RaQでSSHを使おう

株)アライブネット
RS事業部 企画開発G 小田 誠

SSHでできること

- 通信の暗号化ができる
  - パスワードを暗号化してサーバに送る
  - 通信が確立した後も暗号化される
- IPスプーフィング（偽装）を防止できる
  - なりすましができない
- ポートフォワーディングができる
  - TCP/IPを使った簡易VPNとして使える
- 暗号化してファイル転送ができる
- UNIXパスワード以外の認証方法を使える

RaQへのインストール

- **パッケージの入手元**
  - http://www.cobaltresq.com/rpms/openssh-3.0-uC1.i386.rpm
  - http://www.cobaltresq.com/pkg/RaQ3-Unofficial-20020902.pkg
  - **Cobaltパッケージなら、管理画面からインストールします**
  - **RPMならばsshログイン後に rpmコマンドを使います**

PCへのインストール(Windows)

- TeraTerm+TTSSHを入手
  - プロトコル1のみ
  - http://www.vector.co.jp/authors/VA002416/
  - →TeraTerm Version2.3
  - http://www.zip.com/au/~roca/
  - →TTSSH exstention
  - **他にもwww.forest.impress.co.jpでもミラーされている**
- Lhasaなどで解凍する
- TeraTermのSetup.exeを実行
- インストールしたTeraTermのディレクトリにTTSSHのすべてのファイルをコピーする

PCへのインストール（Mac）

- **OS8.x,9.xならMacSSHを使う**
  - **プロトコル2のみの対応**
  - http://www.macssh.com/
  - **解凍してApplicationsフォルダにおく**
  - **エイリアスを作成**
- **OSXならTerminalを開くだけですぐに使えます**
  - **プロトコル2,1ともに使えます**
  - **OpenSSHがすぐに使えます**
  - **MacSSHを使うにはクラシック環境をインストールしておく**

サーバへの接続

- **接続したいホスト名とユーザ名パスワードが必要**
  - **接続の例**

```
$ ssh –l oda rose.alivenet.co.jp
Password:
rose% uname –a
rose% exit
```

簡易VPNとして使う

- TTSSHだけでもできるが専用ソフトもある
  - PortForwarder
    →http://www.fuji-climb.org/pf/
  - 解凍してProgram Filesなどのフォルダに置く
  - 必要に応じてショートカットを作成
  - config.iniを編集 もしくは新規作成

```
Host rose
  HostName rose.alivenet.co.jp
  User oda
  LocalForward  25 localhost:25
  LocalForward  110 localhost:110
```

- 管理画面の暗号化、モバイルでのSMTP利用ができる

FTPの代わりに使う

- WinSCPを利用する
  - http://winscp.vse.cz/eng/
- 解凍する
- Program Filesなどのフォルダにコピーを置く
- 必要に応じてショートカットの作成

さらに進んだステップ

- UNIXパスワード認証ではなくてRSAkey認証を使う
  - PF-SSHKeygenを使って鍵を作る
  - パスフレーズを入力する
  - identity(秘密鍵)とidentity.pub(公開鍵)が作成される
  - identity.pubをログインしたいサーバに何らかの方法で~.ssh/authorized_keysファイルに追加する
  - クライアントでidentityを利用するようにしてログインする
- ネットワークにパスワードが流れません
- 複数のサーバで同じパスフレーズが使えます
- 秘密鍵、公開鍵、パスフレーズの3つがないとダメ

まとめ

- SSHも万能ではない
  - セキュリティホールが見つかることがある
  - サイトが改竄されていたことがある
  - 過信せずなんらかの方法でアクセス制限すべきである