

情報セキュリティ対策の効果に関する
企業の管理者と労働者の意識にギャップはあるか
—Web アンケート調査データを用いた分析—

竹村敏彦

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@ml.kandai.jp

tel: 06-6368-1228

fax. 06-6330-3304

情報セキュリティ対策の効果に関する
企業の管理者と労働者の意識にギャップはあるか
Web アンケート調査データを用いた分析

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

2010年3月

概要

本稿では、年間売上や従業員規模のようなカテゴリーに基づき、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対策を行うことで実感できる効果について違いがあるか否かを検証している。社会科学における情報セキュリティの実証研究が2000年頃まで始まったことや、情報セキュリティに関するデータの収集が困難であることから、この種の研究は新しくまたチャレンジングな研究であるといえる。分散分析の結果から、両者の間で多くの実感できる効果について差異があることが確認できる。

Keywords: 情報セキュリティ, 意識ギャップ, 実証分析, 分散分析

* 関西大学ソシオネットワーク戦略研究センター・研究員
E-mail: takemura@rcss.kansai-u.ac.jp

Are There Awareness Gaps on Effects of Information Security Measure between Managers and Employees? Analysis Using Web-based Survey Data

Toshihiko Takemura*

Assistant Professor, the Research Institute for Socionetwork Strategies,
Kansai University

March, 2010

Abstract

In this paper, the author statistically investigates the difference of effects felt between information security managers and employees by implementing the measures according to categories such as number size of annual sales and employees. This kind of study is new and challenging because empirical study on information security in social science has just started in around 2000 and it is too difficult to collect data on information security. As a result, it is found the difference of effects felt between information security managers and employees in many categories.

Keywords: information security, awareness gap, empirical study, ANOVA

* Research Fellow, Research Center of Socionetwork Strategies, Kansai University
E-mail: takemura@rcss.kansai-u.ac.jp

1 はじめに

社会科学における情報セキュリティの実証研究は 2000 年頃に始まったばかりである。それは、情報セキュリティに関する個票データを収集することが困難であることが主要な理由の一つとしてあげられる。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。

ユーザの情報セキュリティに関するパフォーマンスや情報セキュリティマネジメントに関する研究はいくつかある (Stanton et al (2005)、Tanaka et al (2005, 2007)、Chan and Ho (2006)、Werlinger et al (2008)、Zhang et al (2009)、竹村・峰滝 (2010)など)。しかしながら、これらの研究は、たとえ情報セキュリティ対策を組織で実施していたとしても、世界中で起こっている情報セキュリティ事故や被害がなぜ起こっているかを必ずしもうまく説明することはできない¹。近年、これらの状況をうまく説明できるいくつかの研究が登場しており、それらはユーザや労働者、情報セキュリティ担当者の観点から組織の情報セキュリティ対策を分析しようとしている。簡単ではあるが、ここでそれらの研究を紹介する。

Albrechtsen (2007) は、ノルウェイの IT 企業と銀行の労働者に対して、情報セキュリティに関する知識等についてインタビュー調査を行っている。そしてその結果、ユーザ (労働者) は多くの情報セキュリティ対策に関して気にとめておらず、ましてや対策よりも他の仕事を優先することを明らかにしている。また、Albrechtsen and Hovden (2009)は、いくつかのノルウェイの企業の情報セキュリティ担当者や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ンド」が存在しているかどうかの検証を行い、その存在を確認している。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。これらの研究は新規性があり、またチャレンジングなものである。そして本稿の分析結果は、彼らの主張と多くの共通点を持っている。

日本における同様の研究として、竹村・峰滝・今川 (2009)や Takemura (2010)がある。これらの研究は、Web アンケート調査 (インターネット調査) によって収集された日本の個票データを用いて、組織属性や個人属性と労働者の情報セキュリティ意識の関係を検証している。その結果、労働者の情報セキュリティ意識は組織内の情報の取り扱い状況といった組織属性等によって異なることが明らかにしている。さらに、彼らは、情報セキュリティ機器を新たに導入するのではなく、情報セキュリティ教育を実施していくことが効率的であることを主張している²。

¹ 近年の情報セキュリティの経済学の先行研究をまとめたものとして、Camp (2006)と Anderson and Moore (2009)等がある。

² Hagen and Albrechtsen (2009) は情報セキュリティに対する労働者の知識、意識および行動を向上させる e ラーニングツールの効果の検証を行っており、その効果の存在を確認

本稿では、年間売上や従業員規模のようなカテゴリーに基づき、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対策を行うことで実感できる効果について違いがあるか否かを検証していく。分析には、著者が実施した2種類のWebアンケート調査によって収集された個票データを用いる。これらについて分析することで組織の情報セキュリティ担当者にたいして一つの材料を提示するとともに、効率的な情報セキュリティ対策について議論を行うことが可能となる。

本稿の構成は次の通りである。第2節で2つのWebアンケート調査の簡単な説明および統計手法について説明を行う。第3節では、分析結果を示す。最後に、第4節にてまとめとともに今後の展望を与える。

2 フレームワーク

近年、調査環境の変化により、郵送調査やインタビュー調査、電話調査のいずれも徐々に実施およびその回収率ともに厳しいものとなっている³。とりわけ、本稿で扱う情報セキュリティに関しては、多くの企業が部外者に情報を出したくない（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いる。Kotulic and Clark (2004)でも同様のことを指摘している。このことは、研究者がいくら努力をしたとしても、社会調査を実施したとしても一定以上の回収率を望めないことを意味している。

他方で、近年、マーケティングリサーチの分野である一つの新しい調査手法が注目されている。それがWebアンケート調査（インターネット調査）である⁴。本稿では、著者がこれまで実施した2つのWebアンケート調査によって集められた個票データを用いる。もちろん、Webアンケート調査は様々な統計的な問題が今なお残っている。しかしながら、それを理由としてその手法を採用しないということは、議論の余地は多々あるが、間違いのように思える。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、この手法を採用する意義があるといえる。もちろん、調査の正確性（accuracy）についても議論しなければいけない。しかしながら、本稿では、他者の実施した同様の郵送調査の結果と著者の実施した調査結果を比較し、その傾向が似ていることを確認し、これらのデータを用いて分析することができるかと判断した。

している。

³ 労働政策研究・研修機構 (2005)によれば、環境の変化として、たとえば、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、今日、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。

⁴ 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。

2.1 Web 調査

分析に用いる個票データは著者が 2008 年 11 月と 2009 年 3 月にそれぞれ実施した Web アンケート調査の結果を用いる⁵。以下、それぞれの調査概要を説明する。

2.1.1 情報セキュリティ管理者を対象とした調査

この調査の対象者は、2 年以上組織内の情報セキュリティ、とりわけネットワークセキュリティの業務に携わっている担当者もしくは精通した人物である。なお、この調査は、日本企業の情報セキュリティ対策の現状を把握するために行ったものである。それゆえに、実施している情報セキュリティ対策、情報セキュリティ被害の遭遇状況、直面している情報セキュリティ対策の問題、インターネットへの依存度や業種等、50 以上の質問を行っている。この調査の回答者は 500 人である。

表 1 には情報セキュリティ管理者の属している組織のサマリーを示している。

表 1 企業のサマリー I (情報セキュリティ管理者)

| | (%) |
|---------|--------------------|
| 従業員数 | 74.4 ^{a)} |
| 年間売上 | 59.8 ^{b)} |
| 上場企業の割合 | 17.8 |
| 公共性の水準 | 34.8 ^{c)} |

a) 従業員数が 1000 人以下の企業の割合

b) 年間売上が 30 億円未満の企業の割合

c) 公共性の水準が相対的に高い企業の割合

管理者に対して、社内における情報セキュリティ担当者以外の労働者の情報セキュリティ意識をしている。その結果は図 1 の通りである。図 1 を見てわかるように、「トップ、役員クラスから社員に至るまで情報セキュリティ意識は高い」と回答している割合は約 23% である。一方で、階層によって意識の違いがあると回答している割合は約 77% となっている。さらに、後者の 39% が「情報セキュリティ担当者以外は、意識は低い」と回答している。

⁵ 調査票は、以下の URL にて閲覧することができる。また、一定の手続きを経ることにより、個人や企業を特定できるデータを除いて学術目的に利用することができる。詳しくは、著者に連絡をするか、以下の Web サイトを参照されたい。

URL: <http://www.kansai-u.ac.jp/riss/en/shareduse/database.html>.

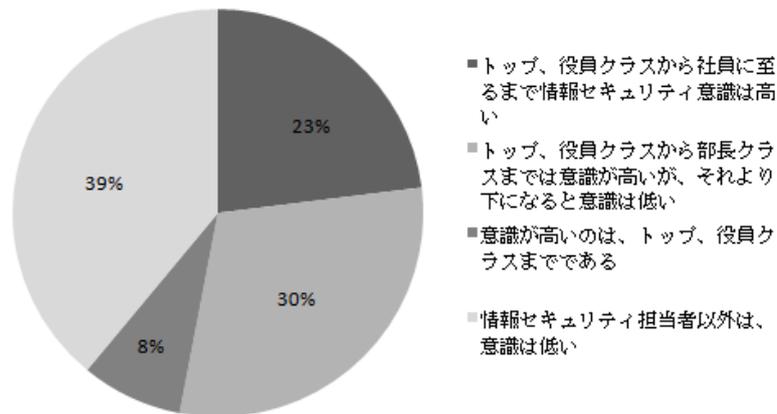


図1 情報セキュリティ意識の水準

次に、管理者に対して情報セキュリティ対策の問題点・課題について質問したところ、図2のような結果が得られた。その中で、約48%が「従業員の情報セキュリティ意識が低い」ことを問題点・課題として指摘している。続いて、25-35%の回答者が「顕在化していない情報セキュリティに関する事故・トラブルがあるのではという不安」や「現在の対策が十分かどうか分からない」、「情報セキュリティ対策に投じる費用対効果が見えにくい」といったことを問題点・課題として挙げている。

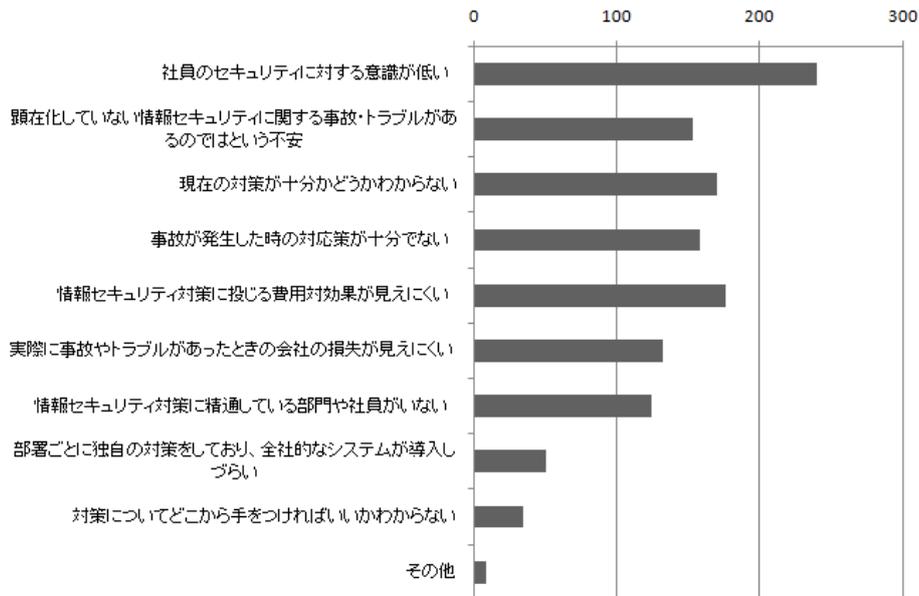


図2 企業における情報セキュリティ対策の問題点・課題

図 1 と図 2 より、特に、従業員の情報セキュリティ意識が低いと管理者が感じていることがわかる。そのような状況において、脅威から情報資産を防護するために、管理者が様々な技術的対策を実施しても、彼らはその効果を確認できないという奇妙な状況が垣間見られる。それゆえに、管理者は非常に困惑し、ジレンマに陥っているように思える。

1.2.2 労働者を対象とした調査

この調査の対象者は、2年以上同一の組織で働いている労働者である。なお、この調査は、労働者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。それゆえに、情報セキュリティ意識、学歴、リスクへの態度、組織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、賃金システム、インセンティブシステム等、50以上の質問を行っている。この調査の回答者は1500人である。

表 2 は労働者が属している組織のサマリーを示している。

表 2 企業のサマリー II (労働者)

| | (%) |
|---------|--------------------|
| 従業員数 | 54.5 ^{a)} |
| 年間売上 | 43.4 ^{b)} |
| 上場企業の割合 | 52.9 |
| 公共性の水準 | 39.0 ^{c)} |

a) 従業員数が 1000 人以下の企業の割合

b) 年間売上が 30 億円未満の企業の割合

c) 公共性の水準が相対的に高い企業の割合

表 1 と表 2 を比較して、上場企業の割合が異なることがわかる。これは、労働者を対象とした調査のみ、割付の 1 つとして上場企業・非上場企業を用いたために起こったと考えられる。

図 3 には、一般的な情報の取り扱いと情報セキュリティ対策に関する労働者の意識についてまとめたものを示している。ここでは、大別すると情報セキュリティ対策とネチケットに関して質問している。図 3 より、ネチケットに関しては、意識は必ずしも低くはないことがわかる。一方で、多くの企業で禁止されているけれども自宅で仕事をしたいと思っていたり、問題が起らなければルールを破ってもよいと思っていたりする労働者が約 37%もいることがわかった⁶。さらに、彼らの 80%が情報セキュリティ対策を実施することで生産性が向上するとは思えないと感じている。

⁶ なお、この割合は「どちらでもいい」という回答を含んだものである。

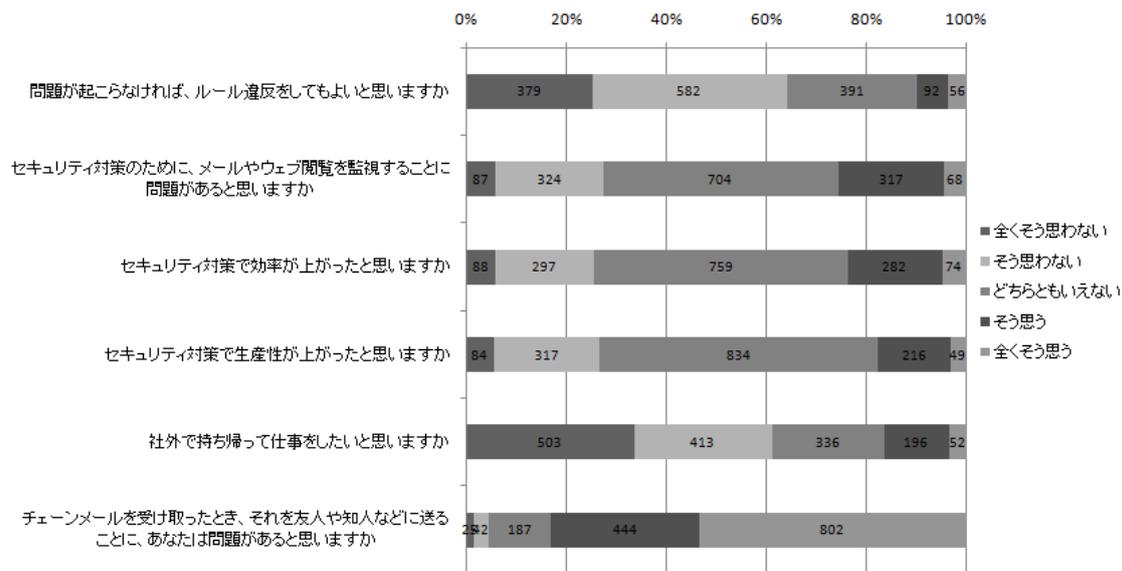


図3 労働者の情報の取り扱いと情報セキュリティ対策に対する意識

このことから、多くの労働者がある程度情報セキュリティ対策の重要性は認識しているものの、必ずしも対策を行うことに労働者が賛成しているわけではないということが示唆される。

2.2 仮説

情報セキュリティ管理者と労働者にとって、売上や収益を最大化すること、またマーケットシェアを拡大することがビジネスとしての目的である。現在のような高度情報化社会においてそれを達成するためには、情報セキュリティ対策が必要となる。もし対策が実施されていなければ、無防備に様々なビジネスリスクに彼らは直面することになる。たとえば、新聞を見ればわかるように、情報漏洩が起これば、株価の下落、企業の信用失墜、減収のようなシナリオを簡単に想像できるであろう。そして、これらのことは情報セキュリティ管理者と労働者もまた認識しているはずである。そして、対策を実施する観点から、情報セキュリティ管理者は情報管理を徹底し、労働者に対しても情報の取り扱いについて喚起をしている。しかしながら、彼らが努力しているにもかかわらず、情報漏洩等の事故は世界中で今なお報告されている。そこで一つの疑問が浮かぶ。それは、「管理者と労働者は同じ目的を達成しようとしているにもかかわらず、なぜ情報漏洩のような事故が起こるのであるのか。」ということである。そこで、本稿では、「情報セキュリティ管理者と労働者の間には情報セキュリティ対策に関する意識ギャップがある」と仮説を立て、そのギャップが上記のような事故につながっていると考える。つまり、この仮説において、そのような事故は対策の必要性に関する意識やリスクへの意識の違いによって引き起こされてい

ると本稿では考える⁷。

2つの調査にはいくつかの共通の質問を行っている。その中で、本稿では、管理者と労働者が対策を実施することで実感できる効果を取り上げることとする⁸。これを取り上げる理由は、2つの調査においてリスクへの意識の違いを直接測定する質問がないためである。この項目は直接的ではないが、間接的にリスクへの意識を測定する指標になりうる。さらに、一般的に言われている「対策が性の経済効果をもたらすかわからない」という問いに対して一つの回答を与えられると考える（図2参照）。そして、管理者に対して労働者の意識に対してどのように管理者が対応すればよいかの材料を提供することができる。

表3には、対策を実施したことで実感できるとされる効果の一部を示している。もちろんこれ以外にも様々な効果があると言われている。

表3 対策を実施したことで実感できる効果

| No | 内容 |
|----|-----------------------|
| E1 | 社員の情報セキュリティに対する意識向上 |
| E2 | リスク管理の重要性に対する理解・認識の向上 |
| E3 | 情報資産の見直し |
| E4 | 業務プロセスの見直し・修正 |
| E5 | 社内における情報の共有・活用 |
| E6 | 企業の社会的責任（CSR）としての自覚 |
| E7 | ビジネスパートナーや顧客からの評価 |
| E8 | 提供する製品やサービスの質の向上 |
| E9 | 競争力の強化 |

表3で示している効果は、1: 全く効果がないと思う、2: あまり効果がないと思う、3: ある程度効果があると思う、4: とても効果があると思う、の4段階で評価している。これらの効果は大別すると組織内で実感できるものとそれ以外（市場等）で実感できるものになる。表3の変数E1からE5は組織内で実感できる効果、E6からE9はそれ以外で実感できる効果をそれぞれ表している。

竹村・峰滝（2010）は、本稿と同様の情報セキュリティ管理者を対象にしたWebアンケート調査によって収集したデータを用いて、対策を実施したことで実感できる効果と技術的対策、マネジメントによる対策の関係を定量的に調べている。そして、彼らは、両者に正の関係があることを確認するとともに、組織内外における効果を実感するために行われる

⁷ たとえば、管理者が過度な対策を実施したり、労働者が対策を遵守しないといったことが想定として考えられる。

⁸ 注意すべき点として、この指標は客観的なものではなく、主観的なものであることが挙げられる。今後この点について、更なる議論を行う必要がある。

情報セキュリティに関するマネジメント対策の種類には若干の相違があることを明らかにしている。

以下、表 4 のカテゴリーに従って、対策を実施したことで情報セキュリティ管理者と労働者が実感できる効果の違いについて統計的に調べていく。

表 4 カテゴリー

| カテゴリー | 内容 | 変数 | 情報セキュリティ管理者の割合 (%) a) | 労働者の割合 (%) b) |
|--------|-----------|----|-----------------------|---------------|
| 上場企業 | 上場企業 | C1 | 18% | 53% |
| | 非上場企業 | C2 | 82% | 47% |
| 公共性 | 公共性が高い | C3 | 65% | 61% |
| | 公共性が低い | C4 | 35% | 39% |
| 年間売上規模 | 1000 万円以下 | C5 | 6% | 5% |
| | 1000 万円以上 | C6 | 24% | 44% |
| 従業員規模 | 300 人以下 | C7 | 59% | 41% |
| | 10000 人以上 | C8 | 9% | 19% |

a) 情報セキュリティ管理者（全サンプル）に対する割合

b) 労働者（全サンプル）に対する割合

2.3 統計手法

第 2.2 節の仮説を検証するために、ノンパラメトリックの手法に基づく分散分析を行う。具体的には、表 4 のカテゴリーにおいて管理者と労働者それぞれのグループの中央値に差異があるかどうかを調べる。ノンパラメトリックの手法に基づく分散分析の特徴として、データが正規分布に必ずしも従う必要が無く、順序データを用いることができるといったことが挙げられる。そして、本稿では、Mann-Whitney テストと Wilcoxon テストを行う。ここで簡単に各テストの手順を説明する。

Mann-Whitney の順位和検定 (Mann-Whitney の U 検定) と Wilcoxon の順位和検定は 2 群間の中央値の差異を調べる検定であり、得られた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 (W 及び U) とする。ただし、データに同一順位がある場合には、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。W や U の分布は近似的に正規分布にしたがうとされるため、標準正規分布表から漸近有意確率を求める。なお、両者の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」である。

3 分析結果

分散分析の結果を表 5 に示す。概して、表 5 の結果から、情報セキュリティ管理者と労働者の間で実感できる効果について表 4 における多くのカテゴリーで異なるといえる。

C1 と C6 の結果から、上場企業もしくは年間売上規模が 1000 万円以上の企業における情報セキュリティ管理者と労働者の間で対策によって実感できる効果には違いがないことが統計的に確認することができる。つまり、上場企業もしくは年間売上規模が 1000 万円以上の企業においては、情報セキュリティ管理者と労働者の間には実感できる効果に対する意識ギャップはないと結論づけることができる。

表 5 分析結果

| | C1 | | | | C2 | | | |
|----|---------|----------|--------|----------|----------|----------|--------|----------|
| | U | W | Z | asp | U | W | Z | asp |
| E1 | 34877.5 | 349698.5 | -0.211 | 0.833 | 133254.0 | 217920.0 | -2.642 | 0.008*** |
| E2 | 34793.5 | 38798.5 | -0.256 | 0.798 | 133276.0 | 217942.0 | -2.718 | 0.007*** |
| E3 | 33936.0 | 37941.0 | -0.683 | 0.494 | 125066.0 | 209732.0 | -4.282 | 0.000*** |
| E4 | 33322.0 | 348143.0 | -0.993 | 0.321 | 130934.5 | 215600.5 | -3.053 | 0.002*** |
| E5 | 32389.5 | 347210.5 | -1.462 | 0.144 | 130330.0 | 214996.0 | -3.213 | 0.001*** |
| E6 | 34907.0 | 38912.0 | -0.195 | 0.845 | 133961.0 | 218627.0 | -2.443 | 0.015** |
| E7 | 35111.0 | 39116.0 | -0.088 | 0.930 | 129226.5 | 213892.5 | -3.402 | 0.001*** |
| E8 | 34593.0 | 349414.0 | -0.339 | 0.734 | 122096.5 | 206762.5 | -4.860 | 0.000*** |
| E9 | 33769.0 | 348590.0 | -0.738 | 0.461 | 117653.5 | 202319.5 | -5.761 | 0.000*** |
| | C3 | | | | C4 | | | |
| | U | W | Z | asp | U | W | Z | asp |
| E1 | 44643.0 | 59868.0 | -2.866 | 0.004*** | 132197.0 | 185498.0 | -3.492 | 0.000*** |
| E2 | 46538.0 | 61763.0 | -2.040 | 0.041** | 128594.5 | 181895.5 | -4.329 | 0.000*** |
| E3 | 42248.0 | 57473.0 | -3.886 | 0.000*** | 125850.0 | 179151.0 | -4.656 | 0.000*** |
| E4 | 47857.5 | 63082.5 | -1.350 | 0.177 | 126441.5 | 179742.5 | -4.572 | 0.000*** |
| E5 | 46078.5 | 61303.5 | -2.142 | 0.032** | 133326.0 | 186627.0 | -3.219 | 0.001*** |
| E6 | 47614.5 | 62839.5 | -1.503 | 0.133 | 127727.0 | 181028.0 | -4.341 | 0.000*** |
| E7 | 42897.5 | 58122.5 | -3.470 | 0.001*** | 133677.5 | 186978.5 | -3.111 | 0.002*** |
| E8 | 43639.0 | 58864.0 | -3.147 | 0.002*** | 124366.0 | 177667.0 | -4.890 | 0.000*** |
| E9 | 43958.5 | 59183.5 | -2.962 | 0.003*** | 119361.0 | 172662.0 | -5.873 | 0.000*** |

| | C5 | | | | C6 | | | |
|----|---------|----------|--------|----------|---------|----------|--------|---------|
| | U | W | Z | asp | U | W | Z | asp |
| E1 | 1017.5 | 1545.5 | -1.305 | 0.192 | 40278.5 | 47781.5 | -0.085 | 0.932 |
| E2 | 890.5 | 1418.5 | -2.333 | 0.020** | 40358.0 | 47861.0 | -0.045 | 0.964 |
| E3 | 739.5 | 1267.5 | -3.345 | 0.001*** | 40343.5 | 260459.5 | -0.050 | 0.960 |
| E4 | 956.0 | 1484.0 | -1.696 | 0.090* | 37300.0 | 257416.0 | -1.579 | 0.114 |
| E5 | 975.5 | 1503.5 | -1.570 | 0.116 | 40165.0 | 260281.0 | -0.138 | 0.891 |
| E6 | 1081.0 | 1609.0 | -0.812 | 0.417 | 40345.0 | 260461.0 | -0.050 | 0.960 |
| E7 | 947.0 | 1475.0 | -1.782 | 0.075* | 39193.0 | 259309.0 | -0.612 | 0.540 |
| E8 | 875.5 | 1403.5 | -2.351 | 0.019** | 40236.0 | 47739.0 | -0.099 | 0.921 |
| E9 | 738.0 | 1266.0 | -3.271 | 0.001*** | 40422.5 | 47925.5 | -0.010 | 0.992 |
| | C7 | | | | C8 | | | |
| | U | W | Z | asp | U | W | Z | asp |
| E1 | 76942.5 | 121195.5 | -4.150 | 0.000*** | 6122.0 | 46308.0 | -0.758 | 0.448 |
| E2 | 77571.0 | 121824.0 | -4.049 | 0.000*** | 6308.5 | 46494.5 | -0.390 | 0.697 |
| E3 | 67129.0 | 111382.0 | -6.958 | 0.000*** | 6117.0 | 46303.0 | -0.743 | 0.457 |
| E4 | 70667.5 | 114920.5 | -5.928 | 0.000*** | 6228.5 | 46414.5 | -0.527 | 0.598 |
| E5 | 75959.0 | 120212.0 | -4.420 | 0.000*** | 5459.0 | 45645.0 | -1.992 | 0.046** |
| E6 | 76965.0 | 121218.0 | -4.116 | 0.000*** | 5807.0 | 45993.0 | -1.350 | 0.177 |
| E7 | 72643.0 | 116896.0 | -5.314 | 0.000*** | 6316.0 | 46502.0 | -0.355 | 0.722 |
| E8 | 66528.0 | 110781.0 | -7.082 | 0.000*** | 6137.5 | 46323.5 | -0.680 | 0.496 |
| E9 | 64767.0 | 109020.0 | -7.554 | 0.000*** | 5996.5 | 46182.5 | -0.931 | 0.352 |

***: p<0.01、 **: p<0.05、 *: p<0.1

他方で、C2、C4 と C7 の結果から、非上場企業もしくは公共性が低い企業、従業員規模が 300 人以下の企業においては、情報セキュリティ管理者と労働者の間で対策によって実感できる効果に違いがあることを統計的に確認している。そのような企業においては、情報セキュリティ管理者と労働者の間には実感できる効果に対する意識ギャップが存在すると結論づけることができる。

この他にも、C3、C5 と C8 の結果から、公共性が高い企業や年間売上規模が 1000 万円以下の企業、従業員規模が 10000 人以上の企業においては、情報セキュリティ管理者と労働者の間で対策によって実感できる効果のいくつかに違いがあることを統計的に確認している。これらの結果からだけでは、明確な結論を示すことはできないが、企業規模の違い等によって情報セキュリティ管理者と労働者の間には実感できる効果に対する意識ギャップが存在することは予想できる。そして、企業規模が大きくなれば、両者の間で実感できる効果の違いが現れにくくなるとも考えられる。これらについては、今後、更なる分析を

行い、検討していきたい。

4 まとめと今後の展望

本稿では、ノンパラメトリックの手法に基づく分散分析を用いて、いくつかのカテゴリ一によっ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たことで実感できる効果に差異があるか否かを検証してきた。その結果、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統計的にわかった。

最後に、今後の課題及び展望について述べる。情報セキュリティの経済学における実証分析は、第1節でも触れたように、必ずしも蓄積が進んでいるとはいえない。そのため、本稿のような情報セキュリティ対策・投資に関する定量的な社会科学からの分析及びその蓄積が必要とされる。その意味において、本稿で用いた Web アンケート調査及びその他の社会調査法（郵送法など）によって収集したデータを、個人情報等が特定できない形での公開、また、それらを用いたさまざまな角度からの実証分析を試みていく必要がある。さらに、本稿では、ノンパラメトリックな手法に基づく（一次元配置の）分散分析を行ったが、ここから得られる情報（施策のための材料）は、多重比較等のより高度な手法を用いたものに比べるとまだ不十分である。そこで、今後、より多くの情報を得るために、多重比較や共分散構造分析などの手法を用いて、これらの結果が精緻なものであるかの更なる検証を行っていきたい。

謝辞

本稿は、文部科学省の科学研究費補助金交付課題「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）、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。

参考文献

- [1] Albrechtsen (2007). A Qualitative Study of Users' Views on Information Security. *Computer and Security*, Vol.26, pp276-289
- [2] Albrechtsen, E. & Hovden, J. (2009) The information security digital divide between information security managers and users, *Computer and Security*, Vol.28, pp476-490
- [3] Anderson, R. & Moore, T. (2009) Information Security: Where Computer Science, Economics and Psychology Meet, *Philosophical Transactions of the Royal Society*, Vol.367, pp.2717-2727

- [4] Camp, L. J. (2006) The State of Economics of Information Security, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.6038&rep=rep1&type=pdf>
- [5] Chan, S. E., & Ho, C. B. (2006) Organizational factors to the effectiveness of implementing information security management, *Industrial Management & Data Systems*, Vol.106, No.3, pp345-361
- [6] Couper, M. P. (2000) Web Surveys: A Review of Issues and Approaches, *Public Opinion Quarterly* Volume 64: pp464-494
- [7] Hagen, J. M. & Albrechtsen, E. (2009) Effects on employees' information security abilities by e-learning, *Information Management & Computer Security*, Vol.17, No.5, pp338-407
- [8] Kotulic, A.G. & Clark, J.G. (2004) Why There Aren't More Information Security Research Studies, *Information and Management*, Vol.41, pp597-607
- [9] Liu, W., Tanaka, H., Matsuura, K. (2007) Empirical analysis methodology for information security investment and its application to reliable survey of Japanese firms, *IPSJDC*, Vol.3, pp.585-599.
- [10] Stanton, J. M., Stama, K. R., Mastrangelob, P. & Jolton, J. (2005) Analysis of end user security behaviors, *Computers and Security*, Vol.24, pp124-133
- [11] Takemura, T. (2010) 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
- [12] Tanaka, H.; Matsuura, K. & Sudoh, O. (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, pp37-59
- [13] Werlinger, R., Hawkey, K. & Beznosov, K. (2008) An integrated view of human, organizational, and technological challenges of IT security management, *Information Management & Computer Security*, Vol.17, No.1, pp4-19
- [14] Zhang, J., Reithel, B. J., & Li, H. (2009) Impact of perceived technical protection on security behaviors, *Information Management & Computer Security*, Vol.17, No.4, pp330-340
- [15] 竹村敏彦・峰滝和典 (2010) 「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—」 第7巻, forthcoming
- [16] 竹村敏彦・峰滝和典・今川拓郎 (2009) 「労働者の情報セキュリティ意識に関する研究」 RCSS Discussion Paper Series, No.85
- [17] 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