情報処理学会論文誌 Vol.58 No.12 1912–1925 (Dec. 2017)

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

畑島 隆[1,a)] 坂本 泰久[1]

受付日 2017年3月13日, 採録日 2017年9月5日

概要：働き方改革が提唱されるなど，テレワークが再度脚光を浴びている．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は困難である．本稿では，テレワークについて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．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365サンプルの従業員を「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，尺度得点の差を検定した．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．

キーワード：不安全行動，テレワーク，性向分析，質問紙設計，情報セキュリティ，情報漏洩

Analysis of the Tendency of Teleworkers toward Unsafe Acts on Information Security

Takashi Hatashima[1,a)] Yasuhisa Sakamoto[1]

Received: March 13, 2017, Accepted: September 5, 2017

Abstract: As a new workstyle, telework is in the limelight. The introduction of information security solutions and the establishment of regulations are advancing measures on the part of companies. On the other hands, human errors occur regardless of intention, it is difficult to maintain a state where security is ensured for the entire information system including facilities and people. In this paper, we defined teleworking as task using business data. As an information security unsafe act, we focused on behaviors that are not malicious, such as internal fraud, which there is an intention in the act itself and intention to violate the rules. Based on these definitions, in order to propose effective information security measures in teleworking, we made a research question as to "Whether there is a characteristic in the propensity of the employee oneself who performed information leakage behavior without intention of malice". Then, we did internet survey with questionnaire which measures "knowledge for security incident and about security", "tendency of employee oneself", "tendency to telework", "own information leakage behavior". The 365 employees obtained as a result of the data cleaning were divided into two groups according to whether or not the experience of "unintentional information leakage behavior", and was examined the difference in the scale score. As a result, among the propensity of employee, it was suggested that it is effective that suppressing the risk-taking behavior, in particular, the propensity of acting dared confidently. It was also suggested that it is effective to exclude dangerous situations from the information security environment of the workplace. In addition, while certain effects of information security measures can be expected, it is suggested that there are individual differences in the effect of countermeasures.

Keywords: unsafe act, telework, tendency analysis, questionnaire design, information security, information leakage

© 2017 Information Processing Society of Japan

1. はじめに

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 [1]．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 [2] 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 [3] として近年再度脚光を浴びている．現在，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 [4]．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．

テレワークに対しても情報セキュリティ対策は喫緊の課題 [5] である．テレワーク実施における情報セキュリティ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での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あげられる．

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 [6] 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 [7] 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」，「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 [8]．

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 [9] 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．

我々の研究では，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定義する．情報システムはヒューマンエラーを抑止するソリューションであるが，情報システムによる環境整備は多額のコストが発生するため，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おいて不安全行動をはじめとしたヒューマンエラーの抑止が必須の課題であるが，我々は特に不安全行動の抑止に注目している．

我々はテレワークにおける業務を業務に関するデータを用いた業務行動と定義する．そして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「情報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を研究動機としている．

これまでに我々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）[10] 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 [11] ことを示したほか，質問紙調査を実施した文献 [12] 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．さらに我々は，文献 [12] に示す調査および本稿との同時調査 [13] において，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

[1] 日本電信電話株式会社 NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories, Nippon Telegraph and Telephone Corporation, Musashino, Tokyo 180–8585, Japan
[a)] hatashima.takashi@lab.ntt.co.jp

© 2017 Information Processing Society of Japan

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．

本稿では，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 [9] 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を，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」をしてしまった回答者群と対照群との検定によって，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 [14] 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．

2 章では関連研究を述べる．3 章で前述のリサーチクエスチョンを検証する質問紙の設計について述べる．4 章ではインターネット質問紙調査実施結果の概要とリサーチクエスチョンに対する検定結果を述べる．5 章で検定結果の考察を示すとともに，本稿の優位性と限界を述べ，6 章でまとめる．

2. 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 [15] 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 [16] は情報セキュリティ対策における阻害要因について，施策を推進する責任者および担当者の意識と行動に着目し，大企業と中小企業の 2 母集団を比較により施策推進の阻害要因を示した．前述のほか情報セキュリティポリシに対する遵守意識を行動モデル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 [17]，Ifinedo [18] 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 [19] 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 [20] 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 [21] 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，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や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，当事者の普段の性向についての検討や，従業員全般の性向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 [22] 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 [23] 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稿とは対象が異なる．

以上のことから，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．

3. 質問紙設計

3.1 不安全行動の分類

1 章で示したように，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使われる言葉であ

© 2017 Information Processing Society of Japan

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 [24]．このように，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 [25]．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 [25]．

また，和田ら [26] 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 [8] 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」をあげている．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 [12] 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向に特徴がある」

このリサーチクエスチョンに対して，既存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．

3.2 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や，これらをふ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 モデルがあげられる．各モデルの解説は文献 [27] に詳しい．TRA と計画的行動理論は，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．

図 1 KAB モデル
Fig. 1 Knowledge-Attitude-Behavior model.

KAB モデルは，Knowledge 層，Attitude 層，そして Behavior 層から構成される（**図 1**）．Parsons ら [27] 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 [28] 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 [29] 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 [15] 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．

3.3 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 1**）の設定根拠を説明する．また，検討の結果得られた質問紙を付録 A.1 にあげる．

3.3.1 Knowledge 層

Knowledge 層は，ウィルス感染経験，IT 知識および IT

© 2017 Information Processing Society of Japan

表 1 測定尺度と KAB モデル階層の対応
Table 1 Measurement scale and KAB model.

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	テレワーク導入の効果への好感度	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報告	Behavior 層

スキルを設定した浜津ら [28] にならい，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 [30] 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 [5] 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（Q9）するとともに，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 [31] 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，文献 [31] 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．

3.3.2 Attitude 層

Attitude 層は，人間の行動を公私に分ける分類法により，「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 [32] にあげられた 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 [8] があ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あげ，手続が面倒であるかを尋ねた．

我々は 1 章に示した先行研究 [11] 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示した．また，貢献感の獲得には，前述のテレワーク実施事例 [32] 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 [33] 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 [34] とされている．

「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 [35] を設定した（Q4）．また村田 [8] があ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 [36] を設定した（Q2）．

また，3.1 節であげたリスクテイキング行動として，森泉ら [37] 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

© 2017 Information Processing Society of Japan

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）．

3.3.3 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．

4. 調査および分析

4.1 調査の概要

本稿で分析とする個票データの収集のために，インターネット調査会社のパネル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．本稿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．日本の労働者構造を反映するために，サンプル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，サンプル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）[38] 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，これ以外の区分では 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サンプルを抽出する目的で設定した．

4.2 回答の概要

約 4 万人に対して**表 2** の産業別構成人員比を目標として事前調査を実施した．4.1 節にあげた抽出条件を通過したサンプルであって，インターネット調査会社によって回答時間が短すぎるサンプルを除外した結果，1,242 サンプルの個票データを獲得した．取得サンプルの産業構成人員比率は表 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．

表 2 産業構成人員比率と取得サンプル比率
Table 2 Industrial staff ratio and acquired sample ratio.

業態名称	産業構成人員比（%）	取得サンプル比率（%）
製造業	18.0	25.4
情報通信業	3.5	4.3
運輸業・郵便業	5.9	4.0
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*1	8.0	5.8
医療・福祉	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

n=1242

4.3 サンプルのクリーニング

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 [39]．

この問題に対して今回の調査では，4.2 節であげた調査会社によるスクリーニングに加え，独自のデータ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 [40] 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．これに対して本稿では，(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クリーニングを行い精度の向上を図った．以下にデータクリーニングの手順を述べる．

(1) 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．
(2) 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

*1 学術研究・専門技術サービス・教育・学習支援業

© 2017 Information Processing Society of Japan

いこと．

(3) (2) 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 サンプルが得られた．

4.4 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．

4.4.1 テレワーク実施割合の分析

「サンプルのクリーニング」で得られた 719 サンプルについて，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 サンプル（50.8%），また 0 分と回答したのは 354 サンプル（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 [2] における広義のテレワーカの定義に従った．

4.4.2 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 サンプル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 3** に示す．信頼性はクロンバックの α 係数によって検証する．クロンバックの α 係数は 0 から 1 ま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 [39]．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．

表 3 尺度得点の平均値，標準偏差，およびクロンバックの α 係数
Table 3 Mean, standard deviation, and Cronbach's coefficient alpha.

	設問数	選択肢数	平均	SD	α 係数
職務満足度の高さ（業務に対する性向）					
職務内容 *2	9	4	24.56	5.49	0.91
職場環境 *3	8	4	20.13	4.65	0.86
人間関係 *4	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 *5	6	5	15.88	4.51	0.72
確信的敢行性 *6	3	5	4.99	2.27	0.75
ギャンブル志向性 *7	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 *8	13	7	66.76	10.12	0.90
競争的達成動機 *9	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	3.37	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

n=365

4.5 内部不正を意図しない情報漏洩の経験があるテレワーク実施者の分析

4.5.1 分析手法

本項以降において，本稿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 サンプルのうち，「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 サンプルであり，「いいえ」と回答したのは 345 サンプルだった．

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．正規性の検定に Shapiro-Wilk 検定，等分散の検定に F 検定を用い，有意水準を 5%とした．

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%（$p < 0.05$）において有意差があるとし，有意水準 10%（$p < 0.1$）の場合は

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

© 2017 Information Processing Society of Japan

表 4 尺度得点の差の検定結果
Table 4 Test results of the difference of scale score.

	意図しない漏洩経験あり n=20		意図しない漏洩経験なし n=345		差の有意差
	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	ns
職場環境	22.05	4.84	20.02	4.62	ns
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	ns
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	ns
競争的達成動機	48.05	10.96	45.78	8.95	ns
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	ns
テレワーク手続の面倒感（業務に対する性向）					
	17.65	4.36	17.44	3.88	ns
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．†$p < 0.1$，*$p < 0.05$，**$p < 0.01$，***$p < 0.001$，ns：統計的に有意ではない（Not statistically significant）

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．

4.5.2 内部不正を意図しない情報漏洩経験の有無による尺度得点の差の検定

意図しない情報漏洩経験の有無による 2 群それぞれの尺度得点の差を検定した結果を**表 4** 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 3 のとおりだった．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，確信的敢行性が最も厳格な水準（0.1%水準）で有意であり，次いでギャンブル指向性（1%水準），状況的敢行性（5%水準）であった．

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，10%水準で有意傾向に差が認められた．

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ことが認められた．

5. 全体考察

5.1 考察

本節では，4.5.2 項にあげた検定結果から，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．

「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 [37]）を測定する尺度において最も有意水準が大きな差であったことから，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，3.1 節にあげた村田 [8] 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

© 2017 Information Processing Society of Japan

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あげられる．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あげられる．

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．また，岡野ら [21] の示した手続の整備は，テレワークに対しては有意な差が得られなかった（Q8）．

3.1 節において業務に対する性向の 1 つとしてあげた貢献感については，職務満足度を測る安達の尺度 [33] のうち人間関係について，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 10%水準で有意に大きい傾向がみられることが分かったものの，5%水準では有意でなかった．3.3.2 項に示した我々の先行研究 [11] 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，本稿のように，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 [25] 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 [19] 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%水準では有意でなかったものの 10%水準で有意に高かった．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が示唆された．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．

5.2 本稿の優位性

本稿の優位性として，以下があげられる．

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クロンバック 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．オンライン調査モニタ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 [40] 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．

5.3 本稿の限界

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．

調査会社はモニタ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（たとえば文献 [41], [42]）．これに対して本研究で収集した 1242 サンプルがフィルタリングによって 719 サンプルまで減った理由については，(1) 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，(2) 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モニタ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，(3) 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．

© 2017 Information Processing Society of Japan

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．

本稿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. まとめ

本稿では，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行動性向の比較により，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ものの，対策の効果には個人差があることも示唆された．

本稿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，本稿の対象となっていない．これらを用いた検討と本稿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．

謝辞 本稿の構成についてアドバイスをいただいた，千葉工業大学谷本茂明先生に謹んで感謝の意を表する．

参考文献

[1] 日本テレワーク協会, 入手先 ⟨http://www.japan-telework.or.jp⟩ （参照 2017-02-16）.

[2] 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）.

[3] 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).

[4] 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）.

[5] 総務省：テレワークセキュリティガイドライン，入手先 ⟨http://www.soumu.go.jp/main_content/000238665.pdf⟩ （参照 2017-02-16）.

[6] 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).

[7] 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).

[8] 村田厚生：ヒューマン・エラーの科学，日刊工業新聞社 (2008).

[9] 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）.

[10] 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）.

[11] 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).

[12] 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).

[13] 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).

[14] 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).

[15] 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).

[16] 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).

[17] 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).

[18] 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).

[19] 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).

[20] 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).

[21] 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).

[22] Weeger, A. and Heiko G.: FACTORS INFLUENCING FUTURE EMPLOYEES' DECISION-MAKING TO PARTICIPATE IN A BYOD PROGRAM: DOES RISK MATTER?, *Proc. 22nd Eur. Conf. Inf. Syst. Tel Aviv 2014* (online), available from ⟨http://aisel.aisnet.org/ecis2014/proceedings/track16/3/⟩ (2014).

[23] 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).

[24] 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).

[25] 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).

[26] 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

© 2017 Information Processing Society of Japan

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).
[27] 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).
[28] Kruger, H.A. and Kearney, W.D.: A prototype for assessing information security awareness, *Comput. Secur.*, Vol.25, No.4, pp.289–296 (2006).
[29] 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).
[30] 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）.
[31] 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）.
[32] 総務省：テレワークの意義・効果，入手先 ⟨http://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/18028_01.html⟩（参照 2016-05-08）.
[33] 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).
[34] 堀　洋道，山本眞理子：心理測定尺度集 I.，サイエンス社 (2001).
[35] 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).
[36] 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).
[37] 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).
[38] 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）.
[39] 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).
[40] 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).
[41] 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/monitor_policy.html⟩（参照 2017-06-22）.
[42] 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）.

付　　録

A.1 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 [*10] 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

[*10] 逆転項目：Q2-6，9，10，11，19

© 2017 Information Processing Society of Japan

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
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
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

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

© 2017 Information Processing Society of Japan

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[*11] 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ィ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)

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[*12] 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

[*11] 逆転項目:Q9-5, 14

[*12] 逆転項目:Q11-3

© 2017 Information Processing Society of Japan

畑島 隆 （正会員）

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

坂本 泰久

1989 年東京大学工学部機械工学科卒業．同年日本電信電話株式会社入社．アイデンティティ管理技術，情報セキュリティ技術等の研究開発に従事．

© 2017 Information Processing Society of Japan