参考

https://inaba-serverdesign.jp/blog/20170913/clamav_scan_virus_install.html
https://www.yokoweb.net/2017/04/15/ubuntu-server-clamav/

概要

OSS のアンチウィルスソフト。

インストール

Centos

```
yum install clamav clamav-data
```

もし常時スキャンしたい場合はデーモンも入れる

```
yum install clamd
```

Ubuntu

```
apt install clamav
```

もし常時スキャンしたい場合はデーモンも入れる

```
apt install clamav-daemon
```

設定ファイル

パス	意味
/etc/clamav/freshclam.conf	Ubuntu の freshclam の設定ファイル。
/etc/freshclam.conf	Centos の freshclam の設定ファイル。

ウイルス定義の自動更新

CentOS の場合は

```
/etc/cron.d/clamav-update
```

により、自動で更新される。
Ubuntu の場合は、

```
clamav-freshclam.service
```

のサービスが上がる。

手動スキャン

ログファイル出力先作成

```
mkdir -p /var/log/clamav
mkdir -p /var/log/clamav/virus
```

ログローテート

vim /etc/logrotate.d/clamav-full-scan

```
/var/log/clamav/clamscan.log
{
        monthly
        notifempty
}
```

スキャンシェル

vim /usr/local/bin/clam-full.sh

```
#!/bin/sh

log=/var/log/clamav/clamscan.log
echo ======================================== | tee -a ${log}
date | tee -a ${log}
hostname | tee -a ${log}
freshclam
clamscan / \
     --infected \
     --recursive \
     --log=${log} \
     --move=/var/log/clamav/virus \
     --exclude-dir=^/boot \
     --exclude-dir=^/sys \
     --exclude-dir=^/proc \
     --exclude-dir=^/dev \
     --exclude-dir=^/var/log/clamav/virus

# --infected 感染を検出したファイルのみを結果に出力
# --recursive 指定ディレクトリ以下を再帰的に検査 圧縮ファイルは解凍して検査
# --log=FILE ログファイル
# --move=DIR 感染を検出したファイルの隔離先
# --remove 感染を検出したファイルを削除
# --exclude=FILE      検査除外ファイル（パターンで指定）
# --exclude-dir=DIR  検査除外ディレクトリ（パターンで指定）

if [ $? = 0 ]; then
  echo "ウイルス未検出." | tee -a ${log}
else
  echo "ウイルス検出!!" | tee -a ${log}
fi
```

cron.daily

vim /etc/cron.daily/clam-full-daily.sh

```
#!/bin/sh

/usr/local/bin/clam-full.sh
```