# 【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<sup>1</sup>) に接続されたのが 1995 年

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<sup>2</sup>, Nimda<sup>3</sup>, Sircam<sup>4</sup>, Netsky<sup>5</sup>) 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<sup>6</sup>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<sup>7</sup>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<sup>8</sup>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<sup>9</sup>を運用した。多少の False Positive<sup>10</sup>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<sup>11</sup>)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.

http://www.ipa.go.jp/security/virus/virus\_sub.html #W32/CodeRed

<sup>3</sup> http://www.ipa.go.jp/security/virus/virus\_sub.html #W32/Nimda

<sup>4</sup> http://www.ipa.go.jp/security/virus/virus\_sub.html #W32/Sircam

http://www.ipa.go.jp/security/virus/virus\_sub.html #W32Netsky

<sup>6</sup> http://getpopfile.org/docs/jp

<sup>7</sup> http://en.sourceforge.jp/projects/bsfilter/

<sup>8</sup> http://spamassassin.apache.org/

<sup>9</sup> http://www.maiamailguard.com

<sup>10</sup> 正常メールが迷惑メールと誤って判定されること

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



[English]

Fig. 1 Maia Mailguard ログイン画面

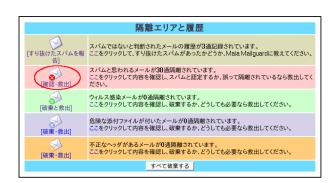


Fig. 2 隔離エリアと履歴

これらのメールの状態を確定する							
スコア	受信日時	差出人	宛先	件名	・スパム	○正規メール	○破損
42.429	2008-03-24 08:37:03	Married Street,	STREET, SQUARE,	. 散*哭栖,窮尿*霧	(r	C	0
34.687	2008-03-24 05:14:26	manufactured.	ARREST SERVICE	. 新着会員メッセージ	0	C	0
32.311	2008-03-24 02:30:34			. TPM_ 楽蝋巣_関債_自?_講	C	C	0
30.955	2008-03-24 02:37:53	AND DESCRIPTION OF	and to see the second	. 念岬 劇尖 俊棋 廢劑 晒餐膳	0	C	C
29.841	2008-03-24 03:29:23	Marine Street	Minute office	. Incredible soluti	(*)	C	0
24.823	2008-03-24 04:41:44	man man	-	. Vlagra (Sildenafi	0	C	0
24.644	2008-03-24 05:55:42	Market Street	street side	. 泌,採,盾,臀,斥強·隈 嗎二·	(°	C	0
24.224	2008-03-24 03:17:13	Market Street	man and a	. Put an end to you	(*)	C	0
23.559	2008-03-24 05:35:44	AND DESCRIPTION OF THE PERSON NAMED IN	the second lines.	焼ラ「itワウノミヘスヌカネ * Mt		0	0
21.254	2008-03-24 04:42:28	MARKET STREET	street with	, special deal on r		0	0
21.244	2008-03-24 02:40:36	medical con-	the supposed lines.	仟恢瞳寫廣道級單晒塘寫臺?朕砿实		C	C
21.244	2008-03-24 06:26:22	management .	and contract of	. 仟恢瞳寫廣送級單路填寫產?朕祉尖	0	0	C
18.964	2008-03-24 03:17:05	mentioned.	more plant	. Rolex is not for	0	C	0
18.045	2008-03-24 03:18:34	married to the last	and the same of	. 悲來伏恢柴回珠電鼓砿尖	(0)	9	0
18.045	2008-03-24 03:18:38	medicario.	distance of the last	恭來伏恢柴回職電殼鉱尖	0	0	C
17.663	2008-03-24 07:01:34	MARKET THE PARTY NAMED IN	Service plants	. Most Popular Watc	0	0	0
16.134	2008-03-24 06:55:29	Maria Maria Maria	AND RESIDENCE.	FW: Be a ceos-wit	æ	C	C
15.564	2008-03-24 07:01:16	entranspolic .	named to the last	. Reward your exper	0	0	0
15.525	2008-03-24 04:22:00	Marine Marine	Section of the last	. agp video card slots	(8)	0	0
15.2	2008-03-24 02:56:30	TO THE ROOM PARK	-	砂垢坦叟返過荷括式匍屬假尖	0	0	C
15.9 Done	2008.03.24.02.56:31			(166日日日日本本村村 中田田田田)	a.	aia,asahikawa-me	-

Fig. 3 隔離中の迷惑メール一覧

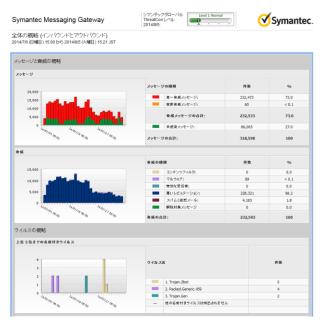


Fig. 4 Brightmail Gateway のレポート機能

## 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<sup>14</sup>に学外の送信者の MTA<sup>15</sup>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

<sup>12</sup> http://e-words.jp/w/OP25B.html

http://salt.iajapan.org/wpmu/anti\_spam/admin/ tech/explanation/spf/

<sup>14</sup> http://e-words.jp/w/RBL.html

<sup>15</sup> 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/NEW
  - http://itpro.nikkeibp.co.jp/article/NEW S/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.