社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38 (47)
2007／7／20

迷惑メールにおける誘導手法に関する一考察

柴田 賢介† 神谷 造† 佐野 和利† 荒金 陽助† 塩野入 理†
金井 敦†

† 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所〒 180-8585 東京都武蔵野市緑町 3-9-11

あらまし 迷惑メールはトラフィックの増大などによる基幹ネットワークへの影響のみならず，フィッシングやワンクリック詐欺等のサイバー犯罪の契機として，利用者に直接の被害を及ぼす可能性がある．利用者が受信する迷惑メールの数が増大するにつれ，迷惑メールの送信者は如何にして利用者に迷惑メールを読ませるか，もしくはメール中のリンクをクリックさせるかといった誘導手法を洗練させている．本研究では，このような迷惑メールの誘導手法の現状を把握することを目的とし，実際の迷惑メールを用いて評価者による調査を実施した．まず，プレ調査として 100 通程度の迷惑メールから誘導手法と考えられるものを抽出し，本調査では約 3,500 通の迷惑メールを対象として誘導手法の分類，抽出を行なった．本論文では，今回実施した調査の内容および得られた知見とその考察について述べる．
キーワード 迷惑メール，サイバー犯罪，ソーシャルエンジニアリング

A Study of Spam Mail Combined with Social Engineering

Kensuke SHIBATA†, Itaru KAMIYA†, Kazutoshi SANO†, Yosuke ARAGANE†, Osamu SHIONOIRI†, and Atsushi KANAI†

† NTT Information Sharing Platform Laboratories, 3-9-11 Midori-Cho Musashino-Shi Tokyo 180-8585 Japan

Abstract The spam mail has become a serious threat as the trigger of cyber crime as well as adverse effect of backbone traffic. As the number of spam mail increases, senders of spam mails perfect their technique of social engineering which directs receivers to web sites. In this paper, we show the result of analysis about 3,500 spam mails to explain the trends of social engineering. We extract some kinds of remarkable techniques and get new insight from these spam mails.
Key words Spam mail, Cyber crime, Social engineering

1. はじめに

近年のインターネットの普及により，様々なオンラインコミュニケーションの手段が提供されている．中でもメールは，瞬時に低コストで相手にメッセージを送れるという利点から，個人間だけでなく，企業内および企業間での主要なコミュニケーション手段として広く利用されている．しかし，メールの特徴の 1 つである，相手のメールアドレスさえ知っていればメールを送信することができるという点を悪用し，不特定多数の相手にメールを送りつけるという行為が蔓延している．

総務省では，一方的に送信される広告宣伝メールを「迷惑メール」と定義し，その対策のあり方について検討がなされている [1]．現在インターネット上でやりとりされるメールのうち，約 70% が迷惑メールであるとの報告もあり [2]，利用者に対して不要なメールが届くといった被害だけでなく，ISP(Internet Service Provider) において運用されているメールサーバの負荷増大といった影響が懸念される．また，年々被害が増加しているサイバー犯罪の中には，フィッシング詐欺やワンクリック詐欺のように，迷惑メールを契機として利用者の金銭的被害に結びつくものも増えてきている．

このような迷惑メールの現状に対し，技術的な側面および法的な側面からの対策がなされている．技術的な側面からの取り組みとしては，迷惑メールの現状を把握するための実験／解析を行なっているものや，迷惑メール対策として一般的に普及しているベイジアンフィルタリングに関する研究等が挙げられる [3]〜[7]．法制度の面では，米国においては 2004 年 1 月に施行された「CAN-SPAM 法」により，メールヘッダ改ざんの禁止，および受け取り拒否の意思を示した受信者に対する送信の禁止 (オプトアウト制度) 等が定められている [8]．日本では，2002 年 7 月に施行された「特定電子メール送信適正化法」および「改正特定商取引法」により，広告宣伝メールの Subject に「未承諾広告※」と記載すること，およびオプトアウト制度

等が定められている [9].

最近の迷惑メールの傾向としては，広告や宣伝によって利用者に商品を購入させたり，利用者をサイバー犯罪の被害に陥れるといった目的を達成するために，メールの文中で巧妙な手口を用い，利用者を誘導しようと試みるものが見られるようになっている．本論文では，実際の迷惑メールを調査対象とし，上記のような巧妙な手口 (これを誘導手法と呼ぶ) がどのように用いられているのかを調べ，迷惑メールの現状を把握することによって今後の迷惑メール対策の一助とする．まず第 2 章では，迷惑メールを契機とするサイバー犯罪であるフィッシング詐欺を例とし，メール中で用いられる誘導手法について概説する．第 3 章では，迷惑メールの誘導手法に関する調査の概要とその結果について述べ，第 4 章で調査結果の考察を行ない，第 5 章をまとめとする．

2. 迷惑メールにおける誘導手法

本章ではまず，迷惑メールを契機とするサイバー犯罪の 1 つであるフィッシング詐欺を例とし，迷惑メールに用いられる誘導手法を概説する．フィッシング詐欺とは，金融機関等を装った詐称メール（フィッシングメール）を用いて受信者を偽装 Web サイト（フィッシングサイト）に誘導し，クレジットカード番号やアカウント名，パスワード，社会保障番号等の個人情報を詐取するものである [10]．フィッシングメールには，利用者をフィッシングサイトへと誘導するための手法が巧みに使われている [11]．以下に，誘導手法の例を示す．

2.1 メールヘッダに用いられる手法

（1） From フィールドを用いた詐称

メールの送信元を示す From フィールドは，メールの送信者が自由に記述することができるフィールドであるため，詐欺師はフィッシング詐欺の対象となる金融機関の名称を本フィールドに記述して送信することが可能である．この手法を用いることにより，金融機関になりすましたメールを容易に送信することが可能となる．

（2） Subject フィールドを用いた詐称

メールの主題を表す Subject フィールドは，From フィールドと同様にメールの送信者が自由に記述することが可能である．フィッシング詐欺師は，詐欺の対象となる金融機関が普段送信しているメールの Subject に酷似したフォーマットの Subject を記述することにより，金融機関になりすましたメールを送信する．

（3） 焦燥感を誘引する表現 (Subject フィールド)

「至急」や「3 日以内に」といった緊急度の高い内容であることを想像させるキーワードを Subject 中に含めることにより，メール本文への関心を高める．

利用者は MUA のメール一覧表示機能でメールの From，Subject フィールドを確認する際に，以上のような手法によって「普段取引している金融機関からメールが届いたので，内容を確認しなければならない」，もしくは「至急内容を確認しなければならない重要なメールだ」といった勘違いをしてしまい，メール本文を閲覧するという行動へと誘導される．

2.2 メール本文に用いられる手法

（1） 本文の見た目を偽装する

メール本文は，当然のことながらメールの送信者が自由に記述することが可能であり，HTML メールを用いることによって画像を表示させることも可能である．詐欺師はフィッシング詐欺の対象となる金融機関のロゴファイルをコピーして流用したり，フォントや文面を酷似させたメールを作成し，金融機関になりすましたメールを送信する．

（2） 実際の遷移先とは異なる URL の表示

HTML メールの場合，メール本文にハイパーリンクを記述する際に A タグを使うことにより，実際に遷移する URL と，利用者がメール本文を閲覧する際に表示される URL を異なるものとすることが可能である．つまり，詐欺の対象となる金融機関の URL を表示 URL とし，実際の遷移先 URL をフィッシングサイトとすることにより，利用者の目を欺くことが可能となる．

（3） 焦燥感を誘引する表現

Subject に用いられる手法と同様に，「3 日以内に Web サイトを訪れ，情報を更新しなければ今後の利用ができなくなります」といった利用者の焦燥感を高める表現を用いることにより，利用者が遷移先の URL を確認したり，メールに付与されている電子署名の有無を確認するといった操作を省略させ，利用者がフィッシング詐欺に遭っていることに気づきにくくさせる．

（4） 同情を誘う表現

大地震が発生した直後に，地震の被害者への募金を行なうように呼びかけ，クレジットカード番号等の個人情報を盗み取ろうとするフィッシング詐欺に多く見られる手法であり，本文中に利用者の同情を誘うような表現を含め，利用者による冷静な判断を不可能とする．

上記のような手法を用いることにより，利用者はメール本文を閲覧した際に，「ハイパーリンクから Web サイトを訪れ，情報を更新しなければ金融機関のサービスが使えなくなってしまう」といったような勘違いから，リンクをクリックし，遷移先の Web サイト (フィッシングサイト) において個人情報を入力／送信してしまい，個人情報が詐欺師の手に渡ってしまうことになる．

2.3 調査における着眼点

以上のように，迷惑メールのごく一部と言えるフィッシングメールに限っても様々な誘導手法が含まれている．フィッシングメールにおいては，メールの From フィールド，Subject フィールドおよび本文等に誘導手法が用いられている．From フィールドの偽装はフィッシングメールに特有の手法と考えられることから，本調査においては迷惑メールの Subject フィールドおよび本文について，下記に挙げる誘導手法に着目した．

- 利用者が MUA においてメールを一覧表示した際に，本文を閲覧するという利用者の行動を誘引することを目的とした，Subject に用いられる誘導手法．
- 本文を閲覧している利用者が，添付ファイルをクリックする，もしくはハイパーリンクをクリックするといった行動を誘引することを目的とした，メール本文中に用いられる誘導手法．

本論文では，上記二点の誘導手法に着目し，最近一年間に届いた迷惑メールに含まれる誘導手法の傾向を分析することを目的として調査を行なった．本調査の結果と考察について，次章以降で述べることとする．

3. 誘導手法の調査

3.1 調査方法

迷惑メールの誘導手法に関する調査を行なうにあたり，まず最初に大まかな傾向の把握を目的として少数の迷惑メールを用いた予備調査を実施した．予備調査においては，100 通程度の迷惑メールを対象とし，著者らによってこれらの迷惑メールの Subject，本文を閲覧し，合議の上で含まれている誘導手法を抽出した．この結果を図 1 に示す．図中，手法名の末尾に (*) が付いていないものが予備調査で得られた手法である．合計 22 個の手法が抽出されており，類似しているものを大項目としてまとめている．

この予備調査で得られた結果をもとに，本調査を実施した．本調査では，18 人の迷惑メール受信者から提供された日本語の迷惑メール約 3,500 通を用意し，評価者 4 名が分担して迷惑メールの Subject および本文を閲覧して，手法を抽出するという方法で実施した．調査の対象となる迷惑メールは，2005 年 12 月から 2007 年 1 月の間に受信者へ届いたものを使用している．

評価者は，予備調査で抽出した 22 個の手法には含まれない新たな手法を発見した場合にはこれを抽出し，既に定義された手法を含むメールである場合には手法のいずれかに分類するという作業を行なった．抽出された誘導手法は，被験者 4 名および著者らによる合議の上，新たな手法として定義するか否かを判定した．また，1 通のメールの中に複数の手法が含まれるケースを想定し，1 通のメールから複数の手法を抽出／分類することを可能とした．メールの本文に用いられている手法を評価する際には，メール送信者の意図がどのようなものであるかを調べるため，メール本文の目的 (送信者は何のために迷惑メールを送信しているか) についても調査した．

3.2 調査結果

まず，今回調査対象となっていた迷惑メールの内容の傾向を示すために，迷惑メール本文の目的に関する結果を図 2 として示す．結果は，出会い系，援助交際等のサイトサービスに関するメールが大部分を占めており，総務省において 2004 年に実施されたサンプル調査と比較して，大きい変化は見られない [1].

次に，手法の抽出および分類に関する結果を図 1 に示す．予備調査では抽出できておらず，本調査において新たに抽出された誘導手法には手法名称の末尾に (*) を付与している．新たに抽出された誘導手法の中で代表的なものとしては，手法 ID(c04) の「知り合いからのメールを装う」が挙げられる．評価者からは調査後に，「知り合いからのメールを装ったものは，つい本文を読んでしまいそうになった」といった感想が挙がるなど，効果的な手法として使われていることが分かる．また，プレ調査では抽出できていなかった大項目として，大項目 (i) の「怒らせる手法」が新たに抽出された．広告宣伝目的であるにもかかわらず，挑発的な文言によって一旦利用者を怒らせ，逆に強い関心を持たせるという効果があるものと思われる．

また，図 3，図 4 として，Subject および本文のそれぞれについて，調査対象メール数に対する各手法が用いられた回数の割合を降順に示す．今回の調査では，1 つの迷惑メールから複

大項目	小項目 (手法名)	ID	表現の例
興味を高める手法	低出費の示唆	a01	「無料」などの記述
	高収入、特典の示唆	a02	「年収1000万円以上」、「高額収入」、「XXポイントプレゼント」、「情報見放題」等得られる物に関しての記述がある
	限定であることの示唆	a03	「当選通知」、「あなただけの特典」、「特別会員」等、メール受信者に限定した権利であることを示唆する記述がある
	目的を示す表現を直接的に示す	a04	提供サービスなど目的に直接つながる表現が存在する
	目的を示す表現を伏せて，もしくはぼやかして示す	a05	「こちらのサイトに行くと○○○が入手可能」、「(何をするのか明らかにせず) サイドビジネスをしませんか」等目的を不明瞭にする記述がある
	内容を想像させる	a06	対象商品のプロフィールの記述や、サイトサービスにおいて出会う相手の視点で紹介する記述がある
	季節感を出す	a07	「クリスマス」、「花火」等の季節イベントを示唆する文言の記述がある
	提示内容をRich化する	a08	絵文字、飾り文字、gifアニメ、Flashアニメなど、単純なテキストベースではない情報の伝達手段がとられている
信頼感を高める手法	第三者視点で商品、リンク先の紹介を行う	b01	既に利用しているユーザによるサイトの信頼性や商品の良さを紹介する記述等がある
	メール停止方法について記す	b02	配信不要はこちら等の記述がある
	説明を詳細に行なうことにより、現実感を高める	b03	商品情報の詳細や、例えば配送方法やキャンセル手段のような情報まで記述している
	信頼を高める文言を記す	b04	「安心」、「初心者向け」などの記述やコピーライト等第三者に認定されているといった記述がある
	サイト運営方針を語る(*)	b05	「秘密厳守」、「会員獲得のためXXXXした」等の記述や例えば、個人情報保護方針の記述がある
勘違いさせる手法	ビジネス用語を使用してビジネスメールのようにみせる	c01	「打ち合わせ」等の記述がある
	差しさわりのない文言を使用して普通のメールのようにみせる	c02	サブジェクトに「ご協力お願いします!」のみ等の記述がある
	他のメールを装う	c03	例えば、寄付のお願い等
	知り合いからのメールを装う(*)	c04	機種変します等、知り合いからのメールと勘違いさせる
親近感を高める手法	地域を示す	d01	「吉祥寺駅」等の記述がある
	文面を礼儀正しいものにする	d02	「突然のメールお許しください」等の記述がある
	会話口調(*)	d03	会話口調で、親近感を高める
手軽さを感じさせる手法	資格についての記述	e01	「年齢制限無し」、「履歴書不要」等の記述がある
	投資についての記述	e02	「初期投資0円」等の記述がある
	時間がかからない、精神的負担が軽い(*)	e03	「簡単登録」等、サイトサービスの利用までの手間がかからないことをアピールしたり、また「お試し」「遊び感覚で」等精神的負担が軽減する表現がある
	個人情報の漏洩リスクが少ない(*)	e04	「フリーアドレスでもOK」、等の記述がある
焦らせる手法	期限の提示	f01	「今月中に○○しないと権利がなくなります」等の記述
	先行者利益を提示	f02	「先着××名様まで」等の記述や、ゴト情報で「ホールでの該当機種が入れ替えられ始めてます」等の記述がある
	価値観を押し付ける(*)	f03	価値観を押し付け登録などの動作を促す手法、「登録しないあなたがおかしい」等の記述がある
怖がらせる手法	攻撃の示唆	g01	「XXしないと法的手段に訴えます」等の記述がある
同情させる手法	惨状の示唆	h01	「地震被害」、「心臓手術」、「難病」等の記述がある
怒らせる手法	挑発(*)	i01	挑発的な記述で目立たせ、逆説的な効果をうたう手法。例えば「まだ独身を貫けるつもりですか」の記述で、いい相手が見つかるよとの示唆
その他	その他	z00	その他

図 1 プレ調査および本調査によって得られた誘導手法

Fig. 1 Spam mail techniques extracted by our examination.

目的	割合
サイトサービス (出会い系, 援助交際等)	91.5%
売買 (アダルトグッズ, 薬物, PCソフト, ブランド品等)	3.2%
求人	1.8%
金融サービス	0.2%
解読不能 (文字化け, 文字がないメール等)	0.1%
その他	3.1%

図 2 調査対象迷惑メールにおける本文の目的

Fig. 2 Purposes of the body of surveyed spam mail.

手法ID(本文)	件数	割合
a01-低出費の示唆	1911	49.5%
b02-メール停止方法について記す	1717	44.4%
a06-内容を想像させる	1073	27.8%
a04-目的を示す表現を直接的に示す	871	22.5%
a02-高収入, 特典の示唆	798	20.7%
b04-信頼を高める文言を記す	608	15.7%
b01-第三者視点で商品, リンク先の紹介を行う	584	15.1%
b03-説明を詳細に行い現実感を高める	412	10.7%
a03-限定であることの示唆	348	9.0%
a08-表示内容をリッチ化	322	8.3%
b05-サイト運営方針を語る	262	6.8%
a05-目的を示す表現を伏せる	261	6.8%
e03-時間がかからない, 精神的負担が軽い	256	6.6%
f01-期限の提示	223	5.8%
d02-文面を礼儀正しいものに	211	5.5%
e04-個人情報の漏洩リスクが少ない	208	5.4%
z00-その他	100	2.6%
d01-地域を示す	87	2.3%
c04-知り合いからのメールを装う	82	2.1%
a07-季節感を出す	78	2.0%
f02-先行者利益の提示	63	1.6%
d03-会話口調	61	1.6%
h01-惨状の示唆	36	0.9%
e01-資格についての記述	13	0.3%
c03-他のメールを装う	6	0.2%
f03-価値観を押し付ける	5	0.1%
i01-挑発	5	0.1%
c02-差しさわりのない文言	4	0.1%
e02-投資についての記述	4	0.1%
c01-ビジネス用語の使用	1	0.0%
g01-攻撃の示唆	1	0.0%

図 3 本文に多く用いられる手法

Fig. 3 Ranking of techniques order of preference.(body)

手法ID(本文)	件数	割合
a06-内容を想像させる	838	25.2%
z00-その他	598	18.0%
a04-目的を示す表現を直接的に示す	515	15.5%
c04-知り合いからのメールを装う	386	11.6%
c03-他のメールを装う	237	7.1%
a01-低出費の示唆	195	5.9%
a02-高収入, 特典の示唆	195	5.9%
c02-差しさわりのない文言	184	5.5%
a05-目的を示す表現を伏せる	183	5.5%
a03-限定であることの示唆	121	3.6%
d02-文面を礼儀正しいものに	96	2.9%
d03-会話口調	66	2.0%
a07-季節感を出す	48	1.4%
b04-信頼を高める文言を記す	45	1.4%
f01-期限の提示	43	1.3%
c01-ビジネス用語の使用	41	1.2%
a08-表示内容をリッチ化	34	1.0%
b02-メール停止方法について記す	29	0.9%
e03-時間がかからない, 精神的負担が軽い	26	0.8%
b01-第三者視点で商品, リンク先の紹介を行う	14	0.4%
b03-説明を詳細に行い現実感を高める	10	0.3%
h01-惨状の示唆	9	0.3%
e04-個人情報の漏洩リスクが少ない	6	0.2%
b05-サイト運営方針を語る	5	0.2%
d01-地域を示す	4	0.1%
e01-資格についての記述	4	0.1%
f03-価値観を押し付ける	2	0.1%
g01-攻撃の示唆	1	0.0%
i01-挑発	1	0.0%
e02-投資についての記述		0.0%
f02-先行者利益の提示		0.0%

図 4 Subject に多く用いられる手法

Fig. 4 Ranking of techniques order of preference.(subject)

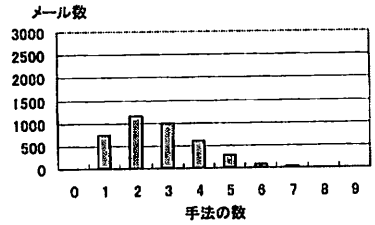

図 5 1 通の迷惑メール (本文) に対して用いられていた手法の数

Fig. 5 The number of techniques used in a spam mail.(body)

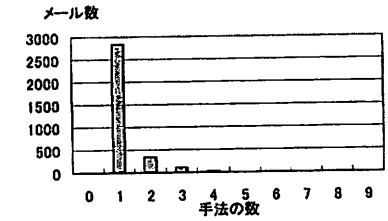

図 6 1 通の迷惑メール (Subject) に対して用いられていた手法の数

Fig. 6 The number of techniques used in a spam mail.(subject)

数の手法を選択することを許可しており，迷惑メールの数に対する手法の回数の割合をとったため，割合の合計値は 100% を超えている．本文に関しては，手法 ID(a01) の「低出費の示唆」，および手法 ID(b02)「メールの停止方法について記す」に分類されるものが多くの割合を占めており，直接的な表現が依然として多く用いられる傾向にある．逆に，Subject に関しては，手法 ID(a06)「内容を想像させる」もしくは手法 ID(z00)「その他」に多く分類されており，ぼやかした表現によって曖昧にすることにより，利用者を本文へと誘導しようという送信者の意図が窺える．

4. 考　　察

4.1 誘導手法の連携に関する考察

3.2 節において，個々の誘導手法が用いられる頻度についての調査結果を示した．本節では，複数の誘導手法を連携して用いることにより，さらに効果を高める手法となり得るのではないかとの仮説の下で，誘導手法の連携に関する考察を行なった．

まず，本文と Subject について，メール 1 通に対してどの程度の数の手法が同時に用いられているのかを調べた．これを図 5，図 6 として示す．本文については用いられた手法の数の平均値が 2.75，標準偏差が 1.36 となり，Subject については平均値が 1.19，標準偏差が 0.52 となった．Subject は文字数が少ないことから，1 つの誘導手法を用いて尋かれるケースが多いと

手法ID(本文)	手法ID(本文)	件数	割合
a01-低出費の示唆	b02-メール停止方法について記す	897	23.2%
a01-低出費の示唆	a06-内容を想像させる	523	13.5%
a04-目的を示す表現を直接的に示す	b02-メール停止方法について記す	487	12.6%
a01-低出費の示唆	a02-高収入，特典の示唆	431	11.2%
a01-低出費の示唆	a04-目的を示す表現を直接的に示す	430	11.1%
a02-高収入，特典の示唆	b02-メール停止方法について記す	427	11.1%
a01-低出費の示唆	b04-信頼を高める文言を記す	419	10.8%
a06-内容を想像させる	b02-メール停止方法について記す	397	10.3%
b02-メール停止方法について記す	b04-信頼を高める文言を記す	248	6.4%
a04-目的を示す表現を直接的に示す	a06-内容を想像させる	226	5.8%
b02-メール停止方法について記す	b03-説明を詳細に行い現実感を高める	206	5.3%
a01-低出費の示唆	a08-表示内容をリッチ化	204	5.3%
a01-低出費の示唆	a03-限定であることの示唆	194	5.0%
a03-限定であることの示唆	b02-メール停止方法について記す	194	5.0%
a01-低出費の示唆	b01-第三者視点で商品，リンク先の紹介を行う	191	4.9%
b01-第三者視点で商品，リンク先の紹介を行う	b02-メール停止方法について記す	187	4.8%
a01-低出費の示唆	b05-サイト運営方針を語る	182	4.7%
a01-低出費の示唆	b03-説明を詳細に行い現実感を高める	173	4.5%
a04-目的を示す表現を直接的に示す	b03-説明を詳細に行い現実感を高める	173	4.5%
a01-低出費の示唆	e03-時間がかからない，精神的負担が軽い	163	4.2%

図 7　本文に多く用いられている連携手法

Fig. 7　Ranking of techniques in combination order of preference.(body)

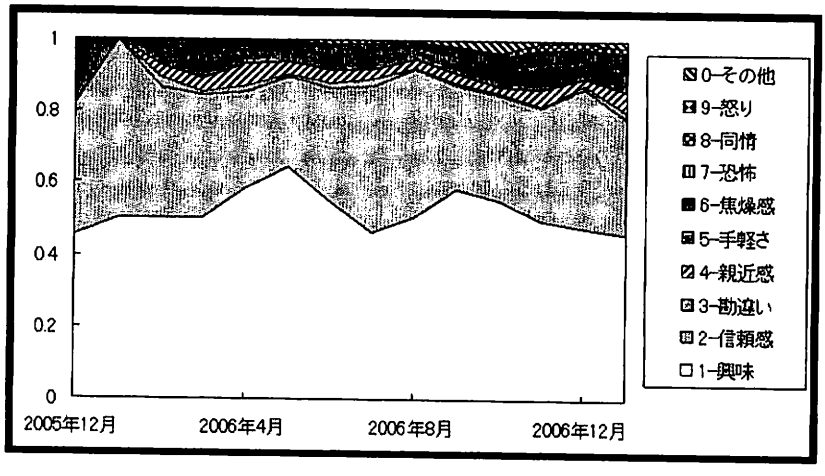

図 8　誘導手法の推移 (本文)

Fig. 8　Time-shift of technique.(body)

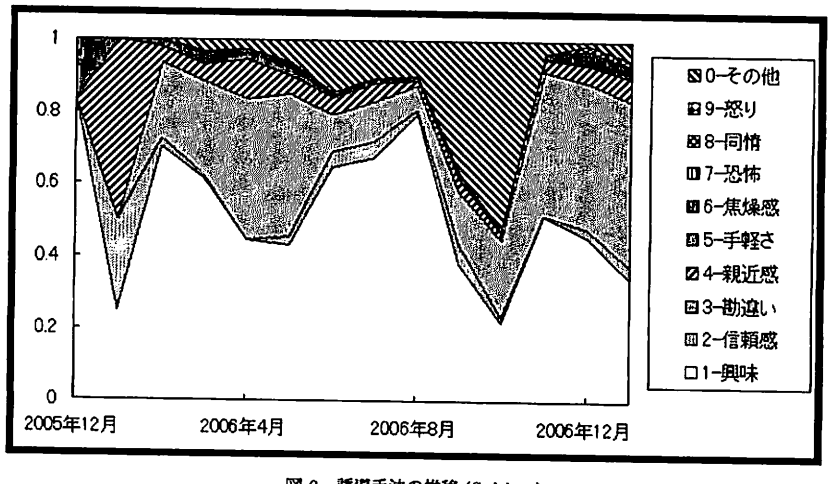

図 9　誘導手法の推移 (Subject)

Fig. 9　Time-shift of technique.(subject)

考えられる．

そこで，複数の誘導手法を用いるケースが多いとの結果を得たメール本文について，どの誘導手法を組み合わせて用いられる傾向があるかを調べた．この結果を図7として示す．図7においても，図3，図4と同様，迷惑メールの数に対する手法の回数の割合をとっている．また，1通のメールにおいて3個以上の手法が連携して使用された場合には，個々の手法の組み合わせを重複してカウントしている(例：手法a01，a02，b01が1通のメールで観測された場合，a01-a02，a02-b01，a01-b01の3種類の手法連携が行なわれたとしてカウントされる)．複数の手法が使われる場合についても，図3における単独の場合と同様に，手法ID(a01)の「低出費の示唆」，および手法ID(b02)「メールの停止方法について記す」が用いられているケースが多いことが分かる．これらの手法に含まれているキーワードを重点的に用いてフィルタリングを行なうことにより，現在の大部分の日本語迷惑メールを判別できる可能性があると言える．

4.2 誘導手法の推移に関する考察

3.2節において，各誘導手法が用いられる割合についての調査結果を示した．本節では，誘導手法が用いられる割合の時間的な変化を観測した場合に，何らかの傾向が見られるのではないかとの仮説の下に考察を行なった．

図8，図9として，横軸にメールの受信月，縦軸にはその月に観測された誘導手法の総数に対する個々の手法の割合をとったグラフを示す．このグラフにおいては，メールの総数に対する手法の割合ではなく，手法の総数に対する個々の手法の割合を縦軸としているため，合計は100%となっている．グラフでは，誘導手法の大項目毎の比率を示している．手法の比率は3.2節で述べたとおり，本文の誘導手法は大項目(a)「興味を高める手法」，大項目(b)「信頼感を高める手法」の順に多く観測されているのに対し，Subjectの誘導手法は大項目(b)「信頼感を高める手法」の代わりに大項目(c)「勘違いさせる手法」が多く観測された．グラフ上での大きな推移は観測されなかったが，少数ながら，大項目(h)「同悄させる手法」，大項目(i)「怒らせる手法」等の手法については，2006年5月以降に観測され始めた新しい手法であることが分かった．

5. まとめと今後の課題

本論文では，被害が増大している迷惑メールの現状把握を目的とし，メールのSubjectおよび本文に含まれる誘導手法に着目した調査を行なった．調査では，評価者を用いて迷惑メールに用いられている誘導手法の分類および抽出を行ない，著者らによるプレ調査では抽出できなかった誘導手法を抽出した．また，誘導手法の連携および推移に着目した考察においては，特にメール本文において用いられている手法に偏りが見られること，また，昨年あたりから用いられるようになってきている手法が見られる等の知見を得ることができた．今後は，今回の調査で得られている結果を基に，さらに分析を深めていくことにより，迷惑メール対策およびサイバー犯罪対策の検討を進めていく予定である．

文　献

[1] 総務省 迷惑メールへの対応の在り方に関する研究会，“迷惑メールへの対応の在り方に関する研究会 最終報告書”，http://www.soumu.go.jp/s-news/2005/pdf/050722_2_02_00.pdf，Jul. 2005.

[2] Symantec 社，“The State of Spam-A Monthly Report-March 2007”，http://www.symantec.com/avcenter/reference/Symantec_Spam_Report_-_March_2007.pdf，Mar. 2007.

[3] Tanzila Ahmed and Charles Oppenheim，“Experiments to identify the causes of spam”，Aslib Proceedings New Information Perspectives，Vol.58，No.3，pp.156-178，Mar. 2006.

[4] 長谷川明生，“Spamメールの解析”，情報処理学会研究報告，Vol.2004，No.77，pp.37-42，Jul. 2004.

[5] 市川貴久，奥田隆史，井手口哲夫，Xuejun Tian，“ケーススタディによるspamメールの到着間隔特性の解析”，電子情報通信学会研究報告，Vol.106，No.524，pp.59-64，Jan. 2007.

[6] 王哦，堀良彰，櫻井幸一，“中国語迷惑メールにおけるベイジアンフィルタの適用と評価”，情報処理学会研究報告，Vol.2006，No.43，pp45-50，May. 2006.

[7] 大橋泰樹，松浦幹太，“ベイジアンフィルタと社会ネットワーク手法を統合した迷惑メールフィルタリングとその最適統合法”，情報処理学会論文誌，Vol.47，No.8，pp2548-2555，Aug. 2006.

[8] Galen A. Grimes，“Compliance With the CAN-SPAM Act of 2003”，Communications of the ACM，Vol.50，No.2，pp.56-62，Feb. 2007.

[9] 岡村久道，“サイバースペース法律相談所 第3回 迷惑メールの法的規制”，情報通信ジャーナル，Vol.22，No.7，pp24-25，Jul. 2004.

[10] Anti-Phishing Working Group，“APWG Phishing Trends Activity Report for April，2007”，http://www.antiphishing.org/reports/apwg_report_april_2007.pdf，Apr. 2007.

[11] 柴田賢介，荒金陽助，塩野入理，金井敦，“電子メールの解析によるフィッシングおよびファーミング対策方式の提案”，マルチメディア，分散，協調とモバイル(DICOMO2006)シンポジウム，pp.477-480，Jul. 2006.