作成：平成 19 年 5 月 8 日
修正：平成 29 年 3 月 1 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、学内ネットワークからの接続に限り、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。また、何らかの理由でパスワードが第三者に知られてしまうと、不正アクセスの被害を受ける可能性があります。

これらの理由により、本学では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利用する場合は「パスワード認証」によるユーザ認証を禁止しており、「公開鍵認証」によるユーザ認証で接続する必要があります。

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。

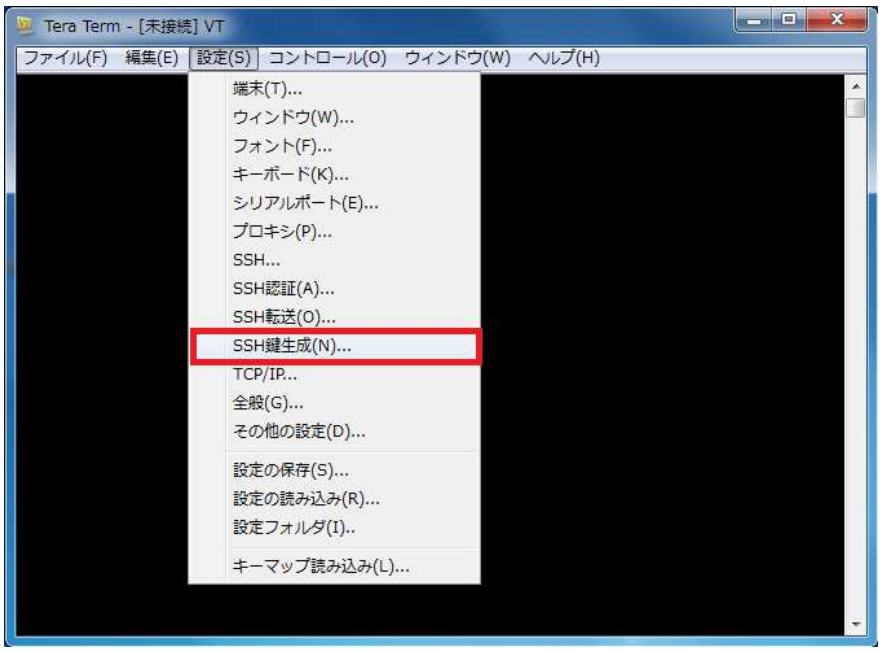
3. 公開鍵と秘密鍵の作成方法

公開鍵と秘密鍵の作成方法にはいくつかありますが、ここでは本学の情報処理教室等で利用できる Windows クライアントにインストールしている TeraTerm を利用します。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。

3.1. 公開鍵と秘密鍵の作成

1. 共通アプリケーションにある「TeraTerm」を起動すると、下記のウインドウが表示されるのでキャンセルを押します。

2. 「設定」から「SSH 鍵生成」を選択します。



3. 鍵の種類を「RSA」、ビット数を「2048」にして生成ボタンを押します。

4. 鍵のパスフレーズを入力して、公開鍵を保存します。公開鍵の保存は任意の場所で結構ですが、このあと保存する秘密鍵とセットにしておくと良いでしょう。

5. 秘密鍵を保存します。秘密鍵はUSBメモリ等に保存し、家に持ち帰ることができるようにしておくとよいでしょう。**秘密鍵はむやみにコピーせず、オンラインストレージ等に保存したり、他人に渡したりしないよう、厳重に管理してください。**

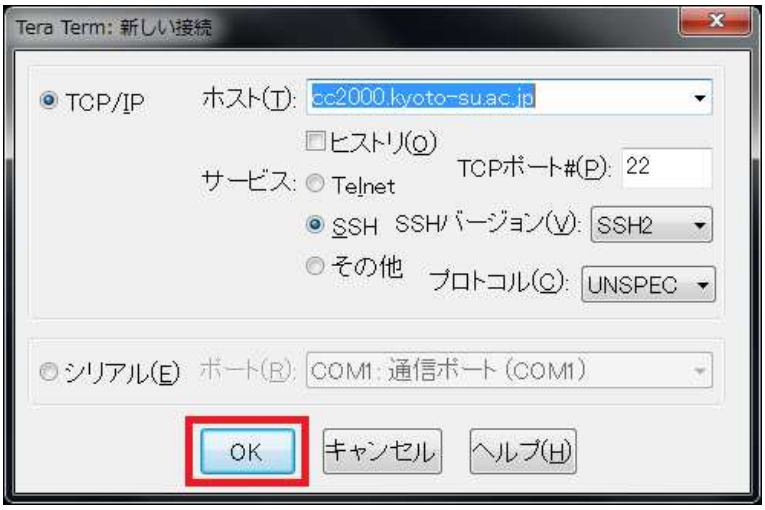
秘密鍵が保存できたら、閉じるボタンを押してウインドウを終了します。

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。

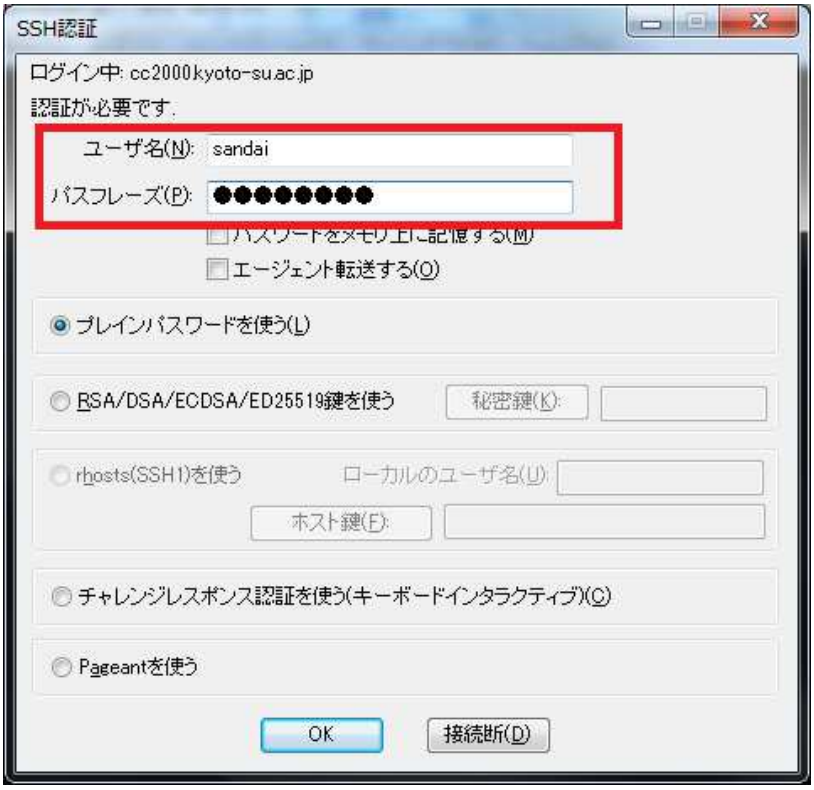
3.2. 公開鍵のサーバ登録

公開鍵認証を行うには、接続するサーバの自身のユーザ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。下記の手順に沿って進めてください。登録は**学内ネットワークに接続した端末で実施します。**

1. TeraTerm を起動し、接続先サーバを確認して OK を押します。



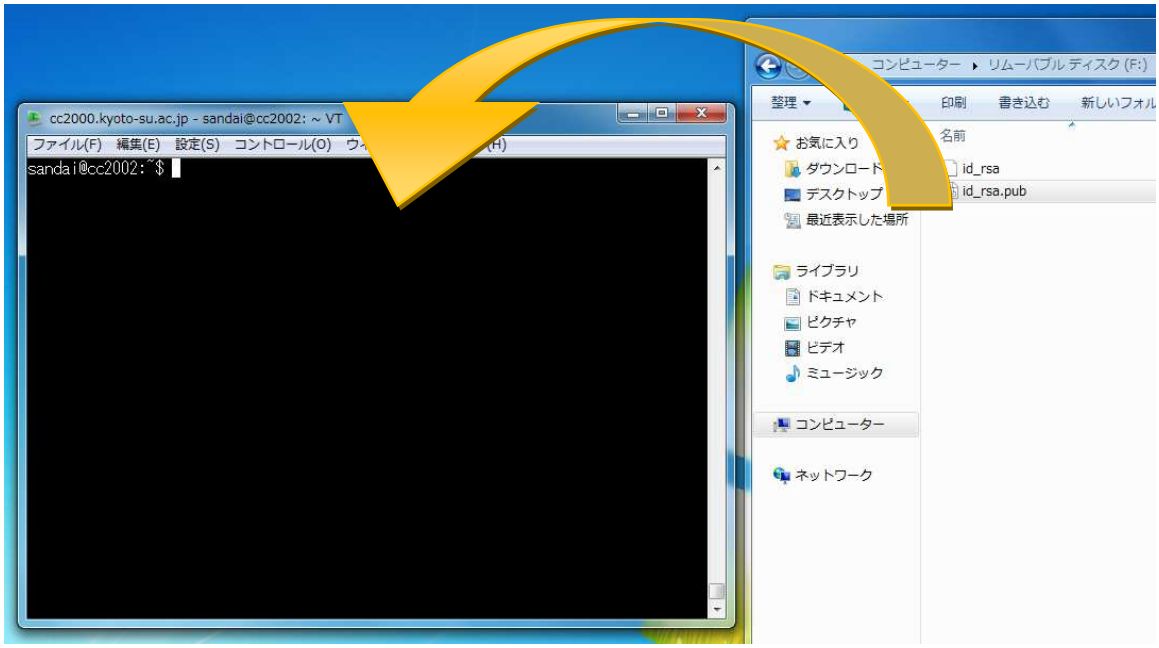
2. 「ユーザ名（本学ユーザ ID）」、「パスフレーズ（**POST にログインする際のパスフレーズ**）」を入力します。



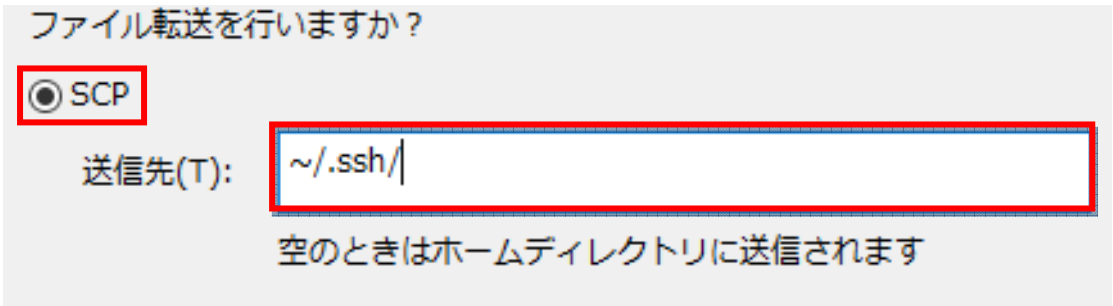
3. ログインができたら先ほど作成した公開鍵を cc2000 に設置します。まずは設置するための場所を作成します。下記の通りにコマンドを実行してください。
※「~/.ssh」が既に存在している場合は、このステップは不要です。

```
$ mkdir ~/.ssh
$ chmod 700 ~/.ssh
```

4. 公開鍵の「id_rsa.pub」を TeraTerm にドラッグ＆ドロップします。



5. コピー先を指定するダイアログが表示されますので「~/.ssh/」と入力し、「SCP」を押します。（ssh の前にある「.」をつけ忘れないようお願いします。）



6. 公開鍵を登録します。下記のコマンドを実行してください。

```
$ cd ~/.ssh
$ cat id_rsa.pub >> authorized_keys
$ chmod 600 authorized_keys
$ rm id_rsa.pub
$ exit
```

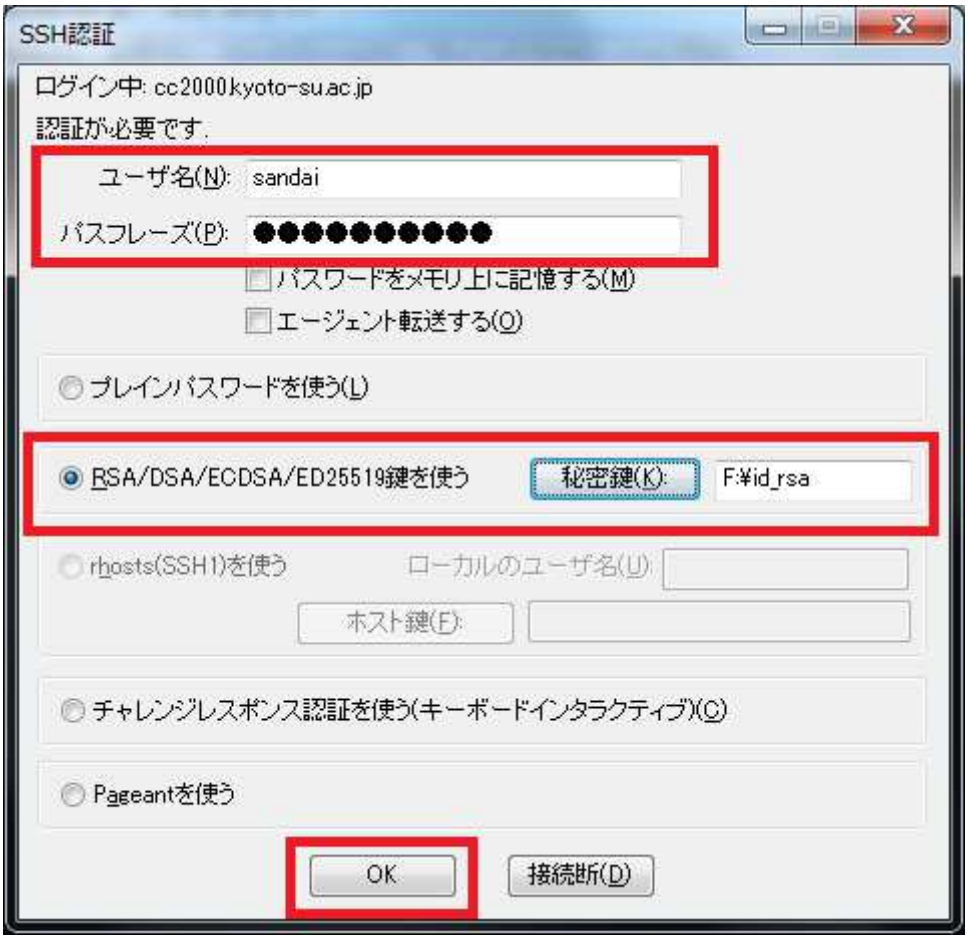
※exit を入力すると TeraTerm が終了します。

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、接続先サーバを確認して OK を押します。

2. 「ユーザ名（本学ユーザ 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/ECDSA/ED25519 鍵を使う」にチェックを入れ「秘密鍵」ボタンをクリックし、作成した秘密鍵を選択し、OK を押します。



3. 以上で公開鍵認証が行われ、ログインが完了します。