

SSHの仕組み

SSHの仕組み

サーバサイド班 甲本健太 ↗

目次

- SSHとは
 - SSH接続の流れ
 1. クライアントによるサーバの認証
 2. セッションキーの生成
 3. サーバによるクライアントの認証
- SSHのログを見てみよう
- (おまけ) RSAとECDSA
- 参考

SSHとは

SSHとは**Secure Shell**（安全なシェル）の略称であり、安全にリモートコンピュータと接続するためのプロトコル。

- ・ サーバに接続して作業するときなどに利用する



実演

```
$ ssh -i {秘密鍵}
```

SSH接続の流れ

認証段階

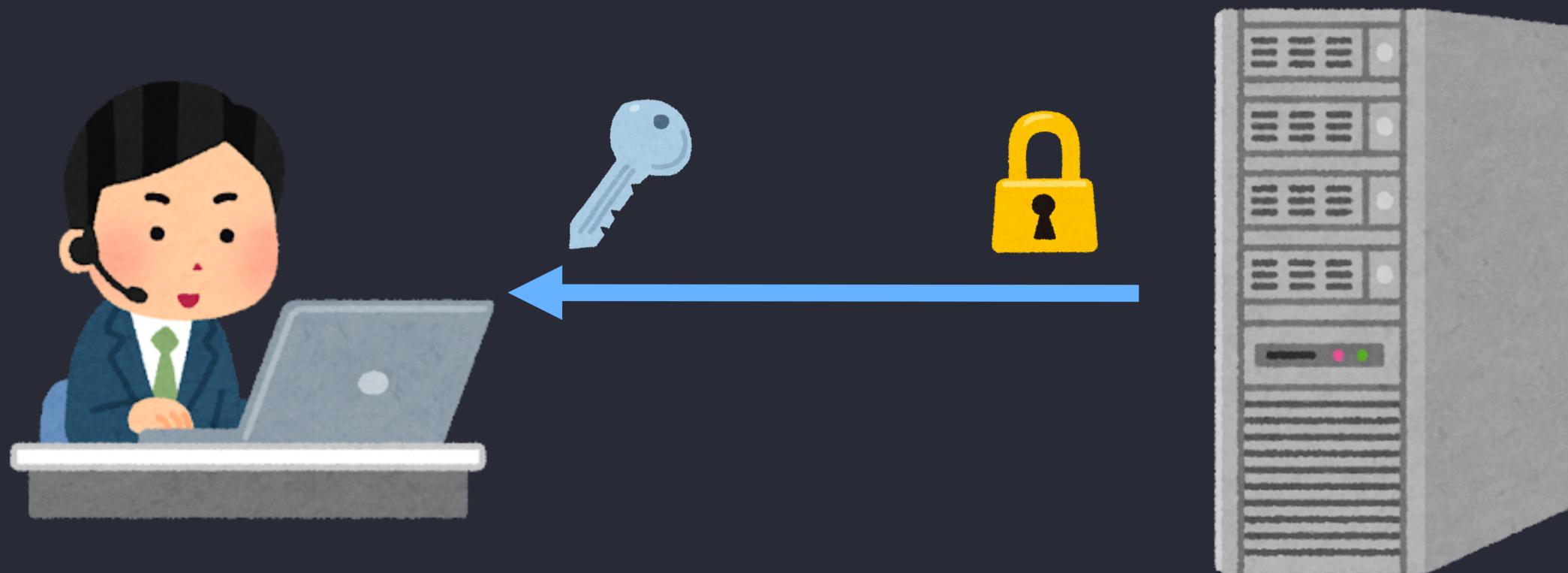
1. クライアントによるサーバの認証
 2. セッションキーの生成
 3. サーバによるクライアントの認証
-

通信段階

4. データを暗号化して通信

1. クライアントによるサーバの認証

クライアント側が、サーバが怪しいものでないかを調べる



初めてサーバにアクセスするとき

サーバの公開鍵を検証し、手動で検証を行う

→ Are you sure you want to continue connecting (yes/no) ?

ローカルの `known_hosts` ファイルにその情報を保存する。

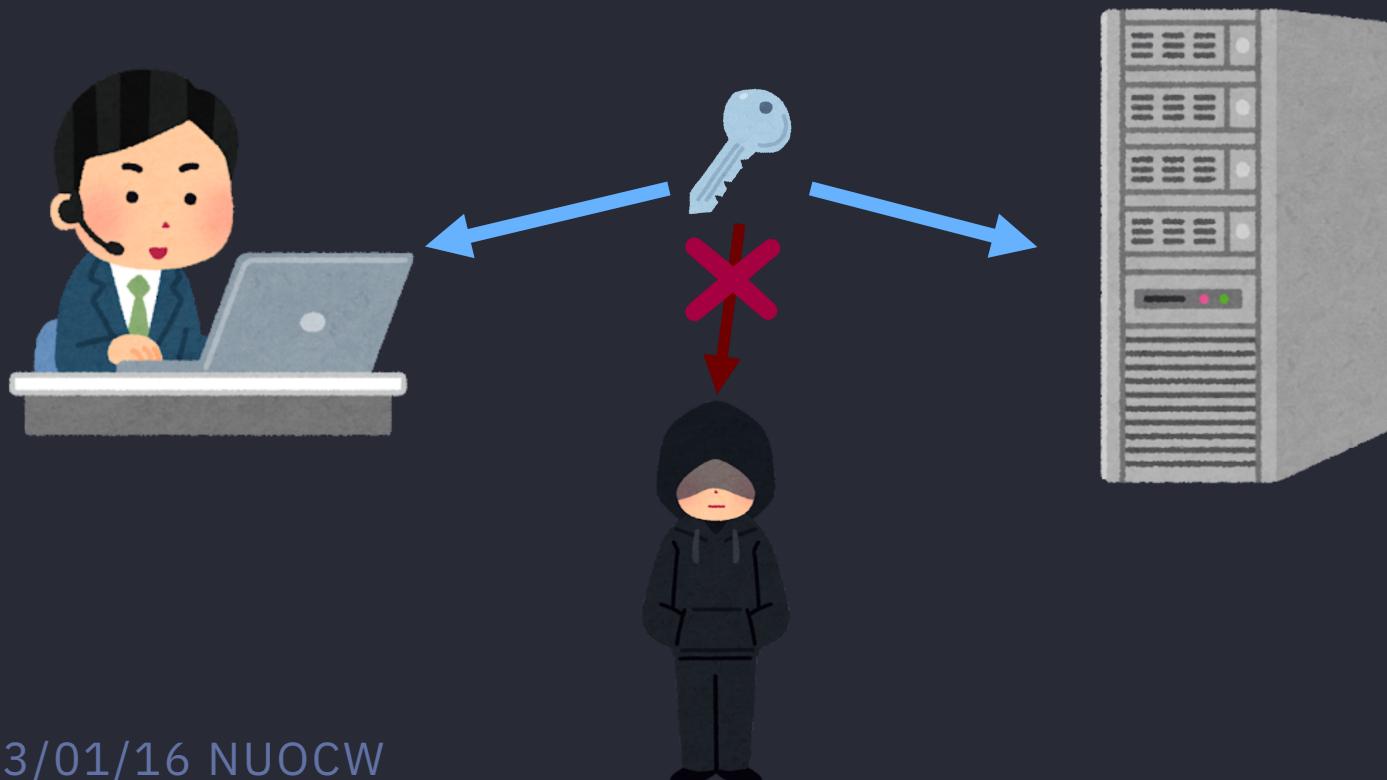
2回目以降

ローカルの `known_hosts` にある公開鍵情報からサーバの身元を確認

2. セッションキーの生成

通信の暗号化をするための鍵を生成する。

ディフィー・ヘルマンの鍵交換を用いて、中間者攻撃に対処



3. サーバによるクライアントの認証

サーバ側が、正しいクライアントに接続しているかを調べる



クライアント認証の流れ

1. 鍵ペア（公開鍵、秘密鍵）を生成する
2. サーバ側に公開鍵を渡す
3. サーバがトークン（乱数）をクライアントに送る
4. 自分の秘密鍵を用いてトークンを暗号化する
5. 暗号化したトークンをサーバに送る
6. 自分の持っている公開鍵でトークンを復号する
7. 復号結果と、送られたトークンが一致すれば成功

c.f. 電子署名

SSHのログを見てみよう

`ssh` コマンドに `-v` オプションをつけると接続の際のログを確認できる

```
+ Powell ~
; ssh ocv.nagoya-u.jp pub3
OpenSSH 9.0p1, LibreSSL 3.3.6
debug1: Reading configuration data /etc/ssh/config
debug1: /etc/ssh/config line 19: Applying options for _ocv_pub3
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 21: include /etc/ssh/ssh_config.d/* matched no files
debug1: /etc/ssh/ssh_config line 54: Applying options for *
debug1: /etc/ssh/ssh_config line 55: Applying provider $SSH_SK_PROVIDER did not resolve; disabling
debug1: Connecting to ocv.nagoya-u.jp port 22.
debug1: Connection established.
debug1: identity file /etc/ssh/id_rsa type 0
debug1: identity file /etc/ssh/id_rsa-cert type 1
debug1: Local version string SSH-2.0-OpenSSH_9.0
debug1: Remote protocol version 2.0, remote software version OpenSSH_8.2p1 Ubuntu-4ubuntu0.5
debug1: Connecting to ocv.nagoya-u.jp port 22.
debug1: Authenticating to ocv.nagoya-u.jp:22 as 'root'
debug1: load hostkeys: fopen /etc/ssh/known_hosts: No such file or directory
debug1: load hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: Kex algorithm: curve25519-sha256,
debug1: Kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: host key: /etc/ssh/ssh_host_ed25519 SHA256:0Lp0fjOhfQm9M2EybfedMnqYV8m1keK6+rnumQ0Q
debug1: load hostkeys: fopen /etc/ssh/known_hosts: No such file or directory
debug1: load hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: Host 'ocv.nagoya-u.jp' is known and matches the ED25519 host key.
debug1: Found key in /etc/ssh/known_hosts:13
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 134217728 blocks
debug1: get_agent_identities bound agent to hostkey
debug1: get_agent_identities ssh_fetch_identitylist: agent contains no identities
debug1: SSH2_MSG_EXT_INFO received
.debug1: /ssh/id_rsa RSA SHA256:TkmBirfsbEWQSBe4e3Iczs2o78Dy03IsCq60uj4co explicit
.debug1: SSH2_MSG_EXT_INFO received
.debug1: server-sig-algs=<ssh-ed25519,sk-ssh-ed25519@openssh.com,ssh-rsa,rsa-sha2-256,rsa-sha2-512,ssh-dss,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ecdsa-sha2-nistp256@openssh.com>
.debug1: SSH2_MSG_SERVICE_ACCEPT received
.debug1: Authentications that can continue: publickey
.debug1: Next authentication method: publickey
.debug1: Offering public key: /ssh/id_rsa RSA SHA256:TkmBirfsbEWQSBe4e3Iczs2o78Dy03IsCq60uj4co explicit
.debug1: /ssh/id_rsa RSA SHA256:TkmBirfsbEWQSBe4e3Iczs2o78Dy03IsCq60uj4co explicit
Authenticated to ocv.nagoya-u.jp ([133.6.120.68]:22) using "publickey".
.debug1: Requesting no-more-sessions@openssh.com
.debug1: Entering interactive session.
.debug1: pledge: filesystem
.debug1: client_input_global_request: rtype hostkeys-0@openssh.com want_reply @
.debug1: client_input_hostkeys: searching ./.ssh/known_hosts for ocv.nagoya-u.jp / (none)
.debug1: client_input_hostkeys: searching ./.ssh/known_hosts2 for ocv.nagoya-u.jp / (none)
.debug1: client_input_hostkeys: hosts file ./.ssh/known_hosts2 does not exist
.debug1: client_input_hostkeys: host key found matching a different name/address, skipping UserKnownHostsFile update
.debug1: Remote: /ssh/authorized_keys:1 key options: agent-forwarding port-forwarding pty user-rc x11-forwarding
.debug1: Remote: /ssh/authorized_keys:1 key options: agent-forwarding port-forwarding pty user-rc x11-forwarding
.debug1: Sending environment.
.debug1: channel 0: setting env LC_TERMINAL_VERSION = "3.4.19"
.debug1: channel 0: setting env LANG = "ja_JP.UTF-8"
.debug1: channel 0: setting env LC_TERMINAL = "lTerm2"
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-132-generic x86_64)
```

(おまけ) RSAとECDSA

- RSA
 - 素因数分解ベースの暗号
- ECDSA
 - 楕円関数上での離散対数問題

参考

- Secure Shell (Wikipedia)

https://ja.wikipedia.org/wiki/Secure_Shell

- OpenSSH (公式)

<https://www.openssh.com/>

- Understanding SSH Workflow

<https://medium.com/@hellomudit/understanding-ssh-workflow-66a0e8d4bf65>