【現状報告】 迷惑メール対策の経緯と今後

The circumstances and future of the measure against an unsolicited junk e-mail

岡崎　知也
Tomoya OKAZAKI

国立大学法人　旭川医科大学　情報基盤センター
Information and Communication Technology Center,
National University Corporation Asahikawa Medical University

概要

本稿では迷惑メールに対してこれまで本学が実施してきた対策と新たに発生している問題点について報告する．本学に LAN が設置され，電子メールが利用され始めてから間もなく迷惑メールが送られてくるようになった．本学に届く迷惑メールの対策としてサーバ・クライアントでそれぞれ対策を施し，また本学が迷惑メールの送り手とならないための対策も施して一定の効果を上げることができている．しかしながらこれらの対策の結果新たな問題も発生しており，このことに関する考察についても報告する．

1. はじめに

国内の一般社会に電子メールが普及して約 20 年経っている．これとほぼ同じ時期に迷惑メールの存在も問題しされ続けており，現在も対策が必要な状況である．

本稿では，本学における迷惑メールに対してこれまで行ってきた対策と新たに発生している問題点について報告する．

2. 電子メール・迷惑メール

2.1. 迷惑メールの歴史

インターネットの前身である ARPANET に初めて電子メールが送信されたのが 1971 年，そして世界最初の迷惑メールはディジタル・イクイップメント・コーポレーション（DEC）が 1978 年 5 月に送信した営業メールであるとされている [1].

日本においてもインターネットが一般社会に普及し始めた 1994 年，最初の大規模な迷惑メールとなった“Green Card Spam”が登場し [2]，国内でも主に宣伝・詐欺を目的とする迷惑メールが当時から現在にわたるまで送信されており，社会問題となっている．

2.2. 本学への影響

本学に学内 LAN が設置され，学術情報ネットワーク（SINET[1]）に接続されたのが 1995 年

[1] http://www.sinet.ad.jp/

である. その 1～2 年後に Web サーバを稼働させたのとほぼ同時に, webmasterやWebページに掲載している教職員のアドレスへ広告のメールが送信されたのが本学における迷惑メールの始まりのようである.

2000 年～2003 年頃にかけてはコンピュータウィルス・ワームによるメール（Code Red[2], Nimda[3], Sircam[4], Netsky[5]）が学内で多く見られた.

ほぼ同じ頃より, 学内の教職員の個人アドレス宛にも国内外から種々の迷惑メールが送信されるようになり, その数も徐々に増加していき, それ以来大学全体としての対策を取らざるを得ない状況になっていった.

3. 対策

3.1. 受信側の対策

3.1.1. クライアント側

本学において迷惑メールの問題が顕在化した当初は, 利用者自らが手動で削除したり, 着信拒否リストで対応したりといった簡単なものであったが, 次第に手動で対応しきれない件数となり, 送信者アドレスもその都度変えてきて着信拒否リストが意味をなさなくなっていった.

メールソフトの変更に抵抗のない利用者は Thunderbird のような迷惑メールフィルタ機能を持ったものに乗り換えていた. また, POPFile[6]をサーバとメールソフトの間にかませて自動で迷惑メールを振るい落とす利用者もいたが, 全学的には敷居が高いようで, 一部の利用者のみが行っていた様子であり, サーバ側での対策も求められるようになっていった.

3.1.2. サーバ側

クライアント側で対応のとれない利用者のために, bsfilter[7] を POP3 プロキシとして動作させ, 迷惑メールと判定されたものについては件名の先頭に"[SPAM]"の文字列を付加するようにした.

2008 年から現在のシステムが導入された 2010 年にかけて, メールサーバの前段で SpamAssassin[8]を動作させ, さらに利用者ごとに迷惑メールと判定される閾値を Web インターフェースから設定でき, また各利用者が正規メールと迷惑メールをSpamAssassinに学習させることができるよう, Maia Mailguard[9]を運用した. 多少の False Positive[10]が発生したが, 隔離の履歴を Web やダイジェストメールにより各利用者に確認してもらうことで大きな問題にはならず, 本学においては迷惑メール対策の効果が大きいと概ね好評価であった. Fig.1 ～ Fig.3 にスクリーンショットを示す.

現在のシステム（2010 年～2015 年予定）では迷惑メール対策アプライアンス(シマンテック社 Brightmail Gateway[11])を採用しており, 導入前と比較すると本学利用者のメールボックスに着信する迷惑メールは大幅に減少しており, 3.1.1 に示すクライアント側での対策はほとんど必要なくなっている. Brightmail Gateway には種々のレポート機能があり, その１つである「全体の概略」レポートを Fig. 4 に示す.

---

2 http://www.ipa.go.jp/security/virus/virus_sub.html#W32/CodeRed

3 http://www.ipa.go.jp/security/virus/virus_sub.html#W32/Nimda

4 http://www.ipa.go.jp/security/virus/virus_sub.html#W32/Sircam

5 http://www.ipa.go.jp/security/virus/virus_sub.html#W32Netsky

6 http://getpopfile.org/docs/jp

7 http://en.sourceforge.jp/projects/bsfilter/

8 http://spamassassin.apache.org/

9 http://www.maiamailguard.com

10 正常メールが迷惑メールと誤って判定されること

11 http://www.symantec.com/ja/jp/messaging-gateway

Fig. 1　Maia Mailguard ログイン画面

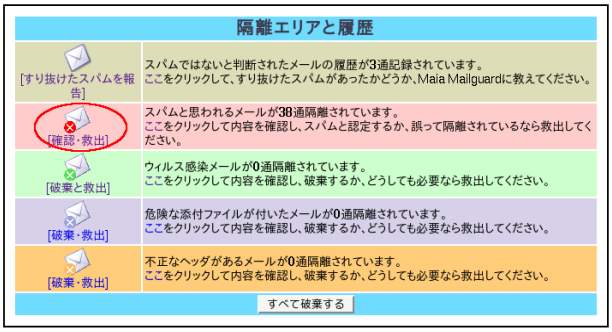

Fig. 2　隔離エリアと履歴

Fig. 3　隔離中の迷惑メール一覧

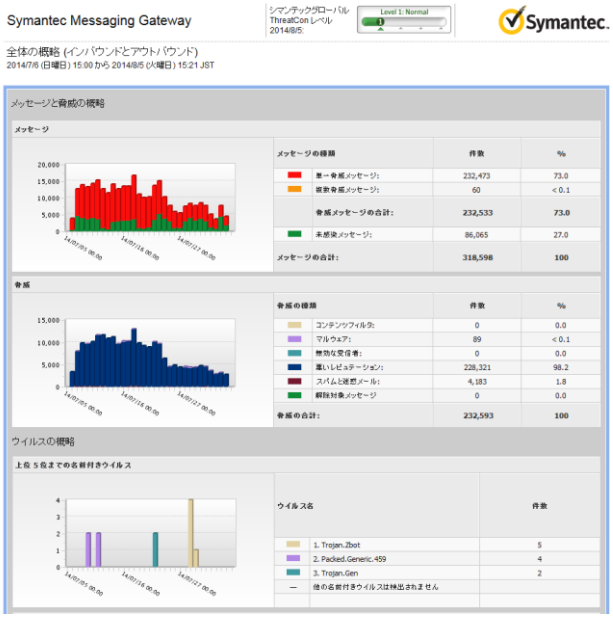

Fig. 4　Brightmail Gateway のレポート機能

3.2. 送信側の対策

メール送信時，本学の教職員には学外・学内からの接続を問わず SMTP 認証を必須としている．OP25B[12]は学内の事情により実施していない．

また，送信ドメイン認証のための SPF[13]レコードを本学 DNS サーバに登録し公開している．

4.　新たな問題

現在導入している迷惑メール対策ゲートウェイは相当の効果を上げており，「迷惑メールが送られてきて困る」という相談を受けることはなくなっている．しかしながら，同システムが採用している RBL[14]に学外の送信者の MTA[15]が登録されてしまったことにより，本学へのメール送信ができないということが数回発生している．その都度先方の MTA の IP アドレスを調

12 http://e-words.jp/w/OP25B.html
13 http://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/spf/
14 http://e-words.jp/w/RBL.html
15 http://e-words.jp/w/MTA.html

べ, 本学側のホワイトリストへ登録することにより個別対応を行ってきた.

一方, 3.2 で述べたとおり本学の利用者が送信を行う際には SMTP 認証を行うこととしており, 利用者の便宜のため学外からも Submission ポート(TCP/587)を通して接続することを認めているが, ある利用者の SMTP アカウントが乗っ取られてしまい, 3rd Party Relay の状態に陥ってしまったことがあった. このことが原因で本学の MTA が RBL に載ってしまい, 特定のドメインに対して本学からの送信ができない事例が発生した.

また, 本学ではメーリングリストを利用して全学生への一斉送信を行うことがあるが, 配信されていないというケースが頻発した. 学生用アドレスは現在本学のオンプレミスのサーバにより発行・運用しているが, 学生の一部は外部のメールサービスに転送してメールを確認している. その転送先のメールサービスによってバルクメールと判断されてしまい, 自動的に破棄されたことによるものと思われる.

5. おわりに

本稿では, 本学における迷惑メールの状況, その対策の経緯, および現状として新たに発生している問題について報告をおこなった.

4 で述べた, 本学の MTA が意図せず 3rd Party Relay となってしまった問題については今後の課題であるが, 来年初めのシステム更新の要件として「万が一 SMTP アカウントが乗っ取られた場合, 学外へ送信する単位時間あたりのメール数を制限する」という対策を盛り込んだことにより, 改善が期待される.

迷惑メールについては, 100% 有効な対策は存在せず, 従来の対策手法を破るものがいずれ出現することが予想され, 今後も対策に力を注ぎ続ける必要があると思われる.

謝辞

筆者の本研究会への参加に際しご快諾頂いた高井章副学長・情報基盤センター長に感謝の意を表します.

(参考文献)

[1] ITpro, “ニュース - sendmail 開発者 Eric Allman が語る「ネットの夜明けとスパムの歴史」: ITpro,” [オンライン]. Available: http://itpro.nikkeibp.co.jp/article/NEWS/20061121/254431/.

[2] INTERNET Watch, “sendmail の開発者が語るメール 25 年の歴史、「メールを使いすぎ」と警告も,” [オンライン]. Available: http://internet.watch.impress.co.jp/cda/event/2006/11/22/14023.html.