情報処理学会論文誌　Vol. 50　No. 9　2023–2033 (Sep. 2009)

個別アドレス発行によるメーリングリストへのスパムメール削減方式の提案と評価

高橋 健一[†1]　境 顕宏[†2]
堀 良彰[†1,†2]　櫻井 幸一[†1,†2]

特定のグループ内での情報交換を図るためにメーリングリストが利用されている．しかし，一方で多量のスパムメールの発生により，スパムメールと正当な電子メールの区別の作業に労力を割く必要が出てきている．スパムメールを防ぐための代表的な方法として，スパムメールフィルタリングや White/Black list の利用がある．しかし，false positive や false negative といった誤検知の問題や設定の困難さなどの問題がある．そこで，メーリングリストのそれぞれのメンバごとに個別アドレスを発行する方法を提案する．本提案においてメーリングリストへの投稿はそれぞれに発行された個別アドレスにメールを送信することで行う．各メンバが異なる個別アドレスを利用するため，スパムメール増加の原因となったメンバを特定することができる．また，その原因となったメンバの個別アドレスを無効化し，異なる個別アドレスを発行することで，メーリングリストでのスパムメール増加を防ぐことができる．このため，メーリングリストの他のメンバに影響を与えることなく，スパムメールの増加を止めることができる．また，本提案では，メンバに特別なソフトウェアのインストールを要求せず，既存のメールクライアントで利用可能な仕組みを実現する．

Personal Mailing List Address to Block Spam Mail and Its Evaluation

Kenichi Takahashi,[†1] Akihiro Sakai,[†2]
Yoshiaki Hori[†1,†2] and Kouichi Sakurai[†1,†2]

Mailing lists are used for information exchange in specific groups. However, in the recent times, the number of spam mails received has increased, and considerable amount of time is wasted in filtering spam mails. Spam filtering techniques are widely used tool, however, they produce false positive and false negative results. We propose a system to block spam mails in a mailing list. In our system, we assign different posting addresses to different mailing list members. A mailing list member sends a mail to the mail address assigned to him for sending a mail to the mailing list. When a spam mail is received, the address that is the cause of the spam mail is identified and invalidated, and a new address is assigned to the member. Thus, we can block spam mails from the invalidated address. Furthermore, our system is highly compatible with current mail systems because our system does not require any particular software to be installed in the client machines.

1. はじめに

インターネットの普及により，電子メールは我々の生活や仕事にとってなくてはならないものになってきている．また，特定のグループ内での情報交換を図るためにメーリングリストがよく利用されている．しかし，一方で多量のスパムメールの発生により，必要な電子メールがスパムメールの中に埋もれたり，スパムメールと正当な電子メールの区別の作業に労力を割いたりする必要が出てきている．Symantec の報告[1] によれば電子メール全体の75%以上がスパムメールといわれている．また，ウイルスやワームを添付したスパムメールやフィッシングサイトへのリンクを持つスパムメールなども多く出回っており，機密情報を漏洩させる事件やマシンに損害を与える事件が発生している．

スパムメールを防ぐための代表的な方法として，スパムメールフィルタリング[2] の利用がある．スパムメールフィルタリングでは，スパムメールでよく使われる単語や単語の組を登録し，それらを一定の割合以上で含む電子メールをスパムメールと判断する．スパムメールの特徴を学習し，スパムメールの判断に役立てるものも多い．しかし，スパムメールフィルタリングには，false positive や false negative といった誤検知の問題がある．たとえば，Medicine や Viagra といった単語を含む電子メールにはスパムメールが多いが，製薬会社ではそれらの単語を定常的に利用するかもしれない．このような電子メールがスパムメールと判断されると業務に支障をきたす．また，AT&T がスパムメールと判断されないようにするための特許を取得[3] するなど，スパムメールの防止はいたちごっこのような状況である．

White/black list で正当な/スパムメールの送信者やドメインを制限する方法もあるが，メールマガジンなど，送信者が限定される特殊なメーリングリストを除いて white/black

†1 財団法人九州先端科学研究所
Institute of Systems, Information Technologies and Nanotechnologies
†2 九州大学大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University

list を適切に設定することは難しい．電子メールの送信元ドメインを認証する方法[4),5)] も提案されているが，送信元メールサーバの協力が必要であるという問題がある．

本論文ではメーリングリストを対象とし，メーリングリスト内のスパムメールを排除する方法を提案する．メーリングリストは研究室や研究開発プロジェクトなどの特定の制限されたメンバ間での情報交換を図るために利用される．メーリングリストではメーリングリストのアドレスがそのメンバに知らされ，メンバがメーリングリストアドレスに向けて電子メールを送信すると，同じ内容の電子メールがメーリングリストのメンバに配信される．このため，メーリングリストのメンバ増加にともなって，ユーザの不注意やその他の原因によってメーリングリストアドレスが漏洩する危険性が増加する．しかし，一方でメーリングリストアドレスはメーリングリストへの投稿のためだけに利用されるため，そのアドレスが漏洩する機会は少ない．たとえば，オンラインサービス利用のためのユーザ登録にメーリングリストのアドレスを利用する必要はない．すなわち，メーリングリストアドレスはメーリングリストへの投稿のため以外の利用を考慮する必要がない．しかし，メーリングリストでも同様にスパムメールが発生している．あるメーリングリストでは 3 年前にほとんど発生していなかったスパムメールが現在では週 150 通程度届くようになっている．しかし，スパムメールの増加によりメーリングリストアドレスの変更が必要になっても，メンバが同じメーリングリストアドレスを利用しているため，容易にそのアドレスを変更することが難しい．

そこで，メーリングリストのそれぞれのメンバごとに個別アドレスを発行する方法を提案する．本提案においてメーリングリストへの投稿はそれぞれに発行された個別アドレスにメールを送信することで行う．各メンバが異なる個別アドレスを利用するため，スパムメール増加の原因となったメンバを特定することができる．また，その原因となったメンバの個別アドレスを無効化し，異なる個別アドレスを発行することで，メーリングリストでのスパムメール増加を防ぐことができる．このため，メーリングリストの他のメンバに影響を与えることなく，スパムメールの増加を止めることができる．

以下，2 章で関連研究について述べ，3 章でスパムメール発生の原因を分析する．4 章で現在のメーリングリストと同様の利便性を実現するための要求事項を検討し提案手法について述べる．5 章で提案システムの評価を行い，6 章でまとめとする．

2. 関 連 研 究

正当なメールとスパムメールに現れる特徴の違いによって，スパムメールをフィルタリングし遮断することが行われている[2)]．これらのフィルタリングには確率統計的手法を用いた学習型のフィルタリング手法が利用されることが多い．また，メールが送信されてきた経路情報を利用してスパムメールを判断する研究[6),7)] もある．しかし，これらのフィルタリング手法には false positive や false negative の問題があり，スパムメールの判断に限界がある．

インターネットで公開されているブラックリスト（DNSBL: DNS Base Blackhole List）[8)] を利用することでスパムメールを排除する方法がある．しかし，これらのリストの精度は必ずしも高くなく，スパムメール送信元でないメールサーバが誤って登録されることもある．このため，正当なメールを排除してしまうといった危険性がある．

メーリングリストへの投稿者や投稿元ドメインを限定することで，スパムメールを排除することができる．メールマガジンなどの投稿者が制限される状況では有効な方法である．しかし，メンバからの投稿を許すメーリングリストでは，外出先などから一時的に gmail や yahoo メール，携帯電話，また，自宅に立ち上げた SMTP サーバなどを利用してメーリングリストに投稿することができなくなり，ユーザの利便性を損ねる．

メーリングリストを対象としたスパムメール対策の方法として文献 9)，10) が報告されているが，これらはメーリングリストにフィルタリング手法を応用することが目的であり，フィルタリング手法と同様の問題を持つ．

スパムメール対策に使い捨てのメールアドレス（DEA: Disposal E-mail Address）[11)] を利用する方法がある．Spamex（http://www.spamex.com/）や myTrashMail.com（http://mytrashmail.com/）などがサービスを提供している．また，Gmail ではアカウント名中の “+” から後方がメールアドレスとして認識されないという特徴を持ち，これを利用することで使い捨てアドレスのように利用することができる．しかし，使い捨てメールアドレスをそのままメーリングリストに適用することは難しい．

メールの送信元とされるドメイン名を検証することで成りすましやフィッシングの問題に対処するための方法として Sender ID Framework[4)] がある．しかし，Sender ID Framework ではインターネットサービスプロバイダの協力が必要で，その効果は限定的である．DKIM（Domain Key Identified Mail）[5)] では電子署名を利用することで送信元ドメインの認証を行う．しかし，電子署名を生成，検証するための特別なライブラリを送受信メールサーバの双方にインストールする必要がある．また，メーリングリストでの利用やメールの転送を不得手とするという欠点[12)] がある．TEOS（Trusted E-mail Open Standard）[13)] では認証情報やコンテンツの情報を電子メール内に埋め込むことでスパムメールを排除することを試みているが，同様に，それを実現するための特別なライブラリのインストールが必要になる．

スパムメールは同一の送信者から大量に送信されることが多い．このため，メール送信時

に Challenge & Reponse 型の負荷をかけることで大量のスパムメール送信を防止するための提案[14),15)] が行われている．また，文献 16)，17) ではメール送信者に一定量の課金を行うことで，スパムメール送信者に金銭的な負担を負わせることが提案されている．しかし，これらの仕組みをマルチキャストが必要なメーリングリストに適用することは難しい．また，正当なメールの送信者にもスパムメール送信者と同様に負荷がかかるといった問題や，メールを送受信する両者に特別なソフトウェアが必要になるといった問題がある．

privango [18)] ではメールの受信条件を暗号化しメールアドレスに埋め込むことで，自動的に受信条件に合わないメールを排除することを提案している．文献 19) ではメールサーバが自動的に alias アドレスを生成し，スパムメールが発生したときにその alias アドレスを削除することでスパムメールを排除することを提案している．しかし，複雑なメールアドレスとなり覚えられないといった問題や受信条件を埋め込むための操作が必要であるといった問題がある．

3. スパムメール発生の原因

本論文ではメーリングリストを対象としてスパムメールを排除するための方法を提案する．一般にメーリングリストは特定のグループ内のメンバの情報交換のためだけに利用され，それ以外のユーザがメーリングリストアドレスを知る必要がない．すなわち，グループ内のメンバ以外がメーリングリストアドレスを知ることがないため，スパムメール送信者もそのアドレス宛にスパムメールを送信しないはずである．しかし，多くのメーリングリストにおいてスパムメールが発生している．これは何らかの原因でメーリングリストアドレスがスパムメール送信者に漏洩しているためである．メーリングリストアドレス漏洩の原因としては以下の 5 点（**図 1**）が考えられる．

原因 1　メーリングリストアドレスを Web 上で公開していた．または，メーリングリストアドレスをユーザ登録などに利用した．

原因 2　メーリングリストのメンバ以外宛の電子メールにメーリングリストアドレスを誤って，または故意に併記した．そのメールの受信者がメーリングリストアドレスを（原因 3 や 4 などを含むほかの理由で）漏洩させた．

原因 3　メンバの誰かのマシンに電子メールアドレスを収集するためのスパイウェアがインストールされていた．または，Web メールなどを一時的に利用したときに，その Web メールサーバの脆弱性や管理者の悪意により，メーリングリストアドレスが漏洩した．

原因 4　送信者とメーリングリストサーバ間の通信が盗聴された．

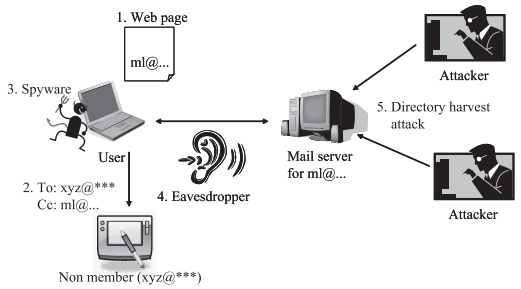

図 1　アドレス漏洩の原因
Fig. 1　Causes of address leakage.

原因 5　スパムメール送信者が適当に生成して送信した電子メールアドレスの中に偶々メーリングリストアドレスが含まれており，スパムメール送信の成功とともに有効なメールアドレスとして登録された（DHA: Directory Harvest Attack）．

原因 1〜4 はユーザの不注意でメーリングリストアドレスが漏洩したといえる．原因 5 に関してはユーザの不注意とは関係なく発生する．スパムメール送信者はこれらの原因によって漏洩したメールアドレスを収集し，スパムメールの送信に利用する．収集されたメールアドレスはスパムメール送信者間や業者間で転用・転売され，いったんメールアドレスが漏洩すると他のスパムメール送信者からもスパムメールが送られてくる可能性が高くなる．このため，スパムメールが増加する一方で，それを減少させることは難しい．そこで，これらの原因などで漏洩したメーリングリストアドレスを無効化することでスパムメールの増加を防ぐ方式を提案する．

4. 個別アドレス発行によるスパムメール削減方式

メーリングリストにおいてスパムメールを削減するために，メーリングリストのそれぞれのメンバごとに異なる個別アドレスを発行する方法を提案する．

4.1 要求事項

スパムメールを排除するための仕組みとして Sender ID Framework [4)] や TEOS（Trusted Email Open Standard）[13)] といった様々な仕組みが提案されている．しかし，送信元メールサーバの協力や特別なソフトウェアライブラリのインストールが必要であるなどの問題がある．このため，既存のメーリングシステムと同程度に簡易に利用可能で，特別なソフトウェアを必要としない仕組みが求められる．このことを実現するためには以下の要求事項を

満たす必要がある．

- ユーザに専用ソフトウェアのインストールを要求せず，既存のメールクライアントで利用可能であること．
- POP や SMTP などの既存プロトコルでメール送受信が可能であること．
- 既存のメーリングリストと同程度に簡易にユーザが利用可能であること．これを実現するには
  - 個別アドレスとして，ユーザが容易に覚えやすいアドレスが利用可能なこと．
  - 個別アドレスさえ知っていれば，どこからでも（事前登録していないメールサーバやメールアドレスから）送信可能であること．
  - メーリングリストに対して容易に返信可能であること．

  を実現する必要がある．

本提案ではスパムメール増加の原因となったメンバに割り当てた個別アドレスを無効化し，スパムメールを減少させることを目的としている．このため，スパムメール増加の原因となったメンバが特定されると，その特定されたメンバが不利益を被ることになることが考えられる．また，DHA による個別アドレス漏洩は他の原因と異なりメンバの不注意と関係なく発生する．このため，以下の要求事項を加える．

- スパムメールが投稿されたときに，誰の個別アドレスを使ってスパムメールが投稿されたかがメーリングリストのメンバに知られないこと．
- DHA による個別アドレス漏洩と他の原因を区別できること．

そこで，以上のような要求事項を満たしたスパムメールを排除するための仕組みを提案する．

4.2 提 案 手 法

既存のメーリングリストシステムでは，メーリングリストのメンバ間で同じ投稿用メールアドレスを利用するため，そのアドレスを変更することは難しい．そこで，メーリングリストのそれぞれのメンバごとに異なる投稿用メールアドレス（個別アドレス）を発行する方法を提案する．提案手法の概要を**図 2** に示す．

(1)　メーリングリストの管理者はメーリングリストのメンバを決定する．
(2)　それぞれのメンバごとに異なる個別アドレスを発行する．ここで，各メンバは発行された個別アドレスを（重複しない）任意のアドレスに変更することができる．
(3)　各メンバは各自に発行された個別アドレスにメールを送信することでメーリングリストに投稿する．

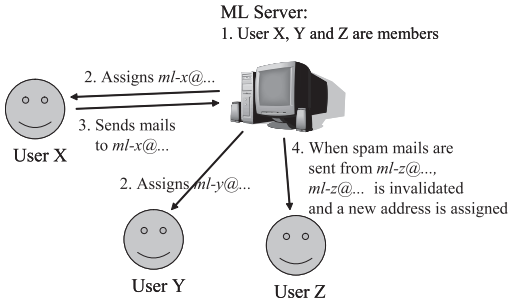

図 2　提案手法の概要
Fig. 2　Overview of our proposed system.

(4)　スパムメールが増加した場合，スパムメール発生の原因となっている個別アドレスを無効化し，そのメンバに対して新たな個別アドレスを発行する．

メンバごとに異なる個別アドレスを発行するため，あるメンバの個別アドレスを無効化したとしても他のメンバに影響を与えない．このため，スパムメール増加の原因となったメンバだけに負荷を課すことで，漏洩したアドレスを無効化することができる．以下，メーリングリストの作成，メーリングリストへの投稿，返信，スパムメール発生時の処理，DHA の特定，その他の機能の順で説明する．

4.2.1 メーリングリストの作成

メーリングリストの作成はその管理者によって行われる．管理者はメーリングリストアドレスやメンバの決定，各種設定を行う．ここで決定したアドレスはメーリングリストへの投稿に利用することはできない．投稿されてきても無効なメールとして無視する．各種設定には Reply-To に利用するアドレスやスパムメール発生時のペナルティ設定などが行われる．これらの設定が終わると，メーリングリストシステムは Address-ML Table，Address-Sender Table，Penalty Table，History DB を設定する．Address-ML Table は発行した個別アドレスが，どのメーリングリストに対するものであるかを管理する．Address-Sender Table はそれぞれの個別アドレスを誰に発行したのかを管理する．Penalty Table はスパムメール発生の原因となったメンバに与えたペナルティ値を管理する．History DB はこれまでに投稿されたメールを保存するためのデータベースである．

次にメーリングリストシステムはメーリングリストのメンバのそれぞれに対してランダムな個別アドレスを生成し，それを Address-ML Table，Address-Sender Table に記録す

From: ml@...
To: userX@***
Reply-To: xyz123@...
Subject: Invitation to the mailing list
メーリングリストのメンバとして登録しました．
xyz123@... にメールを送信することでメーリングリストへの投稿ができます．…

図 3　入会案内の例
Fig. 3　An example of an Invitation Mail.

る．ここで作成した個別アドレスを Reply-To とした入会案内をメンバに向けて送信する．**図 3** にメーリングリストアドレスが ml@...，メンバのアドレスが userX@***，発行された個別アドレスが xyz123@... のときの入会案内の例を示す．

入会案内を受け取ったメンバは自分の希望する個別アドレスを返信する．メーリングリストシステムは Address-ML Table，Address-Sender Table をメンバが希望した個別アドレスに書き換え，受理確認メールを送信する．同様にメーリングリスト作成時以外のメンバ追加も行うことができる．

4.2.2　メーリングリストへの投稿

メーリングリストへの投稿は個別アドレスに電子メールを送信することで行う．メーリングリストに配信されるメールの From，To，Reply-To はメーリングリストの設定によって変わるが，ここでは To をメーリングリストアドレス，From を送信者，Reply-To をメーリングリストへの返信（投稿）とするときの流れを**図 4** に示す．

メーリングリストシステムはまず投稿された電子メールとその Message-Id を組として History DB に保存する．次に Address-ML Table から，どのメーリングリストに向けて投稿されたものであるか特定し，To をそのメーリングリストアドレスに変更する．次に投稿されたメールに Reply-To が設定されていた場合には Reply-To のアドレスを From に利用する．設定されていない場合は From をそのまま利用する．そして，Address-ML Table を参照することで Reply-To を各メンバに発行した個別アドレスに変換する．最後に Address-Sender Table を参照しそのメールを各メンバに配信することでメーリングリストへの投稿が完了する．

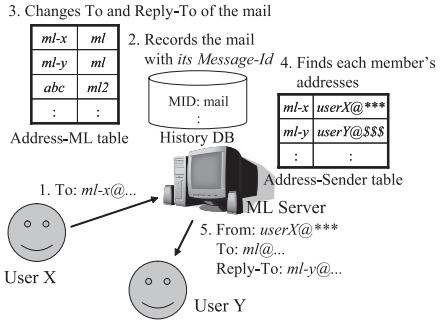

図 4　メーリングリストへの投稿の流れ
Fig. 4　Flow of sending a mail to mailing list.

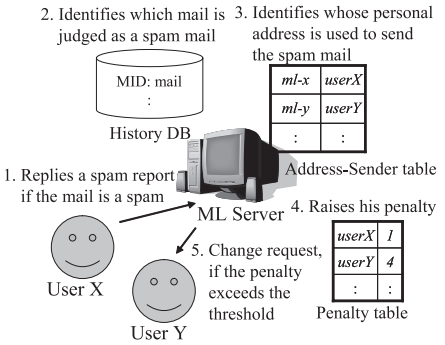

図 5　スパムメール発生時の流れ
Fig. 5　Flow when spam mail is received.

4.2.3　メールへの返信

メンバは既存のメーリングリストと同様に返信を行う．各メンバに発行された個別アドレスが Reply-To に設定されているため，そのまま返信することでメーリングリストへの返信が行える．メーリングリストシステムの動作はメーリングリストへの投稿と同様である．

4.2.4　スパムメールの判断

スパムメールはメーリングリストのメンバによって判断される．**図 5** にスパムメール発生時の流れを示す．

メーリングリストからのメールを受信したときに，メンバはそれがスパムメールかどうか

判断する．スパムメールだと判断すれば，そのメールに対してスパムメール報告を返信する．メーリングリストシステムはスパムメール報告を受け取ったときに，その報告の In-Reply-To から，History Table 中のどのメールがスパムメールとして判断されたか特定する．次に Address-Sender Table から，誰に発行した個別アドレスに向けてそのメールが投稿されたものであるか特定し，Penalty Table のそのメンバのペナルティ値を上げる．ただし，ここで悪意のある報告が発生する可能性があるので複数人の報告によりスパムメールが投稿されたと判断するなど工夫が必要である．

また，既存のスパムメールフィルタリングソフトをメーリングリストシステムに導入することでスパムメールと判断する方法も考えられる．スパムメールフィルタリングソフトによるスパムメール判断はメーリングリストへの投稿時に行われ，そのメールを配信することなく，そのメンバのペナルティ値を上げる．

一定値以上のペナルティ値になると，そのメンバに個別アドレスの変更要求を送信し，そのアドレスを無効化する．メンバは変更要求に対して希望する別のアドレスを返信することで，そのアドレスが個別アドレスとして利用できるようになる．

4.2.5　DHA の特定

DHA による個別アドレス漏洩は他の原因と異なりメンバの不注意と関係なく発生する．このため，DHA による個別アドレス漏洩は他の原因との区別が必要になる．

DHA によって個別アドレスが漏洩する場合，スパムメール送信者（またはメールアドレス収集者）は有効な個別アドレス以外にも複数のメールアドレス向けにスパムメールの送信を試みているはずである．すなわち，スパムメール送信者は無効な個別アドレスにもスパムメールの送信を試みているはずである．このため，無効な個別アドレス向けに送信されたメールを調査することで DHA の発生を特定することができる．具体的には有効な個別アドレスに似たダミーのアドレスを監視用アドレスとして登録する．たとえば，alice1@... が有効であるとすると，alice@... や alice2@... を監視用メールアドレスとして登録する．alice1@... に加えて，alice@... や alice2@... などにも，同様のスパムメールが送られてきている場合，それは DHA によって発生したものであると判断する．このとき，スパムメールの増加によって個別アドレスの変更が必要になっても，個別アドレス変更要求に DHA で漏洩した可能性が高いことを明示する．このことで，メンバは個別アドレスの漏洩の原因が自分にないことを知ることができる．

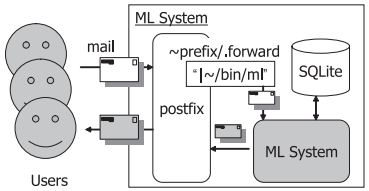

図 6　実装の概要
Fig. 6　Overview of the implementation.

4.2.6　その他の機能

投稿履歴の取り寄せ　投稿履歴要求をメーリングリストシステムに送信することで，それまでに投稿されたメールを取り寄せることができる．

メーリングリストからの退会　メーリングリストからの退会は退会要求を送信することで行う．システムは Address-ML Table，Address-Sender Table，Penalty Table から，そのメンバの情報を削除し，退会が完了した旨を返信する．

個別アドレスの変更　個別アドレス変更要求をメーリングリストシステムに送信することで，個別アドレスを変更することができる．個別アドレス変更要求を送信した後の流れは，入会案内を受け取ったときと同様である．

これらの機能はオプションであり，メーリングリストの管理者の設定によって利用が制限される．

4.3　実　　装

本システムを perl5.8.8 で実装した．Address-ML Table などの管理には SQLite を利用した．また，本システムでは実際のメール配送は行わず，既存の SMTP サーバ（postfix）を利用することとした．実装システムの概要を**図 6** に示す．

個別アドレスには *prefix*“-”*suffix* という形式を利用した．prefix はメーリングリストアドレスとして固定し，suffix にメンバ固有の識別子を利用する．メーリングリストの作成時にはランダムな文字列を suffix として生成する．prefix-に届いたメールが *.forward* の設定により本メーリングリストシステムに標準入力として渡される．システムに渡されたメールには前節までに述べた処理が施され，メンバへ配信するメールを postfix に渡すことでメールの送信を行う．

また，`Subject` が特別なキーワード（**表 1**）であった場合，システムは個別アドレス変更要求やスパムメール報告などであることを判断する．逆にこれらのキーワードが用いられな

表 1　メンバコマンド一覧
Table 1　Command list.

Subject	説明
`spamreport`	引用元のメールがスパムメールであることを報告する
`changesuffix` *arg1*	個別アドレスの suffix を *arg1* に変更する
`summary` *args*	*args* で指定した番号の投稿履歴を取り出す
`bye`	メーリングリストから退会する

いメールに対してはメーリングリストへの投稿として扱う．

本システムは 7 月 18 日からあるメーリングリストで運用を始めた．11 月 18 日までの間に約 180 通のメールがメーリングリストに投稿されている．以前運用していたメーリングリストでは同時期に 1,500 通のスパムメールが発生しているが，本システムに移行してからはスパムメールは 2 通[⋆1]しか発生していない．ただしこれはアドレス変更の効果によるもので，本システム導入によるスパムメールの削減効果ではない．

5. システムの評価

5.1 シミュレーション実験

提案システムのスパムメール削減効果を確かめるためにシミュレーション実験を行った．本シミュレーション実験における設定を以下に示す．

- 1 年を 360 日，1 月を 30 日とする．
- 各メンバがアドレスを漏洩する確率は 1 日につき 1/360.
- 1 度のアドレス漏洩に対して，以後毎日平均 1 通のスパムメールが送られてくる．
- メーリングリストのメンバ数を M とする．
- 既存メーリングリストシステムは 1 年の終わりに 1 度のメーリングリストアドレス変更を行う．
- 提案システムではスパムメール受信時に各メンバが P の確率でスパムメール報告を送信し，N 通のスパムメール報告により個別アドレスを変更する．

既存メーリングリストシステムにおけるメンバ数の違いによるスパムメール件数を**図 7** 左に，P=5%，N=3 としたときの提案システムにおけるメンバ数の違いによるスパムメール件数を図 7 右に示す．

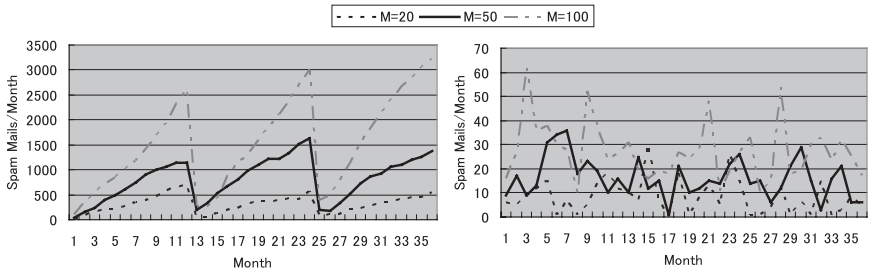

図 7　メンバ数の違いによるスパムメール件数の変化
Fig. 7　A number of spam mails on a number of mailing list member.

表 2　アドレス変更回数/年（3 年平均）
Table 2　A number of address change in a year.

	M=20	M=50	M=100
既存システム	20	50	100
提案システム	18	52.4	98.6

既存メーリングリストシステムでは 1 年を通じてスパムメール数は増加していき，1 年の終わりのメーリングリストアドレス変更によって一時的にスパムメール数は 0 になる．M=20 の場合では平均で 10.5 通/日，M=50 の場合では 27 通/日のスパムメールが発生した．一方で提案システムではスパムメール発生にともなって適時個別アドレスの変更が行われているため，スパムメール数は 1 年を通じてそれほど増えない．M=50 の場合では平均で 0.54 通/日，M=100 の場合でも平均で 0.91 通/日程度しか発生しなかった[⋆2]．また，アドレスの変更は既存メーリングリストでは年 1 回 × M 人=M 人回発生する．提案システムでも各メンバが平均年 1 回の確率で個別アドレスを漏洩させるため約 M 人回[⋆3]発生することとなり，アドレス変更回数はほぼ変わらない．実験結果（**表 2**）でもほぼ同様となっている．また，既存メーリングリストシステムでは漏洩者が特定されないため，スパムメールが

⋆1 2 通のスパムメール報告があったが個別アドレス変更までには至っていない．また，実験用に個別アドレスをホームページ上で公開したことにより発生したことも分かっている．

⋆2 4.2.4 項で述べたようにスパムメールフィルタリングソフトを導入することで提案システム，既存メーリングリストシステムともにスパムメール件数を減らすことができる．このとき，両者ともにほぼ同じ割合でスパムメール件数が減ることになる．

⋆3 個別アドレス漏洩から変更までの間に，複数回個別アドレスが漏洩しても 1 度の変更で済むため理論的には M より若干少ない．

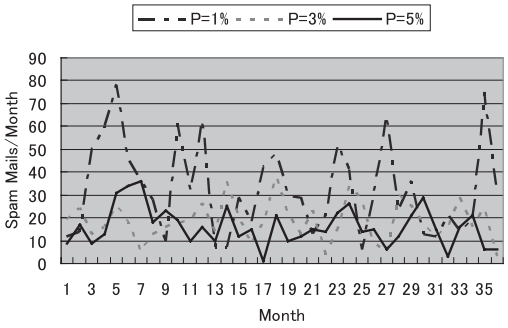

図 8　スパムメール報告確率の違いによるスパムメール件数の変化
Fig. 8　A number of spam mails on a probability of spam report.

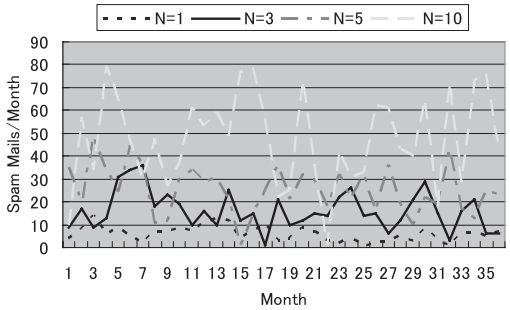

図 9　個別アドレス変更までに必要なスパムメール報告数の違いによるスパムメール件数の変化
Fig. 9　A number of spam mails when N spam reports cause a personal mailing list address change.

発生しても自分が原因とは考えない可能性が高い．一方，提案システムではアドレス変更要求が送信されてくるため，以後注意を払うこととなる．このため，提案システムでは各メンバの注意によりアドレス漏洩の確率が減少し，よりスパムメールの削減効果が見込めるようになるのではないかと推測する．

次にスパムメール受信時の各メンバのスパムメール報告送信確率の違いによるスパムメール数の変化を実験した．M=50，N=3 としたときの実験結果を**図 8** に示す．

スパムメール報告送信の確率が高ければ高いほど，スパムメール発生件数に対して個別アドレスの変更が早く行われ，スパムメール削減効果が高くなる．実験結果では P=1%，すなわち 100 人に 1 人しかスパムメール報告を送信しなかったとしても，平均で 1.1 通/日しかスパムメールが発生しておらず，既存メーリングリストシステムに比べて高いスパムメール削減効果が見込めることが分かった．

また，個別アドレス変更が必要になるスパムメール報告数の違いによるスパムメール数の変化を実験した．M=50，P=5%のときの実験結果を**図 9** に示す．

個別アドレス変更が必要になるまでのスパムメール報告数が低ければ低いほど，少しのスパムメール発生で個別アドレス変更が行われる．しかし，N=1 の場合ではたった 1 度の誤送信で，それがスパムメールと判断され，個別アドレスの変更が必要になる可能性がある．このようなことを防ぐためには N をある程度大きなものとする必要がある．実験結果では N=1 の場合に平均で 0.2 通/日，N=10 の場合でも平均で 1.6 通/日のスパムメールしか発生しておらず，既存メーリングリストシステムに比べて十分に高いスパムメール削減効果が見込めることが分かった．

5.2　性 能 評 価

負荷が集中するメーリングリスト作成時，および，頻繁に発生するメール配信処理の性能を評価した．提案システムではメールの送受信に既存のメールサーバを利用することとしている．このため，メールの送受信を除いた性能を評価した．

実験は CestOS 5.2，Intel Pentium D 2.8 GHz，1 GB メモリの計算機上で行った．メーリングリスト作成時には suffix として 8 文字のランダムな文字列を利用することとした．実験の結果，20 人のメンバが参加するメーリングリストを作成した場合で 0.17 秒，50 人で 0.39 秒，100 人で 0.79 秒で処理できた．すなわち，メーリングリスト作成時，1 秒間に 100 人以上のメンバを処理可能であった．個別アドレスの変更は 46.1 回/秒を処理可能であった．また，1 k バイトの本文を持つメールのメーリングリストへの投稿に対して，20 人が参加するメーリングリストでは 44.1 通/秒，50 人では 40.0 通/秒，100 人では 35.2 通/秒のメールを処理可能であった．これはメーリングリストにとって十分な処理能力であると考える．

5.3　個別アドレス漏洩原因別の効果

個別アドレス漏洩の原因を**図 10** に分析する．

原因 1〜4 はメンバのマシンやネットワーク環境の脆弱性，または不注意により発生する．原因 5 に関してはメンバの不注意とは関係なく発生する．

原因 1，2 は基本的にメンバの不注意によって発行された個別アドレスをメーリングリストのメンバ以外に知らせているため発生する．原因 1 についてはメーリングリストシステム以外の場所で発生しているため，メーリングリストシステムで原因を特定することは困難である．原因 2 については，多くの場合，個別ドレスが漏洩した可能性を To や Cc を見る

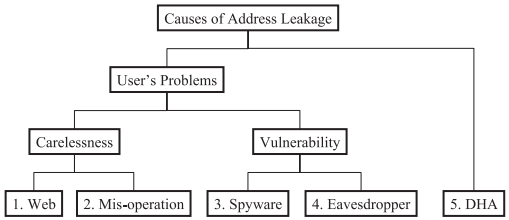

図 10　個別アドレス漏洩の原因分析
Fig. 10　Analysis of causes of personal mailing list address leakage.

ことで知ることができる．ただし，Bcc に個別アドレス以外のアドレスが記載されていた場合は，メーリングリストシステムでそれを知ることができない．一方でメンバは自分の管理する Web ページを確認することやメール送信ログを確認することによって，自分で個別アドレスが漏洩した原因を突き止めることができる．このため，これらの原因によって発生したスパムメールは，漏洩した個別アドレスを無効化・再発行し，そのメンバに注意を促すことで基本的に解決できる．

原因 3，4 はメンバのマシンやネットワーク環境の脆弱性によって発生する．原因 3 はスパイウェアやウイルスがメンバのマシンにインストールされていることで発生する．このため，スパイウェアが定期的にメールアドレスを収集する場合には，個別アドレスを無効化・再発行しても解決できない．また，スパイウェアが無効化・再発行に関するメールを自動的に削除・変更しているような場合にはメーリングリストシステムからの通知のすべてが無効化される危険性がある．このため，個別アドレスを頻繁に変更してもスパムメールが減らない状況が続いたときには口頭で注意を促すなどといったことが必要となる．このとき，そのメンバに異なるマシンから投稿履歴を取り寄せてもらい，削除・改竄されているメールがないか確認してもらうことが有効である．削除・改竄されたメールが確認できた場合，そのメンバのマシンにスパイウェアがインストールされている可能性があり，そのための対策を実施することができる．原因 4 もそのユーザのメールが絶えず盗聴されている環境を考えると，個別アドレスの無効化・再発行では解決できない．このため，原因 3 と同様の対処が必要となる．原因 4 はメールを暗号化することでも解決できるが，そのためのソフトウェアが必要になり，一時的に Web メールや他のマシンを使ってメーリングリストに投稿することが難しくなる．これらの原因で発生する問題に関してはメーリングリストに問題を及ぼすだけでなく，機密情報の漏洩や踏み台マシンとしての利用，データの削除などの問題が併発している可能性が高い．このため，繰り返し個別アドレスの漏洩が発生するとき，そのメンバに対して脆弱性が存在する可能性を知らせることができるといった利点がある．

原因 5 はメンバのマシン環境や（スパムメール送信者に推測が容易な個別アドレスを設定したこと以外の）不注意とは関係なく発生する．原因 5 と他の原因の区別は 4.2.5 項の方法によって行える．これは特定のメンバに限定して何度も繰り返し発生するものではなく，1 度の個別アドレスの無効化・再発行だけで解決できる．また，本提案システムでは個別アドレスとして *prefix*“-”*suffix* という形式を利用している．既存のメーリングリストシステムは *prefix* だけをメーリングリストアドレスとして利用しているものと見ることができる．すなわち，本提案システムの個別アドレスは既存のメーリングリストのアドレスよりも DHA への耐性を持っているといえる．

5.4 利 便 性

本システムでは既存のメールシステムの枠組みでメーリングリストのスパムメールを削減する．本システムでは暗号化や認証といった特別な手続きを実現するためのソフトウェアを必要とせず，既存のメールクライアントで利用可能である．また，アクセスコントロールによって送信元を制限する方式ではないため，一時的に gmail や yahoo メール，携帯電話を利用してメーリングリストに投稿・返信することが可能である．しかし，本システムでは任意の個別アドレスをメンバが要求するといった処理が追加されている．これは個別アドレスを漏洩させていないメンバにとってメーリングリスト登録時だけの処理であり，それほど負担になるものではないと思われる．個別アドレスを漏洩させたメンバは，スパムメール発生時に個別アドレスの変更が必要になるが，スパムメール発生の原因となったメンバに少々の負担を課すことは仕方ないものだと考える．すなわち，スパムメール発生の原因となったメンバの負担だけでスパムメールを防止することができる．このように本システムは，メンバにほとんど負担を与えることなく，既存のメーリングリストと同程度に簡易に利用可能であるといえる．

6. おわりに

本論文ではメーリングリストのメンバごとに異なる個別アドレスを発行し，スパムメール発生の原因となった個別アドレスを無効化・再発行することでスパムメールを削減するための仕組みを提案した．本提案ではユーザごとに異なる個別アドレスを利用するため，メーリングリストの他のメンバに影響を与えることなく，漏洩した個別アドレスを無効化しスパムメールを防止することができる．本提案システムでは，メンバに特別なソフトウェアのイン

ストールを要求せず，既存のメールクライアントで利用可能な仕組みを実現している．また，既存のメーリングリストと同様の操作でメーリングリストへの投稿や返信を可能とする．本提案システムをシミュレーション実験により評価した結果，既存のメーリングリストシステムに比べて高いスパムメール削減効果が期待できることが分かった．今後の課題として，メーリングリストサーバとの通信なしに個別アドレスを変更することや forward/backward セキュリティへの対応，Social Network Service へ応用することなどがあげられる．

謝辞　本研究は科学技術振興機構の戦略的国際科学技術協力推進事業と電気通信普及財団の研究調査助成の支援を受けて行った．

参 考 文 献

1) Symantec: The State of Spam Report. http://www.symantec.com/business/theme.jsp?themeid=state_of_spam (accessed 2008-11-20).
2) 田端利宏：SPAM メールフィルタリング：ベイジアンフィルタの解説，情報の科学と技術，Vol.56, No.10, pp.464–468 (2006).
3) Pfleeger and S.L., Bloom, G.: Canning Spam: Proposed Solutions to Unwanted Email, *IEEE Security & Privacy*, Vol.3, No.2, pp.40–47 (2005).
4) Microsoft: The Sender ID Framework (SIDF). http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx (accessed 2008-11-20).
5) DKIM.org: Domain Key Identified Mail (DKIM). http://www.dkim.org/ (accessed 2008-11-20).
6) 藤井優尚：経路情報に基づくスパムメールの判別方法，早稲田大学修士論文 (2004).
7) Samano, J.Z., Matsuura, K.: Using time to classify spam, 情報処理学会研究報告，CSEC-39, Vol.2007, No.126, pp.19–24 (2007).
8) DNSBL.info: DNSbl Information. http://www.dnsbl.info/ (accessed 2008-11-20).
9) 菊池時夫：メーリングリストにおける SPAM/WORM 防止法，情報処理学会研究報告，DSM-38, Vol.2005, No.83, pp.41–46 (2005).
10) 増井健司：メーリングリスト宛メールへの個人別スパム処理ポリシを適用可能とする配送システムの構築，情報処理学会研究報告，DSM-40, Vol.2006, No.38, pp.139–144 (2006).
11) Seigneur, J. and Jensen, C.D.: Privacy Recovery with Disposable Email Addresses, *IEEE Security & Privacy*, Vol.1, No.6, pp.35–39 (2003).
12) Lawton, G.: E-Mail Authentication Is Here, but Has It Arrived Yet?, *IEEE Computer*, Vol.38, No.11, pp.17–19 (2005).
13) Schiavone, V., Brussin, D., Koenig, J., Cobb, S. and Church, R.E.: Trusted Email Open Standard (TEOS). http://www.cobbsblog.com/spam/teos/TEOSwhitepaper1b.pdf (accessed 2008-11-20).
14) Dwork, C. and Naor, M.: Pricing via processing or combatting junk mail, *CRYPTO'92*, LNCS 740, pp.137–147 (1993).
15) Roman, R., Zhou, J. and Lopez, J.: Protection against Spam Using Pre-Challenges, *Proc. 2005 IFIP International Information Security Conference*, pp.281–293 (2005).
16) Kraut, R.E., Sunder, S., Telang, R. and Morris, J.: Pricing Electronic Mail to Solve the Problem of Spam, *Human-Computer Interaction*, Vol.20, No.1&2, pp.195–223 (2005).
17) Kuipers, B.J., Liu, A.X., Gautam, A. and Gouda, M.G.: Zmail: Zero-sum Free Market Control of Spam, *Proc. 25th IEEE International Conference on Distributed Computing Systems Workshop*, pp.20–26 (2005).
18) Takahashi, K., Abe, T. and Kawashima, M.: Stopping Junk Email by Using Conditional ID Technology: privango, *NTT Technical Review*, Vol.3, No.3, pp.52–56 (2005).
19) Kawashima, M., Abe, T., Minamoto, S. and Nakagawa, T.: Cryptographic Alias E-mail Addresses for Privacy Enforcement in Business Outsourcing, *Proc. 2005 workshop on Digital identity management*, pp.46–53 (2005).

(平成 20 年 11 月 29 日受付)
(平成 21 年 6 月 4 日採録)

高橋　健一（正会員）

1976 年生．1999 年九州大学工学部情報工学科卒業．2001 年九州大学大学院システム情報科学研究科修士課程修了．2004 年九州大学大学院システム情報科学府博士課程修了．博士（工学）．同年財団法人九州システム情報技術研究所（現，九州先端科学技術研究所）入所．情報セキュリティ，エージェントシステム，ユビキタス技術等の研究に従事．電子情報通信学会，電気学会各会員．

境　　顕宏（学生会員）

1983 年生．2006 年九州工業大学情報工学部知能情報工学科卒業．2008 年九州大学大学院情報工学研究科情報科学専攻博士前期課程修了．現在，九州大学大学院システム情報科学府情報工学専攻博士後期課程に在籍．ソフトウェア工学，形式検証，ネットワークセキュリティに興味を持つ．日本ソフトウェア科学会学生会員．

堀　　良彰（正会員）

1969 年生．1992 年九州工業大学情報工学部電子情報工学科卒業．1994 年九州工業大学大学院情報工学研究科情報システム専攻修士課程修了．1994 年九州芸術工科大学芸術工学部助手．2004 年九州大学大学院システム情報科学研究院准教授．博士（情報工学）．ネットワークセキュリティ，コンピュータシステムセキュリティ，ネットワークアーキテクチャの研究に従事．電子情報通信学会，ACM，IEEE コンピュータソサイエティ各会員．

櫻井　幸一（正会員）

1963 年生．1988 年九州大学大学院工学研究科応用物理学専攻修士課程修了．同年三菱電機（株）入社．現在，九州大学大学院システム情報科学研究院情報工学部門教授．1997 年 9 月より 1 年間コロンビア大学計算機科学科客員研究員．2004 年より九州システム情報技術研究所・第 2 研究室（現，九州先端科学技術研究所・情報セキュリティ研究室）室長併任．暗号理論，情報セキュリティ，社会情報工学の研究に従事．博士（工学）．2000 年情報処理学会坂井特別記念賞，2000 年・2004 年情報処理学会論文賞，2005 年 IPA 賞受賞．日本数学会，ACM，IEEE 各会員．