情報処理学会論文誌 Vol.59 No.12 2105–2119 (Dec. 2018)

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

畑島 隆[1,a)] 谷本 茂明[2] 金井 敦[3] 冨士 仁[1] 大久保 一彦[1]

受付日 2018年2月26日, 採録日 2018年9月7日

概要：情報セキュリティ対策の効果が上がらない原因として，情報セキュリティ対策施策に対してICT利用者が疲弊する，情報セキュリティ疲れ（Information security fatigue）が注目されている．本研究では，情報セキュリティ疲労度測定尺度と情報セキュリティ対策実施度測定尺度を組み合わせた，情報セキュリティコンディションマトリクスによって，ICT利用者の情報セキュリティ対策に対する状態を可視化した．先行研究において作成した各測定尺度を用いて実施した大学生に対する質問紙調査結果に対して，潜在ランク理論を情報セキュリティ疲労度で3ランク，情報セキュリティ対策実施度で2ランクに分類する設定で適用した．これらの組合せによって構成される情報セキュリティコンディションマトリクスによって，大学生の情報セキュリティ対策に対する状態を6群に分類した．質問紙調査の自由回答文から各群の特徴を抽出し，情報セキュリティ対策に対する態度として理想的な状態を明らかにするとともに，この状態を維持させる方策，および他の5群を理想状態に移行させるための方策を明らかにした．本研究の成果によって，情報セキュリティ対策施策のパーソナライズ化が実現可能となり，内部不正や情報漏洩といった情報セキュリティインシデントを抑止し，情報セキュリティ対策の費用対効果を向上させることが期待できる．

キーワード：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，潜在ランク理論

Proposal of Information Security Fatigue Countermeasures for College Students by Improved Information Security Condition Matrix

Takashi Hatashima[1,a)] Shigeaki Tanimoto[2] Atsushi Kanai[3]
Hitoshi Fuji[1] Kazuhiko Ohkubo[1]

Received: February 26, 2018, Accepted: September 7, 2018

Abstract: Information security fatigue, which indicates that ICT users are exhausted for information security countermeasures, is regarded as a factor in reducing the effectiveness of information security measures. In this paper, we clarified how ICT users are tired of information security countermeasures by "information security condition matrix" combined with information security fatigue degree scale and information security measures implementation scale. The latent rank theory was applied to the questionnaire survey results for college students using each scale created in our previous research. Each scale was classified into three ranks by information security fatigue degree and two ranks by information security measures implementation degree. As a result, the respondents were classified into six groups by the information security condition matrix. We extracted the features of each group by analyzing open-ended questions of the questionnaire survey and clarified the ideal state as an attitude toward information security measures. Then, we presented a strategy to maintain this condition and a strategy to shift the other five groups to the ideal condition. The results of this research will make it possible to personalize information security countermeasures, suppress information security incidents such as internal fraud and information leakage, and improve cost effectiveness of information security measures.

Keywords: information security fatigue, information security condition matrix, latent rank theory

1. はじめに

ICT（Information Communication Technology）は現代社会に深く根付いている．安心安全なICT利用には，標的型攻撃やランサムウェアのような高度化の一途にあるサイバー犯罪への対応や，メールの誤送信といったヒューマンエラーによるインシデントの防止が必須であるため，情報セキュリティ対策は情報処理産業の従事者だけでなく，すべてのICT利用者に実施が求められる．しかしICT利用者が企業や学校，情報セキュリティ関連の公的機関などから実施を求められる情報セキュリティ対策は，高度かつ複雑化される一方であるため，情報セキュリティ施策が施策実施者の意図どおりの効果が上がらない現状があり，この状況を解明し改善するための研究が数多く行われている．

これらの課題に対して我々は，情報セキュリティ対策施策に対してICT利用者が疲弊する「情報セキュリティ疲れ（Information security fatigue）」[1]に着目し，情報セキュリティ疲れに陥ることで，企業や学校，公的機関などが実施する情報セキュリティ対策施策の効果が上がらなくなっていると仮説を設定した．本研究ではそのなかでも萌芽的な研究対象として，大学生のセキュリティ疲れに着目した．大学生に着目した理由は，以下のような経緯により，情報セキュリティ対策による負担が大学生においても企業の従業員と同様に増加しているとみられるためである．

まず，2005年から広島大学で全国の大学に先駆けてすべての学生および教職員にウィルス対策ソフトが無償配布[2]されたように，大学生が利用する端末が情報セキュリティ上保護されるようになった反面，大学生は安全な状態を維持するためにウィルス対策ソフトやパターンファイルの定期的な更新といった，情報セキュリティに対する能動的な対応が求められる作業負担が発生するようになったことがあげられる．

また，2006年から国立情報学研究所が高等教育機関を対象とした情報セキュリティ対策のためのサンプル規程集[3]を公開開始し，これに対応して各大学は個別施策として体系的な情報セキュリティ対策を強化してきたことや，さらに，2016年に東京電機大学のCSIRT（Computer Security Incident Response Team）が日本シーサート協議会[4]に大学として初加盟[5]したのを皮切りに2018年2月1日現在10大学が加盟するようになり，情報セキュリティインシデントに対応する企業間の連携ネットワークに大学も参加するようになったこともあげられる．

以上のように，大学による企業と遜色ない組織的な情報セキュリティ対策の実施傾向がみられ，大学に通う学生にも対応が要求されているため，大学生は情報セキュリティ疲れを起こしやすくなっていると考えた．

我々は先行研究[6], [7], [8], [9]において，情報セキュリティ疲れを測定するために，「ICT利用者が情報セキュリティ対策施策に対応するうちに，情報セキュリティ対策の実施に疲弊感を持ち，その結果，情報セキュリティ対策の実施をしなくなる状態」を情報セキュリティバーンアウトと呼び，「情報セキュリティ対策の実施に疲弊感を持っている状態」を情報セキュリティ疲れと定義した．この定義に従うことによって，後述する2.3節に示した一般的なバーンアウトの測定に用いられる手法である質問紙調査による測定を可能とした．また同様に，情報セキュリティに対するICT利用者の態度の状態を，複数の心理尺度の組合せによって可視化する情報セキュリティコンディションマトリクスを提案した[6], [7]．

本研究では情報セキュリティコンディションマトリクスを2次元で表現し，縦軸に情報セキュリティ疲労度尺度，横軸に情報セキュリティ対策実施度を設定した．それぞれの測定尺度からなる質問紙調査を大学生に実施し，潜在ランク理論を用いて情報セキュリティコンディションマトリクス上で6群に分類した．分類された6群それぞれの特徴を，質問紙調査の自由回答に対するアセスメントによって抽出した．

上記6群のうち情報セキュリティ対策に対する態度が理想状態にある大学生が所属する群はその状態を維持させ，その他の群は理想状態に近づけることによって，情報セキュリティ対策の効果を向上させることを目的としたアセスメントおよび対応策の提示と評価を実施した．

以下，2章で関連研究を述べ，3章で本論文に用いる概念の定義を行う．4章では，情報セキュリティコンディションマトリクスの仮説と，本研究で用いる改善モデルを提案する．5章では，情報セキュリティコンディションマトリクスを構成する2軸の測定尺度と自由回答からなる質問紙の作成と，質問紙調査の概要，および調査結果への潜在ランク理論の適用による回答者の6群への分類結果を述べる．6章では，質問紙調査結果の分析として，各群の特徴抽出と情報セキュリティに対する態度として理想的な状態に移行させるためのアセスメントおよび対応策の提示と評価について述べる．最後に7章において本論文をまとめる．

2. 関連研究

2.1 情報セキュリティ疲れ

情報セキュリティ疲れは，2009年のFurnellとTompsonによる記事[1]が初出とみられ，近年の学術面ではUsable Security分野の主要会議であるSOUPS 2016（Twelfth Symposium on Usable Privacy and Security 2016）において

[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)] hatashima.takashi@lab.ntt.co.jp

ワークショップが開催されたことがあげられる．同ワークショップで Parkin ら [10] は，ヒューマンエラーの研究者である Reason [11] が示したヒューマンエラーに関する認知状態 Cognitive Control Mode の概念を援用し，ルーチン作業として実施を求められる情報セキュリティ対策（たとえば 2 要素認証）に起因する情報セキュリティ疲れの発生要因は，指示される情報セキュリティ対策の変化にともない Cognitive Control Mode の変更を強いられることが，情報セキュリティ疲れのホットスポットであると説明している．また，同じく 2016 年には NIST（US National Institute of Standards and Technology）の研究者ら [12] による情報セキュリティ疲れを軽減するための 3 つの提言が，情報セキュリティ専門家や IT プロフェッショナルではない 40 名への聞き取り調査によって情報セキュリティ疲れの実態を分析した結果として示されている．このように，情報セキュリティ疲れは Usable Security 研究者の関心が集まる研究分野である．

2.2 情報セキュリティ施策に対する行動

情報セキュリティに対する企業施策に係わる研究として，情報セキュリティ対策の施策が進まない問題について，質問紙調査と因子分析や構造方程式モデリングによって行動モデルを構築し，施策の改善に関する提案をするものがあげられる．

諏訪ら [13] は情報セキュリティ対策意識について情報セキュリティ行動基本モデルを設定し，インターネット利用者を対象とした質問紙調査結果に対する共分散構造分析によって，意識的セキュリティ行動，習慣的セキュリティ行動，そして予防的セキュリティ行動のそれぞれ要因の異なる 3 つの行動パターンがあることを示した．菅野ら [14] は情報セキュリティ対策における阻害要因について，施策を推進する責任者および担当者の意識と行動に着目し，大企業と中小企業の 2 母集団を比較により施策推進の阻害要因を示した．前述のほか，情報セキュリティポリシに対する遵守意識を行動モデルの適用により解明する研究が多数報告されている（たとえば Bulgurcu ら [15]，Ifinedo [16] など）．

しかし，ICT 利用者の心理状態を測定，分類することによって情報セキュリティ対策施策の効果向上のアセスメントと対策の提示を行うことを目的とした本研究とはアプローチが異なる．

2.3 バーンアウト

バーンアウト（Burn out）は燃え尽き症候群とも訳され，久保 [17] は，“この概念を初めて学術論文で取り上げた Freudenberger (1997) によると「辞書的な意味でいえば，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．

実証的なバーンアウト研究は，バーンアウトはどのような状態なのかを測定する取組みから始まり [18]，その測定には質問紙調査が用いられている．バーンアウトの測定尺度は Maslach らによって MBI（Maslach Burnout Inventory）が開発され，1982 年に MBI マニュアル第 1 版が作成されて以降，多くの研究者に採用されてきた [19]．

情報セキュリティに対するバーンアウトの研究として，Chandran ら [20] による SOC（Security operations center）に従事するセキュリティアナリストの職業的燃え尽きについて，アナリストらの行動を継続的に記録した記述を分析した研究がある．しかし，これは一般的なバーンアウトを課題としており，本論文で述べる情報セキュリティ施策に対して実際に対策を実施する ICT 利用者が感じる情報セキュリティ疲れとは課題が異なるため，本研究の新規性を損なわない．

2.4 MBI におけるバーンアウト段階説

バーンアウトに至る過程を段階的に表した「バーンアウト段階説」の代表例として，**表 1** に示すように，看護師やソーシャルワーカーを対象としたバーンアウトの測定尺度である MBI-HSS（Maslach Burnout Inventory – Human Services Survey）を構成する 3 因子それぞれの尺度得点を上位群と下位群に分け，その組合せによる 8 段階に対して順序付けをした Golembiewski の 8 段階モデル（eight-phase model）[17] がある．このモデルでは，I から VIII へと段階が進むにつれバーンアウトが悪化した状態を示している．しかし，すべての状態を経由するわけではなく，バーンアウトが急性的であるか慢性的かであるかによっても進行径路が異なっている．また，バーンアウトの過程が 1 つではなく，職種によりバーンアウトの過程にはかなりの違いが認められることが報告されている [17]．

また，**表 2** に示すように，増田ら [21] は心理尺度（ヒューマン・サービス（対人援助職））に限らないすべての職業に対するバーンアウト測定尺度 MBI-GS（Maslach Burnout Inventory – General Survey）と，抑うつ状態自己評価尺度日本語版および JCQ（Job Content Questionnaire）日本語版を用いた質問紙調査の結果により，対人援助職に限らないバーンアウトの判定基準（増田らの判定基準で，「強

表 1 Golembiewski の 8 段階モデル [17]
Table 1 Golembiewski's eight-phase model [17].

	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

表 2 増田らによるバーンアウト判定基準 [20]
Table 2 Criteria for burnout [20].

	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

表 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
Table 3 Correspondence table of Table 2 and Table 3.

増田らの判定基準 (MBI-GS による)	Golembiewski の 8 段階モデル (MBI-HSS による)
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

バーンアウト」「バーンアウト」「疲労」「うつ状態」「問題なし」の 5 状態）を示している．増田らも Golembiewski と同様に MBI-GS の 3 つの測定尺度に設定したしきい値に対する尺度得点の高低によってバーンアウトの判定を実施している．その特徴として下位尺度にも影響の順序づけがあり，疲弊感が高いことがバーンアウト状態や疲労状態と判定する条件とし，また，疲弊感は低いがシニシズム（冷笑感）が高いときをうつ状態と呼び，疲弊感もシニシズムも低い状態であれば，職務効力感の尺度得点にかかわらず問題なしと判定している．

用いる測定尺度が異なるため直接比較できないが，参考として**表 3** に MBI-HSS による Golembiewski の 8 段階モデルと，MBI-GS による増田らの判定基準との対比を示す．

2.5 潜在ランク理論

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，Shojima [22] による潜在ランク理論を利用した．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は，その素点の得点差を評価するものではなく，数段階のレベル分けして判定し，質的評価できることが期待されている．この課題に対して荘島は，ノンパラメトリックな項目反応理論としてニューラルテスト理論（Neural Test Theory，NTT）を立ち上げ，これを潜在的な順序グループを推定する一般モデルとして拡張した潜在ランク理論（Latent Rank Theory，LRT）を提唱している．

潜在ランク理論は，潜在尺度に順序尺度を仮定することで，学力テストにおける各設問の正解と不正解の 2 値や，質問紙調査における多段階のリッカート尺度による回答結果

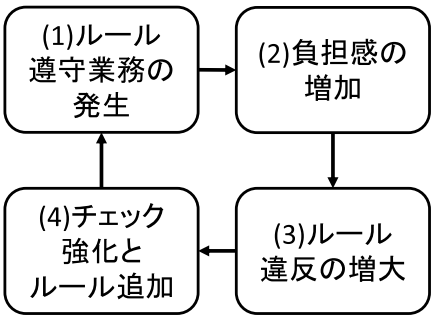

図 1 情報セキュリティ対策における悪循環 [6], [7], [8], [9]
Fig. 1 Vicious cycle on cooperate information security [6], [7], [8], [9].

といったデータを入力とし，あらかじめ設定する段階（ランク）数に所属する確率を推定する手法である．なお，テスト理論における項目反応理論（Item Response Theory，IRT）は母集団に左右されず項目の難易度を推定できる点が優れているが，潜在尺度に連続尺度を仮定している [23] ため，本論文への適用は潜在ランク理論がより適している．

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 [24] 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 [25] や，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，過去の知見によるカットオフポイントによる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 [26] があげられる．

3. 本研究で用いる概念の定義

3.1 情報セキュリティ疲れ

我々は，「ICT 利用者が情報セキュリティ対策施策に対応するうちに，情報セキュリティ対策の実施に疲弊感を持ち，その結果，情報セキュリティ対策の実施をしなくなる状態」を情報セキュリティバーンアウトと定義し，また，前述した「情報セキュリティ対策の実施に疲弊感を持っている状態」を情報セキュリティ疲れと定義している．

情報セキュリティ疲れの発生要因の 1 例として，我々は情報セキュリティに関係するルールの厳格な運用があると仮説している [6], [7], [8], [9]．企業や学校といった組織は，情報漏洩といった情報セキュリティインシデントを予防するためにセキュリティルールを制定し，その遵守や運用での対処を求める（**図 1** の (1)）．これに対してその組織に属する ICT 利用者は，その負担から，当初は遵守行動をとるが，一般に ICT 利用の効率化と相反するため，生産性の追求や施策への意義を見い出せないといった理由により，次第に情報セキュリティ対策を省略もしくは自身の判断で簡略化するようになる（図 1 の (2)）．これによりルールに対する逸脱行為が増大する（図 1 の (3)）．そうすると，ルール違反を防止するためのチェックリストやルール自体の追

加が行われる（図 1 の (4)）．この結果，ルールや手続が増加することとなり（図 1 の (1)），ICT 利用者の負担がさらに増大する（図 1 の (2)）．このように，ICT 利用者のセキュリティ疲れは悪化するばかりであり，また，組織側においてもセキュリティルールや運用手続も増大するため，対策の費用対効果は悪化するばかりであるという課題があるとみられる．

なお，一般的にバーンアウトとは，2.3 節にあげたバーンアウトの測定尺度によって測定されるように，従事する業務全体を対象としている．それに対して，本研究で呼ぶ情報セキュリティバーンアウトおよび情報セキュリティ疲れは，情報セキュリティ施策のみを対象としている点が異なるが，測定のために質問紙調査を実施するという手法は援用に値すると判断し，研究を進めている [6], [7], [8], [9]．また，本研究ではバーンアウト段階説を，情報セキュリティ疲れの程度を段階的に可視化する手法として援用した．

3.2 情報セキュリティコンディションマトリクス

我々の研究動機は，上記のような情報セキュリティ疲れから発生する問題を解決することである．これを実現する研究として，ICT 利用者の情報セキュリティ対策に対する態度として理想的な状態や情報セキュリティ疲労を起こしている状態などの可視化と解決法の検討を進めている．我々は先行研究 [6], [7] において，状態の可視化手段として，情報セキュリティコンディションマトリクスを提唱している．これは，複数の測定尺度の組合せによって，ICT 利用者の情報セキュリティ対策に対する態度がどのような状態であるかを 2 次元の有限個の状態で表現するものである，

情報セキュリティコンディションマトリクスのそれぞれの状態に対して，情報セキュリティ対策の施策を強化だけでなく軟化させる方向に変化させるといった柔軟で動的な施策変更により，利用者各人が情報セキュリティ対策の施策に対して情報セキュリティ疲れを起こした状態とならないようにすることで，内部不正や情報漏洩といった情報セキュリティインシデントを抑止し，情報セキュリティ対策の費用対効果を向上させることが期待できる．

4. 改善型情報セキュリティコンディションマトリクスの提案

4.1 情報セキュリティコンディションマトリクスの仮説

我々は先行研究 [7] において，2.5 節に示した潜在ランク理論を用いて縦軸に 3 段階の情報セキュリティ疲労度をとり，横軸に 2 段階の情報セキュリティ対策実施度とした 6 群の状態からなる 2 次元の情報セキュリティコンディションマトリクスの仮説を**図 2** のように提案し，6 群それぞれについて状態の定義とリスクアセスメントを実施した．

本論文では，先行研究 [7] と同様に情報セキュリティコンディションマトリクスを用いて，それぞれの状態に配置される回答者の特徴を考察することによって，各群のアセスメントと対策案の提示および評価を行う．

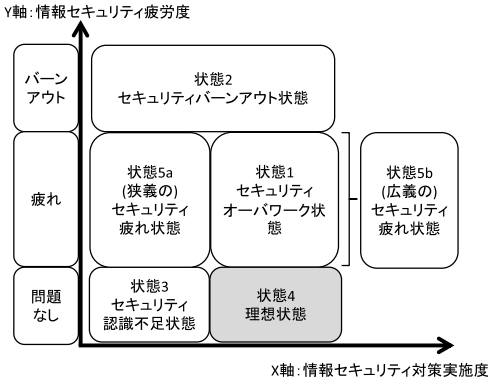

図 2 情報セキュリティコンディションマトリクスの仮説 [7]
Fig. 2 Hypothesized information security condition matrix [7].

4.2 情報セキュリティ疲労度（F 群）および情報セキュリティ対策実施度（Im 群）によるランク付け

我々は 4.1 節に示した仮説を検証した先行研究 [8] において，情報セキュリティ疲労度尺度決定のための質問項目と情報セキュリティに関して感じていることを自由回答させる設問のそれぞれを尋ねる調査を実施した．これを分析した結果，情報セキュリティ疲労度を 5 段階に分類した場合，中間に当たる 3 段階目が情報セキュリティ対策に対して適度な緊張感を持つ理想状態であることを明らかにした．同研究では，そのほか，情報セキュリティ疲労度が中間状態よりも高い場合には，情報セキュリティ対策に対する冷淡な感覚や情報セキュリティ対策の実施責任に対する負担感，そして対策の重要性を認識しているものの実施する意思がともなわない状態であることを明らかにした．

また，その反面，情報セキュリティ疲労度が中間状態よりも低い場合には，先行研究 [8] における自由回答から「個人情報の漏洩を完全に防ぐことは困難であるため，そのリスクを承知でサービスを利用するべきである．企業の個人情報が流出した際に，世間が大騒ぎするが，そんなに騒ぐほどでもないと思う」や「情報セキュリティ対策はとても大切なことだと考えているが，あまり日常で考えたことはなかった．あればいいなと思うだけであった」という意見が獲得されたことから，自身が情報セキュリティ対策を行う当事者であることを意識せず，情報セキュリティ対策を実施していないことがうかがえたことを根拠として，情報セキュリティ対策への当事者意識の低さがみられることも明らかにした．

この知見を用いて，本論文では，初期検討として F 群と Im 群それぞれについて最小数を用いた．すなわち，情報セキュリティ疲労度を示す F（Fatigue）群のうち中間に当たる群を F0 群とし，それより低い群を F-群，高い群を

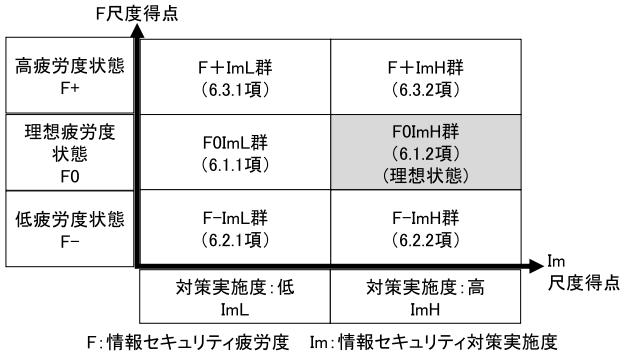

図 3 改善型情報セキュリティコンディションマトリクス
Fig. 3 Improved information security condition matrix.

F+群と定義する 3 ランクを設定した．また，同様に情報セキュリティ対策実施度を示す Im（Implementation）群は，情報セキュリティ対策実施度が低い群を ImL 群，高い群を ImH 群と定義する 2 ランクを設定した．以上により，本論文では F 群と Im 群の組合せによる 6 群に対して検討を進めた．

4.3 情報セキュリティコンディションマトリクスの改善

4.1 節と 4.2 節における検討の結果，情報セキュリティ疲労度は，4.2 節に示すように低すぎると弊害が生じることが分かった．一方，情報セキュリティ対策実施度は高いほうが良いことは自明である．

以上により，図 2 に示した情報セキュリティコンディションマトリクスは，**図 3** のように改善され，F0ImH 群が理想状態であると定義された．

本論文では，以降，6 群それぞれの特徴を図 3 に示した項番号において考察することにより，情報セキュリティコンディションマトリクスのアセスメントを実施し，これらの対策の提案と評価を実施する．

5. 大学生の情報セキュリティ疲れの質問紙調査による測定と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可視化

5.1 質問紙の作成

5.1.1 情報セキュリティ疲労度尺度

情報セキュリティ疲労度を測定する質問紙について説明する．情報セキュリティについて個人の内的要因を心理測定尺度によって可視化する研究は，3.1 節に示したように 2.3 節にあげた一般的な意味でのバーンアウトと異なり，これまであまり行われていないため，一般的なバーンアウトの測定尺度を援用して作成した．

具体的には，(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 件法の 23 項目で構成される質問紙を先行研究 [8] において作成し，(2) 先行研究 [9] 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 1）を作成するという手順で実施した．

妥当性に関する内容妥当性，基準関連妥当性，および構成概念妥当性の検討は以下のように行った．まず内容妥当性は筆者らのディスカッションにより行った．そして基準関連妥当性は情報セキュリティ分野における萌芽的研究分野であることから既存尺度との相関を求めることが困難として今後の研究課題とした．最後に構成概念妥当性は共分散構造分析を用いた確認的因子分析により検討した結果，3 つの下位尺度による 2 次因子構造が得られた．

5.1.2 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，先行研究 [27] で用いた尺度を援用した．具体的には，測定にウィルス感染経験，IT 知識および IT スキルを設定した浜津ら [28] にならい，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 [29]，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 [30] における「テレワーク勤務者が実施すべき対策」から翻案し 17 項目を作成した [27] 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 件法の 11 項目からなる質問紙（付録質問 2）を作成した．テレワークセキュリティガイドラインを援用した理由は，大学生は企業に勤める人におけるテレワークのように，場所を問わず PC を利用すると考えられるためである．質問 2 は前述のように大学生など企業に勤めない人にも求められる一般的な情報セキュリティ対策項目として設計されているため，本研究において大学生を対象として尋ねることは妥当である．なお，今回質問紙調査をした両大学においても，質問 2 の各項目は施策の深浅（たとえば情報セキュリティハンドブック [31] のような文書の公開の有無など）はあるものの，いずれも学生に対しての実施が求められている．

5.1.3 情報セキュリティに対する所感の自由回答

また，各群ごとの特徴抽出を抽出する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，お考えを自由に記述してください」を設けた（付録質問 3）．

5.2 質問紙調査の実施

作成した質問紙を用いた調査を，首都圏内の私立大学 2 大学で実施した．調査は 2017 年 9 月 28 日から同年 10 月 11 日に実施され，392 票が回収された．被験者は首都圏内の私立大学に通う 1 年生から修士課程 2 年生の 310 名，および別の首都圏の私立大学に通う 2 年生 82 名であった．いずれも調査開始時に文書と口頭で依頼し合意を得た．なお，謝礼は提示していない．これらから欠損値があるデータを

除外した 337 票を有効回答（有効回答率 86.0%）とした．

有効回答者の年齢は，全体では 337 名（平均 19.64 歳，標準偏差（SD）1.38）であり，男女別では男性が 276 名（平均 19.66 歳，標準偏差 1.40），女性が 61 名（平均 19.54 歳，標準偏差 1.34）であった．

なお，各設問の回答に付与する得点は，情報セキュリティ疲労度測定尺度では，「ない」を 1 点，「まれにある」を 2 点，「ときどきある」を 3 点，「しばしばある」を 4 点，「いつもある」を 5 点とした．また，情報セキュリティ対策実施度測定尺度では，「まったく実施していない」を 1 点，「たまに実施している」を 2 点，「ときどき実施している」を 3 点，「よく実施している」を 4 点，「いつも実施している」を 5 点とした．

5.3 潜在ランク理論による回答者の分類

本研究では，潜在ランク理論による分析に荘島によるソフトウェア exametrika（エクザメトリカ）[32] 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 [33] とされている．

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，4.2 節に示したように，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 4** 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 5** に，情報セキュリティ対策実施度の尺度得点は**表 6** にそれぞれ示すようになった．

6. 改善型情報セキュリティコンディションマトリクス各群のアセスメント結果および対策案と評価

本章では，最初に，5 章の質問紙調査結果をもとに，図 3 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．次に，4.3 節に示した理想状態である F0ImH 群にそのほかの 5 群が移行するための対策や，F0ImH 群がその状態を維持するための対策について具体例を提案する．

以下の各項に詳細を述べるように，情報セキュリティコンディションマトリクスを構成する 6 群について，5.1.3 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実施し，**表 7** に示す 14 件の対策案 (1)〜(14) が導かれた．これらの対策案は，本論文において実施した質問紙調査の有効回答 337 件のうち，自由回答が記された 135 件から演繹的に導出することにより客観性を担保したが，自由回答からは大学生の ICT 利用状況や特性に関するものがほとんどみられなかった．

表 4 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 4 Number of respondents on information security condition matrix.

回答者数 (N=337)		Im 群	
		実施度低 [ImL]	実施度高 [ImH]
F 群	疲労度＋ [F+]	53	54
	疲労度 0 [F0]	60	60
	疲労度− [F−]	61	49

表 5 情報セキュリティ疲労度の尺度得点と標準偏差
Table 5 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+]	40.08 (5.20)	41.09 (6.42)
	疲労度 0 [F0]	30.00 (3.36)	31.53 (4.53)
	疲労度− [F−]	20.80 (3.58)	21.76 (3.35)

表 6 情報セキュリティ対策実施度の尺度得点と標準偏差
Table 6 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+]	30.34 (4.39)	41.00 (3.72)
	疲労度 0 [F0]	29.03 (5.33)	39.92 (3.93)
	疲労度− [F−]	28.82 (4.80)	40.31 (3.53)

表 7 改善型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のアセスメント結果および対策案と評価

Table 7 Results of assessing open-ended questions by group for information security condition matrix, countermeasure and evaluation.

群略称 (論じる 項番号)	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 群に移行させる ・理想状態を維持する	対策効果の評価(6.4 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 (6.1.1)	・市販製品を使う意志はあるが，製品の選定ができない ・情報セキュリティ対策についての自身の練度に不安を持つ ・対策の重要性や必要性は認識しているが実施できていない	(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】	変化なし	上昇 [ImH へ]
		(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	変化なし	上昇 [ImH へ]
		(3)情報セキュリティ対策ソリューションの提供【ソリューションの提供】	変化なし(a)	上昇 [ImH へ]
F0ImH (6.1.2) (理想状態)	・状況に応じた情報セキュリティ対策の難しさに対する指摘をする ・情報セキュリティ対策実施度に対する自己評価が高い ・情報セキュリティに関する知識獲得に積極的な姿勢をみせる	(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が可能	変化なし	変化なし
		(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
F−ImL (6.2.1)	・情報セキュリティ対策の実施当事者であるという意識が薄い ・必要性は認識しつつ対策は実施していない ・何をどれだけやれば良いのかがわからない	(6)当事者意識を喚起する教育の実施	上昇 [F0 へ]	上昇 [ImH へ]
		(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指示【マニュアル化】	上昇 [F0 へ]	上昇 [ImH へ]
F−ImH (6.2.2)	・情報セキュリティソリューションに依存する ・スマートフォンの情報セキュリティ対策に言及する ・情報セキュリティ対策実施への練度は高い ・実施はしているが面倒さを訴える	(6)当事者意識を喚起する教育の実施	上昇 [F0 へ]	変化なし
		(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	上昇 [F0 へ]	変化なし
		(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 (6.3.1)	・対策を実施していない認識を持ちながら脆弱な状態を維持している ・情報セキュリティ対策を実施していないことを認識し，自己分析する ⇒確信的に情報セキュリティ対策の実施をおろそかにしている ・実施中の具体的な情報セキュリティ対策への不満や要望を示す	(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	降下(b) [F0 へ]	上昇 [ImH へ]
		(11)情報セキュリティ対策に関するヒアリング(ガス抜きと具体的な不実施理由の聴取)	降下 [F0 へ]	上昇 [ImH へ]
F+ImH (6.3.2)	・情報セキュリティ対策の当事者としての意識が高い ・対策推進への提言を示す ・疲労感を直接表す(しんどい) ・属人的な対応の難しさを訴える	(11)情報セキュリティ対策に関するヒアリング(ガス抜き)	降下 [F0 へ]	変化なし
		(12)情報セキュリティ教育の間隔を延伸	降下 [F0 へ]	変化なし(a)
		(13)情報セキュリティ教育の簡易化	降下 [F0 へ]	変化なし(a)
		(14)組織的な教育体制の整備	降下 [F0 へ]	変化なし

a 1 段階降下の可能性あり
b 変化なしの可能性あり

6.1 情報セキュリティ疲労度が中程度な各状態（F0 群）の特徴とアセスメント

6.1.1 情報セキュリティ疲労度が中程度で，実施度が低い状態（F0ImL 群）

この群は，情報セキュリティ疲労度が中程度で，情報セキュリティ対策実施度が低いグループである．この群に属する回答者（表 4）は 60 名であった．情報セキュリティ疲労度尺度得点（表 5）は平均 30.00 点，標準偏差 3.36 であり，情報セキュリティ対策実施度尺度得点（表 6）は平均 29.03 点，標準偏差 5.33 であった．

この群では，「セキュリティ対策は何をどうすれば正解なのか分からない．種類が多くどれをインストールすればよいか分からない（回答者 ID 61）」，「PC の有料ソフトが高く買えない（回答者 ID 267）」のように，情報セキュリティ対策に市販製品を使う意志はあるが，製品の選定ができないために対策実施もできていない様子がみられた．

また，「セキュリティ対策は必要だと思う．しかし，設定が分かりにくかったり，ややこしく，正しく対策ができているのか不安になることもある（回答者 ID 304）」のように，セキュリティ対策についての自身の練度に不安を持つ様子もみられた．

さらに，面倒という回答のうちでも「やらなければいけないと分かってはいるが面倒くさいと感じてやっていない（回答者 ID 13）」のように対策を実施していないとの回答と，「面倒だと感じることも多いですが，必要なことだと思いました（回答者 ID 55）」，「面倒だけど必要（回答者 ID 200）」，「重要だが面倒くさいイメージです（回答者 ID 321）」のように対策の重要性や必要性は認識するが質問紙調査の結果では情報セキュリティ対策実施度が低い回答がそれぞれみられた．

以上のようにこの群は，情報セキュリティ対策についての意識は持っているが，自分自身がどれだけ対策できているかという練度に不安を持っていたり，面倒さから対策を実施していなかったりする回答者の集合であるとみられる．

この群を理想状態に移行させるには，情報セキュリティソリューションの推奨環境を提示することで，製品選定の補助（対策案 (1)）をしたり，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（対策案 (2)）で，対策がどの程度できているか，何が足りていないかを認識させたりすることが有効であると考えられる．また，面倒であるとの認識が多くみられるため，これを解消する必要がある．その方策としては，情報セキュリティ対策が面倒だと思ってしまう過剰な負担感を解消するために，大学側がセキュリティアップデートを集中管理する OS 環境や，ウィルスパターンの配信やウィルススキャンの定期実行をコントロールする統合セキュリティ対策ソフトウェアの提供といった情報セキュリティ対策ソリューションの提供（対策案 (3)）や，チェックリスト（対策案 (2)）による必要最低限な対策の体系的な提示が有効であると考えられる．

6.1.2 情報セキュリティ疲労度が中程度，実施度が高い状態（F0ImH 群：理想状態）

この群は，情報セキュリティ疲労度が中程度で，情報セキュリティ対策実施度が高いグループであって，4.3 節で示したように本研究では理想状態であると仮定されている．この群に属する回答者（表 4）は 60 名であった．情報セキュリティ疲労度尺度得点（表 5）は平均 31.53 点，標準偏差 4.53 であり，情報セキュリティ対策実施度尺度得点（表 6）は平均 39.92 点，標準偏差 3.93 であった．

この群では，「ガバガバのセキュリティもあればガチガチのセキュリティもあるからセキュリティ対策ができないと考える（回答者 ID 14）」のように，状況に応じた情報セキュリティ対策の難しさに対する指摘がみられた．

そのほか，「情報セキュリティ対策はほとんどの人が実施しているが設定が面倒であり，時間がかかるものが多い．もっと手軽でパソコンなどにうとい中高年の人などにも使いやすいセキュリティ対策ソフトがあると良いかもしれない（回答者 ID 81）」や，「必要なことではあるが，簡便にできるようにしていくべき．面倒という理由で実行しない人々も一定数いるため（回答者 ID 152）」のように，自分はできているが情報セキュリティ対策はもっと容易であるべきと提言する回答がみられた．つまり，情報セキュリティ対策実施度に対する自己評価の高さもうかがわれた．また，「情報セキュリティ対策とはどの程度の範囲を示すのか身近な例で知りたい（回答者 ID 30）」という，より情報セキュリティに関する知識獲得に積極的な姿勢もみられた．

この群に対しては上記のように，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が可能（対策案 (4)）であるとみられる．この群の状態を維持させるには，現状理想状態であることを知らせてこの状態を維持するモチベーションを喚起する（対策案 (5)）ことが有効であると考えられる．理想状態から他の状態への移行は，たとえば 6.2.2 項の回答者 ID 62 のように，対策をしていたのに問題が起こってしまってがっかりすることで当事者意識の薄れが起こるために F 群が低下して，F−ImH 群に移ることが考えられる．

6.2 情報セキュリティ疲労度が低い状態（F−群）の特徴とアセスメント

6.2.1 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，情報セキュリティ疲労度は低く，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 4）は 61 名であった．情報セキュリティ疲労度尺度得点（表 5）は平均 20.80 点，標準偏差 3.58 であり，情報セキュリティ対策実施度尺度得点（表 6）は平均 28.82

点，標準偏差 4.80 であった．

この群では，「自分は大丈夫だろうと思いがち（回答者 ID 51）」，「社会に出ていない以上，機密性の高いファイルなどを扱うことが少ないためか当事者意識が薄いのかなーとアンケートを通じて思いました（回答者 ID 74）」，「セキュリティ対策は個人でやるものなのかどうか分からない（回答者 ID 306）」のように，情報セキュリティ対策の実施当事者であるという意識の薄さがみられた．

また，「難しいイメージが強く，ふだんあまり気にかけていない（回答者 ID 23）」，「対策しなくてはいけないと思いつつも実際は特に何もしていないことに危機感を覚える（回答者 ID 296）」，「パスコードや指紋認証も面倒で off にしてしまっている（回答者 ID 322）」のように，情報セキュリティ対策の必要性は認識しつつ対策は実施していない回答傾向がみられた．

そのほか，「正しい情報セキュリティが分からない（回答者 ID 67）」，「全然知識がなかったと感じました（回答者 ID 47）」，「情報セキュリティ対策は重要だと思っていますが，実際に自分がどのような対策をしたらよいのかが分からない（回答者 ID 57）」，「情報セキュリティ対策についてどのくらいが対策しているといえるか，具体的に何が対策なのか分からない（回答者 ID 289）」のように，情報セキュリティ対策について，何をどれだけやればいいのかが分からないという回答傾向がみられた．

この群を理想状態に移行させるには，この群は 4.2 節に示したように，当事者意識の薄さから F−群に属しているため，意識を喚起 [8] する教育の実施（対策案 (6)）と，情報セキュリティ対策マニュアルの提供といった実施すべき対策の具体的な指示（対策案 (7)）が有効であると考えられる．

6.2.2 情報セキュリティ疲労度が低く，実施度が高い状態（F−ImH 群）

この群は，情報セキュリティ疲労度は低く，情報セキュリティ対策実施度は高いグループである．この群のような情報セキュリティ疲労度が低い状態（F−群）は，4.2 節で述べたように情報セキュリティ対策への意識が低い状態であるため，情報セキュリティ疲労度が中程度の状態（F0 群）へ移行させる必要があることから，この群は理想状態ではない．

この群に属する回答者（表 4）は 49 名であった．情報セキュリティ疲労度尺度得点（表 5）は平均 21.76 点，標準偏差 3.35 であり，情報セキュリティ対策実施度尺度得点（表 6）は平均 40.31 点，標準偏差 3.53 であった．

この群には，(1) 能動的な行動をとらなくても情報セキュリティ対策が行われている状況に依存しているため，情報セキュリティ対策についての当事者意識が低い状況と，(2) 能動的に情報セキュリティ対策を継続しているものの，面倒さやモチベーションの低下を感じてしまったために当事者意識が下がっている状況のそれぞれがみられる．(1) については，では，「そもそも対策をしなくても，サービスが勝手にやっているのでは？（回答者 ID 71）」のような，情報セキュリティソリューションへの依存による受動的な実施状況がみられたことがあげられる．

また，「PC ではセキュリティソフトを入れたり，対策の情報を確認しているが，スマートフォンはあまり意識を持っていなかった（回答者 ID 63）」，「スマートフォンが普及しはじめて必要とされているがあまり重要視されていないような気がする（回答者 ID 80）」，「スマホにセキュリティ対策ソフトを入れるのは面倒くさい（回答者 ID 174）」のように，スマートフォンの情報セキュリティ対策に言及がみられた．

また，「指紋認証は信用できないと思う（回答者 ID 2）」や「指紋認証の精度が上がれば良いなと思う（水に濡れていたりすると）認証できないときがあるので（回答者 ID 269）」のように，具体的な情報セキュリティ対策実施をあげ，情報セキュリティ対策実施への練度の高さがうかがえた．

最後に (2) については，「とても面倒だと感じるが，怖いので仕方なく行っている（回答者 ID 44）」，「面倒だと感じることも多いですが，必要なことだと思います（回答者 ID 56）」，「面倒だけど大切なことだから一所懸命やったのに，結局問題が起こるとがっかりする（回答者 ID 62）」のように，能動的に実施はしているものの面倒さを訴える回答が多く，特に回答者 ID 62 からは最適な状態（F0ImH 群）であったがモチベーションが低下してしまった結果，当事者意識が低下する状況がみられ，情報セキュリティ疲労度の低下が起こり現在の状態（F−ImH 群）になっている様子もみられることがあげられる．

この群を理想状態に移行させるには，6.2.1 項と同様に情報セキュリティ対策の当事者としての意識を喚起 [8] する教育の実施（対策案 (6)）のほか，情報セキュリティ対策サービスやこれに含まれる指紋認証といった情報セキュリティソリューションの利用だけでは対策は万全ではなく，自身による能動的な対策が必要であることを教育する（対策案 (8)）必要がある．また，情報セキュリティインシデントが発生した後に「がっかり」する傾向に対しては，インシデント発生後にはモチベーションを回復させる内容の教育を実施（対策案 (9)）する必要があるとみられる．たとえば，盗難に遭った PC において記憶領域を暗号化していた場合のように，対策をしておいたことで被害のダメージが小さくできた可能性があることや，対策を実施しないと同じようなインシデントが自分の身に降りかかることがあることを伝える内容が考えられる．なお，スマートフォンの情報セキュリティ対策についてはこの群のみで言及されていたが，どの群においても対策が必要である．

6.3 情報セキュリティ疲労度が高い状態（F+群）の特徴とアセスメント

6.3.1 情報セキュリティ疲労度が高く，実施度が低い状態（F+ImL 群）

この群は，情報セキュリティ疲労度が高く，情報セキュリティ対策実施度が低いグループである．この群に属する回答者は 53 名（表 4）であった．情報セキュリティ疲労度尺度得点（表 5）は平均 40.08 点，標準偏差 5.20 であり，情報セキュリティ対策実施度尺度得点（表 6）は平均 30.34 点，標準偏差 4.39 であった．

この群では，「別に知られて困るような情報はないので，まったくしていない（回答者 ID 264）」のように，自己判断の結果，あえて対策を実施していないという回答や，「セキュリティに対して甘いですか？（回答者 ID 69）」のように，対策を実施していないことへの認識を持ちながら脆弱な状態を維持している回答が得られた．そのほか，「情報セキュリティに対しての対策をあまりしていない．知識がないので対策をしないという考えになってしまう（回答者 ID 249）」のように，情報セキュリティ対策を実施していないことを認識し，自己分析する回答がみられた．

換言すると，確信的に情報セキュリティ対策の実施をおろそかにしている様子がみられたことが，本論文の調査ではこの群において特徴的であった．

そのほか，「無料ソフトを使用しているがライセンスが切れると有料ソフトを買うようにうながすのがうっとうしい（回答者 ID 45）」という感情を示す回答や，「パスワードの保存をすべての媒体でできるようにしてほしい（回答者 ID 248）」という回答のように，実施中の具体的な情報セキュリティ対策への不満や要望がみられた．

この群を理想状態に移行させるには，確信的な情報セキュリティ対策の不実行，つまり，情報セキュリティに対する自信過剰を揺るがす必要がある．これには，標的型攻撃の演習のような，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（対策案 (10)）が有効であると思われる．演習が有効であるとした根拠としては，演習としてでも標的型攻撃を成功させてしまった場合に，自分は被害を発生させないという情報セキュリティ対策への過剰な自信を揺らがせる効果があると思われるため，情報セキュリティに対する自信過剰状態が特徴であるこの群からの移行が期待できることがあげられる．また，この群において特徴的であった，実施中の具体的な情報セキュリティ対策への不満や要望に対して，ヒアリングによってガス抜き（対策案 (11)）を行うことによって，情報セキュリティ疲労度を低減できると考えると同時に 2.2 節に示した関連研究が解明しようとする情報セキュリティ対策行動を行わない具体的な理由を収集することができると思われる．なお，対策案 (11) は本論文の調査においてはこの群および 6.3.2 項に示す “情報セキュリティ疲労度が高く，実施度が高い状態を表す群（F+ImH 群）” に特徴的に現れたが，対策を行わない理由を収集し，そこで回答者の考えていることを改めて調べたうえで適切な対策を提案することで回答者に対策の実施を促すことは，他の群に対しても有効な対策案であるとみられる．

6.3.2 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，情報セキュリティ疲労度が高く，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 4）は 54 名であった．情報セキュリティ疲労度尺度得点（表 5）は平均 41.09 点，標準偏差 6.42 であり，情報セキュリティ対策実施度尺度得点（表 6）は平均 41.00 点，標準偏差 3.72 であった．

この群では，「説明にパソコンに詳しくない人に理解が難しい言葉を用いるのでもっと分かりやすくすべき（回答者 ID 33）」や，「小学生のときに教育を受けていれば良かったと思うことがあった（回答者 ID 182）」，「情報セキュリティはもっと厳しく管理したほうがよい（回答者 ID 212）」のように，情報セキュリティ対策の当事者としての意識の高さや，対策推進に対する提言を示す様子がみられた．

また，「最近はなにかとパスワードなどの設定が多くてしんどい（回答者 ID 25）」のように，疲労感を直接表す「しんどい」という言葉がこの群だけでみられた．

さらに，「適切なセキュリティ対策が分かりにくい．最終的には自己責任になるから，これというセキュリティ対策を教えてもらったり教えるといった友人との共有が困難だと思う（回答者 ID 259）」のように，属人的な対応の難しさを訴え，情報セキュリティ対策の浸透を人間関係に依存させることへの困難さを指摘する回答がみられたことにより，大学側からの情報セキュリティ教育が求められる様子がうかがわれた．

この群を理想状態に移行させるには，疲労感に対するガス抜きとして，情報セキュリティ対策に関するヒアリング（対策案 (11)）が有効であると考える．また，対策に対する意識は高く対策実施度も高いことから，日本の自動車運転免許制度のように情報セキュリティ教育間隔の延伸（対策案 (12)）や，簡易化（対策案 (13)）によって F 群を低下させることが考えられる．また，属人的な対策に限界を感じているため，組織的な教育体制の整備（対策案 (14)）が有効であると考えられる．

6.4 対策案の評価

これまでに示した 14 件の対策案（表 7）について，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，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，ランクの上昇と下降の評価については，改めて言及しない限り前後 1 段階の移動があることを示す．

F0ImL 群（6.1.1 項）の対策である対策案 (1) と対策案 (2) は，情報セキュリティ対策の書面による提示と本人による確認作業である．これらは F 群の変化に対する効果は薄く，Im 群を上昇させる効果があると考える．同じ群の対策である対策案 (3) は，情報セキュリティ対策ソリューションの提供である．これも F 群の変化に対する効果は薄く，Im 群を上昇させる効果があると考えるとみられるが，情報セキュリティソリューションへの依存の結果 F−ImH 群に陥る恐れがあるため，F 群については降下させる可能性も存在する．

理想群である F0ImH 群（6.1.2 項）を維持させる対策である対策案 (4) と対策案 (5) について述べる．対策案 (4) は情報セキュリティに対する知識獲得の要求に応え，より高度な対策の実施を促せることから F 群と Im 群ともに状態を維持できると考える．また，対策案 (5) は現状態を維持させるためのモチベーションの喚起であることから，対策案 (4) と同様に F 群と Im 群ともに状態を維持できると考える．

F−ImL 群（6.2.1 項）の対策である対策案 (6) と対策案 (7) は，教育の実施と対策実施内容の具体化であり，F 群と Im 群ともに上昇させる効果があると考える．また，対策案 (6) は F−ImH 群（6.2.2 項）の対策案でもあるが，この群での対策としては，F 群を上昇させるが，Im 群は最上位であるため変化がないものとした．

同じく F−ImH 群（6.2.2 項）の対策である対策案 (8) と対策案 (9) はそれぞれ注意喚起と教育である．これらは F 群を上昇させ，Im 群は維持させる効果があると考える．

F+ImL 群（6.3.1 項）の対策である対策案 (10) と対策案 (11) について評価する．対策案 (10) は確信的に情報セキュリティ対策をおろそかにしている人に対して，模擬的とはいえインシデントを起こさせる施策であるため，自分の情報セキュリティ対策に対する練度に不安を持つ F0ImL 群へと F 群を降下させると考える．しかし，模擬的に情報セキュリティ被害に遭わされるため，情報セキュリティ疲労度が高い状態である F+群を維持させてしまう効果も考える．一方，Im 群については，演習によって対策への自信が揺るがされるため情報セキュリティ対策実施の必要性を感じて上昇すると考える．対策案 (11) はヒアリングによる不満解消によって情報セキュリティ対策に理解を示し F 群は降下させ，Im 群は上昇させると考える．

最後に F+ImH 群（6.3.2 項）の対策である対策案 (11)，対策案 (12) と対策案 (13) および対策案 (14) について評価する．対策案 (11) は F+ImL 群での同対策案に対する評価と同様に，ヒアリングによる不満解消によって F 群は降下させると考え，また Im 群についてすでに高い状態にあるため変化させないと考える．対策案 (12) と対策案 (13) は情報セキュリティに対して実施を強いられる事項の緩和であるため，F 群を降下させると考える．また Im 群については変化を与えないと考えるが，教育不足から情報セキュリティ対策に自身の練度に不安を持つことで F 群が降下してしまう可能性もあると考える．対策案 (14) は組織的な体制整備により属人性が解消されて F 群を降下させるが，Im 群は変化させないと考える．

6 章冒頭でも述べたように，14 件の対策案および対策の効果は，本論文において実施した質問紙調査の有効回答 337 件のうち自由回答が記された 135 件から演繹的に導出することにより，客観性を担保した．

ここで，F 群と Im 群のそれぞれについて対策効果の評価を述べる．まず F 群は，各群に属する回答者が本研究の成果によるものであるため，先行研究による比較は困難であり，追跡調査による検討が必要であるため今後検討すべき課題である．

それに対して Im 群の対策効果には，(1) ImL 群にあるものが ImL 群のままである，(2) ImL 群にあるものが ImH 群に移行する，(3) ImH 群にあるものが ImL 群に移行する，(4) ImH 群にあるものが ImH 群のままであるという 4 パターンが存在する可能性がある．本研究では，すべての対策について，対策施策を実施した効果が認められるのであれば，ImL 群にある回答者は ImH 群へ移行し（対策効果パターン (2)），ImH 群にある者はその状態を維持する（対策効果パターン (4)）ものとして評価した．そのため，施策を緩和する意味を持つ対策案 (12) および対策案 (13) は，Im 群が 1 段階降下する可能性がある旨の注釈をつけた．

さらに，本研究で現れなかった対策効果パターン (1) と (3) について説明する．ImL 群が ImL 群のまま変化しないこと（対策効果パターン (1)）については，2.2 節であげたように施策を実施しても効果が上がらないことを問題意識とした研究課題となっている．最後に，対策案の実施により ImH 群が ImL 群に低下してしまうこと（対策効果パターン (3)）があるとすれば，対策として望ましくないため，その対策案は見直し対象としてあげることができると考えられる．

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 F0ImH 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る．

6.5 本論文の限界

なお，これらの対策案は今回の調査の結果導出された範囲であるという限界がある．

たとえば，6.3.1 項にあげた F+ImH 群においてみられた確信的に情報セキュリティ対策をおろそかにしている様子のように，セキュリティリスクを理解したうえで情報セキュリティ対策を行っていない様子は本調査から抽出されたが，その反対に，情報セキュリティリスクに対する理解

が不足しているために対策を行っていないことも考えられるためである．これらに対しては．対策案 (1)，(2)，(3)，および (6) といった対策が有効であると考えられる．この限界に対応するための，より大きなサンプルでの調査実施などによる網羅性の追求は今後の検討事項である．

また，またその他の例として，本論文では全回答者を調査結果の分析によって 6 群のいずれかに振り分け，各群に対してアセスメントおよび対策の立案と評価を実施したが，各回答者がかつて所属していた群の履歴による影響は考慮されていないことがあげられる．これは，今回の調査によって得られた自由回答から回答者がかつて所属していた群を考察することは困難であることが理由である．このような同一人物の情報セキュリティ疲労度と情報セキュリティ対策実施度の時系列変化については，検証にあたって同一人物に対する追跡調査が必要となるため，今後検証すべき事項である．

7. おわりに

本研究によって，ICT 利用者の情報セキュリティ対策施策に対する心理状態の可視化が実現され，ICT 利用者の状態に応じた最適な情報セキュリティ対策の実施案が 14 件示され，評価が行われた．

具体的には，情報セキュリティ対策施策の効果が上がらない原因として，ICT 利用者の情報セキュリティ疲れに着目し，情報セキュリティ疲労度と，情報セキュリティ対策実施度それぞれの測定尺度を作成し，質問紙調査を大学生に対して実施した．調査結果に潜在ランク理論を適用し，これらの測定尺度を軸として構成される情報セキュリティコンディションマトリクスによって，ICT 利用者の状態を可視化した．質問紙の自由回答に対するアセスメントによって，情報セキュリティ対策施策に対する ICT 利用者の理想状態を明らかにし，この状態を維持する施策を示した，また，その他の状態についても特徴を明らかにし，理想状態に移行させるための施策を示した．

これらの知見を用いることにより，情報セキュリティ対策施策のパーソナライズ化やオンライン学習によるシステム化の実現が可能と考えるが，環境の構築は今後の課題である．また，今回は萌芽的な研究として大学生を対象としたが，すべての ICT 利用者を対象とした調査を実施し，社会人などの大学生以外の母集団に対しても検討を拡げ，より強固な手法として確立させたい．

本研究の成果によって，情報セキュリティ対策施策のパーソナライズ化が実現可能となり，内部不正や情報漏洩といった情報セキュリティインシデントを抑止し，情報セキュリティ対策の費用対効果を向上させることが期待できる．

謝辞 今回の質問紙調査に協力していただいた千葉工業大学社会システム科学部および法政大学理工学部の皆様，質問紙調査結果のデータ入力をしていただいた千葉工業大学社会システム科学部永井啓太様，植草皓様に謹んで感謝の意を表する．

参考文献

[1] Furnell, S. and Thomson, K.-L.: Recognizing and addressing ‘security fatigue’, *Comput. Fraud Secur.*, Vol.2009, No.11, pp.7–11 (2009).
[2] 広島大学：情報セキュリティ対策，入手先 ⟨https://www.hiroshima-u.ac.jp/about/initiatives/jyoho_ka/ism⟩（参照 2018-02-14）.
[3] 国立情報学研究所：高等教育機関における情報セキュリティポリシー策定について，入手先 ⟨http://www.nii.ac.jp/service/sp/⟩（参照 2018-02-14）.
[4] 日本シーサート協議会：一般会員（チーム）情報，入手先 ⟨http://www.nca.gr.jp/member/index.html⟩（参照 2018-02-14）.
[5] 東京電機大学：大学初！東京電機大学が日本シーサート協議会へ加盟，入手先 ⟨https://www.csirt.dendai.ac.jp/csirt/public/notice/大学初！東京電機大学が日本シーサート協議会へ/⟩（参照 2018-02-14）.
[6] 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).
[7] 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-2, No.30, pp.1–7（オンライン），入手先 ⟨http://id.nii.ac.jp/1001/00182533/⟩ (2017).
[8] 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).
[9] 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).
[10] Parkin, S., Krol, K., Becker, I. and Sasse, M.A.: Applying Cognitive Control Modes to Identify Security Fatigue Hotspots, *12th Symposium on Usable Privacy and Security* (*SOUPS 2016*) (2016).
[11] Reason, J.: Human error, Cambridge University Press (1990)，十亀 洋（翻訳）：ヒューマンエラー［完訳版］，海文堂出版 (2014).
[12] Stanton, B., Theofanos, M.F, Prettyman, S.S. and Furman, S.: Security Fatigue, *IT Prof.*, Vol.18, No.5, pp.26–32 (2016).
[13] 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, pp.2204–2212 (2012).
[14] 菅野泰子，島田裕次：情報セキュリティ対策における阻害要因の構造に関する企業規模別比較研究，日本情報経営学会誌，Vol.30, No.3, pp.109–121 (2010).
[15] Bulgurcu, B., Cavusoglu, H. and Benbasat, I.: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Q*, Vol.34, No.3, pp.523–548 (2010).
[16] Ifinedo, P.: Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition, *Inf. Manag.*, Vol.51, No.1, pp.69–79 (2014).

[17] 久保真人：バーンアウトの心理学，サイエンス社 (2004).
[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 (2009).
[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] Chandran, S., Bardas, A.G., Case, J., Ou, X., Wesch, M., McHugh, J. and Rajagopalan, S.R.: A Human Capital Model for Mitigating Security Analyst Burnout, *Symposium on Usable Privacy and Security*, pp.347–359 (2015).
[21] 増田真也，北岡和代，荻野佳代子：MBI-GS によるバーンアウトの判定基準：疲弊感 +1 基準とニューラルテスト理論による検討，経営行動科学学会年次大会：発表論文集，No.14, pp.471–476 (2011).
[22] Shojima, K.: Neural test theory: A latent rank theory for analyzing test data, *DNC Res. Note*, Vol.8-1 (2008).
[23] 小山由紀恵，木村哲夫：Neural Test Theory を使った Can-do Statements の分析，統計数理研究所共同研究リポート，Vol.254, pp.59–77（オンライン），入手先 ⟨http://presentation.web.nitech.ac.jp/publication/36.pdf⟩（参照 2018-02-22）.
[24] 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）.
[25] 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).
[26] 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).
[27] 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).
[28] 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 (2015).
[29] 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/10threats2016.html⟩（参照 2017-04-21）.
[30] 総務省：テレワークセキュリティガイドライン，入手先 ⟨http://www.soumu.go.jp/main_content/000238665.pdf⟩（参照 2017-02-16）.
[31] 法政大学：情報セキュリティハンドブック，入手先 ⟨http://hic.ws.hosei.ac.jp/cms/wp-content/uploads/securityHandbook_2018-1.pdf⟩（参照 2018-07-02）.
[32] 荘島宏二郎，exametrika，入手先 ⟨http://antlers.rd.dnc.ac.jp/~shojima/exmk/index.htm⟩（参照 2017-04-27）.
[33] 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 1 [9]

あなたは最近 6 カ月ぐらいの間に，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[*1]に ◯ をつけてください.

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

[*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

質問 2 [27]
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思う番号[*2]に ◯ をつけてください．

項番	設問
1	PC やスマートフォンにウィ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をとる
10	見られてはいけないデータを誰でもアクセスできるところに保存しない
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

質問 3
情報セキュリティ対策について，お考えを自由に記述してください．

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．

[*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

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）．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，ネットワークセキュリティの研究開発に従事．2008 年から現在，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．

冨士 仁 （正会員）

1993 年東京理科大学大学院工学研究科修士課程修了．同年日本電信電話（株）入社．情報セキュリティ等の研究に従事．現在，同社セキュアプラットフォーム研究所主席研究員．情報学博士．電子情報通信学会，日本品質管理学会各会員．本会理事．

大久保 一彦

1989 年東京大学大学院工学系研究科修士課程電気工学専攻修了．同年日本電信電話株式会社通信網総合研究所入社．米国 MIT Sloan ビジネススクール（Management of Technology）修了．ネットワークセキュリティおよび情報セキュリティにかかわる研究開発に従事．電子情報通信学会，IEEE 各会員．