情報処理学会論文誌 Vol.61 No.12 1845–1858 (Dec. 2020)

個人のインターネット利用における セキュリティ対策行動開始のきっかけの分析

澤谷 雪子[1,a)] 佐野 絢音[1] 山田 明[1] 窪田 歩[1]

受付日 2020年3月6日, 採録日 2020年9月10日

概要：インターネット利用時のセキュリティ対策が様々な被害を防ぐにもかかわらず，対策を行っていない一般ユーザは一定数存在する．このようなユーザへの働きかけにより適切なセキュリティ対策行動を促す手法を検討しており，本論文では，対策行動開始のきっかけを分析し，これらのきっかけと行動との関係を明らかにすることを目的とする．デプスインタビューによりセキュリティ対策行動を開始した事例について調査を行い行動開始のきっかけや行動の促進・阻害要因に関する仮説立てを行った後，454 名のインターネットユーザに対しアンケート調査を実施し，仮説の検証を行った．その結果，以下の知見を得た．まず，セキュリティ意識の高まるきっかけは「環境変化」「対策推奨」「脅威伝聞」「脅威体験」の 4 つに分類することができ，これらの「きっかけとなる状況との遭遇」に加えて「対策の重要性の認識」が対策行動実施の促進要因となるが，「対策への不満」が阻害要因となりうる．特に，ICT 理解度の低いユーザは，「きっかけとなる状況との遭遇」とともに「対策の重要性の認識」も高まるが「対策への不満」も高まり，対策行動に移行しないユーザが多いことが示された．

キーワード：セキュリティ対策行動，セキュリティ意識，ICT 理解度，構造方程式モデリング

Analysis of Trigger Factors for Starting Good Security Behavior of Internet Users

Yukiko Sawaya[1,a)] Ayane Sano[1] Akira Yamada[1] Ayumu Kubota[1]

Received: March 6, 2020, Accepted: September 10, 2020

Abstract: There are still a fraction of the Internet users who does not take security behavior. In this paper, we conducted an interview with the Internet users who had no/little awareness of security behavior but take behavior and created the hypothesis of the factors that related to the change of users' behavior. Then we carried out a questionnaire to 454 participants and conducted quantitative analysis. As a result, we found that four elements "environmental changes," "recommendation of security behavior," "experience of someone encountering a threat," and "experience of user encountering a threat" raise users' security awareness. We also found that the two factors, the trigger factor composed of these elements and the factor "recognition of importance of measurements" are the promotive factors and "dissatisfaction to the security behavior" is the inhibitive factor. In addition, the promotive factors and inhibitive factor are highly correlated among one another and the impact of inhibitive factor to the behavior is higher in the case that the level of users' understanding of ICT is lower.

Keywords: security behavior, security awareness, understanding of ICT, structural equation model

1. はじめに

インターネットにおけるマルウェアやフィッシング詐欺など様々な攻撃に対し，OS アップデートやウィルス対策ソフトの利用など，個々のユーザがセキュリティ対策を行

[1] 株式会社 KDDI 総合研究所
KDDI Research, Inc., Fujimino, Saitama 356–8502, Japan
[a)] yu-sawaya@kddi-research.jp

う必要があるが，対策を行っていない一般ユーザは一定数存在する．平成 30 年度の調査によればインターネットを利用している世帯のうち，何らかのセキュリティ対策を実施している世帯の割合は 68.5%となっている [1]．実施しているセキュリティ対策別の実施割合が最も高い対策で「セキュリティ対策ソフトの導入もしくは更新」が 53.4%と半数程度である．また次いで「セキュリティ対策サービスの新規契約もしくは更新」(24.2%) となっており，「不確かなインターネット回線には接続しない」については 18.8%程度と，総じて低い．そこでセキュリティ対策に興味関心がないユーザ，もしくはセキュリティ対策に関心はあるが行動に移していないユーザに対し，有効なセキュリティ対策推進施策が必要となる．

ここで，本研究で扱うセキュリティ対策について定義する．文献 [2] に基づくと，情報セキュリティ対策の基本としてソフトウェアの更新，ウィルス対策ソフトの利用，パスワードの管理・認証の強化，設定の見直し，脅威・手口を知り対策するという 5 点が必要とされている．この 5 つの中で「設定の見直し」に関しては主に IoT 機器の設定に関する対策について記載されており，IoT 機器の普及率 (2019 年度の調査で世帯保有率 6.9% [3]) を考慮すると調査対象がきわめて限定的になる可能性がある．そこで，本論文では，文献 [2] で必要とされている 5 つの中で「ソフトウェアの更新」,「ウィルス対策ソフトの利用」,「パスワードの管理・認証の強化」,「脅威・手口を知り対策」の 4 つをセキュリティ対策として扱う．

セキュリティ対策の実施には促進要因と阻害要因が存在することが明らかになっており [4], [5]，対策行動実施者の促進要因と阻害要因のバランスによりセキュリティ対策行動の実施・未実施を分けていると考えられる．しかし，対策未実施者を実施者に促すための決め手となる要因が明らかでない．

そこで本論文では，対策の未実施状態から実施状態へと移行するための意識変化・行動開始のきっかけを分析し，これらのきっかけと対策行動との関係を明らかにする．実施していないセキュリティ対策があったが対策を行うに至った体験を持つインターネットユーザを対象としたインタビュー調査により，無関心，または関心があったが行動に移していなかった状態から対策行動実施への遷移における要因の仮説立てを行い，次に 454 名のインターネットユーザに対しアンケート調査を実施し，仮説の定量的検証を行った．

調査の結果，以下のことが明らかになった．まず，セキュリティ意識の高まるきっかけは「環境変化」「対策推奨」「脅威伝聞」「脅威体験」の 4 つに分類することができ，これらのきっかけとなる状況との遭遇率と実際の意識の高まりを考慮すると「脅威伝聞」が多くのユーザの意識を高めていると考えられる．また，これらの「きっかけとなる状況との遭遇」に加えて「対策の重要性の認識」が対策行動実施の促進要因となるが,「対策への不満」が阻害要因となりうる．さらに，ICT 理解度の低い群では,「きっかけとなる状況との遭遇」とともに「対策の重要性の認識」も高まるが「対策への不満」も高まり，ICT 理解度の高い群と比べて対策行動に移行するユーザの割合が少ない．

これらの結果に基づき，情報提供の手段や内容を工夫することや，ICT 理解度に応じてそれぞれ異なる働きかけを行うことにより，適切なセキュリティ対策行動を促すことができると考えられる．

本論文では，セキュリティ意識の高まりと行動の関係に関する分析結果を詳細に述べる．2 章以降の構成は以下のとおりである．まず，2 章で本論文の検討に関連する既存研究を示し，3 章で本研究の方針を整理する．次に 4 章および 5 章でそれぞれ定性調査，定量調査の結果を示す．6 章で考察を行い，最後に 7 章で本論文のまとめを行う．

2. 関連研究

2.1 意識・心理とリスク

認知傾向要因や意識・性格などとリスクや被害との遭遇の関係を分析した既存研究が存在する．

文献 [6] では，サイバー攻撃などによる IT 被害経験者を対象としたアンケート調査により，被害を受けた原因を探っている．セキュリティ対策への心理負担度やコスト認知，ベネフィット認知などのユーザ要因と，ウィルス感染や不正利用，プライバシ情報漏えい，詐欺などへの被害経験との相関関係を解析している．この文献では，被害の種別によって，ユーザの心理的・行動的傾向との相関が異なることを明らかにしている．

文献 [7] では，PC の操作ログと，認知傾向要因，および IT リスクとの関係性をそれぞれ解析しており，利用規約説明の表示時間の短さとベネフィット認知の強さ，および，ベネフィット認知とウィルス感染リスクの相関の高さの相関性から，利用規約表示時間の短いユーザのウィルス感染リスクが高い可能性があると述べている．

2.2 意識・心理と行動

認知傾向要因や意識・性格などと行動の関係性を分析している既存研究も多数存在する．

文献 [4] では，人がなぜセキュリティ行動をしないのかという観点から，セキュリティ対策に対する認知，セキュリティスキル，知識と「セキュリティ対策行動」に関する因果関係を分析しており，セキュリティ対策への阻害因子として「無効感」「コスト感」があげられ，また促進因子として「貢献感」「関心」「外部要請」があげられている．

文献 [8] ではセキュリティ対策行動としてウィルス対策ソフト・OS・ソフトウェアの更新に焦点を絞り，Big Five を含めた性格要因，認知要因，経験要因との関連性を分析

しておりPCユーザ，スマートフォンユーザの行動に与える性格要因がそれぞれ異なることを明らかにしている．

文献 [9] では組織におけるセキュリティ対策行動は脅威の感受性，脅威の重大さの認知，組織に対する満足度が影響していることを重回帰分析により分析している．また，文献 [10] では，セキュリティ対策行動には知識よりも対策できる能力があるという自己認識や自信が関係していることを重回帰分析により明らかにしている．

セキュリティ意識の向上を図り対策行動を促す研究も行われている．文献 [11] では，一般のIT利用者に対して，セキュリティ意識の高まりと行動を促すために，マンガをベースにしたリスク学習とインタラクティブな形式での学習フレームワークを提案しており，これがITに詳しくない利用者の認識を向上させることに貢献することを分析している．文献 [12] では，ウィルスに感染するまでの過程を体験的に学習する授業実践を行っており，感染の体験によりリスクの理解が深まることを確認している．

3. 本研究の方針と手順

本論文は対策行動を開始するきっかけと，対策行動を促すための要因を明らかにすることを目的としている．これを実現するために，定性調査で傾向分析や仮説立てをしたのち，定量調査により，傾向の量的検証および仮説の検証を行う．

インタビューなどの定性調査において，セキュリティ対策を必要と思っておらず，実施していないユーザに対してその理由を聴取した場合，ユーザ自身がその理由を認知していない場合には明確な回答を得ることができない．また，「どのようなサービスや働きかけがあれば対策をするか」という質問に対する回答を得たところで実際に対策を実施するかどうかまでは不明となる．一方，何らかの対策を開始したユーザに対してそのきっかけや認知したこと，対策行動に移した際の経緯や，他に対策行動に移せなかったことがあればその経緯を聴取し，これらを明らかにすることにより，現在対策を対策の必要性を感じておらず実施していないユーザに対してきっかけを与える方法や促進および阻害要因に関する仮説立ておよび定量調査へとつなげることができる．

そこで，本論文では，はじめに「実施していないセキュリティ対策があったが，対策を行うに至った体験」を持つインターネットユーザを対象とし，インタビュー調査を実施する．無関心，または関心があったが行動に移していなかった状態から対策行動実施へ移した経験から，何がきっかけとなりどのように感じて行動に移したかを聴取することにより，対策行動へとつながる要因の仮説立てを行う．次に，これらの仮説について定量的検証を行うためにアンケート調査を実施し，ユーザのセキュリティ対策行動促進要因に関する考察を行う．

4. 定性調査

セキュリティ対策行動につながる促進要因や阻害要因，および行動に至るまでの各要因の関係性の仮説を立てるためにインタビュー調査を行う．

4.1 調査概要

4.1.1 対象者選定

「実施していないセキュリティ対策があったが，対策を行うに至った体験」を持つインターネットユーザを対象とし，無関心，または関心があったが行動に移していなかった状態から対策行動実施への遷移に関連する要因を調査するにあたり，対象者は以下のように選定した．

- PC・スマートフォン（以下スマホ）などの端末およびインターネット利用に関するセキュリティ対策で，一定期間の未対策状態から対策への行動開始経験を1つでも有すること
- 行動開始のきっかけを記憶していること

上記に該当する対象者をリサーチ会社に登録しているウェブモニタから選定した．

4.1.2 聴取内容

主な行動促進および阻害要因の探索と，対応するそれらの関係性の構造を把握するために，以下のような態度および行動を変えた要因やプロセスを対象者から聴取する．

- セキュリティ意識の高まったきっかけ：無関心，または関心があったが行動していなかった状態から意識の変化やセキュリティ対策行動につながったきっかけとなる出来事
- 意識の高まりにともなうセキュリティ対策への認識と行動の変化：きっかけを契機に意識したこと，実施したセキュリティ対策およびしようと考えたがしなかった対策，およびその理由

4.1.3 聴取方法

インタビュー形式には，主に座談会形式で討議するフォーカスグループインタビューと1対1で行うデプスインタビューが存在する．グループインタビューは対象テーマについて深くグループに対し聴取する手法であり小集団で話すことによりグループ内の相互影響を生かしながら聴取する方法である．デプスインタビューはグループでは聞くことのできない個人的・専門的な情報を多く引き出す手法である [13]．聴取する内容は個人の記憶の回想をともなう個人に完結した内容であることからデプスインタビュー形式とした．聴取の流れとしては，PCやスマホの利用時における以下のような経験に対し，回想をもとに対象者に自由に述べてもらう形式とした．

- セキュリティ意識の高まった出来事とそのときの意識
- 実施しているセキュリティ対策と実施している経緯
- 実施しようと思ったが実施していない対策とその経緯

表 1 対象者属性
Table 1 Information of participants.

対象者#	性別	年齢	職業
1	男性	60代	会社員
2	男性	40代	会社員
3	女性	40代	専業主婦
4	女性	20代	学生
5	女性	40代	個人事業主
6	男性	20代	会社員
7	女性	20代	学生
8	女性	60代	専業主婦

4.2 調査対象者

ユーザビリティテストなどの定性調査において，対象者が5名を超えると得られる新たな知見は他の対象者と重複し，網羅性が確保できるという経験則に基づく試算 [14], [15] を参考に，インタビュー対象者を8名とした．これにより，網羅性に加え，インタビュー対象者間の発言の共通性も確認することができると期待できる．

対象者の属性は**表 1** に示すとおりである．性別については男性が5名，女性が3名と男性の方がやや多いが，人口の男女比に対して有意な偏りがない（Fisher の直接確率検定に基づく）ため対象者の内訳としては問題ないと考えられる．また，年代については20代，40代，60代とやや離散的であるが20代～60代と総じて広く，職業についても会社員，個人事業主，専業主婦，学生と複数の業種となっていることから，特定の性年代，および職業に偏らない幅広い意見を得ることができ，仮説立案につながると考えられる．

4.3 結果

4.3.1 対象者の特徴

インターネット上のサービスやセキュリティ対策などのICTへの理解について，インタビュー対象者間でばらつきがあった．ICTへの理解が低い対象者の最も顕著な共通項として，(1) 迷惑メールや詐欺サイトを自分で判断できないこと，および (2) 端末の情報漏洩について端末紛失や盗難による漏洩と比較してインターネットを介した漏洩に対する懸念が薄いことがあげられた．そこで (1)，(2) のいずれにも該当するICT理解度の低い対象者とし，いずれも該当しない対象者をICT理解度の高い対象者とする．それぞれの内訳は以下のとおりである．

- ICT理解度の低い対象者：#1，#3，#5，#7，#8
- ICT理解度の高い対象者：#2，#4，#6

やや，ICT理解度の低い対象者が多いが，差は小さいことから，この分類により，ICT理解度での共通性や相違性を確認することができ，仮説立案につながると考えられる．

4.3.2 セキュリティ意識の高まったきっかけ

PCやスマホの利用時におけるセキュリティ意識の高まった出来事を聴取した結果，以下のようなきっかけがあることが分かった．

表 2 意識の高まったきっかけ（括弧内青字はICT理解度の高い回答者，赤字はICT理解度の低い回答者）
Table 2 Trigger factors of attitude change.

カテゴリ	内容
環境変化	クレジットカード利用開始（#7）
	ネットバンキング使用開始（#2、#8）
対策推奨	知人・家族のセキュリティ対策推奨（#4、#8）
	店舗でのウィルス対策ソフトの推奨（#4）
脅威伝聞	知り合いがウィルスに感染（#6）
	ウィルスに関する記事（#2、#4）
	PCのウィルスの蔓延の情報（#2）
	詐欺被害報道（#1、#2、#5、#7）
	知人がワンクリック詐欺に遭遇した（#1）
	知人が端末を紛失し不正に利用された（#1）
脅威体験	自分のSNSアカウントが乗っ取られた（#4）
	不審なサイトへの誘導（#1、#3、#4、#6）
	迷惑メール（#1、#2、#3、#7、#8）
	ショッピングサイトを騙る不審なメールが来た（#3）
	通信事業者を騙る電話で個人情報を聞かれた（#7）
	クレジットカードの不正請求（#5）
	予期せぬウェブサイトに進んでしまった（#8）

きっかけとなったカテゴリは大きく分けて，自身の環境の変化（環境変化），他者からのセキュリティ対策推奨（対策推奨），他者が脅威に遭遇したことの伝聞（脅威伝聞），および自身の脅威体験（脅威体験）の4つであった．

表 2 に具体的な発言内容を示す．表2の括弧内には発言者のICT理解度を示している．各カテゴリがICT理解度の高さによらず意識の高まりにつながっていると考えられる．

4.3.3 意識の高まりにともなう対策への認識の変化

セキュリティ意識の高まりにより，認知したことについて対象者が回想した内容を集約すると以下のことがあげられる．括弧内は発言者のICT理解度の高さである．

- 個人情報漏洩が心配（高）
- 金銭被害が心配（高，低）
- 自分の被害で他の人に迷惑がかかることが心配（高）
- 意識して気を付けようと感じた（高，低）

上記より，意識が高まったことによりセキュリティに対する認識が変化していることが分かる．また，ICT理解度の高いユーザの方が，他者への影響を考慮しており，影響の範囲を広く考えていることが分かる．

4.3.4 実施している対策

表 3 に，実施している対策と意識の高まりとの関係別に分類した発言を示す．発言から推察されることは以下のとおりである．

- 意識高まり以前から実施していること：すべての対策内容においてICT理解度の高い回答者は何らかの行動を行っており，意識の高まりとは関係なく適切な行動を能動的にとっているようである．ICT理解度が低い対象者にはソフトウェア更新実施者はおらず，PW管理・認証強化に関する対策行動では積極的な実施と

表 3 実施している主な対策（発言者欄青字は ICT 理解度の高い回答者，赤字は ICT 理解度の低い回答者）

Table 3 Current behaviors against threats.

行動状況	対策内容	発言#	発言	発言者
意識の高まり以前から実施	ソフトウェア更新	1	WindowsのOSアップデートは自動に設定している。	#2
	ウィルス対策	2	PCもスマホもウイルス対策ソフトを使っている。今まで入っていて、脅威を防いでくれたりなど良かったと思ったことが実はない。	#6
		3	PCではウィルス対策ソフトを使っている。	#7
		4	PCに入っているセキュリティソフトを使っている。スマホにはインターネットバンキングをしている銀行が推奨しているセキュリティアプリを入れている。	#8
	PW管理・認証強化	5	パスワードは複数のものを使っている。	#2
		6	二段階認証等は、面倒と思いながらサービスによっては必須なので実施している。	#3
		7	パスワードは各サイトごとに別のものを使っている。	#4
	脅威・手口の理解と対策	8	知らないメールは開かない。	#2
		9	携帯通信キャリアの迷惑メール対策サービスを利用しているが漏れてくるため自分で削除しなければならない。	#3
		10	詐欺メールなど判断がつかないメールなどはどんどん消してしまう。	#8
意識の高まり後から実施	ソフトウェア更新	11	OS更新は夜の間にするが、最新になるように気を付けている。スマホのアプリも最新のバージョンにしている。	#5
	ウィルス対策	12	端末購入時にセキュリティの契約をした。	#1
		13	個人情報を盗むウィルスが蔓延した時からウィルス対策をしている。	#2
		14	スマホにまでお金を払ってセキュリティソフトを入れることに抵抗があったが、スマホはPCと同じだからセキュリティソフトは必須、と好きなブロガーの記事で書いていたため導入した。	#4
	PW管理・認証強化	15	キーロガーが心配なので、二段階認証が提供されている場合は設定している。面倒だが、やっている。	#2
		16	クレジットカードの不正使用を契機にサービス毎のパスワードを変えている。	#5
	脅威・手口の理解と対策	17	ブラウザであなたのスマホは今ウイルスに感染しましたという警告が出たり、振り込め詐欺メールが来たときは、驚いて調べて無視した。調べなければわからなかった。	#3
		18	「あなたのAndroidの端末が感染したためこのアプリをインストールしてください」という警告が、機種名とともに表示された。これはおかしいと思って、同じような事例がないか検索したら、「これは詐欺だからインストールしないでください」と出てきた。	#4
		19	フリーWi-Fiは危ないと聞いたため使っていない。	#1
		20	自分の契約している通信会社の回線を使うようにしている。フリーWi-Fiは一度被害にあったため信用していない。	#4
		21	フリーWi-Fiを使おうと思ったら「安全ではありません」と警告が出たので使わなかった。	#8
		22	知人が怪しいメールでウイルス感染したことがあり、その時は意識が高まった。知らない人から届いたメールは開かない。	#6
		23	配送業者を名乗ったメールのリンクをタップしてしまい迷惑メールが増えた。メールは不用意に開かない。	#7
意識が高まったが実施していない	PW管理・認証強化	24	パスワードは変えていない。いちいち変えるのが面倒なので2通りぐらいを使いまわしている。	#1
	脅威・手口の理解と対策	25	フリーWi-Fiでクレジットカードの番号を入れて被害に遭っている人もいるみたい。だから抵抗はあるがどうしてもというときにつなげてしまう。	#5
		26	インターネットバンキングの画面に「あやしいメールに気をつけましょう」と書いてあるが、それを見ると余計不安になるがどれがあやしいメールかの見分けがつかないため実施できない。	#8

いうよりもサービスを使ううえでやむなく利用しているという発言（発言 #6）も確認された．迷惑メールに関しても，発言 #9，10 より，危機意識に基づく対策というよりもむしろ面倒なものを排除したいという気持ちがあるようである．これらのことから，ICT 理解度が低い場合にはセキュリティ対策を意識的にとっているというわけではないようである．

- 意識の高まりにともない実施していること：意識の高まり後から実施している行動については，ICT 理解度の高いユーザは積極的な対策行動をとっている（発言 #13，14，15，18，20，22）．ICT 理解度の低いユーザも同様に積極的に対策行動をとっており，特に実施の手間の少ないソフトウェア更新（発言 #11）から，対策には知識と判断を要する脅威・手口の理解と対策（発言 #17, 19, 21, 23）など，意識の高まり以前には見られなかった安全な行動，危険を避ける行動をとっている．
- 意識が高まったが実施していないこと：PW 管理・認証強化および，脅威・手口の理解と対策については，意識が高まり，対策方法も認知していても不便なことを避け利便性を重視する傾向（発言 #24，25）があることや，自身では判断がつかないことが対策行動への障壁になっている（発言 #26）ことが分かる．この傾向は ICT 理解度の低い場合に強い．

4.3.5 対策への不満

前項で，意識が高まったが実施していない理由について，利便性重視の傾向や自己判断がつかないことがあげられた．このような問題は同様に対策行動の実施者からもあがっており，不満の感じやすさと重要性の認識とのバランスが対策行動を実施するか否かに関わっていると考えられる．対策への不満は表 3 より以下の 3 点に分類できる．

(1) 面倒・不便さ

セキュリティ対策を行うことによる生じる面倒さ，不便さ（発言 #6，15，24，25）

(2) 効果実感のなさ

セキュリティ対策の効果を実感できないこと（発言 #2）

(3) 自己判断への忌避感

巧妙化した攻撃を見破れる自信がないことや，誤操作による被害，正しい対処か確信が持てない，自分では対処の仕方が分からない，などの自己判断を迫られることへの抵抗感（発言 #9，17，26）

これらのことから，対策への不満は行動に負の影響を与えていると考えられる．

5. 定量調査

本章では，前章で得られた結果をもとに，セキュリティ意識の高まるきっかけ，および，きっかけと行動の関係に関する仮説を立て，その検証を行う．

5.1 仮説

前章の結果から，以下のような傾向があると考えられる．

【傾向 1】セキュリティ意識を高めるきっかけとしては，文献 [11], [12] などで以前から提案されている「脅威伝聞」「脅威体験」のカテゴリに加えて「環境変化」「対策推奨」の合計 4 つが存在し，遭遇した場合には ICT 理解度の高さに関係なく意識の高まりが起こる（4.3.2 項より）．

【傾向 2】ICT 理解度の高い群は低い群と比べて意識の高まり以前よりセキュリティ対策を意識的にとっていることに加え，意識の高まりとともにさらなる対策を実施している．また，ICT 理解度の低い群においても意識の高まりがセキュリティ対策の開始につながっている場合がある一方で，ユーザの負担の大きな行動や，実施することにより

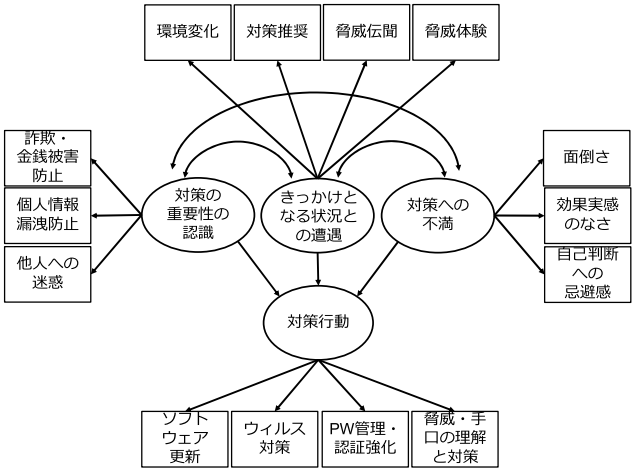


図 1 セキュリティ意識の高まりと対策の因果モデル
Fig. 1 Causal model between behaviors and factors.

利便性が大きく損なわれるような対策への不満が影響し，ICT 理解度意識の高まりが行動につながりにくい傾向にある（4.3.4，4.3.5 項より）．

上記の 2 つの傾向，および，4.3.3 項で示した「対策の重要性の認識」を考慮し，以下のような仮説を立てた．

【仮説】現在，対策行動を実施しているか否かに注目すると「きっかけとなる状況との遭遇」の経験と「対策の重要性の認識」の要因が「対策行動」に正の影響を与えている．また「対策への不満」の要因は「対策行動」へ負の影響を与えており，影響度は ICT 理解度によって異なる．

傾向 1 については，定量調査によりカテゴリごとの遭遇のしやすさや効果の大きさの違いを分析し，より意識の高まりに有効なカテゴリを明らかにする．傾向 2 については意識の高まりと行動の関係性を定量的に分析する．さらに，仮説については**図 1** のような 4 つの潜在変数と 14 の観測変数からなる構造が存在すると考えられるため，この仮説モデルについて検証を行う．

5.2 アンケート実施概要

●調査日

2019 年 11 月 8 日～10 日

●アンケート回答者

調査はリサーチ会社を通じてのウェブアンケートにより実施した．アンケート回答者は調査会社を介して募集を行った．

アンケート回答者は 18 歳以上 69 歳以下とし，内訳は平成 30 年通信利用動向調査世帯構成員編の過去 1 年間のインターネット利用経験者数 [16] に従い割付けを行い，インターネットをプライベートで最低でも月 2～3 回利用しているユーザの回答を回収した．傾向 1 および 2 の分析や仮説の検証には総インターネット利用者の実態に合った回答者群を用いる必要があるため，きっかけとなる状況との遭遇状況や意識の高まった経験の有無，対策行動の実施状況などで対象者のスクリーニングは行っていない．また，この調査会社では 400 万名以上のモニタを有しており，この中から割付けを行いながらランダムに対象者を募集しているため，実際のインターネットユーザの回答からは大きく逸脱しておらず，分析結果も一般化可能であると考えられる．

アンケート回答者の総数は 454 名であり，50.4%が男性で平均年齢は 44.3 歳である．付録 A.2 にアンケート回答者の性年代別内訳を掲載する．

●質問項目

質問項目の概要は以下のとおりである．詳細は付録 A.1 に示す．

【ICT 理解度】

インターネットに関する知識についての質問，および知識レベルの自己認識についての質問である．この質問は文献 [17], [18], [19] などを参考に作成した．アンケートにおける回答選択肢は「正しい」「間違い」「分からない」とし，正解者の割合を付録 A.1 に示している．また，あわせて，知識の有無に対する自己認識についての質問を行っている．

【きっかけとなる状況との遭遇】

前章で得られた，意識の高まりにつながる可能性がある経験の有無に関する質問である．また，それらの経験の中で実際に意識が高まった体験があるかどうかについて聴取する質問である．アンケートでは，各状況を提示し，複数回答形式で回答者が経験したことがある状況をすべて選択し，さらに，経験したことのある状況の中から，意識が高まったことがある状況を複数回答形式で回答者がすべて選択する方法で聴取している．

【セキュリティ対策行動】

各種セキュリティ対策の実施状況と，実施している対策の中でセキュリティ意識の高まりを契機に開始した対策について聴取する質問である．アンケートでは，各対策を提示し，複数回答形式で回答者が実施している対策をすべて選択し，さらに，【きっかけとなる状況との遭遇】の質問において何らかの意識が高まった状況がある回答者を対象に，意識が高まったことで初めて実行した対策について複数回答形式で聴取している．

【セキュリティ対策の重要性の認識】

前章であげた，セキュリティ意識が高まった際に感じるセキュリティ対策の重要性について，現在の意識を聴取する質問であり，「まったくあてはまらない」，「あまりあてはまらない」，「どちらともいえない・分からない」，「あてはまる」，「かなりあてはまる」の 5 件法で聴取している．

【セキュリティ対策への不満】

前章であげたセキュリティ対策を実施することにともなう不満に関する質問であり，「まったくあてはまらない」，「あまりあてはまらない」，「どちらともいえない・分からない」，「あてはまる」，「かなりあてはまる」の 5 件法で聴取している．

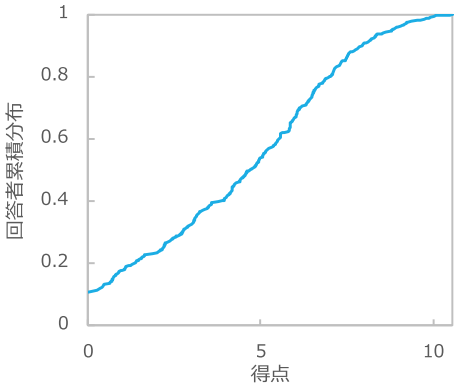


図 2 ICT 理解度の総得点分布
Fig. 2 Cumulative distribution of test score.

●回答結果

付録 A.1 に質問事項と，質問が意図するユーザ要因，およびアンケート調査結果の統計を示す．ICT 理解度測定については正解率を記載している．きっかけとなる状況との遭遇状況については，全回答者のうち各状況に遭遇した人数の割合（状況遭遇者），および，全回答者のうち各状況により意識の高まったことのある回答者（意識高まり経験者）の割合を掲載している．また，セキュリティ対策の実施状況については各対策の実施者割合を掲載している．知識の自己認識，セキュリティ対策の重要性の認識およびセキュリティ対策への不満については 5 件法を用いているため回答選択肢 1〜5 の平均値および分散値を掲載している．

5.3 分析

5.3.1 ICT 理解度の定義

5.1 節の仮説検証には，定性調査においてきっかけや行動と関係の深かった ICT 理解度の高さを定義する必要がある．そこで，アンケート調査のうち【ICT 理解度】をもとに ICT 理解度の高さを計算する．付録 A.1 に各質問に関する全回答者のうちの正解者率を掲載している．正解者率は 0.066〜0.720 の間の値を示しており分散が大きいため，正解数に基づき ICT 理解度を分類すると正確な評価にならない可能性が高い．そこで，各質問項目における項目困難度（この場合，1 − 正解者率）をそれぞれの質問に対する得点とし，それらの和を回答者それぞれの得点合計値とすることで ICT 理解度の数値化を行った．**図 2** に得点合計値に対する回答者の割合の累積分布を示す．得点合計値による大きな分布の偏りがないことが分かる．また，この ICT 理解度に関する得点合計値は知識の自己認識の質問（付録 A.1【知識の自己認識】）に対する回答との順位相関係数が 0.351 と正の相関があることから，回答者の主観的な ICT 理解度と客観的な ICT 理解度の両者が整合していると考えられる．

本研究では得点合計値が中央値より大きい回答者を ICT 理解度の高い群，それ以外の回答者を ICT 理解度の低い群

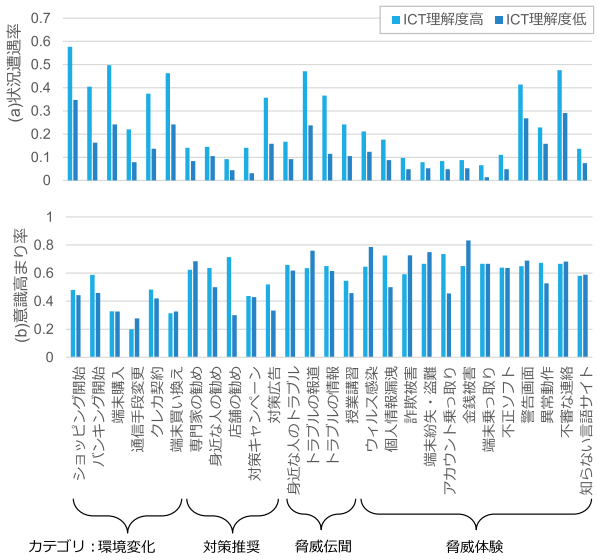


図 3 意識の高まるきっかけとなる状況遭遇率と状況による意識高まり率
Fig. 3 Ratio of participants who encountered occasion that raise their security awareness and whose level of awareness was actually raised by the occasion.

とした．今回は得点が中央値と一致する回答者は存在しなかったため，回答者は均等な 2 群（それぞれ 227 名）に分けられている．これにより，セキュリティ対策行動実施に関わる要因について，ICT 理解度による影響の概略を明らかにすることができる[*1]．

5.3.2 傾向 1：セキュリティ意識の高まるきっかけ

セキュリティ意識の高まるきっかけの分析にあたり，ICT 理解度別に以下の 2 つの値の比較を行う．

(a) 状況遭遇率：各状況において，全回答者のうち，経験したことのある状況として回答した回答者数の割合

(b) 状況による意識高まり率：各状況において，(a) の経験したことのある状況として回答した回答者のうち，意識が高まったことのある状況として選択した回答者の割合

なお，前述のとおり ICT 理解度の高い群の総回答者数，低い群の総回答者数はともに 227 名である．**図 3** に ICT 理解度別に，各状況における (a)，(b) の値を示す．

図 3 (a) よりすべての項目において，ICT 理解度が高い回答者の方がきっかけとなる状況との遭遇者数も多いことが読み取れ，有意差が認められる項目が多い[*2]．これはユーザの ICT 理解度と ICT 利用経験に関係があることが考えられる．なお，何らかの意識の高まりを経験した回答者は

[*1] 2 つの ICT 理解度の群の総得点に関する箱ひげ図を付録 A.3 に掲載している．得点の中央値で ICT 理解度を分割することにより中央値付近の得点の回答者は理解度が同程度であっても異なる群に属する現象が生じるが，異なる群の回答者間で得点の逆転（低い群に高い得点の回答者が混入することや高い群に低い得点の回答者が混入すること）は起きない．そのため，本分類による ICT 理解度を用いた群間比較による結果は信頼できると考えられる．

[*2] 有意差が認められなかった項目は「専門家の勧め」，「身近な人の勧め」，「店舗の勧め」，「詐欺被害」，「端末紛失・盗難」，「アカウント乗っ取り」，「金銭被害」，「異常動作」であった．

ICT 理解度が高い群で 176 名（同群の 77.5%），低い群で 146 名であった（同群の 64.3%）．また，図 3 (b) によると，きっかけと遭遇した場合，すべての項目において最低でも遭遇者の 20%のユーザの意識が高まっており，「店舗の勧め」以外は ICT 理解度の有無で有意差はなく[*3]，「店舗の勧め」も状況遭遇率が低いため ICT 理解度の意識高まりへの影響は小さいと考えられる．これらのことから，ICT 理解度の高さによってきっかけとなる状況と遭遇する頻度は異なるが，遭遇した場合には，ICT 理解度の高さに関係なく意識の高まりが起こると考えられる．このことから傾向 1 で示したとおり，ICT 理解度によらずすべてのユーザに対し，文献 [11], [12] などで提案されている「脅威伝聞」「脅威体験」のカテゴリに加えて「環境変化」「対策推奨」の合計 4 つのカテゴリが意識の高まりのきっかけとなりうる．きっかけとなるカテゴリ間で比較すると，遭遇率での比較では「環境変化」,「脅威伝聞」が高い傾向にある．また意識の高まる割合が比較的高いカテゴリは「脅威伝聞」「脅威体験」である．このことから，意識が高まるきっかけとしては，特に「脅威伝聞」が多くのユーザの意識を高めていると考えられる．

5.3.3 傾向 2：きっかけとなる状況との遭遇と行動の関係

次に意識の高まりと現在行っている対策についての関係を分析する．ここでは ICT 理解度別に以下の 3 つの値について比較を行う．

(a) 対策実施者数：総回答者数は ICT 理解度高群および低群それぞれ 227 名のうち，各対策における実施者の数である．

(b) 意識高まりによる実施者割合：各対策実施者（(a) で示した人数）に対する，意識の高まりの後に開始した回答者数の割合であり，各対策が意識の高まりを起点にしたかどうかを示している．

(c) 意識高まりの行動寄与率：何らかの意識が高まった経験を持つ回答者（ICT 理解度が高い群：176 名，低い群：146 名）に対する，意識の高まり後に開始した対策行動を選択した回答者の割合であり，意識高まりの結果開始した行動を示している．

図 4 (a) に対策実施者数，(b) に意識高まりによる実施者割合，そして (c) に意識高まりの行動寄与率を示す．

実施者の割合は総じて ICT 理解度の高い群が多いが[*4]（図 4 (a)），意識高まりによる実施者割合に注目すると，ICT 理解度の低い群では，ICT 理解度の高い群と比べて意識の高まりが主体的な対策行動実施者の増加に貢献している項目が存在する（図 4 (b)）．対策行動別に確認すると，ICT 理解度が低い場合に「OS アップデート」は対策

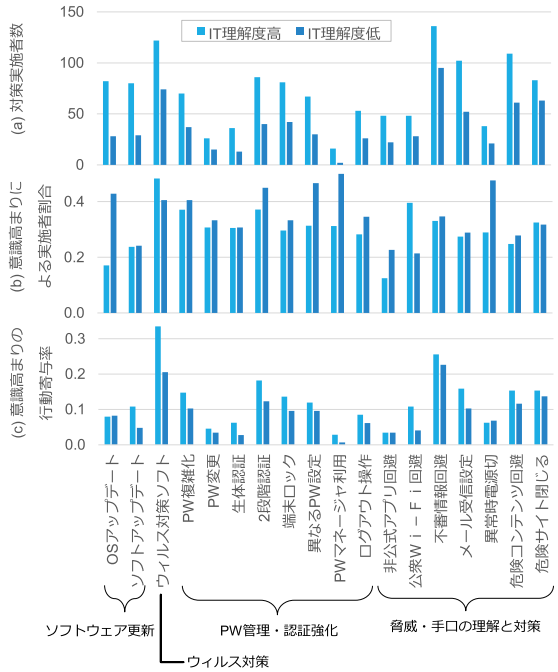


図 4 セキュリティ対策行動実施者状況

Fig. 4 Statistics of participants who take secure behavior.

行動に意識の高まりが大きく貢献しており有意に割合が高く[*3]，ICT 理解度が高いユーザは意識の高まる前から実施していたことを，ICT 理解度が低いユーザが意識の高まりとともに実施したことが推測できる．OS アップデートはワンクリックで対処可能であったり，自動更新設定を 1 度導入することで対応可能な対策であるため，ICT 理解度の低いユーザにとっても意識の高まりとともに開始しやすいと考えられる．

意識高まりの行動寄与率に注目すると，ICT 理解度が高い場合の方が多くの行動において割合が高く（図 4 (c)），有意差が認められた対策は「ソフトアップデート」,「ウィルス対策ソフト」,「公衆 Wi-Fi 回避」であった．コストが発生するウィルス対策ソフトの利用を開始することや，利便性よりも安全性を重視し公衆 Wi-Fi を利用しないことなど，対策をより強化していることがうかがえる．つまり，ICT 理解度の低い群では，意識の高まりが行動につながりづらく ICT 理解度の高いユーザでは行動につながりやすいと考えられる．

これらのことから ICT 理解度が低い群では，意識の高まりは簡単に実施可能な対策行動をはじめとする様々な対策行動を主体的に開始するきっかけとなっている．負担の大きな行動や，実施しないことにより利便性が高まるような対策行動については ICT 理解度の高い群よりも行動につながりにくいと考えられる．また，ICT 理解度の高いユーザ群は，意識の高まりとは無関係に対策を実施していることに加え，意識の高まりにより，安全性を重視し，対策をより強化していることが考えられる．このことは定性調査で得られた傾向 2 の傾向と同様であるといえる．

[*3] 独立性の検定に基づく．対象者総数が少ない場合（40 以下）の場合は Fisher の直接確率検定を利用し，多い場合にはクラメールの連関係数に基づく検定を行い，有意水準 5%以下の場合を有意差ありとした．

[*4] 有意差が認められない対策は「PW 変更」であった．

5.3.4 仮説：因果関係

構造方程式モデリングを行い仮説で示した構造を分析する．(1) 定義した潜在変数の妥当性検証，(2) ICT 理解度によらない構造の妥当性の検証およびモデルの分析を行ったうえで，最後に，(3) ICT 理解度の高さを考慮した場合の構造の妥当性の検証および ICT 理解度の違いによる相違点が存在するかどうかを分析する．

分析には統計分析プログラムの HAD [20] を用いた．

(1) 各潜在変数の定義と妥当性

本分析では，図 1 で示したような各因子の関係性の概略を明らかにすることを目的としており，きっかけとなる状況との遭遇，対策の重要性の認識，対策への不満，および行動の各因子をそれぞれ 1 つの潜在変数として扱うこととする，それにともない，それぞれの潜在変数の観測変数を以下のように定義する．

(A) きっかけとなる状況との遭遇：付録 A.1 の環境変化，対策推奨，脅威伝聞，脅威体験の 4 つのカテゴリそれぞれの意識の高まった個数を観測変数とした．各観測変数のとりうる値は環境変化が 0〜6，対策推奨が 0〜5，脅威伝聞 0〜4，脅威体験 0〜12 である．

(B) 対策の重要性の認識：付録 A.1 に示す質問「対策の重要性の認識」カテゴリ内の 3 つの質問（詐欺・金銭被害防止，個人情報漏洩防止，他人への迷惑）に対する回答を観測変数とした．観測変数のとりうる値はそれぞれ 1〜5 である．

(C) 対策への不満：付録 A.1 に示す質問「対策への不満」カテゴリ内の 3 つの質問（面倒さ，効果実感のなさ，自己判断への忌避感）に対する回答を観測変数とした．観測変数のとりうる値はそれぞれ 1〜5 である．

(D) 行動：付録 A.1 のソフトウェア更新，ウィルス対策，PW 管理・認証強化，脅威・手口の理解と対策の 4 つのカテゴリそれぞれの経験個数を 4 つの観測変数とした．各観測変数のとりうる値はソフトウェア更新が 0〜2，ウィルス対策が 0〜1，PW 管理・認証強化が 0〜8，脅威・手口の理解と対策 0〜7 である．

ここで，上記のように観測変数を 4 つの潜在変数に集約化したことの妥当性を評価する．一般に複数の観測変数が存在した場合にどのように下位尺度が構成されているかを検証する場合，探索的因子分析により評価を行う．それぞれの潜在変数に関し，下位尺度を 1 とした探索的因子分析を行い，因子負荷量および α 係数に基づく評価を行った．

表 4 に潜在変数に対応する観測変数の因子分析の結果を示す．因子負荷量は文献 [4] や [8] で示されている基準と同程度を満たしており，それぞれ 1 因子から構成されていると考えられる．また，**表 5** に各潜在変数に対応する観測変数における内的整合性を検証する指標である α 係数の値を示す．α 係数は，0.6 以上であり文献 [19] で良好とされる値を超えているため定義した 4 つの潜在変数に対応する観測変数はそれぞれ内的整合性があると判断できる．これらのことから，(A)〜(D) で観測変数を集約化した 4 つの潜在変数は妥当であると考えられる．

表 4 因子分析結果（各因子は因子負荷順にソート）
Table 4 Result of factor analysis.

(A)きっかけとなる状況との遭遇

観測変数	因子負荷量
脅威伝聞	.790
対策推奨	.739
環境変化	.716
脅威体験	.700

(B)対策の重要性の認識

観測変数	因子負荷量
詐欺・金銭被害防止	.848
個人情報漏洩防止	.841
他人への迷惑	.566

(C)対策への不満

観測変数	因子負荷量
面倒さ	.712
効果実感のなさ	.595
自己判断への忌避感	.489

(D)行動

観測変数	因子負荷量
脅威・手口を知り対策	.742
PW管理・認証強化	.687
ソフトウェア更新	.670
ウィルス対策	.523

表 5 因子分析結果の α 係数
Table 5 α values in factor analysis.

潜在変数	α係数
(A)きっかけとなる状況との遭遇	.779
(B)対策の重要性の認識	.792
(C)対策への不満	.622
(D)行動	.678

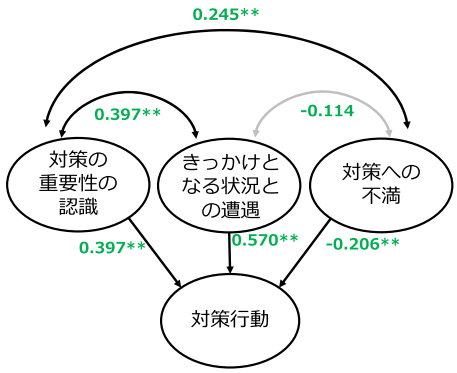
(2) モデルの妥当性の検証

次に図 1 で示したモデルの妥当性を検証するために構造方程式モデリングによる解析を行った．その結果，仮説モデルがデータに適合しているか否かを確認する指標である，CFI（Comparative fit index），GFI（Goodness-of-Fit Index），RMSEA（Root Mean Square Error of Approximation）の値はそれぞれ CFI = 0.958，GFI = 0.952，RMSEA = 0.052 であった．CFI，GFI は 1 に近いほどモデルの適合度が高く，0.9 以上で良好とされる [21]．また RMSEA は 0 に近いほど良く，0.05 [22]，0.06 [23] または 0.07 [24] 以下においてモデルは良好であるといわれている．CFI，GFI は基準を満たしており，RMSEA は最も厳しい基準（0.05 以下）の条件を満たしていないものの他の基準（0.06 および 0.07）は満たしているため，本モデルは妥当であると考えられる．

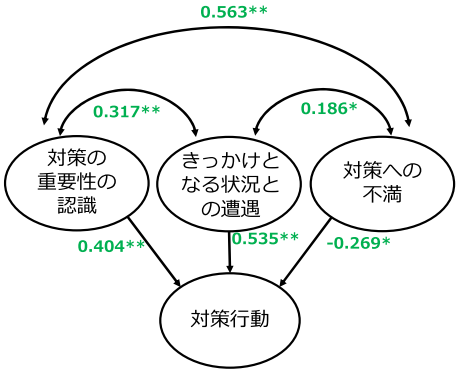
図 5 (a) に本モデルの評価結果を示す．このモデルの構造によると，過去の「きっかけとなる状況との遭遇」および現在の「対策への重要性の認識」が現在の対策行動に対し正の影響を与えており，「対策への不満」は負の影響を与えていることである．これは仮説と一致している．

(3) ICT 理解度の高さによる因果関係相違点の分析

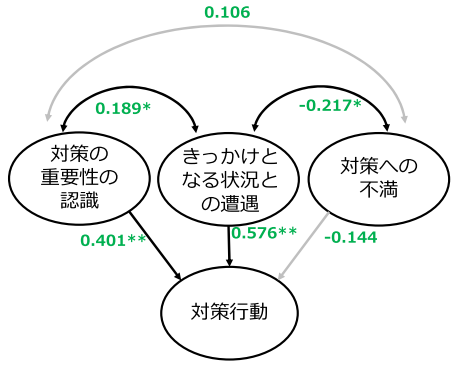
ICT 理解度を考慮しない場合の構造が把握できたため，次に ICT 理解度によってパスの重み（パス係数）や因子構造が異なるかどうかを検証する．文献 [5] と同様の手法を用いて ICT 理解度の高さに基づき多母集団同時分析を行った．多母集団同時分析は各母集団におけるパス係数や因子



(a) ICT 理解度を考慮しないモデル



(b) ICT 理解度の低いユーザモデル



(c) ICT 理解度の高いユーザモデル

図 5 モデル分析結果（パス係数はモデル別に標準化，観測変数は記載省略，**：有意水準 1%以下，*：有意水準 5%以下，有意水準の範囲外のパスを灰色で着色している）

Fig. 5 Result of causal model evaluation.

構造の差の有無を検証するための手法であり，母集団間でパスや分散，共分散などのパラメータが等値であるという制約（等値制約）の条件を設け，等値制約条件の異なるモデルの適合度の比較を行うことにより最適なモデルの検証を行う．等値制約条件の異なる複数のモデルの適合度を比較するためには，まず，それぞれのモデルにおいて，CFI，GFI，RMSEA を算出する．そして，これらの値が良好であるモデル間で AIC（Akaike's Information Criterion：赤池情報量基準）を比較し，この値が最も小さくなるモデルを

表 6 各種パラメータ

Table 6 Parameters for evaluating goodness of the models.

パラメータ	モデルの種類		
	等値制約なし	因子負荷等値制約	パス係数等値制約
CFI	.950	.946	.938
GFI	.934	.929	.924
RMSEA	.052	.052	.055
AIC	366.8	363.0	370.6

最適と判断する [25]．

はじめに以下の 3 つのモデルの CFI，GFI，RMSEA，AIC を算出し，比較を行い，最適なモデルを導出し，その後モデルの係数の比較を行う．

等値制約なしモデル：配置不変性とは，それぞれの母集団を独立に解析した場合においても，同じモデルが適用できることを示す性質であり等値制約を設けないモデルである．

因子負荷等値制約モデル：潜在変数から観測変数へのパス（因子負荷）が等値であるという仮定のもと，因子負荷に等値制約を設けたモデルである．

パス係数等値制約モデル：共分散，各要因間および要因と行動間のパスの重みに群間で差を設けないモデルであり因子負荷に加え，共分散，各要因間および要因と行動へのパスにも等値制約を設けたモデルである．

表 6 に各モデルの妥当性の指標となるパラメータを示す．CFI の変動は 0.01 以下であれば適合度が維持されているため [26]，等値制約なしモデルと因子負荷等値制約モデルでは適合度が同程度に高いといえる．また，GFI は等値制約なしモデルで最も高いが，最も低いパス係数等値制約モデルと比較しても 0.01 でありその差は小さい．RMSEA は等値制約なしモデルと因子負荷等値制約モデルが最も低く，AIC は因子負荷等値制約モデルで最も低い．これらのことから，因子負荷のいずれかの一部が等値ではない可能性を完全に否定できるものではないが因子負荷等値制約モデルが 3 種のモデルの中では最適なモデルといえるため，ICT 理解度の高さによってモデルの構造や因子構造は変わらずパス係数の大きさが異なることが考えられる．

次に因子負荷等値制約モデルにおけるパス係数および共分散関係の相違点を比較した．図 5 (b)，(c) に ICT 理解度の低いユーザモデル，および ICT 理解度の高いユーザモデルをそれぞれ示す．

ICT 理解度の高い群と低い群におけるモデルを比較すると，「きっかけとなる状況との遭遇」と「対策の重要性の認識」が「対策行動」へ正の影響を与えていること，および「対策への不満」は負の影響を与えていることは共通であり，図 5 (a) ICT 理解度を考慮しないモデルとも合致している．

ICT 理解度の高い群と低い群では，「対策への不満」がセキュリティ対策へ与える影響としては，ICT 理解度の低い群の方が大きい．さらに，「対策への不満」と他の要因および対策行動との関わり方が大きく異なることが読み取れ

る．ICT 理解度の低い群では，意識の高まるきっかけとなる状況との遭遇と対策への不満，および対策の重要性の認識の 3 つの要因における正の相関がある．つまり，意識の高まる状況と遭遇や，対策への重要性の認識の高まりとともに面倒さ，効果実感のなさ，自己判断への忌避感が存在していることを表している．これが，傾向 2 で示した ICT 理解度が低いユーザの一部で意識が高まったにもかかわらず行動をとらない理由と考えられる．ICT 理解度の高い群ではこれらの要因間が負の相関となっており，きっかけとなる状況との遭遇が対策への不満も引き下げることに関連していると考えられる．

6. 考察

6.1 結果に基づく行動促進手法の検討

仮説の検証結果に基づくと，ICT 理解度の高い群と低い群におけるモデルを比較すると，「きっかけとなる状況との遭遇」と「対策の重要性の認識」が「対策行動」へ正の影響を与えていることが分かった．きっかけとの遭遇を効果的に対策行動へとつなげるためには，傾向 1 に関する定量調査から明らかとなった，意識の高まるきっかけとして特に効果のあった「脅威伝聞」と「脅威体験」をユーザに体験してもらうことがあげられる．疑似的な「脅威体験」を提供することに加えて，ユーザの ICT 理解度の高さに合わせた内容で継続的に脅威情報を提供していくことも対策行動促進における施策としては有効と考えられる．

また，傾向 2 の定量調査や仮説検証結果に基づくと，ICT 理解度の低い群では意識の高まるきっかけとなる状況と遭遇するとともに重要性の認識も高まるが，対策に対する不満が生じている．そこで，意識の高まりが生じるシーンで対策を一元的に実施できるような仕組みを提供することにより不満を解消するようなサービスがあげられる．たとえば「環境変化」や「脅威伝聞」などユーザが遭遇する割合の高い状況下で，簡単に始められる対策行動（例：ワンクリックで OS 更新できることや自動更新設定できること，パスワードマネージャをひと度導入すれば複雑なパスワード管理も可能なこと，など）を伝達することで理解と対策行動を促すことも考えられる．

6.2 きっかけとなる状況との遭遇についての理解

定性調査において攻撃者によりアカウント（ID/PW）が乗っ取られている可能性があり，二段階認証である SMS 認証用のメッセージを受信している事例が存在した．アカウント乗っ取りの疑いがある場合，PW を変更するなどの対策が必要であるが回答者は迷惑メッセージとして認識し，メッセージを無視する対策をとっていた．このことから，ユーザの理解できない，または，認識できない脅威は意識の高まりにはつながらない可能性がある．傾向 1 に関する定量調査において，ICT 理解度の低いユーザの脅威体験への遭遇率が低い結果が得られたが，ICT 理解度の高いユーザが認識できた脅威を，ICT 理解度の低いユーザが認識できていなかったことも考えられる．これについてはさらなる裏付けが必要となるが，ICT 理解度の低いユーザに対し，脅威に対する理解を促し意識を高めてもらう施策が有効である可能性がある．一例をあげると，このような脅威に対し，何が根本的な問題として存在するのかを理解度別に示し，ユーザの理解を深めることで意識の高まりを促すことが考えられる．

6.3 構造方程式モデリングにおける潜在変数の設定

構造方程式モデリングによる評価では，「きっかけとなる状況との遭遇」，「対策の重要性の認識」および「対策への不満」と「対策行動」の関係性の概要を分析するため，それぞれ 1 つの潜在変数として分析しており，適合度も高いモデルとなった．しかし，各潜在変数をさらに複数の潜在変数として細分化することでより細かな分析が可能になると考えられる．この点についての検証は今後の課題とする．

6.4 意識が高まらない要因

傾向 1 の定量調査による分析において，同じ状況に遭遇しても意識が高まるユーザと高まらないユーザが存在した．このような違いが生じる理由としては，文献 [8], [27] などで述べられているような性格やパーソナリティなどの要因が考えられる．今回の分析結果に対し，同様の原因が存在するかどうかについては今後調査を行い分析する予定である．

7. まとめ

インターネットの安全な利用のためには，セキュリティ対策に興味関心がないユーザ，もしくはセキュリティ対策に関心はあるが行動に移していないユーザに対する推進施策が必要となる．本研究では対策推進施策を検討するための情報となりうる，一般ユーザのセキュリティ対策行動のきっかけ，およびそれに付随する行動への促進要因と阻害要因を定性調査と定量調査により分析した．「環境変化」「対策推奨」「脅威伝聞」「脅威体験」の「きっかけとなる状況との遭遇」に加えて「対策の重要性の認識」が対策行動実施の促進要因となり，「対策への不満」が阻害要因となりうる．特に，ICT 理解度の低いユーザは，「きっかけとなる状況との遭遇」とともに「対策の重要性の認識」も高まるが「対策への不満」も高まり，対策行動に移行しないユーザが多いことが分かった．今後は本知見を活かした具体的なセキュリティ対策施策促進方法について検討を行う．

謝辞 本研究成果は，国立研究開発法人情報通信研究機構（NICT）の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発（WarpDrive: Web-based Attack Response with Practical and Deployable Research InitiatiVE）」に

より得られたものです．

参考文献

[1] 総務省：総務省報道資料平成 30 年通信利用動向調査の結果（オンライン），入手先 ⟨https://www.soumu.go.jp/johotsusintokei/statistics/data/190531_1.pdf⟩（参照 2020-02-18）．

[2] 情報処理推進機構：情報セキュリティ 10 大脅威 2019（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000072668.pdf⟩（参照 2020-02-18）．

[3] 総務省：ICT サービスの利用動向（オンライン），入手先 ⟨https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/pdf/n3200000.pdf⟩（参照 2020-02-18）．

[4] 諏訪博彦, 原 賢, 関良 明：情報セキュリティ行動モデルの構築，情報処理学会論文誌，Vol.53, No.9, pp.2204–2212 (2012).

[5] 澤谷雪子，山田 明，半井明大，浦川順平，松中隆志，窪田 歩：セキュリティリスク回避行動に影響を与えるユーザ要因間の構造の解析，情報処理学会論文誌，Vol.57, No.12, pp.2696–2710 (2016).

[6] 寺田剛陽, 津田 宏, 片山佳則, 鳥居 悟：IT 被害に遭いやすい心理的・行動的特性に関する調査，2014 年マルチメディア，分散，協調とモバイルシンポジウム，pp.1498–1505 (2014).

[7] 片山佳則，寺田剛陽，鳥居 悟，津田 宏：ユーザ行動特性分析による個人と組織の IT リスク見える化の試み，2015 年暗号と情報セキュリティシンポジウム (2015).

[8] 佐野絢音，澤谷雪子，山田 明，窪田 歩：ユーザのセキュリティ対策行動における心理的な要因の影響評価，2019 年コンピュータセキュリティシンポジウム (2019).

[9] Klein, H.R. and Luciano, M.E.: What Influences Information Security Behavior? A Study with Brazilian Users, *Journal of Information Systems and Technology Management*, Vol.13, No.3, pp.479–496 (2016).

[10] Sawaya, Y., Sharif, M., Christin, N., Kubota, A., Nakarai, A. and Yamada, A.: Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior, *Proc. CHI'17*, pp.2202–2214, ACM (2017).

[11] 原田要之助，佐藤雄二，植田 修，長原欣司，上河内栄治，岡田周平，楠美淳弥，豊田訓久，西郡裕子，長谷川真大：利用者のセキュリティ意識を高めるケーススタディの一考察マンガを用いたインタラクティブ教育の提案，情報処理学会研究報告，Vol.2016-EIP-72, No.11, pp.1–6 (2016).

[12] 山本利一，白崎 清，牧野亮哉：コンピュータウィルスを体験的に学習する「情報とコンピュータ」の授業実践，日本教育情報学会学会誌，Vol.17, No.3, pp.75–81 (2002).

[13] 上野啓子：マーケティング・インタビュー：問題解決のヒントを「聞き出す」技術，東洋経済新報社 (2004).

[14] Nielsen, J. and Landauer, K.T.: A mathematical model of the finding of usability problems, *Proc. CHI'93*, pp.206–213, ACM (1993).

[15] Nielsen Norman Group: Why You Only Need to Test with 5 Users (online), available from ⟨https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/⟩ (accessed 2020-06-26).

[16] e-Stat 政府統計の総合窓口：平成 30 年通信利用動向調査 / 世帯構成員編（オンライン），入手先 ⟨https://www.e-stat.go.jp/⟩（参照 2020-02-18）．

[17] Trend Micro is702：＜クイズで判定＞あなたのセキュリティレベルは？インターネット犯罪に巻き込まれないために（オンライン），入手先 ⟨https://www.is702.jp/special/1314/⟩（参照 2020-02-18）．

[18] 内閣サイバーセキュリティセンター情報セキュリティ自己診断チェックリスト（オンライン），入手先 ⟨https://www.nisc.go.jp/security-site/files/checklist_20120417_02.pdf⟩（参照 2020-02-18）．

[19] Egelman, S. and Peer, E.: Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS), *Proc. CHI'15*, pp.2873–2882, ACM (2015).

[20] 清水裕士：フリーの統計分析ソフト HAD：機能の紹介と統計学習・教育，研究実践における利用方法の提案，メディア・情報・コミュニケーション研究，1 巻，pp.59–73 (2016).

[21] Netemeyer, G.R., Bearden, O.W. and Sharma, S.: *Scaling procedures: Issues and applications*, Sage Publications, Inc. (2003).

[22] Browne, M.W. and Cudeck, R.: Alternative ways of assessing model fit, *Testing structural equation models*, Bollen, A.K. and Long, S.J. (Eds.): pp.136–162, Sage Publications, Inc. (1993).

[23] Hu, L. and Bentler, M.P.: Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives, *Structural Equation Modeling*, Vol.6, No.1, pp.1–55 (1999).

[24] Steiger, J.H.: Understanding the limitations of global fit assessment in structural equation modeling, *Personality and Individual Differences*, Vol.42, No.5, pp.893–898 (2007).

[25] 菅野泰子，島田裕次：情報セキュリティ対策における阻害要因の構造に関する企業規模別比較研究，日本情報経営学会誌，Vol.30, No.3, pp.109–121 (2010).

[26] Cheung, W.G. and Rensvold, B.R.: Evaluating goodness-of-fit indexes for testing measurement invariance, *Structural equation modeling*, Vol.9, No.2, pp.233–255 (2002).

[27] 上市秀雄，楠見 孝：パーソナリティ・認知・状況要因がリスクテイキング行動に及ぼす効果，心理学研究，Vol.69, No.2, pp.81–88 (1998).

付　　録

A.1　質問票

【ICT理解度】以下に挙げられていることは正しいでしょうか、間違っているでしょうか？当てはまるところをお選びください。
回答選択肢：正しい、間違い、分からない

カテゴリ	質問ID	質問内容（括弧内は正解）	正解者率
知識	知識1	ＩＰアドレスから、利用しているプロバイダや地域が第三者に知られることがある。（正しい）	0.564
	知識2	使用しているウェブブラウザの情報※などはウェブサイト管理者に知られることがある。※ブラウザの設定情報など（正しい）	0.531
	知識3	単語や意味のあるフレーズを含むパスワードよりもランダムな文字列のパスワードの方が攻撃者は推測しづらい。（正しい）	0.553
	知識4	有名なサイトに偽装したウェブサイトにアクセスしてしまった場合、自分の個人情報が詐取されることがある。（正しい）	0.670
	知識5	有名なサイトに偽装したウェブサイトにアクセスしてしまった場合、金銭的被害が生じることがある。（正しい）	0.641
	知識6	ＵＲＬの打ち間違いをした場合、デバイスやアカウントが危険にさらされるかもしれない。（正しい）	0.337
	知識7	ＩＰアドレスとは通信の際に自分や相手の端末を識別する番号である。（正しい）	0.522
	知識8	ＷｉｰＦｉはデバイスを無線で利用するために使われる。（正しい）	0.540
	知識9	ウェブブラウザはウェブサイトの表示をする。（正しい）	0.377
	知識10	プライベートブラウジングモードとはウェブサイト閲覧時のパスワード、閲覧履歴などを自動で消去してくれる。（正しい）	0.170
	知識11	使用しているウェブブラウザ情報※などはウェブサイト管理者に知られることがある。※使用ブラウザ名など（正しい）	0.522
	知識12	ＩＰアドレスから、電話番号が第三者に知られることがある。（間違い）	0.205
	知識13	喫茶店等のＷｉｰＦｉは店のオーナーがセキュリティ対策をしているので、クレジットカード番号のようなプライバシー情報を入力してもよい。（間違い）	0.641
	知識14	パスワードの変更を指示する旨とウェブページへのリンクがメールで届いた際は、すぐにリンク先にアクセスし、パスワードを変更する必要がある。（間違い）	0.463
	知識15	ウェブブラウザは情報を表示するだけなので、ウェブブラウザを通じてウイルスに感染することはなく安全である。（間違い）	0.540
	知識16	利用しているＰＣ・スマートフォン・タブレットとＷｅｂサイトの間が安全な通信になっているかを確認することは難しい。（間違い）	0.152
	知識17	自分のＩＰアドレスは秘密情報であり、他人に伝えることは危険である。（間違い）	0.066
	知識18	受信メール内に記載のウェブサイトへのリンクは安全だ。（間違い）	0.654
	知識19	メールで受信した添付ファイルを開くのは安全だ。（間違い）	0.720
	知識20	ＰＣ・スマートフォン・タブレットのウイルス感染を防ぐために、プライベートブラウジングモードを使うと安全である。（間違い）	0.148
	知識21	ウィルスを能動的にダウンロードしない限りウィルス感染を防ぐことができる。（間違い）	0.581

【知識の自己認識】インターネットのしくみやオンライン上でのトラブル・犯罪・不正行為についてのあなたの知識のレベルはどれくらいですか？一番あてはまるものを１つお選びください。

カテゴリ	質問ID	回答選択肢	平均	分散
知識の自己認識	知識の自己認識	1:疑問や問題があっても何をどのように相談すればわからないし、全く理解できていない 2:人に相談したり教えてもらっても理解できない 3:人に相談したり教えてもらったりすれば理解できる 4:人から相談されたら教えることができる 5:人からよく相談されたり詳しく教えたりできる	2.974	0.911

【きっかけとなる状況との遭遇】
(1)以下の中からパソコンやスマホなどを利用していて経験したことがある状況をお選びください。
(2)経験したことがある状況の中で、オンライン上でのトラブル・犯罪・不正行為やその対策について、意識が高まったことがある状況をお選びください。

カテゴリ	質問ID	回答選択肢	全体に占める(1)の選択者の割合	全体に占める(2)の選択者の割合
環境変化	ショッピング開始	ネットショッピングを始めた・始めようと思った	0.463	0.216
	バンキング開始	ネットバンキングを始めた・始めようと思った	0.284	0.156
	端末購入	パソコンやスマホを購入した・しようと思った	0.370	0.121
	通信手段変更	通信回線やネットへの接続手段を変更した・しようと思った	0.150	0.033
	クレカ契約	ネットでも使うクレジットカードを契約した	0.256	0.119
	端末買い換え	パソコンや携帯電話などを買い換えた	0.352	0.112
対策推奨	専門家の勧め	著名な専門家がセキュリティ対策を勧めるのを見聞きした	0.112	0.073
	身近な人の勧め	家族・友人・知人からセキュリティ対策を勧められた	0.126	0.073
	店舗の勧め	家電店や電話ショップで対策を勧められた	0.068	0.040
	対策キャンペーン	ウイルス対策ソフトなどの対策手段が安く売られていた	0.086	0.037
	対策広告	ウイルス対策ソフトなどの対策手段の広告を見た	0.258	0.119
脅威伝聞	身近な人のトラブル	家族・友人・知人のトラブルやセキュリティ対策を見聞きした	0.130	0.084
	トラブルの報道	オンライン上でのトラブル・犯罪・不正行為やセキュリティ対策についての報道を見聞きした	0.355	0.240
	トラブルの情報	オンライン上でのトラブル・犯罪・不正行為やセキュリティ対策についての知識・情報を習得した	0.240	0.154
	授業講習	学校や職場などでセキュリティリスクについての授業や講習を受けた	0.174	0.090
脅威体験	ウイルス感染	ウイルス感染した・感染しそうになった	0.167	0.117
	個人情報漏洩	個人情報が漏洩した・漏洩しそうになった	0.132	0.086
	詐欺被害	詐欺被害にあった・あいそうになった	0.073	0.046
	端末紛失・盗難	端末の盗難・紛失を体験した・しそうになった	0.066	0.046
	アカウント乗っ取り	アカウントが乗っ取られた・乗っ取られそうになった	0.066	0.042
	金銭被害	金銭の被害（銀行、クレジットカードの不正利用など）にあった・あいそうになった	0.070	0.051
	端末乗っ取り	端末の乗っ取り（不正に操作される）の被害にあった・あいそうになった	0.040	0.026
	不正ソフト	不正アプリ・ソフトの被害にあった・あいそうになった	0.079	0.051
	警告画面	危険を知らせる情報や警告が画面に表示された	0.341	0.227
	異常動作	パソコンやスマホが異常な動作をした	0.194	0.119
	不審な連絡	不審なメールや電話があった	0.383	0.258
	知らない言語サイト	意図せず知らない言語のウェブサイトに進んでいた	0.106	0.062

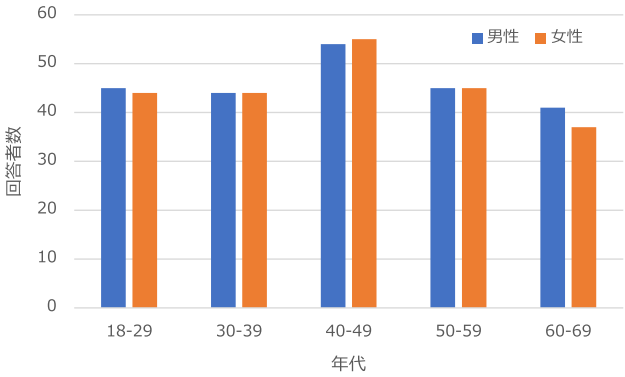
【セキュリティ対策の実施状況】
(1)ご家庭用・個人用でのインターネット利用に関して、現在実行されているセキュリティ対策をお選びください。
(2)ご家庭用・個人用でのインターネット利用に関して、意識が高まったことで初めて実行されたセキュリティ対策があればお選びください。

カテゴリ	質問ID	質問内容	全体に占める(1)の選択者の割合	全体に占める(2)の選択者の割合
ソフトウェア更新	OSアップデート	最新のＯＳへの迅速なアップデート	0.242	0.081
	ソフトアップデート	ソフト・アプリの迅速なバージョンアップ	0.240	0.081
ウィルス対策	ウィルス対策ソフト	ウイルス対策ソフト・ウイルス対策アプリのインストール	0.432	0.276
PW管理・認証強化	PW複雑化	複雑なパスワードの設定	0.236	0.127
	PW変更	パスワードの頻繁な変更	0.090	0.040
	生体認証	生体認証の利用	0.108	0.047
	2段階認証	２段階認証（ワンタイムパスワード、ＳＭＳ認証など）の利用	0.278	0.155
	端末ロック	パソコンやスマホのロック（パスワード、パスコード、指紋認証等）	0.271	0.118
	異なるPW設定	アカウントやＩＤごとに異なるパスワードの設定	0.214	0.109
	PWマネージャ利用	パスワードマネージャーの利用	0.040	0.019
	ログアウト操作	ログインが必要なサービスは終了後ログアウトする	0.174	0.075
脅威・手口の理解と対策	非公式アプリ回避	非公式のスマホアプリを利用しない	0.154	0.034
	公衆Ｗｉ－ＦｉⅠ回避	公衆ＷｉｰＦｉを利用しない	0.167	0.078
	不審情報回避	不審なメールやリンクは開かない	0.509	0.242
	メール受信設定	迷惑メール機能や受信拒否機能の利用	0.339	0.134
	異常時電源切	パソコンやスマホが異常な動作をしたら電源を切る	0.130	0.065
	危険コンテンツ回避	リスクのありそうなサイト・コンテンツは利用しない	0.374	0.137
	危険サイト閉じる	危険そうなサイトが開いたらそのページをすぐに閉じる	0.322	0.146

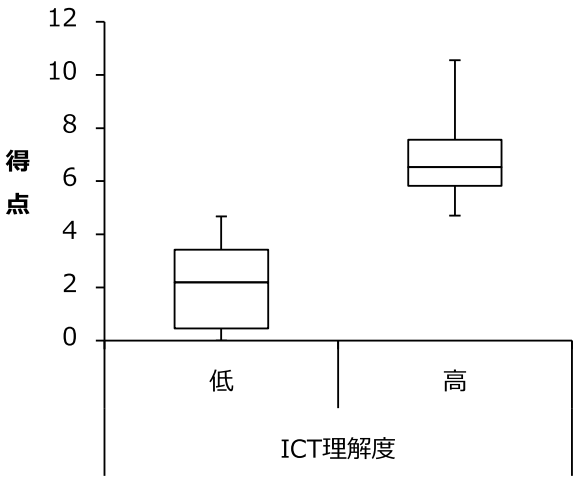
【セキュリティ対策への意識】
オンライン上でのトラブル・犯罪・不正行為などへのセキュリティについておたずねします。以下のようなお気持ちや状況は、あなた自身にはどの程度あてはまりますか？一番当てはまるものをお選びください。
回答選択肢：全くあてはまらない(1), あまりあてはまらない(2), どちらとも言えない・分からない(3), あてはまる(4), かなりあてはまる(5)

カテゴリ	質問ID	質問内容	平均	分散
セキュリティ対策の重要性の認識	詐欺・金銭被害防止	セキュリティ対策は詐欺や金銭被害を防ぐために必要だと思う	3.819	0.793
	個人情報漏洩防止	セキュリティ対策は個人情報の漏洩を防ぐために必要だと思う	3.800	0.871
	他人への迷惑	セキュリティ対策をしていないと他人や世の中に迷惑がかかると思う	3.489	0.727
対策への不満	面倒さ	セキュリティ対策をするのは面倒だ	3.194	1.031
	効果実感のなさ	ウイルス対策ソフトなどの対策をしても効果がわからない・実感できない	3.024	0.880
	自己判断への忌避感	セキュリティ対策は政府や業界や企業側でやってほしい・おまかせにしたい	3.119	0.966

A.2 アンケート対象者の性年代別分布



A.3 総得点の ICT 理解度別箱ひげ図



澤谷 雪子 （正会員）

2006 年東北大学大学院工学研究科電気・通信工学専攻博士前期課程修了．同年 KDDI（株）入社．現在，（株）KDDI 総合研究所でサイバーセキュリティの研究開発に従事．

佐野 絢音 （正会員）

2018 年静岡大学大学院総合科学技術研究科情報学専攻修士課程修了．同年 KDDI（株）入社．現在，（株）KDDI 総合研究所でサイバーセキュリティの研究開発に従事．

山田 明 （正会員）

2001 年神戸大学大学院自然科学研究科電気電子工学専攻博士前期課程修了．同年 KDDI（株）入社．2009 年東北大学大学院情報科学研究科博士後期課程修了．2010～2011 年 Carnegie Mellon University 客員研究員．現在（株）KDDI 総合研究所にてサイバーセキュリティ，DDoS 攻撃対策の研究開発に従事．

窪田 歩 （正会員）

1995 年京都大学大学院情報工学専攻博士前期課程修了．同年国際電信電話株式会社（現，KDDI）入社．2003～2004 年米国 UC Berkeley 客員研究員．現在，（株）KDDI 総合研究所でネットワークセキュリティの研究開発に従事．