横浜国立大学におけるスパムメール対策

SPAM-Mail Prevention in Yokohama National University

志村 俊也， 徐 浩源， 長谷部 勇一
Toshiya Shimura, Haoyuan Xu, Yuichi Hasebe

tshimura@ynu.ac.jp， haoyuan@ynu.ac.jp， yuichi@ynu.ac.jp

横浜国立大学　情報基盤センター

Information Technology Service Center,　Yokohama National University

概要

本学では、2008 年 2 月より、学内に送信されてくる全てのメールに対してスパムメール対策を実施している。本稿では、実施に至るまでの過程、および実施後の運用状況などを報告する。

キーワード

スパムメール対策， DNS リアルタイムブラックリスト方式， IP Reputation データベース

1. はじめに

本学では、2008 年 2 月より、トレンドマイクロ社の E-mail Reputation Services Advanced （以後 ERSA と呼ぶ）を利用したスパムメール対策を実施している。ERSA は、MTA 側に実装されている DNS リアルタイムブラックリスト機能を利用した製品であるので、『学外から送信されてくるスパムメールは受信せず拒否する』という対策が前提となっている。誤判定によって正常なメールが届かない状況もあり得るが、その事を十分理解した上で、本学では、『ホワイトリスト登録等の例外設定は一切行わず、学外から送信されてくる全てのメールに対して一律に実施する』という厳しい姿勢で対策に臨んでいる。

しかしながら、本対策は、その是非について 7 ヵ月間に渡って全学レベルで審議した上での導入であったため、対策実施後の学内の評価は非常に高く、誤判定等の問題はほとんど発生していない。本稿では、このスパムメール対策に関する実施に至るまでの過程・実施後の運用状況について報告する。

2. システム構成と対策方法

2.1 メールシステムの概要

最初に、本学のメールシステムの概要を説明する。本学のメールシステムは、

①┌ 情報基盤センターが管理運用する全学メールサーバ
② 各部局・研究室が個々に管理運用しているメールサーバ（約 60 台）

の 2 種類で構成されている。学外⇔学内間で送受信される全てのメールは、トレンドマイクロ社の Interscan

Messaging Security Suite （以後 IMSS と呼ぶ）によるウィルスメール検索処理を受けた後、受信者に届く仕組みとなっている（図 1 参照）。具体的には、① の全学メールサーバ宛てのメールは、サーバ本体に搭載されている IMSS でウィルス検索を行ない、②に該当する各部局・研究室のメールサーバ宛てのメールは、基幹ファイアウォール直下のレイヤ 4 スイッチで『メールゲートウェイ』にリダイレクトし、メールゲートウェイに搭載されている IMSS でウィルス検索を行った後、本来の配信先へ再配信する仕組みを取っている 。 全学メールサーバとメールゲートウェイの仕様は表 1 に示す通りである。

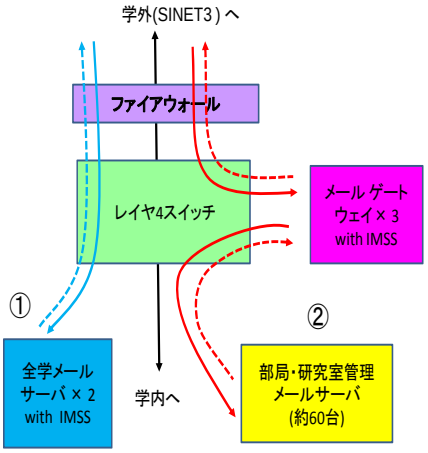

図 1　横浜国立大学メールシステムの概要。
青い線は、全学メールサーバに対するメールの送受信、赤い線は、メールゲートウェイを介した部局・研究室管理のメールサーバに対するメールの送受信経路を示す。

	全学メールサーバ	メールゲートウェイ
構成台数	2 (クラスター構成)	3(負荷分散)
メーカー	富士通	富士通
機種	PRIMEPOWER 450	PRIMERGY RX300 S2
CPU	SPARC　64V 1.87GHz	Xeon 3.2　GHz
CPU 数	4	2
RAM	8GB	6GB
OS	Solaris 9	RedHat　Enterprise Linux ES　v.3
MTA	Postfix	Postfix
登録アカウント数	約 10,000	管理者アカウントのみ

表 1　全学メールサーバとメールゲートウェイの仕様

2.2　スパムメール対策方法

次に、スパムメール対策方法として ERSA を採用した経緯について説明する。本学のメールシステムは 2.1 節で説明した構成となっている関係で、スパムメール対策は、全学メールサーバ とメールゲートウェイ周辺の 2 か所で実施する必要がある。しかし、双方とも周辺機器を含めてレンタル機器群として導入しているものであり、保守契約上の問題からハードウェア型のスパムメール対策製品をこのシステム中に追加で組み込むことはできない。そのため、対策は全学メールサーバ及びメールゲートウェイ上で動作するソフトウェア型製品に限定されることになるのだが、ここで注意すべきことは、双方に搭載されている IMSS のスパムメール対策機能（エンドユーザメールのコンテンツ検索・隔離機能）が、以下の理由により利用できないという点である。

①┌　全学メールサーバ上で IMSS のコンテンツ検索を利用する場合、スパムメールと判定したエンドユーザメールを隔離・保存するディスク領域を別途確保する必要がある。これは、ハードウェアの増設あるいは大幅なシステム構成変更（クラスター構成の解除など）を伴うため、早急な実施が困難である。

②┌ メールゲートウェイは、各部局・研究室管理メールサーバ宛てのメールをリレー処理するゲートウェイの役割を担うものであるため、学内各メールサーバに登録されているエンドユーザアカウントそのものがメールゲートウェイには存在しない。このため、エンドユーザメール隔離作業自体が実施不可能である。

このことは、IMSS に限らずエンドユーザメールのコンテンツ検索・隔離型製品による対策実施が、現状のシステム構成およびレンタル契約の範囲では極めて難しいことを意味する。

こうした本学特有の事情のため、現実を踏まえた実施可能な対策は、MTA ベースの対策に限定される。そして、MTA ベースの対策の中で最も有効な対策として当センターが選択したのが、SMTP 接続の初期段階で接続元の IP アドレスを元にスパムメール発信元かどうか判定する『DNS リアルタイムブラックリスト方式』である。この方式を実施する際に重要となるのが参照先ブラックリストデータベースの選定である。選定において重要視した点は、

①┌ ブラックリストデータベース自身が信頼のおけるものであること。
②　ブラックリストデータベース提供者による十分な

サポート体制が整っていること。

③ ブラックリストデータベース参照が単体として販売されていること。

の 3 点である。当センターで検討した結果、ERSA が最適であるとの結論に至り、採用に至った。

3. 実施に至るまでの過程

ERSA による対策は、誤判定によって正常なメールが届かない状況もあり得るので、全学一律の実施に当たっては、対策方針・方法を明確にした上で全学的な合意を得る必要がある。全学的な合意は、従来、スパムメール対策はメールに対する事実上の検閲にあたるので実施を見送った経緯を踏まえ、今回の対策が、メールの内容ではなくメールの発信元で判断するものであること、また、スパムメールと誤判定された場合でも、発信元に返送されメールのドロップとはならないことを説明した上で、各部局単位で本対策についての是非を審議してもらい、各部局からの審議結果を集約するという形で得ることにした。実施に至るまでの経緯は以下の通りである。

[2007 年 7 月] ： 各部局の代表者で構成される情報基盤センター運営員会を通じて、スパムメール対策の方針・方法を説明。全学メールサーバに対してのみ 1 ヵ月のテスト運用を実施することの是非について、各部局内での審議を要請。

[2007 年 9 月] ： 全学メールサーバに対する 1 ヶ月のテスト運用についての合意を全部局から得る。

[2007 年 11 月] ： 1 ヵ月のテスト運用を実施。

[2007 年 12 月] ： テスト運用の結果を元に、学内に送信されてくる全てのメールに対して一律実施することの是非について、各部局内での審議を要請。

[2008 年 1 月] ： 本格運用についての合意を全部局から得る。

[2008 年 2 月] ： 本格運用開始。

4. テスト運用

スパムメールの判定は、メールの送信元 IP アドレスが ERSA レピュテーションデータベース、すなわちブラックリストに登録されているかどうかだけで判断される。ERSA は Standard Reputation と Dynamic Reputation で構成され、Standard Reputation IP アドレスは、データベースに常時登録されている IP アドレスであり、Dynamic Reputation IP アドレスは、トレンドマイクロ社のスパムメール監視システムが新しいスパムメール送信元を検知した後、数分以内に登録する IP アドレスであり、発信がなくなると自動的にデータベースから削除される。

ERSA は、この Dynamic Reputation IP アドレスの利用に関して、次に示すレベル 0～4 の 5 段階のレベルを提供している。

<レベル 4> 1 通でもスパムメールを検出した場合、その送信元の IP アドレスをデータベースに登録。

<レベル 3> スパムメールを少数検出した場合にその送信元 IP アドレスをデータベースに登録。

<レベル 2> スパムメールを多数検出した場合にその送信元 IP アドレスをデータベースに登録。

<レベル 1> スパムメールを送信しているかどうかに関係なく、既知の有効なメールサーバからのメールを全て許可。

<レベル 0> Dynamic Reputation を利用しない。

検索レベルが高いほど判定されるスパムメールの数も多くなるが、同時に誤判定の数も増加する。従って、本格運用時の設定レベルを確定させるため、テスト運用では、5 段階全てのレベル をテストした。その際、最も強い制限であるレベル 4 での影響を調査することが主目的であったため、テスト総時間数の約半分をレベル 4 での運用に割り当てた。

表 2 にテスト運用の結果を示す。レベル 2 ～ 4 での対策の場合、学外からの SMTP 接続の 7 ～ 8 割がスパムメールと判定されており、ERSA がスパム対策として有効であることが確認できた。誤判定に関しては、レベル 4 での運用において、「届くはずのメールが来ない」などの学内からの問い合わせが数件あった。この誤判定問題への対処と、レベル 3 における SMTP 接続の遮断割合とレベル 4 での遮断割合が、それぞれ 0.754, 0.794 であり、大差ないことなどから、当センターはレベル 3 での本格運用を全学に対して提案し、合意を得るに至った。

LV	H	A	B	C
4	321	1,072,350	851,261	0.794
3	110	340,942	257,212	0.754
2	80	275,350	196,355	0.713
1	88	360,386	197,710	0.549
0	56	177,051	61,267	0.346

LV : レベル
H : テスト運用時間総数 (hours)
A : 学外からの SMTP 接続総数
B: ERSA によって拒否された SMTP 接続総数
C: 遮断割合 (B/A)

表 2. SMTP 接続数で見たスパムメール対策の効果

5. 本格運用

表3に最近のスパムメール対策の運用状況を示す。集計期間は、2008年7月1日～2008年7月21日の3週間である 。学外からの SMTP 接続数の平均は、1日あたり 約28万回で、18%が全学メールサーバへの接続であり、82%がメールゲートウェイへの接続である。ERSAによって拒否された学外からのSMTP接続数の平均は1日あたり22万回で 、これはSMTP接続全体の約81%にあたる。拒否された SMTP 接続の 約 60%が standard Reputation で40%が Dynamic Reputation によるものである。

全学メールサーバとメールゲートウェイの遮断効果を比較すると、全学メールサーバにおけるスパムメール遮断率は SMTP 接続総数の 70%で、テスト運用時とほぼ同じであるのに対して、本格運用時から対策が開始されたメールゲートウェイのそれは84%に及ぶ。全学メールサーバ以上に対策の効果が表れていることがわかる。

スパムメール送信者は、一回の SMTP 接続で一通のメールを送信するわけではなく、一度に複数の宛先にメールを送付することも多々ある。拒否したメールの平均数は、1日あたり約30万通であり、ERSA によって拒否された SMTP 接続 1 回あたりの配送数に換算すると 1.35 通となる。

	全学メールサーバ	メールゲートウェイ	全体
A	49,126	226,274	275,600
B	34,604	189,614	224,218
C	70.4(%)	83.7(%)	81.3(%)
D	50,080	254,653	304,733
E	1.45	1.34	1.35

A: 学外からの1日あたりの SMTP 接続総数の平均値
B: ERSA によって拒否された学外からの 1 日あたりの SMTP 接続総数の平均値
C :学外からの SMTP 接続数に対する ERSA によって拒否された SMTP 接続数の割合 (C=B/A)
D: ERSA によって拒否された1日あたりのメール総数の平均値
E: ERSA によって拒否された SMTP 接続 1 回あたりの配送メール数の平均値 (E=D/B)

表3 2008年7月1日～2008年7月21日（3週間）のスパムメール対策の運用状況

ERSA の導入は、バウンスメール対策に対しても大変有効である。特に、メールゲートウェイに対する効果は絶大である。メールゲートウェイは、学外⇔各部局・研究室管理メールサーバ間のメールを処理するリレーサーバとして機能しているため、学内各メールサーバが返送するバウンスメールも、最終的にはメールゲートウェイが返送処理を請け負うことになる。そのため、対策実施前は、メールゲートウェイ 1 台あたり、1 日で約 1 万通のバウンスメールが deferred され queue に溜まるという状況であり、2～3 日おきに deferred されているバウンスメールの削除を実施していた。(バウンスメールの大部分は、学外ドメインの MALER-DAEMON 宛てのメールであるため、削除は、MAILER-DAEMON 宛てのメールのみ実施)。しかし、ERSA による対策実施後は、deferred されるバウンスメールが 1 台あたり、1 週間で約 3,000 通程度にまで減少し、メールゲートウェイの運用状況が飛躍的に改善された。

6. 今後の課題

今後、本学では、メールのコンテンツ検索・隔離も含めた一層のスパムメール対策強化について検討していく予定であるが、当面の課題は、すり抜けてくるスパムメールに対して費用をかけずにどう対策を取るかである。現在、当センターが検討しているのが、接続元 SMTP クライアントに対する「DNS 逆引き登録確認」の導入である。この方法の導入の是非に関しては、各大学において様々な意見があると思うが、本学では、「DNS の逆引き登録が存在しない = 身元不詳のメールサーバ」と判断し、2008 年 11 月にテスト運用を行い、2009 年 1 月に本格導入を予定している。

すり抜けてくるスパムメールに対する DNS 逆引き登録確認の有効性を大雑把に見積もるため、筆者の一人（志村）に送付されてきたスパムメール 1,000 通のヘッダー情報を調べたところ、DNS 逆引き登録がされていないメールが 754 通存在した。（メールの集計期間 : 2008 年 5 月 31 日～2008 年 7 月 24 日） 。調査に使用したメールが一個人宛てのメールであるというサンプリングバイアスを考慮しても、すり抜けてくるスパムメール全体の 50%程度は、DNS 逆引き登録の確認で受信拒否できることを期待している。

謝辞

富士通（株）には、全学メールサーバおよびメールゲートウェイのメール送受信関連ログから、スパムメールの一日あたりの拒否件数を調べ、自動で管理者に通知するツール、及び、deferred されているバウンスメールの削除ツールを無償で作成してもらいました。ここに感謝の意を表します。