イーサネットのソフトウェア実装とトンネリングシステムの開発

安全でかつ自由な仮想ネットワーク(VPN)を手軽に実現する『SoftEther』

開発代表者：　　登　大遊
担 当 ＰＭ：　　竹内　郁雄
プロジェクト管理組織：　　三菱マテリアル株式会社

１．背景

本来、インターネットは、世界中のコンピュータ同士が自由に通信できることを目的として構築されたものである。　しかし、現状ではグローバル IP アドレスの不足に伴い、NAT の導入とプライベート IP アドレスの活用が進んでいる。　また、機密性の高い内部ネットワークをインターネットから分離するため、セキュリティ対策の導入が進んでいる。　このため、現在では、必ずしも自由な通信が行えない状態にある。

特に、インターネット上で TCP/IP による通信を行うためには、少なくとも片方はグローバル IP アドレスを持つ必要がある。

本プロジェクトでは、Ethernet に対応した LAN カードやスイッチング HUB などのネットワーク機器をソフトウェア（SoftEther）で仮想的に実装する。　SoftEther は、この仮想ネットワーク機器間の伝送をカプセル化されたフレームパケットにより実現する、新たなトンネリングシステムである。　このため、仮想 HUB ソフトウェアをグローバル IP アドレス上で動作させておけば、インターネット上に自由な仮想ネットワークを構築可能である。

SoftEther により、すべてのネットワークアプリケーションが透過的に使用可能となることを目標とする。

なお、開発者は筑波大学に所属しているが、学内ネットワークを利用していて、その無線 LAN の使い勝手の悪さから本システムを着想した。

２．目的

本プロジェクトでは、IEEE802.3（Ethernet）プロトコルに対応した LAN カードやスイッチング HUB などを仮想的に実装するソフトウェア（SoftEther）を開発する。SoftEther は、この仮想 LAN カードと仮想スイッチング HUB 間の伝送をカプセル化されたフレームパケットにより実現する、新たなトンネリングシステムである。SoftEther の概念図を図１に示す。

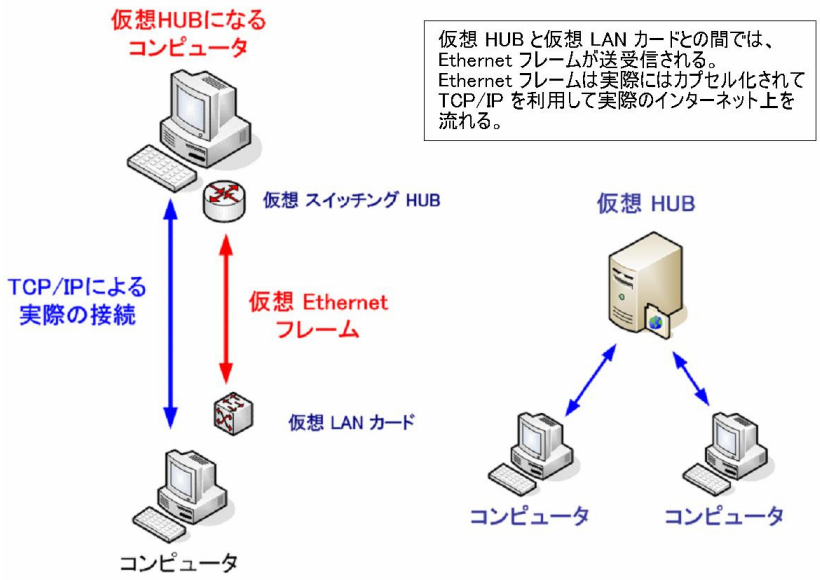


図1　SoftEtherにより実現する仮想ネットワークの概念図

まず、(1)直接的な TCP/IP 接続、(2)HTTP プロキシ経由接続、(3)SOCKS 経由接続、(4)SSH 経由接続に対応した伝送モジュールを組み込むとともに、(a)簡単なインストールと接続が可能な操作性、(b)ユーザー認証とパケットの 128bit 暗号化によるセキュリティ、(c)一時的に接続が切れた際の双方でのバッファリングと再同期機能を実現した。

図2　仮想HUBと仮想LANカードとの間の通信方法

Windows 版（Windows 2000 以降）については、12 月 17 日に公開開始後、順次改訂し、現在は Version 1.0 が最新である。

その他の OS のサポートについても準備を進めており、現在、Linux 版、Free BSD

版並びに Mac OS X版の仮想 HUB ソフトウェアを開発中である。　未公開ではあるものの、一通りの動作について確認済みである。

３．開発の内容

SoftEther については、公式 Web サイト（http://www.softether.com/）で詳細なドキュメントを公開している。　こちらを参照願う。　以下では、概略を紹介する。

３．１　Ethernet フレームの解析、仕様調査

SoftEther の設計・開発に先立ち、IEEE802.3 CSMA/CD（Ethernet）フレームの解析並びに仕様調査を行った。

３．２　仮想ネットワークの設計

SoftEther は、スイッチング HUB と LAN カードをソフトウェア的にエミュレートすることにより、仮想ネットワークを実現するソフトウェアである。

仮想 HUB を特定のコンピュータ上で稼動させておき､そのコンピュータに対して、インターネット等を経由して仮想 LAN カードを接続する。　こうして接続された仮想 HUB と仮想 LAN カードはあたかも仮想 LAN ケーブルによって接続されているかのように振舞う。

仮想 HUB 並びに仮想 LAN カードは、Windows 上のシステムコンポーネントとしてインストールされる。　したがって、全ての通信アプリケーションは仮想 HUB や仮想 LAN カードの存在を意識することなく、仮想ネットワークを利用した通信が可能である。

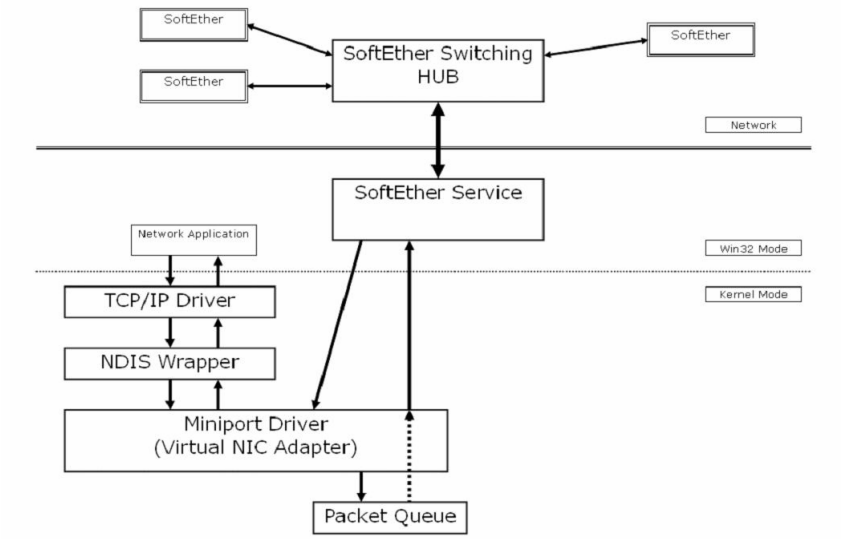


図３ 仮想ネットワークの動作原理

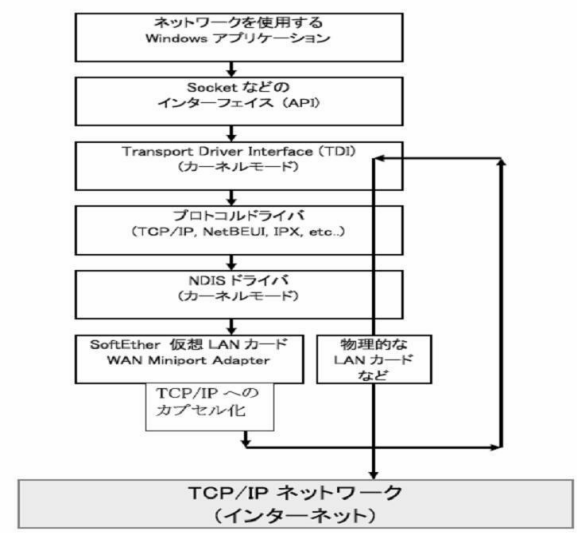
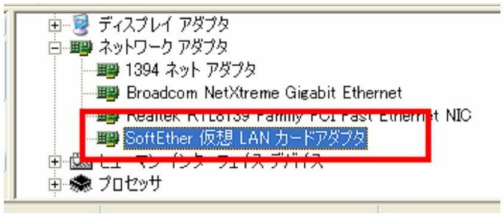


図４　仮想LANカードの動作原理

仮想ネットワークの動作原理を図３に、仮想 LAN カードの動作原理を図４にそれぞれ示す。

３．３　仮想 LAN カードデバイスドライバの開発

仮想 LAN カードは、SoftEther 仮想ネットワークに接続するコンピュータにインストールする仮想のデバイスドライバである。　仮想 LAN カードをインストールすると図５のようになる。　以下では、仮想 LAN カードをインストールしたコンピュータを「仮想クライアント」、仮想 HUB 機能を提供するサーバーを「仮想 HUB」と称する。



デバイスマネージャ／ネットワークアダプタ

コントロールパネル／ネットワーク接続

図５　インストールした仮想LANカード

SoftEther 仮想 LAN カードの最大の特長は、OS やその上で動作するネットワーク通信を行う全てのソフトウェアから、物理的な LAN カードと全く同一に認識されるという点にある。

仮想クライアントを仮想 HUB に接続するためには、「SoftEther 接続マネージャ」を利用する。　接続マネージャで、接続先の仮想 HUB を指定し、接続を開始すると図６のように仮想ネットワークに接続される

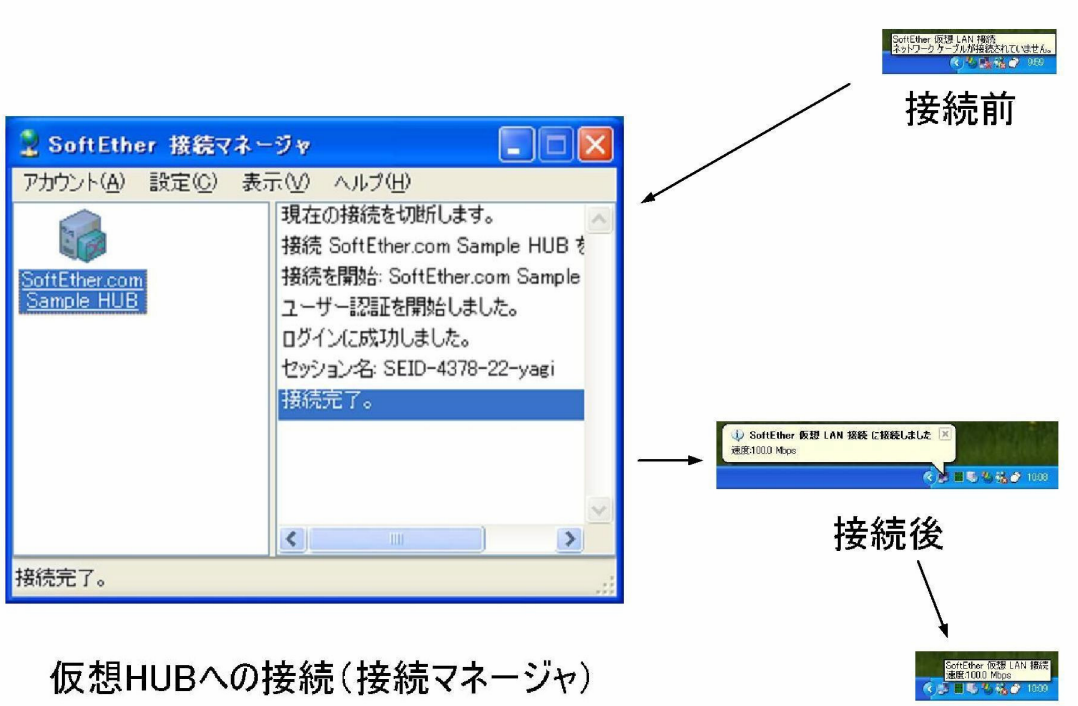


図６　仮想ネットワークへの接続

３．４　仮想 HUB ソフトウェアの開発

仮想 HUB は、通常のスイッチング HUB（Ethernet 100Base-TX Switch）をエミュレートするソフトウェアであり、仮想 HUB 機能を提供するコンピュータ上に常駐するサーバープロセスである。

IEEE802.3（Ethernet）に準拠しており、基本はレイヤー２の処理であるが、IP 層、TCP/IP 層、アプリケーション層での高度な処理（セキュリティ機能）を搭載している。

表１　仮想HUBと仮想クライアントの接続方法

直接TCP/IP接続 ・仮想HUBが、仮想クライアントと同じネットワーク上に存在する場合や、NATやファイアウォールなどを経由して直接接続可能な場合に適用
HTTPプロキシ経由接続 ・外部との通信は全てHTTPプロキシサーバーを経由して行う構成となっているネットワーク環境に適用
SOCKSサーバー経由接続 ・SOCKSサーバー(現在はSocks v4のみに対応)を経由して通信する
SSHサーバー経由接続 ・SSHのPort Forwarding機能を使用して、SSHサーバーを経由して通信する

現在、仮想 HUB と仮想 LAN クライアントの接続方法としては、表１に示す通信方法をサポートしている。　いすれの方法を用いるかについては、仮想クライアントの SoftEther 接続マネージャ上で、接続先の仮想 HUB を登録する際に設定する（図７～11 参照）。

図７　仮想HUBと仮想クライアントの接続方法の設定

図８　直接TCP/IP接続の場合

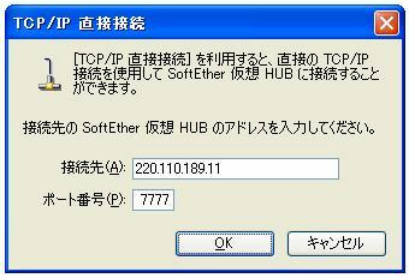


図９　HTTPプロキシ経由接続の場合

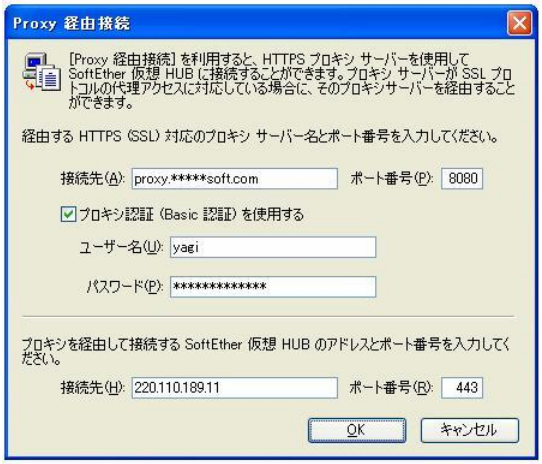


図10　SOCKSサーバー経由接続の場合

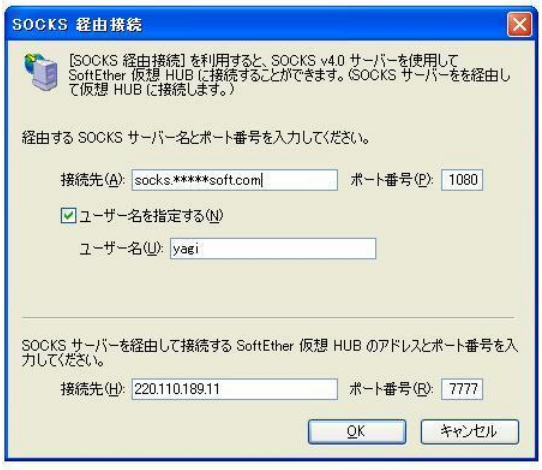
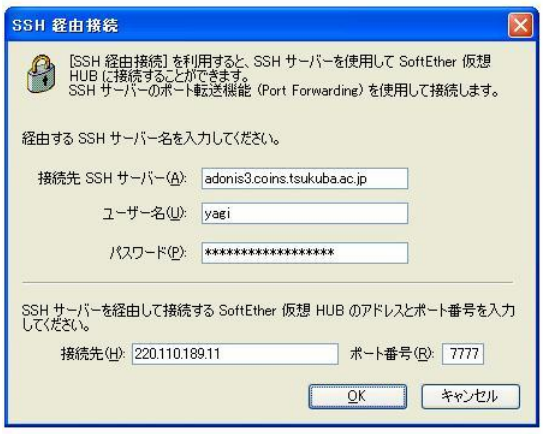


図11　SSHサーバ経由接続の場合



現在、仮想 HUB を管理する方法として、管理コンソールを提供している。

管理コンソールへ接続するためには、Telnet クライアント（接続先ポート番号 8023）を利用する。　なお、SoftEther をインストールしたコンピュータでは、「SoftEther 仮想 HUB Telnet 管理クライアント」（図 12）が利用できる。

図12　SoftEther仮想HUB Telnet管理クライアント

管理コンソールでは、表２に示すような機能を提供している。

表２　仮想HUB管理コンソールの主要機能

a．メインメニュー

メインメニュー	
0	状態表示
1	ユーザー管理
2	セッション管理
3	プロトコル管理
4	パスワード設定
5	ログ管理
9	ログアウト（切断）

b．ユーザー管理メニュー

ユーザーの管理	
1	ユーザー一覧
2	ユーザー作成
3	ユーザー削除
4	ユーザー情報表示
5	ユーザー情報編集
9	ユーザー管理の終了

c．セッション管理メニュー

セッションの管理	
1	セッション一覧
2	セッション情報表示
3	セッション強制切断
4	MACアドレス表示
5	IPアドレス一覧表示
9	終了

d．プロトコル管理メニュー

プロトコル管理	
0	TCP/IP接続（直接接続）
1	HTTPプロキシ経由接続
9	終了

e．ログ管理メニュー

ログ管理メニュー	
0	ログ状態表示
1	ログファイル設定
2	ログ保存設定
9	ログ管理終了

f．ログファイル設定

ログファイルの切り替えスケジュール	
1	切り替え無し
2	1ヶ月ごと
3	1日ごと
4	1時間ごと
5	1分ごと
6	1秒ごと
9	戻る

g．ログ保存設定

ログ保存設定（保存する／保存しない）	
	システムログ
	管理ログ
	アクセスログ
	TCPコネクションログ
	TCPデータログ
	DHCPパケットログ
	UDPパケットログ
	ICMPパケットログ
	ARPパケットログ
	IPパケットログ
	Ethernetパケットログ
	ブロックパケットログ

なお、仮想 HUB では、セキュリティオプションとして以下のものをユーザーごとに設定可能である。

表3 各ユーザーに対して設定可能なセキュリティオプション

接続を拒否する
セッション再接続を禁止する
DHCPサーバーが割り当てたIPアドレスを強制
使用可能なIPアドレスを1つに制限
使用可能なMACアドレスを1つに制限
既存のIPアドレスとの重複を禁止
既存のMACアドレスとの重複を禁止
ブロードキャストパケットを禁止
DHCPサーバーの動作を禁止
すべてのDHCPパケットをフィルタリング

さらに、128bit RC4 互換暗号化と電子署名による盗聴・改ざん防止並びにユーザー認証をサポートしており、また、256 までの VLAN 機能を用意している。これにより、仮想 HUB を実装した 1 台のサーバー上で、最大 256 台の HUB 機能を提供可能である。

３．５ SoftEther プロトコルの実装

仮想 LAN カードと仮想 HUB 間を接続するためのトランスポート層（SoftEther プロトコル）については、図 13 に示す SoftEther フレームを取扱い、各伝送モジュールで送受信することとした。

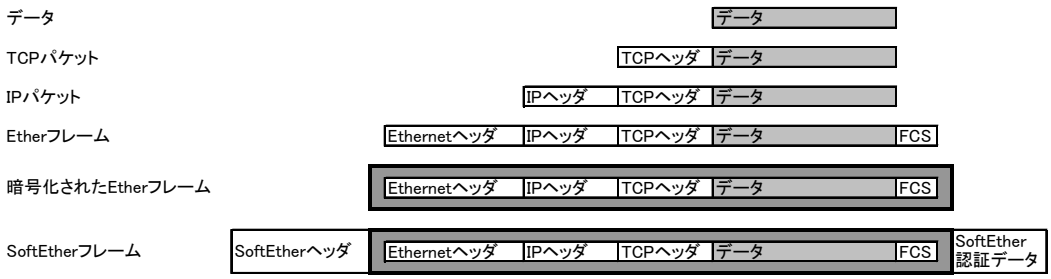


図13 SoftEtherフレームのフォーマットについて

なお、各仮想クライアントは、仮想 HUB との接続経路がどの伝送モジュールに拠るかを意識することなく、全く同等の扱い（図 14）となる。

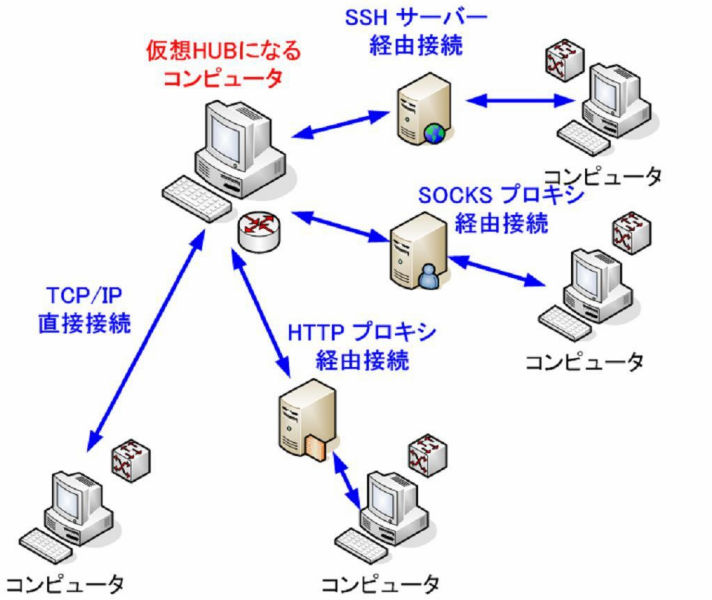


図14　仮想HUBと仮想クライアント間の接続経路

３．６　テスト並びに仕上げ

12 月 17 日の SoftEther ベータ版の公開開始に合わせて、実験用公開仮想 HUB（hub.softether.com, 220.110.189.11、ポート番号：443, 7777）並びにメーリングリスト（softether@ml.open.coins.tsukuba.ac.jp）のサービスを開始し、現在も引き続き、テスト運用とユーザーニーズの収集、開発へのフィードバックを行っている。

現在は Windows 版（Windows 2000 以降）のみ公開しており、Version 1.0 最新である。　その他の OS のサポートについても準備を進めており、仮想 HUB については、未公開ではあるものの Linux 版、Free BSD 版並びに Mac OS X版を開発中であり、一通りの動作について確認済みである。

既にダウンロード数は、累計で 70 万件を超えており、また、実験用公開仮想 HUB の利用も常時 200 ユーザー以上が接続しているといった状況である。

これまでのところ、公開仮想 HUB の性能（DELL 社製 PowerEdge 600SC、Intel Celeron 2GHz、メモリ DDR SDRAM 1GB）では、1,000 ユーザーを超えると並列処理のパフォーマンスが悪化するため、300 ユーザー程度が現実的な目安のようだ。

当該仮想 HUB の性能の限界値としては、トラフィックは 60Mbps 程度が上限と思われ、また、MAC アドレステーブル登録数は 3,000 程度、IP アドレステーブル登録数は 20,000 程度でパフォーマンスが悪化することがわかった。

４．特徴および従来の技術との相違

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、SoftEther による仮想ネットワーク内では OS がサポートしている全てのプロトコルを任意に使用することができる。　例えば、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ネットワーク内で使用可能である。

また、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、「直接 TCP/IP 接続」にてファイアウォールや NAT を通過できる。　直接 TCP/IP 接続で通信できない場合、(1) 外部との通信は HTTP プロキシサーバーを経由して行う構成となっている環境では「HTTP プロキシ経由接続」を、(2) SOCKS サーバーが利用可能な環境であれば「SOCKS サーバー経由接続」を、(4) SSH サーバーが利用可能な環境であれば「SSH サーバー経由接続」を選択することで外側にある仮想 HUB と接続可能となる。

SoftEther により実現する仮想ネットワークの最もシンプルな例は図 1 に示した通り遠隔地にあるコンピュータ同士の接続であるが、仮想クライアント上でブリッジ機能を動作させることにより、図 15 に示すように遠隔地にある LAN 同士を接続することも可能である。

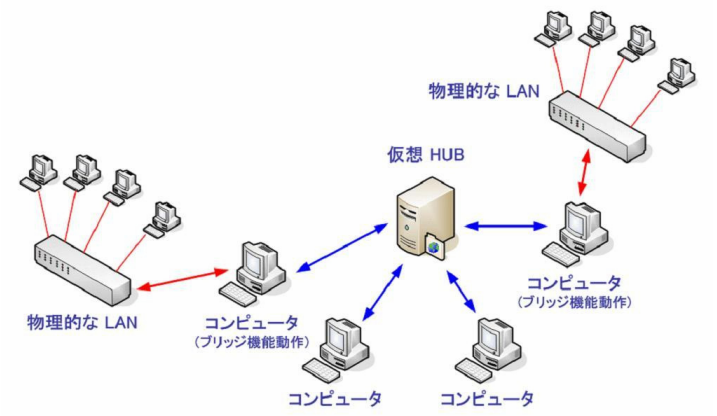


図15　SoftEtherによる遠隔地にあるLAN同士の接続

このように、従来は、高価なハードウェアや専用ソフトウェアの導入が必須であった VPN やリモートアクセスが、SoftEther により容易に可能となった。　また、仮想ネットワーク内では全てのプロトコルを使用できるため、LAN 上の機器に対するアクセスと全く同等の操作が可能であり、一般の利用者でも容易に活用できるという利点がある。

本プロジェクトでは、当初予定していた機能は網羅できたと考えている。

また、最適化に注力した結果、TCP over TCP にもかかわらず、環境にもよるが、実際の転送速度の 60～80%あるいはそれ以上のパフォーマンスが出ることもあり、性能的にも十分評価できるものと考える。

安定性を重視した実装としており、再接続機能による仮想専用線化、双方向でのバッファリングと再同期によるモバイル環境や不安定な ADSL 接続等においても『切れにくい』を実現した。

今後は、認証方式や管理ツールの強化、仮想 HUB のカスケード接続やクラスタ化等に引き続き対応する。　なお、詳細については差し控えさせて頂くが、伝送速度のさ

らなる効率化のアイデアがあり、UDP を使用したトンネリングを行う場合と実用上ほとんど変わらないパフォーマンスを実現可能と考えている。　これらを SoftEther 2 として、モジュール化した設計・実装で SoftEther とは別に開発を行う。

５．期待される効果

SoftEther はネットワーク通信における非常に広い範囲の分野において応用が可能なソフトウェアである。

開発者（登 大遊）は平成 16 年 4 月 1 日付けで「ソフトイーサ株式会社」を設立した。今後、SoftEther の開発・拡張や配布は、ソフトイーサ株式会社を中心して行われることになる予定である。

SoftEther に続いて開発中の SoftEther 2 においては、従来の高価な VPN 専用ハードウェアが必要であったような高負荷環境における VPN システムにおいても、十分導入可能なレベルのシステムを実現したいと考えている。このことにより、離れた場所にあるネットワーク同士を、より安いコストで、かつ非常に安全に接続することが構うになる。

また、個人にとっても SoftEther は非常に便利なソフトウェアである。たとえば、友人や親族などの間で家庭内 LAN 同士を接続することが簡単にできる。家庭用ビデオ機器やテレビゲーム装置など、Ethernet に対応したデバイス同士を、家庭間 VPN によって相互に通信させることも SoftEther を利用すれば非常に容易である。

６．普及の見通し

SoftEther の合計ダウンロード数は、2003 年 12 月から 2004 年 3 月の間で合計 70 万ダウンロードを超え、個人ユーザーおよび法人ユーザーの間において、短期間のうちに一気に普及したと言える。今後、SoftEther および SoftEther 2 において、より大規模な環境においても導入可能な商用版の開発や、通信速度の向上、機能の強化などを行うことにより、VPN のスタンダード・システムとしての地位を確立したいと考えている。

SoftEther はすべてのコンピュータのユーザーにとって有益なソフトウェアであるので、より多くのコンピュータに SoftEther がインストールされ、多くの場面で活用されることを目標として、SoftEther の開発を続けていく所存である。

７．開発者名

登 大遊　（筑波大学第三学群情報学類、ソフトイーサ株式会社代表取締役）
yagi@yagi3.jp

付録

〇関連Ｗｅｂサイト

http://wwww.softether.com/