Macintosh による SSH 通信

小澤義明 *

1 はじめに

近年の傾向として、各大学でファイアウオールが設置されています。京都大学でも「安全なギガビットネットワークシステム (KUINS-III)」が本年四月より運用開始されました。
これらは我家を守るために高い塀をめぐらし、外部からの侵入を未然に防ぐことや、我家のいたずら息子の悪さでご近所に迷惑をかけない等を目的としています。しかし、外の世界での安全性は保証されていません。
インターネットの世界で安心して通信するための一つの方法として、通信内容を暗号化して安全な通信を行う SSH(Secure SHell) があります。また、ファイアウオール越しに他機関のサーバと通信する場合は通常 SSH の利用が必須となります。

今回は Macintosh における SSH の利用を簡単に紹介します。

2 Macintosh 用 SSH 通信ソフト

次の URL
http://www.openssh.org/ja/windows.htmlをアクセスすると、 Macintosh 用に次の二種類の SSH 通信クライアントソフトが紹介されています。これらはいずれもフリーのソフトですが、端末エミュレータです。

1. NiftyTelnet 1.1 SSH
   SSH1 プロトコルといわれる古いタイプの通信法を用います。また、日本語の表示ができなのが致命的ですが、 scp(secure copy client) 機能を有しています。
2. MacSSH
   SSH2 プロトコルで通信します。うれしいことに、日本語の表示ができます。

本センターのサーバ群 (スーパコンピュータ (vpp)、計算サーバ (spp)、メールサーバ (sakura)) は、 OpenSSH を用いており、 SSH1 および SSH2 のいずれのプロトコルでも通信できますが、日本語が使える MacSSH を中心にその利用法を紹介することにします。しかし、 NiftyTelnet 1.1 SSH も使い勝手が悪いのですが、 scp(secure copy client) 機能を有していますので、この scp の利用についても紹介します。

2.1 MacSSH および NiftyTelnet 1.1 SSH の入手

MacSSH はhttp://www.macssh.com/から入手します。原稿執筆時のバージョンは MacSSH 2.1fc3 でした。なお、 MacSSH のホームページでシェアウエアですが MacSFTP(Secure FTP client) もダウンロードできます。これは 15 日の試用期間つきで $25 です。日本円 (2,890 円) での支払もできるようになっていました。
一方、 NiftyTelnet 1.1 SSH は、
http://www.lysator.liu.se/~jonasw/freeware/niftyssh/ から入手できます。バージョンは NiftyTelnet 1.1 SSH r3 でした。
それぞれを Netscape や IE でダウンロードしますと、通常はダウンロードしたフォルダに新しいフォルダ (MacSSH PPC, niftytelnet-1.1-ssh-r3 フォルダ) に解凍してくれます。
解凍しない場合は、 Stuffit Expander(フリーソフ

* おざわよしあき (京都大学学術情報メディアセンター)

ト) が有るか sherlock [1]で検索してください。見つからなければ、http://www.stuffit.com/expander/macindex.htmlからダウンロードして下さい。

3 MacSSH の利用

MacSSH は端末のエミュレート機能だけを有しています。ただし、 FTP 機能が内蔵されていますが、安全な通信はできませんので注意してください。

MacSSH をダブルクリックして起動します。「File」メニューから「Open Connection...」を選択し、現れたウインドウの ”Host Name” に接続先のホスト名あるいは IP アドレスを入力し、 [Connect] をクリックします。これで SSH 通信が確立されますが、日本語を使うためにいくつかの設定をする必要があります。

3.1 環境設定

MacSSH を起動し、環境の設定をします。「Edit」メニューの「Terminals」を選択します。現れた [Terminals] ウインドウの [Edit] をクリックします。次に現れた [Edit Terminal...] ウインドウの [Terminal] タブの [Emulation] を ”VT100”に (図 1)、 [Font] タブの [Font] を ”Osaka- 等幅 ”にし、適当なフォントサイズを入力します (図 2)。次に、これは好みによりますが、 [Color] タブの [Normal forground color] を黒色に、 [Normal background color] を白色に変更し、 [OK] をクリックします (図 3)。 [Terminals] ウインドウを [OK] をクリックして閉じます。

[1]アップルメニュー をクリックし、プルダウンメニューから選択します

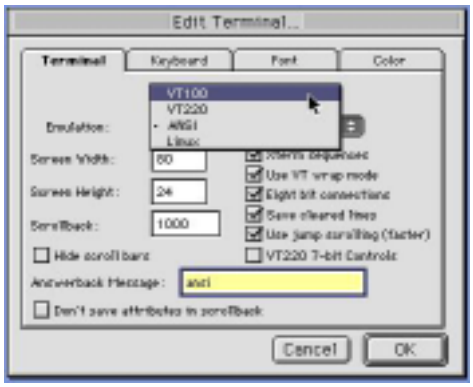

図 1. emulation を VT100 に

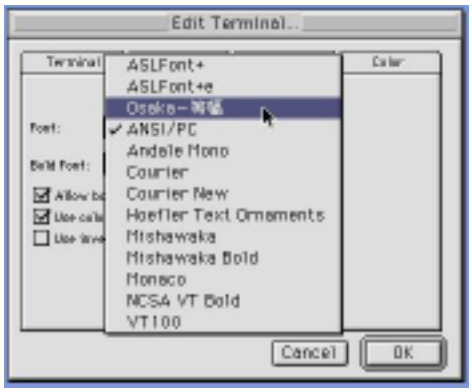

図 2. Font を Osaka 等幅に

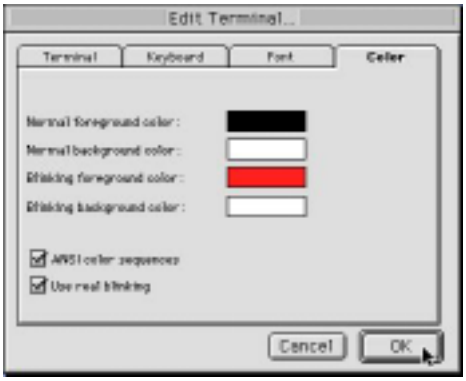

図 3. forground color の変更

次に、「Favorites」メニューの「Edit Favorites...」を選択します。 [Favorites] ウインドウの [Edit] をクリックします。 [Edit Favorite...] ウ

インドウの [General] タブの [Translation Table] を ”EUC-JP”に設定し、 [OK] をクリックして [Edit Favorite...] ウインドウを閉じます (図 4)。この設定と Font 設定で日本語表示が可能となりました。 [Favorites] ウインドウを [OK] をクリックして閉じます。

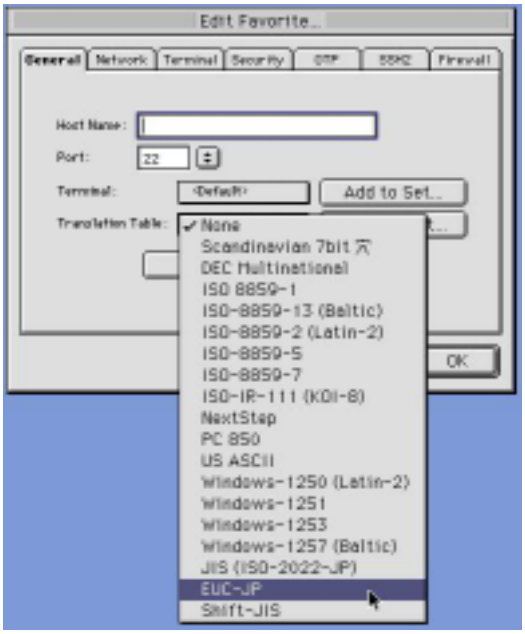

図 4. Translation Table の変更

3.2 本センターのサーバと接続する

環境設定が終了しましたので、本センターの計算サーバ (spp.kudpc.kyoto-u.ac.jp) と接続してみましょう。

「File」メニューから「Open Connection...」を選択し、 [Open Connection...] ウインドウの [Host Name] に接続先を入力し、 [Connect] をクリックします (図 5)。

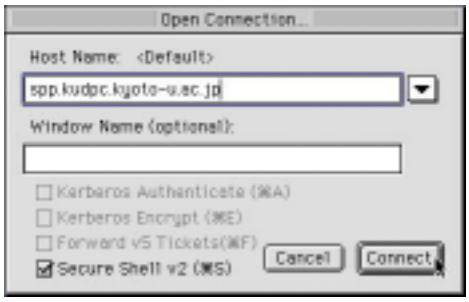

図 5. 接続先サーバの指定

[SSH2 Login] ウインドウの [User Name] に利用者番号を、 [Password] にパスワードを入力し、 [OK] をクリックします (図 6)。 MacSSH で初めてサーバに接続した場合は、サーバの公開鍵が Macintosh に保存されていないので、 [Host Key Unknown] ウインドウが現れ、公開鍵を受入れ・保存するか否かの問合わせがありますので、 [Accept & Save] をクリックし、保存しておきます (図 7)。

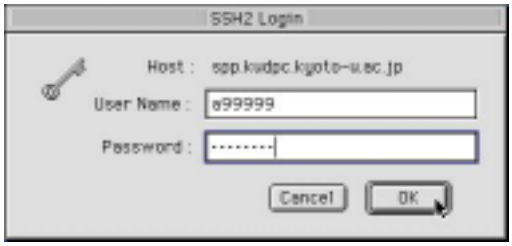

図 6. ログイン

図 7. サーバの公開鍵の受入れ・保存

計算サーバと SSH2 で接続が完了しました。画面左下に「鍵がかかった錠」 が表示されています。

サーバと Macintosh の間の通信は暗号化され、安全な通信が確保されました (図 8)。

図 8. 計算サーバと安全な通信

図 9. プロトコルに SSH-3DES を設定

4 NiftyTelnet 1.1 SSH で scp する

NiftyTelnet 1.1 SSH は日本語が使えない、SSH1 プロトコルという古いタイプの通信法、ではあるのですが、 scp(secure copy client) 機能を有していますので、サーバとの間で安全にファイルのコピーができます。ここでは、その使用法を簡単に紹介します。

4.1 環境設定

Scp を利用するために一個所だけ環境設定が必要です。まず、 NiftyTelnet 1.1 SSH を起動します。 [New Connection] ウインドウの [Edit...] をクリックします。

[Telnet Shortcut] ウインドウの [Protocol] メニューに暗号化の手法を指定します。今回は SSH-3DES を選択しました (図 9)。次に、 [OK] をクリックして終りです。

4.2 サーバと scp する

本センターの計算サーバとの間で安全なファイルコピーをやってみます。

[New Connection] ウインドウの [Hostname] に計算サーバのアドレスを入力し、 [Scp...] をクリックします (図 10)。

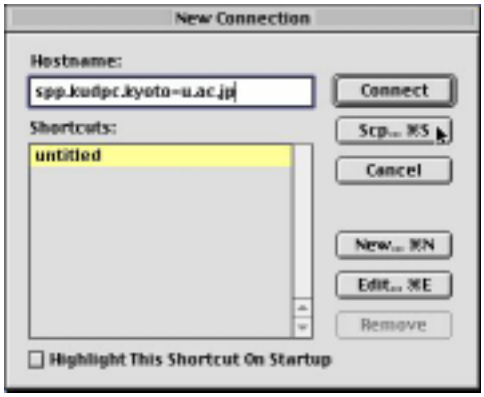

図 10. 計算サーバと scp で接続

図 11 のウインドウが現れます。

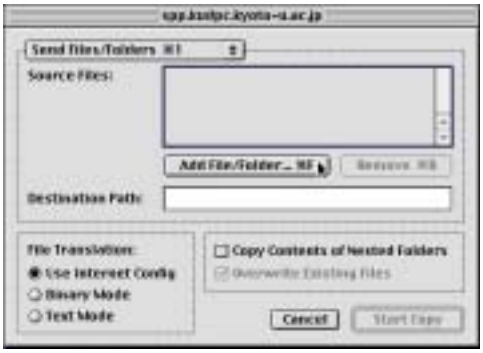

図 11. 被コピーファイル / フォルダの決定

4.2.1 Macintosh のファイルをサーバにコピー

まず、 Macintosh のファイルをサーバにコピーしてみます。図 11の上方を [Send Files/Folders] にします。 [Add File/Folder...] をクリックすると、ファイル / フォルダ選択ウインドウが現れますので、サーバへコピーするファイルまたはフォルダを決定します。 [source files] に決定したファイルまたはフォルダが表示されます。複数のファイル / フォルダをコピーする場合は、さらに [Add file/folder...] をクリックして追加します。次に、 [Destination Path] にサーバの格納するパスを指定します。ホームディレクトリに転送する場合は、指定しません。今回は、$HOME/Images ディレクトリのもとにファイルコピーします。準備が整えば、 [Start Copy] をクリックします (図 12)。

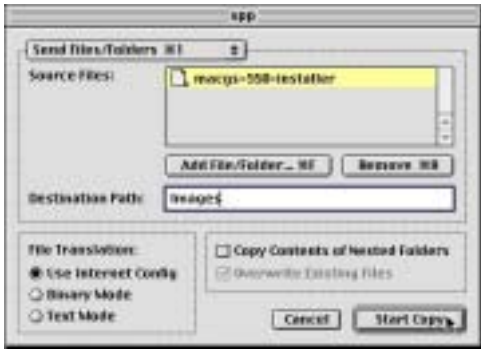

図 12. 準備を整え、 Start Copy のクリック

指定したフォルダにさらにフォルダがある場合、そのフォルダも含めてコピーをしたい場合、図 12の右下の [Copy Contents of Nested Folders] のチェックボックスをオンにしておきます。

NiftyTelnet 1.1 SSH で初めてサーバに接続した場合は、サーバの公開鍵が Macintosh に保存されていないので、 [Host Identification Alert] ウインドウが現れ、公開鍵を受入れ・保存するか否かの問合わせがありますので、 MacSSH と同様に [Accept & Save] をクリックし、保存しておきます。

次に、 [SSH Login] ウインドウの [User Name] に利用者番号、 [Password] にパスワードを入力し、 [Login] をクリックします (図 13)。

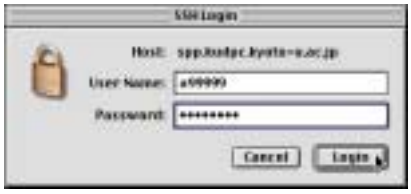

図 13. scp の開始

図 14の様にファイルのコピー状況が表示されます。

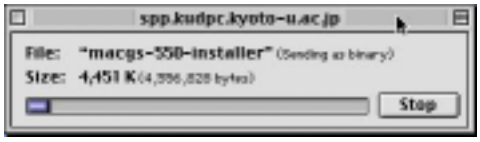

図 14. ファイルのコピー状況

4.2.2 サーバのファイルを Macintosh にコピー

逆に、サーバのファイルを Macintosh の方へコピーします。

図 15 の様に、ウインドウ上方を [Receive Files/Folders] に切替えます。 [Source Files] にサーバのファイル / ディレクトリを入力します。次に、 [Pick Folder] をクリックして Macintosh のコピー先フォルダを設定します。
今回は、デフォルトのデスクトップを設定しました。

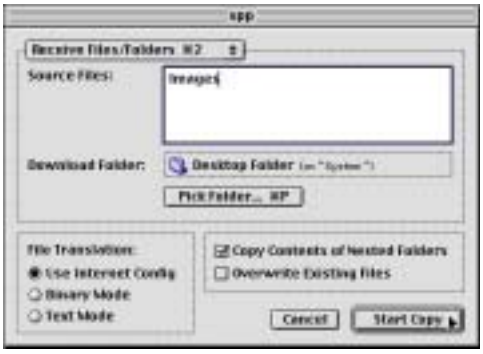

図 15. サーバから Macintosh へコピー

また、右下の [Copy Contents of Nested Folders] のチェックボックスをオンにしました。これは、コピーを再帰的に行うことを指定しています。
［Start Copy] をクリックすると、 [SSH Login] ウインドウが表示されますので、 [User Name] に利用者番号、 [Password] にパスワードを入力し、 [Login] をクリックします (図 13)。
コピーが開始され、図 14の様にコピー状況が表示されます。

5 MacSSH によるポートフォワーディング

ポートフォワーディングは、 Macintosh から例えば telnet を使った通信を、別の通信経路を用いてサーバの telnet サーバに届けることです。たいていは、 SSH の安全な通信の仕組みを、この別の通信経路に用います。
これによって、クライアントやサーバの変更なしに、 ftp、 pop、 IMAP などの通信を行うことができます。これは、 SSH の安全な通信経路をトンネルにみたて、トンネルの中は ftp や pop、 IMAP の通信を流し、通信を外部から隠蔽しているイメージで、トンネリングといいます。

5.1 ポートフォワーディング設定

ここでは、 FTP を例にポートフォワーディングの設定を簡単に紹介します。
ここで注意することは、 FTP 通信の仕組みで、 user-id、 password については暗号化された安全な通信経路を利用しますが、データの転送は安全ではありません。
FTP 以外の pop、 telnet、 SMTP、 IMAP などはすべて安全な通信となります。
相手のサーバを本センターの計算サーバとします。
MacSSH を起動し、「Favorites」メニューの「Edit Favorites...」を選択します。今回は、 [Favorites] ウインドウの [New] をクリックします。
[Edit Favorite...] ウインドウの [General] タブの [Alias] に適当な文字列を入力します。今回は、 ”SPP (FTP)”としておきました。 [Host Name] は ”spp.kudpc.kyoto-u.ac.jp”を入力します (図 16)。

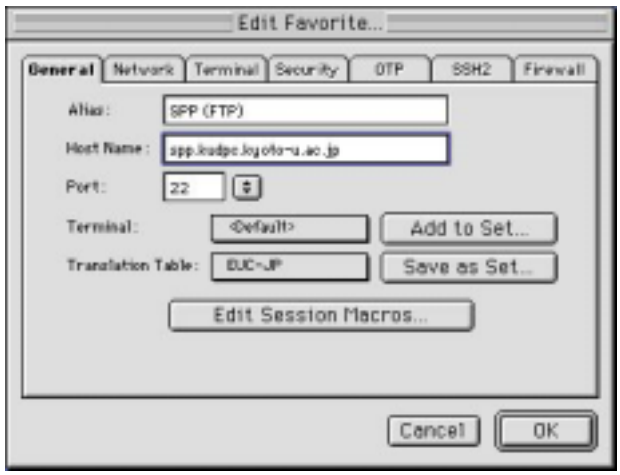

図 16. General タブの設定

次に、 [Security] タブをクリックし、 [Username] に計算サーバの利用者番号を入力します。
[Password] へのパスワードの入力ですが、ご利用の Macintosh の管理状況によって安全性を第一に考慮してください (図 17)。

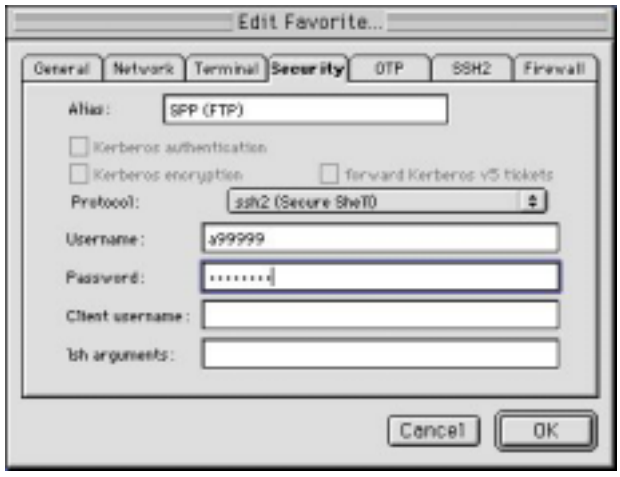

図 17. Security タブの設定

続いて、 [SSH2] タブをクリックします。
[Method] プルダウンメニューから ”Local TCP port forward”を選択します。その下の、 [Local

port] に FTP の ”21”を、 [Remote host] に ”spp.kudpc.kyoto-u.ac.jp”、 [Remote port] にも ”21”を入力します (図 18)。

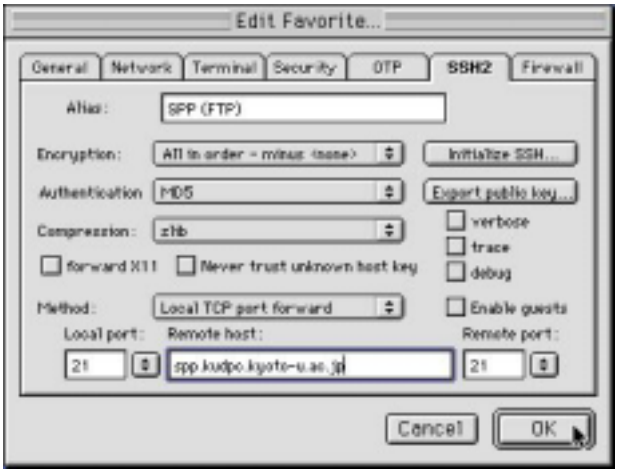

図 18. SSH2 タブの設定

この、 [Local port]、 [Remote port] に、 POP3 なら ”110”を、 SMTP なら ”25”を、それぞれ目的に合わせて入力します。

[OK] をクリックして、ウインドウを閉じ、 [Favorites] ウインドウも [OK] をクリックして閉じます。

5.2 Fetch によるポートフォワーディングの利用

MacSSH を起動します。下図のように「Favorites」メニューの [SPP (FTP)] をクリックします。

図 19. Favorites メニューからの接続

前節のポートフォワーディング設定でパスワードを設定しなかった場合、パスワード入力ウインドウが現れますので、入力します。

続いて、 Fetch を起動します。 [New Connection.] ウインドウの [Host] に ”127.0.0.1”を、 [User ID] には計算サーバの利用者番号を、 [Password] にパスワードを入力し、 [OK] をクリックします (図 20)。

図 20. Fatch の接続先は 127.0.0.1

後は、通常の Fetch の利用となります。

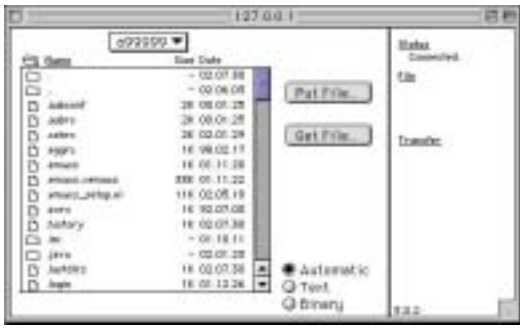

図 21. Fetch 接続完了

ここでは、 Fetch(FTP) を用いたポートフォワーディングを紹介しましたが、 POP3、 IMAP についても同様です。 MacSSH の「Favorites」メニューで、新たに POP3 または IMAP のポートフォワーディングの設定をします。メールクライアントには、 Eudora や Netscape などがありますが、 POP3、 IMAP サーバのアドレスを ”127.0.0.1”に変更するだけです。

ファイアウオール越しに、プロバイダなどのメールサーバに POP3(IMAP) と SMTP の両方でアクセスする等の場合はどうすれば良いのでしょうか。

MacSSH の「Favorites」メニューで、新しい設定を開きます。 General タブの設定は相手先に応じた内容で、 SSH2 タブの設定は、 [Method] プルダウンメニューを ”Request pty (default)”にしておきます。 Security タブの [Username] と [Password] は相手先に応じた値、そして、 [lsh arguments] に ”–L 110: 相手先アドレス:110 –L 25: 相手先アドレス:25”を設定します。
メールクライアントの方は、 POP3(IMAP) サーバのアドレスだけでなく、 SMTP サーバのアドレスも ”127.0.0.1”に変更します。

6 おわりに

書かなくちゃ、書かなくちゃと、一年過ぎてしまい、時期を逸してしまった感もありますが、今回やっと Macintosh による SSH 通信を書くことができました。 Macintosh ユーザがはたしていらっしゃるのか、みんな Mac OS X に移行してしまって、OpenSSH を使っているよなんて声も聞こえそうです。

MacSSH で公開鍵を利用する認証方法も紹介する予定でしたが、都合で割愛します。次の URL http://www.ists.dartmouth.edu/IRIA/knowledge_base/keyxchange.htmで詳細に述べられていますので、トライしてください。