すれば、これらの問題を解決できます。

また、IP電話プロトコル（VoIP）やウィンドウズメッセンジャーなどのビデオチャットを利用する2台のコンピュータ同士の間にNATやファイアーウォールなどが存在すると、うまく通信できないという問題がありました。しかし、2台のコンピュータが同一のSoftEther仮想ハブに接続することにより、それらのコンピュータ間は自由に通信できるようになるため、NATやファイアーウォールが原因で動作しないプロトコルはすべて利用できるようになります。つまり、たとえ物理的に2点のコンピュータの間に障壁があっても、SoftEtherの接続がいったん確立すると、それは問題ではなくなるということです。

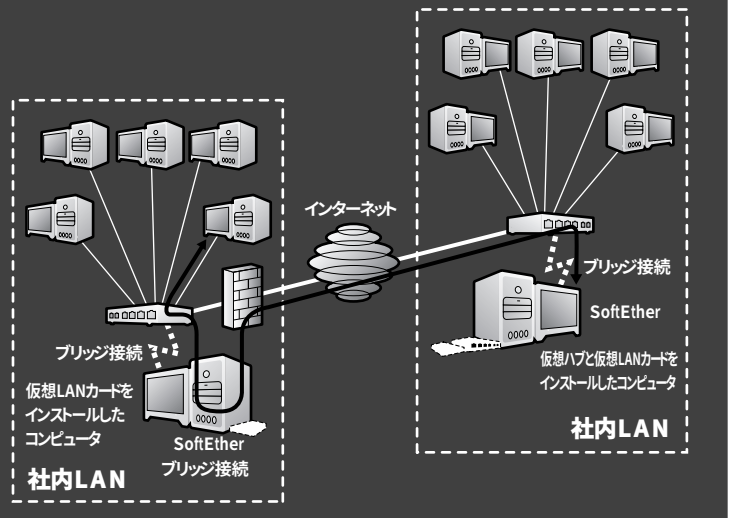
次はパフォーマンスの向上とプラットフォーム非依存を目指す！

筆者は現在、『SoftEther 2』の開発計画を立てています。SoftEtherを公開した後、非常にたくさんのご意見とご要望をいただいており、これらをできる限りすべて実装した、高機能で高性能、かつプラットフォームに依存しないVPNシステムソフトウェアを開発することが目標です。

SoftEther 2の第一目標は、「仮想ネットワークの通信と直接通信との間の体感速度がまったく区別つかないほどの高速化」です。SoftEtherはTCP over TCPの通信速度悪化の問題を解決しましたが、それでも20%程度かそれ以上は転送速度が低下してしまいます。SoftEther 2ではこの「速度差」がほとんどない仮想ネットワークをTCPコネクションのみで実現します。

SoftEther 2では、仮想ハブを構成する各機能をモジュール化する予定です。つまり、認証部分、カプセリング部分、暗号化部分、トンネリング部分、伝送部分といったそれぞれの機能を独立したモジュールとして開発し、後から簡単に追加や拡張ができるようにします。

［ イーサネットのMACフレームを直接流すことができる ］



●SoftEtherについて

SoftEtherの開発作業は、IPA（情報処理振興事業協会）の「未踏ソフトウェア創造事業（未踏ユース）」の採択案件として行い、IPAから開発補助を受けるとともに、電気通信大学教授 竹内PMより開発時に指導とアドバイスを受けた。

SoftEtherはフリーウェアで、下記のウェブサイトからソフトウェアをダウンロードできる。詳しい使い方の解説やオンラインマニュアルも入手できる。

URL http://www.softether.com/

CD-ROM収録！

付録のCD-ROMにもSoftEtherが収録されています。

［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