SSH2 公開鍵認証移行マニュアル

２００６年４月３日

遺伝情報実験センターでは２００５年１２月１２日より、パスワード認証による接続を受け付けなくなりました。今後も ssh 接続を行いたい場合には ssh2 公開鍵認証を行えるようにしてください。

１．Linux, UNIX, Mac OSX の場合

①の作業は自分が使用するコンピュータで行ってください。

① 自分の RSA または DSA 公開鍵と秘密鍵のペアを作成します。この操作を行うと、通常 ~./ssh というフォルダに id_rsa と id_rsa.pub という二つのファイルが作られます。既に鍵ペアを持っている場合はこの作業を省略して構いません。

```
[dhcp-178-217:~] USER % ssh-keygen -t rsa?
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/USER /.ssh/id_rsa): ?通常はこのままリターン
Enter passphrase (empty for no passphrase):      ←パスフレーズを入力
Enter same passphrase again:       ←もう一度同じものを入力
Your identification has been saved in /Users/USER /.ssh/id_rsa.
Your public key has been saved in /Users/USER/.ssh/id_rsa.pub.
The key fingerprint is:
72:46:02:24:fc:50:08:d1:cc:ea:73:8b:55:35:04:37 USER @*****.gen-info.osaka-u.ac.jp
```

ここで入力するパスフレーズは当センターのログインパスワードと違うものを使用することを推奨します。

② 当センターのサーバーマシンに公開鍵を転送します。大阪大学内では FTP で転送することができます(学外からは FTP での転送はできません)。

まず、スタートアップメニューのプログラム→アクセサリからコマンドプロンプトを起動します。コマンドプロンプト画面で cd “c:¥Program Files”と入力し（cd c:¥prog と入力後 Tab キーを押すと自動的に入力されます）

```
[dhcp-178-217:~] USER % cd ~/.ssh↵
[dhcp-178-217:~] USER % ftp 133.1.178.5↵
Connected to 133.1.178.5.
220 idngs1 FTP server (SunOS 5.8) ready.
User (133.1.178.5:(none)): USER↵ ←ユーザー名を入力
331 Password required for USER.
Password: ←当センターのログインパスワードを入力
230 User USER logged in.
ftp> put id_rsa.pub↵
200 PORT command successful.
150 Binary data connection for id_rsa (133.1.178.******).
226 Transfer complete.
ftp: ** bytes sent in 0.00Seconds 20000.00Kbytes/sec.
ftp> bye↵
221 Goodbye.
```

③ 当センターのサーバーマシンの~/.ssh/ authorized_keys **というファイルに公開鍵を格納します。このファイルはテキストファイルです。複数の公開鍵を格納することができます。**

```
[dhcp-178-217:~] USER % telnet 133.1.178.5↵
(ログイン名とパスフレーズ)
> cd ~/.ssh↵
> cat ~/id_rsa.pub >> authorized_keys↵
> chmod 600 authorized_keys↵
> rm ~/id_rsa.pub↵
> exit↵
```

②, ③の代わりに authorized_keys **に** id_rsa.pub **の内容をコピー&ペーストで追記しても構いません。**

以上で設定は終わりです。

2．WINDOWS の場合

これから行う作業は自分が使用するコンピュータで行う内容です。

① UTF-8 TeraTerm Pro をダウンロード&インストールします。
例えば http://sourceforge.jp/projects/ttssh2/ からダウンロードできます（2006 年 4 月 3 日現在）。

② メニューから「setup」(または「設定」) →「SSH KeyGenerator」を選択します。(図.2-1)

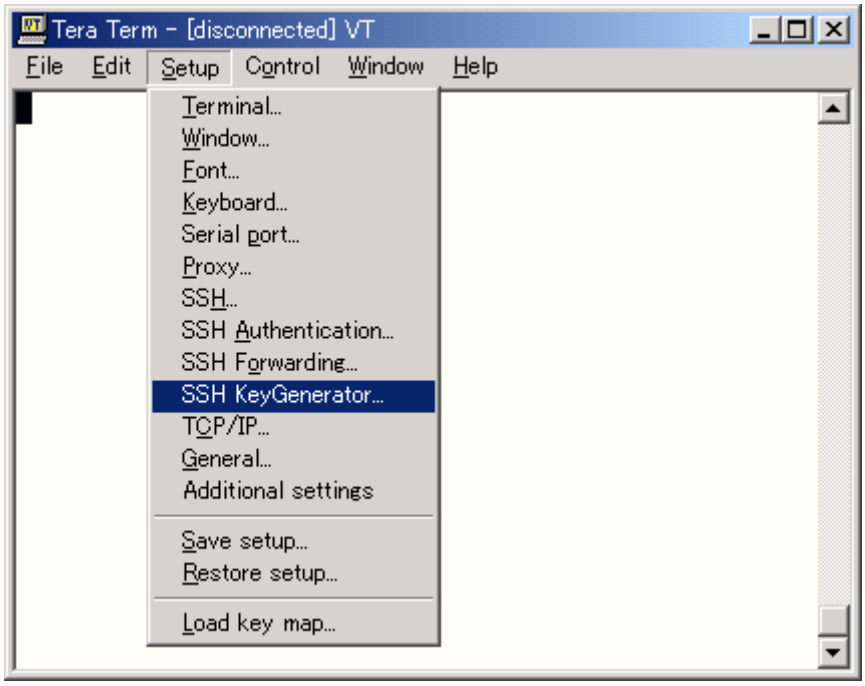

図.2-1

③ RSA を選び、Generate をクリックしてください。(図.2-2)

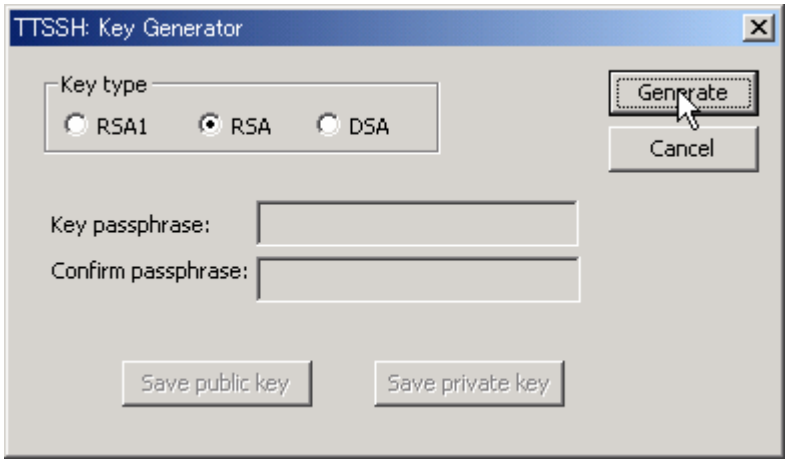

図.2-2

④ 公開鍵認証用のパスワードであるパスフレーズを入力（ログイン ID のパスワードとは別である事が望ましい）し、Save public key と Save private key をクリックしてくだ

さい。(図.2-3)それぞれ保存場所を聞かれるので自分のわかる場所に(例えば My Documents など)に保存してください。

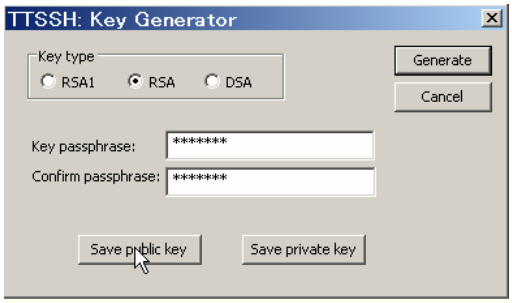

図.2-3

⑤ UTF-8 TeraTerm Pro を telnet で接続します。(図 2-4)

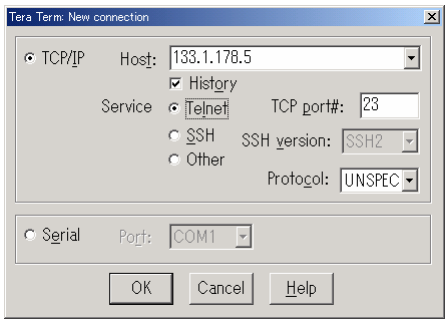

図.2-4

"login:"と出たらユーザー名と当センターのログインパスワードを入力して接続して下さい。

⑥ emacs で~/.ssh/authorized_keys に id_rsa.pub の内容をコピー&ペーストで追記します。
まず、emacs ~/.ssh/authorized_keys と入力し、emacs で authorized_keys を開きます。

```
SunOS 5.8

login: USER?
Password:
Last login: Mon Apr  3 17:06:43 from ＊＊＊＊
Sun Microsystems Inc.   SunOS 5.8          Generic Patch     October 2001
idngs1[USER<1>]% emacs ~/.ssh/authorized_keys?
```

次に、④の操作で保存した id_rsa.pub ファイルを適切なプログラム（ワードパッド等）で開き、内容を全てコピーし、emacs で開いた authorized_keys に貼り付けます。(図.2-5)

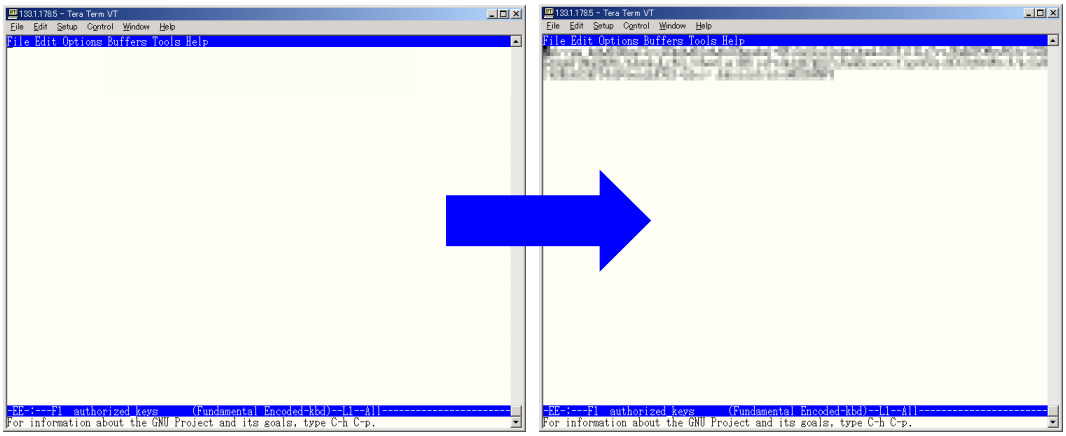

図.2-5

これを保存(Ctrl+x→Ctrl+s)し emacs を終了(Ctrl+x→Ctrl+c)して、exit でログアウトします。

以上で設定は終わりです。

⑦ メニューから「setup」→「SSH Authentication」を選択し、「Use RSA/DSA key to log in」から先ほど保存した id_rsa を呼び出して OK をクリックしてください。最後に「setup」→ 「save setup」(または「設定の保存」)で、設定を保存してください。(図.2-6)

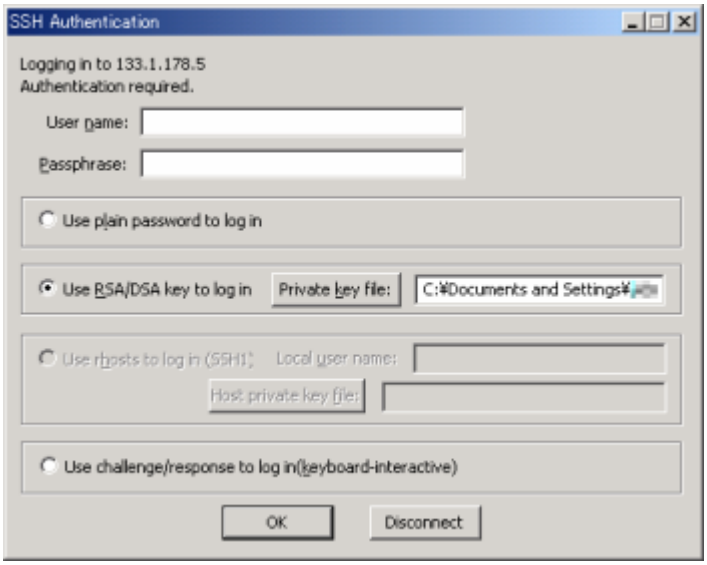

図.2-6

これでユーザーネームとパスフレーズを入力する事で ssh2 による接続が可能となりました。

参考文献

http://www.netlab.is.tsukuba.ac.jp/~one/ssh/#RSAAuth