Ed25519 での設定例

ここでは、Ed25519 形式の鍵を使ってログインする場合の概略を示します。
操作自体は Windows の PowerShell や Mac の Terminal.app や Linux の各種ターミナルで基本的に共通です。
赤文字は実際に入力する文字列です。青文字は注釈です。user や hostname を含む一部の表記は環境に依存します。

まず、鍵を新規に作成します。

```
user@hostname ~ %ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/user/.ssh/id_ed25519): (デフォルトで良ければ Enter を入力)
Enter passphrase (empty for no passphrase): (パスワードを入力します)
Enter same passphrase again: (パスワードを入力します)
Your identification has been saved in /Users/user/.ssh/id_ed25519 (秘密鍵ファイル)
Your public key has been saved in/Users/user/.ssh/id_ed25519.pub (公開鍵ファイル)
The key fingerprint is:
SHA256:****************************************** user@hostname.domain
The key's randomart image is:
+--[ED25519 256]--+
|             |
|             |
|             |
|             |
|   (省略)    |
|             |
|             |
|             |
|             |
+----[SHA256]-----+
user@hostname ~ %
```

ここで作成された公開鍵 ~/.ssh/id_ed25519.pub (/Users/user/.ssh/id_ed25519.pub) の情報をこちらのページの案内にしたがってアップロードします。
鍵ファイルの作成された場所については上記のログ中に記述がありますので、それをご確認ください。
公開鍵ファイルは一行のテキストファイルです。ファイルそのものではなく、その内容をアップロードします。
秘密鍵ファイル(ここでは ~/.ssh/id_ed25519)は絶対にアップロードしてはいけません。

なお、ここで作成した鍵は WinSCP, cyberduck, FileZilla などのソフトで接続する際に利用することもできます。

公開鍵のアップロードが完了したら実際にログインしてみます。

```
user@hostname ~ %ssh uid@ccfep.ims.ac.jp (uid は RCCS 指定の三文字のアカウント名です(例: xxx))
The authenticity of host 'ccfep.ims.ac.jp (133.48.230.13)' can't be established.
ED25519 key fingerprint is SHA256:0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI. (別のものが表示される場合があります)
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?yes (初回ログイン時のみ必須です)
Warning: Permanently added 'ccfep.ims.ac.jp' (ED25519) to the list of known hosts.
Enter passphrase for key '/Users/user/.ssh/id_ed25519': (上で設定したパスワードを入力します)
[uid@ccfep* ~]$ (正しくパスワードを入力できればログインが完了します)
```

二度目以降のログインではパスフレーズの入力以外の部分は出力されません。

Tips

補足情報です。

ホスト署名

上記 *** key fingerprint is 以下には以下のどれかが表示されます。

- 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/j7jqgUJlIxWehryCtStIp1Dir (SHA256)

設定ファイル(~/.ssh/config)の活用

~/.ssh/config に以下のような設定を書くことで ssh ccfep だけでログインできるようにすることも可能です。
uid は自身の三文字 ID に置き換えてください。(複数の鍵がある場合には IdentityFile も指定する必要があるかもしれません。)

```
Host ccfep
  HostName ccfep.ims.ac.jp
  User uid
```