情報処理学会論文誌　Vol. 52　No. 9　2526–2536 (Sep. 2011)

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

小松文子[†1,†2]　高木大資[†3]
吉開範章[†4]　松本勉[†5]

情報セキュリティの分野において，個人が対策する意思があっても，対策を実行しないなどの現象が知られており，個人の振舞いや意思決定などについての研究が始まっている．本論文では，効果的な情報セキュリティ対策推進に役立てるために，社会心理学における説得の心理学の研究を援用し，個人が，説得メッセージによって態度変容するための要因を調査，分析した．特に，質問紙調査だけでなく，実験も組み合わせることにより，個人の振舞いの違いを調査した．質問紙調査で回答された対策実行意図と，実際の実験の実行が異なることが分かった．そして，質問紙調査の実行意図と実験での実際の実行との振舞いが異なるグループについては，メディアスキルが有意に差があることを統計的に明らかにした．

Survey and Experiment on Promotion of Information Security Measurements by Persuasive Message

Ayako Komatsu,[†1,†2] Daisuke Takagi,[†3]
Noriaki Yoshikai[†4] and Tsutomu Matsumoto[†5]

The research of individual behavior and the decision making, etc. starts in the field of the information security. For effective information security measures promotion, the research of the psychology of the persuasion in the social psychology was invoked, and in this thesis, the individual investigated, and analyzed the factor because of the attitude transformation by the persuasion message. Especially, the difference of individual behavior was investigated by combining not only the questionnaire investigation but also the experiments. It has been proven that the execution intention answered by the questionnaire investigation and an actual experiment is different. And, the media skill statistically clarified that there was intentionally a difference about the group with a different behavior with actual execution by the execution intention and the experiment on the questionnaire investigation.

1. はじめに

日本ネットワークセキュリティ協会が毎年報告している「個人情報漏えいインシデント調査」によれば，毎年の個人情報漏えいのインシデントは増え続け，その原因は，個人のミスや紛失，管理ミスなど，人間に起因するものが多い[3]．また，政府の国家情報セキュリティセンター（NISC）は，セキュアジャパン 2008[4] において，企業や組織におけるセキュリティ対策疲れを認めている．また，企業や組織に属さないネットワークユーザによる情報セキュリティ対策の例では，サイバークリーンセンター（CCC）によるボット対策事業が行われてきた．CCC では，ISP（インターネットサービスプロバイダ）を通してボットに感染した PC の利用者に対して，その感染の事実を知らせ，ボット駆除ツールを提供している．しかし，駆除ツールをダウンロードする割合は，32.4%[11] と低い．感染 PC の利用者が対策を実施しないことによる，ネットワーク全体の安全性の低下が懸念されている．このような背景から，情報セキュリティ対策についての新たなアプローチが始まっている．個人の振舞いや意思決定に注目した研究がその 1 つである．本論文では，情報セキュリティ対策を実施する個人の振舞いを調査分析し，特に説得の心理学における「説得コミュニケーションによる態度変容の既存研究」を援用し，効果的な情報セキュリティ対策推進のための要因を探求することを目的として質問紙調査と実験を実施，分析したので報告する．

本論文の構成は以下のとおりである．2 章で関連研究について述べ，3 章で解決すべき課題を述べ，4 章で質問紙調査と実験の概要，5 章で結果と分析を述べ，6 章で考察，7 章でまとめを述べる．

†1 横浜国立大学大学院環境情報学府情報メディア環境学専攻
Graduate School of Environment and Information Sciences, Yokohama National University
†2 独立行政法人情報処理推進機構
Security Economics Laboratory, Information-Technology Promotion Agency
†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
†4 日本大学理工学部数学科
Department of Mathematics, College of Science and Technology, Nihon University
†5 横浜国立大学大学院環境情報研究院
Research Institute of Environment and Information Sciences, Yokohama National University

2. 関 連 研 究

2.1 社会的ジレンマ状況における個人の振舞い，意思決定

個人の振舞いや意思決定と社会との関連についての研究には，情報セキュリティ対策の状況を，個人の合理性と社会の最適性の乖離である社会的ジレンマ状況であると想定した質問紙による実証研究の報告がある[6]．この報告では，実行意図はあるものの，実際の状況は，CCC の対策ツールダウンロード率にみられるように低く，両者にギャップが存在することが指摘されている．また，社会的ジレンマ状況を表す 4 つの認知要素である自己への危機感，社会への危機感，無効感，コスト感[12] のうち，実行意図に最も影響をあたえたのは，自己への危機感であったという分析結果を報告している．

2.2 説得メッセージによる態度変容

対策実行意図が，自己への危機感に最も影響するという既存研究の結果は，対策推進のメッセージである注意喚起メッセージに危機感をあおるような情報を含めるとよい，ということである．このような，ある態度を変えるために，どのようなメッセージを送ることが効果的かについての研究は，社会心理学の「説得の心理学」の領域で行われている．ここで「説得」とは，「送り手が，おもに言語的コミュニケーションを用いて，非強制的なコンテキストの中で，納得させながら受けての態度や行動を意図する方向に変化させようとする社会的影響行為あるいは，社会的影響過程である」[17] と定義される．

2.2.1 防護動機理論

説得の心理学の領域で，危機感を喚起する理論に，Rogers による，脅威アピールによる「防護動機理論」（以降，PMT と呼ぶ：Protection Motivation Theory）[1),5)] がある．防護動機理論では，個人の態度変容の規定要因として，与えられたメッセージの内容による「深刻さ」，「生起確率」，「コスト」などの個人の認知がマイナス要因として，「効果」，「自己の能力」がプラス要因として影響するとされるモデルである．さらに，防護動機理論をふまえて，集団における個人の存在を考慮した場合では，戸塚らにより，集団と関連する要因として，「責任」，「実行者割合」や「規範」などの認知を加えて態度変容を規定することを実証した研究がなされている[7]．

PMT を情報セキュリティ教育へ適用した例では，高脅威メッセージは，逆に対処の率を下げることなどを示した実証研究[8] や，屋内の無線 LAN におけるセキュリティ脅威についての個人の意識について[10] モデルを適用した例が報告されている．このように，リスク下における個人の態度変容は，その現象やおかれた個人の状況によって，異なる結果となることが知られている．

2.2.2 精緻化見込みモデル

説得メッセージを与えられた際に，個人の状況による態度変容をモデル化したもののうち，実証的に説明力が高いとされているのが，Petty らの精緻化見込みモデル（以降 ELM と呼ぶ：Elaborative Likelihood Model）である[2),⋆1]．ELM では，説得メッセージを個人が処理し，態度変容を起こすルートとして 2 つあると定義する．説得メッセージの内容を吟味し，理解し論理的に対処行動をとる場合の「中心ルート」と，メッセージを与えられた個人に内容を理解する能力が不足している場合は，メッセージの送り手の信頼の程度などメッセージの内容に直接関係しない要因に影響される「周辺ルート」の 2 種類のルートである．周辺ルートで態度変容をした人間は，その態度は比較的一時的で，他の情報に影響されやすい．一方で中心ルートで態度変容した場合には，対処行動をとるかとらないかにかかわらずその態度は比較的持続的である[13]．ELM を適用した研究のなかには，リスク下の個人の状況を対象とするといった情報セキュリティに類似した状況で，鳥インフルエンザのリスクの現象に適用し，脅威がいかに影響するかを新聞などのメディアから抽出し，その態度変容のモデルを構成した既存研究がある[9]．しかし，これは，個人の状況に与える不安要因を新聞から抽出しモデルに適合させたもので，実際に個人の認知の状況を調査し実証をしたものではない．

3. 課 題 設 定

これまで述べた説得メッセージによる態度変容の理論やモデルは，CCC のボット対策事業における注意喚起メールによってボット駆除を要請する状況に適用できると考える．この事業は，CCC が ISP の協力を経て，ISP がそのユーザであるネットワーク利用者に対して，PC がボットウイルスに感染しているかを検知し，CCC に代わって，ボットウイルスに関する説明，ボット感染の事実と，感染除去方法であるボット駆除ツールのダウンロード方法などを示す．これは，CCC または ISP が送り手となって，言語的コミュニケーションである注意喚起メールによって，自発的に，情報セキュリティ対策を実行するという態度や行動を起こさせることを目的としているということができる．さらに，既存研究[6] で報告されている質問紙調査の結果による，態度変容への脅威の影響分析や，実行意図と実際の振舞いとのギャップを分析するには，注意喚起メールを提示されたときの実際の対策を迫られる人

⋆1 付録 B に精緻化見込みモデルの図を示したので参照されたい．

間の振舞いを観察する必要があると考える．そのうえで，実際の行動にいたる態度変容を起こす認知要素を明らかにすることは，注意喚起メールの満たすべき要件が明らかになり，対策推進に有効であると考え，質問紙調査による実行意図の調査と実験を連携して実施することとする．以下に，本調査と実験で解決すべき課題をあげる．

- 対策を実施する意図があるにもかかわらず，対策を実施しない個人のセキュリティ脅威への認知の状況や IT スキル，被害の経験ありなしなどの意図と行動との関係はどのような状況であるか．
- どのように説得メッセージを発信すれば態度変容を起こすことができるか．どのような要素を注意喚起メールに含めることが効果的か．

本論文では，これらの課題に対して，すでに述べた PMT，ELM を適用し解決をすすめていくとする．まず，ELM によれば，注意喚起メールの文章の内容を理解可能な能力を保持する者，保持しない者は，それぞれ態度変容を引き起こす情報が異なる．したがって，参加者の理解能力を持つ・持たないを情報関連メディアのスキルや関与の程度によって分類し，態度変容の結果を観察する．次に中心ルートを経由した態度変容は，持続的であり，周辺ルートを経由した態度変容は，変わりやすい．したがって，態度変容の持続性を質問紙調査での実行意図と実験での実行との関連を分析し，明らかにする．

4. 質問紙調査と実験の設計

質問紙調査と実験の全体の流れを**図 1** に示す．質問紙調査では，CCC の注意喚起のプロセスと同等に，まず，ボットウイルスに関する説明文，次に注意喚起メールの内容を提示し感染していることを知らせ，駆除ツールダウンロード方法を示したのちに，対策意図の有無を質問する．これらの回答者のなかから，実験参加者を募り実験を実施した．

4.1 質問紙調査

質問項目は，PMT，ELM で規定された認知要素，ELM で利用する個人の状況を表す IT メディアスキルや関与度を測る情報を得ることを目的としている．また，正確な意図を聞き出すことを目的とするため，本来のアンケート趣旨は伏せたうえで，質問内容も多様に分散させ，アンケートからも趣旨を類推させないようにする．質問項目の詳細は，付録を参照されたい．

まず，実行意図と，PMT の質問項目（**表 1**）の認知要素の関連を**図 2** に示す．

次に，ELM の質問項目では，中心ルート要因として，メッセージの説得力，理解度を，周辺ルートの要因として，ISP への信頼や送り手（CCC）への信頼を設定した（**表 2**）．ま

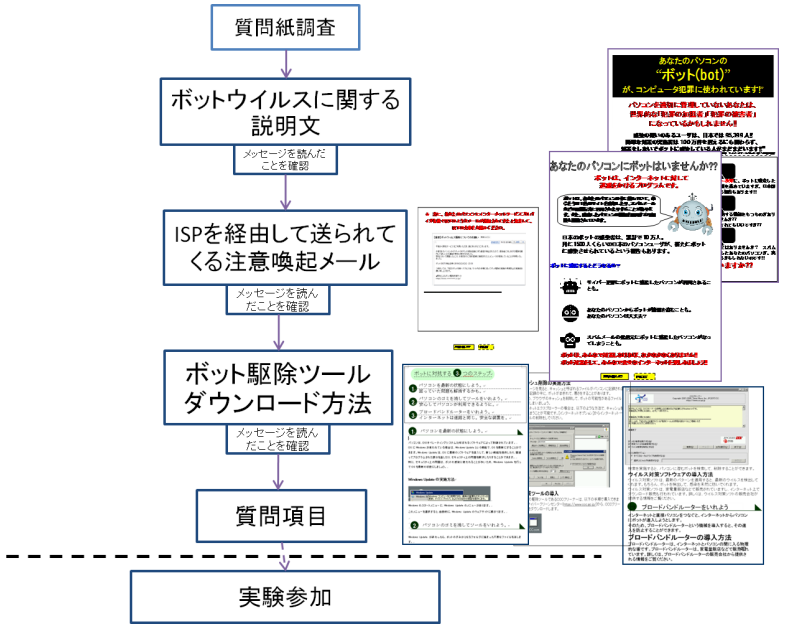


図 1　質問紙調査と実験
Fig. 1　Flow of questionnaire and experimentation.

表 1　防護動機理論，集合的防護動機理論における認知の要素
Table 1　Cognitive elements of PMT.

認知要素	説明（以下を認知している）
深刻さ認知	ボットの脅威が自分の PC に及ぼす被害の深刻さ
生起確率認知	ボットウイルスが PC に感染する可能性
効果性認知	示された対策がウイルスを防止することに効果がある
コスト認知	示された対策をすることの手間やリスクがある
実行能力認知	自分がその対策をすることは技術的・知識的に困難である
責任認知　*	自分には，対策を実行する責任がある（社会に対して）
実行割合認知　*	示された対策を他の多くの人が実施している
規範認知　*	自分が実施することを他人が期待していること
ジレンマ認知　*	他人の対策と自分の対策が相克すること

認知要素に*が付与されたものは，集合的防護動機理論で定義された要素

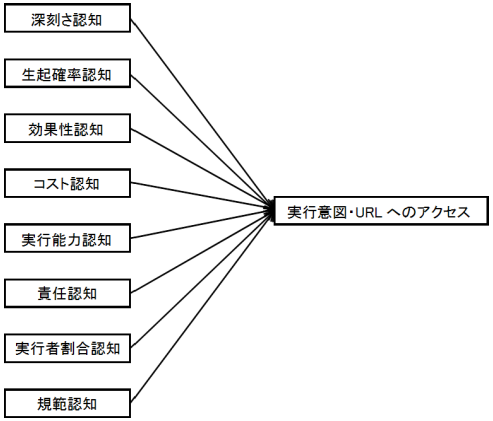


図 2　防護動機理論の認知要素と実行意図への関連
Fig. 2　PMT factors on implementation intention.

表 2　精緻化見込みモデルの認知要素
Table 2　Cognitive elements of ELM.

認知要素	説明（以下を認知している）
メッセージの説得力	示されたメッセージが説得力があると思われること
メッセージの理解度	示されたメッセージを理解しているかの程度
送り手への信頼	メッセージの送り手を信頼しているか（自分に対する相手の行動意図が期待できること）本実験の場合は，CCC
ISP への信頼	契約している ISP を信頼しているか．

た，これらの要因が，IT メディアの熟練度（スキル）や，ボットウイルスについての関与・知識の度合いによって，異なる影響を受けることを想定した（**図 3** 参照）．

既存研究との比較のために，社会的ジレンマ状況の認知要素[12]，アンケートの目的を類推させないように一般的信頼感などについて質問を準備した．ここで，一般的信頼感とは，社会心理学で使用されることが多い 3 項目の信頼感を図る尺度であるが，本来の目的を類推させないために含めたもので，分析には使用していない．

4.2 実　　験

実験システムを構築し，前述した質問紙調査の回答者のなかから，実験参加者を 100 名募り，心理学実験の実施を計画した．実験参加者は，質問紙調査の回答で，これまでウイルス経験があるもの，ないものをほぼ均等になるように召集する．本来の目的を知らせないために，参加者には，実験の名称を「集合知を使ったゲーム環境下における心理実験」と伝える．実験は，仮想ゲームを実行する中でウイルス感染を知らせ，個人の意思によって対策実行させる（実行しない）ということに疑問を持つことなく実施させるため，もっともらしい実験名や，ウイルスの検出を知らせるメッセージも本物らしく設計する．なお，実験にあたっては，参加者に真実を知らせないで行うことなど，主催者としての責務について，（社）日本心理学会会員倫理綱領[15] に基づき運営する．実験室は，外部からの影響を受けない消音室を使用する．3 つの実験室を同時に使用し，それぞれの実験室には，PC が接続されており，これらの PC は，それぞれ監視用 PC にその動きがミラーリングされる．実験の設備構成の概要を**図 4** に，参加者の画面，実験室などの様子を**図 5** に示す．

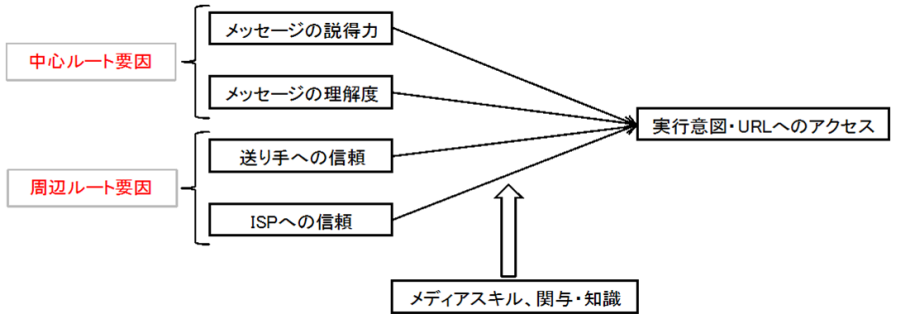


図 3　精緻化見込みモデルの認知要素と 2 つのルートの関連
Fig. 3　IT skills and involvement/knowledge effect on intention to implementation.

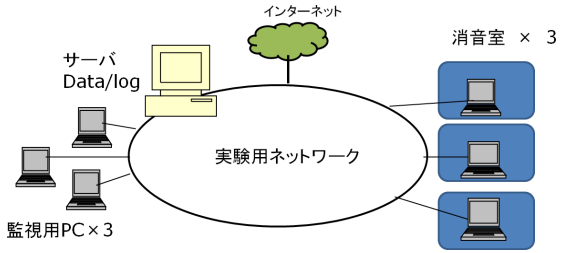


図 4　実験設備構成の概要
Fig. 4　Outline of experiment equipment.

4.2.1　実験シナリオの主な流れ

実験参加者は，以下のような流れの実験に参加することとした．紙面の関係で本論文に関連する部分のみ紹介する．

① 事前説明
実験の運営係によって，実験室（消音室）の PC を利用し，本実験用に開発したソフトを用いた仮想作業である集合知を集めて多数決できまっていくゲームを行うことを説明する．その後，実験室へ案内する．

② 実験室内の PC の画面は，4 つに分割され，それぞれは，他の参加者（さくらである）の回答の様子，ゲームの説明，他参加者とのチャットが可能な画面，問題表示，回答選択画面が現れる（図 5 の左下図参照）．

③ 被験者にブラウザの余計な操作をさせないために，ブラウザは全画面表示（メニュー表示なし）にする．

④ 最初に実験の練習として 5 分程度のトレーニングを行う．

⑤ 実験が開始されると，1 問あたりの回答可能時間を表示し，時間内での回答を意識させる．

⑥ ゲーム開始 30 分で，未知のウイルスに感染した可能性があることをポップアップメッセージによって告知する．参加者がとる対策のための操作は質問紙調査で示した対策方法と同様である．

⑦ 対策をとらない回答者には，繰り返し警告を表示する．最後まで対応を実施しない場合でも，45 分後に終了する．

⑧ 事後説明，インタビュー：実験の本来の目的が推測されていないかを確認するとともに，倫理規定[15] に基づき，実験目的などの事前の虚偽の説明に対する謝罪し，謝金を支払う．

図 5　実験設備と参加者 PC 画面
Fig. 5　Experiment equipment and participants' PC snap shot.

5.　結果と分析

5.1　質問紙調査と実験の結果

株式会社クロス・マーケティング[⋆1]の保有する Web アンケート環境およびモニタ会員を用いてインターネット調査によって行った．インターネット調査を用いた理由としては，本調査のテーマがボットウィルスであり，インターネットを利用している人々を効率的に抽出する必要があったためである．調査期間は 2010 年 3 月 9 日〜3 月 10 日で，総回答数は 2,254 名であった．**表 3** に本調査における性別および年齢階層別の回答者数を示す．

実験は，質問紙調査の回答者の中から希望をつのり，2010 年 4 月 17 日〜5 月 29 日の期間に，1 回あたり 3 名の参加者に対して計 35 回行った．当日のキャンセル者，無断欠席者が 5 名発生したが，最終的に実験参加者 100 名を確保できた．事後のインタビューでは，ほとんどが情報セキュリティの実験であることに気づいていないことが確認された．この意味では実験は成功したといえる．実行意図について，質問紙調査と実験の結果を**表 4** に示す．ここで，「意図あり・なし」は付録質問事項の PMT に関連した質問事項の対策実行意図（4 件法）の問いにおいて「実行する」，「どちらかといえば実行する」と回答した参加者

表 3　調査対象者の年齢・男女構成
Table 3　Gender and age composition.

	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	1144	1110

⋆1 株式会社クロス・マーケティング：現在約 150 万名のモニタ会員を保有している．

表 4　質問紙調査での実行意図と実験での実行結果
Table 4　Implementation intention in the questionnaire and actual implementation in the experiment.

質問紙調査(人)			実験(人)	変更タイプ
意図あり	34	対策実行	13	1
		対策不実行	21	2
意図なし	59	対策実行	24	3
		対策不実行	35	4
全体	93		93	

である．実験の欄には，実際に対策を実行したか，しなかったか（不実行）の人数を示している．実験参加者 100 名のうち，事後のインタビューで自分の PC ではないから対策を実行しなかったと答えた 7 名を除き 93 名を有効サンプルとした．質問紙調査では，意図ありと回答したものが 34 名，このうち，対策を実行したものは，13 名で，対策を実施しないものは，21 名であった．意図なしと回答した 59 名のうち，対策実行したものは 24 名，実行しなかったものは 35 名であった．質問紙調査の実行意図がかならずしも実験の結果と整合しない，という結果となった．

5.2　質問紙調査と実験の結果分析

質問紙調査の結果に対し，まず，実行意図に対する PMT や ELM に関連した認知要素が実行意図にいかに影響しているか明らかにするために，ロジスティック回帰分析を行った．ロジスティック回帰分析は，従属変数が有無などの 2 値の場合の回帰分析に用いられる．なお，実験結果との比較のために，質問紙調査における統計分析の対象サンプルも実験参加者 93 名を対象としている．独立変数である各認知要素は，付録 A(1) にある質問項目の回答を，それぞれ 1 から 4 まで数値化し，ネガティブポジティブに並べなおし（反転して）使用する．対策実行意図も 4 件法であるが，その回答を 2 値にするため，あてはまる，どちらかといえばあてはまるを 1，あてはまらない，どちらかといえばあてはまらないを 0 とした．集団的 PMT の認知要素の分析では「効果性認知」が有意に実行意図に影響していることが示された（**表 5**）．

次に，ELM の中心ルートの情報である「文章の説得力」，「理解度」と周辺ルートの情報である「送り手への信頼」や，「ISP への信頼」を独立変数とし，実行意図へ影響するかを分析した．これらの認知要素も，PMT の認知要素の分析と同様に，付録 A(3) にある質問項目を 1 から 4 まで数値化し反転した．理解度は，付録 A(2) の 5 問の問いの正答数（1〜5）とした．さらに，回答者の状況を表す属性であるメディアスキルの高低，関与の有無の違いによる認知要素と実行意図，実行への影響を分析した．IT メディアスキルの高低は付録 A 質問項目の (4) メディアスキルを算出するための 11 項目，(5) 関与度を算出するための項目 3 項の質問結果に対して，主成分分析を実施し，第 1 主成分得点の中央値を境界とし，高低群に分割した．結果をみると，まずメディアスキルの低い群については，周辺ルートである送り手への信頼が実行意図へ有意に影響していることを示している（**表 7** の質問紙調査の欄を参照）関与度の高低による影響には，有意な差を見つけることはできなかった．

表 5　防護動機理論の認知要素への実行意図の影響
Table 5　Influence of implementation intention on the cognitive elements of PMT.
（ロジスティック回帰分析）n = 93

従属変数：実行意図（1：あり，0：なし）	
認知要素	回帰係数
深刻さ認知	0.4309
生起確率	-0.0176
効果性認知	1.3810**
実行能力認知	-0.4244
コスト認知	-0.0663
責任認知	0.2312
実行者割合認知	0.5003
規範認知	-0.3471
ジレンマ認知	0.4133
定数項	-5.8851**
*:P<.1,**:P<.05,***:P<.01	Pseudo R2=0.2257

実験参加者全員に対して，実験での実際の対策実行を従属変数とし，説得メッセージに対する参加者の認知要素の影響を分析した（**表 6** 参照）．結果は，質問紙調査では，送り手への信頼が実行意図に有意に影響し，実験では，質問紙での理解度が実行意図に有意に影響したことが示された．ただし，決定係数が低いため結果を採用するには他の認知要素との関連も考慮する必要がある．

5.3　実験実行意図有無の分析

次に，メディアスキルの高低，関与度の程度の違いによって，ELM の認知要素が質問紙調査の実行意図，実験での対策実施に影響しているかを，統計的な有意性によって比較した．実験では，メディアスキル低群の実験において，文章の説得力が最も影響し，次に送り

表 6　質問紙調査と実験の意図，実行の標準化回帰係数の有意比較
Table 6　Comparison between implementation of regression coefficient and of intentions and in the questionnaire and experiment.

（実験参加者全員 n = 93）

	質問紙調査	実験
送り手への信頼	-1.0238**	-0.3652
ISP への信頼	-0.2953	00.0530
文章の説得力	-0.5270	0.2914
理解度	-0.1542	0.5130*
Pseudo R2	0.2478	0.0583

*:P<.1,**:P<.05,***:P<.01

表 7　IT メディアスキル高低群の違いによる影響
Table 7　Influences due to differences in high/low groups for IT skills.

	メディアスキル高(n=46) 標準化回帰係数		メディアスキル低(n=47) 標準化回帰係数	
	質問紙調査	実験	質問紙調査	実験
送り手への信頼	1.2866	-0.7428	1.1887*	0.0074
ISP への信頼	-0.3776	-0.1986	0.2971	0.3504
文章の説得力	-0.3776	0.6415	1.5970*	0.0019
理解度	-0.4998	0.6081	0.5151	0.2574
Pseudo R2	0.2271	0.1287	0.4232	0.0276

*:P<.1,**:P<.05,***:P<.01

手への信頼という結果となった．しかし，IT メディアスキル高群では各変数の質問紙調査での実行意図，実験実行にそれぞれ有意な変数を見つけることはできなかった（表 7）．

また，関与度高低による，関与度低群で送り手への信頼が有意であったが，他に対策意図，実行へ有意な影響を持つ変数はなかった（**表 8**）．

5.4　意図と異なる実行を行う者についての分析

質問紙調査と実験での，意図と実行との相違について分析する．再び，表 3 を参照すると，変更タイプ欄のケース 2（意図あり，不実行）の 22 名，ケース 3（意図なし，実行）の 24 名が振舞いを変更した参加者（以降変更ありと呼ぶ）である．ケース 1，4 は意図と実行を変更しない（以降変更なし，と呼ぶ）．2.3 節で述べたように，ELM によれば，中心ルートでの態度変容の結果は，「比較的持続的で，抵抗があり，予測可能」であり，一方周辺ルートでの態度変容の結果は，「態度は比較的一時的で，影響されやすく，予測できない」と定義されている．そこで，中心ルート，周辺ルートに対する参加者の属性である，IT メディアスキルの高低，および関与度の程度，理解度の各属性に関し，変更あり，変更なしの参加者の相違を，マン・ホイットニーの U 検定（異なる 2 集団の代表値の検定）を利用して検証した．結果を表 7 に示す．変更ありのグループは，なしのグループに比較して明らかに，関与度，メディアスキルの平均値が高い．また，U 検定の結果も，意図と異なる実行を行う者は，意図と同じく実行する者と比較し，メディアスキル，理解度に有意な違いがあることが示された（**表 9**）．

なお，ELM の，説得メッセージの内容を精緻化，理解したうえで対処行動をとる中心ルー

表 8　関与度の高低による実行意図（質問紙）・実行（実験）への影響
Table 8　Influences on implementation intention due to in high/low level of involvement.

	関与度高群 (n=42) 標準化回帰係数		関与度低群 (n=51) 標準化回帰係数	
	質問紙調査	実験	質問紙調査	実験
送り手への信頼	0.8377	-0.9144	1.2312*	0.0620
ISP への信頼	-0.0662	0.3960	0.3913	-0.1638
文章の説得力	0.6408	0.5456	0.5019	0.0911
理解度	-0.4540	0.7921	0.1444	0.3323
Pseudo R2	0.2103	0.1459	0.2958	0.0284

表 9　意図と実行の違いと参加者の状況の U 検定
Table 9　U-test of the difference between intention and implementation and the circumstances of participants.

	平均値： 上：変更なし(48) 下：変更あり(45)	検定統計量 U	P 値
関与度	-0.2701	876	0.0860*
	0.2880		
メディアスキル	-0.4826	784	0.0228**
	0.5148		
理解度	2.0201	760	0.0098***
	2.7111		

*:P<.1,**:P<.05,***:P<.01

トプロセスの中で，PMT で規定されている要因が，評価処理されると仮定し，態度変容が一貫している変更なしの群について，これらの要因が影響しているかを分析したが，結果に有意な要因を見い出すことはできなかった．

6. 考　　察

情報セキュリティ対策におけるボットネット対策を例として，個人へ対策推進を促す説得メッセージの影響について，質問紙調査と実験環境での実験を実施した．これらの結果をもとに，セキュリティ対策推進の説得メッセージのありかたについて考察する．

6.1 質問紙調査の結果から

PMT に関連した分析では，実行意図へ統計的に有意に影響を与える認知要素は，既存研究[6] で示されていた恐怖心による脅威に対応する「深刻度認知」ではなく，そのセキュリティ対策の「効果性認知」であった．ELM に関連した分析では，メディアスキルの低い群では，説得メッセージの処理において，メッセージの内容を十分吟味して態度変容を起こす中心ルートの情報である「文章の説得力」と，周辺ルートの情報である「送り手への信頼」によって，実行意図を形成していることが示された．これらにより，実行意図を形成するために，対策推進が個人にどのような効果があるかを分かりやすく知らせるとともに，メディアスキルが低い群に対して，よく利用する信頼ある送り手からメールを送出することが必要である．また，これらの群が周辺ルートで処理することを想定すれば，メッセージの正確性よりも，直観的な納得感が得られる情報を提示することが効果的であると考えられる．

6.2 実験と質問紙調査との関係分析からの考察

認知要素のうち，実験での対策実行に有意に影響したのは，「理解度」であった．実験参加者は，情報セキュリティとは別の作業である「集合知を使った心理ゲーム」を終了させることが求められているため，短時間に意思決定をする必要がある．一方，質問紙調査では，喚起メッセージや対策方法などを読むことに時間の制約がない．このため，実験では，より直観的に対策をとることが想定される．しかし，理解度が対策実行に有意であったという点は，意図だけでなく，実行に移るには，ELM における中心ルートで形成される説得メッセージの「理解」が必要であることを示すのではないかと考える．次に，質問紙調査での実行意図と実験での実行が異なる状況について，回答と実行が異なる（変更あり）群と変更なし群の検定でメディアスキルに有意に差があることが明らかになった．ELM による，中心ルートの要因であるメディアスキルの高い群は意図を変更せず，低い群は意図を変更しやすいという定義を説明する結果は得られず，逆に，メディアスキルが高い群は，実際の実験行動では，意図とは異なる行動をとり，低い群は，意図と整合した行動をとる．これは，メディアスキルが高い群は，実験における実際の環境からの情報も使い行動を起こすのではないか，と考えられ，またメディアスキルが低い群は，そのような情報から行動することはない，のではないかと考える．

7. 今後の課題

情報セキュリティ対策推進の要因を探求するために，今後は，以下に述べる課題に取り組んでいく必要があると考える．

(1) メディアスキルが低い群に対しての対策推進要因
さらに詳細な認知要素の影響を分析していくことが必要と考える．特に，送り手への信頼感は，多様な意味を持つ可能性があるため，今後詳細に検討すべきと考える．

(2) 実施意図と実行について経験などの関与度の分析
今回の実験では，ウイルスへの経験などの関与度が対策実行に影響しているという結果を得られなかった．一般的には被害にあった経験を持つと，その後は防御動機が働くと考えられる．しかし，既存研究[8] の脅威が高くなると逆に意図が低くなるという現象からも，経験によって被害を想定できると，逆に逃避し，実行しないという現象がある可能性がある．このような場合にどのように意図や実行を推進すべきかについて取り組む必要があると考える．

(3) 実験環境のモデル化
質問紙調査と実験を組み合わせた研究は，これまでほとんど行われていなかった．今回は心理学実験を参考として実施したが，実験自体のモデル化の試みや，効率の良い実験，分析手法についての研究も必要と考える．

8. おわりに

実際の個人の振舞いを観察するために，実際にネットワークを使用する状況を構築し，質問紙調査に続けて，これまで情報セキュリティ分野では，行われることが少ない心理実験を行い，いくつかの新たな知見が得られた．すなわち，情報セキュリティ対策実施を要請する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，メディアスキルの低い群に対しては，周辺情報である送り手の信頼性などの情報を含めることや，直観的なメッセージにすることが効果的である．また，対処行動は一貫性が乏しいと考えられる．対策推進対象の属性に応じた情報セキュリティ対策を継続して実施する必要性が示唆された．

謝辞　本論文の調査は，（独）情報処理推進機構における「情報セキュリティ事象の社会科学的分析に関する調査」によって実施されたデータを使用している．納税者に感謝する．調査と実験に尽力していただいたエクセリードテクノロジー（株）の沼田博士に感謝する．本調査の社会心理学分野の調査に助言いただいた東京大学池田謙一教授に感謝する．

参　考　文　献

1) Rogers, R.W.: A protection motivation theory of fear appeals and attitude change, *Journal of Psychology*, Vol.91, pp.93–114 (1975).
2) Petty, R.E. and Cacioppo, J.T.: The Elaboration Likelihood Model of persuasion, *Advances in Experimental Social Psychology*, Vol.19 (1986).
3) NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ：2009 年情報セキュリティインシデントに関する調査報告書 (2010.9.2).
4) 内閣官房情報セキュリティセンター：セキュアジャパン 2008 (2008.6).
5) Rogers, R.W.: Cognitive and Physiological process in fear appeals and attitude change: A revised theory of protection motivation theory, *Social Psychophysiology*, pp.153–176, New York, Guilford (1983).
6) 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，pp.1711–1725, Vol.51, No.9 (2010).
7) 戸塚唯氏，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，実験社会心理学研究，Vol.44, pp.54–61 (2005).
8) 猪俣敦夫，東　結香，上田昌史，小松文子，藤川和利，砂原秀樹：防護動機理論に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 (2010.5).
9) 山崎瑞紀，吉川肇子，堀井秀之：社会事象に関する不安喚起モデル校正の試み—高病原性鳥インフルエンザを例として，社会技術研究論文集，Vol.2, pp.379–388 (2004.10).
10) Irene, W., Gek-Woo, T. and Low, R.: A Protection Motivation Theory Approach to Home Wireless Security, *Proc. International Conference on Information Systems* (*ICIS 2005*), Paper31 (2005).
11) サイバークリーンセンター（CCC）：サイバークリーンセンター活動実績，入手先⟨https://www.ccc.go.jp/report/201009/1009monthly.html⟩.
12) 海野道郎：誰が社会的ジレンマを定義するのか?，社会学研究，東北社会学研究，No.80, pp.1–28 (2006.6).
13) 神山貴弥：情報処理と説得：精査可能性モデル，説得心理学ハンドブック，深田博巳（編著），pp.418–455, 北大路書房 (2004.8).
14) 今井芳昭：依頼と説得の心理学，サイエンス社 (2006.9).
15)（社）日本心理学会：日本心理学会会員倫理綱領，入手先⟨http://www.psych.or.jp/members/rinri.html⟩.
16) 南風原朝和，市川伸一，下山晴彦（編）：心理学研究法入門，東京大学出版会 (2001.3).
17) 深田博巳：説得研究の基礎知識，説得心理学ハンドブック，深田博巳（編著），pp.2–44, 北大路書房 (2004.8).

付　　録

A.1　質問項目一覧

(1) 防護動機理論に関連した質問項目

・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)
・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」(「そう思う」〜「そう思わない」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」(「そう思う」〜「そう思わない」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」(「そう思う」〜「そう思わない」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」(「そう思う」〜「そう思わない」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」(「そう思う」〜「そう思わない」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」(「そう思う」〜「そう思わない」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」(「そう思う」〜「そう思わない」の 4 件法)
・規範認知

「自分がボットウィルス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」(「そう思う」～「そう思わない」の 4 件法)

・ジレンマ認知

「インターネット上の大多数の人がボットウイルスの駆除を行っていない」(「自分は対策を行ったほうがよいだろう」と「自分も対策を行わなくてもよいだろう」のいずれかを選択)

(2) 理解度

下記の文章理解度を問う 5 つのクイズに対する正答数（1～5 点）(「ボットウィルスに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ほか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」)

(3) 精緻化見込みモデルに関連した項目

・文章の説得力

「先ほどの文章には説得力がある」(「あてはまる」～「あてはまらない」の 4 件法)

・送り手への信頼

「先ほどのメールの送信者は信頼できる」(「あてはまる」～「あてはまらない」の 4 件法)

・ISP への信頼

「契約しているインターネットサービスプロバイダは信頼できる」(「そう思う」～「そう思わない」の 4 件法)

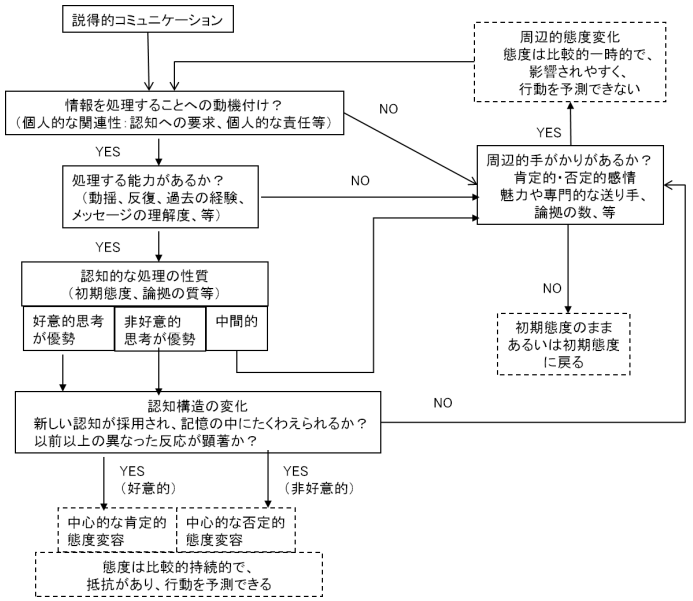
(4) メディアスキルを算出するための項目

「ワープロソフトで文章を作る」,「パソコンでメールのやりとりをする」,「ヤフー（Yahoo!）やグー（goo）などで必要な情報を見つける」,「自分の好きなホームページをお気に入りに入れる」,「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」,「インターネットや CD の百科事典を使って調べる」,「電子メールにファイルを添付して送信する」,「ホームページを作る」,「チャットによる会話」,「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」，と「Twitter の閲覧や書き込み」の 11 項目の第 1 主成分得点（それぞれ「できるし，よくする」～「何のことか分からない」の 4 件法)

(5) 関与度を算出するための項目

「今までにボットウィルスに関する報道を見たり聞いたりしたことがある」,「今までに，ボットウィルスについて人と話したことがある」,「ボットウィルスが何であるかは，この文章を読む前からすでに知っていた」(それぞれ「あてはまる」～「あてはまらない」の 4 件法)
(分析の際には，3 項目の第一主成分得点を使用)

A.2　精緻化見込みモデル



引用：THE ELABORATION LIKELIHOOD MODEL OF PERSIASION [2] を文献 13) を参考に邦訳

(平成 22 年 12 月 1 日受付)
(平成 23 年 6 月 3 日採録)

小松　文子（正会員）

日本女子大学卒業，NEC にて，汎用計算機の 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従事．NEC に復帰し，製品開発部門で PKI 関連の製品開発・サービス開発・技術支援を経て後，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取り組む．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．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．現在，東京大学大学院人文社会系研究科博士課程（心理学修士)・日本学術振興会特別研究員（DC2)．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．おもな論文・「他者の目撃記憶に関する情報と再認の遅延が他者への同調的な目撃記憶に及ぼす影響」社会心理学研究，24(3)，pp.189–199，「地域コミュニティによる犯罪抑制：地域内の社会関係資本および協力行動に焦点を当てて」社会心理学研究，26(1)．

吉開　範章

1979 年日本電信電話公社（現，NTT）電気通信研究所に入所．主として，高速ディジタル伝送方式の研究実用化，ネットワーク・アーキテクチャ，ITS，ネットコミュニティの研究開発に従事．ITU-T SG13 の「B-ISDN と他網との相互接続」に関する責任者として国際標準化にも従事．1992 年から 93 年には，Bell Communication Research（現，Telcordia Technology. Inc.）の客員研究員．現在は，「信頼できるネットワーク社会」に関する研究に興味を持つ．2009 年 4 月より日本大学理工学部教授．工学博士（東京工業大学)．

松本　　勉（正会員）

1986 年 3 月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年 4 月横浜国立大学講師．2001 年 4 月より同大学院環境情報研究院教授．2007 年 4 月〜2011 年 3 月は同大学教育研究評議員を兼務．2011 年 4 月より同大学理工学部副学部長を兼務．日本学術会議連携会員．暗号アルゴリズム・プロトコル，耐タンパ技術，生体認証，人工物メトリクス等の「情報・物理セキュリティ」の研究教育に 1981 年より従事．1982 年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を 4 名で創設．2005〜2010 年国際暗号学会 IACR 理事．1994 年第 32 回電子情報通信学会業績賞，2006 年第 5 回ドコモ・モバイル・サイエンス賞，2008 年第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞（研究部門）受賞．