Web アンケート調査から見た

情報セキュリティ意識・行動についての一考察

～地域間比較～

竹村　敏彦

Working Paper Series Vol.FY2016-07
2017 年 1 月

佐賀大学経済学部
地域経済研究センター

〒840-8502　佐賀市本庄町 1 番地

Consideration about Information Security Awareness and Behaviors Using Results of the Web-based Survey[¶] - An Interregional Comparison -

Toshihiko TAKEMURA[*]
Faculty of Economics, Saga University

Abstract

Recently, information security incidents and accidents such as individual information leakage become a serious social problem, and then handing the problems are urgent issues. Actually, many of firms implement the technical measures using various information security technology and the enhanced management measures. Unfortunately, the number of the incidents and accidents do not decrease. In this article, we focus on human factor, which plays important role in information security measure. Concretely, we test whether or not there is a difference between regions for the information security behaviors and awareness. As a result, we can find statistically the difference between regions in some awareness such as compliance awareness.

Key Words: Information Security Awareness, Information Security Behavior, Security Economics, Web-based Survey

[¶] This work was supported by Center for Regional Economic Studies, Faculty of Economics, Saga University (grant-in-aid for independent study) and by the Japan Society for the Promotion of Science: Grant-in-Aid for Scientific Research (C) (16K03631). The author is grateful to useful and valuable comments from Mamoru Matsumoto (Associate Professor, Faculty of Economics and Business Administration, the University of Kitakyushu). The remaining errors are the author's.
[*] Corresponding to tosihiko@cc.saga-u.ac.jp

アンケート調査から見た情報セキュリティ意識・行動についての一考察[¶]

～地域間比較～

佐賀大学経済学部　竹村 敏彦[*]

要旨

昨今、個人情報の漏えいをはじめとする情報セキュリティに起因する事件・事故が社会問題となり、この問題への対応が喫緊の課題になっている。企業もその対応として様々な情報セキュリティ技術を用いた対策やマネジメントの強化を行っているが、依然としてその数は減っているとはいえない。本研究では、情報セキュリティ対策において重要な側面の一つである「ヒト」に焦点を当てた分析を行う。具体的には、情報セキュリティに対する個人の行動や意識に関して、地域間で相違があるかどうかを検証する。分析の結果、いくつかの意識などにおいて地域間で相違があることが統計的に確認された。

キーワード：情報セキュリティ意識、情報セキュリティ行動、セキュリティエコノミクス、Webアンケート調査

[¶] 本稿の一部は、佐賀大学経済学部地域経済研究センター自主研究プロジェクト研究助成および独立行政法人日本学術振興会の科研費（16K03631）の助成を得て行った研究成果である。草稿の段階において松本守先生（北九州市立大学経済学部）には有益なコメントをいただいた。記して感謝の意を申し上げたい。なお、残る誤りは著者の責任である。

[*] Corresponding to tosihiko@cc.saga-u.ac.jp

1. はじめに

昨今、個人情報の漏えいをはじめとする情報セキュリティに起因する事件・事故が社会問題となり、この問題への対応が喫緊の課題になっている。企業もその対応として様々な情報セキュリティ技術を用いた対策やマネジメントの強化を行っている。しかしながら、依然としてその数は減っているとはいえない。また、いくつかの（経営者や担当者に対する）情報セキュリティ対策・投資に関する調査において「情報セキュリティ対策の費用対効果が見えない」といった意見が上位にランキングされている。それゆえに、今なお情報セキュリティ対策への投資などは積極的に行われていないという現状である。

本稿では、どのような技術を導入することで、様々な脅威や組織の資産を不正・誤用や詐取から防護するかなどについて議論を行うのではなく、もう一つの重要な側面である「ヒト」に焦点を当てた分析を行う。例えば、多くの企業で策定・運用されているセキュリティポリシーを取り上げてみる[1]。セキュリティポリシーが策定・運用され、また適切な技術が導入されていたとしても，企業の構成員である従業員の全てがセキュリティポリシーを守っているとは限らず，その一部の従業員によって個人や企業が情報漏えいをはじめとする情報セキュリティインシデント被害に遭遇したという事例が報告されている（情報処理推進機構, 2016）。これらの事件・事故においてセキュリティポリシーやガイドラインに従っていれば防げたものも少なくない。つまり、情報セキュリティインシデント被害などは技術の不備の問題よりも、ヒトの問題に起因することが想像できる。この場合であれば、セキュリティポリシーを違反することは情報漏えいなどの情報セキュリティインシデント被害の引き金となりうることや企業が行っている情報セキュリティ対策が時として無効になることを意味している。ここで一つの疑問が生じる。それは「なぜ人は決められたルールを守ろうとしないのか」ということである。その理由として、Dhillon and Moores (2001)、Vroom and von Solms (2004)や Stanton, et al. (2005)などによれば、人間の怠慢や無知、不十分な情報セキュリティ意識などのヒューマンエラーに起因すると考えられている[2]。言い換えると、現在多くの企業が実施している情報セキュリティ対策を無効にしないためにはこのヒューマンエラーに対する対策、さらには情報セキュリティ意識の底上げを考える必要がある。

本稿では、情報セキュリティに対する行動や意識に関して、地域間で相違があるかどうかの検証を行う。著者の知る限り、情報セキュリティに対する意識や行動に関する地域間比較はほとんど行われていない。地域間比較を行う理由は、もし地域間に情報セキュリティ意識や行動に違いがあれば、情報セキュリティ対策として有効とされる教育やトレーニングを

[1] セキュリティポリシーとは、企業をはじめとする組織においてどのような情報資産をどのような脅威からどのようにして守るのかについての基本的な考え方、および情報セキュリティを確保するための体制、組織および運用を含めた規程・ルールのことをいう。

[2] 一つの可能性として、そもそも守れないセキュリティポリシーやガイドラインを策定・運用していることも考えられるが、近年発生している事件・事故を見てみると、その可能性は高くないことがうかがえる。

一律の内容で行うよりも、その地域にあった内容にすべきであると考えるためである。つまり、地域ごとに教育・トレーニングの内容をカスタマイズするべきか否かについての情報を提供できると考える。

2. 関連研究

本節では、企業に所属する従業員の情報セキュリティ意識・行動に関するいくつかの先行研究を紹介する。

先駆的な研究である Albrechtsen (2007)は、ノルウェーの 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、ノルウェーの企業の情報セキュリティ担当者と従業員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、従業員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指摘している。

日本における同様の研究として、Takemura (2010)や Takemura, et al. (2010)がある。彼らは日本の企業の従業員を対象に行った Web アンケート調査から、従業員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、従業員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従業員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, et al. (2010)は、従業員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。さらに、竹村 (2010)は同様の Web アンケート調査から、情報セキュリティの観点から適切な行動をとっている従業員グループの方が問題ある行動をとっているグループよりも、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、教育の有効性について論じている。

近年では、様々な情報セキュリティ行動に関する研究 (勤務中のインターネットの私的利用、コンピュータの誤用・悪用や著作権法違反、セキュリティポリシー違反、情報漏えいにつながる行動など）の蓄積が行われている（Peace, et al, 2003; D'Arcy, et al, 2009; Ifinedo, 2012; Takemura and Komatsu, 2013 など)。これらの情報セキュリティ行動及びそのメカニズムに関する研究に共通することとして、心理学からのアプローチが試みられている。このアプローチに関しては Anderson and Moore (2009)などが詳しい。また、情報セキュリティに関する研究、とりわけ実証研究の困難さについては Kotulic and Clark (2004)などを参照されたい。

3. アンケート調査概要

本稿では、著者が 2016 年 2 月にクローズ型のインターネットアンケート調査形式により実施された「労働者の情報セキュリティ意識および行動に関する調査 2016」(以下、2016 年調査と称す）によって収集した個票データを用いて分析を行う[3]。

2016 年調査の目的は一般労働者の情報セキュリティ意識および行動を把握し、情報セキュリティ教育や情報セキュリティマネジメントを行う際の情報を提供することにある。調査対象者は 2 年以上同一の企業で働いており、日常業務でパソコンや電子メールなどを利用している一般的な労働者である。この調査は、オーバーサンプリングや計測している回答時間から一般的な回答者と比べて回答時間が早い者を不良回答者として取り扱いサンプルから外すなどして、最終的に 1,236 人の有効回答数を得ている。調査対象者の構成は表 1 のようになっている。

2016 年調査の質問項目は、情報セキュリティ意識, 情報セキュリティ行動、情報リテラシーのみならず、職場環境、リスク許容など多岐にわたり、質問総数は約 60 問である。

質問項目の内容は、星野他（2008)、Peace, et al, (2003)、Takemura (2011)などで用いられているものを参考に作成されている.

表 1：調査対象者の構成

		#	(%)
年齢	20～39 歳	385	31.15
	40～49 歳	328	26.54
	50 歳以上	523	42.31
勤続年数	5 年未満	302	24.43
	5～9 年	306	24.76
	10 年以上	628	50.81
上場・非上場	上場企業	618	50.00
	非上場企業	618	50.00
従業員数	100～299 人	511	41.34
	300～999 人	178	14.40
	1000～4999 人	213	17.23
	5000 人以上	334	27.02

[3] この調査形式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。この調査手法の詳細な利用可能性・妥当性については石田他（2009)などを参照されたい。

4. 分析

4.1 情報セキュリティ意識・情報セキュリティ行動

本研究では、地域によって情報セキュリティ意識や情報セキュリティ行動の水準が異なるかどうかの検証を行う。以下、取り上げる項目（意識・行動）について簡単な説明を行う。

1）情報セキュリティ意識

情報セキュリティ意識とは、様々な形で存在する情報を取り扱うときに、個人が持っているセキュリティレベルを（高く）維持しようと考える意識のことをいう。これは情報セキュリティ教育・トレーニングなどで培われるとされ、情報セキュリティ意識の向上は情報セキュリティの観点から問題となる行動・意図を抑止する効果を持つことが明らかになっている（Reason, et al., 1998; D'Arcy, et al., 2009）。

2）コンプライアンス意識

本稿で考えるコンプライアンスとは法律や規則といったルールを守ることだけを指すのではなく、社会的規範やモラルを守ることも含んだ概念である（浜辺, 2005）。

組織に属する個人の行動全てをルールによって規定することができない。そのため、情報セキュリティの観点から問題となる行動を予防するには、（形式的な）コンプライアンスの仕組みを整備するだけでは不十分であり、法律や倫理の積極的な遵守に向けた意識改革が必要となることを Siponen (2000)は指摘している[4]。そのため、本稿ではコンプライアンスの仕組みの整備ではなく、個人のコンプライアンス意識に注目する。

3）セキュリティポリシー違反意図

従業員の情報セキュリティポリシー違反には意図的なものと意図的ではないものがある。意図的でない情報セキュリティポリシー違反もまた組織的の情報セキュリティに関する脅威となるけれども、本稿ではとりわけ意図的なセキュリティポリシー違反を取り上げる。なお、セキュリティポリシー違反意図は実際の行動ではなく、その意図を表すものを用いる。

上述したように、セキュリティポリシーは組織におけるセキュリティ対策について総合的・体系的かつ具体的にとりまとめた指針であり、セキュリティポリシーの遵守が組織において必要とされる。多くの組織において情報セキュリティポリシーが整備・運用されてはいるが，セキュリティポリシーは法律・法令ほどの強制力は必ずしもないために、遵守されないこともある。 その結果として，コンピュータの不正利用・誤用に加えて，情報セキュリティインシデント被害や事故に遭遇しやすくなることが指摘されている（Pee, et al., 2008; Siponen, M. and Vance, 2010; Takemura, 2014）。また、彼らはセキュリティポリシーを遵守させるよりもそれを違反させないことを考えることが有効な情報セキュリティ対策につながると主張している。

---

[4] 本研究で考えるコンプライアンスとは法律や規則といったルールを守ることだけを指すのではなく，社会的規範やモラルを守ることも含んだ概念である（浜辺, 2005）．

4）勤務中のインターネットの私的利用

私的目的のために，勤務中に SNS を閲覧・書き込みをしたり、オンラインショッピングをしたりするといったことは「(勤務中の）インターネットの私的利用（Cyberloafing, Cyberslacking)」や「業務と関係ないコンピュータの利用(Non-Work-Related Computing)」と呼ばれ、企業のセキュリティ対策においても注目を浴びている（Vitak, et al., 2001)。これらの行動は（労働）生産性の低下，時として情報漏えい、企業の評判を落とすことや株価の低下につながることが Weatherbee (2010)や Takemura (2014)等で指摘されている。

5）情報漏えいにつながる行動

情報セキュリティの観点から問題とされる行動には、その行動を取った個人にとっては少なくとも目的（例えば，営業成績を上げることや自らの生産性を高めることなど）に適っているかもしれないが、組織にとっては不利益を被ったり、リスクに晒されたりすることもある。情報漏えいが社会問題化されているにも関わらず、Takemura(2011)、情報処理推進機構（2013)や Takemura and Komatsu (2013)などによれば，（例えそれが組織でルールとして禁止されていたとしても）組織においてこの種の行動をとっている個人の数は一定数以上存在していることがわかっており，その数は減少傾向にあるとは言い難い状況にある。

4.2 分析結果

上述した要因はいずれも単項目ではなく、それらを適切に測定すると考えられる複数の質問項目によって構成されている。そのために、要因の作成を行う必要がある。以下、簡単ではあるがその手順を示す。

まず、被説明変数およびいくつかの説明変数に関して，質問項目から作成される要因（構成概念）を作成するために（一因子モデルとして）因子分析を行う。

セキュリティポリシー違反意図と勤務中のインターネットの私的利用についての質問項目は Peace, et al. (2003)で用いられているものをカスタマイズしたものを用いている。また、情報セキュリティ意識についての質問項目は Takemura (2010)で用いられているものを採用している。コンプライアンス意識についての質問項目は星野他（2008)に従って作成されたものを採用している。情報漏えいにつながる行動についての質問項目は竹村他(2015）で用いられているものを採用している。

まず、因子分析に先駆けて、2016 年調査で得られた質問項目から構成される要因の信頼性を確認するため、クロンバックの α 信頼性係数を求めた（表 2)。その結果、表 2 に示したいずれの要因の α 信頼性係数も 0.60 を大幅に上回っており、ある程度の妥当性を有しているといえる[5]。

[5] Hair, et al. (1998)によれば、クロンバックの α 信頼性係数が 0.60 以上であればその要因の一貫性（信頼性・再現性）は高いと考えられている。

表 2：クロンバックの α 信頼性係数

	質問項目数	α
情報セキュリティ意識	15	0.944
コンプライアンス意識	4	0.884
セキュリティポリシー違反意図	3	0.830
勤務中のインターネットの私的利用	3	0.853
情報漏えいにつながる行動	7	0.911

次に、これらの質問項目を用いて因子分析を行い、そこから因子得点を計算した。各要因は表 2 にあるその名前の通り、計算された値が大きくなるほどその傾向が強い（程度が大きい）ことを表す[6]。例えば、セキュリティポリシー違反意図はその数値が大きいほど、違反意図が高いことを意味している。また、図 1 にはセキュリティポリシー違反意図に関する回答者の分布を示している．図 1 を見てわかるように，セキュリティポリシー違反意図が高くなるにつれて個人の数は減少傾向にある。

第 4.1 節で説明した 5 つの要因について、 関東地方および近畿地方とその他の地域の 2 グループに分けてそれぞれの意識の平均値の差の検定（t 検定）を行った。表 3 にその分析結果を示している。

表 3 を見てみると、関東地方および近畿地方とその他の地域で有意な差異が確認されたのは、「情報セキュリティ意識」「コンプライアンス意識」「セキュリティポリシー違反意図」

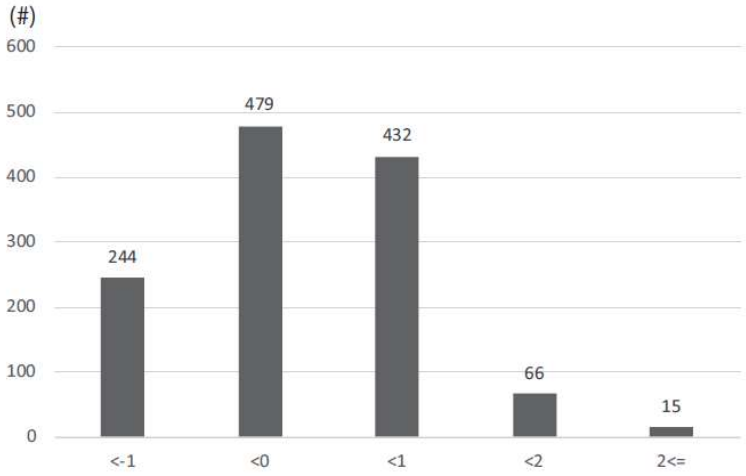

図 1：セキュリティポリシー違反意図

[6] 因子分析の結果については紙面の都合上省略している．

表 3：ケース 1（関東地方および近畿地方 vs. その他の地域）

項目	グループ	#	平均値	S.E
情報セキュリティ意識	その他地域	482	-0.072	0.043
	関東地方および近畿地方	754	0.046	0.037
	diff(=mean(0) - mean(1))		-0.119	0.058
	t = -2.062 Ho: diff = 0 degrees of freedom = 1234 Ha: diff < 0 Ha: diff != 0 Ha: diff > 0 Pr(T < t) = 0.020** Pr(|T| > |t|) = 0.039** Pr(T > t) = 0.980			
コンプライアンス意識	その他地域	482	-0.060	0.042
	関東地方および近畿地方	754	0.039	0.034
	diff(=mean(0) - mean(1))		-0.099	0.054
	t = -1.840 Ho: diff = 0 degrees of freedom = 1234 Ha: diff < 0 Ha: diff != 0 Ha: diff > 0 Pr(T < t) = 0.033** Pr(|T| > |t|) = 0.066* Pr(T > t) = 0.967			
セキュリティポリシー違反意図	その他地域	482	0.094	0.042
	関東地方および近畿地方	754	-0.060	0.033
	diff(=mean(0) - mean(1))		0.154	0.054
	t = 2.874 Ho: diff = 0 degrees of freedom = 1234 Ha: diff < 0 Ha: diff != 0 Ha: diff > 0 Pr(T < t) = 0.998 Pr(|T| > |t|) = 0.004*** Pr(T > t) = 0.002***			
勤務中のインターネットの私的利用	その他地域	482	0.066	0.043
	関東地方および近畿地方	754	-0.042	0.034
	diff(=mean(0) - mean(1))		0.108	0.055
	t = 1.985 Ho: diff = 0 degrees of freedom = 1234 Ha: diff < 0 Ha: diff != 0 Ha: diff > 0 Pr(T < t) = 0.976 Pr(|T| > |t|) = 0.047** Pr(T > t) = 0.024***			
情報漏えいにつながる行動	その他地域	482	-0.013	0.044
	関東地方および近畿地方	754	0.009	0.035
	diff(=mean(0) - mean(1))		-0.022	0.056
	t = -0.393 Ho: diff = 0 degrees of freedom = 1234 Ha: diff < 0 Ha: diff != 0 Ha: diff > 0 Pr(T < t) = 0.347 Pr(|T| > |t|) = 0.694 Pr(T > t) = 0.653			

***: p<1%, **: p<5%, *: p<10%をそれぞれ表す。

「勤務中のインターネットの私的利用」であった。つまり、これらの意識等の水準は地域間で違いがあることが確認された。また、分析結果を詳しく見てみると、「情報セキュリティ

意識」や「コンプライアンス意識」の水準は関東地方および近畿地方の方がその他の地域よりも高いことがわかった。逆に、「セキュリティポリシー違反意図」「勤務中のインターネットの私的利用意図」といった情報セキュリティの観点から問題となりうるものの水準については関東地方および近畿地方よりもその他の地域の方が高いことがわかった。

一方で、情報漏えいにつながる行動については有意差が確認されなかった。つまり、情報漏えいにつながる行動のとりやすさは地域を問わないことがわかった。

5. おわりに

本稿では、2016 年 2 月に実施した「労働者の情報セキュリティ意識および行動に関する調査 2016」と題するインターネット調査によって収集した個票データを用いたデータ分析を通じて、情報セキュリティ意識等の水準が地域によって異なるか否かの検証を行った。その結果、情報セキュリティ意識等の水準は地域間（関東地方および近畿地方と、その他の地域）で違いがあることが確認された。さらに、関東地方および近畿地方の方が他の地域よりも意識水準が高いことがわかった。この違いが出たことについては、更なる分析が必要であるが、一つの可能性として、大都市圏では情報セキュリティ意識を高めるための企業のセミナーなどが頻繁に開催されているが、それ以外の地域ではそのような機会が少ないことも指摘されている。今後の展望としては、本稿で取り上げた意識以外にも情報セキュリティインシデント被害経験等を踏まえた分析を行っていきたい。

参考文献

1. Albrechtsen, E., A Qualitative Study of Users' Views on Information Security. Computer and Security, Vol.26, 276-289, 2007
2. Albrechtsen, E. and Hovden, J., The Information Security Digital Divide between Information Security Managers and Users. Computer and Security, Vol.28, 476-490, 2009
3. Anderson, R. and Moore, T., Information Security: Where Computer Science, Economics and Psychology Meet. Philosophical Transactions of the Royal Society, Vol.367, 2717-2727, 2009
4. D'Arcy, J., Hovav, A., Galletta, D., User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, Vol.20, No.1, 79-98, 2009
5. Dhillon G., Moores, S., Computer Crimes: Theorizing about the Enemy Within, Computers and Security, Vol.20, No.8, 715-723, 2001.
6. Hair, Jr, J.F., Anderson, R.E, Thatham, R.L., Black, W.C., Multivariate Data Analysis, Prentice-Hall International, 1998

7. Ifinedo, P., Unedrstanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory, Computers and Security, Vol.31, 83-95, 2012.
8. Kotulic, A.G. and Clark, J.G., Why There Aren't More Information Security Research Studies, Information and Management, Vol.41, pp597-607, 2004
9. Peace, A.G., Galletta, D.F., Thong, J.Y.L., Software Piracy in the Workplace: A Model and Empirical Test, Journal of Management Information Systems, Vol.20, No.1, 153-177, 2003
10. Pee, L.G.. Woon, I.M.Y., Kankanhalli, A., Explaining Non-Work-Related Computing in the Workplace: A Comparison of Alternative Models, Information and Management, Vol.45, No.2, 120-130, 2008
11. Reason, J., Parker, D., Lawton R. Organizational Controls and Safety: The Varieties of Rule-Related Behaviour, Journal of Occupational and Organizational Psychology, Vol.71, 289-304, 1998
12. Siponen, M., A Conceptual Foundation for Organizational Information Security Awareness, Information Management and Computer Security, Vol.8, 31-41 2000
13. Siponen, M. and Vance, A., Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations, MIS Quarterly, Vol.34, No.3, 487-502, 2010
14. Stanton, J., Stam, K., Mastrangelo, P., Jolton, J., Analysis of End User Security Behaviors, Computers and Security, Vol.24, No.2, 124-133, 2005.
15. 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, 20-26, 2010
16. Takemura, T., Empirical Analysis of Behavior on Information Security, Proc. of 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, 358-363, 2011
17. Takemura, T., Unethical Information Security Behavior and Organizational Commitment, Approaches and Processes for Managing the Economics of Information Systems, Tsiakis, T., Kargidis, T. and Katsaros, P. (Eds.), 181-198, IGI Global Publication, 2014
18. Takemura, T., Komatsu, A.: An Empirical Analysis on Information Security Behaviors and Awareness. In: Bohme, R. (edt), *Economics of Information Security and Privacy*. Springer, 95-114, 2013
19. 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, 25-32, 2010
20. Vitak, J., Crouse, J., LaRose, R., Personal Internet Use at Work: Understanding Cyberslacking, Computers in Human Behavior, Vol.27, 1751-1759, 2001
21. Vroom, C., von Solms, R., Towards Information Security Behavioural Compliance, omputers and Security, Vol.23, No.3, 191-198, 2004.
22. Weatherbee, T.G. Counterproductive Use of Technology at Work: Information and Communications Technologies and Cyberdeviancy, Human Resource Management Review, Vol.20, No.1, 35-44, 2010
23. 石田浩・佐藤香・佐藤博樹・豊田義博・萩原牧子・萩原雅之・本多則恵・前田幸男・三輪哲「信頼できるインターネット調査法の確立に向けて」『SSJDA リサーチペーパーシリーズ』, SSJDA-42, 2009.
24. 情報処理推進機構「日本的経営と情報セキュリティ研究会報告書」http://www.ipa.go.jp/security/fy24/reports/nihontekikeiei/, 2013
25. 情報処理推進機構「オンライン本人認証方式の実態調査報告書」 https://www.ipa.go.jp/security/fy26/reports/ninsho/, 2014
26. 情報処理推進機構『情報セキュリティ白書 2015』情報処理推進機構, 2015.
27. 情報処理推進機構『情報セキュリティ白書 2016』情報処理推進機構, 2016.
28. 竹村敏彦「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」『情報通信政策レビュー』創刊号, 35-46, 2010
29. 竹村敏彦・三好祐輔・花村憲一「情報漏えいにつながる行動に関する実証分析」『情報処理学会論文誌』, 第 56 巻 12 号, 2191-2199, 2015
30. 浜辺陽一郎『コンプライアンスの考え方: 信頼される企業経営のために』中央公論新社, 2005
31. 星野崇宏・荒井一博・平野茂美・柳澤秀吉「組織風土と不祥事に関する実証分析」『一橋経済学』, Vol.2, No.2, 157--177, 2008
32. 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.