

SoftEther トンネリングの検出プログラム試作

A Prototype Program for Detecting SoftEther Tunnels

<http://www.tani.cs.chs.nihon-u.ac.jp/g-2005/yoshihiro/>

谷 研究室 相川 善弘

Yoshihiro Aikawa

概要

トンネリングソフト SoftEther を使用した通信を検知するプログラムの作成を試みる。

1:はじめに

インターネットは、通信を見ることができる。ネットワーク上には、ハッキングやウィルスの危険があるので、ネットワーク管理者はファイアウォールを設置する。ファイアウォール間の通信は秘密が守られないので、間の通信をトンネル化する。その場合、すべての通信は管理者がコントロールする。

ソフトイーサは、ユーザーがトンネリングを行うソフトである。ユーザーは便利だが、管理者はコントロールできないので、セキュリティが無効になる危険性がある。ソフトイーサを検知する必要がある。

この研究は、SoftEther を使用した通信を検知する方法を発見し、プログラムの作成を行う事を目的としている。

2:ソフトイーサ【SoftEther】とは？

登大遊氏が開発した、Ethernet の LAN カードとハブの機能をエミュレートするソフトウェア。フリーソフトウェアとして公開されており、誰でも自由に利用できる。

ソフトウェアとして実装された仮想的なスイッチングハブと仮想的な LAN カードにより、TCP/IP ネットワーク上に仮想的な Ethernet ネットワークを構築する。物理的に離れたコンピュータ同士で Ethernet LAN を形成することができるため、いわゆる VPN を構築するためのソフトということもできる。物理的な LAN とブリッジを介して接続することもできる。

仮想 LAN カードはデバイスドライバになっており、OS やアプリケーションからは通常の LAN カードと同じように認識され、特別な対応は必要ない。また、仮想ハブも同様に通常のハブと同じように認識され、利用できる。

データリンク層のレベルで VPN を構築できるため、ファイアウォール等の設定に影響されることが無く、最も自由度が高い VPN システムである。これは、ファイアウォール等の設定を緩和するという危険を冒さな

くても安全に自由度の高い VPN を構築することができるということでもある。

SoftEther 上の TCP/IP 通信は、既存の TCP/IP ネットワークの管理者が監視したり遮断したりすることができない。このため、企業などで不用意に利用すると、管理者のセキュリティ対策が無効になり、重要な情報が流出したり、ウイルスが流入するといった危険に晒される可能性がある。十分な知識と周到な計画に基づいて利用する必要がある。

3:ソフトイーサの特徴

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するプロトコル) 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。

・ SoftEther

Ethernet での LAN カードおよびスイッチング HUB を、ソフトウェア的にエミュレートして仮想化し、これまで自由な通信が困難であった環境でも複数台のコンピュータやネットワーク間を通信することができるようにするソフトウェア。名称は、SoftwareEthernet(ソフトウェア的なイーサネット) に由来する。

・ SoftEther 仮想 HUB

SoftEther の一部として提供される、ソフトウェア的にエミュレートされたスイッチング HUB。単に「仮想 HUB」と呼ぶこともある。複数台の仮想 LAN カードを接続することができ、各仮想 LAN カードを搭載したコ

ンピュータ間での通信を中継する、物理的な Layer-2 スイッチング HUB と同等の働きを行うが、付加機能として Layer-3 レベルでのパケットフィルタリングやログ機能を提供し、仮想 LAN 内での安全性を高めることもできる。

・SoftEther 仮想 LAN カード

SoftEther の一部として提供される、ソフトウェア的にエミュレートされた EthernetLAN カード。単に「仮想 LAN カード」と呼ぶこともある。仮想 LAN カードは仮想 HUB に対して接続する。1 台の仮想 HUB に接続された複数台のコンピュータは、Ethernet レベルで相互に通信することが可能となる。仮想 LAN カードはカーネルモードで動作するデバイスドライバとして実装されている。OS やソフトウェアからは、一般的な LAN カードと全く同等に見えるので、OS 自身の通信を含め、すべてのネットワークアプリケーションが動作する。

・SoftEther 仮想 LAN

SoftEther の仮想 HUB と、1 台以上の仮想 LAN カードをインストールしたコンピュータによって構成される、仮想的なローカルエリアネットワーク (LAN)。この LAN の通信仕様は、仮想的なものであることを除き、すべて Ethernet の仕様に基づいたものである。また、SoftEther 仮想 LAN と、物理的な LAN をブリッジ接続することもできる。

・仮想 MAC フレーム

SoftEther 仮想 LAN 内で仮想的に送受信される Ethernet レベルでのフレームパケット。一般的な Ethernet の仕様に基づいたフレームと同等のものが流れており、仮想 MAC フレームをブリッジ接続によって物理的な LAN 上での電気信号に変えることもできる。

・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 にかかなりの確率で接続することができる。

・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ない、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。

・SoftEther パケット

SoftEther プロトコルを含む TCP/IP パケット。このパケットは SoftEther 仮想 LAN ではなく、実際の (物理的な) ネットワーク上を流れ、仮想 LAN カードと仮想 HUB の間で送受信される。SoftEther パケットには、仮想 LAN カードと仮想 HUB の間で構築される仮想 LAN を流れる仮想 MAC フレームを暗号化、電子署名してカプセル化されたものが入っている。

・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。ユーザーが後から自由に変更することも可能である。

・利用できるプロトコル

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。

4: ソフトイーサによるネットワーク

・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なくなる。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ため、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ため、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ため、WindowsXP/WindowsServer2003 以降で使用可能である。(Windows2000 はブリッジになることはではない。)

・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ため、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。

・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 との間を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。

・ブリッジ接続の危険性

ブリッジ接続によって、構築した仮想 LAN に複数台のコンピュータを接続させたい場合でも、それぞれのコンピュータに SoftEther 仮想 LAN カードをインストー

ルする必要は無く、1 台のコンピュータでブリッジ接続を構成するのみで物理的な LAN 上のコンピュータすべてが仮想 LAN と自動的に通信可能になるので、大変便利である。また、コンピュータのユーザーが物理的な LAN のネットワーク管理者の設定無しに自由にこのようなブリッジ接続が行えるため、管理者の手を煩わせる必要が無いのだが、これはネットワーク管理者から見れば脅威となる。ネットワークのブリッジ (カスケード接続) は従来でも一般ユーザーが勝手に行うことができたが、それは物理的なカスケード接続であり、何らかの物理的なケーブルが必要となっていたので、ネットワーク管理者はそんなことが行われていないかどうかを容易にチェックできた。しかしながら、SoftEther 仮想 LAN はハードウェア的には全く何も必要無いので、仮想 LAN と物理的な LAN とのブリッジ接続をしても、ネットワーク管理者がそれを発見・チェックする可能性は低く、ユーザーの利用方法によっては物理的な LAN が外部と直接ケーブルで接続されたようになってしまうので、セキュリティ的に危険な状態となる。しかしながら、これを防止する容易な方法は存在しない。

・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。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、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。

・PC to PC 接続

SoftEther の利用形態の 1 つ。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 を稼働させ、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。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。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。

・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。

・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。

- ・ 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。

- ・ 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。

参考文献

- ・ SoftEther 活用ガイド

登 大遊 著 ASCII

- ・ 魔法のトンネル SoftEther

ランティス 著 秀和システム

- ・ TCP/IP ネットワーク実験プログラミング

村上 公保 著 オーム社

- ・ TCP/IP アナライザ作成とパケット解析

小高 知宏 著 オーム社

- ・ マスタリング TCP/IP

竹下 隆史 著 オーム社

