Vol.2021-CSEC-95 No.14
Vol.2021-SPT-45 No.14
Vol.2021-EIP-94 No.14
2021/11/8

在宅型テレワークにおける 情報セキュリティポリシーの違反要因の調査

床波大貴† 稲葉緑†

概要：情報セキュリティの確保に組織的に取り組む情報セキュリティマネジメントでは，従業員に，組織の情報セキュリティポリシーの遵守を徹底することが重要である．昨今，テレワークが急速に広まっているが，情報セキュリティポリシーの遵守は徹底されているとは言い難い．テレワークではシャドーIT のリスクが懸念され，特に許可のない私物端末の利用については，ゼロトラストに基づく技術的な対策が行き届きにくい．そのため，テレワークにおける私物端末の利用に関する情報セキュリティポリシーの違反要因を明らかにし，対処することが重要である．本稿は，テレワークにおける許可のない私物端末の利用に関する情報セキュリティポリシーの違反要因を調査し，その違反要因を明らかにするための調査方針を示す．

キーワード：情報セキュリティポリシー，遵守，テレワーク，シャドーIT

Investigating Factors Contributing to Violations of Information Security Policies in Home-Based Telework

HIROKI TOKONAMI† MIDORI INABA†

Abstract: In information security management, which is a systematic approach to ensure information security, it is important to ensure that employees comply with the information security policy of the organization. Recently, telework has been spreading rapidly, but it is difficult to say that the information security policy is thoroughly observed. In telework, the risk of shadow IT is a concern, and it is difficult to take technical measures based on zero-trust for the use of personal devices without permission. Therefore, it is important to identify and deal with the violation factors of the information security policy regarding the use of personal devices in telework. This paper investigates the violation factors of the information security policy regarding the use of personal devices without permission in telework, and presents a research policy for clarifying the violation factors.

Keywords: Information security policy, Compliance, Teleworking, ShadowIT

1. 背景

1.1 はじめに

情報セキュリティの確保に組織的に取り組む情報セキュリティマネジメントでは，従業員に，組織の情報セキュリティポリシーの遵守を徹底することが重要である．なぜなら，従業員が情報セキュリティポリシーに則って行動しない場合，目的とする情報セキュリティが確保されず，情報セキュリティインシデントを発生させる可能性があるからである．例えば，宮城県教育委員会は，従業員が個人情報を私物端末で管理することを禁止するルールに違反した後，ウイルスに感染した私物端末から個人情報が流出した可能性を発表した[1]．また，茨城県警では，従業員が内部規定に違反して，私物のスマートフォンで捜査情報を撮影後，アプリケーションを利用して同僚に流出した[2]．このような違反は，損害を与える悪意がなくとも，故意に情報セキュリティポリシーから逸脱する行為をさす[3][4]．情報セキュリティポリシーとは，セキュリティ体制の構築と実施に関する指示，ガイドライン，手順を提供するものであり[5]，主に情報システム部門や情報セキュリティ部門において維持管理されている[6]．

1.2 テレワークにおける情報セキュリティポリシー

昨今，新型コロナウイルス感染症の影響により，働き方の新しいスタイルとしてテレワークが急速に広まっている[7]．テレワークとは，情報通信手段を活用した，場所や時間にとらわれない柔軟な働き方であり[8]，働く場所によって在宅型，施設利用型，モバイル型に分類される[9]．特に在宅型は，その他の形態と比べて大きく増加した[7]．また，テレワークでは会社支給の PC 端末や私物端末が利用されている[10]．

このような組織を取り巻く新しい環境における情報セキュリティポリシーの遵守徹底の重要性から，多くの組織はテレワーク実施に関するセキュリティのルール制定に取り組んでいる[11]．

しかし，情報セキュリティポリシーの遵守は徹底されているとは言い難い．なぜなら，IPA の調査において，テレワークを導入する組織の従業員のうち，テレワークの実施

† 情報セキュリティ大学院大学

Vol.2021-CSEC-95 No.14
Vol.2021-SPT-45 No.14
Vol.2021-EIP-94 No.14
2021/11/8

に関するセキュリティの社内規定，ルール，手順等を意識していない，または行動していない回答者の割合が 18.0%を占めるからである[12].

以上から，本研究は，テレワークにおける情報セキュリティポリシーが徹底されない理由に着目し，違反要因を調査することをテーマとする．

2. 現状

2.1 テレワークにおけるゼロトラストの普及

テレワークの拡大に伴い，組織ではゼロトラストの優先度が高まっている．Okta の調査によると，テレワークの拡大によって組織におけるゼロトラストの優先度が高まった組織が 83%を占める[13]．ゼロトラストとは，セキュリティの信頼性を担保するための考え方である[14]．NIST はゼロトラストを「リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体」と定義している[15]．ゼロトラストには「資産の整合性とセキュリティ動作を監視し，測定する」「資産，ネットワーク，通信の現状について可能な限り多くの情報を収集する」のように，資産に関する情報を技術的に監視，管理するという原則が存在する[15].

今後も，多くの組織でゼロトラストが導入されていく可能性が高い．なぜなら，Okta の調査によると，国内では既にゼロトラストに基づくセキュリティの取組みを実施している組織が 31%を占めており，今後 18 ヶ月の間で実施する予定の組織が 37%を占めるためである[13].

2.2 テレワーク下のセキュリティリスク

テレワークでは，仕事の生産性を確保するため，遠隔での作業を可能にする端末や，遠隔でのコミュニケーションを円滑にするソフトウェア，クラウドサービスなどの ICT ツールの活用が不可欠である．IPA が国内のテレワーク実施経験のある組織に対して行った調査によると，既存の情報セキュリティポリシーのうち「個人が所有する端末の業務利用」「会社が許可していないアプリケーション・ソフトウェア・クラウドサービスの業務利用」はコロナ禍においても特例や例外を認めず禁止する組織が多い[12]．しかし，コロナ禍によってテレワークの導入を余儀なくされ，一時的に特例や例外を認める組織も存在する[12].

このような ICT ツールの利用制限の緩和がみられるテレワーク下で，大手セキュリティ企業は，組織の中で従業員が使用する端末, ソフトウェア, クラウドサービスのうち，IT 部門の正式な承認を受けていないシャドーIT[16]によるセキュリティリスクを懸念している．例えば，トレンドマイクロが世界 27 か国のテレワークを実施している従業員に対して行った調査によると，39%が個人用端末から企業データにアクセスし，56%が使用許可のないアプリを使用し，66%が認可のないアプリ上に企業データをアップロードしている[17]. この結果に対して, トレンドマイクロは，テレワーク環境ではシャドーIT がセキュリティリスクを上げる原因になることを指摘している[17]．LAC は，テレワーク下において情報システム担当者を悩ませていることに，従業員が無断で許可されていないデバイスやクラウドサービスを利用するシャドーIT を挙げている[18].

Mallmann らは，文献調査からシャドーIT を「クラウドサービスの使用」「アプリケーションの開発」「ソフトウェアのインストール」「従業員が所有する端末(以下，私物端末)の使用」の 4 つの種類に分類している[19]．大手セキュリティ企業が懸念視するシャドーIT のうち，「私物端末の使用」については，端末の管理が従業員に任されるため，ゼロトラストが原則とする監視等の技術的な対策が行き届きにくいと考えられる．そのため，本研究では，テレワーク下のセキュリティリスクのうち,「許可のない私物端末の使用」を取り上げる．

キヤノンマーケティングジャパンの調査によると，従業員は，私物端末を利用して，ビジネスメールの送受信，オフィスソフト等での資料作成・閲覧，画像や動画の撮影・加工・編集，LINE 等のアプリケーションを利用した連絡を行うことが多い[20]．そのため，ゼロトラストが原則とするネットワークや通信の監視を実施した場合でも，許可なく私物端末を利用することにより，私物端末上で生成された資料や画像等の情報が，組織のネットワークが届かない範囲で第三者に流出するリスクがある．

2.3 私物端末利用ルールと遵守状況の実態

許可のない私物端末の使用に伴うセキュリティリスクに対して，国は，実施すべき対策にルールの整備を挙げている．例えば，総務省は，テレワークセキュリティガイドラインの中で，システム・セキュリティ管理者が実施すべき対策に，業務上利用可能な対象を定めた上で，許可されていない対象については事前申請とセキュリティ上の問題ないことを条件に許可するルールを提示している[21]. IPA は，実施すべき対策にルールの整備や見直しを挙げている[22]が，どのようなルールにすべきか明らかにしていない．

企業も情報セキュリティポリシーの整備を進めているが，許可のない私物端末の使用ルールについては十分に規定されているとは言い難い．例えば，モバイルコンピューティング推進コンソーシアムセキュリティ委員会の調査によると，私物を利用することを禁止するルールを整備している企業は 40%に満たない[23]．IPA の調査によると，テレワークにおけるセキュリティルールを制定する企業のうち，私物端末で秘密情報を扱う場合の対策の実施に関するルールの制定率は 40%に満たない[24].

情報セキュリティポリシーが十分に整わない中で，情報

Vol.2021-CSEC-95 No.14
Vol.2021-SPT-45 No.14
Vol.2021-EIP-94 No.14
2021/11/8

セキュリティポリシーに違反して，許可のない私物端末を利用する従業員は一定数存在すると考えられる. なぜなら，IPA の調査において，テレワークの際の情報の取扱いルールのうち，個人所有の機器の業務での利用範囲・用途，業務に利用する個人所有の機器の登録に関するルールに対して，たまに守れていない，または守っていない回答者の割合が 15%弱を占める[12]からである.

このような許可のない私物端末を利用する行為は，前述の通り既に国内で情報漏えいの情報セキュリティインシデントをもたらしており[1][2], テレワークを導入する組織に対しても，同様のインシデントが発生するリスクをもたらす可能性がある.

3. 先行研究

3.1 私物端末の利用に関するポリシーの違反要因

3.1.1 情報セキュリティポリシーの認知不足

IPA の調査によると，テレワーク実施に関するセキュリティのルールに対して,「ルールが周知できていない」という課題意識をもっている回答者が 20%以上を占める[22]. この調査結果は，情報セキュリティポリシーを認知できていない場合に，情報セキュリティポリシーの遵守意図が下がる可能性を示唆する．そのため，テレワーク下の私物端末の利用に関する情報セキュリティポリシーを認知できていないことが，違反して許可のない私物端末を利用する要因となる可能性がある.

3.1.2 情報セキュリティポリシーの理解不足

IPA の調査によると，テレワーク実施に関するセキュリティのルールに対して,「社員の理解が不十分」という課題意識をもっている回答者が 20%以上を占める[22]．この調査結果は，情報セキュリティポリシーで定められている内容を十分に理解できていない場合に，情報セキュリティポリシーの遵守意図が下がる可能性を示唆する．そのため，テレワーク下の私物端末の利用に関する情報セキュリティポリシーを十分に理解できていないことが，違反して許可のない私物端末を利用する要因となる可能性がある.

3.1.3 パフォーマンス向上の認知

Ortbach ら[25]は，業務のパフォーマンス向上の認知が，業務遂行のために会社が提供していない IT 技術を使用する意思に正の影響を与えることを確認している. Shalow ら[26]は，従業員が使用するツールに慣れ親しみ，効率的に取り組めるため, プロジェクトに自分の Mac 端末を用いる場合があることをインタビュー調査で確認している．このような認知は，職場環境を問わず，私物端末の利用に伴って喚起されるものと考えられるため，テレワーク環境においても，違反して許可のない私物端末を利用する要因となる可能性がある.

3.1.4 利用にかかるコスト認知

Zimmermann ら[27]は，正式な手段として IT を利用するのにかかる時間や労力が, 組織の管理下にない IT ソリューションの利用を促す主な理由であることをインタビュー調査で確認している. このような認知は, 職場環境を問わず, 情報セキュリティポリシーを遵守しなければならない場面で喚起されるものと考えられるため，テレワーク環境においても，違反して許可のない私物端末を利用する要因となる可能性がある.

3.1.5 セキュリティリスクの認知不足

Tu ら[28]は，セキュリティリスクの重大性及び可能性の認知が，BYOD ルールの遵守意図にそれぞれ正の影響を与えることを確認している．BYOD とは，従業員が個人所有のモバイル機器を職場に持ち込み，それを使って企業の情報やアプリケーションにアクセスすることを指す[28]. Hovav ら[29]も，セキュリティ脅威の認知が BYOD ルールの遵守意図に正の影響を与えることを確認している．これらの調査結果は，セキュリティリスクの認知度合いが低いほど, BYOD ルールの遵守意図が下がる可能性を示唆する. このような認知は，職場環境を問わず，私物端末の利用に伴って喚起されるものと考えられるため，テレワーク環境においても，違反して許可のない私物端末を利用する要因となる可能性がある.

3.1.6 自己効力感の認知不足

Tu ら[28]は，自己効力感の認知が，BYOD ルールの遵守意図に正の影響を与えることを確認している．自己効力感とは，自分が適応反応をうまく実行できる見込みを指す[30]．この調査結果は，情報セキュリティポリシーに対する自己効力感の認知度合いが低く，情報セキュリティポリシーを遵守できないと感じる場合ほど，情報セキュリティポリシーの遵守意図が下がる可能性を示唆する．このような認知は，職場環境を問わず，情報セキュリティポリシーを遵守しなければならない場面で喚起されるものと考えられるため，テレワーク環境においても，違反して許可のない私物端末を利用する要因となる可能性がある.

3.1.7 有効性の認知不足

Tu ら[28]，Hovav ら[29]は，有効性の認知が，BYOD ルールの遵守意図に正の影響を与えることを確認している. 有効性の認知とは，対処行動の効果性を指す[30]．この調査結果は，情報セキュリティポリシーの有効性の認知度合いが低く，情報セキュリティポリシーの効果を感じにくい場合ほど，情報セキュリティポリシーの遵守意図が下がる可能性を示唆する. このような認知は, 職場環境を問わず,

Vol.2021-CSEC-95 No.14
Vol.2021-SPT-45 No.14
Vol.2021-EIP-94 No.14
2021/11/8

情報セキュリティポリシーを遵守しなければならない場面で喚起されるものと考えられるため，テレワーク環境においても，違反して許可のない私物端末を利用する要因となる可能性がある．

3.1.8 他者の許可のない私物端末の利用に対する認知

Mallmann ら[19]は，同僚による許可のない私物端末の利用に対する認知や，ユーザーの間でその技術が知られ，流行っているという信念が，従業員による許可しない私物端末を含む IT リソースの利用意図に正の影響を及ぼすことを明らかにしている．Ortbach ら[25]は，同僚と上司による会社が提供していない IT 技術の利用に対する認知が，従業員による会社が提供していない IT 技術を利用する意思に正の影響を与えることを確認している．

このことから，同僚による許可のない私物端末の利用に対する認知は，従業員による許可のない私物端末の利用を促進する要因になることが示唆されている．しかし，在宅型のテレワークでは，職場の関係者が周りにいない状況が想定されるため，違反して許可のない私物端末を利用する要因にならない可能性がある．

3.1.9 他者の視線からの回避認知

中俣ら[31]は，社会的規範からの逸脱の一つであるゴミのポイ捨てに対する監視カメラの効果を検証しており，監視カメラの存在がゴミを捨てにくくする要因になっていることを確認している．橘ら[32]は，大学建物内下足進入禁止の規則違反を社会的迷惑行為と定義し，他者の視線を喚起させるポスターが社会的迷惑行為を抑制することを確認している．また，宮本ら[33]は，職場内コミュニケーションと職場内で経験したことのある違反行為の関係を調査し，一人で働く時間の割合が 1 割未満の回答者よりも，1 割から 5 割の回答者の違反経験が多いことを確認している．そして，組織成員を職場環境から孤立させることは違反意識を促す可能性に言及している．Zhong ら[34]は，暗闇環境が人の利己的行為に及ぼす影響に関する実験を行っている．その結果，明るい環境よりも暗闇環境において人の利己的行為が誘発されることが確認された．また，暗闇環境における匿名性の知覚が，暗闇環境の利己的な行動への影響を媒介していることがわかった．この結果に対して，Zhong らは，暗闇の経験が，「自分は他人の注意や監察から守られている」という心理的信念を誘発し，有害な結果をもたらす可能性に言及している[34].

このことから，他者の視線が届きにくい環境では，規範からの逸脱行為が起きやすいと考えられる．また，「自分は他人の注意や監察から守られている」という認知によって，規範からの逸脱行為が促される可能性がある．在宅型のテレワークでは，職場の関係者が周りにおらず，職場の関係者の注意が及びにくい状況において業務を行う場面が多いと推測されるため，このような他者の視線からの回避認知が違反して許可のない私物端末を利用する要因となる可能性がある．

3.1.10 正当化認知

Haag ら[35]は，許可のない私物のスマートフォン等の ICT ツールの利用ルールに対する違反行動に影響を及ぼす要因を，中和技法に基づき調査している．中和技法は，既存の規範に反した行動を正当化することで，その規範を効果的に回避する方法を提供する考え方を前提にしたものである[36]．Haag ら[35]は，メールによって時間内にファイルを送信する実験において，ルールを遵守した人と違反した人の正当化による違反態度を比較している．そして，違反した人の方が，違反しなかった人と比較して，理不尽な情報セキュリティポリシーなら違反してよいとする「非難」，害が及ばなければ違反してよいとする「被害の否定」，ルール違反が必要と見なされるならば罪悪感を覚えるべきではないとする「必要性の防衛」からなる正当化による違反態度がそれぞれ高いことが確認された[35]．本実験は，被験者がその他の関係者から隔離された部屋で行われたことから，職場の関係者の注意の及びにくいテレワーク環境でも，同様の正当化認知が，違反して許可のない私物端末を利用する要因となる可能性がある．

3.2 違反要因のまとめ

人間の心理や行動に関連する要因は，個人的要因と環境的要因に区別することにより，要因の整理が促進される[37]．そこで，先行研究に基づき抽出した私物端末の利用ポリシーに対する違反要因を，以下の表 1 に整理した．

表 1．ポリシーの違反要因

分類	要因
個人的要因	情報セキュリティポリシーの認知不足
	情報セキュリティポリシーの理解不足
	パフォーマンス向上の認知
	利用にかかるコスト認知
	セキュリティリスクの認知不足
	自己効力感の認知不足
	有効性の認知不足
環境的要因	他者の利用度合いに対する認知
	他者の視線からの回避認知
	正当化認知(非難)
	正当化認知(被害の否定)
	正当化認知(必要性の防衛)

在宅型テレワークは，オフィス環境と異なり，職場の関係者が周りにおらず，職場の関係者の注意が及びにくい状況において業務を行う場面が多いと想定される．そのため，他者が関係する環境的要因に差がみられる可能性がある．例えば，抽出した要因のうち，他者の利用度合いに対する認知については，オフィス環境では違反要因になる一方で，

在宅型テレワークでは違反要因にならない可能性がある．また，他者の視線からの回避認知については，在宅型テレワークにおいてのみ違反要因になる可能性がある．

4. 研究目的

テレワークにおいて，許可のない私物端末の利用はゼロトラストに基づく技術的な対策が行き届きにくい．そのため，テレワークにおける私物端末の利用に関する情報セキュリティポリシーの違反要因を明らかにし，対処することが重要である．

しかし，先行研究の知見だけでは，違反要因が明らかになったとは言い難い．なぜなら，許可のない私物端末の利用要因に着目した先行研究は確認されたが，テレワーク環境にも当てはまるかどうかは定かでないからである．

以上から，本研究は，テレワーク下での許可のない私物端末の利用に関する情報セキュリティポリシーの違反要因を調査することを目的とする．

5. 方法

5.1 研究対象

本研究は，テレワーク導入の拡大に伴うセキュリティリスクを背景とするため，国内で緊急事態宣言を機に在宅型テレワークが導入された組織に勤めている従業員を対象とする．

また，テレワークでは会社支給の端末だけでなく，従業員所有の端末が利用されることも多い[9]ため，私物端末の利用が禁止されている組織に勤めている従業員と，私物端末の利用が一部許可されている組織に勤めている従業員の両方を対象とする．

5.2 研究手法

本研究は，情報セキュリティポリシーの違反要因を明らかにする先行研究の多くが採用していること，違反に影響を及ぼしうる要因を操作することが難しいことから，オンライン(Web)型・個別自記入式の質問紙調査法を採用する．在宅型テレワークを実施している従業員と，オフィスで業務を行っている従業員を比較することで，会社が許可していない私物端末の業務利用に関する情報セキュリティポリシーの違反意図，及びその要因を明らかにする．

6. まとめと今後の研究

情報セキュリティの確保に組織的に取り組む情報セキュリティマネジメントでは，従業員に，組織の情報セキュリティポリシーの遵守を徹底することが重要である．昨今，テレワークが急速に広まっているが，情報セキュリティポリシーの遵守は徹底されているとは言い難い．テレワークではシャドーIT のリスクが懸念され，特に許可のない私物端末の利用については，ゼロトラストに基づく技術的な対策が行き届きにくい．そのため，テレワークにおける私物端末の利用に関する情報セキュリティポリシーの違反要因を明らかにし，対処することが重要である．

本稿は，許可のない私物端末の利用に関する情報セキュリティポリシーの違反要因を調査した．その結果，7 種類の個人的要因と 5 種類の環境的要因が抽出された．また，先行研究の知見だけでは，在宅型テレワークにおける違反要因が明らかになったとは言い難いことを述べ，違反要因を検証するための調査方針を示した．

今後は，調査方針に沿って違反要因の調査を進め，調査結果を踏まえた考察を行う．

引用文献

[1] CyberSecurity.com, [私用 PC ウイルス感染で特別支援学校の生徒情報が流出か｜宮城県教育委員会(2018.11.2）https://cybersecurity-jp.com/news/27929
[2] CyberSecurity.com, 行事予定など撮影し同僚に流出、茨城県警の女性警官が訓戒処分(2020.10.23) https://cybersecurity-jp.com/news/44053
[3] Guo et al, Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model, Journal of Management Information Systems, Vol.28, No.2, pp.203-236 (2011)
[4] Reason et al, Organizational controls and safety: The varieties of rule-related behavior, Journal of Occupational and Organizational Psychology, 71, p.289-304(1998)
[5] Whitman, Information Systems Security and the Need for Policy , Information Security Management: Global Challenges in the New Millennium(2001)
[6] 情報セキュリティ大学院大学 原田研究室, 2018 年情報セキュリティアンケート調査結果(2018)
[7] 国土交通省, 令和2年度テレワーク人口実態調査―調査結果の抜粋―(2021)
[8] 日本テレワーク協会, テレワークとは https://japan-telework.or.jp/tw_about/
[9] 総務省, テレワークの動向と生産性に関する調査研究報告書(2010)
[10] 総務省, テレワークセキュリティに係る実態調査(1 次実態調査)報告書(2020)
[11] 総務省, テレワークセキュリティに係る実態調査(2 次実態調査)報告書(2021)
[12] 情報処理推進機構, ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査(2021)
[13] Okta ,アイデンティティを中心としたゼロトラスト導入実態調査（2021）
[14] 勝村幸博, ゼロトラスト―Google が選んだ最強のセキュリティー―, 日経 BP(2021)
[15] NIST，Zero Trust Architecture，SP 800-207 (2020)
[16] Mario Silic, Shadow IT – A view from behind the curtain, Computers & Security Volume 45, September 2014, Pages 274-283(2014)
[17] トレンドマイクロ, テレワークの意識調査：安全のためにセキュリティ教育が重要なワケ(2020.08.24) https://blog.trendmicro.co.jp/archives/25968
[18] LAC，With コロナ時代の 7 つのサイバーリスク～いま経営者が考えるべき、テレワークとサイバーセキュリティとは～

Vol.2021-CSEC-95 No.14
Vol.2021-SPT-45 No.14
Vol.2021-EIP-94 No.14
2021/11/8

(2020.07.07)
https://www.lac.co.jp/lacwatch/people/20200707_002224.html
[19] Mallmann et al, We are social: a social influence perspective to investigate shadow IT usage, ECIS2018, Portsmouth, UK. (2018)
[20] キヤノンマーケティングジャパン，情報セキュリティ意識に関する実態調査レポート 2021～コロナ禍で高まる「シャドーIT」の情報セキュリティリスク～(2021.07.08)
[21] 総務省，テレワークセキュリティガイドライン第 5 版(2021)
[22] 情報処理推進機構, 情報セキュリティ白書 2021(2021)
[23] モバイルコンピューティング推進コンソーシアムセキュリティ委員会，モバイルデバイスの積極的な利活用における個人情報保護法の影響調査（その２）(2021)
[24] 情報処理推進機構，企業における営業秘密管理に関する実態調査 2020 調査実施報告書(2021)
[25] Ortbach et al, What Influences Technological Individealization?-An Analysis of Antecedents to IT Consumerization Behavior, Americas Conference on Information Systems, USA(2013)
[26] Shalow et al, The Blurring Boundaries Of Work-Related And Personal Media Use: A Grounded Theory Study On The Employee's Perspective, ECIS 2013 Completed Research. Paper 212(2013)
[27] Zimmermann et al, On the emergence of shadow IT -A transaction cost-based approach, 22nd European Conference on Information Systems(2014)
[28] Tu et al, Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory, Journal of the Midwest Association for Information Systems, Volume2019, Issue1, Article2(2019)
[29] Hovav et al，This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy，Pervasive and Mobile Computing 32, 35-49(2016)
[30] 木村堅一，脅威アピールにおける防護動機理論研究の検討，The Japanese Journal of Experimental Social Psychology，Vol. 37, No. 1, 85-96(1997)
[31] 中俣友子，阿部恒之，ごみのポイ捨てに対する監視カメラ･先行ゴミ・景観・看板の効果，心理学研究第 87 巻第 3 号 pp.219-228(2016)
[32] 橘美沙，小野夏月，橋詰佳代子，坂口遥菜，森影佳子，中村有里，他者の視線を喚起させるポスターの提示による社会的迷惑行為への影響，川崎医療福祉学会誌 Vol.28 No.1 241-247(2018)
[33] 宮本聡介，上瀬由美子，鎌田晶子，岡本浩一，組織制度・職場コミュニケーションが違反意識・違反経験に及ぼす影響，社会技術研究論文集 Vol.1 228-238(2003)
[34] Chen-Bo Zhong et al, Good Lamps Are the Best Police: Darkness Increases Dishonesty and Self-Interested Behavior, Psychological Science 21(3), 311-314(2010)
[35] Haag et al, The Acceptance of Justifications among Shadow IT Users and Nonusers-An Empirical Analysis, Information&Management 56, 731-741(2019)
[36] Rogers et al, Neutralization Techniques: Toward a Simplified Measurement Scale, The Pacific Sociological Review Vol. 17, No. 3, pp. 313-331(1974)
[37] 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)