情報処理学会論文誌 Vol.53 No.2 485–493 (Feb. 2012)

防護動機理論を援用したボット対策促進メッセージによる受信ユーザの態度変容要因の抽出と知識による影響の分析と検証

島 成佳[1,2,a)] 小松 文子[2] 高木 大資[3] 北村 浩[1,4]

受付日 2011年5月23日, 採録日 2011年11月7日

概要：インターネットは，企業活動や市民生活において共有のインフラであり，社会生活に影響のないように安全な環境が望まれている．情報セキュリティでは，安全な環境の維持に，少しでも多くの利用者に情報セキュリティ対策を行うように求めているが，利用者に情報セキュリティ対策の意思があっても，対策を実施しないという現象が知られている．利用者による対策実施向上のための新しいアプローチとして，個人の振舞いや意思決定に関する研究が始まっている．本論文は，情報セキュリティ対策としてボット対策をターゲットとし，社会心理学における説得の心理学の研究をもとに，防護動機理論の説得メッセージによる態度変容に関わる要因を明らかにするアンケート調査を実施して分析した結果を報告する．また，防護動機理論の説得メッセージによる態度変容において，情報技術の知識が影響することを新たに明らかにした．

キーワード：情報セキュリティ，リスク認知，防護動機理論，ボット対策

Survey and Analysis on Attitude Transformation Factors Based on Protection Motivation Theory for Anti-bot Promotion

Shigeyoshi Shima[1,2,a)] Ayako Komatsu[2] Daisuke Takagi[3] Hiroshi Kitamura[1,4]

Received: May 23, 2011, Accepted: November 7, 2011

Abstract: Users hope for secure environment in the Internet that is social infrastructure. However, cases where information security measures are not executed even if users have the execution intention of information security measures. For effective information security measures promotion, researches of individual behavior and the decision making based on the social psychology has started in the information security field. In this paper, we conducted a questionnaire investigation of an anti-bot measure based on the research of the psychology of the persuasion in the social psychology and analyzed the questionnaire investigation. Factors of the persuasion message of Protection Motivation Theory that influenced the attitude transformation for the anti-bot measure were clarified. In addition, the knowledge of information technologies influenced the attitude transformation by the persuasion message of Protection Motivation Theory.

Keywords: information security, risk perception, Protection Motivation Theory, anti-bot measure

1. はじめに

インターネットは，個人や企業の社会生活や社会経済活

[1] 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[2] 独立行政法人情報処理推進機構セキュリティセンター
IT Security Center, Information-technology Promotion Agency, Japan, Bunkyo, Tokyo 113–6591, Japan
[3] 東京大学大学院人文社会系研究科
Graduate School of Humanities and Sociology, The University of Tokyo, Bunkyo, Tokyo 113–8654, Japan
[4] 日本電気株式会社サービスプラットフォーム研究所
Service Platforms Research Laboratories, NEC Corporation, Kawasaki, Kanagawa 211–8666, Japan
[a)] s-shima@ipa.go.jp

動に浸透し，社会インフラとして公共財の性格を持っており，利用者から安全な環境であることを望まれている．安全な環境を損なう情報セキュリティインシデントは，インターネットを公共財の価値として減少させる事象である．情報セキュリティインシデントを防止する情報セキュリティ対策では，利用者が情報セキュリティ対策を実施することにより，利用者のパソコンや個人情報等の情報資産を守るだけでなく，公共財としてのインターネットの保護にもつながる [1]．安全なインターネット環境の維持には，少しでも多くの利用者による情報セキュリティ対策の実施が期待されており，情報セキュリティ領域では，これまでの技術的対策と異なるアプローチとして，新たに個人の振舞いや意思決定に注目した研究が始まっている．

本論文では，情報セキュリティ対策としてボット対策を取り上げ，注意喚起による利用者のボット対策の実行割合向上を目的に，利用者の対策実行意図に影響を与える要因を明らかにすべく，社会心理学における説得の心理学の既存研究を援用したアンケート調査を実施し，分析した結果を報告する．

本論文の構成は以下のとおりである．2 章でボット対策，3 章で関連研究，4 章で課題設定，5 章でアンケート調査設計，6 章で分析結果，7 章で考察を述べ，8 章のおわりにでまとめを述べる．

2. ボット対策とは

ボットとはコンピュータウイルス（悪意のプログラム）の一種である．ボットが利用者のコンピュータに感染すると，そのコンピュータは攻撃者からインターネットを介して遠隔操作可能になるという特徴がある．そのため，攻撃者から操られるコンピュータの様子が，ロボット（Robot）と似ていることから，ボット（BOT）と呼ばれる．ボットに感染したコンピュータは，ボットに感染した多数のコンピュータから構成されるボットネットに組み込まれ，攻撃者の支配下に置かれ，迷惑行為や犯罪に利用される．ボットネットはこれまで SPAM メール配信や DDoS 攻撃に使用されてきたと考えられてきた．しかしながら，2010 年 2 月の Mariposa と呼ばれる 1,200 万台以上のボットに感染したコンピュータから構成された巨大ボットネットの摘発等により，現在はネットワークを介した様々な犯罪に使用されていることが明らかとなった [2]．また，攻撃者はボットネットの拡大も図っており，2010 年の年初から年末にかけて，ボットに感染したコンピュータは 654%も増加している [2]．このようにボットがインターネットにおいて犯罪に使用されることと，感染の広がりを見せていることから，近年ボット対策が情報セキュリティにおいて重要な課題の 1 つとなっている．

国内では，ボット対策として，経済産業省と総務省の連携のもと，2006 年にサイバークリーンセンター（Cyber Clean Center: CCC）[*1]が開設された．サイバークリーンセンターは，IPA や JPCERT/CC 等の公的機関やインターネットサービスプロバイダ（ISP）の協力のもと，ボットの駆除と感染防止対策を推進してきた．その活動の 1 つとして，ボットに感染したコンピュータを発見し，そのコンピュータの利用者に ISP を通じて注意喚起メールを送付してきた．この注意喚起メールでは，利用者がサイバークリーンセンターの Web サイトにアクセスし，ボットの危険性を説明文から理解し，駆除ツールをダウンロードして実行することを促していた．この注意喚起メールによって，ボットに感染したコンピュータの利用者がボットを駆除すると，ボットに感染したコンピュータの減少だけでなく，他のコンピュータへの感染拡大防止にもつながる．しかしながら，注意喚起メールを受信したボット感染コンピュータの利用者のうち，サイバークリーンセンターのボット対策サイトへの訪問率は約 39%で，駆除ツールのダウンロード率は約 30%にとどまっている [4]．サイバークリーンセンターでは，訪問率やダウンロード率の向上のため，注意喚起メールのタイトルや本文の構成を工夫する等の試行錯誤による施策を試みてきたが [5]，高い訪問率やダウンロード率の向上につながらなかった．そのため，試行錯誤による経験的な施策では限界であり，新たなアプローチによる施策が必要と考えられる．

振り込め詐欺対策でも，2008 年当時，広報啓発活動による注意喚起を行ってきたが，被害が続く状況から現状の対策のみでは限界であり，新たな試みが必要であったことが，平成 20 年版国民生活白書 [6] で述べられている．そして，被害防止に向けた新たな試みの 1 つとして，内閣府の調査事業で実施された，社会心理学等の学術的なアプローチによる対策が紹介されている．内閣府の調査事業報告書では，詐欺の手口に関して実験結果から振り込め詐欺被害者の意思決定メカニズムを説明し，時間的切迫感が振り込みをしてしまう要因であることを明らかにし，対策として「少し待つ」ことが有効であると示唆している [7]．注意喚起では，社会心理学等の学術的なアプローチからの対策を取り入れることにより，注意喚起メールによる利用者の対策実施率の向上につながると考えられる．

3. 関連研究

3.1 防護動機理論・集合的防護動機理論

個人の態度や行動を変化させる効果的なメッセージに関する研究は，社会心理学の一分野である「説得の心理学」[8] で行われている．説得の心理学では，“説得メッセージ” の受け手による “態度変容” のプロセスが，**図 1** のようなプロセスで示される．個人は，説得メッセージを受け取ると，まずは説得メッセージを理解する．そして，これまでの記

[*1] https://www.ccc.go.jp/ccc/index.html, 本事業は 2011 年 3 月に終了している．

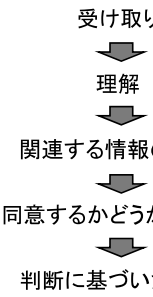

図 1 “説得メッセージ” による “態度変容” のプロセス
Fig. 1 Process of attitude transformation based on persuasion message.

憶や知識等から関連する情報を想起して，想起した情報をもとにして同意するかどうかを判断して行動する．

ボット対策において，ISP から利用者に送信する注意喚起を “説得メッセージ” とし，駆除ツールをダウンロードする行動を “態度変容” ととらえると，説得の心理学の枠組みにあてはめることが可能である．

サイバークリーンセンターは，注意喚起にメールと Web を組み合わせ，ボットに感染したコンピュータの利用者にメールで感染を知らせ，Web サイトでボットの危険性を説明してボット駆除ツールのダウンロードと実行を促していた．説得の心理学では，このように注意喚起でボットの危険性を説明（脅威アピール）し，ボット駆除ツールのダウンロートと実行（対処行動）を促すコミュニケーションによる態度変容の研究として，Rogers により防護動機理論 [9], [10] が提唱されている．

防護動機理論では，受け手に直面する問題の脅威をアピールすると，その脅威を予防・低減させて自分自身を守ろうとする動機から，対処行動が発生するとしている．対処行動の規定要因としては，「深刻さ認知」，「生起確率認知」，「効果性認知」，「コスト認知」，「実行能力認知」の 5 つが影響するとされている．

また，受け手にアピールする脅威には，一個人で対処できる脅威と一個人で対処できない脅威が存在する．たとえば，前者は歯周病という脅威に，歯磨きという対処行動で脅威を予防・低減できる．一方，後者は電力不足による停電という脅威に，一個人のみの節電行為では脅威を予防・低減できない．脅威の予防・低減には，集団での節電行為が必要となる．このような脅威に集団的な対処行動を促す脅威アピールに関する研究として，集合的防護動機理論が提唱されている [11]．

集合的防護動機理論では，対処行動の規定要因として，「深刻さ認知」，「生起確率認知」，「効果性認知」，「コスト認知」，「実行能力認知」の防護動機理論の 5 つに，「責任認知」，「実行者割合認知」，「規範認知」の 3 つを加えた 8 つが影響するとされている．

情報セキュリティに防護動機理論・集合的防護動機理論を適用した研究としては，情報セキュリティ対策における説得メッセージによる態度変容の研究 [12] や情報セキュリティリテラシ教育における子供たちを取り巻くセキュリティリスクを解明するモデルの研究 [13] が報告されている．これらの研究から，脅威アピールにおける個人の態度変容は個人の状況によって異なることが知られている．

3.2 情報モラル教育

近年，学校ではインターネットや携帯電話の普及にともなうトラブルや事件の増加から，情報モラル教育が実施されている．情報モラル教育の領域では，インターネットや携帯電話の利用において正しく行動するための判断を育成することを目的とした指導法や教材開発，実践等の取組みが報告されている [14]．情報モラルに関する研究では，道徳的規範知識，情報技術の知識，合理的判断の知識という 3 種類の知識を組み合わせた指導法が提唱されている [15], [16]．これら 3 種類の知識は，情報社会において，正しい行動を判断するために必要な要素であるとしている．情報社会における特徴としては，道徳的規範知識に加えて，情報技術の知識が必要なことである．また，合理的な判断の知識は道徳的規範知識と情報技術の知識を組み合わせて判断するための考え方の枠組みであり，新たに情報技術の知識を導入することで必要となった知識である．情報モラルにおける判断では，情報技術の知識が低いと道徳的規範の知識が高くても，誤った判断をくだしてしまう．たとえば，そのような利用者は献血募集のチェーンメールが送られてくると，人道的な観点からチェーンメールを転送してしまうことがある [17]．このように情報社会では，正しい行動を判断するために，情報技術の知識を必要とする．

4. 課題設定

本論文では，インターネット利用者を対象にボット対策の注意喚起メールで，脅威のアピール：注意喚起，対処行動：駆除ツールのダウンロードと実行（対策実行意図）を促し，対策実行意図に影響を与える防護動機理論・集合的防護動機理論の対処行動を規定する要因を明らかにする．なお，ボット駆除ツールをダウンロードして実行するという対策実行意図は，個人的な対処行動ととらえられるが，個人がボット対策を行うことでインターネット上の他者を守ることにもなるという集団的な対処行動ともとらえられるため，どちらの対処行動ととらえることが適切であるかについても明らかにする．

また，ボット対策をインターネット利用における行動の 1 つとすると，駆除ツールのダウンロードと実行（対策実行意図）に至る判断が情報モラルにおける判断をする 1 場面ととらえることが可能である．このとき，利用者は情報技術の知識が低いと，適切な対策実行意図の判断を誤ってしまう可能性がある．そのため，防護動機理論・集合的防護動機理論でも，対策実行意図に至る判断（図 1 の「同意

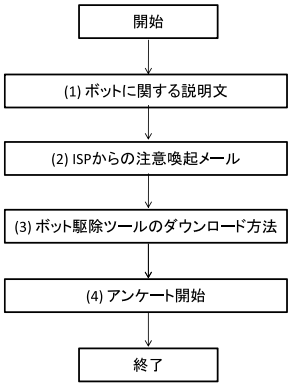

図 2 アンケートの流れ
Fig. 2 Questionnaire process.

するかどうかの判断」）において，情報技術の知識が影響を与えていると仮定できる．本論文では，情報社会に適用する場合に，防護動機理論・集合的防護動機理論の説得メッセージにおいて，情報技術の知識が影響を与えるかどうかを分析して検証する．

5. アンケート調査設計

参加者に実施したアンケート調査の流れを述べたのちに，防護動機理論・集合的防護動機理論と情報技術の知識に関するアンケート項目を示す．

5.1 アンケート調査の流れ

アンケート調査では，サイバークリーンセンターのボット対策の手順を参考にし，**図 2** の流れに示すように，参加者に，(1) ボットに関する説明文，(2) ISP から送信された注意喚起メール，(3) ボット駆除ツールのダウンロード方法の文書を提示したのちに，(4) アンケートを実施した．

アンケートは，参加者が 3 つの提示した文書を読み終わったことを確認したのちに，防護動機理論・集合的防護動機理論と情報技術の知識に関するアンケートを開始した．なお，回答の正確性を図るため，参加者にアンケートの趣旨を類推されないように，アンケート項目には，上記の項目以外にも多様な項目を混ぜて，アンケートを実施した．

5.2 防護動機理論・集合的防護動機理論

防護動機理論・集合的防護動機理論に関するアンケート項目では，対策実行意図と，対策実行意図を規定する防護動機理論の 5 つの要因と集合的防護動機理論の 8 つの要因についての項目を設定した．また，防護動機理論の対処行動を規定する 5 つの要因，集合的防護動機理論の対処行動を規定する 8 つの要因が，対策実行意図に影響を与える関係を**図 3** に示す．

以下は，対策実行意図のアンケート項目である．

- 対策実行意図「自分に先ほどのようなメールが送られてきた場合，指示された対策を行う」（「あてはまる」〜「あてはまらない」の 4 件法）

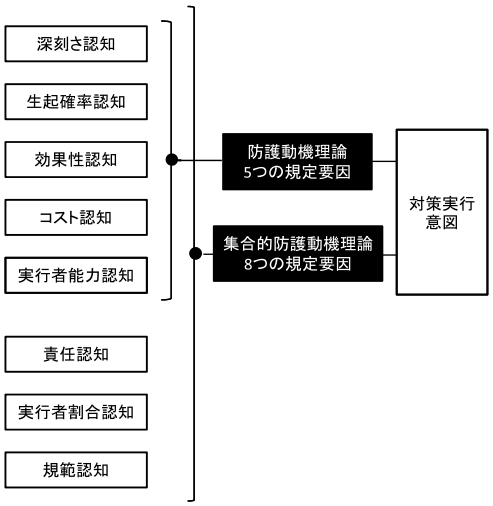

図 3 実行対策意図と防護動機理論・集合的防護動機理論の対処行動を規定する要因の関係
Fig. 3 Relation between execution intention and factors of Protection Motivation Theory/Collective Protection Motivation Theory.

以下は，防護動機理論・集合的防護動機理論のアンケート項目である．

- 深刻さ認知「ボットウィルスに感染した場合，パソコンに深刻な被害がもたらされるだろう」（「あてはまる」〜「あてはまらない」の 4 件法）
- 生起確率認知「将来，自分自身のパソコンがボットウィルスに感染する可能性があるだろう」（「あてはまる」〜「あてはまらない」の 4 件法）
- 効果性認知「先ほどの文章で示された対策は，ボットウィルスの感染予防に有効だ」（「あてはまる」〜「あてはまらない」の 4 件法）
- コスト認知「先ほどの文章で示された対策は，自分にとって，実行に伴う負担やリスクが大きい」（「あてはまる」〜「あてはまらない」の 4 件法）
- 実行能力認知「先ほどの文章で示された対策を実行することは，自分にとって技術的・知識的に難しい」（「あてはまる」〜「あてはまらない」の 4 件法）
- 責任認知「自分にはこの駆除手順を実行する責任がある」（「あてはまる」〜「あてはまらない」の 4 件法）
- 実行者割合認知「先ほどの文章で示されたボットウィルス対策は，多くの人が実行しているだろう」（「あてはまる」〜「あてはまらない」の 4 件法）
- 規範認知「自分がボットウィルスの対策を実行することを，周囲の人たちは期待しているだろう」（「あてはまる」〜「あてはまらない」の 4 件法）

5.3 情報技術の知識

情報技術の知識に関するアンケート項目では，ボットに関する理解度を測る項目と，コンピュータ利用に関係する

IT スキルを測る項目を設定した．

5.3.1 理解度の項目

理解度を測る，ボットに関する 5 つのクイズを以下に示す．クイズでは参加者に「はい」，「いいえ」の選択式で回答を求めた．理解度の得点は，5 つのクイズの正解数の合計から求めた．

- ボットウイルスは自分自身をバージョンアップさせる機能がある．
- ボットウィルスはネットワーク上の他のパソコンに感染することがある．
- ボットウィルスは指令サーバを変更することがある．
- ボットウィルスはインターネット上でネットワークスキャン活動を行う．
- ボットウィルスはパソコン上から情報を盗み出すことがある．

ただし，クイズの内容が理解できず意図を持たずに回答した参加者の得点を排除するために，クイズ以外に「説明文が理解できない」という項目を用意し，「はい」，「いいえ」の選択式で回答を求めた．

5.3.2 IT スキルの項目

IT スキルでは，インターネットを利用するときに，利用するアプリケーションやサービス全般のスキルを問う項目を設定した．すべての項目は，「1. できるし，よくする」〜「4. 何のことか分からない」までの 4 件法で回答を求めた．IT スキルの得点は，参加者の IT スキルの特徴抽出と，その特徴に与える各項目の影響を考慮して，以下の 11 項目を主成分分析して得られた主成分得点とした．

(1) ワープロソフトで文章を作る．
(2) パソコンでメールのやりとりをする．
(3) ヤフー（yahoo）やグー（goo）等で必要な情報を見つける．
(4) 自分の好きなホームページをお気に入りに入れる．
(5) 写真やビデオをコンピュータに取り込んだり，文章にはりつけたりする．
(6) インターネットや CD の百科事典を使って調べる．
(7) 電子メールにファイルを添付して送信する．
(8) ホームページを作る．
(9) チャットによる会話．
(10) mixi や GREE といった，ソーシャル・ネットワーキング・サービスの閲覧や書き込み．
(11) Twitter の閲覧や書き込み．

6. アンケート調査の分析結果

6.1 アンケート調査の概要

本論文では，ボット感染者となり注意喚起メールを受信する可能性のある，インターネット利用者を対象とする．インターネット利用者は，現状攻撃手法の複雑化・巧妙化により，誰もがボットに感染して注意喚起メールを受信する可能性がある．誰もがボット感染する例として，ドライブ・バイ・ダウンロード攻撃は，Web サイトを閲覧するだけで利用者の意図にかかわらずウイルス（ボット）をダウンロードさせ，知らぬ間に感染させる．また，ゼロディ攻撃は，ソフトウェアで判明した脆弱性が対応されるまでの間に，その脆弱性を突いてウイルス（ボット）を感染させる．このように情報技術の知識の有無にかかわらず，現状誰もがウイルスに感染してしまう．

表 1 性別・年齢階層別参加者の構成
Table 1 Number of respondents by sex and age.

	男性	女性
20〜29 歳	280	266
30〜39 歳	287	276
40〜49 歳	284	275
50〜59 歳	293	293
合計	1,144	1,110

（※）最小値：20，最大値：59，平均値：40.02，標準偏差：10.53

本論文では，インターネットを利用する人々を効率的に抽出するため，株式会社クロス・マーケティングの保有するモニタ会員および Web アンケート環境を用いたインターネットによるアンケート調査とした．これらのモニタ会員も，インターネットを利用すると，意図せずにボットに感染する可能性があるという点で「注意喚起メールを受信する可能性のあるインターネット利用者」と同じである．

本アンケート調査は 2010 年 3 月 9 日〜3 月 10 日の期間に実施し，2,254 人から回答を得た．また，本アンケート調査では，インターネット利用者の誰もが感染することから，参加者の年齢や性別において，**表 1** に示すように偏りのないサンプルとした．

6.2 対策実行意図への防護動機理論と集合的防護動機理論の影響

ボット対策における参加者の意思決定では，防護動機理論と集合的防護動機理論のモデルによるロジスティック回帰分析の結果（**表 2**）から，防護動機理論の対処行動を規定する変数群のモデルよりも，集合的防護動機理論の対処行動を規定する変数群のモデルの方が，正解率[*2]が高く（正解率：66.28%（防護動機理論）< 70.72%（集合的防護動機理論）），モデルの説明力が高い．このことから，一見個人的な対処行動に思えるボット対策も集合的な事象であることを参加者に認識させると，参加者の対策実行意図を高めることが可能であると示唆された．さらに，集合的な事象ととらえた場合に，対処行動を規定する要因として，責任認知と実行者割合認知が他の要因よりも対策実行意図に影響を与えることが統計的に示唆された．

また，防護動機理論と集合的防護動機理論の両方で対処

[*2] モデルによる対策実行意図の有無の予測結果と，実際の対策実行意図の有無の回答が一致している割合

表 2 従属変数：対策実行意図，独立変数：防護動機・集合的防護動機の対処行動を規定する要因のロジスティック回帰分析結果
Table 2 Results of Logistic Regression Analysis for factor of Protection Motivation Theory and Collective Protection Motivation Theory.

従属変数：	対策実行意図			
	防護動機		集合的防護動機	
独立変数	β	有意確率	β	有意確率
深刻さ認知	0.1320	*	0.0702	
生起確率認知	0.1508	**	0.1001	
効果性認知	0.7673	***	0.5398	***
コスト認知	0.2694	***	0.2416	***
実行能力認知	−0.1714	**	−0.1358	**
責任認知			0.3667	***
実行者割合認知			0.3547	***
規範認知			0.0485	
疑似決定係数	0.196		0.252	
正解率	66.28%		70.72%	

Note：（有意確率）$***p < .001$，$**p < .01$，$*p < .05$，$\dagger p < .10$

表 3 理解度得点ごとの参加者数
Table 3 Number of respondents in each group of understanding level.

得点	0 点	1 点	2 点	3 点	4 点	5 点
度数	153 人	614 人	855 人	346 人	125 人	161 人
割合	6.8%	27.2%	37.9%	15.3%	5.5%	7.1%

行動を規定する要因として，効果性認知とコスト認知が他の要因よりも対策実行意図に影響を与えている．特に効果性認知は，回帰係数 β の値が他の要因と比べても高く，対策実行意図に強い影響を与えていることが統計的に示唆された．

6.3 情報技術の知識による態度変容に与える影響

6.3.1 理解度の得点

理解度の得点は，ボットに関する 5 つのクイズの正答数によって計算した（0〜5 点）．ただし，クイズ以外の質問項目の「説明文が理解できない」に「はい」と答えた参加者は，説明文が理解できなかったものとし，得点を 0 点とした．理解度の得点ごとの参加者数は，**表 3** のとおりであり，参加者全体の平均得点は 2.07 点である．

6.3.2 IT スキルの得点

IT スキルの得点は，主成分分析の第 1 主成分と第 2 主成分の各 IT スキル項目の係数（**表 4**）から，各参加者の第 1 主成分得点と第 2 主成分得点を計算して求めた．

第 1 主成分は，すべてのスキル項目の係数がプラスに評価されるため，第 1 主成分得点が高いと，インターネットを利用する全般的なスキルが高いと評価する．第 1 主成分得点の参加者全体の平均は，24.37 であった．一方，第 2 主成分は，ソーシャルメディアと呼ばれるアプリケーションやサービスの利用にかかわる項目の係数がプラスに評価

表 4 IT スキルの主成分分析の結果
Table 4 Results of principal component analysis of IT skill.

IT スキル項目	第 1 主成分の係数	第 2 主成分の係数
1	0.668	−0.262
2	0.729	−0.379
3	0.690	−0.381
4	0.703	−0.307
5	0.767	−0.046
6	0.721	−0.172
7	0.789	−0.216
8	0.603	0.488
9	0.623	0.539
10	0.608	0.495
11	0.560	0.587

表 5 意図ありと意図なしの 2 群の代表値の検定
Table 5 Results of the Mann-Whitney test of execution intention.

	対策実行意図（度数）	得点平均	検定値
理解度	意図あり（541）	2.13	0.02
	意図なし（1,713）	2.04	
スキル 1	意図あり（541）	24.39	0.93
	意図なし（1,713）	24.36	
スキル 2	意図あり（541）	−0.76	0.43
	意図なし（1,713）	−0.79	

されているため，第 2 主成分得点が高いと，ソーシャルメディアを利用するスキルが高いと評価する．第 2 主成分得点の参加者全体の平均は，−0.78 であった．

6.3.3 対策実行意図に与える情報技術の知識の影響

対策実行意図への情報技術の知識の影響に関する分析結果を**表 5** に示す．

理解度は，対策実行意図の「意図あり」と「意図なし」において，「意図あり」の方が平均の得点が高かった．さらに，異なる 2 群の代表値の検定である U 検定（Mann-Whitney 検定）においても有意の差がある（検定値：0.02 < 有意水準：0.05）．これにより，理解度が対策実行意図において影響していることが統計的に示唆された．

一方，IT スキルは，対策実行意図の「意図あり」と「意図なし」において，「意図あり」の方が平均の得点が高かった．しかし，異なる 2 群の代表値の検定である U 検定（Mann-Whitney 検定）において，スキル 1（検定値：0.93 > 有意水準：0.05）とスキル 2（検定値：0.43 > 有意水準：0.05）ともに有意の差がなかった．これにより，IT スキルが対策実行意図において影響しているといえないことが統計的に示唆された．

6.3.4 防護動機理論・集合的防護動機理論の対処行動を規定する要因に与える情報技術の知識の影響

理解度が実行意図に影響していることが示唆されたことから，防護動機理論・集合的防護動機理論の対処行動を規定

表 6 理解度得点の 6 群の代表値の検定
Table 6 Result of Kruskal-Wallis test about six different groups of understanding level.

規定要因項目	検定値
深刻さ認知	0.00
生起確率認知	0.00
効果性認知	0.00
コスト認知	0.38
実行能力認知	0.00
責任認知	0.00
実行者割合認知	0.01
規範認知	0.00

する各要因においても影響しているかを分析する．異なる理解度得点の 6 群における防護動機理論・集合的防護動機理論の対処行動を規定する各要因の差を検定（Kruskal-Wallis 検定）すると，コスト認知以外の要因に有意の差があることから（コスト認知以外の項目の検定値 < 有意水準：0.05），理解度がコスト認知以外の規定要因に影響していることが統計的に示唆された（**表 6**）．

7. 考察

ボット対策を例としたアンケート調査により，利用者へのボット対策推進を促す説得メッセージに関する利用者の態度変容の影響を分析した結果から，注意喚起における説得メッセージのあり方について考察する．

ボット対策の対策実行意図に影響を与える防護動機理論と集合的防護動機理論の対処行動を規定する要因を分析した結果から，防護動機理論よりも集合的防護動機理論の方が説明力が高いことが明らかになった．これにより，説得メッセージには，集団的な対処行動を促す脅威をアピールすることが効果的であると示唆された．その中でも，責任認知と実行者割合認知が対策実行意図に影響していることから，たとえば，説得メッセージの受信者自身がボットによる脅威の発生にかかわっており，ボット対策の実行に責任があることを理解させる内容や，多くの利用者がボット対策を実施すると感じさせる内容を説得メッセージに記載することが効果的であると考えられる．また，効果性認知が対策実行意図への影響が高いことから，説得メッセージに対処行動によって脅威を防止・低減できることを利用者に分かりやすく知らせることが効果的であると考えられる．

ボット対策の対策実行意図の「あり」「なし」の 2 群において，ボットに関する理解度が影響していることが明らかになった．さらに，理解度が情報スキルにおける判断と同様に，態度変容のプロセスにおける「同意するかどうかの判断」（図 1）に関連しており，防護動機理論・集合的防護動機理論の対処行動を規定する要因のうち，コスト認知以外のすべてに影響していることが明らかになった．そのため，コスト認知以外の規定要因では，ボットに関して理解することで，対策実行意図が「あり」となることが示唆された．コスト認知はボットに関して理解しても，対策実行の行為自体が利用者にコストとして感じられたために理解度が影響していないという結果になったと推測される．これらから，ボット対策では，説得メッセージの脅威アピールとして，利用者に理解させることが効果的であることが示唆された．たとえば，ボットに感染したコンピュータの利用者に，ボットの脅威やボット対策の意義を分かりやすく説明することや，説得メッセージに補足説明や補足説明先リンクを加えることが効果的であると考えられる．また，上記で述べたように，防護動機理論・集合的防護動機理論の対処行動を規定する要因において，効果性認知が実行意図に強い影響を与えていることから，特にボット対策実施の効果を分かりやすく知らせることが有効であると考えられる．

現在も新しい手法の攻撃が出現しており，それらの攻撃は巧妙化，複雑化しているため，ボット対策では利用者に新たな攻撃の脅威や対策の有効性を伝えることが難しくなっている．そのため，新たな攻撃でも利用者が理解しやすいように，情報セキュリティの専門家が攻撃の脅威や対策の有効性を要約したり，類似となる例を示したりし，分かりやすく解説する活動が重要になってくると考えられる．

今回の調査では，情報技術の知識の IT スキルが対策実行意図に影響していなかったが，ボット対策を理解するためのスキル（たとえば，ネットワークやソフトウェアの知識）を問う項目であれば実行意図に影響を与えたかもしれない．

8. おわりに

本論文では，ボット対策における実行者割合の向上を目的として，社会心理学のアプローチから防護動機理論を援用して，脅威アピールによる対処行動を促す規定要因を明らかにし，注意喚起の説得メッセージのあり方を提示した．防護動機理論では，ボット対策のような情報社会の事象において，情報技術の知識として理解度が影響していることを明らかにした．ただし，本分析の結果は一般的なインターネット利用者を対象としたものにはなっていないことに注意が必要である．また，AIDS 教育に関する HIV 対処行動意図の研究 [18] では，修正防護動機理論 [10] の報酬認知（未対応の方がメリットが大きい）が用いられている．本研究では報酬認知の要因として駆除ツール実行によるマシントラブル回避が考えられるため，報酬認知の要因を含むアンケート調査・再分析をし，さらにモデルの精緻化を図りたい．

情報社会では，技術の発展が速く，それらの技術を利用したアプリケーションやサービスが日々新たに創出されている．同時に，それらのアプリケーションやサービスに関連した攻撃が発生しており，注意喚起を理解するための新

たな情報技術の知識が必要となるため，利用者への継続的な情報技術の教育や情報提供が重要である．また，情報モラル教育では，情報社会の多様で変化する情報モラルにおいて，判断する場面ごとの教材や指導に限界があるとし，新たな場面においても正しい行動がとれるような考え方や態度を育成する研究が始まっている [19]．情報セキュリティ対策においても同様の研究が必要であり，本論文に関しては利用者が新たな場面や類似する場面で対処可能になるため，“説得メッセージ” による “態度変容” のプロセスにおける「関連する情報の想起」（図 1）に関する研究を始めることにより，さらに効果的な説得メッセージのあり方を提示可能となる．

謝辞 本研究に，貴重なご意見をいただきました，竹村俊彦助教（関西大学），ならびにデータを提供していただきました，独立行政法人情報処理推進機構の皆様に，謹んで感謝の意を表する．

参考文献

[1] 小松文子，赤井健一郎，上田昌史，松本 勉：情報セキュリティ対策は社会的ジレンマか？—ボットネット対策への適用，電子情報通信学会技術研究報告 IEICE Technical Report，Vol.109, No.113, pp.273–280 (2009).
[2] DAMBALLA: Top 10 Botnet Threat Report - 2010 (2011.02), available from ⟨http://www.damballa.com/downloads/r_pubs/Damballa_2010_Top_10_Botnets_Report.pdf⟩.
[3] 独立行政法人情報処理推進機構：情報セキュリティに関する脅威に対する意識調査 (2009)，入手先 ⟨http://www.ipa.go.jp/security/fy20/reports/ishiki02/documents/200802_ishiki.pdf⟩.
[4] サイバークリーンセンター（CCC）：平成 19 年度サイバークリーンセンター（CCC）活動報告 (2008)，入手先 ⟨https://www.ccc.go.jp/report/h19ccc_report.pdf⟩.
[5] サイバークリーンセンター（CCC）：ボットの脅威との戦い—サイバークリーンセンター（CCC）活動レポート (2010)，入手先 ⟨https://www.ccc.go.jp/report/h21ccc_report.pdf⟩.
[6] 内閣府：平成 20 年版国民生活白書 (2008).
[7] 内閣府：消費者の意思決定行動に係る経済実験の実施及び分析調査報告書 (2008).
[8] 深田博己（編著）：説得心理学ハンドブック，北大路書房 (2004).
[9] Rogers, R.W.: A protection motivation theory of fear appeals and attitude change, *Jorunal of Psychology*, Vol.91, pp.93–114 (1975).
[10] 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).
[11] 戸塚結氏，深田博己：脅威アピール説得における集合的防護動機モデルの検討，社会心理学研究，Vol.44, pp.51–61 (2005).
[12] 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).
[13] 猪俣敦夫，東 結香，上田昌史，小松文子，藤川和利，砂原秀樹：防護動機理論を基づく情報セキュリティリスク解明モデルの高等学校教育への実践，情報処理学会研究報告，Vol.2010-CSEC-49, No.12 (2010).
[14] 文部科学省：中等教育資料（特集 情報モラルの育成），Vol.57, No1 (2008).
[15] 村井 実：道徳は教えられるか／道徳教育の倫理，小学館 (1987).
[16] 松田稔樹：情報モラルをどう捉えて教育するのか，日本教育工学会第 15 回全国大会講演論文集，pp.17–18 (1999).
[17] 玉田和恵，松田稔樹：「3 種の知識」による情報モラル指導法の開発，日本教育工学会論文誌，Vol.28, No.2, pp.79–88 (2004).
[18] 高木雪子：HIV 対処行動意図に及ぼす AIDS 教育の影響過程，広島大学大学院教育学研究科紀要第三部第 55 号，pp.267–276 (2006).
[19] 梅田恭子，江島徹朗，野崎浩成：情報技術の知識の高低を考慮した情報モラル指導方略の提案，愛知県立大学研究報告，No.59, pp.175–179 (2010).

島 成佳 （正会員）

1997 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．1997 年日本電気株式会社入社．インターネットセキュリティおよび通信アーキテクチャの研究開発に従事．2007 年より電気通信大学大学院情報システム学研究科に在籍．2010 年より（独）情報処理推進機構．修士（情報科学）．

小松 文子 （正会員）

日本女子大学卒業，NEC にて，汎用機 OS 開発，ネットワークプロトコル国際標準化活動を経て，JEIDA（現 JEITA）にてセキュリティ評価認証制度の導入に取り組む．その後，PKI に関連した製品開発・サービス開発・技術支援を経て，中央研究所にて，効果的なセキュリティ対策についての研究に従事．2005 年 NEC 上席システムズアーキテクトに認定．2008 年より（独）情報処理推進機構情報セキュリティ分析ラボラトリーラボラトリー長．博士（情報学）．おもな著書に『PKI ハンドブック』（ソフトリサーチセンター）．

高木 大資

2008 年明治学院大学大学院心理学研究科修士課程修了．地理情報システム（GIS）の郵送調査データへの適用に関心があり，地域住民の社会関係資本が地域内の犯罪発生に与える影響を，空間統計学によって説明・予測することに関心がある．2008 年 4 月より東京大学大学院人文社会系研究科博士課程に在籍．心理学修士（明治学院大学）．

北村 浩

1990 年名古屋大学大学院理学研究科物理専攻博士課程後期課程途中退学．同年日本電気株式会社入社．通信プロトコルの研究開発に従事．現在日本電気株式会社サービスプラットフォーム研究所主幹研究員．2004 年より電気通信大学大学院情報システム学研究科客員助教授．2011 年より電気通信大学大学院情報システム学研究科客員教授．インターネットの通信アーキテクチャおよび通信プロトコルの研究開発および標準化提案活動に従事．工学博士．電子情報通信学会，IEEE 各会員．