Vol.2010-CSEC-49 No.12
2010/5/11

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

猪俣敦夫[†1] 東結香[†1] 上田昌史[†3]
小松文子[†2] 藤川和利[†1] 砂原秀樹[†4,†1]

本論文では，Rogers よる防護動機理論 (PMT) に着目した情報セキュリティリスク解明モデルを提案する．特に，子供達を取り巻くネット環境におけるリスクをセキュリティ脅威と定義し，我々が実施中の問題解決型学習にて用いる脅威アピール説得により，その対応の仕方がどのように変容するのかを PMT ベースのモデルを提案する．今回，大阪府内の高等学校で実施した実証実験の結果を報告し，考察を与える．

Proposal of a solution model for the information security risk based on Protection Motivation Theory and its implementation to high school education

Atsuo Inomata,[†1] Yuka Higashi,[†1] Masashi Ueda,[†3]
Ayako Komatsu,[†2] Kazutoshi Fujikawa[†1]
and Hideki Sunahara[†4,†1]

In this paper, we propose a solution model for the information security risk based on Protection Motivation Model by Rogers. Firstly we define the security risk as Internet risk surrounding children especially high school student and then construct the model by the threat appeal persuasion on PMT that we have already put in practice at our ordinal problem-based learning. Furthermore we executed an experimentation at a high school in Osaka and evaluated.

†1 奈良先端科学技術大学院大学 (NAIST)
†2 (独) 情報処理推進機構 (IPA)
†3 国立情報学研究所 (NII)
†4 慶應義塾大学 (Keio University)

1. はじめに

インターネットや携帯電話利用の急増により情報通信の仕組みが複雑化し, それに伴いセキュリティに対する注目が高まりつつある. 一方, 企業・組織・政府においてサイバー攻撃等への対策手段を講じるための費用も莫大である．当然ながら，実際のセキュリティ水準を向上させていくことが理想であるが，現実，そう簡単なことではない．この理由は様々な要因にもよるが，情報セキュリティ技術を適切に取捨選択することが困難であるためとも考えられる．その大きな要因の 1 つがセキュリティ対策コストがあげられる．ここ数年，この問題に目を向けた学際的研究として情報セキュリティ投資研究が注目を浴びている．ここでは，情報セキュリティ技術の確保を目指し技術的な問題や情報セキュリティ投資に関する経済的な動機付けの問題が重要であると指摘されており，すなわち情報セキュリティ投資の費用対効果, その最適性の分析を実施することが急務である．特に，ROSI(Return On Security Investment) への注目が高まり，情報セキュリティに対する最適投資規模を明確化することを目的とした Gordon-Loeb モデル[1] が導入され，中程度の脆弱性に対して最適なセキュリティ投資が行われていることが既に示されている．さらに松浦らによって彼らのモデルに対する投資戦略の実証やモデルに導入される関数系の実証研究が大きな成果[2] をあげている．これにより例えば，企業・組織等において適切な情報セキュリティ対策のためのコスト見積もりや不要な投資の削減等，現実ある程度の見通しが見えてきたとも言えよう．

1.1 動向と関連研究

2005 年に発生した米国同時多発テロ以降，セキュリティエコノミクスと呼ばれる研究領域が Ross Anderson[3] らによって主導的に進められ，国際的にも重要課題として注目されてきている．我が国においても，社会科学的観点からも情報セキュリティに関わる様々な事象を分析する試みが，(独) 情報処理推進機構の小松ら[4] のグループによって開始されている．彼らは，ELSEVIER の研究論文データベース Science Direct に格納された情報から社会科学的手法を用いた研究動向を紹介した上で近年の傾向を調査し[6]，2004 年以降特に，経済学・ゲーム理論といった定量的手法を用いた研究が増加していることを示した．また，情報セキュリティ対策の普及に生じる問題を社会的ジレンマとして捉えた研究[5] においては，DOWES の定義[7]”社会が最適とする現象と個人が合理的と判断する現象の乖離”をもとに，情報セキュリティ対策の現状を社会的ジレンマと仮定した上でユーザごとの合理的選択・判断についてゲーム理論によるモデルを提案しているなど大変興味深い．一方，Ross は自身の Blog[8] にて”security engineers together with psychologists, behavioral economists and

others interested in deception, fraud, fearmongering, risk perception and how we make security systems more usable”，セキュリティ技術者はより幅広い研究領域を見据えた分析等が必要であることを示唆しており，Security Human Behaviour(SHB) ワークショップを開催し心理学の観点も踏まえた幅広い検討を進めている．

1.2 恐怖-脅威アピール研究

我が国において，情報セキュリティの諸技術や専門的知識を教育する場は多数あるものの，実際に正しくそれらを運用させていくためのリテラシ教育や想定外のセキュリティインシデントが発生した際の対応等の教育体制は未だ不十分である．また，インターネットを始めとして携帯電話等の通信端末の普及により，成人だけでなく未成年 (子供) まで今日まで全く想定していなかった未知のリスクに曝される危険性がある．我々は，ある程度予測可能なインシデントを実際に受講者に体験させ, それに対応できる能力を養成する危機管理演習など新しい形のセキュリティ教育を既に実施済み[9][10] である. 以下，現状の問題点をまとめる．

- 短時間で様々な対応 (思考・作業) が必要になるため，個人だけでなく複数人での適切な連携が行われにくい
- 予期せぬ未知のインシデントによる脅威の度合いを定量的に評価しにくいため，被害の深刻さを測定することが困難
- リスクへの対応 (対策) したことによる安心感，満足感を定量的に評価しにくい

そこで本論文の目的は，情報セキュリティリテラシ教育において，脅威アピール説得手法を用いた教育を実施することで，受講生の対応がどのように変容するかを測定することを目的とする. 特に，情報セキュリティに関するリスク意識が乏しい，かつインシデント対応経験の少ない子供達を対象とし，インターネットや携帯電話の利用において潜むリスク，その一例として SNS やプロフ，掲示板，ウィルス，BOT，詐欺・脅迫行為等の事例をセキュリティ脅威とし，個人情報の取り扱い方や盗聴・漏洩，インシデントに遭遇した際の対応の仕方の変容を確認する. 既に，我々は PMT を情報セキュリティの脅威モデルに適用したセキュリティリスク解明モデルを提案済み[11] であり，本稿ではその有用性に対する実証実験を行う．

2. 脅威アピール説得

深田によると，脅威アピール (threat appeal) とは，特定の話題について話す側が受ける側を説得する際，脅威の危険性を強調して脅すことによりその脅威へ対処する特定の対処行動 (coping behavior) の勧告 (recommendation) に対する受ける側の受容を促進させることを意図した説得的コミュニケーションである，と定義される[12]．また，脅威事象として 1 個人で対処できる脅威と 1 個人では対処できない脅威が存在する．例えば，前者は虫歯対策の歯磨きであり，後者は猛暑日にエアコンの過剰利用により発生する電力不足問題があげられる．ここで注意すべき点は，後者は環境配慮行動の問題と類似していることである．以下の 4 項目に整理する．

(1) 説得に及ぼす恐怖の効果の媒介因 (コミュニケーション内容の学習量，話す側やコミュニケーションに対する攻撃・評価・反応等) の明確化
(2) 恐怖と説得効果との間の関係の規定因 (勧告される対処行動の効果性等) の解明
(3) 説得効果の規定因として受け側の個人差要因 (防衛的回避傾向, 対処能力, 脅威に対する関連性)
(4) 脅威情報 (恐怖情報) の成分別効果

これら説得効果を予測する理論としては, 緊張提言モデル (Hovland, Janis & Kelley,1953), 3 次元モデル (Janis,1967), 防護動機理論 (Rogers,1983) が提唱されているが，本稿では特に高校生を対象とした分析を進める．そこで我々が実践するセキュリティ教育で用いる脅威アピール説得手法をベースに受講者の対処行動の変容を確認するため，Rogers による防護動機理論 (Protection Motivation Theory) をもとにモデルを構築した．

2.1 防護動機理論

Rogers は，脅威アピールを構成するコミュニケーションが単一ではなく複数と捉え，3 つの刺激変数が含まれると述べている[13]．

(1) 脅威の有害さ (Magnitude of noxiousness):描写された事態の有害さの程度
(2) 脅威事象の生起確率 (Probability of occurrence):対処行動が遂行されない場合，既にある行動が修正されない場合にその事態が生起する条件確率
(3) 勧告された対処行動の効果性 (Response efficacy):有害な刺激を減少, 除去しうる対処反応のし易さ

上記 3 成分が，それぞれ独立した認知を生じさせ，これらの認知が複合的に結合して防護動機を生み出す，と仮定する (図 1)． Rogers & Mewborn は喫煙問題を取り上げた実験を行っているが，禁煙が肺癌を予防するのに効果的である高効果性情報を呈示された被験者の方が，効果的でないと低効果性情報を提示された被験者よりも一貫して説得効果が高かった，という結果を報告している．

1976 年以降，PMT の 3 成分による相乗的結合説得効果を検討した研究ではその仮説を支持しない結果が報告され，1983 年に Rogers によって新たに PMT が修正された (図 2). その変更点は，1. 認知媒介過程を生起させる情報源タイプの記載, 2. 認知媒介過程の追加お

Vol.2010-CSEC-49 No.12
2010/5/11

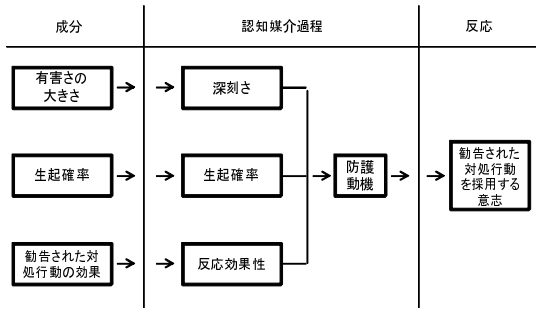

図 1 防護動機理論

よびその構造化, 3. 対処様式タイプの記載, である． 情報源は, 環境的源泉は言語的説得 (脅

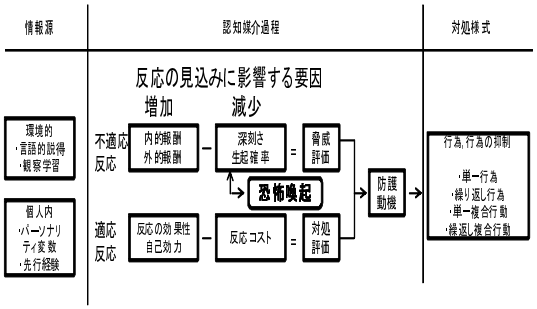

図 2 修正防護動機理論

威アピールとの接触による観察), 観察学習 (他者に生じた脅威の観察)，個人内源泉はパーソナリティ変数と脅威に対する先行経験に分類される．ここで重要な事は，情報の源泉に関わらず認知的評価として脅威評価と対処評価が形成され，その結合によって防護動機が生まれる点である．さらに木村は，修正防護動機理論に基づきエイズ予防行動意図を規定する認知的要因を特定するための分析も実施しており[17]，防護動機理論の唱える認知的要因が行動意図に及ぼす効果についての検討結果は大変興味深い．一方，情報セキュリティ対策は個人行動だけでなく複数人，かつ並行的行動を実施することが多い．そこで集合的な行動モデルについても検討する必要があると考えられる．

2.2 集合的対処行動

集合的対処行動とは，環境配慮行動の問題等我々の生活における比較的大きな範囲で広がる可能性を持つ脅威に対して，多くの人々が並行的に実行する対処行動を指す．例えば，焼却場から排出されるダイオキシンを減らすことを目的としたゴミ分別問題等が挙げられる．集合的対処行動を勧告する脅威アピール説得の効果を説明するために集合的防護動機モデル[14] が深田・戸塚によって提唱されている (図 3)． 集合的対処行動意図を規定する要因は,

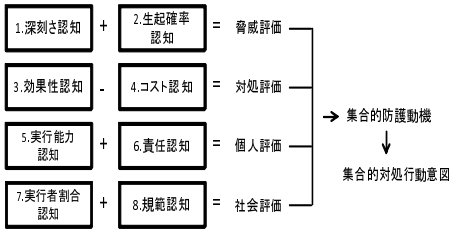

図 3 集合的防護動機モデル

以下の 4 カテゴリに属する 8 つの認知に整理される．

(1) 脅威評価:脅威の深刻さ, 脅威の生起確率
(2) 対処効果:対処行動の効果性, 対処行動実施コスト
(3) 個人評価:受け側の対象行動実行能力, 脅威に対する責任の認識
(4) 社会評価:他者の実行に対する対応の認識, 対処行動による規範や期待

3. PMT に基づくリスク評価モデル

戸塚によると，説得の受け側の関心によって影響要因がどのように異なるかを明確化させることは重要であるとしており，我々もこの方針をサポートすることとする．そこで，情報セキュリティ対策の行動意図 (計画的で意図的な行動の動機) を設定し, それが実際の行動を導くと仮説を立て，セキュリティ教育で伝える (リアルな) 脅威によって働く行動意図形成の要因として

- 対策行動に対する態度 (その対策行動に対する肯定, 否定の評価)
- 主観的規範 (周りから期待されているか否かといった社会的圧力の評価)
- 影響を与える別要因として, 実行可能性評価 (実行することが容易か困難か) を想定
- 動機 (行動意図) と実際の行動, その両者に影響を与える

Vol.2010-CSEC-49 No.12
2010/5/11

と設定するなお，Ajzen と Fishbein は，人間の全ての行動は合理的に行為理論 (Theory of Reasoned Action:TRA)[23] によって予測できると述べており，行動に対する態度 (主要な結果に関する信念，その結果に関する評価) および主観的規範 (準拠集団の意見を知覚した規範的信念，それに従うモチベーション)，この双方から行動意図が生まれ行動に遷移するという非常に簡潔なモデルを定義している．また，近未来の社会的行動を説明・予測する理論として Ajzen による計画行動理論 (Theory of Planned Behavior:TPB)[18] がある．我々が提案するモデルにおいて、意志決定 (行動遷移) については TRA と TPB をベースとする．一方，計算機の利用行動を説明する Davis らによる技術受容モデル (Technology Acceptance Model:TAM)[19] も存在するが，TAM の適用可能性については今後の課題である．

さらに，子供達が直面するセキュリティ脅威は，何かしらの脅威事態解決のために，直接関係のない不適応的対処 (Maladaptive Coping) を考慮する必要がある．これは，前述したセキュリティ対策ソフトウェアのインストールを実際に実行するのか否かという問題と類似しているとも判断できる．この理由として，

(1) 必ずしも脅威に直面するわけではない
(2) どのくらいの脅威か体験出来ない
(3) 必要の無い知識を学習しなければならない
(4) 周囲が全員知っているわけではない

等が考えられ，思考回避 (Avoidance) や Fatalism(運命諦観) など現状をそのまま受け入れてしまう等とも言われており，Milne による Adapted PMT(図 4) がふさわしいと判断し，モデルを設計した．

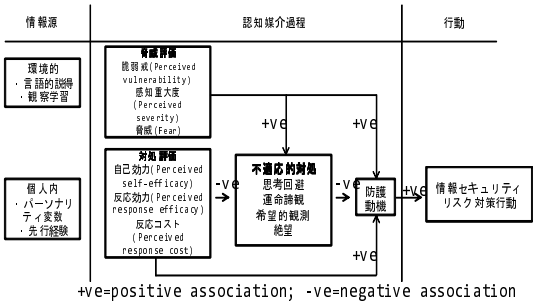

図 4 修正 PMT に基づいた提案モデル

4. 実証実験

4.1 実験計画と方法

高校生を取り巻く情報セキュリティリスク脅威の問題と対策を検討するために，大阪府の高等学校 (全校約 700 名の女子高) にて，脅威アピール説得手法を用いた情報セキュリティに関する出張出前講座を実施し，実証実験を実施した．本講座では，SNS・プロフ利用，個人情報 (住所, 電話番号, メールアドレス, 写真) の漏洩，ネットショッピング，誹謗中傷等による精神的問題，倫理・モラル，の計 5 話題におけるリスクを取り上げ，複数人のグループでディスカッションして問題解決にあたる演習を実施した. なお，理論的，技術的な知識として高校で学習する数学を使った暗号の仕組み，インターネット上で使われている認証，ウィルスの振る舞い，盗聴・詐称の仕組み，パスワードの脅威，IC カード等の耐タンパー性について，あらかじめ演習の前に講義を行った．手順を以下に示す．

(1) フェイスシートおよび講義前のリスク認知に関する調査
(2) 理論的・技術的知識の講義
(3) グループごとのディスカッション演習
(4) 講義後のリスク認知に関する調査

取り扱ったセキュリティ脅威を以下に示す．

- 18 才以上と年齢を偽り SNS へ登録後，プリクラ写真と共に友人の個人情報を掲載してしまった
- 携帯電話サイトのフィッシングサイトと知らず認証用パスワードを入力してしまった
- パスワード認証ページで暗号化されておらずかつ不正な証明書のサイトを信用し，個人情報を入力してしまった
- 漫画喫茶ならば大丈夫だと思い，匿名掲示板で友人の誹謗中傷する記事を書き込みしてしまった

さらに PMT を構成する各要因と情報セキュリティリスク対策行動意図との関連性について，木村による仮説[17] と同様に以下に示す仮説を設定した．

(1) リスク対策行動意図に対し，深刻さ，生起確率，反応効果性，自己効力の 4 つの認知的要因は促進効果を持ち，内的報酬，外的報酬，反応コストの 3 つの認知的要因は抑制効果を持つ
(2) 4 変数から構成される脅威評価及び 3 変数から構成される対処評価は，相互にリスク対策行動意図に効果を持つ

(3) 脅威評価が高い場合の方が，低い場合よりも行動意図に対する対処評価の効果は大きくなる交互作用が得られる

さらに提案モデルによる検証を実施するために以下のように質問紙調査を設計した. なお，かなりそう思う，から全くそう思わない，という 4 段階評定で回答を得た.

(1) セキュリティリスクに関する経験と知識の測定
フェイスシート以外に専門性についての理解度を把握するために簡単なテストを実施する.

(2) 深刻さの測定
インターネットや携帯電話利用において潜むリスクから自分を守るために事前にリスクを学習する, 自分が知らないサイト（相手）以外に接続を試みない, 自分が知らないサイト（相手）でも興味を持てば接続を試みる, ウィルス対策ソフトウェアや携帯電話のアクセス制限機能を利用する

(3) 生起確率の測定
上述したようなリスクの被害を受けた場合, 両親, 兄弟, 友人に話すことができない, 友人を失うことがある, 周囲の人に迷惑を与えることがある今後の生活に支障（影響）がある何らかの手段を講じるによりこのリスクを処置（対策）することができる

(4) 反応効果性の測定
ウィルス対策ソフトウェアや携帯電話のアクセス制限機能を利用すれば防ぐことができる, 上述したようなリスクに関してあらかじめ学習しておけば防ぐことができる, 自分が知らない（相手）サイト以外へアクセスをしなければ防ぐことができる, 自分が知らない（相手）サイトにアクセスしてもリスクに出合うことはない

(5) 内的報酬の測定
自分が知らない（相手）サイトにアクセスしたことで満足感が得られる, 交友関係が広がる,

(6) 外的報酬の測定
ウィルス対策ソフトウェアや携帯電話のアクセス制限機能を利用したことで周囲から評価を得る, 自分が知らない（相手）サイトにアクセスしないことで周囲から評価を得る, 上述したようなリスクを学習し伝えることで周囲から評価を得る

(7) 自己効力の測定
ウィルス対策ソフトウェアや携帯電話のアクセス制限機能を使用する自信がある, これらの使用について友人に伝える自信がある, 上述したようなリスクへの対策などの知識を学習する意識がある, 自分が知らない（相手）サイトへアクセスを試みない自信がある, 自分が興味を持ったサイト（相手）でもアクセスを試みない自信がある

(8) 反応コストの測定
ウィルス対策ソフトウェアや携帯電話のアクセス制限機能利用のための費用が問題である, 導入（方法）が困難である, これらの機能を利用することが面倒である, これらの機能を利用することで満足感が減少する, これらの機能を利用することで周囲に迷惑がかかる

4.2 実験結果

出張出前講座による実験操作の適切性を確認するために実施した結果を示す.

- 脅威評価操作： 深刻さ認知と生起確率認知に対して 5 要因の分散分析を実施したところ，両測度に対して脅威評価操作の主効果がみられた.
  $F(1, 631) = 162.35, p < .001; F(1, 631) = 47.44, p < .001$)
  いずれも低脅威評価条件 ($M = 2.69, SD = 0.80; M = 2.22, SD = 0.70$) よりも高脅威評価条件 ($M = 3.41, SD = 0.69; M = 2.61, SD = 0.72$) の得点が有意に高かった．これらの測度に対しては脅威評価以外の要因の効果もみられたが、脅威評価操作の効果が大きかったため本操作は成功したと判断した.
- 対処評価操作：効果性認知とコスト認知に対して 5 要因の分散分析を実施したところ，両測度に対して対処評価操作の主効果がみられた.
  なお，効果性認知に関しては，低対処評価条件よりも高対処評価条件の得点が有意に高かった．一方，コスト認知に関しては低対処評価条件よりも高対処評価条件の得点が有意に低かった.

4.3 考　　察

前節で述べた実証実験の結果から，出張出前講座による実験操作については、脅威評価、対処評価において概ね成功したと判断できる．すなわち，脅威評価 (高) と対処評価 (高) であれば，集合的防護動機モデルが効果的であると仮定するような脅威アピール説得が，集合的対処行動意図を促進することをこの結果を示している.

ただし、今回は性別は女性，年齢層は高校生のみと限定としたため、今後，男子学生や共学校，大学等においても実証実験を行い詳細な分析を実施する必要がある．結果として，本稿では戸塚，深田による脅威アピール説得における集合的防護動機モデルを我々もサポートする.

5. ま と め

本論文では，防護動機理論に着目し，我々が実施する情報セキュリティリテラシ教育により子供達を取り巻くセキュリティリスクを解明するために提案したモデルを評価するために，実際に大阪府内の女子高等学校で実証実験を実施した結果を報告し，考察を与えた．今後，PMT が規定する諸認知や行動意図が情報セキュリティリスク解明の一要素になりうるかを正確に測定出来るかが鍵となるため，より分析の精緻化を行う必要がある．

- 推奨する対処行動は 1 つに限定されるのか
- 学生各々の家のネットワーク環境・スキル・知識は異なっているため，全員の学生が実行可能な対処行動を設定可能かどうか
- 全員の学生が理解可能な質問を設定可能かどうか

上記を厳密に議論する必要がある．さらに，脅威評価と対処評価の交互作用効果について考慮する必要もある．これは，交互作用効果により，対処評価の実験操作が強く働き低対処評価条件の被験者の効果性認知が非常に低くなる可能性があるためである．今後，さらに他校においても実証実験を実施し，提案モデルの有用性について評価を進める予定である．

謝　　辞

本研究を進めるに辺り，同志社大学 中谷内一也教授，千葉科学大学　戸塚唯志教授から本研究を進めるに辺り貴重なご意見を頂いた．ここに深謝する．

付　　録

参 考 文 献

1) Gordon, L.A. and Loeb, M.P, "The economics of information security investment", ACM Transactions, on Infomation & Systems, Sec.5, pp.438-457, 2002.
2) K.Matsuura, "Productivity Space of Information Security in an Extension of the Gordon-Loeb's In vestment Model", Workshop on the Economics of Information Security(WISE2008), 2008.
3) Ross Anderson, "Security Economics and Critical National Infrastructure", Workshop on the Economics of Information Security(WISE2009), 2009.
4) 杉浦, 小松, 上田, 山田, "情報セキュリティエコノミクスの挑戦", Proc. of CSS2008, pp.725-730, 2008.
5) 小松, 赤井, 上田, 松本, "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- ", IPSJ 研究報告, IPSJ-SIG-SPT-40(109), pp.265-280, 2009.
6) 持永, 杉浦, 小松, 村野, 赤井, "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", IPSJ 研究報告, IPSJ-SIG-SPT-41(109), pp.281-287, 2009.
7) Dowes, R., "Social Dilemmas", Review of Psychology, No.31, pp.169-193, 1980.
8) R.Anderson, "Light Blue Touchpaper", http://www.lightbluetouchpaper.org/
9) 情報セキュリティ研究所, http://www.riis.or.jp/
10) 文部科学省　先導的 IT スペシャリスト教育プログラム (IT-Keys), https://it-keys.naist.jp/
11) 猪俣, 東, 上田, 藤川, 砂原, "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一検討", CSS2009 予稿集, pp.979-985, 2009.
12) 深田, "説得心理学ハンドブック", 北大路書房, 2002.
13) 木村, 深田, 周, "恐怖-脅威アピール・モデルの説明力の比較", 名桜大学総合研究所紀要, pp.13-18, 2001.
14) 戸塚, 深田, "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", The Japanese Journal of Experimental Social Psychology, Vol.44, No.1, pp.54-61, 2005.
15) 戸塚, 深田, "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", Journal of Experimental Social Psychology, Vol.44, No.1, pp.54-61, 2005.
16) Rogers, R. W, "A protection motivation theory of fear appeals and attitude change", Journal of Psychology, Vol.91, pp.93–114, 1975.
17) 木村, "エイズ予防行動意志に及ぼす脅威の大きさ, 対処行動の効果性およびコストの効果:脅威アピールにおける修正防護動機理論の検討", 広島大学教育学部紀要, 第一部心理学, No.44, pp.59-66, 1996.
18) Ajzen, I., "From Intentions to Actions: A Theory of Planned Behavior", in J.Kuhl and J.Beckmann(Eds.), Action Control: From Cognition to Behavior, Springer, pp.11-39, 1985.
19) Davis,F.D.,R.P.Bagozzi, P.R.Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models", Management Science, Vol.35, No.8, pp.982-1003, 1989.
20) S.Milne, P.Sheeran, and S.Orbell, "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory", Journal of Applied Social Psychology, Vol.30, pp.106-143, 2000.
21) Magdalena Cismaru, "Using Protection Motivation Theory to Increase the Persuasiveness of Public Service Communications", Tha Saskatchewan Institute of Public Policy, Unicersity of REGINA, No.40, SIPP No.40, 2006.
22) T.Chenoweth, R.Minch, T.Gattiler, "Application of Protection Motivation Theory to Adoption of Protective Technologies", Proc. of Hawaii International Conference on System Science, IEEE, 2009.
23) Fishbein, M., Ajzen, I, "Belief attitudes, intention, and behavior: An introduction to theory and research", Addison-Wesley, 1975.