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

猪俣 敦夫† 東 結香† 上田 昌史‡ 藤川 和利† 砂原 秀樹†§

†奈良先端科学技術大学院大学 情報科学研究科
630-0192 奈良県生駒市高山町 8916-5

(atsuo,yuka-h)@is.naist.jp, fujikawa@itc.naist.jp

‡国立情報学研究所 情報社会相関研究系
101-8430 東京都千代田区一ツ橋 2-1-2
ueda@nii.ac.jp

§慶應義塾大学メディアデザイン研究科
108-8345 東京都港区三田 2-15-45
suna@wide.ad.jp

あらまし 近年，人間が関わる多様なリスクを説明するために説得心理学の恐怖-脅威アピール研究が注目されつつある．そこで本論文では，防護動機理論に着目した情報セキュリティリスク解明のためのモデルを提案する．特に，プロフ等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化するのかを PMT により説明するためのモデルを構築する．今回，予備実験として実施した大阪府内の高等学校でのヒアリング結果を踏まえて検討する．

A study to understand and elucidate model for information security risk based on Protection Motivation Theory

Atsuo Inomata† Yuka Higashi† Masashi Ueda‡ Kazutoshi Fujikawa† Hideki Sunahara†§

†Nara Institute of Science and Technology
8916-5 Takayama-Cho Ikoma-Shi Nara 630-0192 Japan

(atsuo,yuka-h)@is.naist.jp, fujikawa@itc.naist.jp

‡National Institute of Infromatics
1-1-2 Hitotsubashi, Tokyo 101-8430 Japan
ueda@nii.ac.jp

§Keio University
4-1-1 Hiyoshi, Kanagawa 223-8526 Japan
suna@wide.ad.jp

Abstract Recently Protection Motivation Theory is focused for the interdisciplinary research area not only psychology but also various risks for information security. It has a potentially valuable meaning for predicting adoption of a human behavior. In this paper, we propose PMT-based model for solving risk of information security, especially younger people. Our goal is to explain how to change their behavior and action by a new security learning for young people.

1 はじめに

情報セキュリティ技術の進歩が著しく，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は膨大になりつつある．これに併せて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そうならないのが現実である．これは，様々な要因にも寄るが，

情報セキュリティ技術を適切に取捨選択し適用することが困難であると考えられる．その大きな要因の１つがセキュリティコストである．近年，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されつつある．その主要な成果では，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と我々も考える．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て Gordon-Loeb モデルが導入され，これにより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をあげている．また，情報セキュリティ対策投資効果を計量する生産性パラメータを定義し，それをミクロ経済モデルで表現することにも成功している．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のある程度の見通しが見えてきたとも言えよう．

2　恐怖-脅威アピール研究

米国同時多発テロ以降，セキュリティエコノミクスという新しい研究領域が Ross Anderson[1] らによって主導的に進められ，国際的にも急務の課題として重要視され始めるようになってきた．特に，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小松ら [2] によって開始されている．一例として 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文献 [4] では，2004 年以降，経済学，ゲーム理論といった定量的な研究手法を用いたものが大幅に増加していることが示されている．その中でも，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 [3] においては，DOWES の定義 [5]”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研究がある．また，Ross は自身の Blog[6] 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”，すなわち，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いる．彼は Security Human Behaviour(SHB) ワークショップも開催しており，心理学の観点からの検討も進めている．

一方，我が国においては，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場合の対応などの教育について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やそれに類した通信端末の普及により，成人だけでなく未成年 (子供) まで，今まで想定していなかった未知のリスクにさらされる危険性も生まれている．既に様々な状況に即したインシデントを実際に体験させ、それに対応できる能力を養成する危機管理の体験演習など新しい形のセキュリティ教育も実施しており [7][8]，そこで得られた知見をもとに洗い出された問題点を以下にまとめる．

- 短時間で様々な対応が必要になるため，個人だけでなく複数人での適切な連携が適切に行われない
- 予期せぬインシデントによる脅威の度合いが様々であり，その脅威による被害の深刻さを図ることが困難
- 確実に安全性の対応 (完了) したことによる安心感，満足感が得られにくい

そこで我々は，説得心理学における脅威アピール研究に着目し，あらかじめ情報セキュリティリスクやリテラシ教育を実施することで，彼ら

の対応がどのように変化するのかを把握するかのモデルを PMT を用いて構築する．特に，情報セキュリティに関するリスク意識が乏しい，かつ経験の少ない子供達を対象として，インターネットや携帯電話を利用した SNS やプロフ，掲示板，メール等におけるリスクをセキュリティ脅威と定義し，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がどのように変化していくのかを明確に説明出来るようにすることが目標である．今回，防護動機理論を情報セキュリティの脅威モデルに適用するために，実際に高等学校でのヒアリングをした結果を踏まえて検討した．

2.1 脅威アピール研究

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 [9]．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，後者は猛暑日などに発生する電力不足問題である．特に後者は環境配慮行動の問題と類似していると言えよう．上記を整理すると以下の 4 項目に分類される．

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

上述した説得効果を予測する理論として，例えば, 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，我々は特に高校生を対象として情報セキュリティリスク分析を進めるため，既に実施しているセキュリティ教育手法で用いる脅威アピールの実施による対処行動の結果を実証するため，今日最も受け入れられている防護動機理論 (Protection Motivation Theory:PMT) をもとにモデルの検討を進めた．

2.2 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 [10].

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)．興味深い実証結果

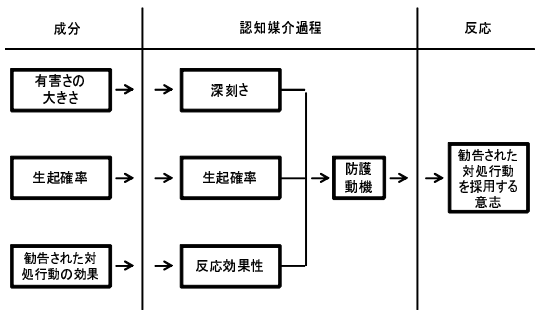

図 1: 防護動機理論

として 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．

2.3 修正防護動機理論

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)．その大きな変更点は，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 (脅威アピー

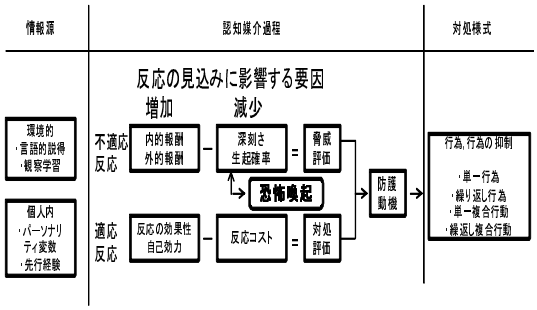

図 2: 修正防護動機理論

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．

2.4 集合的対処行動

次に，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等である．この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 [11] が深田・戸塚によって提唱されている (図 3)．集合

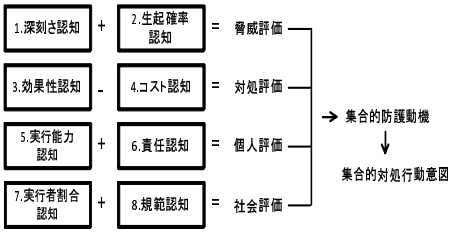

図 3: 集合的防護動機モデル

的対処行動意図を規定する要因は，以下の 4 カテゴリに属する合計 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 によるリスク評価モデル

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述べている．我々もこの点をサポートする考えをとり，特に中高生においては友人, 教師, 家族からの影響が比較的高いことが予想される，と仮定を立てており，この方針をより効果的に示すために上記 8 認知が影響を与えているかどうかを調べる必要があると考える．

3.1 PMT における既存研究

PMT は，一般的に健康面を考慮する人々が対処する行動への動機付けを説明・説得する際に利用される事例が多数存在する．

その中において PMT を情報セキュリティに適用した興味深い研究がある．Tim らはウィルス駆除ソフトのような保護技術に対して，PMT を適用したモデルを提案 [14] している (図 4)．情報セキュリティ対策は，例えばソフトウェアのイ

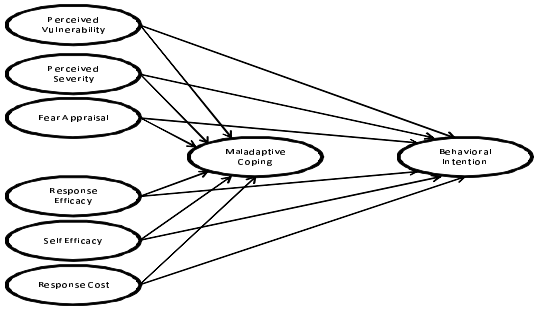

図 4: Antispyware への PMT 適用

ンストール (という行動) をとろうとする意志が働くかどうか，すなわち行動について言及する必要がある．これは Ajzen と Fishbein によると，人間の全ての行動は合理的に行為理論 (Theory of Reasoned Action:TRA) によって予測できると述べており，これは行動に対する態度 (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概念である．一方 TRA 以外では，計画行動理論 (Theory of Planned Behavior:TPB) および技術受容モデル (Technology Acceptance Model:TAM) 等も存在する．

3.2 提案モデル

本章では，我々が既に実施中の問題解決型学習 (Problem-Based Learning:PBL) を子供達へのセキュリティ・リテラシ教育 [7][8] に取り込むことにより，彼らがその対策を実際にどのように行動に移すのかという点を PMT をもとに説明するためのモデルを検討する．なお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．この理由は，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，等が考えられる．また，一般的に思考回避 (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，これにより PMT の中でも Milne による Adapted PMT(図 5) によるモデルがふさわしいと考える．

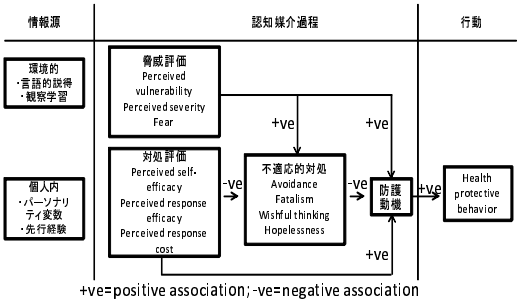

図 5: Adaptive PMT

3.3 ヒアリングの実施

子供達を取り巻くセキュリティ脅威としてどのようなリスクを考慮する必要があるのかその項目を洗い出す事を目的として，大阪府の学校 (全学年約 700 名の女子高等学校) にてヒアリングを実施した．その結果、主として 1. 常時接続を持つ家庭は確実に増加，2. 高等学校「情報」ではモラル教育などは一般的に不足，3. チェーンメール等一般的知識は有しているがトラブル発生時の対応は未知，4. 学校が個人をどこまで管理するかは大きな問題，例えば政府や自治体への要望，5. 子供だけでなく保護者の理解不足も大きい，等の意見があげられた．そこで今回取り上げる話題として，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 話題を選定した．これにより本実験で実施する質問紙調査では，次の 6 項目，1. 対処行動意思, 2. 恐怖感情, 3. 深刻さ, 4. 生起確率, 5. 反応効果性, 6. 自己効力, を設定する．なお，この本実験ではフェイスシートも併せて実施し，その結果から恐怖-脅威アピールの対象者として潜在的な危険に曝されている，および潜在的な危険を引き起こす行動をとる物を最終的な分析対象者とする予定である．

3.4 考察

今回，PMT を用いるため最終的な評価，すなわち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がある．交互作用効果とは，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，という点である．この理由から質問紙調査の設計には高校生の携帯電話やインターネット利用の状況を十分考慮する必要がある．

4 まとめ

本論文では，防護動機理論に着目し，我々が実施中のセキュリティ教育により子供達を取り巻くリスクを解明するモデルの検討を行なった．今後，大阪府・兵庫県の高等学校で実証実験を実施し，提案モデルの有効性について検証し報告する予定である．

謝辞

本研究を進めるに辺り，同志社大学 中谷内一也教授，(独) 情報処理推進機構 小松文子室長から貴重なご意見を頂いた．ここに深謝する．

参考文献

[1] Ross Anderson, ”Security Economics and Critical National Infrastructure”, Workshop on the Economics of Information Security(WISE2009), 2009.

[2] 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.

[3] 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.

[4] 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.

[5] Dowes, R., ”Social Dilemmas”, Review of Psychology, No.31, pp.169-193, 1980.

[6] R.Anderson, ”Light Blue Touchpaper”, http://www.lightbluetouchpaper.org/

[7] 情報セキュリティ研究所

[8] IT-Keys, https://it-keys.naist.jp/

[9] 深田, ”説得心理学ハンドブック”, 北大路書房, 2002.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] Fishbein, M., Ajzen, I, ”Belief attitudes, intention, and behavior: An introduction to theory and research”, Addison-Wesley, 1975.