SSH公開鍵のRSA暗号からED25519暗号への移行

概要

新しいOS(Ubuntu22.04、RHEL9系等)では旧来のRSA暗号で生成した鍵でのSSH公開鍵認証が行えないため、より暗号強度が高いed25519暗号により生成した鍵への移行をお願いいたします。

本ページではSSH公開鍵のRSA暗号からed25519暗号への移行手順を記載します。

ed25519アルゴリズムで暗号化した秘密鍵・公開鍵の生成方法

II ;にログインの上、秘密鍵・公開鍵を生成します。

ssh-keygenコマンドのオプションで -t ed25519 を指定することでed25519アルゴリズムで暗号化した秘密鍵・公開鍵を生成できます。

```
$ ssh-keygen -t ed25519
```

コマンドが正常に完了すると、それぞれ以下の鍵ファイルが生成されます。

- 秘密鍵: /home/USER/.ssh/id_ed25519
- 公開鍵: /home/USER/.ssh/id_ed25519.pub

生成した公開鍵はstarsの~/.ssh/authorized_keysに登録します。

```
$ cat ~/.ssh/id_ed25519 >> ~/.ssh/authorized_keys
```

生成した秘密鍵はお使いのMac/Windowsにコピーし、その秘密鍵でSSHログインできることを確認してください。

秘密鍵・公開鍵の生成はTeratermなどのソフトウェアの機能で生成したものでも問題ありません。

生成した公開鍵の配布方法

各サーバへのログインに生成した公開鍵をログインしたい場合は、サーバにssh-copy-idコマンドで配布します。

```
$ ssh-copy-id -i ~/.ssh/id_ed25519.pub <target_host>
```

【必要に応じて】ユーザ設定ファイルの変更

~/.ssh/config でSSHログイン時に使用する秘密鍵ファイルを指定している場合は修正します。

```
Host rdfp03
  Hostname rdfp03
  User monkpod
  IdentityFile ~/.ssh/id_ed25519
```