最近のOpenSSHの話

小谷　大祐

daisuke at kotachi.com

2008/7/12

今日のはなし

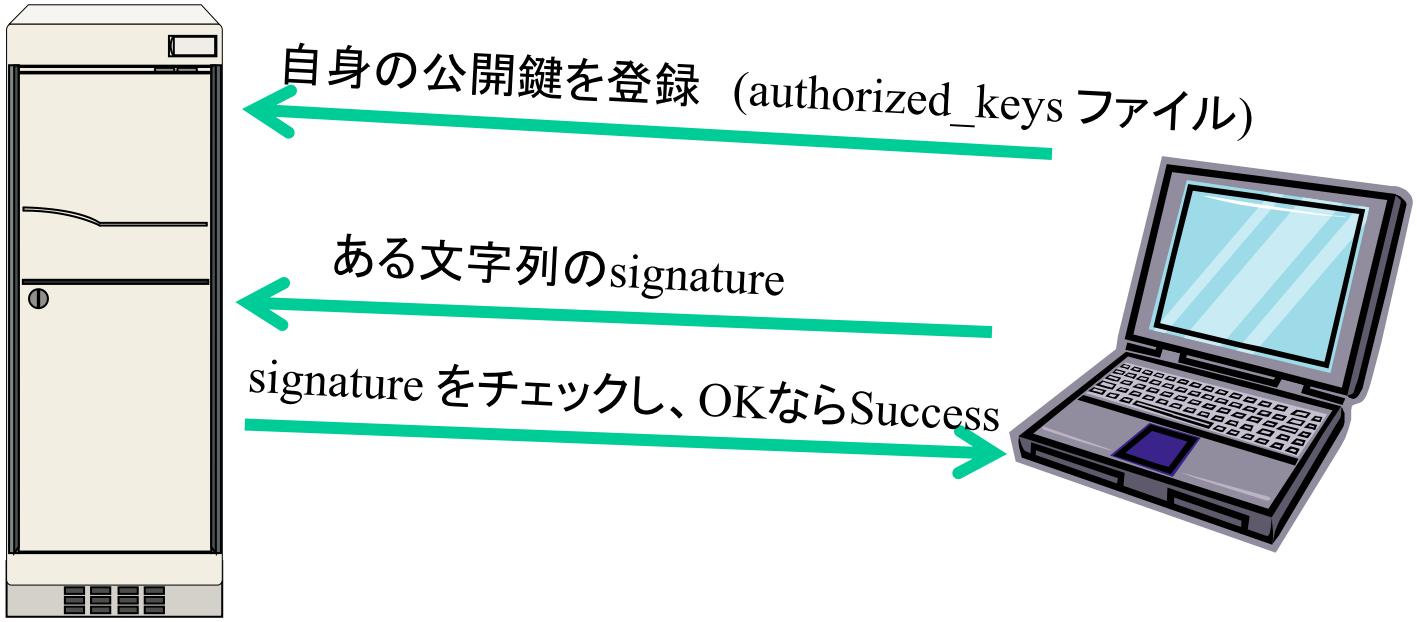
- ちょっとだけ関係あります。

Nov 30 16:10:25 localhost sshd[8986]: Invalid user college from **.***.**.***
Nov 30 16:10:31 localhost sshd[8999]: Invalid user hydra from **.***.**.***
Nov 30 16:10:40 localhost sshd[9004]: Invalid user work from **.***.**.***
Nov 30 16:10:45 localhost sshd[9006]: Invalid user smmsp from **.***.**.***
Nov 30 16:10:51 localhost sshd[9008]: Invalid user jack from **.***.**.***
Nov 30 16:10:57 localhost sshd[9010]: Invalid user jerry from **.***.**.***
Nov 30 16:11:03 localhost sshd[9012]: Invalid user bb from **.***.**.***
Nov 30 16:11:08 localhost sshd[9014]: Invalid user zzz from **.***.**.***
Nov 30 16:11:14 localhost sshd[9016]: Invalid user natasha from **.***.**.***
Nov 30 16:11:20 localhost sshd[9018]: Invalid user elena from **.***.**.***
Nov 30 16:11:26 localhost sshd[9020]: Invalid user lspeed from **.***.**.***

公開鍵認証のススメ

- ssh へのブルートフォースがすごい
  - 毎日確実に来る。
- hostごとにパスワードを覚える必要がない
- 共有アカウントでもパスワードまで共有する必要がない
- ちなみに、RFC4252的には必須
  - Password はoptional

公開鍵認証とは



RemoteHost

Client

Reference: RFC4252

実際の話

- 公開鍵認証のみの設定に踏み切るのは難しい
  - 「俺は鍵持ち歩きたくねぇ！」
  - 「鍵作るの面倒くせぇ！」
  - 「どのPC端末からでも入りたい」
  - 他の管理者のレベルがそこまで高くない

今日のはなし

- 条件別に　PasswordAuthentication yes/no を制御する方法
- あと面白そうなものの紹介

Matchオプション

- OpenSSH 4.4～
- User, Group,Host,Address単位で
  - PasswordAuthentication [yes/no]
  - PermitRootLogin(4.8～)
  - AllowTcpForwarding　[yes/no](ポート転送）
- などを設定可能に

Matchオプションの使い道

- 組織内はパスワード認証OK,組織外不可
- 組織内/外で PermitRootLogin の扱いを変える

- ChrootDirectory, ForceCommandを使って sftp only user の自由度を制限
  - いまのところ使いづらいけど^^;

Matchオプションの書き方

Match (条件1）

　条件1に合致した場合の設定

Match (条件2)

　条件2に合致した場合の設定

注意！Host/Address で CIDRのaddress/mask の形で指定することはできない

×Match Address 192.168.0.0/24

Match オプションの例1

- matcha139 ユーザのみパスワード認証許可

```
PasswordAuthentication no
Match User matcha139
    PasswordAuthentication yes
```

Match オプションの例2

- *.example.jp, 192.168.0.0/24 からのみパスワード認証許可

```
PasswordAuthentication no
Match Host *.example.jp
    PasswordAuthentication yes
Match Host 192.168.0.*
    PasswordAuthentication yes
```

Matchオプションの例3

- matcha139ユーザはsftpのみ

```
Subsystem internal-sftp
Match User matcha139
    ForceCommand internal-sftp
```

その他

- ChrootDirectory
  - chroot
  - chroot 先の permission 等に制限あり

おしまい