様式 C-19

科学研究費補助金研究成果報告書

平成２２年　５月　７日現在

研究種目：若手研究(B)
研究期間：2008 ～ 2009
課題番号：20730196
研究課題名（和文）情報セキュリティに対する脅威の経済分析と有効な情報セキュリティ政策の提案
研究課題名（英文）Economic Analysis on Information Security Incidents and Suggestion on Effective Information Security Policies

研究代表者
竹村　敏彦（TAKEMURA TOSHIHIKO）
関西大学・付置研究所・助教
研究者番号：00411504

研究成果の概要（和文）：本研究の目的は、情報セキュリティに対する脅威の経済・経営に与えるインパクトを分析し、情報セキュリティ対策、また政府として取るべき政策として何が有効であるかを明らかにすることである。この目的を達成するために、本研究では、Web アンケート（インターネット）形式の調査を実施し、収集・蓄積した個票データをもとに行動経済学やミクロ経済学の視点を踏まえた実証分析を行った。その結果、労働者と管理者の間にも情報セキュリティ及びその対策について意識の差異があること、また、労働者間においても労働形態や組織属性などによって情報セキュリティ意識や行動に差異があることを確認している。そして、これらの差異を埋めるためには、情報セキュリティ教育が有効であることを明らかにし、政府としてもそれをサポートする施策が必要であることを主張している。

研究成果の概要(英文)：The purpose of this research is to clarify the effective information security countermeasures and policies by quantitatively analyzing impact of information security incidents toward economy and business. For the purpose, from the viewpoints of behavioral economics and microeconomics, I carry out some empirical analyses using micro data collected from the Web-based survey. As a result, it is found that there is an information security gap between workers and managers and there is also a difference in information security awareness and behavior between workers by some attributes such as working pattern and the organization attributes. Then, it is insisted that information security education is effective and that the government should support the education.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	900,000	270,000	1,170,000
2009 年度	1,000,000	300,000	1,300,000
年度			
年度			
年度			
総　計	1,900,000	570,000	2,470,000

研究分野：　社会科学
科研費の分科・細目：経済学・経済政策
キーワード：情報セキュリティの経済学、Web アンケート（インターネット）調査、リスクマ

ネジメント、心理学的要因、情報セキュリティ意識、情報セキュリティ行動、セキュリティインシデント、情報通信技術

１．研究開始当初の背景

経済学や経営学において、情報通信技術（ICT）に関する実証研究で注目されてきたのは、ICT の利活用や ICT 投資がもたらす正の経済効果（生産性、効率性や企業価値の向上等）であった。ICT による正の経済効果の存在が理論的かつ実証的に確認され、その研究蓄積も進んでいる。そして、それらの研究の多くは「積極的に ICT 投資をおこなうべきである」ということを主張している。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。これらは 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。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などの様々な情報セキュリティインシデント（ICT 化の副産物）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）などの調査によれば、情報セキュリティインシデント被害などが年々急増傾向にあることが明らかになっている。

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など盛んに行われており、それらの研究蓄積もかなり進んでいる。一方で、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」という一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 2000 年に入るまであまり行われてこなかった。その意味において、まだ情報セキュリティ経済学（Economics of Information Security）は国内外を問わずまだ萌芽状態にある。しかしながら、社会・組織における情報セキュリティの重要性が認識されるに従って、徐々にではあるが研究の蓄積が進められるようになった。その多くが、理論的もしくは定性的研究にとどまっており、国内外ともに、定量的（実証）研究は今なおそれほど多くない。

実証研究がこれまでほとんど行われてこなかった主要な理由としては、分析するための個票データが整備されていない（そもそもデータがない）ことが挙げられる。また、情報セキュリティは内容がとてもセンシティブなものであり、企業などになかなか（調査）協力をしてもらえないというもう一つの側面も持っている。この問題を何らかの形で解決しなければ、情報セキュリティの実証分析が進まないことになる。

２．研究の目的

本研究の目的は、日本における情報セキュリティに対する脅威の経済・経営に与えるインパクトを定性的のみならず定量的に分析し、経済活動を安心して行うことができるために必要とされる情報セキュリティ対策、また政府として取るべき政策は何であるかを具体的に提示することにある。

本研究で行う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、（情報セキュリティに関する政策の一材料となりうることを考えると）実務的にも大きな意義を持っている。

３．研究の方法

本研究では、一部では公表されているデータを用いて分析を行っているが、主要な部分は、（本研究を通じて）独自に収集・蓄積を行った個票データを用いて分析を行う。

以下、研究の方法に関して順に説明を行う。

（１）個票データの収集・蓄積－Web アンケート調査の実施－

利用できる情報セキュリティに関する個票データがないため、本研究では、近年注目を浴びている調査手法である Web アンケート（インターネット）形式の調査を平成 20 年度および平成 21 年度に計 2 回実施し、個票データの収集・蓄積を行った。この調査法は様々な統計的な問題（サンプルが無作為に抽出されていないなど）が指摘されている。しかしながら、労働政策研究・研修機構（2005）「インターネット調査は社会調査に利用できるか」『労働政策研究報告書』No.17 でも述べられているように、調査の目的が個人や組織の意思決定の一つの有益な判断材料を提示することであれば、この方法を採用することに意義がある。

この調査は、2 年以上、同一組織（企業）で働き、調査会社にモニターとして参加している個人（労働者）を対象とし、彼らのインターネット利用および情報セキュリティへの意識を把握するために行ったものである。それゆえ、情報セキュリティ意識、学歴、リスクへの態度や賃金体系、組織属性、企業内で実施されている情報セキュリティ対策に関する状況、情報セキュリティ被害遭遇状況などに関して 50 問以上にもわたる質問を行っている。

調査に際しては、モニターを利用する Web アンケート調査では、調査対象者への調査票公開時期（曜日・時間）によって、サンプルに偏りが生じるために、表 1 に従った事前割付を行った。なお、表 1 に示した通り平成 20 年度と平成 21 年度において調査対象者の割付が若干異なっている。平成 21 年度は『労働力調査』（総務省）の地域別集計に基づき地域別割付を行っている。また、サンプルサイズは平成 20 年度では 600（人）、平成 21 年度では 1268（人）となっている。

表 1 調査対象者割付基準

割付項目	H20	H21
職業形態	○	○
上場・非上場	○	○
年齢		○
性別		○
地域		○

質問内容に関して、平成 22 年度のアンケート調査では情報セキュリティおよびその対策に対する意識（awareness）に加えて、新たに「行動（behavior)」についても質問を追加した。

（2）経済分析

本研究では、定性分析および定量（実証）分析を行う。定性分析としては、文献および過去の関連事例をとりあげた研究を行った。一方で、実証分析としては、主として、収集・蓄積した個票データを用いた研究を行う。その際の理論的フレームワークとして、心理学的要因をモデルに組み込みやすいミクロ経済学や行動経済学を用いた。また、統計手法としては、ノンパラメトリックな手法に基づく分散分析、順位相関分析、ロジスティック回帰分析や時系列分析などを用いた。

（3）研究体制・研究協力者からの支援

本研究は、経済学のみならず、情報工学や経営学、法学、社会心理学や政策実務といった様々な観点から遂行される必要がある。そのために、研究協力者からの支援をうけながら小規模研究会の開催や研究成果の外部発信を積極的に行った。

① 小規模研究会の開催

平成 17 年度から研究代表者が主催している研究会のメンバーや研究協力者、政策実務か等（URL: http//www2.ipcku.kansai-u.ac.jp/~a084034/project.html を参照）と、アンケート調査の企画・設計に関する綿密な議論をはじめとする研究全般に関する研究会を、大阪および東京にて、平成 20 年度および平成 21 年度に年 6 回（計 12 回）開催した。それと同時に、文理融合・学際的な共同研究をメンバーとともに行った。

② 研究成果の外部発信

研究成果は、上述したように、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ため、国内外の学会・研究会などで報告し、それを査読付学術雑誌に投稿するだけでなく、竹村敏彦（研究代表者）のホームページを通じて積極的に研究成果に関する情報の外部発信を行った。

また、本研究で収集・蓄積した個票データは、学術的にも実務的にも価値があるものであることを鑑みて、個人や組織を特定化できる情報を除き、学術目的にのみ利用できる体制（データ共同利用）をとっている。この活動はこの分野の学術発展に寄与するものである。詳しくは竹村敏彦（研究代表者）のホームページを参照されたい。

4．研究成果

（1）迷惑メールの経済損失の試算

業務上、電子メールを利用している企業など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。この認識の下、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額を経済学的フレームワークによって試算した。なお、分析に際して、1996 年度から 2005 年度における各産業の GDP、資本ストックと労働力で構成されるデータによるパネルデータ分析を行い、セミマクロの生産関数の各係数パラメータを推計した。その推計結果をもとに、データ通信協会が実施したアンケート調査結果とリンクし、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ところ、表 2 の試算結果が得られた。

表 2 から産業毎に被害の大きさの差異があることが分かる。また、迷惑メールによる日本全体の GDP 損失が年間 9600 億円、労働損失時間が約 2 億時間にも及んでいることを確認することができる。

もし十分な迷惑メール対策をしなければ、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

表 2　迷惑メールによる産業別 GDP 損失（一部抜粋）

産業	GDP 損失（億円）
農林水産業・鉱業	6.36
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
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

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、そのレベルもインターネット・サービス・プロバイダ（ISP）、企業のシステム管理者や個人で異なる。その一例を表 3 にまとめている。

表 3　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
ブラックリスト等利用	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 3 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。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といえる。

（2）企業の情報セキュリティ対策の分析

① 企業を取り巻く経営環境および企業の情報セキュリティ対策への意識の変化

情報セキュリティインシデントは、人間の欲望、実態の無視や未熟さに起因するもの（Winny 事件や情報紛失・漏洩に代表されるもの）と金銭目的のネット犯罪に起因するものに大別される。これらは、インターネットがビジネスプラットフォームとなった昨今、特に、インターネットを業務に利用している企業にとって大きな脅威であり、また無視できない存在となっている。例えば、顧客情報や機密情報漏洩は必ずしもサイバーアタックなどによってネットワークを通じて起こるものでなく、日本ネットワークセキュリティ協会（2007）『2006 年情報セキュリティインシデントに関する調査報告書』によれば、その主たる理由は、紛失・置き忘れ、盗難、誤操作や設定ミスといった人為的ミス（ヒューマンエラー）であることが指摘されている。これらのことから、単なる技術導入だけでなく適切な情報セキュリティに関するマネジメントの導入・実施の必要性を指摘することができる。しかしながら、近年の急速な ICT 化により、様々なマネジメントやガバナンスが存在しており、全てを実施することは容易ではない。そのため、企業は自らにとって必要なものを適宜選択して、（PDCA サイクルに基づき継続的に）実施していく必要性があることを提案している。そして、これらを継続的に実施していくためには、企業価値向上などにつながるような戦略的な情報セキュリティ対策について経営者などに認識させていく必要があることについても併せて議論している。また、政府に対しても、省庁間の政策や法整備などのコーディネートおよび政策パッケージ作成の必要性などについての示唆を与えている。

② 企業価値向上などにつながる情報セキュリティ対策についての分析

情報セキュリティ対策等に関するいくつかの報告書では、情報セキュリティ対策・投資に対して、「費用対効果を考えると対策・投資の優先度が低くなる」、「対策として何をしてよいかわからない」という意見を企業がもっていることが明らかにされており、一部の企業で積極的に情報セキュリティ対策を行うインセンティブを持っていない感がある。それゆえに、企業に積極的に情報セキュリティ対策を行うインセンティブについて考える必要がある。本研究では、技術的対策だけでなく、マネジメント対策の必要について検証を行う。特に、様々なマネジメント対策の中でも特に有効となるものが何かを明らかにする。これは、技術は必要条件であるが、必ずしも十分条件にはなっていないことを意味している。同様のことが、マネジメントや政策にも当てはまる。つまり、技術、マネジメントと政策は相互補完的な関係にある。

この考え方の下で、本研究開始前（平成 20 年）に、竹村敏彦（研究代表者）が実施した本研究の調査に密接に関連する（2 年以上の）情報セキュリティ管理者もしくは精通した人物を対象とした「企業の情報セキュリティ対策に関する調査」（Web アンケート調査）によって収集・蓄積した個票データ（サンプルサイズは 500（人））をもとに、ロジスティック回帰モデルを用いて、情報セキュリティ対策とその効果の関係についての分析を行った。なお、表 4 には、対策を実施することによって企業価値向上につながると思われる効果を示している。

分析の結果、技術的対策よりもマネジメント対策、とりわけ情報セキュリティ教育や情

表 4　企業価値向上につながる効果
（一部抜粋）

No	内容	(%) a)
1	情報資産の見直し	58.6
2	業務プロセスの見直し・修正	61.6
3	経営層による情報セキュリティへのコミットメントの獲得	65.4
4	組織における情報セキュリティマネジメント能力の向上	66.4
5	ビジネスパートナーや顧客からの評価	59.0
6	競争力の強化	46.8
7	社会的責任としての自覚	69.6

a）効果を実感している企業の割合を表わしている。

報共有といったことが重要であることを明らかになった。そして、企業がこれらの対策を行えるように、政府は、ビジネス環境の整備（例えば、法制度や認証制度などの充実など）を行い、また人材育成や情報共有の具体的な方法を提示するとともに、それらに関するセミナー等の開催を積極的に行っていくことが必要とされる。これらを行うことで、企業に情報セキュリティ対策を行わせるインセンティブを与え企業の情報セキュリティ水準を底上げさせると同時に、企業価値向上に伴う経済活性化が期待される。

（3）労働者の情報セキュリティへの意識についての分析

平成 20 年度に実施した Web アンケート調査によって収集・蓄積した個票データをもとにして、「労働形態、所属組織の属性や個人属性によって労働者自身の情報セキュリティおよびその対策への意識に違いがない」という仮説を、ノンパラメトリックな手法に基づく分散分析（Mann-Whitney の順位和検定や Kruskal-Wallis 検定）によって検証を試みた。なお、労働者の情報セキュリティおよび情報セキュリティ対策への意識について、大別して 4 種類の指標（個人情報への意識、対策への意識、モラル、インターネットへの意識）を用い、いずれも意識が低いと小さい値、逆に意識が高いと大きな値をとる 5 段階の順序データである。

分析の結果、労働形態や組織属性、個人属性によって情報セキュリティ意識に差異が確認している。例えば、情報セキュリティを強化している（もしくは、しすぎている）企業において、情報セキュリティ意識に違いがあることがわかった。そして、これらの分析結果をもとにして、情報セキュリティ対策につながるモチベーションを持たせる企業システム（権限移譲、ストックオプションなど）の導入・充実や情報セキュリティ教育の充実が必要であることなどを指摘している。

（4）組織と労働者の間の情報セキュリティへの意識の違いについての分析

平成 20 年度に実施した Web アンケート調査などの個票データをもとに、ノンパラメトリックの手法に基づく分散分析によって、上場の有無、事業の公共性、年間売上規模や従業員規模といったカテゴリーによって、情報セキュリティ管理者と労働者の間で、情報セキュリティに対する意識の違い（ギャップ）があるか否かの検証を試みた。具体的には、情報セキュリティ対策を実施したことで実感できる効果に差異があるか否かを調べた。

分析の結果、非上場企業、公共性の低い企業、企業規模が小さい企業において、情報セキュリティ管理者と労働者の情報セキュリティ対策を実施して実感できる効果に差異があることが確認された。そして、様々な情報セキュリティ対策の中でも、企業は情報セキュリティ教育を行うことが情報セキュリティに対する意識を高めることにもつながり、有効となることを主張している。また、政府としては社会全体としてのセキュリティ水準を高めるためには、情報セキュリティ教育をサポートするようなセミナーの開催などの実施が重要な施策であり、もっと全国的に展開すべきであることを提案している。

（5）労働者の情報セキュリティへの意識と行動の関係についての分析

平成 21 年度に実施した Web アンケート調査によって収集・蓄積した個票データをもとにして、労働者の情報セキュリティおよび情報セキュリティ対策への意識と実際の行動の関係について「個人は情報セキュリティおよび情報セキュリティ対策の観点から問題があると認識していれば、そのような行動を起こさない」という仮説を 5 つの指標を作成し、順位相関分析によって検証を試みた。

各項目に関して、個人の意識については 7 段階（「1. 強く思わない」、「2. そう思わない」、「3. ややそう思わない」、「4. どちらともいえない」、「5. ややそう思う」、「6. そう思う」、「7. 強くそう思う」）で評価する形をとっており、また、行動については 4 段階（「1. 全くない」、「2. 数度程度ならある」、「3. たまにある」、「4. よくある」）もしくは 2 段階（「1. はい」、「2. いいえ」）で評価する形をとっている。

表 5 は順位相関分析の結果である。表 5 より、一般的には、情報セキュリティおよび情報セキュリティ対策に対する意識が高いほど、情報セキュリティおよび情報セキュリティ対策の観点から問題となる行動をとらないことを読み取ることができる。さらに、労働形態（正規・非正規）を 1 つの媒介と解釈し、「労働形態と意識」と「労働形態と行動」の関係をノンパラメトリックな手法に基づ

表５　Spearman の順位相関係数

意識と行動	係数
チェーンメールへの対応	-0.318***
情報セキュリティ対策の遵守よりも仕事の生産性や効率性を優先すること	-0.026
他人の暗号化されていない無線ネットワークを利用したネット接続	-0.217***
ウィルス対策ソフトを導入していない PC の利用	-0.292***
情報セキュリティ教育	-0.228***

注）***: 1%水準

く分散分析（Mann-Whitney の順位和検定）によって情報セキュリティおよび情報セキュリティ対策への意識と行動の関係が異なるか否かについて検証した。その結果、労働形態によって情報セキュリティおよび情報セキュリティ対策への意識の違いはほとんど確認されなかったが、いくつかの行動については違いがあることを確認している。そして、違いが確認された項目に関して、非正規労働者よりも正規労働者の方が情報セキュリティ対策に関して問題がある行動をとっている傾向があることを併せて確認している。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 27 件）

① Takemura, T., A Quantitative Study on Japanese Workers' Awareness to Information Security Using the Data Collected by Web-Based Survey, American Journal of Economics and Business Administration, 査読有, Vo.2, No.1, 2010, pp.20-26
② 筬島専・吉見憲二・豊川正人・竹村敏彦・海野敦史「女性の就業促進のためのテレワーク利用に関する課題」『早稲田大学大学院国際情報通信研究科紀要 2008-2009』査読有, 2009, pp.154-165
③ Takemura, T., Osajima, M., Kawano, M., Positive Analysis on Vulnerability, Information Security Incidents, and the Countermeasures of Japanese Internet Service Providers, International Journal of Business, Economics, Finance and Management Sciences, 査読有, Vol1, No.3, 2009, pp.220-227
④ Takemura, T., Ebara, H., Economic Loss Caused by Spam Mail in Each Japanese Industry, Selected Proceedings of 1st International Conference of Social Sciences, 査読有, Vol.3, 2008, pp.29-42
⑤ Takemura, T., Ebara, H., Economic Losses Caused by Spam Mail in Japan, Journal of International Development, 査読有, Vol.8, No.1, 2008, pp.23-33

他 査読有 3 件、査読無 19 件

〔学会発表〕（計 18 件）

①「Takemura, T., Minetaki, K., An Empirical Study on the Effects of Information Security Countermeasures, The 6th Annual Forum on Financial Information Systems and Cyber-security, Maryland, USA, 28th, October, 2009
②「竹村敏彦・峰滝和典・今川拓郎「労働者の情報セキュリティ意識に関する実証分析」2009 年日本経済学会秋季大会, 専修大学, 2009 年 10 月 11 日
③「竹村敏彦「情報セキュリティ対策を効果的に実施するためにはーアンケート調査データによる実証分析ー」情報セキュリティ心理学とトラスト(SPT)研究発表会, 情報処理推進機構, 2009 年 10 月 7 日
④「Takemura, T., An Economic Approach to Issues on the Information Security, International Workshop on Information Systems for Social Innovation 2009, Tokyo, Japan, 30th, September, 2009（招待講演）
⑤「竹村敏彦・筬島専「情報セキュリティ対策・政策に関する現状と課題」第 56 回日本情報経営学会全国大会, 横浜商科大学, 2008 年 5 月 25 日

他 国内学会 5 件、国際会議 8 件

〔図書〕（計 1 件）

① K. Jayanthakumaran (Ed.), Advanced Technologies, IN-THE, 2009, 698（分担執筆；Takemura, T., Osajima, M., Kawano, M., Economic Analysis on Information Security Incidents and the Countermeasures: The Case of Japanese Internet Service Providers, Chapter 5, pp.73-89）

〔その他〕
ホームページ等
http://www2.ipcku.kansai-u.ac.jp/~a084034/

６．研究組織
(1)研究代表者
竹村　敏彦（TAKEMURA TOSHIHIKO）
関西大学・付置研究所・助教
研究者番号：00411504