mod_dosdetector による制御

http://c-brains.jp/blog/wsg/10/06/24-134947.php

インストール

```
yum install httpd-devel

cd /usr/local/src
   wget        http://downloads.sourceforge.net/project/moddosdetector/moddosdetector/version-0.2
/mod_dosdetector-0.2.tar.gz?use_mirror=jaist
tar -xzvf mod_dosdetector-0.2.tar.gz
cd /usr/local/src/mod_dosdetector-0.2
make
make install
```

設定ファイル

/etc/httpd/conf/httpd.conf

```
# デフォルトでは favicon のコンテンツタイプは指定されていないので設定
AddType image/vnd.microsoft.icon .ico

LoadModule dosdetector_module /usr/lib64/httpd/modules/mod_dosdetector.so

# モジュール設定
DoSDetection On
DoSPeriod 5
DoSThreshold 10
DoSHardThreshold 20
DoSBanPeriod 30
DoSTableSize 100
DoSIgnoreContentType ^(image/|application/|text/javascript|text/css)

 LogFormat "%{SuspectHardDoS}e %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
dosdetector
CustomLog logs/dos_suspect_log dosdetector env=SuspectDoS

RewriteEngine On
RewriteCond %{ENV:SuspectHardDoS} =1
RewriteRule .*  - [R=503,L]
ErrorDocument 503 "Server is busy."
```

■設定値について

DoSDetection

DoS 攻撃の検知を有効にするかどうか。

DoSPeriod

DoS 攻撃の判定を行う時間を設定。（秒）

DoSThreshold

DoSPeriod の間にこの数だけアクセスがあれば DoS 攻撃の疑いありとみなし、環境変数 SuspectDoS を 1 にセットする。

DoSHardThreshold

DoSPeriod の間にこの数だけアクセスがあれば DoS 攻撃の疑いが強いとみなし、環境変数 SuspectHardDoS を 1 にセットする。

DoSBanPeriod

DoS 攻撃の疑いが設定されてから解除するまでの時間。（秒）

DoSTableSize

クライアントの追跡記録を保存する数。多すぎるとその分リソースを消費する。

DoSIgnoreContentType

追跡記録から除外するコンテンツタイプをパターンマッチングな文字列で指定。