コンピュータウィルス対策行動の規定要因に関する検討

浜津翔[†1]　栗野俊一[†2]　吉開範章[†2]

我々は，コンピュータウィルスに感染したと通知を受けた時，ヒトがどのように判断し，行動するのかを調査するために，説得心理学を基礎としたアンケート調査と実験を行ってきた．今回，集団的防護動機理論を基礎としたウィルス対策実行意思の説明モデルを作成し，分析を行い，各要因が対策実行意思に与える影響力について調査を行ったので，報告する．

Study on the determining factor of measure against a computer virus

SHO HAMATSU[†1]　SHUN-ICHI KURINO[†2]　NORIAKI YOSHIKAI[†2]

1. まえがき

DDoS 攻撃は，今ではインターネットを用いた各種サービスの安定的な提供に対する主要な脅威の 1 つとなっており，金銭目的や組織に対する抗議・嫌がらせ，社会的・政治的意図等を動機としてさまざまなサービス妨害攻撃が発生している[1]．インターネット上で，DDoS 攻撃が脅威と考えられる要因の一つが，ボットネットワークの存在である．サイバークリーンセンター(CCC) は，ボットに感染したコンピュータを検出し，ISP を通じてユーザに注意喚起のメールで駆除ソフトのダウンロードを勧めていた．しかし，駆除ツールをダウンロードしたユーザは 3 割だけという報告がある[2]. もし, 駆除ソフトのダウンロードが 100% 実現できれば，ボットネット自体を無くし，DDoS 攻撃への対策となると考え，説得心理学を基礎とした新しい情報セキュリティ対策について研究を行っている．

今回，集団的防護動機理論を基礎としたウィルス対策実行意思の説明モデルを作成し，分析を行い，各要因が対策実行意思に与える影響力について調査を行ったので，報告する．

2. 先行研究

従来，災害や地震などでのパニックに対する説得心理学の研究はなされていたが，情報セキュリティ環境でのリスク認知・パニック心理に関する研究はなされていない．個人の振る舞いや意思決定と社会との関連についての研究としては，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に想定した実証研究の報告がある[3].

独立行政法人 情報処理推進機構(IPA) が，コンピュータウイルス感染環境下で，ヒトが情報セキュリティ脅威についての情報を与えられた際に，どのように認知し，また実際にどのように行動を行うかについて Web を用いたアンケート調査，仮想環境での行動観察実験による調査報告を行っている[4]．そこには，集団的防護動機理論[5]の規定となる 8 つの認知要因が，互いに独立して対策実行意思へ影響を及ぼす集団的防護動機モデルを用いて評価し，対策実行意思に最も影響を与える要因は，従来の癌対策やゴミ対策において言われる「脅威認知」ではなく，「効果性認知」であると報告されている．その後，我々の研究室で，IPA の実験環境，および実験手順等を見直し，再度，実験を実施した[6]．その実験データや事後アンケート結果を用いて調査・分析した結果，各認知要因間に相関を示す場合が多数存在することが分かった．

そこで，対策実行意思へ影響を及ぼす要因の関係について，再度見直すこととした．

3. 集団的防護動機理論とボットウィルス対策

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一つに，脅威アピールがある．これは，脅威の危険性を強調して，対処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コミュニケーションである．防護動機理論は，脅威アピールの説得効果を説明する理論である[5]. 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す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ている．

本研究では，ボットウィルスを脅威の対象としており，多くの人が集団的にボットウィルスを対策することで，はじめてボットネットの脅威の低減を期待できることから，集団防護動機理論の枠組みで検討する必要がある．

集団防護動機理論では，対処行動の規定要因として，深

†1 日本大学 大学院 理工学研究科 吉開研究室
Yoshikai Laboratory. Graduate School of Science and Technology Nihon University.
†2 日本大学 理工学部 数学科 吉開研究室
Yoshikai Laboratory. Department of Mathematics. College of Science and Technology, Nihon University.

刻さ認知(直面する脅威の深刻の程度についての認知)，生起確率認知(直面する脅威が生起する確率についての認知)，効果性認知(勧告された対処行動の効果性についての認知)，コスト認知(対処行動の実行に伴うコストについての認知)，実行能力認知(受け手自身に対処行動を実行する能力があるかどうかについての認知)，責任認知(直面する脅威事象の発生や対処行動の実行に責任を感じているかどうかについての認知)，実行者割合認知(どの程度の割合の人が当該の対処行動を実行するかについての認知)，規範認知(対処行動をとることが準拠集団の規範や期待に沿っているかどうかについての認知) の 8 つが影響するとされている．

4. Web アンケートと実験の概要

4.1 Web アンケート

今回の分析で用いた Web アンケートは，集団的防護動機理論の 8 つの規定要因に関する質問項目と，対策実行意思に関する質問項目であり，各質問項目に対して「1: そう思わない」～「4: そう思う」の 4 段階で回答を求めた．質問内容は，次の通りである．

・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．

・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．

・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．

・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．

・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．

・責任認知: 自分にはこの駆除手順を実行する責任がある．

・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．

・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．

4.2 実験の概要

今回の分析では，文献[6]で述べた実験により得たデータ及び，事後アンケート結果を用いている．実験の目的は，ウィルス感染環境下における実験協力者の行動に関する情報を得ることである．実験は，仮想ゲームの休憩時間にウィルス感染を伝えるインシデントを表示し，実験協力者が対策するまで段階的(level1～level3) に状況を変更させながら，それに対する行動を観察した．

level 1 実験協力者の画面にインシデント表示がされる．

level 2 チャット内で，ある一人の実験参加者にもインシデントがあった事が語られ，それに対応して，別の実験参加者から，感染による被害(応答が遅くなる) があった事も報告される．

level 3 画面が暗くなり，ウィルス対策以外の操作ができなくなる．

また，実験後には，本実験の目的である，ウィルス感染環境下における実験協力者の行動に関する情報を得るために，事後アンケートをインタビュー形式で行った．その内容は，実験後に，実験本来の目的を明かした上で，実験協力者に直接，実験中に感じた感情や，行動の意図などの説明を求めるものである．

5. ウィルス対策実行意思の説明モデルの作成

事後アンケートの質問項目の中には，対策した/しなかった理由を問う項目があり，その回答の中から，対策実行意思に影響を与える要因を読み取った．その要因と，基となった回答は，次の 7 つである．

ただし，level 1 では，インシデント表示しか行わないので，実験協力者は次の三つ認知が刺激されると思われる．

1-1. 深刻さ認知 ： ボットウィルス感染による被害の深刻さを表す．

1-2. 実行能力認知 ： 提示された対処行動を実行する能力があるかどうか．

1-3. コスト認知 ： 提示された対処行動の実行に伴うリスクがあるかどうか．

level 2 では，他の実験参加者にもインシデントがあり，それに対して，対策を行ったと報告されることから，深刻さ認知，実行能力認知，コスト認知に加えて，効果性認知，責任認知，実行者割合認知の 3 つの認知が刺激されると思われる．

2-1. 効果性認知 ： 提示された対処行動に効果があるかどうか

2-2. 責任認知 ： 提示された対処行動を実行する責任が自分にあるかどうか．

2-3. 実行者割合認知 ： 提示された対処行動を実行している人がどの程度いるのか

level 3 では，インシデント表示のみで，ウィルス対策以外の操作ができなくなることから，level 1 と同じ認知が刺激されると思われる．

深刻さ認知 → 対策実行意思

「ポップアップが何度も出てくるのと，『感染しました』という普段聞きなれない(普段は可能性がありますという単語)言葉だったので対応した．」(level 1 対策者の発言)

コスト認知 → 対策実行意思

「ポップアップが出てすぐ対策をしようと思ったが，ゲームへの悪影響を考慮して対策しなかった．」(level 2 対策者の発言)

実行能力認知 → 対策実行意思

「『はい』を選択していくことで，駆除が簡単にできると思ったから対策した．」(level 1 対策者の発言)

効果性認知 → 対策実行意思

「チャットで『やったらできた』という発言があったので，自分も対応した.」(level 2 対策者の発言)

責任認知 → 対策実行意思

「ゲームをやっていて，ゲームに参加している他の方に迷惑がかかってしまうから対策した.」(level 2 対策者の発言)

実行者割合認知 → 対策実行意思

「チャットでも他の人が駆除したと言っていたため対策した.」(level 2 対策者の発言)

規範認知 → 対策実行意思

「ウィルスは対策するもので．ウィルスが出れば必ず対策は行う.」(level 1 対策者の発言)

この他に，要因間の相関関係を示唆する回答があった．その関係と，基となった回答は，次の 3 つである．

深刻さ認知 → 効果性認知

「だんだん頻繁に出るようになって，やればできるかなと思った.」(level 3 対策者の発言)

この回答をした方は，level 2 で与えられた情報には対策するに至るまでの要因はなく，最終的には，提示された対処行動の効果に期待して対策を行ったと発言していたので，この相関関係があると考えた．

深刻さ認知 → 責任認知

「他者に迷惑がかかると思ったから対策した.」(level 1 対策者の発言)

深刻さ認知 → 規範認知

「自身の PC でなくてもウィルス対策はすべき.」(level 1 対策者の発言)

「深刻さ認知 → 責任認知/ 規範認知」の 2 つの関係については，level 1 で，責任認知と規範認知を刺激する情報を与えていなかったにもかかわらず，その 2 つの認知が，対策の要因と読み取れる発言があったので，相関関係があると考えた．

この他に対策実行意思に影響を与える要因，要因間の関係が存在すると考えられる．それは，次の 3 つである．

生起確率認知 → 深刻さ認知

理由: ボットウィルスによる被害に遭う確率が高くなれば，深刻さが増すと考えられるため．

規範認知 → 責任認知

理由: ウィルス対策が規範に沿っていれば，対策実行に対して責任を感じると考えられるため．

効果性認知 → 実行者割合認知

理由: ウィルス対策の効果が大きければ，それを実行する人も多くなると考えられるため．

上述した，対策実行意思に影響を与える要因，要因間の関係を仮定することによって，ウィルス対策実行意思の説明モデルを構成する．

6. 分析結果

6.1 共分散構造分析を用いたモデルの評価

ウィルス対策実行意思の説明モデルと Web アンケート結果を用いて，集団的防護動機理論の規定要因が対策実行意思へ与える影響について，共分散構造分析によって分析を行った. 調査対象者は事前アンケートの回答者 1700 名である．

はじめに，認知要因間が独立であると仮定して分析を行った．その結果を図 1 に示す．図 1 に示された数値は，標準偏回帰係数であり，当該予測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の平均的変化を意味する．

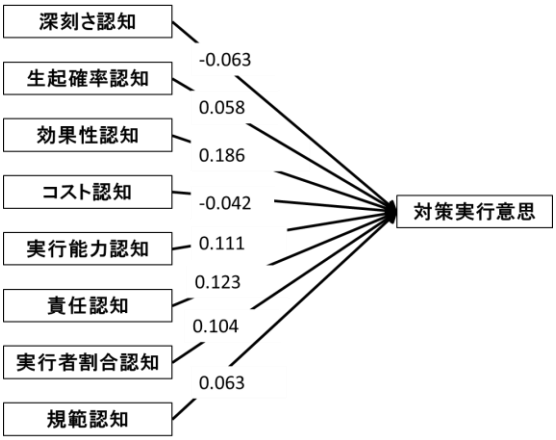

図 1 独立を仮定したモデル

共分散構造分析では，モデルを評価するために適合度指標が用いられ，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．このモデルの適合度指標は, GFI = 0.664, AGFI = 0.460, RMSEA = 0.251, CFI = 0.080, SRMR = 0.232 となり，モデルの適合度が低いという結果が得られた．

次に，作成したモデルに従い分析を行った．その結果を図 2 に示す.

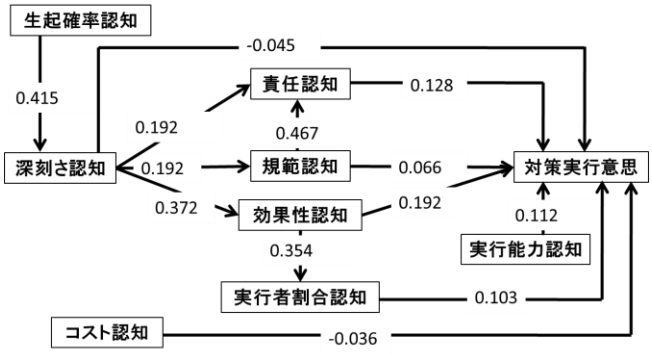

図 2 ウィルス対策実行意思の説明モデル

このモデルの適合度指標は，GFI = 0.841，AGFI = 0.688，RMSEA = 0.200，CFI = 0.521，SRMR = 0.159 である．この

結果から，独立を仮定したモデルより適合度指標が高くなっていることが分かる．

6.2 対策実行意思に与える影響力の大きさ

次に，各要因が対策実行意思に与える影響力の大きさを計算する．ある要因から対策実行意思に直接パスが引かれる場合，そのパスの標準偏回帰係数を，その要因の直接効果と呼び，別の要因を経由して対策実行意思にパスが引かれる場合は，間接効果と呼ぶ．間接効果は経由するパスの標準偏回帰係数の積で表され，対策実行意思に与える影響力の大きさは直接効果と間接効果の和で表される．各要因が対策実行意思に与える影響力の大きさを表 1 に示す．

表 1 各認知要因の影響力

	効果性	責任	規範	実行能力	実行者割合	深刻さ	生起確率	コスト
影響力	0.228	0.128	0.126	0.112	0.103	0.089	0.037	−0.036

6.3 実験データに対するモデルの適合度

次に，実験データに対するウィルス対策実行意思の説明モデルの適合度を調査する目的で，推定される共分散行列と実験データを加えた標本分散行列を用いて，図 2 のモデルに対して，適合度指標の算出を行った．用いた実験データは，実験での対策の有無「1: 対策を行った」,「4: 対策を行わなかった」の 2 値であり，Web アンケートの対策実行意思に関する質問項目の代わりに用いた．適合度指標を計算した結果, GFI = 0.673, AGFI = 0.331, RMSEA = 0.300, SRMR = 0.203 となり，低い適合度が示された．

7. 考察

各要因が対策実行意思に与える影響力の大きさを計算した結果,「対策実行意思」に最も影響を与える要因は「効果性認知」であった．このことから，対処行動がボットウィルス対策にどれだけ効果があるかを認知させることで，より効果的に対策を促すことができると考えられる．

また,「生起確率認知」,「コスト認知」は,「対策実行意思」に対して与える影響力は小さかった．このことから，ボットウィルスの脅威が発生する確率を強調するような説得メッセージでは，効果的に対策を促すことができないと考えられる．さらに，対策に伴う負担やリスクが大きくても，対策実行の意思決定にあまり影響を与えないと考えられる．

実験データに対するモデルの適合度の調査で，適合度が低いという結果が得られた．Web アンケートの対策実行意思に関する質問項目の代わりに 6.3 で使用した実験データを用いてることから, この 2 つのデータの差が大きいほど, 6.1 で得られた適合度指標と 6.3 で得られた適合度指標の差が大きくなる．つまり，Web アンケートにおける対策実行意思と現実における対策実行とは乖離していることを示していると考えられる．

8. 今後の課題

今回はウィルス感染環境下における汎用モデルの検討を行った．

別の報告[8]では，脅威資料から脅威を正常に認知出来るのは，PC 習熟度が高習熟で，感染経験のある協力者だけであるという結果が得られている．中習熟および低習熟の協力者は，脅威資料から脅威を正常に認知出来ないという結果と，ウィルス感染経験のない協力者に比べて，感染経験のある協力者の方が脅威の認知効果が有意に高いという結果が得られている．

つまり，従来通りの脅威アピール説得が有効であるのは，感染経験を積んだ上級者レベルのユーザに限られ，一般的なレベルおよび初心者レベルのユーザに感染経験を積ませて認知効果を高めることは可能だが，脅威アピール説得で実際に対処行動実行を促すのは困難であることが考えられる．このことから，ユーザの属性によって，ウィルス対策実行意思の説明モデルが違うと考えられるので，今回作成したモデルに対して，属性による修正を今後検討する必要がある．

9. まとめ

ウィルス感染環境下における，集団的防護動機理論を基礎とした汎用モデルを作成し，分析を行い，各要因が対策実行意思に与える影響力について調査を行った．

分析の結果,「対策実行意思」に最も影響を与える要因は「効果性認知」であり,「生起確率認知」,「コスト認知」は,「対策実行意思」に対して与える影響力は小さかった．

さらに Web アンケートにおける対策実行意思と現実における対策実行とは乖離していることが確認できた．

参考文献

1) サービス妨害攻撃の対策等調査- 報告書 - http://www.ipa.go.jp/security/fy22/reports/isec-dos/2010_isec_dos.pdf

2) サイバークリーンセンター活動実績 https://www.ccc.go.jp/report/201101/1101monthly.html

3) 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.51.9, 2010

4) 独立行政法人情報処理推進機構・技術本部 セキュリティセンター “リスク認知と実行に関する調査報告書”, 2012.

5) 深田博己 編著: 説得心理学ハンドブック(北大路書房) , 2004

6) 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.

7) 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”, 情報処理学会研究報告,CSEC,2007(16),pp.327-331,2007.

8) 吉開, 神田, 浜津, 佐藤, 栗野: “情報セキュリティにおける脅威資料への認知効果に関する実証的検討”, 電子情報通信学会研究技報 SITE, 2013.5.