

[大規模科学計算システム]

鍵ペアの作成とログイン方法

情報部情報基盤課 共同研究支援係 共同利用支援係

1. はじめに

本センターのシステムは、セキュリティ対策として、公開鍵認証方式による SSH 接続を採用しています。また、フロントエンドサーバは、ログインサーバを経由しなければログインできない構成としています。

本稿では、公開鍵認証方式で使用する鍵ペアの作成と各サーバのログイン方法についてご紹介します。解説では以下のターミナルソフトを使用する例をご紹介します。

(Windows の場合) Windows PowerShell
 (macOS/Linux の場合) ターミナル

本センターのシステムをはじめて利用する方は、以下の手続きが必要です。

- (1) 利用者番号の取得 (利用申請 : <https://www.ss.cc.tohoku.ac.jp/apply-for-use/>)
- (2) 鍵ペアの作成 (4 章)

以前のシステムを利用していた方は、(1)(2)の手続きは不要です。以前使用していた利用者番号および鍵ペアをそのままご利用いただけます。5 章からお読みください。

2. ログイン認証方式

表 1 に、各サーバのログイン認証方式を示します。

表 1 各サーバのログイン認証方式

サーバ名	用途	ログインホスト名	認証方式
ログインサーバ	フロントエンドサーバの入口 (踏み台サーバ)	login.cc.tohoku.ac.jp	公開鍵
フロントエンドサーバ	計算機の利用 (コンパイル、ジョブ実行、等)	(※1)	公開鍵またはパスワード
データ転送サーバ	ストレージシステムとの大容量のデータ転送	file.cc.tohoku.ac.jp	公開鍵
HPCI 用ログインノード	HPCI、HPCI-JHPCN ユーザ専用ログインノード	hpcif.cc.tohoku.ac.jp	公開鍵
-	センター内施設の利用(※2)	-	パスワード

(※1) フロントエンドサーバは、ログインサーバからしかログインできません。本稿では多段 SSH による接続方法を解説します。

(※2) 本センター内の施設（大判カラープリンタ、利用者端末、講習会端末）はパスワード認証を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。

3. 鍵ペアの作成からログインまでの流れ

図 1 に、鍵ペア作成からログインまでの流れを示します。①は 4 章、②③は 5 章で詳しく解説します。

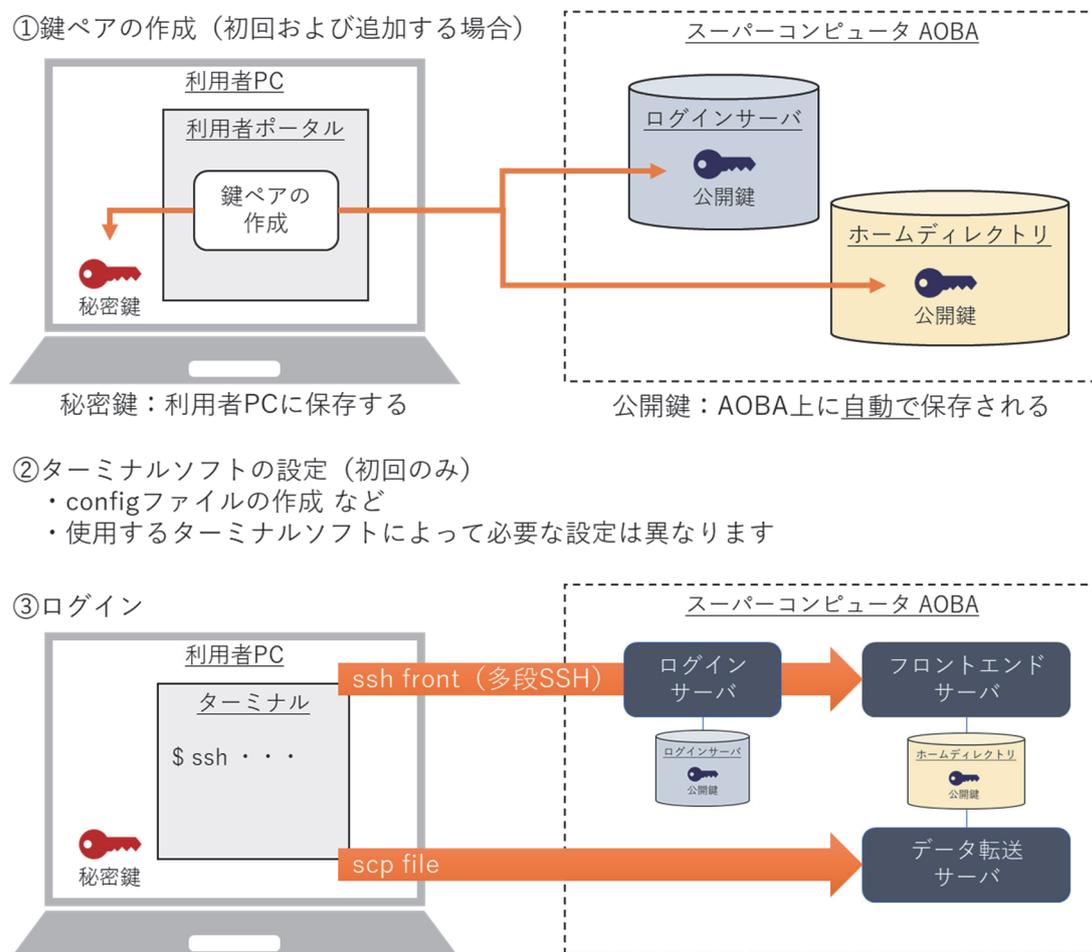


図 1 鍵ペア作成からログインまでの流れ

① 鍵ペアの作成（初回ログイン時、および、ログイン端末を追加する場合）

利用者ポータルで鍵ペアを作成します。作成された秘密鍵は、利用者のローカル PC に保存します。公開鍵は、スーパーコンピュータ AOBA のホームディレクトリ上に自動で保存されます。

② ターミナルソフトの設定（初回ログイン時）

各サーバにログインするための設定を行います。使用するターミナルソフトによって必要な設定は異なります。

③ ログイン

利用者のローカル PC に保存した秘密鍵を使ってログインします。フロントエンドサーバは、ログインサーバを経由して多段 SSH でログインします。

4. 公開鍵認証方式で使用する鍵ペアの作成

4.1. 公開鍵認証方式を使用する上での注意事項

以下の注意事項を必ず守ってください。守らない場合、不正アクセス（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）のリスクが非常に高まり、大変危険です。ご注意ください。

- ・ パスフレーズなしの秘密鍵を使用しないこと
- ・ 秘密鍵、パスフレーズを使いまわさないこと
- ・ 秘密鍵を持ち出さないこと（メールに添付しない、USB メモリ等に保存しない）
- ・ 秘密鍵をスーパーコンピュータ AOBA のホームディレクトリに保存しないこと
- ・ 公開鍵と秘密鍵の鍵ペアを同一ノード上に保存しないこと

4.2. 鍵ペアの作成（初回ログイン時、および、ログイン端末を追加する場合）

○初回ログイン時

鍵ペアの作成は、利用者ポータルで行います。

(1) 以下の URL 先から利用者ポータルを開きます。

利用者ポータルには、利用者番号とパスワード（※）でログインします。

利用者ポータル：<https://www.ss.cc.tohoku.ac.jp/portal/>

(2) 「SSH 公開鍵登録」ボタンをクリックします。

(3) 利用者ポータルの画面の説明に従い、鍵ペアを作成します。

（パスフレーズを設定し、鍵生成・登録ボタンをクリック）

(4) 作成された秘密鍵を利用者のローカル PC に保存します。保存先は以下を推奨します。

フォルダがない場合は新規作成します。

（Windows の場合） C:¥Users¥ユーザ¥.ssh

（macOS/Linux の場合） ~/.ssh

公開鍵は、ホームディレクトリ（~/ssh/authorized_keys）に自動で保存されます。

※利用者ポータルで使用するパスワードの変更方法は、6 章を参照してください。

○別の PC からログインする場合（ログイン端末を追加する場合）

既存の秘密鍵を使いまわすのではなく、ログイン端末ごとに鍵ペアを作成してください。初回ログイン時と同じ手順で、新しい鍵ペアを追加します。

5. 各サーバのログイン方法

5.1. ターミナルソフトの設定（初回ログイン時）

利用者のローカル PC 上で、ターミナルソフトの設定を行います。

以降の解説は、次のフォルダを「.ssh フォルダ」と呼び、秘密鍵を「id_rsa_cc」というファイル名で.ssh フォルダに保存した場合とします。

（Windows の場合） C:¥Users¥ユーザ¥.ssh

（macOS/Linux の場合） ~/.ssh

各ログインホストのホスト名は、次の文字列で設定するものとして解説します。ホスト名には任意の文字列を設定することができます（他の設定との重複は不可）。他の文字列を設定した場合は、以降の解説におけるホスト名を読み替えてください。

（ログインサーバ） login

（フロントエンドサーバ） front

（データ転送サーバ） file

（HPCI 用ログインノード） hpcif

(1) macOS/Linux の場合は、秘密鍵のパーミッションの変更（600 に設定）が必要です。ターミナルソフトを起動し、以下のコマンドを実行します。

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

以降は Windows、macOS/Linux 共通です。

(2) .ssh フォルダの「config」というファイルをテキストエディタで開きます。ファイルがない場合は新規作成します。拡張子はつけません。

（フォルダの設定を「拡張子を表示しない」にしている場合、意識せずに拡張子付きのファイルを作成している可能性があります。config ファイルに拡張子がついていると、ログインできません。ご注意ください）

(3) config ファイルに以下の設定を記述します。太字下線の部分は、ご自身の環境に合わせて読み替えてください。

○フロントエンドサーバを利用するための設定 (※)

```
# ログインサーバの設定 (ホスト名を”login”とする場合)
Host login                                # ホスト名を指定
HostName login.cc.tohoku.ac.jp           # ログインホスト名を指定
User 利用者番号                          # 利用者番号を指定
IdentityFile ~/.ssh/id_rsa_cc           # 秘密鍵の保存場所とファイル名を指定

# フロントエンドサーバの設定 (ホスト名を”front”とする場合)
Host front
HostName front.cc.tohoku.ac.jp
User 利用者番号
ProxyCommand ssh -CW %h:%p login      # login 経由で多段 SSH する設定
IdentityFile ~/.ssh/id_rsa_cc
```

○データ転送サーバを利用するための設定

```
# データ転送サーバの設定 (ホスト名を”file”とする場合)
Host file
HostName file.cc.tohoku.ac.jp
User 利用者番号
IdentityFile ~/.ssh/id_rsa_cc
```

○HPCI 用ログインノードを利用するための設定

```
# HPCI 用ログインノードの設定 (ホスト名を”hpcif”とする場合)
Host hpcif
HostName hpcif.cc.tohoku.ac.jp
User 利用者番号
IdentityFile ~/.ssh/id_rsa_cc
```

(※) Windows の場合、フロントエンドサーバへのログイン時に以下のようなエラーが出る場合があります。

```
$ ssh front
CreateProcessW failed error:2
posix_spawn: No such file or directory
```

エラーが出た場合は次の要領で `config` ファイルを書き換えてください。

[1] ターミナルソフトを起動し、以下のコマンドで `ssh` の絶対パスを調べる。

```
$ gcm ssh
CommandType  Name  Version  Source
-----
Application  ssh.exe  x.x.x  C:¥WINDOWS¥System32¥OpenSSH¥ssh.exe
```

[2] `config` ファイルの「ProxyCommand ssh …」の行の「ssh」の部分、絶対パス ([1] で「Source」に表示された文字列) に書き換える。

```
# 修正前
ProxyCommand ssh -CW %h:%p login
# 修正後
ProxyCommand C:¥WINDOWS¥System32¥OpenSSH¥ssh.exe -CW %h:%p login
```

5.2. フロントエンドサーバのログイン方法

ターミナルソフトを起動し、以下のコマンドを実行するとログインします。ホスト名を別の文字列で設定している場合は「`front`」の部分を読み替えてください。

```
$ ssh front
```

フロントエンドサーバは冗長構成になっており、自動的に `front1` または `front2` が選択されます。どちらにログインしても、動作は変わりません。

なお、フロントエンドサーバでは一定時間以上のプロセスは実行できません。また、大容量のデータ転送はシステムに高い負荷がかかります。大容量のデータ転送を行う場合は、データ転送サーバをご利用ください。

5.3. データ転送サーバの利用方法

データ転送サーバは、ログインして利用するのではなく、利用者のローカル PC 上から `scp` コマンドや `sftp` コマンドで利用します。詳しくは以下をご参照ください。

データ転送 (ストレージ) : <https://www.ss.cc.tohoku.ac.jp/storage/>

5.4. HPCI 用ログインノードのログイン方法

ターミナルソフトを起動し、以下のコマンドを実行するとログインします。ホスト名を別の文字列で設定した場合は「`hpcif`」の部分を読み替えてください。

```
$ ssh hpcif
```

5.5. ログインシェルの確認と変更

ログインシェルは、デフォルトでは `csch` が設定されています。設定の確認および変更は以下の手順で行います。ログインシェルの変更がシステム全体に反映されるまで、15 分程度かかります。

- (1) フロントエンドサーバにログインする。
- (2) 以下のコマンドを実行する。

○ログインシェルの確認

```
front1 $ fchsh (ログインシェルの確認)
Enter Password: (パスワードを入力)
loginShell: /bin/tcsh (現在のログインシェルが表示される)
```

○ログインシェルの変更

```
front1 $ fchsh /bin/bash (ログインシェルを/bin/bashに変更)
Enter Password: (パスワードを入力)
Changed loginShell to /bin/bash (ログインシェルが変更された)
```

6. パスワードの変更

利用者ポータルなどで使用するパスワードの変更は、以下の手順で行います。

- (1) 以下の URL 先から利用者ポータルを開きます。
利用者ポータルには、利用者番号とパスワードでログインします。
利用者ポータル : <https://www.ss.cc.tohoku.ac.jp/portal/>
- (2) 「パスワード変更」 ボタンをクリックします。
- (3) 利用者ポータルの画面の説明に従い、新しいパスワードを設定します。
- (4) 以下で使用するパスワードが変更されます。
 - ・利用者ポータルへのログインパスワード
 - ・大判カラープリンタのプリンタサーバへのログイン
 - ・ログインシェルの変更時のパスワード

7. おわりに

本稿では、鍵ペアの作成とログイン方法についてご紹介しました。センターのシステムを安全にご利用いただければ幸いです。ご不明な点、ご質問等ございましたら、お気軽にセンター（利用相談）までお問い合わせください。

利用相談 : <https://www.ss.cc.tohoku.ac.jp/consultation/>

また、センターからのお知らせは、ウェブサイトにてご確認ください。

センターウェブサイト : <https://www.ss.cc.tohoku.ac.jp/>