SoftEther による Ethernet の仮想化とトンネリング通信

Virtual Ethernet system and Tunneling Communication with SoftEther

筑波大学 第三学群 情報学類 1年
登 大遊
College of Information Sciences,
3rd Cluster of Colleges,
University of Tsukuba
Daiyuu Nobori

概要

そもそも、インターネットは任意のネットワーク間やコンピュータ間で IP を用いて自由に通信できるようにするために構築されたものであるが、現状のインターネットでは IP アドレスの枯渇などの問題により、すべてのコンピュータにグローバル IP アドレスを付与することが不可能になっている。また、インターネットに接続可能な社内 LAN や学内 LAN などにおいても、IP アドレスの不足やセキュリティ上の問題により、NAT や Proxy サーバー、ファイアウォールなどを経由しなければインターネットへアクセスすることができない場合が大半となっている。このような制限の多いネットワーク環境において、本来のインターネットの目的である任意の複数のコンピュータやネットワーク同士で通信を可能にするためのソフトウェアである『SoftEther』について解説し、その活用方法などについても紹介する。

1. はじめに

SoftEther は、既存のネットワーク上の色々な制限・障壁を越えて、コンピュータ間やネットワーク間を自由に通信できるようにするためのソフトウェアである。利用方法によっては、VPN (仮想プライベートネットワーク) を構成することもできるが、従来の VPN プロトコル (PPTP、L2TP / IPSec など) では通信できなかったような環境でも、色々なサーバーを経由することによって通信可能となる。また、PPTP などの VPN プロトコルは、仮想的な PPP (ダイヤルアップで使用されるプロトコル) を IP の上で確立するが、SoftEther の場合は仮想的な Ethernet を確立するため、既存の物理的な Ethernet 間をブリッジ接続することも可能であり、既存のネットワーク環境を大きく変化させることもできる。

一言で言うと、SoftEther も VPN の一種である。しかし、既存の VPN には無い多くの特徴を備えており、その応用範囲は極めて広いと認識している。

2. 現状の問題点

現在ではインターネットが普及し、ほとんどの会社や学校ではその構内ネットワーク(LAN)を経由してインターネットにアクセスが可能であることが一般的になっている。しかしながら、多くの場合、図 1 のようにインターネットと LAN との間に NAT、Proxy サーバー、ファイアウォールが設置されており、IP のレイヤから見た本来の「自由な通信」が困難な環境であることが多い。

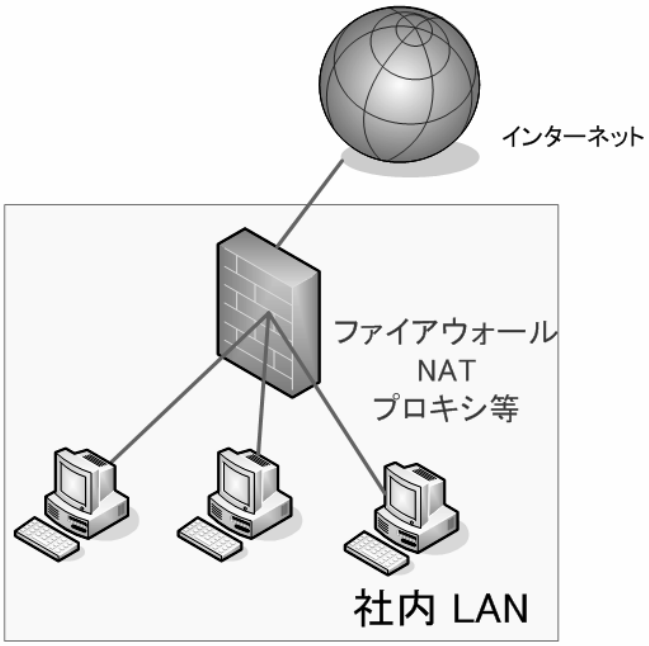

図 1 ファイアウォール等による LAN とインターネットとの間の通信制限

IP による自由な通信とは IP アドレスを持った複数のコンピュータ同士が自由にパケットを交換できる状態を指すが、昨今では IP アドレスの不足、

LAN のセキュリティの確保、LAN 利用者 (社員など) のインターネットへのアクセスの監査が必要である、などの様々な理由により、LAN とインターネットとの間に上記のような障壁を設けることにより、利用上の制限の多いネットワークになってしまっている施設が多数存在する。

このような環境では、本来のインターネット接続環境で動作するように書かれた TCP/IP を利用する色々なソフトウェア(優秀なフリーソフトを含む)の一部が正しく動作しない、または全く使用できないといった状況が生じることが多い。

現状の IP アドレス不足の問題や、構内 LAN のセキュリティの向上に向けた各種の取り組みの結果、上記のような「制限の多いインターネット接続環境」は今後ますます増加していくと予想される。

たとえば LAN からインターネットへアクセスする際に HTTP や SSH など限られた(管理者が安全だと判断している)ポートしか通さないようなファイアウォールシステムがある社内 LAN を考えてみる。ここでは、利用者がインターネットを利用する方法は必然的にホームページ閲覧程度のものになってしまう。しかし、パワーユーザーはその他の通信アプリケーションも LAN 内で使いたい。たとえば、メールの送受信や IRC サーバーへの接続、自宅の PC に FTP で接続する、Windows のリモートデスクトップ機能を使う、など挙げればきりが無い。

少しネットワークソフトに詳しいパワーユーザーであれば、上記のような環境では SSH のポート転送を使ってある程度障壁を回避することができる。また自宅に PC がある人は、自宅で SOCKS サーバーを立てておいて、LAN 内から SSH のポート転送経由で自宅の SOCKS に接続し、そのコネクションの上でさらに別の通信アプリケーションを乗せて使う、といった少し高度な技を使うことによって、これまでパワーユーザーはその場しのぎの方法で LAN のファイアウォールによる通信制限を回避し、使用したいアプリケーションやプロトコルを使ってきた。

しかしながら、上記のような方法を使うのは大変不便であるし、各アプリケーション利用の際に別のソフトウェアを常時起動させておいてそれに依存するという状態は、あまり好ましくないものである。できれば、制限の多い LAN の中でも、外のインターネットや別の LAN 内のコンピュータと直接自由に(TCP/IP レベルで)通信がしたい。筆者も、大学の設置している無線 LAN の制限の多さに不満を持っていたため、こういった通信上の障壁を根本から解消できるような、便利で強力なユーティリティ・ソフトウェアを開発したいと思った。

3. Virtual Private Network 技術

VPN (Virtual Private Network) というものが普及し始めている。インターネット上に仮想的な通信トンネルを張り、カプセル化・暗号化された IP パケットを転送することで、インターネットを一時的な専用線にするという技術である。

前で述べた、制限の多い LAN で外部のネットワークやコンピュータと自由に通信する方法の 1 つとして、既存の VPN ソフトウェアの利用が考えられる。しかしながら、ここで議論の対象としているのはシステム管理者ではなく LAN の一般ユーザーであるので、VPN を LAN にインストール・構成して外部に接続することは不可能である。また、たとえば LAN 内の自分の PC を VPN クライアントとして、自宅にある VPN サーバーに接続することによって自由にインターネットにアクセスするという試みも失敗に終わるであろう。LAN のファイアウォールで、許可されていない VPN プロトコルのパケットは遮断されているためである。Windows に標準で付属している PPTP は GRE パケットを使用するが普通のファイアウォールや NAT は GRE を通さない。L2TP/IPSec を使用する VPN プロトコルも通らない。その他の各ベンダー独自の VPN 製品も、ファイアウォールを通過できないので一般ユーザーが外部との通信に使用することはできない。したがって、一般ユーザーが既存の VPN プロトコルを社内 LAN などで使用することは不可能に近く、いずれにせよシステム管理者の許可が必要になってしまう。

しかし、この VPN の概念を拡張することによって、既存の制限が多い社内 LAN・学内 LAN などでも一般ユーザーレベルで使用可能な、外部とのトンネリング接続が自由に行えるソフトウェアを開発できると考えた。

4. Ethernet の仮想化とカプセル化

『SoftEther』は、Software Ethernet の略である。Ethernet をソフトウェア的に実装しようという意味を

持たせるとともに、Soft=柔軟、Ether=媒体なので、どのようなネットワーク環境にも柔軟に対応して通信することができる媒体としてのソフトウェアであるという意味である。

SoftEther の基本原理は、Ethernet の各機器をソフトウェア的にエミュレートするというものである。現在の Ethernet は、主に 3 つの機材によって構成されている。すなわち、LAN カード、スイッチング HUB、LAN ケーブルである。

このうち、LAN カードとスイッチング HUB をソフトウェアで仮想化し、その間の通信を LAN ケーブルの代わりに TCP/IP を使用して行うことにより、従来の Ethernet のフレームを仮想的にコンピュータ間で送受信することができる。

SoftEther システムでは、エミュレートされた LAN カードを『SoftEther 仮想 LAN カード』、スイッチング HUB を『SoftEther 仮想 HUB』と呼ぶ。

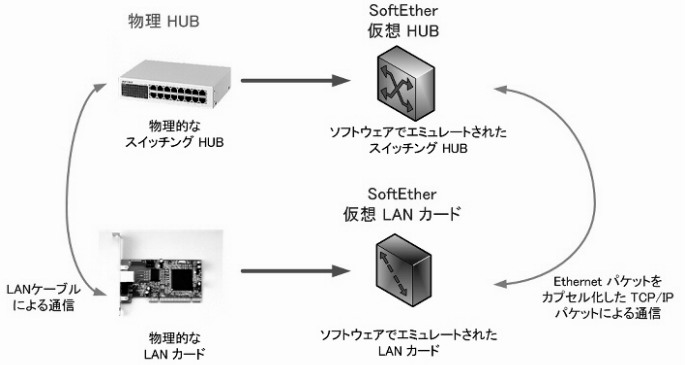

図 2 物理的 HUB と仮想 HUB、
物理的 LAN カードと仮想 LAN カードの対応

仮想 HUB は物理的な HUB と同様に、複数台のコンピュータを接続することができる。仮想 HUB に接続されたコンピュータ間では、Ethernet レベルで自由にパケットを送受信することができる。物理的な LAN カードが HUB にケーブルで接続されるのに対し、仮想 LAN カードは TCP/IP 接続による仮想的な通信網で仮想 HUB に接続される。この TCP/IP 通信は実際にはそのコンピュータが物理的に接続されているコンピュータに装着されている物理的な LAN などの回線によって行われるのだが、仮想 LAN カードを使用して通信しているソフトウェアはそのことを知る必要は無い(知ることもできない)。つまり、SoftEther は仮想 HUB と複数の仮想 LAN カードとの間で、TCP/IP パケットにカプセル化された仮想的な MAC フレーム パケットを、既存のインターネット接続の回線にトンネリングさせて通信を行うためのソフトウェアである。

物理的な HUB と仮想 HUB、物理的な LAN カードと仮想 LAN カードの関係を図 2 に示す。

SoftEther の仮想 LAN カードと仮想 HUB との間で交換されるパケットは、物理的な Ethernet システムで LAN ケーブル上を電気的に流れる MAC フレームとほぼ同形式である。これを仮想 MAC フレームと呼ぶ。

実際には、SoftEther で送受信される仮想 MAC フレームは、128bit 暗号化された上で電子署名を付加されたものを TCP/IP でカプセル化し、それをコンピュータが既存で持っている LAN などの通信回線を経由して目的地である仮想 HUB を動作させているコンピュータに送信する。仮想 HUB では受け取ったパケットを解読、電子署名をチェックし、この内容をカプセル解除してから宛先の MAC アドレスを調べ、その MAC アドレスのコンピュータへ転送する。これが、SoftEther 仮想 HUB のスイッチング機能である。

図 3 に、SoftEther による仮想 HUB と仮想 LAN カードとの通信方法を示す。

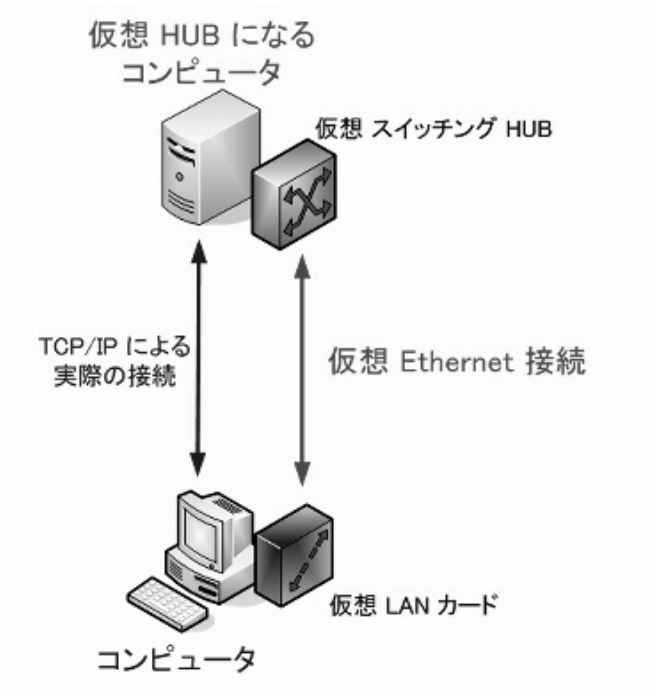

図 3 仮想 HUB と仮想 LAN カードとの通信

5. SoftEther プロトコルによるファイアウォールの通過

SoftEther は、仮想 LAN カードと仮想 HUB との間の通信に専用の SoftEther プロトコルを使用する。また、SoftEther プロトコルを含むパケットを「SoftEther パケット」と呼ぶ。SoftEther プロトコ

ルは TCP/IP 上で動作し、基本的に仮想 LAN カードがインストールされているコンピュータから仮想 HUB がインストールされているコンピュータに対して TCP/IP パケットが届く場合であれば必ず接続できる。図 4 のように、実際の 2 台のコンピュータ間はすべてTCP/IPパケットによって行うことができる。

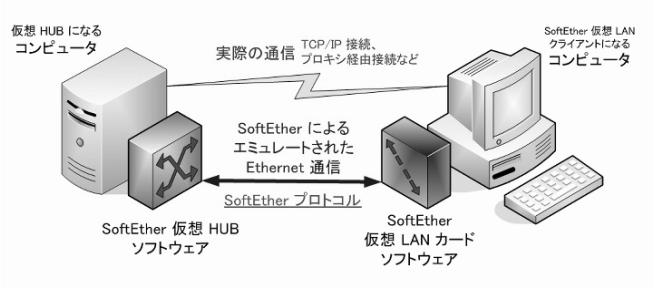

図 4 仮想 HUB と仮想 LAN カードとの通信の図解

しかし、直接 TCP/IP で仮想 HUB に接続できない環境では、HTTP プロキシサーバーや SSH サーバー、SOCKS サーバーなどを経由して接続することができるので、セキュリティの厳しい社内 LAN でも、大抵の場合は外部の仮想 HUB に接続することができる。

現在主流となっているファイアウォールには、大きく分類して透過型と Proxy 型の 2 種類がある。透過型は IP レベルまたは TCP レベルでパケットの内容をチェックし、許可されていないポートへのアクセスを遮断するものである。また、NAT 技術によりアドレス変換を行う場合もある。NAT 自身も透過型ファイアウォールの 1 つである。

Proxy 型ファイアウォールは、HTTP プロキシなどに代表されるものであり、ファイアウォールとなるコンピュータが各プロトコル固有の代理サーバー機能を提供する。LAN 内の各クライアントは、この Proxy サーバーとなったコンピュータのアドレスを Web ブラウザのオプション設定などに入力することによって、インターネット上の Web ページを見ることができる。しかし、Proxy が対応していないプロトコルは使用することができないので、たとえば POP3/SMTP を使用したメールの読み書きさえもできない場合が多い。

SoftEther プロトコルは、これら 2 種類のファイアウォール両方をうまく経由して、インターネット側にある仮想 HUB に対してアクセスすることができる。具体的には、透過型ファイアウォールや Proxy がほぼ必ず許可している HTTPS 通信を偽装して外部と通信する。一旦外部とのコネクションに成功したら、あとは SoftEther プロトコルをそのホストと PC との間で流せば、SoftEther 仮想 LAN カードと仮想 HUB との間で完全に自由な通信が実現し、事実上 LAN の厳しいファイアウォールを越えて外部のホストとの通信ができるようになる。

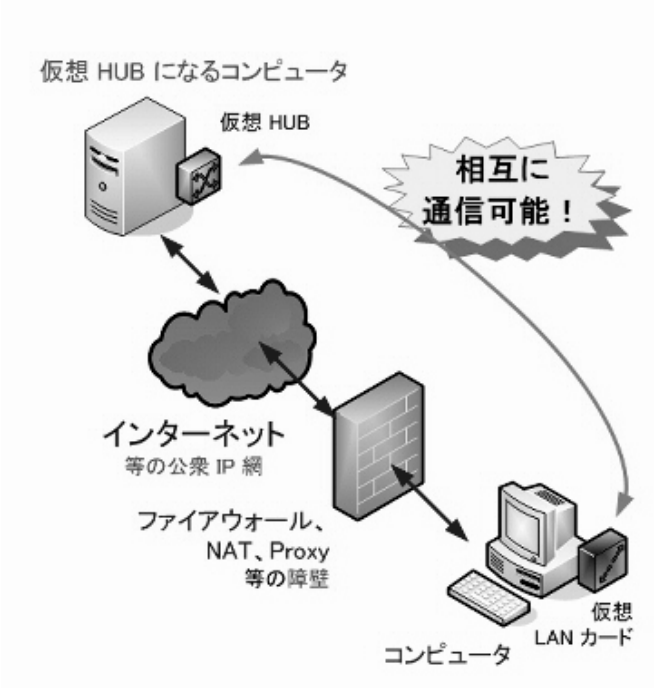

図 5 ファイアウォールを越えた
Ethernet レベルでの自由な通信

SoftEtherプロトコルは、他にもSOCKSサーバーや SSH サーバーなどを経由して仮想 HUB に接続することもできる。使用するプロトコルは、利用するネットワーク環境において、利用者が適切に選択することができる。

SoftEther プロトコルは、既存のファイアウォールを越えて外部の仮想 HUB に接続し、セッションを確立することを機能にするため、柔軟性を持ったつくりになっており、ほとんどの企業ファイアウォールや Proxy などを通過して仮想 HUB に接続することが可能である。図 5 のように、ファイアウォールを経由して外部のホストと Ethernet (MAC)レベルでのパケットを送受信することができる。

6. SoftEther による仮想ネットワーク

SoftEther は優れた仮想ネットワーク機能を提供する。SoftEther が持つ主な機能と利用方法には以下のようなものがある。

SoftEther プロトコル SoftEther の仮想 HUB と仮想 LAN カードの間の通信で使用される専用プロトコル。SoftEther プロトコルを含むパ

ケットを「SoftEther パケット」と呼ぶ。SoftEther プロトコルは TCP/IP 上で動作し、基本的に仮想 LAN カードがインストールされているコンピュータから仮想 HUB がインストールされているコンピュータに対して TCP/IP パケットが届く場合であれば必ず接続できる。しかし、直接 TCP/IP で仮想 HUB に接続できない環境では、HTTP プロキシサーバーや SSH サーバー、SOCKS サーバーなどを経由して接続することができるので、セキュリティの厳しい社内 LAN でも、外部の仮想 HUB にかなりの確率で接続することができる。

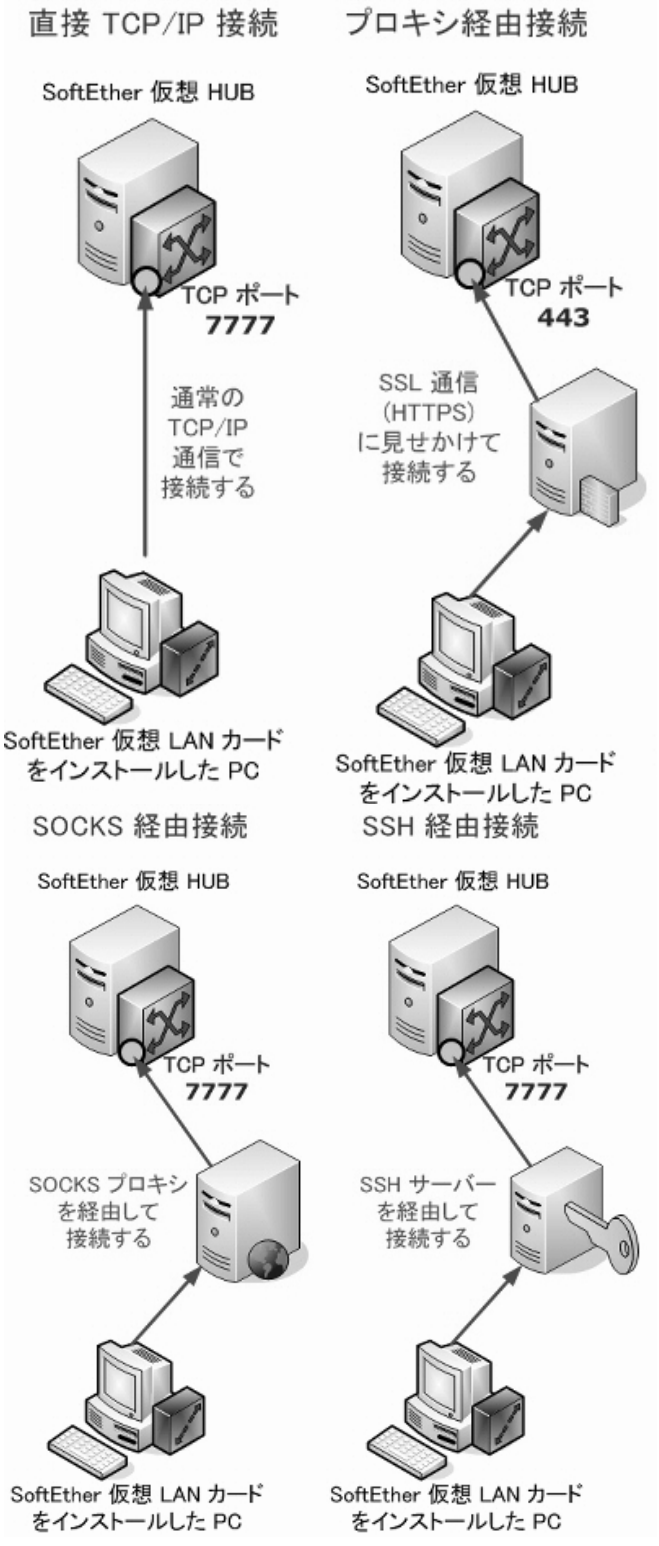

図 6 SoftEther で使用可能な 4 つの接続方法

SoftEther プロトコルによる接続方法

SoftEther プロトコルは TCP/IP をベースにしており、OS やネットワーク機器、ファイアウォールから見ると、一般的な TCP/IP パケットと何ら変わりは無く、ファイアウォールや NAT を通過できる。通過できない場合や、ネットワーク内で Proxy サーバーなどが唯一の外部とのゲートウェイである場合でも、SoftEther プロトコルは Proxy サーバーや SSH サーバー、SOCKS サーバーを経由して外側にある仮想 HUB と接続可能である。具体的には、SoftEther プロトコルは待ち受けポートとして TCP/7777 および TCP/443 を利用する。後者は、通信内容を SSL (HTTPS) 通信であるかのように Proxy を誤解させるためのものである。これらのポート番号は仮想 HUB で常に待機状態となっているが、仮想 HUB の管理者はポート番号を自由に変更することもできる。

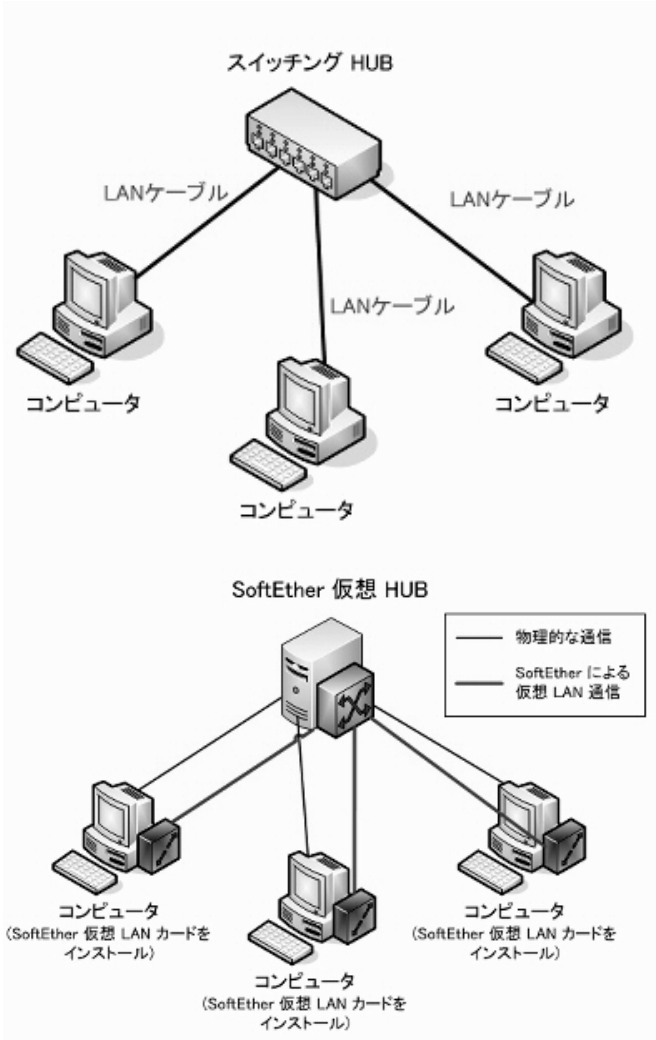

図 7 SoftEther 仮想 LAN と物理的な LAN との比較

仮想 MAC アドレス SoftEther 仮想 LAN カードごとに固有に付けられた MAC アドレス。仮想 LAN カードも Ethernet 的に見ると一般的な LAN カードと変わらず、相互の通信

には MAC アドレスが必要不可欠である。SoftEther 仮想 LAN が物理的な LAN とのブリッジを行っていない場合は、各仮想 LAN カードの仮想 MAC アドレスはその仮想 LAN 内のみで一意であれば問題無いが、仮想 LAN と物理的な LAN をブリッジ接続する場合、仮想 LAN 内の各仮想 LAN カードの MAC アドレスは物理的な LAN 上の各 LAN カードの MAC アドレスと重複してはならない。仮想 MAC アドレスは、仮想 LAN カードをコンピュータにインストールする際に、コンピュータに装着されている物理的な LAN カードの MAC アドレスやインストール日時などをハッシュした値をもとにしたものが設定されるので、偶然重複してしまう可能性は限りなく低いが、ユーザーが後から自由に変更することも可能である。

仮想 LAN 上で利用可のプロトコル SoftEther 仮想 LAN カードは、OS や各ソフトウェアから見ると一般的な LAN カードと同じに見えるので、仮想 LAN 内では OS がサポートしているすべてのプロトコルを任意に使用することができる。たとえば、Windows は TCP/IP や IPv6、NetBEUI、IPX などをサポートしているが、これらはすべて仮想 LAN 内で使用可能である。

プライベート IP アドレス SoftEther で構成された仮想 LAN 内で TCP/IP を使用して通信を行う際は、通常はその仮想 LAN 内で通用するプライベート IP アドレスを決めておくのが一般的である。もちろん、内部でグローバル IP アドレスを使用して、物理的 LAN との間でルーティングまたはブリッジ接続することも可能であるが、IP アドレスが枯渇している現状ではあまりそのようなことはしないだろうから、通常はプライベート IP アドレスを使用することになる(物理 LAN とブリッジ接続する場合は、物理 LAN 側が使用している IP アドレスのルールに基づいて使用することも可能である)。

DHCP の利用 SoftEther 仮想 LAN 内でも、DHCP サーバーを立ち上げることができる。この場合、仮想 LAN に接続する複数台のコンピュータは、個別に IP アドレスを設定する必要が無くなる。この方法で注意しなければならないのは、SoftEther 仮想 LAN と物理的な LAN をブリッジ接続する場合である。既存の物理的な LAN 上に DHCP サーバーがある場合、2つの DHCP サーバーが競合してしまい、大規模なネットワークトラブルに発展する可能性があるので、DHCP を運用する場合は TCP/IP ネットワークに関する詳しい知識が必要となる。

デフォルトゲートウェイ 仮想 LAN カードも OS から見れば普通の LAN カードであるため、仮想 LAN カード上で TCP/IP を設定し、仮想 LAN 上の1台のコンピュータで NAT サービスなどのルーティングサービスを有効にしておけば、その仮想 LAN に接続されたコンピュータは NAT となっているコンピュータの IP アドレスをデフォルトゲートウェイに設定することにより、すべてのインターネットに対してのパケットは仮想 LAN 上を経由して流れることになる。これは、社内 LAN などでインターネットアクセスの制限が多い場合に特に役に立つ。

ブリッジ接続 仮想 LAN は Ethernet の仕様に基づいた LAN であるが、あくまでもソフトウェア的に実装された仮想的なものであるので、実際の通信は LAN ケーブルではなく SoftEther パケット内にカプセル化されており、そのままでは物理的な LAN と接続することができない。しかし、仮想 LAN と物理的な LAN の間をブリッジ接続することにより、仮想 LAN と物理的な LAN が同じネットワークセグメントに属しているかのように自由に通信することができるようになる。これを、仮想 LAN と物理的な LAN とのブリッジ接続と言う。ブリッジ接続は、OS がブリッジドライバを持っている必要があるので、Windows XP / Windows Server 2003 以降で使用可能である。

ブリッジ接続の方法 ブリッジ接続を行うには、ブリッジ接続したい物理的な LAN に物理的に接続されているコンピュータに仮想 LAN カードをインストールし、仮想 LAN に接続した状態で、2 つのネットワークアダプタに対して Windows 上で「ブリッジ接続」を構成する。ブリッジ接続が成立したら、仮想 LAN と物理的な LAN は実際に接続されている状態と同等になるので、その仮想 LAN に接続している仮想 LAN カードをインストールしたコンピュータと物理的な LAN 上のコンピュータは、Ethernet レベルで完全に自由に通信を行えるようになる。

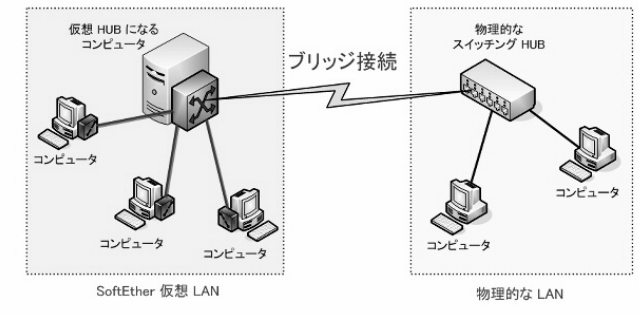

図 8 ブリッジ接続

ブリッジ接続の利点 ブリッジ接続は物理的な LAN 上の物理的な HUB と、仮想 LAN 上の仮想 HUB とを「カスケード接続」するようなものである。カスケード接続とは、物理的な2つ以上の HUB をクロスケーブルなどで接続することにより、双方の HUB に接続されているコンピュータが自由に通信できるようにするものであるが、仮想 LAN と物理的な LAN との間のブリッジ接続により、これと全く同等の状態を作ることができる。

ある物理的な LAN と仮想 LAN をブリッジ接続したい場合は、物理的な LAN と仮想 LAN の両方に接続されているコンピュータ1台のみでブリッジを構成すればよい。すると自動的にそれぞれの LAN に接続されているすべてのコンピュータは相互に通信が可能になる。その際のフレーム パケットはブリッジとなったコンピュータを通過することになる。

通常、仮想 LAN に接続されているコンピュータは実際には何らかの物理的な LAN (社内 LAN など) に接続されている場合が多いのだから、そのコンピュータ上でブリッジを構成することにより、物理的な LAN 上のコンピュータすべては仮想 LAN とも接続可能になる。さらに、ブリッジ接続を行うには、物理的な LAN のネットワーク管理者に設定を依頼すること無く、コンピュータを持っているユーザーであれば誰でも自由にブリッジ接続を行うことができ、これを防止する簡単な手段は存在しない。

仮想 HUB と仮想 LAN カードの共存 本来、仮想 HUB は Ethernet 上での物理的なスイッチング HUB をソフトウェア的に実装したものであるので、単独のソフトウェアとして1台のコンピュータで動作させるものであるが、それだと少数のコンピュータ同士で相互接続を行う際に仮想 HUB を動作させるためだけに専用のコンピュータが1台必要になる。

そこで、図 9 のように、仮想 HUB と仮想 LAN カードをまとめて1台のコンピュータにインストールし、そのコンピュータは仮想 HUB であるサーバーとしての機能も、仮想 LAN カードであるクライアントとしての機能も同時に持つことができる。この場合、このコンピュータの仮想 LAN カードの接続先アドレスは自分自身 (localhost) を指定する。

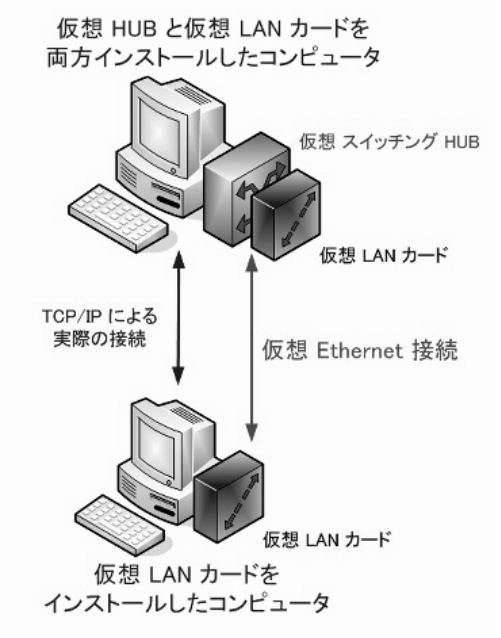

図 9 仮想 HUB と仮想 LAN カードを同じコンピュータで動作させる図

7. SoftEther の活用方法

SoftEther のシステムを使用すると、場所的またはネットワーク的に離れた場所にある複数台のコンピュータ同士、コンピュータと LAN、または LAN と LAN 同士が相互に接続し、Ethernet レベルで自由に通信することができるようになる。

もちろん、これは社内 LAN のファイアウォールや Proxy を越えた形で行うことができ、インターネットを経由して世界中から複数台のコンピュータが 1 つの仮想 LAN に接続したり、その仮想 LAN と物理的な LAN とをブリッジ接続したりすることも簡単にできるようになる。

PC to PC 接続ネットワーク的に離れた場所にある2台以上のコンピュータを自由に通信できるようにするための利用方法。2台以上のコンピュータのうち1台で SoftEther 仮想 HUB を稼動させ、各コンピュータに SoftEther 仮想 LAN カードをインストールして仮想 HUB に対して接続させることにより、接続したすべてのコンピュータ間でネットワーク上の障壁を越えて自由に通信することができるようになる。仮想 HUB は、それに接続したい各コンピュータから SoftEther プロトコルによって接続できる場所にある必要がある(つまり、仮想 HUB はグローバル IP アドレスを持っているかマッピングされている必要がある)。通常はインターネット上のグローバル IP アドレスを持ったマシン上に設置する。図 10 のような接続方法となる。会社内などでこのような接続を行う際には、その社内 LAN を利用するユーザーであれば、自分のコンピュータをこのように設定すれば勝手に行うことができるが、事前にシステム管理者の

同意を得ておくことを強く推奨する。

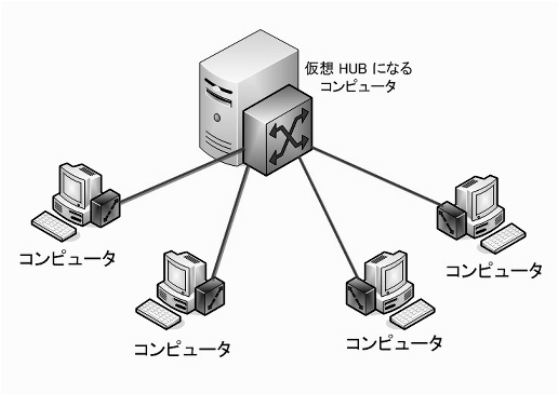

図 10 SoftEther による PC 同士の接続
（1つの仮想 LAN を構成しすべての PC がそれに接続する形）

PC to LAN 接続 SoftEther の利用形態の1つ。コンピュータを離れた場所から社内 LAN に接続し、自由に通信させたい場合などに利用する。社内 LAN に接続されているコンピュータのうち1台に仮想 LAN カードをインストールする。また、そのコンピュータと、離れた場所から接続したいコンピュータの両方から接続できる場所に仮想 HUB をインストールしたコンピュータを置く。通常はインターネット上のグローバル IP アドレスを持ったマシン上に設置する。社内 LAN で仮想 LAN カードをインストールした1台のコンピュータ上で、社内 LAN に接続されている LAN カードと仮想 LAN カードの間でブリッジ接続を構成する。また、仮想 HUB にも接続する。この状態で、仮想 LAN と社内 LAN はブリッジ接続されたことになるので、その仮想 LAN に接続したコンピュータはすべて社内 LAN と自由に通信することができるようになる。これは VPN としての利用形態である。会社内などでこのような接続を行う際には、その社内 LAN を利用するユーザーであれば、自分のコンピュータをこのように設定すれば勝手に行うことができるが、事前にシステム管理者の同意を得ておくことを強く推奨する。

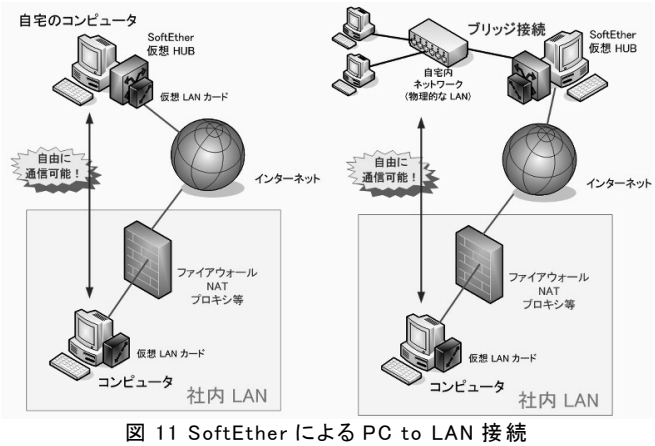

図 11 SoftEther による PC to LAN 接続
（片方の物理的 LAN と仮想 LAN をブリッジ接続する形）

LAN to LAN 接続 SoftEther の利用形態の1つ。離れた場所にある2つ以上の物理的な LAN 同士を SoftEther を利用してブリッジ接続することにより、相互で Ethernet レベルの自由な通信が可能となる。具体的には、接続したい各 LAN 上で1台ずつのコンピュータを選び、SoftEther 仮想 LAN カードをインストールする。そして、これらのコンピュータから接続可能な位置に SoftEther 仮想 HUB をインストールする。状況によっては、仮想 HUB は仮想 LAN カードをインストールしたコンピュータのうちの1台と共存することもできる(詳しくは「仮想 HUB と仮想 LAN カードの共存」を参照のこと)。この状態で、各コンピュータが仮想 HUB と接続し、各コンピュータ上で仮想 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、各 LAN 同士が SoftEther 仮想 LAN を経由してすべてカスケード接続 (ブリッジ接続) された状態になり、各 LAN 上のコンピュータは自由に通信することができるようになる。これは VPN としての利用形態である。会社内などでこのような接続を行う際には、その社内 LAN を利用するユーザーであれば、自分のコンピュータをこのように設定すれば勝手に行うことができるが、事前にシステム管理者の同意を得ておくことを強く推奨する。

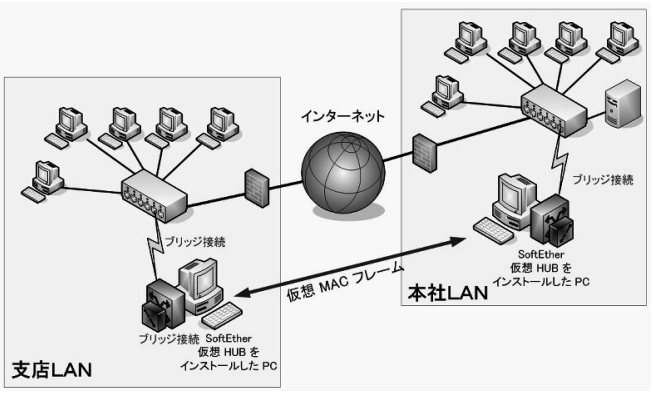

図 12 SoftEther による LAN to LAN 接続
（LAN 同士を仮想 LAN にブリッジする形）

制限の厳しい社内 LAN での活用 社内 LAN で SoftEther を使用すると、既存の社内 LAN と外部に任意に設置した SoftEther 仮想 HUB との間で SoftEther 仮想 LAN を構築することができ、既存の厳しいセキュリティをすべて回避した自由な通信が可能になる。たとえば、自宅に常時接続を持っているユーザーの場合、自宅のコンピュータに SoftEther 仮想 HUB と仮想 LAN カードをインストール・起動しておき、仮想 LAN カードと物理的なインターネットに接続されている LAN カードとの間で NAT を有効にしておく。Windows の場合は、「インターネット接続の共有」が利用できる。この状態で、社内のコンピュータにも SoftEther 仮想 LAN カードをインストールし、自宅の IP アドレスを指定して自宅の仮想 HUB に接続する。そして、デフォルトゲートウ

ェイを仮想 LAN 上の自宅のコンピュータに設定すると、インターネットへのアクセスが完全に自由に行えるようになる。自宅のコンピュータのファイルも自由にコピーすることができる。SoftEther プロトコルは、直接的な TCP/IP 接続が利用できない場合は、HTTP Proxy 経由接続、SOCKS 経由接続、SSH 経由接続をサポートするので、社内 LAN のシステムに合わせて設定することにより、大抵の社内 LAN で外部と接続することができる。

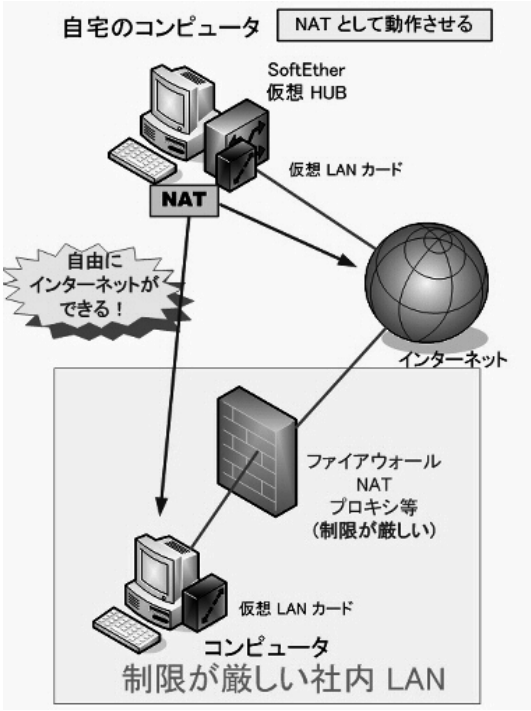

図 13 社外に NAT を立てておき SoftEther 経由で社内 LAN からアクセスしてインターネットを利用する活用法

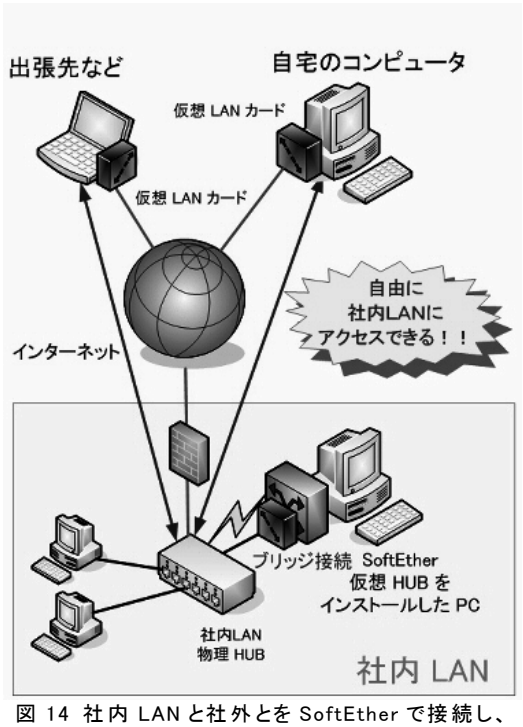

図 14 社内 LAN と社外とを SoftEther で接続し、出張先や自宅から自由にアクセスする活用法

図 14 の方法では、社内に SoftEther 仮想 HUB を立てておき、出張先や自宅からそれに接続することによって社内 LAN に自由にアクセスして仕事の続きを行える例を示している。ただし、この図の方式を使うには、外側から内側への SoftEther 仮想 HUB の TCP/IP ポートへのアクセス許可がファイアウォールによって必要であり、一般ユーザーがこのようなことを行うのは難しい。

そこで、このような場合はインターネット側に SoftEther 仮想 HUB を立てればよい。社内 LAN からインターネット側の仮想 HUB へのアクセスは、ファイアウォールや Proxy があっても容易に可能であるので、接続したままの状態にしておき、出張先や自宅などから同じ HUB に接続すればよい。こうすることによって、ファイアウォールの設定を変更しするために管理者の手を煩わせることなく、社内のイントラネットに自宅からアクセスして仕事の続きができるので大変便利なのだが、このような利用を行う場合は、事前に社内のシステム管理者の承諾を得てから行うべきである。

7. SoftEther プロトコルの持つ機能

SoftEther プロトコルは、その安全性・安定性の向上のために、以下のような機能を含んでいる。

ユーザー認証 SoftEther 仮想 HUB は、TCP/IP 的に見るとサーバー ソフトウェアであり、各仮想 LAN カードから接続する際にはユーザー認証を必要とすることができる。ユーザー認証にはユーザー名とパスワードが使用され、128-bit MD5 ハッシュ・アルゴリズムおよび 128-bit RC4 互換暗号化アルゴリズムを使用したチャレンジ＆レスポンス方式による安全な認証を行うことができる。

暗号化通信 SoftEther プロトコルでの通信は、デフォルトですべて暗号化される。暗号化レベルは 128-bit で、アルゴリズムには RC4 互換暗号化アルゴリズムを使用できる。共有鍵はユーザー認証時のチャレンジ＆レスポンス処理で安全に交換される。

電子署名 パケットの改ざんを防ぐため、SoftEther プロトコルでの通信は、すべて電子署名が付加されている。電子署名には 128-bit MD5 ハッシュ・アルゴリズムが使用される。

自動再接続機能 SoftEther プロトコルでの通信

(TCP/IP による仮想 LAN カードと仮想 HUB 間の通信) が TCP/IP 的に切断されてしまったり、SoftEther 仮想 LAN カードをインストールしたクライアントの物理的な接続が切れた場合 (LAN ケーブルが抜けた、PHS や無線 LAN で電波が途切れたなど)、SoftEther プロトコルは切断を認識し、次に接続に成功するまで再接続を試行する。再接続は、デフォルト設定では接続に成功するまで永久に行われるが、設定を変更して一定回数だけ再接続を試行したり、自動再接続を無効にすることもできる。

セッション再接続機能とバッファリング 自動再接続機能により SoftEther 仮想 HUB に対して再接続した場合、前回の切断時から 60 秒以内に再接続すれば、仮想 LAN 上では切断が行われていなかったかのように動作する機能がセッション再接続である。これは、仮想 HUB と仮想 LAN カードの両方で、相手先に送るべき Ethernet パケットを切断中もバッファリングしておき、接続が再開したら再同期処理を行って相手先に送信することにより、Ethernet レベルでのパケットロスは全く無かったかのように振る舞うことが可能である。この機能は、モバイルネットワークや品質の悪いインターネット接続回線 (遠距離 ADSL など) で非常に有効な機能である。仮に、再接続前と再接続後の物理的な IP アドレスが変化した場合でも、問題無く再接続できる。再接続のために、初回接続時の認証時に 128-bit 暗号で交換される 128-bit のセッション ID が使用される。

デフォルトゲートウェイ設定による通信切断の防止機能 SoftEther では、SoftEther 仮想 LAN 側のホストで NAT やルーターを動作させ、各 SoftEther 仮想 LAN カードをインストールしたコンピュータは、接続後はそのコンピュータをデフォルトゲートウェイとして通信することができる。しかし、単純にこれを行ってしまうと、SoftEther 仮想 LAN への接続が完了した瞬間、コンピュータのデフォルトゲートウェイがこれまでの物理的な LAN 側から仮想 LAN 側へ移動してしまい、SoftEther プロトコルが必要とする TCP/IP 通信のパケットも仮想 LAN カード側を通ろうとするので、無限ループが発生し、そのコンピュータは SoftEther 接続がタイムアウト切断されるまで完全に通信不能になってしまう。これを防止するため、SoftEther 仮想 LAN カードドライバは仮想 HUB への接続完了後デフォルトゲートウェイを移動する直前に、その仮想 HUB の IP アドレスへの接続に必要な物理的な LAN 側を通るためのサブネットマスク 255.255.255.255 のスタティックルーティングテーブルエントリを追加する。この機能によって、デフォルトゲートウェイを仮想 LAN 側のホストに設定する場合でも、問題無く通信できる。

図 15 仮想 HUB への接続アカウントの設定画面

8. SoftEther 仮想 HUB の持つ機能

SoftEther 仮想 HUB は、以下のような機能を持っている。

スイッチング機能 仮想 HUB は、Ethernet レベルでは一般的なスイッチング HUB (Layer-2 スイッチ) と同様に機能する。すなわち、各仮想 MAC フレームの宛先 MAC アドレスを見て、対応するポート (仮想 LAN カードからの接続) に対して送出する機能である。実験により、SoftEther 仮想 HUB は、現在 Celeron 2.0GHZ 搭載のコンピュータにて最大 50 Mbps 以上の性能を出せることがわかった。

管理コンソール機能 仮想 HUB の管理者は、Telnet 接続を用いて仮想 HUB のポート 8023 に接続し、仮想 HUB のすべての管理機能にアクセスすることができる。仮想 HUB のメンテナンス Telnet 接続は、物理的な LAN やインターネット経由でも行えるが、それ自身の仮想 HUB によって構築した仮想 LAN を経由して接続することも、システム構成によっては可能である。

Layer-3 ログ機能 仮想 HUB では、各ユーザーの接続 / 切断ログ以外に、各ユーザーが実際に送受信したパケットの内容 (ヘッダ情報) をログファイルとして常に保存することが可能である。仮想 HUB は各パケットを Layer-3 以上のレベルで解釈し、IP パケット、TCP パケットの接続・切断、TCP パケットによるデータ転送、DHCP によるアドレス割り当て、ARP による MAC アドレス解決などの重要なイベントのみを細かく設定してログをとることができる。すべてのログを有効にした場合は、パケット数と同じだけのログ行数になり、1時間あたり数 100 MBytes になってしまうこともあるが、このような場合でもログへの書き込みキャッシュを自

動的に最適化するため、ログ保存のためのパフォーマンスの影響は少ない。

Layer-3 パケットフィルタ機能 仮想 HUB は、物理的な HUB と異なり、離れたところから複数のコンピュータが接続できる。その中の1台でおかしな設定をしたものがあったり、悪意をもったものがあったりすると、その仮想 HUB で構成される仮想 LAN 全体に影響が出るばかりか、物理的な LAN まで影響が広がる場合もある。物理的な HUB であればケーブルを抜いておけばいいのだが、仮想 HUB では予めそのような変なパケットを通さないようにしておけば大変安心である。仮想 HUB には、オプションとして Layer-3 パケットフィルタ機能を搭載している。一般的に用いられている Layer-3 スイッチのすべての機能は搭載することができていないが、SoftEther 仮想 LAN 上で必要になると思われる基本的なセキュリティ機能を多く搭載している。これらのパケットフィルタ設定は、ユーザーごとに設定できる。たとえば、DHCP を禁止するオプションは各クライアントが接続の際に使用するユーザーで設定しておき、DHCP サーバーとして動作させたいコンピュータが接続する際に使用するユーザー名のみこのオプションを設定しておかなければよい。
パケットフィルタオプションの一部を以下で紹介する。

① DHCP サーバーの動作を禁止する
そのユーザーの接続は、DHCP サーバーとして動作することを禁止する。具体的には、DHCP OFFER と DHCP ACK パケットを無視する。1つの仮想 LAN 内で複数の DHCP サーバーを動作させないためである。

② DHCP パケットをすべて禁止する
そのユーザーの接続は、すべての DHCP パケットの送受信を禁止する。2つ以上の LAN を SoftEther によってブリッジ接続する際、各 LAN にすでに DHCP サーバーが存在していると、ブリッジ接続した瞬間、DHCP 競合が発生する。そのような場合にこのオプションを有効にする。

③ DHCP が割り当てた IP アドレスを強制する
クライアント コンピュータが使用する IP アドレスは、DHCP サーバーが割り当てた IP アドレスのみ使用できるようにする。その他の IP アドレスを発信元としたパケットはすべて無視する。これは、CATV インターネット接続業者などが使用している専用ルーターで使用されている機能をソフトウェア的に実装したものである。

④ IP アドレスを1つに制限する
各クライアントの仮想 LAN 内での IP アドレスを1つに制限する。1つの仮想 LAN クライアントが複数の IP アドレスを持つことを禁止し、最初の IP アドレスのみ有効にする。

⑤ MAC アドレスを1つに制限する
各クライアントの仮想 LAN 内での MAC アドレスを1つに制限する。1つの仮想 LAN クライアントが複数の MAC アドレスを持つことを禁止し、最初の MAC アドレスのみ有効にする。これを有効にすると、その接続のクライアント コンピュータ側ではブリッジを構成することはできなくなる。

⑥ 重複する IP アドレスを禁止する
クライアントが仮想 LAN に接続した際、すでに別のクライアントが使用している IP アドレスを使用しようとした場合、そのパケットを無視する。これにより、仮想 LAN 内での IP アドレスの重複による通信妨害を防止する。

輻輳(ふくそう)制御機能 SoftEther プロトコルでは、すべての Ethernet MAC フレームは TCP/IP によって通信される SoftEther パケットにカプセル化される。従って、通常のインターネットや LAN などでは転送能力を超えたパケットが HUB やルーターを流れた場合、そのパケットは無視される (切り捨てられる) のだが、SoftEther 仮想 LAN の場合はすべてのパケットを順番に転送しようとするので、状況によっては大幅な輻輳が発生していまい、通信が不可能になる。特に、悪意のあるユーザーによってブロードキャストパケットによる DoS 攻撃が行われた場合、攻撃の対象となった仮想 HUB がすべてのパケットを正しく転送しようとして、結果的にすべての接続クライアント間の通信が麻痺してしまう。これを防止するため、SoftEther 仮想 HUB には輻輳制御機能が備わっており、現在の回線の転送能力を超えたパケットを切り捨てると共に、大量の DoS 攻撃によるパケットを遮断する。

9. SoftEther ソフトウェアの実装

SoftEther のソフトウェア部分は、大きく分けて、仮想 LAN カードと仮想 HUB の 2 つに分かれる。

仮想 LAN カードは、Windows のデバイスドライバとして実装されている。したがって、Windows の OS 本体や、ネットワーク通信を行おうとするすべてのアプリケーション・ソフトウェアから見れば、全く本物の LAN カードであるかのように見え、すべ

ての通信アプリケーションが動作する。つまりSoftEther が仮想化しているレイヤは Layer-2 のEthernet であるため、それ以上のレイヤでの通信要求はすべて SoftEther 仮想 LAN カードが受け付けることができる。

SoftEther 仮想 LAN カードはカーネルモードで動作する部分とユーザーモードで動作する部分に分かれており、図 16 のように相互協調して動作している。

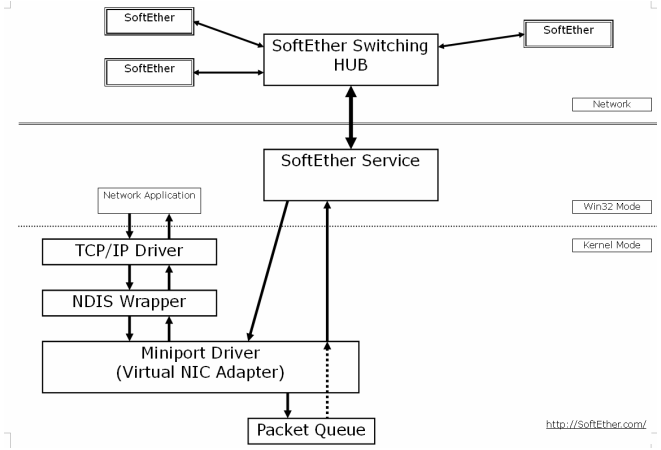

図 16 SoftEther のユーザーモードとカーネルモードでの動作

移植性を高めるために、パケットのカプセル化、暗号化、伝送などの比較的重要な処理を行う部分をなるべくカーネルモードプログラムから除外し、ユーザーモードで実行されるようにした。その結果、独自に記述した Windows NT カーネル対応のデバイスドライバのコードは非常に小さく抑えることができた。もちろんシステムモジュールとして動作しているため、Windows の起動と同時に SYSTEM 権限で起動し、自動的に仮想 HUB に接続することもできる。

図 17 Windows のデバイスドライバとして実装された SoftEther 仮想 LAN カード

SoftEther 仮想 HUB は、Windows のサービスプロセスとして動作する。HUB のコードはすべてユーザーモード用として書かれており、Linux などへの移植が容易になるように注意して開発した。

SoftEther は、フリーソフトウェアとして公開され、プロトコル仕様などもオープンになる。2003 年 11 月に SoftEther の情報とベータ版を配布するサイト http://www.softether.com/ を立ち上げた。同サイトでは、期間限定で SoftEther の便利さを体感してもらうため、誰でも無料で接続できる実験用の Anonymous HUB を公開する予定である。

SoftEther ソフトウェア本体は、現在のところ、Windows 2000、Windows XP、Windows Server 2003 に対応している。将来的には、Linux や PC-UNIX などにも対応したい。ソースコードの大半を Win32 API に依存しないように注意して記述したため、比較的容易に移植が可能であると思われる。

SoftEther Web サイト:
http://www.softether.com/
開発者 登 大遊 メールアドレス:
yagi@yagi3.jp

当開発作業はIPA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、アドバイスを受けている。

参考文献

(1) Microsoft Corporation.
Windows Driver Development Kit, January 2003. http://msdn.microsoft.com/

(2) Simoneau Paul. *TCP/IP プロトコル徹底解析*.
ISBN: 4822280373

(3) Olaf Titz. *Why TCP Over TCP Is A Bad Idea*.
http://sites.inka.de/sites/bigred/devel/tcp-tcp.html

(4) ASCII CORPORATION.
Best of msdn magazine 2000.
ISBN: 4756136680

(5) ASCII CORPORATION.
WDM デバイスドライバプログラミング完全ガイド
ISBN: 4756133967