「SoftEther」の可能性
ーリモートメンテナンスの手段となりうるのかー

2004/5/14

Science House Inc.
Tomizawa

サイエンスハウス
富澤

話の初めから恐縮ですが・・・

サイエンスハウスにサーバを構築する必要のあるシステム開発をご依頼して頂く際には、サーバマシンはネットワーク管理者が監視しているデータセンターを極力ご利用頂きますようお願いいたします。
その理由は、この後の話の中からご理解頂けると切に願っています・・・

それでは、よろしくお願いいたします。

なぜ「SoftEther」に目を付けたか・・・

・・・それはサーバをリモートメンテナンス(例えば自宅から)する環境を容易に構築出来そうだったからです。

(お金の掛かる環境は、はなから却下されるわけですが・・・)

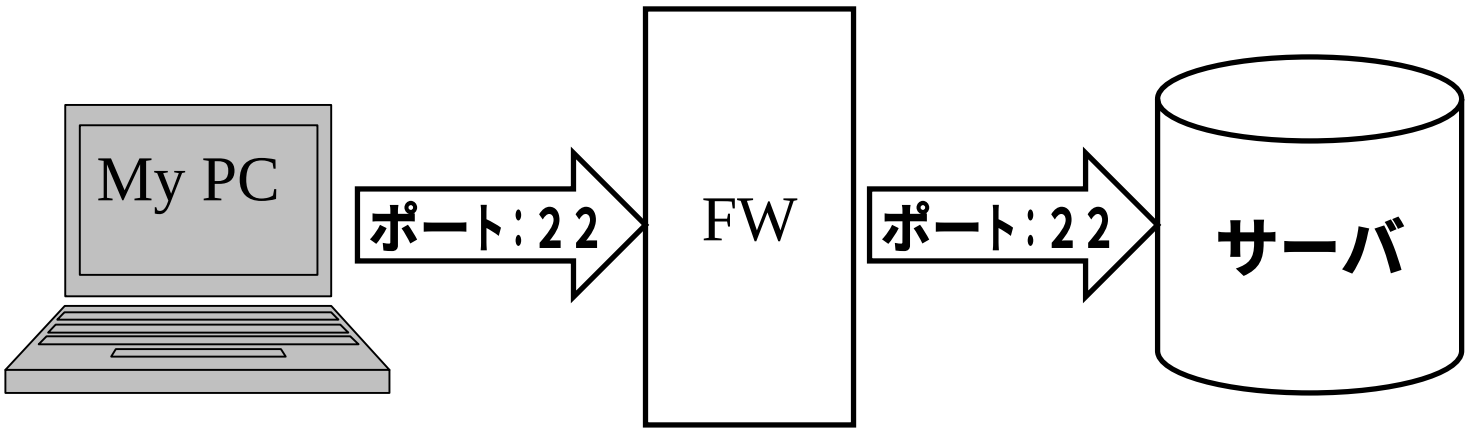
このような結論に達したその経緯を順を追って説明させていただき、更に「SoftEther」で実際にテスト環境を構築し、その可能性を探ってみようと思います。

Webサーバの例

ここでは実際に稼動しているLinuxサーバを例に挙げてメンテナンス作業を説明いたします、細かい設定については近年騒がれているソーシャルセキュリティーホールになるので省かせて頂きます、またIISも却下です。(理由は攻撃者が多いので、と言うのもあるのですが、実際はお金が・・・)

簡単なホームページを公開しているサーバでの作業について説明いたします。

サーバのリモートメンテナンスは全てSSHで行っています。



通常SSHなら通信は暗号化され、更に認証もしてますから安全と考えられています。

(「暗号が破られればお終いじゃないか」、と言う話は省きます、別の方お願いいたします)。

また、Linuxは暗号化通信機能をOpenSSLに依存しているため、最近発見された、DOS攻撃 (サービス妨害)を招く脆弱性が2つあり、

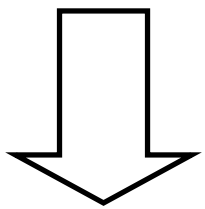
1つ目はdo_change_cipher_spec()関数のnull-pointer assignment
2つ目はKerberos暗号セット利用時

2つともあまり関係ない‥でも怖いからバージョンアップしておかなければ‥‥

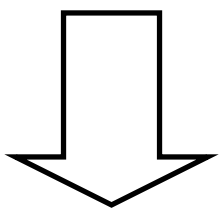
つまり、

①SSHでしかアクセスできない。
(ポートは22)

②固定IPでないとアクセスできない。
(認証だけに頼るのはもちろん危険、特定のIPにしかアクセス権限を与えていない。)



それなら、専用回線を設けよう・・・高い無理だ・・・



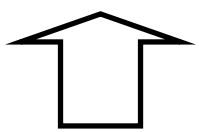
それなら、固定IPを買おう・・・・・・まだ高い無理だ・・・

そこで、VPNの登場！

VPN とは・・・

VPN (Virtual Private Network、仮想プライベートネットワーク) は、インターネットなどを暗号化通信によりプライベートな専用ネットワークのように利用する方法です。インターネット上の 2 つの地点を接続し、そのセッション上で仮想的なネットワーク (LAN) を構成することにより、離れた場所にあるコンピュータ同士やネットワーク同士を安全かつ自由に接続することができます。 また、一般的な VPN は PPP (1 対 1 の接続プロトコル) を拡張して実装されています。

しかし、従来のVPNはネットワーク管理者に協力を得ないと実現できないものがほとんどでした。
（FWに穴を開けるなどの特別な設定が必要だったり、VPN対応の高価な機器を揃えたりする必要があった。）



開発者がネットワークの管理まで手を出すと大変だ。

そして、「SoftEther」が登場するわけです。

なぜなら、宣伝文句が

SoftEther によるメリット

SoftEther を使うと、社内 LAN などでファイアウォールの設定変更などの危険な設定を行うことなく、簡単かつ安全な VPN セッションを遠隔地のネットワークとの間で張ることが可能です。

と、あったからです。

つまりネットワークの設定は触らずにリモートアクセスが可能なのです。

ん？待てよ・・・

ファイアーウォールの設定なし？！

つまりFWを透過するって事？！

疑問です(危ないです)、早速調査しましょう。

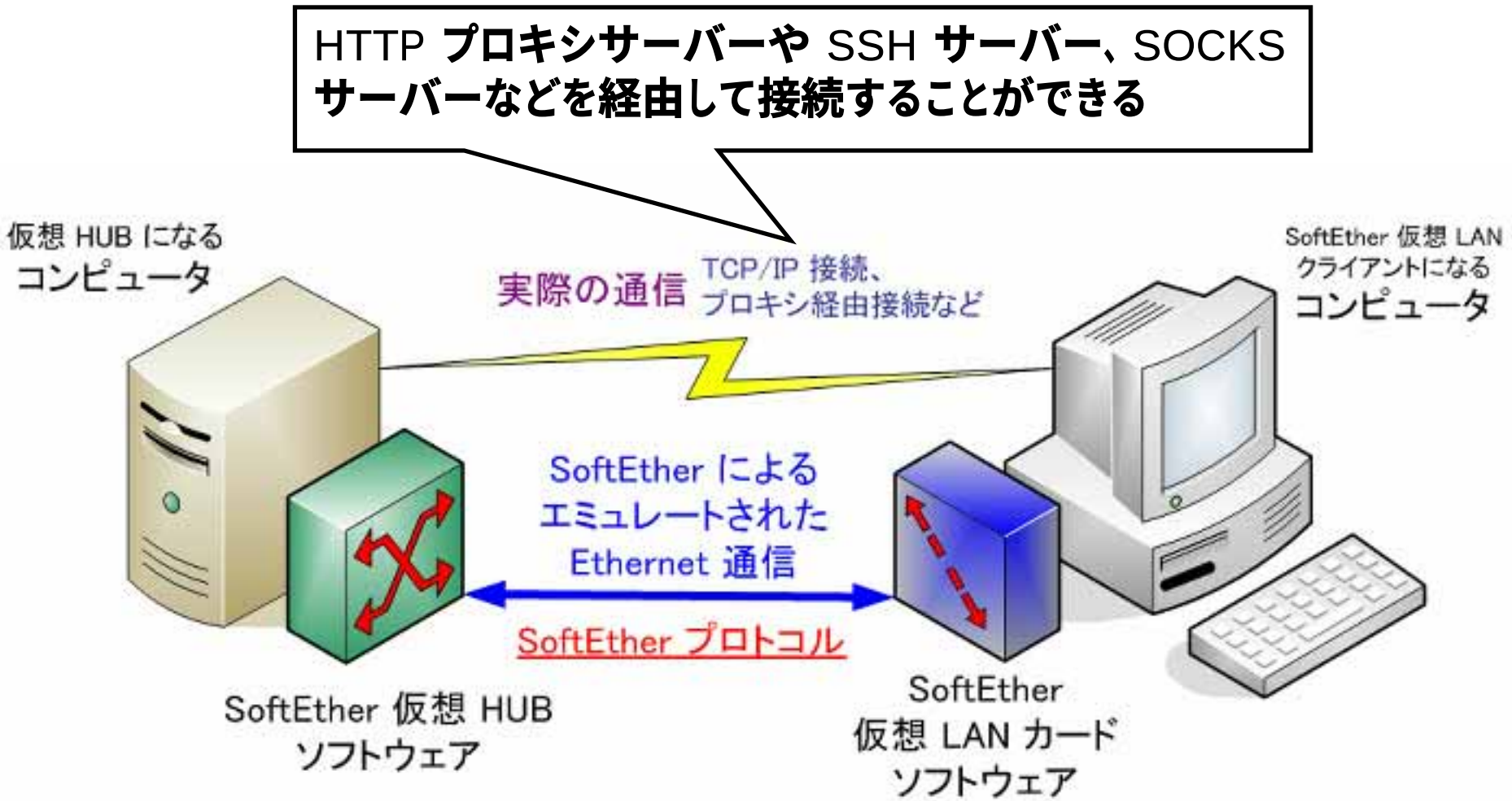
「SoftEther」とは・・

特徴：簡単にまとめると、
「SoftEther」もVPN を構築することができるソフトウェアやプロトコルの中の 1 つですが、スイッチング HUB と LAN カードをエミュレーションすることによって仮想ネットワークを実装する。

出所：情報処理振興事業協会 (IPA) の未踏ソフトウェア創造事業
未踏ユース部門による支援を受けて開発されました。

経歴：公開後1週間で「SoftEther は使い方によってはセキュリティ ホールの原因となるソフトウェアである。」という理由から配布が中止され、独自の暗号化方式を使用していたものを長く使われ信頼のあるSSLに変更して配布再開しています。さらに現在は先ほどのOpenSSLのセキュリティーホールに対応しver1.0として無料で公開されています。
全てWindows用なのですが、現在Linux用の仮想HUBが開発されテスト段階です。

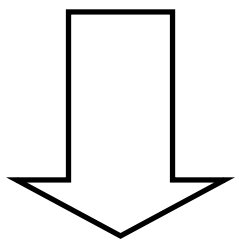
詳しくはこちらです→http://www.softether.com/jp/



例えば、普通のWeb閲覧などでもよく使われるHTTPSというプロトコル(セキュアなWebページデータの転送手段)上で仮想のプライベートネットワークが構築できてしまう。

なるほどこれならFWを透過することができます、更にProxy、NATなど他のどんな制限も受けません、なぜなら仮想スイッチングHUBを制限(例えば社内のFW)の外に置いてしまえばいいのですから。

そうすることによりファイアウォール外からのアクセスを許可されていない人でも、ファイアウォールを越えてどんな通信でもできるようにしてしまえるのです。



本当にネットワークの設定をせずに開発者でも簡単にリモートアクセスの環境が作れてしまうのです。

・・・・早速テストしてみましょう。

テスト内容:

(1)**社外(社内**FW**の外)に仮想スイッチング**HUB**を構築する。**

(2) (**壊れても良い)マシンが足りないので仮想スイッチング**HUB**と同じマシンに仮想**LAN**カードも設置する。**

(3)**社内**LAN**内(**FW**の内側)のマシンに仮想**LAN**カードを設置する。**

(4)(**怖いので**)Norton Internet Security**を有効にする。**

(5)**接続する。**

(6)**ファイルを共有してみる。**

(7)**接続を切る。**

注意:**試す方はオンラインマニュアルを熟読して下さい。(ネットワークの知識の無い良い大人は真似しないで下さい。)**

(1)社外(社内FWの外)に仮想スイッチングHUBを構築する。

通常のインターネット回線を開きます、(ここにはFWはありません)
SHの固定IP中の×.×.×.188を割り振りました。

(2) 仮想スイッチングHUBと同じマシンに仮想LANカードも設置する。

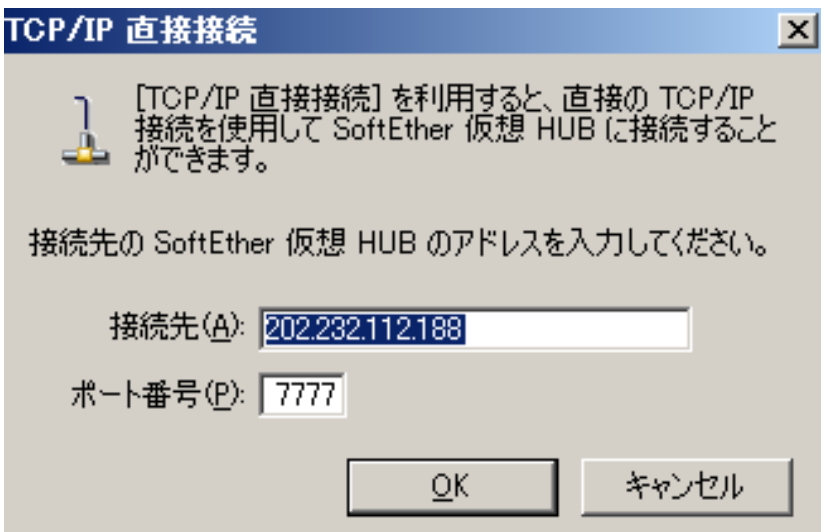
仮想LANを仮想HUBに接続します、仮想LANから×.×.×.188に接続するだけです。(仮想LAN側からHUBにユーザを作る為です。)

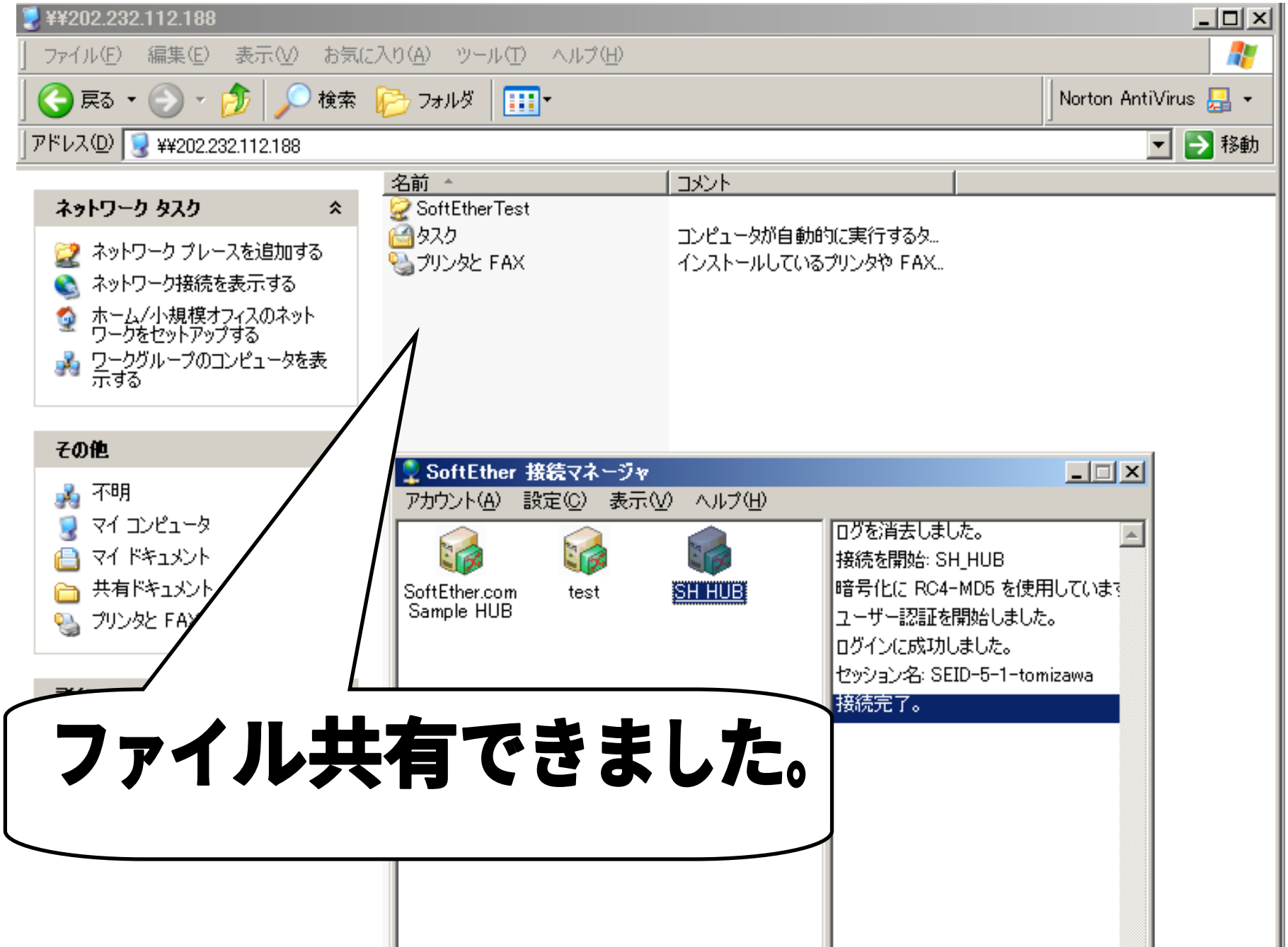
(3)社内LAN内(FWの内側)のマシンに仮想LANカードを設置する。

同じく通常のインターネット回線を開き、仮想LANを設置します。

(5)接続する。

社内の仮想LANからIP×.×.×.188(ポート7777)に接続するだけです。




¥¥202.232.112.188
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 フォルダ
Norton AntiVirus
アドレス(D) ¥¥202.232.112.188
移動
ネットワーク タスク
ネットワーク プレースを追加する
ネットワーク接続を表示する
ホーム/小規模オフィスのネットワークをセットアップする
ワークグループのコンピュータを表示する
その他
不明
マイ コンピュータ
マイ ドキュメント
共有ドキュメント
プリンタと FAX
名前
コメント
SoftEtherTest
タスク
コンピュータが自動的に実行するタ...
プリンタと FAX
インストールしているプリンタや FAX...
SoftEther 接続マネージャ
アカウント(A) 設定(C) 表示(V) ヘルプ(H)
SoftEther.com Sample HUB
test
SH_HUB
ログを消去しました。
接続を開始: SH_HUB
暗号化に RC4-MD5 を使用しています
ユーザー認証を開始しました。
ログインに成功しました。
セッション名: SEID-5-1-tomizawa
接続完了。
ファイル共有できました。

接続テストの際にSoftEther.comが実験用に用意しているスイッチングHUBに接続してみたのですが、大変でした。

アタックを受ける事、数回・・・。

ワームW32.Spybot.Wormに感染する事1回・・・。

Norton Internet Securityでアタックは検出できたのですが、攻撃者の通信の内容も暗号化されているため非常に危険です。

結果的に恐ろしいほど簡単にリモートアクセスの環境を手にすることが出来ました。

ただ、従来安全とされていた通信の中で暗号化された通信を行うわけですからネットワーク管理者はこれからは例えばhttpsの通信でさえ暗号化されたウィルスやワームに(これはウィルス検知が出来ない事を意味します)気を配る必要があるわけです。

将来的にはこの技術を利用し社内LANに常設するハッキングもありえます。

用途の理解とネットワークの十分な知識をもって進んでいきましょう。