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

2005－DSM－38 (8)
2005／8／5

メーリングリストにおけるSPAM/WORM防止法

菊地 時夫
高知大学理学部

概要

インターネットメールにおいてSPAMとWORMの問題は年々深刻になってきている。特にメーリングリストにおいては、これらの防止は必須の課題である。現状では、会員のみに投稿を制限することくらいしか設定していないことが多いが、WORMは会員アドレスを騙って発信されることもあり、ソフトウェアのサポートを目的としたメーリングリストでは会員以外の投稿も認める必要がある。ウェブ連携メーリングリスト管理システムMailmanでは最新バージョンにおいて、これらの問題を解決するための改良を行ったので紹介したい。

Stopping SPAM/WORMs in Mailing Lists

Tokio Kikuchi
Kochi University

Abstract

There is growing anxiety on the problem of SPAM/WORMs on the Internet mail messages. It is essential to stop these unwanted messages flowing through a mailing list. SPAMs may be stopped by restricting post to members of the list, but WORMs can go through by forging the 'From:' address as a member. Moreover, some lists for supporting products like softwares (free or enterprise) cannot restrict posting to the members. Mailman, a web-integrated mailing list manager, achieved advances in stopping SPAM/WORMs from being delivered to the members of mailing lists, in the latest release version.

1 はじめに

インターネット接続環境の普及により、現在では大多数の人がメールを使える環境にあり、またメール無しでは仕事ができないという人も増えている。この中で、SPAMと呼ばれる無差別広告メールや、ウィルス感染によるWORMメールも増加する一方で、深刻な問題となっている。

一方、メールでの個別連絡から一対多、多対多の情報交換を可能とする、メーリングリストについては、メールの可能性を広げるものとして古くから存在しているが、SPAMにとっては1通を多数に配布してくれるのでターゲットとして絶好であり、また、WORMが流れた場合にも影響力が大きい。

Web連携メーリングリスト管理システムとして、最近利用が広がってきているMailman[2][1]においては、SPAMフィルターや添付ファイル保管機能を備えるなど、セキュリティに対する配慮を

[2]試しに, リストの案内ページの"他人がおせっかいで入会手続き"でGoogle検索したら5130件ヒットした

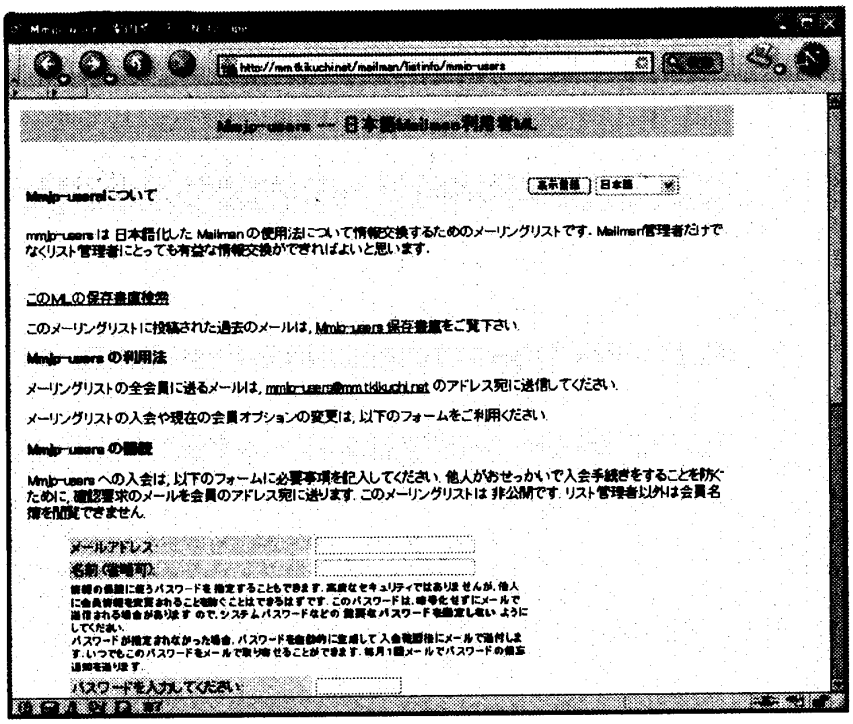

図 1: 典型的な Mailman メーリングリスト案内ページ

おこなってきているが、必ずしも十分とは言えなかった。ここで典型的な Mailman のリスト案内ページを図 1 に示す。Mailman 2.1.6 のリリースに当たって、筆者が開発チームの一員として改良を加えたことにより、SPAM/WORM に対抗する必要な機能を備えることができるようになったので紹介する。

2 メーリングリストのタイプ

一般にメーリングリストは、その発信配送形態によって、次のような 3 つのタイプに分けることができる。

1. ディスカッション型

   主に討論を目的としており、リスト参加者の誰もが等しく発言権を持つ。

2. アナウンス型

   いわゆるメルマガやニュースレターと呼ばれるもので、発信者は一人または非常に限定されており、多くの読者へ配送する。

3. グループサポート型

   一般にはこの型は意識されることが少ないが、会社に対する意見やソフトウェアや製品についてサポートをするとき、受け付けたメールを複数で読み対応するためのメーリングリストである。

多くのフリーソフトではディスカッション型メーリングリストによるサポートが行われているが、実際の議論の進行は質問と回答の形で進むことが多く、実質上グループサポートになっていく

傾向が見られる。

3 従来のSPAM防止法

前記3つのタイプのうち最初の2つについては、それぞれSPAM防止法は確立していると言ってよいだろう。つまり、メール発信権を会員または特定少数に限ることである。多くのspammerは発信者アドレスによってふるい落とされない様に、頻繁に発信者アドレスを変えたり詐称したりしているため、メールを発信するたびにリストに入会（subscribe）するのは非効率的なことである。従って、ディスカッション型のリストでは会員のみに発言権を制限しているのが殆どである。また、同様に発言を特定少数に限るアナウンス型リストでも、SPAMが流れることはほとんど無い。

しかし、一方でグループサポート型のメーリングリストでは、不特定多数からのメールを受け付けることが必要であり、また、そのメールアドレスが公開されているため、多くのSPAMをひきつけやすいという特徴を持っている。前にも述べたように、多くのフリーソフトサポートはディスカッション型を用いているが、いちいち入会しなくても質問を受け付けられるように、非会員からの投稿を認めているリスト[3]もあり、そこでは多量のSPAMが流れてきて、繰り返し問題になっている。

この場合の解決策は司会プロセス（moderation）を導入することで、

1. リスト会員（サポートスタッフ）からのメールは無条件で配送。
2. 非会員からのメールは一旦配送を保留し、司会者が配送するかどうかを決定する。
3. オプションとして、できれば、配送を一度認めた非会員からのメールは、次回からは無条件で配送する。

のような形が考えられる。

しかし、このような改善を行ったとしても、SPAMが多くなると、配送する必要のある質問などのメールがSPAMに埋もれてしまう可能性があり、司会者の負担もばかにならなくなってくる。なんらかの方法で、SPAMを自動的に判断して破棄することができれば、そのほうが望ましい。

4 WORMの問題

以上のように、多少の問題は残るがSPAMについては比較的効果的にリスト配送をくいとめることができる。しかし、一方でWORMについては、発信者のアドレスをもとにしたメール配送の可否決定方法では不十分である。つまり、ある会員のPCがウィルスに感染した場合、その会員が登録されているディスカッションリスト宛てにWORMの付いたメールが発信され、そのままリストに配送されてしまうことがありうる。

WORMによる被害が広範に認識されている現在では、個々にアンチウィルスソフトを利用するのが常識となってきているようだが、それでもなお、頻繁にウィルスデータを更新できないような、低速回線での利用者も残っており、リストサーバを通過する時点でWORMを止めることは必要である。

[3]一例としてはFreeBSD-Users-JP

5 Mailman (2.1.6) の設定

はじめにも述べたように、Mailman 2.1.6 においては SPAM/WORM 防止のために、多彩な項目を Web インタフェースを通じて設定することができる。特に、WORM の場合で問題になるのは添付ファイルであり、これについては、添付ファイルを取り除いて配布したり、メールそのものを保留や破棄することができる。以下にその詳細を見ていく。

5.1 添付ファイルの除去

Mailman のリスト管理インタフェースは

`http://server/mailman/admin/listname`

の URL でアクセスでき、管理者のパスワードでログインした後に、各種の設定項目を分類したリンクが表示される。

添付ファイルの除去は最後から 2 番目にあり、ここでは MIME タイプと添付ファイルの拡張子を基にして、それぞれ指定したものを残したり削除したりすることができる。

WORM 防止のためには平文テキスト（`plain/text`）以外を通さないことが究極の選択と考えられる[4]が、職場等のポリシー・利便性のためにはそのような合意形成が難しいことも考えられる。この場合例えば画像ファイル（`image`）を許可するなど、必要に応じて MIME タイプを追加すればよいはずであるが、現実には MIME タイプを偽る WORM もある。これは Microsoft Windows が MIME タイプでなく、拡張子を見て動作を決めていることに起因する問題である。Mailman 2.1.6 では従来の MIME タイプによるフィルタリングに加えて拡張子による除去もできるようになっており、一般に危険と考えられている拡張子はリスト作成時にデフォルトとして入っているので、後はフィルタリングを有効にすればよい。

5.2 メール全体に対する処置

「添付ファイルの除去」で、危険な添付ファイルの配布を防止できるが残りの意味不明のメールが配布されてしまう。図 2 に示す、プライバシーの下のスパムフィルターでは、従来からメールのヘッダ情報に基づいて、正規表現によるメールの振り分け（通過、保留、拒否、破棄）ができていたが、2.1.6 ではヘッダ情報を添付部分からも収集することにより、添付ファイル名に入っている拡張子も検査することができるようになった。

ここに

`content-.*name.*\.(exe|com|cmd|bat|pif|vbs|scr|zip)`

を入れて、「拒否」又は「破棄」に設定することで WORM メール全体が流れないようにすることができる。

6 対 SPAM ツールとの連携

WORM に対する処置は、以上のように添付ファイルに対する問題であったが、SPAM に関してはメール本文の特徴などを把握する必要があるため、メーリングリスト管理システム単体での処理は難しく、spamassassin[2] などのツールを併用する必要がある。

[4]実際には添付のコンテナとしての `multipart` も除外する必要がある

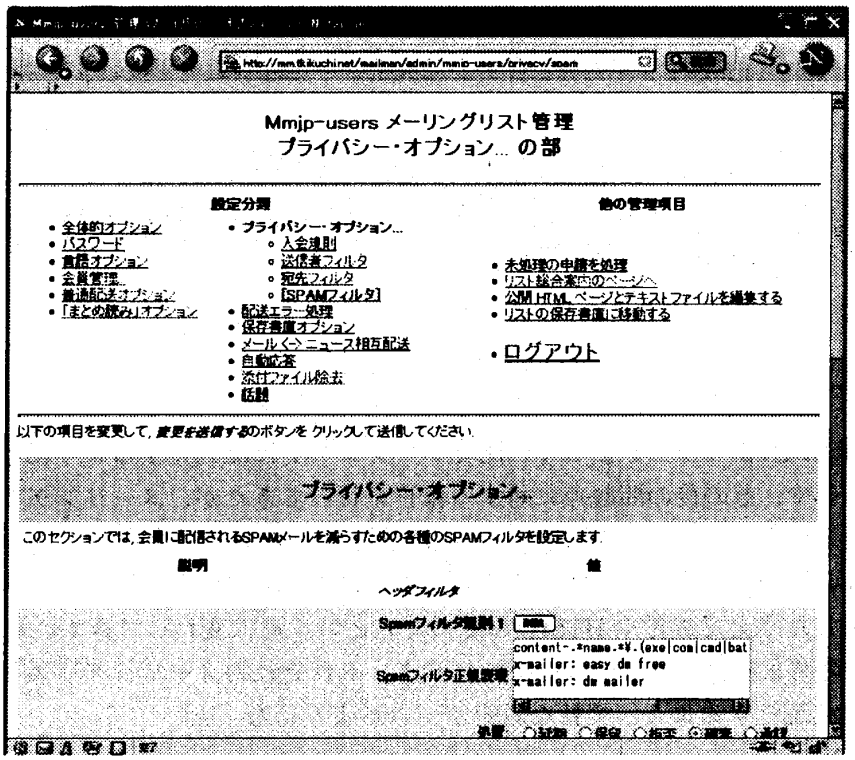

図 2: Mailman 管理インタフェース（スパムフィルター）

SpamAssassin を利用するには、一般には procmail[3] を使ってローカル配送時に通し spamassassin が付加するヘッダ情報によって振り分けるのが一般的である。しかし、メーリングリストの配送は aliases によって直接配送プログラムに渡されるため、特別の手当てが必要である。

Mailman においては subject（件名）に付ける prefix（前置き）や本文の最初と最後に付けるヘッダとフッタなどの処理を行うため、パイプラインに並べたモジュールを順に実行している。ここに、独自のモジュールを挿入して処理を行うことができるようになっており、spamassassin を起動してその結果を使ってメールに対する処置を行うことができるようなモジュールがパッチとして登録されているので、これを利用することができる。

また、postfix[4] の filter などを通して spamassassin のチェックを行っている場合には、前述のスパムフィルターのところでヘッダをチェックして、処置することができる。

6.1 スパムフィルターの利用

前述のように、効果的な SPAM 対策には、外部ツールの併用が必要であるが、Mailman のスパムフィルター単体でもいくらかのスパム対策を行うことができる。例えば、SPAM の中には宛先（To: ヘッダ）にいいかげんなアドレスを入れているものも多いが、従来からある「宛先フィルター」では保留にすることしかできず、従って -owner アドレス宛てに通知メールが配送されて、管理者にとってはわずらわしいことになっていた。

正規表現に基づくスパムフィルターでは、まず

```
\nto:.*your-list-name
cc:.*your-list-name
```

のパターンで、宛先がきちんと書かれているものを通し、それ以外を

ドット1個のパターン（全てに一致）で破棄することができる。

このように、正規表現を駆使することでかなりの部分まで、対SPAM/WORM対策を施すことができるのが、新しいMailmanの特徴である。

7 おわりに

2004年8月末にCVSコミッタとして、開発プロジェクトに深入りするようになり、それまでに溜めていたパッチや、その後の問題点に対する修正を行ってきたが、メーリングリストに対する要求は益々多彩なものとなってきている。添付やHTMLの問題はその典型で、かつては、読むことのできない人もいるから、あるいはウィルスの危険があるからという理由で全て排除できたが、最近は安全を確保したうえで添付やHTMLを認めたいという形に変わってきている。Mailman 2.1.6では、その全ての要求にかなうものではないにせよ、それぞれのメーリングリストのポリシーを最大限安全な形で実現できるよう、柔軟な設定ができるようになった。

謝辞

Mailmanの開発の中心となっているBarry Warsaw, 日本語化（i18n翻訳作成）にあたってご協力をいただいた多数の皆さんに感謝します。

参考文献

[1] Warsaw, B. et al.: Mailman, the GNU Mailing List Manager, http://www.list.org/ (1998-2005).

[2] The SpamAssassin(tm) Project: Welcome to SpamAssassin, http://spamassassin.apache.org/ (-2005).

[3] van den Berg, S. R. et al.: Welcome to procmail.org, http://www.procmail.org/ (-2005).

[4] Venema, W. et al.: The Postfix Home Page, http://www.postfix.org/ (-2005).