# Postfixを用いてS25Rを設定してみました

Echigo BSD Users Group
神保道夫

2008/11/22@長岡市民センター

# 不正なSPAMメールを防ぐ方法

- メールサーバー側でSPAMメールを対策する仕組みとしては、
  ・SPFを利用して、不正なIPアドレスからの送信メールを拒否する方法
  ・spamasassinを利用してSPAMメールと思われるものを振り分ける方法
  ・S25Rを利用して、ウイルスに感染したPCからの無差別メール送信をブロックする方法

などがあります。今回は、S25Rについて紹介します。

# S25Rとは？

- S25Rとは、（Selective SMTP Rejection：選択的SMTP拒絶）の略称です。概略としては、
  ・逆引きできないクライアントを応答コード「450」（「後で再試行せよ」の意味）で拒否。
  ・逆引き名からメールサーバでないと推定されるクライアントを応答コード「450」で拒否。
  →幾つかのルールに従い、常時接続及びダイアルアップ用ホストとメールサーバーを判別する。ただし、このルールも完璧ではないので、すり抜ける可能性はある。
  ・応答コード「450」による拒否に対して規則的に再試行する正当なメールサーバをホワイトリストで救済。

# S25Rの利点と欠点

- 利点
  スパムとウィルスメールの全アクセスに対する阻止率は、約99%。
  宛先の正しいスパムの阻止率は97%以上。
- 欠点
  初期の偽陽性判定率約13%。ホワイトリストの保守（自動化可能）が必須です。
  メールログを監視できない人は使わないでください。
  メールの受信の遅延がいやだと思う人は使わないでください。

# S25Rの効果

- ホワイトリストを作る前の非阻止率は、小規模のサイトでおよそ13%程度。大規模サイトで、約1000項目程度。2週間程度の運用で、非阻止率は下がっていく。

# PostfixでのS25Rの導入例

- main.cf に対しての変更例

```
smtpd_client_restrictions =
        permit_mynetworks,
        reject_unauth_destination,
        check_client_access regexp:/usr/local/etc/postfix/white-list.txt,
        check_client_access regexp:/usr/local/etc/postfix/white-list2.txt,
        check_client_access regexp:/usr/local/etc/postfix/rejections.txt
smtpd_helo_required = yes
smtpd_helo_restrictions =
        permit_mynetworks,
        reject_invalid_hostname,
        check_helo_access  regexp:/usr/local/etc/postfix/helo_restrictions.txt
smtpd_sender_restrictions =
        permit_mynetworks,
        reject_non_fqdn_sender,
        reject_unknown_sender_domain
```

これでとりあえず運用してみました。

# S25Rの現時点での問題点

この設定だと、IPv4のメールサーバーに関してはかなりカバーできますが、IPv6のメールサーバーからのメール送信は、逆引きの設定がされていないと、ホワイトリストにルールが何も書かれていないため、何らかの対策が必要です。(逆引きが書けないfeel6とか・・・)

- 逆に、IPv6のメールサーバーを無条件に受け取ろうと思ったら、こんな感じ？
  http://d.hatena.ne.jp/clams/20060406/p1
  2500文字もの正規表現、書けませんがな！

# しょうがないので別の解を探す

- S25R方式をグレイリスティング（再試行するホストを許可する方法）またはタールピッティング（応答遅延）と組み合わせることによって正当なホストを許可する方式が佐藤潔氏によって提供されています。詳しくは、
  http://k2net.hakuba.jp/targrey/
  を参照してください。

# 私の現在の試行方法

- FreeBSD 7-STABLEで、
  ・ports/mail/postgreyにtargrey-0.31-postgrey-1.32.patchを当ててインストール
  ・ports/mail/postfixに、postfix sleep patchを当ててインストールして運用しています。(いずれも、佐藤潔さんのページに設定方法が載っています)。
- 学習機能が働いていけば、自動的にIPv6のホストでも受信してくれるので、問題ないみたいです(まだ、試験が必要かもしれません)
- ebug.jp からは、SPAMメールも来るので、受信が遅れます。しょうがないので、別途ルールを書いて、無条件受信するようにしました。

# 詳細については・・・

- http://www.gabacho-net.jp/anti-spam/anti-spam-system.html

こちらのページをご覧ください。