2004 年度 卒業論文

MTA における spam メール判別方法

提出日： 2005 年 2 月 2 日

指導：後藤滋樹教授

早稲田大学　理工学部情報学科
学籍番号： 1G01P060-4

高橋 真理

目次

図一覧

表一覧

第 1 章

はじめに

1.1 研究の背景

電子メールはインターネットにおいて最も普及しているサービスの 1 つであり、現在では通信手段として必要不可欠な存在になっている。一方、電子メールはセキュリティ上、最も問題を含んでいるサービスの 1 つでもある。

その中でも問題となっているのが、 spam メールという、見ず知らずの相手から一方的に送られてくる「詐欺まがいの儲け話」や「アダルトサイトへの誘導」、「違法なソフトウェアの販売」などの広告メールである。

spam メールが引き起こす問題としては、受信者への物理的・精神的負担、ネットワーク・サーバへの負荷などが主に挙げられる。 spam 受信者は本来なら必要のない処理に時間と資源を費やし、通信費を負担せねばならない。また、ネットワーク・サーバにおける無駄な処理も軽視できなくなってきている。

spam メールが拡大した原因は、インターネット上から容易に大量のメールアドレスを収集できること、アドレスを自動生成できるといったことや、発信者が少ない費用と負担で多くの対象にメールを送信できるということがある。

インターネットのメールシステムは、協同的な環境の中での協同的な環境を前提として構築されているため、 spam メールのみを規制するのは難しい。 1990 年にインターネットの商用化が始まってから、多くの人が spam 問題の解決に取り組んできたが、解決策は単体としては未だに見つかっていない。

1.2 研究の目的

法律による規制が厳しくなったとしても、 spam メールの存在自体がなくなるという可能性は低いであろう。それならば、いかに spam メールの被害を受けずにすませるかということが重要

となる。現在よく用いられている spam メール対策法は、メールのヘッダや本文から判別する方法、送信元アドレスから判別する方法などが主流となっている。特に前者のメール本文から判別する方法は、やり方によっては非常に高い精度で spam メール判別が可能である。しかしこの方法では、 spam メールの受信や判別のための解析によってネットワークにかなりの負荷がかかるため、今後 spam メールが急増することを考慮すると、必ずしも最良の方法とは言えない。一方、後者の送信元による判別は、ネットワークへの負担は減るものの、非 spam メールを受信拒否してしまうことが多々ある。

そこで本論文では、 spam メール自体をできるだけ受信せずに、それでいて非 spam メールを誤検出せずにすむ方法を検討する。上記の条件を満たすには、 1 つの手法のみで実現することは困難であると考え、複数の対策手法を用いることにした。本研究では、以下の 4 つの手法を使用することで spam メールを判別する。

- 送られてきたメールに一時エラーを返すことで、一旦再送を促し、その返信の挙動によって spam メールかどうかを判別する方法
- Postfix 2.1 の機能を利用して SMTP セッション中に判別する方法
- メールのヘッダの値によって判別する方法
- 逆引き FQDN によって判別する方法

1.3 本論文の構成

本論文は以下の章により構成される。

第 1章 はじめに

研究の背景と目的を述べる。

第 2章 spam メール

spam メールの定義と現状、本研究で独自に収集した spam メールのヘッダの解析結果を述べる。

第 3章 従来の対策法

spam メールの既存の主な対策法について述べる。

第 4章 実験概要

本研究で行った実験の内容を述べる。

第 5章 実験結果

第 4章で説明した実験の結果と評価を示す。

第 6章 まとめ

本論文をまとめる。

第 2 章

spam メール

2.1 spam メールの定義

spam メールの語源は、 Hormel Foods 社の味付け豚肉の缶詰の商品名とされている [1]。同社は大文字表記の「SPAM」を商標として登録しており、 spam メールのことは小文字で「spam」と表記するのが通常である。 spam メールの由来と概要については、 RFC2635 に記載されている。

spam メールの定義に関しては幅広い見解があり、共通の確固たる定義はないというのが現状である。まず、 Geoff Mulligan 氏の著書『spam の撃退』 [2] における spam メールの定義を下記に示す。

- 配送されることを望んだわけではないのに送られてくるメッセージ
- 非常に大きなメッセージ

しかしこれらの定義では、非 spam メールも spam メールと判別してしまう可能性がある。

そこで本論文では上記の条件をふまえて、以下のようなメールを spam メールと定めることにする。

- 不特定多数の相手に自動的に送りつけられる、広告・宣伝・勧誘・誘導・詐欺を目的とするメッセージ
- 受信者の意向を無視して送られてくるメッセージ
- コンピュータウイルスやワームの動作によって無差別に発信されるメッセージ

広義には電子掲示板にメッセージを書き散らす掲示板 spam、チャットやインスタントメッセージにメッセージを流して会話を妨害するチャット spam、 blog において無差別にコメントを書き

散らすコメント spam、無差別にトラックバックを行うトラックバック spam などもあるが、本論文ではこれらの spam については議論しないこととする。

なお最近では、電子メールの spam を「UBE (Unsolicited Bulk Email)」や「UCE (Unsolicited Commercial Email)」と表記することも増えてきている。また日本国内では、「迷惑メール」や「ジャンクメール」とも呼ばれるが、これは携帯電話の広告メールに用いられることがほとんどである。

2.2 spam メールの現状

セキュリティベンダーの日本国内初の調査 [3] [4] によると、インターネットユーザの 83.2 % が spam メールを受信したことがある。受信者の比率は、高い順に、 20 代男性が 92.9 %、 40 代男性が 91.1 %、 50 歳以上の女性層が 75.9 %など、 spam メールが年代や性別に関係なく無差別に送られていることも明らかになった。多数のインターメットメールユーザが spam メールを受信した経験を持ち、今なお被害を受けているのである。また spam メールを受信する割合は、平均で約 20 %であることが判明した。さらに 50 %前後受信する割合は 13 %に達しており、頻度の面でも深刻な状況を示している。

日本国内でさえ上記のような被害を受けているが、世界の spam メールの約 60 %が米国を発信源としているため、米国では日本以上に問題が深刻であり、さらなる被害が予想される。米 FrontBridge 社によると、同社が 2004 年 10 月に受信した電子メールのうち、 spam メールの割合は約 87 %を占めた [5]。他にも米 Postini 社の調査では、 2004 年 9 月に受信したメールのうち、 spam メールは約 75 %であった [5]。このような被害状況を受け、米国では spam メールを規制する連邦法が施行された。日本においても、携帯電話のインターネットサービスで迷惑メールが問題となり、それを規制する法律が制定された。

spam メールの被害はこれからも増加が予想されており、個人間の電子メールに加え、 spam メールや通知メールの増加によって、世界全体の 1 日当たりの電子メール数は 2006 年には 600 億通へと増加し、しかもその半数近くが spam メールであると予測されている [6]。また地域別に見ると、図 2.1 のように増加していくと見込まれている [7]。グラフ中の数値は、 spam メールの増加率を表す。

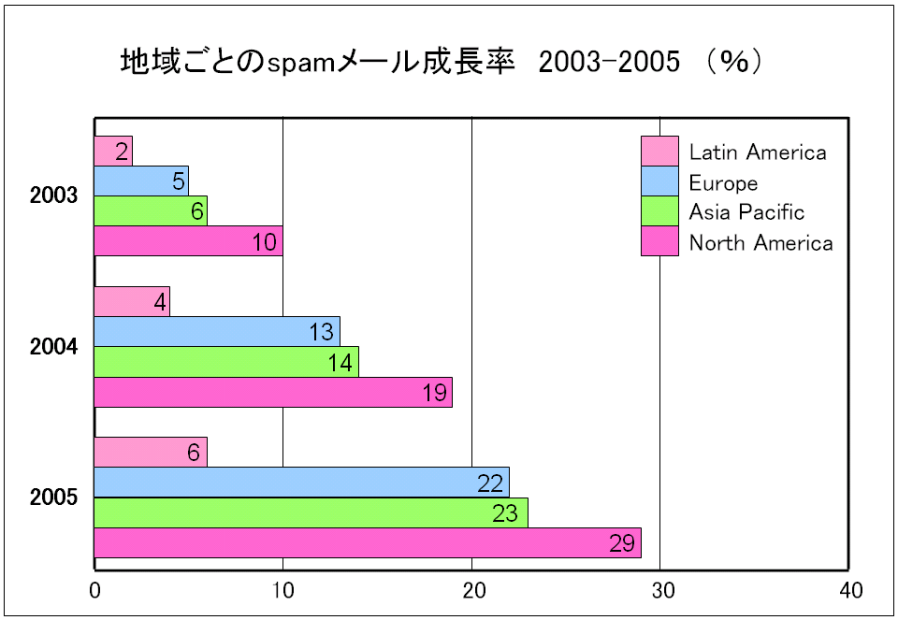

図 2.1: 地域ごとの spam メール成長率 (2003 - 2005)

このように増え続ける spam メールの被害影響としてユーザが懸念していることは「ウイルスの感染」であり、それは全体の 7 割にも達する。また「業務の生産性・効率の低下」、「サーバ・ネットワークへの負荷」、「プライバシー・機密情報の漏洩」などもそれぞれ約 5 割と、これらもかなり高い値となっている。

spam メールによって引き起こされる実際の問題は、以下の 3 つである。

- メールの受信や処理による無駄な時間、接続料金、資源、精神的ストレス
- 回線やサーバの資源の浪費
- Third-Party Mail Relay（spam メール送信の踏み台にされること：不正中継）による資源の浪費、業務の遅延、信頼の低下

以上のような spam メールのによる被害が深刻化しているにもかかわらず、spam メール対策はあまり進んではいないのが実情である。「何も対策していない」ユーザの割合は 29 %、「手動で削除している」割合は 52 %と消極的な対応が主である。また、企業・団体においてもシステム的に spam メール対策を実施し、spam 対策ツールを導入しているのは全体の 12 %にとどまり、未だ少数派であることが判明している。

2.3 spam メールのヘッダ解析

電子メールには、通常ヘッダ情報が付加されている。ここには、メールの送受信に不可欠な情報や重要なデータが書き込まれている。

下記に主なヘッダを示す。「必須」とあるのは、メールの送信に常に必要となるヘッダである。また「X-」で始まるものは、特に決まりはなく、メールソフト、サーバ、送信者などがつけるヘッダである。中には習慣的なものや遊び心でつけたものもある。

Received: メールがメールサーバに到着するまでに通った経路

Date: メールが完成した時間（必須）

From: メールを書いた本人、文責者（必須）

Subject: メールの件名

Sender: メールの送信者（From: に複数のアドレスがある場合は必須）

To: メールの主たる受信者

Cc: 主な受信者以外のメール受信者

Message-ID メール識別子

Reply-To: 返信先のメールアドレス

MIME-Version: 対応している MIME のバージョン

Content-Type: メール本文の種類

Content-Transfer-Encoding: 使用したエンコードの方法

X-Mailer: 送信者が送信に利用したメーラー

X-MimeOLE: OutlookExpress が独自に挿入するヘッダ

X-Priority: 重要度を示すヘッダフィールド

X-MSMail-Priority: OutlookExpress 独自のメール重要度

X-IP: メール送信元 IP アドレス

X-Originating-IP: メール生成元 IP アドレス (hotmail)

X-Sender-IP: メール送信元 IP アドレス (Excitemail)

X-UIDL: ローカルメールボックス内のメール識別子

ヘッダ情報は上記のものだけでなく、他にも数多くの種類のヘッダが存在している。ヘッダ情報に基づいて spam メールをフィルタリングする手法は、最も一般的で、古くからある方法の 1 つである。

本論文では上に挙げたヘッダのうち、以下の 8 つの解析結果を示す。

- Content-Type
- charset （これは Content-Type 内に含まれる）
- Content-Transfer-Encoding
- X-Priority
- X-MSMail-Priority
- X-Mailer
- X-MimeOLE
- X-IP (X-Originating-IP)

本研究の対象となるメールについて述べる。 2004 年 9 月から 11 月までの 3ヶ月間で受信したメール数は 10866 通、非 spam メールは 10383 通であった。この中から、 spam メールと非 spam メールをそれぞれ 3000 通ずつランダムに選び、ヘッダの解析を行った。

得られた結果から、 spam メール判別に役立ちそうな spam メールの特徴を以下に述べる。

2.3.1 spam メールに圧倒的に多く見られる特徴

- Content-Type が「multipart/xxxx」のもので、パートの区切りが所定の書式でないもの
- Content-Transfer-Encoding が「8bit」、「quoted-printable」のもの
- 日本語のメールなのに「quoted-printable」でエンコードしているもの
- X-Mailer が「Microsoft Outlook Express」なのに、 Priority, X-MSMail-Priority, X-Mime OLE がないもの
- hotmail を利用しているのに、 X-Originating-IP ヘッダがないもの
- X-IP ヘッダがあるもの

2.3.2 spam メールに比較的多く見られる特徴

- Content-Type が「text/html」のもの
- charset がないもの
- charset が「Windows-1251」、「Windows-1252」、「iso-8859-1」、「koi8-r」、「GB2312」、「eur-kr」であるもの
- X-Mailer がないもの
- X-Mime OLE に「Microsoft」という文字列を含まないもの

2.3.3 spam メールにはほとんど見られない特徴

- charset が「iso-2022-jp」のもの
- Content-Transfer-Encodig が「7bit」のもの

第 3 章

従来の spam 対策法

spam メールの対策には様々な手法が考えられており、多くの人が自分に合った方法を用いて spam メールを排除しようとしている。まだ決定的な方法というものは存在していない。以下に現存する主な spam メール対策方法を述べる [8] [9]。

3.1 技術的な対策

3.1.1 メール内容による判別

ユーザに合わせた柔軟な処理が可能であり、学習機能があればより細かい要求に応えることができる。しかし、 spam メールを受け取った後に判別するため、トラフィックが減ることは期待できない上、未知のメールには基本的に対応できない。

- **構造化テキストフィルタ**
  指定したヘッダ、本文に含まれる単純な文字列で、受信メールを分類するフィルタ手法。非常に単純なもので、正規表現による一致などの高機能は利用できないが、ほとんどすべての電子メールクライアントがこの機能を備えている。

- **ルールベースフィルタ**
  ヘッダや本文などにおける spam メールと非 spam メールを判別できる特徴を、あらかじめルールとして記述しておき、ルールに合致した分の合計スコアが一定値以上の場合に spam メールと判別する方法。最も人気が高く、代表的なツールとして SpamAssassin が有名である。典型的な spam メールの検出率は非常に高いが、新しい手口を用いた未知の spam メールに対してはルールを作成するまで対応できない。また、 spam メールと似ている非 spam メールを誤検出してしまうということもあり得る。

- **コンテンツベースフィルタ**
  メール本文内の字句情報を学習させることによって判別する方法。既知のメールからサン

プルを収集して、 spam 指標確率を生成し、それによって受信したメールが spam メールかどうかを判別する統計学的な手法である。ベイジアンや K-Nearest-Neighbor 法などのアルゴリズムがある。ルールベースフィルタと似ているが、実際はルールベースフィルタ以上の性能を示す上、 Graham スタイルのベイズフィルタは単純で高速であると言われている。ただ、 spam メールの字句情報を常に学習させ続けなければならないということや、送信側が本文に無関係の単語や文章を挿入したりすると、フィルタリングを通過してしまうという欠点もある [10] [11]。

3.1.2 通信セッションによる判別

この方法は、セッションを遮断することでトラフィックの減少が期待できる。ただし非 spam メールまで排除してしまう可能性がある。

- **ホワイトリスト**
  あらかじめリストに登録され、明示的に承認された送信者からのメールのみを受信する方法。限られた相手からのメールしか受信できず、リストにない送信者のメールは受信できないため、条件が厳しすぎて、ごく小規模でしか利用できない。

- **ブラックリスト**
  あらかじめリストに登録されている送信者からのメールを必ず拒否する方法。ホワイトリストよりは実用的であるが、拒否する条件が緩すぎるため、あまり効果的ではない。

- **分散協調型ブラックリスト**
  ユーザ間で spam メールデータベースを共有し、このデータベースへの登録の有無によって spam メールかどうかを判別する方法。一人のユーザが削除ボタンを押すと、他の何百万人ものユーザに、そのメッセージが spam メールであることを警告として知らせることができる。同一内容のメッセージが多数のユーザに送信されるという、 spam メールの性質を利用した方法である。 Razor, Pyzore, DCC などのツールが有名である。判別時までに他のユーザがデータベースに登録しないと検出できないため、検出率は比較的低いが、他の手法では見逃してしまう spam メールにも適応でき、誤検出の割合も無視できるほど小さいのが特徴である [12]。

- **チャレンジーレスポンス**
  送信者にコストを課し、それを支払った送信者のメールのみを受信する方法。ホワイトリストに含まれている送信者からのメールのみを受信し、それ以外のメッセージの場合は、リストに登録するために返信を要求する指示（チャレンジ）が送信者に返信される。 spam メール送信者がこの呼びかけに応答することはまずないと言ってよい。正当な送信者が呼

びかけに応えた場合は、ホワイトリストに登録され（レスポンス）、以降は自動的にフィルタを通過可能となる。この方法は spam メールをかなり高い確率で防ぐことができるが、正当な送信者に負担をかける上、呼びかけに応え損なった非 spam メールを破棄してしまうことが多かったり、自動応答システムに対応していないなど、問題も多い [13] [14]。

3.1.3 その他

- **メールアドレス型**
  使い捨てメールアドレスや、条件付きメールアドレスを使用する方法。有効期限によって短期間にアドレスが変更されたり、暗号化した ID からのアドレスを生成したりすることで、メールアドレス自体を覚えられなくしてしまうので非常に有効である。しかし、正当なメールのやりとりに利用するのは不便であるため、利用範囲は限られてしまう [15]。

3.2 法律面の対策

spam メール防止に関する法律の制定は、ラベル付け強制案と全面禁止案の 2 つの方向で進められてきた。ラベル付け強制案では、フィルタリングに利用できるラベル（文字列など）がメッセージに含まれている限りは、無制限に spam メールが許可される。これは事実上 spam メールを合法化するものであり、対策手段を持たない spam 受信者に負担を強いている。それに対して、全面禁止案は spam メールを違法にしようというものである [16]。

日本においては、特定電子メール（個人に対し、営利を目的とする団体及び個人が、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する電子メール）の送信の適正化等に関する法律 [17] や、特定商取引に関する法律 [18] などによって、 spam メールの送信方法に対する以下のような規制が行われている。

- 送信拒否の通知をしたものに対して、送信者が特定電子メールの送信をすることの禁止（オプトアウト）
- 商品やサービスの販売を目的とした広告である場合は、広義の通信販売と見なし、取扱業者の所在などの連絡先を明示しなければならない
- 表示義務

  Subject: 欄

  「未承諾広告※」から始まる文字列。また、「未承諾広告※」を表示するためにエンコードした際の文字コードは、本文のそれと同じでなければならない。「未承諾広告

※」、「未__承__諾__広__告※」、「未承言若廣告米」などの表示はすべて違法である。

From: 欄

送信に用いたアドレス。

通信文の最前部

〈事業者〉、〈送信者〉を記載

氏名または名称（事業者と送信者が別の場合は、それぞれ要記載）

再送拒否用のアドレス

再送拒否が可能で、以降の宣伝送信が停止される旨

メール内の任意の場所

経路情報（ヘッダ）

宣伝者または送信者のアドレス

宣伝者または送信者の代表者か責任者の氏名（法人の場合）

メール中またはメール本文に記載された URI 上のページ

送信者の住所

送信者の電話番号

このような法律が定められているものの、 spam メール送信そのものに対する規制が不十分であるため、問題も多い。

一方米国では、電子メールだけでなく、郵便を利用したダイレクトメールや電話勧誘販売に対するオプトアウト登録システムが国によって始められており、電子メールでは、メールサーバに多大な負荷をかけるような spam メール送信者への罰則強化が進められている。

2004 年 1 月 1 日に施行された、米国初の spam メール規制法「CAN-SPAM 法（Controlling the Assault of Non-Solicited Pornography and Marketing Act）」 [19] は、商業的な電子メールの送信者に対し、広告主の住所をメッセージに含めること、商用メールである旨を「はっきりと目立つところに」記載すること、受信者に今後の送信を希望しないという選択肢を提供することを義務づけている。ヘッダの改ざんや詐欺的な内容の記述なども罰せられる。また、公的機関が作成する「Do-Not-Spam」リストに記載されたアドレスには、許諾を得ずに広告メールを送ってはならない。しかし、規制の対象となるのは企業だけで、政治団体や宗教団体、非営利団体が送信する広告メールは規制されない。そして、事前に許諾を得た相手にのみ広告メールの送信が許される「オプトイン」方式ではなく、受信者が受け取り拒否の意志を示すことにより以後の送信

を差し止める「オプトアウト」方式を採用している。このような規制はあるものの、詐欺的でない広告メールを一方的に送付されても受信者が業者を訴える権利は認められていない。

州法レベルではもっと厳しい規制を課す法律も制定されているが、 CAN-SPAM 法は州法に優先するため、州法の規制が無効になってしまうという問題がある。特にカルフォルニア州などは非常に厳格なアンチ spam 法を敷いており、一般的なメールマーケティング事業すら立場が危うくなっていたため、メールマーケティング関連各社は CAN-SPAM 法の施行を歓迎している状況である [20]。

今後は、米国を拠点としている spam 業者の多くが、連邦法の及ばない国外に業務を移すこともありうるため、 spam メールに対する国境を越えた解決策を検討する必要がある。

第 4 章

実験の概要

4.1 Greylisting による判別

spam メールを送信するメールサーバは、特定の個人に確実にメールを送ることよりも、大量のメールを短時間に送信することを重視するため、送信先のメールサーバの一時エラーに対しては、おそらく再送処理を行わないと考えられる。また、spam メール送信者は open proxy を利用することが多いが、この open proxy なクライアントを次々と踏み台を替えて再送することはあるものの、再接続してくることは少ない。一方 MTA (Message Transfer Agent) は、一時拒否されても一定期間は再送処理を行おうとする。この特徴を利用して、一定時間が経過するまで一時拒否（SMTP 一時エラーコード「4xx」応答）して、それでも接続してきたら、spam メール送信者ではないとみなして、メッセージを受け取ることにする。SMTP (RFC2821, RFC821, RFC1123) [21] [22] [23] を守るサーバは、30 分以上待ってから再送信するはずであり、5 分以内に再接続してくるものは spam メールの可能性が非常に高い。

以下に Greylisting [24] による判別の一連の流れを示す。

1. 接続を記録するためのデータベースを用意する。
2. クライアントの IP アドレスと envelope-from（送信者メールアドレス）と envelope-to（受信者メールアドレス）を一組の triplet（組み合わせ）とする。
3. 接続してきたクライアントの triplet がデータベースにない場合は、triplet と接続の時間をデータベースに記録する。そして本文を受け取る前に、一時拒否（SMTP エラーコード「4xx」応答）し、再送を要求する。
4. データベースに、接続してきたクライアントの triplet があれば、現在の時間と triplet の時間を比較して、一定時間経過していなければ一時拒否し、再送を要求する。すぐに再送されたメールは spam メールの可能性が高いからである。通常は 15 分から 1 時間後に再送されるので、データベースに記憶していた triplet を照合して、再送メールであれば受信する。

5. 一定時間が経過していれば受信する。さらに判別できる条件があればその判別を元に受け取るか拒否（「4xx」もしくは「5xx」）する。

本論文では、再送受付時間を 8 分、 greylist 状態の時間切れと autowhite 状態の時間切れを 3 日とした。

以下に Greylisting の時間的な流れを図 4.1 に示す [25]。

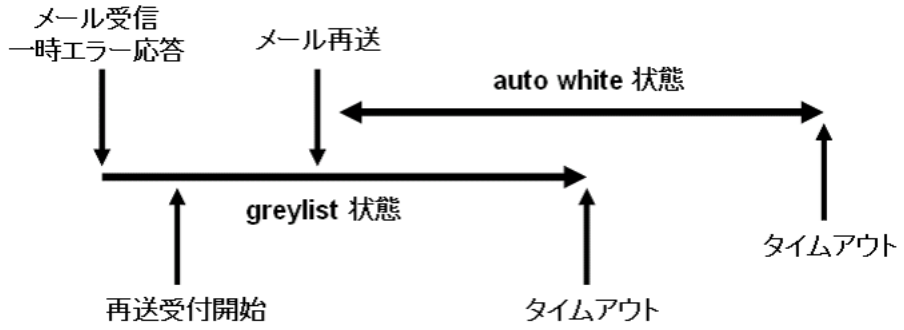

図 4.1: Greylisting の時間的な流れ

open proxy 経由の（MTA 経由でない） spam メールはこの方法で十分対応可能である。この制限を回避するには、同じ IP アドレスから、同じ envelope-from で、同じ envelope-to のメッセージを一定時間後に再送するしかない。その間に、 open proxy をリストする DNSBL などのブラックリストに登録されてしまえばさらに容易に拒否できる。しかも spam 送信者は envelope-from や踏み台にする open proxy を次々と替えて接続するので、この方法は有効である。

今後は open proxy も一定時間後に再接続するようになるかもしれないが、時間が経つほど DNSBL などに登録されてしまう確率が高くなり、配送コストも高くなるので、そのように変化しても問題はないと言える。

問題は MTA を経由して配送される spam メールである。 MTA は一時拒否されても一定期間は再配送しようとする。そのため MTA 経由の spam メールには効果がない。しかし、 open relay な MTA や、自分で運用している MTA を使って spam メールを配送するのは、あまり賢い方法とは言えない。既にそういった IP アドレス範囲や spam メールに甘い ISP は DNSBL などに登録され、拒否できるからである。 ISP の MTA を使用するのも足がつきやすいので、継続的な spam メールの配送には向いていない。

Greylisting による判別では、ウイルスやワームの拡散もある程度防ぐことができる。それはウイルスやワームの配送方法が open proxy を利用した spam メールの配送方法とそっくりだからである。

この方法の問題点は、一時拒否されると IP アドレス（ホスト）を次々と替えて再接続してくる MTA があるので、これをホワイトリストに登録するなどの対策が必要ということがある。な

お、メーリングリストなどの MTA を Greylisting の判別の対象とするのは意味がないので、こういったホストもホワイトリストに入れるべきである。

他にもこの判別方法の大きな問題として、メールの遅延がある。メールのやりとりが遅延しては困る相手の場合は、ホワイトリストを整備しなければならない。

本論文では、 Greylisting を利用するにあたって、 Postfix 用の実装である Postgrey を用いた [26]。

4.2 SMTP セッションによる判別

Postfix は、安全で、より簡単で、パフォーマンスが高い MTA を作るという目的で開発され、設計の初期からセキュリティを考慮して開発されてきた。その最新バージョンである Postfix 2.1 は 2004 年 4 月にリリースされたが、今まで以上に不正中継対策をはじめとするセキュリティに力を入れた内容になっており、例えば、 SMTPD アクセスポリシー [27] という機能が使えるようになり、外部のポリシーサーバによって、接続の許可などを行わせることができるようになっている。

MTA での spam メール対策として、配送プロセス中における spam メールの判別と排除を行うことにする。

Postfix は、次の 3 つのいずれかの段階で spam メールを判別する。

- SMTP 接続時点
- SMTP コマンドが入力された時点
- 配送メッセージを受け取った後

サーバのリソース消費は、 SMTP 接続の初期であればあるほど少なくてすむ。

以下の図 4.2 に、メッセージの配送プロセスと、 spam メール対策に関連するパラメータを示す [28]。

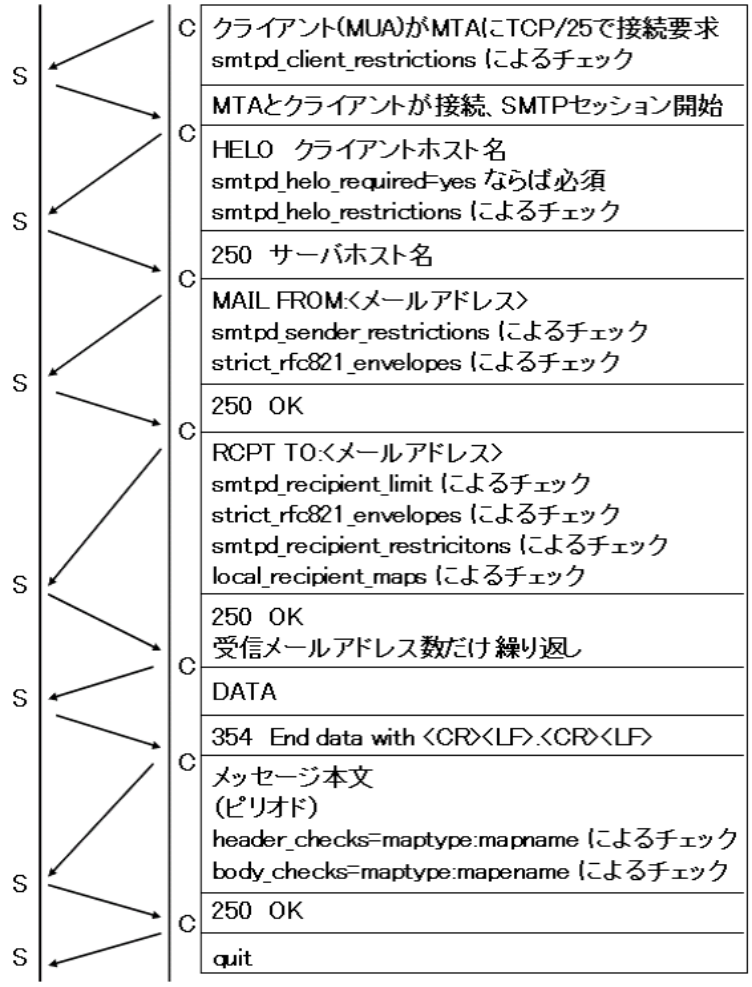

図 4.2: SMTP の流れと spam メール関連パラメータ

主な設定を以下に示す。（main.cf 内）

```
# デフォルトは yes。 RCPT コマンドまで待たずに制限の効果を出す。
smtpd_delay_reject = no

# 送信者のメールアドレスがそのホストで扱うドメインで、アドレスがそのホストで有効でない場合は拒否する。 Postfix 2.1 から利用可。
reject_unlisted_sender = yes

# SMTP の VRFY コマンドを使用不可にする。
disable_vrfy_command = yes

# 不正中継対策。この 2 つを「no」と指定すると、すべて転送拒否してしまう。
```

```
allow_percent_hack = yes
swap_bangpath = yes

# SMTP の ETRN コマンドの使用をホスト名が不正なホストには使用不可とする。
smtpd_etrn_restrictions  =
    permit_mynetworks,
    reject_invalid_hostname

# 自分のネットワークからの接続を無条件で許可し、 IP アドレスからホスト名への逆引きができないホストの接続を拒否。

# RBL ホスト、 RHSBL ホストの指定
# http://www.ordb.org, http://www.mail-abuse.com, http://dsbl.org/,
# http://www.shub-inter.net/index.shtml, http//www.dnsbl.au.sorbs.net/,
# http://www.ahbl.org/, http://www.five-ten-sg.com/,
# http://www.spamhaus.org/SBL/, http://www.spamhaus.org/SBL/,
# http://blacklist.jippg.org/, http://www.shub-inter.net/index.shtml
smtpd_client_restrictions =
    permit_mynetworks,
    permit_mx_backup,
    reject_rbl_client relays.ordb.org,
    reject_rbl_client relays.mail-abuse.org,
    reject_rbl_client list.dsbl.org,
    reject_rbl_client spamips.shub-inter.net,
    reject_rbl_client dnsbl.sorbs.net,
    reject_rbl_client dns.ahbl.org,
    reject_rbl_client blackholes.five-ten-sg.com,
    reject_rbl_client sbl.spamhaus.org,
    reject_rbl_client xbl.spamhaus.org,
    reject_rbl_client mail-abuse.org,
    reject_rhsbl_client relays.mail-abuse.org,
    reject_non_fqdn_sender,
    reject_non_fqdn_recipient,
```

```
    reject_unauth_pipelining,
    reject_unknown_sender_domain,
    reject_unknown_recipient_domain,
    reject_unknown_client,
    permit

# HELO コマンドで, ホスト名を通知しないホストの接続を拒否。
smtpd_helo_required = yes

# 正しい書式でホスト名を通知してきたホストのみ接続を許可。
smtpd_helo_restrictions =
    permit_mynetworks,
    reject_invalid_hostname,
    reject_unknown_client,
    permit

# 実際には存在しないドメイン名が送信元メールアドレスに使われているメールを拒否。
smtpd_sender_restirictions =
    permit_mynetworks,
    permit_mx_backup,
    reject_non_fqdn_sender,
    reject_non_fqdn_hostname,
    reject_sender_login_mismatch,
    reject_unlisted_sender,
    reject_unknown_sender_domain,
    reject_rhsbl_sender relays.mail-abuse.org,
    reject_rhsbl_sender spamips.shub-inter.net,
    warn_if_reject reject_unverified_sender,
    permit

# RFC821 で定義されている書式に適合しないメールアドレスが通知された場合、受信を拒否
する。
strict_rfc821_envelopes = yes
```

```
# デフォルト = 1000。配送ごとにいくつの宛先をとるかを制御する。大規模サーバの場合は大きめに設定する。
smtpd_recipient_limit = 1000

# ホスト名と転送先ドメインとして許可されているドメインが、宛先メールアドレスに指定されているものを受信。
smtpd_recipient_restrictions =
    permit_mynetworks,
    reject_non_fqdn_recipient,
    regexp:/etc/postfix/recipient_checks.reg,
    check_client_access hash:/etc/postfix/reject_ip,
    check_client_access hash:/etc/postfix/reject_sender,
    reject_sender_login_mismatch,
    reject_unknown_recipient_domain,
    reject_unverified_recipient,
    reject_unauth_destination,
    check_policy_service unix:private/policy

# SMTP 受付時にユーザテーブルを検索して、存在しないメールアドレスが RCPT TO に指定されると、 550 でエラーを返すのがデフォルトの仕様。
local_recipient_maps
```

4.3 ヘッダチェックによる判別

2 章で述べた spam メールの解析結果に基づいて、特定のヘッダの有無によってポイントを加算し、spam メールの判別を行う。

判別に用いるヘッダと、そのポイントは以下の通りである。

```
Content-Type:       ⇒ multipart/xxxx（パートの区切りがおかしい）: 10
                    ⇒ text/html : 5
charset:            ⇒ なし: 5
                    ⇒ Windows-1251, Windows-1252, iso-8859, koi8-r, GB2312,
                       eur-kr : 5
                    ⇒ iso-2022-j : -5
X-Priority:         ⇒ なし（X-Mailer : Microsoft Outlook Express の場合）: 10
X-MSMail-Priority:  ⇒ なし（X-Mailer : Microsoft Outlook Express の場合）: 10
X-Mailer:           ⇒ 乱数、ランダムで意味のない文字列: 10
X-MimeOLE:          ⇒ なし（X-Mailer : Microsoft Outlook Express の場合）: 10
                    ⇒ 「Microsoft」という文字列を含まない: 5
X-IP:               ⇒ あり: 10
X-Originating-IP:   ⇒ なし（hotmail の場合）: 10
```

これらの合計ポイントが 20 点以上の場合は、そのメッセージを spam メールと判別し、受信を拒否する。

上記の判別は、ローカルホスト上にある外部プログラムを pipe で呼び出して行う。これは、Postfix からの出力を pipe を通して受け取って処理するもので、フィルタ済みのメッセージは sendmail コマンドで Postfix に戻されるという仕組みである。外部プログラムを呼び出す流れを図 4.3 に示す [28]。また Postfix の構造の全体図を図 4.4 に示す [28]。

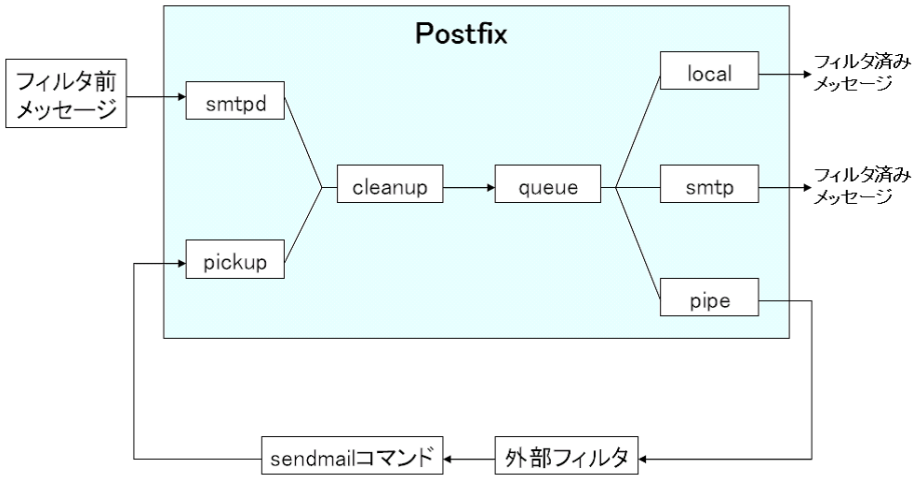

図 4.3: 外部プログラムを呼び出す仕組み

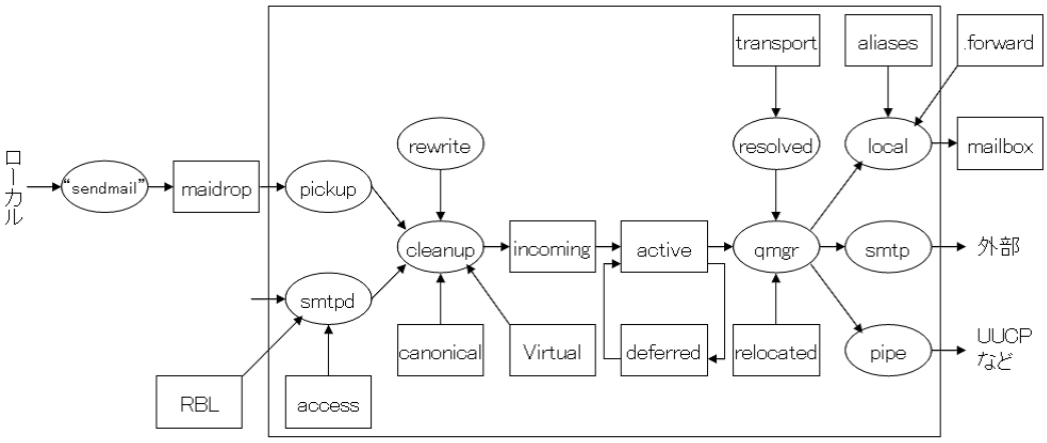

図 4.4: Postfix の構造

4.4 FQDN チェックによる判別

メール中継サーバからの SMTP アクセスのみを受け付け、エンドユーザからの直接の SMTP アクセスを拒絶することで、 spam メールを受信せずにすませる方法。

メッセージを受け取る前にこの判別を行うので、メールトラフィックを減らすことができる。また、ドメインを偽の送信者アドレスに悪用されてしまった被害者に殺到する不正な返信もなくすことができる。

正当なメールは ISP や組織のメール中継サーバを経由し、 spam メールはエンドユーザ用回線につながったコンピュータから直接送られてくることが多い。また、正当なメール中継サーバは逆引き FQDN (Fully Qualified Domain Name) を持ち、逆引き FQDN のない IP アドレスはダイヤルアップ、 ADSL、ケーブルネットワークなどのエンドユーザ用回線に使われることが多い。

この特徴を利用して、 FQDN を見ることで、 SMTP アクセスしてきたクライアントがメール中継サーバかエンドユーザのコンピュータかを判別できる。

そして逆引き FQDN のない IP アドレスからの SMTP アクセスを、一部の例外を除いて拒絶する。

逆引き FQDN のない IP アドレスはエンドユーザ用回線に使われることが多い、と述べたが、エンドユーザ用回線の IP アドレスにも逆引き FQDN を持つものは多い。しかし、その逆引き FQDN にはメール中継サーバとは違った特徴がある。エンドユーザ用回線の逆引き FQDN は、多くの IP アドレスへの名前割り当てを行うため、比較的多くの数字を含むことが多い。一方、メール中継サーバの場合は、管理者が覚えやすい名前を好むので、通常は数字をあまり含まない。よって、正規表現を用いることで、エンドユーザ用回線と推定される IP アドレスからの SMTP アクセスは幾つかの例外を除いて拒絶することができるのである。

以下に FQDN チェックを行うにあたっての一般規則と、その判別を行うのに必要な記述を示す [29]。

4.4.1 一般規則

`# main.cf` に以下を追加する。

```
smtpd_client_restrictions =
  check_client_access regexp:/etc/postfix/client_restrictions
```

`# /etc/postfix/client_restrictions` に以下の規則を追加する。

1. **逆引き失敗**

   IP アドレスから FQDN を検索できない。逆引き FQDN の順引きの結果が、元の IP アドレスに一致しない。

2. **逆引き FQDN の最下位（左端）が、数字以外の文字列で分断された 2 つの数字列を含む**

   エンドユーザ用回線の FQDN には、この規則に合致するものが最も多い。

   例： 220-139-165-188.dynamic.hinet.net a12a190.neo.rr.com

   ⇒ `/^[^\.]*[0-9][^0-9\.]+[0-9]/ 450 may not be mail exchanger`

3. **逆引き FQDN の最下位の名前が、 5 個以上連続する数字を含む**

   例： YahooBB220030220074.bbtec.net

   ⇒ `/^[^\.]*[0-9]{5}/` `450 may not be mail exchanger`

4. **逆引き FQDN の上位 3 階層を除き、最下位または下位から 2 番目の名前が数字で始まる**

   例： 398pkj.cm.chello.no

   host.101.169.23.62.rev.coltfrance.com

   ⇒ `/^[^\.]+\.)?[0-9][^\.]*\.[^\.]+\..+\.[a-z]/` `450 may not be mail exchanger`

5. **逆引き FQDN の最下位の名前が数字で終わり、かつ下位から 2 番目の名前が 1 個のハイフンで分断された 2 つの数字列を含む**

   例： wbar9.chi1-4-11-085-222.dsl-version.net

   ⇒ `/^[^\.]*[0-9]\.[^\.]*[0-9]-[0-9]/` `450 may not be mail exchanger`

6. **逆引き FQDN が 5 階層以上で、下位 2 階層の名前がともに数字で終わる**

   例： m500.union01.nj.comcast.net

   ⇒ `/^[^\.]*[0-9]\.[^\.]*[0-9]\.[^\.]+\..+\./` `450 may not be mail exchanger`

7. **逆引き FQDN の最下位の名前が「dhcp」、「dialup」、「ppp」または「adsl」で始まり、かつ数字を含む**

   例： dhcp0339.vpm.resnet.group.upenn.edu

   adsl-1415.camtel.net

   ⇒ `/^(dhcp|dialup|ppp|adsl)[^\.]*[0-9]/` `450 may not be mail exchanger`

メールサーバがこれらの規則によって SMTP アクセスを拒絶するときは、応答コード「450（再試行要求）」を返すとよい。それにより、いずれかの規則に合致する正当なメール中継サーバをホワイトリストに登録し、救済できるからである。

4.4.2 ブラックリスト

前述のルールをすり抜けるエンドユーザ用回線の拒絶に用いる。具体的には以下のような特徴がある。

- 末端ホスト名が 16 進番号を含む
- 末端ホスト名が番号を表す英字を含む
- メール中継サーバであるかのような FQDN である
- ドメインを代表するメールサーバが spam メールを送信する

4.4.3 ホワイトリスト

一般規則やブラックリストに引っかかる正当なメール中継サーバを救済するために用いる。具体的には以下のような特徴がある。

- 逆引き失敗
- 逆引き FQDN が複数の IP アドレスに対応している
- ホスト名が一般規則に合致する
- エンドユーザ用回線を利用している

第 5 章

実験結果

5.1 実験環境

表 5.1に本研究で用いた実験環境を示す。

表 5.1: 実験環境

CPU	モバイル Pentium 3 750MHz
Memory	512MB
OS	FreeBSD 4.10
Software	Postfix 2.1.5 Postgrey 1.16

5.2 評価

第 4 章で述べた 4 種類の判別方法に基づき、実験を行った。それぞれを単独で判別した場合と、複数の方法を組み合わせた場合との結果を比較する。実験はそれぞれの方法を一週間ずつ行った。

判定方法の組み合わせは、以下の 15 通りである。

- Greylisting
- SMTP セッション
- ヘッダチェック
- FQDN チェック

- Greylisting + SMTP セッション
- Greylisting + ヘッダチェック
- Greylisting + FQDN チェック
- SMTP セッション + ヘッダチェック
- SMTP セッション + FQDN チェック
- ヘッダチェック + FQDN チェック
- Greylisting + SMTP セッション + ヘッダチェック
- Greylisting + SMTP セッション + FQDN チェック
- Greylisting + ヘッダチェック + FQDN チェック
- SMTP セッション + ヘッダチェック + FQDN チェック
- Greylisting + SMTP セッション + ヘッダチェック + FQDN チェック

複数の手法を用いても、排除するための条件が and になるので、排除率自体は上がるわけではない。例えば、 Greylisting と FQDN チェックの 2 つを組み合わせたとすると、それぞれの排除率が掛けあわされた値に下がってしまう。つまり、複数の方法を組み合わせるのは駆除率を上げるのではなく、フィルタリングによる悪影響を最小限にするため、また、誤検出を減らすための工夫ということになる。

判別結果は以下の表と図のようになった。（図表において Greylisting : G, SMTP セッション: S, ヘッダチェック: H, FQDN チェック: F と略すこととする。）

表 5.2: 実験結果（メール数）

	spam 数	非 spam 数	受信数合計	spam 排除数	誤検出数
Greylisting	7401	5664	13065	7038	350
SMTP セッション	7812	6308	14120	6670	399
ヘッダチェック	8686	6078	14764	6928	344
FQDN チェック	7420	6489	13909	7308	268
G + S	7244	5755	12999	5913	232
G + H	8202	5166	13368	6256	228
G + F	8094	5329	13423	7461	169
S + H	7230	6273	13503	5474	233
S + F	759	6262	14021	6288	192
H + F	7368	6194	13562	5742	138
G + S + H	6851	5608	12459	5195	201
G + S + F	7205	5546	12751	5813	88
G + H + F	7744	5285	13029	5765	35
S + H + F	7660	6372	14032	5803	63
G + S + H + F	7275	5751	13026	4704	10

表 5.3: 実験結果（割合）

	spam 率	非 spam 率	spam 排除率	誤検出率
Greylisting	56.65	43.35	95.1	2.679
SMTP セッション	55.33	44.67	85.38	2.826
ヘッダチェック	58.82	41.16	79.76	2.33
FQDN チェック	53.35	46.65	98.76	1.927
G + S	55.73	44.27	81.63	1.785
G + H	61.36	38.64	76.27	1.706
G + F	60.3	39.7	92.17	1.259
S + H	53.54	46.46	75.71	1.726
S + F	55.34	44.66	81.04	1.369
H + F	54.33	45.67	77.93	1.018
G + S + H	54.99	45.01	75.8	1.613
G + S + F	56.51	43.49	80.68	0.6901
G + H + F	59.44	40.56	74.44	0.2686
S + H + F	54.59	45.41	75.76	0.449
G + S + H + F	55.85	44.62	64.66	0.07676

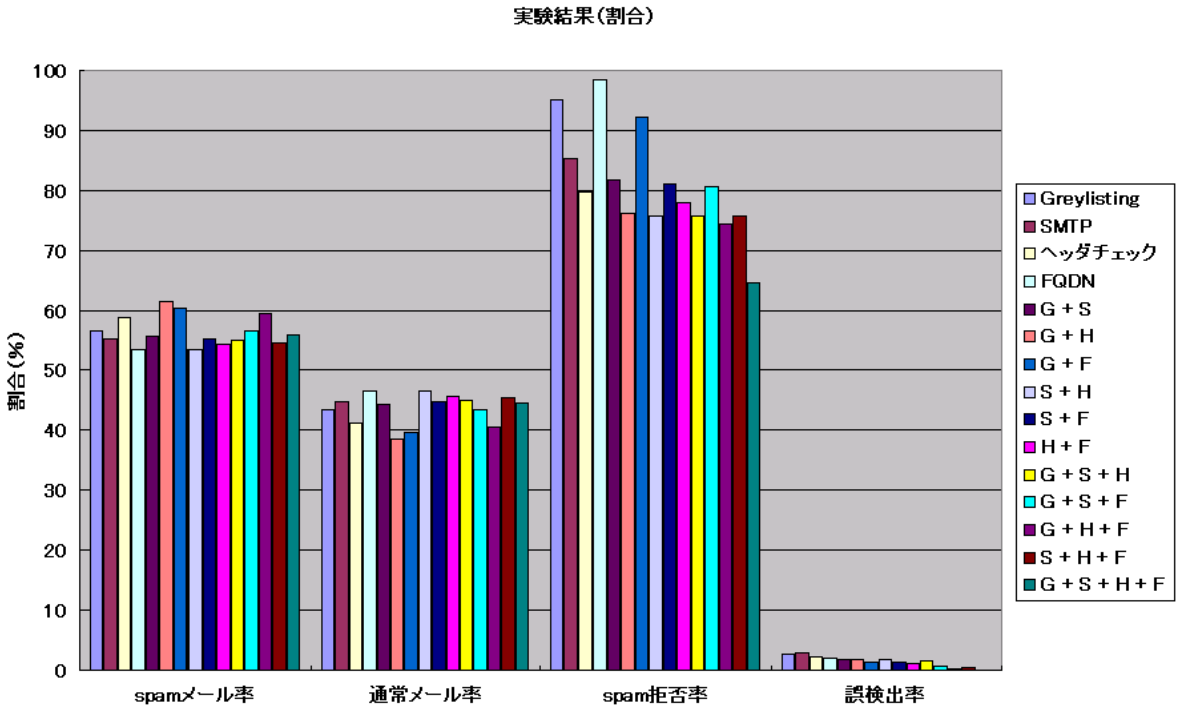

図 5.1: 実験結果（割合）

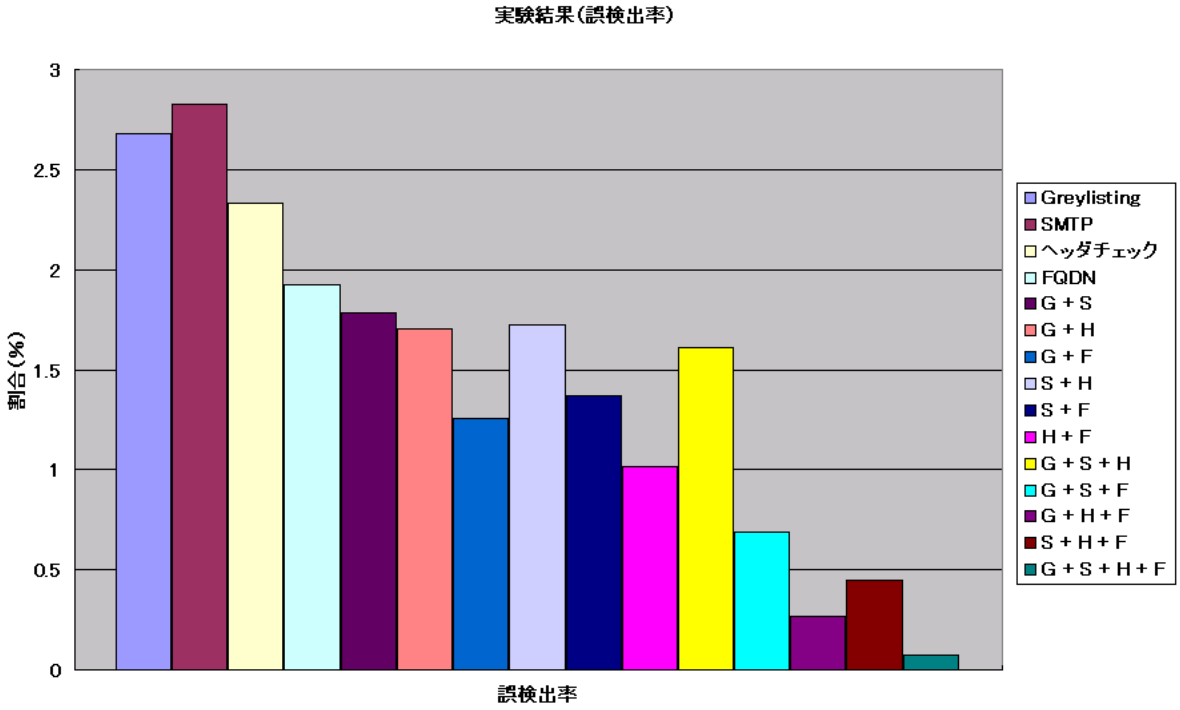

図 5.2: 実験結果（誤検出率）

以上から分かるように、平均 80 %以上の確率で spam メールを判別することができた。最も判別率が高かったのが、 FQDN チェックの 98.49 %であり、 100 %に近い結果を得ることができた。しかし、すべての方法で必ず誤検出が発生し、 FQDN チェックを用いた場合は比較的少なめであったものの、 Greylisting や SMTP セッションを用いて判別した場合は、他の方法に比べて高い確率で誤検出が発生した。判別率は複数の方法を組み合わせると下がってしまうが、誤検出も複数の方法を併用することでかなり下げることができた。特に、 4 種類の判別法すべてを用いた場合は約 65 %の判別率しか得られず、 spam 排除の効果はだいぶ小さくなってしまったものの、誤検出の割合も最小となった。

以下に、組み合わせに用いた 4 つの方法に見られた特徴を述べる。複数の方法を組み合わせた場合は、単独の方法の場合の結果と数値の違いはあるものの、特徴はそれぞれの方法とほぼ同様であった。

5.2.1 Greylisting

- 約 95 %の判別率を得られる
- 誤検出をする確率が高い
- メッセージの再送による遅延時間（大体 1 時間から数時間）がある
- 再送の設定がきちんとされていない送信元からのメッセージは、ホワイトリストを整備しなければ受信できない
- 正しいメールサーバを使われると、回避されてしまう

5.2.2 SMTP セッション

- 約 85 %の判別率を得られる
- 誤検出をする確率が最も高い
- チェックの設定を、緩いものから厳しいものまで柔軟に設定できる
- 特殊なツールやプログラムを必要としない

5.2.3 ヘッダチェック

- 約 80 %の判別率を得られる
- メッセージの受信状況や接続拒否などのログを確認して、頻繁に設定を変更する必要がある

- ブラックリストへの誤登録や、登録が悪用されている可能性がある

5.2.4 FQDN チェック

- 約 98 %の判別率を得られ、本実験では最高の値となった
- 誤検出をする確率が単独では最も少ない
- 仕組みが単純なため、実行しやすい
- 逆引き設定がきちんと行われていない送信元からのメッセージは、ホワイトリストを整備しなければ受信できない
- ホワイトリストの整備がかなり重要である。リストを更新する必要がある

第 6 章

まとめ

6.1 結論

本論文では、 MTA による spam メールの判別方法の利用についての実験を行い、検証した。実験から分かったことを以下にまとめる。

- 判別方法は単独で用いた方が高い判別率を得られる。
- 最も高い判別率を得られたのは、 FQDN チェックを用いた場合であり、ほぼ 100 %の判別率が得られた。
- 誤検出は複数の方法を組み合わせることで減らすことができる。
- 最も誤検出を抑えられたのは、すべての方法を組み合わせた場合であり、 1 万通あたり 7 通ほどの発生率となり、非常に小さい値である。
- 判別率と誤検出率の両方を考慮すると、最も効率がよいのは、 Greylisting と FQDN チェックの 2 つを組み合わせる方法である。
- ヘッダチェックは、他の方法に比べ、判別率が少なめであった。
- どの方法を用いても、必ず誤検出が発生した。
- Greylisting と SMTP セッションによる判別は、誤検出が他の方法に比べて圧倒的に多くなった。

6.2 今後の課題

本論文で行った実験について、今後検討すべき課題を以下に挙げる。

- 誤検出の発生

  これは最重要課題である。誤検出が発生してしまっては、 spam 対策どころの問題ではなくなってしまうし、多くのユーザは必要なメールを破棄してまで spam を排除することを重視するとは思えないからである。今回の実験では、非 spam メールは主にホワイトリストを用いて判別した。しかし、必ず誤検出が発生したことを考えると、ホワイトリストだけでは誤検出をなくすことは難しそうである。 MTA 上の対策のみで誤検出をなくすには、よほどうまくホワイトリストを整備するか、新しい規則や機能、プログラムなどを作成せねばならないであろう。現実的な方法をとるなら、 spam 判別の設定を緩めて多少の spam メールには目をつぶるか、 MUA 上の処理や他の spam 対策法を併用するというのが最も現実的な方法である。

- 設定、保守の簡易化

  ホワイトリスト、ブラックリストをはじめとして、設定は頻繁に確認し、必要に応じて変更しなければならない。また、ブラックリストを提供しているサイトなどを利用するにしても、サービスを停止してしまうケースも多く、特定のブラックリスト提供サイトの情報だけを鵜呑みにはできない。設定を変更すると他の機能に影響することも多く、変更は慎重に行わなければならない。ログを解析し、問題を検討し、変更を適用するという一連の動作を頻繁に行うのは、重要ではあるものの非常に手間がかかり、煩雑である。この手間を省くためにも恒久的に使用できる方法ができれば便利であるが、そのためには、まず法的な面の整備や仕様や設定方法、マナーの徹底などが前提として必要になる。また、メールログの記録やホワイトリストのメンテナンスを自動化することができたら非常に有用であるが、これにはある程度のリスクを伴うことを許容しなければならないだろう。

- RFC や FQDN などの設定の徹底

  これらを徹底することで、 spam メールの拒否は格段に簡単になるであろうと予想されるが、実際には非常に困難な問題である。この実現には、長い時間をかけて不正な設定を利用できないような仕様に移行したり、法的に措置をとれるようにすることが必要である。しかし、電子メールは古くから存在し、多くの利用者がいる上、日常的に欠かせない存在となっていることを考慮すると、なかなか実現は難しそうである。とは言え、早い内にできることから始めておくべきだと考える。

- 大規模な組織による運用

  規模が大きければ大きいほど、リスクのコントロールが重要になってくる。管理者がいかに spam メールを排除したくても、メールユーザが必要とするメールまで排除するわけに

はいかない。管理者は被害実態と送信者の挙動を細かに調べ、慎重な対策をとらなければならない。

- 今後の有用性

  spam メール対策には、いまだ決定的な判別方法は存在していない。本論文では最高で約 98 %の spam メール拒否に成功し、誤検出も最小で 1 万通あたり 7 通ほどに抑えることができたが、これが今後恒久的に利用できる保証はまったくない。 spam 送信者が工夫を凝らして抜け道を模索し続けている以上、受信者側も常に対策を考え続けなければならない。ただ、今後ますます spam メールが増えることを考慮すると、従来数多く利用されてきたメール内容による判定よりも、 MTA による判別法が重要になってくるのではないかと思われる。

謝辞

本学士論文の作成にあたり、日頃より御指導を頂いた早稲田大学理工学部コンピュータ・ネットワーク工学科の後藤滋樹教授に深く感謝致します。そして、貴重な助言およびアドバイスをくださいました後藤研究室の諸氏に感謝致します。

参考文献

[1] RFC2635:『DON'T SPEW』, 1999.

[2] Geoff Mulligan:『spam 撃退』, 株式会社ピアソン・エデュケーション, 1999.

[3] symantec, press center[2004/2/12],
http://www.symantec.com/region/jp/news/year04/040212.html

[4] アットマーク・アイティ, @IT リサーチ [2004/11/27],
http://www.atmarkit.co.jp/news/survey/2004/07spam/spam.html

[5] Japan.internet.com, Web マーケティング [2004/11/24],
http://japan.internet.com/wmnews/20041124/7.html

[6] INTERNET Watch, ニュース [2002/9/27],
http://internet.watch.impress.co.jp/www/article/2002/0927/idg.htm

[7] UNCTAD, (United Nations Conference on Trade and Development),
『E-COMMERCE AND DEVELOPMENT REPORT 2003』,
United Nations publication 2003/1.

[8] IBM, deceloperWorks[2002/9],
http://www-6.ibm.com/jp/developerworks/linux/021129/j_l-spamf.html

[9] 渥美 清隆: 『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』,
情報処理学会, 研究報告, DSM-33, pp.23–28, 2004.

[10] 関根 義明:『ベイズ型スパムフィルタの日本語メールへの適用』, 2003 年度卒業論文, 2004.

[11] Mehrn Sahami, Susan Dumais, David Heckerman, Eric Horvitz:
『A Bayesian Approach to Filtering Junk E-Mail』, AAAI Workshop on Learning for Text Categorizon, AAAI Technical Report WS-98-05, pp.55–62, July 1998.

[12] 漣 一平, 山井 成良, 岡山 聖彦, 宮下 卓也, 丸山 伸, 中村 素典:『遅延評価による分散協調型 spam フィルタの検出率向上』, 情報処理学会論文誌, Vol.22, No.22, pp.139–144, 2004.

[13] 岩永 学, 田端 利宏, 櫻井 幸一:『チャレンジーレスポンスとベイジアンフィルタリングを併用した迷惑メール対策の提案』, 情報処理学会論文誌, Vol.45, No.8, pp.1939–1947, 2004.

[14] Proper principles for Challenge/Response anti-spam systems, 1997, http://www.templetons.com/brad/spam/challengeresponse.html

[15] NTT privango サービス, http://www.privango.jp/info/index.jsp

[16] David Wood:『電子メールプロトコル』, オライリー・ジャパン, 2000.

[17] 総務省:『特定電子メールの送信の適正化等に関する法律　条文 (PDF)』, http://www.soumu.go.jp/joho_tsusin/top/pdf/meiwaku_01.pdf

[18] 経済産業省:『特定商取引に関する法律　法律改正及び省令改正説明用資料』, http://www.meti.go.jp/policy/consumer/tokushoho/kaisei2002/setsumeikai.pdf

[19] IT 用語辞典 e-Words, CAN-SPAM 法とは【Controlling the Assault of Non-Solicited】, http://e-words.jp/w/CAN-SPAME6B395.html

[20] Hotwired Japan, Wired News[2004/1/29], http://howired.goo.ne.jp/news/news/business/story/20040205108.html

[21] RFC2821:『Simple Mail Transfer Protocol』, 2001.

[22] RFC821:『Standard for ARPA Internet Text Messages』, 1982.

[23] RFC1123:『Requirements for Internet Hosts』, 1989.

[24] Greylisting: The Next Step in the Spam Control War, http://projects.puremagic.com/greylisting/

[25] 吉田 和幸:『greylisting の運用について』, 学術情報処理研究, No.8, 2004. http://hakuto.tottori-u.ac.jp/ipc2004/jacn8/ipc13.pdf

[26] Postgrey - Postfix Greylisting Policy Server, http://isg.ee.ethz.ch/tools/postgrey/

[27] Postfix SMTP アクセスポリシー委任,
http://tmtm.org/ja/postfix/doc/SMTPD_POLICY_README.html

[28] 荒木 靖宏: 『Postfix 詳解』, オーム社, 2004.

[29] 浅見 秀雄: 『阻止率 99 %のスパム対策方式の研究報告』, 2004.
http://gabacho.reto.jp/anti-spam/anti-spam-system.html