社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（35）
2008 / 7 / 25

メーリングリストへの投稿先アドレス無効化によるスパムメール防止

高橋健一† 境頴宏†† 櫻井幸一†,††

† （財）九州先端科学技術研究所 〒814-0001 福岡市早良区百道浜 2-1-22 SRP ビル 7F
†† 九州大学大学院システム情報科学研究院 〒819-0395 福岡市西区元岡 744

あらまし 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，本稿ではメーリングリストのメンバごとに異なる投稿先のメールアドレスを発行し，スパムメールが発生した投稿先メールアドレスを無効化・再発行することでスパムメールを排除することを提案する．本提案ではユーザごとに異なる投稿先メール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ずに漏洩した投稿先メールアドレスを無効化しスパムメールの発生を抑えることができる．また，本提案システムでは，ユーザ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．

キーワード メーリングリスト，スパム，メールアドレス無効化

Invalidation of a Mailing-list Address against Spam

Kenichi TAKAHASHI†, Akihiro SAKAI††, and Kouichi SAKURAI†,††

† Institute of Systems, Information Technologies and Nanotechnologies 2-1-22 Momochihama, Sawara-ku, Fukuoka, 814-0001, Japan
†† Faculty of Information Science and Electrical Engineering, Kyushu University 744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan

Abstract Mailing list is a popular tool for information exchange in a specific group. However, we are suffering with spam mail increasing and have to spend a lot of time to filter out spam mails from received mails. The representative ways against spam mails are to use a spam mail filtering tool, but they have matters, such as false positive/negative. We propose a mechanism to cut spam mails increasing. In our proposal, we assign different addresses to different mailing list members. When a mailing list user contributes to the mailing list, he sends a mail to the mail address assigned to him. When a spam mail causes, the system identifies whose address is the cause of the spam mail, and invalidates the address, assigns a new address to him. Then we can stop spam mails from the invalidated address. Furthermore, our system has high compatibility in current mail systems, because our system does not need to install any special softwares in client machines.

Key words Mailing list, spam mail, invalidation of mail address

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く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言われている．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．例えば，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の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 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まり普及していない．.

本稿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伴って，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．例えば，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．一方でスパムメールの増加などの理由でメーリングリストアドレスの変更が必要になった場合でも，メンバが同じメーリングリストアドレスに向けて投稿する必要があるため，容易にそのアドレスを変更することが難しい．また，メーリングリストアドレスを漏洩させたメンバを追跡することも難しい．

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先のメールアドレスを発行する方法を提案する．メンバごとに異なる投稿先メールアドレスを割り当てるため，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投稿先メールアドレスを無効化し，異なる投稿先メールアドレスを再発行することで，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．

以下，2. 章ではメーリングリストにおいてスパムメールが発生する原因を分析する．3. 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．4. 章で関連研究を述べ，5. 章でまとめとする．

2. メーリングリストにおけるスパムメール発生の原因

本稿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．

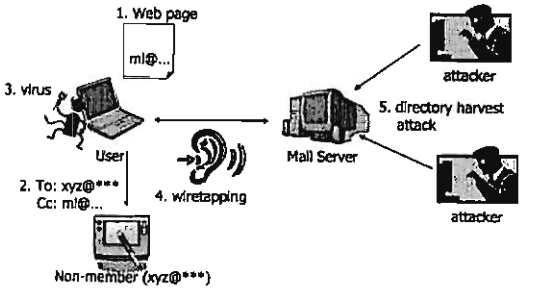

図 1　メーリングリストアドレスの漏洩

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．連絡先として Web ページに自分の電子メールアドレスを公開することはある．しかし，メーリングリストアドレスを Web ページなどで公開する必要性はない．

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．（メーリングリストとそれ以外のユーザに同時に同じ内容のメールを送りたい場合もあるが，イレギュラーな使い方としてここでは考えない．）

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．

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．

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共に有効なメールアドレスとして登録された．(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，一旦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．

3. メーリングリストにおけるスパムメールの排除

メーリングリストにおいてスパムメールを排除するために，メーリングリストのそれぞれのメンバごとに異なる投稿先のメールアドレスを発行する方法を提案する．

3.1 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) [6] 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
  - 投稿先メールアドレスとして，ユーザが容易に覚えやすいアドレスが利用可能なこと．
  - 投稿先メール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を使って）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，その特定されたユーザが不利益を被ることになることが考えられる．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，誰に発行したメール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．

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．

3.2 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先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先メール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．

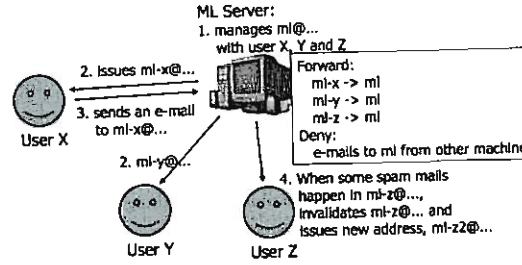

図 2 提案手法の概要

（2） 各メンバに投稿先メールアドレスを発行する．ここで，各メンバは発行された投稿先メールアドレスを（重複しない）任意のアドレスに変更することができる．

（3） 発行された投稿先メールアドレスに投稿することでメーリングリストに投稿する．

（4） スパムメールが増加した場合，スパムメールが増加した投稿先メールアドレスを無効化し，そのメンバに対して新たな投稿先メールアドレスを発行する．

メンバごとに異なる投稿先メールアドレスを発行するため，あるメンバの投稿先メール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，その他の処理の順で説明する．

3.2.1 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の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 は発行した投稿先メールアドレスが，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 はそれぞれの投稿先メール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投稿先メールアドレスを生成し，それを Address-ML Table，Address-Sender Table に記録する．ここで作成した投稿先アドレスを Reply-To とした入会案内（図 3）をメンバに向けて送信する．

入会案内を受け取ったメンバは自分の希望する投稿先メールアドレスをメール本文の先頭に記入し返信する．メーリングリストシステムはメンバが希望した投稿先メールアドレスで，

From: ml@...
To: userX@***
Reply-To: xyz123@...
Subject: Invitation to ml@... mailing list

You are registed as a member of our mailing list. You can use xyz123@... to contribute the mailing list, but do not use ml@.... If you hope to change the mail address for your contributions to the mailing list, please reply with an address you want to use.

図 3　入会案内の例：メーリングリストアドレスが ml@...，メンバのアドレスが userX@***，ランダムに生成された投稿先メールアドレスが xyz123@... のときの例．

Address-ML Table，Address-Sender Table を書き換え受理確認メールを送信する．

メーリングリスト作成時以外のメンバ追加も同様に行うことができる．

3.2.2　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投稿先メール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，本稿では 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．

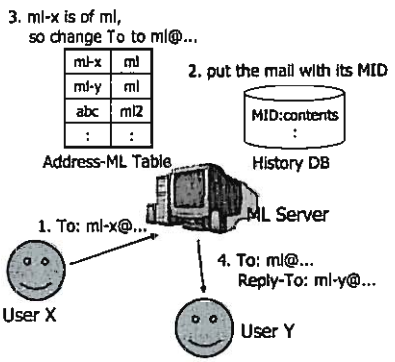

図 4　メーリングリストへの投稿の流れ

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投稿先メールアドレスに変換し，そのメールを Address-Sender Table を参照し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．

3.2.3　メールへの返信

ユーザ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投稿先メールアドレスが 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．

3.2.4　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．

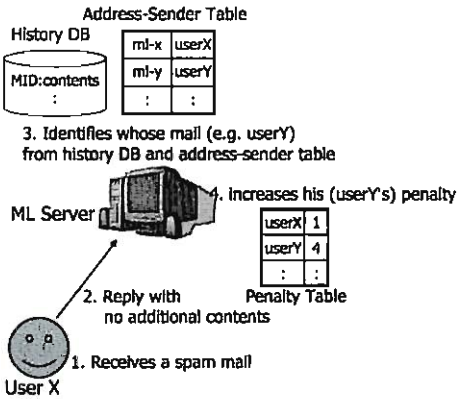

図 5　スパムメール発生時の流れ

メーリングリストからのメールを受信したときに，ユーザ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本文に文章を追加することなく返信する．メーリングリストシステムはスパムメールとの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，誰に発行した投稿先メール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．どれ位のペナルティを与えるかはそれぞれのメーリングリストの設定に依存する．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，そのユーザに投稿先メール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．変更要求にはスパムメール送信の原因となった（一つ，または複数の）事由の候補が記入される．スパムメール送信の原因となった事由の特定については次節で述べる．また，何度も無効化，再発行を繰り返すようなユーザに対してはメーリングリストから削除するなどの強制的な行為が必要になる．

3.2.5 その他

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空メール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，そのユーザの情報を削除し，退会が完了した旨を返信する．

投稿先メールアドレスの変更 投稿先メール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，投稿先メールアドレスを変更することができる．投稿先メール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．

3.3 メールアドレス漏洩の原因特定

メールアドレス漏洩の原因を図 6 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．メーリングリストシステム側でこれらの原因を必ずしも単一の原因に特定することが難しい．しかし，これらはユーザの原因で発生しているため，これらの原因を区別せずとも，同様のペナルティをスパムメールの発生時に課すことで問題がないと思われる．一方，ユーザは自分自身の環境を調査することである程度の原因特定が可能である．

原因 1，2 はメンバの不注意によって発行された投稿先メール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．このため，これらの原因で発生した投稿先メールアドレスの漏洩は，漏洩させたメンバに発行したアドレスを無効化・再発行し，ユーザが注意することで基本的に解決できる．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，To や Cc を見ることで，メーリングリストのメンバ以外に投稿先メールアドレスが漏洩した可能性を知ることができる．ただし，Bcc にメーリングリストへの投稿先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．しかし，これらの場合であっても，ユーザは自分の管理する Web ページを確認することや送信ログを確認することによって，自分でメールアドレスが漏洩した原因を突き止めることができる．

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により発生する．このため，スパイウェアやスパイウェアが本システムの仕組みを知っており，ユーザに代わって自動的に再発行のプロセスを実行するような場合には，そのユーザに発行したアドレスを無効化・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全てが無効化される危険性がある．これはメンバのマシン環境に依存するため，メーリングリストシステム側で根本的な対処を行うことはできない．投稿先メールアドレスを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，スパイウェアによって自動的に削除・改変されたメールがないか確認してもらうといった処理が必要である．メンバは自動的に削除・改変されたメールを確認した場合，スパイウェアやウイルスが自分のマシンにインストールされている可能性を知ることができ，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，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．メールの暗合化や電子署名などによって解決することもできるが，メンバが暗合化を行うためのソフトウェアのインストールを行う必要があり，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．

原因 3，4 はユーザのマシンやネットワーク環境の脆弱性により発生している．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，これらの原因の発生を知ることで，自分の環境に脆弱性が存在する可能性を知ることができるという利点となる．

一方，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可能な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．これに対してはメンバにペナルティを課すべきではない．このため，原因 1〜4 によって発生したスパムメールであることと原因 5 によって発生したスパムメールであることをメーリングリストシステム側で明確に区別する必要がある．原因 5 によって投稿先メール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）は有効なメール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誰も登録していないメール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，未登録のメールアドレス向けに送信されたメールを調査することで原因 5 の発生を特定することができる．具体的には正規のメールアドレスに似たダミーのアドレスを監視用メールアドレスとして登録する．例えば，taka1@... が有効であるとすると，taka0@... と taka2@... を監視用メールアドレスとして登録する．taka1@... に加えて，taka0@... や taka2@... などにも，同様のスパムメールが送られてきている場合，それは原因 5 によって発生したものであると判断する．このとき，投稿先メールアドレスの無効化・再発行は必要になるが，スパムメール発生に対するペナルティを与えない．

3.4 提案システムの利便性

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排除するための方法を提案した．本システムでは暗合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

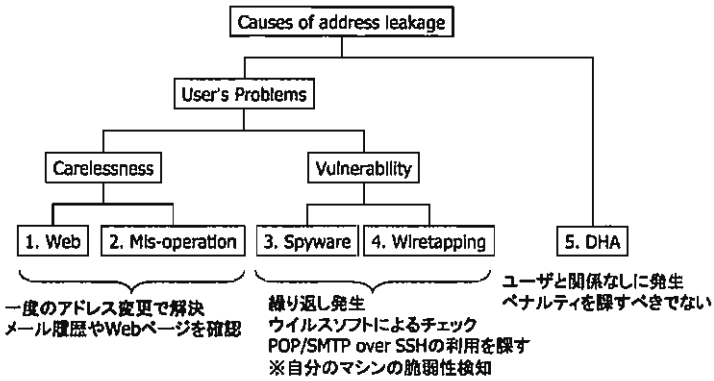

図 6　メールアドレス漏洩の原因分析

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投稿先メール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，それほどメンバの負担になるものではない思われる．一方でメンバは投稿先メールアドレスを自分自身で覚えやすいアドレスに自由に設定することができるため，メンバの利便性が増すものと思われる．投稿先メールアドレスを漏洩させたメンバは，スパムメール発生時に投稿先メールアドレスの変更が必要になるが，スパムメール増加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いえる．このように本システムは，それほどメンバに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．

4. 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もある [7]．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．

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）[9] 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．本提案はメーリングリストの投稿先をユーザごとに異なるものとする提案であり，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できない．

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がある [10]．TEOS（Trusted E-mail Open Standard）[6] 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が行われている [11], [12]．また，[13] や [14] 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 [15] 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．[16] 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といった問題がある．

5. おわりに

本稿ではメーリングリストのメンバごとに異なる投稿先のメールアドレスを発行し，スパムメールが発生した投稿先メールアドレスを無効化・再発行することでスパムメールを排除することを提案した．本提案ではユーザごとに異なる投稿先メール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ずに漏洩した投稿先メールアドレスを無効化することができる．

本提案システムでは，ユーザ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．

今後の課題として本提案システムを実験により評価することや，メールサーバとの通信なしにオフラインで投稿先メールアドレスを変更すること，アドレスを漏洩させたユーザのプライバシを守るためにメーリングリストの管理者も容易に特定できないようにすることなどが挙げられる．

謝辞 本研究は科学研究費補助金（18700076）の支援を受けて行なった．

文　献

[1] Symantec, The State of Spam Report, http://www.symantec.com/business/theme.jsp?themeid=state_of_spam, 2008.
[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] S.L. Pfleeger, G. Bloom, Canning Spam: Proposed Solutions to Unwanted Email, IEEE Security & Privacy, Vol. 3, No. 2, pp. 40-47, 2005.
[4] The Sender ID Framework (SIDF), http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx.
[5] Domain Key Identified Mail (DKIM), http://www.dkim.org/.
[6] V. Schiavone, D. Brussin, J. Koenig, S. Cobb, R.E. Church, Trusted Email Open Standard (TEOS), http://www.cobbsblog.com/spam/teos/TEOSwhitepaper1b.pdf, 2003.
[7] 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.
[8] DNS Blacklist (DNSBL), http://en.wikipedia.org/wiki/DNSBL.
[9] J. Seigneur, C.D. Jensen, Privacy Recovery with Disposable Email Addresses, IEEE Security & Privacy, Vol. 1, No. 6, pp. 35-39, 2003.
[10] G. Lawton, E-Mail Authentication Is Here, but Has It Arrived Yet?, IEEE Computer, Vol. 38, No. 11, pp. 17-19, 2005.
[11] C. Dwork, M. Naor, Pricing via processing or combatting junk mail, CRYPTO'92, LNCS 740, pp. 137-147, 1993.
[12] R. Roman, J. Zhou, J. Lopez, Protection against Spam Using Pre-Challenges, Proc. of 2005 IFIP International Information Security Conference, pp. 281-293, 2005.
[13] R.E. Kraut, S. Sunder, R. Telang, J. Morris, Pricing Electronic Mail to Solve the Problem of Spam, Human-Computer Interaction, Vol. 20, No. 1&2, pp. 195-223, 2005.
[14] B.J. Kuipers, A.X. Liu, A. Gautam, M.G. Gouda, Zmail: zero-sum free market control of spam, Prof. of the 25th IEEE International Conference on Distributed Computing Systems Workshop, pp. 20-26, 2005.
[15] K. Takahashi, T. Abe, M. Kawashima, Stopping Junk Email by Using Conditional ID Technology: privango, NTT Technical Review, Vol. 3, No. 3, pp. 52-56, 2005.
[16] M. Kawashima, T. Abe, S. Minamoto, T. Nakagawa, Cryptographic alias e-mail addresses for privacy enforcement in business outsourcing, Prof. of the 2005 workshop on Digital identity management, pp. 46-53, 2005.