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

2008－DPS－134 (8)
2008－CSEC－ 40 (8)
2008／3／6

Best Match Security：性向とセキュリティ意識の相関に関する検討

中澤 優美子[†] 西垣 正勝[††, †††]
[†]静岡大学情報学部 〒432-8011 浜松市中区城北 3-5-1
[††]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
[†††]独立行政法人科学技術振興機構, CREST
Email: [††]nisigaki@inf.shizuoka.ac.jp

あらまし 電子マネーなど高機能なITサービスの普及に伴い，セキュリティ対策の重要性は益々高まっている．サービスプロバイダは個別にセキュリティ対策を講じているが，セキュリティに対する意識や考え方はユーザによって異なるため，期待されるような効果が得られていないという現実がある．そこで本研究では，性向，経験，環境といった要因を基に，個人ごとに最も適したセキュリティ対策を自動的に策定するシステムの実現を目指す．本稿では，その第一歩として性向に焦点を当て，各種認証方式に対するセキュリティ意識との関係性を調査する．

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，セキュリティ意識，性向，性格検査

Best Match Security: A study on correlation between preference disposition and security consciousness

Yumiko NAKAZAWA[†] Masakatsu NISHIGAKI[††, †††]
[†]Faculty of Informatics, Shizuoka University
[††]Graduate School of Science and Technology, Shizuoka University
[†††]Japan Science Technology and Agency, CREST
Email: [††]nisigaki@inf.shizuoka.ac.jp

Abstract The importance of security measures become gradually increasing with the spread of services on the Internet. Although the service providers are supplying security countermeasures to users, those measures do not make sufficient effect because of different consideration and attitude towards security among individuals. Here in this paper, 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. As the first step, this paper focuses on users' preference disposition and investigates its relation with their security consciousness.

Keyword security management, security measures, security consciousness, preference disposition, personality test

1. はじめに

近年，電子マネー，オンラインショッピング，インターネットバンキングなどITサービスの高機能化に伴い，セキュリティ対策の重要性が高まっている．現在までのところ，ITサービスの安全性を確保するために，あるサービスを利用する全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．しかし，セキュリティに対する意識や考え方はユーザによって大きく異なるため，サービスプロバイダから一方的に提供される一元的なセキュリティ対策では期待されるような効果が得られていないという現実がある．

実際，パスワードの忘却を恐れ，自分の誕生日など安易なパスワードを設定しているユーザは少なくない[1]．面倒くさがり屋や利便性を最優先するユーザは，必要最低限のセキュリティ対策以外は設定を無効にしているだろう．これらは，提供されたセキュリティ対策の実効力をユーザ自身が低下させている例である．また，逆に，過去に失敗や苦い経験（携帯電話の紛失など）を持つユーザや心配性のユーザは，不安を解消するために，使い難くても構わない

ので厳重なセキュリティ対策を望むかもしれない．これらは，提供されているセキュリティ対策の実効力にユーザが満足していない例である．

このように，各個人が持つ経験や，思考や行動によって特徴づけられる性向（類型的な性質の傾向）に応じ，ユーザがどのセキュリティ対策の利用を選択するか，そして，それらのセキュリティ強度をどの程度に設定するかが異なってくると考えられる．また，それらは，システムの使用環境や扱う情報の価値からも影響を受けると予想される．

以上より，全ユーザの安全を確保するには，ユーザの適性やセキュリティ意識など様々な要因を考慮し，一人ひとりに適した対策を講じることが肝要であることが分かる．そこで本研究では，性向，経験，環境といった要因を基に，個人ごとに最も適したセキュリティ対策を自動的に策定するシステムを実現することを最終目標とする．本稿では，提案する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，持ち物認証，PIN認証，生体認証の利用に関するセキュリティ意識との関係性を調査する．

2. 提案方式

2.1 コンセプト

提案システムの概観を図1に示す．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．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．

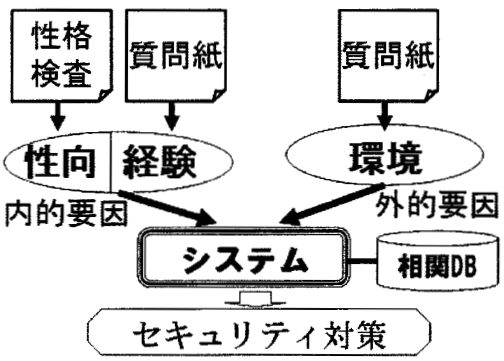

図１：提案方式の概観

システムは，性格検査や質問紙などを用いユーザの情報（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，ユーザ個人に最も適したセキュリティ対策を提示する．ユーザのニーズや嗜好に合致したセキュリティ対策が示されるため，ユーザが不便を感じてセキュリティ設定をあえてオフにしたり，セキュリティ機能を不適切に運用するというような「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

2.2.1 相関DBの作成

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[2]．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[3]．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，サービスに対するアプリケーションの習熟度（例：タイピング）等を経験として定義する．似通った性向を持つ者同士でも，対象（サービス）によって経験が異なるため，安全性への関心が変わってくると予想される．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，利用限度額，保障の有無等がこれに該当する．ユーザの置かれた状況が安全か危険か，脅威が発生した際の被害の大きさ等によって心理的不安が変化し，ユーザの安全性への関心が変動すると考えられる．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度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，利便性と安全性のどちらに重きを置いているか，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．

2.2.2 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．

相関DBが完成すれば，この相関DBを利用して，ユーザごとに適したセキュリティ対策を決定することが可能となる．その具体的な手順は以下のとおりである．(1) ユーザは，あるサービスの利用を開始する前に，2.2.1節で示したものと同型の性格検査や質問紙を用い，自分の性向や経験，そのサービスの環境（利用形態）をシステムに入力する．(2) システムは，相関DBを利用することによって，そのようなタイプのユーザがそのサービスを利用する際のセキュリティ意識を知ることができる．(3) システムは，そのようなセキュリティ意識を有するユーザに適したセキュリティ対策を選定し，ユーザに提示する．

3. 調査

提案方式を実現するためには，相関DBの作成が非常に重要である．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．ここではその第一段階として，まずはユーザの性向にのみ焦点をあて，持ち物認証、PIN認証、生体認証の利用に関するセキュリティ意識との相関について調査した．

3.1 調査方法

本調査には，情報セキュリティの研究に従事している大学生11名（男性9名：女性2名，平均年齢23.2歳，標準偏差1.5）に参加してもらった．

性格検査および質問紙を用いて調査実験を実施した．以下に調査の流れを示す．

【STEP-1】 被験者に性格検査を受けてもらう．
【STEP-2】 被験者にセキュリティ意識に対する質問に回答してもらう．
【STEP-3】 アンケート結果に対してクラスタ分析を行うことにより、セキュリティ意識の似ている被験者をグルーピングする．
【STEP-4】 クラスタごとに性向特性の平均と分散を求め，セキュリティ意識の似ている被験者に共通する性向を調べることにより、セキュリティ意識と成功の関係を分析する．

【STEP-1】で用いる性格検査には，柳井らが開発した新性格検査[4]を採用した．本検査は，性格の特性理論に基づき，性格の多面的特性を測定するための検査である．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．

【STEP-2】では，携帯電話に適応可能なセキュリティ対策として，今回は「持ち物認証」，「PIN認証」，「生体認証」の3種類の本人認証技術に着目して調査を行った．各対策案についての意識を測るため，23項目からなる質問紙を作成した．紙面の都合で質問項目を列記することはできないが，各認証方式に対する以下の4つの観点からの質問となっている．

1) 家の鍵，携帯電話，ATMの認証として利用したいか．
2) 許容できる負荷の限度（暗証番号の桁数や所持する認証トークンの個数）．
3) 各認証方式に関連した実際の利用状況（推測困難な暗証番号を設定するようにしているか，普段所持しているものを机の上に放置することはないか等）．ただし，生体認証を実際に利用している被験者が少なかったため，生体認証に対しては「使用する際，利便性・安全性のどちらを重視するのか」等といった関心を尋ねる質問とした．
4) それらの認証を使用するにあたって心理的不安はないか。

桁数や個数を問う形式となっていない質問に対しては，7段階の評定による回答を求めるようにした．

【STEP-3】では，【STEP-2】で得た被験者11人分の回答に対し，ウォード法 によるクラスタ分析を行い，セキュリティ意識が似ている被験者ごとに分類する．ここで，クラスタ分析とは，対象の持つ数値から対象間の距離（結合距離）を考え，距離の遠近により対象を分類する手法である[5]．ウォード法は，クラスタ分析手法の中で最も使われている手法であり，クラスタ内の分散を最小にする[6]．なお，今回は被験者が少数のため，男女を区別せずに分析を行った．分類されたクラスタごとに，クラスタ内の被験者に共通するセキュリティ意識（【STEP-2】の質問に対する回答）に関する傾向を調べた．

【STEP-4】では，【STEP-3】で分類されたクラスタごとに，【STEP-1】により得られた13の性向特性に対するクラスタ内の被験者の平均値と分散値を算出した．クラスタ内の平均値が被験者全体の平均値とかけ離れており，かつ，クラスタ内の分散が被験

者全体の分散よりも小さい性向特性を各クラスタの特徴的な性向として抽出する。これにより、セキュリティ意識の似ている被験者に共通する性向が抽出できるので、これを利用して「どういうタイプの被験者」が「どういうセキュリティ意識」を有しているか考察する.

3.2 調査結果

【STEP-3】で行ったクラスタ化の結果を図2に示す. 今回は, 結合距離を指標として, 図2の破線の位置でクラスタに分類した[7]. 結果的に, 「持ち物認証」は5つのクラスタ (C_{a1}〜C_{a5}), 「PIN認証」も5つのクラスタ (C_{b1}〜C_{b5}), 「生体認証」については4つのクラスタ (C_{c1}〜C_{c4}) が生成された. 分類されたクラスタごとに, 被験者のセキュリティ意識 (【STEP-2】の質問に対する回答) を目視で分析し, 各クラスタ内の被験者に共通するセキュリティ意識を「各クラスタに属する被験者のセキュリティ意識に関する傾向 (項目A) 」として抽出した.

続いて, 【STEP-4】で求めた13の性向特性のクラスタごとの平均を図3, 図4, 図5に示す (紙面の都合上, 分散に関する結果は割愛する) . 図の縦軸は各々の性向特性の強さを表しており, 値が大きいほどその特性が強いことを示す. この中から, クラスタ内の平均値が被験者全体の平均値とかけ離れており, かつ, クラスタ内の分散が被験者全体の分散よりも小さい性向特性を「各クラスタに属する被験者の性向に関する特徴 (項目B) 」として抽出した.

最後に、項目Aと項目Bの相関を調べることにより、「どういうタイプの被験者 (項目B) 」が「どういうセキュリティ意識 (項目A) 」を有しているのか考察した。全クラスタの内, 何らかの相関が確認されたクラスタについて、「セキュリティ意識 (項目A) 」、「性向 (項目B) 」、「セキュリティ意識 (項目A) と性向 (項目B) の相関」に関する考察を以下に列記する.

a) 持ち物認証

C_{a2}:

セキュリティ意識:セキュリティ意識が適度に高く, 持ち物認証に対する不安がない.

性向:「非協調性」, 「抑うつ性」が低い.

セキュリティ意識と性向の相関:非協調性が低いことから、周囲と同調しやすい性向であると解釈できる。このため, 自分の置かれている環境 (情報セキュリティの研究室) に同調し、相応のセキュリティ意識を所持しているのだと推測できる. 抑うつ性が低いことから楽観傾向にあると解釈できる。このため、持ち物認証に対する不安が少ないのだと推測できる.

C_{a3}:

セキュリティ意識:セキュリティ意識が高いが, 持ち物認証に対する不安が大きい.

性向:「神経質」の値が極めて高い.

セキュリティ意識と性向の相関:神経質であるため、認証トークンを落としてしまうことに対する不安が大きいのだと推測できる。神経質であるため、リスクが生じることに対しても敏感であると解釈でき、このためセキュリティ意識が高いのだと推測できる.

b) PIN認証

C_{b1}:

セキュリティ意識:許容できる暗証番号の桁数が非常に長くセキュリティ意識も高いが, その一方で, PIN認証を許容したくない気持ちが高い.

性向:「神経質」, 「抑うつ性」, 「活動性」の値が高い.

セキュリティ意識と性向の相関:神経質, 抑うつ性が高いことから、物事に対して心配しやすく危機に敏感であると解釈でき、このためセキュリティ意識が高いのだと推測できる. 活動性が高いことから, 素早い行動を求める傾向にあると解釈できる。このため, ログインの度に暗証番号を入力する手間が生じるPIN認証に不便を感じており、PIN認証を許容したくない気持ちが強くなっているのだと推測できる.

C_{b2}:

セキュリティ意識:セキュリティ意識が適度に高いが, PIN認証に対する不安が大きい.

性向:「神経質」, 「抑うつ性」の値が高い.

セキュリティ意識と性向の相関:神経質、抑うつ性が高いことから、物事に対して心配しやすく危機に敏感であると解釈できる。このため, 不正者に暗証番号が解読されることに対する不安が大きいのだと推測できる。神経質、抑うつ性が高い性向をもつため、リスクが生じることに対しても敏感であると解釈でき、このためセキュリティ意識も高いのだと推測できる.

C_{b3}:

セキュリティ意識:セキュリティ意識が高く, PIN認証を許容する気持ちが高い.

性向:「規律性」の値が高い.

セキュリティ意識と性向の相関:規律性が高いことから、規則を守る傾向にあると解釈できる。

このため、適切なセキュリティ意識を有し、PIN認証を利用することが社会的なルールであると納得しているのだと推測できる.

C_{b6}：

セキュリティ意識：セキュリティ意識が非常に低く，PIN認証に対する不安も低い

性向：「攻撃性」が極めて低い.

セキュリティ意識と性向の相関：攻撃性の低い性向を有する者は物事を広く捉えることができ，環境に適応し易いことが知られている[8]. このため、暗証番号を設定して自分の情報を守るという意識が希薄であるのではないかと推測した.

c) 生体認証

C_{c3}：

セキュリティ意識：安全性よりも利便性を重視している. 生体認証を許容する気持ちが高い.

性向：「社会的外向性」が高く，「非協調性」，「規律性」，「神経質」の値が低い傾向にある.

セキュリティ意識と性向の相関：外向性や協調性が高いことから周りと同調する傾向にあり，かつ、規律性や神経質の性向が低いことから，セキュリティに関して大雑把な考えをする傾向にあると解釈できる. よって，安全性に多少の問題があるとしても，利便性を重視して生体認証を利用したいと考える傾向にあると推測できる.

C_{c4}：

セキュリティ意識：安全性を絶対的に重視している. 生体認証に対する不安が大きく，生体認証を利用したくない気持ちが高い.

性向：「神経質」の値が極めて高い.

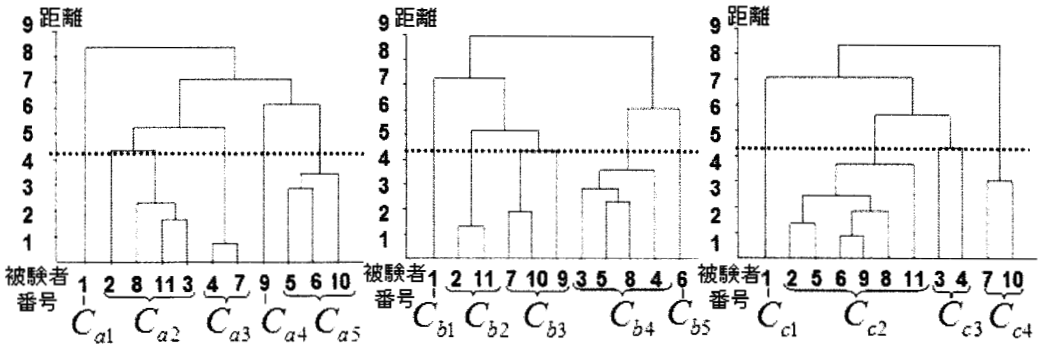

図2：クラスタ・デンドログラム（右から，持ち物認証，PIN認証，生体認証）

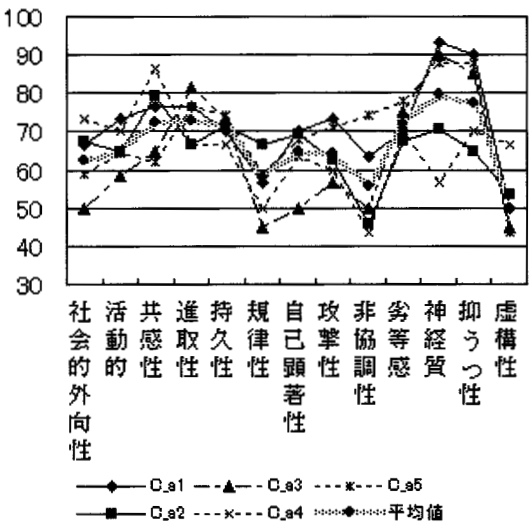

図3：クラスタごとの性向特性の平均値（持ち物認証）

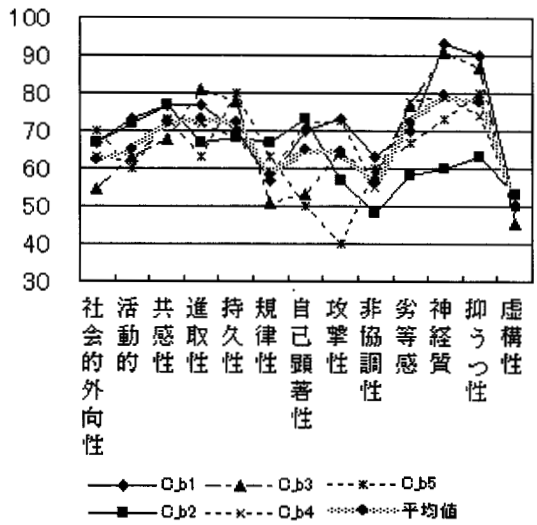

図4：クラスタごとの性向特性の平均値（PIN認証）

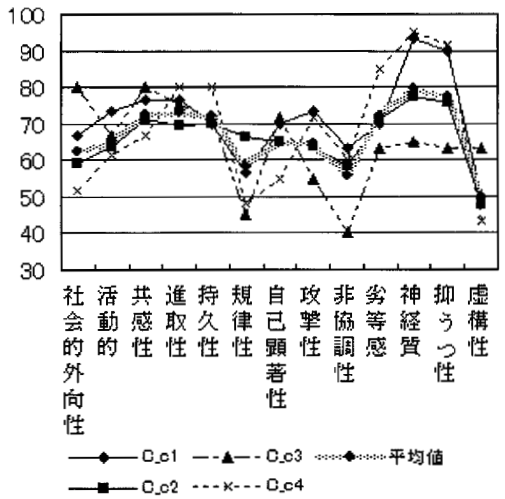

図5：クラスタごとの性向特性の平均値（生体認証）

セキュリティ意識と性向の相関：神経質であるため、リスクが生じることに対して敏感であると解釈でき、これが安全性の重視につながっているのだと推測できる．生体情報を登録するにあたっての抵抗や生体情報漏洩の懸念から，生体認証の安全性を疑問視しており、これが生体認証に対する不安を感じさせ、生体認証の利用からも遠のかせているのだと推測できる．

備考：

被験者全体的に生体認証に対する不安の度合いが他の認証と比べて高い傾向にあった．今回の被験者は全員，生体認証をATMなどの実用の場で利用した経験を有しておらず、これが結果に影響しているのではないかと考えられる．

3.4 考察

小規模な実験ではあるが，セキュリティ意識と特定の性向の要因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，今回の被験者は全員、情報セキュリティの研究に従事している学生であり，セキュリティに対する経験や情報機器に触れる機会が多いと考えられる。これが本調査結果に少なからず影響を与えている可能性は否定できない．

4. まとめと今後の課題

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．本システムを使用することにより，ユーザのニーズや嗜好に合致したセキュリティ対策を施すことができるため，ユーザが不便を感じてセキュリティ設定をあえてオフにしたり，セキュリティ機能を不適切に運用するというような「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．

本稿では，提案システムの実現可能性を検討するため，性向と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．11名のデータを基にクラスタ分析を行った結果，いくつかの性向特性とセキュリティ意識の間に相関があるという感触を得ることができた．しかし，今回の被験者全員が情報セキュリティの研究に従事している学生であること，および，被験者が11人という非常に小規模な調査であったことから，今後はより実社会に近い環境を想定した大規模な調査を行っていく必要があると考えている．

謝辞

今回の研究にあたり，東芝ソリューション株式会社加藤岳久様には方式に関しての助言を頂いた．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，及川ひとみ様には研究指針に関しての助言を頂いた。静岡大学情報学部 林部敬吉教授，漁田武雄教授には性格検査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] 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 (2008-01-22確認)

[2] 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）

[3] 大村政男：図解雑学 心理学，ナツメ社（1999）

[4] 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）

[5] 竹内光悦，元治恵子，山口和範：アンケート調査とデータ解析の仕組みがよ～く分かる本，秀和システム（2005）

[6] 上藤一郎，森本栄一，常包昌宏：調査と分析のための統計，丸善（2006）

[7] 菅民郎：多変量解析の実践（下），現代数学社（1993）

[8] 田中純夫，山田泰行，杉浦幸，菊地奈美，今野亮，水野基樹：中学生の攻撃性と学校適応との関連―中学生用機能的攻撃性尺度（FAS）の作成を通して―，順天堂大学スポーツ健康科学研究，第10号，pp50-58（2006）