防護動機理論を用いたコンピュータウイルス対策への日豪認知比較の検討

新保佳奈[1]　吉開範章[1]

概要：米国の大手ネットサービスが大規模 DDoS 攻撃を受け，サービスを妨害される等，コンピュータウイルスの脅威は日々深刻さを増すが，一方で，PC がウイルスに感染したとしても，それを放置し対策を行わないユーザがいることが報告されている．このようなユーザに対し，説得心理学を用いてウイルス対策を実行する要因を明らかにし，その要因を刺激する説得により対策を実行させるための研究が行われている．しかし、このウイルス対策実行の要因は，その人の価値観や習慣等によって異なる可能性がある．そこで本研究では，日本の大学生とオーストラリアの大学生を対象に，質問紙調査を用いて，ウイルス感染状態を通知された際のウイルス対策実行の要因を調査・比較した．その結果，日本人は，対策の効果性についての認知が対策実行意思に影響を与えていることを確認したが，一方で，オーストラリア人は，与えられたウイルス感染情報自体を，信用しない傾向にあることが明らかになった．

Study on Comparison of Cognition of Computer Virus Measures based on Protection Motivation Theory

KANA SHIMBO[1]　NORIAKI YOSHIKAI[1]

1. はじめに

2016 年 10 月，Twitter，Amazon，Netflix 等の大手ネットサービスが, Mirai と呼ばれるコンピュータウイルスに感染させた PC を利用した大規模な DDoS 攻撃により, 5 時間にわたってサービスを妨害されるといった，深刻な被害を受けた[1]．この例のようにコンピュータウイルスの脅威は深刻であるが，その種類は日々新たに増え，あらかじめ，その感染を防ぐことは難しくなってきている．したがって，PC がウイルスに感染することを前提に, 感染時にユーザが PC をそのままにせず, 感染前の状態に戻すことが, 情報社会におけるセキュリティ対策としては極めて重要である．しかし現実には，所持する PC がウイルスに感染したとしても，それを放置し，対策を行わないユーザが多数存在することが報告されている[2]．そこで，ウイルス対策を行う要因を説得心理学を用いて明らかにし，その要因を刺激する説得により，対策を行わせる研究が行われている[3]．これまでの研究により，ウイルス対策実行意思に影響を与える要因は，対策の効果性についての認知であることがわかっている．しかし，この研究は日本人のみを対象に行われており，ウイルス対策実行意思を促す要因は，人の価値観や習慣等によって異なる可能性がある．そこで，本研究においては，日本の大学生とオーストラリアの大学生を対象に，ウイルス対策の要因を調査し，その違いを検討した．

本論文の構成は，以下の通りである．まず，2 章にて，先行研究の状況と現状の課題，そしてその課題に対する本研究のアプローチを示す．3 章にて，本研究における質問紙調査の方法の概要を示し, 4 章にその調査結果, 5 章に調査結果に対する考察，そして 6 章にまとめを示す．

2. 先行研究状況

2.1 説得心理学の応用

文献[3]において，PC がボットウイルスに感染した状況は PC のユーザにとって脅威であると仮定し，脅威の危険性を強調して説得を行う「脅威アピール[4]」を用いて，ユーザにボットウイルス対策を実行させるための研究が行われている．以下に，その概要を述べる．

2.1.1 集合的防護動機理論

脅威アピールにおいて，説得の受け手が脅威への対処行動を行う要因は，防護動機理論によって説明されている．また，脅威への対処行動を集団で行うことによってはじめて脅威が低減される場合，その対処行動を行う要因は，集合的防護動機理論[5]によって説明されている．ボットウイルスに感染した PC で構成されるボットネットと呼ばれるネットワークは，DDoS 攻撃やスパムメールの大量送信などの脅威を引き起こす．その脅威を低減するためには，各ユーザがボットウイルス対策を行う必要があることから，文献[3]では，集合的防護動機理論を適用してボットウイルス対策実行意思に影響を与える

1 日本大学大学院・理工学研究科
Graduate School of Science and Technology, Nihon University

表 1. 集合的防護動機理論による脅威への対処行動の要因
Table 1. Factors of coping behavior for threat based on collective protection motivation theory.

認知要因	内容
深刻さ認知	当該の脅威に関する深刻さについての認知
生起確率認知	当該の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	当該の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添っているかどうかについての認知

要因を明らかにし，その要因を刺激するような説得を行うことで，ウイルス対策を行わないユーザに対策を実行させることが可能になると仮定している．

2.1.2 対策実行意思モデルの提案

集合的防護動機理論においては，脅威及びその対処行動に関する 8 つの認知（表 1.参照）が，対処行動の実行意思に影響を与える要因であるとされている．文献[3]では，集合的防護動機理論を用いて，ボットウイルス対策の要因を説明する「対策実行意思モデル」を提案している（図 1.）．このモデルでは，対策実行意思に対し，集合的防護動機理論に基づくボットウイルスに対する 8 つの認知が影響を与えているとし，さらにそれらに対し，「IT 知識」,「IT スキル」,「ウイルス感染経験」の 3 つの潜在因子が影響を与えるとしている．

2.1.3 質問紙による調査とモデルの有効性

文献[3]では，ウイルス感染状況を想定した質問紙調査を行い，その調査データに対し，対策実行意思モデルに基づき作成したパスモデルにより共分散構造分析を行っている．その結果，モデルが高い適合度で調査データを表したことが示されている．また，共分散構造分析の結果について，対策の効果性認知が，対策実行意思に影響を与えることがわかっている．

2.2 研究の課題

先行研究では，日本人のみを対象に調査を行っていたが，

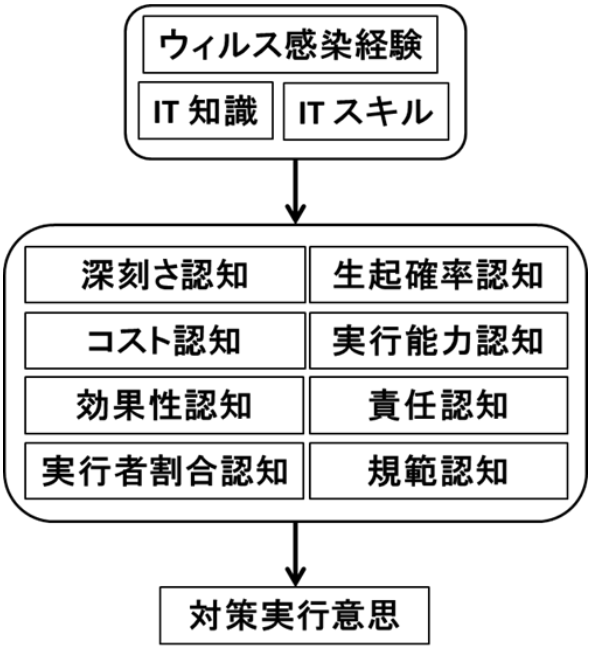

図 1. 対策実行意思モデル
Fig 1. Protection Motivation Model for bot virus.

ウイルス対策の要因は，その価値観や習慣等によって異なる可能性がある．

ウイルスに感染している PC のユーザに対し，感染を気付かせ，PC を感染前の状態に戻すよう注意喚起を行う取り組みが，実際に行われている．

日本において，総務省主管の ACTIVE[6]（以前のサイバークリーンセンター）が，ACTIVE に協力している ISP を通じて，インターネット上でウイルスに感染している PC とそのユーザを特定し，ユーザに感染を呼びかける注意喚起活動を行っている．この活動により，日本におけるボットウイルス感染率が，2~2.5%から 1%に削減されたという効果が出ている[7].

一方，オーストラリアにおいても，通信メディア庁主管の AISI[8]が，日本と同様に，ウイルス感染した PC のユーザにウイルス対策を促す活動を行っている．しかし，オーストラリアでは，AISI の活動報告は存在せず，さらに，その活動に対し、インターネット上にて懐疑的な意見が多数見受けられる[9].

このように，2 カ国において同じ活動が行われているが，その効果についての比較検討をした報告は存在しない．そこで，日本人とオーストラリア人という，異なる国民性を持った人の間では，ウイルス対策に対する態度が異なると考え，本研究では，日本人とオーストラリア人，それぞれのウイルス対策実行意思に影響を与える要因を分析し，その比較を行った．

3. 調査方法

基本的には，文献[3]に従っている．ボットウイルス感染状況を想定し，ウイルスに対しどのように認知するか，ま

平素から、弊社サービスをご利用頂き、誠にありがとうございます。

お客様のパソコンからボットの感染活動に伴う通信が検出されましたので、感染者に対して、ボットの駆除を案内してほしいとの連絡が弊社に寄せられました。

弊社において調査しました所、お客様のご契約回線に接続されたコンピュータが感染していることが判明しました。

ボット検出日時：2016/XX/XX/　23：36

つきましては、下記のボット対策サイトへアクセス後、サイト内の手順に従って、ボット駆除の実施や再発防止の実施をお願い申し上げます（https://www.xxxxxxxx.co.jp）。

図 2. 提示する文章

Fig. 2 Sentences showed in the questionnaire survey.

た，対策を実行する意思があるかについて，質問紙を用いて調査する．そして調査結果に対し，対策実行意思モデルに基づき，共分散構造分析を行い，ウイルス対策実行意思に影響を与える要因を明らかにする．

3.1. 質問紙調査

3.1.1. ウイルスの脅威の理解

まず，回答者に対し，ボットウイルスとその脅威を説明するビデオを提示し，ボットウイルスに感染することによるリスクを理解させる．

3.1.2 ウイルス感染状況の想定

次に，回答者に対し，「回答者の PC がボットウイルスに感染したこと」と「ボットウイルスの駆除方法と駆除の催促」を知らせる文章(図 2.)が届いたという情報を提供する．文章の送信元は，日本の場合は「政府から委託を受けた ISP」, オーストラリアの場合は「政府」とした．これは，極力，文章が信頼できるものであることを示す為である．

3.1.3 質問紙

文章が届いたという仮定の下，文章によって提示されたボットウイルス対策を実行する意思があるかどうか，また，集合的防護動機理論に基づき，対処行動に影響を与えると考えられる，ボットウイルスに対する認知について，調査する．対策実行意思モデルにおいて，各認知要因に影響を与えるとされている「IT 知識」「IT スキル」「ウイルス感染経験」についても調査する．質問項目は付録 1. の通りである．また，提示する文章に対する信頼度，文章を読む意思を調査するための質問項目も設けた．

3.2 分析手法

以下の手法で分析を行う．

1）質問紙調査にて得た回答データから対策実行意思モデルにおける変数間の単純相関係数を算出する．

2）有意な相関を持つ変数間に対し，対策実行意思モデルに基づき，パスモデルを作成する．

具体的には，集合的防護動機理論による 8 つの認知と対策実行意思との間に相関がある場合，認知要因から対策実行意思への片方向への影響があるとし，パスを引く．8 つの認知要因と，その潜在因子との間に相関がある場合，潜在因子が認知要因に片方向の影響を与えているとし，パスを引く．認知要因間，または潜在因子間に相関がある場合，双方向のパスを引く．

3）回答データに対し，2）のパスモデルを用いて，共分散構造分析を行う．

4. 調査結果

4.1 日本人に対する調査結果

4.1.1 調査条件

日本大学理工学部数学科の 1 年生 114 人を対象に, Web アンケートを用いて質問紙調査を行った．

4.1.2 調査結果の分析

まず，質問紙調査にて得た回答データから，対策実行意思モデルにおける変数間の単純相関係数を算出した（表 2.）．そして，各変数間のうち，有意な相関を持つ変数についてパスを引いたパスモデルを作成した．

そして，作成したパスモデルを用いて，共分散構造分析を行った（図 3. ）．回答データに対する，このモデルの適合度は，表 3 の通りとなった．GFI，AGFI，CFI は値が 0.9 以上かつ，RMSEA，SRMR は値が 0.1 以下であれば適合度が高いとされる．今回のパスモデルは，十分，適合度が高いと判断できる．

4.1 オーストラリア人に対する調査結果

4.1.1 調査条件

シドニー大学 IT スクールの学部生（86 人）を対象に，日本人と同様，Web アンケートを用いて質問紙調査を行った．

4.1.2 調査結果の分析

提示した文章の内容に対し，回答者の 89%が「信用しない」と回答した(図 4.)．つまり，オーストラリア人の回答者の多くが「ウイルス感染状況」を想定するための文章を信用しなかった為，集合的防護動機理論に基づく質問に対し，有意なデータを収集することができず，「ウイルス感染状況において，対策実行意思があるかどうか」を調査することができなかった．

5. 考察

5.1 日本人に対する調査結果の考察

質問値調査データの分析結果から，日本人においては，

表 2. 単純相関行列（日本）

Table 2. Simple correlation matrix (Japan).

	Y	A	B	C	D	E	F	G	H	L	M	N
Y	1.000											
A	−0.064	1.000										
B	0.012	0.087	1.000									
C	0.484	0.249	0.076	1.000								
D	−0.185	0.009	0.187	−0.274	1.000							
E	−0.050	−0.146	−0.017	−0.298	−0.251	1.000						
F	0.221	0.064	0.162	0.399	−0.184	−0.057	1.000					
G	0.248	0.062	−0.023	0.289	0.027	−0.075	0.289	1.000				
H	0.311	0.061	0.150	0.335	−0.060	0.096	0.466	0.398	1.000			
L	−0.180	0.035	−0.059	−0.216	0.062	0.245	−0.062	−0.094	−0.195	1.000		
M	−0.008	0.005	0.109	−0.055	0.011	0.062	0.109	−0.197	−0.011	0.247	1.000	
N	0.015	0.091	0.065	0.040	0.024	0.227	0.040	−0.164	−0.077	0.513	0.246	1.000

Y：対策実行意思　A：深刻さ認知　B：生起確率認知　C：効果性認知　D：コスト認知　E：実行能力認知　F：責任認知　G：実行者割合認知　H：規範認知　L：IT 知識　M：ウイルス感染経験　N：IT スキル

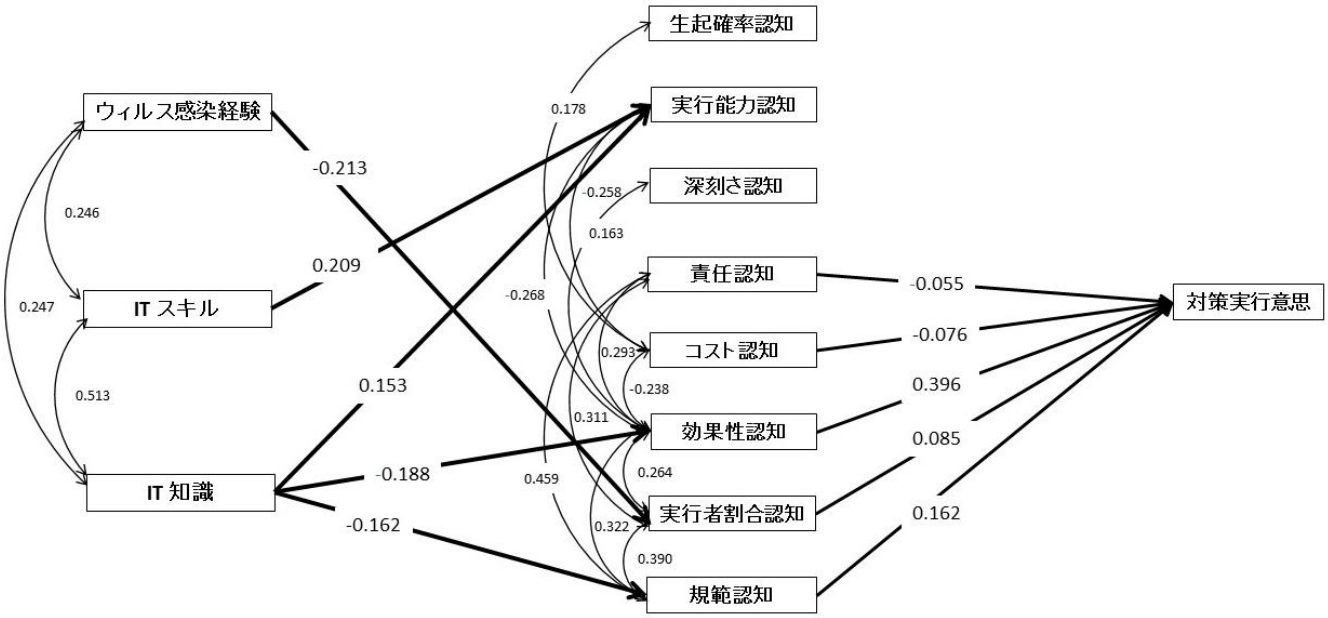

図 3. 共分散構造分析の結果（日本）

Fig 3. Result of Covariance Structure Analysis.

表 3. 適合度指標（日本）

Table 3. Goodness of fit (Japan).

GFI	0.937
AGFI	0.891
CFI	0.996
RMSEA	0.012
SRMR	0.064

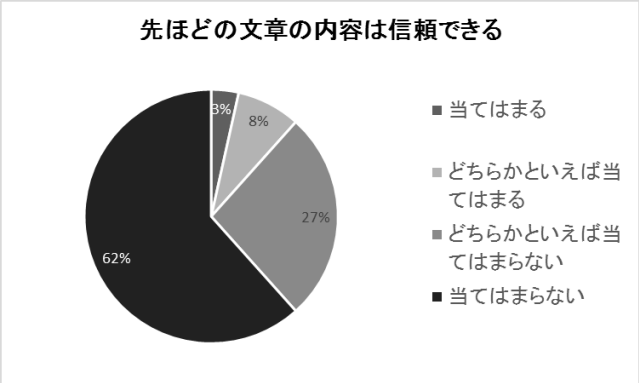

図 4. 文章の内容への信頼度（オーストラリア）
Fig 4. Trust of the content in the sentence (Australia).

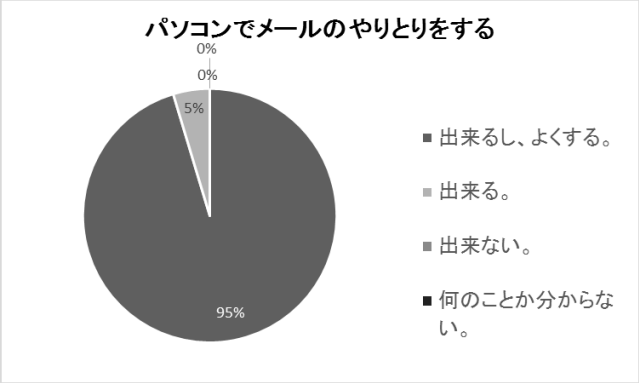

図 5. メールの使用率（オーストラリア）
Fig 5. Usage rate of email (Australia).

提示したボットウイルス対策に対する効果性認知が，対策実行意思に影響を与えていることがわかった．

先行研究[3]においても，同様の結果が出ており，先行研究の有効性を確認することができた．

5.2 オーストラリア人に対する調査結果の考察

質問紙調査データの考察結果から，オーストラリア人は，提示した文章の内容を信用しない傾向にあることがわかった．ウイルス感染状況にあるユーザに対し，感染しているという情報を提示したとしても，その情報を信用してもらえないことは問題である．

そこで，オーストラリア人の調査対象者が，なぜ提示された情報を信用しなかったのか，その原因について，考察を行った．

5.2.1 情報の伝達手段の信頼度

一般的に，個人にあてて文章が送られて来る場合，手紙の郵送か，または，メールを通じて送られることが考えられる．今回は，回答者のうち 4 人が「提示された文章はメールで送られてきた」と考えていた．そこで，メールを介する情報の信頼性について考える．

標的型攻撃やフィッシング詐欺など，メールを利用した攻撃は多く存在しており，メールで得る情報に対し，懐疑的になる人は多いと考えられる．オーストラリアの回答者のほとんどが，IT に関する専門的知識を有し，高度な IT スキルを身につけており，メールに関する詐欺について，59%が標的型攻撃を知っていて，また，88%がフィッシング詐欺を知っていた．このことから，メールに関する詐欺についての知識を持っている回答者が多いことがわかる．

一方で，メールという情報通信手段は，世界中において普及している．今回の回答者についても，95%が，メールを頻繁に利用することがわかっている（図 5.）．

以上から，メールにて情報が送られてきた場合，一般的には，その情報が信用できるかどうか，内容を吟味し，慎重に判断することが考えられる．今回の回答者は，提示した文章に対し，6 割以上が，最初から最後まで文章を読むと回答している（図 6.）．

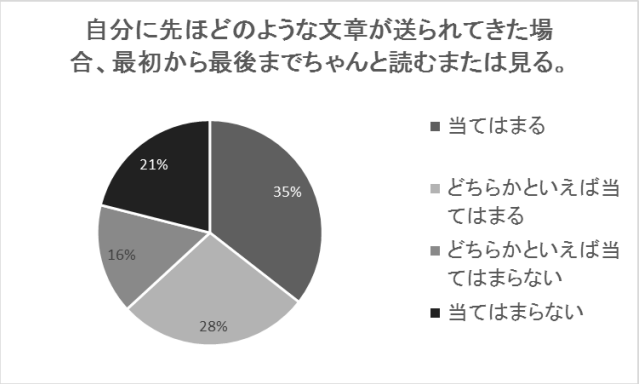

図 6. 文章を読む意思（オーストラリア）
Fig 6. Intention of reading the sentence (Australia).

5.2.2 情報の内容の信頼度

提示された文章に対し，表 4. のように，フィッシング詐欺だと考えた回答者が複数いた．では，なぜ提示した文章を，詐欺であると考えたのかについて，考察する．

表 4. 提示された文章に対するフィードバック
Table 4. Feedback to the sentence.

「その文章」が本当に政府からのものであるか，または政府からのメールにより名言されているものであるか，不明瞭である．私はこれをフィッシングメールと確信する．
私はこの調査に，「上にある例のメールはスパムメールである」と気づきながら回答した．
明らかな釣りである
私は，これを，フィッシングの攻撃を受けやすいかどうかをテストするために設計したのだと確信している（だから「政府」のメールを信頼していない）．
私はこのような偽物のリクエストを，いつも，時には電話でも，受け取る．

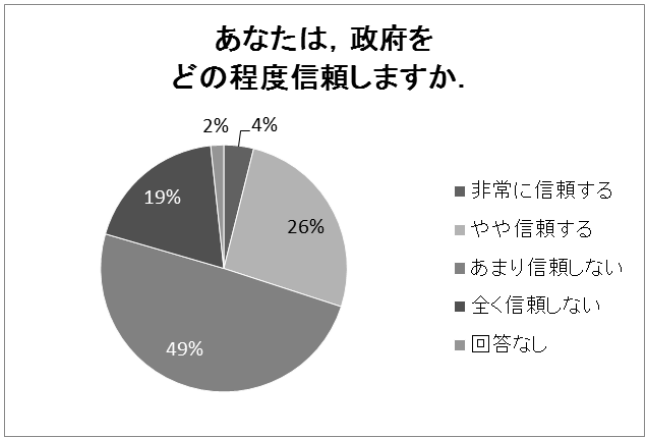

図 7. 政府への信頼度（オーストラリア）
Fig 5. Trust of the government (Australia).

今回提示した文章は,ボットウイルス対策を行うために，Web ページへアクセスすることを誘導する内容が含まれている．一方，フィッシング詐欺も，重要な個人情報を盗み出すために，詐欺の対象に対し，送信者を詐称したメールを用いて，偽の Web ページへアクセスすることを誘導する行為であり[10]，今回提示した文章の内容は，フィッシング詐欺にて求められる行為と同様の行為を求めていることから，詐欺であると判断した回答者がいたと考えられる．

5.2.3 情報の送信者への信頼度

オーストラリア人の場合は，情報の発信源を「政府」としたことも、詐欺だと思われた原因となった可能性が考えられる．図 6 の通り，文章を最後まで読まないと考えた回答者も 3 割以上いたが，その中でも，フィッシング詐欺であると考えた回答者がいることがわかった．この回答者については，「政府から文章が届いた」という情報から，文章の送信者が詐称されているのではないかと考え，文章を読まなかった可能性が考えられる．

また，世界価値観調査［11］によると，オーストラリア人の 68%が政府を信頼していない（図 7. ）．つまり，政府を信頼していないため，政府から届いた情報について信用しないと考えた可能性がある．

6. まとめ

国民性により，ウイルス対策実行意思に影響を与える要因が異なるかどうかについて，日本の大学生とオーストラリアの大学生を対象に調査を行った．

その結果，日本人は，ウイルス対策の効果性認知が影響を与えることがわかり，先行研究の有効性を確認できた．今後は，対策の効果性を示すような説得メッセージを作成し，その効果の検証を行う必要がある．

一方で，オーストラリア人は，「ウイルスに感染している状況である」ことを知らせる情報を信用しない傾向にあることがわかった．つまり，日本人にウイルス対策を実行させるためには，対策の効果性を強調することが重要である一方で，オーストラリア人にウイルス対策を実行させるためには，まず，ウイルス感染状況を知らせる情報の提供方法について，見直す必要があることがわかった．特に，提示した文章を詐欺だと考える人が多いため，詐欺だと判断されないような，情報の伝達手段や発信源，文章の表現を工夫するなどの改善が必要である．

謝辞　調査データの収集・分析に御協力いただいたシドニー大学 Stavrakakis 博士に，感謝致します．

なお，本研究は，科学研究費補助金 No.26330386 による助成を受けて実施した．

参考文献

[1] 情報処理推進機構セキュリティセンター : 情報セキュリティ 10 大脅威，情報処理推進機構セキュリティセンター(オンライン)，入手先〈https://www.ipa.go.jp/files/000058504.pdf〉(参照 2017-05-02).
[2] 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，情報処理推進機構セキュリティセンター(オンライン)，入手先〈https://www.telecom-isac.jp/ccc/report/201101/1101monthly.html〉(参照 2017-04-24).
[3] 浜津翔，栗野俊一，吉開範章：集団的防護動機理論に基づく情報セキュリティ対策実行意思モデルの提案とその活用，情報処理学会論文誌，Vol.56. No.12，pp.2200-2209(2015).
[4] 深田博己：説得心理学ハンドブック，北大路公房(2002).
[5] 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，No.1，pp.54-61(2005).
[6] ACTIVE：ACTIVE(マルウェア対策支援)，ACTIVE(オンライン)，入手先〈http://www.active.go.jp/〉(参照 2017-04-24).
[7] 有村浩一：ボット対策プロジェクト「サイバークリーンセンター」からみた国内のマルウェア対策，会誌「情報処理」，Vol.51，No.3，pp.275-283(2010).
[8] ACMA : Australian Internet Security Initiative(オンライン)，入手先〈http://acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/〉(参照 2017-05-02).
[9] ACMA : The AISI: interviews with industry(オンライン)，入手先〈http://acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/the-aisi-interviews-with-industry〉(参照 2017-05-02).
[10] 総務省：フィッシング詐欺に注意(オンライン)，入手先〈http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/05.html〉(参照 2017-05-02).
[11] World Values Survey : WVS Database(オンライン)，入手先〈http://www.worldvaluessurvey.org/wvs.jsp〉(参照 2017-05-02).

付録

A.1 質問項目

3.1.3 節で示した，質問紙調査における質問項目を表 A.1 に示す.

表 A.1 質問項目
Table A.1 Item in the questionnaire.

変数	質問文	回答
対策実行意思	自分に先ほどのような文章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	ボットウイ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.	
起確率認知	将来，自分自身の PC がボットウイ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，ボットウイ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イルス対策は，多くの人が実行しているだろう.	
規範認知	自分がボットウイ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.	
IT 知識	あなたのパソコンの習熟度について最も近いものをひとつお選びください.	選択肢から１つ回答
ウイルス感染経験	あなたはこれまでに，お使いになっているパソコンがウイルスに感染した経験がありますか．あてはまるものをお選びください.	「ある」「無い」「わからない」の３つから１つ回答
IT スキル	あなたのメディア操作のスキルについておうかがいいたします．あなたは以下の各操作をおこなうことができますか．あてはまるものをお選びください. ・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）やグーグル（ｇｏｏｇｌｅ）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 DVD 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 ・Facebook や Twitter 等の、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	10 個の IT スキルの例に対し，それぞれ 4 件法で回答