SSH鍵作成(PuTTY版)

最終更新: 2021/5/24 (PuTTY 0.75 で動作検証)

はじめに

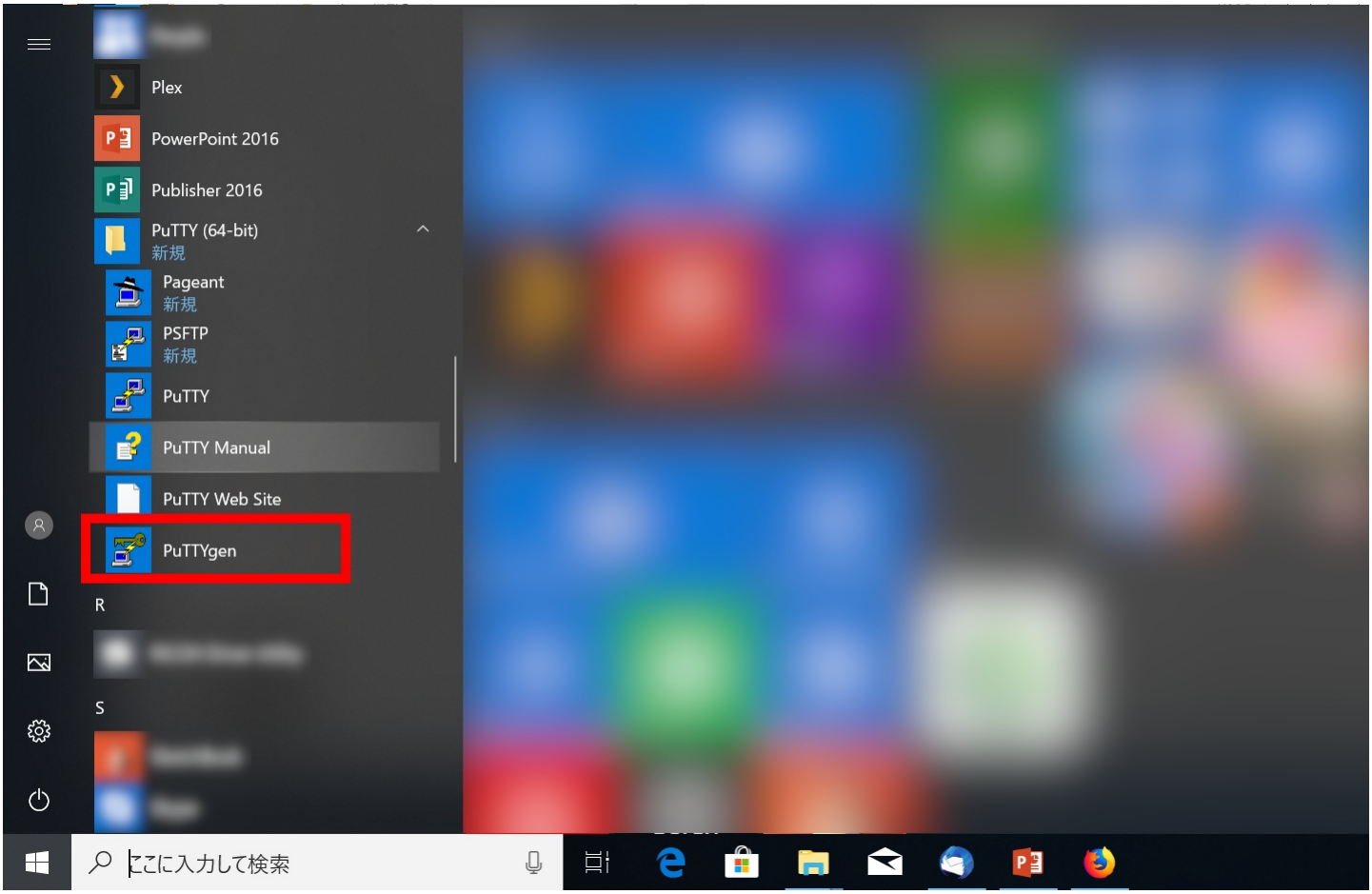
このページではPuTTYとPuTTYgenを使ったSSH鍵の作成方法とフロントエンドノードへのログイン方法について説明します。

PuTTYのインストール

PuTTYの公式サイト(https://www.putty.org)よりダウンロードできます。最新安定版のダウンロードページからMSI版(Windows Installer)をダウンロードし、指示に従ってインストールするのが手軽です。
PuTTYを既に導入済みで、PuTTYgenが無い場合には、ダウンロードページの Alternative binary files 以下のリストから PuTTYgen (puttygen.exe) を選んでダウンロードしてください。

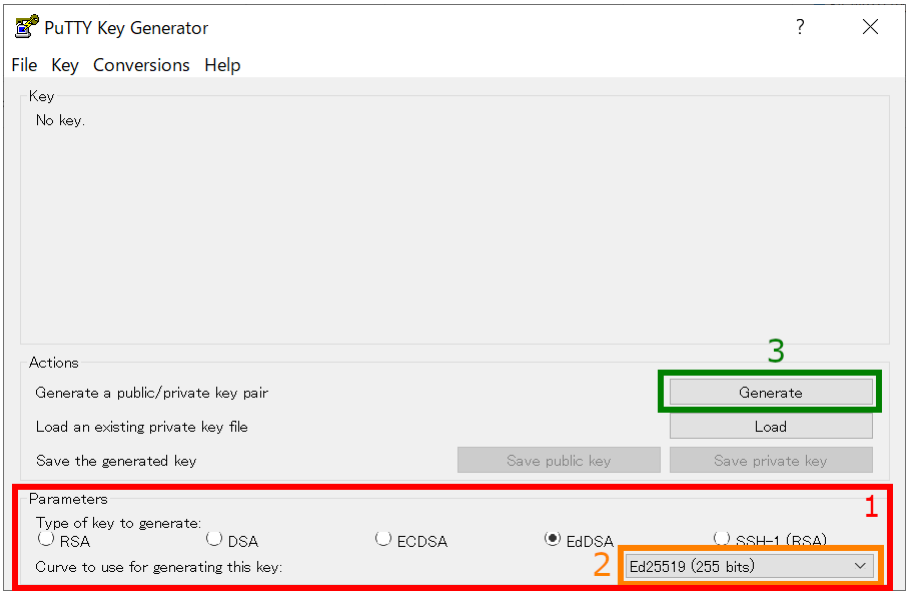
SSH鍵の作成(PuTTYgen)

PuTTYgenを起動する



PuTTYgenは上の画像のようにスタートメニュー等から起動できます。

鍵の作成(1) - 鍵の種類を選択



PuTTYgenを起動すると上のようなウインドウが表示されます。

1. 鍵の種類を選択します

RCCS では Ed25519, ECDSA (256, 384, 521 ビット), RSA 4096ビット ※の鍵を推奨しています。
特にこだわりが無いようでしたら、Ed25519をご利用ください。
Ed448 はフロントエンドノードへのログインには利用できませんので、選ばないようお願いいたします。

※PuTTY 0.74 以前の RSA では SHA2 のアルゴリズム(rsa-sha2-256/512)に未対応です。そのため、将来的に SHA1 の署名方式(ssh-rsa)が無効化された場合に問題になる可能性があります。(なお、SHA1 でも SHA2 でも鍵の形式自体は共通です。十分な長さの鍵があるのであれば鍵を作り直す必要はありません。)

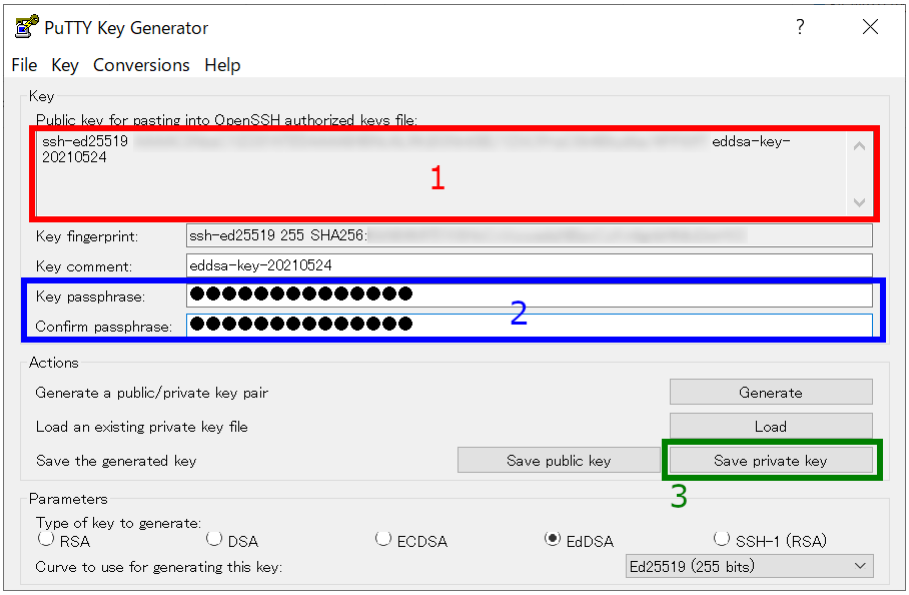
2. 鍵のビット数を指定する

ECDSA や RSA を選択すると 2 の位置に鍵のビット数を選ぶボックスが表示されますので、そちらにて選択、入力してください。

3. 鍵の生成を開始する

クリックすると鍵の生成が始まります。マウスカーソルを動かさないと処理が進みませんのでご注意ください。

鍵の作成(2) - パスフレーズの設定と保存



鍵が生成されると上のような画面に切り替わります。

1. OpenSSH 形式の公開鍵

ここに文字列として表示される鍵を当サイトに登録することになります。一旦メモ帳などに書き出し、保存しておくことをおすすめします。ssh- あるいは ecdsa- から始まる文字列全体を保存して下さい。下の "Save public key" で保存する書式の鍵ではダメですのでご注意ください。

公開鍵を失くした、あるいは保存するのを忘れた場合、秘密鍵が残っていれば "Load" ボタンや "Conversion" メニューから読み込むことで復元できます。(秘密鍵を失くした場合には鍵を作り直す必要があります。)

2. 秘密鍵のパスフレーズ設定

秘密鍵のパスフレーズを設定します。RCCS では「英小文字」「英大文字」「数字」「記号」の 4 種を全て含む 10 文字以上のものを指定するようお願いしております。

3. 秘密鍵の保存

パスフレーズを設定後、このボタンをクリックして秘密鍵を保存します。rccs.ppk や ccfep.ppk のようにわかりやすい名前をつけることをおすすめします。
秘密鍵は他人の触れない場所に保存してください。

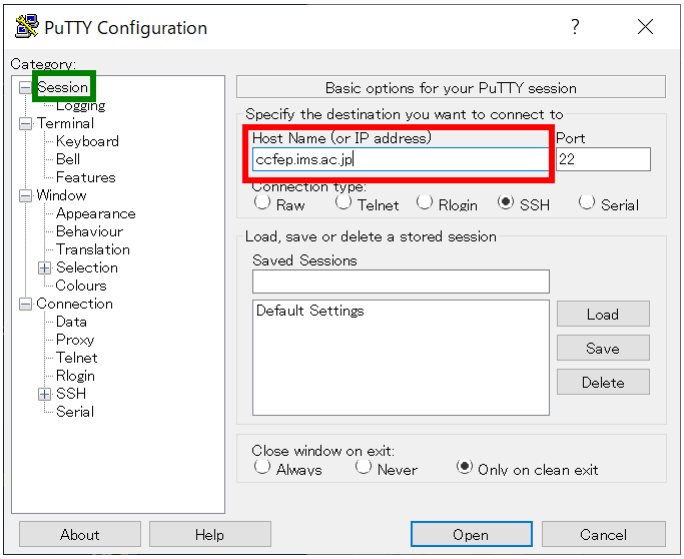
公開鍵の登録(共通)

実際にログインする前に保存した公開鍵を当サイトに登録する必要があります。
以下のリンク先に手順がありますので、それにしたがってご登録ください。
https://ccportal.ims.ac.jp/account

一個上の項目における 1. OpenSSH 形式の公開鍵を使う点にご注意ください。**"Save public key" の方ではありません。**

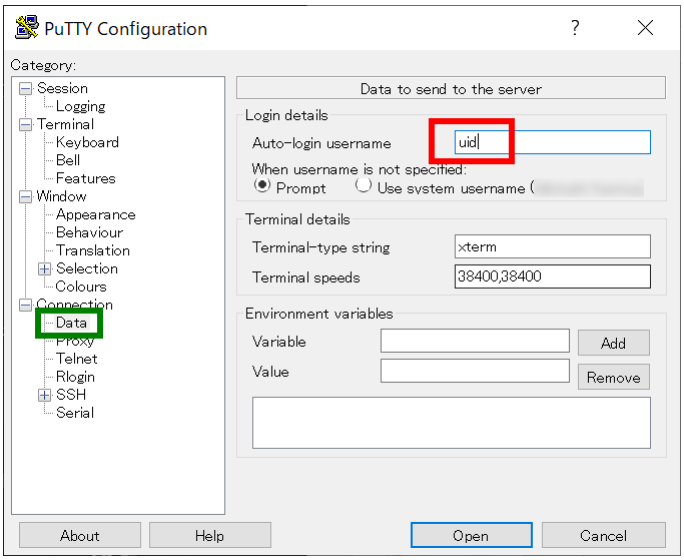
ログイン(PuTTY)

PuTTY を起動して接続先を設定する



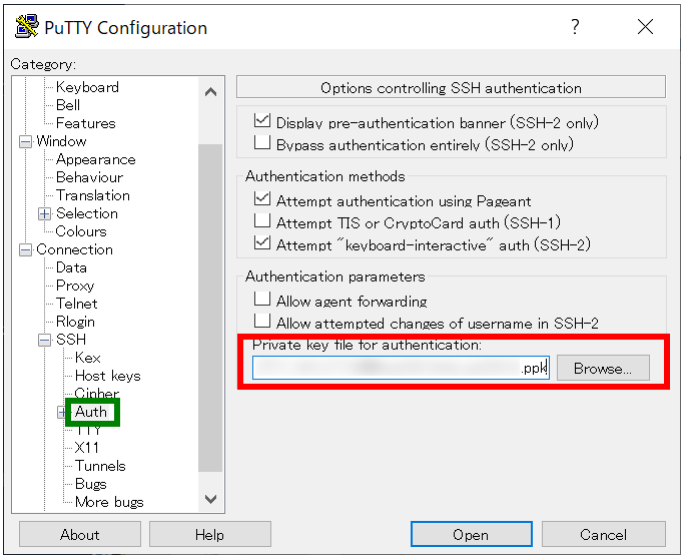
PuTTY を起動し、"Session" 項目の "Host Name (or IP address)" にフロントエンドノードの ccfep.ims.ac.jp を指定します。(まだ設定が続きますので "Open" を押さないでください)

ユーザー名の指定



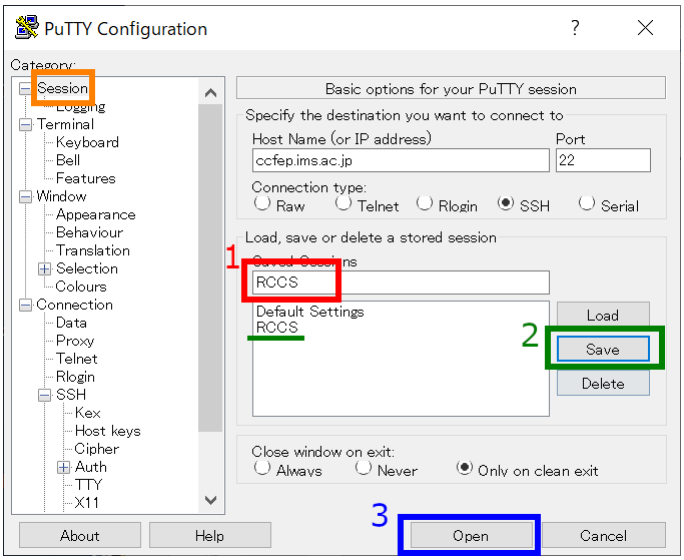
"Connection" 内の "Data" に移動します。"Auto-login username" でユーザー名が指定できますので、RCCS より指定された 3 文字の ID を入力して下さい。
このステップは省略することもできます。その場合、接続時に入力を求められることになります。

秘密鍵ファイルの指定



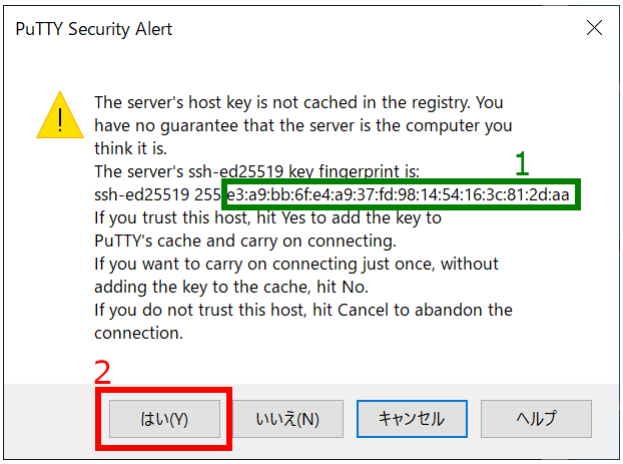
"Connection" の "SSH" 内にある "Auth" の項目に移動します。そこに秘密鍵を指定する場所があるので、先ほど PuTTYgen で作成した秘密鍵を指定します。

設定の保存



このままでも接続できますが、ここで一旦設定を保存します。"Session" に戻り。
1 のテキストボックスでこの接続に名前を付け、2 の Save ボタンを押すと保存され、左のリストに登録されます。
設定を保存できたら、3 の "Open" ボタンを押して実際に接続を開始します。

初回接続時の注意



初回の接続時には上のようなダイアログが表示されます。1 で表示されるサーバーの fingerprint が以下のどれかと一致することをお確かめください。

- 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/j7jqgUJIlxWehryCtStIp1Dir (SHA256)

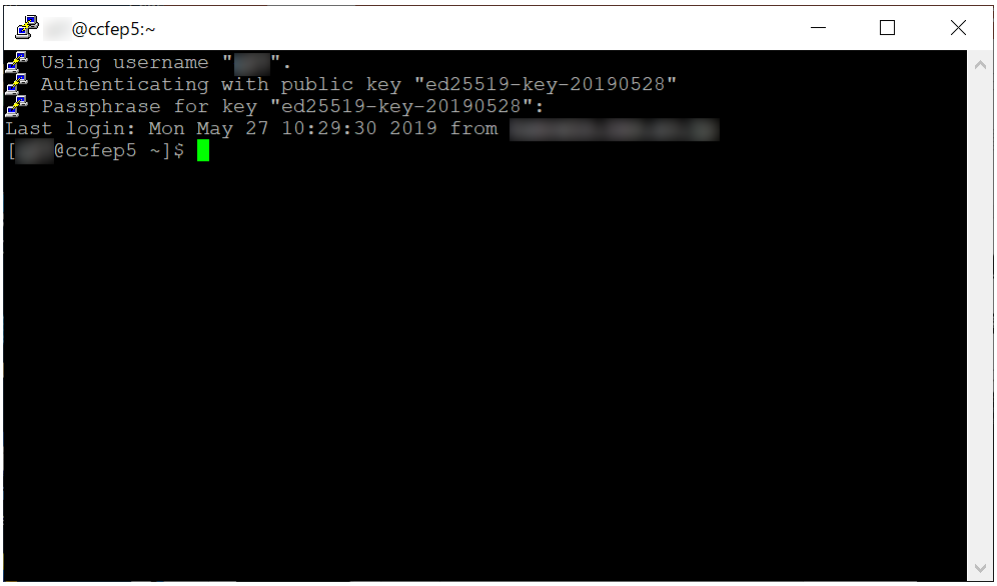
fingerprint に問題が無いようでしたら、2. ボタンを押して続行します。

秘密鍵のパスフレーズ入力

サーバーへの接続に成功すると上のような画面が表示され、パスフレーズの入力を求められますので、入力してください。

(メモ: Pageant に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 への登録時には入力が必須です。))

ログイン完了



公開鍵が正しく登録されており、正しい秘密鍵を選んで正しいパスフレーズを入力できていれば、上の画面のようにログインが成功し、プロンプトが表示されます。