Vol.2021-DPS-188 No.4
Vol.2021-EIP-93 No.4
2021/9/9

コロナ禍のテレワーク導入と組織のセキュリティ対策への影響に関する分析*

小山明美[1]　森淳子[1]　小川隆一[1]　竹村敏彦[2]

概要：テレワークについては働き方改革に有用な手段として，導入の検討や実施がされてきた．2020 年 4 月に緊急事態宣言が発出され，外出自粛が求められたことにより，多くの組織は，想定を超える規模，勢いでテレワークを実施しなければならなくなった．事業継続の為，短期間での対応せざるを得なかったため，制度の整備や既存ルールの見直し，リスクの評価等は十分な議論ができないままにテレワークを導入した組織もあり，このような組織ではセキュリティ対策についても，情報の取扱に関する特例や手続きの簡略化等が行われた．本研究では，2020 年 11 月に独立行政法人情報処理推進機構が実施した「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」の調査結果から，セキュリティ対策緩和の実態と組織の特性について分析を行った．その結果，業種，規模，テレワークの導入時期等とセキュリティ対策への影響について整理し，緩和された対策について緊急事態宣言から半年経過しても対応がされず，リスクが増大している可能性があることがわかった．

キーワード：テレワーク　セキュリティ対策　ニューノーマル　サプライチェーン

A Study of Adaptation to Telework under the Spread of COVID-19 Affecting the Organizational Security Measures

AKEMI KOYAMA[1]　JUNKO MORI[1]　RYUICHI OGAWA[1]
TOSHIHIKO TAKEMURA[2]

Abstract: Telework has been considered and used as a useful tool for work style reform. A state of emergency was issued in April 2020, demanding that people refrain from going out. As a result, many organizations needed to work from home quickly over a wide area. We needed to prioritize business continuity and achieve it in a short period of time. Some organizations started working from home without enough discussion about organizing, reviewing existing rules, and risk assessment. Such organizations are mitigating security measures. For example, we acknowledged deviations in the handling of information and simplification of procedures. In this study, we analyzed the actual situation of security measure mitigation and the characteristics of the organization from the survey results of "Telework and IT supply chain security survey in New Normal" conducted by IPA in November 2020. As a result, the type of industry, scale, time of introduction of telework, and the impact on security measures were summarized. It was also found that the mitigated measures may not be dealt with even six months after the state of emergency was declared, and the risk may have increased.

Keywords: Telework, Security measure, New normal, Supply chain

1. はじめに

テレワーク[a]は，ライフワークバランスの向上や育児・介護中の就業の継続，働き方改革による経営改善，災害時等の事業継続性確保のための有用な手段として，導入の検討や実施がされ，徐々に導入率は上昇している．総務省の通信利用動向調査[1]によると，2019 年のテレワーク導入率は 20.2%に留まっていたものの，新型コロナウイルス感染症（COVID-19）が猛威を振るった 2020 年の導入率は 47.5%となり，わずか 1 年で倍以上の企業・組織がテレワークを導入・運用をはじめたことが報告されている．また，その中で，テレワーク導入の目的を「非常時（感染症の流行等）の事業継続」と回答する割合が 7 割と最も多かった．このことからも，2020 年 4 月に緊急事態宣言[b]が発出されて，外出自粛が求められたことにより，多くの企業・組織は，想定を超える規模，勢いでテレワークを実施しなければならなくなったことが導入率を急増させた要因として考えられる．

テレワークの推進にあたって，総務省から安心してテレワークを導入・活用するための指針として「テレワークセキュリティガイドライン第 4 版」[2]，厚生労働省からテレワークにおける労務管理の留意点を記載したものとして「情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン」[3]や自営型テレワーク[c]の適切

* 本研究の意見は，著者たち個人に帰属し，所属機関の公式見解を示すものではないことをことわっておく．

1 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan
2 城西大学
Josai University

a 本研究で想定しているテレワークは，在宅勤務，モバイル勤務，サテライトオフィス勤務などを含んだものである．

b 本研究では，特段の補足説明がない限り，第一回目（2020 年 4 月 7 日～5 月 25 日）の緊急事態宣言を指す．

c 自営型テレワークとは，「注文者から委託を受け，情報通信機器を活用して，主として自宅又は自宅に準じた自ら選択した場所において，成果物の

Vol.2021-DPS-188 No.4
Vol.2021-EIP-93 No.4
2021/9/9

な実施に向けた「自営型テレワークの適切な実施のためのガイドライン」[4]などが公表されており，導入検討時に参照可能な種々のガイドラインがコロナ禍以前から存在している．

従来の日本の就業形態としては，オフィスや工場，店舗等決められた場所（職場）に通勤する，あるいは取引先等に出向くというスタイルが一般的であった．業務に必要な設備や機材は組織が用意し，従業員に貸与し，決められた場所に保管された情報が利用できるようにする．したがってテレワークを導入するためには，職場以外で利用できるICT 機器の準備や就業規則および関連する規程等の改定，従業員への周知徹底など，金銭的，時間的，体制的に多大なリソースの準備が必要とされる．従来のテレワークの利用は出社が困難である場合の代替手段であり，利用者や利用期間は限定的なものを想定していた．そのため，緊急事態宣言の発出により多くの企業・組織が一斉に準備を開始したことで端末の調達，ネットワークやツールの利用拡大などが集中し，対応が間に合わず，急場しのぎで個人所有機器の利用等の対応をせざるを得かったものであった．また，2021 年 1 月には第 2 回目の緊急事態宣言が出され，コロナ禍の収束が見通せない状況であったため，個人的・組織的な対応が急がれた．この混沌とした状況の中で,「ニューノーマル」と呼ばれる新しいワークスタイルや IT の活用方法が注目され，緊急事態宣言の解除後も新型コロナウイルス感染リスクだけでなく，働き方改革，オリンピック・パラリンピック，環境問題等以前から求められてきた課題の対策としても有効とされた．

新型コロナウイルス感染拡大防止において最優先であったことは，長期間の外出自粛の中でも事業を継続させることであった．しかしながら職場環境で行うことを前提としていた業務を，職場以外で実施するには，必要な情報を持ち出すか，職場以外から職場環境にアクセスしなければならない．情報の持ち出しや外部からの情報へのアクセスは，情報セキュリティ上最も基本的な対策として，禁止とするか，あるいは，安全性を確保できる技術的対策のもとに許可されることが多い．禁止としている情報を勝手に持ち出したり，許可されていない状態で外部から情報にアクセスしたりすることは不正行為として，処罰される対象となりうる．緊急事態宣言下においては，組織として在宅勤務を命じたことから，事業継続のために，組織が特例や例外処置として一時的に禁止行為の緩和や許可を受けるための手続きを簡素化，あるいは省略する組織が少なくなかったことが報告されている[5].

これらの ICT 環境をはじめとしたニューノーマルへの対応（業務実施場所の多様化，コミュニケーションのオンライン化）に伴う変化により，IT サプライチェーンにおけるリスクならびに情報セキュリティにも影響を与えていると考えられる（ニューノーマルに対応した IT システム・社内ネットワーク・ソフトウェア開発の受委託，また，それに関する契約の変更，セキュリティ・リテラシー教育内容の高度化，BYOD の増加，社内ネットワーク外で使用される端末の増加, オンライン会議やクラウドサービス等の IT ツールの利用増加など）. それゆえに, ニューノーマルにおける IT サプライチェーンに関して, 従来の契約内容を再考する必要があると思われる．例えば，機密情報を取り扱う場合などは作業環境について指定することもあるものの，テレワークを作業環境として想定されていることは少なく，委託先，再委託先の社員がテレワークをする場合の情報セキュリティ対策についても再確認が望ましい．また，情報共有についても対面の会議形式で行われていた定例会など, オンライン会議に変更されることが多くなり，コミュニケーションが十分に取りにくくなることがある．使い慣れないツールの利用は設定間違いなどで情報流出等のリスクもあるため, 使用する環境にあわせて管理ルールを取り決め, 守られていることを点検することも必要となる．

IPA では，2020 年 11 月にニューノーマルへの対応に伴う変化により, IT サプライチェーンの情報セキュリティにどのような影響が生じているのかを確認するとともに，新たな情報セキュリティリスクについての認識や対応の実態から，ニューノーマルにより生じた課題の整理と対策の方向性を示し，今後の情報セキュリティリスク低減への取り組みに資することを目的として「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」[5]を実施した．この調査の中で委託元企業ならびに委託先企業に対して，セキュリティ対策の社内規定・規則・手順等について一時的な特例や例外を認めたか，もし認めたのであればそれは緊急事態宣言解除後その特例や例外が継続されているのかといった質問を行っている．本研究では，この質問について深掘りをすべく，コロナ禍においてテレワークを実施していた組織のセキュリティ対策に影響を与える要因は何であったかについて統計的分析を試みる．

2. 関連研究

組織における規則やルール等の違反に関する研究はいくつかある．例えば，文献[6]はセキュリティの観点から問題となることを禁止している組織の規則やルールを破る従業員についての分析を試みている．彼らの分析の結果，セキュリティ意識の高い従業員はルール違反をしない傾向にあることや正規雇用の従業員の方が非正規雇用の従業員よりもどちらかというとルールを破る傾向があること等を明らかにしている．また，文献[7]では，情報漏えいにつなが

作成又は役務の提供を行う就労」のことである．

る行動に直接的・間接的に影響を与えている要因について分析を行っている．その結果，従業員を取り巻く環境が大きな影響を与えていること等を明らかにしている．これらの研究では，必ずしもテレワークを想定していないものの，テレワークにおいて，ルールとして禁止された行為を行うことは，セキュリティ意識が高いゆえに抵抗感があり，結果として事業継続に支障が出る恐れがある．一方で，テレワークは，内部不正などをはじめとする情報セキュリティの観点からの問題のある行動をとりやすい職場環境になり得ることも示唆される[8]．それゆえに，十分なリテラシー向上のための教育・トレーニングに加えて，有効かつ実現可能なルール等の整備を行うことが求められる．

文献[9]では，内部規範に逸脱した事象に対して，違反や罰則を適用するのではなく，例外措置を適用することが効果的な場合があることを示唆する分析を行っている．また，例外措置は原則規定からの一時的な措置であると考え，定期的な見直しをマネジメントの一環として行う必要性について言及している．

コロナ禍における情報セキュリティ対策等に対する不安について研究しているものもある[10]．文献[10]は，コロナ禍でテレワークやオンライン会議などを急遽導入することになり，マニュアルの整備や教育訓練などが十分行われなかったことに対して，従業員が感じるセキュリティに関する不安（インシデントが発生した場合にどのような問題が発生するか）と個人属性や個人が所属している企業属性の関係についての多重コレスポンデンス分析を行っている．セキュリティ・インシデント発生時の対応に不安を感じているのは「勤務地が首都圏以外」および「テレワークの実績が浅く実施頻度が低い場合」であることなどを明らかにしている．コロナ禍における情報セキュリティ対策等に関する研究の蓄積はまだそれほど進んでいない．今後，これらの蓄積が進むことが求められる．

3. アンケート調査

3.1 調査概要

IPA では 2020 年度に「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」[5]を実施した．この調査の目的は，ICT 環境をはじめとしたニューノーマルへの対応に伴う変化により，IT サプライチェーンの情報セキュリティ対策にどのような影響が生じているのかを確認するとともに，新たな情報セキュリティ上のリスクについての認識や対応の実態から，ニューノーマルにより生じた課題の整理と対策の方向性を示すことである．この調査では，2020 年 11 月 2 日から 11 月 13 日にかけて個人を対象としたウェブアンケート調査，2020 年 11 月 18 日から 12 月 11 日にかけて企業・組織を対象とした郵送調査，2020 年 10 月 6 日から 2021 年 2 月 16 日にかけてインタビュー調査をそれぞれ実施している．本研究では，この中で，企業・組織を対象とした調査（以下，「企業・組織調査」と称す）を取り上げる．「企業・組織調査」は，ニューノーマルへの組織の対応方針，対応状況及び IT サプライチェーンに関する変更について実態を把握することを目的としている．また，これまで IPA が継続して調査を実施している IT システム・サービスの業務委託に関する調査にならい，「企業・組織調査」は，1) 委託元として IT 企業等に対して IT システム・ソフトウェアの製造・開発・保守・運用等を発注・委託している，IT サービスの提供を受けている企業・組織の担当者（委託元企業），2) 顧客から IT システム・ソフトウェアの製造・開発・保守・運用等を受託している，もしくは IT サービスを提供している企業の担当者（委託先企業）をそれぞれ対象とした調査（2 種類）を実施している．これらの調査票は，委託元企業と委託先企業に共通の質問がほとんどであるが，委託元企業や委託先企業に特有の質問が一部あるという構成になっている．前者の最終的な回答者（有効回答者）数は 218 人，後者は 287 人である．また，調査票には，テレワークの実施状況，テレワークを導入する際のセキュリティ対策の社内規定・規則・ルールやセキュリティ・インシデントへの対応体制や手順，委託先企業もしくは委託元企業との状況などを問う質問項目があり，それぞれの質問総数は 45 問程度である．なお，「企業・組織調査」は当時の状況を表しているものであり，現在では状況が大きく変わっている可能性があることを断っておく．

以下，本研究と関連する質問項目に関する回答結果の概況を紹介する．これらの質問項目以外については文献[5,11]を参照されたい．

3.2 質問項目と概況

「企業・組織調査」を実施した 2020 年 11 月は，最初の緊急事態宣言が発出された 2020 年 4 月から半年経過し，7 月から 8 月に第 2 波と呼ばれる新型コロナウイルス感染者数の増加が見られたもののその後減少し，経済活動が徐々にコロナ禍以前の状態に戻りつつある状況であった．そこで，「企業・組織調査」では，2020 年 10 月 31 日を「現在」と考え，テレワーク導入時期などについては，緊急事態宣言前，緊急事態宣言中，緊急事態宣言後と細かく時期を分けた設問とした．

(1) テレワークの実施状況（2020 年 10 月 31 日時点）

「企業・組織調査」では，2020 年 10 月 31 日時点でのテレワークの実施状況について質問をしている．その集計結果が，図 1 である．図 1 から，委託先企業と委託元企業でテレワークの実施状況が異なることが見てとれる．委託元企業について見てみると，テレワークの経験ある回答者と経験がない回答者はほぼ同数となっている．一方で，委託先企業については 95%以上の回答者がテレワークの経験が

Vol.2021-DPS-188 No.4
Vol.2021-EIP-93 No.4
2021/9/9

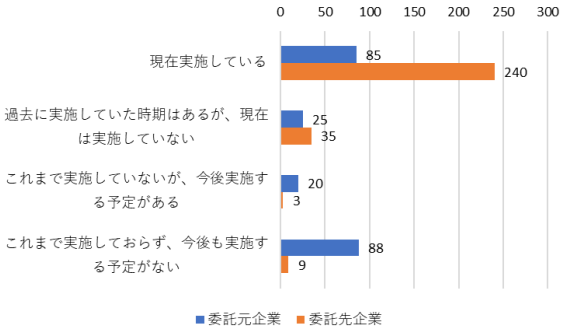

図 1：テレワークの実施状況

あると答えている．

以下，この中で，「現在実施している」「過去に実施していた時期はあるが，現在は実施していない」を選択したテレワークの経験がある回答者（委託元企業の回答者数は 110 人，委託先企業の回答者数は 275 人）を対象として，以下の質問項目を見ていく．

(2) テレワークの開始時期

「企業・組織調査」では，テレワークの経験がある回答者に対して，いつからテレワークを実施しているかについて質問している．図 2 はその集計結果である．図 2 を見てわかるように，委託元企業に関しては，緊急事態宣言中（2020 年 4 月 7 日～5 月 25 日）と回答した割合が最も高く（50.9%），委託先企業に関しては緊急事態宣言前（～2020 年 4 月 6 日）と回答した割合が最も高い（50.0%）．

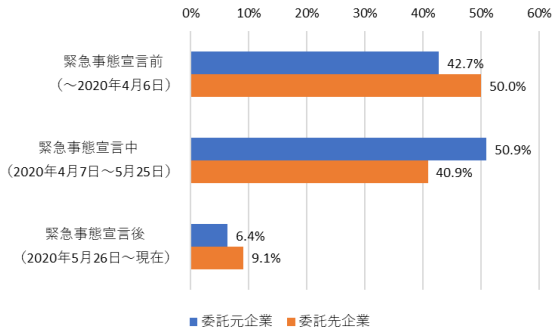

図 2：テレワークの開始時期

(3) テレワークの実施状況（実施の割合，頻度）

「企業・組織調査」では，テレワークの経験がある回答者に対して，平均的な全社員に占めるテレワーク実施社員の割合，および，テレワークを実施している社員の実施頻度について質問をしている．これらの結果をまとめたものが図 3 と図 4 である．図 3 と図 4 を見ても，図 1 や図 2 と同様に，委託元企業と委託先企業の回答者の間で相違があることがわかる．このことから，委託先企業ではテレワークがある程度浸透していることがわかる．

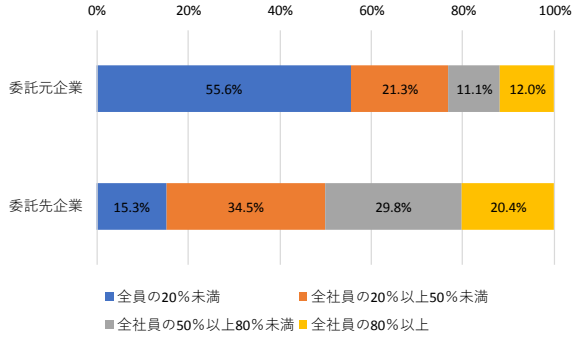

図 3 ：全社員に占めるテレワーク実施社員の割合

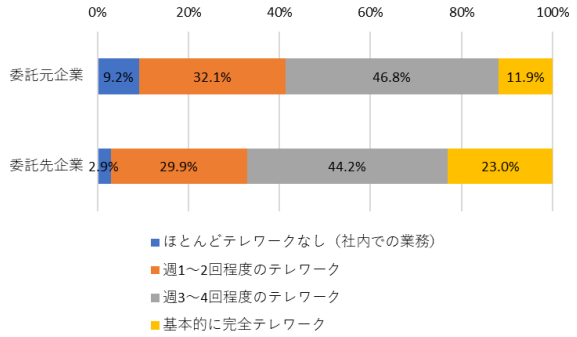

図 4：テレワークを実施している社員の実施頻度

(4) セキュリティ対策の社内規定・規則・手順等の状況

「企業・組織調査」では，緊急事態宣言中またはコロナ禍の影響により特例や例外を認めなければならないセキュリティ対策の社内規定・規則・手順等について質問している．具体的には，「機密情報のクラウドストレージサービスへの保存」「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」などに対して，5 つの選択肢（「a.もともと社内規定・規則・手順等で認めている」「b.一時的にやむを得ず特例や例外を認めたが，その後社内規定・規則・手順を変更した」「c.一時的にやむを得ず特例や例外を認め，現在も認めている」「d.一時的にやむを得ず特例や例外を認めたが，現在は認めていない」「e.特例や例外を認めたことはなく禁止している」）から状況を選択してもらう形式をとっている[d]．この集計結果をまとめたものが表 1 である．

表 1 を見てわかるように，「機密情報のクラウドストレージサービスへの保存」「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」に関して，「社内規定・規則・手順等で認めている」もしくは「特例や例外を認めたことはなく禁止している」を選択している回答者の割合が多い．表 1 の赤枠は，一時的な特例・例外での対応を表している．なお，第 3 節でこの質問項目

d 「企業・組織調査」には，この 2 つ以外にも「機密情報の社外持ち出し（機密情報が含まれる書類・USB メモリ等の電子記録媒体）」などもあるが，本研究ではクラウドサービスならびにシャドーIT についてフォーカスを当てるため，この 2 つを取り上げることにした．

Vol.2021-DPS-188 No.4
Vol.2021-EIP-93 No.4
2021/9/9

表 1：セキュリティ対策の社内規定・規則・手順等の状況

	委託元企業		委託先企業	
	機密情報のクラウドストレージサービスへの保存	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	機密情報のクラウドストレージサービスへの保存	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
もともと社内規定・規則・手順等で**認めている**	34. 26%	18. 52%	45. 45%	26. 18%
一時的にやむを得ず特例や例外を認めたが，その後社内規定・規則・手順を変更した	1. 85%	1. 85%	1. 45%	0. 73%
一時的にやむを得ず特例や例外を認め，現在も認めている	11. 11%	16. 67%	9. 45%	8. 00%
一時的にやむを得ず特例や例外を認めたが，現在は認めていない	3. 70%	1. 85%	1. 45%	1. 82%
特例や例外を認めたことはなく**禁止している**	49. 07%	61. 11%	42. 18%	63. 27%

の中身を詳しく見ていく．

(5) 回答者属性

「企業・組織調査」では，回答者が属している企業・組織の従業員数や業種について質問している．図 5 は従業員規模の分布，また図 6 は業種の分布（左側は委託元企業，右側は委託先企業のものである）を表している．なお，「企業・組織調査」では 27 業種の中から選択してもらっているが，ここでは簡単化したものになっている．

委託元企業は従業員規模が 1001 人以上である回答者が最も多く（35%），委託先企業は 20～49 人である回答者が最も多い（30%）．また，委託元企業で最も多い業種は製造業，委託先企業のそれはソフトウェア業である．

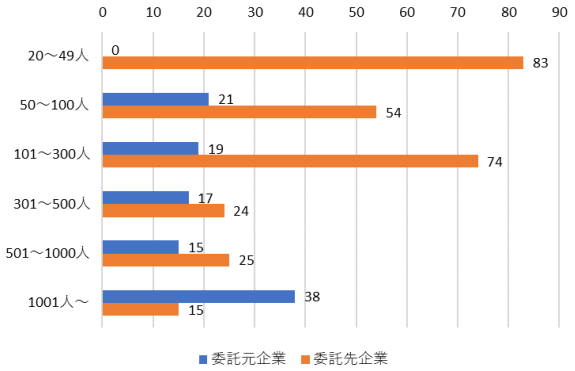

図 5：従業員規模（数字は回答数）

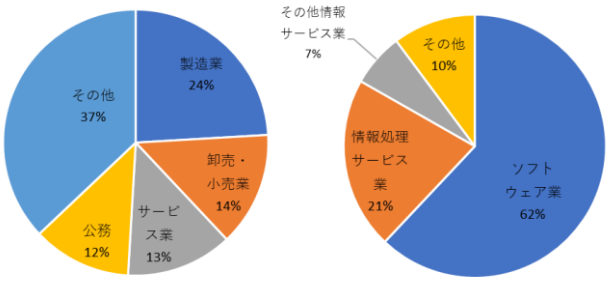

図 6：業種（左：委託元企業，右：委託先企業）

4. フレームワーク

本研究では，「企業・組織調査」によって収集された個票データに対して，多項ロジット回帰モデルを適用し，「機密情報のクラウドストレージサービスへの保存」「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」に関する社内規定・規則・手順等の状況に影響を与える要因の探索を試みる．

以下，概念モデルならびに分析に用いるデータの加工等について簡単に説明を行う．

(1) 概念モデル

本研究では，社内規定・規則・手順等の状況を被説明変数とする，多項ロジット回帰モデルを考える．多項ロジットモデルとは，順序性のないカテゴリデータを被説明変数とするポピュラーな分析手法の一つである．詳しくは文献[12]等を参照されたい．

本研究における被説明変数としては，前節で紹介した「機密情報のクラウドストレージサービスへの保存」「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」に関する社内規定・規則・手順等の状況を用いる．また，これらに影響を与える要因（説明変数）としては，前節で紹介した「テレワークの開始時期」「平均的な全社員に占めるテレワーク実施社員の割合」「テレワークを実施している社員の実施頻度」「従業員規模」と「業種」を用いる．図 7 は概念モデルを表している．

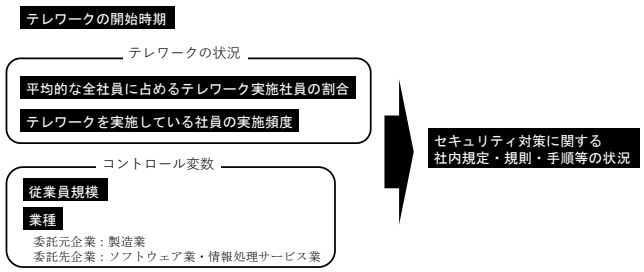

図 7：概念モデル

(2) 社内規定・規則・手順等の状況（被説明変数）

コロナ禍において社会全体で急速なデジタル化が進められたことにより，従来から懸念されていたデジタル化に

おける個人ならびに企業・組織に関する課題の顕在化・深刻化が進み，それらへの対応が急務となった[13,14]．この中でも，テレワークにおけるセキュリティに関する社内規定・規則・手順等について見てみると，これらを一時的であれ，特例・例外を認めて対応した場合，セキュリティの観点からリスクに晒されることとなり，また問題行動を引き起こすことにもなり得る．とりわけ，セキュリティ対策の特例・例外を認め，リスクの低減策が検討されていない状態が常態化することによって，インシデントの発生，被害の拡大を招くことが懸念される[13]. 例えば, テレワークの実施によって組織ネットワークにおける境界線の曖昧化が進み，この曖昧化した境界線の内外で,サイバー攻撃が激化したことも指摘されている[15]. また, 情報漏えいや内部不正等の可能性についても指摘されている[13,16].

本研究では，「機密情報のクラウドストレージサービスへの保存」「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（シャドーIT）の業務利用」に関する社内規定・規則・手順等の状況について考える．

前節で見たように，これらに対して5つの選択肢が与えられている．このまま分析に用いることもできるものの，「一時的にやむを得ず特例や例外を認めたが，その後社内規定・規則・手順を変更した」「一時的にやむを得ず特例や例外を認めたが，現在は認めていない」の回答の割合は表1を見てわかるように小さい．これを考慮して，一時的にやむを得ず特例や例外を認めたというものに関する選択肢を1つにまとめることとする（表1の赤枠の箇所）．そのため，被説明変数は「社内規定・規則・手順等によって許可されている」「全面的に禁止されている」「一時的な特例・例外での対応をする」といった3つの（順序性はない）カテゴリ変数とする．

(3) 影響すると考えられる要因（説明変数）

(2)で見た社内規定・規則・手順等の状況に影響を与える要因として，上述したように,「テレワークの開始時期」「平均的な全社員に占めるテレワーク実施社員の割合」「テレワークを実施している社員の実施頻度」「従業員規模」と「業種」を用いる.「テレワークの開始時期」は 3 カテゴリ,「平均的な全社員に占めるテレワーク実施社員の割合」「テレワークを実施している社員の実施頻度」はともに 4 カテゴリ,「従業員規模」は 6 カテゴリである．なお,「業種」に関しては，委託元企業の分析では「製造業」，委託先企業の分析では「ソフトウェア業」および「情報処理サービス業」をダミー変数として用いる．

本研究では「テレワークの開始時期」をテレワークの着手のスピードを表すものであると解釈している．働き方改革や事業継続計画（BCP）対策の一環として従来からテレワークの導入について議論していた企業も少なからずあった．新型コロナウイルス感染症の拡大に伴いそれを実践していくことになったが，それについて準備が十分できていたか否かを表す要因としてこの質問を採用した．そして，「早くからテレワークを実施している企業ほど, 社内規定・規則・手順等の状況としても一時的なものでなく整備されている」という仮説を立てている．

テレワークといっても様々な形態があり，またそれを社内でどの範囲で実施していくかについても考えて行かなければならない[5]．実際に，前節で見たように，完全なテレワーク（全社員がほぼ毎日テレワークを実施している）は容易ではない．そこで,「テレワークの実施状況が進んでいる企業ほど，社内規定・規則・手順等の状況としても一時的なものでなく整備されている」という仮説を立てている．

この他に，コントロール変数の役割として,「従業員規模」と「業種」ダミーを用いる．ここでは,「従業員規模の差異によって社内規定・規則・手順等の状況も異なる」「業種の差異によって社内規定・規則・手順等の状況も異なる」という仮説も合わせて立てている．

5. 分析

5.1 分析結果

「企業・組織調査」における委託元企業と委託先企業の最終回答者（有効回答者）数は 218 人と 287 人であるが，本研究では，テレワークを経験している回答者（前者の数は 110 人，後者は 275 人）をそれぞれ対象として分析を行う[e]．なお，多項ロジット回帰分析を行う際，ベースアウトカム（基準とする選択肢）を設定する必要があるが，本研究では「一時的な特例・例外での対応をする」をそれにしている．そのため，推計されたパラメータは「一時的な特例・例外での対応をする」という選択肢から見て「社内規定・規則・手順等によって許可されている」（もしくは「全面的に禁止されている」）という選択肢を選ぶ確率を高くすめる（低くする）か否かを調べることができる．

表 2 は委託元企業，表 3 は委託先企業を対象としたもので「機密情報のクラウドストレージサービスへの保存」「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（シャドーIT）の業務利用」を被説明変数とする多項ロジット回帰分析の結果をそれぞれ表している．なお，表中の*は 10%，**は 5%，***は 1%水準で統計的に有意であることを示している．

それぞれの表の見方であるが，例えば表 2 の委託元企業の「シャドーIT の業務利用」の Case2 で説明すると，「社内規定・規則・手順等によって許可されている」においては「開始時期」,「全面的に禁止されている」においては「頻度」が統計的に有意となり，それ以外の要因については統

e なお,「企業・組織調査」の質問項目の一部には，欠損値がある．そのため，分析に用いられるサンプル数はこれらの数字と全て一致するとは限らないことをあらかじめ断っておく．

Vol.2021-DPS-188 No.4
Vol.2021-EIP-93 No.4
2021/9/9

表 2：分析結果 1

		機密情報のクラウドストレージサービスへの保存						シャドーITの業務利用					
		Case 1			Case 2			Case 1			Case 2		
		Coef.	z	p値	Coef.	z	p値	Coef.	z	p値	Coef.	z	p値
社内規定・規則・手順等によって許可されている	従業員数	0.123	0.570	0.568	0.141	0.650	0.513	0.080	0.350	0.729	0.081	0.350	0.728
	開始時期	0.360	0.670	0.501	0.264	0.500	0.616	1.129	1.900	0.058	1.124	1.900	0.057*
	割合	0.838	2.310	0.021**	0.714	2.120	0.034**	0.510	1.540	0.125	0.495	1.570	0.117
	頻度	-0.109	-0.250	0.801	0.032	0.080	0.937	-0.522	-1.080	0.279	-0.509	-1.080	0.280
	製造業D	0.925	1.220	0.223				0.081	0.100	0.921			
	_cons	-1.990	-0.920	0.356	-1.819	-0.850	0.396	-1.924	-0.810	0.418	-1.907	-0.800	0.422
全面的に禁止されている	従業員数	0.198	0.980	0.326	0.203	1.000	0.318	0.131	0.680	0.495	0.133	0.700	0.487
	開始時期	0.322	0.650	0.514	0.304	0.620	0.535	0.597	1.200	0.231	0.578	1.170	0.242
	割合	0.380	1.050	0.295	0.324	0.960	0.339	0.201	0.700	0.484	0.176	0.640	0.520
	頻度	-0.446	-1.100	0.270	-0.395	-1.030	0.302	-0.917	-2.330	0.020**	-0.885	-2.330	0.020**
	製造業D	0.237	0.320	0.748				0.205	0.320	0.749			
	_cons	-0.090	-0.050	0.963	-0.071	-0.040	0.971	1.409	0.720	0.470	1.443	0.740	0.459
Number of Obs.		106			106			106			106		
LR chi 2		LR chi 2(10)=15.37			LR chi 2(8)=13.17			LR chi 2(10)=15.9			LR chi 2(8)=15.79		
Log likelihood		-100.141			-101.240			-91.188			-91.247		
Pseudo R2		0.071			0.061			0.080			0.080		

表 3：分析結果 2

		機密情報のクラウドストレージサービスへの保存									シャドーITの業務利用								
		Case 1			Case 2			Case 3			Case 1			Case 2			Case 3		
		Coef.	z	p値	Coef.	z	p値	Coef.	z	p値	Coef.	z	p値	Coef.	z	p値	Coef.	z	p値
社内規定・規則・手順等によって許可されている	従業員数	0.419	2.340	0.019**	0.431	2.390	0.017**	0.434	2.410	0.016**	0.076	0.440	0.658	0.106	0.620	0.536	0.152	0.920	0.360
	開始時期	-0.801	-2.390	0.017**	-0.862	-2.530	0.012***	-0.865	-2.590	0.01***	-0.340	-0.880	0.379	-0.388	-0.990	0.320	-0.209	-0.560	0.577
	割合	-0.163	-0.750	0.452	-0.170	-0.790	0.428	-0.172	-0.800	0.423	-0.189	-0.760	0.446	-0.194	-0.790	0.429	-0.194	-0.800	0.421
	頻度	0.419	1.610	0.108	0.464	1.760	0.079	0.469	1.780	0.075*	0.721	2.350	0.019**	0.721	2.330	0.02**	0.668	2.200	0.028**
	ソフトウェアD	0.004	0.010	0.994	-0.014	-0.030	0.975				-0.274	-0.430	0.665	-1.046	-1.900	0.057			
	情報処理D	0.178	0.250	0.801							2.050	1.740	0.082*						
	_cons	0.453	0.320	0.747	0.436	0.310	0.754	0.415	0.310	0.757	-0.385	-0.240	0.814	0.375	0.230	0.815	-0.657	-0.440	0.658
全面的に禁止されている	従業員数	0.572	3.150	0.002***	0.600	3.310	0.001***	0.594	3.290	0.001***	0.127	0.820	0.414	0.153	0.970	0.332	0.194	1.280	0.201
	開始時期	0.224	0.660	0.507	0.093	0.280	0.780	0.071	0.220	0.826	-0.040	-0.120	0.908	-0.092	-0.260	0.792	0.079	0.240	0.812
	割合	-0.132	-0.600	0.548	-0.156	-0.720	0.469	-0.156	-0.720	0.469	-0.144	-0.640	0.524	-0.147	-0.660	0.509	-0.145	-0.670	0.506
	頻度	0.195	0.730	0.462	0.219	0.830	0.404	0.226	0.870	0.387	0.464	1.670	0.095	0.473	1.680	0.092*	0.419	1.530	0.127
	ソフトウェアD	1.137	2.010	0.044**	0.125	0.290	0.773				-0.320	-0.560	0.573	-0.968	-1.900	0.058*			
	情報処理D	1.781	2.470	0.014***							1.834	1.620	0.105						
	_cons	-2.302	-1.560	0.119	-1.171	-0.840	0.403	-1.052	-0.780	0.434	0.570	0.390	0.697	1.197	0.830	0.409	0.237	0.180	0.859
Number of Obs.		273			273			273			273			273			273		
LR chi 2		LR chi 2 (12)=52.33			LR chi 2(10)=38.62			LR chi 2(8)=38.36			LR chi 2 (12)=16.92			LR chi 2(10)=12.92			LR chi 2(8)=8.48		
Log likelihood		-240.706			-247.560			-247.688			-229.296			-231.301			-233.518		
Pseudo R2		0.098			0.0724			0.0719			0.036			0.027			0.018		

計的に有意とはなっていない.「社内規定・規則・手順等によって許可されている」における「開始時期」の符号は正であることから，開始時期が遅いほど，一時的な特例・例外での対応をすることよりも社内規定・規則・手順等によって許可されていることが起こりやすくなることがわかる.しかしながら,「全面的に禁止されている」においては「開始時期」の符号が統計的に有意でないことから，開始時期の違いによって一時的な特例・例外での対応をすることと全面的に禁止されていることの起こりやすさには違いがないことがわかる.また,「全面的に禁止されている」における「頻度」の符号は負であることから，テレワークの頻度が高くなるほど，全面的に禁止されていることよりも一時的な特例・例外での対応をすることが起こりやすくなる.一方で, テレワークの頻度の違いによって社内規定・規則・手順等によって許可されていることと一時的な特例・例外での対応をすることの起こりやすさには違いがない．これらのことから,「社内規定・規則・手順等によって許可されている」と「全面的に禁止されている」に対して影響を与える要因は必ずしも一致するとは限らず，また影響の程度も異なることがわかる.

5.2 考察

本研究では，4 つの仮説を立てた．以下,「機密情報のクラウドストレージサービスへの保存」は「クラウドへの保存」,「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（シャドーIT）の業務利用」については「シャドーIT の業務利用」と記す.

・仮説「早くからテレワークを実施している企業ほど，社内規定・規則・手順等の状況としても一時的なものでなく整備されている」

「クラウドへの保存」について，委託先企業では，開始時期が遅いほど「社内規定・規則・手順等によって許可されている」よりも,「一時的な特例・例外での対応をすること」が起こりやすいことがわかった．しかし，委託元企業については開始時期による違いはなかった.「シャドーITの業務利用」については，委託元企業が Case2 の場合にのみ開始時期が遅いほど,「社内規定・規則・手順等によって許可されている」が起こりやすいことがわかった．しかし

委託先企業については開始時期による違いはなかった．
・仮説「テレワークの実施状況が進んでいる企業ほど，社内規定・規則・手順等の状況としても一時的なものでなく整備されている」

「クラウドへの保存」について，委託元企業では，テレワークを実施している従業員の割合が多いほど，「社内規定・規則・手順等によって許可されている」方が，「一時的な特例・例外での対応をすること」よりも起こりやすいことがわかった．委託先企業では，実施状況による違いはなかった．また，「シャドーIT の業務利用」については，委託元企業ではテレワークの実施頻度が多いほど「全面的に禁止」することよりも「一時的な特例・例外での対応」をすることが起こりやすいことがわかった．そして委託先企業では，実施頻度が多いほど「社内規定・規則・手順等によって許可されている」方が，「一時的な特例・例外での対応をすること」よりも起こりやすいことがわかった．
・仮説「従業員規模の差異によって社内規定・規則・手順等の状況も異なる」

委託元企業では，従業員規模の差異による違いはなかった．一方，委託先企業では，「クラウドへの保存」について，「従業員規模」が多くなるほど「一時的な特例・例外での対応をする」ことよりも，「社内規定・規則・手順等によって許可されている」もしくは「全面的に禁止」とすることが起こりやすいことがわかった．しかし，「シャドーIT の業務利用」については委託先企業でも違いはなかった．
・仮説「業種の差異によって内規定・規則・手順等の状況も異なる」

委託元企業では，「業種」の差異による違いはなかった．一方，委託先企業では，「クラウドへの保存」について，ソフトウェア業や情報処理サービス業なるほど，「一時的な特例・例外での対応をする」ことよりも，「全面的に禁止」とすることが起こりやすいことがわかった．

6. おわりに

緊急事態宣言直後に急速に進んだテレワーク導入は，事業継続が優先され，セキュリティ対策の検討や実施が十分されていないことが懸念された．IPA の調査により，一部の企業・組織では一時的な特例・例外を認め，それが，緊急事態宣言から半年後経過したのちもまだ継続されていることがわかった．本研究では，一時的な特例・例外を認める要因を企業・組織の特徴から分析した．分析の結果，「機密情報のクラウドストレージサービスへの保存」「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」について，従業員数，テレワークの開始時期，実施率，頻度，業種など，社内規定・規則・手順等を整備するか，一時的な特例・例外を認めるかに影響することがあることがわかった．

調査から半年以上経過し，コロナ禍の期間の長期化とともに企業・組織の状況にも変化が予想される．一時的な特例・例外がその後見直され，適切なセキュリティ対策が施されたのか等，継続的な調査実施について検討をしたい．

参考文献

[1] 総務省, 令和 2 年通信利用動向調査の結果, 2020 年＜https://www.soumu.go.jp/johotsusintokei/statistics/data/210618_1.pdf＞(参照 2021-08-12)
[2] 総務省, テレワークセキュリティガイドライン第 4 版, 2018 年＜https://www.soumu.go.jp/main_content/000545372.pdf＞(参照 2021-08-12)
[3] 厚生労働省, テレワークの適切な導入及び実施の推進のためのガイドライン, 2019 年＜ https://www.mhlw.go.jp/content/000759469.pdf＞(参照 2021-08-12)
[4] 厚生労働省, 自営型テレワークの適正な実施のためのガイドライン, 2018 年＜https://homeworkers.mhlw.go.jp/guideline/＞(参照 2021-08-12)
[5] 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 年＜https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html＞(参照 2021-08-12)
[6] Takemura, T., Komatsu, A., Empirical Study on Information Security Behaviors and Awareness, The Economics of Information Security and Privacy, Springer, 95-114, 2013.
[7] 竹村敏彦・三好祐輔・花村健一, 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, 56(12), 2191-2199, 2015 年.
[8] 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, 58(12), 1912-1935, 2017 年.
[9] 村﨑康博・稲葉緑・原田要之助, 情報セキュリティポリシーにおける例外措置の利用者による実施阻害要因および対応に関する一考察, 研究報告セキュリティ心理学とトラスト（SPT）, 2018-SPT-30(1), 1-8, 2018 年.
[10] 森淳子・小山明美・小川隆一・竹村敏彦, テレワークにおけるセキュリティ等への不安に関する分析～ニューノーマルに向けた示唆～, マルチメディア, 分散, 協調とモバイル(DICOMO2021)シンポジウム, 7G-2
[11] 情報処理推進機構, テレワークの実施における不安に関する調査結果（個人編 中間報告）, 2021 年＜https://www.ipa.go.jp/security/fy2020/reports/scrm/index.html＞(参照 2021-08-12)
[12] Hosmer, D.W., Lemeshow, S., Sturdivant, R.X., Applied Logistic Regression (Wiley Series in Probability and Statistics): Third Edition, Wiley, 2013.
[13] 情報処理推進機構, 情報セキュリティ白書 2021, 情報処理推進機構, 2021 年＜https://www.ipa.go.jp/security/publications/hakusyo/2021.html＞参照 2021-08-12)
[14] 総務省, 令和 3 年版情報通信白書, 2021 年＜https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/index.html＞(参照 2021-08-12)
[15] トレンドマイクロ, 2020 年年間セキュリティラウンドアップ, 2021 年＜https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20210318-01.html＞(参照 2021-08-12)
[16] 三菱総合研究所, ポストコロナ時代の情報セキュリティー, マンスリーレビュー, 2020 年 6 月号, 2020 年＜https://www.mri.co.jp/knowledge/mreview/202006-4.html＞(参照 2021-08-12)