Web アンケート調査データを用いた情報セキュリティ教育に対する意識と行動に関する分析

竹村敏彦[1]

本稿では、日本の労働者を対象に行った Web アンケート調査によって収集したミクロデータを用いて、情報セキュリティ教育に対する意識と実際にとっている行動の関係について定量分析を試みている。その結果、概して、適切な行動をとっている労働者グループの方が問題ある行動をとっている労働者グループよりも、情報セキュリティ教育への意識の方が高くなっていることを確認している。また、組織で情報漏洩等の防止のために全面的に禁止されている事項に関して、問題のある行動をとっている労働者グループとそうでない労働者グループに情報セキュリティ教育への意識に違いがあるかについても検証している。その結果、顧客情報データの社外持出しに関しては意識の差があることを統計的に確認することができなかったが、顧客情報データの電子メールへの添付などの問題のある行動に関しては意識の違いがあることを明らかにし、また後者の情報セキュリティ教育に対する意識の方が前者よりも高くなっていることを確認している。

１．　はじめに

情報通信技術（ICT）が経営パフォーマンスの向上や経済を牽引に貢献しているという個票データ（ミクロデータ）に基づく実証研究は、1990 年代に入って米国を中心に世界各国で行われ、現在もその研究蓄積は進んでいる。それらの研究蓄積の中で、Solow (1987) で主張された「生産性パラドックス」を支持する研究は 2000 年に入り皆無となり、ICT 投資が企業や経済全体に対して正の経済効果をもたらすということで一つのメルクマールに達した。そして、次の段階として、より効率的に ICT 投資を行うための組織に関する研究蓄積が進められている[2]。これらの研究の多くでは、積極的な ICT 投資を促進すべきであると主張されている。一方で、ICT のもう一つの側面についても近年注目を浴びている。それは ICT と密接に関連している情報セキュリティに関する問題である。特に、多くの企業が直面している情報セキュリティに関する問題として、企業の情報セキュリティ水準が向上していないこと、情報セキュリティインシデント被害に遭遇することや労働損失が生じていることといった様々な問題が挙げられる。これらの問題に対する解決策として、暗号化技術などに代表される最新の技術に関する研究、経済学や経営学の視点からのマネジメントシステム等に関する定性的研究やゲーム理論を用いた理論的研究は盛んに行われている。なお、これまでの情報セキュリティの経済学（Economics of Information Security）に関する包括的なサーベイは Camp (2006)や Anderson and Moore (2009)等を参照された

[1] 関西大学ソシオネットワーク戦略研究機構

[2] ICT 投資の経済分析に関する先行研究は、篠崎（2003）、実積（2005)や竹村（2008)等を参照されたい。

い。これらの研究蓄積は、「規範」としてすべき技術的対策やマネジメント的対策、指針を教えてくれるが、それが実際うまく機能しているかを知る術までは教えてくれない。また、田中・松浦（2003）や Chan and Ho (2006)等で指摘されているように、情報セキュリティの問題の多くは、技術の問題よりはむしろヒトや組織の問題に起因すると考えられている。その意味においても、経済学や経営学的視点（社会科学的視点）に立った定量的研究（実証研究）が必要とされるものの、国内外ともにその研究はまだ少ない。その理由として、経済学者や経営学者の多くが ICT のもたらす正の経済効果を測定することにのみ関心がいっていたため、情報セキュリティに関する問題がそれほど大きなものであると思っていなかったことや、そもそも分析に利用できるミクロデータがなかったもしくは容易に利用できなかったことが挙げられる。

例えば、数少ない日本における経済学的視点に立った企業のセキュリティ対策に関する実証分析として、上野・田中 (2007)や竹村・峰滝 (2010)がある。前者は、情報セキュリティ投資への動機付けや効率的な対策の実施のあり方について、情報処理実態調査のミクロデータを用いて、実証分析を行った研究である。そして、分析の結果から、ファイアウォール等のハードウェアやセキュリティ対策アプリケーション等のソフトウェアによる技術的対策にとどめるのではなく、セキュリティマネジメントや人材教育といった目には見えない資産（intangible asset）への投資が重要となることを指摘している。後者は、企業が情報セキュリティ対策を実施したことで実感できる組織内外における効果（例えば、情報資産の見直しや競争力の強化等）について、インターネットアンケート調査（Web アンケート調査）により収集したミクロデータを用いて、実証分析を行った研究である。彼らは、効果を実感しやすい対策とそうでない対策があることを確認している。

いずれの研究も人材教育などの充実が効果的な情報セキュリティ対策につながることを主張している[3]。これらの研究は、企業や組織のセキュリティ管理者にとっては有益な情報を提供するものであり、社会的意義が多分にある。しかしながら、組織で対策をする側でなく、対策をされる側について考慮されていない。つまり、これらの研究は、組織としての情報セキュリティ対策の動機付けについて知ることができるが、組織の構成員である個人（従業員や役員等）の対策への動機付けについては知ることができない。

近年、組織の情報セキュリティ対策への意識を調べる研究が始められている。先駆的な研究として Albrechtsen (2007)がある。彼は、ノルウェイの IT 企業と銀行の従業員を対象に行った情報セキュリティに関する知識等に関するインタビュー調査から、多くの個人が多くの情報セキュリティ対策をあまり気にとめておらず、対策よりも他の業務を優先する傾向があることを確認している。また、Albrechtsen and Hovden (2009)は、ノルウェイの企業の情報セキュリティ担当者と労働者それぞれに対してインタビューを行い、情報セキュリティ実務に関して両者に「組織内デジタルデバイド」が存在していることを確認している。そして、彼らは、労働者に関する主な問題として情報セキュリティ対策に対する動機付けや知識の欠如を挙げている。

同様に、日本における研究として、Takemura (2010)や Takemura, Tanaka and

[3] 田中・松浦 (2003)では、費用対便益比率の低いユーザに対策をさせる必要があり、そのためにはどのようなマネジメントを行うべきかについていくつかの示唆を与えている。

Matsuura (2010)がある。彼らは日本の労働者を対象に行った Web アンケート調査から収集されたミクロデータを用いて、労働者の情報セキュリティ意識と組織の関係について統計分析を行っている。そして、Takemura (2010)は、労働者の情報セキュリティ意識と組織の関係について、組織の属性によって労働者自身の情報セキュリティ意識に違いがあることを明らかにしている。また、Takemura, Tanaka and Matsuura (2010)は、労働者と情報セキュリティ担当者の情報セキュリティ対策に対する意識にギャップがあるという分析結果を提示している。

これらの研究は、組織が情報セキュリティ対策を行っているといっても、実際の現場ではそれがうまく機能していないことを示唆し、また、組織の情報セキュリティ水準を向上させるためには、個人のセキュリティ対策に対する意識を変える必要性について指摘しているに過ぎない。個人の情報セキュリティ意識を高めることができたとしても、それが実際の行動に反映されていなければ意味が無い。つまり、根本的な情報セキュリティ対策としては、意識を高めるとともに、それが実際の行動に反映されるためにはどうすればよいか、またどのような動機付けを行う必要があるかまで考える必要がある[4]。竹村・田中・松浦 (2010)は、労働形態によって情報セキュリティ意識や実際にとっている労働者のセキュリティに関する行動に違いがあるかの検証を試みている。そして、労働形態によって情報セキュリティ意識に違いはほとんど確認されなかったものの、労働者のセキュリティに関する行動について違いがあることを確認し、非正規労働者よりもむしろ正規労働者の方が情報セキュリティに関する問題ある行動をとる傾向があることを指摘している。あわせて、彼らは順位相関分析を行い、個人は情報セキュリティ意識が高い程、情報セキュリティ対策の観点から問題となる行動をとりにくいことを確認し、情報セキュリティ意識を高めることができる情報セキュリティ教育の必要性について議論している。

本稿は、竹村・田中・松浦 (2010)で確認された結果を踏まえて、具体的にいくつかの情報セキュリティ対策の観点から問題となる行動を取り上げ、それらと情報セキュリティ教育に対する意識の関係を調べ、労働者の視点に立った情報セキュリティ教育の実施について議論を行う。彼らの研究との違いは、具体的な行動を取り上げて、情報セキュリティ教育に対する意識と実際の行動の関係を明らかにしようとしている点にある。また、組織が（強制的に）実施している情報漏洩対策を取り上げ、その対策の有効性に関する分析もあわせて行っている。これらの分析により、労働者の情報セキュリティに対する行動が意識の違いによって異なるか否かについて基礎的な情報を知ることができるとともに、有効な情報セキュリティ対策について議論する 1 つの材料を提示することができる。そしてこれは、学術的のみならず、実務的にも大きな意義があり、企業組織のみならず産業や国全体における情報セキュリティ水準の向上に寄与することを期待できる。

本稿の構成は次の通りである。第 2 節では、情報セキュリティに関する労働者のミクロデータを収集するために行ったアンケート調査の概要および分析に用いるデータの説明を行う。第 3 節は分析手法を簡単に紹介するするとともに、分析結果を示し、考察を行う。第 4 節では情報セキュリティ教育をサポートする取組を紹介する。そして、第 5 節にて本

[4] 行動経済学や実験経済学において、塚原 (2009)等に見られるように労働者の動機付けに関する研究が近年行われている。

稿のまとめを与えるとともに今後の研究の展望を示す。

２．　Web アンケート調査の概要

近年、社会調査環境の変化により、郵送アンケート調査やインタビュー調査、電話アンケート調査のいずれも実施および高回収率ともに厳しいものとなっている[5]。とりわけ、本稿で取り上げる情報セキュリティにおいては、多くの企業が「部外者に情報を出したくない」や「部外者と情報共有を望まない」といった理由により、調査の協力が得られなくなってきている[6]。これらの最初のデータ収集という壁を乗り越えるために、本稿では、マーケティングリサーチの分野で注目されている Web アンケート調査を採用した。なお、この調査法はサンプルが無作為に抽出されていない等の統計的な問題が指摘されている。しかしながら、労働政策研究・研修機構 (2005)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。また、本稿の結果は現時点では日本の労働者全てに対して妥当性をもつとまで言えないが、(限定的ではあるが) 調査会社にモニターとして参加している労働者に対して妥当性を有していることは主張できる。勿論、調査の正確性（accuracy）について議論する必要があるが、その議論については Web アンケート調査によって収集されたサンプルの歪みの補正を試みている星野 (2010)などに譲りたい[7]。

ここで、著者が 2010 年 3 月に Web アンケート調査法によって行った「労働者の情報セキュリティ対策に対する意識調査」で収集したミクロデータを利用する。この調査は、同一企業で 2 年以上働き、(Web アンケート調査会社にモニターとして参加している) PC やインターネットを業務で利用している個人を対象とし、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。そのため、彼らに対して、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等の 50 問以上にわたる質問を行っている[8]。

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・時間帯）によって、サンプルに偏りが生じるために、(事前) 割付を行った。その割付項目としては、年齢層（15 歳から 24 歳、25 歳から 64 歳までの 5 歳刻み、65 歳以上の 10 分類)、性別、地域（北海道・東北、南関東、北関東・甲信越・北陸、東海、近畿、中国・四国、九州・沖縄の 7 分類)、労働形態（正規・非正規)、所属している企業の上場状況（上場企業・非上場企業）を用いている。まず、労働形態および企業の上場状況により、表 1 のように基礎的な割付を行った。続いて 2009 年に実施された『労働力調査』(総務省) の

---

[5] 環境の変化として、回収率の低下、拒否率の増加、プライバシーや個人情報保護法への過剰反応等が挙げられる。さらに、サンプリングに用いる選挙人名簿等の利用制限もあるため、個人を対象とした調査は困難を極めている。

[6] 実際に、Kotulic and Clark (2004)は、情報セキュリティに関する実務家を対象としたアンケート調査の困難さの理由を指摘している。

[7] Couper (2000) は Web アンケート調査に関する問題を示すとともにその可能性について議論を行っている。

[8] アンケートの調査票については、ウェブサイト（http://www2.ipcku.kansai-u.ac.jp/~a084034/）に公開予定である。

地域別集計に従い、それぞれのサンプルについて年齢層、性別、地域による割付を行った[9]。

表 1：割付

	上場企業	非上場企業
正規	440	331
非正規	440	331

Web 調査は、一般的に、指定したサンプルサイズに達するまで実施されるため、郵送アンケート調査のように回収率が低くなることはない。本調査では、非上場企業の労働者のサンプル確保が難しかったために、最終的なサンプルサイズは 1268 となっており、これらのサンプルを用いて以下、分析を行っていく。

時として、技術やマネジメントによる情報セキュリティ対策は従業員の生産性や効率性を損なう過剰な（硬直的な）ものとなってしまうことや、逆に従業員が生産性や効率性を追求するために対策を回避しようとすることがある。これは、ヒトや組織の問題であり、いくら優れた技術でもっても解決することはほぼ不可能である。これらのヒトや組織の問題を起こさないためには、先行研究でも指摘されていたように、管理者および従業員（労働者）に対策をしようとする動機付けを行う必要がある。言い換えると、自発的に情報セキュリティ対策を行うためには、その必要性および重要性を理解させなければならない。そのために有効な手段が本稿で取り上げる情報セキュリティ教育である。このことは、学術的のみならず、実務的にも広く認識されている[10]。そのため、本稿では情報セキュリティ教育に対する意識に注目する[11]。

情報セキュリティ教育に対する意識に関する質問として、表 2 に挙げた 5 つの項目を取り上げる。これらの項目は一般的に情報セキュリティの教科書で主張されているものである。そして、表 2 の項目 A-3)～A-5)は、自発的に情報セキュリティ教育に参加する意欲があることを表す指標となっている。労働者はこれらの項目を 7 段階（「1．強くそう思わない」、「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」）で評価している。いずれの項目において評価が高くなるに従って、情報セキュリティ教育に対する意識が高いと判断することができる。そして、いずれの項目も情報セキュリティ（教育）の対策の観点からいずれも望

9 総務省「労働力調査」は以下のウェブサイトで閲覧することができる。
URL: http://www.stat.go.jp/data/roudou/index.htm

10 学術的には、先行研究として取り上げた上野・田中 (2007)や竹村・峰滝 (2010)において情報セキュリティ教育の意義について指摘され、また実務的には、情報処理推進機構（IPA）の情報セキュリティに関するウェブサイト（URL: http://www.ipa.go.jp/security/）や日本ネットワークセキュリティ協会教育部会 (2009)等について情報セキュリティ教育の必要性・重要性について指摘している。

11 情報セキュリティ教育に対する労働者の意識は、情報セキュリティ教育に対する理解がある個人が「基本的な情報セキュリティの理解を深めたい」、「情報セキュリティの脅威と対策について知識を得たい」や「最新の動向を知りたい」等と自発的に情報セキュリティを意識していると考えられ、情報セキュリティ対策の必要性および重要性を理解していると解釈することができる。

まれることであり、この項目から個人がこれらの点を認識しているかを調べることができる。なお、表 2 には情報セキュリティ教育への意識をはかる 5 つの項目の度数分布を示している。表の上段は相対度数、下段は行比率をそれぞれ表している。また、表 3 にはこれらの項目の基本統計量を与えている。

表 2　情報セキュリティ教育への意識

	低い＜－意識－＞高い						
	1	2	3	4	5	6	7
A-1) 定期的に情報セキュリティ教育は受けるべきである	12	33	70	399	473	222	59
	0.9%	2.6%	5.5%	31.5%	37.3%	17.5%	4.7%
A-2) 定期的でなくとも情報セキュリティ教育は受けるべきである	14	24	52	297	516	283	82
	1.1%	1.9%	4.1%	23.4%	40.7%	22.3%	6.5%
A-3) 情報セキュリティ教育の内容をもっと充実させてほしい	15	26	65	493	411	199	59
	1.2%	2.1%	5.1%	38.9%	32.4%	15.7%	4.7%
A-4) 情報セキュリティ教育の研究の機会をもっと増やすべきである	17	29	63	447	451	197	64
	1.3%	2.3%	5.0%	35.3%	35.6%	15.5%	5.0%
A-5) 自らが進んで、情報セキュリティについて学ぶべきである	14	29	60	449	460	187	69
	1.1%	2.3%	4.7%	35.4%	36.3%	14.7%	5.4%

表 3　情報セキュリティ教育への意識の基本統計量

	平均値	歪度	最頻値	標準偏差
A-1) 定期的に情報セキュリティ教育は受けるべきである	4.73	-0.383	5	1.099
A-2) 定期的でなくとも情報セキュリティ教育は受けるべきである	4.94	-0.594	5	1.106
A-3) 情報セキュリティ教育の内容をもっと充実させてほしい	4.65	-0.224	4	1.090
A-4) 情報セキュリティ教育の研究の機会をもっと増やすべきである	4.68	-0.341	5	1.109
A-5) 自らが進んで、情報セキュリティについて学ぶべきである	4.69	-0.266	5	1.095

表 2 と表 3 から、いずれの項目も情報セキュリティ教育に対する意識が中レベル（評価としては 4）より高くなっている労働者が大半を占めていることを読み取ることができる。このことより、意識として、情報セキュリティ教育の必要性および重要性を理解している労働者が多いと考えられる。次に、情報セキュリティ（対策）に関する具体的かつ身近な行動に関する質問として、表 4 にある 7 つの項目を取り上げる。表 4 の項目 B-1)～B-4) は対策しなければ情報漏洩をはじめとする情報セキュリティ被害につながりやすい行動、項目 B-5)は社会問題化している違法性のある行動、また項目 B-6)と B-7)は情報セキュリ

ティ教育に関する行動である。これらの項目は、情報セキュリティ教育や教科書で一般的に言われていることであり、情報セキュリティを理解していれば、実際に対策を行うもしくは不適切な行動をとらないことが期待されるものである。つまり、表 4 の項目 B-4)では「2. いいえ」が選ばれ、項目 B-4)を除く項目では「1. はい」が選ばれることが期待される。

表 4　情報セキュリティ（対策）に関する行動

	1. はい	2. いいえ
B-1) 自宅のパソコンはボット対策をしている	272	996
	21.5%	78.5%
B-2) 自宅のパソコンはウィルス対策ソフトを導入している	1084	184
	85.5%	14.5%
B-3) 自宅のパソコンは OS のアップデートなどがあれば、こまめに対応している	891	377
	70.3%	29.7%
B-4) 無承諾でアップロードされた音楽ファイル等の違法なコンテンツをダウンロードしたことがある	210	1058
	16.6%	83.4%
B-5) 自宅のパソコンにログインする時、パスワードを設定している	539	729
	42.5%	57.5%
B-6) 定期的、もしくは不定期で情報セキュリティ教育は受けている	312	956
	24.6%	75.4%
B-7) 自らが進んで、情報セキュリティについて学んでいる	270	998
	21.3%	78.7%

表 4 を見ると、項目 B-2)、B-3)と B-5)については期待されるように 70%以上の労働者が適切な行動をとっていることがわかる。一方で、残りの項目については適切な行動をとっている労働者の割合は必ずしも高いとはいえない。とりわけ、情報セキュリティ教育に関する行動である項目 B-6)と B-7)に関しては 25%よりも低い水準にとどまっており、情報セキュリティ教育を受けるまでに至っていない労働者が多いことがわかる。多くの労働者が適切な行動をとっている項目 B-2)、B-3)と B-5)は簡単に実施できる行動である一方で、項目 B-1)は情報セキュリティの脅威である「ボット」の認知が低いため、また、項目 B-5)はコンピュータの利便性を重視しているため、それらを実施している労働者の割合が高くなっていないと考えられる。

表 4 の情報セキュリティに関する行動に関する各項目は、必ずしも強制的に実施が義務づけられておらず、ある意味で自発的にとられるものである。一方で、近年、多くの組織で情報漏洩等を防止するために実施されている対策（禁止事項）がある。その中で、本稿では、表 5 に示した 4 つの項目（USB などのメディア媒体での顧客情報データの社外持出し、顧客情報データの電子メールへの添付、2 ちゃんねる等のサイトへのアクセス、紙媒体での顧客情報データの社外持出し）を取り上げる。これらの項目は情報セキュリティ管理者もしくはシステム管理者が情報セキュリティシステムや規定によりコントロールを

行っているものである。つまり、これらはある種、強制的に実施されている対策と見なすことができる[12]。

表 5　情報漏洩等を防止するために実施されている対策と行動

項目＼経験		C-1) メディア媒体での顧客情報データの社外持出し	
		経験あり	経験なし
メディア媒体での顧客情報データの社外持出し	全面的に禁止	74	420
	禁止されていない	95	139
		C-2) 顧客情報データの電子メールへの添付	
		経験あり	経験なし
顧客情報データの電子メールへの添付	全面的に禁止	46	407
	禁止されていない	79	149
		C-3) 職場での 2 ちゃんねる等のサイトへのアクセス	
		経験あり	経験なし
2 ちゃんねる等のサイトへのアクセス	全面的に禁止	45	531
	禁止されていない	150	183
		C-4) 紙媒体で顧客情報データの社外持出し	
		経験あり	経験なし
紙媒体での顧客情報データの社外持出し	全面的に禁止	51	436
	禁止されていない	80	149

表 5 から、約 63～68%の割合の企業でこれらの項目が全面的に禁止されていることがわかる。また、各項目に対応させる形で、それらの行動をこれまで経験したことがあるか否かをまとめたものである。表 5 から、組織で全面的に禁止されているか否かに関わらず、これらの行動をとった経験のある労働者の割合は 20%前後になっていることがわかる。さらに、組織で全面的に禁止されているにもかかわらず、問題のある行動をとっている労働者の割合は、項目 C-1)がもっとも多く約 15.0%、そして項目 C-2)、C-3)、C-4)と、順に約 10.2%、約 7.8%、約 10.5%となっている[13]。なお、第 3.3 節では、これらの組織で全面的に禁止されているにもかかわらず、問題のある行動をとっている労働者を対象にして分析を行う。

3．　分析

3．1．　Mann- Whitney の順位和検定

本節では、情報セキュリティ教育への意識と情報セキュリティ対策の観点から問題とな

[12] なお、表 5 では「(上長やシステム部門から許可を得る等）条件付きで可能となっている」や「わからない」と回答した個人を除いている。

[13] 組織で全面的に禁止となっているとしても、それを遵守していない労働者の中には例外的な許可をもらっている者も含まれているかもしれないが、アンケート調査においてそのようなケースに関する詳細な質問を行っていないため、その是非は不明である。

る行動の関係を Mann-Whitney の順位和検定によって分析する[14]。具体的には、表 4 および表 5 でそれぞれ取り上げた情報セキュリティ対策の観点から問題となる行動をとっているグループとそうでないグループに分け、表 2 の情報セキュリティ教育への意識が両グループ間で異なるか否かを統計的に調べる。ここでは、「情報セキュリティ対策の観点から問題となる行動が情報セキュリティ教育に対する意識の違いによって生じている」という仮説を立て、その検証を行う。

Mann-Whitney の順位和検定（Mann-Whitney の U 検定）は 2 つのグループ間の中央値の差異を調べる検定であり、データそのものではなく、小さい順に並べたデータの順位和を検定統計量（U）として用いる。なお、データに同一順位がある場合には、一般的に、平均順位を用いて計算する。これらの統計量から、標準偏差と平均値を用いて Z 値を計算する。U の分布は近似的に正規分布に従うとされるため、標準正規分布表から漸近有意確率を求める。

Mann-Whitney の順位和検定における帰無仮説は「2 つのグループ（情報セキュリティ対策の観点から問題となる行動をとっているグループとそうでないグループ）における情報セキュリティ教育への意識の中央値には差異がない」というものである。そして、本稿で期待される結果は、「情報セキュリティ教育への意識が高ければ、情報セキュリティ対策の観点から問題となる行動をとりにくい」ことを支持するものであり、情報セキュリティ対策の観点から問題となる行動をとっていないグループの中央値の方が他方のグループよりも高くなっていることを確認できるものである。Mann-Whitney の順位和検定の分析結果を示したものが表 6 と表 7 である。

３．２．　分析結果（1）

表 6 には、表 2 で取り上げた情報セキュリティ教育への意識と表 4 で取り上げた 7 つの情報セキュリティ（対策）に関する身近な行動の関係を分析した結果である。

例えば、行動項目 B-1)「自宅のパソコンはボット対策をしている」の意識項目 A-1)「定期的に情報セキュリティ教育は受けるべきである」に関しては、ボット対策をしているグループとそうでないグループにおける情報セキュリティ教育への意識に違いがあることを 1%有意水準で統計的に確認している。また、対策をしているグループとそうでないグループの平均ランクは、順に 685.54 と 620.56 となり、前者のグループの平均ランクが後者よりも高くなっている。同様に、多くのケースで、統計的に情報セキュリティ教育への意識の違いがあることを確認し、また、対策をしているグループの平均ランクは対策をしていないグループの平均ランクよりもいずれも情報セキュリティ教育への意識が高くなっていることも確認している。つまり、適切な行動をとっている労働者グループは情報セキュリティ教育への意識が高く、逆に、適切な対策を施していない労働者グループは情報セキュリティ教育への意識が低くなる傾向があることがわかる。しかしながら、行動項目 B-5)

[14] Mann-Whitney の順位和検定はノンパラメトリックな手法であり、データが正規分布に従っていることを必ずしも仮定せず、本稿で用いるような順序尺度のデータに利用することができるといった特徴がある。

表 6　Mann-Whitney 検定の結果（1）

行動項目	意識項目	平均ランク		Mann-Whitney の U	Z 値	漸近的有意確率
		1.はい	2.いいえ			
B-1	A-1)	685.54	620.56	121574.000	-2.717	0.007***
	A-2)	676.25	623.10	124099.000	-2.226	0.026**
	A-3)	676.72	622.97	123973.500	-2.257	0.024**
	A-4)	695.92	617.73	118750.000	-3.277	0.001***
	A-5)	712.19	613.28	114324.000	-4.152	0.000***
B-2	A-1)	650.54	539.99	82338.500	-3.966	0.000***
	A-2)	653.02	525.38	79650.500	-4.587	0.000***
	A-3)	651.61	533.70	81180.000	-4.250	0.000***
	A-4)	652.97	525.69	79707.000	-4.577	0.000***
	A-5)	652.36	529.29	80368.500	-4.433	0.000***
B-3	A-1)	667.29	557.01	138738.000	-5.135	0.000***
	A-2)	673.71	541.83	133017.500	-6.150	0.000***
	A-3)	656.97	581.38	147929.000	-3.536	0.000***
	A-4)	658.07	578.81	146957.000	-3.699	0.000***
	A-5)	676.81	534.51	130257.500	-6.651	0.000***
B-4	A-1)	688.76	594.38	167218.000	-4.753	0.000***
	A-2)	680.46	600.52	171694.000	-4.032	0.000***
	A-3)	678.28	602.13	172869.000	-3.852	0.000***
	A-4)	671.70	607.00	176415.500	-3.266	0.001***
	A-5)	669.89	608.33	177388.500	-3.112	0.002***
B-5	A-1)	566.83	647.93	96879.500	-3.071	0.002***
	A-2)	591.23	643.09	102003.000	-1.967	0.049**
	A-3)	597.86	641.77	103396.500	-1.670	0.095*
	A-4)	616.86	638.00	107385.500	-0.802	0.422
	A-5)	611.07	639.15	106169.000	-1.068	0.286
B-6	A-1)	792.73	582.86	99767.000	-9.208	0.000***
	A-2)	773.63	589.09	105728.500	-8.110	0.000***
	A-3)	679.79	619.72	135007.000	-2.647	0.008***
	A-4)	689.01	616.71	132129.500	-3.179	0.001***
	A-5)	707.02	610.83	126510.000	-4.236	0.000***
B-7	A-1)	757.39	601.25	101549.000	-6.511	0.000***
	A-2)	746.39	604.23	104520.500	-5.938	0.000***
	A-3)	748.01	603.79	104083.500	-6.041	0.000***
	A-4)	728.62	609.04	109316.500	-4.998	0.000***
	A-5)	810.60	586.86	87182.000	-9.366	0.000***

***: p<1%, **: p<5%, *: p<10%

「無承諾でアップロードされた音楽ファイル等の違法なコンテンツをダウンロードしたことがある」の意識項目 A-4)「情報セキュリティ教育の研究の機会をもっと増やすべきである」と A-5)「自らが進んで、情報セキュリティについて学ぶべきである」に関しては、両グループの情報セキュリティ教育への意識の違いを統計的に確認することができない。これは、必ずしも情報セキュリティ教育への意識の高さが違法性のある行動（違法行為）をとどまらせることと関係ないことを意味していると解釈することができる。言い換えると、違法性のある行動をとることに関しては、情報セキュリティ教育ではなく他の要因が働いていることが考えられる。

３．３．　分析結果 (2)

表 7 は、表 5 で取り上げた全面的に禁止されているにもかかわらず、問題のある行動をとっている労働者とそうでない労働者の情報セキュリティ教育への意識に違いがあるか否かを分析した結果を示している。

表 7　Mann-Whitney 検定の結果 (2)

行動項目	意識項目	平均ランク		Mann-Whitney の U	Z 値	漸近的有意確率
		1.経験あり	2.経験なし			
C-1	A-1)	229.84	250.61	14233.500	-1.200	0.230
	A-2)	227.99	250.94	14096.500	-1.330	0.184
	A-3)	241.09	248.63	15065.500	-0.437	0.662
	A-4)	241.32	248.59	15082.500	-0.421	0.674
	A-5)	230.93	250.42	14314.000	-1.133	0.257
C-2	A-1)	159.37	234.64	6250.000	-3.832	0.000***
	A-2)	152.65	235.40	5941.000	-4.230	0.000***
	A-3)	168.40	233.62	6665.500	-3.336	0.001***
	A-4)	179.09	232.42	7157.000	-2.720	0.007***
	A-5)	190.03	231.18	7660.500	-2.105	0.035**
C-3	A-1)	199.08	296.08	7923.500	-3.940	0.000***
	A-2)	189.21	296.91	7479.500	-4.374	0.000***
	A-3)	240.89	292.53	9805.000	-2.084	0.037**
	A-4)	239.89	292.62	9760.000	-2.126	0.033**
	A-5)	226.97	293.71	9178.500	-2.707	0.007***
C-4	A-1)	235.38	245.01	10678.500	-0.482	0.630
	A-2)	215.48	247.34	9663.500	-1.599	0.110
	A-3)	241.41	244.30	10986.000	-0.145	0.885
	A-4)	220.99	246.69	9944.500	-1.288	0.198
	A-5)	217.89	247.05	9786.500	-1.466	0.143

***: p<1%, **: p<5%, *: p<10%

例えば、行動項目 C-2)「顧客情報データの電子メールへの添付」の意識項目 A-1)「定期的に情報セキュリティ教育は受けるべきである」に関しては、顧客情報データの電子メールへの添付が組織で全面的に禁止されているにもかかわらず、過去に顧客情報データを電子メールに添付した経験があるグループとないグループにおける情報セキュリティ教育への意識に違いがあることを 1%有意水準で統計的に確認している。また、経験があるグループの平均ランクは 159.37 で、経験がないグループの平均ランクである 234.64 よりも小さな値をとっている。同様の傾向が、行動項目 C-2)「顧客情報データの電子メールへの添付」と C-3)「職場での 2 ちゃんねる等のサイトへのアクセス」の全ての意識項目において確認されている。この結果は、情報セキュリティ教育への意識が高ければ、問題のある行動を起こしにくくなる（対策を遵守する）可能性があることを示唆している。
一方で、行動項目 C-1)「メディア媒体での顧客情報データの社外持出し」と C-4)「紙媒体で顧客情報データの社外持出し」の全ての意識項目における全ての情報セキュリティ教育への意識項目については経験があるグループとないグループの意識の違いを統計的に確認することができない。つまり、組織で全面的に顧客情報データの社外持出しが禁止されているにもかかわらず、問題ある行動をとっている労働者とそうでない労働者の情報セキュリティ教育への意識には違いがないことをこの結果は意味している。このことは、Albrechtsen (2007)や竹村・田中・松浦 (2010)で指摘しているように、労働者が業務の効率性・生産性を情報セキュリティ対策よりも優先しようとしていることが一つの要因となっていることが考えられる。その意味において、顧客情報をはじめとする秘密情報の持出しについてはもっと労働者に理解を促すような更なる策を講じる必要がある。

４．　情報セキュリティ教育をサポートする取組

情報セキュリティ分野において日本政府による個人に対するセキュリティ教育を強化する動きが見られる。例えば、第 1 次情報セキュリティ基本計画においては「IT 利用に不安を感じる」とする個人を限りなくゼロにすることが目標とされ、情報を管理する側に係る対策に取組みの重点がおかれていた。しかし、第 2 次情報セキュリティ基本計画においては、これに加えて、「情報を預ける側の主体の意識や情報を預けるに際しての行動」を啓発することの重要性が指摘され、学校や地域における情報モラル等に関する情報セキュリティ教育の推進や一般利用者のセキュリティレベルを効果的に上げるための取組の実現が目指されている。情報セキュリティ教育に関する具体的な取組みの一例として、総務省、文部科学省及び関係公益法人等の協力の下、主に児童の保護者・教職員向けにインターネットの安心・安全に向けた講座を全国規模で行う「e-ネットキャラバン」が 2006 年 4 月から実施されていることが挙げられる。また、国民一般に対して、インターネットと情報セキュリティに関する知識の習得に役立ち、また利用方法に応じた情報セキュリティ対策を講じるための基本的な情報を提供することを目的とした総務省のウェブサイト「国民のための情報セキュリティサイト」[15]が、2003 年 3 月以来開設されている。更に、総務省と経済産業省の連携によるボット対策プロジェクトとして、「サイバークリーンセンター」が 2006 年 12 月に開設され、ボット感染者の減少・撲滅を目指したボット対策情報の発信等

[15] URL: http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm

が行われている。このような取組の積み重ねを通じて、情報セキュリティに関する国民の意識が高揚し、第 2 次情報セキュリティ基本計画が基本理念として掲げる「成熟した情報セキュリティ先進国の実現」に向けた基盤が形成されることが期待される。この他にも、IPA が定期的に国内各地で行っている「情報セキュリティセミナー」や情報セキュリティに関する講習会等は、労働者が情報セキュリティに対する意識を高める上で、一定の効果が期待できるものと考えられる。以上のような施策は、本稿の分析結果から見ても有意義で望ましいものであり、今後の更なる充実が期待される。なお、この情報セキュリティ教育をサポートする政府の取組については、竹村・海野 (2009)が詳しいので参照されたい。

５．　まとめと今後の展望

本稿では、日本の労働者を対象に行った Web アンケート調査によって収集したミクロデータを用いて、情報セキュリティ教育に対する意識に注目し、それと実際にとっている行動の関係について定量分析を試みている。その結果、概して、適切な行動をとっている労働者グループの方が問題ある行動をとっている労働者グループよりも、情報セキュリティ教育への意識の方が高くなっていることを確認している。しかしながら、違法性のある行動をとることに関しては、情報セキュリティ教育に対する意識でははかることができなかった。次に、組織で情報漏洩等の防止のために全面的に禁止されている事項に関して、問題のある行動をとっている労働者グループとそうでない労働者グループの情報セキュリティ教育に対する意識に違いがあるかについても検証している。その結果、顧客情報データの社外持出しに関して意識の差があることを統計的に確認することができなかったものの、顧客情報データの電子メールへの添付などの問題のある行動については意識の違いがあることを明らかにするとともに、後者の情報セキュリティ教育に対する意識の方が前者よりも高くなっていることを確認している。そして、情報セキュリティ教育への意識が高ければ、問題のある行動を起こしにくくなる（対策を遵守する）可能性について示唆を与えている。

さらに、政府としての情報セキュリティ教育をサポートする取組（前述の「e-ネットキャラバン」や IPA の「情報セキュリティセミナー」等）を紹介し、それが有効な施策であることを指摘するとともに、それらは労働者が情報セキュリティに対する意識を高める上で、一定の効果が期待される可能性があることについて言及している。

最後に、今後の研究の展望を示す。第 1 節でも触れたように、情報セキュリティの経済学における実証分析はまだ十分な蓄積が進んでいない。そのため、労働形態や心理的状態、個人属性等をはじめとして様々な角度から労働者の情報セキュリティに対する意識と実際に彼らがとっている行動の関係について更なる分析を行う必要がある。これは、学術的発展および実務的にも有益な情報を与えることにつながると考えられる。本稿もまた学術的発展の一助になることを期待したい。

謝辞

本稿は、文部科学省の科学研究費補助金交付課題「企業と個人の情報セキュリティ対策に関する実証分析」（課題番号 22730241・若手研究（B）・研究代表者 竹村敏彦）および財団法人村田学術振興財団研究助成の研究助成課題「企業の戦略的情報セキュリティ対

策・投資に関する実証分析」（研究代表者 竹村敏彦）の助成を受けて行った研究成果である。また、匿名の査読者から有益なコメントをいただいた。記して感謝する。残る誤りは全て筆者の責に帰すものである。

参考文献

[1] Albrechtsen, E., A Qualitative Study of Users' Views on Information Security. Computer and Security, Vol.26, pp276-289, 2007, USA

[2] Albrechtsen, E. and Hovden, J., The Information Security Digital Divide between Information Security Managers and Users. Computer and Security, Vol.28, pp476-490, 2009, USA

[3] Anderson, R. and Moore, T., Information Security: Where Computer Science, Economics and Psychology Meet. Philosophical Transactions of the Royal Society, Vol.367, pp2717-2727, 2009, USA

[4] Camp, L.J., The State of Economics of Information Security. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.6038&rep=rep1&type=pdf, 2006, USA

[5] Chan, S.E. and Ho, C.B., “Organizational Factors to the Effectiveness of Implementing Information Security Management” Industrial Management & Data Systems, Vol.106, No.3, pp345-361, 2006, USA

[6] Couper, M.P., Web Surveys: A Review of Issues and Approaches, Public Opinion Quarterly, Vol.64, pp464-494, 2000, USA

[7] Kotulic, A.G. and Clark, J.G., Why There Aren't More Information Security Research Studies, Information and Management, Vol.41, pp597-607, 2004, USA

[8] Solow, R. M., We'd Better Watch Out. New York Times Book Review, July 12, p36, 1987, USA

[9] 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, Vo.2, No.1, pp20-26, 2010, USA

[10] Takemura, T., Tanaka, H. and Matsuura, K., Awareness Gaps on Effects of Information Security Measure between Managers and Employees: An Empirical Study Using Micro Data Collected from Web-based Survey. Short Paper Proceedings of the Fourth IFIP WG 11.11 International Conference on Trust management, pp25-32, 2010, Japan

[11] 上野景真・田中秀幸「情報セキュリティ投資と企業価値に関する実証分析：インタンジブル・アセットとしての情報セキュリティ」『経済政策ジャーナル』Vol.4、No.2、pp43-46、2007

[12] 日本ネットワークセキュリティ協会教育部会『情報セキュリティプロフェッショナル教科書』ASCII、2009

[13] 実積寿也『IT 投資効果メカニズムの経済分析: IT 活用戦略と IT 化支援政策』九州大学出版会、2005

[14] 篠崎彰彦『情報技術革新の経済効果－日米経済の明暗と逆転－』日本評論社、2003

[15] 竹村敏彦『情報通信技術の経済分析―企業レベルデータを用いた実証分析－』多賀出版、2008
[16] 竹村敏彦・海野敦史「インターネット利用者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』H21 年 8 月号、pp13-21、2009
[17] 竹村敏彦・田中秀幸・松浦幹太「労働者の情報セキュリティ対策に対する意識と行動に関する研究」関西大学、Mimeo、2010
[18] 竹村敏彦・峰滝和典「情報セキュリティマネジメントとその効果に関する実証分析－教育・情報共有をサポートする政策の必要性－」『経済政策ジャーナル』Vol.7、No.2、pp46-49、2010
[19] 田中秀幸・松浦幹太「情報セキュリティ・マネジメントの制度設計」『日本セキュリティ・マネジメント学会・特定非営利活動法人ネットワークセキュリティ協会主催 Network Security Forum 2003』、pp1-17、2003
[20] 塚原康博「人間の行動動機と労働者の行動」『行動経済学の理論と実証』（千田亮吉・塚原康博・山本昌弘 編著）勁草書房、pp50-71、2009
[21] 星野崇宏「Web 調査の偏りの補正: 行動経済学における調査研究への適用」RCSS Discussion Paper Series、No.97、2010
[22] 労働政策研究・研修機構「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、2005