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

日景 奈津子† カール ハウザー†† 村山 優子†

本研究では，情報セキュリティ技術に対する利用者の安心感について，その構造を明確にする．安心感の要因を把握するための調査実験を行い，探索的因子分析を実施した．その結果，セキュリティ技術の安全性に関わる因子，システムの操作性や使いやすさに関わる因子等，6 因子を抽出した．さらにそれらの因子が，外的要因と内的要因の 2 つのグループに大別され，安心感を構成しているという仮説を立て，共分散構造分析により検証した．本論文では，調査実験および分析結果とともに安心感の構造について報告する．

A Statistical Discussion of the Sense of Security, Anshin

Natsuko Hikage,† Carl Hauser†† and Yuko Murayama†

In this research, we identify the structure of Anshin — the sense of security. We conducted the user survey and came up with six major factors by the explanatory factor analysis (EFA). With the results, we had a hypothesis that those six factors could be categorized in two groups; one is environmental-based and the other is personal-based. The two groups would consist Anshin. We verify our hypothesis by using structural equation modeling (SEM). This paper reports on our survey and analysis.

1. はじめに

従来の情報セキュリティ分野では，工学的な立場からセキュアな技術を提供すれば利用者は安心するという仮定の下，研究開発が進められてきた．その評価方法の多くは，安全性評価や性能評価により，その達成度を客観的に示すことで行われている．セキュリティ技術の客観的安全性だけではなく，利用者の安心感の重要性について，ヒューマンクリプトという概念が提唱されてきた[1]．ヒューマンクリプトは人に安心を与えるためのセキュリティ技術であり，システムが利用者の意思どおりに機能していることを保証し，かつそれを利用者に納得させることを目的としている．

本研究では，技術の安全と利用者の安心の関係について，その枠組みを**図 1** に示すとおり検討した．横軸は情報セキュリティ技術の安全性の程度を表し，縦軸が利用者の心的状態を表す．図 1 のように 4 象限で安心と安全をとらえたとき，高いセキュリティが確保され，利用者が不安を感じていない状態が最も望ましい状態である．また，技術的に危険な状態では，利用者はそれを認識し，不安である状態が望ましい．

しかし，情報セキュリティ技術が「安全」でも「安心」が得られない状況も起こりうる．これは，図 1 の領域 1 に該当する．村上は，この「安全」でも「安心」が得られない状態が最も顕著に現れているのは原子力の分野であると考察している[2]．原子力発電の現場は，他の様々な現場に比べ客観的な安全性において優れているといわれているが，人間がときに犯すミスやエラーが凶器となる事件が発生しており，原子力発電に対する不安はいまだ払拭されない．また飯塚らは，情報セキュリティ対策を十分に施したシステムであっても，利用する場所によって利用者の安心感に大きな差があることを実験的に示している[3]．このように，安全性が確保されているシステムであっても，ユーザビリティの問題や利用者の主観を考慮しないインタフェース設計等が要因となり，利用者に不安をいだかせる場合がある．

一方，危険であるという認知が欠如した状態で安心していることもありうる．これは図 1 の領域 2 に該当する．この状態について吉川らはリスクコミュニケーションの観点から，知識がなく安心している状態を「無知型安心」とし，見かけ上の安心ではなく，知識や情

† 岩手県立大学大学院ソフトウェア情報学研究科
Graduate School of Software and Information Science, Iwate Prefectural University
†† ワシントン州立大学
School of Electrical Engineering and Computer Science, Washington State University

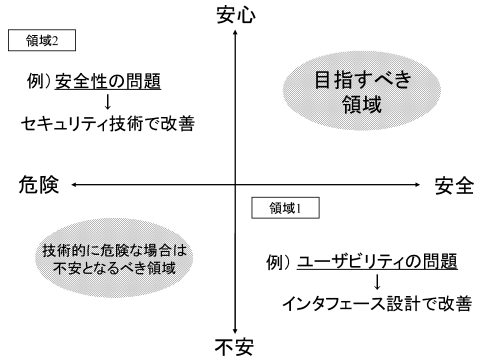

図 1 安心とセキュリティ技術の関係
Fig. 1 A relation between secure feeling and security technology.

報取得を経た「能動型安心」が望ましい状態であると指摘している[4]．また，吉川らの提唱する「無知型安心」の例として，フィッシング詐欺の被害者の状態はこの領域に分類できる．Dhamija らによると，フィッシング詐欺の手口は知識不足や注意不足の利用，表示による欺き等に分類される[5]．特に，SSL が提供する鍵アイコンの意味や SSL 証明書等の確認方法を知らないまま，真偽の判定をサイトの見た目（コンテンツやドメイン名等）のみで判断する場合が最も多い．このことから，吉川らの提唱する「能動型安心」に加え，危険であることを認知させ，利用者を安易に安心させないことも重要である．

以上の背景から，本研究ではネットワークを基盤とする環境でのセキュリティ技術と利用者が考えている安心感についての関係を明らかにし，安全かつ利用者が安心して利用できるシステムの構築を目指してきた．その中で，筆者らは安心感を定量的に評価するための安心度評価モデルについて提案し，実験的検討を進めてきた[6),7)]．しかし，具体的な評価指標や，安心感に影響を及ぼすであろうと仮定した諸要因の妥当性が不明瞭であった．

本研究では，情報セキュリティ技術に対する安心感の潜在的な要因を把握する目的で，質問紙調査による調査実験を行った．本論文では，利用者の安心感に影響を及ぼす諸要因について述べ，その構造について考察する．以降，2 章では，安心感に関する基礎的検討として関連研究について概説し，3 章では探索的因子分析により抽出した安心感要因について考察し，安心感の構造についての仮説を述べる．4 章では共分散構造分析を用いて仮説の検証を行い，5 章でまとめを行う．

2. 関 連 研 究

本章では，安心の定義について紹介し，安心感に関する既存研究について議論する．

吉川らは，社会学の立場から安全と安心について議論し，安全が技術的に達成できる事柄であるのに対し，安心はそれだけでは達成できない心理的な要素を含むものであると述べている[4)]．国内では，多くの場合安心ととらえられている概念を，欧米ではトラスト（信頼）と表現することが多く，その概念は心理学，社会学，経済学，特に近年では電子商取引における信頼形成に関する研究分野等において，その重要性が指摘されてきた[8)~11)]．Lewis らは，トラスト（信頼）には，認知的なトラスト（Cognitive Trust）と感情的なトラスト（Emotional Trust）があることを報告している[8)]．しかし，従来研究においては，認知的トラストの定義や枠組みについては確立されつつあるが，感情的トラストについて言及している研究は前者に比べ比較的少ない．以下にそれぞれの定義を紹介する．認知的トラストとは，トラストする者（Trustor）の，トラストされる者（Trustee）への，論理的根拠のある期待（Rational Expectation）であり，認知的評価である．論理的根拠とは，相手が能力（Competence），誠実さ（Integrity），善意（Benevolence）を持ち合わせているであろうという期待である[11)]．一方，感情的トラストは，相手に対する，自分自身の安心感（Secure Feeling）や情緒的安定（Emotional Security）による主観的評価である[10)]．このことから，安心感とはトラストの感情的側面である Emotional Trust と同義であるといえる．

一方国内では，山岸が安心と信頼を区別した定義を提唱している[12)]．両者は「相手は自分を裏切らないという期待」であるという点では同じであるが，その根拠が異なるという．安心は「相手に裏切りの誘因が存在しない場合，相手の協力行動に対する期待」であり，それに対し信頼は「相手に裏切りの誘因が存在する場合，相手の協力行動に対する期待」であると定義している．

どのような要因が利用者の安心感に影響を及ぼしているかを把握するためには，安心感について評価することが求められる．しかし，利用者の安心感については，心理的な側面が強い概念であることから，定量的に評価することは困難であることが予想される．安心感の定量的な扱いの困難さは，村上の提唱する安全学においても指摘されており[2)]，安心感については主観的にしか評価できない．人間の主観や感性を評価する手法として，主観評価法がある．主観評価法は主に心理学の分野で用いられてきたが，工学分野においても特にヒューマンインタフェースの評価方法としてその

重要性が認知されている．心理学的アプローチでは，このような主観的かつ抽象的な構成概念について，数値としてデータ化する手続きを測定とよび，その手続きは一般に質問紙尺度を用いて行われる[13]．実用性の高い尺度の一例として，コンピュータと接触する際の個人の内に喚起される不安を測定するコンピュータ不安尺度[14]があり，情報教育の現場で多用されている．過去の研究において尺度の妥当性や信頼性が検証されている尺度は，客観性があることが認められている．

また，コンピュータシステムに対する利用者の主観評価については，80 年代から 90 年代前半にかけて，ユーザビリティ評価に関する研究分野を中心に満足度の主観評価尺度が開発されてきた[15)~20)]．これらの評価尺度は，今日のようにインターネットが一般家庭に至るまで普及する以前に開発されたものであり，ネットワークを介した情報操作に主眼を置いてはいない．ネットワークを介して誰もが様々な情報を扱うようになった現在では，セキュリティ面での安全性対策は必須である．このように利用者を取り巻く環境が変化しつつある中，単なる操作性や満足感だけではなく，情報セキュリティ技術に対する利用者の安心感について，その評価指標や評価手法を検討することは重要な研究課題であるといえる．

一方，酒井らは，原子力発電所に対するイメージが安心感に与える影響について検討した結果，安心を感じられる根拠は客観的に測れるものではなく，自分自身の経験や他者との相互関係に基づくものであることを示した[21]．先に述べた飯塚らの検討においても，情報セキュリティ対策を十分に施したシステムであっても，利用する場所によって利用者の安心感に大きな差があることを確認し[3]，安心して個人情報を扱うことのできる公共作業環境について実験的検討を進めている[22]．また，高橋らはインタフェース工学の立場から安心要素および不安要素についての心理学実験を実施し，インタフェースの色彩や音声等の情報表示手法の違いが安心感に影響があることを実験的に示した[23]．

これらの既存研究により得られた知見を以下のようにまとめた．1) 安心感は主観的であると同時に，トラストの感情的な側面（Emotional Trust）とも同義である．2) 技術の客観的安全性を確保することは利用者の安心感にとって重要であるが，安心感にはそれ以外の潜在的な要因があることが予想される．以上のことから，安心感の構造を明確にするためには，心理的要因も含めた，安心感の潜在的な要因を明らかにする必要がある．

3. 安心感要因に関する調査実験

前章での議論から，本研究では安心感の潜在的要因を把握するため，質問紙を用いた調査実験を実施した．3.1 節では，質問紙で使用する尺度についての検討内容を述べる．3.2 節以降では，質問紙調査のデータに基づいて，探索的因子分析を実施した結果について報告する．

3.1 主観評価尺度に関する予備検討

はじめに，質問紙を作成するにあたり，以下に示す既存の評価尺度について検討した．

(1) ユーザの PC 操作に対する満足感に関する尺度として，CUS（Computer User Satisfaction）[15]，UIS（User Information Satisfaction short-form）[16]，EUCS（End-User Computing Satisfaction）[17] 等がある．

(2) ユーザビリティに関して，ユーザの主観的な満足感や不安感等の客観的に測りにくい指標についてアンケートやインタビュー等の手法を用いることが有効である[24]．特に満足度を測るための代表的な主観評価尺度として，QUIS [18]，SUMI [19]，SUS [20] がある．

(3) 2 章で紹介したリスクコミュニケーションに関する既存研究には，原子力に関する意識調査[25]や原子力発電所に対する安心感調査[21]において，質問紙を用いた調査や検討がいくつか行われている．

これらのうち (1) と (2) で紹介した既存尺度は，主としてネットワークを介した情報操作を想定しておらず，必ずしも情報セキュリティに対する満足感を測定するものではない．今回の調査対象である情報セキュリティに対する安心感について調査する場合には，そのまま使用することは困難であるが，システムの操作性に対する一般的な項目については，既存尺度を参考にし作成した．(3) のリスクコミュニケーションに関する関連研究で用いられている質問項目については，原子力発電所等の科学技術分野全般を対象としたものであるが，対象を情報システムや情報サービスに対応する形に変更を加えることにより，応用可能であると考えた．

また，本研究の先行調査として 2006 年 7 月に実施した予備実験[26]で使用した設問項目について再検討し，さらに同調査で得られた自由記述回答から，人々が情報セキュリティ技術に対する安心感についてどのように感じているかを整理した．それにより，技術の安全性やリスク理解に関する項目，および評価対象に

表 1 測定項目の記述統計量（N = 425）
Table 1 Amount of descriptive statistics (N = 425).

測定項目	平均値	S.D	歪度	尖度
A01 サービスを提供する事業主や会社自体を信頼している	4.440	1.673	-0.474	-0.703
A02 サービスを提供する事業主や会社は社会的信用がある	5.466	1.486	-1.137	0.849
A03 サービスを提供する事業主や会社は確かな能力や実績がある	4.551	1.453	-0.367	-0.280
A04 サービスを提供する事業主や会社は利用者を裏切るはずはない	3.151	1.565	0.376	-0.657
A05 サービスを提供する事業主や会社は善意に基づいている	3.409	1.524	0.127	-0.639
A06 大手の会社や事業主が提供するシステムやサービスは安心である	4.104	1.588	-0.348	-0.675
A07 適切な個人情報管理対策が実施されている	4.045	1.572	-0.107	-0.692
A08 入力した個人情報は適切に管理され、外部に漏洩することは決してない	2.718	1.684	0.847	-0.134
A09 システムや技術そのものを信頼している	3.475	1.429	-0.072	-0.588
A10 何かトラブルがあっても確実な保証がある	2.986	1.580	0.500	-0.449
A11 何かトラブルがあってもシステムが回復すれば大丈夫だ	2.541	1.377	0.783	0.105
A12 何かトラブルがあってもシステムが支援をしてくれる	3.016	1.336	0.280	-0.522
A13 安全性がきちんと確保されている	3.619	1.520	0.068	-0.666
A14 安全であることを実感できる	3.511	1.476	0.096	-0.604
A15 安全性対策には十分な配慮がなされている	3.856	1.517	-0.073	-0.656
A16 自分はシステムの仕組みについてある程度理解している	3.028	1.529	0.326	-0.756
A17 自分はセキュリティ対策をしているので大丈夫だ	2.934	1.372	0.251	-0.648
A18 自分は情報技術についてよく知っているほうだ	2.774	1.496	0.459	-0.638
A19 自分はどんなリスクや脅威があるか理解をした上で利用している	3.965	1.637	-0.180	-0.771
A20 適切な情報提示の仕方である	3.831	1.346	-0.319	-0.260
A21 システムのデザインに親しみがもてる	3.593	1.464	-0.191	-0.658
A22 システムのデザインが魅力的だ	3.431	1.494	-0.080	-0.758
A23 システムのデザインのレイアウトや色使いがきれいだ	3.525	1.516	-0.149	-0.788
A24 システムが使いやすい	4.078	1.413	-0.430	-0.288
A25 システムの操作性が優れている	4.028	1.409	-0.401	-0.346
A26 操作方法の説明が丁寧で、親切な印象をうける	3.960	1.431	-0.313	-0.547
A27 わずらわしい作業が少なく、簡単に利用できる	3.854	1.564	-0.188	-0.740
A28 ぱっと見て受けた印象で、説明や情報量が適切である	3.976	1.542	-0.302	-0.613
A29 いつも利用しているので使い慣れている	4.442	1.597	-0.611	-0.337
A30 いつも利用しているので経験上心配はない	3.809	1.606	-0.161	-0.757
A31 自分の知人や家族が使っていたので、安心だ	3.614	1.637	0.101	-0.779
A32 具体的な根拠はないが、なんとなく安心だ	3.127	1.591	0.243	-0.889
A33 具体的な根拠はないが、何となく気に入っている	3.412	1.558	-0.074	-0.937
A34 親切な対応やサービスに好感が持てる	3.861	1.516	-0.351	-0.628
A35 自分の趣味や嗜好に合っている	3.904	1.561	-0.422	-0.498

※ 数値は，まったくそうは思わない（1点），そうは思わない（2点），あまりそうは思わない（3点），どちらともえいない（4点），ややそう思う（5点），そう思う（6点），非常にそう思う（7点）の7点尺度である

対する主観的な印象に関する項目を新たに作成した．以上の検討の結果，計 35 項目の設問項目を作成した．

3.2 調 査 方 法

質問紙調査は次のとおり実施した．

調査日時 2006 年 10 月 30 日〜2006 年 11 月 15 日

手続き 学部 1〜4 年次対象の複数の講義時間内で，自記式の集合調査を実施した．事前に担当教員と受講学生の了解を得たうえで調査用紙を配布し，15 分程度の回答時間を設け，その場で回収した．調査の趣旨説明から回収まで計 20 分程度で完了するように行い，被験者の負担には十分考慮したうえで実施した．

被験者 ソフトウェア情報学部 320 名，短期大学部国際文化学科 51 名，総合政策学部 30 名，社会福祉学部 27 名，看護学部 24 名の学生計 452 名に回答を依頼した．すべての被験者は情報処理に関する基礎教養科目を履修済みであり，日常的にインターネットを利用している．

回収票 452 名のデータのうち，記入漏れ等の無効票を除いた 425 件を分析に用いる有効票とした．425 件の内訳は，ソフトウェア情報学部 307 名，短期大学部国際文化学科 46 名，総合政策学部 25 名，社会福祉学部 26 名，看護学部 21 名であった．また，平均年齢は 19.45 歳（18 歳〜36 歳）であった．

調査内容 前節で検討した 35 の設問項目が安心感の根拠や理由として納得できるかどうかについて，非常にそう思う（7 点）〜まったくそうは思わない（1 点）の 7 段階で評定を求めた．状況設定とし

表 2 最尤法，因子数 6，Promax 回転後の因子パターン行列（N = 425）
Table 2 Factor pattern matrix (N = 425).

変数	I	II	III	IV	V	VI
A13 安全性がきちんと確保されている	**0.942**	0.053	-0.081	0.013	0.003	-0.062
A15 安全性対策には十分な配慮がなされている	**0.910**	0.041	0.077	-0.030	-0.035	-0.165
A14 安全であることを実感できる	**0.836**	-0.068	0.119	0.034	0.002	-0.102
A07 適切な個人情報管理対策が実施されている	**0.707**	0.005	0.033	-0.043	-0.031	0.119
A08 入力した個人情報は適切に管理され、外部に漏洩することは決してない	**0.630**	-0.059	-0.086	0.014	-0.082	0.207
A10 何かトラブルがあっても確実な保証がある	**0.599**	-0.046	-0.043	-0.068	0.139	0.143
A12 何かトラブルがあってもシステムが支援をしてくれる	**0.516**	0.010	-0.130	0.229	0.083	0.086
A25 システムの操作性が優れている	-0.064	**1.080**	-0.101	-0.070	0.013	0.009
A24 システムが使いやすい	-0.031	**0.948**	-0.066	0.049	-0.022	-0.040
A26 操作方法の説明が丁寧で、親切な印象をうける	0.032	**0.710**	0.056	0.002	0.007	0.076
A27 わずらわしい作業が少なく、簡単に利用できる	0.076	**0.478**	0.124	0.108	0.021	0.032
A28 ぱっと見て受けた印象で、説明や情報量が適切である	0.083	**0.445**	0.274	0.086	0.061	-0.077
A29 いつも利用しているので使い慣れている	-0.059	0.017	**0.912**	-0.076	0.074	-0.120
A30 いつも利用しているので経験上心配はない	0.054	-0.117	**0.872**	-0.062	0.056	-0.007
A33 具体的な根拠はないが、何となく気に入っている	-0.199	0.035	**0.478**	0.228	-0.075	0.213
A31 自分の知人や家族が使っていたので、安心だ	0.120	0.010	**0.471**	0.041	-0.155	0.172
A35 自分の趣味や嗜好に合っている	-0.056	0.178	**0.454**	0.133	0.014	0.027
A34 親切な対応やサービスに好感が持てる	0.121	0.242	**0.399**	0.050	0.026	0.014
A22 システムのデザインが魅力的だ	0.034	-0.065	0.005	**1.029**	0.006	-0.025
A23 システムのデザインのレイアウトや色使いがきれいだ	0.027	0.143	-0.052	**0.855**	-0.032	-0.042
A21 システムのデザインに親しみがもてる	-0.042	0.124	0.025	**0.805**	0.009	0.003
A18 自分は情報技術についてよく知っているほうだ	-0.068	0.006	-0.071	0.073	**0.906**	0.088
A16 自分はシステムの仕組みについてある程度理解している	0.165	-0.042	-0.027	0.009	**0.720**	-0.058
A19 自分はどんなリスクや脅威があるか理解をした上で利用している	-0.092	0.078	0.096	-0.102	**0.680**	-0.089
A17 自分はセキュリティ対策をしているので大丈夫だ	0.054	-0.022	0.094	0.003	**0.677**	0.098
A04 サービスを提供する事業主や会社は利用者を裏切るはずはない	0.006	-0.042	-0.017	-0.015	0.046	**0.855**
A05 サービスを提供する事業主や会社は善意に基づいている	-0.019	0.000	-0.039	0.031	0.070	**0.788**
A06 大手の会社や事業主が提供するシステムやサービスは安心である	0.165	0.074	0.051	-0.033	-0.154	**0.504**
A03 サービスを提供する事業主や会社は確かな能力や実績がある	0.257	0.079	0.069	-0.159	0.003	**0.408**
固有値	10.239	3.781	2.372	1.385	1.366	1.056
寄与率 (%)	35.306	13.038	8.179	4.777	4.709	3.641
累積寄与率 (%)	35.306	48.344	56.523	61.300	66.009	**69.650**

てはインターネットを介して個人情報を送信するような場面での「安心感」について尋ねた．実際の質問紙で提示した説明文と設問項目を付録 A.1 に示す．

3.3 探索的因子分析

調査結果から，7 段階評価での得点化により算出した測定項目の平均値，標準偏差，歪度および尖度を**表 1** に示す．これによると，平均値が中央値の 4 点より低い 2〜3 点台の項目も複数見受けられるが，歪度と尖度の値については極端に分布が偏った項目は認められない．そこで，すべての項目を分析に用いることが可能であると判断した．

安心感の因子構造を把握するため，全 35 項目を用いて探索的因子分析を実施した．分析には統計解析ソフトウェアである SPSS 14.0J for Windows を使用した．因子の抽出には最尤法を用いた．初期解における固有値の減衰状況（第 1 因子から順に 11.764，4.160，2.658，1.736，1.467，1.357，0.891，...）から，第 6 因子と第 7 因子間に大きな変化があることを確認し，因子の解釈可能性も考慮したうえで最終的に 6 因子解を採用した．因子数を 6 に固定したうえで最尤法および Promax 回転による因子分析を行った．その結果，いずれの因子にも 0.35 以上の負荷量を示さなかった項目や複数の因子に 0.35 以上の同等の負荷量を示した項目計 6 項目を除き，最終的に計 29 項目から 6 因子を抽出した．Promax 回転後の因子パターン行列を**表 2** に，因子相関行列を**表 3** に示す．なお，Promax 回転前の 6 因子で 29 項目の全分散を説明する割合である累積寄与率は 69.65%であった．

表 3 因子相関行列
Table 3 Factor correlation matrix.

因子	I	II	III	IV	V	VI
I	-	0.37	0.46	0.23	0.40	0.52
II		-	0.69	0.72	0.27	0.39
III			-	0.54	0.29	0.46
IV				-	0.20	0.36
V					-	0.15
VI						-

因子の解釈について以下のように検討した．第 1 因子は，セキュリティ技術の安全性に関する項目に高い負荷量を示していることから，“セキュリティ技術

(Security Technology) 因子" と命名した．第 2 因子は，システムの操作性や使いやすさに関する項目に高い負荷量を示していることから，"ユーザビリティ (Usability) 因子" と命名した．第 3 因子は，ユーザ自身の経験に基づく安心感に関する項目に高い負荷量を示していることから，"経験 (Experience) 因子" と命名した．第 4 因子は，デザインに対するユーザの趣味嗜好に関する項目に高い負荷量を示していることから，"プリファランス (Preference) 因子" と命名した．第 5 因子は，セキュリティ技術やリスクに対する理解に関する項目に高い負荷量を示していることから，"知識 (Knowledge) 因子" と命名した．第 6 因子は，サービスやシステム提供者の社会的信用に関する項目に高い負荷量を示していることから，"信用 (Belief) 因子" と命名した．

各因子の内的整合性を確認するため，信頼性係数アルファを算出したところ，第 1 因子の 7 項目で $\alpha = 0.90$，第 2 因子の 5 項目で $\alpha = 0.91$，第 3 因子の 6 項目で $\alpha = 0.85$，第 4 因子の 4 項目で $\alpha = 0.84$，第 5 因子の 3 項目で $\alpha = 0.95$，第 6 因子の 5 項目で $\alpha = 0.79$ が得られた．以上の結果から，因子構造の明確さおよび信頼性の高さは十分に示された．

3.4 安心感の構造についての仮説

探索的因子分析の結果，安心感の要因として 6 因子が抽出可能であることを確認した．2 章で示したように，安心感とは主観的な感情であり，トラストの感情的側面 (Emotional Trust) とも同義であることを述べた．本節では，Emotional Trust にも該当する，主観的な安心感が，さらに 2 つの構造に分かれるという新たな仮説を述べる．

抽出された因子は，評価の対象側に依存する因子と評価者 (利用者) 自身に依存する因子が混在している点が見受けられる．前者の性質は，情報システムやサービスを提供する側，あるいは情報システムやサービスそのものの環境に依存することから，外的要因 (Environmental-Based Factor) と定義する．また，後者の性質は，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よるものであることから，内的要因 (Personal-Based Factor) と定義する．安心感とは，上述の定義に基づき，セキュリティシステムに依存する外的要因と利用者自身の心理的な考えに依存する内的要因の 2 つに分類されると仮定する．

ここで改めて抽出された 6 つの因子について考察すると，評価者自身にとっての外的要因と内的要因が混在している．第 1 因子のセキュリティ技術因子は，

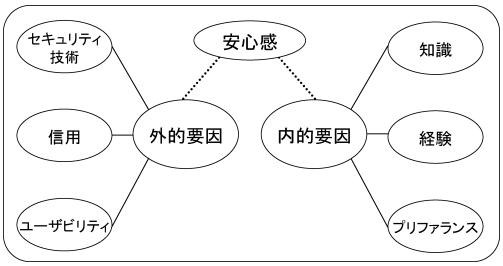

図 2 2 つの性質による安心感要因の分類
Fig. 2 Classification based on multi dimension of a security.

サービスやシステムの安全対策能力や保証能力を表す項目であり，システム側に依存する要因である．インタフェースを介した印象については，第 2 因子のユーザビリティ因子と第 4 因子のプリファランス因子があるが，前者がシステムの操作性や設計の親切さを表す項目であるのに対し，後者はデザインに対する好みや親しみやすさ等，個人の主観に依存する感情である．第 3 因子の経験因子は，利用者自身の個人的な経験に基づくものである．また，第 5 因子の知識因子は，コンピュータリテラシの程度や，リスクや脅威に対する認知を表す項目であるが，その根拠は自身の事前知識に依存するものである．第 6 因子の信用因子に含まれる項目は，設問の A04 や A05 に代表されるように，システム提供者側に依存する要因である．以上の考察から，抽出された 6 因子は，先に定義した外的要因と内的要因の 2 つの性質に分類できる．分類したモデルの構成を**図 2** に示す．

4. 共分散構造分析による安心感要因の検証

4.1 因果モデルの作成

本節では，3.4 節で示した安心感構造の仮説について，共分散構造分析を用いて妥当性の検証を試みる．共分散構造分析 (Structural Equation Modeling；以下 SEM とよぶ) とは，ある事象に対する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る[27]．因子 (構成概念) を含めた因果関係の検討や，すでに得ている知見や仮説を検証する機能を持つことから，SEM を選択した．構築した因果モデルの妥当性を確認するためには，そのモデルがどの程度受容できるかを表す適合度指標を用いる．代表的な適合度指標としては，カイ 2 乗検定，GFI，CFI，RMSEA，AIC 等がある．カイ 2 乗検定については，標本数 N に強い影響を受け，大標本の場合は必ずモデルが棄却されるという性質が知られていることから[28]，今回はカイ 2 乗検定を除いた残りの 4 つの適

合度指標を採用した．以下にその概要を示す．

GFI 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[28]．

CFI CFI（Comparative Fit Index）値も同様に，1に近いほどモデルのあてはまりが良いとされ，0.9以上であることを受容の基準としている[28]．

RMSEA 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以上であればあてはまりが悪いと判断する．受容の判定基準は0.08以下とされている[27]．

AIC AIC（Akaike Information Criterion）の値が小さいモデルほどあてはまりの良いモデルと判断する．AIC値に絶対的な意味はなく，複数のモデル間の比較をする際の相対的基準として用いられる[27]．

本研究では，3.4節で考察した仮説に基づいて分類した，安心感の外的要因であるセキュリティ技術因子，信用因子，ユーザビリティ因子の3因子間，および内的要因であるプリファランス因子，経験因子，知識因子の3因子間において，それぞれ中程度の相関が見られたことから，その背後に高次因子を仮定した因果モデルを構築した．通常，因子分析は複数の観測変数によって各因子が計測されるが，因子の背後にさらに因子を仮定するような2段階の因子構造を測定することを高次の因子分析とよぶ[29]．6つの因子のそれぞれに高い負荷量を示す上位3項目を選定し，これらをSEMに用いる観測変数とした．分析には共分散構造分析ソフトウェアであるAmos5.0Jを使用した．構築した高次因子モデルと解析結果を**図3**，**図4**および**表4**に示す．

ここで，SEMにおけるモデル表現[27]について補足する．ある現象や状態に対して，直接計測されるものを観測変数とよび，直接観測されない構成概念は潜在変数とよぶ．通常，前者は四角形で表し，後者は楕円形で表す．なお，図中の観測変数名は，表2の探索的因子分析の結果と対応している．SEMにおける因果モデルの基本は，因果の結果が因果の原因による結果として決まるものであるが，それだけでは説明できない部分がある．これを観測値に対しては「誤差」とし，構成概念に対しては「攪乱」とよぶ．図中の誤差変数はe1〜e9に，攪乱変数はd1〜d3に該当する．変数

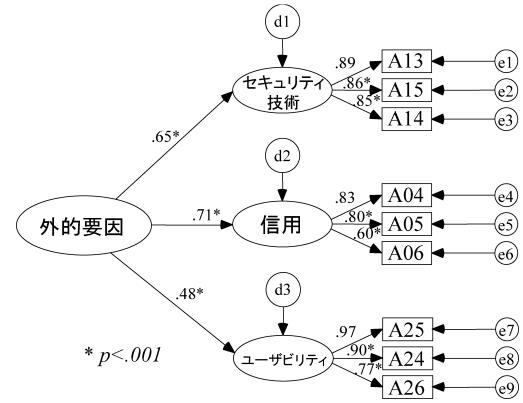

図3 モデル1：外的要因に基づく安心感についての2次の因子モデル

Fig. 3 Model1: High-order factor model about a sense of security based on environmental factors.

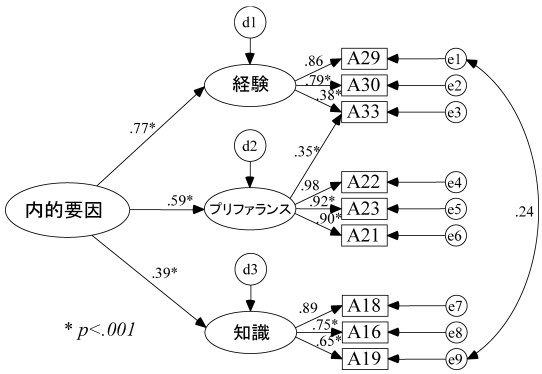

図4 モデル2：内的要因に基づく安心感についての2次の因子モデル

Fig. 4 Model2: High-order factor model about a sense of security based on personal factors.

表4 モデル1および2の適合度指標

Table 4 Fit index of model1 and model2.

適合度指標	GFI	CFI	RMSEA	AIC
モデル1（図3）	0.974	0.987	0.055	94.403
モデル2（図4）	0.978	0.991	0.047	88.541

間の関係が，因果関係であれば矢印をともなう直線で示し，相互に関係する場合は矢印をともなう円弧で表され，これらをパスとよぶ．パスに隣接して出力されている数字はパス係数であり，因果関係や相関関係の程度を表している．図3および図4内のパス係数は，観測変数の分散をすべて1に標準化したときの推定値（標準解）として出力されている．なお，有意確率が測定されないパス（セキュリティ技術因子 → A13，信用因子 → A04，ユーザビリティ因子 → A25，経験因子 → A29，プリファランス因子 → A22，知識因子 → A18）があるのは，モデルの識別性を確保する

ため潜在変数から観測変数へのパスのうち，モデル内で最も上にあるパスについてパス係数を 1 に固定し拘束を加えているためである．

4.2 分析結果

図 3 の “外的要因” 因子を高次因子として分析した結果，適合度指標はいずれも基準値を満たす値を示しており，全体的に良好である．また，高次因子から下位の 3 因子へのパス係数はいずれも十分に高い値を示しており，有意水準 0.1%で有意である．続いて，図 4 の “内的要因” を高次因子として分析した結果，適合度指標はいずれも基準値を満たす値を示しており，全体的に良好である．また，高次因子から下位の 3 因子へのパス係数はいずれも高い値を示しており，有意水準 0.1%で有意である．なお，後者のモデルについては，下位の 3 因子のそれぞれに高い負荷量を示す上位 3 項目を観測変数とする当初のモデルについて分析を行った後，修正指数を利用して修正を加えた結果，より適合状態の良いモデルを選択したものである．修正箇所は，第 2 因子から観測変数 A33「具体的な根拠はないが，何となく気に入っている」へのパスで，これにより適合度指標の改善が期待され，また因子の解釈上も大きな無理はないためパスを加えた．同様の理由で，修正指数に基づいて誤差変数間の e1 と e9 の間に共変動を加えた．

これらの結果は，3 因子の背後にそれぞれ総合的な高次因子の存在を考えることの妥当性を示しているといえる．さらに，外的要因と内的要因に分類したモデルの有意性を確認する目的で，図 2 のような分類を行わずに 6 因子すべてを用いて検証的因子分析を実施した．検証的因子分析モデルには，探索的因子分析で得られた表 2 のパターン行列を用いて，6 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，さらに 6 因子間に共変動を仮定した．その結果，GFI = 0.933，CFI = 0.967，RMSEA = 0.058，AIC = 453.38 となり，全体的に良好ではあるが，AIC については前述の 2 つのモデルより大幅に増加している．AIC は相対的な指標であり，AIC の値が小さいモデルほど優れていると判断できることが知られている[27]．また，2 つの高次因子を設けた方がより構成概念の性質を理解しやすいという理由から，高次因子を仮定したモデルの方が妥当であるといえる．

4.3 仮説の検証

4.2 節での分析結果について，総合的な考察を行う．まず，探索的因子分析で抽出した 6 つの因子は潜在的な安心感要因を示すものであり，利用者の安心感を評価するには，複数の指標について検討しなければならないことを示唆している．同時に，各要因の持つ安心感への影響の強さは，評価対象と各ユーザの主観的な判断に依存するものであるが，今後継続的に調査を続けデータの安定性を確認できれば，統計的にその重みの程度を示すことは可能である．

本調査において抽出した因子であるセキュリティ技術因子，ユーザビリティ因子，経験因子，プリファランス因子，知識因子，信用因子は，Hoffman らの提案するトラストモデル[30] の諸要因；Security，Usability，Reliability，Privacy，Availability，Safety とも一部類似している．Hoffman らは安全性や信頼性を含むセキュリティの上位概念としての包括的なトラストとして位置づけており，本研究のトラストモデルへの発展可能性を示唆している．

3.4 節では，安心感要因として抽出された 6 因子は，対象となるセキュリティシステムに依存する外的要因と個人の主観的な考えに依存する内的要因が混在していることを指摘し，新たな安心感の構造モデルを示した．仮説に基づいて各因子を外的要因と内的要因に分類し，それぞれ高次の因子を仮定したモデルについて SEM を用いて分析した結果，適合度指標が良好であったことから，その仮説の妥当性を示すことができた．2 つの高次因子が下位の安心感要因を強く規定していることは確認できたが，そのうち高次の “内的要因” に含まれる “知識因子” については，他のパス係数と比較すると，その値は 0.39 とやや低めである．

知識の扱いについて先行研究の知見とあわせて見ると，前述した Xiao らのモデル[11] や Hoffman らのモデル[30] においては，トラスト全体に影響を及ぼす別の要因として扱われている．対象（サービスやシステム）の評判やうわさ，経験値等も含めた性質として知識を解釈している点で，本研究と異なる．本研究では，情報技術やセキュリティ対策に対する理解は，ユーザ自身の主観的知識に基づくものであることから，内的要因を構成する因子に含めることが可能であると判断した．知識に着目した研究として，Slovic が，科学や技術のリスク認知においては，専門家と一般の人々とではそのとらえ方に大きな差があることを確認している[31]．それに関連して，永井ら[25] や木村ら[32] の調査研究においても，主観的な知識量の差が原子力発電に対する受容態度に影響を及ぼすことを示唆している．“知識因子” の扱いについては，今回採用したモデル以外の解釈の可能性もあることから，今後の課題として継続的な調査を続けていきたい．

最後に，今回使用したサンプルの問題点として，被験者の属性による偏りがあげられる．被験者がすべて

学生であること（平均年齢 20 歳）や，分析に用いた 425 件のサンプルのうち，半数以上が情報分野の学問を専攻していること等である．このような，年齢や専門性の違いによるコンピュータリテラシの程度の差は，安心感のとらえ方に大きく影響を及ぼすといえる．今後，ユーザ属性の違いによる安心感への影響を検証するため，被験者の属性ごとでより多くのデータを収集したうえでの追試が望まれる．今後の課題として，アンケートやその分析をより実社会に近い環境を想定して行い，エンドユーザの情報セキュリティ対策の提言まで高めていきたい．

5. おわりに

本研究では，情報セキュリティ技術に対する利用者の安心感の構造を明確化するため，質問紙を用いた調査実験を実施した．安心感要因として抽出された因子は，外的要因であるセキュリティ技術因子，ユーザビリティ因子，信用因子，および内的要因である経験因子，プリファランス因子，知識因子に分類できることを確認し，共分散構造分析を用いてその妥当性を示した．

今後は，継続的な調査実験を進めることで安心感を測定するための評価尺度の開発を行い，主観評価指標としての応用可能性について検討していきたい．同時に，安心感を提供することが，フィッシング詐欺のようなソーシャルエンジニアリングを駆使する犯罪に悪用される脅威について，対策を講じる必要がある．よって，本研究で得られた安心感要因を応用し，虚偽の安心を防ぐための技術についても検討する．

謝辞 本研究は，科学技術振興機構（JST）の戦略的国際科学技術協力推進事業の助成を受けている．本研究を進めるにあたり多大なるご指導をいただいた岩手県立大学の Basabi Chakraborty 助教授，瀬川典久講師，藤原康宏講師，サイバー大学の後藤幸功准教授，東京工科大学の宇田隆哉講師に感謝いたします．因子分析および共分散構造分析についてご指導をいただいた科学技術振興機構の山崎瑞紀氏，国立保健医療科学院の松村真木子氏，国立情報学研究所の岡田仁志助教授ならびに上田昌史助手に感謝いたします．また，本研究に際し有益なご助言をいただいた東京電機大学の佐々木良一教授ならびに応用セキュリティフォーラム（ASF）の皆様に感謝いたします．最後に，多数の有益なコメントをくださった匿名査読者，担当委員の方々に感謝の意を表します．

参考文献

1) 今井秀樹：暗号のおはなし［改訂版］，第 7 章 ヒューマンクリプトとは，日本規格協会 (2003).
2) 村上陽一郎：安全と安心の科学，集英社新書 (2005).
3) 飯塚重善，小川克彦：パブリックスペースにおける PC 利用環境の設計のための利用者広報距離による一考察，ヒューマンインタフェース学会論文誌，Vol.8, No.1, pp.69–75 (2006).
4) 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).
5) Dhamija, R., Tygar, J.D. and Hearst, M.: Why phishing works, *Proc. SIGCHI Conference on Human Factors in Computing Systems CHI'06*, pp.581–590 (2006).
6) 対馬伸行，杉野栄二，村山優子，宮崎正俊：認知–感情モデルに基づくセキュリティシステム評価法の提案，2004 年暗号と情報セキュリティシンポジウム（SCIS2004）予稿集，pp.7–11 (2004).
7) Murayama, Y., Hikage, N., Hauser, C., Chakraborty, B. and Segawa, N.: An Anshin Model for the Evaluation of the Sense of Security, *Proc. 39th Hawaii International Conference on System Science* (*HICSS'06*), Vol.8, p.205a (2006).
8) Lewis, J.D. and Weigert, A.: Trust as a Social Reality, *Social Forces*, Vol.63, No.4, pp.967–985 (1985).
9) McAllister, D.J.: Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations, *Academy of Management Journal*, Vol.38, No.1, pp.24–59 (1995).
10) Xiao, S. and Benbasat, I.: The formation of trust and distrust in recommendation agents in repeated interactions: a process-tracing analysis, *Proc. 5th International Conference on Electronic Commerce* (*ICEC'03*), pp.287–293 (2003).
11) 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.5, No.1–2, pp.181–207, Kluwer Academic Publishers (2004).
12) 山岸俊男：信頼の構造—こころと社会の進化ゲーム，東京大学出版会 (1998).
13) 南風原朝和，市川伸一，下山晴彦：心理学研究法入門，東京大学出版会 (2001).
14) 平田賢一：コンピュータ不安の概念と測定，愛知教育大学研究報告，Vol.39, pp.203–212 (1990).
15) Bailey, J.E. and Pearson, S.: Development of

a Tool for Measuring and Analyzing Computer User Satisfaction, *Manage. Sci.*, Vol.29, No.5, pp.530–545 (1983).
16) Baroudi, J.J. and Orlikowski, W.J.: A Short-Form Measure of User Information Satisfaction: A Psychometric Evaluation and Notes on Use, *Journal of Management Information Systems*, Vol.4, No.4, pp.44–58 (1988).
17) Doll, W.J. and Torkzadeh, G.: The measurement of end-user computing satisfaction, *Manage. Inf. Syst. Q*, Vol.12, No.2, pp.259–274 (1988).
18) Chin, J.P., Diehl, V.A. and Norman, K.L.: Development of an instrument measuring user satisfaction of the human-computer interface, *Proc. SIGCHI Conference on Human Factors in Computing Systems* (*CHI'88*), pp.213–218 (1988).
19) Kirakowski, J. and Corbett, M.: SUMI: The Software Measurement Inventory, *British Journal of Educational Technology*, Vol.24, pp.210–212 (1993).
20) Brooke, J.: SUS: A quick and dirty usability scale, *Usability Evaluation in Industry*, Jordan, P., Thomas, B., Weerdmeester, B. and McClelland, I. (Eds.), pp.189–194 (1996).
21) 酒井幸美，守川伸一，ハフシメッド，大橋智樹：原子力発電所に対する安心感の構造—「安心」のイメージに関する調査をもとに，原子力安全システム研究所 INSS JOURNAL，Vol.10, pp.10–21 (2003).
22) 飯塚重善，後藤雄亮，小川克彦：パブリックスペースでの情報利用時の安心度表現の試み，情報処理学会研究報告，Vol.2006, No.72, pp.63–70 (2006).
23) 高橋孝輔，仲谷美江，西田正吾：安心感を考慮した情報提示方法に向けて，ヒューマンインタフェースシンポジウム 2002 論文集，pp.289–292 (2002).
24) Nielsen, J.: *Usability Engineering*, Academic Press (1993).
25) 永井廉子，林知己夫：原子力発電に対する公衆の態度—態度の強度測定を中心にして，原子力安全システム研究所 INSS Journal，No.6, pp.24–54 (1999).
26) 日景奈津子，村山優子：安心感の定量的評価モデルに関する因子分析的検討，コンピュータセキュリティシンポジウム 2006（CSS2006）論文集，pp.191–196 (2006).
27) 山本嘉一郎，小野寺孝義：AMOS による共分散構造分析と解析事例［第 2 版］，ナカニシヤ出版 (2002).
28) 狩野　裕，三浦麻子：AMOS, EQS, CALIS によるグラフィカル多変量解析—目で見る共分散構造分析［増補版］，現代数学社 (2002).
29) 豊田秀樹：SAS による共分散構造分析，東京大学出版会 (1992).
30) Hoffman, L.J., Lawson-Jenkins, K. and Blum, J.: Trust beyond security: An expanded trust model, *Comm. ACM*, Vol.49, No.7, pp.94–101 (2006).
31) Slovic, P.: Perception of Risk, *Science*, pp.280–285 (1987).
32) 木村　浩，鈴木篤之：原子力の社会的受容に影響を与える因子の探索—東京都杉並区の調査結果，日本原子力学会和文論文誌，Vol.2, No.1, pp.68–75 (2003).

付　　録

A.1 実験で使用した質問紙の概要

「皆さんが普段パソコンや携帯電話を使って，インターネットで情報検索したり，何かのサービスやシステムを利用するにあたって，個人を特定する情報（あなたのお名前，住所，電話番号，銀行口座番号，クレジットカード番号等）を入力するような場面を想像してください．そのような場面で，実際にそのサービスを利用するかどうかを判断したり，情報を入力するときの「安心感」についてお聞きします．以下にあげる項目が，安心感の根拠や理由になっているかどうかについて，「まったくそうは思わない（1 点）」〜「非常にそう思う（7 点）」の 7 段階で，あなたのお気持ちに最もよくあてはまるところにそれぞれ 1 つずつ○をつけてください.」

(1) サービスを提供する事業主や会社自体を信頼している
(2) サービスを提供する事業主や会社は社会的信用がある
(3) サービスを提供する事業主や会社は確かな能力や実績がある
(4) サービスを提供する事業主や会社は利用者を裏切るはずはない
(5) サービスを提供する事業主や会社は善意に基づいている
(6) 大手の会社や事業主が提供するシステムやサービスは安心である
(7) 適切な個人情報管理対策が実施されている
(8) 入力した個人情報は適切に管理され，外部に漏洩することは決してない
(9) システムや技術そのものを信頼している
(10) 何かトラブルがあっても確実な保証がある
(11) 何かトラブルがあってもシステムが回復すれば

大丈夫だ
(12) 何かトラブルがあってもシステムが支援をしてくれる
(13) 安全性がきちんと確保されている
(14) 安全であることを実感できる
(15) 安全性対策には十分な配慮がなされている
(16) 自分はシステムの仕組みについてある程度理解している
(17) 自分はセキュリティ対策をしているので大丈夫だ
(18) 自分は情報技術についてよく知っているほうだ
(19) 自分はどんなリスクや脅威があるか理解をしたうえで利用している
(20) 適切な情報提示の仕方である
(21) システムのデザインに親しみが持てる
(22) システムのデザインが魅力的だ
(23) システムのデザインのレイアウトや色使いがきれいだ
(24) システムが使いやすい
(25) システムの操作性が優れている
(26) 操作方法の説明が丁寧で，親切な印象を受ける
(27) わずらわしい作業が少なく，簡単に利用できる
(28) ぱっと見て受けた印象で，説明や情報量が適切である
(29) いつも利用しているので使い慣れている
(30) いつも利用しているので経験上心配はない
(31) 自分の知人や家族が使っていたので，安心だ
(32) 具体的な根拠はないが，なんとなく安心だ
(33) 具体的な根拠はないが，何となく気に入っている
(34) 親切な対応やサービスに好感が持てる
(35) 自分の趣味や嗜好に合っている

(平成 18 年 12 月 7 日受付)
(平成 19 年 6 月 5 日採録)

日景奈津子（正会員）

平成 17 年岩手県立大学ソフトウェア情報学部卒業．平成 19 年同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．同年 4 月日本電信電話株式会社入社．現在，NTT 情報流通プラットフォーム研究所所属．在学中は情報セキュリティの心理学的側面からの研究に従事．2005 年 CSS2005 学生論文賞受賞．ACM 会員．

カール ハウザー

1980 年コーネル大学大学院博士課程修了．Ph.D. in Computer Science（コーネル大学）．IBM Research Laboratory，Xerox Palo Alto Research Center 勤務を経て，2001 年よりワシントン州立大学准教授．現在に至る．並列プログラミング，ネットワーク，プログラミング言語，分散コンピューティングシステムの研究に興味を持つ．現在はパワーグリットコミュニケーションの研究に従事．

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，ネットワークセキュリティの研究に従事．IEEE，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．