情報処理学会論文誌 Vol. 52 No. 9 2537–2548 (Sep. 2011)

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

加藤岳久[†1] 中澤優美子[†2] 漁田武雄[†3]
山田文康[†3] 山本匠[†1] 西垣正勝[†1]

大学での情報システムの導入が進んでいるが，それを利用する学生のセキュリティ教育は十分とはいえず，また学生自身はセキュリティ事故や被害に遭った経験も少ない．このため，学生のセキュリティ意識は高いとはいえず，大学の情報システムの安全性を担保するためには，企業等における情報システムと比べて，よりいっそうのセキュリティ対策が必要であると考えられる．そこで本研究では，セキュリティ事故の原因につながる末端ユーザ（学生）のセキュリティ意識と，セキュリティ意識を左右するユーザの性格に関して調査した．本論文では，セキュリティ対策の対象として本人認証技術を取り上げ，性格検査の結果とパスワード認証，持ち物認証，生体認証に関するセキュリティ意識の相関に対する 400 名程度の規模の調査を行ったので報告する．調査の結果，性格とセキュリティの意識との間にある程度の関係性が存在することが確認できた．

A Study on Correlation between User Disposition and Security Consciousness with Respect to User Authentication

Takehisa Kato,[†1] Yumiko Nakazawa,[†2]
Takeo Isarida,[†3] Fumiyasu Yamada,[†3]
Takumi Yamamoto[†3] and Masakatsu Nishigaki[†1]

Information systems have been commonly used in universities to support students in their study and campus life. In general, students don't receive adequate security education and have little experiences with security incidents. This means that the security consciousness of students is usually not high enough compared to company employees, and therefore security measures for the university information systems should be designed in consideration of this kind of students' inexpertness. This motivates us to study a connection between security consciousness (which is behind security incidents) and user disposition (which is behind their security consciousness) of students. This paper carries out user studies with about 400 university students to investigate on correlation between users' disposition and their security consciousness for user authentication such as password, token and biometrics.

1. 背　景

情報システムの導入なくして，情報資産やサービスの様々な運用管理を行うことが困難な時代になっている．企業だけでなく，大学でも情報システムの導入が進み，学生は各種証明書発行や履修状況の確認等，様々なサービスをオンラインや端末から利用することが可能になっている．非接触 IC カードの学生証による学内施設への入退室管理や，生体認証による講義の出欠管理等の運用も始まっている．最近では，学生に対するサービスの可用性向上の目的だけでなく，コスト削減や環境対策という面からも，大学における情報システムをクラウド・コンピューティング環境によって提供する大学も現れている[1)]．

企業等では，情報セキュリティ対策の導入に合わせ運用管理規程の制定や社員への教育の実施，セキュリティ監査等，Information Security Management System（ISMS：情報セキュリティマネジメントシステム）を導入し，セキュリティ対策が確実に運用されるよう社員個々のセキュリティ意識を高めセキュリティ事故を防いでいる．しかし，それでもなお，セキュリティ事故をなくすことはできていないというのが現実である．ましてや大学では，学生の多くが（企業における社員と比べて）十分なセキュリティ教育を受けておらず，セキュリティ事故や被害に関わった経験も少ないため，セキュリティ事故の発生確率は格段に高いと想像される．よって，学生が利用する情報システムにおいては，企業等の情報システムと比べてよりいっそうの安全性を高める工夫が必須だといえる．

†1 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University
†2 静岡大学情報学研究科
Graduate School of Informatics, Shizuoka University
†3 静岡大学情報学部
Faculty of Informatics, Shizuoka University

2. 関連研究と本研究の目的

2.1 関 連 研 究

情報システムの安全性を高めるためには，セキュリティ事故の原因を究明し，それに対して効果的な対策を実施していくことが肝要といえる．セキュリティ事故の原因を究明する研究に関しては，著者らの調べた限り，従来までに企業の社員等のセキュリティ教育および経験がある程度豊富であるユーザを対象とし，以下のような研究が展開されている．

NPO（Nonprofit Organization：特定非営利活動法人）日本ネットワークセキュリティ協会の報告では，個人情報漏えいインシデントの原因として，管理ミス，誤操作，紛失・置忘れが上位 85%以上を占め，ヒューマン・エラーが引き金になっているとある[2]．また大山らは，情報セキュリティに限らず，一般に事故の多くは，初期における情報摂取のあり方（危険源の見落とし）に関連し，この段階でのミスが被害を拡大するため，初期段階で危険を予知し回避することが重要であるとしている[3]．以上から，情報セキュリティ事故の多くの原因がヒューマン・エラーであり，初期段階における危険源の見落としを防ぐことが重要であることが分かる．

金らは，企業での情報セキュリティ事故の発生原因の 85%が社員によるものであり，かつ意図しないものであることから，企業の情報セキュリティ意識を企業と社員との戦略ゲームとして定式化している[4]．大和田らは，情報セキュリティ事故の原因の 1 つに，従業員のリスク認知意識の欠如からなる規則違反があげられ，教育によるリスク認知向上施策等，3 つの柱からなる情報セキュリティ対策モデルを提案している[5]．これらから，危険源の見落としによるセキュリティ事故を引き起こすのは末端のユーザであり，ヒューマン・エラーの原因としては，ユーザのセキュリティに関する知識とリスクに対するセキュリティ意識の低さによるところが小さくないことが分かる．

廣瀬は，性向のビッグファイブ（外向性，協調性，勤勉性，情緒安定性，知性）に，エラーを起こしやすい性格特性（いい加減さ，気の弱さ，軽率さ，自制心の弱さ，疲れやすさ）を加えた性格に関する設問と，エラーに関する設問の質問紙を用いた調査を行い，性格とヒューマン・エラーの相関について因子分析を行った[6]．その結果，エラー因子群と性格因子群との間で有意な相関が見られ，特に勤勉性の低さ，いい加減さ，軽率さで高い相関があったと報告している．また竹村は，労働者への Web 調査結果から，問題行動をとる労働者のセキュリティ意識が低いことを示し，情報セキュリティ教育への意識が高ければ，問題行動を起こしにくくなり，対策を遵守する可能性があるとしている[7]．これらから，セキュリティ事故の原因であるヒューマン・エラーを左右するのは末端ユーザのセキュリティ意識であり，そのセキュリティ意識とユーザの性格との間には，ある程度の相関が存在していることが分かる．

以上から，セキュリティ事故の原因は末端ユーザのヒューマン・エラーによるものが多く，それはユーザ個々人のセキュリティに関する知識や意識の低さによって引き起こされる傾向にあることが推測される．そして，ユーザのセキュリティ意識にはユーザの性格特性が関与し，勤勉性等が低いとセキュリティに関する知識や意識も低くなり，問題行動を起こしやすくなってセキュリティ事故の誘発につながる，ということが推測される．

2.2 本研究の目的

2.1 節で示した文献 6)，7) の調査は，企業等に勤める社員に対して実施されたものであり，すでにある程度のセキュリティ教育を受け，（ケーススタディを含めた）セキュリティ事故に関する経験もあるユーザが対象である．これに対し，情報セキュリティに関する教育やセキュリティ事故・被害等の経験が浅い大学生を対象とした場合に，ユーザの性格とセキュリティ意識との相関がどのような関係になるのか明らかにし把握することは重要であり，学生が利用する大学の情報システムの安全性を高めるうえで非常に有用となる．

そこで筆者らは先行調査[8),9)]において，情報セキュリティ教育や経験が少ないと考えられる大学 1 年生を対象に，性格とセキュリティ意識について，質問紙を用いた調査を行ってきている．著者らの調査では，セキュリティ意識の対象として本人認証を取り上げている．その理由は，情報システムでユーザが直接関与するセキュリティ対策の 1 つが本人認証であり，データの暗号化やファイアウォールによるパケットフィルタリング等のように組織が管理するシステムが機械的に実施する対策に比べ，パスワード管理の運用や IC カード等をつねに所持すること等に対する得手不得手といったユーザの意識が大きく関連するからである．

なお，質問紙を用いた調査では，回答者が社会的に望ましいとされる回答を選ぶという「社会的に望ましい回答の構え（Social desirability response set）」の発生が問題として指摘されている[10)]．すなわち，セキュリティ意識そのものを被験者に問う調査の場合，回答者に「他人に対して，自分が正しいセキュリティ対策をしていないと思われたくない」という自己防衛本能が働き，意図的または無意識的に回答を変化させる可能性がある．また，回答者の「本来，セキュリティ対策はこうあるべき」という潜在意識により，回答者が自覚しないレベルで自分の回答にバイアスをかける可能性が考えられる．このため本研究では，性格検査というニュートラルな質問紙を通じ間接的にセキュリティ意識を問うことでユーザのセキュリティ意識を調査するというアプローチを採り，セキュリティ意識に対するユーザ

の本心を測ることを目指す．

先行調査[8),9)]では，性格とパスワード認証に関するセキュリティ意識との関係について大学 1 年生 200 名程度の規模での調査を実施し，その分析結果を報告した．本論文では，調査の信頼性を高めるため，性格とパスワード認証に関するセキュリティ意識との相関に関して，さらに大学 1 年生 200 名程度に対する追調査を行い，両調査をあわせ計 400 名規模の分析結果を報告する．今回の追調査では，本人認証技術としてパスワード認証のほかに持ち物認証，生体認証に関する質問紙を用いた調査も同時に実施したので，その分析結果も報告する．また，持ち物認証，生体認証に対しては，経験・環境がセキュリティ意識にどのような影響を与えているのか考察を行った．

3. セキュリティ意識と性格の相関分析

先行調査[8),9)]とあわせ情報系学部の大学 1 年生 400 名程度の被験者を対象に，性格とパスワード認証に関するセキュリティ意識との相関の分析を行った．同時に，パスワード認証以外の本人認証技術として代表される持ち物認証，生体認証に関して情報系学部の大学一年生 200 名程度の調査を行った．

3.1 性格，経験，環境とセキュリティ意識の定義

先行調査[8),9)]を含め本研究では，性格，経験，環境，セキュリティ意識を以下のように定義する．本研究では，パスワード認証に関しては性格とセキュリティ意識との間の関係を，持ち物認証，生体認証に関しては性格・経験・環境とセキュリティ意識との間の関係を調査した．

【性格】性格は，神経質，のんき等，様々な要因から構成されていると考えられている[11)]．性格を構成する要因それぞれの影響力は個人ごとに異なり，それによって個性が形成されていると考えられる[12)]．利用者の性格については，利用者へ質問紙を用いた性格検査を実施し調査する．

【経験】本研究では，過去の体験から現在の自分自身に生かされている教訓（例：携帯電話の紛失）等を経験と定義する．利用者の経験については，利用者へ質問紙を用いた調査を実施し回答を得る．

【環境】サービスを受ける場所，利用限度金額，保障の有無等がこれに該当する．利用者の環境は，そのサービスを利用する利用形態を，利用者へ質問紙を用いた調査を実施し回答を得る．

【セキュリティ意識】利用者各個人における安全性への関心や各セキュリティ対策の嗜好と定義する．普段何文字のパスワードを利用しているか，生体認証の利用（生体情報の登録）に抵抗がないか等，具体的な質問項目による質問紙を用いて，利用者のセキュリティ意識を調査する．

3.2 調査方法と結果

今回の調査は，2008 年 12 月に実施された前回の調査[8)]と同じ環境で，2009 年 12 月に行った．被験者は本学情報学部 1 年次対象のある講義の受講生であり，講義時間内に質問紙を用いた調査を行った．その講義の科目名，教室，開講曜日・時間は前回の調査[8)]と同じであるが，前回の調査から 1 年が過ぎ，受講者（被験者）は入れ替わっている．被験者は 184 名（男性 113 名：女性 71 名，平均年齢 19.0 歳，標準偏差 1.1）に対して実施した．

今回の質問紙は，性格とパスワード認証に関するセキュリティ意識を問う質問に加え，持ち物認証および生体認証に関するセキュリティ意識についても質問した．性格とパスワード認証に関するセキュリティ意識を問う質問事項は，前回の調査と同じである．ただし今回の調査では，持ち物認証および生体認証に関するセキュリティ意識に対する質問を加えた分，質問総数が増加した．このため，被験者の集中力の持続の低下を避けるために，パスワード認証に関するセキュリティ意識を問う質問事項は，前回のものから一部の質問を割愛した．

結果の分析に関しては，性格とパスワード認証に関するセキュリティ意識の間の関係については前回の被験者 194 名（男性 124 名：女性 70 名，平均年齢 19.1 歳，標準偏差 1.0）と今回の被験者を合算し，不備回答等を除いた，373 名（男性 232 名：女性 141 名，平均年齢 19.0 歳，標準偏差 1.0）を 1 つの被験者集団として扱った．性格と持ち物認証に関するセキュリティ意識の間の関係，および，性格と生体認証に関するセキュリティ意識の間の関係については，今回の 184 名の被験者を対象として分析を行った．

今回の調査の流れを以下に示す．

STEP1　被験者に性格検査を受けてもらう．

STEP2　被験者に本人認証技術（パスワード認証・持ち物認証・生体認証）に関するセキュリティ意識の質問に回答してもらう．

STEP3　STEP1，STEP2 で得られた回答から，互いの相関値を求める．

STEP4　STEP2 で得られた各質問の回答値を被験者ごとに合算し，その値と STEP1 で得られた回答との相関値を求める．

STEP1 で用いる性格検査には，柳井らが開発した新性格検査[12)]を採用した．新性格検査は，性格の特性理論に基づき，性格の多面的特性を測定するものであり，12 の下位尺度と 1 つの虚構性尺度を含む，社会的外向性，活動性，共感性，進取性，持久性，規律性，自己

顕示性，攻撃性，非協調性，劣等感，神経質，抑うつ性，虚構性の 13 特性を，130 項目の質問（各特性 10 項目ずつ）を通じて点数化する．本調査では，この中から，虚構性尺度を除いた 12 特性に対し，因子負荷量の高かった 6 項目を抜粋したものを使用した（全 72 項目）．性格検査中，検査者は一定の速度で質問を読み上げ，被検査者に回答を促した．その後，被検査者には 15 分程度の回答時間が設けられ，セキュリティに関する質問を回答させた．質問の回答は，その場で検査者が回収した．

STEP2 では，本人認証技術における利用者のセキュリティ意識を測るために質問紙を用いた検査を行った．被験者は，パスワード認証，持ち物認証，生体認証の順番に回答を行う．本調査では，被験者が客観的に回答できるよう，事実だけを問う形の質問紙を多用するようにした．紙面の都合で質問の詳細は割愛するが，概要を以下に述べる．

■パスワード認証■

情報処理推進機構の発表する安全なパスワードを作成するための条件[13] を参考にして，以下の 3 つを基本項目とする計 9 項目を問うための質問紙を作成した．

p-1）パスワードを実際にどの程度適正に/安全に作成したか（パスワードの桁数，使用した文字種別の複雑さ，安全性を意識して作成したか，パスワードの強度を評価するツール等を使って安全性を確認したか）．

p-2）パスワードをどの程度正しく運用しているか（キャッシュ機能・メモを使うか，定期的に更新をしているか，更新する場合の更新期間はどの程度か）．

p-3）主観的に自分のパスワードを評価するとどの程度の強度か（使用しているパスワードの強度を自分で評価するとどの程度か）．

■持ち物認証■

持ち物認証では，持ち物は学生が日常生活において携帯し，かつ，決済の手段として利用可能な “学生証カード” を対象とし，そのカードの利用を問う質問事項を作成した．なお，本学の学生証カードは，希望する学生に対して，大学生協のポストペイ機能が付与できる．

同時に，“商用カード（クレジットカードやキャッシュカード）” の利用に関する項目も追加し，以下の 3 つを基本項目とする計 7 項目の質問を作成した．以降，持ち物認証の持ち物とはこれらのカードを指す．

t-1）持ち物をどの程度正しく運用しているか（学生証を置き忘れたとき心配になるか，学生証を人に貸すか，カードごとに暗証番号を使い分けているか）．

t-2）持ち物の安全性に対してどの程度配慮しているか（学生証を多機能にして利便性を上げたいか，カードを多く持つことを許容できるか）．

t-3）持ち物に対する許容はどの程度か（認証のためにいくつまで持ち物を携帯できるか，気に入った持ち物ならばいくつまで携帯できるか）．

■生体認証■

現時点では生体認証を ATM 等の実用の場で利用した経験を有する学生は少ないと推測し，質問紙の冒頭で生体認証の概略とそのメリットについて記述した．そのうえで，被験者が生体認証を使用する場面を仮定したときの心情について，以下の 2 つを基本項目とする計 5 項目の質問を作成した．今回は，対象を生体認証の分野で最も普及している指紋認証に限定した．

b-1）デメリットがあっても指紋認証を使いたいと思うか（グミ指等によるなりすましの脅威があっても使いたいか，日頃から指先の皮膚が荒れないように気を遣う必要があっても使いたいか，スキャナに対する指の置き方が悪い場合等は何度も指紋入力のやり直しを求められるが使いたいか）．

b-2）指紋認証に不安はないか（生体情報を外部へ提供することに抵抗があるか，安全性と利便性のどちらを重視したいか）．

STEP2 によって，各被験者が「各認証技術に対してどの程度のセキュリティ意識を持っているか」を表す指標（以下，実効度）が求められる．ここで，すべての質問項目が，利用者のセキュリティ意識が高いほど実行度が大きくなるような質問となっている．パスワードの桁数のように数量を問う形式の質問は，被験者の回答値をそのまま実効度の点数とした．数量を問う形式となっていない質問に対しては，数段階の評定による回答を求めるようにした．

STEP3 と STEP4 では，STEP1，STEP2 で得られた回答から，性格とセキュリティ意識の間の相関値を求める．STEP3 では，STEP2 のセキュリティ意識に関する質問紙における計 21 の質問事項を個別にとらえ，「パスワードの桁数，使用した文字種別の複雑さ，等の 21 の質問事項それぞれ（以下，セキュリティ意識要因）に対する被験者の回答」と「STEP1 の新性格検査から得られた被験者の 12 の性格特性」の関連を調べる．

これにより，被験者のパスワード認証に対するセキュリティ意識を構成する因子と性格特性との関係性を分析できる．

算出した相関値から性格特性を以下の 4 つに分類する．

① あるセキュリティ意識要因（質問事項）に対しては正の有意な相関を持ち，他の要因と負の相関を持たない性格特性

② あるセキュリティ意識要因に対しては負の有意な相関を持ち，他の要因と正の相関を

表 1　パスワード認証に関する各セキュリティ意識要因と各性格特性との相関分析結果*1
Table 1　Correlation analysis between user disposition and security consciousness (user behavior) for password authentication.

	社会的外向性	活動性	共感性	進取性	持久性	規律性	自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
パスワードの桁数	−0.10 †	−0.05	−0.05	−0.12 *	0.01	0.02	−0.03	−0.04	0.06	−0.02	0.11 *	0.04
使用した文字種別の複雑さ	0.02	0.01	−0.02	0.00	−0.01	0.02	0.02	0.08 †	0.03	−0.07	0.06	−0.11 *
安全性を意識して作成したか	0.07	0.09 †	0.01	−0.03	0.19 **	0.13 **	−0.03	−0.01 †	0.04	−0.07	0.05	0.03
評価ツールで安全性を確認したか	0.01	−0.03	−0.01	−0.05	0.02	0.10 †	−0.01	0.09 †	0.06	0.11 *	0.11 *	0.09 †
パスワードキャッシュ機能の利用	−0.01	0.02	−0.06	−0.02	0.04	0.02	−0.03	−0.06	−0.08	−0.01	0.06	−0.01
パスワードをメモに残すか	−0.02	−0.05	−0.09 †	0.01	−0.02	−0.06	−0.12 *	−0.11 †	−0.06	−0.04	−0.05	−0.03
定期的に更新しているか	0.16 **	0.11 *	0.00	0.04	0.12 *	0.17 **	0.05	−0.01	−0.07	−0.11 †	−0.11 †	−0.15 **
更新と答えた場合その更新期間は	0.02	−0.02	0.02	0.00	−0.08	−0.02	−0.04	−0.08	−0.01	0.03	0.06	0.03
強度を自己判定するとどの程度か	0.15 *	0.04	0.01	−0.01	0.04	0.11 *	0.06	−0.01	−0.01	−0.13 *	−0.04	−0.03

$^{**}p<.01$, $^{*}\ p<.05$, $^{\dagger}\ p<.10$

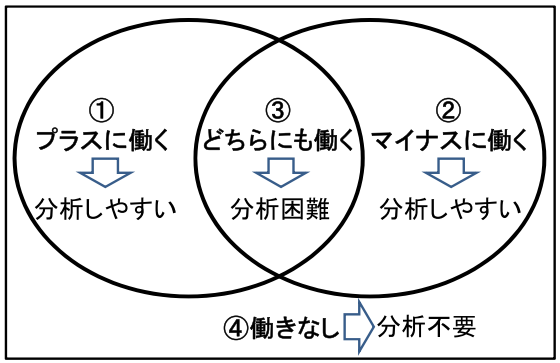


図 1　相関値から分類した性格特性
Fig. 1　Classification of user disposition with correlation analysis.

持たない性格特性

③ あるセキュリティ意識要因に対しては正の有意な相関を持ち，別の要因に対しては負の相関を持つ性格特性

④ どのセキュリティ意識要因とも有意な相関を持たない性格特性

①〜④ の関係を図示すると**図 1** のようになる．③ 群は，「あるセキュリティ意識要因に対してはプラスに作用し，別のセキュリティ意識要因に対してはマイナスに作用する」性格特性であり，各種認証方式に対する安全性を向上させるのか低下させるのかに関する考察が難しいと推測される．また ④ 群については，セキュリティ意識要因との関係が見出せない性格特性となる．そこで本論文では，これら 4 種類の性格特性のうち，① 群と ② 群とに焦点を当て，「どの性格特性」が「どのセキュリティ対策」に「どう影響するのか」を分析した．

STEP4 では，STEP2 のセキュリティ意識に関する質問紙における全質問事項の回答を合算して被験者のセキュリティ意識に関する総合点（以下，セキュリティ意識レベル）を求め，これと「STEP1 の新性格検査から得られた被験者の 12 の性格特性」との間の相関値を求める．これにより，被験者の各認証技術に対するセキュリティ意識の全体的な傾向と性格特性との関係性を分析する．なお，STEP2 の質問紙の全質問事項に対する総合点は，被験者の各質問事項に対する回答を標準化したうえで加算し算出する．

STEP3（各セキュリティ意識要因と各性格特性との相関値）と STEP4（セキュリティ意識レベルと各性格特性との相関値）における相関分析結果を，認証技術ごとに，それぞれ**表 1**，**表 2**，**表 3**，**表 4**，**表 5**，**表 6** に示す．相関値が正である性格特性は各セキュリティ意識要因・セキュリティ意識レベルに対してプラスに働く性格特性であり，その性格特性を

⋆1 表 1 について STEP3 では，相関値を質問ごとに独立して算出した．その際，未回答等の回答不備は分析から除いたため，質問ごとで被験者数にある程度の差異がある．また，「更新と答えた場合その更新頻度は」に関する質問では，「更新する」と回答した者のみが分析対象で，その数は 93 名であった．

表 2　パスワード認証に関するセキュリティ意識レベルと各性格特性との相関分析結果
Table 2　Correlation analysis between user disposition and security consciousness (consciousness level) for password authentication.

	社会的外向性	活動性	共感性	進取性	持久性	規律性	自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
セキュリティ意識レベル（パスワード）	0.12 *	0.07	−0.04	−0.03	0.12 *	0.17 **	−0.02	0.01	0.02	−0.09	0.03	−0.06

**p<.01 , * p<.05 , † p<.10

表 3　持ち物認証に関する各セキュリティ意識要因と各性格特性との相関分析結果*1
Table 3　Correlation analysis between user disposition and security consciousness (user behavior) for token authentication.

	社会的外向性	活動性	共感性	進取性	持久性	規律性	自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
学生証を置き忘れた時、どの程度心配になるか	−0.23 †	−0.22 †	−0.25 *	−0.07	−0.20	−0.11	−0.20	0.00	−0.06	0.09	0.22 †	0.14
学生証を人に貸すか	−0.28 *	0.15	−0.23 †	0.22 †	0.12	−0.06	0.15	0.28 *	0.10	−0.10	0.04	0.04
カードごとに暗証番号を使い分けているか	−0.08	0.12	−0.01	0.07	0.00	0.06	−0.04	−0.05	0.09	−0.04	0.20 *	0.03
学生証を多機能にして利便性を上げたいか	0.16	0.00	0.09	0.08	−0.09	0.07	−0.06	−0.12	0.08	0.04	0.09	−0.07
カードを多く持つことを許容できるか	−0.01	−0.09	−0.03	0.00	0.04	0.04	−0.10	0.16	0.03	0.17 †	0.13	0.19 †
認証のため追加で持ち物を持てるか	−0.22 †	0.11	0.10	0.13	0.29 *	0.05	0.03	0.14	0.21	0.05	0.12	0.21
気に入った持ち物ならばどの程度持てるか	0.01	0.05	0.27 *	0.12	0.22 †	−0.11	0.27 *	0.02	−0.01	−0.10	0.01	0.04

**p<.01 , * p<.05 , † p<.10

表 4　持ち物認証に関するセキュリティ意識レベルと各性格特性との相関分析結果*2
Table 4　Correlation analysis between user disposition and security consciousness (consciousness level) for token authentication.

	社会的外向性	活動性	共感性	進取性	持久性	規律性	自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
セキュリティ意識レベル（学生証）	−0.22	0.04	−0.02	0.15	0.12	−0.05	0.05	0.13	0.15	0.00	0.17	0.14

**p<.01 , * p<.05 , † p<.10

	社会的外向性	活動性	共感性	進取性	持久性	規律性	自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
セキュリティ意識レベル（カード）	−0.07	0.02	−0.02	0.06	0.03	0.07	−0.10	0.08	0.08	0.09	0.23 **	0.15 †

**p<.01 , * p<.05 , † p<.10

有する被験者はセキュリティ意識が高い傾向にあることを示す．相関値が負の性格特性は，その逆であり，セキュリティ意識にマイナスに働くことを示す．また，表 1〜6 においては，検定の結果，各セキュリティ意識要因と各性格特性の間に有意な相関（1%水準：相関値 p が 0.01 未満，5%水準：相関値 p が 0.05 未満，10%水準：相関値 p が 0.1 未満）が認められた項目も示した．

⋆1 表 3 について，学生証を決済の手段として頻繁に利用している者のみを対象としたため，学生証の調査に関する被験者数は 68 名であった．また，カードに関する質問は 2 枚以上所持していることを前提とし，該当者は 108 名であった．

⋆2 表 4 について，学生証に関する調査とカードに関する調査で被験者が異なるため，持ち物認証のセキュリティ意識レベル（合計点）は各々で算出している．

表 5　生体認証に関する各セキュリティ意識要因と各性格特性との相関分析結果
Table 5　Correlation analysis between user disposition and security consciousness (user behavior) for biometric authentication.

	社会的外向性	活動性	共感性	進取性	持久性	規律性	自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
なりすましの危険があっても生体認証を使うか	0.00	0.07	0.04	0.19 **	−0.04	0.01	0.14 †	0.05	0.15 *	−0.04	−0.07 *	0.07
認証精度のため手に気を使えるか	−0.02	0.04	0.11	0.05	0.16 *	0.12 †	0.11	−0.06	−0.07	−0.03	0.08	0.06
何度も入力し直すことがあっても良いか	−0.04	0.01	0.07	0.23 **	0.02	0.05	0.07	0.03	0.06	−0.01	0.01	0.14 †
生体情報を外部に提供することに抵抗があるか	0.03	−0.03	−0.03	−0.08	−0.04	0.07	−0.06	−0.05	0.02	0.04	0.13 †	−0.07
安全性と利便性どちらを優先するか	0.04	−0.03	−0.02	−0.17 *	0.07	0.06	−0.02	0.08	−0.07	0.00	0.12 †	0.02

**p<.01 , * p<.05 , † p<.10

表 6　生体認証に関するセキュリティ意識レベルと各性格特性との相関分析結果
Table 6　Correlation analysis between user disposition and security consciousness (consciousness level) for biometric authentication.

	社会的外向性	活動性	共感性	進取性	持久性	規律性	自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
セキュリティ意識レベル（生体認証）	0.01	0.02	0.06	0.07	0.06	0.11	0.08	0.01	0.03	−0.01	0.11	0.07

**p<.01 , * p<.05 , † p<.10

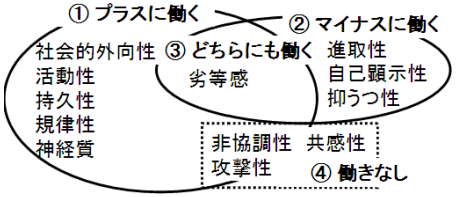


図 2　パスワード認証に関する各セキュリティ意識要因に影響を与える性格特性
Fig. 2　User disposition that will affect user's security consciousness for password authentication.

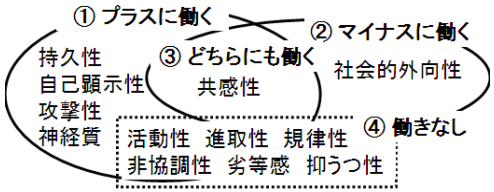


図 3　持ち物認証に関する各セキュリティ意識要因に影響を与える性格特性
Fig. 3　User disposition that will affect user's security consciousness for token authentication.

3.3 考　　察

3.3.1　STEP3 の考察

表 1，表 3，表 5 から，相関の数値は全体的に低く，性格特性とセキュリティ意識要因との間に十分な相関関係を見出すことは困難であるという結果であった．そこで，各セキュリティ意識要因との間に有意な相関（5%水準：相関値 p が 0.05 未満）が認められた性格特性を対象にして，3.2 節の ①〜④ 群の分類を行った結果を，認証技術ごとに**図 2**，**図 3**，**図 4** に示す．また，それぞれの ① 群と ② 群の性格特性に対し，性格特性とセキュリティ意識要因との間に相関が生じる理由を考察した．考察の中で，セキュリティ意識に対してプラスに働く性格特性を「○」で示しており，マイナスに働く性格特性は「●」で示す．なお，統計的な検定においては有意差が認められたとはいえ，これらの相関の数値自体は小さい．こ

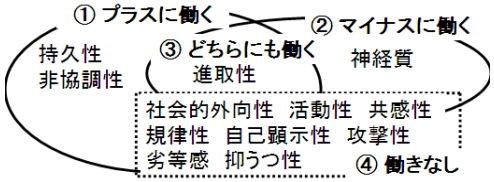


図 4　生体認証に関する各セキュリティ意識要因に影響を与える性格特性
Fig. 4　User disposition that will affect user's security consciousness for biometric authentication.

こでは，有意差が認められた項目は有意差が認められなかった項目よりは相関の傾向が強いのであろうという見通しに基づき，有意差が認められた項目に対して考察を行っているが，本項の考察を一般化するためにはさらなる検討が必要である．

■パスワード認証■

○規律性

規律性は，「安全性を意識してパスワードを作成したか」，「パスワードを定期的に更新しているか」の 2 項目と正の相関を示した．規律性が高いと自他に対する道徳的態度，安全性や一定の秩序・規則を守ろうとする傾向が強いことが知られている．このため，規律性の高い被験者は，安全なパスワードの作成・運用に対する項目と高い正の相関を示したと考えられる．

○神経質

神経質は，「パスワードの桁数」，「評価ツールでパスワードの安全性を確認したか」の 2 項目と正の相関を示した．神経質の度合いの高い者は，問題の細部を気にかけマニュアルを読む傾向にある[14]．このため，神経質の度合いの高い被験者は，安全性を確保するためのパスワードの作り方や運用法を自ら調べ，正しく理解していたと考えられる．

●抑うつ性

抑うつ性は，「パスワードに使用した文字種別の複雑さ」，「パスワードを定期的に更新しているか」の 2 項目と負の相関を示した．抑うつ性の高い人は，不安になりやすく，日常的に失敗を起こしやすい傾向にあることが知られている[15]．抑うつ性の高い人は，認証に失敗する恐れから，パスワードを比較的安易なものに設定したり，パスワードの変更を行わなかったりする傾向にあると考えられる．

■持ち物認証■

○自己顕示性

自己顕示性は，「気に入った持ち物ならばいくつまで持てるか」の 1 項目と正の相関を示した．自己顕示性の高さは，自身を際立って目立たせたい気持ちの強さを表している．そのため，自己顕示性の高い被験者は，好みに合う物は自らを際立たせてくれるので所持してもよいと思う傾向にあったと考えられる．

○神経質

神経質は，「カードごとに暗証番号を使い分けているか」の 1 項目と正の相関を示した．神経質の高い者は，日常生活の中で不安をいだきやすい傾向にある[16]．神経質の度合いの高い被験者は，万が一暗証番号の漏洩が生じたとき，すべてのカードで番号を同じにしたときに受ける被害の大きさを恐れ，使い分けを行っていると考えられる．

●社会的外向性

社会的外向性は，「学生証を人に貸すか」の 1 項目と負の相関を示した．社会的外向性の高い人は，対人接触を好み，人と広く付き合うことを楽しむ傾向が強い．このため，社会的外向性の高い被験者は，人と打ち解けやすいので自らの心を開きやすく，決済機能の付いたカードでも気軽に貸す傾向にあると考えられる．

■生体認証■

○持久性

持久性は，「認証精度のため日頃から指先の皮膚が荒れないように手に気を遣えるか」の 1 項目と正の相関を示した．持久性の高さは最後までやりとげたいという粘り強さを示す要因である．そのため，持久性の高い被験者は日常生活でも指先に気を遣うことができる傾向にあったと考えられる．

●神経質

神経質は，「グミ指等によるなりすましの危険があっても生体認証を使うか」の 1 項目と負の相関を示した．神経質の高い者は，日常生活の中で不安をいだきやすい傾向にある[16]．このため，神経質の度合いの高い被験者は情報漏洩に対する脅威を意識しやすいと考えられる．

また，「生体認証を外部に提供することに抵抗があるか」と正の有意性傾向（10%水準：相関値 p が 0.1 未満）が見受けられることから，神経質の高い者は，まだ一般的ではない生体認証に対して漠然とした不安を持っていると考えられる．

以上のように，各認証技術に関する各セキュリティ意識要因と特定の性格特性との間に，ある程度の関係性があることを確認できた．特定の性格特性を調査することで，利用者が利用するパスワードの桁数やその運用方法等，利用者のセキュリティ対策に対する行動をより詳細に推測できる可能性が示唆される．よって，利用者の特性を事前に測り利用者の行動を知ることが，ヒューマン・エラーを未然に防ぐことにつながると期待している．

3.3.2　STEP4 の考察

表 2，表 4，表 6 についても相関の数値は全体的に低いという結果であった．そこで 3.3.1 項と同様に，セキュリティ意識レベルとの間に有意な相違（5%水準：相関値 p が 0.05 未満）が認められた性格特性に対して考察を行う．ここにおいても，統計的な検定においては有意差が認められたとはいえ，これらの相関の数値自体は小さいため．本項の考察を一般化するためにはさらなる検討が必要である．

パスワード認証では，STEP3 の分析（セキュリティ意識要因と性格特性の相関）で得られた結果と同様に，セキュリティ意識レベルにおいても，社会的外向性と規律性と持久性の 3 つの性格特性との間に正の相関を示した．できることなら，簡潔な性格検査からユーザのセキュリティ意識が導き出せることが望ましい．今回の調査結果から，パスワード認証のセキュリティ意識レベルはこれらの 3 つの性格特性から測ることができる可能性が示唆される．

一方で，持ち物認証・生体認証においては，STEP3 の分析で何らかのセキュリティ意識要因との間に高い相関を示した性格特性であっても，すべてのセキュリティ意識要因を総合したセキュリティ意識レベルとの間では有意な相関がほとんど認められなかった．この理由を調査するためには，パスワード認証のように調査人数を拡大させ，各性格特性を構成する質問事項 1 問ずつとの詳細な相関分析を行う等のさらなる検討が必要であると考える．

4. パスワード認証に関するセキュリティ意識と性格の正準相関分析

3 章の相関分析より，パスワード認証に関するセキュリティ意識と性格との間に，（相関値そのものは低いが）ある程度の関係性があることが示唆された．本項では，この結果を補強するために，パスワード認証に関するセキュリティ意識と性格特性がどのように関係しているのかを，多変量解析の 1 つである正準相関分析によって解析する．

正準相関分析とは，2 群の相関が高くなるような重み付けを考え新たな変量を合成して作成する手法で，重回帰分析と主成分分析の応用例と考えられる[17]．重回帰分析は複数の説明変数（独立変数）を用いて単一の目的変数（従属変数）を表す推定式を作成するのに対して，正準相関分析では 2 つの変数群の関係を示す手法である．3.3.2 項では，各セキュリティ意識要因すべての合算値をセキュリティ意識レベルと定義付け，性格特性との相関をとることで関係性を調査した．本章では，複数あるセキュリティ意識要因の中のどのセキュリティ意識要因が，どの性格特性と関係があるのかを調査することで，より総合的な検討を行う．

パスワード認証に関するセキュリティ意識の質問項目は 9 項目であるが，本論文の正準相関分析においては，有効回答数の少ない項目を除いた 8 項目（**表 7**）を第 1 変数群として用いた．第 1 変数群の各変量を $x_1, x_2, \cdots, x_8$ とする．性格特性は，性格検査における 12 項目をそのまま第 2 変数群とした．第 2 変数群の各変量を $y_1, y_2, \cdots, y_{12}$ とする．

正準相関分析ツールによって，これら各組の変量の線形結合

$$X = a_1x_1 + a_2x_2 + \cdots + a_8x_8$$

$$Y = b_1y_1 + b_2y_2 + \cdots + b_{12}y_{12}$$

表 7　パスワード認証に関するセキュリティ意識と性格特性との正準相関分析結果（第 1 正準変量）
Table 7　Canonical analysis between user disposition and security consciousness for password authentication.

第1変数群（X）（パスワードに関するセキュリティ意識）	x_i	a_i	第2変数群（Y）（性格特性）	y_i	b_i
パスワードの桁数	x_1	−0.213	社会的外向性	y_1	0.683
使用した文字種別の複雑さ	x_2	−0.133	活動性	y_2	0.422
安全性を意識して作成したか	x_3	0.541	共感性	y_3	0.137
評価ツールで安全性を確認したか	x_4	0.179	進取性	y_4	0.160
パスワードキャッシュ機能の利用	x_5	0.137	持久性	y_5	0.523
パスワードをメモに残すか	x_6	−0.005	規律性	y_6	0.647
定期的に更新しているか	x_7	0.747	自己顕示性	y_7	0.166
強度を自己判定するとどの程度か	x_8	0.538	攻撃性	y_8	−0.098
			非協調性	y_9	−0.227
			劣等感	y_{10}	−0.357
			神経質	y_{11}	−0.368
			抑うつ性	y_{12}	−0.264
			正準相関係数		0.356

によって表される合成変量 X（パスワードに関するセキュリティ意識全体）および合成変量 Y（性格特性全体）との相互関係を計算した．正準相関分析の結果，危険率 5%水準で有意であったのは第 1 正準変量のみであった．今回は第 1 正準変量に対する解釈を行う．第 1 正準変量における各 x_i および各 y_i の相関値 a_i，b_i を表 7 に示す．

表 7 より，パスワードに関するセキュリティ意識（X）の第 1 正準変量の中で特に関連の高い変量（結合係数 a_i の値が大きい変量）は，「x_7：定期的に更新しているか」「x_3：安全性を意識して作成したか」「x_6：強度を自己判定するとどの程度か」の 3 つであることが分かる．3.2 節の STEP2 に関する説明で述べたように，今回のパスワードに関するセキュリティ意識を問う質問紙は 3 つの基本項目 p-1〜p-3 から作成されている．x_7，x_3，x_6 がそれぞれ p-2，p-1，p-3 に関する質問であることから，第 1 正準変量の主要因は質問全体を構成していると解釈できる．すなわち，パスワードに関するセキュリティ意識の第 1 正準変量は「パスワードに関するセキュリティ意識全体」を表していると考えられる．また，同じく表 7 より，性格特性（Y）の第 1 正準変量の中で特に関連の高い変量（結合係数 b_i の値が大きい変量）は，「y_1：社会的外向性」「y_6：規律性」「y_5：持久性」である．よって，

第 1 正準変量は，社会的外向性，規律性，持久性の 3 つの性格特性がパスワードに関するセキュリティ意識全体に深く関わっていることを示している．これは 3.3.2 項の相関分析で得られた結果と同様であり，この 3 つの性格特性からパスワード認証に関するセキュリティ意識の全体的な傾向を測定できるという結果を支持している．

5. 経験・環境がセキュリティ意識に与える影響の分析

今回の持ち物認証や生体認証に関する調査では，学生証カード，商用カード，生体認証に対する利用頻度が被験者ごとに大きく異なっていた．本研究では各セキュリティ対策を日常的に利用している利用者の当該セキュリティ対策に対する意識を調査することが目的であるため，学生証カードに対しては被験者を「群 1：学生証カードに決済機能が付いており，頻繁に利用する」，「群 2：学生証カードに決済機能が付いているがときどきしか利用しない」，「群 3：学生証カードに決済機能が付いていない」の 3 つの群に，商用カードに対しては被験者を「群 1：商用カードを 2 枚以上所有している」，「群 2：1 枚所有している」，「群 3：所有していない」の 3 つの群に，生体認証に対しては被験者を「群 1：生体認証を利用したことがある」，「群 2：利用したことがない」の 2 つの群に分類し，それぞれ群 1 の被験者のみを対象として 3 章（および 4 章）の分析を実施している．

本章では，3 章において対象外とした被験者群に対しても 3 章と同様の分析を実施し，3 章で得られた結果と比較することによって，群ごとにセキュリティ意識要因に違いがあるのか検証する．本論文では，本研究の第 1 段階として，利用者の「性格」とセキュリティ意識との関連を調査することを主目的としているが，上記のそれぞれの群の特性を比較することによって，「環境」（学生証を決済手段として使用しているか否か）や「経験」（生体認証の使用経験の有無）にセキュリティ意識がどのように依存しているのかに関する基礎的な知見を得ることができると考える．

■持ち物認証■

学生証カードに対しては，群 1（学生証カードに決済機能が付いており，頻繁に利用する），群 2（学生証カードに決済機能が付いているがときどきしか利用しない），群 3（学生証カードに決済機能が付いていない）の 3 つの群ごとに算出したセキュリティ意識レベルの平均値を**表 8** に示す．商用カードに対しては，群 1（商用カードを 2 枚以上所有している），群 2（1 枚所有している），群 3（所有していない）の 3 つの群ごとに算出したセキュリティ意識レベルの平均値を**表 9** に示す．なお，各質問事項において回答尺度が異なるため，被験者の回答を標準化したうえで平均値を算出している．

表 8　学生証カードの利用によって分類した各群のセキュリティ意識レベルの平均値
Table 8　Comparison of security consciousness according to types and frequency of use of student ID cards.

	決済機能有 頻繁に使用	決済機能有 時々使用	決済機能無
学生証を置き忘れた時、どの程度心配になるか	0.10	0.05	−0.13
学生証を人に貸すか	0.22	0.04	−0.24
学生証を多機能にして利便性を上げたいか	−0.14	0.04	0.10
認証のため追加で持ち物を持てるか	0.13	0.22	−0.27
気に入った持ち物ならば幾つまで持てるか	0.16	0.04	−0.18

表 9　商用カードの所持枚数によって分類した各群のセキュリティ意識レベルの平均値
Table 9　Comparison of security consciousness according to the number of credit cards possessed.

	2枚以上	1枚	0枚
カードを多く持つことを許容できるか	0.48	−0.82	−0.65

なお表 8 において，群 1 の被験者は 68 名，群 2 の被験者は 47 名，群 3 の被験者は 63 名であった．また表 9 において，群 1 の被験者は 108 名，群 2 の被験者は 54 名，群 3 の被験者は 15 名であった．

表 8 の結果から，学生証カードに関しては，決済機能の使用頻度にかかわらず，決済機能の付加された学生証カードを持つ被験者（群 1 と群 2）はセキュリティ意識が高くなっていることが分かる．金銭のやりとりが可能である持ち物となるため，自然と管理の重要性を認識できているのだと考えられる．

また，表 8 の決済機能のない学生証カードの被験者（群 3）や，表 9 の商用カードを所持していない被験者（群 3）を見ると，これらの群に属する被験者は，カードを所持したくない気持ちを強く持っていることが分かる．これより，現在，日常生活でカードを多用していない人は，今後もカードを持ちたくないと思う傾向にあると考えられる．

■生体認証■

生体認証に対しては，群 1（生体認証を利用したことがある），群 2（利用したことがない）の 2 つの群ごとのセキュリティ意識レベルの平均値を**表 10** に示す．なお表 10 において，群 1 の被験者は 151 名，群 2 の被験者は 26 名であった．

表 10 の結果から，生体認証の使用経験がある被験者（群 1）は，使用経験のない被験者（群 2）よりも生体認証を利用したい気持ちが強いことが分かる．これにより，過去に生体

表 10　生体認証の使用経験に関して分類した各群のセキュリティ意識レベルの平均値
Table 10　Comparison of security consciousness according to experiences in using biometric authentications.

	使用経験有	使用経験無
なりすましの危険があっても生体認証を使うか	0.64	−0.11
認証精度のため手に気を遣えるか	0.44	−0.08
何度も入力し直すことがあっても良いか	0.51	−0.09
生体情報を外部に提供することに抵抗があるか	−0.10	0.02
安全性と利便性どちらを優先するか	0.12	−0.02

認証の利点を実感したことがある人は，デメリットを提示されても使いたい気持ちを維持できる傾向にあると考えられる．以上のように，簡易な調査ではあったが，経験や環境がセキュリティ意識に影響を与えていることが確認できた．

6. ま と め

本論文では，ユーザの性格と本人認証技術（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に焦点を当て，先行調査[8),9)]とあわせ，パスワード認証に関しては大学 1 年生 400 名規模の，持ち物認証と生体認証に関しては大学 1 年生 200 名規模の調査を実施し，分析を行った．その結果，いくつかの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ある程度の関係性が存在することが確認できた．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唆された．

本論文は，本人認証技術における個人の性格とセキュリティ意識との関係を主に検証している段階である．今後は，被験者数をさらに拡大して分析精度を高めるとともに，経験や環境とセキュリティ意識の関係についても本格的な調査を行っていく予定である．そして，その成果を基に，大学における情報システムの安全性向上策の定式化を検討していく．

謝辞　岩手県立大学ソフトウェア情報学部村山優子先生，藤原康宏先生，及川ひとみ様，静岡大学情報学部竹内勇剛先生には研究指針に関する助言をいただいた．また，東海学院大学岡本香先生にはデータの解析に関する助言をいただいた．ここに深く謝意を表する．また，本研究は一部，（財）セコム科学技術振興財団の研究助成を受けた．

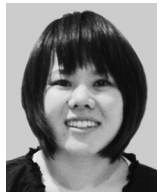
参 考 文 献

1) 静岡大学情報基盤センター：クラウドによる新情報基盤 SUCCES の紹介，静岡大学情報基盤センター広報，Vol.1 (2009).
2) セキュリティ被害調査ワーキンググループ：2009 年情報セキュリティインシデントに関する調査報告書，第 1.1 版，NPO 日本ネットワークセキュリティ協会 (2010.9).
3) 大山　正，丸山康則：ヒューマンエラーの科学，麗澤大学出版会 (2004).
4) 金　楨蘭，樋口　清：企業･組織内の情報セキュリティ意識に関する研究，(財) 情報通信学会第 27 回全国大会 (2010.6)，入手先⟨http://www.jotsugakkai.or.jp/doc/taikai2010/J4-3 Kim.pdf⟩（参照 2011-03-10）.
5) 大和田竜児，内田勝也：従業員のリスク行動に対する企業の取り組みモデルの提案，情報処理学会研究報告，2010-DPS-142(52), pp.1–81 (2010.2).
6) 廣瀬文子：ヒューマンエラー傾向測定手法作成の試み（その 1）—調査票作成ならびにエラーと性格特性に関する検討，（財）電力中央研究所研究報告書 (2007.4).
7) 竹村俊彦：Web アンケート調査データを用いた情報セキュリティ教育に対する意識と行動に関する分析，情報通信政策レビュー (2010.7)，入手先⟨http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/01/takemura2010.pdf⟩（参照 2011-03-10）.
8) 中澤優美子，西垣正勝：Best Match Security：性向とセキュリティ意識の相関に関する検討，情報処理学会研究報告，2008-CSEC-40, pp.43–48 (2008.3).
9) 中澤優美子，西垣正勝：Best Match Security：性向とパスワード認証のセキュリティ意識との相関に関する検討，情報処理学会研究報告，2008-CSEC-40, pp.43–48 (2009.3).
10) 岩脇三良：心理検査における反応の心理，日本文化科学社 (1973).
11) 辻岡美延：新性格検査法—YG 性格検査・応用・研究手引き，日本心理テスト研究所 (2000).
12) 柳井晴夫，柏木繁男，国生理枝子：プロマックス回転法による新性格検査の作成について（I），心理学研究，Vol.58, No.3, pp.158–165 (1987).
13) 情報処理推進機構：安全なパスワードにしよう—パスワードの心得，入手先⟨http://www.ipa.go.jp/security/personal/base/computer/point1.html⟩（参照 2010-05-09）.
14) 松尾太加志：どのような人がマニュアルを読むのか，日本心理学会第 67 回大会 (2003).
15) 大橋智樹，行場次朗，守川伸一：CFQ によって測定されるエラー傾向と性格特性の関連，日本産業組織心理学会第 16 回大会 (2000).
16) 田中　存，菅　千索：大学生活不安に関する心理学からのアプローチ，和歌山大学教育学部紀要，教育科学 (2007).
17) 林知乙夫：新版多変量解析，新版多変量解析，朝倉書店 (1985).

(平成 22 年 11 月 30 日受付)
(平成 23 年 6 月 3 日採録)

加藤　岳久（正会員）

1989 年信州大学工学部卒業．1991 年同大学大学院修了．同年株式会社東芝総合研究所入社．符号理論，情報セキュリティの研究に従事．2003 年より東芝ソリューション（株）にてネットワークセキュリティ，プライバシ保護の研究に従事．現在，同社技術統括部主任．静岡大学創造科学技術大学院にて情報セキュリティ研究に従事．



中澤優美子（正会員）

2008 年静岡大学情報学部情報科学科卒業．2010 年同大学大学院修士課程修了．在学中，情報セキュリティに関する研究に従事．

漁田　武雄（正会員）

1973 年横浜国立大学教育学部小学校教員養成課程卒業．1975 年広島大学大学院教育学研究科修士課程修了．1976 年同大学院教育学研究科博士課程後期中退．1976 年広島大学教育学部学部助手，1980 年国立特殊教育総合研究所精神薄弱研究部重度精神薄弱教育研究室研究員，1982 年静岡大学教養部講師，1983 年静岡大学教養部助教授，1995 年静岡大学情報学部教授．博士（文学）．人間の記憶の文脈依存機構の解明に関する研究に従事．

山田　文康（正会員）

1972 年東京工業大学工学部社会工学科卒業．1974 年同大学大学院修士課程修了．日本能率協会総合研究所客員研究員を経て，1981 年大学入試センター研究部助手．同助教授の後，1995 年静岡大学情報学部教授．修士（工学）．データ科学，質的多変量データ解析，文系学生に対する統計教育，アンケートにおけるデータの信頼性・妥当性に関する研究等に従事．

山本　　匠（正会員）

2006 年静岡大学情報学部情報科学科卒業．2007 年 9 月同大学大学院修士課程修了．2010 年 9 月同創造科学技術大学院博士課程修了．日本学術振興会特別研究員（DC1），同研究員（PD）を経て，2011 年 4 月三菱電機株式会社情報技術総合研究所入社．在学中，情報セキュリティに関する研究に従事．

西垣　正勝（正会員）

1990 年静岡大学工学部光電機械工学科卒業．1992 年同大学大学院修士課程修了．1995 年同大学院博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．同講師，助教授の後，2006 年より同創造科学技術大学院助教授．2007 年同准教授，2010 年同教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シミュレーション等に関する研究に従事．