原著論文

組織における個人情報保護行動モデルの構築
―従業員の個人情報保護行動を促進するためには―

Develop a Model of Behavior of Personal Information Protection in Organizations

キーワード：
個人情報保護，アンケート調査，人間行動モデル，情報管理，共分散構造分析
keyword：
Personal information protection, Questionnaire, Human behavior model, Information management, Covariance Structure Analysis

東京都市大学　梅　原　英　一
Tokyo City University　Eiichi UMEHARA

株式会社日本能率協会総合研究所　加　藤　菜美絵
JMA Research Institute Inc.　Namie KATO

奈良先端科学技術大学院大学　諏　訪　博　彦
Nara Institute of Science and Technology　Hirohiko SUWA

立命館大学　小　川　祐　樹
Ritsumeikan University　Yuki OGAWA

京都橘大学　杉　浦　　昌
Kyoto Tachibana University　Masashi SUGIURA

原稿受付：2019年５月27日
掲載決定：2019年12月11日

梅原英一・加藤菜美絵・諏訪博彦・小川祐樹・杉浦　昌

要　約

個人情報は，管理や取扱いに十分な注意が必要な情報である。多くの組織では，個人情報を保護するための組織内の規則およびルールが策定されている。さらに従業員に個人情報保護に関する教育と訓練を行っている組織も多い。組織では個人情報保護に対する注目が高まっている。しかし，情報漏洩や紛失などの事故は依然として発生している。そこで本研究では，組織に所属する従業員の個人情報保護行動モデルを構築する。600人の従業員にアンケート調査を実施し，探索的因子分析，検証的因子分析および共分散構造分析を用いて分析した。その結果，知識が態度に影響を与え，態度がスキルに影響を与え，個人情報保護行動につながる個人情報保護行動モデルを構築した。この結果を踏まえて，従業員の個人情報保護を促進する方法を提案する。

Abstract

Personal information needs to be carefully managed and handled in an organization. Rules in an organization and laws for protecting personal information have been developed. In addition, many organizations provide employees with education and training on personal information protection. A focus on such protection is increasing in organizations. However, incidents such as information leakage and loss are still occurring. Therefore, our aim was to develop a personal information protection behavior model of employees working in an organization. We conducted a questionnaire survey on 600 employees. This questionnaire was analyzed using exploratory factor analysis, confirmatory factor analysis and covariance structure analysis. As a result, we developed a personal information protection behavior model in which knowledge affects attitudes, attitudes influence skills, and leads to personal information protection behavior. On the basis of this result, we propose how to promote personal information protection for employees.

1　はじめに

情報技術の進展により情報の入手は容易になる。個人情報を利用することにより，企業はサービス向上や売上，利益増を目指すことが可能になる。しかし個人情報は流出してしまうと取り返しのつかない被害になってしまう可能性もある。このことから管理や取扱いには十分な注意が必要である。個人情報の保護法制として，「個人情報の保護に関する法律（個人情報保護法）」が2003年５月に公布されている。また2015年９月の改正で個人情報の定義の明確化，新たに匿名加工情報および要配慮個人情報が定義され，第三者提供に係る事項の追加等，その取扱いに関する規定も整備された。経済産業省（2016）は，「この改正では，特定の個人を識別することができないように加工された『匿名加工情報』を新たに定義し，本人の同意に代わる一定の条件の下，ビッグデータをはじめとするパーソナルデータの自由な利活用を認めることにより，新産業・新サービスが創出できる環境を整えることとされた。」と述べており，ビッグデータやAIへのデータ活用への道を開いたと言える。しかし，大手就職情報サイトが学生の内定辞退率を人工知能（AI）で予測し，企業に販売していた問題で個人情報保護委員会から指摘を受け，その販売を一時休止した（2019年８月２日読売新聞）報道に見られるように，企業の個人情報保護に対する行動が十分に確立されているとは言い難い。

個人情報保護マネジメントシステムは，2005年の個人情報保護法の施行を受けて，JIS Q15001：2006として公表された。その後2015年の個人情報保護法の改正を受けてJIS Q15001：2017が公表された。この改正点は要配慮個人情報，トレーサビリティの確保，オプトアウト規制の強化，外国事業者への第三者提供，個人データの消去の努力義務，匿名加工情報などがある。また，ISO 9001（QMS）やISO 14001（EMS），ISO/IEC 27001（ISMS）などのマネジメントシステム規格との整合性を図るため，ISO規格に近接した規格構成をとっている。これはOECD個人情報保護の８原則（OECD（2013））(収容制限の原則，データ内容の原則，目的明確化の原則，利用制限の原則，安全保護の原則，公開の原則，個人参加の原則，責任の原則）に対応する個人情報保護マネジメントシステムである。

実際に多くの組織では従業員に対して，個人情報保護に関する教育・研修を実施するなどの対策を講じており，個人情報保護に対する関心は高まっている。

しかし，このような法律や規格及び教育等の組織的な対策があるにもかかわらず，個人情報の漏洩事故は起こっている。NPO日本ネットワークセキュリティ協会（2017）によると，2014年に起こった個人情報漏洩件数は1,591件，2015年は78件，2016年は468件であった。近年減少しているようにみえるが，これは１件あたりの漏洩人数が少ない場合や漏洩した個人情報が暗号化されていたもしくは機微な情報が漏洩していない場合は公表不要であると判断される場合があることによる影響も考えられると述べている。１件あたりの漏洩人数は３万1,453人，１件あたりの平均想定被害賠償額は６億2,811万円である。個人情報漏洩による被害は，企業の信用を失うだけでなく，企業の存続にも影響を与える。

これらの背景に基づき，本研究は組織に所属する従業員が，個人情報保護行動をとるためのモデルを構築することを目的とする。このことは，従業員が個人情報保護行動をとるためのメカニズムを明らかにし，個人情報行動を促進するための示唆を提示することとなり，社会的意義があると考える。

本論文の構成を以下に示す。２章では関連研究を整理し，３章では関連研究の整理に基づき個人情報保護行動モデルの仮説を設定する。４章では調査概要について述べ，５章では調査結果を報告

する。6章では結果に基づく考察について述べる。7章で結論と今後の課題をまとめる。

2　関連研究

人間の社会的行動に関する研究は，社会心理学の分野で多くなされている。人間の行動を説明するモデルとして，Ajzen & Fishbein（1980）の合理的行動理論や，Ajzen（1991）の計画的行動理論がある。Ajzen & Fishbein（1980）は，人間が行動にいたるまでの心理プロセスを段階的な構造を持つとして，態度が行動意図を規定し，行動意図が行動を規定するモデルを構築している。このモデルは，消費行動やweb上のコミュニケーション行動，環境配慮行動，情報セキュリティ行動など様々な分野で応用されている（廣瀬 1994，小池ら 2003，三坂 2003，諏訪ら 2006，諏訪ら 2012）。

諏訪ら（2006）は，なぜ人々が環境配慮行動を示さないのかを明らかにするための研究を行っている。環境配慮行動は，環境保全に対する積極的な態度に関わらず行動に至らない「高態度低行動」の典型的な行動である。この図式はセキュリティ行動や個人情報保護行動にも当てはまる。すなわち，セキュリティや個人情報保護に対する知識や態度は身についているものの，行動が伴わないという態度と行動の不一致が発生するのである。

この不一致を説明するために，諏訪ら（2006）は，Ajzen & Fishbein（1980），Ajzen（1991）らの理論に基づく「環境配慮行動の要因連関モデル（広瀬 1994）」，「環境問題認識の構造モデル（小池ら 2003）」，「環境問題の認知・行動モデル（三坂 2003）」などの先行研究に基づき，関心・動機・行動モデルを構築している。さらに，この関心・動機・行動モデルを拡張して情報セキュリティ分野に適用し，なぜ人々は情報セキュリティ行動を示さないのかを調査している。その結果，（1）セキュリティ知識，セキュリティスキルといったユーザが持つ知識レベルが無力感，関心，コスト感，貢献感，外部要請というセキュリティ態度に影響を与えること，（2）セキュリティ行動には，予防的セキュリティ行動，習慣的なセキュリティ行動，および意識的なセキュリティ行動の3種類があること，（3）セキュリティ態度が3つのセキュリティ行動に影響を与えることを示している。

井上ら（2017）は，これらの先行研究によって積み上げられた知見を個人情報保護の分野に適用し，大学生に対するアンケート調査に基づいて個人情報保護の関心とそれに関連する行動との関係を分析している。その結果，彼らは関心が行動に影響を与えることを明らかにしている。しかしながら，この調査の対象者の多くは大学生であり，組織における個人情報保護行動の対象者としてふさわしいとは言い難い。また，組織における情報セキュリティや個人情報保護行動へ影響を及ぼす要因についても議論されてない。

組織における情報セキュリティの分野において，浜屋（2009，2011）は，会社員を対象にアンケートを行い，情報セキュリティが組織に与える影響を分析している。その結果，職場の実態を踏まえた情報セキュリティ対策が行われていないと，従業員の士気を低下させ，組織活性化を奪うと述べている。さらに，浜屋（2009）は，従業員の情報セキュリティ行動の実効性を高めるためには，組織風土を考慮した対策を講じる必要があると述べている。しかしながら，この研究では組織におけるセキュリティに着目しており，組織における個人情報保護行動に着目しているわけではない。

杉浦ら（2011）は，組織内でセキュリティ対策を指示する立場のセキュリティ推進部門とその指示を受けて実施する立場の従業員の行動をモデル化し，組織内のセキュリティ対策をゲーム理論により分析している。この研究では事例の一部として組織における個人情報保護行動を対象にしているものの，ゲーム理論に基づいて従業員の行動を構造的にモデル化するものであり，行動を規定

する要因やその構造について調査したものではない。

組織の一員としての従業員の個人情報保護行動を議論するには，社会心理学の知見に基づく人間行動モデルが必要であるが，モデル構築にあたり組織風土などの組織特有の要因を検討する必要がある。本研究では，従業員が個人情報保護行動を示すためのメカニズムを明らかにするために，諏訪ら (2012) の情報セキュリティモデルを拡張し，組織風土を含めた組織における個人情報保護行動モデルを構築することを目的とする。

3　仮説の構築

本章では，個人情報保護行動に影響を与える要因について先行研究に基づき検討し，個人情報保護行動モデルの仮説を構築する。

3.1　従業員の個人情報保護行動モデル

本研究では，諏訪ら（2012）の一般個人を対象とした情報セキュリティ行動モデルを拡張し，従業員の個人情報保護行動モデルを構築する。彼らの合理的行動理論および計画的行動理論に基づく情報セキュリティ行動のモデルは，情報セキュリティに関する知識・スキルが態度（情報セキュリティに関するコスト感，貢献感，外部要請）に影響を与え，この態度が情報セキュリティ行動（予防的，習慣的，意識的行動）に影響を与えていた。本研究でも，知識（知識，スキル，経験）が個人情報保護に関する態度に影響を与え，個人情報保護に関する態度が，組織内の個人情報保護行動を促進すると仮定する。このために（１）知識（知識，スキル，経験），（２）態度（関心，リスク認知，有効性認知，コスト感，組織風土），（３）行動（人的，技術的）という３つの要因を設定した。

これらの要因を用いて，諏訪ら（2012）の一般個人の情報セキュリティ行動の仮説を拡張し，組織の従業員を対象とした個人情報保護行動モデルを構築した。その結果，本研究の基本的な仮説は，「個人情報保護の知識・スキル・経験が態度に影響を与え，これらの態度が個人情報保護行動を促進する」とする。これを図１に示す。

組織においては，ある程度の個人情報保護に関する教育が行われていることが想定されるため，従業員は個人情報保護に関する知識・スキル・経験を保有している。それらの知識・スキル・経験から個人情報保護に関する態度に影響を与える。この態度が個人情報保護行動を促進するというモデルである。

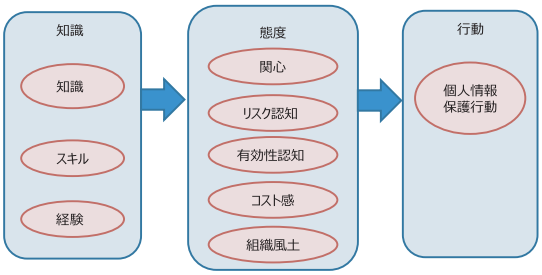


図１　仮説：従業員の個人情報保護行動モデル

3.2　個人情報保護行動の要因

3.1節の仮説における３つの要因（（１）知識（知識，スキル，経験），（２）態度（関心，リスク認知，有効性認知，コスト感，組織風土），（３）行動（人的，技術的））を説明する。

3.2.1　知識（知識，スキル，経験）

本研究では，諏訪ら (2012) のモデルと同様に，個人情報保護行動には，個人情報保護や情報セキュリティに関する知識やスキルが必要であると仮定する。また彼らのモデルと同様に，このような知識やスキルには，従業員自身またはそれらの近くにいる人々によって引き起こされる個人情報漏洩事件の経験も含まれると考える。所属する組織の個人情報保護に対する組織風土や自身や身近な人（同僚や先輩，上司）が個人情報に関する被害を受けたことがある，被害を与えたことがあるといった経験も要因に含まれると考えた。

3.2.2　態度（関心，リスク認知，有効性認知，コスト感，組織風土）

本研究では，諏訪ら（2012）のモデルを組織の従業員を想定して拡張し，個人情報保護の態度に対する要因として５つ設定した。（１）個人情報保護に対する従業員の「関心」，（２）脅威に対する危機感などの従業員の「リスク認知」，（３）個人情報に対する「有効性認知」，（４）個人情報保護にかける従業員の「コスト感（時間や努力）」，（５）「組織風土」である。

諏訪ら(2012)は，態度の要因として情報セキュリティに対する「関心」，脅威への危機感といった「リスク認知」，セキュリティ対策への「有効性認知」，「お金がかかる」「手間がかかり，面倒である」といった「コスト感」，他者からセキュリティ行動を要請される「外部要請」の５つを仮定した。本研究ではこのうち「外部要請」を除外した。これは従業員の個人情報保護は，一般個人と異なり業務として取り扱うため「外部要請」ではなく，強制と考えたためである。

一方，浜屋(2011)は，組織における情報セキュリティ対策には，情報セキュリティポリシーの策定や情報セキュリティ教育などの正式な対策だけでなく，情報セキュリティに関する組織風土の開発も必要であると述べている。そこで本研究では個人情報保護に対する組織的な態度の要因として組織風土を設定した。

3.2.3　行動（人的，技術的）

本研究では個人情報保護行動には，人的側面を含む個人情報保護行動と，ITの利用など技術面を含む情報セキュリティ行動の２種類があると仮定した。

4　調査概要

３章で設定した仮説を検証するために，アンケート調査を実施した。質問項目は，「個人情報保護に関する知識」，「個人情報保護に関するスキル」，「個人情報保護に関する経験」，「個人情報保護に関する態度及び所属する組織の組織風土」，「個人情報保護に関する行動」に大別される。

4.1　調査方法

調査方法は，インターネット調査とし，2017年９月１日～25日に実施した。調査対象は，正社員または契約社員として就業し，業務で個人情報を扱う20歳～59歳のインターネットモニターである。回答者が600人になった時点で回収を終了している。なおサンプルが偏らないように，回収時に性別／年代での割付を実施し，各75名ずつ回収を行った。表１に被験者の特徴を示す。

表１　被験者の特徴

性別年代＼役職		常勤					非常勤			合計
		役員	部長	課長	係長	他	役員	係長	他	
男	20		1	3	11	54		1	5	75
	30	1	4	11	12	46			1	75
	40	2	9	14	24	23			3	75
	50	5	15	20	16	17			2	75
女	20	1			2	64	1		7	75
	30	1	2	2	6	52			12	75
	40	1		2	8	52			12	75
	50	5	2	7	9	41			11	75
合計		16	33	59	88	349	1	1	53	600

4.2　調査項目

本調査では，個人情報保護行動モデルに基づき調査項目を設定した。なお知識以外の要因は，基本的に本人がどう考える／思うかが問題となる。よって，これらの要因については，諏訪ら(2012)などの従来研究を参考に質問紙を設定し，本人の考え・思いを収集したうえで因子分析を用いて潜在変数を作成する。一方で，知識は本人が考える／思うのではなく，正しい答えが存在し，それに

対して本人が正しい答え（知識）を所持しているかが問題になる。そのため，正誤の存在する問題の正当総数により指標化する。

4.2.1　個人情報保護に関する知識

個人情報保護士認定公式テキスト（2016）を参考に個人情報と要配慮個人情報を問う23項目を作成した。被験者に対し，各項目に対して書いてある内容が個人情報にあてはまると思えば「はい」あてはまらないと思えば「いいえ」の回答を依頼した。

t検定を使用して，管理グループ（役員，部長，課長，係長）と非管理グループ（その他）の間で個人情報保護に関する知識に統計的に有意な差があるかどうかを調べた。 その結果，管理職の正解率は83.5％，非管理職の正解率は83.6％であり，両者の間に有意差は見られなかった。そのため，従業員の個人情報保護に関する知識は，役職によって異ならないことがわかった。

4.2.2　個人情報保護に関するスキル

個人情報保護行動は情報セキュリティ行動を含むので，諏訪ら（2012）の情報セキュリティスキルの質問項目に加え，個人情報保護士認定公式テキスト(2016)を参考に「一定時間以上にわたって席を離れる場合は机上の書類は引き出しに保管するか，施錠管理のできるロッカーに保管することができる」といった個人情報保護行動特有の項目を追加し，合計31項目を設定した。それぞれの項目について，実際にスキルを持っているかどうかを「全くそう思わない」から「とてもそう思う」までの５段階で回答を依頼した。

4.2.3　個人情報保護に関する経験

従業員自身や身近な人（同僚や先輩，上司）の個人情報漏洩や被害を受けた経験について10項目を設定した。各質問に対して，被験者は，実際に経験したかどうかに関して，「全くそう思わない」から「とてもそう思う」までの５段階で回答をした。

4.2.4　個人情報保護に関する態度・組織風土

個人情報保護に対する態度および個人情報保護に対する組織風土について27項目の質問を設定した。それぞれの項目について，あてはまるかどうかを「あてはまらない」から「あてはまる」までの５段階で回答を依頼した。

4.2.5　個人情報保護に関する行動

4.2.2節の「個人情報保護に関するスキル」で設定した31項目について，実際に実施しているかどうかを，「全く実施していない」から「とてもよく実施している」までの４段階で回答を依頼した。実施しているかどうか分からない場合は，「実施しているか分からない」を選択するように依頼した。

5　調査結果

本章では，４節で設定した項目の分析結果を述べる。分析方法として，個人情報保護に関する知識については，スコアとして23問中の正解総数を使用した。そのほかの要因については因子分析を用いた。探索的および検証的因子分析を用いて，観察変数および潜在変数を特定した。その後，知識スコアを加えて共分散構造分析を行い，パス図を作成した。

5.1　個人情報保護に関する知識

図２に個人情報保護に関する知識に対する被験者の正解数の分布を示す。個人情報に関する平均点は12.4点（15点満点），標準偏差は1.6であった。要配慮個人情報に関する平均値は6.9点（８点満点），標準偏差は1.7であった。この二つを合計した平均は19.2点（23点満点），標準偏差は2.7であった。本研究では各被験者の合計点を知識の説

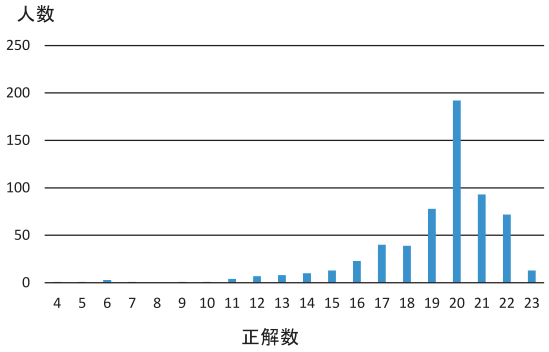


図２　個人情報保護に関する知識の正解数

明変数として用いる。

5.2　探索的因子分析

アンケートから要因を特定するために，SPSS Statistics Ver.22を用いて，スキル，経験，態度・組織風土，行動のそれぞれについて探索的因子分析を行った。

5.2.1　個人情報保護に関するスキル

スキルに関する項目に対して因子分析(最尤法，プロマックス回転）を行った。その結果，固有値１以上の因子が４因子抽出された。累積寄与率は69.9％であった。この４因子を「情報セキュリティスキル」，「人的セキュリティスキル」，「個人情報保護スキル」,「システムセキュリティスキル」とすることにした。

5.2.2　個人情報保護に関する経験

経験に関する項目に対して因子分析（最尤法，プロマックス回転）を行った。その結果，固有値１以上の因子が２因子抽出された。累積寄与率は56.1％であった。この因子を「他人の被害を聞いた事がある」，「被害を与えた経験がある」とすることにした。

5.2.3　個人情報保護に関する態度・組織風土

態度と組織風土に関する質問項目に対して因子分析（最尤法，プロマックス回転）を行った。その結果，固有値１以上の因子が６因子抽出された。累積寄与率は61.6％であった。この因子を「個人情報は重要（関心，有効性認知）」，「個人情報保護対策は面倒（コスト感）」，「職場が個人情報保護に熱心（組織風土）」，「被害を避けたい（リスク認知）」，「関心がない」，「個人情報保護対策は効果がない」とすることにした。

5.2.4　個人情報保護に関する行動

行動に関する質問項目に対して因子分析（最尤法，プロマックス回転）を行った。その結果，固有値１以上の因子が４因子抽出された。累積寄与率は65.4％であった。この因子を「人的セキュリティ行動」，「個人情報保護行動」，「システムセキュリティ行動」,「不審な物には気をつける行動」とすることにした。

5.3　検証的因子分析

探索的因子分析の結果に基づき，共分散構造分析に使う潜在変数とそれに対応する観測変数を特定する。統計ソフトはSPSS Amos Ver.22を使用した。

5.3.1　個人情報保護に関するスキル

本モデルの適合度指標はGFIが0.935，CFIが0.971，P値が0.01未満で統計的に有意であった。潜在変数は４つで，「情報セキュリティスキル」で５つの測定変数，「人的セキュリティスキル」で４つの測定変数，「個人情報保護スキル」で４つの測定変数，「システムセキュリティスキル」で２つの測定変数が抽出された。これを表２に示す。

5.3.2　個人情報保護に関する経験

本モデルの適合度指標はGFIが0.905，CFIが0.930，P値が0.01未満で統計的に有意であった。潜在変数は２つで，「他人の被害を聞いた事がある」に７つの測定変数，「被害を与えた経験がある」に２つの測定変数が抽出された。これを表３に示す。

表２　スキルの潜在変数と測定変数

潜在変数	測定変数
情報セキュリティスキル	有害なウェブサイトへのアクセスを防止するソフトまたはサービスを導入・活用方法を理解し，かつ実行できる(Q7-1-3)
	WindowsUpdate 等によるセキュリティパッチの更新の手順を理解し，かつ実行できる(Q7-1-1)
	セキュリティ対策ソフトを導入・活用方法を理解し，かつ実行できる(Q7-1-2)
	ウェブサイトの安全評価ツールの役割を理解し，かつ実行できる(Q7-1-4)
	重要なデータをバックアップする手順を理解し，かつ実行できる(Q7-1-6)
人的セキュリティスキル	業務時間中に一定時間以上にわたって席を離れる場合は，机上の書類は引き出しに保管するか，裏返しにしておくことができる(Q7-3-7)
	業務時間終了後は，すべての書類や電子媒体，ノートパソコンなどを机上に放置せず，施錠管理できるロッカーに保管することができる(Q7-3-8)
	業務時間中は，使用していない書類や電子媒体などを机上に放置せず，施錠管理できるロッカーに保管することができる(Q7-3-6)
	情報の重要性に応じて，オフィス内の情報の置き場所を分けることができる(Q7-3-9)
個人情報保護スキル	第三者に個人情報を提供する場合は，本人に同意を得ることができる(Q7-2-8)
	本人からの「個人情報の開示請求」には応じることができる(Q7-2-7)
	個人情報を他人に渡す際は，本人の同意を得ることができる(Q7-2-6)
	第三者に個人情報を提供する場合は，第三者に提供した記録をとることができる(Q7-2-9)
システムセキュリティスキル	システムの品質確保のため，やむを得ず本番データによるテストが必要な場合には，個人情報を含む本番データ利用の事前承認をし，個人情報のマスキング，置き換え，暗号化ができる(Q7-2-2)
	個人情報を管理しているファイルサーバーにパスワードを設定できる(Q7-2-1)

表３　個人情報保護に関する経験の潜在変数と測定変数

潜在変数	測定変数
他人の被害を聞いた事がある	忙しいときに個人情報保護のことを考えるのは面倒である(Q9-10)
	他人が，私の身近な人（同僚や先輩，上司）の個人情報を流出した経験がある(Q9-7)
	他人が，私の身近な人（同僚や先輩，上司）の個人情報を流出して被害を受けた経験がある(Q9-9)
	私の身近な人（同僚や先輩，上司）は，他人の個人情報を流出して被害を受けた経験がある(Q9-8)
	私の身近な人（同僚や先輩，上司）は，他人の個人情報を流出した経験がある(Q9-6)
	他人が，私の個人情報を流出した経験がある(Q9-3)
	他人が，私の個人情報を流出して被害を受けた経験がある(Q9-5)
被害を与えた経験がある	私は，他人の個人情報を流出した経験がある(Q9-2)
	私は，他人の個人情報を流出して被害を与えた経験がある(Q9-4)

5.3.3　個人情報保護に関する態度・組織風土

本モデルの適合度指標はGFIが0.896，CFIが0.939，P値が0.01未満で統計的に有意であった。潜在変数は６つ抽出された。第１が「個人情報保護は重要（関心，有効性認知）」という態度で測定変数が６つ，第２に「個人情報保護対策は面倒（コスト感）」という態度で測定変数が５つ，第３に「職場が個人情報保護に熱心（組織風土）」という組織風土で測定変数４つ，第４に「被害を避けたい（リスク認知）」という態度で測定変数が３つ，第５に「関心がない」という態度で測定変数が２つ，第６に「個人情報保護対策は効果がない」という態度で測定変数が２つである。これを表４に示す。

表４　個人情報保護に関する態度・組織風土の潜在変数と測定変数

潜在変数	測定変数
個人情報保護は重要（関心，有効性認知）	社会にとって，個人情報保護は重要な問題である(Q8-1-10)
	個人情報保護は，高めるべきである(Q8-1-6)
	個人情報の流出は，身近な問題である(Q8-1-7)
	個人情報保護に，関心を持っている(Q8-1-8)
	コストをかけても個人情報保護対策をすべきである(Q8-1-9)
	現代社会は，個人情報保護対策を求めている(Q8-1-5)
個人情報保護対策は面倒（コスト感）	複数パスワードの管理は面倒くさい(Q8-2-5)
	データのバックアップは，手間がかかる(Q8-2-4)
	セキュリティ対策ソフトの導入は，お金がかかる(Q8-2-2)
	WindowsUpdate 等によるセキュリティパッチの更新は，わずらわしい(Q8-2-1)
	個人情報保護対策を行うと，利便性が損なわれる(Q8-2-3)
職場が個人情報保護に熱心（組織風土）	個人情報保護について，詳しい同僚や先輩，上司がいる(Q8-1-1)
	職場の同僚や先輩，上司は個人情報保護対策をしている人が多い(Q8-1-2)
	職場が，個人情報保護教育に熱心である(Q8-1-4)
	職場から，個人情報保護対策を求められている(Q8-1-3)
被害を避けたい（リスク認知）	私が，個人情報保護対策を行うと，被害にあう確率を下げる効果がある(Q8-3-1)
	私が，個人情報保護対策を行うと，被害の規模を小さくする効果がある(Q8-3-2)
	WindowsUpdate 等によるセキュリティパッチの更新は，安全性を高める効果がある(Q8-3-3)
関心がない	個人情報漏洩やウィルス感染は，私には関心ない(Q8-2-10)
	私の個人情報が流出しても大した問題ではない(Q8-2-7)
個人情報保護対策は効果がない	私が，個人情報保護対策をしても被害を防ぐことはできない(Q8-3-4)
	私が，個人情報保護対策をしても効果はない(Q8-3-3)

5.3.4　個人情報保護に関する行動

本モデルの適合度指標はGFIが0.902，CFIが0.954，P値が0.01未満で統計的に有意であった。潜在変数は４つで，「人的セキュリティ行動」に６つの測定変数，「個人情報保護行動」に８つの測定変数，「システムセキュリティ行動」に５つの測定変数，「不審な物には気をつける行動」に３つの測定変数が抽出された。これを表５に示す。

表５　個人情報保護に関する行動の潜在変数と測定変数

潜在変数	測定変数
人的セキュリティ行動	業務時間終了後は，すべての書類や電子媒体，ノートパソコンなどを机上に放置せず，施錠管理できるロッカーに保管している(Q10-3-8)
	パソコンを他人に使用されないように，パスワード付きのスクリーンセーバーを起動し，一定時間が経つと画面がロックされる設定にしている(Q10-3-4)
	業務時間中に一定時間以上にわたって席を離れる場合は，机上の書類は引き出しに保管するか，裏返しにしている(Q10-3-7)
	情報の重要性に応じて，オフィス内の情報の置き場所を分け，そのエリアに入室しアクセスできる人を社員証やバッジなどによりアクセスできる人を識別している(Q10-3-10)
	業務時間中は，使用していない書類や電子媒体などを机上に放置せず，施錠管理できるロッカーに保管している(Q10-3-6)
	情報の重要性に応じて，オフィス内の情報の置き場所を分けている(Q10-3-9)
個人情報保護行動	個人情報を他人に渡す際は，本人の同意を得ている(Q10-2-6)
	メールや FAX を送る際に操作マニュアルどおりに運用している(Q10-2-10)
	個人情報を取得するときは，何に使うか目的を決めて，本人に伝えている(Q10-2-3)
	第三者に個人情報を提供する場合は，第三者に提供した記録をとっている(Q10-2-9)
	取得した個人情報は安全に管理をしている(Q10-2-5)
	取得した個人情報を決められた目的にのみ使用している（ほかの目的には使わない）(Q10-2-4)
	本人からの「個人情報の開示請求」には応じている(Q10-2-7)
	第三者に個人情報を提供する場合は，本人に同意を得ている(Q10-2-8)
システムセキュリティ行動	有害なウェブサイトへのアクセスを防止するソフトまたはサービスを導入，活用している(Q10-1-3)
	セキュリティ対策ソフトを導入，活用している(Q10-1-2)
	暗号化された USB メモリの利用や重要なファイルを暗号化している(Q10-1-5)
	WindowsUpdate 等によるセキュリティパッチの更新している(Q10-1-1)
	ウェブサイトの安全評価ツールを利用している(Q10-1-4)
不審な物には気をつける行動	不審な電子メールの添付ファイルは開かないようにしている(Q10-1-7)
	怪しいと思われるウェブサイトにはアクセスしないようにしている(Q10-1-8)
	よく知らないウェブサイトではファイル（ソフトウェア）をダウンロードしないようにしている(Q10-1-9)

5.4　共分散構造分析

5.3節で抽出した潜在変数を用いて因果関係をモデル化するために共分散構造分析を行った。その結果を図３に示す。GFIが0.773，CFIが0.766，P値が0.01未満であった。この結果から個人情報保護に関する知識が従業員の態度や組織風土に影響を与える。次にこれらの態度や組織風土によりスキルの向上が図られる。最終的に，これらのスキルを用いて個人情報保護行動を示すということが明らかになった。

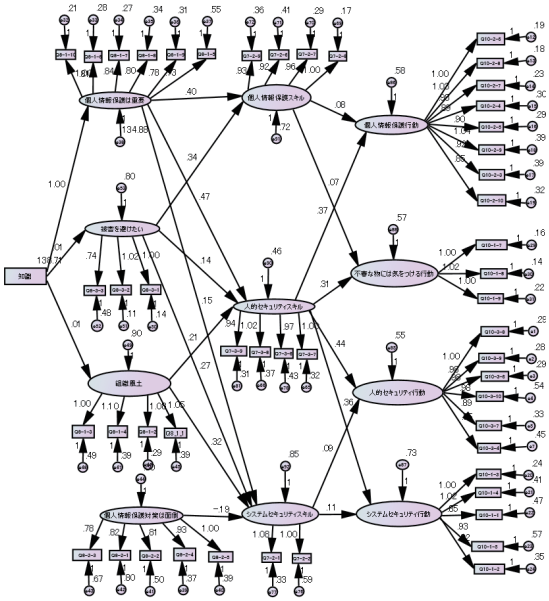
図３は，図１に示した仮説及び諏訪ら（2012）の一般的な被検者を対象とした情報セキュリティ行動モデルと異なった。参考までに，諏訪らと同様の知識―スキル―態度―行動モデルで共分散構造的分析を行ったが有意な結果は得られなかった。この点に関しては，本研究の被験者が一般的な個人ではなく，組織の従業員であったことによる可能性が考えられる。

また，態度・組織風土―知識―スキル―行動モデルも検討したが，GFIが0.725と低下したために採用しなかった。

5.5　分析結果

本研究で得られた従業員の個人情報保護モデルは「知識―態度・組織風土―個人情報保護スキル―個人情報保護行動」となった。

第１に，個人情報保護の知識があると，現代社会は個人情報保護を求めている，個人情報保護に関心を持っているというような「個人情報保護は重要（関心，有効性認知）」，個人情報保護対策を行うと被害の規模を小さくする効果がある，Windows Update等によるセキュリティパッチの更新は，安全性を高める効果があるといった「被害を避けたい（リスク認知）」という態度に正の影響を与えるだけでなく，職場から個人情報保護



P=.000 GFI=.773 CFI=.766 RMSEA=.090 DF=1206 AIC=7274.656 CHI=7034.656

図３　従業員の個人情報保護行動モデル

対策を求められている，職場の同僚や先輩，上司は個人情報保護対策をしている人が多いといった「職場が個人情報保護に熱心（組織風土)」にも正の影響によりを与えていたことがわかった。その結果，従業員は「私の職場から個人情報保護が要求される」こと，および「職場の同僚，先輩，上司の多くが個人情報を保護すること」を認識するようになる。

第２に，知識の有無に関わらず，個人情報保護対策を行うと，利便性が損なわれる，複数のパスワードの管理は面倒くさいといった「個人情報保護対策は面倒（コスト感)」という否定的な態度があることが分かった。このような手間を厭う態度は，人間が本来持っているものである可能性がある。この否定的な態度がシステムセキュリティスキルに悪影響を及ぼしている事が分かった。しかしながら，「関心がない」および「個人情報保護対策は効果がない」は有意な潜在変数とはならなかった。

第３に，これら態度や組織風土は，「個人情報保護スキル」，「人的セキュリティスキル」，「システムセキュリティスキル」という３つのスキルに影響を与える。「個人情報保護スキル」は，「個人情報保護は重要（関心，有効性認知)」および「被害を避けたい（リスク認知)」という態度と正の相関があった。

「人的セキュリティスキル」および「システムセキュリティスキル」は,「個人情報保護は重要(関心, 有効性認知)」,「被害を避けたい(リスク認知)」及び「職場が個人情報保護に熱心（組織風土)」と正の相関があった。また，「システムセキュリティスキル」のみは「個人情報保護対策は面倒（コスト感)」と負の相関が見られた。

第４に，従業員がこのようなスキルを身につけると，「個人情報保護行動」「人的セキュリティ行動」「システムセキュリティ行動」「不審な物には気をつける行動」につながる。「個人情報保護行動」と「不審なものに気をつける行動」は，「個人情報保護スキル」および「人的セキュリティスキル」と正の相関があった。「人的セキュリティ行動」と「システムセキュリティ行動」は，「人的セキュリティスキル」および「システムセキュリティスキル」と正の相関があった。

結論として，従業員の知識を向上させることが不可欠である。さらに，個人情報保護に対する従業員の態度を改善し，組織内の個人情報を保護するための組織風土を改善する必要がある。その結果，従業員の個人情報保護に関するスキルが向上する。このスキルを使用することで，従業員は個人情報保護行動をすると考えられる。

6　考察

本章では，従業員に個人情報保護行動を促進させる対策，および先行研究の情報セキュリティ行動モデルとの比較について述べる。

6.1　組織における個人情報保護行動の促進対策

分析の結果，個人情報保護に関する知識が，従業員の態度や組織風土に影響を与え，それがスキルの向上につながり，個人情報保護行動をするということが明らかになった。そこで従業員に対して個人情報保護行動を促進する方策を提案する。

第１に従業員に個人情報保護に関する知識を完全に理解させる必要がある。本研究のアンケートで個人情報に関する知識を問う問題がある。業務で個人情報を扱う従業員は完全に理解すべき問題である。しかし不正解の比率が10％を超えているものがある。以下（　）内が不正解率である。個人情報に関する知識では，「官報，電話帳，職員録等で公にされている情報」（33.5％），「防犯カメラに記録された情報等，本人が判別できる映像情報」（14.3％），「特定個人を識別できる情報が記述されていなくても，周知の情報を補って識別することにより特定の個人を識別できる情報」（10.8％），「企業の財務情報等，法人等の団体そのものに関する情報」（63.8％），「記号や数字等の文字列だけから特定個人の情報であるかどうかの区別がつかないメールアドレス情報」（10.8％）の不正解率が10％を超えた。また，要配慮個人情報では人種（22.8％），信条（30.3％），社会的身分（21.8％）の不正解率が10％を超えた。これはどれも基礎的な知識である。これは社内研修などで従業員に必ず周知させなければならない。

第２に知識をベースに従業員の個人情報を保護することに対する態度を徹底しなければならない。態度や組織風土では，「個人情報保護は重要（関心，有効性認知）」，「被害を避けたい（リスク認知）」，「職場が個人情報保護に熱心（組織風土）」，「個人情報保護対策は面倒（コスト感）」の４因子が抽出された。パス図より「個人情報保護は重要」および「被害を避けたい」も３つのスキルすべてに，「職場が個人情報保護に熱心」は人的セキュリティスキルとシステムセキュリティスキル，「個人情報保護対策は面倒」はシステムセキュリティスキルと有意な関係があった。３つのスキルを高めるためには，個人情報保護の重要性とそのリスク認識をまず従業員に周知させる必要がある。その上で，個人情報保護に対する組織風土の向上および対策が面倒というコスト感を低減させ，セキュリティスキルの向上を促進すべきである。

第３に，従業員の態度や社内風土を改善した上で，従業員に個人情報保護に関するスキルを身につけさせる必要がある。スキルは３因子が抽出された。個人情報保護スキルは「個人情報保護行動」および「不審なものに気をつける行動」，人的セキュリティスキルは「不審なものに気をつける行動」，「人的セキュリティ行動」および「システムセキュリティ行動」，システムセキュリティスキルは「システムセキュリティ行動」を向上させる。従業員にはこれら３つのスキルをすべて身につけさせる必要がある。

6.2　仮説との比較

5.4節で述べたように，本研究の個人情報保護行動モデルは，図１に示した仮説及び諏訪ら（2012）の一般的な被検者を対象とした情報セキュリティ行動モデルと異なった。異なる点は２つである。

第１に，図１の仮説及び諏訪ら（2012）のモデルは知識とスキルが態度に正の影響を与える。この態度が情報セキュリティ行動を引き起こすというモデルであった。一方，本研究のモデルは知識が態度や組織風土に影響を与える。その結果，従業員のスキルが向上し，個人情報保護行動を引き起こすというものである。

この点に関しては，本研究の被験者が組織で個人情報を業務で取り扱っている人に限定したことによる可能性がある。彼ら全員が個人情報についてある程度の知識を持っていた可能性が高い。さらに業務として扱っているので，組織内の個人情報保護に関するマニュアルや社内規則が整備され

ていた可能性が高い。故に，事前に研修等で取扱規程が周知されている可能性が高い。つまり，知識のみならず態度・組織風土も事前に周知されている可能性が高い。その個人情報保護に関する知識や態度及び組織風土が高ければ，従業員の個人情報保護に関するスキルが向上する可能性がある。以上の点から，個人情報保護行動が組織内で行われている可能性がある。その結果，本研究で得られた知識―態度・組織風土―スキル―行動モデルが統計的に有意になった可能性がある。この点に関する詳細な調査は今後の研究課題とする。

第２に，個人情報保護に関する態度・組織風土の潜在的変数である「関心がない」と「個人情報保護対策は効果がない」の２つはスキルや行動と有意な関係が得られなかった。同様に，個人情報保護に関する経験の２つの潜在変数である「他人の被害を聞いた事がある」と「被害を与えた経験がある」もスキルや行動と有意な関係が得られなかった。この点に関しても，諏訪ら（2012）の情報セキュリティに関するモデルと異なる点である。

「関心がない」や「個人情報保護対策は効果がない」と言った態度，「他人の被害を聞いた事がある」，「被害を与えた経験がある」が統計的に有意にならなかったことは，本研究の被験者が「組織で個人情報を業務にとして扱っている従業員」に限定したことによるものと考えられる。諏訪ら（2012）の研究の被験者は一般的な個人であるのに対し，本研究の被験者は業務で個人情報を扱っている。つまり，個人情報保護の重要性は理解していた可能性が高かったと思われる。この点に関しても詳細な分析は今後の検討課題とする。

経験に関しては，知識及び態度・組織風土の中で，「被害を与えた経験がある」と「被害を避けたい（リスク認知）」は有意ではなかったが，それ以外の潜在変数とは統計的に有意であった。故に，経験が知識及び態度・組織風土に影響を与えており，その結果として知識や態度・組織風土が向上する可能性は捨てきれない。しかしこのモデルのGFIは0.748と低下したので，本論文では採用しなかった。経験が個人情報保護に関する知識及び組織風土にどのように影響を与えるかの詳細な分析についても今後の検討課題としたい。

7　結論と今後の課題

本研究は，諏訪ら（2012）が提示した合理的行動理論および計画的行動理論に基づく個人の情報セキュリティ保護行動モデルを拡張し，組織の従業員の個人情報保護行動モデルを仮説として設定した。これは，知識・スキルおよび経験が個人情報保護に対する態度に影響を与え，それが個人情報保護行動に影響を与えるというモデルであった。本研究ではこの仮説を検証するために600名の個人情報保護を扱う組織の従業員にアンケート調査を実施し，共分散構造分析によりモデルを構築した。しかしながら本研究では，仮説として提示したモデルは統計的に有意にならなかった。また個人情報保護に関する経験など一部の要因も統計的に有意とはならなかった。

本研究で統計的有意となったモデルは，知識の向上が従業員の個人情報保護に対する態度や個人情報保護に関する組織風土を向上させる。その態度や組織風土が従業員の個人情報保護のスキル向上を促す。そのスキルが向上すると従業員の個人情報保護行動が促進されるというモデルであった。

この差異の原因としては，諏訪ら（2012）のモデルが一般個人の情報セキュリティ行動を対象としたのに対し，本研究のモデルは個人情報保護を扱う組織の従業員を対象としたためという可能性が考えられる。従業員は業務の一環として個人情報を扱っている。故に，個人情報保護の重要性およびそのリスクや過去の事故や他人の経験は，程度の差はあれ事前に認識していた可能性がある。また知識も従業員教育等で従業員に周知されていた可能性がある。この点に関する詳細な分析は今後の検討課題としたい。

また個人情報保護行動モデルの適合度はGFIが0.773，CFIが0.766，RMSEAが0.090，P値が0.01未満である。一定の成果は出ているものの改善の余地がある。豊田（2007）は，GFIが一般的に0.9以上あれば説得力あるパス図であると判断すると述べている。RMSEAも当てはまりが悪いとされる0.1には達していないが，十分とされる0.05よりも大きい。この点から，本研究のモデルの適合度向上が課題であると考えられる。

本研究で得られたモデルによると，従業員に個人情報保護行動を行わせるためには，まず従業員の知識を向上させることが不可欠である。本研究のアンケート結果でも知識の分野で正解率の悪い項目が存在することが分かった。どの分野の知識が特に必要かを明らかにすることは今後の課題である。また同様に態度や組織風土に関しても「個人情報保護は重要（関心，有効性認知）」，「被害を避けたい（リスク認知）」，「職場が個人情報保護に熱心（組織風土）」，「個人情報保護対策は面倒（コスト感）」を改善するための具体的な施策を開発する必要がある。この点も今後の課題である。

参考文献

Ajzen, I. and Fishbein, M.: Understanding Attitudes and Predicting Social Behavior, Englewood Cliffs, NJ: Prentice-Hall, Inc.（1980）.

Ajzen, I.: The Theory of Planned Behavior, Organizational Behavior and Human Decision Processes, No.50: pp.179-211（1991）.

OECD（2013）The OECD privacy framework. <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> Accessed 2019, April 19.

経済産業省（2016）事業者が匿名加工情報の具体的な作成方法を 検討するにあたっての参考資料, <https://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/tokumeikakou.pdf> Accessed 2019, April 19.

NPO日本ネットワークセキュリティ協会（2017）2016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～. <http://www.jnsa.org/result/incident/data/2016incident_survey_ver1.2.pdf.> Accessed 2019, April 19.

広瀬幸雄（1994）「環境配慮行動の規定因について」,『社会心理学研究』10，No.1，pp.44-55.

小池俊雄他（2003）「環境問題に対する心理プロセスと行動に関する基礎的考察」,『水工学論文集』47，pp.361-366.

諏訪博彦・山本仁志・岡田勇・太田敏澄（2006）「環境配慮行動を促す環境教育プログラム開発のためのパスモデルの構築」,『日本社会情報学会誌』18，No.1，pp.59-70.

三阪和弘（2003）「環境教育における心理プロセスモデルの検討」,『環境教育』13，No.1，pp.3-14.

諏訪博彦・原賢・関良明（2012）「情報セキュリティ行動モデルの構築―人はなぜセキュリティ行動をしないのか」,『情報処理学会論文誌』53，No.9，pp.2204-2212.

井上沙紀・梅原英一（2017）「個人情報の関心と知識及び行動の関係」,『電子情報通信学会技術研究報告』116，No.488，pp.177-182.

浜屋敏（2009）「情報セキュリティと組織感情 Enterprise2.0」, <https://www.fujitsu.com/jp/group/fri/report/research/2009/report-345.html.> Accessed 2019, April 19.

浜屋敏（2011）「日本における情報セキュリティ逸脱行為と組織文化・風土との関係」, <https://www.fujitsu.com/jp/group/fri/report/research/2011/report-373.html> Accessed 2019, April 19.

杉浦昌・諏訪博彦・太田敏澄（2011）「組織のITセキュリティ対策のゲーム理論による分析―セキュリティ推進部門と従業員の間の指示と実施

のゲーム」,『情報処理学会論文誌』52，No.6, pp.2019-2030.
中村博監修・柴原健次他（2016）『個人情報保護士認定試験公式テキスト』日本能率協会マネジメントセンター，393p.
豊田秀樹（2007）『共分散構造分析[Amos編]』東京図書，254p.