

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 5.1 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
- 2020/1/15 一部画像を Tera Term 4.105 のものに更新
- 2021/2/2 推奨暗号種類など一部を更新
- 2022/1/5 Tera Term 4.106 で動作確認
- 2023/1/16 RSA 鍵についての注意を更新
- 2023/3/6 Tera Term 5.0 beta 1 に関する記述を追加
- 2023/6/2 用語の微修正
- 2023/11/20 ダウンロードサイト修正と5.0での動作確認
- 2024/1/18 Tera Term 5.1 で動作確認

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、ログインサーバ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

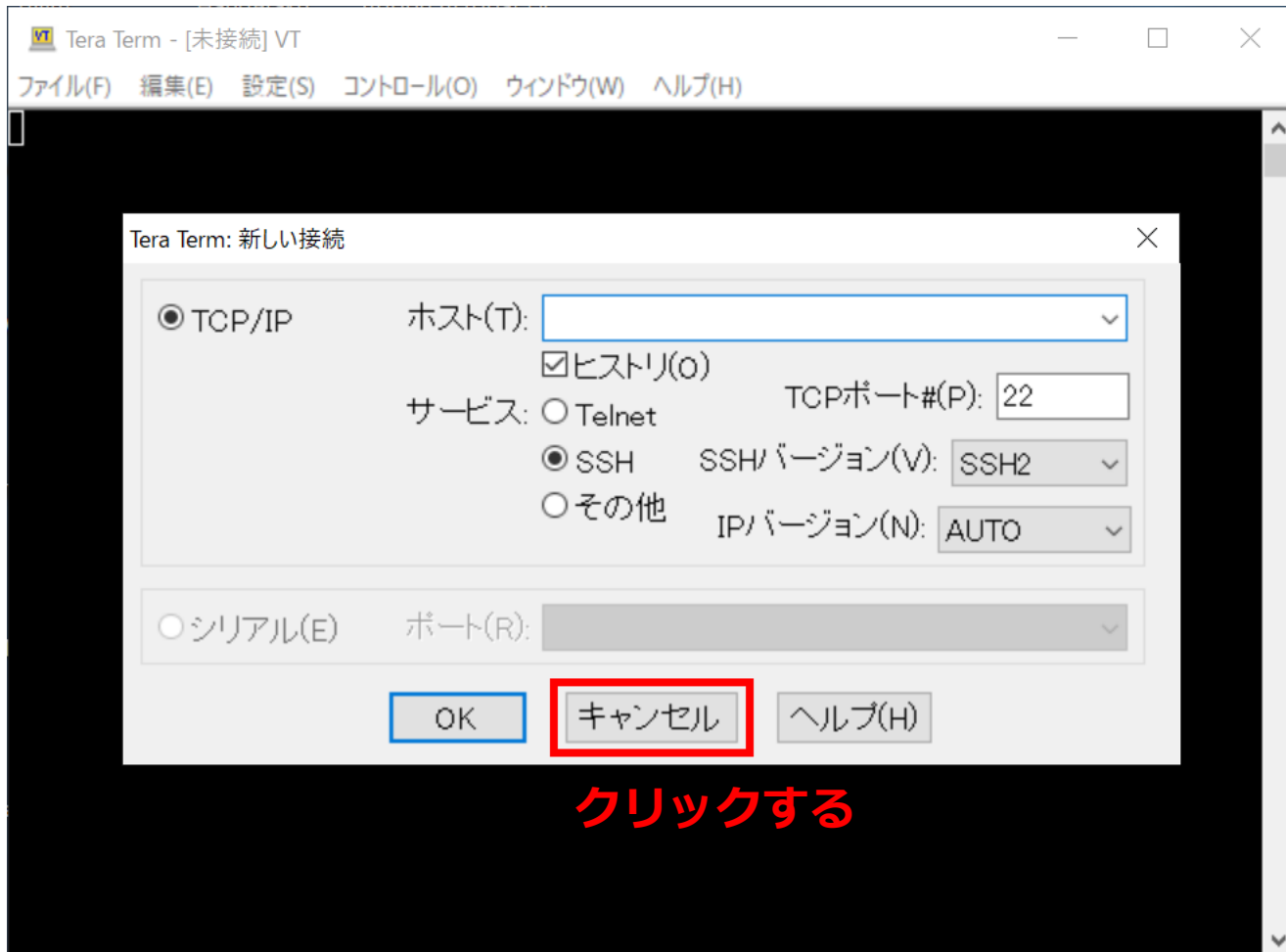
Tera Term は以下のサイトよりダウンロードができます。

<https://teratermproject.github.io/>

指示に従ってインストールしてください。

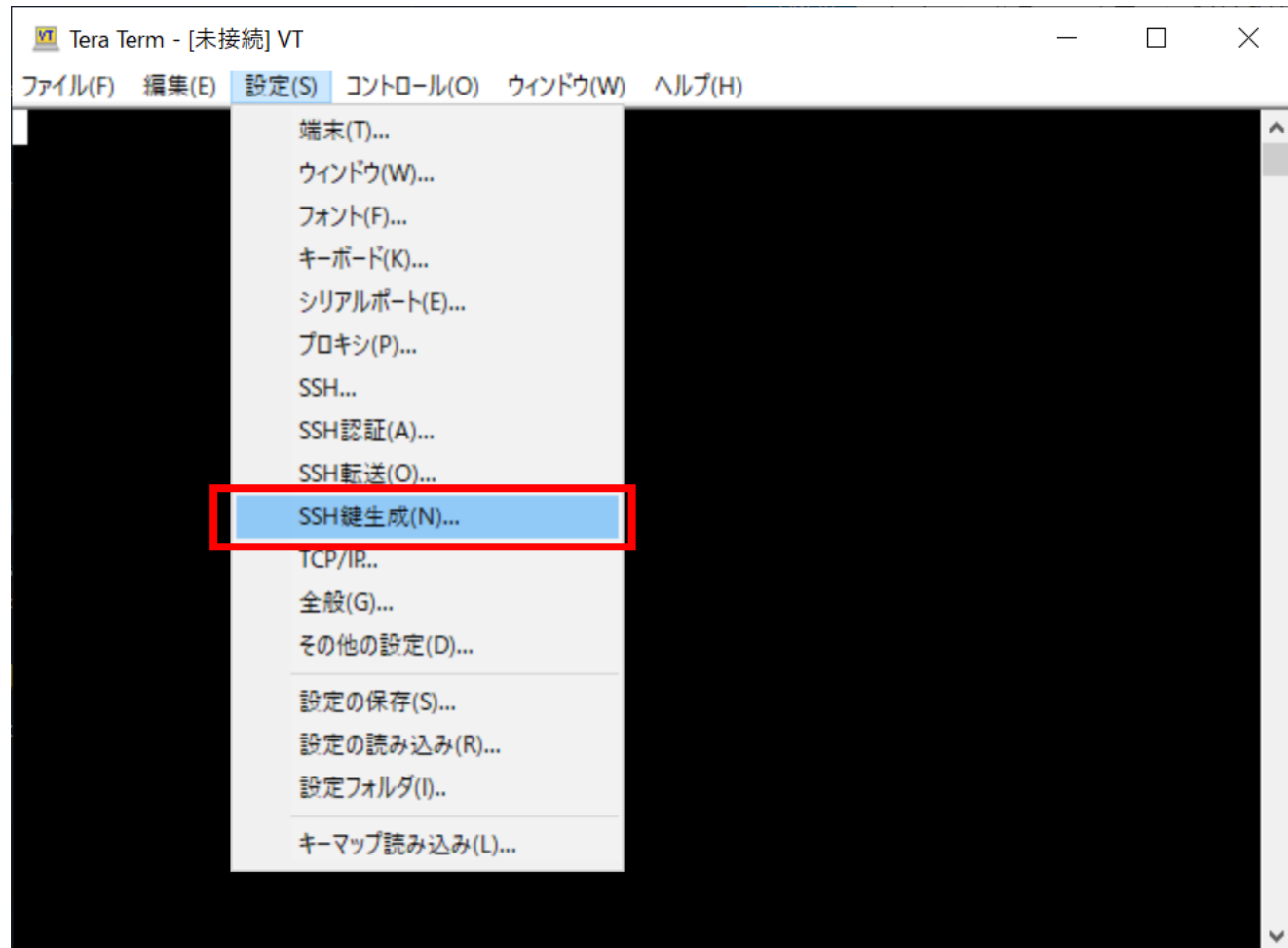
SSH鍵の作成(1)

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。

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)

1 鍵の種類を指定

2 ビット数指定 (RSAの場合)

3 鍵を"生成"

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(I) 秘密鍵の保存(P)

* RSA 鍵を使う場合は Tera Term 5.0, 4.107 あるいはそれ以降のバージョンが必要です。

鍵の種類については以下のものを推奨しています

- ED25519
- ECDSA-521, ECDSA-384, ECDSA-256
- RSA 4096 ビット (RSA を選択してビット数を 4096 に)*

どれを選べばよいのかわからない場合は ED25519 をお試しください

SSH鍵の作成(4)

生成が終わったら、パスワードを設定し、**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)

RCCS では秘密鍵のパスワードには

- 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ます。

公開鍵保存

秘密鍵保存

複数の鍵を利用される場合は適宜名前を設定した方が良いでしょう。

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。

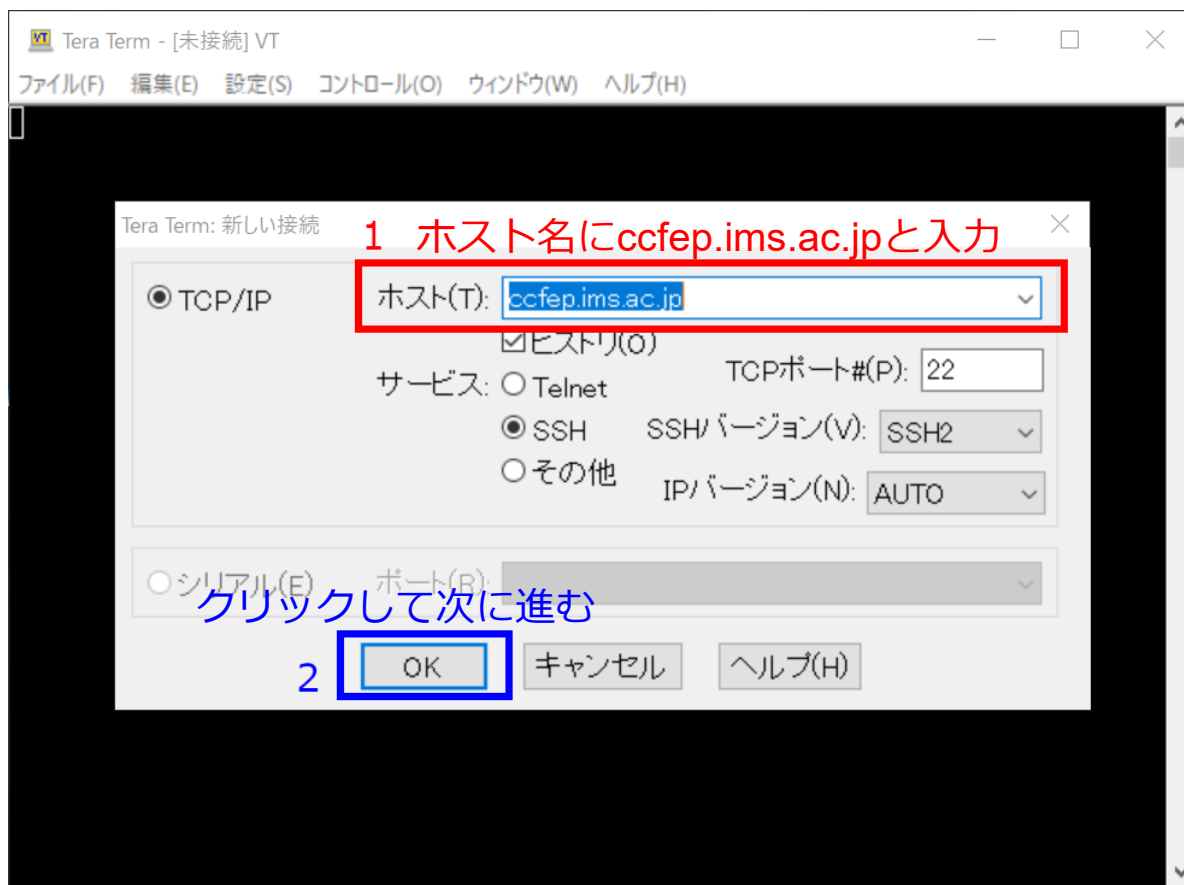
以下のリンクに手順がありますので、
こちらに従って登録して下さい。

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

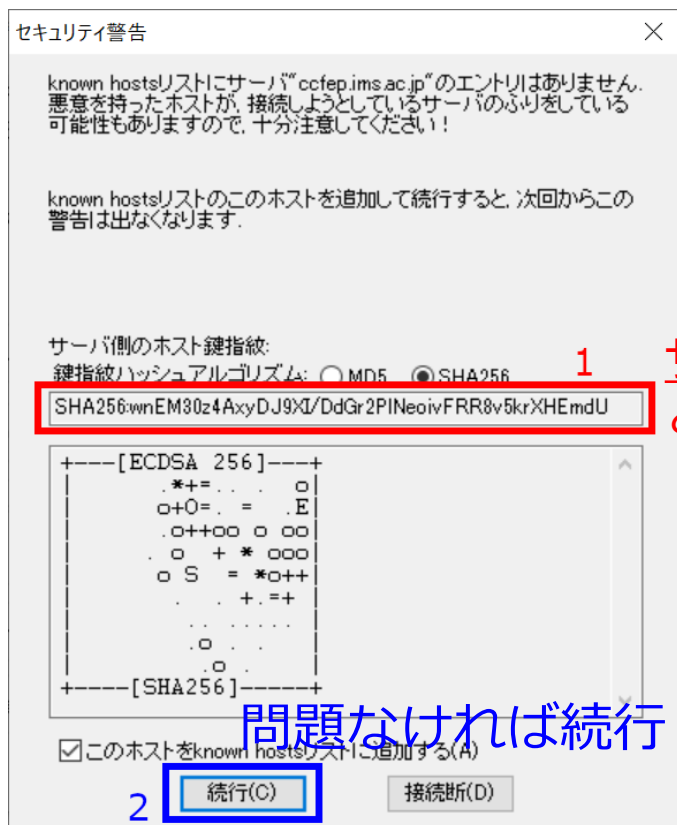
ログイン(1)

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。

有効な鍵の
fingerprint

- SHA256:wnEM30z4AxyDJ9XI/DdGr2PINeoivFRR8v5krXHEmdU
- SHA256:0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZEloIvqXvbl
- 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。

The screenshot shows the 'SSH認証' (SSH Authentication) dialog box. The title bar includes a close button (X). The main text reads 'ログイン中: ccfep.ims.ac.jp' and '認証が必要です.' (Authentication is required). The 'ユーザ名(N):' field contains 'ccfep' and is highlighted with a green box and labeled '1'. The 'パスフレーズ(P):' field contains 10 black dots and is highlighted with a red box and labeled '2'. A dropdown menu next to it is open, showing '鍵生成の際に設定した' and 'パスフレーズ'. The 'パスワードをメモリ上に記憶する(M)' checkbox is checked and highlighted with an orange box and labeled '3'. The '認証方式' (Authentication Method) section has 'RSA/DSA/ECDSA/ED25519鍵を使う' selected with a radio button, highlighted with a blue box and labeled '4a'. The '秘密鍵(K):' field contains 'id_rsa' and is highlighted with a blue box and labeled '4b'. The 'OK' button at the bottom is highlighted with a red box and labeled '5'. There is also a '接続断(D)' button.

指定された3文字のユーザアカウント
1 を指定してください

鍵生成の際に設定した
パスフレーズ
2 を入力してください

チェックを外すとよりセキュアです

クリックして有効化

4a

4b

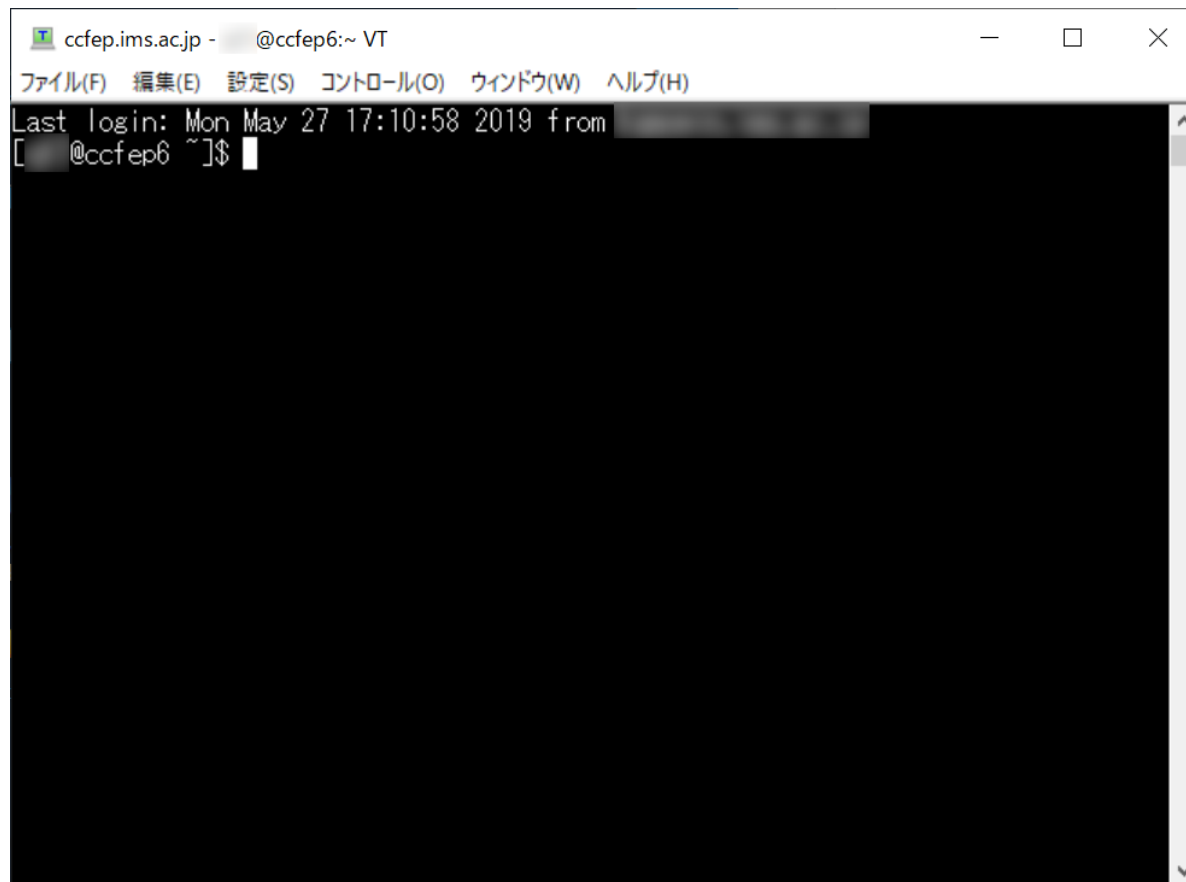
作成した秘密鍵を
指定してください

5 OK

(設定でデフォルトのユーザ名や鍵ファイルの場所を指定することもできます)

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。

A terminal window titled "ccfep.ims.ac.jp - @ccfep6:~ VT" with standard window controls. The menu bar includes "ファイル(F)", "編集(E)", "設定(S)", "コントロール(O)", "ウィンドウ(W)", and "ヘルプ(H)". The terminal output shows "Last login: Mon May 27 17:10:58 2019 from [redacted]" followed by a prompt "[redacted]@ccfep6 ~]\$" with a cursor.

```
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 ~]$
```