作成：平成 19 年 5 月 8 日
修正：平成 22 年 5 月 25 日

SSH で公開鍵認証方式を使いログインする

目　次

1. はじめに

はじめに、このドキュメントは PKI（公開鍵認証基盤）についてある程度知識がある方を対象に記述しています。従って「公開鍵認証」「秘密鍵」「公開鍵」「パスフレーズ」など、以下の説明の中で出てくる用語がわからない方は各自で調べて、十分に用語を理解した上でこのドキュメントを読み進めてください。

本学の遠隔端末接続サービスでは、SSH のユーザ認証方式の一つである「パスワード認証」を許可しています。この「パスワード認証」を使用した場合、通信経路はホスト認証によって暗号化されますが、パスワードが通信経路に流れます。

より安心して通信を行うために「公開鍵認証」というユーザ認証方式があります。このユーザ認証方式は証明書によって認証を行うため、パスワードが通信経路に流れることがなくなります。ここでは「公開鍵認証」によるユーザ認証を用い、自宅などのインターネット上から本学の遠隔端末接続サービスを、より安心して利用する方法について説明します。

2. 留意事項

公開鍵認証を利用する場合、以下の事項に留意してください。

- 作成した秘密鍵は適切な場所に保管するようにしてください。
- パスフレーズを設定しないことができますが、その場合は秘密鍵が他人に入手されると、不正にログインされるなどの危険性が高くなります。必ずパスフレーズを適切に設定してください。
- 認証情報の暗号化の完全性を保証するものではありません。

3. 公開鍵と秘密鍵の作成方法

公開鍵と秘密鍵の作成方法にはいくつかありますが、ここでは本学の遠隔端末接続サーバである cc2000（以下 cc2000 という。）上で、公開鍵と秘密鍵を作成する方法について「sandai」というユーザ ID を例に説明します。

お使いのクライアントで TeraTerm などの SSH クライアントを利用し、ホスト名「cc2000.kyoto-su.ac.jp」としてログインしてください。

3.1. 公開鍵と秘密鍵の作成

1) cc2000 へのログインが完了したら、ssh-keygen というコマンドで秘密鍵と公開鍵を作成します。以下のように実行してください。

```
$ ssh-keygen -t dsa
```

2) ここで選択する「DSA」とは SSH が使用する暗号化アルゴリズムの一つです。同じく暗号化アルゴリズムとして「RSA」、「RSA1」がありますが、ここではよりセキュリティ強度の高い SSH2 プロトコルに対応した「DSA」認証を使用します。

3) ssh-keygen コマンドの実行例は以下のようになります。なお下記例でのディレクトリ PATH は個人の環境によって異なります。

```
$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/NF/home/misc0/sandai/.ssh/id_dsa):
→ 作成する秘密鍵のパス名を入力、または Enter キーを押してください。
Created directory '/NF/home/misc0/sandai/.ssh'.
→ ディレクトリ「/NF/home/misc0/sandai/.ssh」が作成されました
Enter passphrase (empty for no passphrase):
→ 秘密鍵につけるパスフレーズを入力（１０文字以上を設定してください）
Enter same passphrase again:
→ 確認のため、もう一度パスフレーズを入力
Your identification has been saved in /NF/home/misc0/sandai/.ssh/id_dsa.
→ 秘密鍵「id_dsa」が作成されました
Your public key has been saved in /NF/home/misc0/sandai/.ssh/id_dsa.pub.
→ 公開鍵「id_dsa.pub」が作成されました
The key fingerprint is:
```

```
69:8f:84:54:98:52:3e:66:8a:02:ed:3d:ca:66:bf:19 sandai@cc2001
```
→　公開鍵のフィンガープリントが表示されます

4)　これで公開鍵と秘密鍵の作成が完了しました。作成された秘密鍵は、適切な方法でクライアントにダウンロードし、他人が見ることができない安全なフォルダに保存・管理してください。

5)　なお、ダウンロード方法については以下のコンピュータ環境の使い方をご覧ください。

学内向け TOP ページ >> コンピュータ環境の使い方 >> ファイル転送サービス利用手引き

- FTPS を使用したファイル転送方法について
- SCP を使用したファイル転送方法について

次項では、作成した公開鍵を接続先のサーバに登録する方法を説明します。

3.2.　公開鍵のサーバ登録

公開鍵認証を行うには、接続先サーバのログインするユーザのホームディレクトリ以下の所定ファイル(.ssh/authorized_keys)に公開鍵を登録する必要があります。ssh-copy-id というコマンドで公開鍵を登録することができます。ssh-copy-id コマンドの書式は以下のとおりです。

```
ssh-copy-id -i 公開鍵ファイル 接続先ユーザ名@接続先ホスト名
```

ここでは公開鍵を登録する方法を説明します。コマンドを実行する際に登録先サーバのパスワードの入力が求められます。ここでは「cc 環境のパスワード」を入力してください。

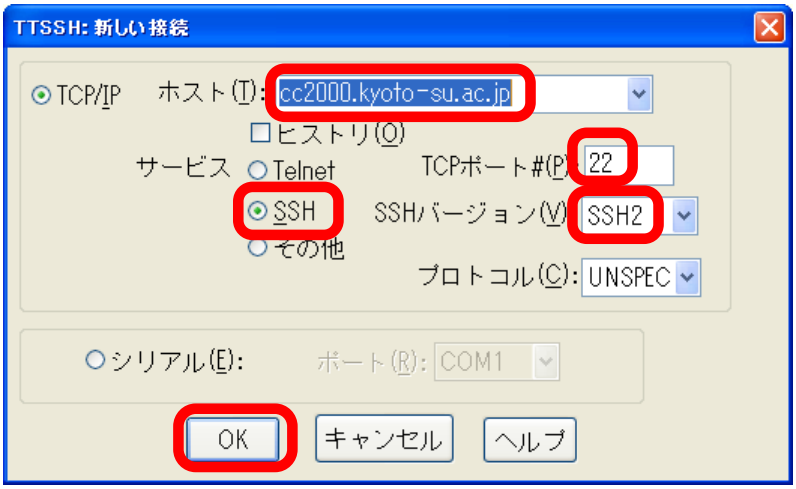
```
$ ssh-copy-id -i ~/.ssh/id_dsa.pub sandai@cc2000
Password:　　←　cc 環境のパスワードを入力してください
Now try logging into the machine, with "ssh 'cc2000'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

これで公開鍵の登録が完了しました。それでは次項で実際に公開鍵を使用して cc2000 にログインできるか確認してみましょう。

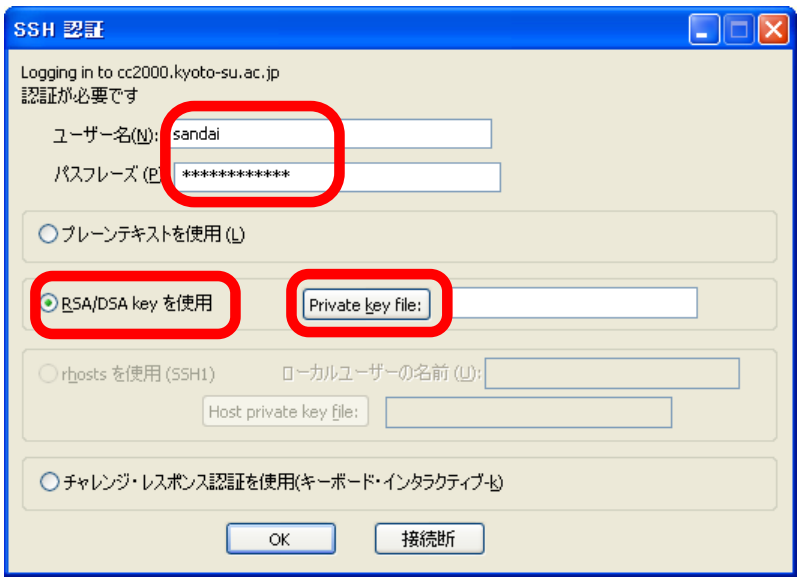
4. 公開鍵認証によるログイン方法

この項では、３の項で作成・保存した公開鍵と秘密鍵を用いた、公開鍵認証によるログイン方法について説明します。ここでは TeraTerm を使用し、cc2000 に「sandai」というユーザ ID で、公開鍵認証でログインする方法を説明します。

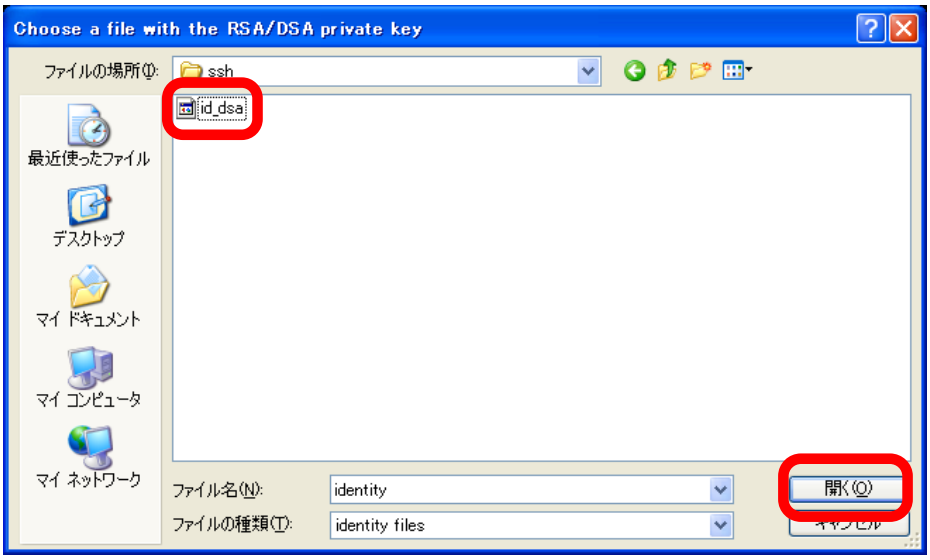
1) TeraTerm を起動して、「新しい接続」画面を表示します。ホストに「cc2000.kyoto-su.ac.jp」、サービスは「SSH」、TCP ポートは「22」、SSH バージョンは「SSH2」にそれぞれ設定します。それ以外の部分は初期値のままで結構です。設定を確認後、「OK」ボタンをクリックします。



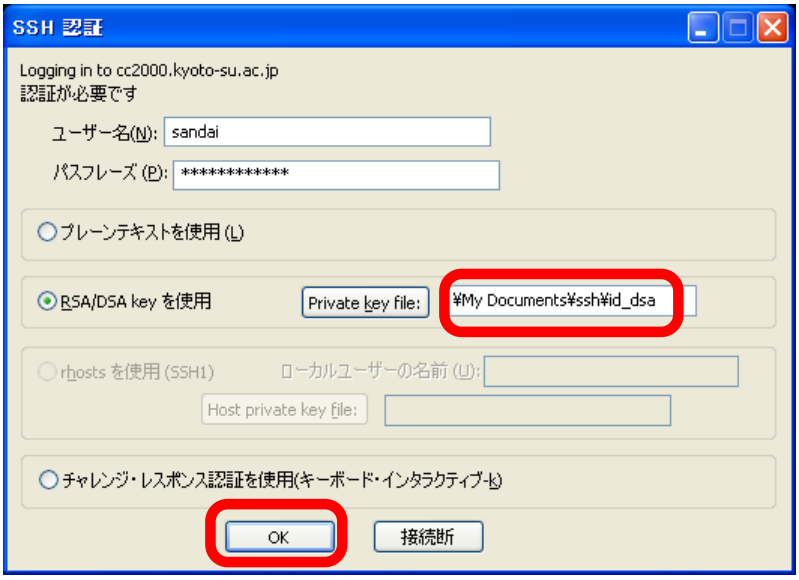
2) SSH で接続するための設定をします。「ユーザ名（cc 環境のユーザ ID)」、「パスフレーズ（鍵作成時に設定したパスフレーズ)」を入力します。次に「RSA/DSA key を使用」にチェックを入れ「Private key file:」ボタンをクリックします。



3)　３の項で作成した秘密鍵「id_dsa」を選択し、「開く」ボタンをクリックします。



4)　「ユーザ名」「パスフレーズ」「Private key file:」を再確認して「OK」ボタンをクリックします。



5)　以上で公開鍵認証が行われ、ログインが完了します。ログイン後はパスワード認証時と同じ操作で利用できます。