様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　５　月　２８　日現在

機関番号：　１７２０１
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５３８０３４５

研究課題名（和文）情報セキュリティ行動と有効な情報セキュリティ対策に関する実証研究

研究課題名（英文）Empirical Analysis on Information Security Behaviors and Effective Information Security Measures

研究代表者

竹村　敏彦（TAKEMURA, Toshihiko）

佐賀大学・経済学部・准教授

研究者番号：００４１１５０４

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：本研究の目的は、企業組織や労働者を対象としたアンケート調査から得られたデータを定量分析し、企業および従業員の情報セキュリティ対策のあるべき姿を明らかにすることである。この目的を達成するために、Web（インターネット）アンケート調査を実施し、収集・蓄積した個票データを行動経済学やミクロ経済学の視点を踏まえてデータ分析を行った。その結果、多くの情報セキュリティ行動に影響を与えている要因として職場における環境が影響を与えていることが多いため、まず職場環境の改善に取り組むべきあることを明らかにした。

研究成果の概要（英文）：In this research, I aim to clarify the effective information security measures and policies by quantitatively analyzing impact of information security incidents toward economy and business. Therefore, I built behavioral model based on behavioral economics and microeconomics, and carried out some empirical analyses using micro data collected from the Web-based survey. As a results, it is found that the organization must put a high priority on improving the workplace environment such workplace climate and job satisfaction.

研究分野：　セキュリティエコノミクス・産業組織論・行動経済学

キーワード：　情報セキュリティ　セキュリティエコノミクス　行動経済学　情報漏えい　サイバーリスク　炎上　セキュリティマネジメント　Web（インターネット）アンケート調査

１．研究開始当初の背景

情報セキュリティ技術（例えば、暗号化技術等）に関する研究の歴史は古く、その研究蓄積は膨大な量となり、実社会で実装されて安心・安全な社会の構築に寄与している。一方で、昨今、新聞やテレビ等で取り上げられているように情報セキュリティに起因する事件・事故が多いのも事実である。その原因として不十分な技術的対策もあるが、その多くはその技術を利用する人間の問題であることも様々な研究で指摘されている（ヒトが一番の脆弱性であると指摘している研究も少なくない）。このことから、2000 年頃から情報セキュリティに対して経済学・人間行動の視点からアプローチするセキュリティエコノミックス（Security Economics）と呼ばれる研究が海外にて本格的に始動した。当初、ゲーム理論などを用いた理論モデルの構築が行われたが、それを検証する実証分析はあまり行われなかった。その理由として、情報セキュリティはセンシティブな情報であるために調査協力が容易でなかったため、（小規模な）インタビュー調査の結果に基づく限定的な研究といった状況にとどまっていたことが挙げられる。

しかしながら、海外においてセキュリティエコノミックスの重要性・有用性が認められたことや情報セキュリティ対策が社会的に見て喫緊の課題であることを受けて、セキュリティエコノミックスにおける実証分析での様々な挑戦が行われた。日本においても情報処理推進機構が継続的な郵送調査を実施したり、竹村敏彦（研究代表者）も継続的な Web アンケート調査を実施し分析したりすることで、この萌芽的分野の深化に大きく寄与してきた。

２．研究の目的

本研究では、継続的に実施する企業組織や労働者を対象としたアンケート調査から得られたデータを定量分析し、高度情報化時代における安心・安全社会を実現するために必要とされる企業および従業員の情報セキュリティ対策のあるべき姿を明らかにする。それと同時に、情報セキュリティ対策を実施しなかったことによって生じる経済損失（システムの停止に伴う逸失利益等）額や過剰な対策を実施したことによって生じる経済損失（労働生産性の低下等）額等の試算もあわせて行う。これらの定量的な分析結果に実務家、政策実務家との議論を踏まえて、有効かつ実現可能な情報セキュリティ対策および政策のグランドデザイン（投資対効果を含む）を具体的に提示する。

本研究で行うセキュリティエコノミックス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、主として、継続的に収集・蓄積した情報セキュリティ行動および意識に関する調査から得られた個票データを用いて分析を行っている。

（１）　Web アンケート調査の実施～個票データの収集・蓄積～

本研究では、調査手法として Web アンケート（インターネットアンケート）形式の調査を 2013～2015 年度に計 3 回実施し、個票データの収集・蓄積を行った。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・彼女の情報セキュリティ意識や情報セキュリティに関する行動を把握するために行ったものである。そのために本調査を行う前に事前調査（スクリーニング調査）を実施し、その中で雇用形態（正規・非正規）と所属する組織の上場の有無によって事前割付を行った（表１参照）。

表１：調査対象者割付

	上場	非上場
正規雇用	25%	25%
非正規雇用	25%	25%

本調査では、情報セキュリティ意識、プライバシー意識、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に加えて、行動経済学的質問等に関する 60 問以上にわたる質問を多岐にわたって行った。なお、これらの内容に関しては過去に実施した調査を精査の上、項目の新規追加、削除を行い、その時々の情報セキュリティに関するトピックやその動向を把握できる調査内容にした。調査の実施に際して、モニター利用する調査では調査票の公開時期（曜日・時間帯）によってサンプルに偏りが生じることが知られているので、これらについて配慮して実施している。なお、サンプルサイズは 2013 年度では 1,507 人、2014 年度では 1,236 人、2015 年度では 1,236 人となっている。

（２）　データ分析

本研究では、主として、収集・蓄積した個票データを用いたデータ分析を行った。その際、心理学的要因をモデルに組み込みやすい行動経済学や行動科学の理論的フレームワークを採用した。また、データ分析手法としては、ロジット回帰分析や構造方程式モデリング等を用いた。

（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受けなが

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

2005 年度から竹村敏彦（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、政策実務家等と、アンケート調査の規格・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佐賀、東京および大阪にて、研究機関を通じて 30 回程度開催した。

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、それを査読付き学術雑誌に投稿することに加えて、竹村敏彦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、個人や組織を特定できる情報を除き、学術目的にのみ利用できる体制をとっている。この活動はこの分野の学術発展に寄与するものである。詳しくは竹村敏彦に問い合わせをされたい。

4．研究成果

（1） 情報セキュリティ行動および意識の動向

2013～2015 年度に実施した Web アンケート調査の結果からみた情報セキュリティ行動や個人の意識の変化などについてその一部を紹介する。

① 情報セキュリティ・インシデント被害状況の推移

過去 2 年間で自身が遭遇したトラブル（コンピュータウイルス感染など）の被害状況の推移を図 1 に示している（一部抜粋）。

ウイルス感染およびネット上での誹謗中傷の被害状況に関してはここ 3 年間でほぼ横ばいとなっている。（職場において発生したとされる）内部不正に関してはわずかながら上昇傾向にあることがわかる。

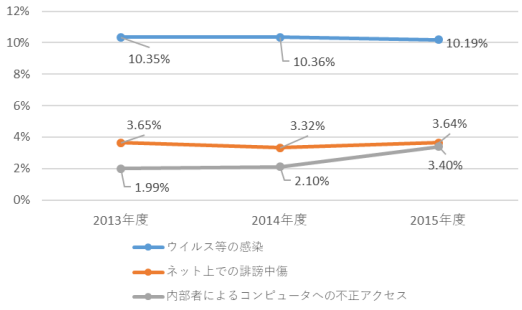


図 1：情報セキュリティ・インシデント被害状況の推移

② 満足度の推移

職場（会社）において仕事全般、職場、IT

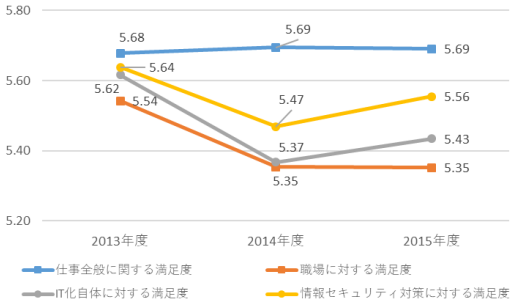


図 2：満足度の推移

10 点満点で評価した結果（平均値）およびその推移を図 2 に示している。

仕事全般に関する満足度は 3 年間でほぼ横ばいであるのに対して、それ以外の満足度の推移には変化が見られる。また、職場および IT 化に関する満足度よりも情報セキュリティ対策に対する満足度はいずれの年度においても高いことがわかる。

他の質問項目の推移に関しては竹村のホームページを参照されたい。

（2） 情報セキュリティ・インシデント被害遭遇に関する研究

田中他「情報セキュリティ・インシデントによる経済損失の推計に関する研究」（経済政策ジャーナル、第 11 巻第 2 号、2015 年）では、情報セキュリティ・インシデントが日本の経済活動にどのような影響を及ぼすかについて、JIP データや情報処理推進機構(IPA)調査などを用いて、生産関数に基づくマクロ経済の観点から分析を行った。その結果、インシデントに伴うシステムやデータの復旧に伴う作業によって、日本全体で年 46 億円から 94 億円程度の損失があった可能性があることを示した（表 2 参照）。

この研究で考案したような復旧に伴う経済的損失については、そのための人件費を積み上げる方法は提案されていたが、生産関数に基づいて推計することによっても推計が可能であることを示した。

表 2：損失額の推計値（単位：100 万円）

2009 年	2010 年	2011 年
5,781	4,534	9,436

（3） ネット炎上・悪意ある投稿に関する分析

昨今、ソーシャルメディアの普及に伴い、個人が容易にプライベートな情報を気楽に発信できる時代となった。その一方で、不謹慎・モラルに欠ける投稿を行った結果、「炎上」という社会問題が起こっていることは周知の事実である。これら炎上させた個人や企業の行動分析についてはいくつか行われているものの、その炎上の一躍を担っている炎上に加担している個人に注目している研究はこれまでほとんどない。例え不謹慎なソーシャルメディアへの投稿であったとしても、

その投稿に対する批判的なコメントをした側も、その様態によっては法的責任を負う場合がある。そこで、ネット炎上に参加する個人および悪意ある投稿をする個人の行動分析に関する研究を行った。

① ネット炎上に参加する個人の行動分析

竹村・花村「ネット炎上に加担する個人属性に関する考察」(第 69 回日本情報経営学会、2014 年）では、 組織が保有するこれらのリスクを低減させる施策を検討することを目的に、今まで焦点を当てられてこなかった炎上への参加行動に影響を与える要因について、アンケート調査で収集した個人の意識や所属組織の環境などの要素を用いて分析を行った。その結果、個人の意識の問題であると同時に、その個人が所属する組織の環境からも影響を受けることがわかった(表 3 参照)。炎上への参加行動を抑止するために組織が取り組むべき施策としては、情報モラル、業務倫理、法律に抵触する可能性などの内容を盛り込んだ情報セキュリティ教育・トレーニングの実施が重要であること等が示唆された。

表 3：分析結果 1

	Coef.	Std. Err.	P>z	[95% Conf.	Interval]
抵抗感	-0.720	0.131	0.000	-0.976	-0.464
コンプライアンス意識、	-0.669	0.155	0.000	-0.972	-0.366
セキュリティポリシー違反意識	0.256	0.150	0.087	-0.037	0.549
情報セキュリティ意識	-0.830	0.162	0.000	-1.148	-0.512
不正･違反放置	1.285	0.166	0.000	0.960	1.610
コミュニケーション重視	-0.247	0.138	0.075	-0.518	0.025
年齢	-0.018	0.009	0.052	-0.035	0.000
性別	0.652	0.234	0.005	0.193	1.111
営業職ダミー	0.032	0.300	0.915	-0.557	0.621
事務職ダミー	-0.193	0.242	0.426	-0.668	0.282
主観的な知識	0.285	0.118	0.016	0.053	0.517
ネット依存	0.011	0.136	0.933	-0.255	0.277
_cons	-1.197	0.782	0.126	-2.729	0.335
Number of obs = 1507					
LR chi2(12) = 463.88 (Prob > chi2 = 0.00)					
Log likelihood = -303.152					
Pseudo R2 = 0.434					

② 悪意ある投稿をする個人の行動分析

炎上のきっかけとなるが悪意ある投稿を行う個人にどのような特徴を有するのかをアンケート調査によって収集したデータを用いて行動経済学的要因を組み込んだ行動モデルの検証を行った。分析の結果、「SNS に関する知識」「ID リセットの経験の有無」「プライバシー性に関する意識」「他者志向性（同調行動）」等が悪意のある投稿をする傾向に影響を与えていることがわかった(表 4 参照)。とりわけ、悪意のある投稿に関しては、単に知識を増やすだけでは悪意ある投稿をする可能性が高くなるといった結果が得られた。これらの結果を受けて、「倫理教育の充実」「リセットをしづらくするための対策」を悪意ある投稿を抑止する効果がある対策として提案を行っている。なお、この分析結果は、今後、論文化を行う予定である。

表 4：分析結果 2

	Coef.	Std. Err.	z	P>z
SNSに関する知識	0.061	0.024	2.53	0.011
IDリセット経験の有無	0.509	0.160	3.18	0.001
プライバシー性に関する意識	-0.241	0.078	-3.11	0.002
社交性	0.139	0.092	1.51	0.132
公的自己意識	-0.319	0.118	-2.71	0.007
言語的攻撃	0.306	0.091	3.37	0.001
他者志向性（同調行動）	0.508	0.124	4.09	0
時間非整合性	-0.145	0.242	-0.6	0.549
危険回避度	0.007	0.004	1.58	0.115
ヒューリスティックス	-0.013	0.070	-0.19	0.849
年齢	-0.112	0.034	-3.27	0.001
年齢の 2 乗	0.001	0.000	2.42	0.015
職業ダミー	0.145	0.198	0.73	0.466
_cons	-0.286	0.629	-0.45	0.649
Number of obs	1238.000			
LR chi2(13)	120.61			
Log likelihood	-542.767			
Pseudo R2	0.1			
Prob > chi2	0			

（４） パスワード管理に関する研究

近年、パスワード管理の不徹底に起因するインシデント被害の報告が増えている。竹村他「SNS ユーザのパスワード管理に関する実証分析」（CSS2015、2015 年）では、アンケート調査の結果を用いて、行動経済学・社会心理学の視点からパスワード設定・管理等に関する行動に影響を与えている要因を探索した。その結果、パスワード管理に影響を与える要因として「判断力」「プライバシー性に関する意識」があることが確認された。このことから、判断力やプライバシー性に関する意識を向上させることで、適切なパスワード管理を行うようになることが示唆された。表 5 はこの多項ロジット分析の結果をまとめたものである。なお、表 5 にある Category については表 6 の通りである。例えば、Category1 は使い回しをせず、強いパスワードを設定していることを表している。

表 5：分析結果 3

From Category 1	To Category 2	To Category 3	To Category 4
年齢			○(−)
アカウント数	○(−)		○(−)
アカウント数(2乗)			○(+)
形式主義			
判断力	○(−)	○(−)	○(−)
リスク評価			
プライバシー性に関する意識	○(−)	○(−)	○(−)
時間非整合性			
インシデントに関する知識	○(−)		○(−)

表 6：カテゴリーの説明

値	サービスごとのパスワード設定	パスワードの強さ	#
1	YES	YES	155
2	YES	NO	386
3	NO	YES	129
4	NO	NO	568

（５） 情報セキュリティポリシー違反に関する研究

多くの企業において情報セキュリティポリシーの策定および運用が行われているにもかかわらず，その構成員である従業員の一部が情報セキュリティに関する基本的なルールを定めた情報セキュリティポリシーを遵守せず、その結果として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

被害につながった事例も少なくはない。情報セキュリティポリシーの遵守は、技術的な対応には限界があり、最終的には個人の問題となる。

① ポリシー違反意図に関する分析

Takemura,T.,“Empirical Analysis of Intentional Security Policy Violation in the Workplace”（佐賀大学経済論集、2014年）では、アンケート調査によって収集された情報セキュリティ行動や意識に関するデータを用いて情報セキュリティポリシー違反する意図に影響を与える要因について計画的行動理論に基づくモデルの検証を行った。分析結果は表7に示している。この結果、ポリシー違反意図に対する「行動に対する態度」と「主観的な規範の認知」の有意性は確認されたが、「知覚された行動の統制可能性」「処罰の厳格さ」「処罰の確実性」の有意性は確認されなかった。また、仕事に対する満足度、職場におけるソーシャルキャピタルの構築といった職場環境の充実が個人のポリシー順守に有効となることを明らかにしている。

表7:分析結果4

Variable (Factor)	Estimate	z	p-value
Attitude	0.9833	11.25	0.000
Subjective norm	0.3144	2.98	0.003
Perceived behavioral control	−0.9231	−5.84	0.000
Punishment severity	0.3693	2.37	0.018
Punishment certainty	0.1799	1.28	0.201
Social capital	−0.2156	−2.92	0.004
Job satisfaction	−0.0615	−2.14	0.033
Gender (Male=1; Female=0)	−0.4549	−2.82	0.005
Age	−0.0147	−2.12	0.034
Annual income	0.0570	0.82	0.412
/cut-1	−3.594	0.47	
/cut-2	−0.709	0.46	
/cut-3	3.551	0.50	
Pseudo R2	0.2005		
Log likelihood	−1144.037		
LR chi2(10)	397.06		

② ポリシー違反意図に関する分析

竹村・島「職場におけるポリシー違反意図と職場風土の関係についての分析」（SCIS2016、2016年）では、アンケート調査によって収集された情報セキュリティ行動や意識に関するデータを用いて情報セキュリティポリシー違反する意図に影響を与える要因について実証分析を行った。その結果、情報セキュリティポリシーを違反する意図に影響を与える要因として、情報リテラシーや個人を取り巻く職場風土などがあることが明らかになった（表8）。とりわけ、情報セキュリティポリシー違反を抑止する効果としては，組織にとって悪しき職場風土の改善を行うことが、 有効であり、優先される事項であることが示唆された。

表8：分析結果5

	Coef.	S.E.	β
不正・違反放置風土	0.195^{***}	0.024	0.204
普遍的倫理意識	-0.121^{***}	0.029	−0.108
帰属集団の正当化・組織防衛	0.287^{***}	0.033	0.256
懲罰からの自己防衛	0.022	0.030	0.020
情報リテラシー	-0.215^{***}	0.026	−0.230
被害遭遇可能性に対しての意識	-0.046^{**}	0.023	−0.049
インシデント等に関する自信過剰	0.010^{*}	0.006	0.040
ヒューリスティックス	0.007	0.029	0.006
cons	−0.011	0.067	—

***: p1%, **: p5%, *: p10%
Adj. R^2= 0.269
$F(8, 1227)$=57.84^{***}

（6） 漏えいにつながる行動に関する研究

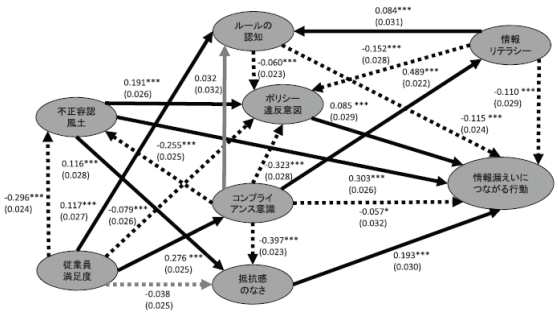
近年、サイバー攻撃や内部不正によるインシデントが複数報道されており、その中には原因調査や復旧作業等に多大な費用が発生し、企業経営に影響を及ぼす事例も報告されている。和泉他「サイバーリスクに関する実証分析」（CSS2015、2015年）では、リスクマネジメントのひとつの対策であるリスク移転としてのサイバー保険に着目し、企業のサイバーリスクに対する体制整備や各種セキュリティ対策との関連についてアンケート調査結果を分析することにより、サイバー保険の有効性・サイバー保険加入企業の特徴等について明らかにしている。この分析結果は表9のようになった。表9を見てわかるように、リスク分析や高度なセキュリティ対策の実施が，サイバー保険の加入に影響を与えることが確認された。

表9:分析結果6

項目	Coef.	Std. Err.	z	P>|z|
リスク分析の実施	0.794432	0.269163	2.95	0.003
CISOの任命	0.311318	0.271224	1.15	0.251
高度セキュリティ対策の実施傾向	0.54677	0.155764	3.51	0.000
基本セキュリティ対策の実施の傾向	0.252845	0.177178	1.43	0.154
情報漏えいの懸念の大きさ	0.243462	0.177944	1.37	0.171
風評被害の懸念の大きさ	-0.03246	0.160229	-0.2	0.839
人為的リスクの影響度の大きさ	-0.46624	0.269625	-1.73	0.084
偶発的リスクの影響度の大きさ	0.371312	0.283235	1.31	0.19
業種	0.201199	0.282021	0.71	0.476
従業員数	0.225587	0.104371	2.16	0.031
_cons	-3.11815	0.438274	-7.11	0
Number of obs = LR chi2(10) = 221.11 Prob > chi2 = 0.0 Log likelihood = -282.04726 Pseudo R2 = 0.2816				

（7） 漏えいにつながる行動に関する研究

竹村他「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巻第12号、2015年）では、情報漏えいにつながる個人の行動に着目し、その行動がどのような要因に直接的・間接的に影響を受けているかなどについて分析を行い、そこからこの種の行動を防止・抑止するために組織がとるべき効果的な施策について考察している。構造方程式モデリング（SEM）による分析の結果（図3参照）から、情報漏えいにつながる行動をとらせないようにするためには、不正容認風土を改善することが最も大きな効果があること、またコンプライアンス意識の向上は直接的な効果はそれほど大きくないも



a) 実線はパス係数の推定値が正，破線は負であることを表す．
b) ***: $p < 1\%$, *: $p < 10\%$

図 3：SEM の分析結果

ので、様々な要因を介した間接的な効果を踏まえた総合効果は不正容認風土の改善に次ぐ効果があることが示唆された。これに加えて、 不正容認風土に影響を与える要因としてコンプライアンス意識および従業員満足度の向上があることから、職場環境の改善とともに従業員満足度の向上策の実施やコンプライアンス教育の実施がより大きな効果を生む可能性があることを指摘している。

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 6 件）

① 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，査読有，第 56 巻第 12 号，2015，2191-2199
https://ipsj.ixsq.nii.ac.jp/ej/index.php?active_action=repository_view_main_item_detail&page_id=13&block_id=8&item_id=146635&item_no=1

② 田中秀幸・竹村敏彦・飯高雄希・花村憲一・小松文子，情報セキュリティ・インシデントによる経済損失の推計に関する研究，経済政策ジャーナル，査読有，第 11 巻第 2 号， 2015，59-62

③ 竹村敏彦，日本の国際競争力強化に向けた戦略と課題，情報通信政策レビュー，査読無，第 8 巻第 1 号(特別寄稿)，2014，25-40
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/08/08-2takemura2014.pdf

④ Takemura, T., Empirical Analysis of Intentional Security Policy Violation in the Workplace，佐賀大学経済論集，査読無，第 46 巻第 6 号，2014，21-40
http://portal.dl.saga-u.ac.jp/bitstream/123456789/121635/1/takemura_201403.pdf

⑤ 熊谷洋子・島成佳・竹村敏彦・小松文子，人情報活用オンラインサービスに対する信頼感と利用意図に関する要因分析，日本セキュリティ・マネジメント学会誌，査読有， 第 27 巻第 2 号，2013，3-15

⑥ Hanamura, K., Takemura, T., Komatsu, A., Analysis of the Characteristics of Victims in Information Security Incident Damages: The Case of Japanese Internet Users, The Review of Socionetwork Strategies, 査読有，Vol.7, No.1, 2013, 43-51
DOI: 10.1007/s12626-013-0032-6

〔学会発表〕（計 7 件）

① 竹村敏彦・島成佳，職場におけるポリシー違反意図と職場風土の関係についての分析，SCIS2016，ANA クラウンプラザホテル熊本ニュースカイ（熊本），2016 年 1 月 21 日

② 竹村敏彦・田村滋基・児玉弘，SNS ユーザのパスワード管理に関する実証分析，CSS2015，長崎ブリックホール（長崎），2015 年 10 月 22 日

③ 和泉あゆみ・小松文子・加藤慎也・竹村敏彦，サイバーリスクに関する実証分析，CSS2015，長崎ブリックホール（長崎），2015 年 10 月 22 日

④ 安藤玲未・島成佳・竹村敏彦，組織情報の外部提供に関する分析と考察，DICOMO2015 シンポジウム，ホテル安比グランド（岩手），2015 年 7 月 8 日

⑤ 竹村敏彦・花村憲一，ネット炎上に加担する個人属性に関する考察，第 69 回日本情報経営学会，ホテル日航八重山（沖縄），2014 年 11 月 9 日

⑥ 小津敦・竹村敏彦，クラウドコンピューティングの普及が我が国のマクロ経済に与える影響，第 31 回情報通信学会，大阪大学（大阪），2014 年 6 月 29 日

⑦ 竹村敏彦・小津敦，我が国のクラウドコンピューティング・ビッグデータの利活用の現状について，第 68 回日本情報経営学会，大正大学（東京），2014 年 5 月 24 日

〔図書〕（計 1 件）

① Takemura, T., Unethical Information Security Behavior and Organizational Commitment, Tsiakis, T., Kargidis, T., Katsaros, P. (Eds.), Approaches and Processes for Managing the Economics of Information Systems. IGI Global Publication, 2014, Chapter 11, 181-198

〔その他〕
ホームページ等
http://ecolab.eco.saga-u.ac.jp/

６．研究組織

(1)研究代表者

竹村　敏彦（TAKEMURA, Toshihiko）
佐賀大学・経済学部・准教授
研究者番号：00411504