千葉工業大学
博士学位論文

インターネット利用者の行動分析研究：
Web ページ関心度,
セキュリティ不安全行動,
セキュリティ疲れ

2023 年 3 月

畑島 隆

目次

第 I 部　序論　10

第 1 章　インターネット利用行動分析の意義　11

第 I 部の参考文献　17

第 II 部　Web ページ関心度（TBI）の研究　18

第 2 章　はじめに　19

第 3 章　関心度（TBI）の開発，特性分析と可視化ツール CyberRanking の開発　21

3.1　関心度（TBI）の開発 22

3.1.1　WWW の商用利用および TV との視聴形態の比較 22

3.1.2　Web サーバへのアクセスログ解析調査 23

3.1.3　Web ページのための視聴度指標の要件 23

3.1.3.1　リアルタイムな視聴度調査が可能であること 23

3.1.3.2　コンテンツ単位の調査分析が行われること 24

3.1.3.3　アクセスの時系列傾向を考慮していること 25

3.2　関心度（TBI）の定義 25

3.2.1　関心度（TBI）算出式の定義 25

3.2.1.1　増加関数の定義 27

3.2.1.2　減衰比関数の定義 27

3.2.1.2.1　概要 27

3.2.1.2.2　情報活用度の低下 28

3.2.1.2.3　陳腐化 28

3.2.1.2.4　関心の減衰 28

3.2.1.2.5 減衰比関数 28
3.2.1.3 減衰比関数の推定 29
3.2.1.4 関心度（TBI）算出式の確定 29
3.2.2 関心度（TBI）算出式の評価 30
3.2.3 関心度（TBI）の NTT DIRECTORY での応用 32
3.2.4 CyberRanking 34
3.2.4.1 概要 34
3.2.4.2 アクセスログ収集動作部 34
3.2.4.3 分析動作部 35
3.2.4.4 視覚化動作部 35
3.3 議論 37
3.3.1 関心度（TBI） 37
3.3.2 CyberRanking 37
3.4 まとめ 38

第 4 章 第 II 部のまとめ 39

第 II 部の参考文献 40

第 III 部 インターネット利用者のセキュリティ不安全行動の研究 42

第 5 章 はじめに 43

第 6 章 テレワークにおける意図しない情報漏洩による不安全行動 44
6.1 序章 44
6.1.1 はじめに 44
6.2 本研究の概要と構成 45
6.3 関連研究と本研究の対象 47
6.4 質問紙設計 49
6.4.1 不安全行動の分類 49
6.4.2 情報セキュリティ不安全行動モデルの選択 50
6.4.2.1 KAB モデルに沿った構成概念検討による質問紙設計 . . 51
6.4.2.2 Knowledge 層 51
6.4.2.3 Attitude 層 52

6.4.2.4 Behavior 層 53
6.5 調査と分析 54
6.5.1 調査の概要 54
6.5.2 回答の概要 54
6.5.3 スクリーニング 54
6.5.4 分析 55
6.5.4.1 テレワーク実施割合の分析 55
6.5.4.2 尺度得点の基本統計量と信頼性 55
6.6 内部不正を意図しない情報漏洩経験の有無によるテレワーク実施者の分析 56
6.6.1 分析手法 56
6.6.2 内部不正を意図しない情報漏洩経験の有無による各尺度得点の平均の差の検定 57
6.7 全体考察 61
6.7.1 考察 61
6.7.2 本研究の優位性 62
6.7.3 本研究の限界 63
6.8 まとめ 64

第 7 章 私有モバイル端末の業務利用におけるセキュリティ不安全行動としてのリスク補償行動 65
7.1 はじめに 65
7.2 概要と構成 65
7.3 関連研究 66
7.4 質問紙 66
7.5 分析 67
7.5.1 回答者の分類（Q3） 67
7.5.2 業務データを保存している場所 68
7.5.3 私用モバイル端末の許可状態別業務利用形態（Q3) と業務データ取り扱い状況（Q5) の関係分析 69
7.5.3.1 カイ二乗検定 69
7.5.3.2 業務許可形態（Q3) と業務データ取り扱い状況（Q5) の残差分析 70
7.6 考察と議論 75

7.6.1 規約の通りに私有モバイル端末を業務利用する人：Q3(1) 75
7.6.2 規約があるが自分の判断で私有モバイル端末を業務利用する人：Q3(2) 76
7.6.3 規約が無いので自分の判断で私有モバイル端末を業務利用する人：Q3(3) 77
7.7 まとめ 77

第 8 章 第 III 部のまとめ 79

第 III 部の付録 81
III-1 第 6 章の質問紙 81
III-2 第 7 章の質問紙 87

第 III 部の参考文献 90

第 IV 部 セキュリティ疲れの研究 94

第 9 章 はじめに 95

第 10 章 セキュリティ疲労度測定尺度の開発 98
10.1 セキュリティ疲れの定義 98
10.1.1 先行研究におけるセキュリティ疲れの定義 98
10.1.2 本研究でのセキュリティ疲れの定義 99
10.2 セキュリティ疲労度測定尺度開発の概要 99
10.2.1 セキュリティ疲労度測定尺度 SFS-13 および SFS-9 99
10.2.2 一般的なバーンアウトとその測定尺度 100
10.2.2.1 バーンアウト（燃え尽き症候群） 100
10.2.2.2 Maslach らによるバーンアウト尺度（MBI-HSS，MBI-ES，MBI-GS） 100
10.2.2.2.1 ヒューマン・サービスにおけるバーンアウト (MBI-HSS，MBI-ES) 101
10.2.2.2.2 全ての職業に対するバーンアウト (MBI-GS) 101
10.2.2.3 (日本版) バーンアウト尺度 101

10.2.2.4 バーンアウトメジャー 101
10.2.3 情報セキュリティに対するバーンアウトの研究 101
10.2.4 一般的なバーンアウトと情報セキュリティ疲れに対するバーンアウトとの差異 102
10.2.5 バーンアウト段階説と潜在ランク理論 102
10.2.5.1 バーンアウト段階説 102
10.2.5.2 潜在ランク理論 105
10.2.6 その他の情報セキュリティに関する測定尺度研究と本研究の関係 . 105
10.3 大学生版セキュリティ疲労度測定尺度 SFS-13 開発の予備調査：セキュリティ疲れの段階別特徴 108
10.3.1 SFS-13 開発手順（予備調査，本調査，確認調査） 108
10.3.2 質問項目の検討と予備調査版質問紙の作成 109
10.3.3 予備調査の実施 114
10.3.4 予備調査結果の検討 114
10.3.5 セキュリティ疲労度の段階別性質 115
10.3.5.1 セキュリティ疲労度の潜在ランク理論による可視化 . . . 115
10.3.5.1.1 セキュリティ疲労度 1 (疲労度レベル“– –”)117
10.3.5.1.2 セキュリティ疲労度 2 (疲労度レベル “–”) 117
10.3.5.1.3 セキュリティ疲労度 3 (疲労度レベル“0”) 118
10.3.5.1.4 セキュリティ疲労度 4 (疲労度レベル“+”) 118
10.3.5.1.5 セキュリティ疲労度 5 (疲労度レベル“+ +”) 118
10.4 大学生版セキュリティ疲労度測定尺度 SFS-13 の開発 119
10.4.1 SFS-13 開発のための本調査 119
10.4.2 SFS-13 確定本調査結果の分析 119
10.4.3 得られた因子構造に対する信頼性と妥当性の検討による SFS-13 の確定 122
10.4.4 SFS-13 確定後の確認調査 125
10.4.4.1 確認調査 125
10.4.4.2 確認調査結果の分析 125
10.4.5 情報セキュリティ疲労度測定尺度の利用方法 127
10.4.6 考察 128
10.4.6.1 SFS-13 開発研究に関する考察 128
10.4.6.2 本研究の限界点 129

10.5 SFS-13 開発研究のまとめ 129
10.6 汎用版セキュリティ疲労度測定尺度（SFS-9）の開発 131
10.6.1 測定尺度開発行程と質問紙調査 131
10.6.1.1 測定尺度開発工程 131
10.6.1.2 質問紙調査 131
10.6.1.2.1 調査の概要 131
10.6.1.2.2 質問紙の構成 132
10.6.2 汎用版セキュリティ疲労度測定尺度 SFS-9 の開発 133
10.6.2.1 SFS-9 の因子構造 133
10.6.2.2 因子分析 134
10.6.2.3 因子の命名 135
10.6.3 信頼性の検討 136
10.6.4 妥当性の検討 136
10.6.4.1 内容的妥当性 136
10.6.4.2 基準関連妥当性 136
10.6.4.2.1 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の連関 . . . 137
10.6.4.2.2 セキュリティ疲労度の自己申告結果とセキュリティ疲労度測定結果の連関 138
10.6.5 構成概念妥当性 139
10.6.6 SFS-9 の大学生への適用 140
10.6.7 汎用版情報セキュリティ疲労度測定尺度 SFS-9 の確定 140
10.6.8 考察 141
10.6.8.1 因子構造 141
10.6.8.2 信頼性の検討 142
10.6.8.3 妥当性の検討 142
10.6.8.3.1 基準関連妥当性 142
10.6.8.3.2 構成概念妥当性 142
10.6.8.3.3 大学生への適用 142
10.6.9 SFS-9 の利用例 143
10.6.9.1 バックグラウンドファクタによる差異 143
10.6.9.1.1 平均の差の検定結果 143

10.6.9.1.2 バックグラウンドファクタによる差異に関する考察 143
10.6.10 SFS-9 開発研究の限界 145
10.7 SFS-9 開発研究のまとめ 145
10.8 セキュリティ疲労度測定尺度開発研究のまとめ 145

第 11 章 セキュリティ疲労度測定尺度の応用 147
11.1 セキュリティコンディションマトリクスの提案 149
11.1.1 セキュリティコンディションマトリクスの仮説 149
11.1.2 セキュリティコンディションマトリクスの検証 153
11.1.2.1 質問紙の作成 153
11.1.2.1.1 セキュリティ疲労度測定尺度 153
11.1.2.1.2 セキュリティ対策実施度 153
11.1.2.1.3 セキュリティ対策に関する個人の所感 . . . 154
11.1.2.2 質問紙調査の実施 154
11.1.2.3 セキュリティコンディションマトリクスへの回答者の割付 154
11.1.3 改善型セキュリティコンディションマトリクスに基づくリスクアセスメント 158
11.1.3.1 セキュリティ疲労度 F0 の群 158
11.1.3.1.1 F0ImL 群 158
11.1.3.1.2 F0ImH 群 159
11.1.3.2 セキュリティ疲労度 F–の群 160
11.1.3.2.1 F–ImL 群 160
11.1.3.2.2 F–ImH 群 160
11.1.3.3 セキュリティ疲労度 F+ の群 162
11.1.3.3.1 F+ImL 群 162
11.1.3.3.2 F+ImH 群 163
11.1.4 リスクアセスメント結果の机上評価 164
11.1.5 本研究の限界 166
11.1.6 おわりに 166
11.2 認知的方略を用いたセキュリティコンディションマトリクス細分化によるセキュリティ疲労対策アセスメントの詳細化 167

11.2.1 概要 167
11.2.2 認知的方略 167
11.2.3 質問紙調査 168
11.2.4 分析 169
11.2.5 認知的方略で分割した各群の考察 169
11.2.5.1 LM 群（メタ認知低群） 169
11.2.5.2 RP 群（悲観主義群） 170
11.2.5.3 DP 群（防衛的悲観主義群） 170
11.2.5.4 RO 群（楽観主義群） 170
11.2.6 まとめ 170
11.3 内部不正に対するセキュリティ疲労度測定尺度の貢献 171
11.3.1 概要 171
11.3.2 内部不正のリスク要因と対策 171
11.3.3 セキュリティコンディションマトリクスによる内部不正が発生しうる人的側面の可視化 172
11.3.4 内部不正におけるリスク項目と対策案 173
11.3.4.1 リスク項目の抽出 173
11.3.4.2 リスク要因に対する対策方針検討 174
11.3.4.3 リスク対策方針に対する SFS-13 の貢献度の机上評価 . . 174
11.3.5 まとめ 175
11.4 セキュリティ疲労度測定尺度の応用研究のまとめ 175

第 12 章 第 IV 部のまとめ 177

第 IV 部の参考文献 178

第 IV 部の付録 184

IV-1 第 10 章の質問紙（SFS-13 開発） 184
IV-2 第 10 章の質問紙（SFS-9 開発） 186
IV-3 大学生版セキュリティ疲労度測定尺度 SFS-13 188
IV-4 セキュリティ疲労度測定尺度 SFS-9 189
IV-5 第 11 章の質問紙（セキュリティコンディションマトリクス開発） 190
IV-6 外山の認知的方略測定尺度 [外山 2015] 193

第 V 部　結論　194

第 13 章　結論　195

第Ⅰ部

序論

第 1 章

インターネット利用行動分析の意義

学術や軍事を目的としない情報流通やコミュニケーションの手段としてのインターネットは国内では 1990 年代後半から普及が始まり，2020 年代である現代では社会基盤として不可欠である．本研究はインターネットを日常利用する人間の行動分析による研究を 3 つの観点から実施したものである．3 つの観点とは，Web ページへの関心の現れとしての情報選択行動，私有端末を用いたリモートワークやテレワーク時につい行われる従業員による不安全行動，そして求められるセキュリティ対策行動に疲弊し正しく実施が出来なくなるセキュリティ疲労である．これら研究によって，インターネット利用者にとってより快適なサービスや，よりセキュアな利用環境を構築に貢献するものである．

本研究と関連する 1994 年以降のインターネットの年表と本研究の実施時期を示した図 1.1 に従って研究内容を述べる．国内では，インターネットの商用利用は雑誌インターネットマガジンの創刊やベッコアメ・インターネットなどの個人向けインターネットサービスプロバイダの創業があった 1994 年頃から始まったとみられる．これによりインターネットを用いた情報流通が一般的に行われるようになり，電子メールや WWW(World Wide Web) が一般に用いられるようになった．WWW では企業や個人による Web ページが多数作成されたことから，1995 年 12 月に開設された NTT DIRECTORY[NTT DIRECTORY1995]，1998 年に創立された Google のような Web ページ検索サービスが開始された．

第 Ⅱ 部では，この時期に実施した Web ページへのアクセス行動を分析しアクセス傾向の測定指標を開発する研究について述べた．具体的には，インターネット利用者が Web サーバ上のどのページに関心を寄せているかを示す指標である関心度（TBI: Time-Based Interest）の算出方法を開発した．そして TBI を NTT DIRECTORY に結果表示順の一つとして実装 [NTT DIRECTORY1998] した．これによりインターネット上の大部分の Web

ページが TBI の算出対象となったため，TBI は当該ページへのアクセス傾向をもとにインターネットユーザ全体の視聴度合いを推定する指標として機能した．TBI は単純に TBI の値を増加させる関数と，演繹的に設定したアクセスとアクセスの時間間隔に応じて TBI の値を減衰させる指数関数により構成され，TBI を減衰させる関数で用いられる減衰定数は NTT DIRECTORY の実サービスログの分析により導出した．

また，本研究の第 Ⅲ 部と第 Ⅳ 部の研究では，情報セキュリティについて人間の行動面や心理面から研究する，セキュリティ心理学に係わる研究を行った．セキュリティ心理学の国内の研究コミュニティとしては 2008 年に情報処理学会 SPT 研究グループとして発足され，2012 年に現名称となった情報処理学会セキュリティ心理学とトラスト (SPT) 研究会 [SPT] などが知られている．

第 Ⅲ 部では，テレワークや私有端末の業務利用（BYOD: Bring Your Own Device）におけるセキュリティ不安全行動 (unsafe act) の研究を実施した．ネットワークの高度化，および，ノート PC の普及や 2008 年の iPhone3G の国内販売開始にみられる情報端末の小型化により，オフィス以外の場所から業務を実施する支給された業務端末によるテレワークや BYOD が実用的になり，2011 年の東日本大震災や 2019 年の働き方改革，そして 2020 からの感染症拡大といった事象を背景として普及が進んだ．普及に従い要求が高まる情報セキュリティについては，2004 年に総務省からテレワークセキュリティガイドラインの初版が発行され，その後 2021 年に第 5 版が発行されたような啓蒙が行われてきた [総務省テレワーク]．

不安全行動は，安全マニュアル違反や明確な違反行為でなくてもインシデント発生のリスクを高める行為である [芳賀 2007]．情報セキュリティ分野においてもこのようなインターネット利用の不安全行動は存在すると考える．本研究では，まず，テレワーク時のセキュリティ不安全行動のうち意図しない情報漏洩について，インシデントを発生させやすいテレワーカーの性向に特徴があることを示した．そして，規約の整備状況および許可状況，そしてと BYOD ユーザの業務実施状況というそれぞれ観点を組み合わせた分析によって，セキュリティ不安全行動がリスク補償行動によって説明可能であることを示した．前者の研究では，(1) 確信的に敢行してしまう性向を抑止する施策が効果的，(2) テレワークに関する情報セキュリティ対策であっても，従業員が所属する職場のセキュリティ環境を危険度の低い状態にする施策が有効，(3) 情報セキュリティ対策の実施を促す施策に一定の効果があることは論を待たないが，本研究では有意な差は見られず，対策効果に個人差があることが示唆されるという 3 点の知見が得られた．後者の研究では，会社の規約に従って BYOD を実施する人はルールや規則に従っていることでセキュリティ事故のリスクを低く見積り，個人に関する情報のような機微な業務データをセキュリティリスク

の高い場所に保存するといったセキュリティインシデントリスクの高い業務行動する傾向がみられるという知見が得られた.

最後に，第 Ⅳ 部では，高度化し複雑化するばかりのセキュリティ対策に対してインターネット利用者が疲弊し，セキュリティ対策を実施施策の効果が上がらなくなるセキュリティ疲れ (Security Fatigue) について研究した．セキュリティ疲れの研究は，2016 年に国際会議 SOUPS2016(Twelfth Symposium On Usable Privacy and Security Workshop) でワークショップが行われた [SOUPS2016] ことから注目を集め始めた.

本研究では，セキュリティ疲労度の測定尺度の開発，セキュリティ疲労度とセキュリティ対策実施度を組み合わせたセキュリティコンディションマトリクスの開発を行った．セキュリティ疲労度測定尺度は，一般的な燃え尽き症候群 (バーンアウト) の測定手法の援用により開発した．開発は，セキュリティ対策に疲弊したインターネット利用者が「セキュリティ疲れ状態」となり，この状態が進行することで情報セキュリティ対策を実施しなくなる状態を「セキュリティバーンアウト状態」と仮説することにより進めた．質問紙調査をもとに大学生版測定尺度 SFS-13(Security Fatigue Scale-13）および汎用版測定尺度 SFS-9 について信頼性と妥当性の検討を行うとともに，セキュリティについての所感を自由回答形式で求めた結果の分析から，セキュリティ疲労度は低すぎても高すぎても好ましくなく，中程度であるときに適度な緊張感を持ってセキュリティ対策を行っている理想状態であるという，セキュリティ疲労度測定尺度の性質を示した．また，セキュリティコンディションマトリクスを提案し，セキュリティ対策に対するインターネット利用者の理想状態であるのは，セキュリティ対策に対して適度な緊張感を持ち，かつ，セキュリティ対策を実施している状態であると定義した．このセキュリティコンディションマトリクスを用いたリスクアセスメントとして，理想状態で状態を維持するための対策および理想状態以外の各状態から理想状態に近づけるための対策をそれぞれ示した.

人間の行動データの取得方法は多様に存在するが，自然科学的なアプローチと社会科学的なアプローチという分類法で分けることができると考える．自然科学的なアプローチはさらにログ取得と行動の解析といった分類ができる．ログ取得では行動の対象となる機械や情報システムに記録されるログを分析対象データとし，行動解析では行動をセンサーで記録して得られたデータを利用し，行動の様子そのものを記録し解析した結果をデータとして利用する．一方，社会科学的なアプローチにも様々な分類法があるが，心理学で用いられるデータの収集方法による分類である調査法，面接法，観察法，実験法が挙げられる [磯崎 2020]．本研究の第 Ⅱ 部では自然科学的なアプローチを用い，利用者の行動の結果として Web サーバに記録される検索ログやアクセスログを分析した．そして第 Ⅲ 部および第 Ⅳ 部では社会科学的なアプローチを用い，質問紙による調査結果の分析を行った.

これらの研究結果によってインターネット利用行動が測定可能となれば，測定可能となった行動にそれぞれに対応した定量的な指標や活動指針が得られる．この指標や活動指針を基準として，有益なサービス開発や，よりよい利用環境を提供するための技術開発，より安心安全にインターネットを利用するための規約の整備の実施が可能となる．

本研究の構成を図 1.2 に示す．第 I 部では序論を述べた．第 Ⅱ 部では，**2** で概要を示し，**3** で TBI（Time-Based-Interest：関心度）と呼ぶ，Web ページに対する関心の度合いを測定するインターネット視聴度指数の開発を行い，開発当時日本最大級であった Web ページ検索サービス NTT DIRECTORY の利用行動をもとにした TBI の性質の考察，および NTT DIRECTORY での TBI 順によるコンテンツ表示サービスの提供 [NTT DIRECTORY1998] を行った．そして **4** でまとめた．第 Ⅲ 部では，インターネット利用者による不安全行動の研究を質問紙調査により行った．まず，**5** で概要を示し，**6** でテレワークにおいて意図せず情報漏洩を行ってしまった人の性格や行動を各種測定尺度による質問紙調査により観測し，意図せず情報漏洩をしたことがないと回答した人と統計的に有意な差がみられる測定尺度があることを示した．次に **7** で私有モバイル端末を業務利用する人について，利用規約の整備状況及び利用許可状況によって業務データの利用傾向に統計的に有意な差がみられることを示した．そして **8** でまとめた．第 Ⅳ 部では，**9** で概要を示したあと，**10** でインターネット利用者がセキュリティ対策の実施に疲労している状態を測定する尺度であるセキュリティ疲労度測定尺度：SFS（Security Fatigue Scale）の開発および尺度得点に応じた疲労状態のモデル化を，質問紙調査により行った．さらに **11** で測定尺度を用いたセキュリティリスクアセスメントの応用研究を，質問紙調査及びリスクアセスメント手法を用いて行い，セキュリティ疲労度測定尺度の有効性を示した．そして **12** でまとめた．第 V 部では結論を述べた．

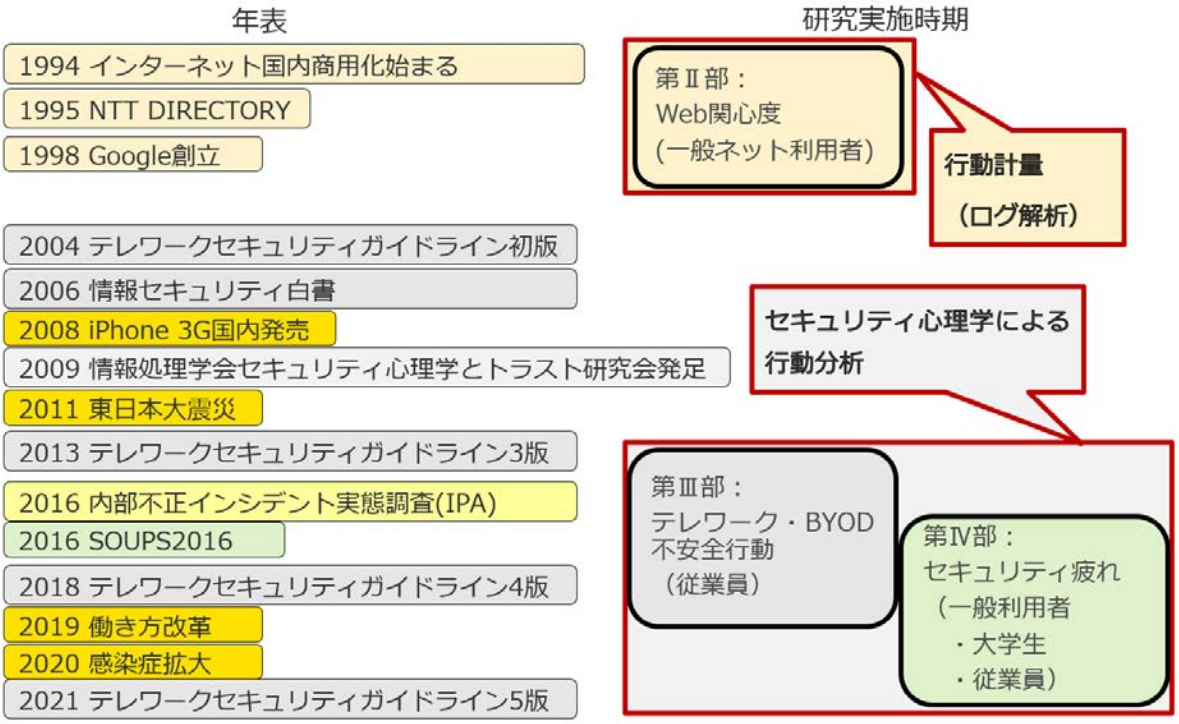

図 1.1　本研究に係わる年表と各部で述べた研究の実施時期

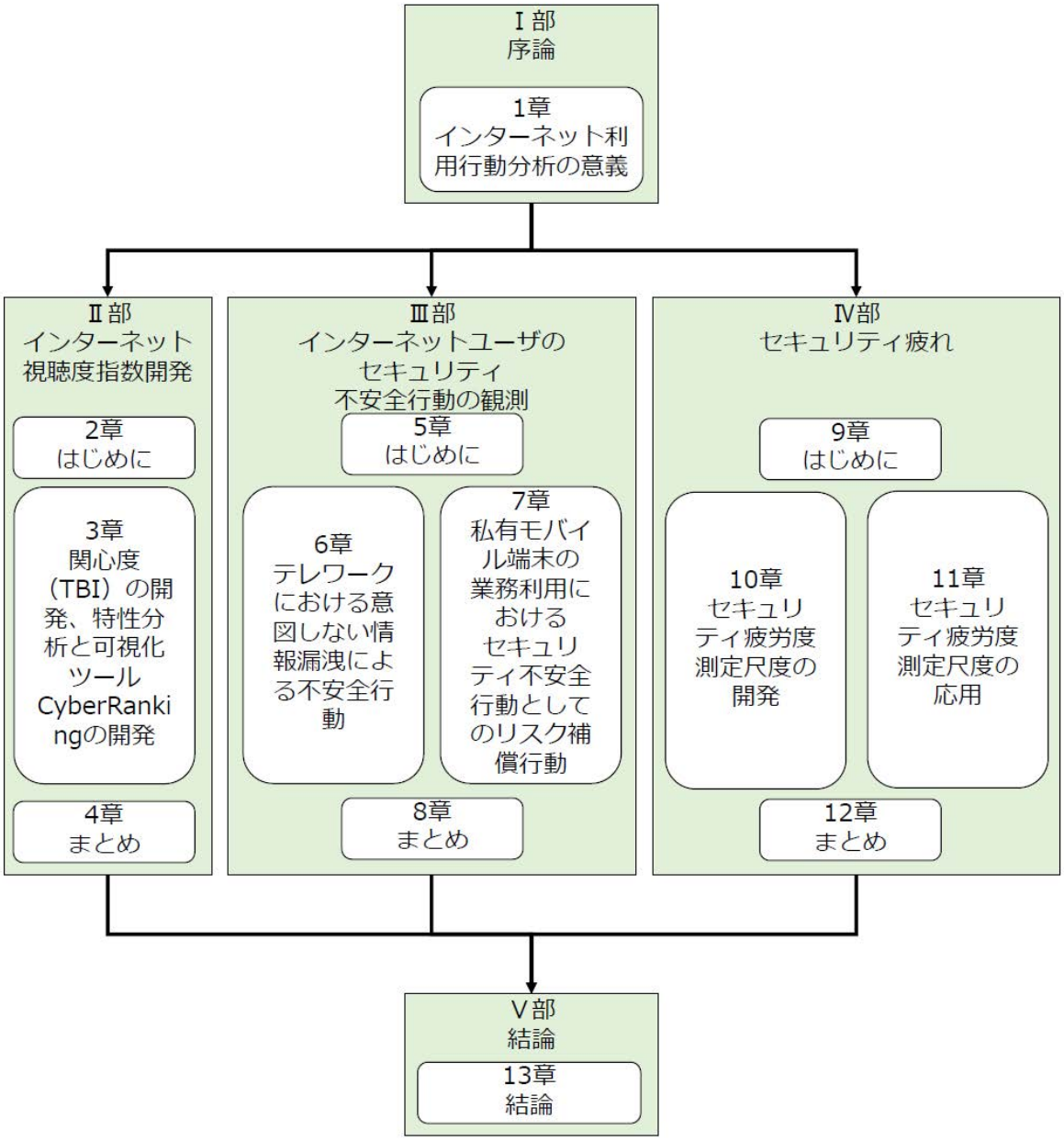

図 1.2　本研究の全体構成

第 I 部の参考文献

[磯崎 2020] 磯崎 三喜年，森島 泰則，西村 馨，直井 望，荻本 快, 現代心理学入門, ナカニシヤ出版 (2020).

[総務省テレワーク] sloppy 総務省，テレワークにおけるセキュリティ確保，参照先〈https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/〉（参照 2023-01-08）.

[NTT DIRECTORY1995] NTT 技術資料館資料，NTT DIRECTORY, 参照先〈https://hct.lab.gvm-jp.groupis-ex.ntt/panel/pdf/C-2-6.pdf〉（参照 2022-12-13）.

[NTT DIRECTORY1998] Internet Watch, ユーザーの「関心度」でサイトを評価「Super NTT DIRECTORY」実験版公開，インプレス，参照先〈https://internet.watch.impress.co.jp/www/article/980702/nttdir.htm〉（1998）（ 参照 2022-12-13）.

[SOUPS2016] Twelfth Symposium On Usable Privacy and Security Workshop, 参照先〈https://www.usenix.org/conference/soups2016〉（参照 2023-01-08）.

[SPT] 情報処理学会セキュリティ心理学とトラスト (SPT) 研究会， 参照先〈https://www.iwsec.org/spt/〉（参照 2023-01-08）.

第 II 部

Web ページ関心度（TBI）の研究

第 2 章

はじめに

インターネットの国内商用利用の黎明期である 1995 年から 2000 年にかけて，インターネット上に多数存在する Web ページに対する視聴率を模した指標として，当該ページへのアクセス傾向をもとにインターネットユーザ全体の視聴度合いを推定する指標 TBI（Time-Based Interest，日本語では関心度）の開発，および，TBI を始めとしたアクセスログ傾向を表示するツールの CyberRanking の開発や，TBI の検索サービスへの提供を行った [畑島 1996][畑島 1997][畑島 2000].

インターネットの商用利用が進むにつれて，WWW(World Wide Web) サイトや Web ページ開設の費用対効果やアクセス頻度の数値化が求められるようになった．Web サーバーのアクセスログからは，Page View（Web ページの閲覧回数），Visit（Web ページの閲覧時間，タイムアウト時間），ユーザのアクセス経路などの指標を抽出することが可能であり，当時これらの指標は，One to One マーケティングや Web サイトのパーソナライズなどに利用されていた．しかし，これらの指標は，アクセスの時間的集中度合いを考慮していないため，Web ページにユーザが興味を寄せている度合いをリアルタイムに判断するのには不十分であった．当時の検索サービス（例：Yahoo![Yahoo]），サイトランキング（例：100hot.com [100hot]），パーソナライズ（例：MyYahoo！ [MyYahoo]）などのサービスでも，アクセスの時間的集中度合いは使用されていなかったため，ユーザがどの程度そのページに興味をもっているかをリアルタイムに知ることは困難であった.

本研究では，アクセスログの情報（アクセス先 URL と当該 URL へのアクセスの時間間隔）を利用したウェブページの視聴度指標 TBI を開発し，TBI をディレクトリサービスに適用してその有用性を評価した．さらに，TBI や当時用いられていた指標を算出可能なアクセスログ解析システム CyberRanking を開発した．CyberRanking は分析対象の Web サーバのアクセスログを CyberRanking サーバに転送して分析を実行し，クライアントの

Web ブラウザで 2 次元あるいは 3 次元のグラフで表示するツールである.

第 3 章

関心度（TBI）の開発，特性分析と可視化ツール CyberRanking の開発

1995 年から 2000 年にかけて，インターネット上に多数存在する Web ページに対する視聴率を模した指標として，当該ページへのアクセス傾向をもとにインターネットユーザ全体の Web ページに対する関心度（TBI:Time-Based Interest）の開発を行った [畑島 1996][畑島 1997][畑島 2000]．関心度を，ページへのアクセス数を刺激として関心度を増加させる関数と，時間経過に伴い関心度を減衰させる関数の組み合わせであると定義した．後述するように，TBI は測定対象の Web ページに対する Web サーバアクセスログの時系列傾向を考慮し，当該 Web ページへのアクセス履歴を時間関数により得点化したものである．

本研究では，時間変化に伴い TBI を減衰させる関数のパラメータを，研究当時日本のインターネットで有数の規模であった Web ページ検索サイト NTT DIRECTORY[NTT DIRECTORY1995] の検索ログを用い，特定のイベントに対する興味の減衰度合いを算出することにより導出した．さらに本研究では，得られた TBI 算出式を用いて 2 件の応用開発を行った．その結果，NTT DIRECTORY が収集した Web ページの TBI を算出し，TBI の順位と度数が Zipf の法則 [Zipf1949] に従うことが判った．そして，実サービスで検索結果の表示順の一つとして NTT DIRECTORY でサービス提供 [NTT DIRECTORY1998] した結果，TBI 順が一番多く使われていたことを示した．

また，本研究ではアクセスログ解析システム CyberRanking を開発した．CyberRanking は Web サーバのアクセスログを解析し，Web ブラウザ上で 2 次元あるいは 3 次元のグラフで表示するツールである．

3.1　関心度（TBI）の開発

3.1.1　WWW の商用利用および TV との視聴形態の比較

関心度（TBI）の研究開発を開始した当時は学術や軍事を目的としないインターネット利用の黎明期であったが，その普及においては電子メールや WWW(World Wide Web) を利用した形での商用利用が企業を中心に始まろうとしていた．WWW の利用形態は企業による自身の企業案内や製品紹介といった自社の広告や営業の媒体としてだけでなく，自社のページの空きスペースを他社の広告スペースとして貸し出す形態である広告事業，当時電子モールと呼ばれていたオンラインショッピングサイトなど，多岐に渡ろうとしていた．

企業が商業活動として Web サイトを設置する場合費用対効果の検討が求められ，その手段としてアクセスログ解析が行われていた．当時のアクセスログ解析ではどれだけ見られたかの度数（Web ページに対しては PageView とも呼ばれた）の算出が基本であり，詳細分析として，地域やユーザ属性ごとにアクセス頻度を人口統計学的に解析されているのみであった．これは，当時の TV 視聴率調査をそのまま Web ページの視聴度調査に援用したものと思われる．しかし，Web ページと TV ではメディアの性質が異なる．当時の Web ページは静的コンテンツがほとんどであったため，検索結果などに記載されたハイパーリンクを踏む，ブックマークをクリックするなど，能動的にアクセス行動を起こさないと閲覧が出来なかった．一方 TV は，ながら見と呼ばれる視聴行動が代表的なように，一旦アクセスすればその後行動を起こさなくても時間が経てば次の番組コンテンツが閲覧可能となるような視聴形態もある情報提供方式である．当時の Web ページのアクセス状況の解析では，一定時間当たりの当該ページへのアクセス数を評価指標としていた．これは，コンテンツ（番組）へのアクセス数と調査世帯数から導出される TV 視聴率調査と同様の手法であると考えられる．しかし，前述のように Web ページと TV ではメディアの性質が異なるため，従来の手法では Web ページへのアクセスによって発生する Web ページの視聴度を表現できるとは言えないと考えた．

この研究では，Web ページに対するインターネット視聴行動計測手法を確立するために必要となる事項を検討したのち，当該ページへのアクセス傾向をもとに，当該ページのインターネットユーザ全体の視聴度合いを推定する指標である Web ページに対する関心度（TBI）の開発について述べる．

3.1.2 Web サーバへのアクセスログ解析調査

Web サーバに残されるアクセスログには，当該サーバ上のそれぞれの Web ページについて，いつ，どこからアクセスされたかを記録している．このため，アクセスログからは Web サーバの利用状況を知ることが出来ると同時に，アクセスしてきたインターネットユーザがどのようなことに関心があるかを知ることが出来る．

アクセス数を調査する際には，同一ユーザからの同一ページへの複数アクセスをどのようにカウントするかが問題となる．当時存在した Internet Profile Corporation[IPC] の I/PRO サービスのうち I/COUNT サービスでは，Web サーバログを同社に転送し，1 日当たりのアクセス頻度をドメイン別に集計したものをサービス提供していた．このサービスでは，同一ファイルへの閲覧リクエストのうち一定時間以上のアイドルタイムを開けた跡に検出されたものを Visits という名称で指標化していた．同様に NetCount[NC]，WEB Counter[WC] といったサービスも提供されていたが，いずれも 1 日間や 1 週間のような一定期間におけるアクセス数を指標としていた．

3.1.3 Web ページのための視聴度指標の要件

ここでは Web ページに対する従来の視聴度調査指標の問題点を述べ，Web ページのメディアとしての性質を TV との比較により説明し，提案の根拠を述べる．表 3.1 は **3.1.1** と **3.1.2** で述べた TV の視聴率調査と，従来の Web サーバの利用動向調査の比較である．

3.1.3.1 リアルタイムな視聴度調査が可能であること

研究対象とした NTT DIRECTORY は検索サービスであることから，興味の移り変わりの早い Web コンテンツに対してリアルタイムに動向を把握し，利用者の関心が高い情報を提供することが利用者にとって有益であると考えた．

従来の調査手法では，いずれもアクセスログに含まれている時間単位の頻度変化が平準化されている．例えば，一定時間のアクセス頻度 1 日当たりの Web ページアクセス数として指標化して算出しており，これは 1 分単位や番組単位などの一定時間の視聴頻度を指数化する TV の平均視聴率と同様の方式であると考えられる．表 3.1 に従って TV に対する調査手法と従来の Web ページに対する調査手法の差異を考察する．コンテンツの性質から，TV であれば番組がひとつの単位でありこれは放送枠という時間で区切られている一方，従来の Web ページ調査では，コンテンツは Web ページ単位であった（研究当時

表 3.1　TV と Web ページの視聴度分析手法の比較

	TV （平均視聴率）	従来の Web ページ	Web ページに 対する 開発手法
コンテンツ	番組	ページ	ページ
指標算出の 時間区切り	番組単位	一定の算出 期間単位	なし (重みの時間 減衰あり)
ログが持つ情報	視聴番組と 視聴時間	アクセス先と アクセス時刻	アクセス先と アクセス時刻
指標の性質	時間単位の 平均視聴数	時間単位の アクセス数	時系列を 考慮
ログ分析タイミング	1 日など 区分単位終了時	1 日など 区分単位終了時	リアルタイム 算出可能

は動的な Web ページの存在は見られなかった）．つまり，TV には番組枠がありひとつの番組は決められた時間に決められた長さで放送される一方，Web ページには Web サーバから削除されない限りコンテンツ提供時間に区切りは無い．ログが持つ情報については，TV であれば視聴番組（もしくは視聴チャンネル）と視聴時間が記録されるのに対して，Web ページではアクセス先の Web ページの URL とアクセス時刻が記録される．指標の性質については，TV の平均視聴率は時間で区切られた範囲での平均視聴者数であり，従来の Web ページでは時間単位のアクセス数であると言える．ログ分析のタイミングについては，TV は 1 日などの区分単位が終了した後に算出され，これは従来の Web ページでも同様である．

3.1.3.2　コンテンツ単位の調査分析が行われること

コンテンツ単位の調査分析が行われることは従来の指標算出方法も同様である．TV ではどれだけの時間そのチャンネルを選択していたかを計測可能であるのに対して，Web ページの場合は Web ページが格納されている Web サーバにアクセスした時刻はログから知ることが出来るが，いつまで見ていたかを知ることは困難である．従って，視聴度の算出に当たっては，当時の技術では Web ページを開いている時間を知ることは難しかったため時間単位での区切ることを避け，コンテンツ（Web ページ）単位であるべきと考えた．

3.1.3.3　アクセスの時系列傾向を考慮していること

アクセスの時系列傾向を考慮していることは TBI の特徴である．Web においてユーザによるアクセスが持つ意味を，TV の場合のザッピングと同様に Web でも様々なページに短時間でアクセスして回るネットサーフィンを例として考察する．当時の TV 放送で選択可能なチャンネル数は高々 10 程度であった．一方で Web では当時でも世界中に数千万件以上に及ぶコンテンツにアクセス可能であった．

また，Web ページに対するユーザのアクセス行動は，TV のチャンネル選択と較べて，より能動的なアクセスであると考えられる．これは，Web でコンテンツにアクセスするためには特定の URL をそれら膨大なコンテンツの中から指定する必要があることから言えると考えた．換言すると，Web ページに対するユーザのアクセス行動は，その Web ページへの関心の表れであるから，関心の集まり度合いを評価するためには，一定時間のアクセス数よりも，個々の Web ページへのアクセス傾向の時系列情報を考慮すべきであると考えた．具体的には，関心度測定対象の Web ページへのアクセスの時間間隔を考慮すべきと考えた．

3.2　関心度（TBI）の定義

関心度（TBI）の定義を行う．**3.1.3.3** で述べたように，TBI は測定対象の Web ページに対する Web サーバアクセスログの時系列傾向を考慮し，当該 Web ページへのアクセス履歴を時間関数により得点化したものである．TBI は **3.2.1** に後述するように， 当該ページに対するアクセス時の TBI 値は時間をパラメータとする下記の関数からなる算出式により構成されると定義した．その性質として当該ページに対するアクセスが集中すると TBI の値は高くなり，アクセスの間隔が空くと TBI は減衰していくことと定義した．

1. 当該ページへのアクセスにより作用する増加関数
2. 当該ページへのアクセス間隔をパラメータとする減衰比関数

3.2.1　関心度（TBI）算出式の定義

TBI を算出する式 F_n を，アクセス発生による TBI の増加と時間経過による TBI の減衰から構成されるとして式 3.1 のように定義した．

$$F_n = g(\delta t) + h(\delta t)F_{n-1} \tag{3.1}$$

ここで，n はページへの関心度算出開始以降のアクセス数，t は時間，$g(\delta t)$ は TBI 増加関数，$h(\delta t)$ は TBI 減衰比関数，δt は $n-1$ 番目と n 番目のアクセスの間の時間間隔 ($\delta t = t_n - t_{n-1}$) である．

なお，アクセスがない期間の，時刻 t における $F(t)$ は式 3.2 で与えられる．

$$F(t) = h(\delta t)F_n \tag{3.2}$$

ここで，$\delta t = t - t_{n-1}$, t はアクセス間の時刻 ($t_n < t < t_{n+1}$), δt は最後にそのページにアクセス してからの経過時間 ($\delta t = t_n - t_{n-1}$) である．

TBI の時間的変化を図 3.1 に示す．横軸を経過時間として，TBI の時間変化は TBI 評価式である $F(t)$ もしくは TBI 算出対象 Web ページへの n 回目のアクセス発生直後の TBI 値である F_n としてプロットされている ．図 3.2 にアクセスログからの TBI 算出システムの構成概要を示す．サーバのアクセスログから監査対象となる各ページの URL を抽出する．式 3.1 の定義から，TBI はアクセスがあったことによる増加関数 $g(\delta t)$ による増加と，リポジトリに保存されている F_{n-1} の値に時間経過による減衰比関数 $h(\delta t)$ を掛け合わせたもの和として表現される．式 3.1 で計算した結果得られた F_n はリポジトリに格納され，次 $n+1$ 回目のアクセス発生に算出される F_{n+1} の計算に用いられる．

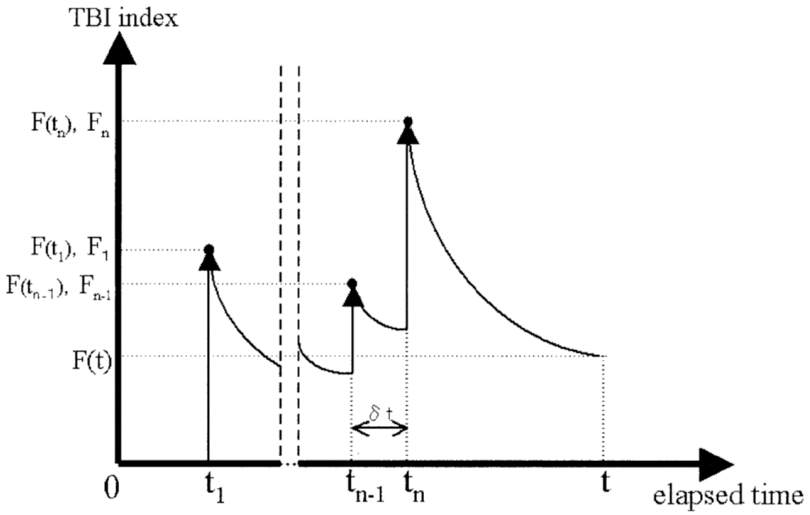

図 3.1　TBI 値の時間的変化 [畑島 2000]

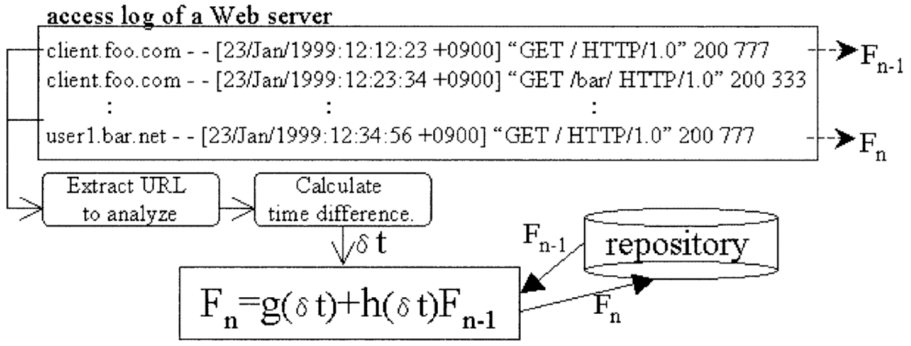

図 3.2　TBI 算出システムの構成概要 [畑島 2000]

3.2.1.1　増加関数の定義

TBI の増加式は，ユーザがページにアクセスするたびに TBI がどのように増加するかを示しており，以下の 2 つの要件をもつ $g(t)$ を定義した（式 3.3）．1) TBI を減少させない．2) アクセス間の時間が 0 のとき （つまり同時アクセス発生時）にはインデックスを予め定めた $g(t)$ の最大値だけ増加させる．

$$\begin{aligned} g(t) &> 0, \\ g(0) &= max(g(t))(const.), \\ g'(t) &\geq 0 \end{aligned} \tag{3.3}$$

算出される値は，時間パラメータ δt に依存し，最後にページにアクセスしたときの値が算出される．なお，本研究では，$g(t)$ を定数とした（式 3.4）．

$$g(\delta t) = const. \tag{3.4}$$

3.2.1.2　減衰比関数の定義

■3.2.1.2.1　概要　減衰比関数は，あるページに対する興味度が，利用度の低下，陳腐化，興味度の低下によって低下していくことを表すよう定義した．

減衰比関数 $h(t)$ には 3 つの要件を設定した．1) 単調に TBI を減衰させること．2) 減衰率は正でなければならないこと．3) ユーザが同時にアクセスしたとき（$t = 0$）には TBI

を減衰させないこと．これらにより，式 3.5 を定義した．

$$\begin{aligned} 0 \leq h(t) \leq 1, \\ h(0) = 1, \\ h'(t) \leq 0, \\ h''(t) \geq 0, \end{aligned} \tag{3.5}$$

■3.2.1.2.2　情報活用度の低下　利用者は情報を得るために Web ページにアクセスする．本研究の実施当時は，ストック型のコンテンツでなければ Web ページの内容は常に最新であるべきであり，古くなった Web ページは淘汰されていくものと想定していた．そのため図書館の蔵書管理を援用できると考えた．図書館の蔵書容量には限りがあるので，どの本を残し，どの本を処分して新しい本を置くかが課題となる．Cole[Cole1963] は，図書館における定期刊行物の利用が，時間とともに指数関数的に減少することを示した（式 3.6）．

$$R(x) = R(N)e^{-Lx} \tag{3.6}$$

ここで，$R(x)$ は x 年前に出版された雑誌のリクエスト数，$R(N)$ は全雑誌のリクエスト数の合計，L と N は定数である．

■3.2.1.2.3　陳腐化　情報は類似する内容の新規コンテンツの出現などによって陳腐化する側面を持つ．それは学術論文であっても同様であり，Griffith ら [Griffith1979] は論文に引用された文書の日付の範囲を調査し，引用数は時間の経過とともに指数関数的に減少することを示した．このように，情報は時間の経過とともに陳腐化するため，情報に対する関心度は下がっていくと考える．

■3.2.1.2.4　関心の減衰　噂や流行，時事問題などは，短期的には興味レベルを急激に上昇させることがあるが，人はすぐに興味を失ってしまう．認知科学の研究により，記憶は使われなくなることで減衰することがわかっており，暗記の保持率は経過時間 t に指数関数的に再係数化される [古川 1996]．これを数式化すると式 3.7 となる

$$R(t) = R(\infty) + R(t) - R(\infty)e^{-\alpha t} \tag{3.7}$$

ここで，$R(\infty)$ は $R(t)$ の $t \to \infty$ としての定数であり，α は減衰比である．

■3.2.1.2.5　減衰比関数　以上の検討から演繹的に減衰比関数を指数関数で定義した．式 3.5 で $h(0) = 1$ としたため，減衰比関数は式 3.8 となる．

$$h(\delta t) = e^{-\alpha \delta t} \tag{3.8}$$

ここで，α は減衰定数，δt は最後のアクセスからの経過時間である．

3.2.1.3 減衰比関数の推定

以上の検討を踏まえ，NTT DIRECTORY の検索ログを用いて，減衰率を実験的に推定した．ユーザが入力したキーワードは，関心のあるトピックを反映していると仮定した．特定のトピックに対する検索数と全体の検索数の推移によって関心の減衰比を求めた．

トピックに関連するキーワードは，シソーラスを用いて抽出した「選挙」に関連する日本語の単語群を用いて，関心度の低下を推定した．選挙はイベントが発生する度に人々の関心を集めるが，開票集計後は急速に関心が薄れるため，関心の低下を推定するのに適した例であると考えた．換言すると選挙は，結果が出ると関心が低下するため，選挙に関するページを検索するために投稿されたキーワード数の低減を分析することにより，減衰比関数を推定出来ると考えた．また，検索の実施回数は，深夜は少なく日中に多いことは想像に難くないように，計測する時間帯に依存する．この影響を排除するために，式 3.9 で表される Access Share（一定時間内に検索されたキーワードの総数に対する割合）を用いて推定を行った．

$$AccessShare = \frac{(Numberoftargetkeywords)}{(Numberofallkeywords)} \tag{3.9}$$

図 3.3 は，研究当時実施されたある全国的な選挙に対する Access Share の選挙後の経時変化を示したものである．式 3.5 から，$h(0) = 1$ にピークがあるようにプロット点の系列を正規化した．その結果，減衰定数 $\alpha = 0.2765$ が導出されたため，減衰比関数として式 3.10 が導かれた．この減衰比関数によれば，関心の度合いはおよそ 2.5 時間で半減することが示されている．

$$h(\delta t) = e^{-\ 0.2765\delta t} \tag{3.10}$$

3.2.1.4 関心度（TBI）算出式の確定

3.2.1.1 の議論に基づき，1 アクセスごとに TBI は 1 ポイント増加するように増加関数を設定した．すなわち定数（$g(\delta t) = 1$）とした．

式 3.11 に，特定のページへの n 回目（n は自然数）のアクセスしたあと，それ以降であり，$n+1$ 回目のアクセスが発生する前の任意の時刻 t における TBI の算出式を示す．

$$\begin{aligned} F(t) &= F_n e^{-\ 0.2765\delta t}, \\ \delta t &= t - t_n, \\ t_n &< t < t_{n+1} \end{aligned} \tag{3.11}$$

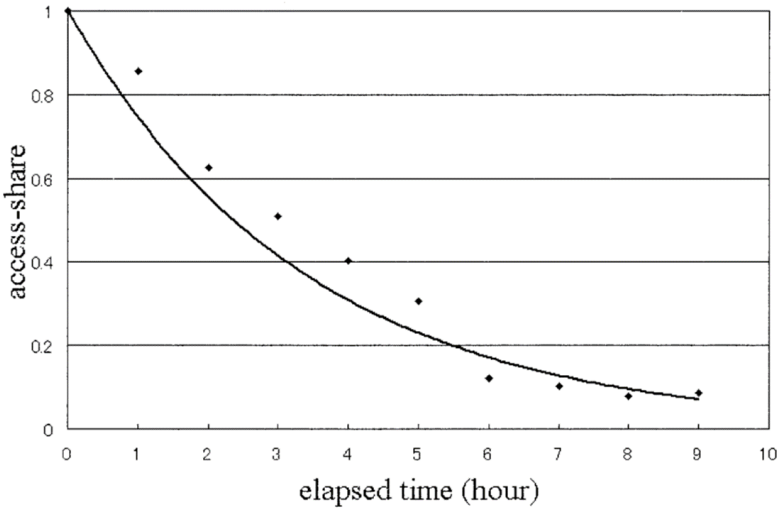

図 3.3　ある選挙後のアクセスシェアの変化 [畑島 2000]

これらにより，n 番目のアクセス発生時の TBI 算出式である式 3.12 を導いた．

$$\begin{aligned} F_n &= 1 + F_{n-1} e^{-0.2765\delta t}, \\ \delta t &= t_n - t_{n-1} \end{aligned} \tag{3.12}$$

3.2.2　関心度（TBI）算出式の評価

導出した TBI 算出式（式 3.12）により得られる TBI 値が，アクセス数によって Web サイトをランク付けする際によく用いられる指標である PageView の代替となりうるかを検証した．Web 文書の人気度に関する研究 [Cunha1995] では，ページビューを指標として，文書へのアクセス数と全体の人気度の順位は Zipf の法則 [Zipf1949] に従うことが示されている．そこで TBI も Zipf の法則に従うかを調べた．

検討には 1999 年 3 月 23 日から 6 月 9 日までの NTT DIRECTORY のアクセスログを使用した．このディレクトリには当時約 23 万件のリンクが含まれていた．各 URL の TBI と page view（アクセス数）を計算した結果を図 3.4 に両対数図として示す．

それぞれの曲線を構成するプロットはそれぞれの Web ページについて算出された指標値である．x 軸はその Web ページの人気順であり，y 軸は算出された値を表している．

図 3.4 のプロットの近似式である式 3.13，式 3.14 で示すように，$x-y$ プロットは非常によく類似しており，その方程式はどちらの分布も $y = Cx^{-\alpha}$(C は定数，α は指数) の形で表される Zipf の法則に従うことが示された．

TBI

$$y = 7297.8x^{-0.6857}, \quad R^2 = 0.9943 \tag{3.13}$$

Page View

$$y = 7571.1x^{-0.6691}, \quad R^2 = 0.9923 \tag{3.14}$$

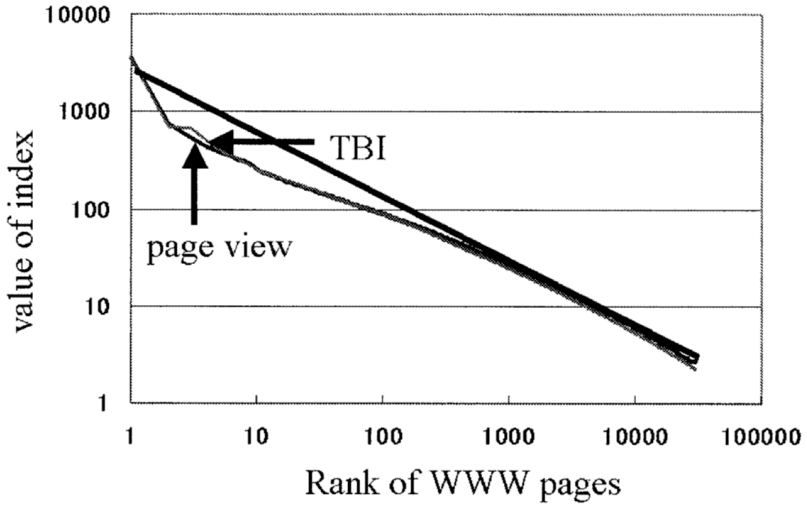

図 3.4　TBI と PageView の順位 (*x* 軸) と算出値（*y* 軸）の指数の両対数図 [畑島 2000]

3.2.3　関心度（TBI）の NTT DIRECTORY での応用

1998 年 7 月に NTT DIRECTORY[NTT DIRECTORY1998] に TBI を導入した．図 3.5 は当時の NTT DIRECTORY のスクリーンショットである．ここに表示されているハイパーリンクは，式 3.12 を用いて算出した TBI 値の順にソートされている．このサイトでは，日付順，タイトル順，TBI 順，URL 順，ブックマーク数順の 5 種類のソート機能が実装されたいた．当時のログ分析の結果，表示順として 65% が TBI 順を選択しており，最も多く利用されていた（図 3.6）．

図 3.5　NTT DIRECTORY[NTT DIRECTORY1998] での検索画面（TBI 順で表示）[畑島 2000]

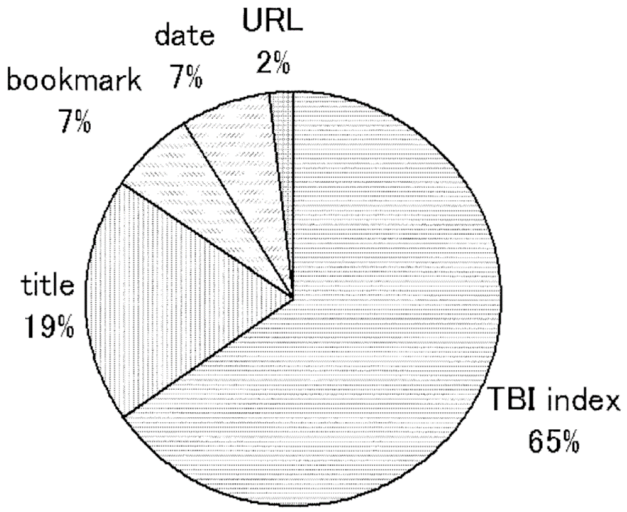

図 3.6　NTT DIRECTORY でのハイパーリンクソート方法の利用割合 [畑島 2000]

3.2.4 CyberRanking

3.2.4.1 概要

開発したアクセスログ解析システム CyberRanking は，TBI，および当時用いられていた評価値による分析結果を表示可能である．CyberRanking の構成は，図 3.7 に示すように 3 つの動作部によって成り立つ．まずアクセスログ収集動作部で分析対象となる Web サーバのアクセスログを収集する．そして分析動作部で指標を算出し，視覚化動作部で分析者の Web ブラウザに分析結果を表示するためのデータセットを作成する．

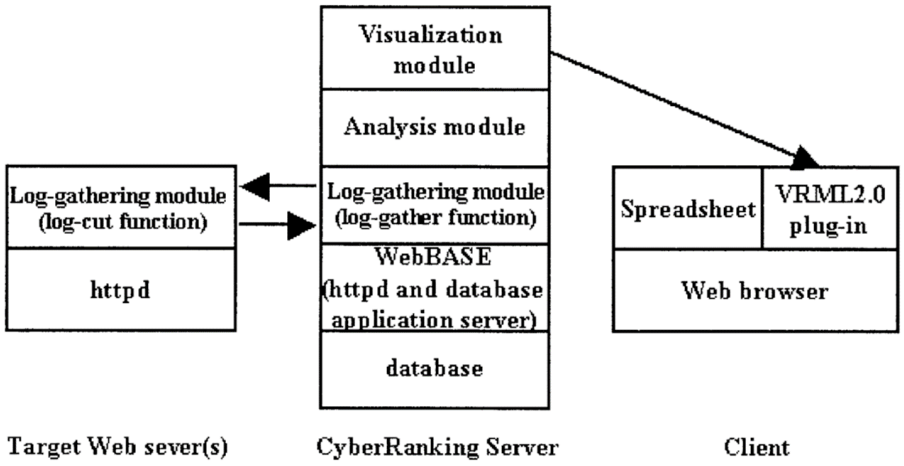

図 3.7　CyberRanking の構成 [畑島 2000]

3.2.4.2 アクセスログ収集動作部

この動作部には 2 つのモジュールが存在する．まず，Log-gathering モジュールのうち分析対象の Web サーバにイントールされるものを log-cut 機能と呼ぶ．log-cut 機能は，httpd と，分析対象 Web サーバのアクセスログをサーバログが生成されるディレクトリから定期的に切り出す機能，および切り出したアクセスログを前述の httpd がアクセス出来るディレクトリに転送する構成されている．転送が必要な理由は，一般的にアクセスログはその Web サーバが情報公開に使っている httpd への HTTP リクエストでは取得できないディレクトリに生成されるためである．

そして，log-gather 機能は CyberRanking サーバに搭載され，分析対象サーバから切り出されたログや当該サーバの Web ページ情報を収集する．具体的には，分析対象サーバ

に搭載した log-cut 機能の http へのリクエストによって分析対象サーバから切り出したログを収集することと，分析対象サーバに http-robot を送り込み，分析対象サーバの Web コンテンツ群のサイトマップやページタイトルを収集することを行う．収集した各データは当時の著者所属組織で開発された Web サーバとデータベースを連携するアプリケーションサーバ WebBASE[山本 1998][WebBASE] で処理され，データベースに格納される．

3.2.4.3　分析動作部

分析動作部で算出可能な指標値は，表 3.2 に示すように，全ログ収集期間，週間，日刊，1 時間単位，ドメイン，Web ページ単位で算出可能である．

表 3.2　CyberRanking で算出可能な指標値

指標	全アクセス数 アクセス元ドメイン別	算出単位
Page View	全アクセス数	1,2,3,4,5
	アクセス元ドメイン別	1,2,3,4,6
Visit	全アクセス数	1,2,3,4,5
	アクセス元ドメイン別	1,2,3,4,6
TBI	全アクセス数	1,2,3,4,5
	アクセス元ドメイン別	1,2,3,4,6
訪問あたりの ページアクセス数	全アクセス	5,6

1：全ログ収集期間，2：週間，3：1 日単位，
4：1 時間単位，5：ドメイン，6：Web ページ単位

3.2.4.4　視覚化動作部

視覚化動作部では，分析結果を Web ブラウザから参照するためにデータセットを作成する．図 3.8 と図 3.9 に表示結果の例を示す．ユーザインターフェースは JavaScript で記述され，グラフは VRML（Virtual Reality Modeling Language）2.0 で作成されている．本動作部から出力されるデータを Web ブラウザで受信することにより 2 次元および 3 次元のグラフの作成が可能である．

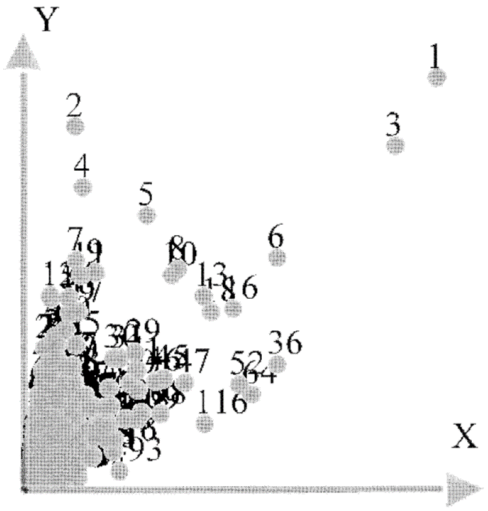

図 3.8　表示されるグラフ例（2D）[畑島 2000]

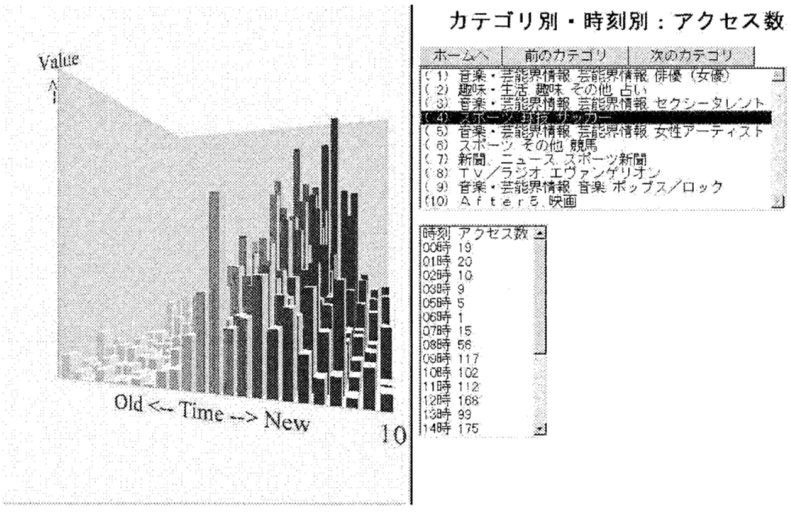

図 3.9　表示されるグラフ例（3D）と指標値例 [畑島 2000]

3.3 議論

3.3.1 関心度（TBI）

アクセスログ解析の関連研究手法は，キーワードベースの解析とユーザベースの解析に分類される．前者は野見山ら [野見山 1996] が文書中のキーワードの重みと文書に対するアクセス頻度に基づく指標を用いたランク付け手法を提案している．後者は Shardanand と Maes[Shardanand1995] はユーザによって文書に付与されたスコアを元に別のユーザが付与するスコアを予測する手法を評価している．しかし，前述のように，アクセス頻度とそのアクセス間隔という，アクセスログに含まれている最小限のデータのみで算出され，時系列情報も考慮されている TBI とは異なる．また，他のユーザがつけたスコアに基づいて，コンテンツを推薦する手法も提案されている．小林ら [小林 1998] はユーザが選択した情報に基づいて推薦を行う手法を提案している．しかし，時間の経過とともに興味が変化することは考慮されていない．また，上記と較べ，TBI の算出に必要なパラメータは最後のアクセスからの時間とその時のインデックスのみであることから，上記の手法よりも導入の容易性と拡張性があると考える．

ただし，本研究で導出した TBI には検討すべき課題が残存している．例示すると，1) **3.2.1.3** で述べた減衰比関数の減衰定数の導出には特定の選挙という短期間に集中的にアクセスが発生するイベントのみを用いたが，より一般的な事象に対する分析の実施検討も必要とみられる．2) 増加関数を定数としたが，例えば，アクセスが集中しすぎた後にはコンテンツに対して飽きが発生し，関心の高まり度合いが低下する（1 アクセス当たりの TBI の増加値が変化する）といった仮説も考慮できるため，増加関数を時間関数とすることも検討課題である．3) TBI では同一 URL であれば Web ページが書き換わっていても同一コンテンツと判断してしまうため，ページ内容の見直しや更新が TBI 指標に与える影響についての考慮が必要である．といった点が挙げられる．

3.3.2 CyberRanking

CyberRanking は，Web ページのアクセス傾向を様々な指標により閲覧出来るため，Web コンテンツのナビゲーターとしての利用が可能であった．また，データ連携には当時革新的であった Web サーバとデータベースを連携機能を持つアプリケーションサーバ WebBASE を利用していたためデータベースからのデータ取得や取り扱いが容易であり，例えば OLAP（online analytical processing）システムとの連携などの機能拡張も可能で

あった.

3.4 まとめ

関心度（TBI：Time-Based Interest）を Web ページの人気を反映した指標として開発し，その算出式と性質について考察した．TBI の減衰率をページへの最終アクセスからの経過時間をパラメータとした指数関数として導出した．実サービスのログを用いた分析により，TBI はページへのアクセス数による単純な指標 Page View と同様に Zipf の法則に従うことが示された．また，TBI をはじめとした指標の分析結果を表示する分析システム CyberRanking を開発した.

第 4 章

第 II 部のまとめ

第 II 部では Web ページを対象としたインターネット利用者の行動を測定する研究について述べた．開発した測定指標である関心度（TBI）の研究動機は，インターネット利用者の行動結果である Web ページへのアクセス状況を用いて，Web ページへの関心の集まり度合いを指標化することであった．Web ページ検索サービス NTT DIRECTORY のログを用いた分析の結果，同一 Web ページへのアクセスの間隔をパラメータとし，アクセスの発生により TBI が増加し，アクセスされていない期間は指数関数的に減衰する性質を持つ TBI 算出式を導出した．TBI は NTT DIRECTORY におけるサイト表示順の指標として実装され一般的に利用された．また，TBI や当時用いられていた指標を分析し表示するアクセスログ解析システム CyberRanking を開発した．

第 II 部の参考文献

[小林 1998] K. Kobayashi, Y. Sumi, and K. Mase, Information presentation based on individual user interests, Proc. IEEE Second International Conference on Knowledge-Based Intelligent Electronic Systems, pp.375–383, Adelaide, April 1998 (1998).

[野見山 1996] 野美山 浩，紺谷 精一，渡辺 日出雄，串間 和彦，堤 泰治郎, 個人適応型情報検索システム　－個人の興味を学習する階層記憶モデルとその協調的フィルタリングへの適用－, 70(1996-FI-042), pp.49 – 56, 情報処理学会 (1996).

[畑島 1996] 畑島 隆，元田 敏浩, WWW アクセスログの有効な解析法について，第 53 回全国大会講演論文集, pp.217 – 218，情報処理学会 (1996).

[畑島 1997] 畑島 隆，元田 敏浩, 時系列情報を考慮したアクセスログ解析，第 54 回全国大会講演論文集, pp.327 – 328，情報処理学会 (1997).

[畑島 2000] T. Hatashima and T. Motoda, An “Interest” Index for WWW Servers and CyberRanking, IEICE TRANS. INF. & SYST., VOL.E83–D, NO.4, APRIL 2000 (2000).

[古川 1996] 古川 俊之, 寿命の数理, 行動計量学シリーズ 13, pp.191–196, 朝倉書店 (1996).

[山本 1998] S. Yamamoto, R. Kawasaki, T. Motoda, and K. Tokumaru, Internet/Intranet application development system WebBASE and its evaluation, IEICE Trans. Inf. & Syst., vol.E81-D, no.12, pp.1450–1457, Dec. 1998 (1998).

[100hot] 100hot.com, 参照先〈http://www.100hot.com/〉（参照 1999）.

[Cole1963] P.F. Cole, Journal usage versus age of journal, J. Documentation, vol.19, pp.1–11 (1963).

[Cunha1995] C.R. Cunha, A. Bestavros, and M.E. Crovella, Characteristics of WWW client-based traces, Technical Report TR-95-010, Boston University Computer Science Department, June 1995 (1995).

[Griffith1979] B.C. Griffith, P. Servi, A. Anker, and M.C. Drott, Aging of scientific literature: A citation analysis, J. Documentation, vol.35, pp.179–196 (1979).

[IPC] I/PRO,Internet Profile Corporation, 参照先〈http://www.ipro.com/〉(参照 1996).

[MyYahoo] My Yahoo!, 参照先〈http://my.yahoo.com/〉(参照 1999).

[NC] Net Count, 参照先〈http://www.netcount.com/〉(参照 1996).

[NTT DIRECTORY1995] NTT 技術資料館資料, NTT DIRECTORY, 参照先〈https://hct.lab.gvm-jp.groupis-ex.ntt/panel/pdf/C-2-6.pdf〉(参照 2022-12-13)

[NTT DIRECTORY1998] Internet Watch, ユーザーの「関心度」でサイトを評価「Super NTT DIRECTORY」実験版公開, 参照先〈https://internet.watch.impress.co.jp/www/article/980702/nttdir.htm〉(1998)(参照 2022-12-13).

[Shardanand1995] U. Shardanand and P. Maes, Social information filtering: Algorithms for automating“Word of Mouth,”Proc. ACM Conference on Human Factors in Computing Systems (CHI’95), pp.210–217 (1995).

[WebBASE] WebBASE, 参照先〈http://webbase.ntts.co.jp/〉(参照 1999).

[WC] WEB Counter, Computer Networking Service Inc., 参照先〈http://www.digits.com/〉(参照 1996).

[Yahoo] Yahoo!, 参照先〈http://www.yahoo.com/〉(参照 1999).

[Zipf1949] G.K. Zipf, Human behavior and the principle of least-effort, Addison-Wesley, Cambridge, MA (1949).

第 III 部

インターネット利用者のセキュリティ不安全行動の研究

第 5 章

はじめに

インターネットユーザのセキュリティ不安全行動に関する研究について述べる．現代生活においてインターネットは不可欠であるが，様々な脅威が存在するゆえに情報セキュリティ対策も必須となっている．企業活動においても同様で，業務においてインターネットを利用する際にはセキュリティ対策が求められる．しかし，セキュリティ対策が求められているにもかかわらず，悪意の有無は問わず行動の意図を持ってその対策行動から外れた行動をしてしまうケースがみられる．そのような行動は，安全マニュアル違反や明確な違反行為でなくても事故や労働災害のリスクを高める行為として不安全行動 (unsafe act) と呼ばれる [芳賀 2007].

本研究はテレワークを題材としてセキュリティ不安全行動を研究し，インターネット利用者の利用行動の測定と解明を行った．最初に **6** では，テレワーク全般を対象とした．そして **7** では，研究を実施していた 2010 年代中盤はテレワークの実施形態として BYOD（Bring Your Own Device：私有端末の業務利用）が注目されていたため研究対象とした．

構成は次の通りである．**6** では，意図せず情報漏洩をしてしまったテレワーカーと，情報漏洩したことがないテレワーカーの間に性格や行動（性向）の差があるのかを，質問紙調査により示した．その結果，テレワーク時の意図しない情報漏洩というセキュリティ不安全行動はテレワーカーのリスクテイキング行動傾向や職場のセキュリティ環境の整備度によって差異が見られた．**7** では，規約の整備状況および許可状況と BYOD ユーザの業務実施状況の分析の結果，情報セキュリティにもリスク補償行動が働いているとみられることを示した．具体的には，会社から許可されて業務を実施している人は，漏えい時に重大事態となるような情報区分の業務データであっても頻度高く取扱う行動がみられたり会社のガバナンスが効かない保存先に格納したりする傾向がみられることを質問紙調査により明らかにした．

第 6 章

テレワークにおける意図しない情報漏洩による不安全行動

6.1　序章

6.1.1　はじめに

働き方改革が提唱される [内閣官房 2016] など，テレワークが脚光を浴びている．企業の情報システムにおいては情報セキュリティソリューションの導入や規約の整備によって企業側の対策が進む一方，ヒューマンエラーは実施者の違反の意図にかかわらず発生するため，設備と人を含めた情報システム全体に対してセキュリティが担保された状態の維持が課題となっている．

本研究では，テレワークを業務データを用いた業務遂行と定義し，情報セキュリティに対するヒューマンエラーのうち，行為そのものには違反の意図がある情報セキュリティ不安全行動に着目し，そのなかでも，内部不正の意図はない行動に注目した [畑島 2017b]．そのうえで，テレワークにおける効果的な情報セキュリティ対策の提案を目的として「情報漏洩行動を悪意を意図せずとも実施してしまった従業員本人の性向に特徴があるか」をリサーチクエスチョンとして設定した．そして，「セキュリティインシデント経験およびセキュリティに対する知識」，「従業員本人の性向」と「業務に対する性向」，および「自分自身の情報漏洩行動経験」を測定する尺度からなる質問紙を設計し，インターネット調査を実施した．データクリーニングの結果得られた従業員 365 名分の回答を「意図しない情報漏洩行動」の実施経験の有無によって 2 群に分け，各測定尺度について尺度得点の平均値の差を検定した．有意な差が認められた測定尺度を考察した結果，従業員本人の性向

のうち，リスクテイキング行動を抑止すること，特に，確信的に敢行してしまう性向を抑止することが有効であることが示唆された．また，職場の情報セキュリティ環境から危険な状況を除外することも有効であることが示唆された．さらに，情報セキュリティ対策の励行は一定の効果が見込まれるものの，対策の効果には個人差があることも示唆された．

6.2 本研究の概要と構成

テレワークは 1980 年代後半からサテライトオフィスと呼ばれ，オフィスを離れた環境での働きかたとして提唱されている [テレワーク 2017]．インターネットの一般的普及が進んだ 2002 年からは国土交通省によって人口実態調査 [国交省 2017a] が実施されており，2011 年の東日本大震災を教訓とした BCP（Business Continuity Planning）対策や，ワーク・ライフ・バランスや生産性の向上を謳う働き方改革の政府戦略 [内閣官房 2016] として近年再度脚光を浴びている．

テレワークは“ICT（Information and Communication Technology）を活用した場所や時間にとらわれない柔軟な働き方”と定義され，働く場所により自宅利用型テレワーク（在宅勤務），モバイルワーク，施設利用型テレワーク（サテライトオフィス勤務など）の 3 つに分類されている [国交省 2017b]．近年の情報端末の小型化と通信環境の高度化により，業務に利用する情報通信端末は従来のデスクトップ型に加え，ノート PC やタブレットのような携帯型情報端末が用いられている．これら携帯型端末を業務利用するオフィスではアクセスフリーと呼ばれる自由な座席での業務実施が可能であるほか，普段職場で利用している業務端末を持ち出せることが，テレワーク推進の一助となっている．

テレワーク時の情報セキュリティ対策 [総務省テレワークセキュリティ] は喫緊の課題であるが，対策は情報システムを用いた対策と運用による対策に大別され，これらを組み合わせて実施されている．さらに，情報システムによる対策は，情報端末の整備と設備環境整備に区分される．端末の整備においては，会社からの端末支給を行う場合と，私有する端末を利用許可する BYOD（Bring Your Own Device）に分類される．そして，設備環境整備においては，会社のシステムへリモートアクセスするための会社側の情報システムや通信環境の整備と，EMM（Enterprise Mobility Management）などのモバイルセキュリティ管理ソリューションの導入といった従業員の端末側へも介入する環境整備に区分される．また，運用面による対策としては，規約の整備，利用規約への誓約書の提出やセキュリティ教育の実施が挙げられる．

テレワークのセキュリティを企業の視点からみると，テレワーク導入による業務効率の改善などのメリットが見込めても，その改善効果の定量化が難しいといった市場調査

[日経 BP2013a] があるように，情報漏洩対策といったセキュリティ対策の重要性を認識があっても効果を確認できないため，リモートアクセス環境や管理ソリューションに設備投資できず規約の整備など運用による対策 [日経 BP2013b] によって対応している．同様に従業員の視点からみると，会社の許可範囲を逸脱したり，許可外であるが善意によって業務実施を不正の意図はなく「ついつい」や「良かれと思って」業務実施したりすることは，セキュリティインシデントを引き起こす要因となる．このような違反として処罰対象とするほどでもない「不安全な行動（unsafe act）」の積み重ねが重大リスクの潜在要因となることは，“1 つの重大事故の背後には 29 の軽微な事故があり，その背景には 300 の異常が存在する”としたハインリッヒの法則として指摘されている [村田 2008].

このように，情報セキュリティソリューションの導入によってセキュリティインシデントのリスク低減が行われても，ヒューマンエラーは実施者の意図にかかわらず発生するため，設備と人を含めた情報システム全体に対してセキュリティが担保された状態の維持は困難である．また，悪意を意図して行われる内部不正や内部犯行は規約がある場合でも発生している現状である [IPA2017] が，これを抑止する完璧な規約を制定し維持することも困難であることは想像に難くない.

本研究の研究動機は，情報システムを利用して業務を実施する従業員のヒューマンファクタを起因としたセキュリティ不安全行動について，情報セキュリティに関する従業員の知識・練度や従業員本人の行動性向に合わせた情報セキュリティ施策を行うことにより，不安全な行動を抑止することである．不安全行動とは善意および悪意や行動の軽重にかかわらず安全に関わる規則違反であると認識した行動であり，これに対してヒューマンエラーとは，安全に関わる規則違反であることを認識しない場合も含むとする．情報システムはヒューマンエラーを抑止する一面を持つソリューションであるが，システム環境整備は多額のコストが発生するため，導入可能な組織ばかりではない．したがって，情報セキュリティの維持には運用によるヒューマンエラーの抑止も重要であり，本研究では特に不安全行動の抑止に注目している.

本研究では情報セキュリティインシデントを起こす不安全行動の行動モデルを計画的行動理論（TPB，Theory of Planned Behavior）[NIPH2017] に従って仮説構築し，質問紙調査結果によって共分散構造分析を行った結果，その行動には「貢献感」が作用していることを示した先行研究 [畑島 2016a] および別途研究 [畑島 2016b] において私有端末におけるモバイルワークにおいては規約があることによる抑止効果はある反面，規約があるがゆえに個人情報などの機微な情報を扱う傾向もみられることを示した．さらに，業務データの保存先選択と企業の規約制定状況 3 群で構成されたクロス集計に対する検定の結果，統計的に有意な組合せの考察によりテレワーク環境を整備するにあたって着手すべき施策を

提言した [畑島 2017a].

また，テレワークにおける効果的な情報セキュリティ対策を提案するためのリサーチクエスチョンとして，情報セキュリティ不安全行動のなかでも重要な課題であって，内部不正・内部犯行 [IPA2017] という重要インシデントの火種となる，許可されていない業務データの持ち出し，業務メールの適切でない宛先への送信，SNS などへの業務情報の不用意な書き込みといった情報漏洩行動について，「情報漏洩行動を悪意を意図せずとも実施してしまった従業員本人の性向に特徴があるか」を設定し，質問紙調査により解明した．その実施として，質問紙を構成する各測定尺度得点の差について情報セキュリティにおける不安全な行動である「意図しない情報漏洩をしたことがある」と自己申告した回答者群とそのような情報漏洩をしたことがないとする対照群との間で尺度得点の平均値の差の検定を実施し，行動の特徴を考察した．情報セキュリティ不安全行動の行動モデルには，文献 [畑島 2016c] で実施した先行研究調査と本稿での検討によって KAB モデル（Knowledge Attitude Behavior model）を選択した．**6.3** では関連研究と本研究の対象を述べる．**6.4** で質問紙の設計について述べる．**6.5** ではインターネット質問紙調査結果の概要を述べ，**6.6** でリサーチクエスチョンである内部不正を意図しない情報漏洩経験の有無によるテレワーク実施者の分析結果を述べる．そして **6.7** で分析に対する考察を示すとともに，本稿の優位性と限界を述べ，**6.8** でまとめる．

6.3　関連研究と本研究の対象

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，セキュリティ対策の施策が進まない要因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を用いた行動モデル分析結果による改善手法の提案がなされている．諏訪ら [諏訪 2012] 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，質問紙調査結果に対する共分散構造分析の結果として，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 [菅野 2010] 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 母集団の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を用いて解明する研究が多数報告されている（たとえば Bulgurcu ら [Bulguru2010]，Ifinedo[Ifnedo2014] など）．

また，情報漏洩インシデント発生要因について，竹村ら [竹村 2015] は個人の心理的要因による行動に着目した質問紙調査し，共分散構造分析により得られる発生要因の直接効

果，間接効果および総合効果の考察から，不正容認風土が情報漏洩につながる行動に最も大きな直接的影響を与える要因であり，ルールの認知は比較的大きな影響を与えないことを示した．しかし，これらはテレワークを実施する従業員対象としておらず，本研究とは課題設定が異なる．

従業員本人の行動を観察した結果により情報セキュリティ施策を変えようとする研究として，片山ら [片山 2015] は情報セキュリティ被害に遭いやすいユーザの検知のために PC の操作ログと普段の心理・行動との相関を報告している．しかし，被害対象が標的型攻撃のような外部からの攻撃に対する性向を対象としており，本研究が対象としている外部からの攻撃がないときでも本人の行動結果から発生するセキュリティインシデントとは対象が異なる．

情報セキュリティ対策による内部不正の抑止について，岡野ら [岡野 2016] は「職場からの許可のない情報持ち出し行動」というセキュリティルール違反行動の抑止について，持ち出し経験者などへのグループインタビューによって構築した要因と抑止策の仮説を質問紙調査の分析によって検討している．その結果，外部からのプレッシャに根本原因があることと，セキュリティ研修だけでは持ち出し行動は防げない可能性を示唆し，個人リスクの認知教育および手続や相談先の整備を提案している．しかし，持ち出し行為実施者に当時の心理を聞いており，当事者の普段の性格や行動についての検討や，従業員全般の性格や行動およびこの両者の比較は検討されていない．

テレワークについて，Weeger ら [Weeger2014] は私有端末を業務利用する BYOD のセキュリティを課題とした行動モデリングと構造分析によって，BYOD を実施する従業員がベネフィットとリスクについてどのように感じているか，BYOD に参加させるためにどのようなメリットを提示すればよいかといった，意思決定とリスク認知の理論のバランスを考慮したモデルを提案している．しかし，検討対象を BYOD に特化しており，利用端末が業務端末の場合もあるテレワークとは対象が異なっている．

また，テレワークに関する行動分析の研究には Weinert ら [Weinert2014] があるが，テレワークに否定的である要因の分析対象が IT プロフェッショナルであり，業種業態を問わない本研究とは対象が異なる．

以上の先行研究調査から，本研究の問題意識である，テレワーク時に情報漏洩行動を意図せず実施してしまった従業員本人の性向を検証する研究は，実施の意義があると判断した．

6.4　質問紙設計

6.4.1　不安全行動の分類

6.1 で示したように，テレワークにおける情報セキュリティインシデントの発生要因としての不安全行動に着目する．不安全行動は産業安全の分野でよく用いられる用語であり，安全マニュアル違反や明確な違反行為でなくても事故や労働災害のリスクを高める行為を指すほか，エラーを意図しない行動の結果として生じる危険行動を含める場合がある [芳賀 2007] ように，不安全行動の定義には行動科学や認知心理学といったアプローチの違いにより様々な分類法が存在する [Reason2014].

Reason は心理状態に注目した分類として，不安全行動のうち規則違反の意図がありつつ行動した結果である違反（Violation）を，「日常的規則違反」，「例外的規則違反」，および「破壊行為」に分類している [Reason2014].

また，和田ら [和田 2012] は不安全行動を，法令違反やマナー違反，約束違反といった違反行動と，リスクテイキング行動の重なる領域と定義している．なお，リスクテイキング行動については，規則の有無に関係なくメリットの獲得を目指してあえて危険性のある行動をとることと定義している．

違反型ヒューマンエラーについて，村田 [村田 2008] は「マナーや規則を守らない」，「手抜き」，そして「怠惰」というそれぞれの行為と説明している．その原因として「善意や好意による場合」，「いい格好をしたい」，「安全ボケによる手抜き」，そして「面倒な手順の手抜き」を挙げている．また，違反の実施原因を習熟度からも分類し，初心者は知識不足に起因することが多く，熟練者は意図的や故意であることが多いと説明している．

本研究では，テレワークを業務データを用いた業務遂行と定義した．そのうえで業務に対する情報セキュリティ不安全行動として，行為そのものに意図があり規則違反の意図もあるが，内部不正の意図はなく，「ついつい」「良かれと思って」と実施した行動 [畑島 2016b] を対象とする．換言すると本稿の対象は，Reason の不安全行動の分類における違反（Violation）から内部犯行のような破壊行為を除外した，日常的規則違反と例外的規則違反である．以降，意図とは内部不正・内部犯行といった悪意の意図を指す．

そして，業務データを用いた業務遂行によって発生する情報セキュリティ不安全行動のうち，テレワークにおける最大の懸念事項である情報漏洩について，以下の仮説を設定した．「情報漏洩行動を悪意を意図せずとも実施してしまった従業員本人の性格や行動に特徴はあるか」というリサーチクエスチョンに対して，先行研究の知見により情報セキュリ

ティに対する行動性向について行動モデルを設定するとともに，モデルを構成する概念を測定尺度とした質問紙調査結果の分析と考察を実施した．

6.4.2 情報セキュリティ不安全行動モデルの選択

従来の情報セキュリティに対する行動モデル研究は，行動経済学や行動心理学などで提唱されてきた行動理論が用いられており，その例として，合理的行動理論（TRA，Theory of Reasoned Action）およびこれを拡張した計画的行動理論（TPB，Theory of Planned Behavior）や，これらを踏まえたコンピュータの利用行動を説明する行動意思モデルである技術受容モデル（TAM，Technology Acceptance Model）および KAB モデルが挙げられる．各モデルの解説は文献 [Parsons2014] に詳しい．

TRA と TPB は，行為の前提に行動遂行の意図があり，その結果行動が起こされるとしている．本研究では，悪意による行動遂行の意図はない場合を観測するため，これらのモデルは不適当である．また，TAM は情報システムを利用する動機を解明するモデルであるため，本研究への適用はそぐわない．

KAB モデルは，Knowledge 層，Attitude 層，そして Behavior 層から構成される（図 6.1）．Parsons ら [Parsons2014] は，情報セキュリティの人的要素について，インターネット利用行動 7 種類に対するセキュリティ行動の質問紙調査を実施し，Knowledge 層から Attitude 層，Attitude 層から Behavior 層，そして Knowledge 層から Behavior 層に向かってパスを接続したモデルで説明できることを示している．

Kruger ら [Kruger2006] も，情報セキュリティ意識向上プログラムの効果測定メソッドの提案において測定する各分野における細分項目として，Knowledge 層，Attitude 層と Behavior 層の 3 つの側面から測定している．また浜津ら [浜津 2015] は，説得心理学における集団的防護動機理論の規定要因に加え情報セキュリティに関する経験や知識を Knowledge 層に据えたモデルを提案し，質問紙調査と仮想的にインシデントを発生させた実験によって，情報セキュリティ対策の実行意志に深刻さ認知，効果性認知，および生起確率認知が影響すると示している．また，諏訪ら [諏訪 2012] が企業の従業員が情報セキュリティ対策の行動をしない理由について計画的行動理論に基づいた仮説モデルに対して質問紙調査を実施した研究においても，その結果は KAB モデルに沿っている．

これらにより，情報セキュリティインシデントにおけるリスク行動解明のための質問紙を構成する概念の設計フレームワークとして KAB モデルは妥当とし，従業員の性向を分析する質問紙調査の設計モデルとして採用した．

図 6.1　KAB モデル

6.4.2.1　KAB モデルに沿った構成概念検討による質問紙設計

前節に述べた KAB モデルによる情報セキュリティ不安全行動モデルに従って，それぞれの階層における構成概念を検討する．そして，それぞれの構成概念を測定する尺度となる質問項目（表 6.1）の設定根拠を説明する．検討の結果得られた質問紙を付録 Ⅲ-1 に示す．

6.4.2.2　Knowledge 層

Knowledge 層は，この層にウイルス感染経験，IT 知識および IT スキルを設定する浜津ら [浜津 2015] の方法に倣った．本研究においては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 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 [IPA2016] 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 [総務省テレワークセキュリティ] 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 項目を作成する（Q9）とともに，情報セキュリティに関する組織内部環境に対する危険認知の程度を測るため，IPA が実施したインシデント調査 [IPA2014] の質問紙から 4 項目を抽出し翻案して用いた（Q10）．

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に対して設定した Q9 については，セキュリティ対策実施ができるのはセキュリティに対する知識があるからであり，また，対策の度合いが情報セキュリティに対する経験の度合いとして現れることから妥当とした．なお，セキュリティ知識については，たとえば，Q9 の設問 9「悪意のあるソフトウェアが配布されているサイトにはアクセスしない」における悪意のあるサイト，および Q9 の設問 14「興味がある情報なら怪しげだと思うサイトでもアクセスする」における怪しげなサイトをそれぞれ認識するには，セキュリティに対する知識と経験が必要であることから，これらを設問として設定した．

情報セキュリティに関する組織内部環境に対する危険認知の程度に対して設定した Q10 については，総務省 [総務省 2016a] で実施された質問紙調査において，不正を実施した内部者が認知していた事象を問う設問から抽出しているため妥当とした．

6.4.2.3 Attitude 層

Attitude 層は，従業員の性向（性格や行動）について「業務に対する性向」と「従業員本人の性向」に分けて構成概念を設定した．「業務に対する性向」について，総務省によるテレワーク推進の平成 25 年度取組 [総務省 2016a] に挙げられた 55 社のテレワーク実施事例から特徴的な項目を抽出した．この結果，テレワークに導入に関する好感度 7 項目（Q7）と，手続の簡便性の追求（村田 [村田 2008] が挙げた違反型ヒューマンエラーの原因のうち「手続の手抜き」）の態度 5 項目（Q8）を質問項目とした．後者はテレワークに関する申請項目を挙げ，手続が面倒であるかを尋ねた．

6.1 に示した先行研究 [畑島 2016a] において，私有モバイル端末を利用するモバイルワークでは社内や取引先などの業務遂行に係るステークホルダーに対する貢献の意図によってモバイルワーク行動がなされていることを述べた．また，貢献感の獲得には，前述のテレワーク実施事例 [総務省 2016a] の分析によって「職場のコミュニケーションがとれている」,「評価が公平である」，そして「承認欲求が満たされる」からなる 3 つの構成要素に持つことが分かった．このうち承認欲求については,「従業員本人の性向」として後述する．

これらの結果により，貢献感の測定尺度として，評価の公平感や職場のコミュニケーションについては職務満足度を測る安達の尺度 [安達 1998] から職務内容，職場環境，および人間関係の 3 つの下位尺度（27 項目）を用いた（Q1）が，セールスマンを対象とするために測定尺度として既存研究に追加したと説明されている給与に対する測定尺度は除外した．なお，測定尺度から下位尺度を選んで使用することは，下位尺度の項目をすべてそのまま使用するなら問題はないとされている [堀 2001].

「従業員本人の性向」には，業務や普段の物事を遂行したい気持ちに対する測定尺度として，23 項目で構成される達成動機を測る堀野の尺度 [堀野 1987] を設定した（Q4）．また，村田 [村田 2008] が挙げた違反型ヒューマンエラーの原因のうち「いい格好をしたい」を採用し，20 項目で構成される承認欲求に関する植田らの測定尺度 [植田 1990] を設定した（Q2）．さらに，**6.4.1** で挙げたリスクテイキング行動として，森泉ら [森泉 2011] によるリスクテイキング行動尺度のうち，妥当性の再確認が必要としている安全性配慮尺度（防犯や安全への配慮をともなう行動に対するリスク傾向）を除外し，状況的敢行性（状況に左右されるような行動に対するリスク傾向），確信的敢行性（状況に左右されにくく個人内の一貫した信念に基づいた行動に対するリスク傾向），そしてギャンブル志向性（個人のギャンブル傾向）からなる 14 項目を用いた（Q3）.

6.4.2.4 Behavior 層

情報セキュリティリスクのある行動を自己申告させ，Behavior 層とした（Q11）．設問に「意図せず情報漏洩をしたことがある」（Q11 の設問 2）と，「意図して情報漏洩をしたことがない」（Q11 の設問 3）の両方を設定し，ここで問う意図は内部不正や内部犯行といった悪意の意図の有無であることを認識させた．これらの設問について，「はい」と「いいえ」の 2 件法で回答させることによって，リサーチクエスチョンとして設定した分析対象である「情報漏洩行動を悪意を意図せずとも実施してしまった従業員本人」を抽出した．

表 6.1　測定尺度と KAB モデル階層との対応

質問番号	測定尺度名	KAB モデル階層
Q1	職務満足度の高さ	Attitude 層 （業務に対する性向）
Q2	承認欲求の強さ	Attitude 層 （従業員本人の性向）
Q3	リスクテイキング行動傾向の強さ	Attitude 層 （従業員本人の性向）
Q4	達成動機の強さ	Attitude 層 （業務に対する性向 ・従業員本人の性向）
Q5	勤務時間・テレワーク実施時間	KAB モデル外
Q6	端末別のテレワーク実施時間	KAB モデル外
Q7	テレワーク導入効果への好感度	Attitude 層 （業務に対する性向）
Q8	テレワーク手続の面倒感	Attitude 層 （業務に対する性向）
Q9	自身の情報セキュリティ対策実施度	Knowledge 層
Q10	職場の情報セキュリティ環境危険度	Knowledge 層
Q11	情報セキュリティリスクのある行動の自己申告	Behavior 層

各測定尺度の出典は **6.4.2.2**，**6.4.2.3**，**6.4.2.4** を参照

6.5　調査と分析

6.5.1　調査の概要

インターネット調査会社に登録している調査モニターを対象としたインターネット質問紙調査を 2016 年 12 月に実施した．本研究の検討対象は業務データを用いた業務遂行としてのテレワークであるため，インターネット調査は研究手法として妥当であると考える．

日本の労働者人口構造を反映するために，調査協力者の業態区分は産業力調査による区分について一部を統合して用い，調査協力者の割付けには労働力調査 2016 年 3 月第 7 表（主な産業，雇用形態別役員を除く雇用者数）[総務省 2016b] において正規労働者と非正規労働者の人数を合算し，産業構成人員比を算出した結果を用いた．また，調査対象は，業務として電子データを扱うことがあること，および，中小企業基本法に定義される小規模企業者人数や，小規模企業共済加入条件以上の人員数の企業の従業員および公務業であって，役職が経営層や役員でない一般従業員とした．人員数については，卸売業と小売業が含まれる区分では 6 人以上，それ以外の区分では 21 人以上が対象となった．人員数の制約は，一般従業員の性向を分析するために，一般従業員が経営層や役員の業務を担うことが少なくなると思われる事業規模の企業から調査協力者を抽出する目的で設定した．

6.5.2　回答の概要

約 4 万人に対して表 6.2 の産業別構成人員比を目標として調査依頼を送信し，目標数まで回答を受け付けた．**6.5.1** に挙げた抽出条件を通過した調査協力者の回答からインターネット調査会社によって回答時間が短すぎる調査協力者を除外した結果，1242 名分の個票データを獲得した．調査協力者の産業構成人員比率は表 6.2 となった．製造業が多く，その他サービス業が少ないものの，おおよそ国内産業の構成人員比を反映するものとなったと考える．

6.5.3　スクリーニング

インターネットを利用する質問紙調査の問題点として，調査に回答することによって得られる報酬を目的として調査対象ではないのに回答に参加したり，調査対象であっても不誠実に記入したりする参加者によって精度が下がるといった問題点が指摘されている

[宮本 2014].

この問題に対して今回の調査では，**6.5.2** で挙げた調査会社によるスクリーニングに加え，独自のスクリーニングを実施することによって対応した．報酬目的や不誠実な参加者は，オンライン調査モニターが教示文や質問項目を読まずに回答する傾向が指摘されている [三浦 2015] など，調査項目の内容を理解するための認知コストを払わないとされている．これに対して本研究では，(1) 1 週間の労働時間として平日 2 時間程度の短時間勤務者を考慮するとともに，回答を急ぐために 1 桁の数値によって 10 時間より小さい労働時間を入力する回答者を除外．(2) (1) とは逆に，回答として求めた 1 週間の時間数より大きすぎる数値を入力する回答者を除外．(3) 労働時間の合計を回答として求めていることを理解し，正確な計算を行った回答者のみを採用というスクリーニングを行い精度の向上を図った．

具体的なスクリーニング手順を以下に述べる．(a) この 3 カ月のおおよその 1 週間の総労働時間平均に対する回答（Q5）が 10 時間以上であること．(b) テレワークの 3 パターン（在宅勤務，モバイルワーク，施設利用型勤務）ごとの労働時間（Q5），およびテレワークにおける端末別（支給端末，私有端末）の利用時間（Q6）が 1 週間の合計時間（10080 分）より小さいこと．(c) (b) で手入力させた，労働時間 3 パターンの合計，および端末別の利用時間の合計について，計算結果それぞれが正しいこと．上記手順を実施した結果，719 名分のデータが得られた．

6.5.4 分析

本調査結果の分析には，統計解析ソフトウェア R version 3.3.2 を用いた．

6.5.4.1 テレワーク実施割合の分析

データクリーニングの結果得られた 719 名の回答の内訳は，会社端末と私有端末のいずれかもしくは両方に対してテレワーク時間を 1 分以上と回答したのは 365 名（50.8%），それに対して 0 分と回答したのは 354 名（49.2%）であった．この分類は国土交通省テレワーク人口動態調査 [国交省 2017a] における広義のテレワーカーの定義に従った．

6.5.4.2 尺度得点の基本統計量と信頼性

本項以降，テレワークを実施する 365 名について分析を実施する．本研究で利用した各層の構成概念に対する測定尺度について，基本統計量と信頼性を算出した結果を表 6.4 に示す．信頼性は Cronbach の α 係数によって検証する．Cronbach の α 係数は 0 から 1 ま

表 6.2　産業構成人員比率と調査協力者比率（$N = 1242$）

業態名称	産業構成 人員比率（%）	調査協力者 人員比率（%）
製造業	18.0	25.4
情報通信業	3.5	4.3
運輸業・郵便業	5.9	4.3
卸売業・小売業	17.2	17.9
金融業・保険業	3.0	3.6
不動産業・物品賃貸業	1.7	2.1
教育業ほか（注）	8.0	5.8
医療業・福祉業	14.4	12.5
その他サービス業	16.8	9.9
その他非製造業	7.2	6.9
公務	4.3	7.6
合計	100.0	100.0

注：学術研究・専門技術サービス
・教育・学習支援業

での範囲の値をとり，α 値が 0.6 以上であれば「高い」，0.8 以上であれば「非常に高い」信頼性と表記されることが多い [宮本 2014]．このことから，本研究で用いる測定尺度はいずれも高い信頼性を持っていることが分かった．なお，測定尺度の選択肢数が異なっているのは，既存研究による測定尺度を改変せず用いたためである．

6.6　内部不正を意図しない情報漏洩経験の有無によるテレワーク実施者の分析

6.6.1　分析手法

本項以降において，本研究のリサーチクエスチョンである「情報漏洩行動を意図せずとも実施してしまった従業員本人の性向に特徴があるか」に対して検証を実施する．具体的には，「意図しない情報漏洩経験がある群」と，その対照群である「意図しない情報漏洩経験がない群」のそれぞれの各測定尺度に対する尺度得点の差を検定し，その結果の考察

によって実施する．

テレワーク実施者 365 名のうち，「私は意図せず業務データを漏洩させたことがある」の設問（Q11 の 2 項目目）に「はい」と回答したのは 20 名であり，「いいえ」と回答したのは 345 名だった．

リサーチクエスチョンから導かれる帰無仮説”「意図しない情報漏洩経験がある群」と「意図しない情報漏洩系経験がない群」の尺度得点の間に差はない”に対する検定手法の選択方法として以下の手順をとった．まず，2 群の得点分布に対して正規性と等分散性を調べた．以下，有意水準を 5% とした．正規性の検定に Shapiro-Wilk 検定，等分散の検定に F 検定を用った．上記検定の結果，2 群ともに正規性が認められた「達成動機の強さ」の下位尺度である「競争的達成動機の強さ」に対しては Welch の t 検定を実施した．そして，2 群の得点分布に正規性がなく，2 群の得点分布が不等分散であった「リスクテイキング行動傾向の強さ」の下位尺度である「確信的敢行性」に対しては Brunner-Munzel 検定を実施するとともに，等分散であった前述以外の測定尺度には Mann-Whitney の U 検定を実施した．いずれの検定において有意水準を 5%（$p < .05$）において有意差があるとし，有意水準 10%（$p < .1$）の場合は有意傾向に差が認められると判定した．これらの検定は標本数が揃っていない場合でも利用可能である．

6.6.2 内部不正を意図しない情報漏洩経験の有無による各尺度得点の平均の差の検定

意図しない情報漏洩経験の有無による 2 群間の尺度得点それぞれの平均の差を検定した結果を表 6.3 に示す．なお，2 群に分割前の尺度得点の平均と標準偏差は表 6.4 の通りだった．以下に各尺度得点の検定結果を述べる．

職務満足度の高さについては，職務内容と職場環境には有意な差がみられなかったが，人間関係の良さを測定する尺度において，「意図しない情報漏洩経験がある群」のほうが「意図しない情報漏洩経験のない群」よりも尺度得点が大きいことに有意傾向に差がみられた．

承認欲求の強さにおいては有意な差はみられなかった．

リスクテイキング傾向の強さは，状況的敢行性，確信的敢行性，ギャンブル指向性のいずれの下位尺度においても，「意図しない情報漏洩経験がある群」の得点は「意図しない情報漏洩経験のない群」の得点より有意に大きいことが認められた．各下位尺度の検定の有意水準では，確信的敢行性が 0.1% 水準で有意差があり，ギャンブル指向性は 1% 水準，状況的敢行性は 5% 水準でそれぞれ有意な差が見られた．

達成動機の強さは，自己充実的達成動機と競争的達成動機のいずれにおいても有意な差はみられなかった．また，テレワーク導入効果への好感度およびテレワーク手続の面倒感について，いずれも有意な差が認められなかった．

自身の情報セキュリティ対策実施度については，「意図しない情報漏洩経験がある群」の得点が「意図しない情報漏洩経験のない群」の得点より小さいことについては $p < .1$ であり 5 %水準では有意ではなかった．

テレワーク実施者の職場の情報セキュリティ環境危険度について，「意図しない情報漏洩経験がある群」の得点は「意図しない情報漏洩経験のない群」の得点より有意に大きい ($p < .001$) ことが認められた．

表 6.3　尺度得点の平均の差の検定結果（$N = 365$）

	意図しない情報漏洩経験あり（$n = 20$）		意図しない情報漏洩経験なし（$n = 345$）		有意差
	平均	*SD*	平均	*SD*	
職務満足度の高さ（業務に対する性向）					
職務内容	26.35	5.07	24.46	5.51	*n.s.*
職場環境	22.05	4.84	20.02	4.62	*n.s.*
人間関係	34.45	4.03	32.59	4.08	†
承認欲求の強さ（従業員本人の性向）					
	59.35	8.23	58.87	8.23	*n.s.*
リスクテイキング行動傾向の強さ（従業員本人の性向）					
状況的敢行性	18.45	4.31	15.74	4.48	*
確信的敢行性	7.60	3.60	4.84	2.08	***
ギャンブル志向性	11.00	3.45	8.62	3.75	**
達成動機の強さ（従業員本人の性向・業務に対する性向）					
自己充実的達成動機	66.55	11.03	66.77	10.08	*n.s.*
競争的達成動機	48.05	10.96	45.78	8.95	*n.s.*
テレワーク導入の効果への好感度（業務に対する性向）					
	22.60	3.47	23.70	3.36	*n.s.*
テレワーク手続の面倒感（業務に対する性向）					
	17.65	4.36	23.70	3.36	*n.s.*
自身の情報セキュリティ対策実施度（Knowledge 層）					
	60.35	8.47	63.92	12.02	†
職場の情報セキュリティ環境危険度（Knowledge 層）					
	19.20	4.20	11.72	5.60	***

検定は「達成動機のうち，競争的達成動機の強さ」は Welch の t 検定，
「リスクテイキング行動のうち，確信的敢行性」は Brunner-Munzel 検定，
その他は Mann-Whitney の U 検定による．
†：$p < .1$, ∗：$p < .05$, ∗∗：$p < .01$, ∗∗∗：$p < .001$,
n.s.：統計的に有意ではない（Not statistically significant）

表 6.4　尺度得点の平均値，標準偏差，Cronbach の α 係数（$N = 365$）

	設問数	選択肢数	平均	SD	α
職務満足度の高さ（業務に対する性向）					
職務内容[*1]	9	4	24.56	5.49	0.91
職場環境[*2]	8	4	20.13	4.65	0.86
人間関係[*3]	10	4	32.69	4.10	0.84
承認欲求の強さ（従業員本人の性向）					
	20	5	58.90	8.22	0.83
リスクテイキング行動傾向の強さ（従業員本人の性向）					
状況的敢行性[*4]	6	5	15.88	4.51	0.72
確信的敢行性[*5]	3	5	4.99	2.27	0.75
ギャンブル志向性[*6]	5	5	8.75	3.77	0.78
達成動機の強さ（従業員本人の性向・業務に対する性向）					
自己充実的達成動機[*7]	13	7	66.76	10.12	0.90
競争的達成動機[*8]	10	7	45.91	9.07	0.87
テレワーク導入の効果への好感度（業務に対する性向）					
	7	5	23.64	3.77	0.82
テレワーク手続の面倒感（業務に対する性向）					
	6	5	17.45	3.90	0.79
自身の情報セキュリティ対策実施度（Knowledge 層）					
	17	5	63.73	11.87	0.91
職場の情報セキュリティ環境危険度（Knowledge 層）					
	4	7	12.13	5.78	0.86

[*1] Q1-1～10
[*2] Q1-11～17
[*3] Q1-18～27
[*4] Q3-1～6
[*5] Q3-7～9
[*6] Q3-10～14
[*7] Q4-1,3,4,6,7,8,10,12,14,16,19,21,23
[*8] Q4-2,5,9,11,13,15,17,18,20,22

6.7　全体考察

6.7.1　考察

6.6.2 に挙げた検定結果から，リサーチクエスチョン「情報漏洩行動を悪意を意図せずとも実施してしまった従業員本人の性向に特徴があるか」を考察し，テレワークにおける効果的な情報セキュリティ対策を提案する．

本考察によって得られた示唆は以下通りであった．

1. 確信的に敢行してしまう性向を抑止する施策が効果的
2. テレワークに関する情報セキュリティ対策であっても，従業員が所属する職場のセキュリティ環境を危険度の低い状態にする施策が有効
3. 情報セキュリティ対策の実施を促す施策には一定の効果がある

「従業員本人の性向」では，「意図しない情報漏洩経験がある群」は，「意図しない情報漏洩経験のない群」よりもリスクテイキング行動傾向（Q3）が有意に強いことが示された．その反面，承認欲求（Q2）および達成動機（Q4）については有意な差が得られなかった．これにより，各人のリスクテイキング行動を抑止することによって情報セキュリティ対策が効果的となるという示唆を得た．なかでも，確信的敢行性（状況に左右されにくく個人内の一貫した信念に基づいた行動に対するリスク傾向 [森泉 2011]）の尺度得点から，意図しない情報漏洩であっても，従業員本人に確信的な心理があるときには情報セキュリティリスクの高い行動をしまうことが示唆された．その原因は，**6.4.1** に挙げた村田 [村田 2008] の説明による善意や好意によるものと考察する．以上より，(1) 確信的に敢行してしまう性向を抑止する施策が効果的であることが示唆された．

つまり，確信的敢行性の強い個人であっても，行動を起こさないように働きかける施策の実施が効果的である．その施策としては，たとえば，情報セキュリティインシデントの起因となった行動について，行動によって発生する情報セキュリティ上のリスクの説明だけでなく，行動した結果として行為者に発生するデメリットを認知させる教育が挙げられる．施策の一例として，(a) 善意や好意からの行動に対しては，その行為の結果が自身や組織にデメリットをもたらすことを明示する．(b) 処分の厳しさを明示するとともに，実際に大きな処分を受けた事例を明確に提示し，メールや回覧といった方法で定期的に閲覧させるといったセキュリティ教育施策が挙げられる．

また，「業務に対する性向」では，情報セキュリティに特化しない職場環境に関する職務

満足度（Q1）およびテレワーク実施の好感度（Q7）には有意な差が得られなかった．そして，岡野ら [岡野 2016] の示した手続の整備も，テレワークに対しては有意な差が得られなかった（Q8）．

Attitude 層において業務に対する性向の 1 つとして挙げた貢献感については，職務満足度を測る安達の尺度 [安達 1998] のうち人間関係 (Q1) について，意図しない情報漏洩経験者のほうが対照群よりも尺度得点において 5% 水準で有意差はなかった．**6.1** に示した我々の先行研究 [畑島 2016a] では，私有端末をモバイルワークに用いる行動の主要因として，社内や取引先といった業務遂行に係るステークホルダに対する貢献の意図があることが示唆された．しかし，本研究のように，テレワークについて会社支給端末を用いた業務を含めた場合，貢献感は意図しない情報漏洩という行動の主要因とはならないことが示唆された．

Knowledge 層では，（2）テレワークに関する情報セキュリティ対策であっても，従業員が所属する職場のセキュリティ環境を危険度の低い状態にする施策が有効であるという示唆が得られた（Q10）．換言すると，Reason の示す日常的規則違反 [Reason2014] を発生させやすい状況を排除することが有効であると思われる．このような状況は，竹村ら [竹村 2015] が情報漏洩につながる行動に対して最も直接的な影響を与える要因とした「不正容認風土」が類似する概念とみられるが，不正容認風土が容認されている状況を想定した設問による質問紙調査や，不正容認風土が容認されている環境を仮定したモニター実験などにより，さらなる検証が必要と考える．

また，自身の情報セキュリティ対策実施度（Q9）においては，意図しない情報漏洩経験がない群の尺度得点は，対照群と比べて 5% 水準では有意差はなかった．このため，(3) 情報セキュリティ対策の実施を促す施策には一定の効果があることは論を待たないが，本研究では有意差が見られなかった．ただし，意図しない漏洩経験がない群の尺度得点の標準偏差が対照群に比べて大きく，情報セキュリティ対策を励行する施策の効果には個人差が大きいことも示唆されたことにより，前述の職場のセキュリティ環境やリスクテイキング行動の抑止に比べると施策実施による効果が薄くなっていると考察する．

6.7.2 本研究の優位性

本研究の優位性として，以下が挙げられる．本質問紙は信頼性が高いと思われる．これは，情報セキュリティ分野における先行研究で用いられることが多い KAB モデルを採用した質問紙設計において，テレワーク実施者自身の性向については社会科学の既存研究であり信頼性と妥当性が認められている測定尺度を用いることにより質問項目の充足性が担

保されていること，および，ほかの尺度についても今回の調査結果における Cronbach の α 係数によって高い信頼性が認められたことが根拠である．

また，今回の調査結果データは信頼性が高いと思われる．これは，構成概念の設計において産業全体を対象とした政府によるテレワーク実態調査の分析結果を用いていることと，独自のフィルタリングによって誠実な回答のみを分析対象としたことにより従来のインターネット質問紙調査の弱点に対応したことによる．

インターネットを用いた質問紙調査においては，調査項目の内容を理解するための認知コストを払わない回答者が存在する問題が指摘されている．オンライン調査のモニターが教示文や質問項目を読まずに回答する傾向を調査した三浦ら [三浦 2015] の調査では，長文の教示文において後続の質問に回答しないことを求める IMC（Instructional manipulation check）と呼ばれる手法では半数以上が教示に従わず，また，リッカートタイプ尺度の設問において回答する選択肢を指定する教示文の指示と異なる回答が 13.3% であった．

このように，不誠実な回答者を排除する対策は有効であるが，従来の情報セキュリティ心理学の調査研究においては，実施した対策を明示する論文はみられなかった．このため，不誠実な回答を排除した本研究のデータは精度が高くなっているといえる．

6.7.3 本研究の限界

まず，インターネット質問紙調査の弱点である回答報酬のみを目的とした不誠実な回答に対して，設問内で数値計算させた結果の検算により排除したが，誠実な回答者であるにもかかわらず計算ミスをしてしまった回答者を排除してしまった可能性がある．

次に，調査会社はモニターの獲得やその品質管理，および回答時の精度向上といった調査の信頼性を確保する取り組みを実施している（たとえば [マクロミル 2017], [インテージ 2017]）．これに対して本研究で収集した 1242 名分の個票データがフィルタリングによって 719 名分まで減った理由については，(a) 設問数が多かったために回答時の集中力が低下していたこと，(b) 計算ミスに対するアラートを表示する調査会社のサービスメニューを利用しなかったため，そのサービスに慣れている実験協力者が回答を修正する機会があると思っていたのに与えられなかったこと，(c) 質問項目をよく読まず，1 週間の労働時間を求める問いに対して 1 日の労働時間を記入した回答者の存在が考えられることが考えられる．

そして，内部不正・内部犯行の意図がないことは Behavior 層の 2 項目の設問によって設問意図を認識させたが，誤認や設問文の誤読による回答が含まれる可能性がある．

最後に，本研究では各構成概念の直接的な効果を測定尺度得点の差の検定によって求めたが，構成概念相互間の間接効果やそれらを総合した効果も考えられる．この解明には共分散構造分析やロジスティック回帰分析による数式モデル化によって，各構成概念をパラメータとした全体構造の記述による解法があり，今後取り組みたい．

6.8 まとめ

本研究では，テレワークにおける効果的な情報セキュリティ対策を提案するために，「情報漏洩行動を悪意を意図せずとも実施してしまった従業員本人の性向（性格や行動）に特徴があるか」をリサーチクエスチョンとして設定し，質問紙調査を実施した．意図しない情報漏洩の経験者と非経験者の性向の比較により，従業員個人の性向を考慮した効果的な情報セキュリティ対策の実施指針を示した．

その結果，(1) 従業員本人の性向のうち，リスクテイキング行動を抑止すること，特に，確信的に敢行してしまう性向を抑止する施策が有効であることが示唆された．また，(2) 職場の情報セキュリティ環境から危険な状況を除外する施策も有効であることが示唆された．さらに，(3) 情報セキュリティ対策を励行する施策は一定の効果が見込まれることは論を待たないが本研究においては有意差が見られず，対策の効果には個人差があることも示唆された．

本研究では分析対象としなかった，テレワーク非実施者との比較は今後実施予定である．また，今回実施した調査には，業務データの機微度区分とその許可状況や業務利用状況に関する設問項目が含まれていたが，それらについては **7** で述べた．これらを用いた検討と本研究の知見などを統合し，より効果的な情報セキュリティ対策の提案を実施していきたい．

第 7 章

私有モバイル端末の業務利用におけるセキュリティ不安全行動としてのリスク補償行動

7.1　はじめに

2015 年から 2016 年にかけて，テレワークのうち私有の端末を業務に用いる BYOD（Bring Your Own Device）について，企業からの許可のある状態での正しい BYOD で行われているか，もしくは，企業からの許可がないが私有端末を業務利用しているシャドー IT（Shadow IT）として行われているかについて調査した [畑島 2017c]．調査協力者を企業の規約による許可と実施の状況により 3 分類，それぞれの状況で業務に用いるデータを機密度により 4 分類，そして業務データの保存場所を 10 分類した区分を用いて BYOD の実施行動を明らかにした．

7.2　概要と構成

テレワークとは，社員が特定のオフィスに通勤することなく，特定の企業と雇用契約を結ぶワークスタイルである．日本では，災害対策や地域活性化，ワーク・ライフ・バランスの向上などを目的に，政府が成長戦略としてテレワークを推進している．近年では，個人所有の高性能端末や通信環境が普及し，個人のモバイル端末が業務に利用できるようになった．個人所有のモバイル端末を労働協約の範囲内で利用することを BYOD，BYOD 以外の状況で個人所有のモバイル端末を利用することをシャドー IT と呼ぶ．社員が自分

の好きな端末を業務に使えるようになると，ちょっとした作業をオフタイムに行えるようになるというメリットがある．しかし，モバイルデバイス管理（MDM : Mobile Device Management）などのアプリケーションを一定のルールに従って導入すると，機能制限が発生するために個人所有の端末を自由に使えなくなるというデメリットもある．

本研究は，従業員の社内規則に対する行動意識と情報セキュリティ遵守のためのルールとの関係を明らかにすることを動機 [畑島 2016a][畑島 2016b] として，モバイルワークを導入・管理・運用する際に，ステークホルダがメリット・デメリットを考慮できるように，人間の行動から情報セキュリティリスクを調査した．なお，本研究では企業側の観点ではなく従業員自身の観点から従業員の行動に着目した．そのため，「従業員が利用しているネットワークの種類」や「従業員が働いている場所」など，企業側の観点からの分析は除外した．

7.3 関連研究

Weeger[Weeger2014] は，BYOD の行動モデリングと構造分析について研究した．そして，BYOD を導入する際の意思決定とリスク認知のバランスを考慮したモデルを提案した．菅野 [菅野 2010] らは，情報セキュリティを阻害する要因として，情報システム管理者と従業員の意識と行動に着目した．その結果，企業の従業員には 3 種類のセキュリティ行動があることを発見した．竹村 [竹村 2015] らは，個人の精神的要因に起因する行動を明らかにするため，アンケートを実施した．彼らは，直接効果，間接効果，工場全体の効率の 3 つの要因を考慮し，構造方程式モデリング（SEM: Structural Equation Modeling. 共分散構造分析とも呼ばれる.）により求めた．そして，情報漏洩を抑制するためには，不正を許容する組織の雰囲気を改善することが最も効果的であることを明らかにした．情報セキュリティの行動科学の観点から，セキュリティポリシーの遵守を説明する研究（例えば，Bulgurcu ら [Bulguru2010]，Ifinedo[Ifnedo2012]）が多数報告されている．

7.4 質問紙

質問紙は付録 Ⅲ-2 の通りである．従業員数 100 人以上の企業に所属し，個人所有のモバイル端末を業務で使用している人を対象に調査した．スクリーニングのため，「あなたは個人所有のモバイル端末を，ご自身の業務に利用されますか．(SQ1)」と質問した．その後，「あなたは次のモバイル端末を何台お持ちですか？会社などから支給・貸与された端末は含みません．(Q1)」と所有台数を質問したあと，前問で「仕事にも利用する」と回

答した人に「私有モバイル端末を仕事に利用することについて，あなたの職場では，どのようなとり決めになっていますか．(Q2)」と尋ね，「あなた自身の，私有モバイル端末を使ったモバイルワークの実施方法は以下のどれに近いですか.」(Q3) と尋ねた．そして「あなたが私有モバイル端末を使ってモバイルワークをするときに利用する情報は，以下のどんな場所に保存されていますか．(Q4)」と，業務データの保存場所を複数回答で尋ねた．最後に Q5 で，「あなたは，私有端末を使ったモバイルワークで以下のそれぞれの情報を扱うことがありますか.」として，機密度による 4 区分のデータ（「個人に関する情報（Q5_1)」，「機密性の高い情報（Q5_2)」，「機密性の低い業務情報（Q5_3)」，「業務に関する公開情報（Q5_4)」）の処理頻度を尋ねた．Q5 の回答選択肢は，「A：とてもよく扱う」，「B：よく扱う」，「C：扱う」，「D：どちらとも言えない」，「E：扱わない」「F：あまり扱わない」，「G：まったく扱わない」であった．

7.5 分析

調査はインターネット調査業者に依頼し 2015 年 3 月 9 日から 12 日にかけて行い，619 件の有効回答を得た．

7.5.1 回答者の分類（Q3）

表 7.1 は，Q3「あなた自身の，私有モバイル端末を使ったモバイルワークの実施方法は以下のどれに近いですか.」への回答をまとめたものである．最初の項目で「会社の規約通りに実施している（Q3(1)）」と回答したのは 295 名であり，回答全体の 47.7% の人が会社の規則に従って私物のデバイスを使用していることがわかった．この利用形態は BYOD に分類される．

一方，「会社に規約があるが，自分の判断で実施している（Q3(2)）」と回答したのは 65 名であり，10.5% が，社内で禁止されている場合でも，個人所有の端末で業務を実施していると回答があった．

そして「会社に規約が無いので，自分の判断で実施している（Q3(3)）」と回答したのは 259 名であり，41.8% が個人所有の端末を使用して業務を行っていると回答があった．Q3(2) と Q3(3) の利用形態は，シャドー IT に分類される．

表 7.1　私有モバイル端末を使ったモバイルワークの実施方法（Q3)

選択肢	設問文	n	%
Q3(1)	会社の規約通りに実施している	295	47.7%
Q3(2)	会社に規約があるが，自分の判断で実施している	65	10.5%
Q3(3)	会社に規約が無いので，自分の判断で実施している	259	41.8%
	合計	619	100.0%

7.5.2　業務データを保存している場所

表 7.2 は，Q4「あなたがテレワーク・モバイルワークに利用する業務情報は，次のどんな場所に保存されていますか.」に対して複数回答を求めた結果である．Q3 の回答結果による 3 区分それぞれにおける業務データの保存場所数の平均は，10 カ所の選択肢を設定したうち，Q3(1) は 2.73 箇所，Q3(2) は 2.49 箇所，Q3(3) は 2.72 箇所であった.

表 7.2 の Q3(1) の列を参照すると，私有モバイル端末を使った業務を，会社から許可された通りに実施している人の業務データの保存場所は，社内の情報システム (49.5%) が一番多く，二番目に多かったのが会社が用意したクラウドサービス (30.5%)，三番目が私有モバイル端末 (26.4%) であることがわかった.

また Q3(2) の列を参照すると，私有モバイル端末を使った業務を，会社の規約はあるが自分の判断で実施している人の業務データの保存場所は，私有モバイル端末 (38.5%) が一番多く，二番目に多かったのが自宅 (24.6%)，三番目が社内の情報システム (21.5%) であることがわかった.

最後に Q3(3) の列を参照すると，私有モバイル端末を使った業務を，会社の規約がないので自分の判断で実施している人の業務データの保存場所は，私有モバイル端末 (35.9%) が一番多く，二番目に多かったのが社内の情報システム (32.8%)，三番目が自宅 (24.7%) であることがわかった．また，この群に属する 10 %以上の人が私有の保存環境である（個人用の）クラウドストレージ（5 位，17.0%），外部記憶装置（6 位，14.7%）を利用していることがわかった.

ここから，私有モバイル端末の業務利用を自身の判断で行っている人（Q3(2) と Q3(3)）が，私有モバイル端末に業務データを保存している人（それぞれ 38.5%，35.9%）が最も多いことや，自宅にも業務データを保存する人（それぞれ 24.6%，24.7%）が多いことがわかった.

表 7.2　業務利用するデータの保存場所（Q4）（$N = 619$）

	Q3(1)		Q3(2)		Q3(3)	
Q4	%	#	%	#	%	#
社内の情報システム	49.5	1	21.5	3	32.8	2
会社が用意したクラウドサービス	30.5	2	18.5	5	13.1	7
社内の情報を保存した外部記憶媒体 (USB メモリなど)	21.4	4	20.0	4	20.5	4
私有モバイル端末	26.4	3	38.5	1	35.9	1
クラウドストレージ (Dropbox，OneDrive，Google Drive など)	7.1	8	7.7	7	17.0	5
クラウドサービス (Gmail，Evernote など)	8.8	7	10.8	6	14.7	6
ファイル転送サービス (宅ふぁいる便など)	7.1	8	3.1	8	6.2	8
お客様・取引先など，自社以外の情報システム	14.7	6	1.5	10	5.0	9
自宅	15.3	5	24.6	2	24.7	3
その他（自由回答）	1.7	10	3.1	8	2.7	10
保存箇所（複数回答）合計		804		162		704
回答者数（n）		295		65		259
平均回答箇所数		2.73		2.49		2.72

さらに，Q3 の 3 パターンの業務利用形態に共通して 4 番目に利用が多かったのが USB メモリなどの外部記憶装置（順に 21.4%，20.0%，20.5%）であり，全グループで 20 %を超える人が保存していることがわかった．

7.5.3　私用モバイル端末の許可状態別業務利用形態（Q3) と業務データ取り扱い状況（Q5) の関係分析

Q3 によって区分した会社の規約による私有モバイル端末の業務利用形態と Q5 によって得られた 4 つの機密度区分データそれぞれについての利用頻度のクロス集計表 4 件に対する分析結果を述べる．データ分析には統計分析ソフトウェア R version 3.2.0 を用いた．

7.5.3.1　カイ二乗検定

まず，表 7.3，表 7.5，表 7.7，表 7.8 のように Q3 と Q5 の回答をクロス集計し，カイ二乗検定を実施した．その結果，5% 水準で有意であった表 7.3，表 7.5，表 7.8 については

残差分析に進んだ．一方で表 7.7 で表した「私有モバイル端末の業務利用規約ごとの端末利用形態」と「テレワークにおける機密性の低い業務データの取り扱い頻度」の間には有意差は見られなかった．

7.5.3.2　業務許可形態（Q3) と業務データ取り扱い状況（Q5) の残差分析

次に，表 7.3，表 7.5，表 7.8 において残差分析を行った結果を，順に表 7.4，表 7.6，表 7.9 に示す．残差分析によって，各表における回答者の利用形態（Q3(1)，Q3(2)，Q3(3) の 3 群）について，扱う業務データの機密度（Q5_1，Q5_2，Q5_3，Q5_4 の 4 問の設問）それぞれについて，私有モバイル端末での取り扱い頻度（選択肢 A から G）のうちどの選択肢を選んだ回答が有意に多いもしくは有意に少ないかを分析する．分析結果である表 7.4，表 7.6，表 7.9 には，それぞれ調整済み標準化残差が示されており，絶対値が 1.96 以上であれば，5% 水準で有意である．結果が正の値であれば，期待値よりも有意に多い回答数であったことが示され，逆に結果が負の値である場合，そのセルには期待値よりも有意に少ない回答数であったと示される．

上記で得られた有意な回答選択肢について，私用モバイル端末の許可形態別業務利用形態（Q3 の各設問）の区分ごとに考察する．

表 7.3 と表 7.4 は Q5_1「個人に関する情報」を，Q3 で 3 群に分割した回答者（Q3(1),Q3(2),Q3(3)）が，私有モバイル端末でどのような頻度で扱っているのかを表す度数表および調整済み標準化残差の表である．表 7.4 を参照すると，Q3(1) は選択肢 A，B，C が有意に多いことがわかった．また，Q3(2) では選択肢 F が有意に多いことがわかった．そして Q3(3) については，選択肢 A，B，C が有意に少なく，選択肢 G が有意に多いことがわかった．

表 7.5 と表 7.6 は Q5_2「機密性の高い情報」を，Q3 で 3 群に分けた回答者（Q3(1),Q3(2),Q3(3)）が，私有モバイル端末でどのような頻度で扱っているのかを表す度数表および調整済み標準化残差の表である．表 7.6 を参照すると，Q3(1) は選択肢 A，C が有意に多く，選択肢 E が有意に少ないことがわかった．また，Q3(2) では有意な差がなかった．そして Q3(3) については，選択肢 A，B，C が有意に少なく，選択肢 E が有意に多いことがわかった．

表 7.8 と表 7.9 は Q5_4「業務に関する公開情報」を，Q3 で 3 群に分けた回答者（Q3(1),Q3(2),Q3(3)）が，私有モバイル端末でどのような頻度で扱っているのかを表す度数表および調整済み標準化残差の表である．表 7.9 を参照すると，Q3(1) は選択肢 B が有意に多く，選択肢 G が有意に少ないことがわかった．また，Q3(2) は選択肢 A が有意に少なく，選択肢 F が有意に多いことがわかった．そして Q3(3) については，選択肢 B が

有意に少なく，選択肢 G が有意に多いことがわかった.

表 7.3　度数・カイ二乗検定：規約に対する行動 3 群（Q3) と「個人に関する情報」の私有モバイル端末での取り扱い頻度（Q5_1) のクロス集計

		n	A	B	C	D	E	F	G
Q3(1)	会社の規約通りに実施している	295	20	38	69	30	41	30	67
Q3(2)	会社に規約があるが,自分の判断で実施している	65	1	3	14	11	11	14	11
Q3(3)	会社に規約が無いので,自分の判断で実施している	259	6	14	41	39	51	34	74

$$\chi^2(12) = 37.25, p < .001 * **$$

表 7.4　分散分析・調整済み標準化残差：規約と行動の 3 群別（Q3) の,「個人に関する情報」の私有モバイル端末での取り扱い頻度（Q5_1) のクロス集計

		A	B	C	D	E	F	G
Q3(1)	会社の規約通りに実施している	2.81	3.33	1.99	-1.95	-1.75	-1.74	-1.02
Q3(2)	会社に規約があるが,自分の判断で実施している	-1.18	-1.28	0.32	1.02	0.07	2.23	-1.51
Q3(3)	会社に規約が無いので,自分の判断で実施している	-2.11	-2.58	-2.22	1.34	1.73	0.34	1.97

表 7.5　度数・カイ二乗検定：規約に対する行動 3 群（Q3) と「機密性の高い情報」の私有モバイル端末での取り扱い頻度（Q5_2) のクロス集計

		n	A	B	C	D	E	F	G
Q3(1)	会社の規約通りに実施している	295	15	33	76	47	38	27	59
Q3(2)	会社に規約があるが,自分の判断で実施している	65	1	9	14	10	6	11	14
Q3(3)	会社に規約が無いので,自分の判断で実施している	259	3	13	45	41	59	32	66

$$\chi^2(12) = 35.52, p < .001 * **$$

表 7.6　分散分析・調整済み標準化残差：規約と行動の 3 群別（Q3) の,「機密性の低い情報」の私有モバイル端末での取り扱い頻度（Q5_2) のクロス集計

		A	B	C	D	E	F	G
Q3(1)	会社の規約通りに実施している	2.77	1.92	2.27	0.07	-2.37	-1.62	-1.40
Q3(2)	会社に規約があるが,自分の判断で実施している	-0.76	1.49	-0.06	-0.10	-1.70	1.51	-0.19
Q3(3)	会社に規約が無いので,自分の判断で実施している	-2.34	-2.87	-2.27	0.00	3.48	0.70	1.53

表 7.7　度数・カイ二乗検定：規約に対する行動 3 群（Q3) と「機密性の低い情報」の私有モバイル端末での取り扱い頻度（Q5_3) のクロス集計

		n	A	B	C	D	E	F	G
Q3(1)	会社の規約通りに 実施している	295	18	42	99	53	27	20	36
Q3(2)	会社に規約があるが, 自分の判断で実施している	65	0	7	23	11	8	7	9
Q3(3)	会社に規約が無いので, 自分の判断で実施している	259	9	25	92	39	32	22	40

$$\chi^2(12) = 12.50, n.s.(p = .406)$$

表 7.8　度数・カイ二乗検定：規約に対する行動 3 群（Q3) と「業務に関する公開情報」の私有モバイル端末での取り扱い頻度（Q5_4) のクロス集計

		n	A	B	C	D	E	F	G
Q3(1)	会社の規約通りに 実施している	295	20	44	101	50	29	18	33
Q3(2)	会社に規約があるが, 自分の判断で実施している	65	0	7	23	16	3	8	8
Q3(3)	会社に規約が無いので, 自分の判断で実施している	259	15	22	76	54	35	11	46

$$\chi^2(12) = 26.95, p < .001 * **$$

表 7.9　分散分析・調整済み標準化残差：規約と行動の 3 群別（Q3) の,「業務に関する公開情報」の私有モバイル端末での取り扱い頻度（Q5_4) のクロス集計

		A	B	C	D	E	F	G
Q3(1)	会社の規約通りに 実施している	1.16	2.30	0.98	-1.46	-0.76	0.12	-1.96
Q3(2)	会社に規約があるが, 自分の判断で実施している	-2.09	-0.27	0.56	1.13	-1.70	2.28	-0.43
Q3(3)	会社に規約が無いので, 自分の判断で実施している	0.13	-2.16	-1.34	0.78	1.83	-1.54	2.25

7.6　考察と議論

7.6.1　規約の通りに私有モバイル端末を業務利用する人：Q3(1)

まず，業務データの保存場所のついては，**7.5.2** で示した表 7.2 の Q3(1) の列を参照すると，会社の情報システム（49.5%) や会社が用意したクラウドサービス (30.5%) が利用場所の 1 位と 2 位であり，会社のガバナンスが効いた場所への保存が上位を占めている．しかしその一方で，私有モバイル端末への保存（26.4%）や外部記憶媒体（21.4%）自宅での保存（15.3%）もそれぞれ 3 位，4 位，5 位に位置している．

t

上記により考察すると，この群の利用者は個人に関する業務データや機密性が高い情報を私有モバイル端末で扱う傾向があるが，会社のガバナンス効いている保存場所での取り扱いが多いものの，端末内や自宅といったガバナンスが効いていない保存場所を使っても取り扱う恐れがあることがわかった．これは，本研究の当時は **6.2** で述べたように，会社と私有モバイル端末間のデータ通信に係わるリスクへの対応策としてセキュリティに対応するシステムソリューションが費用対効果を確認できないとして導入が進まず，規約や人的側面による対処がされていたことに係わるとみられる [日経 BP2013a][日経 BP2013b]．テレワークにおける個人に関する情報の取扱いは，2022 年に発行された最新のテレワークセキュリティガイドライン（第 5 版）においても注意喚起される継続的なセキュリティ上の課題である [総務省テレワークセキュリティ]．この状態は業務データの漏洩というセキュリティインシデントの発生要因なるが，これの説明はリスク補償 (risk compensation) 行動により可能であると考える．リスク補償とは，自分の置かれた状況がより危険 になったとき，あるいはより安全になったときに，人々は感知したリスクのレベルに応じて自分の行動を調整するという人間行動の理論である [Hedlund2000]．一例として Pearman ら [Pearman2016] は，ウイルス対策ソフトをインストールしている人は，OS のアップデートを無効にしたり，ソフトウェアのアップデートを延期したり，拒否したりする傾向が強いと指摘している．

本研究では，図 7.1 に示すように，まず，(1) 従業員は業務データを処理する際にルールや規則に従っていると認識しているためにセキュリティ事故のリスクを低く見積もっているとみられる．そのため，(2) 個人に関する情報のような機密性の高い業務データを取扱う際にもリスクレベルが低いと考え，セキュリティインシデントのリスクレベルが増加するようなリスク補償行動をしてしまっていると考えられる．

リスク補償の理論を情報セキュリティに応用した検討は今後の課題である．ただし，この群の回答者は個人に関する情報であっても正当な業務として取り扱っている可能性もあることは考慮が必要な事項である．

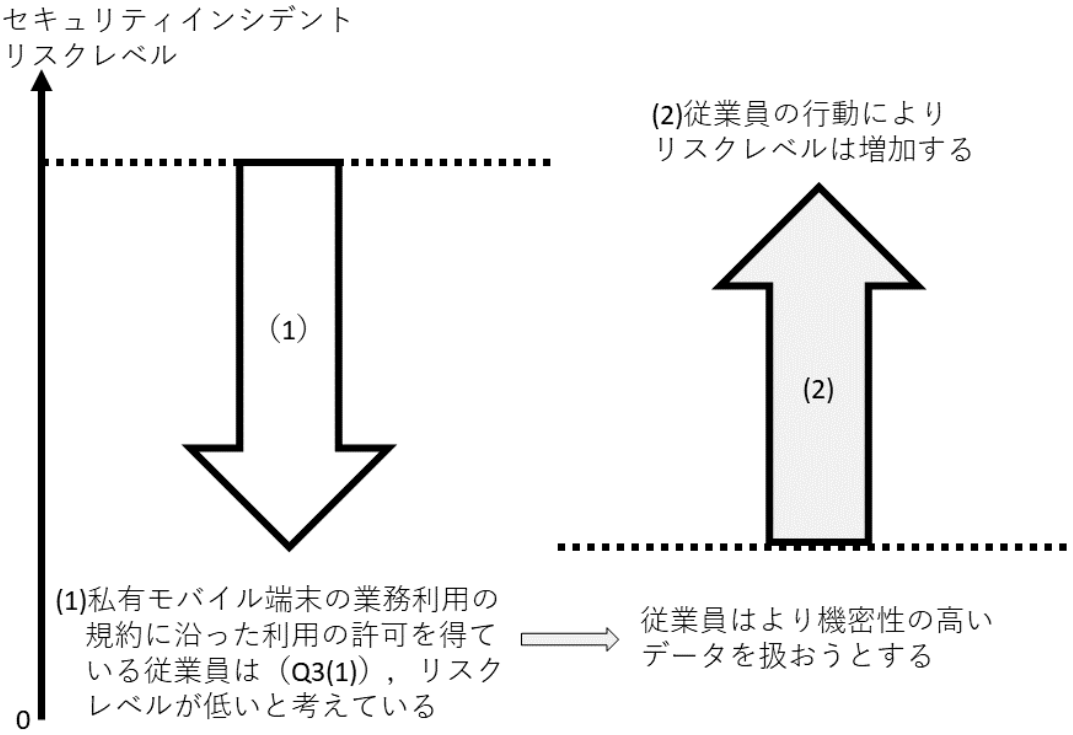

図 7.1　リスク補償行動

7.6.2　規約があるが自分の判断で私有モバイル端末を業務利用する人：Q3(2)

まず，業務データの保存場所のついては，**7.5.2** で示した表 7.2 の Q3(2) の列を参照すると，私有モバイル端末（38.5%）が最も多く，次いで自宅（24.6%），社内の情報システム（21.5%）の順となっている．

業務に関する個人データについては（Q5_1；表 7.4），選択肢 F（あまり利用しない）の回答数が有意であった．また，機密性の高い情報（Q5_2；表 7.6）では，有意差は見られ

なかった．業務に関する公開情報（Q5_3；表 7.9）では，選択肢 A（とてもよく扱う）の回答が有意に少なく，選択肢 F（あまり扱わない）の回答が有意に多かった．

このグループの参加者は規約があるが自分の判断で利用している．つまり利用禁止されているにもかかわらず利用していたり，規約を意図的に逸脱して，私有モバイル端末で業務データを取り扱っている．その結果，個人に関する業務データで選択肢 F（あまり扱わない）の回答が有意に多かったように，私有モバイル端末による業務データ取り扱いのリスクを認識した上で，リスクに配慮しつつも規約を逸脱して業務を行っていると考えられる．また，この群はグレーゾーンで業務しているため，リスクを取る行動の詳細を明らかにしないという対応をしていることも想定される．

7.6.3 規約が無いので自分の判断で私有モバイル端末を業務利用する人：Q3(3)

まず，業務データの保存場所のついては，**7.5.2** で示した表 7.2 の Q3(3) の列を参照すると，私有モバイル端末（35.9%）が 1 位であり，社内の情報システム（32.8%），自宅（24.7%）と続いた．また，会社が用意したクラウドサービスの利用（13.1%）は 3 群の中で一番少なかった．

個人に関する業務データについては（Q5_1；表 7.4），機密性の高い情報（Q5_2；表 7.6），業務に関する公開情報（Q5_3；表 7.9）の傾向は **7.6.1** で述べた結果とは対照的であった．個人に関する業務データについては（Q5_1；表 7.4）と機密性の高い情報（Q5_2；表 7.6）では，「扱う」とする選択肢（A，B，C）の回答が有意に少なかった．また，漏えい時のリスクの高いデータは扱わないことを有意な差で回答している．しかし，この群も 7.6.2 で述べた群と同様に，リスクを取る行動の詳細を明らかにしないという対応をしていることも想定される．

7.7 まとめ

会社の規約を守る人は，セキュリティ事故のリスクを低く見積り，より機密度の高いデータを取り扱う，リスク補償行動の傾向がみられると考えられる．この行動は不安全行動の一種であり，情報セキュリティインシデントが発生した場合，情報セキュリティリスクがより高くなることが見込まれる．ただし，個人に関する情報の取扱であっても企業のルールや規則を遵守した正当な業務として取り扱っている可能性もあることは本研究の制約事項である．

このような人間の行動を考慮した情報セキュリティの研究は，より安全なインターネット社会の実現に貢献すると考えられる．

第 8 章

第 III 部のまとめ

第 Ⅲ 部では，インターネットユーザのセキュリティ不安全行動について述べた．セキュリティ不安全行動とはセキュリティ対策が求められているにもかかわらず，その対策行動から外れた行動のことである．この行動はセキュリティインシデントの引き起こす好ましくない行動である．

本研究では，テレワークを題材として不安全行動を解明することにより，インターネット利用者の利用行動の測定と解明を行った．**6** ではテレワーク全般を対象とした．**7** の研究を実施していた 2010 年代中盤は，テレワークの実施形態として，BYOD（Bring Your Own Device：私有端末の業務利用）が注目されていたため，研究対象とした．

6 における，テレワーカーによるテレワーク時の意図しない情報漏洩というセキュリティ不安全行動がテレワーカーの性格によって発生の仕方が異なるかの解明については，以下の知見が得られた．

1. 確信的に敢行してしまう性向を抑止する施策が効果的
2. テレワークに関する情報セキュリティ対策であっても，従業員が所属する職場のセキュリティ環境を危険度の低い状態にする施策が有効
3. 情報セキュリティ対策の実施を促す施策には一定の効果があることは論を待たないが，本研究では有意な差は見られず，対策効果に個人差があることが示唆される

続いて，**7** における，規約の整備状況および許可状況と業務実施状況の分析によるセキュリティ不安全行動がリスク補償行動によって説明可能であることについては，以下の知見が得られた．

1. 会社の規約を守る人は，その規約に従うがゆえに，ルールや規則を遵守しているた

め，セキュリティ事故のリスクを低く見積り，より機密度の高いデータを取り扱う傾向がある．

この行動は不安全行動の一種であり，情報セキュリティインシデントが発生した場合，情報セキュリティリスクがより高くなることが見込まれる．

III-1　第 6 章の質問紙

Q1 あなたが仕事全般について持っている意識についてお伺いします．項目を読んであなた自身に当てはまる項目をお選びください．（4 件法）

1. 私は今の仕事に興味を持っている
2. 私は仕事を通じて全体として成長した
3. 私はこの会社につとめていることを誇らしく思う
4. 今の仕事は私に適している
5. 社外の人々は，私の仕事を尊敬に値する仕事だと思っている
6. 私の仕事は「やり甲斐のある仕事をした」という感じが得られる
7. 私は職場のみんなに認められている
8. 私はよい仕事をして昇進できると思う
9. 私はこの会社にいて，着実な人生設計がたてられる
10. 私の会社ではみんなの意見や要望が取り上げられている
11. 私の会社では，昇進や昇格が公平に行われる
12. 私の会社では各部門の協力体制がうまくできている
13. 私の会社の幹部は幹部として仕事にあかるい
14. 私の会社では，休憩時間は自分の思うように利用することができる
15. 私の会社はみんなの福利厚生に努力している
16. 私の会社では事業計画や会社の発展の様子を従業員に知らせてくれる
17. 残業もふくめて今の労働時間は適当だと思う
18. 私と顧客（仕事相手）との間には信頼関係が成り立っている
19. 私と私の上司の間には適切な距離がたもたれている
20. 私の上司は仕事以外の個人的な事で相談にのってくれる
21. 私の職場の人間関係はよい
22. 私の同僚は仕事以外の個人的な相談にのってくれる
23. 私の職場のチームワークはよい
24. 私は，私のする仕事について顧客（仕事相手）から感謝されている
25. 私と同僚の間には適切な距離がたもたれている
26. 私の上司は，仕事における指導監督ぶりが適切である
27. 私の同僚は仕事のうえで協力的である

Q2 それぞれの項目について，あなた自身に当てはまりますか．項目を読んであなた自身に当てはまる項目をお選びください．（5 件法）

1. 私は，人を喜ばせるために，自分の意見や行動を変える
2. 私は，人とうまくやったり好かれるために，人が望むように振舞おうとする傾向がある
3. 私は，励ましがなければ自分の仕事を続けることが困難である
4. 私は，自分の考えがグループの意見と異なるとき，自分の考えを言いにくい
5. 私は，友人が自分を支持してくれることがわかっているときだけ，すすんで議論に加わる
6. 私は，人からよく思われるために自分を変えようとは思わない
7. 私は，自分の進む道を必ずしも自分で決めていないと思うことが，時々ある
8. 私は，パーティーのような社交の場では，他人のいやがることをしたり，言ったりしないよう注意している
9. 私は，自分の行動を弁解したり，謝罪する必要があると感じることはめったにない
10. 私にとって，人との様々な交流の中で,”上手に”振舞うことは重要ではない
11. 私はたいてい，人が反対しても自分の立場を変えない
12. 重要人物に取り入るのは賢明である
13. どれほど良い人間かで，友人の数が決まる
14. 最もうまい人の扱い方は，相手の考えに同意したり，相手の喜ぶようなことを言うことである
15. たとえ自分のほうが正しいとわかっていても，他人からみれば間違っていると思われるようなことは，人前ですべきではない
16. 人と接するときは，積極的であるより，控え目なほうがよい
17. 私は，同じ状況であっても，相手が違えば異なる行動をとる
18. 誰かが私のことをあまり良く思っていないことがわかったら，次にその人に会ったとき，印象を良くするためにできるだけのことをする 1
19. 私に対してどんな批判があろうと，私はそれを受け入れることができる 2
20. 私は，どうすべきかをサイコロで決めたいと思うことがよくある

※逆転項目：6，9，10，11，19

Q3 次のそれぞれの項目は，あなた自身の行動や価値観にどれくらい当てはまりますか．（5 件法）

1. 歩行時，道路を斜め横断する
2. 歩行時，赤信号でも車が来なければ渡る
3. 歩行時，信号のないところで道路を横断する
4. 歩きながら携帯電話でメールする
5. 駆け込み乗車をする
6. 夜，無点灯で自転車に乗る
7. 大事な約束を破る
8. 仮病をよく使う
9. 会議など，重要度の高い決められた時間に遅刻する
10. ギャンブルが好きだ
11. もし自分の街にカジノがあったら行ってみたい
12. 大金をギャンブルにつぎ込む人の気持ちがわかる
13. 何事も「賭け」がないとつまらない
14. ギャンブルは有害だと思う

Q4 それぞれの項目について，あなた自身に当てはまりますか．項目を読んであなた自身に当てはまる項目をお選びください．（7 件法）

1. いつも何かの目標を持っていたい
2. ものごとは他の人よりうまくやりたい
3. 決められた仕事の中でも個性をいかしてやりたい
4. 人と競争することより，人とくらべることができないようなことをして自分をいかしたい
5. 他人と競争して勝つとうれしい
6. ちょっとした工夫をすることが好きだ
7. 人に勝つことより，自分なりに一生懸命やることが大事だと思う
8. みんなに喜んでもらえるすばらしいことがしたい
9. 競争相手に負けるのはくやしい
10. 何でも手がけたことは最善をつくしたい
11. どうしても私は人より優れていたいと思う
12. 何か小さなことでも自分にしかできないことをしてみたいと思う

13. 勉強や仕事を努力するのは，他の人に負けないためだ
14. 結果は気にしないで何かを一生懸命やってみたい
15. 今の社会では，強いものが出世し，勝ち抜くものだ
16. いろいろなことを学んで自分を深めたい
17. 就職する会社は社会で高く評価されるところを選びたい
18. 成功するということは，名誉や地位を得ることだ
19. 今日一日何をしようかと考えるのはたのしい
20. 社会の高い地位をめざすことは重要だと思う
21. 難しいことでも自分なりに努力してやってみようと思う
22. 世に出て出世したいと強く願っている
23. こういうことがしたいなあと考えるとわくわくする

Q5 あなたの 1 週間の勤務時間はどれくらいですか．そのうちテレワーク・モバイルワークをする時間はどれくらいですか．ここ 3 ヵ月ほどのおおよその平均をお答えください．

勤務時間	【 】時間	【 】 分
在宅勤務		【 】 分
モバイルワーク		【 】 分
施設利用型勤務		【 】 分
合計		【 】 分

Q6 Q5 でお答えいただいたテレワーク・モバイルワークの勤務時間を，以下のような端末にわけて考えると，それぞれどれくらいの勤務時間になりますか．

1 週間合計のテレワーク・モバイルワーク勤務時間

会社支給の端末	【 】 分
個人所有の端末	【 】 分
合計	【 】 分

Q7 あなたがテレワーク・モバイルワークを行うときについて次のことをどう思いますか．あなたのお気持ちにもっとも近いものをお選びください．（5 件法）

1. 仕事関係の人に邪魔されず集中して仕事ができること
2. 通勤で疲弊しないこと
3. すきま時間も業務に利用できること
4. アプトプットした成果によって評価が決まること
5. 仕事の進め方に自分の裁量があること
6. オフィスワークとテレワーク・モバイルワークで評価基準が変わらない
7. フェイス・トゥ・フェイスのコミュニケーションができる

Q8 あなたがテレワーク・モバイルワークを行うときについて次のことをどう思いますか．あなたのお気持ちにもっとも近いものをお選びください．（5 件法）

1. 勤務形態が許可されるために申請が必要
2. 当日の始業時・終業時に上長に連絡が必要
3. 当日の成果物をあらかじめ設定する
4. テレワーク・モバイルワークで使うために端末の準備が必要
5. テレワーク・モバイルワークで使うためにセキュリティ対策が必要

Q9 あなた自身は，次の情報セキュリティ対策を実施していますか．（5 件法）

1. サービスごとに変えるといったパスワード管理をしている
2. 信頼できないサイトでクレジットカード情報を入力しない
3. 作業に使う端末で使う OS やソフトを常に最新の状態にしている
4. 作業に使う端末にウイルス対策ソフトをインストールしている
5. 業務データを故意に流出させようとしている
6. 定期的に情報セキュリティ対策を自主点検している
7. 定期的に情報セキュリティに関する教育・啓発活動に参加している
8. 情報セキュリティ事故の発生時の連絡体制を確認している
9. 悪意のあるソフトウェアが配布されているサイトにはアクセスしない
10. 端末に業務に不要なデバイスを接続しない
11. 端末や記録媒体の紛失・盗難について対策を行っている
12. 自宅や外で使う業務情報の原本を安全な場所に保存する
13. 機密性が求められる電子データの送受信時には暗号化する

14. 興味がある情報ならば怪しげだと思うサイトでもアクセスする
15. 公共の場所などで作業を行う場合，端末の画面にプライバシーフィルターを装着したり作業場所を選んだりして，画面の覗き見防止に努める
16. 社外から社内システムにアクセスするための利用者認証情報（パスワード，IC カード等）を適正に管理する
17. インターネット経由で社内システムにアクセスする際，安全性の高い通信手段のみを用いる（例：個人認証がない公衆 Wi-Fi を利用しない）

※逆転項目：5，14

Q10 あなたがおつとめの会社は，以下のことがどれくらい当てはまりますか.（7 件法）

1. 社内の開発物や重要な情報を誰にも知られずに閲覧・編集できる
2. 社員の大半のパソコンでセキュリティ設定が管理されず，社員任せになっている
3. 職場で頻繁に情報セキュリティのルール違反が繰り返されている
4. システム管理がずさんで，顧客情報を簡単に持ち出せることを知っている

Q11 あなた自身について，以下のそれぞれの項目について，よりよく当てはまるほうをお答えください.（2 件法）

1. 情報セキュリティ事故を起こしてペナルティを受けたことがある
2. 私は意図せず業務データを漏洩させたことがある
3. 私は意図して業務データを漏洩させたことはない

III-2　第 7 章の質問紙

SQ1 あなたは個人所有のモバイル端末を，ご自身の業務に利用されますか

	仕事にも利用する	仕事には利用しない
スマートフォン		
タブレット		
ノート PC		

Q1 あなたは次のモバイル端末を何台お持ちですか？会社などから支給・貸与された端末は含みません

スマートフォン	【 】
タブレット	【 】
ノート PC	【 】
いずれも所有していない	

Q2 私有モバイル端末を仕事に利用することについて，あなたの職場では，どのようなとり決めになっていますか.

1. 利用規約に従うことで許可されている
2. 利用規約があり，業務利用時には専用のアプリケーションを使うことも決められている
3. 利用規約はなく，黙認されている
4. 利用は禁止されている
5. その他

Q3 あなた自身の，私有モバイル端末を使ったモバイルワークの実施方法は以下のどれに近いですか

1. 会社の規約通りに実施している
2. 会社に規約があるが，自分の判断で実施している
3. 会社に規約が無いので，自分の判断で実施している

Q4 あなたが私有モバイル端末を使ってモバイルワークをするときに利用する情報は，以下のどんな場所に保存されていますか．

1. 社内の情報システム
2. 会社が用意したクラウドサービス
3. 社内の情報を保存した外部記憶媒体 (USB メモリなど)
4. 私有モバイル端末
5. クラウドストレージ (Dropbox，OneDrive，Google Drive など)
6. クラウドサービス (Gmail，Evernote など)
7. ファイル転送サービス (宅ふぁいる便など)
8. お客様・取引先など，自社以外の情報システム
9. 自宅
10. その他（自由回答）

Q5 あなたは，私有端末を使ったモバイルワークで以下のそれぞれの情報を扱うことがありますか.

質問	A よてもよく よく扱う	B よく扱う	C 扱う	D どちら とも 言えない	E あまり 扱わない	F 扱わない	G まったく 扱わない
Q5_1 個人に関する 情報							
Q5_2 機密性の高い 情報							
Q5_3 機密性の低い 公開情報							
Q5_4 業務に関する 公開情報							

第 III 部の参考文献

[安達 1998] 安達智子：セールス職者の職務満足感 共分散構造分析を用いた因果モデルの検討，心理学研究，Vol.69, No.3,pp.223–228 (1998).

[インテージ 2017] 株式会社インテージ：品質に対する取り組み—モニターの品質管理，入手先〈https://www.intage.co.jp/service/net/quality-monitor/〉（参照 2017-06-22）.

[植田 1990] 植田 智，吉森 護：日本版 MLAM 承認欲求尺度作成の試み，広島大学教育学部紀要 第一部，No.39, pp.151–156(1990).

[岡野 2016] 岡野祐樹，奥山浩伸：セキュリティルールの違反行動の抑止に関する一考察，情報処理学会論文誌，Vol.58, No.1,pp.258–268 (2016).

[片山 2015] 片山佳則，寺田剛陽，鳥居 悟，津田 宏：ユーザー行動特性分析による個人と組織の IT リスク見える化の試み，2015 年暗号と情報セキュリティシンポジウム，4D1-3(2015).

[国交省 2017a] 国土交通省：テレワーク人口実態調査，入手先〈http://www.mlit.go.jp/crd/daisei/telework/p2.html〉（参照 2017-02-16）.

[国交省 2017b] 国土交通省：テレワーク, 入手先〈http://www.mlit.go.jp/crd/daisei/telework〉（参照 2017-02-16）.

[菅野 2010] 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).

[諏訪 2012] 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).

[総務省 2016a] 総務省：テレワークの意義・効果，入手先〈http://www.soumu.go.jp/mainsosiki/johotsusin/telework/1802801.html〉（参照 2016-05-08）.

[総務省 2016b] 総務省統計局：労働力調査 過去の結果の概要，入手先

〈http://www.stat.go.jp/data/roudou/rireki/gaiyou.htm〉（参照 2016-10-21）.
[総務省テレワークセキュリティ] 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 2023-01-22）.
[竹村 2015] 竹村敏彦，三好祐輔，花村憲一：情報漏えいにつながる行動に関する実証分析，情報処理学会論文誌，Vol.56, No.12,pp.2191–2199 (2015).
[テレワーク 2017] 日本テレワーク協会，入手先〈http://www.japan-telework.or.jp〉（参照 2017-02-16）.
[内閣官房 2016] 内閣官房高度情報通信ネットワーク社会推進戦略本部：世界最先端 IT 国家創造宣言 2016 年 5 月 20 日改訂版 (2016).
[日経 BP2013a] 日経 BP 社：企業ネット実態調査 2013，日経コミュニケーション，2013 年 10 月号，pp.14–17 (2013).
[日経 BP2013b] 日経 BP 社：ネットワークの実態調査 2013 どこまで許す？ BYOD，日経 NETWORK 2013 年 7 月号，pp.38–47(2013).
[芳賀 2007] 芳賀 繁：事故と安全の心理学 リスクとヒューマンエラー，東京大学出版会 (2007).
[畑島 2016a] 畑島 隆，坂本泰久：私有端末を用いたモバイルワークにおける行動モデルの検討，情報科学技術フォーラム講演論文集，Vol.15, RO-003 (2016).
[畑島 2016b] 畑島 隆，坂本泰久：私有端末によるモバイルワークに関する行動意識調査 － 規約制定の情報漏えい対策効果，信学技報，Vol.115, No.486, pp.109–114 (2016).
[畑島 2016c] 畑島 隆，坂本泰久：テレワークにおける情報セキュリティ不安全行動に関する検討，信学技報，Vol.116, No.138,pp.11–16 (2016).
[畑島 2017a] 畑島 隆，坂本泰久：テレワークに関する行動意識調査 － 規約制定の情報漏洩対策効果，信学技報，Vol.116, No.488,pp.195–200 (2017).
[畑島 2017b] 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).
[畑島 2017c] Hatashima, T., Sakamoto, Y.: Study on effect of company rules and regulations in telework involving personal devices,, IEICE Transactions on Information and Systems, Volume E100-D, Issue 10, pp. 2458–2461, DOI:10.1587/transinf.2016OFL0001 (2017).
[浜津 2015] 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).
[堀 2001] 堀 洋道，山本眞理子：心理測定尺度集 I，サイエンス社 (2001).
[堀野 1987] 堀野 緑：達成動機の構成因子の分析：達成動機の概念の再検討，教育心理学

研究，Vol.35, No.2, pp.148–154(1987).

[マクロミル 2017] 株式会社マクロミル：モニタの品質管理ポリシー，入手先〈https://www.macromill.com/advantage/monitorpolicy.html〉（参照 2017-06-22）.

[三浦 2015] 三浦麻子，小林哲郎：オンライン調査モニタの Satisfice に関する実験的研究，社会心理学研究，Vol.31, No.1, pp.1–12(2015).

[宮本 2014] 宮本聡介，宇井美代子：質問紙調査と心理測定尺度計画から実施・解析まで，サイエンス社 (2014).

[村田 2008] 村田厚生：ヒューマン・エラーの科学，日刊工業新聞社 (2008).

[和田 2012] 和田一成，臼井伸之介，篠原一光，神田幸治，中村隆宏，村上幸史，太刀掛俊之，山田尚子：違反行動の生起における課題遂行コストとリスク認知の影響，労働科学，Vol.88,No.1, pp.1–12 (2012).

[森泉 2011] 森泉慎吾，臼井伸之介：リスクテイキング行動尺度の信頼性・妥当性の再検討，労働科学，Vol.87, No.6, pp.211–225(2011).

[Bulguru2010] 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).

[Hedlund2000] J. Hedlund, Risky business: safety regulations, risk compensation, and individual behavior, Injury Prevention, vol.6, no.2, pp.82–89,June 2000. DOI: 10.1136/ip.6.2.82 (2000).

[Ifnedo2012] Ifinedo, P.: Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory, Comput. Secur., vol.31, no.1, pp.83–95. DOI: 10.1016/j.cose.2011.10.007 (2012).

[Ifnedo2014] 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).

[IPA2014] 情報処理推進機構：「組織内部者の不正行為によるインシデント調査」報告書の公開，入手先〈https://www.ipa.go.jp/security/fy23/reports/insider/index.html〉（参照 2014-08-25）.

[IPA2016] 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）.

[IPA2017] 情報処理推進機構：日本的経営と情報セキュリティ研究会報告書，入手先〈http://www.ipa.go.jp/security/fy24/reports/nihontekikeiei/index.html〉（参照 2017-02-16）.

[Kruger2006] Kruger, H.A. and Kearney, W.D.: A prototype for assessing information security awareness, Comput. Secur., Vol.25, No.4, pp.289–296 (2006).

[NIPH2017] 国立保健医療科学院：一目でわかるヘルスプロモーション理論と実践ガイドブック 日本語版, 入手先〈http://www.niph.go.jp/soshiki/ekigaku/hitomedewakaru.pdf〉（参照 2017-02-16）.

[Parsons2014] 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).

[Pearman2016] S. Pearman, A. Kumar, N. Munson, C. Sharma, L. Slyper, L. Bauer, and N. Christin, Risk compensation in home-user computer security behavior: A Mixed-Methods Exploratory Study, 12th Symp. Usable Priv. Secur. (SOUPS 2016), Denver CO, USA, 2016. 入手先〈https://www.usenix.org/sites/default/files/soups16poster23-pearman.pdf〉（参照 2022-08-09）.

[Reason2014] Reason, J.: Human error, Cambridge University Press(1990). 十亀 洋（訳）：ヒューマンエラー［完訳版］，海文堂出版 (2014).

[Weeger2014] Weeger, A. and Heiko G.: FACTORS INFLUENC-ING FUTURE EMPLOYEES’DECISION-MAKINGTO PARTICIPATE IN A BYOD PROGRAM: DOESRISK MATTER?, Proc. 22nd Eur. Conf. Inf. Syst. Tel Aviv 2014(online), available from 〈http://aisel.aisnet.org/ecis2014/proceedings/track16/3/〉(2014).

[Weinert2014] Weinert, C., Maier, C., Laumer, S. and Weitzel, T.: Does teleworking negatively influence IT professionals?, Proc.52nd ACM Conference on Computers and People Research(SIGSIM-CPR ’ 14), pp.139–147 (2014).

第 IV 部

セキュリティ疲れの研究

第 9 章

はじめに

2017 年以降, セキュリティ疲れ (Security Fatigue) について, セキュリティ疲労度測定尺度 (SFS: Security Fatigue Scale) の開発と応用研究を行っている [谷本 2017] [畑島 2017d] [畑島 2017e] [畑島 2018a] [畑島 2018b] [畑島 2018c] [畑島 2020] .

情報端末を用いる全ての人に対して，情報セキュリティ対策が常に求められている．対策が必要となる原因であるサイバー犯罪やヒューマンエラーによるインシデントへ対応の多様化により，求められる情報セキュリティ対策施策の種類は増えるとともに内容は複雑化している．本研究の問題意識として，これらの施策に対して ICT（Information Communication Technology）利用者が疲弊することを「セキュリティ疲れ (Security Fatigue)」と呼び，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セキュリティ対策施策の効果が上がらなくなっていることを挙げる．

本研究の研究動機は，一般 ICT ユーザのセキュリティ疲れ状態を可視化することにより，セキュリティ疲れ状態を回避し理想的な状態を維持させる方法を導くことである．

セキュリティ疲れの発生要因の一例として企業における厳格なルール運用があると考える．企業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 9.1(1))．これに対して現場の従業員は，その負担から，当初は遵守行動をとるが業務の効率化と相反するため生産性を求めたり，施策に効果を認識できなかったりするような「セキュリティ疲れ」の発生により，次第にセキュリティ対策を省略や自身の判断で簡略化するといった，セキュリティ疲れによって現れると思われる行動をとるようになる (図 9.1(2))．これによりルールに対する逸脱行為が増大する (図 9.1 (3))．その結果，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 (図 9.1(4))，ルールや手続が増加することとなり (図 9.1(1))，現場の負担が増大する (図 9.1(2))．このように，セキュリティ疲れは悪化するば

かりであり，企業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セキュリティ施策の費用対効果は悪化するばかりである．

本研究ではこのような悪循環によりインターネット利用者が「セキュリティ疲れ状態」となり，この状態が進行することで情報セキュリティ対策を実施しなくなる状態を「セキュリティバーンアウト (Security Burnout) 状態」と仮定した．そしてこの仮定をもとに，一般的な燃え尽き症候群 (バーンアウト) の測定手法の援用によりセキュリティ疲労度の測定尺度を開発した．セキュリティ疲労度測定尺度はまず，予備調査（**10.3.5.1.5**）と本調査・確認調査（**10.5**）によって 13 項目の設問から構成される大学生版セキュリティ疲労度測定尺度 SFS-13[畑島 2018a]（付録 Ⅳ-3）を開発し，その後，対象を社会人にも拡げた研究（**10.6**）により，9 項目の設問から構成される汎用版セキュリティ疲労度測定尺度 SFS-9[畑島 2020]（付録 Ⅳ-4）を開発した．

また，SFS-13 開発の予備調査（**10.3.5.1.5**）では，測定尺度の利用結果である尺度得点の段階分けに **10.2.5.2** で説明する潜在ランク理論 **10.2.5.2** を適用し，各段階別のセキュリティ疲れの特徴を調べた．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，自由記述による設問「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特徴を考察した．

その結果，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，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あるが行動が伴わないといったことが代表的なセキュリティ疲れ行動傾向がそれぞれあることが示唆された．この傾向は，**11.1.3** で後述のセキュリティコンディションマトリクスに基づくリスクアセスメント実施時に調査対象者数を拡大した調査においても同様にみられることを確認した．

さらに本研究では，**11** で述べるセキュリティ疲労度測定尺度の応用研究を行った．具体的には，セキュリティ疲労度測定尺度と他の測定尺度の組み合わせによって ICT 利用者各人が情報セキュリティに対してどのようなコンディションにあるのかを有限個の状態として表現する「セキュリティコンディションマトリクス」を開発した [畑島 2018b]．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実施強度を強化だけでなく，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の実施が検討出来るようになる．その結果，利用者各人が情報セキュリティ対策の施策に対して疲労していないの維持により，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の抑止，および，情報セキュリティ対策の費用対効果の向上が期待できる．

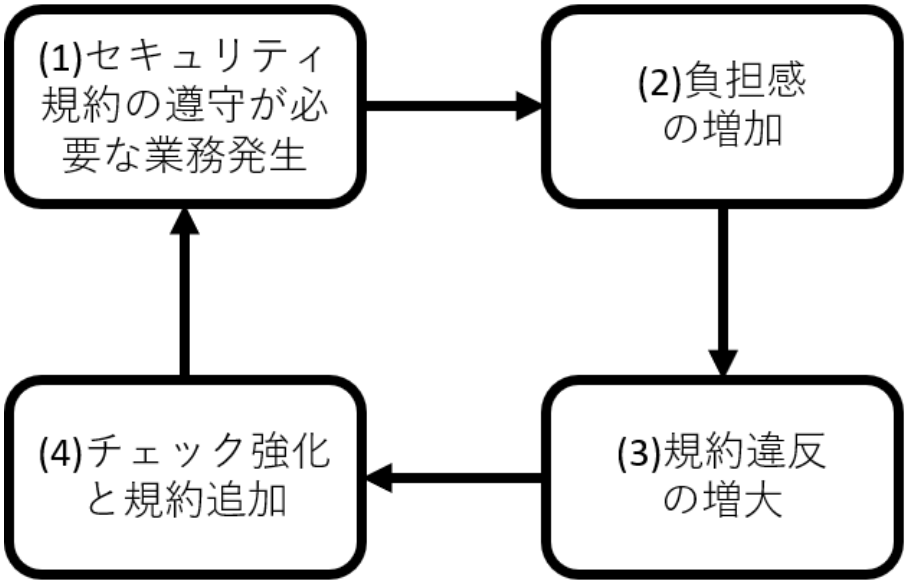

図 9.1　企業の情報セキュリティ対策における悪循環 [畑島 2017d]

第 10 章

セキュリティ疲労度測定尺度の開発

10.1　セキュリティ疲れの定義

10.1.1　先行研究におけるセキュリティ疲れの定義

文献調査の結果, セキュリティ疲れを指す”Security Fatigue” というフレーズは, 2006 年の McLaughlin[McLaughlin2006] や 2014 年の McGraw[McGraw2014] で出現しており, 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 [Furnell2009] と見られた．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 [Stanton2016] 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 [Stanton2016] 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 [Kearney2016] 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．

情報セキュリティ疲れが起きる発端についての考察として, Furnell ら [Furnell2009] が, 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 [Stanton2016] 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．

また，情報セキュリティ研究にバーンアウトの考え方を導入した研究として，Pham ら [Pham2019] 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，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について知見を示している．

10.1.2　本研究でのセキュリティ疲れの定義

本研究では，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定義している．この定義のもと，セキュリティ疲れが悪化した状態を情報セキュリティバーンアウトと仮説し，一般的なバーンアウトに関する研究を援用している．

10.2　セキュリティ疲労度測定尺度開発の概要

10.2.1　セキュリティ疲労度測定尺度 SFS-13 および SFS-9

当初取り組んだ，13 項目の質問から構成される大学生版セキュリティ疲労度測定尺度（SFS-13：Security Fatigue Scale-13，付録 Ⅳ-3）の開発（予備調査を **10.3**，本調査及び確認調査，信頼性と妥当性の検討を **10.4** で実施）では，調査対象を大学生とした．その後調査対象を一般に拡げ，9 項目の質問から構成される汎用版のセキュリティ疲労度測定尺度（SFS-9：Security Fatigue Scale-9，付録 Ⅳ-4 ）を開発（**10.6**）し，信頼性と妥当性を検証した．これにより日本語による情報セキュリティ疲労度測定尺度を完成させた．

当初大学生を対象とした理由は，本研究が大学との共同研究であったため大学生を対象としたデータ収集の容易さもあるが，社会人のように業種や職種によるセキュリティ対策経験の差が少ないと思われたこともある．その他の理由として，まず，2005 年から広島大学が全国の大学に先駆けて全ての学生及び教職員にウイルス対策ソフトを無償配布したこと [西村 2012] [広島大学 2018] が挙げられる．さらに，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 [NII2018] を公開開始するという，各大学を単位とする施策が行われてきたこともある．そして，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に大学として初加盟 [東京電機大学 2018] したのを皮切りに，2018 年 2 月 1 日現在 10 大学が加盟中 [CSIRT2018] であるように，大学においても企業と遜色ない組織的な

情報セキュリティ対策が求められる傾向がみられたことも理由である．

10.2.2　一般的なバーンアウトとその測定尺度

ここでは一般的なバーンアウトとその測定尺度について述べる．なお，**10.1.2** で前述のように本研究では，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定義している．この定義のもと，セキュリティ疲れが悪化した状態を情報セキュリティバーンアウトと仮説し，一般的なバーンアウトに関する研究を援用している．つまり，一般的なバーンアウト測定尺度は職務全体のバーンアウトに対する尺度であるため，本研究が対象とする情報セキュリティ対策に対するバーンアウトとは対象が異なる．これは，本研究で扱う情報セキュリティ対策に対するバーンアウトは，セキュアな業務遂行の一環としてもしくは安全なインターネット利用という行動の一部として発生するものであるためである．

10.2.2.1　バーンアウト（燃え尽き症候群）

一般的に知られるバーンアウト (Burn out) は燃え尽き症候群とも訳される．久保は，“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 [久保 1999] ．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っている [板倉 2009] .

10.2.2.2　Maslach らによるバーンアウト尺度（MBI-HSS，MBI-ES，MBI-GS）

久保 [久保 1999][久保 2004] の説明にもとづき，Maslach らによって開発されたバーンアウトの測定尺度 MBI (Maslach Burnout Inventory) について言及する．MBI は 1982 年にマニュアルの初版が作成され [Maslach][Maslach1998]，当初は看護職や教育職といったヒューマン・サービス従事者の状態を測定する尺度として開発された．現在では下記に挙げる 3 種類の測定尺度が存在しており，バーンアウトに関する研究の大多数において用いられている ．3 種類の MBI とは，MBI 測定尺度開発の初期から使われている看護師やソーシャルワーカーを対象とした MBI-HSS (Maslach Burnout Inventory – Human Sur-vices Survey)，教員を対象とする際に用いられる MBI-ES (Maslach Burnout Inventory – Educational Survey)，および，次に述べるヒューマン・サービス以外の職種を含めて対

象とした MBI-GS(Maslach Burnout Inventory – General Survey) である．

■10.2.2.2.1　**ヒューマン・サービスにおけるバーンアウト** (MBI-HSS，MBI-ES)　MBI-HSS および MBI-ES は，下位尺度として，emotional exhaustion(情緒的消耗感)，depersonalization (脱人格化)，及び personal accomplishment (個人的達成感) の 3 つの下位尺度を持ち，7 件法による合計 22 項目の設問から構成されている．

■10.2.2.2.2　**全ての職業に対するバーンアウト** (MBI-GS)　ヒューマン・サービス (対人援助職) に限らない，全ての職業におけるバーンアウト尺度 MBI-GS は，“仕事との関係”の中で生じる心の疲労や仕事に対する態度を調査する国際比較研究に使用されている．日本語版は北岡らによって翻訳され，国内での調査により信頼性と妥当性の検証が行われた [北岡 2011]．MBI-GS の下位尺度は exhaustion (疲弊感 [北岡 2011]，消耗感 [板倉 2009])，cynicism (シニシズム：冷笑感 [北岡 2011])，及び professional efficacy (職業上の効力感 [板倉 2009]) の 3 つを持ち，7 件法による合計 16 項目の設問から構成されている．

10.2.2.3　(日本版) バーンアウト尺度

久保は（日本語版）バーンアウト尺度 [久保 1999] を MBI 等を参考に新規開発し MBI をそのまま翻訳した項目は存在しないと説明している．(日本版) バーンアウト尺度の下位尺度は，情緒的消耗感，脱人格化，個人的達成感の低下の 3 つを持ち，5 件法による合計 17 項目の設問から構成されている．

10.2.2.4　バーンアウトメジャー

バーンアウトメジャー (BM: the Burnout Measure) は Pines と Aronson により開発され，下位尺度のない単一尺度として「情緒的な資源が必要とされる状況に長期間関わらざるを得なかった結果生じた身体的，情緒的，精神的に消耗した状態」を測定する 21 項目の設問から構成されている [久保 2004] .

10.2.3　情報セキュリティに対するバーンアウトの研究

情報セキュリティに対するバーンアウトの研究として，2015 年の Chandran ら [Chandran2015] 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つきについて，セキュリティ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存在する．しかし，Chandran らの研究は職業的燃え尽きを対象としていることから，本研究の問題意識である情報セキュリティ対策を要請される本人がもつ

疲弊感とは研究対象が異なる．

10.2.4　一般的なバーンアウトと情報セキュリティ疲れに対するバーンアウトとの差異

本研究は，セキュリティバーンアウトに対しても一般的なバーンアウトの測定手法を援用が可能ではないかという動機付けにより行った．そのため，セキュリティ疲労度測定尺度の開発は，**10.2.2** で述べた MBI 等と同様に，質問紙調査の因子分析および，得られた因子構造に対する信頼性と妥当性の検討を行うことにより実施した．

ただし，現在一般的にバーンアウトと呼ばれている状態では，職業的燃えつきを起こしており，バーンアウトの対象は従事する業務全体である．それに対して本研究で呼ぶセキュリティバーンアウトでは，情報セキュリティ施策に対する疲労のみを対象としている点が異なる．

10.2.5　バーンアウト段階説と潜在ランク理論

10.2.5.1　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は Golembiewski の 8 段階モデル (eight-phase model) である．Golembiewski の 8 段階モデルは，表 10.1 に示すように MBI-HSS の 3 因子それぞれをしきい値によって高低の 2 値に分けることによって得られる 2^3 の 8 段階に対して順序を仮定している．

Golembiewski の 8 段階モデルでは，表 10.1 に示されるように，段階 I から段階 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．なお，Golembiewski の 8 段階モデルの性質として，進行径路はすべての段階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異なっていることや，バーンアウトの過程が一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示されている [久保 2004] .

その他，表 10.2 に示すように増田ら [増田 2011] は心理尺度 (MBI-GS，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測定のための判定基準 (増田らの判定基準で,「強バーンアウト」「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 MBI-GS の 3 つの尺度得点に対してしきい値を設定し，その高低によってバーンアウトの判定を行っている．その特徴として，下位尺度にも影響の順序

があり，疲弊感が高いことが「バーンアウト」や「疲労」状態の条件としている．例えば，疲弊感は低いがシニシズム (冷笑感) が高いときが「うつ状態」であって，疲弊感もシニシズムも低い状態であれば職務効力感の度合いにかかわらず「問題なし」と判定している．

参考として表 10.3 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．この表では対比に用いられている測定尺度が異なるため直接比較はできないことに注意が必要である．

表 10.1　Golembiewski の 8 段階モデル

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

L:Low,H:High

表 10.2　増田らによるバーンアウト判定基準 [増田 2011]

	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	L	L	L	L	H	H	H	H
職務効力感	L	L	H	H	L	L	H	H
シニシズム	L	H	L	H	L	H	L	H

L:Low,H:High

表 10.3　バーンアウトに対する Golembiewski のモデルと増田らの判定基準との対比（ただし直接比較ではない）

MBI-GS による 増田らの判定基準	MBI-HSS による 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

10.2.5.2　潜在ランク理論

本研究では，得られたセキュリティ疲労度測定尺度の得点をレベルわけする際に，荘島による潜在ランク理論（Latent Rank Theory, LRT）[荘島 2008] を適用している．

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が提唱した潜在ランク理論 [荘島 2008] は，ノンパラメトリックな項目反応理論として立ち上げられたニューラルテスト理論（Neural Test Theory, NTT）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ものである．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 値や多段階のリッカート尺度による質問紙調査における各項目の回答結果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．

本研究への適用が考えられる理論として，テスト理論における項目反応理論 (Item Response Theory, IRT) が挙げられる．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．しかし，潜在尺度に連続尺度を仮定している [小山 2007] ため本研究への適用は適切ではない．

潜在ランク理論の適用分野例を述べる．まず，教育分野では，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 [文部科学省 2017] 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 [小山 2007][荘島 2009] で用いられている．その他，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は，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 [清水 2014] で用いられている．

潜在ランク理論による分析には，荘島によるソフトウェア exametrika(エクザメトリカ)[荘島 2017] が利用可能である．

10.2.6　その他の情報セキュリティに関する測定尺度研究と本研究の関係

セキュリティ疲労度以外の，情報セキュリティ分野における質問紙を用いた測定尺度研究について述べ，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の測定尺度である本研究の意義を述べる．そして，本研究とセキュリティ疲れに関する周辺研究との差異について述べる．

情報セキュリティに関する測定尺度研究例を挙げる．Parsons らは，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 [Parsons2014]．Egelman らは，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 [Egelman2015][Egelman2016]，また，Faklaris らは，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 [Faklaris2019] ．これらはセキュリティ疲労度を測定していない．

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 [Sharif2018] 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．

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．しかし，本研究が開発を意図するセキュリティ疲れ，換言すると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 10.1 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 10.2 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ひと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．

図 10.1　先行研究で用いられている行動モデル [畑島 2020]

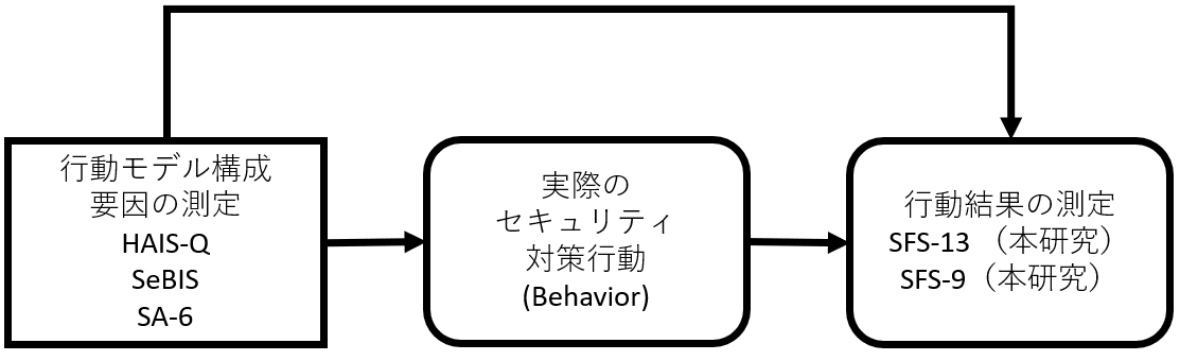

図 10.2　情報セキュリティ関連測定尺度研究と本研究の関係 [畑島 2020]

続いて，本研究とセキュリティ疲れに関する周辺研究との差異について述べる．

本研究では Furnell ら [Furnell2009] と同様にオンラインセキュリティに着目しているが，本研究で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 [Stanton2016] 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，本研究でも同様の結果を得ている [畑島 2017e]．具体的には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 [Stanton2016] が示す「鈍感」や「うんざり」という感情についても，本研究の成果 [畑島 2018b] でも同様の傾向が現れている．

Kearney ら [Kearney2016] 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 [Pham2019] 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，本研究において **10.6.4.2** で実施している基準関連妥当性の検討および **10.6.9.1** で実施している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ため，測定尺度としての検討は不十分である．

10.3　大学生版セキュリティ疲労度測定尺度 SFS-13 開発の予備調査：セキュリティ疲れの段階別特徴

大学生版セキュリティ疲労度測定尺度 SFS-13 開発における予備調査および本調査の実施手順を以下に述べる．

10.3.1　SFS-13 開発手順（予備調査，本調査，確認調査）

ここでは，情報セキュリティ疲れの尺度を具現化するための測定尺度開発の手法及び手順について説明する．**10.2.2** において前述のようにバーンアウトのような人の疲れに関わる状態の可視化には質問紙調査の結果得られる測定尺度を用いる調査法が使われており，本研究においてもバーンアウトを援用する観点から，質問紙調査を用いる．本研究では，前述した一般的なバーンアウトを参考に情報セキュリティ疲労度を測定する質問紙を新規作成した．質問紙の作成手順を表 10.4 に示し，以降において各手順の詳細について説明する．作成手順及び検証方法の決定においては，心理尺度の一般的な手法とみられる文献 [菅原 2006] および [村上 2013] を参照し，分析には統計分析ソフトウェア R version 3.4.1 を用いた．

詳細は以降に述べるが，ここでも SFS-13 の開発のために初期作成した質問紙の概要を述べる．**10.2.2** で述べた先行研究による MBI-GS および久保らによる (日本版) バーンアウト尺度の説明を援用し，情報セキュリティ疲れを測定する設問数 28 項目の質問紙を新規作成した．設問は，「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たか」を尋ね，「ない」，「まれにある」，「時々ある」，「しばしばある」，「いつもある」の 5 件法での回答を求めた．質問紙には質問意図の推察を避けるためのダミー設問を 3 項目，ライスケールとしての設問を 1 項目，類似質問に対して回答にブレがみられる回答者を除くための設問 1 項目含めた．このため，情報セキュリティ疲れの測定に用いる設問数は 23 項目である．また，情報セキュリティ対策についての考えを自由記述させる設問を 1 項目，回答させた質問紙について思ったことを自由記述させる設問を 1 項目設定した．予備調査では，質問紙調査を実施し，その結果に対して潜在ランク理論を用いて解析し，得られたランクごとの特徴を自由回答から抽出した．本調査および確認調査によって，因子分析等により SFS-13 の確定を行った．

表 10.4　大学生版セキュリティ疲労度測定尺度 SFS-13 となる質問紙の作成手順

項番	手順項目	実施手法	本研究の項番
(1)	構成概念の検討	一般的なバーンアウト尺度の構成概念を援用し検討	**10.3.2**
(2)	項目候補収集（予備調査版質問紙作成	既存尺度の設問文の翻案や構成概念名をキーワードとした検討により作成	
(3)	内容妥当性の検討	筆者ら 2 名による検討	
(4)	予備調査の実施	大学生を対象とした質問紙調査（2017 年 7 月実施）	**10.3.3**
(5)	予備調査結果の検討	筆者ら 2 名による検討	**10.3.4**
(6)	本調査	大学生を対象とした質問紙調査（2017 年 7 月実施）	**10.4.1**
(7)	本調査結果の分析による測定尺度項目（質問項目）の決定	探索的因子分析	**10.4.2**
(8)	信頼性の検討	α 係数の算出と評価	**10.4.3**
(9)	妥当性の検討（ここまでで質問紙確定）	構成概念妥当性の検討（確認的因子分析の実施）	
(10)	確認調査	大学生を対象とした質問紙調査（2017 年 9 月～10 月実施）	**10.4.4.1**
(11)	確認調査結果の分析（尺度得点の分析）	記述統計量および男女別の尺度得点の平均値の差の検定	**10.4.4.2**

10.3.2　質問項目の検討と予備調査版質問紙の作成

情報セキュリティ分野においては，セキュリティ疲れのような人の内的要因を心理測定尺度の作成によって可視化するための質問紙調査に関する検討はあまり行われていなかった．このため，質問紙調査の設計段階における質問項目考案のために，一般的なバーンアウトの心理測定尺度として幅広く使われている MBI のうち測定対象を一般労働者とした

MBI-GS 及び日本人を対象に開発された (日本版) バーンアウト尺度の下位尺度名を久保 [久保 2004] の説明にもとづき援用した．バーンアウト尺度を援用した理由を以下に述べる．我々は **9** に示したように，セキュリティ疲れが複雑化する情報セキュリティ対策施策への対応作業により発生することを問題視している．このため，セキュリティ疲れは情報セキュリティ対策施策への対応として作業により発生するためであることから，労働者が業務を実施ことにより発生するバーンアウトの考え方を援用できると考えた．上述のように，セキュリティ疲れ測定尺度の開発において，一般の職業従事者による業務実施によって発生するバーンアウトを測定する手法であるバーンアウト尺度を援用した．本研究で用いる質問紙の構成概念の検討 (表 10.4(1)) のために，MBI-GS や (日本版) バーンアウト尺度から 5 項目の仮説因子名 (表 10.5) を参考とした．

それぞれの仮説因子は次のように説明される．これらは久保 [久保 2004] が説明した参照元の因子名を，筆者らのディスカッションにより情報セキュリティ対策に翻案して決定したものである．まず，仮説因子の消耗感は「情報セキュリティ対策について力を出し尽くし，消耗してしまい，その疲労感が累積していく状態」であり，仮説因子の冷笑感は「情報セキュリティ対策そのものに対する意欲の低下」である．そして仮説因子の効力感は「情報セキュリティ対策を実施することによる成功体験の実感」であって，仮説因子の個人的達成感の低下は「情報セキュリティ対策における達成感や充実感の低下」である．最後に，仮説因子の脱人格化は「情報セキュリティ対策に対するネガティブな感情や行動傾向」であると決定した．

それぞれの仮説因子に属する設問 (表 10.5) として，セキュリティ疲れを話題とした情報セキュリティ専門家とのフリーディスカッションを踏まえ，新しく設計した 5 項目と，文献 [Stanton2016] の知見を参照した 2 項目，および一般のバーンアウトに関する設問 [Stanton2016][板倉 2009] を，本研究が意図する情報セキュリティ疲れが対象となるように再検討した 17 項目からなる合計 24 項目を抽出した．このうち，不誠実な回答者を除外する目的で質問意図の類似する設問 (PQ9 と PQ25 のペア) を設定し，回答にかい離のある場合には分析対象として採用しないこととした．更に，不誠実な回答者を除外するためのライスケール 1 問と，質問紙への回答に興味を失わせないことを意図してダミー設問を 3 項目設定し，全 28 項目の質問とした．

この結果によって，大学生版セキュリティ疲労度測定尺度 SFS-13 開発に用いた初期質問紙（表 10.6）を 28 項目の設問から構成した (表 10.4 (2))．設問の教示文は「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」とし，回答は「ない」，「まれにある」，「時々ある」，「しばしばある」，「いつもある」の 5 件法 (1〜5 点) で求めた．そのほか，「情報セキュリティ対策について考えること」と，「質問文や質問内容

について思ったこと」を自由回答で求める 2 問を設定した．これらの内容的妥当性について筆者のうち 2 名によって検討し (表 10.4 (3))，質問紙調査を実施した．

表 10.5　仮説因子名と SFS-13 作成仮質問紙の設問番号の対応

仮説因子名	設問番号
消耗感	PQ1, PQ5, PQ6, PQ9, PQ14, PQ19, PQ25（PQ9 の類似質問）, PQ28
冷笑感	PQ2, PQ7, PQ12, PQ15, PQ16, PQ17
効力感	PQ3, PQ8, PQ14, PQ18
個人的達成感の低下	PQ20, PQ22, PQ27
脱人格化	PQ23, PQ24, PQ26（PQ2 の類似質問）

PQ26 は予備調査では類似質問としていなかったが，
本調査では PQ2 の類似質問として設定した．

表 10.6: セキュリティ疲労度測定尺度 SFS-13 開発に用いた初期質問項目

予備調査・本調査の設問番号	設問文	仮説因子名
PQ1	ソフトウェアの最新化やパスワードの定期的な更新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	消耗感
PQ2	情報セキュリティ対策は意味が無いと思うことがある	冷笑感
PQ3	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	効力感
PQ4	PC やスマートフォンを使っているとワクワクする	ダミー項目
PQ5	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	消耗感
PQ6	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	消耗感
PQ7	情報セキュリティ対策は必要悪だと思うことがある	冷笑感
PQ8	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	効力感
PQ9	情報セキュリティ対策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	消耗感
PQ10	SNS で人と交流するのが楽しいと思うことがある	ダミー項目
PQ11	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	効力感
PQ12	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	冷笑感
PQ13	PC やスマートフォンをなくしたり壊したりしないかとヒヤヒヤすることがある	ダミー項目

PQ14	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	消耗感
PQ15	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	冷笑感
PQ16	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	冷笑感
PQ17	指示される情報セキュリティ対策に一貫性がないと思うことがある	冷笑感
PQ18	私はセキュリティ対策に自信があると思うことがある	効力感
PQ19	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	消耗感
PQ20	本来やることを忘れるほど情報セキュリティ対策に熱中することがある	個人的達成感の低下
PQ21	手で入力するときパスワードを間違えることがある	ライスケール
PQ22	私の性分は情報セキュリティ対策に向いていると思うことがある	個人的達成感の低下
PQ23	情報セキュリティ対策がつまらなく思えてしかたのないことがある	脱人格化
PQ24	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	脱人格化
PQ25	情報セキュリティ対策のために心にゆとりがなくなったと感じることがある	消耗感
PQ26	情報セキュリティ対策は，私にとってあまり意味がないと思うことがある	脱人格化
PQ27	情報セキュリティ対策が楽しくて，知らないうちに時間が過ぎることがある	個人的達成感の低下
PQ28	情報セキュリティ対策のために体も気持ちも疲れはてたと思うことがある	消耗感

10.3.3　予備調査の実施

表 10.4 (4) に示した予備調査を 2017 年 7 月 12 日に実施した．調査対象者は，首都圏内の私立大学に通う大学 3 年生であり，調査開始時に文書と口頭で依頼し同意を得た．なお，謝礼は提示しておらず，性別や年齢については回答を求めていない．不誠実な回答者による回答の除外は，以下の手順 (1)〜(4) で行った．

(1) 未回答項目がある回答者を除外
(2) 全ての設問に同一の選択肢を回答した回答者を除外
(3) ライスケールとして設定した設問「手で入力するときパスワードを間違えることがある」に「ない」と回答した回答者を除外
(4) 不誠実な回答を検出する設問を PQ9 と PQ25 のペア (尺度には設問番号が小さい方を採用) とし，それぞれの組み合わせにおいて選択した番号の差の絶対値が 3 以上であった回答者を除外

これらの条件を設定した理由を以下に述べる．三浦ら [三浦 2015] は目的を達成するために必要最小限を満たす手順を決定し追求する行動をとることや，設問をよく読まないことに起因する不誠実な回答が 10% 程度発生することを指摘している．つまり，不誠実な回答者は，(a) 目的を達成するために必要最小限を満たす手順を実施するため，全設問でほぼ同一の選択肢を選ぶことや，(b) 設問項目をよく読まないため，類似する設問に対してかけ離れた選択肢を選ぶことがあると言える．(a) については，極端に不誠実な回答者として，全ての設問で同一の回答である回答者を手順 (2) にて除外した．(b) については，手順 (4) において除外する極端に不誠実な回答者として，5 件法において一方で 1 を選んだ場合に他方で 4 若しくは 5 を選ぶ場合，同様に 5 を選んだ場合に 1 もしくは 2 を選ぶ場合のように，中間値である 3 を越えた選択肢を選択する回答者を除外するために，選択した番号の差の絶対値が 3 以上である回答者を除外した．

以上により調査協力者 50 名分の回答のうち，有効回答は 44 名分であったため，有効回答率は 88.0% であった．

10.3.4　予備調査結果の検討

予備調査は質問文の内容や質問紙の回答のしやすさを確認する目的で実施し，有効回答数が充分でないことから因子分析による設問項目抽出は実施していない．表 10.6 の質問

紙自体に対する意見や感想の自由回答を参考として著者が設問文の再検討した結果，質問文に変更は不要としたが，以降の調査では PQ2 と PQ26 のペアも類似質問として不誠実な回答者の検出に用いることとした (表 10.4(5)).

10.3.5 セキュリティ疲労度の段階別性質

セキュリティ疲労度の段階別性質を調べた（表 10.7）．具体的には，測定尺度のクラス分けに **10.2.5.2** で説明した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た．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，自由記述による設問「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抽出した．その結果が表 10.7 である．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，セキュリティ疲れの程度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なった．予備調査では，後述のように潜在ランクの段階数として 1 から 5 の 5 段階を設定し，潜在ランク 3 を疲労度の相対的レベルの基準とし，疲労度レベル“0”と設定し，潜在ランク 1 および 2 をそれぞれ疲労度レベル“- -”と“-”，潜在ランク 4 および 5 をそれぞれ疲労度レベル“+”と“+ +”とした．

セキュリティ疲労度のそれぞれのランクにおける特徴を，各ランクに属する回答者の回答をもとに考察した結果は以下の通りであった．なお，この結果は **11.1.3** で後述するセキュリティコンディションマトリクスによるリスクアセスメントにおいても同様の傾向が得られた．

I おおよそ尺度得点が中位にある状態が，情報セキュリティ対策実施に対する適度な緊張感がある理想状態である
II 尺度得点が高得点になると，情報セキュリティ対策の実施責任に対するする負担感や，重要性の認識と対策実施の意思にかい離がみられる
III 尺度得点が下位になると実施対策について当事者意識が希薄となる

10.3.5.1 セキュリティ疲労度の潜在ランク理論による可視化

潜在ランク理論の分析には荘島によるソフトウェア exametrika(エクザメトリカ)[荘島 2017] を用いた．潜在ランク数を 5 段階と設定し，分析手法として自己組織化マップ (SOM: Self-Organizing Map) を選択した．回答結果を単純集計した場合，設問は

表 10.7　情報セキュリティに対する所感に対する自由回答のセキュリティ疲労度レベルごとの特徴

潜在ランクによる分類 (疲労度レベル)	情報セキュリティ対策に対する自由回答結果の特徴
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

すべて 5 件法による 23 問であることから合計得点は 5 点から 115 点の範囲となる．有効回答者 44 名の図 10.3 にセキュリティ疲労度段階別の単純集計得点について描画した箱ひげ図を示す．潜在ランク理論による分析では，個々の設問で高い得点を示す回答者が少ない項目で高得点の回答をした場合，分析結果であるセキュリティ疲労度が高くなるなど，単純に尺度得点を求め得点順に並べた際とは被験者の序列が異なる結果が得られる．

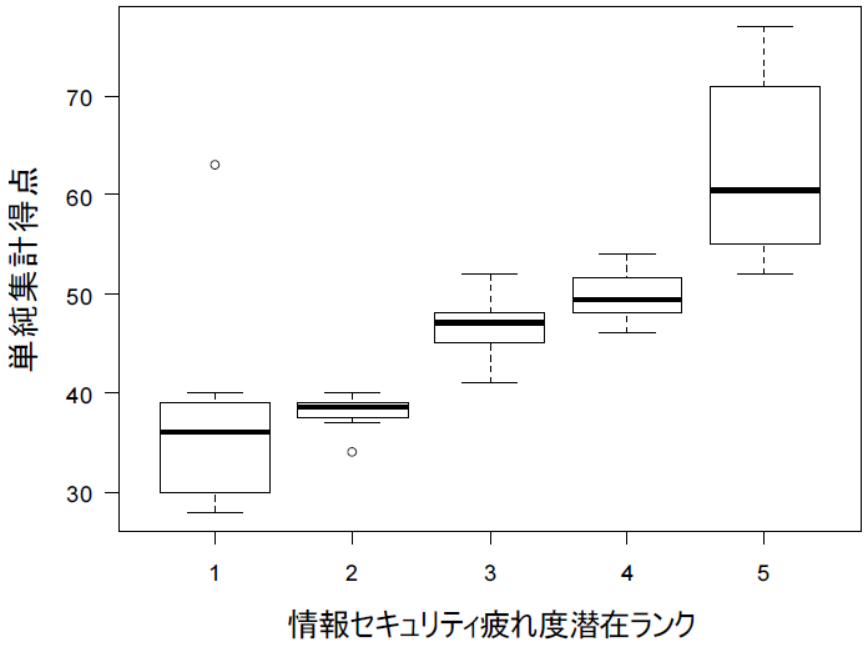

図 10.3　潜在ランクごとのセキュリティ疲労度尺度得点 [畑島 2017e]

■10.3.5.1.1　**セキュリティ疲労度 1 (疲労度レベル“– –”)**　セキュリティ疲労度 1 に属する回答者は 9 名で，単純集計得点の最小値は 28，最大値は 63 だった．このランクに属する回答者の自由記述では，“情報は大切なのでセキュリティ対策はしっかりやっていきたい (回答者 ID 13：回答者 ID は分析時に新しく採番したものであって回答者個人を特定出来ない．以下同様．)”や，“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．(回答者 ID 18)”といった記述があった．このように，情報セキュリティ対策への当事者意識の薄さがあり，効力感を疑う記述がみられた．

■10.3.5.1.2　**セキュリティ疲労度 2 (疲労度レベル “–”)**　セキュリティ疲労度 2 に属する回答者は 8 名で，単純集計得点の最小値は 34，最大値は 40 だった．このランクに属する回答者の自由記述では，“chrome などの Web ブラウザの機能で自動でログインする機能や ID，パスワードを記憶しておく機能がスマホのアプリもログイン保持されているのである限り個人のセキュリティに対する意識は高まらないと思った．(回答者 ID 24)”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．(回答者 ID 28)”といった記述があった．

前者からはソフトウェアの機能による情報セキュリティ対策への依存感が指摘されており，後者からは情報セキュリティ対策に対しての認識はあるものの実施していないという当事者意識の薄さがみられた．

■10.3.5.1.3　**セキュリティ疲労度 3 (疲労度レベル“0”)**　セキュリティ疲労度 3 に属する回答者は 9 名で，単純集計得点の最小値は 41，最大値は 52 だった．このランクに属する回答者の自由記述では，“ハッキングや DoS 攻撃，DDoS 攻撃等日々セキュリティの弱い部分をついてくる出来事が多いので，対策していくのは必然だと考えている．対策せずに被害が出たら身から出たさびだ．(回答者 ID 10)”や，“対策を行うことがあたりまえで，していないのはありえないと考えます．PC を新規購入した時にセキュリティ対策ソフト等をインストールするだけで，定期的に改善したり，触れることはありません．(回答者 ID 22)”といった記述があった．このように，情報セキュリティ対策の実施について，対策していないことに「身から出たさび」と表現するほどに当然のこととして捉えており，情報セキュリティ対策への態度として適度な緊張感があり，対策に疲れるでもないという理想状態に近いものとみられる．しかし，セキュリティ対策ソリューション自身の更新は不要との認識から，対策ソリューションへの信頼感と過信もみられる．

■10.3.5.1.4　**セキュリティ疲労度 4 (疲労度レベル“+”)**　セキュリティ疲労度 4 に属する回答者は 8 名で，単純集計得点の最小値は 46，最大値は 54 だった．このランクに属する回答者の自由記述では，“SNS にさほど変な情報がなければセキュリティ対策をする必要がないと考えている．企業など大きな規模のものはするべきだと考えている．(回答者 ID 14)”や，“厳重なセキュリティを利用していても，個人がウイルスなどに対してある程度の知識を持っていなければ，あまり意味がないと思う．(回答者 ID 27)”といった記述があった．このように情報セキュリティ対策についての冷淡な感覚や情報セキュリティ対策の効力感に疑いを持つ様子がみられ，軽度の情報セキュリティ疲れ状態が表現されているとみられる．

■10.3.5.1.5　**セキュリティ疲労度 5 (疲労度レベル“+ +”)**　セキュリティ疲労度 5 に属する回答者は 10 名で，単純集計得点の最小値は 52，最大値は 77 だった．このランクに属する回答者の自由記述では，“今まで重要視してこなかったセキュリティ対策が，これから会社などに入って重要になってくると思うと少し不安になります．(回答者 ID 19)”や，“「大切だ」ということはわかるのだが，イマイチ実行に移せないでいる．簡単にすると質を保てなくて，逆に難しくすると面倒さが勝ってしまう．バランスが非常に難しい分野だと思う．(回答者 ID 25)”，といった記述のほか，“必要なことだと思うが，時々面倒に

なる．(回答者 ID 15)”，“情報セキュリティ対策は大切だと思うが，面倒くさいと感じることがある．(回答者 ID 38)”といった記述がみられた．1 つ目の記述からは情報セキュリティ対策の実施責任に対する負担感がみられ，以降の記述からは重要性の認識に実施への意思が伴わない状態であることが表現されているとみられる．

10.4　大学生版セキュリティ疲労度測定尺度 SFS-13 の開発

10.4.1　SFS-13 開発のための本調査

本調査として予備調査（**10.3.3**）で用いた質問紙を用いた再調査 (表 10.4(6)) を 2017 年 7 月 28 日に実施し，103 名分の回答を得た．実験協力者は予備調査と同一の首都圏内の私立大学に通う 1 年生であり，**10.3.3** に述べた 2017 年 7 月 12 日実施の予備調査と重複した回答者は存在しない．調査開始時に文書と口頭で依頼し合意を得た．なお，謝礼は提示しておらず，性別や年齢については回答を求めていない．**10.3.4** で述べたように，質問文及び構成に変更がないことから 2 回の調査で得られた合計 153 名分の回答を本調査の回収データとした．不備のある回答を除外するデータクリーニングは，**10.3.3** に示した手順で行った．その結果 81 名分の有効回答が得られたため，有効回答率は 52.9% であった．有効回答率が低くなったのは，予備調査と同様のフィルタリング（**10.3.3** の手順 (4)）での除外条件が厳しくなったためであると考察する．具体的には，**10.3.4** で述べたように，**10.3.3** の手順 (4) の不誠実な回答を検出する設問を，PQ9 と PQ25 のペアに加えて本調査では PQ2 と PQ26 のペアとの 2 件 4 問 (尺度には設問番号が小さい方を採用) とし，それぞれの組み合わせにおいて選択した番号の差の絶対値が 3 以上である回答者を除外した．

10.4.2　SFS-13 確定本調査結果の分析

表 10.4(7) の本調査結果の分析は以下のように行い，信頼性と妥当性の検討が済んでいない因子分析表（表 10.8）を得た．回答者数（サンプルサイズ）の適切性を，相関分析に充分なサンプルサイズを定量的に評価する代表的な手法である Kaiser-Meyer-Olkin のサンプリング適切性基準 (KMO)[青木 2017] によって判断した．KMO は，因子分析の対象データについて，その分析を実施することに意味があるかどうかを判定するものである．KMO は，観察された相関係数と偏相関係数の比によって表され，変数間の偏相関係数が小さいほど 1 に近づき，因子分析を実施することが妥当であると判定される．本調査の結果に対して青木の R プログラム [青木 2017] を用いた分析の結果は 0.82 と算出された．青木 [青木 2017] が示すように，0.8 以上であれば meritorious(価値がある) とされている

ため，本調査の結果は因子分析の適用に充分な回答者数であることが認められた．

因子分析は以下のように実施した．因子数決定には平行分析を採用し，3 つの下位因子が得られた．回転方法に promax 回転，推定方法として最小残差法を採用した因子分析において因子負荷量が 0.3 以下である設問項目と，複数の因子で因子負荷量が 0.3 以上である設問項目を除外した．これを 3 回繰り返すことにより表 10.8 に示す因子パターンと因子間相関をもつ 13 項目が得られた．得られた 3 つの下位因子の累積寄与率は 49.3% であり，因子間相関は，0.339〜0.579 であった．

表 10.8 に示すように，各下位因子には因子名としてそれぞれ「(情報セキュリティ対策からの) 回避願望」(5 項目),「(情報セキュリティ対策に対する) 消耗感」(3 項目),「(情報セキュリティ対策に対する) 当事者意識」(5 項目) を付与した．因子名の付与は，著者，大学教授 1 名および大学生 3 名によるディスカッションによって行った．

具体的は，それぞれの因子名は各下位因子を構成する設問文を総合した名称をつける作業により，以下のように決定した．まず，本研究の回避願望は「責任の転嫁や無責任さをもち，対策から離れたくても離れられない状態にある」であるとした．また，本研究の消耗感は「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もつ」とし，最後に本研究の当事者意識は「自分の行動に対する達成感をもち，誠実な対応への意識がある」とした．それぞれの因子名を決定する際に出た意見を以下に述べる．回避願望では,「責任感の転嫁」,「拒絶感や排斥感」,「(情報セキュリティ対策からは) 離れたくても離れられない」といった様子が見受けられるとの意見が出た．消耗感では,「面倒くささ」,「やらされ感」,「重圧感」,「徒労感」といった様子が見受けられるとの意見が出た．当事者意識では,「意識の高さ」,「誠意ある行動」,「回避願望因子と対極的な概念」といった様子が見受けられるとの意見が出た．

表 10.8　SFS-13 確定本調査の因子分析結果（信頼性と妥当性の検討の検討前）

設問番号	回避願望	消耗感	当事者意識の低さ	共通性	設問文
PQ12	**0.866**	-0.137	-0.152	0.577	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
PQ19	**0.723**	-0.038	0.169	0.494	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
PQ24	**0.648**	0.021	-0.018	0.368	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
PQ15	**0.600**	0.038	-0.032	0.368	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
PQ16	**0.595**	0.050	0.098	0.630	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
PQ5	0.044	**0.897**	-0.112	0.773	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
PQ6	-0.093	**0.809**	-0.074	0.583	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
PQ14	0.069	**0.352**	0.256	0.292	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
PQ8	-0.239	0.110	**0.928**	0.725	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
PQ11	-0.089	-0.175	**0.800**	0.512	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
PQ18	0.110	-0.044	**0.568**	0.388	私はセキュリティ対策に自信があると思うことがある
PQ7	0.065	0.063	**0.524**	0.348	情報セキュリティ対策は必要悪だと思うことがある
PQ9	0.220	-0.079	**0.460**	0.346	情報セキュリティ対策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
因子寄与	2.458	2.291	1.654		
因子寄与率	0.189	0.176	0.127		
累積寄与率	0.189	0.365	0.493		
因子負荷行列	1 0.579 0.351	 1 0.339	 1		

10.4.3 得られた因子構造に対する信頼性と妥当性の検討による SFS-13 の確定

質問紙の信頼性を，Cronbach の α 係数により求めた (表 10.9)．情報セキュリティ疲労度尺度全体の α 係数を算出したところ 0.83 (95% 信頼区間 0.78–0.89) であり 0.8 以上を示したことから，情報セキュリティ疲労度尺度の信頼性が確認された．また，下位尺度についても α 係数を求め，尺度項目間の類似度である内的整合性を評価した．その結果，それぞれの下位尺度について，回避願望 0.81 (0.74–0.87)，消耗感 0.73 (0.63–0.83)，当事者意識 0.78 (0.70–0.85) となり，内的整合性が確認された (表 10.4(8))．

表 10.9　SFS-13 確定本調査の信頼性の検討

下位因子名	設問数	平均	*SD*	α 係数 （95% 信頼区間）
回避願望	5	9.72	4.11	0.81 (0.74–0.87)
消耗感	3	10.56	2.66	0.73 (0.63–0.83)
当事者意識	5	10.63	4.04	0.78 (0.70–0.85)
全体	13	30.90	8.24	0.83 (0.78–0.89)

検討すべき妥当性 (表 10.4(9)) 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．

内容妥当性は設問設計時に確認すべきものであり，本研究では **10.3.2** において確認した．

基準関連妥当性について，村上 [村上 2013] 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”と指摘している．本研究で測定しようとする情報セキュリティ疲労度については，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であるとして今後の研究課題とした．

構成概念妥当性は，R の共分散構造分析（構造方程式モデリング）パッケージ lavaan を用いた確認的因子分析によって検証した．質問紙調査結果を因子分析した結果得られる下位因子構造に対して確認的因子分析を実施すると，測定方程式によって観測変数である各質問項目と構成概念である下位尺度のつながりが方程式で表されると同時に，構造方程式によって因子間の因果関係である各尺度間の関係も方程式で表現される．つまり共分散構造分析では柔軟なモデル構造の定義が可能であり，数理的な分析により最適なモデル構造の導出が実現されるため，妥当な手法であると考える．

確証的因子分析によりモデル構造を変更しつつ適合度の高いモデルを探索した結果，図 10.4 に示すように 2 次因子構造のモデルが得られた．図中の数値はパス係数であり，誤差変数は省略した．「情報セキュリティ疲労度」から各因子間へのパス係数は，「回避願望」へは 0.695,「消耗感」へは 0.617，そして「当事者意識の低さ」へは 0.707 であり，それぞれの下位因子の「情報セキュリティ疲労度」に対する影響の差異は小さかった．

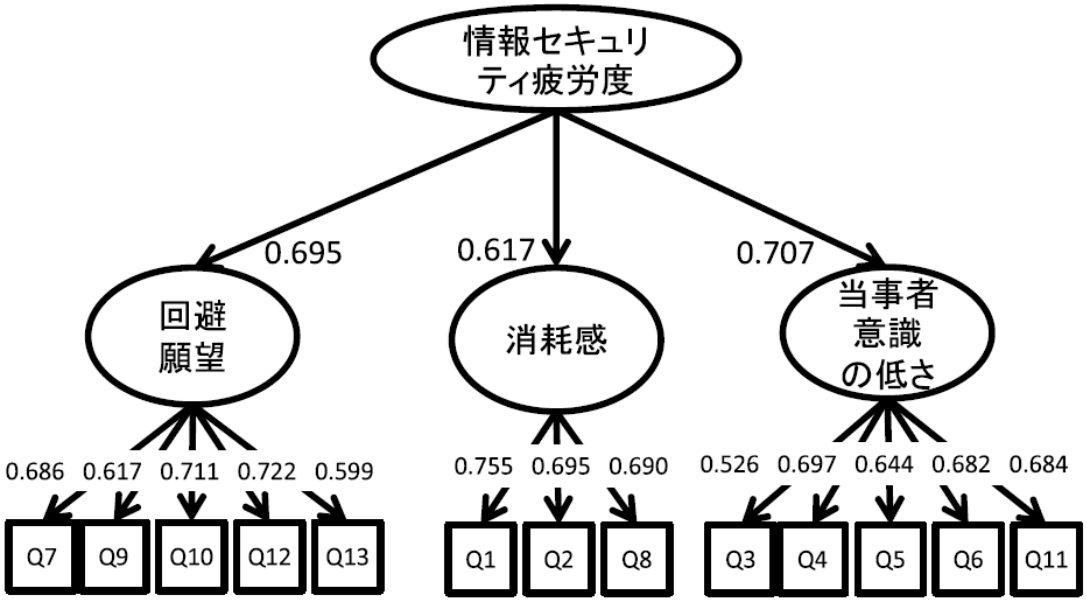

図 10.4　SFS-13 の下位因子構造を表すパス図 [畑島 2018a]

また，それぞれの下位因子から観測変数である設問項目へパス係数 0.526〜0.755 であり，ばらつきは小さかった．また，$\chi^2(62) = 93.37, p < 0.01$ であり，適合度指標は GFI (Good Fit Index) は 0.962，CFI (Comparative Fit Index) は 0.903，RMSEA (Root Mean Square Error of Approximation) は 0.079 であった．GFI を参照するととてもあてはまりが良く，CFI ではあてはまりが良く，RMSEA についてはややあてはまりの良いモデルであると示された．

以上の検討により，最終的に情報セキュリティ疲労度を測定する尺度として 3 因子からなる 13 項目からなる大学生版セキュリティ疲労度測定尺度 SFS-13 を確定した．この結果（質問紙の完成版）を表 10.10 に示すとともに，付録 Ⅳ-3 に掲載する．

表 10.10　確定したセキュリティ疲労度測定尺度 SFS-13

項番	質問文	因子名	初期質問項目の項番（表 10.6）
Q1	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	消耗感	PQ5
Q2	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	消耗感	PQ6
Q3	情報セキュリティ対策は必要悪だと思うことがある	当事者意識	PQ7
Q4	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	当事者意識	PQ8
Q5	情報セキュリティ対策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	当事者意識	PQ9
Q6	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	当事者意識	PQ11
Q7	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	回避願望	PQ12
Q8	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	消耗感	PQ14
Q9	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	回避願望	PQ15
Q10	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	回避願望	PQ16
Q11	私はセキュリティ対策に自信があると思うことがある	当事者意識	PQ18
Q12	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	回避願望	PQ19
Q13	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	回避願望	PQ24

10.4.4　SFS-13 確定後の確認調査

10.4.4.1　確認調査

10.4.3 で確定した質問紙の尺度得点を計測する確認調査を首都圏内の私立大学 2 大学で行った (表 10.4(10))．調査は 2017 年 9 月 28 日から同年 10 月 11 日に実施し，調査協力者は予備調査と同一の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，及び前記と異なる首都圏の私立大学に通う 2 年生 82 名による 392 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，謝礼は提示しなかった．今回は性別と年齢について回答を求めた．これらから欠損値あるデータを除外した 337 票を有効回答とした (有効回答率 86.0%)．有効回答者の年齢について記述統計量を表 10.11 に示す．男性は 276 名（平均 19.66 歳，標準偏差 (SD) 1.40），女性は 61 名（平均 19.54 歳，標準偏差 1.34），全体では 337 名（平均 19.64 歳，標準偏差 1.38）であった．

10.4.4.2　確認調査結果の分析

ここでは確認調査結果の分析を行う (表 10.4(11))．尺度得点は，回答は，「ない」を 1 点，「まれにある」を 2 点，「時々ある」を 3 点，「しばしばある」を 4 点，「いつもある」を 5 点として，全体及び下位尺度ごとに加算したものを用いた．このため尺度得点の範囲は 13 点から 65 点となる．この尺度得点により質問項目に対する回答を定量的に処理することが可能となる．

具体的な利用例を以下に示す．確認調査結果の尺度得点の記述統計量は表 10.12 のようになった．全体の平均得点は 30.77 であり，標準偏差は 9.00 であった．男性の平均得点は 30.30，標準偏差 8.90 であり，女性の平均得点は 32.89，標準偏差 9.24 であった．男性と女性の尺度得点について平均の差の検定結果は 5% 水準で有意であった．下位尺度ごとの尺度得点の記述統計量は表 10.13 のようになった．尺度得点の平均の差の検定を実施したところ，消耗感 (男性 (平均 9.61，標準偏差 2.89)，女性 (平均 10.72，標準偏差 2.69)) について，1% 水準で有意な差が認められた．その他の回避願望 (男性 (平均 10.01，標準偏差 4.21)，女性 (平均 10.59，標準偏差 4.78)) と，当事者意識 (男性 (平均 10.68，標準偏差 4.09)，女性 (平均 11.57，標準偏差 4.20)) では有意な差は認められなかった．

また，後述の **10.4.5** で示すセキュリティ疲労度の算出手法のうち”(a) 回答結果を予備調査（**10.3.3**）と同様の採点でセキュリティ疲労度の尺度得点を算出し，尺度得点の順位を用いてあらかじめ決めた人数分布の割合によって段階付けをする方法”を用いて，尺度得点の上位 25% を疲労度が高程度，中間を疲労度が中程度，下位 25% を疲労度が低程度

と 3 段階に分類した.

SFS-13 開発当時は，このように段階分けされた各群には **10.3.5** に示した特徴が現れるものと考えられるが，より精緻な特徴の解明を探求する場合は大規模調査による検証が必要であるとしていた．その後の研究（**11.1.3**）において SFS-13 を用いたセキュリティコンディションマトリクスによるリスクアセスメントを実施した際に同様の傾向がみられることを確認した．一例として，尺度得点の四分位値で疲労度の低 (L：n=75)，中 (M：n=180)，高 (H：n=82) の 3 段階に段階分けした情報セキュリティ疲労度の各段階の下位尺度得点は表 10.14 のようになったように，疲労の段階がどの程度であるかを可視化することも実現した.

以上のように，大学生版セキュリティ疲労度測定尺度 SFS-13（表 10.10）を用いて調査を実施し，全体の記述統計量の分析が可能となる．また，全体の評価だけでなく，個人の状態の把握なども可能であり，今後，セキュリティ疲労度に対する具体的な対策の提案に結び付けられることを明らかにした.

表 10.11　SFS-13 確認調査結果：有効回答者の記述統計量

大学生全体 (n=337)		男性 (n=276)		女性 (n=61)	
平均年齢	SD	平均年齢	SD	平均年齢	SD
19.66	1.40	19.54	1.34	19.64	1.38

表 10.12　SFS-13 確認調査結果：尺度得点の性別記述統計量

性別	n	平均	SD	歪度	尖度
男性	276	30.30	8.90	0.34	-0.57
女性	61	32.89	9.24	0.63	0.89
全体	337	30.77	9.00	0.40	-0.18

尺度得点について男女の平均の差が 5% 水準で有意であった.

表 10.13　SFS-13 確認調査結果：下位尺度得点の性別記述統計量

下位尺度	属性	平均	SD
回避願望	男性	10.01	4.21
	女性	10.59	4.78
	全体	10.12	4.32
消耗感	男性	9.61	2.89
	女性	10.72	2.69
	全体	9.81	4.32
当事者意識	男性	10.68	4.09
	女性	11.57	4.20
	全体	10.85	4.12

消耗感の尺度得点について男女の平均の差が 1% 水準で有意であった.

表 10.14　SFS-13 確認調査結果：尺度得点の四分位値で分類した疲労度段階別の下位尺度得点の記述統計量

下位尺度	疲労度段階	平均	SD
回避願望	疲労度高（H）	15.93	2.89
	疲労度中（M)	9.47	3.04
	疲労度低（L）	6.22	1.30
消耗感	疲労度高（H）	11.85	2.06
	疲労度中（M)	10.34	2.30
	疲労度低（L）	6.76	2.25
当事者意識	疲労度高（H）	15.60	3.28
	疲労度中（M)	10.71	2.94
	疲労度低（L）	6.80	1.97

10.4.5　情報セキュリティ疲労度測定尺度の利用方法

本研究では，セキュリティ疲れを測定する測定尺度を一般的な燃え尽きを測定するバーンアウト測定尺度の援用により作成し，大学生に対する質問紙調査により確定することによって，情報セキュリティ疲労度の可視化を行った．**10.4.4.2** で分析したように，本研究で得られた質問紙を用いた調査によって ICT 利用者の情報セキュリティ疲労度を明らか

にすることにより，疲労度の段階に合わせた対策施策が可能となる．得られた測定尺度 SFS-13 を利用した確認調査の結果，尺度得点全体に対する大学生の男女間の平均の差について 5% 水準で有意な差が認められ，下位尺度である消耗感においては 1% 水準で有意であった．換言すると，大学生を対象とした本研究においては，女性は男性と比較して消耗感が大きく表れる結果，より情報セキュリティ疲れを起こしうる傾向が示された．

セキュリティ疲労度を用いた対策の実施例として，**10.3.5** で述べた各段階に属した回答者に対するヒアリング等によるアセスメントにより各状態の特徴を抽出した研究のように，中間段階を理想状態とし，理想状態にある場合はこれを維持し，それ以外の状態にある場合は理想状態に近づけるためにそれぞれの段階に有効な施策を設計し実施する方法が想定される．このような施策について，実施の前後で情報セキュリティ疲労度尺度得点の分布や，個人の尺度得点の変化を考察することにより対策効果の測定が可能であると考える．そのほか，複数の組織に対する質問紙調査を実施する場合においては，情報セキュリティ対策の実施の程度によって，組織ごとの情報セキュリティ疲労度の分布の比較といった評価が可能であると考える．

対策の実施前後の効果測定に対する具体的な想定例としては，パスワードを定期的に変えることを強制する情報セキュリティ対策施策について，NIST のガイドライン [Grassi2017] では実施すべきでないと記され，総務省の情報提供 [総務省 2018] でも不要と記されていることを知っている場合は，その対策の実施を求められることについて，確定した測定尺度 SFS-13(表 10.10 もしくは付録 Ⅳ-3）の Q3 のように，必要悪であると感じることが強くなることが考えられる．

10.4.6　考察

10.4.6.1　SFS-13 開発研究に関する考察

本研究では，大学生版セキュリティ疲労度測定尺度 SFS-13 を用いた質問紙調査を測定対象に対して実施し，得られた回答について以下のように分析することにより，疲労度の段階分けを実施している．各回答者の疲労度の算出については，下記の手法が想定される．(b) は全国調査などの大規模な蓄積が実現されれば絶対的な評価に近づくものと思われるが，そうした規模での調査の実現性については将来の課題とし，萌芽的な研究である本研究では (a) を想定した．

(a) 1 回の調査に閉じた分析により相対的な疲労度を算出する方法
(b) それまでに蓄積された分析の結果との比較や回答結果と合わせた再計算によって相対

的な評価を実施する方法

相対的な疲労度算出の具体例として，以下の方法が挙げられる．

(i) 回答結果を **10.5** で示した予備調査と同様の採点で情報セキュリティ疲労度の尺度得点を算出し，尺度得点の順位を用いてあらかじめ決めた人数分布の割合によって段階付けをする方法
(ii) 先行研究（**10.3.5**）で実施例を示した荘島による潜在ランク理論 [荘島 2008] を用いて段階付けをする方法

本測定尺度の品質について，質問紙調査においては，**10.3.3** と **10.3.4** と **10.4.1** に示した手順により不誠実な回答者が除外されており，回答者数の充足性は **10.4.2** で Kaiser-Meyer-Olkin のサンプリング適切性基準 (KMO) による検証がなされ，また **10.4.3** において信頼性と妥当性の検討がなされていることから，因子分析の実施に充分なものとなっていると考える．

10.4.6.2　本研究の限界点

本研究では，セキュリティ疲労度を測定する萌芽的研究として，その測定に一般的なバーンアウトの測定尺度を援用できる仮定のもと，尺度の測定手法について提案した．このため，**10.2.2** で述べたようにバーンアウト尺度は職業的燃えつきによる一般生活全体に対する疲労度であるのに対し，情報セキュリティ疲労度が ICT 利用時の情報セキュリティ対策実施に対する疲労度であることが留意点である．

また，本研究では，初期検討として，調査並びに評価が比較的容易である大学生を対象とした質問紙調査を実施したが，調査規模への懸念がある．本調査では 1 大学 81 名への調査であったが，KMO によるサンプリング適切性基準は満たしていた．確認調査では 2 大学の 350 名を対象とし，充分なデータ収集ができた．これらの結果を踏まえたより大規模の調査，社会人への調査は，今後の課題とした．

10.5　SFS-13 開発研究のまとめ

本研究では **10.3** と **10.4** で述べた方法で大学生版セキュリティ疲労度測定尺度 SFS-13 を開発した．

ICT 利用者が常に求められる情報セキュリティ対策施策に対して疲弊してしまう“セキュリティ疲れ”について，一般的なバーンアウトの測定尺度を援用した質問紙を作成し

た．大学生を対象とした質問紙調査によって「(情報セキュリティ対策からの) 回避願望」(5 項目),「(情報セキュリティ対策に対する) 消耗感」(3 項目),「(情報セキュリティ対策に対する) 当事者意識」(5 項目) の三つの下位尺度による 13 項目の質問紙が導かれた．確認調査の結果，情報セキュリティ疲労度の男女別の尺度得点平均値に 5% 水準で有意な差が認められ，下位尺度である消耗感の男女別の尺度得点平均値に 1% 水準で有意な差が認められた．換言すると，女性は男性と比較して消耗感が大きく表れる結果，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た．本研究で得られた質問紙調査によって，ICT 利用者の情報セキュリティ疲労度可視化を実現し得ることを明らかにし，今後，情報セキュリティ対策における悪循環の対処法に供し得ることを示した．

10.6　汎用版セキュリティ疲労度測定尺度（SFS-9）の開発

大学生版セキュリティ疲労度測定尺度 SFS-13 の研究（**10.4**）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．開発した測定尺度（表 10.10 もしくは付録 IV-3）は，職業的バーンアウトを援用していることからもみられ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したものにとどまっていた．本研究により開発した汎用版セキュリティ疲労度測定尺度 SFS-9（Security Fatigue Scale-9）[畑島 2020] 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である．

10.6.1　測定尺度開発行程と質問紙調査

10.6.1.1　測定尺度開発工程

測定尺度の開発手順は，SFS-13 開発時（表 10.4）と同様に実施する．具体的には，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．

本研究では，付録 IV-2 に示した質問紙が本番調査の質問紙にあたる（**10.6.1.2.2**）．この質問紙には，**10.4** で得られた測定尺度 SFS-13（表 10.10 もしくは付録 IV-3）が含まれている．

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因子構造を確定し（**10.6.2.2**），下位尺度の命名や構成する概念の決定を行う（**10.6.2.3**）．そののち信頼性の検討（**10.6.3**）および妥当性の検討（**10.6.4**）を実施し，本研究の汎用版セキュリティ疲労度測定尺度 SFS-9 を確定する．

10.6.1.2　質問紙調査

■10.6.1.2.1　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 **10.6.2.2** 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 Ⅳ-2 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 Ⅳ-2 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．業種ごとの回答者数割付けは，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，**10.4** で述べた SFS-13 開発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回答者での検証を実施する目的で収集した．

■10.6.1.2.2　**質問紙の構成**　本研究に用いる質問紙は付録 Ⅳ-2 に示す設問で構成した．

設問 1 大学生版セキュリティ疲労度測定尺度 SFS-13
設問 2 情報セキュリティに対する所感（自由回答）[畑島 2017e]
設問 3 情報セキュリティ疲労度の自己申告（5 件法）
設問 4 ICT 利用に関する質問（利用歴，1 日の利用時間）
設問 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通りであった．設問 1 への回答結果に対して **10.6.2** 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，設問 2 および設問 3 を用いて基準関連妥当性の検証した（**10.6.4.2**）．また設問 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，**10.6.2.2** において不誠実な回答者の除外に用いた．そして設問 5 は，**10.6.9.1.1** 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際の区分設定に用いた．なお，同じく **10.6.9.1.1** 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設定を行ったが，これら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．

10.6.2　汎用版セキュリティ疲労度測定尺度 SFS-9 の開発

本章では **10.6.1.1** 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 SFS-9 の開発内容を述べる．

10.6.2.1　SFS-9 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 version3.6.1 を用いた．

まず得られた因子構造を示し，続いてこれを導くために実施した因子分析（**10.6.2.2**）および因子の命名（**10.6.2.3**）の詳細について述べる．因子分析は大学生版尺度の開発時 **10.4.2** 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実行し，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 10.15 に示す因子パターンを持つ 9 項目が得られた．

表 10.15　SFS-13 を社会人に対して質問紙調査した結果の因子分析表

項目	因子 I	因子 II	因子 III	共通性
因子 I 情報セキュリティ対策に対する意欲の低下				
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	**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
因子 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
因子 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**	0.681
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
	1		
因子負荷行列	0.188	1	
	0.486	0.244	1

10.6.2.2　因子分析

まず因子分析の前処理として，質問紙調査 **10.6.1.2** の結果から不誠実な回答を除外した．除外ルールは以下の通りとした．

a) 設問 1 のすべての項目の回答が同一であるものを除外
b) 設問 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

この除外処理の結果，社会人の回答者数は 1134 件となり，有効回答率は 91.2% であった．有効回答者の全体および男女の構成は表 10.16，年齢分布は表 10.17 のようになり，社会人全体（n=1134）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，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，**10.6.2.1** 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 SFS-13 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 Ⅳ-2 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 Ⅳ-2 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 Ⅳ-2 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 Ⅳ-2 設問 1–8）」の 4 項目を除外した．その結果 9 項目の設問から構成される因子構造となった．

表 10.16　有効回答者（社会人）の構成

社会人全体 N=1134		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

表 10.17　調査対象者の人数分布（社会人）

年齢	男性（%）	女性（%）	全体（%）
12 歳〜19 歳	0(0.0)	1(0.2)	1(0.1)
20 歳〜24 歳	8(1.2)	28(6.3)	36(3.2)
25 歳〜29 歳	31(4.5)	84(1.8)	115(10.1)
30 歳〜34 歳	63(9.2)	97(21.7)	160(14.1)
35 歳〜49 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

10.6.2.3　因子の命名

上述の因子分析の結果，因子構造は表 10.15 に示すようになった．それぞれの下位尺度を以下のように命名した（表 10.15）．

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 [Stanton2016] 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 [北村 2001] 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 [久保 2004] 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 [Stanton2016] 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．

10.6.3　信頼性の検討

10.15 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））．

10.6.4　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 [吉田 2007] .

10.6.4.1　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，本研究は **10.4** で述べた成果である大学生版の質問紙（付録 Ⅳ-2 設問 1）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．

10.6.4.2　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：自由回答者の SFS-9 ランク］と［データ B：自由回答］の組み合わせ，および［データ A：SFS-9 ランク］と［データ C：疲労度自己申告］の組み合わせの，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 [南風原 2002].

以下に本項で用いるデータを整理する．［データ B：自由回答］以降のデータ数が 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．

- ［データ X：SFS-9 全回答］：付録 Ⅳ-2 設問 1 の 13 項目（つまり SFS-13）に対する回答のうち．**10.6.2.2** で実施した因子分析の結果残った 9 項目（つまり SFS-9 の

候補）に対する回答（n=1134）

- ［データ A：SFS-9 ランク］：［データ X：SFS-9 全回答］に対して **10.2.5.2** 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（n=1134）
- ［データ B：自由回答］：付録 Ⅳ-2 設問 2 の記述回答形式の設問に回答にした全実験参加者を，セキュリティ疲労度の 5 段階の特徴分類（**10.7**）に従って筆者らの議論により振り分けた結果（n = 348）
- ［データ C：疲労度自己申告］：付録 Ⅳ-2 設問 3 に対する回答結果．つまり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（n=1134）
- ［データ D：自由回答者の SFS-9 ランク］：［データ X：SFS-9 全回答］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結果（n = 348）

■10.6.4.2.1　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の連関　ここでの検討により，「本研究で検討を進めてい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：自由回答者の SFS-9 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セキュリティ疲労度レベルごとの自由回答の特徴分類（表 10.7）に従って 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 10.5 の横軸［データ D：自由回答者の SFS-9 ランク］（n = 348）を参照すると，ランク 4 が最も多く（合計 124 名），ランク 2 が最も少なかった（合計 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（合計 137 名），ランク 1 が最も少なかった（合計 28 名）．

表 10.5 に対してカイ 2 乗検定を行った結果，Cramer の連関係数（Cramer’s association coefficient）は $V = 0.26$（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 [水本 2008] では効果量は小（0.10〜0.30）であり，有意だった（$\chi^2(16) = 96.97$，$p < 0.001$）．

Cramer の V について豊田 [豊田 2016] 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．なお水本ら [水本 2008] 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 10.5 に対して Spearman 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，$p < 0.001$）．

図 10.5　横軸［データ D：自由回答者の SFS-9 ランク］，縦軸［データ B：自由回答］の対応表 [畑島 2020]

■10.6.4.2.2　セキュリティ疲労度の自己申告結果とセキュリティ疲労度測定結果の連関

同様にして，「本研究で検討を進めてい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：SFS-9 ランク］（n=1134）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：疲労度自己申告］（n=1134）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 10.6 に横軸にとった［データ A：SFS-9 ランク］（n=1134）と，縦軸にとった［データ C：疲労度自己申告］（n=1134）との対応表を示す．横軸の［データ A：SFS-9 ランク］では疲労度 5（合計 389 名）が最多であり疲労度 4（合計 112 名）が最少であった．縦軸の［データ C：疲労度自己申告］では，疲労度 3（合計 418 名）が最多であり疲労度 5 が最少（合計 76 名）であった．

10.6.4.2.1 と同様に表 10.6 の Cramer 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（$\chi^2(16) = 272.75$

，$p < 0.001$）．このことから，**10.6.4.2.1** 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ことがわかった．

また，表 10.6 に対して Spearman 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，$p < 0.001$）．

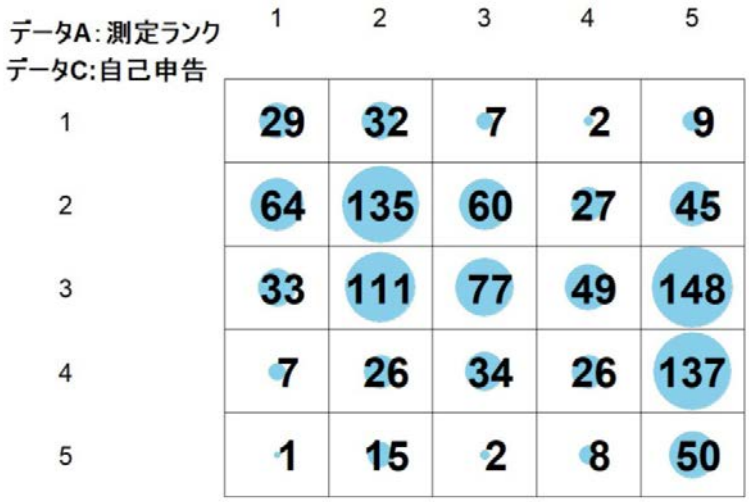

図 10.6　横軸［データ A：SFS-9 ランク］，縦軸［データ C：疲労度自己申告］の対応表 [畑島 2020]

10.6.5　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 10.15）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，SFS-13 から 4 項目を除外して得られた，セキュリティ疲労度測定尺度 SFS-9（表 10.15 もしくは付録 Ⅳ-4）を確定した．

10.6.6　SFS-9 の大学生への適用

10.6.1.2.1 で取得した大学生からの回答を利用し，社会人からの回答を利用して得られた因子構造（表 10.15）に対して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，**10.6.2.2** 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，大学生の回答者数は 593 件となり，有効回答率は 96.0% であった．

大学生の有効回答者の構成は表 10.18，年齢分布は表 10.19 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，大学生回答者に対しても大学生版測定尺度 SFS-13 の研究 (**10.4**) における適合度指標を上回り，本研究の社会人回答者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））．

10.6.7　汎用版情報セキュリティ疲労度測定尺度 SFS-9 の確定

以上の検討から，表 10.15 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．

表 10.18　有効回答者（大学生）の構成

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

表 10.19　調査対象者の人数分布（大学生）

年齢	男性（%）	女性（%）	全体（%）
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〜49 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

10.6.8　考察

10.6.8.1　因子構造

10.6.2.1 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 Ⅳ-2 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 Ⅳ-2 設問 1–5）と除外項目 3（付録 Ⅳ-2　設問 1–7）および除外項目 4（付録 Ⅳ-2 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，「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（**10.4**）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（**10.4**）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た．

10.6.8.2 信頼性の検討

信頼性検討のために Cronbach の α を求めた結果，**10.6.3** に挙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．

10.6.8.3 妥当性の検討

■10.6.8.3.1 **基準関連妥当性** 基準関連妥当性について村上 [村上 2013] 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 **10.2.6** に挙げた情報セキュリティ心理尺度は図 10.2 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（付録 Ⅳ-2 設問 2）と情報セキュリティ疲労に関する自己申告（付録 Ⅳ-2 設問 3）を用いた．

これらを用いた **10.6.4.2.1** および **10.6.4.2.2** での検討により，基準関連妥当性を確認した．なお，**10.6.4.2.1** で挙げたように，水本ら [水本 2008] 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，Cramer の連関係数 V や Spearman の ρ による評価は確定的なものではない．

■10.6.8.3.2 **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（10.4）と本研究（**10.6**）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（**10.4**）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，より一般的な回答が得られ，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．

■10.6.8.3.3 **大学生への適用** **10.6.4.1**，**10.6.6** および **10.6.8.3.2** 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 [村山 2018] を参照した．

10.6.9　SFS-9 の利用例

10.6.9.1　バックグラウンドファクタによる差異

■10.6.9.1.1　平均の差の検定結果　表 10.20 に示すように，バックグラウンドファクタの 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 Student の t 検定を，仮定できなかった場合は Welch 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（なお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），さらに (5) 情報システムの利用者（平均 3.26，SD1.47）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．

■10.6.9.1.2　バックグラウンドファクタによる差異に関する考察　表 10.20 の分析結果である **10.6.9.1.1** を参照し，バックグラウンドファクタによる差異を考察する．(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，(**10.4**) で述べた大学生版測定尺度 SFS-13 の下位尺度を統計的検定した研究において，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.

表 10.20　SFS-9 により測定されたセキュリティ疲労度の平均値の差の検定

		SFS-9 による疲労度の平均と SD		$t(df)$,p と効果量 r
(1)	（全体） 男性と女性	男性 n=842 3.19 (1.51)	女性 n=885 3.44 (1.40)	$t(1700.5) = -3.540$, $p < 0.001$, $r = 0.008$
(2)	大学生と社会人	大学生 n=593 3.42 (1.44)	社会人 n=1134 3.27 (1.47)	$t(1725) = -2.021$, $p < 0.05$, $r = 0.05$
(3)	（社会人） 技術系と非技術系	技術系 n=263 3.33 (1.51)	非技術系 n=871 3.25 (1.46)	$t(1132) = 0.754$, $p = 0.451$, $r = 0.02$
(4)	（社会人） 個人年収	400 万円未満 n=394 3.26 (1.49)	400 万円以上 n=513 3.22 (1.49)	$t(905) = -0.407$, $p = 0.684$, $r = 0.02$
(5)	（社会人） 利用者と 管理者・運用者	利用者 n=1003 3.26 (1.47)	管理者・運用者 n=102 3.17 (1.45)	$t(1103) = 0.612$, $p = 0.541$, $r = 0.01$
(6)	（社会人・利用者） 組織が決めた 規約の有無	規約あり n=844 3.30 (1.48)	規約なし n=159 3.04 (1.40)	$t(1001) = -2.080$, $p < 0.05$, $r = 0.06$

10.6.10　SFS-9 開発研究の限界

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．

10.7　SFS-9 開発研究のまとめ

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（**10.4**）の大学生版尺度 SFS-13 は 3 因子 13 項目で構成されていたが，本研究の結果 4 項目削減された 3 因子 9 項目の構成へと簡便化した．また，本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．

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 10.2 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 [Sharif2018] 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構築研究などにおいて，データを分類するための基準として，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．

10.8　セキュリティ疲労度測定尺度開発研究のまとめ

本研究ではセキュリティ疲労度測定尺度 SFS-13（**10.3**，**10.4**）および，その汎用版である SFS-9（**10.6**）を開発した．

測定尺度の導出には，一般的なバーンアウトの測定方法を援用し，質問紙調査により実施した．仮説となる質問紙を用いて調査協力者に質問紙調査を実施し，因子分析の結果得

られた因子構造について，因子名の命名，信頼性と妥当性の検討を行うことで質問紙を確定した．本研究ではまず，調査対象を大学生とした大学生版セキュリティ疲労度測定尺度 SFS-13 を開発したのち，調査対象を一般に広げた汎用版セキュリティ疲労度測定尺度 SFS-9 を開発した．

得られた測定尺度を用いた応用研究を次の **11** で述べる．

第 11 章

セキュリティ疲労度測定尺度の応用

本章では前章の研究で開発したセキュリティ疲労度測定尺度を用いた応用研究について述べる．本章ではそれぞれについて概要を述べ，続いてそれぞれの詳細を述べる．具体的には，以下の研究を実施した．

- セキュリティコンディションマトリクスとその応用
  1. セキュリティ疲労度測定尺度による測定結果とセキュリティ対策の実施度をマトリクス化したセキュリティ状態の可視化．および，理想状態の維持もしくは理想状態への行動変容を促す施策に対するリスクアセスメントと机上検討．
  2. 上記 1 の各状態に対して，別の測定尺度を用いて更にセキュリティコンディションマトリクス上の状態を細分化しての 1 同様のリスクアセスメント．
- セキュリティ疲労度測定尺度の性質に関する考察の一例として，情報セキュリティに対する内部犯行者の性質の測定
  1. 情報セキュリティインシデントのうち内部不正について潜在的犯行者 (likely offenders) の性質をセキュリティ疲労度測定尺度によって観測可能であるかの検討

なお，研究の時系列関係から，本章で述べたそれぞれの研究で用いたセキュリティ疲労度測定尺度は SFS-13 である．つまり，SFS-9 はこれら研究以降に開発されたものである．

本章の構成は次の通りである．**11.1** では，セキュリティコンディションマトリクスの提案，マトリクス各状態に属するインターネット利用者の性向の分析，およびセキュリティ疲労改善のためのリスクアセスメント研究結果 [畑島 2018b] を順に述べる．

本研究ではまず，2017 年 7 月にセキュリティコンディションマトリクスを提案した [畑島 2017d]．これは，縦軸にセキュリティ疲労度の段階，横軸にセキュリティ対策実施

度をとった平面で構成されるものである．セキュリティコンディションマトリクスにはセキュリティ疲労について理想的な状態の可視化が可能である．その状態とは，縦軸の「セキュリティ疲労度」が中程度という理想的状態であり，横軸の「セキュリティ対策実施度」が高レベルにある状態である．

セキュリティコンディションマトリクスを構成する両軸それぞれ個別の理想状態について説明する．まず，セキュリティ疲労度の理想状態について，本研究でも 2017 年の SFS-13 開発の予備調査結果と同様に，セキュリティ疲労度の測定と同時に自由回答でセキュリティ対策についての所感を聞き，セキュリティ疲労度各段階に属する人の所感をまとめ，その段階の特徴を抽出した．セキュリティ疲労度には理想状態があり，セキュリティ対策について適度な緊張感がある状態を指す．本研究で実施した調査結果を分析した結果，この状態はセキュリティ疲労度を数段階に分類したときの中間に当たる段階が該当することが判明した．また，セキュリティ対策実施度はより高いほうがより理想的であることは論を待たない．

以上により，セキュリティコンディションマトリクスにおける理想状態とは，図 11.2 に示した状態である．換言すると，理想状態とは，縦軸の「セキュリティ疲労度が中間レベル」かつ横軸の「セキュリティ対策実施度が高いレベル」にあるときである．

理想状態以外は望ましくない状態である．そこで本研究では，リサーチクエスチョンとして，「理想状態にある人はその状態を維持し，それ以外の状態にある人を理想状態に近づけるにはどのような施策が取り得るか」を設定し，リスクアセスメントの手法により考えうる施策を抽出し効果を机上検討した．

11.2 では，別の側面からの心理測定尺度を用いて分類された各群に対してセキュリティコンディションマトリクスを適用することで群をさらに細分化し，その細分化された群ごとにリスクアセスメントを行った研究 [小川 2020] について述べる．具体的には，認知的方略と呼ばれる 4 パターンに人の行動パターンを分類したもので更に細分化し，それぞれのパターンについて **11.1.3** で述べたリスクアセスメントを同様に実施した．本件は共著研究であるため，概略について述べるのみとする．

11.3 では，セキュリティ疲労度測定尺度の性質に関する考察研究の例を述べる [畑島 2018d]．情報セキュリティインシデントの重大な要素である内部犯行について，実行者の性質を知ることでインシデントに対策がしうると考えられる．そこで本研究では，セキュリティ疲労度測定尺度が内部犯行者の性質を観測する質問をどれだけ含有しているかについて考察した．

11.1　セキュリティコンディションマトリクスの提案

11.1.1　セキュリティコンディションマトリクスの仮説

セキュリティ疲れ研究は，情報セキュリティ対策を求められる ICT 利用者がセキュリティ施策に対して疲れてしまうことによって，対策効果が低下することに問題意識を持つ．その解決策として，情報セキュリティ疲れや情報セキュリティバーンアウトの状態を把握する基準作りに関心を持ち，セキュリティコンディショマトリクスの検討を行った．

セキュリティコンディションマトリクスの検討は，セキュリティ疲労度測定尺度の開発と同時に行った．当初の研究 [畑島 2017d] でのセキュリティコンディションマトリクスの仮説を説明する．

当初のセキュリティコンディションマトリクスでは，縦軸としてセキュリティ疲労度をとり 3 段階にランク分けし，横軸に情報セキュリティ対策実施度をとり 2 段階にランク分けした 6 つ状態で検討していた．図 11.1 はセキュリティコンディションマトリクスの縦軸であるセキュリティ疲労度軸を **10.2.5.1** に示した「バーンアウト段階説」を用いて詳細化したものである．

換言すると，仮説段階ではセキュリティ疲労度は低ければ低いほど理想的であり，逆にセキュリティ疲労度が高くなるにつれ，その状態は疲労状態，バーンアウト状態と悪化していくことを想定していた．

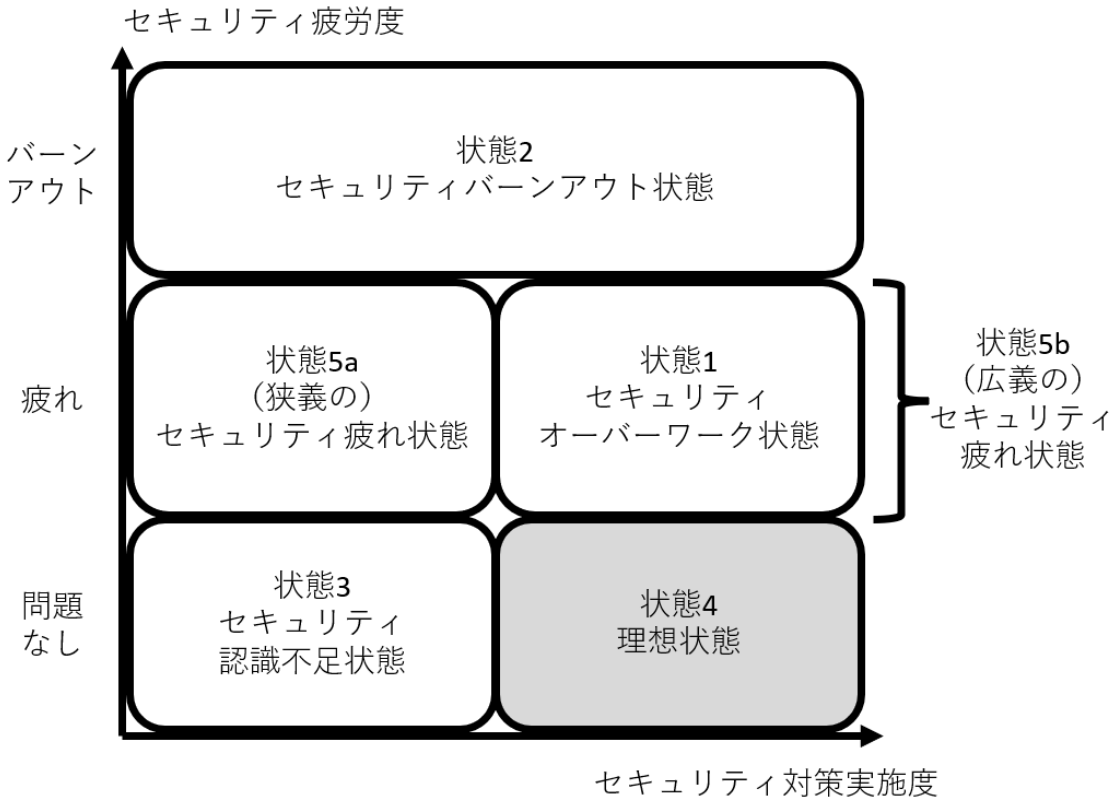

図 11.1　仮説のセキュリティコンディションマトリクス [畑島 2017d]

仮説セキュリティコンディションマトリクスを構成する各状態を説明する．

- 状態 1：セキュリティオーバーワーク状態 情報セキュリティ対策実施度は高いが，情報セキュリティ疲れがみられる状態である．この状態は状態 5b に述べるように広義の情報セキュリティ疲れ状態に含まれる．
- 状態 2：セキュリティバーンアウト状態 情報セキュリティコンディションマトリクスで最悪の状態である．この状態になると，情報セキュリティ遵守度にかかわらず情報セキュリティ対策を実施できなくなっており，危険な状態となっている．ビジネスや軍隊のようなプロジェクトのマネジメントではバーンアウト状態からの解消として，転地療法のように，バーンアウトを発生させた環境を抜本的に解消することが可能であるが，ICT は生活に根付いているため，これを解消することが困難であると考え，本研究における問題意識となっている．
- 状態 3：セキュリティ認識不足状態 情報セキュリティ疲れの状態は問題がないが，情報セキュリティ対策実施度が低いため，ICT 利用者の情報セキュリティ状態としては危険な状態である．このため，情報セキュリティ疲れを起こさず理想状態に移

行させる施策が必要である．

- 状態 4：理想状態 情報セキュリティ疲れの状態に問題がなく，情報セキュリティ実施度も高い理想的な状態である．ICT 利用者はこの状態にあることが望ましい．
- 状態 5a：狭義のセキュリティ疲れ状態 情報セキュリティ疲れの状態あって，情報セキュリティ実施度が低い状態である．疲労度が進展してバーンアウトとなることを回避する必要がある．即時的な対策施策として，集中的な研修やチェックリストの励行強化などにより情報セキュリティ実施度を上げて一時的にセキュリティオーバーワーク状態にすることが考えられるが，同時にセキュリティ疲れが進行するとバーンアウトしてしまうため，慎重な施策が必要である．一方，情報セキュリティ疲れ状態を問題ない状態にすると，ICT 利用者のセキュリティ疲れは低減されているが，セキュリティ認識不足状態となる．これも危険な状態であるためこの状態に留まることを避ける必要がある．
- 状態 5b：広義のセキュリティ疲れ状態 セキュリティオーバーワーク状態と狭義の情報セキュリティを併せて，広義の情報セキュリティ疲れ状態と定義する．この状態からバーンアウトしないよう，セキュリティ疲れを低減させることが求められる．

10.3.5 で述べたように，セキュリティ疲労度測定尺度の研究においてセキュリティ疲労度の段階ごとの性質を明らかにした．具体的には，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，**10.3.5** で述べた先行研究 [畑島 2017e] で作成した設問（付録 Ⅳ-1 設問 2）「あなたは，情報セキュリティについて，どのように考えていますか，お考えを自由に記述して下さい」に対する自由回答結果から「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，本研究では，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て，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 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，本研究では F 群と Im 群の組合せによる 6 群に対して検討を進めた．

10.3.5 の結果から，情報セキュリティ疲労度は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 11.1 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 11.2 にのように改善され，F0ImH 群が理想状態であると定めた．

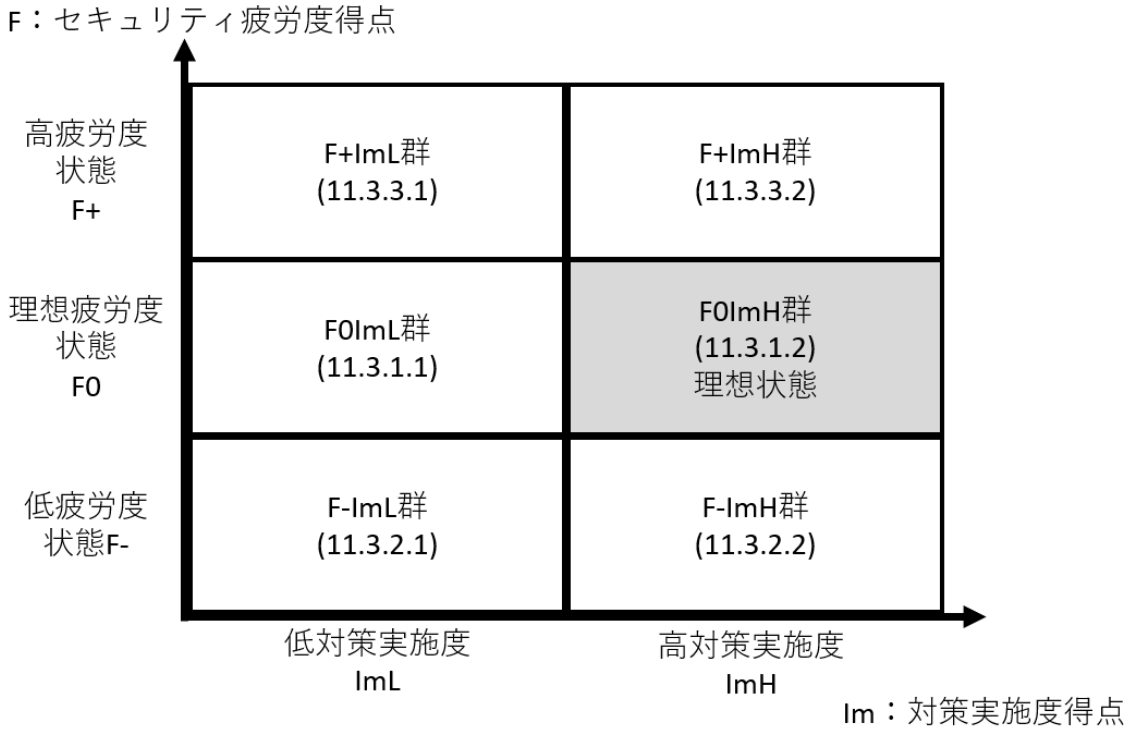

図 11.2　導出したセキュリティコンディションマトリクス [畑島 2018b]

11.1.2　セキュリティコンディションマトリクスの検証

11.1.1 での議論は質問紙調査の回答者数が限られたものであった．そこで同じ質問紙を用い調査規模を拡大してセキュリティコンディションマトリクスを検証した結果を述べる．結論として，**11.1.1** で導出したセキュリティコンディションマトリクス（図 11.2）と同様のマトリクス構造が得られた．

ここではセキュリティコンディションマトリクスを構成する 6 群それぞれの特徴を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．考察は図 11.2 に示した項番ごとに行う．

11.1.2.1　質問紙の作成

本研究で用いた質問紙を付録 Ⅳ-5 に示し，以下に各設問項目を説明する．

■11.1.2.1.1　セキュリティ疲労度測定尺度　設問 1 のセキュリティ疲労度測定に使用した質問項目は，本検証時最新であった **10.4** で導出したセキュリティ疲労度測定尺度 SFS-13 である．

■11.1.2.1.2　セキュリティ対策実施度　設問 2 の情報セキュリティ対策実施度の測定には，**6** で述べた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に関する先行研究 [畑島 2017b] で用いた尺度を援用した．具体的には，測定にウイルス感染経験，IT 知識および IT スキルを設定した浜津ら [浜津 2015] 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 [IPA2016]，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 [総務省 2017] 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．なお本調査で使用した質問項目は，ここ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 11 項目である．

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．設問 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と考える．また，今回質問紙調査を実施した両大学においても，設問 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 [法政大 2018] 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．

■11.1.2.1.3　セキュリティ対策に関する個人の所感　設問 3 として，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．

11.1.2.2　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 日に実施し，392 名から回答を得た．調査協力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 名分を有効回答（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．

11.1.2.3　セキュリティコンディションマトリクスへの回答者の割付

潜在ランク理論を用いて回答者をセキュリティコンディションマトリクスに割りつけた．セキュリティ疲労度測定尺度 SFS-13 およびセキュリティ対策実施度の質問それぞれに潜在ランク理論による分析を行った．分析には荘島によるソフトウェア exametrika（エクザメトリカ）[荘島 2017] 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した．手順 (1) では，潜在ランク数を 2 から順に大きくして exametrika を都度実行し，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 [植野 2010] とされている．

情報セキュリティ疲労度尺度 SFS-13 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 を実行した．分類数は **11.1.1** での仮説検証と同様に，F 群においては 3 群，Im 群においては 2 群にとした．exametrika 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 11.1 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 11.2 に，情報セキュリティ対策実施度の尺度得点は表 11.3 にそれぞれ示すようになった．

表 11.1　セキュリティコンディションマトリクス各群への割付人数

人数 (N=337)		Im 群 実施度低 ImL	Im 群 実施度高 ImH
F 群	疲労度高 F+	53	54
	疲労度理想 F0	60	60
	疲労度低 F–	61	49

表 11.2　セキュリティ疲労度の尺度得点と標準偏差

疲労度得点 (SD)		Im 群 実施度低 ImL	Im 群 実施度高 ImH
F 群	疲労度高 F+	40.08 (5.20)	41.09 (6.42)
	疲労度理想 F0	30.00 (3.36)	31.53 (4.53)
	疲労度低 F–	20.80 (3.58)	21.76 (3.35)

表 11.3　セキュリティ対策実施度の尺度得点と標準偏差

対策実施度得点 (SD)		Im 群	
		実施度低	実施度高
		ImL	ImH
F 群	疲労度高	30.34	41.00
	F+	(4.39)	(3.72)
	疲労度理想	29.03	39.92
	F0	(5.33)	(3.93)
	疲労度低	28.82	40.31
	F–	(4.80)	(3.53)

表 11.4　改善型セキュリティコンディションマトリクスに基づくリスクアセスメント結果および対策案と効果 [畑島 2018b]

群名 (論文内番号)	アセスメント結果 (各群に属する回答者の特徴)	対策案 ・理想状態への移行 ・理想状態の維持	対策効果の評価 (**11.1.4**) セキュリティ 疲労度 F	 セキュリティ 対策実施度 Im
F0ImL (**11.1.3.1.1**)	・市販製品を使う意志はあるが，製品の選定が出来ない ・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 (**11.1.3.1.2**)	・状況に応じた情報セキュリティ対策の難しさに対して指摘出来る ・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態度を見せる	(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 セキュリティ対策の提示が可能	維持	維持
		(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	維持	維持
F–ImL (**11.1.3.2.1**)	・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よいかわからない	(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) マニュアル化などの情報セキュリティ対策 内容のマニュアル化【マニュアル化】	上昇 (F0 へ)	上昇 (ImH へ)
F–ImH (**11.1.3.2.2**)	・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 (**11.1.3.3.1**)	・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 ・対策を実施していないことを認識し，自己分析する → 確信的に対策の実施を疎かにしている ・実施中の具体的な対策への不満や要望を示す	(10) 模擬的にセキュリティインシデントに 遭わせる演習の実施	降下 (F0 へ)	上昇 (ImH へ)
		(11) 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 (**11.1.3.3.2**)	・対策の当事者としての意識が薄い ・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) 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)	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) は 1 段階効果の可能性あり．(b) は変化無しの可能性あり．

11.1.3 改善型セキュリティコンディションマトリクスに基づくリスクアセスメント

ここでは表 11.4 のように得られた改善型セキュリティコンディションマトリクスに基づくリスクアセスメント結果について，群ごとに説明する．

11.1.3.1 セキュリティ疲労度 F0 の群

■11.1.3.1.1 F0lmL 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 11.1）は 60 名であった．情報セキュリティ疲労度尺度得点（表 11.2）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 11.3）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 ID321)」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，ウイルスパターンの配信やウイ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．

■11.1.3.1.2　F0ImH 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 11.1）は 60 名であった．情報セキュリティ疲労度尺度得点（表 11.2）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 11.3）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 **11.1.3.2.2** 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．

11.1.3.2 セキュリティ疲労度 F–の群

■11.1.3.2.1 F–lmL 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 11.1）は 61 名であった．情報セキュリティ疲労度尺度得点（表 11.2）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 11.3）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．

■11.1.3.2.2 F–lmH 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 11.1）は 49 名であった．

情報セキュリティ疲労度尺度得点（表 11.2）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 11.3）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．

前者である (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挙げられる．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 ID269）」のように，具体的な情報セキュリティ対策実施を挙げ，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．

後者である (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 ID56）」，「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挙げられる．

この群を理想状態に移行させるには，**11.1.3.2.1** 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．

11.1.3.3 セキュリティ疲労度 F+ の群

■11.1.3.3.1 F+lmL 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 11.1）であった．情報セキュリティ疲労度尺度得点（表 11.2）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 11.3）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，本研究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挙げられる．

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，**6.3** や **10.2.6** 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) は本研究の調査においてはこの群および **11.1.3.3.2** 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．

■11.1.3.3.2　**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 11.1）は 54 名であった．情報セキュリティ疲労度尺度得点（表 11.2）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 11.3）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．

11.1.4　リスクアセスメント結果の机上評価

これまでに示した 14 種類の対策案（表 11.4）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．14 種類の対策案および対策の効果は，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．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（**11.1.3.1.1**）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（**11.1.3.1.2**）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（**11.1.3.2.1**）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（**11.1.3.2.2**）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（**11.1.3.2.2**）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（**11.1.3.3.1**）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うる．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（**11.1.3.3.2** ）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．

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，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挙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．

11.1.5　本研究の限界

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，**11.1.3.3.1** に挙げた 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，より大きな回答者数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，本研究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挙げられる．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，今後検討すべき事項である．

11.1.6　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，今回はセキュリティコンディションマトリクスに関する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．

11.2 認知的方略を用いたセキュリティコンディションマトリクス細分化によるセキュリティ疲労対策アセスメントの詳細化

11.2.1 概要

セキュリティコンディションマトリクスの応用例を述べる．セキュリティコンディションマトリクスは **11.1** で述べた分類方法以外でも同様の手法で検討が可能である．ここでは，セキュリティコンディションマトリクスの各群に対して他の心理尺度を用いて細分化しリスクアセスメントした結果 [小川 2020] を述べる．本研究においては，調査協力者を認知的方略（cognitive strategy）と呼ぶ 4 種類の行動パターンに分類し，それぞれの群に対してセキュリティコンディションマトリクスを求めることでセキュリティ疲れの状態を細分化し，細分化された各群について **11.1.3** 同様のリスクアセスメントを実施した．本件は共著による共同研究であるため，概略について述べるのみとする．

11.2.2 認知的方略

認知的方略の定義について，外山 [外山 2015] は，「問題状況に直面した際に，人が目標や行動に向かうための認知・計画・予期・努力の一貫したパターンのことである」と Norem の説明 [Norem1989] を紹介している．本研究では，認知的方略の測定尺度として外山 [外山 2015] が作成した質問紙（付録 Ⅳ-6）を用いた．この測定尺度は，悲観的予期”と “熟考” の 2 つを構成概念とする従来の認知的方略測定尺度（DPQ：Defensive Pessimism Questionnaire）に対して熟考の内容を細分化し，開発されたものである [外山 2015]．外山の測定尺度は，4 つの下位因子として「失敗に対する予期・熟考」，「過去のパフォーマンスの認知」，「性向に対する熟考」，「計画に対する熟考」を持つ．外山 [外山 2015] は，それぞれの下位尺度得点を用いたクラスター分析によって，表 11.5 に示す 4 群（防衛的

悲観主義群，楽観主義群，悲観主義群，メタ認知低群）が得られたことを報告している．

本研究においても外山の測定尺度を用いて質問紙調査を行い同様の手順でクラスター分析を行った結果，同様の 4 群が得られた．この 4 群に対してセキュリティコンディションマトリクスを適用して調査協力者を細分化し，セキュリティ疲労対策のアセスメントを行った．

表 11.5　外山による認知的方略の 4 分類 [外山 2015]

群名	外山の分類	説明
LM 群	メタ認知低群 (Low Meta-cognition)	メタ認知能力の低い人の群 （メタ認知とは，“自己の認知活動 （知覚，情動，記憶，思考など）を 客観的に捉え，評価した上で制御 すること”を意味する．）
RP 群	悲観主義群 (Regular/Realistic Pessimism)	物事すべてを悪いように考える人や， 将来について暗い見通しを持つ人の群
DP 群	防衛的悲観主義群 (Defensive Pessimism)	物事を悪いように考えることで，将来を 明るくしようと努力する人の群
RO 群	楽観主義群 (Regular/Realistic Optimism)	物事すべてを良いように考える人や， 将来の成り行きについて明るい見通しを 持つ人の群

11.2.3　質問紙調査

質問紙は，セキュリティ疲労度測定尺度 SFS-13，外山の認知的方略測定尺度，および，自由回答を求めた設問「あなたは，どのような時に情報セキュリティ対策に対して疲れを感じますか．」により構成した．この質問紙を用いたインターネットアンケート調査を，2019 年 12 月 23 日から同年 12 月 25 日にかけて，調査会社に依頼し実施した．全回答者 1036 名のうち社会人による 521 名の回答を分析対象とした．

11.2.4　分析

得られた回答を外山の分析 [外山 2015] と同様に, 各下位尺度の標準得点に基づきウォード法によるクラスター分析を実施した．その結果，外山の分析同様の 4 パターンが得られた．各パターンの特徴は表 11.6 に示す通りである．

表 11.6　本調査結果による認知的方略の 4 分類パターンの得点傾向

群名	外山の分類	本調査で得られた標準得点の傾向
LM 群	メタ認知低群 (Low Metacognition)	計画や成功の熟考得点ならびに過去のパフォーマンス認知が低く，失敗に対する予期・熟考パターンの得点は, 平均点あたりである.
RP 群	悲観主義群 (Regular/Realistic Pessimism)	失敗に対する予期・熟考パターンが非常に高く, 成功に対する熟考得点ならびに過去のパフォーマンス認知が低い.
DP 群	防衛的悲観主義群 (Defensive Pessimism)	熟考に対する得点が標準得点よりも高い.
RO 群	楽観主義群 (Regular/Realistic Optimism)	失敗に対する予期・熟考パターンが低く, その他の得点は高い.

11.2.5　認知的方略で分割した各群の考察

以下の考察は，共著研究の成果 [小川 2020] であって，認知的知的方略によって得られた 4 群それぞれに対してセキュリティコンディションマトリクスによるリスクアセスメントを実施した結果である．

11.2.5.1　LM 群（メタ認知低群）

LM（メタ認知低）群は，自分が周りからどう見られているのかを把握できておらず, 結果を上手く出せない人の群である．この群の特徴は，セキュリティ疲労度が理想状態である割合が約 5% と低く，セキュリティ対策実施度が低い割合が約 81% と高かった．主

な対策は，情報セキュリティ対策ソリューションの提供や当事者意識を喚起するための教育が挙げられる．

11.2.5.2　RP 群（悲観主義群）

RP（悲観主義）群は，物事すべてを悪いように考える人や，将来の成り行きについて暗い見通しを持つ人の群である．ここの群の特徴は，セキュリティ疲労度が理想状態の割合は約 21% であった．一方，セキュリティ疲労度が高い割合は約 19% と比較的低かった．主な対策は，情報セキュリティ教育の簡易化や情報セキュリティインシデントの模擬演習などが挙げられる．

11.2.5.3　DP 群（防衛的悲観主義群）

DP（防衛的悲観主義）群は，過去のパフォーマンスに対してポジティブな認知をもつが，将来に対する低い期待を設定する人の群である．この群の特徴は，セキュリティ疲労度が理想状態である割合は約 19%，セキュリティ疲労度かつ対策実施度が低い割合は約 47% であった．主な対策は，組織的な教育体制の整備や情報セキュリティインシデントの模擬演習が挙げられる．

11.2.5.4　RO 群（楽観主義群）

RO（楽観主義）群は，物事すべてを良いように考える人や，将来の成り行きについて明るい見通しを持つ人の群である．この群の特徴は，セキュリティ疲労度が理想状態である割合は約 32% と比較的高く，セキュリティ実施対策度が高い割合も約 61% と高い．主な対策は，当事者意識を向上させる教育や情報セキュリティ対策ソリューションの提供が挙げられる．

11.2.6　まとめ

本研究では，人間の行動パターンの分類方法のひとつである認知的方略の測定尺度によって得られた 4 群ごとにセキュリティコンディションマトリクスを求め，セキュリティ疲労に対するアセスメントを実施した．セキュリティコンディションマトリクスが 6 群であったことから，合計 24 群の行動パターンに対するアセスメントを実施したこととなる．このように，セキュリティコンディションマトリクスによるリスクアセスメントは，他の測定尺度などを用いて調査対象者をさらに細分化したうえでの考察のような拡張が可能である．

11.3　内部不正に対するセキュリティ疲労度測定尺度の貢献

11.3.1　概要

本研究は，内部不正（internal fraud）によるセキュリティインシデントに対して，セキュリティ疲労度測定尺度やセキュリティコンディションマトリクスがその抑止にどれだけ貢献するか明らかにしたものである [畑島 2018d]．ここまでに述べたセキュリティ疲労度測定尺度によってセキュリティ疲労度を段階ごとにモデル化した研究（**10.3.5**）や，セキュリティコンディションマトリクスにより細分化しリスクアセスメントを行う研究（**11.1.3** および **11.2.5**）は具体的なセキュリティインシデントに即した評価が十分ではなかった．そこで本研究では重要なセキュリティ課題である内部不正を対象としてセキュリティ疲労度モデルの有効性を評価した．

11.3.2　内部不正のリスク要因と対策

2010 年に発生したサイバー犯罪の発生原因に関する米国 CERT(Computer Emergency Readiness Team) の調査 [CERT2021] によると，外部からの攻撃は 58% であり内部人物による不正は 21 %と報告されている．また，被害額に関してどちらの方が大きいかを問う設問に対しては，外部からの攻撃であるとの回答が 38% であったのに対し，内部人物による不正であるとの回答は 33% であった．このように，攻撃の頻度に差があるにもかかわらず被害金額の多寡には大きな差がないため，内部不正の影響が無視できないことが示されている．

内部者による不正発生理由のひとつとして，厳密なルールによるセキュリティポリシーの形骸化を挙げる．企業は情報漏洩というセキュリティインシデントを防ぐためセキュリティ対策を実施し，その対策は次第に厳しいルールを策定する傾向がある．従業員はセキュリティを守るために必要なルールだと認識するため生産性が多少低下するとしても従う．しかし時間の経過によって組織は次第に図 9.1 のような悪循環に陥ることは，セキュリティ疲労度に関して述べる第 Ⅳ 部の冒頭である **9** において示した通りである．

11.3.3　セキュリティコンディションマトリクスによる内部不正が発生しうる人的側面の可視化

本研究で議論する内部不正は Reason[Reason2014] によるヒューマン・エラーの分類で呼ぶ violation（違反）が故意に実行されている状態である．以下に，セキュリティコンディションマトリクスにおける内部不正実施者（internal offender）の位置づけを図 11.3 を用いて述べる．縦軸である情報セキュリティ疲労度の測定では，内部犯行を行うために情報セキュリティに対する意識が高くなっていたり，情報セキュリティシステムが邪魔であると回答することから，情報セキュリティ疲労度尺度で測定すると高い疲労度として現れる．横軸である情報セキュリティ対策実施度の測定では，犯行者は犯行を隠すために，対策は実施していると答えると考えられる．つまり，内部不正実施者による intentional violation（意図的な違反）は，疲労度が高く，かつ対策実施度が高い状態で発生すると考えられる．このように，セキュリティコンディションマトリクスによって内部不正が発生しうる状態の人的側面が可視化される．

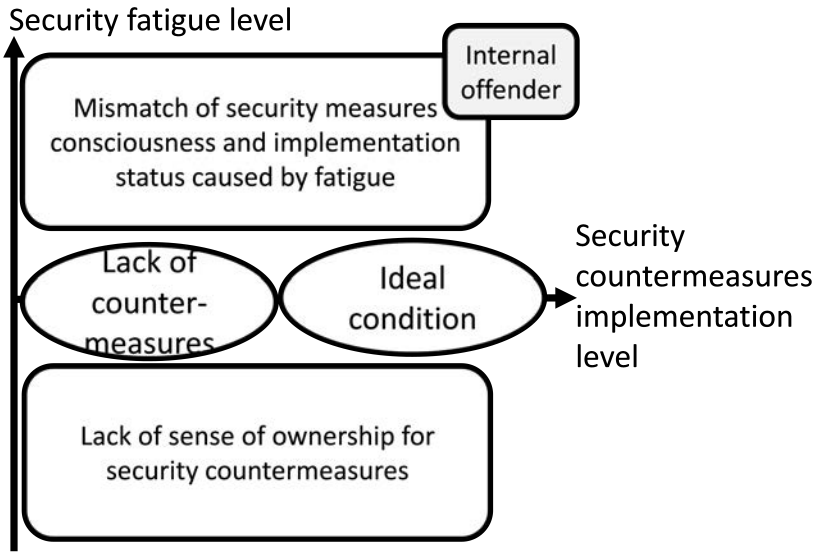

図 11.3　セキュリティコンディションマトリクスにおける内部不正実施者（Internal offender）の位置づけ [畑島 2018d]

11.3.4　内部不正におけるリスク項目と対策案

11.3.4.1　リスク項目の抽出

内部不正に関するリスク要因の抽出とリスク対策の策定をセキュリティの研究者とプロジェクトマネジメントの研究者によるディスカッションによって実施した．加えて，リスク対策案に対してセキュリティ疲れ状態のモデルがどの程度寄与しうるかの評価を行った．内部不正は犯罪と親和性が高いことから犯罪心理学の知見を援用した．犯罪心理学では集団や犯罪行為に影響を与える犯罪者の行動と心的プロセスを分析している．Cohen と Felson による Routine Activity Theory[Cohen1979] では犯罪の三角形が提唱されており，likely offenders（動機付けられた犯行者）, suitable targets（適当な標的）, および the absence of capable guardians（能力のある監視者の不在）の 3 要因が同時に出現した時に犯行が実行されると説明されている．そこで，犯罪の三角形の三要因を用いて内部不正のリスク要因をマインドマップ法によって導出し，さらに，Risk Breakdown Structure[Hillson2002] を用いてリスクを網羅的かつ体系的に抽出した．その結果，表 11.7 に示す 33 個のリスク項目を抽出した．

表 11.7　内部不正に対する 33 件のリスク項目とリスク対応戦略 [畑島 2018d]

No.	Tier 1	Tier 2	Tier 3	Tier 4/factor of risk	Impact	Frequency of occurrence	Countermeasure
1	1 likely offenders	1.1 motivation, pressure	1.1.1 external factor	1.1.1.1 職務における外部評価の低さ	LOW	LOW	Acceptance
2				1.1.1.2 不正により手に入れた情報を行使する対象の存在	LOW	LOW	Acceptance
3				1.1.1.3 ストレスを発生させるIT環境	LOW	LOW	Acceptance
4				1.1.1.4 厳しいノルマへの抵抗感	LOW	HIGH	Mitigration
5			1.1.2 internal factor	1.1.2.1 職務に対する冷笑感	LOW	HIGH	Mitigration
6				1.1.2.2 判断や行動の誤り(sudden impulse)	LOW	HIGH	Mitigration
7				1.1.2.3 精神的疲労による失敗	LOW	HIGH	Mitigration
8				1.1.2.4 肉体的疲労による失敗	LOW	HIGH	Mitigration
9		1.2 attitude, justification	1.2.1 external factor	1.2.1.1 不正が容認されている組織構造	HIGH	LOW	Transference
10			1.2.2 internal factor	1.2.2.1 一時的な行為に対する正当化	LOW	LOW	Acceptance
11				1.2.2.2 IT利用に対する自信	HIGH	LOW	Transference
12				1.2.2.3 犯罪ではないという思い込み	LOW	HIGH	Mitigration
13		1.3 Recognition of opportunities	1.3.1 external factor	1.3.1.1 不正が可能と認識するIT環境の存在	HIGH	HIGH	Avoidance
14				1.3.1.2 対価を得たいと思う損失の発生(金銭的・心理的)	HIGH	LOW	Transference
15			1.3.2 internal factor	1.3.2.1 心理的な情報セキュリティ上の死角の確信	LOW	HIGH	Mitigration
16	2 suitable targets	2.1 external factor	2.1.1 personal information	2.1.1.1 人事	HIGH	HIGH	Avoidance
17				2.1.1.2 顧客	HIGH	LOW	Transference
18			2.1.2 product information	2.1.2.1 機密	LOW	HIGH	Mitigration
19				2.1.2.2 ノウハウ	LOW	HIGH	Mitigration
20				2.1.2.3 製品	LOW	LOW	Acceptance
21				2.1.2.4 インサイダー	LOW	LOW	Acceptance
22			2.1.3 money	2.1.3.1 賄賂（リベート）	HIGH	LOW	Transference
23				2.1.3.2 出張費用	HIGH	LOW	Transference
24				2.1.3.3 その他金銭	HIGH	LOW	Transference
25			2.1.4 IT system information	2.1.4.1 ID	LOW	HIGH	Mitigration
26				2.1.4.2 パスワード	LOW	HIGH	Mitigration
27				2.1.4.3 ソフトウェア	LOW	HIGH	Mitigration
28				2.1.4.4 ハードウェア	LOW	LOW	Acceptance
29	3 absence of capable guardians	3.1 external factor	3.1.1 time	3.1.1.1 勤務時間外	LOW	HIGH	Mitigration
30				3.1.1.2 残業中	LOW	HIGH	Mitigration
31				3.1.1.3 休日	LOW	HIGH	Mitigration
32			3.1.2 place	3.1.2.1 セキュアでない職場環境の存在	HIGH	LOW	Transference
33			3.1.3 occasion	3.1.3.1 物理的な情報セキュリティ上の死角の確信	LOW	HIGH	Mitigration

11.3.4.2　リスク要因に対する対策方針検討

表 11.7 に示すように，抽出した 33 個のリスク項目に対してリスクを区分し対応戦略を検討した．具体的には，内部不正のリスク要因に対してプロジェクトマネジメントにおいて用いられているリスク区分・リスク対応戦略 (Risk Avoidance（回避）, Risk Mitigation（低減）, Risk Acceptance（受容）, Risk Transference（転嫁）)[PMBOK2017] に分類するため，Risk Probability（リスクの確率）と Risk Impact（リスクの影響）の高低により 4 種類に分類した (図 11.4).

11.3.4.3　リスク対策方針に対する SFS-13 の貢献度の机上評価

セキュリティ疲労モデルが内部不正の抑止にどの程度貢献するかを机上評価する．SFS-13 は人的側面の測定尺度であるため，内部不正のリスク要因の抽出結果における大分類（表 11.7 の Tier1）のうち，内部不正の人的側面である likely offenders に関するの 15 項目を検討対象とした．具体的には，SFS-13 を構成する 13 項目の設問文と likely offenders に関する 15 項目のリスク要因を用いて，どの設問文が個々のリスク要因を説明

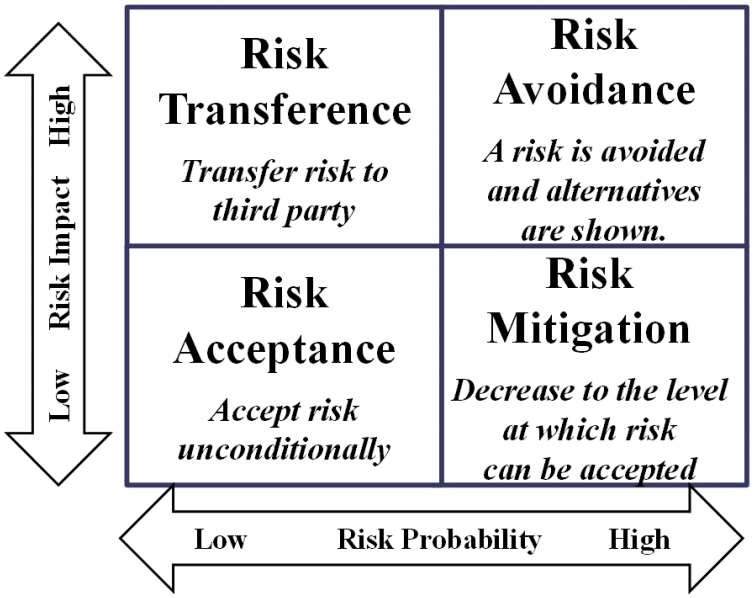

図 11.4　リスク区分・リスク対応戦略 [畑島 2018d]

できているかを照合する机上評価を実施した．評価結果を表 11.8 に示すように，リスク要因 15 項目のうち 8 項目を SFS-13 の設問で言及されていた．換言すると，SFS-13 による質問紙調査において当該の 8 項目の設問への回答結果によって，内部不正に関わるリスク要因のうち約 53%（= 8/15）を観測しうることを示した．

11.3.5　まとめ

セキュリティ疲労度測定尺度とセキュリティコンディションマトリクスの有効性について検討した．まず，内部不正に関わるセキュリティインシデントに着目し，攻撃者がセキュリティコンディションマトリクスのどの状態に位置するのかを考察した．そして，Routine Activity Theory と Risk Breakdown Structure により，内部不正が実行される 33 項目のリスク要因とリスク対策方針を示した．さらに，33 項目のうち likely offenders を対象とする 15 項目の対策について，セキュリティ疲労度測定尺度が 8 項目である約 53%（=8/15）を観測しうることを示した．

11.4　セキュリティ疲労度測定尺度の応用研究のまとめ

本章では前章の研究で開発したセキュリティ疲労度測定尺度を用いた応用研究について以下のように述べた．

表 11.8　likely offenders に対する内部不正要因とセキュリティ疲労との関係 [畑島 2018d]

No.	Tier 1	Tier 2	Tier 3	Tier 4/factor of risk	Observable with security condition matrix
1	1 likely offenders	1.1 motivation, pressure	1.1.1 external factor	1.1.1.1 職務における外部評価の低さ	
2				1.1.1.2 不正により手に入れた情報を行使する対象の存在	
3				1.1.1.3 ストレスを発生させるIT環境	○
4				1.1.1.4 厳しいノルマへの抵抗感	○
5			1.1.2 internal factor	1.1.2.1 職務に対する冷笑感	○
6				1.1.2.2 判断や行動の誤り(sudden impulse)	
7				1.1.2.3 精神的疲労による失敗	○
8				1.1.2.4 肉体的疲労による失敗	
9		1.2 attitude, justification	1.2.1 external factor	1.2.1.1 不正が容認されている組織構造	○
10			1.2.2 internal factor	1.2.2.1 一時的な行為に対する正当化	
11				1.2.2.2 IT利用に対する自信	○
12				1.2.2.3 犯罪ではないという思い込み	
13		1.3 Recognition of opportunities	1.3.1 external factor	1.3.1.1 不正が可能と認識するIT環境の存在	○
14				1.3.1.2 対価を得たいと思う損失の発生(金銭的・心理的)	
15			1.3.2 internal factor	1.3.2.1 心理的な情報セキュリティ上の死角の確信	○

- セキュリティコンディションマトリクスとその応用
  1. セキュリティ疲労度測定尺度による測定結果とセキュリティ対策の実施度をマトリクス化したセキュリティ状態の可視化．および，理想状態の維持もしくは理想状態への行動変容を促す施策に対するリスクアセスメントと机上検討．(**11.1**)
  2. 認知的方略測定尺度を用いて更にセキュリティコンディションマトリクス上の状態を細分化しての同様のリスクアセスメント（**11.2**）
- セキュリティ疲労度測定尺度の性質に関する考察の一例として，情報セキュリティに対する内部犯行者の性質の測定
  1. 情報セキュリティインシデントのうち内部犯行の実行者の性質の，セキュリティ疲労度測定尺度による観測可能性の検討（**11.3**）

このように，セキュリティ疲労度測定尺度そのものや，その他の測定尺度との組み合わせによるセキュリティコンディションマトリクスによって，インターネット利用者のセキュリティ対策に対する疲労度や，内部犯行を起こしやすい状態の観測が可能であることを示した．

第 12 章

第 IV 部のまとめ

第 IV 部では，セキュリティ疲れの測定尺度（SFS-13，SFS-9）開発と，測定尺度の応用について述べた．本研究によって，インターネット利用者のセキュリティ対策実施行動による疲労の測定が可能となった．

インターネット利用者がセキュリティ対策に疲労してしまうことによって，セキュリティリスクは高まり，同時にセキュリティ対策の効果も低下することが懸念される．本研究によってセキュリティ疲労度やセキュリティ対策に対する本人の状態が可視化される．これを活用することによって，セキュリティ疲労に対する状態が理想状態であれば維持させ，理想状態以外であればよりよい状態へと移行させるための施策を実施させることが可能となる．

第 IV 部の参考文献

[青木 2017] 青木繁伸：相関係数行列の吟味，入手先〈http://aoki2.si.gunma-u.ac.jp/lecture/PFA/pfa6.html〉 (参照 2017-10-06).

[板倉 2009] 板倉宏昭：バーンアウトとプロジェクトマネジメント (〈特集〉人とチームのマネジメント), プロジェクトマネジメント学会誌, vol.11, no. 1, pp.17–19 (2009).

[植野 2010] 植野真臣，荘島宏二郎：学習評価の新潮流，朝倉書店 (2010).

[小川 2020] Ogawa, M., Tanimoto, S., Hatashima, T., Kanai,A.: Information Security Fatigue Countermeasures Using Cognitive Strategy Scale Based on Web Questionnaires, 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW), pp.362–367, DOI:10.1109/CANDARW51189.2020.00075 (2020).

[北岡] 北岡 (東口) 和代, 増田真也, 荻野佳代子, 中川秀昭, : MBI-HSS, MBI-GS の日本版に関して, 入手先〈http://kokoro.w3.kanazawa-u.ac.jp/pdf/mbi.pdf〉 (参照 2016-05-09).

[北岡 2011] 北岡 (東口) 和代, 荻野佳代子, 増田真也, 中川秀昭：バーンアウト測定尺度 Maslach Burnout Inventory-General Survey(MBI-GS) の概要と日本版について, 北陸公衆衛生学会誌, vol.37, no. 2, pp.34–40 (2011).

[北村 2001] 北村英哉：社会心理学キーワード，有斐閣 (2001).

[久保 1999] 久保真人：ヒューマン・サービス従事者におけるバーンアウトとソーシャル・サポートとの関係, 大阪教育大学紀要. IV, 教育科学, vol.48, no. 1, pp.139–147 (1999).

[久保 2004] 久保真人：バーンアウトの心理学. サイエンス社 (2004).

[小山 2007] 小山由紀恵，木村哲夫，“Neural Test Theory を使った Can-do Statements の分析, (2007).

[清水 2014] 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).

[菅原 2006] 菅原健介：心理尺度の作成方法，心理測定尺度集 3，松井豊 (編)，pp.397–408, サイエンス社 (2006).

[総務省 2017] 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/maincontent/000238665.pdf〉（参照 2017-02-16）.

[総務省 2018] 国民のための情報セキュリティサイト：安全なパスワード管理,”総務省, 入手先〈http://www.soumu.go.jp/mainsosiki/johotsusin/security/business/staff/01.html〉(参照 2018-03-29).

[荘島 2008] Shojima, K.: Neural test theory: A latent rank theory for analyzing test data, DNC Res. Note, vol.8–1 (2008).

[荘島 2009] 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).

[荘島 2017] 荘島宏二郎, exametrika, 入手先〈http://antlers.rd.dnc.ac.jp/˜shojima/exmk/index.htm〉(参照 2017-04-27).

[谷本 2017] 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).

[東京電機大学 2018] 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，東京電機大学，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).

[外山 2015] 外山美樹：認知的方略尺度の作成および信頼性・妥当性の検討，教育心理学研究，Vol.63，No.1，pp.1–12 (2015).

[豊田 2016] 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).

[西村 2012] 西村浩二，大東俊博，岩沢和男，隅谷孝洋，稲垣知宏，中村純，宮内祐輔，三戸里美，相原玲二：広島大学における情報セキュリティ・コンプライアンス教育の取組み，情処学インターネットと運用技術研報，vol.2012–IOT-1, no.2,pp.1–6 (2012).

[南風原 2002] 南風原朝和：心理統計学の基礎，有斐閣 (2002).

[畑 2015] K. Hata, S. Yoneda, S. Tanimoto, H. Sato, and A. Kanai: A Proposal of Slow Policy Level based on Cost-effectiveness of ISMS’s Countermeasure, in Proceedings of the 9th International Conference on Project Management (ProMAC2015), pp. B19-124-B19-129 (2015).

[畑島 2017d] 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）.

[畑島 2017b] 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).

[畑島 2017e] 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).

[畑島 2018a] 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).

[畑島 2018b] 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).

[畑島 2018c] 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).

[畑島 2018d] : Hatashima, T., Nagai, K., Kishi, A., Uekusa, H., Tanimoto, S., Kanai, A., Fuji, H., 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), pp. 707–712, DOI: 10.1109/COMPSAC.2018.10323 (2018).

[畑島 2020] 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 SFS-9 の開発と信頼性・妥当性の検討，情報処理学会論文誌，Vol.61, No.9, pp.1472–1485 (2020).

[浜津 2015] 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).

[広島大学 2018] 広島大学：情報セキュリティ対策，広島大学，入手先〈https://www.hiroshima-u.ac.jp/about/initiatives/jyohoka/ism〉(参照 2018-02-14).

[法政大 2018] 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/securityHandbook2018-1.pdf〉（参照 2018-07-02）.

[増田 2011] 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).

[三浦 2015] 三浦麻子，小林哲郎：オンライン調査モニタの Satisfice に関する実験的研究，

社会心理学研究，vol.31, no.1,pp.1–12, (2015).

[水本 2008] 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).

[村上 2013] 村上宣寛：心理尺度のつくり方，北大路書房 (2013).

[村山 2018] 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).

[文部科学省 2017] 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).

[吉田 2007] 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).

[CERT2021] CERT: 2011 Cybersecurity Watch Survey Presentation (2011) available from〈https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=54027〉(accessed 2018-04-03).

[Cisco2019] Cisco: Cisco 2019 Asia Pacific CISO Benchmark Study, available from〈https://www.cisco.com/c/m/ensg/products/security/offers/benchmark-reports-2019.html〉(accessed 2020-03-19).

[Chandran2015] 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).

[Cohen1979] L. E. Cohen and M. Felson: Social Change and Crime Rate Trends: A Routine Activity Approach, Am. Sociol. Rev., vol. 44, no. 4, pp. 588–608 (1979).

[CSIRT2018] 日本シーサート協議会：一般会員 (チーム) 情報，日本シーサート協議会，入手先〈http://www.nca.gr.jp/member/index.html〉(参照 2018-02-14).

[Egelman2015] Egelman, S. and Peer, E.: Scaling the Security Wall?:Developing a Security Behavior Intentions Scale (SeBIS), Proc. 33rd Annual ACM Conference on Human Factorsin Computing Systems(CHI’15), pp.2873–2882 (2015).

[Egelman2016] 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).

[Faklaris2019] 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(SOUPS2019) (2019).

[Furnell2009] Furnell, S. and Thomson, K.-L.: Recognizing and addressing‘security fatigue,

Comput. Fraud Secur., vol.2009, no. 11, pp.7–11 (2009).

[Grassi2017] P. A. Grassi, J.L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K.K. Greene, and M.F. Theofanos, Digital identity guidelines: authentication and lifecycle management, Gaithersburg, MD, June 2017 (2017).

[Hillson2002] D. Hillson: Use a risk breakdown structure (RBS) to understand your risks, in Proceedings of the project management institute annual seminars & symposium, 2002, vol. 10 (2002).

[IPA2016] 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）.

[Kearney2016] Kearney, W.D. and Kruger, H.A.: Theorizing on risk homeostasis in the context of information security behaviour, Inf. Comput. Secur., Vol.24, No.5, pp.496–513(2016).

[Maslach] Maslach Burnout Inventory: available from 〈http://www.mindgarden.com/117-maslach-burnout-inventory〉 (accessed 2017-05-09).

[Maslach1998] Maslach, C., Jackson, S. E. and Leiter, M. P.: The Maslach Burnout Inventory Manual. (1998).

[McGraw2014] McGraw, G.: Security Fatigue? Shift Your Paradigm, Computer., Vol.47, No.3, pp.81–83 (2014).

[McLaughlin2006] McLaughlin, L.: What Microsoft’s identity metasystem means to developers,IEEE Softw., Vol.23, No.1, pp.108–111 (2006).

[NII2018] 高等教育機関における情報セキュリティポリシー推進部会,“高等教育機関における情報セキュリティポリシーの策定について,”国立情報学研究所, http://www.nii.ac.jp/service/sp/,（参照 2018-02-14）.

[Norem1989] Norem, J.K.,: Cognitive strategies as personality: Effectiveness, specificity, flexibility, and change., D.M.Buss&N.Cantor(Eds.), Personalitypsy-chology; Recent trends and emerging directions, pp.45–60, NewYork:Springer-Verlag (1989).

[Parkin2016] Parkin, S., Krol, K., Becker, I. and Sasse, M. A.: Applying Cognitive Control Modes to Identify Security Fatigue Hotspots, Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) (2016).

[Parsons2014] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C.: Determining employee awareness using the Human Aspects of Information Security Ques-tionnaire (HAIS-Q),Comput. Secur., Vol.42, pp.165–176(2014).

[Pham2019] 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).

[PMBOK2017] P. M. Institute: PMBOK Guide and Standards (2017). available from 〈https://www.pmi.org/pmbok-guide-standards〉 (accessed 2018-04-03).

[Reason2014] Reason, J.: Human error, Cambridge University Press(1990). 十亀 洋（訳）：ヒューマンエラー［完訳版］，海文堂出版 (2014).

[Sharif2018] 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).

[Stanton2016] Stanton, B., Theofanos, M. F, Prettyman, S. S. and Furman, S.:Security Fatigue, IT Prof., vol.18, no. 5, pp.26–32, 2016.

IV-1　第 10 章の質問紙（SFS-13 開発）

「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
(選択肢は，1：ない，2：まれにある，3：時々ある，4：しばしばある，5：いつもあるの 5 件法).

1. ソフトウェアの最新化やパスワードの定期的な更新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
2. 情報セキュリティ対策は意味が無いと思うことがある
3. 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
4. PC やスマートフォンを使っているとワクワクする
5. 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
6. 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
7. 情報セキュリティ対策は必要悪だと思うことがある
8. 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
9. 情報セキュリティ対策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
10. NS で人と交流するのが楽しいと思うことがある
11. 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
12. 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
13. PC やスマートフォンをなくしたり壊したりしないかとヒヤヒヤすることがある
14. 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

15. 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
16. 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
17. 指示される情報セキュリティ対策に一貫性がないと思うことがある
18. 私はセキュリティ対策に自信があると思うことがある
19. 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
20. 本来やることを忘れるほど情報セキュリティ対策に熱中することがある
21. 手で入力するときパスワードを間違えることがある
22. 私の性分は情報セキュリティ対策に向いていると思うことがある
23. 情報セキュリティ対策がつまらなく思えてしかたのないことがある
24. 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
25. 情報セキュリティ対策のために心にゆとりがなくなったと感じることがある
26. 情報セキュリティ対策は，私にとってあまり意味がないと思うことがある
27. 情報セキュリティ対策が楽しくて，知らないうちに時間が過ぎることがある
28. 情報セキュリティ対策のために体も気持ちも疲れはてたと思うことがある

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．

IV-2　第 10 章の質問紙（SFS-9 開発）

「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 (選択肢は，1：ない，2：まれにある，3：時々ある，4：しばしばある，5：いつもあるの 5 件法)

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. 情報セキュリティ対策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（選択肢は 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：とてもそう思うの 5 件法）

1. 私は，情報セキュリティ対策をきちんと出来ている
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

設問 4：あなた自身ことを教えてください

情報端末の利用歴（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（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（会社や大学）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

IV-3　大学生版セキュリティ疲労度測定尺度 SFS-13

- 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
  (選択肢は，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）

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. 情報セキュリティ対策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

IV-4　セキュリティ疲労度測定尺度 SFS-9

- 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
  (選択肢は，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）

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. 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
4. 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
5. 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
6. 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
7. 私はセキュリティ対策に自信があると思うことがある
8. 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
9. 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

IV-5　第 11 章の質問紙（セキュリティコンディションマトリクス開発）

「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
(選択肢は，1：ない，2：まれにある，3：時々ある，4：しばしばある，5：いつもあるの 5 件法).

1. ソフトウェアの最新化やパスワードの定期的な更新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
2. 情報セキュリティ対策は意味が無いと思うことがある
3. 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
4. PC やスマートフォンを使っているとワクワクする
5. 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
6. 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
7. 情報セキュリティ対策は必要悪だと思うことがある
8. 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
9. 情報セキュリティ対策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
10. NS で人と交流するのが楽しいと思うことがある
11. 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
12. 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
13. PC やスマートフォンをなくしたり壊したりしないかとヒヤヒヤすることがある

14. 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
15. 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
16. 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
17. 指示される情報セキュリティ対策に一貫性がないと思うことがある
18. 私はセキュリティ対策に自信があると思うことがある
19. 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
20. 本来やることを忘れるほど情報セキュリティ対策に熱中することがある
21. 手で入力するときパスワードを間違えることがある
22. 私の性分は情報セキュリティ対策に向いていると思うことがある
23. 情報セキュリティ対策がつまらなく思えてしかたのないことがある
24. 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
25. 情報セキュリティ対策のために心にゆとりがなくなったと感じることがある
26. 情報セキュリティ対策は，私にとってあまり意味がないと思うことがある
27. 情報セキュリティ対策が楽しくて，知らないうちに時間が過ぎることがある
28. 情報セキュリティ対策のために体も気持ちも疲れはてたと思うことがある

設問 2：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に○をつけてください.
(選択肢は，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の 5 件法).

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，時々変更する，パスワード管理ソフトを使うなど）
4. 信頼出来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を開かない
7. 最新の情報セキュリティ情報をチェックする
8. 端末や記憶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

設問 3：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．

IV-6　外山の認知的方略測定尺度 [外山 2015]

1. 失敗に対する予期・熟考
    - その状況で私は失敗するだろうと考える
    - その状況で失敗している自分の姿が何度も心に浮かぶ
    - その状況で私が良い結果を残すのは難しいだろうと考える
    - その状況で何か良くないことが起こるだろうと考える
    - その状況で私は失敗したらどうしようかとくよくよ考える
2. 過去のパフォーマンスの認知
    - 過去の同じような状況では，たいてい優れた結果をおさめてきた
    - これまでは，このような状況では良い結果だったことが多い
    - 過去の同じような状況では，だいたい私はちゃんとうまくやってきた
    - 過去の同じような状況では，あまり良い結果が残せなかった (逆転項目)
    - 過去の同じような状況では，失敗したことがほとんどない
3. 性向に対する熟考
    - その状況で成功している自分の姿が何度も心に浮かぶ
    - その状況で自分が成功している様子をよく想像する
    - その状況で自分がうまくやってのけている様子を何度も思い浮かべる
    - もしもその状況で成功したらどんなに嬉しいだろうかと，よく想像する
    - その状況で私は成功するだろうと考える
4. 計画に対する熟考
    - その状況にのぞむ前に，十分時間をかけて対応策を練る
    - その状況で失敗しないためにはどうしたら良いのかを，時間をかけて考える
    - その状況にのぞむ前に，これから何をどうすれば良いのかの計画をじっくり考える
    - その状況にのぞむ前に，プランニングに時間をかける
    - その状況でうまくやるためにはどうしたら良いのかを，時間をかけて考える

第Ⅴ部

結論

第 13 章

結論

本研究はインターネット利用者の利用行動を測定する手法の開発とその応用についての検討結果である．

第 Ⅱ 部では，関心度（TBI:Time-Based Interest）の研究について述べた．関心度研究はインターネット利用者の情報収集行動を定量化し Web ページの人気を反映した指標の開発を意図した．インターネット利用者が検索サイトに掲載されたリンクを選択しリンク先の情報を参照する行動の定式化を，アクセス発生によって TBI を増加させる関数とアクセスが発生しないままでいる経過時間によって TBI を減衰させる関数からなる方程式により行った．TBI が指数関数的に減衰することの演繹的定義，およびを特定のイベントについての Web サイト検索サービス NTT DIRECTORY のアクセスログを用いて TBI の減衰比に係わる定数 α を導出した．

関心度（TBI）の性質として，TBI の得点順位を横軸，TBI の算出値を縦軸とした 2 次元グラフを作成すると，TBI は Zipf 分布に従い，これは単純なアクセス数を元にした指数 PageView と同様の性質であることがわかった．また，関心度（TBI）は検索サイトの検索結果表示順として利用することでインターネットを利用する人々の関心を集めるサイトへのアクセスが容易となった．NTT DIRECTORY での実装実験では 65 %の人が検索結果表示順として TBI 順が選択された．

第 Ⅲ 部ではインターネット利用者がセキュリティ対策を求められていても，善意および悪意や行動の軽重にかかわらず安全に関わる規則違反であると認識した行動であるセキュリティ不安全行動を起こしてしまうことに関する 2 件の研究について述べた．

前者の研究ではリサーチクエスチョンとして，「情報漏洩行動を悪意を意図せずとも実施してしまった従業員本人の性向に特徴があるか」を設定した．そのなかでも，内部不正の意図はない行動に着目し，セキュリティインシデントを抑止する方策の検討に資するこ

とを意図して研究した．換言すると，「ついつい」や「良かれと思って」セキュリティ規則に違反する行動をしてしまう人の行動を観測し，セキュリティインシデントを抑止する方策の検討に資することを意図して研究した．その結果，従業員本人の性向のうちリスクテイキング行動を抑止すること，特に，確信的に敢行してしまう性向を抑止することが有効であることを示した．また，テレワークという普段の職場から離れる勤務形態に対するセキュリティ対策としても職場の情報セキュリティ環境から危険な状況を除外することが有効であることを示した．

後者の研究では，私有端末を使ったモバイルワーク・テレワーク（BYOD）におけるセキュリティ不安全行動について，企業からの許可のある状態での正しい BYOD として行われているか，もしくは，企業からの許可がないが私有端末を業務利用しているシャドー IT（Shadow IT）として行われているかに着目して検討した．その結果，規約の整備状況および許可状況と BYOD ユーザの業務実施状況の分析によるセキュリティ不安全行動がリスク補償行動によって説明可能であることを示した．換言すると，会社の規約を守る人はその規約に従うがゆえにルールや規則を遵守しているため，個人に関する情報のような機密性の高い業務データを取扱う際にもリスクレベルが低いと考え，セキュリティインシデントのリスクレベルが増加するようなリスク補償行動をしてしまっていると考えられる．

第 Ⅳ 部では，インターネット利用者が求められる情報セキュリティ対策に対して疲弊するために，対策施策の効果が上がらなくなることを「セキュリティ疲れ」と呼び，セキュリティ疲れ状態を可視化することにより，セキュリティ疲れ状態を回避し理想的な状態を維持させる方法を導くための研究を行った．

具体的には，セキュリティ対策に疲弊したインターネット利用者が「セキュリティ疲れ状態」となり，この状態が進行することで情報セキュリティ対策を実施しなくなる状態を「セキュリティバーンアウト状態」と仮定し，一般的な燃え尽き症候群 (バーンアウト) の測定手法の援用によりセキュリティ疲労度測定尺度を開発した．セキュリティ疲労度測定尺度については，まず，大学生を対象とした 13 項目からなる測定尺度 SFS-13 を開発し，次に，社会人を対象とし，同時に大学生に対しても質問紙調査を行うことで汎用化した，SFS-13 から簡易化され 9 項目から構成される SFS-9 の開発を行い，これらの性質について研究を行ったほか，SFS-13 を用いて実施した測定尺度の応用研究について述べた．その結果，開発した測定尺度は，尺度得点が低ければ低いほど理想的であるものではなく，セキュリティ対策に対する意識を適度に持っていると考えられる尺度得点が中程度である状態が理想的であることが判った．

測定尺度の応用研究では，まず，セキュリティ疲労度測定尺度による測定結果とセキュリティ対策実施度の測定結果を縦横の軸に取った「セキュリティコンディションマトリク

ス」を開発した．セキュリティ疲労度測定尺度によってセキュリティ疲れ状態が可視化され，セキュリティコンディションマトリクスによって，セキュリティ対策にするインターネット利用者の理想状態が「セキュリティ対策に対して適度な緊張感を持っており，かつ，セキュリティ対策を実施している」状態であることを示したしたほか，それ以外の状態にある時に理想状態に近づけるためのセキュリティ対策についてアセスメントを行った．次に，セキュリティコンディションマトリクスの各状態に対して更に認知的方略と呼ばれる人の行動規範により細分化し，細分化されたそれぞれの状態に対してリスクアセスメントを行った．最後に，セキュリティ疲労度測定尺度が内部不正の潜在的な犯行者の観測に用いうるかを検討した．

上記のように，インターネット利用者の行動を Web サーバのアクセスログ解析（関心度）や，質問紙調査（不安全行動，セキュリティ疲れ）によって観測する研究を行ったが，これらの研究には限界点も存在する．まず，関心度（TBI）研究においては，関心の減衰が顕著に表れるとみられる選挙というイベントを対象として検討したものであり，短期間に集中的にアクセスが発生するイベントに対する関心の集中と減衰の度合いを測定するものであるため，汎用性を検証することに研究の余地がある．次に，セキュリティ不安全行動研究においては，質問紙調査により行動分析を実施しているため，回答協力者の主観に依存していることは否めない．実際に行動を観測するユーザ実験による検証について研究の余地がある．最後に，セキュリティ疲労度についても，質問紙調査による測定であるため主観に依存することや，質問紙調査への回答を回収し集計したのち初めて疲労度が判明するため即時性に劣ることは否めない．実際のインターネット利用行動をセンシングし，セキュリティ疲労の特徴を抽出することでリアルタイムな観測が可能となるが，実行動を記録し分析することとなるため実運用の際にはセキュリティとプライバシーに対する検討が必須である．

本研究で行ったようにインターネット利用行動の測定が可能となれば，利用行動に応じたサービス開発やよりよい利用環境を提供するための技術開発が実現可能となる．本研究がインターネット利用者の利用行動に応じたサービス開発やよりよい利用環境を提供するための技術開発に利用されることを期待する．

謝辞

本研究をまとめるにあたり，ご指導ご鞭撻くださいました千葉工業大学社会システム科学部プロジェクトマネジメント学科谷本茂明教授に深く感謝いたします．谷本教授には教授が私の現職である日本電信電話株式会社研究所に在籍時代から暖かくご指導くださり，大学に移られてからもセキュリティ疲れの共同研究の形でご指導いただきました．心より感謝申し上げます．また，学位論文審査において貴重なご指導ご助言を賜りました，千葉工業大学 岩下基教授，滝聖子教授，矢吹太朗准教授，そして東京都市大学 関良明教授に心より感謝申し上げます．

まず，関心度（TBI）の研究は山本修一郎教授（現名古屋国際工科専門職大学情報工学科学科長），元田敏浩氏（現 NTT アドバンステクノロジ社）の御指導により，第 54 回情報処理学会全国大会優秀賞をいただいたものでした．心より感謝申し上げます．また，研究対象であった NTT DIRECTORY の運営に係わられていたすべての皆様に深く感謝申し上げます．

そして，セキュリティ不安全行動の研究では坂本泰久氏（現 NTT アドバンステクノロジ社）の御指導，度重ねての議論による成果であり，本文中に触れていない関連研究で第 15 回情報科学技術フォーラム （FIT2016）奨励賞をいただきました．心より感謝申し上げます．

さらに，セキュリティ疲れの研究では谷本教授とともに三者共同研究としてご指導くださいました法政大学理工学部応用情報工学科金井敦教授にも御指導御鞭撻を賜った成果であり，初期検討の成果に対して情報処理学会コンピュータセキュリティシンポジウム (CSS)2017 において同学会セキュリティ心理学とトラスト（SPT）研究会より CSS2017SPT 論文賞をいただいたほか，共著論文として本研究では **11.2** で述べた CANDAR2021 のワークショップ WICS(7th International Workshop on Information and Communication Security) において Best Paper や，本文中では触れませんでしたが共著者が DICOMO2019 ヤングリサーチャ賞をいただきました．また，千葉工業大学谷本研究室の皆様には予備調査回答のデータ入力や測定尺度の下位因子名称決定の議論など多大なる協力をいただきました．心より感謝申し上げます．セキュリティ疲れ測定尺度開発の予備調査として実施した質問紙調査を進めるにあたり，回答に快く協力してくれた千葉工業大学社会システム科学部並びに法政大学理工学部の学生に感謝いたします．

また，学会においての様々な皆様からのご助言が本研究の大きな助けとなっています．特に，セキュリティ疲れの研究では情報処理学会セキュリティ心理学とトラスト（SPT）

研究会の研究発表会や様々な学会活動において数多くの研究者の皆様から貴重な御助言をいただきました．心より感謝申し上げます．また，論文の査読や編集を御担当くださいました皆様にも深く感謝申し上げます．

なお，本研究は日本電信電話株式会社研究所に在職中の成果から構成されています．ご指導ご助言いただいたここに記しきれない皆様に心より感謝申し上げます．

最後に，家族に感謝いたします．