OpenSSH

IBM i での Web 環境でセキュアなリモート接続環境を提供する SSH の構築方法の説明です。

関連 URL

・「IBM Portable Utilities for i5/OS」:http://www-03.ibm.com/servers/enable/site/porting/tools/openssh.html

・「Open SSH 公式サイト・日本語」→ http://www.openssh.com/ja/index.html

・「Open SSH 日本語マニュアル」→ http://www.unixuser.org/~euske/doc/openssh/jman/

・「sshd_config の設定」→ http://www14.plala.or.jp/campus-note/vine_linux/server_ssh/sshd_config.html

・「TeraTerm リリースの公式リポジトリ」→ http://sourceforge.jp/projects/ttssh2/releases/

背景と機能概要

IBM i を通常操作するには 5250 が一般的である。昨今のインターネット環境で 5250 を使う場合 VPN 等コストがかかってしまう。今回紹介するのは OpenSSH (Open Secure Shell)と言うセキュアな環境を提供してくれる OSS だ。通信経路の暗号化や認証を強化することで、リモートホストとの通信をより安全にする OSS だ。このソフトウェアは IBM i に導入されており、環境設定のみの操作になる。また公開鍵、秘密鍵と言ったデータの安全を守る勉強にもなると思われる。この OpenSSH の活用場面として

・VPN は使えないが、インターネット環境から遠隔地にある、IBM i をリモート操作したい。

・VPN のコスト的な問題を解決したい。

・別途サーバーや機器を設置するのでは無く、IBM i の 1Box で行いたい。

・Telnet や FTP でもセキュアな通信を使いたい。

・遠隔地で 5250 エミューレタを使いたい. . . などなど。

OpenSSH の特徴

(１)強力な暗号化機能 (3DES, Blowfish, AES, Arcfour)

(２)ポート転送 (従来プロトコルの通信を暗号化)

(３)強力な認証 (公開鍵、One-Time パスワード と Kerberos 認証)

(４)SFTP クライアントおよびサーバのサポート (SSH1 および SSH2 プロトコル)

(５)データ圧縮

OpenSSH の導入方法

V6R1 以上については、「STRTCPSVR SERVER(*SSHD)」コマンドが用意されており、それを実行するだけだ。
実行するだけで、SSH デーモンとホストキーを自動生成してくれる。SSH 終了時も、「ENDTCPSVR SERVER(*SSHD)」コマンドを実行するだけで簡単だ。したがって、IBM i の"QSTRUP"などのスタートアッププログラムで、「STRTCPSVR SERVER(*SSHD)」を追加するだけで、SSH サーバーの出来上がりとなる。
但し、このコマンドは、V5R4 と V5R3 では提供されていないので、次に V5R4 と V5R3 の場合について説明する。
この資料は V6R1 以上でも参考になる。

（1）5250 エミュレータで IBM i にサインオンする。（コード・ページを”939”にして、英小文字を使える環境にする）

（2）「CHGJOB CCSID(5035)」をコマンドラインで実行して、ジョブの CCSID＝5035 に変更する。

（3）「call qp2term」をコマンドラインで実行して、PASE シェルを呼び出す。

（4）「ssh-keygen -t rsa1 -f /QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-3.5p1/etc/ssh_host_key -N ""」をシェルで実行して、 SSH1 の RSA のキーを生成する。

（5）「ssh-keygen -t rsa -f /QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-3.5p1/etc/ssh_host_rsa_key -N ""」をシェルで実行して、SSH2 の RSA のキーを生成する。

（6）「ssh-keygen -t dsa -f /QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-3.5p1/etc/ssh_host_dsa_key -N ""」をシェルで実行して、SSH2 の DSA のキーを生成する。

（7）SSH デーモンの起動

SSH デーモンとは、SSH サーバーを常駐させておく、UNIX プログラムだ。SSH デーモンを起動する為には、PASE シェルより「sshd」コマンド実行する。（「sshd」コマンドを使うには、”/QOpenSys/usr/sbin”に、PATH が通っている必要がある、PATH が通っていない場合はフルパスで指定する。）これで、SSH サーバーは起動した状態になる。

SSH サーバーを終了させるには、PASE シェルを使って「ps ax」を実行して、SSH デーモンのプロセスIDを確認し、その後「kill プロセスID」で終了させる。

（８）公開鍵認証の設定

①sshd_config の設定（今回は公開鍵認証を行う）

②「/QOpenSys/QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-3.5p1/etc/sshd_config」ファイルを編集する。

---------- 省　略 ----------

 # root でのログインの許可

PermitRootLogin no

 # RSA 認証が成功した時、rhosts を使った認証を許可。

RhostsRSAAuthentication no

 # パスワード認証を許可

PasswordAuthentication no

 # 空のパスワードを許可

PermitEmptyPasswords no

 # 特定ユーザのみ接続許可をする

AllowUsers（ユーザ名１）（ユーザ名２）・・・・

---------- 省　略 ----------

③設定を変更した後は、SSH デーモンの再起動を行う。

（９）公開鍵・秘密鍵の作成

公開鍵認証では、ペアーとなる公開鍵・秘密鍵を作成する必要があるので、以下の通り行う。

（※注意 ：SSH に接続するユーザー名は８文字以内にする必要がある）

①SSH 接続ユーザーのホームディレクトリ（/home/（ユーザー名）/.ssh）を作成。

> mkdir /home/（ユーザ名）

> cd /home/（ユーザ名）

> mkdir .ssh

> cd .ssh

②「ssh-keygen」コマンドを実行して、公開鍵と秘密鍵を生成し、公開鍵の登録を行う

> ssh-keygen -t rsa

Enter file in which to save the key (/home/(ユーザ名)/.ssh/id_rsa):

> (実行キー)

Enter passphrase (empty for no passphrase):

> (秘密鍵のパスフレーズ入力)

Enter same passphrase again:

> (確認のため、再度同じパスフレーズを入力)

自身の公開鍵が /home/(ユーザ名)/.ssh/id_rsa.pub に保管されました。

> cat id_rsa.pub >> authorized_keys

ここで作成された、"id_rsa.pub"が公開鍵で、"id_rsa"が秘密鍵になる。"id_rsa"は必ず、クライアント側で厳重に保管する必要がある。間違っても、サーバーに置いたままにしない事だ。それこそ、玄関の横に家の鍵をぶら下げてあるようなものだ。

(10)パーミッション・所有権の設定

SSH の公開鍵認証では、ディレクトリや公開鍵ファイルに正しいパーミッションと、SSH に接続するユーザーに所有権を与えておく必要がある。

chmod 755 /home/(ユーザ名)

chmod 700 /home/(ユーザ名)/.ssh

chmod 644 /home/(ユーザ名)/.ssh/authorized_keys

chown (ユーザ名) /home/(ユーザ名)

chown (ユーザ名) /home/(ユーザ名)/.ssh

chown (ユーザ名) /home/(ユーザ名)/.ssh/authorized_keys

以上で IBM i の設定は終了だ。

(11)ルーター等の設定編|

外からの SSH ポート(省略は 22 番ポート)が、IBM i の SSH ポートへ転送が可能になっている必要がある。これらの設定については、それぞれのメーカー、機種等により、異なるので割愛する。

OpenSSH での接続方法

今回は Windows を前提に、TeraTerm(執筆時はバージョン 4.63)でのクライアント設定を説明する。

まず、TeraTerm のリリースリポジトリ(http://sourceforge.jp/projects/ttssh2/releases/)から、ダウンロード&インストールをする。インストールが完了したら、TeraTerm を起動する。クライアントとして、使う為には、幾つかの設定と手順があるので、以下に挙げておく。

①メニューの[漢字コード]を選択し、送受信とも"Shift_JIS"とする。

②メニューの[設定]→[SSH 認証]を選択し「ssh の接続ユーザー」と、「秘密鍵」を設定する。

③メニューの[設定]→[設定の保存]を選択し、設定を保存する

(次回から設定読込で使う事ができる)

④メニューの[ファイル]→ [新しい接続]を選択し、

”ホスト”に IBM i のグローバルなアドレスを設定する。

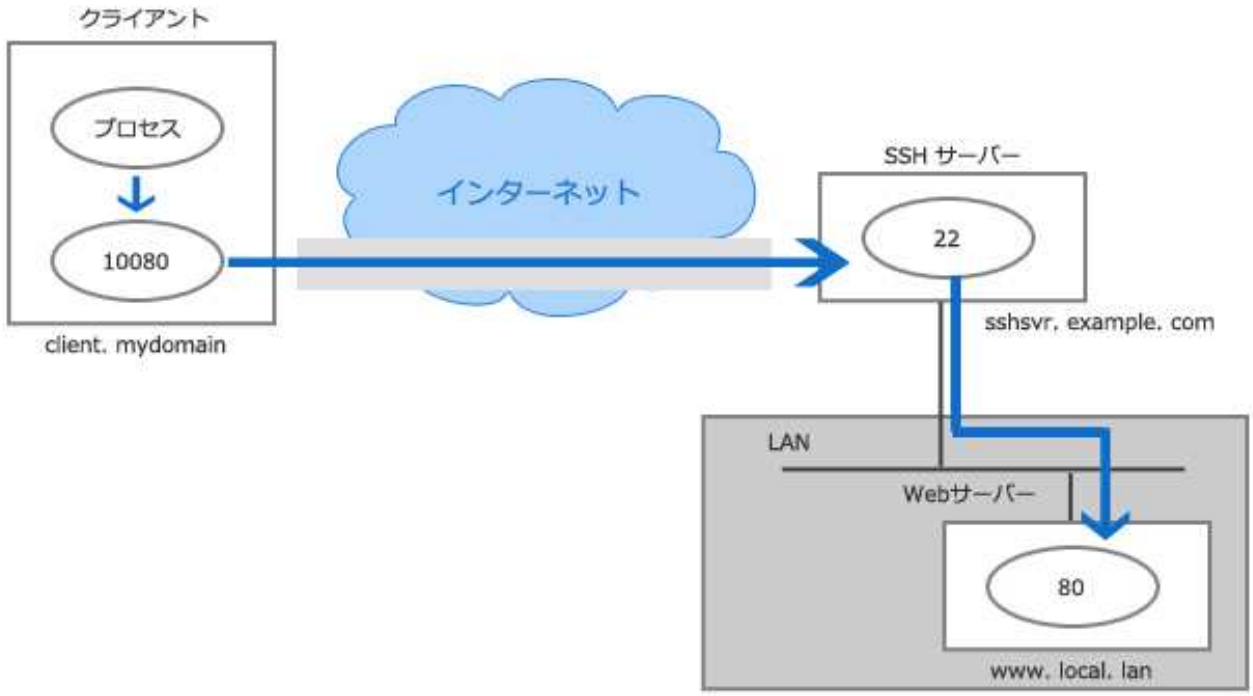
”SSH バージョン”に SSH2 を設定する。

⑤SSH 認証画面が表示されたら、パスフレーズに秘密鍵を作成した時のパスフレーズを入力する。

OKボタンを押せば、SSH サーバーへ繋がるはずだ。

前述の SSH セッションを維持したまま、今度はポートフォワード機能を使い、5250 エミュレータを操作してみる。

このポートフォワード機能とは、自分の任意のローカルポート介して、SSH サバー越しに、別のサーバーの任意のポートに通信可能な機能だ。



5250 エミュレータは Telnet 接続なので、遠隔地の IBM i の 23 番ポートを、localhost の適当なポートに割り当ててしまう事により、SSH 越しに接続する事が出来る。

最初に TeraTerm でのポートフォワードの設定を行う

①メニューの [設定] → [SSH 転送] を選択し、追加ボタンを押す。

”ローカルポート”に、クライアントの任意ポート、例えば 8881 を設定する。

”リモートホスト側”に、IBM i のアドレスと、”ポート”23 番ポートを設定する。

OKボタンを押せば、ポートフォーワードの設定完了だ。

続いて PCOM の設定だ。

①ホスト名のアドレスを「localhost」にする

②ポートを 8881 を設定する。(Teraterm と同じ値)

これでセキュアな環境でインターネットを介した通信が可能となる。

最後に

セキュアな環境はますます重要になってきている。コストをあまりかけることなく新しい技術を利用できるのが OSS だ。IBM i の資産を継承しつつ、新しい技術を活用できる OSS の価値は高いはずだ。

以上