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

調査報告書

2021年4月発行

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

改版履歴

年月日	内容
2021 年 4 月 7 日	発行

目次

付録資料

- アンケート調査票
  - I. 個人調査
  - II. 組織調査
- アンケート調査単純集計結果
  - I. 個人調査
  - II. 組織調査

空白ページ

1 はじめに

1.1 調査背景・目的

2020 年 4 月、特別措置法に基づき我が国史上初の緊急事態宣言[1]が出され、約 2 か月間に及ぶ外出自粛が実施された。長期間の外出自粛の中でも事業を継続させるため、職場以外の環境での「テレワーク(在宅勤務、モバイル勤務、サテライトオフィス勤務)」やインターネットを介してのコミュニケーション（オンライン会議、オンライン面接）に取り組む組織が多かった。このような新しいワークスタイルや IT の活用方法は、ニューノーマルと言われ、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・パラ、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である。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ることからも、今後このような新しいワークスタイルや IT の活用方法は継続する可能性が高い。一方、これらの対策実施のために行われた急速な ICT 環境の整備は、業務継続を優先した為、セキュリティ対策については利用者個人にまかされてしまっていることも多く、十分とは言えない。ニューノーマルでも安全に事業を継続するためにはルール作り、端末・ネットワークのセキュリティ対策等を利用と並行して進めざるを得ない。

独立行政法人情報処理推進機構（IPA）では、これまで IT システム・サービスの業務委託（以下、IT サプライチェーン）におけるセキュリティの責任範囲の調査を行ってきたが、ニューノーマルにより ICT 環境は大きく変化しており、作業場所や情報の持ち出し、使用する機器等についてセキュリティ要件の見直しや日常の管理方法を考慮する必要があると考えられる。

そこで、本調査においては、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調査を実施した。

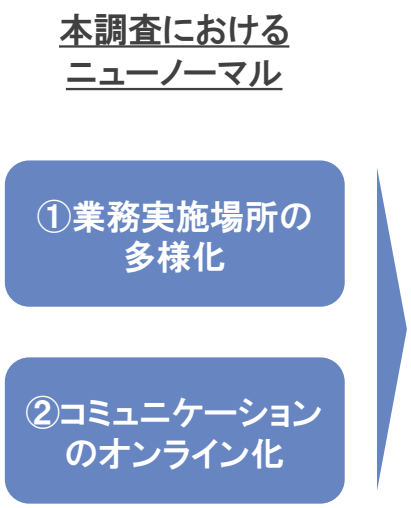
[1] 本報告書にて記載のある「緊急事態宣言」は、特段の補足説明がない限り第一回目（2020 年 4 月 7 日～5 月 25 日）の緊急事態宣言を指す

1.2 調査実施における前提

【ニューノーマルの整理】

本調査においては、「ニューノーマル」の対象として①業務実施場所の多様化、②コミュニケーションのオンライン化の 2 点を想定の上、ニューノーマルへの対応によって生じる ICT 環境を含めた IT サプライチェーンを担う組織の変化と、当該組織の活動を構成する個人（従業員、派遣者、外部委託先要員等）の変化を抽出・整理した（**エラー! 参照元が見つかりません。**）。これらの変化から想定しうる IT サプライチェーン上の情報セキュリティリスクに与える影響を本調査の対象範囲として調査設計を行っている。

図 1-1：ニューノーマルの整理概要



ニューノーマルの変化の例	
組織	急速なテレワーク・ファーストへの移行
	ニューカマーの台頭 （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・ソフトウェアの開発受委託）
	受委託契約の変化
	セキュリティ・リテラシー教育の内容の高度化 （機密情報の社外持ち出し頻度の増加、利用ツール・デバイスの増加）
	従業員の利用端末の変化 （BYODの増加、タブレット端末等の利用増、社内ネットワーク外で使用される端末の増加）
組織を構成する個人	多様な働き方の増加 （時差勤務・育休産休・テレワーカーとオフィス勤務者の混在）
	情報／書類の社外持ち出し
	社内に比べ物理的なセキュリティの低い場所での勤務 （カフェテリア等公衆の場所、サテライトオフィス、自宅）
	使用する機器、サービスの変化
	ITツールの利用の増加（オンライン会議・メール・チャット・アップローダー・クラウドサービス等）

※赤字はICT環境変化

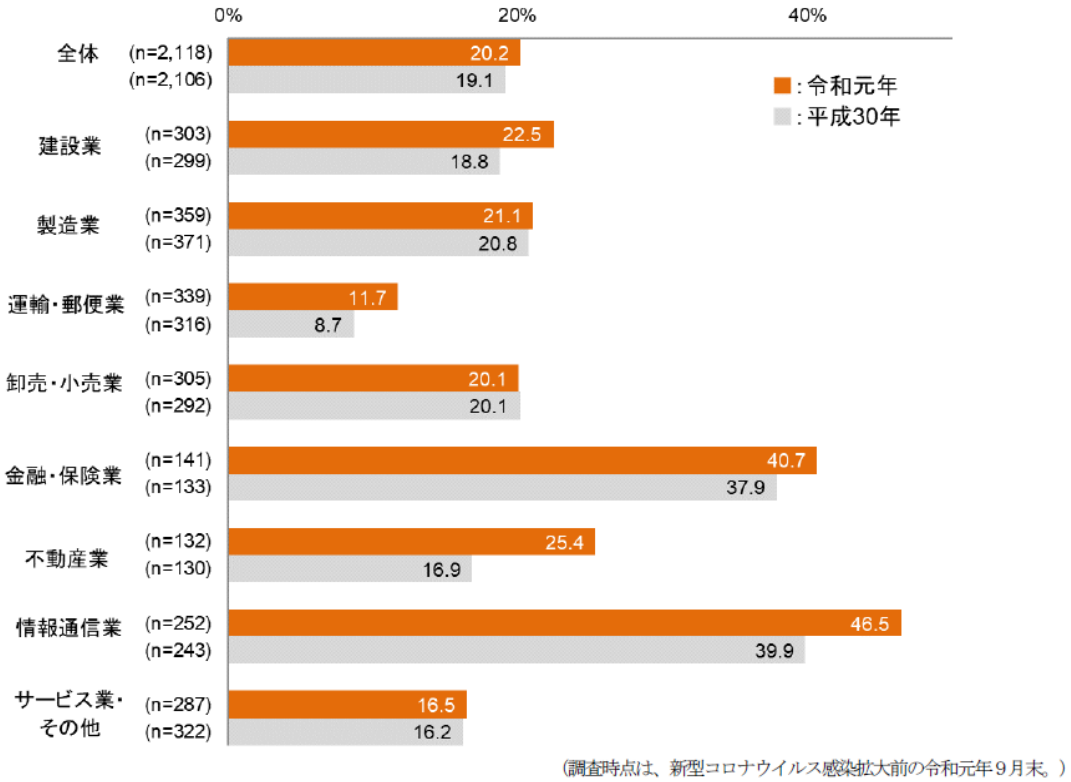
【テレワーク導入状況について】

2019 年の「通信利用動向調査[2]」（総務省）によると、2019 年 9 月末時点において「テレワークを導入している」と回答した割合は全体で約 2 割、情報通信業においては 5 割近くに上っており（図 1-2）、一定数の組織においてはコロナ禍以前から新たな勤務形態として着実に浸透してきていたと言えよう。

---

[2] 総務省「令和元年通信利用動向調査」
https://www.soumu.go.jp/johotsusintokei/statistics/data/200529_1.pdf

図 1-2：産業別テレワークの導入状況



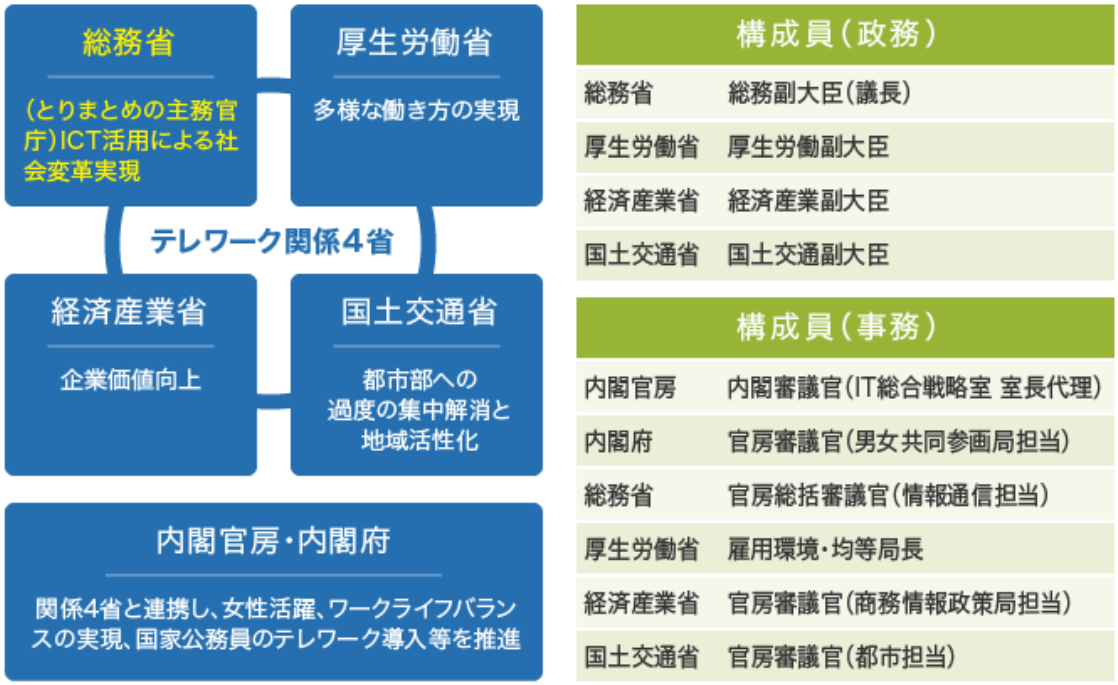
出典：「2019 年通信利用動向調査」（総務省）より抜粋

テレワークは、ワーク・ライフ・バランスの実現、人口減少時代における労働力人口の確保、地域の活性化、非常時における業務継続の確保など、種々の課題に有効と考えられていることから、コロナ禍以前より関係府省が連携し、その普及・推進を図られていた。具体的には、内閣官房長官指示により 2016 年 7 月から関係府省連絡会議を開催し、テレワーク推進に向けた各府省の取組の共有や連携施策の検討・推進がなされており、関係府省が連携して取り組みを進めていた状況にある（図 1-3）。テレワークの推進にあたっては、その導入支援を目的とした情報提供手段として、総務省から「テレワーク総合情報サイト」[3]が、厚生労働省からは「テレワーク総合ポータルサイト」[4]が開設されており、それぞれテレワークの導入事例やテレワーク導入にあたって活用可能な支援策等が示されている。また、テレワーク導入の際のガイドラインとして、総務省からは組織等がテレワークを実施する際の情報セキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針とし

[3] 総務省「テレワーク総合情報サイト」https://telework.soumu.go.jp/
[4] 厚生労働省「テレワーク総合ポータルサイト」https://telework.mhlw.go.jp/

て「テレワークセキュリティガイドライン　第 4 版[5]」（2018 年 4 月）が、厚生労働省からは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」（2019 年 9 月）や自営型テレワーク[6]の適切な実施に向けた「自営型テレワークの適切な実施のためのガイドライン」（2018 年 2 月）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た。

図 1-3：テレワーク関係府省連絡会議



出典：厚生労働省「テレワーク総合ポータルサイト」より抜粋

しかしながら、新型コロナウイルス感染症の拡大により、感染拡大防止と業務継続を両立する必然性から、これまでの勤務形態を継続する想定でいた組織においても、テレワークの導入・定着は喫緊の課題になったといえよう。「新型コロナウイルス感染症緊急経済対策」（2020 年 4 月 7 日閣議決定）や 2020 年度第一次・二次補正予算では、税制措置としてテレ

[5] 総務省「テレワークセキュリティガイドライン　第 4 版」
https://www.soumu.go.jp/main_content/000545372.pdf

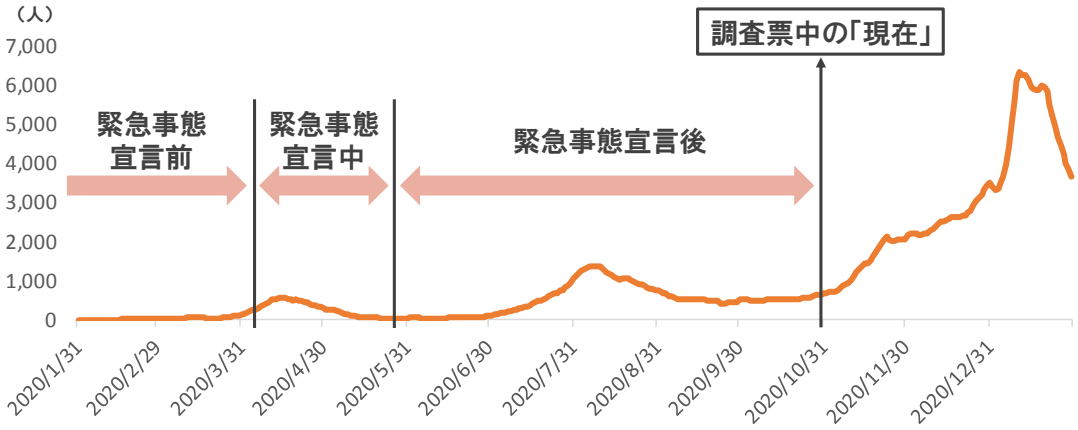
[6] 自営型テレワークとは、「注文者から委託を受け、情報通信機器を活用して、主として自宅又は自宅に準じた自ら選択した場所において、成果物の作成又は役務の提供を行う就労」のこと

ワーク等のための設備投資が中小企業経営強化税制の対象とされた[7]ほか、経済産業省、総務省、厚生労働省からテレワーク促進のため助成金等、各種予算措置が取られることとなり、テレワーク導入対象組織の裾野は格段に広がっている状況にある。

【調査対象時期・期間の前提】

本調査では、IT サプライチェーンにおける状況の中からコロナ禍がもたらした変化をより明確に把握するために、一部の調査項目については緊急事態宣言前（～2020 年 4 月 6 日）、緊急事態宣言中（2020 年 4 月 7 日～5 月 25 日）、緊急事態宣言後（2020 年 5 月 26 日～10 月 31 日）、それぞれの期間の状況を問う形としている。また、調査回答者の回答時期の差異による回答内容のブレを防止するため、アンケートに回答する際の前提として、設問中の「現在」は 2020 年 10 月 31 日時点を指す旨を明示している。ちなみに、この 2020 年 10 月 31 日は、緊急事態宣言の解除後、再度新型コロナウイルスの感染者数が増加したいわゆる第 2 波の終焉後に相当し、個人・組織ともにこれまでのニューノーマルへの対応や今後の方針についてある程度考慮する余裕のある時期との仮定の基で設定したものである（図 1-4）。

図 1-4：我が国新型コロナウイルス陽性者数推移（週次平均）と
本調査設問での設定期間



出典：厚生労働省公表データより NTT データ経営研究所作成

1.3 調査に際しての仮説

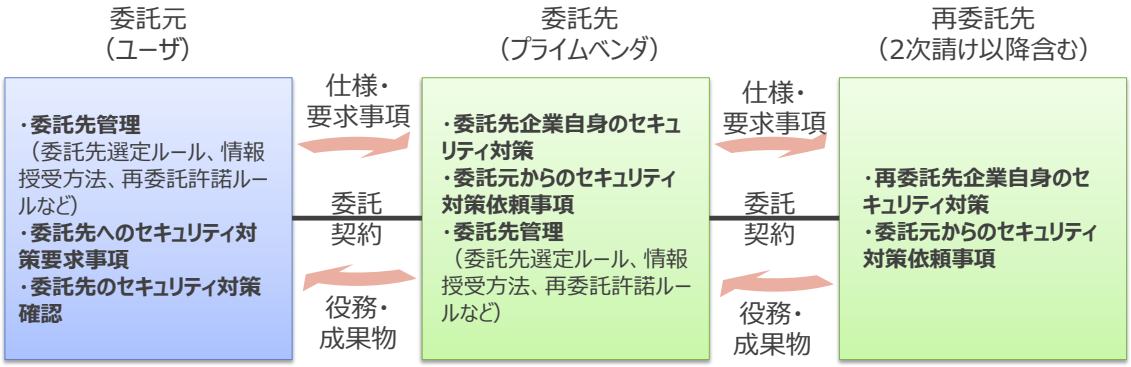
本調査においては、「IT システム・サービスに関する業務を系列組織やビジネスパートナー等に外部委託し、 その業務委託が、委託先企業・組織の再委託先、再々委託先へと連鎖する委託形態」 を「IT サプライチェーン」と定義している（図 1-5）。IT サプライチェーン

[7] テレワーク等のための中小企業の設備投資税制のリーフレット
https://www.nta.go.jp/taxes/shiraberu/kansensho/keizaitaisaku/pdf/keizaitaisaku_1.pdf

のセキュリティを確保するための委託元の役割は、委託先管理や委託先へのセキュリティ対策の要求事項の策定、委託先のセキュリティ対策の確認である。また、委託先の役割は、自身のセキュリティ対策（委託元からの依頼を含む）の実施や再委託先の管理である。そして、再委託先の役割は、自身のセキュリティ対策（委託元からの依頼を含む）の実施である。

以降、本報告書中にある「委託元企業・組織」（以下、委託元）とは IT システム・サービスの開発・提供を委託する組織を指し、「委託先企業・組織」（以下、委託先）とは委託元から IT システム・サービスに関する業務を受託する組織を指す。

図 1-5：IT サプライチェーンのイメージ



本調査では、ニューノーマルへの対応に伴い、自組織のみならず、取引先（委託先や再委託先、もしくは委託元）における情報セキュリティリスクが高まっているのではないか、そのため、情報セキュリティを確保する上では IT サプライチェーン全体を見据えた対策が必要であるが、現時点においては委託元/委託先共にそれらへの対応が不十分なのではないかとの問題意識を発端とし、調査設計を行っている。このような組織における現状の課題を整理するため、調査に際しては IT サプライチェーンの起点となる委託元と委託先（プライムベンダ）との関係にフォーカスした上で、以下の仮説（図 1-6）を設定し、アンケートやインタビューを用いて実態を調査した。

図 1-6 本調査の仮説一覧

報告書記載箇所	仮説	
2.1 章	仮説 1：セキュリティガバナンス/コンプライアンスの低下	
	仮説 1-1	業務優先でテレワークへ急速に移行したことで、セキュリティガバナンス/コンプライアンスの水準が低下し、元に戻すことが厳しい組織が多いのではないか
	仮説 1-2	ニューノーマルによって事業経営の環境が大きく変化することにより、セキュリティガバナンス/コンプライアンスが低下した組織が多いのではないか
2.2 章	仮説 2：ルール・運用、マネジメント力の低下	
	仮説 2-1	組織の現状の規定やルールだけでは、環境に大きな変化が生じるニューノーマルのセキュリティ対策・管理は不十分と感じている人が多いのではないか
2.3 章	仮説 3：今後想定されるセキュリティ脅威や情報セキュリティリスク（セキュリティインシデントの増加を含む）	
	仮説 3-1	テレワークへの急速な移行に伴い、取引先に影響を及ぼしうる内部不正（秘密の不正持ち出し、シャドーIT[8]利用等）が増えるのではないか
	仮説 3-2	習熟していないウェブ会議ツールの活用方法の誤り等により、使用者が気付かないうちに情報が漏えいする情報セキュリティリスクが高まっているのではないか
	仮説 3-3	業務の自動化・無人化や、職員等が孤立して仕事をしているために、セキュリティインシデント発生時の迅速・適切な対応が難しくなっているのではないか
	仮説 3-4	未知の脆弱性に伴うセキュリティインシデントが増加し情報漏えい、サービス停止、マルコード不正組み入れ等のセキュリティインシデントが増えるのではないか
	仮説 3-5	訪問や移動を必要としない取引を望む組織が増え、新たなセキュリティ脅威や情報セキュリティリスクが顕在化するのではないか
2.4 章	仮説 4：組織と従業員の責任分界点	

[8] シャドーIT：組織側が把握せずに従業員または部門が業務に利用しているデバイス機器やクラウドサービスなどを指す

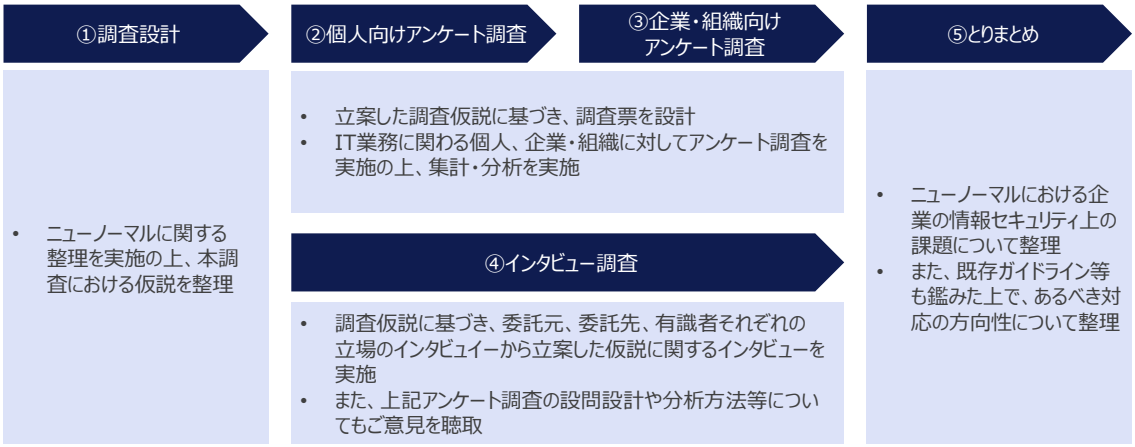
報告書記載箇所	仮説	
	仮説 4-1	BYOD[9]でテレワークをした場合のセキュリティ対策が個人任せになっている為セキュリティインシデントが起きないか不安を感じているのではないか
	仮説 4-2	BYOD でセキュリティインシデントが発生してもフォレンジックなどの調査ができないのではないか
2.5 章	仮説 5：委託先選定、再委託先許諾への影響	
	仮説 5-1	テレワークの実施の可否、テレワーク実施時のセキュリティ対策内容が業務委託先選定の条件となるのではないか
	仮説 5-2	委託先として、事業収益が最優先で、セキュリティガバナンス/コンプライアンスの意識が低いニューカマーが増えているのではないか
2.6 章	仮説 6：委託先へのセキュリティ対策要求等の変化	
	仮説 6-1	ニューノーマルへの対応に向けて、委託元は委託先へのセキュリティ対策やセキュリティ確保に関する証跡提出等の要求を強化することが増えるのではないか

[9] BYOD とは Bring Your Own Device の略で、個人が所有する PC やスマートフォン等の機器・端末を指す。アンケート調査票中の、個人が所有する機器・端末を表す用語については、本報告書内では BYOD との用語で統一した

1.4 本調査の実施概要

本調査では、調査設計タスクで前述の仮説を立案したのち、仮説に基づいたアンケート調査（個人向け、企業・組織向け）と委託元、委託先、有識者に対してのインタビュー調査を実施、その結果を受けとりまとめ作業を実施した（図 1-7）。各タスクの概要は次の通りである。

図 1-7：本調査タスクの流れ



① 調査設計

調査設計を行うにあたり、ニューノーマルの整理を実施したのち、調査仮説を立案した。

【ニューノーマルの整理】

本調査の対象とする新しいワークスタイルや IT 活用方法について規定するため、組織に生じうる変化を抽出した上で、それらの変化が IT サプライチェーンにおける情報セキュリティリスクに与える影響を洗い出した。

【仮説の立案】

ニューノーマルの整理によって抽出した IT サプライチェーンにおける情報セキュリティリスクに与える影響から、ニューノーマルの環境下にある組織の課題仮説を抽出の上、仮説を分類・整理した。

※「ニューノーマルの整理」については「1.2　調査実施における前提」、仮説内容については、「1.3 調査に際しての仮説概要」参照

② 個人向けアンケート調査（以下、個人調査）

IT 企業・組織の従業員／IT 企業・組織以外の IT 担当者が、ICT 環境や働き方の変化、セキュリティの意識や脅威の変化、今後想定される情報セキュリティリスク等についてどのように考えているかの実態把握を行うため、以下の通り調査を実施した。

- 方法：リサーチ会社を利用したウェブアンケート
- 対象：リサーチ会社の登録モニター（国内居住、18 歳以上対象）
- 期間：事前調査：2020 年 11 月 2 日～11 月 13 日
- 有効回答者数：2,372 人
  - IT 企業・組織の従業員・大規模（101 人以上）：717 人
  - IT 企業・組織の従業員・中小規模（100 人以下）：610 人
  - IT 企業・組織以外の組織の IT 部門に所属する IT 担当者・大規模（301 人以上）：526 人
  - IT 企業・組織以外の組織の IT 部門に所属する IT 担当者・中小規模（300 人以下）：519 人

③ 企業・組織向けアンケート調査（以下、組織調査）

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ため、以下の通り調査を実施した。

- 方法：郵送アンケートとウェブアンケートの併用
- 対象：企業・組織データベース等から抽出した組織
  （情報システム・IT 企画関連業務の担当者）
- 期間：2020 年 11 月 18 日～12 月 11 日
- 有効回答者数：505 社
  - 委託先（IT 企業・組織）・総従業員数／職員数 101 人以上の企業・組織・大規模：139 社
  - 委託先（IT 企業・組織）・総従業員数／職員数が 20 人以上 100 人以下の企業・組織・中小規模：148 社
  - 委託元・総従業員数／職員数が 301 人以上の組織・大規模：112 社
  - 委託元・総従業員数／職員数が 50 人以上 300 人以下の組織・中小規模：106 社

④ インタビュー調査

インタビュー調査では、テレワークのセキュリティやサプライチェーンリスクマネジメントの有識者、実践や推進の事例を有する組織の方から今後の取り組みでの留意点、自社の実

践事例、上記アンケート調査の仮説や結果に対する意見等を聴取している。なお、インタビュー調査はオンラインでの会議形式で実施している。(図 1-8)

図 1-8：インタビュー実施概要

#	種別	属性	実施日	目的
1	有識者	セキュリティの専門家	2020 年 10 月 5 日	・仮説・個人調査票作成に向けた意見収集 ・顧客他組織の情報セキュリティ対策の実態聴取
2		IT 企業の経営層	2020 年 12 月 14 日	・仮説・組織調査票作成に向けた意見収集 ・自組織での情報セキュリティ対策実践事例の聴取
3		セキュリティの専門家	2021 年 1 月 22 日	・個人・組織調査の分析結果に対する意見取集 ・情報セキュリティ確保に向けた留意点の聴取
4		セキュリティの専門家	2021 年 1 月 22 日	
5		テレワークの専門家	2021 年 1 月 25 日	
6	委託元	IT 企業	2020 年 10 月 21 日	・仮説・組織調査票作成に向けた意見収集 ・自組織での情報セキュリティ対策実践事例の聴取
7		製造業	2020 年 10 月 27 日	
8	委託先	IT 企業	2020 年 10 月 30 日	
9		IT 企業	2021 年 2 月 16 日	・個人・組織調査の分析結果に対する意見取集 ・業界内での情報セキュリティ対策の実態聴取

⑤ とりまとめ

上記アンケート調査、インタビュー調査の結果を踏まえて、ニューノーマルにおける組織の情報セキュリティ上の課題について整理を実施した。また、それらの課題に対して、既存のガイドライン活用等も含めたあるべき対応の方向性について整理を実施した。

2　調査結果

本章では、図 1-6 に記載した本調査における仮説それぞれに対して、アンケート調査である個人調査・組織調査および、有識者等へのインタビュー調査によって実態を把握し、仮説の有効性を検証した。

2.1 「セキュリティガバナンス/コンプライアンスの低下」について

以下の 2 つの仮説について、調査を実施した。なお、本調査では、「組織がテレワークに対するセキュリティを確保するためのルールを定めずにテレワークを継続している状態」または「組織が、従業員のセキュリティに関するルールの遵守状況を確認できない状態」を「セキュリティガバナンス/コンプライアンスが低下した状態」と定義し、その実態を調査した。

- 仮説 1-1「業務優先でテレワークへ急速に移行したことで、セキュリティガバナンス/コンプライアンスの水準が低下し、元に戻すことが厳しい組織が多いのではないか」
- 仮説 1-2「ニューノーマルによって事業経営の環境が大きく変化することにより、セキュリティガバナンス/コンプライアンスが低下した組織が多いのではないか」

2.1.1 調査結果

【テレワークへの急速な移行】

まず、テレワークの導入の実態を確認したところ、組織調査の結果より、委託先のテレワークの実施割合が約 9 割と、委託元（約 5 割）よりも高いことが明らかになった（図 2-1）。また、テレワークの実施経験がある組織の内、委託先は約 5 割、委託元は約 6 割が緊急事態宣言発出以降にテレワークを導入している（図 2-2）。この結果より、緊急事態宣言をきっかけとしてテレワークへ急速に移行した組織が多いことが分かる。

図 2-1：テレワークの導入状況（組織調査 Q2）

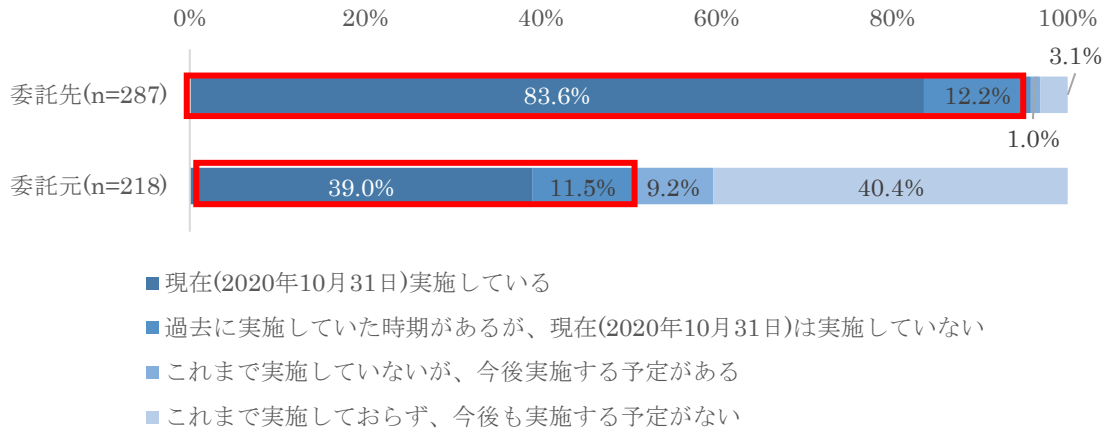
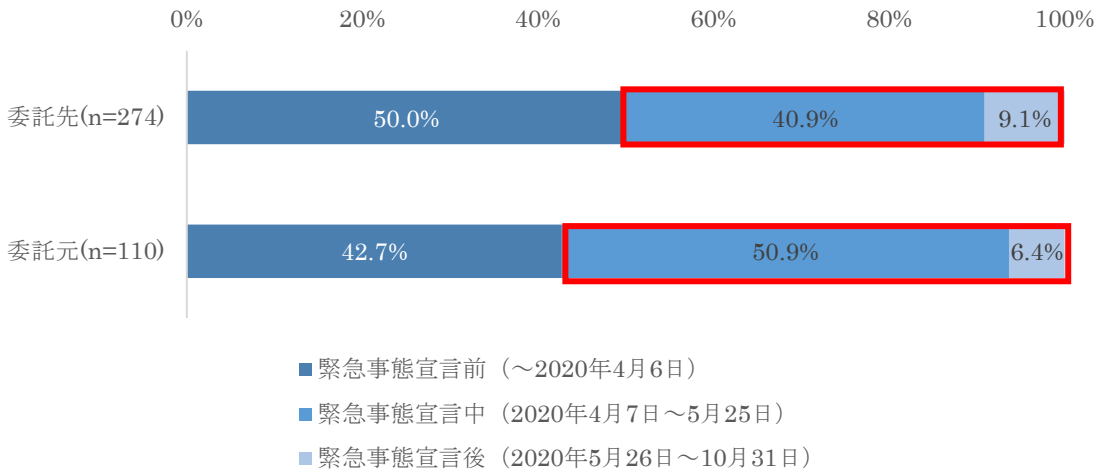
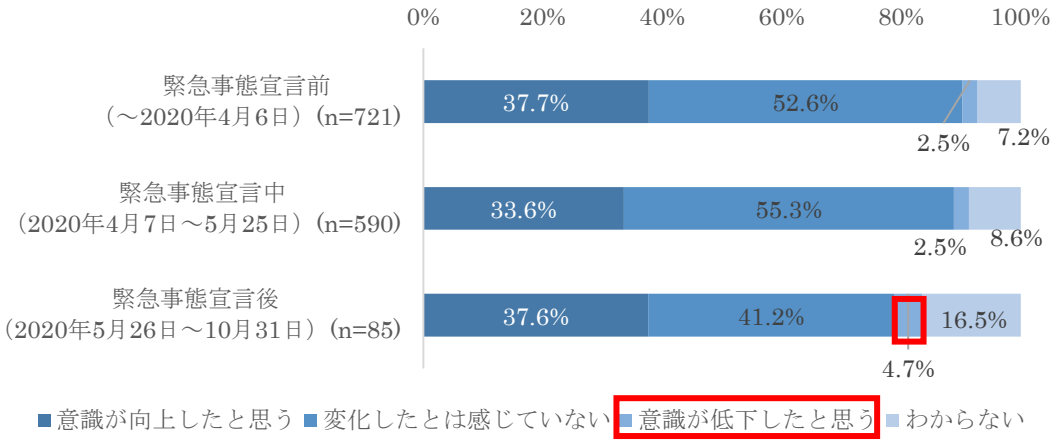


図 2-2：テレワークの導入時期（テレワーク実施経験組織）（組織調査 Q3）



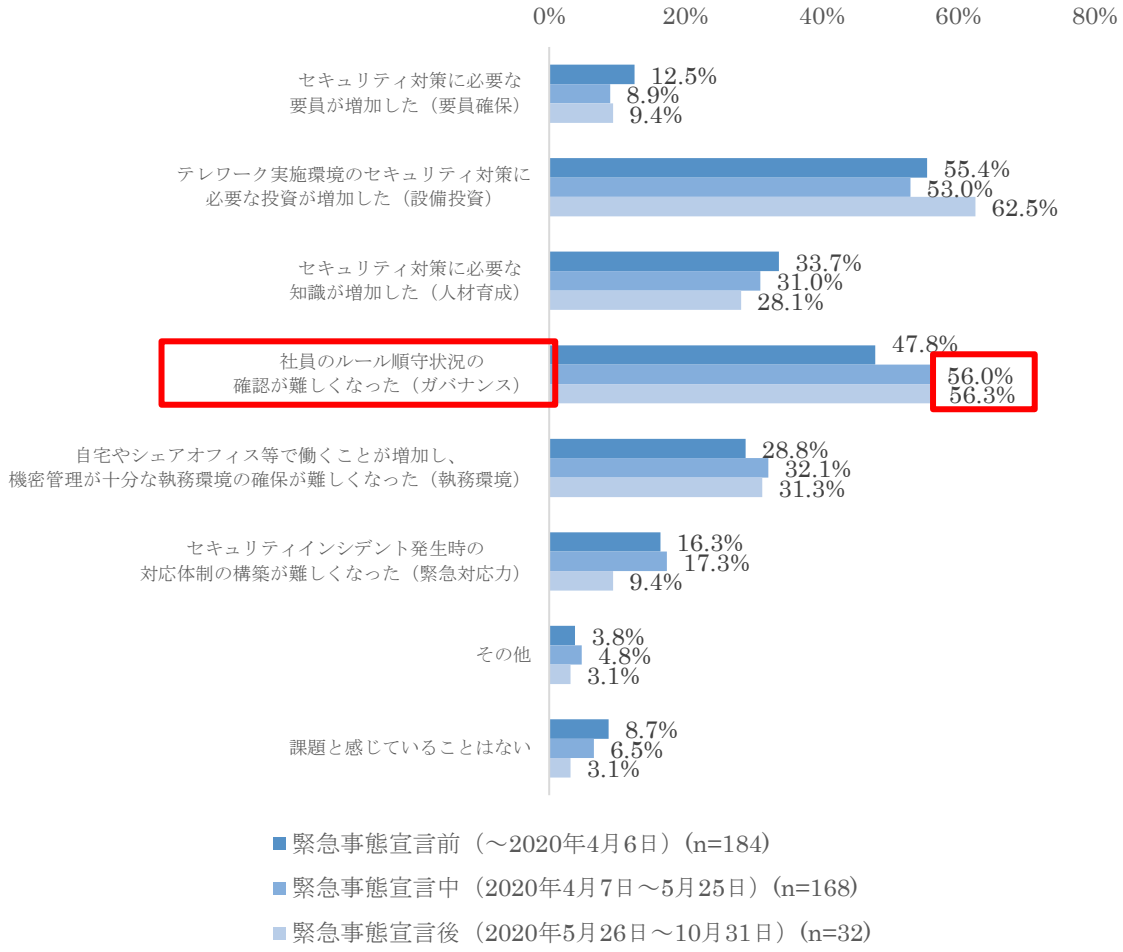
2020 年 4 月 7 日の緊急事態宣言発出以降にテレワークを導入した組織においては、本来セキュリティの観点から望ましくないにも関わらず、業務継続上やむを得ない対応であったことや、準備期間の少なさが影響し、セキュリティガバナンス/コンプライアンスの低下が起こっているのではないかとの仮説 1-1 のもと、その実態を実施した。図 2-3 は、テレワーク導入組織の回答者に対し、「テレワークの導入によるガバナンス/コンプライアンスに対する意識の変化」について問う設問の回答結果である。緊急事態宣言の解除後にテレワークを導入した組織の従業員は、緊急事態宣言前や緊急事態宣言中にテレワークを導入した組織よりも、ガバナンス/コンプライアンスについて「意識が低下したと思う」と回答した割合がやや高くなっている。

図 2-3：テレワークの導入によるガバナンス/コンプライアンスに対する意識の変化（テレワーク導入時期別）（個人調査 Q12）



また、図 2-4 は、テレワークの導入時期別に、「テレワーク実施時のセキュリティ上の課題」について問う設問の回答結果である。この結果より、緊急事態宣言発出以降にテレワークを導入した組織の方が、緊急事態宣言前にテレワークを導入した組織よりも、従業員のルール遵守状況の確認が難しくなったと感じている割合が高い結果となった。

図 2-4：テレワーク実施時のセキュリティ上の課題
（テレワーク導入時期別）（組織調査 Q9）



テレワークを導入した組織において、従業員は自宅等のオフィスとは異なる環境で業務を行うことになる。組織は、従業員のテレワークによるセキュリティインシデントを防ぎ、テレワークの際のセキュリティを確保するために新たなルールを定める必要がある。図 2-5 は、テレワークを導入した組織に対して、テレワークの実施に向けたセキュリティ対策に関するルールの策定時期を、テレワークの導入時期別で分析した結果である。（なお、設問で取り上げたルールの中から、「情報の機密レベル分けに応じたアクセス制御等の情報管理」についての回答結果を抜粋した）。緊急事態宣言中にテレワークに急速に移行した組織

では、緊急事態宣言前からテレワークを導入していた組織と比較して回答時点においてルールを定めていない割合（約 3 割）が高く、ルールが策定されないまま業務を継続しており、これら組織においてはセキュリティガバナンスが低下していることが伺える。また、委託元/委託先の観点で比較をしたところ、大規模の委託先では約 9 割が緊急事態宣言前から「情報の機密レベル分けに応じたアクセス制御等の情報管理」に関するルールを策定している一方で、中小規模の委託元では約 5 割が現時点でもルールを策定していない状況にあることには留意が必要である（図 2-6）。

図 2-5：テレワークのセキュリティ対策の社内規定・規則・手順の策定状況：
情報の機密レベル分けに応じたアクセス制御等の情報管理
（テレワーク導入時期別）（組織調査 Q10）

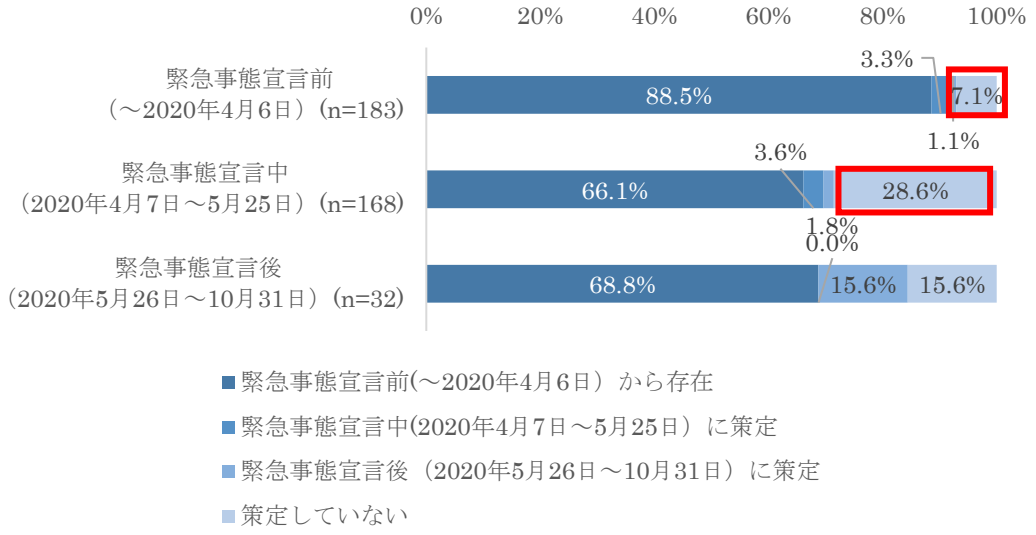
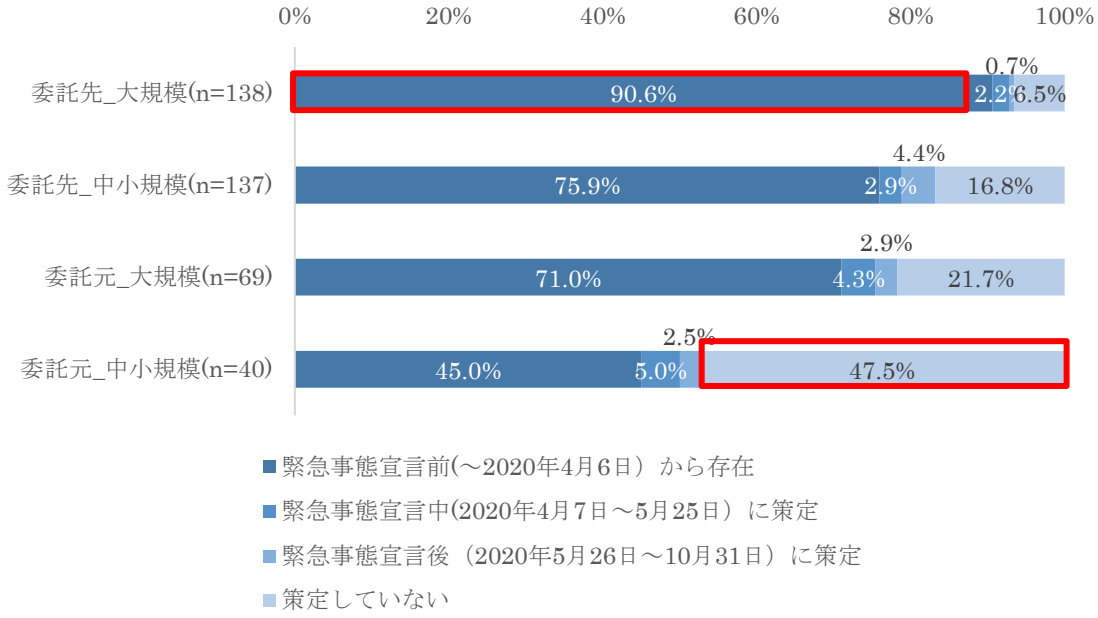


図 2-6：テレワークのセキュリティ対策の社内規定・規則・手順の策定状況：
情報の機密レベル分けに応じたアクセス制御等の情報管理
（規模別）（組織調査 Q10）



さらに、ニューノーマルへの対応に伴う、既存の社内規程・規則・手順等の緩和（特例や例外を認める）の実態を確認したところ（図 2-7）、委託先・委託元ともに、いずれの項目においても約 1～2 割の組織で、一時的にやむを得ず既存の社内規程・規則・手順等の特例や例外を認め、その後も社内規定・規則・手順等を変更せずに特例や例外を認める状態が続いていることが明らかになった。また、委託先と委託元を比較すると、いずれの項目においても委託元の方が委託先よりも既存の社内規定・規則・手順等の緩和状態が継続されている割合が高い。また、特に「BYOD の業務利用」、「機密情報が保存することができる会社支給 PC の持ち出し」の端末に関する社内規定・規則・手順等に関して、継続して特例や例外を認めている組織が 1 割以上存在している。なお、「BYOD の業務利用」、「機密情報が保存することができる会社支給 PC の持ち出し」について、規模別で比較をしたところ（図 2-8）、「BYOD の業務利用」では大規模の委託先・委託元が、「機密情報が保存することができる会社支給 PC の持ち出し」では中小規模の委託元が、他の組織よりも特例や例外を認める状態がある傾向が確認できた。

以上の結果を踏まえ、ニューノーマルへの対応に伴い、一時的にガバナンス/コンプライアンスの水準を低下させたものの、元の水準に戻すことができていない組織が存在していることが伺える。

図 2-7：既存の社内規定・規則・手順等の緩和の実態（組織調査 Q11）

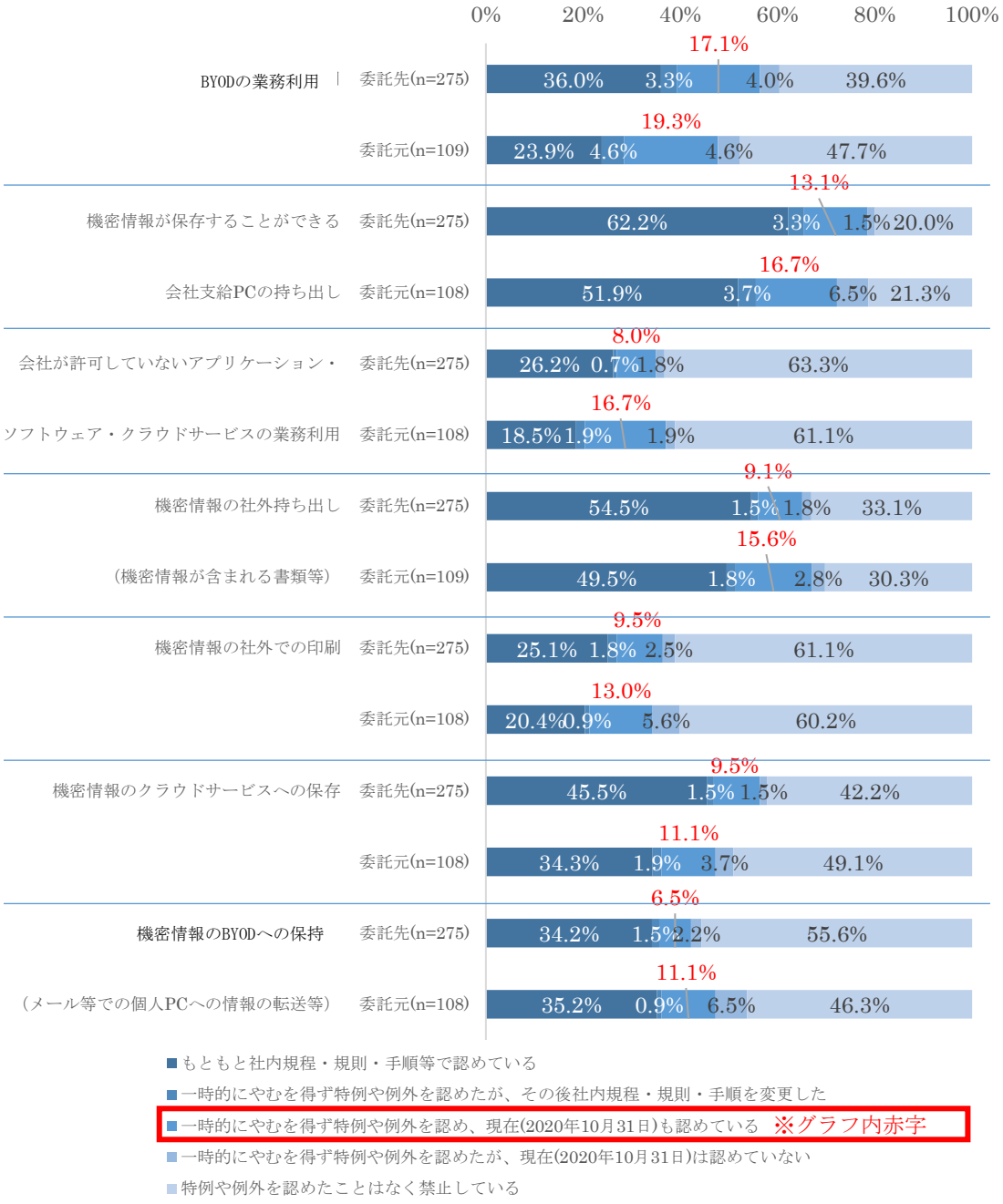
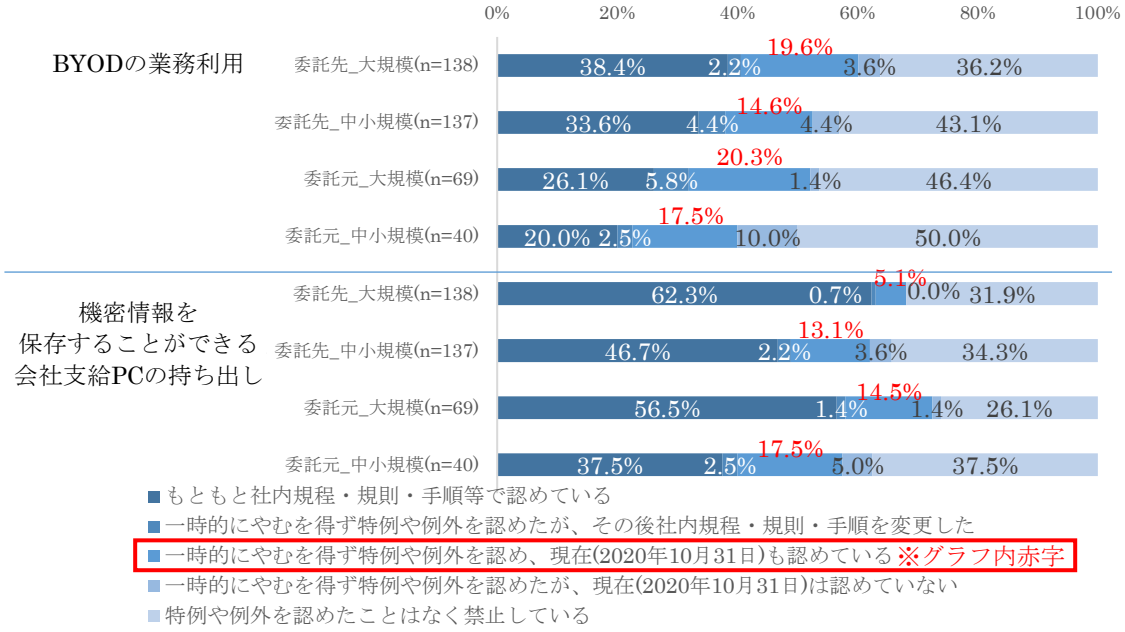


図 2-8：既存の社内規定・規則・手順等の緩和の実態
（「BYOD の業務利用」および「機密情報が保存することができる会社支給 PC の持ち出し」の規模別の分析）（組織調査 Q11）



最後に、テレワークの導入後および緊急事態宣言発出以降に発生したセキュリティインシデント（内部不正含む）の発生の実態を確認した。まず、テレワーク導入後の従業員による内部不正については、委託先は約 8 割、委託元は約 7 割の組織がテレワーク導入前と増減がないと回答する結果になった（図 2-9）。なお、委託先と委託元で比較をすると、委託元の約 2 割（委託先は約 1 割）が内部不正を「把握できていない」と回答している。また、緊急事態宣言発出以降のセキュリティインシデントについても、同様に委託元・委託先共に約 8 割の組織が発生していないと回答する結果となった（図 2-10）。しかしながら、インタビュー調査からは、テレワークへの急速な移行により、組織から従業員に支給する IT 機器（PC やカメラ、マイク等）の調達が間に合わないという事象が発生するとともに、調達が完了するまでの“つなぎ”の期間において、情報セキュリティリスクが高まった認識があるとの意見が得られた。また、テレワーク、BYOD 等の活用によって、勤務状況を全く見られていない中、従業員が無意識の内に情報セキュリティリスクを発生させている可能性があるとの指摘もあった。以上の結果と、前述した約 5 割の組織が従業員のルール遵守状況の確認が難しくなっている（図 2-4）との回答結果を踏まえ、セキュリティインシデントの発生リスクの高まりやその発生実態を明確に認識できていない組織が存在している可能性がある。なお、参考として、テレワークを実施した経験がある組織のうち、緊急事態宣言発出以降にセキュリティインシデントが発生したと回答した組織数を図 2-11 に記す。

図 2-9：テレワーク導入後の情報セキュリティに関する従業員の内部不正
（緊急事態宣言発出以降にテレワークを導入した組織）（組織調査 Q14）

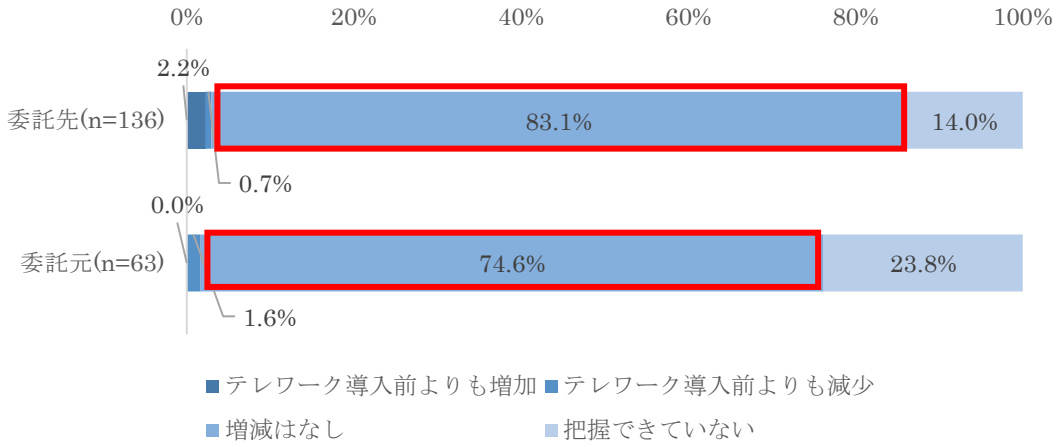


図 2-10：緊急事態宣言発出以降(2020 年 4 月以降)に
発生したセキュリティインシデント
（テレワーク実施経験組織）（組織調査 Q18）

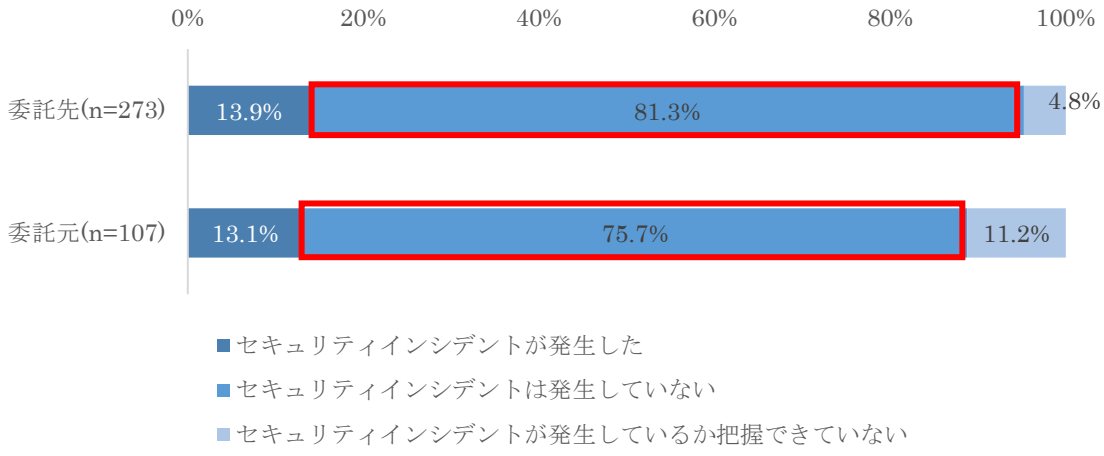


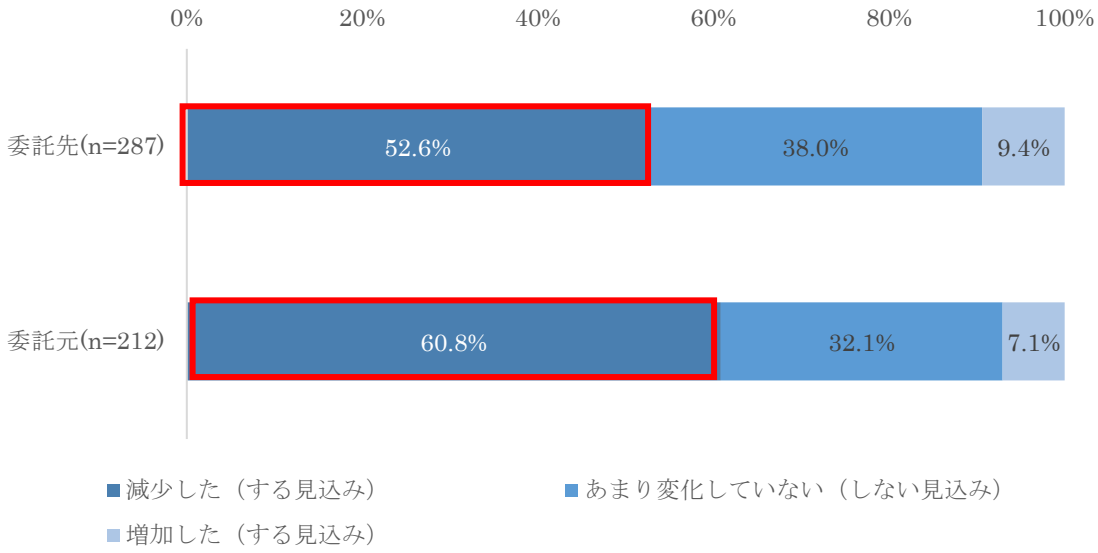
図 2-11：緊急事態宣言後(2020 年 4 月以降)に
セキュリティインシデントが発生したと回答した組織数
（テレワーク実施経験組織、かつ、
セキュリティインシデントが発生したと回答した組織）（組織調査 Q18）

セキュリティインシデント	テレワーク導入時期		
	緊急事態宣言前（～2020 年 4 月 6 日）	緊急事態宣言中（2020 年 4 月 7 日～5 月 25 日）	緊急事態宣言後（2020 年 5 月 26 日～10 月 31 日）
合計回答組織数	42	9	1
テレワークで使用する端末のマルウェア感染	8	2	0
テレワークで使用する端末からの情報漏えい	0	1	0
テレワークで使用する端末の紛失・盗難	7	1	0
自宅ルータのマルウェア感染	0	1	0
自宅ネットワークの盗聴	0	1	0
ウェブ会議ツールのセキュリティ上の問題(脆弱性を悪用した攻撃・情報漏えい等)	1	2	0
クラウド・SNS のセキュリティ上の問題（機密ファイルの流出、風評被害の発生等）	3	0	0
メールの誤送信	28	4	0
紙資料の紛失・盗難	4	0	1
紙資料の不正な持ち出し	1	0	0
その他	7	3	0

【業績悪化】

組織調査において、コロナ禍による業績（売上）の影響を確認したところ、委託先は約 5 割、委託元は約 6 割の組織が、コロナ禍により売上が減少した（する見込み）結果となっている（図 2-12）。

図 2-12：コロナ禍による業績（売上）への影響（組織調査 Q1）



これらコロナ禍により、業績が悪化した組織においては、本来計画していたセキュリティ対策やテレワーク等のニューノーマルにおける情報セキュリティリスクへの対応のための新たなセキュリティ対策のための予算が事業継続のため資金として充てがわれることによって十分なセキュリティ対策が行われず、セキュリティガバナンス/コンプライアンスの低下が起こっているのではないかとの仮説 1-2 のもと、その実態を調査した。緊急事態宣言発出以降にテレワークを導入した組織に対して、コロナ禍による業績への影響の観点で、「テレワーク実施時のセキュリティ上の課題」を確認したところ、業績の悪化と、ガバナンスの低下の明確な関連性は確認することができなかった（図 2-13、図 2-14）。また、インタビューでも、「セキュリティガバナンスと業績が関連するようには考えられない」との意見が得られた。

図 2-13：テレワーク実施時のセキュリティ上の課題
（委託先、業績(売上)変化別、テレワーク実施経験組織）（組織調査 Q9）

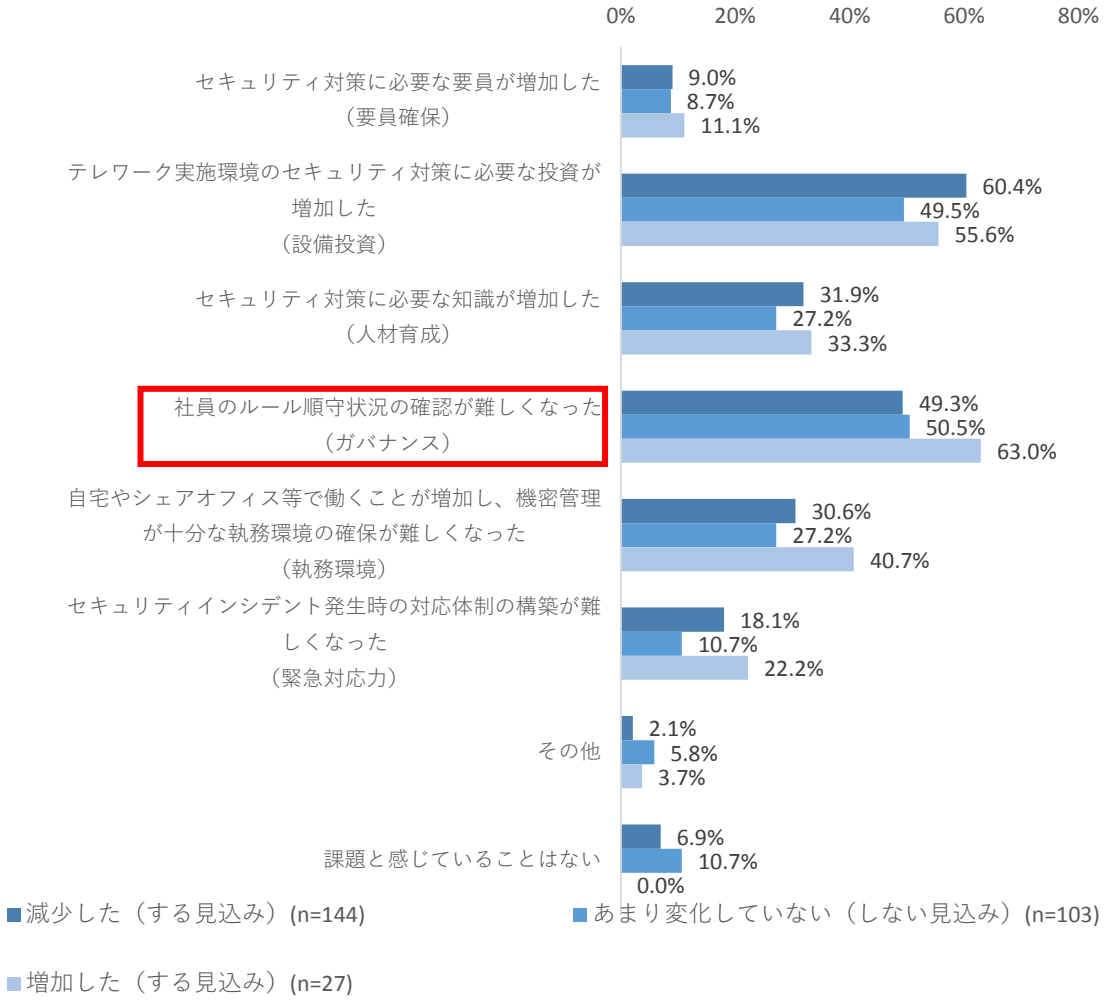
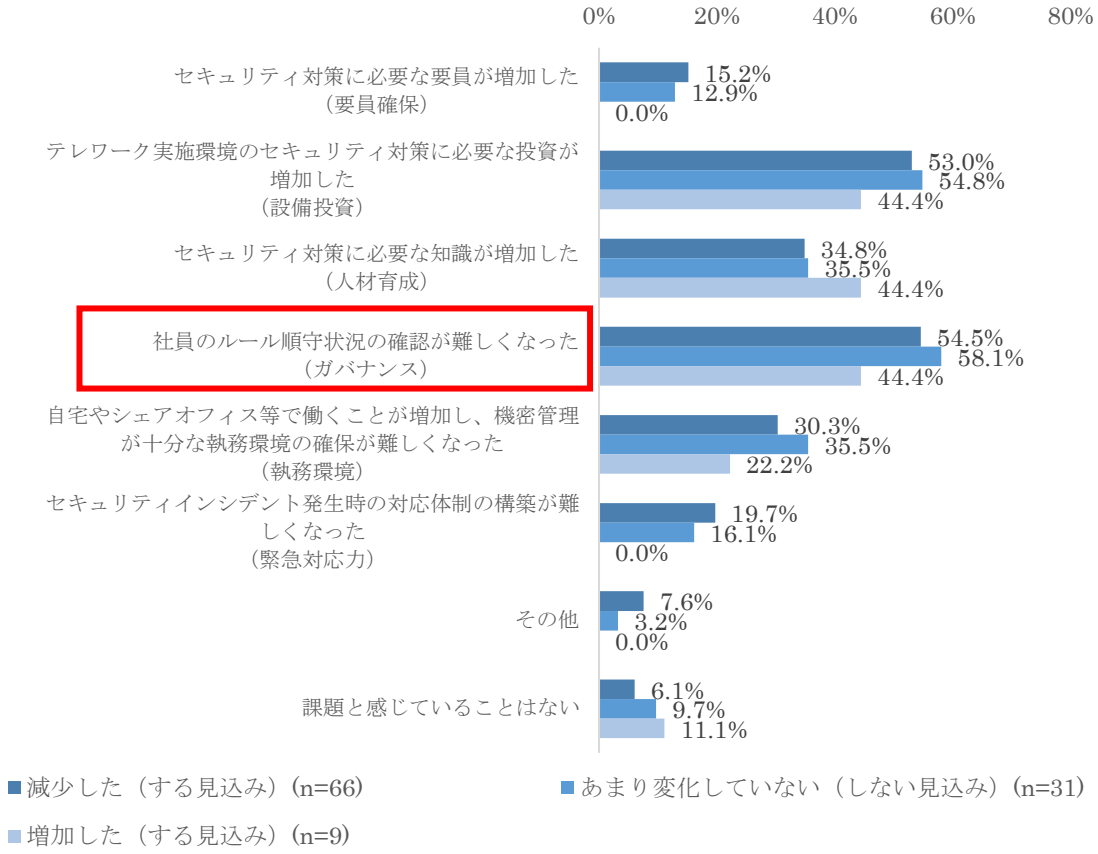


図 2-14：テレワーク実施時のセキュリティ上の課題
（委託元、業績(売上)変化別、テレワーク実施経験組織）（組織調査 Q9）



2.1.2 まとめ（「セキュリティガバナンス/コンプライアンスの低下」について）

本調査結果からは、「テレワークへの急速な移行」によって、組織のセキュリティガバナンス/コンプライアンスの水準が低下し、元の水準に戻すことに苦労している組織が存在していることが確認できた。

まず、組織調査では、緊急事態宣言発出以降にテレワークを導入した組織の約 2-3 割が、テレワークのためのセキュリティ対策に関するルールを定めずに、調査実施時点においてもテレワークを継続していることが明らかになった。また、個人調査からは、緊急事態宣言前にテレワークを導入した組織の従業員よりも、緊急事態宣言発出以降にテレワークを導入した組織の従業員の方が、ガバナンス/コンプライアンスについての意識が低下している傾向が確認できた。なお、インタビュー調査からは、テレワークへの急速な移行により、組織から従業員に支給する IT 機器（PC やカメラ、マイク等）の調達が間に合わないという事象が発生するとともに、調達が完了するまでの“つなぎ”の期間において、情報セキュリティリスクが高まった認識があるとの意見を得ることができている。特に今回のコロナ禍によるテレワークへの急速な移行にともない、移行中もしくは移行直後においては、一時的に情報セキュリティリスクが高まることが示唆される。

また、緊急事態宣言発出以降にテレワークを導入した組織の方が、緊急事態宣言前にテレワークを導入した組織よりも、従業員のルール遵守状況の確認が難しくなったと感じている組織が多いことが明らかになった。さらに、ニューノーマルへの対応に伴い、一時的に既存の社内規定・規則・手順等の特例や例外を認めたものの、その後社内規定・規則・手順等の変更をせずにその緩和状態を継続させており、低下したガバナンス/コンプライアンスの水準を元の水準に戻すことができていない組織が確認できた。なお、インタビューからも「セキュリティガバナンスと業績が関連するようには考えられない」との意見もあり、業績悪化と「ガバナンス/コンプライアンスの低下」の明確な関連性は確認することができなかった。

ニューノーマルが定着し、継続していくことが予測されている昨今の状況下において、情報セキュリティを確保するために、ニューノーマルによる新しい環境に合わせた既存のルールの変更や新しいルールの制定等のセキュリティ水準を安全な水準に保つ取り組みが組織には求められる。

2.2 「ルール・運用、マネジメント力の低下」について

以下の仮説について、調査を実施した。

- 仮説 2-1「組織の現状の規定やルールだけでは、環境に大きな変化が生じるニューノーマルのセキュリティ対策・管理は不十分と感じている人が多いのではないか」

2.2.1 調査結果

組織調査にて、ニューノーマルにおける現状の社内規定やルールの課題について確認したところ、現状の規定等に対して、「曖昧な部分が多い」、「働き方の変化に対応していない」といった課題を抱えている組織が委託元・委託先ともに多いことが明らかになった（図 2-15）。同様に個人調査においても、テレワークを想定したセキュリティの社内規定、ルール、手順等を意識していると回答した従業員に対し、それら社内規定、ルール、手順の課題について確認したところ、組織調査と同様に、「曖昧な部分が多い」が約 4 割と最も高い回答率を示しており、「働き方の変化に対応していない」についても約 2 割の回答率と一定の値を示していることから（図 2-16）、組織の現状の規定やルールだけでは、環境に大きな変化が生じるニューノーマルのセキュリティ対策・管理は不十分と感じている人が多いことが伺える結果となった。

また、「ルールが周知できていない（されていない）」、「従業員の理解が不十分」と回答された割合に着目すると、組織調査では委託元の方が委託先よりも高くなっており（図 2-15）、個人調査でも同様の傾向（IT 企業以外の組織の回答率が高い）を示している（図 2-16）。業種の特性として IT に関する知識が豊富な委託先と比較し、委託元ではそれらの知識が不足していること背景に、委託先よりもルールの周知や従業員の理解が進んでいない可能性も考えられる。

図 2-15：テレワーク実施時の社内規程・規則・手順等の課題
（テレワーク実施経験組織）（組織調査 Q13）

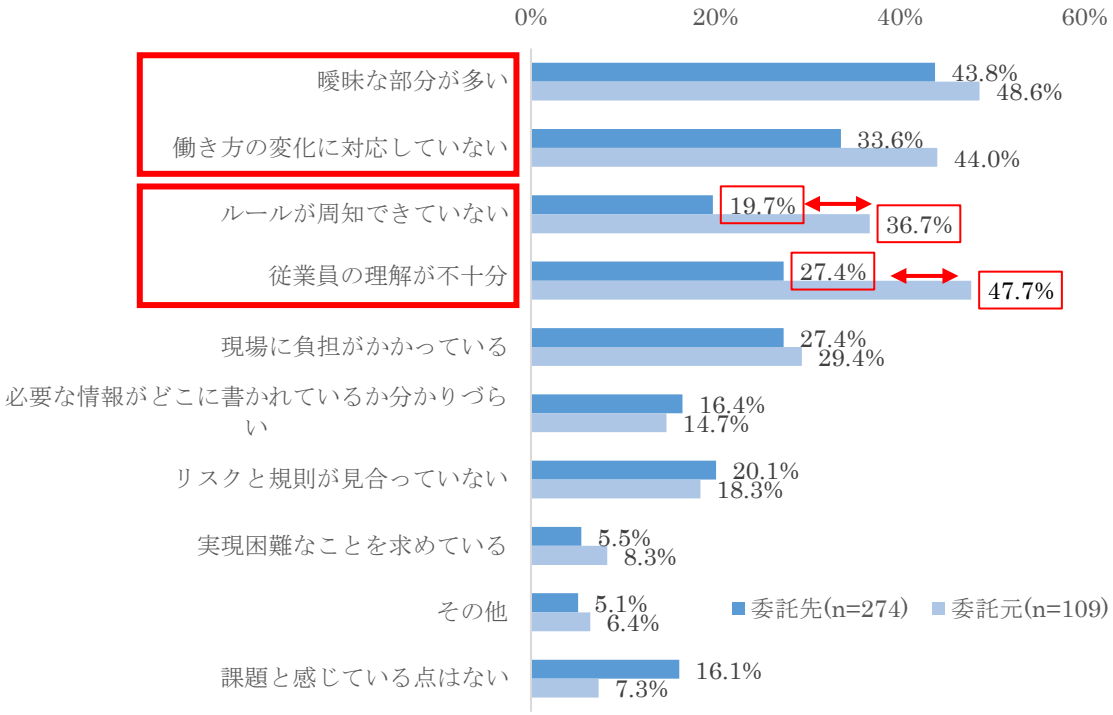
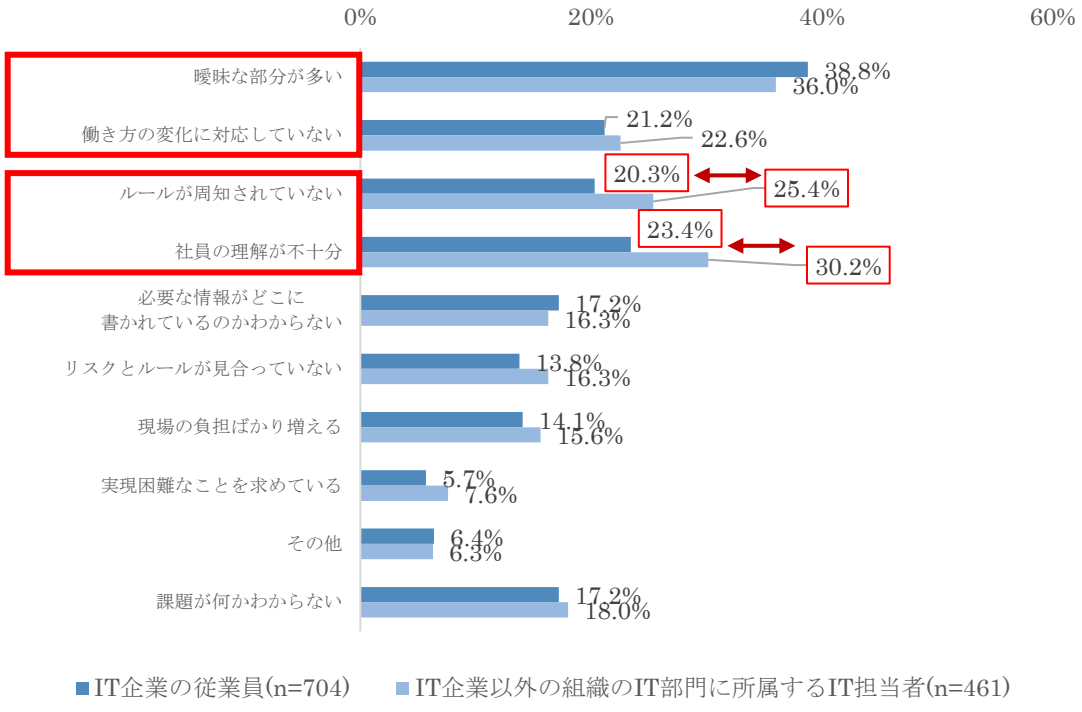


図 2-16：テレワーク実施時の社内規程・規則・手順等の課題（個人調査 Q16）



また、組織調査にて、BYOD の利用状況を確認したところ、業務で BYOD の利用を認めている組織の割合は、PC に関しては、委託先では大規模・中小規模共に約 4 割（大規模委託先の方が 4 ポイント多い）、委託元では大規模が約 3 割、中小規模が約 5 割という結果となった（図 2-17）。また、スマートフォン（タブレット含む）に関しては、委託先では大規模の約 4 割、中小規模の約 5 割、委託元では大規模の約 3 割、中小規模の約 4 割が BYOD の利用を認めているとの結果となった（図 2-18）。

特に、中小規模の委託元では BYOD の PC 利用を、中小規模の委託先では BYOD のスマートフォン（タブレットを含む）利用を他の組織よりも高い割合で認めている傾向がある。一方で、大規模の委託元では、PC・スマートフォン等ともに BYOD の業務利用を認めていない割合が他の組織よりも高い傾向にある。

図 2-17：BYOD（PC）の利用状況（組織調査 Q20）

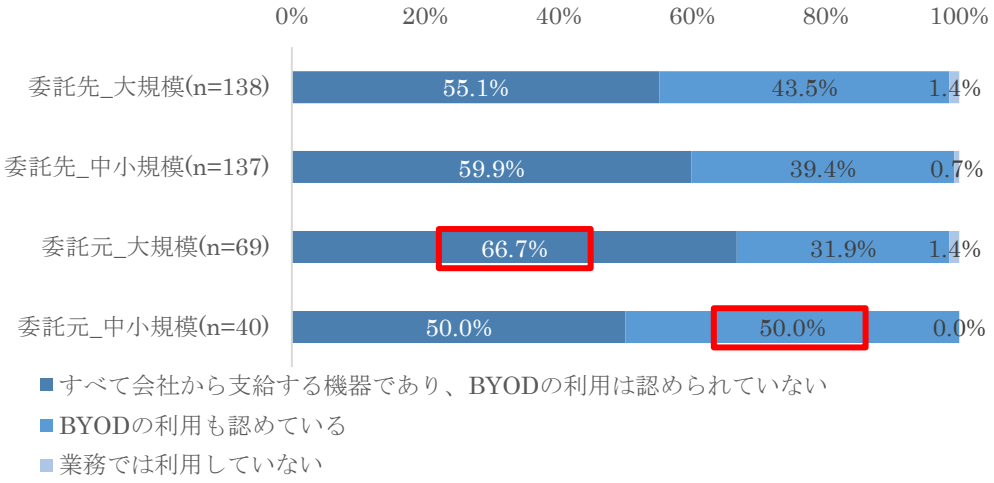
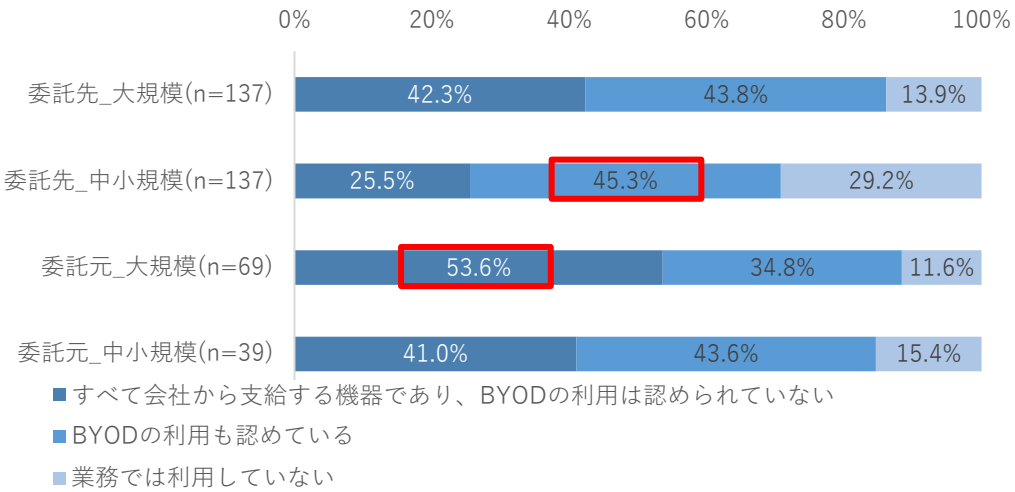
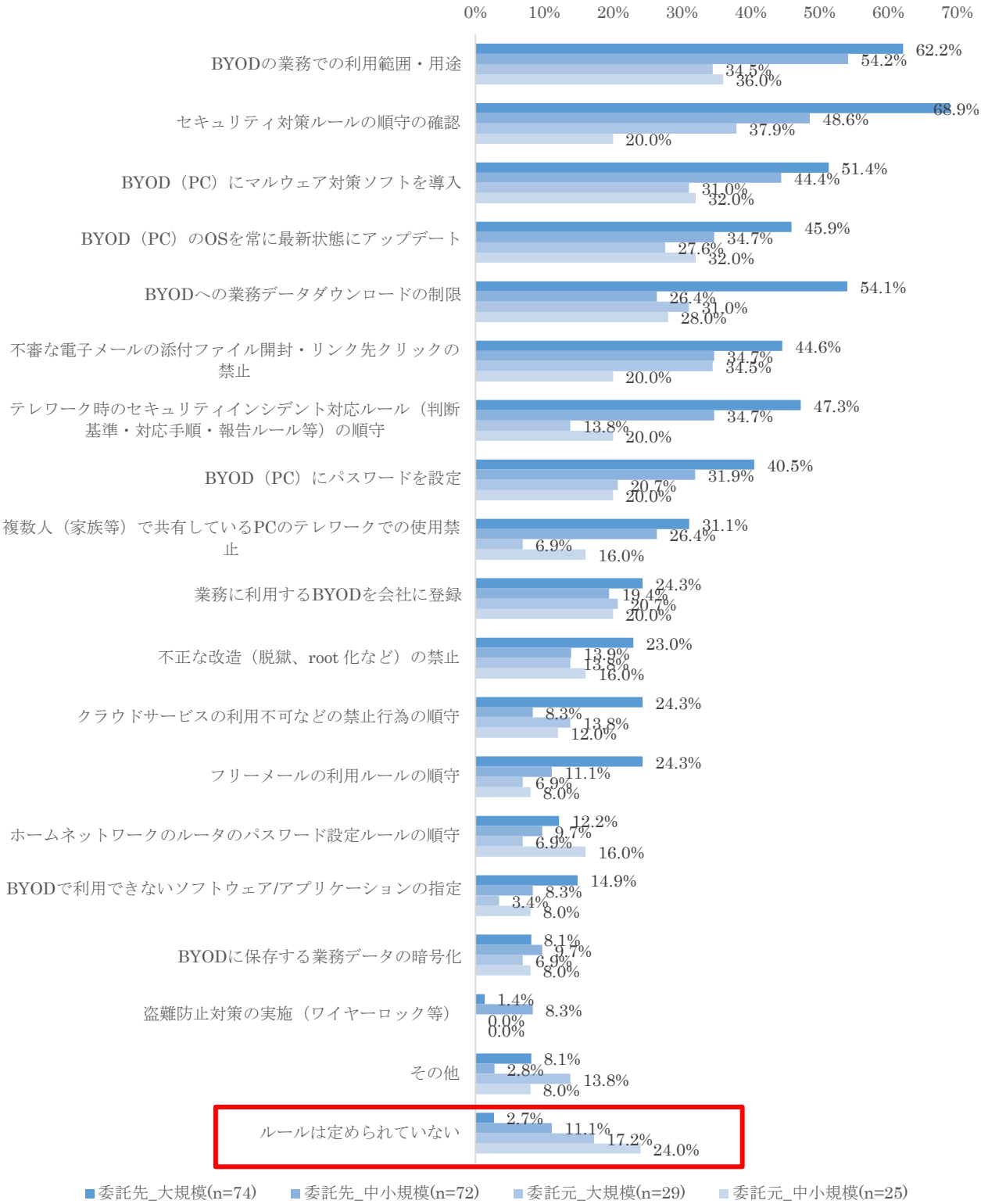


図 2-18：BYOD（スマートフォン（タブレット含む））の利用状況（組織調査 Q20）



BYOD には、端末への不正プログラムの感染による業務情報の漏えいや、セキュリティの低い通信環境の利用に伴う通信内容の盗聴・改竄、BYOD を踏み台とした業務システムへの不正アクセスや業務システムからの情報漏えい等の情報セキュリティリスクが伴う。そのため、BYOD を導入する組織にはセキュリティを確保するためのルールの整備が求められる。BYOD のルールとして定められているセキュリティ対策の状況を確認したところ、委託先の方が、委託元よりも、いずれのセキュリティ対策についてもルールとして定めている傾向があることが明らかになった（図 2-19）。また、大規模の委託先以外の組織（中小規模委託先、大規模・中小規模委託元）の 1 割以上の組織で、ルール自体が定められていない状況であることが明らかになった。なお、「ルールが定められていない」と最も高い割合で回答した組織は中小規模の委託元（約 2 割）であった。ルールが不十分な状況で BYOD を導入している組織においては、ルールの運用・マネジメント力が低下している可能性があると考えられる。

図 2-19：BYOD 利用時にルールとして定められているセキュリティ対策
（組織調査 Q22）



さらに、個人調査にて、組織がルールを策定していない BYOD に関するセキュリティ対策の実施状況を確認したところ（図 2-20）、「いずれの対策も実施していない」の割合が約 2 割（図 2-20 内の赤枠）であり、残りの約 8 割（図 2-20 内の青枠）は、組織によってルールが策定されていないものの、何かしらのセキュリティ対策を行っていることが明らかになった。特に、情報漏えい対策となる、「怪しいクラウドサービスを利用しない」や「パスワードの設定」や、ウイルス感染対策となる「BYOD（PC）の OS を常に最新化にアップデートする」や「BYOD（PC）にウイルス対策ソフトを導入している」の回答率が高い。また、BYOD の利用時に発生したセキュリティインシデントについて、個人の責任となる不安があるセキュリティインシデントを複数回答の設問で確認したところ（図 2-21）、「不安に感じている」セキュリティインシデントとして、直接的に BYOD に関連したセキュリティインシデント（ウイルス感染、情報漏えい、紛失、盗難）が約 3 割と高い回答率となった。

図 2-20：BYOD に関する個人によるセキュリティ対策の実施状況（個人調査 Q28）

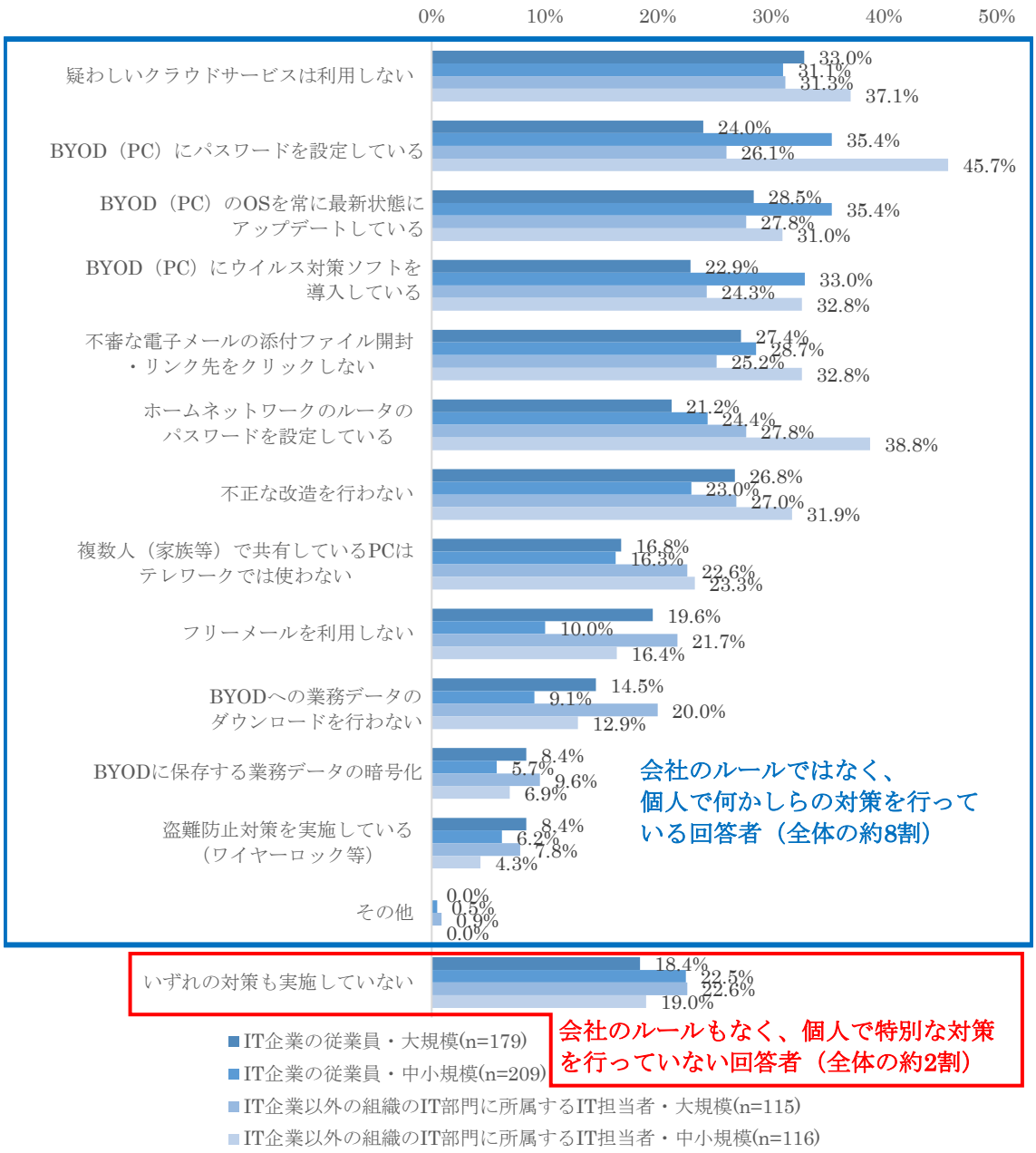
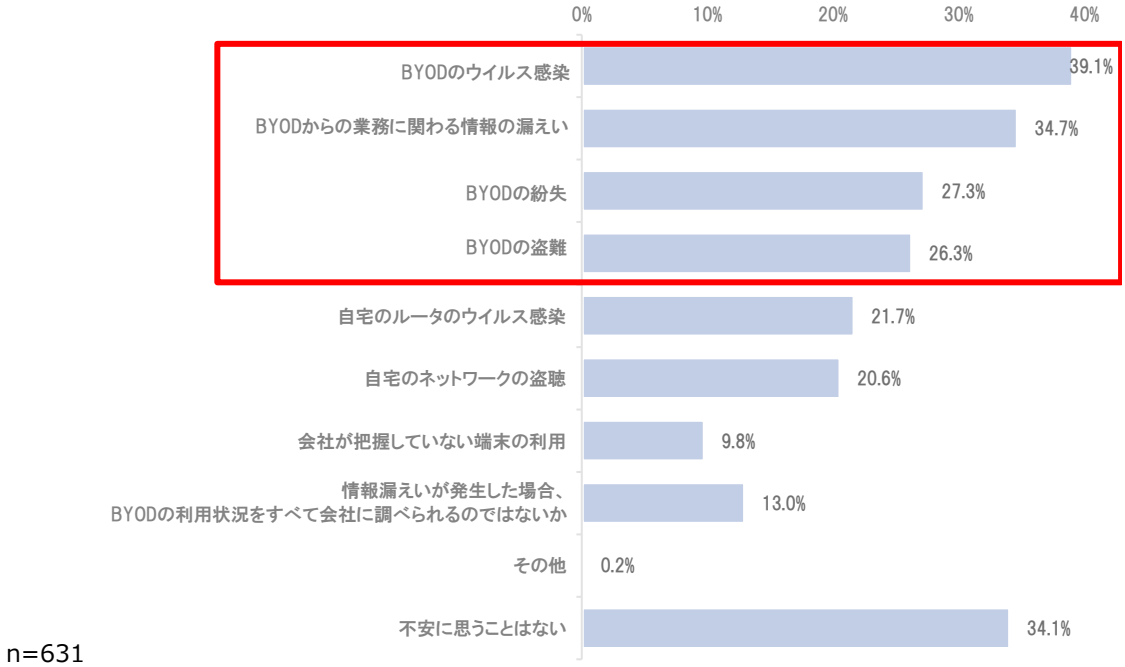


図 2-21：個人責任の不安がある BYOD 利用時のセキュリティインシデント
（個人調査 Q29）



n=631

2.2.2 まとめ（「ルール・運用、マネジメント力の低下」について）

組織調査では、ニューノーマルにおける現状の社内規定やルールに対して、「あいまいな部分が多い」、「働き方の変化に対応していない」等の課題を抱えている組織が委託元・委託先ともに多いことが確認された。同様に、個人調査においても、社内規定やルールに対して、「あいまいな部分が多い」との回答率が高く、組織の現状の規定やルールだけでは、環境に大きな変化が生じるニューノーマルのセキュリティ対策・管理は不十分と感じている組織や個人が多いことが伺える結果となった。

さらに、従業員個人へのセキュリティ対策の依存度が高くなってしまう BYOD のセキュリティに関するルールが、大規模の委託先以外の組織（中小規模委託先、大規模・中小規模委託元）の約 1 割以上の組織では定められていないことが確認された。BYOD のセキュリティに関するルールは、委託先の方が委託元より策定している傾向が全体的に強い。大規模の委託元は BYOD を認めていない割合が高く、それに伴いルール自体が不要のため、BYOD に関するルールを策定する傾向が低いと考えられる。一方で、従業員が保有する PC の BYOD 利用を認める割合が高い中小規模の委託元は、BYOD に関するルールを策定している割合が低くなっている。また、個人調査にて、組織がルールを策定していない BYOD に関するセキュリティ対策の実施状況や、個人の責任となる不安がある BYOD 利用時のセキュリティインシデントを確認したところ、約 8 割の回答者が組織によってルールが策定されていない状況下でも自主的に BYOD に関するセキュリティ対策を実施している（特に情報漏えい対

策やウイルス感染対策の回答率が高い）とともに、多くの回答者が BYOD のウイルス感染、情報漏えいに対して個人の責任となる不安を抱えていることが明らかになった。

以上の結果を踏まえ、環境に大きな変化が生じるニューノーマルに対して、現状の社内規定やルールでは不十分と感じている組織・従業員が多いことに加え、特に BYOD の利用を認めている割合が高い中小規模の委託元において、ニューノーマルに対応するための適切なルール・管理、マネジメント力が低下していることが確認された。

2.3 「今後想定されるセキュリティ脅威や情報セキュリティリスク（セキュリティインシデントの増加を含む）」について

以下の 5 つの仮説について、調査を実施した。

- 仮説 3-1「テレワークへの急速な移行に伴い、取引先に影響を及ぼしうる内部不正（秘密の不正持ち出し、シャドーIT 利用等）が増えるのではないか」
- 仮説 3-2「習熟していないウェブ会議ツールの活用方法の誤り等により、使用者が気付かないうちに情報が漏えいする情報セキュリティリスクが高まっているのではないか」
- 仮説 3-3「業務の自動化・無人化や、職員等が孤立して仕事をしているために、セキュリティインシデント発生時の迅速・適切な対応が難しくなっているのではないか」
- 仮説 3-4「未知の脆弱性に伴うセキュリティインシデントが増加し情報漏えい、サービス停止、マルコード不正組み入れ等のセキュリティインシデントが増えるのではないか」
- 仮説 3-5「訪問や移動を必要としない取引を望む組織が増え、新たなセキュリティ脅威や情報セキュリティリスクが顕在化するのではないか」

2.3.1 調査結果

【内部不正の増加】

本調査では、テレワークへの急速な移行に伴い、取引先に影響を及ぼしうる内部不正（秘密の不正持ち出し、シャドーIT 利用等）が増えるのではないかとの仮説の基、組織調査においてテレワーク導入後における内部不正の増減について調査を行った。結果として、組織として把握している内部不正については委託先・委託元ともに約 8 割が「増減はなし」と回答している（図 2-22）。一方で、内部不正の増減について「把握できてない」という回答も一定割合存在することや、緊急事態宣言発出以降にテレワークを導入した組織における課題として「従業員のルール順守状況の確認が難しくなった」との回答が委託元・委託先ともに 5 割以上存在している（図 2-23）。また、インタビュー結果からは、組織のオフィス内で業務を遂行している限りは周囲の目もあり内部不正に対しての抑止力が働いているが、テレワークや BYOD 等の活用によって、勤務状況を全く見られていない中では、従業員が無意識の内に情報セキュリティリスク（意図しない情報の持ち出しや、不適切なソフトウェアのインストール等）を発生させている可能性があるとの意見があった。以上の結果を踏まえ、仮に内部不正が発生していたとしても、テレワーク等のニューノーマルの影響によって、従業員の勤務状況を把握できていない組織は、内部不正の発生の実態を把握しきれていない可能性がある。

図 2-22：テレワーク導入後の情報セキュリティに関する従業員の内部不正
（緊急事態宣言発出以降にテレワークを導入した組織）（組織調査 Q14）

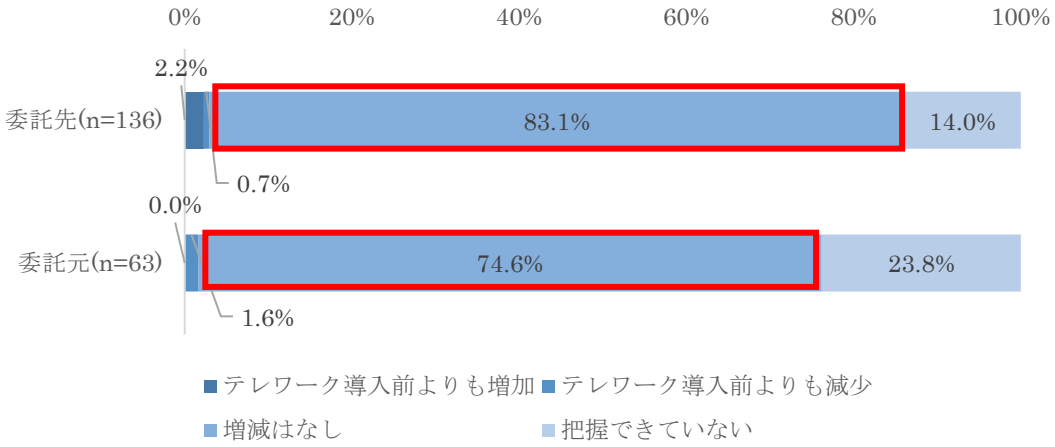
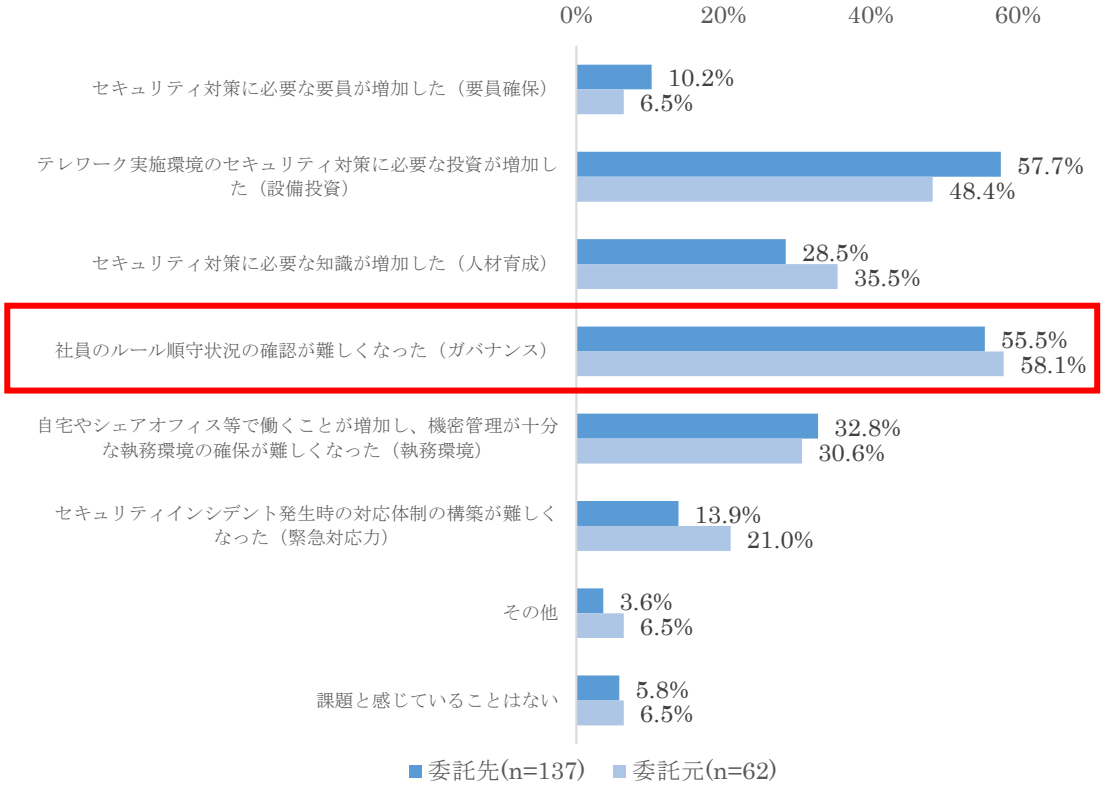


図 2-23：テレワーク実施時のセキュリティ上の課題
（緊急事態宣言発出以降にテレワークを導入した組織）（組織調査 Q9）



また、内部不正リスクの一つとして、秘密の不正持ち出しやシャドーIT の利用に関する調査も行っている。秘密の不正持ち出しについては、組織調査にてテレワークで情報を社外に持ち出す際の情報取扱規則の制定状況をそのルールごとに確認したところ、全体として委託元の方が委託先よりも現時点で制定されていないと回答された割合が高い傾向にあった（図 2-24）。その中でも「重要情報の暗号化」については、委託先・委託元それぞれで規模の小さい組織ほど制定されていないと回答された割合が高く、中小規模の委託元に至っては 6 割近くが制定されていないと回答する結果となった（図 2-25）。

図 2-24：テレワークで情報を社外に持ち出す際の情報取扱規則の
制定状況（テレワーク導入組織）（組織調査 Q16）

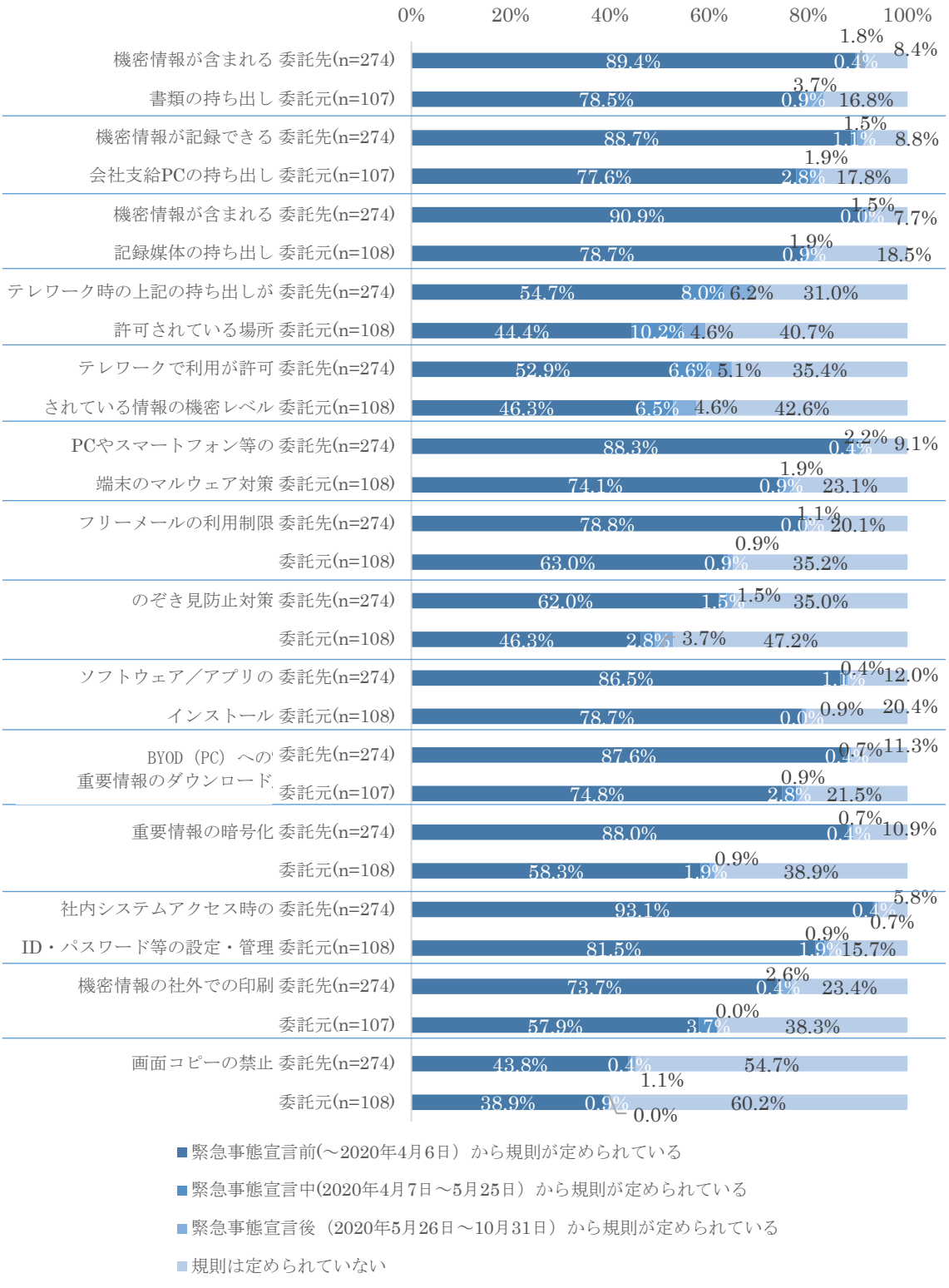
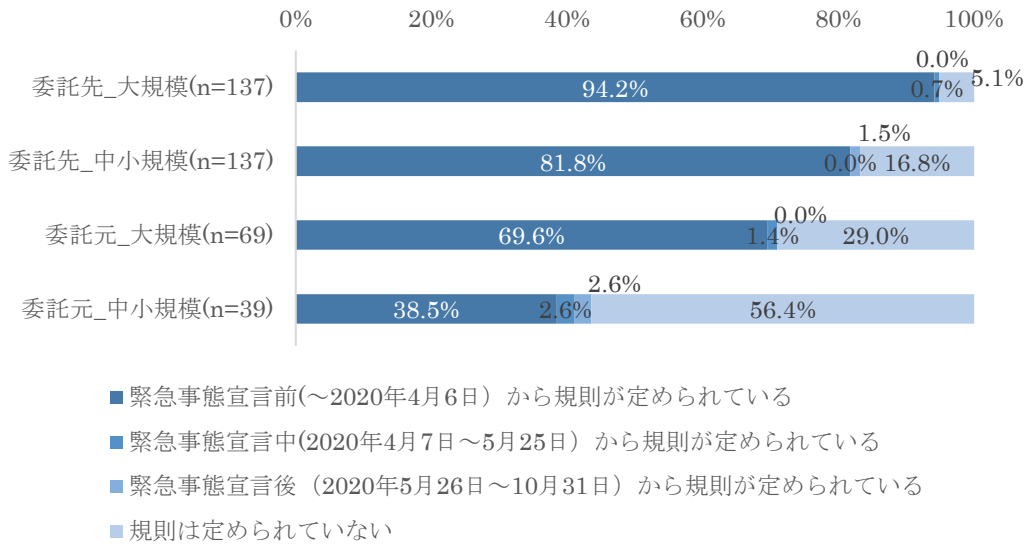


図 2-25：テレワークで情報を社外に持ち出す際の情報取扱規則の
制定状況：重要情報の暗号化
（テレワーク導入組織）（組織調査 Q16）



シャドーIT については、個人調査にて、会社支給の機器にアプリケーションをインストールする際のルールの有無について確認したところ、IT 企業の従業員、IT 企業以外の IT 担当者ともに、中小規模組織の方が大規模組織よりも「明確なルールが定められていない」と回答された割合が高い結果となっている（図 2-26）。

さらに、「事前に申請を行って承認されてからインストールする」ルールが定められている場合においても、実際にそのルールを守ることができていない割合については、IT 企業以外の IT 担当者の方が高い結果となっている他、中小規模の組織の方が大規模と比較して高い傾向にあることからも（図 2-27）、テレワークへの移行が特に委託元や中小規模組織におけるシャドーIT の増加を加速させている可能性がある。

図 2-26：会社支給パソコンへの
ソフトウェアインストールに関するルール（個人調査 Q30）

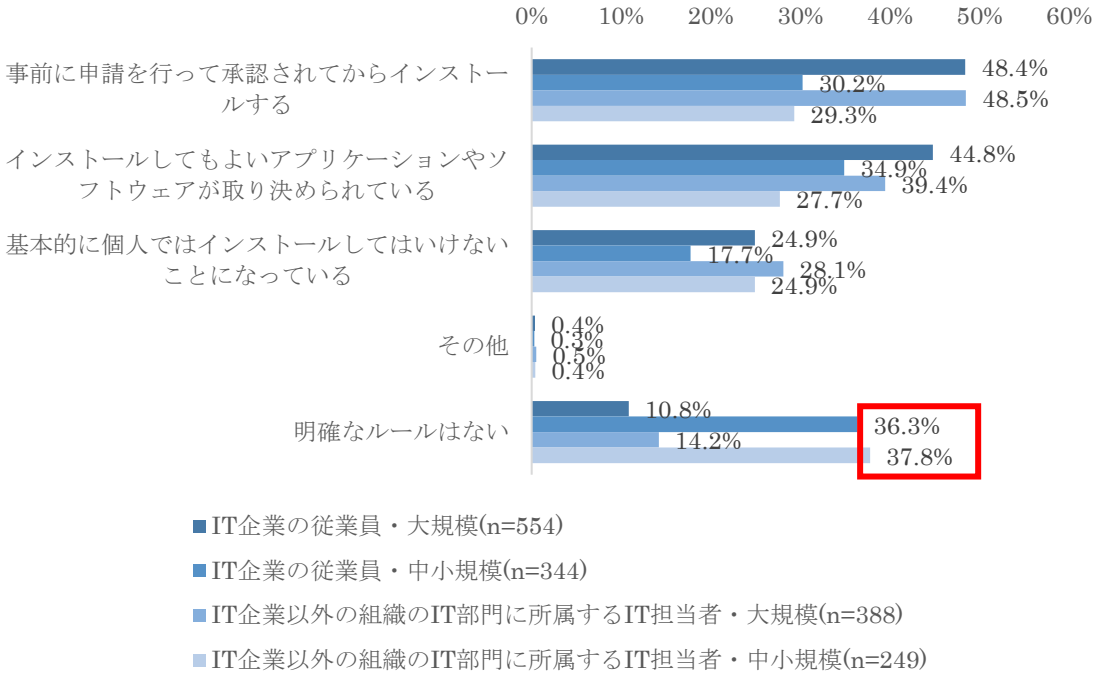
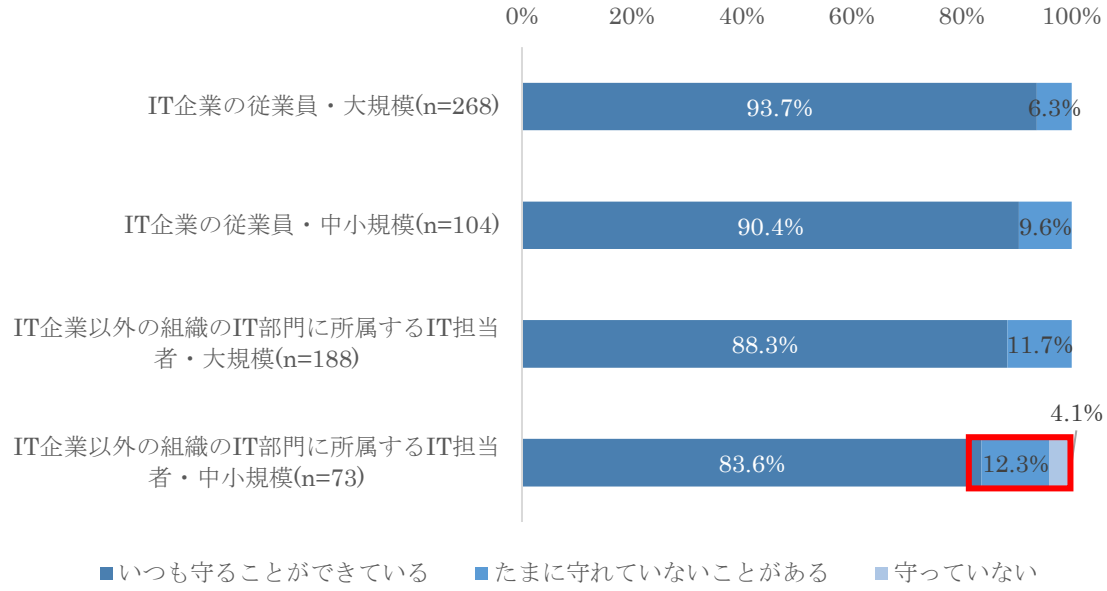


図 2-27：テレワーク利用時の会社支給パソコンへのソフトウェアインストールに
関するルールの遵守状況（個人調査 Q31）

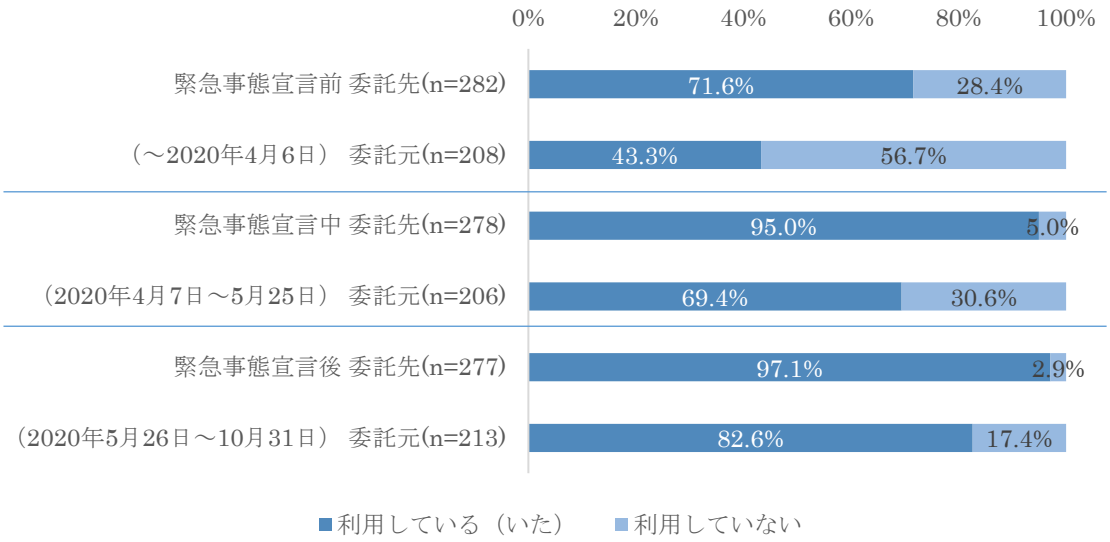


※本設問（Q31）は、Q30（図 2-26）にて、「事前に申請を行って承認されてからインストールする」というルールが定められていると回答した個人を対象とした設問

【ウェブ会議ツールからの情報漏えい】

ウェブ会議ツールについては、習熟していないウェブ会議ツールの活用方法の誤り等により、使用者が気付かないうちに情報が漏えいするリスクが高まっているのではないかとの仮説の基、調査を実施した。そもそものウェブ会議ツールの利用状況について、組織調査にて調査したところ、緊急事態宣言がなされたことを契機に利用が広まっていることが確認できた（図 2-28）。特に委託先においては 10 割近い導入率となっている。

図 2-28：ウェブ会議ツール利用状況（組織調査 Q27）



一方で、ウェブ会議ツールの利用ルールの制定状況については、ルールごとにその制定割合に差がある結果となった（図 2-29）。このことからも自社で利用ルールを定めていたとしても、取引先等会議先のルール制定状況と異なる場合には、結果として制定したルールの遵守が困難である事態が発生していることが伺える。その中でも「会社が許可したツールのみ利用可能」というルールについては、委託先・委託元それぞれで規模の小さい組織ほど制定されていないと回答された割合が高く、中小規模の委託元に至っては現時点においても約 7 割が制定されていないと回答する結果となった（図 2-30）。

図 2-29：ウェブ会議ツールの利用ルールの制定状況（組織調査 Q28）

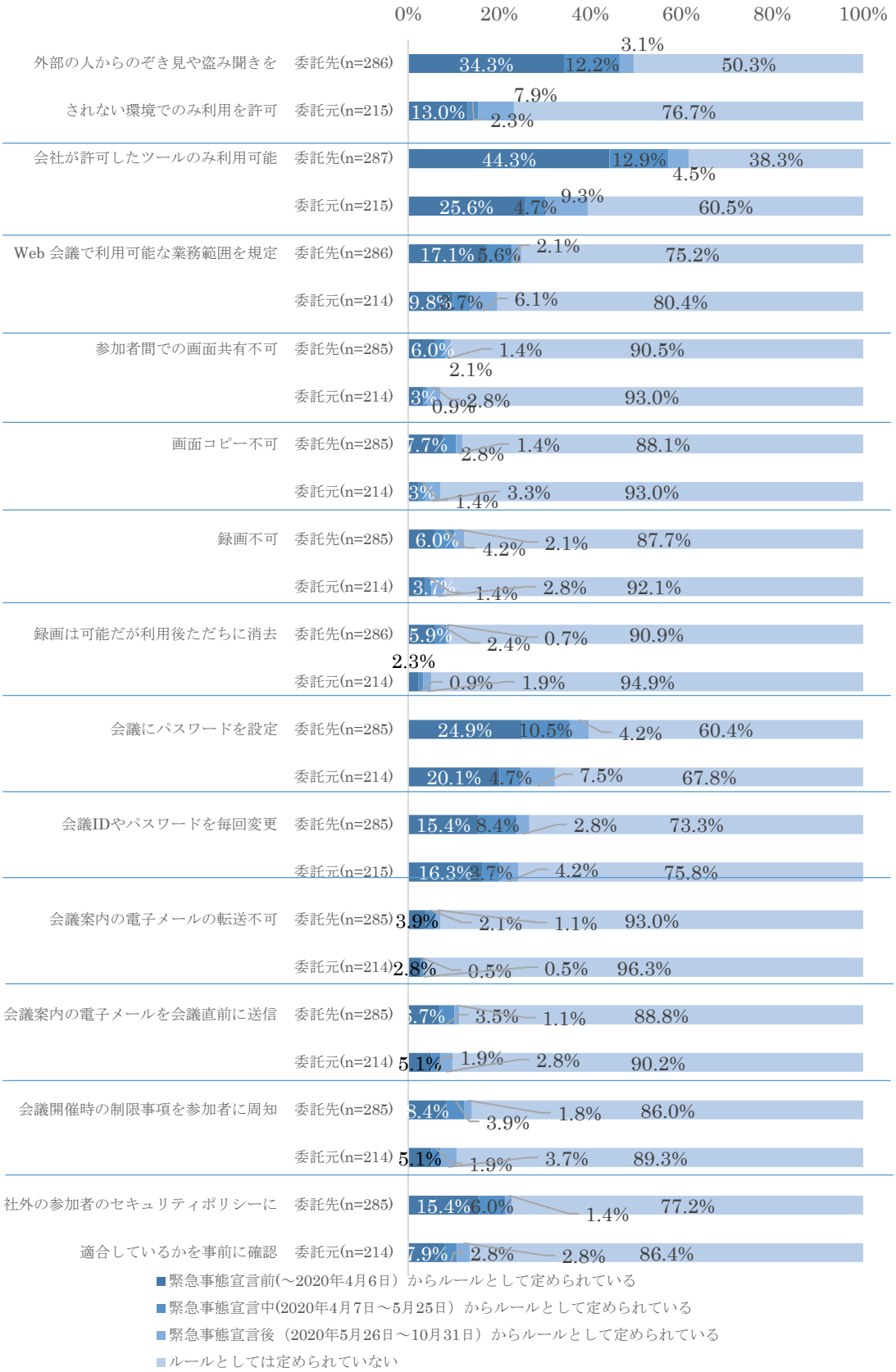
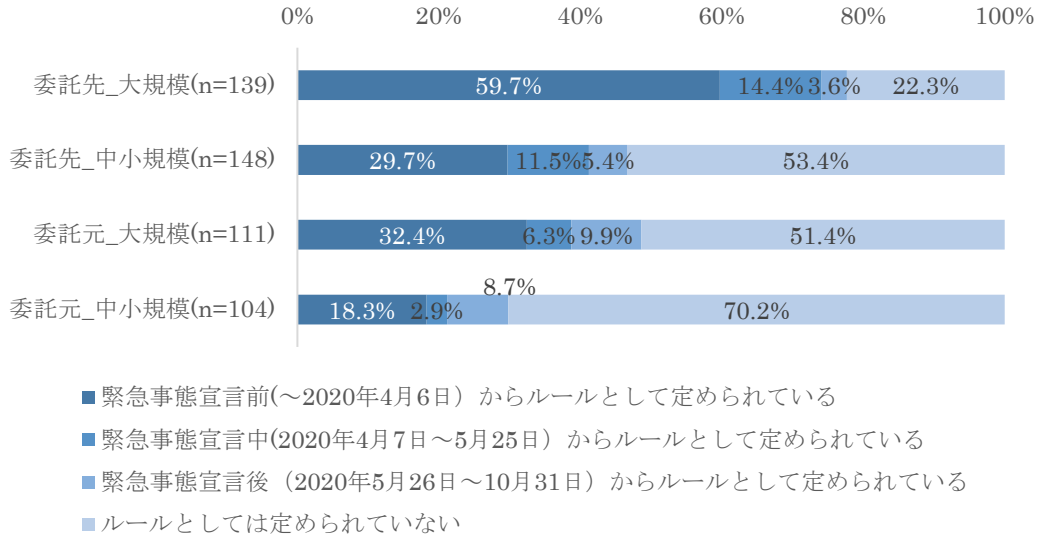


図 2-30：ウェブ会議ツールの利用ルールの制定状況：
会社が許可したツールのみ利用可能（委託元）（組織調査 Q28）



【セキュリティインシデントの増加と対応力低下】

個人向け調査結果からは、テレワーク導入組織に勤める回答者のうち、2 割 5 分程度がほぼ完全にテレワークでの勤務を実施している結果となった（図 2-31）。本結果をもとに、テレワーク実施頻度別でのテレワーク中のセキュリティインシデント発生時の対応への不安について確認したところ、テレワークの実施頻度が少ない回答者程、セキュリティインシデント発生時に「参照すべきマニュアルが参照できない」、「連絡すべき担当に連絡ができない」等の不安が大きい結果となっている（図 2-32）。このことからも、テレワークに慣れていない人では、テレワーク環境でセキュリティインシデントが発生した場合に、必要となる連絡やマニュアルに従った対応等が難しいといったケースが発生しうる可能性がある。

図 2-31：テレワーク実施頻度（個人調査 Q9）

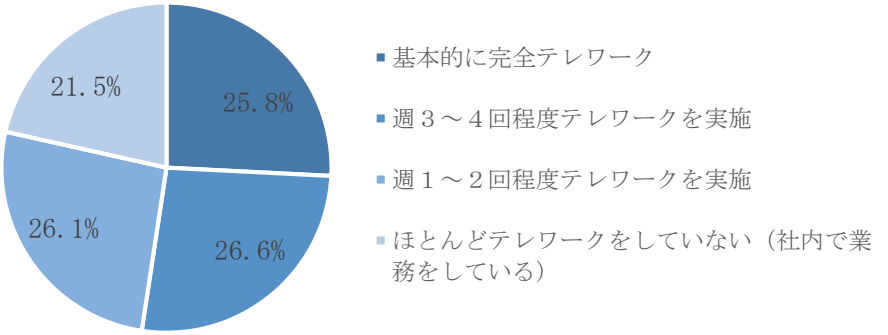
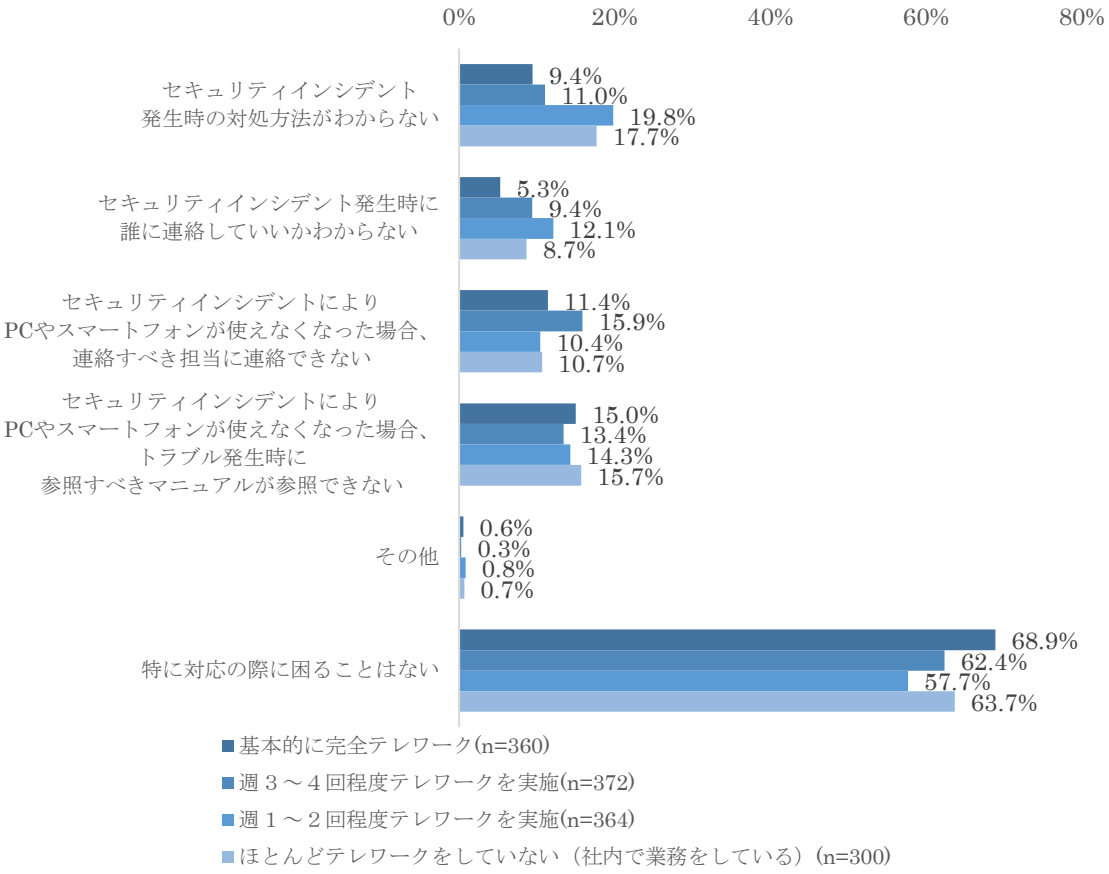


図 2-32：テレワーク実施頻度別のテレワーク中のセキュリティインシデント発生時の対応への不安（個人調査 Q22）



【未知の脆弱性】

未知の脆弱性の増加については、インタビュー調査にて、セキュリティポリシーが整備されていない状況下において、テレワークへの移行により組織の物理的な活動範囲が従業員の自宅環境等まで広がることや、業務利用ツールが増加することにより、多くの脆弱性を抱えることになるとの意見を頂戴することができた。具体的には、自宅のネットワーク環境において取られているセキュリティ対策は従業員によりばらつきがあり、組織として把握することができない。また、テレワークへの移行によって重要情報等が情報セキュリティ上脆弱な自宅ネットワークを経由するリスクが増加すること、ウェブ会議ツールをはじめとした業務利用ツールが増加することで、各ツールに関する未知の脆弱性に接する機会が増加すること等が考えられる。

【訪問や移動を必要としない取引増加による新たなセキュリティ脅威や情報セキュリティリスクの顕在化】

多くの組織において緊急事態宣言前と比較し取引先組織の行動が変化したとの回答があり、特に委託先（IT 組織）から見た委託元の行動変化としては、オンライン会議の増加や委託元でのテレワークの増加などが挙げられている（図 2-33、図 2-34）。

図 2-33：緊急事態宣言前と比較した委託先から見た委託元の行動変化（組織調査 Q33）

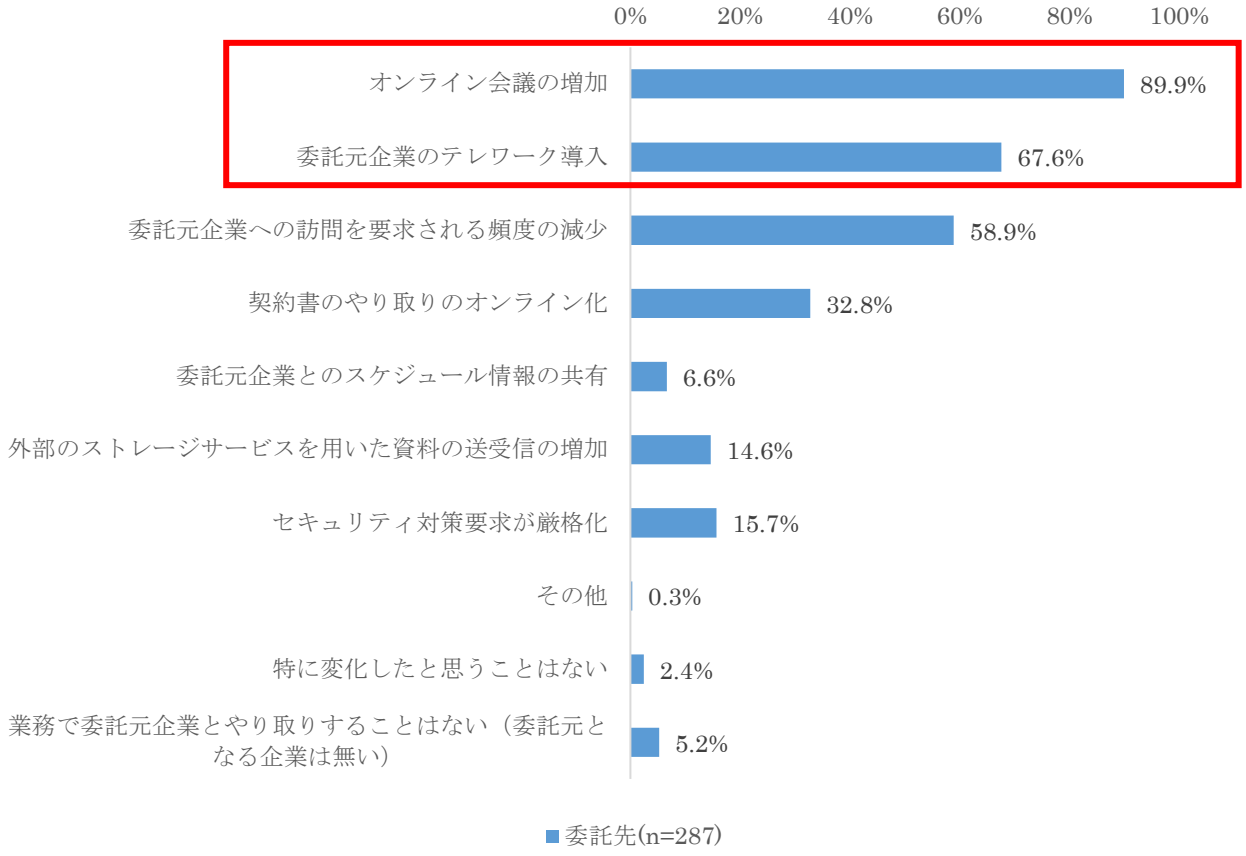
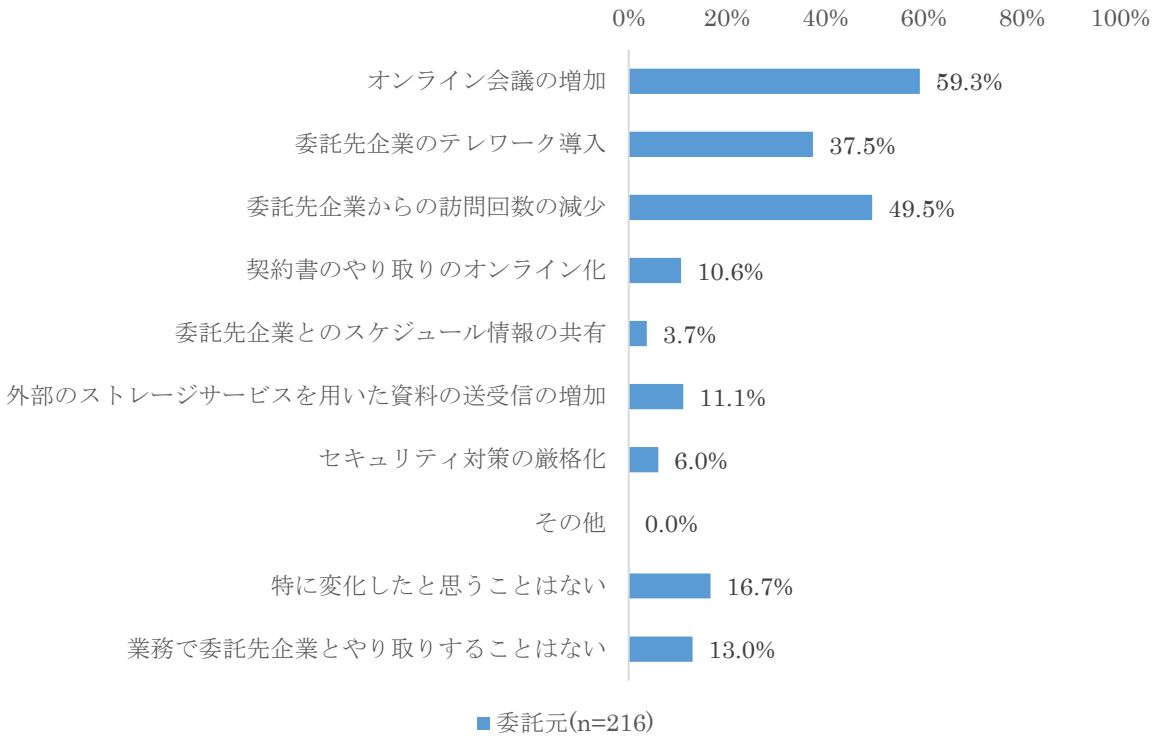


図 2-34：緊急事態宣言前と比較した委託元からみた委託先の行動変化（組織調査 Q33）



また、取引先の行動変化に伴う課題として、委託先からは「コミュニケーションの質・頻度の低下」と回答された割合が最も高い結果となっているが（図 2-35）、委託元からは「必要な IT 知識が急速な増加」が最も回答割合の高い課題として挙げられており、委託元が委託先を管理するのに際して IT 知識が不足しつつある状況が懸念される（図 2-36）。

図 2-35　委託先から見た委託元の課題（組織調査 Q34）

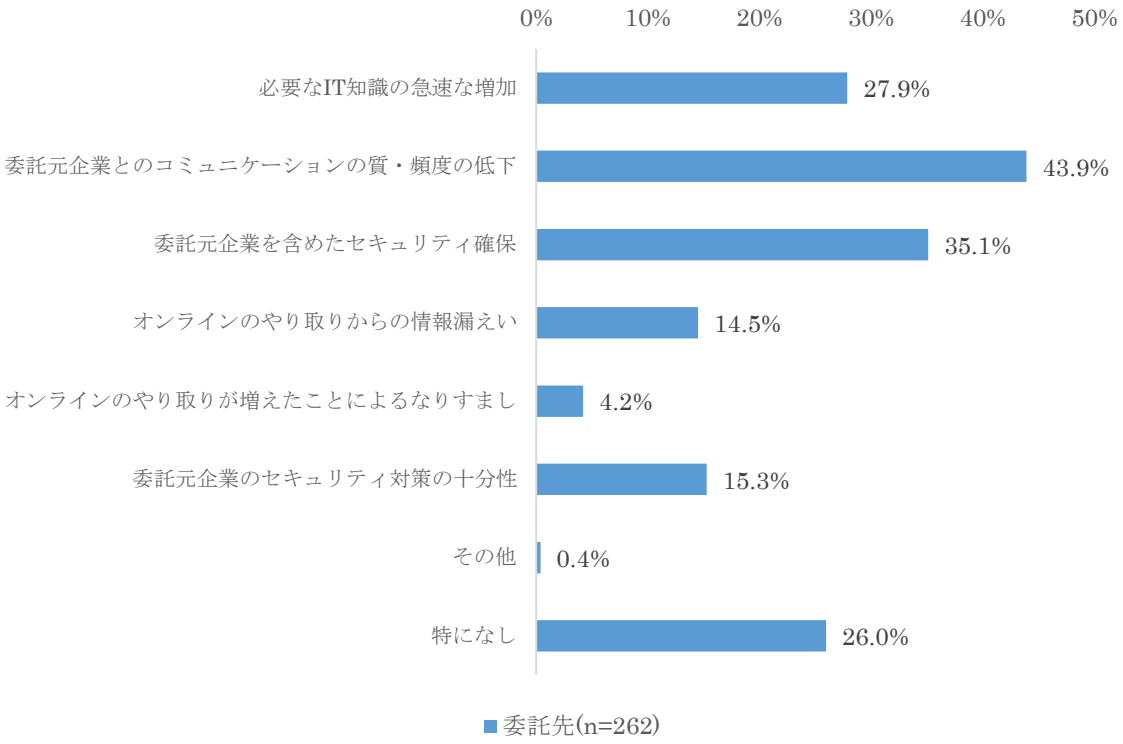
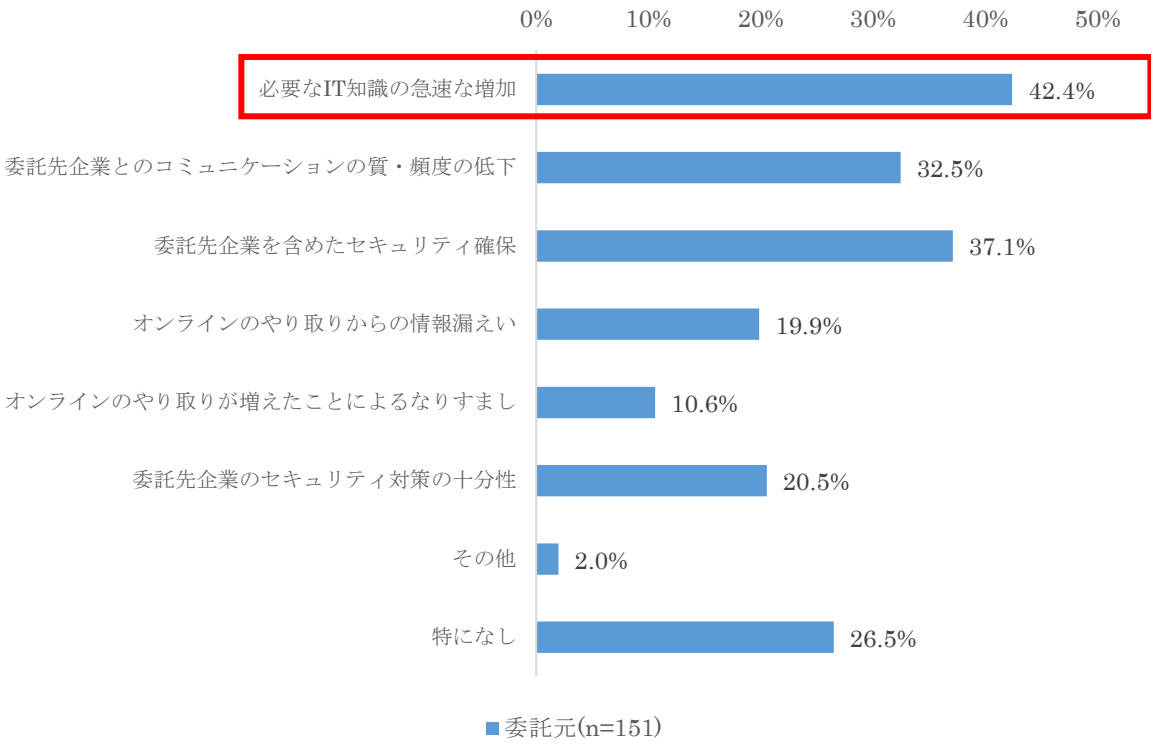


図 2-36：委託元から見た委託先の課題（組織調査 Q34）



2.3.2 まとめ（「今後想定されるセキュリティ脅威や情報セキュリティリスク」について）

今後想定されるセキュリティ脅威や情報セキュリティリスクついて、ニューノーマルへの対応に伴い各組織において把握しきれていない懸念があることが確認された。例えば内部不正について、テレワーク導入後も「増減はなし」と回答している組織が多い一方で、内部不正の増減について「把握できてない」という回答も一定割合存在することや、緊急事態宣言発出以降にテレワークを導入した組織における課題として「従業員のルール順守状況の確認が難しくなった」との回答も多い。さらに、BOYD のルール制定状況についても、シャドーIT 等に関して明確な取り決めがなされていないケースも存在することから、ニューノーマルへの対応に起因する内部不正のリスクや実態の把握が困難になっている懸念がある。

ウェブ会議ツールの利用に際しては、自組織でルールを整備していたとしても、取引先のルール制定状況とのギャップによりルール順守が困難なケースが発生することも多いと想定される。特に中小規模の委託元にて各ルールが制定されていない割合が高く、委託元と委託先で会議する場合など、結果として委託先自身が制定したルールの遵守が困難となり、結果として意図しないセキュリティインシデント発生の確率か高まることが懸念される

また、テレワークへの急速な移行に伴って従業員が孤立した環境で業務を実施することにより、テレワークに慣れていない人では、テレワーク環境でセキュリティインシデントが発生した場合に、必要となる連絡やマニュアルに従った対応等が難しいといったケースが発生しうる可能性があることも確認できた。

未知の脆弱性については、インタビューにおいてテレワークに移行した際に自宅等のネットワーク環境を組織側で把握できないことから脆弱性が残るリスクがあること、ウェブ会議ツールをはじめとした業務利用ツールが増加することで、未知の脆弱性に接する機会が増加する可能性があるとのご意見を頂戴することができた。

また、訪問や移動を必要としない取引など、取引先のニューノーマルへの対応に伴い、特に委託元においては委託先を管理するにあたり必要な IT 知識が不足しつつある状況が示唆される。このことは、委託先や再委託先に対して適切な情報セキュリティ上の対策を求めることのみならず、委託元自身の情報セキュリティリスクへの対応も困難にすることから、IT サプライチェーン全体の情報セキュリティリスクを増加させる一つの要因になる可能性がある。

2.4 「組織と従業員の責任分界点」について

以下の 2 つの仮説について、調査を実施した。

- 仮説 4-1「BYOD でテレワークをした場合のセキュリティ対策が個人任せになっている為セキュリティインシデントが起きないか不安を感じているのではないか」
- 仮説 4-2「BYOD でセキュリティインシデントが発生してもフォレンジックなどの調査ができないのではないか」

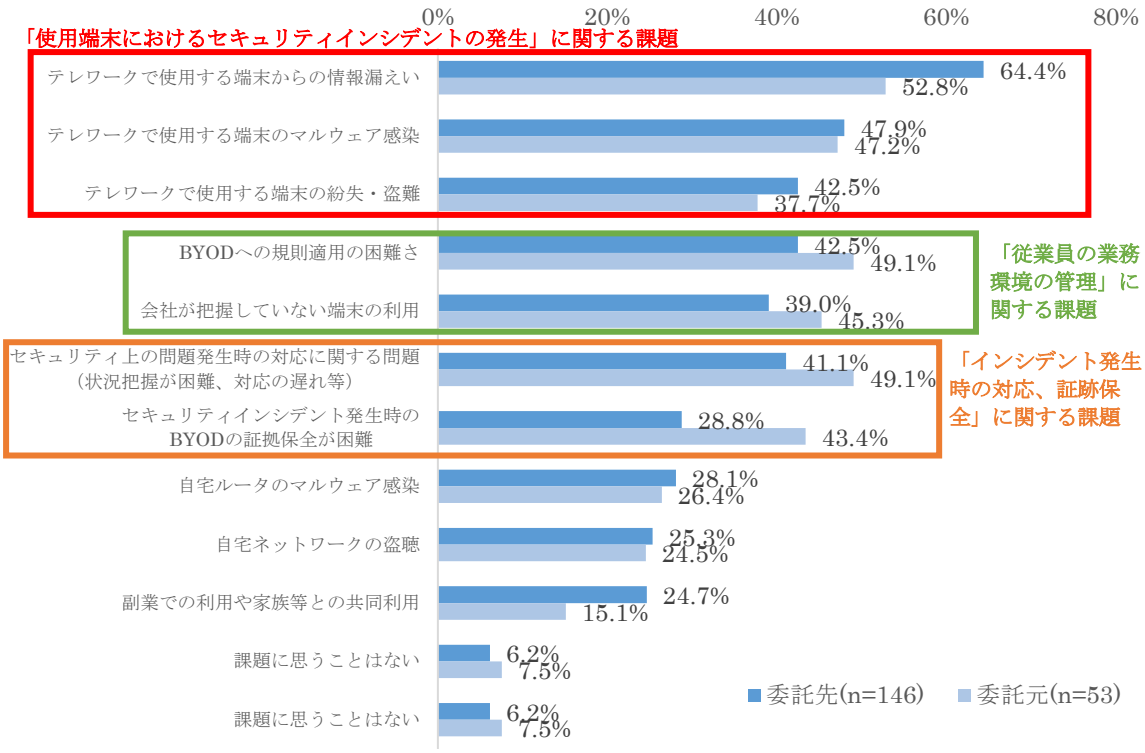
2.4.1 調査結果

【セキュリティ対策が個人任せになっている】

組織調査にて、BYOD を利用している組織に対して、BYOD の利用に伴う課題を確認したところ（図 2-37)、「使用端末におけるセキュリティインシデント発生」（端末からの情報漏えい、端末のマルウェア感染、端末の紛失・盗難)、「従業員の業務環境の管理」（BYOD への規則適用、利用端末の把握)、「セキュリティインシデント発生時の対応、証跡保全」（問題発生時の対応、端末の証跡保全）について課題認識を持っていることが明らかになった。セキュリティインシデントの発生時の対応は重要な課題であるが、特に従業員の業務環境の管理に焦点を当てると、従業員が利用する端末の把握や、それらの端末への規則適用が困難であると感じている組織が多いことがわかる。なお、委託元と委託先を比較すると、委託元の方がセキュリティインシデント発生について、委託先の方がセキュリティインシデント発生時の対応と個人業務環境の管理について課題意識を持っている傾向が確認できた。

以上の結果より、BYOD を利用している組織では、BYOD で業務を行う従業員に規則を適用させることが困難であると感じており、そのような組織においては、セキュリティ対策が従業員個人任せになっていることが伺える。

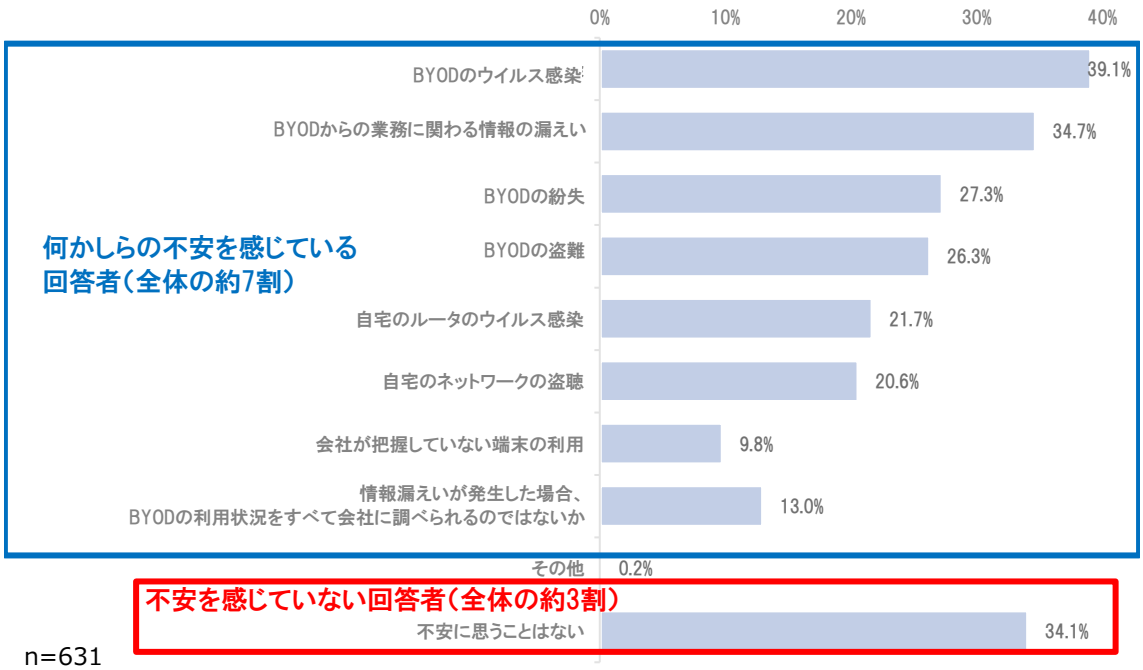
図 2-37：BYOD の利用に伴う課題（組織調査 Q24）



【セキュリティインシデント発生時の BYOD の調査】

さらに、個人調査にて、BYOD の利用時に発生したセキュリティインシデントについて、個人の責任となる不安があるセキュリティインシデントを複数回答の設問で確認したところ（図 2-38）、「不安に思うことはない」の割合が約 3 割（図 2-38 内の赤枠）であり、残りの約 7 割（図 2-38 内の青枠）は、何かしらのセキュリティインシデントが発生した際は個人の責任になる不安を感じていることが明らかになった。このことからも、セキュリティインシデントが発生した際の組織と従業員個人との責任分界点が明確に定められていないケースが多く、セキュリティインシデント発生後の対応が困難になる潜在的リスクが高い状況にあることが伺える。また、図 2-37 にて、セキュリティインシデント発生時の BYOD の証跡保全に関する組織の課題認識が明らかになっていることに加え、図 2-38 にて、組織と従業員間でセキュリティインシデント発生に備えた明確な規則が定められておらず責任分界点が曖昧であるということからも、セキュリティインシデントが発生した際に BYOD を調査することは難航することが予測される。

図 2-38：個人責任の不安がある BYOD 利用時のセキュリティインシデント
（個人調査 Q29）



n=631

2.4.2 まとめ（「組織と従業員の責任分界点」について）

本調査結果では、「組織と従業員の責任分界点」の実態の調査を行ったところ、BYOD を利用している組織では、セキュリティ対策を従業員個人任せになっている可能性があり、セキュリティインシデントが発生した際の組織と従業員個人との責任分界点が明確に定められていないということが明らかになった。また、このことから責任分界点を明確にするための規則の策定や、技術的なソリューションが導入されていないことが推察され、仮にセキュリティインシデントが発生した際には、影響範囲を特定するためのフォレンジック等の調査が難航することが予測される。

まず、セキュリティ対策が従業員個人任せになっている実態について、組織調査より、BYOD を利用している組織では、従業員が利用する端末の把握やその端末へ規則を適用させることが困難であると感じている組織が多いことが明らかになり、そのような組織ではセキュリティ対策が従業員個人任せになっている可能性がある。

次に、組織と従業員の責任分界点の曖昧さについて、個人調査にて、BYOD の利用時に発生した個人の責任となる不安があるセキュリティインシデントを確認したところ、「不安に思うことはない」の割合が約 3 割であり、残りの約 7 割は、何かしらのセキュリティインシデントが発生した際は個人の責任になる不安を感じていることが明らかになった。

個人が BYOD 利用時に個人の責任となる不安があるセキュリティインシデントと、組織が懸念している BYOD 利用に伴う課題を比較すると、両者とも、端末のウイルス感染や、端末からの情報漏えい、端末の紛失・盗難に対する回答率は高かった。一方で、個人調査では、会社が把握していない端末の利用や、情報漏えい時の端末の調査の回答率は低い傾向があったが、組織調査では、従業員の利用端末の把握、セキュリティインシデント発生時の対応や証跡保全の回答率は高く、ここに個人と組織間で認識のギャップがあった。この個人と組織間で認識のギャップがあるセキュリティインシデントについては、組織側は課題と認識している一方で、個人は組織任せにしている（個人は自身の責任になる不安を感じていない）ため、特に組織が主導権を持って対策を講じていく必要がある。

2.5 「委託先選定、再委託先許諾への影響」について

以下の 2 つの仮説について、調査を実施した。

- 仮説 5-1「テレワークの実施の可否、テレワーク実施時のセキュリティ対策内容が業務委託先選定の条件となるのではないか」
- 仮説 5-2「委託先として、事業収益が最優先で、セキュリティガバナンス/コンプライアンスの意識が低いニューカマーが増えているのではないか」

2.5.1 調査結果

【テレワークの導入やセキュリティ対策内容が委託先選定条件に与える影響】

組織調査にて、委託先に対して、委託元からのテレワーク実施に対する認可の状況について調査を実施したところ（図 2-39）、約 5 割の大規模委託先と約 4 割の中小規模委託先において、委託元からテレワークの実施が認められていない業務が存在していることが明らかになった。一方で、委託元に対して、委託先のテレワークの実施に対する認可の状況を確認したところ（図 2-40）、約 2 割の委託元（大規模、中小規模共）が、委託先に対してテレワークの実施を認可していない（一部業務限り含む）状況であることが明らかになった。委託元と委託先の結果に生じている差は、委託先においては、複数の委託元の中で一社でも該当する組織があれば、「テレワークの実施が認められない業務が存在している」と回答することが想定されるため、委託元と比較してテレワーク実施認可の割合が小さくなる傾向があると考えられる。また、規模別で比較をすると、大規模の委託元・委託先の方が、中小規模の委託元・委託先よりも、テレワークの実施を認めていない（大規模委託元）、認められていない（大規模委託先）と回答する割合が高い。

図 2-39：委託元からのテレワーク実施認可状況（委託先）（組織調査 Q36）

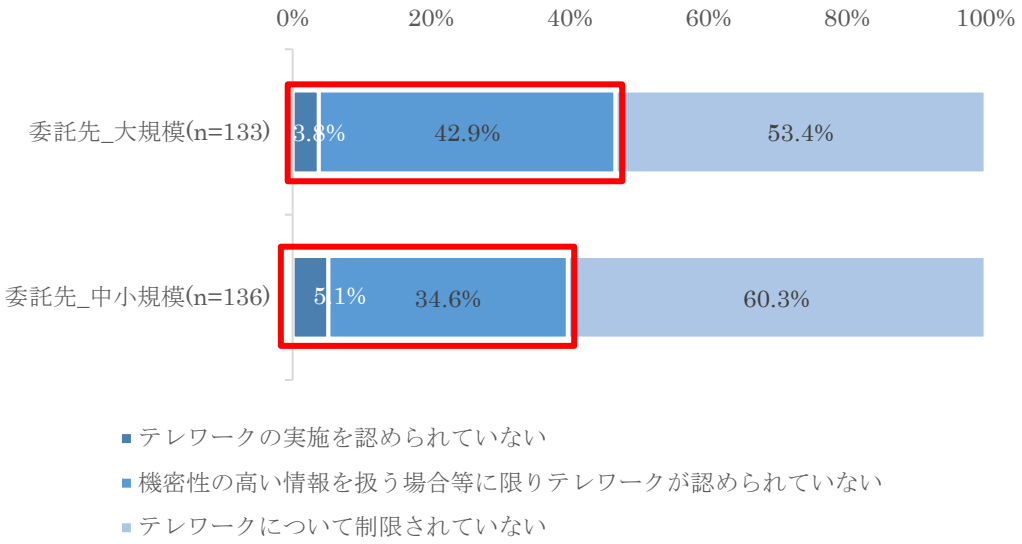
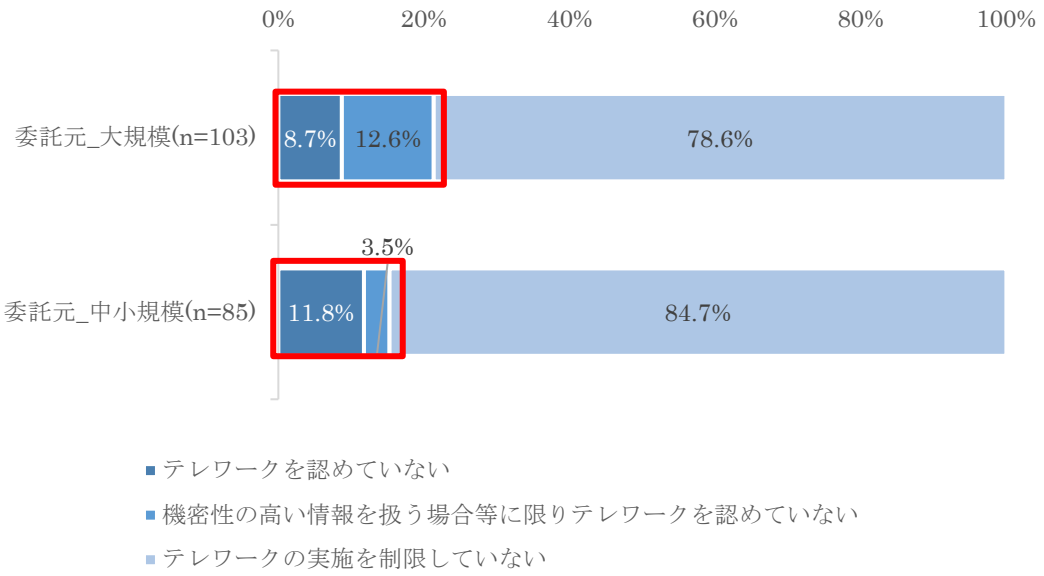


図 2-40：委託先へのテレワーク実施認可状況（委託元）（組織調査 Q36）



また、委託元と委託先に対して、現場での業務実施が条件となっている業務の実態（図 2-41、図 2-43）と、今後の現場での業務実施の見込み（図 2-42、図 2-44）について調査を行った。まず、委託先への調査結果から、約 7 割の委託先が、委託元から現場での作業を要求されており、その委託先のうち約 8 割が今後も現場での業務実施を要求される見込みであると回答しているまた、委託元への調査結果からは、約 4 割の委託元が、委託先に対して現場での業務実施を条件としており、その委託元のうち約８割が今後も現場での業務実施を要求することを見込んでいることが確認された。

有識者のインタビュー調査からは、テレワークの実施有無が、委託先・再委託先選定の際の要件となるケースの増加は現時点では確認できていない一方で、今後テレワークでの業務実施がより多くの組織に普及した際にはセキュリティ確保に向けた要求が増えてくる可能性が高いとの指摘があった。

図 2-41：委託元からの現場での業務実施が条件となる業務の実態
（委託先）（組織調査 Q39）

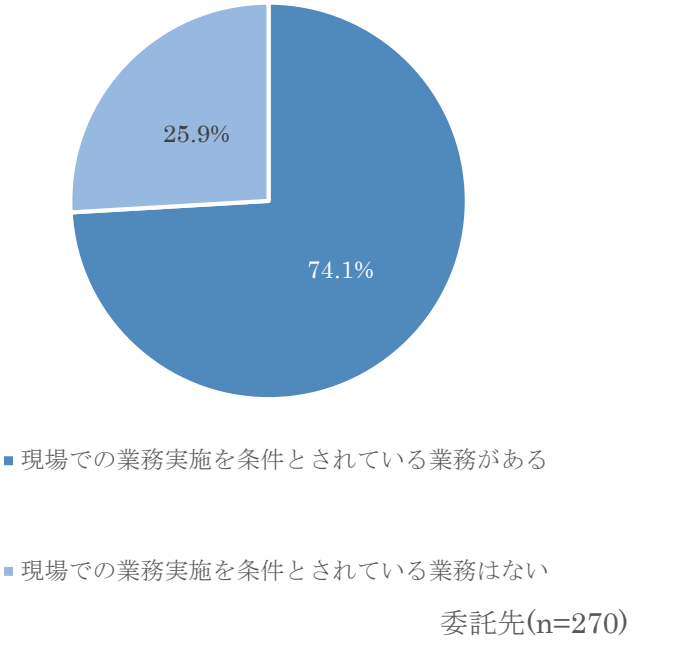


図 2-42：今後の委託元からの現場での業務実施要求見込み
（委託先）（組織調査 Q39）

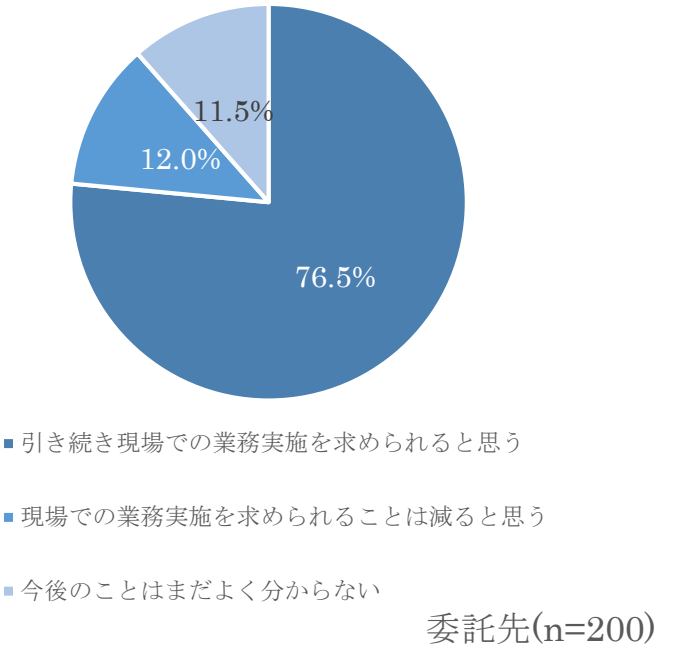
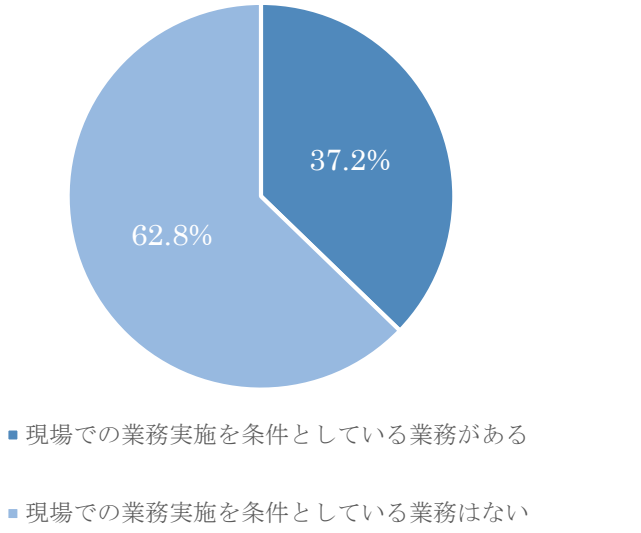
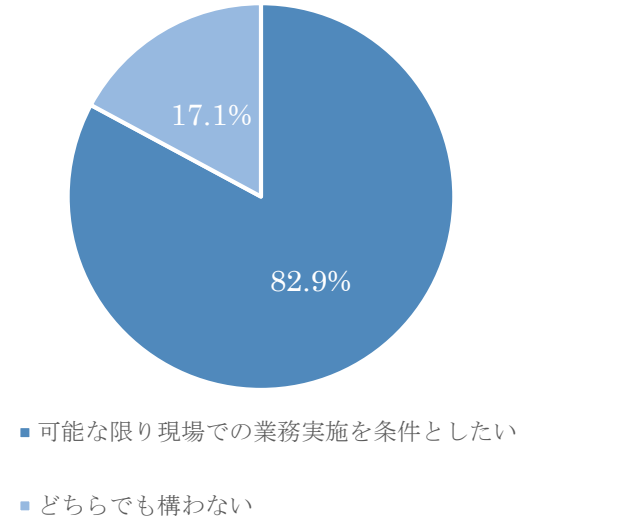


図 2-43：委託先への現場での業務実施が条件となる業務の実態
（委託元）（組織調査 Q39）



委託元(n=188)

図 2-44：今後の委託先への現場での業務実施要求見込み
（委託元）（組織調査 Q39）



委託元(n=70)

【セキュリティガバナンス/コンプライアンスの意識が低いニューカマーの増加】

組織調査にて、委託元に対して新たな委託先との取引状況を、委託先に対して新たな委託先（委託元の視点では再委託先）との取引の状況をそれぞれ確認したところ、新規の委託先との取引が増加した委託元は全体の約 2 割（図 2-45）、新規の委託先（委託元の視点では再委託先）との取引が増加した委託先は全体の約 1 割であった（図 2-46）。

また、有識者へのインタビュー調査からは、ニューノーマルにおける DX の推進等を背景に、IT サプライチェーンに不慣れな委託元（過去に業務委託をした経験がない、または経験が少ない）による社外向けサービス／アプリケーションの開発委託が急増しており、委託元のセキュリティガバナンスが不十分な IT サプライチェーンが増加する可能性があるとの指摘があった。

図 2-45：新たな委託先との取引（委託元）（組織調査 Q41）

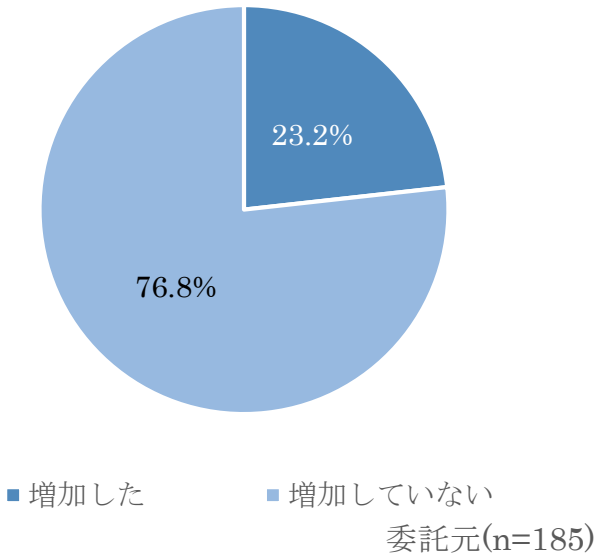
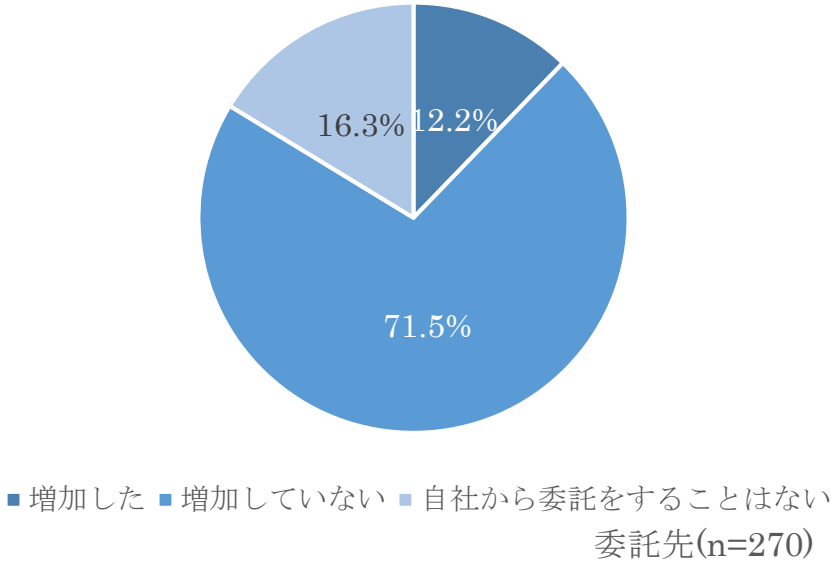


図 2-46：新たな再委託先との取引（委託先）（組織調査 Q41）



2.5.2 まとめ（「委託先選定、再委託先許諾への影響」について）

現時点において、現場での業務実施を業務委託の際の条件としている組織については、今後もそれらの条件を継続して要求する見込みであることが確認された。アンケート結果からは、約 2 割の委託元が、委託先に対してテレワークの実施を認可していない（一部業務限り含む）状況である。また、約 4 割の委託元が委託先に対して現場での業務実施を条件としている業務を要求しており、さらにその委託元のうち約 8 割が今後も現場での業務実施を要求することを予測している。現時点においてはテレワークの実施の可否やテレワーク実施時のセキュリティ対策内容が業務委託先選定の条件になっているケースの増加は確認できないものの、有識者インタビューからは今後テレワークでの業務実施が一般化した際にはセキュリティ確保に向けた要求が増えてくる可能性が高いとの指摘があった。

次に、セキュリティガバナンス/コンプライアンスの意識が低いニューカマーの増加について、まず組織調査から、新規の委託先との取引が増加したと回答した委託元が 2 割強程度、新規の再委託先との取引が増加した委託先が 1 割強程度存在することが確認され、緊急事態宣言発出以降に新たな委託先と取引を開始している組織がいることが確認できた。さらに、有識者へのインタビュー調査から、IT サプライチェーンに不慣れな（過去に業務委託をした経験がない、または経験が少ない）委託元による社外向けサービス／アプリケーションの開発委託が急増しており、委託元のセキュリティガバナンス/コンプライアンスが不十分な IT サプライチェーンが増えている可能性があるとの指摘があった。サプライチェーン上に新規の委託先や再委託先が増加することによって、サプライチェーンが複雑化する質の変化だけではなく、新規の委託元の参入によって新しい IT サプライチェーンが構築され

る量の変化（一つの委託元からの業務委託が増える事によるサプライチェーンの数の増加）も予測され、今後ますますサプライチェーン全体でのセキュリティ対策・管理の重要性が高まっていくことが想定される。

2.6 「委託先へのセキュリティ対策要求等の変化」について

以下の仮説について、調査を実施した。

- 仮説 6-1「ニューノーマルへの対応に向けて、委託元は委託先へのセキュリティ対策やセキュリティ確保に関する証跡提出等の要求を強化することが増えるのではないか」

2.6.1 調査結果

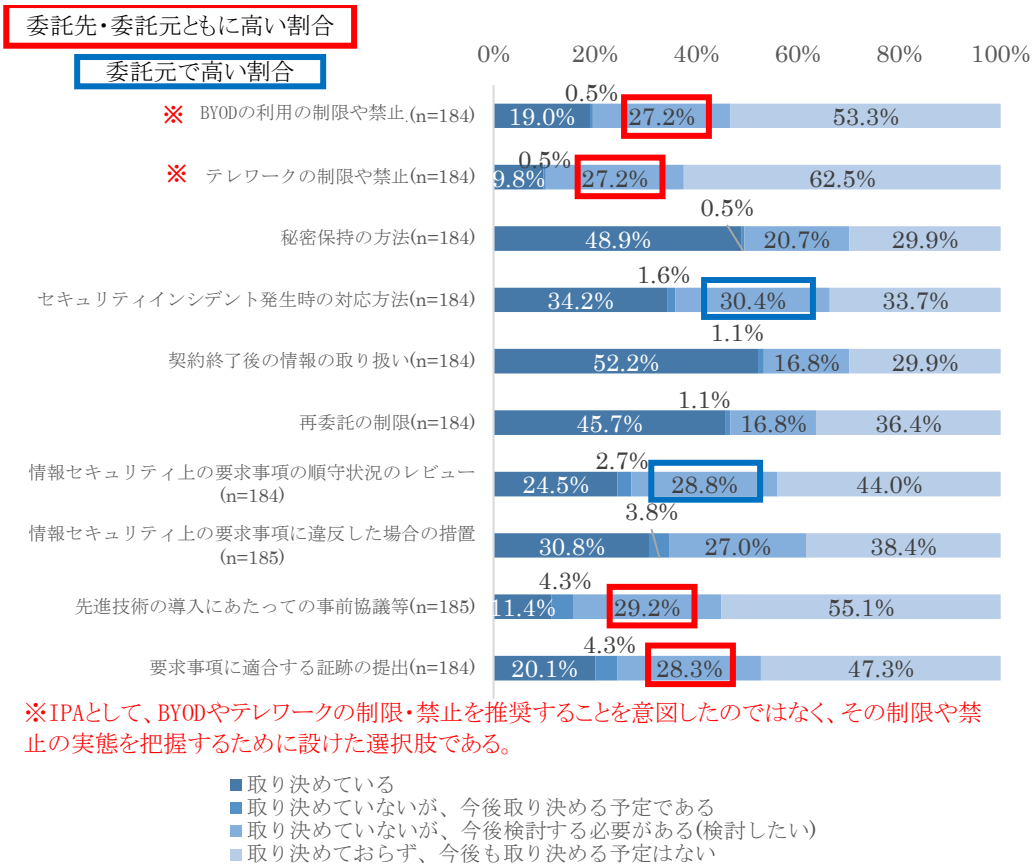
組織調査にて、IT サプライチェーンのセキュリティ対策・管理の動向を把握するために、委託元と委託先それぞれに対して、契約上の要求事項の取り決めの状況を確認したところ、現状、契約上取り決めていない要求事項について、「今後取り決める予定である」と回答した組織は、委託先・委託元ともに、1 割未満にとどまっている（図 2-47、図 2-48）。特に、ニューノーマルにおいてテレワークや BYOD の実施の可否や実施時の条件について取り決めを行う組織が増えるのではないかとの想定の基、その実態を把握するために設けた「テレワークの制限や禁止」や「BYOD の利用の制限や禁止」等の要求事項についても、「今後取り決める予定である」と回答された割合は低い結果となった。

また、現状、契約上取り決めていない要求事項については、そのほとんどで 2 割～3 割程度が「今後検討する必要がある（検討したい）」と回答している。BYOD やテレワークに関する要求事項と、先端技術の導入時の事前協議、要求事項に適合する証跡の提出に関する要求事項については、委託元・委託先ともに「今後検討する必要がある（検討したい）」と回答した割合が高い傾向にある。また、委託元においては、セキュリティインシデント発生時の対応方法や、情報セキュリティ上の要求事項の順守状況のレビューについても、「今後検討する必要がある（検討したい）」と回答した割合が高かった。

なお、委託元と委託先の結果を比較すると、要求事項の取り決めの状況の認識に乖離（委託元は取り決めていないと認識している割合が高い一方で、委託先は取り決めていると認識している割合が高い要求事項が存在）が確認できる。契約は、委託元と委託先行間のものであるため、本来であれば、双方の結果は同一になると思われるが、厳格なセキュリティ要件を定める情報通信業等の委託元を顧客とする委託先と 2 次・3 次受けの委託先間の契約ではより詳細に要求事項が取り決められていることから、委託元と委託先の間でこのような認識の乖離が生じている可能性があると考えられる。

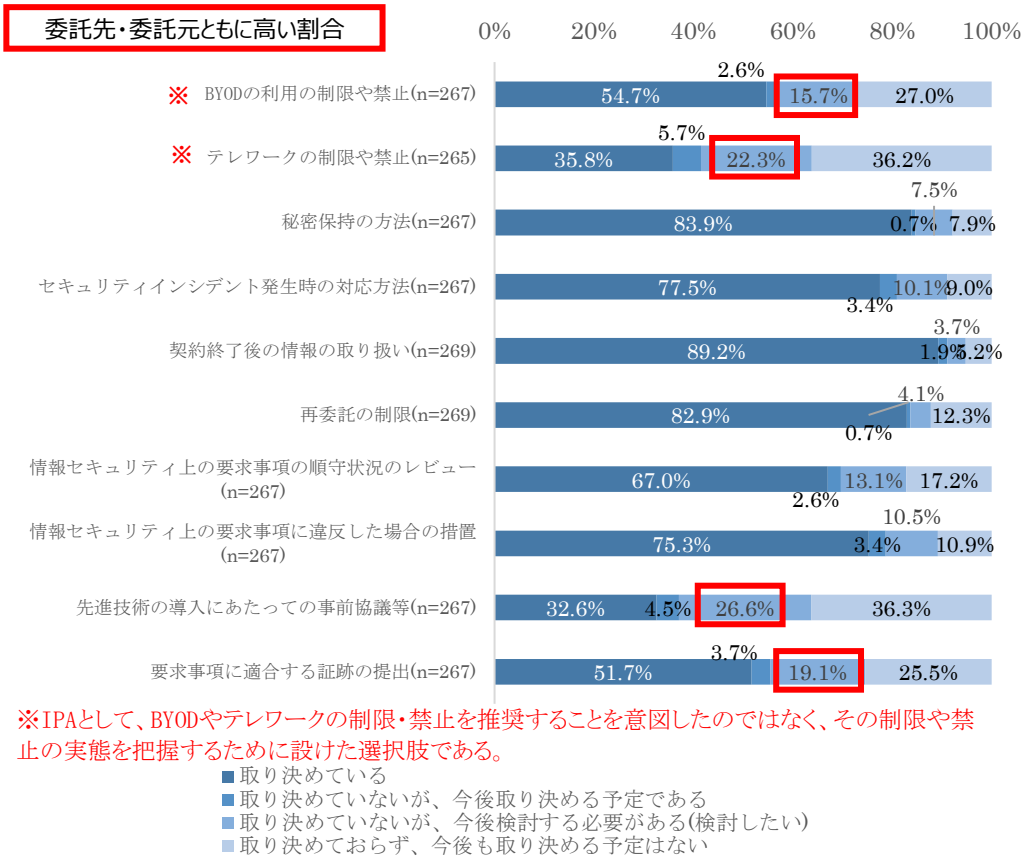
以上の結果から、現時点で明確に管理が強化されている様子は確認できないものの、今後の組織による検討の結果次第で、委託元が、委託先の情報セキュリティリスクを低減するためのセキュリティ対策の要求事項（特に、セキュリティインシデント発生時の対応方法や先端技術の導入時の事前協議、要求事項に適合する証跡の提出等に関する要求事項）を強化していく可能性があると考えられる。

図 2-47：委託先への契約上の要求事項（委託元）（組織調査 Q40）



※IPAとして、BYODやテレワークの制限・禁止を推奨することを意図したのではなく、その制限や禁止の実態を把握するために設けた選択肢である。

図 2-48：委託元からの契約上の要求事項（委託先）（組織調査 Q40）



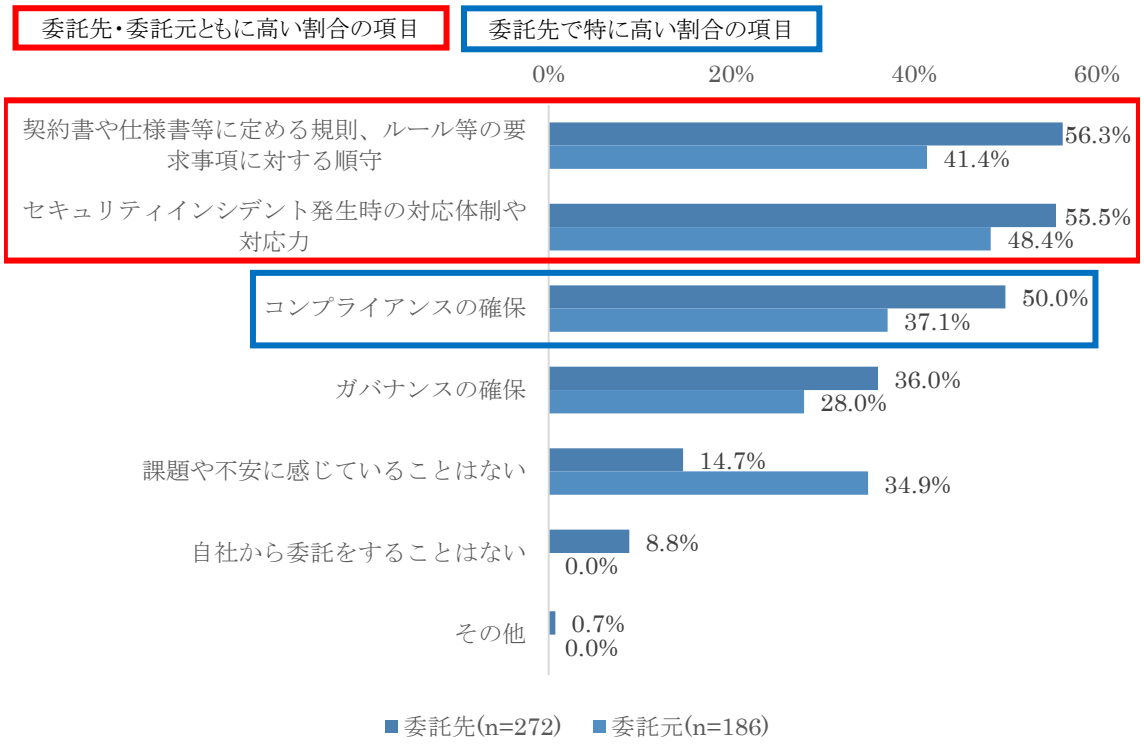
また、参考情報として、委託元と委託先に対して「新たな委託先または再委託先」に関する課題や不安について（図 2-49）、委託先に対して「新たな委託元」に関する課題や不安について（図 2-50）確認した。

まず、図 2-49 より、4 割以上の委託元が委託先に対して、「契約書や仕様書等に定める規則・ルール等の要求事項に対する遵守」、「セキュリティインシデント発生時の対応体制や対応力」について課題や不安を感じていた。また、委託先については、5 割以上が再委託先に対して、「契約書や仕様書等に定める規則・ルール等の要求事項に対する遵守」、「セキュリティインシデント発生時の対応体制や対応力」、「コンプライアンスの確保」について課題や不安を感じている状況が明らかになった。委託元と委託元の結果を比較すると、委託先の方が全体的に課題・不安を感じていると回答した割合が高い傾向にある。この理由として、委託元との契約において、セキュリティに関する詳細な要件や責任範囲が定まっていないことが多く[10]、再委託先以降のサプライチェーン上で発生したセキュリティインシデントの責

[10] IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査」https://www.ipa.go.jp/security/fy30/reports/scrm/index.html

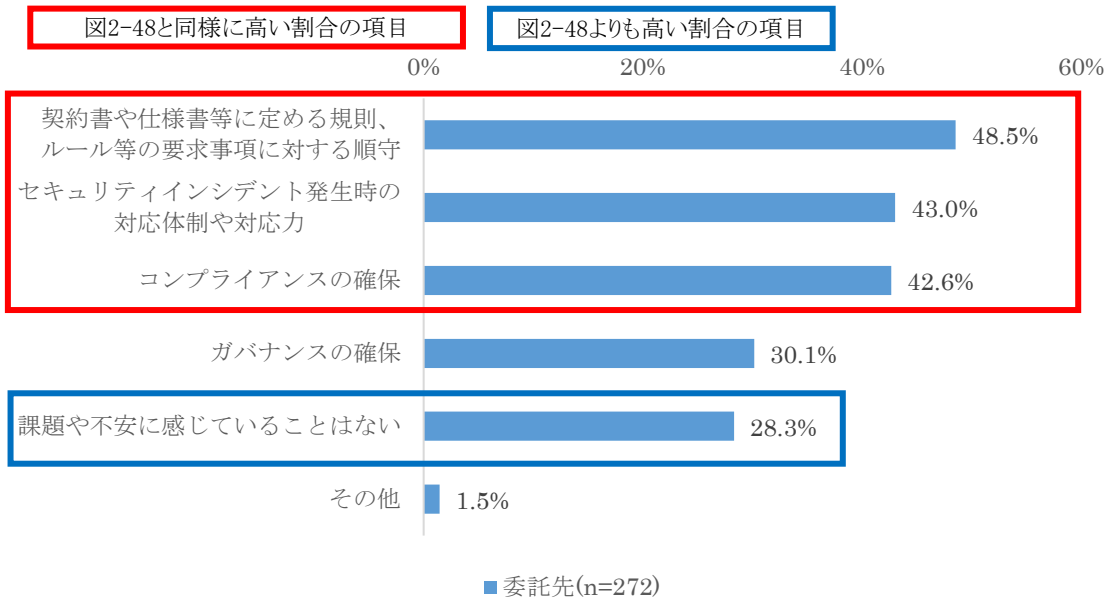
任はすべて当該委託先の負担となる可能性があるため、委託先は再委託先に対して強い課題意識を有していると考えられる。

図 2-49：新たな再委託先に関する課題・不安（組織調査 Q42）



さらに、図 2-50 より、委託先は新たな委託元に対して、「契約書や仕様書等に定める規則・ルール等の要求事項に対する遵守」、「セキュリティインシデント発生時の対応体制や対応力」、「コンプライアンスの確保」の課題や不安を感じている割合が高いことが明らかになった。それぞれの項目の回答割合は図 2-49 の方が高いものの、図 2-49 と同様の傾向が確認された。また、「課題や不安に感じていることはない」の回答割合は、図 2-49 の結果よりも高くなっており、委託先においては、新規の委託元よりも新規の委託先に対してより強く課題や不安を感じている傾向がある。

図 2-50：新たな委託元に関する課題・不安（委託先）（組織調査 Q42）



2.6.2 まとめ（「委託先へのセキュリティ対策要求等の変化」について）

現時点で、委託元がニューノーマルへの対応に向け、委託先に対してセキュリティ対策に関する要求を強化している明確な実態は確認できなかったものの、BYOD やテレワークに関する要求事項や、各種の要求事項の順守状況のレビュー・要求事項に適合する証跡の提出等に関する要求事項について検討する必要があると感じている組織が存在することが確認できた。また、4 割以上の委託元が、委託先に対して、「契約書や仕様書等に定める規則・ルール等の要求事項に対する遵守」や「セキュリティインシデント発生時の対応体制や対応力」について課題や不安を感じていた。以上を踏まえ、今後の委託元による検討の結果次第で、委託先の情報セキュリティリスクを低減するためのセキュリティ対策の要求事項が、テレワーク等に関する要求事項の増加や、既存の要求事項の順守状況の確認、セキュリティインシデント発生時の対応体制・対応力等の観点で、強化されていく可能性があると考えられる。

2020 年度における委託先と委託先間の契約は、緊急事態宣言が発出された 2020 年 4 月以前に締結されたものであるため、テレワーク等のニューノーマルに対応するための要求事項が契約に盛り込まれていなかったことが予測される。取引先との契約締結後に、急遽双方の ICT 環境の変化が余儀なくされ、新たなセキュリティ脅威が生じ、脆弱性が発見されることも想定されるため、今後の契約の際には、情報セキュリティリスク低減のため、委託元から委託先への要求事項が強化される可能性がある。

3 課題と対応

本調査によって、ニューノーマルへの対応に伴い変化した情報セキュリティリスクについては正確な把握が難しいことや、テレワークなどを急ぎ導入せざるを得なかったことから、情報セキュリティリスクに対応するための組織の管理体制やルールの整備ができていない（もしくは進んでいない)、また、規程やルールの適切な運用が難しいケースが多く存在することが明らかになった。やむなく認めざるを得なかった特例や例外がそのままの状態で長く続くことは、セキュリティリスクが増大している可能性があり、インシデントの発生が危惧される。

特に中小規模の委託元においては、自社内のガバナンス・マネジメント、及び、委託先を管理するために必要となる IT 関連の知識が不足しているケースが多いことが伺える結果となった。委託元と委託先のセキュリティ対策レベルの差があることを認識せずに機密情報のやり取りなどをしていると情報漏えいなどが懸念される。IT サプライチェーンの起点となる委託元のこのような課題は、IT サプライチェーン全体の情報セキュリティリスクを高めてしまうことが懸念されることから早急な対策が求められよう。また、委託元から委託先に対しては、委託先におけるニューノーマルへの対応に起因して発生しうる情報漏えい等への適切な対策を求める声も多い。しかし、契約や仕様などで具体的な対策の明示や状況の確認はまだされていないことが多く、課題と考えられる。

本章では、それぞれの課題を解説した上で、それらの課題解消のため今後必要となる対応、委託元・委託先に対する提言について記載している。

3.1 ニューノーマルにおけるセキュリティ上の課題

今回の「２．調査結果」から抽出した主な課題については（図 3-1）の通りである。以降では、これら抽出した課題ごとにその内容を記載する。

図 3-1： 調査仮説と抽出した課題

調査仮説（第二章構成）	抽出した主な課題
2.1「セキュリティガバナンス/コンプライアンスの低下」について	① セキュリティガバナンス/コンプライアンスの低下
2.2「ルール・運用、マネジメント力の低下」について	② ニューノーマルへの規程・業務等の対応の遅れ
2.3「今後想定されるセキュリティ脅威や情報セキュリティリスク（セキュリティインシデントの増加を含む）」について	③ セキュリティインシデントの把握・検知能力の不足
2.4「組織と従業員の責任分界点」について	④ BYOD 利用時の責任分界点の曖昧さ
2.5「委託先選定、再委託先許諾への影響」について	⑤ 契約上の要求事項の対応の遅れ
2.6「委託先へのセキュリティ対策要求等の変化」について	

① セキュリティガバナンス/コンプライアンスの低下

ニューノーマルへの対応に伴い、多くの組織においてセキュリティガバナンス/コンプライアンスの低下が起きている可能性が高いことが想定される結果となった。

組織調査では、緊急事態宣言発出以降にテレワークを導入した組織における課題として「従業員のルール順守状況の確認が難しくなった」との回答が 6 割近く存在していることが分かっており、ルール順守のためのマネジメント方法が確立できておらず、従業員に対してガバナンスを効かせることができていない状況が伺える。特に中小規模の委託元では、テレワークの実施に向けたセキュリティ対策としての「情報の機密レベル分けに応じたアクセス制御等の情報管理」に監視、現時点でも約 5 割がルールを策定していないなど、コロナ禍以前からテレワーク普及率の高い委託先と比較して課題が大きい。

また、有識者インタビュー結果からも、テレワークの導入により、従業員の作業環境・場所を完全に把握することができなくなったことで、従業員に対してガバナンスを効かせることが難しくなっているとのご意見があった。特に日本型組織の特徴と指摘される、従業員相互に協働して業務を進める働き方が主流のケースでは、個々の従業員の責任範囲が曖昧であること、多くの関係者間で情報を共有するために重要な情報がメール等でやり取りされる場面が多くなることなどを要因として、テレワーク実施時の適切なルール運用（マネジメント）が難しく、組織としてガバナンスを効かせにくいため情報セキュリティリスクが高まる状況にあることが指摘されている。

本調査では、テレワークへの急速な移行に伴い、組織から従業員に支給するIT機器（PCやカメラ、マイク等）の調達が間に合わないという事象が発生し、調達が完了するまでの“つなぎ”の期間において一時的に適切なルールの運用（マネジメント）ができずセキュリティ水準のレベルが低下する事態が発生していることも示唆された。例えばインタビュー調査を実施した某委託先では、コロナ禍以前からテレワーク実施に際して仮想デスクトップ方式（以下VDI）を採用していたが、第一回目の緊急事態宣言時に多くの従業員が在宅でのテレワークに移行した際、VDI回線がひっ迫し利用者を制限せざるを得なかったため、一時的に外部SaaSサービスの利用を許可したとの話も伺うことができた。投資余力の関係でセキュアなIT環境整備への対応が難しい組織においては、緊急対応的に許可した情報セキュリティリスクの高いサービスの利用がそのまま継続されている等、適切なマネジメントがなされない状態が常態化している懸念もある。

さらに、ニューノーマルへの対応に伴うコンプライアンスの低下も懸念される。有識者インタビューからは、テレワーク勤務中では、他者による監視の抑止効果がないために業務と無関係の行為（業務とは関係のないウェブサイトの閲覧等）が誘発されやすくなることや、組織内でのオンライン飲み会の普及に伴って業務時間の切り換えの問題やハラスメント等の問題が発生しやすくなるなど、ガバナンス/コンプライアンスが形骸化している可能性があるとの指摘もあった。

② ニューノーマルへの規程・業務等の対応の遅れ

ニューノーマルへの移行に際してテレワークなどを急ぎ導入せざるを得なかったことから、規程やルールの制定が進んでいない組織や、そもそもの業務の進め方自体がテレワークに対応しきれていない組織が存在することが想定される結果となった。

アンケート調査からは、テレワークの情報セキュリティを確保するためのルール（テレワークの場所、テレワークで使用が可能な情報の機密レベル等）を定めずに、テレワークを継続して導入している組織が一定数存在することが確認できている。また、有識者インタビューからも、関連する規程やルールを整備・周知できていないまま現在に至っている組織が多いとのコメントの他、テレワークへの移行に伴いルール整備している組織としていない組織との間に、情報セキュリティを確保する上でのルールの整備状況や、それらルールの従業員理解や周知における課題認識にギャップが生じているとの意見もあった。インタビューを実施した委託先からは、テレワークを採用しているもののルールが未整備な委託元に対して、電子ファイルとして情報を渡して良いのか等の課題感を持っているとの声も上がっている。また、組織調査ではBYOD利用に際して、ルールが全く定められていないとの回答も一定数存在し、適切なルールの運用がなされていない状況にあることが示唆される。

また、現在委託元が委託先に対して特定の場所で業務を実施することを条件とした取り決めを行っているケースも多い。今後、テレワークによる勤務形態が一般化する中で、委託

元として委託先に対しどのような管理を実施し、そのためにどのような取り決めをするべきかについて検討する必要がある。

その他、有識者インタビューでは緊急事態宣言でテレワークへ急速に移行したものの、コロナ禍以前から社内コミュニケーションにチャットツール等をうまく活用できていなかった組織においては、ニューノーマルへの業務対応が難しく、第一回目の緊急事態宣言終了後に勤務体制を戻した組織も存在するとのお話を伺うことができた。課題①でも触れた通り、従業員相互に協働して業務を進める働き方が主流の日本型組織では、個々の従業員の業務・責任範囲が曖昧であることや対面でのコミュニケーションを重視する傾向がある。テレワーク移行時には個々の従業員の業務と取り扱う情報の範囲を明確に規定する必要があるが、日本型組織の業務の進め方ではそれが難しい。また、組織内外のコミュニケーションについても、対面でのコミュニケーションを重視している場合オンラインで完結させることが難しいなど、業務のあり方そのものがニューノーマルへの対応が難しいケースが多いことが伺える。

③　セキュリティインシデントの把握・検知能力の不足

ニューノーマルへの対応に伴い、発生したセキュリティインシデントを検知することが困難となっていること、また、組織において今後想定されるセキュリティ脅威や情報セキュリティリスクを把握しきれていないことが懸念される結果となった。

内部不正については、テレワーク導入後もその発生件数に「増減はなし」と回答している組織が多い一方で、そもそも「把握できてない」という回答も一定割合存在している。また、緊急事態宣言発出以降にテレワークを導入した組織における課題として「従業員のルール順守状況の確認が難しくなった」との回答が多く、その実態を把握しきれていない状況にある。有識者インタビューでは、「明確な内部不正は簡単には従業員も行うことはないが、テレワーク、BYOD 等の活用によって、勤務状況を全く見られていない中、従業員が無意識の内に情報セキュリティリスクを発生させている可能性がある」との指摘があった。例えばテレワーク勤務中では、他者による監視の抑止効果がないために、従業員が業務とは無関係なウェブサイト等に業務端末からアクセスする危険性が高いといえる。さらに、委託先インタビューからも、「管理者（第三者）がいない中どのように労務管理するか苦慮している。また、テレワークでは、ツール等の使用による PC ログ取得を基にセキュリティ上の違反行為がないかを満足に確認することができない。セキュリティ上のリスクは高くなったと言える。」との意見も伺うことができた。2016 年 3 月に独立行政法人経済産業研究所から公表されたディスカッションペーパー[11]によると、「技術ノウハウの流出パターン」として最も多

[11] 「日本企業の技術ノウハウの保有状況と流出実態に関する質問票調査」

いのが「自社退職従業員」となっており、テレワーク勤務による孤立した環境は、これら「自社退職従業員」経由での情報流出を増加させる要因となり得る。

内部不正の他、総務省が公表している「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）」の中では、テレワーク環境において「マルウェア感染」「不正アクセス」「盗難・紛失」「情報の盗聴」といった外部からの脅威が想定されるとの記載があり、今後テレワークが一般化することでこれらの脅威が増加する可能性が高いと言えよう。しかしながら、これらの脅威への対策として、自社でルールを整備していたとしても、取引先のルール制定状況とのギャップによりルール順守が困難なケースが発生することも多いと想定される。例えばウェブ会議ツールについては、特に中小規模の委託元にて各ルールが制定されていない割合が高く、委託元と委託先で会議する場合など、結果として委託先自身が制定したルールの遵守が困難である事態が発生している可能性が高い。さらに、委託元から見た場合、委託先の行動が変化したことによる「必要な IT 知識の急速な増加」が課題として挙げられており、ニューノーマルにおける ICT 環境の急激な変化に対して、委託元の知識習得が追い付いていないことが懸念される。IT サプライチェーンの起点となる委託元におけるこれらの課題は、IT サプライチェーン全体の情報セキュリティリスクを増加させる一つの要因になる可能性がある。

④ BYOD 利用時の責任分界点の曖昧さ

特に BYOD の利用を認めている組織においては、組織と従業員の責任分界点が曖昧なケースが多く、セキュリティインシデント発生後の対応が困難になることが懸念される結果となった。

組織調査では、従業員が利用する端末の把握やその端末へ規則を適用させることが困難であると感じている組織が多いことが明らかになっている。また、個人調査にて、BYOD の利用時に発生した個人の責任となる不安があるセキュリティインシデントを確認したところ、「不安に思うことはない」の割合が約 3 割であり、残りの約 7 割は、何かしらのセキュリティインシデントが発生した際は個人の責任になる不安を感じていることが明らかになった。このように、組織と従業員の責任分界点が曖昧であることから、利用されている BYOD 端末に対して組織として行使できる権限が不明確な状況にあり、仮にセキュリティインシデントが発生した際には、影響範囲を特定するためのフォレンジック等、組織として実施すべき調査が難航することが予測される。

⑤　契約上の要求事項の対応の遅れ

現時点においては、ニューノーマルの対応で増加したテレワークの導入、ウェブ会議ツールの使用、BYOD の使用などに関する契約上の要求事項について検討が進んでいないケースが多いことが想定される結果となった。一方で、BYOD やテレワークに関する要求事項や、各種の要求事項の順守状況のレビュー・要求事項に適合する証跡の提出等に関する要求事項について検討する必要があると感じている組織は、委託元・委託先ともに多い。そのため、今後の契約に向けては、情報セキュリティリスク低減に向けた要求事項を如何にして契約書案に盛り込むことができるかがポイントとなる。

3.2 今後必要となる対応

本調査では、委託先については既に大半の組織においてテレワークが導入され、ウェブ会議ツールを利用したコミュニケーションのオンライン化も相当程度定着していることが伺える結果となった。委託元については委託先程ではないものの、テレワークの導入やウェブ会議ツールの利用は着実に拡大しており、今後は委託先・委託元間での取引円滑化を図る意味でもこれらニューノーマルへの対応は委託先、委託元双方で不可逆的な変化として定着するものと想定される。そのため、本調査で整理したニューノーマルにおけるセキュリティ上の課題については早急な対応が必要となる。インタビューで得られた結果も踏まえ、課題についてあるべき対応方針を整理した（図 3-2 図 3-2：課題と対応方針の関係）。以下、それぞれの対応方針について概要を記載する。

図 3-2：課題と対応方針の関係

課題	課題への対応方針				
	Ⅰ．業務自体の改革・改善	Ⅱ．社内規定・ルールの整備	Ⅲ．ルールの周知・教育	Ⅳ．ICT環境整備	Ⅴ．業務委託契約条項の改定
①セキュリティガバナンス・コンプライアンスの低下	○	○	○	○	―
②ニューノーマルへの規定・業務等の対応の遅れ	○	○	―	―	―
③セキュリティインシデントの把握・検知能力の不足	○	○	○	○	○
④BYOD利用時の責任分界点の曖昧さ	―	○	○	○	―
⑤契約上の要求事項の対応の遅れ	―	―	―	―	○

【凡例】○：課題解決に資すると想定される対応方針

Ⅰ．業務自体の改革・改善

本調査においては、従業員相互に協働して業務を進める働き方が主流の日本型組織では、テレワークに移行した際の円滑な業務遂行が難しい、もしくはセキュリティインシデント発生の可能性が高まることが指摘されている。日本型組織がテレワークを導入した場合、個々の従業員に責任範囲が曖昧であることや、仕事を進める際に多くの情報を共有しなくてはならないため、自然と重要な情報がメール等で多くの関係者間でやり取りされる傾向が強い。結果、重要情報が不特定多数の関係者にまで広がってしまい、情報保有者を明確に把握しきれなくなることから、情報保有者に対してのガバナンスを効かせることが難しくなる。また、不特定多数の関係者それぞれが重要情報を保管することになるため、その分セキュリティインシデントの脅威も増加することが想定される。また、テレワーク中の情報共

有に支障を来たし、緊急事態前言終了後に以前のワークスタイルに回帰するなどニューノーマルへの対応が難しい組織も存在する。

インタビューでは、セキュリティガバナンスの確保やニューノーマルへの対応が容易な組織の特徴として、以下の要素が挙げられている。

- 働き方として、従業員個々人の責任・業務範囲が明確なプロフェッショナルワークになっている組織の場合、仕事の責任範囲が明確で契約等で管理し易く、リスクも把握しやすい
- コミュニケーションツール（チャットツール等）をうまく活用して情報を共有している組織の場合、テレワークへの移行に伴うインパクトは比較的小さく、ニューノーマルへの対応が容易

このように、ニューノーマルに対応するためには、従業員個々人の責任・業務範囲を明確するための業務自体の改革と、コミュニケーションをオンラインで完結可能とするための業務改善が必要となる。まずはコミュニケーションをオンライン上で完結させることを前提とした業務改善を行うことで、ニューノーマルでの従業員相互の協働作業を円滑にすることができ、ガバナンスの確保も可能となることが期待される。また、業務自体の改革については業種ごとの特性や組織戦略上の判断もあり時間を要するが、ニューノーマルにおける情報セキュリティリスクに対応するためにも着実かつ計画的に実行していく必要がある。

Ⅱ．社内規程・ルールの整備

ニューノーマルに対応した社内規定の整備については、既存のガイドライン等を参照することによりある程度の網羅性を担保した取り組みが可能になると想定される。テレワーク導入やウェブ会議システム、BYOD 利用に伴う情報セキュリティリスクへの対応のためにも、自組織の状況に合わせ、ガイドライン等を参考に社内規程・ルールを整備することが望まれる。様々な機関から関連する文書が公表されているが、図 3-3 にて代表的な文書を挙げる。ちなみに、組織調査ではテレワーク導入組織に対して参考にしたガイドラインを問う設問も実施しており、テレワーク導入組織の 4 割強が「テレワークセキュリティガイドライン（総務省）」を参考にしたと回答している。

図 3-3：関連ガイドライン・ホームページ概要

ガイドライン名・ホームページ	発行元・運用者	概要
テレワークセキュリティガイドライン第4版	総務省	テレワークにおける情報セキュリティ対策の考え方、対策のポイント、テレワークトラブル事例と対策一覧などがまとめられている
テレワーク時における秘密情報管理のポイント	経済産業省	テレワークに対応した規程の整備等について、Q&A形式でまとめられている
サイバーセキュリティ経営ガイドラインVer2.0 実践のためのプラクティス集 第2版	IPA	テレワークへの対応を前提としたものではないが、サイバーセキュリティリスクに対応するためのポリシーや規程改訂について、具体的な改訂プロセスを含むプラクティスが掲載されている
中小企業の情報セキュリティ対策ガイドライン	IPA	一般的な情報セキュリティ規程の作成手順についての解説や、情報セキュリティ関連規程のサンプル（付録5）を参照することができる
テレワークモデル就業規則～作成の手引き～	厚生労働省	テレワーク導入の際に検討が必要な就業規則についての考え方や、参考すべき規定例、組織におけるセキュリティガイドライン策定の必要性等のがまとめられている
テレワークのガイド・事例等（https://japan-telework.or.jp/suguwakaru/guide/）	一般社団法人日本テレワーク協会	テレワーク導入の際に参考となる各種ガイドラインや事例集等が掲載されている
みんなでしっかりサイバーセキュリティ（https://www.nisc.go.jp/security-site/telework/index.html）	内閣サイバーセキュリティセンター	テレワーク実施者を対象とし、情報セキュリティを確保するための対策や注意点を簡易に説明している

Ⅲ．ルールの周知・教育

3.1 章「②ニューノーマルへの規程・業務等の対応の遅れ」でも述べた通り、社内規程・ルールの整備がなされたとしても、それらの周知がなされずに従業員の理解が不足しているケースが多く存在する。特にテレワーク等のニューノーマルな働き方に移行している場合、従業員における社内規程・ルールの周知・理解を担保するための仕組みが重要となる。

インタビューにおいては、従業員に対して、在宅勤務時の規則等について E ラーニングでの訓練実施や、セキュリティインシデント発生時の連絡ルートを整備することが、従業員の不安払拭にも重要であるとの意見があった。「テレワークセキュリティガイドライン 第4版」（総務省）では、従業員の教育・啓発に関して、以下の様な対策例が挙げられている。

- 分かりやすい「メッセージ」を作成し、イントラネット内で通知したり、テレワーク勤務者が目をとめやすいところにポスターとして掲示したりすること等により、常に意識させる
- テレワーク先で緊急事態が発生した場合の連絡先等は、名刺サイズのカードの形で印刷して配布することで、テレワーク勤務者に常に携帯してもらう
- 就業規則等にテレワーク時の機密保持とその違反時の罰則に関する規定を定めるとともに、ルール遵守のメリットを理解してもらう

Ⅳ．ICT 環境の整備

テレワークより第三者の監視の目が届きにくい従業員に対するガバナンスの確保や、発生したセキュリティインシデントを適宜検知するためには、相応の ICT 環境の整備が必要になる。

情報セキュリティ水準を確保するため ICT 環境については、業種・業務の特性の他、投資余力や社内の ICT 環境検討人材の有無など、各組織が置かれている状況によって取り得る対策が異なる。特に投資余力の小さい事業者においては、BYOD の利用を前提とせざるを得ないケースも存在することが想定され、セキュリティ水準と ICT 環境への投資可能金額がトレードオフの関係になってしまうことが危惧される。

特に重要となるのが、従業員が利用する端末の運用方式であり、「中小企業等担当者向けテレワークセキュリティの手引き（初版）」（総務省）では図 3-4 の通り分類がなされている。このうち、BYOD 端末の利用が想定されているのが方式⑤～方式⑧の 4 つとなり、「⑦会社非接続方式（手元作業型）」以外は、BYOD 端末に電子データを保存しない形とできるため、比較的セキュリティインシデントにつながりにくいといえる。

図 3-4：テレワーク方式の概要

方式		オフィスネットワークへの接続方式	クラウドサービス利用	テレワーク端末へのデータ保存	概要
方式①	会社支給機器を使った、VPN／リモートデスクトップ方式	VPN、リモートデスクトップ等	利用する/利用しないどちらも含む	保存する ※リモートデスクトップ接続の場合は「保存しない」場合も含む	会社支給のテレワーク端末からオフィスネットワークにVPN接続し、業務を行う方式。 または、会社支給のテレワーク端末からオフィスネットワークにリモートデスクトップ接続し、業務を行う方式。 いずれの場合も手元端末上で作業をするケースも含む。
方式②	会社支給機器を使った、会社非接続方式（クラウドサービス型）	接続しない	利用する	保存する/保存しないどちらも含む	会社支給のテレワーク端末から、インターネット上のクラウドサービスで提供されるアプリケーションソフトウェアにアクセスし、業務を行う方式。手元端末上で作業を実施するケースも含む。
方式③	会社支給機器を使った、会社非接続方式（手元作業型）	接続しない	利用しない	保存する	会社支給のテレワーク端末をテレワーク環境に持ち出して、あらかじめ保存しておいたファイルの編集・閲覧作業のみを手元端末上で実施し、業務を行う方式。
方式④	会社支給機器を使った、セキュアブラウザ方式（安全なインターネット活用を促進する機能を備えたWebブラウザの利用）	セキュアブラウザ	利用する	保存しない	会社支給のテレワーク端末から、特殊なセキュアブラウザ（手元端末へのデータ保存制限等）を活用し、社内システムやクラウドサービスのアプリケーションソフトウェアにアクセスし、業務を行う方式。
方式⑤	個人所有機器を使った、VPN／リモートデスクトップ方式	VPN、リモートデスクトップ等	利用する/利用しないどちらも含む	保存する ※リモートデスクトップ接続の場合は「保存しない」場合も含む	従業員所有のテレワーク端末からオフィスネットワークにVPN接続し、業務を行う方式。手元端末上で作業を実施するケースも含む。 または、従業員所有のテレワーク端末からオフィスネットワークにリモートデスクトップ接続し、業務を行う方式。 いずれの場合も手元端末上で作業をするケースも含む。
方式⑥	個人所有機器を使った、会社非接続方式（クラウドサービス型）	接続しない	利用する	保存する/保存しないどちらも含む	従業員所有のテレワーク端末から、インターネット上のクラウドサービスで提供されるアプリケーションソフトウェアにアクセスし、業務を行う方式。手元端末上で作業をするケースも含む。
方式⑦	個人所有機器を使った、会社非接続方式（手元作業型）	接続しない	利用しない	保存する	従業員所有のテレワーク端末をテレワーク環境に持ち出して、あらかじめ保存しておいたファイルの編集・閲覧作業のみを手元端末上で実施し、業務を行う方式。
方式⑧	個人所有機器を使った、セキュアブラウザ方式（安全なインターネット活用を促進する機能を備えたWebブラウザの利用）	セキュアブラウザ	利用する	保存しない	従業員所有のテレワーク端末から、特殊なセキュアブラウザ（手元端末へのデータ保存制限等）を活用し、社内システムやクラウドサービスのアプリケーションソフトウェアにアクセスし、業務を行う方式。

出展：「中小企業等担当者向けテレワークセキュリティの手引き（初版）」（総務省）

また、一般社団法人日本テレワーク協会が公表している「中堅・中小企業におすすめのテレワーク製品一覧」には、どのようなICT環境を整備すべきかについての解説がなされている。同資料では、中堅・中小企業がテレワークを実現するために最低限必要なシステム何かという問いに対し、テレワークに必要な最低限の環境として、ハードウェア環境とソフトウェア環境それぞれについての解説とともに、安全なテレワーク環境実現方式や関連するシステムの紹介が記載されており、ICT環境整備の際の参考資料として活用できる。

Ⅴ．業務委託契約条項の改定

コロナ禍の中で業務継続が優先されたことにより、2020 年度の業務委託契約については、委託元と委託先間で締結された契約条項の一部逸脱を許容せざるを得ないケースや、そもそもコロナ禍によるニューノーマルへの対応が想定されていないことから生じる業務実態と契約での要求事項とのミスマッチが放置されていたケースが多いことが想定される。コロナ禍の影響は 2021 年度以降も継続すると想定されることから、IT サプライチェーン上の情報セキュリティリスク低減し、セキュリティ水準を確保するために必要な条項を今後の契約内容に盛り込む必要がある。

具体的な契約内容については、IPA が 2021 年 1 月に公開した「情報システム・モデル取引・契約書」第二版（以下、モデル契約書）が参考になると考えられる。モデル契約書では、委託元及び委託先の責任者がソフトウェアに具備するセキュリティ仕様を決定する権限と責任を有することが明記された。また、セキュリティ条項について大幅な見直しが行われており、例えば、一旦確定したセキュリティ仕様であってもソフトウェア開発業務の工程で見直しを余儀なくされることも考えられるため、変更管理の手続によって変更できることが明記されている。さらに、IPA ではモデル契約書に合わせて、情報システム調達に伴うシステム開発業務プロセスにおいて、最適なセキュリティ仕様を策定する為の理想的なモデルプロセスを解説した「セキュリティ仕様策定プロセス」（以下、モデルプロセス）を公開している。今後の契約の締結の際には、本モデル契約書やモデルプロセス（特に以下の観点で参考にいただきたい）を参考に、契約条項を検討してくことが望まれる。

- 企画支援プロセス：RFP 作成時に、非機能要件となる「作業環境」としてテレワークや BYOD の可否を確認すること。可とする場合は、セキュリティ対策の要件の検討をおこなうこと
- 要件定義作成支援プロセス：外部委託先の作業環境について具体的に定義すること
- 運用業務プロセス：定められた通りの環境で業務が実施されていることを確認すること

4　提言

我が国においては、コロナ禍以前から働き方改革が声高に叫ばれており、政府においてもワーク・ライフ・バランスの実現、人口減少時代における労働力人口の確保、地域の活性化、非常時における業務継続の確保などを目的として関係府省が連携してテレワークの普及・推進が図られてきたが、コロナ禍により期せずしてテレワークへの急速な移行が実現されることとなった。これまでにも生産性向上の観点からペーパーレス化やハンコレス化など、テレワークとの親和性が高い各種ソリューションが存在していたが、テレワークへの移行に伴いそれらソリューションを導入・定着した組織では、従業員が出社する必然性は確実に低くなっていると考えられる。さらに、昨今ではテレワークへの移行に伴い物理的なオフィスの縮小を図る組織が増えているとの報道もある。これらの組織は、新型コロナ感染拡大防止のための一時的な対応ではなく、恒久的な勤務体系としてテレワークを位置づけたと考えられる。本調査では、特に委託先においてテレワークへの移行が進んでいることが分かっているが、前述背景を鑑みた場合、この変化は不可逆的なものになると想定される。まだテレワークへの移行が限定的な委託元においても、委託先の変化に合わせる形で、コミュニケーションや提供サービスのオンライン化など含めたニューノーマルへの対応が常態化することを前提とした対策を講じる必要がある。

特に中小規模の委託元については、ニューノーマルへの対応に伴い必要となる社内規程やルールが整備できていないケースが多くみられる結果となった。「1.2　今後必要となる対応」中の「Ⅱ．社内規程・ルールの整備」でも述べた通り、まずは既存のガイドライン等を参考とした社内規程・ルールの整備が急務であると考える。その後、それらの社内規程・ルールを適切に運用するための「Ⅲ．ルールの周知・教育」や、投資余力等の組織特性に応じた「Ⅳ．ICT 環境の整備」を推進していくことが望まれる。

委託先においても、IT サプライチェーン上の情報セキュリティリスクを低減させるためには自組織に閉じた社内規程・ルールの整備や適切な運用のみならず、委託元や再委託先における社内規程・ルールとの整合を意識し、場合よっては委託元に対してその必要性を啓発しながら対応を促していくことが必要となる。

また、「Ⅴ．業務委託契約条項の改定」でも述べた通り、ニューノーマルへの対応後の業務実態と契約での要求事項とのミスマッチを解消するため、委託元と委託先双方が協働してセキュリティ水準を確保するために必要な条項を今後の契約内容に盛り込む活動が求められる。委託元から委託先に対して適切なガバナンスを効かせるためには、契約上の要求事項として、例えばどの業務においてどのような条件の基テレワークの実施を認めるのかを明確にすることも重要になる。

今後、ニューノーマルへの対応が常態化することにより、組織の物理的な活動範囲はコロナ禍以前と比較して各段に拡大することとなる。その際には、一定の対応を行ったとしても従来の業務遂行方法を継続している限り情報セキュリティ水準の維持が難しい場面が出て

くることが想定される。そのため、3.2 章「Ⅰ．業務自体の改革・改善」でも述べた通り、中長期的には従業員個々人の責任・業務範囲を明確にする業務自体の改革が必要となる。

また、多くの組織でテレワーク実施時に採用されているリモートデスクトップ方式では利用者増加により VPN 回線のトラフィックが増加し速度遅延等が発生しうることや、情報セキュリティ上の懸念からテレワーク環境下において利便性の高い社外クラウドサービス等の利用を制限し続けることが、事業の効率性・競争力維持の観点から大きな問題になると想定され、今後は、如何にして情報セキュリティ水準の維持と利便性を両立して業務を遂行できるかがポイントとなる。

近年、「ゼロトラスト」と呼ばれる情報セキュリティ上の概念が急速に広まりつつある。これは、組織内ネットワークと外部ネットワークを分け、信頼できる組織内ネットワークへの外部からの侵入を防止する従来の「境界型セキュリティ」の考え方とは違い、内部・外部を区別することなく、あらゆる方向からの脅威を前提として全ての利用者・端末・ネットワークを監視し、アクセスの都度ユーザー・デバイスの認証を必要とする考え方である。あらゆる場所・デバイスからのアクセスを前提としているという点において、ニューノーマルにおける業務実施場所の多様化と親和性の高い概念と言えよう。2020 年 6 月に公表された「政府情報システムにおけるゼロトラスト適用に向けた考え方」の中では、利便性を保ちながら、クラウド活用や働き方の多様化に対応する方法として、政府の情報システムにおいてゼロトラストを適用するための取り組み方の方向性が示されており、今後官民両面で検討が進んでいくものと想定される。「ゼロトラスト」がニューノーマル時代の情報セキュリティ対策の答えになるかは現時点では明確には言えないが、少なくとも情報セキュリティ水準の維持と利便性を両立した新たな対策の形を模索していく必要があろう。

以上