

SSH鍵作成とログイン Tera Term 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)

(Tera Term 4.102 (SVN# 7452) で動作確認)

更新履歴

- 2019/5/28 初稿作成
- 2019/7/9 初回ログイン時の説明追加

イントロダクション

この資料ではTera Term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

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

Tera Termのインストール

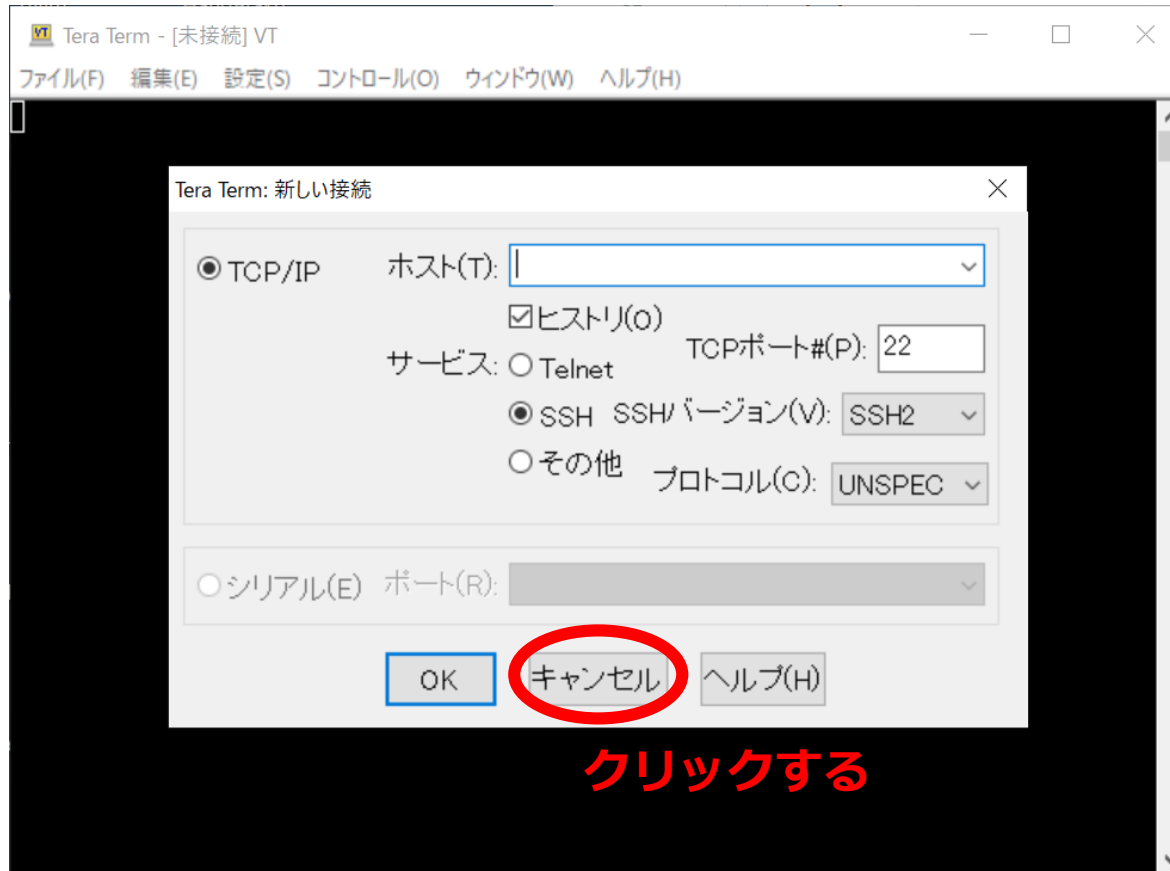
Tera Term は以下のサイトよりダウンロードができます。

<https://ja.osdn.net/projects/ttssh2/>

指示に従ってインストールしてください。

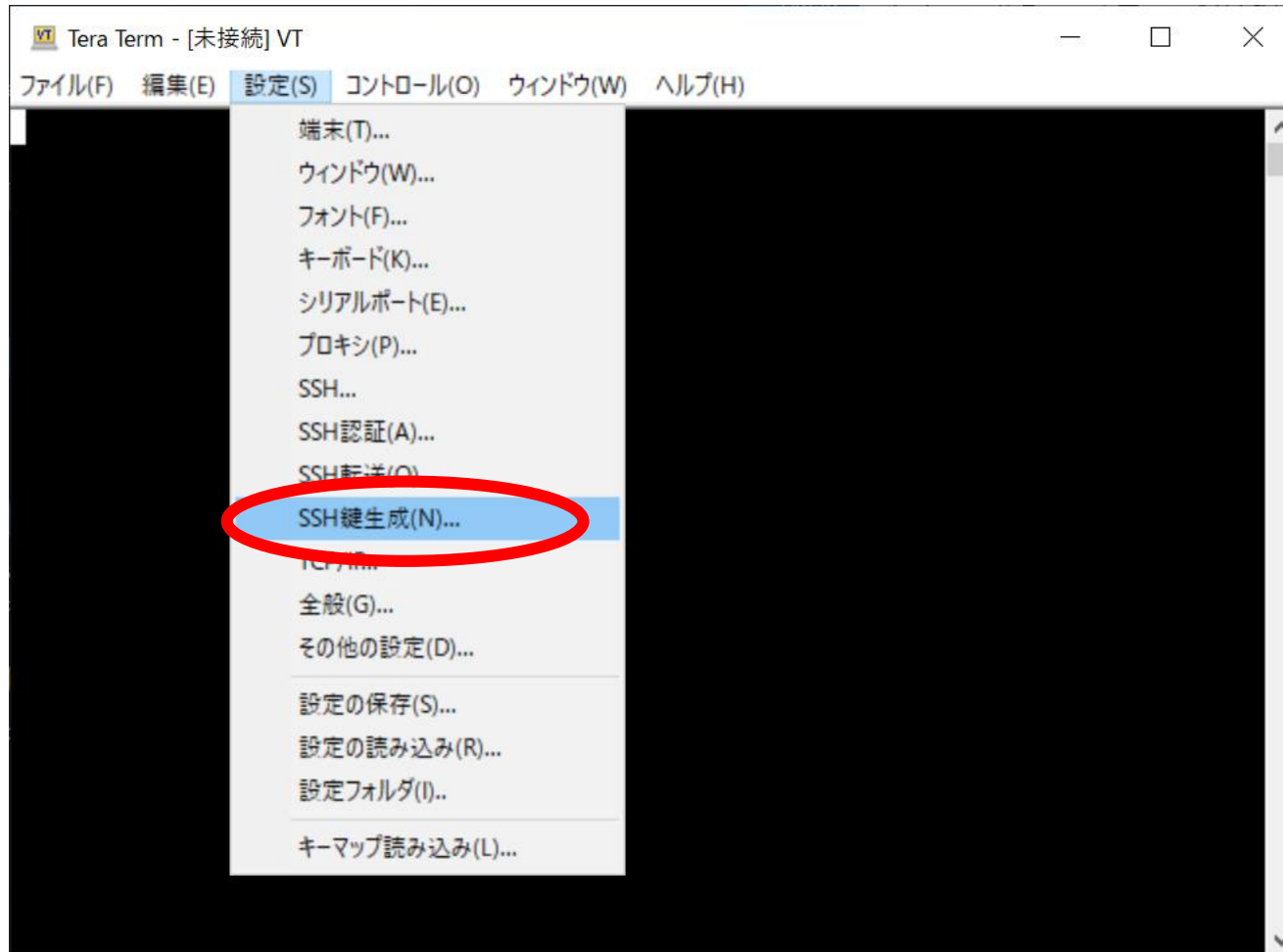
SSH鍵の作成(1)

Tera Term を起動して、接続を一旦キャンセルします。



SSH鍵の作成(2)

「設定」タブより、SSH鍵作成を選択します。



SSH鍵の作成(3)

以下のウィンドウが表示されたら、鍵の種類を指定して「生成」ボタンを押します。

1. 鍵の種類を指定

TTSSH: 鍵生成

鍵の種類

RSA1 RSA DSA

ECDSA-256 ECDSA-384

ECDSA-521 ED25519

ビット数(B): 4096

生成(G)

閉じる(C)

鍵のパスフレーズ:

パスフレーズの確認:

コメント(O):

bcrypt KDF形式(K) ラウンド数(N): 16

公開鍵の保存(D) 秘密鍵の保存(P)

3. “生成”ボタンをクリック

2. ビット数指定
(RSAの場合)

鍵の種類については以下のものを推奨しています

- RSA 4096ビット (上の例のようにビット数を 4096 にする)
- ECDSA-256, ECDSA-384, ECDSA-521, ED25519

どれを選べばよいのかわからない場合は RSA 4096 ビットをお試してください

SSH鍵の作成(4)

生成が終わったら、パスフレーズを設定し、**公開鍵**と**秘密鍵**の両方を保存します。(個別に保存する必要があります)

1. 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にお願いしています。

TTSSH: 鍵生成

鍵の種類

RSA1 RSA DSA

ECDSA-256 ECDSA-384

ECDSA-521 ED25519

ビット数(B): 4096

生成(G)

閉じる(C)

鍵を生成しました。

鍵のパスフレーズ: ●●●●●●●●●●

パスフレーズの確認: ●●●●●●●●●●

コメント(O): RCCS Key

bcrypt KDF形式(K) ラウンド数(N): 16

公開鍵の保存(D) 秘密鍵の保存(P)

2. 複数の鍵を使い分ける場合、識別用のコメントをつけると便利です。そうでなければデフォルトのままでも問題ありません。

3(a): 公開鍵保存

3(b): 秘密鍵保存

二つの鍵の内、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。

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(通常.pub拡張子)を登録する必要があります。

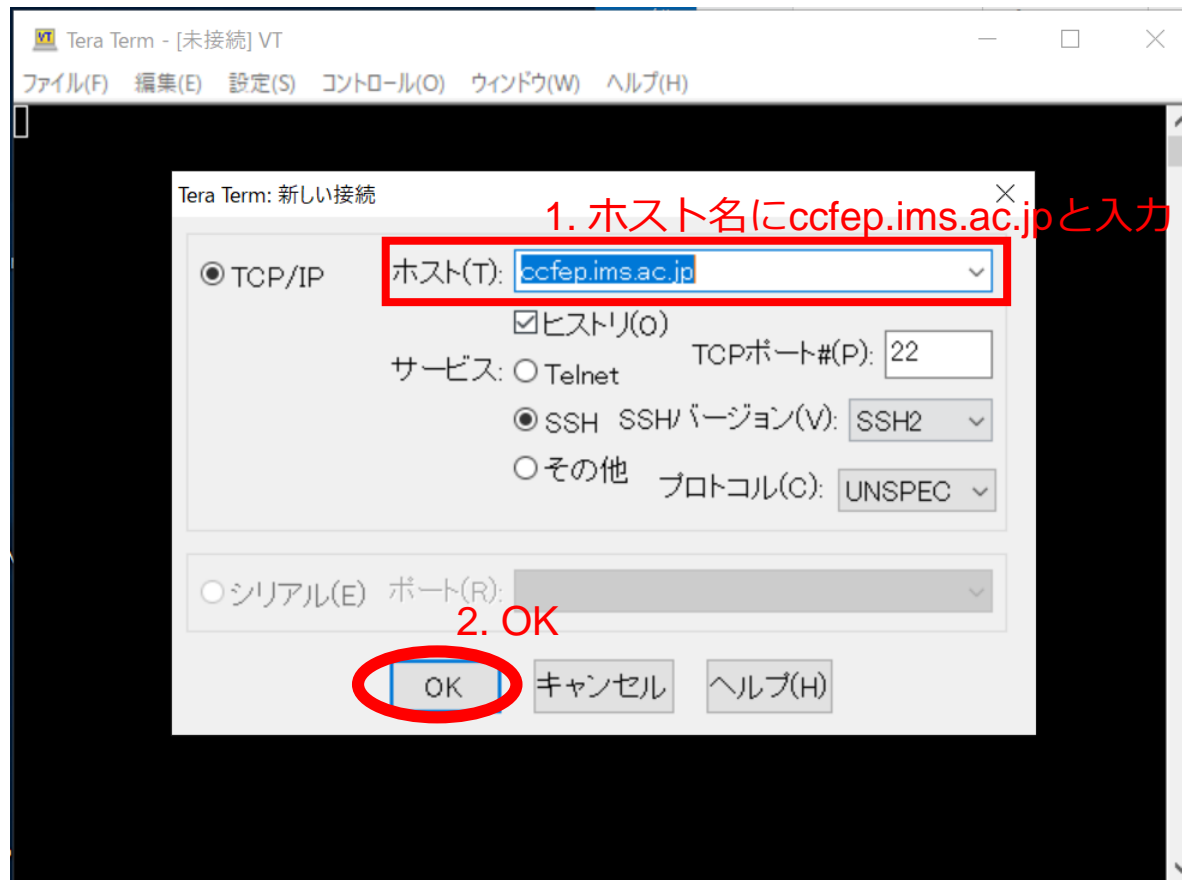
以下のリンクに手順がありますので、
こちらに従って登録して下さい。

<https://ccportal.ims.ac.jp/account/>

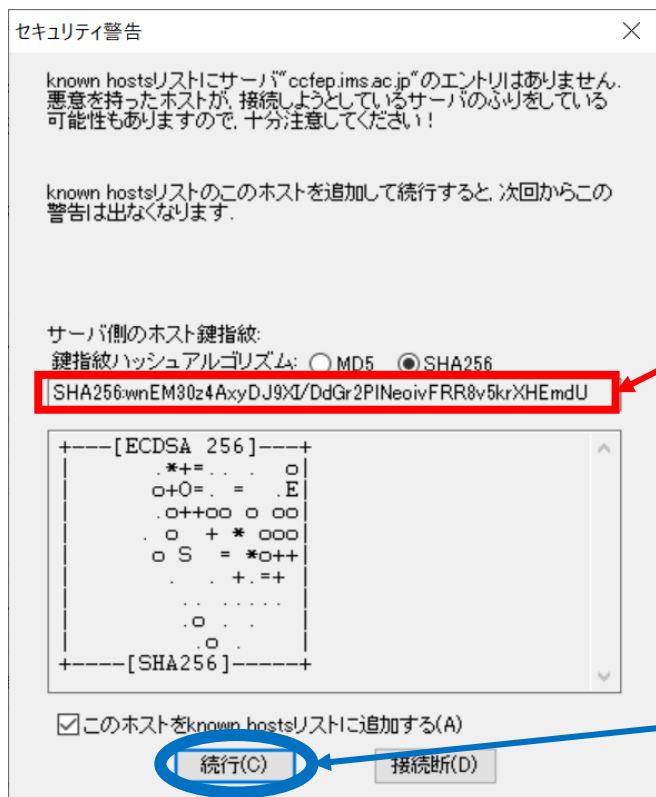
ログイン(1)

Tera Termを再起動もしくは「ファイル」->「新しい接続」を選択して初期画面に戻ります。

ホストに `ccfep.ims.ac.jp` と入力し、OK を押します。



ログイン(2)



初回接続時には、左のようなセキュリティ警告が表示されます。

1. サーバ鍵の指紋(fingerprint)が以下のいずれかと一致することを確認してください。

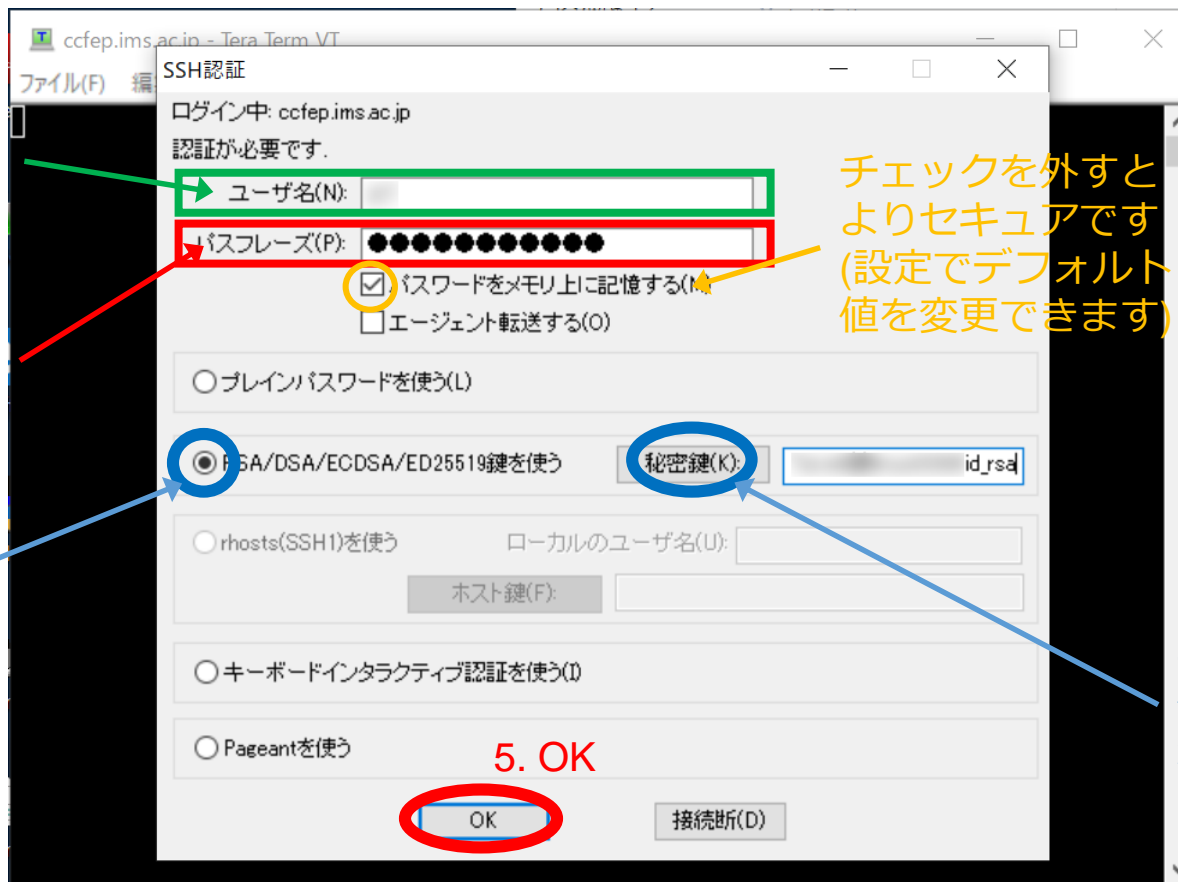
2. 問題なければ続行

有効な鍵の
fingerprint

- SHA256:wnEM30z4AxyDJ9XI/DdGr2PINEoivFRR8v5krXHEmdU
- SHA256:0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZEIolfVqXvbl
- SHA256:Nhg+9Lgj3XeuW///A/j7jqgUJllxWehryCtStlp1Dirs
- MD5: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

ログイン(3)

ユーザ名、秘密鍵ファイルの場所、秘密鍵ファイルのパスフレーズを指定します。



1. 指定された3文字のユーザアカウントを指定してください

2. 鍵生成の際に設定したパスフレーズを指定してください

3. クリックして選択してください

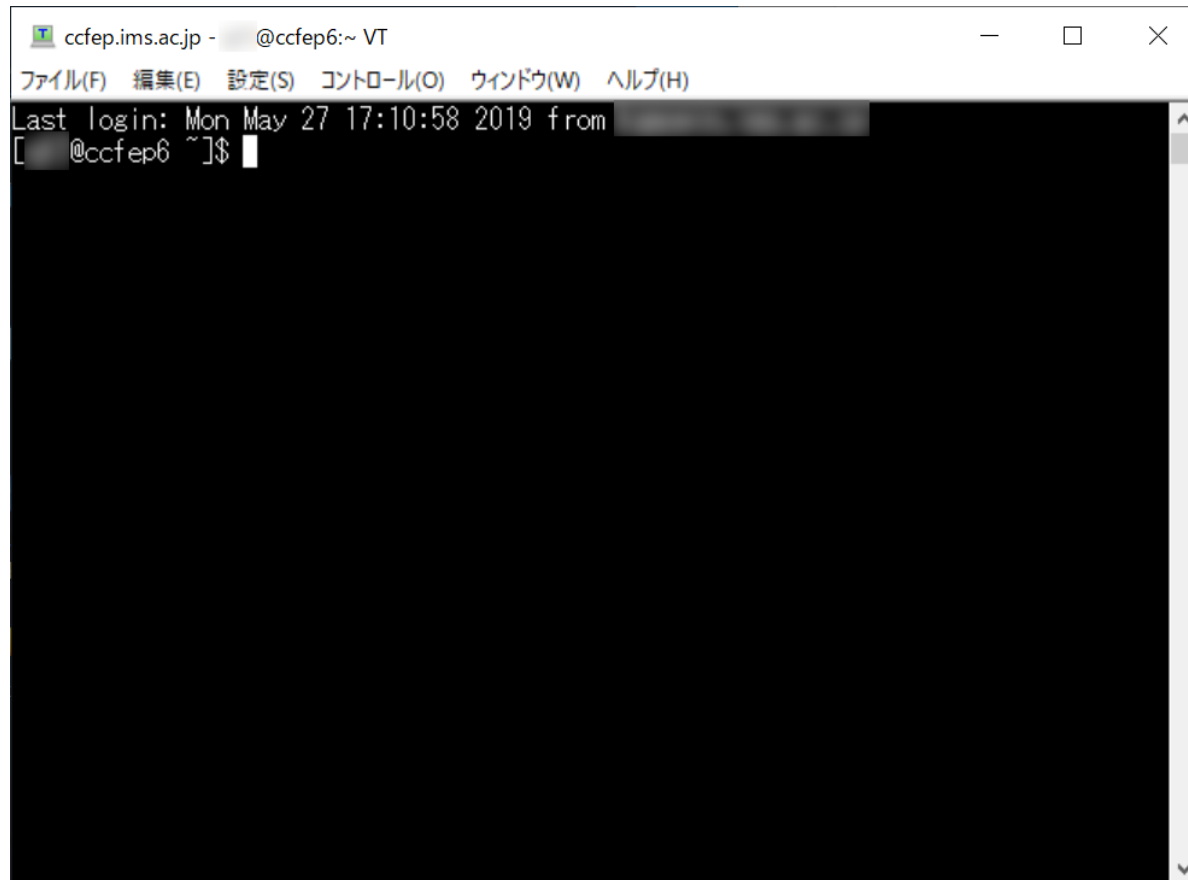
チェックを外すとよりセキュアです(設定でデフォルト値を変更できます)

4. クリックして、保存した秘密鍵を選択してください

5. OK

ログイン(4)

設定がうまくいっていれば以下のようにログインできます。



```
ccfep.ims.ac.jp - @ccfep6:~ VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
Last login: Mon May 27 17:10:58 2019 from [REDACTED]
[REDACTED]@ccfep6 ~]$
```