spam メール対策システムの現状

Status of Management System for Anti spam

松平 拓也†, 車古 正樹†, 井町 智彦†
Takuya MATSUHIRA†, Masaki SHAKO†,Tomohiko IMACHI†

takusng@kenroku.kanazawa-u.ac.jp, shako@office0.ipc.kanazawa-u.ac.jp
imachi@kenroku.kanazawa-u.ac.jp

†金沢大学総合メディア基盤センター
〒920-1192 石川県金沢市角間町

†Information Media Center of Kanazawa University
Kakuma-machi, Kanazawa, Ishikawa 920-1192, Japan
TEL: 076-234-6923 FAX: 076-234-6918

概要

近年 spam メールが増加の一途を辿っており，非常に大きな問題となっている．金沢大学では spam メール対策を 2003 年 11 月から始め，spam メール対策システムを構築し，2004 年 11 月から運用を行っている．本対策システムの spam フィルタの定義は手動で行っており，これまではフィルタ定義のための標本メール抽出は，spam によく利用されるキーワード等の定義者による予測で行っており，非常に労力を要する作業となっていた．これに対し，2005 年 10 月から SpamAssassin を導入し，メールをスコアリングすることで spam メール抽出，spam フィルタ定義の省力化を図っている．本稿では，SpamAssassin 導入による効果及びそこから得られた統計について報告する．

キーワード

spam 対策, SpamAssassin, spam 統計

1. はじめに

近年，spam メールの大幅な増加が問題になっている．金沢大学でも spam メールの急増が顕著に現れており，2005 年 12 月では 1 日当り全到来メール約 6 万件中, 約 4～5 万件を spam メールと検知していたが 2006 年 7 月では全到来メール約 11 万件中約 9～10 万件を spam メールとして検知している（図 1）．約半年の間で spam メール数がそれ以前の 2 倍近くになっていることが見て取れる．

金沢大学では 2003 年 11 月より本格的に spam メール対策に取り組み, 2004 年 11 月には spam メール対策システム[1]の運用を開始し，誤認率が低く，かつユーザ及びネットワークへの負荷が最小限となるよう対策を講じている．[2]

本対策システムはトレンドマイクロ社製 Interscan Message Security Suite（以下 IMSS と呼ぶ）[3]を利用し，

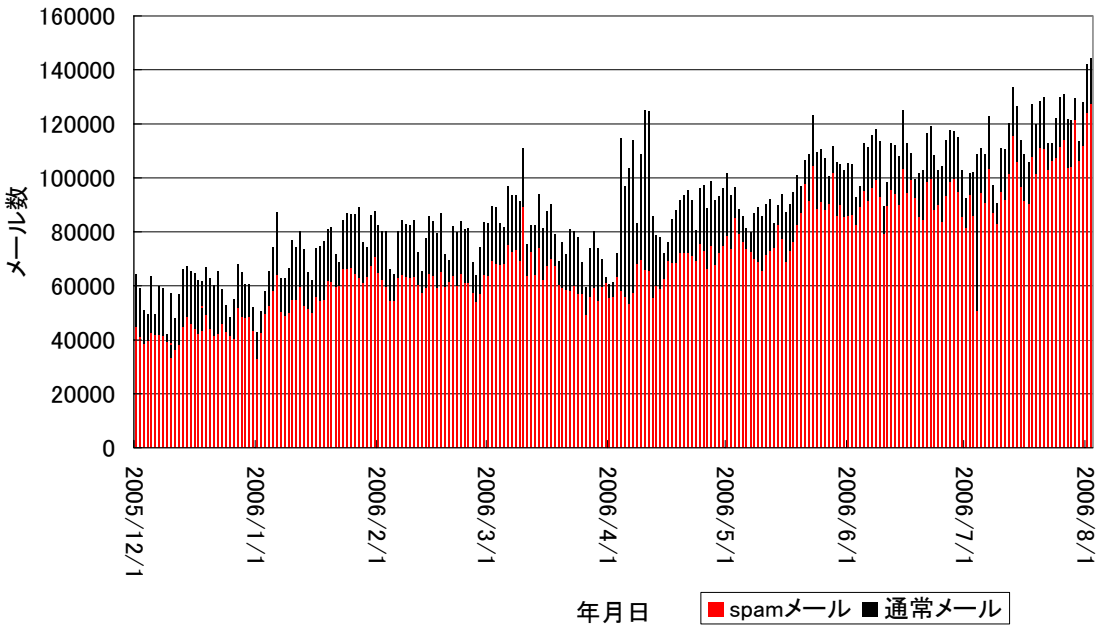

図 1　1 日毎の spam メール数と通常メール数

spam の疑いのあるメールを隔離しており，その際に使用されるフィルタ定義は管理者が手動で行っている．

これまでフィルタ定義を行うための標本メール抽出は，定義者がある程度 spam が利用しそうなキーワード等を考えて行っていた．しかしながら，この方法では以下の事項が問題となっていた．

- キーワードに合致しない spam メールは抽出することができない．
- 抽出してから定義を行う形式では短期間に集中して大量に送られる spam メールには対応できない．
- 空メールや形式に特徴のない spam メールを定義することができない．

これらの問題を解決するために，今回，SpamAssassin を導入し，SpamAssassin でメールにスコアをつけることで，上記の問題の解決を図るとともに，フィルタ定義の省力化を図ることにした．

本稿では SpamAssassin の運用経験及び，そこから得られた統計について報告する．

2. システム構成

2.1. SpamAssassin 概要

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定する OSS である．メールの形式に問題がないか，本文及び Subject に特定の語句を含んでいないか，メールの発信元・中継サーバが DNSBL に登録されていないか，本文に記載されているメールアドレスや URL のドメインが URIBL に登録されていないか等のルールに合致した場合に，ルールに対応した点数を累積加算していく．合計点数があらかじめ設定してある閾値を超えると spam メールであると判断される．

2.2. SpamAssassin 本格運用まで

まず，SpamAssassin の動作の確認を行うため，SpamAssassin サーバを 1 台用意し，メールの一部配送を，SpamAssassin サーバを経由させるようにした．

SpamAssassin を動作させているマシンのスペックは表 1 の通りである．

機種名	富士通　PrimePower200
OS	Solaris8
CPU	SPARC（400MHz×2）
メモリ	1Gbyte

表 1　SpamAssassin 稼動サーバのスペック

また，MTA には sendmail を，SpamAssassin への受け渡しには spamass-milter を用いて稼動を開始した．

SpamAssassin のスコア設定は，最初は TLEC（Tokyo Linux Entertainment Community）が提供している local.cf（スコア等の設定ファイル）のサンプル[4]を利用し，そこに定義されていないものについてはデフォルトのスコア設定を用いた．

SpamAssassin でスコアリングされたメールを管理者宛にも転送し，SpamAssassin のスコア調整を行っていった．

spam メールが Required_score（spam メール判定の閾値）

の点数以上に，正規メールが Required_score の点数未満になるように，抽出メールが到来するごとに，メールのヘッダに付加された X-Spam ヘッダを元に適宜 local.cf のスコア設定を変更していった. TLEC のサンプルは yahoo 等のフリーメールアドレスの利用，メールマガジン，中国やロシア等の英語以外の言語及び地域に非常に厳しく，大学で利用するには大幅な改善が必要であった.

稼動当初は順調であったが，稼動後約一ヶ月後に SpamAssassin を経由したメールの，メールヘッダが他のメールのものと付け替わって配送されるケースがあることが判明し，一度 SpamAssassin の利用を中断した．調査を行ったが，原因解明には至らなかった.

そのため，MTA を sendmail から postfix に変更し，SpamAssassin への受け渡し（filter）についてはサイエンティフィック研究会が公開しているスクリプト[5]に変更し運用を再開した.

その後，しばらく様子を見たところ，同様の現象が再発せず，動作が安定してきたので学外からのすべてのメールを SpamAssassin でスコアリングするように配送経路を変更し，現在のネットワーク構成に至っている.

2.3. ネットワーク構成

図 2 に 2006 年 8 月現在のメール配送構成図を示す. 学外を経由してきたメールはファイアウォールを通り，対学外メール中継サーバに集められる．次に SpamAssassin サーバに送られ，すべてのメールに対してスコアリングを行う．現在 SpamAssassin サーバは postfix-2.2.11，SpamAssassin3.1.4 を使用している．また 3 台用意し，負荷分散及び冗長化を図っている．それぞれのマシンのスペックは表 1 に示すとおりである.

2.3 に詳細を示すが, 一定のスコアを超えたメール及び特定のヘッダを付加されたメールは IMSS によって隔離される．また，一定の得点内のメールは定義者の標本抽出メールとしてユーザに配送するとともにフィルタ定義者にも配送される．一定の得点以下で，コンテンツフィルタ定義にもマッチしないメールはユーザに配送される.

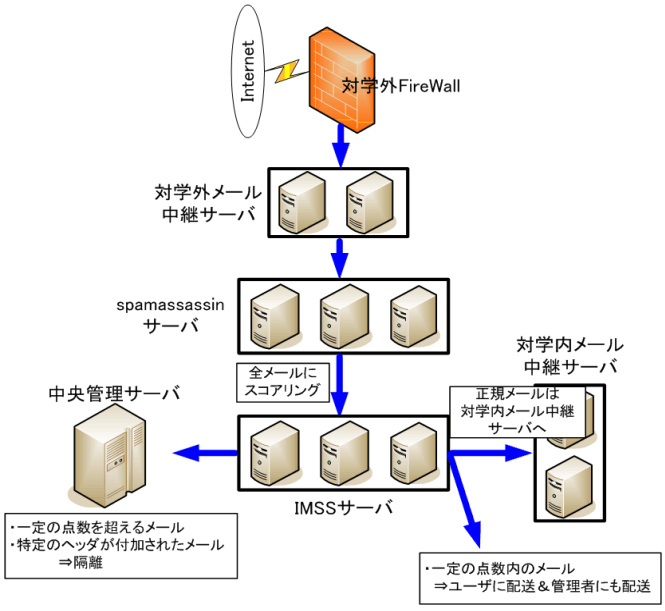

図 2　メール配送構成図

2.4. 運用規則

現在の SpamAssassin 及び SpamAssassin に関わる IMSS フィルタ定義の運用規則は以下の通りである.

- SpamAssassin ではスコアが 4 点以上のメールを spam と認識させ、「X-Spam-Flag: YES」ヘッダを付加する.
- 4～8.9 点までのメールはユーザに配送するとともに，フィルタ定義のための標本抽出メールとして定義管理者にも転送する．但し，他のフィルタ定義にマッチした場合はそのメールは隔離される.
- 9 点以上のメールはすべて spam メールと判断し IMSS で隔離される．ただし，このフィルタ定義は優先順位が下位になっているため，上位に存在する別のフィルタ定義にマッチしなかったメールに対してのみ有効となる.
- SpamAssassin で 4 つ以上の URIBL にヒットした場合は隔離する.
- HTML 内に画像のみリンクしてあるメール（HTML_IMAGE_ONLY）は隔離する.
- DNSBL の CBL（Composite Blocking List）に登録されており，かつ SURBL に登録がある場合
- Auto－whitelist，ベイジアン DB は利用する.

3. 運用状況

3.1. Requied_score の適切性

現在，SpamAssassin での Required_score（spam 判定の閾値）は 4.0 点に設定している．この閾値が妥当であるかどうかを判断するため，2006/7/24～2006/8/2 までの 10 日間に IMSS で隔離されたメールのスコアの分布の作成を行った．（表 2，図 3）.

この表，図からわかるように，SpamAssassin では IMSS で隔離されたメールの 99%を spam メールと判断している．この表，図を見る限りでは Required_score の 4 点の設定は妥当であると判断できる.

次に, 表 3 に 2006/8/24～2006/8/2 間の抽出メール（4.0～8.9 点のスコアをつけられたが IMSS で隔離されなかったメール）の割合を示す.

表 3 より 6.9%のメールが IMSS では隔離されずに抽出メールとして転送されてきている.

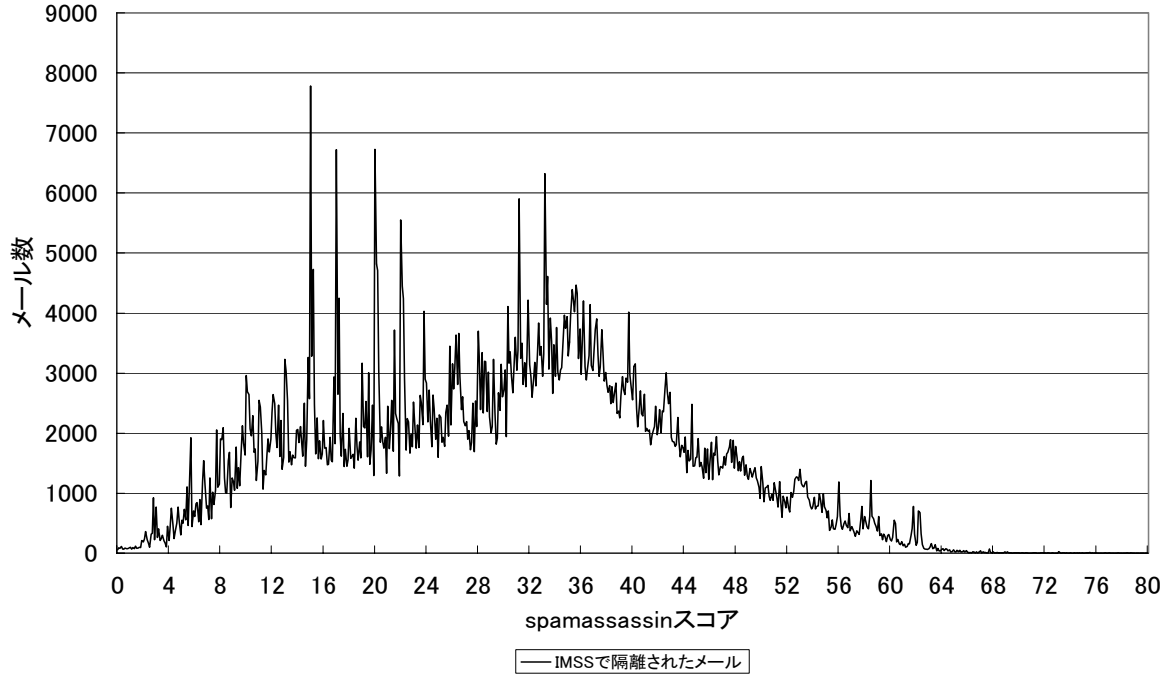

図 3 隔離メールのスコアグラフ（2006/7/24～2006/8/2）

SpamAssassin スコア	メール数の合計	全隔離メール数に対する割合
～-0.1	3049	0.3%
0.0～3.9	8035	0.7%
4.0～8.9	46455	4.0%
9.0～14.9	115588	10.1%
15.0～19.9	111813	9.9%
20.0～24.9	127963	11.3%
25.0～29.9	125566	11.1%
30.0～34.9	169515	15.0%
35.0～39.9	160782	14.2%
40.0～44.9	106350	9.4%
45.0～49.9	74457	6.6%
50～	83336	7.4%
合計	1132909	100%

表 2 隔離メールのスコアの割合（2006/7/24～2006/8/2）

この抽出メールの中にはメールマガジンや正規メールもしばしば見受けられる．そのため，4.0～8.9 点のメールを隔離すると多くの誤認識（False Positive）が起きる危険性が生じる．

隔離されたメール数	抽出メール数	Score における抽出メールの割合
46455	3468	6.9%

表 3 抽出メール（4.0～8.9 点）の割合（2006/7/24～2006/8/2）

また，本学の spam メール対策システムでは誤認識したメールをユーザが自動で再配送できるようになっている．そして，同様の誤認識が再び発生しないよう，そのメールを定義管理者に通知されるようになっている[1].

表 4 に 2006/7/24～2006/8/2 に隔離されたメールでユーザが再配送を行ったメールの SpamAssassin スコアの割合を示す．（但し，明らかに spam メールと思われるメールは除いている．）

この期間では全体で 47 件の再配送があった．4 点未満のメールの多くはメールマガジンであった．また，4 点以上のメールも 16 件隔離されている．特に 9 点を超えるメールは中国やロシアのメールであった．このため，これらのメールのアドレスは強制的に配信するように IMSS の定義を変更した．

SpamAssassin スコア	誤認識メール数
～-0.1	27
0.0～3.9	4
4.0～8.9	5
9.0～9.9	3
10.0～10.9	3
11.0～11.9	1
12.0～12.9	4
合計	47

表 4 誤認識メールのスコアの割合（2006/7/24～2006/8/2）

これらいくらかの表から，SpamAssassin で誤認識（False Positive）を発生させたくない場合は Required_score を 15 点以上にする必要があるように感じる．

3.2. SpamAssassin による IMSS での隔離

2.4 節で述べたとおり，SpamAssassin で特定のヘッダを付加されたメールや 9 点以上のスコアをつけられたメールは IMSS で隔離するようにしている．

表５に2006/7/24～2006/8/2の間にSpamAssassinによってIMSSで隔離されたメールの割合を示す．（IMSSフィルタ定義については[6]を参照）

IMSS フィルタ定義	Hit 件数	隔離メール全体に占める割合
.OCCUR. [URLs:	97472	8.6%
HTML_IMAGE_ONLY_*	94320	8.3%
.REG. Yes, score=[1-9][0-9]¥.[0-9] .OR. Yes,score=9¥.[0-9]	34568	3.1%
.WILD. *surbl.org/lists.htm*.AND. .WILD.*cbl.abuseat.org/lookup.cgi?i p=*	47813	4.2%

表 5　誤認識メールのスコアの割合（2006/7/24～2006/8/2）

このように，SpamAssassinによるIMSSでの隔離は隔離全体の24.2%で全体の1/4を占めている．

「.OCCUR. [URLs:」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，信頼性にはやや問題がある．その為，現在は４つ以上のリストにヒットした場合に隔離としている．

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，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．

また，「.REG. Yes, score=[1-9][0-9]¥.[0-9] .OR. Yes, score = 9¥.[0-9]」はスコアが 9 点以上のメールで，隔離全体の3.1％はSpamAssassinを利用しなければ通過（false Negative）していることになる．

「.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る．

このように，SpamAssassinにより，spamメール隔離の自動化がある程度実現でき，定義管理者の負荷軽減に貢献できていると考えられる．

4. まとめ

4.1. 問題点

SpamAssassinを導入することである程度，フィルタ定義を省力化できるようになったがSpamAssassinでは現在以下の問題を抱えている．

1) メールヘッダが他のメールのものと着け替わる場合が稀にある（2.2節参照）
2) メールがスコアリングされない場合がある
3) メールの配送が遅延する場合がある

現在これらの問題の原因解明を行っている．3）についてはAuto-whitelist，ベイジアンDBの参照をやめると改善される傾向があり，DBの肥大化が問題ではないかと考えている．そしてそのことに付随してSpamAssassinがタイムアウトし，その結果 2）が発生するのではないかとも推測される．

4.2. 結び

今回，SpamAssassinを利用することで，IMSSフィルタ定義の為の標本メール自動抽出，及び一部のspamメールの自動隔離が可能となり，フィルタ定義における省力化に一定の効果があったと考えられる．

しかしながら，4.1節で述べたようにいくつか問題点を抱えており，それらの改善が急がれる．問題点より，SpamAssassinは多数のメールを処理することは苦手であると推測される為，SpamAssassinを利用するにはGreylisting等のソースブロッキング方式を併用して，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．

5. 参考文献

[1]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，学術情報処理研究誌，No9，pp.45-53，2005

[2]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，学術情報処理研究誌，No9，pp.55-62，2005

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

[4]http://tlec.linux.or.jp/docs/user_prefs

[5]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

[6] 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，学術情報処理研究誌，No8，pp.63-68，2004

[7] http://spamassassin.apache.org/