

UNIXサーバー構築

第6章 SSHサーバ

SSH (Secure Shell) とは？

■ リモートアクセス

遠隔地など離れた場所からサーバを操作すること。リモートアクセスでよく使用されるプロトコルとしてtelnetやSSHがあげられる。

■ telnet

以前はリモートアクセスに使用されることが多かった、データを暗号化せず送信するためあまり使用されない。

■ **SSH** (Secure Shell)

リモートアクセスに使用される。**データを暗号化**するため使用されることが多い。ポート番号22を使用する。

SSHサーバの設定ファイル

UbuntuではデフォルトSSHサーバは動作していないのでopenssh-serverのインストールが必要となる。

■ SSHサーバのインストール

```
sudo apt install -y openssh-server
```

■ SSHサーバの起動

```
sudo systemctl start ssh
```

```
sudo systemctl enable ssh
```

SSHサーバの設定

SSHの設定ファイル

/etc/ssh/**sshd**_config * 類似したファイル名があるので注意すること。

設定項目	設定内容
PermitRootLogin	rootでの直接ログインの設定 noで拒否。yesで許可
PermitEmptyPasswords	空パスワードの場合の処理。noにして空パスワードを禁止する。
Port	ポート番号を指定する。デフォルトは22。
AllowUsers	ログインできるユーザーを限定する

SSHサーバの設定(鍵認証)

鍵認証の設定項目

設定項目	設定内容
PasswordAuthentication	デフォルトではパスワードのログインが許可されている。鍵を使用する場合はno

■鍵の作成

鍵の作成はUNIXサーバー上でも作成できますが、今回はTeraTermで鍵(公開鍵、秘密鍵)の作成を行います。

■鍵の置き場所(鍵の作成は別紙参照)

公開鍵・・・サーバー、秘密鍵・・・クライアント