

# 情報セキュリティ意識に対する 楽観主義バイアスの影響分析

宮地勇作 小松文子

**概要:** 情報セキュリティの事故には、人を原因とした事案は多い。本論文は、人の心理に潜むバイアスに注目し、情報セキュリティ意識における楽観主義バイアスの影響を分析することを目的としている。そこで質問紙調査によって、「被害経験」「楽観主義バイアス」「意識」「知識」を調査し、楽観主義バイアスが情報セキュリティ意識に与える影響を分析したので、報告する。

**キーワード:** 情報セキュリティ, バイアス, 心理

## Analysis on Influence of the optimism bias in the Information Security Awareness

YUSAKU MIYACHI AYAKO KOMATSU

**Abstract:** There are many cases of information security accidents caused by people. this paper focuses on bias on human psychology and aims to analyze the effects of optimism bias on information security awareness. Therefore, the questionnaire survey was used to investigate “damage experience,” “optimism bias,” “consciousness,” and “knowledge,” and analyzed the effects of optimism bias on information security awareness.

**Keywords:** Information security, Bias, Psychology

### 1. はじめに

高度に発達した情報化社会において、企業や組織の資産となりうる情報をサイバー攻撃や、不正技術による悪用から防ぐ情報セキュリティの重要性が高まっている。情報セキュリティを脅かす情報の改ざんや、漏洩させるなど事象の原因として技術的なシステムの問題を想起しがちである。しかし JNSA セキュリティ被害調査ワーキンググループによると、2018 年に発生した個人情報漏洩インシデントは 443 件、想定損害賠償総額 2684 億 5743 万円であり、件数のうち約 70%がヒューマンエラーによるものであることがわかっている(図 1)。このことから高度化した情報技術を用いて悪用しようとする人々から情報を守るには技術的なセキュリティのみならず人的セキュリティを考えるのが重要である。本論文は、このようなヒューマンエラーの原因となる個人の心理と情報セキュリティの関連を明らかにすることを目的とする。

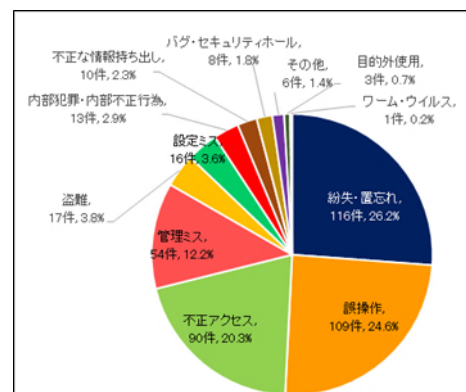


図 1 2018 年個人情報漏洩インシデント (JNSA)

人々が情報セキュリティを実施しない心理を考えるにあたり、リスク認知に関するバイアスに注目する。リスク認知のバイアスとは技術的なリスクの定義から逸脱していることを、「ゆがみ」として捉えたものである[2]。例えば、日本は地震発生件数が世界 TOP10 に入るほどの地震大国である。東日本大震災でも被害を大きくしたのは「この地震でそれほど大きな被害は出ないだろう」と考えてしまうバイアスによるものだとされている。他にもバイアスが働いて被害を大きくした例として大邱地下鉄放火事件がある。2003 年 2 月 18 に起きた大邱地下鉄放火事件では、乗客は煙が充満する車内の中で口や鼻を抑えながらも、座席に座ったまま逃げようとはせず、車内にとどまっている様子が

乗客によって撮影されていた。結果としてこの事件は世界の地下鉄火災史上2番目となる192人の死者を出した[3]。このように「自分だけは大丈夫」、「これくらいなら大丈夫」と思ってしまう心理が情報セキュリティにも働くとすれば、重大な問題である。バイアスには確証バイアスや後知恵バイアス、正常性バイアスなど様々なバイアスがあるが、それらのバイアスは何らかの物事が起きた時に自分を正当化するバイアスである。情報セキュリティの意識はインシデントが起こる前から持っているものであるため、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した。

## 2. 先行研究

本章では、情報セキュリティに関する行動の研究、楽観主義バイアスの研究、リスク認知のバイアスの研究について紹介する。

情報セキュリティに関する行動の研究で、諏訪ら[4]は情報セキュリティ基本行動モデルを構築し、結果として3タイプのセキュリティ行動が存在すること、それぞれのセキュリティ行動が異なる要因によって規定されていることを明らかにしている。また、セキュリティ行動の阻害要因として、コスト感の影響が大きく、すべてのセキュリティ行動に対して負の影響を及ぼしていることを明らかにしている。寺田ら[5]は人の行動特性が原因となるヒューマンエラーに注目し、メールの誤送信対策ツールや標的型対策ツールを開発した。メール誤送信対策ツールを使用することで送信を中止した割合(潜在的な誤送信確立)は約1%であり、午後1~3時は平均誤送信率が2%近くに上昇することを明らかにしている。また標的型メール対策ツールに関しては、ツール使用者20名と非利用者33名に対して標的型メールを送信し、開封するかどうかを評価するテストをおこなったところ、開封したのはツール利用者1名、非利用者11名という結果で標的型メール対策ツールの効果を実証している。川越ら[6]は情報セキュリティ分野におけるヒューマンエラー対策は技術的には充実しているが、結果としてヒューマンエラー低減の効果が上がっているのかどうかは明確ではなく、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課題はエラーマネジメントの不在であると考えている。また、エラーマネジメントの取組には情報セキュリティに特化した特殊な技能や技術が必要とされるわけではなく既存の取り組みに「新たな次元を与える」ものに過ぎない。としている。

楽観主義の研究において、笹竹[7]は女子大生の防犯意識は、性に関する危険な出来事の被害体験によってどのような影響を受けるかを明らかにするため、直接法、間接法を用いている。被害に遭う確率を他者と比較する楽観主義バイアス(頻度)と、被害に遭った場合の結果の重大性を他者と比較する楽観主義バイアス(程度)の2つを測定してい

る。結果として、被害体験がある場合には楽観主義バイアス(頻度)が低くなるが、防災意識の形成にまでは至らないことを明らかにしている。また、防犯意識を従属変数にし、被害体験と楽観主義バイアス(程度)を独立変数にした分散分析では、直接法では被害の有無にかかわらず、楽観主義バイアス(程度)が高いと防犯意識が低く、間接法では、特に被害体験がある場合に楽観主義バイアス(程度)が高いと防犯意識が低いことを明らかにしている。橋本ら[8]は楽観性の高い学生は楽観性の低い学生よりも健康状態がよいという結果を得ていること、楽観性が主観的幸福感を予測することを紹介している。また、楽観性とポジティブ志向の定義を紹介し楽観性、ポジティブ志向と主観的幸福感の関連を調べ、楽観性と主観的幸福感の関連についてのみ正の関連が見られた。としている。新見ら[9]は価値割引と楽観性の関連について調べている。時間的遅延によって金銭的価値を割引く傾向と2側面の楽観性(気楽さと前向きさ)との関連を検討したところ、有意な相関関係はほとんど見られなかったとしている。しかし2側面の楽観性得点に基づいて4群を構成し、価値割引率を比較したところ、気楽さ得点のみが高い気楽さ有意群が前向きさ得点のみが高い前向き有意群よりも価値割引率が高いことを明らかにしている。楽観性を測定する方法として坂本ら[10]はLOT(Life Orientation Test)と、その改訂版であるLOT-R(the revised Life Orientation Test)があり、LOT、LOT-Rを作成した原著者自身もLOT-Rの使用を推奨しているにも関わらず、日本においてはLOTが使用・紹介されることが多いとしている。このことからLOT-Rを翻訳し信頼性を検討することを目的としている。結果として内的一貫性( $\alpha$ 係数で.62)となっており、LOT-Rが6項目と少ないことを考慮すれば、一応、許容範囲であるとしている。

リスク認知の研究において、長瀬[11]はリスクを2つのタイプに分けてリスクが過小評価される要因を明らかにしている。1つは目の前に捕食者などの外敵が現れたような状況で、まさしく「いま、そこにある危機」であるタイプのリスクで「リスク1」としている。もうひとつはまれに襲ってくる天災などのリスクであり「リスク2」としている。結果として過小評価されるのは「リスク2」であり、バイアスが働く多くの事象はこの「リスク2」に分類される。要因として①鮮烈なイメージが喚起しにくい、②リスクの存在が距離的に遠く感じる、③起こる確率が比較的低く、起こるとしても遠い先に思われる、④リスクにさらされている時間が長時間に及ぶ。を挙げている。

目前に危険が迫ってくるまではその危険を認めない傾向を示す正常性バイアスの研究において、広瀬ら[12]は被験者がいる待合室に煙を流入させ、どのくらいの時間で避難するか。という実験を行っている。実験の条件として、人数(1人/3人/5人/10人)、煙の流速(通常速度/2倍の速度)、注意喚起(あり/なし)としている。結果として、煙の流入速度は

2倍の速度の方が早く避難をしており、人数条件は1人の時より3人の時の方が避難するまでの時間は長くなった。サクラ条件は3人のうち2人がサクラで煙の流入に気づいても最後まで平然としているおり、被験者も最後まで避難しようとはしなかった。注意喚起は「お待ちになっている間、何か心配なことがありましたら、いつでも私たちにおっしゃってください」と伝えるだけで注意喚起をしないと比べて避難するまでの時間を短くすることができている。以上のことより、注意喚起は正常性バイアスを予防するうえで効果的であり、周囲の人々の反応が、その場の意味付けを大きく変えてしまうことを示しており正常性バイアスを助長するとしている。

### 3. 仮説

既存研究を調べた結果、人の心理に注目した情報セキュリティの研究は存在するが、楽観主義バイアスに着目し、情報セキュリティとの関係性を示した研究は著者の知る限りなかった。そこで楽観主義バイアスと情報セキュリティの関係性を明らかにするため以下の仮説を設定した。

#### 3.1 楽観主義バイアスが高い人は情報セキュリティに対する意識が低い(H1)

楽観主義バイアスが高いということは同じ境遇の他者と比べて「危険性は小さいだろう」と考えてしまうということである。情報セキュリティにおいても「自分がサイバー犯罪に巻き込まれるはずがない」と考えることにより、日常的に安全な行動をとらない。すなわち、情報セキュリティに対する意識が低い。と仮定した。

#### 3.2 情報セキュリティに対する被害に遭った人はセキュリティに対する意識が低い(H2)

バイアスが働くのは前述した既存研究[11]における「リスク2」であるとしており、要因として、起こる確率が比較的強く、起こるとしても遠い先に思われるからである[11]。つまり、情報セキュリティ対策をしない原因は情報セキュリティに関する被害に遭う確率を低く見積もっているため情報セキュリティに対する意識が低い。と考えた。そこで、情報セキュリティに関する被害に遭わないから意識が低いのであれば、情報セキュリティに関する被害に遭ったことがある人はセキュリティに対する意識が高い。と仮定した。

#### 3.3 情報セキュリティに関する知識がある人は楽観主義バイアスが低い(H3)

人はよく知っている内容や体験した内容についてその発生確率を高く見積もる。と言われており、想像のしやすさのバイアス (Biases of imaginability)、情報が鮮烈 (vivid) であることからのバイアスなどがある。そこで、情報セキュリティに関する知識がある人は楽観主義バイアスが低い。と仮定した。

## 4. 調査

仮説を検証するために、質問紙調査によりデータを収集し、分析する。

### 4.1 調査方法

本調査は、株式会社マクロミルのインターネット調査を利用した。調査期間は2019年9月24日～26日の3日間である。調査対象者の割り当ては、総務省の通信利用動向調査[13]を元に、インターネットを利用している人を想定して設定した(表1)。

	男性	女性	計	割合
20~24歳	32	32	64	6.1%
25~39歳	58	55	113	10.8%
30~34歳	58	45	103	9.9%
35~39歳	56	48	104	10.0%
40~44歳	61	61	122	11.7%
45~49歳	86	62	148	14.1%
50~54歳	69	60	129	12.3%
55~59歳	57	33	90	8.6%
60歳以上	114	58	172	16.5%
計	591	454	1045	100%

表1 調査対象者の分布

### 4.2 調査項目

楽観主義バイアスとセキュリティ意識、セキュリティ知識の関係を調査するための項目を以下に述べる。

#### 4.2.1 情報セキュリティに関する被害経験の有無

情報セキュリティに関する被害経験の有無については、「被害に遭ったことがある」、「被害に遭ったことがない」で問う。

#### 4.2.2 楽観主義バイアスの測定

楽観主義バイアスの測定では直接法と間接法、LOT-Rを用いた。直接法では「あなた自身が、情報セキュリティに関する被害に遭う可能性は同年代の人と比較すると低いでしょうか高いでしょうか」という質問に対して「低い」、「やや低い」を選んだ人は楽観主義バイアスが高いとしている。

間接法では「あなた自身が、情報セキュリティに関する被害に遭う可能性を推測してください」という自己評価の質問に続いて「あなた以外の同年代の人が、情報セキュリティに関する被害に遭う可能性を推測してください」という他者評価の質問をしており、どちらの質問も1が「被害に遭うことはない」、5が「被害に遭うことがある」という選択肢であり、他者評価で選択した値から自己評価で選択した値を引いて正であれば楽観主義バイアスが高いとしている。

LOT-Rは10項目が設定されており(付録参照)、Q25-2,5,6,8はフィルター項目であり、Q25-3,7,9は逆転項目で

あるため、Q25-3,7,9 は点数を逆転化している。直接法については「低い」から「高い」まで、間接法については「被害に遭うことはない」から「被害に遭うことはある」まで、LOT-R については「強くそう思わない」から「強くそう思う」まで、それぞれ 5 段階で質問している。

#### 4.2.3 セキュリティ意識の測定

セキュリティ意識は(独)情報処理推進機構(IPA)が実施した情報セキュリティの脅威に対する意識調査[14]の情報セキュリティ対策の実施状況(Q11)を利用した。「怪しいと思われるウェブサイトにはアクセスしないようにしようと思っている」から「ウェブサイトの安全評価ツールを利用する必要があると思っている」までの 6 間で構成されており、質問に対し、「1. 非常に当てはまらない」から「5. 非常に当てはまる」までの 5 つの選択肢を用意している。それぞれ 6 問の回答に準ずる値をセキュリティ意識とし、6 問の合計点数をその回答者のセキュリティ意識の点数としている。

#### 4.2.4 セキュリティ知識の測定

セキュリティ知識はセキュリティ意識と同様に IPA が 2018 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[14]の事前調査票 Q8 を参考に作成している。「フィッシング詐欺」から「セクストーション」まで 5 間で構成されている。各項目に対して書いてある内容が正しいと思えば「正しい」、間違っていると思えば「間違っている」、分からなければ「わからない」を選択するよう回答を依頼している。「わからない」という回答項目を設定することにより、知識がない場合のいい加減な回答を排除できると考える。5 つの質問に対する正答数をセキュリティ知識の量としている。

### 5. 調査結果

#### 5.1 楽観主義バイアスと情報セキュリティ意識の関係

直接法、間接法における楽観主義バイアスの高低については 4.2.2 で述べたように分類した。LOT-R におけるバイアスの高低意識の高低については全体数 1045 を 0~209(0~20%)、210~418(21~40%)、419~627(41~60%)、628~836(61~80%)、837~1045(81~100%)の 5 つのグループに分け累積比率 0~20%のグループ(0~209)をバイアスが低く、81~100%のグループ(836~1045)をバイアスが高いとした。結果として、0~20%グループの 209 が 15 点に含まれるため合計点数が 15 以下の回答者をバイアスが低く、81~100%グループの 837 が 20 点に含まれるため 20 以上の回答者をバイアスが高いとしている(図 2)。

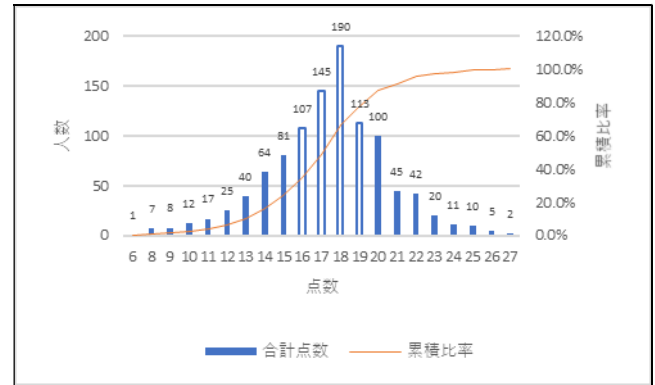


図 2 LOT-R の合計点数結果

また、意識の高低についても LOT-R 同様、1045 を 5 つのグループに分けた結果、意識の合計点数が 21 以下の回答者を意識が低く、27 以上の回答者を意識が高いとしている(図 3)。

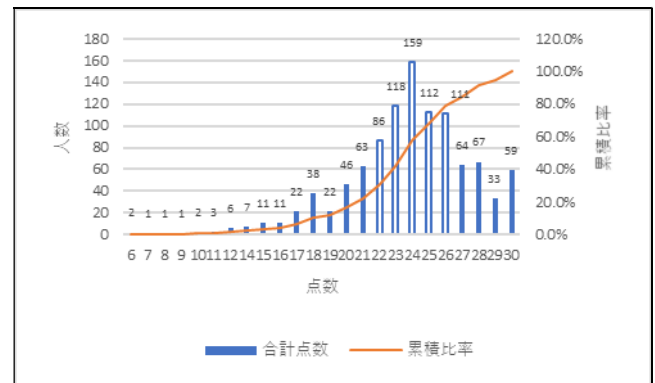


図 3 意識の合計点数結果

楽観主義バイアスと情報セキュリティに対する意識について、直接法と間接法、LOT-R の結果をそれぞれ表 2、表 3、表 4 に示す。

仮説 H1「楽観主義バイアスが高い人は情報セキュリティに対する意識が低い」を支持するには、バイアスが高い回答者は意識が低いという傾向を示すはずだが、表 2、表 4 に示すように直接法、LOT-R で計測したバイアスが認められる回答者は意識が高い傾向がある。なお、表 3 に示すように間接法で測定したバイアスが認められる回答者は意識が低い傾向にある。直接法で測定した楽観主義バイアスと情報セキュリティに対する意識に関連があるのかを調べるため、カイ 2 乗分析を行った。帰無仮説を「直接法で測定した楽観主義バイアスと情報セキュリティに対する意識は独立でない」とし、対立仮説を「直接法で測定した楽観主義バイアスと情報セキュリティに対する意識は独立である」とする。カイ 2 乗値は 0.084 であり、p 値は 0.771 であるので帰無仮説を棄却せず、直接法で計測した楽観主義バイアスとセキュリティ意識には有意水準 5% で関連があると言える。間接法、LOT-R で測定した楽観主義も同様にセ

セキュリティ意識との関係を調べたところ、間接法で測定した楽観主義とセキュリティ意識には関連があり、LOT-Rで測定した楽観主義とセキュリティ意識には関連がないことが統計学的に分かった。

直接法	バイアス 高		バイアス 低		計
意識 高	87	56.9%	43	58.9%	130
意識 低	66	43.1%	30	41.1%	96
計	153		73		226

表2 直接法で測定した楽観主義バイアスと意識

間接法	バイアス 高		バイアス 低		計
意識 高	30	48.4%	14	30.4%	44
意識 低	32	51.6%	32	69.6%	64
計	62		46		108

表3 間接法で測定した楽観主義バイアスと意識

LOT-R	バイアス 高		バイアス 低		計
意識 高	50	50.5%	75	67.0%	125
意識 低	49	49.5%	37	33.0%	86
計	99		112		211

表4 LOT-Rで測定した楽観主義バイアスと意識

### 5.2 情報セキュリティ意識とセキュリティ対策の関係

同じ調査において、セキュリティ対策の実施状況を調査する項目が4項目あり、これを使用した[15]。セキュリティ対策実施状況と意識の関係を表5に示す。表の左にある数字は4項目中で何項目セキュリティ対策を実施しているかを示している。表5に示すようにセキュリティ意識が高い人はセキュリティ対策を実施しており、セキュリティ意識が低い人はセキュリティ対策を実施していない。

	意識 高		意識 低	
4	48	40.3%	12	13.2%
3	37	31.1%	10	11.0%
2	14	11.8%	14	15.4%
1	10	8.4%	24	26.4%
0	10	8.4%	31	34.1%
	119		91	

表5 セキュリティ意識とセキュリティ対策の関係

### 5.3 被害経験の有無とセキュリティ意識の関係

被害経験の有無とセキュリティ意識の結果を表13に示す。意識の高低については5.1と同様に分類した。仮説H2「情報セキュリティに関する被害に遭った人はセキュリティに対する意識が高い」を支持するには被害経験がある回答者は意識が高い傾向にあるはずだが、表6に示すように

被害経験がある回答者は意識が低い傾向にある。5.1, 5.2と同様被害経験の有無とセキュリティ意識の関連を調べた結果、統計学的に関連があることが分かった。

	経験 有		経験 無		計
意識 高	19	43.2%	204	49.2%	223
意識 低	25	56.8%	211	50.8%	236
計	44		415		459

表6 被害経験の有無と意識の結果

### 5.4 情報セキュリティ知識と楽観主義バイアスの関係

知識の有無についてはLOT-R、意識同様に5つのグループに分けた結果、知識の合計点数が1以下の回答者を知識がなく、4以上の回答者を知識があるとしている(図4)。情報セキュリティに関する知識と楽観主義バイアスについての結果を直接法、間接法、LOT-Rの順にそれぞれ表7、表8、表9に示す。仮説H3「情報セキュリティに関する知識がある人は楽観主義バイアスが低い」を支持するには知識がある人はバイアスが低いという傾向を示すはずであり、表9では仮説を支持できる結果になっている。しかし表7、表8では知識がある回答者はバイアスが認められる傾向にある。5.1, 5.2同様にセキュリティ知識と楽観主義バイアスの関連を調べた結果、知識と直接法、LOT-Rで測定したバイアスには関連があるが、知識と間接法で計測した楽観主義バイアスには関連がないことが統計学的に示された。

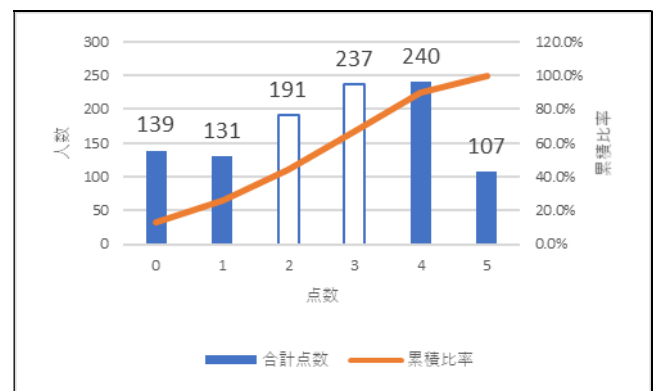


図4 知識の合計点数結果

直接法	知識 有		知識 無		計
バイアス 高	131	68.6%	82	41.6%	213
バイアス 低	60	31.4%	25	12.7%	85
計	191		107		298

表7 知識と直接法で測定した楽観主義バイアスの結果

間接法	知識 有		知識 無		計
バイアス 高	56	68.3%	26	44.1%	82
バイアス 低	26	32.7%	33	55.9%	59
計	82		59		141

表 8 知識と間接法で測定した楽観主義バイアスの結果

LOT-R	知識 有		知識 無		計
バイアス 高	88	45.6%	54	51.4%	142
バイアス 低	105	54.4%	51	48.6%	156
計	193		105		298

表 9 知識と LOT-R で測定した楽観主義バイアスの結果

## 6. 考察

仮説を検証するための分析結果について考察する。分析結果を表 10 にまとめた。仮説を支持できる結果になった場合には○、支持できなかった場合には×としており、カイ 2 乗検定の結果、関連があれば有、関連がなければ無としている。

方法	H1			H2	H3		
	直接法	間接法	LOT-R		直接法	間接法	LOT-R
仮説	×	○	×	×	×	×	○
関連	有	有	無	有	有	無	有

表 10 本調査の結果まとめ

仮説 H1 では間接法、の場合のみ仮説を支持できる結果となり、直接法、LOT-R に関しては仮説に反する結果となった。また、直接法、間接法で測定した楽観主義バイアスと意識には統計学的に関連があることがわかったが、LOT-R で測定した楽観主義バイアスと意識には統計学的に関連がないことが分かった。仮説を支持できなかった理由として、質問の中にセキュリティ対策に関する項目がないためセキュリティ対策を実施しているか不明であるからだと考える。セキュリティ意識を持ちセキュリティ対策をしている場合、自分以外の人と比較して被害に遭う確率を低く見積もるのは当然のことであるので、このような結果を示すと考える。

仮説 H2 に反する結果になった原因として選択肢に問題があったと考える。本調査は被害経験の有無 2 択で質問しており、いつ頃被害に遭ったかを考慮していない。「喉元過ぎれば熱さを忘れる」という言葉の通り、人は何か悪いことが起きても時間が過ぎることでその時の危機感や緊張感を忘れるとすれば、被害経験の有無 2 択に加えてどれくらい前に被害に遭ったかを問う必要がある。被害経験の質問項目を増やすことで結果として被害経験時期に近いほど情報セキュリティに対する意識が高いという傾向が見られる可

能性がある。

仮説 H3 では LOT-R の場合のみ仮説を支持できる結果となったが直接法、間接法に関しては仮説に反する結果となった。また、知識と直接法、LOT-R で計測したバイアスには関連があることが分かっており、さらに直接法は仮説とは逆の関連を示している。本調査で仮説に反する結果が出た原因として質問内容の難易度に問題があったと考える。質問内容として「フィッシング詐欺」から「セクストーション」までの 5 問を設定しているが 5 問中 4 問の正答率が過半数を超えており、情報セキュリティを学んでいなくても答えることが可能な質問だと考える。仮説 H3 を設定した理由として「知識がある人は情報セキュリティに関する被害を想像できている」としているので情報セキュリティを学んでいなくても答えることができるのは質問項目として適していない。そこで本調査では質問項目の難易度を上げるために本調査で実施した質問項目に加え、さらに専門的な知識を要する質問項目を増やすことで仮説を支持することができる可能性がある。

今後、情報セキュリティに対する意識と楽観主義バイアスの関係を研究する場合には、質問項目について、さらに深く考えることを勧める。

## 7. まとめ

情報セキュリティに大きな影響を及ぼす原因の一つとして楽観主義バイアスをとりあげ、情報セキュリティと楽観主義バイアスの関係性を調査した。結果として仮説を支持することはできなかった。しかし、情報セキュリティに関連するインシデントの原因にヒューマンファクタが大きく影響していることは事実である。今後、人的要因に焦点を当てた研究を進めることによって、より幅広い情報セキュリティ対策を講ずることができ、安全な情報社会に貢献できると考える。

## 参考文献

- [1] Weinstein, N. D. 1980 Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), 806–820.
- [2] 日本リスク研究学会『リスク学事典』丸善出版,2020,p.220
- [3] 広瀬忠弘『人はなぜ逃げ遅れるのか 災害の心理学』集英社,2004,p.12
- [4] 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, Vol.53 No.9 2009
- [5] 寺田剛陽 片山佳則 鳥居悟 津田宏：人の行動特性に基づくセキュリティ対策 FUJITSU. 67, 1, p.72-82 (01,2016)
- [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研究報告, 2008-CSEC-41, 2008/5/22
- [7] 笹竹英穂: 性に関する危険な出来事の被害体験が防犯意識に与える影響-楽観主義バイアスの視点から-, 犯罪心理学研究代 51 巻 第 2 号
- [8] 橋本京子 子安増生: 楽観性とポジティブ志向および主観的幸福感の関連について, パーソナリティ研究, 2011, 第 19 巻, 第 3 号, 233-244
- [9] 新見直子 宮下みのり 前田健一: 遅延による価値割引と楽観性の関連, 広島大学心理学研究, 第 9 号, 2009
- [10] 坂本真士 田中江里子: 改訂版楽観性尺度(the revised Life Orientation Test)の日本語版の検討, 健康心理学研究, Vol.15, No.1
- [11] 長瀬勝彦: リスク認知のバイアス-なぜリスクが過小評価されるのか-, 組織化学, Vol.45, No.4:56-65(2012)
- [12] 広瀬弘忠 杉森伸吉: 正常性バイアスの実験的検討, 東京女子大学心理学紀要, 2005 年, 創刊号, pp.81-86
- [13] 総務省 通信利用動向調査(平成 30 年)
- [14] IPA 情報セキュリティの脅威に対する意識調査の情報セキュリティ対策の実施状況(2018 年 12 月)
- [15] 田崎来実: 個人のリスク認知と情報セキュリティ対策行動, セキュリティ心理学とトラスト研究発表会, 2020.3

## 付録 質問項目

### 被害経験

Q22 あなたはこれまで情報セキュリティに関する被害に遭ったことがありますか。

### 楽観主義バイアス(直接法)

Q23 あなたが業務中に情報セキュリティに関する被害に遭う確率はあなたと同様の業務環境の人と比較すると低いでしょうか高いでしょうか。推測して回答してください。  
※業務で使用しない方は、ご自身が使用している環境と同様の環境の人と比較して回答してください。

### 楽観主義バイアス(間接法)

Q24-1 あなた自身が情報セキュリティに関する被害に遭う可能性を推測してください

Q24-2 業務環境などが同様のあなた以外の人が情報セキュリティに関する被害に遭う可能性を推測してください※業務で使用しない方は、ご自身が使用している環境と同様の環境の人と比較して回答してください。

### 楽観主義バイアス(LOT-R)

Q25-1 はっきりしないときでも、ふだん私は最も良いことを期待している

Q25-2 私はたやすくリラックスできる

Q25-3 何か私にとってうまくいかなくなる可能性があるれば、それはきっとそうなるものだ

Q25-4 私は自分の将来についていつも楽観的である

Q25-5 私にはたくさんの友人がいる

Q25-6 忙しくあり続けることは私にとって大切である

Q25-7 私はものごとが自分の思い通りにいくとほとんど思っていない

Q25-8 私は非常にたやすくとりみだしてしまうようなことはない

Q25-9 良いことが私に起こるなんてほとんどあてにしていない

Q25-10 概して、私は悪いことよりも良いことの方が自分の身に起こると思う

### セキュリティ意識

Q26-1 怪しいと思われるウェブサイトにはアクセスしないようにしようと思っている

Q26-2 不審な電子メールの添付ファイルは開かないようにする必要があると思っている

Q26-3 セキュリティ対策ソフトを導入、活用する必要があると思っている

Q26-4 Windows Update 等によるセキュリティパッチの更新は必要だと思っている

Q26-5 暗号化された USB メモリの利用や重要ファイルの暗号化は必要であると思っている

Q26-6 ウェブサイトの安全評価ツールを利用する必要があると思っている

### セキュリティ知識

Q27-1 フィッシング詐欺についてメールのタイトルや本文については偽装できても、メールの送信者欄(From アドレス)まで偽装することは不可能です

Q27-2 ワンクリック詐欺について、突然、アダルトサイトの会員登録完了などの画面が表示された場合、時間が経つと追加請求されることがあるのですぐに誤登録であることを電話やメールで伝えることが大切です

Q27-3 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 以外でセキュリティホールが発見されることはありません

Q27-4 偽セキュリティソフトは正常なパソコンにも関わらず、不具合が多数発見されたという表示をして、対処するために対策ソフトを購入するように促します

Q27-5 セクストーションとは SNS などでも知り合った異性からプライベートな写真や動画のやりとりを持ち掛けられた後、その写真や動画をばら撒かれたくなければ金銭を支払え、などと脅迫されることです

### セキュリティ対策

Q9-1 現在使用しているソフトウェアが最新のものであるか確認していますか

Q9-2 ウィルス対策ソフトウェアが定期的に更新されている

ることを確認していますか

Q9-3 現在使用しているパソコンがバックアップされているか確認していますか

Q9-4 ソフトウェアの更新を求められたら直ぐにインストールしていますか