

SSHポート転送機能

2001年10月30日

稲田 稔

SSHの暗号化機能

- SSHによりloginするときの通信を暗号化できた
- その他の通信を暗号化することはできないか？

 SSHのポート転送機能を利用すれば可能

SSHのポート転送機能

- 暗号化機能のないネットワークサービスの通信路を暗号化することが可能
- SSHクライアントとSSHサーバの間に暗号化通信路を作成し、ネットワークサービスがそれを利用して通信する
 - ネットワークサービスアプリケーション自体に変更を加えずに暗号化通信ができる
- 暗号化通信路の作成方法には2種類ある
 - ローカルポート転送
 - リモートポート転送

ローカルポート転送

- SSHクライアントとサーバ間のSSH暗号通信路を利用して、SSHサーバの先にあるホストに接続する機能
- クライアント側でsshコマンドを実行するときに“-L”オプションを指定する

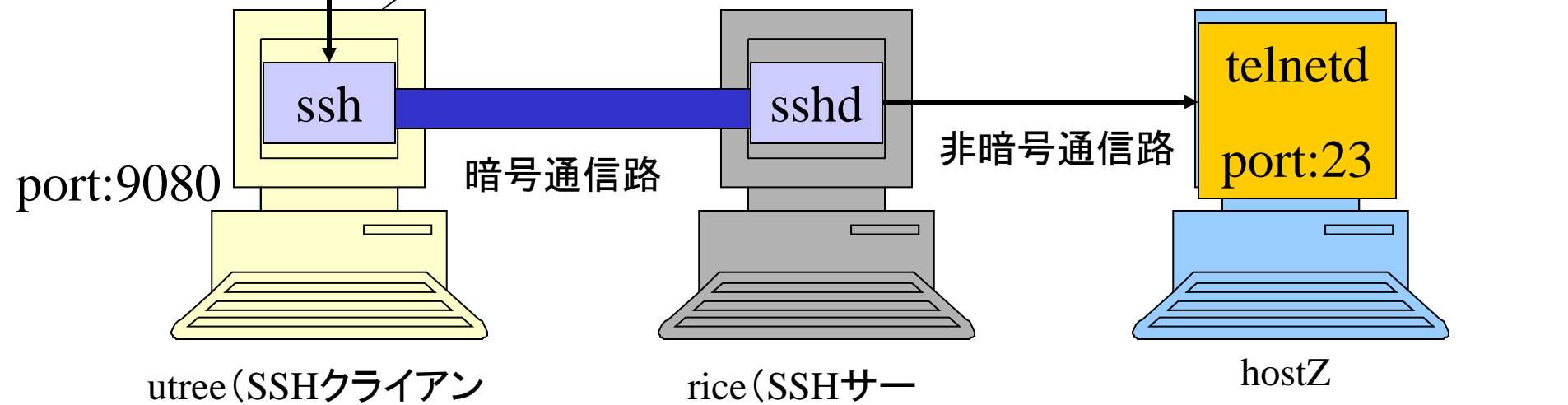
```
% ssh -L ローカルポート番号:リモートホスト名:リモートポート番号:SSHサーバホスト名
```

- ローカルポート番号 : SSHクライアント側の待ちポート番号
- リモートホスト名 : SSHサーバが転送するホスト名またはIPアドレス
- リモートポート番号 : 転送先ホストのポート番号
- SSHサーバホスト名 : SSHサーバのホスト名またはIPアドレス

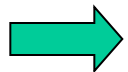
ローカルポート転送の例

```
% telnet utree 9080
```

```
utree% ssh -L 9080:hostZ:23 rice
```



utreeとriceの間にSSH暗号通信路を作り、
utreeのポート番号9080に来た通信をSSH通信路を通してhostZのポート23に転送(接続)する



実際に通信するのはutree(ローカル)のポート番号9080に接続したホストとhostZのtelnetd

リモートポート転送

- SSHクライアントとサーバ間のSSH暗号通信路を利用して、SSHクライアント側にあるホストに接続する機能
- クライアント側でsshコマンドを実行するときに“-R”オプションを指定する

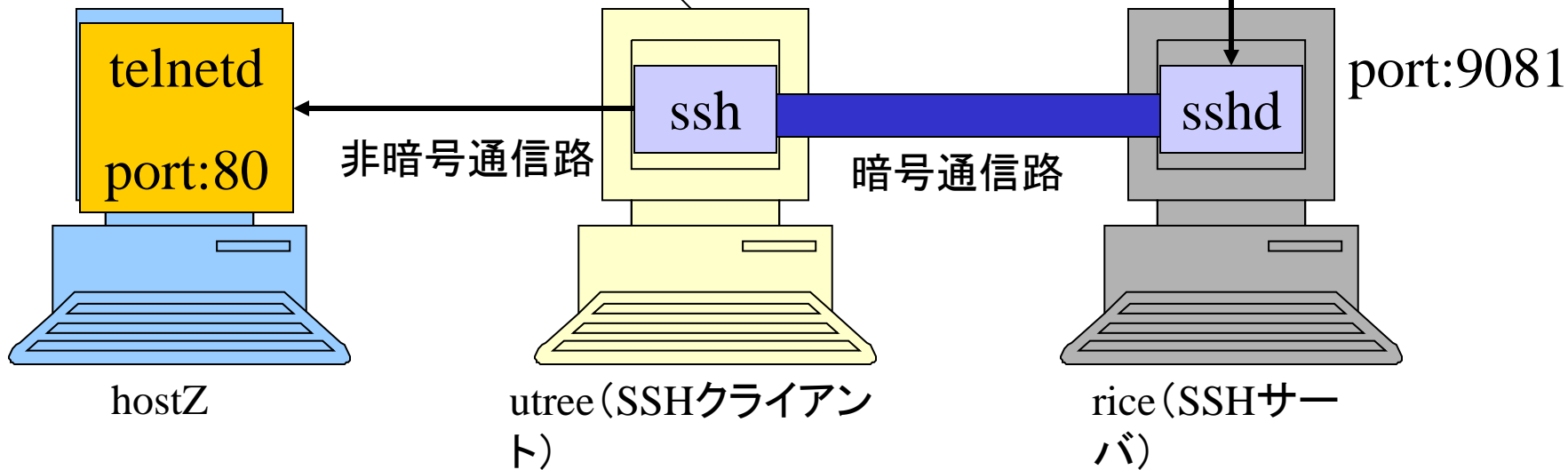
```
%ssh -R リモートポート番号:ローカルホスト名:ローカルポート番号:SSHサーバホスト名
```

- リモートポート番号 : SSHサーバ側の待ちポート番号
- ローカルホスト名 : SSHクライアントが転送するホスト名またはIPアドレス
- ローカルポート番号 : 転送先ホストのポート番号
- SSHサーバホスト名 : SSHサーバのホスト名またはIPアドレス

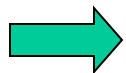
リモートポート転送の例

```
utree% ssh -R 9081:hostZ:80 rice
```

```
% telnet rice 9081
```



utreeとriceの間にSSH暗号通信路を作り、
riceのポート番号9080にきた通信をSSH通信路を通してhostZのポート23に転送(接続)する



実際に通信するのはrice(リモート)のポート番号9081に接続したホストとhostZのtelnetd

実験

- ローカルポート転送
 - 適当なホストとSSH接続を確立し、ローカルポート転送による通信を行う

```
%ssh -L ローカルポート番号:リモートホスト名:リモートポート番号:SSHサーバホスト名
```

- ローカルポート番号:SSHクライアント側の待ちポート番号
- リモートホスト名:SSHサーバが転送するホスト名またはIPアドレス
- リモートポート番号:転送先ホストのポート番号
- SSHサーバホスト名:SSHサーバのホスト名またはIPアドレス

実験例(1)

- %ssh -L 9080:hatsune:80 hatsume
- SSHサーバと接続を確立した状態

```
inata@maaya[~]%netstat -a | less
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4    0      0 localhost.9080          *.*                     LISTEN
tcp6    0      0 :::1.9080               *.*                     LISTEN
tcp4    0      0 maaya.1025             hatsune.db.is.ky.ssh   ESTABLISHED
tcp4    0      0 *.6000                 *.*                     LISTEN
tcp4    0      0 *.55556                *.*                     LISTEN
tcp4    0      0 *.5556                 *.*                     LISTEN
tcp4    0      0 *.ssh                  *.*                     LISTEN
tcp46   0      0 *.ssh                  *.*                     LISTEN
tcp4    0      0 *.printer              *.*                     LISTEN
tcp6    0      0 *.printer              *.*                     LISTEN
tcp6    0      0 *.ftp                  *.*                     LISTEN
tcp4    0      0 *.ftp                  *.*                     LISTEN
tcp4    0      0 *.1022                 *.*                     LISTEN
tcp4    0      0 *.1023                 *.*                     LISTEN
tcp4    0      0 *.sunrpc               *.*                     LISTEN
udp4    0      0 *.1042                 *.*                     LISTEN
udp4    0      0 maaya.1005             ayukawa.nfsd           *.*
udp4    0      0 *.55555                *.*                     LISTEN
udp4    0      0 *.rplay                *.*                     LISTEN
udp4    0      0 *.1014                 *.*                     LISTEN
udp4    0      0 maaya.1016            maaya.1023             *.*
```

9080番ポート
が接続待ち

SSHサーバとの
接続

実験例(2)

- 自ホストの9080番ポートにtelnetで接続

```
inata@maaya[~]%telnet localhost 9080
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /~inata/index.html HTTP/1.1
Host:hatsune

HTTP/1.1 404 Not Found
Date: Fri, 26 Oct 2001 08:48:09 GMT
Server: Apache/1.3.14 (Unix)
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

124
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>404 Not Found</TITLE>
</HEAD><BODY>
<H1>Not Found</H1>
The requested URL /~inata/index.html was not found on this server.<P>
<HR>
<ADDRESS>Apache/1.3.14 Server at www.db.is.kyushu-u.ac.jp Port 80</ADDRESS>
</BODY></HTML>
```

自分自身のポート9080にtelnetで接続

hatsuneのポート80(http)に接続されている

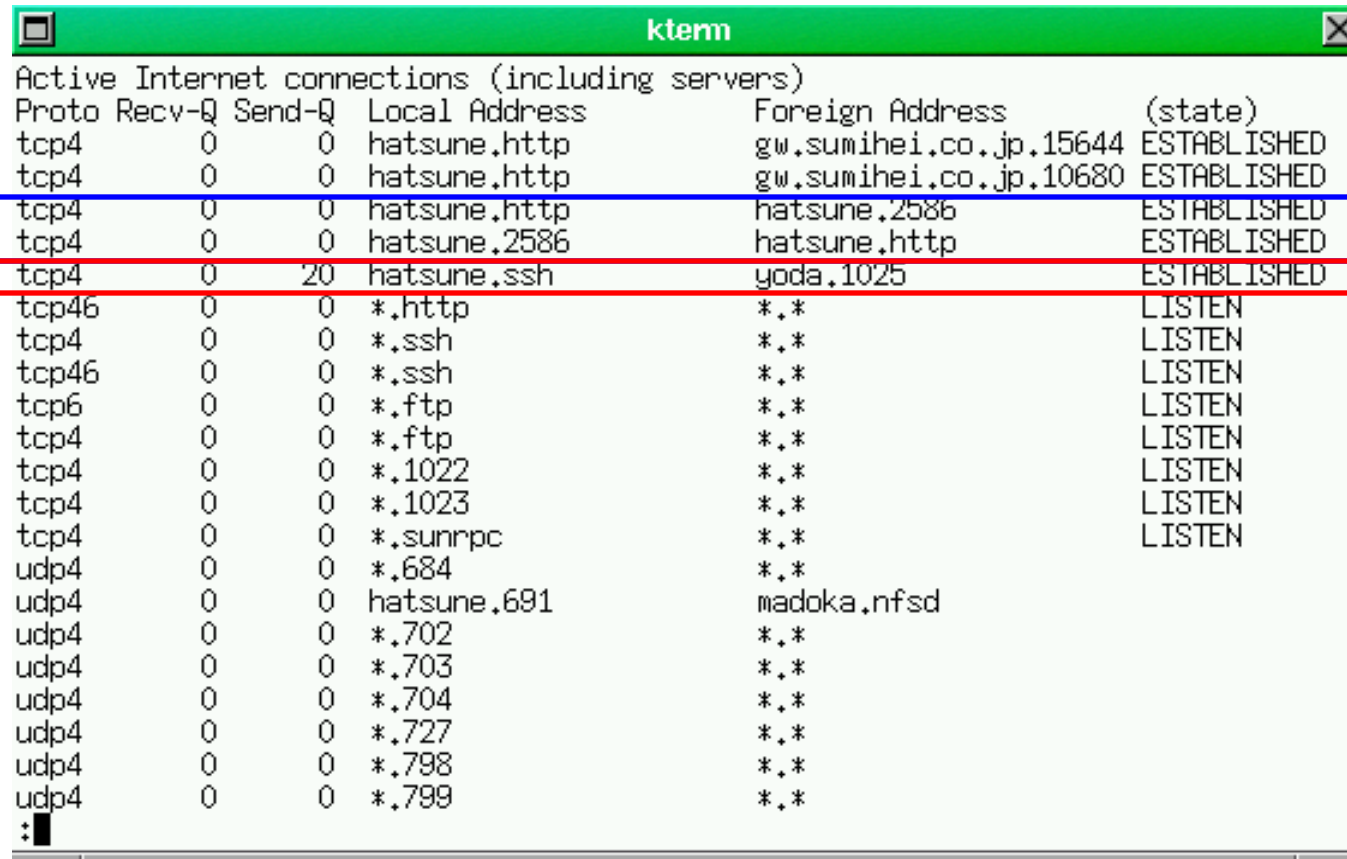
実験例(3)

- 自ホストの9080番ポートにtelnetで接続した状態

```
inata@maaya[~]%netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4    0      0 localhost.9080          localhost.1028          ESTABLISHED
tcp4    0      0 localhost.1028          localhost.9080          ESTABLISHED
tcp4    0      0 localhost.9080          *.*                     LISTEN
tcp6    0      0 :::1.9080               *.*                     LISTEN
tcp4    0      0 maaya.1025             hatsune.db.is.ky.ssh    ESTABLISHED
tcp4    0      0 *.6000                  *.*                     LISTEN
tcp4    0      0 *.55556                  *.*                     LISTEN
tcp4    0      0 *.55556                  *.*                     LISTEN
tcp4    0      0 *.ssh                    *.*                     LISTEN
tcp46   0      0 *.ssh                    *.*                     LISTEN
tcp4    0      0 *.printer                *.*                     LISTEN
tcp6    0      0 *.printer                *.*                     LISTEN
tcp6    0      0 *.ftp                     *.*                     LISTEN
tcp4    0      0 *.ftp                     *.*                     LISTEN
tcp4    0      0 *.1022                   *.*                     LISTEN
tcp4    0      0 *.1023                   *.*                     LISTEN
tcp4    0      0 *.sunrpc                  *.*                     LISTEN
udp4    0      0 *.1062                   *.*                     LISTEN
udp4    0      0 *.1042                   *.*                     LISTEN
udp4    0      0 maaya.1005              ayukawa.nfsd            LISTEN
udp4    0      0 *.55555                  *.*                     LISTEN
```

実験例(4)

- SSHサーバ側の状態



```
kterm
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4    0      0 hatsune.http           gw.sumihe.co.jp.15644  ESTABLISHED
tcp4    0      0 hatsune.http           gw.sumihe.co.jp.10680  ESTABLISHED
tcp4    0      0 hatsune.http           hatsune.2586           ESTABLISHED
tcp4    0      0 hatsune.2586           hatsune.http           ESTABLISHED
tcp4    0      20 hatsune.ssh            yoda.1025              ESTABLISHED
tcp46   0      0 *.http                 *.*                     LISTEN
tcp4    0      0 *.ssh                  *.*                     LISTEN
tcp46   0      0 *.ssh                  *.*                     LISTEN
tcp6    0      0 *.ftp                  *.*                     LISTEN
tcp4    0      0 *.ftp                  *.*                     LISTEN
tcp4    0      0 *.1022                 *.*                     LISTEN
tcp4    0      0 *.1023                 *.*                     LISTEN
tcp4    0      0 *.sunrpc               *.*                     LISTEN
udp4    0      0 *.684                  *.*                     LISTEN
udp4    0      0 hatsune.691            madoka.nfsd            LISTEN
udp4    0      0 *.702                  *.*                     LISTEN
udp4    0      0 *.703                  *.*                     LISTEN
udp4    0      0 *.704                  *.*                     LISTEN
udp4    0      0 *.727                  *.*                     LISTEN
udp4    0      0 *.798                  *.*                     LISTEN
udp4    0      0 *.799                  *.*                     LISTEN
:█
```

SSHクライアントとの接続