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

澤谷 雪子　山田 明　半井 明大　松中 隆志　浦川 順平　窪田 歩
株式会社 KDDI 研究所
356-8502 埼玉県ふじみ野市大原 2-1-15
{yu-sawaya, ai-yamada, ak-nakarai, ta-matsunaka, ju-urakawa, kubota}@kddilabs.jp

あらまし ヒューマンエラーや不安全行動のようなセキュリティリスクにつながる不用意な行動を回避する能力は，知識・経験などのユーザ固有の要因に基づく．我々は，ユーザ要因に応じて，セキュリティリスクの回避を支援する仕組みを目指している．これまで，セキュリティリスク回避行動とユーザ要因に関する相関性が分析されている．しかし，性格や環境のような直接行動に影響を与えないユーザ要因がどのように行動に影響を与えるかについては分析があまり行われていない．本稿では，ユーザ要因の直接的な関係だけでなく間接的な関係を考慮した二階層からなるセキュリティリスク回避行動モデルを提案する．提案モデルの有効性を検証するため，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，調査結果をもとに構造方程式モデリングによる分析を行った．その結果，間接的な要因を考慮した二階層行動モデルは、直接的なモデルに比べて高い適合性を示すことが分かった．

Understanding the Relationships among security risk aversion and User-Related Factors

Yukiko Sawaya　Akira Yamada　Akihiro Nakarai　Takashi Matsunaka
Jumpei Urakawa　Ayumu Kubota
KDDI R&D Laboratories, Inc.
2-1-15 Ohara, Fujimino-shi, Saitama 356-8502, JAPAN

Abstract Since the probability of being victim of attacks depends on each user's knowledge, experience, environment, and deviation in judgement, the risk aversion encouraging system that meets each user's status and circumstance. For this goal, it is needed to analyze both direct and indirect relationships among security risk aversion behaviors and user-related factors. In this paper, we carried out the questionnaire targeting the Internet users and analyzed such relationships and found the factors that influence the security risk aversion by structural equation model.

1　はじめに

パソコンやスマートフォンの普及に伴い，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，インターネット上の詐欺，迷惑メール，不正アクセスなどが問題になっており，警察に対するサイバー犯罪に関する相談件数もまた増加している[1].

情報漏えいやセキュリティインシデントはヒューマンエラーや不安全行動によって引き起こされる可能性が高く，これらセキュリティリスクを回避する行動は，各ユーザの知識，経験，環境，認知判断傾向などのユーザ固有の要因に依存している[2]．そのため，ユーザにセキュリティリスクを回避させるには，各ユーザの置かれた状況や性格などのユーザ要因を考慮する必要がある．しかし昨今のセキュリティ対策ソフト[3]で行っているリスク回避支援は全てのユーザに対して画一的な警告を出力するのみである.

そこで，我々は各ユーザの知識，経験，環境，認知判断傾向などのユーザ要因に応じ，警告や支援を適切なタイミングで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は，前提としてセキュリティリスク回避行動時に関係

する性格・操作技能・判断材料・知識の因果関係を明らかにし，セキュリティリスク回避行動の発生メカニズムを解明する必要がある．

セキュリティリスク回避行動とこれらユーザ要因の顕在化した関係を解明する方法として，従来研究では，ユーザ要因と，セキュリティ被害経験やヒューマンエラー，セキュリティリスクテイキング行動などとの相関分析及び回帰分析が行われている[2,4,5,6]．しかしながらこの方法では，強い相関関係が確認できたとしても他の要因を介した疑似相関である可能性があり，行動とユーザ要因の因果関係を正しく知ることはできない．別の既存研究では，自動車運転などにおける不安全行動と，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・行動傾向に関連性が示されており[7]，これらの背後に共通のユーザ要因が存在することが窺える．

そこで本稿では，まず，ユーザ要因を(1)セキュリティリスク回避行動に直結する前面要因と，(2)これらの要因に影響を与える背景要因とに分類し，これらとセキュリティリスク回避行動との関係性に関するモデルを提案する．次にこの提案モデルを検証するために構造方程式モデリングを行い，行動とユーザ要因それぞれの直接的及び間接的な因果関係を解析する．これにより，今まで明らかにできていない各ユーザ要因と行動の因果関係，および，セキュリティリスク回避行動に強く影響を与えているユーザ要因を明らかにする．

2　関連研究と本稿の目的

本章では，セキュリティ被害とユーザ要因の関係性や，一般的な不安全行動とユーザ要因との関係性の解析，一般的なリスクテイキングにおけるユーザ要因間の因果関係の解析に関する文献について述べた後，本稿の目的について述べる．

2.1　ユーザ要因とセキュリティ被害

文献 4 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，被害に遭いやすいユーザの心理や行動における特性を明らかにしている．また，文献 5 では， IT 被害に遭いやすいユーザ特有の心理特性と，ユーザの行動を示す PC の操作ログとの相関分析を行い，行動ログからの被害の可能性を推定している．

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，性格特性と種々の認証技術に関するセキュリティ意識との間に関係性が存在することを述べている．また，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．

2.2　不安全行動とユーザ要因

文献 7 では，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，同性同世代の中では，ある場面でより不安全な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 8 によるとリスクを低減できる安全技術や能力の向上により，リスクが低下したと認識した際に，リスク回避行動をとらなくなるという．これはリスク補償と呼ばれており，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と述べている．

文献 6 においても，飲酒や喫煙などのリスクテイキング行動間に相関がみられることを示している．また，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．

2.3　ユーザ要因間の因果関係解析

文献 9 では，受験，スキー，パチンコなどにおけるリスクテイキング行動に関するユーザ要因間の因果関係を分析している．リスク認知（損失に対する認識），利益に対する認識（ベネフィット認知），能力の自己評価などの認知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は認知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．

2.4　本稿の目的

相関分析や回帰分析ではユーザ要因とセキュリティ回避行動に強い相関関係が確認できたとしても他の要因を介した疑似相関である可能性がある．また，文献 5 にあるように，IT 被害に遭いやすい心理特性と相関関係が強い操作傾向が必ずしも行動に影響を与えるユーザ要因であるとは限らないため，行動とユーザ要因の因果関係を正しく知ることはできない．

一方，自動車事故や作業事故などの安全や，受験，スキー，パチンコなどの一般的な行動に関するリスクテイキング行動とユーザ要因の因果関係の解析は行われているものの，最適なモデルは提案されていない．また，インターネットにおけるセキュリティリスク回避とユーザ要因の因果関係は未だ解明されていない．

そこで，本稿では，セキュリティリスク回避行動とユーザ要因の因果関係，及びユーザ要因間の因果関係についてのモデルを提案し，これを検証する．これによりインターネット上のセキュリティリスクの低減に強く影響を与える要因の特定を行う．

3　提案モデル

本章では，セキュリティリスク回避行動と，行動に直接的及び間接的に影響を与える可能性のあるユーザ要因について整理し，これらの関係性に関するモデルを提案する．

3.1　ユーザ要因の定義

前章で挙げた文献をもとにパスワード漏えい，ウィルス被害などのセキュリティリスク回避行動に影響を与える要因を以下の環境要因，心理要因，状況要因，認知要因，知識習得要因，技術習得要因，及び操作技能要因に分類する．

(a) 認知要因

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．セキュリティリスクを正しくリスクとして認識できるかどうか（リスク認知）や，セキュリティリスク回避行動の煩雑さや面倒さを排除するため，セキュリティリスク回避行動をとりたくないと感じているか（ベネフィット認知）に関する要因を含む．また文献 8 で述べているリスク補償も判断に関する要素であるため，認知要因とする．

(b) 知識習得要因

セキュリティリスク回避方法に関する知識を習得した経験に関する要因である．セキュリティリスク回避のための適切な行動について調べたり聞いたりして知識を習得した経験の有無である．

(c) 技能習得要因

操作技能を習得した経験に関する要因である．タイピング練習ソフトなどの使用経験や，セキュリティリスク回避のための操作方法などを習得した経験の有無である．

(d) 操作技能要因

意図したとおりの操作が適切にできるかを示す要因であり，タイピング，クリック，タップ操作などを含む．

(e) 環境要因

ユーザの置かれた環境に関する要因である．セキュリティ設定などに詳しい家族や知人の有無，リスクに対して厳格な地位・立場に置かれている，セキュリティ業務経験があるなどの知識を習得しやすい環境に置かれていたかについての要因である．

(f) 心理要因

ヒューマンエラーや不安全行動に関連の深い心理に関する要因である．軽率さ，いい加減さなどの性格特性を含む．

(g) 状況要因

ユーザの置かれた状況に関する要因である．焦りの発生する状況，疲れなどを引き起こす状況などが該当する．

3.2　リスク回避行動とユーザ要因の関係

ユーザがセキュリティリスク回避行動をとる際，判断または操作の慣れ，ミスのない操作のいずれかまたはすべてが必要となる．一方，心理要因や環境要因などは，行動までの認知判断傾向や操作傾向に影響する背景的な要因であると考えられる．そこで図 1 のようにユーザ要因を前面要因と背景要因とに分類した因果関係のモデルを提案する．

リスク回避行動に直接関係する判断または操作

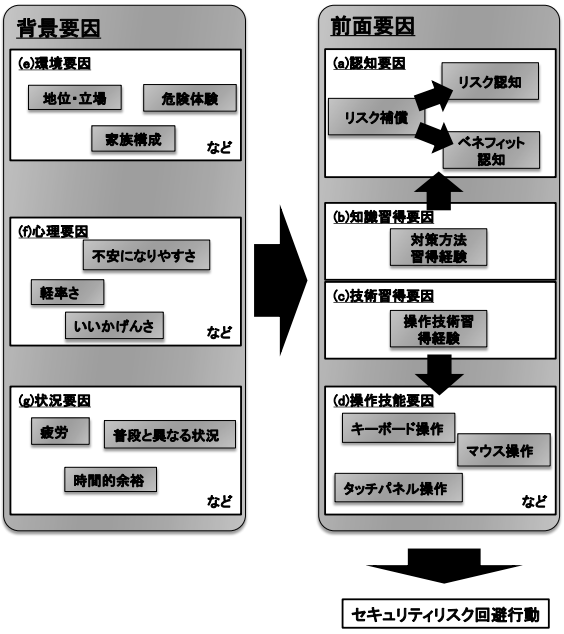

図 1　背景要因を考慮した
セキュリティリスク回避モデル

の慣れ，ミスのない操作に関する要因は，認知要因，知識習得要因，技術習得要因及び操作技能要因であるため，これらを前面要因とし，その他の環境要因・心理要因・状況要因を背景要因として仮定する．

また，前面要因間でも，技能習得要因は操作技能要因に，知識習得要因は認知要因に影響を与えることが想定されるため，この間にも因果関係を仮定する．さらにリスク補償はリスク認知，ベネフィット認知に影響を与える要因であると仮定する．

4 評価

本章では，前章で示した提案モデルをアンケート調査結果に基づいて検証する．

本評価検証では，対象とするセキュリティリスクを，ウェブサイト利用におけるパスワード漏えいリスクとし，各ユーザ要因がどのように影響を与えるかを示す．それに加えて，セキュリティリスク回避行動に強く影響を与える要因を調査する．提案モデルの検証には構造方程式モデリングを利用する．

4.1 検証対象

ウェブサイト利用におけるパスワード漏えいリスクを回避する行動は，文献 10 に基づき，(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等とする．

本評価では，アンケート調査に基づき分析を行うため，実際の状況にならないと計測できないない要因である，状況要因，操作技能要因，及び，この 2 つの要因に関連する技能習得要因については検証の対象外とする．

4.2 アンケート調査

本アンケート調査では，ウェブサイト利用時のパスワード漏えいリスクを有するウェブメールサービスの利用者を対象とした．調査実施概要は以下の通りである．

対象者

ウェブメール機能を有するサービス（Gmail[11]，Hotmail[12]，Yahoo!メール[13]など）の利用者とした．

性別・年齢層別人数

事前調査として 15 歳以上の 30,000 人に対し，ウェブメール機能付きサービスの利用有無を調査し，性・年代別に算定した利用者比率をもとに 623 名の回答者に対し調査を実施した．各性別・年齢層の分布は図 2 の通りである．

質問項目

質問項目は以下のとおりである．

- セキュリティリスク回避行動： 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回避行動，環境・心理・認知・知識習得要因に関する質問項目を設定した．パスワード漏えいリスク回避行動に関する質問項目として，(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について質問した．
- 認知要因： 認知要因はセキュリティリスク回避行動に関連する心理についての質問とした．
- 知識習得経験： セキュリティリスク回避行動に関連する学習経験についての質問とした．
- 環境要因： ユーザの一般的な環境に関する質問とした．
- 心理要因： 楽観的自己感情と悲観的自己感情の 2 点を測定できる楽観主義尺度，軽率さに関係する認知的熟慮性-衝動性尺度，不安に関係する状態-特性不安尺度（STAI）のうち特性不安尺度，いいかげんさに関連する曖昧さ耐性尺度[14,15]を用いた．

付録 1 に質問項目と調査結果を示す．一部の項目については一つの意図を測定するために，複数の質問の回答を合成している．

4.3 解析

質問項目の妥当性検証

構造方程式モデリングを行うにあたり，付録 1 の各項目がモデル検証に適しているかどうかの妥当性を検証する．妥当性検証方法には，回答の平均

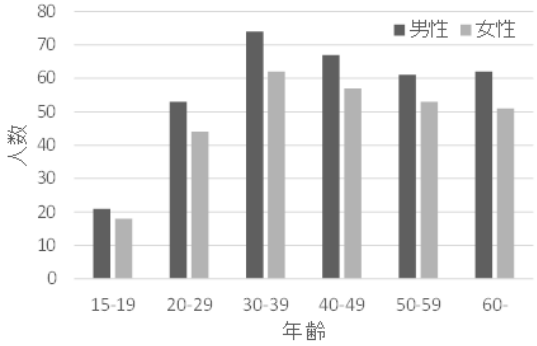

図 2 アンケート対象者分布

値を確認する方法[16]，天井効果・床効果を検証する方法，一部の回答に偏りがないかを判定する方法[17]などがある．今回は，経験などの事実に関する質問を多く含んでいるため，一部の質問に天井効果・床効果が生じる可能性がある．そこで一部の回答に大きな偏りがないかを判定する方法をとり，回答者の 90%以上が同じ回答をしていないことを確認することにより妥当性を検証する．

付録 1 に挙げた項目すべてがこの条件を満たすためこれらすべての項目を用いて構造方程式モデリングを行うこととする．

構造方程式モデリングによる提案モデルの検証

構造方程式モデリングは，共分散構造分析とも呼ばれ，潜在変数（構成概念）及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[18]．仮説モデルがデータに適合しているか否かを確認する方法としては．CFI (Comparative fit index)，GFI (Goodness-of-Fit Index)，RMSEA (Root Mean Square Error of Approximation)などの評価指標を用いる．本評価のモデル作成・評価には HAD[19]を用いる．

まず，提案モデルの前面要因，背景要因の概念に基づいた構造方程式モデルを作成し，各因果関係の重みを意味するパス係数の解析を行う．標準化したパス係数を算出した結果を図 3 に示す．セキュリティリスク回避行動及び前面要因はそれぞれ同じ意図の複数の項目から構成されているため，潜在変数を設けている．それ以外の背景要因についてはそれぞれ異なる意図の質問であるため潜在変数を設けないモデルとした．図 3 の各パスに記載のパス係数は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%，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．この結果から知識習得要因や認知要因のうちリスク認知は，パスワード漏えいリスクの回避行動に正の影響を与えており，認知要因のうちベネフィット認知やリスク補償は負の影響を与えていることがわかる．また，背景要因の中でもこれらの認知要因や知識習得要因にそれぞれ影響を与えるものとそうでないものがあることがわかる．

次に，モデルの適合度について評価を行ったところ，CFI=0.899，GFI=0.911，RMSEA=0.056 であった．CFI 及び GFI は 1 に近いほどモデルへ適合

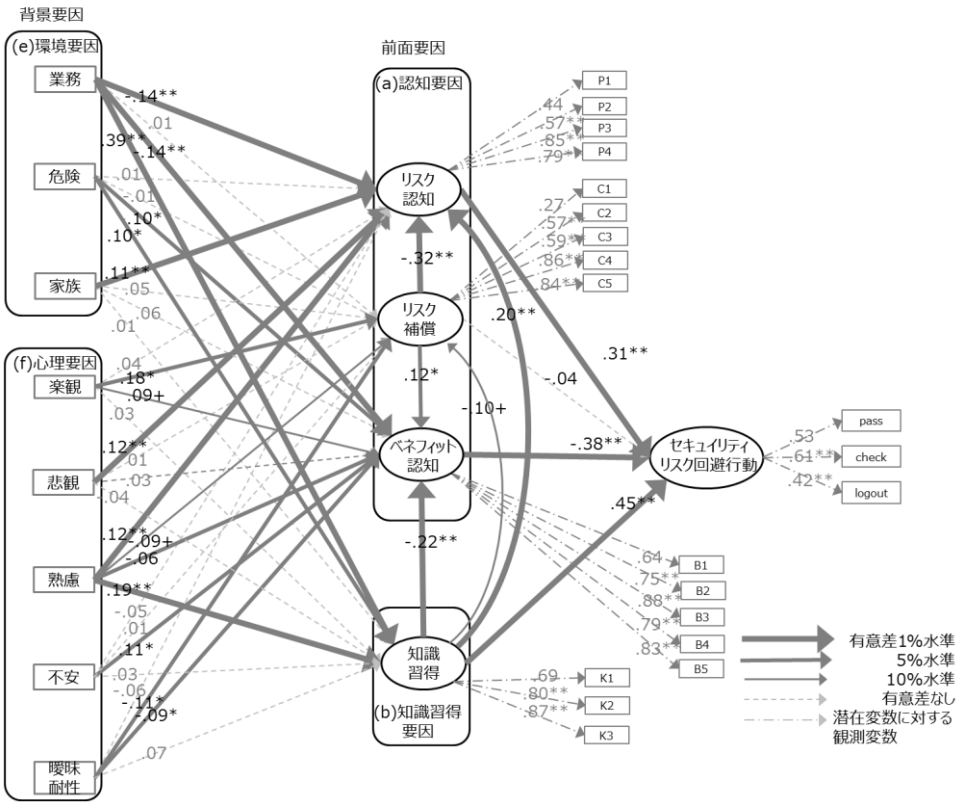

図 3 構造方程式モデリングによる提案モデルの分析

度が高いとされ，0.9 以上で良好とされる．また，RMSEA は 0 に近いほど良いとされ，0.08 未満でモデルは良好であるとみなされる．したがって今回示したモデルが妥当なモデルであることを示している．

5 考察

5.1 前面要因の妥当性

前面要因からセキュリティリスク回避行動への直接効果（前面要因からセキュリティリスク回避行動へのパス係数の値）は，ベネフィット認知とリスク補償が負，リスク認知と知識習得要因は正である．その中でもリスク補償の直接効果は-0.04 と非常に小さい値となっているが他の要因を介して生じる間接効果が存在する．間接効果はパス係数の積で表され，間接効果の和が総合効果である．リスク補償からセキュリティリスク回避行動への総合効果は，リスク認知を介した間接効果-0.32×0.31 と，ベネフィット認知を介した間接効果 0.12×(-0.38)の和-0.18 となり，直接効果と比べて負の効果が大きい．このことから，認知要因の中でもリスク補償は，リスク認知やベネフィット認知を介して影響を与える要因であることが分かった．

5.2 セキュリティリスク回避行動への効果

5.1 節より，リスク補償傾向を持つユーザはセキュリティ回避行動をとらない傾向にあることが裏付けられた．そこで他の要因に関する総合効果について，リスク認知からセキュリティリスク回避行動へのパス係数を 1 として正規化した値を表 1 に記載する．併せて表 1 には，背景要因も含めたすべてのユーザ要因からセキュリティリスク回避行動への直接パスのみを仮定したモデル（直接パスモデル）に関する総合効果を記載している．

知識習得要因，環境要因のうち業務経験，心理要因のうち熟慮性は直接パスのみを考えた場合よりもセキュリティリスク回避行動に与える正の影響は大きく，リスク認知と比べても影響は 50%以上である．このことから，セキュリティに関する知識を得ること，セキュリティに関する業務経験，よく考える傾向にあることがセキュリティリスク回避に関連していることが裏付けられた．

心理要因のうち楽観性，悲観性，不安，曖昧さ耐性に関してはリスク認知と比べて総合効果が 50 パーセント未満であった．このことから楽観性，悲観性，不安，曖昧さ耐性はリスク回避行動自体に大きな影響を及ぼす要因ではないことを確認した．

表 1 各要因の総合効果
（リスク認知を 1 として正規化）

要因		提案モデル	直接パスモデル
認知	リスク認知	1	1
	ベネフィット認知	-1.23	-1.21
	リスク補償	-0.62	-0.24
知識習得		1.99	1.20
環境	業務経験	0.81	0.31
	危険経験	0.1	0.33
	家族	0.03	-0.08
心理	楽観	-0.12	0.13
	悲観	-0.01	0.03
	熟慮	0.62	0.19
	不安	-0.14	-0.19
	曖昧耐性	0.26	-0.04
CFI		0.899	0.843
GFI		0.911	0.878
RMSEA		0.560	0.660

5.3 背景要因の前面要因への効果

心理要因のうち，楽観性がリスク補償に，悲観性がリスク認知にそれぞれ正の影響を強く与えている．また，熟慮性がリスク認知・知識習得要因に正の強い影響を与えているため，ユーザのリスク補償傾向やリスク認知・知識習得の有無を推定するために有効な要因であると言える．

環境要因のうち，業務経験はリスク認知に負の影響を与えている．業務経験がリスク認知を妨げる要因として考えられる背景にあることとして能力に対する自信（リスク補償）が考えられる．今回このような意図の質問を行わなかったため，リスク補償に質問項目を追加・改善し再調査する予定である．一方で，業務経験はベネフィット認知に対しても負の影響，知識習得要因に正の影響を与えており総合効果としては，他の背景要因と比べても影響を与えている要因であることがわかる（表 1）．そのため，業務経験のあるユーザにはリスク認知へ負の影響を出さないよう，認知を正しくするための支援が必要となる．

危険経験も同様に学習経験とベネフィット認知に正の影響を与えている．疑似的な危険や被害をユーザに提示することにより知識習得の契機となると

考えられるが，同時にベネフィット認知も生じてしまうことを意味している．そこでベネフィット認知の生じない疑似被害経験の提示が必要となる．

セキュリティ設定などをしてくれる家族がいるユーザに関しては対策を家族に委ねているため，リスク認知には負の影響を与えることを想定していた．しかし今回の結果では，リスク認知に正の影響を与えていることが分かった．これは，セキュリティ設定をしてくれる家族がセキュリティ対策を教えてくれる家族であるためと考えられる．

6 まとめ

本稿では，パスワード漏えいのようなセキュリティリスク回避行動に影響する前面要因及び背景要因に関するモデルを提案し，認知要因，知識習得要因，環境要因，心理要因についての関係性を検証し，妥当性を確認した．これにより，特定の心理，環境を持つことや，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る．今後はパスワード漏えい以外のセキュリティリスク回避行動における因果関係を検証し，セキュリティリスク間での相違性・共通性を解析する．また，今回検証できなかった状況要因や技能習得要因，操作技能要因に関する解析を進めた上で，ユーザ要因に応じ，適切なセキュリティリスク回避行動を促す仕組みや学習促進の方法について検討し，状況・技能に応じたユーザ補助のシステムの検討を行う．

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，”
http://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf

[2] 加藤，中澤，漁田，山田，山本，西垣，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 2537–2548 (Sep. 2011)

[3] トレンドマイクロ，“「Web 脅威対策」機能について，”
http://esupport.trendmicro.com/support/vb/solution/ja-jp/1313955.aspx

[4] 寺田，津田，片山，鳥居，“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，2014 年 7 月

[5] 片山，寺田，鳥居，津田，“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 年 1 月

[6] M. Zuckerman, D. Kuhlman, “Personality and Risk-Taking: Common Biosocial Factors,” Journal of Personality 68:6, December 2000.

[7] 芳賀，”不安全行動のメカニズム，”信学技報，SSS, 1999

[8] 芳賀，"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-"，信学技報 SSS2009-8

[9] 上市，楠見，“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”，心理学研究第 69 巻第 2 号

[10] 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，”
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2012/ilas2012-report-build.pdf

[11] Google Inc., Gmail - Google の無料ストレージとメール，https://www.gmail.com/

[12] Microsoft, Hotmail, https://login.live.com/

[13]ヤフー株式会社，Yahoo!メール，
https://mail.yahoo.co.jp

[14] 堀，山本，“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 (2001/07)

[15] 堀，吉田，“心理測定尺度集 II 人間と社会のつながりをとらえる＜対人関係・価値観＞，” サイエンス社 (2001/07)

[16] 村上，“心理尺度のつくり方，”北大路書房

[17] 浦上，脇田“心理学・社会科学研究のための調査系論文の読み方，“東京図書

[18] 豊田，“共分散構造分析[入門編]，”朝倉書店，1998

[19] 清水，村山，大坊，“集団コミュニケーションにおける相互依存性の分析(1) コミュニケーションデータへの階層的データ分析の適用 ，”電子情報通信学会技術研究報告，106(146), 1-6, 2006[13]

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．

付録 1　調査内容

変数名	質問意図		質問項目	配点	平均	標準偏差	もっとも割合の高い回答([%])
pass	セキュリティリスク回避行動	パスワード設定	(1)数字・文字・記号のいずれか 2 つ以上を使ったパスワード構成である、またはワンタイムパスワードを使っている (2)8 桁以上のパスワード構成である、またはワンタイムパスワードを使っている (3)サービス毎に異なるパスワードを使っている、またはほかに使っているサービスはない、またはワンタイムパスワードを使っている	(1)(2)(3)のうちいずれも「いいえ」:1 (1)(2)(3)のうちいずれか 1 つが「はい」:2 (1)(2)(3)のうちいずれか 2 つが「はい」:3 (1)(2)(3)のうちいずれも「はい」:4	2.414	0.912	2(41.3)
check		サーバ確認	ウェブメール機能のあるサイトにログインする際、(1)サイト SSL、(2)URL ドメイン、(3)組織情報のいずれかを確認している	いずれかも確認しない:1 いずれかをたまに確認する:2 いずれかをいつも確認している:3	1.650	0.773	1(53.5)
logout		ログアウト方法	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押下する	しない:1 たまにする:2 いつもする:3	1.944	0.807	1(35.5)
P1	認知要因	リスク認知	複雑なパスワードのほうが安全だと思う	全くそう思わない:1 あまりそう思わない:2 どちらともいえない:3 ややそう思う:4 とてもそう思う:5	3.970	0.908	4(42.1)
P1			定期的にパスワードを変えた方が安全だと思う		4.144	0.827	4(44.6)
P1			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		4.140	0.815	4(44)
P1			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		4.262	0.843	5(46.5)
B1		ベネフィット認知	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		3.165	1.086	3(31.9)
B1			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		3.740	0.962	4(46.5)
B1			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		3.554	1.080	4(41.1)
B1			ID・パスワードは忘れてしまうので紙に書いておきたい		3.703	1.036	4(43.3)
B1			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		3.541	1.125	4(37.2)
C1		リスク補償	絶対に人から推測されないパスワードを使っている自信がある		2.554	1.014	3(36.6)
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		2.555	0.935	3(45.4)
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		2.353	0.868	3(44.6)
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		2.639	0.902	3(49.6)
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		2.636	0.952	3(47.2)
K1	知識習得要因	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		当てはまらない 1 当てはまる 2	1.278	0.448	4(72.2)
K2		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			1.307	0.461	4(69.3)
K3		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			1.321	0.467	4(67.9)
業務	環境要因	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、または、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			1.143	0.350	1(85.7)
危険		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、または 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、または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、または 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			1.106	0.308	1(89.4)
家族		家族がいて基本的なセキュリティ設定はしてもらっている			1.260	0.439	1(74)
楽観	心理要因	楽観主義尺度_楽観的自己感情（4~20 点の間）		~8 点:1, 9~12 点:2, 13~16 点:3, 17~20 点:4	2.270	0.617	3(60.5)
悲観		楽観主義尺度_悲観的自己感情（4~20 点の間）		~8 点:1, 9~12 点:2, 13~16 点:3, 17~20 点:4	2.040	0.575	3(69.2)
熟慮		認知的熟慮性~衝動性尺度（10~40 点の間）		~20 点:1, 21~30 点:2 31~40 点:3	1.835	0.504	2(71.9)
不安		状態-特性不安尺度のうち特性不安尺度（20~80 点）		~30 点:1, 31~40 点:2, 41~50 点:3 51~60 点:4, 61~70 点:5, 71~80 点:6	3.599	1.107	3(34.5)
曖昧耐性		心理的健康と関連する曖昧さ耐性尺度（24~120 点の間）		~48 点:1, 49~72 点:2, 73~96 点:3 97~120 点:4	2.754	0.543	2(68.4)