S25R スパム対策方式におけるフィルタ制御

内田保雄* 中川一彦**

A spam filtering system by means of the S25R method

Yasuo UCHIDA* , Kazuhiko NAKAGAWA**

Abstract : The aim of this study is to develop a spam filtering system which can reduce not only the troubles caused by an increasing amount of spam but also the burden that a web manager may incur. The S25R anti-spam system using Reverse lookup failure and six Generic rules---the criteria for recognizing spam---as well as whitelists and blacklists was developed by Asami Hideo. The taRgrey, an anti-spam system combining the S25R with tarpitting and greylisting, was also developed by Sato Kiyoshi. Using these anti-spam systems makes it possible to manage spam on the web.

Key words : spam, S25R, taRgrey, tarpitting, greylisting

1．緒言

従来のスパム対策技術にはメールサーバで受信拒否をする方法（ブロッキング）と、メールを受けとってからフィルタリングする方法（フィルタリング）がある。また現在では、送信者認証というのもある。これは、送信者の認証が全く行われず、メールのアドレス（送信者）には信頼性はないという現在のメールの仕組みを、送信者認証を行うことで、スパムの抑制に繋げる技術のことである。しかし、このような認証手法は広く普及しておらず、数年で急速に普及させることも困難である。また、送信者認証ができるようになっても、金融機関などからのメールと偽り個人情報を盗み出す（フィッシング）という被害は防げるが、送信者がはっきりしただけでは、撲滅までには至らない。

現在使われているメール転送プロトコルは SMTP であり、非常に単純かつ、性善説に基づいたプロトコルであったため、これまでスパム対策のため、SMTP-AUTH や POP Before SMTP などの後付けの認証機能が付加されてきたが、SMTP の持ついくつかの欠点は残されたままである。発信者詐称に対する根本的な解決案である Sender-ID や Cellar-ID といった認証の仕組みも考案されたが、広く使われるには至っていないこと、そして現時点では有力な代替プロトコルは決まってないのが実情[1]となっている。

本研究は、上述したブロッキングとフィルタリングを備えた S25R スパム対策方式[1]のブラックリスト、ホワイトリストによるフィルタ制御を、Web インタフェースによりメンテナンスできるようにすることが目的である。

（2007 年 12 月 4 日受理）

*宇部工業高等専門学校　経営情報学科
**宇部工業高等専門学校　経営情報工学専攻

2．スパム

スパム（メール）とは、多数の利用者を対象に無差別かつ大量に配信されるメールのことであり、迷惑メールとも呼ばれる。スパムを送信してくる人物をスパマーと呼ぶ。

2.1 スパムという言葉の意味

スパムは、受信者の承諾なく送られる宣伝広告メールのうち、法律に定められた形式（特定商取引に関する法律：第二章　訪問販売、通信販売及び電話勧誘販売　第三節　通信販売（第十一条）を守らずに配信されるものを指すため、承諾を取らずに配信される広告でも、件名に「未承諾広告※」の表示をつけるなど、法律で定められた書式で送られているものは、スパムとは呼ばない。また、受け取りたくないと思うメールのすべてが、スパムに該当するわけではなく、自ら以前に配信を希望したものの、今は受け取りたくないと思っている企業からのメールは、スパムではない。

・著者の考えるスパムと対応

他人にとってスパムであったとしても、受信者本人にとってスパムになるとは限らない。受け取る人にとって必要となる情報であるならスパムとはいえない。また時期によって昔は必要としない情報でスパムとしかなりえなかったものが、ある時を境に必要となる情報になるならその人にとってはスパムとはいえなくなると思うが、上述のように「自ら以前に配信を希望したものの、今は受け取りたくないと思っている企業からのメール」は、スパムではないとされている。こ

の考えによるスパム判断のように、個人個人がスパムと思うメールをブラックリストに追加したり、スパムではないと思うメールをホワイトリストに追加したりすることを簡単にできるシステムを開発することが目的である。

2.2 スパムの送信手段

代表的なスパムの送信手段として、次のようなものが挙げられる。

・送信者情報を偽った送信
・知人を装ったメール
・架空アドレスにあてた送信
・自動収集したアドレスの利用
・複数のプロバイダ等を渡り歩いての送信
・外国のサーバを経由したように偽った送信

2.3 スパムによる被害

・個人
　- スパムを削除する時間の浪費。
　- スパムに埋もれることによる大切なメールの見落とし。
・企業
　- 迷惑メールによるシステムダウン。
　- メールやメールマガジンなどを顧客との連絡手段として活用している企業の活動を妨害。
・その他
　- インターネット上の「情報の渋滞」の原因。

2.4 スパム対策技術

現在スパム対策として知られている技術にはブロッキング、フィルタリング、スロットリング、送信者認証といった技術がある。

・ブロッキング
　メールサーバで、受取人のメールアドレスが存在しない場合、メールを受信拒否する方法
・フィルタリング
　メールを受信してからブラックリストやホワイトリスト、ベイジアン・フィルタ等でフィルタリングする方法
・スロットリング
　高速大量配信であり、再送を行わず、タイムアウトが短いというスパムの特徴を利用して、SMTP セッションの応答をゆっくり返す方法
・送信者認証
　送信元のメール・アドレスと IP アドレスから送信者を認証し、送信者を偽っていた場合にスパムと判断する方法

3．選択的 SMTP 拒絶方式

スパム阻止を管理しやすくし、スパム被害を減らすために、浅見秀雄によるスパム対策である選択的 SMTP 拒絶方式 (Selective SMTP Rejection：略称 S25R) を本研究に利用することにした。

S25R は、一般規則である逆引き失敗と逆引き成功ではあるがスパムであるというメールの IP アドレスの逆引き名（完全修飾ドメイン名）の特徴に基づいて作られた 6 つのルール、そしてこの一般規則をすり抜けるスパムを阻止するためのブラックリストやスパムではないがその一般規則にひっかかるメールの救済のためのホワイトリストによって、スパムとウィルスメールを合わせた不正メール対策方式である。

3.1 S25R での逆引き失敗

S25R では逆引きによって、完全修飾ドメイン名が見つからないときや、見つかりはしたものの、その完全修飾ドメイン名を正引きした結果、元の IP アドレスとは一致しない IP アドレスが見つかった場合を逆引き失敗としている。

・逆引き
　192.168.0.1 のような IP アドレスから www.7key.co.jp といった完全修飾ドメイン名を調査することをいう。
・正引き
　www.7key.co.jp のような完全修飾ドメイン名から 192.168.0.1 といった IP アドレスを調査することをいう。
・完全修飾ドメイン名
　ドメイン名・サブドメイン名・ホスト名を省略せずにすべて指定した記述形式のこと。
　例) m500.union01.nj.comcast.net

S25R では「.」によって層を分け、左から一層、二層…となる。左端にいくほど下位層となり、右端にいくほど上位層となる。この各層の特徴からスパムの判断となる 6 つのルールが作られた。

3.2 6 つのルール

S25R において定められているルールであり、一般規則[i)]の 1 つである。

ルール 1：逆引き完全修飾ドメイン名の最下位（左端）の名前が、数字以外の文字列で分断された二つ以上の数字列を含む
　例) 220-139-165-188.dynamic.hinet.net

ルール 2：逆引き完全修飾ドメイン名の最下位の名前が、5 個以上連続する数字を含む
　例) YahooBB220030220074.bbtec.net

ルール 3：逆引き完全修飾ドメイン名の上位 3 階層を除き、最下位または下位から 2 番目の名前が数字で始まる
　例) 398pkj.cm.chello.no

ルール 4：逆引き完全修飾ドメイン名の最下位の名前が数字で終わり、かつ下位から 2 番目の名前が、1 個のハイフンで分断された二つ以上の数字列を含む
例）wbar9.chi1-4-11-085-222.dsl-verizon.net

ルール 5：逆引き完全修飾ドメイン名が 5 階層以上で、下位 2 階層の名前がともに数字で終わる
例）m500.union01.nj.comcast.net

ルール 6：逆引き完全修飾ドメイン名の最下位の名前が「dhcp」、「dialup」、「ppp」、または「adsl」で始まり、かつ数字を含む
例）dhcp0339.vpm.resnet.group.upenn.edu

3.3 ブラックリストとホワイトリスト

・ブラックリスト
一般規則をすり抜けるスパムを拒絶するためのもので、ブラックリストに加えることにより拒絶できるようにする。

・ホワイトリスト
一般規則でスパムではないのにスパムと判断されてしまったメールを救済するためのもので、ホワイトリストに加えることによりメールを受信できるようにする。

3.4 S25R の問題点

効果はあるが、逆引き失敗や 6 つのルールによって拒絶を行う中で、スパムではないメールでも逆引き失敗する場合や逆引き成功しても 6 つのルールに引っかかる場合が存在する。S25R ではホワイトリストでそのようなメールを救済しているためにリスト追加といったメンテナンスが必要となる。そのため、導入時ではホワイトリストのメンテナンスに労力を割く必要がある。また、導入にあたって規模が大きくなると管理が大変となり運用が難しい。これらの問題点を解決できる手法である taRgrey を佐藤潔が作った。

3.5 taRgrey

S25R に tarpitting と greylisting というスパム対策を組み合わせて使うというもので、S25R での逆引き失敗、6 つのルールに当てはまったメールには tarpitting(応答の遅延)をかけ、遅延を抜けられなかったものに greylisting(再送のチェック)をかけ、そこから 2 回再送されたメールは救済するという方法である。これにより、スパムの拒絶率は S25R に比べると低くなったが、正当なメールをスパムとしてしまう誤検出を少なくした。

・tarpitting
スパマーは短時間で大量のスパムを送信してくる。そのため、遅延を促されることはスパマーにとって非効率となる。したがって、遅延を促すことでスパマーから切断するようになる。tarpitting はこの特徴を利用し、受信時に返答を遅延させることでスパムを排除するスパム対策である。

・greylisting
スパマーは短時間で大量のスパムを送信してくる。そのため、再送要求されることはスパマーにとって非効率となる。greylisting はこの特徴を利用し、届いたメールを一度 reject で再送要求し、再送要求に応じたら受け取るというスパム対策である。副作用として再送待ちによるメールの遅延や、正しいメール送信元からのメールの排除があるが、taRgrey ではあやしい接続元に対してだけ再送要求するため副作用は少ない。

・taRgrey の仕組み
taRgrey は、図 1 の仕組みにより受信・拒絶の判断を行う。

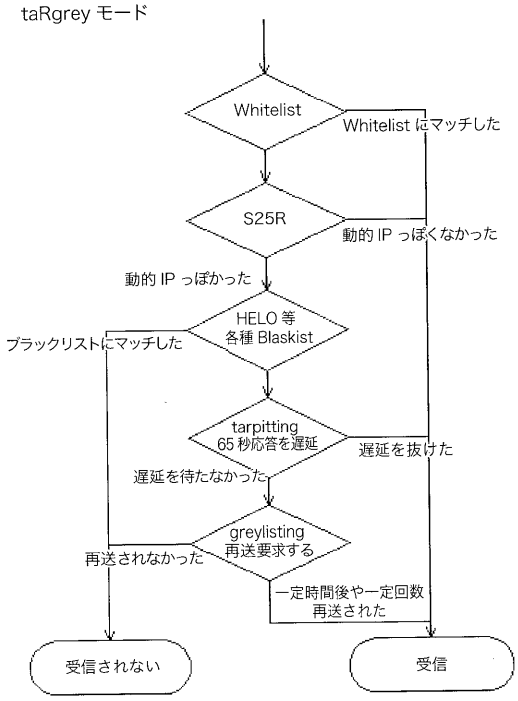

図 1：taRgrey の仕組み[ii)]

4．Web インタフェースによるメンテナンス

S25R の問題点と思われるホワイトリストのメンテナンス作業は、管理者にとっては大きな普段となる。そのため、Web 上で簡単にホワイトリスト、ブラックリストを管理できるシステムを開発した。

Web 上で拒絶されたメールや受信されたメール情報について参照することができるようにし、そのメール情報から一般ユーザでも簡単にホワイトリストへの追加やホワイトリストからの削除、ブラックリストへの追加やブラックリストからの削除が行え、リスト状況の確認もできるようにした。

4.1 メンテナンスの仕組み

メンテナンスの仕組みは次のとおりである。

(1)maillog より拒絶メールまたは受信メールを抽出し、Web 上に表示
(2)Web 上に表示されたメール情報からブラックリストまたはホワイトリストへの登録をするか否かを選択
(3)Web 上で現在のブラックリストまたはホワイトリストを見て、登録されているリストを削除可能

4.2 メンテナンス画面構成

メンテナンス画面の構成は次のとおりである。

ユーザ認証画面
　└機能選択画面
　　└ブラックリスト一覧表示&削除画面(black-list)
　　└ホワイトリスト一覧表示&削除画面(white-list)
　　└受信メール一覧表示＆ブラックリスト登録画面(accept-mail)
　　└拒絶メール一覧表示＆ホワイトリスト登録画面(reject-mail)

・black-list

ブラックリストに登録されている IP アドレスを一覧表示する。

削除にチェックを入れて更新を行うことでブラックリストからその IP アドレスは削除される。

削除以降、ブラックリスト未登録となるため、S25R による拒絶がない限り、受信されるようになる。

削除	ブラックリスト
☐	/\.(internetdsl|adsl|sdi)\.tpnet\.pl$/
☐	/^user.+\.mindspring\.com$/
☐	/^[0-9a-f]{8}\.(.+\.)?virtua\.com\.br$/
☐	/\.catv\.broadband\.hu$/
☐	/[0-9a-f]{4}\.[a-z]+\.pppool\.de$/
☐	/\.dip[0-9]+\.t-ipconnect\.de$/
☐	/\.dip\.t-dialin\.net$/
☐	/\.dyn\.optonline\.net$/
☐	/\.(adsl|cable)\.wanadoo\.nl$/
☐	/\.ipt\.aol\.com$/
更新 リセット	戻る

図2 ブラックリスト一覧表示&削除画面

・white-list

ホワイトリストに登録されている IP アドレスを一覧表示する。

削除にチェックを入れて更新を行うことでホワイトリストからその IP アドレスは削除される。

削除以降、ホワイトリスト未登録となるため、S25R による拒絶にひっかかると、拒絶されるようになる。

削除	ホワイトリスト
☐	/\.bay[0-9]+\.hotmail\.com$/
☐	/\.data-hotel\.net$/
☐	/^web[0-9]+\.mail\.(.+\.)?yahoo\.co\.jp$/
☐	/^web[0-9]+\.mail\.(.+\.)?yahoo\.com$/
☐	/^221x115x158x242\.ap221\.ftth\.ucom\.ne\.jp$/
☐	/^207\.171\.(167\.25|172\.6)$/
☐	/\.data-hotel\.net$/
☐	/^ps23\.suite2\.arena\.ne\.jp$/
☐	/\.bay[0-9]+\.hotmail\.com$/
☐	/^221x115x147x174\.ap221\.ftth\.ucom\.ne\.jp$/
更新 リセット	戻る

図3 ホワイトリスト一覧表示&削除画面

・accept-mail

受信したメールを日付、ホワイトリスト登録済か未登録、送信元アドレス、送信先アドレスの情報を 20 件ずつ表示する。

ブラックリスト登録にチェックを入れて更新することでその受信メールの IP アドレスがブラックリストに登録され、次回から拒絶されるようになる。

ただしホワイトリストに登録されている受信メールをチェックして更新した場合は、ホワイトリストに登録されている IP アドレスは削除され、ブラックリストに登録される。

*ホワイトリスト登録済○ 未登録×

Black-list(B)	*登録	受信日付	送信元
☐B	×	Nov 5 16:28:38	mmz-3868ikakoka=skyfly.itbdns.com@magerr.combzmail.jp
☐B	×	Nov 5 18:29:40	mmz-3868=65086250775525=2jhj2pp=473=ikakoka=skyfly.itbdns.com@magerr.c
☐B	×	Nov 6 18:55:45	mmz-3868=65086252734877=2jhj2sh=473=ikakoka=skyfly.itbdns.com@magerr.c
☐B	×	Nov 7 19:35:54	mmz-3868=65086253753751=2jhj2va=473=ikakoka=skyfly.itbdns.com@magerr.c
☐B	×	Nov 11 11:11:59	mattari-sumurai-nice@ezweb.ne.jp

図4 受信メール一覧表示&ブラックリスト登録画面

・reject-mail

拒絶されたメールを日付、ブラックリスト登録済か未登録、拒絶内容、送信元アドレス、送信先アドレスの情報を 20 件ずつ表示する。

拒絶内容には、拒絶された理由が書かれており、domain UCE-blacklisted(ブラックリスト登録されている)、cannot find your hostname、[202.143.94.34](逆引きを失敗した)、may not be mail exchanger(6 つのルールのいずれかに一致した)などの内容が表示される。

ホワイトリスト登録にチェックを入れて更新することでその拒絶メールの IP アドレスがホワイトリストに登録され、

次回から受信されるようになる。

ただしブラックリストに登録されている受信メールをチェックして更新した場合は、ブラックリストに登録されているIPアドレスは削除され、ホワイトリストに登録される。

*ブラックリスト登録済○ 未登録×

White-list(W)	*登録	拒絶日付	拒絶内容	送信元	送信先
W	×	Nov 4 13:32:49	reverse lookup failure, be patient;	bfsn64n1lvci@yahoo.co.jp	IKAKOKA@SKYFLY.ITBDNS.COM
W	×	Nov 4 15:06:25	S25R check2, be patient;	onlinebanking@wamu.com	ikakoka@skyfly.itbdns.com
W	×	Nov 4 19:24:57	S25R check2, be patient;	onlinebanking@wamu.com	ikakoka@skyfly.itbdns.com
W	×	Nov 5 23:04:13	reverse lookup failure, be patient;	rtaubvnhcpd@yahoo.cn	ikakoka@skyfly.itbdns.com
W	×	Nov 5 23:25:00	S25R check2, be patient;	onlinebanking@wamu.com	ikakoka@skyfly.itbdns.com

図5 拒絶メール一覧表示&ホワイトリスト登録画面

5．S25RとtaRgreyによる運用結果

先行研究であるS25RおよびS25Rとtarpitting、greylistingを組み合わせたtaRgreyを実際に導入し、どのように効果があるかを検討するため、各スパム対策を一週間ずつ運用し、そのデータを元に分析した。また、用いたブラックリスト、ホワイトリストはS25Rに載せてあるものをそのまま使用し途中追加なしとした。

表1 S25R実装時での7日間の分析結果

逆引き失敗	358	68.8%
6つのルール	108	20.7%
ブラックリスト	25	4.8%
受信合計	29	5.5%
拒絶合計	491	94.4%
false positive	0	0%
false negative	29	5.5%

S25Rを実装してから7日間送信されてきたメールの拒絶と受信は表1のようになった。

S25R実装時での7日間でメールサーバに送信してきたメール総数は受信合計と拒絶合計の和にあたる520件であった。そのうち逆引き失敗したメールは358件であり、逆引き成功したが6つのルールと一致したメールは108件であった。逆引き失敗と6つのルールである一般規則をすり抜けたメール54件のうちの25件はブラックリストに引っかかり、残りの29件がスパムではないと判断され受信された。また、false positive（正しいメールを誤まってスパムと判断する）は0件であり、false negative（スパムを誤って通してしまう）は29件であった。表1の割合は、メール総数である520件に対しての割合を示している。

浅見秀雄による統計データ（2004年4月：1ヶ月間）では1ヶ月間に送信されてきたメール総数のうち36.4%が逆引き失敗したとなっている。今回収集したデータで表1のように逆引き失敗したメールは68.8%であった。データ収集の期間の違いや環境の違いがこの差違を生んだものと思われる。しかし、表1を見ると分かるように効果はあるといえる。データ収集をした7日間ではスパムしか送られてこなかったが、同一環境で以前送信された知人10人からのメールではfalse positiveとなることはなかった。

表2 taRgrey実装時での7日間の分析結果(--tarpit=65 --retry-count=2)

S25R(一般規則)	158	80.6%
遅延拒絶	138	70.4%
遅延受信	20	10.2%
返送通告1回目	122	62.2%
返送通告2回目	20	10.2%
返送受信	7	3.5%
受信(38件中スパムは35件)	38	19.3%
受信合計	65	33.1%
拒絶合計	131	66.8%
false positive	0	0%
false negative	62	31.6%

taRgreyを実装してから7日間送信されてきたメールの拒絶と受信は表2のようになった。また、--tarpit=65 --retry-count=2は遅延時間と再送回数を示しており、--tarpit=65で遅延時間65秒、-retry-count=2で再送回数を2回と定めている。

taRgrey実装時での7日間でメールサーバに送信してきたメール総数は受信合計と拒絶合計の和にあたる196件であった。そのメールの中でS25Rによりスパムと判断されたメールは158件であり、そのうち遅延によりスパマーから切断してきたメールは138件で残りの20件は65秒の遅延を抜けスパムではないと判断され救済された。遅延によってスパマーから切断してきたメールは次回送信してくると返送をするように通知されるようになっており、1回目の返送通知を受けたメールは122件、その通知により返送をしてきたメールは20件、この20件には2回目の返送通知が送られ、その通知により返送してきたメールは7件だった。この7件は遅延によって切断してきたが、2回の返送通知においてきちんと返送してきたことにより、スパムではないと判断され救済された。表2の割合は、メール総数である196件に対しての割合を示している。

この度の7日間のデータでは、正しいメールがスパムと判

断されることはなかったが、救済されたメールはすべてスパムであった。false positive を減らす仕組みになっているのが taRgrey なので、false negative が増えてしまう。false positive をなくすことが重要であると考えるため、表 2 の結果は悪いとはいえない。また受信したスパムは 35 件だが、これらは 7 つの IP アドレスからの受信であり、S25R をすり抜ける 1 つの IP アドレスからは 20 件も送られてきていることが分かった。

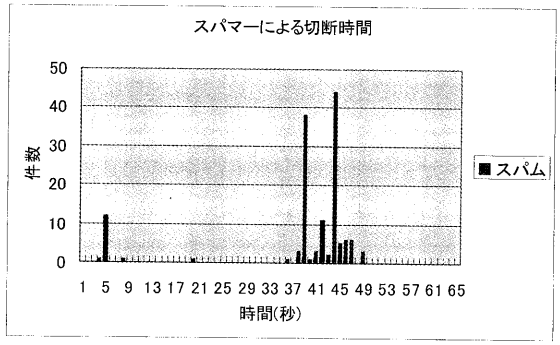

図 6 taRgrey 実装時での 7 日間の分析結果のうち遅延時間によるスパマーからの切断時間

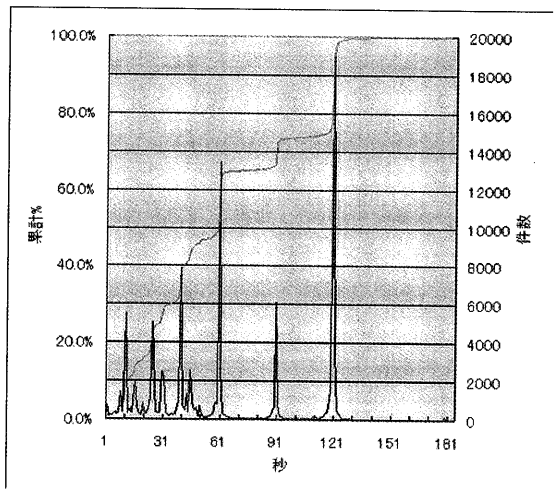

図 7 taRgrey の遅延時間[iii]（出典：和歌山大学システム情報学センターの吉田敦）

佐藤潔のブログ[iii]には他にも 2 件の同様な結果がある。図 4 と似た形となっており、どのグラフも約 120 秒でほとんどのスパマーが切断していることが示されていた。65 秒設定では 60%のスパムしか切断できないことが示されている。今回収集したデータでは遅延時間を taRgrey 標準設定である 65 秒としているため、追試によりこの 120 秒を確かめることはできなかった。今回収集したデータでは図 3 のように 35～50 秒にスパマーの切断時間が集中しており、佐藤潔のブログにある結果でも 30 秒前後や 60 秒前後で切断時間が集中しているため、この結果にそれほど間違いはないことが分かる。taRgrey では false positive を抑えるような設定となっている。

もし、遅延時間を約 120 秒に設定すると false positive が増えるかもしれない。そのため、今の 65 秒のままでも、ホワイトリストとブラックリストの管理をすることで十分と思われる。ただし、false negative が迷惑なほどであるなら、約 120 秒の遅延時間の設定を試してみる価値はある。

表 3 Postfix 初期実装時での 7 日間の分析結果

受信	286
拒絶率	0

taRgrey または S25R を実装したときの結果と実装していないときの結果を比較するために、Postfix のみでの 7 日間のデータ収集を行った。この度の収集では拒絶は 0 件となり、false positive も 0 件だが、すべてのスパムを受信してしまっていることが示された。

6．結言

スパム阻止は望まれるが、阻止率をあげることを優先するあまり、スパムではないメールをスパムと判断してしまう確率をあげてしまってはならない。スパム対策は、受信したいメールを受信者が受けられないというリスクを避けつつ阻止率をあげることが重要であると思われる。このことから false positive が 0 に近いシステムほど優れているといえる。その問題を考えると設定内容から拒絶率が高い S25R よりも、taRgrey の方が false positive を抑えられるのでより優れていると思われる。今回の分析結果からは taRgrey ではスパムを受信しすぎているように見えるが、1 箇所からのスパム送信が多いためであり、ブラックリストとホワイトリストを管理することで解決できる。したがって、今回作成した Web インタフェースによるメンテナンスを利用することで、管理者の負担を軽減することができると同時に、性能を向上させることができるといえる。

謝辞

本研究は、宇部工業高等専門学校平成 18 年度特別教育研究費「S25R スパム対策方式における正当メッセージ拒絶監視システムの開発」（内田保雄）の支援を受けた。記して感謝の意を表する。

参考文献

1) 山井成良・桝田秀夫：特集 spam メールの現状と対策の動向「編集にあたって」，情報処理，Vol. 46 No. 7, pp. 739-766, 2005.

注釈

ⅰ）浅見秀雄がスパムを阻止するために考案したスパム対策(S25R)の仕組みである。
http://www.gabacho-net.jp/anti-spam/anti-spam-system.html を参照。

ⅱ）佐藤潔がS25Rにtarpitingとgreylistingを組み合わせて改良したスパム対策方式である。
http://d.hatena.ne.jp/stealthinu/20061206/p1 を参照。

ⅲ）taRgreyでのtarpittingによる遅延時間の適当な時間を調査するために、スパマーから切断した時間をグラフとしたものである。
http://d.hatena.ne.jp/stealthinu/20070703/p1 を参照。