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

2007－ＥＩＰ－36（３）
2007／5／25

spamメールとサイレントメールを考慮した電子メール利用リスクに関する一考察

奥田 隆史

愛知県立大学情報科学部 〒480-1198 愛知郡長久手町大字熊張字茨ヶ廻間1522-3
E-mail: okuda@ist.aichi-pu.ac.jp

あらまし 迷惑メールやspamメールに対処するため，メール利用者は，アンチスパム・ソフトウェアを利用し，spamメールを自動的に検出・分類している．しかしながら，アンチスパム・ソフトウェアの検出・分類の設定条件によっては，spamメールでないメールまでがspamメールと誤認されてしまう．また，連続的な検出・分類処理により，配信途中で消失してしまうサイレントメールの存在も明らかになっている．本研究では，これまで筆者らが調査したspamメールの到着特性をもとにして，送信した電子メールが受信者に物理的に届かないというリスクあるいは物理的には届いているのであるが目にしてもらえないというリスクについて検討する．迷惑メールやspamメールが増加していることも一因で，メールがサイレントメールとして消失してしまったり，spamメールでないメールまでがspamメールと判断されたりすることがある．本研究では，送信した電子メールが受信者に物理的に届かない現象，あるいは物理的には届いているのであるが目にしてもらえないという現象に着目し，電子メールを利用することにより生ずるリスクについて検討する．

キーワード spamメール，迷惑メール，サイレントメール，リスク，リスクマネジメント

A study on risk for using e-mail system bothered by spam messages and silent mails

Takashi OKUDA

Faculty of Information Science and Technology, Aichi Prefectural University
Kumabari, Nagakute-cho, Aichi, 480-1198 Japan
E-mail: okuda@ist.aichi-pu.ac.jp

Abstract Spam is an unwanted electronic mail often advertisements and commercial messages. The continuing increase in spam has resulted in rapid growth in the use of e-mail client software with spam filtering function. This type e-mail client software usually separates spam from genuine email messages and keeps spam mails out of inbox folder. However, the software often missed genuine messages to spam folder and made silent mails. In this paper, the author shows a model of e-mail arriving process and evaluates risk of using of e-mail system.

Key words spam email message, silent mail, risk, risk management

1. はじめに

我が国におけるインターネット利用人口は，平成16年度末の統計によると約7948万人，人口普及率は62.3%となり，インターネットは生活に欠かせない存在となっている．中でも電子メールは，必要不可欠なコミュニケーションツールとして利用されている[1]．

一方，メール受信者に同意を得ずに大量に送信されるspamメールが増加し，その被害も増加している(注1)(注2)．文献[3]で

(注1)：「SPAM」および「スパム」は米国Hormel Foods社の登録商標であることもあり，本研究では文献[2]にしたがい「spamメール」と表記する．

(注2)：spamメールは別名「ジャンクメール (junk mail)」，「バルクメール (bulk mail)」とも呼ばれる．米国では，UCE (Unsolicited Commercial Email，勝手に送りつけてくる宣伝電子メール) や UBE (Unsolicited Bulk Email，勝手に送りつけてくる大量電子メール) と呼ぶこともある．spamメールは，明確な定義はなされていないが，送信者の目的で分類すると，出会い系サイト広告宣伝メール，架空請求詐欺メール，架空請求詐欺メール，フィッシング目的メールなどに分類される．

は，インターネット上で送受信される電子メールに占めるspamメールの割合は，2005年末の段階で，80〜90%に達していると報告している．

spamによる被害は，「コンピュータウィルスに感染する」，「ワンクリック詐欺の被害にあう」，「フィッシング詐欺サイトに誘導される」などがある[4], [5].

これらの被害に加えて，spamメールの増大により電子メールシステムに与える負荷が，企業の電子メールシステムの運用管理における新たな課題となっている[5]．spamメール対策へのコスト増加や生産性低下などビジネス活動へ深刻な影響を与えるという2次的な被害の問題である[4], [5]．コスト増加には，spam対策用システムの導入・運用コストの増加に加えて，インターネット上のメールのα%がspamとすると，ネットワークリソース，サーバリソースなどの情報資産のα%を無駄に消費するというコストも発生する[6].

生産性低下の例として，文献[5]の調査によれば，エンドユーザーの日常業務にspamメールの及ぼす影響として，

- 仕事のメールが探しにくくなる(36.7%).
- 文面・内容を見ていやな気分になる(31.7%).
- 業務中断で集中力や生産性が低下する(30.6%).
- 仕事のメールを削除してしまう(23.2%).
- ウィルスやスパイウェアが侵入する(17.3%).
- フィッシングによる詐欺被害に遭う(5.8%).
- とくに影響はない(31.7%).

がある．この調査によれば，エンドユーザーに届いたspamメールの処理に一日当たり平均4.4分を費やすことになり，労働日数を年間220日とすると，年間14.6時間，2営業日を損失していることになる．

筆者の職場は大学ということもあり，エンドユーザーである筆者には，職場の電子メールサーバーシステムを経由した全メールが届く(注3)．そのため，日々の教育研究活動において深刻な影響があるため，spamメールに関して，エンドユーザとして調査研究を実施した[7]〜[10].

その結果，改めてspamメールの増加に驚くとともに，電子メールを利用することには，様々なリスクがともなうということを再認識した．本研究では電子メールを利用するリスクについて考察することを目的とし，最初に第2.節で，以後の議論のためにエンドユーザーに届くメールの視点により，メールを分類する．次に，第3.節で文献[7]〜[10]で得られた知見について整理する．第4.節では，リスクアセスメントプロセスで用いられる階層ホログラフィックモデリング法[11]を利用した分析図を提案する．最後に，第5.節でまとめる．

2. spamメールの処理の流れ

前節で述べたspamメールに対して，社会的側面や運用・技術的側面から対処がなされている．社会的側面からの対処として政策・行政サイドによる法律の整備が進められている[12], [13]. 2002年7月には「特定電子メールの送信の適正化等に関する法律（特電法）」が施行され，2005年11月には，特電法が改正され，罰則がより厳しいものとなった．しかし，特電法改正後も，spam送信者は日本国外のサーバを利用して送信することができるため，一向にspamが減少する気配がないのが現状である．

一方，運用・技術的側面でのspamメール対策として，spamメールを排除しながらメール受信を行うための，メール・フィルタリング・ソフトウェア(一次フィルタ)が，組織のメールサーバーに利用されていることが多い[14]〜[16]（図1）(注4)．

エンドユーザー側では，上記の一次フィルタリング結果と各自のメーラーのフィルタリング機能（指定した送信元やメール本文中のキーワードに基づいたフィルタリング）を利用し，メールのダウンロード時に，spamメールと正常メール(spamメール以外)とに自動的に分類・保存している．しかし，「正常メールをspamメールと判断（以後，誤認スパム）」したり，「spamメールを正常メールと判断（以後，誤認メール）」したりすることもある[20]．すなわち，ユーザーの視点で判断するとメッセージフォルダ内のメッセージは，図1に示すように，正常メール(**normal**)と**spam**メールだけでなく，

(a) 誤認メール(**spam, but normal**)：正常メールと判断されたspamメール．

(b) 誤認スパム(**normal, but spam**)：spamメールと判断された正常メール．ユーザーはスパムフォルダ内のメールを一括で削除する際には注意を要する．

が混在することになる．最近では，IPアドレスを利用したスパムフィルタリング処理が原因となって，送信されるメールの0.71〜1.02%(注5)が，相手のメールサーバにさえ届かないで，消失・沈黙メール（**Silent email loss**）となってしまうという問題も顕在化してきている[27]．この消失・沈黙メールに加えて，コンテンツによるフィルタリングの誤処理により消失するメールの割合は1.79〜3.36%(6.5〜13.1日に相当)となる．

3. 受信メールの基礎データ

3.1 spamメールの到着特性の調査結果

ここでは，我々の研究グループが調査した2006年2月10日から5月31日（便宜上，以下，春期とする）[8], [9]ならびに2006年9月1日から12月20日（秋期とする）におけるspamメールの到着特性について整理する[10]．なお，春期には2,671通，秋期には6,262通のspamメールが到着している．

（1） 到着spamメール数：図2に両期のspamメール数の変化状況を示す．これよりspamメール数が増加傾向であることが確認できる．

(注3)：本学の電子メールシステムではspamと判断されるメールに，件名の先頭に[spam]と加え，エンドユーザーに注意を喚起している．

(注4)：一次フィルタの技術方式には，「ベイジアンフィルタ」，「ヒューリスティックフィルタ」，「パターンマッチフィルタ」，「協調型フィルタ」等がある．実際の運用では，受信したメールはSpamAssassin[17]やbsfilter[18]などのフィルタリングソフトウェアを組み合わせて，spamメールを排除している[19].

(注5)：0.71〜1.02%という数字は，1日30通のメールを1年間送信するとして，2.6〜3.7日分のメールが消失することに相当する．

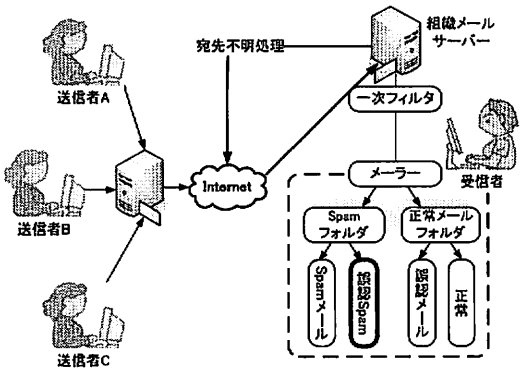

図 1　メールの一般的な処理の流れ

Fig. 1　Typical example of mail filtering and classification

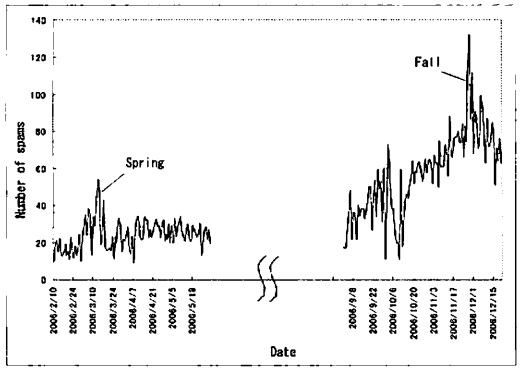

図 2　春・秋期間における spam メール到着数

Fig. 2　Number of total spam messages per day for the spring and fall period

（2）　到着時間帯特性: 春期については午前 9〜10 時に到着する spam メールが最も多く 174 通 (6.5%)，午後 5〜6 時が最も少なく 61 通 (2.3%) であった．春期の到着パターンでは，spam メールは，一般的な企業の始業時間帯をねらって送信され，終業時間帯には送信しないのではないかと推測することができた．秋期については，秋期に比較し時間帯別の到着 spam メール数の差はみられなくなった．

（3）　曜日別到着数の特性:春期は金曜日から月曜日にかけて増加し，火曜日から木曜日にかけて減少している．spam メールは，曜日別では，週末をねらって送信されているということが推測できる．一方，秋期は火曜日が 978 通 (15.9%) と最多で，土曜日が 790 通 (12.9%) と最少となった．秋期は火曜をピークとして週末にかけて到着数が減っている．

（4）　到着間隔特性：秋期のデータでは到着間隔が 1 時間以内のものが 5,705 通と 91.1% を占めている．98.6% が 2 時間以内に到着していることがわかった．なお，春期では 2 時間以内が 86.6%，3 時間以内で 94.0% であった．これから，秋期は集中的に到着していることがわかる．1 時間以内に到着した spam メールを 5 分間隔の時間帯で比較すると，秋期は 5 分以内が 26.0%，10 分以内が 42.5% となり，春期はそれぞれ 15.1%，27.4% というデータが得られた（図 3 参照）．

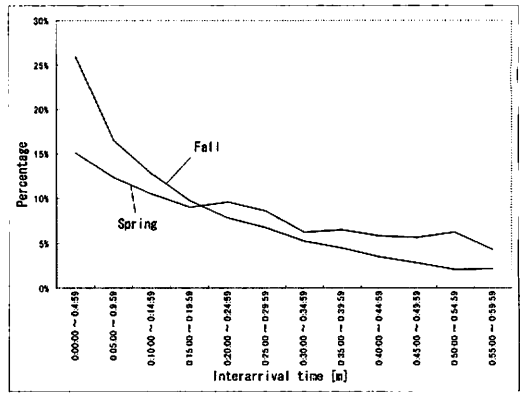

図 3　春・秋期における到着間隔別 spam メール到着数曲線

Fig. 3　Number of total spam messages for inter arrival time for the fall

（5）　最適削除間隔例-春期：時間間隔 $[0, t)$ $(0 \leqq t \leqq 24)$ に到着する spam メール数に着目すると，春期については到着分布を平均到着率 $\lambda = 1.004$ のポアソン分布 [21], [22] で近似することができた．ここで期間中の spam メールの到着を，最大到着率 $\lambda_{max} = 1.567$[数/時] のポアソン分布として近似できるとすると，12.6 時間おきに spam メール削除処理を行えば，90% の確率で上限保存数を 25 以下にすることができる．なお，95% とするには，11.6 時間おきに削除する必要がある．ここで，25 の意味はメーラーの画面で一覧できるメールの数を意味し，この数があまり多くなると誤認スパムが埋もれてしまう．

（6）　最適削除間隔例-秋期：これまでの分析結果により春期データのようにポアソン分布として近似できなかった．そこで，秋期期間中で到着する spam メールが 132 通と最も多かった 11 月 28 日のデータを利用すると，例えば，0 時から 11 時までの間の 12 時間，削除処理をしないとすれば 78 通，12 時から 24 時までだと 54 通の spam メールが保存されることになる．3 時間おきで 29 通以下，2 時間おきで 18 通以下にすることができる．一方，春期では 12.6 時間おきに spam メール削除処理を行えば，90% の確率で上限保存数を 25 以下にすることができた．

3.2　ある教員の電子メール受信事例

spam メールの増大が，生産性低下，spam メール対策へのコスト増加などビジネス活動へ深刻な影響を与えている [4], [23] ということを，具体的な事例で紹介する．なお，対象とする期間は 2006 年 11 月 20 日〜12 月 20 日とし，その期間に受信したメール 3,709 通および発信した 206 通のデータを利用する．なお，受信メールの内訳は spam メール 2,503 通 (67.5%)，正常メール 1,143 通 (30.9%)，誤認メール 63 通 (1.6%) である．

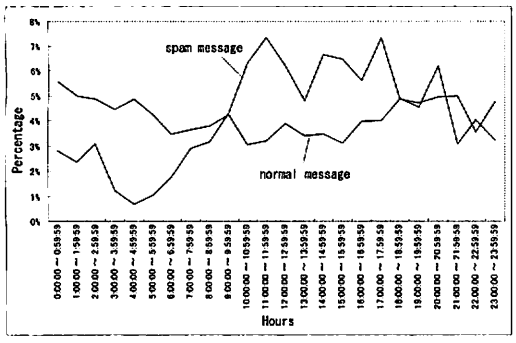

図 4 spam メール・正常メール受信時間帯別曲線 (Nov.11 – Dec.20)
Fig. 4 Hourly total number of received messages (Nov.11 – Dec.20)

なお，誤認スパムは 1 通であった．これらのメールの送受信時刻に着目した特性は以下のとおりである．

(1) 受信メールの到着間隔特性：1 時間以内に到着する spam メールが 2,361 通 (94.3%)，正常メールが 934 通 (81.7%) となった．spam メールの 99%(2,494 通)，正常メールの 93.2% (1,065 通) が 2 時間以内に到着した．

(2) 受信メールの時間帯別特性：図 4 は当該期間に受信される spam メールおよび正常メールの到着時間帯別の変動を示す (到着した各メール総数を 100% とする)．spam メールは，春期の傾向と同様，一般的な企業の始業時間帯をねらって送信され，終業時間帯には送信しないのではないかと推測することができる．一方，正常メールは 9 時台ならびに 19 時台 (米国の始業時間) に増加する傾向がみられる．

(3) メールサーバーに届くメールの総数の概算：組織のメールサーバーには，同じような傾向でランダム到着で各アカウントに対して spam メールが送られてくる．仮に組織のメールアカウント数を N 個，各メールアカウントに送られてくる spam メールの到着率を λ_{spam}，正常メール到着率を λ_{mail} とすると，ポアソン分布の重畳性から，メールサーバに到着するメールの到着率 λ_{total} は

$$\lambda_{total} = N(\lambda_{spam} + \lambda_{mail}) + M\lambda^{+}_{spam} \qquad (1)$$

となる．ただし，$M\lambda^{+}_{spam}$ は spam 送信者が，Botnet [28] などを用いて適当なアカウント相手に送ってくる spam の総数であり，膨大な到着率となることが予想される．今回の調査結果において，受信メールにスパムが含まれていないとすると，メールサーバーに与える負荷は約 70% 以上も減ることになる．

(4) 誤認スパムによる被害：当初懸念していた誤認スパムは，フィルタリングの精度も向上したこともあり，期間中は 1 通だけであった．しかしながら，「送信者が再度送ったとしても，同じようにフィルタリングされ誤認スパムとなる可能性が高い」，「ひょっとしたら紛れていないだろうかという気持ちは残るので精神衛生上良くない」という問題は残る．また，誤認メールは spam メールでありながら正常メールのフォルダにダウンロードされるので，取り扱いには注意を要する．

(5) スパムフィルタリング精度の向上：spam 送信者は巧妙にメールを送信し続けるであろう．しかし，spam メールが多様化すればするほど，学習データが増えることになり，ファイルタリングの精度が向上し，誤認スパムが減っていくことになる．特に，誤認メールは削除するだけでなく，spam メールとしての特徴を登録することで，フィルタリング精度向上のための有効な学習データとして利用できる．

4. リスク理論とリスクマネジメント

リスク定義の着眼点や表現は分野により異なることもあり，リスクの定義はあらゆる分野を通して一定とは限らない．そのため，リスクには概念的にいくつもの定義がなされている [24]〜[26], [29]．従来から用いられている表現手法として，

(1) 好ましくない結果の発生可能性とその大きさの測定

(2) 事態の確からしさと，その結果の組み合わせ

(3) 事象の発生確率と事象の組み合わせ

(4) 望ましくない事象による望ましくない結果の期待値

$$Risk = Magnitude\ of\ hazard \times Probability \qquad (2)$$

で表現する．

がある．この定義の問題点は，リスクを期待損害 (平均値) として考えるために，意思決定に一元的な明確な基準を提供する一方で，個々の事象とリスクとの関連を無視することになる．

最近では，リスクは定義は以下の 3 つの要素：

(1) 事象やシナリオの集合 $s = \{s_i\}$

(2) 事象やシナリオの発生可能性 p_i

(3) 事象やシナリオに関連する結果の大きさ d_i

で定義する [26], [30]．なお，複雑なシステムにおける事象やシナリオを系統的に見つけ出す方法として，階層ホログラフィックモデリング法 (Hierarchical holographic modeling method, HHM 法) が提案されており，情報システムのセキュリティ上のリスクマネジメントレベルの向上に有効とされている [11]．

さて，前節で紹介したように，spam メールの数は一向に減らない．spam メールが減らない背景には，spam メールを送信する人や組織 (以下，spammer) が，情報を一度に大量配信することが少ないリスクで実行できるからである [31]．一方で，spam メールが増加することにより，利用者側には，「仕事のメー

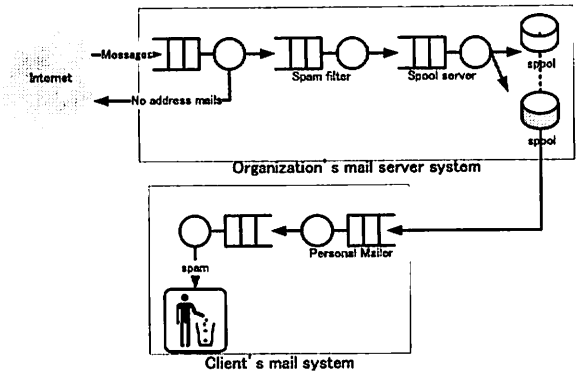

図 5　Spam メール処理の待ち行列網モデル

Fig. 5　Queuing model for spam mail processing system

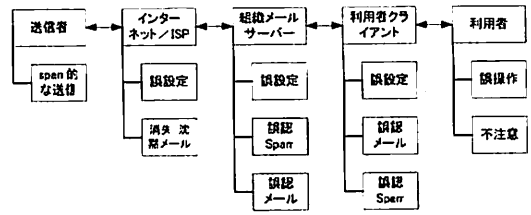

図 6　メールの到達に関する階層ホログラフィックモデル

Fig. 6　Hierarchical holographic model for mail system

ルが探しにくくなる」,「文面・内容を見ていやな気分になる」,「業務中断で集中力や生産性が低下する」,「仕事のメールを削除してしまう」,「ウィルスやスパイウェアが侵入する」,「フィッシングによる詐欺被害に遭う」という事象が生じる確率が増加することになる.

したがって,コミュニケーションの円滑化には,ユーザーは,スパムフォルダに保存されたメッセージが,spam メールなのか誤認スパムなのかを確認後,spam メールを削除する必要がある.しかしながら,spam メール削除処理を頻繁に行うことは,ユーザーにとっては負担となる.削除処理間隔が空きすぎると,誤認スパムがスパムフォルダに埋もれてしまう確率が高くなる.すなわち,文献[32]で定義した「電子メールメッセージの到達確率」が低下することになる.

また,正常メールを spam メールと判断して生ずる誤認スパムに一度でも遭遇すると,エンドユーザーは spam メールか正常メールかを確認しながら業務するという非生産的な作業が増え,生産性が低下することにつながる.頻繁に誤認スパムが発生することも生産性が低下するが,まれにしか誤認スパムが発生しない場合も,Spam フォルダのチェックを怠ることにもなり,誤認スパムに気が付かないという事象が発生する.図 1 およびメールのパケットを呼としてとらえた待ち行列網モデル[33],[34]を図 5 に対して,階層ホログラフィックモデリング法を適用すると,spam メールのリスクアセスメントモデルは図 6 のようになる.なお,リスクアセスメントモデルの構築手法には,文献[35],[36]で提案されている Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM})) approach 手法,文献[39]で提案されている自己組織化マップにより個々のリスクに関連する記述子を積み上げる手法がある.

5. ま と め

本研究では,これまで筆者らが調査した spam メールの到着特性をもとにして,送信した電子メールが受信者に物理的に届かないというリスク（サイレントメール）あるいは物理的には届いているのであるが目にしてもらえない（誤認メール）というリスクについて検討した.その結果,フィルタ処理の精度が向上し,最近は誤認メールの数は減少傾向であるため,誤認メールにより生じるであろう連絡不足によるビジネスチャンスの損失というリスクは減少する傾向であった.しかしながら,spam の増加は止まることがないため,重要なメールが誤認メールとして spam フォルダに紛れ込んでいないかという心配から生ずる生産性の低下につながっていることも確認できた.

そもそも,インターネットでの電子メールサービスは大学を中心とする社会において,研究に関する情報の交換を目的として,非商用サービスとして利用がスタートした.そのため,普及の初期段階では,メールの消失などに関して,利用者は寛容であったと思われる.すなわち,各利用者がゼロリスク(注6)を求めず,リスクを受け入れて利用してきた.むしろ,普及の初期段階では,各ユーザーがリスクに対して何らかの処理を暗黙に行ってきたため,リスクや問題を表出することさえも困難であったと考えられる.最近になっても,電子メールシステムの誤設定がされにくいことが露呈した[37](注7).

さて,現在の所,電子メールの利用において,spam メールが無くなる可能性は現状では低い.すなわち,電子メールをコミュニケーションの道具としては有用であるが,spam の増加とともに,ある程度のリスクを受け入れて利用する[26]道具となっている.フィルタの性能が向上しても,誤認メールや誤認スパムが完全に無くなる可能性は低いため,絶えずリスクにさらされていることになる.サービス提供者は spam メールをフィルタリングすることにより,利用者もやはりメーラーを利用して spam メールをフィルタリングすることにより,それぞれがリスクをマネジメントしながら,電子メールを利用する必要がある.まさに,電子メールの利用においても,地震や台風などの自然災害が原因となるリスクマネジメント問題を検討する時のように,自然災害そのものをいかに防ぐのではなく,自

(注6)：食品の安全性や化学物質の健康影響性に関して,リスク管理の責任を負う行政や産業界は「公衆が過度にゼロリスクを求めている」と感じ,リスクにさらされることに懸念を抱く市民や消費者は「産業界は利潤追求を重要視し,行政は産業界よりの政策を進め,過剰なリスクを我々に押しつけている」と感じている[24],[25].前者は「ゼロリスクを追求する公衆像」として認識されている.

(注7)：会員数約 28 万人の受信メール約 450 万通の一般メール（2006 年 12 月～2007 年 2 月分）が,サーバの設定によって誤って迷惑メールと判断され,消去されるという事態が生じたにもかかわらず,この誤処理が判明したのは,2007 年 3 月 1 日から 4 月 5 日までに,たまたま合計 19 件の問い合わせがあったためだという.被害の割には,問い合わせが少ないこともあり,誤処理が表出しなかった.

然災害そのものをいかに防ぐかではなく，自然災害がもたらすリスクをいかに管理するかを考える方が重要である[29]．自然災害が要因となるリスクに対処するためには，(1) 自然災害が社会インフラの安全性，機能性，整合性に与える影響を分析する，(2) 社会インフラの破壊や損害が人々の生命財産，社会経済，自然環境に及ぼす影響について検討し，災害対策を講じるべきであるとされている．

高等学校においても「教科情報」では，情報モラル教育の一環として迷惑メールについて取り上げられている．そこでは，迷惑メールが問題であるとは書かれており，テストをすれば誰もがいけないと回答することができる．その際，簡単な迷惑メールによる実体験がともなうことにより，生徒の理解が深まることが指摘されている[38]．そこで，今後は，インターネットや電子メールを利用することには一次的なリスクだけでなく二次的なリスクが伴うということを，分野横断的に数値化し[40]，数値を利用して迷惑メールや spam メールへの対処法について啓蒙する方法について考えていく予定である．

謝　辞

本研究を進めるにあたり spam メールについて意見交換をしていただいた愛知県立大学情報科学部井手口哲夫教授，成瀬正教授，田学軍助教に深く感謝する．本研究の一部は平成 19 年度（財）電気通信普及財団研究助成ならびに平成 19 年度愛知県立大学学長特別教員研究費の補助を受けて行われた．ここに記して謝意を示す．

文　献

[1] 総務省．情報通信白書平成 17 年度版，http://www.johotsusintokei.soumu.go.jp/whitepaper/, 2006.
[2] 山井成良，桝田秀夫，“spam メールの現状と対策の動向”，情報処理，Vol. 46, No. 7, pp. 739-740, 2005.
[3] 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, 2005.
[4] Yee-Lin Lai S.Y.T. Lee I.P.L. Png Il-Horn Hann, Kai-Lung Hui, “Who gets spammed?”, *Communications of the ACM*, Vol. 49, No. 10, pp. 83-87, 2006.
[5] 沢村徹，小山安博他，“迷惑メールに勝つ”，*Windows Mode*, No. Nov., pp. 29-59, 2006.
[6] 高倉弘喜，“ネットワーク観測から掌握するサイバー攻撃と spam メールの状況”，サイエンティフィック・システム研究会システム技術分科会 2006 年度第 2 回会合資料集, 2007.
[7] 奥田隆史，市川貴久，井手口哲夫，田学軍，“スパムメール到着特性に着目した最適削除処理について”，経営情報学会 2006 年秋季全国研究発表大会，pp.400-403, 2006.
[8] 市川貴久，奥田隆史，井手口哲夫，田学軍，“フィルタリング処理された spam メールの最適削除間隔について”，電子情報通信学会 2006 年ソサエティ大会，No. A-9-2, 2006.
[9] 市川貴久，奥田隆史，井手口哲夫，田学軍，“フィルタリング処理された spam メールの到着特性分析結果に基づく最適削除処理について”，情報学ワークショップ 2006, pp.103-106, 2006.
[10] 市川貴久，奥田隆史，井手口哲夫，田学軍，“ケーススタディによる spam メールの到着間隔特性の解析”，電子情報通信学会情報ネットワーク研究会，Vol. 106, No. 524, pp. 59-64, 2007.
[11] 下平利和，Hua Xu，“階層ホログラフィックモデリング法の適用によるリスクアセスメントプロセス改善の試み”，統計数理研究所 統計数理，Vol. 54, No. 1, pp. 105-122, 2006.
[12] 岡村久道，“社会的側面から見た spam メール対策：法制面での問題と対策”，情報処理，Vol. 46, No. 7, pp. 787-788, 2005.
[13] 畠山忠史，“社会的側面から見た spam メール対策：政策・行政面での対策”，情報処理，Vol. 46, No. 7, pp. 789-791, 2005.
[14] 編集部，“スパムメール完ぺき撃退術”，月刊アスキー，Vol. 30, No. 3, pp. 82-96, 2006.
[15] 編集部，“電子メールセキュリティ最前線”，*Network Magazine*, No. May, pp. 29-43, 2006.
[16] 安藤一憲，“技術的側面から見た spam メール対策:フィルタリング”，情報処理，Vol. 46, No. 7, pp. 758-761, 2005.
[17] The Apache Spam Assassin Project, http://spamassassin.apache.org/.
[18] bsfilter-bayesian spam filter, http://bsfilter.org/.
[19] 米田聡，“快適メール環境を構築しよう”，日経 Linux, 11 月号，pp.83-89, 2006.
[20] 須藤慎一，“メールの返事が来ない！重要なのに迷惑メールと誤認されゴミ箱に直行”，http://www.nikkeibp.co.jp/style/biz/skillup/spam/060731-8th/, 2006.
[21] Kulkarni Vidyadhar G, *Modeling and Analysis of Stochastic Systems*. Chapman and Hall Texts in Statistical Science Series. Chapman and Hall, New York, 1996.
[22] 牧本直樹，ビジネスへの確率モデルアプローチ，朝倉書店, 2006.
[23] サイエンティフィック・システム研究会，“セキュリティ-対策ソフトでどこまで守れるか-”，サイエンティフィック・システム研究会システム技術分科会, 2007.
[24] 中谷内一也，ゼロリスク評価の心理学，ナカニシヤ出版, 2004.
[25] 中谷内一也，リスクのモノサシ—安全・安心生活はありうるか，日本放送出版協会, 2006.
[26] 瀬尾佳美，リスク理論入門—どれだけ安全なら充分なのか，中央経済社, 2005.
[27] Venkata N. Padmanabhan Sharad Agarwal, Dilip Joseph, “Addressing Email Loss with SureMail: Measurement, Design, and Evaluation”，*Technical Report. Microsoft Research*, 2006.
[28] 関山智也，義徳小林，正和高橋，佐々木良一，“Botnet からのスパムメールに対する応答遅延方式の提案”，情報処理学会研究報告コンピュータセキュリティ，Vol. 81, pp. 191-197, 2006.
[29] 徐馬華，大澤幸生，チャンスとリスクのマネジメント，朝倉書店, 2006.
[30] S. Kaplan and B. J. Garrick, “On the quantitative definition of risk”，*Risk Analysis*, Vol. 1, No. 1, pp. 11-27, 1981.
[31] 伊藤信，堀政浩，“基礎から学ぶメールセキュリティ-スパムメールや情報漏洩，コンプライアンスまで”，*Network Magazine*, No. May, pp. 50-63, 2007.
[32] 石井直人，奥田隆史，“離散時間マルコフ連鎖を用いた電子メールメッセージの到達確率予測”，情報学ワークショップ 2005, pp. pp.115-118, 2005.
[33] 紀一誠，待ち行列ネットワーク，朝倉書店, 2002.
[34] Stefan Greiner, Hermann De Meer, Kishor S. Trivedi, Gunter Bolch, *Queueing Networks and Markov Chains : Modeling and Performance Evaluation With Computer Science Applications*, Wiley-Interscience, 1998.
[35] Cert. Octave method. *http://www.cert.org/octave/methods.html*.
[36] Audrey J. Dorofee Christopher J. Alberts. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Publishing, 2002.
[37] “450 万通メール削除-迷惑対策，誤って適用”，朝日新聞朝刊, 2007 年 4 月 7 日.
[38] 加納寛子，実践 情報モラル教育—ユビキタス社会へのアプローチ，北大路書房, 2005.
[39] 中谷洋明，堀井秀之，村山明生，山口健太郎，“リスク特性とリスクガバナンス構造の類型化及び関係分析の試み”，社会技術研究論文集，Vol. 3, No. Nov, pp. 31-46, 2005.
[40] 山口健太郎，白戸智，堀井秀之，“社会問題解決策の立案に資する分野横断的な知識活用手法の検討”，社会技術研究論文集，Vol. 3, No. Nov, pp. 186-195, 2005.