［大規模科学計算システム］

SSH アクセス認証鍵生成サーバの利用方法

共同利用支援係　共同研究支援係

1. はじめに

大規模科学計算システムでは、セキュリティ強化のため、パスワード認証によるログインを廃止し、公開鍵暗号方式によるログインのみ許可しています※1。SSH アクセス認証鍵生成サーバ（以下、鍵サーバ）はセンターに SSH アクセスするために必要な公開鍵と秘密鍵のペアを生成し、ユーザのホームディレクトリに公開鍵を自動登録するサーバです。本稿では、その利用方法についてご紹介します。

表 1　各ホストのログイン認証方式

ログインホスト名	認証方式	利用システム
front.cc.tohoku.ac.jp	公開鍵	スーパーコンピュータ SX-ACE 並列コンピュータ LX 406Re-2
file.cc.tohoku.ac.jp		データ転送サーバ
―	パスワード※2	利用者端末 大判カラープリンタ 三次元可視化システム

※1：HPCI 課題、JHPCN-HPCI 課題で利用する場合は GSI 認証でのログインも可能です。詳しくは、以下のリンク先の「HPCI ログインマニュアル」をご覧ください。
http://www.hpci-office.jp/pages/hpci_info_manuals

※2：センター内施設（利用者端末・大判カラープリンタ・三次元可視化システム）は、ローカルログインのため、パスワード認証でご利用いただけます。利用にあたり、秘密鍵を持参する必要はありません。

2. 公開鍵暗号方式を使用する上での注意事項

以下のような行為は、不正アクセスのリスク（不正ログイン、クライアントのなりすまし、暗号化された通信の暴露、他サーバへの攻撃等）が非常に高く、大変危険です。ご注意願います。

- パスフレーズなしの秘密鍵を使用
- 秘密鍵、パスフレーズの使い回し
- 秘密鍵のメールへの添付、USB メモリやホームディレクトリへの保存
- 公開鍵と秘密鍵のペアを同一ノード上に保存

3. SSH アクセス認証鍵の生成

利用者番号の発行日から 60 日経過後、または鍵を生成すると、鍵サーバへのログインが自動的にロックされます。一度ログアウトすると、以降は鍵サーバにはログインできなくなりますのでご注意ください。鍵の再登録が必要になった場合は共同利用支援係までご連絡下さい。本人確認の上、ロックを解除します。

(1) 鍵サーバに利用者番号と初期パスワード（変更している場合は変更後のパスワード）で SSH 接続します。

SSH アクセス認証鍵生成サーバ

```
key.cc.tohoku.ac.jp
```

リスト 1　鍵サーバへの SSH 接続例

```
localhost$ ssh 利用者番号@key.cc.tohoku.ac.jp
利用者番号@key.cc.tohoku.ac.jp's password: パスワードを入力
（初回接続時のメッセージ）：yes を入力

key$（コマンド待ち状態）
```

(2) 以下のコマンド（cckey-gen）を実行し、メッセージに従って公開鍵と暗号鍵の鍵ペアを作成します。必ずパスフレーズ（8 文字以上）を設定して鍵を作成してください。

リスト 2　公開鍵と暗号鍵の作成方法

```
key$ cckey-gen
Enter passphrase(8 or more characters)：パスフレーズの入力（必ず設定）
Enter same passphrase again: 同じパスフレーズを再度入力

（生成された秘密鍵の表示）
'利用者番号' registration is completed.
RSA private key is as follws.

8<--------------8<--------------8<--------------8<--------------
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,A3C27C703A6DF938

gp5U3M6wVIvuGLX8OtYBAWC3WwNzX9TPu8eOCA9Pd/i6ijSNcVKp7lGJtuRzjfXV
   （中略）
FSwfyL63gRqxPZEmlcZzfDnhyX7ezdNNveZu37U/nq4TQj9+Q+RWHhjF9jwnuW6F
-----END RSA PRIVATE KEY-----
8<--------------8<--------------8<--------------8<--------------
```

(3) 画面に表示された秘密鍵（---BEGIN RSA PRIVATE KEY--- から ---END RSA PRIVATE KEY--- まで）をコピー&ペーストし、ローカル PC にテキストファイルとして保存します。公開鍵は自動的にユーザのホームディレクトリに登録されます。秘密鍵はセキュリティを考慮して消去されます。

4.　公開鍵暗号方式によるログイン方法

4.1　Linux/OS X のターミナルソフトから接続する方法

生成された秘密鍵をファイル名「id_rsa_cc」として「~/.ssh/」以下に保存した場合

(1) パーミッションを 600 に変更します。(初回のみ)

リスト 3　パーミッションの変更

```
localhost$ chmod 600 ~/.ssh/id_rsa_cc
```

(2) i オプションで使用する秘密鍵を指定して SSH 接続を行います。
(i オプションを省略した場合は ~/.ssh/id_rsa あるいは ~/.ssh/id_dsa が利用されます)

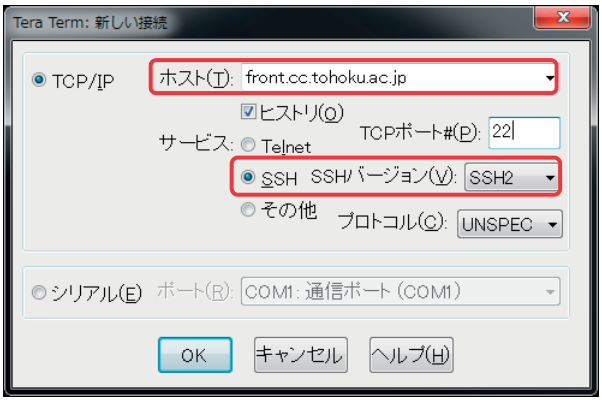
リスト 4　ログインホストへの SSH 接続例

```
localhost$ ssh -i ~/.ssh/id_rsa_cc 利用者番号@front.cc.tohoku.ac.jp
Enter passphrase for key '/home/localname/.ssh/id_rsa_cc':パスフレーズを入力
（初回接続時のメッセージ） : yes を入力
front$ （コマンド待ち状態）
```

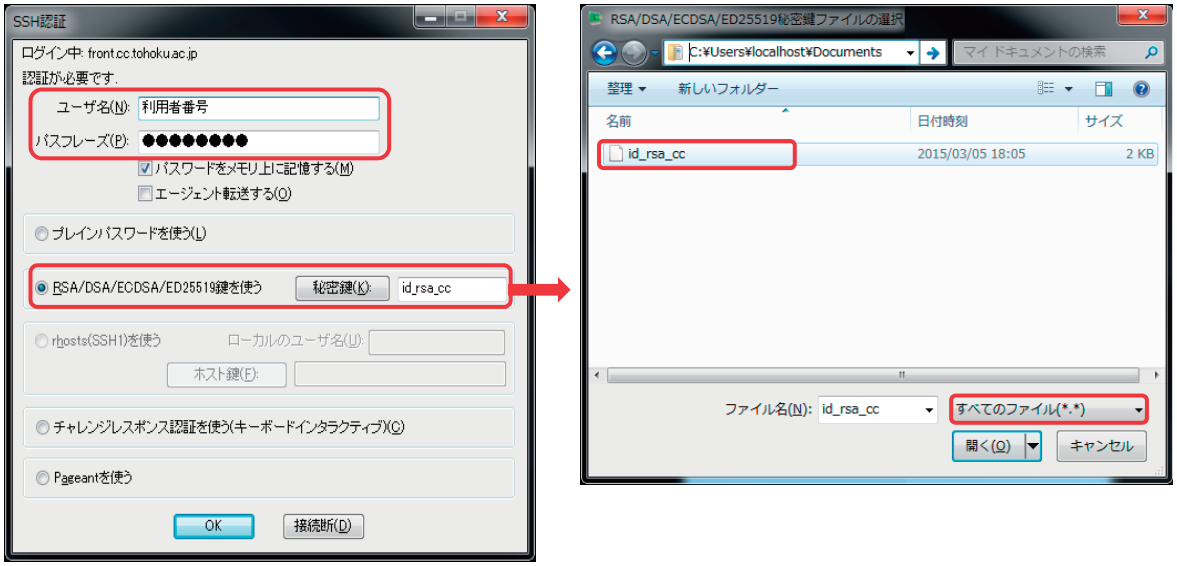
4.2 Windows の Tera Term から接続する方法

生成された秘密鍵をファイル名「id_rsa_cc」として「ドキュメント」以下に保存した場合

(1) 「ホスト名」を指定、「サービス」は SSH2 を選択し、[OK]を押下します。



(2) 「ユーザ名」に利用者番号、「パスフレーズ」に鍵ペアを作成した際に入力したものを入力、「RSA/DSA 鍵を使う」を選択し、「秘密鍵」に保存した秘密鍵のファイルを指定します。
(秘密鍵ファイルの選択画面では、拡張子「すべてのファイル(*.*)」を選択します)
[OK]を押下すると接続されます。



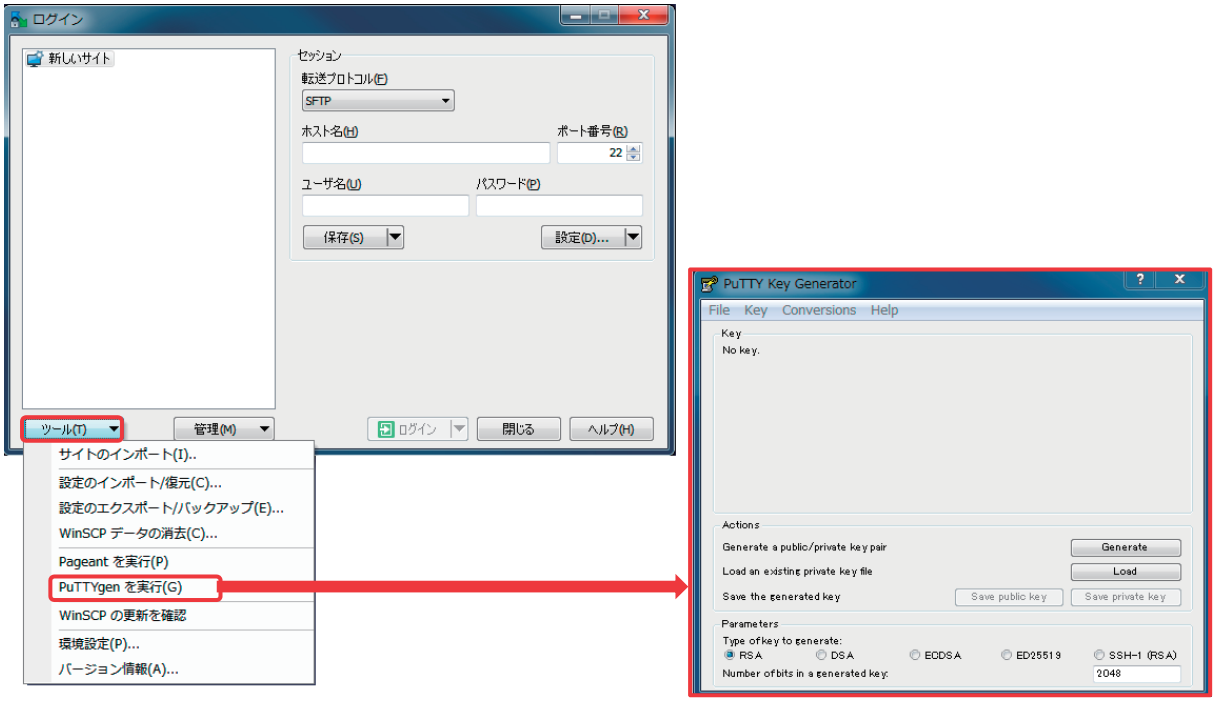
4.3 Windows の WinSCP から接続する方法

WinSCP から接続する場合は、PuTTY 形式の秘密鍵を用意する必要があります。初回接続時は、4.3.1 の手順に従い、鍵サーバで生成した秘密鍵を PuTTY 形式に変換してください。

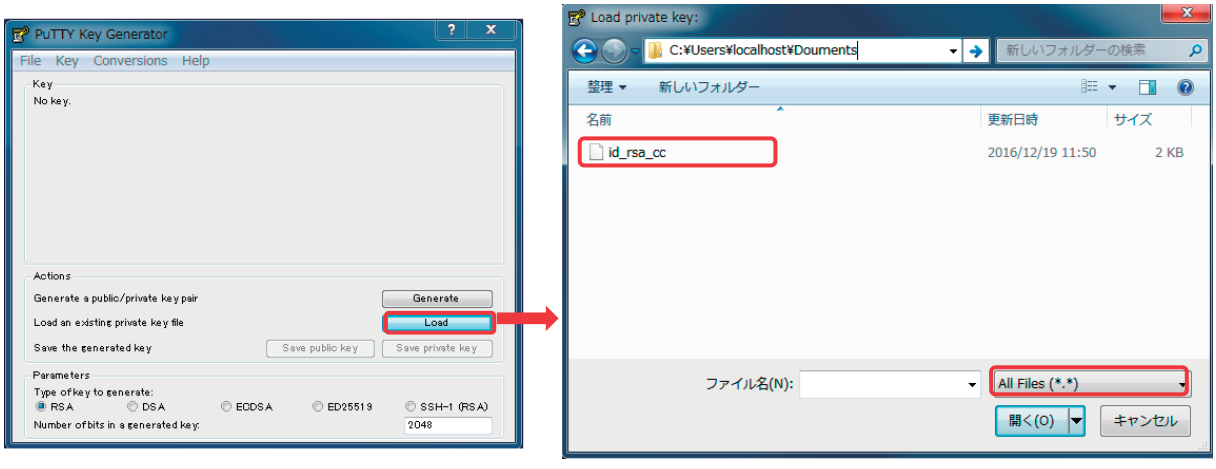
4.3.1 秘密鍵を PuTTY 形式に変換

鍵サーバで生成した秘密鍵をファイル名「id_rsa_cc」として「ドキュメント」以下に保存した場合

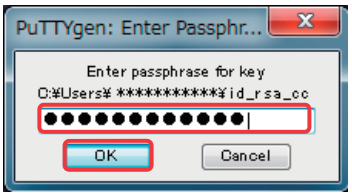
(1) WinSCP のログイン画面から WinSCP 付属の鍵生成プログラム「PuTTYgen」を起動します。
([ツール] 押下→[PuTTYgen を実行] を押下)
PuTTYgen がインストールされていない場合はインストールが必要です。



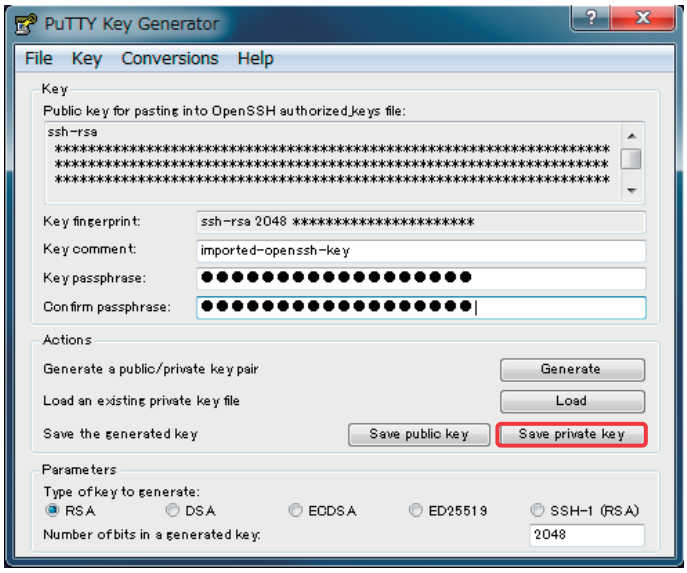
(2) [Load]を押下し、鍵サーバで生成した秘密鍵ファイルを選択して[開く]を押下します。
(秘密鍵ファイルの選択画面では、拡張子「All Files(*.*)」を選択します)



(3)　鍵サーバで生成した秘密鍵のパスフレーズを入力し、[OK]を押下します。



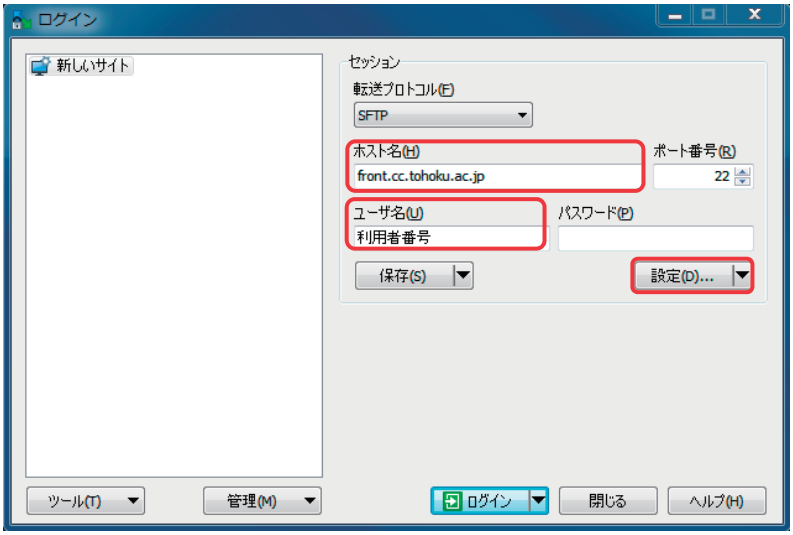
(4)　[Save private key]を押下すると、PuTTY 形式に変換された秘密鍵が保存されます。
（保存先／ファイル名は任意。拡張子は.ppk を推奨）



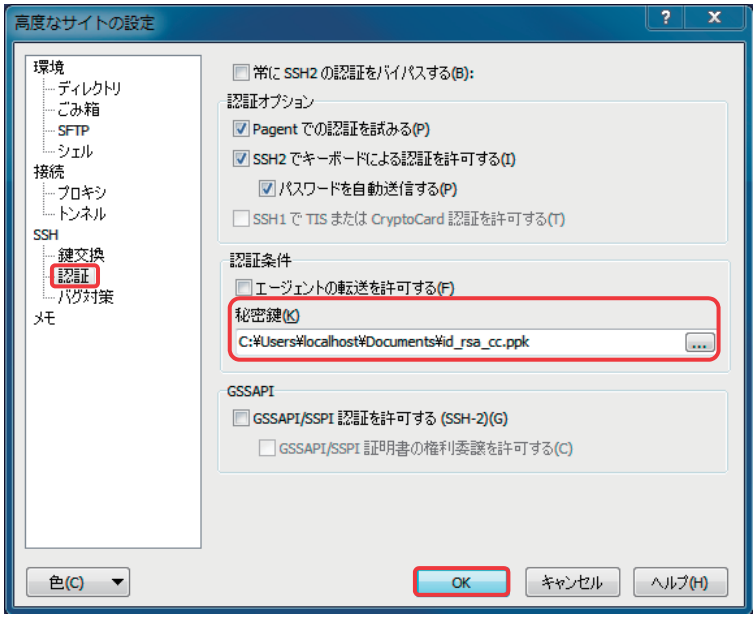
4.3.2　ログイン方法

PuTTY 形式の秘密鍵をファイル名「id_rsa_cc.ppk」として「ドキュメント」以下に保存した場合

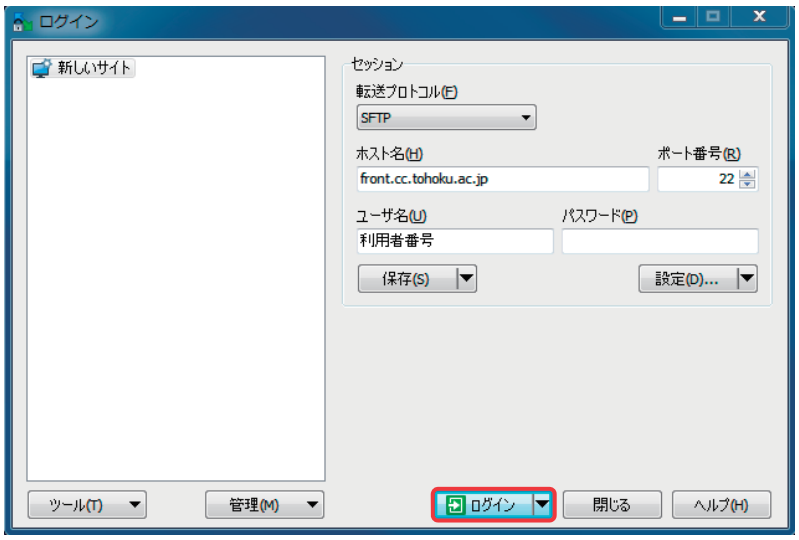
(1)　「ホスト名」を指定、「ユーザ名」に利用者番号を入力し、[設定]を押下する。



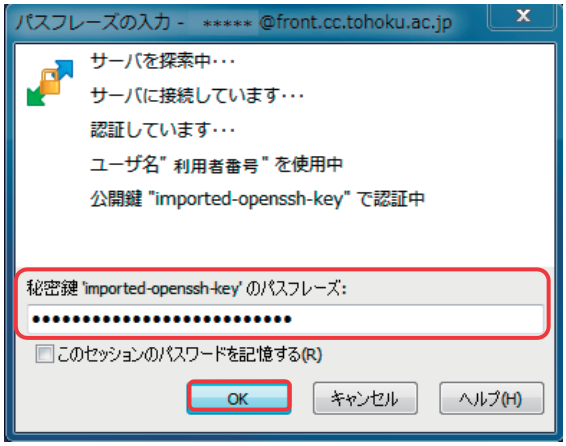
(2) 「SSH」→「認証」を選択し、「秘密鍵」に PuTTY 形式の秘密鍵のファイルを指定して[OK]を押下します。



(3) [ログイン]ボタンを押下します。



(4) パスフレーズを入力し、[OK]押下すると接続されます。



4.4　その他の OS／アプリケーションから接続する場合

各アプリケーションのヘルプを参照ください。

5.　おわりに

本稿では、SSH アクセス認証鍵生成サーバの利用方法を紹介しました。ご不明な点、ご質問等ございましたら、お気軽にセンターまでお問い合わせください。