spam メール対策の多段化における効果

Effect of the multistage system against spam mail

松平 拓也†，車古 正樹†，井町 智彦†，高田 良宏†
Takuya MATSUHIRA†, Masaki SHAKO†, Tomohiko IMACHI†,Yoshihiro TAKATA†

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

†金沢大学総合メディア基盤センター

†Information Media Center of Kanazawa University

概要

spam メールの急激な増加に伴い，電子メール配信のインフラにかかる負荷や，ユーザの生産性の低下が深刻な問題となっている．金沢大学では 2003 年 11 月よりトレンドマイクロ社の Interscan Message Security Suite を導入し，2004 年 10 月に spam メール対策システムを構築，2005 年 10 月より SpamAssassin を導入した．そして 2007 年 3 月よりシマンテック社の Symantec Mail Security 8360 を導入し，3 つの異なる spam メール対策を多段化して運用することで，spam メール検出率が高く，かつ管理者に負担のかからない対策システムを構築することができた．

本稿では spam メール対策の多段化における効果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，Symantec Mail Security，SpamAssassin，Interscan Message Security Suite

Abstract

The extreme increase of spam mail causes many serious problems such as the heavy load of the infrastructure for the delivery of e-mail or the decline of productivity of us.

In Kanazawa University, we have started to filter off spam mail by using of Interscan Message Security Suite since November of 2003, and constructed the “anti-spam system” in October of 2004. Since October of 2005, we have started to apply the scores assigned by SpamAssassin to increase the accuracy of the filtering, and introduced Symantec Mail Security 8360 at the front end on March of 2007.

In this paper, we discuss about the result of analysis about the effect of the multistage system against spam mail.

Keywords

spam mail，Symantec Mail Security，SpamAssassin，Interscan Message Security Suite

1. はじめに

今日，電子メールにおける spam メールの増加が著しく，電子メール配信のインフラに非常に大きな負荷がかかっている．またユーザ側においても，メール分類にかかる手間や重要なメールの見落としといったような生産性の低下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 1 つであると言える．

金沢大学では 2003 年 11 月よりトレンドマイクロ社製 Interscan Message Security Suite[1)]（以下IMSSと呼ぶ）を導入し，本格的にspamメール対策に着手した．そして，2004 年 10 月よりspamメール対策システム[2)]の運用を開始し，誤認識が少なくユーザ・管理者双方に負担が最小限になるようにしている[3)]．さらに，2005 年 10 月より SpamAssassin[4)]を導入し，IMSSとSpamAssassinを併用することで，それまで問題となっていたIMSSのフィルタ定義にかかる手間を簡略化することに成功した[5)]．そして，2007 年 3 月よりシマンテック社のSymantec Mail Security 8360[6)]（以下SMSと呼ぶ）を導入した．これを利用し，発信元IP アドレスがSMSのオープンプロキシリストに登録されているメールを削除することで，以降のメールサーバにかかる負荷を軽減することができた．また，SMSでspamメールと判定したものはIMSSで隔離することで，IMSSフィルタ定義の更なる簡略化を行うことができた．本対策システムで隔離したメールは 1 日に 1 度ユーザにメールで通知し，ユーザが自動で再配送できるように設計している．

このように，SMS ，SpamAssassin ，IMSS を多段化して運用することで，spam メール検出率が高い spam メール対策システムを構築することができた．

本稿ではまず，金沢大学のメール配送経路及びそれぞれのサーバの役割について説明した後，IMSS で隔離したメールを解析し，spam メール対策の多段化の効果について検証した結果について述べる．

2. spam メール対策システム

現在の spam メール対策システム，つまり学外からのメールの処理の流れを説明する．図 1 に spam メール対策システムのメール配送経路を示す．システムは全体で 6 段の構成となり，その全てにおいて IPCOM による負荷分散を行っている．

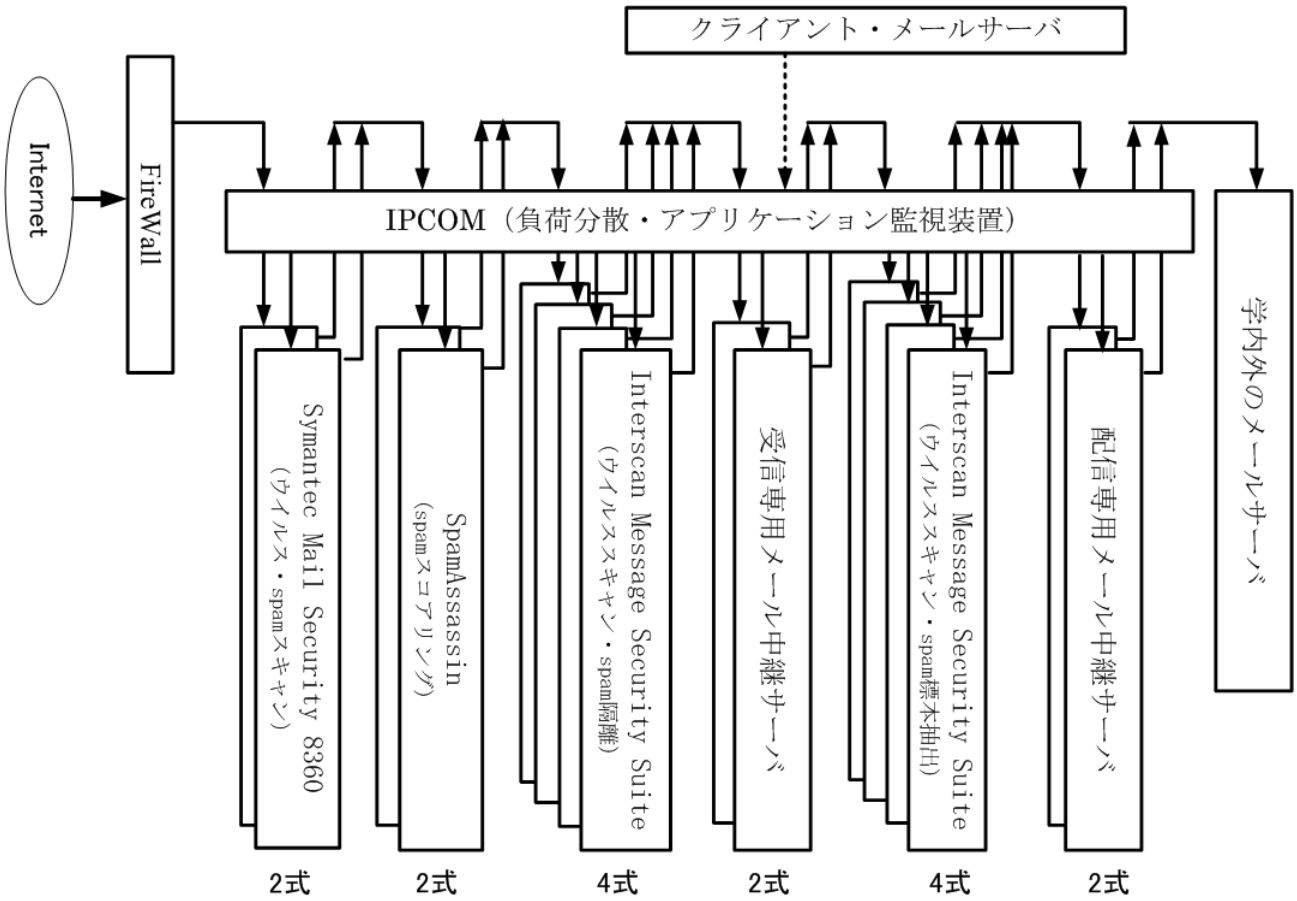

図 1　spam メール対策システムメール配送経路

2.1. アプリケーションレベル負荷分散・監視装置（IPCOM）

本対策システムで使用している各メールサーバは，全て2式以上用意し，負荷分散及び冗長化を図っている．これまでは負荷分散を，DNSラウンドロビンを利用して行っていたが，この方法では機能不全を起こしているサーバに対しても利用を試みてしまい，メールの配送に遅延が起きてしまう問題があった．

この問題を解決する為に，2007年3月に富士通製のIPCOM EX 2000 LB[7]を導入した．IPCOMはアプリケーションレベルで稼働状況を把握することができる負荷分散装置であり，サーバ上の必要アプリケーションが稼動していないことを検知すると，そのサーバへの接続を行わないようにすることができる．そのため，各メールサーバへの接続をIPCOM経由にすることで，サーバのアプリケーションやサーバそのものが停止していた場合でも，メール配送の遅延をなくすことができるようになった．また，同装置が機能不全を起こした場合に備え，以前使用していたIPCOM150[8]を予備機としてスタンバイさせておくことで，メールの配送が停止してしまう事態に対応している．また，IPCOMについては，2005年10月よりIPCOM150，2007年3月より上記IPCOM EX 2000 LBと長期に渡り使用しているが，これまでIPCOMに起因する障害は一度も発生していない．このことから，IPCOMの信頼性は非常に高いと判断している．IPCOM EX 2000 LBの主な性能は表1のとおりである．

表1 IPCOM EX 2000LB の性能

項目	値
インターフェース	1000BASE-T × 4
最大接続サーバ台数	512
最大セッション数	500,000

2.2. SMS サーバ

2007年3月のシステム更新時に対学外のメール中継用サーバとしてSMSを導入した．SMSは8300シリーズの8360を2式導入した．学外からの全てのメールはSMSに集める．SMSではベンダ独自のオープンプロキシリストを参照し，発信元IPアドレスがリストに登録されていた場合はspamメールとして削除することができ，そうすることで，以降のサーバの負荷を軽減できる．SMSのオープンプロキシリストの信頼性については，導入後約1ヶ月間は削除対象となったメールもIMSSサーバで隔離し，ユーザが再配送を試みるかどうかを確認した．

その結果，当該メールの再配送を試みたユーザは皆無であった為，リストの信頼性は実用上十分であると判断している．また，削除対象となったもの以外のメールについてはSpamAssassinサーバにリレーする．但し，シマンテック社独自のspamフィルタ定義でspamと判定されたメールに関しては，メールヘッダ内にspamヘッダを付加している．

2.3. SpamAssassin サーバ

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

合計スコア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．また，スコアの設定はTLEC (Tokyo Linux Entertainment Community)[9]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．

SpamAssassinサーバのスペックを表2に示す．SMS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．但し，メールを1週間あたり100件以上受信している実在しないアドレス宛のものに関しては，SpamAssassinに処理を回す前にMTAで受信拒否している．MTAから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[10]を使用している．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．

表2 SpamAssassin サーバのスペック

台数	2
機種名	富士通 Prime Power 250
OS	Solaris 10
CPU	SPARC64V（2GHz×2）
メモリ	4Gbyte
SpamAssassin のバージョン	3.2.0

2.4. IMSS サーバ

IMSSは2段構成で配置しており，前段のIMSSではコンテンツフィルタを用いてspam判定を行っている．前段

のIMSSサーバのスペックを表3に示す. ベンダ提供のコンテンツフィルタは標本メール抽出のみに利用している. 前段のIMSSがspamと判定したメールは隔離しており, 隔離に使用するフィルタ定義は管理者が手動で定義している[11]. 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
- SMS で spam ヘッダを付加したメール
- SpamAssassin で 13 点を超えたメール

条件に合致しないメールは受信専用メール中継サーバにリレーし，後段の IMSS サーバに送られる.

後段の IMSS では管理者がフィルタ定義するために必要な標本メールの抽出を行っている．これは IMSS が隔離と抽出の両方の作業を同一サーバで行えないためである．後段の IMSS サーバのスペックを表 4 に示す．標本メールは，これまでは管理者が，spam が利用しそうなキーワードを考えて抽出していたが，現在は SpamAssassin のスコアが 4～12.9 点のメールに絞り込んで調査している為，管理者の標本メール抽出にかかる手間は省略化されている．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．メールは全て配信専用メール中継サーバにリレーし，学内の各メールサーバへと配送する.

前段の IMSS サーバの前後には SpamAssassin サーバと受信専用メール中継サーバ，後段の IMSS サーバの前後には受信専用メール中継サーバと配信専用メール中継サーバと，両方の IMSS の前後にメールサーバを配置している．これは以前，IMSS と MTA を同一サーバ上で稼動させた時に，IMSS のサービスが停止しても，サーバが SMTP セッションを受け入れてしまうため，結果として IMSS サーバにメールが溜まってしまうという問題があったためである.

表 3　前段 IMSS サーバのスペック

台数	1	2	1
機種名	富士通 Prime Power 250		
OS	Solaris 8	Solaris 9	Solaris 10
CPU	SPARC64V (1.1GHz×2)	SPARC64V (1.3GHz×2)	SPARC64V (2.0GHz×2)
メモリ	4 Gbyte		

表 4　後段 IMSS サーバのスペック

台数	4
機種名	富士通 Prime Power 200
OS	Solaris 8
CPU	SPARC64GP（400MHz）
メモリ	1Gbyte

3. spam メール対策多段化の効果の検証

3.1. メールの分類

spam メール対策多段化における効果について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 SMS で spam スキャン処理を行う. 送信元 IP アドレスがオープンプロキシリストに登録されていた場合は「spam メール」として削除する. spam と判定したメールには spam ヘッダをつけて SpamAssassin サーバにリレーする．SpamAssassin サーバでは，まずメールを 1 週間あたり 100 件以上受信しているユーザが実在しないアドレス宛のメールを「spam メール」として受信拒否する．そして，それ以外のメールをスコアリング処理した後に，IMSS でフィルタリング処理を行う.

SpamAssassin のスコアが 13 点以上, SMS で spam ヘッダを付加したメール，IMSS のフィルタ定義に一致したメールは「spam メール」として隔離する．SpamAssassin のスコアが 4 点～12.9 点のメールは「標本メール」としてユーザに配送すると共に，IMSS のフィルタ定義作成のために管理者にも転送する．IMSS で非 spam と判定したメールは「正規メール」としてユーザに配送する.

つまり, 本学に送られてくるメールは「spam メール」，「標本メール」，「正規メール」の 3 つに分類することができる.

3.2. 各メールサーバの spam メール検出率

spam メール対策を多段化したことによる効果を調査するにあたり，以下の方法で解析を行った.

全ての spam メールのうち，SMS でオープンプロキシとして削除したメール数，SpamAssassin サーバの MTA で受信拒否したメール数，IMSS で隔離したメール数を割り出す．そして，IMSS で隔離したメールをさらに以下の 4 つのパターンに分類する.

- SMS で spam ヘッダをつけたメールでかつ SpamAssassin で 13 点以上のスコアをつけたメール（A）
- SMS で spam ヘッダをつけたが，SpamAssassin では 13 点未満のスコアをつけたメール（B）

- SMS で spam ヘッダをつけなかったが，SpamAssassin で 13 点以上のスコアをつけたメール（C）
- SMS で spam ヘッダをつけなかったメールでかつ SpamAssassin で 13 点未満のスコアをつけたメールで IMSS のフィルタ定義に合致したメール（D）

これらいずれの条件にもマッチしなかったメールは配送メールとしてカウントする．

これらの結果を表 5，図 3 に示す．今回は 2007 年 7 月 6 日から 2007 年 7 月 15 日までの 10 日間のデータを用いた．

表 5，図 3 から分かるように，この期間においては spam メール全体の約半分である 52%を SMS のオープンプロキシで spam メールと判断し，削除していることが分かる．また，SpamAssassin サーバの MTA で受信拒否しているメールも 3%あり，55%のメールを IMSS でフィルタリングする前にはじくことができていることが分かる．そして，IMSS での処理においては，SMS と SpamAssassin 両方で検出しているメール（A）は 18%あり，SMS のみが spam として検出しているメール（B）は spam メール全体の 4%であった．また，SpamAssassin のみが spam として検出したメール（C）は 18%あり，SMS と SpamAssassin 両方で検出できなかったメールで管理者が定義した IMSS のフィルタ定義で検出したメール (D) は 5%であった．つまり，SMS, SpamAssassin，IMSS それぞれが無かった場合には spam メールのすり抜けが起こることが分かる．この結果から，spam メール対策を多段化したことにより，spam メール検出の向上に効果があると言える．

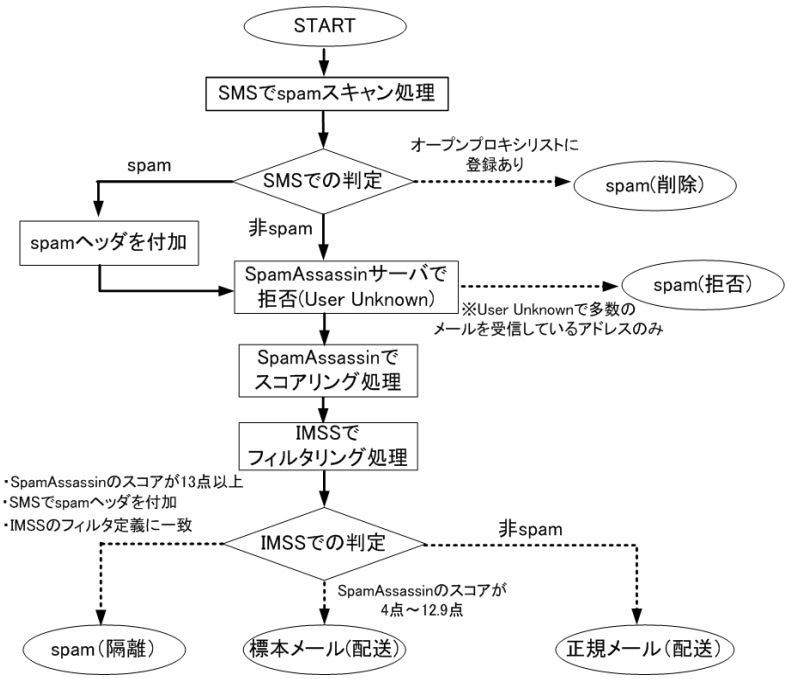

図 2　メール分類のフローチャート

また，表 5 から金沢大学に到来するメールの約 95%を spam メールとして検出することができていることが分かる．つまり，実際に利用者に配送されているメールは全体の約 5%に過ぎないことが分かる．

表 5　メールの内訳

年月日	SMS（削除）	Spam Assassin（拒否）	IMSS（隔離）				spam 合計	配送メール	spam の割合（%）
			A	B	C	D			
2007/7/6	165,070	8,399	56,442	10,754	57,894	11,891	310,450	17,564	94.6
2007/7/7	155,636	8,303	53,434	9,135	54,297	10,847	291,652	8,510	97.2
2007/7/8	147,262	7,997	54,537	8,360	54,259	9,207	281,622	5,894	98.0
2007/7/9	144,389	7,834	53,958	9,472	54,633	10,839	281,125	15,327	94.8
2007/7/10	153,926	8,811	55,319	12,189	56,099	13,497	299,841	17,952	94.4
2007/7/11	157,126	8,262	51,098	14,383	51,956	15,621	298,446	17,498	94.5
2007/7/12	161,620	9,252	55,069	19,191	55,987	21,429	322,548	18,946	94.5
2007/7/13	145,151	13,408	54,235	14,905	55,579	15,984	299,262	17,469	94.5
2007/7/14	152,364	7,802	56,321	10,213	57,142	11,809	295,651	8,441	97.2
2007/7/15	157,342	7,863	51,264	12,018	51,982	13,666	294,135	6,240	97.9
合計	1,539,886	87,931	541,677	120,620	549,828	134,790	2,974,732	133,841	95.7

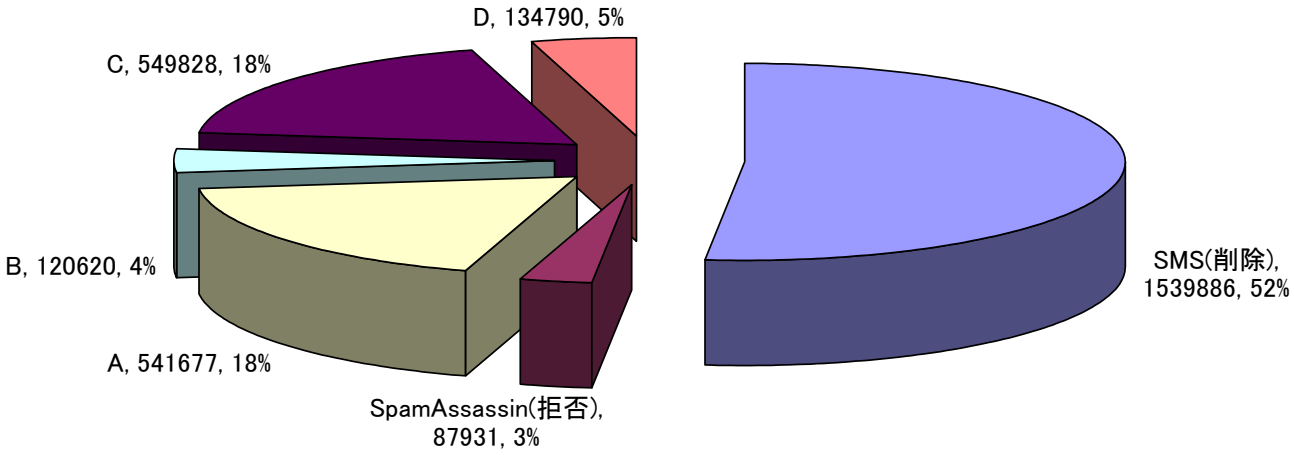

図 3 spam メールの割合

3.3. 実際の spam メール検出率に関する調査例

前節の結果がユーザに実際に与える効果を調べるため, spam メールのすり抜けや誤検出の調査が可能ないくつかのメールアドレスについて, 前節と同期間内 (2007/7/6～2007/7/15) に, どれだけの spam メールが到来し, 何件の spam メールがすり抜けているか調査を行った例を示す. 対象アドレスは, センター職員のもの (A, B, C) 及びセンターのホームページに掲載してあるもの (D) である. その結果を表 6 に示す.

これらのアドレスについては, spam メールのすり抜けはそれぞれ 1, 2 件程度であり, spam メール検出率は 99.5%を超えていた. また, この期間においては正規メールを spam メールと誤判定してしまうケースは 1 件も無かった. 従って, 今回の調査範囲においては spam メール対策の効果は非常に高く, 他のメールアドレスについても効果は高いものと予想される.

3.4. IMSS フィルタ定義数の推移

spam メール対策を多段化することには, IMSS のフィルタ定義にかかる管理者の手間の省力化の狙いもある. そこで次に, IMSS のフィルタ定義数の増減について調査を行った. 調査期間は 2005 年 7 月から 2007 年 6 月の 2 年間である. その結果を図 4 に示す.

2005 年 9 月までは IMSS のフィルタ定義の登録数, 削除数共に多く, 管理者に大きな負担がかかっていたものと思われるが, 2005 年 10 月に SpamAssassin を導入してから登録数, 削除数共に減少傾向にあることが分かる. その後は, IMSS のフィルタ定義の総数は減少に向かっており, そして, 2007 年 3 月に SMS を導入してからは, ほとんど IMSS のフィルタ定義を行わなくてもよくなった. 管理者の作業の大半は不要となった IMSS のフィルタ定義を削除するだけになっていることから, 削除数が登録数を上回り, IMSS のフィルタ定義総数を大幅に減らすことができている. さらに登録及び削除する定義数

表 6　メールアドレスごとの spam メール検出率 (2007/7/6～2007/7/15)

メールアドレス	SMS で削除	IMSS で隔離	spam メールのすり抜け	Spam メール検出率(%)
A	250	230	1	99.8
B	150	196	1	99.7
C	287	298	2	99.7
D(Web に掲載)	197	201	1	99.7

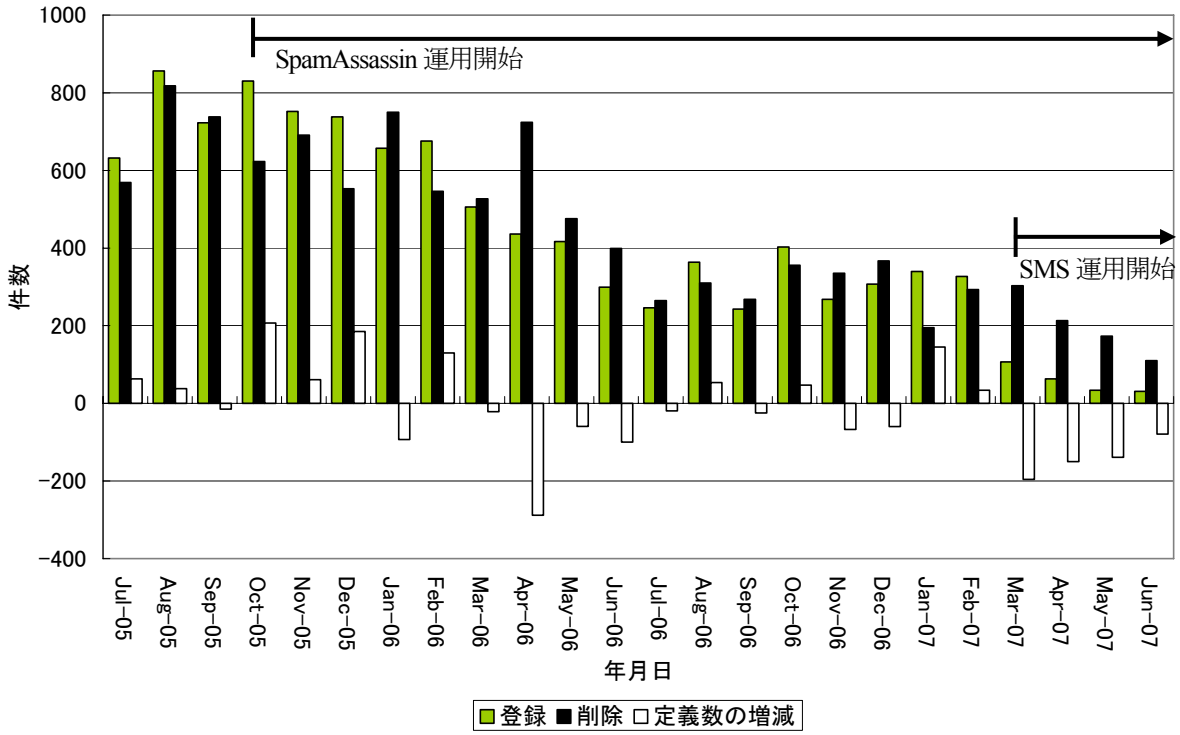

図 4　フィルタ定義数の推移

そのものも少なくなっていることが分かる．つまり，管理者は定義をほとんど触る必要が無くなり，IMSS のフィルタ定義作成にかかる管理者の負担がほとんど無くなっている．その結果，管理者の省力化においても spam メール対策の多段化の効果は非常に大きかったと言える．

4. まとめ

今回の解析において，学外から到来するメールを解析することで, spam メールの約半数を SMS と SpamAssassin サーバの MTA で削除できていることが分かり，SpamAssassin 及び IMSS にかかる負荷を大幅に軽減できていることが分かった．また，SMS，SpamAssassin，IMSS それぞれでしか隔離することができない spam メールがあることが分かり, spam メール対策を多段化して運用することで, spam メールの検出率の向上に効果があることを検証することができた．また，3.3 節でいくつかのアドレスに対して行った spam メール検出率に関する調査においても，spam メールのすり抜けはほとんどなく，正規メールの誤検出は 1 通も無かったことから，調査したアドレスにとって spam メール対策の効果は大きいことが確認された．

さらに，SpamAssassin 導入後，SMS 導入後に管理者の IMSS のフィルタ定義の登録及び削除作業の大幅な減少が確認でき，管理者にかかる労力を大幅に軽減できていることが分かった．従って, spam メール対策の多段化は，各メールサーバ，管理者，ユーザ全てに効果があったと考えることができる．

このように，現在のところ，spam メールメールには十分対応できていると考えており，今後は本対策システム運用の維持･管理に努めていきたいと考えている．また，現システムにおいては SMS と IMSS というベンダの異なるウイルスメール検索エンジンを通しているが，この効果についても調査を行い，ウイルスメール対策の多段化における効果についても検証を行う予定である．

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) SpamAssassin　Project : http://spamassassin.apache.org/

(5) 松平拓也，車古正樹，井町智彦，中野三智子 : “Spam Assassin による spam メール認識率に関する解析”，大学情報システム環境研究，Vol.10，pp.40-48(2006)

(6) Symantec corp.(株) : “Symantec mail security 8360” : http://www.symantec.com/ja/jp/enterprise/products/overview.jsp?pcid=1008&pvid=1721_1
(7) 富士通（株）:“IPCOM EX 2000 LB” : http://primeserver.fujitsu.com/ipcom/products/lineup/ipcom_ex_lb.html
(8) 富士通（株）:“IPCOM 150” : http://primeserver.fujitsu.com/ipcom/products/lineup/ipcom150.html
(9) Tokyo Linux Entertainment Community : http://tlec.linux.or.jp/
(10) 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)
(11) 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)