情報処理学会論文誌 Vol.57 No.12 2696–2710 (Dec. 2016)

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

澤谷 雪子[1,a)] 山田 明[1] 半井 明大[1] 浦川 順平[1] 松中 隆志[2] 窪田 歩[1]

受付日 2016年3月10日, 採録日 2016年9月6日

概要：一般のインターネットユーザが，サイバー犯罪に巻き込まれるセキュリティリスクを回避する能力は，認知傾向要因，学習や被害の経験要因，性格などのパーソナリティ要因などのユーザ固有の要因と関係が深い．我々は，これらのユーザ要因に応じ，警告や支援を可能にするシステムの構築を目指している．これまでに，インターネットにおけるセキュリティリスク回避行動と，認知要因や経験要因，パーソナリティ要因などのユーザ要因との部分的な関係性が明らかになっているが，これらを網羅的に包含した構造が明らかになっていない．本論文では，これを明らかにするためにパスワード漏えいに対するセキュリティリスク回避行動に焦点を当て，セキュリティリスク回避行動と各種ユーザ要因に関するアンケート調査を実施し，仮説モデルを構築したうえで構造方程式モデリングによる分析を行った．その結果，ユーザのパーソナリティ要因の多くは行動に直結するのではなく，ユーザのセキュリティに対する認知傾向要因や経験要因に作用する構造となっていること，および，各認知傾向要因や経験要因に対しそれぞれ強く関与するパーソナリティ要因が存在することが分かった．さらに，性別により，パーソナリティ要因が認知傾向要因や行動に与える影響の大きさが異なることを確認した．これらのことから，パーソナリティ要因や性差に応じた行動の傾向の推定が可能になる．このことは個々のユーザに対応した，セキュリティリスクの回避を支援する仕組みを構築するうえで有益である．

キーワード：セキュリティリスク回避行動，認知傾向，パーソナリティ，ユーザ要因，構造方程式モデリング

Structural Analysis of User Factors that Lead the Security Risk-averse Behaviors

Yukiko Sawaya[1,a)] Akira Yamada[1] Akihiro Nakarai[1] Jumpei Urakawa[1]
Takashi Matsunaka[2] Ayumu Kubota[1]

Received: March 10, 2016, Accepted: September 6, 2016

Abstract: The ability of risk-averse behaviors is based on each user's own personalities, the experiences of acquiring the knowledge against risks or being victim, tendency of judgement, etc. Some studies focus on such cause-and-effect dependencies among behaviors, tendencies of perceptions, and experiences, however, there are no studies that deal all of behaviors, perceptions, experiences, and personalities. In this paper, we carried out the questionnaire about security risk-averse behaviors and user factors and then constructed the hypothesis model and evaluated by structural equation model in order to solve this problem. As a result, personalities of each user effect to the perceptions and experiences of study directly and effect indirectly to the behaviors. Moreover, difference of gender effects the path from personalities to perceptions and as a result, it effects to the risk averse behaviors. From these results, we can estimate each user's perception tendencies by measuring personalities or confirming the gender and it will lead the construction of security risk averse enhancement system which fits each user's factors.

Keywords: security risk averse behavior, perception, personality, user factors, structural equation modeling

[1] 株式会社 KDDI 総合研究所
KDDI Research, Inc., Fujimino, Saitama 356–8502, Japan
[2] KDDI 株式会社
KDDI Corporation, Chiyoda, Tokyo 102–8460, Japan
[a)] yu-sawaya@kddi-research.jp

1. はじめに

パソコンやスマートフォンの普及にともない，幅広いユーザ層がインターネットサービスを利用できる世の中になった．しかしその一方で，一般のインターネットユーザが迷惑メール，端末などへの不正アクセス被害，意図しない情報漏えい，詐欺の被害に遭うケースが多数存在し，サイバー犯罪に関する警察への相談件数もまた増加している [1]．

リスクを回避する行動は，ユーザのリスクに対する知覚や考え方である認知傾向要因，知識習得や被害遭遇に関する経験要因，人格を表すパーソナリティ要因など，各ユーザの固有の要因に依存しているとされている [2]．一般のインターネットユーザが，上記のようなセキュリティ犯罪の被害者になりうる可能性をセキュリティリスクとしてとらえた際にも同様の傾向が存在し，リスク回避行動を促すためにはユーザ固有の要因に応じた働きかけが有効と考えられる．しかし昨今のセキュリティ対策ソフト [3] などで行っているリスク回避支援はすべてのユーザに対して画一的な警告を出力するのみであり，ユーザに応じた支援がなされていない．そこで，我々は個々のユーザ要因に応じ，セキュリティリスクを回避するための警告や支援を可能にするシステムの構築を目指している．これを実現するために，本論文ではユーザ要因が行動にどのように影響しているかを解析し，インターネット利用におけるセキュリティリスク回避行動に作用するユーザ要因を分析する．

これまでに，セキュリティリスク回避行動と，認知傾向要因，経験要因，パーソナリティ要因との断片的な相関性の解析が行われている．これらの結果を統合することにより，どのようにユーザ要因が関連しあっているかを推測可能であるが，どのように相互関係が存在するかということまでは推定できない．また，受験やスキーなど，危険な状況下でその危険をあえて受容する行動であるリスクテイキング行動と，認知傾向要因，経験要因，パーソナリティ要因を網羅的に包含した関係性解析が行われている [4] が，セキュリティリスク回避行動に対する解析は行われていない．

本論文で我々は，セキュリティリスクにおける行動と各ユーザ要因間の関係性の仮説を立て，アンケート調査に基づく仮説の検証を行った．検証に際し，原因側の変数が対照実験を行った場合のような操作可能な変数でない限り，真の因果関係を断定できない制約を持つ [5] と知られているが，仮説の検証に広く用いられている，構造方程式モデリング（SEM）を用いた．

警察庁によるサイバー犯罪の分類に着目すると，セキュリティリスクに関連する項目は，不正アクセス，および，コンピュータ・電磁的記録対象犯罪である．このうち，犯罪件数が多いのは不正アクセスであり [6]，その主な原因として，パスワードの窃取があげられている [7]．そこで本論文では，不正アクセス被害の具体的なリスクである「インターネットサービスにおけるパスワード漏えいリスク」に焦点を当てる．パスワード漏えいリスクに対するセキュリティリスク回避行動を解析対象のリスク回避行動とし，行動と，認知傾向要因，経験要因，パーソナリティ要因の 3 つに関するアンケート調査を，623 名のウェブメール機能付きアカウントを利用するインターネットユーザに実施した．パスワードを含む情報漏えいに関する具体的なリスクとして，文献 [8] では，「ID やパスワード，クレジットカード番号などがインターネットを通じて盗まれ，悪用される危険性があること」，および「共用のパソコンでは自分の利用履歴が残る可能性があること」があげられている．また，これらリスクを回避する行動として「パスワード構成や設定に関する行動」や「ID やパスワードの管理，共用端末利用時の確認行動」があげられている．そこでこれらの行動に関する質問と，各種ユーザ要因に関する質問を行ったうえで，調査結果に基づき，行動と各要因間の構造を分析した．

これにより，次のことが明らかになった．

(1) パーソナリティ要因が認知傾向要因や経験要因へ作用し，認知傾向要因や経験要因がリスク回避行動に作用するという多段構造を形成している．

(2) パーソナリティ要因の中で，楽観性や悲観性，曖昧さ耐性，熟慮性はそれぞれ認知傾向要因や経験要因に関連しているが，不安傾向は関連がない．

(3) 性別によって，パーソナリティ要因が認知傾向要因や行動に与える関連性の大きさが異なる．

これらの結果から，ユーザの適切なリスク回避行動を促進するためには，パーソナリティ要因や性別に応じた支援が必要であると考えられる．また，パーソナリティ要因や性別がどのような認知傾向や経験，行動をもたらすかを推定できるようになるため，支援を行うための仕組みを構築するうえで有益な知見となりうる．

本論文では，セキュリティリスク回避におけるユーザ要因間の関係性を表すモデルの構築と解析結果について詳細に述べる．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 章で仮説モデルを提案し，モデルの検証を行う．そして 5 章で考察を行い，最後に 6 章で本論文のまとめを行う．

2. 関連研究

本章では，セキュリティリスク回避行動および自動車運転などの一般的行動に関する行動と，認知傾向要因，経験要因，パーソナリティ要因との関係性を解析した文献について述べる．

2.1 認知傾向要因とパーソナリティ要因の関係性の解析

まず，認知傾向要因とパーソナリティ要因の関係性を解析した研究がある．文献 [2] では，ユーザの性格と認証技術（パスワード認証，持ち物認証，生体認証）を利用する際のセキュリティ意識との相関を分析し，それらの間に関係性が存在することを明らかにしている．また，生体認証の利用経験など，セキュリティ対策経験や環境がセキュリティ意識に影響を与えることも示している．インターネット利用における不安発生のメカニズムを解析している研究 [9], [10] では，リスクに対する判断材料や不安になりやすいなどの性格特性がリスクの認知につながり，そのリスクに対する不安を発生させていると述べている．

2.2 各種ユーザ要因と行動の関係性の解析

認知傾向要因や意識に関するユーザ要因と行動の関係性に関する研究も各行動科学の分野で行われている．文献 [11] 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いる．文献 [12] 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，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性が異なることを明らかにしている．文献 [13] によるとリスクを低減できる安全技術や能力の向上が，リスクが低下したという認識につながり，リスク回避行動をとらなくなるということを示している．この現象はリスク補償と呼ばれており，自動車などの安全対策の導入においてはリスク補償の発生も考慮するべきであることを示唆している．さらに，リスク補償は，運転時のスピードや確認行動をしないというベネフィットを選択する傾向に影響を与えることも示唆している．文献 [14] では従業員の安全な行動における動機と阻害因子の解析を行っている．セキュリティ対策に関する行動には知識と経験が影響を与えていることを述べている．また，セキュリティ対策を行った効果がすぐに反映されていないことが阻害因子であると述べている．文献 [15] ではコンピュータセキュリティに関する考えと，コンピュータを安全に使うための普段の行動との関連性を調査している．若年層でセキュリティの学習をしていないユーザと高年層で学習しているユーザとでは異なる危険性が存在し，これはセキュリティに関する意識の違いが影響していることを明らかにしている．また，同文献ではウィルスが目に見える形でコンピュータの問題を引き起こすと信じている層は，ブラウジングでウィルスをダウンロードしてしまうと考えているが，自身でそれを防ぐことができないと考えている人が多数派であると述べている．さらに自分が攻撃対象にされないと考えていてもセキュリティ対策をしているユーザ層が存在し，直観的心理と行動は必ずしも直結していないことを示している．

行動とパーソナリティ要因の関係性に関する研究も多様な分野で行われている．文献 [16] では，危険を認識しながらも行動に出てしまう「不安全行動」の性差，年齢差，場面一貫性，誘発要因，抑制要因などを解明しており，ある場面でより不安全行動を選択するグループは他の場面でも不安全に振る舞う傾向が強いことを明らかにしている．さらに，この傾向の個人差は，各種の不安全行動だけでなく，生命リスク回避，一般的不安傾向，金銭的リスク回避などの一般的態度・行動傾向と関連していることも述べている．文献 [17] においても，飲酒や喫煙などのリスクテイキング行動間，およびリスクテイキング行動と性別や性格にも相関があることを示している．文献 [18] では特に勤勉性の低さ，いい加減さ，軽率さは複数のエラー因子と中程度の相関があったと述べている．文献 [19] 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，ベネフィット認知の強さ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．文献 [20] では曖昧な状況を受け入れられる傾向を表す曖昧さ耐性と，購買行動に関する意思決定の関係性を解析しており，曖昧さ耐性がないことが迷わずに購買行動の意志決定をすることと関係があると述べている．

2.3 各種ユーザ要因と行動の包括的な関係性の解析

一般的な行動，認知傾向要因，およびパーソナリティ要因を網羅的に包含し測定したうえで，因果関係を解析した既存研究も存在する．文献 [4] は，受験，スキーなどにおけるリスクテイキング行動と，認知傾向要因およびパーソナリティ要因に関するユーザ要因間の因果関係を分析している．損失に対する認識，利益に対する認識，能力の自己評価などの認知傾向要因がリスクテイキング行動には直接影響しており，刺激欲求，達成動機，楽観性などのパーソナリティ要因は認知傾向要因を経由して影響するものであるとして仮説モデルを検証している．さらに，文献 [21] では様々なリスクテイキング行動と，認知傾向要因，パーソナリティ要因を比較し，リスクに対する不安が自転車盗難や解雇などのリスク回避行動に間接的に影響を与えることを示している．

3. 本研究の方針

前章で述べたとおり，これまでに，セキュリティリスク回避行動と，認知傾向要因，経験要因，パーソナリティ要

因との部分的な因果関係や相関性の解析が行われている．これらの結果を統合することで，どのようにユーザ要因どうしが関連し合っているかを推測可能であるが，どの程度の関連性が存在するかということまでは推定できない．これを測定するためには，行動と，認知傾向要因，経験要因，パーソナリティ要因を包括的に測定したうえで，1つの因果モデルを構築し，解析する必要がある．また，一般的な行動に関してこのような解析は行われているが，セキュリティリスク回避に関する議論は行われていない．そこでセキュリティリスク回避行動と，認知傾向要因，経験要因，パーソナリティ要因との間の包括的な関係性の解明を行う．解析には，SEM を用いる．SEM は概念的な要因や，それを測定するための観測変数を同時に分析するための統計的方法であり，複数の要因が混在する複雑な因果関係を検証することが可能である．SEM は，原因側の変数が対照実験を行った場合のような操作可能な変数でない限り，真の因果関係を断定できないという制約を持つ [5] が，仮説の検証に広く用いられている [4], [11], [21], [22].

リスク回避行動に影響を与える要因には，認知傾向要因や経験要因，パーソナリティ要因などの，環境や状況によって変化しない普遍性の高いユーザ要因のほかに，焦りや，忙しさのような環境や状況に依存するユーザ要因が存在する [12], [19]．これにともない，行動は習慣行動と状況に応じて変化する一時的な行動に分類されると考えられる．本論文では，解析の第1歩として普遍性の高いユーザ要因と習慣行動に焦点を絞り，仮説モデルの構築を行い，評価する．

4. 仮説モデルの構築

本章では，セキュリティリスク回避行動と，行動に影響を与える要因との因果関係に関する仮説モデルの構築について述べる．手順としては以下のとおりである．

（手順 1）リスク回避行動と因果関係が存在する可能性のあるユーザ要因について列挙し，ユーザ要因間の因果関係の仮説を立て，仮説モデルを構築する．

（手順 2）ユーザ要因および行動を測定するためのアンケート質問項目を作成し，アンケート調査を実施したうえで，各要因を構成する質問項目の妥当性を検証する．

（手順 3）仮説モデルの妥当性を検証する．

4.1 手順 1：ユーザ要因の整理と仮説の構築

4.1.1 ユーザ要因の整理

本論文では，環境や状況に依存しない普遍性の高いユーザ要因として，以下の認知傾向要因，経験要因，およびパーソナリティ要因を解析対象とする．

認知傾向要因

ユーザがセキュリティリスク回避行動をとるか否かの判断に関する要因である．文献 [4], [11], [12], [13], [16] に基づき，現在のリスクに対する認知傾向要因を以下の3つに分類する．

(a) リスクに対する危険性を認知すること（リスク認知）
(b) リスクを上回る利益を感じること（ベネフィット認知）
(c) 安全技術や能力によりリスクが低下すると感じること（リスク補償）

ここで，文献 [11], [12] であげられているコスト感，およびコスト認知は，リスクを下げる代わりに作業などのコストが生じることを負担と感じる傾向であり，作業コストを下げる利益とリスクをとる傾向であると考えられるため，本論文ではベネフィット認知の1つとして考える．

経験要因

セキュリティリスクに関連する過去の経験は，文献 [2], [10], [14] に基づきセキュリティ対策経験，被害体験に分けられる．そこで，以下の2つの要因を経験要因とする．

(d) セキュリティリスク回避方法に関する知識や操作を習得した経験（技能習得・活用経験）
(e) 過去に被害に遭遇した経験（危険経験）

パーソナリティ要因

ユーザの行動や考え方の傾向を発生させる，性格や思考傾向を表すパーソナリティ要因である．文献 [4], [9], [10], [18], [20] によると，行動や認知傾向は，楽観性，曖昧さ耐性，勤勉性，いい加減さ，軽率さ，不安傾向と深い関係があるという．また，楽観性については，文献 [23] によると楽観的な側面と悲観的でない側面に分類できる．そこで，これらと関連の深い以下の5つを今回検証対象のパーソナリティ要因とする．

(f) 物事を良い方に明るく考える傾向（楽観性）
(g) 物事を悪い方に考えがちな傾向（悲観性）
(h) はっきりしない曖昧な状況を許容できる傾向（曖昧さ耐性）
(i) 軽率さの低さや勤勉性，いい加減さの低さを表す，よく考えて慎重に結論を下す傾向（熟慮性）
(j) 日常的な不安傾向（不安性）

4.1.2 仮説の構築

次に，各要因間における因果関係の仮説を立てる．仮説モデルの概要を**図 1** に示す．

(1) リスク回避行動と各種要因間の因果関係

既存研究に基づき，本論文では，選択した各種ユーザ要因がリスク回避行動に影響を与えているという前提を置いていることから，認知傾向要因，経験要因，およびパーソナリティ要因が，リスク回避行動の原因と仮定する．

(2) 経験要因と認知傾向要因間との因果関係

経験要因は過去に関する要因であり，認知傾向要因は現在のユーザの思考である．時系列的な因果関係を考慮すると，過去が現在に影響していると考えられるため，経験要因が，認知傾向要因の原因として位置付けられると考えら

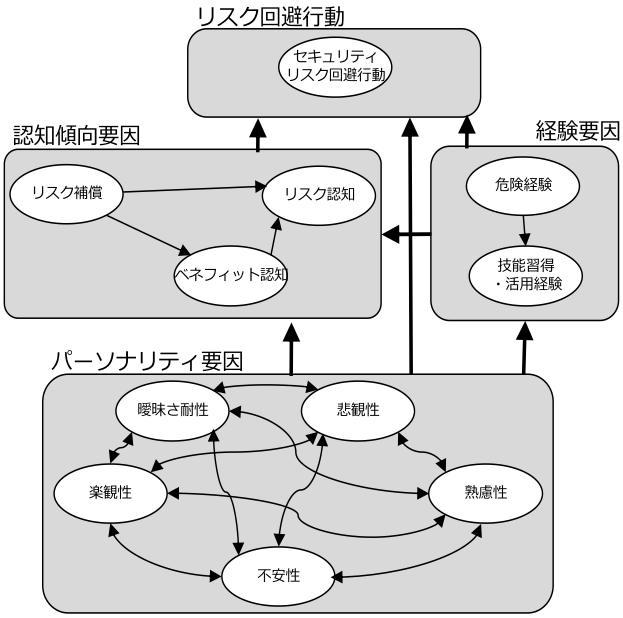

図 1 仮説モデル
Fig. 1 Hypothesis model.

れる．

(3) パーソナリティ要因と，認知傾向要因・経験要因との因果関係

パーソナリティは個人の思考と行動を特徴づける一貫した傾向であり，その性質として，(1) 環境への適応機能に関する全体的な特徴，(2) 知能・感情という要素も含む，(3) 通状況的一貫性，(4) 継時的安定性という性質を持つといわれている [24]．これに基づくと，行動や，リスクに対する考え方である認知傾向要因および経験要因はパーソナリティ要因に基づき生じると考えられる．

(4) パーソナリティ要因内の要因間の因果関係

パーソナリティは上述のとおり，個人の思考と行動を特徴づける一貫した傾向であるため，パーソナリティ要因内の楽観性，悲観性，曖昧さ耐性，熟慮性および不安性の間に明確な因果関係を付加することは難しい．そこで，因果関係は設けず，因子間の相関を表す共分散関係を仮定する．

(5) 認知傾向要因内の要因間因果関係

前述のとおり，リスク補償はリスク認知を低下させる可能性がある．そこで，リスク補償がリスク認知低下の原因と考える．また，リスク補償は，ベネフィットを選択したいと考える傾向を増長させるとされているため，リスク補償要因がベネフィット認知要因の増加の原因と考える．さらに，自分あるいは社会にとって利益があると思われる対象は実際以上に安全であると認知されやすくなる傾向が存在 [25] するため，ベネフィット認知要因がリスク認知要因に影響を与えていると考えられる．

(6) 経験要因内の要因間因果

被害などの経験が学習の契機となるといわれており，文献 [26] のような疑似被害経験を学習教材として利用する研究も多数行われていることから，危険経験が技能習得・活用経験に影響を与えると考えられる．

4.2 手順 2：アンケート調査の実施

前節で示した要因の関係性を明らかにするために，インターネットユーザに対し，セキュリティリスク回避行動とユーザ要因に関するアンケート調査を実施し，これらの測定を行う．

ここで，本論文におけるセキュリティリスク回避行動を明確化する．インターネット利用時のセキュリティリスク回避行動は，利用シーン（使用デバイスや対象としているサービス）や回避するべき対象（情報漏えい，不正利用など）によって様々であり，回答者にこれらすべての行動を問うことは，質問設計の観点からも，回答者の負担からも，現実的ではない．そこで，以下の項目を考慮し対象リスクの選定を行った．

警察庁によるサイバー犯罪の分類に着目すると，セキュリティリスクに関連する項目は，不正アクセス，および，コンピュータ・電磁的記録対象犯罪である．このうち，犯罪件数が多いのは不正アクセスであり [6]，その主な原因として，パスワードの窃取があげられている [7]．そこで「インターネットサービスにおけるパスワード漏えいリスク」に焦点を当て，これを回避するための行動と，前節で示した (a) から (j) に関する質問を調査対象者に行った．

調査は以下の要領で実施した．

4.2.1 調査概要

調査はアンケート調査会社を通じてのウェブアンケートにより実施した．

調査日時

2015 年 6 月 19 日～25 日に行った．

被験者

インターネットサービスにおけるパスワード漏えいリスク回避行動を調査するにあたり，以下のことを考慮して調査対象者を選定した．

個々のユーザが，様々なインターネットサービスを利用しており，複数のアカウントを所持している場合には，ユーザは，どの利用サービスのパスワードに関して回答するか迷う可能性が高い．このような場合には，回答者自身が意図せず一貫性のない回答をすることが考えられるが，被験者が実際利用しているサービスを想像しながら回答できるような質問をすることにより改善できると考えられる．そこで，特定のサービスに関するパスワード利用に関する質問を行うことを前提とする．これにともない，このサービス利用者に被験者を限定するものとする．文献 [27] によると，インターネットを利用する目的・用途の中で最も利用されているサービスはメールサービスであり，ウェブメールの利用者も多いと推測されたため，ウェブメール機能付きのアカウントサービス（Gmail [28]，Hotmail [29]，

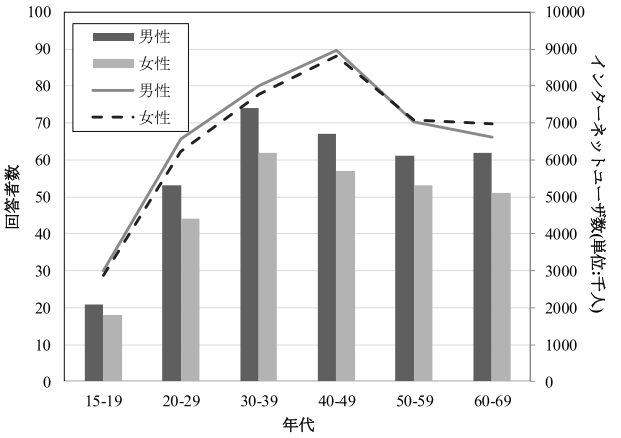

図 2 回答者属性
Fig. 2 Demography of participants.

Yahoo!メール [30] など）に関する質問を行うものとし，被験者をその利用者に限定した．

被験者は，ネットリサーチ会社に登録されている約 100 万人の中から，623 人を選定した．選定した手順は以下のとおりである．まず，このリサーチ会社の登録者の中で，ウェブメール機能付きのアカウントサービスの利用者の割合を推定するために，15 歳以上 69 歳以下の 30,000 人をランダムに抽出した．そしてウェブメール機能付きサービスの利用の有無を調査し，性・年代別にこれらのサービス利用者の性・年代に関する人口構成比を導出した．この人口構成比に合致するように，30,000 人の中から 623 名の回答者を抽出した．各性別・年齢層の分布は**図 2** のとおりである．

ここで，この 623 名の性・年代別抽出結果が妥当か否かを評価する．年代別インターネットの普及状況 [27] と人口推計 [31] から 15 歳以上のインターネット利用者数の概算を算出できる．算出の結果，各性年代ごとのインターネットユーザ数の統計値は図 2 の折れ線グラフのとおりであった．統計値と今回の被験者分布を比較すると，被験者群はやや男性が多く，40 歳代が少ない傾向にあるが，若年層が少なく，高年層になるにつれ横這いという統計値のおおよその分布傾向と合致していた．このことから，被験者は 15〜69 歳における一般のインターネットユーザの分布傾向から逸脱していないと考えられる．

質問項目

前述のとおり，パスワードを含む情報漏えいに関するリスクとして，文献 [8] では，「ID やパスワード，クレジットカード番号などがインターネットを通じて盗まれ，悪用される危険性があること」，および「共用のパソコンでは自分の利用履歴が残る可能性があること」があげられている．また，これらリスクを回避する行動として「パスワード構成や設定に関する行動」や「ID やパスワードの管理，共用端末利用時の確認行動」があげられている．

そこで，本論文では，以下の行動に関する質問を行った．

(1) パスワードの適切な管理・運用
(2) ウェブサイトを管理するサーバの信頼性確認
(3) 利用端末上での適切なログアウト処理

なお，(1) の質問に際し，回答者には，ウェブメール機能を複数利用している場合には，より厳密に回答の一貫性を保てるように，その中の 1 つを想定して回答するよう促す文言も質問票に付加した．

認知傾向要因（(a)〜(c)）および経験要因（(d)，(e)）に関しては，パスワード漏えいリスクに特化した質問内容としている．また，ユーザのパーソナリティ要因を測定するために，既存の心理評価尺度に関する質問を行った．具体的には，(f) 楽観性と (g) 悲観性を測定する楽観主義尺度 [23]，(h) 曖昧さ耐性を測定する曖昧さ耐性尺度 [23]，(i) 熟慮性を測定する認知的熟慮性–衝動性尺度 [23]，および状態–特性不安尺度（STAI）のうち特性不安尺度 [32] を (j) 不安性を測定するために利用した．

回答結果

付録 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．各質問を観測変数とし，観測変数の値は，回答内容に応じて得点数を配分している．パスワードの適切な管理運用を測定するために 4 つの観測変数（Pass1〜Pass4）を示しているが，この 4 つすべてを満たした際にパスワードの適切な管理運用を実行していると考えられるため，4 つの質問に対する回答の和を 1 つの観測変数（Pass）として，掲載している．

同様に，ウェブサイトを管理するサーバの信頼性確認については，SSL の確認手段と頻度をもって 1 つの観測変数とするために，2 つの観測変数（SSL1 と SSL2）の回答の和を 1 つの観測変数（SSL）として掲載している．

4.2.2 観測変数の検証

各ユーザ要因を正しく測定するための条件である，(ア) 各ユーザ要因の観測変数の分布に偏りがないこと，(イ) 各観測変数が意図したユーザ要因を表していること，の 2 点の検証を行った．

(ア) を検証する方法としては，各観測変数に関する統計量が最大値や最小値に偏っているかどうかを確認するための，天井効果および床効果の検証が一般的であるが，項目困難度の検証 [33] もある．本論文で取り扱う観測変数の中には回答選択肢が二択となる質問も含まれる．このような質問の場合は，必ず天井効果，床効果のいずれかが発生するため，適していない．そこで，項目困難度が文献 [33] に記載の上限・下限の基準値範囲内である，0.2〜0.8 の値をとるように設定した．

その結果，全 103 項目中，リスク認知に関する 1 項目，技能習得・活用経験に関する 5 項目，および危険経験に関する全項目（4 項目）の観測変数が不適と判断された．(e) 危険経験は，質問設定の不備も考えられるが，今回のアンケート回答者の中には実際に被害を受けたユーザがそもそも少ないため，質問内容を変えたとしても結果は変わらな

い可能性が高い．そのため，以降の解析では，この (e) 危険経験は除外することにした．その他の観測変数以外は基準を満たしているため，以降の解析に用いることにする．

次に，(イ) 各観測変数が意図した要因を表しているかどうか検証を行った．パーソナリティ要因を測定するための既存の心理評価尺度に関してはすでにこの評価が行われているため，評価の対象外とし，今回質問から作成した行動，認知傾向要因（(a)〜(c)）および経験要因の中の技能習得・活用経験 (d) を評価の対象とする．一般に複数の観測変数が存在した場合にどのような下位尺度が存在するかを検証する場合，探索的因子分析により評価を行う．今回質問を作成したリスク回避行動，認知傾向要因，および，経験要因に関し，それぞれ探索的因子分析を行った．付録 2 にその結果を掲載している．その結果，行動，認知傾向要因（(a)〜(c)）および経験要因 (d) は，因子パターンが文献 [11], [22] に示されている値と同程度を示していた．また，認知傾向要因に関する観測変数は，質問意図どおり 3 つの因子に分類された．なお，各因子数はスクリー基準に基づいて選定している．さらに観測変数間の相関性の高さを表す内的整合性の度合いである α 係数を評価した．これらの係数は 0 から 1 の値をとり，1 に近ければ内的整合性が高いといえる．各種ユーザ要因に関しては 0.7 以上であったが，文献 [22] で良好とされている値と同程度以上であり，内的整合性があることが分かる．行動について 0.546 と他と比べて低くなっていたが，その理由としては，(1) パスワードの適切な管理・運用，(2) ウェブサイトを管理するサーバの信頼性確認，(3) 利用端末上での適切なログアウト処理は，リスク回避行動と一括りにできるものの，それぞれ独立した行動であるためと考えられる．他に比べて劣る結果となったが，楽観主義尺度 [23] における値と同程度（0.591）を示していることから，このまま利用した．

4.2.3 観測変数の削減

SEM によるモデル検証においては，観測変数の総数は 30 以内に収めることが推奨されている [34]．また，1 因子あたり，最低でも 3 個の観測変数であればモデルは安定的である [35] とされている．今回，行動とユーザ要因を合わせて 10 因子存在するため，観測変数の総数は最低でも 30 を超える．そこで，後者の条件を満たす最小の数に観測変数の数を圧縮した．具体的には，文献 [36] で示されている，いくつかの観測変数を合成し，数値の和を観測変数として用いる小包化という手法を用いた．観測変数の合成の方法はいくつかあるが，今回は，文献 [37] において有効とされている領域再現法を利用し，小包化を行った．領域再現法は，ある因子への因子パターンが（最大の項目 + 最小の項目），(2 番目に大きい項目 + 2 番目に小さい項目），(3 番目に大きい項目 + 3 番目に小さい項目）... という組合せで観測変数を合成し，新たな観測変数を定義する手法である．観測変数が奇数となり，合成する対象の観測変数が存在しない場合は，観測変数を 2 倍し，他の合成後の値のとる数値幅と合わせ，正規化する．確認的因子分析を用いて因子パターンを算出する手法と，この手法を繰り返し，各因子への観測変数が 3 個以上，4 個以下となるまで合成した．

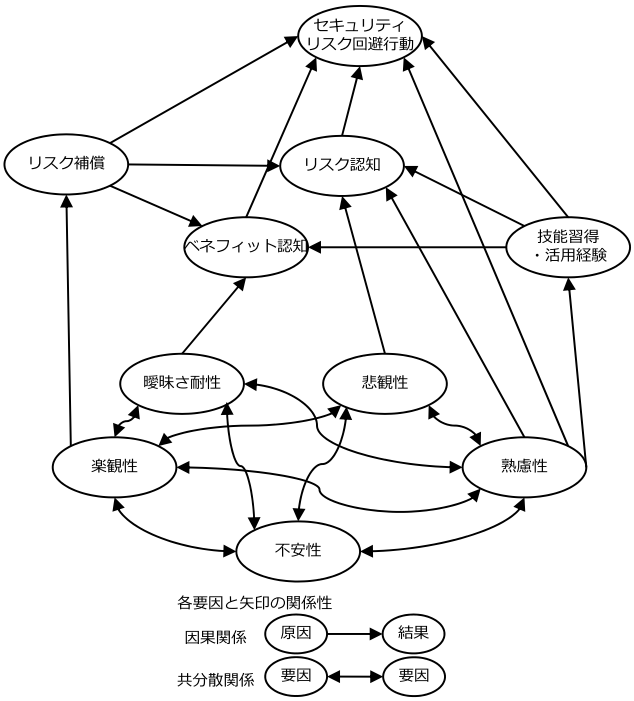

図 3 検証対象の仮説モデル
Fig. 3 Hypothesis model for evaluation.

4.2.4 パスの選定

明確なパス選定の基準がない場合，観測変数に対し，確認的因子分析を行い，因子間相関が高い場所に因果関係や共分散関係を置くことが推奨されている [34]．そこでまず，因子間相関を検証し，原因と結果の組を推定する．小包化した各観測変数に対し確認的因子分析を行い，因子間相関を導出した結果を付録 3 に示す．相関係数は，0.2 未満であればほぼ相関がないといえるため [38]，弱い相関も含む 0.2 以上の因子間にパスを設けることにした．**図 3** に因子間相関が 0.2 以上の要因間の組合せを含む仮説モデルを示す．

4.3 手順 3：提案モデルの妥当性評価

前節までに示した提案モデルの妥当性を SEM により検証する．SEM は共分散構造分析とも呼ばれ，潜在変数（構成概念）および観測変数の因果関係をモデル化し，仮説の妥当性を解析する手法である [34]．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 = 0.928，GFI = 0.895，RMSEA = 0.049 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．RMSEA は 0 に近いほど良く，0.08 未満でモデルは良好であると見なされる．CFI および RMSEA

に基づくと，モデルの適合度が高いといえる．GFI は良好といわれる基準値を超えていないが，観測変数が 30 を超える場合には，これを下回ることも許容されている [34] ため，総合的に判断すると，今回示したモデルは適合度が高い．したがって妥当なモデルであるといえる．

なお，これらの適合度を示す値は，既存論文（文献 [11] など）にも記されているが，回答者数や属性，質問が異なるデータ間での比較に意味をなさないため定量比較は行うことができない．そのため本論文では，既存論文との定量比較は実施していない．

5. 結果と考察

5.1 セキュリティリスク回避行動への各要因の効果

図 4 に，SEM による解析結果を示す．各パスに記載の標準化されたパス係数は，−1〜1 の値をとり，絶対値が大きいほど影響を与えていることを意味する．また，1%，5%，および 10%以内の有意水準を満たしているパスについては，値にそれぞれ **，*，+ を付加して記載している．この結果から，リスク認知や技術習得・活用要因は，パスワード漏えいリスク回避行動に直接正の影響を与えており，ベネフィット認知は直接，負の影響を与えていることが分かる．リスク補償および熟慮性は行動に対する直接の影響が小さいことが分かる．

ここで，各要因の行動への影響を表す総合効果は，以下の式で表される．

総合効果 = 直接効果 + 間接効果

直接効果は，ある要因からの直接的な影響，間接効果はある要因から，他の要因を介した影響である．

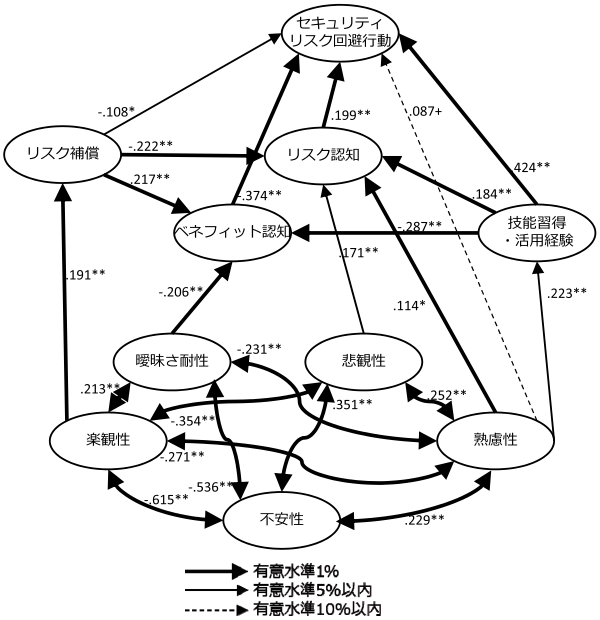

図 4 ユーザ要因とリスク回避行動の構造（CFI = 0.928，GFI = 0.895，RMSEA = 0.049）

Fig. 4 Structural model of risk averse behavior and user factors.

リスク補償の直接効果は −0.108 と小さい値であるが，リスク認知およびベネフィット認知を介した間接効果は $-0.222 \times 0.199 + 0.217 \times (-0.374) = -0.125$ であり，総合効果としては $-0.108 - 0.125 = -0.233$ である．この値は，リスク認知の総合効果より高い値となっている．このことから，認知傾向要因の中でもリスク補償は，直接的に与える影響と同程度に他の要因を介した影響があり，その影響はリスク認知よりも行動に影響があると考えられる．また，行動に最も影響を与える要因は技能習得・活用経験であり，その総合効果は 0.568 であった．

5.2 パーソナリティ要因が行動へ与える影響

熟慮性を除くパーソナリティ要因（楽観性，悲観性，曖昧さ耐性，および熟慮性）は直接行動につながる要因ではなく，他の要因を介した影響を示した．また，熟慮性は，行動に対し，直接効果が 0.087 である一方，間接効果は 0.149 であり，間接的な関係性の方が強い．これらのことから，パーソナリティ要因は，主にユーザの認知傾向や経験に影響を与え，その結果，行動へ影響すると考えられる．このことから，各ユーザのパーソナリティ要因の傾向によって，どのような認知傾向や経験をもたらすかということを推測することができ，ユーザへのリスク回避行動促進への働きかけを効率化することができると考えられる．

ところで，文献 [39] では，因子間相関を加味せず，1 つの可能性として，パーソナリティが認知傾向または経験へ影響を及ぼし，認知傾向または技術習得・活用経験がセキュリティリスク回避行動に影響を与えるという 2 段階構成の仮説を立てそれを検証しているが，因子間相関をもとに構築した本論文における仮説でも同様の構造が得られ，整合性が確認できた．

5.3 パーソナリティ要因が他のユーザ要因へ与える影響

結果から，認知要因と関係性が強いパーソナリティ要因が明らかとなった．リスク補償は楽観性から，リスク認知は悲観性および熟慮性から正の影響を受けており，ベネフィット認知は曖昧さ耐性から負の影響を受けている．この結果より，楽観性の高いユーザが，セキュリティ対策の効果を過大に見積もり，結果としてリスク回避行動をとらないことにつながると考えられる．また，状況に対して悲観的にとらえる傾向や，よく考えて行動する傾向はリスクを適切にとらえることにつながり，リスク認知傾向に影響を与えると考えられる．そして，曖昧さ耐性が低い傾向がベネフィット認知を誘発する理由としては，リスク回避が被害回避に直結するとは限らないため，その曖昧さが許容できず，ベネフィットのみをとらえてしまうことが考えられる．

熟慮性は，技能習得・活用経験にも影響を与える構造となった．これは，よく考えて行動する傾向が，セキュリ

ティ対策や設定に対し，興味を持ち，学習・活用することにつながっていると考えられる．

文献 [10] では，自己認識に基づく「不安になりやすい性格」がリスク認知につながると述べている．しかし，本解析により，客観的な指標による不安性は認知傾向要因やセキュリティリスク回避行動には関連性が薄いことが明らかとなった．これは自己認識による不安と，客観的な指標による不安になりやすさとにギャップが存在することが原因であると考えられる．これらの関係性の解明は今後の課題である．

5.4 性別による違い

文献 [40] において思考や認知の関係性に男女差が存在することが示唆されており，男性では，楽観性がリスク認知や犯罪不安の減少をもたらしていたが，女性では，楽観性はリスク認知や犯罪不安に影響を及ぼしていないことなどが述べられている．そこで，セキュリティリスク回避行動に関し，ユーザ要因が，他の要因や行動に与える影響の大きさに男女差が存在するかどうかを検証する．

まず，リスク回避行動と性別との相関関係を解析したところ，相関係数の大きさは 0.173（男性が 1，女性が 0 と数値化した場合）であり，リスク回避行動に関する大きな男女差が認められなかった．

男女それぞれの群における各ユーザ要因と行動の関係性を解析するために多母集団同時分析を行う．多母集団同時分析は各母集団における因子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最適と判断する [41]．

5.4.1 各種等値制約モデルの検証

等値制約なしモデル：はじめに，男女それぞれを母集団と見なした場合の配置不変性を検証する．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る．配置不変性は等値制約を設けないモデル（これを「等値制約なしモデル」とする）により検証が可能である．検証の結果，CFI = 0.926，GFI = 0.861，RMSEA = 0.050 となり，良好と判断された．このことから，男女それぞれの集団において提案モデルが適用できることが示唆された．このとき，AIC = 1903.9 であった．

因子負荷等値制約モデル：次に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（これを「因子負荷等値制約モデル」とする）の評価を行った．その結果 CFI = 0.925，GFI = 0.858，RMSEA = 0.049 となり，CFI および GFI は等値制約なしモデルと比べてやや低下しているが RMSEA はやや向上しており，それぞれにおいて基準範囲内である．等値制約なしモデルとの CFI の差 ΔCFI は 0.001 であり，これは適合度が維持されていることを示す基準 ΔCFI < 0.01 [42] を満たしているため，等値制約によるモデルの適合度の低下はないと考えられる．また，AIC = 1886.2 であり，等値制約なしモデルと比べて小さい．本モデルは，すべての因子負荷に等値制約を設けており，いずれかの因子負荷の一部に男女差が存在するか否かを評価していないためこの可能性を完全に否定できていないものの，上記の結果から，等値制約なしモデルと比較して，総じて良いモデルであり，因子負荷は男女間で等値である可能性が高いといえる．

パス変数等値制約モデル：最後に，共分散，各要因間および要因と行動間のパスの重みに男女差が存在しないという仮定のもとに，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（これを「パス変数等値制約モデル」とする）を検証した．その結果，CFI = 0.893，GFI = 0.831，RMSEA = 0.050 となり，RMSEA に変化はなかった．しかし CFI，GFI は低下し，さらに CFI が基準値を下回った．さらに AIC = 2171.1 であり，他のモデルと比較しても増大していることもあわせると，共分散，要因および行動間のいずれかのパスの重みに男女差が存在すると考えられる．

5.4.2 男女間におけるパスの重みの違い

男女間でパスの重みにどのような違いが存在するかを検証するために，因子負荷等値制約モデルを用いてパス係数の比較を行う．因子負荷等値制約モデルの標準化パス係数を**図 5** に示す．男性における分析においては，楽観性，悲観性，曖昧さ耐性から認知傾向要因へのパス係数のすべてが有意水準 1%以内となり，熟慮性からリスク認知へのパスも 5%以内となっている．一方女性における分析では，楽観性，悲観性，熟慮性が各認知傾向要因に与える影響が 10%以内の有意水準またはそれ以上という結果となり，曖昧さ耐性がベネフィット認知に与える影響のみが 5%以内水準となっている．このことから男性はパーソナリティ要因と認知傾向要因との関係性が大きいことが分かる．また，熟慮性は女性においてリスク認知経由ではなく行動に直結している傾向があった．

これらのことから性別とパーソナリティ要因の強さがどのような認知傾向や経験，行動をもたらすかを推定することが可能になり，パーソナリティや性別ごとに，セキュリティ対策の習慣化の促進を支援するための足がかりとなるといえる．

5.5 他のリスク回避行動への適用の可能性

本論文における仮説モデルは，セキュリティリスク回避

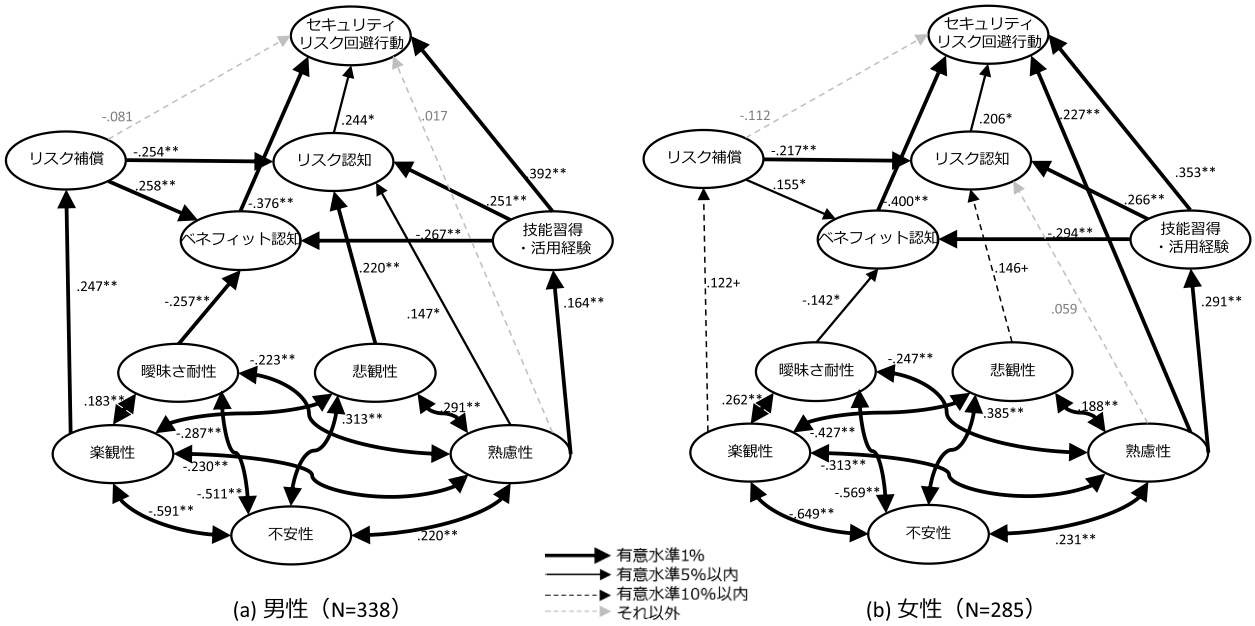

図 5 多母集団性別による因果関係の違い（CFI = 0.925，GFI = 0.858，RMSEA = 0.049，パス係数は男女別に標準化）

Fig. 5 Cause and effect model separated by gender.

に限らない各種行動と認知傾向要因，経験要因，およびパーソナリティ要因に関する文献を含む過去の知見を複数組み合わせ構築したが，パスワード漏えいリスクに対するモデルの妥当性が示唆された．このことから，他のリスクにおいても図 1 に示したような構造が存在しており，既存研究の知見はこの構造の一部を示していると考えられる．また，文献 [4] では，受験，スキーなどにおけるリスクテイキング行動においては，パーソナリティ要因は認知傾向要因を経由して行動に影響すると述べており，本論文における結果と整合性がとれる．したがって，本論文で示した構造は他のセキュリティリスクや，他の一般的なリスクに対する回避行動においても共通のモデルであることが期待される．しかしながら，各要因と行動との具体的な影響的数値を明らかにするためには，対象リスクに応じて各要因に関する質問紙を作成し，再度評価する必要があると考えられる．

今回対象とした被験者はウェブメール機能付きのアカウントサービスの利用者であることから，このサービスの非利用者に比べ，アカウントサービスを利用することにともなうリスクの受容がある．この点においてはリスク回避できていない群である．一方で，この群の中にもアカウントサービスを利用するリスクに対するベネフィットを重視し利用しているユーザや，リスク認知が不完全なユーザなど，利用者のリスク受容の理由が多岐にわたっていると考えられる．これを解明するためには，本論文で提案したモデルを利用し，ウェブメール機能付きのアカウントサービスへの登録を行うか否かのリスク回避に関する調査を行うことにより可能となる．また，アカウントサービスを利用することにともなうリスクを許容したユーザの中で，リスクを認知できていない群と，ベネフィットを重視した群などに分割したうえで，パスワード漏えいリスク回避行動に対するモデルを分析することにより，パスワード漏えいリスク回避行動における，より詳細な解析が可能になる．このように，関連する複数のリスク回避行動に関する解析を組み合わせた解析は今後の課題である．

6. まとめ

本論文では，セキュリティリスク回避行動とユーザ要因に関するアンケート調査を実施し，仮説モデルを構築した．提案モデルの有効性を検証するため，調査結果をもとに SEM による分析を行った結果，このモデルは高い適合性を示す結果となり，仮説が妥当であると示唆された．これにより，特定のパーソナリティ要因を持つことや，性別，認知傾向に応じて，セキュリティリスク回避行動をとるか否かが推定できるようになり，個々のユーザに対応した，セキュリティリスクの回避を支援する仕組みを構築できる目途が立った．本論文では，因果関係の仮説に基づき SEM による解析を行ったが，前述のとおり原因側の変数が対照実験を行った場合のような操作可能な変数でない限り，真の因果関係を断定できないことが指摘されている．また，検討したモデルは高い適合度を示したが，これは必ずしも他の因果関係を想定したモデルを否定する根拠にはならず，検討しなかった他のモデルの中にさらに最適なモデルが存在することも否定できない [5]．これらの点は，本論文で行った SEM による解析の限界としてあげられる．

今回の解析では，ウェブメール機能付きサービスにおけるパスワード漏えいリスクに限定し，認知傾向や経験，パーソナリティに関する普遍的な要因に焦点をあて解析を行ったため，ユーザ要因に応じ，警告や支援を実現するシステム

を構築するにあたり，今後は，今回検証ができなかった被害経験に関する要因，および状況依存の行動やそれにかかわる要因に範囲を拡大して解析を行うこと，およびユーザの状況依存の心理状態の測定方法などの検討を行う予定である．

謝辞 本研究成果は，国立研究開発法人情報通信研究機構の委託研究「ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発」により得られたものである．ここに深謝する．

参考文献

[1] 警察庁：平成 26 年中のサイバー空間をめぐる脅威の情勢について，入手先 ⟨http://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf⟩（参照 2016-06-23）．
[2] 加藤岳久，中澤優美子，漁田武雄，山田文康，山本 匠，西垣正勝：本人認証技術におけるユーザの性格とセキュリティ意識との相関に関する考察，情報処理学会論文誌，Vol.52, No.9, pp.2537–2548 (2011).
[3] トレンドマイクロ：「Web 脅威対策」機能について，入手先 ⟨http://esupport.trendmicro.com/support/vb/solution/ja-jp/1313955.aspx⟩（参照 2016-06-23）．
[4] 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 (1998).
[5] 前田忠彦：日本人の満足度の構造とその規定因に関する因果モデル，数理統計，Vol.43, No.1, pp.141–160 (1995).
[6] 警察庁：平成 27 年度警察白書，入手先 ⟨https://www.npa.go.jp/hakusyo/h27/index.html⟩（参照 2016-06-23）．
[7] 警察庁：平成 26 年中の不正アクセス行為の発生状況等の公表について，入手先 ⟨http://www.npa.go.jp/cyber/statics/h26/pdf040.pdf⟩（参照 2016-06-23）．
[8] 総務省情報通信政策研究所：青少年のインターネット・リテラシー指標［指標開発編］，入手先 ⟨http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2012/ilas2012-report-build.pdf⟩（参照 2016-06-23）．
[9] 山本太郎：インターネット不安発生モデルのリスク認知・信用・信頼スキーマ仮説について，マルチメディア，分散，協調とモバイル（DICOMO2014）シンポジウム，pp.1513–1519 (2014).
[10] 山本太郎：インターネット利用時の不安発生モデルに対する心理学的知見の適用に関する一考察，情報処理学会研究報告セキュリティ心理学とトラスト（SPT），pp.1–6 (2014).
[11] 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).
[12] 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，マルチメディア，分散，協調とモバイル（DICOMO2014）シンポジウム，pp.1498–1505 (2014).
[13] 芳賀 繁：安全技術では事故を減らせない—リスク補償行動とホメオスタシス理論，電子情報通信学会技術研究報告 SSS，安全性，Vol.109, No.151, pp.9–11 (2009).
[14] Blythe, J.M., Coventry, L. and Little, L.: Unpacking security policy compliance: Exploring motivators and barriers of employees' security behaviors, *11th Symposium on Usable Privacy and Security* (2015).
[15] Wash, R. and Rader, E.: Too Much Knowledge? Security Beliefs and Protective Behaviors Among US Internet Users, *11th Symposium on Usable Privacy and Security* (2015).
[16] 芳賀 繁：不安全行動のメカニズム，電子情報通信学会技術研究報告, SSS, 安全性, Vol.99, No.238, pp.29–34 (1999).
[17] Zuckerman, M. and Kuhlman, D.: Personality and Risk-Taking: Common Biosocial Factors, *Journal of Personality*, Vol.68, No.6 (2000).
[18] 廣瀬文子：ヒューマンエラー傾向測定手法作成の試み，電力中央研究所報告 Y 研究報告 No.6014，pp.1–17, 巻頭 1〜4 (2007).
[19] 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（SCIS2015）(2015).
[20] 薬師神玲子，米持圭介：曖昧さ耐性と購買場面における意思決定，青山心理学研究，Vol.4, pp.49–54 (2004).
[21] 上市秀雄, 楠見 孝：後悔がリスク志向・回避行動における意思決定に及ぼす影響，認知科学, Vol.7, No.2, pp.139–151 (2000).
[22] 日景奈津子，カールハウザー，村山優子：情報セキュリティ技術に対する安心感の構造に関する統計的検討，情報処理学会論文誌，Vol.48, No.9, pp.3193–3203 (2007).
[23] 堀 洋道，山本眞理子：心理測定尺度集 I 人間の内面を探る〈自己・個人内過程〉，サイエンス社 (2001).
[24] 木島伸彦，高橋弘司，野口裕之，渡辺直登：パーソナリティ尺度と組織社会化諸尺度との関連性，経営行動科学，Vol.12, No.1, pp.31–48 (1998).
[25] 土田昭司：リスク認知・判断についての社会心理学的一考察，セミナー年報 2008, pp.129–138 (2008).
[26] 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).
[27] 総務省：通信利用動向調査（世帯編）平成 26 年報告書，入手先 ⟨http://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201400_001.pdf⟩（参照 2016-06-23）．
[28] Google Inc.：Gmail – Google の無料ストレージとメール，入手先 ⟨https://www.gmail.com/⟩（参照 2016-06-23）．
[29] Microsoft: Hotmail, available from ⟨https://login.live.com/⟩ (accessed 2016-06-23).
[30] ヤフー株式会社：Yahoo!メール，入手先 ⟨https://mail.yahoo.co.jp⟩（参照 2016-06-23）．
[31] 総務省：統計局人口推計，入手先 ⟨http://www.stat.go.jp/data/jinsui/2014np/⟩（参照 2016-06-23）．
[32] 堀 洋道，吉田富二雄：心理測定尺度集 III 心の健康をはかる〈適応・臨床〉，サイエンス社 (2001).
[33] 村上宣寛：心理尺度の作り方，北大路書房.
[34] 豊田秀樹：共分散構造分析［入門編］，朝倉書店 (1998).
[35] 小島隆矢：Excel で学ぶ共分散構造分析とグラフィカルモデリング，オーム社 (2003).
[36] 狩野 裕：再討論：誤差共分散の利用と特殊因子の役割，行動計量学，Vol.29, No.2, pp.182–197 (2002).
[37] 清水和秋，山本理恵：小包化した変数によるパーソナリティ構成概念間の関係性のモデル化—Big Five・不安（STAI）・気分（POMS），関西大学社会学部 (2007).
[38] 水本 篤：質問紙調査における相関係数の解釈について，外国語教育メディア学会（LET）関西支部 メソドロジー研究部会 2011 年度報告論集，pp.63–73 (2011).
[39] 澤谷雪子, 山田 明, 半井明大, 松中隆志, 浦川順平, 窪田 歩：インターネット上の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の相互関係の分析，コンピュータセキュリティシンポジウム 2015 論文集 (2015).
[40] 荒井崇史, 吉田富二雄：楽観性がリスク認知犯罪不安 防犯行動へ及ぼす影響，筑波大学心理学研究，No.40, pp.9–19 (2010).
[41] 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).

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

付　　録

A.1 質問項目と統計値

（グレーアウトは項目困難度が基準値から逸脱していた項目）

質問意図	観測変数	質問内容	平均値	項目困難度	得点
行動	Pass ＝Pass1 ＋Pass2 ＋Pass3 ＋Pass4	Pass1:ログインパスワードを定期的に変更していない（はい:0、いいえ：1） Pass2:ログインパスワードの構成は数字と文字と記号（はい：1、いいえ：0） Pass3:ログインパスワードの文字数が8桁以上（はい：1、いいえ：0） Pass4:同じログインパスワードを使っているサービスはない（サイトごとに全く違うパスワードを使っている）。（はい：1、いいえ：0）	1.55	0.39	0〜4
	SSL ＝SSL1 ＋SSL2	SSL1:カギマークの確認（いつもする：2，たまにする：1，しない：0） SSL2:httpsを使っていることの確認（いつもする：2，たまにする：1，しない：0）	0.83	0.21	0〜4
	Logout	ログインしたサイトを閲覧終了する際に、ログアウトボタンをはじめに操作する。	1.06	0.53	いつもする：2，たまにする：1，しない：0
リスク認知	a1	複雑なパスワードのほうが安全だと思う	2.97	0.74	
	a2	ID・パスワードは紙に書いておくと誰かに見られる危険があると思う	2.64	0.66	
	a3	定期的にパスワードを変えた方が安全だと思う	3.14	0.79	とてもそう思う：4
	a4	ネットカフェ・学校のPCなどほかの人も使うPCを使う場合には注意しないとパスワードが盗まれることがあると思う	3.14	0.78	ややそう思う：3 どちらとも言えない：2
	a5	ネットカフェ・学校のPCなどほかの人も使うPCを使う場合には注意しないと閲覧履歴が残ってしまうと思う	3.26	0.82	あまりそう思わない：1 全くそう思わない：0
	a6	自分の端末で公衆WiFiを使う場合にパスワードが盗まれることがあると思う	2.63	0.66	
ベネフィット認知	b1	パスワードを考えるのは面倒なので簡単なパスワードにしたい	2.17	0.54	
	b2	定期的にパスワードを変える作業は面倒なのでしたくない	2.74	0.68	とてもそう思う：4
	b3	サービス毎にパスワードを変えるのは面倒なので同じパスワードを使いたい	2.55	0.64	ややそう思う：3
	b4	パスワードはわかりやすいもの（生年月日や並びの数字123）を用いると忘れなくていい	1.68	0.42	どちらとも言えない：2 あまりそう思わない：1
	b5	パスワードを変えると忘れてしまうので変更したくない	2.70	0.68	全くそう思わない：0
	b6	サービス毎に違うパスワードにすると忘れてしまうので同じパスワードを使いたい	2.54	0.64	
リスク補償	c1	パスワード管理ソフトを使えば安全だと思う	1.88	0.47	
	c2	ウィルス対策ソフトを導入しているので、パスワードは漏えいすることはないと思う	1.56	0.39	
	c3	パスワード管理ソフトを使っているのでパスワードは漏えいすることはない	1.35	0.34	
	c4	ネットカフェ・学校のPCなどほかの人も使うPCを使う場合でも、履歴が残らないモードを使うとパスワードが漏えいしなくて安全だと思う	1.64	0.41	とてもそう思う：4 ややそう思う：3
	c5	ネットカフェ・学校のPCなどほかの人も使うPCを使う場合でも、履歴が残らないモードを使うと閲覧履歴が漏えいしなくて安全だと思う	1.64	0.41	どちらとも言えない：2 あまりそう思わない：1
	c6	自分の端末で公衆WiFiを使う場合、履歴が残らないモードを使えばパスワードが漏えいしなくて安全だと思う	1.61	0.40	全くそう思わない：0
	c7	自分の端末で公衆WiFiを使う場合、履歴が残らないモードを使えば閲覧履歴が漏えいしなくて安全だと思う	1.63	0.41	
技能習得・活用経験	d1	情報システムなどのセキュリティを考える仕事をしている・経験がある	0.09	0.09	
	d2	メールサーバ・webサーバなどのサーバを構築し、運用した経験がある	0.10	0.10	
	d3	無線LANルータ設定の暗号化設定をしたことがある	0.26	0.26	
	d4	サーバに適切なファイヤウォールやセキュリティ設定をしたことがある	0.31	0.31	
	d5	フィッシングサイトの被害に遭わないように自分で対策方法を調べたことがある	0.28	0.28	はい：1
	d6	フィッシングサイトの被害に遭わないように対策方法を家族・知人から聞いたことがある	0.16	0.16	いいえ：0
	d7	安全なパスワード設定（桁数や更新頻度など）について調べたことがある	0.31	0.31	
	d8	安全なパスワード設定（桁数や更新頻度など）について家族・知人に聞いたことが ある	0.15	0.15	
	d9	安全なパスワード管理（保存方法など）について調べたことがある	0.32	0.32	
	d10	安全なパスワード管理（保存方法など）について家族・知人に聞いたことがある	0.17	0.17	
危険経験	e1	人のPCにパスワード・履歴が保存され悪用されたことがある	0.04	0.04	
	e2	ID、パスワードが漏えいし、自分のIDからスパムメールや攻撃がおこなわれたことがある	0.06	0.06	自分・家族・知人のいずれかがあてはまる：1
	e3	偽サイトを間違えて本物サイトであると勘違いしてしまったことがある	0.05	0.05	自分・家族・知人のだれもあてはまらない：0
	e4	ID、パスワード、クレジットカード番号などの情報が盗まれ、金銭的被害に遭遇したことがある	0.02	0.02	
楽観性	f1	結果がどうなるかはっきりしない時は、いつも一番良い面を考える。	2.95	0.49	
	f2	いつもものごとの明るい面を考える。	2.94	0.48	非常にあてはまる：5
	f3	自分の将来に対しては非常に楽観的である。	2.83	0.46	ややあてはまる：4
悲観性	g1	何か自分にとってまずいことになりそうだと思うと、たいていそうなってしまう。	3.07	0.52	どちらともいえない：3
	g2	自分に都合良くことが運ぶだろうなどとは期待しない。	3.37	0.59	ややあてはまらない：2
	g3	ものごとが自分の思い通りに運んだためしがない。	2.92	0.48	全くあてはまらない：1
	g4	自分の身に思いがけない幸運が訪れるのを当てにすることは、めったにない。	3.37	0.59	
曖昧さ耐性	h1	もしはっきりした答えにたどり着けない可能性があるなら、問題に取り組むのは嫌だ。	3.10	0.52	
	h2	後になってからこう言っておけばよかったと後悔することが多い。	3.56	0.64	
	h3	答えがないような問題はつまらない。	3.04	0.51	
	h4	物事を成し遂げるためには、正しい方法と間違った方法があると考えている。	3.46	0.61	
	h5	冗談の意味がよくわからないときには、それがわかるまですっきりしない。	3.14	0.53	
	h6	初めて会う人がどんな反応を私に示すかわからないと困る。	3.07	0.52	
	h7	人の考えについていけなくて困ることがある。	3.11	0.53	
	h8	周りの人とのコミュニケーションが欠けていたら私は仕事がうまくできない。	3.36	0.59	
	h9	私ははっきりしない状況にも耐えることができる。 *r	2.85	0.71	
	h10	明確な議題があれば、会議はうまくいくものだ。	3.47	0.62	そうだ：5
	h11	仲の良い友だちと意見が衝突すると困る。	3.15	0.54	どちらかといえばそうだ：4
	h12	自分でコントロールできるような確実なことをするのが好きだ。	3.55	0.64	どちらともいえない：3
	h13	セールスマンに会うと、何を売っているのか知りたがる。	2.30	0.32	どちらかといえばちがう：2
	h14	自分の行動が周りの人にどんな影響を与えるのか分からないと不安である。	2.85	0.46	ちがう：1
	h15	知らない人の多いパーティやコンパはおもしろくないだろう。	3.40	0.60	*rは逆転項目（点数を反転）
	h16	周りの人が笑っていると、なぜ笑っているのかが気になる。	3.18	0.55	
	h17	周囲の人々についてよく知らないと、一緒にいても楽しくない。	3.27	0.57	
	h18	第一印象は重要だと思う。	4.10	0.77	
	h19	今何時なのかをいつも気にしている。	2.78	0.44	
	h20	成功するという確信がないなら、計画を実行に移したくない。	3.02	0.51	
	h21	今日が何日か知っていないと気持ちが悪い。	2.77	0.44	
	h22	他の人が私を評価するときは、はっきりとした評価をして欲しいと思う。	3.30	0.57	
	h23	一旦始めたら、それが終わるまで他の仕事を始めたくない。	3.22	0.55	
	h24	思い通りにできないような状況だと、かなり不安になる。	3.36	0.59	
熟慮性	i1	何でもよく考えてみないと気がすまないほうだ。	2.83	0.61	
	i2	何事も時間をじっくりかけて考えたいほうだ。	2.80	0.60	
	i3	深く物事を考えるほうだ。	2.81	0.60	
	i4	何かを決めるとき、時間をかけて慎重に考えるほうだ。	2.79	0.60	あてはまる：4
	i5	全ての選択肢をよく検討しないと気がすまないほうだ。	2.69	0.56	どちらかと言えばあてはまる：3
	i6	用心深いほうだ。	2.89	0.63	どちらかと言えばあてはまらない：2
	i7	実行する前に考えなおしてみることが多いほうだ。	2.77	0.59	ちがう：1
	i8	買物は、前もっていろいろ調べてからするほうだ。	2.83	0.61	*rは逆転項目（点数を反転）
	i9	計画を立てるよりも早く実行したいほうだ。*r	2.59	0.53	
	i10	よく考えずに行動してしまうことが多いほうだ。*r	2.61	0.54	
不安性	j1	たのしい。*r	2.38	0.46	
	j2	疲れやすい。	2.69	0.56	
	j3	泣きだしたくなる。	1.78	0.26	
	j4	ほかの人と同じくらい幸せであったならと思う。	2.40	0.47	
	j5	すぐに決心がつかず迷いやすい。	2.36	0.45	
	j6	ゆったりした気持ちである。*r	2.67	0.56	
	j7	平静・沈着で落ち着いている。*r	2.61	0.54	
	j8	困難なことがかさなると圧倒されてしまう。	2.52	0.51	
	j9	実際に大したこともないことが気になってしかたがない。	2.35	0.45	全くそうである：4
	j10	幸せである。*r	2.50	0.50	ほぼそうである：3
	j11	物事を難しく考える傾向がある。	2.45	0.48	いくぶんそうである：2
	j12	自信が欠如している。	2.45	0.48	まったくそうでない：1
	j13	安心している。*r	2.67	0.56	*rは逆転項目（点数を反転）
	j14	やっかいなことは避けて通ろうとする。	2.61	0.54	
	j15	憂うつである。	2.09	0.36	
	j16	満足している。*r	2.75	0.58	
	j17	ささいなことに思いわずらう。	2.32	0.44	
	j18	ひどくがっかりした時には気分転換ができない。	2.40	0.47	
	j19	物に動じないほうである。*r	2.89	0.63	
	j20	身近な問題を考えるとひどく緊張し混乱する。	2.15	0.38	

A.2 因子分析結果

A.2.1 行動に関する因子分析結果

観測変数	行動
SSL	**.427**
Logout	**.792**
Pass	**.431**
α係数	.546

A.2.2 認知要因に関する因子分析結果

観測変数	リスク認知	ベネフィット認知	リスク補償
a1	**.584**	.070	.085
a2	**.496**	-.055	.105
a3	**.682**	-.070	.045
a4	**.664**	.062	-.157
a6	**.558**	-.060	-.020
b1	-.050	**.646**	.035
b2	.089	**.753**	-.042
b3	-.023	**.876**	-.002
b4	-.126	**.505**	.069
b5	.038	**.786**	.004
b6	-.011	**.832**	-.002
c1	.183	.068	**.444**
c2	-.025	.053	**.562**
c3	-.065	-.039	**.586**
c4	.037	-.038	**.850**
c5	.035	-.035	**.836**
c6	-.036	-.008	**.795**
c7	-.003	.074	**.793**
α係数	.720	.875	.868

A.2.3 経験要因に関する因子分析結果

観測変数	技能習得・活用経験
d3	**.439**
d4	**.444**
d5	**.697**
d7	**.799**
d9	**.855**
α係数	.789

A.3 小包化後の確認的因子分析結果

（CFI = 0.937，GFI = 0.906，RMSEA = 0.047）
※赤字は因子間相関が確認された相関係数

観測変数	リスク回避行動	リスク認知	ベネフィット認知	リスク補償	技能習得・活用経験	楽観性	悲観性	曖昧さ耐性	熟慮性	不安性
Pass	**.576**	.000	.000	.000	.000	.000	.000	.000	.000	.000
SSL	**.631**	.000	.000	.000	.000	.000	.000	.000	.000	.000
Logout	**.406**	.000	.000	.000	.000	.000	.000	.000	.000	.000
a2+a3	.000	**.623**	.000	.000	.000	.000	.000	.000	.000	.000
a1+a4	.000	**.828**	.000	.000	.000	.000	.000	.000	.000	.000
a6 ×2	.000	**.554**	.000	.000	.000	.000	.000	.000	.000	.000
b3+b4	.000	.000	**.844**	.000	.000	.000	.000	.000	.000	.000
b6+b1	.000	.000	**.911**	.000	.000	.000	.000	.000	.000	.000
b2+b5	.000	.000	**.764**	.000	.000	.000	.000	.000	.000	.000
c4+c1	.000	.000	.000	**.752**	.000	.000	.000	.000	.000	.000
c5+c2	.000	.000	.000	**.850**	.000	.000	.000	.000	.000	.000
c7+c3	.000	.000	.000	**.870**	.000	.000	.000	.000	.000	.000
c6 ×2	.000	.000	.000	**.771**	.000	.000	.000	.000	.000	.000
d9+d4	.000	.000	.000	.000	**.811**	.000	.000	.000	.000	.000
d7+d3	.000	.000	.000	.000	**.793**	.000	.000	.000	.000	.000
d5 ×2	.000	.000	.000	.000	**.728**	.000	.000	.000	.000	.000
f1	.000	.000	.000	.000	.000	**.551**	.000	.000	.000	.000
f2	.000	.000	.000	.000	.000	**.807**	.000	.000	.000	.000
f3	.000	.000	.000	.000	.000	**.660**	.000	.000	.000	.000
g1	.000	.000	.000	.000	.000	.000	**.386**	.000	.000	.000
g2	.000	.000	.000	.000	.000	.000	**.676**	.000	.000	.000
g3	.000	.000	.000	.000	.000	.000	**.694**	.000	.000	.000
g4	.000	.000	.000	.000	.000	.000	**.624**	.000	.000	.000
h1+h22+h12+h15+h3+h19+h6+h10	.000	.000	.000	.000	.000	.000	.000	**.712**	.000	.000
h2+h23+h17+h9+h24+h13+h14+h4	.000	.000	.000	.000	.000	.000	.000	**.828**	.000	.000
h20+h18+h11+h8+h7+h21+h16+h5	.000	.000	.000	.000	.000	.000	.000	**.809**	.000	.000
i3+i8+i4+i9	.000	.000	.000	.000	.000	.000	.000	.000	**.888**	.000
i5+i6+i2+i10	.000	.000	.000	.000	.000	.000	.000	.000	**.918**	.000
i1+i7 ×2	.000	.000	.000	.000	.000	.000	.000	.000	**.760**	.000
j17+j10+j11+j2+j12+j7+j9+j19	.000	.000	.000	.000	.000	.000	.000	.000	.000	**.913**
j8+j13+j5+j4+j18+j6+j15+j1	.000	.000	.000	.000	.000	.000	.000	.000	.000	**.937**
j20+j16+j3+j14 ×2	.000	.000	.000	.000	.000	.000	.000	.000	.000	**.826**

	リスク回避行動	リスク認知	ベネフィット認知	リスク補償	技能習得・活用経験	楽観性	悲観性	曖昧さ耐性	熟慮性	不安性
リスク回避行動	1.000									
リスク認知	.358	1.000								
ベネフィット認知	-.555	-.016	1.000							
リスク補償	-.327	-.271	.267	1.000						
技能習得・活用経験	.619	.250	-.320	-.166	1.000					
楽観性	.014	.009	.080	.204	.030	1.000				
悲観性	.033	.239	.005	-.031	.011	-.396	1.000			
曖昧さ耐性	-.093	-.185	-.227	-.091	.061	.267	-.175	1.000		
熟慮性	.301	.224	-.186	-.101	.218	-.283	.284	-.268	1.000	
不安性	-.065	.077	.125	-.062	-.025	-.630	.435	-.566	.247	1.000

α係数	.546	.697	.876	.885	.813	.710	.681	.828	.885	.920

澤谷 雪子

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 総合研究所にてネットワークセキュリティの研究開発に従事．電子情報通信学会会員．

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 年から 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．電子情報通信学会，ACM，IEEE 各会員．

半井 明大 （正会員）

2012 年東北大学大学院情報科学研究科博士課程前期 2 年の課程修了．同年 KDDI（株）入社．現在，（株）KDDI 総合研究所にてネットワークセキュリティ，デバイスセキュリティ，ヒューマンファクターセキュリティの研究開発に従事．

浦川 順平 （正会員）

2011 年電気通信大学大学院電気通信学研究科情報工学専攻博士前期課程修了．同年 KDDI（株）入社．（株）KDDI 総合研究所にてネットワークセキュリティの研究開発に従事．電子情報通信学会会員．

松中 隆志 （正会員）

2004 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．同年 KDDI（株）入社．（株）KDDI 研究所（現，（株）KDDI 総合研究所）にて無線通信，ネットワークセキュリティの研究開発に従事．現在 KDDI（株）．

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 年から 2004 年米国 UC Berkeley 客員研究員．現在，（株）KDDI 総合研究所にてネットワークセキュリティの研究開発に従事．