

2006 年度卒業論文

懸賞サイト登録による スパム動向調査と解析ツール作成

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

3adm1214 齋藤紗織

3adm3123 望月美貴

目次

第1章 はじめに

第2章 スпамとリスト

2.1 スパムの定義

2.2 リスト

第3章 解析ツール

3.1 概要

3.2 構成

3.3 前準備

3.4 実行プロセス

第4章 実験

4.1 観測方法

4.2 観測結果

4.2.1 スпам受信状況

4.2.2 アドレスの重複

4.3 スпам返信

4.3.1 方法

4.3.2 結果

第5章 スパムの内容

第6章 Web 実験

6.1 観測方法

6.2 観測結果

6.3 懸賞との比較

第7章 結論

参考文献

謝辞

第1章 はじめに

電子メールは、インターネット上のコミュニケーション手段の一つであり、安易な通信手段として広く普及している。しかしながら現在、悪質な業者から送られてくるスパムメールが、電子メールサービス全体に多大な悪影響を及ぼしている。全トラフィック中、約70%がスパムメールである。また、不要なメールが大量に送られてくることへのユーザーのストレスも大きい。こういったスパムは、登録サイトから漏洩したメールアドレスやアドレス検索ロボットによって収集されたアドレスに対して送られるといわれている。しかし、本当にそうだろうか？また、スパムに返信するとどうなるのだろうか？^[1]

本研究では、その実態の定量的な調査・評価を目的として、検証用アドレスを用意して懸賞サイトへ登録する実験を行った。以下の項目について調査した結果を報告する。

1. 懸賞サイトに登録し何件のサイトからスパムが来るか
2. 一つのサイトから一日のスパムの到着頻度
3. 登録してから最初のスパム到着までの時間
4. スパムに返信し、スパムの振る舞いの変化

第2章 スパムとリスト

2.1 スパムの定義

スパムとは、いわゆる未承諾広告メールの事を指し、受信者の意に反し勝手に送られてくる広告メールのことを言う。

今回の実験では、懸賞サイトに登録後に、そのサイトから懸賞に応募した事を通知するメールや、メールマガジンが配信されることがある。また、懸賞サイト登録と同時に、別のサイトへ自動登録される場合がある。そのため、登録した懸賞サイト及び、自動登録されることが明記されていたサイト以外からのメールを**スパム**とする。

2.2 リスト

スパムとスパムではないメールを判別するために、送信元アドレスを二つに区別しリストを作成する。スパムではないメールの送信元アドレス、つまり受信メールのうち、登録した懸賞サイト及び、自動登録されることが明記されていたサイトからのメールの送信元アドレスのリストをハムリスト呼ぶ。また、スパムの送信元アドレス及び、スパムの本文中に記載されていたアドレスのリストをスパムリストと呼ぶ。

第3章 解析ツール

3.1 概要

本研究では開発言語に Java を用い、スパムの判別や解析を自動化するプログラムを作成した。各メールアドレスのログデータからスパム数をカウントし、アプレットでグラフを表示させる。

3.2 構成

Newlog.java	ログデータの更新プログラム
read.java	送信元アドレスと受信日時を抽出プログラム
spamMail.java	スパム判定プログラム
spamCount.java	スパム数のカウントプログラム
Gra.java	アプレットでグラフ表示プログラム
log	各アカウントのログデータをおくフォルダ
w_list	各アカウントのハムリストをおくフォルダ
mailData	各アカウントの受信メールデータをおくフォルダ
spamData	各アカウントのスパムデータをおくフォルダ
b_list	各アカウントのスパムリストをおくフォルダ

3.3 前準備

(1) サーバ上から各メールアドレスのログデータをダウンロードした ajifry1～ajifry100 を log/内におき、複製して ajifry1.txt～ajifry100.txt を作成する。

(2) w_list/内にハムリスト ajifry1.txt～ajifry100.txt を作成する。

3.4 実行プロセス

(1) read.java を実行し、ヘッダ情報から必要なデータを取り出す。

ログデータ log/ajifry1.txt～ajifry100.txt から各メールの送信元アドレスと受信日時を抽出し、それらの一覧 mailData/ajifry1.txt～ajifry100.txt を作成する。各アカウントの最新メールの情報を mailData/lastmail.txt に書き出す。

(2) spamMail.java を実行しスパム判定を行う。

mailData/ajifry1.txt ～ ajifry100.txt の送信元アドレスと、ハムリスト w_list/ajifry1.txt～ajifry100.txt のアドレスを比較し、一致しなければスパムと判断する。スパムメールの一覧を spamData/spamData.txt に書き出す。

(3) spamCount.java を実行し、スパム数をカウントする。

スパムメールの一覧を spamData/spamData.txt から受信日時を抽出し、日付別、曜日別、時間帯別にスパム数をカウントし、それぞれ spamData/day.txt, week.txt, time.txt に書き

出す。

(4) Gra. java を実行しグラフを表示する。

spamData/day.txt, week.txt, time.txt から、アプレットでグラフを作成する。実行画面を図 1 に示す。

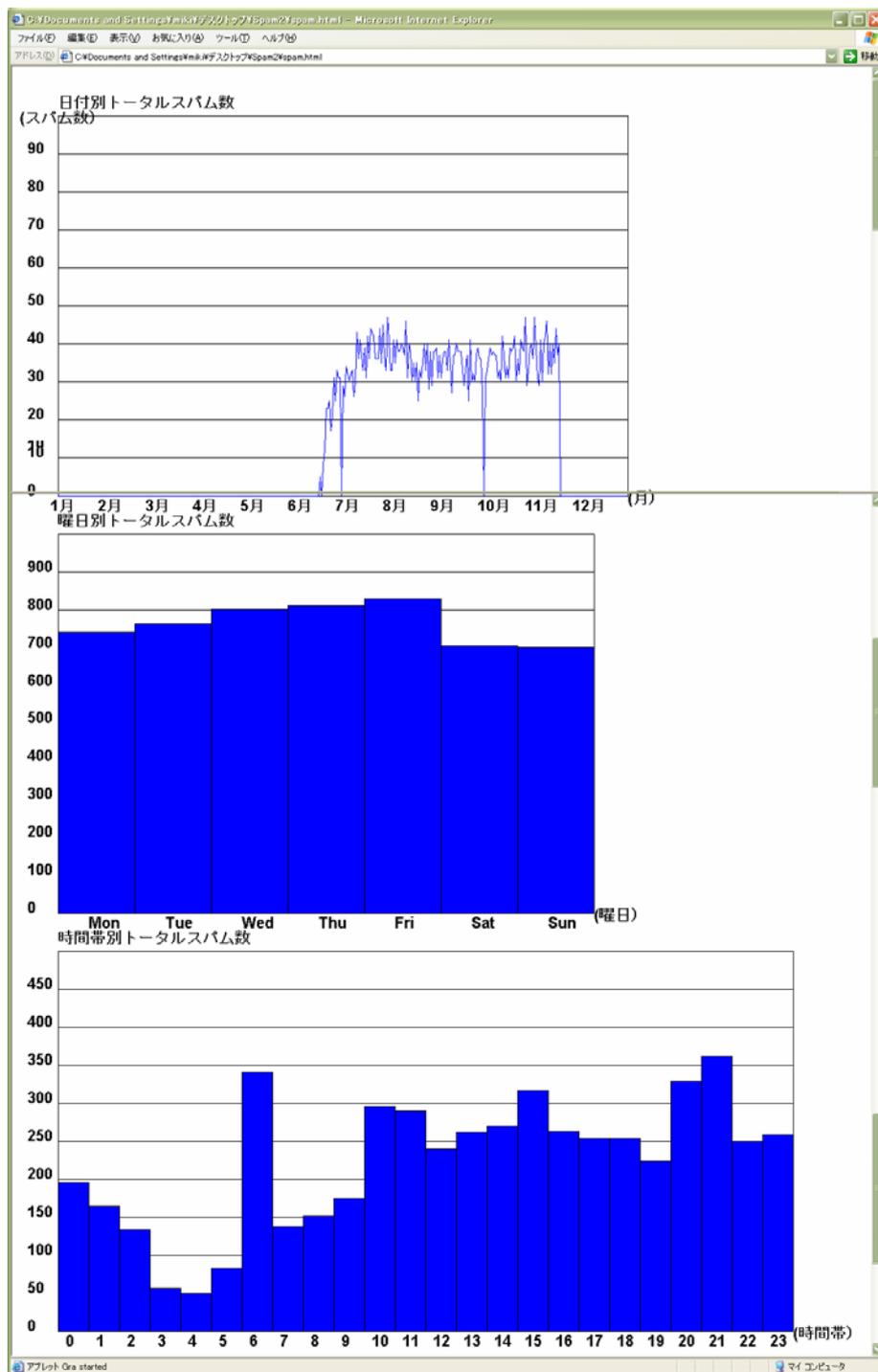


図 1 実行画面

(5) Newlog. java を実行し、ログデータを更新する。

最新のログデータ ajifry1～ajifry100 を log/内におき、以前の最新メール情報を記録している mailData/lastmail.txt と比較する。新しいデータがあれば以降のデータを該当する ajifry***.txt に付け足す。

第4章 実験

4.1 観測方法

100 件の懸賞サイトを選出し、それぞれ別の検証用アドレスで登録した。ただし、携帯電話番号やアドレスの入力が必須のサイトは除外した。実験に使用した懸賞サイトの一覧を表 1 に示す。

表 1 懸賞サイト一覧

検証用アドレス	懸賞サイトアドレス
ajifry1@cs.dm.u-tokai.ac.jp	http://1pri.tv/
ajifry2@cs.dm.u-tokai.ac.jp	http://777.ag/?media_code=a8b120x60c
ajifry3@cs.dm.u-tokai.ac.jp	http://beauty.ichiba.tv/2006/05/pr0606.html
ajifry4@cs.dm.u-tokai.ac.jp	http://bijin.letsn.net/present/
ajifry5@cs.dm.u-tokai.ac.jp	http://car.mag2.com/gasoline.html
ajifry6@cs.dm.u-tokai.ac.jp	http://d-atari.jp/kaido/mag.htm
ajifry7@cs.dm.u-tokai.ac.jp	http://d-atari.jp/kikaku/ds.htm
ajifry8@cs.dm.u-tokai.ac.jp	http://depart.livedoor.com/present/detail?id=1079
ajifry9@cs.dm.u-tokai.ac.jp	http://depart.livedoor.com/present/detail?id=1098
ajifry10@cs.dm.u-tokai.ac.jp	http://donbei.jp/tabekurabe_2006/index.html
ajifry11@cs.dm.u-tokai.ac.jp	http://ga-me7.com/
ajifry12@cs.dm.u-tokai.ac.jp	http://go.prjapan.co.jp/get500.php?i=12572_121_07a4_p39613
ajifry13@cs.dm.u-tokai.ac.jp	http://greenlife.ab-shops.com/
ajifry14@cs.dm.u-tokai.ac.jp	http://homepage1.nifty.com/momiziya/sub13.htm
ajifry15@cs.dm.u-tokai.ac.jp	http://jjil.com/i/prize/z133/?tid=6
ajifry16@cs.dm.u-tokai.ac.jp	http://kindly-life.com/hpgen/HPB/entries/20.html
ajifry17@cs.dm.u-tokai.ac.jp	http://www.e-aidem.com/web_contents/8/plan/con_nekocam_01.html
ajifry18@cs.dm.u-tokai.ac.jp	http://kitchen.netshop-mall.com/
ajifry19@cs.dm.u-tokai.ac.jp	http://kzanmai.jp/
ajifry20@cs.dm.u-tokai.ac.jp	http://letsn.net/present/
ajifry21@cs.dm.u-tokai.ac.jp	http://manga.submit.ne.jp/
ajifry22@cs.dm.u-tokai.ac.jp	http://maruhiro-suisan.net/
ajifry23@cs.dm.u-tokai.ac.jp	http://no1-otoku.com/present/index.html
ajifry24@cs.dm.u-tokai.ac.jp	http://pre.tanoc.net/
ajifry25@cs.dm.u-tokai.ac.jp	http://presen10.com/quiz/top.htm

ajifry26@cs.dm.u-tokai.ac.jp	http://presentmail.jp/janet
ajifry27@cs.dm.u-tokai.ac.jp	http://qscom.net/present.php?SPID=6412
ajifry28@cs.dm.u-tokai.ac.jp	http://reg.yosoo.net/camp.php
ajifry29@cs.dm.u-tokai.ac.jp	http://sandspit.jp/3asp/janet.htm
ajifry30@cs.dm.u-tokai.ac.jp	http://shop.fruitmail.net/page.php?cate=INDEX&page=camp15#go
ajifry31@cs.dm.u-tokai.ac.jp	http://uranai.mag2.com/events/200605leisure/
ajifry32@cs.dm.u-tokai.ac.jp	http://vr.ifbg.jp/signup/signup.cgi?sh=passo7
ajifry33@cs.dm.u-tokai.ac.jp	http://www.1st-chance.net/
ajifry34@cs.dm.u-tokai.ac.jp	http://www.bd-g.com/?ad_code=bdg0003
ajifry35@cs.dm.u-tokai.ac.jp	http://www.bidders.co.jp/dap/sv/cbpre1?seq_exhibit_id=68839736
ajifry36@cs.dm.u-tokai.ac.jp	http://www.bidders.co.jp/dap/sv/cbpre1?seq_exhibit_id=68999975
ajifry37@cs.dm.u-tokai.ac.jp	http://www.bidders.co.jp/dap/sv/cbpre1?seq_exhibit_id=69043933
ajifry38@cs.dm.u-tokai.ac.jp	http://www.bloom-s.co.jp/kenshou/
ajifry39@cs.dm.u-tokai.ac.jp	http://www.boastmain.com/present.htm
ajifry40@cs.dm.u-tokai.ac.jp	http://www.chance.com/
ajifry41@cs.dm.u-tokai.ac.jp	http://www.chancenow.com/member.php?RID=105
ajifry42@cs.dm.u-tokai.ac.jp	http://www.chanken.jp/?ad_code=qcp0001
ajifry43@cs.dm.u-tokai.ac.jp	http://www.choya.co.jp/campaign/umenohi2006/recipe/present/index.html
ajifry44@cs.dm.u-tokai.ac.jp	http://www.c-lifeitem.com/
ajifry45@cs.dm.u-tokai.ac.jp	http://www.deepring.jp/enq/tiffany0601.html
ajifry46@cs.dm.u-tokai.ac.jp	http://www.enjoytokyo.jp/PR091Top.html?mcode=6
ajifry47@cs.dm.u-tokai.ac.jp	http://www.evp.jp/campaign2.php
ajifry48@cs.dm.u-tokai.ac.jp	http://style-up.jp/topics/news/present_0620.html
ajifry49@cs.dm.u-tokai.ac.jp	http://www.fruitmail.net/fm_camp/index.html
ajifry50@cs.dm.u-tokai.ac.jp	http://www.fukazawa-office.com/happy/
ajifry51@cs.dm.u-tokai.ac.jp	http://www.gourmet-digest.com/pre/present060607.htm
ajifry52@cs.dm.u-tokai.ac.jp	http://www.fukubiki.com/vgu/Regist.do
ajifry53@cs.dm.u-tokai.ac.jp	http://www.hayakawa-sm.co.jp/hyousi.htm
ajifry54@cs.dm.u-tokai.ac.jp	http://www.hitget.com/tk_mail/kisoji/present.shtml
ajifry55@cs.dm.u-tokai.ac.jp	http://www.hitget.com/tk_mail/kyoudou/present_main_healthy.html
ajifry56@cs.dm.u-tokai.ac.jp	http://www.hitget.com/tk_mail/roadside/present.shtml
ajifry57@cs.dm.u-tokai.ac.jp	http://www.hokkaidou.co.jp/present_b.htm
ajifry58@cs.dm.u-tokai.ac.jp	http://www.imo.ne.jp/keis-coffee/present/present.html
ajifry59@cs.dm.u-tokai.ac.jp	http://www.j-echo.com/o-kusyonn.htm
ajifry60@cs.dm.u-tokai.ac.jp	http://www.jsweets.com/system/present/cgi-bin/presentpageview.cgi?custid=UPP000048
ajifry61@cs.dm.u-tokai.ac.jp	http://www.kabukun.net/modules/present1/index.php?id=20

ajifry62@cs.dm.u-tokai.ac.jp	http://www.kanzogenki.com/present.html
ajifry63@cs.dm.u-tokai.ac.jp	http://www.kensho11.com/
ajifry64@cs.dm.u-tokai.ac.jp	http://www.kmks.jp/?ad_code=kmp0002
ajifry65@cs.dm.u-tokai.ac.jp	http://www.kujibiki.net/v2/
ajifry66@cs.dm.u-tokai.ac.jp	http://www.lion-pbox.net/camp/item02.html
ajifry67@cs.dm.u-tokai.ac.jp	http://www.love7000.com/present3b.html
ajifry68@cs.dm.u-tokai.ac.jp	http://www.lovekensyo.com/
ajifry69@cs.dm.u-tokai.ac.jp	http://www.lovekensyo.com/present/?link=49236
ajifry70@cs.dm.u-tokai.ac.jp	http://www.lovekensyo.com/present/?link=49563
ajifry71@cs.dm.u-tokai.ac.jp	http://www.mu-ryo.com/top.php?ref=pa0011
ajifry72@cs.dm.u-tokai.ac.jp	http://www.paso-navi.com/dr2/g.cgi?i=janet
ajifry73@cs.dm.u-tokai.ac.jp	http://www.paso-navi.com/u1/g.cgi?i=adw
ajifry74@cs.dm.u-tokai.ac.jp	http://www.poincho.com/j2.html
ajifry75@cs.dm.u-tokai.ac.jp	http://www.point-purse.jp/y/5/ja-net.html
ajifry76@cs.dm.u-tokai.ac.jp	http://www.point-purse.jp/y/8/?m=10018
ajifry77@cs.dm.u-tokai.ac.jp	http://www.prenavi.com/
ajifry78@cs.dm.u-tokai.ac.jp	http://www.present55.com/yosoo/joint.cgi?p=90
ajifry79@cs.dm.u-tokai.ac.jp	http://www.prizegarden.jp/
ajifry80@cs.dm.u-tokai.ac.jp	http://www.redmax.jp/?ad_code=p10192
ajifry81@cs.dm.u-tokai.ac.jp	http://www.standmail.net/diamond/apply1.php?cid=10001&rid=23
ajifry82@cs.dm.u-tokai.ac.jp	http://www.standmail.net/momotaro/apply1.php?cid=10003&rid=20
ajifry83@cs.dm.u-tokai.ac.jp	http://www.syukado.jp/365/index.html
ajifry84@cs.dm.u-tokai.ac.jp	http://www.tadassu.com/cp/apply.php?p=97&mag=janet
ajifry85@cs.dm.u-tokai.ac.jp	http://www.rakuten.co.jp/kuwakabu/699150/699139/
ajifry86@cs.dm.u-tokai.ac.jp	http://www.tubox.com/
ajifry87@cs.dm.u-tokai.ac.jp	http://www.tuduki.net/present/
ajifry88@cs.dm.u-tokai.ac.jp	http://www.yokubariking.com/a1.html
ajifry89@cs.dm.u-tokai.ac.jp	http://www007.upp.so-net.ne.jp/mossmoss/puresent.html
ajifry90@cs.dm.u-tokai.ac.jp	http://zaku-k.jp/pc/index.php?AddCode=c0230
ajifry91@cs.dm.u-tokai.ac.jp	http://zen-pre.com/game/?janet
ajifry92@cs.dm.u-tokai.ac.jp	https://ebet.jp/user/newuser/form1.php/?a=vc
ajifry93@cs.dm.u-tokai.ac.jp	https://www.aucsale.com/jsp/apply_form09.jsp
ajifry94@cs.dm.u-tokai.ac.jp	https://www.diyana.com/mall/present/ace6/
ajifry95@cs.dm.u-tokai.ac.jp	https://www.diyana.com/mall/present/dyna2/
ajifry96@cs.dm.u-tokai.ac.jp	https://www.dreammail.jp/touroku/001/
ajifry97@cs.dm.u-tokai.ac.jp	https://www.jtb.co.jp/west/mail/

ajifry98@cs.dm.u-tokai.ac.jp

<https://www.sagafan.com/present/200606/>

ajifry99@cs.dm.u-tokai.ac.jp

<https://www.sankakukuji.com/join.php?adid=janet>

ajifry100@cs.dm.u-tokai.ac.jp

<https://www.tepore.com/mr/Touroku.htm?LFROM=A&web>

4.2 観測結果

4.2.1 スпам受信状況

観測期間は6/17～11/18である。

使用した100の検証用アドレスのうち12のアドレスが約5000通のスパムを受信した。日付別、曜日別、時間帯別のスパムの頻度をそれぞれ図2、図3、図4、各アカウントの受信状況を表2に示す。

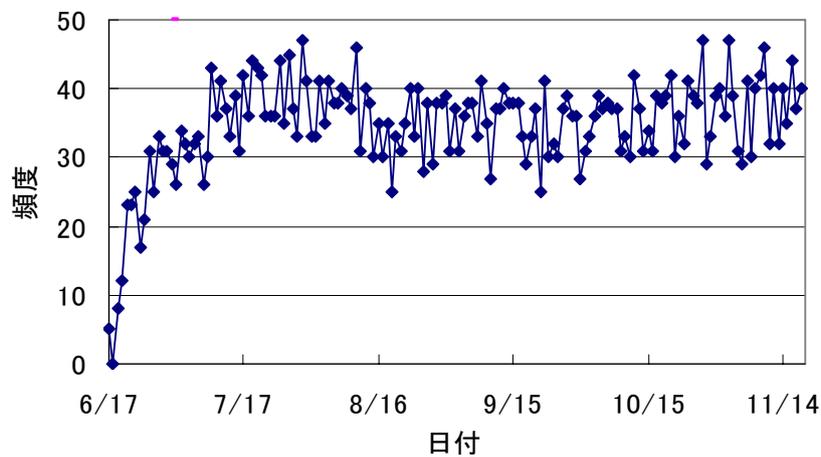


図2 日付別頻度

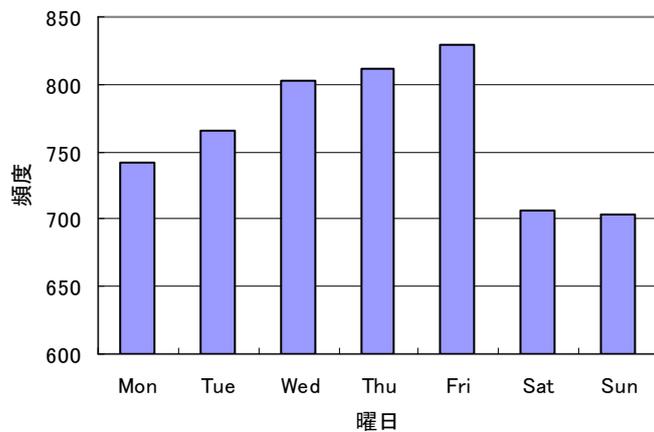


図3 曜日別頻度

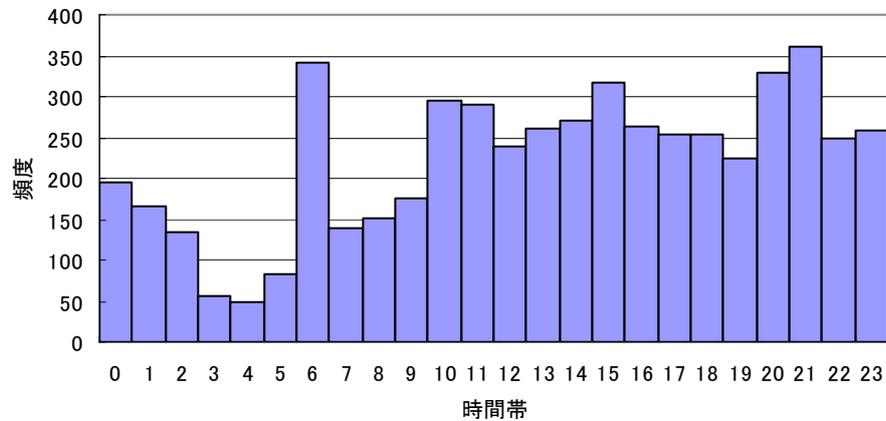


図 4 時間帯別頻度

表 2 アカウント毎の受信状況

アカウント名	メール数			一日のスパム数				最初のスパム 到達時間[日]
	総受信数	スパム数	ハム数	平均	最大	最小	標準偏差	
ajifry1	960	461	499	2.97	6	0	1.18	4
ajifry6	184	24	160	0.15	2	0	0.38	1
ajifry7	2023	1563	460	10.08	16	0	2.78	3
ajifry11	815	106	709	0.68	2	0	0.48	16
ajifry13	6	6	0	0.04	2	0	0.22	34
ajifry15	289	40	249	0.26	1	0	0.44	52
ajifry18	6	6	0	0.04	2	0	0.22	41
ajifry25	1735	1481	254	9.55	15	0	2.7	6
ajifry26	1828	706	1122	4.55	11	0	1.6	3
ajifry55	77	65	12	0.42	4	0	0.7	1
ajifry74	461	455	6	2.94	5	0	1.1	4
ajifry84	2709	448	2261	2.89	6	0	1.36	4
平均		446.75	477.67	2.88	6.00	0.00	1.10	14.08
標準偏差		554.13	657.03	3.57	5.22	0.00	0.89	17.89
最大				10.08	16.00	0.00	2.78	52.00
最小				0.04	1.00	0.00	0.22	1.00

これらの結果から、最短で当日中、平均すると約二週間後に最初のスパムを観測した。アカウント毎の一日のスパム数は、最大で16通、平均では約3通であった。

4.2.2 アドレスの重複

スパムを受信したアカウントのハムリストとスパムリストを、表3に示す。

表3 ハムリストとスパムリスト

アカウント名	スパムリスト	ハムリスト
ajifry1	sendonly@kensyo-present.com	prize@1pri.tv m-pre@mbn.nifty.com game@ga-me7.com ad_ke004@goldrush.st mail@cha7.com fwhv3465@mb.infoweb.ne.jp webmaster@nan-paso.com master@otoku-pro.com
ajifry6	info@redmax.jp	mag015@s-si2.2-d.jp info@s-si2.com mag333@s-si2.2-d.jp
ajifry7	mail@hanayori-kenshou.com mail@moneymeizin.com game@ga-me7.com shop-support@kitaguni.tv mailmag@e-money25.com mailmag@kinrinsama.com mailmag@r-jinyo.com info@pw-driver.net info@tougenkyou.org info@offside-magazine.net info@pw-heaven.net info1@e-chance.tv mailmag@e-romoney.com	oubo@sokko.net mag022@s-si2.2-d.jp mag021@s-si2.2-d.jp e527mail@e-camo.net info@s-si2.com mailmag@mane-kun.com
ajifry11	mmg@comjapon.com	game@ga-me7.com mag@luckyhit.com fwhv3465@mb.infoweb.ne.jp reader@mag2.com mailmag@mag2.com info@banzai777.com info@jra.ch kin-un@adn.mail-box.ne.jp

		m-pre@mbn.nifty.com
ajifry13	nightdream@shopping-e1.com frozenfoods@shopping-e1.com	
ajifry15	support@pii.jp	postmail01@venus.livedoor.com info@yumepo.jp magazine@mitsukeyou.com
ajifry18	homelight@shopping-e1.com frozenfoods@shopping-e1.com	
ajifry25	e527mail@e-camo.net mail@eaglebomber.com mag021@s-si2.2-d.jp mailmag@r-jinyo.com mailmag@e-money25.com mailmag@kinrinsama.com mailmag@mane-kun.com mag022@s-si2.2-d.jp info@pw-driver.net info@s-si2.com info@pw-heaven.net info@tougenkyou.org info@offside-magazine.net mailmag@cyoi-money.com melken@melpre.com	fwhv3465@mb.infoweb.ne.jp help@can-na.jp
ajirfy26	info@kmks.jp info@mu-ryo.com info@bd-g.com zen0@zen-pre.com sendonly@kensyo-present.com support@info-buyer.jp info@k-walker.com zen_html@zen-pre.com	info@presentmail.jp game@ga-me7.com support@optile.jp ad_ke002@goldrush.st info@s-si2.com mag016@s-si2.2-d.jp mag015@s-si2.2-d.jp mail@cha7.com admin@cha7.com eril@toproad.jp webmaster@nan-paso.com master@otoku-pro.com mag333@s-si2.2-d.jp

ajifry55	resipi@mail.spiralsys.com present@yasoba.com cocoyo@mail.spiralsys.com patio@elf.coara.or.jp	healthylife171@yahoo.co.jp
ajifry74	sendonly@kensyo-present.com	thanks@poincho.com info@yokubariking.com
ajifry84	info@eigoden.co.jp mailmag@e-moneydoor.com mailmag@e-m-japan.com mailmag@e-moneyhills.com mag2 ID 0000166774 <mailmag@mag2.com> mag2 ID 0000189347 <mailmag@mag2.com> mag2 ID 0000195119 <mailmag@mag2.com> mag2 ID 0000192854 <mailmag@mag2.com> mag2 ID 0000169164 <mailmag@mag2.com> fit-news@lily.appleworld.com	kuji@tadassu.com mag@luckyhit.com fwhv3465@mb.infoweb.ne.jp mag015@s-si2.2-d.jp staff@quickmail.jp info@s-si2.com mag016@s-si2.2-d.jp tousen@777.ag webmaster@nan-paso.com reader@mag2.com mailmag@c-manech.com master@otoku-pro.com mag2 ID 0000170128 <mailmag@mag2.com> help@can-na.jp mag@soho-island.net eril@toproad.jp mm@55p.jp 2step@lucky.nifty.jp mag333@s-si2.2-d.jp

これらのハムリストとスパムリストを比較すると、アドレスが重複しているケースが二つあった。一つはスパムリスト同士でのアドレス重複、もう一つがハムリストとスパムリストの重複である。主な例を表4、表5に示す。

表4 ajifry7 と ajifry25 のスパムリスト同士の重複

ajifry7 のスパムリスト		ajifry25 のスパムリスト	
メールタイトル	スパムアドレス	メールタイトル	スパムアドレス
花より懸賞	mail@hanayori-kenshou.com	懸賞イン	e527mail@e-camo.net
マネー名人の冒険島	mail@moneymeizin.com	イーグルボンバー	mail@eaglebomber.com

GAME 7 メールマガジン	game@ga-me7.com	遊ぶ・当たる・笑う【TEXT版】[号外]	mag021@s-si2.2-d.jp
『北国からの贈り物』	shop-support@kitaguni.tv	ロマネージーニョ	mailmag@r-jinyo.com
マネー25	mailmag@e-money25.com	マネー25	mailmag@e-money25.com
	mailmag@kinrinsama.com		mailmag@kinrinsama.com
ロマネージーニョ	mailmag@r-jinyo.com	桜塚マネー君	mailmag@mane-kun.com
ドライバー	info@pw-driver.net	遊ぶ・当たる・笑う【HTML版】	mag022@s-si2.2-d.jp
桃源郷	info@tougenkyou.org	ドライバー	info@pw-driver.net
オフサイドマガジン	info@offside-magazine.net	遊ぶ・当たる・笑う【TEXT版】[号外]	info@s-si2.com
HEAVEN	info@pw-heaven.net	HEAVEN	info@pw-heaven.net
懸賞マスター	info1@e-chance.tv	桃源郷	info@tougenkyou.org
ロマネーコンティ	mailmag@e-romoney.com	オフサイドマガジン	info@offside-magazine.net
		ちよいマネー親父	mailmag@cyoi-money.com
		メルプレSTYLE	melken@melpre.com

表 5 ajifry7 のハムリストと ajifry25 のスパムリストの重複

ajifry7 のハムリスト		ajifry25 のスパムリスト	
メールタイトル	スパムアドレス	メールタイトル	スパムアドレス
ババ抜きゲームの結果	oubo@sokko.net	懸賞イン	e527mail@e-camo.net
遊ぶ・当たる・笑う【HTML版】	mag022@s-si2.2-d.jp	イーグルボンバー	mail@eaglebomber.com
遊ぶ・当たる・笑う【TEXT版】	mag021@s-si2.2-d.jp	遊ぶ・当たる・笑う【TEXT版】[号外]	mag021@s-si2.2-d.jp
懸賞イン	e527mail@e-camo.net	ロマネージーニョ	mailmag@r-jinyo.com
遊ぶ・当たる・笑う【TEXT版】[号外]	info@s-si2.com	マネー25	mailmag@e-money25.com
桜塚マネー君	mailmag@mane-kun.com		mailmag@kinrinsama.com
なんでもTOKU	fwhv3465@mb.infoweb.ne.	桜塚マネー君	mailmag@mane-kun.com

TOKU (HTML 版)	jp		
全員、先着プレゼントニュース	help@can-na.jp	遊ぶ・当たる・笑う【HTML版】	mag022@s-si2.2-d.jp
		ドライバー	info@pw-driver.net
		遊ぶ・当たる・笑う【TEXT版】 [号外]	info@s-si2.com
		HEAVEN	info@pw-heaven.net
		桃源郷	info@tougenkyou.org
		オフサイドマガジン	info@offside-magazine.net
		ちよいマネー親父	mailmag@cyoi-money.com
		メルプレSTYLE	melken@melpre.com

これらの結果から、重複したスパムの発信元には強い関係性があることが明らかである。スパムリストとハムリストとで重複した場合には、送信元がスパムと意識してメールを送信するいわゆるスパム業者ではなく、登録したサイトによる個人情報流用によりスパムを受信したと考えられる。

4.3 スパム返信

4.3.1 方法

スパムに返信すると、スパム送信元に対し有効なメールアドレスを告知することになる。それにより返信したアドレス宛に対して新たにスパムが送られてくるか検証する。

受信したスパムアドレスに対し、未使用の検証用アドレスから空メールを送信した。

実施日 10月29日

使用したスパムアドレス数 93件

4.3.2 結果

空メール送信に対する反応の割合を図1に示す。スパムアドレス93件のうち、56件が送信エラーとなった。また、34件はエラーにはならなかったがスパム送信元からの反応はなかった。つまり約97%のスパムアドレスには返信することでの変化は見られなかった。

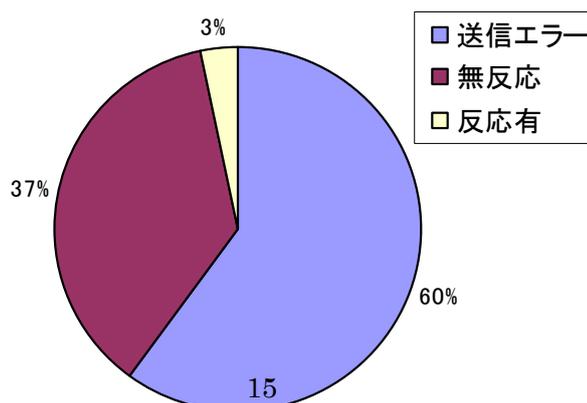


図5 返信反応の割合

返信先からの反応は3件あった。内容の例を図6に示す。これは送られてきたメールが空メールであることへの通知であり、新たにスパムが送られてくるといった当初の予想とは異なった。他の2件も同様であった。

【懸賞Walker】をご利用頂きありがとうございます。
 【懸賞Walker】お客様窓口でございます。
 お客様からメールを頂きましたが、件名・内容が共に空欄でしたので、ご要望が把握できませんでした。ご用件やご質問等ございましたら、お気軽にこちらまでお問い合わせ下さい。
 お手数おかけしますが、よろしく願いいたします。

 【懸賞Walker】: <http://k-walker.com/>
 お問い合わせ窓口: info@k-walker.com

図6 返信反応例

第5章 スパムの内容

第6章 Web 実験

6.1 観測方法

検証用アドレスを記載した実験用ページをウェブ上で公開し、スパムの観測を行った。用意したウェブスペースは、学内のスペース3件、無料レンタルスペース12件、プロバイダが契約会員向けに提供しているスペース8件の計23件である。取得したスペースの一覧を表6に、実験用ページの例を図7に示す。

表6 Web スペース一覧

検証用アドレス	アドレス	種類
ajifry124@cs.dm.u-tokai.ac.jp	http://www.cs.dm.u-tokai.ac.jp/2006/links.html	学内
ajifry125@cs.dm.u-tokai.ac.jp	http://www.cs.dm.u-tokai.ac.jp/~ajifry/	学内
ajifry126@cs.dm.u-tokai.ac.jp	http://pubweb.cc.u-tokai.ac.jp/3adm3123/	学内
ajifry128@cs.dm.u-tokai.ac.jp	http://www.geocities.jp/pregrove/	プロバイダ
ajifry129@cs.dm.u-tokai.ac.jp	http://www.geocities.jp/unojunk/	プロバイダ
ajifry130@cs.dm.u-tokai.ac.jp	http://www.geocities.jp/before_fade_out/	プロバイダ
ajifry131@cs.dm.u-tokai.ac.jp	http://www3.point.ne.jp/~hzpn/index.html	プロバイダ
ajifry132@cs.dm.u-tokai.ac.jp	http://www.geocities.jp/poco_rit_piu_lent/index.html	プロバイダ
ajifry133@cs.dm.u-tokai.ac.jp	http://www15.ocn.ne.jp/~mmr/	プロバイダ
ajifry134@cs.dm.u-tokai.ac.jp	http://www008.upp.so-net.ne.jp/spam/	プロバイダ

ajifry135@cs.dm.u-tokai.ac.jp	http://www.k4.dion.ne.jp/~zico/	プロバイダ
ajifry137@cs.dm.u-tokai.ac.jp	http://ajifry2006.srv7.biz/	無料
ajifry139@cs.dm.u-tokai.ac.jp	http://ajifry.e-city.tv/	無料
ajifry140@cs.dm.u-tokai.ac.jp	http://www.rak3.jp/home/user/ajifry2006/	無料
ajifry142@cs.dm.u-tokai.ac.jp	http://ajifry2006.kt.fc2.com/index.html	無料
ajifry143@cs.dm.u-tokai.ac.jp	http://members.goo.ne.jp/home/ajifry2006	無料
ajifry144@cs.dm.u-tokai.ac.jp	http://www.medianetjapan.com/2/20/internet_computer/ajifry2006/	無料
ajifry145@cs.dm.u-tokai.ac.jp	http://web1.nazca.co.jp/ajifry2006/	無料
ajifry146@cs.dm.u-tokai.ac.jp	http://ajifry2006.web.fc2.com/	無料
ajifry147@cs.dm.u-tokai.ac.jp	http://ajifry2006.hp.infoseek.co.jp/	無料
ajifry148@cs.dm.u-tokai.ac.jp	http://shizuoka.cool.ne.jp/ajifry2006/	無料
ajifry149@cs.dm.u-tokai.ac.jp	http://page.freett.com/ajifry2006/index.htm	無料
ajifry150@cs.dm.u-tokai.ac.jp	http://www.geocities.jp/ajifry2006/	無料



図 7 実験用ページ例

6.2 観測結果

観測期間 6月20日～10月9日

使用した23件の検証用メールアドレスのうち、東海大学の個人用WebサーバPubwebで公開したアドレスがスパムを受信した。

総スパム数は552件、最初のスパムを観測したのは7月6日で、公開日から16日後であった。日付別、曜日別、時間帯別のスパムの頻度をそれぞれ図8、図9、図10に示す。

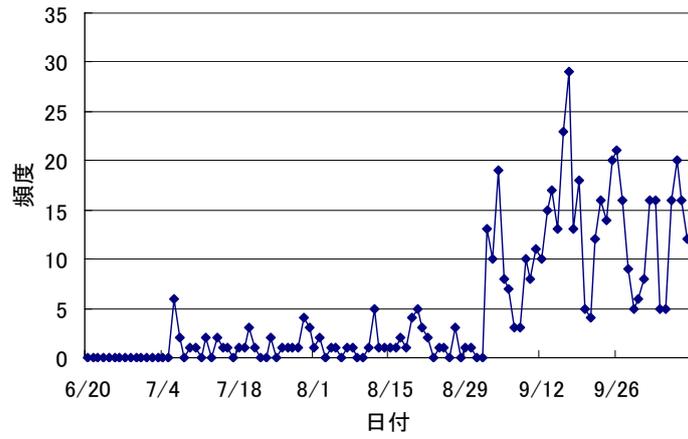


図8 日付別頻度

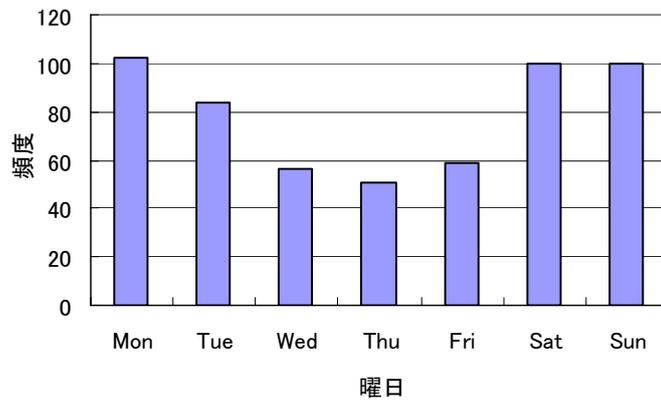


図9 曜日別頻度

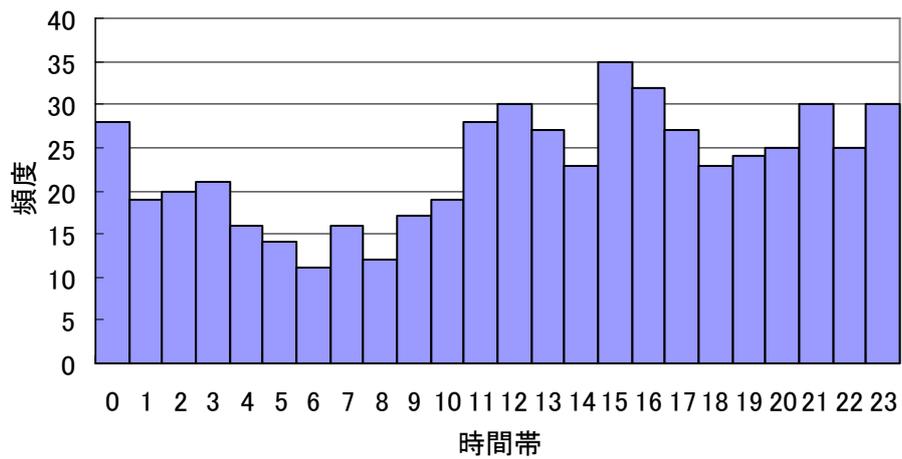


図10 時間帯別頻度

6.3 懸賞との比較

以下、Web で公開した検証用アドレス宛に届くスパムを Web スпам、懸賞に登録した検証用アドレス宛に届くスパムを懸賞スパムと言う。

懸賞スパムが一定のアドレスから定期的に送られてくるスパムであったのに対し、Web スпамは、ほぼ全てのスパムが単発の送信元アドレスであった。また、スパム数の絶対量が違うものの、日付別のスパムの頻度に明らかな違いが見られた。二つを比較したグラフを図 11 に示す。懸賞スパムが登録直後から増え始め、その後 30 から 40 間で推移している。一方 Web スпамは、二週間ほどの無観測期間を経て、二ヶ月間 10 未満で推移し、9 月に入ってから急激に増加している。この Web スпамは一つのメールアカウントが受信したスパム数であるため、懸賞スパムのアカウントごとの一日平均スパム数と比べるとかなりの大量である。

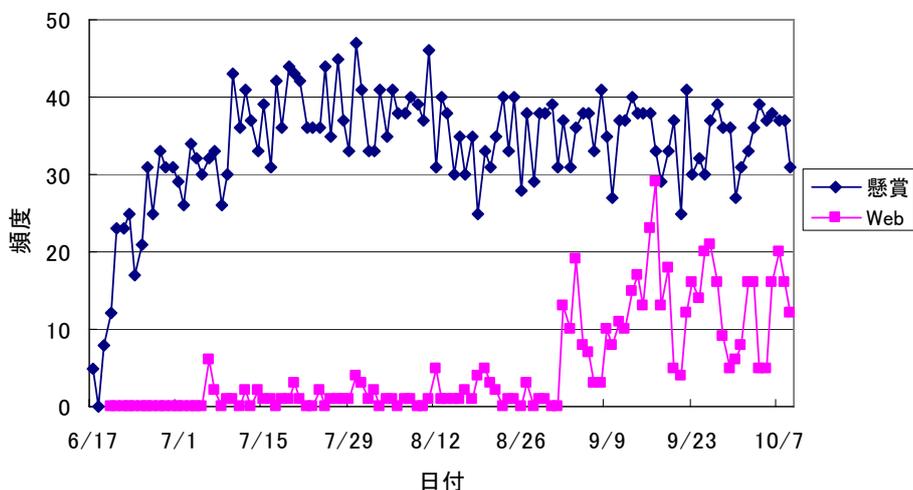


図 11 懸賞スパムと Web スパムの日付別頻度比較

第7章 結論

実験結果から、調査項目に対し、以下が明らかになった。

- 1.登録すると12%の懸賞サイトからスパムが送られる。
- 2.一つのサイトから、一日平均で約3通のスパムが届く。
- 3.登録後スパムが最初に届くまでには、平均で二週間かかる。
- 4.スパムに返信しても、スパムは増えない。

別の懸賞サイトに登録したアカウント同士で受信したスパムの重複があったことから、懸賞サイト同士で登録した情報の流用があると考えられる。また、懸賞スパムと Web スパムとでは、ふるまいに違いがあった。

今後の課題として、Web スパムのサンプル量を増やしより詳細な比較を行うと共に、懸賞と Web 以外のスパム受信の原因を検証し、傾向の比較することが挙げられる。

参考文献

- [1] 景山忠史, spam メールの現状, 情報処理, vol.46, no.7, pp.77-81, 2005

謝辞

本研究を完遂するにあたり、暖かい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申し上げます。

また、多大なご指導を受け賜りました福野直哉氏に、深くお礼申し上げます。

そして、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、謝辞とさせていただきます。