Vol.2010-DPS-142 No.21
Vol.2010-CSEC-48 No.21
2010/3/4

Best Match Security
ー性格と本人認証技術のセキュリティ意識との相関に関する検討ー

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

セキュリティ意識やサービスの利用環境がユーザごとに異なるため，サービスプロバイダにより提供される画一的なセキュリティ対策ではその効果が十分に発揮されないことも多い．この問題に対し，著者らは，ユーザの性格，経験，環境などの要因を基に個人毎に好適なセキュリティ対策を策定するシステムの実現を目指している．本稿では，性格検査の結果と各種本人認証技術（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相関に対する 400 名程度の規模の調査を行い，その結果を報告する

Best Match Security
ーA study on correlation between preference disposition and security consciousness about user authenticationー

Yumiko Nakazawa[†]　Takehisa Kato[††]　Takeo Isarida[†††]
Humiyasu Yamada[†††]　Takumi Yamamoto[††††]
Masakatsu Nishigaki[††††]

The service providers are supplying security countermeasures to users. Because of different considerations towards security and environment for the usage of services among individual users, however, those measures do not always make sufficient effect and are not always useful. As for this problem, we propose to construct a knowledge-based system to recommend the most suitable security countermeasures to each user based on his/her individual disposition, experience and environment. This paper investigates on correlation between users' preference disposition and their security consciousness about user authentication such as password, token and biometrics.

1. 背景

今や情報マネジメントは各組織にとっての最重要課題の一つと認識されている．しかし，その一方で，ISMS（情報セキュリティマネジメントシステム）に関する規定を設けるだけでは事故が減らず，組織内の運用に問題があることが調査によって明らかになってきている．例えば，Verizon Business 社が発表した企業の情報流出事件に関する実態調査報告書[1]では，情報が流出した企業のうち，59%はセキュリティポリシと手順を定めておきながら実行していなかったとの報告がある．また，情報漏洩の 87%は適切な対策を講じれば防止できたと指摘している．これは，情報を利用する上で情報マネジメントの機能や運用だけでなく，システムを利用するユーザの人間性も考慮する必要性を裏付ける結果である．

ところが，既存の IT サービスにおいては，すべてのユーザに対して一律で同じセキュリティ対策（例えば，Web ページや携帯電話におけるパスワード認証や生体認証等）が講じられていることが多い．このような「サービスプロバイダから提供される一元的なセキュリティ対策」では，IT サービスの安全性を確保する上で期待される効果が得られていない可能性がある．

そこで筆者らは，ユーザ個々の性格，経験，環境を考慮した上で好適なセキュリティ対策を決定するシステムを提案している[2]．システムを実現するための第一歩として，まずは性格と本人認証技術に焦点を当て，性格と本人認証技術に関するセキュリティ意識との関係を質問紙により調査を行っている．文献[4][5]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 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．本稿では，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更に 200 名程度に対する追調査を行い，両調査を併せ計 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他に持ち物認証，生体認証に関する質問紙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．

2. 提案方式

2.1 コンセプト

例えば，面倒くさがり屋や利便性を最優先する人は，必要最低限とされるセキュリ

† 静岡大学情報学研究科，Graduate School of Informatics, Shizuoka University
†† 東芝ソリューション(株)，TOSHIBA Solutions Corporation
††† 静岡大学情報学部，Faculty of Informatics, Shizuoka University
†††† 静岡大学創造科学技術大学院，Graduate School of Science and Technology, Shizuoka University

Vol.2010-DPS-142 No.21
Vol.2010-CSEC-48 No.21
2010/3/4

ティ対策以外は設定を無効にしていると推測される．また，過去に携帯電話の紛失などの失敗や苦い経験を持つユーザや，もともと心配性のユーザは，不安を解消するために使いづらいが厳重なセキュリティ対策を施しているだろう．このように，経験や性格に応じ，ユーザが各セキュリティ対策の強度をどの程度に設定し，どの様に利用するかが異なると考えられる．また，システムの使用環境や扱う情報の価値からも，セキュリティ対策は影響を受けると予想される．

以上から，セキュリティ意識と性格との相関を調べ，ユーザごとの性格，経験，環境を入力することによって，当該ユーザのセキュリティ対策に対する実効度を得ることができると考えられる．これをシステムとして実装した場合の概観を図 1 に示す．

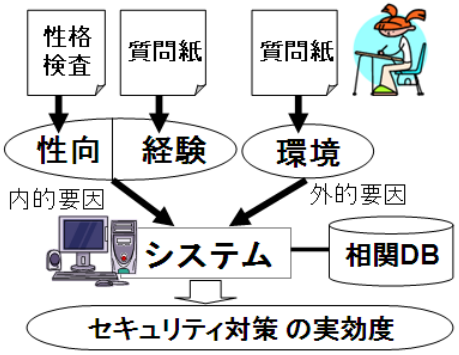

図 1. 提案システムの概観

本システムでは，ユーザを類別する指標として「性格」，「経験」，「環境」の 3 つを用いる．また，ユーザの安全性への関心度や各セキュリティ対策の嗜好を客観的に表す指標として「セキュリティ意識」を用いる．これらの指標に関しては質問紙によるアンケート等をユーザに実施することでデータを収集する．相関 DB は，性格，経験，環境とセキュリティ意識との間の相関（例えば，「几帳面な人はパスワードを適切に管理する傾向にある」，「大雑把な人はパスワードを覚えるより持ち物認証を好む傾向にある」など）に関する知識を集約し，これをデータベース化したものである．

システムは，性格検査や質問紙などによるアンケート調査の結果から得られるユーザの情報（性格，経験，環境）を受け取り，相関 DB と照合・分析を行うことによって，ユーザ個人の各セキュリティ対策における実効度を提示する．ここで実効度とは，例えばパスワード認証においては，乱数性の高いパスワードを設定しているか，十分な長さのパスワードを設定しているか，定期的にパスワードを更新しているかなどの，それぞれのセキュリティ対策をユーザがどの程度正しく運用しているか／運用できると予想されるかを示す度合いである．

セキュリティ対策の実効度を考慮することで，ユーザのニーズや嗜好に合致したセキュリティ対策を決定することができると考えられる．すなわち，ユーザごとに最も高い実効度が望めるセキュリティ対策を見つけて採用してやることにより，ユーザが不便を感じてセキュリティ設定をオフにしたり，セキュリティ機能を不適切に運用したりするという「セキュリティ対策における理想と現実の乖離」が抑えられ，IT 社会のセキュリティレベルが底上げされると期待できる．

2.2 相関DB

本研究では，ユーザを内的要因（性格，経験）および外的要因（環境）に着目して類別する．相関 DB の構築に対しては，事前に多数のユーザに対して性格，経験，環境とセキュリティ意識に関する大規模な調査を行い，そこから要因間の相関関係を抽出し，これを体系化する．以下に，性格，経験，環境，セキュリティ意識に関して説明する．

【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[6]．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[7]．ユーザの性格は性格検査によって調査する．

【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），等を経験として定義する．ユーザの経験は，ユーザに質問紙を実施することにより回答を得る．

【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．ユーザの環境は，そのサービスを利用するにあたっての利用形態をユーザに回答してもらうことによって調査する．

【セキュリティ意識】 ユーザ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，などの質問を通じてユーザから収集する．

3. 調査

提案システムを実現するためには，相関 DB の構築が重要である．そこで，本稿では，提案システムの要ともいえる相関 DB の実現可能性を確認する．

本研究の先行調査[4][5]では，性格に焦点を当て，パスワード認証に関するセキュリティ意識と性格との関係性について 200 名規模の調査を行った．その結果，セキュリティ意識と特定の性格との間にある程度の関係性を確認することができた．

本稿では，性格とパスワード認証に関するセキュリティ意識との相関に関して新たに 200 名規模の追調査を実施し，前回の調査結果と併せ 400 名程度の被験者を対象とした分析を行った．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 200 名程度の調査を行った．

Vol.2010-DPS-142 No.21
Vol.2010-CSEC-48 No.21
2010/3/4

3.1 調査方法

今回の調査は，前回の調査[5]と同じ環境で実施した．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[5]と同じであるが，前回の調査から 1 年が過ぎているため，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問うている．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項目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，質問総数が増加してしまったため，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項目について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と今回の調査の結果を合算して，373 名（男性 232 名 : 女性 141 名，平均年齢 19.0 歳，標準偏差 1.0）を一つ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[8]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により回収された．

STEP2 では，本人認証技術におけるユーザ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[12]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．

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などを使って安全性を確認したか)
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，更新する場合更新期間はどの程度か）
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　■

持ち物認証に関しては，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a”の利用を問う質問事項を作成した．同時に，“カード（クレジットカード・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．

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時心配になる程度は，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）
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）
3）持ち物に対する許容はどの程度か（認証のために追加で持ち物をどのくらい持てるか，また気に入った持ち物ならばどのくらい持てるか）

■　生体認証　■

現時点では生体認証を ATM などの実用の場で利用した経験を有する被験者は少ないと推測したため，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上で，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．

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

a 本学の学生証は、希望する学生は、大学生協のポストペイ機能を付けることが可能である。

Vol.2010-DPS-142 No.21
Vol.2010-CSEC-48 No.21
2010/3/4

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など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）

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）

桁数や個数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．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．

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捉え，「パスワードの桁数，使用した文字種別の複雑さ，・・・などの 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することができる．

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 一つ以上のセキュリティ意識要因（質問事項）と正の相関があり，どの要因とも負の相関がない性格特性

② 一つ以上のセキュリティ意識要因と負の相関があり，どの要因とも正の相関がない性格特性

③ あるセキュリティ意識要因に対しては正の相関を持つが他の要因と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

これら 4 種類の性格特性のうち，本稿ではセキュリティ意識要因への影響が明確な①群と②群に焦点を当て，「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から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ことができる．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上で加算することによって算出する．

3.2 調査結果

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 1~6 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．

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b

	社会的外向性	活動性	共感性	進取性	持久性	規律性
パスワードの桁数	−.10 †	−.05	−.05	−.12 *	.01	.02
使用した文字種別の複雑さ	.02	.01	−.02	.00	−.01	.02
安全性を意識して作成したか	.07	.09 †	.01	−.03	.19 **	.13 **
評価ツールで安全性を確認したか	.01	−.03	−.01	−.05	.02	.10 †
パスワードキャッシュ機能の利用	−.01	.02	−.06	−.02	.04	.02
パスワードをメモに残すか	−.02	−.05	−.09 †	.01	−.02	−.06
定期的に更新しているか	.16 **	.11 *	.00	.04	.12 *	.17 **
更新と答えた場合その更新期間は	.02	−.02	.02	.00	−.08	−.02
強度を自己判定するとどの程度か	.15 *	.04	.01	−.01	.04	.11 *

**p<.01 , * p<.05 , † p<.10

自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
−.03	−.04	.06	−.02	.11 *	.04
.02	.08 †	.03	−.07	.06	−.11 *
−.03	−.01 †	.04	−.07	.05	.03
−.01	.09 †	.06	.11 *	.11 *	.09 †
−.03	−.06	−.08	−.01	.06	−.01
−.12 *	−.11 †	−.06	−.04	−.05	−.03
.05	−.01	−.07	−.11 †	−.11 †	−.15 **
−.04	−.08	−.01	.03	.06	.03
.06	−.01	−.01	−.13 *	−.04	−.03

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

	社会的外向性	活動性	共感性	進取性	持久性	規律性
セキュリティ意識レベル（パスワード）	.12 *	.07	−.04	−.03	.12 *	.17 **

**p<.01 , * p<.05 , † p<.10

自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
−.02	.01	.02	−.09	.03	−.06

b STEP3 では，相関値を質問ごとに独立して算出している．その際，未回答などの回答不備について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」に関する質問においては，「更新する」と回答した者のみが分析の対象であり，その数は 93 名であった．

Vol.2010-DPS-142 No.21
Vol.2010-CSEC-48 No.21
2010/3/4

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c

	社会的外向性	活動性	共感性	進取性	持久性	規律性
学生証を置き忘れた時、どの程度心配になるか	−.23 †	−.22 †	−.25 *	−.07	−.20	−.11
学生証を人に貸すか	−.28 *	.15	−.23 †	.22 †	.12	−.06
カードごとに暗証番号を使い分けているか	−.08	.12	−.01	.07	.00	.06
学生証を多機能にして利便性を上げたいか	.16	.00	.09	.08	−.09	.07
カードを多く持つことを許容できるか	−.01	−.09	−.03	.00	.04	.04
認証のため追加で持ち物を持てるか	−.22 †	.11	.10	.13	.29 *	.05
気に入った持ち物ならば幾つまで持てるか	.01	.05	.27 *	.12	.22 †	−.11

**p<.01 , * p<.05 , † p<.10

自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
−.20	.00	−.06	.09	.22 †	.14
.15	.28 *	.10	−.10	.04	.04
−.04	−.05	.09	−.04	.20 *	.03
−.06	−.12	.08	.04	.09	−.07
−.10	.16	.03	.17 †	.13	.19 †
.03	.14	.21	.05	.12	.21
.27 *	.02	−.01	−.10	.01	.04

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d

	社会的外向性	活動性	共感性	進取性	持久性	規律性
セキュリティ意識レベル（学生証）	−.22	.04	−.02	.15	.12	−.05

**p<.01 , * p<.05 , † p<.10

自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
.05	.13	.15	.00	.17	.14

	社会的外向性	活動性	共感性	進取性	持久性	規律性
セキュリティ意識レベル（カード）	−.07	.02	−.02	.06	.03	.07

**p<.01 , * p<.05 , † p<.10

自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
−.10	.08	.08	.09	.23 **	.15 †

c 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 人であった．また，カードに関する質問は 2 枚以上所持していることが前提であり，該当者は 108 人であった．

d 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

	社会的外向性	活動性	共感性	進取性	持久性	規律性
なりすましの危険があっても生体認証を使うか	.00	.07	.04	.19 **	−.04	.01
認証精度のため手に気を遣えるか	−.02	.04	.11	.05	.16 *	.12 †
何度も入力し直すことがあっても良いか	−.04	.01	.07	.23 **	.02	.05
生体情報を外部に提供することに抵抗があるか	.03	−.03	−.03	−.08	−.04	.07
安全性と利便性どちらを優先するか	.04	−.03	−.02	−.17 *	.07	.06

**p<.01 , * p<.05 , † p<.10

自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
.14 †	.05	.15 *	−.04	−.07 *	.07
.11	−.06	−.07	−.03	.08	.06
.07	.03	.06	−.01	.01	.14 †
−.06	−.05	.02	.04	.13 †	−.07
−.02	.08	−.07	.00	.12 †	.02

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

	社会的外向性	活動性	共感性	進取性	持久性	規律性
セキュリティ意識レベル（生体認証）	.01	.02	.06	.07	.06	.11

**p<.01 , * p<.05 , † p<.10

自己顕示性	攻撃性	非協調性	劣等感	神経質	抑うつ性
.08	.01	.03	−.01	.11	.07

3.3 考察

3.3.1 STEP3 の考察

表 1，表 3，表 5 から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（5%水準：p の値が 0.05 未満）が認められた性格特性を対象にして，3.1 節の①～④群の分類を行った結果を，認証技術ごとに図 2~4 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．

■　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・きまりを守ろうとする傾向が強いことが知られている．

Vol.2010-DPS-142 No.21
Vol.2010-CSEC-48 No.21
2010/3/4

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[10]．このため，神経質の高い被験者は，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のではないかと考えられる．

●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[11]．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のではないかと考えられる．

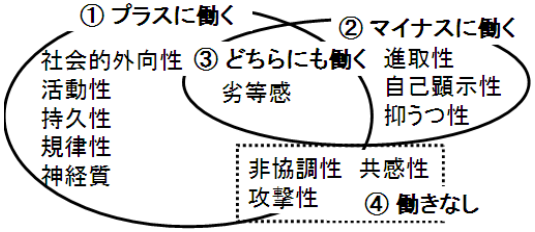

図 2：パスワード認証に関する各セキュリティ意識要因に影響を与える性格特性

■　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幾つまで持てるか」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わしている．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良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抱きやすい傾向にある[13]．神経質の高い被験者は，万が一暗証番号の漏洩が生じた時，全てのカードで番号を同じにした時に受ける被害の大きさを恐れ，使い分けを行っているのではないかと考えられる．

●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，例え決済機能の付いたカードでも気軽に貸す傾向にあるのではないかと考えられる．

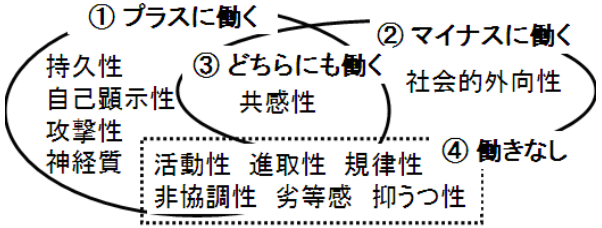

図 3：持ち物認証に関する各セキュリティ意識要因に影響を与える性格特性

■　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遂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抱きやすい傾向にある[12]．このため，神経質の高い被験者は情報漏洩に対する脅威を意識しやすいのではないか考えられる．

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：p の値が 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があるのではないかと考えられる．

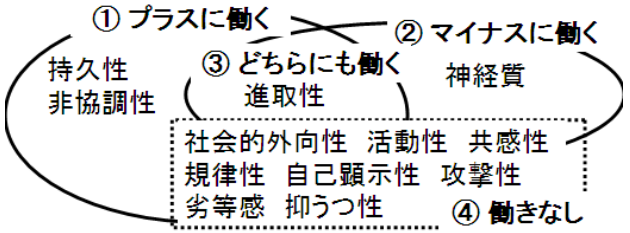

図 4：生体認証に関する各セキュリティ意識要因に影響を与える性格特性

Vol.2010-DPS-142 No.21
Vol.2010-CSEC-48 No.21
2010/3/4

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，ユーザが利用するパスワードの桁数やその運用方法など，ユーザ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，提案システムを用いてユーザの特性を測ることで，事前にユーザの行動を知ることができ，ヒューマンエラーを未然に防ぐことができると期待している．

3.3.2 STEP4 の考察

表 2，表 4，表 6 の中からセキュリティ意識レベルと各性格特性の間に有意な相違（5%水準：p の値が 0.05 未満）が認められた性格特性に対して考察を行う．

パスワード認証においては，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．提案システムにおいては，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などのさらなる検討が必要であると考える．

3.4 経験・環境がセキュリティ意識に与える影響

提案システムを構築するためには，セキュリティ対策を日常的に利用しているユーザの当該セキュリティ対策に対する意識を調査し，データベース化したい．しかし，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，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.そこで,学生証に対しては被験者を「群 1：学生証に決済機能がついており，頻繁に利用する，群 2：学生証に決済機能が付いているが時々しか利用しない，群 3：学生証に決済機能が付いていない」の 3 つの群に，カードに対しては被験者を「群 1：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 3.3 節の分析が実施されている．

本節では，3.3 節において対象外とした被験者群に対しても 3.3 節の STEP2 と同様の分析を実施し，3.3 節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．これによって，セキュリティ意識が経験や環境に依存しているのか否かに関する知見を得ることができる．

■ 持ち物認証 ■

学生証に対しては被験者を「群 1：学生証に決済機能がついており，頻繁に利用する，群 2：学生証に決済機能が付いているが時々しか利用しない，群 3：学生証に決済機能が付いていない」の 3 つの群に分類した．群ごとに算出したセキュリティ意識要因の平均値を表 7 に示す．また，カードに対しては被験者を「群 1：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 つの群に分類した．群ごとに算出したセキュリティ意識要因の平均値を表 8 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上で平均値を算出した．

表 7：学生証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[e]

	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 8：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[f]

	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

表 7 の結果から，学生証に関しては，決済機能の使用頻度に係わらず，決済機能の付加された学生証を持つ被験者（群 1 と群 2 の被験者）はセキュリティ意識が高くなっていることが分かる．金銭のやり取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 7 の決済機能無の被験者（群 3）や，表 8 の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，持ち物（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，日常生活で持ち物を多用していない人は，今後も持ち物を持ちたくないと思う傾向にあると考えられる．

e 群 1 の被験者は 68 人，群 2 の被験者は 47 人，群 3 の被験者は 63 人であった．
f 群 1 の被験者は 108 人，群 2 の被験者は 54 人，群 3 の被験者は 15 人であった．

Vol.2010-DPS-142 No.21
Vol.2010-CSEC-48 No.21
2010/3/4

■ 生体認証 ■

生体認証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 つの群に分類した．各群に対するセキュリティ意識レベルの平均値を表 9 に示す.

表 9: 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**g**

	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

表 9 の結果から，生体認証の使用経験がある被験者（群 1）は，使用経験の無い被験者（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.

4. まとめ

本研究は，性格，経験，環境の 3 要因を基に，個人に最も適したセキュリティ対策を提示するシステムの実現を目指すものである．本稿では，提案システムの実現可能性を検討するために，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）に関するセキュリティ意識との相関に焦点を当て，パスワード認証に関しては 400 人規模の, 持ち物認証と生体認証に関しては 200 人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関係性が存在することを確認することができた．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．今後は，調査範囲を拡大させ，持ち物認証や生体認証の利用に関するセキュリティ意識と性格との関係性を再調査する予定である.

g 群 1 の被験者は 151 人，群 2 の被験者は 26 人であった.

謝辞 今回の研究にあたり，岩手県立大学ソフトウェア情報学部 村山優子教授，藤原康宏講師, 及川ひとみ様, 静岡大学情報学部 竹内勇剛准教授には研究指針に関する助言を頂いた．また, 東海学院大学 岡本香助教にはデータの解析に関する助言を頂いた．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) Verizon Business，2008 Data Breach Investigations Report, http://www.verizonbusiness.com/resources/security/databreachreport.pdf.
2) 中澤優美子，加藤岳久，漁田武雄，山田文康，西垣正勝，Best Match Security－個人に適したセキュリティ対策を講じるシステムの提案－, 情報処理学会研究報告, 2008-CSEC-42, pp.251-258 (2008.7)
3) 辻井重男，笠原正雄 編著，情報セキュリティー暗号・認証・倫理までー，昭晃堂(2003)
4) 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)
5) 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)
6) 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)
7) 大村政男，図解雑学 心理学，ナツメ社 (1999)
8) 国生理枝子, 柳井晴夫, 柏木繁男, 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，pp158-165 (1987)
9) 杉浦幸，田中純夫，山田泰行，中学生の反応的攻撃性の変動要因，順天堂大学スポーツ健康科学研究，No.11，pp. 21-30(2007)
10) 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)
11) 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)
12) 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～, http://www.ipa.go.jp/security/personal/base/computer/point1.html
13) 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)