情報処理学会論文誌 Vol.56 No.12 2200–2209 (Dec. 2015)

集団的防護動機理論に基づく情報セキュリティ対策実行意思モデルの提案とその活用

浜津 翔[1,†1] 栗野 俊一[1] 吉開 範章[1,a)]

受付日 2015年2月27日, 採録日 2015年9月2日

概要：コンピュータ・ウィルスに感染し，そのことを認知した場合でも，ヒトは対策をとるケースが多くないことが報告されている．その要因を明らかにし，情報セキュリティ対策を促すための研究を，説得心理学を基礎とする質問紙と実験により進めている．今回，対策行為に導く施策の実現に向け，対策実行意思に影響を与える要因を明らかにするために，集団的防護動機理論における 8 つの規定要因に，感染経験，IT 知識，IT スキルの 3 つの潜在要因を加えたモデルを提案し，共分散構造分析によりデータ分析するとともに，その結果が正当性基準を十分満足する適合度指標を示したので報告する．また，実験協力者の行動データを同じモデルで分析を行い，対策実行意思に影響を与える要因も明らかになった．さらに，これらの結論を情報セキュリティ対策に活用する方策に関しても述べる．

キーワード：コンピュータ・ウィルス，DDoS 攻撃，説得心理学，防護動機理論

Measure Behavior Intention Model for Information Security Based on Persuasion Psychology and Its Application

Sho Hamamatsu[1,†1] Shun-ichi Kurino[1] Noriaki Yoshikai[1,a)]

Received: February 27, 2015, Accepted: September 2, 2015

Abstract: It is reported that many possessors of infected PCs don't take the required recovery action to eliminate a virus infection, even after being alerted to the need to do so. Research on individual behavior and decision making in a virus infection situation is important for developing information security protection. By the questionnaire and the experiment of the virtual game based on collective intelligence, we have got the individual data under a virus infection environment. This paper shows a new measure behavior intention model including three Latent Variables (virus infection experience, IT Knowledge, IT skill) in addition to eight factors based on Group Protection Motivation Theory, which has a good Fit Index for explaining the data. By analyzing the experiment data in combination with questionnaire results, we also have investigated the factors for the actions of a person taking antivirus measures. Furthermore, how to apply these results into the information security measure is explained.

Keywords: computer virus, DDoS attack, persuasion psychology, protection motivation theory

1. はじめに

インターネット利用者にとって，情報セキュリティ対策は，自分が安全で快適な環境でインターネットを利用するために必須な行為であり，もしコンピュータ・ウイルス感染を検出/認知した場合，ウイルス駆除ソフトを入手・実行して元の状態に戻す行為を実施することが，情報セキュリティ関係者の前提となっている．しかしながら現実には，感染を自覚したとしても，対策や行動をとらない現象が多々みられるという報告がある [1]．そこで，情報推進機構の指導の下，ウィルス感染時のインターネット利用者の行動特性を明らかにすることが，情報セキュリティ対策の推進に必須であると考え，コンピュータ・ウィルスに擬似感染させる環境を構築し，一般人を対象とした心理学実験

[1] 日本大学
Nihon University, Chiyoda, Tokyo 101–8308, Japan
[†1] 現在，富士通エフサス
Presently with Fujitsu FSAS
[a)] yoshikai.noriaki@nihon-u.ac.jp

© 2015 Information Processing Society of Japan

を質問紙調査とともに行う検討がなされた [2]．基本的な考え方としては，ウイルス感染状況は，ヒトにとって脅威であり，その脅威から避難する方法を示すことでヒトは対策をとると仮説を立て，脅威アピール説得について研究し，質問紙調査で回答された対策実行意思と，実際に実験での行動が異なることが示された．情報セキュリティのための対策を研究するうえで，実験の必要性を示したきわめて重要な研究であるが，その後の検討から，質問紙調査の方法，実験システムの構成および実験シナリオなどに，改善すべき点があることが分かった．そこで，今回，新たに考案した調査法と分析法，および，それらをふまえた再調査から得られた主結論を報告する．さらに，それらの結論を情報セキュリティ対策に活用する方策についても述べる．

本論文の構成は以下のとおりである．2 章で，先行研究状況を述べ，3 章で，集団的防護動機理論に基づく，情報セキュリティのための対策実行意思モデルを提案する．4 章では，質問紙と実験による調査方法の概要を示し，5 章に，データ分析結果と考察，6 章に，実験データと質問紙データの違いに関する考察を，それぞれ示す．そして，7 章に，情報セキュリティ行動サイクルへの応用を述べ，8 章に，まとめを示す．

2. 先行研究状況

2.1 説得心理学と情報セキュリティ

情報セキュリティは総合科学であり，「ヒト」の心理・行動の研究が必須であるが，ソーシャルエンジニアリングが研究主体であり，脅威のリスク認知に関する研究は，やっと始まった段階である [3], [4]．脅威事象の例として環境問題，人口増加による影響，放射性降下物など様々な脅威を対象とした防護動機理論に基づく説得心理学の研究が行われている [5], [6] が，情報セキュリティ問題を対象とした防護動機理論の研究は，コンプライアンスのための研究 [7] がなされている程度である．

DDoS 対策として，サイバークリーンセンター（CCC）が感染コンピュータを検出し，インターネットサービスプロバイダ（ISP）を通じてユーザにメールによる注意喚起を行うと同時にボット駆除ツールのダウンロードを勧めていた．しかし，ISP からのメールによって駆除ツールを実際にダウンロードするユーザは，メールを受け取った人の 30%ほどにとどまっているという現状が報告されている [1]．このことから，ボット対策を行うためには，感染コンピュータの検出，駆除ツールの提供といった技術的な側面の整備だけでは不十分であり，ユーザの対策意思や行動に影響を与える社会心理学的要因の検討も不可欠であるということが示唆される．

2.2 集団的防護動機理論の応用

受け手の態度や行動を変化させる説得コミュニケーションの 1 つに，脅威アピールがある．これは，脅威の危険性を強調して，行動の勧告に対する受け手の受容を促進させようとする手法であり，防護動機理論とは，脅威アピールの説得効果を説明する理論である [8]．また，対処行動には，それが一個人の脅威の低減で完結するものと，多くの人が集合的に実行することによってはじめて脅威を低減させることのできるものが存在する．後者の集団的な対処行動を促す脅威アピールの研究として，集団的防護動機理論が提唱され，8 つの認知因子（深刻さ，生起確率，効果性，コスト，実行能力，責任，実行者割合，規範）が実行意思に影響を与えるとしている．

2.3 従来研究の課題

このような立場から，小松らによる嚆矢的な研究 [9] が行われ，我々もそれに続いてきた [12] が，その後の検討により，次のような課題も明らかになってきた．

2.3.1 心理モデルの課題

文献 [9] において，集団的防護動機理論に基づき研究がなされたが，対策実行意思に影響を与える要因の分析において，その結果には，正当性を示す基準に課題がある．たとえば，認知要因が対策実行意思に独立に影響するとして，モデルをたて，各因子が対策実行意思に与える影響度が検証されていた．しかし，一般の人を対象とした場合の質問紙の回答に対し，認知要因が互いに独立であることを仮定し，共分散構造分析 [10] を行ったところ，付録 1 に示すように，モデルの適合度が非常に低いという結果が得られた．

共分散構造分析では，モデルを評価するために，主に 5 つの指標 GFI，AGFI，CFI，RMSEA，SRMR が用いられ，GFI，AGFI，CFI は，1 に近いほど適合が良いモデルと判断され，RMSEA，SRMR は 0 に近いほど適合が良いモデルと判断される [11]．

この結果から，認知要因間に相関関係があることを仮定する必要があると考えられる．

2.3.2 実験システムの課題

文献 [2] は，質問紙調査分析を偏重しがちな従来の研究と異なり，心理実験を行い，その結果と質問紙調査の結果を比較したという点でも画期的であった．しかし，その結果は，同一集団内におけるインシデントに対する対処行動意図（質問紙調査での回答）と，実際にその状況下に置かれたときの対処実行（実験時での行動）の間に開きがあるというものであった．その違いの要因の 1 つは，確かに，状況の違いにあると考えられるが，その一方，実験そのものに含まれる問題が，このような違いを導いた可能性も否めない [12]．つまり，実験環境を改良する必要があると考えられる．

そこで次章以降に，提案する心理モデルおよび改善した実験システムの説明と実験方法について述べる．

© 2015 Information Processing Society of Japan

3. 情報セキュリティのための対策実行意思モデル

情報セキュリティにおける対策実行は，自分の利害だけでなく，ネットワークに接続された周りの人々の利害も考慮した，一種の援助行為と考えられる．そこで，援助行動への意思決定過程 [13] を基に，対策実行意思モデルを構築する．HIV 感染者との共生行動意図を促す研究 [14] においても，このモデル構築法が採用されており，本研究では，その手法に従った．具体的には，援助行動における意思決定過程を，被援助者の欲求に対する知覚の段階，個人的責任を引き受けるかどうかの段階，コストと報酬の査定の段階，方法の決定の段階を経て決定されると仮定している．

各段階における判断に関わると予想される要因として，集団的防護動機理論を用いて 8 つの認知要因を仮定する．さらに，それらの要因は，日常の IT 機器やサービスでの体験を通じて，相関があると考える．結果として，人々がこれまでに得た情報セキュリティに関する知識や経験に関する情報に影響を受けた認知要因が，対策行動意思を規定するという 3 段階モデルを検討する．

3.1 潜在変数の決定

情報セキュリティにおける認知要因に関して，ある種の認知は，現象，事実などの外的な要因（潜在変数）から影響を与えられると考えられる．そこで，次の 2 つの観点から，認知要因に影響を与える潜在変数を決定する．

（1）因子分析の観点から，8 つの認知要因に影響を与える潜在変数の数を決定する．

（2）情報セキュリティ固有の特徴から，潜在変数を特定する．

（1）潜在変数の個数の決定

因子分析の観点から，8 つの認知要因に影響を与える潜在変数の数を決定する．因子分析は，複数の変数の背後にある，隠れた要因を明らかにすることを目的とした分析である．潜在変数の数を決定する方法には複数あり，一般的にはそれらの方法を併用して決定する．付録 2 に示すように，今回は，広く利用されている「ガッドマン・ルール（カイザーガットマン基準）」と「平行分析」の 2 つの方法を併用し，この結果から潜在変数の数を「3」とする．

（2）潜在変数の特定

文献 [2] に記載されている実験データを分析し，ウイルス対策を実施する意思を持つ人は，ウイルス感染の経験があり，IT スキルが高く，IT 知識が深い傾向があることを示した報告 [15] がある．そこで，情報セキュリティにおける認知要因に影響を与える外的要因として，この感染経験，IT スキル，IT 知識の 3 つの要因があると仮定する．

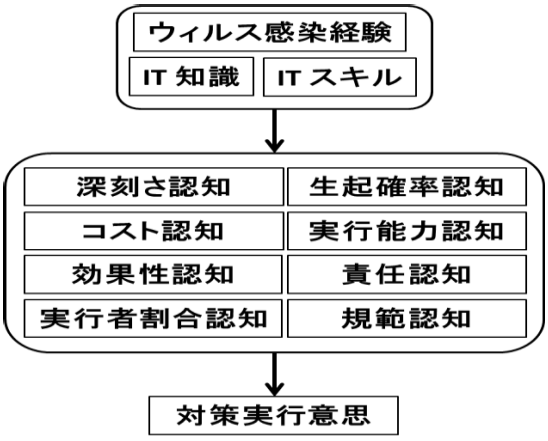


図 1 対策実行意思モデル
Fig. 1 Measure behavior intention model.

3.2 3 段構成モデル

以上の議論から，対象者が，これまでに蓄積した IT 知識と IT スキル，および感染経験によって影響を受けた認知要因が，対策実行意思を規定するという 3 段階モデルを使用する（図 1）．

4. 対策実行意思の調査

4.1 調査方法

Web を用いた質問紙調査と，仮想的なウイルス感染体験を可能とする実験の両方により調査を行った．どちらも基本的な方法は，文献 [2] に従っている．

質問紙調査では，回答者に，まず「コンピュータ・ウイルスに関する説明文」「使用 PC が感染したことを知らせるメッセージ」，「復旧方法に関する説明文」の熟読を依頼し，その後に各質問項目への回答に進む．

実験は，質問紙調査の回答者を対象に，後日，改めて本来の目的とは異なる調査目的を持つ「集合知ゲーム」の心理実験への参加募集を行い，その応募者を対象に本来の目的を伏せた状態で行った．そして，実験終了後，事後インタビューを行い，その時点で本来の実験目的を提示する．

4.2 質問紙調査

質問紙の回答を基に，図 1 の対策実行意思モデルの検証を行う．その方法は，文献 [14] のプロセスに従い，モデルに含まれる因子間の相関関係を分析するために，ピアソンの相関係数を算出し，高い相関関係が見られる因子を見いだし，次に，図 1 の 3 段構成モデルに，その結果を用いて接続関係を修正して共分散構造分析を実施する．

3 段構成の対策実行意思モデルに基づき，感染経験，IT 知識，IT スキルの 3 つと，8 つの認知要因の間に相関があるとなった場合は片方向への影響，8 つの認知要因と対策実行意思の関係についても片方向への影響を与えるとし，他の関係については両方向に影響し合うとした．

今回の調査の対象者は，**表 1** に示すように，2,266 人で

© 2015 Information Processing Society of Japan

表 1 質問紙調査参加者データ
Table 1 Data of participants for questionnaire.

	男性	女性
２０～２９歳	２７９	２７０
３０～３９歳	２７８	２７３
４０～４９歳	２９８	２８３
５０～５９歳	３０７	２７８
合計	１１６７	１１０４

表 2 実験参加者データ
Table 2 Data of participants for experiments.

	男性	女性
２０～２９歳	１３	９
３０～３９歳	１５	１２
４０～４９歳	１９	１３
５０～５９歳	１８	４
合計	６５	３８

あり，年齢は 20 歳から 60 歳まで，ほぼ均等に分布している．

4.3 実験の概要

以下の内容は主に文献 [15] に従う．

実験協力者は，質問紙調査参加者の中から 103 人を選択した．男女比および年齢構成を**表 2** に示す．

PC を持参した参加者は 40 人，貸し出した参加者は 63 人であった．さらに，ウイルス感染経験者は 41 人，経験なしが 62 人であった．

4.3.1 実験方法とシステム構成

(1) 実験の流れ

今回の実験は，文献 [2] の実験にシステム上の改良を加えたものになっており，途中に休憩が入る以外は同じ実験フロー（**図 2**）になっている．

(2) 実験協力者画面

実験協力者は，自ら選択したウェブブラウザを利用して，指定された学内 URL を参照するように指示される．すると，**図 3** のようなゲーム画面が表示される．

4.3.2 実験システムの改良

(1) 前回の実験システムの課題

前回の実験 [2] では，実験内に提示されたインシデント表示に対する対策行動と，事前に行われた Web による質問紙調査の対策意思が対応していないという結果が得られている．そこで，なぜこのような違いが生じたかを確認するために，事後インタビューの内容を検討した結果，次のような課題を見出すことができた [15]．

（**インシデント表示の発生時期**）実験協力者には，ゲームを継続するインセンティブが与えられているにもかかわらず，ゲームの途中でインシデント表示がなされる．この結果，仮に対策意思があっても，このインセンティブが対策行動を阻害した可能性がある．

（**インシデント表示の内容**）インシデント表示には，表示内容の責任元として CCC [16] を利用している．ところが，事後インタビューの分析から，CCC の知名度が低かったことが分かり，この結果，実験協力者に対して，メッセージの内容を信頼させることができていなかった可能性がある．

（**PC の保有者**）大学保有の PC を利用した．このため，仮に，その PC がウィルスに感染していたとしても，実験協力者が，その対処に責任感を持つことができなかった可能

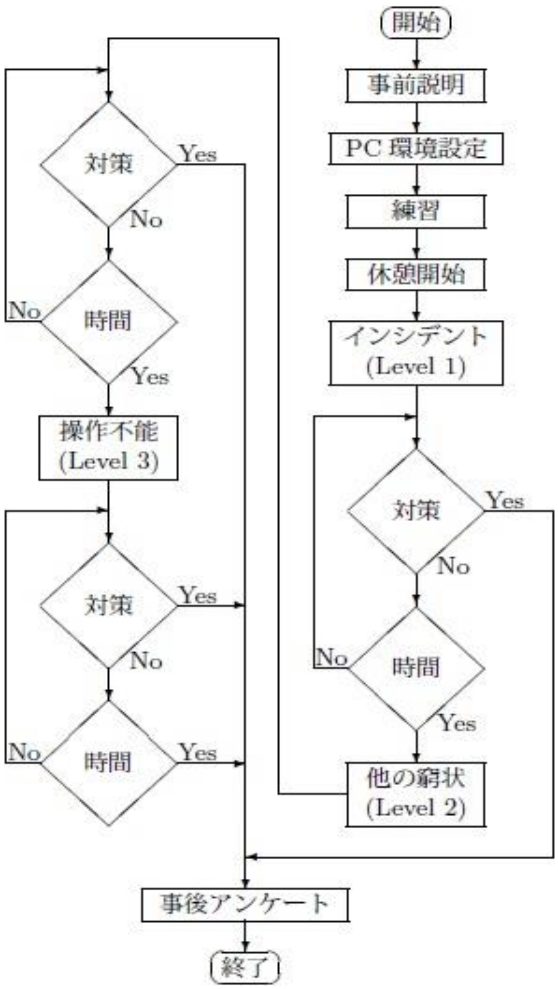


図 2 実験フロー
Fig. 2 Flow of experiment.

図 3 ゲーム画面
Fig. 3 Screen of game.

© 2015 Information Processing Society of Japan

表 3 実験システムの主要な変更点
Table 3 Changes of experiments.

番号	項目	前回	今回
1	インシデント表示の発生時期	ゲーム中	休憩時間中
2	インシデント表示の内容	CCC	著名メーカ/日大
3	PC の保有者	大学	実験協力者
4	チャットスクリプト	固定	可変

性がある．

（**チャットスクリプト**）前回の実験では，チャットスクリプトの表示内容が固定であり，実験管理者が内容を追加できるだけであった．このため，実験協力者の発話に柔軟に対応することができず，実験協力者が，実験そのものに疑問を持った可能性がある．

(2) 実験システムの改良点

そこで，今回は，これらの課題を解決するために，次のような形で改良を行った（**表 3**）．

（**インシデント表示の発生時期**）ゲーム間に休憩の時間を設け，その休憩中にインシデント表示を行う．

（**インシデント表示の表示内容**）インシデント表示に，著名なメーカの提供するウィルス対策ソフトの表示に，実験主管である日本大学のロゴをはめ込んだものを用いる．

（**PC の保有者**）可能な実験協力者には，本人の PC を利用して実験を行う．

（**チャットスクリプト**）スクリプトの記述性を高め，実験協力者の行動によって複数のシナリオを切り換える機能や，シナリオ内の発言の一部を差し替える機能などを追加し，実験協力者の発話への柔軟な対応を可能にする．

5. 分析結果と考察

5.1 質問紙調査

（**調査対象**）一般の人を対象とした Web による質問紙調査の回答結果（2,266 人）を用いて，まず 3 章で提案した対策実行意思モデルの検証を行った．なお，コンピュータの処理の能力不足の問題から，2,266 人分のデータから 1,700 人分のデータを無作為抽出し，多変量解析ツール R [17] を用いて分析を行った．なお，質問の内容および表現は，基本的に文献 [9] で使用された質問と同一のものを使用した．

（**結果分析**）各因子間の単純相関行列の結果を**表 4** に示す．これから，単純相関係数が有為に大きな関係を抜き出してパスモデルを作成し，共分散構造分析を行った．その結果が**図 4** である．

図 4 の数値は，標準偏回帰係数であり，当該予測変数（パスが出ている変数）以外の予測変数の値を一定にしたという条件下で，当該予測変数を 1 単位動かしたときの基準変数（パスを受けている変数）の平均的変化を意味する．

（**適合性**）図 4 に示したモデルの適合度指標は，GFI = 0.985，AGFI = 0.961，RMSEA = 0.049，CFI = 0.973，

表 4 各因子間の単純相関関係
Table 4 Simple correlation between factors.

	Y	A	B	C	D	E	F	G	H	L	M	N
Y	1.000											
A	0.088	1.000										
B	0.163	0.415	1.000									
C	0.301	0.372	0.318	1.000								
D	−0.002	0.155	0.140	−0.079	1.000							
E	−0.126	−0.055	−0.123	−0.048	−0.492	1.000						
F	0.290	0.282	0.300	0.511	−0.044	−0.052	1.000					
G	0.261	0.141	0.180	0.354	0.064	−0.169	0.412	1.000				
H	0.244	0.192	0.234	0.354	0.009	−0.064	0.504	0.510	1.000			
L	−0.049	0.063	0.004	0.048	−0.146	0.466	0.099	−0.038	0.076	1.000		
M	0.025	0.077	0.118	0.044	−0.009	0.102	0.064	−0.005	0.019	0.204	1.000	
N	−0.017	0.153	0.071	0.064	−0.076	0.330	0.120	−0.033	0.082	0.567	0.213	1.000

Y：対策実行意思　A：深刻さ　B：生起確率　C：効果性　D：コスト　E：実行能力
F：責任 G：実行者割合　H：規範　L：IT 知識　M：感染経験 N：IT スキル

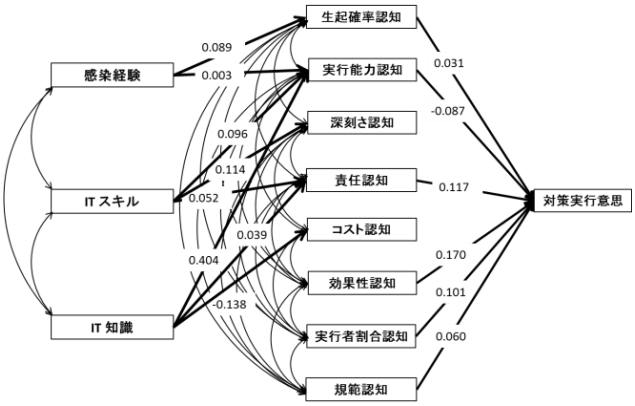


図 4 対策実行意思モデルの分析結果
Fig. 4 Analysis result of measure behavior intention model.

SRMR = 0.035 となり，適合度判定条件（GFI, AGFI, CFI の値が 0.9 以上，RMSEA，SRMR の値が 0.1 未満）を満たしており，適合度が高いといえる．

つまり，今回作成したパスモデルは，認知間の独立を仮定したモデルよりも適合度指標が改善され，しかもその数値は，十分にデータを説明しているレベルの基準を満足していると考えられる．

さらに，提案モデルの汎用性を検証するため，未使用のデータを用いて適合性を計ったところ，GFI = 0.979，AGFI = 0.944，RMSEA = 0.062，CFI = 0.963，SRMR = 0.046 となり，モデルと独立なデータに対しても適合度が高いことを示すことができた．

（**認知要因の影響力**）図 4 の分析結果から，各認知要因が対策実行意思に与える影響力は，「効果性認知」，「責任認知」，「実行者割合認知」が大きな影響を与えていると考えられる．その一方，「深刻さ認知」，「コスト認知」，「生起確率認知」は，対策実行意思にほとんど影響を与えないという結果が得られた．

5.2 実験データからの分析

（**調査対象**）分析対象を実験協力者 103 人に限定し，質問紙調査の回答結果を用いて分析を行った．ただし，対策実行意思の項目に関しては，実験での対策行動に対して得点化（Level 1 対策者 →4 点，Level 2，3 対策者および対策し

© 2015 Information Processing Society of Japan

表 5 実験協力者の行動データ
Table 5 Examine behavior data.

レベル	被験者行動	ウイルス対策	人数	
1	インシデント情報表示後、すぐに対応	実行	34	76
2	チャットメンバーの環境に被害発生後に対応		34	
3	被験者自身の環境劣化後に対応		8	
4	最後まで対応せず	不実行	3	
5	途中退出		24	
合計			103	

表 6 各因子間の単純相関関係（実験）
Table 6 Simple correlation between factors (Experiment).

	Y	A	B	C	D	E	F	G	H	L	M	N
Y	1.000											
A	0.101	1.000										
B	−0.123	0.260	1.000									
C	0.139	0.317	0.249	1.000								
D	−0.113	0.177	0.166	−0.256	1.000							
E	−0.015	0.140	0.091	0.085	−0.372	1.000						
F	0.027	0.010	0.127	0.344	−0.131	0.023	1.000					
G	0.019	0.143	0.134	0.239	−0.035	−0.051	0.393	1.000				
H	0.007	0.154	0.372	0.352	0.002	−0.001	0.491	0.375	1.000			
L	−0.074	0.161	0.046	−0.011	−0.123	0.581	0.134	−0.063	0.035	1.000		
M	−0.015	0.348	0.182	0.120	−0.024	0.335	0.347	0.211	0.234	0.409	1.000	
N	−0.097	0.311	0.217	0.101	−0.036	0.463	0.145	0.066	0.051	0.590	0.460	1.000

なかった人 →1 点，退出かつ対策する意思があった人 →4 点，退出かつ対策する意思がなかった人 →1 点）を行った結果を用いた（**表 5**）．

分析対象を実験協力者に限定した理由は，質問紙調査との結果を比較するためである．実験での行動結果を用いて分析を行うことで，実際の対策行動に影響を与えている要因が明らかになると考えたからである．

（検定力分析）単純相関行列を求める前に，実験協力者 103 人の回答データを用いて，検定力分析 [17] を行った．この分析の目的は，103 人というサンプルサイズで，十分な検定力があるのかを調査するためである．

検定力分析では，サンプルサイズ，有意水準，効果量，検定力の 4 つが，検定結果の良し悪しを決定する重要な要素であるとしており，そのうち 3 つを指定し，残りの 1 つを求めるものである．効果量とは，帰無仮説からのずれを標準化したものであり，2 変量の相関分析の場合，単純相関係数 r が効果量の指標として用いられる．また，社会科学の分野において，検定力分析を行う場合，効果量の大きさを中程度（$r = 0.3$）と仮定することが多い．

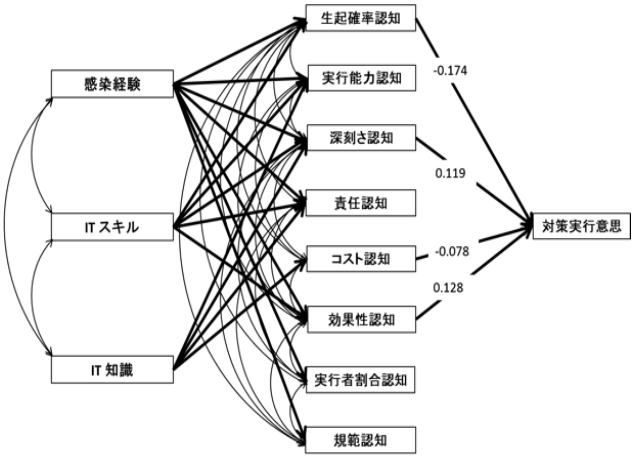
今回は分析においては，サンプルサイズ $n = 103$，有意水準 $\alpha = 0.05$，効果量 $r = 0.3$ として分析を行い，検定力を求めた．

その結果，検定力 $= 0.873$ という結果が得られた．この結果は，実際に相関がある場合，87%の確率で，その相関係数を検出できることを意味している．また，推奨されている検定力 0.8 以上を満たしており，十分な検定力があるという結果が得られた．

（結果分析）実験協力者 103 人の Web 質問紙調査の回答結果を用いて算出した単純相関行列の結果を，**表 6** に示す．

また，パス構成を含む分析結果を**図 5** に示す．

（適合性）実験協力者を対象とした分析結果において，適合度指標は，GFI $= 0.979$, AGFI $= 0.930$, RMSEA $= 0.071$, CFI $= 0.962$, SRMR $= 0.045$ となり，モデルの適合度が



	IT 知識	ウィルス感染経験	IT スキル
深刻さ	−0.017	0.255	0.205
生起確率		0.089	0.189
効果性		0.082	0.091
コスト	−0.121		
実行能力	0.444	0.080	0.174
責任	0.067	0.329	−0.014
実行者割合		0.210	
規範		0.232	

図 5 対策実行意思モデルの分析結果（実験）
Fig. 5 Analysis result of measure behavior intention model (Experiment).

高いという結果が得られた．この結果も，適合度判定条件を満たしており，このモデルが，実験協力者の回答データ（103 人）を十分に表現できているといえる．

（認知要因の影響力）各認知要因が対策実行意思に与える影響力については，「深刻さ認知」，「生起確率認知」，「効果性認知」が大きな影響を与えていることが分かった．この結果は，質問紙調査の対策実行意思に関する回答データを用いた場合の結果と大きく異なっている．

特に，「深刻さ認知」に関しては，質問紙調査の分析結果と異なり，実験協力者を対象とした場合は，一番大きな影響を与えているという結果が得られた．実際，実験後に実施した事後インタビューにおいても，ウイルス感染の恐怖と，感染が与える被害の深刻さや対策しないことによるリスクを考え対策行動を起したと回答した実験参加者が，対策実行者の 79.6%を占めることからも，深刻さ認知の影響は大きいと考えられる．

質問紙調査の場合と異なる結果が表れた理由は，回答環境の違いが考えられる．質問紙調査の場合は，ウイルス感染状態を頭の中で想定して回答しているが，実験では，実際にウイルス感染を擬似体験しており，感染経験のある実験協力者は，ウイルス感染の深刻さを思い出すし，また，未経験の実験協力者は，初めての体験から一種のパニックとなり，事態を深刻に受け止める例が見られた．つまり「感染経験」と「IT スキル」が「深刻さ認知」に与える影響力が，それぞれ 0.255，0.205 と大きいことから，感染経験と IT スキルに依存して，ウィルスの深刻さによる脅威を認識

© 2015 Information Processing Society of Japan

し対策実行意思につながると考えられる．この点については，次章でさらに考察する．

「生起確率認知」が，−0.174 と負の値になっている．これは，「生起確率認知」が，「感染経験」と「IT スキル」から影響を受けていることから，ウィルス感染が発生する確率が高いほど，再発生する度に対策実行が必要であることを経験的に知っており，対策実行に対する意欲がなくなってしまったのではないかと考えられる．

6. 質問紙と実験データの違いに関する考察

これまでの研究から，質問紙による回答データと実験データ間には相関がないことが示されており [2]，さらに今回，提案した対策実行意思モデルにおいても，対策実行意思に影響を与える要因に違いがあることを示す結果となった．この違いの要因について考察する．

人間は，自分の身に危険が及ぶような状況において，警報を受け取ると，その内容を明確にしたり，確認したり，あるいは否定したりするような付加的情報を獲得しようとする．しかし，ここに非日常的な事態を平常的・日常的なものに歪め，危機到来の予兆を異常事態とは無関係な身近で日常的な事柄に引き付けて解釈する傾向が介在する．このことを，日常化へのバイアス [18], [19] と呼ぶ．このバイアスが働くと，危機に関する情報をいくら繰り返し流し続けても人々は平常的な解釈をとり続け，警報を信用するまでに至らない．

ウイルス感染というインシデントが発生したとしても，自分なりの意味を付与し，それに自分なりの意義づけをするが，この付与や意義づけの仕方によって，同じ情報でも様々な意味に受け取ることになる．つまり，ウイルス感染という情報自体は共通でも，自身の経験や知識などを基に意味づけし，日常化へ歪めて解釈する傾向がある．つまり，情報そのものよりも，情報への意味付与や意義づけの仕方が重要であり，今回の実験では，感染対策への意味や意義を感じた実験協力者は，対策をとったし，感じなかった協力者は行動しなかったと考えられる．

一方，質問紙においても，危機感を含む臨場感を回答者が認識するように，事前に脅威文章を読んでもらった後に，回答するプロセスになっているが，実験時ほどの脅威を感じていないこと（たとえば，回答を途中で中止した者はいない）が，データの違いの要因の 1 つと考えられる．さらに，質問紙回答では，ウイルス感染時に対策を実施することは，情報倫理的には当然のこととして，その行動を選択するインセンティブが働くことも，実験データとの違いが発生する要因と考える．

以上のことから，ウイルス対策実行意思を正しく把握するためには，実験が必要であると考えられるが，そのためには，多くのコストと時間と労力が必要となり，常時，実験により対策実行意思に影響する分析を行うことは実用的ではない．

一方，質問紙調査は，長い歴史があり，質問紙の設計や調査法などについて多くの実績があり，また Web を使い，数千人規模の調査であれば，簡単に実施できる．

そこで，両方の調査結果を活用して，情報セキュリティ対策を向上させる方法を次章に述べる．

7. 情報セキュリティ行動サイクルへの応用

情報セキュリティ環境を安全に，かつ正常に運用するためには，**図 6** に示すような情報セキュリティ行動サイクルにおいて，様々な攻撃への対策をコストと便益を考慮して選択すると考えられている [20]．この行動サイクルは，抑止，防御，検出，復旧の 4 段階から構成される．抑止では，攻撃者の様々なコンピュータ攻撃を企てる意図を抑圧し，利用者の情報セキュリティポリシを守り，コンプライアンスを促進させるような情報セキュリティ教育が行われる．防御とは，抑止が利かなかった攻撃に対する次の対策であり，検出は，主としてウイルス検出とシステム動作障害の分析により，被害者を特定し，さらに攻撃元，つまり，加害者を見つけることである．そして，復旧では，システムに正常なプログラムを再インストールして元の状況に戻すが，その後，再発防止のために，違反者への制裁や懲戒，権利剥奪なども行う．

以上の 4 段階のなかで，防御と検出は，基本的に技術的な制御によって実行される．また抑止と復旧は，受身であり，非技術的な制度や運用に関わる設計となる．5 章で，質問紙調査で得られたセキュリティ対策実行意思に影響する認知要因は，効果性，責任，実行者割合であったが，このことを考慮したウイルス対策用ビデオや本などの教材は，「抑止」段階における教育用コンテンツとして使うことで有効になる．従来の教育コンテンツでは，「深刻さ」に重点をおいたコンテンツと見なされるが，教育効果を考えれば，上記の 3 因子に重きをおいたシナリオにした方が効果的であろう．

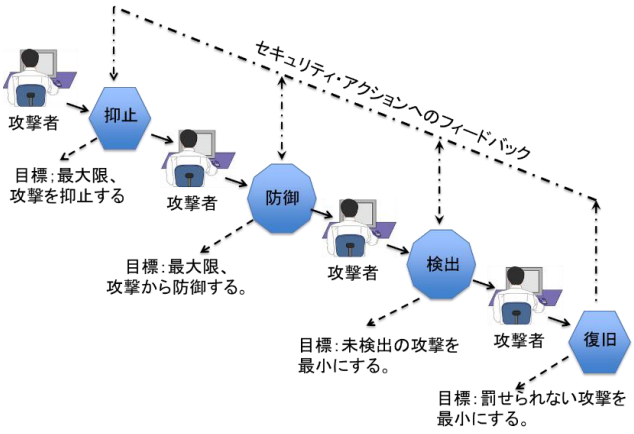


図 6 情報セキュリティ行動サイクル
Fig. 6 Information security action cycle.

© 2015 Information Processing Society of Japan

また，実験データから得られた結論では，質問紙調査のみの分析結果では無視された「深刻さ」が大きな影響力を持つことが分かった．実際に，ウイルス感染しているPCユーザに，復旧作業を開始させるような説得メッセージには，健康や環境時の説得と同じように，「深刻さ」を刺激する内容にすることが重要と思われる．復旧作業において，PCユーザの感染経験およびITスキルが重要な意味を持ち，感染経験があり，しかもITスキルが高いユーザであれば，自立的に復旧作業を行えるが，逆に，感染経験がなく，またITスキルの低いPCユーザには，ウイルス感染の深刻さを強くアピールするとともに，具体的で，やさしい復旧の方法をメッセージに盛り込ませる必要があると思われる．

8. まとめ

情報セキュリティ対策行為に導くことを目的に，対策実行意思に影響を与える要因を，集団的防護動機理論に基づき検討した．その結果，深刻さ，生起確率，効果性，コスト，実行能力，責任，実行者割合，規範の8つの規定要因に，感染経験，IT知識，ITスキルの3つの潜在要因を加えたモデルを提案し，そのモデルが，調査データを十分表現していることを示した．さらに，実験により，対策実行を実施した協力者のデータを同じモデルで分析を行い，対策実行意思に，深刻さ認知，効果性認知，および生起確率認知が影響することを示した．さらに，これらの結論を情報セキュリティ対策に活用する方策に関しても述べた．今後は，今回の結果の正当性を検証するために，実際の教育コンテンツおよび説得メッセージを出すシステムを設計・構築し，予想した効果の確認を工学的に示す予定である．また質問紙調査のみでは，ヒトの思考や行動を把握することは困難であり，今回のような実験が不可欠と考えるが，多くの時間と費用を必要とし，容易に実施できる検討ではない．簡易に，かつ精度の良い実験環境の構築が課題である．

謝辞 この研究を進めるための貴重な機会を与えていただいた情報処理推進機構小松文子博士，質問紙作成と実験方法に貴重な助言をいただいた同志社大学池田謙一教授，高木大資博士，実験方法について助言いただいた東京大学山岸俊男特任教授，さらに実験実施に多大な協力をしてくれた吉開/栗野ゼミの皆様に感謝いたします．

なお本研究は，（独）情報処理推進機構における「情報セキュリティ現象の社会科学的分析に関する調査」の一部として実施し，日本大学学術研究助成金（総合）総11-010，および科学研究費補助金（基盤研究（C）課題番号：26330386）による助成を受けて実施した．

参考文献

[1] 独立行政法人情報処理推進機構セキュリティセンター：サービス妨害攻撃の対策等調査報告書 (2010)，入手先 ⟨http://www.ipa.go.jp/files/000014123.pdf⟩.
[2] 独立行政法人情報処理推進機構：リスク認知と実行に関する調査報告書 (2012)，入手先 ⟨http://www.ipa.go.jp/security/economics/report/behavior/⟩.
[3] 内田勝也，矢竹清一郎，森 貴男，山口健太郎，林 華枝：情報セキュリティ心理学の提案，IPSJ研究報告，CSEC，Vol.2007, No.16, pp.327–331 (2007).
[4] 小川隆一，島 成佳，福住伸一，角尾幸保：高度化したサイバー攻撃対策の心理学的アプローチについて，SCIS2015，No.4D1-1 (2015).
[5] 塚脇涼太，深田博己，樋口匡貴，蔵永 瞳，濱田良祐：様々な環境配慮行動に対する精緻化された集合的防護動機モデルの適用，説得交渉学研究，No.2, pp.41–56 (2010).
[6] Frandsen, K.D.: Effects of threat appeals and media of transmission, *Speech Monographs*, Vol.30, pp.101–104 (1963).
[7] Shropshire, J.D., Warkentin, M. and Jhnston, A.C.: Impact of Negative Message Framing on Security Adoption, *Journal of Computer Information Systems*, Fall, pp.41–51 (2010).
[8] Roger, R.W.: A protection motivation theory of fear appeals and attitude change, *Journal of Psychology*, Vol.91, pp.93–114 (1975).
[9] 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).
[10] 大門貴志，吉川俊博，手良向聡（訳）：Rによる統計解析ハンドブック，メディカルパブリケーション (2010).
[11] 豊田秀樹：共分散構造分析 [入門編]，浅倉書店 (1998).
[12] 栗野俊一，吉開範章，高橋俊雄：コンピュータウイルス感染体験実験法の提案と構築，電子情報通信学会技報SITE112(127)，pp.229–235 (2012).
[13] Taylor, S.E., Peplau, L.A. and Sears, D.O.: *Social Psychology*, 8th ed., Englewood Cliffs, NJ: Prentrice Hall (1994).
[14] 高本雪子，深田博己：エイズ説得に必要な情報の特定とその影響メカニズムの解明，説得交渉学研究，Vol.2, pp.11–27 (2010).
[15] 吉開範章，栗野俊一，飯塚信夫，神田大晃，高橋敏雄：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，Vol.2011-GN-79, No.2, pp.1–6 (2011).
[16] サイバークリーンセンター：サイバークリーンセンター活動実績 (2011)，入手先 ⟨https://www.telecom-isac.jp/ccc/report/201101/1101monthly.html⟩.
[17] 金 明哲：Rによるデータサイエンス，北森出版株式会社 (2007).
[18] Cohen, J.: A power primer., *Psychological Bulletin*, Vol.112, pp.155–159 (1992).
[19] 池田謙一：緊急時の情報処理，東京大学出版会 (1997).
[20] Straub, D. and Welke, R.: Coping with systems risk: Security planning models for management decision making, *MIS Quarterly*, Vol.22, No.4, pp.441–469 (1998).

付 録

A.1 認知間の独立を仮定したモデルの適合度

4.2節で示した質問紙調査データに関する分析結果を**図 A·1**，**表 A·1** に示す．

© 2015 Information Processing Society of Japan

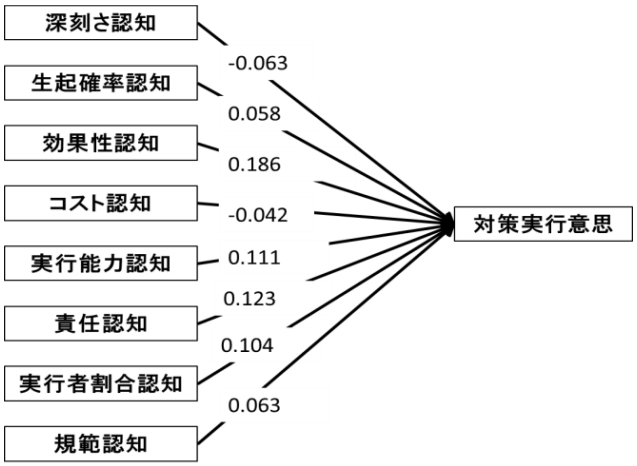


図 A·1 独立を仮定したモデルの分析結果
Fig. A·1 Analysis result of independent model.

表 A·1 独立を仮定したモデルの適合度指標
Table A·1 Fit index of independent model.

GFI	0.664
AGFI	0.460
CFI	0.080
RMSEA	0.251
SRMR	0.232

A.2 潜在変数の個数の決定

因子分析は，複数の変数の背後にある，隠れた要因を明らかにすることを目的とした分析である．潜在変数の数を決定する方法にはいくつかの種類があり，一般的には複数の方法を併用して決定する．今回，多く利用されている「ガッドマン・ルール（カイザーガットマン基準)」と「平行分析」の 2 つの方法を併用し，潜在変数の数を決定した．

○ガッドマン・ルール（カイザーガットマン基準）
観測データから算出した相関行列の固有値が 1 より大きなものの個数を因子数とする方法．

○平行分析
1. 「観測データと同じ観測変数の数」と「観測データと同じ標本サイズ」の乱数データを n 個作成
2. 各乱数データから固有値を算出
3. 「観測データの固有値」＞「各乱数データの固有値」となる最大固有値番号を因子数とする

ガッドマン・ルールの結果を**図 A·2** に示す．

観測データから算出した相関行列の固有値を求めると，2.755，1.526，1.108，0.643，0.593，0.526，0.435，0.414 となる．図 A·2 において，○印は固有値の値である．図 A·2 からも分かるように，1 より大きな固有値が 3 つである．

次に，平行分析の結果を**図 A·3** に示す．

図 A·3 において，点線は，乱数データから算出した固有値の推移を示している．図 A·3 から，「観測データの固有値」＞「各乱数データの固有値」となる最大固有値番号が 3 であることが分かる．

よって，「ガッドマン・ルール（カイザーガットマン基準)」と「平行分析」の 2 つの分析から，8 つの認知要因に影響を与える潜在変数の数は 3 つが適切であると判断できる．

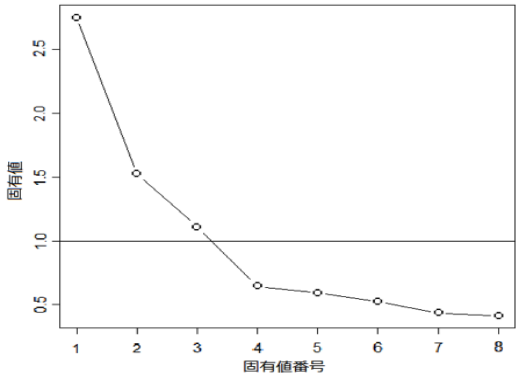


図 A·2 ガットマン・ルールによる因子数決定
Fig. A·2 Number of factors by Guttman rule.

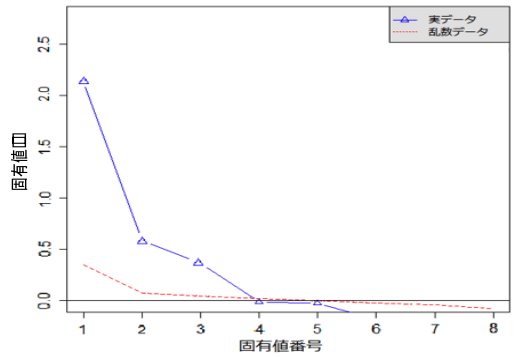


図 A·3 平行分析による因子数決定
Fig. A·3 Number of factors by parallel analysis.

浜津 翔

2013 年日本大学理工学部数学科卒業．2015 年日本大学大学院理工学研究科博士前期課程修了後，株式会社富士通エフサス入社．

栗野 俊一 （正会員）

1986 年早稲田大学大学院理工学研究科博士前期課程修了．1989 年同後期課程中退後，早稲田大学助手．1992 年日本大学助手，2015 年より同大学准教授．博士（理学）．主に，データ構造，アルゴリズムの研究に従事．

© 2015 Information Processing Society of Japan

吉開 範章 （正会員）

1979年電信電話公社（現，NTT）入社．1999年NTT情報流通基盤総合研究所プロジェクトマネージャ．2004年日本大学総合科学研究所教授．2010年より日本大学理工学部教授，現在に至る．博士（工学）．主にネットワークでの活動活性化に関する研究に従事．IEEE，電子情報通信学会，交通工学研究会等各会員．

© 2015 Information Processing Society of Japan