情報通信インフラにおける情報セキュリティ対策に関する研究

竹　村　敏　彦　　関西大学ソシオネットワーク戦略研究機構助教

1 はじめに

高度情報化社会において、インターネットはビジネスプラットフォームとなり、企業をはじめとする様々な組織の業務にとって重要な役割を果たしている。しかしながら、そのインターネットには様々な脅威が存在する。それらの脅威は最新の情報通信技術（ICT）だけでもって対応できるものはない。それはインターネットを介した個人情報の流出や不正アクセスによる情報セキュリティ被害等が新聞やテレビのニュースで取り上げられていることからも明らかである。それゆえに、これらの脅威に対して、企業は ICT の利活用とともに、適切なマネジメント等を実施する必要がある。また、政府も企業活動を円滑に行えるための適切な法整備・環境整備等を実施していく必要がある。しかしながら、企業および政府のいずれにおいても具体的にどのような対策や政策を実施すればよいか、まだわかっていない点が多い。

そこで、本調査研究では、重要インフラの１つであるインターネットを提供しているインターネット・サービス・プロバイダ（ISP）に焦点を当て、ISP の情報セキュリティ対策とその効果について議論を行っている。ここでの議論は、一般企業においても同様に適用できる。

本稿は、次のとおり構成される。第 2 節においては、本調査研究の背景と目的を明らかにし、情報セキュリティの経済分析の必要性と重要性について議論を行う。第 3 節においては、情報セキュリティインシデントのもたらす負の経済効果に関する実証研究と情報セキュリティインシデントと情報セキュリティ対策との関係に関する実証研究の結果を提示し、それぞれのテーマについて議論を行っている。具体的には、まず迷惑メールのもたらす産業別の労働損失および国内総生産（GDP）の試算を行い、それを低減させるために必要な ISP の対策について議論している。次に、ISP を対象とした不正アクセスやシステムトラブルといった情報セキュリティインシデント被害と脆弱性、情報セキュリティ対策（技術的対策およびマネジメント対策）等の関係を定量的に分析し、そこから有効となる政策について議論している。第 4 節では、本調査研究において行ったアンケート調査の概要を示すとともに、その結果から ISP の情報セキュリティ対策の実態を明らかにする。そして、第 5 節において本調査研究全体のまとめを行う。

2 本調査研究の背景と目的

2-1 背景

経済学におけるこれまでの ICT に関する研究は、ICT の利活用や ICT 投資によって企業価値や生産性、効率性の上昇、業務の効率化、新たなビジネスチャンスの創造等の正の経済効果の存在が理論的かつ実証的に確認され、その蓄積も進んでいる。そして、それらの多くで、「積極的に ICT 投資を行うべきである」ということが主張されてきている。また、ICT の進展とあいまって、ビジネスのプラットフォームもインターネットやネットワークを利用したものとなり、多くの経済活動全体がインターネットに依存している。このことは ICT の経済牽引への期待の表れである。

一方で、近年、経済活動がインターネットをはじめとする ICT に強く依存しすぎているとの懸念も指摘されている（山口［2007］）。その背景にあるものとして、ICT やインターネットの急速な普及とともに、マルウェア、不正アクセス、フィッシングやボットネットの拡大等といった様々な情報セキュリティインシデントの存在があり、それらは深刻な問題を引き起こしている。情報処理推進機構（IPA）、日本ネットワークセキュリティ協会（JNSA）やサイバークリーンセンター（CCC）等の調査によれば、情報セキュリティインシデント被害等が年々急増傾向にあることが明らかになっている（情報処理推進機構［2009］）。

情報セキュリティおよびその対策の技術的研究に関しては、情報工学の分野において情報セキュリティインシデント被害を未然に防ぐ自己防衛ネットワーク、迷惑メール対策としてのフィルタリング技術や盗聴防止のための暗号化技術の研究等が盛んに行われており、その研究蓄積もかなり進んでいる。しかしながら、経済学においては、上述したように、多くの研究が「ICT への投資、導入が企業価値創造や生産性・効率性向上に役立つ」という 1 つの側面しか捉えられておらず、情報セキュリティ対策やそのインシデントが経済

や企業活動に与える影響に関する研究はこれまであまり行われてこなかった。しかしながら、近年になり、情報セキュリティの重要性が認められるようになったために、徐々にではあるが研究の蓄積が進められている。ただし、その多くは定性的な分析もしくは Varian [2002]や Gordon and Loeb [2002]等が行ったゲーム理論等を用いた理論分析にとどまっており、定量的な視点に立った実証分析は世界的に見ても少ない。その意味において、「情報セキュリティの経済学」(Economics of Information Security) はまだ萌芽状態にある。

情報セキュリティの経済学における実証分析は、学術的な意義だけでなく、実務的にも大きな意義を持っている（情報セキュリティに関する政策の一材料となりうる)。そのため、今後更なる研究を行い、その蓄積を進められていく必要がある。

2-2 本調査研究の目的

本調査研究の目的は 2 つある。1 つ目の目的としては、情報通信インフラとしてインターネットを個人や企業に提供している ISP を対象にアンケート調査を実施し、そこから情報セキュリティ対策の現状を把握することである。2 つ目の目的としては、情報セキュリティ対策および情報セキュリティインシデントを定性的かつ定量的に分析を行い、企業が取るべき対策と政府が取るべき政策について示唆を与えることである。

3 実証分析

3-1 迷惑メールによる経済損失の試算と ISP の役割

情報セキュリティインシデントの経済全体に与えるインパクトの定量的な分析というものはこれまであまり行われてこなかった。その理由として、それらに関するデータが存在していなかったことや、ICT の正の経済・経営インパクトに注目し、その影の部分である ICT の負のインパクトは研究の対象とされてこなかったこと等が挙げられる。しかしながら、これらの定性的かつ定量的な分析は、政策や対策を考えていく上で必要である。そこで、ここでは、情報セキュリティインシデントの 1 つである迷惑メールに着目して、それが経済に与えている負のインパクトを定量的な分析を試みる。これらの詳細については、Takemura and Ebara [2008a]や竹村・若林 [2008]等を参照されたい[1)]。

本研究では、業務上、電子メールを利用している企業等の組織で働いている労働者（就業者）が迷惑メールの受信に伴い、相当量の処理のための時間浪費を余儀なくされているという認識の下、迷惑メールを処理（削除）するために用いられている労働時間（労働時間の浪費）がどの程度の国内総生産（GDP）水準を低下させるのかといった経済的損失を試算している。その分析するためのフレームワークとしてセミマクロの生産関数を用いている。これらの関係を図示しているのが図 1 である。

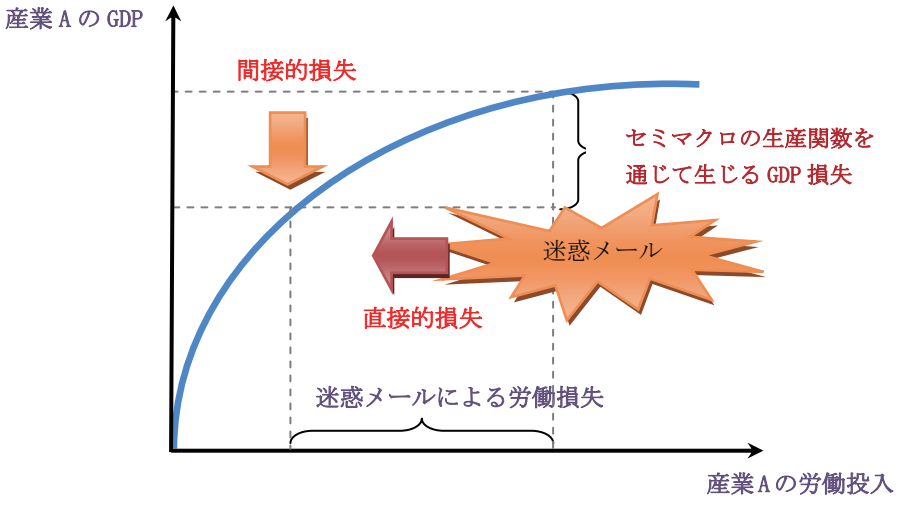


図 1　迷惑メールによって引き起こされる労働損失と GDP 損失の関係

1996 年度から 2005 年度の各産業の GDP、資本ストックと労働力で構成されるデータを用いてパネルデータ分析を行って、生産関数の各係数パラメータを推計し、それをもとに、迷惑メールによって生じた産業別の経済損失額を試算した。その結果が表 1 である。表 1 から産業ごとにその被害の大きさの差異があることが分かる。また、それぞれの総和をとることで、迷惑メールによる日本全体の GDP 損失が年間 9,600 億円、労働損失が 2 億時間にも及んでいることがわかっている（Takemura and Ebara [2008a])。

表 1　迷惑メールによる産業別 GDP 損失（単位：10 億円）

産業	GDP 損失
農林水産業・鉱業	6.36
建設業	26.17
製造業	0. 42
卸売・小売業	36.66
金融・保険業	86.02
不動産業	168.14
運輸業	63.73
通信・放送業	47.00
電気・ガス・水道業	145.29
情報サービス業	161.82
医療・福祉業	68.98
教育・研究支援業	88.90
その他サービス業	58.29

もし十分な迷惑メール対策がなされなければ、今後もこの労働損失および GDP 損失は増加することになる。これらを低減させるための対策が必要である。主要な迷惑メールに対する技術的対策としては、送信対策やフィルタリングがある。また、そのレベルも ISP、企業のシステム管理者と個人で異なる。その一例を表 2 にまとめている。

表 2　迷惑メールに対する技術的対策

内容	主要実施対象
送信ドメイン認証	ISP・企業
フロー制御	ISP・企業
WL/BL/GL 等のリスト利用	ISP・企業
メール内容分析	ISP・企業・個人
ウィルス対策ソフトウェアの導入	ISP・企業・個人

表 2 において近年効果が認められているものとして、送信ドメイン認証がある。特に、送信ドメイン認証の一つであり、ISP が行っている OP25B（Outbound Port 25 Blocking）は最も効果的・有効的な対策であると言われている [2)]。第 4 節でも紹介するが、2009 年 2 月時点で、約 62%のアンケートに回答した ISP が OP25B を実施していることがわかっている。理想としては、全ての ISP が OP25B を実施する必要がある。しかしながら、インターネットユーザの利便性等に関する問題があり、今後更なる議論を行う必要がある。勿論、迷惑メール対策は ISP のみが実施するだけでなく、個人や企業もまたあわせて実施することで高い効果を期待することができる。

3-2 ISP の情報セキュリティインシデントと対策の関係

このわずか十数年で企業のビジネス環境、また個人のライフスタイルは大きく変革した。この背景にはインターネット・ブロードバンドの普及がある。このインターネット環境を提供しているのがISPである。つまり、ISPは情報通信インフラを担う存在であり、社会にとってある種必要不可欠な存在でもある。しかしながら、多くのISP（とりわけ、地域系ISP）は2000年頃を期に、経営状態が良好であると言い難い状況にある。この一因としては、低価格・高品質の接続サービスのみならず、様々なアプリケーションサービス（例えば、IP電話、ブログ、コンテンツサービス等）やオペレーションサービスを提供しなければ、ユーザの確保が困難となっていることが考えられる（榎原・中庭・竹村・横見 [2006]）。

このような状況の下であっても、ISPの多くが情報インフラを担う存在としての自覚を持ち、企業の社会的責任（CSR）という認識に基づいて情報セキュリティ対策を実施している。

第3-1節では、ICTの副産物である迷惑メールに焦点を当て、それに対してISPがOP25Bを実施することの意義について見たが、ここではより具体的に情報セキュリティインシデント被害に遭遇する確率を低下させる対策はどのようなものであるか、言い換えると、情報セキュリティインシデントに対してどのような対策が

有効となるかについて実証分析を行う。なお、詳細についてはTakemura, Osajima and Kawano [2009]を参照されたい。

本研究では、情報セキュリティ対策と被害との関係を調べるために、式 (1)のようなロジスティック回帰モデルを用いる。なお、この式は情報セキュリティインシデント被害との関係として、情報セキュリティ対策だけでなく、脆弱性や ISP の特性を考慮したものである。

$$\log(p_j / 1-p_j) = a + b_V X_V + b_C X_C + cZ_C \quad (1)$$

ここで、p_jは情報セキュリティインシデント j（j =不正アクセスとシステムトラブル）の被害に遭遇する確率、X_V、X_C と Z_Cは、順に脆弱性、情報セキュリティ対策と ISP の特性を表している。また、情報セキュリティ対策は技術的なものとマネジメントによるものに大別している[3)]。

例えば、式 (1)を用いることで、b_C<0（b_C>0）であれば、情報セキュリティ対策がインシデント被害に遭遇する確率を低下（上昇）させることを確認できる。対策の効果としては b_C<0 となることが期待される。

式(1)の係数パラメータを、最尤法（SPSS における変数減少法と変数増加法を併用）を用いて推計した結果が表 3 と表 4 である。なお、$b_{C,NS}$は技術的対策、$b_{C,EDU}$はマネジメント的対策の係数パラメータである。

表 3　推計結果 I（不正アクセス）

	係数パラメータ	標準誤差	exp[B]
$b_{C,NS}$	1.755	0.789	5.686
$b_{C,EDU}$	-4.515	1.966	0.011
Constant	-2.108	1.436	0.121
	Chi-square(5)=2.556 [0.768], 7 Steps　正答率: 80.6%		

表 4　推計結果 II（システムトラブル）

	係数パラメータ	標準誤差	exp[B]
$b_{C,NS}$	0.522	0.292	1.685
$b_{C,EDU}$	-1.968	1.220	0.140
Constant	0.877	1.169	2.403
	Chi-square (5)=7.659 [0.176], 6 Steps　正答率: 73.7%		

表 3 と表 4 より、情報セキュリティ教育を行うことで情報セキュリティ被害に遭遇するリスクを低くすることができるものの、単なる情報セキュリティシステムを導入する対策は不正アクセスやシステムトラブルといった情報セキュリティ被害に遭遇するリスクを高めてしまうことがわかる。この結果は以下のように解釈することができる。まず、多くの種類のシステムを導入するといった技術的対策は必ずしも有効となっていない[4)]。この理由の 1 つとして、とりわけ地域系 ISP が人材不足に直面していることが考えられる。つまり、様々なシステムを導入したとしても、それを適切に運用・管理する人材が不足する場合、その対策から得られる効果は期待できないどころか、逆効果になってしまうことになる。次に、マネジメント対策として情報セキュリティ教育の実施は有効ではあるが、システム監査やペネトレーションテストの実施といったものは必ずしも有効となっていない。このことから、情報セキュリティ教育の（継続的な）実施と充実が重要であることがわかる。なお、一般企業を対象として情報セキュリティ対策の実証分析を行っている田中・松浦 [2006]や竹村・峰滝 [2009]や一般のインターネットユーザの情報セキュリティ対策の実証分析を行っている竹村・海野 [2009]においても同様の主張がなされている。そして、これは ISP だけではなく、業界や政府と連携した形で実施することが、今後望まれる。

4 アンケート調査による ISP の情報セキュリティ対策の実態把握

4-1 ISP を対象とした情報セキュリティ対策に関するアンケート調査について

（1）アンケート調査の目的

インターネットは重要インフラの一つで、それを提供する ISP の果たす社会的役割は重要なものとなっている。しかしながら、ISP の情報セキュリティ対策および投資の実態に関する公表されたデータはなく、その現状把握は困難なものとなっている。そこで、本アンケート調査にて ISP の情報セキュリティ対策および

投資の実態を把握し、またそこから ISP および企業、個人が実施すべき対策、また政府が実施すべき政策について明らかにすることを目的としている。

（２）実施概況

2008 年 12 月時点で「社団法人日本インターネットプロバイダー協会」のホームページに記載されている 583 社の ISP を対象に記名式の郵送アンケート調査を実施した。なお、有効回答率は約 9.4%、アンケート実施期間は 2008 年 12 月から 2009 年 2 月である。

（３）質問項目

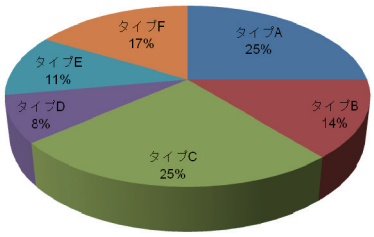
アンケート調査は、大別して、1）事業状況、2）情報セキュリティ対策、3）情報セキュリティ被害・システムトラブルの遭遇状況、4）情報セキュリティに対する意識、5）政府の情報セキュリティ政策に対する意見、で構成されている。

4-2 ISP の情報セキュリティ対策の実態と現状

ここでは、アンケート調査結果の一部（抜粋版）を紹介する。なお、ISP の情報セキュリティに関する実態調査の詳細は竹村 [2009]を参照されたい。

（１）ISP の事業概況

年間売上高・純利益、加入者数、従業員数、提供している接続サービス・アプリケーションサービスや経営戦略等についての項目がある。図 2 には、ISP が競争他社の経営戦略（価格、サービス内容、サービス品質）に対して関心があるものの順位を示したものである。タイプ A とタイプ C はそれぞれ約 25%で、ともに割合が最も高くなっている。また、従業員数に関しては正規社員とアルバイト・パートタイムともに必ずしも多いとは言えない状況にある。年間売上高・純利益に関しては、地域系 ISP と全国系 ISP とで大きな違いが確認されている。



タイプ
A: 価格＞サービス内容＞サービス品質
B: 価格＞サービス品質＞サービス内容
C: サービス内容＞価格＞サービス品質
D: サービス内容＞サービス品質＞価格
E: サービス品質＞価格＞サービス内容
F: サービス品質＞サービス内容＞価格

図 2　競争他社の経営戦略として関心

（２）情報セキュリティ対策

情報セキュリティに関する規定、管理担当者数、連絡体制、アップデート・パッチ適用状況、情報収集、ペネトレーション・システム監査・情報セキュリティ監査の実施状況、P2P の利用規制・OP25B 導入状況、導入システム、情報セキュリティ教育の実施状況や今後の計画等についての項目がある。これらの中で、情報セキュリティに関する規定、P2P の利用規制状況、OP25B 導入状況と情報セキュリティ教育の実施状況についてまとめたものを図 3 から図 6 に示している。

OP25B の導入状況について見てみるとその割合は約 62%になり、過去に行ったアンケート調査と比較して、その割合は高くなっている。また、OP25B を導入している ISP の約 53%が（迷惑メール被害の軽減の）効果を実感していると回答している。さらに、約 20%の ISP が情報セキュリティ教育の実施をしていないものの、

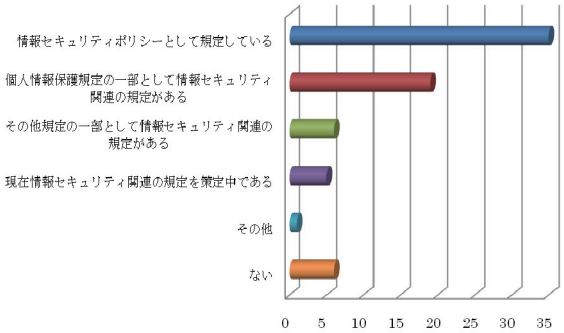


図 3　情報セキュリティに関する規定

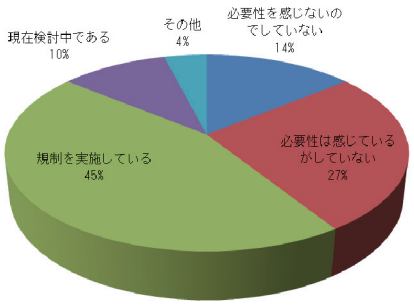


図 4　P2P の利用規制状況

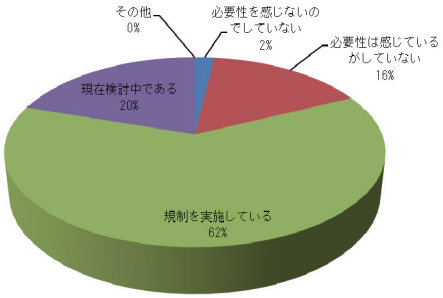


図 5　OP25B 導入状況

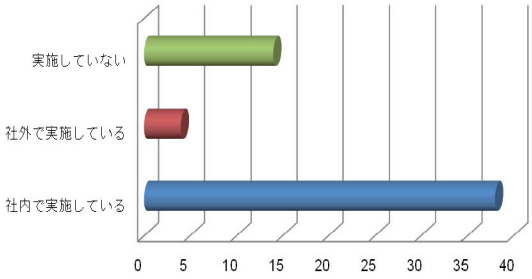


図 6　情報セキュリティ教育の実施状況

その他の ISP は社内もしくは社外において実施していることがわかる。そして実施していない理由として、人材不足が挙げられている。

（３）情報セキュリティ被害・システムトラブルの遭遇状況

不正アクセス被害、迷惑メール被害、マルウェアによる被害、システムトラブルの遭遇状況等についての項目がある。ちなみに、不正アクセス被害、迷惑メール被害、マルウェアによる被害、システムトラブルに遭遇した ISP の割合は、順に 35%、57%、4%、43%となっている。図 7 と図 8 は、迷惑メール被害およびシステムトラブルの状況（ネットワークへの影響度合い）を表している。これらから少なくとも被害に遭遇した場合、ネットワークへ影響を受けることがわかる。

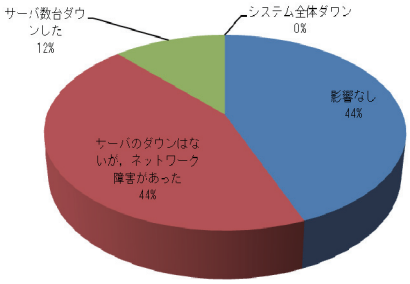


図 7　迷惑メール被害の状況

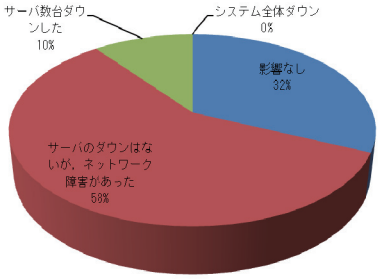
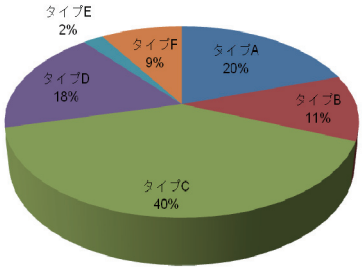


図 8　システムトラブルの状況

（４）情報セキュリティに対する意識

情報セキュリティ対策への優先度、効果的に思う情報セキュリティ対策、情報セキュリティ対策へのイメージ、関心のある最近の ICT 等についての項目がある。図 9 には情報セキュリティ対策の優先順位をまとめたものを示している。これから、既存サービスの現状維持を最優先としている ISP が多いことがわかる。



タイプ
A: 対策＞既存サービスの現状維持＞新規サービスの展開
B: 対策＞新規サービスの展開＞既存サービスの現状維持
C: 既存サービスの現状維持＞対策＞新規サービスの展開
D: 既存サービスの現状維持＞新規サービスの展開＞対策
E: 新規サービスの展開＞対策＞既存サービスの現状維持
F: 新規サービスの展開＞既存サービスの現状維持＞対策

図 9　情報セキュリティ対策の優先順位

（５）政府の情報セキュリティ政策に対する意見

（金銭的・非金銭的な）公的補助の必要性や政策パッケージの必要性、セキュリティ政策の有効性の是非、認証制度への関心、政府への希望等についての項目がある。

とりわけ、非金銭的な公的補助（啓蒙活動や情報提供等）の必要性を求めている ISP の割合は 58%、また「どちらでも」という回答を含めるとその割合は 96%にまで及んでいる。

5 まとめ

本調査研究では、ISP の情報セキュリティ対策の現状の把握を行うとともに、情報セキュリティ対策および情報セキュリティインシデントを定量的に分析してきた。現状把握および 2 つの実証分析については、すでに上述した通りである。多くの ISP は厳しい経営状態にあるにも関わらず、ユーザに安心・安全なインターネットを提供することの必要性を鑑みて、努力を重ねている。一般企業は、情報セキュリティ対策とその意識について、必要とされる情報セキュリティ水準の違いはあるものの、ISP から学ぶべき点が多くあると思われる。

本調査研究が学術的のみならず、現実世界の情報セキュリティ対策に寄与することを期待したい。また、今後もこの調査研究を継続し、この種の情報セキュリティ対策に関する研究の蓄積を行っていく。

【参考文献】

Gordon, L. A., M. P. Loeb. (2002): "The Economics of Information Security Investment" *ACM Transactions on Information and System Security*, Vol.5, pp438-457

Takemura, T., Ebara, H. (2008a): "Economic Loss Caused by Spam Mail in Each Japanese Industry" *Selected Proceedings of the First International Conference on Social Sciences* (Social Sciences Research Society), Vol.3, pp29-42

Takemura, T., Ebara, H. (2008b): "Spam Mail Reduces Economic Effects" *Proceedings of the 2nd International Conference on the Digital Society*, pp20-24

Takemura, T., Osajima, M., Kawano, M. (2008): "Positive Analysis on Vulnerability, Information Security Incidents, and the Countermeasures of Japanese Internet Service Providers" *Proceedings of World Academic of Science, Engineering and Technology*, Vol.36, pp703-710

Varian, H. R. (2002): "System Reliability and Free Riding."*ACM Transactions on Information and System Security*, Vol.5, pp355-366

榎原博之・中庭明子・竹村敏彦・横見宗樹 (2006): 『インターネット・サービス・プロバイダの実証分析』多賀出版

情報処理推進機構 (2009): 『情報セキュリティ白書 2009』実教出版

竹村敏彦 (2009): 「第 3 回インターネット・サービス・プロバイダの情報セキュリティに関する実態調査報告書」関西大学

竹村敏彦・海野敦史 (2009): 「インターネットユーザの情報セキュリティ意識に関する研究」『情報通信ジャーナル』forthcoming

竹村敏彦・峰滝和典 (2009): 「企業価値向上をもたらす戦略的情報セキュリティ対策のための政策」『第 66 回日本経済政策学会全国大会予稿集』

竹村敏彦・若林成嘉 (2008): 「迷惑メールが日本経済に及ぼす影響の調査について」『データ通信』No.163, pp19-30

田中秀幸・松浦幹太 (2006): 「情報セキュリティ投資の経済的動機付けに関する企業レベルの実証研究」研究調査報告書（財団法人電気通信普及財団）第 21 号, pp9-16

山口英 (2007): 「学会への期待」『JSSM セキュリティ公開討論会配布資料』

1) 労働損失や GDP 損失に加えて、労働生産性の低下等、生産関数そのものへの影響について実証分析しているものとして、Takemura and Ebara [2008b]がある。

2) OP25B とは、悪意あるユーザが自前のメールサーバから迷惑メールの送信を行うことや SMTP 拡大型のウィルスに感染した PC からウィルスメールが送信されること等を防止するために、ISP 側で許可した特定のサーバ以外の SMTP（TCP ポートの 25 番）の送信をブロックする対策のことである。

3) 脆弱性指標として、サーバ数とユーザ数の対数をとったものを 2 つ用いている。また、技術的（情報セキュリティ）対策を表す指標として、導入しているシステム数を用いている。マネジメントによる対策を表す指標としては、情報セキュリティ教育の実施状況、ユーザへの注意喚起、ペネトレーションテストの実施状況とシステム監査の実施状況を用いている。ISP の特性を表す指標としては、サービス提供エリア（地域系 ISP もしくは全国系 ISP）を用いている。

4) しかしながら、これらの対策を全くしなければ、逆に被害に遭遇するリスクを高めることになる。

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Economic Loss Caused by Spam Mail in Japanese Industries	RCSS Discussion Paper Series, No.67	2008 年 6 月
Economic Loss Caused by Spam Mail in Each Japanese Industry	The 1st International Conference on Social Sciences (Social Sciences Research Society)	2008 年 8 月
迷惑メールが日本経済に及ぼす影響の調査について	日本データ通信, 第 163 号	2008 年 9 月
Spam Mails Spoil Japanese Economy	The 4th International Conference on Information Communication Technology Policy	2008 年 10 月
Empirical Analysis on Information Security Countermeasures of Japanese Internet Service Providers	RCSS Discussion Paper Series, No.75	2008 年 11 月
Positive Analysis on Vulnerability, Information Security Incidents, and the Countermeasures of Japanese Internet Service Providers	The 5th International Conference of Social Sciences (World Academy of Science, Engineering and Technology)	2008 年 12 月