情報処理学会論文誌 Vol.56 No.12 2191–2199 (Dec. 2015)

情報漏えいにつながる行動に関する実証分析

竹村 敏彦[1,a)] 三好 祐輔[2] 花村 憲一[3]

受付日 2015年2月23日, 採録日 2015年9月2日

概要：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を行う．分析の結果から，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のの，様々な要因を介した間接的な効果をふ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．付け加えて，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が分かった．

キーワード：情報漏えい，構造方程式モデリング，組織風土，コンプライアンス意識，感情

Empirical Analysis on the Behaviors Related with Information Leakage

Toshihiko Takemura[1,a)] Yusuke Miyoshi[2] Ken-ichi Hanamura[3]

Received: February 23, 2015, Accepted: September 2, 2015

Abstract: In this article, we focus on the behaviors related with information leakage among problematic behaviors from the viewpoint of information security measures. We investigate some direct and/or indirect factors affecting to the behaviors, and show the more effective measures which implemented in the organizations for the purpose of detering the behaviors. As a result, we find that the most effectiveness of detering the behaviors is to reform the organizational climate accepting injustice, and that the indirect effects of improving compliance awareness is greater although the direct effect of one is not so great. In addition, we can obtain the more effectiveness by heightening employee satisfaction and implementing compliance education besides reforming the organizational climate because compliance awareness and employee satisfaction affecting to the organizational climate in our model.

Keywords: information leakage, structural equation modeling, organizational climate, compliance awareness, emotion

1. はじめに

国内外の組織において，外部からのサイバー攻撃や内部の従業員に起因する情報漏えいなどの情報セキュリティ事故が多数確認されている（文献 [1] など）．そのため，多くの組織がこれらのセキュリティ事故や被害を防止するために様々な技術的対策を講じている．たとえば，システムにより USB メモリなどの媒体によるデータの持ち出しや仕事と関係のないウェブサイトの閲覧を禁止している組織は少なくない．一方で，この対策を講じたことによる日常業務の生産性や効率性の低下，さらにそもそも対策自体が軽視されるといった利用者である個人に関する問題が指摘されている（文献 [2], [3], [4] など）．技術的対策に加えて，非技術的対策（人的や組織的な面から様々な対策）を講じ

[1] 佐賀大学
Saga University, Saga 840–8502, Japan
[2] 香川大学
Kagawa University, Takamatsu, Kagawa 760–8521, Japan
[3] 情報処理推進機構
Information-technology Promotion Agency, Bunkyo, Tokyo 113–6591, Japan
[a)] tosihiko@cc.saga-u.ac.jp

ている組織も存在している．たとえば，情報セキュリティポリシの策定・整備や実施などがあげられる．非技術的な対策はその運用に融通が利きやすいといった特徴を持つ一方で，技術的対策のようにある種の強制力があるものではない．言い換えると，組織が実施するルールを守ること，もしくはルールを破らないことを技術的対策のように強制することは難しい．情報セキュリティ対策として何らかのルールの策定・整備を考えた場合，それらを策定・整備したとしてもそれを従業員が守らなければ，対策の効果は意味のないものとなってしまうだけでなく，逆に組織全体の情報セキュリティ水準の低下を招いてしまうこともある[*1]．とりわけ，本研究で取り扱うような情報セキュリティの観点から問題となる行動は多くの場合，組織の意思決定とは一致しないことが多い．個人がそのような不適切な行動をとる（誤った判断をする）ことで，たと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，ある種の目的を達成することができるが，時としてこの行動は組織を情報漏えいなどのリスクにさらしたり，不利益をもたらしたりすることがある．それゆえに，組織の情報セキュリティ管理者などは従業員の不適切な行動に注意を払う必要がある．これらの個人の行動，さらにモラルに関する問題への対応として，組織で情報セキュリティ教育やトレーニングを行い，情報漏えいに関するセキュリティ事故や被害を防止・抑止することが試みられている．そしてこれらの効果についても文献 [5], [6] などの先行研究で確認されている．

本研究では，これらの教育やトレーニングが効果的に情報漏えいにつながる行動を防止・抑止することにも有効であるのか，またこれらが有効なときそれを阻害している要因はあるのか，教育などの効果をより大きくするためにはどのようなことを組織として取り組むべきかなどについて考える．そのために，まず，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，その検証を行う．次に，これらの関係を明らかにし，それをもとに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る．本研究では，どのようなことを組織が優先的に行えば，より効果的に個人の情報漏えいにつながる行動を防止・抑止させることができるかを示したい．

2. 関連研究

情報セキュリティの観点から問題となる行動は所属する組織において何らかのルールにより禁止・制限されていることがある．言い換えると，この種の行動をとることは多くの場合，ルール違反にあたる．そして，組織の規模を問わずに，ルールを守らない個人はどの組織にも一定数存在しているといわれている（文献 [7], [8]）．そのルール違反をしている個人は必ずしも悪意を持っておらず，またうっかりミスということも多い[*2]．

これらのある種人間の持つ脆弱性に注目し，ユーザの視点に立った組織の情報セキュリティ対策に関する研究が近年数多く報告されている．これらの研究では，様々なヒトの意識に注目した分析を介してより有効な対策を組織が実施できる可能性についてアプローチしているものや，不正や違反といった行動に注目した分析を介して組織にとって情報セキュリティ対策の観点から問題となる行動を防止・抑止する対策についてアプローチしているものがある．

一般的に，これらの行動分析は行動科学や犯罪心理学でポピュラーな理論的フレームワークが援用されている．具体的な理論的フレームワークとして，計画的行動理論（TPB; theory of planned behavior）や対人行動論（TIB; theory of interpersonal behavior），一般的防護理論（GDT; general deterrence theory）などがある．TPB は，意図が行動にどのように影響を与えているか，またその意図に影響を与えている要因（行動に対する態度，主観的な規範の認知，知覚された行動の統制可能性）を調べることによって個人の行動を予測しようとする理論で，TIB はそれに習慣と感情の要素を新たに組み込んだものである．他方で，GDT はヒトやプロセスのような要素を考慮せずに，組織による対策がどの程度技術を信頼できるかを説明することができる理論である．これらの理論を通じて，情報セキュリティ対策の観点から問題となる行動に影響を与える要因は「個人の意識・感情」と「個人を取り巻く環境（人間関係も含む）」であることが分かる．これらの理論的フレームワークを情報セキュリティ行動への援用の妥当性についてまとめた有益な研究として文献 [10] を参照されたい．以下，簡単に情報セキュリティ対策の観点から問題となる行動を取り上げた関連研究を紹介する．

情報セキュリティポリシ対策に関する研究は多数行われており，大別すると情報セキュリティポリシの遵守に影響を与える要因を探索するものと情報セキュリティポリシ違反に影響を与える要因を探索するものに分けられる（文献 [10], [11] など）．このことからも分かるように，遵守することと違反することは必ずしも同一軸で考えられない概念である．

また，主要な情報セキュリティポリシ違反の具体的な行動に焦点を当てた研究として，業務と無関係なインター

[*1] 文献 [4] では，管理者と一般従業員（ユーザ）の情報セキュリティ対策に対する意識ギャップを「組織内デジタルデバイド」と呼んでいる．彼らは組織全体の情報セキュリティ水準の低下の根本的な原因がこれにあると指摘している．

[*2] 文献 [9] によれば，経年的な傾向として情報漏えいなどの被害の理由の上位としてうっかりミスや誤用といったことが指摘されている．もちろん，内部不正などの情報転売目的とした故意による行動（犯罪）もあるため，すべてが悪意がないとはいいきれない．

ネットの利用（文献 [12] など），コンピュータの不正利用（文献 [13] など）やソフトウェアの著作権法違反（文献 [14] など）がある．これらの行動は，法律に抵触するかどうか，またそれが意識的かどうかによってもその問題の深刻さは異なるが，いずれも情報セキュリティ対策の観点から問題となる行動であり，情報セキュリティインシデント被害・事故に遭遇する可能性や，不正・情報漏えいにつながる可能性も多分に持っている．これに加えて，情報の不適切な取り扱いなどをはじめとする情報漏えいにつながる行動について分析している研究として文献 [7], [8], [15] などがある．この種の行動に関する研究が近年，組織における情報管理という側面から積極的に行われている．

上述したように，「個人の意識・感情」や「個人を取り巻く環境」といった要因がこれらすべての行動（情報セキュリティ対策の観点から問題となる行動），またそれに先行する意図に影響を与えていることが実証研究で示されている．つまり，この種の行動の原因は個人の意識だけでなく，その個人が直面している環境からも大きな影響を受けていることが分かる．そのため，先行研究では共通して，個人にそのような行動をとらせないためには，意識改革のための教育・トレーニングの実施に加えて，広義の意味での職場環境改善の重要性を指摘している．

3. アンケート調査概要

本研究では，2014 年 3 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 2014」と題したインターネットアンケート調査によって収集した個票データを用いて分析を行う．インターネット調査には，ウェブサイトを開設しそこで不特定多数を対象にアンケートを実施する「オープン型」とモニタパネル（ポータルサイトやアフィリエイトプログラムを通じてアンケートに協力してくれる回答者）などを利用し彼らの情報を基にサンプリングを行ってアンケートを実施する「クローズ型」があり（文献 [16]），本研究では後者を採用した．この調査形式を採用した理由として，調査環境の劇的な変化（回収率の低下，プライバシや個人情報保護法への過剰反応による拒否率の上昇など）に加えて，文献 [17] などで指摘されているように，情報セキュリティ特有の問題点として多くの企業が部外者にセンシティブな情報を出したくないといった理由により調査協力がそもそも得られない点をカバーし，効率良く調査対象者を抽出するためである．この調査法はサンプルが無作為に抽出されていないなどの統計的な問題が指摘されている．しかしながら，文献 [18] 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 1 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．また，本研究の結果は現時点では日本の労働者すべてに対して妥当性を持つとまではいえないが，（限定的ではあるが）調査会社にモニタとして参加している労働者に対して妥当性を有していることは主張できる．もちろん，調査の正確性（accuracy）について議論する必要がある．この調査手法の詳細な利用可能性・妥当性については文献 [19], [20] などを参照されたい．

表 1 調査対象者の構成
Table 1 Demographic Information about the Respondents.

項目		#	(%)
年齢	20–39 歳	603	40.01
	40–49 歳	382	25.35
	50 歳以上	522	34.64
勤続年数	5 年未満	567	37.62
	5–9 年	373	24.75
	10 年以上	567	37.62
所属企業の	上場企業	749	49.70
上場の有無	非上場企業	758	50.30
所属企業の	100 人未満	479	31.79
従業員数	100–299 人	186	12.34
	300–999 人	195	12.94
	1,000–4,999 人	231	15.33
	5,000 人以上	296	19.64
	分からない	120	7.96

この調査は 2009 年から毎年継続的に実施しており，そ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．そのため，この調査は，まず調査対象者であるかを調べるための事前調査を約 2 万人に対して実施し，その中から条件を満たす 1,500 人を抽出し，本調査に回答してもらうという 2 段階の方式を採用している．また，オーバサンプリングや，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 1,507 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．

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，コンプライアンス意識，企業内で実施されている情報セキュリティ対策や情報セキュリティ教育の状況だけでなく，組織コミットメント，職場環境，リスク許容度など多岐にわたり，質問総数は約 45 問である．質問項目の内容は，文献 [7], [14], [15], [21] などで用いられているものを参考に作成している．質問項目から作成される要因（構成概念）などについては 4 章で説明する[*3]．

[*3] 本研究で用いる要因は，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．また，アンケート調査票（抜粋版）は URL <http://ecolab.eco.saga-u.ac.jp/inf_sec/question201401.pdf>で公開している．

4. フレームワーク

4.1 行動に影響を与える要因の構造

4.1.1 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 2 章で見たように様々なものがある．その中で，本研究では情報漏えいにつながる行動を取り上げる．この種の行動はその行動をとった個人にとっては少なくとも目的（たとえば，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り，セキュリティの観点から問題のある行動である．情報漏えいが社会問題化しているにもかかわらず，文献 [7], [8], [15], [22] などによれば，（たと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分かっており，その数は減少傾向にあるとはいい難い状況にある[*4]．

4.1.2 行動に影響を与える諸要因

情報漏えいにつながる行動に直接的，間接的に影響を与える要因として，以下の 7 つを採用した．抵抗感のなさやポリシ違反意図といったある種のモラルの欠如に起因する意識が情報セキュリティの観点から問題とされる行動の正当化を助長する効果を持つ一方で，コンプライアンス意識や情報リテラシの向上，ルールの認知はこの種の行動を抑止する効果を持つ．これらの意識などは直接的に行動に影響を与えているだけでなく，相互に影響しあっている可能性もある．また，これらの意識に影響を与えている要因として，従業員満足度などが考えられる．さらに，これらの意識などと密接に関連している要因として，組織風土が考えられる．個人のモラルの欠如に起因する意識が職場風土に影響を与えるのか，逆に職場風土がそのような意識に影響を与えているのかについてはまだ明らかになっていない[*5]．これらの 7 つの要因を採用した理由は，情報漏えいにつながる行動に影響を与える要因として個人の観察可能な属性（性別や年齢，学歴）なども考えられるが，文献 [24] などでも指摘されているように情報セキュリティに関する行動に対して心理的な要因が影響を与えていることをふまえて，本研究ではとりわけ心理的な要因を組み込んでいる．また，心理的な要因だけではなく，個人が直面している環境，とりわけ職場環境もあわせて組み込んでいる．この考え方は関連研究で触れた TPB や GDT などでも取り入れられている（文献 [10] など）．

本研究では「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 2014」の質問項目から作成できる心理的な要因およびそれに影響を与えるであろう他の要因を採用し，情報漏えいにつながる行動に対する諸要因の直接的な影響だけでなく，要因間の関係をふまえた間接的な効果についても見ていく．これらの関係を見ることにより，より効率的な情報セキュリティ教育やコンプライアンス教育の在り方や職場環境改革について議論するための一材料を提供することができると考える．

以下，7 つの要因について簡単に説明するとともに，検証するための仮説を示す．

(1) 抵抗感のなさ

抵抗感とは承服しかねる感情，心理的に覚える抵抗であり，コンプレックスに触れることを避けようとするもの，過去の出来事がまた起こるのではないかという怖れからくるもの，自分が持っている観念やルールにより制限するものなどから生まれる意識である．ある行動をとろうとしているとき，抵抗感が意識的・無意識的にその行動をとどまらせることが期待できるが，抵抗感がなければその可能性は低くなる．この感情による行動の抑止は情報漏えいにつながる行動においてもあてはまる．それゆえに，本研究では以下の仮説を立てて，このことを検証する．

仮説 1 抵抗感を感じないほど情報漏えいにつながる行動をとりやすい．

(2) ポリシ違反意図

意図（intention）とは個人が行動を起こそうとするか否かを決める主要な先行要因であり，本研究では情報セキュリティポリシ違反をしようとするかどうかの意図（ポリシ違反意図）を取り上げる．抵抗感と同様に，ポリシ違反意図はモラル，とりわけ情報モラルと密接に関連するものである．

情報セキュリティポリシは組織における情報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，情報セキュリティポリシ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が確立・整備されてはいるが，情報セキュリティポリシは法律・法令ほどの強制力は必ずしもないために，遵守されず，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（文献 [12], [22], [25]）．また，彼らは情報セキュリティポリシ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．本研究では，この主張を検証するために以下の仮説を立てる．

仮説 2 ポリシ違反意図が高いほど情報漏えいにつながる行動をとりやすい．

(3) 情報リテラシ

情報リテラシとは，情報を主体的に選択，収集，編集，発信する能力と同時に，コンピュータなどを使って論理的に考える知識・能力と広義に解釈することができる．つ

[*4] 多くの研究では行動意図について質問しているが，実際の行動の傾向を測るために，本研究では行動意図ではなく頻度を採用した．

[*5] 文献 [23] によれば職場風土（職場感情）と情報セキュリティ対策の間に関係がある（対策の効果が有効に働く組織とそうでない組織がある）ことを指摘している．

まり，情報リテラシと情報モラルは異なる概念である（文献 [26]）[*6]．情報リテラシの向上は情報セキュリティの観点から問題となる行動を抑止したり，情報セキュリティインシデント被害や事故に遭遇する可能性を低下させたりする効果があることが明らかになっている（文献 [5], [13]）．また，情報リテラシの向上は情報モラルの向上にも寄与すると考えられるため，本研究では以下の 2 つの仮説を立てる．

仮説 3-1 情報リテラシが高いほど情報漏えいにつながる行動をとりにくい．

仮説 3-2 情報リテラシが高いほどポリシ違反意図は低い．

(4) コンプライアンス意識

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（文献 [27]）[*7]．

組織に属する個人の行動すべてをルールによって規定することはできない．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（文献 [28]）．そのため，本研究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．

コンプライアンス意識の向上は単に情報セキュリティの観点から問題となる行動の抑止につながるだけでなく，ルールの遵守やモラルの向上などにも影響を与えると思われる．また，コンプライアンス意識の向上は所属する組織の情報（情報資産）を防護しようとする意識を高め，そこから情報管理などを意識的に行うようになると考えられる．そこで，本研究では以下の 4 つの仮説を立てる．

仮説 4-1 コンプライアンス意識が高いほど情報漏えいにつながる行動をとりにくい．

仮説 4-2 コンプライアンス意識が高いほど抵抗感を感じる．

仮説 4-3 コンプライアンス意識が高いほどポリシ違反意図は低い．

仮説 4-4 コンプライアンス意識が高いほど情報リテラシは高い．

(5) ルールの認知

組織内には，情報資産の防護や情報漏えいを防止させるために，情報の取り扱いに関して様々なルール・規程がある．ここでは，そのルールが規定されているかどうかではなく，そのルールを知っているかどうかについて考える．文献 [7], [8] などで指摘されているように，ルールが規定されていたとしてもそれを知らなければそのルールは本質的な意味を失ってしまうことになる．また，ルールを認知していて情報漏えいにつながる行動をとったならばそれは意識的な行動の結果として，逆にルールを認知していなければ無意識的な行動の結果ととらえることができる．また，ルールの認知はポリシ違反意図などとも密接な関係を持っている．そこで，本研究では以下の 4 つの仮説を立てる．

仮説 5-1 ルールを認知しているほど情報漏えいにつながる行動をとりにくい．

仮説 5-2 ルールを認知しているほどポリシ違反意図は低い．

仮説 5-3 情報リテラシが高いほどルールを認知している．

仮説 5-4 コンプライアンス意識が高いほどルールを認知している．

(6) 不正容認風土

本研究では，組織風土として不正容認風土を取り上げる．不正容認風土とは，職場において日常的に基本的なルールが破られたり，管理者が不正や違反を知りながらそれを放置したりといった組織の体質を表すものである．

文献 [15], [21] では，組織風土が様々な不祥事などに影響を与えることを定量的に分析し，その効果を確認している．しかしながら，上述したような個人の意識と不正容認風土の関係についての分析は行われていない．つまり，個人のモラルの欠如に起因する意識が不正容認風土を醸成するのか，不正容認風土がそのような意識を生むのかについてははっきり分かっていない．そこで本研究では，不正容認風土が情報漏えいにつながる行動，また不正容認風土が個人の意識に影響を与えるかを検証するために以下の 4 つの仮説を立てる．

仮説 6-1 不正容認風土が強いほど情報漏えいにつながる行動をとりやすい．

仮説 6-2 不正容認風土が強いほど抵抗感を感じない．

仮説 6-3 不正容認風土が強いほどポリシ違反意図が高い．

仮説 6-4 コンプライアンス意識が高いほど不正容認風土が弱い．

(7) 従業員満足度

従業員満足度は職場や仕事に関する評価感情（evaluative feeling），つまり職場や仕事に対しての情熱や無関心さを表しており，企業業績や顧客満足度などの向上に寄与することが明らかにされている．一方で，従業員満足度の低い者は情報セキュリティの観点から問題となる行動を正当化したり，これらの行動に対するいかなる否定的な感情にも打ち勝ったりする理由を持ちやすい傾向があることが指摘されている．

文献 [29] では満足度水準とインターネットの不正利用の間に関係があることが確認されているが，本研究では従業員満足度が情報漏えいにつながる行動に対して直接的ではなく，間接的に影響を与えると考える．情報漏えいにつ

[*6] 情報モラル（情報倫理）とは，通常の日常生活上のモラルに加えて，人とのコミュニケーションや情報の選択，収集，編集，発信を適正で安全に節度をもって行うための基本的な考え方と態度（行動規範）のことをいう．本研究では，情報リテラシは主として能力の側面を表し，情報モラルは主として行動規範の遵守（道徳的な側面）を表すと考え両者を区別している．

[*7] なお，本研究ではコンプライアンス意識はより一般的な概念としてとらえて，情報セキュリティに関するものに限定はしていない．

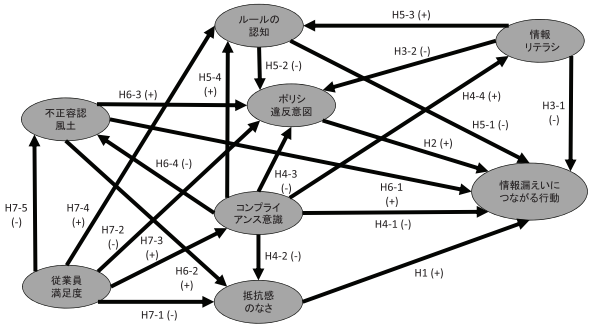


図 1 プロトタイプの提案モデル
Fig. 1 Our Prototype Model.

表 2 クロンバックの α 信頼性係数
Table 2 Cronbach's Coefficient α.

	質問項目数	Cronbach's α
情報漏えいにつながる行動	6	0.91
抵抗感のなさ	9	0.94
ポリシ違反意図	4	0.74
情報リテラシ	6	0.87
コンプライアンス意識	4	0.92
ルールの認知	6	0.96
不正容認風土	8	0.95
従業員満足度	2	0.90

ながる行動は情報セキュリティの観点から問題である行動であるが，個人がどのような目的でその行動をとるかに関わってくる．持ち出した情報を売買するということであれば，不正アクセスなどでみられるように従業員満足度が低いことでそのような行動をとるという直接的な効果があると思われるが，日常業務の簡便化のためにそのような行動をとるということであれば，状況は異なり，必ずしも従業員満足度が直接的に影響を与えるとはいい難い．そこで，従業員満足度はその種の行動を正当化するための要因や職場風土を健全化する要因であると見なし，それを検証するために以下の 5 つの仮説を立てる．

仮説 7-1 従業員満足度が高いほど抵抗感を感じる．
仮説 7-2 従業員満足度が高いほどポリシ違反意図が低い．
仮説 7-3 従業員満足度が高いほどコンプライアンス意識が高い．
仮説 7-4 従業員満足度が高いほどルールを認知している．
仮説 7-5 従業員満足度が高いほど不正容認風土が弱い．

4.2 提案モデル

図 1 には上述した 21 の仮説をまとめたプロトタイプの提案モデルを示している．本研究では，これらの仮説の成否だけでなく，どの要因が「情報漏えいにつながる行動」に強い影響を与えているか，また要因間にどのような関係があるか，などを探索することも目的としている．

図 1 には仮説を構成する要因を楕円で，また因果関係を矢印で表現している．さらにその矢印には影響を表す符号「+」（正の影響）もしくは「−」（負の影響）が付与されている．たとえば，「抵抗感のなさ」から「情報漏えいにつながる行動」の矢印は仮説 1（H1）を表し，前者の後者に対する影響は正である（抵抗感を感じないほど情報漏えいにつながる行動をとりやすい）と仮説を立てているために符号は「+」となっている．

5. アンケート調査結果の分析

図 1 に示した提案モデルを構造方程式モデリング（SEM：Structural Equation Modeling）によって分析・検証を行った．SEM は多重クラス構造や複数の構成概念間の関係を検討することができる（内生変数を扱いながら因果関係を調べることができるという特徴を持つ）統計的手法の 1 つである．SEM については文献 [30] などが詳しい．また，SEM には探索的アプローチ（観察されたデータからモデルを探索し，モデル構築に重きをおくもの）と確証的なアプローチ（複数からなる仮説構成体の検証を行い，モデルの適合性を重要視するもの）があり，本研究では後者によるアプローチを採用する．なお，データ分析のための統計ソフトウェアとしては Stata/MP 13.1 を用いた．

5.1 要因の信頼性評価

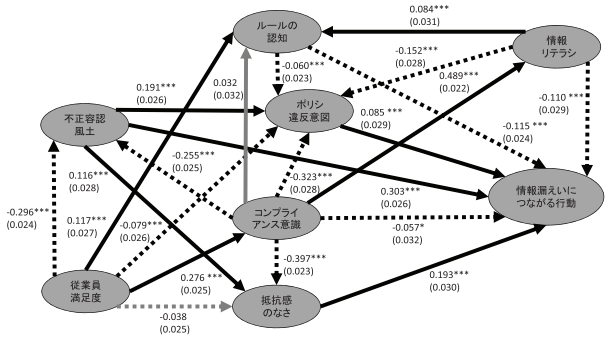
アンケート調査で得られた質問項目から構成される要因の信頼性を確認するため，クロンバックの α 信頼性係数を求める必要がある（文献 [30]）．**表 2** にはクロンバックの α 信頼性係数を調べた結果を示している．文献 [31] によれば，クロンバックの α 信頼性係数が 0.70 以上であればその要因の一貫性（信頼性・再現性）は高いと考えられており，表 2 に示した「ポリシ違反意図」の α 信頼性係数が 0.74 と他の要因に比べて低いものの，いずれの要因の α 信頼性係数も 0.70 を大きく上回っており，個々の要因はある程度の妥当性を有しているといえる．

5.2 SEM の分析結果・考察

SEM を用いて図 1 で示したプロトタイプのモデルを分析した結果，**図 2** に示したパス図を得ることができた．ただし，それぞれのパスに記載されている数値は標準化パス係数，また，その数値の下のカッコ内にはその標準誤差を示している．さらに，標準化パス係数の右肩にある * もしくは *** はそれぞれの係数の値が 10%有意水準もしくは 1%有意水準であること示し，* や *** がないものは有意でないことを示している．

SEM のモデルの適合度を調べる指標として一般的に用いられる RMSEA，CFI，TLI や SRMR を**表 3** に示している（文献 [32]）[*8]．参考として，これらの指標によるモデ

[*8] 文献 [33] にならい，モデルの適合度として GFI や AGFI を用いないというコンセンサスに従い，本研究ではこれらを用いない．



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 2 SEM の分析結果
Fig. 2 Result of SEM.

表 3 モデルの適合度
Table 3 Fitness of our model.

		非常に良好の範囲	悪い範囲
RMSEA	0.053	0.05 未満	0.10 以上
CFI	0.933	0.95 以上	0.90 未満
TLI	0.929	0.95 以上	0.90 未満
SRMR	0.069	0.05 未満	0.10 以上

表 4 直接効果，間接効果と総合効果
Table 4 Direct/Indirect Effects and Total Effects.

	直接効果	間接効果	総合効果
抵抗感のなさ	0.193	—	0.193
ポリシ違反意図	0.085	—	0.085
情報リテラシ	−0.110	−0.023	−0.133
コンプライアンス意識	−0.057	−0.264	−0.321
ルールの認知	−0.115	−0.005	−0.120
不正容認風土	0.303	0.070	0.373
従業員満足度	—	−0.168	−0.168

ルの適合度が良いと判断される範囲と悪いと判断される範囲も表 3 にあわせて示している．なお，それぞれの指標がこの範囲にあればモデルの適合度が良いと判断されることになる．表 3 のそれぞれの指標の数値を見てみるといずれもおおむね適合度が良いと判断される範囲内にあり，本モデルがデータをほどよく説明していることが分かる．

図 2 より，「コンプライアンス意識」から「ルールの認知」および「満足度」から「抵抗感のなさ」へのパス係数はともに有意とならなかった．つまり，仮説 5-4（H5-4）と仮説 7-1（H7-1）は棄却され，必ずしも従業員満足度を高めたとしても抵抗感をいだかせないことにはつながらず，またコンプライアンス意識を高めたとしてもルールの認知にはつながらないことが分かった．この 2 つ以外の仮説についてはすべて棄却されなかった．この 2 つのパス係数以外は 1%もしくは 10%水準で有意となった．つまり，2 つ以外の仮説についてはいずれもその仮説が支持される結果となった．

表 4 には，標準化パス係数（直接効果）とそれから計算される間接効果および総合効果についてまとめている．たとえば「不正容認風土」は「情報漏えいにつながる行動」へのパス係数で測られる直接効果（0.303）に加えて，「抵抗感のなさ」と「ポリシ違反意図」のそれぞれのパスを介して「情報漏えいにつながる行動」への間接効果（0.070）も存在している．そして両者の効果を合わせた総合効果は 0.373 となる．この結果は，「不正容認風土の強さが情報漏えいにつながる行動をとりやすくさせるだけでなく，不正容認風土の強さはポリシ違反意図を高め，また抵抗感を感じさせなくさせ，それが（間接的にも）情報漏えいにつながる行動をとりやすくさせている」ということを意味している．また，「従業員満足度」は「情報漏えいにつながる行動」への直接的なパスがないため，間接効果（−0.168）のみとなり，総合効果とその値は一致する．これは，我々のモデルでは「従業員満足度」は「情報漏えいにつながる行動」に直接的には影響を与えないが，「不正容認風土」へのパス係数（−0.296），「ポリシ違反意図」へのパス係数（−0.079），「コンプライアンス意識」へのパス係数（0.276），「ルールの認知」へのパス係数（0.117）を介して「情報漏えいにつながる行動」に負の影響（従業員満足度が高いほど情報漏えいにつながる行動をとりにくいこと）を意味している．

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として「不正容認風土」（パス係数は 0.303），次に「抵抗感のなさ」（パス係数は 0.193）があり，これらは情報漏えいにつながる行動を助長する要因となっている．また，「不正容認風土」から「ポリシ違反意図」「抵抗感のなさ」へのパス係数はいずれも正の値であり，また「ポリシ違反意図」「抵抗感のなさ」から「情報漏えいにつながる行動」へのパス係数はいずれも正の値であることから，「不正容認風土」は「情報漏えいにつながる行動」へ間接的にも影響を与える（情報漏えいにつながる行動を助長する）ことが分かった．一方で，情報漏えいにつながる行動を低減させる効果をもたらす「コンプライアンス意識」（パス係数の絶対値は 0.057）や「情報リテラシ」（パス係数の絶対値は 0.110）の影響はそれほど大きくはない．このことから，情報漏えいにつながる行動をとる主要な要因として職場風土やある種の不正を正当化する意識があり，それはコンプライアンスや情報リテラシ教育からもたらされる効果よりも影響が大きいことが分かった．

しかしながら，図 2 を見て分かるように「コンプライアンス意識」から「抵抗感」「ポリシ違反意図」「不正容認風土」へのパス係数はいずれも負，また「コンプライアンス意識」から「情報リテラシ」へのパス係数は正の値であり，また「抵抗感」「ポリシ違反意図」「不正容認風土」から「情報漏えいにつながる行動」へのパス係数はいずれも正の値，「情報リテラシ」から「情報漏えいにつながる行動」へのパス係数は負の値であることから，「コンプライアンス意識」が「抵抗感」「ポリシ違反意図」「不正容認風土」「情報リ

テラシ」を介して「情報漏えいにつながる行動」への影響（間接効果）はいずれも負の値となり，総合効果も −0.321 となる．そして総合効果の絶対値で見てみると「不正容認風土」の総合効果に続く大きなものであることが分かる．

これらの結果から，情報漏えいにつながる行動をとらせないためにすべき対策の優先順位としてはまず「不正容認風土」の改善，次に「コンプライアンス意識」の向上が考えられる．

仮説 7-2 から仮説 7-5 で見る「従業員満足度」から「不正容認風土」「ポリシ違反意図」へのパス係数の値は負となり，一方で「コンプライアンス意識」「ルールの認知」へのパス係数の値は正となり，総じて「従業員満足度」の向上が間接的に情報漏えいにつながる行動を軽減する効果（−0.168）を持つことが分かった．

6. おわりに

本研究では，情報漏えいにつながる行動に影響を与えている要因，またそれらの要因間の関係を明らかにするために，モデルを構築し，それを構造方程式モデリング（SEM）を用いて分析した．

その結果，「不正容認風土」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「情報リテラシ」「ルールの認知」は「不正容認風土」「抵抗感のなさ」と比べるとそれほど大きな影響を与えないことが確認された．さらに，「コンプライアンス意識」が「情報漏えいにつながる行動」に対して与える直接的な影響はそれほど大きくないものの，（図 2 のモデルを想定する限り）他の要因を介して与える総合的な影響は「不正容認風土」に次ぐ大きなものとなるという結果が得られた．これに加えて，総じて「従業員満足度」の向上が間接的に「情報漏えいにつながる行動」を軽減する効果を持つことが確認され，一般的には，経営パフォーマンスの向上に用いられる従業員満足度も情報セキュリティの観点から問題となる行動にも影響を与えることが分かった．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，不正容認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直接的な効果はそれほど大きくないものの，様々な要因を介した間接的な効果をふ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も分かった．さらに，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ことが期待される．

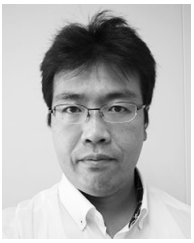
最後に，本研究の今後の展望について述べる．本研究で用いたアンケート調査には情報漏えいにつながる行動のほかにも，情報セキュリティの観点から問題となる行動（著作権侵害，業務と関係ないインターネット利用など）に関する質問項目があり，これらの事象ごとにその構造が同じなのか，異なるのかを明らかにしたいと思っている．また，不正容認風土と組織規模（従業員数）について今回の分析では考慮していなかったが，今後これらの関係についても分析を行っていきたい．さらに，これらの継続的に実施される調査結果を用いて，本研究で提案したモデルの頑健性の検証を行っていきたい．

謝辞 本研究は JSPS 科研費 25380345，26380466 の助成を受けたものです．

参考文献

[1] 情報処理推進機構：情報セキュリティ白書 2014 (2014).
[2] Albrechtsen, E.: A Qualitative Study of Users' Views on Information Security, *Computer and Security*, Vol.26, pp.276–289 (2007).
[3] Post, G.V. and Kagan, A.: Evaluating Information Security Tradeoffs: Restricting Access Can Interfere with User Tasks, *Computers and Security*, Vol.26, No.3, pp.229–237 (2007).
[4] Albrechtsen, E. and Hovden, J.: The Information Security Digital Divide between Information Security Managers and Users, *Computer and Security*, Vol.28, pp.476–490 (2009).
[5] Reason, J., Parker, D. and Lawton R.: Organizational Controls and Safety: The Varieties of Rule-Related Behaviour, *Journal of Occupational and Organizational Psychology*, Vol.71, pp.289–304 (1998).
[6] Whitman, M.E.: In Defense of the Realm: Understanding the Threats to Information Security, *International Journal of Information Management*, Vol.24, pp.43–57 (2004).
[7] Takemura, T.: Empirical Analysis of Behavior on Information Security, *Proc. 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*, pp.358–363 (2011).
[8] Takemura, T. and Komatsu, A.: An Empirical Analysis on Information Security Behaviors and Awareness, *Economics of Information Security and Privacy*, Bohme, R. (Ed.), pp.95–114, Springer (2013).
[9] 日本ネットワークセキュリティ協会：2013 年情報セキュリティインシデントに関する調査報告書：個人情報漏えい編 (2015).
[10] Ifinedo, P.: Understanding Information Systems Security Policy Compliance: An Integeration of the Theory of Planned Behavior and the Protection Motivation Theory, *Computers and Security*, Vol.31, No.1, pp.83–95 (2012).
[11] Warlentin, M. and Willison, R.: Behavioral and Policy Issues in Information Systems Security: The Insider Threat, *European Journal of Information Systems*, Vol.18, No.2, pp.101–105 (2009).
[12] Pee, L.G.. Woon, I.M.Y. and Kankanhalli, A.: Explaining Non-Work-Related Computing in the Workplace: A Comparison of Alternative Models, *Information and Management*, Vol.45, No.2, pp.120–130 (2008).
[13] D'Arcy, J., Hovav, A. and Galletta, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, *Information Systems Research*, Vol.20, No.1, pp.79–98 (2009).

[14] Peace, A.G., Galletta, D.F. and Thong, J.Y.L.: Software Piracy in the Workplace: A Model and Empirical Test, *Journal of Management Information Systems*, Vol.20, No.1, pp.153–177 (2003).
[15] 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（調査編：従業員の組織帰属意識等に関する調査）(2013).
[16] 大隅 昇：インターネット調査の抱える課題と今後の展開，ESTRELA, No.143, pp.2–11 (2006).
[17] Kotulic, A.G. and Clark, J.G.: Why There Aren't More Information Security Research Studies, *Information and Management*, Vol.41, pp.597–607 (2004).
[18] 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).
[19] 星野崇宏：調査観察データの統計科学—因果推論・選択バイアス・データ融合，岩波書店 (2009).
[20] 石田 浩，佐藤 香，佐藤博樹，豊田義博，萩原牧子，萩原雅之，本多則惠，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，No.42 (2009).
[21] 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, pp.157–177 (2008).
[22] 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.), pp.181–198, IGI Global Publication (2014).
[23] 浜屋 敏：情報セキュリティと組織感情，Enterprise 2.0，研究レポート（富士通総研経済研究所），No.345 (2009).
[24] Anderson, R. and Moore, T.: Information Security: Where Computer Science, Economics and Psychology Meet, *Philosophical Trans. Royal Society*, Vol.367, pp.2717–2727 (2009).
[25] Siponen, M. and Vance, A.: Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations, *MIS Quarterly*, Vol.34, No.3, pp.487–502 (2010).
[26] 村田 潔：情報倫理：インターネット時代の人と組織，pp.304–340, 有斐閣選書 (2004).
[27] 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).
[28] Siponen, M.: A Conceptual Foundation for Organizational Information Security Awareness, *Information Management and Computer Security*, Vol.8, pp.31–41 (2000).
[29] Woon, I.M.Y. and Pee, L.G.: Behavioral Factors Affecting Internet Abuse in the Workplace: An Empirical Investigation, *Proc. 3rd Annual Workshop on HCI Research on MIS*, pp.80–84 (2004).
[30] 豊田秀樹：共分散構造分析［応用編］—構造方程式モデリング，朝倉書店 (2004).
[31] Hair, Jr, J.F., Anderson, R.E, Thatham R.L. and Black, W.C.: *Multivariate Data Analysis*, Prentice-Hall International (1998).
[32] 星野崇宏，岡田謙介，前田忠彦：構造方程式モデリングにおける適合度指標とモデル改善について：展望とシミュレーション研究による新たな知見，行動計量学，Vol32, No.2, pp.209–235 (2005).
[33] Sharma, S., Mukherjee, S., Kumar, A. and Dillon, W.R.: A Simulation Study to Investigate the Use of Cutoff Values for Assessing Model Fit in Covariance Structure Models, *Journal of Business Research*, Vol.58, pp.935–943 (2005).



竹村 敏彦 （正会員）

1975 年生．1998 年関西大学総合情報学部総合情報学科卒業．2002 年大阪大学大学院修士課程修了．2006 年同博士課程修了．博士（応用経済学）．2005 年関西大学ポストドクロラルフェロー．2008 年関西大学助教．2013 年佐賀大学准教授．セキュリティエコノミックスの研究に従事．電子情報通信学会，日本経済学会，日本経済政策学会，公益事業学会各会員．

三好 祐輔

1972 年生．2000 年京都大学大学院修士課程修了．2003 年同博士課程修了．博士（経済学）．2003 年京都大学 21 世紀 COE 研究員．2004 年佐賀大学助教授．2015 年香川大学准教授．法の経済分析の研究に従事．2013 年全日本能率連盟賞受賞．日本経済学会，日本経営学会各会員．

花村 憲一

1977 年生．2001 年東邦大学理学部情報科学科卒業．2001 年日本コンピュータセキュリティリサーチ株式会社研究員．2001 年特別認可法人情報処理振興事業協会研究員．2012 年（独）情報処理推進機構主任．企業や個人の情報セキュリティ対策の研究に従事．日本情報経営学会会員．