教育効果を考慮した情報セキュリティ対策の統合型選定方式の提案

加藤 岳久† 上松 晴信††
名坂 浩平†† 西垣 正勝†

著者らは，情報セキュリティ対策を効率よく選択する具体的な方法論として，資産・脅威・対策・教育の関係をモデル化することでセキュリティ対策選択問題として定式化する方法を提案している．本稿では，著者らが行った本人認証技術に対するセキュリティ意識と性格に関する調査結果に対して，交通事故における性格と教育効果の相関を写像することによって，情報セキュリティ事故に対する性格と教育効果の関係を演繹する．そして，この分析結果に基づき，セキュリティ対策選択問題に対して性格とセキュリティ教育のファクタを導入した 2 グループモデルを提案する．

A Proposal of Integrated Security Measure Selection Considering the Effect of Education

Takehisa KATO† Harunobu AGEMATSU††
Kohei NASAKA†† Masakatsu NISHIGAKI†

We proposed a method to formulate an optimization problem to select security countermeasures that maximize cost-effectiveness, in consideration of the relationship between assets, threats, countermeasures, and education. In this paper, we investigate how user disposition and education affect car accidents, and from there, we try to deduce how user disposition and education impact on information security accidents. According to the analysis,.

† 静岡大学創造科学技術大学院，Graduate School of Science and Technology, Shizuoka University
†† 静岡大学大学院情報学研究科，Graduate school of Informatics, Shizuoka University

1. 背景

企業や組織にとって，情報システムを用いずに情報資産や業務の様々な運用管理を行うことは困難である．このため，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である．2005 年 10 月に ISMS 認証基準の国際規格が ISO/IEC 27001:2005 として発行されたことを受け，国内でも 2006 年 5 月に JIS Q 27001 が発行され，ISMS (Information Security Management System： 情報セキュリティマネジメントシステム) 適合認証制度として運用が始まっている．認証を受ける組織の数は堅調に増加している (図 1)．また企業等では，認証を取得しないまでも，情報セキュリティポリシを策定し，ポリシに従い構築したネットワークやシステムの運用管理を行う組織が少なくない[1]．

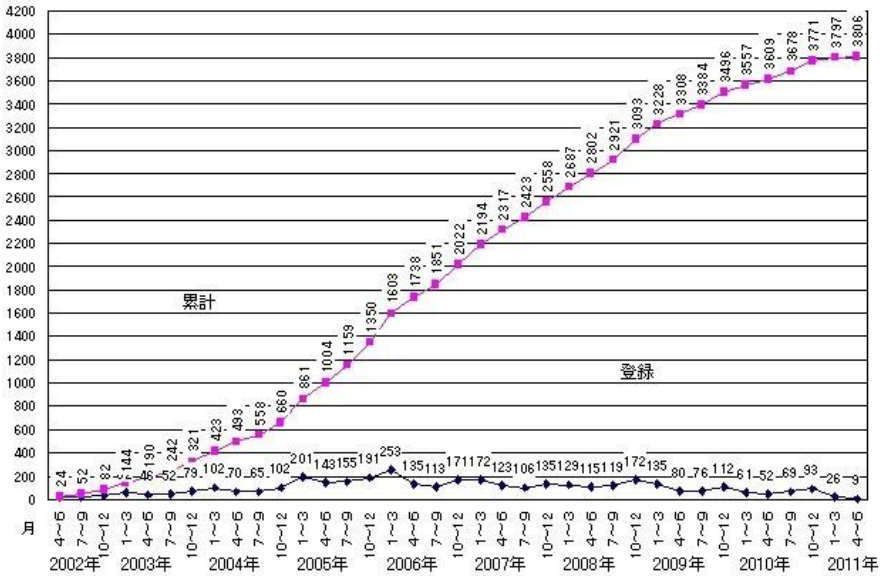

図 1. ISMS 認証取得組織数推移[1]

そこで，組織のリスク分析を行うための方法論やツールが整備される[2]とともに，経済学的なアプローチによって組織にとって最適なセキュリティ対策を選択する方法論の研究が進められてきている[3]-[7]．この中で，2004 年に中村らによって提案された方法[8]は，資産・脅威・対策の関係を適切かつ簡便にモデル化することによってセキュリティ対策選択問題を離散最適化問題として定式化しており，具体的な情報セキュリティ対策を効率よく選択することが可能となっている．

(財)ニューメディア開発協会の調査[9]によれば，企業が ISMS を取得する目的として，情報資産の明確化と整理（約 80%），事故発生時の体制・計画の整備（約 62%），情報流出や漏えいの防止・軽減（約 61%）を挙げている．しかし，その一方で，実業務と ISMS との乖離を約 26.5%の企業が感じており，前回調査から 2 倍以上増加したと報告している．

一方，Verizon Business 社による企業の情報流出事件に関する実態調査報告書[3]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報告している．また，情報漏えいの 87%は適切な対策を講じれば防止できたとも指摘している．この様に，ISMS を導入する企業は多いが，実業務との乖離があり，決められた手順による運用がなされておらず，情報漏えい等のセキュリティ事故の発生につながっていることがわかる．

以上から，組織のリスク分析を行い，情報システムに対する最適なセキュリティ対策を導入したとしても，それを利用するユーザが適切に運用していなければセキュリティ事故を無くす事は難しい．すなわち，情報システムを利用する個々のユーザのセキュリティ意識を高めることが重要で，そのためにセキュリティ教育を行うことが必要と考えられる．そこで著者らは，中村らが資産・脅威・対策の三者を用いて定式化したセキュリティ対策選択問題[8]に，情報セキュリティ教育の効果を導入し，中村モデルの拡張を行った[10]．また，事故を起こす主要因の一つと考えられている「性格」に焦点を当て、400 名規模の大学 1 年生を対象とした本人認証技術とセキュリティ意識と性格に関する質問紙調査を行い，セキュリティ意識と性格との間には確かに相関があることを示した[11]-[13]．

本稿では，情報セキュリティ事故に対する性格と教育効果の関係を分析する．ここでは，従来から様々な角度から豊富な調査が展開されている交通事故に関する既存研究を手掛かりとして，著者らが行った本人認証技術に対するセキュリティ意識と性格に関する調査結果に対して，交通事故における性格と教育効果の相関を写像することによって，情報セキュリティ事故に対する性格と教育効果の関係を演繹する．そして，この分析結果に基づき，中村モデルに対して性格とセキュリティ教育のファクタを導入した 2 グループモデルを提案する．

2. 教育効果を考慮したセキュリティ対策選定手法

本章では，中村らが資産，脅威，対策の関係をモデル化したセキュリティ対策選定問題[8]に対し，教育を加える背景となる調査研究を説明し，著者らが教育を加え定式化したセキュリティ対策選定問題[10]を説明する．

2.1 情報セキュリティ事故の原因と教育の必要性に関する調査研究

文献[3]の通り，情報セキュリティ事故が発生するのは，決められた手順が守られていないことが主要な原因である．

JNSA の調査によれば図 2 の通り，管理ミスが半数を超え，操作ミスが約 1/4 となっており，ユーザの環境や習熟度が原因で情報漏えいした割合は非常に小さい[15]．すなわち，情報セキュリティ事故の場合，ヒューマン・エラーのみがその主な原因となっている．

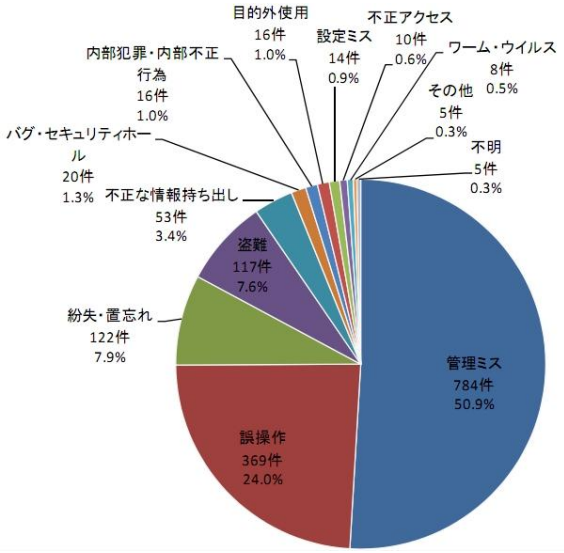

図 2. 漏えい原因比率（件数）[15]

松本は，決められた手順が守られない理由として，従業員のリスク認知意識の欠如による規則違反がその主な原因となっている，と分析している[14]．リスク認知意識の低い従業員の「うっかり」や「慢心」等のヒューマン・エラーが，常識的には認められない操作ミスにつながり，セキュリティ事故が引き起こされる．個人情報漏洩インシデントに焦点をあてた報告[15]においても，やはり，同様の知見が得られており，管理ミス，誤操作，紛失・置忘れなどのヒューマン・エラーが情報漏えいの原因の上位 85%以上を占めていると報告されている．

この様な「うっかり」や「慢心」によるヒューマン・エラーに対し，大和田らは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を提案している[16]．竹村も，従業員への Web 調査結果から，問題行動をとる従業員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，従業員は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[17]．大山らは，初期段階でのミスほど被害の拡大を招くため，事前の教育によって，情報摂取の段階で危険を予知し回避する能力を養成することは確かに重要である，としている[18]．

ISMS の運用に教育が効果的であることは，現場レベルでも認知されており，例えば，情報セキュリティに関するインターネット利用者意識調査 2008 によれば，企業等では，社員への情報セキュリティ教育をきちんと行うべきであり，研修の機会を増やすべきであると考えてい

る（図 3）[19]．また，企業内の情報管理に対しては，技術的対策を求めると共に，情報管理のルールを明確にし，教育により周知徹底を図るべきと考えている（図 4）[19]．

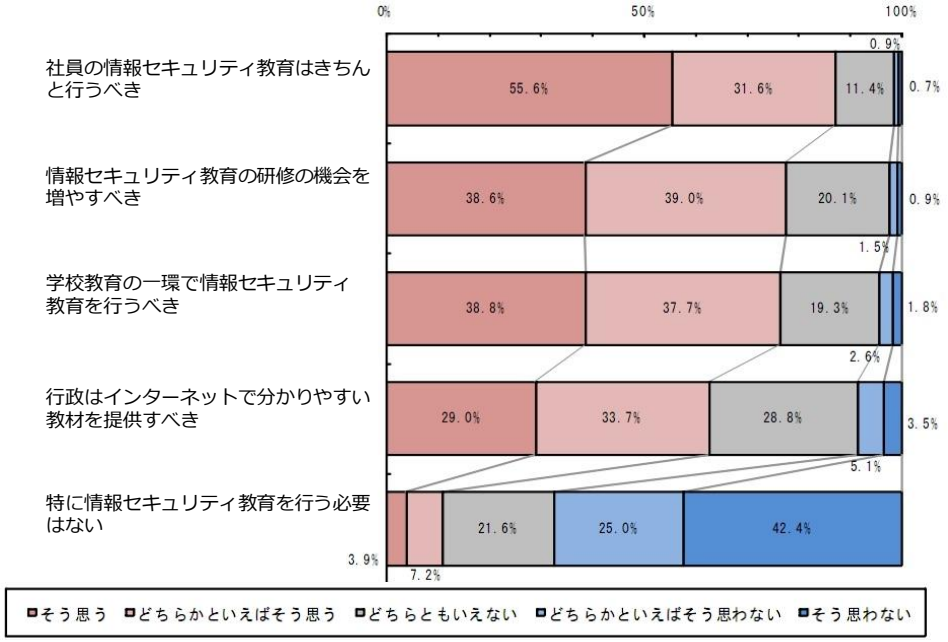

図 3. 情報セキュリティ教育に対する考え方[19]

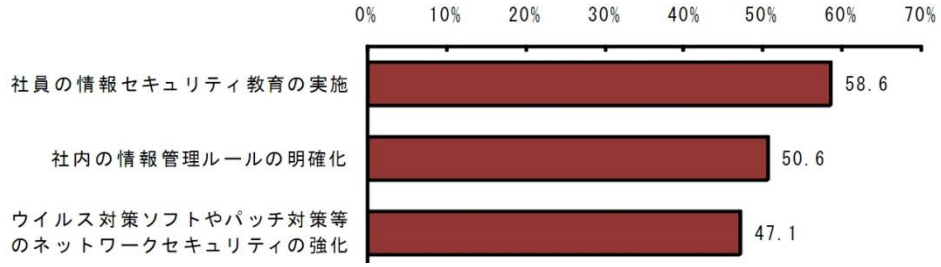

図 4. 企業内の情報管理を徹底させるために望ましいと考える方策[19]

2.2 情報セキュリティ事故の原因と教育の必要性に関する調査研究

2.1 節の研究から，教育を行うことで，決められた手順が運用され事故が減ると考えられていることが分かる．そこで，著者らは，中村らが定式化したセキュリティ対策選択問題[8]に，情報セキュリティ教育の効果を導入した拡張モデルの提案を行った[10]．

拡張モデルでは，前提として図 5 の様に情報セキュリティ対策を，

- A 郡：従業員のセキュリティ意識によって対策効果が変わらない対策
  ゲートウエイに設置されるファイアウォール，データ暗号化，等
- B 郡：従業員のセキュリティ意識によって対策効果が変わる対策
  ユーザ認証，等

に分類する．そして，表 1 のパラメータを用いて，式(2-1)の様に拡張モデルを提案した．

拡張モデルにおいては，情報セキュリティ教育を考慮したセキュリティ対策問題は

$$\sum_k \left\{ V_k \prod_j \left[1 - E_{jk} P_j \prod_{i \in A} \left(1 - R_{ji}^A S_i^A\right) \prod_{i \in B} \{1 - R_{ji}^B \prod_m \left(W_{ijm}\right) S_i^B \} \right] \right\}$$
$$- \left\{ \sum_i C_i S_i + \sum_m C_m S_m \right\} \qquad \cdots (2-1)$$

が最大となるフラグ(S_i, S_m)の組合せを見つける問題に帰着する．これは，

$$S_i = (S_i^A, S_i^B) \in \{0,1\} \quad (1 \le i \le I)$$
$$S_m \in \{0,1\} \quad (1 \le m \le M)$$

となる制約条件の下で，式(2-1)の目的関数を最大化するという離散最適化問題を解くことと等価となる．これにより，資産，脅威，対策，そして教育の 4 つの関係をモデル化し，セキュリティ対策選定問題を定式化した．

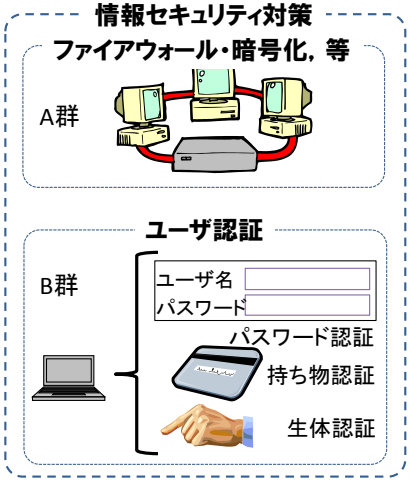

図 5. セキュリティ対策の分類

表 1. 拡張モデルにおけるパラメータ[10]

A_k (*Asset*)	組織内の資産．総資産数を K とし，複数の資産を k $(1 \leqq k \leqq K)$ で区別する．
V_k (*Value*)	資産 A_k の価値
T_j (*Threat*)	資産 A_k に対する脅威．脅威の総数を J とし，複数の脅威を j $(1 \leqq j \leqq J)$ で区別する．
P_j (*Probability*)	一定期間内に脅威 T_j が発生する確率
E_{jk} (*Effect Flag*)	脅威 T_j が資産 A_k に影響するか否かのフラグ
CM_i (*Countermeasure*)	脅威 T_j に対する情報セキュリティ対策．情報セキュリティ対策の総数を I とし，複数の対策を I $(1 \leqq i \leqq I)$ で区別する．
C_i (*Cost*)	情報セキュリティ対策 CM_i にかかるコスト$(1 \leqq i \leqq I)$
S_i	情報セキュリティ対策 CM_i を実施するか否かのフラグ （{0, 1}）
R_{ji} (*Risk Reducing Rate*)	脅威 T_j となる攻撃が発生した場合，情報セキュリティ対策 CM_i によりその攻撃の成功率が減少する割合．脅威 T_j となる攻撃に対する対策を行わなければ，攻撃が発生すると確率 1 で成功する．対策を行なっていれば，攻撃の成功率は $(1- R_{ji})$ に減少する．
SE_m (*Security Education*)	情報セキュリティ教育．情報セキュリティ教育の総数を M とし，複数の教育を m $(1 \leqq m \leqq M)$ で区別する．
C_m (*Cost*)	情報セキュリティ教育 SE_m にかかるコスト$(1 \leqq m \leqq M)$
W_{ijm} (*Comprehension Level*)	情報セキュリティ教育 SE_m の実施によって期待される脅威 T_j および対策 CM_i に関する従業員の理解度
S_m	セキュリティ教育 SE_m を実施するか否かのフラグ （{0, 1}）

3. 交通事故と性格等に関する既存研究

文献[3]および 2.1 節から，情報セキュリティ事故の原因として定めた運用が守られていないことが原因であり，教育の必要性も考慮に入れたセキュリティ対策選定問題を定式化した[10]．しかし，事故を起こす根本原因には性格も関与していると考えられる．そこで，本章では，これまで多様な視点で研究がされており，効果を上げている交通事故と性格について既存研究から性格も事故に深く関わっていることを示す．

米山は，交通事故を起こすドライバーは決まっており，繰り返し大小の事故を起こし，かつ純然たる過失によるものはなく，確信的違反行為や確認義務違反が原因で，加害者に加害意識がないとしている[20]．

澤は，交通事故の主要原因を図 6 の様に分析している[21]．

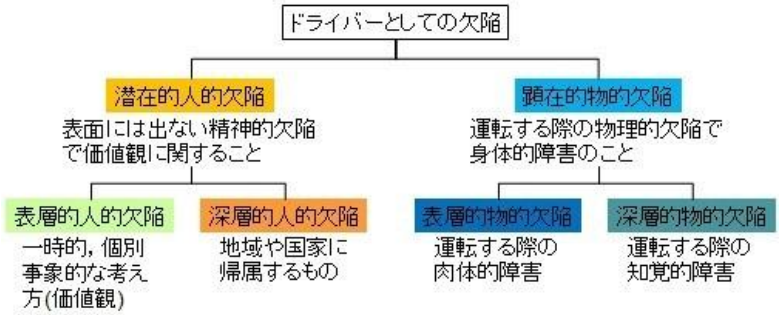

図 6. 交通事故の主要原因[21]

図 6 の通り，交通事故の場合は，人的欠陥と共に物理的欠陥も原因の一つであることがわかる．また，澤は事故を起こすドライバーの特徴として，自分は交通事故を起こさない（もしくは遭わない）と考えるドライバーが約 70%と報告し，誤った過信は危険としている．

交通事故を起こしやすい性格については，様々な見解[20]-[23]があるが，概ね以下の様な性格のドライバーに事故が多いとされている[a]．

(1) 自己中心的でハッタリ屋である．
  – 自分勝手で自己顕示欲が強い．自分を大きく見せようとする．劣等コンプレックスの反射的効果で，パラノイド（偏執質タイプ）である．この様なタイプのドライバーは，狭い道を猛スピードで走ったり，何人たりとも前を走らせたりしないタイプで，危険ドライバーの典型である．

a 性格等以外にも交通事故と関係する要因は存在する。例えば，さっぱりしたものを好むドライバーは事故を起こしやすい．これは，さっぱりした食べ物は，ビタミン B1 やタンパク質が少なく，集中力が無くなったり，疲れやすくなったりするためである．

(2) 感情の起伏が激しい.
– 情緒不安定なタイプである.
(3) 協調性に欠ける.
– 他人とうまく付き合おうとする気が欠けている.
(4) 攻撃的なヒステリー的性格
– 自分の失敗・行動の責任を、他の事物や人に押しつけ, わがままで感情の起伏が激しい. すぐにクラクションを鳴らしたり, ウィンカーを出さずに割り込みしたりする. この性格も, 危険ドライバーの典型である.
(5) 自己抑制が苦手
– 自分の気持ちを抑えられない.
(6) 神経質傾向が強い.
– 物事への拘りが強く, クヨクヨしやすい. もしくは, 常にカリカリしている.
(7) せっかちである.
– 粗雑な行動を取りやすい人で, 粗暴で危険な運転を行う. このタイプは, 信号が青になるとすぐに飛び出す様な運転をする.
(8) 行動にムラがある.
– 行動にムラがある人は,突発的に危険行動を起こす.
(9) 他人の気持ちを察せられない.
– 自分本位のマイペース運転をすることで, 他人に危険を及ぼす.
(10) (1)～(9)の事に自覚がない.

上記(1)～(9)の性格を, それぞれ新性格検査の 13 因子, および Big Five との対応を, 文献[24], [25]を参考にまとめたものが表 2 である. 表 2 から, 交通事故を起こしやすい性格というのは, Big Five からは情緒不安定性があり, 調和性の逆転項目が当てはまることがわかる. 一方, 新性格検査 13 因子では, 神経質かつ抑うつ性で, 自己顕示欲が強く非協調的で攻撃的なタイプが事故を起こしやすいことがわかる. ここで Big Five とは, 性格全体を構成する基本的特性次元（因子）を 5 因子とする主要 5 因子性格特性で, 表現は色々であるが, 開放性, 協調性, 良識性, 情緒安定性, 外向性を 5 因子とすることが多い[43].

図 6 の通り交通事故は, 人的要因, 即ちヒューマン・エラーにより発生したものである. 芳賀によれば, ヒューマン・エラーとは,「人間の決定または行動のうち, 本人の意図に反して, 動物, 物, システム, 環境の機能, 安全, 効率, 快適性, 利益, 意図, 感情を傷つけたり壊したり妨げたりするもの」[26]であり, その多くは思い込みによる危険判断の失敗により発生している[27].

また交通事故の原因として, ドライバーの性格だけでなく, リスクとハザードの知覚の欠如も原因とされている[28]-[30]. Brown & Groeger は, リスクを

a) 事象の不運な結果の測度

b) そのような結果があり得るような条件下への暴露度の測度との比率

と定義し, ハザードを「事故結果に寄与する可能性を持った対象や事象の特性を意味する概念」と定義している[31].

表 2. 交通事故を起こしやすい性格と新性格検査 13 因子, および Big Five との対応

交通事故を起こしやすい性格	新性格検査 13 因子	Big Five
自己中心的でハッタリ屋	自己顕示性	外向性／開放性
情緒不安定	神経質	情緒不安定性
協調性に欠ける	非協調性	(非) 調和性
攻撃的	攻撃性	(非) 調和性
自己抑制が苦手	抑うつ性	情緒不安定性
神経質	神経質	情緒不安定性
せっかち	非協調性	(非) 調和性
行動にムラ	抑うつ性	情緒不安定性
他人の気持ちが察せられない	自己顕示性	外向性／開放性

小川はリスクについて, 事故や事故に伴う重大性の測度が第一の測度で, 事故に遭う様な状況にどれだけ晒されているかの測度を第二の測度と解釈している. またハザードについては,「ある時点で, 他者と衝突する可能性あるいは運転エラーが生じる可能性が、将来の出来事として想定された場合, その可能性と関連をもつすべての交通参加者, 交通状況, 道路施設, 道路環鏡を指す」としている[28]. 交通事故を起こすのは, このリスクやハザードの知覚に問題があるとされている.

これらリスク知覚やハザード知覚は, 高齢者ほど低いという結果[30]もあるが, ドライバー自身が知覚すべき主観的リスクを知覚できない, もしくは低く評価するとリスクを伴う行動をとる, 即ちリスクテイキング行動をとるようになり, 事故を起こすとの結果もある. このため, 教育によりリスク知覚を向上することが重要[27]であり, 現在ではシミュレータ等を用いてリスク知覚を高める教育も行われている[32]-[34].

また, 交通事故と知能との関係に関する研究には, 以下がある.

三橋は, 知的機能が乏しいと事故を起こしやすいと報告[35]している. 知的機能が乏しいため, 見方や考え方の主観性, 状況把握, 状況判断が不適切に続き, 思慮が浅く, 洞察力が乏しく, 単純に考えるようになるため, 内省力が低いことが交通事犯につながりやすいとしている. これは, 例えば走行中の物陰から子供が飛び出してこないのかと考えたり, 前方の車の不自然な停車に何故かと考えなかったりする能力が乏しいことに拠るものである.

三橋は, 法務総合研究所の調査から, 交通刑務所の受刑者は IQ79 以下が約 3 割であり, 一般犯罪者の IQ よりは高いものの, 普通人の IQ に満たない率が高いと報告している. IQ の平均は 90～110 とされており, 知能テストの方法にも依存するがウェクスラー法では, IQ70～80 が境界知能で, IQ70 未満が精神遅滞としている[35].

瀬川は, 事故多発者群について, IQ が低い, またはかなり低い率が 12.6%あり, やや低い

を加えると 53.9%と報告している[36].

また小野は，IQ が高いか低いと事故を起こしやすいと報告している[37]. これは，IQ が低いと注意力が散漫となり，IQ が高いと自分がしていることに不満を覚え，短気傾向となるため，と分析している. この様なことから，知能が高くても低くても事故を起こしやすい性格が支配的で条件的役割となっているとしている.

以上から，交通事故を起こしやすいドライバーは知能レベルが低い傾向，もしくは高い傾向があるが，事故多発者の場合は低い傾向が見られる. そして，事故を起こすのは性格によるところが大きいことがわかる.

以上から，

- 事故を起こしやすい性格がある.
- 事故を起こすのは性格だけでなく，特に事故多発者に対しては知能レベルが関係し，ある程度の高さの知能レベルに達すれば，事故を起こしにくくなる.
- 事故を起こすのは，性格が支配的で条件的役割となっている.

ということが分かる.

以上から事故を起こすのは性格が支配的ではあり，また，知能レベルがある程度高くなれば事故を起こしにくくなる傾向があるということが演繹される.

4. 性格と教育効果に関する 2 グループモデル

2.1 節の調査結果から情報セキュリティ事故を防止するために教育は重要であり，2.2 節の情報セキュリティ教育の効果を導入した拡張モデルの提案を行った[10].

しかしながら，情報セキュリティ事故は教育の効果だけでなく，ユーザ個人の性格も関与していることが考えられる. 3 章で示した交通事故と性格等に関する研究結果からも分かる通り，事故に対しては教育の有無だけでなく，性格も事故を起因する大きな要因であり，事故を起こす性格があることもわかる.

そこで本稿では，図 7 に示す性格と教育効果に関する 2 グループモデルを提案する.

図 7 は，第 1 象限の群が，事故を起こしにくい性格で，かつ教育効果も高く，理想的なタイプといえる. 第 4 象限の群は，教育を受けることで第 1 象限の群になり事故をより起こしにくくなる. 第 1 象限の群も，忘却によって教育効果が薄れてしまうと，第 4 象限の群に戻ってしまうため，再度教育を受ける必要が出てくる. 一方，事故を起こしやすい性格の第 3 象限の群は，教育を受けることで教育効果を得て第 2 象限の群になり，第 3 象限の群に比べて事故を起こしにくくなる. 忘却によって教育効果が薄れてしまうと，再び第 3 象限の群になる.

事故と性格の関係を調査した既存研究の結果から，教育さえ行っておけばすべてのユーザが第 1 象限の群に到達するのではなく，事故を起こしやすい性格の人達は第 2 象限の群に留まることになる. このため、教育を導入する際には，事故を起こしにくい性格のグループ（第 1 象限の群，第 4 象限の群）と事故を起こしやすい性格のグループ（第 2 象限の群，第 3 象限の群）を区別して検討を行う必要がある.

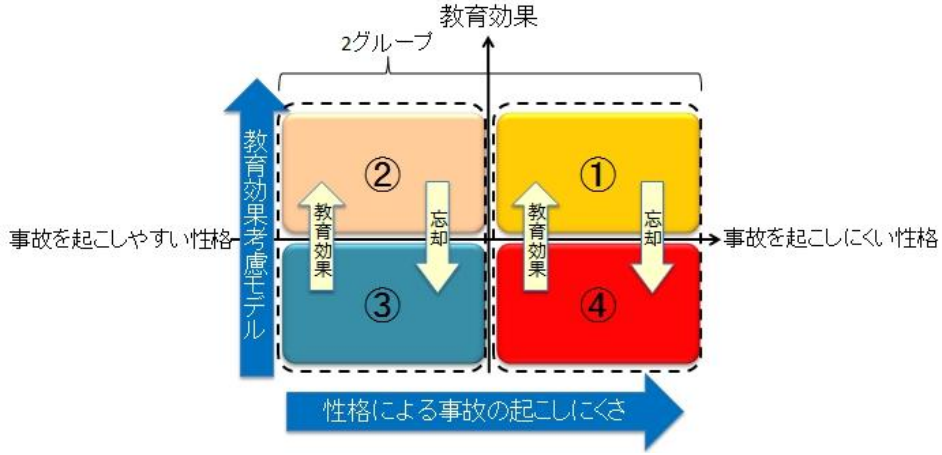

図 7. 性格と教育効果に関する 2 グループモデル

5. 情報セキュリティ事故と性格とに関する既存研究

3 章で，交通事故を起こす性格や原因，リスクテイキング行動，そして知能に関する既存研究について概説した. その結果，交通事故には性格，知能が関わっていることが分かる. そこで，図 7 に示した 2 グループモデルについて，情報セキュリティ事故と性格に関する既存研究を紹介し，その妥当性を示す.

一般に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重要である. 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て 2.1 節の研究が行われ，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事が重要であることがわかる. それに加え，情報セキュリティ事故と性格との関連に関し，以下の研究も展開されている.

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[38]. 大和田らは，情報セキュリティ事故の原因の一つに，従業員のリスク認知意識の欠如からなる規則違反が挙げられ，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[39]. 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依るところが小さくないことが分かる. また廣瀬は, 性向の Big Five (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, 疲れ易さ) 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[40]. その結果, 表 3 の様に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. 表 3 中の (+) は正の有意性を表し, (-) は負の有意性 (逆に有意であること) を表す. ここで, 忘却エラーは物忘れに関するエラー, 偏りエラーとは注意が偏ってしまうことに関するエラー, 入力エラーは入力を間違えることに関するエラー, 短絡的思考エラーは先入観等に囚われることに関するエラーである.

表 3. ヒューマン・エラーと相関の高い性格[40]

ヒューマン・エラー種別	相関が高い性格
忘却エラー	(+)いい加減さ
偏りエラー	(+)軽率さ (+)いい加減さ (−)勤勉性 (−)情緒安定性
入力エラー	(+)軽率さ (−)勤勉性 (+)自制心のなさ (+)いい加減さ
短絡的思考エラー	(−)勤勉性 (+)気の弱さ (+)疲れやすさ

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[41]. 廣瀬の結果[40]とから, 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・エラーに依るものが多く, 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依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.

6. ユーザの性格と情報セキュリティ意識との相関に関する研究

5 章では, 会社等の組織で情報セキュリティ教育を受けたユーザに対する調査で, 教育を受けていないユーザに対しては調査が行われていなかった.

そこで, 著者らは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することで, 純粋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するための調査研究を行った[11]-[13].

具体的には, 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一年生を対象に, 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た. 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一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様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 カードの所持等に対する得手不得手といったユーザの意識や性格が大きく関連すると考えたからである.

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[42]. 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した.

先行調査[11], [12]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一年生 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. さらに, 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, 更に大学一年生 200 名程度に対する追調査を行い, 両調査を併せ計 400 名規模の分析を行った[13]. その結果を表 4 に示す.

表 4 の結果と, 3 章で示した交通事故を起こしやすい性格と, 広瀬の結果[40]から, 事故を起こしやすい性格をまとめたものが図 8 である.

図 8 から, 本人認証でのセキュリティ意識にマイナスに働く性格と, 廣瀬のエラーを起因する性格とはほぼ一致していることがわかる. 所有物認証でマイナスに働く社会的外向性にあてはまる因子は関連研究における因子との関与がないが, これは, 著者らの調査がセキュリティ意識を対象にしており, エラーを起こすことを対象にしていないためと考えられる.

また, 交通事故を起こしやすい性格に, 自己顕示性や神経質, 抑うつ性等, 本人認証でのセキュリティ意識にマイナスに働く性格を含んでいることがわかる. 一方, 交通事故を起こしやすい性格の内, 協調性に欠ける, 攻撃的, せっかち等の性格は, セキュリティ意識に影響する性格との間に関与がないが, これは, 主に運転時における動作に影響を与える性格で, セ

キュリティ意識には影響を与えない因子と考えられる．

以上から，事故やエラーを発生しやすい性格と，本人認証に関するセキュリティ意識にマイナスに働く性格とは共通な部分が多く，情報セキュリティにおいても事故を起こしやすい性格と起こしにくい性格とがあることがわかる．

表 4. 本人認証技術に対するセキュリティ意識要因に影響を与える性格[13]

	プラスに働く性格	マイナスに働く性格	両方に働く性格	働き無し
パスワード認証	社会的外向性，活動性，持久性，規律性，神経質	新取性，自己顕示性，抑うつ性	劣等感	非協調性，攻撃性，共感性
所有物認証	持久性，自己顕示性，攻撃性，神経質	社会的外向性	共感性	活動性，進取性，規律性，非協調性，劣等感，抑うつ性
生体認証	持久性，非協調性	神経質	進取性	社会的外向性，活動性，共感性，規律性，自己顕示性，攻撃性，劣等感，抑うつ性

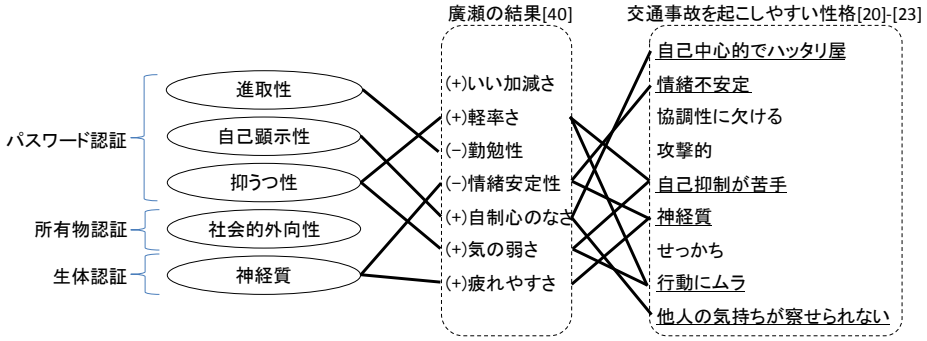

図 8. 事故を起こしやすい性格の共通因子[20]-[23], [40]

7. 交通事故と情報セキュリティ事故との類似点と相違点

3 章で交通事故と性格や知能との相関に関する既存研究を，5 章，6 章で情報セキュリティ事故と性格とに関する既存研究を紹介した．2 つの事故に共通することは，どちらもヒューマン・エラーが原因の大きな要因となっている点である．そして，それは性格に拠るものが大きいという点である．

表 3 から，ヒューマン・エラーに相関が高い性格は，Big Five での情緒不安定性や非調和性，そして非勤勉である，という点で交通事故を起こしやすい性格と類似している．すなわち，IQ の低さも勤勉性の低さも知識レベルの低下を招くことから，どちらの事故も知識レベルが低いと事故を起こしやすいと考えられる．

一方で，交通事故におけるハザード知覚は，情報システムにおける脆弱性の知覚であり，交通事故におけるリスク知覚は，情報セキュリティ事故が発生した時の重大性(例えば，情報漏えいでは漏えいした情報の気密性）の知覚であり，情報システムを利用する環境（社内環境なのかモバイル環境なのか，など）の知覚と言える．

このことから，情報セキュリティ事故の場合も交通事故の場合も，ヒューマン・エラーが主な原因となっている点で共通しており、これに関与する性格が事故要因となっていることが分かる．一方，交通事故原因における外的要因，運転操作，能力等に影響を与える性格は，情報セキュリティ事故には影響を与えないと考えられる．

8. まとめ

本稿では，中村らが提案した資産・脅威・対策の三者モデルに基づく情報セキュリティ対策選択問題に対して，提案した情報セキュリティ教育を考慮した拡張モデルについて，既存研究から教育効果を考慮することの必要性を示した．

3，5，6 章の研究結果から交通事故だけでなく情報セキュリティ事故にも性格を考慮することは必要であり，セキュリティ対策の選択に関する中村モデル[8]に，性格と教育効果のファクタを考慮することは重要である．

今後は，本方式の実用性を検証するためのシミュレーションを行い，有用性を実証する．本稿においては，教育によって期待される従業員の理解度 W_{ijm} によって教育効果を定式化したが，実際の教育現場では期待通りの教育効果が必ず得られるとは限らない．従業員に対するテスト等を通じて実際の教育効果を測り，その結果によってセキュリティ対策選択問題のパラメータを適応的に修正していく必要があると考えている．また，情報セキュリティ事故が発生してしまった後，もしくは事故につながるリスクが新たに発見された場合に実施される事後教育（ケーススタディ，e-Learning，等）も考慮した情報セキュリティ対策選択問題の定式化の方針を具体化し妥当性の評価をしていく．

謝辞

本研究をすすめるにあたり，静岡大学情報学部 漁田教授には心理学に関する解釈に対し，多大なる助言をいただきました．ここに深く感謝いたします．

参考文献

[1] 経済産業省，企業における情報セキュリティガバナンスのあり方に関する研究会 報告書, http:// www.meti.go.jp/report/downloadfiles/g50331d00j.pdf, (2012.5.5 アクセス)

[2] Rok Bojanc, and Borka Jerman-Blazic.: An economic modeling approach to information security risk management, International Journal of Information Management, Volume 28, Issue 5, pp.413-422（2008.10）

[3] Gordon, L.A., Loeb, M.P., The Economics of Information Security Investment, ACM Trans. Information and System Security, Vol.5, No.4, pp.438-457(2002).

[4] 松浦幹太, 情報セキュリティと経済学, 2003 年暗号と情報セキュリティシンポジウム予稿集, Vol.1, pp.475-480（2003.1）

[5] 永井康彦, 藤山達也, 佐々木良一, セキュリティ対策目標の最適決定技法の提案, 情報処理学会論文誌, Vol.41, No8, pp.2264-2271（2000.8）

[6] 榊啓, 矢野尾一男, 小川隆一, 多目的最適化によるセキュリティ対策立案方式の提案, 2007 年コンピュータセキュリティシンポジウム論文集 pp.193-198（2007.10）

[7] 大谷尚通, 不正アクセス行為の状態遷移モデルに基づくセキュリティ脅威と対策作成方法, 2007 年コンピュータセキュリティシンポジウム論文集, pp.283-288（2007.10）

[8] 中村逸一，兵藤敏之，曽我正和，水野忠則，西垣正勝，セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理学会論文誌 Vol.45 No.8, pp.2022-2033(2004.8)

[9] (財)ニューメディア開発協会, ISMS 第三者認証制度をより有効なものにするための ISMS 認証事業所調査, http://www.uchidak.com/isms/2010/2010_ISMS_Report.pdf (2011.4.20 アクセス)

[10] 加藤岳久, 山本匠, 西垣正勝, 教育効果を考慮したセキュリティ対策選定手法の検討, マルチメディア, 分散, 協調とモバイル（DICOMO2011）シンポジウム論文集, pp.135-140, (2011.7).

[11] 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)

[12] 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)

[13] 加藤岳久，中澤優美子，山本匠，漁田武雄，山田文康，西垣正勝，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, 情報処理学会論文誌, Vol.，No.，pp.- (2011.7).

[14] 松本匡史, IPS と NAC によりシステム的に構築する社内セキュリティポリシー, http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1199, McAfee blog (2011.4.18 アクセス)

[15] 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)

[16] 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)

[17] 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) http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/01/takemura2010.pdf (2011.3.10 アクセス)

[18] 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)

[19] NRI セキュアテクノロジーズ，情報セキュリティに関するインターネット利用者意識調査 2008，情報セキュリティレポート Vol.4 No.1 (2008.5), http://www.nri-secure.co.jp/news/2008/pdf/20080522_net.pdf (2011.4.23 アクセス)

[20] 米山 勝嗣，安全運行の教育資料 4. 交通事故の人的要因，倉鋪運送安全指導,倉鋪運送有限会社, http://www.geocities.jp/kura264752/jintekiyouin.html (2012.4.14 アクセス)

[21] 澤 喜司郎，こんなドライバーが事故を起こす，成山堂書店, (1993.8).

[22] 久保田忠男, “交通事故を起こしやすい人の性格”, http://www.mobilkubota.com/manabi/43.html (2012.4.14 アクセス)

[23] 清水 佑三, ‘嘘つき’のススメ－20 代で読むヒト学ココロ学, PHP 研究所, pp.40-41 (1992.11).

[24] 和田，性格特性用語を用いた Big Five 尺度の作成，心理学研究, Vol.67 No.1, pp.61-67 (1996)

[25] 齊藤崇子，中村知靖，遠藤利彦，横山まどか，性格特性用語を用いた Big Five 尺度の標準化，九州大学心理学研究 2，pp.135-144 (2001.3).

[26] 芳賀繁，失敗のメカニズム－忘れ物から巨大事故まで， 日本出版サービス, (2000)

[27] 人はどんなミスをして交通事故を起こすのかーキーワードは”思い込み”, http://www.itarda.or.jp/itardainfomation/info33/info33_1.html，(2012.4.14 アクセス)

[28] 小川和久, リスク知覚とハザード知覚, 大阪大学人間科学部紀要 19, pp.27-40 (1993).

[29] 松浦 常夫，運転中のハザード知覚とリスク知覚の研究動向，実践女子大学人間社会学部紀要 2，pp.15-40 (2006.4)

[30] 蓮花 一己 ，多田 昌裕，高齢ドライバーのリスク回避及びリスクテイキング行動の実証的研究，研究結果報告書集 15，pp.47-50 (2009)

[31] D. Brown & J. A. Groeger，Risk perception and decision taking during the transition between novice and experienced driver status，Ergonomics Volume 31，Issue 4，pp.585-597 (1988)

[32] 國分三輝，古西浩之，樋口和則，倉橋哲郎，梅村祥之，西博章，ドライビングシミュレ

ータによる高齢ドライバの運転行動とリスク知覚の分析(交通関連の安全性)，電子情報通信学会技術研究報告，SSS， 安全性 103(395)，pp.21-24，(2003.10).
[33] 松浦常夫，運転中のハザード知覚とリスク知覚の研究動向，実践女子大学人間社会学部紀要 2，pp.15-40，(2006.4).
[34] 横田祐介，芳賀繁，國分三輝，小川哲男，シミュレーター上の運転行動とリスク知覚、運転経験、安全態度の関係，立教大学心理学研究 46，pp.23-32，(2004.3).
[35] 三橋潤二，交通事犯の要因，交通鑑別ハンドブック，法務省矯正局 (1973).
[36] 瀬川興四郎，青少年の人格特質と交通事故,岩手大学教育学部研究年報 (35), p265-286, (1975.10).
[37] 小野章夫，知能および性格についての事故多発運転群と事故寡少運転者群との比較研究，科学警察研究報告，交通 1(1)(1), pp.111-127, (1960).
[38] 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)
http://www.jotsugakkai.or.jp/doc/taikai2010/J4-3 Kim.pdf (2011.3.10 アクセス)
[39] 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)
[40] 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)
[41] 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)
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/01/takemura2010.pdf
(2011.3.10 アクセス)
[42] 岩脇三良，心理検査における反応の心理，日本文科学社(1973)
[43] 村上宣寛，村上千恵子，主要 5 因子性格検査ハンドブック 改訂版，学芸図書，(2008).