2008 年度卒業論文

迷惑メールは発信時刻を偽るか？

研究指導　菊池浩明　教授

東海大学　電子情報学部　情報メディア学科

5adm2128　鈴木　孝彰

5adm1108　水沼　暁

目次

第 1 章　はじめに
第 2 章　調査と発見
　　2.1　Yahoo!Mail 発信元の調査
　　2.2　全世界の Yahoo!Mail に迷惑メール送信
　　2.3　結果と発見
第 3 章　迷惑メールデータ収集
　　3.1　メールアドレスを WEB 上に公開し迷惑メールを収集
　　3.2　出会い系サイトに登録し迷惑メールを収集
第 4 章　研究に用いた機材
　　4.1　使用機材
　　4.2　SSD/Linux から Debian GNU/Linux 4.0 etch へ移行
第 5 章　迷惑メールデータの可視化
　　5.1　概要
　　5.2　可視化の対象
　　5.3　可視化グラフ
　　5.4　考察
第 6 章　結論と課題
　　6.1　結論
　　6.2　今後の課題
謝辞
参考文献

第1章　はじめに

迷惑メールは多いときに数百件以上届くこともあり、Email の利便性を大きく損なう。先行研究では、迷惑メールの送信元である懸賞サイトに登録し、最初の迷惑メールが届くまでの日数や、懸賞サイトの迷惑メール発信率が報告されている。しかし、送信元で時間を偽装することは容易であり、これらが考慮されていない。

そこで本研究では、迷惑メールの送信元の送信時刻と、受信側の受信時刻の差をとり、偽装時刻の大きさを可視化するシステムを開発した。本システムの実装と、それを用いて抽出した特徴について報告する。本システムを応用し、送信時刻を偽装しているものを迷惑メールと判断すれば、効果的に受信メールから除外することができる。

第2章 調査と発見

2.1 Yahoo!Mail 発信元の調査

個人の Yahoo!Mail から 2008 年 5 月 1 日から 2008 年 5 月 30 日までの迷惑メールデータを取得し、メールヘッダー情報から IP アドレスを抜き出し whois にかけて国コードの調査を行った。その結果を表 2.1 に示す。

表 2.1　50 通の Yahoo!Mail 迷惑メール発信元 IP 国コード数

国コード	国名	数	同一第1オクテット数	第1オクテット
AU	オーストラリア	25	1	59
			1	60
			3	117
			12	121
			2	122
			4	123
			1	124
			1	125
US	アメリカ	5	1	24
			1	65
			1	74
			2	76
NL	オランダ	3	1	77
			1	78
			1	87
IN	インド	3	1	203
			1	210
			1	220
CH	中国	2	1	211
			1	221
GB	イギリス	1	1	82
HK	香港	1	1	219
FR	フランス	1	1	195
TR	トルコ	1	1	195

UY	ウルグアイ	1	1	190
none	不明	7	1	59
			2	66
			1	69
			2	201
			1	201

2.2 全世界の Yahoo!Mail に迷惑メール送信

Yahoo!Mail は全世界で 34 カ国でサービスを行っている。各国で迷惑メールフィルターは同じ振舞いをするか調査を行った。菊池教授から 1000 通の迷惑メールをいただき、その迷惑メールの中からランダムで選んだ 100 通の迷惑メールを各国に送信した。表 2.2 に各国で取得した Yahoo!Mail アカウントと送信元 IP 情報を示す。

表 2.2 取得した Yahoo!Mail アカウントと送信元 IP 情報

アメリカ大陸	Americas	IP address	yahoo mail
アルゼンチン	Argentina	98.136.44.36	numa_turbo_ar@yahoo.com.ar
ブラジル	Brazil	68.142.206.220	numa_turbo_br@yahoo.com.br
カナダ	Canada	98.136.44.39	numa_turbo_ca@yahoo.ca
チリ	Chili	76.13.13.85	numa_turbo_cl2@yahoo.cl
コロンビア	Colombia	76.13.13.82	numa_turbo_co2@yahoo.com.co
メキシコ	Mexico	98.136.44.36	numa_turbo_mx@yahoo.mx
ペルー	Peru	76.13.13.88	numa_turbo_pe2@yahoo.com.pe
アメリカ	yahoo.com	98.136.44.48	numa_turbo_us@yahoo.com
ベネズエラ	Venezuela	76.13.13.71	numa_turbo_ve2@yahoo.com.ve
ケベック（カナダ）	Quebec	76.13.13.71	numa_turbo_que2@yahoo.ca
テレムンド（アメリカ）	Telemundo	76.13.13.88	numa_turbo_tel2@yahoo.com

ヨーロッパ	Europe		
オーストリア	Austria		メールサービス無し
カタラン(スペイン系)	Catalan	76.13.13.71	numa_turbo_cat2@yahoo.es
デンマーク	Denmark	217.146.182.187	numa_turbo_dk@yahoo.dk
フィンランド	Finland		メールサービス無し
フランス	France	87.248.110.149	numa_turbo_fr@yahoo.fr
ドイツ	Germany	87.248.110.137	numa_turbo_de@yahoo.de
イタリア	Italy	87.248.110.173	numa_turbo_it@yahoo.it

オランダ(イギリス系)	Netherlands	76.13.13.72	numa_turbo_net2@yahoo.co.uk
ノルウェー	Norway	87.248.110.166	numa_turbo_no@yahoo.no
ロシア	Russia	76.13.13.65	numa_turbo_rus2@yahoo.com
スペイン	Spain	87.248.110.169	numa_turbo_es@yahoo.es
スウェーデン	Sweden	87.248.110.177	numa_turbo_se@yahoo.se
スイス	Switzerland		メールサービス無し
イギリス	United Kingdom	87.248.110.169	numa_turbo_uk@yahoo.co.uk

アジア	Asia Pacific		
アジア	Asia	76.13.13.72	numa_turbo_asi2@yahoo.com
オーストラリア	Australia	98.136.44.48	numa_turbo_au@yahoo.com.au
中国	China	203.209.250.108	numang_turbong@yahoo.cn
香港	Hong Kong		メールサービス無し
インド	India	203.212.170.72	numa_turbo.in@yahoo.in
インドネシア	Indonesia	119.160.244.191	numa_turbo_ind2@yahoo.co.id
日本	Japan		numa_turbo_jp@yahoo.co.jp
韓国	Korea		韓国在住のみサービス利用可
マレーシア	Malaysia	119.160.244.190	numa_turbo_my2@yahoo.com.my
ニュージーランド	New Zealand	76.13.13.73	numa_turbo_nz2@yahoo.co.nz
フィリピン	Philippines	203.188.202.88	numa_turbo_ph2@yahoo.com.ph
シンガポール	Singapore	68.142.206.220	numa_turbo_sg@yahoo.com.sg
台湾	Taiwan		メールサービス無し
タイ	Thailand	68.142.201.24	numa_turbo_th@yahoo.co.th
ベトナム	Vietnam	203.188.202.89	numa_turbo_vn2@yahoo.com.vn

2.3 Yahoo!Mail を使った迷惑メール収集

Yahoo!Mail アカウントと同時に、Yahoo!がサービスをしている無料 WEB スペース geocities を取得し、WEB ページに Yahoo!Mail のメールアドレスを掲載し迷惑メール収集を行った。表 2.3 に作成した WEB ページを示す。Yahoo!Mail のサービスをしているが geocities のサービスをしていない国にはアメリカの geocities を代わりに登録した。

表 2.3　作成した WEB ページの geocities アドレス

アメリカ大陸	各国の geocities
アルゼンチン	http://ar.geocities.com/numa_turbo_ar/
ブラジル	http://br.geocities.com/numa_turbo_br/

カナダ	http://ca.geocities.com/numa_turbo_ca
チリ	http://www.geocities.com/numa_turbo_cl2/
コロンビア	http://www.geocities.com/numa_turbo_co2/
メキシコ	http://mx.geocities.com/numa_turbo_mx/
ペルー	http://www.geocities.com/numa_turbo_pe2/
アメリカ	http://www.geocities.com/numa_turbo_us/
ベネズエラ	http://www.geocities.com/numa_turbo_ve2/
ケベック（カナダ）	http://www.geocities.com/numa_turbo_que2/
テレムンド（アメリカ）	http://espanol.geocities.com/numa_turbo_tel2/
ヨーロッパ	
オーストリア	
カタラン(スペイン系)	http://www.geocities.com/numa_turbo_cat2/
デンマーク	http://www.geocities.com/numa_turbo_dk/
フィンランド	
フランス	http://www.geocities.com/numa_turbo_fr/
ドイツ	http://de.geocities.com/numa_turbo_de/
イタリア	http://it.geocities.com/numa_turbo_it/
オランダ(イギリス系)	http://www.geocities.com/numa_turbo_net2/
ノルウェー	http://www.geocities.com/numa_turbo_no/
ロシア	http://www.geocities.com/numa_turbo_rus2/
スペイン	http://es.geocities.com/numa_turbo_es/
スウェーデン	http://www.geocities.com/numa_turbo_se/
スイス	
イギリス	http://uk.geocities.com/numa_turbo_uk/
アジア	
アジア	http://www.geocities.com/numa_turbo_asi2/
オーストラリア	http://au.geocities.com/numa_turbo_au/
中国	http://www.geocities.com/numang_turbong@yahoo.cn/
香港	
インド	http://in.geocities.com/numa_turbo_in/
インドネシア	http://www.geocities.com/numa_turbo_ind2/
日本	
韓国	

マレーシア	http://www.geocities.com/numa_turbo_my2/
ニュージーランド	http://www.geocities.com/numa_turbo_nz2/
フィリピン	http://www.geocities.com/numa_turbo_ph2/
シンガポール	http://sg.geocities.com/numa_turbo_sg/
台湾	
タイ	http://www.geocities.com/numa_turbo_th/
ベトナム	http://www.geocities.com/numa_turbo_vn2/

2.4 調査結果と発見

国コードの調査では、オーストラリアの割合が多い。全世界に向けて迷惑メールを送ったが、結果としてはすべて迷惑メール扱いになった。国コードの全世界の Yahoo!Mail で迷惑メールフィルターの振舞いについて調査したかったが失敗した。

しかし、迷惑メールヘッダー情報からある発見をした。迷惑メールの送信元の送信時刻（Date）と、受信側の受信時刻（From）の差があることを発見した。実際の迷惑メールのヘッダー情報を表 2.4 に示す。送信元の時刻では、2007 年 3 月 16 日と記録されているが、受信元の時刻では 2007 年 3 月 20 日と 3 日間の差があることがわかる。他にも迷惑メールの中に時刻偽装をしているものは多く見つけることができた。

表 2.4　送信時刻と受信時刻の差が見られるメールヘッダー

From AuthorLisa@oricomall.com　Tue Mar 20 18:55:56 2007
Return-Path: <AuthorLisa@oricomall.com>
Received: from kuwa.ep.u-tokai.ac.jp (kuwa.ep.u-tokai.ac.jp [150.7.50.207])
by noisy.cs.dm.u-tokai.ac.jp (8.12.11.20060308/8.12.8) with ESMTP id l2K9ttON019133
for <kikn@cs.dm.u-tokai.ac.jp>; Tue, 20 Mar 2007 18:55:55 +0900
Received: from sh.wide.ad.jp (sh.wide.ad.jp [203.178.137.85])
by kuwa.ep.u-tokai.ac.jp (8.11.6/3.7W) with ESMTP id l2K9tta28905
for <kikn@ep.u-tokai.ac.jp>; Tue, 20 Mar 2007 18:55:55 +0900
From: "photog Suri" <AuthorLisa@oricomall.com>
To: kikn@wide.ad.jp
Subject: Keys Amanda Bynes Angelina
Date: Fri, 16 Mar 2007 16:43:50 +0100
MIME-Version: 1.0

第3章　迷惑メールデータ収集

3.1　概要

時刻偽装をする迷惑メールを観測するために、迷惑メールの収集を行った。

3.2　WEB 上にメールアドレスを公開し迷惑メールを収集

ホームページ上にメールアドレスを公開し、迷惑メールを収集した。収集期間は 2008 年 4 月 1 日から 2008 年 11 月 13 日までである。

3.3　無料出会い系サイトに登録し迷惑メールを収集

Yahoo!Japan がサービスをしている「Yahoo!出会い」に登録し、サクラと思われる女性と数回連絡を取り合った。その後、「Yahoo!出会い」とは関係のないメールが届きはじめた。「Yahoo!出会い」とは関係のないメールを迷惑メールとした。

第 4 章 研究に用いた機材

4.1 使用機材

今回の研究を行うにあたって、表１のような機能をもった機材を利用した。

表１、OpenMicroServer

製品名	OpenMicroServer(TM)
型番	OMS-AL400/128
CPU	AMD Alchemy(TM) 400MHz プロセッサ 消費電力：0.5W(Tipcal)
MEMORY	128MB (PCB 基盤直接実装　容量変更不可) PC133 SDRAM 512Mbit(64MB)チップ x2
FLASH ROM	16MB(ユーザエリア 2MB) NOR 型 Spancion チップ
NIC	10/100/1000BaseTX x2 10/100BaseTX x1 (Poe 受電：TypeA/B に対応)
シリアルポート	RJ45・コンソール専用（3 線結線）x1 RJ45・FULL 結線 x1
USB	USB2.0 (TYPE-B) x2
DIO	8bit (Input x4, Output x4) 2mm ピッチ pin
内蔵ストレージ	コンパクトフラッシュ（PI0４まで対応） Transcend CompactFlash 8GB 換装
スイッチ	INIT スイッチ
表示・警告	ステータス LED x3　LAN アクセス LED
外形寸法	102(W)　×230(D)×33(H)mm ゴム足 0,5mm
本体材質	アルミ合金製
価格	56400 円

4.2　SSD/Linux から Debian GNU/Linux 4.0 etch へ移行

マイクロサーバーに搭載される「SSD/Linux」は、Plat’s Home 社が開発・維持・配布を行っており、オープンソースの独自ディストリビューションである。また、マイクロサーバーは Debian 対応している。オープンラボラトリ(http://www.plathome.co.jp/support/labo/)に Debian の OS イメージが配布されています。Debian の OS イメージをダウンロード･展開し、コンパクトフラッシュをルートデバイスとして設定することで Debian をマイクロサーバー上で利用可能にした。

第 5 章　迷惑メールデータの可視化

5.1　概要

メールヘッダー情報から受信･送信元時刻のデータを gnuplot を用い時刻の差を表示する。

5.2　可視化の対象

送信元の送信時刻（Date）、受信側の受信時刻（From）のデータを用いて可視化する。

5.3　可視化グラフ

図 5.1 に無料出会いサイトのメールデータを可視化したものを示す。

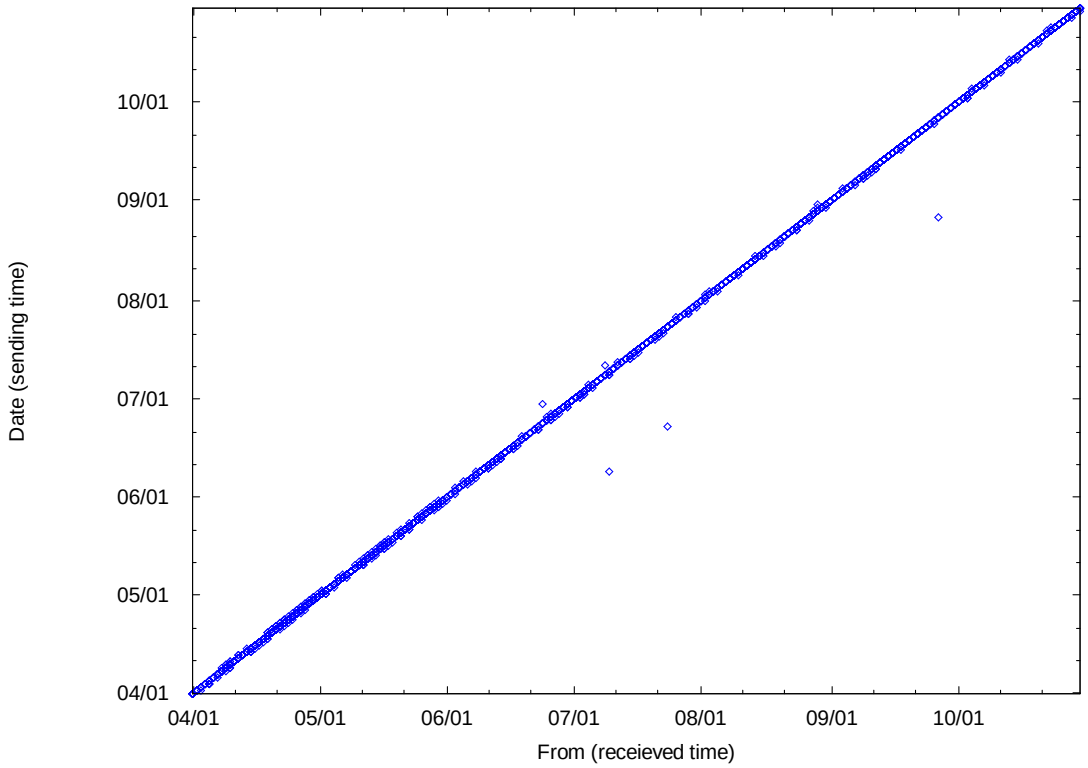

図 5.1　無料出会い系サイトのメールデータ

図 5.2 に WEB 上にメールアドレスを公開したメールデータを可視化したものを示す。

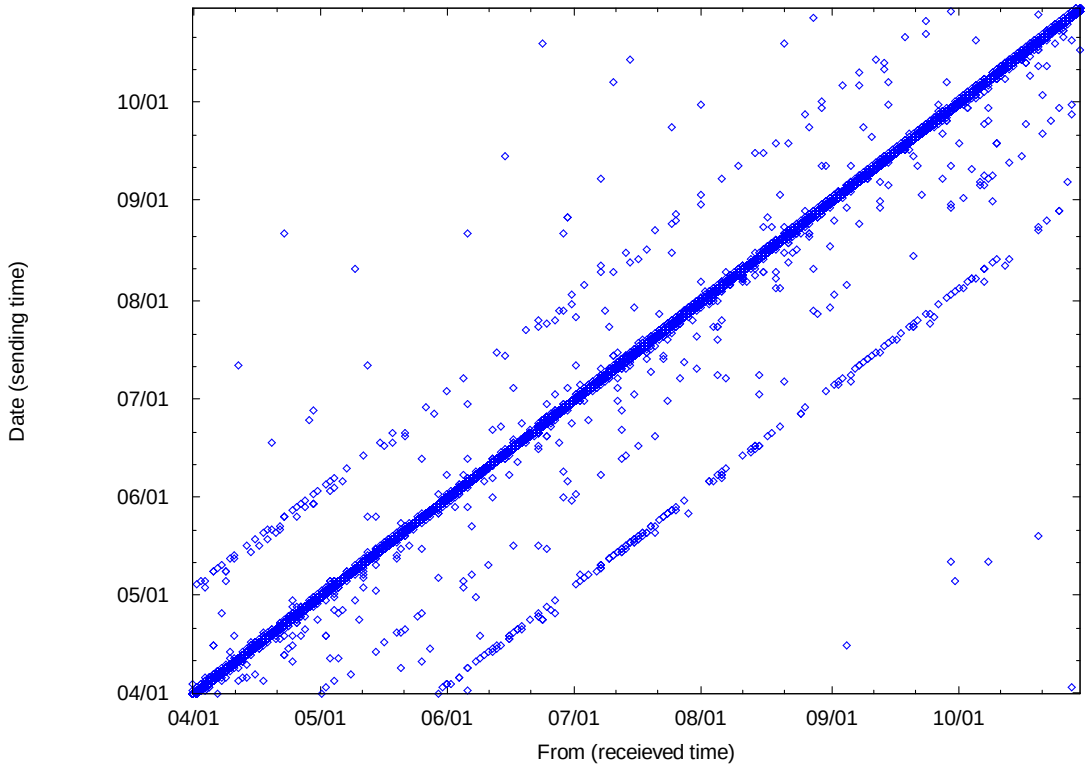

図 5.2 WEB **上に公開したメールデータ**

5.4　考察

無料出会い系サイトのメールデータでは、時刻の差は少ないものが多かった。WEB **上にメールアドレスを公開したメールデータでは、**1 **ヶ月又は** 2 **ヶ月の時刻の差が多く見られた。時刻の差が起こっている迷惑メールは、迷惑メール送信者が迷惑メールとして扱われないようにするための対策を行っているのではないかと考える。また、時刻設定の管理が不十分なメールサーバーが多いのではないかと考えられる。**

第 6 章　結論と課題

6.1　結論

迷惑メールの収集を行い、送信元の送信時刻および受信側の受信時刻の差を可視化することを実現し、時刻の差を知覚しやすくなった。

6.2　今後の課題

送信元の送信時刻および受信側の受信時刻の差の特徴を見つけ、効率的に迷惑メールを防止することが課題にあげられる。

謝辞

本研究を完遂するにあたり，多大なご指導を受け賜りました東海大学電子情報学部情報メディア学科菊池浩明教授に心から感謝を申し上げます。

また，常に暖かいご指導を受け賜りました菊池研究室大学院生の小堀智弘氏に深くお礼申し上げます。

さらに，この一年を共にした菊池研究室の同期の皆さんに感謝の意を述べると共に，謝辞とさせて頂きます。

参考文献

[1]斉藤,望月,“懸賞サイトに登録するとスパムは来るの？”,2006 年度東海大学卒業研究,2007.

付録

Debian GNU/Linux 4.0 etch インストール済パッケージ

迷惑メールの第一オクテットアドレスについての分布図