横浜国立大学におけるスパムメール対策 II

― コンテンツ検索及びエンドユーザーメール隔離システムの導入 ―

SPAM-Mail Prevention in Yokohama National University II

― The Content-Based filtering and The End-User Mail Quarantine ―

志村 俊也†, 徐 浩源†, 額田 順二‡
Toshiya Shimura†, Haoyuan Xu†, Junji Nukata‡

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

†横浜国立大学 情報基盤センター
‡横浜国立大学 情報基盤センター長

† Information Technology Service Center, Yokohama National University
‡ Director of 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、トレンドマイクロ社の有償サービス Email Reputation Services Advanced を利用したスパムメール対策を実施しているが、この対策をすり抜けてくるスパムメールをブロックするため、同じくトレンドマイクロ社の製品である InterScan Messaging Security Suite Plus を利用して、情報基盤センターが管理運用する全学メールサーバに登録されている全アカウントにして、「受信メールのコンテンツ(本文)を検索し、スパムメールと判定されたメールは、受信者に配信せずに隔離する」追加対策を 2009 年 5 月より開始した。本稿では、この追加対策実施に至るまでの過程、及び運用状況を報告する。

キーワード

スパムメール対策, コンテンツ検索、 エンドユーザーメール隔離システム

1. はじめに

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『情報基盤センターが管理運用する全学メールサーバ（@ynu.ac.jp メールサーバ、アカウント数 12,000）宛 及び部局等が管理するメールサーバ宛の全メール 』に対して、DNS リアルタイムブラックリスト方式によるスパムメール対策を全学一律に実施している。ブラックリストは、トレンドマイクロ社の有償サービス Email Reputation Services Advanced (以後、ERSA) を利用している（詳細は、文献 [1] を参照）。この対策によ

り、学外から送信されてくるスパムメールの大部分をブロックできるようになり、劇的な成果を上げているが、このERSAによる対策をすり抜けてくるスパムメールに対処するため、全学メールサーバが受信するメールに対しては、メールのコンテンツ検索を行い、スパムメールと判定された場合は受信者に配信せず隔離し、隔離されたスパムメールを個々の利用者が自身で確認し、必要に応じて取り出すことができるシステム『エンドユーザーメール隔離システム』を導入した。これにより、@ynu.ac.jp 宛てのスパムメールをほぼ 100%ブロックすることに成功した。本稿では、この追加対策を実施に至るまでの過程、および実施後の運用状況を報告する。

2. コンテンツ検索/エンドユーザーメール隔離システム

コンテンツ検索/エンドユーザーメール隔離システム(以後、CF/EUQ) として採用した製品は、ERSA と同じトレンドマイクロ社の InterScan Messaging Security Suite Plus (IMSS) である。メール処理の仕組みを図 1 に示す。

処理の流れとしては、
全学メールサーバに対する SMTP 接続➔ MTA でのスパムメール対策(ERSA) ➔ 添付ファイルのウィルス検索・駆除処理 (IMSS)➔ 受信先アドレスが本メールサーバ上に登録されているアカウント宛てであるかどうかの確認処理 (IMSS) ➔ CF/EUQ 処理 (IMSS)
となっている。ERSA は MTA（postfix）上での対策であり、学外からの SMTP 接続のみを検査対象とし、学内からの SMTP 接続は検査しないように設定している。一方、IMSS は送信元によらず全ての受信メールを処理するシステムとなっている。受信先アドレスが本メールサーバ上に登録されているアカウント宛てであるかどうかの確認作業は、学内端末から全学メールサーバを中継して、他のメールサーバに送信されるメールを隔離してしまった場合、受信者自身で隔離されたメールを確認できないために行うものである。登録アカウント宛であるか否かは、認証サーバ(Active Directory, AD) に LDAP で問い合わせることで確認する。(AD には、アカウント登録情報として、ID 、パスワード(PW)、及びメールアドレスが予め登録されている。) 問い合わせの結果、登録アカウント宛てでなかった場合は、CF/EUQ 処理を実行せず、受信先サーバにメールを配信する。登録アカウント宛てであった場合は、CF/EUQ 処理に移行し、スパムメールと判定された場合は隔離する。スパムメールと判定されなかった場合は、受信者に配信される。

個々の利用者は、CF/EUQ 管理専用ウェブサイトにアクセスすることにより、隔離されたスパムメールを確認することができる。具体的には、管理専用ウェブサイトへのアクセスの際 ID/PW の入力を求められ、CF/EUQ は入力された ID /PW を AD に問い合わせ、AD は受け取った ID /PW に対応するメールアドレスを CF/EUQ 側に返す。CF/EUQ は隔離メールの中から、AD から返されたメールアドレスのメールを抜き出して表示する仕組みとなっている。

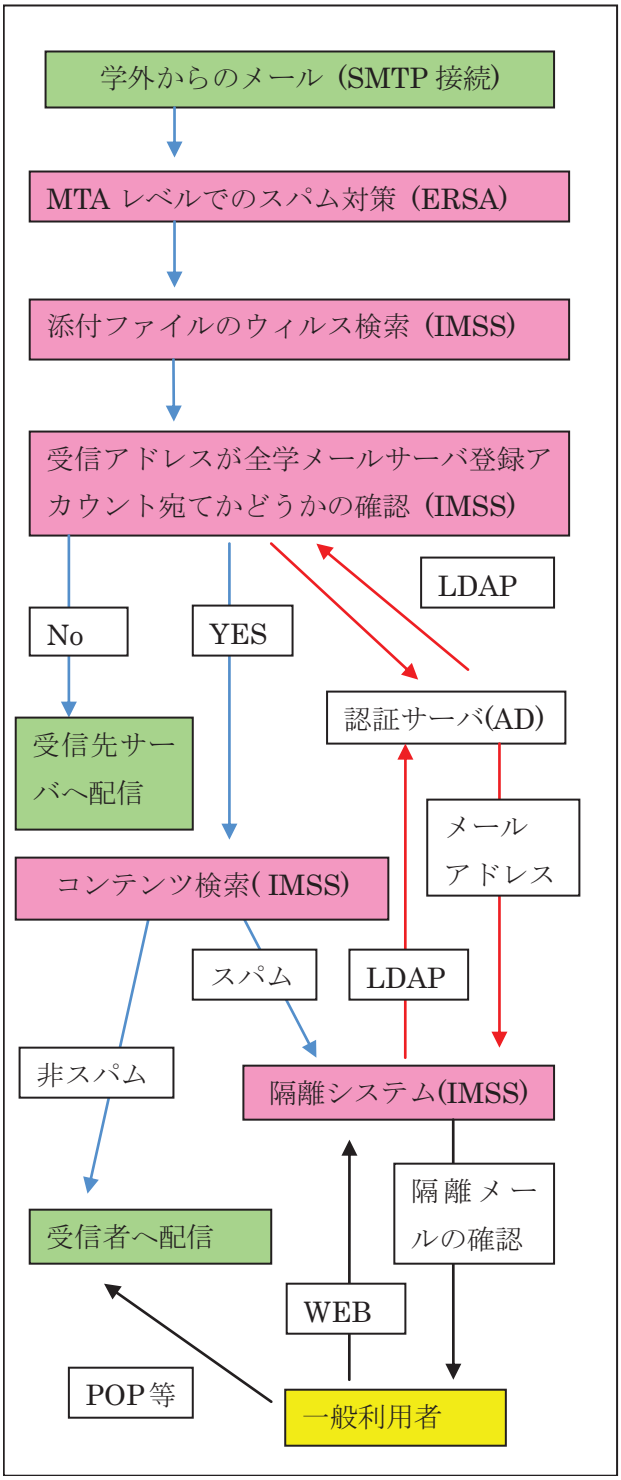

図 1.　メール処理の仕組み

誤判定された隔離メールは、管理専用ウェブサイト上から利用者自身で「非スパムメール」として再配信することが可能である。また、スパムメールとして扱われたくない送信者アドレスを事前にホワイトリストとして登録することも可能である。CF/EUQ に隔離されたメールの保存期間は 35 日間であり、その後は自動消去される。

3. 実施に至るまでの過程

全学メールサーバは、本学の公式メールサーバであるので CF/EUQ を導入するには、ERSA 導入時同様、全学的な合意を得ることが必要不可欠となる。全学的な合意は、ERSA の時と同様(詳細は、文献 [1] を参照)、各部局の代表者で構成される情報基盤センター運営委員会（以後、委員会）を通じて CF/EUQ の是非について各部局単位で審議して頂き、その審議結果を委員会で集約するという手続きで進めることにした。実施に至るまでの過程は以下の通りである。

[2008 年 9 月]　CF/EUQ の必要性及びその具体的な方法を説明し、実施の可能性について意見交換を行う。

[2008 年 11 月]　全学メールサーバに登録されている全アカウントに対して、CF/EUQ の 2 週間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。

[2009 年 2 月]　CF/EUQ のテスト運用に向けて、全学メールサーバのクラスタ構成の設定変更、ディスク領域の拡張（隔離したスパムメールを保存するための領域を作成するため） を行う。また、情報基盤センター関係者のメールアカウントに限定して、CF/EUQ の試験運用を先行して行なう。

[2009 年 3 月]　全学メールサーバに対する 2 週間の CF/EUQ テスト運用実施の合意が全部局から得られ、テスト運用を実施する。

[2009 年 4 月]　テスト運用の結果に加え、CF/EUQ 処理と 2002 年から実施しているメールのウィルス検索･駆除処理との同質性を強調した説明を行い、全学メールサーバに対して CF/EUQ の本格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。

[2009 年 5 月]　全部局から CF/EUQ 本格運用の合意が得られ、正式運用を開始する。同時に、横浜国立大学公式ウェブサイトのトップページ上で、本学がウィルスメール及びスパムメール対策を実施していることの案内、そして、情報基盤センターウェブサイト上で、対策の実施状況[ブロック件数等]の情報公開を開始(更新は 1 週間単位)。

4. 運用状況

CF/EUQ の運用状況を表 1 に示す。データの集計期間は、2009 年 7 月 12 日(日)～8 月 8 日(土)の 4 週間である。学外からの一日当たりの SMTP 接続は、平均 46,965 回で、その中で、ERSA でブロック（接続拒否）した SMTP 接

	平均	最大	最小	標準偏差
[A]　学外からの 1 日当たりの SMTP 接続				
全日	46,965	56,808	30,510	7,168
平日	50,916	56,808	42,348	4,340
土日祝日	38,626	43,570	30,510	3,967
[B]　ERSA でブロックした 1 日当たりの SMTP 接続				
全日	33,355	40,516	23,845	3,802
平日	34,570	40,516	28,213	3,494
土日祝日	30,791	34,958	23,845	3,228
[C]　ERSA でブロックした SMTP 接続 1 回あたりの受信者アドレス数				
全日	1.670	1.910	1.426	0.112
平日	1.653	1.819	1.507	0.086
土日祝日	1.706	1.910	1.426	0.154
[D]　CF/EUQ で隔離した 1 日当たりの SMTP 接続数				
全日	4,340	5,162	3,218	553
平日	4,622	5,162	3,997	388
土日祝日	3,744	4,134	3,218	325
[E]　ERSA 及び CF/EUQ を通過した SMTP 接続数　: E=A-B-D				
全日	9,270	13,198	3,299	3,741
平日	11,724	13,198	9,890	987
土日祝日	4,091	5,050	3,299	744
[F]　ERSA 及び CF/EUQ を通過した SMTP 接続数の全 SMTP 接続に対する割合。(F=E/A)				
全日	0.191	0.267	0.088	0.061
平日	0.231	0.267	0.198	0.016
土日祝日	0.106	0.121	0.088	0.014
[G]　ERSA 及び CF/EUQ でブロックした SMTP 接続の内、CF/EUQ でブロックした割合 :　G=D/(B+D)				
全日	0.115	0.134	0.099	0.009
平日	0.118	0.134	0.110	0.007
土日祝日	0.109	0.121	0.099	0.008

表 1.　F/EUQ の運用状況

続は 33,355 回、CF/EUQ でブロック（隔離）した SMTP 接続数は 4,340 回である。IMSS は、送信元を問わず全てのメールを処理するので、この CF/EUQ ブロック数は、学外からのメールだけでなく、学内から送信されたメールに対するブロック数もカウントされている。CF/EUQ でブロックしたメールの内、送信元が学内であるメールが占める割合は不明であるが、大部分は学外からの送信であることは確実なので、ここでは、CF/EUQ でブロックしたメールは全て学外から送信されたメールであると仮定して話を進めることにする。上記の仮定の下でスパムメール対策を通過したメール数を計算すると、一日当たり平均　9,271 通となり、学外からの全 SMTP 接続の約 20%しかないことがわかる。言い換えると学外から送信されてくるメールの約 80%は、スパムメールであるということが明らかになった。ERSA と CF/EUQ でブロックした SMTP 接続の内、CF/EUQ でブロックした接続の割合は、10%程度であり、スパムメールの 90%が ERSA でブロックされていることになる。

平日と土日祝日の違いを比べてみると、学外からの SMTP 接続数[A]は約 12,000、ERSA でのブロック数[B]は約 4,000、CF/EUQ での隔離数[D]は約 1000、ERSA および CF/EUQ を通過した SMTP 接続数[F]は約 7,000、土日祝日の方が少ない。学外から送信されてくるメールに対するスパムメールの割合は、平日は77%なのに対して、土日祝日は 90%にもなっている。

一般に、スパムメール送信者は、複数の宛先にメールを送信するので、SMTP 接続数(送信メール数)と受信者アドレス数（宛先アドレス数）は、必ずしも一致しない。ブロックした SMTP 接続数に対する ERSA でブロックした受信者アドレス数の割合の平均値は 1.67 であるので、CF/EUQ でブロックした受信アドレス数も送信者数の 1.67 倍程度であると推測できる。

学外からの SMTP 接続数やブロックした SMTP 接続数等の A～G の各数値の 1 日単位の変動に関しては、標準偏差が平均値の 2 割以内であることからもわかるように、１日単位で大きく変化するようなことはなく、大体は、平均値前後を推移している。

CF/EUQ の誤判定率がどの程度かを調べるには、個々の利用者に問い合わせるしかないので、正確な値はわからない。しかし、筆者および本学情報基盤センター関係者の範囲では、通常メールがスパムメールと判定された例は非常に少なく、また、CF/EUQ をすり抜けてくるスパムメールは、筆者については 1 週間に 2,3 通程度であり、これらのことから推測すると、誤判定率は極めて低いと考えられる。従って、全学メールサーバ宛てのスパムメールはほぼ100%ブロックすることに成功したと言える。なお、CF/EUQ の運用開始に伴い、ERSA による対策は不要なのではないかとの意見が当然出てくる。しかし、ERSA による対策は、『全学メールサーバが、バウンスメールアタックの踏み台にならないようする』という、全学メールサーバの学外に対する信頼性を維持するという CF/EUQ では実施困難な重要な役割も担っているため、ERSA による対策は引き続き運用している。

5. 通信の秘密及びプライバシーの保護との関係

CF/EUQ の是非を議論する際に問題となるのが、「通信の秘密」及び「プライバシーの保護」との関係である。本学では、委員会での審議の際、部局の１つである「国際社会科学研究科」からこの問題に関して大変有意義な意見を頂いたため、全部局合意を得ることできた。この意見は、本学のみならず、他大学がスパムメール対策を行う上での参考にもなると思うので、全文をそのまま掲載する。ここで、国際社会科学研究科とは、経営系・経済系・法律系の 3 種類の専攻からなる大学院組織であるが、経営系及び経済系は学部が存在し、それぞれの学部から委員が選出されているので、国際社会科学研究科からは、法律系専攻の代表が委員として選出され、委員会への意見も法律系専攻の意見を表明することが認められている。

平成 21 年 5 月 12 日(月)

スパムメール対策についての
国際社会科学研究科の考え方

○　憲法第 21 条第 2 項によって保障される通信の秘密は、個人として生きていく上で必要不可欠な権利である。この趣旨を受けて、電気通信事業者の取扱中に係る通信の秘密については電気通信事業法により、有線電気通信における通信の秘密は有線電気通信法により、それぞれ罰則をもって保護されている。なお、通信の秘密には、通信の内容だけでなくその存在の秘密が確保されることも含まれ、上記の各法律の保護の及ぶ範囲は、通信内容だけでなく、通信当事者の住所、氏名、通信日時、発信場所等通信の構成要素や通信の存在の事実の有無を当然に含むものと解されている。

○　たしかに、企業・省庁・大学などが、その従業員等が業務に関して相互に通信を行うための LAN を自ら設置・運営する場合については、法人の代表者又は法人若しくは人の使用者その他の従業員が、その法人又は人の業務に関して行う通信の場合は、その者は当該法人又は人の機関たる地位にあり、その効果は直接当該法人又は人に帰属するものであるから、その法人又は人の「自己」の通信であって、「他人」の通信とはならず、電気通信役務（電気通信事業法第 2 条第 3 号参照）に該当しないという見解もある。

○　また、大学がその教職員および学生に対して提供

するメール送受信サービスは、自らの業務の遂行に当たって、またはそれに付随して、電気通信設備を業務上の関係を有する他人との通信の用に供するものであり、「他人の需要」に応ずるものとはいえないから、電気通信事業法の定める電気通信事業者には該当しないとも考えられる（同法第２条第４号参照）。

○　そのため、本学は電気通信事業者に該当せず、教職員および学生に対して提供する通信役務について、電気通信事業法第３条（検閲の禁止）および第４条（秘密の保護）の適用はないと解される。

○　しかしながら、そのことから組織内ネットワークにおける従業員・利用者等の通信に関する利用者の秘密やプライバシーといった権利がまったく保護されないことを意味するわけではない。①会社内のネットワークにおいて、有線電気通信法（同法９条（有線電気通信の秘密の保護））の適用の有無が問題となる可能性があること、および②従業員のプライバシー保護という観点からの配慮が必要であることも指摘されているところである。
（参照）総務省「電気通信サービスＦＡＱ（よくある質問）」
（http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_faq/index.html）

○　もっとも、仮に通信の秘密やプライバシー保護との関係が問題になるとしても、そのことから通信の秘密やプライバシーが無制限に保護されるものではなく、正当業務行為など一定の事情が存在すれば、それらを制約する行為の違法性が阻却される。そして一般に、正当業務行為として認められるためには、⑴行為の必要性及び正当性、⑵手段の相当性が必要であると考えられる。

○　まず、⑴行為の必要性及び正当性の要件については、大量の迷惑メールが送信されてくる状況では、それにより引き起こされるメールサービスの遅延等の支障を防ぐ必要があることから、この要件を満たすと考えられる。また、日々配信されるスパムメールを各教職員が、その都度手動で処理すること自体が、教育研究業務の重大な支障となっているとの認識も示されている。

○　次に、⑵手段の相当性について検討する。本スパムメール対策は、試験運用の結果により、上記必要性との関係において有効なものと確認されているほか、あらかじめ設定した一定の条件に合致するか否かを機械的に検索し、その条件に合致した電子メールを隔離するにとどまるものである（本対策により誤検知されたメールも一定期間保管されるほか、そのメールの発信元を登録して隔離対象から除外することも可能とされている。）。大学内LANの利用が自家消費であるという側面を踏まえれば、現時点において、本スパムメール対策は上記目的を達成するための手段としてなお相当性を失うものではなく、正当業務行為と認められ、仮に通信の秘密やプライバシー保護との関係が問題になるとの立場を採用したとしても、違法性が阻却されると考えることができる。

○　以上より、本スパムメール対策が有効に機能し、かつその誤検知による問題を低減するための措置があわせて実施されているとの認識を前提として、本スパムメール対策に賛成するものとする。すなわち、①本スパムメール対策が目的達成のために相当であることについて定期的に再評価をすること、および②メールが誤検知された場合にそのことを認識することが容易となるよう、外部の通信者に対し、本学が本スパムメール対策を導入していることをホームページ等において告知すること、を条件とした上で、本スパムメール対策の導入に賛成する。

以上

上記のように、法律の専門家からCF/EUQが「通信の秘密」及び「プライバシー保護」には抵触しないとの見解が得られたことの意義は大変大きく、他部局等の個人からの質問や異議申し立てに対する回答としても活用できるので、情報基盤センター職員の説明に割かれる時間を節約でき、説得するための精神的ストレスを減じるという意味も大きい。この国際社会科学研究科の意見は本学の様々な事情を考慮した上でのものなので、他大学に対しても適用できるとは限らないが、スパムメール対策の導入を検討する上で、プライバシー侵害の問題で困っている場合は、本学の事例を参考にして頂ければと思う。なお、この「考え方」に対して、直接的・間接的に、本学国際社会科学研究科に問い合わせたり、意見を伝えたりすることはご遠慮頂きたい。

6. おわりに

本学では、2008年2月から、トレンドマイクロ社の有償サービスERSAを利用したDNSリアルタイムブラックリスト方式のスパムメール対策の全学一律実施を開始し、2009年5月からは、同じくトレンドマイクロ社の製品であるIMSSを利用してCF/EUQによるスパムメール対策を全学メールサーバに登録されている全アカウントに対して導入した。本学のスパムメール対策の特徴は、「全学一律実施」であり、個々の利用者の要望は受け付けないという厳しいものであるため、準備、学内利用者への説明等を含めると、企画から実施まで2年間要した。様々な面で大変ではあったが、その甲斐あって、全学メールサーバに関しては、スパムメールをほぼ100%ブロックすることに成功し、部局・研究室が管理するメールサーバにおいても、約9割のスパムメールをブロックすることに成功した。本学が2年間かけて行ったスパムメール対策が他大学の参考になれば幸いである。

参考文献

[1] 志村俊也, 徐浩源, 長谷部勇一 ： 「横浜国立大学におけるスパムメール対策」、学術情報処理研究、No.12, 2008, P77