様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月　 ６ 日現在

機関番号：１７２０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ０３６３１

研究課題名（和文）IoT社会における情報セキュリティとプライバシーに関する実証分析

研究課題名（英文）Empirical Analysis on Information Security and Privacy in IoT Society

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）　　3,500,000円

研究成果の概要（和文）：本研究では、アンケート調査などから得られた個票データを分析することにより、到来するIoT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1）サービス提供者（企業）のプライバシー管理をはじめとする情報セキュリティ対策のあるべき姿、および2）サービス利用者が持つべきプライバシー意識やリテラシーのあり方を明らかにした。研究の結果、IoTサービス普及に向けた施策の内容が異なることやIoTサービスに対する心理的影響が小さくないことなど、いくつか興味深いことが明らかになった。

研究成果の学術的意義や社会的意義
本研究は国内外ともに新しくセキュリティエコノミックスの進展にもつながることが予想される。これらの研究を行うことで、組織や個人レベルでプライバシー意識および情報セキュリティ対策に対する意識を向上することにもつながり、学術的のみならず実務的にも意義を持っている。また、本研究の成果は具体的な政府の政策についても議論でき、政策立案のための一つの材料となりうる。

研究成果の概要（英文）：In this research, we investigated the conditions needed in IoT (Internet of Things) society though the analyses using on micro data collected from our Web-based survey for firms (or organizations) and IoT users. We especially focused the issues for information security and privacy. We could obtain some interesting results; for instance, we estimate that the users' perceptions and the effect of the countermeasures differ for each type of IoT service, and we find that psychological factors effect toward IoT services.

研究分野：経済政策

キーワード：IoT　セキュリティ　プライバシー　QRコード決済サービス　TAM　情報漏洩　実証分析　インターネット調査

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

世の中に存在する様々なモノに通信機能を持たせ、インターネットに接続したり相互に通信させたりする技術である IoT（Internet of Things; モノのインターネット）の技術面からの研究蓄積は急速に進んでいる一方で、IoT サービスの利用者（ヒト）やサービス提供者などの組織に関する社会科学の視点からの研究は国内外ともに注目は浴びているものの、様々な課題があり、大きな進展はしていない。本研究では、経済学をはじめとする社会科学の視点でもって、到来する IoT（Internet of Things）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 1）サービス提供者（企業）のプライバシー管理をはじめとする情報セキュリティ対策のあるべき姿、および 2）サービス利用者が持つべきプライバシー意識やリテラシーのあり方を明らかにすべく、調査・分析等を行うに至った。

２．研究の目的

本研究の目的は、到来する IoT（Internet of Things）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 1）サービス提供者（企業）のプライバシー管理をはじめとする情報セキュリティ対策のあるべき姿、および 2）サービス利用者が持つべきプライバシー意識やリテラシーのあり方を明らかにし、有効かつ実現可能なエビデンスベースの情報セキュリティ政策の立案に資する情報等を提示することにある。そのために、実施するアンケート調査結果を構築する理論モデルに基づきデータ分析するとともに、これらの分析結果を研究者、実務家や政策実務家とで議論を行う。

本研究で行う実証分析は、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、公表されているデータを用いた分析も行っているが、主要な部分は、継続的に実施して収集・蓄積された Web アンケート調査結果（マイクロデータ）を用いた分析を行った。

以下、研究に関して簡単に説明する。

（１）アンケート調査の実施と収集・蓄積されたマイクロデータのデータベースの構築

本研究では、Web アンケート（インターネット）形式によって、IoT サービスを提供する側の企業（そこに所属する従業員や管理者）、ならびに IoT サービスを利用する個人、さらに近年注目を浴びているキャッシュレスの利用に関して個人を対象とした 3 種類のアンケート調査を実施した。1 つ目の調査は、これまで研究代表者（竹村敏彦）が経年的に実施してきたアンケート調査をベースとして、労働者としての情報セキュリティへの意識や行動に関する質問に加えて、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、回答者の行動経済学的要因等に関する 60 問以上にもわたる質問で構成された調査票でもって、実施された。また、2 つ目と 3 つ目の調査は、それぞれ IoT サービスの利用、QR 決済やクレジットカード決済の利用と情報セキュリティ意識、学歴、個人属性、行動経済学的要因等に関する 50 問程度の質問で構成された調査票でもって、実施された。

（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統計分析を行った。その際、心理学的要因をモデルに組み込みやすいミクロ経済学や行動科学の理論的フレームワークを採用し、また、統計手法としては、ロジット回帰分析や構造方程式モデリング、多重比較などを用いた。また、公表データである株価データについても適切な時系列分析などを採用して分析を行った。

（３）研究体制

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う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（平成 17 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、アンケート調査の企画・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、東京や大阪にて、研究期間を通じて、3 年間で約 20 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。そのため、国内外の学会・研究会などで報告し、それを査読付学術雑誌に投稿するだけでなく、竹村敏彦（研究代表者）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、個人や組織を特定化できる情報を除き、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

ここでは、本研究を通じて明らかになったことを、紙面の都合上、その一部を紹介する。詳細については、発表論文などを参照されたい。

（１）IoT 利用におけるセキュリティ、プライバシー、利便性の関係に関する分析

本研究では、IoT サービスの普及のための条件を調べるために、技術受容モデル（TAM: Technology Acceptance Model）に基づき IoT 利用（意図）に関するモデル（図 1）を提案した。このモデルは Kim, et al. (2008)を参考にして構築されたものである。IoT 利用意図に直接的に影響を与える要因として、プライバシーリスクの認知、セキュリティリスクの認知、IoT の利便性があり、プライバシーリスクとセキュリティリスクは相互に影響しあうといった特徴を有している。また、これらのリスクは IoT の利便性にも影響を与える（つまり、これらのリスクは直接的のみならず、間接的にも IoT 利用意図に影響を与えていることになる）。なお、図 1 にある（＋）は正の影響を与えること、（－）は負の影響を与えることを意味している。

このモデルを検証するために、「防犯サービス」と「予防医療サービス」の 2 つのサービスを想定して回答を求める実施したアンケート調査を実施し、その収集された回答データを用いて構造方程式モデリング（SEM: Structural Equation Modeling）と呼ばれる手法でもって分析を行っている。

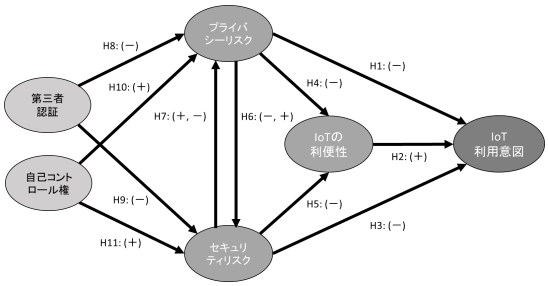
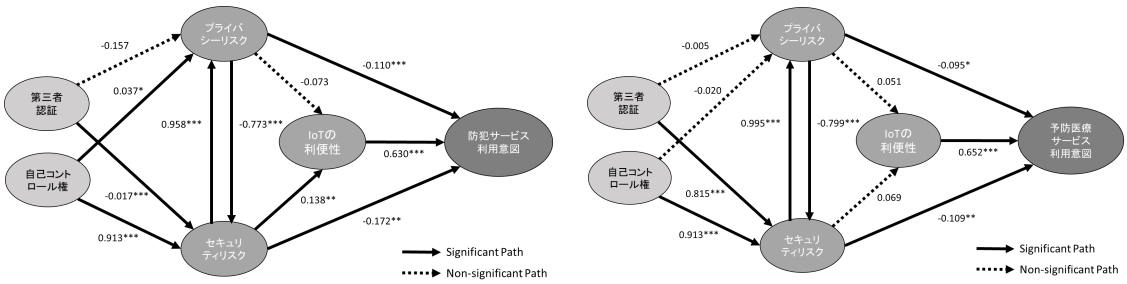


図 1：IoT 利用モデル

図 2 には、それぞれの SEM の分析結果を示している。図 2 を比較してわかるように、提供されるサービスの内容によって、3 つの要素間の関係が異なる。予防医療サービスの場合、プライバシーリスク認知、セキュリティリスク認知のいずれも IoT サービスの利便性には影響を与えない。一方で、防犯サービスの場合、セキュリティリスクのみ IoT サービスの利便性に影響を与えている。また、プライバシーリスクとセキュリティリスクは相互に影響を与えていることがわかる。このことから、IoT サービス内容によってプライバシーリスク認知、セキュリティリスク認知、利便性の関係が異なることから、IoT サービス普及に向けた施策の内容が異なることが示唆される。



(a) 防犯サービス　　(b) 予防医療サービス

図 2：分析結果 I

本研究の詳細は、Ando, et al. (2016)を参照されたい。

（文献）Kim, D.J., Ferrin, D.L., Rao, H.R., A Trust-Based Consumer Decision-Making Model in Electronic Commerce: the Role of Trust, Perceived Risk, and Their Antecedents, Decision Support Systems, Vol.44, No.2, 544-564, 2008.

（２）情報漏洩につながる行動に関する分析

本研究では、情報セキュリティの観点から問題となる行動の中でも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仮説を立て（図 3）、その検証を行っている。この結果を踏まえて、情報漏えいにつながる行動を防止・抑止するために組織（情報セキュリティ管理者）がとるべき施策について考えている。

図 3 には、分析で用いた要因（コンプライアンス意識、不正・違反放置の風土、職場におけるトラストなど）とそれぞれの要因の関係がまとめられている。

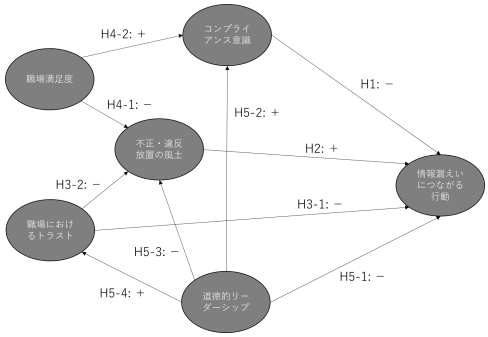


図 3：行動モデル

アンケート調査結果と SEM を用いた分析結果（図 4）、不正・違反放置の風土の改善が情報漏えいにつながる行動に対して最も大きな直接的な影響を与える要因であることが確認された. また、情報漏えいにつながる行動を抑止させる効果が期待される要因であるコンプライアンス意識の向上、職場におけるトラストの形成、職場満足度の向上も情報漏えいにつながる行動を抑止することには貢献するが、その影響度はそれほど大きくないことが確認された。

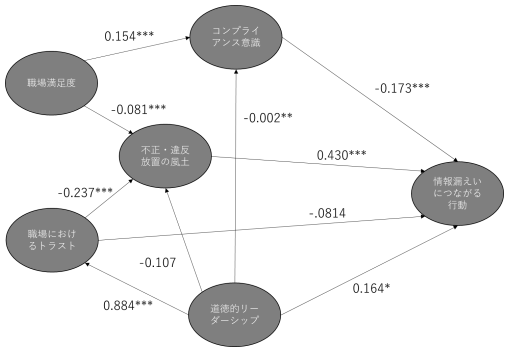


図 4：分析結果 II

このことから、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・違反放置の風土を改善すること（職場環境の改善）が最も大きな効果があることが示唆された。また，コンプライアンス意識の向上は不正・違反放置の風土の改善に次ぎ，大きな効果があることがわかった。さらに、不正容認風土に影響を与える要因として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ことが期待される。

本研究の詳細は、竹村・島 (2016)を参照されたい。

（3）SNS における情報開示行動に関する要因分析

本研究は、個人が SNS 上で「帰属組織に関する機密情報を開示する行動（以下、情報開示行動）」にいたる要因（ユーザへの信頼、情報開示範囲のコントロール、リスク認知や SNS で繋がっている人数など）について行動科学的アプローチにより分析を試みたものである（図 5）。

図 5 で示したモデルを、アンケート調査結果と階層的重回帰分析により検証したところ、表 1 の分析結果が得られた。表 1 を見てわかるように、「コンプライアンス意識」「匿名・非匿名利用」は情報開示行動に影響を与えないが、「ユーザへの信頼」「情報開示範囲のコントロール」「リスク認知」「自己顕示欲」「SNS で繋がっている人数」は情報開示行動に影響を与えることを確認できた。そして、標的型攻撃の未然防止に関して少しでも貢献するためには、「リスク認知」や「情報管理に関する知識」を高める演習や教育を実施することが望ましいとの示唆を与えている。

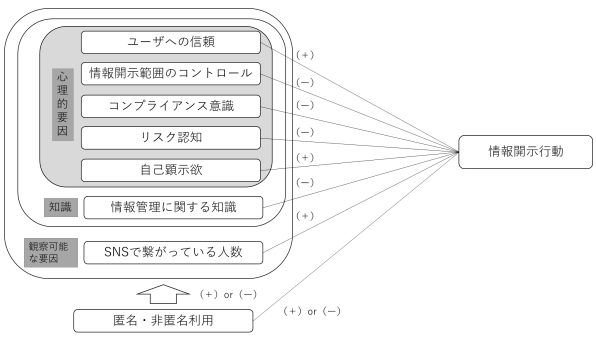


図 5：情報開示行動モデル

表 1：階層的回帰分析の結果

	ステップ 1			ステップ 2		
	係数	t-value	β 係数	係数	t-value	β 係数
ユーザへの信頼	0.282***	7.130	0.254	0.276***	5.540	0.248
情報開示範囲のコントロール	−0.358***	−8.330	−0.297	−0.326***	−6.190	−0.271
コンプライアンス意識	0.018	0.500	0.017	0.011	0.270	0.010
リスク認知	−0.068*	−1.860	−0.063	−0.095**	−2.130	−0.087
自己顕示性	0.196***	5.400	0.190	0.150	3.330	0.146
情報管理に関する知識	−0.082***	−2.740	−0.076	−0.058	−1.560	−0.054
ln(繋がっている人数)	0.030*	1.600	0.042	0.050**	2.130	0.071
匿名ダミー				0.290	1.510	0.137
匿名ダミー × ユーザへの信頼				−0.013	−0.160	−0.008
匿名ダミー × 情報開示範囲のコントロール				−0.101	−1.110	−0.052
匿名ダミー × コンプライアンス意識				0.025	0.300	0.012
匿名ダミー × リスク認知				0.077	0.960	0.040
匿名ダミー × 自己顕示性				0.104	1.370	0.065
匿名ダミー × 情報管理に関する知識				−0.064	−1.030	−0.061
匿名ダミー × ln(繋がっている人数)				−0.040	−1.000	−0.076
（定数項）	0.022	0.230		−0.119	−0.970	
観測数	853			853		
F-value	$F(7,845) = 87.10$***			$F(15,837) = 41.62$***		
Adj R-squared	0.414			0.417		
R-squared	0.419			0.427		
Δ R-squared				0.0081		
(F-value)	2.58*			1.48		

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

本研究の詳細は、小川・安藤・島・竹村（2017)を参照されたい。

（４）QR コード決済サービス普及に関する分析

本研究は、今後日本において普及する FinTech サービスの一つである QR コード決済サービスに注目し、このサービスに関する TAM によるモデリングおよびそのモデルの検証を試みた（図 6)。分析の結果、QR コード決済サービスに関する TAM の妥当性などが示された（表 2)。続いて、地域別・年齢層別にみて、分析モデルの構造が変わるか否かの検証を行った。その結果、本研究における分析モデルの構造は概ね異なることはなかったが、利用意図に影響を与える要因の影響度合いが地域別･年齢層別によって異なることを確認している（表 2 は全体の結果である)。

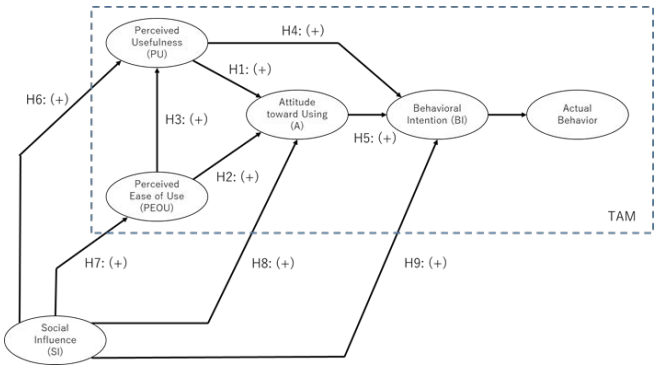


図 6：QR コード決済サービスの分析モデル

表 2：SEM による分析結果

仮説	標準化係数	標準誤差	z値	p値
H1　知覚された有用性 ⇒ 利用への態度	0.2365	0.0309	7.65	0.000
H2　知覚された使いやすさ ⇒ 利用への態度	0.0831	0.0274	3.03	0.002
H3　知覚された使いやすさ ⇒ 知覚された有用性	0.5775	0.0298	19.35	0.000
H4　知覚された有用性 ⇒ 利用への行動意図	0.4088	0.0335	12.21	0.000
H5　利用への態度 ⇒ 利用への行動意図	0.3684	0.0518	7.11	0.000
H6　社会的影響 ⇒ 知覚された有用性	0.2290	0.0233	9.85	0.000
H7　社会的影響 ⇒ 知覚された使いやすさ	0.5802	0.0271	21.38	0.000
H8　社会的影響 ⇒ 利用への態度	0.7671	0.0241	31.84	0.000
H9　社会的影響 ⇒ 利用への行動意図	0.2982	0.0499	5.97	0.000

本研究の詳細は、竹村他（2018)を参照されたい。

（５）プライバシー情報の価値の測定に関する分析

本研究は、仮想的な状況（何らかの理由で自らのプライバシー情報が漏えいしたときに、金銭的な実被害額を全額保証した上で、支払われる慰謝料をいくらくらい要求するかという状況）を想定し、コンジョイント分析を行うことにより、個人のプライバシー情報（氏名・住所・性別・生年月日）の価値の測定を試みた。属性として用いた「慰謝料」「精神的被害」「実被害」

および企業の対応（「金券」「詫び状」「HP」）の係数はいずれも統計的に有意となり、それぞれのコンジョイントカードで設定されている選択肢の効用に影響を与えていることがわかった（表 2）。この結果を用いて限界支払意思額を計算したところ、精神的被害を貨幣価値で測ると約 15486 円、実被害については約 37407 円になった。また、企業の対応について見てみると、500 円の金券を送るよりも、詫び状を送ったりする方が個人にとって高い評価をしていることなども明らかになった。

本研究の詳細は、竹村他（2019)を参照されたい。

表 2：コンジョイント分析の結果

		coef	exp(coef)	se(coef)	z	p
ASC		-0.283	0.754	0.038	-7.42	1.20E-13
慰謝料		0.012	1.013	0.000	43.49	<2.00E-16
精神的被害		-0.193	0.824	0.008	-24.73	<2.00E-16
実被害		-0.466	0.627	0.010	-45.61	<2.00E-16
企業の対応	金券	0.290	1.337	0.026	11.38	<2.00E-16
	詫び状	0.408	1.503	0.025	16.20	<2.00E-16
	HP	0.276	1.318	0.025	10.94	<2.00E-16
	対応無し	0.000				

Likelihood ratio test=8016 on 7 df, p=< 2e-16,
n=111240, number of events=37080

５．主な発表論文等

〔雑誌論文〕（計 10 件）

① 竹村敏彦・武田浩一「FinTech と株価反応に関する一考察～FF5 ファクター・モデルによる検証～」CRES Working Paper Series，査読無，2019，No.FY2018-07，1-14
② 竹村敏彦・神津多可思・武田浩一・末廣徹「地域別・年齢層別に見た FinTech サービス普及に関する分析－QR コード決済サービスを一例として－」CRES Working Paper Series，査読無，2018，No.FY2018-01，1-18
③ 竹村敏彦・神津多可思「新聞記事とニュースリリースから見る地方銀行の FinTech への取組みについての動向分析」CRES Working Paper Series，査読無，2017，No.FY2017-06，1-15
④ 竹村敏彦・野方大輔・武田浩一「FinTech に関するニュースリリースは株価に影響を与えるか?～FF3 ファクターモデルによる検証～」ICES Discussion Paper，査読無，2018，No.17-J-001，1-22
⑤ 小川隆一・安藤玲未・島成佳・竹村敏彦「SNS における情報開示行動に関する要因分析」情報処理学会論文誌，査読有，2017，第 54 巻第 12 号，1890-1900
⑥ Ando，R.，Shima，S.，Takemura，T.，Analysis of Privacy and Security Affecting the Intention of Use in Personal Data Collection in an IoT Environment，IEICE TRANS. INF. & SYST.，査読有，2016，Vol.E99-D，No.8，1974-1981

他、4 本。

〔学会発表〕（計 9 件）

① 小山明美・小川隆一・竹村敏彦「IT サプライチェーン上の情報セキュリティリスク認識に関する分析」2019 年暗号とセキュリティシンポジウム（SCIS2019）琵琶湖大津プリンスホテル 2019 年 1 月 25 日
② 竹村敏彦・片山佳則・鳥居悟・古川和快「プライバシー情報の価値の測定」2019 年暗号とセキュリティシンポジウム（SCIS2019）琵琶湖大津プリンスホテル 2019 年 1 月 24 日
③ 竹村敏彦「QR コード決済サービス利用に関する実証分析」第 76 回日本情報経営学会全国大会、久留米大学、2018 年 6 月 17 日
④ 竹村敏彦・島成佳「情報漏洩につながる行動に関するデータ分析」2018 年暗号とセキュリティシンポジウム（SCIS2018）朱鷺メッセ、2018 年 1 月 24 日
⑤ 渡辺正文・島成佳・竹村敏彦「組織の公開連絡先に送られた攻撃メールの単語に注目した分析」2017 年暗号とセキュリティシンポジウム（SCIS2017）ロワジールホテル那覇、2017 年 1 月 26 日
⑥ 田村滋基・小川隆一・竹村敏彦「悪意のある投稿をする人の特性分析」2017 年暗号とセキュリティシンポジウム（SCIS2017）ロワジールホテル那覇、2017 年 1 月 24 日

他、3 本。

〔その他〕

ホームページ等

① http://ecolab.eco.saga-u.ac.jp/
② 竹村敏彦「現場無視の対策に落とし穴 適切な対応で生産性も上がる～セキュリティー対策と行動経済学」日経ビジネス（2017 年 1 月 23 日号），80-81