Analysis about recognition rate of spam mail by SpamAssassin

SpamAssassin による spam メール認識率に関する解析

Analysis about recognition rate of spam mail by SpamAssassin

松平　拓也*，車古　正樹*，井町　智彦*，中野　三智子*
Takuya MATSUHIRA，Masaki SHAKO，Tomohiko IMACHI，and Sachiko NAKANO

金沢大学
Kanazawa University

今日 spam メールは増加の一途を辿っており，電子メール配信のインフラにかかる負荷が深刻な問題となっている．そのため，spam メール対策は講じるべき優先課題の一つであるといえる．金沢大学では独自の spam メール対策システムを構築し，2004 年 10 月から運用を行っている．そして 2005 年 10 月からは SpamAssassin を導入し，より spam メール認識率の高いシステムの構築を目指している．本稿では，主に SpamAssassin の spam メール認識率について解析した結果について述べる．
キーワード：spam メール，SpamAssassin

Taking counter measures for spam mails is one of the most important tasks because of their heavy increment. In Kanazawa University, we constructed our own anti-spam systems, and have been operating it since October of 2004. And as a new system, we have started to use SpamAssassin since October of 2005. In this document, we discuss about the result of analysis about the accuracy of spam mail detention by using of SpamAssassin.
Keywords：spam mail，SpamAssassin

1. はじめに

近年，インターネットの急速な普及により電子メールはコミュニケーション手段として欠かせない存在となっている．しかしながら，spam メールは増加の一途を辿っており，電子メールの利便性が脅かされている．そのため，spam メール対策は講じるべき優先課題の一つであると考えられる．

金沢大学では 2003 年 11 月にトレンドマイクロ社製 Interscan Message Security Suite(以下IMSSと呼ぶ)[1]を導入し，本格的にspamメール対策を開始した．そして，2004 年 11 月にはspamメール対策システムの運用を開始し[2]，誤認識が少なく，かつユーザ及び管理者への負荷が最小限となるよう対策を講じており，spamメール対策に十分な効果をあげていると考えている[3]．そして，2005 年 10 月より，様々な側面からspamメールの判定を自動で行うことが可能である SpamAssassin[4]を導入し，より精度の高い spamメール対策システム構築を目指している．

本稿ではまず，SpamAssassin をどのような目的で採用したのかを説明した後，spam メール対策システムのどの部分に導入したのか説明を行い，SpamAssassin の運用によって得られた情報を基に SpamAssassin の spam メールの認識率について解析した結果について述べる．

2. 研究の目的

金沢大学では spam メールかどうかの判断は IMSS のコンテンツフィルタで行っている．そして，spam と判断したメールは隔離している．IMSS のフィルタ定義は管理者が手動で設定している．これはベンダ提供のフィルタでは誤認識が多いことが起因している．

IMSS のフィルタ定義を手動で行うには標

*総合メディア基盤センター
〒920-1192　金沢市角間町
Information Media Center
Kakuma, Kanazawa, 920-1192, Japan
E-mail：takusng@kenroku.kanazawa-u.ac.jp

本となるメールが必要である．これまでは定義者が，spam が利用しそうなキーワードを考えて標本メール抽出を行っていたが，最近は spam メールの内容が多様化しており，抽出できないメールが増加している．また，DHA (Directory Harvest Attack)による空メールや，形式に特徴のない spam メールは IMSS のコンテンツフィルタで定義することができない．これらの問題は全て，コンテンツフィルタが，正規表現が使えるとはいえ，パターンマッチングによる判定を行っていることが原因である．

そこで本研究では「spam らしさ」をスコアで判定することができる SpamAssassin を導入し，これまで手作業で行っていた IMSS のフィルタ定義作業を SpamAssassin で簡略化できるか検証するために，SpamAssassin の spam メール認識率の解析を行った．

3. SpamAssassin

SpamAssassin はメールのヘッダや本文を解析することで spam メールかどうかを判断するオープンソースソフトウェアである．

以下のようなルールにマッチすると，ルールに対応したスコアを累積加算していく．

- Received ヘッダの送信元・中継サーバの IP アドレスが DNSBL(DNS-Based Black hole List)に登録されているかどうか
- メール本文に記載されているメールアドレス，URL のドメイン(URI)が URIBL(URI Blackhole List)に登録されているかどうか
- メールの Subject，本文に特定の語句を含んでいないかどうか
- メールの形式が RFC に準拠しているかどうか

合計点数があらかじめ設定してある閾値を超えると spam メールであると判定する．

このように SpamAssassin では閾値を設定し，合計スコアが閾値を超えるかどうかで spam か非 spam であるかを判断するが，その時に想定される問題として，spam メールの取りこぼし(False Negative)と正規メールを spam と見なしてしまうこと(False Positive)があり，閾値との関係は表 1 の様になる．

表 1　SpamAssassin における閾値の設定

	メリット	デメリット
閾値を低く設定	False Negative が減る	False Positive が増える
閾値を高く設定	False Positive が減る	False Negative が増える

つまり，適切な閾値の決定が spam メールの認識率に大きく関わってくることになる．また，ルール毎の配点も spam メールの認識率に大きく関わってくる．現在，約 1 年の運用経験から閾値を 4.0 点に設定している．また，スコアの設定は TLEC (Tokyo Linux Entertainment Community)[5]が提供している設定ファイルをカスタマイズして使用している．

4. spam メール対策システム

SpamAssassin の spam メール認識率の解析方法を説明するにあたり，現在の spam メール対策システムの構成を説明する．

図 1 に 2006 年 11 月 1 日現在の金沢大学における spam メール対策システム構成図を示す．各構成サーバ及びシステムの詳細についてはメール配送経路順に以下で説明する．

4.1 対学外メール中継サーバ

学外から配送されてきたメールは全て対学外メール中継サーバに集めた後，SpamAssassin サーバへとリレーする．メール中継サーバを用意するのはトラブル等で SpamAssassin, IMSS のサービスが稼動していない場合に，全てのメールの受付を拒否

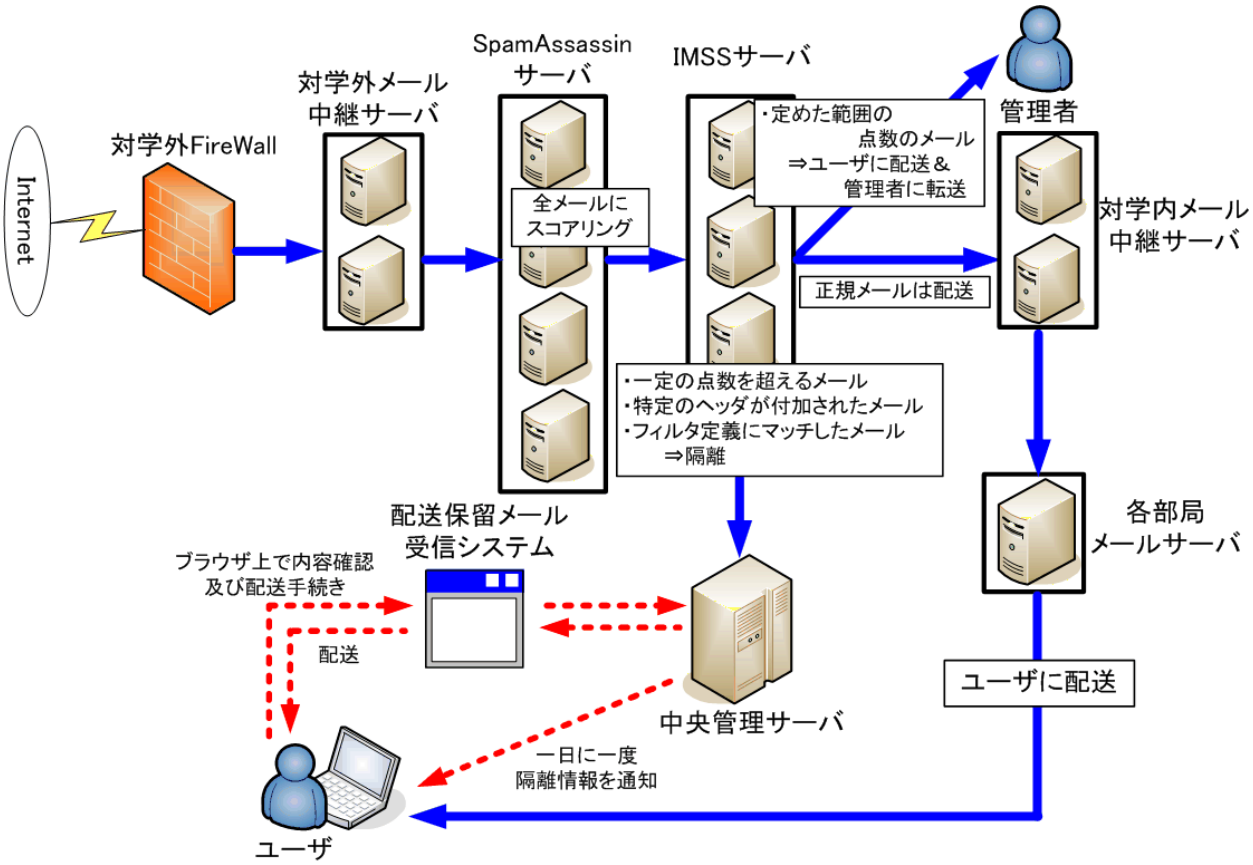

図 1　spam メール対策システム構成図

してしまう危険に対処する為である．また，大量の spam メールが到来しているメールアドレスのうちで実在しないものなど，特定のメールアドレス宛のメールはここで Reject し，以降のサーバに負荷をかけないようにしている．

4．2　SpamAssassin サーバ

対学外メール中継サーバからリレーしてきたメールは全て SpamAssassin サーバでスコアリングを行う．SpamAssassin の判定結果をメールのヘッダに埋め込んだ後，IMSS サーバにリレーする．SpamAssassin サーバは 4 台で構成しており，負荷分散及び冗長化を図っている．サーバは 1 台が高性能である為，これを主サーバとし，3 台を副サーバとして稼動している．主サーバ及び副サーバのスペックは表 2 に示すとおりである．また，MTA には Postfix2.2.11，SpamAssassin のバージョンは 3.1.7 を使用している．また，SpamAssassin への受け渡しはサイエンティフィック・システム研究会が公開しているスクリプト[6]を使用している．

表 2　SpamAssassin 稼動サーバのスペック

	主サーバ	副サーバ
台数	1	3
機種名	富士通 PrimePower250	富士通 PrimePower200
OS	Solaris10	Solaris8
CPU	SPARC64V (2GHz×2)	SPARC64GP (400MHz×2)
メモリ	4Gbyte	1Gbyte

4．3　IMSS サーバ

IMSS はコンテンツフィルタを用いて spam 判定を行っている．IMSS で spam と判定したメールは中央管理サーバに隔離する．IMSS で隔離するメールの条件は以下の通りである．

・ 管理者が登録した IMSS のフィルタ定義にマッチしたメール
・ SpamAssassin で一定のスコアを超えたメール（解析時は 12 点以上に設定）
・ SpamAssassin で特定のヘッダを付加した(特定のルールにマッチした)メール

なお，SpamAssassin の閾値は 4 点に設定しているが，False Positive を避ける為， 4～11.9 点のスコアがついたメールで，IMSS のフィルタ定義にマッチしなかったメールについては隔離を行わず，ユーザに配送するとともに標本メールとして管理者に転送する．管理者は標本メールを目視し，確実に spam と特定できるメールに関して適応したフィルタ定義を IMSS に追加する．IMSS のフィルタ定義にマッチせず，SpamAssassin でも閾値以下のメールは正規メールとしてユーザへ配送する．

4.4 配送保留メール受信システム

中央管理サーバに隔離したメールの情報は，1 日に 1 度，隔離したメールの From，To，Subject 及びメールを識別するためのメール ID のリストをユーザにメールで通知する．1 通のメールで通知することで spam メールにまぎれて重要なメールを見落とす危険性を減らすことができる.ユーザはその情報を基に，ブラウザ上で目的のメールを自動的に再配送することができるようにしており，ユーザ，管理者双方に負担がかからないように設計している．

4.5 メールの分類

spam メール対策システムにおけるメールの分類について説明する．図 2 にメールの分類のフローチャートを示す.

このように全てのメールは，Spam Assassin でスコアリング処理をした後，IMSS でフィルタリング処理を行う．IMSS

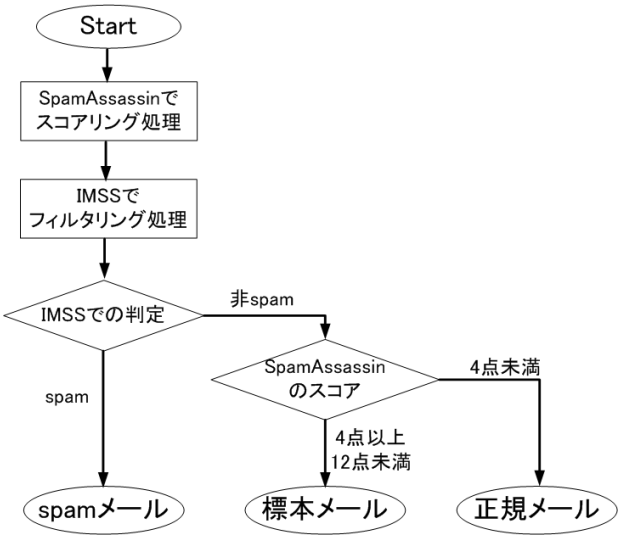

図 2　メール分類のフローチャート

で spam と判断したメールは「spam メール」として隔離する．IMSS で非 spam と判断したメールのうち，SpamAssassin のスコアが 4 点未満のメールは「正規メール」としてユーザに配送，12 点未満のメールはユーザに配送するとともに「標本メール」として管理者にも転送，12 点以上のメールは IMSS で spam メールとして判断し隔離する．

5. spam メール認識率の解析

5.1 解析方法

今回,以下の 3 つの視点から SpamAssassin の spam メール認識率の解析を行った．

1) IMSS との一致性

現在運用中のフィルタ定義のもとで，IMSS の spam メール認識率は，参考文献 3 にあるように非常に高いため，IMSS で隔離したメールのスコアが特定の閾値を超えているかどうかで SpamAssassin のスコアにおける spam メール認識率が測定できる．

2) 標本メールの内容

標本メールは IMSS では非 spam と判定したが SpamAssassin ではスコアが閾値を超えたメールである．つまり IMSS と SpamAssassin で判定の不一致が生じ

た場合ということになる．そこで，標本メールが spam かどうかを管理者が目視で確認することで spam メールの有無について判断できる．

3) 誤認識メールのスコア

ユーザが再配送を行ったメールを誤認識により隔離したメールとして扱い，そのスコアを解析することで，Spam Assassin の spam メール誤認識率が測定できる．

2006 年 10 月 1 日から 2006 年 10 月 14 日までの 2 週間のデータを用いて解析を行った．

5. 2 IMSS との一致性

まずは IMSS と SpamAssassin における判断の一致性について解析を行った．図 3，表 3 に，期間内に IMSS で隔離したメールの SpamAssassin のスコア分布を示す．

この図，表からわかるように，この期間については 4.0 点未満のメールは 0.8%であり，閾値を 4.0 点に設定に設定することで，全体の 99.2%を SpamAssassin では spam と判定することができていることが分かる．

表 3　IMSS で隔離されたメールの累計

SpamAssassin スコア	メール数の合計	全隔離メール数に対する割合(累計)
～-0.1	2,676	0.1 %(0.1%)
0.0～3.9	15,250	0.7 %(0.8%)
4.0～11.9	169,617	4.0 %(4.8%)
12.0～14.9	96,137	9.0 %(13.8%)
15.0～19.9	130,089	6.4 %(20.2%)
20.0～24.9	123,141	6.1 %(26.3%)
25.0～29.9	170,302	8.3 %(34.6%)
30.0～34.9	229,652	11.2 %(45.8%)
35.0～39.9	280,812	13.8 %(59.6%)
40.0～44.9	257,953	12.6 %(72.2%)
45.0～49.9	204,008	10.0 %(82.2%)
50～	362,092	17.8 %(100%)
合計	2,041,729	100%

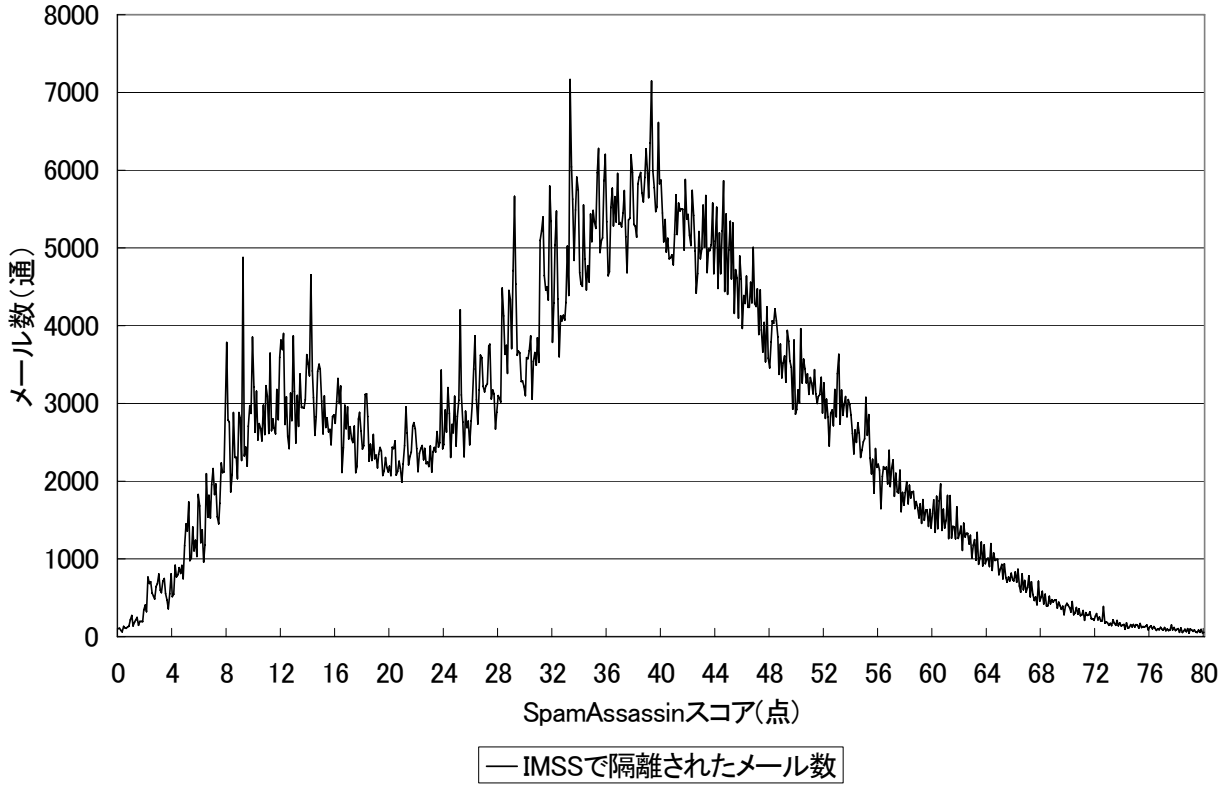

図 3　IMSS で隔離されたメールのスコア分布

5.3 標本メールの内容

次に標本メールの内容についての解析を行った．標本メールは 4.5 で説明したとおり，IMSS では非 spam と判定したが SpamAssassin では spam と判定したメールである．表 4 に期間内の標本メールの割合を示す．

表 4　標本メールの割合

IMSS で隔離したメール数	標本メール数	合計	標本メールの割合
169,617	6,909	176,526	3.9%

このようにスコアが 4～11.9 点を付けられて IMSS で隔離したメールは 169,617 通，標本メールは 6,909 通であり，標本メールの割合は 3.9%であった．しかし，実際に内容を確認するとメールマガジンや正規のメールも多く含まれていた．そのため，スコアが 4～11.9 点のメールを全て隔離すると多くの False Positive が発生する危険性が考えられる．

5.4 誤認識メールのスコア

次に，誤認識メールのスコアについて解析を行った．IMSS で隔離したメールで，ユーザが再配送したメールの SpamAssassin のスコアを解析することで評価できる．表 5 に，期間中のユーザが再配送を行ったメールのスコアによる範囲別の誤認識メール数を示す．ただし，再配送メールで内容的に明らかに spam メールと思われるメールは除いている．

この期間内では全体で 66 件の再配送があった．4 点未満のメールは 50 件あり，大半がメールマガジンであった．4 点以上のメールは 16 件隔離しており，最高で 14.1 点のメールがあった．特に 9 点を超えるメールは中国やロシアなどの英語圏以外から配送されてくるメールである．この解析結果から，15 点未満のメールを隔離すると False Positive が発生すると判断できる．

表 5　スコア範囲別の誤認識メール数

SpamAssassin スコア	誤認識メール数
～-0.1	16
0.0～3.9	34
4.0～11.9	12
12.0～12.9	3
13.0～13.9	0
14.0～14.9	1
15.0～	0
合計	66

5.5 SpamAssassin の有効ルール

4.3 で簡単に述べたが，SpamAssassinで特定のルールにマッチしたメールはIMSSで隔離するように設定している．表 6 に SpamAssassin のルールをベースにした IMSSのフィルタ定義[7]と隔離したメールの割合を示す．

「.OCCUR. [URIs:」は，メッセージ部に記載されている URL 等のドメインが SURBL や url.rbl.jp のリストに登録されていた場合にヘッダに付加される．リストを運用している機関は非営利団体の為，リストの鮮度，信頼性には保証がないので，現在は 4 つ以上のリストにヒットした場合に spam メールと判断し隔離している．

HTML_IMAGE_ONLY_*は HTML メール内にイメージのみをリンクしたメールであり，イメージは IMSS で定義できないため，非常に有効な定義である．

「.WILD. *surbl.org/lists.htm* .AND. .WILD. * cbl. abuseat.org/lookup.cgi?ip=*」は DNSBL である CBL（Composite Blocking List）に登録されており，かつ SURBL に登録されている場合である．この定義に関しては運用経験でこの組み合わせが有効であると判断し，定義をしている．別の DNSBL に変えた場合は正規メールがマッチすることがあった．

表 6　特定ルールにマッチしたメールの割合

IMSS フィルタ定義	Hit 件数	隔離メール全体に占める割合
.OCCUR. [URIs:	362,361	17.7%
HTML_IMAGE_ONLY_*	297,166	14.6%
.WILD.* surbl.org/lists.htm*.AND. .WILD.*cbl.abuseat.org/lookup.cgi?ip=*	228,966	11.2%

6. 考察

5 の解析結果から，現在の閾値である 4 点で隔離を行うと多くの False Positive が発生することがわかった．そのため，Spam Assassin のみで運用した場合で，False Positive をほぼ無くしたい場合は表 5 に示すとおり閾値を 15 点以上にする必要があると考えられる．しかしながら，閾値を 15 点に設定すると表 3 に示すとおり，13.8%の spam メールはすり抜けることになる．

よって，SpamAssassin のみで運用を行った場合は現状よりも spam メール認識率は低下してしまう．そのため結論としては，SpamAssassin でスコアリングを行い，14.9 点までのメールは標本メールとして抽出し，管理者が IMSS でフィルタ定義を行い，15 点以上のメールは全て隔離してしまうのが最も効果的である．つまり，SpamAssassin は IMSS 等のコンテンツフィルタリングできるソフトと併用することが最も有効的であると考えられる．

また，SpamAssassin で標本メールを自動抽出できるようになったことにより，これまで管理者が手動で行ってきた標本メールを抽出するための spam メールに利用される語句の IMSS のフィルタへの定義や利用者から spam メールを収集するといったような手間が無くなり，管理者の負担が軽減された．

7. 問題点

SpamAssassin はメールを様々な側面で解析できるという利点がある一方，サーバにか

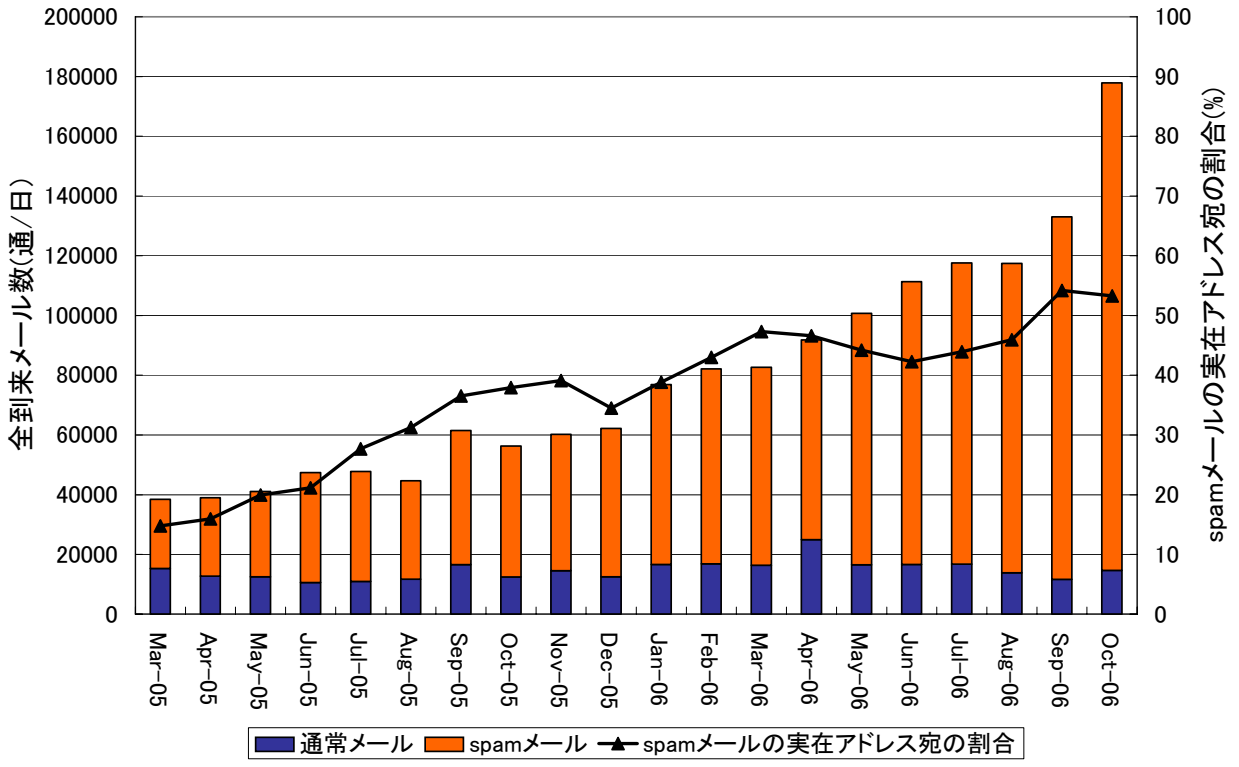

図 4　全到来メール数及び spam メールの実在アドレス宛の割合

かる負荷が大きいという問題を抱えている．

図 4 に金沢大学への全到来メールの内訳を示す．2005 年 3 月では 1 日当りの全到来メール約 4 万通中，約 2～3 万通を spam メールとして検知していたが，2006 年 8 月では全到来メール数約 12 万件中，約 10 万件を spam メールとして検知している．このあたりから表 2 に示すスペックの副サーバの 3 台構成では追いつかなくなり，表 2 の主サーバを新規に導入した．しかし，2006 年 10 月では全到来メール約 18 万件中 16～17 万件を spam メールとして検知しており，現在も増加の一途を辿っている．そのため，現在では 4 台構成でも遅延が起こる場合が発生する．また,処理を行うメール数が膨大であるため，SpamAssassin が内部に持つ Auto- whitelist やベイジアン DB の肥大化もメール配送遅延の原因となっている．

さらに図 4 の折れ線グラフは spam メールの実在アドレス宛の割合を示しており，2005 年 3 月では検知された spam メールのうちの約 15%のみが実在アドレス宛であったが 2006 年 9 月以降は 50%を超えている．このことから，spam メール送信者はある程度実在するアドレスを把握しており，実在するアドレスに対して spam メールを送信していることがうかがえる．そのため，spam メールの取りこぼしはユーザに与える影響が大きくなってきている．

8. まとめと今後の課題

今回，IMSS フィルタ定義の省力化を図るために，SpamAssassin を導入し，運用した結果から SpamAssassin の spam メール認識率の解析を行い，有効性を検証することができた．さらに，標本メール抽出やフィルタ定義の省力化に貢献しており，かつコンテンツフィルタが抱える問題を改善することができた．また，今回得られた解析結果から，SpamAssassin のスコアにより IMSS で隔離する点数の条件を 15 点に変更して運用を行うように変更した．

しかし，spam メール数の増大により，SpamAssassin にかかる負荷が問題になっており，今後は Greylisting 等のソースブロッキング方式を併用し，ある程度 SpamAssassin に通すメールを絞り込む必要があると考えられる．また，SpamAssassin のルール毎のスコアを調整したり，新たにルールを追加したりすることで，SpamAssassin の spam メール認識率を向上させ，標本メール数を減らすことで IMSS のフィルタ定義の更なる省力化を図っていきたいと考えている．

参考文献

(1) Trend Micro(株)：
“Interscan Message Security Suite”：
http://www.trendmicro.com/jp/products/gateway/imss/evaluate/overview.htm

(2) 松平拓也，車古正樹，井町智彦：“spam メール及びウイルスメール対策システムの構築と運用”, 学術情報処理研究, No9, pp.45-53 (2005)

(3) 車古正樹，松平拓也，井町智彦，中野三智子：“spam フィルタに関する統計”，学術情報処理研究，No9，pp.55-62 (2005)

(4) The Apache SpamAssassin Project：
http://spamassassin.apache.org/

(5) Tokyo Linux Entertainment Community：http://tlec.linux.or.jp/

(6) セキュリティガイド委員会, “ネットワークとワークステーション管理のためのセキュリティガイド”, サイエンティフィック・システム研究会(2005)

(7) 車古正樹，松平拓也，中野三智子，井町智彦：“メールシステムの現状と課題”，学術情報処理研究，No8，pp.63-68 (2004)

著者略歴

松平拓也　1981 年生，2004 年信州大学工学部情報工学科卒業，2006 年同大学院工学系研究科博士前期課程情報工学専攻修了，修士（工学），2004 年 4 月より金沢大学総合メディア基盤センター技術職員，ネットワーク管理全般，spam メール対策，ネットワークセキュリティシステム構築等を担当.

車古正樹　1944 年生，1967 年金沢大学工学部卒業，同年金沢大学計算機室教務員，1973 年工学部講師，1996 年総合情報処理センター助教授，2003 年総合メディア基盤センター教授，ネットワーク・セキュリティに関する研究に従事，情報処理学会会員.

井町智彦　1971 年生，1996 年金沢大学工学部電気情報工学科卒業，2002 年同大学院自然科学研究科博士後期課程修了，博士（工学），同年日本学術振興会特別研究員，2003 年金沢大学総合メディア基盤センター助手．全学的なネットワーク管理及び情報セキュリティ対策に従事.

中野三智子　1978 年生，1999 年 3 月金沢学院短期大学生活情報コース卒業，同年金沢大学情報処理センター技術補佐員，2003 年 4 月より同総合メディア基盤センター技術補佐員.