SPFレコードに登録されていないスパムホストへの対処例(Postfix)

2016/04/07
SPFレコードに登録されていない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レコードに登録されていないスパムホストへの対処

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

さすがにさ□□@ezweb.ne.jp はないよねー

```
Apr  6 23:31:55 noriko postfix/smtpd[25350]: warning: hostname abs-
static-86.53.68.58.aircel.co.in does not resolve to address 58.68.53.86:
hostname nor servname provided, or not known
Apr  6 23:31:55 noriko postfix/smtpd[25350]: connect from
unknown[58.68.53.86]
Apr  6 23:31:57 noriko policyd-spf[25355]: None; identity=helo; client-
ip=58.68.53.86; helo=abs-static-86.53.68.58.aircel.co.in; envelope-
from=p0owpreq8i@ezweb.ne.jp; receiver=oreda@hgotoh.jp
Apr  6 23:31:57 noriko policyd-spf[25355]: Softfail; identity=mailfrom;
client-ip=58.68.53.86; helo=abs-static-86.53.68.58.aircel.co.in; envelope-
from=p0owpreq8i@ezweb.ne.jp; receiver=oreda@hgotoh.jp
Apr  6 23:31:57 noriko postfix/smtpd[25350]: 74507B62D02:
client=unknown[58.68.53.86]
Apr  6 23:31:58 noriko postfix/cleanup[25356]: 74507B62D02: message-id=<>
Apr  6 23:31:58 noriko postfix/qmgr[25223]: 74507B62D02:
from=<p0owpreq8i@ezweb.ne.jp>, size=1840, nrcpt=1 (queue active)
Apr  6 23:31:58 noriko postfix/local[25357]: 74507B62D02:
to=<crowller@hgotoh.jp>, orig_to=<oreda@hgotoh.jp>, relay=local, delay=1.9,
delays=1.9/0.01/0/0, dsn=2.0.0, status=sent (delivered to maildir)
Apr  6 23:31:58 noriko postfix/qmgr[25223]: 74507B62D02: removed
Apr  6 23:31:59 noriko postfix/smtpd[25350]: disconnect from
unknown[58.68.53.86] helo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
```

DNSのTXTレコードにあるSPF定義を見てみる

aircel.co.in のTXTレコードを見てみると□.....spf.protection.outlook.comを追いかけてみたけど、まぁ該当のIPアドレスも範囲の定義にも見つからなかった。
だからSPFのStatusが Softfail になったのね。

```
root@noriko:/usr/local/etc/postfix # drill TXT aircel.co.in
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 32883
```

```
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; aircel.co.in.        IN      TXT

;; ANSWER SECTION:
aircel.co.in.   10800   IN      TXT     "v=spf1 ip4:58.68.109.187
ip4:202.148.202.47 ip4:202.148.202.54 ip4:58.68.109.188
include:spf.protection.outlook.com ~all"

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 132 msec
;; SERVER: 133.242.0.3
;; WHEN: Wed Apr  6 23:33:12 2016
;; MSG SIZE  rcvd: 163
root@noriko:/usr/local/etc/postfix #
```

whois でIPアドレスを調べてみる

住所が正しいならインドのあたりっぽい Dishnet Wireless limitedってプロバイダの顧客っぽいですねーこりゃ。

```
root@noriko:/usr/local/etc/postfix # whois 58.68.53.86

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/public/whoisinaccuracy/index.xhtml
#

--- 中略 ---

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '58.68.53.80 - 58.68.53.87'

inetnum:        58.68.53.80 - 58.68.53.87
netname:        DWL-Idea
descr:          DWL-Idea-KOL
country:        IN
admin-c:        RM405-AP
tech-c:         RM405-AP
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-IN-DWL
changed:        rajesh.madhamshetti@aircel.co.in 20090927
```

```
source:         APNIC

person:         Rajesh Madhamshetti
nic-hdl:        RM405-AP
e-mail:         rajesh.madhamshetti@aircel.co.in
address:        Dishnet Limited
address:        19/32, Cathedral Garden Raod,
address:        Nungambakkam,
address:        Chennai
phone:          +91-44-42280000
country:        IN
changed:        rajesh.madhamshetti@aircel.co.in 20070306
mnt-by:         MAINT-IN-DWL
source:         APNIC

% Information related to '58.68.53.0/24AS10201'

route:          58.68.53.0/24
descr:          Dishnet Wireless Limited
origin:         AS10201
mnt-by:         MAINT-IN-DWL
changed:        rajesh.madhamshetti@aircel.co.in 20090109
source:         APNIC

% This query was served by the APNIC Whois Service version 1.69.1-APNICv1r0
(UNDEFINED)


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

リジェクトするホストを rejecthosts に定義する

/usr/local/etc/postfix/rejecthosts に58.68.53.80 - 58.68.53.87をREJECT対象として追加します。

```
58.68.53.80  REJECT
58.68.53.81  REJECT
58.68.53.82  REJECT
58.68.53.83  REJECT
58.68.53.84  REJECT
58.68.53.85  REJECT
58.68.53.86  REJECT
58.68.53.87  REJECT
```

seqコマンドで連番の文字列を作れば少し楽。

```
root@noriko:/usr/local/etc/postfix # seq -f '58.68.53.%g  REJECT' 80 87 >>
rejecthosts
```

あとは postmap cdb:rejecthosts を実行して service postfix reload を実行して完了。

技術資料, Postfix, mail, SPF, whois, seq

From:
https://wiki.hgotoh.jp/ - **努力したWiki**

Permanent link:
https://wiki.hgotoh.jp/documents/mail/mail-015

Last update: **2023/04/14 02:32**