「マルチメディア，分散，協調とモバイル
(DICOMO2018)シンポジウム」 平成30年7月

迷惑メール対策のための新規Eメール基盤技術の提案

山城裕陽[1]　落合 秀也[1]　江崎 浩[1]

概要：情報化社会において、E メールは情報伝達手段として頻繁に用いられている。世界中で送受信されるE メールの総数が大きくなるにつれて、迷惑メールも増加傾向にあり、早急な対処が必要とされている。現在、迷惑メール対策としては迷惑メール送信者の使用するメールサーバを指定し、ブラックリストに登録することで受信拒否を行う方法が一般的であるが、同じメールサーバを用いる別のユーザが巻き込まれるなどの問題点がある。迷惑メールの研究としては、主にフィルタリングのために迷惑メールを検知する手法を示すものが多い。機械学習やニューラルネットワークで迷惑メールの特徴を決定し、特定することに成功している。ところが、迷惑メールの傾向は日々変化していくため、学習が必要な既存手法では迷惑メール送信者とのいたちごっこになってしまう。そのため本研究では、E メールの送信にコストを付加し、コストの支払いを認証局が管理することで、迷惑メールを送信すること自体が難しくなる新しいメールシステムを提案する。また、そのシステムを簡略化したモデルシステムを実装し、迷惑メールを排除できていることを確認した。

1. はじめに

近年、電子メールは世間の人々に広く普及し、プライベートや仕事のやり取りで無くてはならないものとなっている。世界中で電子メールが連絡手段として活用され、一日に送受信される電子メールの総数は増加の一途を辿っている。その中にはいわゆる「出合い系」サイトの広告宣伝や架空請求を始めとした迷惑メールも存在しており、電子メールの総数が増加するのに伴って迷惑メールの数も増加している。

一通りの迷惑メールに関する知識やネットリテラシーのある人の元に迷惑メールが届いた場合、迷惑メールは適切に処理される。しかし、そうではない子供や、ネットに関する知識のない人の元に迷惑メールが届いてしまうことがあり、これが大きな問題を引き起こす。例えば、「差出人や件名が不穏なメールの添付ファイルをダウンロードする際には、ウイルスチェックをしっかりする」といった行為は、現在の迷惑メール傾向を知っている人ならば当然の如く実行することである。ところが現実には、メール添付ファイルに端を発するランサムウェア「WannaCry」に業務用 PC が感染し、業務に支障が出るなどの被害が発生した。また、日頃からパソコンを使用する人ですら引っかかってしまう迷惑メールに、パソコンを使い始めたばかりの子供たちが適切に対処することが難しいことは明らかである。

現状、メールの大量送信などの迷惑行為を行われた場合、送信元のサーバの IP アドレスをブラックリストに登録し、それ以降そのサーバからのメールを受け取らないという対策が一般的である。この対策によるブラックリスト登録は迷惑行為を行っていないユーザを巻き込む可能性があり、メール送信の規制によって時間的・経済的損失を生じさせることがある。また、この対策はあくまで対症療法にすぎず、迷惑メールに対する根本的な解決策にはなり得ない。

そもそも、電子メールは 1964 年に MIT 内部でのコミュニケーションツールとして誕生した。以来 1970 年代から 80 年代にかけて、1982 年の簡易メール転送プロトコル (SMTP) の導入などによってメールクライアントとメール送信/受信サーバのやり取りという電子メールシステムの基礎が築かれた。電子メールが現代社会においてこれだけ広く普及したのは、次の 3 つの特徴を持つからであると考えられる。

- 匿名性
- 低コスト性
- メールアドレス入手の容易性

匿名性とは、電子メールはその宛先をメールアドレスで指定すればよく、メールアドレスは本名である必要性がないということである。この匿名性は顔の見えないインターネットを介したやり取りと非常に相性が良く、現代において電子メールが広く普及したことの一因である。低コスト性とは、現代ではパソコンやスマートフォンなどの情報端末とインターネット環境さえあれば、メールアドレスを取得することは非常に安価で容易であるということである。

[1] 東京大学大学院情報理工学系研究科

手紙を買って切手を貼り、文章を書いてポストに投函するよりも金銭も時間も節約できる電子メールは、忙しい現代社会を生きる人間にとって理想的な情報伝達媒体なのである。メールアドレス入手の用意性とは、他者のメールアドレスを第三者から取得することが非常に容易であるということである。実世界に名簿業者が存在し、そこから手に入れた住所をもとにダイレクトメールが送られてくることがあるように、メールアドレスについても名簿業者が存在する。その手の業者を使えば広告などを容易に数万人単位の人に送信することができる。

ここまで、電子メールの特徴を利点として挙げてきた。ところが、今まで述べてきた特徴はすべて迷惑メール送信者に利用されてしまう欠点と表裏一体なのである。匿名であるがゆえに無責任に違法性のある商品やサービスを宣伝することが可能である。また、詐欺サイトのリンクやウィルスが添付された電子メールを送ることもできる。さらに、低コストであるがゆえに短時間に大量にそれらのメールを送信することも可能である。メールアドレス入手が容易であるがゆえに迷惑メールの対象者を決定することも容易なのである。電子メールの特徴を考えるときには常に、これら違法情報が氾濫していること、攻撃手段となりうること、攻撃対象を容易に選べてしまうこと、といった欠点にも目を向ける必要がある。

本研究の目的は、このような現状を打破し、迷惑メールを根本的に減少させることである。迷惑メールに対して強固な電子メール基盤がどのようなものかを電子メールの特徴から考え、その仕組みを提案する。

なお、本研究では電子メールを用途に応じて 3 種類に分類して考える。

- 企業や学校、個人が主にビジネスに関して取引先との連絡をする際のビジネスメール
- 宣伝広告や web サービスのアカウント作成に対する応答の際に用いられるサービスメール
- 企業や学校の内部での連絡をする際のメーリングリスト

である。ビジネスメールはメールの用法の中でも現代社会で非常に重要なものであり、その他のツールで代用することが非常に難しい。なぜならば、あらゆる対象に送信でき、送受信を行う当人以外に情報がもれず、本文だけではなくファイル添付も可能で、相手を時間的に拘束せずコストが低いものという条件があるからである。これら条件を満たす情報伝達手段は今の所電子メールしか存在しない。サービスメールに関しては、スマートフォンが普及し、各種 SNS が多く用いられる現代において、電子メールという基盤の上で行う必要性が薄いと考えられる。近年では、企業が自社の宣伝を行う Twitter アカウントも存在する。これらを踏まえれば、サービスメールは将来的に個別のアプリケーションや LINE、Twitter などの SNS にとって変わられていくことが予想される。メーリングリストに関してもサービスメールと同様に、Slack などのより高機能な内部連絡ツールが存在する以上、電子メールで行う必要性はないと考える。将来的に他のツールで代用されていくべきである。

電子メールはこれら様々な用途で利用されているが、そのせいで電子メールシステムに変化を与える際の条件が非常に厳しくなっている。そこで、本研究では電子メールを用いる通信を攻撃を受けた際の被害が大きくなりやすく、かつ電子メールでないといけないものに限定し、出来るだけ研究対象がシンプルになるようにする。したがって、本研究における迷惑メール対策は特に、「ビジネスメール」における迷惑メールへの対策を扱うものとする。

本論文では、第 2 節で関連研究について触れ、第 3 節で迷惑メールに対抗する本研究での新たな手法を提案する。第 4 節で実際に作成したモデルシステムについて述べ、第 5 節で本研究に対する議論を行う。第 6 節で本研究のまとめを行う。

2. 関連研究

迷惑メールを電子メール利用者の目に触れる前に判別し、迷惑メールとして専用のメールフォルダに振り分けることをフィルタリングという。また、迷惑メールを判別するときに用いる条件のことをフィルタと呼ぶ。これまでの迷惑メール対策に関する研究では、このフィルタリングを行うためのフィルタをどのように作成するかの手法が主な研究対象であった。評価尺度としてはどれだけ人間にとって楽か、迷惑メールを判別する精度がどのくらいかなどが挙げられる。以下に代表的な手法を示す。

2.1 クラスタリング

Basavaraju[1] は、電子メール本文中の文字列からパターンや特徴を選択・抽出し、それに基づいて電子メールをクラスタリング (グループ分け) することで、迷惑メールを検知することを試みた。

電子メール本文内容から特徴を抽出した後、その特徴が電子メール本文同士でどのくらい似通っているのかを検証する。最後に似通ったものを同じグループとしてまとめる。あるメールについてその処理が終わった後は、それによるグループの変化をその後にもフィードバックする。これをデータサイズ分だけ繰り返した最終的なグループをクラスタとして確立する。

クラスタリングのアルゴリズムとしては k-平均法や BIRCH アルゴリズム、NNC が用いられ、データサイズや手法にもよるが 9 割程度の精度で迷惑メールの判定を行うことを達成している。

ただし、迷惑メールの構成が大きく変更された場合には再度学習を終えるまでフィルタが十分に機能しなくなるこ

とが予想される。

2.2 迷惑メールの特徴決定木

杉井ら [2] は、機械学習システム BONSAI[3] を利用し、迷惑メールの特徴を判別する決定木を作成し、迷惑メールの検出を試みた。作成の過程においては、迷惑メールによく登場する文章を正の学習グループ、あまり登場しないが通常の電子メールではよく使われる文章を負の学習グループとして使用した。

各学習グループの文章を単語に分解し、出現頻度によってグルーピングと記号への置換を行う。その記号を BONSAI に予め設定しておいた値に置換し、それを元に決定木を作成する。こうして作成された決定木をもとに、電子メールを迷惑メールかどうか判別する。

この手法では 10 学習例で 87.5%、50 学習例以上で 9 割以上の正答率を得ることができており、決定木作成も自動であるため人間にとっても非常に楽なものである。しかし、クラスタリングの手法と同様に、迷惑メールの傾向が大きく変わった場合には決定木を作成し直す必要がある。

2.3 ニューラルネットワーク

Özgür ら [4] は、人工ニューラルネットワークとベイジアンフィルタを用いて動的に迷惑メールのフィルタリングを行うことを試みた。この手法では、まず単語 W に対して相互情報量 MI(W) を計算する。その後、MI(W) の大きい単語、つまり通常メールか迷惑メールのどちらかにのみ多く出現する単語から特徴ベクトルを算出し、それを用いて迷惑メールか否かを判断している。

着語 (この場合はトルコ語) で書かれた 750 通の電子メール (うち 410 が迷惑メール、340 が通常の電子メール) に対して行った実験では、約 9 割の割合で正しい判定を行うことができている。また、処理速度についても、1 分間に約 3000 語を処理することが可能であり、非常に高速で迷惑メールの判別を行うことができることが示されている。ただし、トルコ語以外の言語を扱っていないため、現在の迷惑メールの主流言語である英語に対して同じように学習できるかは判然としない。また、迷惑メールの傾向が変われば学習をし直す必要がある。

3. 提案手法

3.1 メール基盤の設計方針

電子メールの「低コスト」という特徴が迷惑メールにも利用されてしまっていることは第 1 節で述べたとおりである。そこで、本研究では電子メールを送信する際に金銭的なコストを発生させることで、迷惑メールを抑圧する仕組みを作成しようと企図する。

迷惑メール送信者は、電子メールを送信する頻度が通常の電子メール利用者よりも非常に高くなることが考えられる。そのため、電子メール送信にコストが発生すると、迷惑メールを送信することによる利益が電子メールを送信するためのコストに見合わなくなり、迷惑メールを送信する理由がなくなる。

一方で、通常の電子メール利用者は、迷惑メール送信者に比べれば低いコストを維持したまま、より安全な電子メールを利用することができる。電子メールにコストがつくと、これまでほぼ 0 コストで利用していた利用者にはあまり好意的には受け取られないだろう。しかし、この点については 2.2 節で述べた通り、他 SNS 等を利用することで解決できるものであると考える。どうしても電子メールでないといけないものについてのみ、電子メールが利用されるようになる。

このように、電子メールの特徴の一つである「低コスト性」を見直すことで、結果として迷惑メールを抑制することが可能である。

3.2 手法概要

本研究で提案する課金システムは次の仕様を満たす。

- 認証局による電子メール送信の際の課金の管理。
- 電子メール送信者による課金。
- 各電子メール利用者の所持金の認証局のデータベースにおける管理。
- コストの送信・受信メールアドレスの組み合わせに応じた認証局データベースでの管理。
- データベースの更新によるコストの任意の値への変更。
- 受信した電子メールが課金されているかの確認と電子メール送信のログの、認証局データベースでの管理。

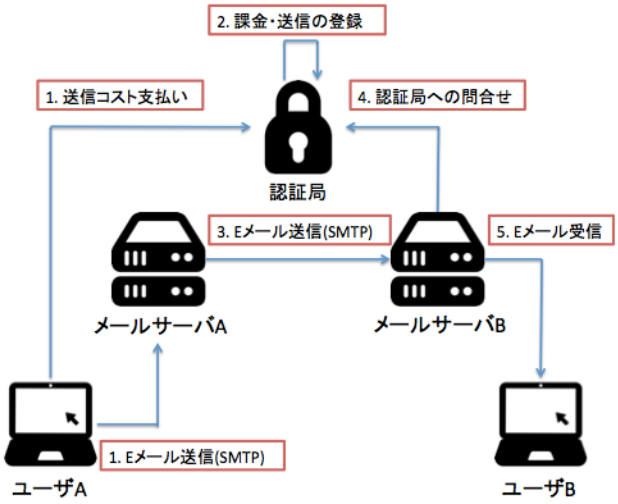

図 1 課金システム概要図

図 1 に本研究で提案する課金システムの概要図を示す。このシステムは送信者 (ユーザ A) から受信者 (ユーザ B) に電子メールを送信する際、次のように動作する。

(1) ユーザ A が認証局に登録してある所持金から送信コ

ストを支払い、電子メールをメールサーバ A へ送信する。
支払うことができない場合は電子メールは破棄される。
(2) 認証局データベースにユーザ A からユーザ B への電子メール送信と課金があった事実を登録する。
(3) メールサーバ A からメールサーバ B へ電子メールが送信される。
(4) メールサーバ B が電子メールを受信したら、認証局に問い合わせる。
課金されていない電子メールは破棄される。
(5) ユーザ B が電子メールを受け取る。

このシステムがどのように迷惑メール対策を実現するのかを述べる。前提として、通常ユーザはこのシステムを採用して電子メールを送受信しているものだとする。

まず、課金システム外からの迷惑メールを考える。課金システムを採用しないメールサーバから送信されてきた電子メールは、受信側のメールサーバまでは到達する。しかし、その後の認証局への問い合わせで課金履歴が確認されず、その時点で破棄される。従って、課金システム外からの迷惑メールには完全に排除することが可能である。

次に、課金システム内からの迷惑メールを考える。受信者側のデフォルトの要求コストをどのくらいの値にするかにもよるが、各受信者について最初の数通は受信されうる。しかし、迷惑メールだということが認識されればその時点で要求コストが跳ね上がり、それ以上その受信者に対して迷惑メールを送信することができなくなってしまう。従って、課金システム内からの迷惑メールを対策することもできる。

4. モデルシステムの作成・実験

実装は送信サーバに Postfix、受信サーバに Dovecot を用いて構成したメールサーバに、Ppymilter[5] というライブラリを用いて Python で作成したデーモンによって機能を追加する形を取った。また、データベースの操作は PostgreSQL を用いた。以下、モデルシステムの設計について説明する。

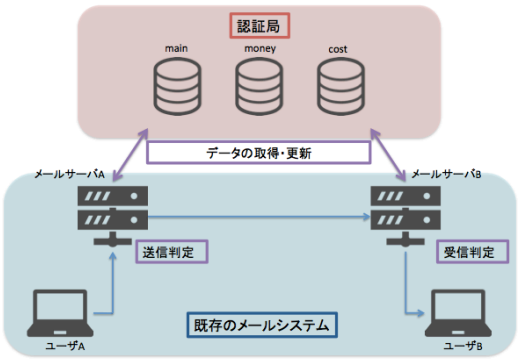

図 2 モデルシステム全体の設計図

図 2 にモデルシステム全体の設計図を示す。既存のメールシステムに認証局に相当する 3 つのデータベース (main, money, cost) を追加した。

main は電子メール送信に伴う課金が成された事実が登録されている。受信側で電子メールを破棄するかどうかの確認や、電子メール送信ログとして活用する。money はユーザの所持金が登録されている。ユーザはメールアドレス単位で登録することにした。cost は (A, B, コスト) のセットで、A(送信者) から B(受信者) に電子メールを送信する際に A に課されるコストが登録されている。

電子メールの送信者から送信側のメールサーバに電子メールが到達すると、送信側メールサーバからデータベースにアクセスする。その後、電子メールを送信できるか判定する。送信が可能ならば課金 (money の更新) を行い、電子メールを受信側メールサーバに届ける。受信側メールサーバは電子メールを受け取るとデータベースにアクセスし、電子メールが受信可能か判定する。

money にユーザの情報が登録されていない場合や、ユーザの所持金が送信時のコストに満たない場合には、送信判定が False となり、電子メールを送信できない。送信側メールサーバで電子メールは破棄され、main の履歴に残らず、受信側メールサーバにも到達しない。

受信側メールサーバに到達した電子メールに対応する送信履歴が main に登録されていない場合、受信判定が False となり、電子メールを受信しない。受信側メールサーバで電子メールは破棄され、受信者が電子メールを受け取ることはない。

正常に送受信が行われた場合は次の手順で処理が行われる。送信側メールサーバで課金 (money の更新) が行われ、main に課金・送信した事実が登録される。受信側メールサーバでは main を確認し、対応する情報の確認を行う。そして、正常に電子メールが受信される。

本研究では、以上の挙動を示すモデルシステムを作成し、それによって電子メールの送受信を行うことに成功した。その際の結果を状況毎に示す。

4.1 ユーザが登録されていない場合

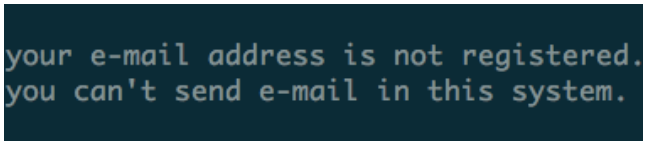

図 3 送信エラー (ユーザ未登録)

図 3 がユーザが登録されていない状態で電子メールを送信しようとした場合のエラー画面である。送信側メールサーバにこのメッセージを出力した後電子メールは破棄され、main に送信記録も残らなかった。

4.2 所持金が足りない場合

```
your money is 100 now.
cost is 10000 now.
your money is not enough. you can't send e-mail now.
```

図 4 送信エラー (所持金不足)

図 4 が所持金が送信コストを下回る場合のエラー画面である。送信側メールサーバにこのメッセージを出力した後電子メールは破棄され、main に送信記録も残らなかった。

4.3 送信記録がない場合

```
you've got suspicious e-mail from outside of this system. discarded.
```

図 5 受信エラー (送信記録なし)

図 5 が送信記録のない電子メールが届いた場合のエラー画面である。受信側メールサーバにこのメッセージを出力した後電子メールは破棄された。

4.4 送信成功の場合

```
your money is 9900 now.
cost is 100 now.
you have sent a new e-mail. your money is 9800 now.
From nobody Thu Feb  8 14:20:47 2018
To: <yuya@yuya-mail2.hongo.wide.ad.jp>
Subject: test
X-Mailer: mail (GNU Mailutils 2.99.99)
Message-Id: <20180208052045.414E34E034B@yuya-mail.hongo.wide.ad.jp>
Date: Thu,  8 Feb 2018 14:20:45 +0900 (JST)
From: yuya@yuya-mail.hongo.wide.ad.jp (yuya)

test1
```

図 6 送信成功

図 6 が送信に成功した場合の出力である。送信側メールサーバにこのメッセージを出力した後、main に送信記録が図 7 のような形式で保存された。タプルの 1 つ目の要素が未配達/既配達を示す Tag である。0 はまだ受信側メールサーバでのメール事実の確認が行われていないことを示す。2 つ目の要素が送信者、3 つ目の要素がメール本文から作成したハッシュ値である。また、コストが 100 であったため、money は送信前後で「yuya@yuya-mail.hongo.wide.ad.jp」の所持金が 10000 から 9900 へと変化した。

```
>>> cur.execute("select * from main")
>>> for row in cur:
...     print row
...
(0, 'yuya@yuya-mail.hongo.wide.ad.jp', '1e1f2abfe927202cb8116c1e2972fa46533e4c45
4d13e3b815fddd7dd2cd0f1c571a31b93fc37a978be05c6c1838ff23e4ce8efa379bd974f32974d2
adf82b24')
```

図 7 送信記録 (main)

4.5 受信成功の場合

```
you have received a new message.
From nobody Thu Feb  8 14:20:49 2018
Received: by yuya-mail.hongo.wide.ad.jp (Postfix, from userid 1000)
 id 414E34E034B; Thu,  8 Feb 2018 14:20:45 +0900 (JST)
To: <yuya@yuya-mail2.hongo.wide.ad.jp>
Subject: test
X-Mailer: mail (GNU Mailutils 2.99.99)
Message-Id: <20180208052045.414E34E034B@yuya-mail.hongo.wide.ad.jp>
Date: Thu,  8 Feb 2018 14:20:45 +0900 (JST)
From: yuya@yuya-mail.hongo.wide.ad.jp (yuya)

test1
```

図 8 受信成功

図 8 が受信に成功した場合の出力である。受信側メールサーバにこのメッセージを出力した後、main の送信記録が参照され、ハッシュ値が一致したものが図 9 のように更新された。

```
>>> cur.execute("select * from main")
>>> for row in cur:
...     print row
...
(1, 'yuya@yuya-mail.hongo.wide.ad.jp', '1e1f2abfe927202cb8116c1e2972fa46533e4c45
4d13e3b815fddd7dd2cd0f1c571a31b93fc37a978be05c6c1838ff23e4ce8efa379bd974f32974d2
adf82b24')
```

図 9 送信記録の更新 (main)

送信の際登録された内容と比べて、Tag の値が 0 から 1 に変化している。今回の実装ではこれを送信事実の確認にあたるものとした。

5. 議論

この章では今回実装したモデルシステムにおいては簡略化したが、実運用上では重要な点について述べ、どのように対応するべきかを議論する。

5.1 メーリングリスト・エイリアスへの対応

メーリングリストは 1 つのメールアドレスに複数のメールアドレスを紐付けておき、そのメールアドレスに電子メールが送信された場合、紐付けられたメールアドレス全てに転送する仕組みである。エイリアスはあるメールアドレスに対して別名を用意しておくことである。

これらに共通するのは、送信者から見える受信者と本当の受信者が異なってしまうことである。つまり、送信者が To:の欄に書き込むメールアドレスと、実際に最終的に配送されるメールアドレスが異なることとなる。

今回のシステムでは電子メール自体の情報から送信者・受信者の情報を取得するため、そのような状況下では正常に動作しない。従って、この場合には特殊な挙動をするように設定する必要がある。すなわち、メーリングリスト参加者からの電子メールには課金を行わないようにしたり、エイリアスであった場合には送信履歴を更新して、送信と受信の一対一対応を保つようにしなければならない。

5.2 コスト決定の方法

本研究においてはコストは既に決定されているものとして扱ってきた。しかし、このシステムの利点はコストをいつでも変更できることである。従って、コストを決定する方策についての考察を行う必要もある。

親しい友人や懇意にしている取引先との電子メールに対するコストは極力小さくしたい。よって、まず手動でいつでもコストを更新できるようにしなければならない。手動で設定したコストは何よりも優先されるべきである。

また、迷惑メール対策の観点で考えると、迷惑メールを検知した場合は自動でコストを高く設定したい。迷惑メールの検知は関連研究にあるような諸手法で高精度で行うことができるため、それに従って自動でコストが変更されるようにすることできるはずである。迷惑メール以外にも、送信頻度などの情報をもとに送信コストをうまく変更していくアルゴリズムを開発すれば、先に述べたように手動でコストを更新する必要もなくなることが考えられる。

このように、システムをより実用的なものにするには、コストを更新するための仕組みを導入しなければならない。

5.3 セキュリティ上の問題

本研究におけるモデルシステムはシンプルさに重点をおいたため、セキュリティ的観点から見ると脆弱なものである。従って、実際のシステムを構成する際にはどのようにしてセキュリティを高めるかを考察する。

認証局との通信を他人になりすましされてしまうと、意図しない課金が発生し、大きな被害が発生する。よって、メールサーバと認証局の通信は SSL/TLS によって暗号化される必要がある。その際、送信元アドレスのドメインと証明書を紐付けておくことにする。そうすれば他人のメールアカウントで電子メールを大量に送信したという情報を認証局に登録することで大量の課金を発生させる攻撃などを回避することもできる。

モデルシステムにおいては認証局のデータベースに SQL によるクエリを直接投げることで認証局との通信を行った。これは暗号化などされていないため、HTTPS などのプロトコルを利用することで暗号化する必要がある。

また、受信側メールサーバと認証局の通信についても改善すべき点がある。モデルシステムの方式では、自分以外が受信者になっている電子メールに関するログも取得することが可能である。つまり、他の人が自分以外の誰にメールを送信しているのかを確認することができるということである。これはメールアドレスのクロールなどに悪用されうる。従って、受信側メールサーバと認証局の通信においては、受信者のドメインと紐付けられた証明書を用いて、自分自身に向けて送信された電子メール以外の情報を取得することができないようにしなければならない。

6. おわりに

本研究では迷惑メールの根本的対策を目指し、迷惑メールの性質も踏まえ、迷惑メールに対応できる、電子メール 1 通ごとにコストを付加したメールシステムを提案した。この手法によって、システム内外からの迷惑メールに対応できることを確認した。

また、提案手法を簡易化したモデルシステムを実装し、動作させることで、現行のシステムからの移行が容易であることも示した。送信ができない場合や、送受信が成功したなどの状況におけるシステムの応答を確認し、モデルシステムとして十分な動作をしていることを確認した。

モデルシステムにおいて無視したメールリスト対策、コスト決定方法、セキュリティなどについても議論を行った。それぞれに対してモデルシステムではどのように振る舞っているのかと、本来ならばどうするべきなのかを述べた。

参考文献

[1] Basavaraju, M., and Dr R. Prabhakar. A novel method of spam mail detection using text based clustering approach. International Journal of Computer Applications 5.4 (2010): 15-25.

[2] 杉井学, and 松野浩嗣. ”機械学習によるスパムメールの特徴の決定木表現.” 情報処理学会研究報告コンピュータセキュリティ (CSEC) 2007.16 (2007-CSEC-036) (2007): 183-188.

[3] Shimozono, Shinichi, et al. ”Knowledge acquisition from amino acid sequences by machine learning system BONSAI.” Transactions of Information Processing Society of Japan 35.10 (1994): 2009-2018.

[4] Özgür, Levent, Tunga Güngör, and Fikret Gürgen. Spam mail detection using artificial neural network and Bayesian filter. Intelligent Data Engineering and Automated LearningIDEAL 2004 (2004): 505-510.

[5] ”GitHub - jmehnle/ppymilter: Git fork of Pure Python Milter from https://code.google.com/p/ppymilter/”, https://github.com/jmehnle/ppymilter