RCSS ディスカッションペーパーシリーズ ISSN-1347-636X
第 85 号　2009 年 5 月
Discussion Paper Series
No.85 May, 2009

労働者の情報セキュリティ意識に関する研究

竹村敏彦・峰滝和典・今川拓郎

RCSS

文部科学大臣認定　共同利用・共同研究拠点
関西大学ソシオネットワーク戦略研究機構
関西大学ソシオネットワーク戦略研究センター
（文部科学省私立大学学術フロンティア推進拠点）

Research Center of Socionetwork Strategies,
“Academic Frontier” Project for Private Universities, 2003-2009
Supported by Ministry of Education, Culture, Sports, Science and Technology
The Research Institute for Socionetwork Strategies,
Joint Usage / Research Center, MEXT, Japan
Kansai University
Suita, Osaka, 564-8680 Japan
URL: http://www.rcss.kansai-u.ac.jp
http://www.kansai-u.ac.jp/riss/index.html
e-mail: rcss@jm.kansai-u.ac.jp
tel: 06-6368-1228
fax. 06-6330-3304

労働者の情報セキュリティ意識に関する研究

竹村敏彦[*]・峰滝和典[†]・今川拓郎[‡]

概要

本研究では、労働形態、所属している組織属性や、個人属性などの違いによって、労働者自身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が異なるか否かを調べることを目的とし、ノンパラメトリックな手法に基づく分散分析をおこなっている。その結果、概して、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された。そして、これらの結果を踏まえて、企業の効率的な情報セキュリティ対策につながるモチベーションをも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の必要性を主張している。

キーワード：情報セキュリティ、労働者、分散分析、情報セキュリティ教育
JEL：C13, D78, L86

[*] 関西大学ソシオネットワーク戦略研究機構・助教 takemura@rcss.kansai-u.ac.jp
関西大学ソシオネットワーク戦略研究センター・研究員
[†] 関西大学ソシオネットワーク戦略研究機構・統計分析主幹 minetaki@rcss.kansai-u.ac.jp
関西大学ソシオネットワーク戦略研究センター・研究員
[‡] 総務省情報通信国際戦略局情報通信経済室・室長
関西大学ソシオネットワーク戦略研究センター・研究員

A Research on Worker's Awareness to Information Security

Toshihiko Takemura*, Kazunori Minetaki†, Takuro Imagawa‡

Abstract

In this paper, we examine whether or not there are differences of the workers' awareness to information security based on various attributes by using analysis of variance based on non-parametric method. As a result, it is found that the workers' awareness to information security is different by attributes such as some organization attributes and the information security educating situation. Then, we suggest the necessity of enhancing information security education and introducing firm system such as authority handover system, and/or stock option system in order to motivate to execute the efficient information security countermeasures.

Keywords: Information security, Workers, Variance of Analysis, Information Security Education

JEL : C13, D78, L86

* Assistant professor, the Research Institute for Socionetwork Strategies (RISS), and Research Fellow, Research Center of Socionetwork Strategies (RCSS), Kansai University, E-mail:takemura@rcss.kansai-u.ac.jp

† Senior Researcher for Statistical Analysis, RISS, and Research Fellow, RCSS, Kansai University, E-mail: minetaki@rcss.kansai-u.ac.jp

‡ Information and Communications Policy Bureau, the Ministry of Internal Affairs and Communications, and Research Fellow, RCSS, Kansai University

1　はじめに

高度情報化社会において、インターネットは個人の生活やビジネス形態を変貌させたのは揺るぎない事実である。とりわけ、IT経済学では、IT投資が企業の経営パフォーマンス（生産性や効率性）の向上、さらに国内総生産や成長率の向上に貢献していることを実証分析の結果から明らかにしている（篠崎 [2003]、実積 [2005]、竹村 [2008]）。言い換えると、IT投資やITの事業への導入は多くの正の経済効果をもたらす[1]。また、近年、情報を有効活用するために情報のデジタル化が進められ、その効果も大きいものであると予想される。

高度情報化社会では、このような正の経済効果について注目されることがこれまで多かった。しかしながら、IT化やデジタル化、さらにユビキタス化が進むにつれて、個人や企業は深刻な問題に直面することになった。その 1 つが情報セキュリティに関する問題であり、本研究ではこの問題を取り上げる[2]。ブロードバンドの普及および情報の高価値化とともに、情報セキュリティインシデント（不正アクセス、マルウェアやフィッシングなど）による被害はビジネスに大きな打撃を与えるものとなっている。特に、ネットワークなどを通じて流出した個人情報や機密情報の量は、従来の情報漏洩と比べて、膨大なものとなっている（日本ネットワークセキュリティ協会 [2008]）。これらの情報セキュリティインシデントによる被害を防護するために、多くの企業は情報セキュリティ対策を講じている。情報セキュリティに関する技術的な側面からの研究（暗号化技術やセキュアネットワークなど）の蓄積は古くから進んでいるが、経済学や経営学の側面からの情報セキュリティ対策・投資に関する研究は、国内外問わずに、2000 年頃まであまり進んでいなかった。特に、情報セキュリティに関する実証分析はあまりおこなわれてこなかった。その理由は、データがなかったことや、たとえデータが存在していても利用できなかったことが挙げられる。それゆえに、情報セキュリティの経済学（Economics of Information Security）の実証分析はまだ萌芽状態にあり、その役割からも早急に、研究蓄積をおこなっていく必要がある。

近年、日本では、総務省や経済産業省、警察庁、IPA、JPCERT/CC、JNSAなどがこれらのデータの蓄積をおこなっており、それらのデータを用いた研究も進められつつある。たとえば、Tanaka et al. [2005]やLie et al. [2007]などは経済産業省の情報処理実態調査のデータを用いてこれらの実証分析をおこなっている。この他にも、独自にデータを蓄積した研究もいくつか存在している。Takemura, et al. [2009] や竹村・峰滝 [2009] は独自に実施したアンケート調査によって収集したデータを用いて実証分析をおこなっている[3]。これらの研究は企業を対象におこなったものである。もちろん、技

---

[1] Brynjolfsson [2004]は ICT 投資が生産性の向上をもたらしやすい組織（デジタル組織）について主張している。このことからも、ICT 投資をおこなえば、それがすぐに生産性向上につながるとはいえないといった議論もある。

[2] この他にも、デジタルデバイドなどの問題もある。

[3] この調査結果は、将来的に企業や個人を特定できるような情報を除き、クリーニングした

術やマネジメントに関する情報セキュリティ対策・投資の効果については、企業や事業所のデータを用いて分析することで十分である。本研究は、これらの研究をさらに一歩進めたもので、労働者の情報セキュリティおよびその対策への意識を知る必要があると考える。それは、情報セキュリティの性質により、たとえ組織的に対策をしていたとしても、これらを構成している労働者の意識が低ければ、組織の情報セキュリティのレベルは低くなってしまうためである。

本研究の目的は、労働形態、所属している組織属性や、個人属性などの違いによって、労働者自身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が異なるか否かを調べることにある。これを調べることによって、効率的な対策について議論することが可能となる。それゆえに、この研究は学術的のみならず、実務的、政策的な意義をもっている。

本研究の構成は以下の通りである。次節では本研究で用いるアンケート調査の概要について簡単に説明する。第 3 節においては、分析手法とその分析結果を示し、その考察をおこなう。そして、最後の節にて、結論と今後の課題について述べる。

2　アンケート調査の概要

第 1 節でも簡単に触れたが、情報セキュリティ対策・投資に関して公表され、容易に利用できるデータベースはほとんどないのが現状である。また、研究内容の特性から、集計されたデータではなく、個票データが必要となる。そのため、われわれは、2009 年 3 月に、労働者の情報セキュリティに関する意識およびその対策状況の把握を目的として、2 年以上勤労している労働者を対象「労働者の情報セキュリティおよびその対策に関する意識調査」（Webアンケート形式）をおこなった[4]。サンプルサイズは 600 件であり、サンプルの割付は労働形態と上場の有無の 2 軸で表 1 のようにおこなった。

形で、関西大学ソシオネットワーク戦略研究機構（The Research Institute for Socionetwork Strategies, Kansai University）に一定の手続きを経ることによって利用可能となる予定である。詳細については、以下の URL を参照されたい。
http://www.kansai-u.ac.jp/riss/shareduse/database.html

[4] 近年、ウェブアンケート調査結果を用いた研究が盛んにおこなわれている。しかしながら、この調査法にはいくつかの克服すべき統計に関する問題などがある。本研究ではこれらについて綿密に議論することを避けているが、これらを全く無視して分析をおこなっていないことをことわっておく。なお、ウェブアンケート調査と他の社会調査の比較をおこなっているものに、大隅 [2002]などがある。また、新たな試みとして、星野 [2007]などは両者の調整をおこなうとったこともおこなわれている。このような研究に今後、期待したい。

表 1　サンプルの割付

上場の有無 / 労働形態	上場企業	非上場企業
正規	200	200
非正規	100	100

表 2 には、労働者の情報セキュリティ意識に関する指標の基本統計量を示している。本研究では、大別して 4 種類（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）でもって情報セキュリティへの意識を考える。いずれも 5 段階（1~5）の質的データ（順序尺度）である。なお、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ようにしている[5]。

表 2　労働者の情報セキュリティ意識に関する指標

	変数	内容	平均	標準偏差
個人情報への意識	X1	個人情報へのアクセス（17-2）	3.72	0.986
対策への意識	X21	ウィルス対策なしの PC 利用（17-5）	4.12	0.960
	X22	チェーメール（17-6）	4.31	0.911
	X23	技術対策のみ（29-8）	3.70	0.899
	X24	教育不必要（29-11）	3.91	0.830
	X25	自己マネジメント意識（19-2）	3.64	0.632
モラル	X31	私用メール（17-11）	3.35	0.941
	X32	ルール違反（17-8）	3.78	1.019
インターネットへの意識	X41	インターネット全般に関する安全性の理解（17-15）	3.67	0.823
	X42	加害者になる可能性（17-17）	2.85	0.894
	X43	被害者になる可能性（17-18）	3.42	0.778

表 3 には、大別して 3 種類（労働形態、所属している組織の属性、個人属性）でもって分析で用いるカテゴリーに関する情報を示している。

[5] 表 3 はもともとの質問票から若干加工している。一部の質問項目において意識の順番が逆になっていたものがあったために、それを全て統一している。

表 3　カテゴリーに関する情報

	内容	説明
労働形態	正規・非正規	1　正規　0　非正規
所属している組織の属性	従業員数	1　9人以下、2　10～49人　3　50～99人　4　100～299人　5　300～999人　6　1,000～2,999人　7　3,000～4,999人　8　5,000～9,999人　9　10,000～99,999人　10 100,000～149,999人　11 150,000人以上
	インフラ度	1　ほとんどない　2　少ない　3　他の業種に比べると高い　4　事業の性質上極めて高い
	禁止事項	USB などの媒体での顧客情報データの社外持出 顧客情報データの電子メールへの添付 紙媒体での顧客データの社外持出 ノートパソコンの社外持出 持ち込みパソコンの社内 LAN 接続 （1　全面禁止　2　条件付きで可能　3　全く禁止されていない）
	モチベーション	権限移譲（1　導入済 0　未導入） ストックオプション（1　導入済 0　未導入） 従業員持ち株制度（1　導入済 0　未導入） 分社化（1　実施済 0　未実施）
	上場の有無	1　上場企業　0　非上場企業
個人属性	年齢層	1　20 代　2　30 代　3　40 代　4　50 代　5　60 代以上
	インターネット歴	1　1 年未満　2　1～2 年未満　3　2～3 年　4　4～5 年　5　6～7 年　6　8～9 年　7　10 年以上
	地域	1　東京　2　北海道・東北　3　関東（東京除く）4　北陸・甲信越　5　東海　6　近畿　7　中国　8　四国　9　九州・沖縄
	情報セキュリティ教育	1　研修や大学教育で教わった　0　誰からも教わっていない

3　分析結果

3.1　分析手法

ここ数十年の情報セキュリティインシデント被害に関する事例から、労働形態や組織によって意識の違いが指摘されている。しかしながら、これらについて定量的な検証・検討がこれまでほとんどおこなわれてこなかった。本研究では、これらについて、以下の 3 点の仮説に基づいて統計的に検証をおこなう[6]。

[6] 同様のフレームワークにて、インターネット利用者を対象に分析をおこなっているものと

1) 労働形態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

2) 所属している組織の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

3) 労働者自身の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

これらの仮説は、高度情報化社会において必要となる性質、言い換えると理想的な社会を表わしている。なお、本研究では、表 2 における所属している組織の属性の「インフラ度」についてのみ差異の存在を期待するものの、表 2 におけるそれ以外の項目については差異がないことを期待する。これは、Takemura et al. [2009]でも言及されているように、インフラ企業は一般企業よりもセキュリティのレベルが高く設定される必要があり、そこに属している労働者もまた同様に、高い意識をもっている必要があると考えるためである。

これらの仮説を検証するために、分散分析をおこなう。分散分析では、カテゴリーごとに平均値や中央値が異なるか否かを知ることができる。

3.2 分析結果

分散分析をおこなう前に、データが正規分布に従っているかについて検定する必要がある。正規性の検定は様々あるが、信頼の高いものとして、Kolmogorov-Smirnov の正規性の検定や Shapiro-Wilk 検定がある。これらの検定では、帰無仮説が「データは正規分布に従わない」である。そのため、もし有意確率が 5%未満であれば、帰無仮説を棄却できず、「データは正規分布に従わない」と判断する。逆に有意でないときは、帰無仮説を棄却でき、「データは正規分布に従わないとはいえない（正規分布に従う）」と判断する。

表 4 には、本研究で用いるデータ（労働者の情報セキュリティ意識に関する指標）に関する Kolmogorov-Smirnov の正規性の検定および Spapiro-Wilk 検定の結果を示している。これを見てわかるように、帰無仮説を棄却することができず、本研究で用いるデータは正規分布に従っていないと判断できる。そのために、そこで一般的な t 検定や Tukey 検定といったパラメトリックな手法で検定をおこなうことができない。そこで、本研究ではノンパラメトリックな手法によって、カテゴリーごとの中央値の差の有無について見ていく。

して竹村・海野 (2009)がある。彼らの分析結果も本稿と類似した結果を得ている。

表 4　正規性の検定

	Kolmogorov-Smirnov の正規性の検定 (探索的)[a]			Shapiro-Wilk		
	統計量	自由度	有意確率.	統計量	自由度	有意確率.
X1	.204	600	.000	.883	600	.000
X21	.248	600	.000	.807	600	.000
X22	.315	600	.000	.741	600	.000
X23	.285	600	.000	.861	600	.000
X24	.261	600	.000	.851	600	.000
X25	.280	600	.000	.771	600	.000
X31	.212	600	.000	.898	600	.000
X32	.245	600	.000	.866	600	.000
X41	.249	600	.000	.868	600	.000
X42	.279	600	.000	.870	600	.000
X43	.310	600	.000	.828	600	.000

a. Lilliefors 有意確率の修正

ノンパラメトリックな手法として、2 カテゴリーであれば、Mann-Whitneyの順位和検定（Mann-WhitneyのU検定）やWilcoxonの順位和検定、3 カテゴリー以上であれば、Kruskal-Wallis検定などがあり、本研究ではこれらの手法を用いて分散分析をおこなう。ノンパラメトリックな手法は、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、本研究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。Mann-Whitneyの順位和検定（Mann-WhitneyのU検定）やWilcoxonの順位和検定における帰無仮説は「2 つのカテゴリーの中央値に差異はない」であり、またKruskal-Wallis検定における帰無仮説は「それぞれ（3 つ以上）のカテゴリーの中央値に差異はない」である[7]。

表 5 から表 21 までが表 3 のカテゴリーに基づいて分析した結果である。なお、表 5、表 13 から表 17、表 21 は Mann-Whitney の順位和検定（Mann-Whitney の U 検定）と Wilcoxon の順位和検定の結果、またそれ以外は Kruskal-Wallis 検定の結果を示している。

[7] 一部のデータは順序性があるために、Jonckheere 検定（Jonckheere の傾向検定）を用いることも可能であるが、本研究では Kruskal-Wallis 検定のみをおこなっている。

表 5　正規・非正規（労働形態）

	Mann-Whitney の U	Wilcoxon の W	Z	漸近有意確率
X1	35464.000	115664.000	-2.369	.018**
X21	38085.500	58185.500	-1.022	.307
X22	37618.000	117818.000	-1.318	.188
X23	39164.500	59264.500	-.450	.653
X24	38112.000	58212.000	-1.014	.310
X25	35665.500	55765.500	-2.412	.016**
X31	34539.000	114739.000	-2.878	.004***
X32	37560.000	57660.000	-1.282	.200
X41	38329.000	118529.000	-.896	.371
X42	35304.500	55404.500	-2.570	.010***
X43	37695.500	117895.500	-1.277	.202

表 6　従業員数（組織属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	10.171	10	.426	600
X21	19.353	10	.036**	600
X22	7.461	10	.681	600
X23	28.206	10	.002***	600
X24	24.436	10	.007***	600
X25	27.260	10	.002***	600
X31	11.166	10	.345	600
X32	12.557	10	.250	600
X41	5.129	10	.882	600
X42	3.588	10	.964	600
X43	8.596	10	.571	600

表 7　インフラ度（組織属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	.882	3	.830	600
X21	7.033	3	.071*	600
X22	3.890	3	.274	600
X23	10.099	3	.018**	600
X24	13.588	3	.004***	600

X25	21.354	3	.000***	600
X31	8.283	3	.041**	600
X32	12.740	3	.005***	600
X41	1.923	3	.589	600
X42	7.386	3	.061*	600
X43	.712	3	.870	600

表 8　USB などの媒体での顧客情報データの社外持出（禁止事項・組織属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	5.218	2	.074*	526
X21	8.620	2	.013***	526
X22	11.431	2	.003***	526
X23	13.686	2	.001***	526
X24	14.055	2	.001***	526
X25	13.337	2	.001***	526
X31	19.504	2	.000***	526
X32	9.475	2	.009***	526
X41	1.199	2	.549	526
X42	8.271	2	.016**	526
X43	3.812	2	.149	526

表 9　顧客情報データの電子メールへの添付（禁止事項・組織属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	9.265	2	.010***	480
X21	3.051	2	.217	480
X22	7.207	2	.027**	480
X23	9.443	2	.009***	480
X24	10.785	2	.005***	480
X25	18.109	2	.000***	480
X31	25.132	2	.000***	480
X32	8.802	2	.012***	480
X41	2.313	2	.315	480
X42	4.261	2	.119	480
X43	.950	2	.622	480

表 10　紙媒体での顧客データの社外持出（禁止事項・組織属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	2.980	2	.225	505
X21	3.829	2	.147	505
X22	4.990	2	.083*	505
X23	11.820	2	.003***	505
X24	12.518	2	.002***	505
X25	16.769	2	.000***	505
X31	16.578	2	.000***	505
X32	6.838	2	.033**	505
X41	.929	2	.628	505
X42	4.807	2	.090*	505
X43	1.661	2	.436	505

表 11　ノートパソコンの社外持出（禁止事項・組織属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	1.797	2	.407	536
X21	1.933	2	.380	536
X22	9.818	2	.007***	536
X23	20.386	2	.000***	536
X24	16.544	2	.000***	536
X25	12.361	2	.002***	536
X31	21.524	2	.000***	536
X32	3.437	2	.179	536
X41	11.038	2	.004***	536
X42	5.934	2	.051**	536
X43	.061	2	.970	536

表 12　持ち込みパソコンの社内 LAN 接続（禁止事項・組織属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	3.964	2	.138	501
X21	18.866	2	.000***	501
X22	16.762	2	.000***	501
X23	26.487	2	.000***	501
X24	25.681	2	.000***	501

X25	19.483	2	.000***	501
X31	11.742	2	.003***	501
X32	8.362	2	.015**	501
X41	3.066	2	.216	501
X42	4.997	2	.082*	501
X43	.008	2	.996	501

表 13　権限移譲（モチベーション・組織属性）

	Mann-Whitney の U	Wilcoxon の W	Z	漸近有意確率
X1	23243.000	147494.000	-1.412	.158
X21	22525.000	146776.000	-1.925	.054**
X22	21261.500	145512.500	-2.872	.004***
X23	22454.500	146705.500	-1.989	.047**
X24	22577.500	146828.500	-1.902	.057*
X25	19224.000	143475.000	-4.312	.000***
X31	25233.500	30486.500	-.109	.913
X32	21978.000	146229.000	-2.254	.024**
X41	21393.000	145644.000	-2.694	.007***
X42	21689.000	145940.000	-2.547	.011***
X43	24323.500	148574.500	-.747	.455

表 14　ストックオプション（モチベーション・組織属性）

	Mann-Whitney の U	Wilcoxon の W	Z	漸近有意確率
X1	17242.500	156370.500	-1.501	.133
X21	14992.000	154120.000	-3.267	.001***
X22	17099.500	156227.500	-1.704	.088*
X23	17594.000	156722.000	-1.275	.202
X24	16477.500	155605.500	-2.137	.033**
X25	13925.000	153053.000	-4.262	.000***
X31	16859.000	155987.000	-1.806	.071*
X32	16128.000	155256.000	-2.354	.019**
X41	17168.000	156296.000	-1.598	.110
X42	18322.000	157450.000	-.721	.471
X43	16770.000	155898.000	-1.969	.049**

表 15　従業員持ち株制度（モチベーション・組織属性）

	Mann-Whitney の U	Wilcoxon の W	Z	漸近有意確率
X1	41087.000	116165.000	-.066	.947
X21	37306.000	112384.000	-2.056	.040**
X22	37548.500	112626.500	-1.999	.046**
X23	33701.000	108779.000	-3.986	.000***
X24	34978.500	110056.500	-3.301	.001***
X25	33944.500	109022.500	-3.986	.000***
X31	39394.500	114472.500	-.945	.344
X32	35443.000	110521.000	-2.987	.003***
X41	36805.000	111883.000	-2.329	.020**
X42	40843.000	115921.000	-.201	.841
X43	39986.000	115064.000	-.671	.502

表 16　　分社化（モチベーション・組織属性）

	Mann-Whitney の U	Wilcoxon の W	Z	漸近有意確率
X1	18594.000	156669.000	-.814	.416
X21	16979.500	155054.500	-2.061	.039**
X22	17399.000	155474.000	-1.805	.071*
X23	17530.000	155605.000	-1.656	.098*
X24	17925.000	156000.000	-1.350	.177
X25	14819.500	152894.500	-3.862	.000***
X31	16253.500	154328.500	-2.579	.010***
X32	16591.500	154666.500	-2.318	.020**
X41	17716.000	155791.000	-1.506	.132
X42	17771.000	155846.000	-1.495	.135
X43	17021.000	155096.000	-2.105	.035**

表 17　上場の有無（組織属性）

	Mann-Whitney の U	Wilcoxon の W	Z	漸近有意確率
X1	42968.000	88118.000	-1.001	.317
X21	41325.500	86475.500	-1.850	.064*
X22	42662.000	87812.000	-1.220	.223
X23	40955.500	86105.500	-2.053	.040**
X24	41180.500	86330.500	-1.935	.053**

X25	38824.000	83974.000	-3.240	.001***
X31	40548.000	85698.000	-2.212	.027**
X32	42635.000	87785.000	-1.171	.242
X41	42458.500	87608.500	-1.284	.199
X42	43891.000	89041.000	-.572	.567
X43	41988.500	87138.500	-1.573	.116

表 18　年齢層（個人属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	3.279	4	.512	600
X21	.537	4	.970	600
X22	1.643	4	.801	600
X23	1.609	4	.807	600
X24	10.541	4	.032**	600
X25	2.149	4	.708	600
X31	5.872	4	.209	600
X32	4.268	4	.371	600
X41	3.034	4	.552	600
X42	6.895	4	.142	600
X43	3.199	4	.525	600

表 19　インターネット歴（個人属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	5.023	6	.541	600
X21	7.293	6	.295	600
X22	8.829	6	.183	600
X23	4.523	6	.606	600
X24	7.522	6	.275	600
X25	4.974	6	.547	600
X31	13.168	6	.040**	600
X32	12.914	6	.044**	600
X41	11.009	6	.088*	600
X42	1.516	6	.958	600
X43	8.185	6	.225	600

表 20　地域（個人属性）

	χ2 乗	自由度	漸近的有意確率	サンプルサイズ
X1	13.830	8	.086*	600
X21	6.423	8	.600	600
X22	7.013	8	.535	600
X23	5.240	8	.732	600
X24	8.200	8	.414	600
X25	5.090	8	.748	600
X31	14.317	8	.074*	600
X32	6.418	8	.600	600
X41	14.713	8	.065*	600
X42	3.462	8	.902	600
X43	16.105	8	.041**	600

表 21　情報セキュリティ教育（個人属性）

	Mann-Whitney の U	Wilcoxon の W	Z	漸近有意確率
X1	44725.500	83785.500	-.027	.979
X21	39309.000	78369.000	-2.761	.006***
X22	41111.500	80171.500	-1.918	.055*
X23	32248.500	71308.500	-6.377	.000***
X24	33323.500	72383.500	-5.817	.000***
X25	32583.000	71643.000	-6.415	.000***
X31	42892.000	81952.000	-.940	.347
X32	39031.000	78091.000	-2.853	.004***
X41	40417.000	79477.000	-2.210	.027**
X42	44380.500	83440.500	-.206	.837
X43	44405.500	83465.500	-.196	.845

これらの結果を見てわかるように、概して、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みられる。

まず、労働形態の違いよって、X1、X25、X31 および X42 の項目の中央値に差異が認められた（表 5 参照）。しかしながら、それ以外の項目では、各項目の中央値に有意な差異は認められなかった。労働形態に関しては、Mann-Whitney 検定をおこなっているので、表 5 と各統計量を用いることで、正規と非正規のどちらの情報セキュリティ意識が高いかについて議論することができる。しかしながら、各項目で中央値の大小が

異なるものとなっており、正規と非正規でどちらの情報セキュリティ意識が高いかについて、一概に、断言することはできない。それゆえに、更なる分析が必要である。

次に、所属する組織属性（表 6 から表 17）について見てみると、少なくともいくつかの項目で中央値に差異が認められた。特徴として、全体的に対策への意識の差があることがわかる。また、項目としても、禁止事項およびモチベーションにおいて差異が確認されるケースが多い。所属している組織属性における禁止事項およびモチベーションでは、多くのケースで差異が確認された。これらの結果について見ていくと、Mann-Whitney 検定をおこなった表 13 から表 16 とそれぞれの統計量から、個人にモチベーションをもたせる企業システムをもつ組織に属している労働者の方がそうでない組織に属している労働者よりも、情報セキュリティ意識が高くなっていることがわかった。このことから、本研究で取り上げたようなモチベーションをもたせる企業システムは、ICT 化のみならず、情報セキュリティへの意識向上に寄与しているといえる。また、表 17 とそれぞれの統計量から、上場の有無によって対策への意識が上場企業の労働者の方が非上場企業の労働者よりも高くなっていることがわかった。所属している組織属性である従業員やインフラに関して、対策への意識にも差異があることがわかった。さらに、Kruskal-Wallis 検定をおこなった表 8 から表 12 から、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）組織において、情報セキュリティ意識に違いがあることがわかった。

さらに、個人属性（表 18 から表 21）について見てみると、情報セキュリティ教育（表 21 参照）を除く項目は、他のカテゴリーと比較して、有意差が確認されるケースが少なくなっていることがわかる。情報セキュリティ教育に関しては主として、対策への意識の差があることがわかる。個人属性においては、表 21 とそれぞれの統計量から、情報セキュリティ教育を受けた労働者は受けていない（独学も含む）労働者よりも情報セキュリティ意識が高くなっていることがわかった。この意味においても、情報セキュリティ教育を充実させていく必要がある。

概して、第 3.1 節で立てた 3 つの仮説（1）労働形態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、2）所属している組織の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、3）労働者自身の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）はいずれも肯定できない。そのために、これらの差異がないような状態にするための企業としての対策および政府としての政策について今後議論していく必要がある。

3.3　政策的含意

情報セキュリティ政策のみならず、情報通信技術（ICT）に関する議論全般において、教育の必要性および重要性はしばしば指摘されている。例えば、ICT 分野の総合的な国家戦略である「IT 新改革戦略」（2006 年 1 月 19 日 IT 戦略本部決定）においては、情

報教育の見直しの必要性についての言及がある。そして、情報セキュリティ分野においても、実際に、政府において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の一例として、総務省、文部科学省およ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」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm）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、前述の「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。

このほかにも、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、インターネット利用者が情報セキュリティおよびその対策への意識を高めるうえで、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、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。

4　結論と今後の課題

本研究では、労働形態、所属している組織属性や、個人属性などの違いによって、労働者自身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が異なるか否かを調べることを目的とし、そのためにノンパラメトリックな手法に基づく分散分析をおこなった。その結果、概して、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みられた。特に、所属している組織属性における禁止事項およびモチベーションでは、多くのケースで差異が確認された。このことから、労働者自身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が異なると結論づけることができる。

また、本研究では、モチベーションをもたせる企業システムは、ICT 化のみならず、情報セキュリティへの意識向上に寄与していることや情報セキュリティ教育の充実をはかることが必要であることなどについても言及しており、これらが企業の効率的な情報セキュリティ対策につながると主張している。

最後に、今後の展望および課題について述べる。この分野（情報セキュリティの経済学）における実証分析は、第 1 節でもみたように、必ずしも蓄積が進んでいるとはいえない。そのため、本研究のような情報セキュリティ対策・投資を経済学的かつ経営学的側面からの定量的な分析の蓄積が必要とされる。今後の研究の展望としては、われわれが、ウェブアンケート調査や郵送調査などによって収集したデータを用いて様々な実証分析を試みていく。また、本研究の分析においてもいくつかの課題が残っており、それをクリアにしていきたい。本研究が、この分野に対する学術的な貢献となるとともに、企業に情報セキュリティ対策・投資をするインセンティブを与えるための一助となったことを期待する。

追記

本研究は、竹村が文部科学省の科学研究費補助金交付課題「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」（課題番号 20730196・若手研究（B）・研究代表者 竹村敏彦）、峰滝と今川が文部科学省の科学研究費補助金交付課題「企業ミクロデータに基づくソフトウェア産業の実証分析：産業構造、生産性、人的資本」（課題番号 21330061・基盤研究（B）・研究代表者 峰滝和典）の助成を受けておこなった研究成果である。

参考文献

[1] 大隅昇 [2002]「インターネット調査の適用可能性と限界 ： データ科学の視点からの考察」『日本行動計量学会』, Vol.29, No.1, pp.20-44.

[2] 実積寿也 [2005]『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.

[3] 篠崎彰彦 [2003]『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.

[4] 竹村敏彦 [2008]『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.

[5] 竹村敏彦・海野敦史 [2009]「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』forthcoming.

[6] 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」『日本経済政策学会第 66 回全国大会開発表資料』

[7] 日本ネットワークセキュリティ協会 [2008]『2007 年度情報セキュリティインシデントに関する調査報告書 ver1.5』

http://www.jnsa.org/result/2007/pol/incident/2007incidentsurvey_v1_5.pdf
[8] 星野崇宏 [2007] 「インターネット調査に対する共変量調整法のマーケティングリサーチへの適用と調整効果の再現性の検討」『日本行動計量学会』, Vol.34, No.1, pp.33-48
[9] E. Brynjolfsson [2004] *Intangible Assets*, Diamond, Inc.
[10] W. Liu, H. Tanaka, K. Matsuura [2007] "Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms," *Information Processing Society of Japan Digital Courier*, vol.3, pp.585-599, 2007.
[11] T. Takemura, M. Osajima, M. Kawano [2009] "Economic Analysis on Information Security Countermeasures: The Case of Japanese Internet SserviceProviders" In *Advanced Technologies* (A. Lazinica Ed.), intechweb.org, forthcoming.
[12] H. Tanaka, K. Matsuura, O. Sudoh [2005] "Vulnerability and information security investment: an empirical analysis of e-local government in Japan," *Journal of Accounting and Public Policy*, vol.24, no.1, pp.37-59.