心理学的手法を用いた人的セキュリティホールの予測と防御

代表研究者　　越智啓太　　法政大学文学部心理学科　教授

1　問題

近年、情報セキュリティの問題は非常に大きな問題となっている。そのため、情報セキュリティ専門の企業が数多く設立され、情報セキュリティサービスを提供する企業も増えている。政府もこの問題には本腰を入れて取り組んでおり、各種の施策を実行している。しかしながら、現実的には情報セキュリティの専門家の養成は間に合っておらず、すべてのレベル（コンピューター端末レベルのセキュリティを行える一般の職員から、高度なハッキングに対応することができ、その防御システムや暴挙体制を構築できる指揮官レベルのエンジニアまで）で人材の不足が懸念されている。その中で現在に至るまで多くのセキュリティ用ソフトウェアツールやソフトウェアサービス、セキュリティ機能を盛り込んだハードウェアなどが開発されてきているが、これらの施策においては一つの大きな問題点がある。それはヒューマンファクターの問題である。

セキュリティ上の脅威としては、悪意を持った攻撃、過失による情報漏洩などさまざまなものが存在するが、このほとんどは実際にはソフトウェア、ハードウェア上の問題ではなく、人間が主になった古典的な脅威である。つまり、悪意を持って人のパスワードをのぞき見ることや、うっかりと不審なメールを開いてしまうこと、好奇心に負けて怪しいアプリをインストールしてしまうなどのヒューマンファクターによる脅威が実際には情報セキュリティインシデントの多くを引き起こしているのである。しかしながら、現在のところ、このヒューマンファクターの問題についてはほとんど明らかになっていない。具体的には、誰がどんな動機でどんな方法で悪意のある攻撃をするのかといった問題や、誰がなぜうっかりと不審なURLをクリックしてしまうのかについてはなにもわかっていないのである。この種の問題は情報工学上の問題というよりも基本的には心理学が扱うべき問題である。

この問題に正面から取り組んだ研究は世界的に見てもほとんど存在しない。一部の犯罪心理学者や情報機関が悪意あるハッカーについての研究を行っている程度である。唯一の例外は、越智（2018）による研究である。彼は、ヒューマンファクターによるセキュリティリスクを人的セキュリティホールと捉え、これを５種類のリスク行動（サイト閲覧・ダウンロードリスク、パスワード公共リスク、パスワード管理リスク、ワイファイリスク、個人行動リスク）と１種類のセキュリティ強化行動に分類し、それぞれの行動の個人差を測定する尺度を構成した。そして、これらの行動に影響している態度や認知構造について分析した。その結果、セキュリティについての社会認識（社会として情報セキュリティがどの程度重要な問題なのかについての認知)、セキュリティについてのコスト感(セキュリティにお金や時間を投資することに対するコスト感覚)、自分の周囲の人のセキュリティ行動（まわりの同僚や友人がどの程度積極的にセキュリティ行動を行っているのか）が、セキュリティリスク行動やセキュリティ強化行動と関連していることがわかった。

この研究では、それぞれのセキュリティ行動を様々な態度、認知尺度の得点から重回帰分析で予測するという方法で行われていた。しかしながら、最終的な説明率はじつはそれほど大きなものではなかった。修正済みＲ二乗値でせいぜい０．１～０．２程度であった。また、リスク行動をとる人物の性格や心理特性との関連についてはあまり明確なことはわからなかった。この研究では確かに５因子性格検査との相関はとられているが、それ以外の心理特性（たとえば、衝動性や攻撃性など）については分析されていなかった。これは、たとえば、セキュリティリスクのある人物の事前スクリーニングなどの目的を考えると十分でないと思われる。また、そもそもなぜ、セキュリティリスク行動を行ってしまうのかという問題についてもヒントが得られるわけでもなかった。

そこで本研究では、越智(2018)によって開発されたセキュリティリスク、セキュリティ強化の尺度を用いながら､それらのスコアと個人の心理特性の関係についてより詳細に分析してみることを試みることにした。具体的に本研究で用いる尺度とその特性についてはこの後詳述するが､非常に数多くある心理尺度の中から、セキュリティリスク、セキュリティ強化行動に関連していると思われる尺度を抽出し、それと越智(2018)により尺度との関連を確認するという方法論で研究を行うことにした。また、副次的な目的ではあるが、越智(2018)によって得られたデータをこの研究と異なった標本を使用して確認することによってその信頼性について検討することにした。

公益財団法人電気通信普及財団
研究調査助成報告書　第35号　2020年度

２，方法

調査参加者：18 歳以上の男女 1500 名、男性 750 名、女性 750 名、年齢層 10 代、20 代、30 代、40 代、50 代以上の 5 つのカテゴリーでそれぞれ 300 名ずつ。

調査方法：調査はウェブ調査で行った。ウェブ調査は（株）クロス・マーケティングに委託した。調査は 2019 年 12 月に行った。調査内容、所要時間の目安等についての解説文書を読んで同意したもののみ調査に回答した。回答に要した時間は 15 分程度であった。なお、調査対象者には商品などと交換することができる一定のポイントが謝礼として与えられた。回答は PC やスマートフォン上で行われ、設問の呈示順序は尺度内でランダム化されていた。

調査項目：調査参加者の性別、職業、職位、セキュリティ行動尺度、10 項目版 5 因子性格検査（10 項目版５因子性格検査（TIPI-J））、だらしさなさ尺度、環境敏感性尺度、セルフコントロール尺度、グラスミックのセルフコントロール尺度、BIS/BAS 尺度日本語版、ダークトライアド尺度、センセーショナルシーキング尺度、社会的剥奪感尺度、怒り反芻尺度、バス・ペリー攻撃性尺度（短気下位因子）、シニニズム尺度、根性尺度（日本語版 Grit-S）、コンピュータについての知識尺度を実施した。それぞれの尺度はいずれもセキュリティリスク、セキュリティ強化と関連していると思われる特性である。それらの尺度を選定した理由については個々の尺度ごとに結果の部分でのべることにする。

３，セキュリティ行動尺度の基本的な分析

３－１，先行研究との比較

まず、最初に先行研究によって構成されたセキュリティリスク尺度、セキュリティ行動強化尺度得点と今回の調査結果について比較を行った。結果を Table 1 に示す。その結果、本研究結果は先行研究のものと類似したものとなっておりセキュリティ行動尺度がある程度の信頼性をもっていることが示された。また、各尺度の得点の男女差について集計したところ、サイト閲覧・ダウンロード尺度、個人情報リスク尺度では男性が有意にリスク行動をとりやすく、ワイファイリスク尺度、個人情報リスク尺度では女性が有意にリスク行動をとりやすかった。パスワードに関するリスクは性差がなかった。リスク行動全体の合計点については男性のほうが得点が高かった。一方、セキュリティ強化得点についても男性のほうが有意に得点が高かった。これらの結果については、おおむね先行研究と同様であった。全体として、男性がハイリスク、ハイセキュリティであり、女性が比較的ローリスク、ローセキュリティであるという傾向が見られたがこれも先行研究とほぼ同様の結果であった。

Table 1 本研究と先行研究における尺度得点

	今回の結果	先行研究の結果
サイト閲覧・ダウンロード尺度	10.35	10.13
パスワード公共リスク尺度	10.03	10.06
パスワード管理リスク尺度	16.26	15.28
ワイファイリスク尺度(逆転処理前)	15.54	14.50
個人情報リスク尺度（逆転処理前）	17.69	16.70
リスク尺度合計	67.45	68.25
セキュリティ強化尺度	25.28	24.65

Table 2 各セキュリティ尺度における性差

	男性	女性	
サイト閲覧・ダウンロード尺度	12.04	8.67	*p<.01*
パスワード公共リスク尺度	10.21	9.85	*n.s.*
パスワード管理リスク尺度	16.39	16.18	*n.s.*
ワイファイリスク尺度(逆転処理前)	15.92	15.15	*p<.05*
個人情報リスク尺度（逆転処理前）	17.31	18.07	*p<.01*
リスク尺度合計	69.41	65.48	*p<.01*
セキュリティ強化尺度	26.66	23.90	*p<.01*

３－２，サイト閲覧・ダウンロード尺度

サイト閲覧・ダウンロード尺度については、平均 10.35、標準偏差 5.31 となった。ただし、歪度が 0．614 であり最低得点に偏った分布となった。重み付けの最小二乗法で因子分析を行った結果、第一因子のみで全分散の 53.36%を説明することができた。アルファ係数はα=0.816 となった。性差×年齢層（１０代～５０代まで５水準）の分散分析を行った結果、性差[F(1,1490)=168.44, p<.01]では有意な差がみられ、男性の方

が得点が高かった。年齢層[F(4,1490)=4.45, p<.01]についても有意差がみられ、多重比較の結果、５０代のリスクがほかの年齢層に比べて低いことがわかった。また、性差×年齢層の交互作用は有意差がみられなかった[F(1,1490)=1.63]。

３－３，パスワード公共リスク尺度

パスワード公共リスク尺度については、平均 10.03、標準偏差 4.68 となった。ただし、歪度が 0. 588 であり最低得点に偏った分布となった。重み付けの最小二乗法で因子分析を行った結果、第一因子のみで全分散の 34.47%を説明することができた。アルファ係数はα=0.653 となった。α係数が比較的低くなった理由は２番目の項目である「他人と共有のパソコンでパスワード入力をしている」という項目の因子負荷量がほかの項目に比べて低くなったことが原因である。性差×年齢層の分散分析を行った結果、性差[F(1,1490)=2.276]で有意な差はみられず、年齢層[F(4,1490)=29.34, p<.01]では、有意差がみられた。多重比較の結果、年齢層が高くなるにつれてリスクが低くなる傾向が示された。性差×年齢層の交互作用は有意差がみられなかった[F(1,1490)=0.401]。

３―４，パスワード管理リスク尺度

パスワード管理リスク尺度については、平均 16.29、標準偏差 5.34 となった。歪度は、-0.234 でありほぼ正規分布に近い形状となった。重み付けの最小二乗法で因子分析を行った結果、第一因子のみで全分散の 36.43%を説明することができた。アルファ係数はα=0.582 となった。α係数が低くなった理由は２番目の項目の「パスワードをノートやメモに書いている」の因子負荷量がほかの項目に比べて低くなったことが原因である。平均値もこの項目だけが低くなっており、パスワードの使い回しや記憶はよくおこなわれているものの、ノートやメモへの記載はそれに比べて少なく、やや関連が薄いことが示された。性差×年齢層の分散分析を行った結果、性差[F(1,1490)=0.589]では有意な差はみられず。年齢層[F(4,1490)=2.671, p<.05]と性差×年齢層の交互作用[F(1,1490)=2.915]に 5%水準で有意な差が見られた。多重比較の結果、男性は 30 代のリスクが低く、女性は 10 代のリスクが高いことが上記の結果を生じさせていた。

３―５，Wi-Fi リスク尺度（逆転項目）

Wi-Fi リスク尺度については、上記の３つの項目と異なり得点が高い場合に、リスクが低いということを意味している。この尺度の平均は、15.54、標準偏差 5.89 となった。歪度が-.009 で最大値と最小値が比較的多かったもののほぼ正規分布に近い形になった。重み付けの最小二乗法で因子分析を行った結果、第一因子のみで全分散の 48.03%を説明することができた。アルファ係数はα=0.779 となった。性差×年齢層の分散分析を行った結果､性差[F(1,1490)=6.407,p<.05]で有意差が見られ男性よりも女性の方がリスクが高かった。年齢層[F(4,1490)=7.719, p<.05]でも有意差が見られ、多重比較の結果、年齢層が低いほどリスクが大きいことがわかった。性差×年齢層の交互作用は有意差がみられなかった[F(1,1490)=0.214]。

３―６，個人情報リスク尺度（逆転項目）

個人情報リスク尺度も得点が高い方がリスクが低いということを意味する。この尺度については、平均 17.69、標準偏差 5.46 となった。歪度が-.345 でやや平均値よりも高い値にピークが来た。重み付けの最小二乗法で因子分析を行った結果、第一因子のみで全分散の 32. 82%を説明することができた。アルファ係数はα=0.645 となった。性差×年齢層の分散分析を行った結果、性差[F(1,1490)=7.528, p<.01]で有意差が見られ女性よりも男性の方がリスクが高かった。年齢層[F(4,1490)=6.620, p<.01]でも有意差が見られ、多重比較の結果、10 代に比べ 30 代、50 代でリスクが高いことがわかった。性差×年齢層の交互作用は有意差がみられなかった[F(1,1490)=1.249]。

３－７，セキュリティリスク尺度の合計

上記５つの尺度の合計点(Wi-Fi リスク尺度と個人情報リスク尺度は逆転済のもの)については､平均 67.45、標準偏差 14.94、歪度-.292 でやや高い位置にピークが来るもののほぼ正規分布に近い形となった。性差×年齢層の分散分析を行った結果、性差[F(1,1490)=29.83, p<.01]で有意差が見られ女性よりも男性の方がリスクが高かった。年齢層[F(4,1490)=7.844, p<.01]でも有意差が見られ、多重比較の結果、年齢層が高くなるほどリスク行動が少なくなることがわかった。性差×年齢層の交互作用は有意差がなかった

[F(1,1490)=0.636]。

３－８，セキュリティ強化尺度

セキュリティ強化尺度については、得点が高い方がリスクが低いということを意味している。この尺度の平均は、25.28、標準偏差 8.75 となった。歪度が-.031 でほぼ正規分布に近い形になった。重み付けの最小二乗法で因子分析を行った結果、第一因子のみで全分散の 38.44%を説明することができた。アルファ係数はα=0.808 となった。性差×年齢層の分散分析を行った結果、性差[F(1,1490)=39.35, p<.01]で有意差が見られ女性よりも男性の方がセキュリティ強化行動を行っていた。年齢層[F(4,1490)=11.78, p<.01]でも有意差が見られ、多重比較の結果、年齢層が高いほどセキュリティ強化行動を行っていることがわかった。性差×年齢層の交互作用は有意差がみられなかった[F(1,1490)=0.625]。

４，各尺度とセキュリティ行動との関連

４―１，10 項目版 5 因子性格検査(小塩・阿部, 2012)

まずはじめに、セキュリティリスク行動、セキュリティ強化行動と性格特性の関連について分析を行う。性格検査としては現在最もポピュラーである 5 因子性格理論にもとづいた性格検査を使用することにする。ただし、本調査は質問項目も多いことから、10 項目からなる短縮版の五因子性格検査(小塩・阿部, 2012)を使用することにした。この尺度とセキュリティの関連についてはすでに越智（2018）が、報告しているがこの研究では、外向性が高く、協調性と勤勉性が低い場合にリスク行動が多くなることと、勤勉性と開放性が高く、神経質傾向が低い場合にセキュリティ強化行動が多くなることが報告されていた。この先行研究では各性格検査のスコアの高群と低群について平均値の差の検定を行っていたが、今回の研究においては、性格検査の各尺度の得点とセキュリティリスク、セキュリティ強化等の尺度の相関を元に分析を行った。

その結果、まず、セキュリティリスク得点は、外向性、協調性、勤勉性、開放性と有意な負の相関があり、神経質傾向とは正の相関があることがわかった。ただし、外向性と開放性の相関は非常に低かった。このうち、外向性とセキュリティリスク行動との関係は、越智(2018)の研究と反対方向のものであり、より詳細な検討が必要であると思われる。また、興味深い結果として、神経質傾向がセキュリティリスク行動と正の相関を持っていたという点である。これは神経質なほど、リスキーな行動をとりやすいということを意味する。この結果は先行研究とは一貫するが、我々の直感とは反している現象だと思われる。通常は、神経質な者はリスキーな行動を避けがちだと考えやすいからである。

次に　セキュリティ強化行動であるが、これも外向性、協調性、勤勉性、開放性と正の相関があり、神経質傾向と負の相関があった。ただし、外向性、協調性との相関は非常に低かった。勤勉性、開放性とセキュリティ強化に正の相関があるというのは直感的にも理解しやすいし、先行研究とも一致するものである。一方で、神経質傾向についてはリスク行動と同様に直感に反する結果となった。つまり、通常は神経質傾向の高さはセキュリティ強化を促進するのに対して、本研究結果はそれを逆に抑制する結果となっている。これも興味深いことに先行研究と一致する結果であった。

４－２，だらしさな尺度

セキュリティのリスクのある人物として、一般的に推測しやすいのは、「だらしない」性格を持ったものである。だらしないがゆえに知らず知らずのうちにセキュリティホールを作り出してしまっているということは十分考えられる。そこで本研究では、この「だらしなさ」とセキュリティリスクの関連について分析を行った見ることにする。ただ、研究方法論上、客観的、あるいは第三者的に見ただらしなさでなく、自己評定されただらしなさとセキュリティ行動の関連を見てみたい。現在のところ、「だらしなさ」についての心理尺度は作られていないので、本研究ではまず、だらしなさ尺度を作成した。だらしなさ、とくにビジネス場面におけるだらしなさを中心として項目を集めて、結果に因子分析を行った。重み付けのない最小二乗法で分析を行い、プロマックス回転をした結果、３つの因子からなる心理尺度が構成された。第３因子までで全分散の４６．３７％を説明することができた。３つの因子は、それぞれ、だらしなさ因子（遅刻が多い、だらしがないなどの４項目から構成される)、汚さ因子（机の周りはいつも整頓されている、部屋はいつもきれいにしているの２項目、いずれも逆転項目)、仕事いい加減因子（すべき仕事や勉強はきっちりとする、上司や

リーダーからの命令には従うの２項目、いずれも逆転項目）と命名した。
セキュリティリスク、セキュリティ強化尺度との相関をとったところ、予想通り、だらしなさに関する３つの因子の得点はいずれもリスク得点と正の相関があり、セキュリティ強化とは負の相関があった。つまり、だらしない人の方がリスクが高く、セキュリティを強化していないことがわかった。とくにリスクとの相関が高く、それは、だらしなさ因子と特に関連していた。

４－３，環境敏感性尺度

ちょっとした物音や話し声などの環境のノイズに敏感で、容易に集中が妨げられてしまう人がいる一方で、このようなノイズに比較的鈍感で、ある程度の騒音下でも比較的早く適応できてしまうものがいる。前者のことをノンスクリーナー、後者のことをスクリーナーという。この傾向の個人差を測定する尺度として作成されたのが、Winstein(1978)による環境敏感性尺度である。ただし、この尺度は古く、項目も現代社会には適合しないものが少なくないため、近年、越智(2019)が最新版の尺度を構成している。また、越智(2019)は環境ノイズに関する環境敏感性尺度に加え、匂い刺激に対する敏感性尺度を構成している。環境に敏感に反応するということは、ウェブ上での操作等に関しても異常を感知しやすく、また、敏感であるため、リスク傾向が低く、セキュリティ強化傾向が高い可能性があるため。ここではこれらの尺度とネットワークセキュリティの相関関係について分析してみた。無相関検定においてはいくつかの尺度間に有意な差が見られ、とくに匂いに関する敏感性との相関が見られたが、相関係数の値は低く、また、その方向性も一貫していなかった。そのため、これらの尺度とセキュリティリスク、セキュリティ強化尺度の間には関連が存在しないと考えて良いだろう。

４―４，セルフコントロール尺度

セルフコントロールとは、より大きな満足を得るために、目の前にある短期的な欲求充足を抑制することができる能力のことを指す。例えば、ある程度の時間我慢してより多くのマシュマロを得るか、とりあえず目の前にあるマシュマロを食べるか (Mischel, Shoda, & Peake, 1988; Mischel, Shoda, & Rodriguez, 1989)、長期的に体重を減らしていき理想的な外見や健康状態を作るか、それとも目の前のケーキを食べるか、なども問題と関連している。この個人差は職業生活、学業成績、対人関係、将来にわたる成功などと関連しており、この傾向が大きい場合より適応的な行動が示され (De Ridder, Lensvelt-Mulders, Finkenauer, Stok, & Baumeister, 2012)、不適応な行動が抑制される (Moffitt, Arseneault, Belsky, Dickson, Hancox, Harrington, ... Caspi, 2011) ということが重ねて示されている。
セルフコントロールを自己評定で測定する尺度としては、Tangney ら(2004)のものが比較的良く使用されている。この尺度のオリジナルバージョンは３６項目からなるが、その短縮版尺度も構成されている。この短縮版尺度についてはわが国で尾崎らが日本語版を作成している (尾崎, 後藤, 小林, & 沓澤, 2016)。
さて、セキュリティリスクは本来ならリスクがある行動を抑制しなければならないのに、その行動から得られる短期的な満足を求め、その衝動を抑えることができずにリスキーな行動を行ってしまうことによって生じる場合があると思われる、とすれば、この尺度はセキュリティリスクと正の相関があることが考えられる。また、セキュリティ強化行動は当面、利得はないにもかかわらず長期的な観点からの投資や予防的な行動を引き起こすことが必要なので、負の相関があることが考えられる。そこで、本研究では、これらの間の関連について算出してみた。
その結果、予想通り、セキュリティリスク得点と比較的高い正の相関とセキュリティ強化得点と有意な負の相関が見られた。前者に関してはとくに、サイト閲覧、ダウンロード尺度と公共パスワード尺度との相関が高く、欲求の抑制ができないことが全体のリスクを引き上げていることを示していた。

４－５，グラスミックのセルフコントロール尺度

上記のセルフコントロールという概念と少し異なった観点から発展してきたセルフコントロール理論として、トラビス・ハーシによる理論がある。ハーシは犯罪学者であり、非行に関する絆理論を提唱したことで有名である。絆理論は非行は家族や学校に対する愛着や余暇の存在 (巻き込み)、将来に対する投資、規範意識の４つの絆によって抑制されるというものであるが (Hirschi, 1969, 2002)、彼は、その後の研究の中でこの絆理論をより発展させ、ゴットフェルソンと共著で犯罪の一般理論を提唱した (Gottfredson, & Hirschi, 1990)。この犯罪の一般理論では個人のセルフコントロール能力が究極的には犯罪行動を抑制すると考えてい

る。したがって、このセルフコントロールはどちらかといえば、逸脱行動や反社会行動などと関連したものである。ハーシの提唱したセルフコントロール概念の個人差を測定する尺度としてもっともポピュラーなのはグラスミックによるもの(Grasmick, Tittle, Bursik, & Arneklev, 1993)である。これは、衝動性や単純作業への適応、危険欲求など６領域各２項目合計１２項目からなる尺度である。ハーシ自体はこの尺度については批判的であり自ら尺度を構成している (Hirschi, 2004)が、一般的にはグラスミックの尺度が用いられることが多い。グラスミックの尺度については上田、尾崎、津富(2009) が日本語版尺度を構成している。

さきにも述べたようにセルフコントロールはリスク行動と正の関係、セキュリティ強化行動と負の関係があると考えられることからこれらの関係を算出した。グラスミックの尺度は６個の下位尺度を含んでいるので、合計点とともに各下位尺度との相関についても分析を行った。その結果、予想通り、合計点、各下位尺度得点ともにリスク行動と比較的高い正の相関が見られた。セキュリティ強化得点との間には有意な負の相関が見られたがこの値は高いとはいえなかった。リスク得点がとくに相関が高かったのは、やはり、サイト閲覧・ダウンロード尺度得点と公共パスワード尺度得点であった。

４－６，根性（グリット）尺度短縮版 (Grit-S)

学業などにおいて優れた成果を出すためには、誘惑などに惑わされずに一貫的な目標を持ち続ける力と、困難に耐えて目標を達成しようと絶えざる努力をする根気の両方が必要だと考えられている。このような考えを元に Duckworth, Peterson, Matthews, & Kelly (2007) は，これらの２つの要素をそれぞれ測定する Grit 尺度、およびその短縮版を作成している。また、この尺度は、西川、奥上、雨宮(2015) によって日本語版も作成されている。この尺度とセキュリティリスク、セキュリティ強化の関連について分析した。

分析の結果、根気下位尺度は、セキュリティ強化と有意な正の相関が見られ、一貫性のなさ下位尺度はセキュリティリスクと正の有意な相関が見られた。セキュリティリスクに関しては、サイト閲覧・ダウンロード尺度得点、公共パスワード尺度得点、パスワード管理との相関が比較的高かったが、ワイファイリスクとは関連がなく、個人情報リスクとはわずかな負の相関があった。根気尺度と一貫性のなさ尺度のを逆転させた得点の合計である根性尺度との相関では、すべてのリスク項目と負の相関があり、セキュリティ強化項目と正の相関が見られた。

４－７，BIS/BAS 尺度日本語版

パーソナリティに関しては、先に分析した５因子性格検査とならんで、Gray(1987)の提唱している生物学的なパーソナリティ理論である強化感受性理論(Reinforcement Sensitivity Theory:RST)が重要である。この理論では、人間の行動は、行動抑制系(Behavioral Inhibition Sysytem:BIS)と行動賦活系(Behavioral Activation System:BAS)によって構成されており、このバランスによってさまざまな個人差が作られるというものである。BIS は、潜在的な脅威や罰刺激を予見して注意を促し、自らの行動を抑制するシステムであり、中隔・海馬へ投射するセロトニン系伝達路と関連していると想定されている。一方、BAS は、報酬の存在や予期によって、行動を活性化させ目標に向けて動機づけを活性化されるシステムで中脳辺縁系ドーパミン経路との関係が想定されている。主観的には BIS はネガティブ感情を、BAS はポジティブ感情を生じさせる。BIS と BAS を測定する尺度としては、Carver, & White(1994)のものが存在し、この尺度がひとつの国際標準となっている。この尺度はひとつの BIS 尺度と三つの BAS 尺度からなる。BAS 尺度は、BAS 駆動系(Drive)、BAS 報酬反応系(Reward Responsiveness)、BAS 刺激探求系(Fun Seeking)から構成されている。この尺度には日本語版が存在する (安田・佐藤, 2002; 上出・大坊, 2005; 高橋・山形・木島・繁桝・大野・安藤, 2007) がこの中でオリジナルの尺度にもっとも近いのは高橋らの尺度である。この尺度の BIS 尺度の具体的な項目としては「非難されたり怒られたりすると,私はかなり傷つく」、「誰かが私のことを怒っていると考えたり，知ったりすると，私はかなり心配になったり動揺したりする」などの項目からなり、BAS 駆動系は「欲しいものがあると，私はたいていそれを手に入れるために全力を挙げる」、BAS 報酬反応系は、「私は，欲しいものを手に入れたとき，興奮し，活気づけられる」、BAS 刺激探求系は、「面白そうだと思えば，私はいつも何か新しいものを試したいと考えている」などの項目からなる。本研究ではこの日本語版尺度とセキュリティリスク、セキュリティ強化の関連について分析してみた。

分析の結果、BIS 尺度、BAS の３つの尺度ともいくつかの関係においては有意な相関は見られたが、相関係数は全体的に低く、セキュリティリスク、セキュリティ強化との関連はあまりないと考えられた。唯一、BAS 刺激探求系の得点に関して、サイト閲覧・ダウンロード尺度とパスワード公共尺度、セキュリティリスクと

の相関がみられた。

４－８，センセーションシーキング尺度

センセーションシーキング（刺激希求）特性は、Zukerman(1971)によって提唱された概念で退屈を避け、新しい刺激を求めていく特性である。この個人差を測定する尺度についても Zukerman によって作成が試みられており、スリルと冒険(Thrill and Adventure: TAS)，新奇な経験(Experience Seeking: ES)，抑制の解放(Disinhibition:Dis)，繰り返しへの嫌悪(Borden Susceptibility:BS)の４つの因子からなる尺度がよく使用されている。センセーションシーキング特性は、ある程度の危険を冒しても新たなことに挑戦する特性であるため、セキュリティ行動も含めてリスクを増加させる可能性がある。そこで、この尺度とセキュリティリスク、セキュリティ強化の関連を調べてみることにした。この尺度については、日本語版も作られている（柴田，2008)。ただし、この尺度はオリジナルな尺度と因子構成が異なり、TAS、DIS の 2 つについてはそのままであるが、ES、BS のかわりに、内的刺激希求(Internal Sensation Seeking: IS)，日常的な新奇性希求(Daily Novelty Seeking:DNS）といわれる因子が使われている。この柴田の尺度を本研究では改変して用いることにした。改良点は、以下の通りである。まず、柴田の尺度では、BIS 下位尺度が「セックスの相手がいつも同じであればやがて退屈するのは当たり前だ」などの性行動に関した質問が 5 項目中の 3 項目も占めていた。そこで、この下位尺度については、そもそもの「抑制の解放」という概念に立ち返り、既成の秩序やルールに対する反発についての項目に入れ替えたものを使用することにした。具体的には「創造的なことをするためには従来の価値観を捨てることも必要だ」などの項目を使用した。次に、DIS 尺度が「形態の着メロをよく変える」などの現代ではあまり一般的ではない行動が含まれているので、これもより一般的な行動である「スマホの機種やプランをよくかえる」に変えた。また、「ぼんやりと物思いにふけることがある」などの内的な刺激希求についての因子についてはリスク行動とあまり関係しないと思われたので今回の研究では使用しなかった。

分析の結果、3 つの下位尺度はいずれもセキュリティリスク行動と関連していた。とくに、サイト閲覧・ダウンロード尺度と公共パスワード尺度との関連が見られた。また、パスワード管理との有意な相関も見られたが、相関係数は低かった。TAS については、セキュリティ強化と正の有意な相関が見られたが、この値も低い値であった。

４－９，ダークトライアド尺度

ダークトライアドは反社会的なパーソナリティ傾向の代表的な３つの概念を包括するものである。３つの概念とは、他者操作的で人を利用して自らの利益を得ようとするマキャベリアリズム、共感性が低く感情が希薄で他者を利用する特性と衝動性を兼ね備えるサイコパシー傾向、他者からの賞賛と注目を求め、他者よりも優れた自己像を誇示しようとするナルシシズム傾向である。これらの特性と対人的、社会的問題行動には密接な関係があることがわかっている。そこで、本研究ではこれらの傾向と情報セキュリティの関係について検討しようと考えた。ダークトライアドを測定するための尺度は少なくないが、その中でももっとも簡便なものとして、 Jonason & Webster (2010) による Dark

Triad Dirty Dozen (DTDD) があり、いくつかの研究で使用されており、日本版の尺度である DTDD-J も開発されている（田村，小塩，田中 & 増井，2015)。

そこで本研究では、これらの関連について、検討してみた。その結果、ダークトライアド傾向はセキュリティリスクと比較的高い正の相関があったが、セキュリティ強化行動とは相関がなかった。この傾向は、マキャベリアリズム、サイコパシー傾向、ナルシシズムのすべてで類似したパターンであった。また、とくに、サイト閲覧・ダウンロード尺度と公共パスワード尺度と高い相関が見られ、ワイファイと個人情報に関しては全く相関が見られなかった。

４－１０，バス・ペリー攻撃性尺度（短気下位因子）

これ以降の４つの尺度はいずれも怒りや敵意に関した尺度である。怒りっぽさやいらいらしやすさと、情報セキュリティリスクやセキュリティ強化行動との関連について検討する。攻撃性についての代表的な尺度としてバス・ペリー攻撃性尺度が存在する（Buss & Perry, 1992）が、この尺度は敵意、短気、言語的攻撃、身体的攻撃の４つの因子から構成されている。このうち、短気因子は、怒りなどの感情的な行動と最も関連していると思われる。この尺度は、具体的には、「ばかにされるとすぐ頭に血が上る」などの項目から構成さ

れている。そこでこの尺度の日本版（安藤，曽我，山崎，島井，嶋田，宇津木，．．．& 坂井，1999）の短気下位因子とセキュリティ尺度の関連について分析した。その結果、セキュリティリスク行動とは有意な相関が見られたが、セキュリティ強化とは関連が見られなかった。セキュリティリスクでは、サイト閲覧・ダウンロード尺度と公共パスワード尺度、パスワード管理と関連しており、ワイファイリスクや個人情報リスクとは関連していなかった。

Table 3　各セキュリティリスク尺度項目とパーソナリティ尺度との関連

	サイト閲覧・ダウンロード	パスワード公共	パスワード管理	ワイファイ	個人情報	リスク合計	セキュリティ強化
セルフコントロール尺度	.311**	.332**	.222**	.186**	.059*	.389**	-.196**
だらしなさ	.288**	.318**	.177**	.124**	.029ns	.325**	-.128**
グラスミックSC尺度	.323**	.329**	.151**	.074**	.038ns	.315**	-.087**
マキャベリアリズム	.299**	.290**	.097**	0.043	0.044	.265**	-0.043
DNS合計	.297**	.344**	.080**	0.041	0.014	.264**	-0.014
ナルシシズム	.251**	.346**	.106**	0.048	-0.019	.248**	-0.025
サイコパス	.260**	.247**	.090**	0.036	0.026	.226**	-0.03
勤勉性	-.125**	-.141**	-.108**	-.187**	-.066*	-.225**	.227**
BAS刺激探求合計	.230**	.293**	.130**	0.01	-0.017	.218**	0.004
短気合計	.225**	.201**	.136**	0.038	0.023	.215**	-0.05
一貫性なさ合計	.251**	.291**	.205**	-0.008	-.102**	.213**	-0.035
社会的剥奪感合計	.280**	.224**	.081**	0	0.001	.199**	0.045
神経質傾向	.097**	.116**	.081**	.168**	.081**	.195**	-.195**
怒り反芻尺度合計	.213**	.179**	.146**	0.035	-0.011	.194**	-0.039
DIS合計	.225**	.255**	.195**	-0.035	-.074**	.189**	0.029
TAS合計	.238**	.246**	.106**	-0.015	-0.043	.178**	.071**
コンピュータについての知識尺度	.173**	0.033	-0.006	-.337**	-.248**	-.154**	.446**
根気尺度合計	-0.034	-0.032	-0.005	-.181**	-.148**	-.149**	.238**
協調性	-.148**	-.099**	0.012	-.084**	-.093**	-.146**	.079**
汚さ	.081**	.061*	.011ns	.155**	.080**	.142**	-.172**
仕事いい加減	.078**	.055*	-.201**	.158**	.287**	.141**	-.104**
BIS尺度合計	.076**	.117**	.189**	0.032	-.122**	.099**	-.066*
シニシズム合計	.168**	.132**	.158**	-.051*	-.117**	.094**	0.027
開放性	0.045	0.012	-.100**	-.087**	-.059*	-.072**	.156**
BAS報酬反応系合計	.102**	.137**	.231**	-.071**	-.203**	.060*	.070**
外向性	-.059*	0.043	-.073**	-0.039	-0.01	-.053*	.072**
喫煙	.113**	0.048	-0.049	-0.004	0.032	0.047	0.051
環境敏感性尺度騒音	0.044	0.03	.102**	-0.031	-.081**	0.02	-0.021
飲酒	.077**	.074*	0.033	-.072*	-0.037	0.019	.106**
環境敏感性尺度匂い	.058*	.080**	.084**	-.102**	-.107**	-0.003	.088**
BAS駆動合計	.110**	.080**	.097**	-.138**	-.169**	-0.017	.149**

セキュリティリスク尺度合計得点によってソートしてある。相関係数が+0.2以上のものと−0.2以下のものに着色してある。

４－１１，怒り反芻尺度

バス・ペリー攻撃性尺度の短気尺度が、おもに怒りやすさについて測定していたのに対して、怒り反芻尺度は、一度生じてしまった怒りを心の中で反芻して維持する傾向についての自己評価尺度である。この尺度は、本研究のために構成した。具体的には、「腹の立つことを思い出すと頭の中で何度もくり返して考えてしまう」、「怒りを頭の中でくり返して次第に怒りが大きくなることがある」などの１２項目からなる。まず、これらの尺度を因子分析した結果、１以上の固有値の因子を採択するという基準で一つだけの因子が抽出され、この因子ですべての分散の 56.1%を説明することができた。そのため、１因子の尺度として使用することにした。この尺度とセキュリティ尺度の関連について分析した結果、セキュリティリスク行動とは有意な相関が見られたが、セキュリティ強化とは関連が見られなかった。セキュリティリスクでは、サイト閲覧・ダウンロード尺度と公共パスワード尺度、パスワード管理と関連しており、ワイファイリスクや個人情報リ

スクとは関連していなかった。

４－１２，社会的剥奪感尺度

社会的剥奪感尺度は、越智・甲斐・喜入・長沼(2016)によって作成された尺度で、相対的剥奪感や社会に対する恨みなどを測定する尺度である。暴力行為などとの関連性が指摘されている。このような感情や態度は、投げやりな態度などと関連して、セキュリティリスクを増加させる可能性があると思われるので、本研究では関連について検討した。その結果、予想通り、セキュリティリスク行動とは有意な正の相関が見られたが、セキュリティ強化とは関連が見られなかった。セキュリティリスクでは、サイト閲覧・ダウンロード尺度と公共パスワード尺度と関連しており、ワイファイリスクや個人情報リスクとは関連していなかった。

４－１３，シニシズム尺度

攻撃性を構成する要素としては、短気以外にも、敵意がある。敵意についての尺度として、もっともよく用いられているのは、Cook, & Medley(1954)による Ho 尺度である。これは、MMPI から敵意や攻撃性に関する項目５０項目を集めて作られたものである。また、近年では先ほども述べたバス・ペリー攻撃性尺度の敵意下位尺度が用いられることも多い。ただし、Ho 尺度は比較的古く現代社会に適応するのは少し難しくなっていることと、バス・ペリー攻撃性尺度の敵意下位尺度はパラノイア的な敵意を測定していると考えられる点が問題点である。これに対して、Smith, & Frohm(1985) は、Ho 尺度の中心的な概念は、他人に対する皮肉的敵意(Cynical Hostility) であることを示し、また、Greenglass ら (1989) は Ho 尺度の中心的な概念は人に対する皮肉的不信(Cynical Mistrust)にあることをしめした。このシニカルな敵意の個人差を測定するために日本で作られた尺度がシニシズム尺度である (井澤・野村, 2004)。この尺度は、「たいていの人は自分の出世のためなら，平気で嘘をつくものと考えている」、「誰も信用しない方が安全である」などの項目からなるものである。この尺度とセキュリティ尺度の関連について分析した結果、上記の３つの怒り・敵意系尺度と同様に、セキュリティリスク行動とは有意な相関が見られたが、セキュリティ強化とは関連が見られなかった。セキュリティリスクでは、サイト閲覧・ダウンロード尺度と公共パスワード尺度、パスワード管理と関連していたが、相関係数は上記諸尺度よりも小さな値だった。ワイファイリスクや個人情報リスクとはわずかな負の相関が見られた。

４－１４，コンピューターについての知識尺度

コンピューターについての知識尺度は越智(2016)が、知識とセキュリティの関連について検討するために作成した尺度であり、URL やパケットキャプチャなどの１６個の専門用語についてどの程度知識があるのかを自己評定する尺度である。今回は時代の進展をふまえ、それに近年急激に普及した基本的なプログラム言語である python を加え、１７項目にしたものを実施し、それとセキュリティリスク、セキュリティ強化との関連について検討した。その結果、セキュリティ強化と非常に高い相関があったほか、ワイファイリスク、個人情報リスクと有意な負の相関が見られた。

各用語とリスクに関する項目の関連をより詳しく見ていくと、ほとんどすべての用語について、詳しく知っていると自己評定するほど、セキュリティ強化を行う傾向、セキュリティリスクが少ない傾向が見られた。また、ワイファイリスク、個人情報リスクについてはやはりすべての用語について詳しいと自己評定するほどそれらのリスクが低いということが示された。一方でパスワード公共、パスワード管理リスクについては、知識との関連が全体として弱かった。興味深いのは知識評定が高いほど、サイト閲覧・ダウンロードリスクがやや高くなるという一貫した傾向が見られたところである。これはそもそもある程度の知識がなければ、あまり危険なサイトに近づいたり、怪しいアプリケーションをダウンロードしないという行動を反映しているのだと思われる。

４－１５，飲酒喫煙習慣

飲酒喫煙習慣と反社会的な行動に関しては、一定の関連性がある可能性がある。そこで、本研究では 7 段階で評定させた自己の飲酒喫煙傾向とセキュリティリスク、セキュリティ強化の関連性について分析してみた。その結果、いずれについても明確な相関関係はみられなかった。

５，考察

５－１，セキュリティリスクの分類

５種類のセキュリティリスク尺度とセキュリティ強化尺度の６つの尺度を分類するために因子分析を行った。重み付けのない最小二乗法で固有値１以上の因子を抽出したところ２つの因子が抽出され全体の分散の49.91%を説明できた。プロマックス回転を行った結果２つの因子が抽出された。第１因子はワイファイリスク尺度、個人情報リスク尺度、それにセキュリティ強化尺度からなっていた。これを第１類型のセキュリティリスクと呼ぶことにする。第２因子はサイト閲覧・ダウンロード尺度、パスワード公共尺度そしてパスワード管理リスク尺度からなっていた。これを第２類型のセキュリティリスクと呼ぶことにする。因子間相関は、-0.045 でほとんど直交していた。セキュリティリスク、強化行動は第１、第２の大きく２つの類型に分けられるということがわかった。

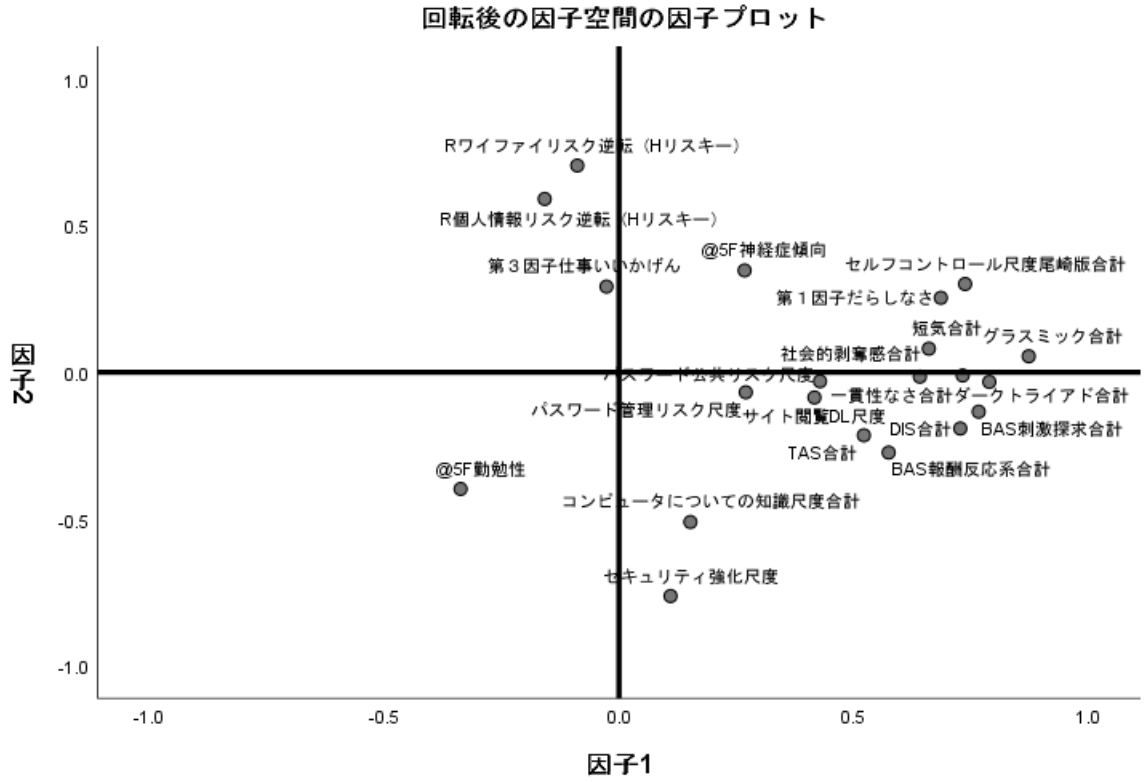

Figure 1. 各尺度間の関係を因子分析によって空間的にプロットしたもの

５－２，個人特性とセキュリティリスクの関連

本研究で用いたすべての心理尺度と５種類のセキュリティリスク尺度、セキュリティ強化尺度との相関係数を上記 Table 3 に示した。これをみると、相関は３つのパターンに大きく分けられることがわかる。まず、第１類型のセキュリティリスク尺度との相関が高いグループ、具体的にはコンピューターについての知識や勤勉性などである。次に第２類型のセキュリティリスク尺度との相関が高いグループ、具体的にはセルフコントロール尺度やマキャベリズム尺度である。第３は、いずれのセキュリティ尺度とも関連していないものである。具体的には環境敏感性やシニニズムなどがあたる。これらの関係性を示すために、第３のグループを除いた個人特性とセキュリティリスク尺度を同時に因子分析し、その因子得点を２次元上にプロットしてみた。これを Figure 1 にあげる。これをみると２つの類型のセキュリティリスクそれぞれに関連している個人特性が明確に二つのグループにわかれることがわかる。

第１類型は基本的にはコンピューターの知識や真面目さと関連している個人特性であり、これらの欠如がワイファイリスクや個人情報リスクを生じさせ、これらが存在することがセキュリティ強化を生じさせるということを示している。

第２類型は基本的には衝動性やだらしなさと関連している個人特性であり、これらの欠如がサイト閲覧・ダウンロードリスクやパスワードに関する各種リスクを生じさせるということになる。

従来、セキュリティリスクの教育においては、知識面での教育が重視されてきた。セキュリティのリスクについて教育すればそれだけ、セキュリティを行うようになると考えられてきたのである。しかし、本研究の結果はそれとは、ほぼ独立な衝動性によるリスクが存在するということが示され、それがサイト閲覧・ダウンロードやパスワードリスクと関連していることが示されたのである。ところで、標的型攻撃の被害に遭うことは、本リスク尺度ではサイト閲覧・ダウンロード尺度と関連し、また、パスワードのぞき見などのソーシャルテクノロジーやショルダーハッキングはパスワード系のリスクと関連する。このセキュリティ上の二大脅威がじつは教育とほとんど関連しないというのは非常に興味深く、恐ろしいことである。つまり、セキュリティ教育がカバーするディフェンスは、一番大きなセキュリティ上の脅威とは無関係である可能性があるということである。これらはむしろ、個人の衝動性などのパーソナリティに起因するものだからである。

Prediction of security holes using psychological methods

KeitaOCHI (Hosei University)

ABSTRACT

In this research, we investigated factors related to personalities that promote or suppress information security. As a result, it was found that opening dangerous sites and poor management of passwords are related to personal impulsiveness. On the other hand, defenselessness regarding personal information and installation of security software were related to knowledge about computers. Furthermore, the two risk factors were found to be independent. From this, it can be said that in order to eliminate human security holes, it is necessary to control impulsive behaviors rather than educate security knowledge.

【参考文献】

安藤明人, 曽我祥子, 山崎勝之, 島井哲志, 嶋田洋徳, 宇津木成介, ... & 坂井明子. (1999). 日本版 Buss-Perry 攻撃性質問紙 (BAQ) の作成と妥当性, 信頼性の検討. 心理学研究, 70(5), 384-392.

Buss, A. H., & Perry, M. (1992). The Aggression Questionnaire.Journal of Personality and Social Psychology,63,452–459.

Carver, C. S., & White, T. L. (1994). Behavioral inhibition, behavioral activation, and affective responses to impending reward and punishment: The BIS/BAS scales. Journal of Personality and Social Psychology, 67, 319–333.

Cook, W. W., & Medley, D. M. (1954). Proposed hostility and pharisaic-virtue scales for the MMPI. Journal of Applied Psychology, 38(6), 414-418.

De Ridder, D. T. D., Lensvelt-Mulders, G., Finkenauer, C.,Stok, F. M., & Baumeister, R. F. (2012). Taking stock of self-control: A meta-analysis of how trait self-control relates to a wide range of behaviors. Personality and Social Psychology Review, 16, 76–99.

Duckworth, A. L., Peterson, C., Matthews, M. D., & Kelly, D. R. (2007). Grit: Perseverance and passion for long-term goals. Journal of Personality and Social Psychology, 92, 1087–1101.

Duckworth, A. L., & Quinn, P. D. (2009). Development and validation of the Short Grit Scale (GRIT–S). Journal of personality assessment, 91(2), 166-174.

Gottfredson, M. R., & Hirschi, T. (1990). A general theory of crime. Stanford University Press.

Grasmick, H., Tittle, C., Bursik, R., & Arneklev, B. (1993). Testing the core implications of Gottfredson and Hirschi's general theory of crime. Journal of Research in Crime and Delinquency, 30, 5-22.

Gray, J. A. (1987). The psychology of fear and stress. Cambridge University Press.

Greenglass, E. R., & Julkunen, J. (1989). Construct validity and sex differences in Cook-Medley hostility. Personality and Individual differences, 10(2), 209-218.

Hirschi, T. (2002). Causes of delinquency (original version published in 1969). Transaction publishers.
Hirschi, T. (2004). Self-control and crime. Handbook of self-regulation, 537-552.
井澤修平, & 野村忍. (2004). シニシズム尺度の作成と妥当性の検討. 行動医学研究, 10(2), 66-72.
上出寛子, & 大坊郁夫. (2005). 日本語版 BIS/BAS 尺度の作成. 対人社会心理学研究, 5, 49-58.
Jonason, P. K., & Webster, G. D. (2010). The Dirty Dozen: A concise measure of the Dark Triad. Psychological Assessment, 22, 420–432.
Mischel, W., Shoda, Y., & Peake, P. K. (1988). The nature of adolescent competencies predicted by preschool delay of gratification. Journal of Personality and Social Psychology, 54, 687–696.
Mischel, W., Shoda, Y., & Rodriguez, M. (1989). Delay of gratification in children. Science, 244, 933–938.
Moffitt, T. E., Arseneault, L., Belsky, D., Dickson, N.,Hancox, R. J., Harrington, H., ... Caspi, A. (2011). A gradient of childhood self-control predicts health, wealth, and public safety. Proceedings of the National Academy of Sciences of the United States of America, 108, 2693–2698.
西川一二, 奥上紫緒里, & 雨宮俊彦. (2015). 日本語版 Short Grit (Grit-S) 尺度の作成. パーソナリティ研究, 24(2), 167-169.
越智啓太. (2018). 情報セキュリティ行動を促進・抑制する要因. 法政大学文学部紀要, 77, 77-104.
越智啓太, 甲斐恵利奈, 喜入暁, & 長沼里美. (2016). 改訂版デートバイオレンス・ハラスメント尺度の作成と分析 (3) 恋愛行動パターンと DV との関連. 法政大学文学部紀要, 73, 109-126.
小塩真司, & 阿部晋吾. (2012). 日本語版 Ten Item Personality Inventory (TIPI-J) 作成の試み. パーソナリティ研究, 21(1), 40-52.
尾崎由佳, 後藤崇志, 小林麻衣, & 沓澤岳. (2016). セルフコントロール尺度短縮版の邦訳および信頼性・妥当性の検討. 心理学研究, 87(2), 144-154.
Smith, T. W., & Frohm, K. D. (1985). What's so unhealthy about hostility? Construct validity and psychosocial correlates of the Cook and Medley Ho scale. Health Psychology, 4(6), 503-520.
柴田由己. (2008). 青年用刺激希求尺度の信頼性・妥当性の検討. パーソナリティ研究, 16(2), 198-208.
高橋雄介, 山形伸二, 木島伸彦, 繁桝算男, 大野裕, & 安藤寿康. (2007). Gray の気質モデル. パーソナリティ研究, 15(3), 276-289.
田村紋女, 小塩真司, 田中圭介, & 増井啓太. (2015). 日本語版 Dark Triad Dirty Dozen (DTDD-J) 作成の試み. パーソナリティ研究, 24(1), 26-37.
Tangney, J. P., Baumeister, R. F., & Boone, A. L. (2004). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. *Journal of Personality, 72*, 271–324.
Tangney, J. P., Boone, A. L., & Baumeister, R. F. (2018). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. In Self-regulation and self-control (pp. 181-220). Routledge.
Weinstein, N. D. (1978). Individual differences in reactions to noise: A longitudinal study in a college dormitory. *Journal of Applied Psychology*, 63(4), 458-466.
安田朝子, & 佐藤徳. (2002). 行動抑制システム・行動接近システム尺度の作成ならびにその信頼性と妥当性の検討. 心理学研究, 73(3), 234-242.
Zuckerman, M. (1971). Dimension of sensation seeking. Journal of Consulting and Clinical Psychology, 36, 45–52.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
情報セキュリティ行動を促進・抑制する要因(2)	法政大学文学部紀要	投稿中