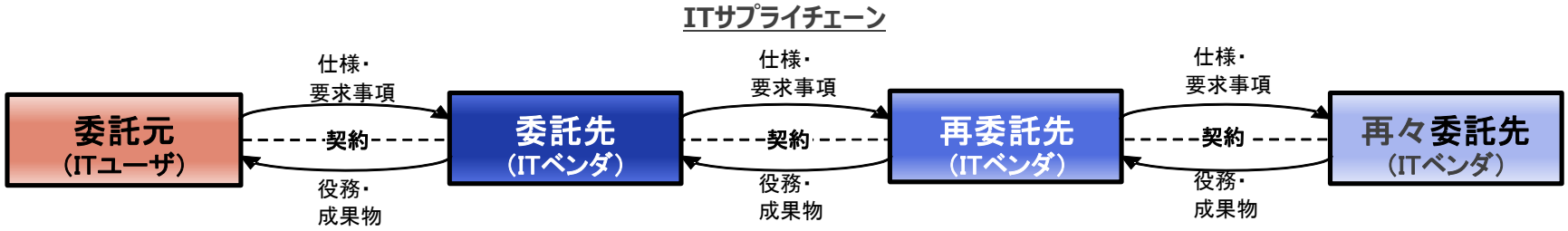
2021年度
企業・組織における
テレワークのセキュリティ実態調査
調査報告書

2022年6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

本調査の位置づけ

- これまでITシステム開発やサービス提供におけるサプライチェーンリスクマネジメント調査として、セキュリティ対策の取り決め内容や責任について委託元(ITユーザ)と委託先(ITベンダ）に対する実態調査を実施してきた



- 2020年4月コロナ感染防止対策として緊急事態宣言が発出され、テレワークやオンライン会議の利用が急速に広がった。このICT環境の変化が業務委託契約上の取り決めやサプライチェーンリスクに影響を与えていないかを2021年度調査として実施。本調査はその継続調査である

背景・目的

背景

2020年11月に実施した「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」により明らかになった課題。

- **ガバナンスの低下**
  - 特例、例外により緩和された対策が見直されていない
  - 働き方の変化(テレワーク、BYOD利用等)に対応した規定やルールが整備出来ていない
  - ICT環境の変化に対して委託先(ITベンダ)より委託元(ITユーザ)の方が対応が遅れている
- **サプライチェーン上のリスクが顕在化**
  - ICT環境変化に親和性の高い委託先(ITベンダ)ではセキュリティ対策の見直し、検討が進んでいるのに対し、委託元(ITユーザ)は事業継続最優先でセキュリティ対策が十分行えない
  - 委託元(ITユーザ)からの業務委託時の取り決めにニューノーマルのリスクを想定したセキュリティ対策の項目が追加されていない

目的

2020年調査からの変化を調査することにより、低下したガバナンスがどこまで回復したかを知る。
今後セキュリティ対策のさらなる強化が必要な課題を明らかにする。

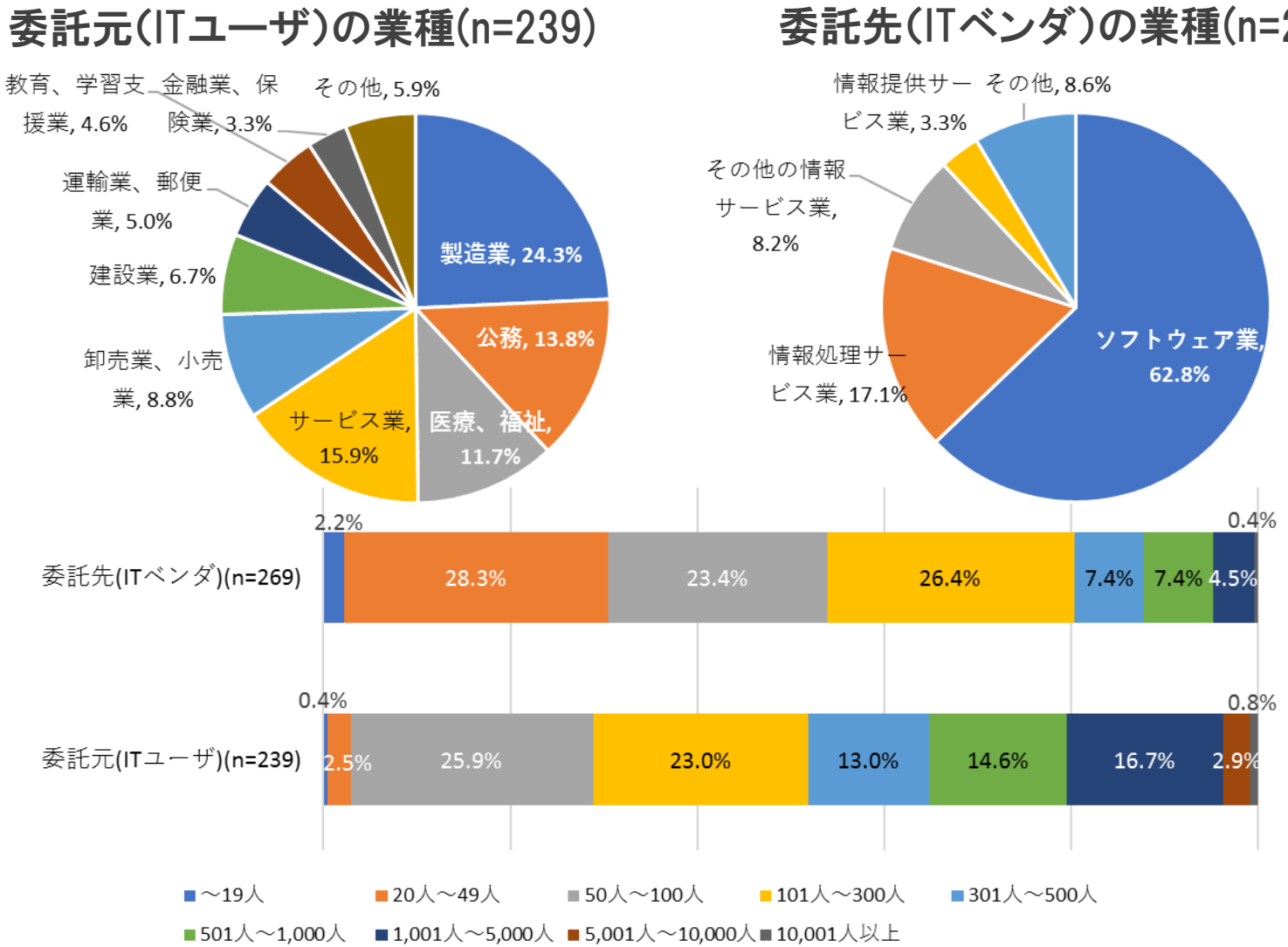
アンケート実施概要

- テレワークについて実施状況、ルール策定の状況、実施に伴う業務委託に関する不安などを調査項目としたアンケートを実施

1. **調査対象：　企業データベース等から抽出した企業・組織**
2. **調査方法：　郵送アンケートとWEBアンケートの併用**
3. **調査期間：　2022年2月18日～3月11日**（前回2020年11月18日～12月11日）
   ※回答に際しては、2022年1月31日時点を「現在」と想定の上で回答いただいた
4. **有効回答数：508社**（505社）
   - **委託先(ITベンダ)・総従業員数・職員数101人以上の企業・大規模：124社**（139社）
   - **委託先(ITベンダ)・総従業員数・職員数100人以下の企業・中小規模：145社**（148社）
   - **委託元(ITユーザ)・総従業員数・職員数が301人以上の企業・組織・大規模：115社**（112社）
   - **委託元(ITユーザ)・総従業員数・職員数が300人以下の企業・組織・中小規模：124社**（106社）
5. **設問数：委託先(ITベンダ)：33問**（45問）、**委託元(ITユーザ)：33問**（44問）

（）内の数字は前回2020年度調査の実績数

回答組織の業種と規模（従業員数）

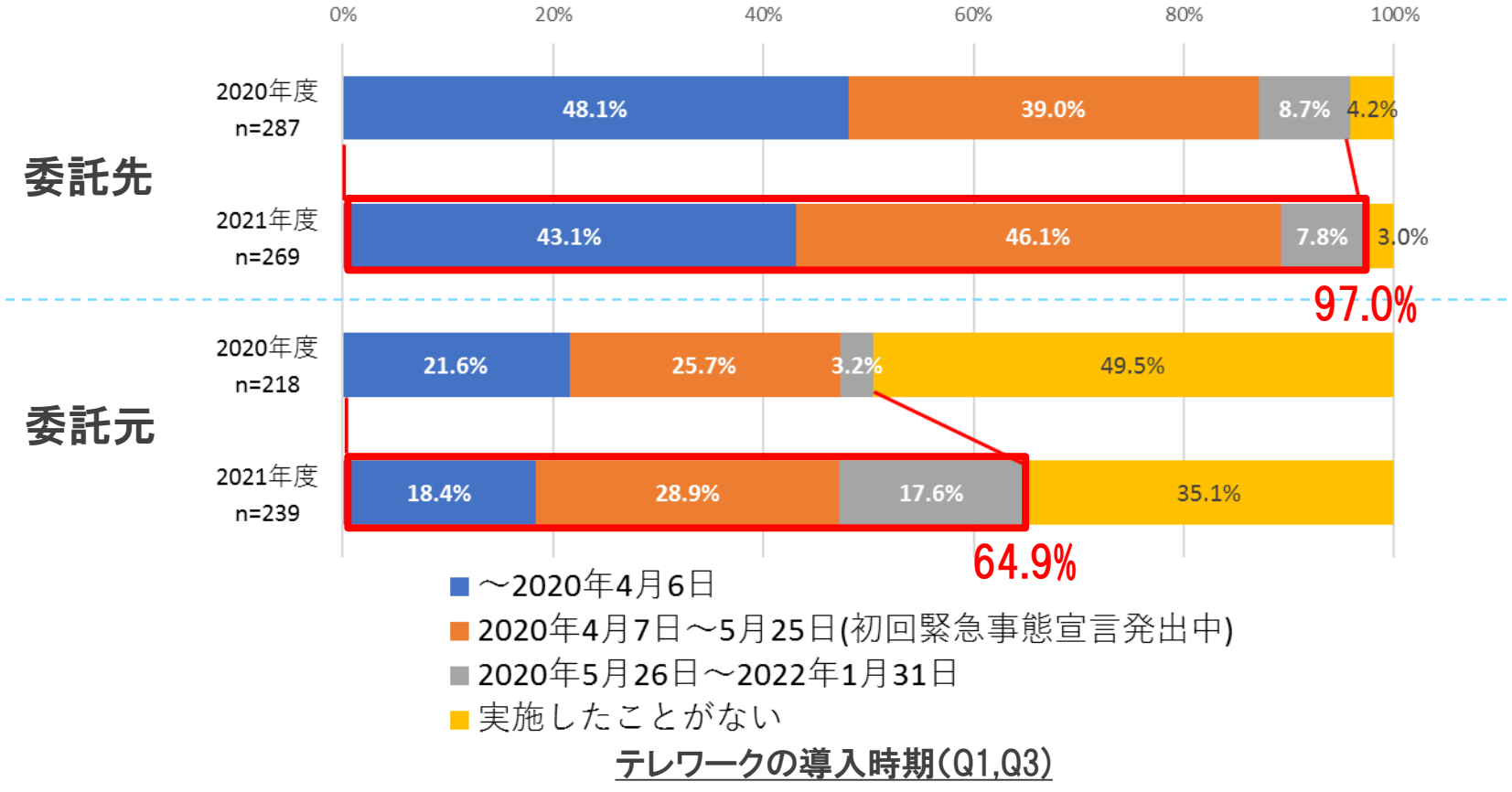


分析結果と課題

2020年度調査との比較

委託元(ITユーザ)のテレワーク導入が進んだ

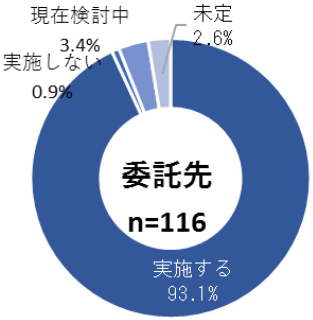
- 委託先(ITベンダ)のテレワーク実施率は97.0%で前回調査から1.2ポイント上昇
- 委託元(ITユーザ)のテレワーク実施率は64.9%で前回調査から14.4ポイント上昇
- 委託元(ITユーザ)では、初回の緊急事態宣言より後にテレワークを導入した組織が増加

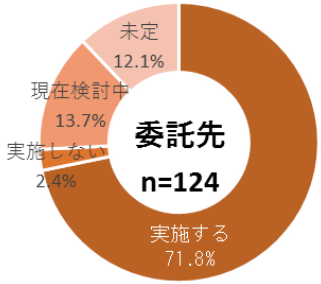


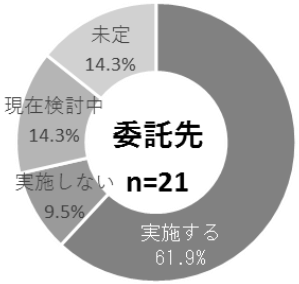
テレワークの導入時期(Q1,Q3)

テレワーク導入時期と今後の継続予定

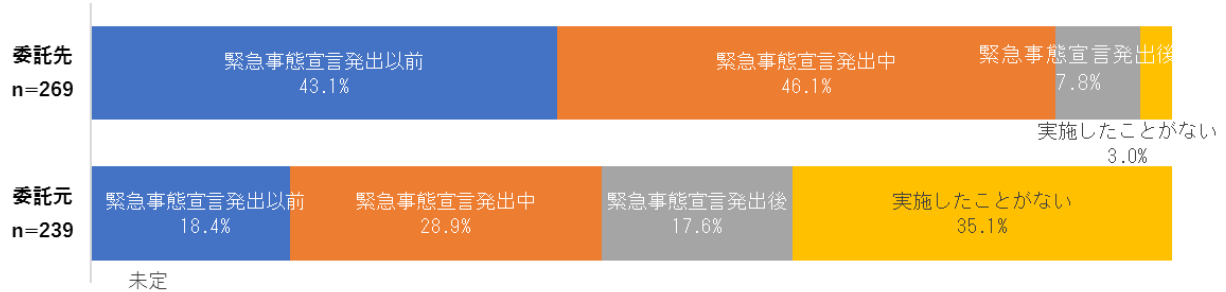
- 「緊急事態宣言発出前」に導入した組織の9割以上が今後も継続予定
- 「緊急事態宣言発出中及び発出後」に導入した組織も半数以上が今後も継続予定
- 事業継続の一時的対策にとどまった組織もあるが、短期間に広く普及し定着しつつある



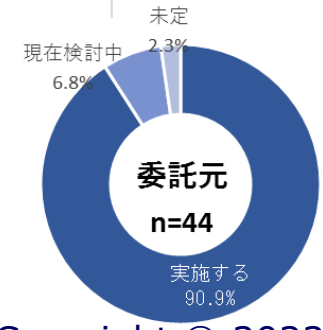


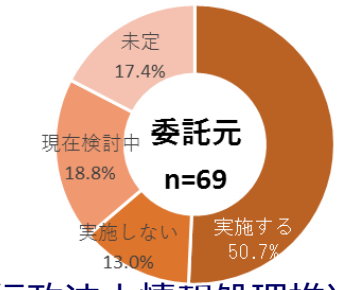


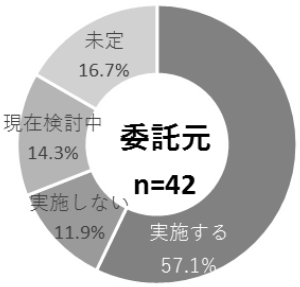
委託先の
2022年4月以降の
テレワーク実施予定
（2022年1月末時点）



テレワーク導入時期





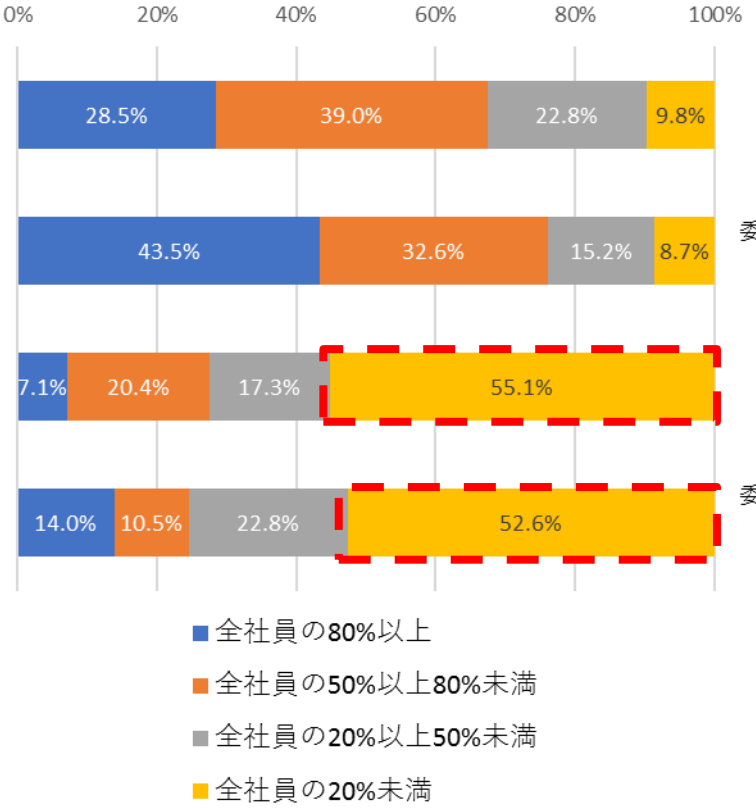


委託元の
2022年4月以降の
テレワーク実施予定
（2022年1月末時点）

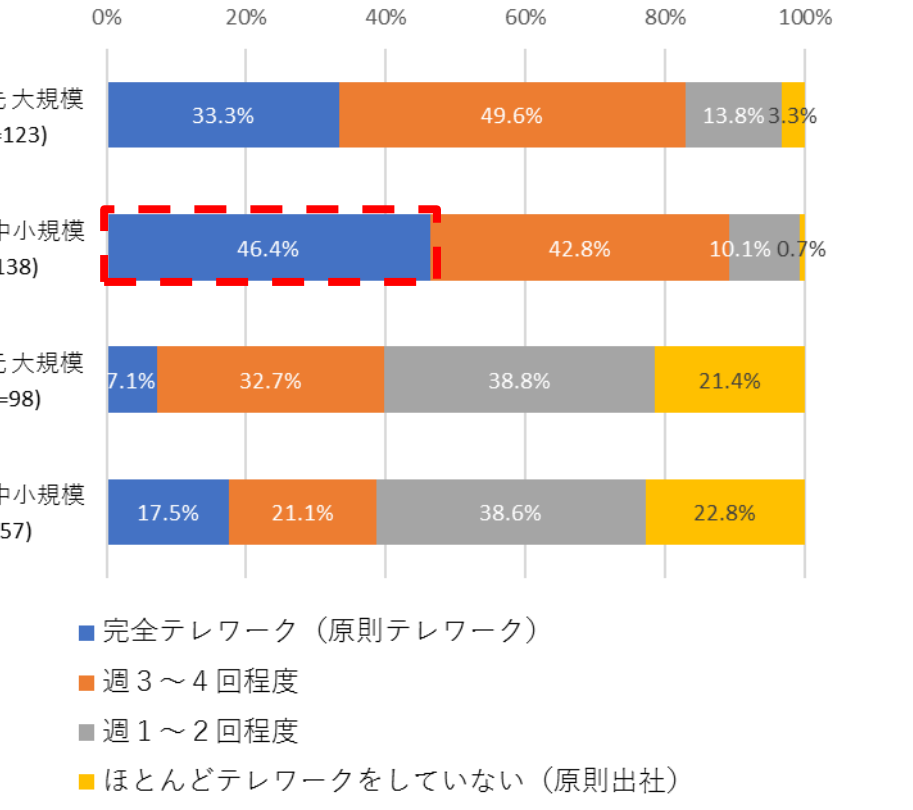
テレワーク実施の割合、頻度（ピーク時）

- 委託先(ITベンダ)では中小規模で完全テレワークを4割以上が実施
- 委託元(ITユーザ)ではピーク時でも社員の20%未満が5割以上

テレワーク実施社員割合(Q4)(テレワーク実施経験有)



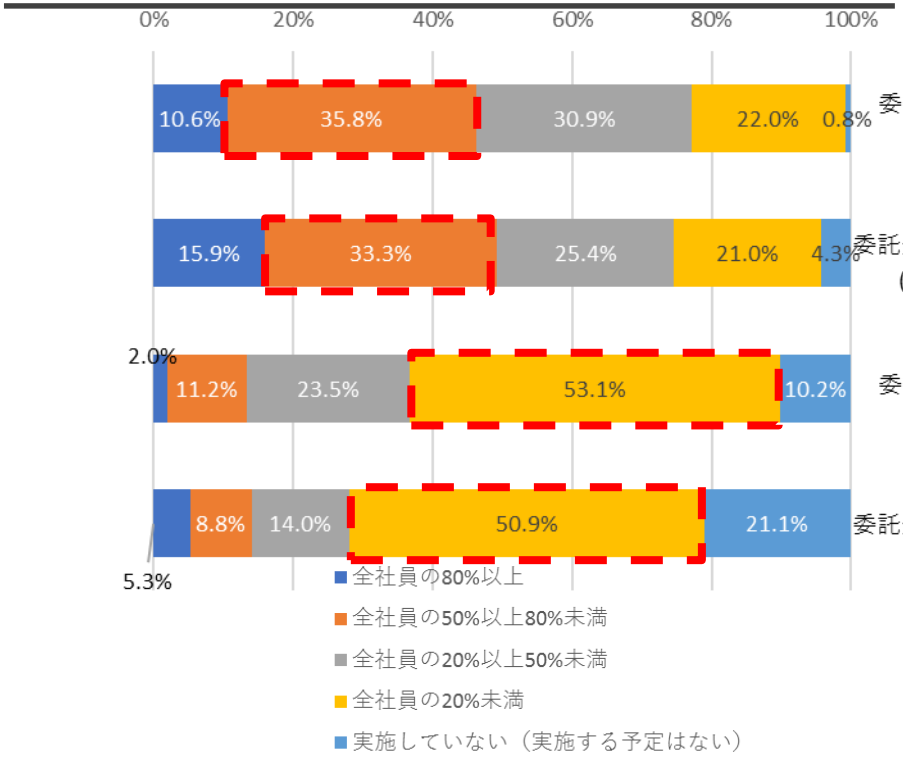
テレワーク実施頻度(Q4)(テレワーク実施経験有)



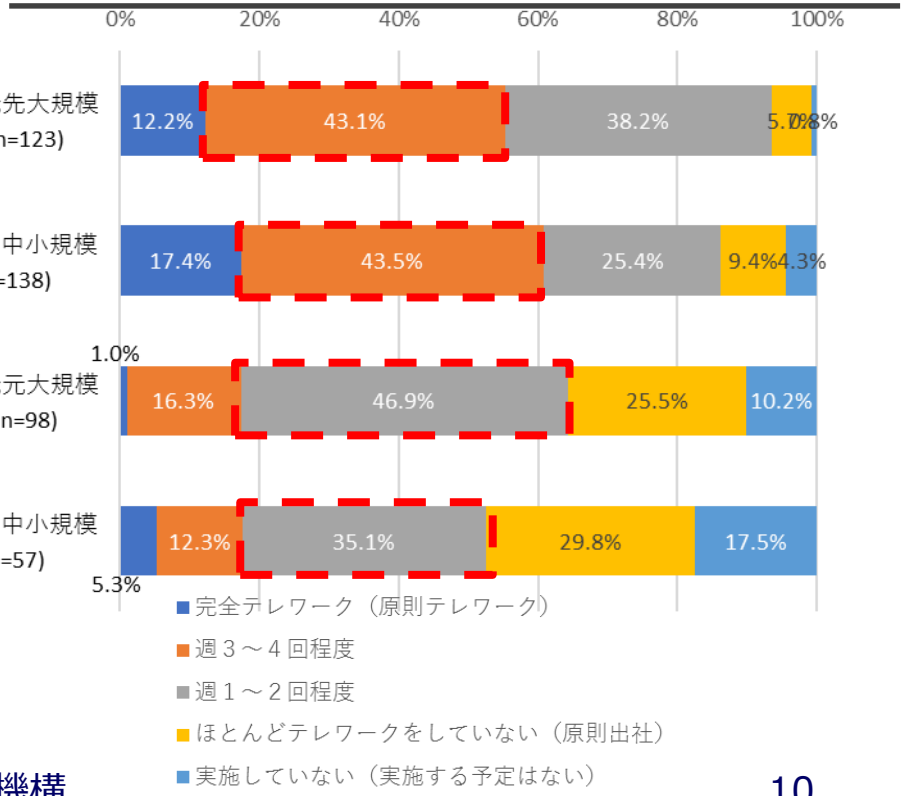
テレワーク実施の割合、頻度（2022年1月末現在）

- 委託先(ITベンダ)：全社員の50%～80%、週３～4回程度実施する組織が多い
- 委託元(ITユーザ)：全社員の20%未満、週１～２回程度実施する組織が多い
- 情報技術関連企業が含まれる委託先(ITベンダ)の方が日常的にテレワークを行いやすいことがうかがえる

テレワーク実施社員割合(Q4)(テレワーク実施経験有)

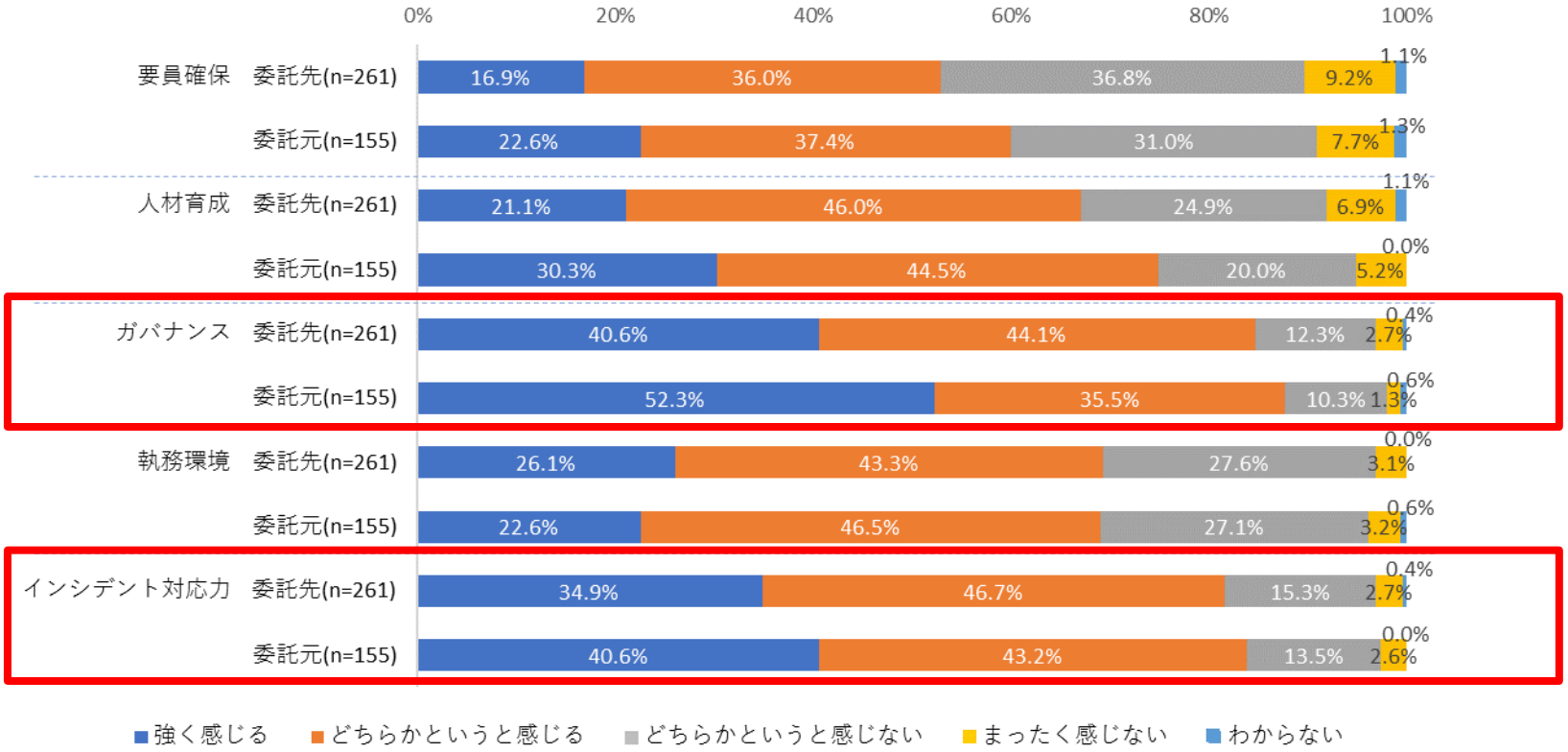


テレワーク実施頻度(Q4)(テレワーク実施経験有)



ガバナンスとインシデント対応力について課題を感じる組織が多い

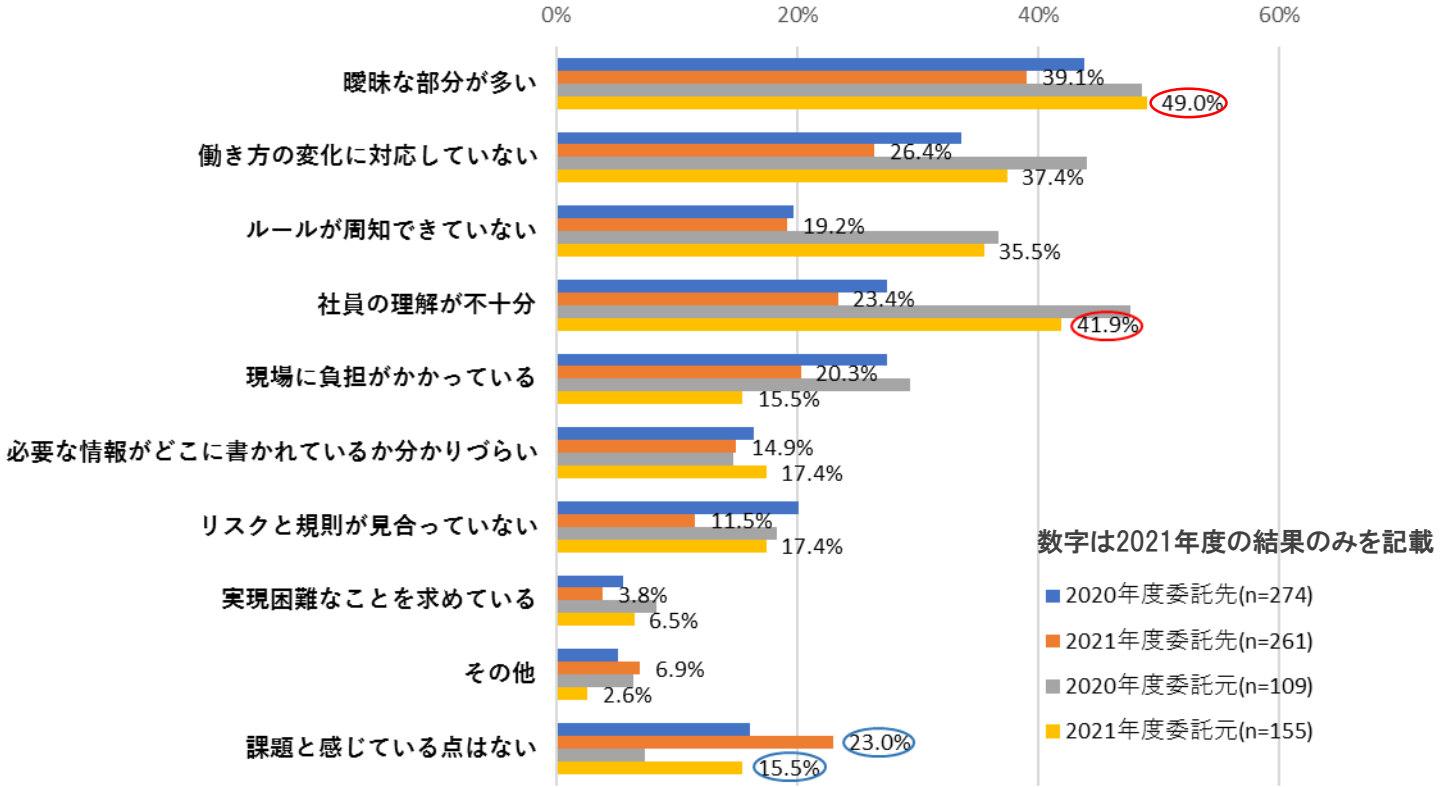
- テレワーク実施時の課題として、「強く感じる」「どちらかというと感じる」と回答した組織が最も多かったのはガバナンス(社員へのルール徹底、順守状況の確認) 続いてインシデント対応力



テレワーク実施時のセキュリティ上の課題（Q６）
（テレワーク実施経験有）

テレワーク実施時の社内ルールの課題は委託元でより多く残る

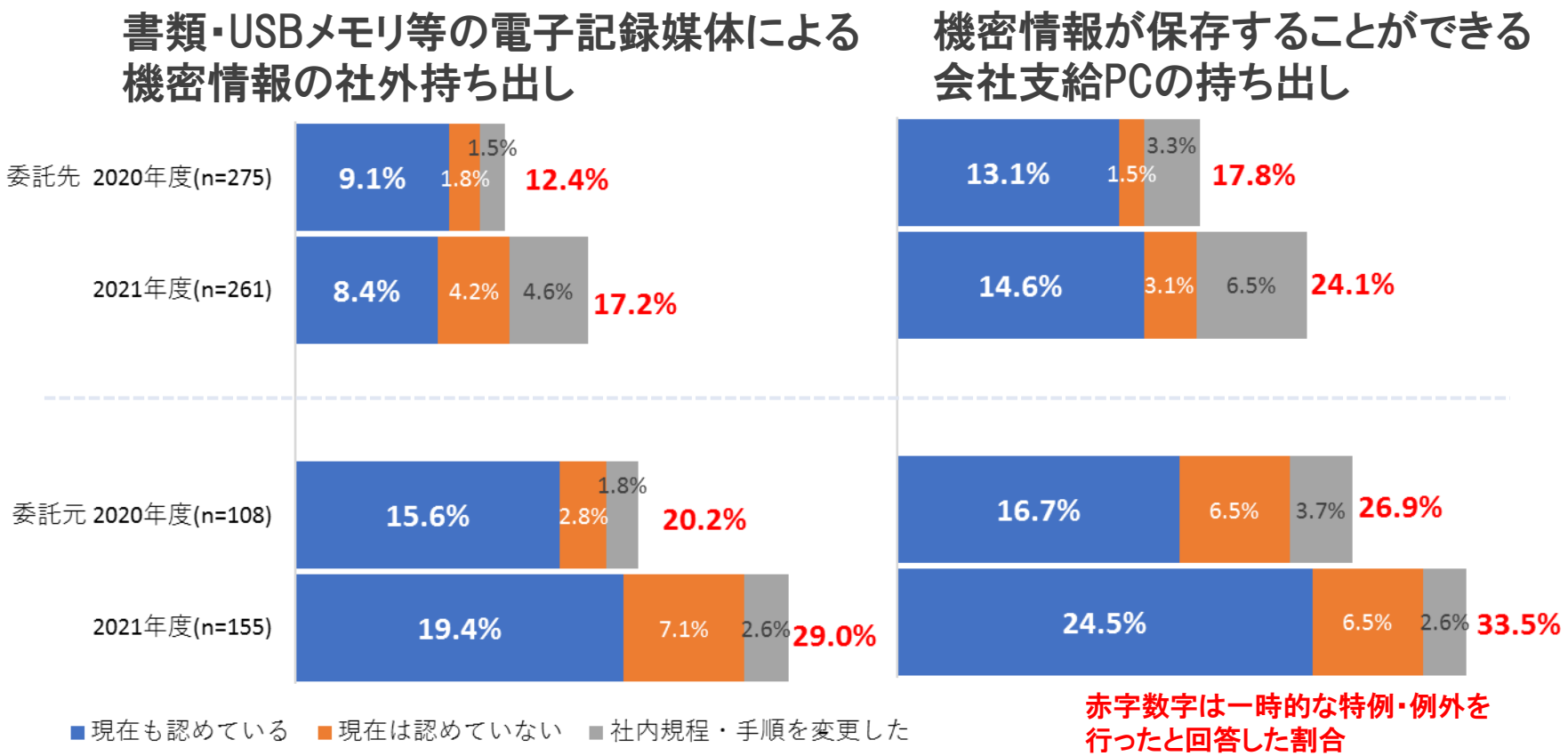
- 社内規程・規則・手順書の課題は一部を除き減少傾向（「課題はない」が増加）
- 委託元(ITユーザ)では「曖昧な部分が多い」「社員の理解が不十分」が4割を超え、いまだに高い傾向



テレワーク実施時の社内規程・規則・手順等の課題（Q10）　（テレワーク実施経験有）

コロナ禍でのセキュリティ対策の特例や例外が増加・長期化している

- 情報の持ち出しについて一時的な特例・例外を認める組織が増加した
- そのまま対策が取られず継続している組織では、リスクの増加が懸念される

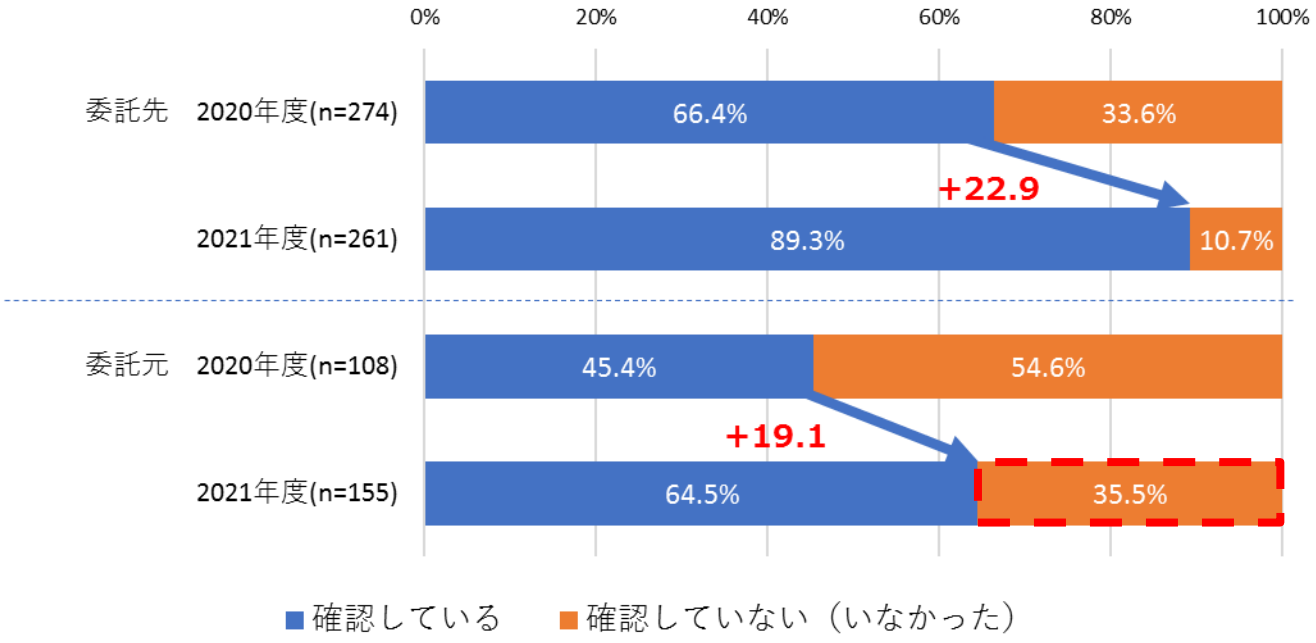


緊急事態宣言中またはコロナ禍の影響により一時的に特例や例外を認めたセキュリティ対策（Q7）（テレワーク実施経験有）

※現在=2022年1月31日

ルールの順守状況の確認は改善傾向がみられるも委託元は3割未実施

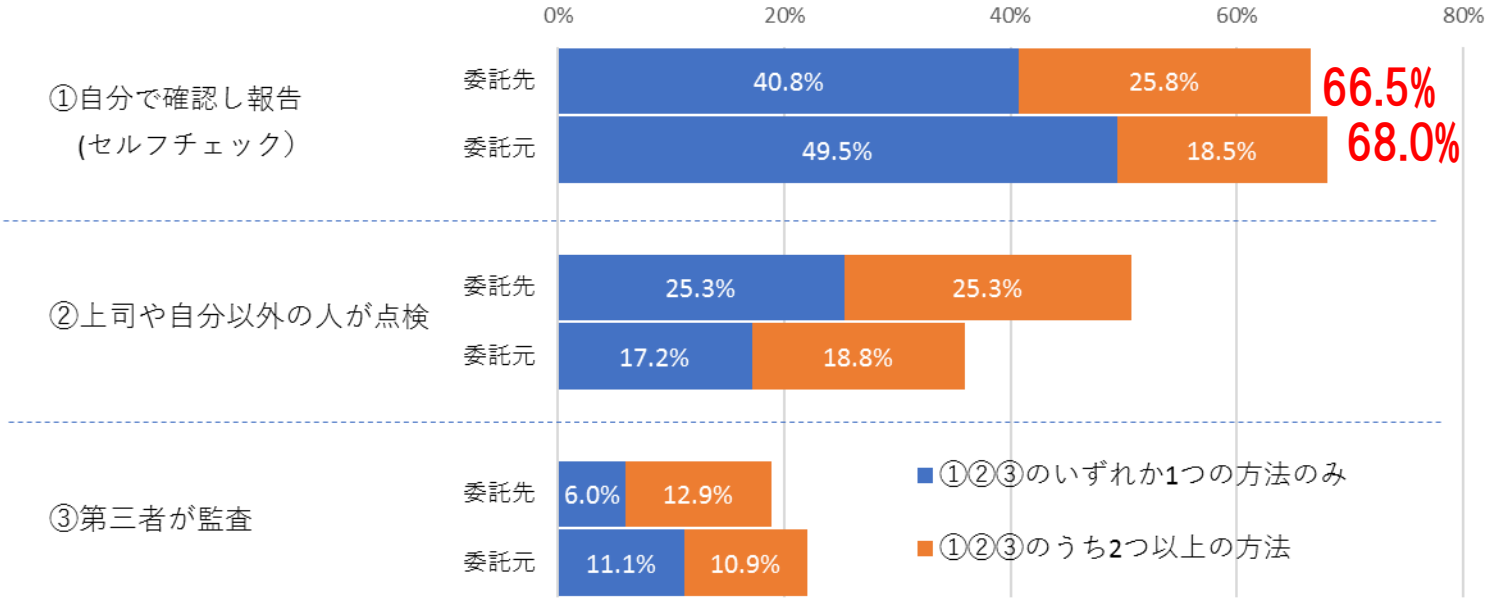
- テレワークに関する社内規定・規則・手順の順守状況を確認している組織は、委託先（ITベンダ）、委託元（ITユーザ）ともに約20ポイント改善傾向
- 委託元（ITユーザ）はいまだに35.5%が未確認



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（Q8）
（テレワーク実施経験有）

テレワークのルールの順守状況の確認方法は自己確認が6割以上

- 委託元(ITユーザ)の68.0%、委託先(ITベンダ)の66.5%がセルフチェック
- 委託先（ITベンダ）の方が複数の方法で確認

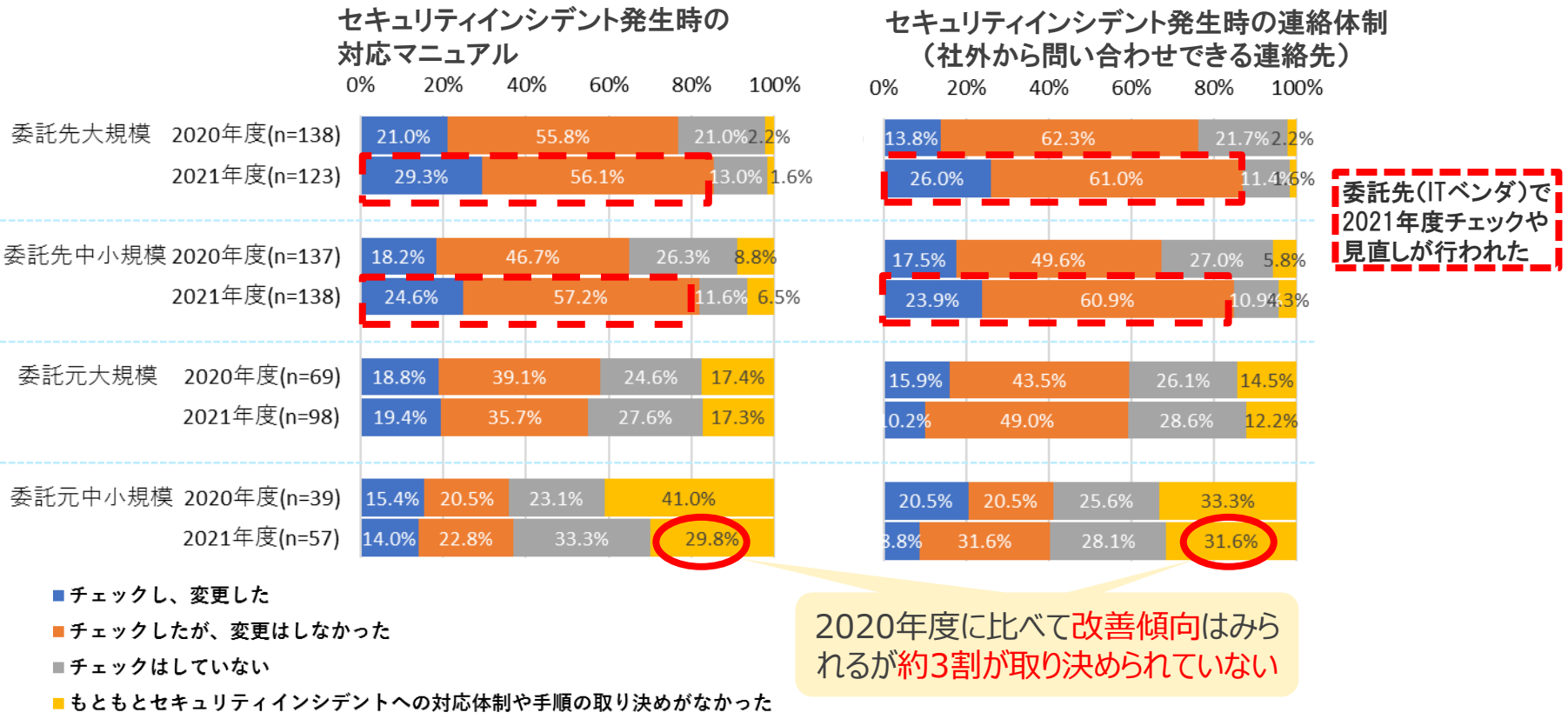


※第三者とは、外部機関や業務上直接かかわりがない社内第三者的な組織や人を指す

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方法（Q8）
（テレワーク実施経験有、確認を実施したと回答した組織）
委託先(n=233) 委託元(n=100)

委託元ではインシデント対応手順や連絡体制の確認・整備が遅れている

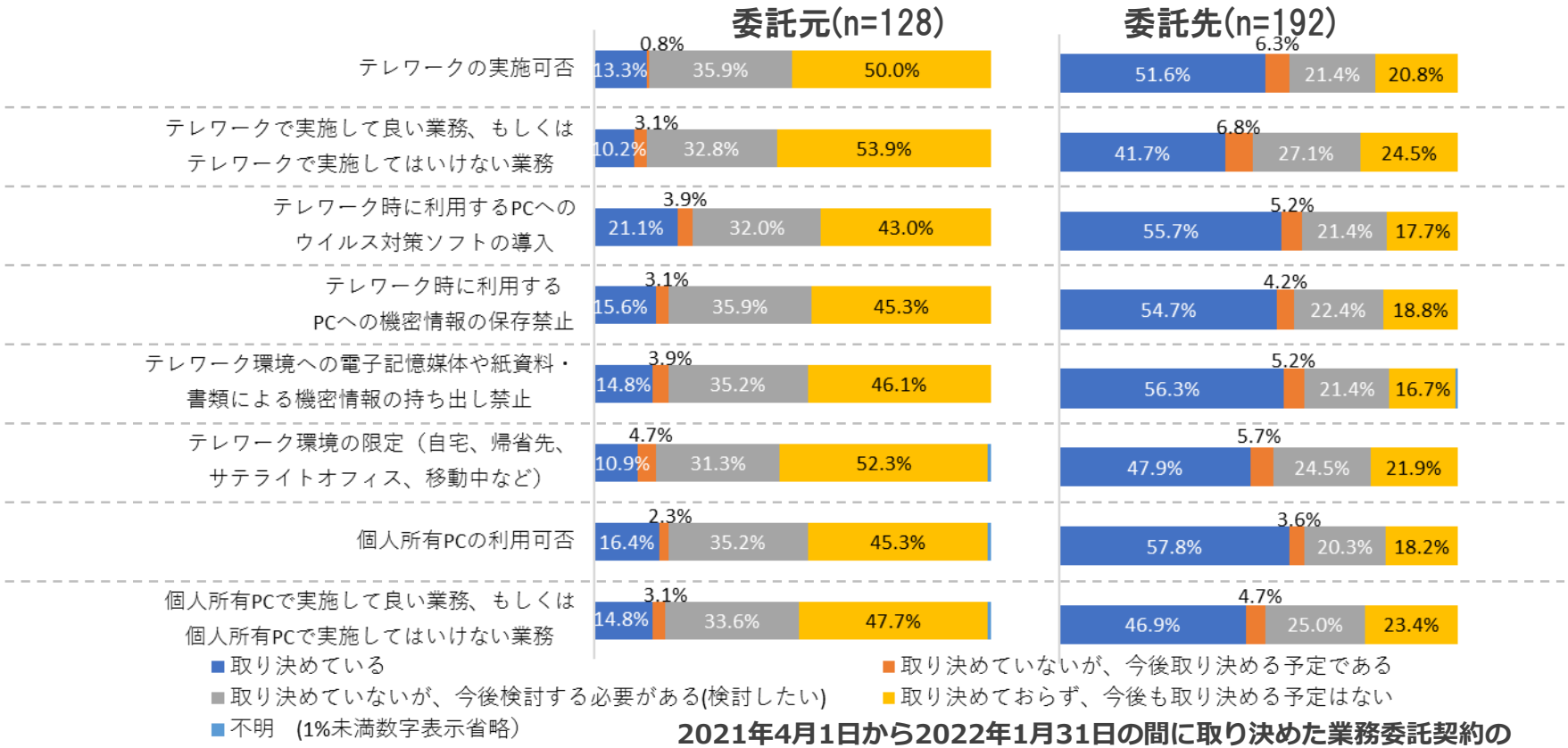
- 委託先(ITベンダ)ではマニュアルや連絡体制のチェックや見直しの割合が増えているが、委託元（ITユーザ）ではあまり変化が見られない
- 委託元(ITユーザ)の中小規模では、対応マニュアルや連絡体制がない組織が約３割



テレワーク導入後のセキュリティインシデント対応マニュアル、連絡体制のチェック(Q11)（テレワーク実施経験有）

ニューノーマルに対応した業務委託契約は徐々に検討が進んでいる

- 情報技術関連の企業が多い委託先(ITベンダ)では、テレワークを想定したセキュリティ要求事項の取り決めを約８割（今後検討、実施予定を含む）が実施
- 委託元(ITユーザ)には今後業務委託契約の項目の見直しの際に検討することで、セキュリティ対策の強化が期待される



2021年4月1日から2022年1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（Q20）(委託先、再委託先のテレワークの実施を認めている)

調査結果から得られた実態

特例・例外を認めた緩和状態の継続
→セキュリティリスクが高い状態が継続している恐れがある

- 一時的に緩めた特例・例外を現在も認めている状況が継続
- 機密情報を保存することができる媒体や会社支給PCの持ち出しについての特例・例外の継続が2020年度より増加。（委託元（ITユーザ）の傾向大）

委託元(ITユーザ)のルール整備や順守状況の確認に課題
→テレワークの頻度が低くルールの整備や確認などが後回しの可能性
→インシデント発生時の対応が迅速に行えない恐れがある

- ルールの曖昧さや社員の理解不足などの課題が残る
- インシデント対応ルールや連絡体制が未整備の組織が多い(特に中小規模)
- ルールの順守状況の確認は2020年度から改善傾向が見られるがいまだに3割の組織では確認が行われていない

委託元(ITユーザ)はテレワークを前提とした契約が進んでいない
→業務委託契約における新たなリスク

- 委託元(ITユーザ)と委託先(ITベンダ)の間の業務委託契約と比較すると、委託先(ITベンダ）と再委託先(ITベンダ）の間の方が高い割合でテレワークを想定した取り決めを実施

調査結果からの推奨事項

特例・例外による緩和状態のリスク評価と対策の検討

- 特例・例外を継続せざるを得ない場合は継続する事によるリスクの評価とリスクを低減するための追加の対策や監視強化、ルールの整備などが急務
- テレワークの継続に影響がない場合、特例・例外を解除して元に戻す事が望ましい

委託元(ITユーザ)のルール整備や順守状況の確認を促進

- テレワークの実施に伴うリスクを評価し、業務への影響度が高いものから段階的にルールの整備を行うことが重要
- ルールが理解されているか、守られているか定期的に確認する事が望ましい
- インシデント発生時には迅速な対応が求められるため、連絡体制の構築が急務、さらにインシデント発生を想定した訓練を実施する事が望ましい

テレワークを前提とした業務委託内容の取り決めの実施

- 委託元(ITユーザ)は、委託先(ITベンダ)がテレワークを行う可能性を想定し、機密性や重要性に応じてテレワークでの作業の可否や情報の管理方法など、テレワーク時に求めるセキュリティ対策を検討した上で具体的に取り決めることが望ましい

（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。

2021年度調査報告
https://www.ipa.go.jp/security/fy2021/reports/scrm/index-telework.html

過去の調査結果
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

本調査内容に関するお問い合わせ先
IPA セキュリティセンター　小山／森
E-mail: isec-info@ipa.go.jp