OpenSSH とは

OpenSSH とはOpenBSD のメンバーがフリーなライセンスでリリースした SSH です。

SSH とは

安全でない cyber network上でネットワークサービスを安全に運用するための通信手段（プロトコル）の 1つです(https://en.wikipedia.org/wiki/Secure_Shell 参照)。 現在(2020年)、本システムでは SSH2 プロトコルでの公開鍵暗号方式を用いた認証(公開鍵認証)を標準とし、特に、ECDSA電子署名を利用することを推奨しています。

なぜ利用申請時に SSH公開鍵が必要なのか?

本システムではアカウントに password を発行しないため。 利用者は、 手元の PC ではできない高速計算や大容量データ処理などを目的に server にログインshell を要求しているはずですが、 本システムでは server ログイン時の利用者の認証において、旧来の password を用いておりません SSH公開鍵認証を用いております。 またpassword の安全な受け渡しや password 紛失時の対応が困難となっていることも背景にあります。

SSH公開鍵認証とは

公開鍵認証(public key authentication)は、ゼロ知識証明(相手に知識を一切与えることなくある命題が正しいことを証明する手段)の一種です。 最初に、利用者は、自分の秘密鍵と公開鍵の対を作ります。 秘密鍵は自分のローカルホスト(最も信頼される端末)においておき、公開鍵は何らかの信頼される方法を使って、ログイン先の server に設置します。 利用者が自分の端末から serverに SSH login するまでの過程は次のようになります。

1. 最初に端末と server の間に暗号化された通信路が確立されます。
2. serverは「チャレンジ」と呼ばれるデータを生成し、それを server上に置かれた利用者の公開鍵を用いて暗号化し、端末に送ります。
3. 端末は、受け取った暗号を利用者の秘密鍵を用いて復号化し、その答えを server に返します。
4. serverは、その答えが合っていれば、その利用者に login を許可します。

Windows 10 OpenSSH に戻る

From:
https://portal.isee.nagoya-u.ac.jp/stel-it/ - **STEL-IT wiki**

Permanent link:
https://portal.isee.nagoya-u.ac.jp/stel-it/doku.php?id=public:about_openssh

Last update: **2020/04/21 17:24**