2004－ＤＳＭ－33　（５）
2004／5／13

アクセス制御とSPAMフィルタを組み合わせた動的SPAM拒否システム

渥美　清隆†

† 静岡大学総合情報処理センター
〒 432-8561 静岡県浜松市城北 3-5-1
E-mail: †kiyotaka@ka-lab.ac

あらまし　本研究はメール管理者に多くの負担をかけることなく，ユーザに届く SPAM メールを削減し，さらにインターネットトラフィックに占める SPAM メールトラフィックの総量を減少させる効果が期待できる動的 SPAM 拒否システムを提案する．具体的にはメールユーザの期待に応える部分として，既存のコンテンツ分析型 SPAM フィルタを適用し，トラフィック量を減少させる部分として，「一見さんお断り」方式による SMTP 接続制御を適用する．この 2 つのシステムを同時に機能させるための仕組みを提案し，どのような効果があったかを報告する．

キーワード　SPAM メール，SPAM フィルタ，SMTP，一見さんお断り，管理コストの低減

A Dynamic SPAM Rejection System which Combined Access Control and a SPAM filter

Kiyotaka ATSUMI†

† Information Processing Center, Shizuoka University
5-1, Johoku-3, Hamamatsu city, Shizuoka Pref., 432-8561, in Japan
E-mail: †kiyotaka@ka-lab.ac

Abstract　This paper show a dynamic SPAM mail refusal system with an administrator's light burden. This system can cut down the SPAM mails which reaches a user and decrease the total amount of the SPAM mail traffic occupied to the Internet traffic. This system has the parts of a SPAM filter, and the parts of SMTP connection control. The parts of a SPAM filter can meet the demand of each user, and SMTP connection control can reduce the amount of traffic with a "Glimpse Mr. Notice system." In this paper, I propose the structure for operating these two parts simultaneously and report how many SPAM mails this system cut down.

Key words　SPAM Mail, SPAM Filter, SMTP, Glimps Mr. Notice, Reduction of Management cost

1. はじめに

現在，インターネットが多くの人たちに接続されるようになってきたが，その一方で特定の人たちが大量のインターネット上のトラフィックを占有する問題が発生している．ここで言う，インターネット上のトラフィックの占有は，通信路の占有だけでなく，中継するネットワーク装置やサーバのパフォーマンスの占有も含んでいる．このようなトラフィックの占有は主に p2p アプリケーションなどによるものと，SPAM メールによるものと考えられている．SPAM メールは不特定多数の人たちに送られるので，受け取った人たちの業務時間をも占有してしまうと言う点で p2p アプリケーションの問題よりも悪いと言うことが出来る．また，SPAM メールを送信するためのコストが相当安くなり，一般企業が SPAM メール送信の誘惑に駆られやすくなったことも事態をより深刻なものとしている．

SPAM メール対策の詳細については 2. 節で述べるが，それぞれの方法に長短があり，これで十分と思われる方法がない．また，SPAM 送信者のリストを作成するなどの取り組み [7] も行われているが，そのリストの維持管理に莫大なコストを支払っている．

本研究では，実用上の観点から，あらゆるコストの上昇を出来る限り伴わずに，SPAM メールを排除する方法として，「一見さんお断り」方式 [6] と SPAM フィルター [1], [2] を組み合わせた方法を提案する．この方法は SPAM メールを排除するだけでなく，SPAM メールの到着そのものも拒否出来るので，SPAM メールによってネットワークが占有されることを回避できる．また，SPAM メール送信者にコストを強制的に負担させることになるので，そもそも SPAM メールを送信しなくなる

ことが期待できる．

本論文では 2. 節で既出の SPAM メール対策について概観する．3. 節で，本研究の提案するシステムについて述べ，そのシステムの実験結果を 4. 節で述べる．

2. 既出の SPAM メール対策

SPAM メールを排除するために様々な方法が提案されているが，これらは大きく 3 つの型に分類することができる．1 つ目はメールの内容を検査して SPAM メールかどうかを判定する方法である．2 つ目はメールの内容を読み込まずに，接続元の IP アドレスや SMTP セッションにおける挙動で SPAM メール送信者であるかどうかを判定する方法である．3 つ目は SPAM メール送信者かどうかに関わらず，SMTP 接続する際に一定のコストを支払うことを強制する方法である．さらにそれぞれの方法は次のように細分化される．

- メールの内容を検査して判定する方法
  - （1） ベイジアンフィルタなどの学習判別 [1]〜[3]
  - （2） ブラックワードリストによる判別
  - （3） Received の妥当性判定 [10]
  - （4） From, To の妥当性判定
  - （5） 電子証明書などで送信者を判定 [13]
- 通信セッションで判定する方法
  - （1） 公開されたブラックリストの利用 [7]
  - （2） 接続相手の DNS 検査 [6], [11], [12]
  - （3） SMTP 接続を一時拒否してその後の再接続状況で判定 [5]
  - （4） SMTP セッション中の HELO, MAIL FROM, RCPT To の引数を検査
- SMTP 接続に対するコストの強制
  - （1） 法律による規制と法律違反通報システム [8]
  - （2） ISP による課金 [9]
  - （3） 故意な通信遅延による時間コスト支払いの強制 [4], [5]

それぞれの方法には以下のような得失があり，いずれについても単独で使用するだけでは不十分なようである．

- メール内容の検査

利点　柔軟な処理が可能．学習機能があればメールユーザの個別要求に応えることも可能．

欠点　SPAM メールを受け取った後に判定するため，SPAM メールトラフィックが減ることを期待できない．

- 通信セッション検査

利点　セッション遮断により SPAM メールのトラフィックの減少が期待できる．

欠点　メールユーザが要求するメールまで遮断してしまう可能性がある．

- 強制的なコスト徴収

利点　コストに見合った SPAM メールのみが送信されるので，SPAM メールのトラフィックの減少が期待できる．

欠点　全てのメール送信者がコストの負担を強制させられる．コスト負担回避方法が用いられる．

本研究では，ベイジアンフィルタなどのメール内容の検査，ブラックリストと一時拒否などの通信セッション判定，時間コストの強制を組み合わせた手法を提案するので，それらの手法についてのみ，もう少し詳しく説明する．

ベイジアンフィルタに代表されるメール内容の検査による SPAM フィルタリングは広告メールが増えだした頃から行われてきている，この分野では比較的古くから検討されてきた方法である．フィルタリングの能力はそのアルゴリズムなどによって左右されるが，いずれの場合にもメールを一旦受け取った後に処理をするため，SPAM メール送信者には受け取ったと思われてしまう欠点がある．このため，SPAM メール送信者は何度もユーザに SPAM メールを送信してしまい，いずれはネットワークの帯域を圧迫しかねない状況となることが予想される．

一方，SMTP 接続制御による方法は，メールの内容を調査せず，メールサーバへの接続元が SPAM を送信するか否かを予想し，SPAM 送信者と予想すれば接続を拒否するものである．RBL などのブラックリストを利用する場合は，RBL に掲載された IP アドレスが接続元で有れば遮断する．一見さん拒否の場合，一度目の接続は拒否し，数分後の 2 度目の接続時にメールを受け取るようにする．これは，SPAM 送信者が使う送信プログラムが，ネットワークの一時的な切断や遅延に対応出来ていないことを利用している．「一見さんお断り」の場合，一度目の接続拒否という行為が SPAM メール送信者に時間的コストの強制的支払いをさせている点も注意しなければならない．

3. 提案するシステムの構成

本システムは図 1 のように，SMTP 接続制御部，リストコントローラ，コンテンツ分析型 SPAM フィルタ部から構成されている．SMTP 接続制御部は透過型ネットワーク装置として構成されているため，ネットワーク上の何処にでも配置可能であるが，説明のため，メールサーバの直前に配置したと仮定する．

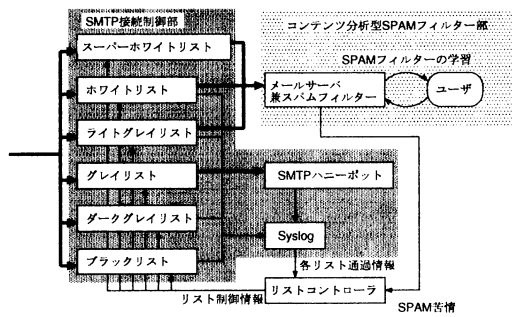

図 1　本システムの構成

3.1 SMTP 接続制御部

SMTP 接続制御部では，スーパーホワイトリスト，ホワイトリスト，ライトグレイリスト，グレイリスト，ダークグレイリスト，ブラックリストを管理しており，IP アドレスが登録される．それぞれのリストに登録されている IP アドレスは SPAM メール送信者の可能性を示しており，表 1 の処理を行う．

ここで，偽受信とは SMTP サーバに偽装した SMTP ハニー

表 1　リスト別の処理

リスト名	処理	意図
スーパーホワイト	通過	ユーザから指定されたメールサーバ
ホワイト	通過	SPAM メール送信者ではないと思われるメールサーバ
ライトグレイ	通過	SPAM メール送信者かもしれないが一旦受理するメールサーバ
グレイ	偽受信	SPAM メール送信者かどうかを調査
ダークグレイ	遮断	初期状態
ブラック	遮断	SPAM メール送信者と判定されたメールサーバ

ポットに SMTP 接続をリダイレクトすることである．

メールサーバ向けへのメールは一旦 SMTP 接続制御部が受信を開始する．送信元がスーパーホワイトリスト，ホワイトリスト，ライトグレイリスト，グレイリスト，ブラックリストのいずれに登録されているかをチェックし，表 1 に従って，メールの通過，偽受信，遮断の処理をする．遮断の場合，送信元から，それ以上の受信は無視する．通過の場合は，送信元から送信されるデータに対して特に何らの処理を加えること無しに，メールサーバにそのままデータを転送する．偽受信の場合は，送信元から送信されるデータを全て SMTP ハニーポットに転送し，送信元と SMTP ハニーポットとを通信させる．SMTP ハニーポットは送信元からの要求に対して 10 秒以上かかるように応答するように作る．これは，SPAM メール送信者があまり応答の良くない SMTP サーバへ通信を諦めてくれる可能性があるためである．この通信では，HELO, MAIL FROM, RCPT TO のみの確認を行い，実際のデータ受信を行う前にエラーコード 451 を送信元に通知する．エラーコード 451 はメールサーバ内で発生した回復見込みがある一時エラーを表し，送信元に対して暫くたってから再送してほしいことを示している．送信元がどのリストにも記録されていない IP アドレスであった場合，ダークグレイリストに登録されているものとして，遮断の処理を行う．SMTP 接続制御部では，ダークグレイリストを管理していないが，リストコントローラでは管理しており，その IP アドレスがダークグレイリストに登録されていなければ，ダークグレイリストに登録する．スーパーホワイトリストに登録されている IP アドレスからの送信の場合を除いて，SMTP 接続制御部で処理した全ての IP アドレスについて，それぞれのリスト名を付与して Syslog に記録する．

3.2　リストコントローラ

リストコントローラは各リストに登録されている IP アドレスの更新を行う部分である．本システムでは，メールを送信しようとする IP アドレスは SPAM メール送信者の可能性をリストという形で表現している．これは，各 IP アドレスが持っている状態とも捉えることが出来，リストコントローラは各 IP アドレスの状態を何らかの条件に従って，状態遷移させる部分とも言える．状態遷移した場合，その情報を SMTP 接続制御部に通知し，リストを更新する．状態遷移は図 2 の通りである．

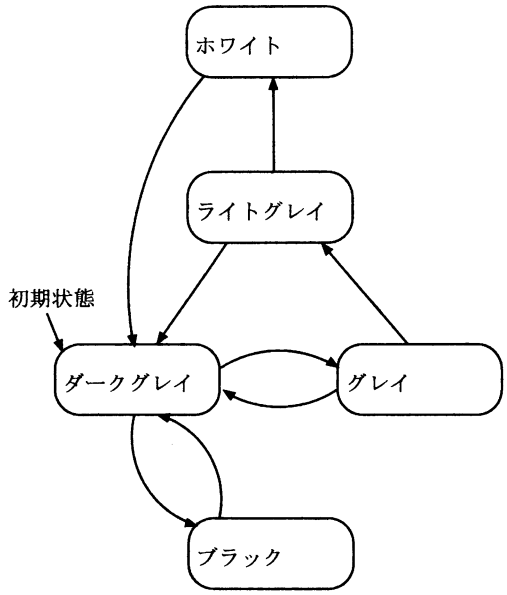

図 2　送信者状態の遷移

状態遷移するための条件を表 2 に示す．ただし，これらの条件は過去 2 週間の範囲内でのみ検索される．

表 2　状態遷移の条件

状態遷移	条件
ホワイト → ダークグレイ	一度も通信がないか，後で述べる SPAM メール苦情を受け付けた
ライトグレイ → ホワイト	5 回以上メールが通過し，許可回数が遮断回数よりも 2 倍以上大きく，一度も SPAM メール苦情を受けていない．
ライトグレイ → ダークグレイ	ライトグレイになってから 3 時間以上経過しても，メール送信の試みがない．
グレイ → ライトグレイ	メール送信の試みがあり，SMTP ハニーポットと HELO, MAIL FROM, RCPT TO の交信が出来たら．
グレイ → ダークグレイ	グレイになってから 3 時間以上経過しても，メール送信の試みがない．
ダークグレイ → グレイ	メール送信の試みがあったら．
ダークグレイ → ブラック	1 どもメールの通過が無く，5 回以上遮断された場合
ブラック → ダークグレイ	2 週間の間に一度も通信がない．

それぞれの状態遷移の意図は次の通りである．ホワイトリスト，ブラックリストからの遷移は，その IP アドレスを持っている計算機の機能の変化に合わせるものである．メールサーバの機能が無くなったり，ウィルスが駆除されたりする場合に対応できる．ライトグレイからホワイトへ，ダークグレイからブ

ラックへの遷移は，それぞれ，SPAM メール送信者であるか否かを本システム上で判断した場合に遷移する．ライトグレイ，グレイ，ダークグレイの遷移は「一見さんお断り」方式を実現した部分となる．スーパーホワイトリストは状態遷移とは関係なく，システム起動時に指定した IP アドレスのリストである．この IP アドレスから SPAM メールが届いてもユーザが許容できる，または，SPAM メールが送信されてもやむを得ない IP アドレスを登録する．これはメーリングリストなどで SPAM メールが混じる場合に利用することなどを想定している．本システムの運用実験では，学内の全 IP アドレスを指定した．

3.3 コンテンツ分析型 SPAM フィルタ部

メールサーバでは，受信したメールをユーザ領域に置く前にコンテンツ分析型 SPAM フィルタ部 (以下，単に SPAM フィルタとする) にて SPAM メールかどうかを判定する．SPAM メールと判定されたメールは SPAM メール候補としてユーザ領域とは別の領域に置かれ，ユーザからは隠蔽する．その日に受信した SPAM メール候補の送信者，件名などを一覧表にして，ユーザに通知し，SPAM メール候補から救済しなければいけないメールをユーザに指定させる．指定された SPAM メール候補はユーザ領域に置かれ，SPAM メール候補から外される．ユーザは SPAM メール候補から外させたメールを受信し，本当に SPAM メールでない場合は，メールサーバにそのことを通知する．また，SPAM フィルタをすり抜けて，SPAM メールを受信してしまった場合も，そのメールが SPAM メールだったことをメールサーバに通知する．このようにして，SPAM フィルタにユーザモデルを学習させる．メールサーバの SPAM フィルタで判定された SPAM メール候補の内，適当な期間内にユーザから救済されなかったメールは本当の SPAM メールとして，SMTP 接続制御部のリストコントローラに通知する (SPAM メール苦情)．

SPAM フィルタは本システムの場合 bsfilter [3] を採用した．本システムでは，特にベイジアンフィルタである必要はなく，以下の条件を満たすもので有れば，いずれでも良い．

- ユーザが考える SPAM メールをモデル化する学習機構を備えていて，ユーザ別に学習可能であること．
- SMTP サーバ上で動作すること．
- SPAM メールと判定したメールを収集し，リストコントローラに通知する機能が備えられること．

bsfilter でも上記の条件を全て満たしているわけではないが，メールサーバ qmail [14] といくつかのプログラムを組み合わせることにより，比較的簡単に実現することが出来る．

SPAM メールの苦情をユーザから直接受けない理由は，偽装された SPAM メールを受け取らないようにするためである．SPAM 苦情受け付けを考えるとき，多くの場合は SPAM メールそのものを転送して欲しいとユーザに要求することになる．しかし，悪意のあるユーザが紛れている場合，メールヘッダにある received 行などを改竄することにより，本来受け取らなければならないメールまで，影響を及ぼすことになる．そこで，このような間接的な SPAM メール苦情処理システムを構築した．

4. 実　　験

3. 節で説明したシステムを実装し，3 週間程度の運用実験を行った．まず，実装について説明し，その後で，実験結果について説明する．

4.1 実　　装

本システムの SMTP 接続制御部およびリストコントローラを 1 台の計算機に実装した．計算機の仕様は表 3 の通りである．

SMTP 接続制御部は実際には linux kernel の iptables の機能を利用し，リストコントローラと SMTP ハニーポットのみプログラムで記述した．プログラミング言語は ruby v1.8 を利用した．それぞれのプログラムのサイズはリストコントローラが 374 行，SMTP ハニーポットが 62 行である．

iptables は管理者権限がないと操作することが出来ないが，本システムのために作られたプログラムに管理者権限をそのまま与えてしまうと，万が一，外部の第三者に制御を取られた場合の対応が出来なくなる．そこで，それぞれのプログラムは独立したユーザで実行することとし，リストコントローラを実行するユーザのみ sudo にて iptables の操作を許可した．危険度の評価から考えると，リストコントローラに比べて SMTP ハニーポットは外部の第三者から任意の文字列を送り込まれるため，危険性が高いと考えられる．しかし，本システムの実装では，外部の第三者が得られる権限は SMTP ハニーポットまでとなり，iptables の操作は出来ない．

この計算機は本学のネットワークの都合により，本学のバリアセグメント上に設置した．そのため，この計算機と SPAM メールから防御したいメールサーバの間にネットワークやサーバが介在している．このことが，後に述べる実験結果に影響を及ぼしている．

メールサーバおよび SPAM フィルタ部の計算機の仕様は表 4 の通りである．普段から研究室で利用しているメールサーバに SPAM フィルタとして bsfilter を組み込んだ．qmail の拡張メールアドレス機能を利用し，bsfilter の学習と SPAM 候補メールの救済をメールの送受信によるユーザインターフェースとして実装した．bsfilter を学習させるには再計算が必要なため，それは 1 日 1 回だけ実行させる．一定期間の間に救済されなかった SPAM メール候補はリストコントローラに通知されるが，この部分についてはセキュリティ上の都合により，現在公開することが出来ない．

表 3　SMTP 接続制御などを実装した計算機の仕様

CPU	AMD Duron 900MHz
メモリ	384MByte (SD-RAM PC-100)
NIC	100Base-TX 2 ポート
OS	Debian GNU/Linux Sarge, Linux kernel 2.6.0

4.2 実験結果

本システムの運用実験を 3 週間ほど行った．その結果を概観するため，図 3 を示す．このグラフの見方であるが，運用実験の開始日から起算して，横軸方向に 1 日目，2 日目と数え上げる．縦軸方向は SPAM メール候補数または各リストに登録さ

表 4　メールサーバの仕様

CPU	Intel Pentium III 1000MHz
メモリ	128MByte (SD-RAM PC-133)
NIC	100Base-TX
OS	Debian GNU/Linux Woody, Linux kernel 2.4.18
MTA	qmail Ver. 1.03
SPAM filter	bsfilter Ver. 1.37

れた IP アドレスの数である．本システムではフェイルセーフのため，SMTP 接続制御部，リストコントローラが停止するとそれまでに記憶した IP アドレスは全て消去され，全てのメールの通過が許可される仕組みとなっている．また，SMTP 接続制御部が停止している間は syslog への記録も停止する．運用実験は開始日より SPAM フィルタによって，SPAM メールと判定された SPAM メール候補の数を数え始め，13 日目より，SMTP 接続制御部，リストコントローラを起動させた．8 日目より 12 日目まではリストコントローラの調整を行っていたため，SPAM 候補メールの数が変動している．また，18 日目，21 日目，22 日目にリストコントローラが停止している．

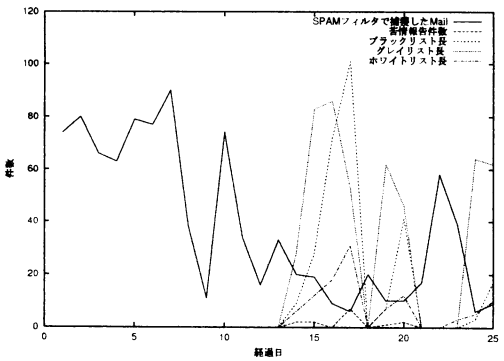

図 3　SPAM フィルタで判定した SPAM 候補メール数とホワイト，グレイ，ブラックの各リスト長

このグラフでまず言えることは，SPAM メール候補が激減することである．これは文献 [15] と同様で，「一見さんお断り」方式により相当数の SPAM メールを拒否出来ていることになる．図 4 はダークグレイリストに登録されている IP アドレスの数の変化を示したグラフである．ダークグレイリストは過去 2 週間の間にメール送信を試みようとした送信元であることを示しているが，その数が 500 から 3000 程度であるのに対して，グレイリストでは 100 以下である．単純に言えるわけではないが，IP アドレスの接続拒否でも SPAM メール送信を妨げるのに十分な効果があると考えられる．

SPAM メール候補が数件ながら残るのは，学内の別のメールサーバを経由して，実験対象のメールサーバに転送される SPAM メールがあるためである．これらの SPAM メールを除けば，SPAM メール候補はほぼ 0 となる．

ホワイトリストとブラックリストは，リストコントローラの実行時間が長ければ順調に IP アドレスの登録数が増えること

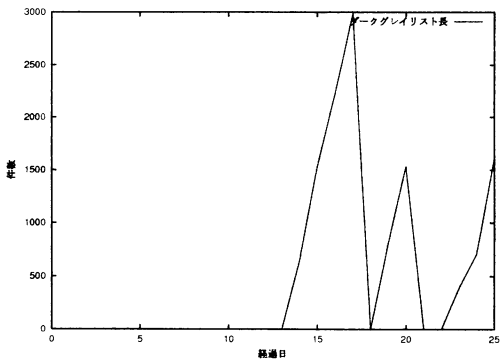

図 4　ダークグレイリスト長

を確認した．それぞれのリストの内容を確認すると，ホワイトリストの中に若干 SPAM メール送信者ではないかと疑われる送信元もあったが，SPAM メール苦情として受け付ければすぐにダークグレイリストに移されるので，ほぼ期待通りの動作している．ブラックリストの方は，ユーザが自ら登録したメーリングリスト (広告メール) のメールサーバと思われる IP アドレスが登録されていた．これは，広告メールを送信するためのプログラムの動作が SPAM メール送信者が使うプログラムの動作と同じためである．このようなメールサーバは RFC に反しているので，利用すべきではないが，やむを得ず受信しなければならない場合は，スーパーホワイトリストに当該 IP アドレスを登録することで対応することになる．

図 5 は SMTP 接続制御部に置いて，通過したメールの数と遮断したメール送信試みの数の変化を表したグラフである．通過許可の数が 100 から 700 くらいの範囲で変化しているのに対して，遮断数は 600 から 2200 くらいの範囲で変化している．各送信元はしばらくの間，ダークグレイ，グレイ，ライトグレイの状態を遷移するため，遮断数が通過許可数の概ね 2 倍以上となる．このグラフでは，その倍率が 3.46 倍から 4.92 倍である．これについても単純に言えるわけではないが，2 倍を超える部分は SPAM メールであった可能性が高い．

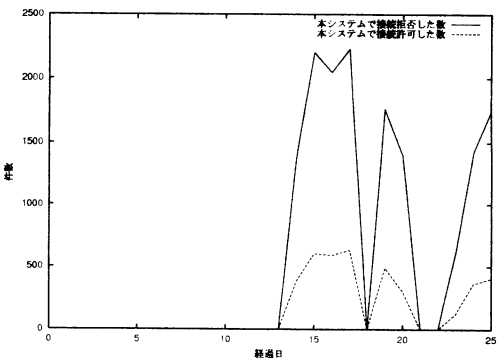

図 5　通過許可数と遮断数

最終的には SPAM メール送信者が当該システム宛の SPAM

メール送信を諦めて，配達リストから削除してもらえれば，遮断数が減少し，通過許可数に対する遮断数の倍率も減少することが期待される．

5. むすび

本システムの運用実績がまだ短く，十分な調査が行えたとは言えない状況にある．また，システムの安定性の観点からも，まだ考慮点が残されている．しかしながら，当初目標とした管理コスト上昇を出来る限り防ぐと言う目的は相当程度実現されていると考える．本システムの運用時に管理者は本システムが正常に稼働しているかどうかを 1 日 1 回程度確認すればよい．万が一停止していたとしても，ほとんどの場合，SMTP 接続制御における遮断は自動的に解除されるようにプログラムが作られているので，メール不達の事態は概ね避けられる．

再起動は記録した IP アドレスのリストを失わせてしまうが，また，記録しなおすので，2, 3 日程度で元の状態に復旧できる．ただし，この復旧期間中，ホワイトリストに登録されていたメール送信元からのメールの到着順序が変わる可能性があるので，ユーザへの周知は必要だろう．

ホワイトリストに登録されていないメール送信元からのメールがユーザに届くまでの時間は，ホワイトリストに登録されているメール送信元に比べると明らかに遅くなる．メール送信元の設定によって一概には言えないが，だいたい 30 分程度の遅延が発生するようだ．しかし，メールアプリケーションは，数秒，数分のリアルタイム性が確保できるサービスではないため，この程度の遅れは許容できるのではないかと考えている．

また，メールサーバまで到達するウィルスも減少したのではないかと考えている．今回の運用実験では，受け取ったウィルス付きメールの数が十分ではないため評価することは出来ないが，ゲートウェイ型アンチウィルスシステムなどを導入しているところでは，このシステムの負荷が軽減されることが期待できる．

今後の課題としては，安定運用の他に，SMTP ハニーポットによって取得した情報をどのように生かすかということがある．本システムでは現在のところ，SMTP ハニーポットと滞り無く交信できれば，送信元はライトグレイリストへ移動される．この移動の制限を厳しくすることで，さらに SPAM メールの抑制ができる可能性がある．

文　献

[1] Paul Grapham: “A Plan for Spam,” http://www.paulgraham.com/spam.html (日本語訳: http://www.shiro.dreamhost.com/scheme /trans/spam-j.html)

[2] Paul Graham: “Better Bayesian Filtering,” http://www.paulgraham.com/better.html (日本語訳: http://www.shiro.dreamhost.com/scheme /trans/better-j.html)

[3] Kenichi Nabeya: “ベイジアン スパム フィルタ”, http://bsfilter.org/

[4] 斎藤, 他: “SPAM メール対策システムの提案と実装”, 電子情報通信学会論文誌 D-I, Vol. J86-D-I, No.7, pp.480-489 (2003).

[5] 前野: “『お馴染さん』方式”, http://spam.qmail.jp/onazimi/

[6] 前野: “非通知拒否方式”, http://spam.qmail.jp/ptr.html

[7] Computerized Horizons: “List of All Known DNS-based Spam Databases,” http://www.declude.com/junkmail /support/ip4r.htm

[8] 総務省: “特定電子メールの送信の適正化等に関する法律”.

[9] ITPro: 広告メールの大量送信を課金—波紋呼ぶ韓国の「オンライン切手」, http://itpro.nikkeibp.co.jp/free/NNB/NEWS /20020509/7/

[10] 下川: “経路情報に基づくスパムメール遮断方式の提案と評価”, 情報処理学会第 66 回全国大会, Vol.3, pp.471-472 (2004).

[11] Meng W. Wong, Mark Lentczner: “Sender Policy Framework (SPF),” http://spf.pobox.com/

[12] Microsoft: “Caller ID for E-mail Technical Specification,” http://www.microsoft.com/mscorp/twc /privacy/spam_callerid.mspx

[13] Sendmail: “Sendmail and Yahoo! Mail Collaborate to Develop and Deploy DomainKyes,” https://www.sendmail.com/smi/news/pressrelease.jsp ?eventOID=80351&localId=USA

[14] D. J. Bernstein: “qmail,” http://cr.yp.to/qmail.html

[15] 鈴木: “東海インターネット協議会における spam 対策”, http://www.tokai-ic.or.jp/spam/