情報事故における性格とセキュリティ意識との相関に関する研究

静岡大学博士論文
「情報事故における性格とセキュリティ意識との相関に関する研究」

2013年1月

大学院 自然科学系教育部
情報科学専攻

加藤　岳久

論文要旨

情報システムの導入なしに，情報資産や業務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．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と認識されている．2005 年 10 月に ISMS (Information Security Management System：情報セキュリティマネジメントシステム) 認証基準の国際規格が ISO/IEC 27001:2005 として発行され，国内では 2006 年 5 月に JIS Q 27001 が発行され，ISMS 適合認証制度として運用が始まった．認証を受ける組織は年々増加し，認証取得をしないまでも，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は少なくない．

組織の情報セキュリティ対策を検討するにあたっては，精緻なインシデントモデルが有用になる．ここで，情報事故の原因の多くがヒューマンエラーによるものであることに鑑みると，人的要因を考慮した形でのインシデントのモデル化が重要となる．そこで本研究では，インシデントの要因の一つと考えられるユーザの「性格」に焦点を当て，情報事故に対するインシデントモデルの構築を行う．

本研究の第 1 のステップでは，これまで多くの調査がなされている交通事故に関する既存研究を元に，情報事故と性格との関係を演繹する．交通事故においては，事故を起こしやすい性格特性と起こしにくい性格特性とがあり，それぞれの性格特性の傾向に関わらず，ドライバはシミュレータ等の疑似体験教育を受けることで，知識（スキル）が高まり事故を起こしにくくなる．これを情報事故のインシデントモデルに写像することによって，性格と教育でユーザを 4 つのグループに分ける「性格 2 グループ×知識 2 グループ」型のインシデントモデルを導く．

本研究の第 2 ステップでは，企業における社員のヒューマンエラーに関する既存研究を元に，ヒューマンエラーを起こしやすい性格特性（性格 A）と起こしにくい性格特性（性格 B）があることを示す．情報事故の 8 割以上がヒューマンエラーによって引き起こされることから，セキュリティ教育を受けたユーザ（社員）インシデントモデルが，ヒューマンエラーを起こしやすい性格特性が強いグループと起こしにくい性格特性が強いグループの 2 つに分かれることが裏付けられる．

本研究の第 3 ステップでは，情報セキュリティ教育の初学者である大学 1 年生約 400 名を対象に本人認証におけるセキュリティ意識に関する質問紙調査を行い，セキュリテ

ィ意識が低い傾向にある性格特性（性格 C）と高い傾向にある性格特性（性格 D）があることを明らかにする．認証情報の取り扱いに関する意識の低さが情報事故の温床となっていることから，情報セキュリティ教育初学者（大学 1 年生）のインシデントモデルも，セキュリティ意識の低い性格特性が強いグループとセキュリティ式の高い性格特性が強いグループの 2 つに分かれることが示される．

本研究の第 4 ステップでは，情報セキュリティ教育を受けたユーザ（第 2 ステップ）も情報セキュリティ教育初学者（第 3 ステップ）も，事故を起こしやすい性格特性は類似しており（性格 A と性格 C），かつ事故を起こしにくい性格特性も類似している（性格 B と性格 D）ことを確認する．幼児期に培われた性格は“三つ子の魂百まで”と言われる様に年齢や経験による影響を受けにくいことから，情報事故においても事故を起こしやすい性格特性と起こしにくい性格特性とがあり，それぞれの性格特性が強いユーザがいる．そして，情報セキュリティ教育を受け知識やスキルが高まることで事故を起こしにくくなる「性格 2 グループ×知識 2 グループ」型のインシデントモデルが妥当であることが示される．

本研究によって構築された「性格 2 グループ×知識 2 グループ型」インシデントモデルを利用することで，組織のセキュリティ対策の選定やユーザ教育の方法を効率化することが可能となると期待される．また，性格と教育に注意を加えた「性格 2 グループ×知識 2 グループ型×注意 2 グループ」インシデントモデルを提案する．

Outline of Thesis

An elaborated incident model is one of the vital elements for developing an effective information security management in organizations. Here, since many information security incidents are due to human error, it is important to consider human factors when we study the incident model. That is why this paper tries to establish an incident model on security accidents, focusing on user personality traits that are known as one of the big factors in security incidents.

In the first step of this study, based on the existing investigations on traffic accidents, we deduce the relationship between the user personality traits and information security incidents. Not a small number of researches on the traffic accidents have reported that there are accident-prone character and accident-avoidance character of car drivers. Then, each character group is further divided into accident-prone drivers and accident-avoidance drivers, respectively, according to the degree of their knowledge (skills). By deducing from the above mentioned fact underlying the traffic accidents, we derive a "2 personalty traits × 2 knowledges" type of information security incident model in which users are classified into four groups according to user personality traits and knowledge.

In the second step, from the existing investigations on human errors made by company employees, it is shown that there are error-prone character (personality A) and error-avoidance character (personality B). Judging from the fact that more than 80% of security incidents are caused by human error, it is reasonable to deduce that the information security incident model with respect to security-educated users (company employees) consists of two groups divided by user personality traits.

In the third step, we conduct a survey questionnaire on security consciousness in user authentication targeting approximately 400 university freshmen, and find that there is security-unconscious character (personality C) and security-conscious character (personality D). Judging from the fact that security-unconsciousness often leads any inappropriate handling of credential information and the subsequent

security flows, it is also acceptable to deduce that the information security incident model with respect to poorly security-educated users (university freshmen) consists of two groups divided by user personality traits

In the fourth step, it is confirmed that the personality traits of incident-prone group is similar between the educated and non-educated users (personality A and C), and also that the personality traits of incident-avoidance group is similar between the educated and non-educated users (personality B and D). As we know, it is said that the "temperament", a core factor of personality traits of human beings, is not affected by age and experiences. Therefore, it can be concluded that in information security incidents, there are incident-prone character and incident-avoidance character of users, and then, each character group is further divided into incident-prone users and incident-avoidance users, respectively, according to the degree of their knowledge (education level). This supports the validness of our "2 personality traits × 2 knowledges" type of information security incident model.

By designing with the proposed incident model in mind, it is expected to achieve more efficient information security management in organizations such as security measure selection, user education, and employee training.

目　次

図目次

表目次

第1章 序論

1.1 情報セキュリティのシステム運用管理の現状

情報システムの導入なくしては，情報資産や業務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．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と認識されている．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おり[1] (図 1-1)，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．

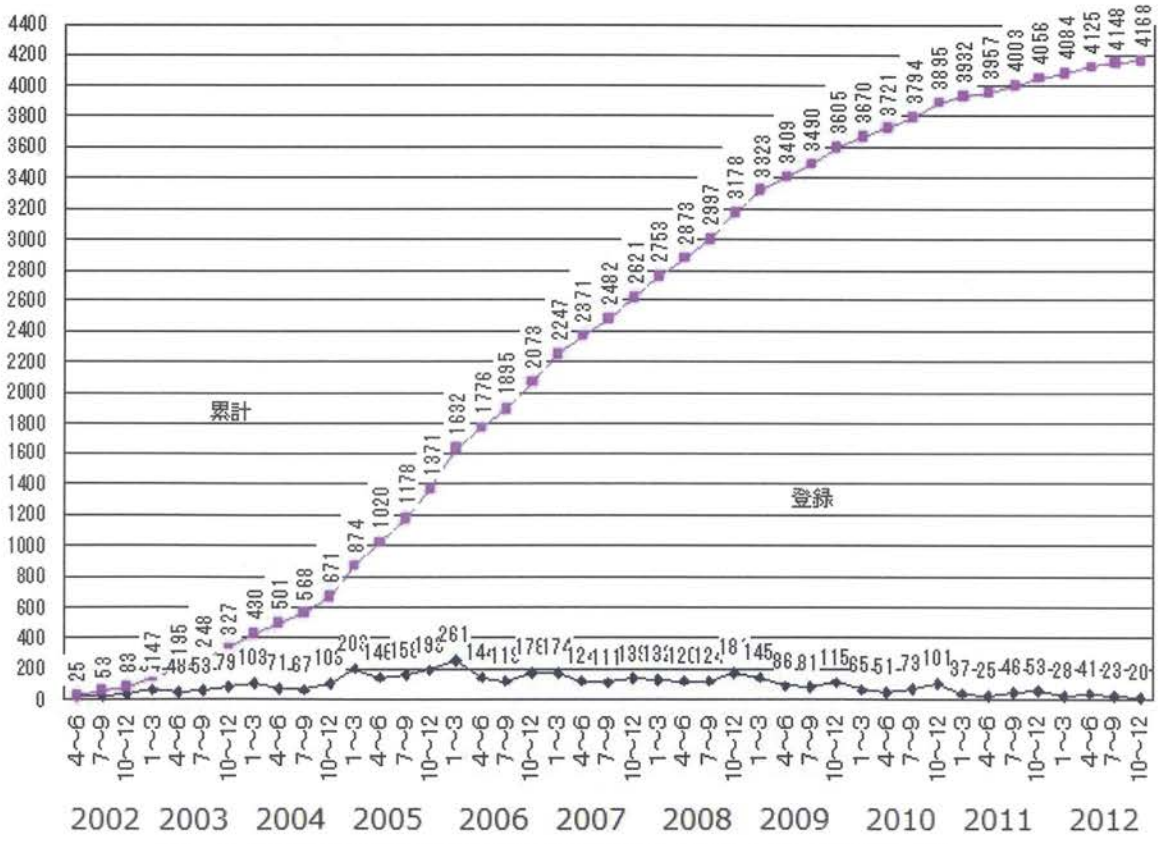


図 1-1. ISMS 認証取得組織数推移(2012 年 11 月 9 日現在) [1]

(財)ニューメディア開発協会の調査[2]によれば，企業が ISMS を取得する目的は，図

1-2 に示すように，営業活動，情報セキュリティ対策，業務改善と続く．

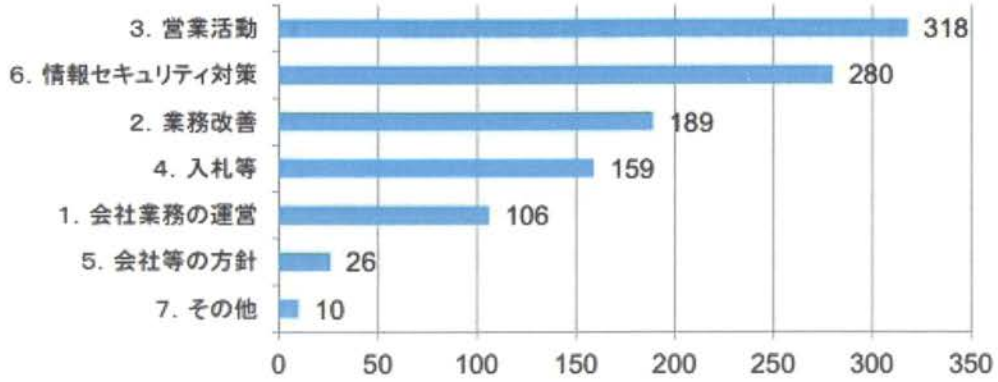


図 1-2. ISMS 認証取得の主な目的(有効回答数 423, 複数選択可)[2]

ISMS 認証を取得した効果は図 1-3 に示す様に，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．

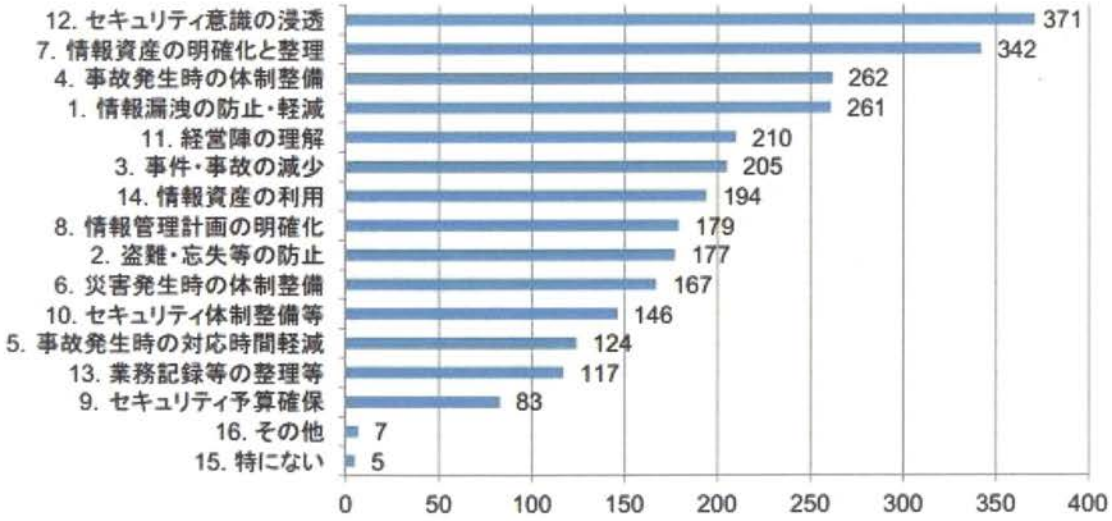


図 1-3. ISMS 認証取得による効果(有効回答数 423, 複数選択可)[2]

しかし，その一方で図 1-4 に示す様に，業務量の増加を約 40%の企業が感じており，業務上の制約，対策コスト，人員等の増加を約 30%の企業が感じている[2]．この様に，ISMS 認証の取得と実業務との間に，乖離があることは否定出来ない．

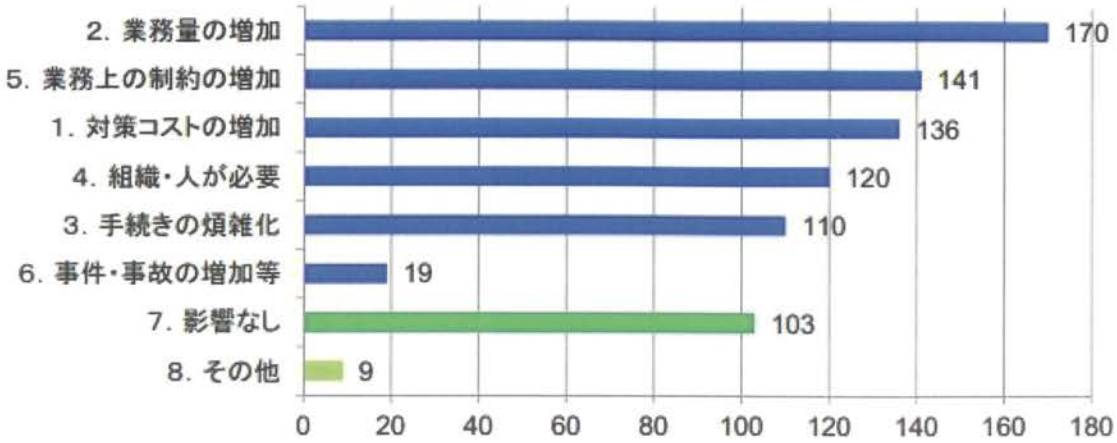


図 1-4. ISMS 認証取得の影響(有効回答数 426, 複数選択可)[2]

この様な乖離は何故起こるのだろうか．そもそも，情報セキュリティ対策を検討するためには，精緻なインシデントモデルが必要で，それに基づき必要なセキュリティ対策や運用を決定する．しかし，図 1-5 に示す様に情報漏えい事故の約 80%が誤操作，管理ミス，紛失・置忘れという，いわゆる“うっかり”や“慢心”といった人的要因によるもの，即ちヒューマンエラーが原因となっている．

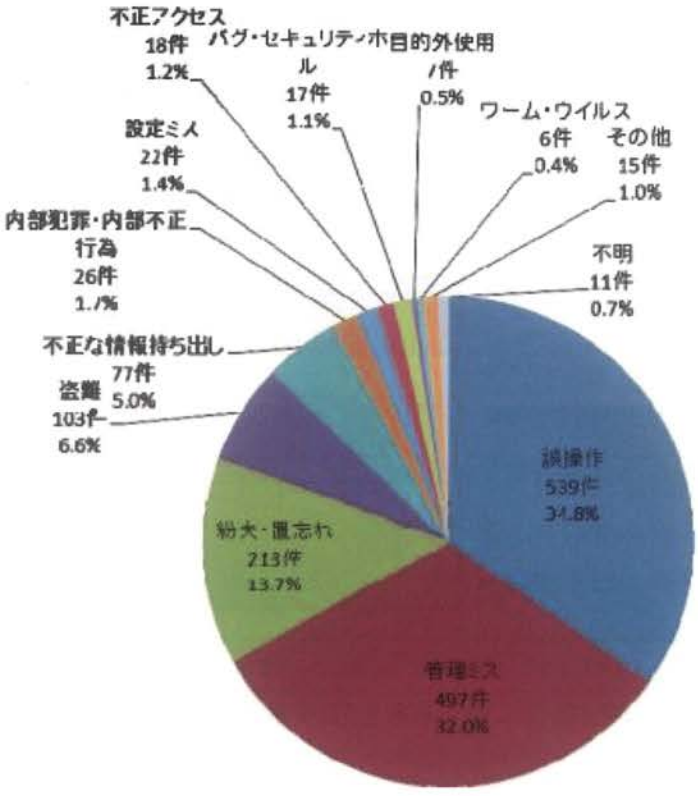


図 1-5. 情報漏えい原因別比率[3]

1.2 情報セキュリティ教育の重要性

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[4]．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，と報告している[5]．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[6]．

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いる．例えば，図1-6に示す様に，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[6]．また図1-7に示す様に，企業では自社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[6]．

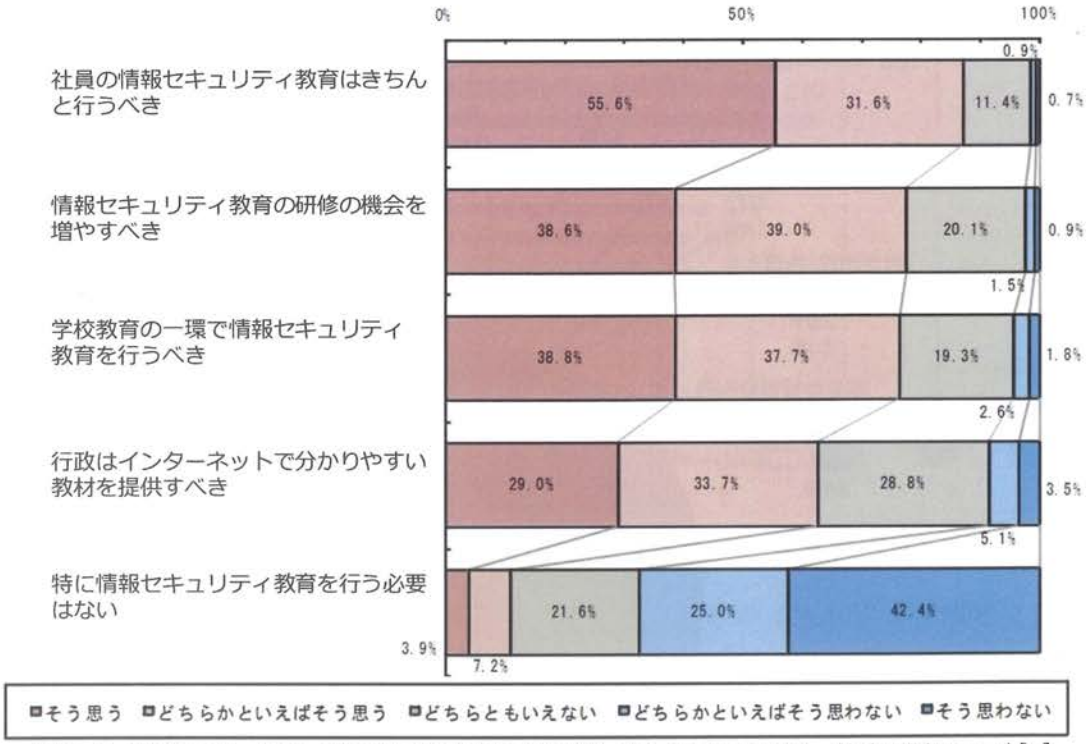


図1-6. 情報セキュリティ教育に対する考え方(有効回答数2,000，複数選択不可)[6]

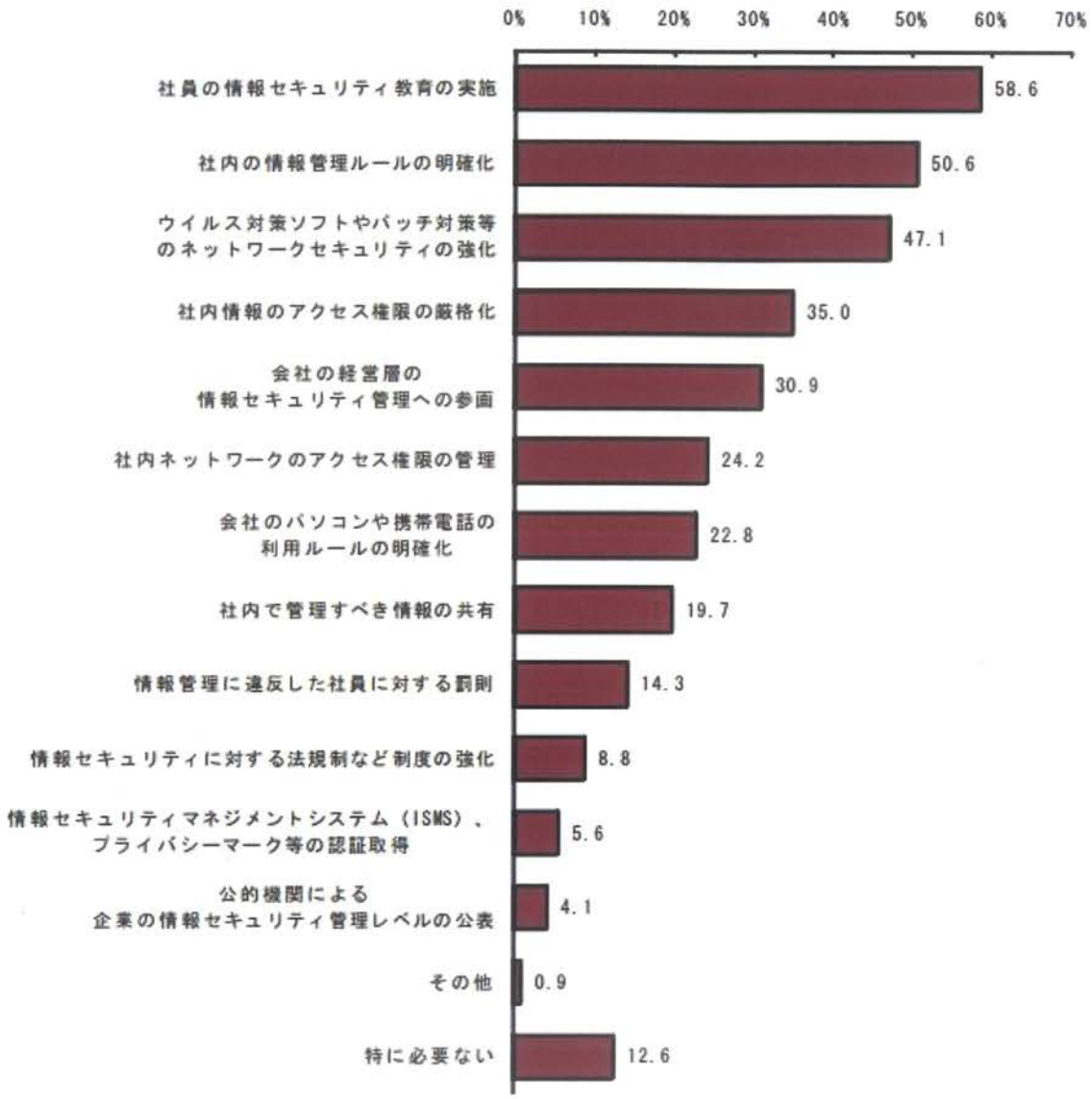


図 1-7. 企業内の情報管理を徹底させるために望ましいと考える方策
（有効回答数 876，複数選択 5 つまで可)[6]

以上から，企業での情報事故の多くはヒューマンエラーが原因で起きており，これを防ぐためには従業員のセキュリティ意識（リスク認知意識）を高めることが重要で，そのためには情報セキュリティ教育の質と量を確保すべき，ということがわかる．即ち，組織において導入されている情報セキュリティ対策の対策効果は，その組織において従業員にどのような情報セキュリティ教育が実施されたかによって左右されることになる．

1.3 事故とヒューマンエラー

本節では，そもそも事故とはどの様なものなのか，ヒューマンエラーとはどの様なも

のなのかについて考え，事故を起こす原因について論じる．

1.3.1 事故の定義

事故には，個人事故と組織事故の 2 種類がある．それぞれ，以下の様に定義される[7]．

- 個人事故：影響が個人レベルで収まるもの
- 組織事故：影響が組織全体に及ぶもの

一般に個人事故の件数が圧倒的に多いが，個人事故が複合的に重なり組織事故に発展する事例は少なくない．例えば，ある担当者のミスにより被害が発生したが報告が遅れ(担当者の個人事故)，その組織長がリカバリしようと隠したがリカバリできず被害を拡大（組織長の個人事故）させてしまい，結果的に組織事故となってしまうケースである．

また，19 世紀以前は事故と言えば機械の故障が大半で，機械の信頼性が低かった 1950 年代まで，その様な状況が続いた．しかし 1970 年代になり機械の信頼性，即ち品質管理が向上し，機械の故障や未知の原因に拠る事故は減少し，システムの安全性が向上した．これにより，事故の原因が人間の操作ミスや勘違いにシフトし，ヒューマンエラーが注目されるようになった[8]．

事故とは，“予期せず，望まざる出来事であり，損傷を伴うもの”[9]や，“計策され，またコントロールされている事象の連鎖の中で，計画されざる事象が起こることがある．それは個人の不適合行為の結果であり，損傷を伴う場合もあり，損傷を伴わない場合もある．これが事故である”[10]と定義される．この様な事から，事故は以下の特徴をもったものと定義[8]される．

- 意外性
  その結果の発生や予想を誰もしていなかったため，不本意な結果を起こしてしまった事故のこと．いわゆる想定外による事故と言える．
- 有害性
  その結果が，誰かにとって不都合な事故のこと．
- 不可逆性

その結果から元の状態への回復が許容出来る範囲内の費用で行えない事故のこと.

また意外でないことは故意であり，それによる有害な事故は事件（犯罪）である．また意外性を満たすが有害性を満たさないものはいわゆるヒヤリ・ハットと呼ばれる事象で，1 件の重大な事故の背景には，29 件の軽微な事故が発生[1]し，さらに 300 件のヒヤリとしたりハッとしたりする事故が発生している，というハインリッヒの法則（図 1-8）にある通り，重大な事故や軽微な事故の背景には多くのヒューマンエラーが発生していると考えられる．

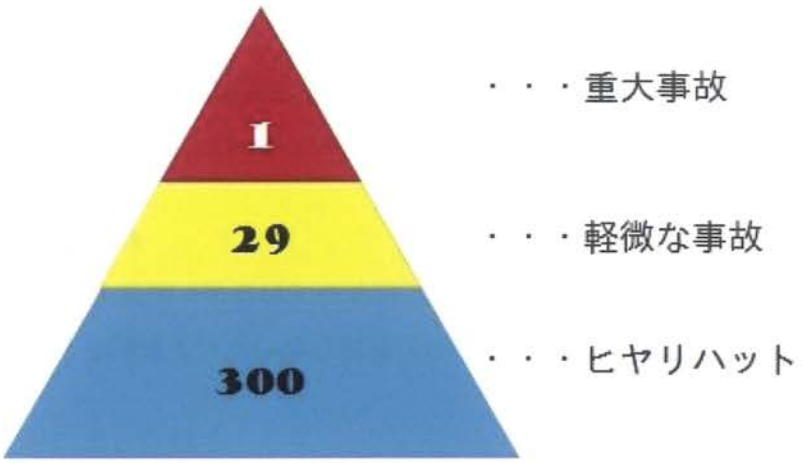


図 1-8. ハインリッヒの法則

1.3.2 ヒューマンエラー

ヒューマンエラーは，一般には“うっかりミス”が原因で発生し，人間が原因となる事故全般と解釈される．J. Reason は，“Planned actions that fail to achieve their desired consequences without the intervention of some chance or unforeseeable agency”（計画された心理的・身体的過程において，意図した結果が得られなかった場合を意味する用語）[11], [12] と定義している．即ちヒューマンエラーとは，全システムで人に割り当てられたタスクを，人がシステムに期待されている通りに行わなかったため本来望んでいた結果とは異なり（意外性），システムの機能や安全性を阻害することで事故や災害となる（有害性）行為であり，本来望まれている行為から逸脱したものであ

1 2004 年 3 月 26 日に発生した六本木ヒルズ森タワー2 階正面入口の回転ドアに 6 歳男児が挟まれ死亡した事故では，事故発生までに六本木ヒルズで 32 件の軽微な事故が発生したとの報告[12]がある．

る．この様に，ヒューマンエラーはシステムと人間の認知・行動特性とのアンマッチで発生するため，システムの設計と改良がエラー防止には大切である．

ヒューマンエラーそのものは，以下の様に分類[7]される．

- (事前の行為の) 意図による分類[7],[9],[13]

  - 行為のスリップ (Slips)[2] や記憶のラプス (Lapses)[3]
    行為の実施もしくは記憶段階での失敗が該当する．“うっかり”や“おっちょこちょい”といったエラーである．

  - 結果が期待通りでないミステイク (Mistakes)
    計画段階での失敗が該当する．後述するルールベース，もしくはナレッジベースで発生する．いわゆる“思い込み”によるエラーである．

  上記2つとも，行為は意図して行なっているが，間違えたのはわざとではないので，(ヒューマンエラーは) 意図しないものと解釈される．

- 行為による分類

  ヒューマンエラーが本格的に研究対象となったのは，アメリカにおける原子力発電が実施されるのに伴いリスク評価をすることになったからである．
  A. D. Swain と H. G. Guttmann は，必要な課題を忘れるオミッション (省略) ・エラー (Ommission Error) と，してはいけないことを行うコミッション (実行) ・エラー (Commission Error) の2つに分類した[14].
  J. Reason は，以下の7つに分類している[7].

  - オミッション
    必要，もしくは計算されたステップが，意図したタイミングで実行されないエラー．

  - 割り込み

2 ある意図が実行されるその過程の中で，自分の思いとは異なる行為をしてしまうエラー

3 作業途中で実行しなければいけない作業を失念してしまうエラー

望んでいない，もしくは意図しない行為の出現や，他の行動の一部分によるエラー

- 反復
  既に実行された不要な行為の繰り返しによるエラー.

- 対象間違い
  行為は正しいが，対象が間違っているエラー

- 順序間違い
  行為は正しいが，順序が間違っているエラー

- タイミング間違い
  行為は正しいが，タイミングが間違っているエラー

- 混合
  本来別々の目標のための 2 つの一連の行為が，意図せずに混ざるエラー

• 状況による分類

- 尚早と固執

  ➢ 一連の行為の中で，これから起きたり，過去に起きたりすることにより決まるエラー．具体的には，役者が後のセリフを早く口に出したり，過去の不適切な行為を繰り返したりしてしまう，ということがある.

- プライミング

  ➢ 一度受けた刺激が，後に受ける刺激に影響する効果による．ある発語や行為を繰り返した後に，別の刺激に対しても前の発話した言葉や行為を行なってしまうことがある.

- 中断と外乱

- 一連の行為の中で，何処まで終えたかが分からなくなる位置喪失エラーである．例えば，作業を中断して復旧した際に，済ませていない作業を済ませたと勘違いし，本来すべき作業を飛ばしてしまうことがある．

– ストレス

- 本来ストレスは，エラーを起こす必要条件でも十分条件でもないが，間違いを起こす可能性を高める要因となっていることは間違いがない．

• 結果による分類

– フリーレッスン

- 対価を支払わなくとも得られた教訓で，被害は小さかったが得られた教訓から事象を学ぶ，いわゆるヒヤリハットをケーススタディとして事例を学ぶこと．

– イクシーダンス

- 人間のパフォーマンスが安全限界ギリギリまでズレている状況で起こったエラーで，場合により機械やシステム，運用上の問題で引き起こされたエラーである．

– インシデント

- 危機一髪の事象で，報告や調査等を行うに値する重大事象である．つまり被害は小さいが，確実に何らかの被害を起こした事象である．この様な被害が少しだけ発生する事でシステム強化につながる．

– 事故

- 発生した事象により，負傷・死亡，資産の損害，環境破壊等の重大な被害をもたらす．これは，個人事故と組織事故との 2 つ

に分類される．

スリップやラプス，または行為の分類にある様々な間違いに見られるように，ヒューマンエラーの多くは注意していれば防げるものが多い．交通安全標語でも，“注意一秒，怪我一生”とあるように，不注意によるエラーで事故につながる事は少なくない．これがヒューマンエラーは不注意から起きる，と言われる所以である．

1.3.3 ヒューマンエラーと不注意

1.2.2 項でヒューマンエラーは不注意から起こると述べたが，そもそも注意とは何だろうか．また，注意を常に持続することは困難で，心的エネルギーが必要である．これは無限ではない．図 1-9 は注意の集中と持続の関係を表したもの[15]で，図 1-9 の通り高い集中力で注意を持続させれば，それはストレスとなる．そして，いずれは集中が途切れ，リラックス，または無気力な状態となる．いわゆる魔が差す等と呼ばれる状況である．この様に常に高いレベルで注意を払う事は難しく，睡眠に対する覚醒（arousal）や活動（activation）に対する不活動，注意（attention）に対する不注意があり，P. Janet は心理的緊張の波と呼んだ．注意力と集中力とは同じとは言えないが，集中している状態とは強く意志的注意を払っている状態である[15]．なお，集中している状態は警戒（vigilance）という概念で表され，生理学的には神経系における警戒する機能である覚醒（arousal）を意味するが，心理学的には注意（attention）の水準を示す用語で，本論では注意（attention）を用いる．

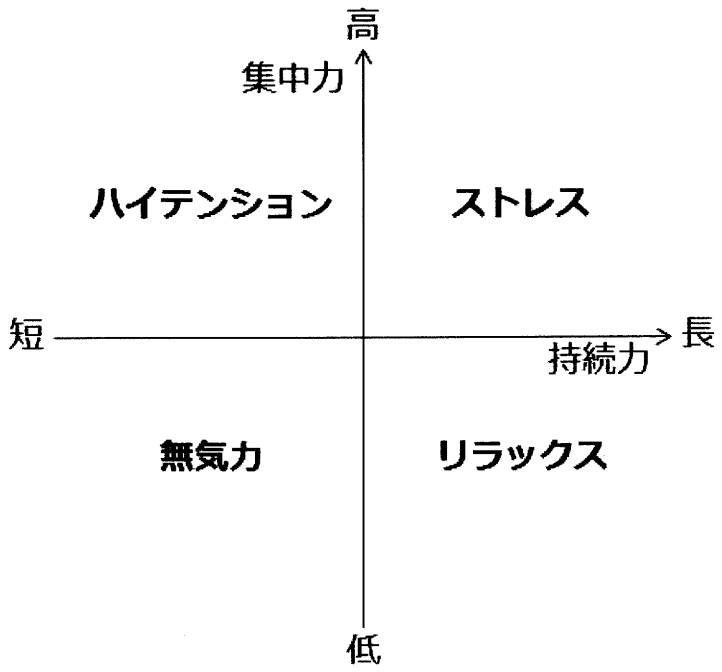


図 1-9. 注意と持続の関係[15]

Eysenck と Keane は，注意について図 1-10 の分類をしている[16]．注意（attention）は，焦点的注意（Focused attention）と分割的注意（Divided attention）に分類される．焦点的注意は，聴覚（Auditory）と視覚的（Visual）とに分類され，分割的注意は課題類似性（Task Similarity)と課題困難性（Task Difficulty）と練習（Practice）とに分類される．焦点的注意は，注意を何処に向けるかという定位や，注意を向けられている範囲の大きさや情報の選択がどの様に行われるかという点が問題になる[17]，分割的注意は，複数の情報源に対して同時処理を行う場合に向けられる注意で，行うべき課題の困難さや類似性，練習の程度が問題となる．つまり，課題が困難であれば多くの注意配分が必要となるが，類似した課題に対しては，相互に課題遂行を促進，干渉することで必要な注意配分が変化する．また，練習により技能が向上すれば，課題は自動遂行されて必要な注意配分量は減るのである．

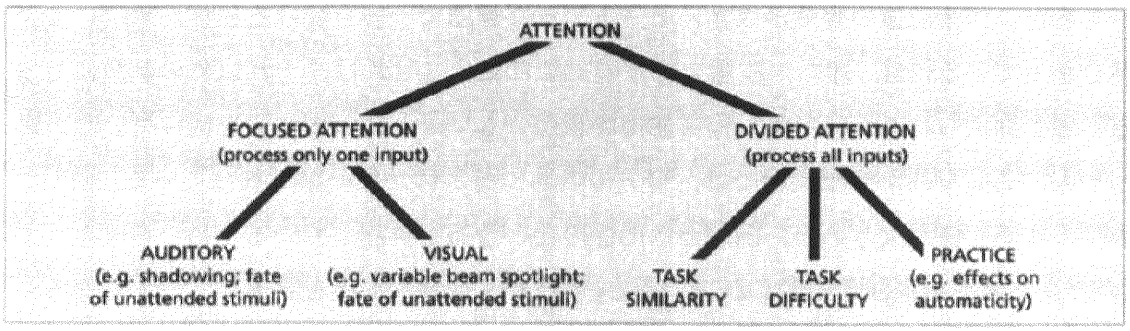


図 1-10. 注意の分類[16]

また別の見方をすれば，注意機能は大きく選択と集中，そして維持に分けられる．選択的注意機能については，視覚系での機能研究があり[18]，資格における選択注意機能は眼球運動と関連していることが分かっている．選択すべき，即ち注意すべき対象に対しては，最も視力が良い黄斑部を向ける（overt attention）．この様に，選択的注意は選択した対象の処理を促進し，処理結果が反応を促進することにある[19]．よって，関係が無いものに注意を向けると，注意すべき対象の処理が滞る．

集中は，作業記憶（working memory）と関係がある．作業記憶とは，精神作業を行いながら関連する情報を保持する機能で，構成要素である執行性注意（executive attention）で重要なことは，今行動するべき課題の要件を保持することと，その課題の要件と関係のない事が反応に影響を与える事を防止する事である[20]．課題の要件を忘れると，行動の節目で習慣的行動が侵入し，スリップ（slips）が発生する．

前述した様に，維持は特定の対象に注意を向け続ける（vigilance）ことである．長時間の監視作業では注意力（検出の成績）が，以下の理由により低下することが判っている．

- 覚醒の低下
- 飽き / 慣れ
- 疲労

作業記憶には，干渉を抑制する注意喚起機能がある．干渉効果としてストループ効果[4]

4 印刷された文字の色や単語について，色単語を読むかインクの色を命名（色命名）する際に，色単語がインクの色と不一致の場合に反応時間が長くなりエラー率も高くなる．

があるが，作業記憶の容量が大きいとストループ課題で干渉を受ける程度が少ないことが分かっている[21]．即ち，注意を特定の対象に集中させれば，それ以外の刺激に対する処理を抑えられる．一方で，作業記憶容量が大きい人に対して注意を向けていない耳へ本人の名前を聞かせた実験では，自分の名前に気が付かない事が判っている[22]．これは，作業記憶が大きいと，課題とは関係のない情報を排除しているためと考えられている．逆に考え事に注意を奪われていると，うっかり大事なことを見落としやすくなる．

1.3.4 ポジティブ・イリュージョンと自己中心性

1.2.3 項では注意について述べたが，ヒューマンエラーを起こす要因として，ポジティブ・イリュージョン（Positive Illusion）がある．

ポジティブ・イリュージョンとは，Taylor と Brown が唱えた考え方で，人は自分に都合が良い偏った認識こそ，精神的適用的に生きていく上で必要である，というものである[23]．即ち，無意識の内に自分自身を過大評価し，平均的な人よりも優れていると認識したり，環境のコントロール，将来について楽観視したりする傾向の事である．これは，後述するリスクを低く見積もる傾向につながる．

人は自分の事を知りたいと思う反面，自分に対して良い感情を持ち，生きる価値があると思う自己高揚（self-enhancement）動機があると言われている．人は，ポジティブ・シンキングが普通であり，ポジティブ・イリュージョンは役に立っている一面があるのかもしれない．人にとってポジティブ・イリュージョンが普通であれば，運が悪いとか避けられなかった等，原因を他者のせいにして自分に都合よく判断してしまうため，操作ミス等のヒューマンエラーを起こしやすくなることが考えられる．

また，ヒューマンエラーを引き起こす要因として，自己中心性（egocentrism）がある．自己中心性とは，自分を中心に物事を捉え，聞き手や他者等の周囲の立場から物事を見られないことを指す様で，J. Piaget が指摘した．Piaget は，成長と共に自己中心性から脱していき，周囲の視点を想定し，それに基づき行動できるとしているが，実験により，大人にも自己中心性が残る事が分かっている[24]．

1.3.5 記憶

認知科学では，人間の思考や記憶について情報処理システムと捉えモデル化することから始まった．特に初期の認知科学では，人間は環境からの情報を感覚器官で情報を知覚し，それに対して処理を行う存在と考え，処理結果は作用子を使った行為として環境にフィードバックされる．情報処理モデルでは，コンピュータと対比して概念及びモデル化される事が多い．情報処理モデル，コンピュータ共に共通する重要な機能として，記憶がある．記憶とは記名 → 保持 → 想起（再生・再認）の 3 つの過程から構成される情報の保持と再生という情報処理の機能である．人間の情報処理モデルでは，コンピュータでの RAM (Random Access Memory) の様に電源を切るとデータが消去されるものを短期記憶 (short-term memory) に，HDD (Hard Disc Drive) の様に電源を切ってもデータが残るものを長期記憶 (long-term memory) と対比している．この短期記憶と長期記憶の 2 種類に人間の記憶を分けてモデル化は，R. C. Atkinson と R. M. Shiffrin により二重貯蔵モデル (Dual-Store Model) として提案[25]され，図 1-11 に示す人間の情報処理モデルを表した[26]．この二重貯蔵モデルにおいて，短期記憶は保持できる容量が極めて小さいため，長期記憶へとつなげる反復学習や（頭の中での）リハーサルが充分でないと知的活動が制限される．なお，エビングハウス (H. Ebbinghaus) の忘却曲線により短期記憶を作業記憶 (Working Memory) と表すこともあるが，厳密には短期記憶が情報の短期的な貯蔵庫という意味が強いのに対し，作業記憶は読書や学習行動等の認知活動に伴う情報処理機能としての記憶という意味が強い．

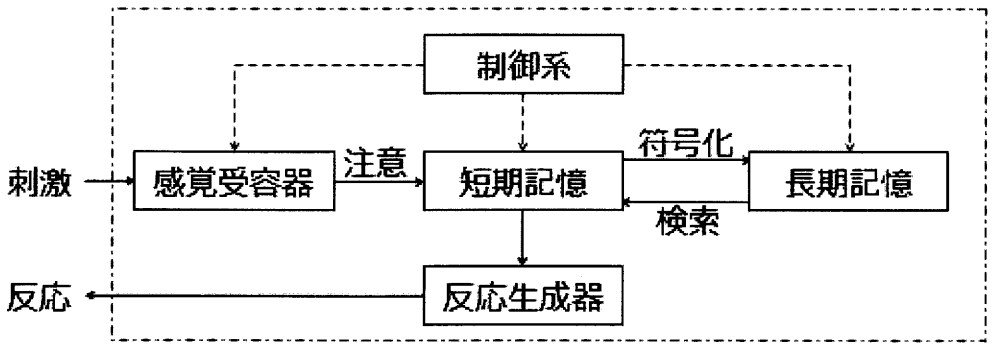


図 1-11. 人間の情報処理モデル[26]

一方，長期記憶は言語的な情報が記憶される宣言的記憶 (declarative memory) と，無意識な行動や手続きが記憶される手続き記憶 (procedural memory) とに分けられる．宣言的記憶は，作業記憶と意味記憶とを行き来させることが出来る記憶[27]で，エピソード記憶 (episodic memory) と意味記憶 (semantic memory) とに分けられる．また明

確に意識が出来ず，意図的な想起も出来ないが長期的に保存されている無意識な記憶を潜在記憶（implicit memory）と呼ぶ．なお，この考え方は，後のガニェ（Robert M. Gagné）の 9 教授事象（nine events of instruction)[28]の基礎となった．

バドリーとヒッチ（A. D. Baddeley & G. Hitch）は，短期記憶の容量は短期貯蔵庫（rehearsal buffer）のスロット数ではなく，処理資源（processing resources）の量で規定されると考えた[29]．図 1-11 に示す通り二重貯蔵モデルでは，注意（attention）は感覚受容器からの入力情報であるが，処理資源という概念を用いて，カーネマン（D. Kahneman）の注意（attention）の容量モデル（capacity model）では，注意と処理資源は同じであり，認知の情報処理システムを駆動する心的エネルギーと定義している．つまり処理資源は有限であり，人間が一度に処理できる課題や処理には限界があるため，注意を向けられる事象は限りがあるとするものである．またミラー（G. A. Miller）から，作業記憶の容量はマジックナンバー7±2[30]と考えられる．

図 1-11 における制御系の機能は，”内的な課題目標に適合するように外界の情報（刺激）を受け取り認知的な処理を行い，行為を選択生成する内的駆動型の心の働き”と定義され，このトップダウン型の機能により，状況に応じて行動や思考過程を柔軟に変化させられる[17]．そして，作業記憶と連携し，特定の情報に注意を向け，情報処理や検索等を制御する．

1.3.6 スキーマ理論

これらの様々な記憶や知識を統合された形として捉えたものにスキーマ（schema，仏語ではシェマ）がある．図 1-11 に示すように人間は外部からの刺激情報を符号化するが，これの基礎となる認識の単位や枠組みがスキーマで，過去の経験から獲得された知識の枠組みである．人間は，慣れた行動については意識することなく，自然に実行することができるが，それが出来るのは行動についてのスキーマが形成されているからである．例えば，家を出て会社に行くまでの電車の乗換えについて，どの車両のどのドアから乗れば次の駅での乗り換えが楽になるか（通勤スキーマ）とか，買い物等で車を運転して出かける一連の行動（運転スキーマ）とかがある．ここで，例えば朝の通勤で会社に向かわず顧客へ直接向かわなければいけないのに，いつもの乗換駅で降りてしまう等のエラーが発生する．これらのエラーには，以下がある[13], [17].

- 記述エラー：意図した行動の細部にわたる心理的記述描写が不十分となる．
- モードエラー：状況の把握を間違え，行為自体は意図通りであるが結果が誤る．
- 囚われエラー：意図した行動が，それと類似し実行頻度がより高い行動に囚われる．
- データ駆動エラー：スキーマ化された行動が，普段の状況と合致したため，意図しないにも関わらず行動を引き起こす．
- 頭部転換エラー：韻が類似した語頭を入れ違える ．

Norman は，この様な（スリップによる）エラー事例を分析し，ATS (Activation：活性化，Trigger：トリガー，Schema：スキーマ）システムモデルを構築し，スリップエラーの発生メカニズムを説明した[13]．

また，三浦は盆栽について専門家と知識のない観察者として学生とで，盆栽の鑑賞時の注視方法に違いがあることを報告[31]している．報告によれば，専門家の平均注視箇所数は 36.6 で盆栽にとって重要なポイント（欠点等）を観察しているのに対し，学生の平均注視箇所数は 51.8 と多く，かつ盆栽の形状全体を捉えていた．これは，知識（スキル）が，眼球運動と認知内容に影響を与えていることの証左であり，”何処を見て”，”何をすべきか”という，特定の行動スキーマが働き，特定の課題に依存した情報処理特性を有する可能性を指摘している．

1.3.7 メタ認知

メタ認知は 1976 年に Flavell が初めて用い[32]，知覚，記憶，学習，言語，自分行動や考え方，性格などを認知することを，より高い（メタな）視点から，即ち別の立場から認知することで，認知を認知する，或いは知っていることを知っていることを意味する．言い換えれば，自分自身を認識することとも言える．

メタ認知には図 1-12 に示す様に

- メタ認知的知識

認知作用の状態を判断するために蓄えられた課題，自己，方略についての知識

- メタ認知的技能
  メタ認知的知能に照らして，認知作用を直接的に調整するモニター，自己評価，コントロールの技能

の２つの働きがある．

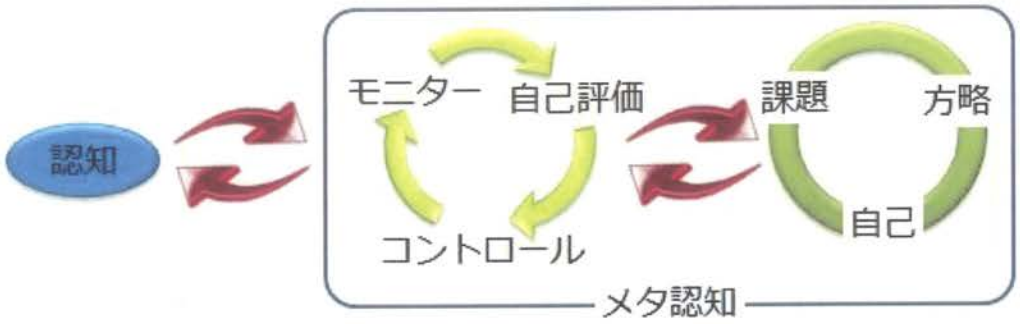


図 1-12. メタ認知の関連図[33]

このメタ認知にも

- 肯定的メタ認知
  メタ認知の働きを考える際に，そのメタ認知が問題解決や学習に，より有効的な働き

- 否定的メタ認知
  メタ認知的知識が行動（勉強や作業）することに阻害的に働き，嫌々実行してしまう負の働き

がある[34]．

意思決定に関するメタ認知的知識と意思決定の間には、強い関連があることが示唆されている．また、思考活動に注意を向け意識化することは、認知能力に大きく影響する。したがって、メタ認知は、さまざまな状況において優れた意思決定を下すために必要な能力であると言える。

問題解決においては自分の理解の状況をモニターすることが必要で，人間には自分自

身の事を知って，それを制御する力，メタ認知力がある．即ち，メタ認知力とは“認知についての認知力”で，図 1-12 に示すように頭の中のもう一人の自分 (homunculus) が自らを監視しコントロールする力である．

重松は，メタ認知力をメタ認知的知識とメタ認知的技能の 2 つからなるとしている[35]．メタ認知的知識とは，環境の状態が認知作用に与える影響，課題が認知作用に与える影響，自己の技能・能力が認知作用に与える影響，認知作用を良くする方略に関し，認知作用の状態を判断するために蓄えられる知識である．

またメタ認知的技能は，認知作用の進行状況を直接確認するモニター，認知作用の結果をメタ認知的知識と照合し直接評価する自己評価，自己評価に基づき直接認知作用を制御するコントロール，の 3 つがあり自己モニタリング力とも言える．この自己モニタリング力が強い人は，慎重になる傾向がありエラーを起こしたとしても大きな事故につながることが少ないと考えられる．

1.3.8 不安全（リスク・テイキング）行動と注意

産業界では，事故は不安全行動によりもたらされると考えられ，場合によりヒューマンエラー対策を無効にするもので大きな問題となっている．

不安全行動にはヒューマンエラーの様に意図しないものもあれば，意図的なものもある．意図しないものはリスク・テイキング行動で，意図するものは違反を容認する心理的要因による違反行動で，重複する部分があるものの異なるものと捉えられる[21]．図 1-12 の様に，経営判断やギャンブルでの選択，結婚相手の選択等は，リスク・テイキングな面はあるが，違反ではないし事故の発生を高めることもない．また，日常において違反ではないがリスクを伴う行動となる，例えば制限速度を超過しての運転や，違法なギャンブルは事故を発生する確率を高める不安全行動である．また，法令やマナーの違反や約束の反故は，社会的信用の失墜や人間関係を損なう等のリスクはあるが，リスク・テイキングとは言えない．

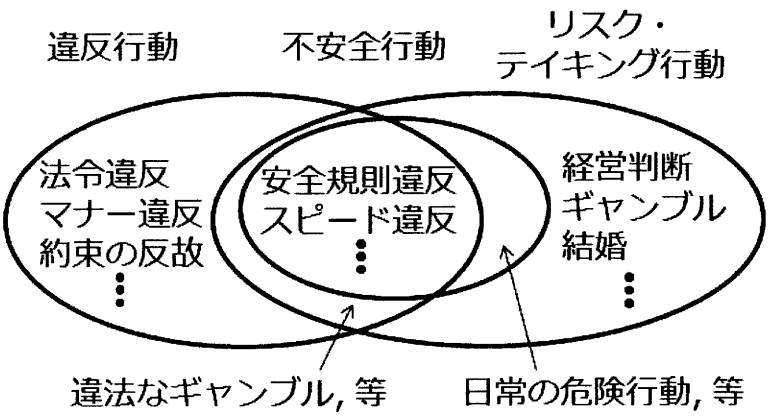


図 1-13. リスク・テイキング行動と違反行動との関係[21]

人が不安全行動をとる場合には，4つのケースがある．

第1のケースは，リスクを小さく見積もるケースである．リスクは，(式 1-1)で表される．

リスク(客観的リスクの主観的見積もり)＝(失敗する確率) × (失敗した時の被害)

・・・(式 1-1)

人は失敗する確率が高くても被害が小さいと見積もる，もしくは被害が大きくても確率が小さいと見積もるとリスクを選んでしまうと考えられる．

第 2 のケースは，成功による効果（報酬）が大きなケースである．ここで効果とは金銭面だけでなく，快楽や達成感等の心理的効果も含まれる．

第3のケースは，リスクを避けたことによるデメリットが大きいケースである．リスクを避けるために，時間，距離，金銭，作業効率等の損失が大きいと不安全行動を選択する事が多い．

第4のケースは，不安全行動で何らかの効果が得られるケースである．これは意図的な行為となるケースが多く，例えば車の運転では敢えてスピードを出す事で眠気をおさめる（覚醒水準を下げる）効果等である．

不安全行動を4つのケースに分類したが，これらは以下の3つの違反に分類される[4]．

- スキルベースレベルの違反

  熟練あるいは習慣化した行為で，例えばある仕事の中の 2 つの作業ステップ

をつなげてしまうなどの軽微な違反が多い.

- ルールベースレベルの違反

  一般に，問題があったりリスクが高かったりする状況では，行動を制御するためにマニュアル等の手順書が整備されていることが多い．定められた手順を守らない事は意図的に行われることが多く，厄介なことは違反することでより良い効果が得られると信じて行われることである．即ち，見込まれる損失よりも利益が大きい場合に行われる．

- ナレッジベースレベルの違反

  マニュアル等の手順書は，既知もしくは予見できるリスクに対して対応が書かれるのが一般的である．しかし，作業する者の経験や知識により，より良い効果が得られることもある．特に事故が発生した際に，当事者の機転により被害を最低限に抑えた事例は多い．

J. Reason は，更にこれらの不安全行動を起こす理由として，重要な 3 つのポイントを挙げている[7]. 1 つ目はコントロールの錯覚で，常習的な違反者に見られ，自分は力があると感じて重大な結果に対して自らコントロールできると過大評価してしまうものである．2 つ目は不死身の錯覚で，自らの違反が良くない結果につながることを過小評価し，自分のスキルが常に潜在的な危険性に勝っていると信じてしまうものである．3 つ目は優越の錯覚で，他人よりも自分のスキル・能力が優れていると評価しているものや，自らの違反のレベルが他人よりもましと評価しているものである．これらは，メタ認知の欠如とも関連し，自己中心性が強く楽観視したために起こるとも考えられる.

これらの錯覚は注意を払うことを妨げる事にもつながり，“おっちょこちょい”とか“そそっかしい”と呼ばれる類のものである.

1.2.2 項で示したように，“おっちょこちょい”や“そそっかしい”と言われるタイプは，落ち着きがなく注意が払えず錯覚し，ついやってしまうコミッション・エラーを起こしやすいと考えられる．また，ぼんやりしてエラーを起こす場合があるが，これは記憶が苦手なためにし忘れるオミッション・エラーを起こしやすい．これらは，どちらか一方が強く出る場合もあるし，両方出る場合もあると考えられる.

Gerald J. S. Wilde は，人間は許容するリスクの水準を持っていて，それは体温等を一定に保つホメオスタシスと同じ様に，一定の水準で均衡するように保たれることをリスク・ホメオスタシスと呼んだ[36], [37]．これは，システムが安全になれば危険性が下がり一時的に事故は減るが，いずれ人は下がった危険を元に戻す様にリスクテイキング

行動をとるようになる，というものである．

1.3.9 情報事故

本研究で扱う情報事故を，図 1-14 の様に定義する．

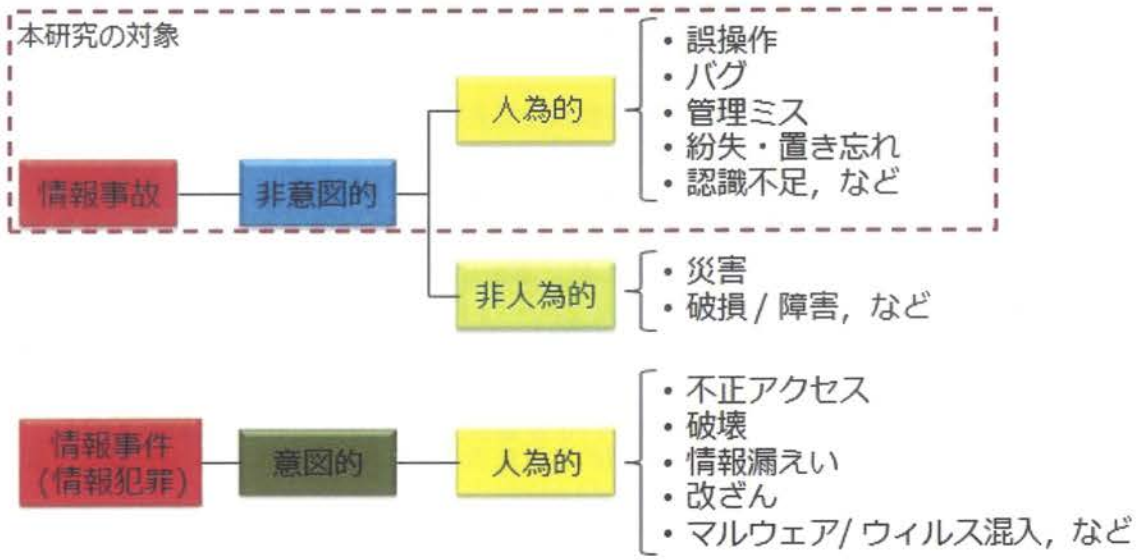


図 1-14. 情報事故の定義

1.2.1 項で示したように，事故には意外性，有害性，不可逆性の性質を持つが，意外性は非意図的な行為であり，前述したように意図的な行為は故意であり，それにより有害性が発生すれば事件（犯罪）である．従って情報システムにおける不正アクセスやシステムの破損や破壊，意図的な持ち出しによる情報漏えい，意図的な改ざん（例えば帳簿データの書き換え，等），マルウェアやウィルスによる情報システムやパーソナル・コンピュータへの攻撃等は，情報事件（情報犯罪）と定義する．

一方，意外性があり非意図的に発生するものを情報事故と定義する．非意図的なものには，人為的なものと非人為的なものがある．人為的なものには，誤操作，(意図せず混入された) バグ，管理ミス，紛失や置き忘れによる情報漏えいや情報資産の喪失等がある，また，安易なダウンロードによる不正なプログラムの実行や不審なメールに添付されたファイルを開いてしまったり，記載されたリンク（URL）を開いたりしてマルウェアやウィルスに感染する等の被害に遭ったり，自分の端末が踏み台にされる等，認識不足による事故も情報事故に含まれる．非人為的なものには，火災（自然発火的なものであり，放火は犯罪である）や落雷により渦電流が流れ電子機器を破損する雷（らい）サ

ージ (Lightning Surge)，地震による情報システムの破壊，サーバ等の機器の破損，ネットワーク障害等がある．

本研究では，情報事故の中で図 1-14 の点線で囲った人為的なものを対象とするが，有害性が小さい（事故までには至っていない）ヒヤリ・ハットやインシデントも対象とする．

1.3.10 情報セキュリティ分野におけるヒューマンエラー対策の動向

これまで情報セキュリティ，特にネットワークセキュリティは OSI 参照モデルのどの階層で，どの様な対策をするのか議論されてきた．OSI 参照モデル[38]は図 1-15 に示す様に 7 階層で構成されている．

それぞれの層は，以下の様に定義されている．

- Layer 1：物理層（Application）
  物理リンク上で，構造を持たないビット列を配送する．

- Layer 2：データリンク層（Data Link）
  単一のリンク上で，情報の塊を配送する．物理層のビット列をパケットに直し，共有リンク上の誰がどのパケットを受け取るか制御を行う．

- Layer 3：ネットワーク層（Network）
  相互接続されたリンクと交換機からなる網をまたがる経路を計算して，送信元から受信先まで複数のリンクを経由してパケットを送信する．

- Layer 4：トランスポート層（Transport）
  ネットワーク越しの 2 つのシステムの間に信頼性のある通信ストリームを確立する．

- Layer 5：セッション層（Session）
  トランスポート層で提供される二者間の信頼性のある通信ストリームに，付加的な機能を追加する．

- Layer 6：プレゼンテーション層（Presentation）

アプリケーションデータを標準のシステムに依存しないフォーマットに符号化する.

- Layer 7 : アプリケーション層 (Application)
  電子メールやファイル転送等のネットワークを利用するアプリケーションがある.

図 1-15. OSI 参照モデル

これらの層に加えて，3 つ層を加えた 10 階層で考えることが提案されている[39].

- Layer 8 : The individual person (ヒューマン)
- Later 9 : The organization (組織)
- Layer 10 : Government or legal compliance (政府，法)

そして，Layer 8 であるヒューマン層に対するセキュリティ対策として，ユーザ単位や業務部門単位にインターネットへのアクセス制御を行ったり，利用可能なアプリケーションの制御を行ったりするセキュリティ製品が販売されている[40].

この様に，情報セキュリティ（ネットワークセキュリティ）において，システムレベルのセキュリティから，更に上位のヒューマンレベルでのセキュリティ対策が講じられる様になってきている.

1.4 新性格検査とビッグファイブ

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[41]．性格を構成する要因それぞれの影響力は個人毎に異なり，それによって個性が形成されていると考えられる[42]．本研究で構築するインシデントモデルでは，幼児期に形成され経験や年齢による影響を受けにくい性格を対象とするが，それを測ることは困難なため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した結果を用いるものとする．

性格検査には幾つか種類があるが，本研究では新性格検査とビッグファイブを参照し行う．

1.4.1 新性格検査

新性格検査とは文章形式の性格テストで，12 の性格特性尺度と 1 つの虚構性尺度の 13 尺度を用いて性格の多面的特性を測定するもの[42]である．各特性は 10 項目からなり，合計 130 項目の質問を通じて点数化し，どの性格特性が強いかを判定する質問紙法性格検査である．なお，質問紙法性格検査としては YG (谷田部・Guilford) 検査が広く用いられていたが，尺度の因子的妥当性やそれらの独立性に問題があることが指摘されている．

本研究では，新性格検査 (虚構性を除く 12 尺度) を用いて対象者の性格特性の傾向を判定するものとする．それぞれの尺度は，以下の通りである．

- 社会的外向性
  他者に対して常に関心を持っていて，人と広く付き合うのが楽しく対人接触を好む性格．

- 活動的
  仕事が速く動作がキビキビしている等，肉体面精神面の両方にまたがる活動的な性格．

- 共感性
  相手が感じたり，考えたりしている事を，あたかも自分がそうであるかの様

に感じ取れる性格.

- 進取性
  従来の慣習に拘らず，進んで新しい事をしようとする性格.

- 持久性
  最後までやり遂げたいという粘り強さを持っている性格.

- 規律性
  自他に対する道徳的態度，一定の秩序・決まりを守ろうとする性格.

- 自己顕示性
  自分を際立って目につくようにする性格.

- 攻撃性
  攻撃行動が生み出される心理過程（攻撃な思考や関心，攻撃的な感情，攻撃への意欲や願望).

- 非協調性
  不満が多い，人を信用しない等の不満性と不信性が強い性格.

- 劣等感
  劣等感に悩まされる，自信が無い等の自己の過小評価，不適応感が強い性格.

- 神経質
  心配性，神経質，ノイローゼ気味，イライラする等の性質がある性格.

- 抑うつ性
  度々憂鬱になる，理由もなく不安になること等がある性格.

これらの特性を人はどれも持っているものであり，新性格検査はその特性の強弱を数値化して評価するものである．例えば，図 1-16 の様に社会的外向性や進取性が高く，自己顕示性や活動性がやや高い，というように，持っている特性の強さが数値の高さで表現される.

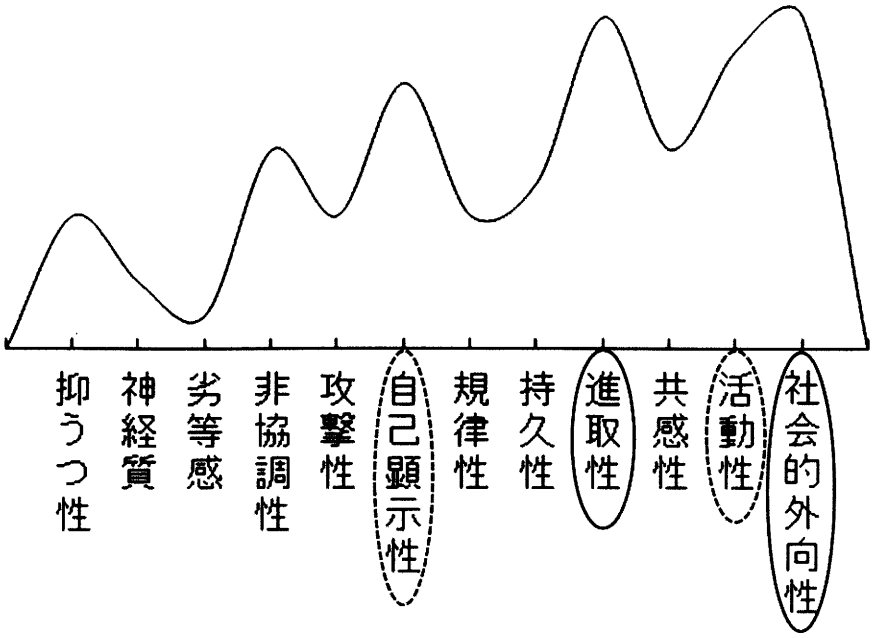


図 1-16. 新性格検査

1.4.2 ビッグファイブ

性格特性を 5 つの特性因子によって包括的に記述するモデルで，元々は辞書等から得られる性格特性を表す語の分類研究や，性格尺度の再分析，或いは複数の尺度から項目を収集し，因子分析によって因子を抽出する研究等を経て 5 因子が抽出され出来たものである．研究者により異なることがあるが，概ね以下の 5 つの尺度が用いられる[43],[44],[45],[46],[47],[48],[49].

- 外向性 (Extraversion)
  - タイプ

    社会や物質に対するエネルギッシュなアプローチをするタイプ．激情型，エネルギー，熱狂，社交性，活動性，主張性，肯定的感情，リーダシップ．
  - 反対の傾向

    閉鎖的，非活動的，内向的，控えめ，よそよそしい，物静か．
- 協調性 (Agreeableness)
  - タイプ

調和性，同調性格社会性，ボランティア．

- 反対の傾向

  敵意，敵対行動，ねたみ，ひがみ，ひねくれ者，嫉妬深い，怒り，短気，身勝手，自己中心的，我儘．

- 勤勉性/良識性（Consciousness）
  - タイプ

    良心，誠実，統制，勤勉，社会的慣習やルールに基づく，計画的，親切，人情，良心，粘り強い，熱心，ひたむき，従順，謙虚，忠実．

  - 反対の傾向

    衝動的，無責任，身勝手，中途半端．

- 情緒安定性/神経症傾向（Neuroticism）
  - タイプ

    唯一否定的な要素のタイプ．情緒不安定性，否定的，不平不満，感情的．

  - 反対の傾向

    活動的，行動的，開放的，エネルギッシュ，楽観的，能天気，快楽主義，気まま．

- 知性/経験への開放性（Intelligence / Openness to Experience）
  - タイプ

    知的好奇心，知性，遊戯性，開放性，独創性，公平性，意思が強い．

  - 反対の傾向

    小心，意気地なし，軽率，不注意，間抜け，軽はずみ，意志薄弱，中途半端．

1.5 研究テーマと目標

1.5.1 本研究の動機

これまでの情報セキュリティ対策はネットワークや利用するシステムへの技術的な対

策と，その運用管理に関する情報セキュリティマネジメントの導入による対策のみであったため，上述した様に人的要因であるヒューマンエラーによる事故についての対策が遅れ，事故の発生に結びついている．これは 1980 年代にシステム化が進んだことにより，事故が故障等からヒューマンエラーにシフトしたことと類似している．

交通事故や一般的な事故について，ヒューマンエラーと性格との相関に関する研究は行われ，その成果が例えば車の運転における適正診断等に活かされている．しかし，情報事故に関する研究は見つかっていない．

また組織の情報セキュリティ対策を検討には，精緻なインシデントモデルが有用である．これまでのモデルは，図 1-14 に示す意図的で人為的な情報事件（情報犯罪）に対するもので，様々な情報セキュリティ対策製品がある．しかし図 1-5 で示されるように，情報事故，特に組織にとって運営を左右する情報漏えい事故の原因の 80%がヒューマンエラーによるものであることに鑑みると，人的要因を考慮した形でのインシデントのモデル化が重要である．しかし未だモデル化が行われず，利便性は二の次に運用をより厳しくし対応しているのが実情である．

そこで本研究では，情報事故の主要因であるヒューマンエラーに焦点を当て，その原因の重要なファクターであるユーザの「性格」に着目し，これまでされてこなかった人的要因を考慮した形でのインシデントのモデル化のため，セキュリティ意識と性格との相関を明らかにし情報事故に対するインシデントモデルを構築しようと考えたのが，本研究の動機である．

1.5.2 本研究のテーマと目標

本研究では，1.4.1 で述べた通り，セキュリティ意識と性格との相関を明らかにし，人的要因を考慮した形での情報事故に対する精緻なインシデントモデルを構築し，情報事故を低減することを目標としている．この目標を達成するため，情報事故における性格と教育とに関する 2 グループモデルを提案する．2 グループモデルとは，そもそも事故を起こしやすい性格特性が強いグループと事故を起こしにくい性格特性が強い（事故を起こしやすい性格特性が弱い）グループとが存在し，かつ教育等により事故を起こしにくくなるグループと，教育を受けていないため事故を起こしやすいグループとに分かれる，ということを表したモデルである．本論文では，この 2 グループモデルの妥当性を

示し，ヒューマンエラーによる事故を低減するシステムを提案する．

そこで，本研究では2グループモデルの妥当性を示すために，以下のアプローチを採った．

STEP1

これまで多くの調査がなされている交通事故に関する既存研究を元に，交通事故と性格の関係を演繹する．交通事故においては，事故を起こしやすい性格特性と事故を起こしにくい（事故に関与しない）性格特性とがある．また，シミュレータを用いた教育等により，事故を起こしにくくする効果がある．これを情報事故のインシデントモデルに写像することで，性格特性の傾向と教育に応じてユーザを 4 つのグループに分ける「性格 2 グループ×知識 2 グループ」型のインシデントモデルを導く．

STEP2

教育を受けた社会人に対するヒューマンエラーに関する既存研究を元に，ヒューマンエラーを起こしやすい性格特性（性格 A）とヒューマンエラーを起こしにくい（もしくは起こしやすさに関与しない）性格特性（性格 B）があることを示す．情報事故の8割以上がヒューマンエラーによって引き起こされることから，セキュリティ教育を受けたユーザ（一般社会人）のインシデントモデルが，ヒューマンエラーを起こしやすい性格特性が強いグループと，ヒューマンエラーを起こしにくい性格特性が強いグループの 2 つに分かれることを裏付ける．

STEP3

大学1年生約400名を対象に本人認証におけるセキュリティ意識に関する質問紙調査を行い，セキュリティ意識が低い傾向にある性格特性（性格 C）と高い傾向にある性格特性（性格 D）があることを明らかにする．認証情報の取り扱いに関する意識の低さが情報事故の温床となっていることから，セキュリティ教育の初学者（ノービス, novis）である大学1年生のインシデントモデルも，セキュリティ意識が高い性格特性が強いグループと，セキュリティ意識が低い性格特性が強いグループの2つに分かれることを示す．

STEP4

セキュリティ教育を受けたユーザ（STEP2）もセキュリティ教育の初学者（STEP3）も，事故を起こしやすい性格特性が強いことは類似しており（性格 A と性格 C），かつ事故を起こしにくい性格特性が強いことも類似している（性格 B と性格 D）ことを確認する．“三つ子の魂百まで”という諺が示す様に，幼児期に形成された性格は年齢や経験による影響を受けにくいと言われていることから，情報事故においても，事故を起こしやすい性格特性が強いグループと事故を起こしにくい（もしくは関与しない）性格特性が強いグループとがあり，それぞれの性格特性が強いユーザの中で，教育による知識の程度で事故を起こしやすいグループと事故を起こしにくいグループとに分かれるという「性格 2 グループ×知識 2 グループ」型のインシデントモデルが妥当であることを示す．

本研究によって構築された性格 2 グループ×知識 2 グループ型のインシデントモデルを利用することによって，組織のセキュリティ対策の選定やユーザ教育の方法を効率化することが可能となると期待される．

1.5.3 本論文の構成

本論文は，1.4.2 で示した様に「性格 2 グループ×知識 2 グループ型」インシデントモデルの妥当性を示して構築し，その考え方に基づきヒューマンエラーによる事故を低減するシステム提案に関する研究をまとめたものである．本論文は，以下の構成となっている．

第 2 章では，1.5.2 項で示した STEP 1～4 について示す．まず交通事故（違反）者と性格との相関，及び教育との相関に関する調査研究から，交通事故（違反）者と性格や教育との間に相関があることを示し，交通事故（違反）における「性格 2 グループ×知識 2 グループ」型のインシデントモデルを示し，その妥当性を示す（STEP 1）．そして，情報事故はヒューマンエラーが主な原因であることから，教育を受け知識（スキル）がある一般社会人におけるヒューマンエラーと性格とに関する調査研究を行い，一般社会人における情報事故と性格との相関について明らかにする．そして，教育を受け知識（スキル）がある場合の「性格 2 グループ×知識 2 グループ」型のインシデントモデルの妥

当性を検証する (STEP 2). そして，教育が充分でない初学者に対して，我々が行ったアンケート調査から情報セキュリティ意識と性格との間に関係があり，初学者においても「性格 2 グループ×知識 2 グループ」型のインシデントモデルが妥当であることを示す(STEP 3). そして，セキュリティ教育を受けた一般社会人もセキュリティ教育の初学者も，事故を起こしやすい性格特性が類似し，かつ事故を起こしにくい性格特性も類似していることを確認する．情報事故においても，交通事故と同様に事故を起こしやすい性格特性が強いグループと事故を起こしにくい（もしくは関与しない）性格特性が強いグループとがあり，それぞれの性格特性が強いユーザの中で，教育による知識の程度で事故を起こしやすいグループと事故を起こしにくいグループとに分かれるという「性格 2 グループ×知識 2 グループ」型のインシデントモデルが妥当であることを示す (STEP 4).

第 3 章では，第 2 章で示した STEP 2 の教育が充分でない初学者に対して，利用者の意識が強く関わる利用者認証と情報セキュリティ意識，そして性格との相関について行った質問紙によるアンケート調査と，その結果に基づく分析について詳細に述べ，情報セキュリティ意識と性格との間に関係があることを示す.

第 4 章では，2 グループモデルに基づき，ヒューマンエラーを低減するシステムを提案する．一つは，性格検査に基づくデータベースを活用した Best Match Security (BMS) データベースの提案である．もう一つは，2 グループモデルに基づく ISMS 運用に関する提案である．最後に，本研究では性格と教育を軸にしたモデルで進めたが，注意もヒューマンエラーの重要な要因と考えられる．そこで，注意を軸に加えたインシデントモデルについて述べる.

第 5 章で本論文の考察を行い，第 6 章で本論文をまとめる.

第2章 交通事故にみる性格と違反者との相関に関する調査研究

2.1. はじめに

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．しかし，事故と性格について調査した文献は乏しく，情報事故に関しては見つかっていない．

そこで本章では，これまで多様な視点で研究がされて効果を上げている交通事故や違反者と性格とについて調査研究を行い，性格も事故や違反に深く関わっていることを示す．交通事故の場合，事故（違反）多発者や重大事故を起こす場合について，運転適性として性格と事故・違反との相関について調査されており，結果が適正診断として活用されている[50].

情報セキュリティにおいても，1.2.7 項で述べた通り，システムセキュリティだけでなくヒューマンセキュリティも注目されるようになっている．そこで，システムを操作するユーザの心理が，情報事故の発生にどの様な影響を及ぼしているか調査することは重要である．この様な観点から，交通事故・違反と性格について調査し，交通事故における性格と教育に関するインシデントモデルを構築し，それを情報事故へ写像することを試みるものである．そこで，情報事故の多くが人的要因による，即ちヒューマンエラーを原因としたものが多いことから，既存研究を援用し教育を受けた一般社会人においてもヒューマンエラーと性格とに相関があり交通事故のモデルを情報事故へ写像し，その妥当性を示す.

2.2. 交通事故と性格と教育との相関（STEP 1）

交通事故における意図的な不安全行動には，酒酔い運転や携帯電話を持ち通話しながらの運転や信号無視等の違反を伴い事故の発生を高める行動がある．交通事故を防止するためには，ヒューマンエラーを防止するための行動レベルの対策（一時停止しましょう，など）ではなく，ヒューマンファクターのレベルでの対策を行うことが大切である．即ち，心理的に注意を向ける，意識する事が大切である.

そこで本章では，交通事故の原因の多くがヒューマンエラーであること，ヒューマンエラーには性格が大きく関与していること，から交通事故（違反）と心理的要因，即ち

性格との関わりに着目し，更にヒューマンエラーを防止する為に効果的なのは教育による知識（スキル）の向上があることから，性格と教育とを軸にした交通事故におけるインシデント・モデルを構築する．

2.2.1. 交通事故と性格との相関に関する調査研究

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[51]．

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[52]．

また文献[53]では，交通事故や違反と身体機能，運転意識等の関係として，図 2-1 の様な概念で考えている．

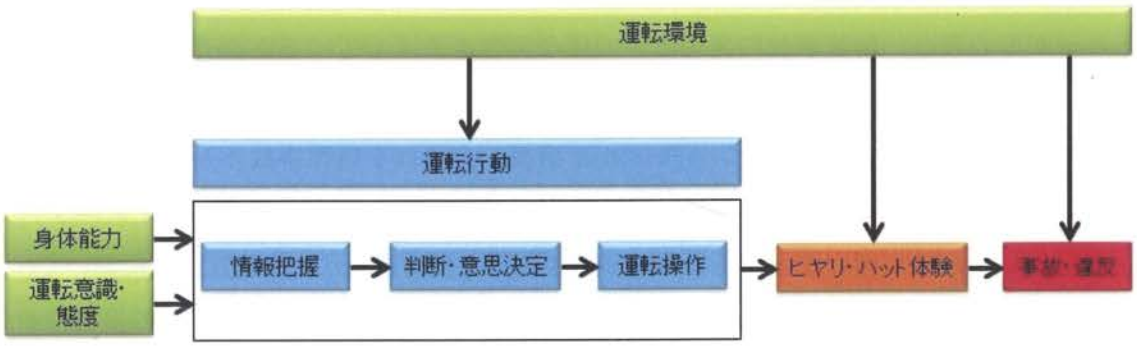


図 2-1. 交通事故・違反と身体機能，運転意識などの関係[53]

図 2-1 では，交通事故や違反の基本要因として，身体能力と運転意識・態度を位置付けている．この 2 つの要因が，運転行動である情報把握，判断・意思決定，運転操作という一連の行動に影響を与える．この運転行動に問題があれば，即ち不安全行動をとれば，たとえ大きな事故には至らなかったとしても，事故に遭いそうになる，もしくは事故を回避してヒヤリとしたりハッとしたりするインシデントであるヒヤリ・ハット[54],[55],[56]体験が発生する．違反をしたからといって，必ずしもヒヤリ・ハット体験につながるわけではないが，不安全行動の回数が多ければヒヤリ・ハット体験は確実に増加し，それに運転環境の条件が重なった時に，事故・違反につながるのである．

交通事故原因の 6 割は思い込みと言われている．思い込みとは，ヒューマンファクタ

ーでは個人レベルのファクターで心理的要因に含まれる．ここでヒューマンファクターとは，“人間の運転，作業，仕事などの活動に影響を及ぼす『個人的要因』及び個人に影響を与える『集団・社会的要因』”と定義される[21]．また個人レベルのヒューマンファクターの心理的要因には，感情・情動，急ぎ・焦り，思い込み・思い違い，面倒等がある．特に，交通事故においては，思い込みが不安全行動の背後にあると考えられる．思い込みとは錯誤であり，夜更けには車が通るはずがないと思い込んだり（時間帯の錯誤），ここは車が通らないと思い込んだり（経験の錯誤）する．

前述の通り，交通事故を防止するためにはヒューマンエラーを防止するための行動レベルの対策ではなく，ヒューマンファクターのレベルでの対策を行い，心理的に注意を向ける，意識する事が大切である．

交通事故を起こしやすい性格については，様々な見解[51],[52],[57],[58]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[5]．

(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．

(2) 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．

(3) 感情の起伏が激しい．

- 情緒不安定なタイプである．

(4) 協調性に欠ける．

---

5 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．

– 他人とうまく付き合おうとする気が欠けている.

(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, およびビッグファイブとの対応を, 文献[59], [60]を参照しまとめたものが表 2-1 である. 表 2-1から, 交通事故を起こしやすい性格というのは, ビッグファイブ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.

交通事故の主原因は思い込みであり, それは人的要因, 即ちヒューマン・エラーにより発生するものである. 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」[61]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[62]. ただし前述の通り, ヒューマンエラーの中でも純然たる過失ではなく確信的違反行為や確認義務違反が原因である[51]ことに注意が必要である.

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[63],[64]. Brown と 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[65].

表 2-1. 交通事故を起こしやすい性格と新性格検査 13 因子，およびビッグファイブとの対応

交通事故を起こしやすい性格	新性格検査 13 因子	ビッグファイブ
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[63]. 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，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[59]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[66],[67],[68].

2.2.2. 交通事故と教育との相関に関する調査研究

交通事故はドライバーの思い込み（不注意）や制限速度超過等の不安全行動（リスク・テイキング行動）により発生する. 交通事故を防止するために教育は効果的で, 特に交通事故防止にはシミュレーションに代表される疑似体験教育が効果的である[66], [69], [70], [71]. ここで, リスクテイキング行動はリスクを承知でリスクを取る行動を対象とする立場[72]と, リスクを把握しているか厳密に考えず事故の可能性がある行動全てをリスクテイキングの対象とする立場[73]がある. 追い越しや信号無視は明らかな意思を持った行動であるが, 多くのドライバーの運転の意思決定は不明瞭な部分があるため, 後者の Trimpop の考え方を採用する.

さて, これらの教育は, ドライバーの不安全行動を抑止することが交通事故防止に直結するが, そのためにはリスク知覚とハザード知覚を高めることが重要である. リスク知覚を成立させる心的過程として, ハザード知覚, リスク効用, 自己技能の評価等が重要視されている[63].

リスクには, スリルを味わうタイプの自発的リスク（voluntary risk）と, 災害や事故等の非自発的リスク（involuntary risk）の 2 種類があり, 非自発的リスクは通常回避行動を取るものであるが, 治療のために手術のリスクを冒す等, トレードオフの原理が働く場合がある, 自発的リスクは若年層がとりがちなリスクで, ハザード性の高い状況を年長ドライバーほど危険だとみなさないことから, 運転技能が要求される場面でリスクを低く知覚する[74].

ドライバーのリスクテイキング傾向を防ぎ, 回避行動を促進するには, 単にハザードとは何か, リスクとは何かを教えるだけではなく, 何が正しい行動か, 自分の運転を正しく見る“スキルのメタ認知”と呼ばれる危険対象を予測し, 早期発見をする能力を育てることが重要である.

このためには, ドライバーのリスク知覚を高めるためにドライバーのハザード知覚を育成し, 自己評価能力を高め, リスク回避の意思決定と行動の方を習得させる必要がある. 即ち, そのための教育が必要であり, 単にケーススタディとして伝えるのではなく, スキルのメタ認知を高める教育が必要である. 即ち, 実質的な技能向上と安全態度の改善につながりつつ, 自分の能力に対する主観的評価は低下する様な教育が望ましい[75],[76]. 逆に, 教育によりリスク知覚とハザード知覚が高まり, リスク回避行動を優先して取るようになれば, 事故を防止することにつながる.

2.2.3. 交通事故におけるインシデントモデル

2.2.1 項から交通事故には，起こしやすい性格特性と起こしにくい性格特性があることが分かった．また 2.2.2 項から，運転シミュレータ等による教育や擬似経験により，リスク回避行動をとり事故を起こしにくくなることも分かった．

また安全管理業務において，性格と業務，年齢という異なる性質の特性間には，特に関連性が見られないという報告[77],[78],[79]がある．このことから，業務の経験や事故体験事例数，年齢等に性格は影響を受けにくく変化しにくいことが分かる．

以上から，まず図 2-2 の様に性格により事故を起こしやすいか，そうでないかの 2 つのグループが存在する．

図 2-2. 交通事故を起こしやすい性格特性の強弱でグループが分かれる 2 グループモデル

また交通事故防止には，運転シミュレータ等の教育でリスク回避行動を促進させる効果があり，リスクのメタ認知を高められることが期待される．即ち図 2-3 の様に，初学者でスキルがなくリスク回避傾向が低いグループと，教育を受けたスキル習得者でリスク回避傾向が高い 2 つのグループに分かれる．

図 2-3. 教育の有無でリスク回避傾向の高低が分かれる 2 グループモデル

教育効果は性格には依存しないことから，交通事故を起こしにくい性格特性が強いグループ

であっても，性格以外の因子により交通事故を起こしやすい人がいた場合，その人も教育によりリスク回避行動を取れるようになり，事故を起こしにくくなることが考えられる．

以上から図 2-2，2-3 は，図 2-4 の様なモデルにまとめられる．

図 2-4 は，第 1 象限の群が事故を起こしにくい性格特性が強いグループで，かつ教育によりリスク回避傾向も高く，理想的なタイプといえる．第 4 象限の群は事故を起こしにくい性格特性が強いグループで，適切な教育を受けることで第 1 象限の群になりリスク回避行動を取るようになり事故を起こしにくくなる．ここで行う教育は（擬似的な）体験を伴い，完全に忘れることは少ない．従って，教育の効果により第 4 象限から第 1 象限に移行すると第 4 象限に戻ることはない．

一方，事故を起こしやすい性格特性が強いグループの第 3 象限の群は，教育を受けることでリスク回避傾向が高くなり第 2 象限の群となり，第 3 象限の群に比べて事故を起こしにくくなる．ここで行う教育も（擬似的な）体験を伴うエピドード記憶であり，忘れることはないものであるため，第 3 象限から第 2 象限に移行すると第 3 象限に戻ることはない．

ここで，教育により第 3 象限から第 1 象限（もしくは，第 4 象限から第 2 象限）へ移ることが考えられる．しかし，本研究では年齢や経験による影響を受けにくい幼児期に形成された性格を対象としているため，教育により第 3 象限から第 1 象限（もしくは，第 4 象限から第 2 象限）へ移ることは無いとする．

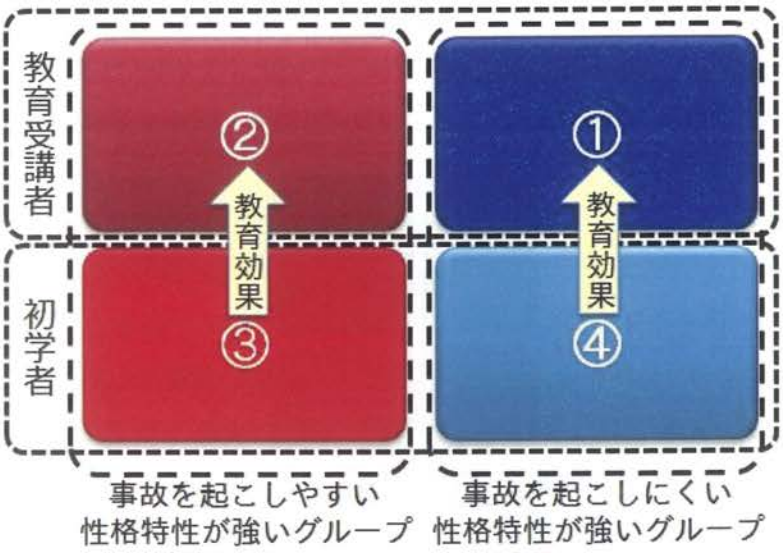


図 2-4. 交通事故における性格と教育とを考慮したインシデントモデル

2.3. 一般社会人におけるヒューマンエラーと性格との相関に関する調査研究 (STEP 2)

2.2 節では，交通事故を起こしやすい性格特性や原因，リスクテイキング行動，そして交通事故防止のための疑似体験等の教育効果に関する既存研究から，図 2-4 の交通事故における性格と教育とを考慮した「性格 2 グループ×知識 2 グループ」型のインシデントモデルを導出した．そこで，図 2-4 で示したンシデントモデルについて，教育を受けた一般社会人においても，ヒューマンエラーと性格とに関してモデルが成立するか，既存研究からその妥当性を示す．

2.3.1. 情報事故と性格との相関

一般に情報システムの安全性を高めるためには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．情報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た研究が行われ，情報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った．それに加え，情報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．

個人情報漏えいインシデントに焦点をあてた報告[3]においても，やはり同様の知見が得られている．図 1-5 に示す様に管理ミス，誤操作，紛失・置忘れ等のヒューマンエラーが情報漏えいの原因の上位約 80%を占めている．

金らは，企業での情報事故の発生原因の 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[80]．大和田らは，情報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[81]．これらから，危険源の見落としによる情報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[82]ところが小さくないことが分かる．

廣瀬は，性格のビッグファイブ（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[82]．ここで，各エラーは事前に原子力発電所で発生するエラーについて調査した結果で，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．その結果を表 2-2 に示す．廣瀬は，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[82]している．表 2-3 は，結果を(+)と(-)で表現したもので，表中の (+) は正の相関を表し，(-) は負の相関を表す．

表 2-2. エラー因子と性格因子の相関分析結果[80]

性格因子 / エラー因子	外向性	協調性	勤勉性	情緒安定性	知性	いい加減さ	気の弱さ	軽率さ	自制心の弱さ	疲れ易さ
忘却	-.0963	-.1563	-.3658	-.1479	-.1995	.4701	.3741	.3526	.2534	.3128
	n.s.	n.s.	***	n.s.	*	***	***	***	**	***
注意の偏り	-.0228	-.2121	-.4313	-.4257	-.2850	.5109	.3691	.5235	.3421	.2784
	n.s.	*	***	***	***	***	***	***	***	**
入力	.0200	-.2401	-.4990	-.2193	-.3272	.4029	.3336	.6038	.4150	.3084
	n.s.	**	***	**	***	***	***	***	***	***
短絡的思考	-.0932	-.2448	-.4713	-.2353	-.3424	.3587	.4561	.3587	.1937	.4072
	n.s.	**	***	**	***	***	***	***	*	***

*:p<.05, **:p<.01, ***:p<.001
網掛けは，r=±0.4 以上の相関が見られたものを示す。

表 2-3. ヒューマン・エラーと相関の高い性格

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[5]．この様に，一般的なヒューマンエラーにおける不安全行動をとってしまう理由や，廣瀬の結果[82]や竹村の結果[5]から，情報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，情報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情報事故の誘発につながる，ということが推測される．

即ち，教育を受けた場合であっても，事故の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り，図 2-4 の様に教育効果がある場合も，第 1 象限と第 2 象限の様に性格によりグループが分かれることが示された．

2.3.2. 交通事故と情報事故との類似点と相違点

2.2 節で示した交通事故と性格との相関に関する調査研究と，教育に関する調査研究，及び 2.3.1 項の調査研究から，交通事故とヒューマンエラーに共通することは，どちらも性格によるものが大きいという点である．

表 2-3 から，ヒューマン・エラーに相関が高い性格は，ビッグファイブ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，どちらの事故も初学者でスキルが乏しい場合，リスク回避傾向が低く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機密性）の知覚と置き換えられ，情報システムやサービスを利用する環境（社内環境なのかモバイル環境なのか，周囲に誰もいないか満員電車の中なのか，など）の知覚と言える．このことから，情報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．

2.4. 初学者における情報事故と性格との相関（STEP 3）

2.3 節では教育を受けた一般社会人におけるヒューマンエラーと性格との相関に関する調査研究から，ヒューマンエラーを起こしやすい性格特性と起こしにくい性格特性とがあり，かつ情報

事故の多くがヒューマンエラーによるものであることから，情報事故においても事故を起こしやすい性格特性が強いグループと，事故を起こしにくい性格特性が強いグループとに分かれることを示した．

一方，情報セキュリティ教育が十分でない初学者については，これまで研究が行われておらず，事故の起こしやすさと性格との相関が分かっていないため図 2-4 における第 3 象限と第 4 象限とに分かれることについては明らかにされていない．そこで我々は，情報セキュリティに対する教育がまだ十分でなく，決済を伴うネットワークサービスや，様々な情報システムやサービスのりよう経験が少ない大学 1 年生を情報セキュリティ教育の初学者とし，本人認証についての情報セキュリティ意識と性格について，400 人規模での質問紙によるアンケート調査を行った[83]，[84]．なお，最近では，高校でも情報セキュリティの教育を受け，携帯電話やスマートフォンを操作する学生も少なくない．しかし，ネットワークを使った様々なサービスや電子決済等に触れる機会は社会人ほど多くはなく経験も乏しいと考え，大学 1 年生を初学者と定義した．

2.4.1. 本人認証に関するセキュリティ意識と性格との相関

本人認証は，記憶による認証，持ち物による認証，生体情報による認証の 3 つがある．そこで，大学 1 年生がイメージしやすい様に記憶による認証としてパスワード認証を，持ち物による認証として IC カード（銀行系カード，学生証，等）を，生体情報による認証として指紋や虹彩等の生体情報を用いた認証を取り上げた．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安全性に関与すると考えたからである．また，情報セキュリティ意識を取り上げたのは，1.2 節で示した様に，情報セキュリティ意識が低いと問題行動を取りやすくなり事故を起こしやすいからである．

それぞれの本人認証について，情報セキュリティ意識について質問紙によるアンケート調査を行い，また対象者に対して行った新性格検査とから，本人認証に関するセキュリティ意識と性格との相関について調査した．本項では，質問紙によるアンケート調査結果について概要のみ示し，詳細は第 5 章で述べることとする．

調査の結果を，表 2-4 に示す．

表 2-4. 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

	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

表 2-4 の結果と廣瀬の結果[82]から，事故を起こしやすい性格をまとめたものが図 2-5 である．図 2-5 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．持ち物認証でマイナスに働く社会的外向性に当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，これは本研究での調査がセキュリティ意識を対象にしており，ヒューマン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．

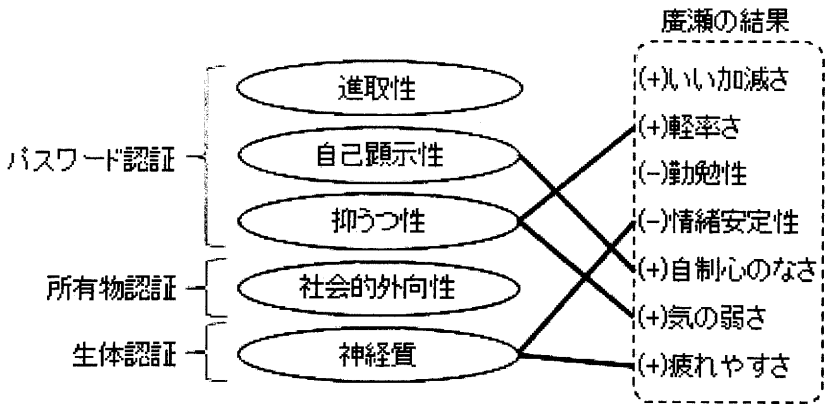


図 2-5. 事故を起こしやすい性格の共通因子

よって，ヒューマンエラーを起こしやすい性格と，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，情報事故を起こしやすい性格特性と起こしにくい（もしくは関与しない）性格特性とがあることが分かり，それは既存研究[82]の結果とほぼ一致している．

また廣瀬は教育を受けている一般的な社会人を対象とし，2.3 節で図 2-4 における第 1 象限と第 2 象限について明らかにしたと言える．さらに，本節では第 3 章で示す本研究での教育が十分でない（スキルが十分でない）初学者である大学 1 年生に対して調査から，図 2-4 における第 3 象限と第 4 象限について明らかにしたと言える．以上から，図 2-6 に示す様に情報事故についても，図 2-4 に示す「性格 2 グループ×知識 2 グループ」型のインシデントモデルが成立することが示された．

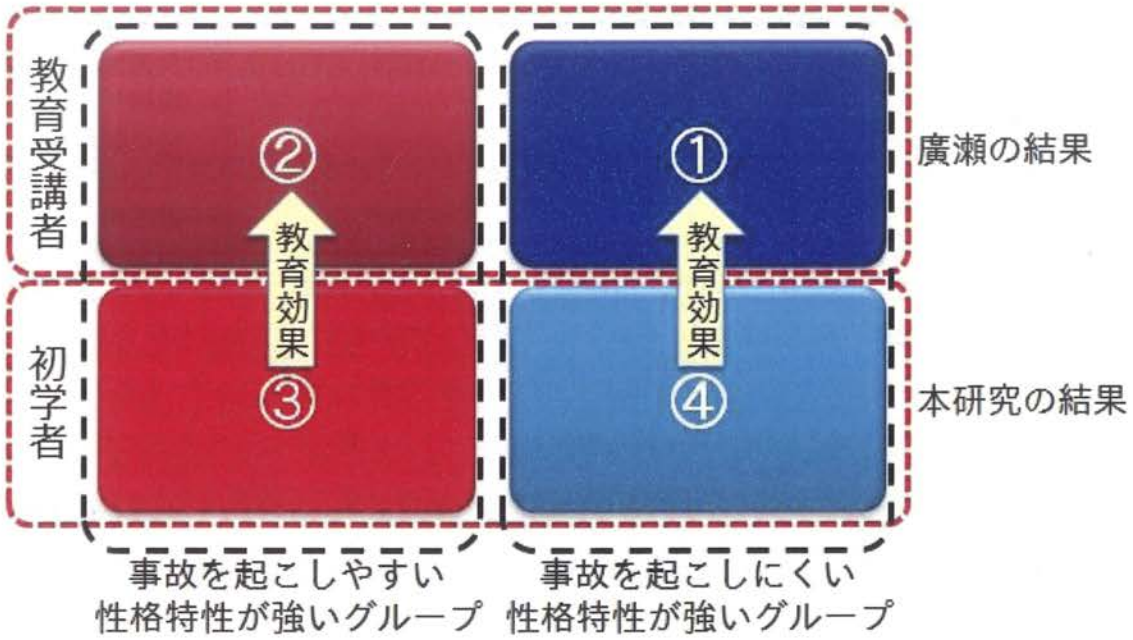


図 2-6. 情報事故における「性格 2 グループ×知識 2 グループ」型のインシデントモデル

2.5. まとめ

本章では，交通事故と性格，および教育に関する既存研究から，

- 交通事故を起こしやすい性格特性がある．
- シミュレーションによる疑似体験を用いた教育により，リスク知覚やハザード知覚を高めリスク回避行動を促進することで，事故を起こしにくくすることができる．

- 疑似体験による教育は，エピソード記憶であり一度習得したものは忘れることがない．

ということが分かった．

交通事故と情報事故に共通することは，どちらもヒューマン・エラーが発生原因の大きな要因であり，性格によるところが大きいという点である．但し，他の交通事故原因である運転操作，能力等は，情報事故とは関係がないと考えられる．

表 2-3 から，ヒューマン・エラーに相関が高い性格は，ビッグファイブ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．即ち，勤勉性の低さもスキル向上の意識が低く，リスク回避傾向の低下を招き事故を起こしやすくなると考えられる．

また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機密性）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，周囲に誰もいないか満員電車の中なのか，など）の知覚と言える．

これらの知覚が乏しいと，リスクテイキング行動をとりがちになり事故を多発する一方で，（昇進や新たな責務を負う等の）経験や教育を受けることで，リスク回避傾向が高くなり事故を起こしにくくなる．

上記の結果を元に，図 2-2，図 2-3 の 2 グループモデルが導き出され，さらに 2 つを合わせた図 2-4 の 4 つの象限に分かれる性格特性の傾向と教育に応じてユーザを 4 つのグループに分ける「性格 2 グループ×知識 2 グループ」型のインシデントモデルが導き出された．

また情報事故に関する既存研究から，情報事故の主原因がヒューマンエラーであり，情報事故防止のために教育が重要であることも分かった．さらに 2.3 節で示した廣瀬の結果から，一般的な教育を受けた社会人について，種別を 4 種類に分類したヒューマンエラーと性格（ビッグファイブ）との相関があることが分かった．以上から，教育を受けた一般社会人においても情報事故に関して図 2-4 の「性格 2 グループ×知識 2 グループ」型のインシデントモデルにおいて第 1 象限と第 2 象限に分かれることが示された．

2.4 節では，2.2 節で示した交通事故（違反）と性格との相関に関する結果と，2.3 節で示し

た教育を受けた（スキルがある）社会人に対する事故と性格との相関に関する結果と，2.4 節で示した教育が充分でない（スキルがない）大学 1 年生に対するアンケート調査から得られた情報セキュリティ意識と性格との相関に関する結果とから，情報事故に関しても図 2-4 に示す「性格 2 グループ×知識 2 グループ」型のインシデントモデルが当てはまることの妥当性を示した．

以上から，情報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り，ケーススタディ等の経験や教育によりスキル低下を防止することも重要であり，情報事故においても図 2-6 の「性格 2 グループ×知識 2 グループ」型のインシデントモデルが妥当であることが分かる．

第3章 利用者認証と性格とセキュリティ意識とのアンケート調査の結果と相関

3.1. はじめに

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格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[85]．

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，ISMS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情報事故を防いでいる．しかし，それでもなお，情報事故をなくすことは出来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）十分な情報セキュリティに関する教育を受けておらず，情報事故や被害に関わった経験も少ないため，情報事故（もしくはヒヤリ・ハット）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一層の安全性を高める工夫が必須だといえる．

2.3節は会社等の組織で既に教育を受けた一般社会人に対する研究で，著者らが知る限り教育を受けていない（スキルや経験に乏しい）初学者に対しての研究は行われていない．

そこで本章では，2.4節で示した調査の詳細を述べる．具体的には，情報セキュリティに関する教育が十分でなく，情報事故やヒヤリ・ハット，それによる被害等の経験が浅い大学生1年生を対象とすることで，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，教育効果が少ない場合でも，性格により「性格2グループ×知識2グループ」型のインシデントモデルに分かれ，図2-6が妥当であることを示す．

3.2. 本研究の目的

既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）情報事故に関する経験もあるユーザ，例えば企業等に勤める社員に対して実施された調査[5]，[82]は行われている．

これに対し，十分な情報セキュリティに関する教育を受けておらず，情報事故や被害に関わった経験が浅い初学者（例えば大学１年生）に対する調査はなかった．さらに，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上で非常に有用となる．

そこで情報セキュリティ教育や情報システムの利用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[83]，[84]．当該調査では，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．

そこで情報セキュリティ教育や情報システムの利用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[83]，[84]．当該調査では，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，以下の理由による．

- 情報システムや情報サービスを利用する全員が本人認証の対象である．
- 情報システムや情報サービス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る．
- 情報セキュリティに関する知識やスキル，経験の有無とは無関係に，誰もが最初に触れる情報セキュリティ対策である．
- 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，ユーザのセキュリティ意識が大きく関連し，セキュリティ意識の高低で安全性が決定する．
  - パスワード管理の運用，IC カード等を常に所持すること等に対する得手不得手

例えばパスワードについては，“123456”，“password”，“12345678”，“abc123”，“qwerty”がよく使われているパスワードで，ユーザのセキュリティ意識が低いと個人にとってではなく一般に安易なパスワードを設定する傾向がある[86]，[87]，[88]，[89]．パスワード解読技術も進歩しており，数字だけならば，20 桁程度であっても瞬時に解読でき，また Windows のアドミニストレータのパスワードを解読するツールも公開されている[90]．

なお，質問紙を用いた調査[83]，[84]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[91]. 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.

アンケート調査[83], [84]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. 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, 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ものである. 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を用いた調査も同時に実施した. 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う.

3.3. セキュリティ意識と性格の相関分析

アンケート調査[83], [84]と併せ情報系学部の大学一年生 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.

3.3.1. 性格, 経験, 環境とセキュリティ意識の定義

アンケート調査[83], [84]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様に定義する. 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[41]．性格を構成する要因それぞれの影響力は個人毎に異なり，それによって個性が形成されていると考えられる[42]．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），等を経験として定義する．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．

3.3.2. 調査方法と結果

調査は，2008 年 12 月に実施されたアンケート調査[84]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・時間はアンケート調査[82]と同じであるが，アンケート調査[84]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．

使用した質問紙は，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，アンケート調査[84]と同じである．ただし本調査では，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，アンケート調査[84]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[84]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．

調査の流れを以下に示す．

STEP i

被験者に性格検査を受けてもらう．

STEP ii

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．

STEP iii

STEP i，STEP ii で得られた回答から，互いの相関値を求める．

STEP iv

STEP ii で得られた各質問の回答値を被験者毎に合算し，その値と STEP i で得られた回答との相関値を求める．

STEP i で用いる性格検査には，柳井らが開発した新性格検査[42]を採用した．新性格検査は，1.3.1 項で述べた様に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ものである．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．

STEP ii 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．質問紙を付録 1 に示す．ここでは，概要を以下に述べる．

- パスワード認証

  情報処理推進機構が発表した安全なパスワードを作成するための条件[92]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時心配になるか，学生証を人に貸すか，カード毎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（認証のために幾つまで持ち物を携帯できるか，気に入った持ち物ならば幾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．その上で，被験者が生体認証を使用する場面を仮定した時の心情について，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）

STEP ii 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．

STEP iii と STEP iv では，STEP i，STEP ii 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．STEP iii では，STEP ii 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，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 3-1 の様になる．③郡は，「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郡については，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．

STEP iv では，STEP ii 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「STEP i 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，STEP ii 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し算出する．

STEP iii（各セキュリティ意識要因と各性格特性との相関値）と STEP iv（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，認証技術毎に，それぞれ表 3.1～3.6 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. また, 表 3.1～3.6 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.

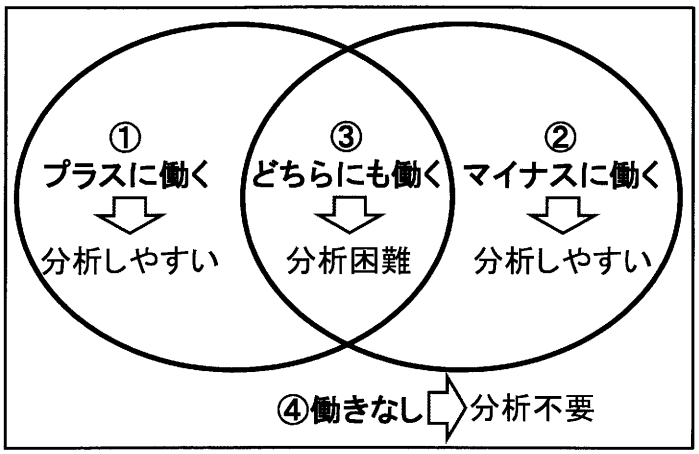


図 3-1. 相関値から分類した性格特性

表 3-1. 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[6]

	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 , † p<.10

表 3-2. 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	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

6 表 3-1 について STEP3 では，相関値を質問毎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，質問毎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 3-3. 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[7]

	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 3-4. 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[8]

	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 †

**$p<.01$, * $p<.05$, † $p<.10$

7 表 3-3 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 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を前提とし，該当者は 108 人であった．

8 表 3-4 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 3-5. 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	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 3-6. 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	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

3.4. 考察

3.4.1. STEP iii の考察

表 3-1, 表 3-3, 表 3-5 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, 3.3.2 項の①～④群の分類を行った結果を, 認証技術毎に図 3-2～3-4 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, 本節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[93]. 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[94]．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．

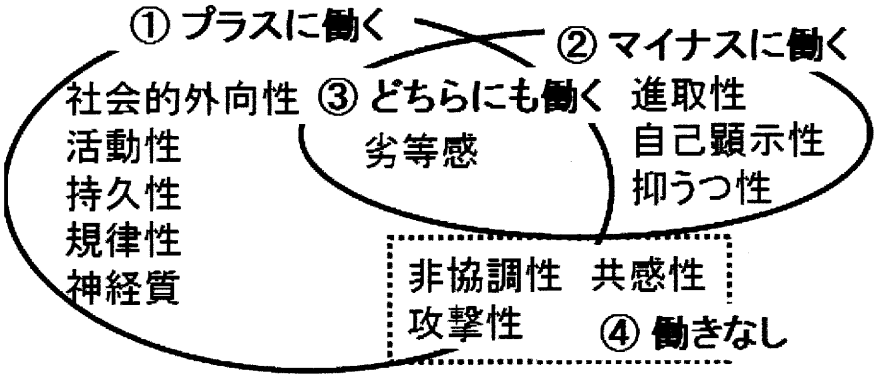


図 3-2. パスワード認証に関する各セキュリティ意識要因に影響を与える性格特性

• 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，「カード毎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[95]．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．

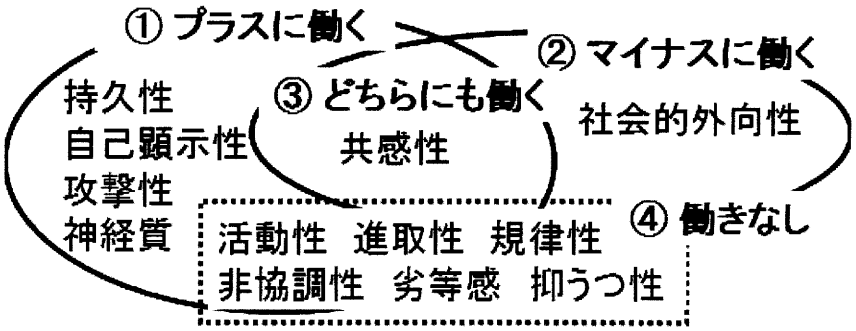


図 3-3. 持ち物認証に関する各セキュリティ意識要因に影響を与える性格特性

• 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[95]．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．

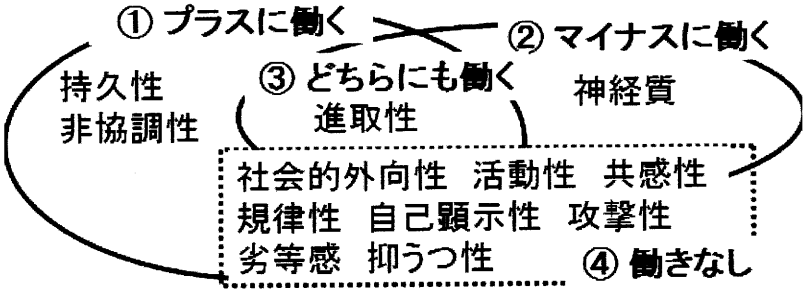


図 3-4. 生体認証に関する各セキュリティ意識要因に影響を与える性格特性

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される．

3.4.2. STEP iv の考察

表 3-2，表 3-4，表 3-6 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 3.4.1 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．本節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，STEP iii 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．出来ることなら，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，STEP iii 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．

3.4.3. パスワード認証関するセキュリティ意識と性格の正準相関分析

3.3 節の相関分析より，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，多変量解析の一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[96]．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．3.4.2 項では，各セキュリティ意識要因全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取ることで関係性を調査した．本項では，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 3-7）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

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

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

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 3-7 に示す.

表 3-7 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 つであることがわかる. 3.3.2 項の STEP ii に関する説明にて述べたように, 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 3-7 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.

表 3-7. 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）

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

3.4.4. 経験・環境がセキュリティ意識に与える影響の分析

持ち物認証や生体認証に関する本調査では，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毎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ついており，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時々しか利用しない」，「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 3.3 節，および 3.4.3 項の分析を実施している．

本項では，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，群毎にセキュリティ意識要因に違いがあるのか検証する．本研究では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ついており, 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時々しか利用しない), 群 3 (学生証カードに決済機能が付いていない) の 3 つの群毎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 つの群毎に算出したセキュリティ意識レベルの平均値を表 3-9 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上で平均値を算出している.

表 3-8. 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

	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 3-9. 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

	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 3-8 において, 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. また表 9 において, 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.

表 3-8 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 3-8 の決済機能の無い学生証カードの被験者（群 3）や，表 3-9 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 つの群毎のセキュリティ意識レベルの平均値を表 3-10 に示す．なお表 3-10 において，群 1 の被験者は 151 人，群 2 の被験者は 26 人であった．

表 3-10. 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

	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 3-10 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．

3.5. まとめ

本章では，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[83]，[84]と併せ，パスワード認証に関しては大学一年生 400 人規模の，持ち物認証と生体認証に関しては大学一年生 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．

以上から性格がセキュリティ意識に影響し，性格により意識が異なることが分かった．これにより情報事故においても，交通事故と同様に事故を起こしやすい性格と起こしにくい性格とに分かれ，図 2-6 の「性格 2 グループ×知識 2 グループ」型のインシデントモデルに当てはめて考えて良いことが示唆された．

第4章 ユーザの適正に合わせたセキュリティ対策の提案と課題

4.1. はじめに

近年，不正アクセスやコンピュータウイルス，情報漏洩などに関する事件の多発から，企業の情報セキュリティ対策は急務となっている．しかし，情報事故やインシデントは無くなることはなく，情報を扱う人間の意識にも問題があることは，これまで述べた通りである．

これは，システムでの情報セキュリティ対策に限界がきており，1.2.7 項で示した様に利用する人間性も考慮する必要性を裏付けている．また現在では，ネットワーク環境が整備されて様々な環境でサービスがシームレスに使えるようになった．特に携帯端末の進展に伴い，自宅や職場だけでなく移動中など場所を選ばすに様々な場所でインターネットを利用することができる．このため，安全確保のセキュリティ対策も一層重要なものになっている．

ところが，IT サービスの安全性を確保するために，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，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期待される効果が得られていない可能性がある．例えば，ベーシック認証でサービスが提供される場合，パスワードの忘却を恐れて自分の誕生日など安易なパスワードを設定していたり，パスワードの変更を行わず使い回したりするユーザは少なくない[97], [98]．この結果，サービスを受けるユーザにとって，認証が厳密であれば良いサービスも使われないこともある．

この様にサービスプロバイダが，どんなに良いサービスを提供しても，サービスの利用方法が不適切であれば，サービスが利用される頻度が減少することが予想される．裏返せば，それらのサービスを利用するユーザが使いやすい認証を採用することで，サービスを広く利用してもらえる可能性がある．

そこで本章では，ユーザの個性を考慮したセキュリティシステムを提供することで，情報セキュリティ対策が効果的に機能する方式の提案を行う．具体的には，ユーザの性格やセ

キュリティ意識を分析することで，一律に考えられていた情報システムの運用管理を，ユーザ個別に判定できると考えた．そこで，ユーザ毎に着目した情報マネジメントの新しい指標を提案する．例えば，面倒くさがり屋や利便性を最優先する人は，必要最低限の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，そもそも性格的に心配性のユーザは，不安を解消するために使い難くいが厳重なセキュリティ対策を施しているかもしれない．

この様に，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性格（類型的な性質の傾向）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．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れば，内面的な要因での分析評価が行える．

4.2. Best Match Security

提案システムのコンセプトを図 4-1 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．

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．

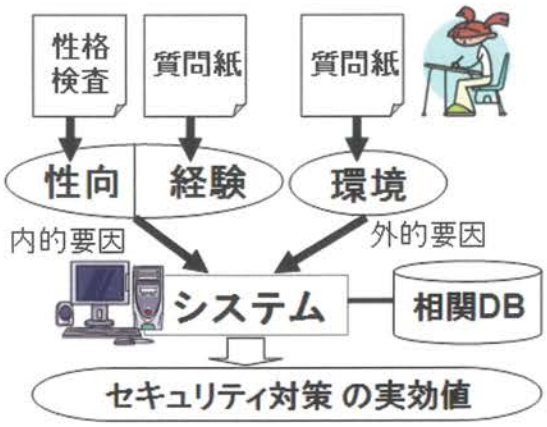


図 4-1. 提案方式の概観

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，パスワード，持ち物認証，生体認証といったユーザ認証で，どの程度正しく運用できるかを示す度合いである．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が示される．このため，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．

本節では，図 2-6 の「性格 2 グループ×知識 2 グループ」型のインシデントモデルに基づき，ユーザが属するグループでセキュリティ対策を行うことで，セキュリティレベルを維持しつつも，利便性を損なわない方式を提案する．

4.2.1. 相関 DB

提案するシステムでは，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[41]．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[42]．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，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．似通った性格を持つ者同士でも，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．

4.2.2. 性格と人間の行動特性の相関

本方式では内的・外的要因とセキュリティ意識の相関 DB を作成する．ユーザの傾向をヒヤリングするにあたり，直接的な質問を用いないことは心理学において注意すべきである[99]．このため，実際にセキュリティ対策の実効度を算出する際には，ユーザに本質を尋ねることはしない様に注意が必要である．ところが，この様な心理的試験では，複数の実験者が異なる仮説や機体を抱いている場合に，同一の実験を行なっても，各自の仮説に沿った反応を意図せずに被験者から得てしまうため，あるいは，実験者の抱く仮説・期待が微妙な手掛かりを通して被験者に影響してしまうため，実験結果に差異が生じる実験者効果が発生する[100]．これらは実験者バイアスの一つであり，3.2 節で示したように，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[91]である．この様に，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あり，直接的な質問からは計り知ることができない．以上のことから質問は間接的なものにする必要がある．そこで間接的な質問としては，本研究で用いた新性格検査を利用する等がある．

性格検査（人格テスト）は，人格という人間の基本的な行動傾向を推測する手段のひとつである．人格を正しく診断することは極めて難しく，古くから多種多様の方法が工夫されてきた．この性格検査には，質問紙法，投影法，作業法などの種類が存在し，その中で本

方式では質問紙法を採用する．質問紙法は，診断しようとする人格の特性や構成要因に基づく具体的行動例によって質問項目群を設定し，それに対する回答を求める方法である[97].

実際に性格検査を実社会に取り入れた例として，企業の入社試験に使われる適性検査，自動車教習所で用いられる OD 式安全性テスト[101]の一部などがある．これらの試験は，普段から自分で意識することのない行動傾向を測ることができることから，自己を見つめ直したり，事故に繋がる危険を回避したりするための手段として利用されている．

提案方式では，性格特性とセキュリティ意識の相関を図ることで，セキュリティに関して普段気付かなかった一面を指摘できると考えている．セキュリティ対策の運用時に起こしやすいミスを指摘することで，利用する以前からユーザが自分自身の行動に注意を向けることができる．

同時に，ユーザ本人が自覚していない能力を引き出すことができれば，その特性から本当に適したセキュリティ対策を提案できると考える．これにより，一人一人がセキュリティに関して敏感に感じ，IT 社会全体のセキュリティレベルが上がるのではないかと期待する．

4.2.3. 相関 DB の利用

相関 DB は，「どのような性格，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．この相関 DB を利用して事前に評価するシステムを構築できると考える．

具体的な手順は以下の通りである．

(1) ユーザは，あるサービスの利用を開始する前に，4.3.2 節で示したものと同型の性格検査や質問紙を用い，自分の性格や経験，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 を利用することで，そのようなタイプのユーザが各セキュリティ対策において実効度をどの程度持っているか知ることができる．

(3) システムは，実効度を適したセキュリティ対策を選定し，ユーザに提示する．

相関 DB を構築するために，ユーザの性格にのみ焦点をあてた性格検査を行う．そして，PIN 認証，持ち物認証，生体認証の利用に関するセキュリティ意識についてアンケート調査する．そして，性格とセキュリティ意識との相関について考察していく．

具体的には，被験者に対して性格検査および質問紙を用いて調査実験を実施する（図 4-2）．以下に調査の流れを示す．

STEP i

被験者に性格検査を受けてもらう．

STEP ii

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 iii

アンケート結果から各セキュリティ対策に関する意識の大きさを算出する

STEP iv

セキュリティ意識の似ている被験者に共通する性格を調べることにより，セキュリティ意識と性格の関係を分析する．

STEP i で用いる性格検査には，柳井らが開発した新性格検査[42]を採用する．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 ii では，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う．各対策案についての意識を測るための質問紙を作成する．各認証方式に対する以下の 2 つの観点からの質問であるように設定する．

1) 各認証方式を実際にどの程度安全に使えるか

2) 各認証方式に関してどの程度負荷を許容して利用することができるか

本調査では純粋な意識調査を行うために，経験や性格的な側面を出来るだけ排除したアンケートにする必要がある．質問紙を作成する際は，質問項目ごとに重み付けを行い，各対策案に関してどの程度セキュリティ意識を持っているのか算出する．この値がユーザの実効度となる．

STEP iii では，STEP ii で得た被験者の回答を集計して点数化を行い，セキュリティ意識が似ている被験者ごとに分類する．

STEP iv では，STEP iii で分類された被験者のグループごとに，STEP i により得られた 12 の性格特性に対するグループ内の平均値と分散値を算出する．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格が抽出でき，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．

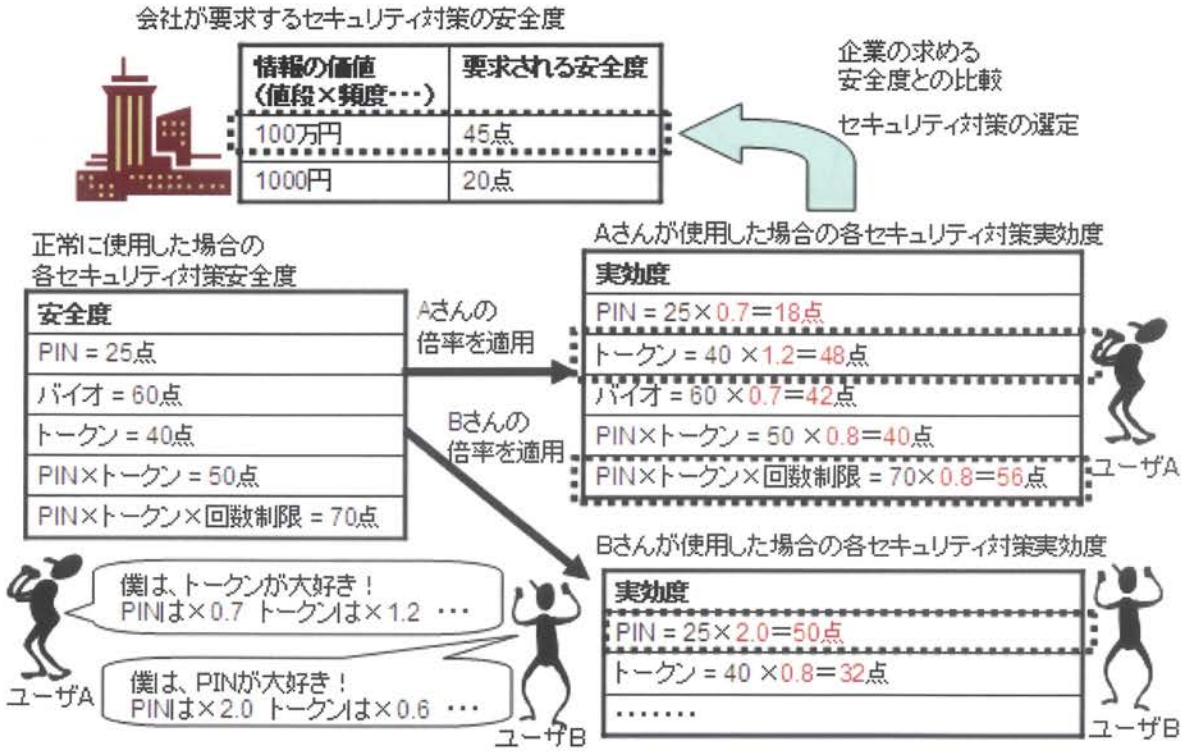


図 4-2. 提案方式の実用例

4.3. 「性格 2 グループ×知識 2 グループ」型インシデントモデルに基づくセキュリティ対策

従来，セキュリティ対策は，システムを利用するユーザの性格やスキルを図 4-3 の様な一様分布と仮定して対策を行なっている．このため，対象から外れたところに属するユーザが事故を起こしやすくなることが考えられる，

これまでの議論の通り，ユーザには事故を起こしやすい性格特性が強いと起こしにくい性格特性が強い 2 つのグループがある．このため，実際には図 4-4 の様な分布になっていると推測される．そこで，事故を起こしやすい性格特性が強いグループと事故を起こしにくい性格特性の強いグループとで，セキュリティ対策の強度を変えることで，事故防止の強化につながると考えられる．

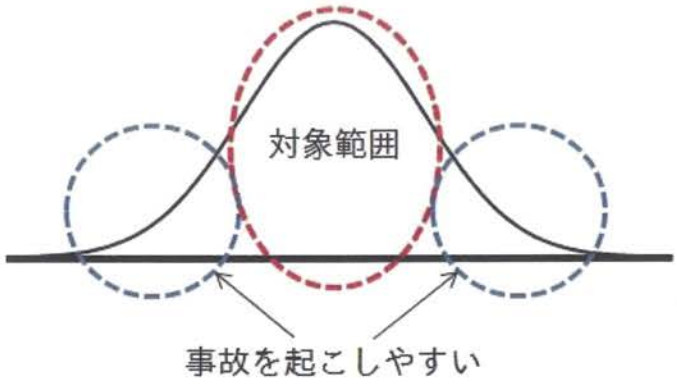


図 4-3. 従来想定していたユーザの分布

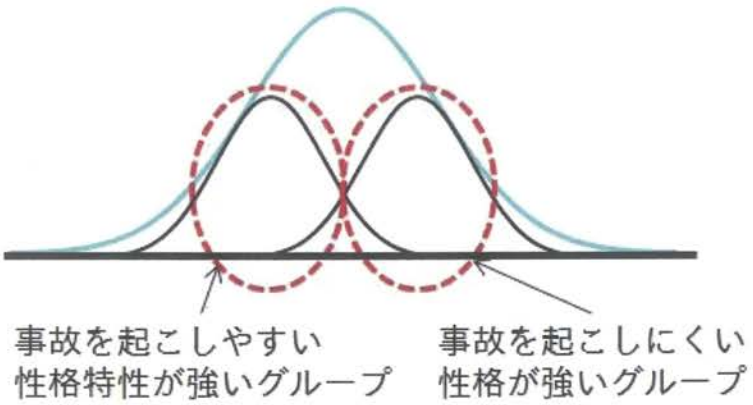


図 4-4.「性格 2 グループ×知識 2 グループ」型インシデントモデルに基づくユーザの分布

本対策では，4.2 節で示した考え方に基づき，予め性格診断やスキルテストを行い，ISMS においてユーザがどのグループに属しているかを調べておく事前のプロセスを導入する (図 4-5)．なお経験や教育，環境（役職や家庭，等）の変化により，グループが変わる可能性が十分に考えられるため，事前に行うプロセスは定期的に確認することが望ましい．

次節では，本方式のコストについて定式化を試みる．

4.3.1. 「性格 2 グループ×知識 2 グループ」型インシデントモデルにおける情報資産，脅威，セキュリティ対策に着目したセキュリティ対策選択問題の定式化

情報システムにおいて，そのセキュリティ対策を考える時，当該システムにおける脅威 (攻撃) を想定し，その驚異によりどの様な影響があるか，リスクアセスメントを行い，セキュリティポリシーを策定して運用する事が多い．これにともない，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[102]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[103], [104], [105], [106],[107][108].

そこで本節では，中村らのセキュリティ対策選択問題の定式化[108]を元に，「性格 2 グループ×知識 2 グループ」型インシデントモデルにおける情報資産，脅威，セキュリティ対策について，セキュリティ問題の定式化を考える．

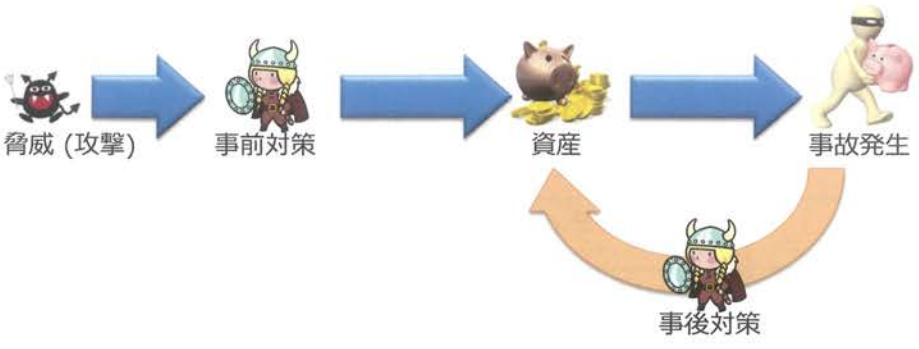


図 4-5. 情報システムにおける脅威

図 4-5 にある通り，情報事故が発生する前に想定した脅威に対する事前対策と，事故発生後に行う事後対策とを考慮する必要がある．事前対策としては，ファイアウォール，NAT

(Network Address Transform)，検疫ネットワーク，等のネットワークセキュリティ，ファイル暗号化，パスワード／トークン／生体を使った利用者認証等がある．事後対策としては，脅威が発生した時に起こりうる情報資産への損失を想定したデータの二重化等のバックアップや，データ損失の際の訴訟リスクに備え，アクセスログや電子メールの保全等のディジタル・フォレンジック対策がある．

本研究では，「性格2グループ×知識2グループ」型インシデントモデルは事故を防止することが目的であるため，事後対策は考慮しないため，事前対策について考える．

中村らは事前対策について，脅威と情報資産，そしてセキュリティ対策の関係をモデル化し，セキュリティ対策選択問題を定式化した．この定式化に用いるパラメータを表4-1に示す．

表 4-1. 定式化に用いるパラメータ

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．

まず，何のセキュリティ対策も施されていない場合の残存資産 RA を考える．情報資産 A_k は，$E_{jk} = 1$ の脅威 Tj の影響を受けると資産が失われる．無対策の状態では，脅威の発生によって資産は必ず失われる（脅威の攻撃成功確率は１である）ため，一定期間内に情報資産 A_k が失われる確率は，その期間内に脅威 T_j が発生する確率 P_j に等しい．よって，情報資産 Ak が残る確率は，情報資産 A_k に対して $E_{jk} = 1$ である全ての脅威 T_j が発生しない確率

$$\prod_j \left(1 - E_{jk} P_j\right)$$

と等しくなる．よって，一定期間後に残存している情報資産 A_k の価値 V_k の期待値は

$$V_k \prod_j \left(1 - E_{jk} P_j\right)$$

となり，残存する全資産の総和である残存資産の期待値 RA は，

$$\sum_k \left\{ V_k \prod_j \left(1 - E_{jk} P_j\right) \right\} \qquad \cdots \text{(式 4-1)}$$

となる．

次に，セキュリティ対策を行った際の残存資産ついて考える．情報セキュリティ対策 CM_i により脅威 T_j の攻撃成功確率は $(1- R_{ji})$ に低減されるため，脅威 T_j の攻撃により資産 A_k が失われる確率は，脅威 T_j の発生確率 P_j とその攻撃成功確率 $(1- R_{ji})$ の積 $P_j(1- R_{ji})$ となる．実際には採用される情報セキュリティ対策は一つではなく，複数の対策 $CM_i\ (1 \leqq i \leqq I)$ それぞれが確率 R_{ji} で脅威 T_j の攻撃成功率を下げる．採用されている全ての情報セキュリティ対策の効果が単純に相乗されると仮定した場合，各対策の選択 / 非選択のフラグ S_i を用い，脅威 T_j の攻撃成功確率は

$$\prod_i \left(1 - R_{ji} S_i\right)$$

と表される．よって，脅威 T_j により一定期間内に情報資産 A_k が失われる確率は，

$$P_j \prod_i \left(1 - R_{ji} S_i\right) \qquad \cdots \text{(式 4-2)}$$

となる．これは，(式 4-1)において $P_j \times 1$（無対策時においては脅威 T_j が確率 P_j で発生した場合に確率 1 で攻撃が成功する）で示されていた資産 A_k の損失確率が，対策の採用によって(式 4-2)に変化することを意味する．従って，(式 4-1)の P_j を(式 4-2)に変更することで，$S_i = 1$ である情報セキュリティ対策 CM_i が選択された場合の残存資産の期待値 RA は

$$RA = V_k \prod_j \left[1 - E_{jk} P_j \prod_i \left(1 - R_{ji} S_i \right) \right] \quad \cdots \text{(式 4-3)}$$

と定式化される．

情報資産を脅威から守ることは，情報セキュリティ対策により多くの情報資産を残すことである．つまり，(式 4-3)の残存資産の期待値 RA を最大化することと同意である．しかし，セキュリティ対策の採用にはコストが発生する．対策のコスト $Cost$ は

$$Cost = \sum_i C_i S_i \quad \cdots \text{(式 4-4)}$$

で表されるため，残存資産 RA からコスト $Cost$ を差し引けば，講じた情報セキュリティ対策の純粋な効果となる．以上より，セキュリティ対策問題は，

$$\sum_k \left\{ V_k \prod_j \left[1 - E_{jk} P_j \prod_i \left(1 - R_{ji} S_i \right) \right] \right\} - \sum_i C_i S_i \quad \cdots \text{(式 4-5)}$$

が最大となるフラグ S_i の組合せを見つける問題に帰着する．これは，

$$S_i \in \{0,1\} \quad (1 \le i \le I)$$

となる制約条件の下で，(式 4-5)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．

(式 4-5)を元に中村らのモデルを拡張し，「性格 2 グループ×知識 2 グループ」型インシデントモデルにおけるセキュリティ対策問題の定式化を行う．そこで情報セキュリティ対策を，図 4-6 の様に

- 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_1 郡：事故を起こしやすい性格のグループに対して行う対策

- B_2 郡：事故を起こしにくい性格のグループに対して行う対策

に分類する．この時，A 郡の対策の効果は，表 4-1 の R_{ji} のみによって表せられる．そして，B_1 郡と B_2 郡の対策について，それぞれ脅威 T_j の攻撃成功確率を考えれば良い．

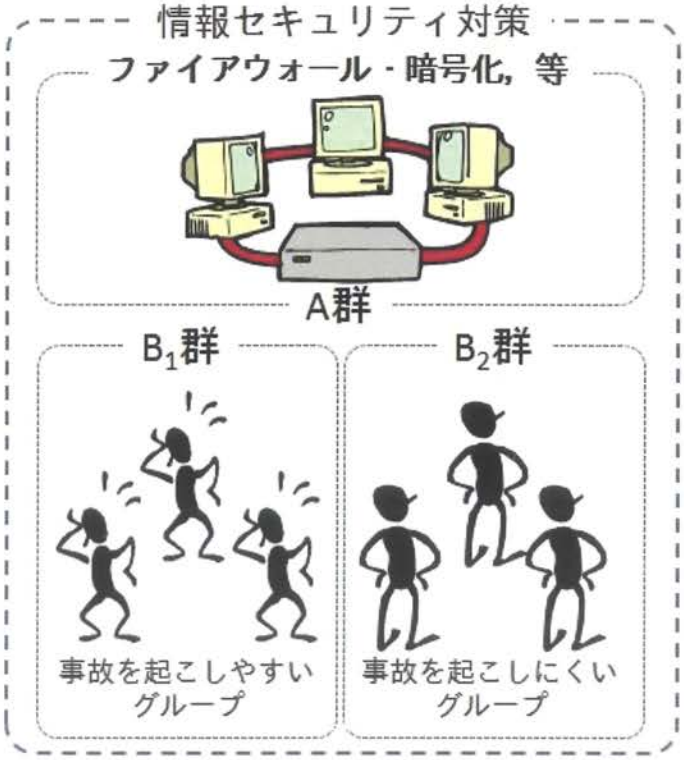


図 4-6.「性格 2 グループ×知識 2 グループ」型インシデントモデル
におけるセキュリティ対策定式化の考え方

A 郡の脅威 T_j の攻撃成功確率は，

$$\prod_{i\in A}\left(1-R_{ji}^{A}S_{i}^{A}\right)$$

で表される．また，B_1 郡の脅威 T_j の攻撃成功確率は，

$$\prod_{i\in B_1}\left(1-R_{ji}^{B_1}S_i^{B_1}\right)$$

で表され，B_2 郡の脅威 T_j の攻撃成功確率は，

$$\prod_{i\in B_2}\left(1-R_{ji}^{B_2}S_i^{B_2}\right)$$

となる．以上から，残存資産の期待値 RA は次式となる．

$$RA=V_k\prod_j\left[1-E_{jk}P_j\prod_{i\in A}\left(1-R_{ji}^{A}S_i^{A}\right)\prod_{i\in B_1}\{1-R_{ji}^{B_1}S_i^{B_1}\}\prod_{i\in B_2}\{1-R_{ji}^{B_2}S_i^{B_2}\}\right] \quad \cdots \text{(式 4-6)}$$

となる．

情報資産を脅威から守ることは，情報セキュリティ対策により多くの情報資産を残すことである．つまり，(式 4-6)の残存資産の期待値 RA を最大化することと同意である．ここで，セキュリティ対策コスト $Cost$ は，

$$Cost=\sum_{i\in A}C_i^{A}S_i^{A}+\sum_{i\in B_1}C_i^{B_1}S_i^{B_1}+\sum_{i\in B_2}C_i^{B_2}S_i^{B_2}$$

を加えることによって，2 グループモデルにおけるセキュリティ対策の定式化は

$$\sum_k\left\{V_k\prod_j\left[1-E_{jk}P_j\prod_{i\in A}\left(1-R_{ji}^{A}S_i^{A}\right)\prod_{i\in B_1}\{1-R_{ji}^{B_1}S_i^{B_1}\}\prod_{i\in B_2}\{1-R_{ji}^{B_2}S_i^{B_2}\}\right]\right\}$$
$$-\left\{\sum_{i\in A}C_i^{A}S_i^{A}+\sum_{i\in B_1}C_i^{B_1}S_i^{B_1}+\sum_{i\in B_2}C_i^{B_2}S_i^{B_2}\right\} \quad \cdots \text{(式 4-7)}$$

となり，(式 4-7)が最大となるフラグ $(S_i^{A},S_i^{B_1},S_i^{B_2})$ の組合せを見つける問題に帰着する．これは，

$$S_i=(S_i^{A},S_i^{B_1},S_i^{B_2})\in\{0,1\}\quad(1\le i\le I)$$

となる制約条件の下で，(式 4-7)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.

4.4. 「性格2グループ×知識2グループ」型に注意力を加えたインシデントモデルの検討

本研究では，第2章から第3章で情報事故における性格と教育に関するインシデントモデルを構築した．ヒューマンエラーを起こす要因として，様々な要因が考えられるが，吝嗇性（Parsimony）の考え方に基づき，主要因である性格と教育に着目し，図2-6の様に2要因を軸とした「性格2グループ×知識2グループ」型インシデントモデルを構築した．

ここで1.2.2，1.2.3項に述べた通り，“うっかり”や“おっちょこちょい”等のヒューマンエラーは不注意から起こるものであり，不注意を防止するには，注意（attention）の選択と集中，そして維持の機能が大切で，それには作業記憶（Working Memory）の大きさが鍵となっている．作業記憶が大きいと，注意すべき対象への集中が高く，“うっかり”というエラーが発生しにくくなる．

ここで，注意が正しく働いているかを確認するには，セルフチェックを行えるメタ認知能力が大切であることを，1.2.4項で述べた．メタ認知力が低いと自己中心的になり，自分に都合の良い解釈をしがちになり，慎重さに欠け（注意が疎かになり）事故を起こした時の被害が大きくなる．

これは，様々なヒューマンエラー対策を無効にする不安全行動，もしくはリスク・テイキング行動につながり，メタ認知能能力が低いとリスクを低く見積もるために起こると考えられる．また事故多発者には，注意力が乏しく意識が向きにくい傾向が見られる[109]が分かっている．

以上から，ヒューマンエラーの発生原因には注意力（attention）が重要であり，情報事故にも大きな影響を与えると考えられる．そこで，「性格2グループ×知識2グループ」型インシデントモデルに注意の軸を加えたモデルを検討する．

注意は，図1-7に示す様に，注意の集中が持続すればストレスとなり，覚醒の低下や飽き / 慣れ，疲労により無気力やリラックスという状態に遷移する．図4-7に示す様に，心理的ストレスが事故を起こす原因[110]となっていることから，長時間の注意の集中は，ストレスとなり事故を起こしやすくなると考えられる．

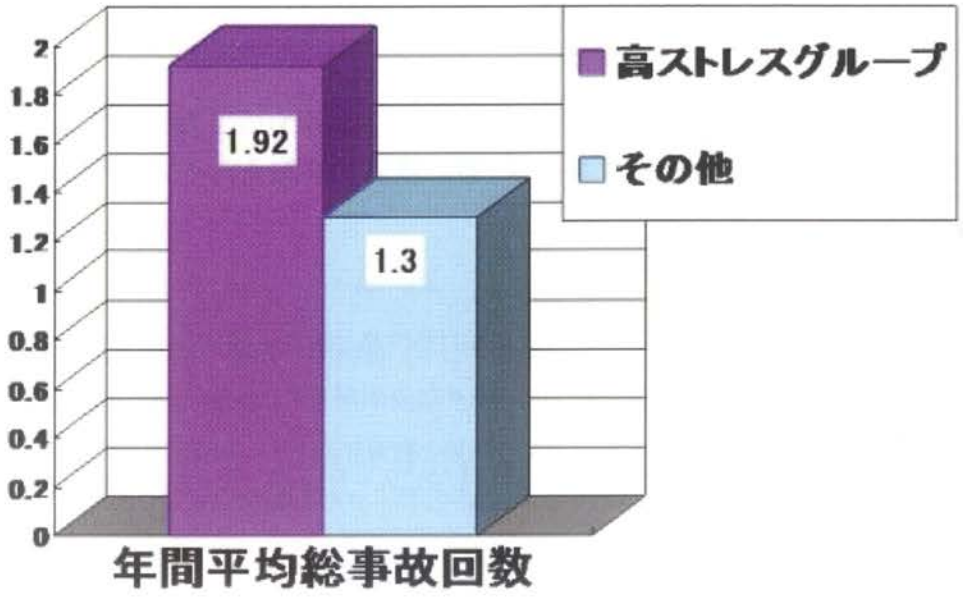


図 4-7. 事故とストレスの関係[110]

同様に，一時的な注意の集中であるハイテンションも持続が短いため，直ぐに無気力，もしくはリラックスの状態に遷移する．例えば車の運転の場合，無気力やリラックスの状態で，外乱（人等の飛び出しや前方走行車の急停止，等）が発生すれば，事故もしくはヒヤリ・ハットにつながる．

以上から，注意について人の状態は図 4-8 の様に，注意が高い状態と低い状態とに遷移すると考えられる．

図 4-8. 注意の遷移

この注意の遷移は，「性格 2 グループ×知識 2 グループ」型インシデントモデルにおける第 1 象限～第 4 象限のグループでも起こりうる．そこで，性格と教育（による知識やスキル）に注意という要因を加えたインシデントモデルは，図 4-9 の様に表される．

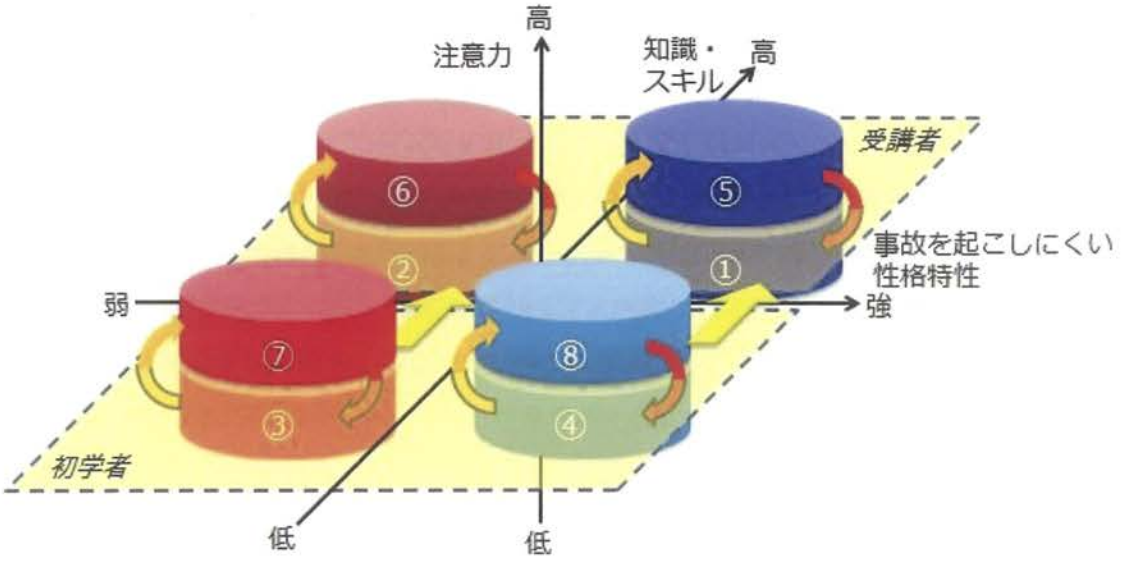


図 4-9.「性格 2 グループ×知識 2 グループ×注意 2 グループ」型インシデントモデル

図 4-10 において，初学者である第 3 及び第 4 象限については，情報事故を起こしにくい性格特性が強い第 4 象限の方が，情報事故を起こしやすい性格特性が強い第 3 象限よりも注意を維持することができると考えられる．同様に，教育を受けた受講者である第 1 及び第 2 象限については，情報事故を起こしにくい性格特性が強い第 1 象限の方が，情報事故を起こしやすい性格特性が強い第 2 象限よりも注意を維持することができると考えられる．

情報事故を起こしやすい性格特性が強い第 2 象限と第 3 象限とでは，第 2 象限の方が注意を維持することができ，第 1 象限と第 4 象限とでは，第 1 象限の方が注意を維持することができると考えられる．

これは，情報事故の原因の多くがヒューマンエラーであり，情報事故を起こしやすい性格特性が強い傾向とそうではない傾向とがあり，さらにヒューマンエラーが注意の不足から起きることから，情報事故を起こしやすい性格特性が強い場合，注意が低くなる傾向が高くなり情報事故を起こしやすいことが理由と考えられる．また，教育を受け疑似体験等で経験を積み，知識やスキルが高まることで注意すべきポイントを絞ることができ，注意を長く持続できると考えられる．しかし，長い時間の注意の持続はストレスであり，注意が途切れることは容易に推察できる．また，人は一旦安心を得ると不安全（リスクテイキング）行動を取りやすくなり，注意が欠如する．

また不安全行動は，1.2.4 及び 1.2.5 項で述べたように自己モニタリング能力が高ければ慎重に

なりエラーを起こしにくい．自己モニタリング能力はメタ認知能力でもあり，メタ認知能力が高ければ，事故を起こしにくい．

図 4-9 の「性格 2 グループ×知識 2 グループ×注意 2 グループ」型インシデントモデルを検証するためには，メタ認知能力と性格，及び教育（経験やスキル）についての相関について調査を行なう必要があり，今後の課題である．

4.5. まとめ

本章では，2 グループモデルに基づいた新たな 2 つのセキュリティ対策方式を提案した．

4.2 節では，事前にユーザに性格検査やセキュリティ意識に対する質問を行い，ユーザのセキュリティ対策に対する意識の大きさを算出し，セキュリティ意識と性格との相関 DB を構築し，相関 DB を用いてユーザ毎に好適な対策や運用を選択するものである．本提案では，パスワード認証 / 持ち物認証 / 生体認証の 3 つの認証が，あるユーザに対して好適かを，この相関 DB を用いることで判定し，ユーザに負担がなくセキュリティ意識が高い認証方式を利用してもらうことで情報事故を防ぐものである．

4.3 節では，事故を起こしやすい性格と事故を起こしにくい性格とが存在する 2 グループモデルに基づき，4.2 節と同様に事前に性格検査やスキルテストを行い，どちらのグループに所属するかで，セキュリティ対策の強度を変える方式である．一般にセキュリティ対策の強度が高くなればなるほど，コストがかかりユーザの利便性も下がる[111], [112]．そこで，事故を起こしにくい性格のグループは，セキュリティ強度を下げることで，セキュリティ対策に係るコストを下げ，かつユーザの利便性を上げる．一方，事故を起こしやすい性格のグループに対しては，セキュリティ強度を上げる．ここで企業等ではリスクアセスメントを行い，セキュリティ対策を考えることから，事故を起こしやすい性格のグループに対して実施するセキュリティ対策を，全ユーザに展開していると考えられる．本方式では，事故を起こしにくい性格のグループに対しては，セキュリティ強度を下げた管理を行うため，その分だけコストを削減できる効果が期待できる．それは，4.3.1 項で示した定式化により，B_2 群の対策分の削減が期待できる．以上から，事故を起こしにくいグループのユーザを増やすことが大切となる．

本研究の最終目的は，情報事故における精緻なモデルを構築することにあるが，本論文ではそ

のベースとなるモデルを構築した段階にある．本論文で構築したモデルが精緻なモデルであるかは，4.2 節のベストマッチセキュリティや，4.3 節に示した 2 グループモデルに基づきセキュリティ対策を変える方式を実装評価することで検証が可能となる．提案方式の実装評価は，今後の課題である．

4.4 節では，本研究で構築した「性格 2 グループ×知識 2 グループ」型インシデントモデルに，注意を加えた「性格 2 グループ×知識 2 グループ×注意 2 グループ」型インシデントモデルを提案した．これは情報事故の原因の多くがヒューマンエラーであり，ヒューマンエラーが注意の欠如から発生する事による．インシデントモデルに注意を加える事で，より精緻なモデルとなるが，注意と強く関わりがあるメタ認知能力と性格，及び教育（経験やスキル）に関する相関について，新たに調査を行なう必要があり，今後の課題としたい．

第5章 考察

本研究では，情報事故において性格との相関について，「性格 2 グループ×知識 2 グループ」型インシデントモデルを構築するため，以下のステップで行った．

STEP1

これまで多くの調査がなされている交通事故に関する既存研究を元に，交通事故と性格の関係を演繹する．交通事故においては，事故を起こしやすい性格特性と事故を起こしにくい（事故に関与しない）性格特性とがある．また，シミュレータを用いた教育等により，事故を起こしにくくする効果がある．これを情報事故のインシデントモデルに写像することで，性格特性の傾向と教育に応じてユーザを 4 つのグループに分ける「性格 2 グループ×知識 2 グループ」型のインシデントモデルを導いた．

STEP2

教育を受けた社会人に対するヒューマンエラーに関する既存研究を元に，ヒューマンエラーを起こしやすい性格特性（性格 A）とヒューマンエラーを起こしにくい（もしくは起こしやすさに関与しない）性格特性（性格 B）があることを示す．情報事故の 8 割以上がヒューマンエラーによって引き起こされることから，セキュリティ教育を受けたユーザ（一般社会人）のインシデントモデルが，ヒューマンエラーを起こしやすい性格特性が強いグループと，ヒューマンエラーを起こしにくい性格特性が強いグループの 2 つに分かれることを裏付けた．

STEP3

大学 1 年生約 400 名を対象に本人認証におけるセキュリティ意識に関する質問紙調査を行い，セキュリティ意識が低い傾向にある性格特性（性格 C）と高い傾向にある性格特性（性格 D）があることを明らかにする．認証情報の取り扱いに関する意識の低さが情報事故の温床となっていることから，セキュリティ教育の初学者（ノービス, novis）である大学 1 年生のインシデントモデルも，

セキュリティ意識が高い性格特性が強いグループと，セキュリティ意識が低い性格特性が強いグループの 2 つに分かれることを示した．

STEP4

セキュリティ教育を受けたユーザ（STEP2）もセキュリティ教育の初学者（STEP3）も，事故を起こしやすい性格特性が強いことは類似しており（性格 A と性格 C），かつ事故を起こしにくい性格特性が強いことも類似している（性格 B と性格 D）ことを確認する．“三つ子の魂百まで”という諺が示す様に，幼児期に形成された性格は年齢や経験による影響を受けにくいと言われていることから，情報事故においても，事故を起こしやすい性格特性が強いグループと事故を起こしにくい（もしくは関与しない）性格特性が強いグループとがあり，それぞれの性格特性が強いユーザの中で，教育による知識の程度で事故を起こしやすいグループと事故を起こしにくいグループとに分かれるという「性格 2 グループ×知識 2 グループ」型のインシデントモデルが妥当であることを示した．

上記 STEP1～4 の結果，交通事故の場合と同様に，情報事故においても性格と相関があり，「性格 2 グループ×知識 2 グループ」型インシデントモデルが成り立つことが示された．特に STEP3 の情報セキュリティ教育の初学者におけるセキュリティ意識と性格との相関に関する調査はこれまで行われておらず，本研究で相関があることが示された意義は大きい．

それぞれの STEP から，以下について明らかにした．

1) STEP1 で，交通事故における違反者の性格との相関について調査研究を行い，交通事故を起こす人には，交通事故を起こしやすい性格特性が強い傾向があることを示した．また，事故を防止するにはシミュレータ等による疑似体験を用いた教育が有効であることから，交通事故を起こしやすい性格特性が強いグループと起こしにくい性格特性が強い 2 つのグループが存在し，かつ教育を受けた受講者と初学者の 2 グループがあることを示し，交通事故における「性格 2 グループ×知識 2 グループ」型インシデントモデルを示した．

2) 交通事故の主な原因が思い込み，即ちヒューマンエラーであり，情報事故も 8 割がヒューマンエラーにより発生することから，STEP2 では教育を受け経験もある一般社会人におけるヒューマンエラーと性格との相関に関する調査研究を行い，教育を受けた一般社会人におい

ても，ヒューマンエラーを起こしやすい性格特性が強いグループと起こしにくい性格特性が強い 2 つのグループに分かれることを示した．

3) STEP3 では，情報セキュリティ教育の初学者である大学 1 年生を対象に新性格検査と認証方式のセキュリティ意識に関する質問紙よるアンケート調査を実施し，初学者においても，認証方式に応じてセキュリティ意識の低い性格特性が強いグループと高い性格特性が強いグループとがあることを示した．ここで認証方式においてセキュリティ意識が低いということは，情報事故を起こしやすいということと同義である．何故ならば，例えばパスワード認証において同じパスワードを使い回したり，パスワード変更をしなかったり，という意識が低いということは，情報事故を起こしやすいからである．

4) STEP1～STEP3 の結果から，交通事故を起こしやすい性格特性と一般社会人におけるヒューマンエラーを起こしやすい性格特性，情報セキュリティ教育の初学者である大学 1 年生におけるセキュリティ意識が低い性格特性には，図 5-1 の様に類似する傾向があることが分かる．

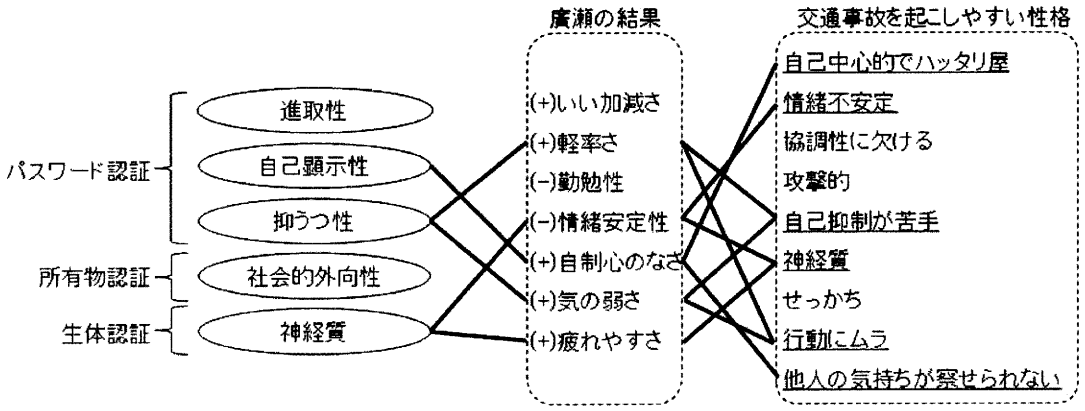


図 5-1. 事故を起こしやすい共通の性格特性

図 5-1 において，交通事故を起こしやすい性格特性には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特性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（非協調性），攻撃的（攻撃性）は，セキュリティ意識にマイナスに働く性格特性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性格特性と考えられる．非協調性は一人よがりな運転操作に関連し，攻撃性は前を走る車を追い抜く運転をしがちになる傾向を示している．せっかちは，廣瀬の結果とは関連が見られないが，進取性と関連がありセキュリティ意識にマイナスに働く性格特性とは関連があることに注意が

必要である.

5) 「性格 2 グループ×知識 2 グループ」型インシデントモデルに基づくセキュリティ対策の方式を 2 つ提案した.

一つ目は, 事前にユーザに性格検査やセキュリティ意識に対する質問を行い, ユーザのセキュリティ対策に対する意識の大きさを算出し, セキュリティ意識と性格との相関 DB を構築し, 相関 DB を用いてユーザ毎に好適な対策や運用を選択するものである. 一つの事例として, パスワード認証 / 持ち物認証 / 生体認証について, ユーザに好適かを判定し, ユーザに負担がなくセキュリティ意識が高い認証方式を利用してもらうことで情報事故を防ぐ.

本方式は, 以下の効果があると考えられる.

- 認証方式を全て準備するためのコストがかかるが, ユーザにフィットした方式のため, ユーザが意識すること無くセキュリティ対策を行えることが期待される. このため, 結果的に情報事故を防止できると考えられる.

- 事前の評価を追加することで, 導入するセキュリティ対策の実効度を予め評価できる. このため, サービスの運用前にリスクを明確にできる.

- 全ユーザに画一的なセキュリティ対策を採用しなければいけない場合, 全ユーザの特性を調査できるので, マジョリティを占める特性に合うセキュリティ対策を選定できるので, 組織全体の実効度を維持できる.

- 年代毎, 職業毎等, 特定フィールドに属するユーザについて特性を調べれば, 企業がセキュリティ製品を開発する際に, 当該製品のターゲットとなるユーザ層の特性をみることで, 当該製品のセキュリティ対策として何を採用すれば受け入れられるかが推定できる.

等の効果が期待できる.

2 つ目は事前に性格検査やスキルテストを行い, どちらのグループに所属するかで, セキュリティ対策の強度を変える方式である. 事故を起こしにくい性格特性が強いグループは, セキュリティ強度を下げることで, セキュリティ対策に係るコストを下げ, かつユーザの利便性

を上げる．一方，事故を起こしやすい性格特性が強いグループに対しては，セキュリティ強度を上げる．

企業等では，画一的なセキュリティ対策を導入し対策を行なっているため，本来事故を起こしにくいユーザに対しても，事故を起こしやすいユーザへの対策を強いることになり，結果的に過剰な対策を行なう結果となっている．本方式では，事故を起こしにくい性格特性が強いグループに対しては，セキュリティ強度を下げた管理を行うため，その分だけコストを削減できる効果が期待できる．提案方式で用いる性格検査やスキルに関する質問紙調査を，自己診断出来るような試験にすることで，提案方式が導入されていない組織のユーザにおいても，ユーザ自らの注意点を意識する事が期待でき，事故防止に繋がると思われる．

また，本研究で構築した「性格 2 グループ×知識 2 グループ」型インシデントモデルに，注意を加えた「性格 2 グループ×知識 2 グループ×注意 2 グループ」型インシデントモデルを提案した．これは情報事故の多くがヒューマンエラーが原因で発生しており，ヒューマンエラーは注意の欠如によるからである．注意を加える事でより精緻なモデルとなりが，注意と強く関わりがあるメタ認知能力と性格，及び教育に関する相関について調査を行なう必要がある．

さらに，常に注意し続けることはストレスであり，1.3.3 項に示した様に，逆に事故を起こしかねない．一方，操作に慣れる等の経験を積む事で注意するポイントを絞り，情報事故におけるリスク知覚やハザード知覚を高め，無意識に注意を向け事故を防止できると考えられる．この様に，如何にストレス無く注意を意識できる様な仕組み等について，どう対策していくかについても今後の課題である．

第6章 まとめ

本研究では，ユーザの性格に着目し事故を起こしやすい性格特性が強いグループと事故を起こしにくい性格が強いグループとに分かれ，教育を受けた受講者と初学者とで分かれる「性格 2 グループ×知識 2 グループ」型インシデントモデルを構築した．

その妥当性を交通事故における調査研究から性格と教育を要因とした「性格 2 グループ×知識 2 グループ」型インシデントモデルを示した．また，教育を受け経験もある一般社会人におけるヒューマンエラーと性格（ビッグファイブ）との相関に関する調査研究から，ヒューマンエラーを起こしやすい性格特性が強いグループと起こしにくい性格特性が強いグループとに分かれることを示した．最後に，これまで調べられていなかった情報セキュリティ教育の初学者である大学 1 年生を対象に，本人認証とセキュリティ意識と性格との相関に関する質問紙による調査を行い，相関があることを示した．そしてセキュリティ意識について相関があるマイナス因子の性格と，交通事故や教育を受けた一般社会人の場合の事故を起こしやすい性格特性と，事故を起こしにくい性格特性とに類似性があることから，初学者においても情報事故を起こしやすい性格特性が強いグループと事故を起こしにくい性格特性が強いグループとに分かれることを示した．

最後に，「性格 2 グループ×知識 2 グループ」型インシデントモデルに基づくセキュリティ対策として，2 つの方式を提案した．一つ目は，ユーザに性格検査やセキュリティ意識に対する質問を行い，ユーザのセキュリティ対策に対する意識の大きさを算出し，セキュリティ意識と性格との相関 DB を構築するものである．事前に相関 DB を用いて算出された各セキュリティ対策の実効度を参照する．実効度を参照することで，サービスやシステムを利用するユーザに対して，どの様な問題が起こるのか，どのようなセキュリティ対策だとリスクが最小限に抑えられるか，等が想定できる．

2 つ目は，事前に性格検査やスキルテストを行い，どちらのグループに所属するかで，セキュリティ対策の強度を変える方式を提案した．情報事故を起こしにくい性格特性が強いグループは，セキュリティ強度を下げることで，セキュリティ対策に係るコストを下げ，かつユーザの利便性を上げられる効果が期待できる．本論文で構築したモデルが精緻なモデルであるかは，これら 2 つの提案方式を実装評価することで検証が可能となるが，実装評価は今後の課題である．

また，「性格 2 グループ×知識 2 グループ」型インシデントモデルに注意を加えた「性格 2 グループ×知識 2 グループ×注意 2 グループ」型インシデントモデルを提案した．これは情報事故の原

因の多くがヒューマンエラーであり，ヒューマンエラーが注意の欠如から発生する事による．インシデントモデルに注意を加える事で，より精緻なモデルとなるが，注意と強く関わりがあるメタ認知能力と性格，及び教育（経験やスキル）に関する相関について，新たに調査を行なう必要があり，また如何にストレス無く注意を意識できる様な仕組み等について，どう対策していくか今後の課題である．

謝辞

本研究を行うにあたり，指導教員として繊細且つ的確なご指導を受け賜りました静岡大学情報学部　西垣 正勝　教授に深く感謝を申し上げます．

また，論文審査委員の立場から適切な助言をくださいました静岡大学情報学部情報科学科　渡辺 尚　教授，静岡大学工学部工学研究科システム工学専攻　大坪 順次　教授，静岡大学情報学部情報社会学科　漁田 武雄　教授，静岡大学情報学部情報社会学科　山田文康 准教授に感謝いたします．

西垣研究室を卒業された，株式会社デンソー　長谷（旧姓 中澤）優美子氏，三菱電機株式会社　山本 匠氏，京セラ株式会社　名坂 浩平氏には，本研究を進めるにあたり，多大なる支援と助言をいただき感謝いたします．さらに，同研究室の上松 晴信氏には 2 グループモデルにつながるアイデアと支援をいただき感謝いたします．また，質問紙調査に協力していただいた静岡大学情報学部 1 年生の皆さまに感謝いたします．

本研究に対し，様々な助言と情報を提供いただいた情報処理推進機構セキュリティセンター 情報セキュリティ分析ラボラトリー ラボラトリー長　小松 文子氏に感謝いたします．

最後に，様々な視点で意見を出して研究を支えてくれた西垣研究室の皆さまに感謝すると共にお礼申し上げます．

参考文献

[1] 一般財団法人日本情報経済社会推進協会(JIPDEC), 認証取得組織数推移、認証機関別・県別認証取得組織数, http://www.isms.jipdec.or.jp/lst/ind/suii.html (2012.11.17 アクセス).

[2] (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 (2012.11.17 アクセス).

[3] セキュリティ被害調査ワーキンググループ, 2011 年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～, NPO 日本ネットワークセキュリティ協会(2012.9).

[4] 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).

[5] 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).

[6] 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 (2012.11.17 アクセス).

[7] ジェームス・リーズン, 佐相邦英[監訳], (財)電力中央研究所ヒューマンファクター研究センター[翻訳], 組織事故とレジリエンス, 日科技連出版社, (2010).

[8] 中田亨, ヒューマンエラーを防ぐ知恵, DOJIN 選書, (2007).

[9] W. Haddon, E. A. Suchman, D. Klein, Accident Research : Methods and

Approaches, Harper & Row, (1964).

[10] F. McGlade, F. D. Laws, Classifyng Accidents : A Theoritical Viewpoint, Traffic Safety, 6(1), pp.2-8, (1962).

[11] James Reason, Human Error, Cambridge University Press, P.17, (1990).

[12] ジェームス・リーズン, 林喜男[訳], ヒューマンエラー ー認知科学的アプローチー, 海洋堂出版, (1994).

[13] Donald A. Norman, Categorization of Action Slips, Psychological Review, Vol.88, No.1, pp.1-15, (1981.1).

[14] A. D. Swain, H. G. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, U. S. Nuclear Regulatory Commission, NRC 24-43, (1983).

[15] 山下 富美代, 現場事故を防ぐ「不注意の心理学」なぜ起きるうっかりミスや勘違い, 日刊建設産業新聞社, (2012).

[16] M. W. Eysenck, M. T. Keane, Cognitive psychology: a student's handbook. 4th ed., Phsycology Press, p.131, (2005).

[17] 原田 悦子, 篠原 一光, 現代の認知心理学 4 注意と安全, 北大路書房, (2011).

[18] M. I. Posner, Orienting of Attention, Quarterly Journal of Experimental Psychology, 32, pp.3-25, (1980).

[19] R. Desimone, J. Duncan, Neural Mechanisms of Selective Visual Attention, Annual Review of Neuroscience, 18, pp.193-222, (1995).

[20] M. J. Kane, R. W. Engle, Working – memory Capacity and the Control of Attention: The Contributions of Goal Neglect, Response Competition, and Task Set to Stroop Interference, Journal of Experimental Psychology: General, 132, pp.47-70, (2003).

[21] 三浦利章(編著), 原田悦子(編著), 事故と安全の心理学 リスクとヒューマンエラー, 東京大学出版会, (2007).

[22] A. R. Conway, N. Cowan, M. F. Bunting, The Cocktail Party Phenomenon Revisited: The Importance of Working Memory Capacity, Psychonomic Bulletin & Review, 8, pp.193-221, (1995).

[23] Taylor, Shelley E. and J.D. Brown, "Illusions and Well-Being: A Social Psychological Perspective on Mental Health," Psychological Bulletin, 103, 193-210. (1988).

[24] Kruger, J, Epley, N, Parker, J and Ng ,Z, Egocentrism Over E-Mail: Can We Communicate as Well as We Think?, Journal of Personality and Social Psychology, vol.89, No.6, pp.925-936, (2005).

[25] R. C. Atkinson and R. M. Shiffrin, Human memory: A proposed system and its control processes., In K. W. Spence and J. T. Spence (Eds.), The Psychology of learning and motivation: Advances in research and theory (vol. 2). New York: Academic Press. pp.89-195, (1968).

[26] R. C. Atkinson and R. M. Shiffrin, The control of short - term memory., Scientific American, 225, pp.82-90, (1971).

[27] 守 一雄, 現代心理学入門 認知心理学, 岩波書店, pp46-48, (1995).

[28] R. M. Gagné, Conditions of Learning, http://www.personal.psu.edu/wxh139/gagne.htm, (2013.3.19 アクセス).

[29] A. D. Baddeley and G. Hitch, Working memory, In G.A. Bower (Ed.), Recent Advances in Learning and Motivation, Vol. 8. New York: Academic Press, pp.47-90, (1974).

[30] J. A. Miller, The Magical Number Seven, plus or minus two: Some Limits on our Capacity for Processing Information, Psychological Review, 63, pp.81-97, 1956.

[31] 三浦 利章, 視覚探索と鑑賞・技能・環境, 基礎心理学研究, 20(1), pp.64-69, 日本基礎心理学会, (2001.9).

[32] J. H. Fravell, Metacognitive aspects of problem solving., Nature of intelligence. , 12; pp.231-236, (1976).

[33] メタ認知の概要, 奈良教育大学, http://www2.nara-edu.ac.jp/CERT/nara-edu/outline/index.html, (2013.1.20アクセス).

[34] 加藤 久恵, 数学的問題解決におけるメタ認知の機能に関する実証的研究(2), 全国数学教育学会誌 数学教育学研究 Vol. 1, pp.65-73, (1995).

[35] 重松敬一, 問題解決と「内なる教師」(メタ認知), 小学校算数実践指導全集第 11 巻, 日本教育図書センター, (1995).

[36] Gerald J. S. Wilde, Critical Issues in Risk Homeostasis Theory, Risk Analysis, Volume 2, Issue 4, pages 249–258, (1982.12).

[37] Gerald J. S. Wilde, Risk Homeostasis Theory and Traffic Education Requirements, Campo Grande 2005, (2005).

[38] チャーリー・カウフマン, ラディア・パールマン, マイク・スペシナー[著], 石橋啓一郎, 菊池浩明, 松井彩, 土居裕介[訳], ネットワークセキュリティ, プレンティスホール出版, pp.7-8, (1997).

[39] Sam Curry, Engineering Security Solutions at Layer 8 and Above, http://blogs.rsa.com/curry/engineering-security-solutions-at-layer-8-and-above/, (2012.11.25 アクセス).

[40] マイナビニュース, SMB でも大企業並みのセキュリティを! "レイヤー8"対応の次世代 UTM「VCR」, 2012.11.5, http://news.mynavi.jp/articles/2012/11/05/vcr1/, (2012.11.25 アクセス).

[41] 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).

[42] 柳井晴夫, 国生理枝子, 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)

[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).

[44] 村上 宣寛, 性格のパワー, 日経 BP 社 (2011.6)

[45] 村上 宣寛, 心理学で何がわかるか, ちくま新書 (2009.9)

[46] 村上 宣寛, 村上 千恵子,性格は五次元だった 性格心理学入門, 培風館, (1999.6)

[47] 齋藤 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 2001 Vol.2, pp.135-144, (2001)

[48] 青木 邦男, 和田及び村上・村上の主要5因子性格特性尺度の因子構造の検討, 山口県立大学学術情報 第4号, pp.27-40, (2011.3)

[49] 村上 宣寛, 村上 千恵子, 性格は五次元だった－性格心理学入門－, 培風館, (1999).

[50] 自動車運転適正診断テスト, http://car.sinritest.com/, (2012.11.25 アクセス).

[51] 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)

[52] 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).

[53] Medsafe.Net, 人間工学と労働安全, http://www.medsafe.net/contents/hot/115ergonomics.html#sanko, (2012. 12. 4 アクセス).

[54] 自動車安全運転センター, 運転者の身体能力の変化と事故、違反の関連、及び運転者教育の効果の持続性に関する調査研究報告, http://www.jsdc.or.jp/search/pdf/all/h11_3.pdf, (2012.12.4 アクセス).

[55] 星野 貴之, 嶋田 喜昭, 舟渡 悦夫, 伊豆原 浩二, 若年ドライバーの性格と交通事故との関連分析, 第 26 回土木計画学研究発表会講演集, Vol.26, (2002), http://www.jsce.or.jp/library/open/proc/maglist2/00039/200211_no26/pdf/162.pdf, (2012.12.5 アクセス)

[56] 自動車運送事業に係る交通事故要因分析検討会, ヒヤリハット調査の方法と活用マニュアル ―多発する交通事故の予防をめざして―事業用自動車用, 国土交通省自動車交通局, (2003), http://www.mlit.go.jp/kisha/kisha03/09/090722/03.pdf, (2012.12.5 アクセス).

[57] 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).

[58] 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).

[59] 和田さゆり, 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).

[60] 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).

[61] 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).

[62] 人はどんなミスをして交通事故を起こすのか－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).

[63] 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).

[64] 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).

[65] 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).

[66] 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).

[67] 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).

[68] 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, Vol.46, pp.23-32, (2004).

[69] 国際交通安全学会, 交通安全教育の手法と評価法の研究　シミュレーターを活用した交通安全教育の検討, http://www.iatss.or.jp/pdf/kenkyu/h18/h852a.pdf, (2012. 12. 18 アクセス).

[70] 関根 太郎, 二輪運転者 h のシミュレータ教育効果, 国際交通安全学会誌, Vol.32, No.4, pp59-67, (2007).

[71] 田中 健次, 稲葉 緑, 高齢運転者へのシミュレータ教育の効果研究, 国際交通安全学会誌, Vol.32, No.4, pp41-48, (2007).

[72] 長山 泰久, 運転適性における態度の問題, 日本心理学会 第 21 回大会発表論文集, p.504, (1967).

[73] R. M. Trimpop, The Psychology of Risk Taking Behavior, Advances in Psychology, Vol.107, North Holand, (1994).

[74] 広瀬 弘忠, 人はなぜ危険に近づくのか, 予防時報, Vol.221, pp.8-13, (2005).

[75] 蓮花 一己, 運転時のリスクテイキング行動の心理的過程とリスク回避行動へのアプローチ, 国際交通安全学会誌, Vol.26, No.1, pp.12-22, (2000).

[76] 中村 隆宏, 4. 安全教育における擬似的な危険体験の効果と課題, 産業安全研究所特別研究報告, NIIS-SRR-NO.32, pp.41-49, (2005).

[77] 宮地 由芽子, 職場安全管理の改善に向けたヒューマンファクタ分析手法, 鉄道総研報告, Vol.21 No.05, pp.11-16, (2007).

[78] 宮地 由芽子, 村越 暁子, 赤塚 肇, 鈴木 綾子, 職場安全風土評価手法の開発, 鉄道総研報告, Vol.23 No.9, pp.23-28, (2009)

[79] 宮地 由芽子, ヒューマンエラーや事故調査に対する思考と性格特性について, 信学技報, Vol.112 No.206, SSS2012-12, pp.5-8, (2012. 9).

[80] 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).

[81] 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).

[82] 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).

[83] 中澤優美子, 西垣正勝, Best Match Security:性格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).

[84] 中澤優美子, 西垣正勝, Best Match Security:性格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).

[85] 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 (2009)

[86] SplashData, Inc., Worst Passwords of 2012 – and How to Fix Them, http://splashdata.com/press/PR121023.htm, (2012.12.31 アクセス).

[87] What's My Pass? 2008, The Top 500 Worst Passwords of All Time, http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time, (2012.12.31 アクセス).

[88] Stuart Brown, Top 10 Most Common Passwords, http://modernl.com/article/top-10-most-common-passwords, (2012.12.31 アクセス).

[89] Daniel Amitay, Most Common iPhone Passcodes, http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes, (2012.12.31 アクセス).

[90] Lockdown.co.uk, Password Recovery Speeds, http://www.lockdown.co.uk/?pg=combi&s=articles, (2012.12.31 アクセス).

[91] 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).

[92] 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, (2010.5.9 アクセス)

[93] 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).

[94] 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).

[95] 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).

[96] 林知乙夫, 新版多変量解析, 朝倉書店, (1985).

[97] 情報処理推進機, 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, (2012.11.27 アクセス)

[98] ITmedia Inc., 2 人に 1 人は「パスワード変更の習慣ない」、ネットユーザーの利用実態, http://www.itmedia.co.jp/enterprise/articles/1212/14/news077.html, (2012.12.12 アクセス).

[99] 日本マーケティング・リサーチ協会(編), 新版マーケティング・リサーチ用語辞典, 同友館, (1998).

[100] 岡田 守弘, 杉戸 るみ子, 対人二者相互関係における期待と役割の効果について, 横浜国立大学教育紀要 18, pp.160-174, (1978.11).

[101] (株)電脳, OD 式安全性テスト OD 式安全性テストの紹介, http://www.dennoo.co.jp/od/shokai.html, (2012.12.7 アクセス).

[102] 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)

[103] 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).

[104] 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) .

[105] 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) .

[106] 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).

[107] 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).

[108] 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).

[109] 吉田 信彌, 事故と心理—なぜ事故に好かれてしまうのか, 中公新書, (2006).

[110] 自動車技術会, 生活ストレスと運転リスクの検査, http://tech.jsae.or.jp/hiyari2/description.aspx, (2012.12.18 アクセス).

[111] ATY コンサルティング, セキュリティ、利便性やコストとのトレードオフ, http://yaokou.cocolog-nifty.com/yaotyan/2008/05/post_efdd.html, (2012.12.5 アクセス).

[112] (独)情報処理推進機構 セキュリティセンター, リモートアクセス環境におけるセキュリティ 5.2 組織としての取り組み, http://www.ipa.go.jp/security/fy18/reports/contents/remote/index.htm, (2012.12.5 アクセス).

筆者発表論文

A 学位論文申請資格に関わる論文

1) 加藤岳久，中澤優美子，漁田武雄，山田文康，山本匠，西垣正勝(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，情報処理学会論文誌 52(9), 2537-2548

B 学位論文内容に関わる論文

1) 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).

2) 中澤優美子，加藤岳久，漁田武雄，山田文康，山本匠，西垣正勝，Best Match Security－性格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，2009-CSEC-44，pp. 43-48 (2009. 3).

3) 中澤優美子，加藤岳久，漁田武雄，山田文康，山本匠，西垣正勝，Best Match Security－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－，情報処理学会研究報告，Vol. 2010-CSEC-48，No. 21(2010. 3)

4) 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，DICOMO2011，pp. 135-140(2011. 7)

5) 加藤岳久，上松晴信，名坂浩平，西垣正勝，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，DICOMO2012，pp. 788-797(2012. 7).

C その他の論文

1) 山本匠，加藤岳久，西垣正勝，振り込め詐欺への現実的な対策についての検討，CSS2010,(2010. 11).

2) Takehisa Kato, Kohei Nasaka, Takumi Yamamoto, Masakatsu Nishigaki, A Study on a Practical Measure against Billing Frauds., NBiS2011, pp.667-672, (2011).

3) 名坂康平, 加藤岳久, 西垣正勝, スマートフォン使用時の不注意による事故防止システムの提案, 情報処理学会研究報告, Vol.2012-CSEC-56 No.28, (2012.2).

付録１　調査に用いた質問紙

情報学部生における「性格特性」「セキュリティ意識」に関する意識調査

静岡大学大学院情報学研究科　西垣研究室　中澤優美子

ご記入いただきました個人情報は、研究のみに利用致します。個人を特定する情報は公表されることはありません。今回の調査結果は当方が責任をもって管理いたします（名前を記入する必要はありません）。
質問紙は２部構成になっております。

第１部　性格検査

□　音声を流します。その速度に合わせて回答して下さい。

□　**考え込まず**に、思いついたまま答えて下さい

□　３択になっていますが、**基本的には「はい」「いいえ」のどちらか**を選択して下さい。**どうしても決められない場合に「どちらでもない」**を選択して下さい。

第２部　セキュリティ意識に関する調査

□　自分の行動を振り返って、**じっくり考えて答えて下さい。**

==========

以下の事項について記述して下さい

１　性別　　１．男　　２．女

２　年齢　　（　　）歳

３　学籍番号　（　　－　　）

第１部　性格検査

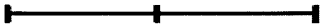
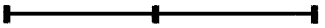
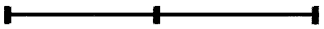
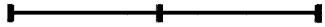
リラックスして、深く考え込まず、お答え下さい

自分に最も当てはまると思ったものに○を付けてください。

	はい	どちらとも いえない	いいえ
1. 話し好きである			
2. 平凡に暮らすより何か変わったことがしたい			
3. 注目の的になりたい			
4. 多くの点で人にひけめを感じる			
5. 心配性である			
6. 人と広く付き合うほうだ			
7. 友達よりもてきぱきと仕事が出来る			
8. やりかけたことは最善をつくす			
9. 机の上や仕事場はいつも整頓してある			
10. 人にとやかく言われると、必ず言い返す			
11. たいていの人は同情を得るため、自分の不幸を大げさに話すと思う			
12. ちょっとしたことが気になる			
13. 憂鬱になることが多い			
14. 困っている人をみると、すぐに助けてあげたくなる			
15. いろいろなものを発明してみたい			
16. こつこつやるほうだ			
17. 物事は順序よく行う			
18. 自分さえよければいいと思う			
19. 物事を難しく考えるほうだ			
20. 何事にも積極的に取り組む			

	はい	どちらともいえない	いいえ
21. 他人の苦しみがよくわかる			
22. どんなことでも試してみたい			
23. 面倒な作業でも投げ出さずにやれる			
24. 生活を規則正しくするよういつも心がけている			
25. 馬鹿にされたら、その仕返しをしたいと思う			
26. 親友でも本当に信用することはできない			
27. 自信を持っている			
28. 神経質である			
29. 生き生きしていると人に言われる			
30. 動作はきびきびしている			
31. 他人の思いもつかないようなことをすることに喜びを感じる			
32. やりかけた仕事は一生懸命最後までやる			
33. きちんとした文章を書く			
34. 何につけても人より目立ちたい			
35. 友人は陰で私の悪口を言っていると思う			
36. 理由もなく自分が惨めに思えてくることがある			
37. 陽気である			
38. 他人の行動をてきぱきと指図できる			
39. 人のために自分が犠牲になるのはいやだ			
40. コンクールで入賞したい			

	はい	どちらともいえない	いいえ
41. 意見が合わないと、相手を批判したくなる			
42. 親切な人でも心の中ではいやいややっていると思う			
43. すぐに元気がなくなる			
44. いつもやる気がある			
45. 他人の世話をするのが好きだ			
46. ふつうの人にできないような問題を解いてみたい			
47. 決めたことは何が何でもやりぬく			
48. 手紙はきちんと整理する			
49. 何かを決める時、自分ひとりではなかなか決められない			
50. わけもなく不安になることがある			
51. 人が自分を認めてくれないと不満だ			
52. 短気である			
53. 自分はつまらない人間だ			
54. 体がだるく感じることがある			
55. 話題には事欠かさないほうだ			
56. 何かと先頭に立って働くほうだ			
57. 人のためにつくすのが好きだ			
58. ねばり強くあきらめないほうだ			
59. 書棚の本はいつも決まった位置に置かれている			
60. 自分のことが話題にされるのは好きだ			

	どちらとも はい　いえない　いいえ
61. 人にハつ当たりすることがよくある	
62. 自分の考えは何かまちがっている気がする	
63. 気疲れしやすい	
64. すぐにふせぎ込んでしまう	
65. 誰とでも気さくに話せる	
66. 気の毒な人をみると、すぐに同情するほうだ	
67. 新しいアイディアを考えるのが好きだ	
68. ちやほやされるのが好きだ	
69. 自分に都合が悪くなると、相手を責めたくなる	
70. 世の中の人は人のことなどかまわないと思う	
71. 人の言いなりになってしまうことがよくある	
72. 失敗するといつまでもくよくよ考える