# 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 概要説明資料

2021年4月

独立行政法人　情報処理推進機構
セキュリティセンター
セキュリティ対策推進部
分析グループ

# 目次

# １．調査実施概要

# 背景・目的

**背景**

- 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が発出され、約2か月間に及ぶ外出自粛が実施された
- 緊急事態宣言をきっかけに職場以外の環境での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）など、いわゆる「ニューノーマル」に対応した組織が急増することとなった
- 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結果、セキュリティ対策が疎かになっているケースも多いと想定される

**目的**

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

# 調査対象（1/2）

- 本調査において対象とする“ニューノーマル”の範囲を、「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」であると設定し、ニューノーマルへの対応によって引き起こされる組織・個人への変化を抽出している。

**本調査における<br>ニューノーマル**

**①業務実施場所の多様化**

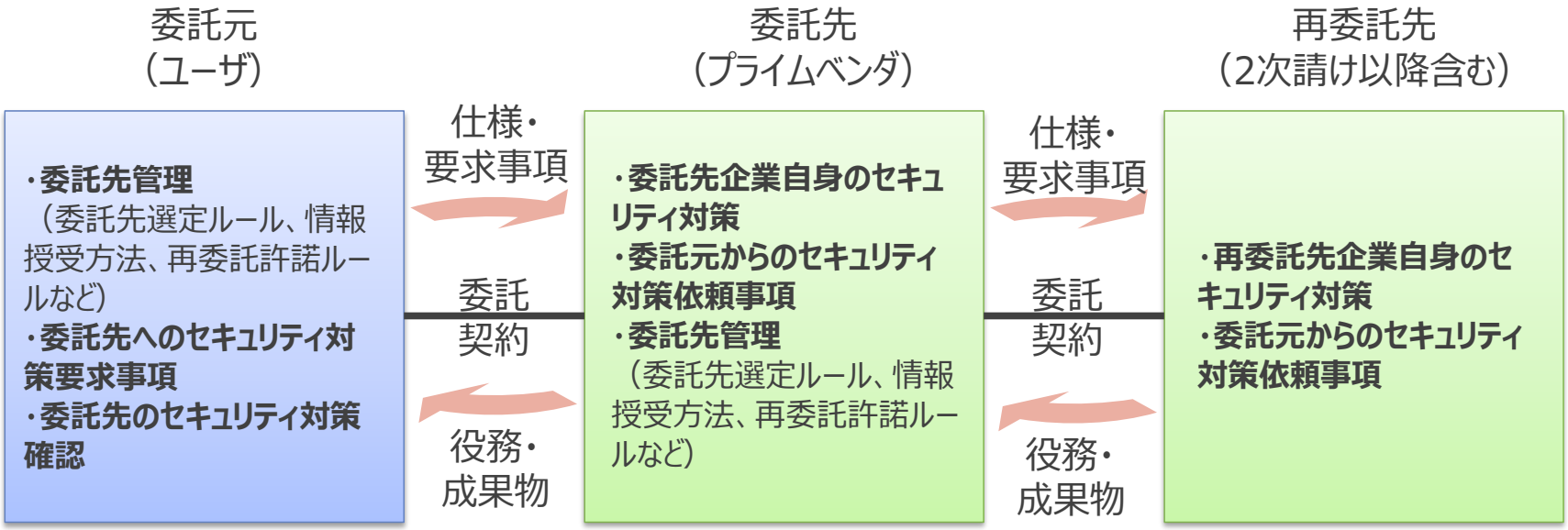
**②コミュニケーションのオンライン化**

| 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<br>（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<br>（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<br>（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<br>（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<br>（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

# 調査対象（2/2）

- 本調査では、ICT環境変化による影響が大きいと思われる委託元と委託先（プライムベンダ）との関係を中心に、ITサプライチェーン（※）に及ぼすであろう情報セキュリティ上の課題を検証することとした。




※ ITサプライチェーン：「IT システム・サービスに関する業務を系列企業やビジネスパートナー等に外部委託し、 その業務委託が、委託先企業の再委託先、再々委託先へと連鎖する委託形態」

# 調査実施概要__アンケート調査

個人向けアンケート（以下、個人調査）、企業・組織向けアンケート調査（以下、組織調査）をそれぞれ実施した。

## 個人調査概要

- <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>
  - 2020年11月2日～11月13日
- <有効回答者数>
  - 2,372人
    - IT企業の従業員・大規模（101人以上）：717人
    - IT企業の従業員・中小規模（100人以下）：610人
    - IT企業以外の組織の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

## 組織調査概要

- <方法>
  - 郵送アンケートとウェブアンケートの併用
- <対象>
  - 企業データベース等から抽出した企業・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）・総従業員数／職員数101人以上の企業・大規模：139社
    - 委託先（IT企業）・総従業員数／職員数が20人以上100人以下の企業・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

# 調査実施概要__インタビュー調査

- インタビュー調査概要
- <方法>
  - 会議ツールを使ったインタビュー

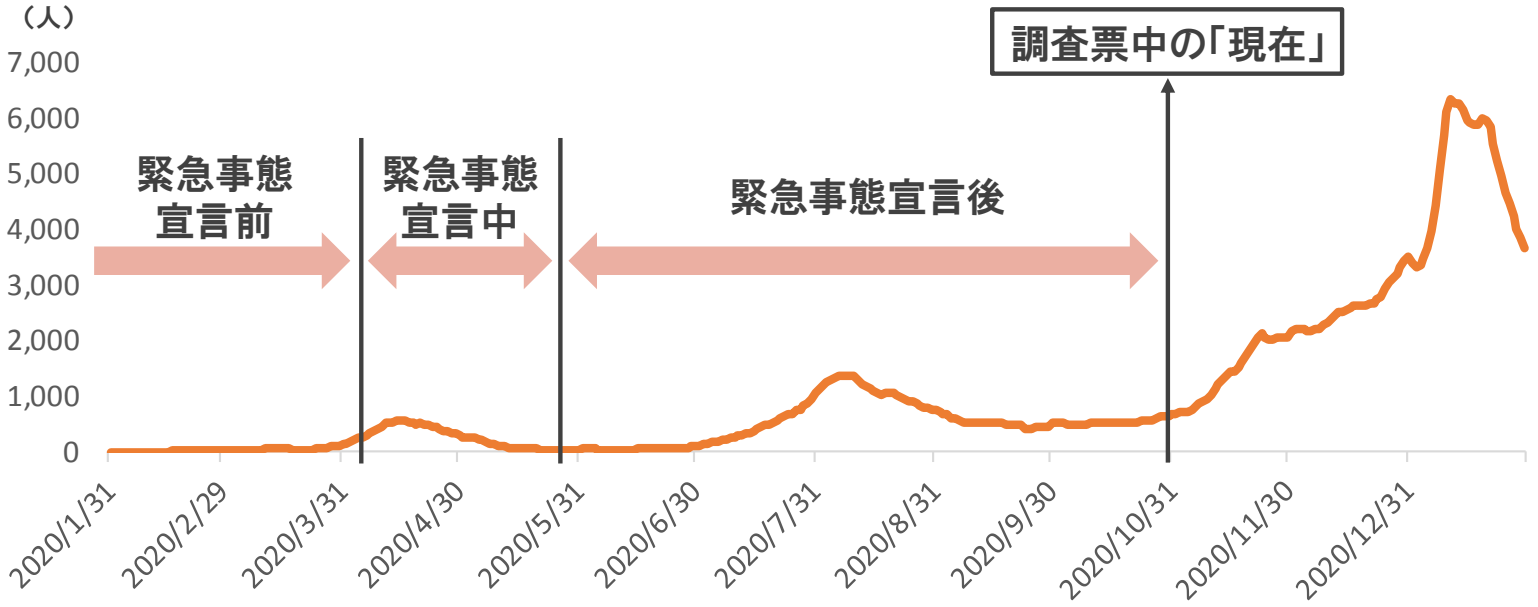
- <対象>
  - セキュリティの専門家、IT企業の経営層、テレワークの専門家、委託元、委託先

- <期間>
  - 2020年10月6日～2021年2月16日

- <回答者>
  - 9人
    - セキュリティの専門家：3名
    - IT企業の経営層：1名
    - テレワークの専門家：1名
    - 委託元(IT企業)：1名、委託元（製造業)：１名
    - 委託先(IT企業)：2名

# （参考）国内の新型コロナウイルス陽性者数推移（週次平均）

- 個人・組織調査における「現在」を、 「2020年10月31日」と定義して調査を実施した。なお、当該時期は、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。

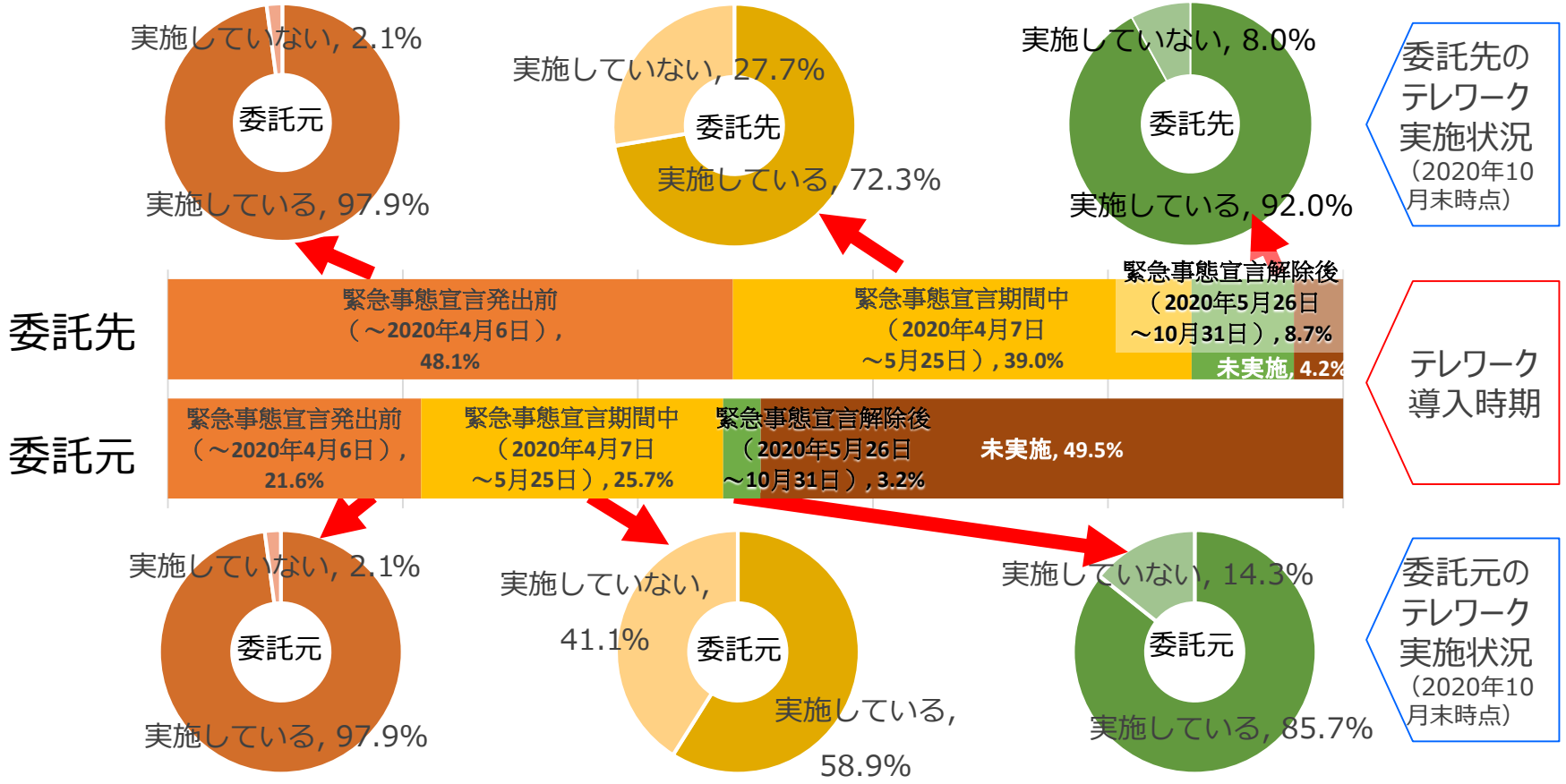



出典）厚生労働省公表データを元に編集

# ２．分析結果と課題

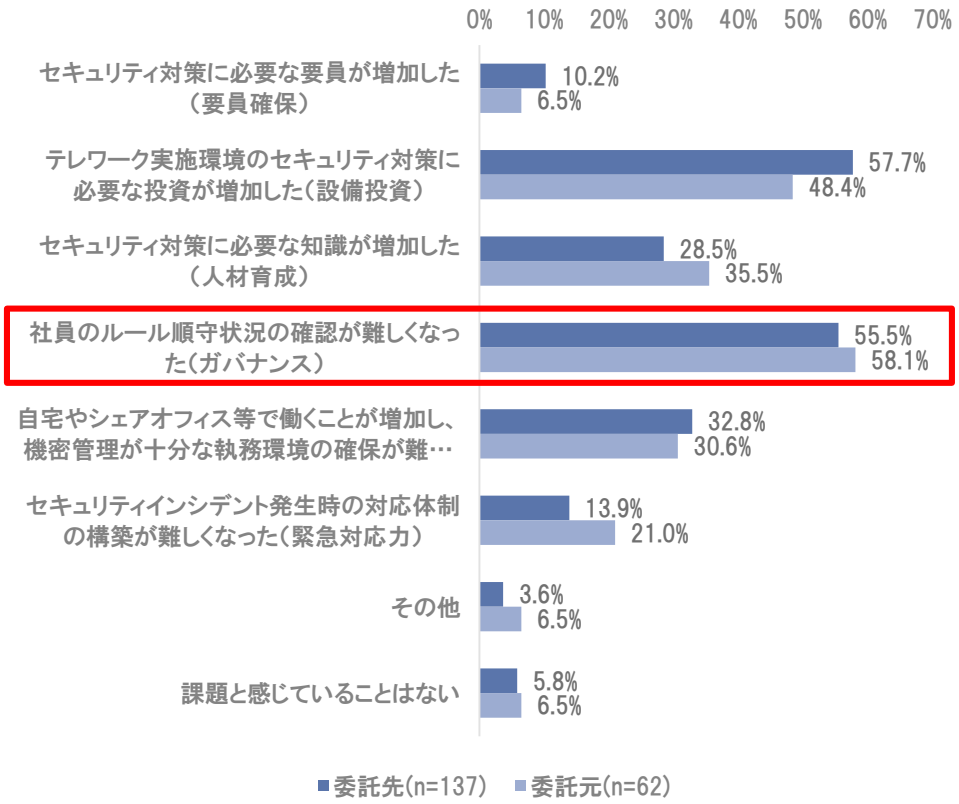
# テレワーク導入時期と継続状況

「緊急事態宣言発出前あるいは解除後」に導入した組織の9割が継続
「緊急事態宣言期間中」に導入した組織も委託先の7割、委託元の6割が継続
事業継続の一時的対策にとどまった組織もあるが、短期間に広く普及し定着しつつある



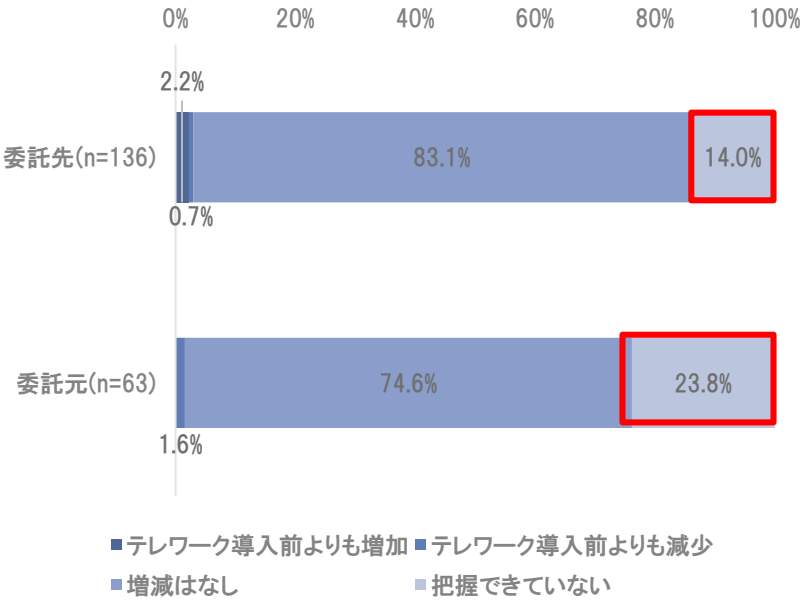
# 規定やルールの順守状況の確認が困難
# インシデント検知能力が下がっている恐れ

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、
約6割が「従業員のルール順守状況の確認が難しくなった」と回答




**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）**

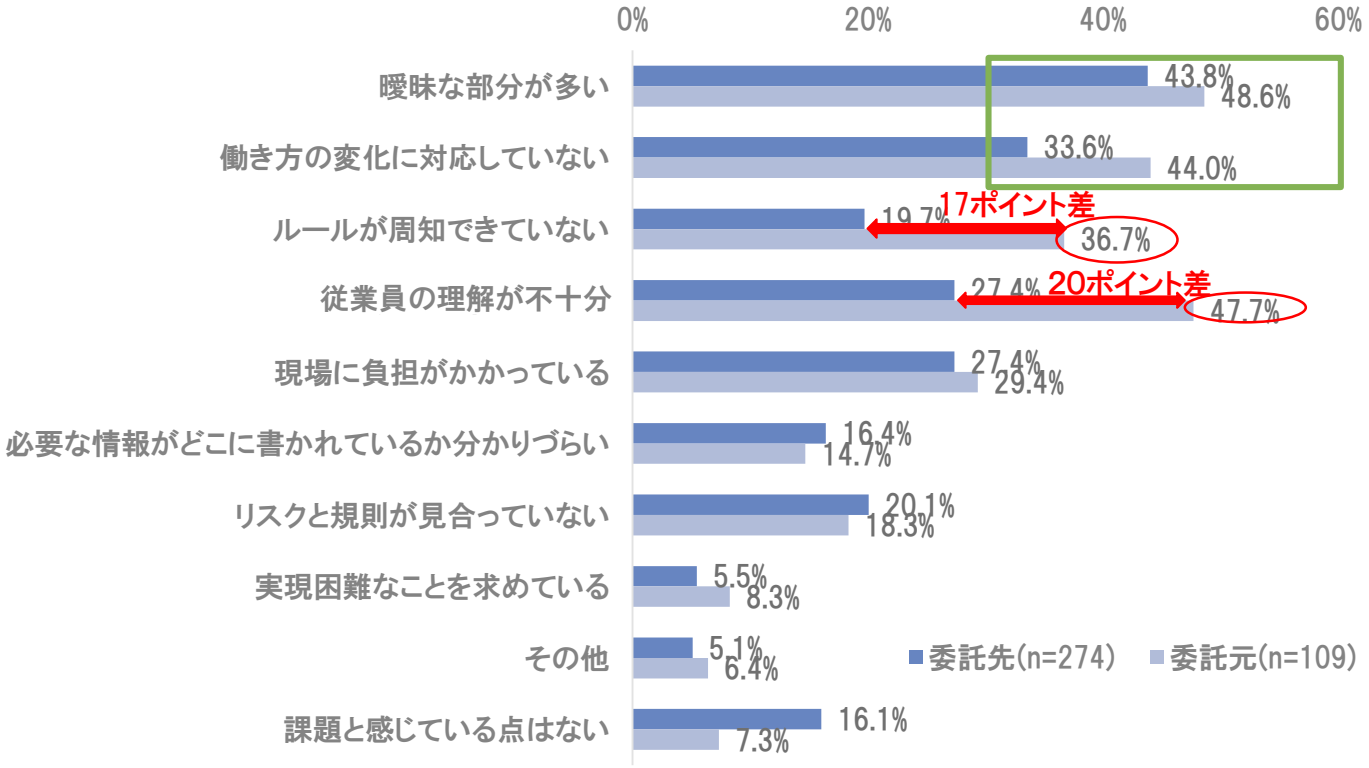
テレワーク導入後も内部不正の発生件数に「増減はなし」と回答している
組織が多い一方で「把握できてない」という回答も一定割合存在




**テレワーク導入後の情報セキュリティに関する**
**従業員の内部不正発生件数**
**（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）**

# 規定やルールの曖昧さ、実態とのかい離有
# 委託元は更に従業員の理解、周知が課題

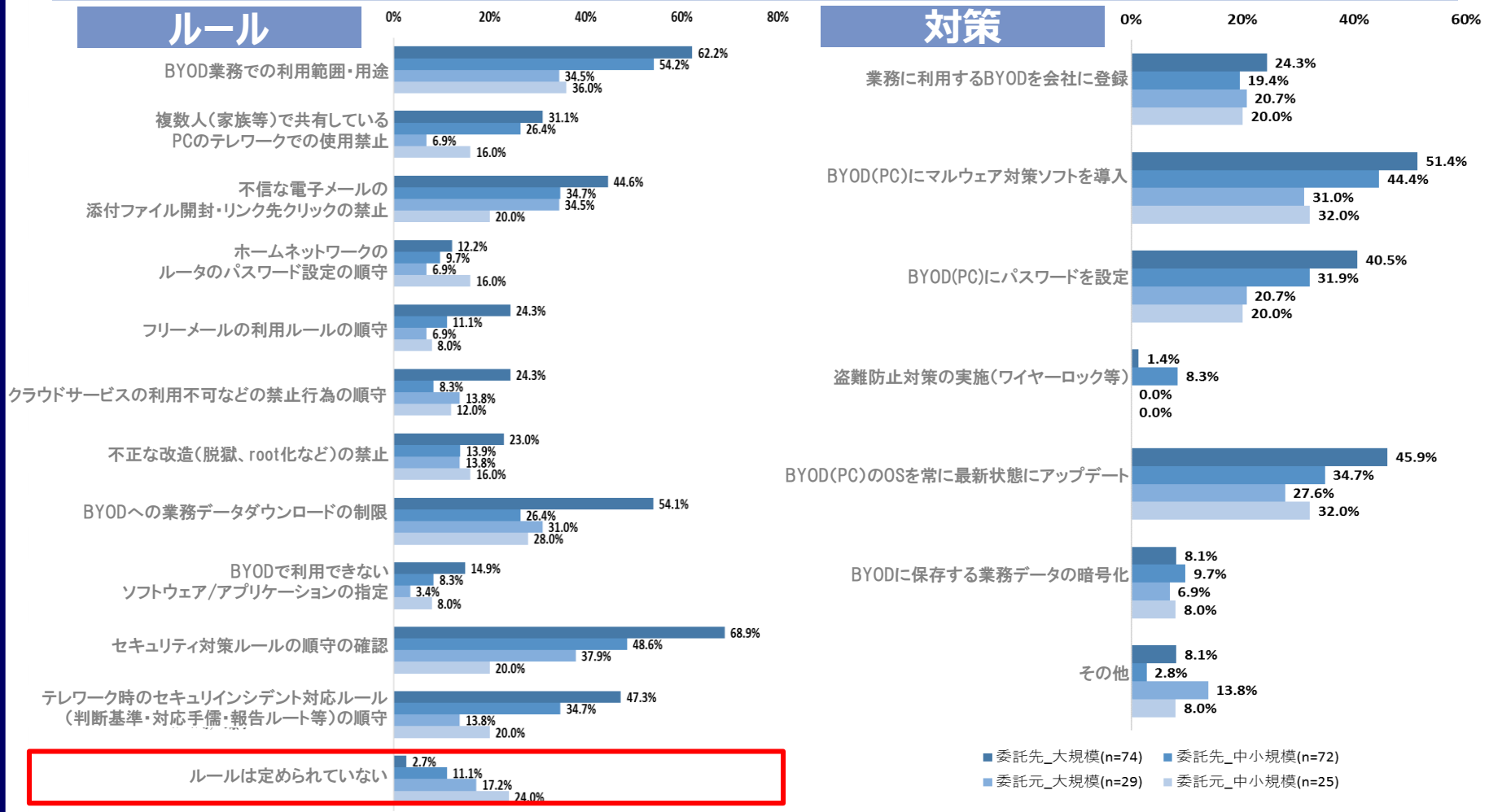
「曖昧な部分が多い」「働き方の変化に対応していない」⇒委託元・委託先共に多い
「ルールが周知出来ていない」「従業員の理解が不十分」⇒　特に委託元に多い




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）

# BYOD利用時のルールを定めていない企業が一定数存在

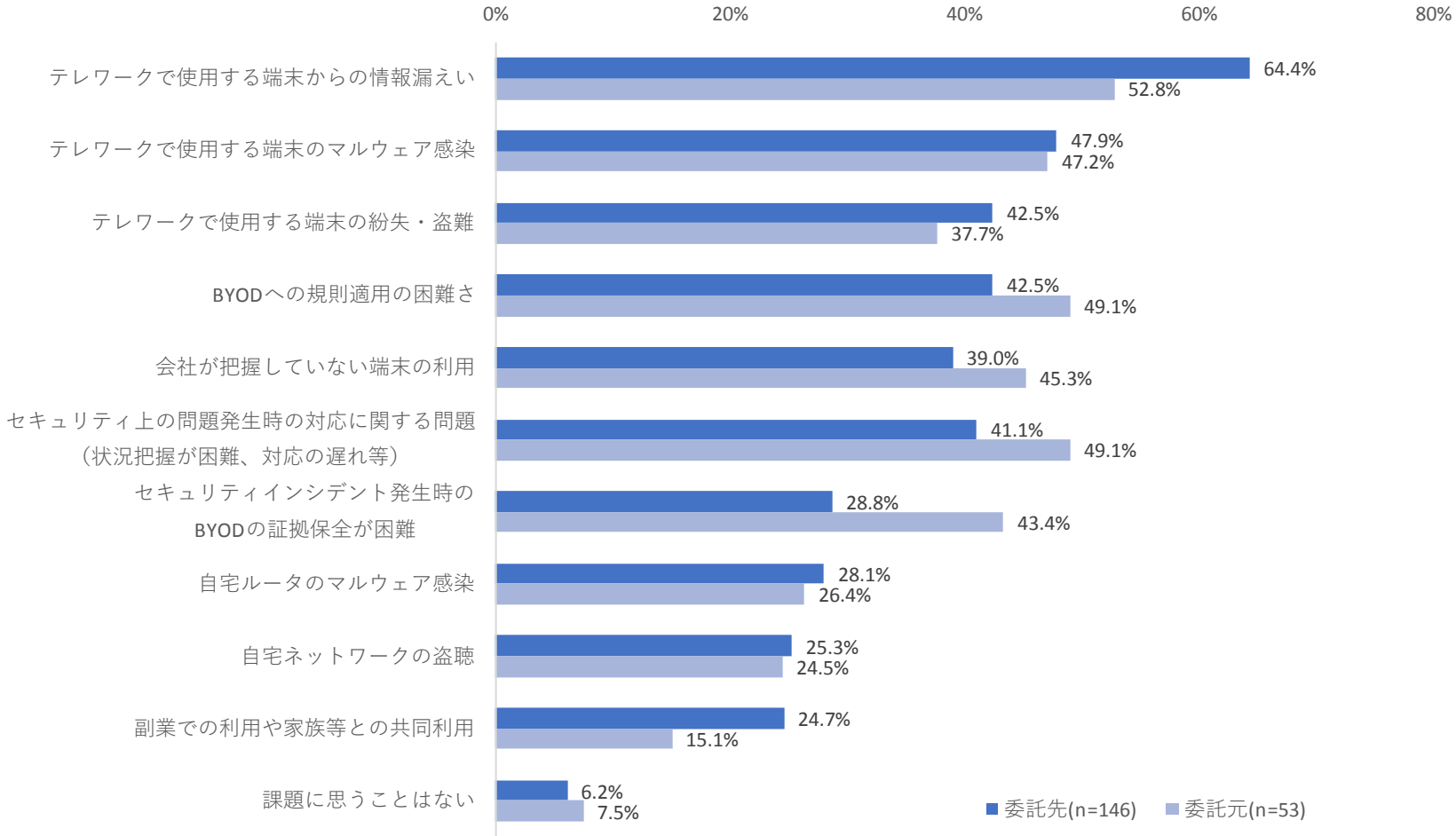
## BYODの利用時のルールを決めていない委託元中小企業が２割５分




**BYOD端末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）**

# BYOD利用時に組織が感じている課題

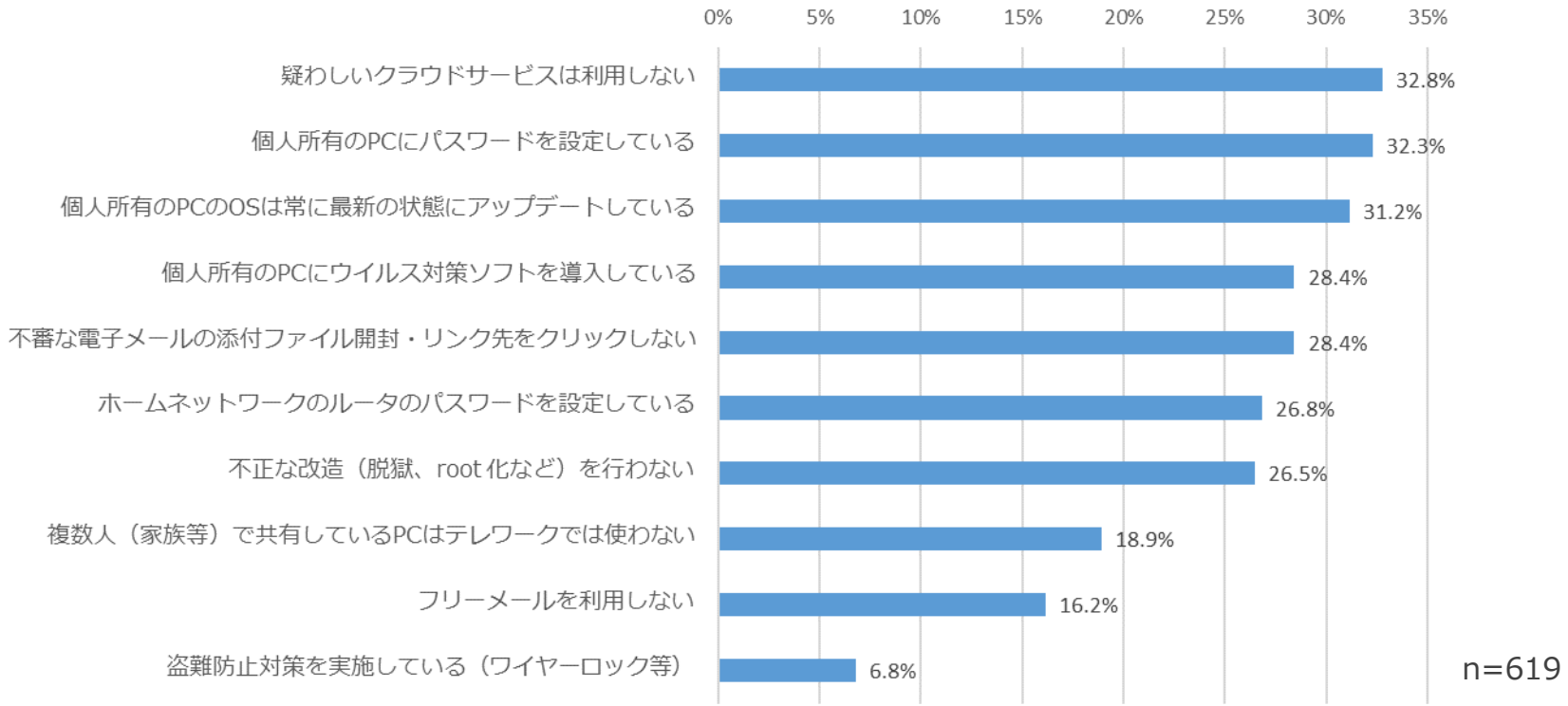
「テレワークで使用する端末からの情報漏えい」が委託先、委託元ともにトップ




**BYODの利用に伴う課題（組織調査Q24）**

# BYODを利用して業務を実施する際に会社でルールが無くても個人で実施しているセキュリティ対策

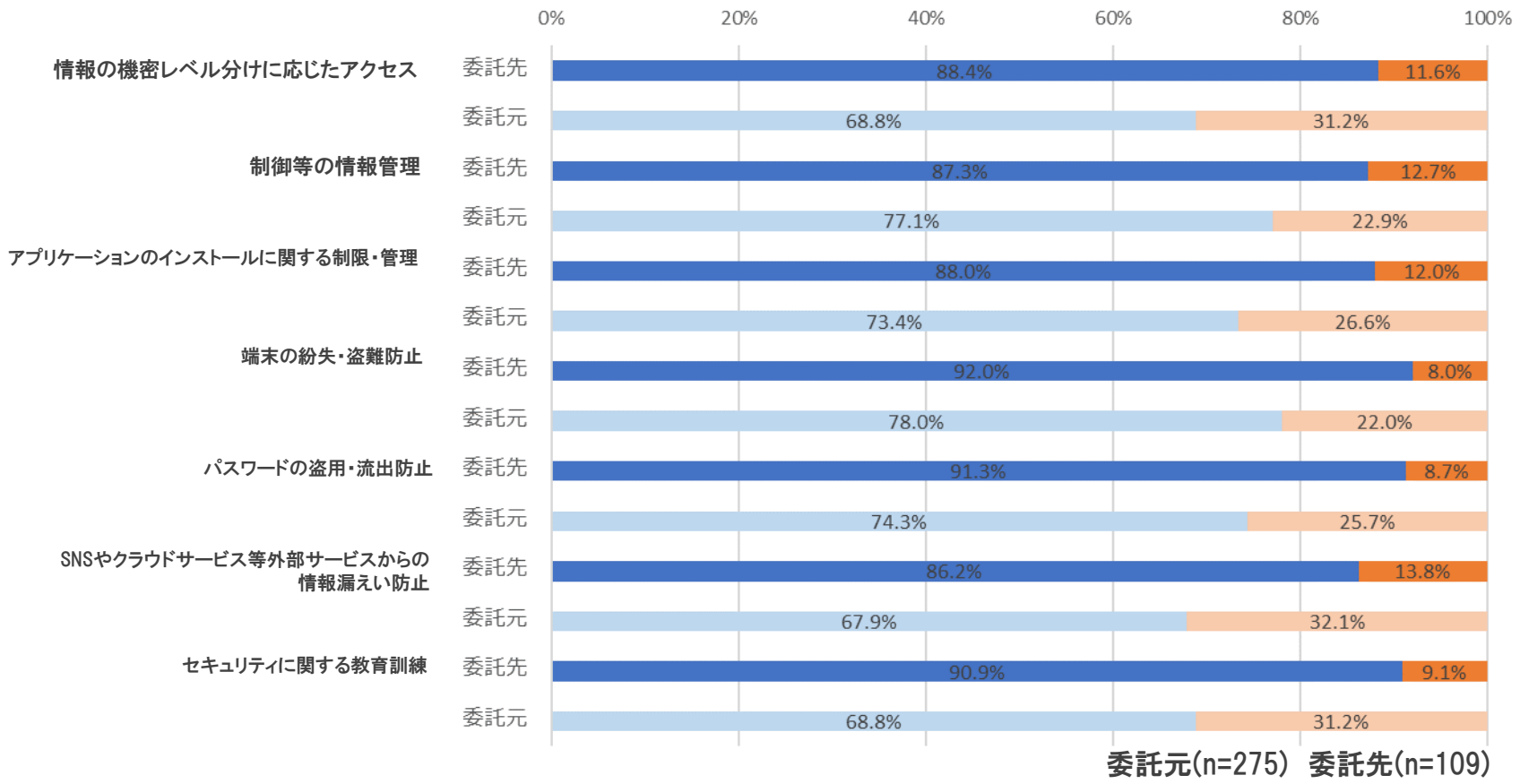
「疑わしいクラウドサービスを利用しない」「個人所有PCにパスワードを設定」
「個人所有のPCのOSを常に最新の状態にアップデート」がトップ３




**会社がルールを決めていないセキュリティ対策を実施状況（BYODを利用した業務実施時）（個人調査Q28）**

# テレワークに関するセキュリティ対策の規定・規則・手順などの取り決めの状況

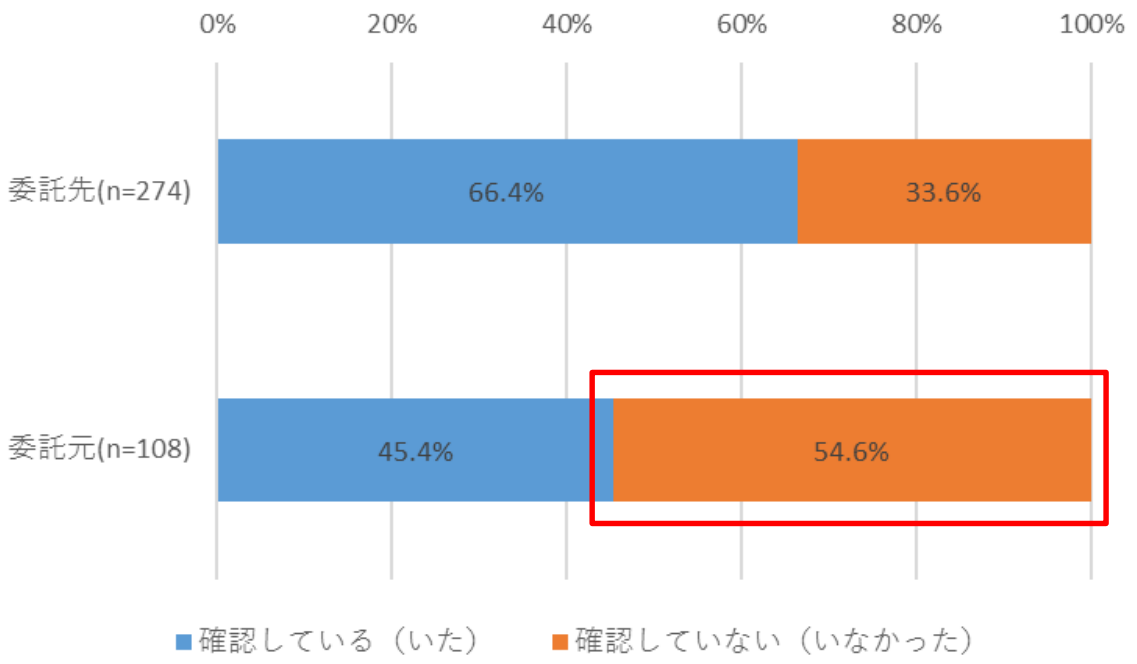
## 委託先の方が規定・規則・手順を取り決めている割合が高い




テレワークに関するセキュリティ対策の規定・規則・手順などの取り決めの状況（組織調査Q10）

# 半分以上の委託元がテレワークに関する社内規定・規則・手順の順守確認を実施していない

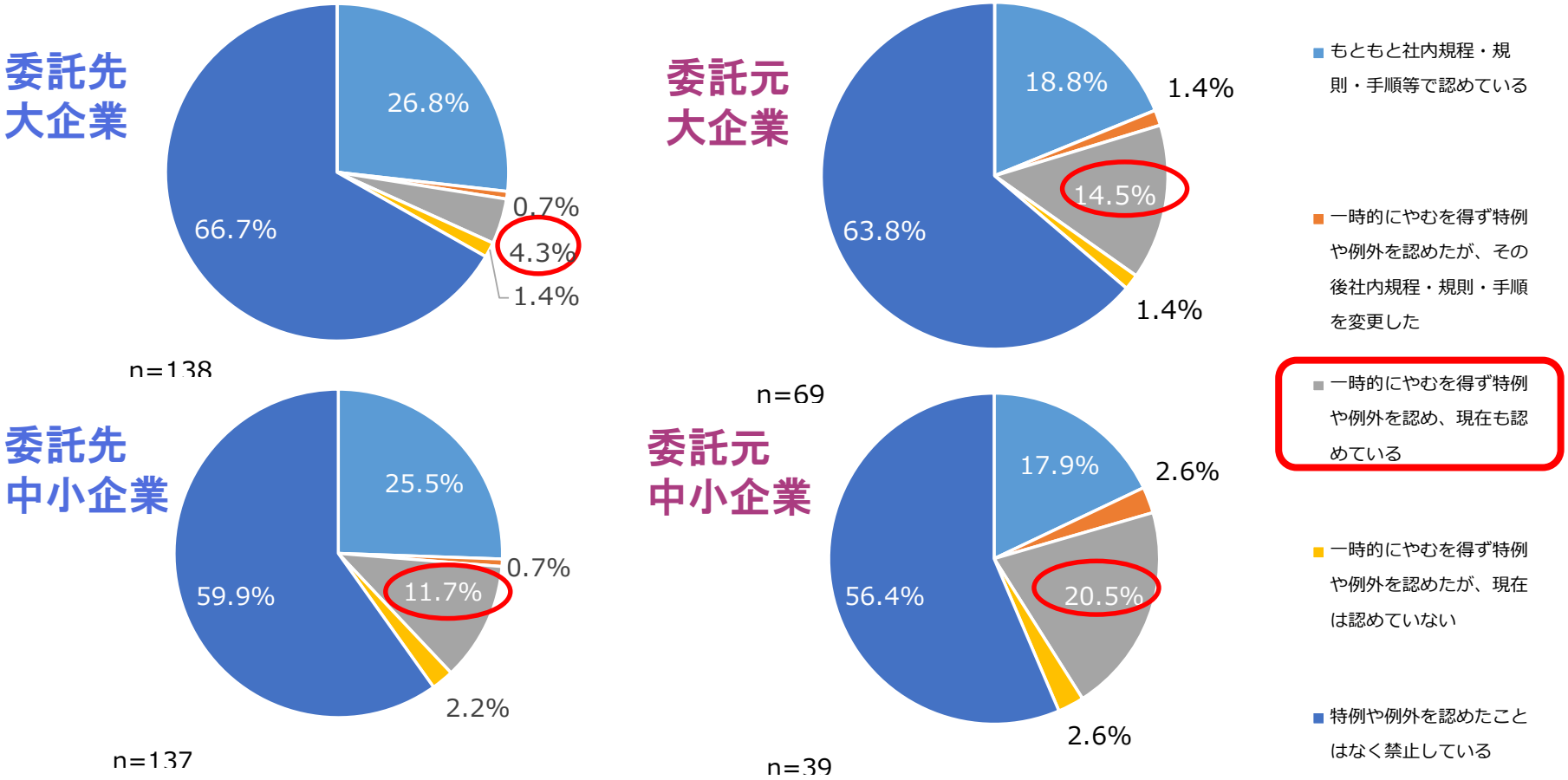
委託先と委託元で社内規定・規則・ルール順守の確認状況に差が発生




テレワークに関する社内規程・規則・手順等が守られているかの確認状況（組織調査Q12）

# コロナ禍でのセキュリティ対策の特例が現状も継続

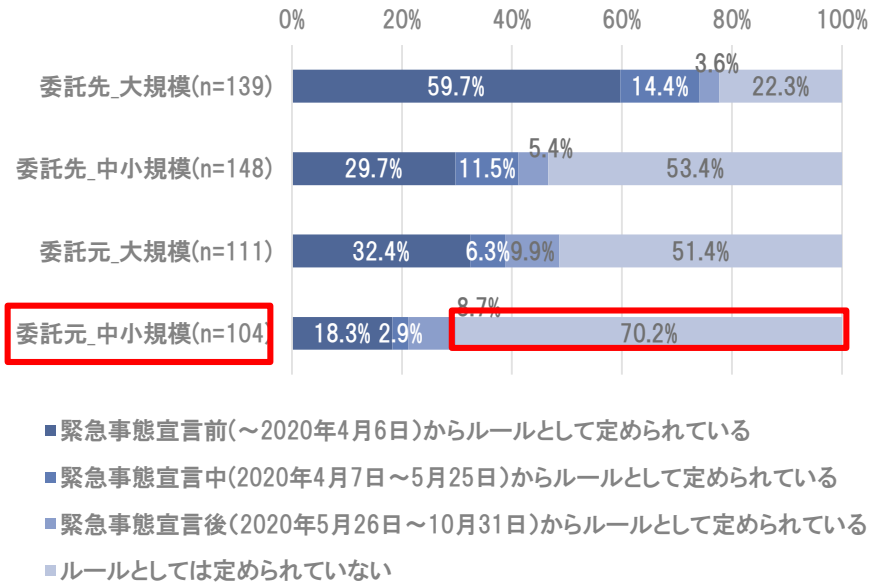
会社が許可していないアプリケーション・ソフトウェア・クラウドサービスの業務利用を
一時的に「やむを得ず」認め、現在も認めている組織がある




緊急事態宣言中またはコロナ渦の影響により特例や例外を認めたセキュリティ対策の社内規定・規則・手順（組織調査Q11）

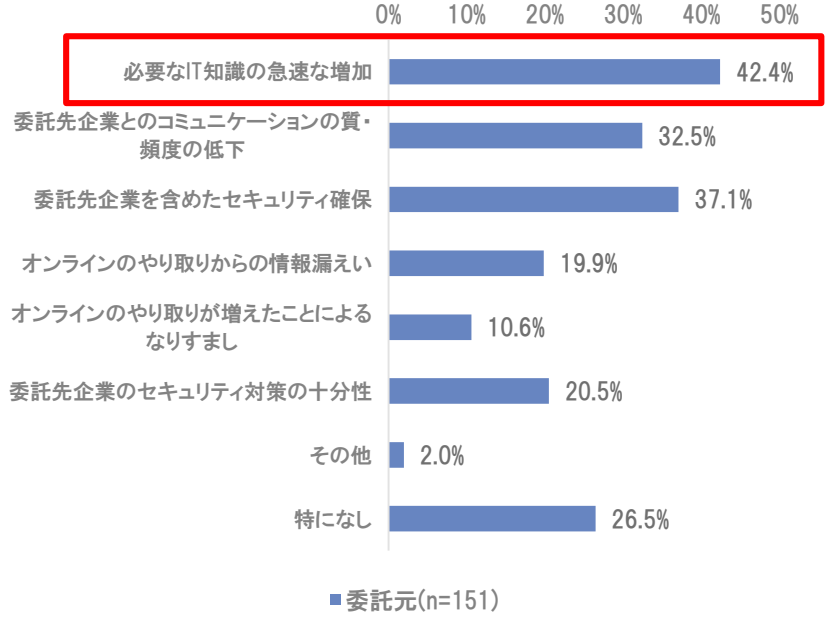
# ルール策定状況の違いによる遵守困難
# 急速な行動の変化に伴うIT知識の不足

特に中小規模の委託元にてルールが制定されていない割合が高い
ウェブ会議相手とのルール策定状況が違うことにより自社の決めたルールの遵守が困難となる可能性が懸念される




**「会社が許可したウェブ会議ツールのみ利用可能」とするルールを制定（委託元）（組織調査Q28）**

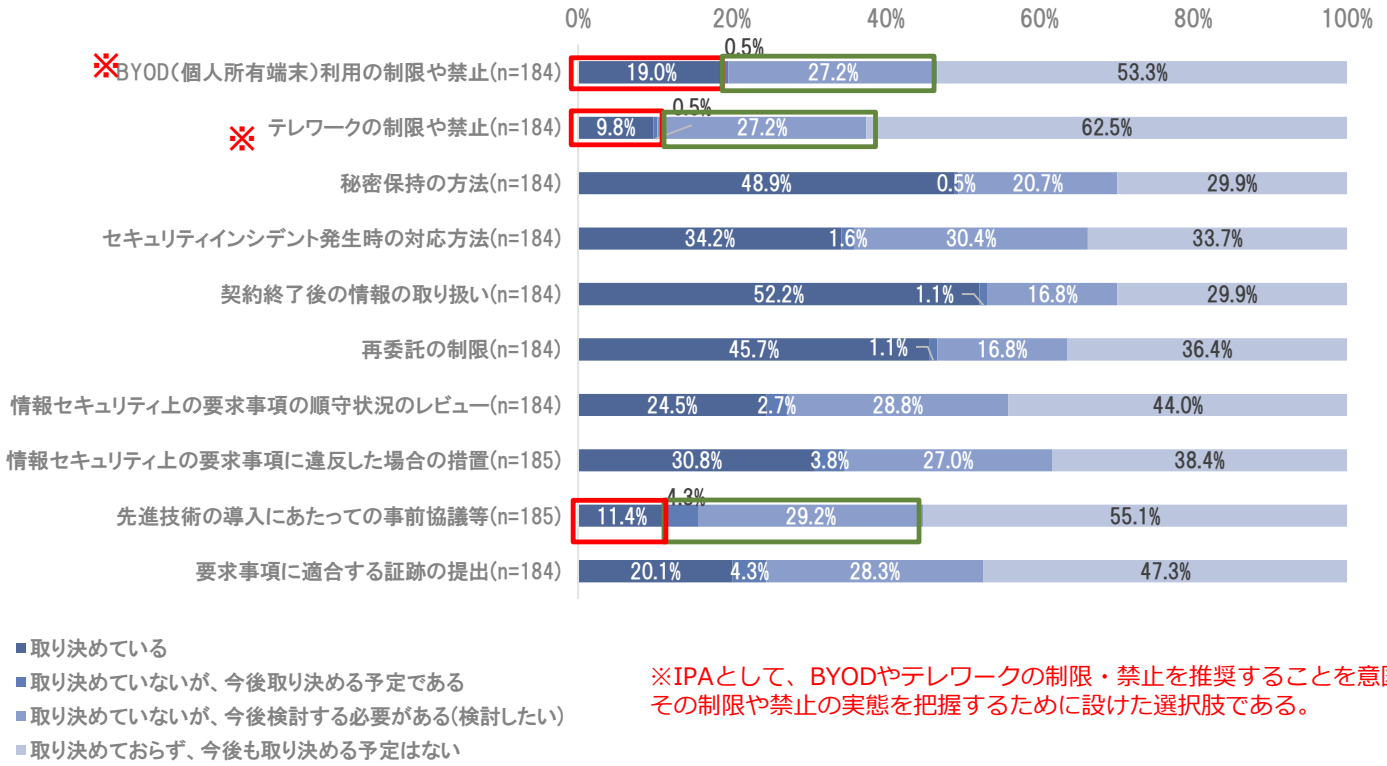
「必要なIT知識の急速な増加」が多く回答された
委託元が委託先を管理する際のIT知識の知識不足が懸念される




**委託元から見た取引先（委託先）の行動変化による課題（組織調査Q34）**

# ニューノーマルに対応した業務委託契約は進んでいない

テレワークの導入、BYODの使用などに関する業務委託契約上の要求事項について検討が進んでいない
一方、これらの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も一定割合存在することから、今後精査・強化が進むことが考えられる




※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。

**2020年4月1日から2020年10月31日の間に取り決めた業務委託契約のセキュリティ要求事項（委託元）（組織調査Q40）**

# ITサプライチェーンにおける業務委託契約時のセキュリティ確保の増加

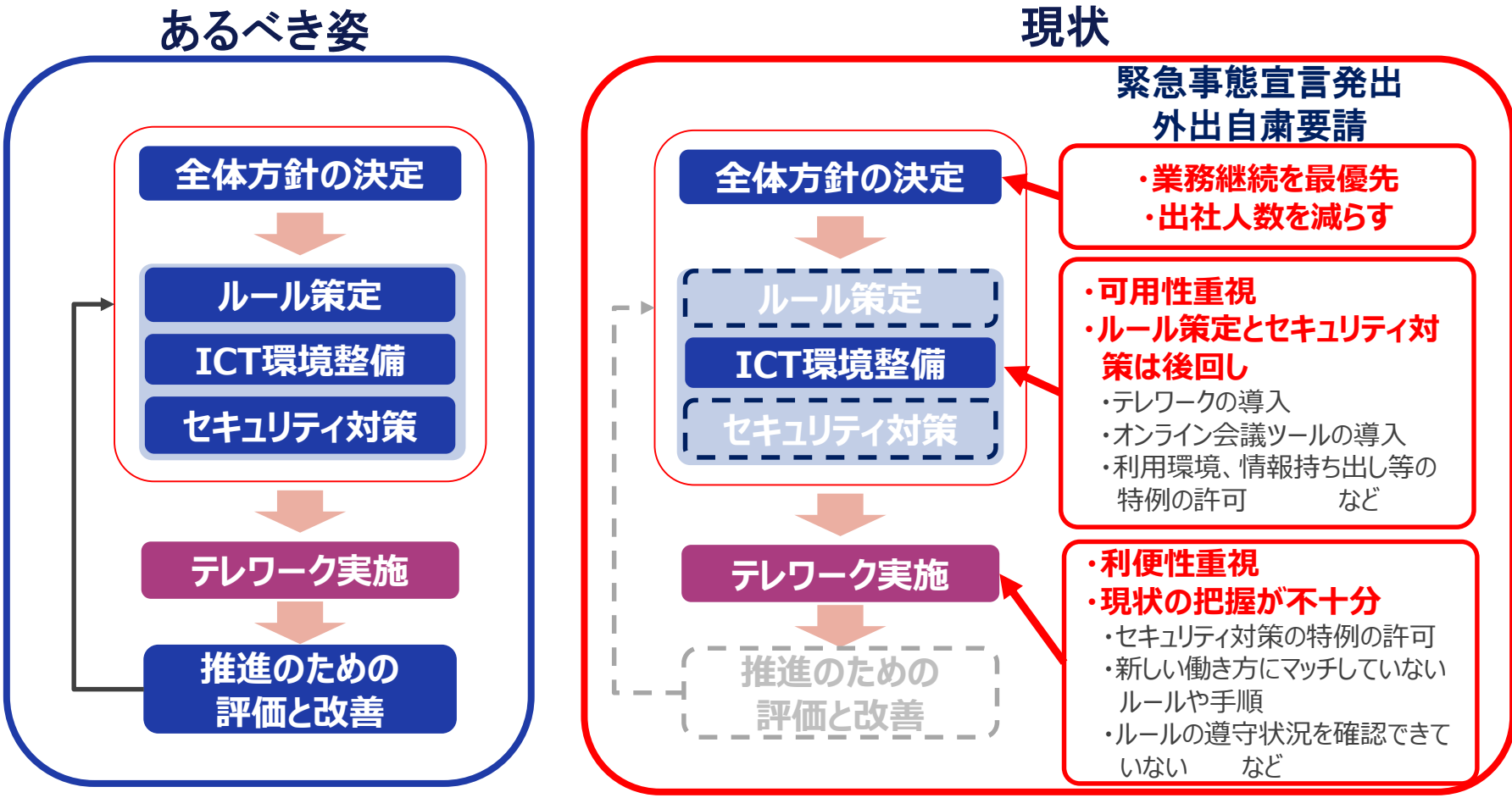
テレワークなどの定着によりITサプライチェーンにおけるセキュリティ確保の要求の増加が考えられる

| ニューノーマルのITサプライチェーンにおける業務委託契約に関する有識者からの指摘事項 |
| --- |
| 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。 |
| 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。 |
| 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。 |

# 3. まとめ

# あるべき姿と現状

- 業務実施場所の多様化やコミュニケーションのオンライン化は不可逆的な変化として定着するものと想定される。




出典　厚生労働省「テレワークではじめる働き方改革」

# 課題

- **ガバナンスが低下している**
  - 規定やルールの順守状況の確認が困難
  - インシデントが検知できない
  - 特例や例外が増え、放置されている
- **働き方の変化(*)に対応した規定やルールが整備出来ていない**

  (*)テレワーク、BYOD利用等
  - 規定やルールが存在していない（あるいは実態に合っていない）
  - 規定やルールの内容が従業員に周知されていない
- **ルール策定状況の違いにより取引先とのセキュリティ対策レベルに差がある**
- **ニューノーマルに対応した業務委託における取り決めが進んでいない**

# 提言

今後ITサプライチェーン上の情報セキュリティを確保するためには、業務実施場所の多様化やコミュニケーションのオンライン化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。

## ＜委託元＞

- 特に中小規模については、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。
  まずは「社内規程・ルールの整備」が急務であり、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「ルールの周知・教育」や、セキュリティリスクの低減や業務の見える化を促進する「ICT環境の整備」を推進していくことが望まれる。

## ＜委託先＞

- 環境変化に対し、自社のルールがマッチしているのか、リスクが提言できているかを見直す必要がある。また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、より委託元とのコミュニケーションを充実させ、セキュリティリスクの状況や必要な対策について説明し、対応を促していくことが必要となる。

## ＜共通＞

- 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。

# （参考）報告書の入手方法

## IPAのサイトからダウンロードいただけます。

**個人編　中間報告**
https://www.ipa.go.jp/security/fy2020/reports/scrm/index.html

**組織編　中間報告**
https://www.ipa.go.jp/security/fy2020/reports/scrm/index-soshiki.html

**最終報告**
https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html