SSH鍵作成とログイン
PuTTY 版

自然科学研究機構
岡崎共通研究施設
計算科学研究センター(RCCS)

(PuTTY 0.71 で動作確認)

更新履歴

- 2019/5/28　　初稿作成
- 2019/7/9　　PuTTYgenについての記述を追加

イントロダクション

この資料ではPuTTYと付属ツールを用いてSSH鍵を作成し、
フロントエンドノードへログインする手順を説明します。

目次

- PuTTYのインストール
- SSH鍵の生成
- 公開鍵の登録
- ログイン

PuTTYのインストール

PuTTY は以下のサイトよりダウンロードができます。

https://www.putty.org/

(Download PuTTY の項目にあるリンクへ移動する必要があります)

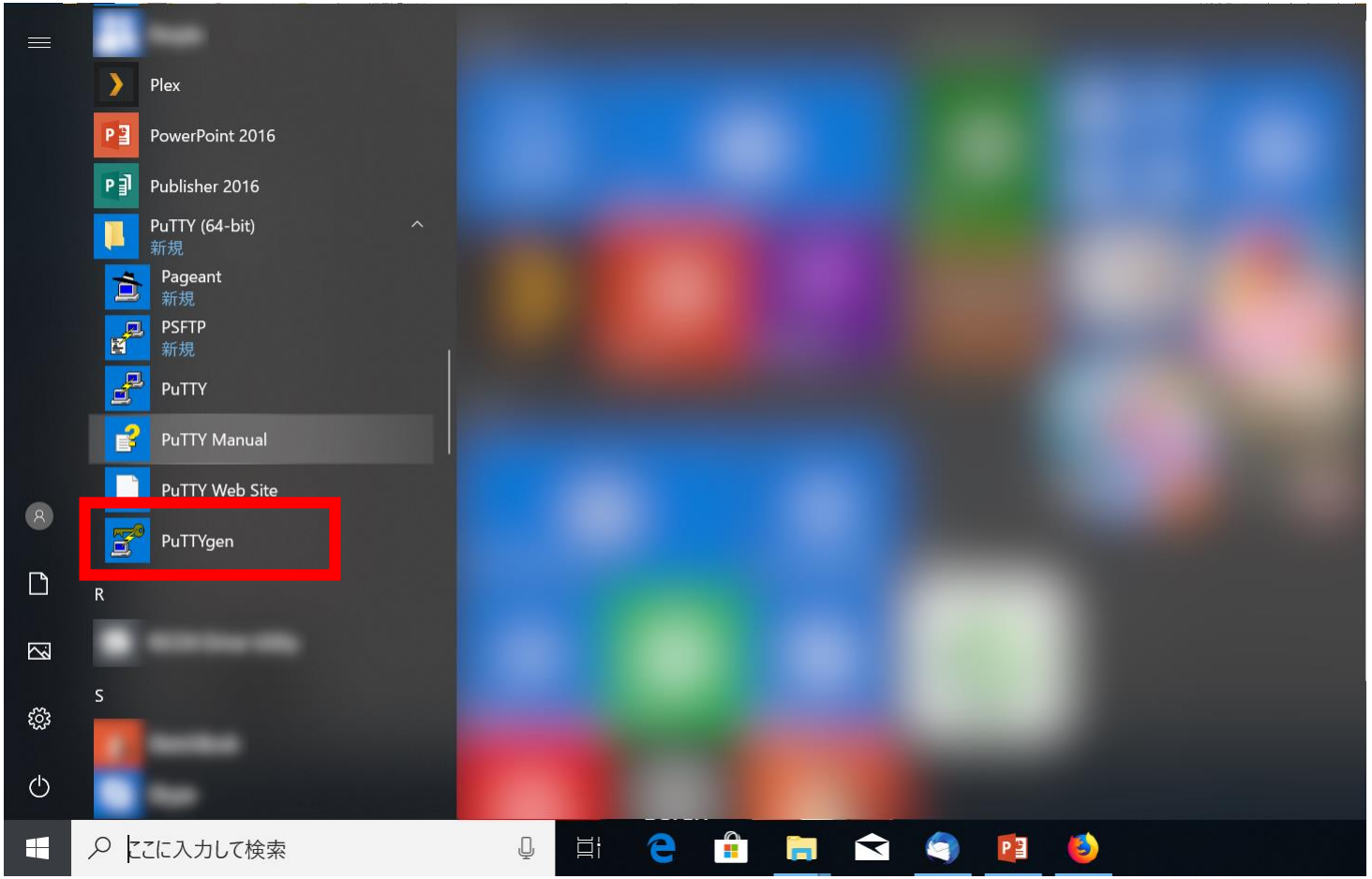
MSI(Windows Installer)版を指示に従ってインストールしてください。

以下では PuTTY および PuTTYgen を利用します。

PuTTYを既にインストール済で PuTTYgen が見つからない場合は、
ダウンロードサイトの Alternative binary files の中から
PuTTYgen (puttygen.exe) を選んでダウンロードしてください。

SSH鍵の作成(1)

PuTTYgen を起動します。
Windows 10 の場合は例えば以下の場所から起動できます。

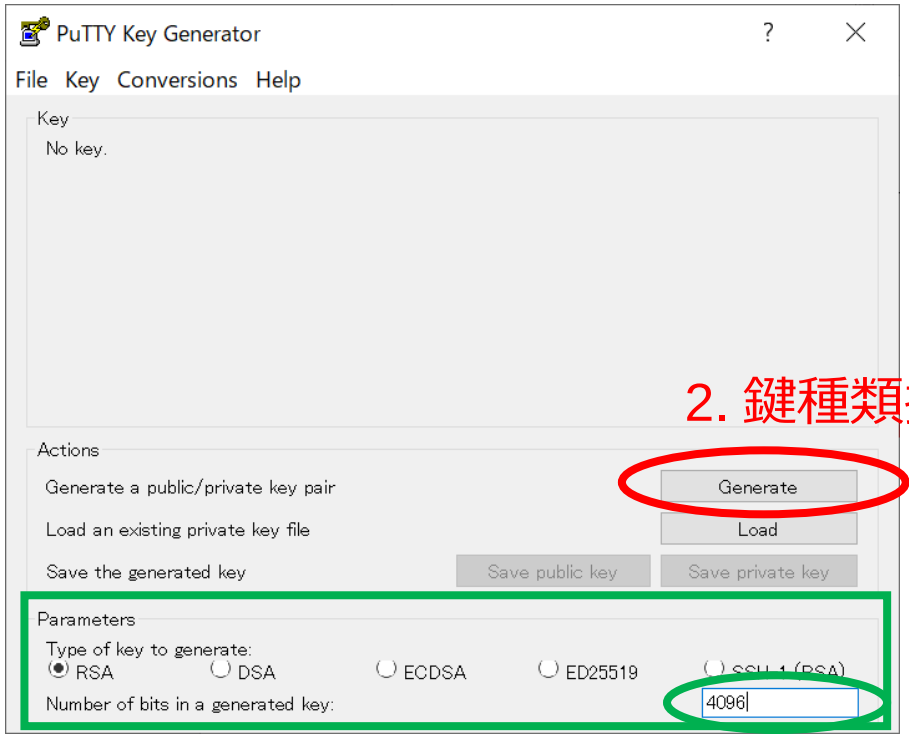


SSH鍵の作成(2)

RCCS では以下のどれかの鍵を推奨しています。

- RSA 4096 ビット (RSA を選択し、右下の数字を 4096 に)
- ECDSA (ビット数 256, 384, 521) または ED25519

良くわからない場合は RSA 4096 ビットをお試しください。



2. 鍵種類指定後クリック

1. 鍵種類の指定

鍵の長さ指定

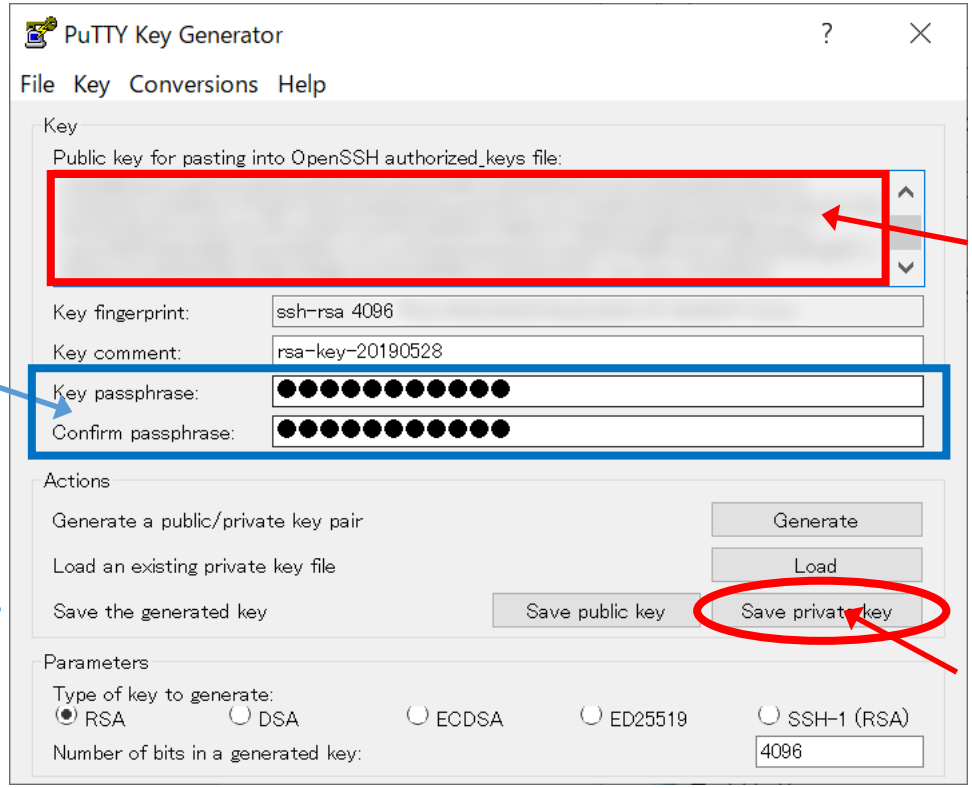
(3. Generate クリック後、マウスを動かさないと先に進みません)

SSH鍵の作成(3)

鍵の生成が終わると以下のような表示になります。

2. RCCS では秘密鍵のパスフレーズには
- 英小文字
- 英大文字
- 数字
- 記号

の4種を含む10文字以上のものを指定するようお願いしています。



1. ログイン用の公開鍵はこちらを使います。
一旦メモ帳などに書き出し、保存することをお勧めします。
(きちんと全体をコピーしてください。)

3. パスフレーズを設定後、ここをクリックして秘密鍵を保存
rccs.ppk や ccfep.ppk のようにわかりやすい名前をつけましょう

- 秘密鍵については他人の触れない場所に保存してください。
- OpenSSH 用の秘密鍵が必要な場合は、Conversions メニューから作成できます
- 公開鍵の保存を忘れた場合も Conversions メニューから鍵を読み込めば復元できます。

公開鍵の登録

実際にログインをする前に生成した公開鍵を
登録する必要があります。

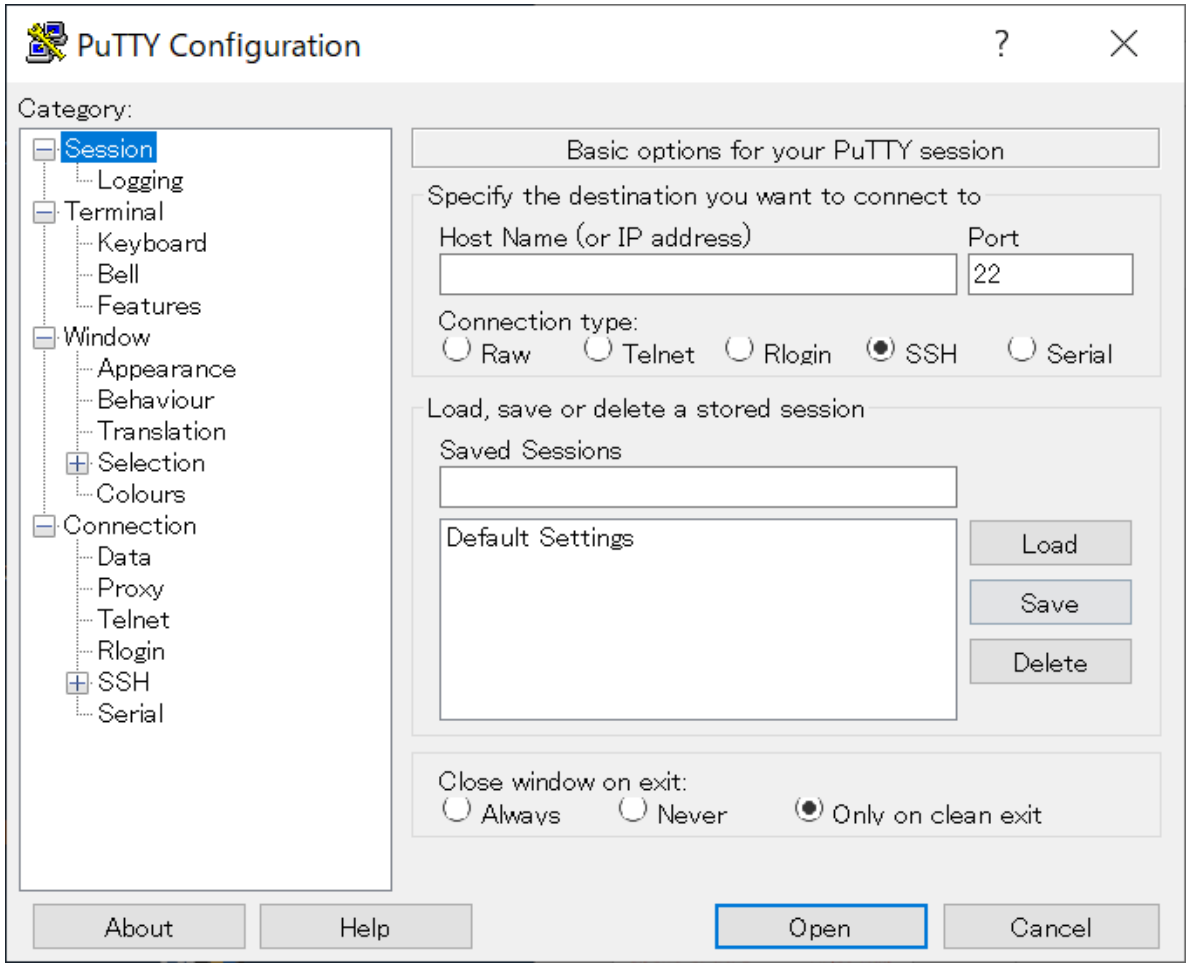
以下のリンクに手順がありますので、
こちらに従って登録して下さい。
https://ccportal.ims.ac.jp/account/

PuTTYgen の 「Save public key」の鍵ではダメです。
画面上部に表示される Public key for pasting into... と
表示されているテキストをコピー & ペースト(もしくは保存したファイルからコピー)してください。

秘密鍵は他人の触れない場所に保存してください。

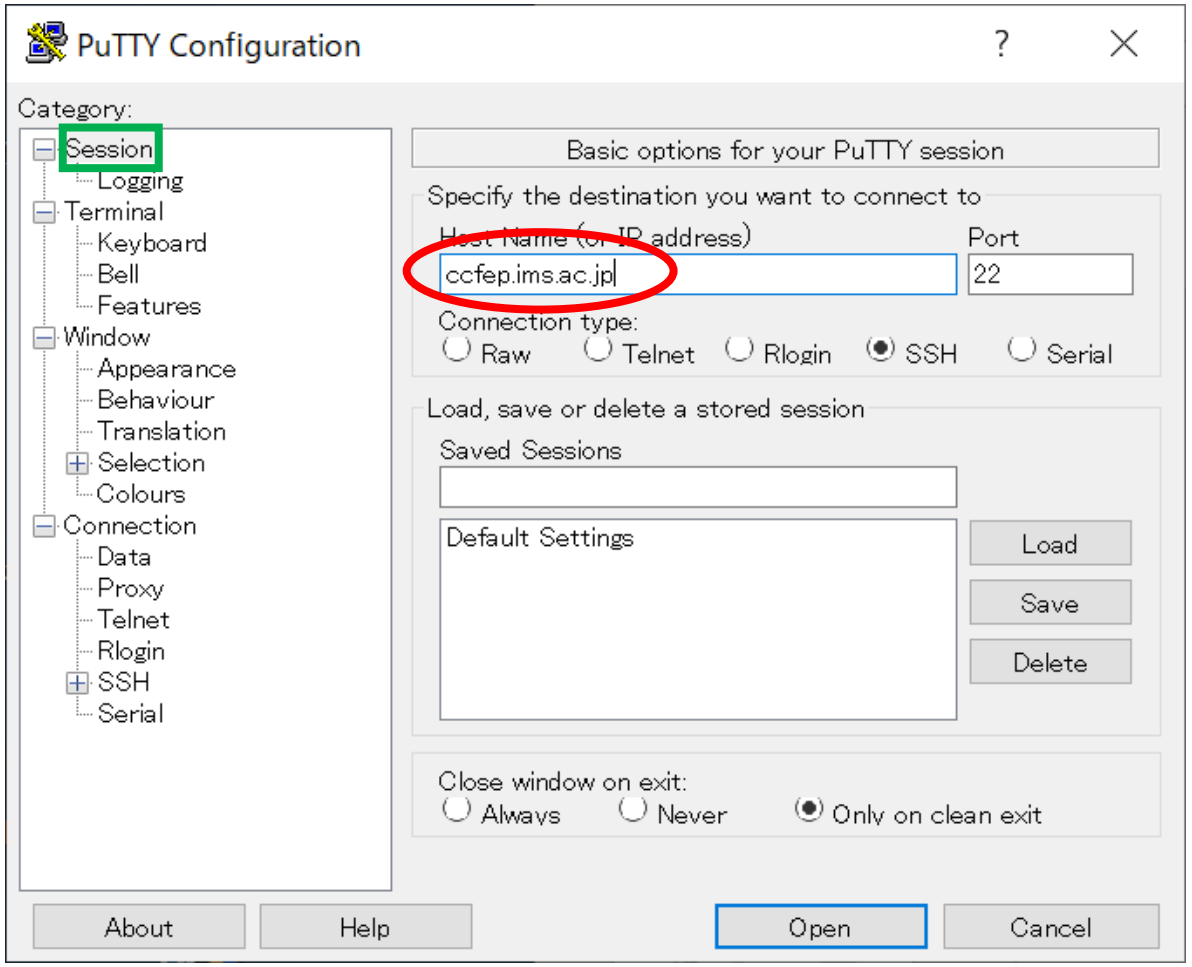
ログイン(1)

それではPuTTYを起動します。



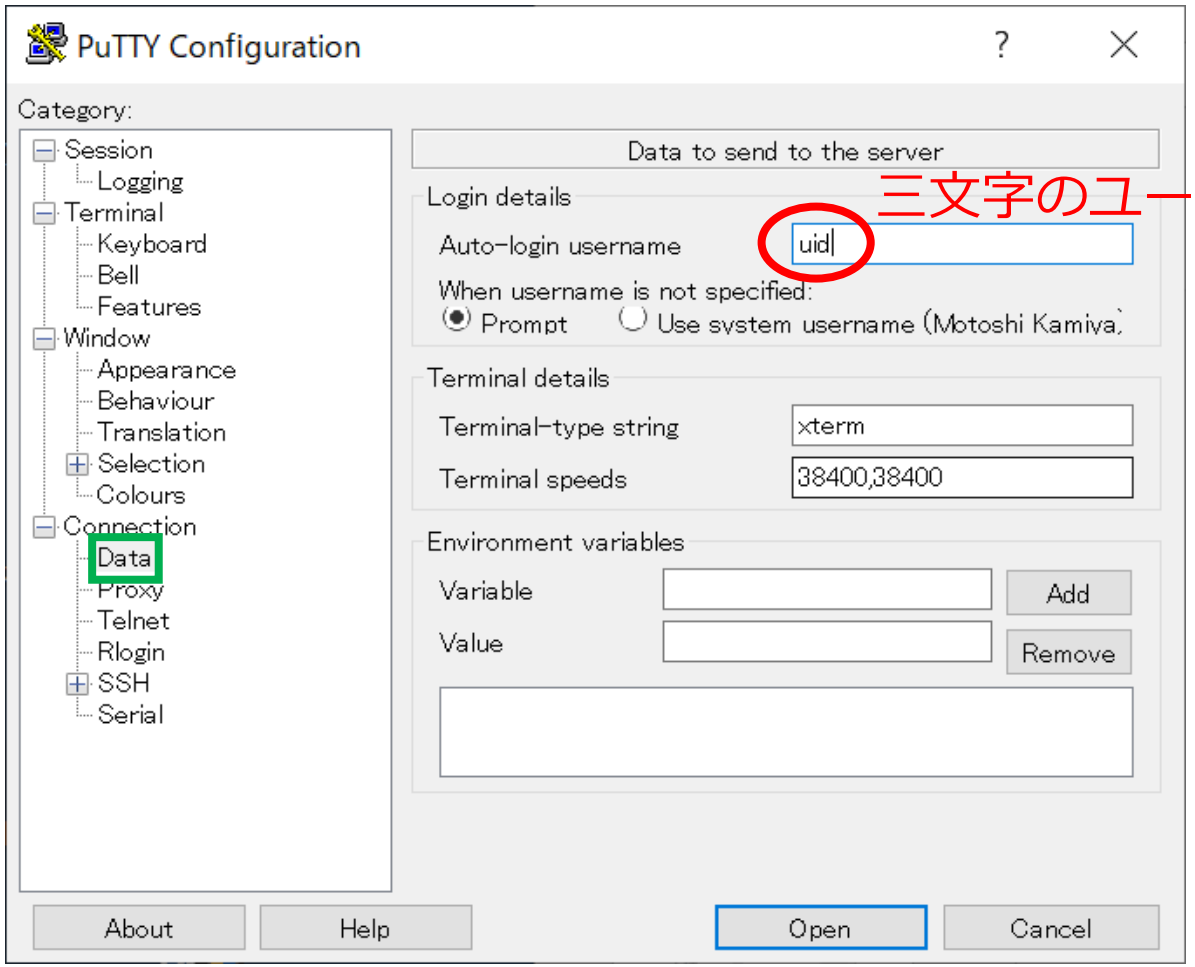
ログイン(2)

「Session」で Host Name に ccfep.ims.ac.jp と入力します



ログイン(3)

Connection -> Data で Auto-login username にユーザ ID 入力

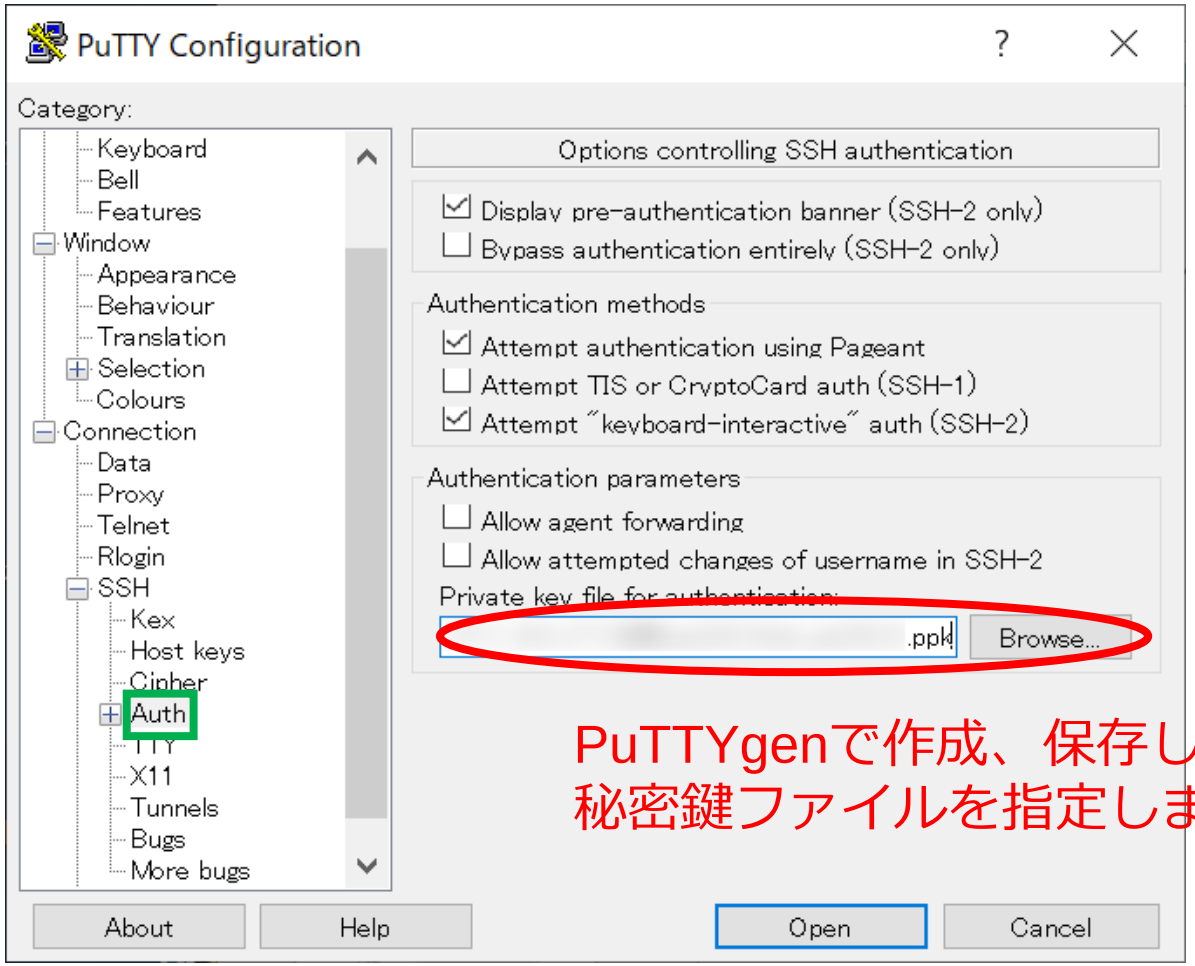


三文字のユーザ ID を入力
(RCCSより指定されたもの)

(このステップは省略できます。省略した場合、接続時に入力することになります。)

ログイン(4)

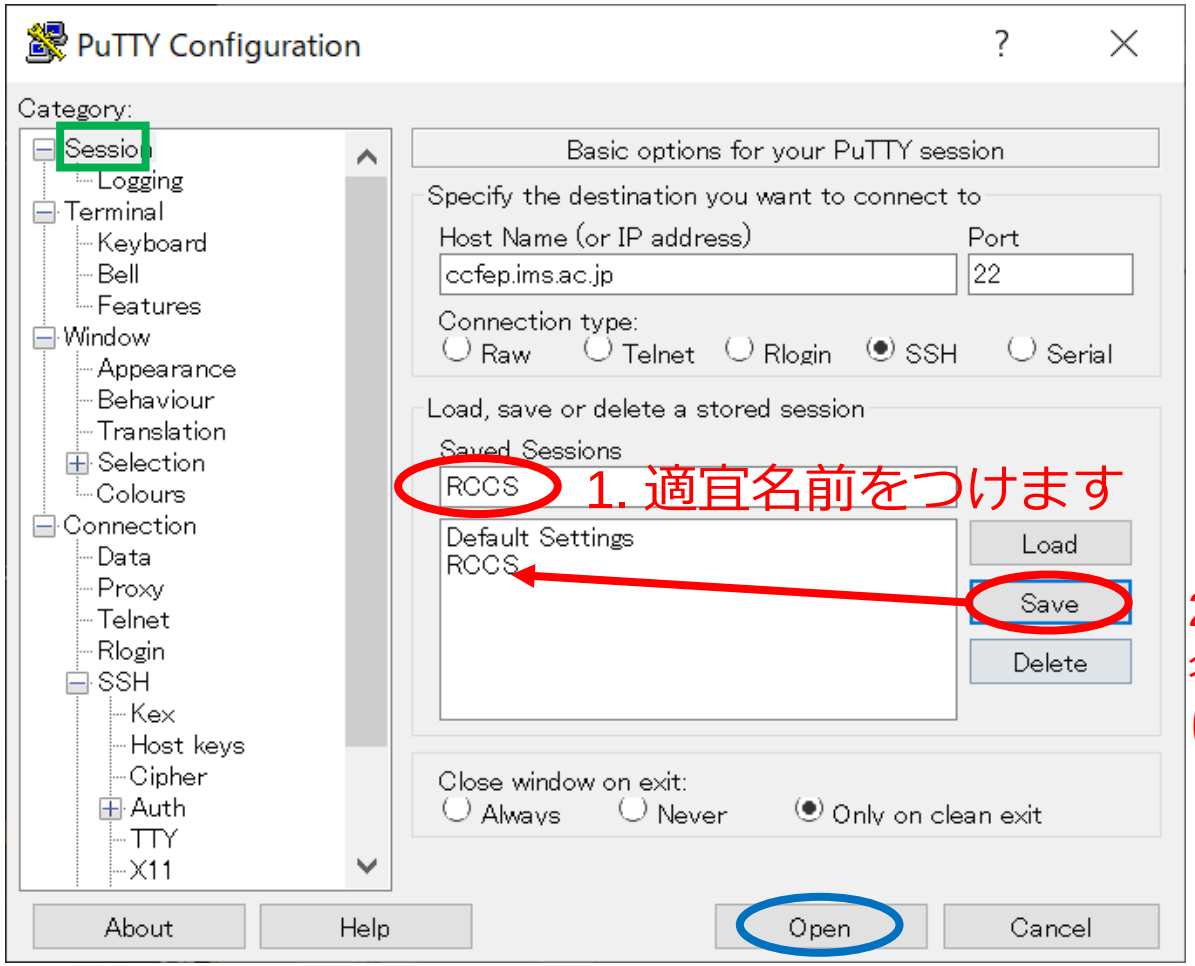
Connection -> Data -> SSH で秘密鍵(.ppkファイル)を指定



PuTTYgenで作成、保存した
秘密鍵ファイルを指定します

ログイン(5)

このまま接続できますが、Session で一旦設定を保存します。

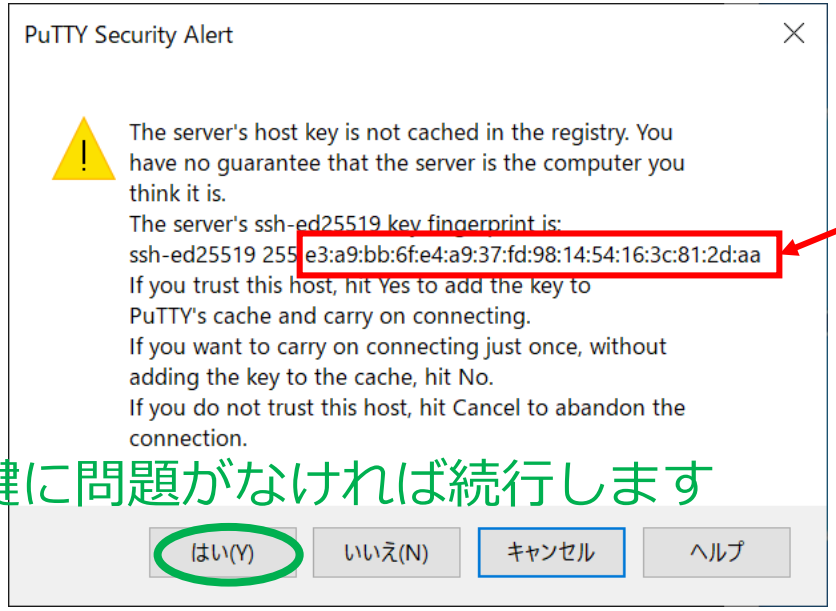


2. 保存すると名前がリストに入ります

3. 保存できたら接続しましょう

ログイン(6)

初回接続時にはまず以下のようなダイアログが表示されます。



1. 表示されるサーバの fingerprint が以下のいずれかと一致していることをお確かめ下さい。

2. 鍵に問題がなければ続行します

有効な鍵の fingerprint

- ad:de:79:30:81:b0:b1:6a:17:f5:6f:ea:f4:b4:3b:de (MD5)
- e3:a9:bb:6f:e4:a9:37:fd:98:14:54:16:3c:81:2d:aa (MD5)
- 07:7e:df:7b:16:47:a8:f5:7c:48:b0:a3:d3:86:71:6a (MD5)

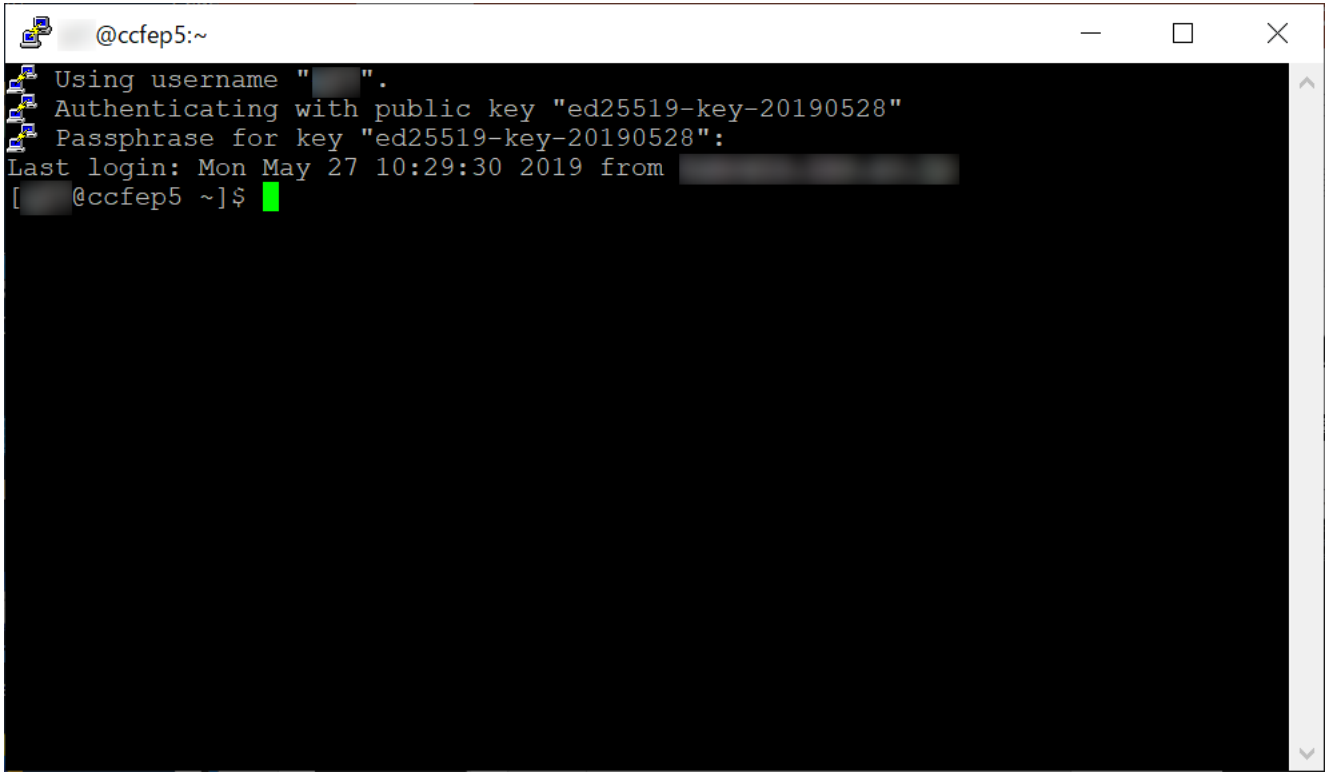
- wnEM30z4AxyDJ9XI/DdGr2PlNeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI (SHA256)
- Nhg+9Lgj3XeuW//A/j7jqgUJlIxWehryCtStIp1Dirs (SHA256)

ログイン(7)

接続すると秘密鍵のパスフレーズを聞かれるので入力します。

ログイン(8)

正しいパスフレーズを入力できれば、以下のようにログインできます。



ヒント：Pageant を起動し、鍵を登録しておけばログインのたびにパスフレーズを聞かれることが無くなります。(Pageant への登録時だけは入力が必要です)