SSH鍵作成(TeraTerm版)

最終更新: 2021/2/3 (Tera Term 4.105 で動作確認)

はじめに

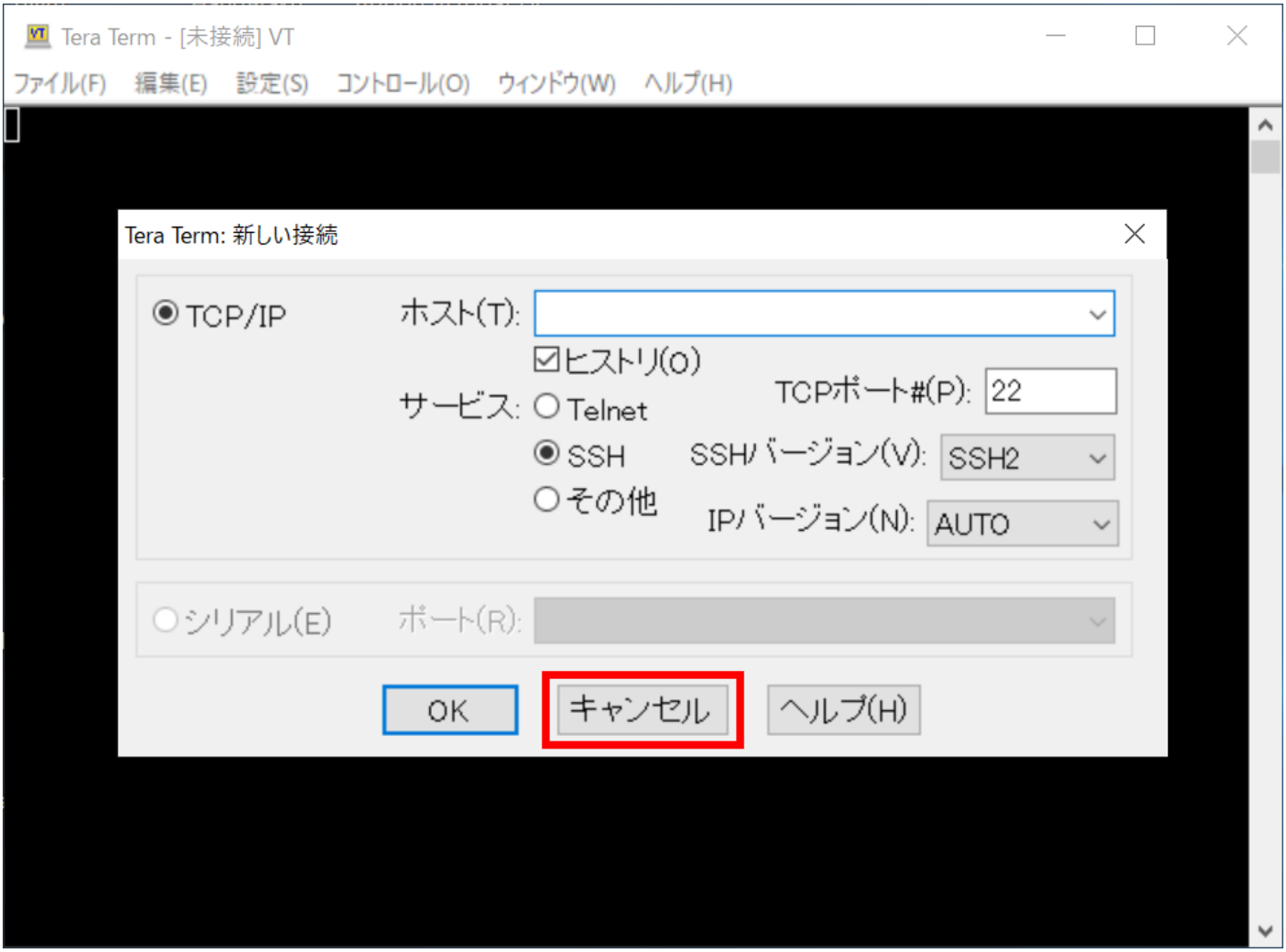
このページでは Tera Term を用いた SSH 鍵の作成方法とフロントエンドノードへのログイン方法について説明します。

Tera Term のインストール

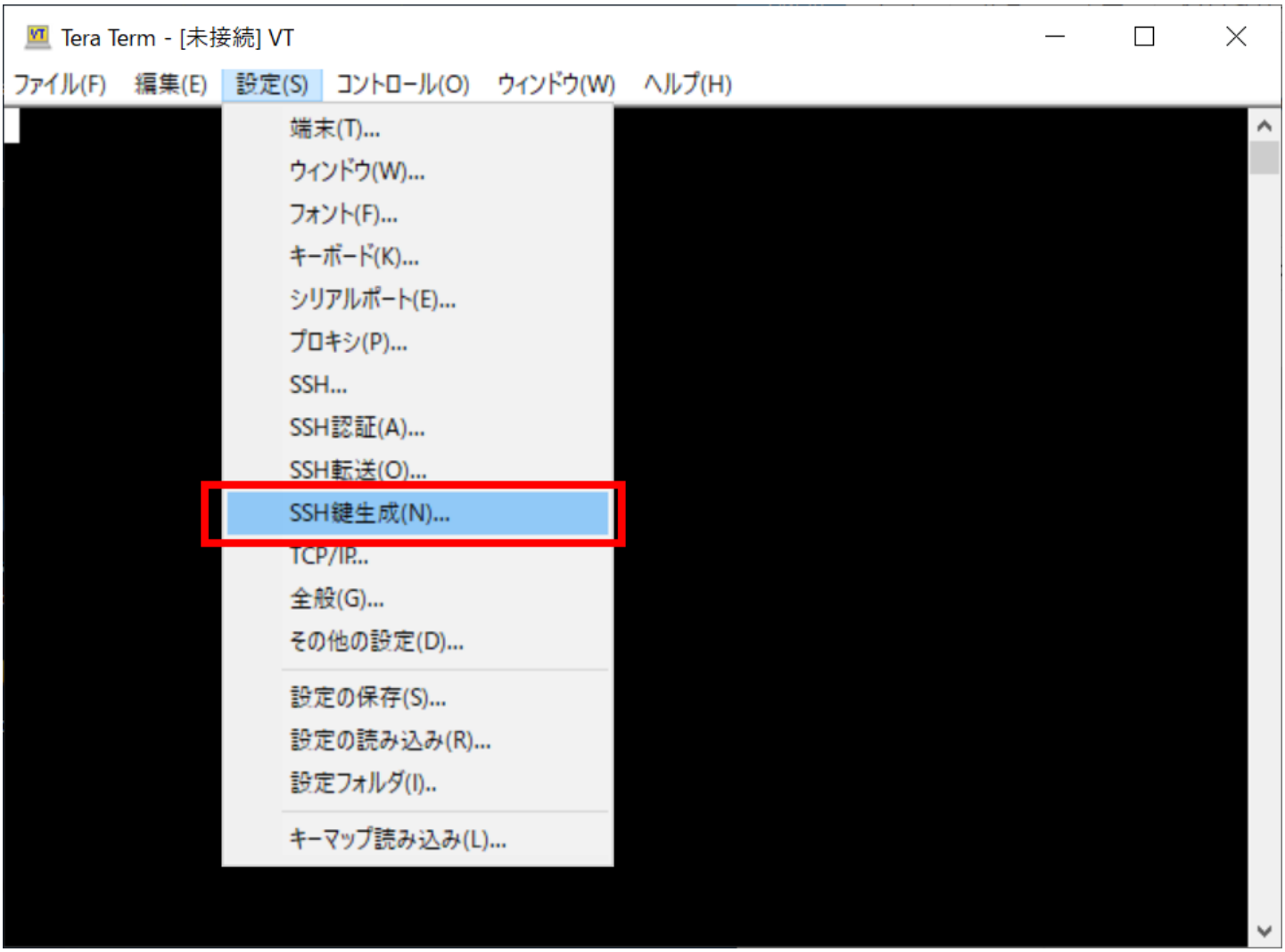
Tera Term は以下のサイトよりダウンロードできます。
https://ja.osdn.net/projects/ttssh2/
インストーラの指示に従ってインストールしてください。

SSH鍵の作成

Tera Term を起動する

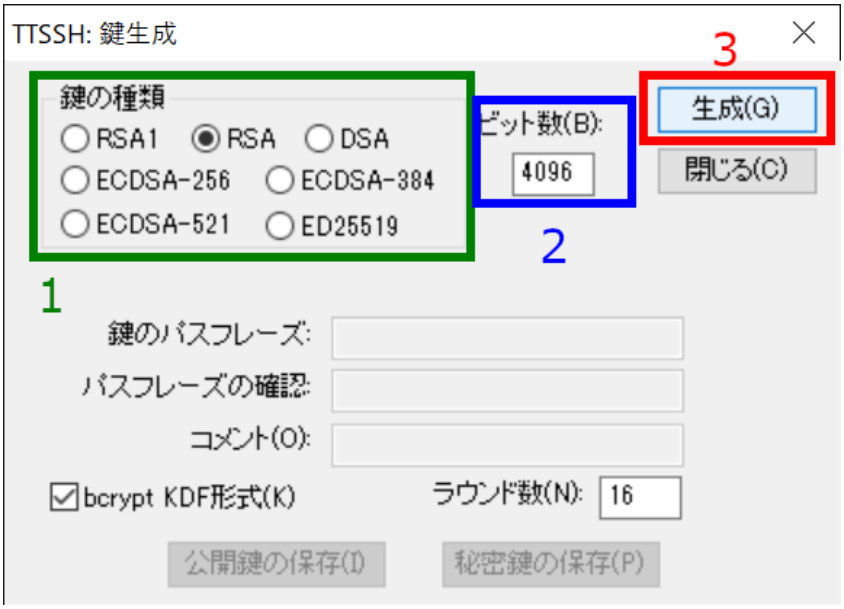


Tera Term を起動後、まずはキャンセルをクリックして鍵の作成に入ります。



「設定」メニューから SSH鍵生成を選びます。

鍵の生成(1) - 鍵の種類を選択



SSH鍵生成に入ると上のようなウインドウが表示されます。

1. 鍵の種類を選択する

RCCS では ED25519, ECDSA-521, ECDSA-384, ECDSA-256, 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 を選択してください。

※Tera Term 4.105 では SHA2 RSA のアルゴリズム(rsa-sha2-256/512)に未対応のため、今後 SHA1 のアルゴリズム(ssh-rsa)が禁止された場合に問題となる可能性があります。(rsa-sha2-256/512 は Tera Term 4.107 での対応が予定されています。)なお、SHA1 でも SHA2 でも鍵の形式は共通です。そのため、新たに SHA2 のアルゴリズムを使うようになる場合でも鍵の再生成は通常不要です。

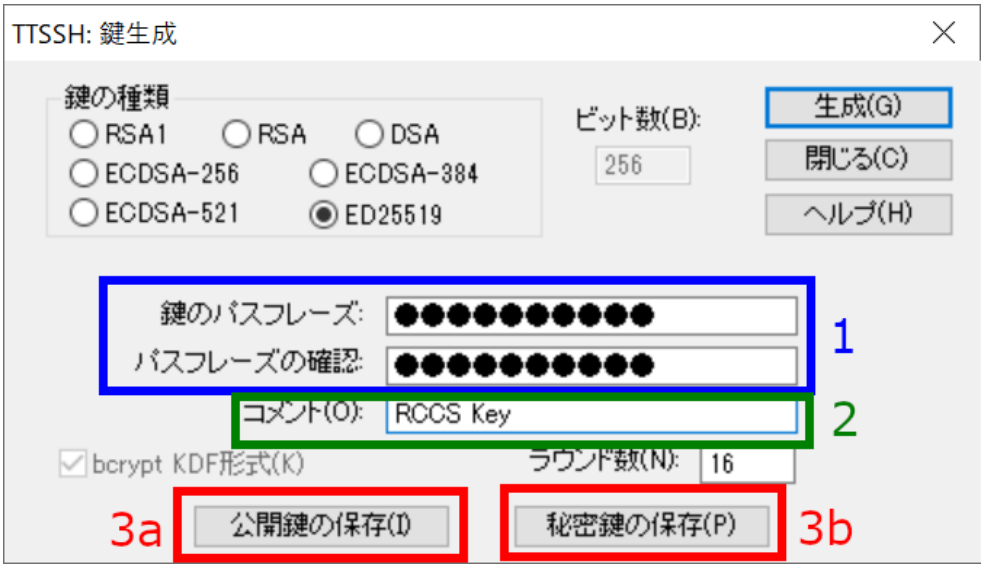
2. ビット数の指定(RSA の時のみ)

RSA 鍵の場合はここでビット数を指定できます。4096 以上の値を推奨しています。

3. 鍵生成開始

鍵種やビット数を指定した後、ここをクリックして鍵を生成します。

鍵の生成(2) - パスフレーズの設定と保存



鍵生成が終了すると、パスフレーズやコメントを設定できるようになります。

1. 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。

2. コメントの設定(optional)

複数の鍵を使い分ける場合、わかりやすい名前をつけておくと便利かもしれません。必要に応じて設定ください。

3. 公開鍵、秘密鍵を保存する

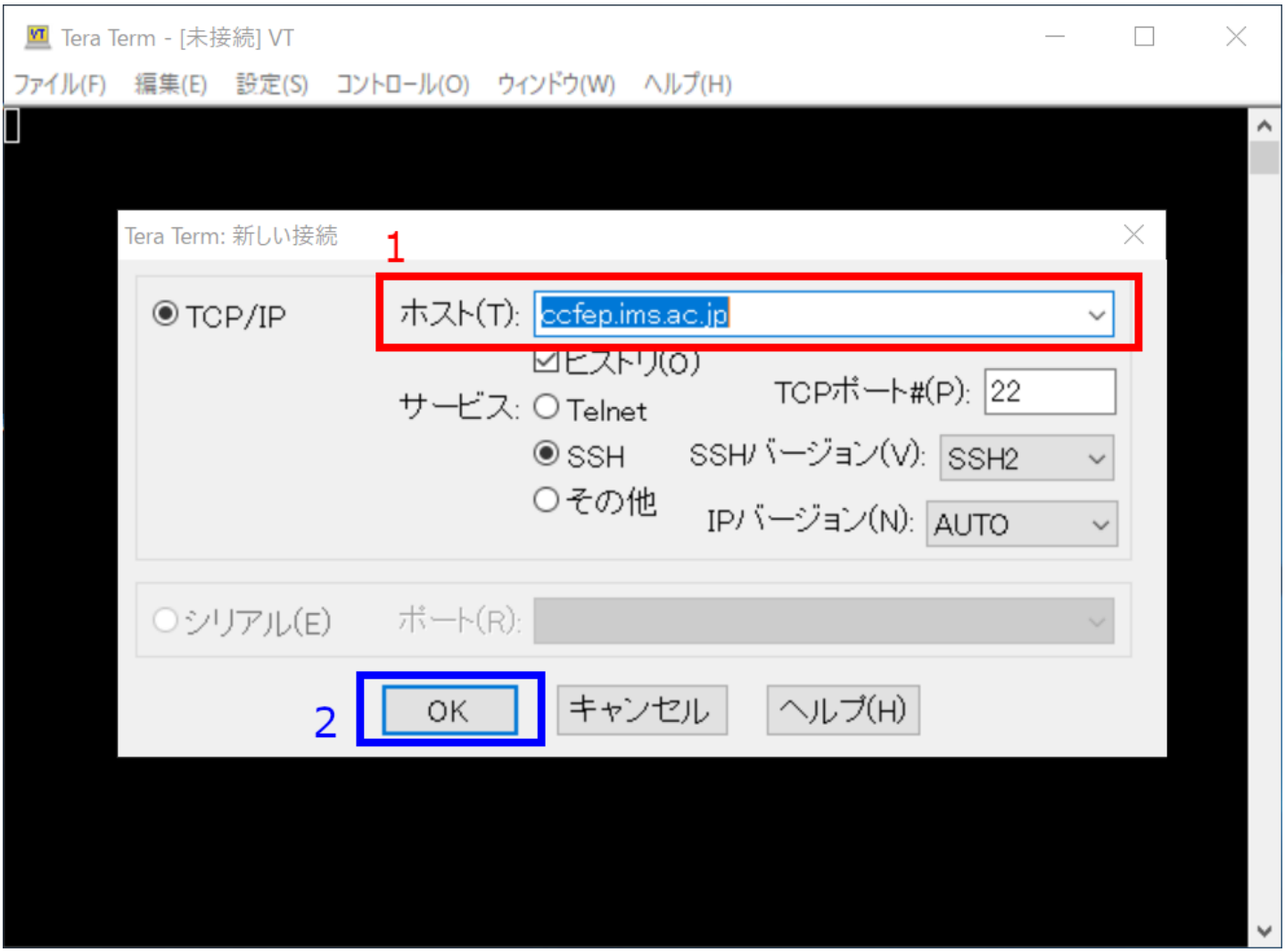
3a と 3b のボタンをクリックし、公開鍵、秘密鍵の両方を保存します。ログインするためには両方が必要です。

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

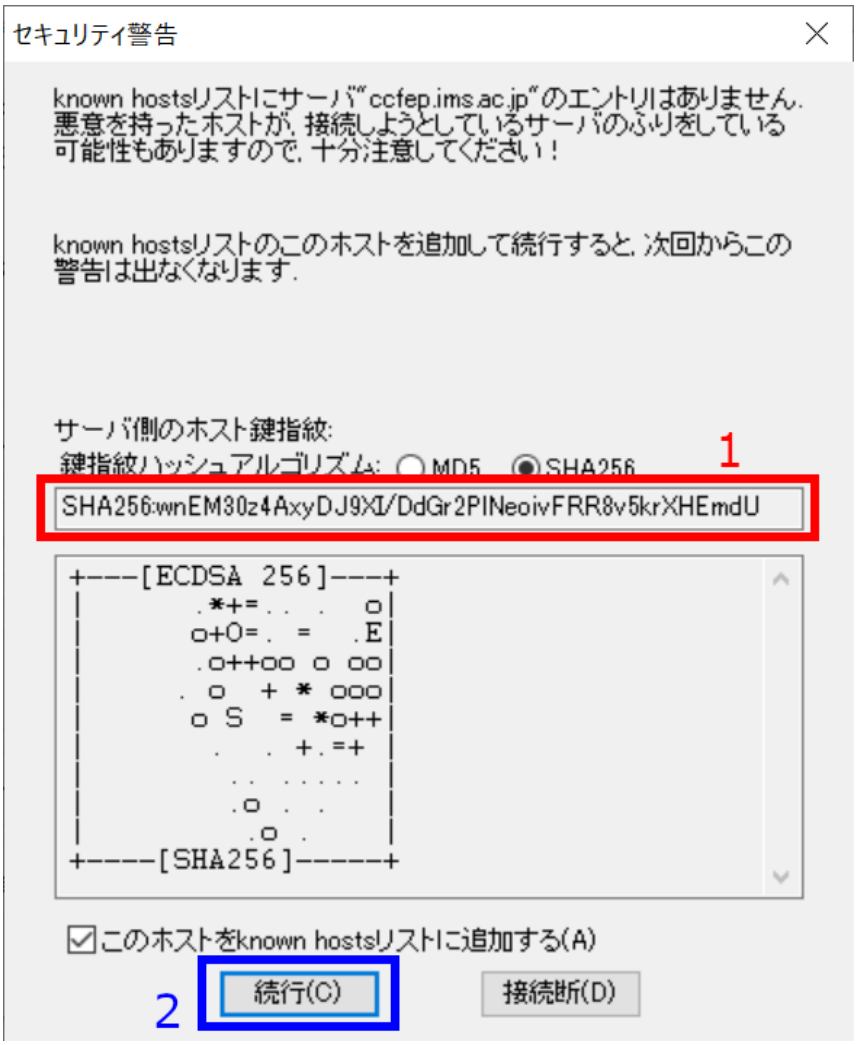
ログイン

ログイン準備



Tera Term を再起動するか、「ファイル」->「新しい接続」を選択して初期画面に戻ります。
そして、ホストに ccfep.ims.ac.jp と入力し、OK を押して先に進みます。

初回接続時の警告



初回接続時には上のようなセキュリティ警告が表示されます。1 で表示されるサーバー鍵の指紋(fingerprint)が以下のいず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/DdGr2PINeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZEIolfVqXvbI (SHA256)
- Nhg+9Lgj3XeuW//A/j7jqgUJIlxWehryCtStlp1Dir (SHA256)

fingerprint に問題無いようでしたら、2 の「続行」をクリックして先に進みます。

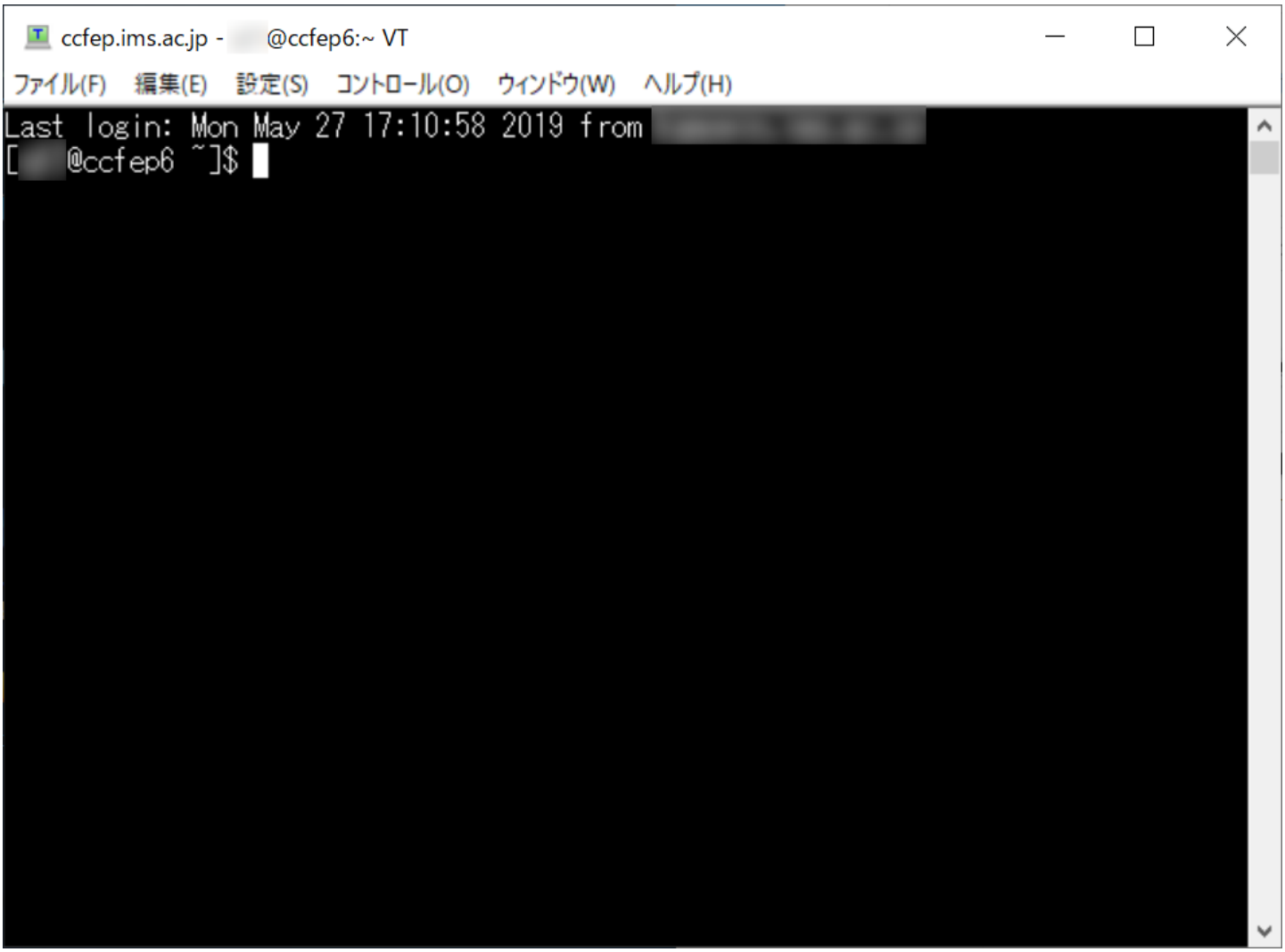
鍵やパスフレーズの指定

上の画面でユーザー名、鍵ファイルの場所などを指定します。

1. RCCS から与えられたユーザー名(3 文字のもの)を入力します。
2. 鍵生成時に指定したパスフレーズを入力します。
3. (optional)チェックを外すとよりセキュアです。
4. 鍵を使うをチェックし、秘密鍵の場所を指定します。
5. 全て完了したら OK を押して認証を行います。

(「設定」->「SSH認証」でデフォルトのユーザー名や鍵ファイルの場所を含めた認証方式を変更することも可能です。)

ログイン完了



設定が全てうまくいっていれば、上の画面のようにログインできます。