Vol.2021-SPT-41 No.41
2021/3/2

情報セキュリティ行動に対する楽観性バイアスの影響分析

中村慎也[1]　小松文子[1]

概要：本研究はリスク認知に影響があるとされる，楽観性と情報セキュリティ行動への影響を調査分析した．インターネットモニタを対象に質問し調査を実施し，楽観性の構成因子である前向きさと気楽さそれぞれに因子と情報セキュリティ意識，認知，行動との関係を主に，因子分析と検定によって分析した．分析の結果，前向きさ因子と情報セキュリティ関連変数に関連性を見出すことはできなかったが，気楽さ因子については，気楽さの強弱を 3 分類した検定の結果，いくつかのセキュリティ行動に対してその強弱が異なることが認められた．

キーワード：情報セキュリティ対策，リスク認知，情報セキュリティ行動，楽観性バイアス

The Impact of Optimism Bias on Information Security Behavior

SHINYA NAKAMURA[†1]　AYAKO KOMATSU[†1]

Abstract: This study investigates and analyzes the influence of optimism on information security behavior, which is said to have an impact on risk perception. We conducted a survey by asking questions to Internet monitors, and analyzed the relationship between the optimism factor and information security awareness, cognition, and behavior mainly by factor analysis and tests. As a result of the analysis, we could not find any relationship between the optimism factor and the information security-related variables. However, as for the optimism factor, the results of the test that classified the strength of optimism into three categories showed that the strength of optimism differed for some security behaviors.

Keywords: Information security measures，risk perception，optimism bias

1. はじめに

近年インターネットが身近なものとなり，企業や組織のシステムや個人が所有する情報機器のセキュリティ対策は重要である．企業が悪意のある第三者によって攻撃され，顧客の個人情報が漏洩してしまう事件も多くなった．セキュリティ対策が注目されるに伴い，企業や組織そして個人のセキュリティ意識も高まっていると考えられる．しかし，被害は減少せず増加する一方である[1]．個人情報漏洩インシデントの情報を集計した NPO 日本ネットワークセキュリティ協会(以下，JNSA)の「2018 年 情報セキュリティインシデントに関する調査報告書」によると、個人情報漏洩の原因の上位は内部の人間が占めている[1]． JNSA の調査結果からシステムを利用する人間のセキュリティ意識の重要性も大切であるということがわかる．そこで本論文ではシステムを利用する側の人間の，特に，リスク認知のゆがみと言われるバイアスのうち，楽観性バイアスと情報セキュリティ行動の関係に注目した．

本論文は，まず 2 節で関連研究を述べ，3 節で研究課題を整理する．次に 4 節で仮説を述べ，5 節で仮説検証のための調査設計を述べる．6 節で分析について述べ，結果に基づき 7 節で考察する．

2. 関連研究

バイアスとは人間の認知のゆがみである．さまざまな局面で起きることがわかっている．災害における認知バイアスの研究において，菊池(2019)は，「主観的なリスク認知」と客観的リスク評定にはズレが生じていることや災害における認知バイアスの「正常性バイアス」「楽観性バイアス」「同調性バイアス」「確証バイアス」の 4 つを紹介し，これらのバイアスが災害時にどのように働くかを述べている[2]．正常性バイアスとは危険や脅威が迫っている事を示す情報に対して，ある範囲内であれば，その異常性を無視や過少視し，異常を日常的な正常文脈の範囲内として処理しようとする認知傾向のことを指す．同調性バイアスは緊急時に主体的な判断ができずに周囲の多数派の人たちの行動に同調してしまう傾向を指し，確証バイアスは人が現在持っている信念，理論，仮説を支持し，確証する情報を求め，反証となる証拠の収集を避ける傾向である．楽観性バイアスは異常事態に関する情報を楽観的に過小評価する傾向を指す．そして防災減災に向けて災害などのリスクについての直接的な知識だけでなく，そのリスクの関連情報を適切に読み解くことでリスクを正しく評価するリスクリテラシーや，思考の介在無く実行させる行動を学習することが重要であると述べている [2].

相馬,都築(2014)は，バイアス矯正の観点をあげている．

1 長崎県立大学
University of Nagasaki

まず，経験や教育を通して優れた方略を学習しバイアスを改善する改善主義，つぎに自然な環境の中でヒューリスティックが優れることから，環境を自然なものとしバイアスを改善する弁明主義，そして意思決定支援システムなどの決定ツールを使用しバイアスを改善する技法主義の 3 つを紹介し，バイアス矯正の方略とそれに対する問題を提示している[3].

吉村[4]は，人の楽観性と生活習慣やリスク認知との関連性を調べるために，まず始めに楽観性の因子分析を行い，そこで確認された前向きさと気楽さの 2 つの因子を用いて，生活習慣やリスク認知などとの関連性を調査，分析を行っている．結果として前向きな人はうつ症状，身体症状の得点が低く，気楽さが高い人はリスクテイキング行動をとる傾向が見られた[4]．荒井,吉田は，楽観性がリスク認知，犯罪不安，防犯行動へ及ぼす影響の分析を行う為に，[4]と同様楽観性の因子分析を行っている．確認されたポジティブ思考，ネガティブ思考回避，援助期待の 3 つの因子を用い調査し，男女別に分析を行っている．男性は楽観性がリスク認知や犯罪不安の減少をもたらし，ネガティブな思考を回避することで防犯行動は減少する．女性はリスク認知や犯罪不安に対して楽観性は何ら影響せず，ポジティブ思考が直接的に防犯行動を増加させていることを報告している[5].

情報セキュリティ行動の研究では，川越,内田(2008)がは，ヒューマンファクタにはエラーと違反の 2 種類が存在することを主張している．そこにはバイアスが働き，リスクを主観的に低く見積もる事を述べている．エラーではフェールセーフやフールプルーフなどのセキュアシステム技術が対策として有効であり，違反には教育及びリスクコミュニケーションが挙げられて いる．しかし，ヒューマンエラーは結果であり，組織的要因によりエラーが生じる考えである「ソーシャルファクタ」をあげ，安全対策にはソーシャルファクタが重要な鍵である事を述べている[6]．諏訪[7]らは，質問調査を統計的に分析し情報セキュリティ行動基本モデルを構築した．構築したモデルは，セキュリティ知識とセキュリティスキルの 2 要因を持つ知識，関心・リスク認知・有効性認知・コスト感・外部要請の 5 要因を持つ態度，意識的セキュリティ行動・習慣的セキュリティ行動の 2 要因を持つ行動の 3 つのプロセス について，知識の 2 要因が態度の 5 要因と行動の 2 要因に影響を与え，態度の 5 要因が行動の 2 要因に影響を与えることを仮定したものである．結果として 3 つのセキュリティ行動要因を確認し，それぞれの行動には様々な要因が起因することを明らかすると共に，セキュリティ行動の阻害要因としてコスト感がある事を示している[7].

情報セキュリティにおけるバイアスの研究は多くはないが，羽田,後藤らは SaaS(Software as a Service)と呼ばれるアプリケーションがクラウドサービスの利用として利用できるモデルに対して，SaaS ベンダと SaaS 利用者には SaaS に対して認識のずれが生じている事を挙げ，セキュリティの観点から SaaS 利用検討プロセスにリスク認知バイアスどう働くかを考察している．そして，認知バイアスを緩和するポイントとして，技術的な評価だけでなく，業務部門，IT 部門，CIO など立場別に認知バイアスをチェックすることで適切な判断ができると述べている [8].

楽観性バイアスと情報セキュリティの関係について，宮地,小松らは，間接法，直接法，LOR 法といった複数のバイアス測定の尺度を利用し，質問調査の結果を分析したが，尺度によって結果は異なり，バイアス測定の難しさを明らかにしている[9].

最後に，セキュリティ行動尺度に関連した研究について述べる．個人のセキュリティ行動を評価する尺度を開発したものである．Serge Egelman らは実験を用いてセキュリティ行動意図尺度(以下，SeBIS)を開発した．SeBIS はユーザの自己報告によるコンピュータセキュリティアドバイスの遵守を測定することに活用できるとしている[14].

3. 研究課題

前述したように様々な分野でバイアスが研究されている．我々は，[9]に引き続き，自分と同じ境遇の他者と比較して，自分はリスクにあう危険性は小さいであろうと評価する楽観主義バイアスに注目をした．本研究では[4]で報告されている楽観性の因子と生活習慣やリスク認知の研究を参照し，楽観性のセキュリティ行動への影響を明らかにすることを課題とする．

4. 検証仮説

楽観性は，「気楽さ」と「前向き」の 2 つの因子に分ける．[4]と[5]とも楽観性について因子分析し，[4]では「気楽さ」と「前向き」が，[5]では「ポジティブ思考」，「ネガティブ思考回避」，「援助期待」が因子として抽出された．「ポジティブ思考」と「前向き」は同様の因子とみなせる．また「ネガティブ思考回避」と「気楽さ」のそれぞれの因子分析の項目を比較し同様の因子とみなせると考えた．これらの 2 因子と情報セキュリティ行動について以下の仮説を立てた．

H1-1：気楽さ因子が高い人はセキュリティ意識が低い

気楽さ因子では「なんとかなる」，「良くないことが起こっても、それは一時的なこと」などを指す． このことから気楽さ因子が高い人はセキュリティ意識が低いのではないかと考えられる

H1-2：気楽さ因子が高い人はセキュリティ行動をしない

[5]によると気楽さ因子が高い人はリスクテイキング行動をする傾向が見られた．これをセキュリティに置き換えたとき，気楽さ因子が高い人はセキュリティ行動をとらない傾向があると考えられる．

H2：前向き因子が高い人はセキュリティ意識が高い.

[5]では前向きな人は健康に意欲的で，うつ症状や身体症状が低いことにつながっている結果が得られた．これをセキュリティに置き換えると，前向き因子が高い人はセキュリティ意識が高いと考えられる．

H3-1：セキュリティ意識はセキュリティ行動に正の影響を与える

[10]においてセキュリティ意識が高い人はセキュリティ知識を持ち，セキュリティ行動をしている事が述べられている．このため，本仮説でもセキュリティ意識はセキュリティ行動に正の影響を与えるとした．

H3-2：セキュリティ認知はセキュリティ知識に正の影響を与える

セキュリティ用語について名前や概要を知っているなどセキュリティ認知 ，セキュリティ用語の名称とその名称の正しい意味や詳しい内容を合わせて知っていることをセキュリティ知識とし，セキュリティ認知がある人はセキュリティ知識もあるのではないかとした．

H3-3: セキュリティ知識はセキュリティ行動に正の影響を与える

セキュリティ知識とセキュリティ行動の関連性について[8]は，セキュリティ知識が予防的セキュリティ行動・習慣的セキュリティ行動・意識的セキュリティ行動の 3 つのセキュリティ行動タイプの内，習慣的セキュリティ行動を直接的に高めていることが示されており，残りの 2 つのセキュリティ行動についても間接的に正の影響を受けていることが示されている．このことからセキュリティ知識はセキュリティ行動に正の影響を与えると仮定した．

5. 調査の設計

5.1 サンプル設計

本調査は，インターネット調査により実施する．具体的な調査方法としては，クロスマーケティング社のインターネットパネルのうち総務省情報通信白書[11]におけるインターネット利用者の割合を 20 代から 70 代以上について割り付けて 1000 名を(男性 499 名，女性 501 名)調査対象とした．

表 1　調査対象者

Table 1　Survey subjects

	男性	女性	計
20 代	71	67	138
30 代	77	77	154
40 代	100	98	198
50 代	87	88	175
60 代	78	77	155
70 代以上	86	94	180
計(人)	499	501	1000

5.2 調査内容

楽観性の因子とセキュリティ意識，セキュリティ知識，セキュリティ行動の関係を調査するための項目を以下に述べる．詳細な項目は付録 A を参照のこと．

4.2.1 楽観性因子の調査

調査項目は[5]の楽観性尺度の項目を採用した．質問に対しては「はい」,「いいえ」の 2 択で答える形式をとっている．

4.2.2 セキュリティ意識の調査

(独)情報処理推進機構(IPA)が行った情報セキュリティ脅威に対する意識調査[12]を参考にした．

4.2.3 セキュリティ認知・知識の調査

セキュリティ意識と同様に IPA が 2019 年度に実施した情報セキュリティの脅威に対する意識調査[12]と徹底攻略情報セキュリティマネジメント教科書平成 29 年度を参考とし，セキュリティ脅威や攻撃について計 10 問の質問項目とした．前半の 5 問は，情報セキュリティ認知の調査項目でセキュリティ脅威や攻撃の名称について質問する．後半の 5 問は情報セキュリティ知識の調査で，前半の 5 問の内容についてその内容が正しいか間違っているかを質問する．回答制御することで知識がない場合の不適切な回答を排除している．

4.2.4 セキュリティ行動の調査

情報セキュリティ行動は情報セキュリティ意識，情報セキュリティ知識と同様に IPA が 2019 年度に実施した情報セキュリティの脅威に対する意識調査[12]を参考とし，Serge Egelman，Eyal Peer [10]のセキュリティ行動を測定の為に作成された 16 項目と合わせて，パスワードやパソコンの取り扱いなど計 23 問の構成としている．

6. 調査結果と分析

調査結果と分析述べる．

6.1 調査結果

調査期間は 2020 年 11 月 14 日，15 日の 2 日間である．20 代～70 代以上の男性 499 人，女性 501 人，合計 1000 人の回答を収集する事ができた．

6.2 分析手順

楽観性を構成する因子を確認する為に，因子分析により因子を抽出する．続いて情報セキュリティ行動の行動タイプを調べる為に，これも因子分析し因子を抽出する．抽出された因子ごとに信頼性を確認する．次に行う相関分析では気楽さ・前向きと意識，意識と行動，認知と知識などといった変数間の関係を分析し，仮説を検証する．

統計分析には IBM の SPPS Statistics26 を使用した ．

6.3 楽観性因子の抽出

楽観性の 10 項目に対して，主因子法，プロマックス回転により因子分析した．その結果，図 1 に示すように 2 因子を確認できた．この因子は[4]と同じ結果であり，それぞれ「気楽さ」「前向きさ」を示している．また，各因子のクロンバックのα係数は気楽さ 0.78，前向きさ 0.73 であった．一般的に期待される 0.8 にはやや低いがある程度の信頼性はあると考えた．

質問項目	因子1	因子2
q2_2 私はきっと幸せになれるだろう	0.704	0.474
q2_5 私にはだいたい悪いことよりも良いことのほうが起こりやすいと思う	0.681	0.535
q2_8 自分に酔い事が起こるとは滅多に思えない(逆転項目)	0.672	0.269
q2_10 私はチャンスに恵まれている	0.648	0.387
q2_3 私の考えるように物事が運ぶとはとうてい思えない(逆転項目)	0.527	0.266
q2_9 いつも気楽でいられる	0.437	0.715
q2_1 将来についていつも楽観的である	0.480	0.653
q2_4 なんとなるさとよく思う	0.490	0.572
q2_6 先の事は気にならない	0.280	0.570
q2_7 特別に努力しなくても，何とかなるものだ	0.173	0.477

図 1　楽観性質問項目の因子負荷行列

Fig. 1　Optimism Question item factor loading matrix

6.4 情報セキュリティ行動因子

セキュリティ行動にはどのような行動タイプがあるのかを調べるために， 21 項目で因子分析を行った．因子分析は主因子法を用い，プロマックス(斜交回転)回転している．分析の結果は図 2 に示すように 4 つの因子を確認することができた．第 1 因子は，暗号化された USB メモリの利用や、重要なファイルの暗号化、機密情報が書かれている媒体は施錠できる場所に保管する、アンチウイルスソフトが最新であることを確認するなど自ら積極的に行っているセキュリティ行動の因子負荷量が大きくなっていた．

このことから第 1 因子を「**積極的セキュリティ行動**」と名付けた．第 2 因子は，web 閲覧中に，意図しないアプリケーションのインストールファイルがダウンロードされる場合にキャンセルを行うことやメール送信の際に，送信先のメールアドレスを確認するなど，注意しながら行うセキュリティ行動の因子負荷量大きくなっていた．このことから第 2 因子を「**注意的セキュリティ行動**」と名付けた．第 3 因子はパスワードを使用してノート PC やタブレット，携帯電話のロックを解除するなど，日常で習慣的に行っているセキュリティ行動の因子負荷量が大きくなっていた．このころから第 3 因子を「**パスワードセキュリティ行動**」と名付けた第 4 因子は SSL，https://など安全に送信される事を最初に確認して web サイトに情報を送信する，誰かから送られたリンクを確認してひらくなどインターネット上のセキュリティ行動の因子負荷量が大きくなっていた．このことから第 4 因子を「**ネットセキュリティ行動** 」と名付けた．4 つの因子それぞれのα係数は，習慣的セキュリティ行動，物理的セキュリティ行動は，積極的セキュリティ行動，注意的セキュリティ行動それぞれ 0.844，0.756，0.793，0.759 であった ． α係数は 0.8 以上が望ましいが，この値であっても一定の信頼はあると解釈した．

6.5 楽観性因子とセキュリティ関連の分析

抽出した二つの楽観性因子と 4 つの行動因子，セキュリティ意識，認知，知識得点の関係を分析する．まず，それぞれを相関分析した (図 3,4)．楽観性因子とセキュリティ関連変数である行動因子や得点との相関が有ると判断することはできなかった．

	因子 1	因子 2	因子 3	因子 4
q6_20 暗号化された USB メモリの利用や、重要なファイルの暗号化を行っている	.869	−.215	−100	−.033
q6_23 機密情報が書かれている媒体は施錠できる場所に保管している確認する	.725	−.201	.185	.021
q6_19 アンチウイルスソフトが定期的に更新されていることを	.656	.285	−.122	−.006
q6_18 使用するプログラムが最新である事を確認しようとする	.611	.292	−.109	−.047
q6_13web サイトを閲覧するときは、リンクをクリックする前にリンクの上にマウスを置いて移動先を確認している	.496	.173	−.032	−.137
q6_22 ゴミから情報を盗まれないよう、機密情報がかかれた紙を捨てる際はシュレッダーにかけている	.402	.166	.187	.152
q6_15web 閲覧中に、意図しないアプリケーションのインストールファイルがダウンロードされる場合はキャンセルを行っている	−.036	.766	.000	.001
q6_16 メールを送信する際、送信先のメールアドレスを確認する	.011	.704	.045	.118
q6_3 新しいオンラインアカウントを作成するとき、サイトの求める最低要件を超えるパスワードを使用しようとする	−.025	.396	.259	−.121
q6_5 設定したパスワードを書いたメモ等 wo パソコン画面やデスクの見えないところに置く(見える所においていない)	−.185	.391	.221	−.112
q6_21 不要になったパソコンやスマーフォンの破棄、またそれに保存されているデータの消去を必ず行っている	.332	.365	.092	.190
q6_2 持っているアカウントごとに異なるパスワードを使用している	.169	.311	.157	−.020
q6_17 ソフトウェアの更新について要求画面が表示されたら、すぐにインストールしている	.167	.305	−.146	−.295
q6_7 パスワードを使用してノート PC またはタブレットのロックを解除する	−.067	.165	.720	.032
q6_6 長時間使用しない場合は自動的にロックされる王にコンピュータを設定している	.110	.024	.678	.002
q6_9 パスワードやパスコードを使って携帯電話のロックを解除する	.038	.085	.543	−.054
q6_8 コンピュータの画面を離れるときは手動でコンピュータの画面をロックする	.265	−.091	.517	−.063
q6_12 逆 SSL、https：／／など安全に送信される事を最初に確認せずにwebサイトに情報を送信している	.007	.001	.023	.751
q6_10 逆.誰かからリンクを送られた時、それがどこに繋がるかを最初に確認せずに開く	.050	.164	−.148	.654
q6_14 逆 セキュリティ上の問題を発見した場合、他の誰かがそれを修正すると思うので、自分がしていた事を続ける	−.161	.037	.078	.618
q6_11 逆;URLバーを見るのではなく、外観と雰囲気に基づいてアクセスしているWebサイトを認識している	.088	−.165	−.060	.607

図 2　セキュリティ行動の因子負荷行列

Fig. 2　Factor load matrix of security behavior

	気楽さ因子	前向き因子	楽観性	セキュリティ意識	セキュリティ認知	セキュリティ知識
気楽さ因子	1	.503**	.987**	-.08*	-.041	.001
前向き因子	.503**	1	.516**	-.011	-.026	.011
楽観性	.987**	.516**	1	-.082**	-.046	.001
セキュリティ意識	-.08*	-.011	-.082**	1	.248**	.187**
セキュリティ認知	-.041	-.026	-.046	.248**	1	.769**
セキュリティ知識	.001	.011	.001	.187**	.769**	1

図 3　楽観性因子とセキュリティ関連変数との相関分析①

Fig.3　Correlation analysis　between optimism factors and security related variables -1

	気楽さ因子	前向き因子	セキュリティ行動因子 1	セキュリティ行動因子 2	セキュリティ行動因子 3	セキュリティ行動因子 4
気楽さ因子	1	.503**	.106	.059	.080*	-.006
前向き因子	.503**	1	.000	-.053	-.103	-.008
セキュリティ行動因子 1	.106**	.000	1	.712**	.638**	-.379**
セキュリティ行動因子 2	.059	-.053	.712**	1	.549**	-.284**
セキュリティ行動因子 3	.080*	-.103	.638**	.549**	1	-.330**
セキュリティ行動因子 4	-.006	-.008	-.379**	-.284**	-.330**	1

図 4　楽観性因子とセキュリティ関連変数との相関分析②

Fig.4　Correlation analysis　between optimism factors and security related variables -2

6.6　楽観性因子とセキュリティ行動因子の関連調査

相関分析では相関を確認することができなかったが楽観性因子のそれぞれを低・中・高の 3 群に分け，行動因子のそれぞれの得点の分布が 3 群のカテゴリで差がないことを帰無仮説として，Kruskal-Wallis のノンパラメトリック検定を行った(図 5)．検定の結果カテゴリ分布が異なるもの（帰無仮説が棄却されたもの）について，さらに 3 群のペアごとに楽観性因子の差が有意であるかを比較した．

仮説検定の要約

	帰無仮説	検定	有意確率	決定
1	行動因子1 の分布は 気楽さ3群 のカテゴリで同じです。	独立サンプルによる Kruskal-Wallis の検定	.002	帰無仮説を棄却します。
2	行動因子2 の分布は 気楽さ3群 のカテゴリで同じです。	独立サンプルによる Kruskal-Wallis の検定	.014	帰無仮説を棄却します。
3	行動因子3 の分布は 気楽さ3群 のカテゴリで同じです。	独立サンプルによる Kruskal-Wallis の検定	.018	帰無仮説を棄却します。
4	行動因子4 の分布は 気楽さ3群 のカテゴリで同じです。	独立サンプルによる Kruskal-Wallis の検定	.255	帰無仮説を棄却できません。

漸近的な有意確率が表示されます。有意水準は .050 です。

図 5　行動因子と気楽さ 3 群の検定

Fig.5　Test of behavioral factors and three groups of carefree

検定によると，行動因子 1，2，3 において，気楽さの得点は有意に異なることがわかった．さらに，これらの差を明らかにするために，3 群のペア（低―中，中―高，低―高）におけるペアごとの比較分析をした（図 6，7，8）

積極的セキュリティ行動では，気楽さ低群と高群に有意な差が認められた．

気楽さ3群 のペアごとの比較

Sample 1-Sample 2	検定統計量	標準誤差	標準化検定統計量	有意確率	調整済み有意確率[a]
気楽さ低群-気楽さ中群	39.030	23.487	1.662	.097	.290
気楽さ低群-気楽さ高群	-77.325	21.975	-3.519	.000	.001
気楽さ中群-気楽さ高群	-38.295	22.161	-1.728	.084	.252

各行は、サンプル 1 とサンプル 2 の分布が同じであるという帰無仮説を検定します。
漸近的な有意確率 (両側検定) が表示されます。有意水準は .05 です。
a. Bonferroni 訂正により、複数のテストに対して、有意確率の値が調整されました。

図 6　積極的セキュリティ行動因子 1 と気楽さ 3 群のペア比較

Fig. 6 Paired Comparison of Positive Security Behavior Factor 1 and three groups of Carefree

気楽さ3群 のペアごとの比較

Sample 1-Sample 2	検定統計量	標準誤差	標準化検定統計量	有意確率	調整済み有意確率[a]
気楽さ低群-気楽さ高群	-46.238	21.975	-2.104	.035	.106
気楽さ低群-気楽さ中群	66.496	23.487	2.831	.005	.014
気楽さ高群-気楽さ中群	20.258	22.161	.914	.361	1.000

各行は、サンプル 1 とサンプル 2 の分布が同じであるという帰無仮説を検定します。
漸近的な有意確率 (両側検定) が表示されます。有意水準は .05 です。
a. Bonferroni 訂正により、複数のテストに対して、有意確率の値が調整されました。

図 7　注意的セキュリティ因子 2 と気楽さ 3 群のペア比較

Fig.7 Paired Comparison of Cautious Security Behavior Factor 1 and three groups of Carefree

気楽さ3群 のペアごとの比較

Sample 1-Sample 2	検定統計量	標準誤差	標準化検定統計量	有意確率	調整済み有意確率[a]
気楽さ低群-気楽さ中群	13.165	23.487	.561	.575	1.000
気楽さ低群-気楽さ高群	-58.245	21.975	-2.651	.008	.024
気楽さ中群-気楽さ高群	-45.080	22.161	-2.034	.042	.126

各行は、サンプル 1 とサンプル 2 の分布が同じであるという帰無仮説を検定します。
漸近的な有意確率 (両側検定) が表示されます。有意水準は .05 です。
a. Bonferroni 訂正により、複数のテストに対して、有意確率の値が調整されました。

図 8　パスワードセキュリティ因子 3 と気楽さ 3 群のペア比較

Fig. 8 Paired Comparison of Password Security Behavior Factor 1 and three groups of Carefree

なお，前向きさと行動因子 4 群の Kruskal-Wallis のノンパラメトリック検定では，統計的に有意な差を見出すことはできなかった．

6.7　楽観性因子とセキュリティ意識

楽観性因子とセキュリティ意識の仮説（H1-1：気楽さ因子が高い人はセキュリティ意識が低い，H2：前向き因子が高い人はセキュリティ意識が高い）を検証するために，意識得点のそれぞれの得点の分布が楽観性因子の 3 群のカテゴリで差がないことを帰無仮説として，Kruskal-Wallis のノンパラメトリック検定を行った(図 9)．検定の結果カテゴリ分布が異なるもの（帰無仮説が棄却されたもの）について，さらに 3 群のペアごとに楽観性因子の差が有意であるかを比較した．

ノンパラメトリック検定

仮説検定の要約

	帰無仮説	検定	有意確率	決定
1	セキュリティ意識得点 の分布は気楽さ3群 のカテゴリで同じです。	独立サンプルによる Kruskal-Wallis の検定	.006	帰無仮説を棄却します。

図 9　セキュリティ意識と気楽さ 3 群の検定

Fig.9　Test of security awareness and three groups of carefree

セキュリティ意識と気楽さ因子得点は有意に異なることがわかった．さらに，これらの差を明らかにするために，3 群のペア（低―中，中―高，低―高）におけるペアごとの比較分析をした（図 10）

セキュリティ意識では気楽さ低群と気楽さ中群、気楽さ高群と気楽さ低群で有意な差が認められた．

気楽さ3群 のペアごとの比較

Sample 1-Sample 2	検定統計量	標準誤差	標準化検定統計量	有意確率	調整済み有意確率[a]
気楽さ中群-気楽さ高群	-4.385	21.183	-.207	.836	1.000
気楽さ中群-気楽さ低群	-62.899	22.450	-2.802	.005	.015
気楽さ高群-気楽さ低群	58.514	21.005	2.786	.005	.016

各行は、サンプル 1 とサンプル 2 の分布が同じであるという帰無仮説を検定します。
漸近的な有意確率 (両側検定) が表示されます。有意水準は .05 です。
a. Bonferroni 訂正により、複数のテストに対して、有意確率の値が調整されました。

図 10　セキュリティ意識と気楽さ 3 群のペア比較

Fig.10　Paired Comparison of Security awareness and three groups of Carefree

前向き因子についても同様の検定を行ったが，有意に異なる結果は得られなかった．

6.8 楽観性因子とセキュリティ認知

楽観性因子とセキュリティ意識の関係について，Kruskal-Wallis のノンパラメトリック検定を行った．その結果，セキュリティ認知と気楽さ因子得点は有意に差がないことが分かった。

また，前向き因子についても同様の検定を行ったが，有意な差を認めることはできなかった．

6.9 楽観性因子とセキュリティ知識

楽観性因子とセキュリティ意識の関係について，Kruskal-Wallis のノンパラメトリック検定を行ったが，セキュリティ知識と気楽さ因子得点は有意に差があることを認められなかった。

前向き因子についても同様の検定を行ったが，有意な差を認めることはできなかった．

6.10　分析のまとめ

以上の結果を表 2 にまとめた．楽観性因子が，セキュリティ関連の変数群と有意に差がある場合に〇を記入している．前向き因子についてはどの得点との検定に対しても有意な差は確認されなかった．積極的セキュリティ行動とパスワードセキュリティ行動で気楽さ低群と高群に，注意的セキュリティ行動で気楽さ低群と中群に，セキュリティ意識で気楽さ低群と中群・低群と高群に有意な差が見られた．

表 2　検定結果のまとめ

Table.2　Summary of approval results

	気楽さ 低―中	気楽さ 中―高	気楽さ 低―高	前向きさ
積極行動	×	×	〇	×
注意行動	〇	×	×	×
パスワード行動	×	×	〇	×
インタネット行動	×	×	×	×
セキュリティ意識	〇	×	〇	×
セキュリティ認知	×	×	×	×
セキュリティ知識	×	×	×	×

7. 考察

本研究では，楽観性の因子に基づくセキュリティへの影響分析を行う為に計 5 つの仮説を立てて検証を行った．

まず，楽観性因子のひとつである前向き因子については，すべてのセキュリティ関連因子，変数に対して統計学的に有意な差を認められなかった．この仮説の前向きな人は健康に意欲的であったこと[4]を根拠に立てたものだが，情報セキュリティは個人の生活のなかではイメージがつきにくい為，前向きな人であってもセキュリティへ意識が働かないと推察する．

つぎにもう一つの楽観性因子である気楽さについては，3 群に分割した場合，セキュリティ行動，意識に有意な差を認めることができた．気楽さにより，セキュリティリスクを十分に認知していないことが意識や行動に影響したと考えられる．仮説で述べた傾向を明らかにすることはできなかったが，気楽さの高低によってセキュリティ行動，ここでは積極的，注意的，パスワード的行動が異なることは確認できた．

一方で，楽観性 2 因子とセキュリティ認知，知識について有意な差が見られなかった．その理由として，人々がセキュリティ教育を十分に受けていないことが考えられる．認知項目 15 点満点で平均は 3.387 点と低くかったためである．今回の認知項目はパスワードリスト攻撃，ランサムウェアだが，一般のユーザがこれらの用語について知る機会が少ないのかもしれない．セキュリティがもっと身近な存在になれば認知する人も多くなり、人によっての認知の差が表れるだろう．

楽観性因子とセキュリティ知識についても．有意な差が見られなかった原因として質問項目の難易度に問題があったと考えられる．質問項目としてパスワードリスト攻撃やセキュリティホールなどの詳しい内容の正否について 5 問で設定しているが，その内，正答率が 7 割近くあったものが 1 問，7 割を超えたものが 2 問あった．そもそも、知識項目の回答は認知項目で「詳しい内容を知っている」,「概要をある程度知っている」と回答した対応する質問項目のみしか回答できないように制御を行っている。認知項目でこれら

の回答を選んだ人はセキュリティ教育を十分に受けている人であったと推測でき，そのような人たちからすると簡単な問題であったと考えられる．その為，今後研究を進めるには質問項目により専門的な知識項目を加えるなど質問項目の難易度を上げる必要がある．

最後に，本論文では，仮説として楽観性因子とセキュリティ行動などの傾向を示した（H3）が，セキュリティ意識，知識，行動についての仮説を最後まで検証することはできなかった．今後さらに詳細に分析していきたい．

8. おわりに

本研究では楽観性の因子に焦点を当て、因子に基づく情報セキュリティの意識，認知，知識と行動への影響分析を行った。楽観性因子では前向きさ因子，気楽さ因子のうち，気楽さ因子がセキュリティ関連変数へ影響していることが示唆された．今後も人と情報セキュリティの関連性の研究を進めることにより，効果ある的確な情報セキュリティ対策を講じることができるのではないかと考えている．

参考文献

[1] 2018 年情報セキュリティインシデントに関する調査結果, JNSA，2019，https://www.jnsa.org/result/incident/2018.html，(参照　2021-1-20)
[2] 菊池 聡, 災害における認知バイアスをどうとらえるか, 日本地すべり学会誌, 2018, 55 巻, 6 号, p. 286-292, 公開日 2019/01/08
[3] 相馬正史 都築誉史：意思決定におけるバイアス矯正の研究動向,立教大学心理学研究 56 巻,p.45-58,2014/03/31
[4] 吉村典子：楽観性が健康に及ぼす影響-リスクテイキング行動，生活習慣，楽観的認知バイアス，健康状態との関連から-,甲南女子大学研究紀要人間科学編 43 号,p.9-18,2007/3/20
[5] 荒井崇史 吉田富二雄：楽観性がリスク認知，犯罪不安，防犯行動へ及ぼす影響,筑波大学心理学研究 40 号,p.9-19,2010/08/10
[6] 川越秀人,内田勝也，情報セキュリティのヒューマンファクタ,社団法人情報処理学会報告書,2008-CSEC-41,2008/5/22
[7] 諏訪博彦 原賢 関良明：情報セキュリティ行動モデルの構築―人はなぜセキュリティ行動をしないのか,情報処理学会論文誌 53 巻 9 号,p.2204-2212,2011/11/30
[8] 羽田真也 後藤厚宏：SaaS 利用検討時のリスク認知バイアスの緩和に関する提案論文,第 78 回全国大会講演論文集 2016 巻 1 号,p.545-546,2016/03/10
[9] 宮地勇作 小松文子：情報セキュリティ意識に対する楽観性バイアスの影響分析,研究報告セキュリティ心理学とトラスト(SPT),2020-SPT-36,28 号,p.1-8,2020/02/24
[10] Serge Egelman　Eyal Peer：Scaling the Security wall developing a Security Behavior Intentions Scale (SeBIS), Proceedings of the SIGCHI Conference on Human Factors in Computing Systems ,2015
[11] 総務省　通信利用動向調査(令和元年), https://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000148.html
[12] (独)IPA 情報セキュリティの脅威に対する意識調査(2019 年度), https://www.ipa.go.jp/security/economics/ishikichousa2019.html (参照　2021-01-21)

付録

付録 A.1 質問項目

調査項目 楽観性と情報セキュリティ行動については，本文中に記載のため省略.

楽観性

q2_1 将来についていつも楽観的である
q2_2 私はきっと幸せになれるだろう
q2_3 私の考えるように物事が運ぶとはとうてい思えない
q2_4 なんとなるさとよく思う
q2_5 私にはだいたい悪いことよりも良いことのほうが起こりやすいと思う
q2_6 先の事は気にならない
q2_7 特別に努力しなくても，何とかなるものだ
q2_8 自分に酔い事が起こるとは滅多に思えない
q2_9 いつも気楽でいられる
q2_10 私はチャンスに恵まれている
選択肢
１．はい　２．いいえ

情報セキュリティ意識

q3_1 インターネットや情報に関するセキュリティ教育を受講した事がある
q3_2 機会があればセキュリティ教育を受講したいと思う
q3_3 情報漏洩等のニュースの報道には関心を持っている
q3_4 情報セキュリティに関する情報収集は必要だと思う
q3_5 怪しいと思われる web サイトにはアクセスしないようにしようと思っている
q3_6 不審な電子メールの添付ファイルは開かないようにしようと思っている
q3_7 不審な電子メールに記載されてある URL にはアクセスしないように使用と思っている
q3_8 セキュリティ対策ソフトを利用している
q3_9 二段階認証を利用できるものは設定している
q3_10 パソコンまたはスマートフォンで覗き見防止フィルターを使用している
選択肢
１．はい　２．いいえ

情報セキュリティ知識

・次の攻撃や脅威などについてご存じですか
q4_1 パスワードリスト攻撃
q4_2 セキュリティホール(脆弱性)
q4_3 DoS 攻撃
q4_4 ランサムウェア
q4_5 ソーシャルエンジニアリング
選択肢
１．　詳しい内容を知っている　２．概要をある程度知っている
３．名前を聞いた事がある程度　４．名前も概要も知らない

次に挙げる攻撃や脅威の概要や説明の内容が正しいか，間違っているか選択してください

q5_1 パスワードリスト攻撃とはユーザのアカウント・パスワードを解読する為に．考えられる全てのパターンを試す攻撃である
q5_2 セキュリティホールが発見されるのは windows や Mac などの OS のみであり，ブラウザなど OS 以外ではセキュリティホールは発見されることはない
q5_3 DoS 攻撃とは特定のサービスやサーバに対して，過剰なアクセスによる負荷をかける等によってサービスを妨害することである
q5_4 ランサムウェアはコンピュータウイルスの一種で，パソコンが感染するとデータ等が正常に利用できなくなることを指す
q5_5 コンピュータを操作している様子を後ろから肩越しに見てパスワードなどの情報を盗み取る攻撃はソーシャルエンジニアリングと手法である

選択肢

１．はい　２．いいえ　３．わからない

情報セキュリティ行動

q6_1 パスワードを変更する必要が無い限り，パスワードは変更しない
q6_2 持っているアカウントごとに異なるパスワードを使用している
q6_3 新しいオンラインアカウントを作成するとき，サイトの求める最小要件を超えるパスワードを使用しようとする
q6_4 必要が無い場合，パスワードに特殊文字を含めない
q6_5 設定したパスワードを書いたメモ等をパソコン画面やデスクの見えるところに置いていない
q6_6 長期間使用しない場合は自動的にロックされるようにコンピュータの画面を設定している
q6_7 パスワードを使用してラップトップまたはタブレットのロックを解除する
q6_8 コンピュータの画面を離れるときは，手動でコンピュータの画面をロックする
q6_9 PIN やパスコードを使って携帯電話のロックを解除する
q6_10 誰かからリンクを送られた時，それがどこに繋がるかを最初に確認せずに開く
q6_11 URL バーを見るのではなく，外観と雰囲気に基づいてアクセスしている Web サイトを認識している
q6_12 SSL，https://など安全に送信される事を最初に確認せずに web サイトに情報を送信している
q6_13 web サイトを閲覧するときは，リンクをクリックする前にリンクの上にマウスを置いて移動先を確認している
q6_14 セキュリティ上の問題を発見した場合，他の誰かがそれを修正すると思うので，自分がしていた事を続ける
q6_15 Web 閲覧中に，意図しないアプリケーションのインストールファイルがダウンロードされる場合はキャンセルを行っている
q6_16 メールを送信する際，送信先のメールアドレスを確認する
q6_17 ソフトウェアの更新についてプロンプトが表示されたら，すぐにインストールしている
q6_18 使用するプログラムが最新であることを確認しようとする
q6_19 アンチウイルスソフトウェアが定期的に更新されている事を確認する
q6_20 暗号化された USB メモリの利用や，重要なファイルの暗号化を行っている
q6_21 不要になったパソコンやスマートフォンの破棄，またそれに保存されているデータ消去は必ず行っている
q6_22 ゴミから情報を盗まれないよう，紙媒体を捨てる際はシュレッダーにかけている
q6_23 機密情報が保存された媒体は施錠できる場所に保管している

選択肢

１．　常に行う　２．頻繁に行う　３．時々行う　４．まれに行う
５．全く行わない