P-12

コンピュータウイルス対策実行に必要な情報の特定と その影響メカニズムに関する検討

Study on Information necessary to measure against a Computer Virus and its Impact Mechanism.

○浜津翔[1]，吉開範章[2]，栗野俊一[2]
*Hamatsu Sho[1], Noriaki Yoshikai[2], Shun-ichi Kurino[2]

Abstract: In the field of information security, even though an individual might intend to take protective action under the virus infection situation, it is an observable fact that many people do not actually do so. The persuasion methodology based on collective protection motivation theory is investigated for carrying out the coping behavior. This report shows a novel model for stimulating the measure intension against the virus infection, and its effectiveness by evaluating the conformity degree in Structured Equation Modeling.

１．まえがき

DDoS 攻撃は，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様々なサービス妨害を引き起こすインターネット上の脅威となっている[1]．対策は，色々な方法が提案されているが，まだ抜本的な解決策はない．一方，総務省および経済産業省主管のサイバークリーンセンターは，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，駆除ソフト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，DDoS 攻撃で踏み台として利用されるボットネットを無くす，新しい DDoS 攻撃対策となる．我々は，この仮説を実現するために，説得心理学を基礎とした情報セキュリティ対策について研究を行っている[5]．

今回，集団的防護動機理論を基に，ヒトの情報セキュリティ対策行動意思を評価するモデルを提案する．このモデルは，適合度指標により，データ分析に優れた特性を持つことが分かった．

２．集団的防護動機理論と対策実行意思モデル

防護動機理論とは，脅威アピールの説得効果を説明する理論であり，特に，集団的な対処行動を促す脅威アピール理論として，集団的防護動機理論が提唱されている[4]．

本研究では，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ヒトの情報セキュリティ対策行動意思をモデル化する．

集団防護動機理論では，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，責任認知，実行者割合認知，規範認知の 8 つが影響するものとしている．

従来は，この 8 つが対策実行意思に独立に影響するとして，モデルをたて，各因子が対策実行意思に与える影響度を検証されていたが，適合度が悪く，改善が必要であった[3]．

これまでの検討で，8 つの観測因子は，互いに独立ではなく，複数の潜在因子が関係していることが分かり，さらに，それらは，ウィルス感染経験，IT 知識，IT スキルの 3 因子が，認知効果に影響を与えているという予測が得られた．

そこで，ウィルス感染経験，IT 知識，IT スキルが，集団的防護動機理論における 8 つの認知要因に影響を与え，8 つの認知要因が対策実行意思へ影響を与える 3 段構成の対策実行意思モデル（図 1）を提案する．

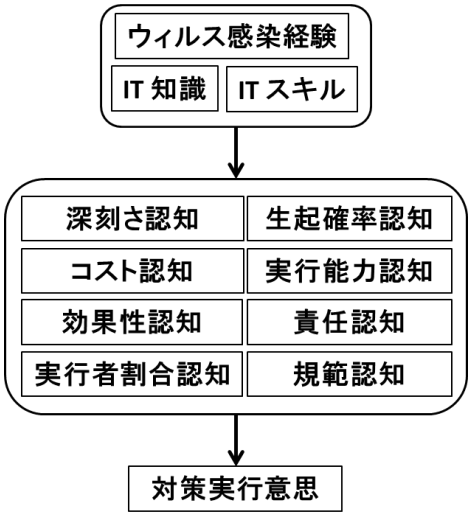

図 1. 対策実行意思モデル

１：日大理工・院（前）　２：日大理工・教員・数学

３．アンケート調査

個人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するかについて，Web を用いた質問紙調査をおこなった．調査は，株式会社クロス・マーケティングの保有する 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て行った．総回答数は 2266 人（男性 1162 人，女性 1104 人）であった．

今回の分析で用いたアンケートの項目は，ウィルス感染経験，IT 知識，IT スキル，集団的防護動機理論の 8 つの規定要因，そして対策実行意思の 12 事項に関する質問項目である．

４．対策実行意思モデルの分析結果と考察

４．１．対策実行意思モデルの作成と分析手順

まず，ウィルス感染経験(L)，IT 知識(M)，IT スキル(N)，深刻さ認知(A)，生起確率認知(B)，効果性認知(C)，コスト認知(D)，実行能力認知(E)，責任認知 (F)，実行者割合認知(G)，規範認知(H)，対策実行意思(Y)，それぞれの単純相関係数を参考にパスの有無を判断することで，パスモデルを作成した．ただし，感染経験，IT 知識，IT スキルの 3 つと，8 つの認知要因の関係については片方向への影響，8 つの認知要因と対策実行意思の関係についても片方向への影響を与えるとし，他の関係については両方向に影響し合うとした．単純相関行列を表 1 に示す．

図 1 の対策実行意思モデルに，単純相関係数の大きさを基準にパスを選択し，次に，対策実行意思に対する共分散構造分析を行う．

表 1. 単純相関行列

	Y	A	B	C	D	E	F	G	H	L	M	N
Y	1.00											
A	0.09	1.00										
B	0.16	0.41	1.00									
C	0.30	0.37	0.32	1.00								
D	0.00	0.15	0.14	-0.08	1.00							
E	0.13	0.05	0.12	0.05	0.49	1.00						
F	0.29	0.28	0.30	0.51	-0.04	0.05	1.00					
G	0.26	0.14	0.18	0.35	0.06	0.17	0.41	1.00				
H	0.24	0.19	0.23	0.35	0.01	0.06	0.50	0.51	1.00			
L	-0.05	0.06	0.00	0.05	-0.15	-0.47	0.10	-0.04	0.08	1.00		
M	0.03	0.08	0.12	0.04	-0.01	-0.10	0.06	0.00	0.02	0.20	1.00	
N	-0.02	0.15	0.07	0.06	-0.08	-0.33	0.12	-0.03	0.08	0.57	0.21	1.00

４．２．分析結果と考察

分析結果を図 2 に示す．図の数値は，標準偏回帰係数であり，当該予測変数（パスが出ている変数）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（パスを受けている変数）の平均的変化を意味する．

共分散構造分析では，モデルを評価するために適合

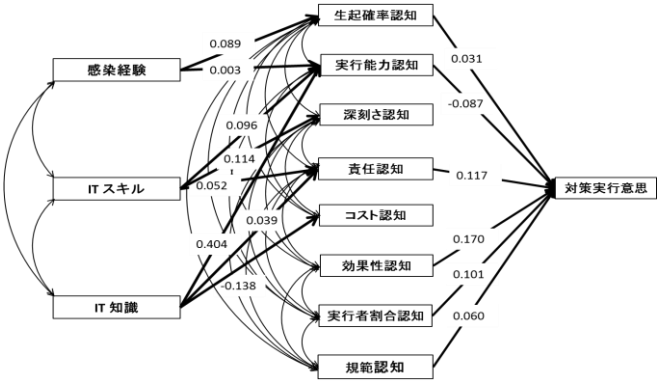

図 2. 対策実行意思モデルによる分析結果

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 = 0.985，AGFI = 0.961，RMSEA = 0.049，CFI = 0.973，SRMR = 0.035 となり，これまで我々が検討してきたモデルの中で，最も適合度が良く，分析結果の正当性基準（GFI, AGFI, CFI > 0.9, RMSEA, SRMR < 0.1）を満足する結果が得られた．

各認知要因が対策実行意思に与える影響力を比較すると「効果性認知」が最も影響を与えることが分かった．また，「深刻さ認知」，「コスト認知」，「生起確率認知」，「規範認知」は対策実行意思にほとんど影響を与えないということが分かった．このことから，現在に利用されている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．

今後は，対策実行を促す方法として，具体的にどのようなメッセージ，メディアを使えば，効果性認知を刺激できるかについて，検討する予定である．

参考文献

[1] 独立行政法人情報処理推進機構セキュリティセンター
“ サービス妨害攻撃の対策等調査 - 報告書 -”
http://www.ipa.go.jp/files/000014123.pdf

[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
“サイバークリーンセンター活動実績”
https://www.telecom-isac.jp/ccc/report/201101/1101monthly.html

[3] 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.

[4] 深田博己 編著: 説得心理学ハンドブック(北大路書房), 2004.

[5] 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, No.33, 2013.5