インスタンスの起動

セキュリティグループ

予めセキュリティグループ作成しておいて、選択する。

サブネット（ゾーン）

```
ap-northeast-1c
```

を選ぶ。

ロール

EC2 API tools を利用する場合は、ロールを設定しておく方が良い。
アクセスキーでも可能だが、セキュリティ的にはロールを利用したほうが良い。
インスタンスを起動するときにロールの設定を忘れずに。

細々したこと

http://d.hatena.ne.jp/bluepapa32/20101108/1289187846

■ timezone の変更

```
$ date
Thu Nov  4 14:58:50 UTC 2010
```

UTC になっている。

```
$ sudo cp -p /usr/share/zoneinfo/Japan /etc/localtime
```

```
$ date
Thu Nov  4 23:59:00 JST 2010
```

JST になった。

■ Locale の変更の補足

http://d.hatena.ne.jp/nekoruri/20150130/glibclocaltime
http://d.hatena.ne.jp/necoak/20120702/1341266925

正しくは tzdata-update を使う。
/etc/localtime を直接編集した場合、glibc のアップデートなどの際に戻ってしまう可能性がある。

/etc/sysconfig/clock にタイムゾーンを書く
vi /etc/sysconfig/clock

```
ZONE="Asia/Tokyo"
UTC=false
ARC=false
```

ZONE

ローカルタイムゾーンの設定。
UTC
ハードウェアクロックに設定するタイムゾーンの設定。
ARC
ARC コンソール特有の epoc time を使用するための設定
SRM
SRM コンソール特有の epoc time を使用するための設定

tzdata-update を実行する

```
sudo /usr/sbin/tzdata-update
```

■時刻同期

CentOS7 では ntpd ではなく、chrony に変わった。
ntpd は不要。

```
systemctl status chronyd
 systemctl enable ntpd
```

■ umask

vi .bashrc

```
umask 022
```

■ su、sudo の設定

vi /etc/pam.d/su

```
auth            required        pam_wheel.so use_uid
```

コメントイン。
visudo

```
%wheel ALL=(ALL) NOPASSWD: ALL
```

secure_path に /usr/local/bin を追加しても良いかも。

管理者ユーザだけグループ追加

```
usermod -a -G wheel ユーザ
```

スワップ領域

http://cloudstory.in/2012/02/adding-swap-space-to-amazon-ec2-linux-micro-instance-to-increase-the-performance/
http://x68000.q-e-d.net/~68user/unix/pickup?dd
標準のままだとスワップ領域を持っていないこともある。
なくてもなんとかなるけど、作りたい時はスワップ領域をイメージファイルとして作成する

■スワップ領域のイメージファイル作成

```
dd if=/dev/zero of=/swapfile bs=1M count=1024
chmod 0600 /swapfile
```

■スワップ領域の初期化

```
mkswap /swapfile
```

■スワップ領域の有効化

```
swapon /swapfile
```

もし /etc/fstab を編集後なら

```
swapon -a
```

でも良い。

■スワップ領域の確認

```
swapon -s
```

■ /etc/fstab: の編集

```
/swapfile swap swap defaults 0 0
```

SSH

パスワードログインの禁止

```
PasswordAuthentication yes
```

を

```
PasswordAuthentication no
```

に修正

ポート変更

デフォルトのポート番号 22 を他のポートにしておくといたずらされにくくなる。
ファイヤーウォールとセキュリティグループの設定でポートを開いておくのを忘れずに。

ファイヤーウォールの設定

EC2 のセキュリティグループで設定しているので、firewalld は無効にしても問題ない。

```
systemctl disable firewalld
```

もし、firewalld でも制御したい場合は以下のようにセキュリティグループで設定したポートを開放する。

```
sudo firewall-cmd --zone=public --add-service=http --permanent
sudo firewall-cmd --zone=public --add-service=https --permanent
sudo firewall-cmd --zone=public --add-service=ftp --permanent
sudo firewall-cmd --zone=public --add-port=60000-60030/tcp --permanent
 sudo  firewall-cmd  --zone=public  --add-port=ssh のポートを変更した場合は変更したポート /tcp
--permanent
sudo firewall-cmd --reload
```

設定されているか確認するには、iptables を使えば良い。

```
sudo iptables --list -n
```

外部からのメールを受信する場合

```
 sudo firewall-cmd --zone=public --add-port=25/tcp --permanent
```

ルールを消す場合は

```
sudo firewall-cmd --zone=public --remove-port=25/tcp --permanent
```

ダイナミック DNS

http://b.n-at.me/archives/182
http://shikichi.ddo.jp/dice_install.html
http://www.jitaku-server.net/domain_dice.html

DiCE の設定

■設定

http://ddo.jp に登録

http://www.hi-ho.ne.jp/yoshihiro_e/dice/linux.html からダウンロード
解凍して適当なディレクトリに移動。(/usr/local/lib/DiCE とする）

```
cd /usr/local/lib/DiCE
./diced | nkf -uw
```

で起動する。 EUC で出力してくるので、文字化け対策のために nkf する。
もし ld-linux.so.2 不足でエラーが出る場合は

```
yum install glibc.i686
```

でライブラリ追加。

```
=-=-=- DiCE DynamicDNS Client -=-=-=
Version 0.19 for Japanese
Copyright(c) 2001 sarad

:?
```

? でヘルプ。

setup で DiCE の環境設定をします。

```
:setup
IP アドレスの検出方法を指定してください
(0) 自動検出
(1) ローカルのネットワークアダプタから検出
(2) 外部のスクリプトから検出
< 現在 :0>
(N) 変更しない  (P) 戻る
>n
-----------------------------------------------
プライベート IP アドレスも検出対象ですか？ (Y/N)
< 現在 : いいえ >
(P) 戻る
>n
-----------------------------------------------
IP アドレスの検出をテストしますか？ (Y/N)
(P) 戻る
>y
検出 IP アドレス >xxx.xxx.xxx.xxx
-----------------------------------------------
IP アドレスの検出をテストしますか？ (Y/N)
(P) 戻る
>n
-----------------------------------------------
IP アドレスをチェックする間隔を指定してください ( 分 )
設定可能範囲は 5 分以上です
< 現在 :10>
(N) 変更しない  (P) 戻る
>n
===============================================
DNS サーバーの負荷を軽減するために頻繁な DNS 更新を防ぐ必要があります
前回の更新から一定時間 DNS 更新処理を行わないように保護時間を設定して
ください ( 分 )  設定可能範囲は 10 分から 1440 分です
< 現在 :60>
(N) 変更しない  (P) 戻る
>30
===============================================
設定を保存しますか？ (Y/N)
(P) 戻る
>y
設定を保存しました
===============================================
```

add でイベント追加

```
:add
新しくイベントを追加します
DynamicDNS サービス名を入力してください
"?" で対応しているサービスを一覧表示します
(P) 戻る
>?          <-- 対応しているサービスを検索
ZENNO.COM livedoor MyDNS.JP pcc.jp
JPN.ch MyIP.US @nifty StaticCling
MyServer ddns.ca p2p did.expoze.com
Dynamx WebReactor unicc Earth
DNS2Go EveryDNS Now.nu dynDNS.it
onamae.com DION ODN ysdn
ddo.jp Netservers todd USA
cjb Dyn.ee BIGLOBE dnip
my-domain ZoneEdit ZiVE yi
theBBS SelfHOsT No-IP nicolas
miniDNS Microtech instat ieServer
HAMMERNODE GetmyIP Dynup Dynu
dyns DynDSL DynDNSdk dyndns
DtDNS dnsQ dhs DDNS.nu
cheapnet changeIP ARTofDNS VALUEDOMAIN
ODS JSPEED IPDYN DnsTokyo
===============================================
>ddo.jp          <-- 今回は ddo.jp を使用
-----------------------------------------------
```

```
<< Dynamic DO!.jp >>
URL: http://ddo.jp/
*** 情報 ***
ユーザー名の入力は不要です
独自ドメインの場合はドメイン名を " ホスト " の所へ入力してください
================================================
ドメイン名を入力してください
"?" でドメイン一覧を表示します
(P) 戻る
>ddo.jp       <-- 取得したドメインが ***.ddo.jp の場合（*** を除いた部分 )
================================================
ホスト名を入力してください
(P) 戻る
>***          <-- 取得したドメインが ***.ddo.jp の場合（ddo.jp を除いた部分 )
================================================
ログインユーザ名を入力してください
(P) 戻る
>***          <-- 取得したドメインが ***.ddo.jp の場合（ddo.jp を除いた部分 )
================================================
ログインパスワードを入力してください
(P) 戻る
>??????       <-- 登録時に設定したパスワード
================================================
登録する IP アドレスを入力してください
空白にすると現在の IP アドレスを自動検出します
(P) 戻る
>               <-- 空白のまま [enter]
このイベントに題名を付けてください
(P) 戻る
>***.ddo.jp の更新              <-- わかりやすい名前を設定
================================================
このイベントを実行するスケジュールを設定します
------------------------------------------------
実行する頻度を指定してください ( 番号入力 )
(0) １回のみ (1) １日１回 (2) １週間に１回 (3) １ヵ月に１回
(4) その他の周期 (5)IP アドレス変化時 (6) 起動時
(N) 変更しない (P) 戻る
>5            <-- サーバーに負荷をかけない
------------------------------------------------
IP アドレスがあまり変化しない環境の場合、更新せずに一定期間を過ぎると
アカウントを削除されてしまうことがあります
IP アドレスの変化が無い時に実行する間隔を指定してください
(0)7 日毎 (1)14 日毎 (2)21 日毎 (3)28 日毎
(4)35 日毎 (5)56 日毎 (6)84 日毎
(N) 変更しない (P) 戻る
>0            <-- ドメインが削除されないよう短めに設定
================================================
詳細オプションを設定します
------------------------------------------------
[ サービスタイプ ]
(0) 無料 (1) 有料
番号 >0
------------------------------------------------
[ SSL ]
(0) 使用する (1) 使用しない
番号 >1
------------------------------------------------
[ オフライン ]
(0)No (1)Yes
番号 >0
================================================
このイベントを有効にしますか？ (Y/N)
( イベントの有効 / 無効は "EN/DIS" コマンドで切替えられます )
> y            <-- イベントを有効にする
================================================
イベントを保存しますか？ (Y/N)
( イベントの有効 / 無効は "EN/DIS" コマンドで切替えられます )
> y            <-- イベントを保存する
```

IP アドレス検出について

一部の環境では IP アドレスの検出が止まってしまう。
IPv6 だと止まってしまうような気がする。
対応策としては、外部スクリプトを利用して IP アドレスの検出を行う。
外部スクリプトとしては

```
http://dyn.value-domain.com/cgi-bin/dyn.fcg?ip
```

```
http://checkip.dyndns.org/
http://info.ddo.jp/remote_addr.php/
```

などがある。これを指定することで検出が可能になる。

```
:setup
IP アドレスの検出方法を指定してください
(0) 自動検出
(1) ローカルのネットワークアダプタから検出
(2) 外部のスクリプトから検出
< 現在 :0>
(N) 変更しない　(P) 戻る
>2
-----------------------------------------------
スクリプトの URL を入力してください
< 現在 :>
(N) 変更しない　(P) 戻る
>http://checkip.dyndns.org/
-----------------------------------------------
プライベート IP アドレスも検出対象ですか？ (Y/N)
< 現在 : いいえ >
(P) 戻る
>n
-----------------------------------------------
IP アドレスの検出をテストしますか？ (Y/N)
(P) 戻る
>y
検出 IP アドレス >xxx.xxx.xxx.xxx
```

サービス登録

vi /etc/systemd/system/dice.service

```
[Unit]
Description=The ddojp
After=network.target remote-fs.target nss-lookup.target

[Service]
Type=notify
EnvironmentFile=/usr/local/lib/DiCE/diced
ExecStart=/usr/local/lib/DiCE/diced -d -l
ExecReload=/bin/kill =HUP ${MAINPID}
ExecStop=/bin/kill ${MAINPID}
RemainAfterExit=yes
PrivateTmp=true

[Install]
WantedBy=runlevel3.target
```

権限付与

```
chmod 755 usr/lib/systemd/system/dice.service
```

サービス登録

```
systemctl enable dice.service
```

サービススタート

```
systemctl start dice.service
```

ログ確認

```
nkf -Ew /usr/local/lib/DiCE/log/events.log
```

cron 登録

普通は必要ないと思うのだけど、一週間に一度の更新が正常に動作していないことがある。
とりあえず、cron で一週間に一度の更新をする。

```
sudo crontab -e
00 02 * * 5 /usr/local/lib/DiCE/diced -l -e 0 > /dev/null
```

毎週金曜日の 2:00 に IP 更新をする。

Apache

インストール

```
yum install httpd
systemctl enable httpd
```

設定

■サーバの設定

httpd.conf の最後に追記するか、etc/httpd/conf.d に設定ファイルを作成する。
vi /etc/httpd/conf/httpd.conf

```
KeepAlive On
KeepAliveTimeout 5
ServerTokens Prod ←　余計な情報を出さない
ServerSignature Off ←　余計な情報を出さない
```

■メモリを食いつぶさないようにプロセス数を制御する

http://www.happyquality.com/2012/02/01/1905.htm
http://9ensan.com/blog/server/sakura-vps-httpd-confi/
以下の内容を httpd.conf の最後に追記する。
（/etc/httpd/conf.modules.d や etc/httpd/conf.d にファイルを作成してもよい）

```
<IfModule prefork.c>
StartServers       2
MinSpareServers    2
MaxSpareServers    5
ServerLimit       32
MaxClients        32
MaxRequestsPerChild 500
</IfModule>
```

ちなみに、httpd が prefork なのか worker なのかは

```
httpd -V | grep MPM
```

でわかる

■ public_html の設定

/etc/httpd/conf.d/userdir.conf を編集する
vi /etc/httpd/conf.d/userdir.conf

```
UserDir public_html ← public_html を有効


<Directory "/home/*/public_html">
    #AllowOverride FileInfo AuthConfig Limit Indexes
    AllowOverride FileInfo AuthConfig Limit Indexes Options
    #Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    Options MultiViews SymLinksIfOwnerMatch IncludesNoExec
    Require method GET POST OPTIONS
</Directory>
```

■ Welcome 非表示

vi /etc/httpd/conf.d/welcome.conf

```
<LocationMatch "^/+$">
    Options -Indexes
#    ErrorDocument 403 /error/noindex.html
</LocationMatch>
```

CGI を使う

```
yum install perl
yum install php
```

php.ini のタイムゾーンを設定しておく

```
date.timezone = "Asia/Tokyo"
```

.htaccess

```
Options +ExecCGI -Indexes
AddHandler cgi-script cgi pl
```

perl の実行権限は suExec によりホーム以下の場合は各ユーザの権限で実行される。
php での実行は、apache ユーザで実行されるので注意。
所有者を apache にするか、sgid と apache の umask の設定で対処する

必要なライブラリの追加

```
yum install perl-CGI
yum install perl-GD
yum install perl-Data-Dumper
yum install php-gd
```

必要に応じてクローラ対策を行う

クローラー対策
bing ボットの行儀が悪いので
vi /var/www/html/robots.txt

```
User-agent: bingbot
Disallow: /
```

とか。

vsftpd

```
 yum -y install vsftpd
sudo systemctl enable vsftpd
```

vi /etc/vsftpd/vsftpd.conf

```
connect_from_port_20=NO ← アクティブモードのデータ転送用ポートを 20 に固定するか
anonymous_enable=NO   ←  anonymous ユーザ ( 匿名ユーザ ) のログイン禁止
chroot_local_user=YES ←  デフォルトでホームディレクトリより上層へのアクセスを禁止する
userlist_deny=NO ←  user_list に書かれているユーザのみを許可する
use_localtime=YES ←  タイムスタンプ時間を日本時間にする
pasv_addr_resolve=YES  ←  PASV モード接続先 IP アドレスをホスト名から取得する
pasv_address=hogehoge.ddo.jp  ←  PASV モード接続先 IP アドレスが牽けるホスト名※
pasv_min_port=60000 ←  PASV モード接続時の最小ポート番号
pasv_max_port=60030 ←  PASV モード接続時の最大ポート番号
force_dot_files=YES ← .htaccess のような隠しファイルも表示する
allow_writeable_chroot=YES ← chroot 先が書き込み可能でも許可する。vsftpd 3.x.x はこれがないと接続で
きない。
listen=YES ← IPv4 ソケットのみリッスンするか
listen_ipv6=NO ← IPv6 ソケットのみリッスンするか
```

この場合は 60000 ～ 60030 も Security Group の設定で通信を許可する

■ユーザーリストの設定

接続を許可するユーザのリストを編集する

```
vi /etc/vsftpd/user_list
```

■ファイルリストの表示について

.htaccess でファイルリストを表示する場合、以下の設定にしておく
文字コードの指定とファイル名の長さを自動に設定。

```
Options Indexes
IndexOptions Charset=UTF-8
IndexOptions NameWidth=*
```

メール送信設定

sendmail コマンドで外部へメールを送る。
ただし、メールサーバは建てない。
なので、他のメールサーバにリレーしてもらう。

具体的な方法は、sendmail コマンドの smtp サーバの設定参照。

バックアップジョブ

EC2 API tools を使って cron でスナップショットを取得してバックアップを取る。

EC2 API tools をインストールする

Amazon EC2 に EC2 API tools をインストール

スナップショットによるバックアップ

Amazon EC2 を snapshot でバックアップ

SSL 設定

Let's Encrypt で SSL 化

メンテナンス記録

2019/11/30 SSL 証明書期限切れ

証明書の期限切れが発生した。cron で毎月 1 日に更新するように設定していたが、先月の実行が失敗していた。
(たぶん、ネットワーク等の不調と思われる)
期限切れの月の更新に失敗してしまうと、そのまま期限切れになってしまうので、毎月 1 日と 15 日に実行するように修正した。

2019/03/10 データストレージ縮小

データ用のストレージがほとんど使われていないので縮小した。
ストレージの縮小機能は無いので、新しいストレージを作成してデータコピーする。

■ストレージ追加

1.EC2 コンソールでストレージ追加、アタッチ
2. ディスクフォーマット
    1. パーティションは作成せずに、loop とした。後にストレージを拡張する際に、拡張が少し楽になるため。ディスク、パーティションの情報確認
    2.sudo mkfs -t ext4 /dev/xvdg
3. ラベル設定
    1.sudo e2label /dev/xvdf DATA
4. データコピー
    1.rsync -av コピー元 コピー先
5. 旧データストレージをでアタッチ
    1. インスタンスを止めて、ストレージをでアタッチ
6. 今後ストレージを拡張するとき
    1.EC2 のコンソールでストレージを拡張
    2.sudo resize2fs /dev/xvdf

■ vsftp の参照先を追加したストレージにする

vsftp で chroot しているため、追加したストレージのディレクトリにシンボリックリンクを貼っても vsftp では参照できない。

```
mount --bind
```

を使って追加したストレージを参照できるようにする。/etc/fstab に以下のようなものを追加

```
マウント元 マウント先 none bind 0 0
```

SSL 化

Let's Encrypt で SSL 化参照

2018/01/13 外部メールの受信設定

AWS Certificate Manager の SSL を利用するためにドメイン宛のメールを受信するために以下を設定

1. セキュリティグループで 25/tcp を許可
2.firewall-cmd --zone=public --add-port=25/tcp --permanent

3./etc/postfix/main.cf を編集
    1.myhostname = xxx.ddo.jp
    2.mydomain = xxx.ddo.jp
    3.myorigin = $mydomain
    4.inet_interfaces = all

ACM の SSL は EC2 では利用できないことがわかったため、一部の設定を戻す。

1. セキュリティグループで 25/tcp を拒否
2.firewall-cmd --zone=public --remove-port=25/tcp --permanent
3./etc/postfix/main.cf を編集
    1.inet_interfaces = localhost

2016/03/05 ストレージ追加

OS 用、データ用のストレージを分けて、バックアップは OS 用ストレージだけ取ることにした。

■準備

```
sudo yum install parted
sudo yum install e2fsprogs
```

■ストレージ追加

新しいボリュームを作成し

```
/dev/sdf
```

として追加した。

■フォーマットとマウント

パーティッションは作成せずに、デバイスをそのままフォーマットした。

```
sudo mkfs -t ext4 /dev/xvdf
```

ラベル設定

```
sudo e2label /dev/xvdf DATA
```

/etc/fstab

```
LABEL=DATA /mnt/data ext4    defaults        0 0
```

■データ用ストレージの拡張を行う場合

1. データ用ボリュームのスナップショット作成
2. スナップショットからボリュームを作成
    1. 容量を拡張する
3. マウントした状態で拡張する場合
    1.resize2fs /dev/xvdf
4. マウントしない状態で拡張する場合
    1.sudo e2fsck -f /dev/xvdf

2.sudo resize2fs /dev/xvdf

2016/03/04 ストレージ拡張

データ量を増やすことになったので、ストレージの拡張を行った。

参考
http://docs.aws.amazon.com/ja_jp/AWSEC2
/latest/UserGuide/ebs-expand-volume.html#recognize-expanded-volume-linux
http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/storage_expand_partition.html

■事前準備

```
yum install parted
yum install e2fsprogs    <- e2fsck とは resize2fs が入っているパッケージ
```

■ボリュームの作成

容量を拡張する
アベイラビリティーゾーンを合わせること

■ボリュームの拡張

古いボリュームをアタッチしたまま起動

```
/dev/sda1 <- 最後の数字まで指定していることに注意
```

起動後に新しいボリュームをアタッチ

```
/dev/sdf
```

ボリュームの状況を確認

```
lsblk
 NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
 xvda    202:0    0  10G  0 disk
 `-xvda1 202:1    0  10G  0 part /
 xvdf    202:80   0  50G  0 disk
 `-xvdf1 202:81   0  10G  0 part
```

parted でボリューム拡張

```
parted /dev/xvdf
```

表示単位をバイトからセクターに変更

```
(parted) unit s
```

状態を表示

```
(parted) print
Number  Start  End        Size       Type     File system  Flags
1      2000s  20971519s  20969520s  primary  ext3         boot
```

始点：2000s
Type：primary
Flags:boot
を書き留めておく。

パーティッションを拡張する。

```
(parted) rm 1
(parted) mkpart primary 2000s 100%
警告が出ることがあるが無視してよい。
(parted) set 1 boot on
(parted) print
(parted) quit
```

ファイルシステムのチェック

```
sudo e2fsck -f /dev/xvdf1
```

拡張

```
sudo resize2fs /dev/xvdf1
```

マウントと確認

```
mount /dev/xvdf1 /mnt
df -h
```

■新しいボリュームをアタッチ

インスタンスをシャットダウン
古いボリュームをデタッチ
新しいボリュームをアタッチ

```
/dev/sda1
```

インスタンス起動

2014/10/25

中国を中心に大量アクセスがあったため、日本国内からのみアクセス可能とした

■流したスクリプト

```
#!/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] : '
iptables -P INPUT DROP          # 受信はすべて破棄

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