社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－DPS－138 (8)
2009－CSEC－ 44 (8)
2009／3／5

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－

中澤 優美子[1] 加藤 岳久[2] 漁田 武雄[3] 山田 文康[3] 山本 匠[4,5] 西垣 正勝[4,6]

[1]静岡大学大学院情報学研究科 〒432-8011 浜松市中区城北 3-5-1
[2]東芝ソリューション(株) 〒183-8512 東京都府中市片町 3-22
[3]静岡大学情報学部 〒432-8011 浜松市中区城北 3-5-1
[4]静岡大学創造科学技術大学院 〒432-8011 浜松市中区城北 3-5-1
[5]日本学術振興会特別研究員 DC
[6]独立行政法人科学技術振興機構，CREST
E-mail: [1]gs08051@s.inf.shizuoka.ac.jp, [2]Kato.Takehisa@toshiba-sol.co.jp, [4]nisigaki@inf.shizuoka.ac.jp

あらまし 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，ユーザの性向，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，性格検査の結果と個人のパスワード認証に関するセキュリティ意識の相関に対する 200 名程度の規模の調査を行い，その結果を報告する．
キーワード セキュリティマネジメント，セキュリティ対策，パスワード認証，性格検査

Best Match Security

－A study on correlation between preference disposition and security consciousness about password authentication－

Yumiko NAKAZAWA[1] Takehisa KATO[2] Takeo ISARIDA[3] Humiyasu YAMADA[3]
Takumi YAMAMOTO[4,5] Masakatsu NISHIGAKI[4,6]

[1]Graduate School of Informatics, Shizuoka University
[2]TOSHIBA Solutions Corporation
[3]Faculty of Informatics, Shizuoka University
[4]Graduate School of Science and Technology, Shizuoka University
[5]Research Fellow of the Japan Society for the Promotion of Science
[6]Japan Science Technology and Agency, CREST
Email: [1]gs08051@s.inf.shizuoka.ac.jp, [2]Kato.Takehisa@toshiba-sol.co.jp, [4]nisigaki@inf.shizuoka.ac.jp

Abstract 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 focuses on users' preference disposition and investigates its relation with their security consciousness about password authentication.
Keyword security management, security measures, password authentication, personality test

1. 背景

近年，不正アクセスやコンピュータウイルス，情報漏洩などが多発し，企業の情報管理に対する関心が急速に高まっている．ISMS（情報セキュリティマネジメントシステム）認証を受ける組織が増加し，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．

その一方で，ISMS に対応した規定を設けても事故が減らず，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た．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ー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，ユーザ個々の性向，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[3]．また，システムを実現するための第一歩として，性向に焦点を当て，複数の本人認証技術（PIN 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ついての調査報告を行っている[4]．しかし，文献[4]では，被験者が 11 名と少なく，セキュリティ意識に影響を与えると仮定した性向の妥当性も不明瞭であった．

そこで，本稿では，調査規模を 200 名程度に拡大し，性向とセキュリティ意識との相関に関して再調査を行った結果を報告する．また，より詳細な分析を行うために，本稿では，本人認証技術をパスワード認証に絞り，性向とセキュリティ意識との関係の妥当性について分析を行った．

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，経験や性向に応じ，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．

なお，本稿では，本人の好みや気質，各個人が持つ経験に伴う行動や思考によって特徴づけられる類似的な傾向を性向と呼ぶ．

以上から，セキュリティ意識と性向との相関を調べ，ユーザごとの性向，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．

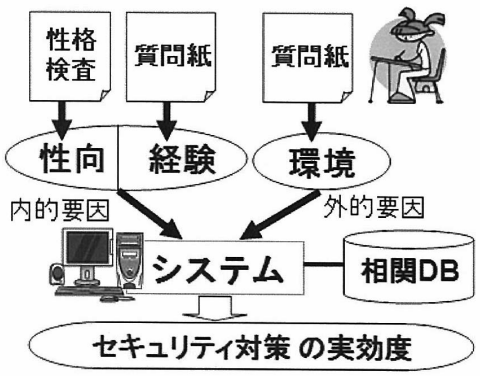

図 1. 提案システムの概観

本システムでは，ユーザを類別する指標として「性向」，「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，性向，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（性向，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（性向，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向，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，性向，経験，環境，セキュリティ意識に関して説明する．

【性向】 性向は，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[5]．性向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[6]．ユーザの性向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，ユーザにアンケート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．

2.3 相関 DB の利用

相関 DB は，「どのような性向，経験，環境」のユーザが「どのようなセキュリティ対策」を「どのように感じ」，「どのように使用しているのか」という知識のデータベースである．また，これを分析することにより，ユーザのタイプごとに間違いやすい失敗や陥りやすいトラブルを類型化することもできるだろう．

また，年代ごと・職業ごとなど，特定フィールドに属するユーザごとの特性が分かれば，企業の製品サービスが「セキュリティ対策としては何を採用すれば消費者に受け入れられるのか」を推定できるようになる．

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]では，ユーザの内的要因に含まれる性向にのみ焦点を当て，「持ち物認証」「PIN 認証（パスワード認証）」「生体認証」の各々の本人認証技術に関するセキュリティ意識と性向との関係性について分析した．その結果，セキュリティ意識と特定の性向との間にある程度の関係性を確認することができた．しかし，先行調査[4]では，被験者が 11 名と少なく，セキュリティ意識に影響を与えると仮定した性向の妥当性も不明瞭であった．

そこで，本稿では，被験者を 194 人と拡大させ，性向とセキュリティ意識との相関に関して再調査を行った．また，より詳細な分析を行うために，本人認証技術をパスワード認証に絞り，性向とセキュリティ意識との関係の妥当性について分析を行った．

3.1 調査方法

本調査は本学情報学部学生 194 名（男性 124 名：女性 70 名，平均年齢 19.1 歳，標準偏差 1.0）に対して実施した．調査は，情報学部 1 年次対象の講義時間内に実施した．本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 被験者にパスワード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[7]を採用した．新性格検査は，性向の特性理論に基づき，性向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，パスワード利用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．紙面の都合で質問の詳細は割愛するが，パスワード利用状況に関するアンケート調査[11]を参考にして以下の 5 つを基本項目とする計 15 項目を問うための質問紙を作成した．STEP2 によって，各被験者が「パスワード認証に関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，すなわち実効度が求められる．

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) セキュリティに影響を与えると思うパスワード桁数はどの程度か（理想とされる／不安に感じるパスワード桁数はどの程度か）

3) パスワードをどの程度正しく運用しているか（パスワードを再利用しているか，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）

4) パスワード認証をどの程度利用しているか（PC／携帯において，パスワード機能をどの程度有効にしているか（例えばPCの場合，OSパスワード・メーラ・スクリーンセーバー等，認証を設定している個数を示す））

5) 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）

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．本調査では純粋な意識調査を行うために，経験や性向に起因する側面をできるだけ排除し，客観的になるよう，事実だけを問う形のアンケートを作成した．項目5)のみ，自分のパスワードの強度に対する主観的評価を問うている．

STEP3とSTEP4では，STEP1，STEP2で得られた回答から，性向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15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15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の性向特性」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向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向特性を以下の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向特性

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向特性

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向特性

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向特性

これら4種類の性向特性のうち，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，「どの性向特性」が「パスワード認証におけるどの対策に」「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の性向特性」との間の相関値を求める．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の全体的な傾向と性向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こととした．

3.2 調査結果

STEP3（各セキュリティ意識要因と各性向特性との相関値）とSTEP4（セキュリティ意識レベルと各性向特性との相関値）における相関分析結果をそれぞれ表1, 2に示す．相関値が正である性向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向特性であり，その性向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．相関値が負の性向特性は，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．

3.3 考察

3.3.1 STEP3の考察

表1の中から各セキュリティ意識要因と各性向特性の間に有意な相関（5%水準）が認められた性向特性を対象にして，3.1節の①～④群の分類を行った結果を図2に示す．

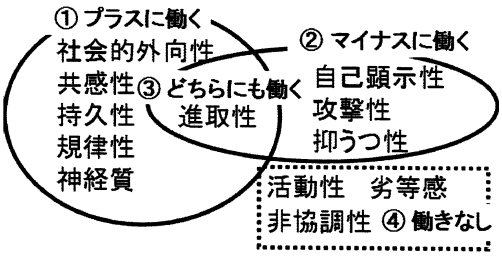

図2：パスワード認証に関する各セキュリティ意識要因に影響を与える性向特性

以下では，①群と②群の性向特性に対し，性向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．

① セキュリティ意識に対してプラスに働く性向特性

●持久性

持久性は，「安全性を意識して作成したか」・「認証機能の利用範囲（携帯）」・「認証機能の利用範囲（PC+携帯）」の3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多くの場面で安全なパスワードを設定している傾向にあったと考えられる．

●規律性

規律性は，「安全性を意識して作成したか」・「定期的に更新しているか」・「強度を自己判定するとどの程度か」の3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．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・運用および自己評価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，「理想と思われるパスワード長」・「不安に感じるパスワード長」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[9]．このため，神経質の高い被験者は，安全性を確保するには十分なパスワード長が必要であることを自ら調べ，正しく理解していたのではないかと考えられる．

②セキュリティ意識に対してマイナスに働く性向特性

●攻撃性

攻撃性は，「不安に感じるパスワード長」と負の相関を示し，同時に，「パスワードの桁数」・「安全性を意識して作成したか」・「定期的に更新しているか」に対しても負の有意性傾向が示されている．高い攻撃性を有する者は物事の判断が自己中心的になることが知られている[8]．このため，一般的に安全だと言われるパスワード長や運用方法を無視して，自分にとって都合の良いパスワード長や運用方法を選択してしまう傾向にあるのではないかと考えられる．

●抑うつ性

抑うつ性は，「使用した文字種別の複雑さ」・「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[10]．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．

以上のように，パスワード認証に関する各セキュリティ意識要因と特定の性向特性との間に，ある程度の関係性があることを確認できた．

特定の性向特性を調査することで，ユーザが利用するパスワードや運用方法など，ユーザのパスワード認証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．

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向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	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	−.02	−.02	−.02	−.19 *	.06	.09	−.04	−.13 †	.08	.02	.12	.07
使用した文字種別の複雑さ	−.04	−.04	−.12	−.02	−.03	.03	.01	−.02	.11	−.10	.06	−.15 *
安全性を意識して作成したか	.07	.09	.01	−.05	.25 **	.26 **	−.03	−.13 †	.08	−.08	.03	.00
評価ツールで安全性を確認したか	.03	−.04	−.06	−.07	.01	.07	−.03	.05	.07	.13 †	.14 †	.13 †
理想と思われるパスワード長	.06	.13 †	.04	−.03	.02	.10	−.08	−.04	.01	−.05	.14 *	.08
不安に感じるパスワード長	−.12	−.02	−.03	−.10	.05	.05	−.06	−.15 *	.03	−.01	.12	.09
パスワードを再利用するか	.15 *	.11	.08	.03	.03	.11	−.01	.06	.05	.02	.06	−.03
パスワードキャッシュ機能の利用	.01	.10	−.08	.12	.13 †	.10	.05	−.04	−.09	−.09	.07	−.04
パスワードをメモに残すか	−.04	−.08	−.11	.00	.01	−.05	−.15 *	−.07	−.05	.00	−.01	.00
定期的に更新しているか	.22 **	.06	.06	−.03	.13 †	.20 **	.00	−.12 †	−.11	−.14 †	−.11	−.20 **
更新と答えた場合その更新期間は	.06	.20	−.16	.36 *	−.19	−.15	.09	−.07	.01	.03	.04	−.06
認証機能の利用範囲(PC)	.03	.03	.25 **	−.04	.07	.07	.03	.00	.01	.04	.12	.09
認証機能の利用範囲(携帯)	.06	.06	.24 **	.06	.20 *	.05	−.04	−.10	−.04	−.09	.07	.02
認証機能の利用範囲(PC+携帯)	.07	.07	.33 **	.03	.21 *	.08	−.02	−.09	−.03	−.05	.12	.06
強度を自己判定するとどの程度か	.19 *	.00	.01	−.08	.09	.17 *	.05	−.04	.12	−.03	.00	.08

** $p<.01$, * $p<.05$, † $p<.10$

☆ STEP3では，相関値を質問ごとに独立に算出している．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，質問ごと被験者数に差異がある．例えば「更新・期間」に関する質問においては、「更新」に関する質問に対して「更新する」と回答した者のみが分析の対象となるため，被験者数は37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向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	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（総合点）	.09	.07	.02	−.10	.15 *	.18 *	−.01	−.15 *	.09	−.10	.09	.00

** p<.01 , * p<.05 , † p<.10

3.3.2 STEP4 の考察

表 2 の中からセキュリティ意識レベルと各性向特性の間に有意な相違（5%水準）が認められた性向特性に対して考察を行う．

STEP3 の分析（セキュリティ意識要因と性向特性の相関）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，規律性と持久性の 2 つの性向特性との間に正の相関を示し，攻撃性との間に負の相関を示した．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，セキュリティ意識レベルはこれらの 3 つの性向特性から測ることができる可能性が示唆される．

一方で，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向特性であっても，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には有意な相関が認められない性向特性が多々存在する．この理由を調査するためには，各セキュリティ意識要因間の因子分析を行うことによってセキュリティ意識レベルを構成する下位概念を探るなどのさらなる検討が必要であると考える．

4. まとめ

本研究は，性向，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，性向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焦点を当て，調査と分析を行った．194 名のデータを基に相関分析を行った結果，いくつかの性向特性とパスワード認証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．今後は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向との関係性を調査する予定である．

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しての助言を頂いた．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] 情報処理推進機構，2007 年度第 1 回情報セキュリティに関する脅威に対する意識調査報告書，http://www.ipa.go.jp/security/fy19/reports/ishiki01/documents/200701_ishiki.pdf

[3] 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)

[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] 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）

[6] 大村政男，図解雑学 心理学，ナツメ社（1999）

[7] 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）

[8] 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）

[9] 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）

[10] 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向特性の関連，日本産業組織心理学会第 16 回大会（2000）

[11] Dinei Florencio and Cormac Herley・Microsoft Research・One Microsoft Way・Redmond, WA , LargeScale Study of Web Password Habits，Proceedings of the 16th international conference on the World Wide Web , pp.657-666（2007）