情報処理学会論文誌 Vol.61 No.9 1472–1485 (Sep. 2020)

情報セキュリティ疲労度測定尺度SFS-9の開発と信頼性・妥当性の検討

畑島 隆[1,a)] 谷本 茂明[2] 金井 敦[3]

受付日 2019年12月9日, 採録日 2020年6月1日

概要：高度情報化社会においては情報セキュリティ対策が不可避であり，要求される情報セキュリティ対策は高度化と複雑化を増すばかりである．このため求められるセキュリティ対策行動を実施することに対して疲弊してしまい，対策を怠るようになる“セキュリティ疲れ（Security Fatigue）”が問題視されている．これまでに筆者らは，大学生を分析対象として情報セキュリティ対策を行うことに対して疲弊してしまうことを測定する情報セキュリティ疲労度測定尺度を開発したが，大学生以外への適用可能性の検討がされていなかった．そこで本論文では，大学生と社会人を対象とした汎用版情報セキュリティ疲労度測定尺度（SFS-9：Security Fatigue Scale-9）を開発し，その信頼性と妥当性を検討した．社会人1,134名に対する質問紙調査結果を分析に用い，因子分析によって3因子9項目を抽出した．信頼性の検討では，高いCronbachのα係数を示した．また妥当性検討においても，情報セキュリティに対する所感の自由回答から分類された疲労度段階や自己申告による疲労度段階と，SFS-9による測定結果との対応関係の統計学的検証により基準関連妥当性を確認した．また，SFS-9は，社会人に対してだけでなく大学生593名に適用した結果でも高い適合度指標を得た．これらにより，SFS-9は大学生版を拡張した汎用的な高い信頼性と妥当性を兼備する測定尺度であると考える．さらにSFS-9を用いた分析結果から，筆者らのセキュリティ疲れに関する研究の仮説「セキュリティ規約の遵守行動によって疲弊する」が5%有意水準で支持された．

キーワード：情報セキュリティ疲れ，情報セキュリティ疲労度測定尺度，尺度開発

Development of Security Fatigue Scale (SFS-9) and Investigation of the Reliability and the Validity

Takashi Hatashima[1,a)] Shigeaki Tanimoto[2] Atsushi Kanai[3]

Received: December 9, 2019, Accepted: June 1, 2020

Abstract: Information security measures are inevitable in an advanced information society, and the required information security measures are becoming increasingly sophisticated and complex. Therefore, “Security Fatigue”, which is exhausted by information security measures and neglects rules, is regarded as a severe problem. To solve this problem, we have developed an information security fatigue measure that measures fatigue toward information security measures for university students. However, the applicability to non-university students has not been verified. In this paper, we developed a general-purpose information security fatigue scale (SFS-9: Security Fatigue Scale-9) for university students and office workers and investigated its reliability and validity. The results of a questionnaire survey of 1,134 office workers were used for analysis, and nine items for three factors were extracted by factor analysis. As a result of the reliability investigation, a high Cronbach's α was shown. Also, in the validity examination, statistically verified the correspondence between (1) the fatigue level classified from free responses to information security feelings and (2) the self-reported fatigue level, and the measurement results by SFS-9. As a result, the validity of the criteria was confirmed. Moreover, SFS-9 obtained high fitness index not only for adults but also for 593 university students. Therefore, SFS-9 is considered to be a general-purpose high reliability and validity scale that is an extension of the university student version. Furthermore, our research hypothesis on security fatigue, “People get fatigued by compliance with security regulations,” was supported at a 5% significance level from the results of the analysis using SFS-9.

Keywords: security fatigue, security fatigue scale, developing scale

1. はじめに

現代の高度に発展した情報化社会では，価値を持つ様々な情報の流通によって社会生活が形成されている．一方で個人や組織は，それぞれを対象としたサイバーアタックやヒューマンエラーによって発生するセキュリティインシデントの脅威につねに晒されている．インシデント対策は，前者に対しては増え続け複雑化するばかりである攻撃手段への対策のため高度化・複雑化し，後者に対してもウィルス対策ソフトといったセキュリティ対策ソリューションの適切な利用や安全なパスワード運用をはじめとした規約の遵守などを求められ，煩雑かつ難解になる一方である．

このような複雑化するセキュリティ対策に情報システム利用者が疲弊してしまう“セキュリティ疲れ（Security Fatigue）”によって，セキュリティ対策施策の効果が上がらなくなったり，ヒューマンエラーが誘発されたりすることが近年問題視されている [1], [2], [3].

これに対する筆者らの研究動機は，情報システム利用者のセキュリティ疲れ状態を可視化することにより，セキュリティ疲れの進行を未然に防ぐことやセキュリティ疲れから抜け出させる手段を提供することにある．

従来の筆者らの研究では，情報セキュリティ対策施策に対して情報システム利用者が疲弊することを情報セキュリティ疲れと呼び，これが進んだ状態を情報セキュリティバーンアウトと仮説設定することで，一般的な職業的バーンアウトに関する研究を援用してきた [4], [5], [6], [7], [8], [9]. これまでの研究で作成された質問紙は，職業的バーンアウトを援用していることからも分かるように社会人も対象として設計してきたが，萌芽的研究であることから背景知識や経験についての個人差が社会人と比較して小さいと思われる大学生を対象とした信頼性と妥当性の検討にとどまっていた．

この課題に対する本研究の目的は，より厳格に情報セキュリティ施策の実施を求められる社会人と従来研究の大学生に汎用的な情報セキュリティ疲労度測定尺度を開発することである．本研究で開発した情報セキュリティ疲労度測定尺度を SFS-9（Security Fatigue Scale-9）と呼ぶ．

本論文の構成を以下に述べる．2 章で関連研究を紹介し，3 章では本研究で実施した質問紙調査の概要を述べる．そして 4 章において 3 章の調査結果を用いた汎用版セキュリティ疲労度測定尺度 SFS-9 の導出手順を述べる．5 章では全体を考察し，6 章で SFS-9 の利用例を述べた後，7 章で本研究の限界を述べ，最後に 8 章で本論文を結ぶ．

[1] 日本電信電話株式会社 NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories, Nippon Telegraph and Telephone Cooperation, Musashino, Tokyo 180–8585, Japan
[2] 千葉工業大学
Chiba Institute of Technology, Narashino, Chiba 275–0016, Japan
[3] 法政大学
Hosei University, Koganei, Tokyo 184–8584, Japan
[a)] takashi.hatashima.ch@hco.ntt.co.jp

2. 関連研究

本章ではまず本研究で援用する職業的バーンアウトと職業的バーンアウトにおける疲労の関係を述べる（2.1 節）．次に情報セキュリティのバーンアウト・情報セキュリティ疲れの関係を述べる（2.2 節）．そののち，情報セキュリティに関する心理尺度開発について先行研究をあげ，本研究との差異および本研究の意義を述べる（2.3 節）．次に情報セキュリティ疲れに関する先行研究（2.4 節）と筆者らの研究（2.5 節）を比較する（2.6 節）．最後に，本研究で情報セキュリティ疲労度の可視化に用いた，潜在ランク理論について述べる（2.7 節）．

2.1 情報セキュリティ疲れと職業的バーンアウト・バーンアウト段階説

本研究では，筆者らの先行研究 [7], [8] と同様に，職業的バーンアウトにおけるバーンアウト段階説を援用し，情報セキュリティ疲れが進行することで情報セキュリティバーンアウトが発生すると仮説設定している．以下に，職業的バーンアウトおよび職業的バーンアウトと疲労の関係を説明するバーンアウト段階説について述べる．

職業的バーンアウトは燃え尽き症候群とも訳され，久保 [10] は，“この概念を初めて学術論文で取り上げた Freudenberger（1974）によると「辞書的な意味で言えば，バーンアウトという言葉は，エネルギー，力，あるいは資源を使い果たした結果，衰え，疲れはて，消耗してしまったことを意味する．（中略）実際のところ，バーンアウトは，人によりその症状も程度も異なる」”と紹介している．

一般的な職業的バーンアウトの測定尺度である MBI（Maslach Burnout Inventory）では，以下に述べるように一般的なバーンアウトにおいてバーンアウトに至る過程を段階的に説明する「バーンアウト段階説」を採用する研究が存在する．

バーンアウト段階説を採る研究例をあげると，付録 A.1 に示す Golembiewski の 8 段階モデル [10] では，3 つの下位尺度（情緒的消耗感，個人的達成感の低下，脱人格化）の高低の組合せによる 8 段階のうち．情緒的消耗感が「High」であると，ほかの 2 つの下位尺度の結果にかかわらずバーンアウトが悪化した状態（V～VIII）に分類される．そのほか，付録 A.2 に示す増田らのバーンアウトの判定基準 [11] では，Golembiewski の 8 段階モデルと同様に 3 つの下位尺度（疲弊感，職務効力感，シニシズム）の高低の組合せによる 8 段階のうち．疲弊感が「High」であると，ほかの 2 つの下位尺度の結果にかかわらずバーンアウトが悪化した状態（疲労～バーンアウト～強バーンアウト）に分類される．

このようにバーンアウト段階説では，付録 A.3 に示すように，疲労状態が進行するとバーンアウトとなるとされており，本研究ではこの関係を仮説として援用している．

2.2 情報セキュリティ疲れと情報セキュリティバーンアウト

上述のように筆者らが仮説として設定している情報セキュリティ疲れと情報セキュリティバーンアウトの関係について，関連研究を述べる．調査レポートにおいては，Cisco [12] が CISO（Chief Information Security Officer）を対象とした調査のレポートにおいて，情報セキュリティ疲れを本質的に脅威や攻撃者に対して先手を打ち防御することを諦めた状態と説明し，バーンアウトにまで進行してしまうことを削減する方策を提案しており，筆者らと同様の考え方を示している．学術研究においては 2.4.2 項に示すように情報セキュリティバーンアウトを取り扱う研究が存在するが，情報セキュリティ疲れとの関係は明らかにしていない．

2.3 情報セキュリティに関する心理尺度

2.3.1 情報セキュリティに関する心理尺度の先行研究

情報セキュリティ分野においても質問紙調査による心理尺度の開発が行われている．Parsons ら [13] は，組織におけるコンピュータセキュリティの脅威はユーザの行動に起因するとして Human Aspects of Information Security Questionnaire（HAIS-Q）を開発している．また，Egelman ら [14], [15] は，セキュリティ行動の意図に着目して Security Behavior Intentions Scale（SeBIS）を開発しており，Faklaris ら [16] は，セキュリティ対策に対する態度に注目して Self-Report Measure of End-User Security Attitudes（SA-6）を開発している．

そのほか，スマートフォンの Web ブラウジングについて Sharif ら [17] は，行動ログからユーザが悪意のあるコンテンツに晒されてしまう直前に予測できるシステムを提案し，調査票による自己申告データのみに依存するモデルは提案モデルよりも精度が低いと述べている．しかし，提案モデルでは対象が Web ブラウジングに限定されており，汎用的なインターネット利用行動の検討には及んでいない．

2.3.2 情報セキュリティ疲労度測定尺度の位置づけと本研究の意義

上述のようにセキュリティ対策行動を起こす各要因を考慮した測定尺度開発が行われているが，本研究が開発を意図する，セキュリティ対策を実施した後の行動状態に関する測定尺度とは異なる．

従来行われている行動モデル構成要因の測定においては，**図 1** に示すようにセキュリティ対策に対する経験や知識，セキュリティに対する態度や行動意図が測定されている．これらに対して本研究は，実際のセキュリティ対策行動の結果を測定するだけでなく，**図 2** に示すように従来の行動モデルにおける構成要素の入力値の 1 つとして用いることによって，セキュリティ対策行動のライフサイクルをより明確に解明する効果があると考える．以上のことから，セキュリティ対策行動の結果として現れる情報システム利用者の状態を測定しようとする筆者らの研究には意義がある．

図 1 先行研究に用いられている行動モデル
Fig. 1 Behavioral model applied by related research.

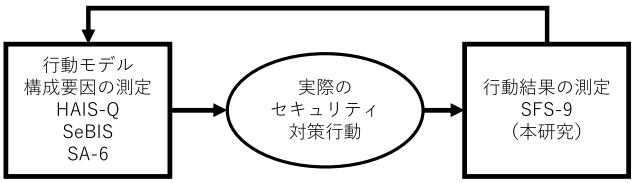

図 2 行動モデルにおける関連研究と本研究の関係
Fig. 2 Relationship between this research and related research in behavioral models.

2.4 情報セキュリティ疲れに関する先行研究

情報セキュリティ疲れに関する先行研究をあげる．これらの先行研究と 2.5 節に述べる筆者らの研究の比較を 2.6 節において行う．

2.4.1 先行研究における情報セキュリティ疲れの定義

フレーズとしての “security fatigue” は 2006 年の McLaughlin [18] や 2014 年の McGraw [19] で出現しているが，情報セキュリティ疲れについて最初に議論されたのは 2009 年の Furnell らの文献 [1] と見られる．同文献で情報セキュリティ疲れの概念を，ワークスペースにおけるオンラインセキュリティ経験に関する概念（“*a concept related to people's experiences with online security in the workplace*”）として説明していると Stanton ら [2] は述べている．

また，パスワード管理に対する情報セキュリティ疲れについて 40 名にインタビュー調査をした Stanton ら [2] は，セキュリティ疲れの論点について，意思決定の疲労が果たす役割とそれに起因する感情的な症状に焦点を当てる（“*focuses on the role that decision fatigue plays and the affective manifestations resulting from it*”）と限定している．そして，セキュリティリスクに対するホメオスタシスを議論した Kearney らは文献 [3] において，セキュリティ疲労は一般に真の脅威であり，特にユーザの認識を変えることが目的の場合のリスクホメオスタシスモデルでも重要で

ある（“*Security fatigue is a real threat in general and also specifically in the risk homeostasis model when the aim is to change perceptions of users.*”）と示している．

さらに情報セキュリティ疲れが起きる発端について，Furnell ら [1] は，ユーザがセキュリティを維持するのが難しくなりすぎたり，面倒になったりするしきい値がある（“*There is a threshold at which it simply gets too hard or burdensome for users to maintain security.*”）と示している．また，Stanton ら [2] は，情報セキュリティ疲れを起こした人は，鈍感になり，うんざりしている（“*people become “desensitized” and “get weary*”）と示している．

2.4.2 先行研究における情報セキュリティ疲れに関する質問紙

Pham ら [20] は，仕事のストレスに関する理論モデルである Job Demands-Resources model を援用して，質問紙調査により情報セキュリティコンプライアンスに対するバーンアウトの構造モデルを解明する研究を行っている．

2.5 情報セキュリティ疲れに関する筆者らの研究

筆者らは先行研究 [4], [5], [6], [7], [8], [9] で，情報セキュリティ疲労度の測定尺度の大学生版を開発し（2.5.2 項），情報セキュリティ疲れの段階ごとの特徴を明らかにした（2.5.3 項）．さらに筆者らは，段階分けされた群それぞれに対して疲労度が理想状態となるための対策案を示した（2.5.4 項）．

2.5.1 情報セキュリティ疲れに関する筆者らの研究の位置づけ

2.4 節にあげた先行研究に対して筆者らは，1 章で述べたように情報セキュリティ対策施策に対して情報システム利用者が疲弊することを情報セキュリティ疲れと呼び，これが進んだ状態を情報セキュリティバーンアウトと仮説設定することで，一般的なバーンアウトに関する研究を援用している．

2.5.2 情報セキュリティ疲労度測定尺度の開発

筆者らは先行研究で，職業的バーンアウトの測定手法を援用した質問紙を作成し，大学生に対して調査を実施した結果によって**表 1** に示す 3 つの下位因子を持つ 13 項目から構成される大学生版情報セキュリティ疲労度測定尺度 [8] を開発した．本研究では，この測定尺度の汎用版の開発と信頼性・妥当性の検討を実施する．

換言すると，筆者らはこれまでに開発した測定尺度によって，大学生の情報セキュリティ疲労度の正確な把握を実現しており，本研究は汎用的な拡張を行うものである．

2.5.3 情報セキュリティ疲れの特徴

また，筆者らは先行研究 [6] において，大学生への質問紙調査結果に対して 2.7 節で説明する潜在ランク理論を適用し，各段階別の情報セキュリティ疲れの特徴抽出を実施している（**表 2**）．具体的には，潜在ランク理論によって 5 段階に分類した回答者それぞれについて，筆者らの議論により自由回答による設問「情報セキュリティについてあなたはどう感じますか」の回答結果を分類している．

その結果，情報セキュリティ疲れは，疲れの程度が中程度であるとき情報セキュリティに対して適度な緊張感を持った理想状態であり，情報セキュリティ疲れが低い状態は当事者意識が低く他者依存傾向があり，その反対に疲れの程度が高い状態では，対策することへの意識は持っているが行動がともなっていない傾向がそれぞれあることを明らかにしている．

2.5.4 情報セキュリティ疲労度測定尺度を用いた応用研究

筆者らは文献 [4] において，セキュリティコンディションマトリクスを提案している．そして文献 [7] において，

表 1 大学生版情報セキュリティ疲労度測定尺度の構成 [8]
Table 1 Composition of Information Security Fatigue Scale for University Students [8].

下位尺度名称	説明	項目数
回避願望	責任の転嫁や無責任さを持ち，対策から離れたくても離れられない状態にある	5
消耗感	対策に対する負担感や徒労感，やらされ感を持つとともに，対策実施に重圧感を持つ	3
当事者意識	自分の行動に対する達成感を持ち，誠実な対応への意識がある	5

表 2 セキュリティ疲労度の段階別特徴 [6]
Table 2 Features according to security fatigue level [6].

セキュリティ疲労度（疲労度レベル）	特徴
5 (++)	・情報セキュリティ対策の実施責任に対する負担感がある ・重要性の認識と対策実施の意思にかい離がみられる
4 (+)	・情報セキュリティ対策への冷淡な感覚がある ・対策の効力感に疑いを持つ
3 (0)	・対策実施に対する適度な緊張感がある ・対策ソリューションに信頼感を持つ（過信の恐れがある）
2 (-)	・対策実施について当事者意識が希薄である ・対策ソリューションに信頼感を持つ（依存の恐れがある）
1 (--)	・情報セキュリティ対策の効力感に疑いを持つ

質問紙調査結果の分析によって得られるセキュリティ疲労度（3群に分類）と情報セキュリティ対策実施度（2群に分類）の6群からなるマトリクスについて各群に対するリスクアセスメントを実施し，より細分化したユーザに対するセキュリティ疲労対策の方針を示している．

2.6 先行研究と筆者らの研究の比較

2.4節で述べた先行研究と2.5節で述べた筆者らの研究を比較する．筆者らの研究ではFurnellら[1]と同様にオンラインセキュリティに着目しているが，筆者らはワークスペースで働く人だけでなく，大学生も対象としている点で異なる．

Stantonら[2]による情報セキュリティ疲れを起こした人の状態については，筆者らの先行研究[6]において検証したように，筆者らの開発した測定尺度を用いて同様の結果を得ている．具体的には，筆者らは先行研究[6]で測定尺度得点が低い場合は当事者意識が低く，高い場合はセキュリティ対策を実施する意思はあるが行動がついてこない状態となることを明らかにしている．また，同じくStantonら[2]が示す「鈍感」や「うんざり」という感情についても，筆者らの先行研究[7]でも同様の傾向が現れている．

Kearneyら[3]はリスクホメオスタシスにおいてセキュリティ疲労が脅威であることを前提としているが，本研究の測定尺度によって実現されるセキュリティ疲労の定量化には触れていない．

Phamら[20]が作成した質問紙は，測定尺度としての利用を意図していないとみられ，本研究では4.3.2項で示す基準関連妥当性の検討および6.1節で示すバックグラウンドファクタによる疲労傾向の差異のような，測定尺度としての特性について議論がされていない．

2.7 セキュリティ疲労度の可視化に用いた関連研究（潜在ランク理論）

本研究では，情報セキュリティ疲れの程度を数段階に分類し可視化する手段として，先行研究[6]と同様にShojima[21]による潜在ランク理論を利用する．

潜在ランク理論は，学力テストによる通信簿の結果や心理尺度測定による判定結果のような分野で，その素点の得点差による評価ではなく，数段階のレベル分けして判定して質的評価できることが期待されている．潜在ランク理論を用いた研究例として，教育分野で学力テスト結果の潜在ランク理論による分析結果とCAN-DOリスト[22]と呼ばれる学習到達目標に対する達成度の定性的な段階評価を組み合わせて利用することによって，学習指導効果を高める研究[23]がある．そのほか，心理臨床に用いられる精神的健康調査票の評価において，過去の知見を基に設定したカットオフポイントを用いたスクリーニングによらず，柔軟な臨床介入判断を行うために導入する研究[24]がある．

3. 測定尺度開発行程と質問紙調査

3.1 測定尺度開発工程

測定尺度の作成は以下に述べるように先行研究[8]と同様に実施する．尺度開発においては，まず構成概念について検討を行い，そののち質問項目候補の収集および内容妥当性の検討を行って，予備調査の質問紙を作成する．そして予備調査結果の分析によって，本番となる測定尺度確定調査の調査紙を確定する．なお本論文では，筆者らの先行研究[8]の測定尺度が本番調査の質問紙にあたる（3.2.2項）．

得られた本番調査結果に対して因子分析の実施によって下位尺度を確定する（4.1.1項）ほか，下位尺度の命名や構成する概念の決定を行う（4.1.2項）．そののち信頼性の検討（4.2節）および妥当性の検討（4.3節）を実施し，本研究の汎用版セキュリティ疲労度測定尺度を確定する．

3.2 質問紙調査

3.2.1 調査の概要

インターネット調査会社を用いたオンライン質問紙調査を実施した．調査期間は2018年9月14日から同年9月16日であった．実験協力者数は1,861名（社会人1,243名，大学生618名）であった．回答の品質管理については欠損値のあるデータの除外などは調査会社の施策によったが，不誠実な回答者の除外は4.1節で示すように独自にも実施した．調査倫理については，インターネット調査会社に意見を求めた結果に従った．具体的には通常の作業工程として行われる質問紙のチェックのほか，付録A.2.1に示す質問紙の設問4を不誠実な回答者の除外目的に用いることに問題がないことを確認した．また，データの使用用途については，付録A.2.1に示す質問紙の冒頭のように一般の意識調査であること，統計的に処理されることをあわせて伝えた．報酬は同調査会社の基準で同社から支払われた．

調査対象は，社会人については，中小企業以上の規模の企業に勤める従業員を対象とした．この理由は，情報セキュリティ対策に企業として取り組んでいることが想定できると考えたためである．具体的には，中小企業基本法による小規模企業人数以上の従業員を対象とした．業種ごとのサンプル割付けは，産業力調査および労働力調査による構成比に近づけるように収集した．また大学生については，全国の大学生を対象とし，先行研究で実施した関東の2大学の学生を対象とした調査よりも一般的なサンプルでの検証を実施する目的で収集した．

3.2.2 質問紙の構成

本研究に用いる質問紙は付録A.2.1に示す設問で構成した．

(1) 情報セキュリティ疲労度測定尺度[8]
(2) 情報セキュリティに対する所感（自由回答）[6]
(3) 情報セキュリティ疲労度の自己申告（5件法）

(4) ICT 利用に関する質問（利用歴，1 日の利用時間）
(5) 情報セキュリティ施策に対する立場

質問紙の本研究での利用方針は以下のとおりであった．(1) への回答結果に対して 4.1 節で述べる分析を行い，汎用版セキュリティ疲労度測定尺度の開発し，(2) および (3) を用いて基準関連妥当性の検証した（4.3.2 項）．また (4) は，PC とスマートフォンの利用歴を年単位，1 日の利用時間を時間単位で自己申告させたものであり，4.1.1 項において不誠実な回答者の除外に用いた．そして (5) は，6.1 節においてセキュリティ疲労度の平均の差の検定を実施する区分の設定に用いた．なお，同じく 6.1 節で用いた性別，年齢層，社会人の職種，年収レベルといった区分の設定には，調査会社からパネルの基本情報として提供されたデータを利用した．

4. 汎用版セキュリティ疲労度測定尺度の開発

本章では 3.1 節に述べた工程に従って実施した汎用版セキュリティ疲労度測定尺度の開発内容を述べる．

4.1 セキュリティ疲労度測定尺度の因子構造

社会人に拡張した汎用的な情報セキュリティ疲労度測定尺度を検討するために，一般的な尺度作成の手順に従ってまず因子分析を行った．本研究の統計的処理には R version 3.6.1 を用いた．

因子分析は大学生版尺度[*1]の設計時 [8] と同様の手法を用いた．具体的には，因子数決定には平行分析を用い，探索的因子分析においては回転に promax 回転，推定方法に最少残差法を用い，因子負荷量が 0.30 以下である設問項目と，複数の因子で因子負荷量が 0.30 以上である設問項目を除外する方針で行った．その結果，本研究の探索的因子分析は 2 回目の分析で収束し，13 項目の設問項目から**表 4** に示す因子パターンを持つ 9 項目が得られた．

4.1.1 因子分析

まず因子分析の前処理として，3.2 節による調査結果から不誠実な回答を除外した．除外ルールは a）質問 (1) のすべての項目の回答が同一であるものを除外，b）質問 (4) において利用歴が PC やスマートフォンの普及前からと思われるほど長いものと 1 日の利用時間が 24 時間を超えるものを除外とした．

この除外処理の結果，社会人のサンプル数は 1,134 件となり，有効回答率は 91.2%であった．有効サンプルの全体および男女の構成は**表 3**，年齢分布は付録 A.3.1 のようになり，社会人全体（n = 1,134）は平均年齢 42.64 歳（標準偏差 11.11），最年少 19 歳，最年長 78 歳であった．なお，

[*1] 先行研究 [8] における適合度は CFI（Comparative Fit Index）0.902，SRMR（Standardized Root Mean square Residual）0.063，RMSEA（Root Mean Square Error of Approximation）0.094 であった．

表 3 有効サンプルの構成（社会人）
Table 3 Composition of effective samples (office workers).

社会人全体 n=1,134		男性 n=686		女性 n=448	
平均年齢	SD	平均年齢	SD	平均年齢	SD
42.64	11.11	46.26	10.50	37.12	9.66

男性（n = 686）は平均年齢 46.26 歳（標準偏差 10.50），最年少 20 歳，最年長 78 歳であり，女性（n = 448）は平均年齢 37.12 歳（標準偏差 9.66），最年少 19 歳，最年長 68 歳であった．

上述の前処理を実施後，4.1 節に述べた方針で探索的因子分析を実施した．

この過程で大学生版セキュリティ疲労度測定尺度から「情報セキュリティ対策は必要悪である（除外項目 1：付録 A.2.1 設問 1–3）」，「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（除外項目 2：付録 A.2.1 設問 1–5）」，「他人や企業に対して情報セキュリティ対策は無駄なのに良くやっているなあと思うことがある（除外項目 3：付録 A.2.1 設問 1–7）」，そして「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（除外項目 4：付録 A.2.1 設問 1–8）」の 4 項目を除外した．

4.1.2 因子の命名

前述のように因子分析の結果は表 4 に示すようになったため，それぞれの下位尺度を以下のように命名した（**表 5**）．

第 1 因子は大学生版における回避願望因子から除外項目 3 を除外したものである．議論の結果，意欲低下因子と命名し，“情報セキュリティ対策に対して無責任になり関心が薄れているが，対策から離れたくても離れられない状態”と説明した．この因子には Stanton ら [2] が示した，「情報セキュリティ疲れを起こした人は，鈍感になっている」が含まれている．

第 2 因子は大学生版における当事者意識因子から除外項目 1 および除外項目 2 を除外したものである．これについて自己効力感因子と命名した．自己効力感は社会心理学において一般的に用いられる用語であり，文献 [25] の説明を用いて “「自分は情報セキュリティ対策をうまく成し遂げることが出来る」いう自己に対する確信がある状態” と説明した．

第 3 因子は大学生版の消耗感因子から除外項目 4 を除外したものであるが，因子名は消耗感因子のままとした．しかし説明は一般的なバーンアウトにおける説明 [10] を援用し，“情報セキュリティ対策を通して力を出し尽くし消耗してしまった状態” と変更した．この因子には Stanton ら [2] が示した，「情報セキュリティ疲れを起こした人はうんざりしている」が含まれている．

表 4 情報セキュリティ疲労度測定尺度 SFS-9
Table 4 Security fatigue scale SFS-9.

項目		I	II	III	共通性
Ⅰ. 情報セキュリティ対策に対する意欲低下					
10 邪魔なので情報セキュリティ対策をさせないでほしいと思うことがある		**0.824**	-0.014	0.012	0.684
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		**0.792**	0.059	-0.095	0.582
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		**0.765**	-0.045	0.106	0.661
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		**0.650**	-0.002	0.019	0.435
Ⅱ. 情報セキュリティ対策に対する自己効力感					
6 情報セキュリティ対策をしっかりしている自分が誇らしいと思うことがある		-0.065	**0.812**	0.030	0.655
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		-0.034	**0.736**	0.091	0.572
11 私はセキュリティ対策に自信があると思うことがある		0.099	**0.710**	-0.093	0.508
Ⅲ. 情報セキュリティ対策に対する消耗感					
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		-0.074	0.058	**0.946**	0.861
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		0.107	-0.036	**0.711**	0.578
	因子寄与	2.353	1.724	1.460	
	因子寄与率	0.261	0.192	0.162	
	累積寄与率	0.261	0.453	0.615	
	因子	1			
	負荷	0.188	1		
	行列	0.486	0.244	1	

4.2 信頼性の検討

4.1 節で求めた 3 つの下位因子について Cronbach の α 係数を算出し，尺度項目間の類似度である内的整合性を分析した結果，高い内的整合性を示した（意欲低下，$\alpha = 0.85$（95%信頼区間 0.83〜0.86）；自己効力感，$\alpha = 0.79$（95%信頼区間 0.77〜0.82）；消耗感，$\alpha = 0.81$（95%信頼区間 0.79〜0.83））．

また，情報セキュリティ疲労度測定尺度全体の Cronbach の α 係数も高い整合性を示した（$\alpha = 0.84$（95%信頼区間 0.82〜0.85））．

4.3 妥当性の検討

検討すべき妥当性の種類には内容的妥当性，基準関連妥当性と構成概念妥当性がある [26]．

4.3.1 内容的妥当性

内容妥当性は設問設計時に確認すべきものであり，本論文は先行研究の成果である大学生版の質問紙 [8] に対する汎用化の検討であるため，先行研究で実施済みとした．

4.3.2 基準関連妥当性

本研究における基準関連妥当性の検証は，以下に述べる［データ D：部分集合の測定ランク］と［データ B：自由回答］，および［データ A：測定ランク］と［データ C：自己申告］のそれぞれの連関を調べることによって行った．連関とは，量的変数に対して相関と呼ばれるものの，質的変数に対する呼称である [27]．

以下に本項で用いるデータを整理する．3.2.2 項の (1) の質問紙を構成する 13 項目に対する回答のうち．4.1.1 項で実施した因子分析の結果残った 9 項目に対する回答を［データ X：回答結果］と呼ぶ（n = 1,134）．［データ X］に対して 2.7 節で述べた潜在ランク理論を適用し，5 ランクに段階分けした結果を［データ A：測定ランク］と呼ぶ（n = 1,134）．そして，3.2.2 項の (2) の回答にした全実験参加者を，表 2 の 5 段階の分類に従って筆者らの議論により振り分けた結果を［データ B：自由回答］と呼ぶ（n = 348）．［データ B：自由回答］が 348 件に減少した理由は，無回答や「面倒」のように全区分で現れる回答であったデータを除外したためである．3.2.2 項の (3) に対する回答結果は，セキュリティ対策に対してどれだけ疲れているかを 5 段階のリッカート尺度で自己申告させた結果であり，これを［データ C：自己申告］と呼ぶ（n = 1,134）．さらに，［データ X：回答結果］のうち，［データ B：自由回答］として採用した実験参加者（n = 348）の回答結果に対して潜在ランク理論を適用し，5 ランクに段階分けしたデータを［データ D：部分集合の測定ランク］と呼ぶ（n = 348）．

表 5 汎用版情報セキュリティ疲労度測定尺度（SFS-9）の構成
Table 5 Composition of information security fatigue scale (SFS-9).

下位尺度名称	説明	項目数
意欲低下	情報セキュリティ対策に対して無責任になり関心が薄れているが，対策から離れたくても離れられない状態	4
自己効力感	「自分は情報セキュリティ対策をうまく成し遂げることが出来る」という自己に対する確信がある状態	3
消耗感	情報セキュリティ対策を通して力を出し尽くし消耗してしまった状態	2

4.3.2.1 自由回答からのセキュリティ疲労度の分類とセキュリティ疲労度測定結果との連関

本目における分析によって，「本研究で検討を進めてい

る 9 項目からなる質問紙に回答した社会人を潜在ランク理論で 5 段階に分類した結果」である［データ D：部分集合の測定ランク］（n = 348）と，「社会人の情報セキュリティに対する自由回答を，大学生を対象にしたセキュリティ疲労度の目安（表 2）によって 5 段階に分類した結果」である［データ B：自由回答］（n = 348）がおおむね連関していることが分かった．以下に分析の詳細を述べる．

表 6 の横軸［データ D：部分集合の測定ランク］（n = 348）を参照すると，ランク 4 が最も多く（124 名），ランク 2 が最も少なかった（24 名）．また，縦軸［データ B：自由回答］（n = 348）を参照すると，ランク 3 が最も多く（137 名），ランク 1 が最も少なかった（28 名）．

表 6 に対してカイ 2 乗検定を行った結果であるクラメルの連関係数[*2]（Cramer's association coefficient）$V = 0.26$（95%信頼区間 0.24～0.33）であり，水本らがまとめた効果量の目安 [28] では効果量は小（0.10～0.30）であり，有意だった（$\chi^2(16) = 96.97$，$p < 0.001$）．なお水本ら [28] は，効果量の目安はあくまで目安であるので研究分野によって変わると注記している．

また，表 6 に対してスピアマンの順位相関係数（Spearman's rank correlation coefficient）を算出した結果，正の相関（$0.4 < |\rho| \leq 0.7$）が認められた（$\rho = 0.44$，95%信頼区間 0.36～0.52，$p < 0.001$）．

4.3.2.2 セキュリティ疲労度の自己申告結果とのセキュリティ疲労度測定結果の連関

4.3.2.1 目と同じ方法を用いて，「本研究で検討を進めている 9 項目からなる質問紙に回答した社会人を潜在ランク理論で 5 段階に分類した結果」である［データ A：測定ランク］（n = 1,134）と，「セキュリティ対策に対してどれだけ疲れているかを 5 件法で自己申告させた結果」である［データ C：自己申告］（n = 1,134）がおおむね連関していることが分かった．以下に分析の詳細を述べる．

表 7 に横軸にとった［データ A：測定ランク］（n = 1,134）と，縦軸にとった［データ C：自己申告］（n = 1,134）との対応表を示す．

横軸の［データ A：測定ランク］では疲労度 5（389 名）が最多であり疲労度 4（112 名）が最少であった．縦軸の［データ C：自己申告］では，疲労度 3（418 名）が最多であり疲労度 5 が最少（76 名）であった．

4.3.2.1 目と同様に表 7 のクラメルの連関係数 V を計算したところ，$V = 0.25$（95%信頼区間 0.22～0.28）であったため，効果量は「小」であり，有意だった（$\chi^2(16) = 272.75$，$p < 0.001$）ことから，4.3.2.1 目に示した自由回答から分析された効果量と同等の効果量が得られた．

[*2] クラメルの V について豊田 [31] は，V は 0 から 1 までの値をとり，値が小さいほど独立（非連関）の程度が高くなり，値が大きいほど連関（独立）の程度が高いと解釈すると説明している．また，カイ 2 乗値と異なりサンプルサイズによる影響を受けないという特徴を持つ．

表 6 セキュリティ疲労度測定尺度によるランク分類結果［データ D：部分集合の測定ランク］（横軸）と自由回答による疲労度の分類結果［データ B：自由回答］（縦軸）（n = 348）

Table 6 Table 6 Rank classification result by security fatigue scale (horizontal axis) and fatigue classification results based on free answers (vertical axis) ($n = 348$).

データB：自由回答＼データD：部分集合の測定ランク	1	2	3	4	5
1	7	8	6	7	
2	9	11	23	42	12
3	8	3	25	41	60
4	3	1	3	22	24
5		1		12	20

表 7 セキュリティ疲労度測定尺度によるランク分類結果［データ A：測定ランク］（横軸）とリッカート尺度によるセキュリティ疲労度の自己申告結果［データ C：自己申告］（縦軸）（n = 1,134）

Table 7 Rank classification result by security fatigue scale (horizontal axis) and Self-report results of security fatigue using the Likert scale (vertical axis) (n = 1,134).

データC：自己申告＼データA：測定ランク	1	2	3	4	5
1	29	32	7	2	9
2	64	135	60	27	45
3	33	111	77	49	148
4	7	26	34	26	137
5	1	15	2	8	50

また，表 7 に対してスピアマンの順位相関係数を算出した結果，正の相関が認められた（$\rho = 0.46$，95%信頼区間 0.41～0.51，$p < 0.001$）．

4.3.3 構成概念妥当性

構成概念妥当性の検討のため，得られた因子構造（表 4）に対して確証的因子分析を実施した．計算には R の lavaan パッケージを用いた．その結果得られた適合度は CFI = 0.970，SRMR = 0.033，RMSEA = 0.067（90%信頼区間 0.057～0.078）であった．この結果，CFI が 0.95 以上，SRMR が 0.05 以下，RMSEA が 0.05 以上 0.10 未満であることから，あてはまりの良いモデルであることが示された．

以上の検討により，情報セキュリティ疲労度測定尺度（表 4）を確定した．

表 8 有効サンプルの構成（大学生）
Table 8 Composition of effective samples (university students).

大学生全体 n=593		男性 n=156		女性 n=437	
平均年齢	SD	平均年齢	SD	平均年齢	SD
20.77	2.92	21.07	2.99	20.67	2.89

4.4 大学生への適用と汎用版情報セキュリティ疲労度測定尺度の命名

3.2.1 項で述べた調査で同時に取得した大学生サンプルを利用して，得られた因子構造（表 4）で確証的因子分析を実施した．その際大学生についても社会人と同様に，4.1.1 項に示した除外ルールを用いて不誠実な回答者を除外した．その結果，大学生のサンプル数は 593 件となり，有効回答率は 96.0%であった．サンプルの構造は**表 8**，年齢分布は付録 B.2 のようになり，大学生全体（n = 593）は平均年齢 20.77 歳（標準偏差 2.92），最年少は 18 歳，最年長は 56 歳であった．また，男性（n = 156）は平均年齢 21.07 歳（標準偏差 2.99），最年少は 18 歳，最年長は 39 歳であり，女性（n = 437）は平均年齢 20.67 歳（標準偏差 2.89），最年少は 18 歳，最年長は 56 歳であった．平均年齢が高い理由は，未成年者の調査会社への登録が少ないと思われることと，社会人学生が含まれているためであると考える．

確証的因子分析の結果は，大学生サンプルに対しても先行研究 [8]（4.1.1 項脚注）を上回り，本研究の社会人サンプルに対するものと同等の適合度指標を持つ，あてはあまりの良いモデルであることが示された（CFI = 0.959，SRMR = 0.043，RMSEA = 0.066（90%信頼区間 0.051〜0.081））．

この結果から，表 4 で示した測定尺度は大学生と社会人に適用可能である汎用的なものであるとして，情報セキュリティ疲労度測定尺度 SFS-9（Security Fatigue Scale-9）と命名した．

5. 考察

5.1 因子構造

4.1 節で述べたように，SFS-9 では大学生版の 13 項目の設問から 4 項目を除外した．除外理由は，除外項目 1（付録 A.2.1 設問 1–3）については 2 回目の因子分析においていずれの下位因子でも因子負荷量が 0.30 に満たず，除外項目 2（付録 A.2.1 設問 1–5）と除外項目 3（付録 A.2.1 設問 1–7）および除外項目 4（付録 A.2.1 設問 1–8）については 1 回目の因子分析において 2 つの下位因子で因子負荷量が 0.30 を超えたためであった．なお，SFS-9 の 3 つの下位因子の累積寄与率は 61.5%であった．

なお，「情報リテラシー能力の高低によりセキュリティ疲れの度合いが左右されるか」については，先行研究において質問項目から除外しているため，陽に現れなかった．具体的には，先行研究 [8] の予備調査項目に「ソフトウェアの最新化やパスワードの定期的な変更のような情報セキュリティ対策を実施する気が起きないことがある（仮説因子名：消耗感）」や，「情報セキュリティ対策は意味がないと思うことがある（仮説因子名：冷笑感）」，「自分が情報セキュリティ対策を実施することで情報セキュリティ事故が防がれていると思うことがある（仮説因子名：効力感）」の設問をしていたが，いずれも因子分析の結果除外している．

5.2 信頼性の検討

信頼性検討のために Cronbach の α を求めた結果，4.2 節にあげたすべての分析対象について α 係数が 0.70 を上回り，内的整合性は確認された．

5.3 妥当性の検討

5.3.1 基準関連妥当性

基準関連妥当性について村上 [29] は，“測定値と問題にしている特性や行動の直接の測度となる複数の外部変数との間の相関係数や回帰係数で評価される” と説明する一方，“日本では基準関連妥当性が確認されたテストはあまりない” と指摘しており，本研究での実施は，より精緻な質問紙の開発において意義がある．関連研究として 2.1 節にあげた情報セキュリティ心理尺度は図 2 に示したように観測のフェーズが異なっているため，本研究では外部変数として情報セキュリティ全体に対する自由回答（3.2.2 項 (2)）と情報セキュリティ疲労に関する自己申告（3.2.2 項 (3)）を用いた．これらを用いた 4.3.2.1 目および 4.3.2.2 目での検討により，基準関連妥当性を確認した．

なお，4.3.2.1 目であげたように，水本ら [28] は効果量の目安はあくまで目安であるので研究分野によって変わると注記している．情報セキュリティに関する質問紙調査における効果量の目安は確立していないため，クラメルの連関係数 V による評価は確定的なものではない．

5.3.2 構成概念妥当性

構成概念妥当性は確証的因子分析により検討した．適合度指標の比較によって，大学生による回答結果を用いた構造モデルの先行研究 [8]（4.1.1 項脚注）と本研究（4.4 節）では本研究のモデルのほうが，よりあてはまりが良いことを示した．この理由として，前記先行研究 [8] では特定の 2 大学の学生に実験参加を依頼していたが，本研究では全国の大学生や一般社会人が対象となっているため，より一般的なサンプルが得られ，より適切な因子構造の分析ができたためと考える．これにより，SFS-9 は大学生版セキュリティ疲労度測定尺度からの改善がなされていると考える．

5.4 大学生への適用

4.3.1 項，4.4 節および 5.3.2 項における検討により，SFS-9 は大学生に対しても適用可能であると考える．なお，大学生版測定尺度を拡張するために大学生版の質問紙を用い

て再調査を行い，信頼性と妥当性を検討する手法は，村山ら [30] を参照した．

6. SFS-9 の利用例

6.1 バックグラウンドファクタによる差異

6.1.1 平均の差の検定結果

表 9 に示す 6 種類の分類方法それぞれについて，測定された疲労度の平均の差を検定することによって，SFS-9 の特性を調べた．まず F 検定によって 2 群間に等分散性を調べ，等分散性が仮定できた場合はスチューデントの t 検定を，仮定できなかった場合はウェルチの t 検定を行った．

実験参加者全体の男女の比較においては，(1) 男性（平均 3.19，SD 1.51）より女性（平均 3.44，SD 1.40）のセキュリティ疲労度が 0.1%水準で有意に高く，効果量の目安は「ほとんどなし」だった．また，(2) 大学生と社会人の比較においては，大学生（平均 3.42，SD 1.44）は社会人（平均 3.27，SD 1.47）よりセキュリティ疲労度が 5%水準で有意に高く，効果量の目安は「ほとんどなし」だった．

社会人の比較を対象とした比較においては，(3) 技術系社会人（平均 3.33，SD 1.51）と非技術系社会人（平均 3.25，SD 1.46），および，(4) 個人収入 400 万円未満（平均 3.26，SD 1.49）と 400 万円以上（平均 3.22，SD 1.49）の実験参加者[*3]，さらに (5) 情報システムの利用者（平均 3.26，SD 1.47）と情報システムの管理・運用者（平均 3.17，SD 1.45）のそれぞれについて，セキュリティ疲労度に有意な差は見られず，効果量の目安はいずれも「ほとんどなし」だった．

その反面，(6) 情報システム利用者のうち，組織が決めた規約がある（平均 3.30，SD 1.48）利用者は組織が決めた規約がない（平均 3.04，SD 1.40）利用者より 5%水準でセキュリティ疲労度が高く，効果量の目安は「ほとんどなし」だった．

6.1.2 考察

(1) の結果から男女間では女性のほうが，(2) の結果から大学生と社会人では大学生のほうが，セキュリティ疲労度が高かった．この理由として (1) については，文献 [8] の大学生版測定尺度の下位尺度を統計的検定した結果，女性は男性と比較して下位尺度「消耗感」が大きく表れ，より情報セキュリティ疲れを起こしうる傾向が認められていたものと同様の結果が得られたものと考える．また (2) については，社会人は職務として情報セキュリティ対策を行うが，大学生は情報セキュリティ対策に職責が発生せず，対策をやらされている感覚が強く出ているものと考える．

(3)，(4)，および (5) の結果から，社会人の業務分野が技術系か否か，および年収レベル，そして情報システムの利用者か管理者かはセキュリティ疲労度に関係しないことが分かった．

[*3] 無回答の実験参加者は除外し，人数がほぼ等分となる年収区分で分割した．

表 9 SFS-9 により測定された疲労度の平均の差の検定
Table 9 T-test for security fatigue measured by SFS-9.

		SFS-9 平均（SD）		t(df), pと効果量 r
(1)	（全体）男性と女性	男性 n = 842	女性 n = 885	t(1700.5) = -3.540
		3.19	3.44	p < 0.001
		(1.51)	(1.40)	r = 0.08
(2)	大学生と社会人	大学生 n = 593	社会人 n = 1134	t(1725) = -2.021
		3.42	3.27	p<0.05
		(1.44)	(1.47)	r = 0.05
(3)	（社会人）技術系と非技術系	技術系 n = 263	非技術系 n = 871	t(1132) = 0.754
		3.33	3.25	p =0.451
		(1.51)	(1.46)	r = 0.02
(4)	（社会人）個人収入	400万円未満 n = 394	400万円以上 n = 513	t(905) = 0.407
		3.26	3.22	p =0.684
		(1.49)	(1.49)	r = 0.02
(5)	（社会人）利用者と管理・運用者	利用者 n = 1003	管理・運用者 n = 102	t(1103) = 0.612
		3.26	3.17	p = 0.541
		(1.47)	(1.45)	r = 0.01
(6)	（社会人・利用者）組織が決めた規約の有無	規約あり n = 844	規約なし n = 159	t(1001) = 2.080
		3.30	3.04	p < 0.05
		(1.48)	(1.40)	r = 0.06

また (6) の結果から，規約を遵守するセキュリティ対策行動を大学生よりも厳密に求められる社会人においては，セキュリティに対する規約がある群のほうが，規約がない群よりもセキュリティ疲れを起こしていることが分かった．

この結果から，本研究の前提としての仮説である「セキュリティ規約の遵守行動によって疲弊する」が支持されたが，効果量を参照すると平均値の変化は標準偏差の 0.06 倍であった．

効果量がおしなべてほとんどなしであったのは，セキュリティ対策に関する規約の有無を問わず，セキュリティ対策行動を実施することが実際には求められるためにセキュリティ対策疲れを起こすことから，平均の差が統計的に優位であってもその差は小さいものとなったと考える．

7. 本研究の限界

本研究の限界を以下に述べる．本研究では社会人および大学生以外の，一般のインターネット利用者を調査対象としていない．これは，一般のインターネット利用者はセキュリティ対策を学校教育や企業施策の一環として実施する経験に乏しいと考えたためである．

しかし，一般のインターネット利用者も報道や企業広告，政府等公的機関からの告知などによって情報セキュリティ被害やその対策の情報には触れていることから，情報セキュリティ対策の必要性は認知し，何らかの情報セキュリティ対策を実施していると思われるため，SFS-9 の適用可能性はあると考える．

8. おわりに

本研究で汎用的な情報セキュリティ疲労度測定尺度 SFS-9 を開発し，信頼性と妥当性を検討した．先行研究の大学生版尺度は 3 因子 13 項目で構成されていたが，本研究によって 4 項目削減し，3 因子 9 項目の構成に簡便化した．

また，筆者らの情報セキュリティ疲れに関する研究の前提である，「情報セキュリティ対策を実施することにより疲弊する」が 5%の有意水準で支持された．

筆者らが開発した SFS-9 を用いて情報セキュリティ対策施策に対して疲労する利用者を検知し，それぞれに対して適切な処置を行うことによって，情報セキュリティ対策施策の費用対効果を高めることが期待できるものと考える．

今後の展望として，図 2 に示したように既存尺度と連携することによって情報セキュリティ対策行動のライフサイクルをより明確に解明する研究がある．また，Sharif ら [17] のように機械学習により情報セキュリティ行動を検知するモデルを構築する際には，データを分類するための基準が必要であるが，情報セキュリティ疲れについては SFS-9 がその一助になると考える．

参考文献

[1] Furnell, S. and Thomson, K.-L.: Recognising and addressing 'security fatigue,' *Comput. Fraud Secur.*, Vol.2009, No.11, pp.7–11 (2009).

[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] Kearney, W.D. and Kruger, H.A.: Theorising on risk homeostasis in the context of information security behaviour, *Inf. Comput. Secur.*, Vol.24, No.5, pp.496–513 (2016).

[4] 畑島 隆，谷本茂明，金井 敦：情報セキュリティ疲れ：情報セキュリティコンディションマトリクスの提案，情報処理学会研究報告セキュリティ心理学とトラスト（SPT），Vol.2017-SPT-24, No.30, pp.1–7 (2017).

[5] 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).

[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，冨士 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).

[8] 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).

[9] 畑島 隆，谷本茂明，金井 敦，大久保一彦：情報セキュリティ疲れのコーピングに関する一検討，情報処理学会研究報告セキュリティ心理学とトラスト（SPT），Vol.2018-SPT-31, No.15, pp.1–7 (2017).

[10] 久保真人：バーンアウトの心理学，サイエンス社 (2004).

[11] 増田真也，北岡和代，萩野佳代子：MBI-GS によるバーンアウトの判定基準：疲労感+1 基準とニューラルテスト理論による検討，経営行動科学年次大会：発表論文集，No.14, pp.471–476 (2011).

[12] Cisco: Cisco 2019 Asia Pacific CISO Benchmark Study, available from ⟨https://www.cisco.com/c/m/en_sg/products/security/offers/benchmark-reports-2019.html⟩ (accessed 2020-03-19).

[13] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C.: Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), *Comput. Secur.*, Vol.42, pp.165–176 (2014).

[14] Egelman, S. and Peer, E.: Scaling the Security Wall?: Developing a Security Behavior Intentions Scale (SeBIS), *Proc. 33rd Annual ACM Conference on Human Factors in Computing Systems* (*CHI '15*), pp.2873–2882 (2015).

[15] Egelman, S., Harbach, M. and Peer, E.: Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS), *Proc. 2016 CHI Conference on Human Factors in Computing Systems* (*CHI '16*), pp.5257–5261 (2016).

[16] Faklaris, C., Dabbish, L.A. and Hong, J.I.: A Self-Report Measure of End-User Security Attitudes (SA-6), *15th Symposium on Usable Privacy and Security* (*SOUPS 2019*) (2019).

[17] Sharif, M., Urakawa, J., Christin, N., Kubota, A. and Yamada, A.: Predicting Impending Exposure to Malicious Content from User Behavior, *Proc. 2018 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '18*), pp.1487–1501 (2018).

[18] McLaughlin, L.: What Microsoft's identity metasystem means to developers, *IEEE Softw.*, Vol.23, No.1, pp.108–111 (2006).

[19] McGraw, G.: Security Fatigue? Shift Your Paradigm, *Computer.*, Vol.47, No.3, pp.81–83 (2014).

[20] Pham, H.C., Brennan, L. and Furnell, S.: Information security burnout: Identification of sources and mitigating factors from security demands and resources, *J. Inf. Secur. Appl.*, Vol.46, pp.96–107 (2019).

[21] Shojima, K.: Neural test theory: A latent rank theory for analyzing test data, *DNC Res. Note*, Vol.08-01 (2008).

[22] 文部科学省：高等学校の外国語教育における「Can-Do リスト」の形での学習到達目標設定のための手引き，入手先 ⟨http://www.mext.go.jp/a_menu/kokusai/gaikokugo/1332306.htm⟩（参照 2017-04-26）.

[23] 荘島宏二郎：ニューラルテスト理論：資格試験のためのテスト標準化理論（学力評価の最前線），電子情報通信学会誌，Vol.92, No.12, pp.1013–1016 (2009).

[24] 清水裕士，大坊郁夫：潜在ランク理論による精神的健康調査票（GHQ）の順序的評価，心理学研究，pp.464–473 (2014).

[25] 北村英哉：社会心理学キーワード，有斐閣 (2001).

[26] 吉田富二雄（編著）：心理測定尺度集 II，pp.436–453，サイエンス社 (2007).

[27] 南風原朝和：心理統計学の基礎，有斐閣 (2002).

[28] 水本 篤，竹内 理：研究論文における効果量の報告のために—基礎的概念と注意点，英語教育研究，Vol.31, pp.57–66 (2008).

[29] 村上宣寛：心理尺度のつくり方，北大路書房 (2013).

[30] 村山恭朗，小野佑希：成人版痩身プレッシャー尺度の開発と信頼性・妥当性の検討，神戸学院大学心理学研究，

Vol.1, No.1, pp.11–16 (2018).
[31] 豊田秀樹：はじめての統計データ分析ベイズ的〈ポストp 値時代〉の統計学，朝倉書店 (2016).

付　　録

A.1 バーンアウト段階説

A.1.1 Golembiewski の 8 段階モデル [10]

	Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ	Ⅵ	Ⅶ	Ⅷ
情緒的消耗感	Low	Low	Low	Low	High	High	High	High
個人的達成感の低下	Low	Low	High	High	Low	Low	High	High
脱人格化	Low	High	Low	High	Low	High	Low	High

A.1.2 増田らのバーンアウト判定基準 [11]

	問題なし	うつ状態	問題なし	うつ状態	疲労	バーンアウト		強バーンアウト
疲弊感	Low	Low	Low	Low	High	High	High	High
職務効力感	Low	Low	High	High	Low	Low	High	High
シニシズム	Low	High	Low	High	Low	High	Low	High

A.1.3 バーンアウトに対するゴレンビースキーのモデルと増田らの判定基準との対応

増田らの判定基準	Golembiewski の 8 段階モデル
強バーンアウト	Ⅷ
バーンアウト	Ⅵ，Ⅶ
疲労	Ⅴ
うつ状態	Ⅱ，Ⅳ
問題なし	Ⅰ，Ⅲ

A.2 質問紙

A.2.1 質問紙

「情報セキュリティ対策に関する意識調査」
本調査は，情報セキュリティ対策に関する意識の調査を目的としています．
プライバシーの保護に配慮し，ご回答はすべて統計的に処理します．

設問 1：あなたは最近 6 ヵ月ぐらいの間に，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思う番号に○をつけてください[*4]．

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	情報セキュリティ対策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情報セキュリティ対策は無駄なのに良くやっているなあと思うことがある
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

設問 2：あなたは，情報セキュリティ対策について，どのように感じていますか．お考えを自由に記述してください．

設問 3：あなたは，あなた自身が以下のことについて，どのように思っていますか．もっともあてはまるものを選んでください[*5]

1	私は, 情報セキュリティ対策をきちんとできている
2	私は, きびしい情報セキュリティ対策を求められている
3	私は，情報セキュリティ対策に疲れている

[*4] 1：ない，2：まれにある，3：時々ある，4：しばしばある，5：いつもある

[*5] 1：まったくそう思わない，2：そう思わない，3：どちらとも言えない，4：そう思う，5：とてもそう思う

設問 4：あなた自身のことを教えてください

- 情報端末の利用歴（1 年単位）
  - PC 利用歴：_____年
  - スマートフォン・タブレット利用歴：_____年
- 1 日の平均利用時間（1 時間単位）
  - PC：_____時間
  - スマートフォン・タブレット：_____時間

設問 5：あなたは所属する組織（会社や大学）での情報端末利用に関して，どのような立場ですか．もっともあてはまるものを選んでください．（ひとつだけ）

1	利用者（組織（会社や大学）が決めた情報セキュリティ対策がある）
2	利用者（組織が決めた情報セキュリティ対策はない）
3	管理者（利用者に組織が決めた情報セキュリティ対策を守らせる立場）
4	管理者（管理者だが、組織が決めた情報セキュリティ対策はない）
5	運用者（利用者や管理者ではないが、情報セキュリティ対策や情報システムについて、運用・維持する立場）
6	その他

A.3 調査対象者の年齢分布

A.3.1 調査対象者（社会人）の年齢分布

年齢	男性(名)（割合）	女性(名)（割合）	全体(名)（割合）
12 歳～19 歳	0 (0.0%)	1 (0.2%)	1 (0.9%)
20 歳～24 歳	8 (1.2%)	28 (6.3%)	36 (3.2%)
25 歳～29 歳	31 (4.5%)	84 (18.8%)	115 (10.1%)
30 歳～34 歳	63 (9.2%)	97 (21.7%)	160 (14.1%)
35 歳～39 歳	93 (13.6%)	67 (15.0%)	160 (14.1%)
40 歳～44 歳	104 (15.2%)	65 (14.5%)	169 (14.9%)
45 歳～49 歳	113 (16.5%)	55 (12.3%)	168 (14.8%)
50 歳～54 歳	110 (16.0%)	26 (5.8%)	136 (12.0%)
55 歳～59 歳	90 (13.1%)	17 (3.8%)	107 (9.4%)
60 歳以上	74 (10.8%)	8 (1.8%)	82 (7.2%)
合計	686 (100.0%)	448 (100.0%)	1134 (100.0%)
最年少	20 歳	19 歳	19 歳
最年長	78 歳	68 歳	78 歳

A.3.2 調査対象者（大学生）の年齢分布

年齢	男性(名)（割合）	女性(名)（割合）	全体(名)（割合）
12 歳〜19 歳	47 (30.1%)	147 (33.6%)	194 (32.7%)
20 歳〜24 歳	101 (64.7%)	279 (63.8%)	380 (64.1%)
25 歳〜29 歳	3 (1.9%)	7 (1.6%)	10 (1.7%)
30 歳〜34 歳	3 (1.9%)	1 (0.2%)	4 (0.7%)
35 歳〜39 歳	2 (1.3%)	0 (0.0%)	2 (0.3%)
40 歳〜44 歳	0 (0.0%)	1 (0.2%)	1 (0.2%)
45 歳〜49 歳	0 (0.0%)	1 (0.2%)	1 (0.2%)
50 歳〜54 歳	0 (0.0%)	0 (0.0%)	0 (0.0%)
55 歳〜59 歳	0 (0.0%)	1 (0.2%)	1 (0.2%)
60 歳以上	0 (0.0%)	0 (0.0%)	0 (0.0%)
合計	156 (100.0%)	437 (100.0%)	593 (100.0%)
最年少	18 歳	18 歳	18 歳
最年長	39 歳	56 歳	56 歳

畑島 隆 （正会員）

1995 年名古屋大学大学院工学研究科博士前期課程修了．同年日本電信電話株式会社入社．アクセスログ解析の研究開発，情報流通プラットフォームの研究開発，社会科学的アプローチによる情報セキュリティ研究に従事．電子情報通信学会会員．

谷本 茂明 （正会員）

1982 年徳島大学工学部電気工学科卒業．1984 年徳島大学大学院工学研究科電気工学専攻修了．同年日本電信電話公社入社．主にプライベートネットワークシステムの研究開発に従事．2009 年より千葉工業大学社会システム科学部准教授．2012 年教授．現在，情報セキュリティマネジメントシステムの研究開発に従事．博士（工学）．電子情報通信学会シニア会員，IEEE Senior Member，プロジェクトマネジメント学会理事．本会シニア会員．

金井 敦 （正会員）

1980 年東北大学工学部通信工学科卒業．1982 年東北大学大学院工学研究科情報工学科博士前期課程修了．同年日本電信電話公社電気通信研究所入社．ソフトウェア開発プロセス，ソフトウェア分散開発環境，Web サービス開発技術，ネットワークコミュニティ，情報セキュリティ，サイバーセキュリティの研究開発に従事．2008 年から，法政大学理工学部応用情報工学科教授．博士（情報科学）．電子情報通信学会シニア会員，IEEE Senior Member．本会シニア会員．