

視覚障害者の大学生における情報セキュリティ疲れの考察

垣野内 将貴¹ 面 和成²

概要: ICT利用者にとって、情報セキュリティ対策は常に考えなければいけない課題で、その対策が面倒であったり、手間がかかったりと、精神的な消耗感（情報セキュリティ疲れ）へとつながることもある。このような情報セキュリティ疲れに陥ることで、情報セキュリティ対策効果が上がらなくなることがすでに明らかにされ、施策が提案されている。しかしながら、視覚障害者には晴眼者の施策では対応できない問題があるにもかかわらず、先行研究では晴眼者のみを対象としており、視覚障害者は対象としていない。さらに、視覚障害者のユーザブルセキュリティの研究でも、認証技術や認証方法に関する研究はされているものの、情報セキュリティ疲れに関する研究はまだ少ない。本稿では、視覚障害者の大学生に限定して調査を行い、結果を分析した。その結果、晴眼者のコンディションマトリクス上の分布は6群がほぼ一様であったのに対し、視覚障害者での分布は大きく異なり、セキュリティ対策実施度が高い学生ほどセキュリティ疲労度も高いことがわかった。また、晴眼者に対する既存研究での対策案では補いきれない部分を考慮して、視覚障害者ならではの施策も明らかにした。

キーワード: セキュリティ疲れ, 潜在ランク理論, 視覚障害者, スクリーンリーダー

Study on information security fatigue in visually impaired university students

Abstract: For ICT users, information security measures are always an issue that must be considered, and it may lead to a sense of mental exhaustion (information security fatigue) due to the troublesome and time-consuming measures. It has already been shown that such information security fatigue prevents the effectiveness of information security measures, and some necessary measures are proposed. However, even though the visually impaired have some problems that cannot be dealt with by the measures taken by the sighted, the previous studies have targeted only the sighted and not the visually impaired. In addition, in the research of usable security for the visually impaired, although there has been research on authentication technology and methods, there is still little research on information security fatigue. In this paper, we conducted a survey only among visually impaired university students and analyzed the results. As a result, we found the distribution on the condition matrix of the sighted students was almost even among the six groups, in contrast, the distribution of visually impaired students was very different, and we found that the higher the level of implementation of security measures, the higher the level of security fatigue. In addition, we clarified the countermeasures for the visually impaired, taking into account the fact that the countermeasures proposed in the existing research for the sighted cannot fully compensate for their effects.

1. はじめに

昨今、著しい ICT 技術の高度化に伴って、情報漏洩やサイバー攻撃など、情報セキュリティに関する脅威が多様化している。これらの脅威への対策として、利用者は情報セキュリティ対策が求められる。総務省の「国民のための情

報セキュリティサイト」では、初心者のための三原則として、「ソフトウェアの更新」「ウイルス対策ソフトの導入」「ID とパスワードの適切な管理」を挙げている [2] が、利用者が使う Web サービス・ソフトウェアは様々であり、必要な対策もその多様化に応じて日々増え、細分化していく。また、攻撃者の技術も日々進歩するため、最新の情報に意識を向ける点も大切である。

2016 年の NIST (US National Institute of Standards and Technology) の調査 [2] で、日々の更新に対して、嫌気が差

¹ 筑波技術大学
Tsukuba University of Technology
² 筑波大学
University of Tsukuba

したり、疲労感を感じて無謀な行動をとったりしてしまうことが明らかになった。このような行動をセキュリティ疲れ (Security fatigue) と呼んでいる [3]。

畑島らはこのセキュリティ疲労度とセキュリティ対策実施度との関連を探り [4], [5], [6], [7], [8], [9], 可視化するモデルとして情報セキュリティコンディションマトリクスという分類で整理した上で、各群に対する施策を提案した。しかし、これは晴眼者に限った話で、視覚障害者においても、同様の分布になるのか、同じような施策で対応可能なのかは明らかになっていない。世界には 2012 年時点で約 2 億 8,500 万人の視覚障害者がおり、そのうち約 3,900 万人が全盲であると推定されている [10]。これは世界の人口の約 3% に相当し、ICT 利用者の中ではさらに高い割合になると思われる。視覚障害者にとって ICT は晴眼者以上に生活必需品となっているため、視覚障害者にとってこれまでの研究結果である施策が有効であるかどうかを検証することには十分な価値があると考えられる。また、Prakash ら [11] が指摘する通り、視覚障害者が ICT 利用時に用いるスクリーンリーダーについての教育がまだまだ不足しており、アクセシビリティを高める上でもその教育が不足していることは大きな問題となっている。

本稿では、視覚障害者の大学生に限定して調査を行い、結果を分析した。その結果、晴眼者のコンディションマトリクス上の分布は 6 群がほぼ同様であったのに対し、視覚障害者での分布は大きく異なり、セキュリティ対策実施度が高い学生ほどセキュリティ疲労度も高いことがわかった。また、晴眼者に対する既存研究での対策案では補いきれない部分を考慮して、視覚障害者ならではの施策も明らかにした。本稿の貢献は、(1) 分布の違いを明らかにしたこと、(2) 視覚障害者ならではの施策を 2 件提案したことにある。具体的には以下の通りである。

- (1) 畑島らの提案した情報セキュリティコンディションマトリクスでの分類を視覚障害者への調査をもとに行ったところ、晴眼者のときには一様だった分布が、視覚障害者の場合は、正の相関が見られた。すなわち、情報セキュリティ対策実施度が高いほど、情報セキュリティ疲労度も高くなることがわかった。
- (2) ICT を利用する視覚障害者と切っても切れない関係にあるスクリーンリーダーについて、特に回答者の多かったグループにおいて、どのような施策が必要なのかを 2 件新たに提案する。

2. 準備

2.1 セキュリティ疲れ

情報セキュリティ疲れ (Security Fatigue) は、Furnell と Thomson により 2009 年に提唱 [3] され、2016 年には NIST の Stanton らによって、実態が分析され、セキュリティ疲

表 1 情報セキュリティコンディションマトリクス
Table 1 Information security condition matrix.

高疲労度状態 F+	F+ImL 群	F+ImH 群 (5.2 節)
理想疲労度 状態 F0	F0ImL 群	F0ImH 群 (理想状態)
低疲労度状態 F-	F-ImL 群 (5.1 節)	F-ImH 群
	対策実施度：低 ImL	対策実施度：高 ImH

F:情報セキュリティ疲労度
Im:情報セキュリティ対策実施度

れを軽減するための 3 つの提言 [2] も示している。また、畑島らによって情報セキュリティ疲れとそれを軽減するための施策がまとめられている [5]。

2.2 潜在ランク理論

学力テストによる通信簿の評価などに代表されるような数段階のランクに分けて評価をする際に、質的評価ができることを目指して作られた理論である。潜在尺度に順序尺度を仮定することで、どのランクに所属する確率が最も高いかを推定して、ランクを決定していく。荘島は exametrika というソフト [12] を開発し、Excel を活用して潜在ランク理論を用いた分析ができるようにしている。

2.3 情報セキュリティコンディションマトリクスによるアセスメント

畑島ら [4] は、表 1 のような情報セキュリティコンディションマトリクスを示し、F0ImH が理想状態であることを定義した。これは、セキュリティ疲労度 (F 群) を 3 ランクに、セキュリティ対策実施度 (Im 群) を 2 ランクに設定して、その組み合わせで 6 群に分類したものである。

2.4 スクリーンリーダー

視覚障害者において、PC やスマートフォンを使う上で、スクリーンリーダーの使用は欠かせない。2018 年 9 月の WebAIM(Accessibility in mind) が弱視者 248 人に対して行った調査 [13] によれば、弱視者のうち 59.9% が PC でスクリーンリーダーを用いており、モバイル・タブレットでは弱視者のうち 58.1% がスクリーンリーダーを用いている。

また、Prakash らは、国際社会において、スクリーンリーダーの正式なトレーニングの機会を増やすことが、社会的地位やその他の機会や資源に関連する要因による格差を減らすのにも役立つ [11] と述べている。

本研究で、視覚障害者がスクリーンリーダーを使ったおかげで高まる安全性や、使ったせいで高まる危険性について明らかにした上で、情報セキュリティ教育の一環として

提供することが、適切で安全な ICT 環境を整えることにつながると思う。

3. 関連研究

3.1 情報セキュリティ施策に対する行動

Koppel らは、ICT の一般ユーザとサイバーセキュリティの専門家とは、パスワードに対する認識は大きく異なっており、一般ユーザにはセキュリティ向上のための誤解や誤ったアプローチが見られることを明らかにした [14]。この中で、適切なセキュリティ対策を実施してもらう上で、このような誤解や誤ったアプローチを減らしていく工夫が必要である。

3.2 視覚障害者における情報セキュリティ

視覚障害者における情報セキュリティについての研究は、CAPTCHA (completely automated public Turing test to tell computers and humans apart) の代わりに独自のシステムを開発した研究 [15] や、既存のオーディオ CAPTCHA を改良したシステムを開発した研究など [16] があるものの、セキュリティ疲れに言及しているものはまだまだ少ない。

一方で、視覚障害者に限らず、スマートフォンのアクセシビリティ機能に関するトレーニング教材を、世界中の学校やすべての障害のある若者が簡単に利用できるようにする必要が明らかになっている [11]。視覚障害者の情報セキュリティ疲れを考える上で、情報セキュリティ教育を含む ICT 教育を充実させることには、このようなトレーニング教材の提示の観点からも意義があると考えられる。

また、視覚障害者に対しての研究として、直接視覚障害者を対象にできず、目隠した晴眼者などを対象とすることも多く、対象を直接視覚障害者に限定したものはまだまだ少ないことがレビュー論文 [17] からも明らかになっている。本研究では、直接視覚障害者を対象として、晴眼者との違いに迫ることを目的としている。

4. 調査と分析の概要

本章で、畑島らがこれまでの研究 [4], [5], [6], [7], [8] で整理した尺度と質問紙についてまとめる。本稿ではこれらを転用し、改良として、4.1.3 項で述べる質問を追加した。分析については、[4] で行われた分析と同様であり、4.3 節にて述べる。

4.1 質問紙の作成

4.1.1 情報セキュリティ疲労度尺度

情報セキュリティ疲労度尺度は、(1) 文献 [18] に掲載の MBI-GS 英語版および久保の (日本版) バーンアウト尺

度 [19] から 5 項目の仮説因子名を抽出した 5 択の 23 項目で構成される質問紙が先行研究 [6] において作成され、(2) 先行研究 [7] において (1) の質問紙を用いて大学生を対象とした質問紙調査を実施し、因子分析と信頼性の検討、および妥当性の検討によって 13 項目に短縮した質問紙 (付録質問 2) を作成するという手順で実施された。

4.1.2 情報セキュリティ対策実施度尺度

情報セキュリティ対策実施度の測定には、ウイルス感染経験や IT 知識および IT スキルを設定した浜津ら [20] にならって、情報セキュリティ対策経験およびセキュリティに対する知識として、IPA (独立行政法人情報処理推進機構) が発表した 2015 年に社会的に影響が大きかった情報セキュリティ 10 大脅威 [21]、および総務省によるテレワークセキュリティガイドライン [22] における「テレワーク勤務者が実施すべき対策」から 2017 年に参照して翻案し、17 項目を畑島らが作成した [8] ものから、大学生など企業に勤めない人も対象とするために企業施策に関する設問を除外した 5 択の 11 項目からなる質問紙 (付録質問 3) を作成した [4]。

4.1.3 情報セキュリティに対して視覚障害者ならではの安全さや危険性に対する所感の自由回答

先行研究で晴眼者に限って情報セキュリティ疲労度と対策実施度を調査していたのに対して、本研究では視覚障害者を対象に調査する。その上で、被験者の独自の経験を抽出する目的で、次のような 2 つの設問を設けた。(質問 1, 4)

- (1) あなたは PC やスマートフォンを使うときに音声と視覚どちらを頼りにすることが多いですか。どちらかに○をつけてください。(音声・視覚)
- (2) 情報セキュリティ対策に関連して、視覚障害のせいで「不正にひっかかりやすい」と感じたり、視覚障害のおかげで「不正にひっかかりにくい」と感じたりしたことがあればお考えを自由に記述してください。

4.1.4 情報セキュリティに対する所感の自由回答

4.1.3 項での設問の他にも、各群の特徴を抽出してアセスメントを実施する目的で、回答者の情報セキュリティに対する所感を自由回答させる設問「情報セキュリティ対策について、その他考えていることがあればお考えを自由に記述してください」を設けた。(質問 5)

4.2 質問紙調査の実施

作成した質問紙を用いた調査を、首都圏内の国立大学で実施した。実施に先がけ、組織内研究倫理審査委員会での審査を経て、承認を得ている。調査は 2021 年 9 月 2 日から同年 9 月 16 日に実施され、11 票が回収された。被験者は首都圏内の国立大学に通う 1 年生 11 名であった。調査開始時に文書と口頭で依頼し合意を得たのち、9 名の未成年者に対しては保護者からも郵便を用いて同意を得た。な

お、謝礼は提示していない。データに欠損値はなく、11票すべてが有効回答となった。

4.3 潜在ランク理論による回答者の分類

本研究では、先行研究 [4] と結果を比較検討するために、同様の分析である荘島によるソフトウェア exametrika(エグザメトリカ)[12] を利用した。分析は、(1) 回答者を分類する潜在ランク数の決定、(2)(1) で決定した潜在ランク数での exametrika の実行と分析結果の考察の順に実施され、手順 (1) では、潜在ランク数を 2 から順に大きくして exametrika をつど実行し、算出される情報量規準が最小となる潜在ランク数を採用する手法があるが、実際には分析結果の用途に合わせて分析者が決定してよいとされている [23]。

今回の質問紙調査結果に対して潜在ランク理論を適用し、回答者を分類した。具体的には、情報セキュリティ疲労度尺度に対する回答と、情報セキュリティ対策実施度尺度に対する回答のそれぞれに exametrika を実行し、2.3 節で示したように、F 群においては 3 群、Im 群においては 2 群にそれぞれ分類した。これらの実行時に設定可能な分析オプションとして、自己組織化マップ (Self-Organizing Map, SOM) を選択した以外はデフォルト値を使用した。この結果、回答者は 6 群に分類され、各群に属する回答者数は表 2 に示すようになった。また、各群の情報セキュリティ疲労度の尺度得点は表 3 に、情報セキュリティ対策実施度の尺度得点は表 4 にそれぞれ示すようになった。

5. 各群のアセスメント結果

本章では、最初に、4 章の質問紙調査結果をもとに、表 1 に示す各群それぞれに対してアセスメントを実施した結果を示す。表 5 に、各群の回答者の特徴、対策案とその評価をまとめる。次に、視覚障害者ならではの回答者の特徴が見られた 2 つの群 F-ImL と F+ImH について、既存研究では挙げられていない、2 件の新対策案 (★1) と (★2) を提案する。この 2 件の新対策案については、4.1.3 項や 4.1.4 項に示した設問に対する自由回答文に対して、特徴を抽出

表 2 情報セキュリティコンディションマトリクス上の回答者数分布
Table 2 Number of repondents on information security condition matrix.

	回答者数 (N=11)	Im 群	
		実施度低 [ImL]	実施度高 [ImH]
F 群	疲労度+ [F+]	0	4
	疲労度 0 [F0]	1	1
	疲労度- [F-]	4	1

表 3 情報セキュリティ疲労度の尺度得点と標準偏差

Table 3 Scale scores and standard deviations of information security fatigue level.

	尺度得点 (SD)	Im 群	
		実施度低 [ImL]	実施度高 [ImH]
F 群	疲労度+ [F+]	該当なし	44.50 (9.64)
	疲労度 0 [F0]	52.00 (0.00)	59.00 (0.00)
	疲労度- [F-]	48.25 (5.74)	64.00 (0.00)

表 4 情報セキュリティ対策実施度の尺度得点と標準偏差

Table 4 Scale scores and standard deviations of implementation of information security measures.

	尺度得点 (SD)	Im 群	
		実施度低 [ImL]	実施度高 [ImH]
F 群	疲労度+ [F+]	該当なし	47.25 (4.92)
	疲労度 0 [F0]	39.00 (0.00)	42.00 (0.00)
	疲労度- [F-]	27.50 (4.51)	47.00 (0.00)

するアセスメントを筆者らのディスカッションによって決定した。なお、先行研究で提案されている 14 件の施策のうち、今回あまり該当しないと思われたもの、今回該当者がいなかった群に対する施策の評価については塗りつぶしてある。

5.1 情報セキュリティ疲労度が低く、実施度が低い状態 (F-ImL 群)

この群は、情報セキュリティ実施度が低く、情報セキュリティ対策実施度も低いグループである。この群に属する回答者 (表 2) は 4 名であった。情報セキュリティ疲労度尺度得点 (表 3) は 48.25 点、標準偏差は 5.74 であり、情報セキュリティ対策実施度尺度得点 (表 4) は 27.5 点、標準偏差は 4.51 であった。

この群では、「私は視覚障害のせいでスマホやタブレットのパスワードをしなくなりました。それはパスワードの解除を大変手間に感じるからです。現代ではセキュリティ対策していないほうが悪いという風潮を聞いたことがあるのでセキュリティ対策をしなければならないと思っています。(回答者 ID4)」など、セキュリティ対策に対して多くの手間を感じている回答や、義務感を感じているものの優先順位が低い回答があった。

加えて、実施度の低さを表すような回答として、率直に対策についての理解が不十分であることを回答した者もい

表 5 情報セキュリティコンディションマトリクスの群別の自由回答アセスメント結果および
対策案と評価

Table 5 Results of assessing open-ended questions by group for information security
condition matrix, countermeasures and evaluation.

群名称 (論じる 節番号)	アセスメント結果 (各群に属する 回答者の特徴)	対策案 ・理想状態 F0ImH に移行させる ・理想状態を維持する	対策効果の評価 (5.3 節)	
			情報 セキュリティ 疲労度	情報 セキュリティ 対策実施度
F0ImL	<ul style="list-style-type: none"> 共有するファイルにパスワードを設定するときは少し面倒なので Sharepoint を使う 画面を拡大しているのでショルダーハッキングを受けやすい自覚がある 	<ul style="list-style-type: none"> (1) 情報セキュリティソリューション推奨環境の提示【推奨環境の明確化】 (2) 情報セキュリティ対策のチェックリストによるセルフチェック (3) 情報セキュリティ対策ソリューションの提供 	変化なし	上昇 (ImH へ)
			変化なし (a)	上昇 (ImH へ)
F0ImH	<ul style="list-style-type: none"> 理想状態ではあるが操作性の変化がおきてしまう不安からアップデートの躊躇が見られる 	<ul style="list-style-type: none"> (4) 情報セキュリティインシデントとその対策のケーススタディを示すなど、より高度な情報セキュリティ対策の提示 (5) 理想状態であることを知らせ、維持するモチベーションを喚起 	変化なし	変化なし
			変化なし	変化なし
F-ImL (5.1)	<ul style="list-style-type: none"> スクリーンリーダーによる操作でアクセスするサイトが多くなり、不正に引っかかりやすいと感じている。 スクリーンリーダーを用いてもどこに飛ぶのかわからずリンクをクリックすることもあるので、健常者よりも不正に引っかかりやすいと感じている。 	<ul style="list-style-type: none"> (6) 当事者意識を喚起する教育の実施 (7) マニュアル化など情報セキュリティ対策内容の具体的な提示【マニュアル化】 (★1) スクリーンリーダーを活用することで回避できるセキュリティインシデントについての理解を促進 	上昇 (F0 へ)	上昇 (ImH へ)
			上昇 (F0 へ)	上昇 (ImH へ)
			変化なし	上昇 (ImH へ)
F-ImH	<ul style="list-style-type: none"> 全て当たり前のことだと感じる 	<ul style="list-style-type: none"> (8) ソリューションに頼らない個人の能動的な対策の喚起 (9) インシデント発生後のモチベーション回復施策(教育等)の実施 	上昇 (F0 へ)	変化なし
F+ImL	該当者なし	(10) 模擬的に情報セキュリティインシデントに遭わせる演習		
F+ImH (5.2)	<ul style="list-style-type: none"> CAPTCHA による認証ができないことに不安を感じている スクリーンリーダーが広告などを読み上げることに對して不安を感じている 視覚障害者にとって情報セキュリティで有利な点はないと感じている。 未経験の不正サイトへのアクセスへの不安を感じている 	<ul style="list-style-type: none"> (11) 情報セキュリティ対策に関するヒアリング(ガス抜き) (12) 情報セキュリティ教育の間隔を延伸 (13) 情報セキュリティ教育の簡易化 (14) 組織的な教育体制の整備 (★2) スクリーンリーダーの機能の限界に関する教育の実施 	降下 (F0 へ)	変化なし
			降下 (F0 へ)	変化なし
			降下 (F0 へ)	変化なし
			降下 (F0 へ)	変化なし
			降下 (F0 へ)	変化なし

a 1 段階降下の可能性あり

た。

また、視覚障害者ならではの情報セキュリティ対策については、「私は視覚障害のせいで不正に引っ掛かりやすいと感じます。なぜなら、PCを音声で操作するのでウェブサイトの探索では様々なリンクにアクセスしているからです。(回答者 ID4)」など、スクリーンリーダーを使用していることが原因でアクセスするサイトが多くなることを挙げた回答があった。一方で、「スクリーンリーダーを使うと細かい文字まで読むので普通だと見落とす注意書きを見落とさない(回答者 ID9)」と、スクリーンリーダーなど補助的に使用しているツールのおかげでセキュリティ対策の精度が向上している様子を挙げた回答もあった。両方の側面を考慮した「音声により、表示されていないことも読み上げてくれることがあるから引っ掛かりづらいこともあると思う。どこに飛ぶのか完全には認識できていないながらリンクをクリックすることがあるので、健常者よりも引っ掛かりやすいこともあると思う(回答者 ID5)」という回答では、両側面を考慮できていることがわかるが、スクリーンリーダーの能力と限界を意識しながらも実施度が低いことを考えると、施策の必要性を感じる。

この群を理想状態に移行させるには、先行研究にある2つの対策案に加えて、スクリーンリーダーが細かい文字を読み上げることによる、不正なリンクへのアクセスを阻止できることは、健常者から見ても、非常に大切な側面をスクリーンリーダーが補助できていると言える。ここから、スクリーンリーダーを活用することで回避できるセキュリティインシデントについての理解を促す(新対策案(★1))ことが効果的であると考えられる。

5.2 情報セキュリティ疲労度が高く、実施度が高い状態 (F+ImH 群)

この群は、情報セキュリティ実施度が高く、情報セキュリティ対策実施度も高いグループである。この群に属する回答者(表2)は4名であった。情報セキュリティ疲労度尺度得点(表3)は44.50点、標準偏差は9.64であり、情報セキュリティ対策実施度尺度得点(表4)は47.25点、標準偏差は4.92であった。

この群では、ICT初心者のセキュリティ対策の負担を考える回答や、「サイトに登録するとき、ロボットであるかどうかの確認や、画像認証などが視覚障害者も使えるようになる」といい、安全だとは思いますが、読み上げてくれないから。オンラインショップで特に感じた。(回答者 ID6)」と認証に関連するスクリーンリーダーのアクセシビリティに不便を感じている回答が見られた。このような回答からも、スクリーンリーダーの限界を教育する場面の不足が伺える。

加えて、「私はロボットではありませんの画像が見分けられないため最近のサイトに登録できなかつたりログイン

できないことがあるので視覚障害者でも判別でき安全なセキュリティ対策をしてほしい。最近では大手の会社のサイトでポップアップの広告が出たりフォーカスしたところと違うリンクが開いたりすることがあるのが問題であると感じている。特に広告などの混ざっているサイト内をスマートフォンやタブレットで見ているときに起きるので厄介。(回答者 ID7)」と、セキュリティ対策の中でも視覚障害者がアクセスしにくいものに不便を感じている回答や、パスワード管理の苦勞に触れる回答もあった。

また、視覚障害者ならではの情報セキュリティ対策については、「視覚障害者はたとえ偽のサイトにアクセスしても、それに気づきにくいと思う。なぜなら、デザインが見えないため、サイトの不真正に気づきにくいからだ。逆に視覚障害者にとって有利な個所はないように思う。(回答者 ID2)」と視覚情報の不足によって正しく情報が得られないことに対して困難を感じている回答や、「視覚障害者は経験を積むことで、サイトが本物かどうかわかるけど、1回目じゃわからない。(回答者 ID6)」と不正なリンクにアクセスしてしまう経験の重要性を感じている回答も見られた。

さらに、「特にiPhoneになるがメールやメッセージの内容を開封せずに読めるため怪しいメールやメッセージを見分けられ引っ掛かりにくいと感じた。(回答者 ID7)」とiOSに搭載されているスクリーンリーダー Voiceover で安全が保たれている側面を認知している回答や、「App Store内にあるアプリで、QRコードを読み込むだけで月額1500円くらいをとられたことがある。(2ヶ月気づかなかつた)理由は、字が小さかつた上に英語で利用に関する説明を書いてあつたから。どんなに字が小さくても説明は絶対に読んだ方がいい。(回答者 ID11)」と、視覚障害が原因で起こつた実害にも触れた回答があつた。

この群を理想状態に移行させるには、先行研究で示された4つの対策の他に、スマートフォンやタブレットで用いるスクリーンリーダーの機能の限界に関する教育も必要であると感じた(新対策案(★2))。

5.3 視覚障害者ならではの対策として検討される対策案の評価

先行研究で示された対策案の他に、表5では新たに2つの新対策案を提案している。本節では、情報セキュリティ疲労度(F群)と情報セキュリティ対策実施度(Im群)のそれぞれに対して、所属する群のランクの上下にどのように効果があるかを評価する。本節における評価は(先行研究の対策案も含めて)、F群とIm群にそれぞれ独立した考察をしており、必ずしもF群とIm群に同時に対策効果が示されるとは限らない。なお、ランクの上昇と降下の評価については、改めて言及しない限り前後1段階での移動があることを示す。

F-ImL 群 (5.1 節) の対策である (★1) は、スクリーンリーダーによって防げるリスクを正しく理解することで、セキュリティ対策に対してより積極的になる教育効果があると考えられる。

F+ImH 群 (5.2 節) の対策である対策案 (★2) についても評価する。スマートフォンやタブレットにおいてスクリーンリーダーを使う視覚障害者は多いものの、その限界についての教育は Prakash らの指摘 [11] の通りまだまだ不十分である。どのような場面でスクリーンリーダーが読み上げないのか、機能の限界について適切に理解することで、より適切な使用を促すことができると考える。適切な理解に基づいた適切な使用ができれば、スクリーンリーダーが読み上げないことへの対策を前もって準備することができ、セキュリティ疲労度を軽減することが可能となるだろう。

これらの対策案を組み合わせることによって、理想状態である FOImH 群に近づける情報セキュリティ対策施策が体系的に構築できるものと考えられる。

6. 考察

視覚障害者の傾向として、セキュリティ疲労度とセキュリティ対策実施度に正の相関が表れているような現状である。すなわち、(1) セキュリティ疲労度が高いものほどセキュリティ対策実施度が高く、(2) その逆も正しいといえる結果が表れている。(1) は、晴眼者に比べて視覚障害者が情報セキュリティ対策を講じる際に、視覚情報に(部分的にしか)頼れないこと、スクリーンリーダーが読み上げないこと等に起因する情報の不足からストレスを感じているものと推察される。一方で、(2) のようにセキュリティ対策実施度が低い者は、スクリーンリーダーを活用することで防げるリスクについての理解が不足しているとも考えられる。両者ともに、適度な緊張感を持ってセキュリティ対策が実施できるようなセキュリティ教育を施す必要がある。

また、標本数が少ないこと、情報システム学科の学生に対してのみのアンケート調査であったことから、結果の偏りが起こったとも考えられる。

対象とする学科や学年を広げ、視覚障害者全般について同様の結論が出せるかどうかは課題として残った。

7. おわりに

我々は畑島らが提案したコンディションマトリクスの分布や各状態に対する施策について、視覚障害者も同様に考えることはできないのではないかという問題意識を持つ。

本稿では分布の特徴として、セキュリティ疲労度とセキュリティ対策実施度の相関について、晴眼者が一様であるのに対して、視覚障害者は正の相関があることがわかった。また、視覚障害者ならではのセキュリティインシデントに対して特有の施策を提案した。

今後は、提案した施策の有効性や、調査対象の拡大を通して視覚障害者に対してより一般的にいえる相関関係や、視覚障害者特有の問題に適応した施策を提案できるよう研究を進めたい。それにより、晴眼者のために考えられた先行研究を振り返り、より個別最適化を図った施策を提案することで、セキュリティ教育のよりよい充実につなげたい。

参考文献

- [1] 総務省:安心してインターネットを使うために国民のための情報セキュリティサイト 入手先 (https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/intro/beginner/index.html) (参照 2021-09-29).
- [2] Stanton, B., Theofanos, M., F, Prettyman, S.S. and Furman, S.:Security Fatigue, IT Prof., Vol.18, No.5, pp.26-32(2016)
- [3] Furnell, S. and Thomson, K.-L.: Recognizing and addressing 'security fatigue, Comput. Fraud Secur., vol.2009, no. 11, pp.7-11(2009)
- [4] 畑島 隆, 谷本茂明, 金井 敦, 富士 仁, 大久保一彦:改善型情報セキュリティコンディションマトリクスによる大学生の情報セキュリティ疲れ対策の提案, 情報処理学会論文誌, Vol.59, No.12, pp.2105-2119(2018).
- [5] Hatashima, T., Nagai, K., Kishi, A., Uekusa, H., Tanimoto, S., Kanai, A., Fuji, H., and Ohkubo, K.: Evaluation of the Effectiveness of Risk Assessment and Security Fatigue Visualization Model for Internal E-Crime, 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)
- [6] 畑島 隆, 永井啓太, 谷本茂明, 金井 敦:大学生の情報セキュリティ疲れの可視化に関する一考察, コンピュータセキュリティシンポジウム 2017 論文集, pp.888-895(2017).
- [7] 畑島 隆, 谷本茂明, 金井 敦:情報セキュリティ疲労度測定尺度の提案(大学生版) -バーンアウト尺度の援用による測定手法の設計と評価, 電子情報通信学会論文誌, Vol.J101-D, No.10, pp.1414-1426(2018).
- [8] 畑島 隆, 坂本泰久:情報セキュリティ不安全行動に対するテレワーク実施者の性向の分析, 情報処理学会論文誌, Vol.58, No.12, pp.1912-1925(2017).
- [9] Tanimoto, S., Nagai, K., Hata, K., Hatashima, T., Sakamoto, Y. and Kanai, A.: A Concept Proposal on Modeling of Security Fatigue Level, 5th International Conference on Applied Computing Information Technology (ACIT 2017) (2017).
- [10] Pascolini, D., Mariotti SP.: Global estimates of visual impairment. Br J Ophthalmol.;96(5):614-618. Crossref. PubMed.(2012)
- [11] Prakash, S., and Frode, E. S.:A glimpse into smartphone screen reader use among blind teenagers in rural Nepal,Disability and Rehabilitation: Assistive Technology(2020)
- [12] 荘島宏二郎, exametrika, 入手先 (<http://antlers.rd.dnc.ac.jp/shojima/exmk/index.htm>) (参照 2021-09-29).
- [13] WebAIM:Survey of Users with Low Vision # 2 Results 入手先 (https://webaim.org/projects/lowvisionsurvey2/#_mobilescreenreader) (参照 2021-10-13)
- [14] R. Koppel, J. Blythe, V. Kothari, and S. Smith.:Beliefs about Cybersecurity Rules and Passwords: A Comparison of Two Survey Samples of Cybersecurity Professionals Versus Regular Users,Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)

- [15] Zhuohao. Zhang, Zhilin. Zhang, H. Yuan, N. M. Barbosa, S. Das and Y. Wang: WebAlly: Making Visual Task-based CAPTCHAs Transferable for People with Visual Impairments, Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)
- [16] V. Fanelle, S. Karimi, A. Shah, B. Subramanian and S. Das: Blind and Human: Exploring More Usable Audio CAPTCHA Designs, Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)
- [17] Brulé, E., Tomlinson, B. J., Metatla, O., and Jouffrais, C. and Serrano, M.: Review of Quantitative Empirical Evaluations of Technology for People with Visual Impairments, CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, April 2020 pp.1-14
- [18] 板倉宏昭：バーンアウトとプロジェクトマネジメント，プロジェクトマネジメント学会誌，Vol.11, No.1, pp.17-19.
- [19] 久保真人：バーンアウト（燃え尽き症候群）ヒューマンサービス職のストレス，日本労働研究雑誌，Vol.558, No.1, pp.54-64(2007).
- [20] 浜津 翔，栗野俊一，吉開範章：集団的防護動機理論に基づく情報セキュリティ対策実行意思モデルの提案とその活用，情報処理学会論文誌，Vol.56, No.12, pp.2200-2209.
- [21] 情報処理推進機構：情報セキュリティ 10 大脅威 2016，入手先 (https://www.ipa.go.jp/security/vuln/10 threats2016.html) (参照 2021-09-29).
- [22] 総務省：テレワークセキュリティガイドライン，入手先 (https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/) (参照 2021-09-29).
- [23] 植野真臣，荘島宏二郎：学習評価の新潮流，朝倉書店 (2010)

付 録

質問 2[7]

あなたは最近 6 ヶ月ぐらいの間に，次のようなことをどの程度経験しましたか。もっともあてはまるとする番号*1に○をつけてください。

質問 3[8]

あなたは，あなた自身が以下のことを実施していると思いますか。もっともあてはまるとする番号*2に○をつけてください。

*1 1:いつもある，2:しばしばある，3:ときどきある，4:まれにある，5:ない

*2 1:まったく実施していない，2:たまに実施している，3:ときどき実施している，4:よく実施している，5:いつも実施している

表 A.1 質問 2

Table A.1 Question No.2

項番	設問
1	こまごまとした情報セキュリティ対策が面倒に感じることがある
2	指示された情報セキュリティ対策を済ませると、「ようやく終わった」と思うことがある
3	情報セキュリティ対策は必要悪だと思うことがある
4	我ながら情報セキュリティ対策を上手くやり終えたと思うことがある
5	情報セキュリティについて気にすることが多くなってしまい，気持ちにゆとりがなくなったと思うことがある
6	情報セキュリティをしっかりしている自分が誇らしいと思うことがある
7	他人や企業に対してセキュリティ対策は無駄なのに良くやっているなと思うことがある
8	情報セキュリティ対策の指示が変わるとどう対応すれば良いか困惑することがある
9	以前より情報セキュリティ対策に興味を持てなくなってきた
10	邪魔なので情報セキュリティ対策をさせないで欲しいと思うことがある
11	私は情報セキュリティ対策に自信があると思うことがある
12	情報セキュリティ対策を，もうやめたいと思うことがある
13	情報セキュリティ対策の結果はどうでも良いと思うことがある

表 A.2 質問 3

Table A.2 Question No.3

項番	設問
1	PC やスマートフォンにウイルス対策ソフトをインストールする
2	メールやメッセージの送り先が正しいか確認する
3	パスワードを適切に管理する（使い回しをしない，時々変更をする，パスワード管理ソフトを使うなど）
4	信頼できないサイトでは情報を入力しない（クレジットカード番号，メールアドレスなど）
5	OS やアプリを常に最新状態にする
6	興味があっても怪しいと思うリンクやファイルは開かない
7	最新の情報セキュリティ情報をチェックする
8	端末や記録媒体をなくしたり盗まれたりしないように対策する
9	大切なデータはバックアップする
10	見られてはいけないデータは誰でもアクセスできる場所に保存しない
11	第三者に読まれたくないデータを受け渡すときは，パスワードをかけて暗号化する