情報セキュリティインシデント被害と
組織コミットメントの関係についての実証分析

竹島　健人
竹村　敏彦

Working Paper Series Vol.FY2016-09
2017 年 3 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

An Empirical Analysis on the Relation between Information Security Incident Damages and Organizational Commitment[¶]

Kento TAKESHIMA[*]
Toshihiko TAKEMURA[†]
Faculty of Economics, Saga University

Abstract

Regardless of existence of various technologies for the information security incident damages which aim to get information and money from individuals and/or organizations, it is reported that the number of cases of the damages does not decrease. It is pointed that many of these problems deeply relate to human errors. In this article, we test whether or not behavioral economic factors and organizational commitments affect to the number of the information security incident damages through the data analysis. As a result, we found that "overconfidence," which is one of behavioral economic factors, affects to the number of the damages. In addition, we suggest the considerable measures in the organizations.

Key Words: Information Security Incident Damage, Organizational Commitment, Behavioral Economics, Web-based Survey

---

[¶] This article revised the graduation thesis titled "About the Relation between Information Security Incident Damages and Organizational Commitments" (Kento Takeshima) submitted to Faculty of Economics, Saga University.

A part of this work was supported by the Japan Society for the Promotion of Science: Grant-in-Aid for Scientific Research (C) (16K03631).

[*] Undergraduate Student, Faculty of Economics, Saga University
[†] Associate Professor, Faculty of Economics, Saga University
Corresponding to tosihiko@cc.saga-u.ac.jp

情報セキュリティインシデント被害と組織コミットメントの関係についての実証分析[¶]

佐賀大学経済学部　竹島 健人[*]
佐賀大学経済学部　竹村 敏彦[†]

要旨

個人や組織の情報や金銭を狙う情報セキュリティインシデントに対する様々な技術が存在するにも関わらず、情報セキュリティインシデント被害の件数は依然として減っていると報告されている。この問題の多くにはヒューマンエラーが深く関わっていることが指摘されている。本稿では、行動経済学的要因と組織コミットメントが情報セキュリティインシデント被害に影響を与えるか否かを、データ分析を通じて、検証する。その結果、行動経済学的な要因の一つである自信過剰が情報セキュリティインシデント被害に影響を与えることなどを確認している。そして、組織が考えるべき対策について提案を与えている。

キーワード：情報セキュリティインシデント被害、組織コミットメント、行動経済学、Webアンケート調査

[¶] 本稿は、佐賀大学経済学部に提出した卒業論文「情報セキュリティインシデント被害と組織コミットメントの関係について」（竹島健人）を加筆修正したものである。

本稿の一部は、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。

[*] 佐賀大学経済学部・学部生

[†] 佐賀大学経済学部・准教授

Corresponding to tosihiko@cc.saga-u.ac.jp

1. はじめに

インターネットが生活に広く普及した現在、個人の利便性は比較的に向上している。しかしながら、コンピュータウイルスやスパイウェアの感染、ワンクリック詐欺など、様々な情報セキュリティ上の脅威がインターネットユーザの身近にあることも事実である。例えば、スパイウェアの中には、表立って情報を盗まず、ユーザが気づかないうちに情報を盗み出すものもあるため、様々な問題を引き起こしている。安藤・島(2014)は、サイバー攻撃の一つであるターゲット型攻撃の脅威は増大傾向にあり、マルウェアの中のスタックネットは重要な情報を盗むだけでなく、制御系システムにまで攻撃を行ったことを指摘している。情報処理推進機構 (2016)によれば、トレンドマイクロ社によると新しいマクロウイルスが 2015 年第 4 半期に 2 万 8000 件となり、前 4 半期から約 3.3 倍増加したことが報告されている。不正プログラム検出数は約 13 万にまで年々増加している。さらに、総務省 (2016)によれば、平成 27 年度においてセキュリティ侵害を受けた企業の割合は低下しているものの、「セキュリティ対策の確率が困難」などのセキュリティ面での問題点を回答した企業の割合は 44.2%に増加していることが明らかになっている。これらのことからもわかるように、IT システム上の脅威は今まで以上に高度化・多様化しており、情報セキュリティ対策が重要になっている。

情報セキュリティ上の脅威に対抗するために、技術的な対策として、インシデントに対抗・予防するためのソフトウェアやハードウェアを導入し、それは有効な手段となっている。この他にも、情報セキュリティ対策としては、情報セキュリティの脅威についての教育・とレーニングの実施や、除法セキュリティマネジメントの導入など、多岐に渡るものがある。それゆえに、個人が自力でインシデント被害を提言することには限界があるとも言える。

本稿では、近年インシデント被害への対策が進んでいるにも関わらず、被害件数が減らないのは、技術的な対策が不十分ということではなく、人間そのもの、ならびにそこ個人を取り巻く（職場）環境に原因があるのではないかと考える。ゆえに、人間の非合理性ならびに職場環境に視点を当てた分析を行う。具体的には、本稿で考える行動モデルに行動経済学に関する要因を加える。行動経済学では、完全に合理的な個人を前提としている従来の経済学とは違って、心理学の視点が組み込み、非合理的な個人を前提として人間の行動を分析する学問である。例えば、日本年金機構の個人情報流出事件を例に挙げると、この事件では、年金機構のデータが外部からのコンピュータウイルスによって約 125 万件流出し、その原因の一つとして職員がパスワードの無設定を放置していたため、情報内容の流出に繋がったことが指摘されている（産経ニュース, 2015)。この事件は、人間が非合理的だからこそ、生じたものと考えられる。人間が合理的であれば、情報流出が生じるリスクを警戒し、無設定を放置することはないだろう。このような非合理的な人間の特徴を踏まえるために、行動経済学的要因を行動モデルに組み込むことにする。また、もう一つの重要なキーとなる要因として、組織コミットメントを用いる。組織コミットメントは、簡単に言うと、組織との関わ

り方のことである。この組織コメットメントを高めることで得られる効果を示したものとして太田（2012)などがある。太田（2012)は、組織コメットメントを高めることによって、離職率を減らすことができることを示している。また、生き生きとした職場づくり、さらに、企業の売り上げにも組織コメットメントはプラスに作用することを示している。加えて、関口他（2014)は、組織コメットメントを高めることによって、職務成果など、組織にとって望ましい結果を得ることができると指摘している。さらに、北野（2014)によると、組織コミットメントが強い場合は情報に対する内部不正行為が起こりにくいことを指摘している。そして、倉谷・城戸（2006)によると、情動的、規範的コミットメントを高めることは、積極的な行動である、達成・挑戦志向の行動や組織市民行動をもたらすことを指摘している。これらの研究からもわかるように、組織コメットメントを高めることによって得られるメリット・効果には様々なものがある。組織コミットメントを高めることで組織は情報セキュリティ意識の向上させることが期待でき、その結果、情報セキュリティインシデント被害を抑制することに繋がることを明らかにすることが期待できるかもしれない。

本稿の目的は、情報セキュリティインシデント被害と組織コミットメントや行動経済学的要因の関係を明らかにし、情報セキュリティインシデント被害への提案を行うことである。そのために、2016 年 2 月に実施された「労働者の情報セキュリティ意識等に関する調査」の個票データを用いて分析を行う。その分析結果を踏まえて、有効となる情報セキュリティインシデント対策を提案したい。

本稿の構成は以下の通りである。第 2 節では関連研究を紹介する。第 3 節において本稿で考える概念モデルの説明ならびに、分析で用いるアンケート調査の概要を示す。第 4 節では分析結果を示し、考察を行う。第 5 節において分析結果を踏まえた提案を行い、第 6 節において本稿のまとめを与える。

2. 関連研究

本節では、情報セキュリティインシデント被害に関する研究を簡単に紹介する。例えば、情報セキュリティ分野と人間の特性について分析をしているものとして内田（2008)がある。内田（2008)では、他からの影響により、何らかの承諾をしてしまう人間の特質は 6 つ（返報性、コミットメントと一貫性、社会的証明、好意、権威、希少性）があり、これらを誰が、どのように利用するかによって、情報セキュリティの脆弱性にも、強化にもなることと示している。さらに、情報セキュリティ分野で生じる事件や事故の原因は必ずしも個人の問題だけで発生するものではなく、「無責任の構造」を生み出す組織特性の是正が必要だということも指摘している。

情報セキュリティインシデントとヒューマンエラーについて分析しているものとして新原・原田（2014)がある。新原・原田(2014)は、国内で発生している情報セキュリティインシデント被害の約 87%がヒューマンエラーに起因していると示している。また、ヒューマ

ンエラーの対策として「時系列事象関連図の作成」「問題点の抽出」「問題点の背後要因の探索」「考えられる対策の列挙」「実施可能な対策の決定」「対策の実施」「実施した対策の評価」があり、この対策を実施することにより、ヒューマンエラー低減に一定の効果があることを示唆している。

情報セキュリティインシデント被害者の属性について分析をしているものとして、花村他（2012)がある。花村他（2012)は、情報セキュリティインシデント被害を「ウイルス」「フィッシング詐欺」「架空請求」「不正利用」の 4 つに分けて、それらに影響を与える要因について分析している。その結果、個人が自信過剰であれば「フィッシング詐欺」や「不正利用」に遭遇する傾向が高まることが明らかにされている。さらに、花村他（2012)では、個人に対して、情報収集・処理能力および意識的なセキュリティ対策を実施することによって、インシデント被害への遭遇確率を低下させることができることもあわせて指摘されている。

この他にも、竹村他（2017)は情報セキュリティインシデント被害につながる意図的に情報セキュリティポリシー違反をする意識について分析を行っている。竹村他（2017)によれば、セキュリティポリシー違反をした際にペナルティを与えることは必ずしもセキュリティポリシー違反を減らすことには繋がらないことが明らかにされている。また、コンプライアンス意識を向上させる教育・トレーニングの機会を増やすことができれば、セキュリティポリシー違反を防止・抑止する効果が得られるとも指摘している。

3. フレームワーク

3.1 概念モデル

本稿では、企業において情報セキュリティインシデント被害に遭う人はどのような人かを検証するために図 1 に示すような概念モデルを考える。先述したように、組織コミットメントと行動経済学的要因が情報セキュリティインシデント被害に与える影響について分析を行う。以下、図 1 に示した要因（組織コミットメント（愛着要素、内在化要素、規範的要素、存続的要素)、リスク回避度、近視眼的尺度、自信過剰、その他の基本属性）における仮説などについて説明を行う。

(1) 情報セキュリティインシデント被害

本稿では、情報セキュリティインシデント被害として、花村他（2012)にならい、「ウイルスやワーム、スパイウェアへの感染」「フィッシング詐欺」「ワンクリック詐欺」の 3 つをとりあげ、それぞれを被説明変数とする。

(2) 組織コミットメント

田尾（1997)では、組織コミットメントとは「愛着要素」「内在化要素」「規範的要素」「存続的要素」の 4 因子に分かれることが示されている。本稿でも田尾(1997）に基づき、この

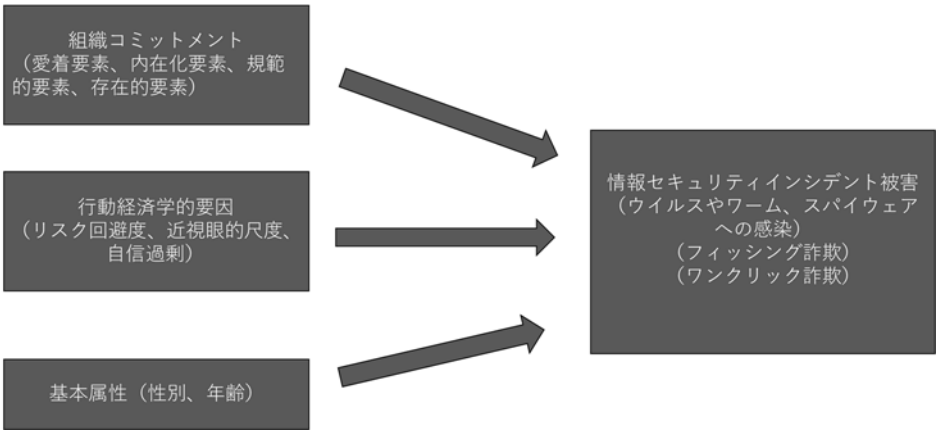

図 1: 概念モデル

4 つの因子を用いて分析を行う。以下、これらの因子について簡単に説明していく。

(a) 愛着要素

愛着要素とは、会社に対して情緒的な愛着を感じている程度を表すものである。企業に対して愛着があればあるほど、情報セキュリティインシデント被害に遭わないために警戒するはずであるため、その結果として情報セキュリティインシデント被害に遭いにくくなると考えられるため、本稿では「愛着要素が高いほど、情報セキュリティインシデント被害に遭いにくい」という仮説を立てる。

(b) 内在化要素

内在化要素は、会社の価値が自分の価値と一致しており、会社のために尽力したいという意識を表すものである。会社に尽力したいと思う人ほど、熱心に仕事を行うと考えられるため、本稿では「内在化要素が高いほど、情報セキュリティインシデント被害に遭いにくい」という仮説を立てる。

(c) 規範的要素

規範的要素は、周囲の目が気になる意識、会社を辞めるべきではないという意識のことを表す。情報セキュリティインシデント被害を起こした場合に、周囲からの注目を受けること、結果的に会社を辞めさせられてしまうことを嫌い、それを考慮して働くと考えられることから、本稿では、「規範的要素が高いほど、情報セキュリティインシデント被害に遭いにくい」という仮説を立てる。

(d) 存続的要素

存続的要素は辞めることに伴うコストに基づいた帰属意識を表すものである。情報セキュリティインシデント被害が原因で会社を辞め、給料もなくなり、社会的信用も減ることを

避け、情報セキュリティインシデント被害を気にしながら働くはずだと考えられるため、「帰属意識が高いほど、情報セキュリティインシデント被害に遭いにくい」と仮説を立てる。

(3) 行動経済学的要因

行動経済学的要因として、「リスク回避度」「近視眼的尺度」「自信過剰」を採用する。以下、これらについて説明していく。

(a) リスク回避度

リスク回避度とは簡単に言うと、個人のリスクを避けたい傾向（リスクに対しての態度）を示す。情報セキュリティ行動（情報セキュリティの観点から問題となる行動）を取り扱った分析をしている Takemura (2014)では、リスク回避度は個々の情報セキュリティ行動と関係があることを指摘している。このことから、日頃からリスクに対して寛容となっていれば、情報セキュリティインシデント被害に対しても寛容となってしまうことが予想される。そのため、本稿では「リスク回避度が高いほど、情報セキュリティインシデント被害に遭いにくい」という仮説を立てる。

(b) 近視眼的尺度

近視眼的尺度とは、目先の利益にとらわれてしまう、つまり直感的であるという概念であり、未来結果熟慮は、近視眼的尺度と逆の意味を持つ概念である。第 1 節で上述した日本年金機構の情報漏えいでは外部からの攻撃を認識したが報告を怠ったために問題が生じたことを取り上げた。この問題は未来の結果をよく考える意識があれば、情報漏えいは起こらなかったのではないかと考えられる。また、Takemura and Komatsu (2013)は、未来結果熟慮は情報セキュリティ行動に影響を与えることを明らかにしている。これらのことを踏まえて、本稿では「近視眼的であればあるほど、情報セキュリティインシデント被害に遭いやすい」という仮説を立てる。

(c) 自信過剰

客観的な知識が豊富であっても、人間の行動心理が影響することで、必ずしも正しい判断を下せるとは限らないといわれている。「自信過剰度」は客観的な知識と主観的な知識の乖離を表す指標の一つとして用いられている。本稿では、花村他 (2012)に基づき、「自信過剰であればあるほど、情報セキュリティインシデント被害に遭いやすい」と仮説を立てる。これは、自信過剰であれば自らの持っている情報セキュリティ知識を過信してしまい、情報セキュリティインシデント被害に遭いやすくなると考えられるからである。

(4) 基本属性（性別・年齢）

情報セキュリティインシデント被害に影響を与える要因（デモグラフィック属性）として、

性別と年齢を使用する。仮説としては、「性別によって情報セキュリティインシデント被害のあいやすさが異なる」「年齢によって情報セキュリティインシデント被害のあいやすさが異なる」というものを考える。

3.2 調査票の概要

本稿の分析では、2016 年 2 月に実施された「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）によって収集された個票データを利用する。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であり、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を利用している一般的な労働者である。

2016 年調査は、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時間に比べて回答時間が早い者を不良回答者取り扱いサンプルから外している。有効回答数は 1,236 人のであった。調査対象者の構成は表 1 の通りである。

表 1: 有効回答数

		#	(%)
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 以上	334	27.02

4. 分析

4.1 要因の加工・作成

ここでは、分析に用いる被説明変数および説明変数、またその加工方法について簡単に説明する。

(1) 過去 2 年間の情報セキュリティインシデント被害の経験

2016 調査には「過去 2 年間で、あなたご自身はパソコンやインターネットを利用していて、以下のようなトラブル（未遂も含む）に遭遇したことがありますか。該当するものをそれぞれお選びください。」という質問がある。本稿では、その項目の中から、「ウイルスやワーム、スパイウェアへの感染」、「フィッシング詐欺」、「ワンクリック詐欺（ツークリック詐欺などの類似のものを含む）」の 3 つを選択し、その回答として「ある」「ない」「わからない」のうち、「ある」と回答した者を分析対象とする。さらに、「トラブル（未遂を含む）に遭遇した回数で該当するものをそれぞれお選びください。」という質問をあわせて行っており、被害にあった場合、その遭遇した回数も調べることができる。表 2 では、それぞれの情報セキュリティインシデント被害への被害経験の有無に被害を受けた回数ついての人数を表している。

表 2: 有効回答数

	被害の回数				
	なし	1 回	2〜5 回	6〜10 回	11 回以上
ウイルスやワーム、スパイウェアの感染	955	67	50	4	5
フィッシング詐欺	1022	22	14	2	1
ワンクリック詐欺	1003	32	17	2	3

(2) リスク回避度

2016 年調査では BDM 法（Becker et al.,1964）に基づく価格付けによってリスク回避度を測定している。調査では、「100 分の 1（1%）の確率で当たり、当たった場合には 100 万円もらえますが、外れた場合には何ももらえない宝くじがあったとします。あなたがこの宝くじを購入するとして、(最大) ひとくちいくらくらいまで支払っていいと思いますか。」という質問を行っている。これは、不確実な収益をもたらす財の確実等価額をたずねる質問である。その回答結果を用いて、個人のリスク回避度を式(1)によって計算している。

$$\mathrm{RA} = \frac{az-p}{\frac{1}{2}\times(az^2-2az+p^2)} \qquad (1)$$

ここで、RA はリスク回避度、Z はくじの賞金 a は当選確率、p は回答者がくじにつけた価格を表している。

図 2 には、算出された回避度を値の分布を示している。さらに、見やすくするために、その値の大きさによって 3 段階に分けている。値が正であればリスク回避的、値がゼロであればリスク中立、値が負であればリスク愛好的としている。よって、図 2 から、回答者の大半がリスク回避的であることがわかる。

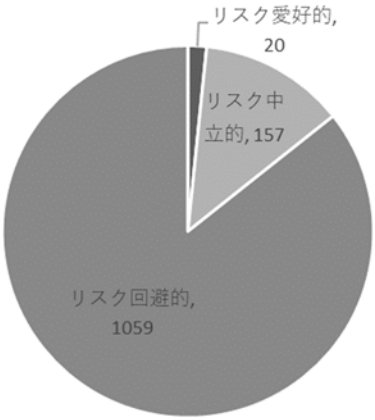

図 2: リスク回避度の分布

(3) 近視眼的尺度

2016 年調査では「以下のことは、あなたご自身にどのくらい当てはまりますか。それぞれ選択肢の中からあなたの考えに最も近いものを 1 つずつお選びください。」という質問に続き、「将来どうなるだろうと考え、毎日の行動で将来に影響を及ぼそうとする」や、「将来のことはなるようになるので、すぐ目の前の関心ごとだけを片付けようとする」などが提示され、それらに対して「当てはまる」から「当てはまらない」の 5 段階のリッカード尺度でもって回答を求める形をとっている（井上・有光, 2007)。これらの質問項目に対する回答データを用いて因子分析を行い、そこから計算される因子得点（スコア）でもって「近視眼的尺度」を定義する。なお、因子分析の結果については第 4.2 節で示す。

(4)（知識に関する）自信過剰度

2016 年調査では、(フィッシング詐欺等の 3 種類に対して、その概要や特徴に関する説明が正しいか間違っているかを問うクイズをそれぞれ 3 問ずつ用意している。これらのクイズに対して、「正しい」「間違っている」「わからない」から選択する形式をとり、正解であれば 1 点、それ以外であれば 0 点を付与した。これらのクイズの得点により、客観的な知識が測定できる。続いて、「インターネット上で発生している情報セキュリティへの攻撃・脅威などについておうかがいします。あなたは、次のようなインターネット上の攻撃・脅威に関する事例をご存じですか。」の（主観的）知識を尋ねる質問に対して、上記と同様に 3 種類のインシデントについて「名前も概要も知らない」「名前を聞いたことがある程度」「概要をある程度知っている」「詳しい内容を知っている」から選択してもらう形式をとっている。そして、「名前も概要も知らない」と回答したときに 0 点、「詳しい内容を知っている」と回答したときに 3 点を付与している。そして、客観的な知識と主観的知識（認知）の得点の乖離を自信過剰の程度として本稿では定義する。この得点差が正の値をとれば、主観的知識が客観的知識を上回っており、自信過剰であると判断する。図 3 を見てわかるように、自

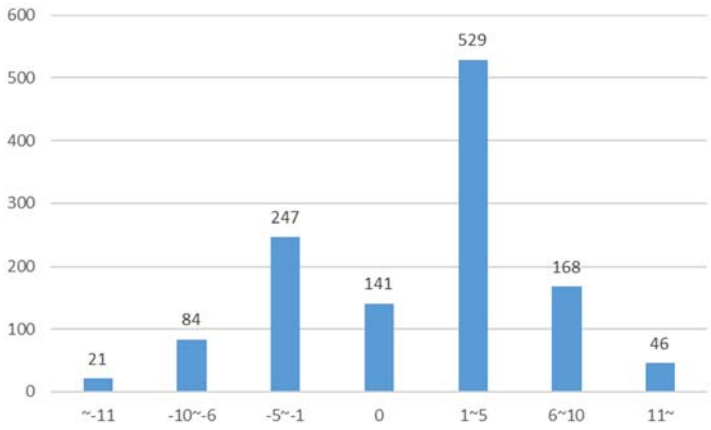

図 3: 自信過剰度の分布

信過剰度がゼロに集中していることから、回答者の多くは自信過剰ではないことがうかがえる。

(5) 組織コミットメント

2016 年調査では「再度、あなたの職場（会社）についてどのように思いを抱いているかについておうかがいします。あなたの考えに最も近いものをそれぞれ 1 つずつお選びください。」と質問している（各質問項目に対しては「そう思う」から「そう思わない」の 5 段階のリッカード尺度でもって回答を求めている）。これらは田尾（1997)で用いられている質問項目を用いており、第 3.1 節で説明した 4 つの要因を測るものである。これらの質問の回答データに対して回帰分析を行い、そこから計算される因子得点を用いて「愛着要素」「内在化要素」「規範的要素」「存続的要素」を定義した。

(6) 基本属性

性別に関しては、男性であれば 0、女性であれば 1 を付与するダミー変数として定義している。

4.2 分析結果

本稿では、分析手法として因子分析とロジット分析を行った、以下その結果などについて説明していく。

(1) 因子分析

因子分析とは、変数同士の相関関係から変数の背後にある共通要因を推定しようとする分析手法であり、心理学の分野で多用されている。因子分析について、詳しくは石黒（2014）などを参照されたい。なお、本稿では一因子モデルを採用している。

因子分析に先駆けて、「近視眼的尺度」および「愛着要素」「内在化要素」「規範的要素」「存続的要素」に関して、それぞれの尺度の内的整合性を確かめるために、クロンバックの α 係数を調べた。その結果を表 3 に示している。それぞれの α 係数は「近視眼的尺度」が 0.7423、「愛着要素」が 0.8774、「内在化要素」が 0.8944、「規範的要素」が 0.8147、「存続的要素」が 0.6717 という結果が得られた。Hair, et al. (1998)によると、α 係数として 0.6 以上であればその要因の信頼性は高いと考えられている。ゆえに、これらの尺度は内的整合性があると判断することができる。

表 3: クロンバックの α 信頼性係数

	質問項目数	α
近視眼的尺度	12	0.742
愛着要素	6	0.877
内在化要素	9	0.894
規範的要素	5	0.815
存続的要素	4	0.672

続いて、「近視眼的尺度」「愛着要素」「内在化要素」「規範的要素」「存続的要素」に関して因子分析行った（因子分析の結果は紙面の都合上、省略する）。因子分析の結果から因子得点を計算した。いずれの要因も計算された数値が大きくなるほど、その要因の名前の傾向が高くなることを意味する。例えば、近視眼的尺度の場合、数値が大きいほど、近視眼的傾向が強いことを意味する。これらの要因の分布を図 4 から図 8 に示す。いずれもピークが一つだけの分布となっており、正規分布に近いことが見て取れる。

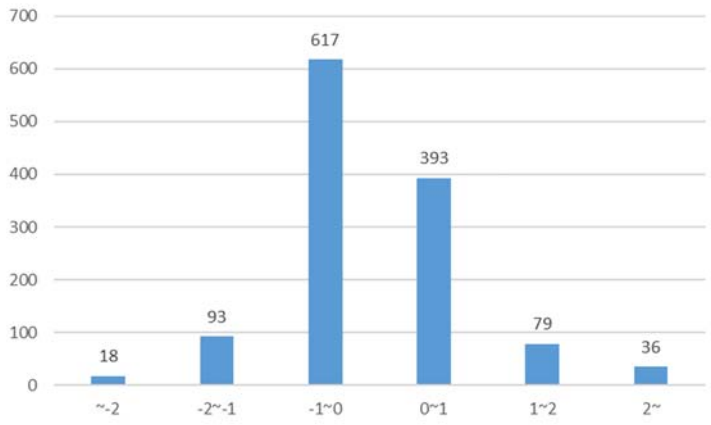

図 4: 近視眼的尺度の分布

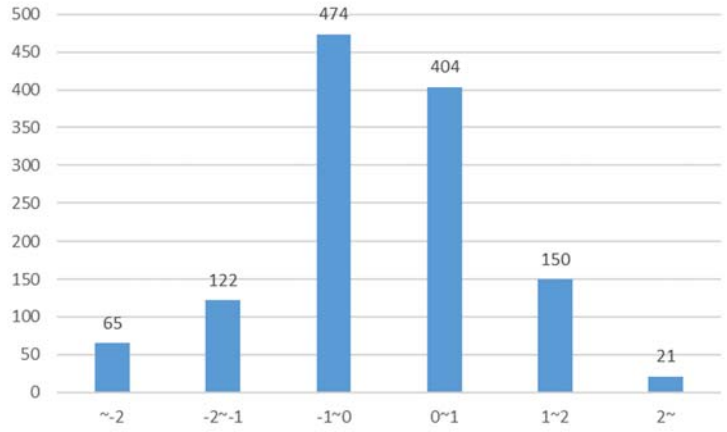

図 5: 愛着要素の分布

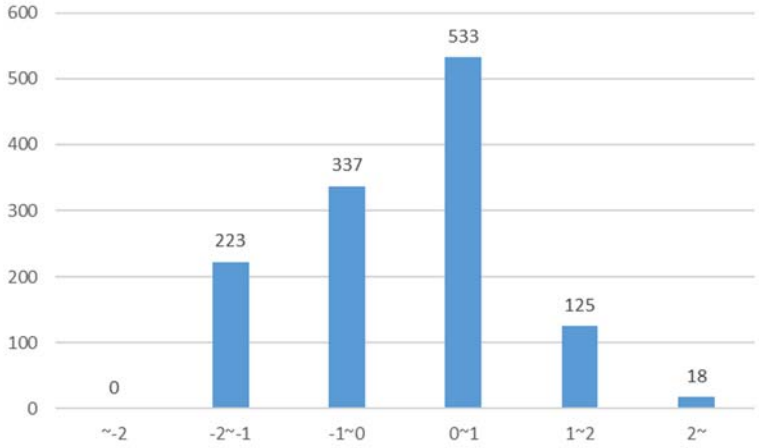

図 6: 規範的要素の分布

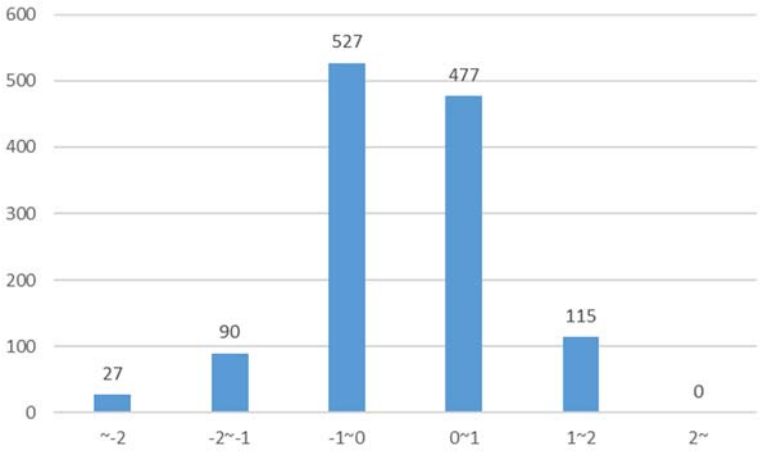

図 7: 存在的要素の分布

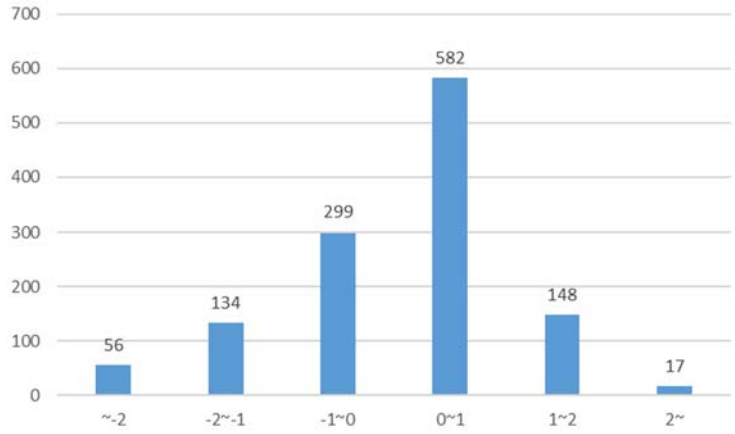

図 8: 内在化要素の分布

(2) 順序ロジット回帰分析

本稿では、被説明変数（情報セキュリティインシデント被害経験）は選択の順序性があるため、順序ロジット回帰分析を採用する。順序ロジット回帰分析の詳細については、北村(2009)を参照されたい。

表 4 から表 6 には「ウイルスやワーム、スパイウェアへの感染」「フィッシング詐欺」「ワンクリック詐欺」を被説明変数とし、説明変数を「性別」「リスク回避度」「年齢」「近視眼的尺度」「自信過剰」「愛着要素」「内在化要素」「規範的要素」「存続的要素」とする順序ロジット回帰分析の結果を示している。

「ウイルスやワーム、スパイウェアへの感染」「フィッシング詐欺」「ワンクリック詐欺」の分析結果を順に見ていく。まず、表 4 の「ウイルスやワーム、スパイウェアへの感染」において、「性別」の係数は 1%水準で有意となり、その値は負となっている。5%水準で有意となった係数は「リスク回避度」で、その値は同じく負となっている。10%水準で有意となっている係数は「自信過剰」であり、その値は正となっている。一方で、「年齢」「近視眼的尺度」「愛着要素」「内在化要素」「規範的要素」の係数はいずれも統計的に有意とならなかった。

次に、表 5 の「フィッシング詐欺」において、「自信過剰」の係数は 1%水準で有意となり、その値は正となっている。それ以外の要因の係数についてはいずれも統計的に有意とはならなかった。

最後に、表 6 の「ワンクリック詐欺」において、組織コミットメントの一つである「内在化要素」の係数が 1%水準で有意となり、その値は正となった。また、「自信過剰」の係数が 5%水準で有意となり、その値は同じく正となった。さらに、10%水準で有意となった係数は「近視眼的尺度」「愛着要素」であり、前者の係数は正、後者の係数は負の値をとった。しかしながら、これらの要因以外の係数はいずれも統計的に有意とはならなかった。表 4 から表 6 を比較すると、情報セキュリティインシデント被害に遭遇する回数に影響を与える

表 4: 分析結果（ウイルスやワーム、スパイウェアの感染）

	Coef.	P>z
性別	-0.591	0.010
リスク回避度	-117329	0.063
年齢	0.008	0.324
近視眼的尺度	0.119	0.260
自信過剰	0.028	0.087
愛着要素	-0.051	0.757
内在化要素	-0.002	0.993
規範的要素	0.116	0.433
存続的要素	0.033	0.805
Number of obs	1081	
LR	LR chi2(9)= 24.70	
cut1	2.243	
cut2	3.086	
cut3	5.027	
cut4	5.62	

表 5: 分析結果（フィッシング詐欺）

	Coef.	P>z
性別	0.386	0.302
リスク回避度	-115215	0.194
年齢	0.016	0.234
近視眼的尺度	0.102	0.576
自信過剰	0.086	0.003
愛着要素	-0.112	0.725
内在化要素	0.476	0.193
規範的要素	0.425	0.104
存続的要素	-0.182	0.498
Number of obs	1061	
LR	LR chi2(9)= 29.36	
cut1	4.976	
cut2	5.848	
cut3	7.608	
cut4	8.711	

表 6: 分析結果（ワンクリック詐欺）

	Coef.	P>z
性別	-0.054	0.868
リスク回避度	-75633.9	0.409
年齢	-0.007	0.572
近視眼的尺度	0.273	0.064
自信過剰	0.057	0.018
愛着要素	-0.483	0.056
内在化要素	0.887	0.002
規範的要素	-0.162	0.429
存続的要素	0.108	0.606
Number of obs	1057	
LR	LR chi2(9)= 27.61	
cut1	3.121	
cut2	4.072	
cut3	5.584	
cut4	6.098	

要因は、情報セキュリティインシデント被害の種類によって異なることが示唆される。

4.3 分析

本稿では、3 つのインシデント被害回数に関する分析を行った。以下、行動経済学要因および組織コミットメントに関する要因についての考察を行う。

3 つの情報インシデント被害回数に影響を与える要因としては「自信過剰」があった。そして、この要因は第 3 節で立てた仮説を支持する結果となっている。これは、自信過剰という行動経済学的要因は少なくともこの 3 つの情報セキュリティインシデント被害に共通して影響を与えることがわかり、自信過剰がもつ負の側面について対策を行うことに大きな意義があるように思える。また、行動経済学的要因であるリスク回避度に関しては、ウイルスやワーム、スパイウェアという被害回数にのみ影響を与えていることが合わせてわかった。さらに、行動経済学的要因である近視眼的尺度については、ワンクリック詐欺の被害回数にのみ影響を与えていることがわかった。これらの結果はウイルスなどの被害と、フィッシング詐欺、ワンクリック詐欺の被害とではその性質が異なることにより生じたと考えられる。つまり、ウイルスなどは不特定多数を対象とし拡散的なものであるのに対して、フィッシングなどは（ある程度）個人を特定とした攻撃であるため（なお、ワンクリック詐欺はちょうどウイルスなどとフィッシングの攻撃の中間的な位置づけにあると考える)、情報セキュリティインシデントの種類によってリスクへの態度や近視眼的な意識が異なったから

ではないかと思われる。

組織コミットメントは田尾（1997)に従い、4 つの要素（愛着要素、内在化要素、規範的要素、存続的要素）に分けて分析に用いたところ、フィッシング詐欺被害回数にのみ、愛着要素と内在化要素が影響を与えていることが確認された。なお、それ以外の情報セキュリティインシデント被害に関しては、組織コミットメントの要素はいずれも影響を与えていないことが確認された。また、規範的要素および存続的要素と、フィッシング詐欺の被害回数の間には関係がないことが合わせて確認された。このことから、組織コミットメントと言ってもその中身によって情報セキュリティインシデント被害回数に与える影響がことなることが示唆された。また、関係が確認されたフィッシング詐欺においては、愛着要素と内在化要素の符号が異なることから、一概に組織コミットメントを高めればよいとは言えないと言える。つまり、愛着要素と内在化要素をともに高めてしまうと、前者は被害を減らすことに寄与するが、後者は逆に被害を増やしてしまうことがわかる。さらに、多くのケースにおいて組織コミットメントが有意とならなかったことについて解釈を与えると、組織コミットメント密接な関係がある組織の構成員である従業員の満足度や処遇といった目に見える要因（要素）の方がより影響を与えている可能性があると考えられる。この可能性については本稿の今後の課題としたい。

5. 提案

第 4 節を踏まえて、本稿では個人が情報セキュリティインシデント被害に遭いにくくするための対策として以下の 2 つを提案したい。

(1) 自信過剰を調べるテストの実施

分析結果から「自信過剰」は 3 つの情報セキュリティインシデント被害回数との関連性が認められ、まあ高い自信過剰は被害経験回数を増やすことが明らかになった。組織の管理者の目線に立つと、組織全体にどれくらい情報セキュリティインシデント被害に遭いやすい従業員がいるのかを知ることは重要であると思われる。そのため、個々人の自信過剰について組織が把握を行うことは有効な対策となりうると考えられる。しかしながら、このことは個人のプライバシーに関する部分であり、その慎重に議論をする必要がある。もし把握するとしても、（例えば）部署レベルでの平均的な自信過剰の程度を把握するなど、個人が特定化されないように配慮する必要がある。

(2) 職位に応じた情報セキュリティ教育・トレーニングの実施

分析結果から、組織コミットメントの中でも「愛着要素」「内在化要素」がワンクリック詐欺被害回数と関連性が確認された。そして、企業に情緒的な愛着を持つ人ほど、情報セキュリティインシデント被害に遭いにくく、一方で、自分と組織の価値が一致し組織に尽くそうと考える人ほど、情報セキュリティインシデント被害に遭いやすいということが示され

た。組織に対して愛着を持たせる様々な仕組みはすでに考えられているので、本稿では内在化要素に関しての提案を考えたい。

田尾（1997)によれば、職位が高くなるにしたがって、内在化の程度が増加することが指摘されている。これは、分析結果と合わせると、職位が高くなるに従って、情報セキュリティインシデント被害回数が増えることを意味することになるかもしれない。実際に、職位が上がるほど、組織の様々な情報にアクセスする権限が増えるため、ターゲットとなりやすくなることは簡単に想像できる。また、セキュリティ教育は職位に関係なく、一律に行われることが多いことを踏まえると、職位に応じた情報セキュリティ教育・トレーニングが必要であると考える。一般的に、新入社員に対して重点的に行われることが多いが、職位が高い課長や部長についても、重点的に教育を行っていくべきだと考える。そのためにも、組織はセキュリティ管理のリーダーを職位が高い従業員の中から決めることも重要であるかもしれない。それは、セキュリティ管理のリーダーを組織内の職位の高い職員たちにさせることによって、他の従業員にも、情報セキュリティについての意識を高めさせる効果も期待されるためである。また、教育の内容については、危機管理の意識を高めるものにしておく必要もある（竹村他, 2017)。

6. おわりに

本稿では、2016 年 2 月に実施された「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」によって収集・蓄積された個票データを用いて、どのような個人属性が情報セキュリティインシデント被害回数と関係があるのかについて分析を行った。その結果、興味深い結果を得ることができた。例えば、本稿で考えた 3 つの情報セキュリティインシデント被害に対して行動経済学的要因の一つである自信過剰が影響を及ぼしていることが確認された。そして、自信過剰がもつ負の側面について対策を行うことに大きな意義・効果があることについて示唆を与えた。また、組織コミットメントについては情報セキュリティインシデント被害との関係は一部確認されるにとどまった。これについては本稿で用いた概念モデルの再考を行うことにより、より両者の関係を明らかにできるのではないかと考える。さらに、本稿では年齢と情報セキュリティインシデント被害回数の間に線形の関係を仮定していたが、情報セキュリティインシデント被害回数と職位との関連性も示唆されるため、職位をモデルに組み込む、もしくは藤嶋他（2017)などで行われているように、年齢と情報セキュリティインシデント被害回数の間に非線形の関係を仮定したモデルの構築を今後考えたい。

参考文献

1. Becker, G.M., Degroot, M.H.,Marschak, J.(1964)”Measuring Utility by a Single Response

Sequential Method," Behavioral Science,Vol9,226-232
2. Hair, J.F., Anderson, R.E, Thatham, R.L., Black,W.C (1998) Multivariate Data Analysis, Prtice-Hall International
3. Takemura, T. (2014) 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, Chapter 11, 181-198
4. Takemura, T., Komatsu, A. (2013) An Empirical Study on Information Security Behaviors and Awareness, Bohme, R. (Ed.), Economics of Information Security and Privacy. Springer, Chapter 5, 95-114
5. 安藤怜未・島成佳 (2014)「IT システムにおけるヒューマンエラーに関する傾向と考察」『コンピュータセキュリティシンポジウム 2014 論文集』 1216-1217
6. 石黒格 (2014) 『改訂 Stata による社会調査データの分析』北大路書房, 157-164
7. 井上美沙・有光興記 (2007)「日本語版未来結果熟慮尺度の作成と信頼性・妥当性の検討」『パーソナリティ研究』 第 16 巻, 第 2 号, 256-258
8. 内田勝也 (2008)「情報セキュリティ心理学とトラストの動向について－情報セキュリティ心理学とトラスト (SPT) 研究グループの活動」『IPSJ SIG Technical Report』 Vol.2008_CESC_041
9. 太田さつき (2012)「コミットメント：組織コミットメント、ジョブインボルブメント、キャリアコミットメント、職務満足」『労働政策研究報告書』No.147
10. 北村行伸 (2009)『ミクロ計量経済学入門』日本評論社, 133-146
11. 倉谷尚孝・城戸康彰 (2006)「行政組織における組織コメットメント―組織コメットメントの先行要因と結果要因の実証研究―」『産能大学紀要』第 26 巻, 第 2 号, 58-59
12. 産経ニュース (2015)「機構本部、4 月にパスワード無設定知りながら放置: 情報内容流出拡大に拍車」 (http://www.sankei.com/life/news/150621/lif1506210012-n1.html)
13. 情報処理推進機構 (2016)「情報セキュリティ白書: 今そこにある脅威：意識を高め実践的な取り組みを」情報処理推進機構
14. 新原功一・原田要之助 (2014)「情報セキュリティインシデントに対するヒューマンエラー対策の提案」『情報処理学会論文誌』55, 巻 10 号, 2318-2326
15. 関口倫紀・歴傑・細見正樹 (2014)「組織コミットメントと職務ストレス: 高水準情緒的コミットメントの逆機能と仕事と家庭の分離志向による調整効果」『経営行動科学学会年次大会発表論文集』17 巻, 397-402
16. 総務省(2016) 「平成 27 年通信利用動向調査の結果」 (http://www.soumu.go.jp/johotsusintokei/statistics/data/160722_1.pdf)
17. 田尾雅夫 (1997)『「会社人間の研究」組織コミットメントの理論と実際』京都大学学術

出版会
18. 竹村敏彦・渡部正文・島成佳（2017）「セキュリティポリシー違反に対して有効となる組織的対策について」『暗号とセキュリティシンポジウム 2017 予稿集』
19. 西脇暢子（2010）「専門職従業員の組織コミットメント: 研究職と技術職の組織コミットメントの比較ならびにパフォーマンスとの関係性」『RIESCE Working Paper Series』No.09-07
20. 花村憲一・竹村敏彦・小松文子（2012）「情報セキュリティインシデント被害者の属性に関する考察」『暗号とセキュリティシンポジウム 2012 予稿集』
21. 藤嶋良起・竹島健人・最所崇将・篠原圭介・原拓哉（2017）「悪意のある投稿をする人はどのような人か〜アンケート調査を用いた実証研究〜」『佐賀大学経済学部学生論集』第 25 号, 145-163