RCSSディスカッションペーパーシリーズ
第33号　2005年11月

Discussion Paper Series
No.33　November, 2005

ISSN 1347-636X

spamメールの経済的損失の試算

榎原 博之・鵜飼 康東・竹村 敏彦

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka 564-8680 Japan
URL : http://www.rcss.kansai-u.ac.jp/
http://www.socionetwork.jp/
e-mail : rcss@jm.kansai-u.ac.jp
tel. 06-6368-1177
fax. 06-6330-3304

spamメールの経済的損失の試算

榎原 博之・鵜飼 康東・竹村 敏彦

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka 564-8680 Japan
URL : http://www.rcss.kansai-u.ac.jp/
http://www.socionetwork.jp/
e-mail : rcss@jm.kansai-u.ac.jp
tel. 06-6368-1177
fax. 06-6330-3304

spamメールの経済的損失の試算

榎原博之* 鵜飼康東† 竹村敏彦‡

2005年11月

概 要

本稿では、近年社会問題化しているspamメール（迷惑メール）がもたらす経済的損失の試算をおこなっている。そのなかで、spamメール問題の本質は、spamメール業界が巨大なマーケットを形成しており、またspamメール送信業者が十分な利益を上げることができるしくみになっていることを示している。さらに、spamメールによる経済的損失は労働力の損失だけでなく、ICT資産、特にメールサーバの追加的な投資が問題であることを明らかにしている。したがって、何らかの政策的処置もしくは経済・社会的制度設計が必要である。

KEYWORD: spamメール, 経済的損失, ICT投資, 制度設計

*関西大学工学部・助教授, 関西大学ソシオネットワーク戦略研究センター・研究員
†関西大学総合情報学部・教授, 関西大学ソシオネットワーク戦略研究センター長
‡関西大学ソシオネットワーク戦略研究センター・ポストドクトラルフェロー

Estimated Economic Losses by spam Mails

HIROYUKI EBARA
Associate Professor, Faculty of Engineering, Kansai University
E-mail: ebara@eip.kansai-u.ac.jp
YASUHARU UKAI
Professor, Faculty of Informatics, Kansai University
E-mail: ukai@rcss.kansai-u.ac.jp
TOSHIHIKO TAKEMURA
Postdoctral Fellow, Research Center of Socionetwork Strategies, Kansai University
E-mail: takemura@rcss.kansai-u.ac.jp

Abstract

Recently, spam mails (unsolicited commercial e-mails) are recognized as social problem, and the mails cause major economic losses. In this paper the economic losses caused by spam mails are estimated. At first, authors show that the essence of spam mail problem is in the mechanism that spammers gain enough profits. Next, it is clear that the spam mails cause not only loss of labor, but also overinvesting in ICT asset (information and communication technology asset). Therefore, economic and social mechanism for spam mails need to be designed.

KEYWORD: spam Mail, Economic Loss, ICT Investment, System Design

1 序論

本稿では、インターネットユーザだけでなく、インターネット・サービス・プロバイダ（以下、ISP とする）にも多大な悪影響を与えている、不特定多数のユーザに一方的に送りつけられるメール、いわゆる spam メールについて考察する。ISP にとって、spam メールの増大は ISP が持つサーバやネットワークなどの ICT（情報通信技術）資産をむだに消費するだけでなく、ヘルプデスクへの問い合わせの増加や、spam メール対策サービスの充実が必要となり、セキュリティ対策と同様、大きな負担となっている（Nelson(2003)）。

電子メールは、インターネットが始まった当初から利用されているアプリケーションのひとつで、現在でも WWW と並んで最も頻繁に利用されているアプリケーションである。多くのユーザが毎日のように利用している電子メールであるが、spam メールの山に悩まされているのも事実である[1)]。シマンテック社の調査によれば、2004 年 7 月の時点で実にメール総数の 65%以上が spam メールだといわれている[2)]。

電子メールは、良識ある研究者間での利用に限られていたインターネット黎明期に設計されたものであるため、簡単に送信者を偽称できるなどのセキュリティ上の問題点を多くかかえている。しかし、spam メール送信者に最大の問題がある。インターネットが普及し、不正アクセスやウィルスなどのセキュリティ問題が重要になってきた当初は、不正アクセス者やウィルス作成者の多くは、愉快犯であって利益を目的とすることはなかった。ところが、21 世紀に入り、急激に利益を追求した者によるセキュリティ犯罪が増加している。例えば、フィッシング詐欺[3)] やキーロガー[4)] を埋め込んだスパイウェア[5)] は、インターネットの落とし穴を巧妙に利用した犯罪で、ユーザの近親者を騙る振り込め詐欺（通称・オレオレ詐欺）と同様、利益を追求した犯罪である。spam メールに関しては、犯罪であるか犯罪でないかは別として、spam メールを送ることを専門とする業者がおり、十分な利益を上げていることは事実である。

現在では、フィルタリングソフトなどを使って spam メールを効率よく除去しているユーザも多く見受けられるが、この対策だけで十分であろうか。spam メールはそれを受け取るユーザにとっての問題だけでなく、その電子メールを運んできたネットワークやサーバにも追加的投資を強いているのである。インターネットは多数のネットワークやサーバを経由してデータを運ぶしくみとなっている。電子メール全体の半分以上が spam メールであるという現状を考えると、もし spam メールをすべてなくすことができれば、インターネット上の電子メールシステム（メールサーバやネットワーク）を半分以下の性能にすることができることになる。

本稿では、spam メールを定義したのち、spam メールを送る専門業者が限界費用が限りなくゼロに近い状態で正の収益を上げている現状を明らかにする。さらに、spam メールによる経済的損失をユーザ側からだけではなく、サーバやネットワークへの投資も含めて算出する。さいごに、spam メールを送信させない、あるいは、配送させないための制度設計を紹介する。

---

1) 世界で最も多くの spam メールを受け取っている人物は、マイクロソフト社会長の Bill Gates 氏であろう。彼は 1 日に 400 万通の電子メールを受け取るという。もちろん、ほとんどが spam メールであり、フィルタリングや spam メール防止技術、そして人海戦術により、実際に Bill Gates 氏が目を通す電子メールは 1 日に 2、3 通らしい。

2) http://www.symantec.com/region/jp/enterprise/articles/20040810.html

3) フィッシング（phishing）詐欺とは、金融機関やクレジットカード会社などからの正規のメールやウェブサイトを装い、暗証番号やクレジットカード番号などを搾取する詐欺のことである。

4) キーロガー（key logger）とは、キーボードからの入力を監視して記録する常駐型ソフトウェアのことである。

5) スパイウェア（spyware）とは、ユーザに気づかれずに常駐して、ユーザの操作履歴や個人情報などを収集する、あるいは、プロセッサの空き時間を借用して計算するソフトウェアの総称である。

2 spamメールとは

ここで、本稿で扱うspamメールを定義しておく。一言でspamメールといっても定義はまちまちであり、個人的解釈も異なっている。日本語でも、spamメールと同義語として迷惑メールがある。英語では、spamメールのことをUCE（Unsolicited Commercial Email）やUBE（Unsolicited Bulk Email）と呼ぶことがある。本稿では、「受信者の同意なしに、無差別かつ大量に一括して送信される、主に宣伝目的の電子メール」と定義する。迷惑メールは、一般に「受信者の同意なしに、無差別かつ大量に一括して送信される、受信者が不快に思う電子メール」と定義されることが多く、コンピュータウイルスによって無差別に送信されるウイルスメールを含む場合が多い。本稿で扱うspamメールにはウイルスメールを含まない。また、携帯電話の迷惑メールも対象外とする。

「SPAM」[6]とは、もともとアメリカHormel Foods社のハムに似た味付け豚肉缶詰の商品名のことである[7]。本書では、「SPAM」がHormel Foods社の登録商標であることから、山井・桝田（2005）と同様、小文字で「spam」と表記することにする。

3 spamメール問題の本質

前節に述べたように、多くのspamメールは専門の業者によって送信されている[8]。従来から存在するダイレクトメールと同様である。ダイレクトメールと大きく違う点は、送信費用がほとんどかからない点である。Judge(2003)によると、アメリカにおいてダイレクトメールを送るのに1通あたりおよそ1.21ドルかかるのに対して、spamメールでは1通あたりおよそ0.0005ドルである。実に、2400倍以上の費用格差がある。この差がspamメール問題の本質となっている。このため、メール送信に課金しようという考え方も起こってきた[9]。Judge(2003)によると、ダイレクトメールの場合、1通あたり1ドル以上かかるため、2%程度の受信者からの問い合わせが期待されるようであるが、spamメールの場合は0.001%で十分収益が上がる。すなわち、10万人にひとりの受信者が商品を購入してくれれば、十分採算がとれることになる。Rockbridge Associates(2005)の調査では、この1年間でspamメールから商品を購入した人は、全体の4%にのぼったと報告されている。これを日本に当てはめて簡単な試算をおこなってみよう。総務省（2005）のデータより2004年度末のインターネットユーザ数は7948万人で、そのうちspamメール受信者は86.6%である。7948万人 $\times$ 0.866 $\times$ 0.04 $\simeq$ 275万人 となる。巨大な潜在的マーケットが存在している。したがって、spamメール送信が産業として十分成り立つことがわかる。

spamメール送信業者は、メールアドレスとメール送信サーバの固定費用があれば、あとはほとんど自動的に限界費用ゼロでspamメールを送ることができる。したがって、メールを送れば送るほど平均費用は低下して、大きな収益を生む可能性が高くなる。つぎに、メールアドレスの取得方法とメール送信サーバの確保方法について述べる。

- メールアドレスの取得法

---

[6] 「スパム」も「SPAM」もアメリカ Hormel Foods 社の登録商標である。

[7] イギリス BBC で放映されたコメディー番組「Monty Python's Flying Circus」で、客がメニューを選んでいると、周りの客や店員が「SPAM、SPAM、SPAM！」と連呼しだし、SPAM を注文せざるを得なくなる、というコントがあった。このコントで執拗に連呼される「SPAM」と、ほしくもないのに大量に送りつけられてくる広告メールが重なって「spam」と呼ぶようになった。

[8] spam メール送信業者のことをスパマー（spamer）と呼ぶ。

[9] 山井・桝田（2005）の「2.5 送信者認証・課金」中村素典と Rockbridge Associates(2005) 参照。

最もよく使われているメールアドレス取得法は、メールアドレス収集ロボットを使ってインターネット上に存在するメールアドレスを収集する方法である[10]。ホームページに問い合わせ先のメールアドレスを載せるのは一般的であるが、これが悪用されている。このため、最近では、spam メール対策として、問い合わせ用のメールアドレスを公開せず、問い合わせ用フォームに記述する形式に変更しているホームページも多い。

つぎに考えられるのは、ランダムにあるいは辞書を使って架空のメールアドレスを作り出し、spam メールを送信する方法である。エラーメールが返信されなければ、有効なメールアドレスとして今後も利用するということになる。この方法は携帯メールでよく利用されているが、インターネットメールでは Hotmail や Yahoo！メールのような有名なメールアドレスを除き、さほど利用されていないようである。

さいごに、他人のメールアドレスを手っ取り早く購入する方法がある。上記の方法で収集したメールアドレスは、インターネット上で 10 メールアドレスあたり数円程度で公然と売買されている。

- メール送信サーバの確保法

  もちろん、正規にメールサーバをたて spam メールを送信している業者もいるが、いつも同じメールサーバから spam メールを送信していると、spam メール送信サーバとしてブラックリストに載り、そこからの電子メールを受け付けなくしているメールサーバが増えてきたため、送信メールサーバを頻繁に変更する spam 業者が多くなってきている。

  電子メールの送信は一般的に、SMTP（Simple Mail Transfer Protocol）[11] が使われている。従来このプロトコルには認証機能がなく、誰でも自由にメール送信できるようになっている。しかし、spam メールの送信に利用されることが多くなってきたため、現在ではほとんどのメールサーバで認証による規制をし、spam メールの送信に利用されないように設定している。

  それでは、spam メール送信業者はどのようにしてメールサーバを確保しているのであろうか。多くの spam メール送信業者は、不正アクセスにより取得したゾンビ PC[12] やボットネット[13] を使用している。spam メール全体の 40%以上はゾンビ PC からの送信であるといわれている（山井・桝田（2005）の「1.2 spam メールの現状」景山忠史）。ゾンビ PC やボットネットはセキュリティ上重大な社会問題であり、日本でも 1 万台以上のゾンビ PC があるといわれている。また、ゾンビ PC やボットネットのレンタルがおこなわれており、手軽に借りることができるようになっている。さらに、このことが不正アクセス者やウイルス作成者の手軽な収益源にもなっている。

このように、21 世紀に入り、メールアドレスの収集業者、メールサーバのレンタル業者、spam メールの送信業者と分業が進み、spam メールが十分利益を生む土壌ができあがってしまっている。

---

10) ここで、ロボットと呼んでいるのは、産業用ロボットや人型ロボットのことではなく、ロボット型サーチエンジンのことである。ロボット型サーチエンジンとは、インターネット（ウェブページ）上を自動的に巡回して、情報やデータを収集するプログラムのことである。

11) SMTP（Simple Mail Transfer Protocol）とは、インターネット上でメールサーバへ電子メールを送信するためのプロトコルである。

12) ゾンビ PC とは、不正アクセスにより遠隔操作ソフトが仕掛けられ、ユーザがそのことに気づかないまま、他のコンピュータやネットワークへの不正侵入のための踏み台や spam メールの送信に利用されているパソコンのことである。

13) ボットネットとは、悪質なプログラムの一種である「ボット」を埋め込んで、攻撃者が自由に操作できるようにしたパソコンで構成されるネットワークのことである。spam メールの送信や、フィッシング詐欺のための偽ウェブサイトの構築、DDoS（分散サービス妨害）攻撃などに使われている。1 万台を超えるゾンビ PC で構成されたボットネットが確認されている。

このシステムを崩すためには、インターネットユーザがspamメールから商品やサービスを購入したり、spamメールに対応したりしないようにする技術と制度の設計が必要である。とりわけユーザのコンピュータがゾンビPCにならないようにセキュリティ対策をしっかりと施すことがISP業界の重要な課題である。

4 spamメールによる経済的損失

本節では、spamメールによる経済的損失を考察する。従来からspamメールによる経済的損失について分析した報告書がいくつか存在する。例えば、2002年の調査結果がNelson(2003)に紹介されている。これによると、当時はまだspamメールの量は電子メール全体の30%程度であったにもかかわらず、すでにアメリカで年間89億ドル、ヨーロッパで年間25億ドルの経済損失があったと試算している。また、Nucleus Research(2004)の2004年5月の調査によると、米国企業がspamメールで被る生産フロンティア低下の損失は従業員ひとりあたり年間1934ドルで、2003年7月の調査に比べて倍増している。ひとりの従業員が1年間で受け取るspamメールの量は平均7500通（前年3500通）で、年間3.1%（同1.4%）の労働生産性低下をもたらしている。最近の報告では、アメリカ メリーランド大学が2005年2月3日に発表した調査報告書が有名である（Rockbridge Associates(2005)）。これによると、アメリカのインターネットユーザがspamメール削除に費やしている時間は、アメリカ全体で週に2290万時間で、給料で換算すると年間215億8000万ドルの経済的損失となる。

本節では、Rockbridge Associates(2005)の調査結果を中心に紹介し、それを日本の場合に当てはめ、spamメールによる経済的損失を試算する。さらに、上記の報告書では議論されていなかったサーバやネットワークへの余剰な投資による経済的損失を算出する。

4.1 アメリカの労働における経済的損失：Rockbridge試算

ここでは、Rockbridge Associates(2005)の調査報告を紹介する。Rockbridge Associates(2005)は、アメリカ メリーランド大学のビジネススクール Robert H. Smithが Rockbridge Associates, Inc. に調査を依頼してまとめたもので、spamメールの調査だけではなく、M-commerce（移動体通信を利用した電子商取引）、E-government（コンピュータやインターネットを利用し、処理を電子化した行政機構）、E-services（コンピュータやインターネットを利用したサービス）、E-health（コンピュータやインターネットを利用した健康管理）、Consumer technology readiness（消費者の最新技術に対する準備状態）も含まれている。調査は、ランダムに選ばれた18歳以上のアメリカ国民1000人を対象に、2004年11月に電話インタビューによりおこなわれた。このうち、インターネットユーザの有効回答数は418人である。1999年から今まで5回おこなわれているが、2003年はおこなわれていない。

調査結果によると、サンプル全体の78%がspamメールを受け取っており、1日に10通以上受け取っている人が36%もいる。平均は1日あたり18.5通である。アメリカ全体では、総人口の77%がインターネットを利用しているので、インターネットユーザ数は全体で、2億2000万人 $\times$ 0.77 = 1億6940万人となる。アメリカ全体の1年間のspamメールの総数は、実に18.5通 $\times$ 1億6940万人 $\times$ 365日 $\simeq$ 1兆1440億通 に及ぶ。さらに、spamメールを受け取っている人のうち、14%は中身を開いて読んでいる。また、この1年間にspamメールから商品やサービスを購入した人は4%おり、これをアメリカ全体で考えると、インターネットユーザの70%がspamメールを受け取るとして、実に1億6940万人 $\times$ 0.7 $\times$ 0.04 $\simeq$ 474万人が購入していることになる。

spam メールの処理に関しては個人差が非常に大きいが、68%のサンプルが少なくとも週に 1 回はメールボックスから spam メールを消去している。27%のサンプルはこの処理を毎日おこなっている。一方、10%のサンプルは spam メールの消去をまったくおこなわず、13%のサンプルは 1ヶ月に 1 回以下しかおこなわない。平均すると、1 週間に 2.9 日 spam メールの処理をおこなっていることとなる。spam メールの消去に要する時間もまちまちである。1 日あたりこの処理に 5 分以上かけるサンプルが 11%いるのに対して、まったく時間を費やさないというサンプルも 17%いる。平均では 2.8 分となる。2.8 分 × 2.9 日 = 8.12 分 となり、1 週間に平均して 8.12 分間 spam メールの処理に費やしていることになる。

この時間を経済的損失としてアメリカ全体で考えると、インターネットユーザ総数はおよそ 1 億 6940 万人であるとして、8.12 分 × 1 億 6940 万人 ÷ 60 分 ≃ 2290 万時間 となる。アメリカ人の 1 週間（40 時間）の平均賃金は 724 ドルであるので、年間で計算すると 724 ドル × 2290 万時間 ÷ 40 時間 × 52 週 ≃ 215 億 8000 万ドル となる。

4.2 日本における経済的損失の試算

ここで、Rockbridge Associates(2005) によるアメリカの結果をもとに、日本での経済的損失を算出してみる。総務省（2005）によると[14]、全体の 86.6%が spam メールを受け取っている。1 日あたり 1 通以下のユーザが半数近く（49.6%）を占めるが、11 通以上受信しているユーザも 15.4%存在する。また、経済産業省のアンケート調査によると[15]、2004 年 11 月における spam メール平均受信数は、1 週間あたり 34.0 通で、1 日あたり 34.0 通 ÷ 7 日 ≃ 4.86 通 となる。インターネットユーザ数は 7948 万人であるので、日本全体の 1 年間の spam メールの総数は、4.86 通 × 7948 万人 × 365 日 ≃ 1410 億通 となる。

アメリカでは spam メールの処理に費やされる時間の平均値は 1 週間あたり 8.12 分であるので、spam メールを受け取る数に比例させて考えると、日本では 8.12 分 × $\frac{4.86 \text{ 通}}{18.5 \text{ 通}}$ ≃ 2.13 分 となる。これを日本全体で考えると、インターネットユーザ総数はおよそ 7948 万人であるので、2.13 分 × 7948 万人 ÷ 60 分 ≃ 282 万時間 となる。日本人の 1 時間あたりの平均賃金は 1235 円[16] であるので、年間で計算すると 1235 円 × 282 万時間 × 52 週 ≃ 1810 億円 となる。

アメリカに比べると、spam メールの数がまだ少ないこともあり、経済的損失も少ないが、それでもかなりの額となっていることがわかる。

4.3 ICT 資産における経済的損失の試算

これまでは、労働力の観点からのみ spam メールによる経済的損失をみてきたが、spam メールによる経済的損失はそれだけではない。本書の研究対象である ISP 業界は、spam メールを防ぐためのシステムやソフトウェアの開発に大きな投資をしている。また、spam メールの配送にはインターネット上のネットワークやサーバが使われており、もし spam メールがなければ、これらの設備投資を他の投資に振り替えることが可能である。しかし、従来の調査報告書には ICT 資産の追加的投資による経済的損失は算出されていない。そこで本稿では、spam メールが存在しないと仮定した場合の ICT 資産に対する最適な設備投資額に比べて、現在余分に投入されている額を全世界およびアメリカ、日本において試算してみる。

[14] 2004 年 1 年間についてのウェブによる調査である。

[15] http://www.iajapan.org/anti_spam/event/2005/conf0510/pdf/3-2.pdf

[16] 厚生労働省統計表データベースシステムのウェブページ（http://wwwdbtk.mhlw.go.jp/ toukei/ kouhyo/ indexk-roudou.html）より、2004 年の「1 時間当たりきまって支給する現金給与額」である。

電子メールにより使用される ICT 資産は主にネットワークとサーバである。まず、ネットワークに関して考察してみる。JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center）のホームページ（http://www.jpcert.or.jp/）の「インターネット定点観測システム（ISDAS）」（http://www.jpcert.or.jp/isdas/）に、日本のある複数地点を流れるパケット[17] を観測し、その量の平均値をポート番号[18] ごとに測定したデータがある。それを見ると、電子メールの配送に使われる SMTP が使用しているポート番号（TCP 25 番）を流れるパケット量は 1%にも満たないことがわかる。したがって、電子メールの配送によるトラヒックはネットワークにほとんど影響していないと考えることができる。このため本書では、spam メールによるネットワーク資産の余剰な投資は無視し得うるほど小さいと仮定する。

つぎに、サーバについて考える。シマンテック社の調査によりメール総数の 65%以上が spam メールだといわれているので、もし spam メールが存在しなければ、メールサーバの性能を半分に落としても問題ないと仮定する。Internet Systems Consortium, Inc.（ISC）のホームページ（http://www.isc.org/index.pl?/ops /ds/reports/2005-01/dist-bynum.php）によれば、2005 年 1 月の時点でのホストコンピュータ（サーバ）数は、全世界で 3 億 1764 万台、アメリカ（COM・NET・EDU・ORG・GOV・BIZ・MIL ドメイン）では 2 億 844 万台、日本（JP ドメイン）では 1954 万台である。サーバ総数のうちメールサーバの割合は、付録 A.2 のアンケート調査の結果からおよそ 10%であることがわかった。この結果より、全サーバ数の 10%がメールサーバであると仮定する。メールサーバ数はそれぞれ全世界で 3176 万台、アメリカで 2084 万台、日本で 195 万台と推定できる。日本でのメールサーバの平均価格は、（社）電子情報技術産業協会（JEITA : Japan Electronics and Information Technology Industries Association）の 2004 年度の統計データ（http://it.jeita.or.jp/statistics/midws/h16/9-work.html#1.html）より、約 36 万円と想定する[19]。性能が半分のもので処理できるので、24 万円のもので十分だと仮定する[20]。1 台あたり 36 万円 − 24 万円 = 12 万円 過剰な投資をしていることになる。コンピュータの価格には大きな地域差がないと仮定して、全世界、アメリカ、日本国内の過剰な投資を計算すると、それぞれ全世界で 12 万円 × 3176 万台 ≃ 3 兆 8000 億円、アメリカで 12 万円 × 2084 万台 ≃ 2 兆 5000 億円、日本国内で 12 万円 × 195 万台 ≃ 2300 億円 と算出される。これは、前節の労働力の経済的損失試算額を上まわる額である。

4.4 経済的損失のまとめ

アメリカと日本を単純な仮定のもとで比較したのが表 1 である。1 ドルは、104.9 円（2004 年 11 月の平均値）で換算している[21]。

表 1 において、「spam メールの数」は、インターネットを利用しているユーザが 1 日に受け取る spam メールの平均値である。「労働力の損失額」は、アメリカの場合、4.1 節で算出したアメリカ全体の損失額で、日本の場合、4.2 節で算出した日本全体の損失額を 1 ドル 104.9 円で US ドルに換算した額である。「GDP あたりの労働力の損失額」は、アメリカと日本の 2004 年の名目国内総

17) パケットとは、コンピュータ通信において、送信先のアドレスなどの制御情報が付加された小さなデータのまとまりのことである。
18) ポート番号とは、サーバ上のサービスを特定するために使われる IP アドレスの下に設けられたサブアドレスである。
19) メールサーバの価格はまちまちであるが、サーバ類のなかでは比較的能力が小さいものであるため、100 万円未満のワークステーションの金額と台数から算出した。
20) コンピュータの性能としては、CPU のクロック数と、メインメモリの容量、そして、ハードディスク容量を考慮して、各コンピュータメーカーの製品価格表から 3 分の 2 から半分程度の価格となることを割り出した。
21) 日本銀行のホームページ（http://www.boj.or.jp/stat/tame/tame0411.htm）より、2004 年 11 月の平均値である。

表 1: spam メールによる経済的損失の試算

	アメリカ	日本
spam メールの数 (1 日の平均)	18.5 通	4.86 通
労働力の損失額	216 億ドル	17 億ドル
GDP あたりの労働力の損失額	0.18%	0.037%
ICT 資産の損失額	238 億ドル	22 億ドル
GDP あたりの ICT 資産の損失額	0.20%	0.048%

生産に対する割合である。「ICT 資産の損失額」は、4.3 節で導出したアメリカおよび日本全体の損失額を 1 ドル 104.9 円で US ドルに換算した額である。「GDP あたりの ICT 資産の損失額」は、アメリカと日本の名目国内総生産に対する割合である。ここで、アメリカの名目国内総生産は 11 兆 7000 億ドル、日本の名目国内総生産は 4 兆 6000 億ドルである[22)]。

「労働力の損失額」と「ICT 資産の損失額」を比べると、アメリカも日本も「ICT 資産の損失額」が上回っている。このことから、ICT 資産における経済的損失も重要で、ユーザサイドによる対策だけでは十分でないことが明らかとなる[23)]。近年、大手全国系 ISP は、メールサーバの無益な増強を避けるために、spam メール対策に力をいれている。

経済的損失額をアメリカと日本で比べると、「GDP あたりの労働力の損失額」はアメリカが日本のおよそ 4.9 倍、「GDP あたりの ICT 資産の損失額」はアメリカが日本のおよそ 4.2 倍である。「spam メールの数」はアメリカが日本のおよそ 3.8 倍であることを考慮すると、損失額はほぼ spam メールの数に比例していると考えることができる。2005 年に入り日本でも、spam メールの数が大幅に増加している現状から 2005 年度の損失額は大幅に増加しているものと思われる。何らかの政策的対応をとらなければ、5 年以内には GDP あたりの損失額は、アメリカと肩を並べるようになるだろう。

5 結論と残された問題

本稿では、spam メール問題の本質は、spam メール業界が巨大なマーケットを形成しており、spam メール送信業者が十分な利益を上げることができるしくみになっていることを明らかにした。さらに、spam メールによる経済的損失は労働力の損失だけでなく、ICT 資産、特にメールサーバの追加的な投資が問題であることを示した。

したがって、社会的厚生の低下を防ぐために、ISP 業者が spam メール対策の追加的投資をおこなうことを容易にする、利子補給政策を含む何らかの政策的対応が必要である。さらに、電子メールユーザが spam メールの送信者や受信者になる意欲をできるだけ低く抑えるような経済・社会的制度を設計することが重要である。ソシオネットワーク戦略研究センターでは、第 3 回ソシオネットワーク戦略研究国際会議（2006 年 1 月 14 日・於関西大学）において、この問題をゲーム理論に

22) The World Bank のホームページ (http://siteresources.worldbank.org/ DATASTATISTICS/ Resources/ GDP.pdf) より。
23) いくらユーザがフィルタリングによって spam メールを排除しても、ユーザまで spam メールが配送された以上、メールサーバやネットワークの ICT 資産は消費されたこととなる。

おけるメカニズムデザインの手法を用いて検討する予定である[24]。

2002年に「特定電子メール送信適正化法」と「特定商取引法」が施行され、施行後は一時的にspamメール数が減ったようであるが、現在また増加傾向にある（山井・桝田（2005）の「4.1 法制面での問題と対策」岡村久道）。さらなる法の改正が必要であろう。そのためにも、送信者の特定が容易にできるしくみ作りが重要である。また、外国のメールサーバを使ったspamメール送信も多いことから、国際的な協力体制も必要である。

本稿の日米のデータを用いて、マクロ生産関数によるGNPの損失額を推計することが可能である。この点については、別稿において検討したい。

参考文献

[1] Judge,P.(2003),"The State of the Spam Problem," *EDUCAUSE review*, pp.60-61, Sep./Oct. 2003. (http://www.educause.edu/ir/library/pdf/erm0357.pdf)

[2] Loder,T., M.Van Alstyne and R.Wash(2004), "Information Asymmetry and Thwarting Spam," Social Science Research Network (SSRN), Jan. 2004. (http://ssrn.com/abstract=488444)

[3] Loder,T., M.Van Alstyne and R.Wash(2006), "An Economic Response to Unsolicited Communication," *Berkeley Journal of Economic Analysis and Policy, forthecoming.*

[4] Nelson,M.(2003),"Spam Control : Problems and Opportunities," Ferris Research, Jan. 2003. (http://www.ferris.com/view_content.php?o=Spam+Control&id=105)

[5] Nucleus Research(2004),"Spam : The Serial ROI Killer," Nucleus Research, Inc. RESEARCH NOTE E50, June 2004. (http://www.nucleusresearch.com/research/e50.pdf)

[6] Rockbridge Associates(2005), "2004 National Technology Readiness Survey," the Center for Excellence in Service at the University of Maryland and Rockbridge Associates, Inc., Feb. 2005. (http://www.rhsmith.umd.edu/ntrs/NTRS_2004.pdf)

[7] 総務省編（2005），『平成17年版情報通信白書』ぎょうせい.

[8] 山井成良・桝田秀夫編（2005），「spamメールの現状と対策の動向」，『情報処理学会誌』，Vol.46, No.7, pp.739 − 791, Jul. 2005.

[9] 財団法人インターネット協会監修（2005），『インターネット白書2005』インプレス.

[24] 詳細は、Loder, Van Alstyle and Wash (2004, 2006) を参照されたい。