

SSH Key Generation (TeraTerm version)

Last Update: Jan 5, 2022 (verified with Tera Term 4.106)

Introduction

The aim of this page is to explain how to login to RCCS supercomputer using Tera Term.

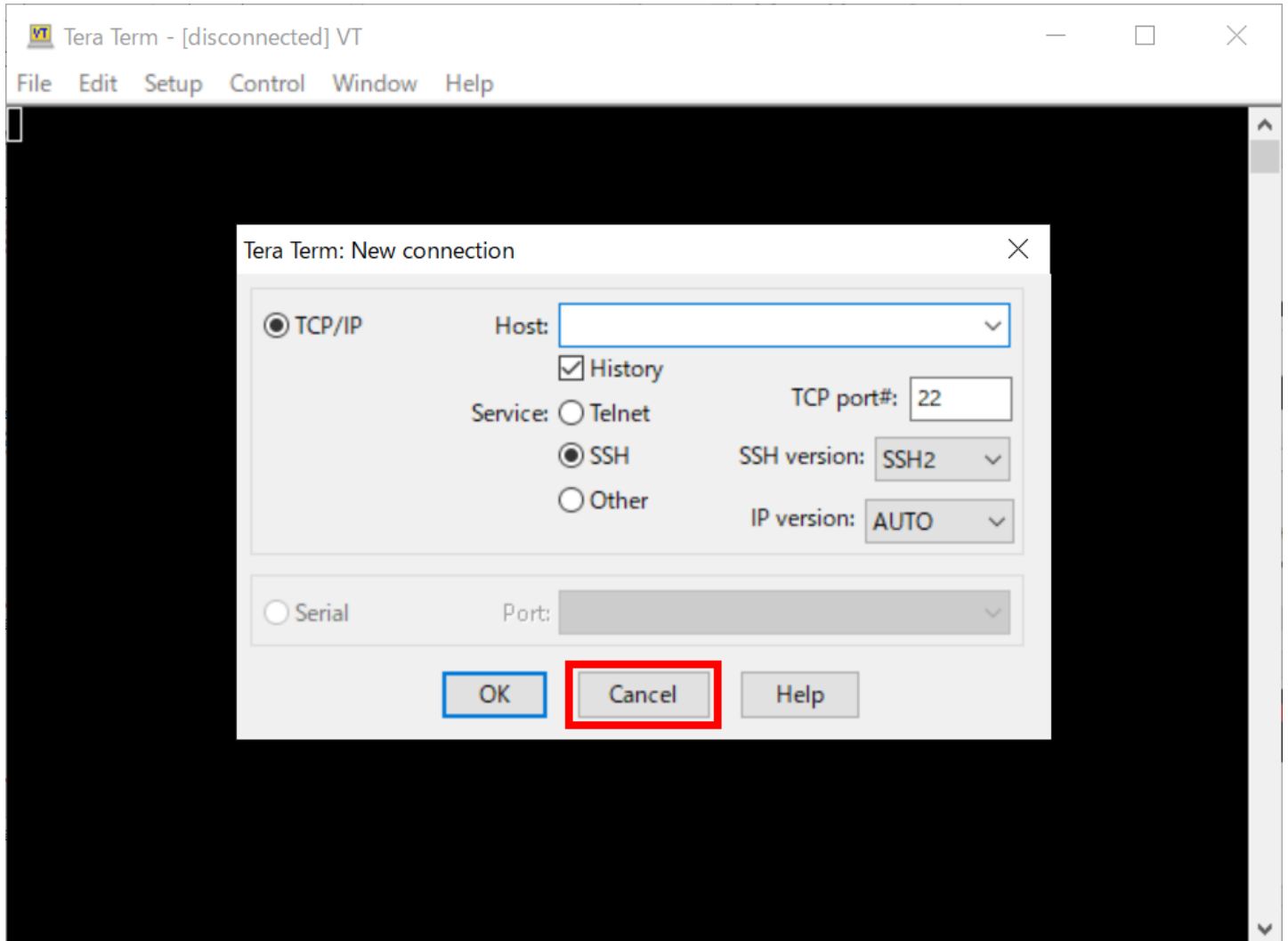
Installation of Tera Term

Tera Term can be downloaded from the following site.

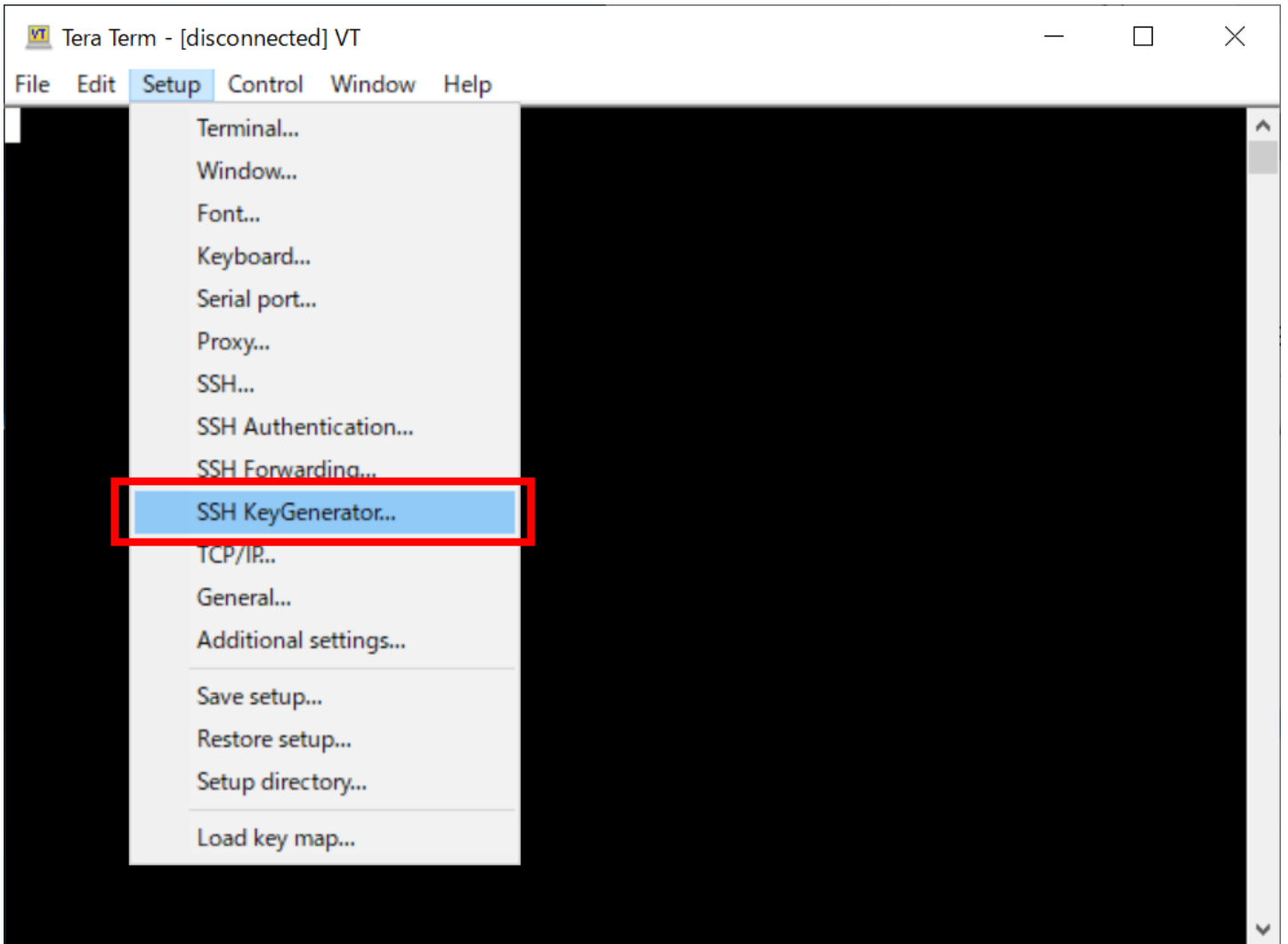
<https://ja.osdn.net/projects/ttssh2/releases>

SSH Key Generation

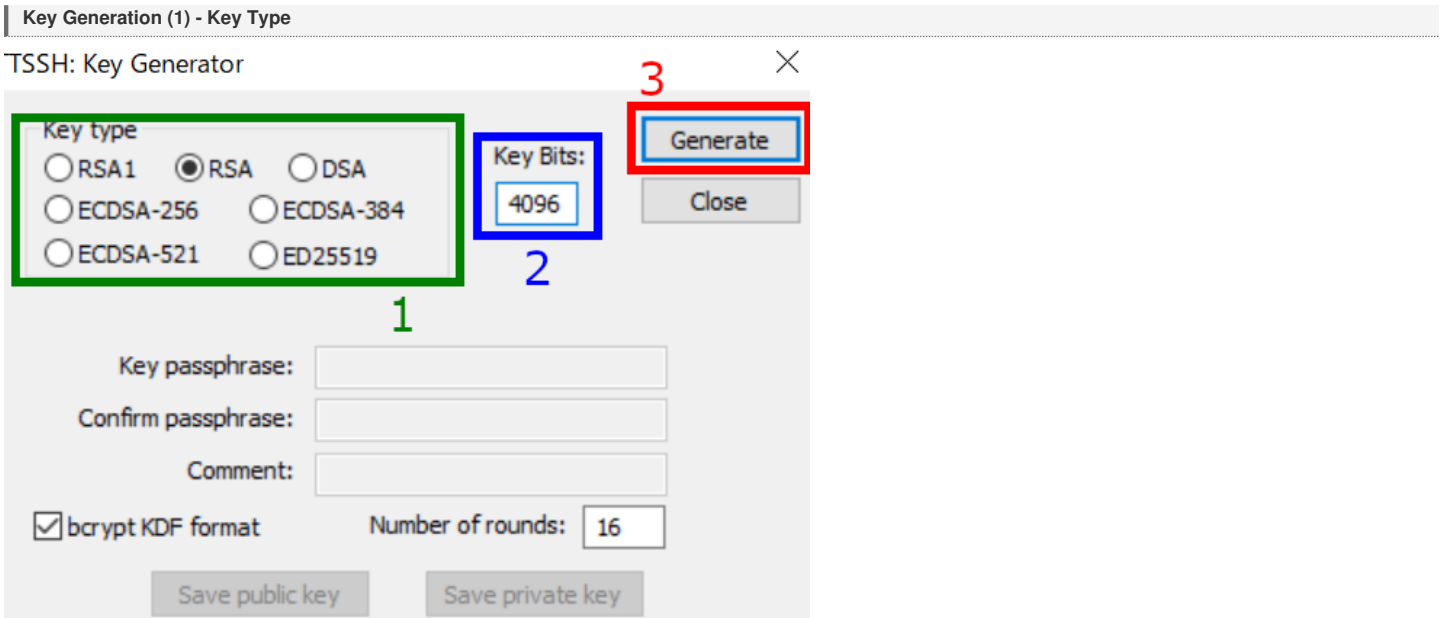
Launch Tera Term



After launching Tera Term, cancel the connection.



Then choose "SSH KeyGenerator" from "Setup" menu to generate your SSH key.



You may see SSH key generator window like above.

1. Choose Key Type

We, RCCS, recommend ED25519, ECDSA-521, ECDSA-384, ECDSA-256, and RSA 4096 bits* types of keys. If you have no preference, please try ED25519.

*Tera Term 4.105 does not support SHA2 RSA algorithms (rsa-sha2-256/512). If SHA1 algorithm (ssh-rsa) is disabled in the near future, you may have a trouble upon RSA authentication. (Those SHA2 algorithms will be available in Tera Term 4.107, though.) Note: RSA key type itself is not relating with SHA1/SHA2. You usually don't need to regenerate RSA key upon migration from SHA1 to SHA2.

2. Choose Key Bits Length (RSA only)

You can choose length of key here in case of RSA. 4096 or more is recommended.

3. Begin Key Generation

After the specification of key type (and length), click this to generate key.

Key Generation (2) - set private key passphrase and save keys

TTSSH: Key Generator

Key type: RSA1 RSA DSA ECDSA-256 ECDSA-384 ECDSA-521 ED25519

Key Bits: 256

Key passphrase:

Confirm passphrase: 1

Comment: 2

bcrypt KDF format Number of rounds:

3a 3b

After the generation of keys, you can set passphrase and comment that key.

1. Private key passphrase

You can set passphrase for private key here. We, RCCS, recommend passphrase of 10 or more characters containing 4 types of characters - "lower-case", "upper-case", "number", and "symbol".

2. Set a comment (optional)

If you are using (or planning to use) more than one key, adding appropriate comment maybe helpful to you.

3. Save public and private keys

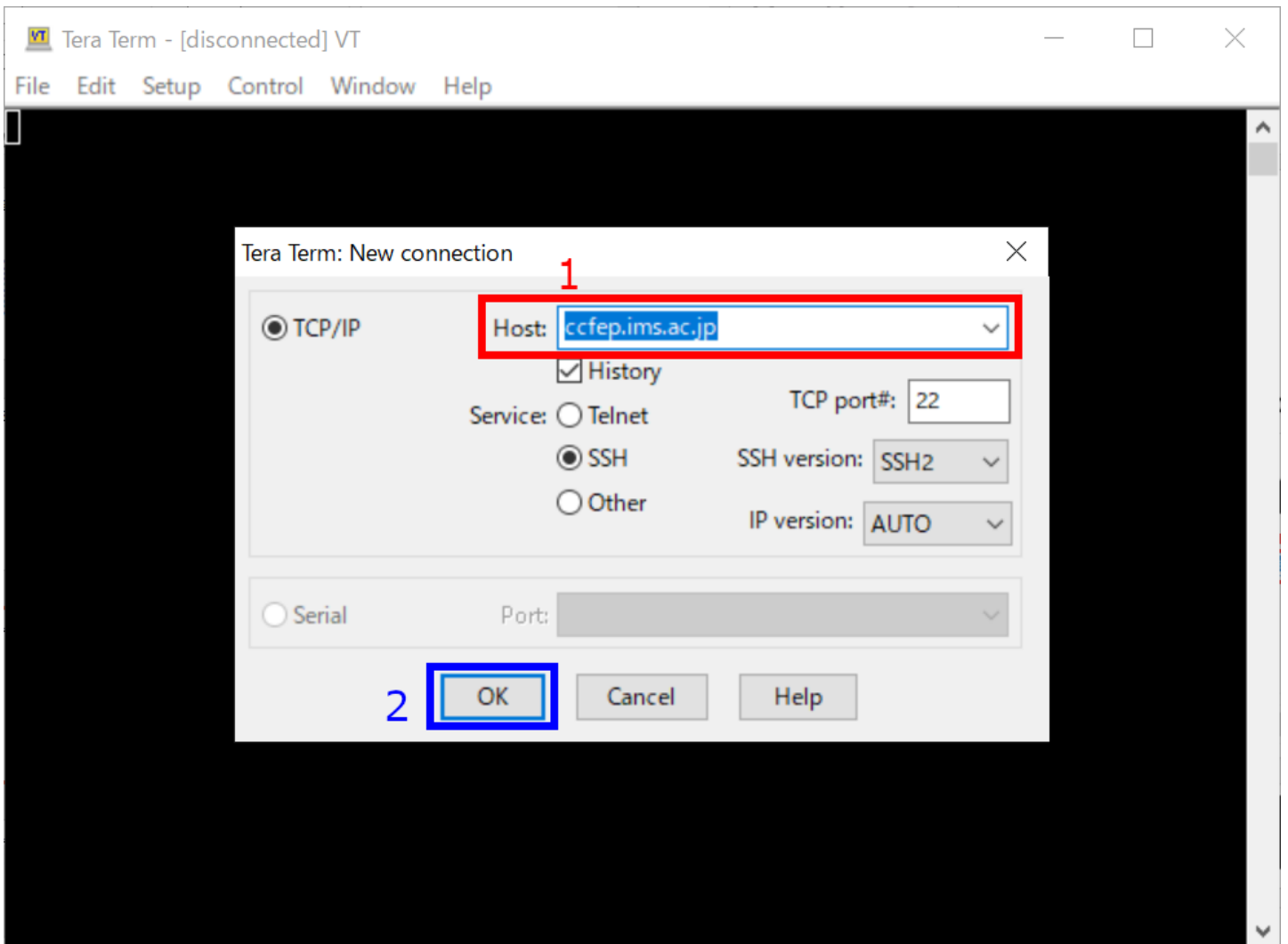
Click buttons 3a and 3b to save public and private keys, respectively.

Register Public Key (Common)

You need to register the public key before login. Please register your public key according to the instructions in <https://ccportal.ims.ac.jp/en/account>.

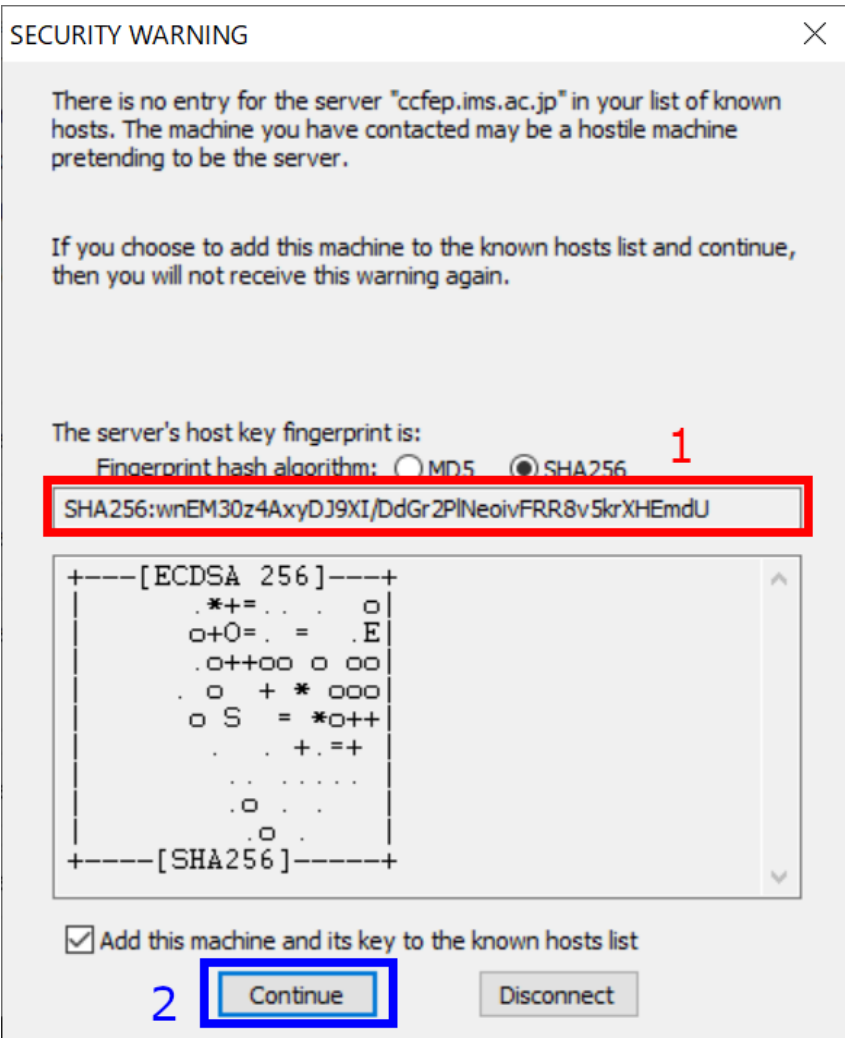
Login

preparations



Restart Tera Term or select "New connection" from "File" menu to go back to first window. Type `ccfep.ims.ac.jp` in Host: textbox and then click OK to proceed.

Security Alert upon first Connection



You may see warning dialog like above upon first connection. Please check the fingerprint of the server (1). It must match with either of the fingerprint in the list below.

- ▶ 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/kBee1pAukyKwenEwXjtPxr9ZEloIfVqXvbl (SHA256)
- ▶ Nhg+9Lgj3XeuW//A/j7jqgUJllxWehryCtStlp1Dir (SHA256)

Click "Continue" (2) if the fingerprint is valid.

Input Login Information

SSH Authentication

The screenshot shows the 'SSH Authentication' dialog box for logging into 'ccfep.ims.ac.jp'. The dialog is titled 'Authentication required.' and contains the following elements:

- 1**: A green box highlights the 'User name:' text box.
- 2**: A red box highlights the 'Passphrase:' text box, which contains several black dots.
- 3**: An orange box highlights the 'Remember password in memory' checkbox, which is checked.
- 4a**: A blue box highlights the radio button for 'Use RSA/DSA/ECDSA/ED25519 key to log in'.
- 4b**: A blue box highlights the 'Private key file:' text box, which contains the text 'id_rsa' and a browse button ('...').
- 5**: A red box highlights the 'OK' button at the bottom right.

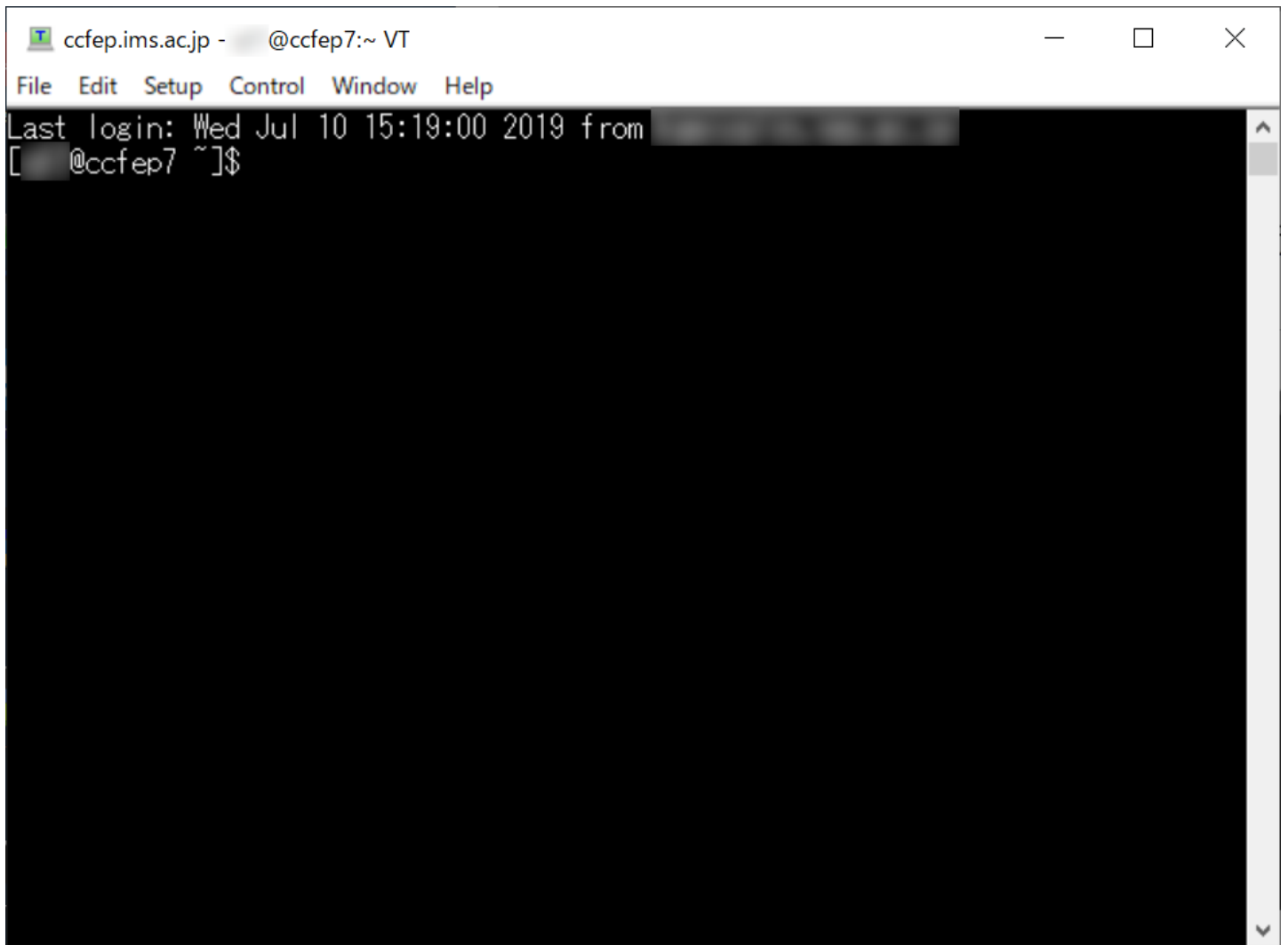
Other visible elements include the 'Forward agent' checkbox (unchecked), the 'Authentication methods' section with radio buttons for 'Use plain password to log in', 'Use rhosts to log in (SSH1)', 'Use keyboard-interactive to log in', and 'Use Pageant to log in'. The 'Disconnect' button is also visible at the bottom right.

You need to input username, private key file path etc. in this window.

1. Your user account name given by RCCS (three-letter ID)
2. Input the passphrase of the private key.
3. (optional) Uncheck to improve security.
4. Check that item (4a) and then input private key file location.
5. Finally, click OK to proceed.

(You can set default user name and authentication method including private key location in "Setup" -> "SSH Authentication".)

Login Completed!

A terminal window titled "ccfep.ims.ac.jp - @ccfep7:~ VT" with a menu bar containing "File", "Edit", "Setup", "Control", "Window", and "Help". The terminal output shows a successful login message: "Last login: Wed Jul 10 15:19:00 2019 from [redacted]". Below this, the prompt "[redacted]@ccfep7 ~]\$" is visible. The rest of the terminal area is black, indicating that the user has successfully logged in and the session is active.

```
ccfep.ims.ac.jp - @ccfep7:~ VT
File Edit Setup Control Window Help
Last login: Wed Jul 10 15:19:00 2019 from [redacted]
[redacted]@ccfep7 ~]$
```

If everything works fine, you will successfully login to the frontend server.