接続する回数を制限する

http://www.atmarkit.co.jp/ait/articles/1007/14/news102.html

ipt_recent を使う

http://www2s.biglobe.ne.jp/~nuts/labo/inti/ipt_recent.html

各 IP アドレスからのアクセスを抑えて、大量の IP アドレスからアクセスされ場合、
この方法ではうまく弾けない。

ipt_recent

・指定した条件にマッチしたパケットの source IP アドレスを、リストに記録する
・「パケットの source IP アドレスがリスト中に存在したら」という条件を使えるようにする

サンプルスクリプト

```
#!/bin/bash
IPTABLES=/sbin/iptables

$IPTABLES -F
$IPTABLES -X
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT

$IPTABLES -N Attacker
 $IPTABLES -A Attacker -m recent --set --name attacker -j LOG --log-level warn --log-prefix
'Attaker:'
$IPTABLES -A Attacker -j DROP

$IPTABLES -A INPUT -p tcp -m state --state NEW -m recent --rcheck --seconds 600 --name attacker -j
DROP

$IPTABLES -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name PreAttacker
 $IPTABLES -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60
--hitcount 5 --rttl --name PreAttacker -j Attacker

$IPTABLES -A INPUT -p tcp --dport 80 -m state --state NEW -m recent --set --name PreAttacker
 $IPTABLES -A INPUT -p tcp --dport 80 -m state --state NEW -m recent --update --seconds 10
--hitcount 10 --rttl --name PreAttacker -j Attacker
```

解説

1. ポート 22 と 80 にアクセスが合った場合に「PreAttacker」リストに IP を追加する
2. ポート 22 と 80 にアクセスが合った場合に「PreAttacker」リストからある条件にマッチするアクセスを行なっている IP アドレスを探す
3. もし、条件にマッチする IP アドレスがある場合は、その IP アドレスを「attacker」リストに追加する
4.「attacker」リストにある IP アドレスからのアクセスは 600 秒間ドロップする

IP アドレスで制御する

特定の国からのアクセスを制御する

■サンプル

```
ZONE_FILE_URL="http://www.ipdeny.com/ipblocks/data/countries"
#for IP in $(wget -O - ${ZONE_FILE_URL}/{cn,tw,kr,ru}.zone | grep -v "^#|^$" )
for IP in $(wget -O - ${ZONE_FILE_URL}/cn.zone | grep -v "^#|^$" )
do
  iptables -A INPUT -s $IP -j DROP
```

```
done
```

特定の国からのアクセスのみを受け付ける

■サンプル（日本のみ許可）

```
#!/bin/sh

IPLIST=cidr.txt

# 初期化をする
iptables -F                     # Flush
iptables -X                     # Reset
iptables -P INPUT DROP         # 受信はすべて破棄
iptables -P OUTPUT ACCEPT       # 送信はすべて許可
iptables -P FORWARD DROP        # 通過はすべて破棄

# サーバーから接続を開始した場合の応答を許可する。
iptables -A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -s 127.0.0.1 -j ACCEPT

if [ -z "$1" ]; then
  date=`date -d '1 day ago' +%Y%m%d`
else
  date="$1"
fi

if [ -e $IPLIST ]; then
    mv $IPLIST "${IPLIST}_${date}"
fi

# 最新の IP リストを取得する
wget http://nami.jp/ipv4bycc/$IPLIST.gz
gunzip -d $IPLIST.gz

# ダウンロードしてきた IP リストで日本の IP だけを許可するようにする
sed -n 's/^JP\t//p' $IPLIST | while read ipaddress; do
    iptables -A INPUT -s $ipaddress -j ACCEPT
done

# Amazon EC2 の Asia Pacific (Tokyo) に割り振られている IP レンジを許可する
iptables -A INPUT -s 46.51.224.0/19 -j ACCEPT
iptables -A INPUT -s 54.248.0.0/15 -j ACCEPT
iptables -A INPUT -s 103.4.8.0/21 -j ACCEPT
iptables -A INPUT -s 175.41.192.0/18 -j ACCEPT
iptables -A INPUT -s 176.34.0.0/18 -j ACCEPT
iptables -A INPUT -s 176.32.64.0/19 -j ACCEPT
iptables -A INPUT -s 54.250.0.0/16 -j ACCEPT


# iptables によって DROP されたアクセスのログを取る
#iptables -A INPUT -m limit --limit 1/s -j LOG --log-prefix '[IPTABLES INPUT DROP] : '

# 設定を保存する場合はコメントを外す
#/etc/init.d/iptables save
```