情報処理学会論文誌 Vol.53 No.9 2204–2212 (Sep. 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

諏訪 博彦[1,a)] 原 賢[1] 関 良明[2]

受付日 2011年11月30日, 採録日 2012年6月1日

概要：スマートな社会を実現するためにはコンピュータセキュリティ技術だけでなく，それを扱うユーザの情報セキュリティに関する行動を解明することが重要である．しかし，人はなぜセキュリティ行動をしないのかといった観点からの研究アプローチは十分ではなかった．我々は，ユーザのセキュリティ行動を促進する方法を検討するために，ユーザのセキュリティ行動に影響を与える要因を抽出し，要因と行動の関係性を明らかにすることを目指す．そのために，先行研究に基づき情報セキュリティ行動基本モデルを構築し，400 人に対する質問紙調査によりモデルの検証を行う．共分散構造分析により情報セキュリティ行動モデルを構築し，3 タイプのセキュリティ行動が存在すること，それぞれのセキュリティ行動が異なる要因によって規定されていることを明らかにしている．本稿では，情報セキュリティモデルに基づき要因と行動との関連性を論じ，なぜ人がセキュリティ行動を実施しないのかを明らかにする手がかりを得た．

キーワード：情報セキュリティ行動，人間行動モデル，共分散構造分析，社会調査

Behavior Model of Information Security

Hirohiko Suwa[1,a)] Satoshi Hara[1] Yoshiaki Seki[2]

Received: November 30, 2011, Accepted: June 1, 2012

Abstract: In order to consider the method that promote the user's security behavior, we find some factors that have the effect on user's security behavior, and some relations from their factors and security behavior. We refer several existing research about information security and psychological process, and develop the basic model of information security behavior. Based on the model, we create a questionnaire technique to solve questions how users perceive the information security and how their behavior relate to their perceptions. As the result, we develop a model taking into account people's knowledge, attitude and behavior for showing some relation perceptions and behaviors. By analyzing the model, we determine that people have three type security behavior and each behavior receive the affect from different factors.

Keywords: information security behavior, model of human behavior, analysis of covariance structure, social survey

1. はじめに

国民の 9 割以上がネット社会に関与する現代において，企業や組織のセキュリティ対策はもちろん，ユーザ個人個人が ICT の情報セキュリティに関する行動（以後，セキュリティ行動と記す）を行うことが，スマートな社会を実現するために重要である．ここでいうユーザとは，セキュリティの知識や意識の高い人や低い人を含んだネット社会に関与している幅広いユーザを想定している．情報セキュリティに対する関心は高まりつつあり，セキュリティ行動の重要性は認知されつつある．しかし一方で，重大なセキュリティインシデントの原因として，ユーザのセキュリティ知識や意識の不足が指摘されている [1], [2]．我々は，ユーザのセキュリティ行動を促進する方法を検討するために，

[1] 電気通信大学
University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[2] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories, Musashino, Tokyo 180–8585, Japan
[a)] h-suwa@is.uec.ac.jp

ユーザのセキュリティ行動に影響を与える要因を抽出し，要因と行動の関係性を明らかにすることを目指す．

要因と行動の関係性は，セキュリティ対策を検討する際に重要な要素となる．たとえば，あるセキュリティ行動を促そうとする場合，行動しない要因が知識がないからなのか，手間がかかるからなのか，リスクを認識していないからなのかによって，おのずと対策は異なる．これまで，人はなぜセキュリティ行動をしないのかといった観点からの研究アプローチは十分ではなかった．情報セキュリティの問題は，ユーザの心理が大きく関与するという考えから，情報セキュリティ心理学の必要性が述べられ [3]，情報セキュリティについて社会心理学の観点から研究が進められている [4]．特に，ユーザの安心感という観点に基づく研究が多くなされている [5], [6], [7]．また，安心感に絡めてユーザがセキュリティ行動を行う要因を模索する研究 [8] や企業の情報セキュリティ対策におけるモチベーションの構造に関する研究 [9] など，セキュリティ行動をとらない理由を探る研究が行われている [10], [11], [12]．さらに，特定の情報セキュリティ行動とその規定因に関する研究として，ボットネット対策を例として，説得メッセージによって態度変容する要因を明らかにする研究が行われている [13], [14]．しかしながら，ユーザに対して複数のセキュリティ行動の実施状況とそれを規定する要因とをあわせて分析している研究は見当たらない．セキュリティ行動はボットネット対策だけでなく，セキュリティ対策ソフトの導入・更新，ファイルの暗号化，怪しいウェブサイトの回避など様々であり，それらの行動とそれぞれを規定する要因の関係性を明らかにするためには，各行動とそれを規定する要因を別々に分析するだけでは不十分であり，あわせて分析する必要がある．

そこで我々は，社会心理学の知見と既存の実態調査を参考としたユーザのセキュリティ行動に関するモデルを構築し，質問紙調査に基づきモデルの検証を行う．このアプローチをとることにより，ユーザの情報セキュリティに対する考え方と行動を分析し，人はなぜセキュリティ行動をしないのかを解明することを試みている．

本稿では，まず，人間の行動モデルやセキュリティに対する調査研究などの関連研究を整理する（2 章）．関連研究の整理に基づきセキュリティ行動に与える要因の抽出とモデル化を行う（3 章）．構築したモデルを検証するために，質問紙による調査（4 章）と分析（5 章）を行う．分析結果に基づきセキュリティ行動に影響を与える要因や，行動を促進する方法について考察する（6 章）．最後に結論を述べる（7 章）．

2. 関連研究

情報セキュリティに関する様々な調査が実施され，ユーザのセキュリティ意識や行動が不十分であることが指摘されている．NRI の行った情報セキュリティに関するインターネット利用者意識調査によると，ユーザのセキュリティに関する知識および意識が不足していることが示されている [1]．また，IPA の報告においても重大なインシデントの原因として，ユーザのセキュリティに関する意識不足による行動があげられている [2]．しかしこれらの調査の多くは，意識や実施状況について個別に集計しており，行動を規定する要因について議論できていない．意識や実施状況を把握することは，情報セキュリティ対策の必要性を議論するうえで重要な知見であるが，どのような対策をとることでセキュリティ行動が促進されるかを検討するためには，行動を規定する要因について議論する必要がある．

ユーザの安心感という観点に基づく研究として，山本らは，利用者の感じる安心を明らかにするため，安心そのものではなく，より認識しやすい不安に着目し不安発生モデルを立てることでユーザの感じる安心感を調査している [5]．藤原らは，利用者にとっての情報セキュリティに関する安心感の要因を明らかにするため，一般ユーザの安心感の要因を因子分析によって研究している [6]．西岡らは，情報セキュリティに関する専門知識を持たない一般ユーザの安心感を調査するための質問紙の作成手法について研究を行っている [7]．日景らは，情報セキュリティ技術に対する利用者の安心感の構造について，安心感の要因を把握するための調査実験を行い，因子分析によってユーザの安心感から 6 因子を抽出している [8]．

さらに，ユーザがセキュリティ行動を行う要因を模索する研究が行われている．菅野らは，企業の情報セキュリティ対策を進める動機となる要因や，対策の実施を阻害する要因を把握する調査を行い，それら 2 つの要因より情報セキュリティ対策のモチベーション因子を明らかにしている [9]．加藤らは，末端ユーザのセキュリティ意識とセキュリティ意識を左右するユーザの性格について調査している [10]．吉開らは，ユーザの情報セキュリティに関する意識を集合知ベースの集団仮想ゲームを用いて調査している [11]．小松らは，セキュリティ対策において，実行主体である利用者の実行がともなわない現状に対し，社会的ジレンマ状況を導入し，個人の意思決定メカニズムを明らかにする研究を行っている [12]．さらに小松らは，心理学領域の防御動機理論と精緻化見込みモデルを援用し，ボットネット対策を対象として説得メッセージの影響について質問紙調査と被験者実験を行い，説得メッセージには理解度を深める情報を盛り込むことなどが効果的であると述べている [14]．

しかしながら，ユーザに対して複数のセキュリティ行動の実施状況とそれらを規定する要因を明らかにすることを目的として，それらをあわせて分析している研究は見当たらない．なぜ人がセキュリティ行動を実施しないのかを明らかにするためには，人間が行動に至るまでのモデルを構築し，それぞれの行動に影響を及ぼす要因を明らかにし

たうえで，それらの要因と各行動との関連性を論じる必要がある．これにより，ユーザに対して様々なセキュリティ行動を促す方法について検討できるようになると考える．我々は，ユーザのセキュリティ行動を説明するためのモデルを構築することを目的とする．

3. モデルの構築

本章では，人間の行動モデルを整理したうえで，セキュリティ行動に影響を与える要因について先行研究に基づいて検討し，情報セキュリティ行動基本モデルを構築する．

3.1 人間の行動モデル

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 らの合理的行動理論 [15] や，Ajzen の計画的行動理論 [16] がある．Ajzen ら [15] は，人間が行動に至るまでの心理プロセスが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，技術受容など様々な分野で応用されている [17], [18], [19], [20]．環境配慮行動の分野では，人はなぜ環境に配慮した行動をしないのかを明らかにする研究に応用されている [19], [21], [22], [23]．たとえば小池らは，知識が関心・動機に影響を与え，関心・動機が行動意図に影響を与える環境問題認識の構造モデルを構築している [22]．我々は，これらの先行研究をふまえ知識が態度と行動に，態度が行動に影響を与えるモデルを仮定する（**図 1** のプロセス）．

3.2 要因の抽出

本節では，3.1 節のプロセスモデルに基づき，各プロセス（知識，態度，行動）に含まれる各要因について述べる（図 1 の要因）．

3.2.1 知識

楠見は，不確実事象に関する認知次元として，スポーツや入試はスキルや知識が高く評価される技術的事象であり，ギャンブルは運が高く評価される確率的事象であると述べている [24]．この観点に従えば，セキュリティ問題は，技術的要素が強い不確実事象と考えられる．松村は，人文系大学生のセキュリティ意識とスキルに関する調査に基づき，理念として理解できる項目については実行しやすいが，パソコンの具体的な仕組みを理解したうえで，技術的な操作が必要となる項目についてはセキュリティスキルが不足していると述べている [25]．このことから，セキュリティ行動はセキュリティ知識のみでは実施できず，ある種の行動にはセキュリティスキルが必要であることが分かる．よって，知識プロセスについては，セキュリティ知識とセキュリティスキルの要因を仮定する．

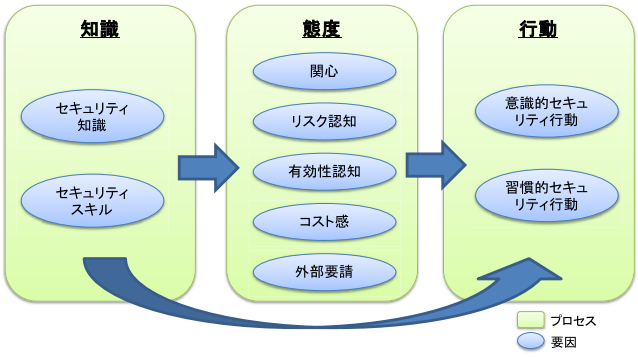

図 1 情報セキュリティ行動基本モデル
Fig. 1 The basic model of information security behavior.

3.2.2 態度

本研究では，関心と動機を態度ととらえている．Rogers の修正防護動機理論では，脅威評価と対処評価が防護動機に影響を与えるとしている [26]．また，NRI のインターネット利用者意識調査によると，セキュリティ対策の問題点として「お金がかかる」「手間がかかり，面倒である」「どのように行えばよいか分からない」「対策を行うと利便性が損なわれる」「危険性が分からない」など，手間やリスクに関する項目が比較的高い値となっている [1]．小松らは，情報セキュリティ対策における個人の利得と認知構造として，コスト感，危機感（自己），危機感（他人），無効性の 4 つに着目している [12]．西岡らは，情報セキュリティに関する専門知識を持たないユーザの意見を整理する中で，7 つの要因を整理し，その中でユーザに近い要因として他者の勧めをあげている [7]．島らは，防護動機理論と集団的防護動機理論を用いてボット対策に影響を及ぼす 8 要因を規定し分析した結果，利用者が個人の問題ではなく他者を含めた集合的な事象であると認識することで対策実行意図を高めることが可能であると述べている [13]．

Rogers の脅威評価や小松らの危機感は，情報セキュリティの「リスク認知」に関わる要因と考えられる．また，対処評価や無効性は，セキュリティ対策の「有効性認知」に関わる要因と考えられる．NRI の調査で問題とされている手間や小松らのコスト感は，セキュリティ対策をするための「コスト感」と考えられる．西岡らの他者の勧めや島らの集合的な事象であると認識することは，他者からセキュリティ行動を「外部要請」されていると感じる要因と考えられる．そこで，情報セキュリティへの関心にこれら 4 要因を加えた 5 要因を態度要因と仮定する．

なお，ウィルス感染やボット対策という特定事象を題材とする吉開ら [11] や小松ら [12] の研究においては，セキュリティ事象の発生頻度が重要な要素として示されているが，本研究では特定事象ではなく情報セキュリティ行動全般に関するモデルの構築を目的としているため，個々のセキュリティ頻度の発生確率や損害の大きさを想定すること

は困難と考え，リスク認知という抽象化された要因を仮定している．

3.2.3 行動

セキュリティ行動といっても，その内容は「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」など意識しないと実施できないものから，「怪しいと思われるウェブサイトにはアクセスしない」など日常的に実施可能なものまで様々である．諏訪らは，環境配慮行動を意識しないと実施しない意識的環境配慮行動と習慣化可能な習慣的環境配慮行動に大別している [23]．彼らは，行動に対する負荷または行動の日常性の大小によって，人々が環境配慮行動を分けて実践していると述べている．我々は，セキュリティ行動も同様な分類が可能であると考え，負荷が高い非日常的な行動を意識的セキュリティ行動，負荷が低く日常的な行動を習慣的セキュリティ行動とする．この2つの行動を行動の要因として仮定する．

3.3 情報セキュリティ行動基本モデル

3.1節，3.2節に基づいて，情報セキュリティ行動基本モデルを構築する（図1）．知識の2要因が，態度の5要因と行動の2要因に影響を与え，態度の5要因が行動の2要因に影響を与えることを仮定するモデルである．このモデルを検証するために，質問紙調査を行う．

4. 調査概要

モデル検証のために，以下の要領で質問紙調査を実施した．

4.1 調査方法

本調査は，インターネット調査により実施している．調査期間は2011年11月18日～19日の2日間である．具体的な調査方法としては，楽天リサーチ株式会社のインターネットパネルのうち，20～59歳を調査対象者とし，5,814人に調査協力依頼を行い，回答者が400人になった時点で回収を終了している．なお，回収時に年齢や性別での割当てを実施し，調査対象は20代から50代までの男女各50人，計400人である．調査内容は，「1．情報セキュリティに関する知識」「2．情報セキュリティに関するスキル」「3．情報セキュリティに関する考え」「4．情報セキュリティに対する行動」の4つに大別されている．「1．情報セキュリティに関する知識」以外の項目については，質問順序を回答者ごとにランダムに変更し，質問順序によるバイアスを取り除いている．詳しい調査項目については，4.2節で述べる．

4.2 調査項目

本調査では，情報セキュリティ行動基本モデルに基づき調査項目を設定している．

4.2.1 知識

知識については，セキュリティ知識に関する10項目とセキュリティスキルに関する10項目を設定している．セキュリティ知識に関する項目は，IPAが2010年に実施した情報セキュリティの脅威に対する意識調査 [27] の情報セキュリティの脅威に対する認識（Q8）を参考に作成している．各項目に対して書いてある内容が正しいと思えば「正しい」，間違っていると思えば「間違い」，分からなければ「分からない」を選択するように回答を依頼している．「分からない」という回答項目を設定することにより，知識がない場合のいい加減な回答を排除できると考える．知識の判定は，回答の正解の数（正答数）としている．認知度の比較的高い「ワンクリック請求」「スパイウェア」「フィッシング詐欺」「セキュリティホール」の4つと認知度の低い「ボット」の計5つについて，各2問ずつ項目を選択している．正答率の高かった各用語の定義に関する質問を1つずつ計5問と，正答率が低かった内容に関する質問計5問で構成し，正答数が偏らないように配慮している．

セキュリティスキルに関する質問項目は，同調査の情報セキュリティ対策の実施状況（Q11）を参考に作成している．ほぼ同じ内容の質問がNRIの情報セキュリティに関するインターネット利用者意識2008 [1] でも採用されており，項目として妥当であると考える．具体的には，「Windows Update等によるセキュリティパッチの更新の手順を理解し，かつ実施できる」など10項目について，実際に実施できるかどうか「まったくそう思わない」から「とてもそう思う」までの5段階で回答を依頼している．スキルの難易度としては，セキュリティパッチの更新やウィルス対策ソフトの導入など比較的実施率の高い項目と，有害なウェブサイトへのアクセスを防止するソフトや暗号化など実施率の低い項目を含めることで，難易度を調整している．

4.2.2 態度

態度については，設定した5要因に対して3項目ずつ15項目を設定している．関心については，「社会にとって，情報セキュリティは重要な問題である」などの3項目を設定している．リスク認知については，「私が，セキュリティ被害にあっても，たいした問題ではない」など3項目である．有効性認知としては，「私が，セキュリティ対策をすると，被害にあう確率を下げる効果がある」など3項目を設定している．コスト感については，「複数パスワードの管理は，面倒くさい」など3項目を設定している．外部要請については，「職場や学校から，セキュリティ対策を求められている」などの3項目を設定している．各項目について，「まったくそう思わない」から「とてもそう思う」までの5段階で回答を依頼している．

4.2.3 行動

セキュリティ行動については，スキルと同様にIPAが2010年に実施した情報セキュリティの脅威に対する意識

表 1 態度に関する因子分析結果
Table 1 The result of factor analysis about the attitudes.

項目	因子1	因子2	因子3	因子4	因子5
私が、セキュリティ被害にあっても、たいした問題ではない	**.736**	−.279	−.001	−.004	.063
ウイルス感染やフィッシング詐欺は、私には関係ない	**.730**	−.249	.030	−.088	−.028
私が、セキュリティ対策をしても、効果はない	**.676**	−.070	−.024	−.285	.130
社会にとって、情報セキュリティは重要な問題である	−.266	**.749**	.107	.191	.156
現代社会は、セキュリティ対策を求めている	−.238	**.622**	.176	.267	.202
情報セキュリティは、高めるべきである	−.211	**.619**	.076	.254	.168
職場や学校が、セキュリティ教育に熱心である	.004	.064	**.835**	.066	.081
職場や学校から、セキュリティ対策を求められている	−.061	.082	**.685**	.216	.114
情報セキュリティについて、詳しい友人がいる	.117	.082	**.387**	.201	−.177
私が、セキュリティ対策をすると、被害の規模を小さくする効果がある	−.151	.249	.226	**.715**	.020
私が、セキュリティ対策をすると、被害にあう確率を下げる効果がある	−.136	.243	.219	**.701**	.011
私が、セキュリティ対策をしないと、人に迷惑をかける	−.159	.268	.387	**.416**	.061
複数パスワードの管理は、面倒くさい	−.067	.106	.041	−.003	**.679**
データのバックアップは、手間がかかる	.005	.153	.098	.045	**.541**
Windows Update等によるセキュリティパッチの更新は、わずらわしい	.196	.042	−.075	−.004	**.518**
因子寄与	1.83	1.72	1.63	1.53	1.19
累積寄与率	12.2	23.7	34.6	44.8	52.7

調査の情報セキュリティ対策の実施状況（Q11）を参考に作成している．「Windows Update 等によるセキュリティパッチの更新している」など 10 項目について，実際に実施しているかどうか「まったく実施していない」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ている．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ている．具体的な項目としては，セキュリティパッチの更新やウィルス対策ソフトの導入など負荷が低く日常的に実施しやすい比較的実施率の高い項目と，有害なウェブサイトへのアクセスを防止するソフトや暗号化など負荷が高く日常的に実施しにくい比較的実施率の低い項目を設定している．

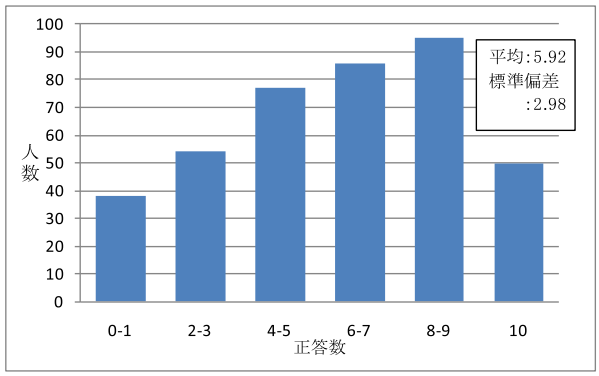

図 2 セキュリティ知識に関する正答数
Fig. 2 The number of correct answers about security knowledge.

5. 調査結果

本章では，各要因の抽出と共分散構造分析 [28] に基づくモデル構築について述べる．

5.1 各要因の分析

本節では，知識，態度，行動の各要因についての分析結果を述べる．分析手法として，セキュリティ知識については正答数を指標とするため平均値や標準偏差で分析し，そのほかの要因については因子分析を用いる．因子分析は，潜在因子を仮定し，質問紙などにより直接観測した複数の変数から直接観測できない潜在因子を抽出する手法であり，心理尺度の研究手法としても用いられている．この手法を用いて，各要因の妥当性について検討する．

5.1.1 知識

セキュリティ知識について正答数を確認した結果，**図 2** のとおりであった．正答数の平均値は 5.92，標準偏差は 2.98 であった．「分からない」と回答した項目を除外した場合の正答率の平均は 87.8%，100%正答した回答者が 192 人であることから，回答者は分からない項目は分からないと回答していると考えられ，正答数により回答者のセキュリティ知識が量れていると考える．よって，正答数をセキュリティ知識とすることとした．

セキュリティスキルに関する 10 項目に対して因子分析（主因子法，バリマックス回転）を実施した結果，1 因子が確認された．因子寄与は 5.88，累積寄与率は 58.8%であり，セキュリティスキルを十分に説明できると考える．よって，この因子をセキュリティスキルとすることとした．

5.1.2 態度

情報セキュリティに対する考えに関する 15 項目に対して因子分析（主因子法，バリマックス回転）を実施した結果，5 因子が抽出された（**表 1**）．因子 2，因子 3，因子 5 については，我々が仮定したとおり関心，外部要請，コスト感が確認されている．しかし，因子 1 と因子 4 は仮定と異なった．因子 1 には，「私がセキュリティ被害にあっても，たいした問題ではない」「ウィルス感染やフィッシング詐欺は，私には関係ない」「私が，セキュリティ対策をしても，効果はない」の因子付加量が大きかった．このことから，因子 1 を無効感と名付けた．因子 4 には，「私がセキュリティ対策をすると，被害の規模を小さくする効果がある」「私が，セキュリティ対策をすると被害にあう確率を下げる効果がある」「私が，セキュリティ対策をしないと，

表 2 行動に関する因子分析結果
Table 2 The result of factor analysis about the behaviors.

	因子1	因子2	因子3
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	**.656**	.089	.111
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	**.635**	.286	.142
ウェブサイトの安全評価ツールを利用している	**.558**	.196	.214
重要なデータのバックアップをしている	**.472**	.297	.242
セキュリティ対策ソフトを導入、活用している	.139	**.832**	.208
ファイアウォール（ルータ等）を利用している	.359	**.576**	.150
Windows Update等によるセキュリティパッチの更新をしている	.288	**.557**	.238
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	.151	.096	**.861**
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	.153	.228	**.578**
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	.218	.203	**.555**

人に迷惑をかける」の因子付加量が大きくなった．このことから因子 5 を貢献感と名付けた．

3.2.2 項で設定した要因のうち，リスク認知要因と有効性認知要因が抽出されなかった．代わりに，無効感と貢献感が抽出された．このことについては，考察で述べる．抽出された 5 因子を態度の要因として設定することとした．

5.1.3 行動

情報セキュリティに対する行動に関する 10 項目に対して因子分析（主因子法，バリマックス回転）を実施した結果，我々の仮定と異なり 3 因子が抽出された（**表 2**）．因子 1 は，暗号化された USB メモリの利用や重要ファイルを暗号化しているなど，負荷が高く非日常的なセキュリティ行動の因子付加量が大きくなった．このことから因子 1 を意識的セキュリティ行動と名付けた．因子 2 は，セキュリティ対策ソフトを導入，活用しているなど，日常的に求められるセキュリティ行動の因子付加量が大きくなった．このことから，因子 2 を習慣的セキュリティ行動と名付けた．因子 3 は，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など，自らが気を使いセキュリティ事故を予防しようとする行動の因子付加量が大きくなった．このことから，因子 3 を予防的セキュリティ行動と名付けた．これら 3 因子を行動の要因として設定することとした．

3.2.3 項では，行動の要因として 2 要因を設定したが，意識的セキュリティ行動要因，習慣的セキュリティ行動要因に加え，予防的セキュリティ行動要因が抽出された．セキュリティ行動には，ウィルスやアタック攻撃などの危険要因に対する防御行動に加え，そもそも危険要因に近づかないようにする予防行動があると考えられる．

5.2 モデルの分析

セキュリティ行動に影響を及ぼす要因を明らかにするために，5.1 節の分析結果に基づき情報セキュリティ行動基本モデルを一部修正したうえで，Amos 19 を用いて共分散構造分析を行った．共分散構造分析は，直接観測される変数から，直接観測できない潜在変数を導出し，その潜在変数間や観測変数との因果関係についてモデルを設定することによって，因果モデルの仮説の妥当性を検討する統計的手法である．質問紙により得た観測変数から各要因を導出でき，その要因間の関係について検証することができる．本研究の目的であるユーザのセキュリティ行動に影響を与える要因と行動の関係性を明らかにする手法として，適していると考える．5.1 節の分析により態度，行動の要因として，3.3 節で構築したモデルと異なる要因が抽出されたため，リスク認知と有効性認知を無効感と貢献感に修正し，さらに予防的セキュリティ行動要因を付加したモデルを構築している．

知識の各要因から態度・行動の各要因へと態度の各要因から行動の各要因へのパスを引き，有意（5%）でないパスを削除した結果を，情報セキュリティ行動モデルとして示す（**図 3**）．なお，セキュリティ知識とセキュリティスキルは，相互に関係しあうと考えられるため，相関のパスを引いている．

セキュリティ知識は，無効感（−.29），関心（.34），コスト感（.21），習慣的セキュリティ行動（.33）に影響を及ぼしている．セキュリティスキルは，外部要請（.37），貢献感（.43），コスト感（−.31）に影響を及ぼしている．セキュリティ知識とセキュリティスキルには，相関関係（.38）が確認されている．

予防的セキュリティ行動に影響を与える要因としては，コスト感（−.51），関心（.33），無効感（−.27）が確認されている．習慣的セキュリティ行動に影響を及ぼす要因としては，セキュリティ知識（.33）と貢献感（.27），コスト感（−.64），関心（.25）が確認されている．意識的セキュリティ行動に影響を与える要因としては，外部要請（.16），貢献感（.31），コスト感（−.81）が確認されている．

6. 考察

本章では，分析結果に対する考察と本調査の限界について述べる．

6.1 情報セキュリティ対策における社会的ジレンマ

因子分析の結果潜在的な因子として，リスク認知と有効性認知ではなく，貢献感と無効感が抽出された．ユーザは情報セキュリティ対策に対する重要性は認識しており，自分が何らかの貢献ができると感じている．しかしながら，情報セキュリティ対策は，1 人だけ実施しても，セキュリティ事故を完全に防いだり，減らせたりするわけではな

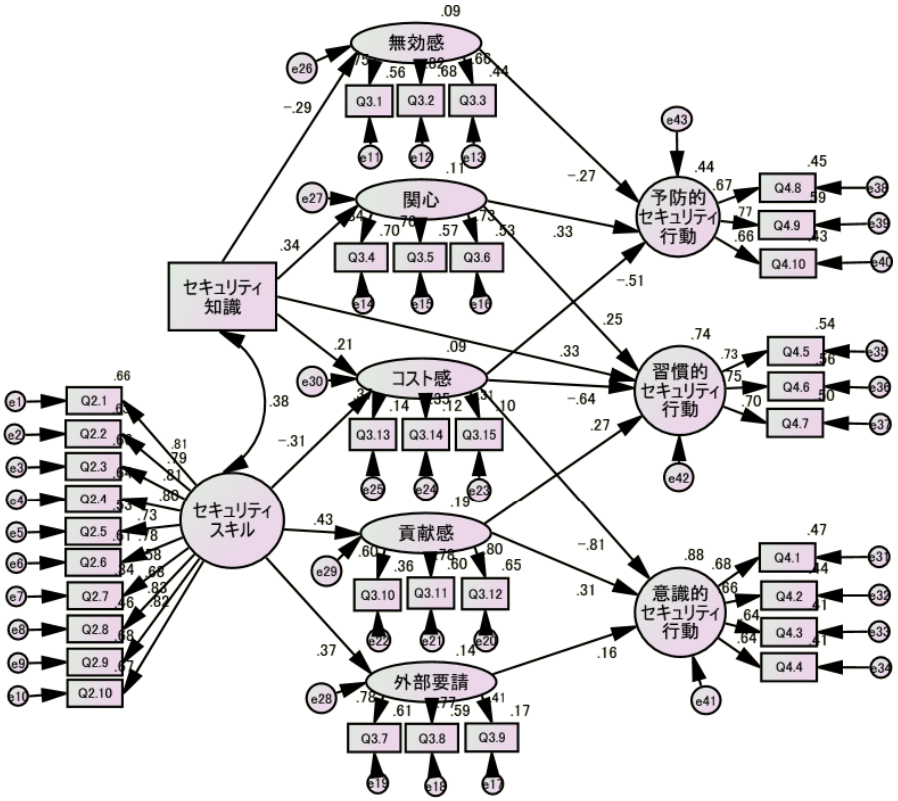

図 3 情報セキュリティ行動モデル
Fig. 3 The model of information security behavior.

い．結果として，自分がやらなくても社会的な影響は少ないと考え，実施しなくなるものと考える．この状態は，小松ら [12] が指摘しているとおり，社会的ジレンマ状態と考えられる．また，ユーザは攻撃者が技術的に高度に専門性を保持していると考え，ユーザは何をしても防げないのではないかという無効感を持っているものと考える．情報セキュリティ対策には，自分 1 人だけでは解決できないという側面があるため，一般的な防護動機理論に基づくリスク認知や有効性認知は異なる因子が抽出されたと考える．このことについては，本研究とは別に，そもそも人々が情報セキュリティ対策をどのようにとらえているのかについて，詳細な検討が必要であると考える．

6.2 3 つの行動因子と行動促進要因の検討

行動プロセスの因子として，予防的セキュリティ因子，習慣的セキュリティ因子，意識的セキュリティ因子が確認されている．このことより，セキュリティ行動にタイプがあることが分かる．

予防的セキュリティ行動は，「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」など，ユーザが気を使うことで実施できる行動である．関心から正の影響を，無効感とコスト感から負の影響を受けている．セキュリティに対する関心を高め，無効感を軽減することで，実施が促進されると考える．

習慣的セキュリティ行動は，「セキュリティ対策ソフトを導入，活用している」など，ユーザが気を使わずに日常的に実施できる行動である．関心と貢献感から正の影響を，コスト感から負の影響を受けている．関心と貢献感を高めることで実施が促進されると考える．

意識的セキュリティ行動は，「暗号化された USB メモリの利用や重要ファイルを暗号化している」など，意識しないと実施できない行動である．貢献感と外部要請から正の影響を，コスト感から負の影響を受けている．貢献感と外部要請を高めることで実施が促進されると考える．

6.3 行動の阻害要因としてのコスト感

セキュリティ行動の阻害要因として，コスト感の影響が大きい．コスト感はすべてのセキュリティ行動に対して，負の影響を及ぼしている．このことから人々のセキュリティ行動を促進させるためには，セキュリティ対策に対するコスト感を低減させることが重要であると考えられる．コスト感には，セキュリティ知識が負の影響を，セキュリティスキルが正の影響を及ぼしている．セキュリティ知識が高まると，セキュリティ対策として実施しなければならないことが増え，コスト感が上昇すると考えられる．コスト感を低減させるためには，具体的な対策手順や実施方法を伝えることが重要であると考える．また，スキルの向上だけでなく，コンピュータセキュリティ技術を向上させ手間やコストを削減し，ユーザのコスト感を低減させることが，スマートな社会を実現することにつながると考える．

6.4 情報セキュリティ行動モデルの活用

本節では，情報セキュリティ行動モデルの効用を考察する．情報セキュリティ行動モデルに基づくと，情報セキュリティ行動は，予防的セキュリティ行動，習慣的セキュリティ行動，意識的セキュリティ行動から構成される．ユーザの情報セキュリティ行動を促進させることを検討した場合，その行動がどのセキュリティ行動に該当するのかを考える手がかりを提供している．

また，本モデルに基づくと，セキュリティ行動に影響を与える要因は，無効感，関心，コスト感，貢献感，外部要請から構成される．ユーザの情報セキュリティ行動を促進させたいならば，増強あるいは軽減すべき要因として何があるかを考える手がかりを提供している．

たとえば，情報セキュリティ行動モデルの応用として，ユーザに暗号危殆化対策 [29], [30] を促進させたいとする．提案モデルに基づくと，この行動は，どちらかといえば習慣的セキュリティ行動に分類されると考える．この行動を促進するためには，コスト感の軽減，セキュリティ知識の充足，貢献感の高揚，関心の喚起，の順に有効であろうという仮説を作ることができる．さらに，コスト感の軽減には，セキュリティ知識を授けることよりもセキュリティスキルを授けることが望ましいことも本モデルから考えられる．

6.5 本研究の限界

情報セキュリティ行動モデルの適合度 [31], [32] は，CFI = .815 [*1]，RMSEA = .072 [*2]であり，一定の成果は出ているものの改善の余地がある．特に CFI の値が低い．この原因を探るために各要因の決定係数を見てみると，行動プロセスの要因は相対的に高いのに対して，態度プロセスの要因が低い値となっている．つまり，態度を説明する要因については，さらに検討する必要があると考える．また，本研究の調査対象はインターネットパネルを用いているため，ランダムサンプルをベースとした一般ユーザの傾向を示したとはいえない．職種やインターネット経験などのサンプルの特徴を考慮した分析は今後の課題である．

日景らは，情報セキュリティ技術に対する利用者の安心感の構造を外的要因と内的要因に大別し，内的要因の規定因として，知識，経験，プリファランスをあげている [8]．内的要因は態度とも考えられ，今後経験やプリファランスなど態度に影響を与える要因について検討し，モデルの適合度のさらなる向上を目指す必要があると考える．

また，本研究は質問紙調査に基づく分析であり，実際にどのような方法がユーザのセキュリティ行動の変容に効果があるのかを実証的に検証したものではない．今後，情報セキュリティ行動モデルに基づいた教育や対策案を提案し，実際に行動が変化することを確認するための実証実験が必要と考える．

[*1] CFI は，1 に近いほどモデルのあてはまりが良く，0.9 以上が受容の目安となる．詳しくは文献 [31] を参照．

[*2] RMSEA は，0 に近いほどモデルのあてはまりが良く，0.08 以下が受容の目安となる．詳しくは文献 [32] を参照．

7. 結論

我々は，ユーザのセキュリティ行動を促進する方法を検討するために，ユーザのセキュリティ行動に影響を与える要因を抽出し，要因と行動の関係性を明らかにすることを目的とした．先行研究に基づき情報セキュリティ行動基本モデルを構築し，400 人に対する質問紙調査の結果を共分散構造分析することで情報セキュリティ行動モデルを構築した．モデルにより，3 タイプのセキュリティ行動が存在すること，それぞれのセキュリティ行動が異なる要因によって規定されていることを明らかにした．情報セキュリティ行動モデルを用いることで，行動に影響を及ぼす要因を明らかにしたうえで，その要因と行動との関連性を論じることができ，なぜ人がセキュリティ行動を実施しないのかを明らかにする手がかりを得た．これは，コンピュータセキュリティ技術を用いてスマートな社会を実現するための基盤になると考える．

謝辞 本研究の一部は，科研費（23500308）の助成を受けたものである．

参考文献

[1] NRI Secure Technologies：情報セキュリティに関するインターネット利用者意識 2008，NRI Secure Technologies（オンライン），入手先 ⟨http://www.nri-secure.co.jp/news/2008/pdf/20080522_net.pdf⟩（参照 2011-10-31）．

[2] IPA：2011 年版 10 大脅威『進化する攻撃その対策で十分ですか？』，IPA（オンライン），入手先 ⟨http://www.ipa.go.jp/security/vuln/documents/10threats2011.pdf⟩（参照 2011-04-13）．

[3] 内田勝也，矢竹清一郎，森 貴男ほか：情報セキュリティ心理学の提案，情報処理学会研究報告，CSEC, Vol.2007, No.16, pp.327–331 (2007).

[4] 持永 大，杉浦 昌，小松文子ほか：情報セキュリティ事象の社会科学的アプローチによる研究の動向，情報処理学会研究報告，CSEC, Vol.2009-CSEC-46, No.41, pp.1–7 (2009).

[5] 山本太郎，千葉直子，植田広樹ほか：インターネットにおける不安から見た安心の模索，電子情報通信学会技術研究報告，Vol.111, No.123, pp.41–47 (2011).

[6] 藤原康宏，山口健太郎，村山優子：情報セキュリティの専門知識を持たない一般ユーザを対象とした安心感の要因に関する調査，情報処理学会論文誌，Vol.50, No.9, pp.2207–2217 (2009).

[7] 西岡 大，藤原康宏，村山優子：情報セキュリティ技術に関する一般ユーザの意見を反映した安心感調査のための質問紙作成手法の提案，情報処理学会論文誌，Vol.52, No.9, pp.2508–2525 (2011).

[8] 日景奈津子，カールハウザー，村山優子：情報セキュリティ技術に対する安心感の構造に関する統計的検討，情報処理学会論文誌，Vol.48, No.9, pp.3193–3203 (2007).

[9] 菅野泰子，寺田真敏，山田安秀ほか：企業の情報セキュリティ対策におけるモチベーションの構造に関する考察，情報処理学会論文誌，Vol.50, No.9, pp.2193–2206 (2009).

[10] 加藤岳久，中澤優美子，漁田武雄ほか：本人認証技術におけるユーザの性格とセキュリティ意識との相関に関する考察，情報処理学会論文誌，Vol.52, No.9, pp.2537–2548 (2011).
[11] 吉開範章，栗野俊一，飯塚信夫ほか：集合知ゲームを用いた情報セキュリティ対策への意識調査に関する検討，情報処理学会研究報告，GN, Vol.2011-GN-79, No.7, pp.1–6 (2011).
[12] 小松文子，高木大資，松本　勉：情報セキュリティ対策における個人の利得と認知構造に関する実証研究，情報処理学会論文誌，Vol.51, No.9, pp.1711–1725 (2010).
[13] 島　成佳，高木大資，吉開範章ほか：情報セキュリティ対策の促進を促す説得コミュニケーションによる態度変容の調査報告，暗号と情報セキュリティシンポジウム（SCIS2011）(2011).
[14] 小松文子，高木大資，吉開範章，松本　勉：情報セキュリティ対策を要請する説得メッセージによる態度変容の調査と実験，情報処理学会論文誌，Vol.52, No.9, pp.2526–2536 (2011).
[15] Ajzen, I. and Fishbein, M.: *Understanding Attitudes and Predicting Social Behavior*, Englewood Cliffs, NJ: Prentice-Hall, Inc. (1980).
[16] Ajzen, I.: The Theory of Planned Behavior, *Organizational Behavior and Human Decision Processes*, No.50, pp.179–211 (1991).
[17] Seligman, C. and Ferigan, J.E.: A two factor model of energy and water conservation, *Social Psychological Applications to Social Issues*, Vol.1, pp.279–299, Plenum Press (1990).
[18] 山本仁志，諏訪博彦，岡田　勇，山本浩一：ブログ空間上のコミュニケーション発生メカニズムの分析，日本社会情報学会誌，Vol.20, No.1, pp.29–42 (2008).
[19] 広瀬幸雄：環境配慮行動の規定因について，社会心理学研究，Vol.10, No.1, pp.44–55 (1994).
[20] Davis, F.D.: Technology Acceptance Model for Empirically Testing New End-user Information Systems Theory and Results, *Unpublished Doctoral Dissertation*, MIT (1986).
[21] 三阪和弘：環境教育における心理プロセスモデルの検討，環境教育，Vol.13, No.1, pp.3–14 (2003).
[22] 小池俊雄ほか：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，No.47, pp.361–366 (2003).
[23] 諏訪博彦，山本仁志，岡田　勇，太田敏澄：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，Vol.18, No.1, pp.59–70 (2006).
[24] 楠見　孝：不確実事象の認知と決定における個人差，心理学評論，Vol.37, No.3, pp.337–366 (1995).
[25] 松村真木子：人文系大学生の情報セキュリティ意識とスキル，情報処理学会研究報告，CSEC, Vol.43, pp.69–74 (2006).
[26] Rogers, R.W.: Cognitive and physiological process in fear appeals and attitudes change: A revised theory of protection motivation, *Social Psychophysiology*, Cacioppo, J.T. and Petty, R.E. (Eds.), pp.153–176, Guilford Press, New York (1983).
[27] IPA：2010 年度情報セキュリティの脅威に対する意識調査報告書, IPA（オンライン），入手先 ⟨http://www.ipa.go.jp/security/fy22/reports/ishiki/documents/2010-ishiki.pdf⟩（参照 2011-10-31）.
[28] 豊田秀樹：共分散構造分析＜入門編＞—構造方程式モデリング，朝倉書店 (1998).
[29] IPA：暗号の危殆化に関する調査報告書，IPA（オンライン），入手先 ⟨http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/documents/crypt_compromize.pdf⟩（参照 2011-11-29）.
[30] 武藤健一郎：SSL における暗号危殆化サンプル調査の報告，JNSA（オンライン），入手先 ⟨http://www.jnsa.org/seminar/pki-day/2011/data/03_mutoh.pdf⟩（参照 2011-11-29）.
[31] 狩野　裕，三浦麻子：AMOS，EQS，CALIS によるグラフィカル多変量解析—目で見る共分散構造分析増補版，現代数学社 (2002).
[32] 山本嘉一郎，小野寺孝義：Amos による共分散構造分析と解析事例，第 2 版，ナカニシヤ出版 (2002).

諏訪 博彦　（正会員）

1998 年群馬大学社会情報学部卒業．2006 年電気通信大学大学院情報システム学研究科博士後期課程修了．博士（学術）．現在，電気通信大学大学院情報システム学研究科社会知能情報学専攻社会情報システム学講座助教．ソーシャルメディアに関する研究に従事．

原 賢

2011 年電気通信大学電気通信学部電子工学科卒業．現在，同大学大学院情報システム学研究科博士前期課程在学中．一般ユーザの情報セキュリティ行動改善に関する研究に従事．電子情報通信学会学生会員．

関 良明　（正会員）

1985 年東北大学工学部通信工学科卒業．同年日本電信電話株式会社入社．以来，グループウェア，オフィスシステム，情報セキュリティの研究開発に従事．博士（情報科学，東北大学）．現在，NTT セキュアプラットフォーム研究所所属．電気通信大学大学院情報システム学研究科客員准教授．電子情報通信学会シニア会員．社会情報学会，ACM，IEEE 各会員．