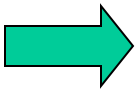
SSHポート転送機能

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

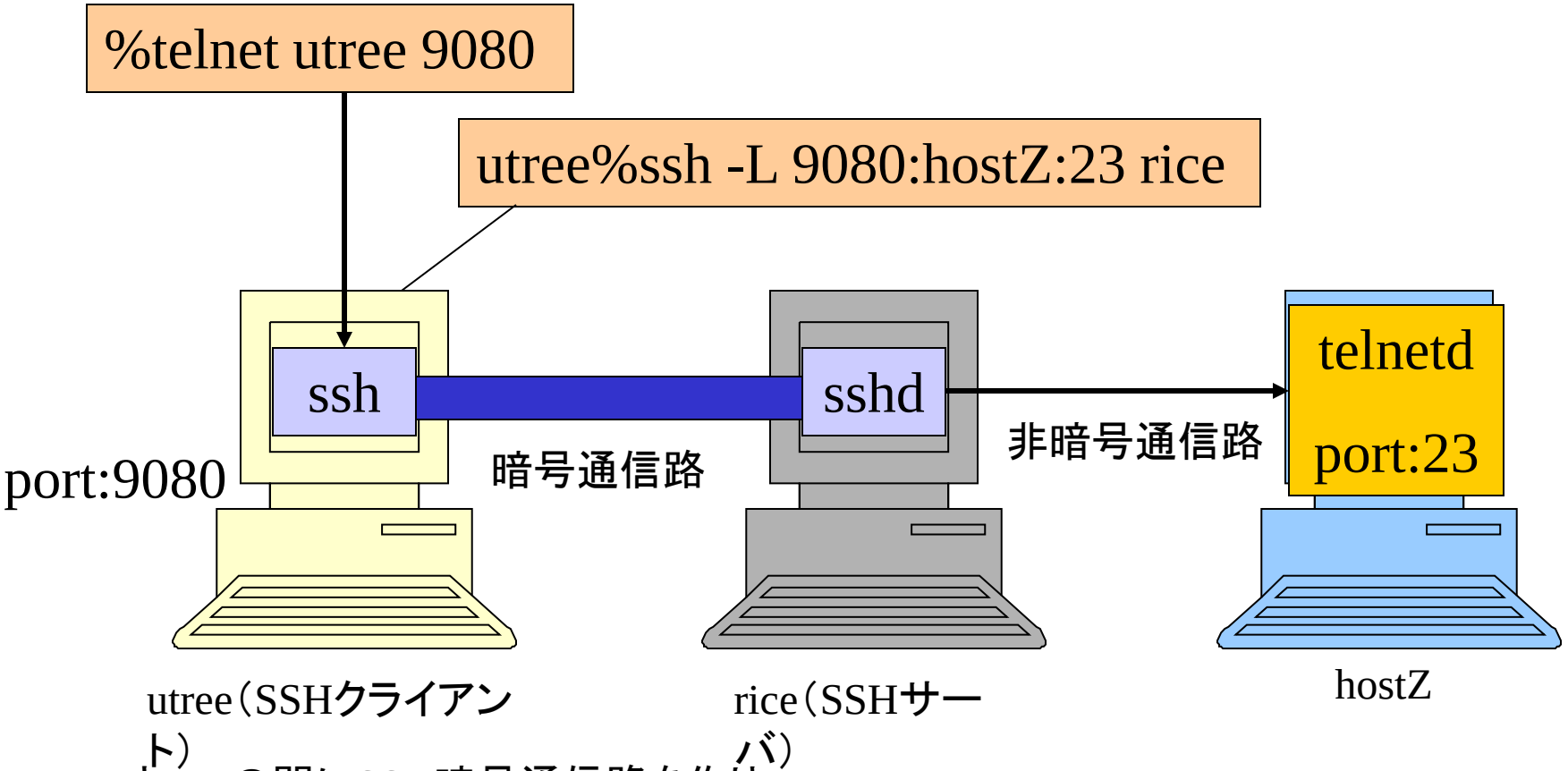
ローカルポート転送

- 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



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

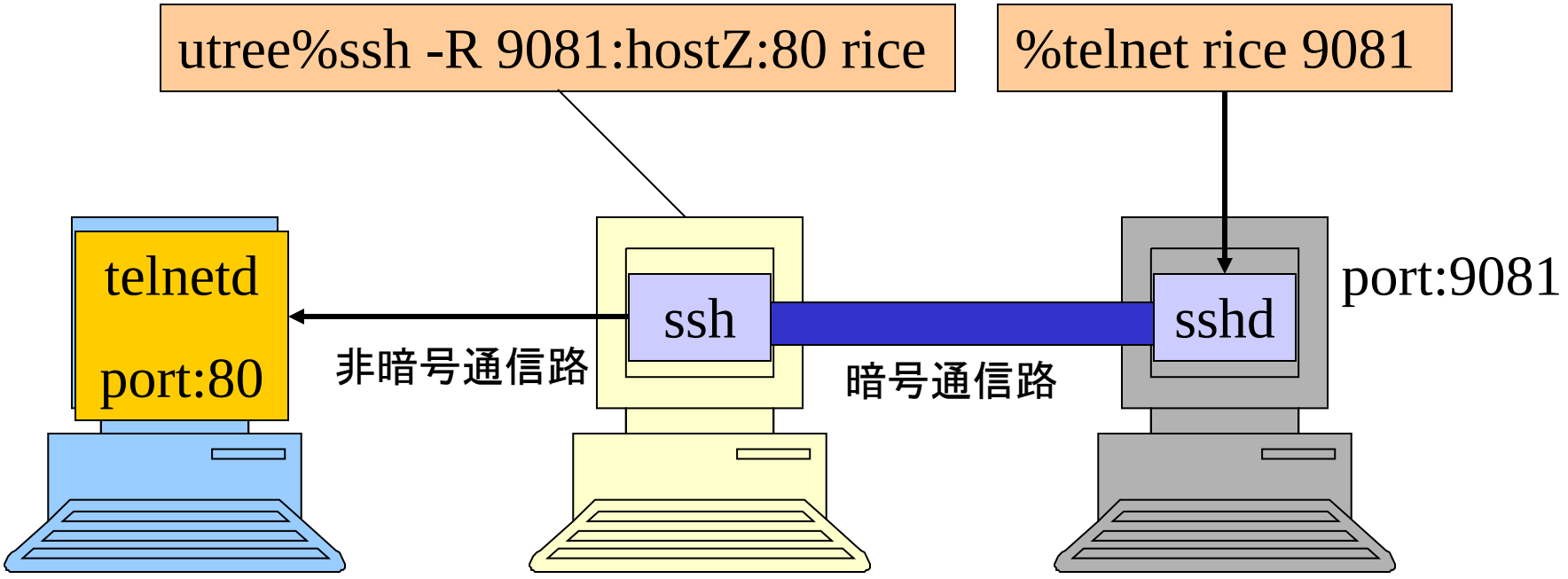
リモートポート転送

- 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とriceの間にSSH暗号通信路を作り、
rice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

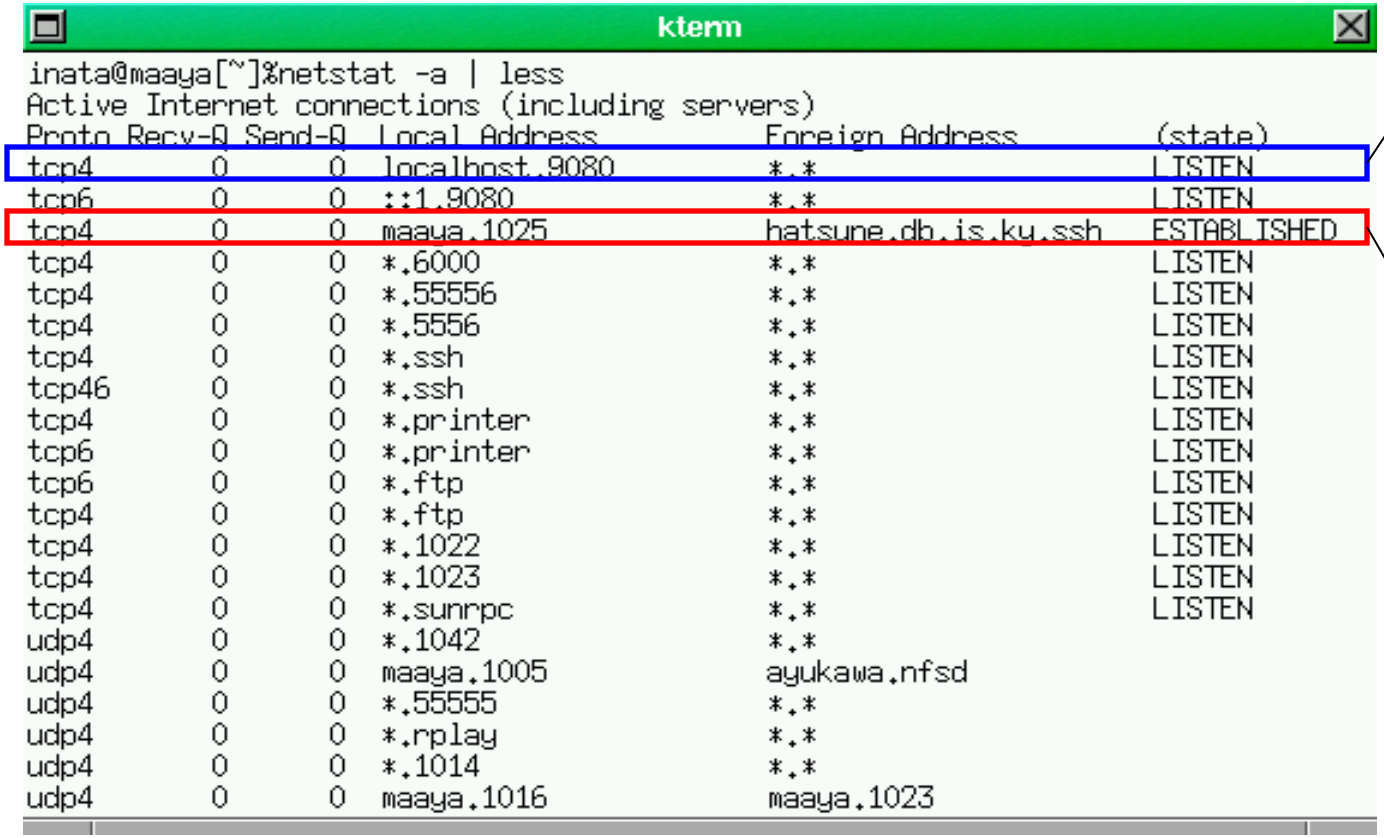
- ローカルポート転送
  - 適当なホストとSSH接続を確立し、ローカルポート転送による通信を行う

%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

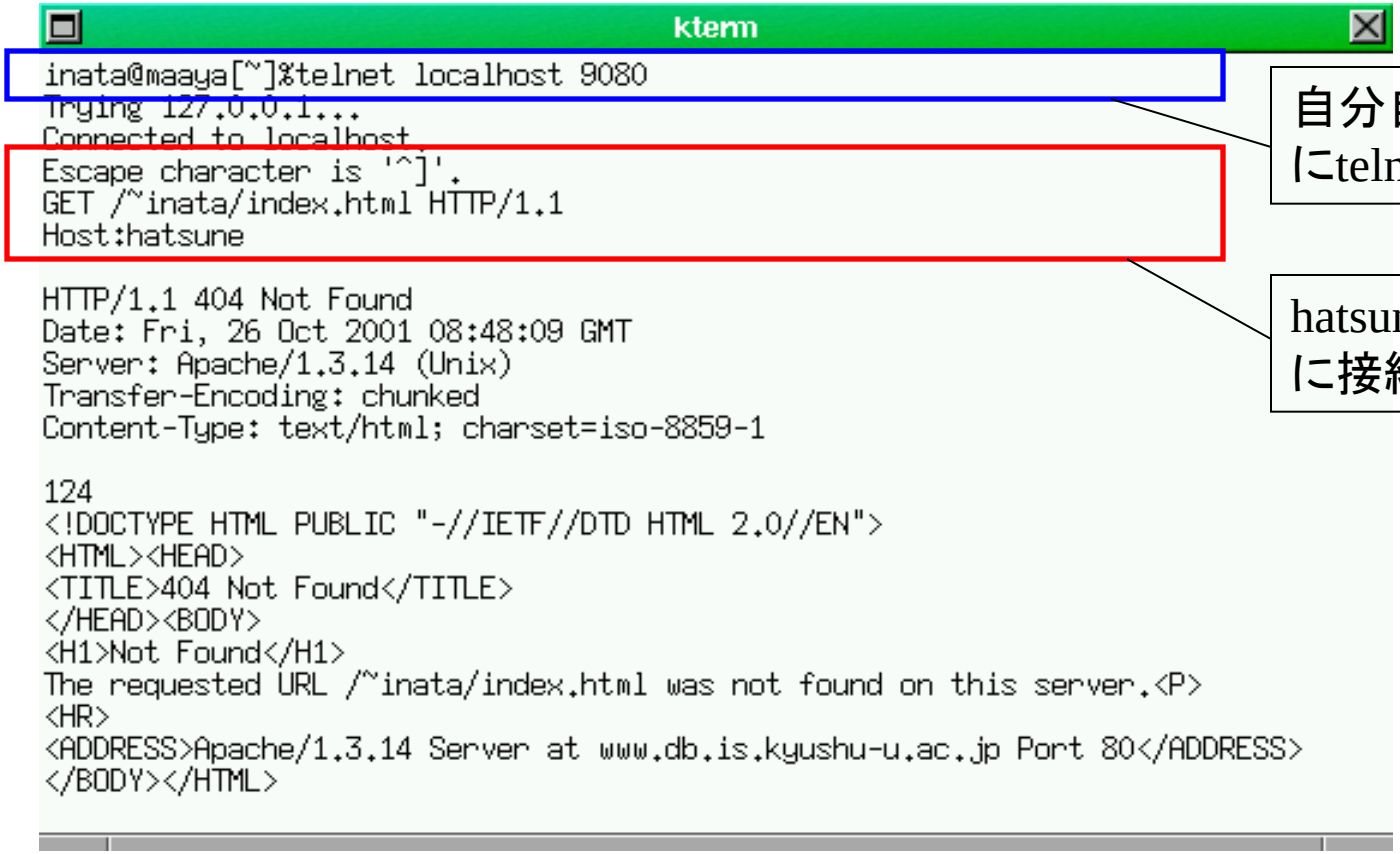


9080番ポートが接続待ち

SSHサーバとの接続

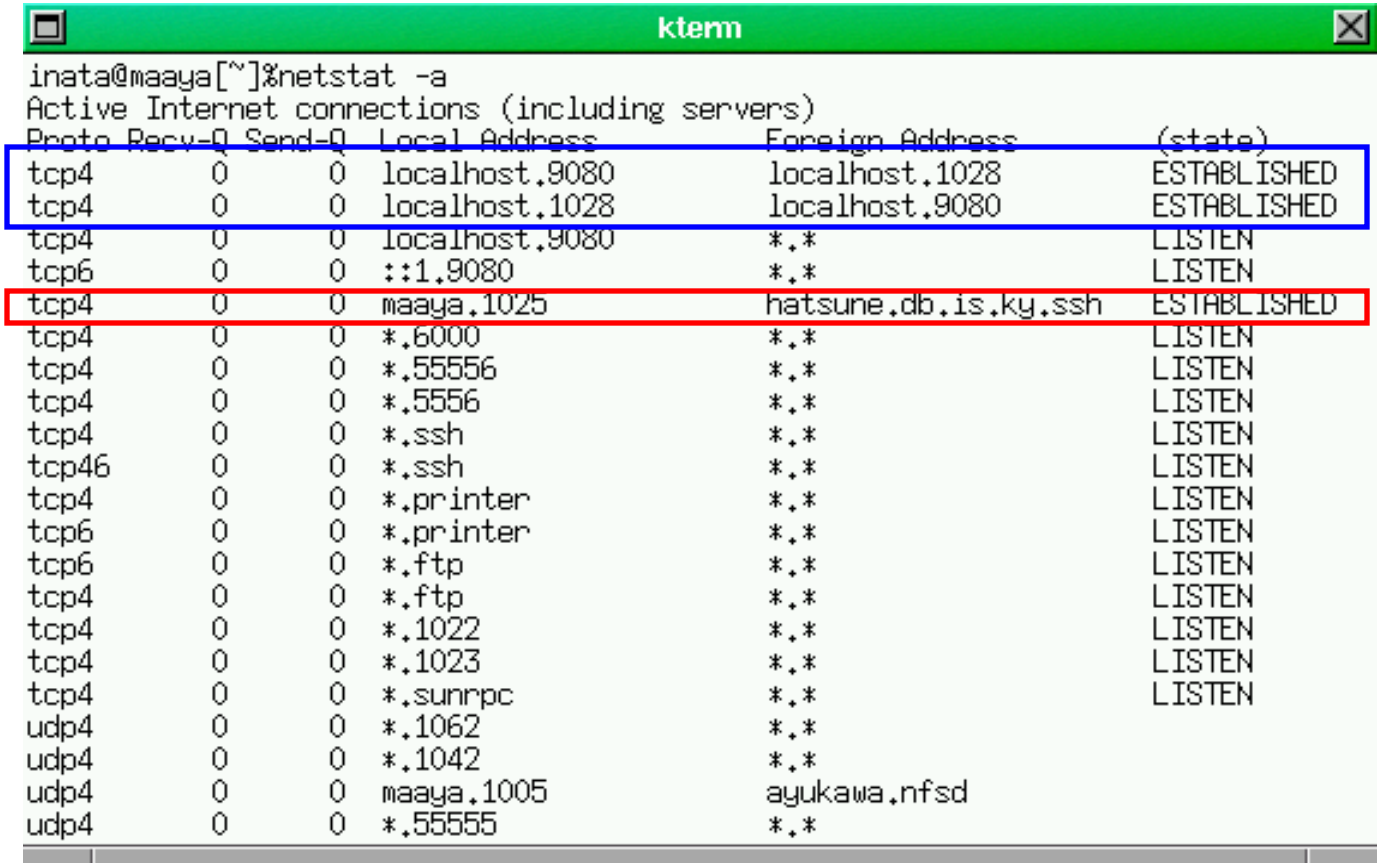
実験例(2)

- 自ホストの9080番ポートにtelnetで接続



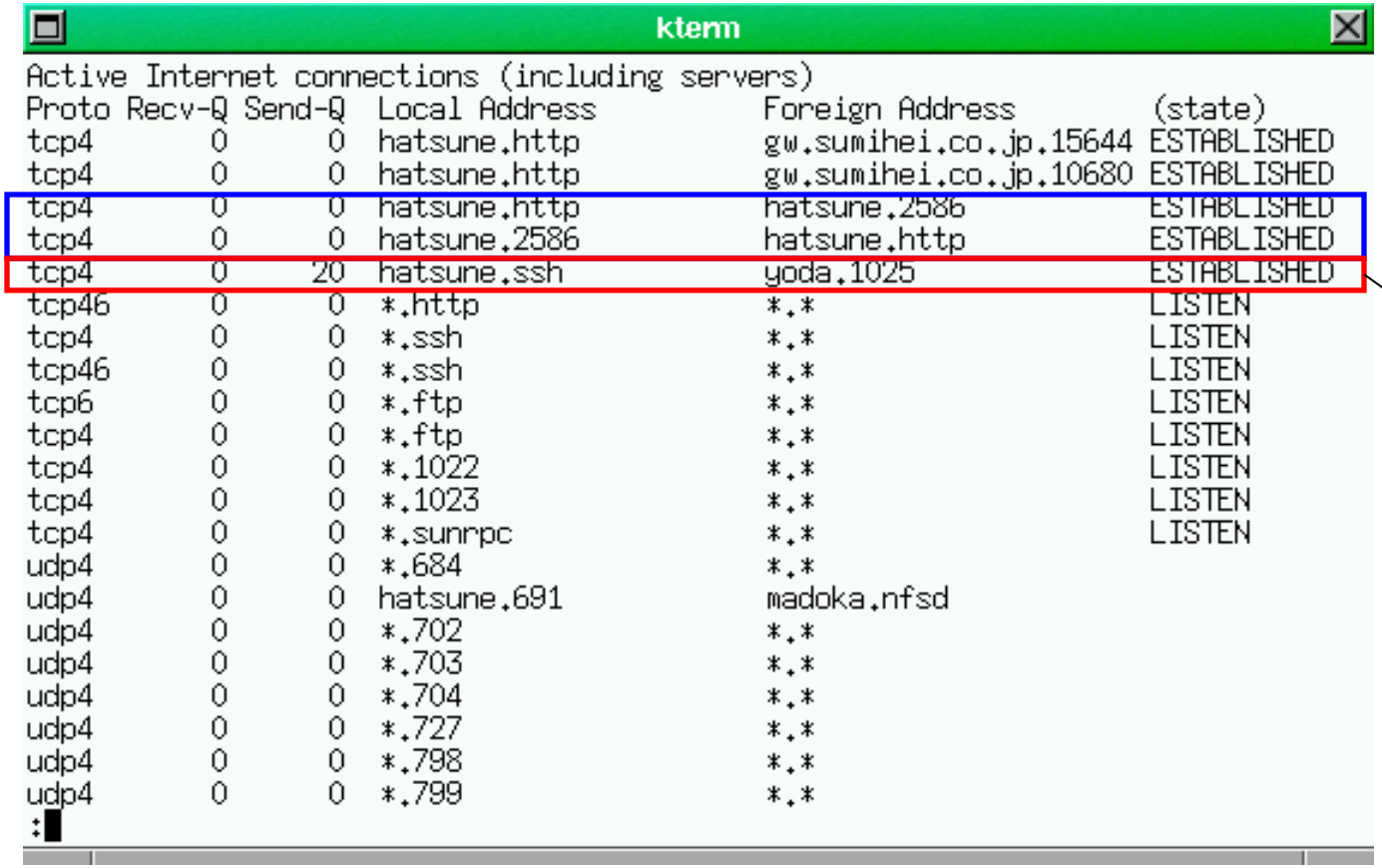
実験例(3)

- 自ホストの9080番ポートにtelnetで接続した状態



実験例(4)

- SSHサーバ側の状態



SSHクライアントとの接続