SSH鍵作成とログイン(MobaXterm版)

最終更新: 2024/5/17 公式サイトへのリンク追加

はじめに

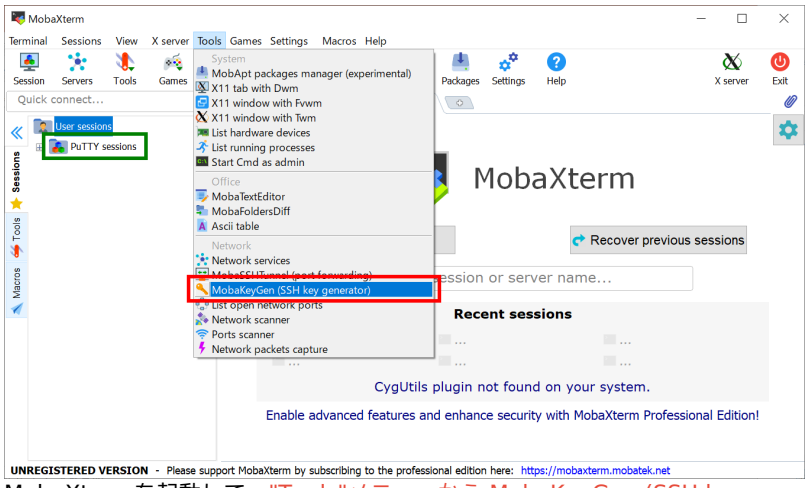
このページではMobaXtermを使ったSSH鍵の作成方法とログインサーバへのログイン方法について説明します。

インストール

https://mobaxterm.mobatek.net/ からダウンロード可能です。

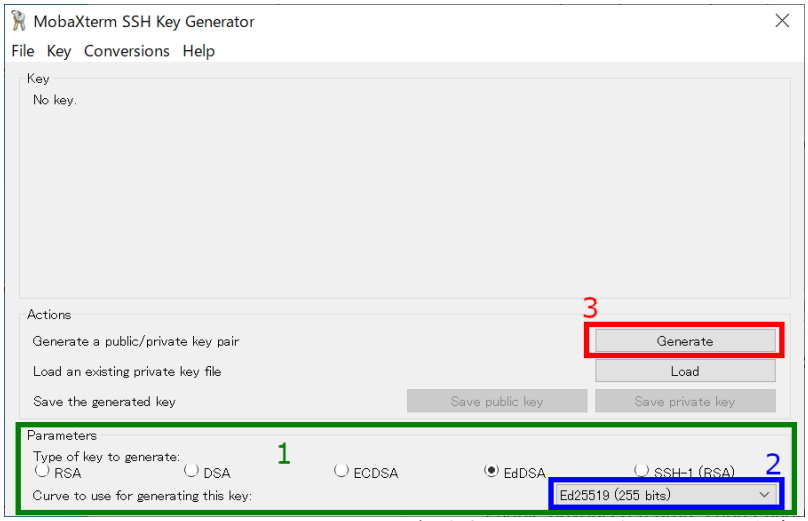
SSH鍵の作成(MobaKeyGen)

MobaXtermを起動してMobaKeyGenを呼び出す



MobaXtermを起動して、"Tools"メニューから MobaKeyGen (SSH key generator)を呼び出します。
なお、PuTTY の設定が存在している場合、それが左ペインの PuTTY sessionsに読み込まれます(レジストリから読み出し?)。
こちらに有効な設定が既に存在する場合、そのまま利用して接続することも可能です。

鍵生成(1) - 鍵種類の選択



MobaKeyGen (SSH Key Generator)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 EdDSA (Ed25519), ECDSA (256, 384 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、EdDSA (Ed25519)をご利用ください。
Ed448 は未対応のため、選択しないようお願いします。

* 古い MobaXterm Personal では RSA SHA2 のアルゴリズム(rsa-sha2-256/512)に未対応のため、できるだけ新しいバージョンを使うようお願いします。

* ECDSA-521 鍵は PuTTY 0.68-0.80 の問題のため、利用停止となりました

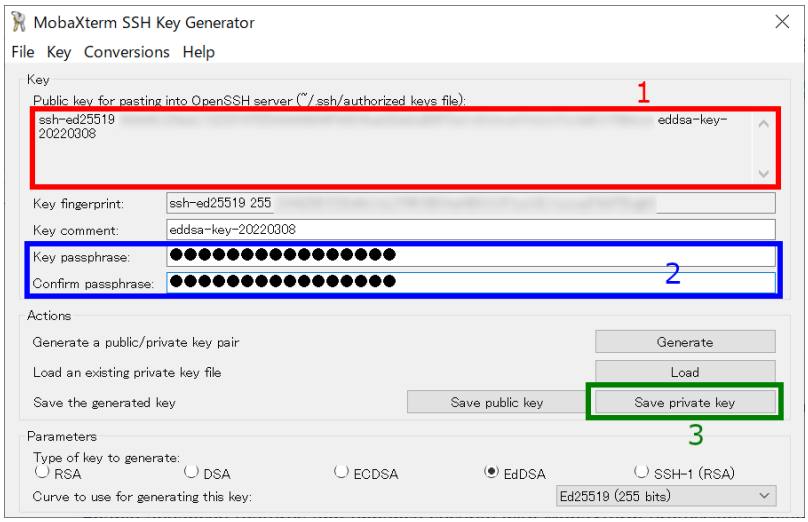
2. 鍵のビット数/方式を指定します

EdDSA、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、そちらで選択あるいは入力してください。
Ed448 は未対応のため、選択しないようお願いします。

3. 鍵の生成を開始する

クリックすると鍵の生成が開始されます。クリック後、マウスカーソルをしばらく動かさないと処理が進行しません。

鍵の生成(2) - パスフレーズの設定と鍵の保存



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。

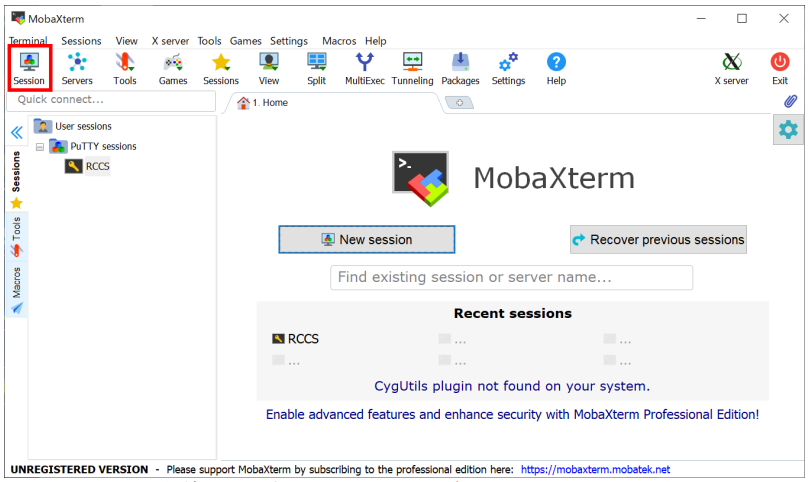
公開鍵の登録(共通)

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、これにしたがってご登録ください。
https://ccportal.ims.ac.jp/account

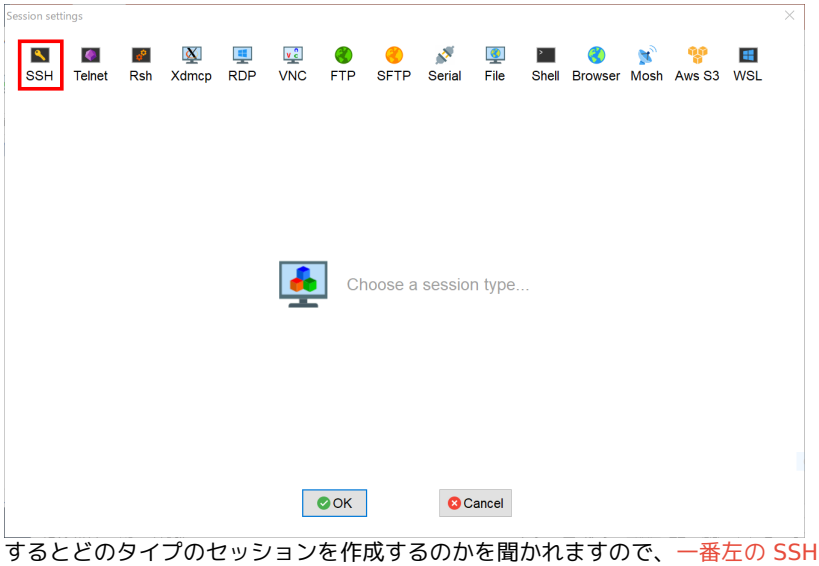
一個上の項目における 1. OpenSSH 形式の公開鍵を使う点にご注意ください。**"Save public key" の方ではありません。**

ログイン

新しいセッションの作成

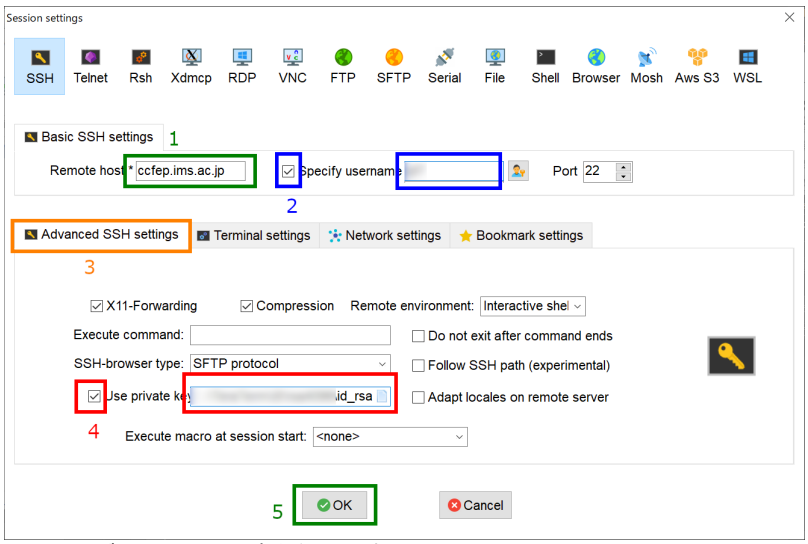


MobaKeyGen を終了して初期画面に戻り、左上にある Session をクリックし、新規のセッションを作ります。



するとどのタイプのセッションを作成するのかを聞かれますので、一番左の SSH を選択します。

SSH接続設定を行う



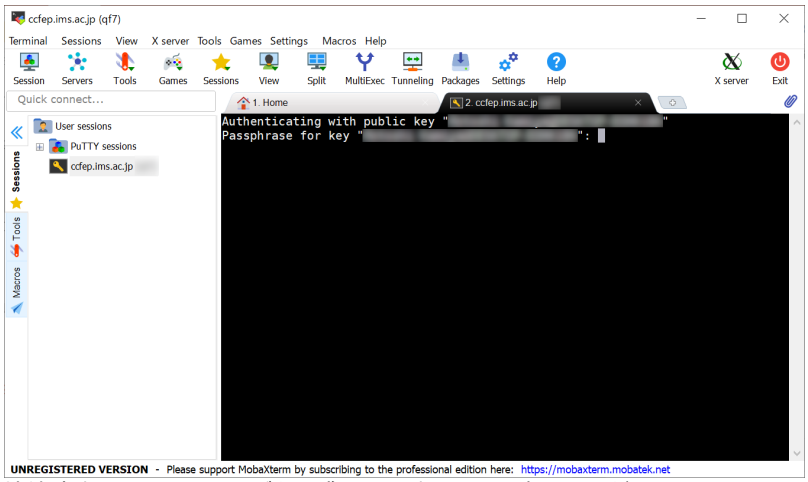
このページでは以下の設定を行います。

1. ホスト名として ccfep.ims.ac.jp を入力します。
2. "Specify username" をチェックし、RCCS 指定の 3 文字のユーザー ID を入力します。
3. "Advanced SSH settings" タブをクリックして開きます。

4. "Use private key" をチェックし、先ほど作成した秘密鍵ファイルを指定します(OpenSSH でも PuTTY の形式でも大丈夫のようです)

5. 上記設定が全て完了したら OK を押し、接続を開始します。

パスフレーズの入力

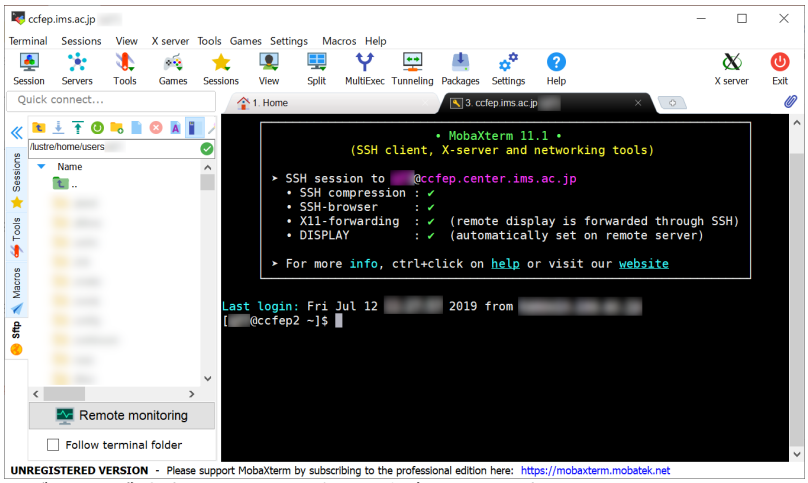


接続時するとパスフレーズを要求されますので、入力してください。

メモ: MobaXterm はデフォルト設定では初回接続時の接続先ホストの検証を行いません。"Settings" -> "Configuration" の SSH タブ、SSH settings 枠中の "Validate host identity at first connection" をチェックすると検証を行うようになります。ccfep の有効な fingerprint は以下のものです。

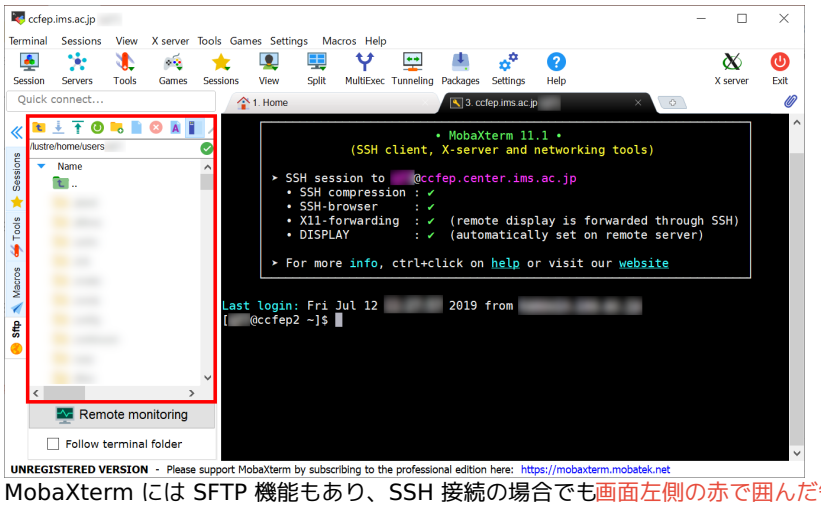
- ad:de:79:30:81:b0:b1:6a:17:f5:6f:ea:f4:b4:3b:de (MD5)
- e3:a9:bb:6f:e4:a9:37:fd:98:14:54:16:3c:81:2d:aa (MD5)
- 07:7e:df:7b:16:47:a8:f5:7c:48:b0:a3:d3:86:71:6a (MD5)
- wnEM30z4AxyDJ9XI/DdGr2PlNeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI (SHA256)
- Nhg+9Lgj3XeuW//A/j7jqgUJllxWehryCtStIp1Dir (SHA256)

ログイン完了



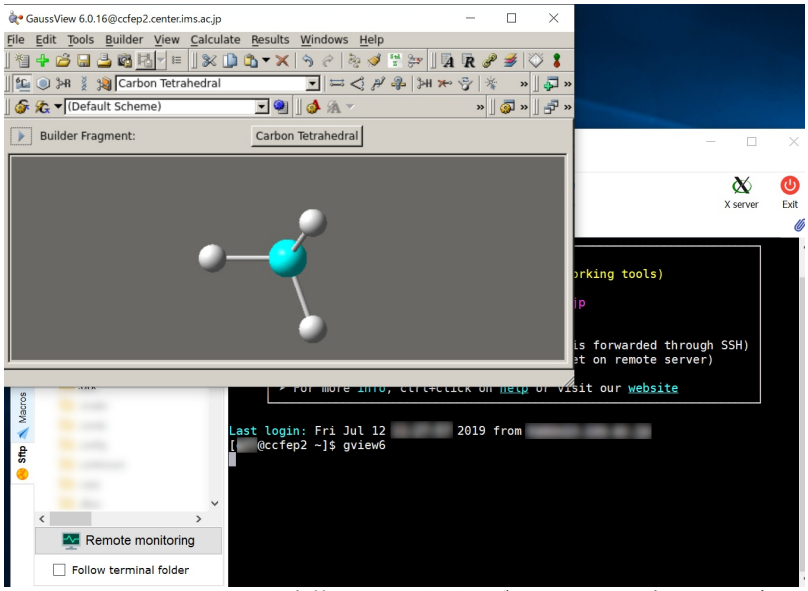
ログインに成功すると上のような画面が表示されます。

ヒント1: SFTP



MobaXterm には SFTP 機能もあり、SSH 接続の場合でも画面左側の赤で囲んだ領域でファイルのダウンロード等ができます。

ヒント2: X11



MobaXterm は Xserver を内蔵しているため、デフォルトの設定でも問題無く X window アプリが利用できます。
(ログイン時の表示で X11-forwarding の項目にチェックが入っていない場合は利用できません。)