情報処理学会論文誌 Vol.54 No.9 2197–2207 (Sep. 2013)

専門知識のないユーザを対象とした情報セキュリティ技術に関する安心感の構造

西岡 大[1,a)] 齊藤 義仰[1] 村山 優子[1]

受付日 2012年12月3日, 採録日 2013年6月14日

概要：社会全体で情報セキュリティ技術に対し安心・安全が求められている傾向にある．情報セキュリティ技術の分野では，安全な技術を提供すれば利用者は安心するという論理の下，技術の安全性を確保するための議論に主眼が置かれており，安心感の構造について十分な議論がされていない．我々は，ユーザ調査において知識のないユーザの意見を反映した質問紙を作成し，因子分析と多変量分散分析から，情報セキュリティ技術に関する知識のないユーザが求める安心感の要因の抽出とユーザの属性と安心感の要因との関係性を明らかにしてきた．因子分析の結果，「善意の認知」，「能力や誠実さの認知」，「ユーザの心象」，「第 3 者の企業に対する評判情報の認知」の 4 種類の安心感の要因を抽出した．また，分散分析から情報セキュリティ技術に関する知識のないユーザ特有の安心感の要因について分析を行った．分析の結果，「ユーザの心象」と「第 3 者の企業に対する評判情報の認知」は情報セキュリティ技術に関する知識のないユーザ特有の安心感の要因であることが判明した．本論文では，これまでの知見をもとに安心感の構造について考察を行い，考察した安心感の構造の妥当性を検証した内容について報告する．

キーワード：安心，トラスト，因子分析，共分散構造分析

A structure of Anshin with information security from users without technical knowledge

Dai Nishioka[1,a)] Yoshia Saito[1] Yuko Murayama[1]

Received: December 3, 2012, Accepted: June 14, 2013

Abstract: Society as a whole has a tendency to seek security and Anshin in the information security. Conventional researches have been based on the assumption that users would feel Anshin when provided with secure systems. Therefore, the structure of Anshin has not been discussed. We have conducted a few user surveys about Anshin and have identified latent factors from users without technical knowledge. In this survey, we created a questionnaire the questionnaire to reflect the feedback from the users without technical knowledge about information security and analyzed with factor analysis and multivariate analysis of variance. As a result of factor analysis based on the result of the user survey, we extracted “Perceived benevolence”, “Perceived competence and integrity”, “user impression” and “Perceived reputation of the company provided by a third party”. Furthermore, as results of multivariate analysis of variance and compared with preliminary survey, we found that “user impression” and “Perceived reputation of the company provided by a third party” were Anshin factor from the users without technical knowledge on information security. In this paper, we report a structure of Anshin which is created based on our findings.

Keywords: Anshin, trust, factor analysis, structual equation modeling

1. はじめに

近年，テロ等の国際的な犯罪，鳥インフルエンザ等の感染症，東日本大震災等の大規模自然災害，無差別殺人等の

[1] 岩手県立大学ソフトウェア情報学部
Faculty of Software and Information Science, Iwate Prefectural University, Iwate 020–0193, Japan
[a)] d.nishioka@comm.soft.iwatepu.ac.jp

凶悪犯罪，食品偽装等の食品に関わる問題といった，国民の安全・安心の確保に対する課題が数多く存在しているため，日本では「安全」と「安心」に関する議論が活発に行われている [1]．情報セキュリティの分野でも，相次ぐ情報漏洩事件やフィッシング詐欺等の危険やリスクが増加しているため，「安全」で「安心」な情報セキュリティの実現について議論が行われている [2]．この議論では「安全」と「安心」は併記され，安全な技術を提供すれば利用者は安心するという論理の下で研究が進められてきた．しかし，我が国では海外に比べ情報通信の利用に安心と感じる国民が少なく [3]，「安全」でも「安心」が得られない状態である．

以上の背景から，客観的な指標で示すことが可能な安全だけでなく，ユーザの感情である安心感について要因の解明や構造を明確にすることは重要な研究課題である．

我々は，情報セキュリティ技術の，技術的な側面の「安全」ではなく，ユーザの主観的な側面の「安心」に着目し，情報セキュリティ技術を利用するユーザの情報セキュリティ技術に対する安心感を調査してきた [4], [5], [6], [7]．

先行研究 [4], [5] で利用した質問紙は，情報セキュリティ技術に関する知識を持つユーザの意見をもとに質問紙を作成している．しかし，セキュリティを利用する多くのユーザは情報セキュリティ技術に関する知識がない．そのため，知識のないユーザから，オンラインショッピング時における情報セキュリティ技術に関する意見を収集し，最終的に 34 問からなる質問紙を作成した [6]．

また，作成した質問紙を用いて，1,030 名を対象に Web 調査を行い，因子分析から，「善意の認知」，「能力や誠実さの認知」，「ユーザの心象」，「第 3 者の企業に対する評判情報の認知」の 4 種類の安心感の要因を抽出し，多変量分散分析から，「ユーザの心象」，「第 3 者の企業に対する評判情報の認知」の 2 種類の要因が情報セキュリティ技術に関する知識のないユーザ特有の安心感の要因であることを明らかにした [7]．

本論文では，これまでの知見をもとに安心感の構造について考察を行い，考察した安心感の構造の妥当性を検証した内容について報告する．次章で安心やトラストの関連研究について報告する．3 章では情報セキュリティ技術に対する安心感の要因を抽出した内容について報告する．4 章では，3 章で抽出した安心感の要因をもとに安心モデルを作成し，情報セキュリティ技術に関する安心感の構造を明らかにした内容について報告し，5 章で考察を行い，6 章でまとめを述べる．

2. 関連研究

欧米における，安心の類似概念はトラストであり，心理学や社会学の分野で研究が行われている．また，トラストは日本語で信頼と訳されることが多い．しかし，トラストおよび信頼の定義は定まっておらず，様々な研究で定義が異なる．

山岸 [8] は，「安全」と「安心」の間に「信頼（トラスト）」を考慮する必要があると考え，信頼（トラスト）を，「社会的不確実性が存在しているにもかかわらず，相手が自分に対してひどい行動はとらないだろうと考えること」，安心を「そもそもそのような社会的不確実性が存在していないと感じること」としてとらえている．村上 [9] は，危険に対して客観的数値で表せるものを安全とし，ユーザの危険に対して主観的判断を安心としている．安全は定量的に評価が可能であることに対して，安心は心理的，主観的な側面が強く評価することは難しいとしている．しかし，安心と安全の定義が異なっているにもかかわらず，一般的に安全と安心について区別せず一緒に用いられていることが多い．

トラストは，トラストを構築する段階（trust building），トラストを安定させる段階（stabilising trust，and dissolution），終了する段階の 3 つの段階が存在するとされている [10]．トラストのモデルや定義として，Marsh [11] は，−1 から 1 の範囲で定量化できるトラスト計算モデルの作成した．Xiao ら [12] は e-commerce の分野においてユーザが認知することで生じるトラストとユーザの感情から生じるトラストが存在するとしている．また，Gambetta [13] は，トラストの定義を，あるユーザが他のユーザもしくはグループが自分に対し好意的かどうかの主観確率のレベルとしている．トラストにも心理的，主観的側面を持つ概念が存在しており，Lewis [14] は，トラストに関する感情的側面が重要であるとし，トラストは非合理的なものであると位置づけている．

また，Solomon ら [15] は，トラストする対象者によって，トラストする範囲が限定されるとしている．Riegelsberger ら [16] や Falcone ら [17] はトラストモデルにおいて，トラストの行動を起こす前に，相手をトラストするか判断する状態が重要だと述べている．トラストを確立するためには，トラストされる者やサービスに関する十分な情報を得て知識を貯める必要があるとされている [18]．ユーザがサービス事業者をトラストするための手法として，ユーザ自身の経験を蓄積していく手法と，サービスを利用する前に，ユーザが相手をトラスト可能かどうか Trusted third party に尋ねる [19] 手法が存在する．

トラストは，様々な条件で変化するとされている．Greenspan ら [20] は，対話時，メディアの違いによるトラストの影響について，即時対応を行うことが可能なメディアを利用することが，相手をトラストするのに効果的であると報告している．Robert ら [21] は，一般的にメディア利用した場合，対面での会話よりトラストを減少させるとされているが，メディアの影響ではなく，メディア利用時のユーザの行動がトラストを減少させると報告している．Robert はトラストを減少させる原因として，関連研究調査

から，「人はオンライン上では情報を誇張して他者に伝達する傾向を持っている [22]」，「メディアは対面での会話の動作を誇張して表現する傾向がある [23]」，「実世界での振舞いより抑制はされておらず感情的になりやすい傾向がある [24]」，「人はオンライン上では性別等を偽ることがあり情報を偽造する傾向がある [25]」の 4 種類の原因が存在するとしている．

情報セキュリティ技術において，個人情報を保護するための研究が様々行われてきた．しかし，セキュリティ対策について，一般人には難しく，無関心であり [26]，避ける傾向にある [27] とされ，セキュリティ対策におけるユーザビリティを向上させる研究が数多く行われている．

Andrew ら [28] は，ソーシャルメディアを利用しているユーザが，誤って他者には知られたくない個人情報を記載してしまう問題に対して，ソーシャルメディア上に提供できる情報を制限するシステムを構築した．Min ら [29] は，オンラインサービスにおいて，ID とパスワードを求められた際，そのサイトが，フィッシングサイトかどうか判断し，適切なサイトへのリンクを提示するシステムを構築した．Ka-ping ら [30] は，1 つのパスワードで，利用しているすべてのオンラインサービスごとに変換可能なシステムを構築した．

これらの内容から，安心感の定義は，心理的，主観的概念であることが示された．また近年，情報セキュリティの分野において，技術的側面だけでなく，人間的側面に関して研究を進めることが重要視されている．情報セキュリティ技術における研究の代表例として，ソーシャルエンジニアリング [31] がある．ソーシャルエンジニアリングとは，社会の仕組みや人間の行動的・心理的側面を利用し，情報取得や改ざん等攻撃を手法である．しかし，ユーザが求める安心の要因や特徴について，分かっていないことは多い．したがって，安心感の要因や特徴を検討することは重要な研究課題であるといえる．

3. 情報セキュリティ技術に対する一般ユーザの安心感の要因

前章の既存研究の知見から，安心感や安心感の類似研究であるトラストは，様々な定義，要因の整理，要因に影響を及ぼす概念の整理，モデルの構築が行われていることが判明した．しかし，既存研究では，全体像について示されているが，各要因におけるユーザの属性について違いは十分な議論が行われていない．そこで，本章では，これまで実施してきた調査において，ユーザが求める安心感の要因を明らかにし，各要因に対して影響を及ぼすユーザの属性について分析した内容について報告する．まず，3.1 節で，調査で利用した質問紙について報告し，3.2 節で実施したユーザ調査の概要について報告する．次に，3.3 節で，ユーザ調査の結果をもとに，因子分析を用いて，安心感の要因の抽出を内容について報告し，最後に，ユーザの属性と抽出した安心感の要因との関係について，3.4 節で，ユーザの知識レベルが影響を及ぼす安心感の要因，3.5 節で，ユーザの経験レベルが影響を及ぼす安心感の要因について報告する．

3.1 質問紙の作成

先行研究 [4] では，情報セキュリティに関する知識のあるユーザからの意見を反映した質問紙を作成し，大学生 425 名を対象とした情報セキュリティ技術に関する安心についての質問紙調査を行い，因子分析を用いて情報セキュリティ技術に関する安心の要因の抽出を行った．分析の結果，セキュリティ技術，ユーザビリティ，経験，プリファランス，知識，信用の 6 種類の要因を抽出し，さらにこれらの要因が外的要因と内的要因の 2 種類のグループに大別されることを示した．

先行研究 [4] における，情報セキュリティに関する知識の定義は，情報セキュリティ技術に関して，専門教育を受けているユーザを知識があるユーザ，受けていないユーザを知識がないユーザとしている．この調査対象者は情報セキュリティの知識があるユーザが約 70%（425 人中 307 人）であったため，情報セキュリティの知識がないユーザの感じる安心要因を抽出するには至らなかった．

その後の研究 [5] では，問題を解決するために，被験者を情報セキュリティの知識がないユーザに変更し，765 名の知識がないユーザを対象に質問紙調査を行い，因子分析を用いて安心の要因の抽出を行った．先行研究 [5] における情報セキュリティに関する知識の定義は，先行研究 [4] の定義と同じである．調査の結果，認知的トラスト，親切さ，理解，プレファランス，親しみの 5 種類の要因を抽出した．

当該調査では，先行研究 [4] で使用した質問紙を改善し調査を実施している．先行研究 [4] では，「インターネットでの情報検索や，何かのサービスやシステムを利用するにあたり，個人情報を入力するような場面」を被験者に想像してもらい質問紙調査を実施した．先行研究 [5] において，予備調査の段階で，先行研究 [4] の調査で利用した質問紙を用いて質問紙調査を実施したが，被験者から，具体事例が想像しにくいとの意見が出たため，前提条件を「インターネット上のショッピングやチケット予約，オークション等のサービス利用時に，クレジットカードを番号を入力する場面」に改善している．また，質問項目も，前提条件に合わせ，「ショッピング等のサービス」や「ショッピング等のサービスを運営している企業」という文章を各質問項目に導入した．

情報セキュリティを利用するユーザの多くは，情報セキュリティに関する知識がない．しかし，これらの調査で用いた質問紙は，情報セキュリティに関する知識のないユーザからの意見を反映していないため，これらのユーザ

の安心感の要因が抽出できない可能性がある．そこで，先行研究 [6] では，情報セキュリティ技術に関する知識のないユーザの意見を質問紙に反映させる手法を提案し，情報セキュリティ技術に関する知識のないユーザのオンラインショッピング時における安心感についての意見を反映させた質問紙の作成を行い，34 問で構成される質問紙を作成した．

先行研究 [6] における情報セキュリティに関する知識の定義も，先行研究 [4], [5] の定義と同じである．質問紙作成時において，先行研究 [5] と同様の前提条件で内容を被験者が想像した場合，被験者は複数の場面を想定し，各被験者で場面の想定が異なるとが予測されるため，条件を一定にするために，前提条件を「オンラインショッピング時，クレジットカードを番号を入力する場面」とし，上記の前提条件の場面での意見を求め，質問紙を作成した．

3.2 ユーザ調査

先行研究 [7] では，先行研究 [6] で作成した専門知識のないユーザの意見を反映させた 34 項目からなる質問紙を用いて Web 調査を実施した．この調査の被験者は，情報セキュリティ技術に関する知識がないユーザを対象としているが，先行研究 [7] における情報セキュリティに関する知識の定義は，先行研究 [4], [5], [6] の定義と異なる．

調査では，安心感の要因に対する知識レベルの影響を調査ことも念頭においていたため，回答者の知識レベルを得点化できるようにユーザの情報セキュリティ技術に関する知識について複数の質問を行い，回答結果から，ユーザの知識レベルの得点化を行った．

知識に関する質問では，独立行政法人情報処理推進機構（IPA）[32] と野村総合研究所（NRI）[33] が行った調査で利用された，脅威に関して，70%以上のユーザが説明できる項目を 2 問（「ワンクリック不正請求の流れ」と「フィッシング詐欺の仕組み」），10%未満のユーザしか説明できない項目を 2 問（「ボットネットの仕組み」，「マルウェアの定義」），対策に関して，70%以上のユーザがセキュリティ対策を行っている項目を 2 問（「不信な電子メールの添付ファイルは開けないようにしている」，「怪しげなサイトへアクセスしないようにしている」），10%未満のユーザしかセキュリティ対策を行っていない項目を 2 問（「無線 LAN の暗号化を行っている」，「重要なファイルを暗号化している」）を選択し利用した．ユーザの知識レベルの得点化については，各設問において説明できる，または対策を行っていると回答した項目を 1 点，説明できない，または対策を行っていないと回答した項目を 0 点とし，その合計をユーザの知識レベルとした．合計得点が 8 点のユーザに関しては，情報セキュリティ技術に関する知識のあるユーザとして扱うことにした．

調査は，2011 年 2 月 22 日（火）〜24 日（木）に行った．調査は，調査会社に依頼した．Web 調査の結果，1,030 名からの回答を得た．被験者の知識の得点化の結果，得点が 8 点である回答者は 30 名存在した．そのため，30 名を情報セキュリティ技術に関する知識のあるユーザとして分析から除外した．また，全質問項目に対し同じ回答をしているユーザ 110 名，回答に矛盾のあるユーザ 2 名を削除し，最終的に 888 名で分析を実施した．

3.3 知識のないユーザの安心感の要因

前述の調査結果を用いて因子分析を実施し，情報セキュリティ技術に関する安心感の要因を抽出した．Web 調査から天井効果，床効果，尖度，歪度の値を確認した結果，天井効果がある項目は存在しなかったが，床効果がある項目が 3 つ存在した．また，尖度や歪度の値に問題がある項目は存在しなかった．そのため，3 項目を除いた，31 項目に対する回答を因子分析の対象とし分析を実施した．

分析には，統計解析ソフトウェア，PASW Statistics 18 を利用し，因子の抽出には最尤法を用いた．本調査では，共通性が 0.20 以下の項目を削除し分析を行った．分析した結果，3 項目の共通性の値が 0.20 以下のため，2 項目を削除し 29 項目を用いて再度分析を行った．その結果，初期解における固有値の減衰状況から 4 因子解とした．

各因子について，α 係数を算出したところ，第 1 因子の 14 項目で $\alpha = 0.908$，第 2 因子の 6 項目で $\alpha = 0.899$，第 3 因子の 5 項目で $\alpha = 0.668$，第 4 因子の 4 項目で $\alpha = 0.781$ が得られた．29 項目の全分散を説明する割合である累積寄与率は 58.292%であった．抽出された因子は「善意の認知」，「能力や誠実さの認知」，「ユーザの心象」，「第 3 者の企業に対する評判情報の認知」と名付けた．それぞれの特徴を以下に記す．

「善意の認知」

第 1 因子は，「あなたの操作や手続きのミスに対して解決を助けてくれる方法が用意されている」や「尋ねたいことがあり質問フォームから尋ねると，定型文のみの自動返信ではなく尋ねた内容について記載されている返信が早い」等の 14 項目で構成される．第 1 因子は，企業が客観的なトラストの要因である「善意」を持っているかどうか，ユーザ自身が主観的に判断することを示した因子である．

認知的トラストとは，相手をトラストする為の客観的な判断基準とされ，トラストされる者の能力（Competence），誠実さ（Integrity），善意（Benevolence）の 3 要因から構成される [34]．善意は，「善良な心，他人のためを思う心，他人の行為を好意的に見ようとする心」と定義されている．ユーザ自身のミスから発生したトラブルやユーザ自身が疑問に感じる内容に対して，サービスを提供している企業がユーザの為に，善意のもと対応していると，ユーザが感じると安心することを示している．認知的トラストでは，善意は客観的な項目として扱われているが，先行研究 [35] で

は，トラストにおける感情部分が安心であるとしている．このことから，第1因子を企業が「客観的な情報である善意」を持っているかどうか，ユーザが主観的に認知することを示す「善意の認知」と名付けた．

「能力や誠実さの認識」

第2因子は，「サービスを提供する会社は個人情報を漏洩させないと感じる」や「サービスを提供する会社は個人情報管理対策を適切に実施していると感じる」等の6項目で構成される．

第2因子は，企業が客観的なトラストの要因である「能力と誠実さ」を持っているかどうか，ユーザ自身が主観的に判断することを示した因子である．能力は「仕事を遂行するために必要な能力を有していること」，誠実さは「他人や仕事に対してまじめに責任を果たしていくこと」と定義されている．企業が管理している個人情報に対して，漏えいさせない能力を所持し，個人情報管理を誠実に行っていると，ユーザが感じると安心することを示している．

能力や誠実さは善意と同様に客観的な項目として扱われているが，トラストにおける感情部分が安心であるため，第2因子を企業が「客観的な情報である能力と誠実さ」を持っているかどうか，ユーザが主観的に認知することを示す「能力と誠実さの認知」と名付けた．

「ユーザの心象」

第3因子は，「具体的な根拠があるわけではないが全体的に安心な気がする」や「似たようなサービスを利用した経験からシステムが問題ないと感じる」等の5項目で構成される．この因子は，ユーザ自身の直感や経験をもとに安心するかどうかユーザが判断する因子である．これらの項目は，第1因子と第2因子とは異なり，サービスを提供している企業からの情報を利用せず，ユーザ自身の心象から安心するかどうか判断している．そのため，第3因子を「ユーザの心象」と名付けた．

「第3者の企業に対する評判情報の認知」

第4因子は，「サービスを提供する会社はTVや新聞などで紹介されている」や「サービスを提供する会社はTVや新聞などで紹介されている有名な商品を扱っている」等の4項目で構成される．この因子は，新聞やTVのように第3者から提供される情報をもとに安心するかどうかユーザが判断する因子である．これらの項目は第1因子と第2因子とは異なり，サービスを提供する企業からの情報ではなく，第3者という別の情報源からの情報をもとに安心するかどうか判断している．そのため，第4因子を「第3者の企業に対する評判情報の認知」と名付けた．

3.4 知識差における安心感の要因への影響

先行研究 [7] では，ユーザの知識が安心感の要因に影響を及ぼす因子を抽出している．

この調査では，知識の差について，ユーザが脅威を説明できる項目を2問，ユーザが脅威を説明できない項目を2問，セキュリティ対策を行っている項目を2問，セキュリティ対策を行っていない項目を2問尋ねた．各設問において説明できる，対策を行っていると回答した項目を1点，説明できない，対策を行っていないと回答した項目を0点とし，その合計を求めた．8点のユーザに関しては，情報セキュリティ技術に関する知識のあるユーザとして，分析対象から除いた．また，合計得点が0〜2点のユーザを，知識レベルが下位のユーザ群，3，4点のユーザを知識レベルが中位のユーザ群，5〜7点のユーザを知識レベルが上位のユーザ群とし，3種類に分類し分析した．

情報セキュリティ技術の知識の差から各因子に有意な差が認められるか否かについて検証するために，因子得点を従属変数，知識の差を独立変数とした多変量分散分析を行った．分析の結果，第3因子「ユーザの心象」では，知識が下位群のユーザと上位群のユーザとの間では5%水準で有意差が認められ，中位群のユーザと上位群のユーザの間では1%水準で有意差が認められた．第4因子「第3者の企業に対する評判情報の認知」では，知識が下位群のユーザと中位群のユーザとの間では5%水準で有意差が認められ，下位群のユーザと上位群のユーザとの間では0.1%水準で有意差が認められ，中位群のユーザと上位群のユーザとの間では1%水準で有意差が認められた．

以上の結果から，知識レベルが低いユーザほど第3因子と第4因子を重視する傾向にあることが明らかになった．

3.5 経験差における安心感の要因への影響

欧米の安心感の類似表現であるトラストは，ユーザの経験がトラストに影響する [36] と示されている．安心感は，トラストの感情部分である [35] ため，トラストと同様に，ユーザの経験が安心感の要因に影響を及ぼす可能性がある．

ユーザの経験差と安心感の要因との関係は，3.4項で実施した調査と同様に多変量分散分析を用いて分析した．本調査では，ユーザの経験として，年間のオンラインショッピングの利用経験ついて尋ねている．ユーザの経験レベルの差を，年間のオンラインショッピングの利用回数が0〜5回までを，経験レベルが下位のユーザ群，6〜19回までを，経験レベルが中位のユーザ群，20回以上を，経験レベルが上位のユーザ群とし，3種類に分類し分析した．

分析の結果，分析の結果，多変量主効果は知識の差において1%水準で有意な差が認められた．経験の差において，第4因子に1%水準で有意差が認められた．以上の結果，経験レベルが低いユーザほど第4因子を重視する傾向があることが明らかになった．

3.6 知識のないユーザの安心感の特徴

先行研究 [4], [5] と先行研究 [7] の安心感の要因を比較したところ，先行研究 [4], [5] にはない「第3者の企業に対

する評判情報の認知」が先行研究 [7] で抽出されたことと，先行研究 [4] の「知識」と，「知識」と同様の内容の因子である先行研究 [5] の「理解因子」が，先行研究 [7] では抽出されていないことが判明した．トラストの研究では，評判情報がトラストに関係する一要因 [37] として研究が進められている．そのため，「第 3 者の企業に対する評判情報の認知」は，ユーザの安心感においても重要な要因であると考えられる．

先行研究 [5] では，セキュリティ技術や対策について詳しいユーザほど「理解因子」を重視すると述べている．先行研究 [4] の被験者は，情報セキュリティ技術に関する知識があるユーザであり，また，先行研究 [5] の被験者は，情報セキュリティ技術に関する専門的な知識がないものの，日常的に情報機器を利用しているユーザであったため，「知識」や「理解因子」が抽出されたと考えられる．

また，前述の比較結果と知識レベルが低いユーザほど，先行研究 [7] における第 3 因子「ユーザの心象」，第 4 因子「第 3 者の企業に対する評判情報の認知」を重視する傾向から，「ユーザの心象」，「第 3 者の企業に対する評判情報の認知」は，情報セキュリティ技術に関する知識がないユーザ特有の要因であること考えられる．被験者の属性について，経験に関しての分析も実施したところ，経験レベルが低いユーザほど，「第 3 者の企業に対する評判情報の認知」を重視する傾向もあることから，知識や経験以外のユーザの属性が一般ユーザの安心感に影響を及ぼす可能性があると考えられるため，年齢や性別等の他の属性の影響についても調査する必要がある．

4. 情報セキュリティ技術に関する一般ユーザの安心感の構造

前章では，オンラインショッピングを利用する際，一般ユーザの情報セキュリティ技術に関する安心感の要因は，4 種類存在し，外的要因と内的要因に分類する可能性を示した．また，ユーザの知識と経験レベルと安心感の要因との関係について分析し，知識レベルは，第 3，第 4 因子に影響を及ぼし，経験レベルは第 4 因子に影響を及ぼすことが判明した．

本章では，安心感の構造を明確にするため，今まで得られた知見をもとに，オンラインショッピング時における一般ユーザの情報セキュリティ技術に関する安心感の構造について検討した内容について報告する．

4.1 安心感の要因の妥当性の検証

3.3 節で行った因子分析は，明確な仮説を持たずに，観測変数に影響を及ぼす因子を探索的に求める探索的因子分析である．そのため，抽出した 4 因子の妥当性の検証を行うため，4 因子すべてを用いて検証的因子分析を実施した．検証的因子分析とは，探索的因子分析の結果を検証することを目的とした手法である．検証的因子分析では，共分散構造分析を用い抽出した因子の妥当性を検証する．

共分散構造分析とは，因果モデルを設定し，その仮説の妥当性を検討するための統計的手法であり，モデルがどの程度受容できるか適合度指標から判断する．共分散構造分析を用いた調査の実例として，山崎らは [38]，新型インフルエンザを含めた鳥インフルエンザへの不安構造として「感染とその影響への不安」，「対応への不安（ヒト感染前）」，「対応への不安（ヒト感染後）」の 3 種類のモデルを作成し，共分散構造分析を用いて各モデルの妥当性を示している．

共分散構造分析に用いられる適合度指標は，GFI，CFI，RMSEA，AIC 等がある．GFI（Goodness-of-Fit Index）は 0〜1 までの値をとり，1 のときモデルが完全に適合していることを意味する．一般に 0.9 以上であればモデルを受容できる．CFI（Comparative Fit Index）値も同様に，1 に近いほどモデルの当てはまりが良いとされ，0.9 以上であればモデルを受容できる．RMSEA（Root Mean Square Error of Approximation）値は 0 に近いほどモデルの適合度が高く，0.1 以上であればモデルが受容できない．受容の判定基準は 0.08 以下とされている．AIC（Akaike Information Criterion）の値が小さいほど当てはまりの良いモデルと判断する．AIC 値は，複数のモデルを比較する際の相対的基準として用いられる．

本調査の検証的因子分析モデルには，探索的因子分析で得られた 4 因子のそれぞれに高く負荷する上位 3 変数を観測変数とし，4 因子間すべてに共分散を仮定した．作成した検証的因子分析モデルを**図 1** に示す．

図中において，「善意の認知」を「善意」，「能力や誠実さ

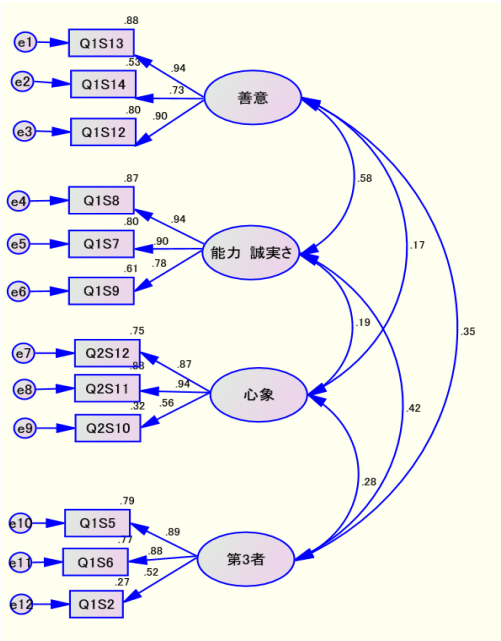

図 1 検証的因子分析モデル
Fig. 1 Result of confirmatory factor analysis.

の認知」を「能力　誠実さ」,「ユーザの心象」を「心象」,「第 3 者の企業に対する評判情報の認知」を「第 3 者」と表記している．また,「Q1S13」や「Q1S14」は質問項目を意味する．Web 調査では，質問項目 1 から 20 までを 1 ページ目，質問項目 21 から 34 までを 2 ページ目に提示している．そのため，質問項目 1 から 20 を Q1S1–Q1S20，質問項目 21 から 34 を Q2S1–Q2S14 と表記している．

分析の結果，GFI = 0.965，CFI = 0.978，RMSEA = 0.057，AIC = 247.441 となり，全体的に良好であり，探索的因子分析で得た 4 因子の妥当性を示した．

各因子の共分散を調べたところ,「善意」と「能力　誠実さ」で 0.58,「善意」と「心象」で 0.17,「善意」と「第 3 者」で 0.35,「能力　誠実さ」と「心象」で 0.19,「能力誠実」と「第 3 者」で 0.42,「心象」と「第 3 者」で 0.28 であった．この結果から,「善意」と「能力　誠実さ」,第 4 因子において中程度の相関があり,「心象」は他の因子から独立している因子であるといえる．

先行研究 [4] では，安心感の要因を大別し 2 種類の要因に分類した．情報システムやサービスを提供する側，情報システムやサービスそのものの環境に依存する要因を外的要因，情報システム等の環境的な要因に依存することなく，個人の主観的な判断基準や個人の経験や知識に依存する要因を内的要因としている．

本調査の結果においても,「善意」と「能力　誠実さ」は，オンラインショッピングを提供する企業からの情報をもとに安心する要因,「第 3 者」は，サービス提供者以外の第 3 者から提供された情報をもとに安心する要因であり，先行研究の外的要因と類似する．また,「心象」は，ユーザ自身の主観的な判断基準に基づく因子であるため，先行研究における内的要因に類似する．

4.2　外的要因と内的要因の妥当性の検証

先行研究 [4] では，安心感の要因を外的要因と内的要因に分類した．本調査の結果においても 4.1 節で示したとおり，外的要因に該当する因子は,「善意の認知」と「能力と誠実さの認知」,「第 3 者の企業に対する評判情報の認知」の因子であり，内的要因に該当する因子は,「ユーザの心象」の因子である．また,「善意の認知」と「能力と誠実さの認知」は企業からの情報をもとにユーザが安心する要因,「第 3 者の企業に対する評判情報の認知」は，サービス提供者以外の第 3 者から提供された情報をもとにユーザが安心する要因であるため，外的要因において異なる属性を持つといえる．そこで，本調査で得られた結果を外的要因と内的要因に分類，さらに，外的要因を「企業」と「第 3 者」に分類したモデルを作成し，共分散構造分析を用いて妥当性の検証を行う．

分析では，4 因子のそれぞれに高く負荷する上位 3 変数を観測変数とし分析した．作成した外的要因と内的要因の概念を加えた安心モデルを図 **2** に示す．

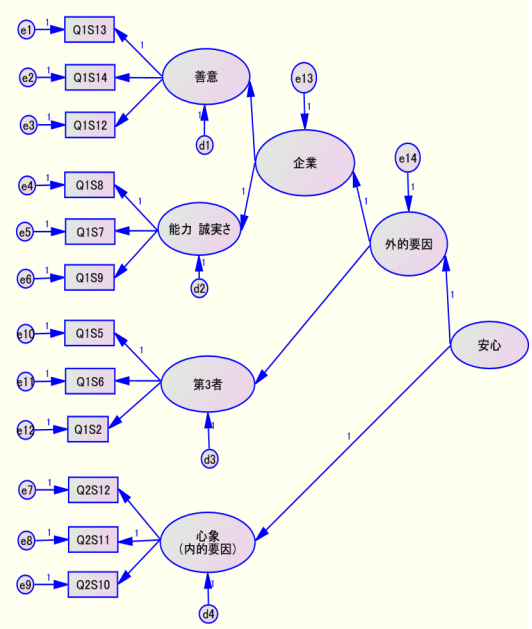

図 **2**　外的要因と内的要因の妥当性検証モデル

Fig. 2　Result of confirmatory factor analysis including environmental part and personal part.

分析の結果，GFI = 0.965，CFI = 0.979，RMSEA = 0.056，AIC = 245.473 となり，全体的に良好であり，知識のないユーザの安心感においても，外的要因と内的要因の概念が存在することを示した．

4.3　安心感の構造

4.1 節では，知識のないユーザのオンラインショッピング時における一般ユーザの情報セキュリティ技術に関する 4 種類の安心感の要因は，外的要因，内的要因に分類され，外的要因は企業と第 3 者の 2 種類の対象者から提供される情報をもとに安心感が生じることが判明した．そこで，4.1 節で作成したモデルを基準とし，3.5 節と 3.6 節で示した．知識レベルと経験の差の安心感の要因への影響に関する知見を導入した安心感のモデルを作成する．

ユーザの知識は，分散分析の結果から，第 3 因子と第 4 因子に影響を及ぼすことが判明している．そのため，ユーザの知識を第 3 因子と第 4 因子に影響を与えるように示した．また，ユーザの経験は，第 4 因子に影響を及ぼすことが判明している．そのため，ユーザの経験を第 4 因子に影響を与えるように示した．また，モデルの作成にあたって，4.1 節の安心モデルでは，4 因子のそれぞれに高く負荷する上位 3 変数のみを観測変数として分析したが，より詳細なモデルを作成するために，因子負荷量の値が 0.7 以上の項目を観測変数として共分散構造分析を行う．図 **3** に，作成したオンラインショッピング時における一般ユーザの情報セキュリティ技術に関する安心感モデルを示す．

分析の結果，GFI が 0.839，CFI が 0.870，RMSEA が

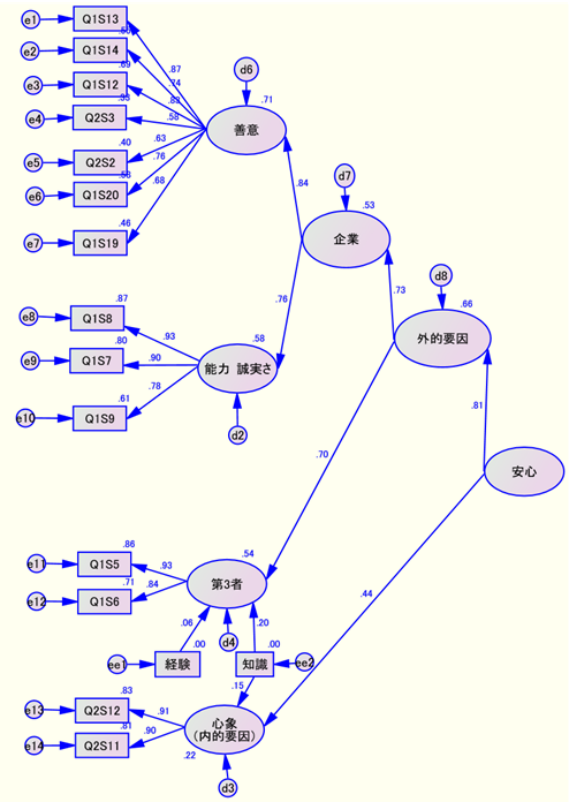

図 3 オンラインショッピング時における一般ユーザの情報セキュリティ技術に関する安心感モデル

Fig. 3 Anshin model about information security for users without technical knowledge in online shopping.

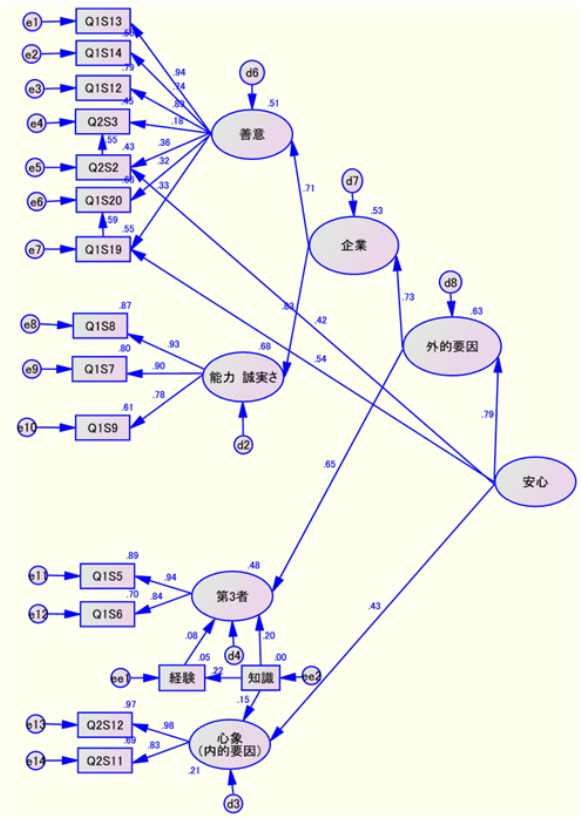

図 4 修正した安心モデル

Fig. 4 Improved Anshin model.

0.112，AIC が 1260.310 となり，適合度指標はいずれも基準値を満たさなかった．そのため，作成したモデルに問題があることが判明した．そこで，修正指数を利用してモデルの修正を加えた．修正指数をもとに修正したモデルを図 4 に示す．

修正指数をもとにモデルを修正したところ，5 つのパスが新たに追加されることが判明した．モデルを修正した結果，GFI が 0.958，CFI が 0.972，RMSEA が 0.053，AIC が 409.347 となり，適合度指標はいずれも基準値を満たすことが判明した．

追加したパスの関係性について考察すると「システムの操作性」,「企業のユーザへの対応方法」,「知識と経験との関係」の 3 つの関係が示された．

「システムの操作性」は「質問項目 19：サービスで利用されているシステムの操作がしやすい」と「質問項目 20：サービスで利用されているシステムの操作方法に関する質問に対して親切な対応が受けられる」で成り立っている．

「企業のユーザへの対応方法」と「質問項目 22：尋ねたいことがあり質問フォームから尋ねると，定型文のみの自動返信ではなく尋ねた内容について記載されている返信が早い」「質問項目 23：コールセンターに問い合わせると自動音声オペレータではなく対話可能なオペレータの対応がある」で成り立っている．

「知識と経験との関係」は「ユーザの情報セキュリティ技術に関する知識」と「オンラインショッピング利用経験」で成り立っている．

「システムの操作性」と「企業のユーザへの対応方法」は，Nielsen [39] が提唱している，5 つのユーザビリティ特性に合致すると考えられる．Nielsen の定義では，学習しやすさ（Learnability），効率性（Efficiency），記憶しやすさ（Memorability），間違えにくさ（Errors），主観的満足度（Satisfaction）があげられている．学習しやすさは，すぐ，簡単にシステムを使用することができるかどうかの基準である．効率性は，効率良くシステムを利用できるかの基準である．記憶しやすさは，期間をあけ，再度システムを利用した際に，負担なく操作を行えるかどうかの基準である．間違えにくさは，ユーザの操作間違えにくさや，間違えが発生した際，ユーザが間違えの内容について理解しやすいかの基準である．主観的満足度は，ユーザのシステムに対する主観的な満足度の基準である．

新しい関係が示された，質問項目において，「Q1S19」は，操作のしやすさの観点から学習しやすさに合致するといえる．「Q1S20」は，親切な対応を求める観点から主観的満足度に合致するといえる．「Q2S2」は対応の速さや自動返信ではない対応の観点から効率性や主観的満足度に合致するといえる．「Q2S3」は，対話を求める観点から主観的満足度に合致するといえる．これらのことから，「システムの

操作性」と「企業のユーザへの対応方法」について情報システムのみのではなく，オンラインショッピング全体に対するユーザビリティが，ユーザを安心させる新たな要因ではないかと考えられる．

5. 考察

4 章では，安心感の構造を明確にするため，知識と経験と安心感の関係を導入した，オンラインショッピング時における一般ユーザの情報セキュリティ技術に関する安心感のモデルを作成した．作成したモデルの妥当性を検証した結果，因子分析により抽出した 4 種類の因子とは別に，オンラインショッピングに対する安心感の要因としてユーザビリティ因子が存在する可能性が示された．そこで，本章では，ユーザビリティ因子が存在すると仮定した場合の安心モデルについての考察を行う．**図 5** にユーザビリティ因子を導入した安心モデルを示す．

ユーザビリティは「Q1S19」,「Q1S20」,「Q2S2」,「Q2S2」の 4 項目で構成される．また，善意に含まれていた残りの「Q1S13：あなたの操作や手続きのミスに対して契約解除や返金に応じる等の寛大な対応をしてもらえると感じる」,「Q1S14：あなたの操作や手続きのミスに対して解決を助けてくれる方法が用意されている」,「Q1S12：お金に関するトラブルが起きてもクレジットカード会社が保証してくれる」の 3 項目は，金銭面のトラブルが起きた際の保証についての項目であるといえる．そのため，これらの 3 項目で構成される要因を保証と名付けた．

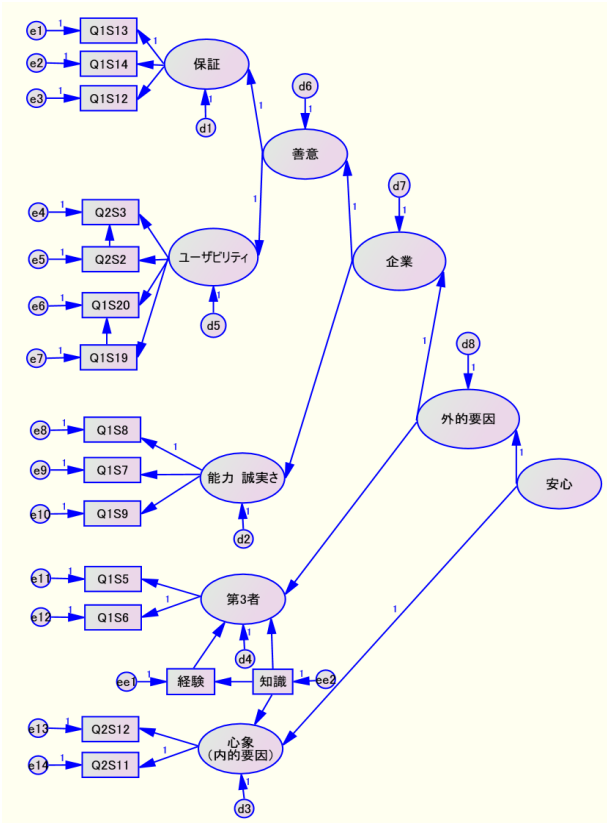

図 5 ユーザビリティ因子を導入した安心モデル
Fig. 5 Anshin model including the usability factor.

これらの考察をもとに，善意を「保証」と「ユーザビリティ」に分類し，共分散構造分析を実施した．分析の結果，GFI が 0.965，CFI が 0.979，RMSEA が 0.046，AIC が 355.167 となり，適合度指標はいずれも基準値を満たし 4 章で示したモデルより妥当性が高いことが示された．このことから，善意は「保証」と「ユーザビリティ」で構成される要因であるといえる．

本調査は，情報セキュリティ技術に関する安心感の調査をしているにもかかわらず，本来はサービスを提供する企業に責任がない場合でも対処してくれる「保証」，情報システムのみのユーザビリティではない，オンラインショッピング全体に対する「ユーザビリティ」，知識のないユーザが重視する安心感の要因として，第 3 因子「ユーザの心象」，第 4 因子「第 3 者の企業に対する評判情報の認知」といった，情報セキュリティ技術に直接関与しない要因が抽出されている．これは，吉川らの，「無知型安心」と合致する [40].「無知型安心」とは，ユーザはリスクに対する知識がないにもかかわらず安心している状態のことであり，フィッシング詐欺の被害者の行動に当てはまる．

このことから，本研究で得られた知見だけを応用する場合，ユーザに安心感を与えることは危険につながる可能性がある．ユーザに対し，安心感の要因をどのように提示するか考察する必要があるといえる．

また，本調査は，情報セキュリティ技術に関する安心感の要因を明らかにすることを目的としているが，被験者が前提条件を想像しやすくするために，「オンラインショッピング時」に限定している．そのため，抽出した安心感の要因は，オンラインショッピングに限定された要因である可能性が高い．今後の展望として，前提条件を変更した場合の安心感の要因を明らかにし，オンラインショッピング時の情報セキュリティ技術に関する安心感の要因と違いがあるのかについて検証する必要があるといえる．

6. まとめ

本論文では，情報セキュリティ技術に関する知識のないユーザのオンラインショッピング時における情報セキュリティに対する安心感の要因を明らかにする探索的因子分析および共分散構造分析により検討した．安心感要因として抽出された 4 因子は，先行研究で示された，外的要因と内的要因に分類可能であることを確認した．また，外的要因は，企業からの情報をもとに安心する要因とサービス提供者以外の第 3 者から提供された情報をもとに安心する要因の 2 種類に分類され，企業からの情報をもとに安心する要因である「善意の認知」は「保証」と「ユーザビリティ」に分類されることを示した．

安心感は主観的要因であることから，様々な状況下にお

いて違いが生じるといえる．そのため，今後，オンラインショッピング以外の，安心が求められる状況下について調査を継続的に行うこと考えている．

謝辞 本研究は，科研費（基盤研究（B）21300026）の助成を受けたものである．今回の調査に際し，質問紙作成や分析結果の考察等についてご助言いただきました，東京電機大学非常勤講師の氏家豊氏，東ワシントン大学の井上敦教授，ワシントン州立大学の Carl Hauser 准教授，岩手県立大学の柴田義孝教授，澤本潤教授，瀬川典久講師，兵庫医科大学の藤原康弘准教授に深く感謝いたします．また，Web 調査の実施にあたり協力をいただいた，被験者の皆様に謹んで感謝の意を表します．

参考文献

[1] 文部科学省：安全・安心科学技術について（平成 19 年 11 月）(2007).
[2] 経済産業省：情報セキュリティ教育に関する調査報告書（2004 年 6 月）(2004).
[3] 総務省：平成 21 年版情報通信白書 (2009).
[4] 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，Vol.48, No.9, pp.3193–3203 (2007).
[5] 藤原康宏，山口健太郎，村山優子：情報セキュリティの専門知識を持たない一般ユーザを対象とした安心感の要因に関する調査，情報処理学会論文誌，Vol.50, No.9, pp.2207–2217 (2009).
[6] 西岡 大，藤原康宏，村山優子：情報セキュリティ技術に関する一般ユーザの意見を反映した安心感調査のための質問紙作成手法の提案，情報処理学会論文誌，Vol.52, No.9, pp.2500–2525 (2011).
[7] 西岡 大，藤原康宏，村山優子：専門知識のないユーザを対象とした情報セキュリティ技術に関する安心感の調査，情報処理学会論文誌，Vol.53, No.9, pp.2213–2224 (2012).
[8] 山岸俊男：安心社会から信頼社会へ，中公新書 (1999).
[9] 村上陽一郎：安全と安心の科学，集英社新書 (2005).
[10] Kautonen, T. and Karjaluoto, H. (Eds.): Trust and New Technologies: Marketing and Management on the Internet and Mobile Media, Edward Elgar (2008).
[11] Marsh, S.: Formalising trust as computational concept, PhD Thesis, *Department of Mathematics and Computer Science*, University of Stirling (1994).
[12] Xiao, S. and Benbasat, I.: Understanding Customer Trust in Agent-Mediated Electronic Commerce, *Web-Mediated Electronic Commerce, and Traditional Commerce, Information Technology and Management*, Vol.4, No.1-2, pp.181–207, Kluwer Academic Publishers (2004).
[13] Gambetta, D.: Can we trust trust?, *Trust: Making and Breaking Cooperative Relations*, Blackwell: Oxford Press, pp.213–237 (1990).
[14] Lewis, J.D.: Trust as a social reality, *Social Forces*, Vol.63, No.4, pp.967–985 (1985).
[15] Solomon, R.C. and Flores, F.: Building Trust, Oxford University (2001).
[16] Riegelsberger, M.J., Sasse, A. and McCarthy, D.J.: The mechanics of trust: A framework for research and design, *International Journal of Human-Computer Studies*, Vol.62, pp.381–422 (2005).
[17] Falcone, R. and Castelfranchi, C.: A belief-based model of trust, *Trust in Knowledge Management and Systems in Organizations*, chapter XI, pp.306–343, Idea Group Publishing (2004).
[18] Wang, Y. and Vassileva, J.: A review on trust and reputation for web service selection, *ICDCSW '07: Proc. 27th International Conference on Distributed Computing Systems Workshops*, Washington, DC, USA: IEEE Computer Society (2007).
[19] Dragoni, N.: Toward trustworthy web services: Approaches, weaknesses and trust-by-contract framework, *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, Vol.3, pp.599–606 (2009).
[20] Greenspan, S., Goldberg, D., Weimer, D. and Basso, A.: Interpersonal Trust and Common Ground in Electronically Mediated Communication, *CSCW2000*, pp.251–260 (2000).
[21] Sainsbury, R. and Baskerville, R.: Distrusting Online: Social Deviance in Virtual Teamwork, *Proc. 39th Annual Hawaii International Conference*, Vol.6, p.121a (2006).
[22] Joinson, A.N.: Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity, *European Journal of Social Psychology*, Vol.31, No.2, pp.177–192 (2001).
[23] Sherman, R.C.: The mind's eye in cyberspace: Online perceptions of self and others, Giuseppe, R. and Galimberti, C. (Eds.), Towards CyberPsychology: Mind, Cognitions and Societyin the Internet Age, IOS Press, Amsterdam, pp.53–73 (2001).
[24] Bubas, G.: Computer mediated communication theories and phenomena: Factors that influence collaboration over the Internet, *3rd CARNet Users Conference* (2001).
[25] Whitty, M.T.: Liar, liar! An examination of how open, supportive and honest people are in chat rooms, *Computers in Human Behavior*, Vol.18, No.4, pp.343–352 (2002).
[26] DeWitt, A.J. and Kuljis, J.: ALIGNING USABILITY AND SECURITY: A USABILITY STUDY OF POLARIS, *Proc. 2nd Symposium on Usable Privacy and Security*, pp.1–7 (2006).
[27] Brustoloni, J.C. and Villamarín-Salomón, R.: Improving Security Decisions with Polymorphic and Audited Dialogs, *Proc. 3rd Symposium on Usable Privacy and Security*, pp.76–85 (2007).
[28] Besmer, A., Lipford, H.R., Shehab, M. and Cheek, G.: Social Applications: Exploring A More Secure Framework, *Proc. 5th Symposium on Usable Privacy and Security*, Article No.2 (2009).
[29] Wu, M., Miller, R.C. and Little, G.: WEB WALLET: PREVENTING PHISHING ATTACKS BY REVEALING USER INTENTIONS, *Proc. 2nd Symposium on Usable Privacy and Security*, pp.102–113 (2006).
[30] Yee, K.-P. and Sitaker, K.: PASSPET: CONVENIENT PASSWORD MANAGEMENT AND PHISHING PROTECTION, *Proc. 2nd Symposium on Usable Privacy and Security*, pp.32–43 (2006).
[31] Mitnick, K.D. and Simon, W.L.: The Art of Deception, Wiley Publishing (2002).
[32] 独立行政法人情報処理推進機構：2009 年度情報セキュリティの脅威に対する意識調査 (2009).
[33] NRI セキュアテクノロジーズ株式会社情報セキュリティに関するインターネット利用者意識調査 2008 (2008).
[34] Mayer, R.C., Davis, J.H. and Schoorman, F.D.: An Integrative model of organizational trust, *Academy of Management Review*, Vol.20, No.3, pp.709–734 (1995).

[35] Murayama, Y. and Fujihara, Y.: Anshin as Emotional Trust, *Proc. HICSS-42 Symposium on Credibility Assessment and Information Quality in Government and Business*, (in CD) (Jan. 2009).
[36] Viklund, J.M.: Trust and Risk Perception in Western Europe: A Cross-National Study Risk Analysis, Vol.23, No.4, pp.727–738 (2003).
[37] 山岸俊男，吉開範章：ネット評判社会，NTT 出版 (2009).
[38] 山崎瑞紀，吉川肇子：鳥インフルエンザ（新型インフルエンザ）に関する不安要因の構造，日本社会心理学会第 47 回発表論文集，pp.676–677 (2006).
[39] Nielsen, J.: Usability Engineering, Morgan Kaufmann (1994).
[40] 吉川肇子，白戸　智，藤井　聡，竹村和久：技術的安全と社会的安心，社会技術研究論文集，Vol.1, pp.1–8 (2003).

西岡 大　（正会員）

昭和 59 年生．平成 20 年岩手県立大学大学院ソフトウェア情報学研究科博士前期課程修了，平成 24 年 9 月同大学院ソフトウェア情報学研究科博士後期課程修了．博士（ソフトウェア情報学）平成 25 年 4 月より岩手県立大学ソフトウェア情報学部助教．現在に至る．情報セキュリティに関する安心感の研究に従事．ACM，日本セキュリティマネジメント学会各会員．

齊藤 義仰　（正会員）

平成 18 年静岡大学大学院理工学研究科博士過程終了．博士（情報学）．平成 16 年から平成 19 年まで独立行政法人情報通信研究機構（NICT）特別研究員・専攻研究員．平成 19 年 10 月より岩手県立大学ソフトウェア情報学部講師．平成 23 年 10 月より准教授．現在に至る．IEEE，ACM，電子情報通信学会各会員．

村山 優子　（正会員）

津田塾大学学芸学部数学科卒業．三菱銀行および横河ヒューレット・パッカード社に勤務．昭和 59 年 University College London 大学院理学部計算機科学科修士課程修了．平成 2 年同大学大学院博士課程修了．Ph.D.（ロンドン大学）．慶應義塾大学環境情報学部非常勤講師を経て，平成 6 年 4 月より広島市立大学情報科学部情報工学科講師，平成 10 年 4 月より岩手県立大学ソフトウェア情報学部助教授．平成 14 年 4 月より教授．現在に至る．インターネット，トラストおよび安心の研究に従事．情報処理学会監事，IFIP TC11 Vice Chair，IEEE シニアメンバ，ACM，電子情報通信学会，映像情報メディア学会，日本 OR 学会，情報知識学会各会員．