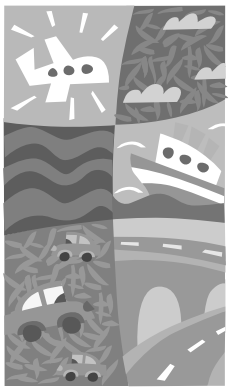


モバイルは今

SSHによるポート転送

楯岡 孝道
電気通信大学 tate@cs.uec.ac.jp

勤怠管理や施設予約などの事務的なやりとりを，イントラネット上のWebアプリケーションによって提供するケースが増えている．こういったサービスを外出先からインターネット経由で利用したいことはないだろうか．

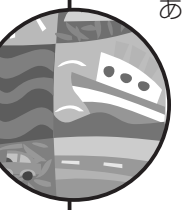
インターネットを経由して離れたオフィスを接続するために一般的なのはVPN（Virtual Private Network）だろう．外出先のノートパソコンを1つのリモートオフィスと考え，本来のオフィスとノートパソコンの間にVPNを構成することで，あたかもオフィスのネットワークに直接接続しているかのようにイントラネットのサービスを利用することができる．

しかしVPNの設定は，オフィス，ノートパソコン両端に管理者権限での設定が必要な上，仮想的とはいえノートパソコンをオフィスの内側に接続するという性格上，慎重に設定，運用する必要がある．たとえば，オフィスのネットワークがインターネットからはファイヤウォールで守られていても，VPN接続するノートパソコンがウイルスに感染すると，ファイヤウォールを通過してオフィス内の計算機に感染を広げてしまう可能性がある．

今回紹介するSSH（Secure SHell）のポート転送機能はこのような場合に簡便な解となり得る．なお，実行例はすべてOpenSSH実装（http://www.openssh.org/）のものを示したが，他の多くのSSH実装でも同様に利用可能である．

●

SSHは本来遠隔ホストにログインするためのアプリケーションだが，その機能の1つにTCPポート転送機能がある．ポート転送機能は，SSHのクライアント上で指定したローカルTCPポートへの接続を，SSHのコネクションを経由して，サーバからの特定ホスト／ポート宛の接続として転送する機能である．



たとえば，SSHのオプションとして -L X:target:Y を指定し，クライアント（ssh client）ローカルのX番ポートへの接続を，サーバ（ssh server）からホストtargetのY番ポートへの接続として転送した場合，その接続は**図-1**のようになる．SSH自体の接続を確立した時点で(a)のようにクライアント（ssh）とサーバ（sshd）の両プロセス間の仮想回線が確立される．この仮想回線の通信内容は暗号化され，通常のログイン操作などもこの回線を通じて行われる．さらにSSHクライアント（ssh）はローカルTCPポートX番を，ローカルホスト内アプリケーションからの接続が受けられる状態にする．

ここで，アプリケーションがクライアントのローカルTCPポートX番に接続する(b)と，sshは仮想回線中を通じてこの情報をsshdに送る．これを受けたsshdは新たにホストtarget，Y番ポート宛に接続し(d)，これを元の接続(b)と結びつける．これによってアプリケーションがローカル宛に行った通信は，SSH仮想回線(c)とsshdからtargetへのTCP接続(d)を通じて転送され，あたかもアプリケーションはYのポートに直接接続しているかのように動作することができる．

また，ホストtargetにとっては(d)の接続はホストssh serverからの接続となる．したがって，ssh serverがイントラネット内にあれば，ssh clientの接続位置によらず，イントラネットからの接続だと判断される．

この転送は同時に何本でも行えるので，イントラネット内のWebサーバに並列アクセスをするような使い方も可能である．また，オプションの指定によって逆にサーバ側のTCPポートへの接続を転送することもできる．なお，ローカルTCPポートには通常ループバックと呼ばれる当該ホスト以外からは接続できないIPアドレスを用いるため，他のホストからの接続を転送してしまうことはない．

下記のコマンド例では，クライアント上からhttp://

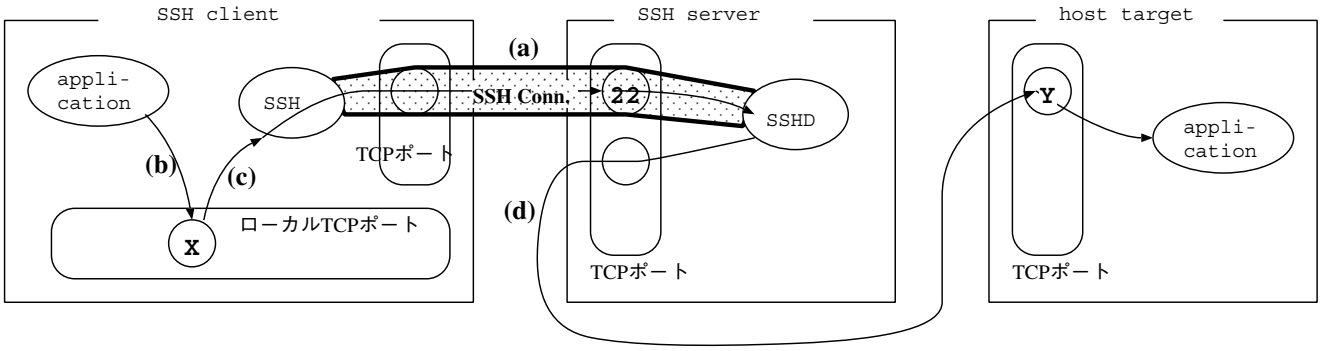


図 -1　ポート転送の例

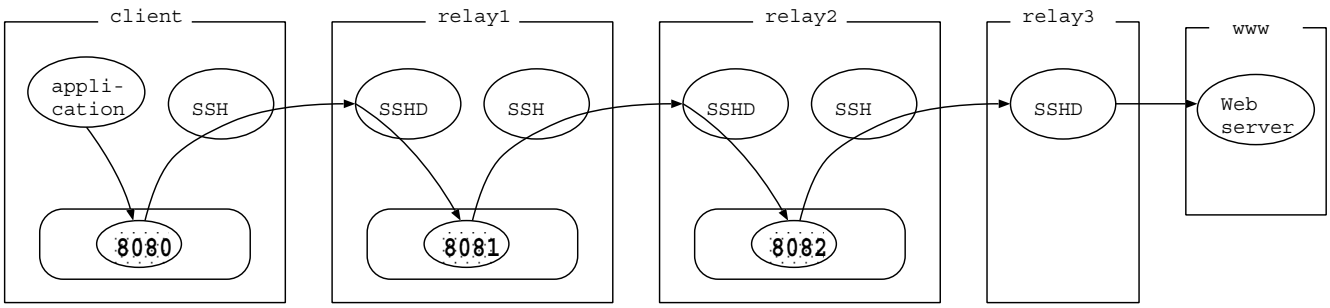


図 -2　多段階のポート転送

localhost:8080/ にアクセスすることで，serverを経由して，http://www:80/ にアクセスすることができる．

```
% ssh -L 8080:www:80 server
```

また，上記の原理が分かっていれば，各ホスト上でポート転送を繰り返し，直接接続できないサーバへの転送も実現できる．下記のコマンド例では Webアクセスを**図-2** のように 3 段中継して実現している．先の例同様に http://localhost:8080/ にアクセスすることで，最終的にホスト wwwの 80 番ポートへ接続できる．なお，% の左側はどこのホストで実行するコマンドかを表している．

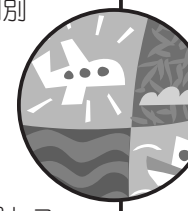
```
client% ssh -L 8080:localhost:8081 relay1
relay1% ssh -L 8081:localhost:8082 relay2
relay2% ssh -L 8082:www:80 relay3
```

上記の例はUNIX系OS上で動作確認を行ったが，Windows等でもコマンドライン版のSSHをインストールすれば実行可能である．また，PortForwarder（http://www.fuji-climb.org/pf/JP/）のように，このポート転送に特化したGUIアプリケーションも開発されている．このようなアプリケーションを利用すれば，より手軽にポート転送を利用することができる．

●

SSHのポート転送機能は，任意のTCPポートへの接続を転送できるため，非常に汎用性がある．SSHによるログインが可能ならば，ほとんどすべてのTCPサービスを中継可能と言えるだろう．また，仮想回線の通信内容は暗号化されるため，インターネットを経由した場合の安全性も高い．

今回はHTTPで利用される 80 番ポートを例にしたが，まったく同様にしてSMTP（25 番），POP3（110 番）などの転送も可能である．10 月号で紹介したように，SMTPやPOP3 の通信をポート転送することで，本来オフィス内からのみ利用可能なメールサーバをインターネットを通じて利用することもできる．この場合，SMTPサーバはオフィス内から接続されたと見なすため，メールの受信者にはメールの送信者がどこにいたか判別できないという利点もある．また，7 月号で紹介したVNC は通信内容を暗号化しないが，SSHのポート転送を用いることで，それを暗号化することができる．



もちろん，本来のアクセス制御範囲を超えてアクセスすることになるため，慎重な運用が必要なのは言うまでもない．たとえば，ローカルTCPポートは当該ホストからしかアクセスできないが，逆に言えばホスト上からなら誰でもアクセスできるため，信頼できない共用ホストで利用するのは危険である．

それを差し引いても，SSHでログインできる環境さえあれば，管理権限のない利用者であっても，さまざまなTCPサービスに利用できるため，応用範囲は広い．一度試してみてはいかがだろうか．

（平成 15 年 10 月 30 日受付）