01_Linuxサーバデータベース - Fail2Banによる不正アクセスからの保護

概要

fail2banを導入し、不穏なアクセスからサーバを保護します。

どういう保護を行うか

1. Ubuntu系の標準ファイアウォールufwと連携します
2. ufwが検知した不審なアクセス元は恒久的にアクセスを禁止します
3. sshdに関しては接続3回失敗で恒久的にアクセスを禁止します

参考記事:
https://blog.fernvenue.com/archives/ufw-with-fail2ban/

前提：

まっさらな状態で(上記手段でアンインストールした上で)

sudo aptitude install fail2ban

を実行した状態とします。

手順

ここからはroot権限の方が確実です。

jail.localを編集します。

教義・信仰に沿ったエディタで以下のファイルを編集(作成)します。

- ファイル名 /etc/fail2ban/jail.local

○内容

```
[ufw]
enabled=true
filter=ufw.aggressive
action=iptables-allports
logpath=/var/log/ufw.log
maxretry=1
bantime=-1
ignoreip =  127.0.0.0/8  ::1
#  ignoreipは任意の(自分のアクセス元)を指定ください

[sshd]
enabled=true
filter=sshd
mode=normal
port=22
protocol=tcp
logpath=/var/log/auth.log
maxretry=3
bantime=-1
ignoreip =  127.0.0.0/8  ::1
#  ignoreipは任意の(自分のアクセス元)を指定ください
```

- ファイル名 /etc/fail2ban/filter.d/ufw.aggressive.conf

○内容

```
[Definition]
failregex = [UFW  BLOCK].+SR=<HOST>  DST
ignoreregex =
```

設定反映

```
systemctl enable fail2ban
systemctl  start  fail2ban
systemctl  statsu  fail2ban
```

これで、不審なアクセスは次回以降は有無を言わせずブロックする設定となります。

ファイル

O_春節でパソコンを使うお姉さん2024010507(ftmm).jpg	225 KB	2024/01/05	手動人形