S25Rスパム対策方式のご紹介

浅見秀雄
deo@gabacho-net.jp
http://www.gabacho-net.jp/anti-spam/

2009年8月29日

S25Rとは

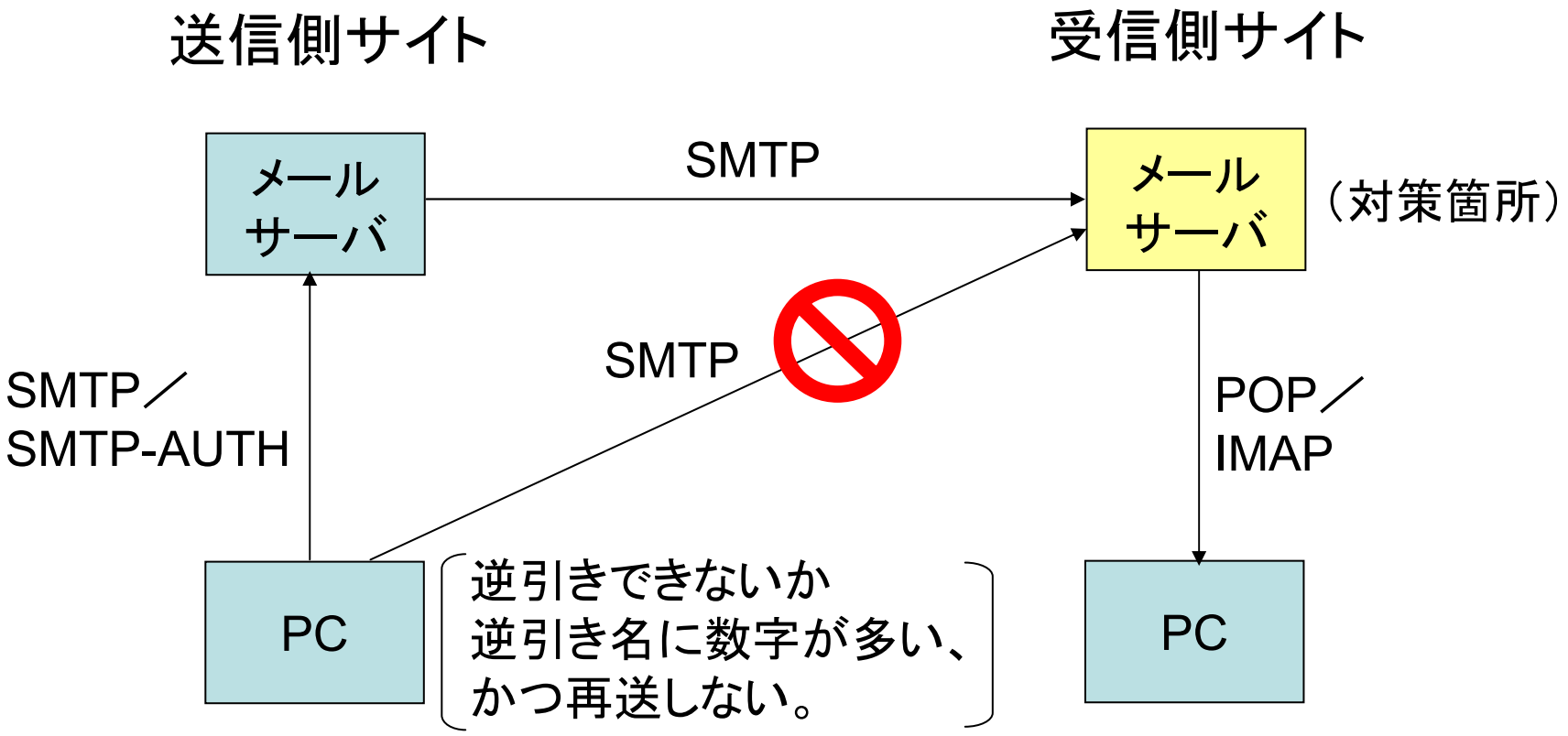
The **S**elective SMTP **R**ejection Anti-spam System
(port **25**)

選択的SMTP拒絶方式

動作原理

- 逆引きに基づいてエンドユーザーコンピュータと推定したホストに再送要求（応答コード「450」）を返して受信拒否。
- メールサーバを誤判定した場合は再送アクセスが来るので、ホストをホワイトリスト登録して受信。

メール経路制限のコンセプト



設定方法

/etc/postfix/main.cf

```
smtpd_client_restrictions =
  permit_mynetworks,
  check_client_access regexp:/etc/postfix/white_list,
  check_client_access regexp:/etc/postfix/rejections
```

/etc/postfix/white_list

```
誤判定されるメールサーバの許可条件
```

/etc/postfix/rejections

```
下記に引っかからないエンドユーザーコンピュータの拒否条件
/^unknown$/                              450 reverse lookup failure, be patient
/^[^.]*[0-9][^0-9.]+[0-9].*¥./                    450 S25R check, be patient
/^[^.]*[0-9]{5}/                                  450 S25R check, be patient
/^([^.]+¥.)?[0-9][^.]*¥.[^.]+¥..+¥.[a-z]/         450 S25R check, be patient
/^[^.]*[0-9]¥.[^.]*[0-9]-[0-9]/                   450 S25R check, be patient
/^[^.]*[0-9]¥.[^.]*[0-9]¥.[^.]+¥..+¥./            450 S25R check, be patient
/^(dhcp|dialup|ppp|[achrsvx]?dsl)[^.]*[0-9]/      450 S25R check, be patient
```

ブロックされるホスト名の例

unknown

evrtwa1-ar3-4-65-157-048.evrtwa1.dsl-verizon.net

pcp04083532pcs.levtwn01.pa.comcast.net

398pkj.cm.chello.no　host.101.169.23.62.rev.coltfrance.com

wbar9.chi1-4-11-085-222.dsl-verizon.net

d5.GtokyoFL27.vectant.ne.jp

dhcp0339.vpm.resnet.group.upenn.edu　PPPbf708.tokyo-ip.dti.ne.jp

スパム阻止率の比較

DNSBL	50～60%？
E-mailレピュテーション	約70%
ベイジアンフィルタ	80～90%
S25R	97～99%

やってはいけないこと

- 「REJECT」と指定する（応答コード「554」）。

- ログを監視せずに再送アクセスを放置する。

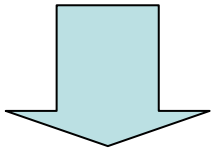
※再送期間はPostfixやsendmailのデフォルト設定で5日（＝救済猶予時間）。
※2日ほどで再送をやめるメールサーバもある。
※1時間ほどで再送をやめるメールサーバは救済困難。公開ホワイトリストの組み込み、またはgreylistingの併用（Rgreyなど）を推奨。

偽陽性（false positive）判定率

ホワイトリストがなければ約13%

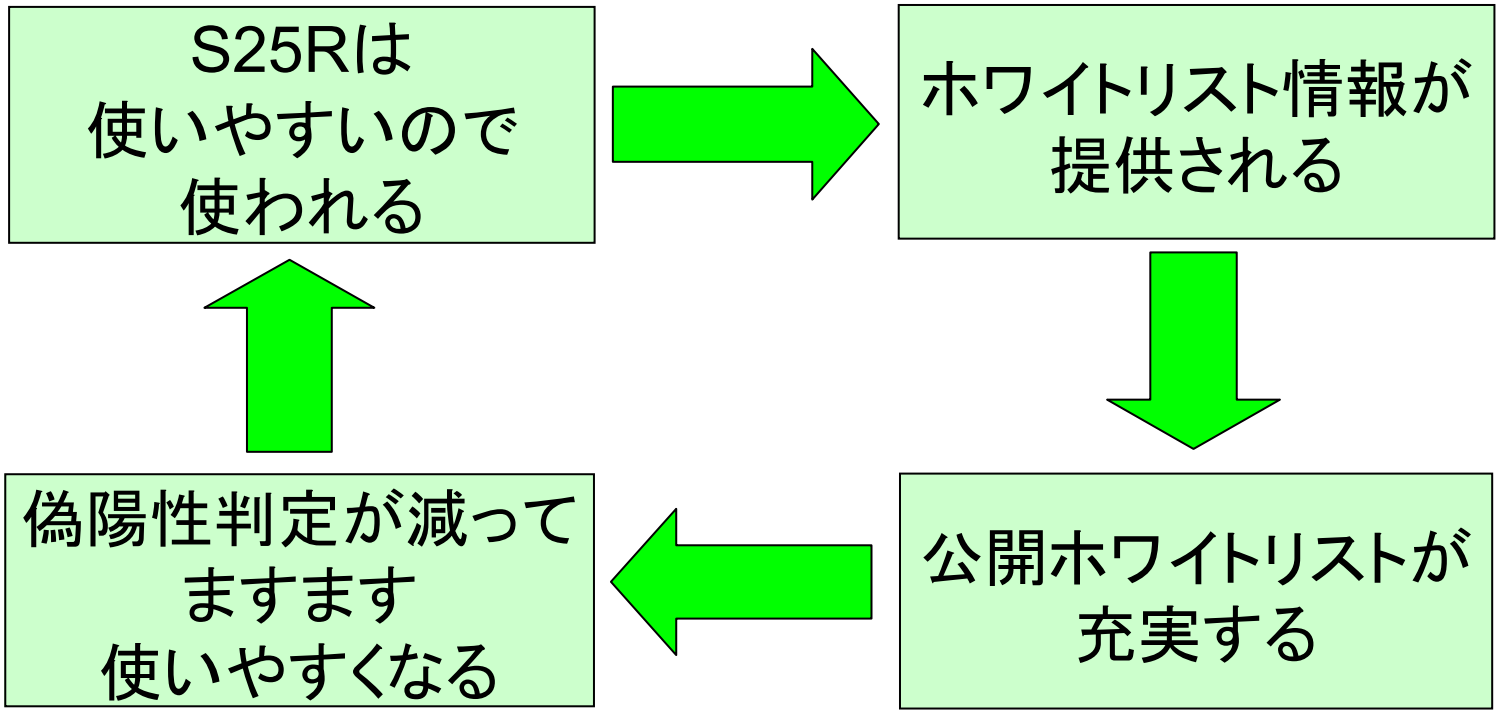
正当なメールサーバがS25Rに引っかかる主なケース

- 逆引きできない／パラノイド検査不適合
- ISPが多くの回線に割り振る連番入りの逆引きホスト名
- 多くのサーバを持つ事業者の連番入りの逆引きホスト名



ホワイトリストの充実で偽陽性判定率は下がる。

ホワイトリストの好循環



公開ホワイトリスト：登録数は現在約700件

再送アクセスを容易に見つけるためのログソーティングスクリプト

- 再送アクセス（IPアドレス、送信者アドレス、受信者アドレスが同じ）は、連続した行で表示。
  ⇒正当なメールサーバの挙動を示していればホワイトリスト登録。

おおむね、1分以上の間隔で
30分以上にわたって再送。

- 再送されなかったアクセスは、空白行で分断された単独の行として表示。
  ⇒ほったらかしてよい。
- 推定メッセージ数（≒対策をしていなければ受けてしまったであろうスパムの数）を表示。
  ⇒統計に使える。

偽陽性判定からの救済の自動化

偽陽性判定からの救済は、greylistingやtarpittingの併用で自動化できる。

	手動	自動
長所	•付加ソフトウェアが不要（Postfixの場合）。 •再送するスパムアクセスに強い。	•監視の労力が少ない。 •再送期間が短くても救済できる。
短所	•監視に労力がかかる。 •再送期間が監視間隔より短いと救済し損ねる。	•付加ソフトウェアが必要。 •再送するスパムアクセスにだまされる（greylistingで阻止率は約1%低下）。

ほかのボランティアによる発展

Postfix用	Rgrey Starpit taRgrey
qmail用	qmail用S25R対応パッチ Qgrey s25rtarpitgreylist
sendmail用	smtp_wrapper milterでの実現
XMail用	XMailCFGでの実現
メールクライアント用	Becky!のフィルタ設定（私） Becky! S25R スパムフィルタ MailUtl3

S25Rに対する賞賛

- 驚異的な効果だ。正当なメールはちゃんと届く。
- スパムのせいでディスクがあふれて困っていた。助かった。
- もう元に戻す気になれない。
- 当社はS25Rを推奨します。（ホスティングサービスの顧客に）

S25Rに対する批判

批判	回答
逆引きできない正当なメールサーバもある。	再送中にホワイトリスト登録して受信できる。
逆引きホスト名に多くの数字を含む正当なメールサーバもある。	再送中にホワイトリスト登録して受信できる。
ダイナミックIPアドレスのメールサーバを排除するものだ。	ISPのメールサーバを経由して送信してほしい。
逆引き結果だけで勝手に決め付けて受信拒否するのは困る。	受信側でのホワイトリスト登録を待ってください。再送アクセスを放置するのは運用の誤り。
個人サイトくらいにしか使い物にならない。	公開ホワイトリストが大規模サイトにも対応できるようになった。
受信が遅延する。	greylistingかtarpittingの併用で遅延を少なくできる。少しの遅延も困るなら使うべきでない。
再送要求で送信側にリソース負荷をかける。	メールが送信キューに滞留しても問題にならない。インターネット中継回線の負荷は減る。

S25Rはなぜ広まったか

導入サイト数：推定1000以上

- 効果が高い。
- 無料で導入できる。
- 高スキルがなくても実装・運用できる。
- 送信側で何かをしてもらう必要がない。
- 公開ホワイトリストが協力者によって充実。
- greylistingやtarpittingの併用が実現。
- qmail、sendmail、XMailにも適用可能になった。
- 名前も良かった？

ISPへの要望　IPアドレス1個の接続でもユーザーが自ドメインの逆引き名を付けることができるサービスの提供

おまけ：将来性を予見するための教訓

普及したものを当初批判した人たち

阿川弘之	・・・	新幹線
糸川英夫	・・・	家庭用VTR
コンピュータのプロやセミプロたち	・・・	Windows

継続した努力で大衆のニーズに
応えたものが勝つ。