spam 対策システムの導入について

浜　　正　樹

［**要旨**］電子メールは、多数のインターネットアプリケーションの中でも、ユーザーへの普及が進み、インフラとしての重要度が最も高いものの 1 つである。その一方で、spam と呼ばれる一方的に送りつけられる不要な広告メールも横行し、世界的な問題となっている。本紀要論文では、平成 19 年度より実稼動している spam メール対策システムについて、その対策手法、仕様および効果などについて報告し、今後の課題について述べる。

1．はじめに

本学では、平成 17 年頃から spam の受信が急増し、その選別処理がユーザーを悩ませており、情報教育研究センターにも対策を求める声が大きくなってきた。そこで、手軽に始められる対策方法として、まず所謂メールソフトである MUA でのフィルタリング処理を採用し、IMP や Outlook Express 等のメールソフト側でのユーザーによる処理を促進した。しかし、MUA での対策は、選別処理が煩雑なため、運用は短期間で破綻を来した。

実際のところ、本質的な対策はメールゲイトウェイである MTA で実施する必要があり、ソース IP アドレスの整合性検査、Throttling や ORBL 利用など様々な対策手法が知られている。

しかし、上記の一般的な対策手法を、そのまま本学の MTA に適用すると、全ユーザーに画一的な対策を強要することになってしまい、柔軟な運用が不可能になってしまうことが懸念された。そこで、ユーザーやグループ別に spam 対策が可能で、更に spam と認識されたメールの隔離保存が可能なシステムを調達し、これを MTA として採用した。

本紀要論文では、spam 対策システム導入にあたり検討した仕様を中心に述べ、導入後の効果などについてもふれる。

本稿の構成は、次の通りである。まず、2 章では、spam の定義などを説明し、3 章では、spam に対してよく知られた対策手法について概略を述べる。4 章で、導入にあたって検討したシステムの仕様、およびその検討結果について記述する。5 章では、本年度 4 月以降に稼動している spam 対策システムのログから、本学における spam 対策の効果などを考察する。最終章では、まとめと共に今後の課題について述べる。

2．spam の概略

2.1．spam の定義

IPA（独立行政法人 情報処理推進機構 セキュリティセンター）[1] によれば、spam とは「宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメール」と定義されている。同義語としては、迷惑メール、ジャンクメール、DM メールおよび広告メールなどが使われる場合もある。より正確には、UBE（Unsolicited Bulk Email）または UCE（Unsolicited Comercial Email）と呼ぶことが提唱されているが、歴史的な背景から俗称である「spam」が最も定着しており、本稿でもこの呼称を採用する。なお、大文字で表記された「SPAM」は、Hormel Foods 社が販売するハム缶詰の名前であり、商標登録されている。Hormel Foods 社の Web サイト [2] に UCE が「spam」と呼ばれるようになった経緯が説明されている。

2.2．spam メールの状況

日本では、平成 14 年に制定された「特定電子メールの送信の適正化等に関する法律」[3]（以下、特電法と略記する）によって spam に対する法的な規制が定められており、広告を中心として不要なメールを送信した場合の処罰が決められている。また、その適正化推進機関として「迷惑メール相談センター」[4] が設置されている。この迷惑メール相談センターでは、上記の法律に違反した spam を受信した場合の情報提供や相談受付を行っている。同センターで公表

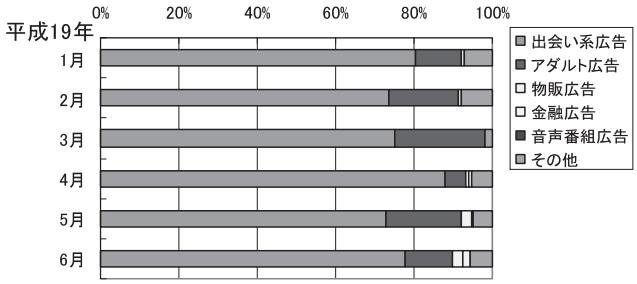

図 1　日本における spam メールの広告内容比率

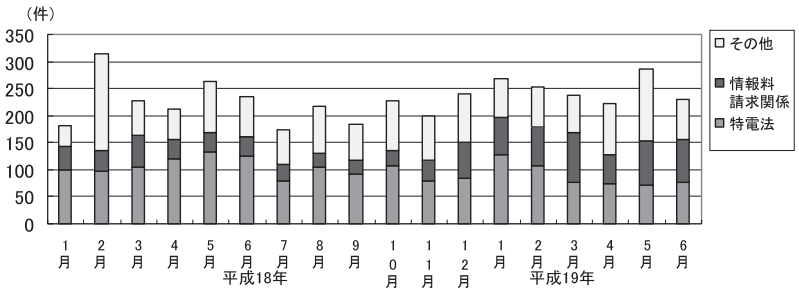

図 2　迷惑メール相談センターにおける電話相談件数の推移

されたアンケート結果によれば、日本における spam の特徴は図 1 に示された状況となっており、通説の通りに出会い系広告が大きな割合を占めていることが分かる。

また、電話相談の件数も図 2 に示す推移となっており、月別に相談数の多少の増減があるものの減少傾向にあるとは言い難い。

更に、図 3 によれば、特電法違反メールの件数も、減少傾向が見られないことが分かる。

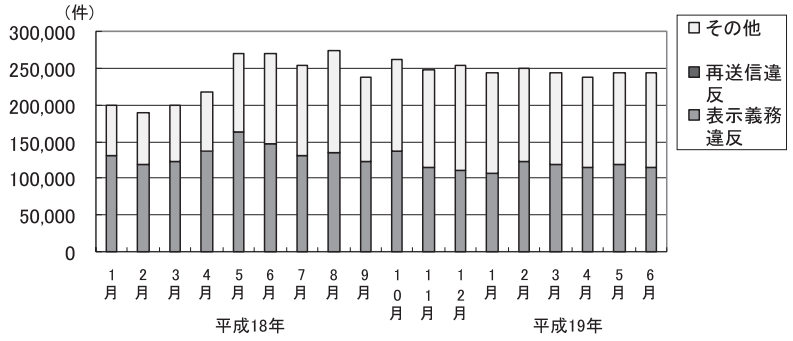

図 3　違反メールの件数推移

一方、本学では、平成 17 年度までは、意外なことに教員の役職者を中心とした数人にしか spam 被害の申し出が無かった。しかし、その被害内容については、上記のグラフと同じく出会い系の勧誘などが多かった。特に、大学の特徴であるが、週 3 ～ 4 回の出校や長期休暇の存在により、毎日のメールチェックを行わない教員も少なくない。この場合、休日明けの MUA によるメールチェックで、極端に多数の spam の削除作業を強いられ、教育や研究などの業務の妨げになるのみならず、受け取るべき正常なメールまで誤削除してしまうという問題が発生していた。

更に、平成 18 年度からは、一般の教員や学外折衝の多い事務局部署からも spam 被害の申し出が増えてきた。そこで、本郷キャンパス情報教育委員会では、spam 対策システムの導入の検討を開始した。

3．spam 対策

3.1．MUA における対策

spam を受信してしまった場合、ユーザー側で MUA の設定により、spam をフィルタリングし自動的に削除することが可能である。

本郷キャンパスで採用している Webmail「IMP3.2」も、このフィルタリング機能を有しており、情報教育研究センターでもその利用を推奨している。

このフィルタリング機能には、大きく分けて、ブラックリストとキーワードによるフィルタリングの 2 つのタイプが有る。

図 4 に示す設定インターフェースでは、送信者のメールアドレスや本文に含まれるキーワードを指定し、そのキーワードを含むメールを spam と判定して、MUA ログイン時に自動削除する等の処理を指定可能である。特に、受信拒否したいメールアドレスを具体的に指定すれば、ブラックリストとしての機能を果たすことも可能である。

しかし、これらの方法では、ユーザーに設定作業などの負担を強いる上、運用上次のような欠点がある。

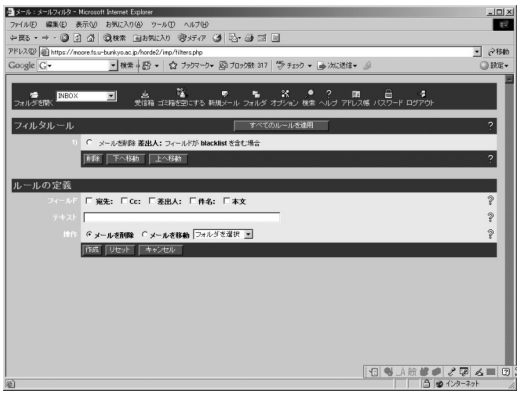

図 4　IMP3.2 のフィルタ設定画面

まず、ブラックリストによる受信拒否であるが、近年の spam 送信者は送信者アドレスを常に変更しながら送信してきていることが知られており、ブラックリスト自体に余り効果がないとされている。加えて、本学の IMP3 では、ブラックリストの登録数の上限が 99 と少なく、日々増加する spam 送信者名の登録には向いていないことも分かる。

次に、キーワードによるフィルタリングであるが、一般のユーザーにはキーワード自体の選定が難しい。一方で、spam 対策システムの開発ベンダーなどを中心に、spam に使われるキーワードのデーターベースが開発されており、こちらの利用を行うことが現実的な対応であると考えられる。

3.2. MTA における対策

本学での spam 被害者の人数が限られていると推測されるものの、被害状況は 2．2 節で述べた状況と同様と考えても良く、個人のフィルタ設定に頼るには、あまりに spam の量が多すぎるため、MTA で自動的に spam の選別を行うことが現実的である。本章では、MTA に於ける代表的な spam 対策について概説する。対策手法は、大きく分けてブロッキングとフィルタリングの 2 種類が知られている。

以下の 3.2.1.～ 3.2.5.は、spam 送信の特徴を利用したブロッキングであり、3.2.6.～ 3.2.7.は、spam の本文の内容や特徴を利用したフィルタリングである。

なお、MTA による spam 対策には、非常に多くの種類があり、本紀要論文の範囲ですべてを網羅することは不可能である。本学で検討した対策手法のみに限り記述していることをお断りしておく。

3.2.1．MTA ブラックリストおよび Open Relay Black List

MTA ブラックリストは、古くから対策に使われている手法で、spam を送信する MTA を登録し、受信拒否する仕組みである。しかし、MTA ブラックリストの情報収集は、一般ユーザーには非常に困難なため、Open Relay Black List（以下、ORBL と略記）と呼ばれる公開リストを併用する手法が普及している。

この ORBL とは、元々、不正メール中継が可能な MTA を独自に調査し、その IP アドレスをインターネット公開したものである。spam が全世界に広がり始めた初期には、不正メール中継防止を怠っている MTA を悪用して spam を大量送信されるケースが多かったため、この ORBL が spam をブロックするために有効な情報源であると考えられている。

また、最近の ORBL は、本来の不正メール中継可能な MTA の調査のみならず、インターネットの一般ユーザーから申告された spam 送信 MTA を登録・公開する傾向にある。

よく知られた ORBL としては、以下のサイトが挙げられる。

http://www.spamcop.net/

http://www.mail-abuse.com/

http://dsbl.org/main

http://www.spamhaus.org/

http://blacklist.jippg.org/

3.2.2．ソース IP アドレスの整合性検査

メールの送受信は、MTA（メールゲイトウェイ）間で SMTP と呼ばれるプロトコルを用いて行われる。そこで、メール送信のために接続してきた MTA の IP アドレスの DNS 逆引きを行い、そのホスト名が正確に回答されるか検査する手法が、ソース IP アドレスの整合性検査である。

この手法が、spam メールのブロックに適していると考えられている理由は以下の通りである。MTA は、所属ドメインの正規のメールサーバであることをインターネット全体に告知するために、通常 DNS の正引き（MX レコード）と逆引き（PTR レコード）の双方を登録する。一方、最近の spam は、ウイルスに感染したパソコン（「ゾンビ」と呼ばれる）から、パソコン所有者の意図と無関係に大量送信されるケースが多いが、一般ユーザーの利用しているパソコンの PTR レコードが登録されていることは少ない。従って、DNS 逆引き問合せでホスト名が回答されない場合、正規の MTA 経由のメールではなく spam であると判断できると考えられている。

更に、逆引き問合せで得られたホスト名から、その所属ドメインの MX レコードを問合せて、接続してきた MTA の IP アドレスが当該ドメインの正規のメールサーバのものであるか検査する手法をパラノイド検査と呼ぶ。

これらの手法の有効性については、よく知られているが、最近の spam 送信には、ゾンビではなく、わざわざ正規のドメインを取得し、PTR レコードも登録したパソコンが用いられる

ケースも増えている。その場合は、単なるソース IP アドレスの整合性検査ではブロックできない。そこで、パラノイド検査が重要視されてきているが、残念なことに正規の MTA の PTR 登録を忘れているドメインも散見される。この場合には正常メールにも拘らずパラノイド検査でブロックされてしまうというトラブルも発生する。

しかし、本対策手法がよく知られるようになってから、3 ～ 4 年以上は経っており、ほぼ常識的な spam 対策手法であると認識されるようになってきている。

3.2.3. Tempfailing

SMTP 接続してきた MTA との通信を、一時的に拒否することで再送を促す手法である。SMTP の仕様を定めた RFC2821[6] によれば、送信できなかったメールは一定時間後に再送するよう決められている。MTA に採用されているメール転送ソフトは、通常この仕様を満たしている。しかし、前述したゾンビは再送を行わないケースが多いため、この一時拒否を行うことで、spam のブロックが可能であると考えられている [5]。この手法は、「一見さんお断り方式」や「お馴染みさん方式」などという俗称でも呼ばれている。

この手法も非常に有効であるが、正規の MTA であるにも拘らず、RFC に従った再送を行わない MTA が存在するため、正常なメール送信が失敗するトラブルや極端なメール配送遅延が発生するトラブルが起きることがある。

3.2.4. Greylisting

Bjarne Lundgren によって提唱された手法 [7] で、一時受信拒否を行った後の再送受信の際に、SMTP 接続時に得られる 3 種類の情報「送信者アドレス、受信者アドレス、送信 MTA の IP アドレス」（以下、triplet と記述）を検査し、過去の triplet データベースとの照合を行う。triplet データベースは、ブラックリストデータベースとホワイトリストデータベースの 2 種類から構成されている。一度、受信を許可したメールの triplet は、自動的にホワイトリストに入り、次回からは再送要求なしに受け取ることができる。

良く考えられたシステムであるが、再送処理を行わない MTA からの受信が失敗するという問題がある。また、triplet データベースの保守が重要であり、メールサーバ管理者の負担が増えるという問題点もある。

3.2.5. Throttling

spam 送信には、広告配信という目的があるため、大量のメールを高速に送信する必要がある。そのため、「SMTP 接続を短い時間しか確保しない」という特徴が観測されている。

そこで、SMTP の接続応答を意図的に遅らせることで、SMTP の接続時間を延ばし、spam 送信を放棄させる手法である。

この手法は、設定が手軽な上に有効性が確認 [8] [9] されているが、Tempfailing と同様に正規の MTA でもメールの遅延を引き起こすことがある点が問題である。

3.2.6. ヒューリスティックフィルタ

spam の特徴、キーワードおよび本文中の URL などに対し、それぞれ重み付けを行い、独自

のルールに基づいて計算した数値で、spam の判定を行うフィルタリング手法である。

例えば、無意味な長い英単語が本文に含まれるメール、送信者と受信者のアドレスが同一なメール、および極端に本文が短い上にリンク付きの画像が含まれるメールなどの特徴を「spam らしさ」として捉えることで判定を行っている。

一般に、商用製品の場合、このヒューリスティックフィルタの詳細なアルゴリズムは公開されていない。spam 送信者にヒューリスティックフィルタを解析されて、潜り抜ける手法を考案されることを防ぐためというのが主な理由である。

3.2.7. ベイジアンフィルタ

Paul Graham が 2002 年に発表した論文「A Plan for Spam」[10] に基づいて、統計学で良く知られた確率論的手法によるベイズ理論を応用したフィルタである。

具体的には、spam と正常メールの集合を別々に学習することで、メールに含まれる単語の出現率から、ベイジアンフィルタ自身が spam の判定基準を確立していく仕組みである。

画期的な手法であるが、最近は spam 送信者も、その回避策を研究してきている。その例としては、以下のメールの様に、単語の間に「—」、「－」や「＋」など無意味な記号を埋め込み、単語による spam 判定そのものを難しくする手法などが知られている。

> Mi*ning Se-ctor -.-+- Delt.a Mi,ning UP_DATE
>
> H*O*T SECTOR,: Addit io_nal i,nformati.on on (O,_T_C: DM'XC) D'M+X,C is ex-pec.ted to arri,ve s.o,o_n-.
> F_o_r t+hose of y'o+u w.h'o curre+n-tly o,w,n t*h'i s comp*any t+h-i-s w.i'l,l be gre+at n,e-w's..
> F,o-r t-hose t.h-a't do_n't cur+ren-tly o.w-n t,h'i-s compa_.ny, y,o.u n.e.e_d to g+e't in on t'h.i_s n-o*w*.
>
> T*h-e compa_ny r-ece_ntly tr+aded as h+i*g_h as . 1 3 a n.d w,i_t_h a_n-y sign+if,icant n*e,w.s sho,uld be a_b'l*e

図 5　ベイジアンフィルタを潜り抜けた spam 例

3.3. その他

3.2 節で挙げた spam 対策は、メール受信に関する対策を示したものであるが、これからは、spam の送信者にならないための対策も講じていかなければならない。

一般に、spam 送信者は送信メールアドレスを詐称していることが多い。事実、本学のドメイン名を詐称した spam が、あるプロバイダに向けて多数送信され、結果として当該プロバイダから本学側に対策を要請されてしまったこともある。

これらの問題に関連した対策として、自ドメインからの送信メールに認証や電子署名を行うというアイデアがある。特に、電子署名の場合、受信者がその署名を検証することにより、正しい送信者から送信されたメールであるのか判定が可能になる。これらの仕組みの普及を通してメールの匿名性を無くしていくことで、長期的に spam を減少させることが可能であると期待されている。

以下に、代表的な手法の概略を記述する。

・ SMTP Authentication

RFC2554[11] に定義されている手法で、メール送信時にユーザーのパスワード認証を行う仕組み。MUA 側での対応が必須である。

・ SPF/Sender ID

双方とも、DNS と連携して、送信メールアドレスの偽装防止を行う仕組みで、インターネットでの今後の定着が期待されている。

SPF[12] は、DNS に登録された SPF レコードを利用して、自ドメインの MTA の IP アドレスのリストを公開し、受信側で Mail From に現れるドメインから送信されたメールかどうか検証可能にした仕組みである。

一方、Sender ID[13] は、Microsoft 社の提唱によるもので、Mail From に現れるドメイン名のみならず、受信メールのヘッダーの一部も含めて受信側で偽装の検証が可能である。

・ Domain Keys/DKIM

Domain Keys[14] は、yahoo.com が提唱した手法で、送信側の保持する秘密鍵を用いて、メールに電子署名を施し、受信側で送信側の公開鍵を用いて、メールの正当性を検査できる仕組みである。DKIM[15] は、Domain Keys に Cisco Systems などが提案した規格を統合した仕様である。

4．spam 対策システムの設計

4.1．設計方針

一般に、spam 対策システムを導入する場合の性能評価基準としては、false negative 率と false positive 率が代表的である。false negative とは、spam を検知できず正常メールとして見逃してしまうことを指す。一方、false positive とは、誤検知を指し、受信すべき正常メールを spam として検知してしまうことを指す。当然のことながら、false positive の方が深刻な現象であり、その発生率は限りなく 0%に近くなければならない。しかし、false positive 率が確実に 0%である spam 対策システムは存在しないため、spam と認識された後のメールの取り扱いについて、以下の仕様を必須条件とした。

・spam と認識したメールは隔離され、受信者がその内容を確認した上で、再送・削除が可能であること。

また、本学では、様々や要求を持つユーザーがメールを利用しており、3 章で述べた spam 対策を一斉に全学的に適用することが、大きな混乱を招く場合も想定される。現状では、spam の被害を認識し、spam 対策システムの利用手順を理解できるユーザーに限定して対策を講ずることの方が望ましい。そこで、以下の要件を重視した。

・ spam 対策を実施するユーザーをグループで指定できること。

・個人別に spam 対策の種別を指定可能であること。

以上に加えて、3 章で述べたブロッキング対策の内、以下の要件を採用した。

・ソース IP アドレスの整合性検査およびパラノイド検査によるブロッキングが可能であること。

・ Dos 攻撃を行う接続 IP アドレスに対し、受信拒否や Throttling 処理を行うこと。

・メールシステム管理者およびユーザーがブラックリストを作成できること。また、ユーザーが個人別にホワイトリストを作成できること。

・ ORBL が利用可能であること。

一方、Tempfailing については、正常なメールが不達になる危険性が排除できないこと、Greylisting については、ユーザー数の増加に伴うメールシステム管理者の負担の増大が避けられないことを考慮して、今回の導入では要件に入れることを見送った。

一方のフィルタリングについては、ヒューリスティックフィルタおよびベイジアンフィルタ共に、実績や有効性が認められるため、双方を要件に含めることにした。

その他、spam 対策以外に検討した要件を、次に述べる。

本学のメールシステムのトポロジーは、図 6 に示す通りであるため、今回導入するシステムは、文京学園全体（u-bunkyo ドメイン）で送受信される総てのメールを経由させることになる。従って、導入予定のシステムには、spam メール対策に加えて MTA 機能やウイルス対策

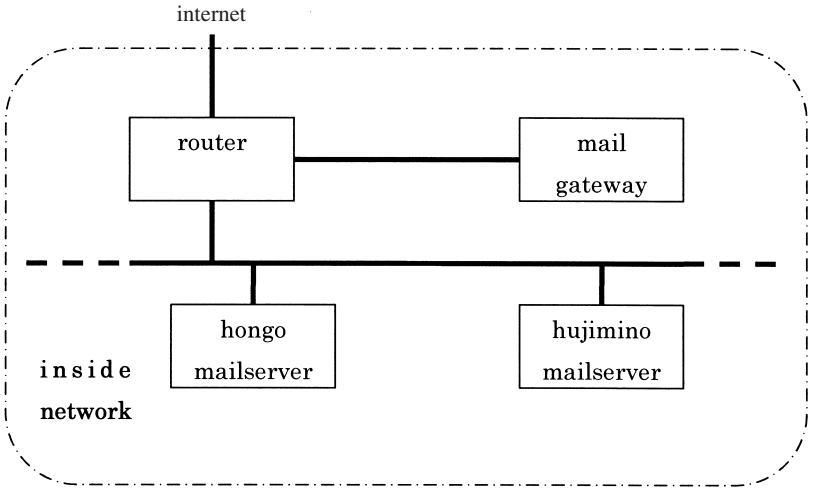

図 6　文京学園のネットワークトポロジー

機能を要件として加えることで効率の良い運営を行うことができる。

また、隔離された spam 候補のメールの確認・削除・再送作業や spam メールシステム管理には、Web インターフェースが用いられるため、その機能要件にセキュリティを含めることにした。近年、Web アプリケーションの安全性は大きな問題となり、クロスサイト・スクリプティング [16] や SQL インジェクション [17] などの脆弱性により、情報漏洩や情報改竄などが発生していることが指摘されているからである。

Web アプリケーションのセキュリティについての技術的な詳細は、本紀要論文の範囲に含まれないため割愛する。

以上の検討を踏まえて、ベンダー各社に提示した仕様書から抜粋して、包括的業務要件およびソフトウェア要件について引用する。

4.2. 包括的業務要件

4.2.1. MTA 機能

・本学のドメイン（u-bunkyo.ac.jp）の SMTP ゲイトウェイとして、SMTP リレー機能およびメールハブ機能を提供すること。

4.2.2. spam 対策機能

・本学のドメインで受信するメールに対し、spam メールを隔離する機能を有すること。
・本学のドメインから送信するメールに対して、spam 検査を行えることが望ましい。
・spam メール対策機能は、100 ユーザー以上を対象に実行可能であること。また、4000 ユーザー以上にも対処可能であること。

4.2.3. ウイルス対策機能

・本学のドメインで送受信するメールに対し、ウイルス検査を行い、ウイルスプログラムの隔離または削除を行うこと。
・ウイルス感染メールの送受信者に警告のメールを送る機能は、有効/無効化を選択できること。
・ウイルス対策は、4000 ユーザー以上を対象に実行可能であること。

4.3. ソフトウェア要件

4.3.1. MTA 機能要件

・ SMTP（RFC2822）および ESMTP（RFC1869）によるメールリレーが可能であること。
・メールハブとして、サブドメインのメールサーバへの転送機能を有すること。
・リレー制限機能を有すること。
・ MIME ヘッダの最大長を検査・制限できること。
・受信メールに対し、ソース IP アドレスの整合性を検査し、不合格なメールは受信拒否する機能を有すること。更に、パラノイド検査が実行可能であることが望ましい。
・キューに入ったメールの状態を表示し、送信および削除の操作が可能であること。
・送信先 MX 別に、キューの処理が可能であることが望ましい。

・Dos 攻撃に対し、同一 IP アドレスからの 1 分間のメール送信数や SMTP セッション数に閾値を決めて受信拒否やスロットリング処理を行う機能を有することが望ましい。
・サブドメインのメールサーバに、送信者アドレスに対応するアカウントの存在を問い合わせ、存在しない場合は、受信拒否する機能を有することが望ましい。
・ SPF/Sender ID に対応していることが望ましい。
・ Domain Key に対応していることが望ましい。
・ DKIM に対応していることが望ましい。
・ SMTP Auth に対応していることが望ましい。

4.3.2. spam フィルタリング機能要件

・ spam フィルタリングは、登録されたユーザーグループごとに設定可能であること。
・システム管理者がブラックリストおよびホワイトリストを設定可能であること。ブラックリストには、複数の RBL を指定可能であること。また、ブラックリストによる処理には、マーキングおよび受信拒否などが可能であること。更に、登録されたユーザーごとにホワイトリストを設定可能であることが望ましい。
・システム管理者が、フィルタリングルールを設定可能であること。更に、登録されたユーザーごとにフィルタリングルールを設定可能であることが望ましい。
・ヒューリスティックフィルタを設定可能であること。（spam キャラクター、キーワード、URL など） 更に、スコア判断が可能である場合には、加点して評価する。
・ベイジアンフィルタが利用可能であることが望ましい。
・spam として認識したメールは、すべて隔離すること。また、その保存が 60 日以上可能であること。また、90 日以上保存可能であることが望ましい。
・本文が同一テキストのメールが多数送信された場合、受信拒否を行う機能を有することが望ましい。

4.3.3. ウイルス対策機能要件

・送受信双方の SMTP セッションに対し、メールの MIME や uuencode などの添付ファイルをウイルススキャンする機能を有すること。
・ウイルス監視対象には、圧縮アーカイブ内のファイルを含むこと。
・ウイルスデータベースを自動的に更新する機能を有すること。

4.3.4. Web インターフェース機能要件

本節では、システム管理者および登録ユーザーが、システム設定および隔離メールの管理を行う際に利用する Web インターフェースについて、特にセキュリティの観点を重視した要求仕様を記述する。

・電子証明書をインストール可能であること。すべてのページが SSL で閲覧可能であること。
・パスワード認証が可能であること。認証は、LDAP および IMAP が可能であること。また、ドメインごとに認証サーバを選択可能であること。更に、認証時の通信は、SSL または TLS

を経由して行われことが望ましい。

・パスワードやセッション情報は、有限期限、推測されにくい文字列、一定以上の桁数などの制限を設けて不正使用を防止すること。

・以下を考慮したセキュリティ対策を行うこと。

・悪意ある文字列の入力チェックもしくは無害化

・ SQL インジェクションの防御

・コマンドラインインジェクションの防御

・パストラバーサルの防御

・パラメータ改竄の防御

・クロスサイトスクリプティングの防御

・バッファーオーバーフローの防御

・管理者用 Web インターフェースについては、送信者別に、送信メール数のカウントが表示されることが望ましい。また、送信ドメイン別に、送信メール数のカウントが表示されることが望ましい。

・一般ユーザー用 Web インターフェースについては、ホワイトリストへの登録機能を有することが望ましい。また、ホワイトリストのインポート機能およびエクスポート機能（双方とも CSV 形式ファイルが利用可能であること）を有することが望ましい。

4.4. 導入システムの検討

以上の要求仕様をもとに、以下の 3 機種について仕様および性能の比較検討を行った。

表 1　検討システム一覧

製品名	開発会社
SPAM Block	DeepSoft 社
SPAMSQR	Softnext 社
Secure Messaging Gateway	McAFee 社

包括的業務要件、MTA 機能要件およびフィルタ機能要件については、次の表 2 に示す審査結果となった。（別紙「技術審査採点表」参照）

表 2　技術審査得点概要

製品名	包括的業務要件	MTA 機能要件	spam フィルタ機能要件
SPAM Block	27	36	58
SPAMSQR	27	28	62
Secure Messaging Gateway	24	18	47

この結果より、SPAM Block が MTA としての機能に優れていること、また SPAMSQR が望ましい spam フィルタ機能を有することが分かった。Secure Messaging Gateway は、アンチウイ

ルスソフト会社が開発しているためか、今回要求した要件を全般的に満たすことが出来なかった。

更に、ハードウェア要件や保守契約要件などの検討を加えると、最終的な技術審査総合点は、次の表 3 の通りとなった。

本学のシステム導入案件は、総合評価方式に従った入札で決定され、その提案システムの評価順位は、技術審査総合点/導入価格の数値をもって決定される。本件は、総合評価方式による審査の結果、最終的に SPQMSQR を採用することになった。

表 3　技術審査総合点

製品名	総合点
SPAM Block	153
SPAMSQR	150
Secure Messaging Gateway	119

5. 導入システム運用後の評価

4 章で述べたように、検討の結果 SPAMSQR を本学の spam 対策システムとして採用し、平成 19 年 4 月より本格稼動した。

これにより、ORBL によるブラックリストやソース IP アドレスの整合性検査およびパラノイド検査によるブロッキングは、本郷キャンパス所有のドメイン全体に適用されている。

また、平成 19 年 9 月 1 日現在、spam フィルタリング機能は、教員や代表的な事務局メールアドレスを中心に登録された 32 名に適用されている。

平成 19 年度 4 月から 8 月の spam 対策ソフトの運用について、その効果を調査した。

まず、ブロッキングの効果であるが、表 4 および図 7 によると採用したブロック手法が、充分な機能を果たしていることが分かる。

表 4　パラノイド検査およびブラックリストによるブロック数

	4月	5月	6月	7月	8月
パラノイド検査	3367	4195	3838	2184	2916
ブラックリストブロック	7	4	5	9	14

しかし、図 8 によればブロッキング処理を実施しても 50%近いメールが spam であることが判明しており、ブロッキングだけでは spam の選別は難しいことを示している。

一方、フィルタリング処理の false positive 率についても注意が必要である。表 5 には、SPAMSQR が正常メールおよび spam と判定し隔離したメールの件数、更にユーザーが隔離メールのうち正常なメールであると判定して再送したメールの件数をまとめた。この結果をもとにして、false positive 率についても図 9 のグラフにまとめた。

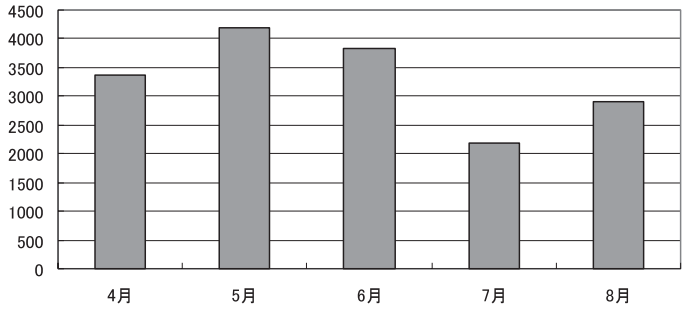

図７　パラノイド検査によるブロック数の推移

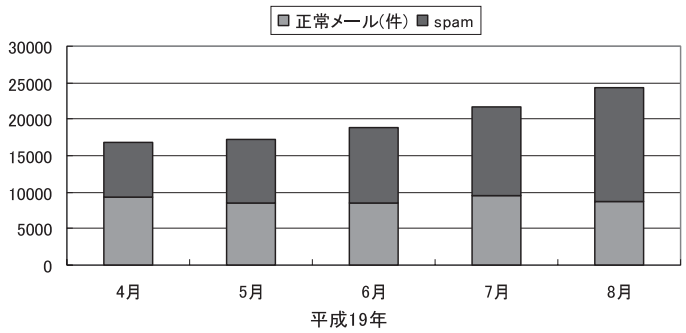

図８　正常メールと spam の件数

表５　SPAMSQR で選別された spam

	4月	5月	6月	7月	8月
正常メール（件）	9160	8319	8394	9459	8688
隔離メール（件）	7672	8946	10558	12242	15720
再送メール（件）	132	123	84	90	49
false positive 率	1.72%	1.37%	0.80%	0.74%	0.31%

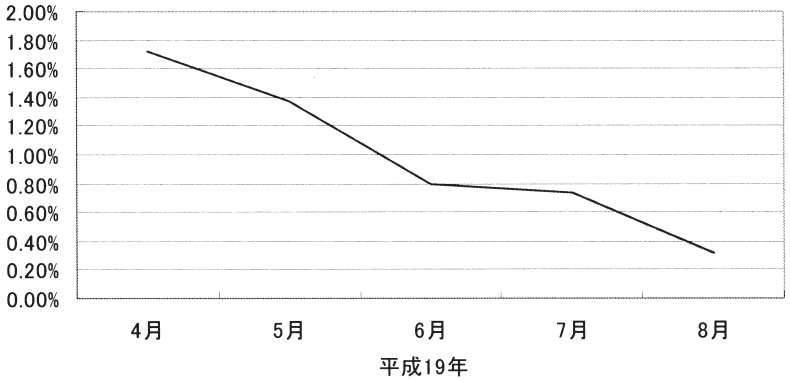

図９　false positive 率の推移

結果的に、false positive 率は順調に 0%に近づいている。これは、ユーザー個別のホワイトリスト作成が可能となっていることや本システムで採用した複合的なフィルタリング機能が効果的に機能していることによると考えられる。

6. まとめ

本 spam 対策システムは、現在の登録ユーザーの状況を調べた限り有効であると考えられる。今後は、この結果を基に、本郷キャンパス内でのユーザー拡大を進めて、更に定量的で精密な調査を行っていきたい。

更に、ふじみ野キャンパスも含めて spam 対策の対象ドメインを広げていくことも重要な課題である。そのために、全学的なメール配送経路の見直しなどの大規模なシステム設定修正に着手しているところである。別の機会にその結果を報告したい。

また、来年度以降となるが、本学所有ドメインからの送信メールに SPF や DKIM による認証技術を導入することで、spam 加害の抑制にも取り組んで行きたいと考えている。

謝辞

本紀要論文の作成にあたって、本郷キャンパス情報教育研究センター職員大岩義典氏に貴重な助言を頂いた。ここに記して感謝の意を表する。

参考文献

1）IPA: UBE（迷惑メール）中継対策　http://www.ipa.go.jp/security/ciadr/antirelay.html.
2）Hormel Foods Sales, LLC ： SPAM and the Internet. http://www.spam.com/legal/spam/.
3）総務省：特定電子メールの送信の適正化等に関する法律
http://www.soumu.go.jp/joho_tsusin/top/pdf/meiwaku_01.pdf.
4）迷惑メール相談センター: http://www.dekyo.or.jp/soudan/index.html.
5）鈴木常彦・後藤邦夫・山口榮作・石川雅彦(2004）: MTA による spam 対策の実践報告　情報処理学会研究報告　2004-DSM-034　pp61-64
6）RFC2821: Simple Mail Transfer Protocol. http://www.ietf.org/rfc/rfc2821.txt.
7）Bjarne Lundgren ： Greylisting.org. http://www.greylisting.org.
8）前野年紀・鈴木常彦（2004）: spam 送信ホストの見分け方、情報処理学会第 9 回分散システム/インターネット運用技術シンポジウム報告集　pp.25-29
9）吉田 和幸： throttling による spam メール抑制の効果について(サービス管理, ビジネス管理, 料金管理, 及び一般）情報処理学会研究報告 [分散システム/インターネット運用技術] Vol.2005 No.39(20050512） pp.69-73
10）Paul Graham: A Plan for Spam. http://www.paulgraham.com/spam.html.
11）RFC2554: SMTP Authentication. http://www.faqs.org/rfcs/rfc2554.html.
12）RFC4408: Sender Policy Framework（SPF）for Authorizing Use of Domains in E-Mail, Version 1. http://www.ietf.org/rfc/rfc4408.txt.
13）RFC4406: Sender ID: Authenticating E-Mail. http://www.ietf.org/rfc/rfc4406.txt.

14）Yahoo! Anti-Spam Resource Center: DomainKeys: Proving and Protecting Email Sender Identity. http://antispam.yahoo.com/domainkeys.
15）RFC4871: DomainKeys Identified Mail（DKIM） Signatures. http://www.ietf.org/rfc/rfc4871.txt.
16）高木浩光・関口智嗣・大蒔和仁：クロスサイトスクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策　http://securit.gtrc.aist.go.jp/research/paper/css2001-takagi-dist.pdf.
17）警察庁： SQL Injection 攻撃の脅威と対策について
http://www.cyberpolice.go.jp/server/rd_env/pdf/20060330_SQLInjection.pdf.
18）本郷キャンパス情報教育委員会： spam 対策システム仕様書 Ver. 200612051130

技術審査採点表

		基礎点	加点	WBC	JIP	CTC
1	包括的業務要件					
1.1.	MTA機能					
1.1.1	本学のドメイン(u-bunkyo.ac.jp)のSMTPゲイトウェイとして，SMTPリレー機能およびメールハブ機能を提供すること。	3		3	3	3
1.2.	SPAM対策機能					
1.2.1	本学のドメインで受信するメールに対し，spamメールを隔離する機能を有すること。	3		3	3	3
1.2.2	本学のドメインから送信するメールに対して，spam検査を行えることが望ましい。	3		3	3	3
1.2.3	spamメール対策機能は，100ユーザー以上を対象に実行可能であること。 また，4000ユーザー以上にも対処可能であること。	3		3	3	3
1.3.	ウイルス対策機能					
1.3.1	本学のドメインで送受信するメールに対し，ウイルス検査を行い， ウイルスプログラムの隔離または削除を行なうこと。	3		3	3	
1.3.2	ウイルス感染メールの送受信者に警告のメールを送る機能は，有効/無効化を選択できること。	3		3	3	3
1.3.3	ウイルス対策は，4000ユーザー以上を対象に実行可能であること。	3		3	3	3
1.4.	既存システムとの接続					
1.4.1	本学ドメインでのメール受信については，既存のメールゲイトウェイ(ns.u-bunkyo.ac.jp)を セカンダリSMTPサーバとして併用すること。但し，そのためのDNS設定は，本学側で行なう。	3		3	3	3
1.4.2	本学ドメインからのメール送信については，既存のメールゲイトウェイ(sendmail 8.13.8)を 経由してから，提案する当該システムで転送すること。	3		3	3	3

		基礎点	加点	WBC	JIP	CTC
2	ハードウェア要件					
2.1.	CPUは，X86互換で動作周波数1GHz以上とし，1～2基有すること	3		3	3	3
2.2.	メモリは，PC-133以上の転送能力を持ち，512MB以上の容量を確保すること	3		3	3	3
2.3.	HDDは，回転数7200以上，容量70GB以上を確保すること。	3		3	3	3
2.4.	HDDの接続インターフェースは，UATA規格またはUltra SCSI規格を満たすこと。	3		3	3	3
2.5.	HDDの冗長構成は，RAID 1 で構成すること。その実装は，ソフトウェア・ハードウェアを問わない。	3		3	3	3
2.6.	LANアダプター(100/1000Base-TX)を2つ以上有すること。	3		3	3	3
2.7.	既存の無停電電源装置(APC Symmetra RM SYHF6K)に接続可能であることが望ましい。	3		3	3	3

		基礎点	加点	WBC	JIP	CTC
3						
3.1.	MTA機能要件					
3.1.1	SMTP(RFC2822)およびESMTP(RFC1869)によるメールリレーが可能であること。	3		3	3	3
3.1.2	メールハブとして，サブドメインのメールサーバへの転送機能を有すること。	3		3	3	3
3.1.3	リレー制限機能を有すること。	3		3	3	
3.1.4	MIMEヘッダの最大長を検査・制限できること。	3		3	3	3
3.1.5	受信メールに対し，ソースIPアドレスの整合性を検査し，不合格なメールは受信拒否する 機能を有すること。更に，パラノイド検査が実行可能な場合は，加点して評価する。	3	3	6	6	6
3.1.6	キューに入ったメールの状態を表示し，送信および削除の操作が可能であること。	3		3	3	3
3.1.7	送信先MX別に，キューの処理が可能であることが望ましい。	3		3	2	0
3.1.8	Dos攻撃に対し，同一IPアドレスからの1分間のメール送信数やSMTPセッション数に閾値を決めて受信拒否や スロットリング処理を行なう機能を有することが望ましい。	3		3	3	0
3.1.9	サブドメインのメールサーバに，送信者アドレスに対応するアカウントの存在を問い合わせ， 存在しない場合は，受信拒否する機能を有することが望ましい。	3		3	0	0
3.1.10	以下の仕様に対応していることが望ましい。 ・SPF/Sender ID ・Domain Key ・DKIM ・SMTP Auth		3 2 2 2	2 2 0 2	0 0 0 2	0 0 0 0
3.2.	SPAMフィルタリング機能要件					
3.2.1	SPAMフィルタリングは，登録されたユーザーグループごとに設定可能であること。	3		3	3	3
3.2.2	システム管理者がブラックリストおよびホワイトリストを設定可能であること。 ブラックリストには，複数のRBLを指定可能であること。また，ブラックリストによる処理には， マーキングおよび受信拒否などが可能であること。 更に，登録されたユーザーごとにホワイトリストを設定可能である場合には，加点して評価する。	3	3	6	6	3
3.2.3	システム管理者が，フィルタリングルールを設定可能であること。更に，登録されたユーザーごとに フィルタリングルールを設定可能である場合には，加点して評価する。	3	3	6	6	6
3.2.4	ヒューリスティックフィルタを設定可能であること。(SPAMキャラクター，キーワード，URLなど) 更に，スコア判断が可能である場合には，加点して評価する。	3	2	3	5	3
3.2.5	ベイジアンフィルタが利用可能であることが望ましい。	3		3	3	3
3.2.6	SPAMとして認識したメールは，すべて隔離すること。また，その保存が60日以上可能であること。 また，90日以上保存可能であれば，加点して評価する。	3	2	5	5	5
3.2.7	送信元を変更して多数送信されてくるメールの文や添付内容の同一性を検出し，その受信数制限を行なう機能を 有することが望ましい。	3		3	0	0
3.3.	ウイルス対策機能要件					
3.3.1	送受信双方のSMTPセッションに対し，メールのMIMEやuuencode などの添付ファイルをウイルススキャンする 機能を有すること。	3		3	3	3
3.3.2	ウイルス監視対象には，圧縮アーカイブ内のファイルを含むこと。	3		3	3	3
3.3.3	ウイルスデータベースを自動的に更新する機能を有すること。	3		3	3	3
3.4.	Webインターフェース機能要件					
3.4.1	電子証明書をインストール可能であること。すべてのページがSSLで閲覧可能であること。	3		3	3	2
3.4.2	パスワード認証が可能であること。認証は，LDAPおよびIMAPが可能であること。 また，ドメインごとに認証サーバを選択可能であること。 更に，認証時の通信は，SSLまたはTLSを経由して行なわれる場合には，加点して評価する。	4	3	4	5	2
3.4.3	パスワードやセッション情報は，有限期限，推測されにくい文字列， 一定以上の桁数などの制限を設けて不正使用を防止すること。	3		3	3	3
3.4.4	以下を考慮したセキュリティ対策を行なうこと。 ・悪意ある文字列の入力チェックもしくは無害化 ・SQLインジェクションの防御 ・コマンドラインインジェクションの防御 ・パストラバーサルの防御 ・パラメータ改竄の防御 ・クロスサイトスクリプティングの防御 ・バッファーオーバーフローの防御	5		5	5	2
3.4.5	管理者用Webインターフェースについては，送信者別に，送信メール数のカウントが表示されることが望ましい。 また，送信ドメイン別に，送信メール数のカウントが表示される場合は，加点して評価する。	3	2	3	3	1
3.4.6	一般ユーザー用Webインターフェースについては，ホワイトリストへの登録機能を有することが望ましい。 また，ホワイトリストのインポート機能およびエクスポート機能(双方ともCSV形式ファイルが利用可能であること) を有する場合は，加点して評価する。	3	3	2	6	5

		基礎点	加点	WBC	JIP	CTC
4	保守契約要件					
4.1.	「8. 4. Webインターフェース機能要件」に記載したセキュリティ対策が実施済みであることを書面にて証明し， 機能追加などを行なった際にも，セキュリティチェックを実施し，その結果を報告すること。	3		2	3	0
4.2.	ハードウェア故障の際には，3日以内に速やかに交換し，運用に重大な支障を来たさないこと。	3		3	3	3
4.3.	ソフトウェア脆弱性が発見された場合は，3 週間以内に速やかにパッチを配布・適用すること。	3		3	3	3
4.4.	導入時には，本学担当者に充分なトレーニングを行い，詳細なマニュアルを納入すること。	3		3	3	3

合計得点		138	30	153	150	119

備考　CTC提案のシステムには、MTA機能が実装されていないため、要件3.1.4～3.1.10については、本学の既存MTAサーバの機能について採点した。