SPFレコードに登録されているスパムホストへの対処例(Postfix)

2016/04/04
SPFレコードを登録しているホストを制限する例。あくまで例なのでこれを参考にするなら自己責任で。

SPFレコードを登録されたスパムホストへの対処

Postfix postfix-policyd-spf-pythonの環境でのログ

toramaki.net ですか。

```
Apr  4 03:04:34 amame postfix/smtpd[13591]: connect from
unknown[45.120.197.160]
Apr  4 03:04:35 amame policyd-spf[13596]: None; identity=helo; client-
ip=45.120.197.160; helo=dhgiw7wob8.dushfc; envelope-
from=jfsofy+err9899s722@toramaki.net; receiver=iam@hgotoh.jp
Apr  4 03:04:35 amame policyd-spf[13596]: Pass; identity=mailfrom; client-
ip=45.120.197.160; helo=dhgiw7wob8.dushfc; envelope-
from=jfsofy+err9899s722@toramaki.net; receiver=iam@hgotoh.jp
Apr  4 03:04:35 amame postfix/smtpd[13591]: 8F07EB62D02:
client=unknown[45.120.197.160]
Apr  4 03:04:35 amame postfix/cleanup[13597]: 8F07EB62D02: message-
id=<20160404030425@wfzaixz.okdmkus>
Apr  4 03:04:35 amame postfix/smtpd[13591]: disconnect from
unknown[45.120.197.160] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Apr  4 03:04:35 amame postfix/qmgr[13467]: 8F07EB62D02:
from=<jfsofy+err9899s722@toramaki.net>, size=3147, nrcpt=1 (queue active)
Apr  4 03:04:35 amame postfix/local[13598]: 8F07EB62D02:
to=<crowller@hgotoh.jp>, orig_to=<iam@hgotoh.jp>, relay=local, delay=1.2,
delays=1.1/0.01/0/0.02, dsn=2.0.0, status=sent (delivered to maildir)
Apr  4 03:04:35 amame postfix/qmgr[13467]: 8F07EB62D02: removed
Apr  4 03:07:55 amame postfix/anvil[13593]: statistics: max connection rate
1/60s for (smtp:45.120.197.160) at Apr  4 03:04:34
Apr  4 03:07:55 amame postfix/anvil[13593]: statistics: max connection count
1 for (smtp:45.120.197.160) at Apr  4 03:04:34
Apr  4 03:07:55 amame postfix/anvil[13593]: statistics: max cache size 1 at
Apr  4 03:04:34
Apr  4 03:08:29 amame postfix/pickup[13468]: 9366DB62D14: uid=0 from=<root>
^C
root@amame:/usr/local/etc/postfix #
```

DNSのTXTレコードにあるSPF定義を見てみる

toramaki.net のTXTレコードを見てみると……includeだから spf-stx.burn-oxygen.com に共用されてるTXTレコードがあるのね。

```
root@amame:/usr/local/etc/postfix # drill TXT toramaki.net
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 53967
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; toramaki.net.        IN      TXT

;; ANSWER SECTION:
toramaki.net.   3138    IN      TXT     "v=spf1 include:spf-stx.burn-
oxygen.com ~all"

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 0 msec
;; SERVER: 133.242.0.3
;; WHEN: Mon Apr  4 03:10:21 2016
;; MSG SIZE  rcvd: 86
root@amame:/usr/local/etc/postfix #
```

接続してきた相手のIPアドレスが 45.120.197.160 なので“ip4:45.120.196.0/22”の定義に合致するのね。

```
root@amame:/usr/local/etc/postfix # drill TXT spf-stx.burn-oxygen.com
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 59089
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; spf-stx.burn-oxygen.com.     IN      TXT

;; ANSWER SECTION:
spf-stx.burn-oxygen.com.        147     IN      TXT     "v=spf1
ip4:45.120.196.0/22 ip4:45.124.217.0/24 ip4:103.58.71.0/24
ip4:103.227.8.0/22 ip4:103.232.203.0/24 ip4:103.243.243.0/24
ip4:103.248.70.0/24 ip4:103.251.157.0/24 ~all"

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 0 msec
;; SERVER: 133.242.0.3
;; WHEN: Mon Apr  4 03:15:56 2016
;; MSG SIZE  rcvd: 226
root@amame:/usr/local/etc/postfix #
```

リジェクト対象一覧を作成する

怪しいので全部リジェクト対象にする。

ネットマスクが24のものは単純に変換できる。

ネットワークアドレス	変換
45.124.217.0/24	45.124.217 REJECT
103.58.71.0/24	103.58.71 REJECT
103.232.203.0/24	103.232.203 REJECT
103.243.243.0/24	103.243.243 REJECT
103.248.70.0/24	103.248.70 REJECT
103.251.157.0/24	103.251.157 REJECT

ネットマスクが22のものは複数の変換結果に分割して対応。

ネットワークアドレス	変換
45.120.196.0/22	45.120.196 REJECT
	45.120.197 REJECT
	45.120.198 REJECT
	45.120.199 REJECT
103.227.8.0/22	103.227.8 REJECT
	103.227.9 REJECT
	103.227.10 REJECT
	103.227.11 REJECT

/usr/local/etc/postfix/rejecthosts の名前でファイルを作成。

rejecthosts

```
45.124.217   REJECT
103.58.71    REJECT
103.232.203  REJECT
103.243.243  REJECT
103.248.70   REJECT
103.251.157  REJECT
45.120.196   REJECT
45.120.197   REJECT
45.120.198   REJECT
45.120.199   REJECT
103.227.8    REJECT
103.227.9    REJECT
103.227.10   REJECT
103.227.11   REJECT
```

postmapコマンドでハッシュ化する。※ここでは hashを使わずcdbでデータベース化しているよ！

```
root@amame:/usr/local/etc/postfix # postmap cdb:rejecthosts
```

```
root@amame:/usr/local/etc/postfix #
```

/usr/local/etc/postfix/main.cf のsmtpd_client_restrictionsパラメタにcheck_client_accessオプションでrejecthostsを指定する。

```
smtpd_client_restrictions =
     permit_mynetworks
     check_client_access cdb:/usr/local/etc/postfix/rejecthosts
     permit
```

service postfix reload を実行してPostfixにrejecthosts.cdbの使用を指示して終了。

リジェクトされるとこんなログになる

103.232.203.73 は 103.232.203.0/24 に合致するのでリジェクト対象。

```
Apr  4 04:38:42 amame postfix/smtpd[14042]: warning: hostname r001-
stc001.xq0t0qyc does not resolve to address 103.232.203.73: hostname nor
servname provided, or not known
Apr  4 04:38:42 amame postfix/smtpd[14042]: connect from
unknown[103.232.203.73]
Apr  4 04:38:43 amame postfix/smtpd[14042]: NOQUEUE: reject: RCPT from
unknown[103.232.203.73]: 554 5.7.1 <unknown[103.232.203.73]>: Client host
rejected: Access denied; from=<ginnfts+err73884s1043@se2.vurbyietloam.xyz>
to=<oreda@hgotoh.jp> proto=ESMTP helo=<ha5etjt>
Apr  4 04:38:43 amame postfix/smtpd[14042]: disconnect from
unknown[103.232.203.73] ehlo=1 mail=1 rcpt=0/1 data=0/1 rset=1 quit=1
commands=4/6
```

技術資料, Postfix, mail, SPF