L-030

ユーザのメール閲覧サイクルを考慮した遅延評価による迷惑メール検出率の調査
Analysis of spam Mail Detection Rate with Delay Evaluation on Cycle of Fetching Mail

奥村 慎太郎† 鈴木 康介‡ 松澤 智史† 武田 正之†
Shintarou Okumura Kousuke Suzuki Tomofumi Matsuzawa Masayuki Takeda

1. はじめに

近年，電子メールの快適な利用を妨げる問題として迷惑メールが挙げられる．symantec社による2008年5月の迷惑メールに関するレポート[1]によると，全世界のメールの80%以上が迷惑メールであるとされている．これらは社会への経済的被害[2]を与えている．迷惑メール被害の例として，正常なメールとの選別に消耗する時間が挙げられる．また同社の調査で，2006年の企業における迷惑メールの処理時間は従業員1人あたり平均4.4分/日であり，迷惑メール受信比率が30%を超える企業では平均11.2分/日かかることも判明している[2]．こういった迷惑メールを拒否するために，迷惑メールフィルタを用いたフィルタリングと呼ばれる手法が存在する．フィルタはサーバ側で行うものとクライアント側で行うものの2種類があり，サーバ側で行う代表的なものとして事例ベース型フィルタ，IPアドレスフィルタがある．しかしフィルタリングは，迷惑メールフィルタの種類によってはFalse Positive(正常なメールを迷惑メールだとする誤判定)が無視できない量で発生するという短所も存在する．よって迷惑メールフィルタは検出率が高く，かつFalse Positiveの発生確率が低くあることが望ましい．

2. 既存の迷惑メールフィルタ

2.1 事例ベース型フィルタ

ある迷惑メールを受け取ったユーザが，迷惑メールに記載された URL などの特徴からチェックサムを計算してユーザ間で共有するデータベースに登録し，後に同じ迷惑メールを受信したユーザが，チェックサムを計算しデータベースに問い合わせることで迷惑メールをブロックする手法である．このフィルタリングはユーザが既知の迷惑メールを登録するという特性上，時間の経過によってデータベースが充実し，かつ False Positive は無視できる程小さくなるという利点がある．しかし初見の迷惑メールには対応できないため，検出率は比較的低くなる．松浦らの研究[3]によれば，事例ベース型フィルタの 1 つである Pyzor を用いて実験した場合，False Positive は 0.0%であったが，検出率は67.8%と低い数値になったと報告されている．

2.2 IP アドレスフィルタ

不当なメールの中継を許すサーバの，IPアドレスを列記したデータベース(ブラックリスト)をフィルタとして用いることで，迷惑メールを遮断する手法である．このようなデータベースはDNSBL(DNS Base Blackhole List)と呼称され，運用するサービスが世界中に存在していること，常に更新され続けていること，DNSBLの組み合わせによって検出率の向上が見込めることが特徴である．迷惑メールの送信元IPアドレス4071件と，正常なメールサーバのIPアドレス186件を7種類のDNSBLに問い合わせた結果，1種類のDNSBLに検出された迷惑メールは全体の91.8%(False Positiveは6.4%)，2種類に検出されたメールは76.6%(0.5%)，3種類に検出されたメールは60.6%(0.0%)であった．しかしこの手法も事例ベース型フィルタと同様に，初見の迷惑メールには対応できないという欠点がある．

†東京理科大学 理工学部 情報科学科
Dept. of Information Sciences, Tokyo University of Science
distinct@mt.is.noda.tus.ac.jp
‡清水建設株式会社 SHIMIZU CORPORATION

3. 遅延評価

事例ベース型フィルタと IP アドレスフィルタは，時間経過によってフィルタリングのデータベースが充実するという共通点を持つ．よってこれらの手法では，検出を行う時間を，メールがメールサーバに到着した時刻からユーザがメールをダウンロードする時刻へと遅延させることで検出率の向上が見込める．この手法は遅延評価と呼ばれ，漣らによる小規模の実験で報告されている[4]．

また松浦らの報告[3]によると，和歌山大学システム工学部のメールサーバで遅延評価を運用させたところ，148,206通の迷惑メールに対して，遅延評価を用いない場合は112,731 通（76.1%)が検出できたが，用いた場合は 8,604 通（5.8%）多く検出できたとされている．

4. 本研究の目的

遅延評価はメールの到着時刻からユーザがメールをダウンロードするまでの待ち時間を利用するため，迷惑メール検出率はユーザのメール閲覧時刻や閲覧間隔に左右される．したがって検出率はユーザの環境やライフスタイルによって大きく変化すると考えられる．またユーザの環境やライフスタイルが検出率に影響を与えるのであれば，検出率の大小は，ユーザの属するユーザ群(例えば学生，社会人など)によって大別される可能性もある．ユーザ群毎に遅延評価が有効であるかどうかを知ることができれば，それを遅延評価システム導入時の指標と考えることが可能である．

5. 実験及びその評価

5.1 実験環境及び実験手法

IP アドレスフィルタにおいて，各ユーザ及びユーザ群に対して遅延評価が有効に働くかどうかをシミュレートした．ユーザは本学教員 18 名と学生 29 名の計 47 名，ユーザ群は教員と学生の 2 つを対象とした．

実験を行うにあたって迷惑メールの到着分布が必要となるので，2008/5/27～2008/6/30 に収集した迷惑メール 3,314 通の到着時刻を，1 日を基準とした秒数(0 秒から 86,400 秒)で抽出し，1 日に 3,314 通全てが到着するものとして分布を作成した．また 3,314 通の迷惑メールを，それぞれ 24 時

間の間 7 種の DNSBL に問い合わせ続けることで，送信元 IP アドレスが 2 種の DNSBL に登録されるまでの経過秒数と検出率との関係を求め，迷惑メール検出率の時間推移とした．検出率は以下の式で求める．

検出率＝2 種の DNSBL に登録済みの迷惑メール件数
/全迷惑メール件数

ユーザが閲覧を行う時刻を 1 日毎にまとめたものを，メール閲覧サイクルと呼ぶ(以後サイクルと表記)．サイクルは，教員と学生のメールサーバにおける POP，IMAP ログから 1 日のアクセス記録をユーザ毎に抽出した結果，教員のサーバで 2008/5/18/～2008/6/18 のログより 508 種類，学生のサーバで 2008/2/19～2008/6/26 のログより 316 種類，合計 824 種類を抽出できた．

1 つのサイクルにおける迷惑メール検出率を導出する方法を示す．迷惑メール 1 通毎に，メール到着時刻からその時刻以降で最も近い閲覧時刻までの待ち時間を求め，遅延時間とする(到着時刻以降に閲覧が無かった場合は 1 日が繰り返しているものとして，到着時刻からサイクルの閲覧開始時刻までを遅延時間とする)．迷惑メール検出率の時間推移においてその遅延時間に対応した検出率が，迷惑メール 1 通に対する検出率となる．この手法を迷惑メール 3,314 通それぞれに対して適用すると 3,314 個の検出率が得られるので，その総和を求める．

1 つのサイクルにおける検出率＝
検出率の総和/全迷惑メール件数

これを全サイクルに対して適用する．これにより，ユーザ毎及びユーザ群毎に検出率の傾向を把握することができる．

5.2 ユーザの環境やライフスタイルと検出率の関係

抽出した全てのサイクルを用いて，遅延評価を用いた IP アドレスフィルタの検出率と，サイクルとの関連性を検証した．その結果，遅延評価を用いない場合の検出率が 78.3%であるのに対し，全サイクルに対して用いた場合の平均検出率は 89.3%であった(教員 89,7%，学生 88.5%)．また，閲覧回数が少なく使用時間が短いサイクルほど検出率が高いことが判明した．閲覧回数において最も高い平均検出率を記録したのは閲覧回数が 1 回のみのサイクルにおける 93.1%であり，使用時間については 1 時間単位で検出した結果，最も高い平均検出率を記録したのは使用時間が 1 時間未満のサイクルにおける 93.0%であった．よって，遅延評価とサイクルの間には大きな関連があると言える．

5.3 ユーザ群と検出率の関係と考察

教員と学生を区別する属性を決定するために，決定木学習アルゴリズム ID3[5]の発展である C4.5[6]を用いた結果，6 枚の葉(A～F 区分)を持つ決定木が得られた(図 1)．図中の数値は分類されたサイクル数を表す．

A 区分では教員の割合が大きい．A 区分のサイクルは，深夜には閲覧せず，主に朝～夕方に閲覧を開始する．よって教員は学生と比べて閲覧開始時刻が遅く，使用時間は短いと考えられる．使用時間の短いサイクルや閲覧回数の少ないサイクルは検出率が高くなるため，A 区分のサイクル

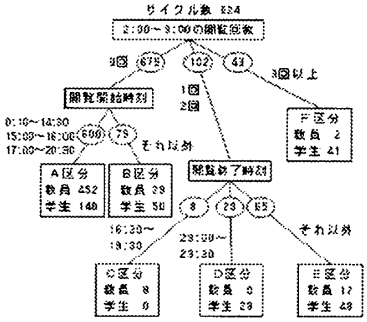

図 1　教員と学生を分類する決定木

は，検出率が高くなる可能性がある．そこで A 区分の条件を満たすサイクルの平均検出率を求めたところ 90.1%となり，遅延評価を用いた場合の平均検出率 89.3%を上回った．よって，朝～夕方に職場などで閲覧を開始する教員に関しては遅延評価がより有効に働くと考えられる．

D，F 区分では学生の割合が大きい．D 区分のサイクルは 2:00～3:00 に閲覧し，かつ閲覧終了時刻が遅いため，使用時間が長いと予想される．F 区分のサイクルは 2:00～3:00 に 3 回以上閲覧しているため，定期閲覧などで閲覧回数が多くなっていると考えられる．よって両区分のサイクルは検出率が低くなる可能性がある．区分の条件を満たすサイクルの平均検出率を求めると，D 区分 81.9%，F 区分 83.7%と，共に 89.3%を下回った．よって夜遅くに閲覧を行う学生や，定期閲覧などで深夜に一定回数以上閲覧する学生については，大きな効果は期待できないと考えられる．

6. まとめ

本稿ではユーザのメール閲覧サイクルと遅延評価の有用性について評価を行った．その結果，遅延評価を用いた場合の平均検出率は 89.3%であるが，閲覧回数が 1 回のみのサイクルでは 93.1%，使用時間が 1 時間未満のサイクルでは 93.0%であり，サイクルと遅延評価には関連があると示せた．また教員，学生というユーザ群と遅延評価の有用性について評価した結果，朝～夕方に閲覧を開始する教員の平均検出率は 90.1%，夜遅くに閲覧する学生は 81.9%，深夜の閲覧が多い学生は 83.7%であり，ユーザ群における区分によっても遅延評価の効果が異なることが判明した．

7. 今後の展望

本稿では教員と学生という 2 つのユーザ群を用意し分析を行ったが，今後は教員と学生以外のユーザ群に対しても，遅延評価の有用性について調査を進めていきたい．

参考文献

[1]symantec, “The State of Spam A Monthly Report - May 2008”
[2]田代 有里, “spam メールによる国民経済的損失”, ISFJ 日本政策学生会議, 産業競争政策 001 (2006)
[3]松浦 広明, 齋藤 彰一, 上原 哲太郎, 和田 俊和, “データベースに基づくサーバサイド迷惑メール検出システム”, 電子情報通信学会論文誌, Vol.J88-B, No.10, pp.1934-1943 (2005)
[4]連 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”, 情報処理学会研究報告, 2004-DPS-117/2004-CSEC-24, pp.139-144 (2004)
[5]J. R. Quinlan, “Induction of decision trees,” Machine Learning, Vol.1, pp.81-106 (1986)
[6]J. R. Quinlan, C4.5: Programs for Machine Learning, Morgan Kaufmann, San Mateo, CA (1993)