RO-004

ユーザのメール取得間隔と遅延評価を用いた IP アドレスフィルタの効果との関連調査

Relationships between Mail Fetching Patterns and Effects of IP Address Filter on Lazy Evaluation

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ている．迷惑メールとは受信者の意向を無視して大量送信されるメールを指し，その内容は商品の紹介やワンクリック詐欺，ウィルスを含んだメールなど多種多様である．また symantec 社による 2009 年 3 月の迷惑メールに関するレポート[1]によると，世界に流通するメールの約 86%が迷惑メールであるとされている．また迷惑メールの通信量の多さはネットワークのトラフィックに多大な影響を及ぼしているため，社会的に大きな問題となっている．

この迷惑メールの被害を抑えるための手法として，迷惑メールフィルタが挙げられる．迷惑メールフィルタとは，メールが迷惑メールかそれ以外のメール(以後正当なメール)かを判別する手法である(またフィルタを用いることをフィルタリングと呼ぶ)．一般的なフィルタは，メールが迷惑メールかどうかの判定を行い，迷惑メールであった場合は隔離もしくは削除，迷惑メールではなかった場合はメールボックスやユーザに配送，という挙動をとる．メールを迷惑メールだと判定することを検出と呼び，判定にかけた迷惑メール数に対して検出できた迷惑メール数が占める割合のことを検出率と呼ぶ．ユーザはフィルタを導入することで迷惑メールを受け取ることなく，電子メールを利用することができる．

しかし迷惑メールフィルタの種類によっては，検出率が高い一方で False Positive(本論文では False Positive を，正当なメールを迷惑メールだと判断する誤検出と定義する)が無視できない量で発生するという現象も見受けられる．False Positive が多いフィルタは，本来ユーザが受け取りたい正当なメールがユーザに配送されないといった事態を頻繁に引き起こしてしまうため，極力 False Positive は少なくする必要がある．

また迷惑メールの内容について，2009 年 1 月には全体の 23%を占めた一般的な商品(機器や服など)についての迷惑メールが 2009 年 2 月には 15%となっており，インターネットやレジャー施設についての迷惑メールが増加傾向にあることが symantec 社によって報告されている[1]．この報告が示すように，流通する迷惑メールの内容は日々変化している．よって迷惑メールフィルタは，検出率が高いこと以外にも，次の要件を満たすことが必要だと言える．

(1) 様々な内容の迷惑メールに柔軟に対応できる
(2) False Positive の発生確率が低い

そこで本論文では，調整によって(1)(2)の要件を満たすことが可能な IP アドレスフィルタ(2.2 節参照)に，遅延評価(2.3 節参照)と呼ばれる検出率を上げる手法を導入したシミュレーションを行い，遅延評価に効果が期待できるかを調査する．またユーザがメールを取得する間隔と，遅延評価による検出率の増加効果との関連を調査し，定量的な評価を行うことで，ユーザのメール取得間隔が遅延評価の効果に与える影響の度合いを調査する．

2. 関連研究

2.1 事例ベース型フィルタ

事例ベース型フィルタは，同一内容の迷惑メールが複数のユーザに送信されるという迷惑メールの特徴を利用しており，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．複数のユーザでデータベースを共有することから，分散協調型フィルタとも呼ばれる．このフィルタはユーザが既知の迷惑メールを登録するという特性上，False Positive の発生率が無視できる程小さくなるという特徴がある．

しかし事例ベース型フィルタの欠点として，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という点が挙げられる．松浦らの研究[2]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

迷惑メールの中継を許すサーバ(以後踏み台サーバ)の IP アドレスを列記したデータベースをブラックリストと呼ぶ．IP アドレスフィルタは，メールを受け取ったユーザがそのメールを配送したメールサーバの IP アドレスをこのブラックリストに問い合わせ，迷惑メールをブロックする手法である．このブラックリストというデータベースの名称か

† 東京理科大学大学院 理工学研究科 情報科学専攻
Dept. of Information Sciences, Graduate School of Science and Technology Tokyo University of Science
distinct@mt.is.noda.tus.ac.jp
†† 清水建設 株式会社
SHIMIZU CORPORATION
††† 東京理科大学 理工学部 情報科学科
Dept. of Information Sciences, Tokyo University of Science

* F. J. Tobin, "Pyzor," http://pyzor.sourceforge.net/

ら，別名ブラックリスト方式とも呼ばれる．データベースは DNS(Domain Name System)上に構築されることから，DNSBL(DNS Base Blackhole List)あるいは RBL(Realtime Blackhole List)と呼称される(以後は DNSBL で統一する)．この DNSBL に登録される IP アドレスは，DNSBL を運用するサービスのポリシーによって決定される．

IP アドレスフィルタの特徴として，運用するサービスが世界中に存在していること，選出した DNSBL によって検出できる迷惑メールが大きく異なることが挙げられる．しかし，踏み台サーバの IP アドレスが登録されるということは，確かに迷惑メール送信者は同じ経路を使用しての送信行為が不可能になるが，同時に踏み台サーバからの正当なメールも受け付けなくなってしまう．加えて一部の DNSBL では，迷惑メールを送信している踏み台サーバの近くに迷惑メール送信者がいると判断して(例えば IP アドレスにおける)近辺のサーバをすべて DNSBL に登録する，といった挙動をとる．この場合，False Positive の可能性が極めて増加することになる．また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．

IPアドレスフィルタは調整によって1章の要件(1)(2)を満たすことが可能となる．(1)については，複数のDNSBLを用いることで様々な内容の迷惑メールに対応できる．(2)については，DNSBL重ね合わせ検出(複数のDNSBLに検出されたメールのみ迷惑メールだと判定する手法)によって，False Positiveの発生確率を低くすることが可能であることが先行実験[3]により判明している．

2.3 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データベース(IP アドレスフィルタの場合は DNSBL)を用いてフィルタリングを行い，そのデータベースは常に更新され続けているために時間経過によって充実する，という共通の特性を持つ．これらのフィルタリングは，メールがメールサーバに到着した時点でデータベースに問い合わせを行う．よって，メールサーバ到着時点で迷惑メールだと判断されなかったメールは，たとえ迷惑メールであってもそのままメールボックスに保存され，ユーザからの受信要求に従ってユーザの手元に配送されてしまう．

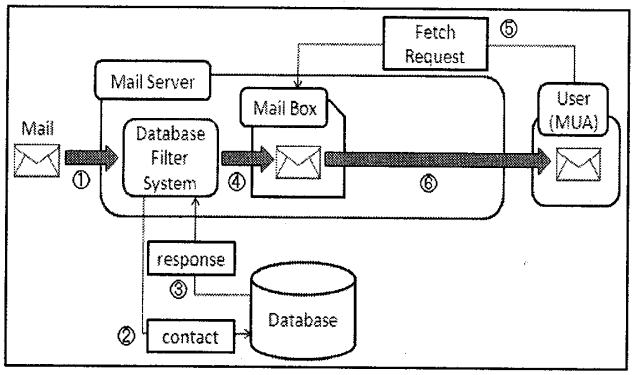

図 1 : 通常のデータベースフィルタ

通常のデータベースフィルタのプロセスを示す(図 1).

① メールがメールサーバに到着する．
② メールサーバがデータベースに問い合わせを行う．
③ データベースが，メールが迷惑メールか否かを返す．
④ メールが迷惑メールではないと判断された場合，メールサーバはメールボックスにメールを配送する．迷惑メールだと判断された場合は破棄する．
⑤ ユーザが MUA(メールクライアント)を用いて，メールサーバにメールの取得要求を行う．
⑥ メールサーバがユーザにメールを配送する．

しかしこれらのフィルタリングは，問い合わせを行うタイミングを，メールがメールサーバに到着した時刻から，ユーザがメールサーバからメールを取得する時刻に遅らせることで，メールサーバ到着時にデータベースに登録されていなかった迷惑メールがメールの取得時には新たに登録されており，再度データベースに問い合わせることで迷惑メールを検出できる可能性がある．この手法は問い合わせ時間を故意に遅らせることから遅延評価と呼ばれる．この遅らせた時間(メール到着時からメール取得時までの時間)を遅延時間と呼ぶ．

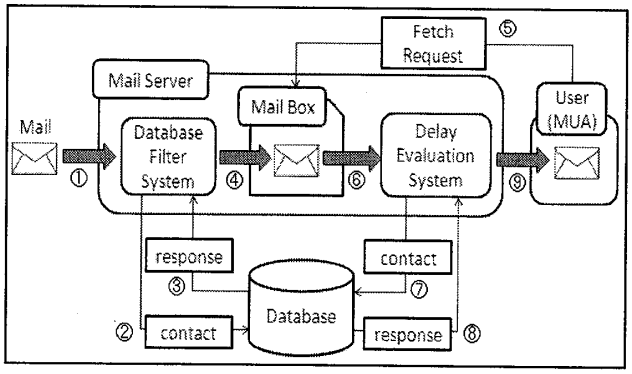

図 2 : 遅延評価を用いたデータベースフィルタ

遅延評価を用いたデータベースフィルタのプロセスを示す(図 2).

① メールがメールサーバに到着する．
② メールサーバがデータベースに問い合わせを行う．
③ データベースが，メールが迷惑メールか否かを返す．
④ メールが迷惑メールではないと判断された場合，メールサーバはメールボックスにメールを配送する．迷惑メールだと判断された場合は破棄する．
⑤ ユーザが MUA を用いて，メールサーバにメールの取得要求を行う．
⑥ ユーザへのメール配送前に，遅延評価システムが作動する．
⑦ ②と同様．
⑧ ③と同様．
⑨ メールサーバがユーザにメールを配送する．ただし⑧で迷惑メールだと判断された場合は破棄する．

遅延評価については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[2]によると，和歌山大学システム工学部のメールサーバに事例ベース型フィルタを用いたメール検出システムを組み込み，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．

3. 実験

3.1 実験目的

松浦らの報告[2]では事例ベース型フィルタにおいて遅延評価は有効であるとされているが，事例ベース型フィルタと同様に，時間経過によって充実するデータベースを使用する IP アドレスフィルタにおいても遅延評価は有効であると考えられる．加えて，IP アドレスフィルタは比較的検出率が高いため(2.2 節参照)，検出率の低い事例ベース型フィルタに遅延評価を導入した場合(2.1 節参照)より高い効果が期待できる．

また，遅延時間はメールサーバにメールが到着する時刻とユーザがメールを取得する時刻で定義されるため，メール到着時刻が一意に定まる場合でも，ユーザによってメールを取得する時刻が異なればユーザごとにその遅延時間は異なる．従って遅延時間を用いる遅延評価はユーザによって遅延評価の効果が異なる可能性がある．

そこで本論文では，ユーザが遅延評価導入時に得られる効果について定量的な評価を行うため，IP アドレスフィルタにおける遅延評価のシミュレーションを行い，ユーザごとに遅延評価の効果を調査した．

3.2 実験環境

遅延評価の仮想実験にあたり，遅延評価に利用する遅延時間は，メールがメールサーバに到着する時刻とユーザがメールを取得する時刻によって定義されるため，以下の 2 つの分布を定義し作成した．

(1) 迷惑メールの到着分布(3.2.1 節参照)
迷惑メールがメールサーバに到着する時刻を定義

(2) ユーザのメール取得分布(3.2.2 節参照)
ユーザがメールを取得する時刻を定義

3.2.1 迷惑メールと正当なメールの収集

迷惑メールの収集を行うため，本実験用にメールサーバ(Ubuntu 8.04.2，Postfix + Dovecot)を用意し，サーバに迷惑メールの収集を行うメールアドレスを 1 つ作成した．このメールアドレスをインターネット上に公開し，無差別に送られる迷惑メールの対象とすることで，迷惑メールの収集を行った．収集期間を 2009/3/14～2009/3/31 と定めたところ，1 日あたり 40 通～120 通の迷惑メールが到着し，収集期間全体で 1572 通の迷惑メールを収集することができた(収集後はすべてのメールが迷惑メールであることを確認した)．そして，これら迷惑メールがメールサーバに到着した時刻を秒単位で記録し続けることで，迷惑メールの到着分布を定義した．

また，DNSBL の重ね合わせを用いるため(3.3 節に後述)，False Positive について検証する必要がある．よって前述のメールサーバとは別にメールサーバ(CentOS 5.3, Postfix + Dovecot)を用意し，正当なメールを収集するメールアドレスを作成した．収集期間を 2009/3/14～2009/3/31 と定めたところ，1 日あたり 5 通～10 通の正当なメールが到着し，収集期間全体で 106 通の正当なメールを収集することができた(収集後はすべてのメールが正当なメールであることを確認した)．

3.2.2 ユーザのメール取得分布

実験対象のユーザとして本学学生 11 名と教員 15 名の計 26 名を選んだ．そのユーザらが使用するメールサーバにおける 2009/3/14～2009/3/31 の POP/IMAP ログから，各ユーザのメール取得時刻を秒単位で抽出することで，メールの取得分布を定義した．その結果，対象ユーザ 26 名から 26 種類のメール取得分布が作成できた．

3.3 実験手法

あるメール取得分布に対しての検出率を求める方法を示す．1 つのメール取得分布を選び，各迷惑メールの到着時刻(迷惑メールの到着分布に従う)から，その時刻以降で最も近いメール取得時刻までの時間を遅延時間とする．到着時刻以降で 2009/3/31 以前にメール取得が無い迷惑メールは遅延時間が定義できず遅延評価の対象とはならないため，遅延時間が定義可能な迷惑メールのみを検出対象メールとする．

ここで検出について，重ね合わせ検出[3](2.2 節参照)によって何種類の DNSBL に登録されていた場合に検出と判断するのが適しているかを調べる．収集した迷惑メールと正当なメール(3.2.1 節参照)から，各メールを配送したメールサーバの IP アドレス 1572 件を 6 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が全体の 85.5%であった．一方，正当なメールを配送したメールサーバの IP アドレス 106 件を問い合わせた結果，同条件で検出された正当なメールは 4.8%であった．よって False Positive は 4.8%となる．また 2 種類に検出された迷惑メールが 73.4%(正当なメールが 0.0%)，3 種類に検出された迷惑メールは 59.6%(正当なメールが 0.0%)であった．よって，迷惑メールが 2 種類の DNSBL に登録されていた場合に検出されたと判断することで，十分に False Positive が低いと判断できる．問い合わせに用いた 6 種類の DNSBL を以下に示す．

- bl.spamcop.net
- dnsbl-1.uceprotect.net
- dnsbl.sorbs.net
- psbl.surriel.com
- ubl.unsubscore.com
- xbl.spamhaus.org

また，迷惑メール到着時以降も各 DNSBL に問い合わせ続け，そのメールが各 DNSBL に登録された時刻を記録することで，メール到着時には登録されずメール取得時には登録されている迷惑メールを判断することが可能である．

その結果を用いて，検出対象メールを以下の 3 パターンに分ける．

- 遅延評価無しの検出メール
  迷惑メールの到着時刻に行う DNSBL 問い合わせで，2 種類以上の DNSBL に登録されていた迷惑メール

- 遅延評価による追加検出メール
  迷惑メール到着時刻の DNSBL 問い合わせでは 1 種類以下の DNSBL にのみ登録されていたが，メール取得時刻の問い合わせでは 2 種類以上の DNSBL に登録されていた迷惑メール

- 未検出メール
  メール取得時刻の DNSBL 問い合わせでも 1 種類以下の DNSBL にしか登録されていなかった迷惑メール

また，検出率は次式により定義する．

(A) 遅延評価無しの場合の検出率(%)
= (遅延評価無しの検出メール数(通)
/ 検出対象メール数(通)) * 100

(B) 遅延評価有りの場合の検出率(%)
= {(遅延評価無しの検出メール数(通)
+ 遅延評価による追加検出メール数(通))
/ 検出対象メール数(通)} * 100

この手法をメール取得分布すべてに適用することで，各メール取得分布に対応した(A)遅延評価無しの場合の検出率と，(B)遅延評価有りの場合の検出率を得ることができる．

3.4 実験結果

すべてのメール取得分布に対して(A)(B)を求めた．また，(B)式の“遅延評価による追加検出メール数”による検出率の増加分を遅延評価の効果とし，(B)-(A)によって求めた．この結果に関しての詳細(各ユーザのメール取得分布ごとの，検出対象メール数，(A)，(B)，(B)-(A))を表 1 に示す．

表 1 : ユーザのメール取得分布に対する検出率

ユーザ	検出対象メール数(通)	(A)(%)	(B)(%)	(B)-(A)(%)
1 学生	1556	73.4	86.5	13.1
2 学生	1560	73.5	82.5	9.0
3 学生	1534	73.3	86.8	13.5
4 学生	1547	73.3	86.3	13.0
5 学生	893	70.2	79.8	9.6
6 学生	1557	73.4	75.7	2.3
7 学生	1553	73.4	86.5	13.1
8 学生	1560	73.5	76.0	2.5
9 学生	1557	73.4	85.6	12.2
10 学生	1540	73.4	85.8	12.4
11 学生	1560	73.5	74.9	1.4
12 教員	1553	73.4	80.6	7.2
13 教員	1553	73.4	81.3	7.9
14 教員	1164	71.0	85.7	14.7
15 教員	1548	73.3	86.3	13.0
16 教員	1377	72.6	85.6	13.0
17 教員	1372	72.6	83.2	10.6
18 教員	1543	73.3	81.6	8.3
19 教員	1553	73.4	82.2	8.8
20 教員	1553	73.4	86.5	13.1
21 教員	1547	73.3	85.3	12.0
22 教員	1444	73.1	87.8	14.7
23 教員	1451	73.1	86.8	13.7
24 教員	1553	73.4	81.2	7.8
25 教員	1554	73.4	83.8	10.4
26 教員	1444	73.1	87.2	14.1

4. 考察

4.1 IP アドレスフィルタにおける遅延評価の効果

表 1 の実験結果より，(A)遅延評価無しの場合の平均検出率を求めたところ 73.0%となり，(B)遅延評価有りの場合の平均検出率は 83.0%となった．また，遅延評価の効果の平均は 10.0%となった．この結果より，IP アドレスフィルタは遅延評価によって新たに迷惑メールを検出することが可能であり，IP アドレスフィルタにおいて遅延評価は有効であることが判明した．また，本実験における遅延評価の効果(10.0%)は，事例ベース型フィルタを用いたメール検出システムにおいて遅延評価を実装した実験[2](2.3 節参照)の効果(5.8%)を上回り，事例ベース型フィルタにおける遅延評価よりも効果が大きいことが示せた．

またメール取得分布ごとではなく，学生や教員といったユーザ群ごとに遅延評価の効果が異なる可能性がある．そこで表 1 のデータより，学生のみと教員のみに限定して(A)と(B)の平均検出率を求めたところ，学生のみの場合は(A)が 73.1%であるのに対し，(B)が 81.6%となり(A)を 8.5%上回った．教員のみの場合は(A)が 72.8%であるのに対し，(B)が 84.4%となり(A)を 11.6%上回った．この結果から，遅延評価の効果は学生と教員で大きく異なることが判明した．教員の方が学生に比べて遅延評価の効果が高いが，これについては学生と教員のメールを取得する頻度が関連していると考えられる．1 日を 1 時間ごとに区切り，学生と教員それぞれについてメール取得回数と総取得回数の合計を算出し，メール取得回数の総取得回数に対する割合を求めた結果が図 3 である．

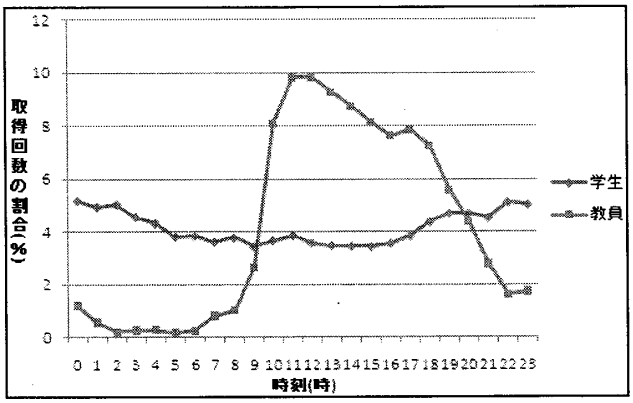

図 3 : 学生と教員のメール取得頻度

図 3 より，学生は常に取得を行うのに対し，教員は 10:00～22:00 に集中して取得を行う傾向にあることが分かる．教員の場合は深夜～朝にかけて取得を控えているため，その時間は DNSBL が更新され続ける．よって常に取得を行うために遅延時間が比較的短くなる学生より，教員の方が長い遅延時間を持っているため，教員は学生よりも遅延評価の効果が大きくなったと考えられる．

4.2 遅延時間と遅延評価の効果の関係

2.3 節で述べたように遅延評価は，メールサーバへの到着時に登録されていなかった迷惑メールが遅延時間中にデータベースに登録されることを期待して，ユーザがメールを取得する時刻に再びデータベースに問い合わせを行う手法である．よって遅延時間中にデータベースが充実することを考えると，遅延時間が長いほど迷惑メールを検出できる可能性が高くなると考えられる．そこで遅延時間と遅延評価の効果の関連を調べた．

1 つのメール取得分布を選び，本実験で用いた 1572 通すべての迷惑メールの遅延時間を求め，その遅延時間の平均をとる．この手法をすべてのメール取得分布に対して適用することで，メール取得分布ごとに平均遅延時間を求めた．平均遅延時間と遅延評価の効果(表 1 参照)について作成した散布図を図 4 に示す．

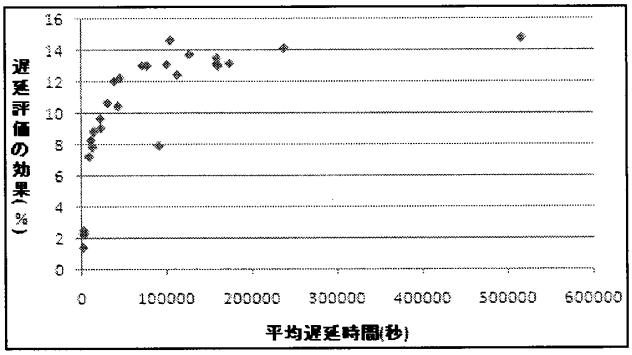

図 4 : 平均遅延時間と遅延評価の効果の関係

図 4 より，遅延評価の効果は平均遅延時間の増加に伴い対数的に増加すると予想できる．そこで平均遅延時間に自然対数変換を行った値と，遅延評価の効果について再度作成した散布図が図 5 である(図 5 の回帰直線については後述)．

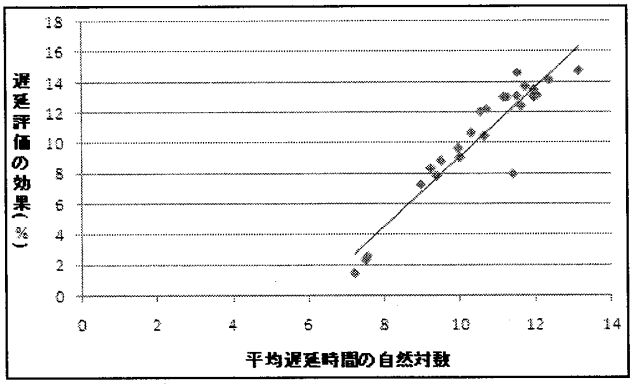

図 5 : 平均遅延時間の自然対数と遅延評価の効果から導出される回帰直線

図 5 より遅延評価の効果は，平均遅延時間の自然対数の増加に伴い比例的に増加する(すなわち平均遅延時間の増加に伴い対数的に増加する)と予想される．そこで図 5 より単回帰分析によって回帰直線を導出し，回帰直線がデータに当てはまっているかの検定を行うことで，比例的に増加しているかを調べた．

4.2.1 単回帰分析による回帰直線の導出

単回帰分析とは，n 個の標本について説明変数の値 x_i と目的変数の値 y_i が与えられているとき，x_i の値から y_i の値を予測する回帰直線$\hat{y}_i = \alpha + \beta x_i$を導出する手法である．この式の未知の母数である α と β を推定する手法として，一般的に最小 2 乗法[5]が用いられる．最小 2 乗法とは誤差項 $y_i - \alpha - \beta x_i$ の 2 乗和を最小にする α，β(これを$\hat{\alpha}$，$\hat{\beta}$で表す)を$(x_i, y_i)(i=1, 2, \ldots, n)$を用いて推定する方法である．

ここで x_i に平均遅延時間の自然対数，y_i に遅延評価の効果を与え，最小 2 乗法を適用すると$\hat{\alpha}$ = -0.138，$\hat{\beta}$ = 0.023 となり，回帰直線の式は$\hat{y} = 0.023x - 0.138$で表せる(図 5)．

4.2.2 回帰直線の検定

回帰直線がデータの何割程度を説明できているかを確かめる尺度として決定係数[6]が挙げられる．単回帰分析における決定係数は相関係数の 2 乗で求められる．相関係数は 2 つの変数の間の相関を表す統計学的指標であり，絶対値が 0.70 以上であれば強い相関があるとされている．n 個の標本について説明変数の値 x_i と目的変数の値 y_i が定められていれば相関係数ρ_{xy}を求めることが可能である．

ここで x_i に平均遅延時間の自然対数，y_i に遅延評価の効果を与え，相関係数を導出するとρ_{xy}=0.940 となり，強い正の相関があることが判明した．また，それを 2 乗した決定係数は 0.884 となったため，この回帰直線はデータの 8 割以上を説明できていることが示せた．決定係数は 0.7~0.8 以上であれば十分データに当てはまっているとされるため，この回帰直線はデータへの当てはまりが良いと言える．よって回帰直線の式$\hat{y} = 0.023x - 0.138$より，遅延評価の効果は平均遅延時間の自然対数の増加に伴い比例的に増加するこ

と，すなわち平均遅延時間の増加に伴い対数的に増加することが示せた．

図 4 において，平均遅延時間が 0～100,000 秒の間は遅延評価の効果が大きく上昇するが，図 4 は対数的に増加しているため 100,000 秒以降の上昇量は微小である．よって IP アドレスフィルタに遅延評価を導入する場合は同様の分析を行い，少なくとも基準となる遅延時間(本論文の実験では 100,000 秒)はメール取得を控えることで，遅延評価に大きな効果を期待することができる．

4.3 メール取得分布と遅延評価の効果の関係

遅延評価において，ある迷惑メールに対して遅延時間を求めることを考えると，その遅延時間はユーザがメールを取得する時刻によって異なるため(4.1 節に記述したように，特に教員は 10:00～22:00 とそれ以外の時間で取得頻度が大きく異なる)，遅延時間を利用する遅延評価の効果はユーザのメール取得分布に影響を受けると考えられる．そこで，遅延時間に関連するメール取得分布の特徴量として，メール取得分布ごとに平均メール取得間隔，10:00～21:59 の平均メール取得間隔，22:00～9:59 の平均メール取得間隔，最長メール取得間隔を抽出し(定義は下記参照)，遅延評価の効果との関連を調べた．各メール取得分布から抽出した特徴量を表 2 に示す．

(1) 平均メール取得間隔(秒)
2009/3/14～2009/3/31 における，ユーザのメール取得要求ごとの間隔を秒数で抽出し，平均をとった値

(2) 10:00～21:59 の平均メール取得間隔(秒)
平均メール取得間隔と同様だが，ある取得要求とその次の取得要求がともに 10:00～21:59 に入っているときのみ，その取得要求の差によって間隔を求める

(3) 22:00～9:59 の平均メール取得間隔(秒)
時間以外は 10:00～21:59 の平均メール取得間隔と同様

(4) 最長メール取得間隔(秒)
2009/3/14～2009/3/31 における，ユーザのメール取得要求ごとの間隔を秒数で抽出した中での最大値

表 2 : 各メール取得分布から抽出した特徴量

ユーザ	(1)	(2)	(3)	(4)
1 学生	27,082	3,755	498	509,398
2 学生	5,335	2,005	1,429	130,147
3 学生	55,976	2,034	1,678	553,060
4 学生	92,959	2,532	1,678	254,659
5 学生	3,703	2,339	1,279	158,991
6 学生	3,604	2,827	2,162	28,798
7 学生	98,188	2,909	2,163	394,447
8 学生	2,460	2,626	2,275	32,624
9 学生	28,785	2,726	2,259	249,369
10 学生	7,879	2,603	2,231	476,881
11 学生	2,527	2,570	2,304	28,591
12 教員	2,551	1,375	2,405	48,887
13 教員	5,184	1,550	2,125	329,433
14 教員	25,544	1,498	2,103	338,166
15 教員	44,292	1,599	2,098	572,037
16 教員	44,463	1,708	2,098	268,484
17 教員	1,465	940	1,827	173,359
18 教員	2,872	1,070	1,751	47,935
19 教員	3,304	1,110	1,846	66,981
20 教員	30,561	1,117	1,836	639,170
21 教員	11,841	1,148	1,802	143,768
22 教員	31,511	1,148	1,802	1,251,743
23 教員	42,185	1,153	1,783	334,496
24 教員	1,444	1,016	1,649	75,436
25 教員	1,858	906	1,524	231,053
26 教員	176,472	905	1,524	595,479

関連を調べる手法として，4.2 節と同様に散布図を作成する．各特徴量と遅延評価の効果を表した散布図を示す(図 6～図 9)．ただし図 7，図 8 の遅延評価の効果に関しては，(2)と(3)の定義によって取得要求の時間が限定されているため，検出対象メールもそれぞれ該当する時間に取得が行われたメールのみに限定した．また，限定したことで検出対象メールが存在しなくなったメール取得分布の遅延評価の効果は 0 と定義した．

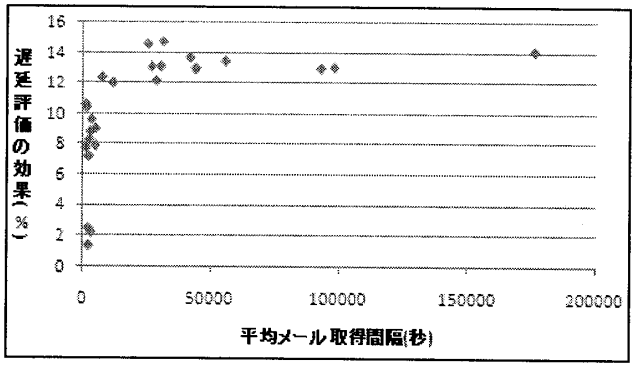

図 6 : 平均メール取得間隔と遅延評価の効果の関係

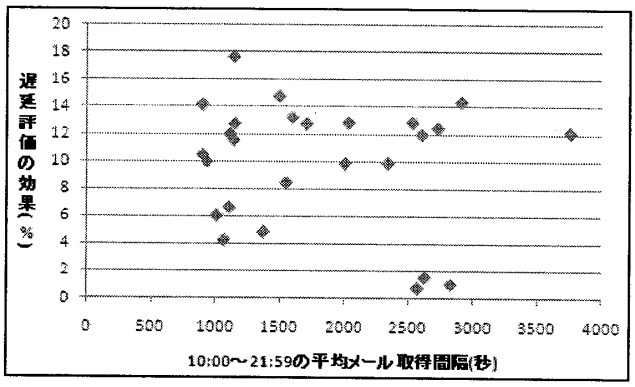

図 7 : 10:00～21:59 の平均取得間隔と遅延評価の効果の関係

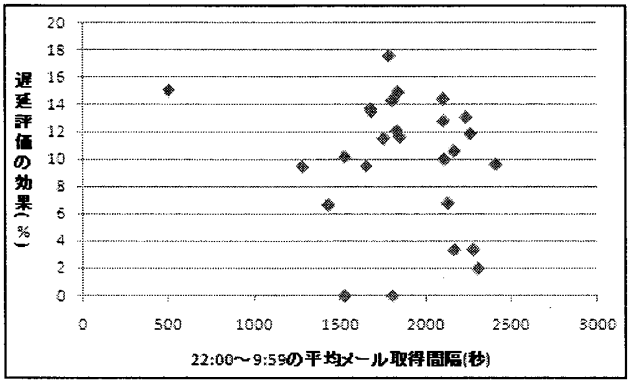

図 8 : 22:00～9:59 の平均取得間隔と遅延評価の効果の関係

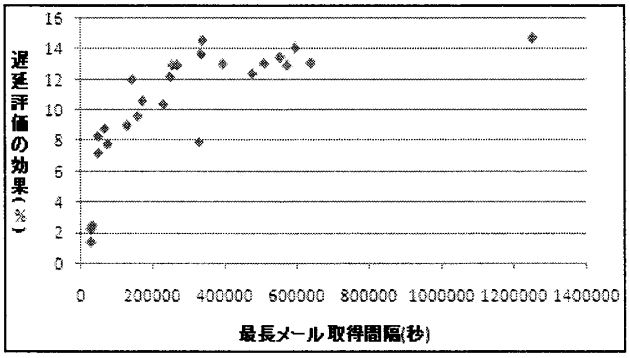

図 9 : 最長メール取得間隔と遅延評価の効果の関係

図 7，図 8 はともに，特徴量と遅延評価の効果に関連がないと考えられる．この原因として，ある時間帯に限定して特徴量を抽出すると，その時間帯以外に行われた取得要求による遅延評価の効果が無視されるため，メール取得分布の特徴を適切に表せないと考えられる．例えば 12:00，23:00，23:01 に取得要求を出すような取得分布の場合，12:00～23:00 の 11 時間の間隔は考慮されず，23:00～23:01 の 1 分間の間隔のみが特徴量として抽出されてしまう．

図 6，図 9 はともに対数的に増加すると予想されるため 4.2 節と同様に，x_i に各特徴量(明らかに関連があるとは言えない(2)と(3)は除く)の自然対数，y_i に遅延評価の効果を与え，回帰直線を導出して検定を行うことで，変化量が定量的に増加するかを調べた．その結果を表 3 に示す．

表 3 : 特徴量の自然対数から求めた回帰直線の検定

	平均メール取得間隔	最長メール取得間隔
回帰直線	$\hat{y} = 0.019x$ - 0.075	$\hat{y} = 0.032x$ - 0.286
相関係数	0.742	0.894
相関関係	強い正	強い正
決定係数	0.551	0.800
当てはまり	悪い	良い

表 3 より，平均メール取得間隔については回帰直線の当てはまりが悪いことが判明した．この原因として，例えば極端に長いメール取得間隔と極端に短いメール取得間隔を両方持つメール取得分布の場合，平均メール取得間隔はそのメール取得分布の特徴を適切に表せていない可能性があることが考えられる．回帰直線の当てはまりが悪いため遅延評価の効果の増減を定量的に把握するのは難しいが，相関係数は 0.742 であり強い正の関連があることが示せた．最長メール取得間隔については当てはまりが良く，回帰直線の式$\hat{y} = 0.032x - 0.286$ より，遅延評価の効果は最長メール取得間隔の自然対数の増加に伴い比例的に増加すること，すなわち最長メール取得間隔の増加に伴い対数的に増加することが示せた(図 10).

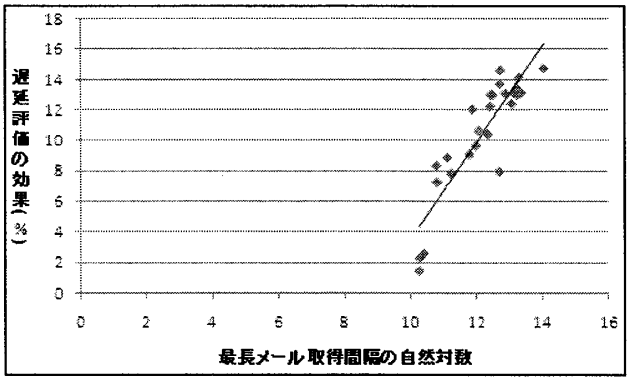

図 10 : 最長メール取得間隔の自然対数と遅延評価の効果から導出される回帰直線

この結果より，IP アドレスフィルタに遅延評価を導入するユーザは自身の最長メール取得間隔を考慮することで，遅延評価の効果を高めることが可能である．例えば MUA の設定によって 30 分ごとの定期取得を行うユーザの場合，最長メール取得間隔も 30 分(=1800 秒)と短く，遅延評価に大きい効果は期待できない．そのようなユーザは定期取得を控え，メールを閲覧する時刻にのみメール取得を行い，最長メール取得間隔を延ばすことで遅延評価の効果改善が可能である．

また 4.1 節より学生と教員で効果が異なることが判明しているため，この分析は学生と教員が属する組織に IP アドレスフィルタと遅延評価を導入する際に，得られる効果について指針を提供できる．例えば大学に導入する際に学生には効果が小さいと判明していれば，前述の手段を学生に適用することで，学生に対して効果の向上が期待できる．またユーザ群を増やして分析を行うことで，学生や教員以外が属する組織に対しての指針提供も可能であると考えられる．

5. まとめ

本論文では IP アドレスフィルタにおける遅延評価の効果を調べるため遅延評価のシミュレーションを行い，遅延評価の効果に対して定量的な評価を行った．その結果，遅延評価無しの場合の平均検出率は 73.0%であるのに対し，遅延評価有りの場合の平均検出率は 83.0%となり，遅延評価は有効であることが示せた．その効果は 10.0%であり，事例ベース型フィルタに遅延評価を導入した場合よりも効

果が高いことが判明した．

また，学生は遅延評価によって平均検出率が 73.1%から 81.6%に上がったが(8.5%の効果)，教員は平均検出率が 72.8%から 84.4%に上がり(11.6%の効果)，学生や教員といったユーザ群によっても効果が異なることが判明した．

そして，ユーザのメール取得分布から抽出した各特徴量の自然対数 x_i と遅延評価の効果 y_i の回帰直線を求めた結果，最長メール取得間隔の式は $\hat{y} = 0.032x - 0.286$ となり，最長メール取得間隔によって遅延評価の効果は対数的に増加することが判明した．よって IP アドレスフィルタに遅延評価を導入するユーザや組織は，最長メール取得間隔を考慮することで遅延評価による効果の向上を期待することができる．これより，本論文における分析はユーザや組織に対し，遅延評価の効果改善の指針を提供することが可能であると考えられる．

参考文献

[1] symantec, “The State of Spam A Monthly Report - March 2009”

[2] 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)

[3] 奥村 慎太郎, 鈴木 康介, 松澤 智史, 武田 正之, “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”, FIT2008, L-30, pp157-158 (2008)

[4] 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”, 情報処理学会研究報告, 2004-DPS-117/2004-CSEC-24, pp.139-144 (2004)

[5] 杉原 左右一, “統計学”, 晃洋書房, ISBN4-7710-1390-X, pp231-237 (2003)

[6] 武藤 眞介, “統計解析ハンドブック”, 朝倉書店, ISBN4-254-12061-3, pp220-221 (2001)