広告メールの件名規制にともなうスパムメールへの対策

リスク工学特別演習グループ課題 13 番：インターネットセキュリティ
担当教官：片岸一起

025203 河副文夫　025204 鎌田芳雄　025207 多賀慶

1．はじめに

インターネットの急速な普及は社会を大きくかえた。中でも電子メールは Web とならんで現在のインターネットの中核をなしており、いまや我々の生活に欠かすことはできないものとなっている。

電子メールの歴史は長く「ARPANET」としてインターネットが本格的にスタートした 2 年後の 1971 年には、米国 BBN 社が、現在の電子メールの基礎となるシステムを開発している。この電子メールシステムはその後、ARPANET 用に改良され、インターネットを利用する学者や研究者の間で急速に広まった。電子メールは、郵便の手紙に比べ、配達にかかる時間が非常に短い、電話のように相手の都合を気にすることなく、自分のペースでメッセージを送ったり読んだりできるといった利点があるため、手紙、電話に代わる新たなコミュニケーションツールとして、老若男女を問わず、世界中に普及している。しかし、電子メールが誕生してから 30 年が経った今日では、他のインターネット技術同様、電子メールもセキュリティ上の多くの問題を抱えており、その解決が望まれている。

2．電子メールの抱える問題

世界のインターネット利用者は 4 億人に上るといわれ、現在では年間 2 兆 7000 万通ものメッセージが世界中に送られている。電子メールの利用目的も個人宛の手紙から企業の広告メール、共通の趣味を持つ人へのメールマガジンと非常に幅広い。電子メールは Web と共に現在のインターネットでは中心的な存在であり、インターネットの持つオープン性から、悪意を持った人間に狙われる機会も多い。一般に電子メールの本文はテキストとして平文でネットワーク上を伝送されることから、改竄、盗聴、なりすまし等がその直接の脅威となる。

また、電子メールの引き起こす間接的な脅威としては、いわゆる spam の問題があげられる。大量のメールが無差別に送られることに起因して、トラフィックが混雑し、時としてサーバダウンのリスクをも招くことになる。さらに、spam では、メールの内容自体が電子メール利用者の望まないものであることも多く、それが深刻な問題となることも決して少なくない。spam はメールサーバ管理者、メール利用者の両者にとって大きな脅威となり得る。次節以降では spam とは何かを説明するとともに、その問題を分析し、詳述する。

3．spam とは

郵便では、ビラの印刷代や切手代など送る数に応じたコストが発生するが、電子メールの場合、アメリカでは市内通話は電話を切らない限り同額であるように、たとえ 1 万人に送ってもほとんどコストはかからない。このことから、電子メールを宣伝に用いることは、電子メールが誕生した初期から行われてきた。さらに、名簿を売買し郵便を利用したダイレクトメールを配送する商売が存在するのと同じく、電子メールでも電子メールアドレスを売買し、広告メールを送りつける商法が生まれた。電子メールの持つコスト、手間、時間における利点から、広告を配信する相手を選ばず、無差別に大量の広告メールの配信が行われるようになった。

このような不特定多数を対象とした大量の広告メールがいわゆる”spam”の代表である。日本の法律では spam という言葉は使われていないが、それに代わるものとして、[その送信をすることに同意する旨の通知をした者等一定の者以

外の個人に対し、電子メールの送信をする者（営利を目的とする団体及び営業を営む場合における個人に限る。以下「送信者」という。）が自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メール]を「特定電子メール」と定義している。

電子メールの簡便さから、このような spam は個人でも容易に行うことが可能であり、電子メールアドレスだけを無差別に集めた CD-ROM の販売も実際に行われている。「10 万件の電子メールアドレスがたった 100 ドルで手に入る。」というふれこみで、その宣伝のダイレクトメール自体もその CD-ROM にある電子メールアドレスに送りつけられている。

実際の spam の例としては 1994 年に行われたアメリカ永住権抽選手続き代行の宣伝があげられる。この抽選というのは、アメリカの永住権が抽選で当たるというもので、その応募書類作成を $95 で代行する、という宣伝であった。しかし、実際はこの応募自体にはお金はかからず、応募要項をきちんと読めば自分で作成するのも決して難しいものでない。つまり、この メールは単に不特定多数に大量に送られたというだけでなく、内容も詐欺同然といって良いものであった。

3.1. spam の語源

“SPAM” はもともと、Hormel Foods 社の缶詰の商品名であり、この SPAM の缶詰をネタにしたコント が spam の語源となった、というのが定説である。そのコントの内容は

> とあるレストランで夫婦が食事をしようとするが、メニューには SPAM が入ったものしかない。ウエイトレスと SPAM のメニューについて口論していると、後ろにいたバイキングたちが「SPAM、SPAM…」 と歌を歌い出し、それにかき消されて会話が続けられなくなってしまう。

というもので、ここから、同じことを何度も何度も繰り返されること、そしてそれによって本来の会話や議論を妨げるような迷惑行為を spam と呼ぶようになったとされている。

3.2. spam の分類

“spam” は俗称であり、正式には、種類によって以下のように分類される。

- UCE (Unsolicited Commercial Email): 勝手に送りつけてくる広告電子メール
- UBE (Unsolicited Bulk Email): 勝手に送りつけてくる大量の電子メール
- EMP (Excessive Multi-Posting): 過度の量のマルチポスト
- ECP (Excessive Cross-Posting): 過度の量のクロスポスト

電子メールによって送られるものは UCE、UBE、また Netnews に大量に投稿される迷惑記事は EMP、ECP と呼ばれている。本文では UCE、UBE を合わせてスパムメールと呼ぶ。

3.3. スパムメールによるリスク

スパムメールはメールサーバ管理者、メール利用者の両者にリスクをもたらす。本節ではメールサーバ管理者のリスクとメール利用者のリスクにわけてこれを分析する。

3.3.1. メールサーバ管理者のリスク

送り付けるスパムメールの数は数万、数十万通にも及ぶので回線、サーバのリソースを食い潰す。AOL では一日数千万通にもおよぶメールの 30% 近くが spam ではないかと予想され、大規模な ISP では顧客数が多いので受信にあたってもかなりの負担を負わされることになる。大量のメールは DoS 攻撃と同様にトラフィックを混雑させ、場合によってはサーバのダウンをも招く。

また、スパムメールを送付する人は、そのメールが大部分の人にとって歓迎されないことを知っているため、第３者のサーバを中継して送信することが多い。そのため、こういった中継に利用されたメールサーバの管理者には多くの受信者から抗議、苦情のメールが押し寄せることになり、サーバおよび、それを管理する団体の社会的信用の失墜も免れない。また、このような第３者のメールの中継をするサーバをブラックリストに掲載し、そのサーバからの受信を拒否する団体が現れているため、サーバ管理者は、利用者からのクレームだけでなく、これらの対応にも追われることになる。

3.3.2. メール利用者のリスク

新聞の折り込み広告や郵便のダイレクトメールは受け取るためにお金はかからない。電話も同様である。しかし電子メールの場合、受け取る側がお金を払っている。プロバイダへの接続料金、電話代、コンピュータの電気代などはメールを読む人間が払っていることになる。とくに携帯電話ではパケット通信料として直に受信者に金銭上の負担がかかる。

また、スパムメールの内容は受信者の性別、年齢、職種、趣味などで分類されていることはまずなく無差別に送り付けられるので受信者にとっては興味がない内容のものがほとんどあり、受信するにあたって時間的資源を浪費することになる。特に最近では電子メールでのやり取りがビジネスの中に組み込まれ、欠かせない存在になってきており、重要なメールとスパムメールのようなジャンクメールとが混在してしまうことは仕事の効率などを下げる要因になる。また、アダルトサイトの広告やアダルト画像などが添付されたメールなどを受信することは精神衛生上良くないという側面も見逃せない。メールアドレスを持つ子供にこのようなスパムメールが来ることも問題である。さらに、メールの内容が違法性のある場合もあり、「無限連鎖講の防止に関する法律」に引っかかるもの、詐欺であるもの、違法な商品販売であるものといったメールを見て、違法と知らずにそれらを購入したり、騙されたりという可能性もある。

4．スパムメールの現状

4.1. スパムメール被害実態調査

2002 年に総務省の関連団体によってスパムメール被害実態調査[1]が行われた。その結果の一部を図1,2,3 に引用する。

スパムメールの受信状況に関しては、「受信したことがない」という回答はわずか 4.5%であり、ほとんど（95.5%）の電子メール利用者は何らかの迷惑メール受信の受信経験があるということになる。メールの種類別では「勝手に送りつけられてくる広告メール全般(出会いサイト紹介係含む)」（83.1%）が最も多い。

利用者や ISP（インターネットサービスプロバイダ）がスパムメールに対してどのような認識をしているのかを見てみると、どちらも合計すると 9 割以上がスパムメールは問題だと考えている。問題ではないは ISP で 2%、利用者で 1.4%程度とごくわずかである。

現状と将来のスパムメール対策に目を向けると「スパムメール対策は何も行っていない」という回答は 5.5%しかないが、一般的な対策は「とにかく削除する」（87.8%）というものであった。受信拒否やフィルタリングなどの対策は 4 割以下と少ないことがわかる。

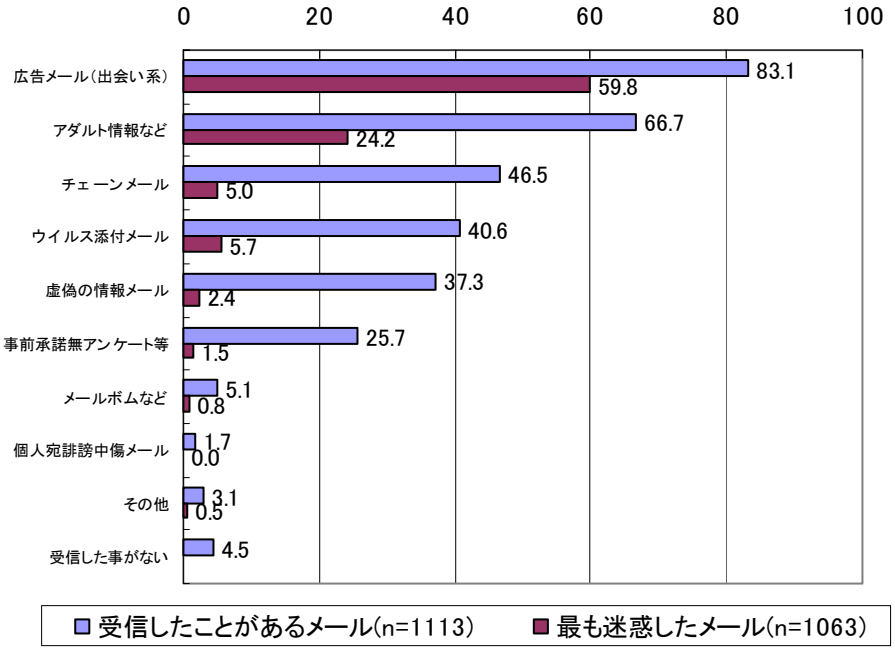

図1　スパムメールの受信状況

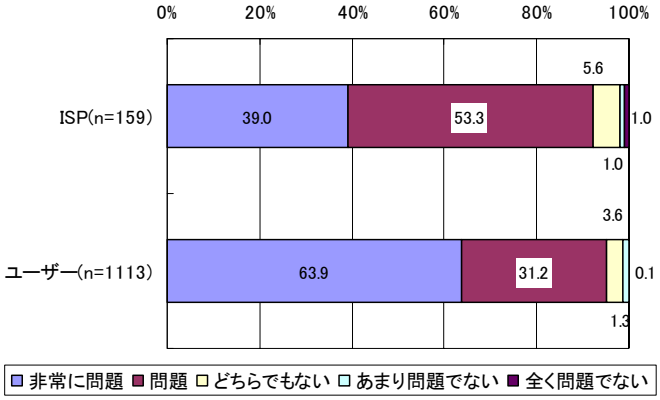

図2　スパムメールは問題だと思うか（択一回答）

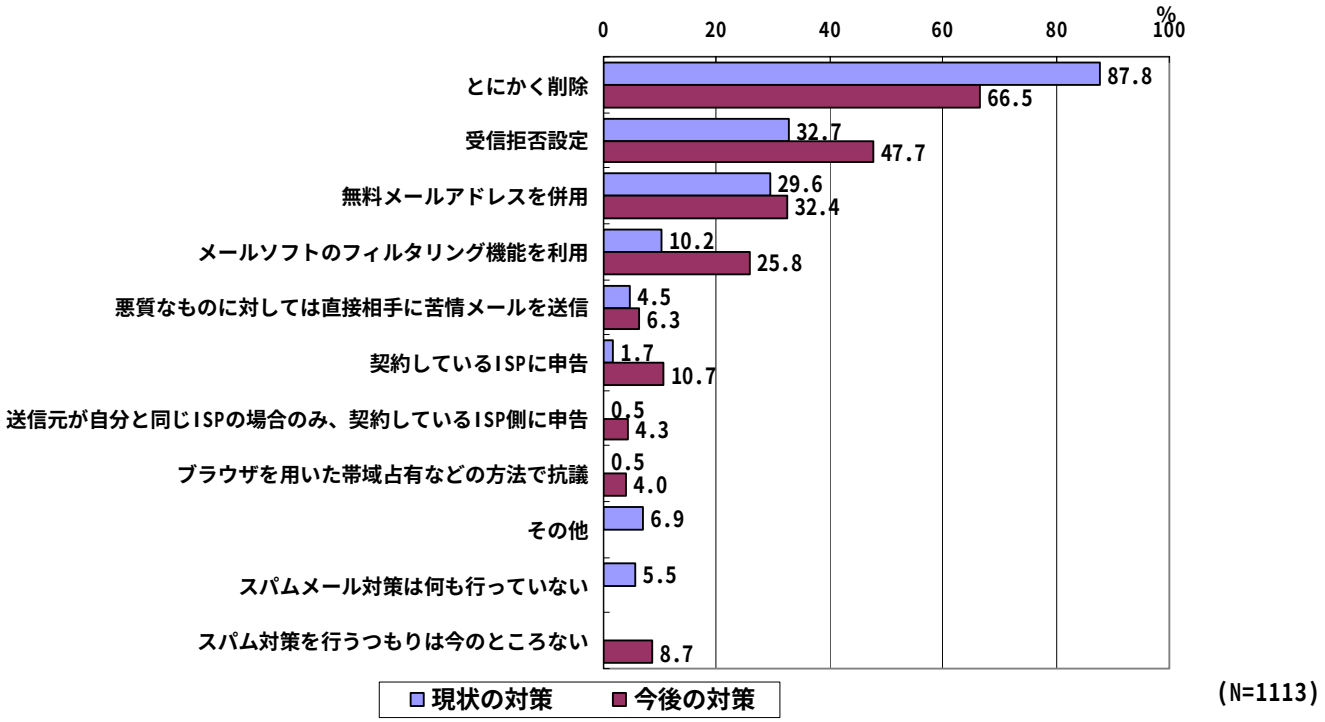

図3　現状と将来のスパムメール対策（複数回答）

4.2.　現在のスパムメール対策

現在、ISP で行われているスパムメール対策は自ドメイン外のメール中継の禁止、メールアドレス、ドメイン名によるフィルタリングが主なものである。

インターネットの発展期には、バケツリレー式にデータを転送する UUCP というプロトコルが使われており、メール中継を誰にでも許さなければ電子メール自体が成り立たない状態であったため、スパムメールの転送を許していた。しかし、現在では、直接 IP 接続することが可能となったので、自ドメイン外へのメール中継が MTA の設定によって禁止されているメールサーバがほとんどである。アドレスによるフィルタリングはスパムメールの送信元であるメールアドレスを登録し、そのアドレスからのメールを拒否するといったものである。

前述のスパムメール被害実態調査によると、過半数の ISP が現在行っているスパムメール対策は「サーバの設定などで不正中継を防止するなど」（82.6%）と「送信元が自社利

（表示の方法等）

第二条　法第三条各号に掲げる事項は、次の各号に定める特定電子メールの受信に係る通信端末機器の映像面に表示される場所に表示されるようにしなければならない。

一　法第三条第一号に掲げる事項　当該特定電子メールに係る表題部の最前部

二　法第三条第二号に掲げる事項（当該特定電子メールの送信者の氏名又は名称に限る。）、同条第四号に掲げる事項及び同条第五号に掲げる事項（次条第一号に掲げる事項に限る。）

三　法第三条第二号に掲げる事項（当該特定電子メールの送信者の住所に限る。）及び同条第五号に掲げる事項（次条第二号に掲げる事項に限る。）　任意の場所（当該事項を当該特定電子メールに係る場所以外の場所に表示されるようにするときは、その場所を示す情報を当該特定電子メールに係る任意の場所に表示されるようにしなければならない。）

四　法第三条第三号に掲げる事項　当該特定電子メールに係る送信者の電子メールアドレスの表示部

五　法第三条第五号に掲げる事項（次条第三号に掲げる事項に限る。）　当該特定電子メールに係る任意の場所

2　法第三条第一号に掲げる事項の表示は、「未承諾広告※」とする。

3　第一項第一号から第三号までに掲げる事項（同項第三号に掲げる事項については、当該特定電子メールに係る任意の場所に表示されるようにするときに限る。）は、通信文で用いられるものと同一の文字コードを用いて符号化することにより表示されるようにしなければならない。ただし、特定電子メールの送信に必要な範囲において、他の符号化方法により重ねて符号化したものは、重ねて符号化する前の文字コードを用いて符号化しているものとみなす。

4　送信者は、第一項第二号に掲げる事項の表示の直前に、「〈送信者〉」と表示されるようにしなければならない。

図4　特定電子メールの送信の適正化等に関する法律の一部

用者の場合は警告や退会処分」（53.8%）である。一方で、予算や人手などの制約要因によってスパムメール対策を行えないISPも1割程度存在している。

4.3. スパムメールに対する法律の整備

スパムメールの広がりと被害の拡大を受けて、特定電子メールの送信の適正化等に関する法律が2002年6月21日に交付されている。（施行：2002年7月1日）その一部を抜粋し、図4に示す。要約すると、一時に多数の者に対してされるスパムメールに対して

・メール件名の文頭に「未承諾広告※」と表示すること

・受信者に受け取り拒否の手段を提供すること

といったものであり、違反すれば罰せられる。

4.4. 実際のスパムメール

NTTドコモの携帯を用いて、実際にどのようなスパムメールが届いたか調査した結果を述べる。メールアドレスは英数字をまぜた7文字であり、すでに存在していたものではなく新規に変更したものを利用した。このメールアドレスに2002年8月の一ヶ月間に届いたスパムメールを調査した。その結果、一ヶ月間に133通の広告メール（出会い系：130通）が届いた。最初の3日は、スパムメールは送られてこなかったが、その後は一日平均約5通、多い日で8通のメールが昼夜を問わず送られている。送信元のアドレスは3箇所であり、一つのアドレスから複数の違った内容のメールが送られてきた。

また、4.3.の法律施行を受けて全ての広告メールの件名に「未承諾広告※」の文字が入っていた。ただ、件名がきっかり「未承諾広告※」であるメールは19通であり、その他のメールの件名は「未承諾広告※*」となっていた。（*はスペースを含む任意の文字列）

NTTドコモは2001年11月に携帯電話にインターネットから送られる電子メールの84%が、実在しないアドレスへのメールであると発表している。このほとんどが、ランダムに送られた広告メールであり、残りの16%の中にも、たまたま相手にヒットしたメールがあるので、携帯電話へインターネットから送られる電子メールのほとんどは広告メールであるといっても過言ではない状況である。

5．スパムメール対策

本章では、メール利用者のリスクを軽減するためのスパムメール対策を提案する。前節で述べたスパムメールの現状をもとに、要求項目を検討し、設計方針をまとめる。

5.1. 現在のスパムメール対策の問題点

自ドメイン外のメール中継の禁止は、送信元を隠したスパムメールを抑制するが、自ドメイン内のメールアドレスに直接送られてくるスパムメールを防ぐことができない。

また、スパムメールの送信者はYahoo、Hotmailなどのフリーメールなどを利用し、メールアドレスをかえながらメールを送ってくるのでメールアドレスによるフィルタリングでは、対処療法的な対策しか立てることができない。ドメイン指定受信ではスパムメールではない必要なメールも受信できない可能性がある。

MUA上では、より高度なフィルタリングができるソフトウェアが開発されているが、そのためには一度メールを受信しなければならず、通信料の問題の解決にはならない。

5.2. 要求仕様の検討

まず、第一の要求仕様として、スパムメールによってもたらされる金銭的、時間的リスクを軽減することがあげられる。

また、電子メール利用者の９割以上がスパムメールは問題としていながらも、受信拒否やフィルタリングなどの対策は4割以下と利用者による対策はほとんどなされていない。これは、利用者に十分な知識がないこと、設定に手間がかかることが、その原因であると考えられる。そこで、第二の要求仕様として、スパムメール対策にともなう煩雑な設定といった負担を利用者にかけないことをあげる。

さらに、前章よりスパムメールの８割以上が広告メールであることがわかる。よってこれらの広告メールが直接利用者のもとに届けられるのを防げば、スパムメールによるメール利用者のリスクはかなり軽減されるものと思われる。そこでこれらの広告メールが利用者に直接届けないことを第三の要求仕様とする。

最後に、これらの広告メールを必要とする利用者が存在することも想定して、利用者の必要に応じて広告メールも閲覧できるようにすることを第四の要求仕様とする。

5.3. 設計方針

要求仕様の第一、第二を満たすために対策はMTA上で行うものとする。今回は、sendmail (ver.8.11.6-3)というMTAを使用する。

また、5.1.の考察より、メールアドレス、ドメイン名によるフィルタリングでは、広告メールが利用者に届けられるのを事前に阻止することが難しいこと思われる。その一方で、4.4.より現在ほとんどの広告メールは法律を遵守し、件名に「未承諾広告※」と明示していることがわかる。そこで第三の要求仕様を満たすために、メールの件名をフィルタリングし、件名に「未承諾広告※」とあるメールが利用者に届かないようにする。法律によって未承諾広告メールの件名の文頭は「未承諾広告※」と指定されていることから、件名の文頭が「未承諾広告※」の場合にフィルタリングを行なう。

第四の要求仕様を満たすため、フィルタリングしたこれらのメールは別に保存し、利用者の必要に応じて広告メールも閲覧できるようにする。フィルタリングされた未承諾広告メールは、利用者のホームディレクトリバックアップすることにする。

6．システムの実現

6.1. 構築したシステムの概要

5.3.の設計方針に基づき、未承諾広告メールフィルタを構築した。その際には、ＰＣにＯＳをインストールするところから始めた。その後ＭＴＡの設定を行ない、そこからシステムの構築を始めた。システムの構成に使用したサーバのスペックは以下のようになっている。

[OS] RedHat Linux 7.2
[CPU] PentiumII 300MHz
[Memory] 64MB
[HDD] 10G

使用したＭＴＡはsendmail(ver.8.11.6-3)で、システムはローカルエリアネットワーク(ＬＡＮ)上に構築した。

6.2. システムの構築方法

システムの構築方法としては以下のようになっている。

1. sendmailが渡すメール配信プログラムを作成するフィルタリングプログラムに変更する。
2. フィルタリングを行なうプログラムで、送られてきた電子メールを一時ファイルに保存する。

3. ヘッダ部分の「Subject:」行に書かれた件名をチェックする。
4. 件名の文頭が「未承諾広告※」の場合は保存しておいたファイルを利用者のホームディレクトリにコピーする。それ以外であった場合は保存しておいた電子メールを普通の場合と同様に送信する。

6.3. システムの構築

6.3.1. sendmail.cfの設定

sendmailの動作はsendmail.cfという設定ファイルが決定している。sendmail.cfの最後のほうにメール配信プログラムを指している部分があり、以下のように書かれてある。標準ではprocmailになっている。

```
Mlocal,     P=/usr/bin/procmail,
            F=lsDFMAw5:/|@qSPfhn9,
            S=EnvFromL/HdrFromL,
            R=EnvToL/HdrToL,
            T=DNS/RFC822/X-Unix,
            A=procmail -t -Y -a $h -d $u
```

従って、この部分を作成したフィルタリングを行なうプログラムを指すように変更する。そして、プログラムの最後で元々のメール配信プログラムに渡すことによってメールを送信する。

プログラムを指すようにこの部分を変更すると以下のようになる。

```
Mlocal,     P=/filter/./cm_filter,
            F=lsCDFMAw5:/|@qSPfh9,
            S=EnvFromL/HdrFromL,
            R=EnvToL/HdrToL,
            T=DNS/RFC822/X-Unix,
            A=./cm_filter -Y -a $h -d $u $g
```

ただし、

/filter/./cm_filter

は作成したフィルタリングプログラムのことである。

変更を行なった後にsendmailを再起動すると、sendmailは標準のprocmailには渡さずに今回作成したプログラムに渡すことになる。

6.3.2. フィルタリングプログラム

フィルタリングを行なうプログラムはシェルスクリプトで書いた。プログラムの動作としては以下のようになる。

動作の説明をすると、最初に送信されてきたメールをファイル(mail)に保存する。次にヘッダー部分を取り出し、ファイル(header)に保存する。その後、「件名の文頭12byte分(未承諾広告※の分)」,「送信先」,「メールの固有ID」を取り出す。件名をチェックし、件名の文頭が「未承諾広告※」の場合は、各利用者のホームディレクトリ内のspamディレクトリに、メールの固有IDをファイル名として送信されてきたメールを保存する。これをバックアップとする。(ただし、spamディレクトリはあらかじめ作成しておく。またspamディレクトリを作成する理由としては、整理のためである。)件名の文頭が「未承諾広告※」でない場合は通常通りに送信する。

このときに件名の文頭の「未承諾広告※」内部のスペースや、半角全角等の違いは考えられていない。つまり件名の文頭が「未承諾広告_※」となっていた場合のようにスペースが間にある場合は、このメールは未承諾広告メールではなく、通常のメールとして考えられ、通常通り送信を行なう。ただし、_はスペースを意味する。まとめると、件名の文頭が「未承諾広告※」と一字一句でも同じでない場合は、フィルタリングを行なう対象にはならない。最後に一時的に保存されたファイル(mail、header)は削除する。

フローチャートは図 5のように、実際のスクリプトは以下のようになる。

```
#!/bin/bash
# filter for sendmail

# sendmail からメールを受け取り, ファイル(mail)に保存
cat > mail

# 最初の空行までのヘッダ部分を取り出し, ファイル(header)に保存
sed -n '1,/^[ ]*$/p' mail
> header

# Subject:行の件名の最初の12byte(「未承諾広告※」のみ)を取り出す
subject=`grep "^Subject:" header
```

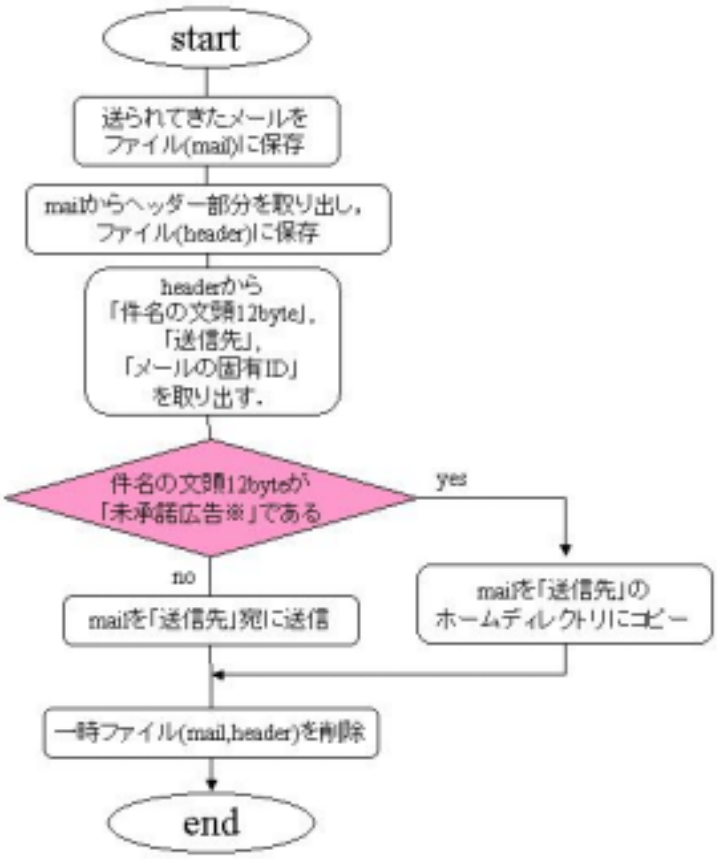

図５　特定電子メールの送信の適正化等に関する法律の一部

```
  | cut -f2 -d' '
  | cut -c 0-12`

# To:行の宛先から利用者名を取り出す
user=`grep "^To:" header
  | cut -f2 -d' '
  | cut -f1 -d'@'`

# Message-Id:行のIDを取り出す
ID=`grep "^Message-Id:" header
  | cut -f2 -d' '
  | cut -f1 -d'@'
  | cut -f2 -d'<'`

# 件名の文頭が「未承諾広告※」の場合は送信せず
# 違う場合は普通に送信
if [ $subject != "未承諾広告※" ]
then
# 普通に送信
# 送信後，一時ファイル(mail,header)を削除
/usr/bin/procmail -Y -a
"servername" -d $7 < mail
rm -f *
else
# 保存しておいたファイル(mail)を利用者のホームディレクトリ
にコピー
# 送信後，一時ファイル(mail,header)を削除
cp mail /home/$user/spam/$ID
rm -f *
fi
```

ただし実際のファイル名等はフルパスを与える。

７．システムの評価

構築を行なったシステムの評価を行なうため、以下のような実験を行なった。

7.1. 実験内容

実験は件名の文頭が「未承諾広告※」のメールと、それ以外のメールを送ってフィルタリングできるか実験した。

また、フィルタリングされた場合は利用者のホームディレクトリにバックアップされるかどうかを調べた。

具体的な実験は以下の4つである。

7.2. 実験

7.2.1. 実験1

まずは動作確認として件名が「未承諾広告※」ではない普通のメールを送った。送ったメールの内容は以下のものである。

To:user1
From:user2
Subject:test

This is test mail.

7.2.2. 実験2

次に件名の文頭が「未承諾広告※」である、フィルタリングされるべき未承諾広告メールを送った。送ったメールの内容は以下のものである。

To:user1
From:user2
Subject:未承諾広告※

This is spam mail.

7.2.3. 実験3

次に件名の文頭が「未承諾広告※です。」である、フィルタリングされるべきではないが、未承諾広告メールの条件(文頭が未承諾広告※)を満たしているメールを送った。送ったメールの内容は以下のものである。

To:user1
From:user2
Subject:未承諾広告※です。

This is not spam mail.

7.2.4. 実験4

次に未承諾広告メールであるが法律を守っていない(文頭が未承諾広告※でない)メールを送った。具体的には件名の「未承諾広告※」の「未承諾広告」と「※」の間にスペースが入っている。送ったメールの内容は以下のものである。

To:user1
From:user2
Subject:未承諾広告 ※

This is false spam mail.

7.3. 実験結果

実験結果は表 1のようになる。

表1　実験結果

件名	配信	バックアップ
test	○	-
未承諾広告※	×	○
未承諾広告※に関する報告	×	○
未承諾広告 ※	○	-

表1から分かるように件名が「未承諾広告※」となっているものは希望通りフィルタリングされて受信されていない事がわかる。また、件名が「未承諾広告※です。」のようなメールもきちんとフィルタリングされている。また件名が「未承諾広告 ※」のフィルタリングされるべきメールが、フィルタリングされていない。また、フィルタリングされたメールの場合は、利用者のホームディレクトリにメール固有ID名でファイルが保存されていることを確認した。

8．システムの問題点と今後の課題

今回は5.3.の設計方針を満たすシステムの構築を行ない、5.2.の要求仕様を満たすシステムを構築することができた。

しかしながらいくつかの改良すべき点は存在する。システムの問題点と今後の課題について、以下で詳述する。

8.1. システムの問題点

8.1.1. 法律[2]を厳密に守った未承諾広告メール以外の未承諾広告メールへの対応

今回提案したシステムでは、実験4のように、件名の文頭が「未承諾広告※」と少しでも違った場合、そのメールに対してはフィルタリングを行なわない。このように実装した理由としては、法律[2]では、件名の文頭が「未承諾広告※」のもののみを未承諾広告メールと認識し、それ以外のものはたとえスペースや半角全角の違いがあろうと未承諾広告メールとはみなさない。そこで法[2]を犯しているものに対しては法的手段を取る事が出来るからということが理由となっている。

しかしながら実際問題として未承諾広告メールを送るものが、いちいちこの法律[2]を守っているかは疑問である。いくら法的に訴える事が出来ようと、その手間が面倒であることは明らかである。

8.1.2. 未承諾広告の条件(件名の文頭が未承諾広告※)を満たしている、普通のメールへの対応

今回提案したシステムでは、未承諾広告の条件(件名の文頭が未承諾広告※)を満たしているメールは全てフィルタリングしてしまっている。そのため、もし、「未承諾広告※についての報告」といった広告メールでないメールがあった場合、そのメールもフィルタリングの対象となる。この問題に対して現在は、バックアップを取るという手法で対応してはいるが、普通に送信されてこないという問題は、依然残る。

8.2. 今後の課題

今後の展開としては、まず、8.1.1.に対して、実験4の場合のような不法なメールに対しても柔軟に対応していけるシステムを実装する必要がある。

さらに、8.1.2.に対しては、利用者に「未承諾広告※」を件名の文頭に使用するとフィルタリング対象となる旨を伝える必要がある。

また、利用者の中にはこれらの未承諾広告メールを通常通り配信して欲しいという人がいる可能性もある。そこで利用者単位での対応ができる必要がある。

９．これまでの法整備

スパムメール、特に広告メールの一方的な送りつけが社会問題化していることから、経済産業省では「特定商取引に関する法律施行規則の一部を改正する省令」[6]を2002年1月10日付けで改正し、広告メールにおける表示に以下の事項を新たに義務付けた。

- 件名に「！広告！」と表示し、広告である旨を本文中でも明記する
- 事業者のメールアドレスの表示
- 受信者がメールの受け取りを希望しないときの連絡方法の表示、連絡方法の無い場合はその旨を本文中で明記し件名に「！連絡方法無！」と表示

2002年4月11日に「特定電子メールの送信の適正化等に関する法律」[2]、同12日に「特定商取引に関する法律の一部を改正する法律」[3]が成立した。総務省はその施行にあたっての細則[4]を省令で交付し、経済産業省はそれに合わせて先行している省令[6]を改正した[7]。

１０．通信事業者各社のスパムメール対策

10.1. 特定電子メール関連二法について

「特定電子メールの送信の適正化等に関する法律施行規則」[4]、「特定商取引に関する法律の一部を改正する法律施行規則」[7]により、特定電子メールに該当する広告メールは以下の事項を義務づけられることになる。

- 件名の文頭に「未承諾広告※」と表示する
- 本文に<送信者>という表示を設け、それとともに送信者の氏名または名称、住所、電話番号を記載する
- 受信拒否ができる旨と、受信拒否を連絡するためのメールアドレスを記載する
- 受信拒否の意志を示した相手への再度の送信の禁止

また、これを守らないメールへの対応を行う指定法人として[4]では日本データ通信協会を、[7]では日本産業協会を指定している。違法な特定電子メールの受信者にはこの2つの団体へ連絡することが求められている。これまで、受信者が特定電子メールの送信元に直接対応することや送信拒否の連絡をとることにはリスクが存在した。送信者が自動で作成したメールアドレスにスパムメールを送り付け、返信を

表2. 「迷惑メール」について通信事業者各社が公表しているポリシーの例[8~16]

事業者名	業種	ポリシー・声明の概要	苦情窓口
OCN	プロバイダ	迷惑メールの規定・禁止 自社契約者の迷惑メール行為への対応 他事業者の契約者に対しては 事業者への対応の要請も行う	不明
ODN	プロバイダ	自社契約者の迷惑メール行為への対応	有
ライブドア	プロバイダ	迷惑メール行為の対応	不明
NTT－ME	プロバイダ	迷惑メールの規定・禁止 自社契約者の迷惑メール行為への対応	有
インターリンク	プロバイダ	関連法規[2][3]の紹介 自社契約者の迷惑メール行為への対応	有
bit-drive	プロバイダ	迷惑メールの禁止とその理由の説明 自社契約者の迷惑メール行為への対応	有
MSN	プロバイダ	利用規約中で禁止 自社契約者の迷惑メール行為への対応	有
MSN Hotmail	メールサービス	同上 迷惑メール対策機能を設置	有
Yahoo!Japan	メールサービス	迷惑メール禁止のため 利用規約を補足する声明を公開 迷惑メール行為は利用規約に従い対応	有
freemail	メールサービス	悪質なスパムメールの手口の紹介 自社契約者の迷惑メール行為への対応	有

利用してメールアドレスの名簿を作成するといった悪質な行為を行っている可能性があったからである。今後は公的機関が悪質な業者への対応を受信者に代わって行うことになる。

また、総務省は上記の「未承諾広告※」という表記について、サーバ管理の面からは1バイト文字による表記が簡便であることを認めつつも、フィルタリングの効率よりも利用者にとっての一見したときのわかりやすさを優先したとしている[5]。

これらの点から、今回の法規制は先行した法律[6]に対し、よりエンドユーザ、特に初心者ユーザ向けに配慮したスパムメールへのポリシーを示したものと考えられる。

10.2. 現行法の抱える問題

これまで、特定電子メール関連二法を中心に述べてきたが、これらの法整備が十分というわけではなく、一部にはこれからも議論の余地がある。例としては、施行規則[4]において通信形態・文字コードが制限されていること、海外からの英文のスパムメールに対する不備、海外の規制（カリフォルニア州ボーウェン法では広告メールに「ADV」という件名への付記が行われている）との差をどうするか、といった件が挙げられる[6]。

また、メールセキュリティにおいて、受信者からメールの送信の承諾を得ることをオプトイン、承諾しないメールを送信停止できることをオプトアウトと呼ぶが、この定義においてどこまでをスパムメールに含めるかで見解が分かれている。

アメリカ合衆国ではオプトイン・オプトアウトを満たさない状況がスパムメールに当たると判断するのが一般的となっているが、EU ではオプトアウトを守っているメールについても未承諾で送られてくる最初のメールをスパムメールと判断する個人の権利の保護を重視したポリシーがとられている。今回の法規制では日本はオプトアウトのメールを認

めるポリシーを採択したが、この是非についても議論の余地がある。

10.3. 携帯電話でのメールサービスについて

携帯電話では、NTT ドコモに続き KDDI、ツーカーグループも利用者向けに「未承諾広告※」を件名に含むメールのフィルタリング機能の提供を発表しているが、NTT ドコモではこれに加えてインターネット経由で i モード宛てに送信されたメールのヘッダ情報を利用者の希望に応じて提供するサービスを 10 月 1 日より開始した。

このサービスは、「未承諾広告※」メールのフィルタリングと合わせることで、悪質なスパムメール送信者の摘発と今後の抑止に大きく役立つものと考えられる。

10.4. 通信事業者各社のポリシー

主な通信事業者各社について、各社ホームページ上で公開されている、いわゆる「迷惑メール」についてのポリシーを表 2 に示した。「迷惑メール」は、スパムメールのほかにも受信者に被害をあたえる電子メール（またそれを用いた行為）を指す言葉として現在広く使われているが、具体的に何が迷惑メールに該当するかの判断は各社・利用者間にまだ差があるようである。

各社の取り組みは様々であるが、基本的にはスパムメールに属するメールの類やメールによる他の利用者への迷惑行為を禁止し、利用者の被害への窓口を設け、悪質な利用者に対して措置を取れるように利用規約に従って対処する、などのポリシーが主流となっている。今回の法規制[1~3、6]に応じて、利用者に特定電子メールのフィルタリングサービスを利用者に宣伝している業者（ニフティ、インターリンクなど）もある。

通信事業者は利用者が直接対応する相手であるが、スパムメールに限らずともネットワーク上の問題にどのようなポリシーで対応するか難しい立場にある。提供しているサービスの利用を制限する措置は、しばしば通信という業務上個人のプライバシーや通信の守秘義務などに抵触する可能性がある。広告を行う業者も通信事業者にとって顧客の一部である。通信事業者側は、問題に対する社会的なコンセンサスが得られるまで一貫した対策をとることが出来ないことが多い。今回の法規制によって公的なメールポリシーの一端が示されたことになる。今後通信事業者各社がどのようなメール対策のポリシーをとり、スパムメールの問題に対応するべきかが今後の課題といえる。

11. 今後の電子メールの展望

適切な特定電子メールの送受信環境を成立させ、ひいてはスパムメールのリスクの減少のためには、今回の法規制への理解と遵守がユーザや社会に浸透し、オプトイン・オプトアウトのような電子メールの利用のモラルの原則も公共に認知される必要がある。同時に、今後ますます多様化していくであろうメールの利用形態を考え、公的機関・通信事業者・広告主・受信者を包括するメールセキュリティのポリシーをいずれは公的に成立させる必要がある。今回の法規制によって国はその一端を示したが、今後そのポリシーに基づいてどのようなセキュリティを社会に構築するかという点では、事業者・利用者も含めた議論によって公的な支持が得られる形を模索しなければならない。

12. おわりに

本課題では、インターネットセキュリティの具体例としてスパムメールの問題を取り上げた。スパムメールについての背景、実情を調査し、スパムメール対策のために提案するシステムの要求仕様を検討した。その際、広告メールフィルタ実現のために、今年の 7 月に施行された、特定電子メールの送信の適正化等に関する法律に着目し、設計を行った。要求仕様、及び設計方針に基づき、実際に、システムを構築し、広告メールのフィルタリングが正しく行われていることを確認している。さらに、法律施行後の状況、通信事業者各社の取り組みを通じて、提案システムの今後の課題、電子メール全般の展望についてまとめた。

参考文献

[1]「スパムメール被害実態調査結果」，E ジャパン協議会

[2] 特定電子メールの送信の適正化等に関する法律

[3] 特定商取引に関する法律の一部を改正する法律

[4] 特定電子メールの送信の適正化等に関する法律施行規則、総務省

[5] 特定電子メールの送信の適正化等に関する法律施行規則案に対する意見募集の結果、総務省

[6] 特定商取引に関する法律施行規則の一部を改正する省令、経済産業省
[7] 特定商取引に関する法律の一部を改正する法律施行規則、経済産業省
[8] 迷惑メールに対する OCN の対処について
http://www.ocn.ne.jp/rules/spam.html
[9] ODN サービス一覧：電子メールご利用にあたって
http://www.odn.ne.jp/infoodn/e_read.html#meiwaku
[10] 迷惑メールについて（livedoor）
http://www.livedoor.com/announce/mail001.html
[11] WAKWAK のメールサーバを使ったメールの利用について　WAKWAK の Web サーバの利用について
http://www.wakwak.com/info/new-service/rule1217.html
[12] 迷惑メールについてのお知らせ
http://www.interlink.or.jp/INFO/infolist.cgi?t=info&show=37
[13]「迷惑メール」の対応について
http://www.bit-drive.ne.jp/spam-policy.html
[14] MSN Web サイト使用条件と通知:マイクロソフト コーポレーションとお客様との間の契約書
http://privacy.msn.co.jp/tou/default.asp
[15] Yahoo!メール使用に関するガイドライン
http://www.yahoo.co.jp/docs/info/guidelines/mail.html
[16] freemail よくあるご質問と回答集：SPAM でお困りのユーザ様
http://www.freemail.ne.jp/spam.html
[17] Mulligan, Geoff 著, 宇夫陽次朗, 藤田充典 訳, “Spamの撃退：Sendmail, Procmailの設定とメールフィルタリング”, ピアソン・エデュケーション(1999)
[18] 森慎一, 塩谷幸治, 新川晃太郎, “BS 7799 照準 セキュリティポリシーの考え方”, 株式会社SCC(2001)