

テレワークにおける実施およびルール策定の 状況、実施に伴う業務委託に関する不安に 関する調査結果

～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
個人編 中間報告～

2020年12月

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

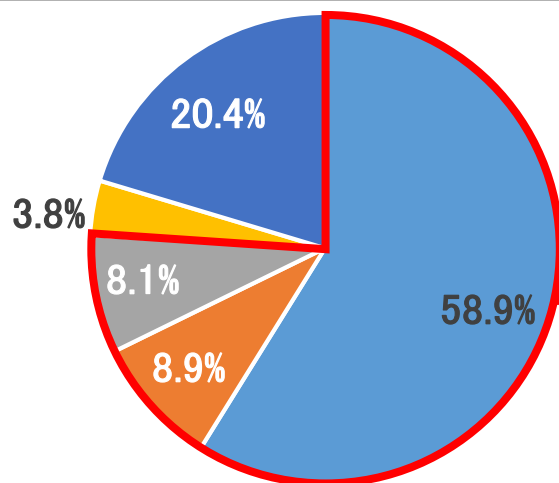
セキュリティ分析グループ

◆ 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： リサーチ会社の登録モニター
 (国内居住、18歳以上対象)
2. 調査方法： リサーチ会社を利用したWEBアンケート
3. 調査期間： 2020年11月2日(月)～11月13日(金)
4. 有効回答者数：2,372人(データクリーニング後)
 - 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企業以外の企業・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企業以外の企業・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
5. 設問数： スクリーニング設問 5問 本調査設問 42問

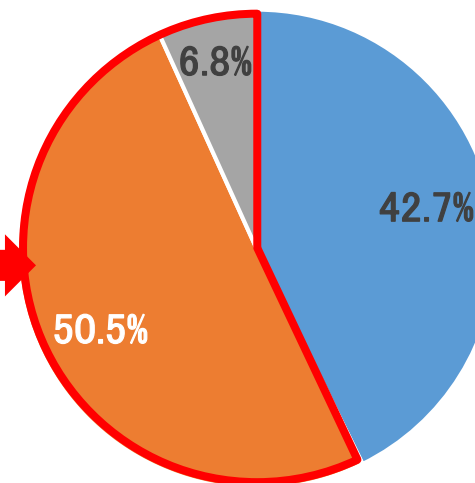
1. テレワーク実施経験のある企業のうち 約6割が緊急事態宣言以降にテレワークを導入

テレワークの導入状況(n=2372)



- 現在実施している
- 過去に実施していた時期があるが現在は実施していない。
今後また実施する予定はある。
- 過去に実施していた時期があるが現在は実施していない。
今後実施される予定はない。
- これまで実施していないが、今後実施する予定がある。
- これまで実施しておらず、今後実施する予定もない。

テレワークの導入時期(n=1800)

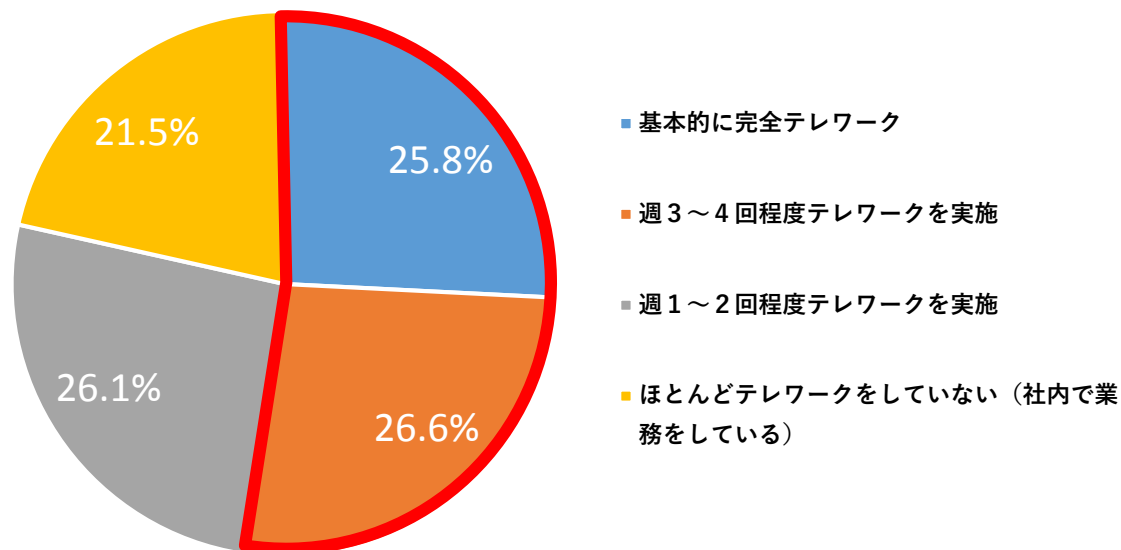


- 緊急事態宣言前（～2020年4月6日）
- 緊急事態宣言中（2020年4月7日～5月25日）
- 緊急事態宣言後（2020年5月26日～10月31日）

業務環境の変化に対応するためのセキュリティ対策の確認が必要
IPAでは「テレワークを行う際のセキュリティ上の注意事項」を公開しています
<https://www.ipa.go.jp/security/announce/telework.html>

2. テレワークを導入している企業の従業員のうち 5割強が週3回以上のテレワークを実施

テレワーク実施頻度(n=1396)

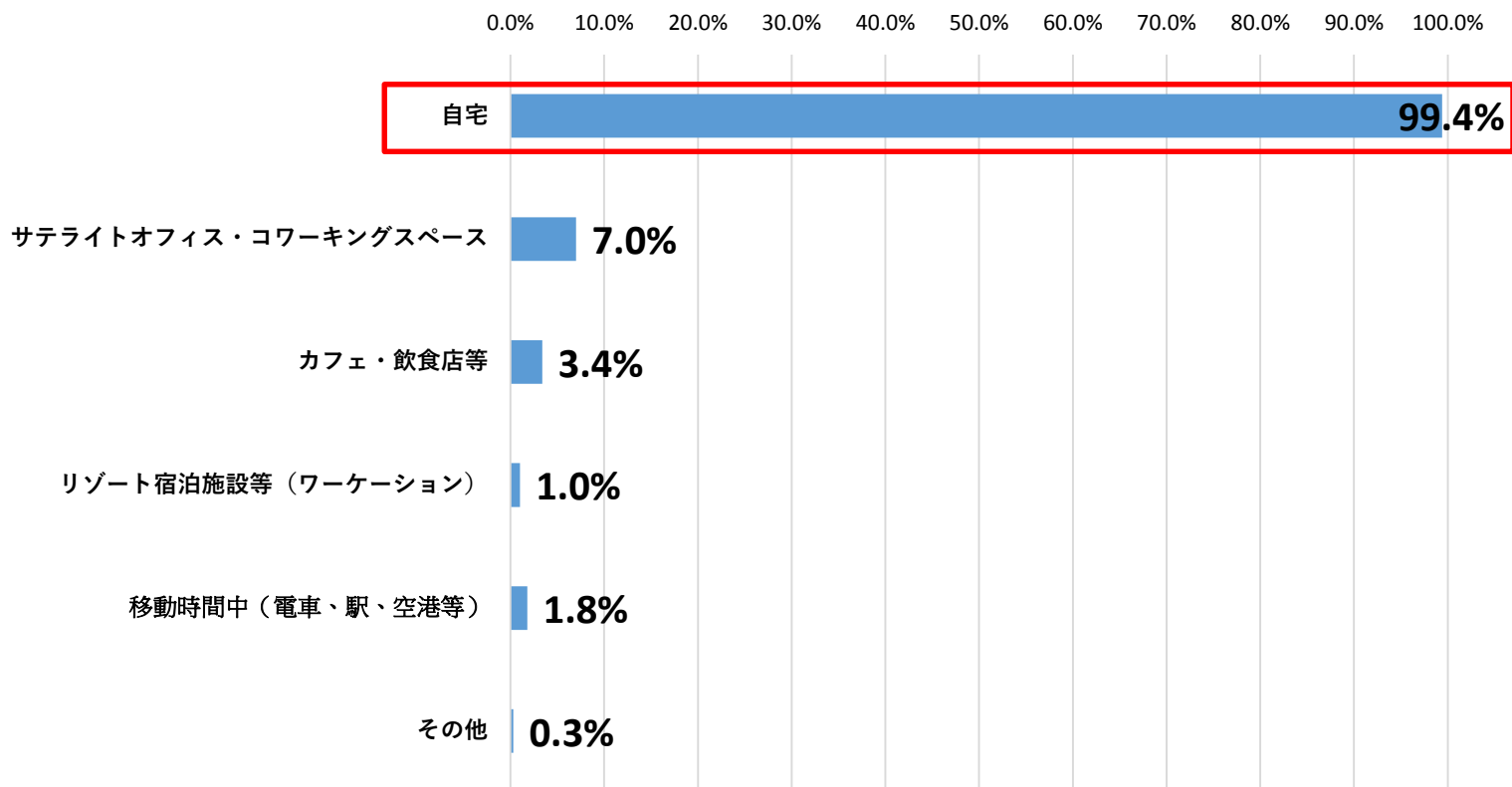


テレワーク環境から職場環境に戻る際のセキュリティ対策の確認が必要
IPAでは「テレワークを行う際のセキュリティ上の注意事項」を公開しています
(テレワークから職場に戻る際のセキュリティ上の注意事項を参照)

<https://www.ipa.go.jp/security/announce/telework.html>

3. テレワーク実施者の99%以上が 自宅でテレワークを実施

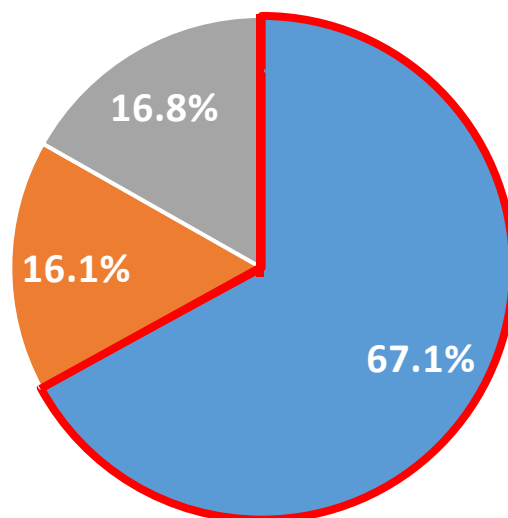
テレワーク実施場所(複数回答)(n=1096)



自宅のテレワーク環境が新しい脅威になりえる

4. テレワーク実施経験者の7割弱が 今後もテレワークを継続したいと回答

2021年1月以降もテレワークを続けたいか(n=1800)

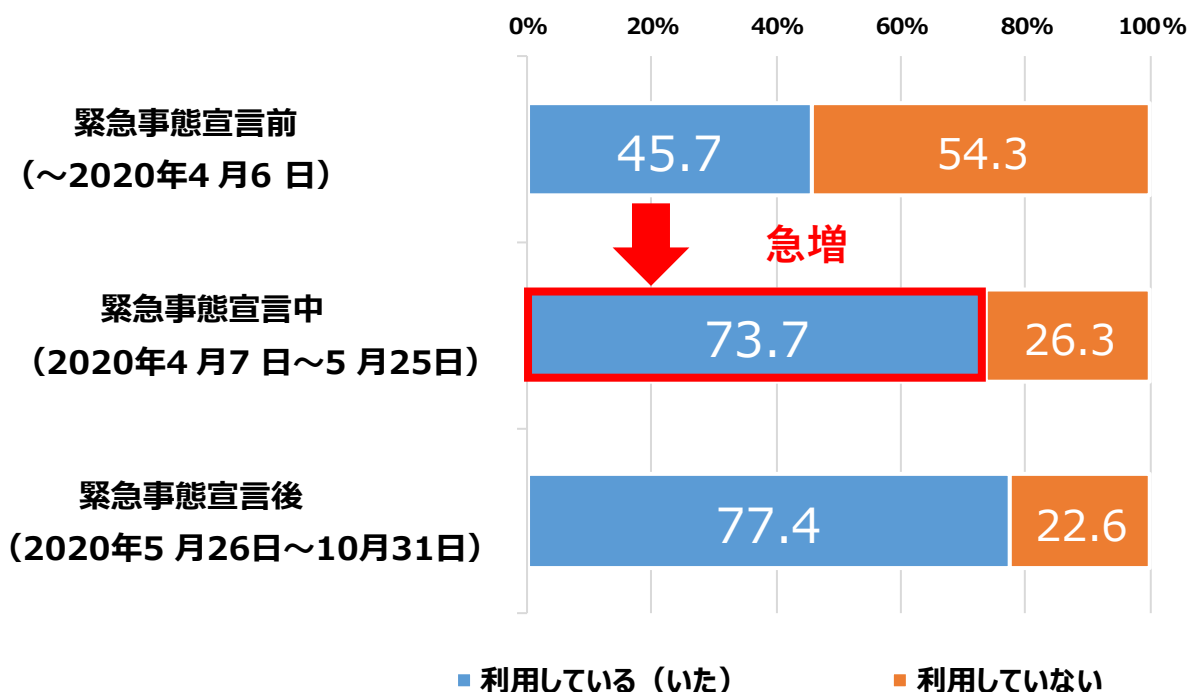


■ 続けたいと思う ■ 続けたいとは思わない ■ わからない

今後もテレワークを継続したいと考える人が多数
テレワークのセキュリティ対策の強化が必要

5. 緊急事態宣言以降 WEB会議ツールの利用が急増

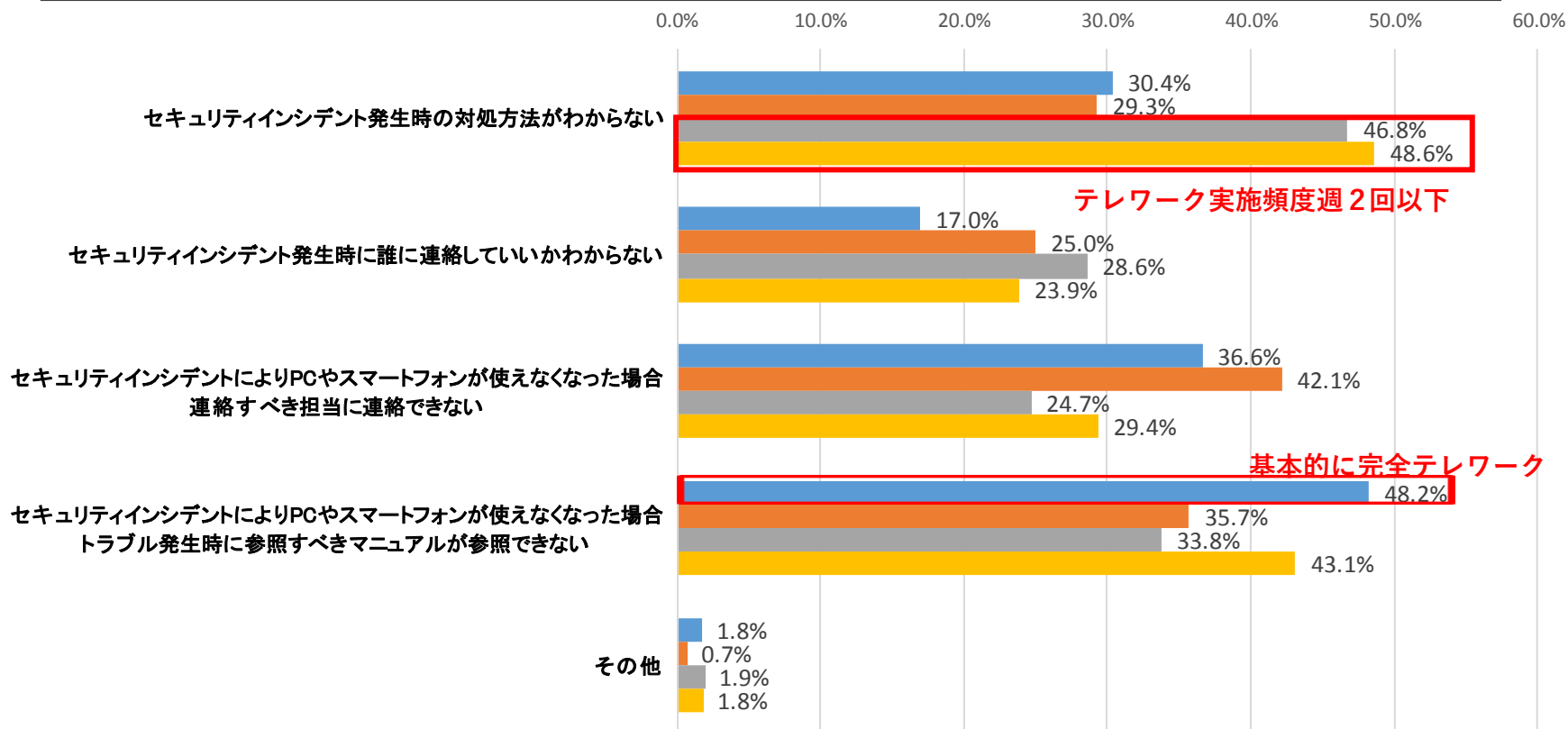
WEB会議ツールの時期別利用有無(n=2372)



業務環境の変化に対応するためのセキュリティ対策の確認が必要
IPAでは「Web会議サービスを使用する際のセキュリティ上の注意事項」を公開しています
<https://www.ipa.go.jp/security/announce/webmeeting.html>

6. 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の傾向に違い

テレワーク中のトラブル発生時の対応への不安(テレワーク実施頻度別)(n=1800)

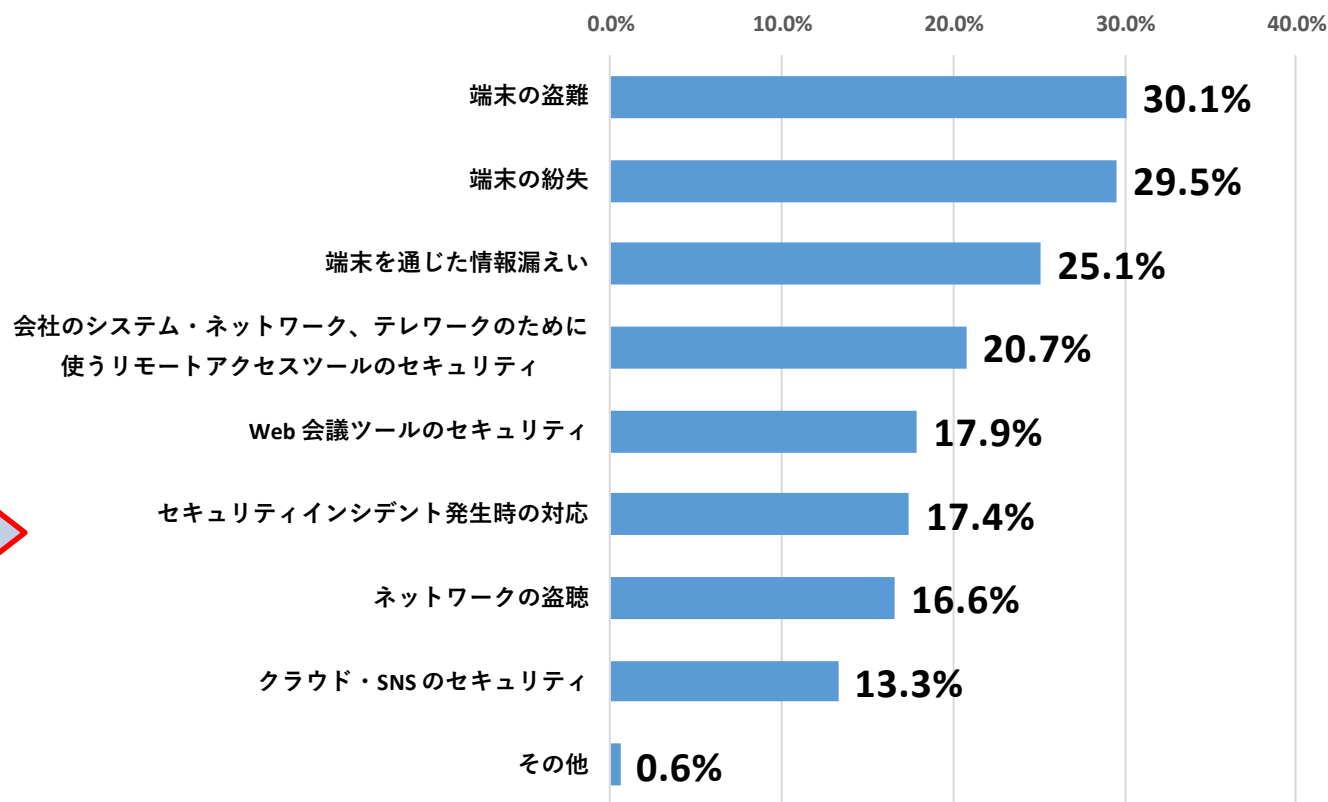
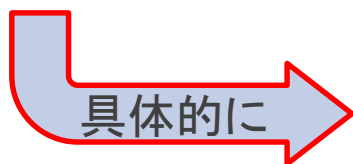
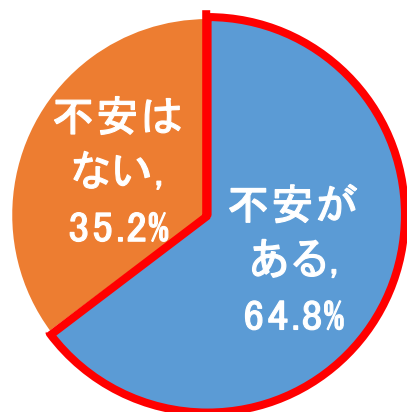


■基本的に完全テレワーク ■週3~4回程度テレワークを実施 ■週1~2回程度テレワークを実施 ■ほとんどテレワークをしていない(社内で業務をしている)

完全テレワーク実施者はマニュアルが参照できないことが不安
週2回以下のテレワーク実施者は対象方法がわからないことが不安

7. テレワークの実施で6割が不安

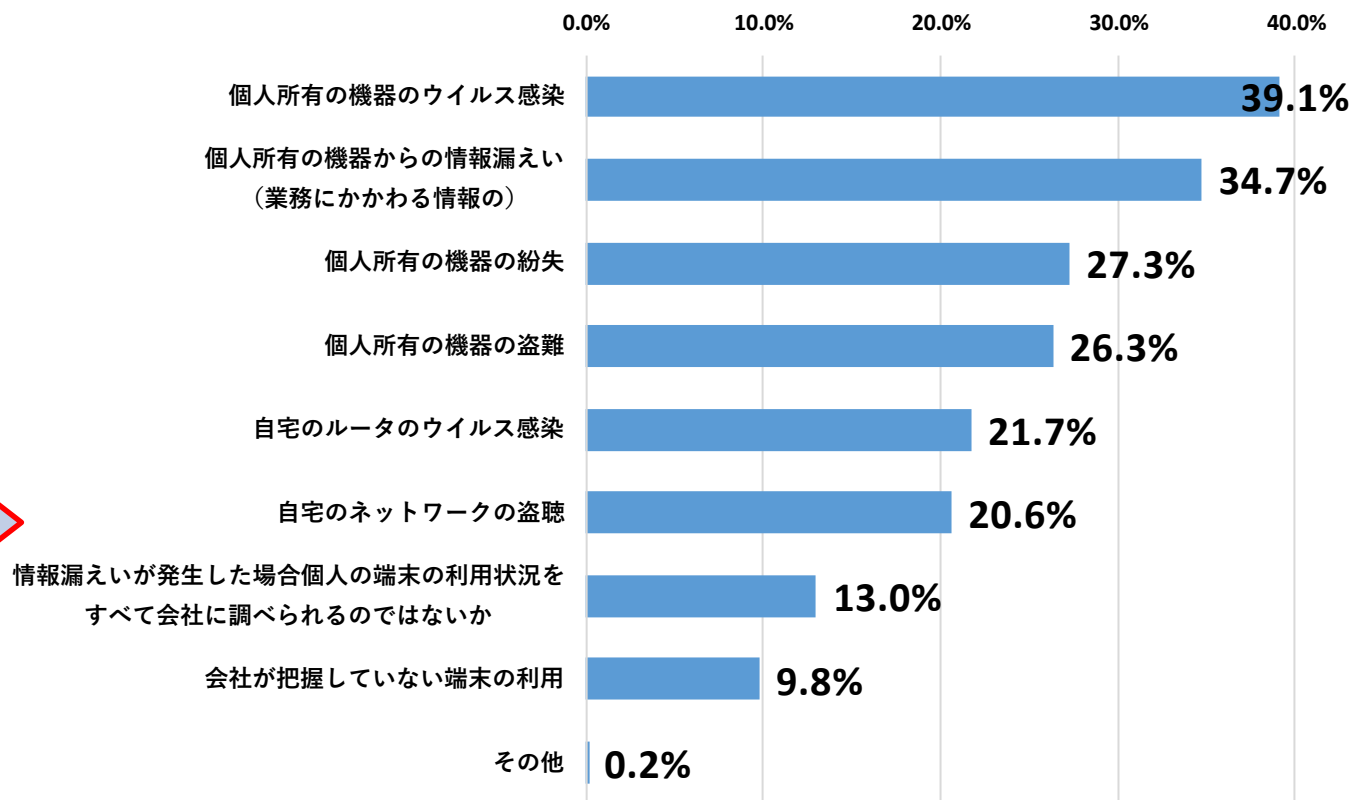
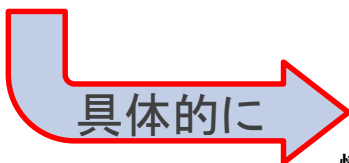
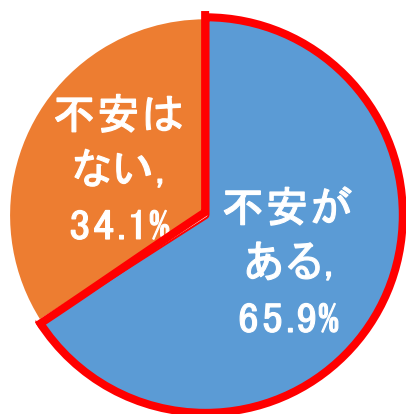
テレワークの実施で不安に思うこと(複数回答)(n=1607)



テレワークの実施における不安のトップ3は
 端末の紛失(30.1%,483人)、盗難(29.5%,474人)、情報漏えい(25.1%,403人)

8. 個人端末でのテレワークにおける インシデント発生時の責任への不安

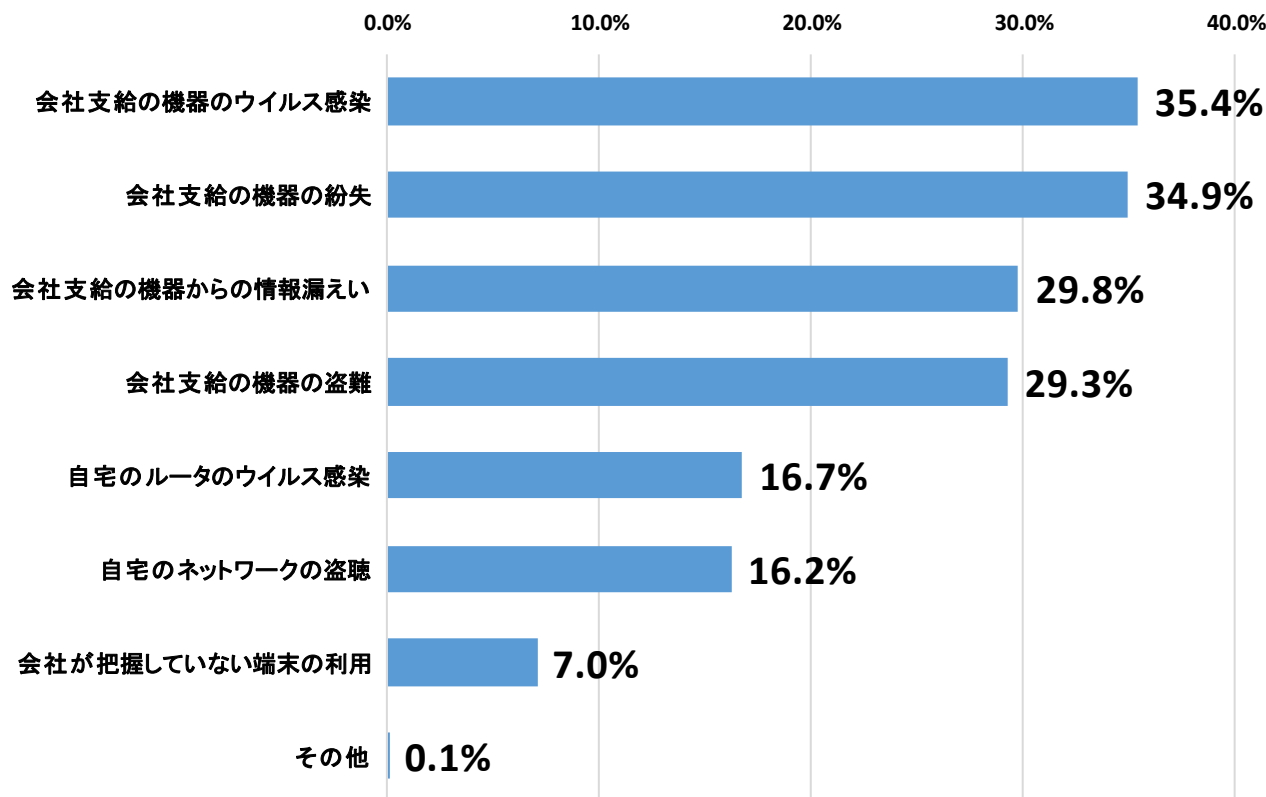
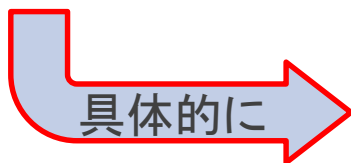
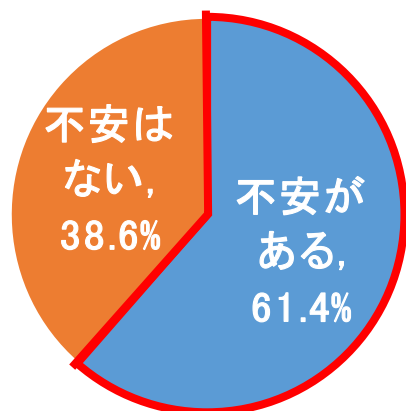
自分の責任になってしまうのではないかと不安のあるセキュリティインシデント(複数回答) (n=631)



個人端末でのテレワーク実施における不安のトップ3は
ウイルス感染(39.1%,247人)、情報漏えい(34.7%,219人)、端末の紛失(27.3%,172人)

9. 会社支給端末でのテレワークにおけるインシデント発生時の責任への不安

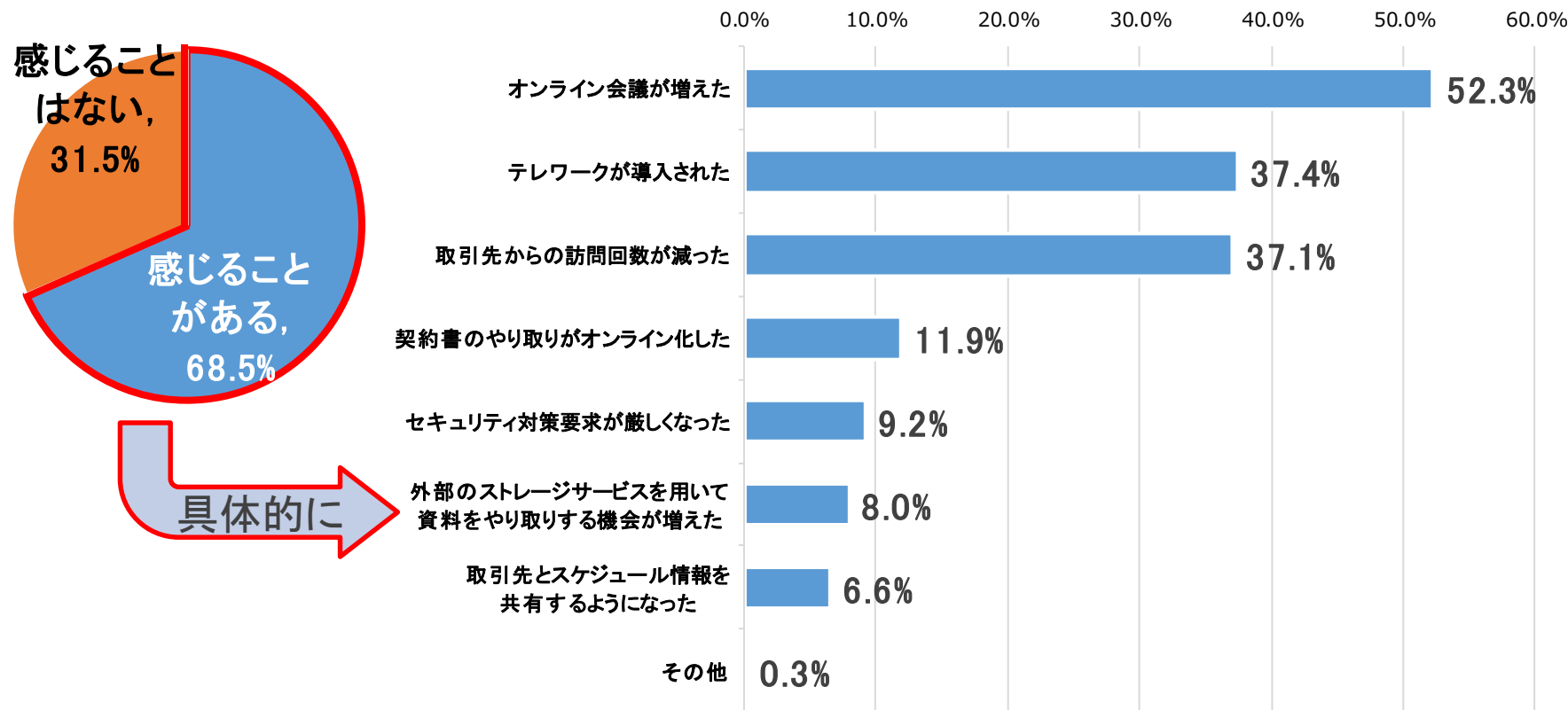
自分の責任になってしまうのではないかと不安のあるセキュリティインシデント(複数回答) (n=1535)



会社支給端末でのテレワーク実施における不安のトップ3はウイルス感染(35.4%,543人)、端末の紛失(34.9%,536人)、情報漏えい(29.8%,457人)

10. 一年前と比べて取引先の行動に変化を感じている人は7割

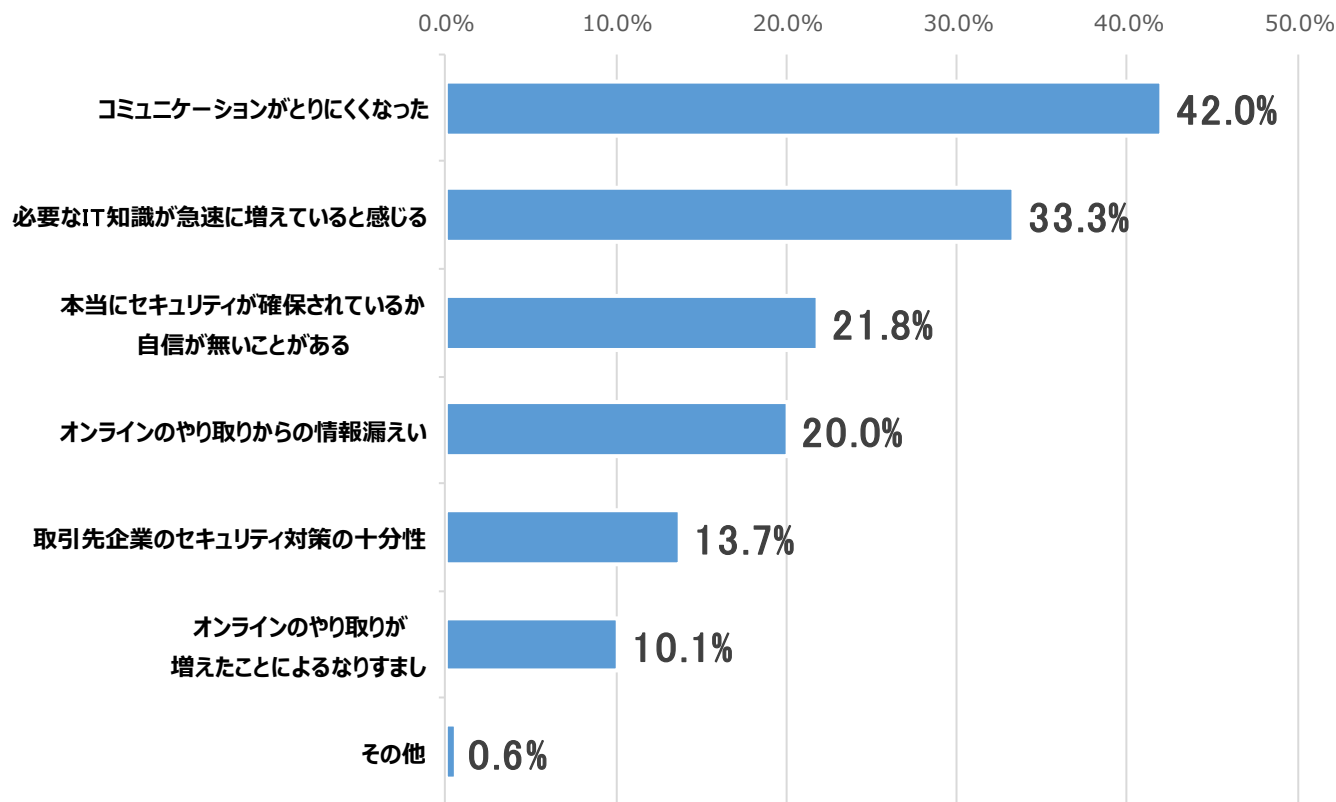
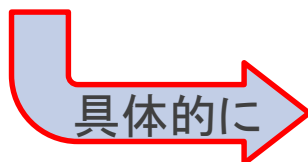
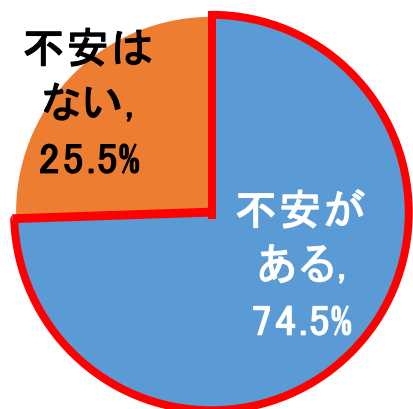
一年前と比べて取引先の行動の変化を感じる事(複数回答)(n=2372)



オンライン会議の増加(52.3%,1240人)、テレワークの導入(37.4%,887人)に伴い取引先からの訪問回数が減少(37.1%,879人)し、働き方が大きく変化していることがうかがえる

11. 取引先の行動の変化に伴い 7割強の人が不安を感じている

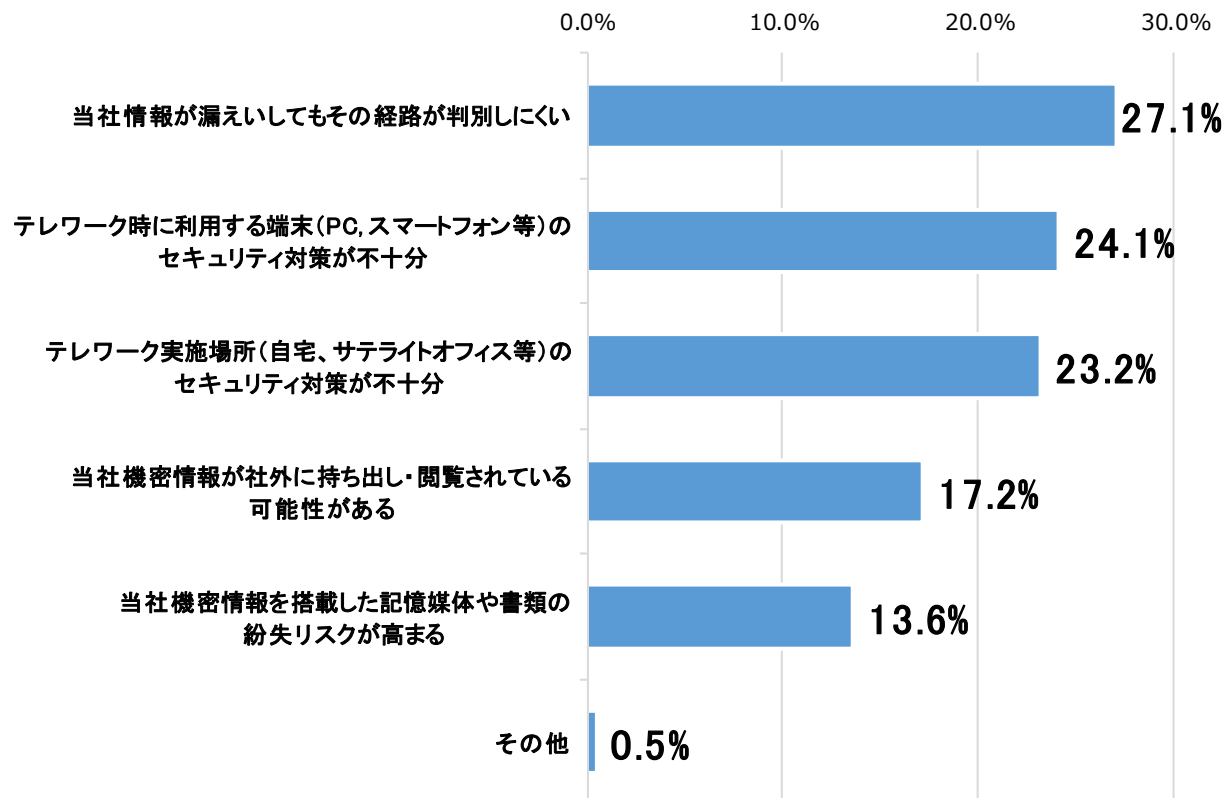
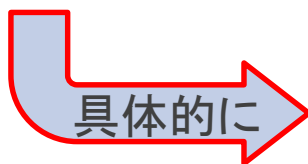
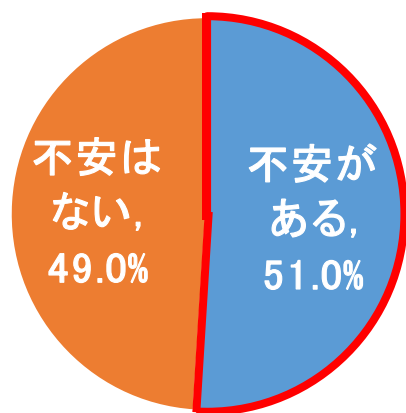
取引先の行動が変化したことで感じる不安(複数回答)(n=1626)



コミュニケーションがとりにくくなったと感じている人が42.0%(683人)で最多
急激な働き方の変化によりコミュニケーションのとりにくさを実感していることがうかがえる

12. テレワークの導入に伴う取引先のセキュリティ対策に不安を感じている人が5割

取引先がテレワークを実施することへの不安(複数回答)(n=1986)

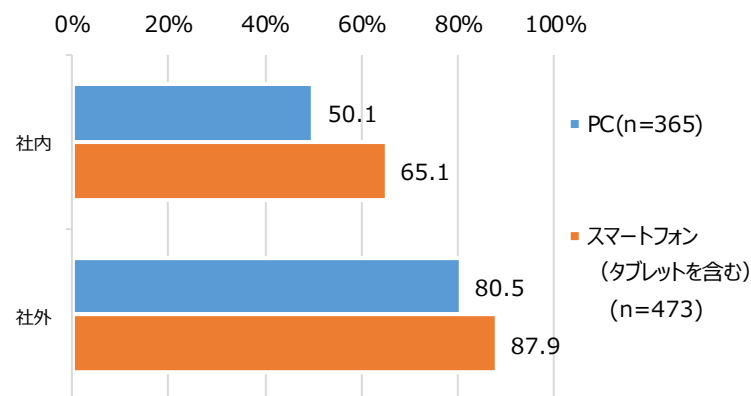
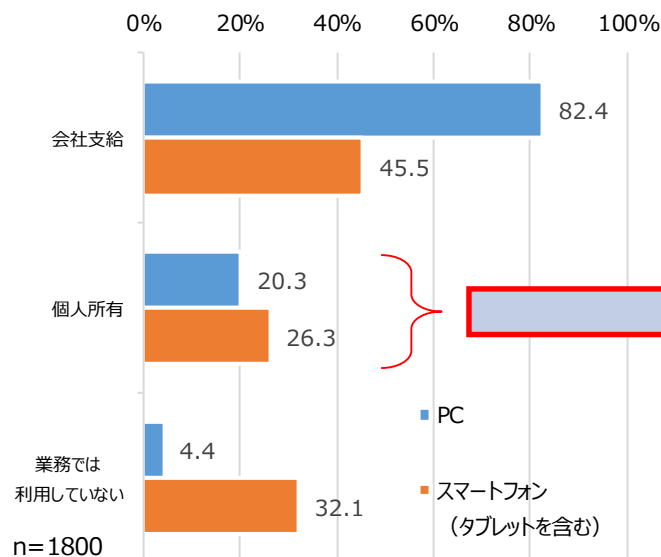


情報漏えい時の経路が判明のしにくさに不安を感じている人が27.1%(538人)で最多
テレワークの普及に伴う脅威として対策を強化していく必要がある

13. テレワークで利用するPCは 8割以上が会社支給

テレワークで利用する機器の所有元(n=1800)

個人所有機器の利用場所

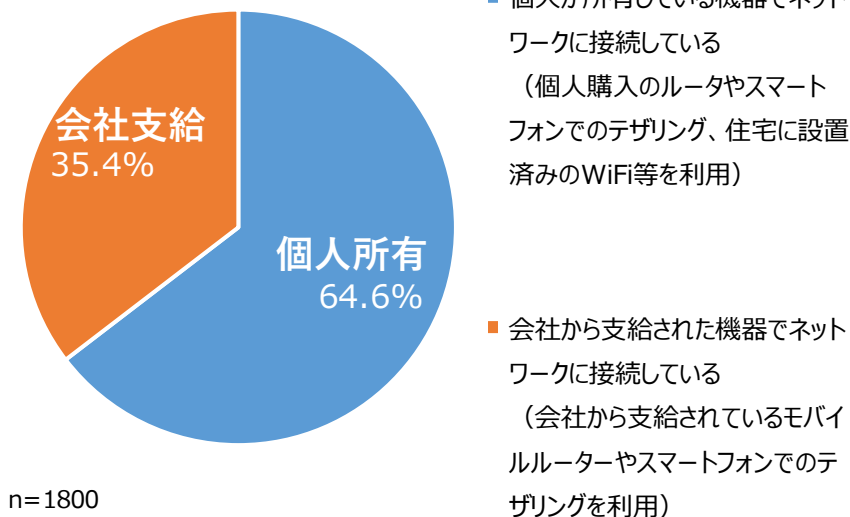


テレワークで利用するPCを会社から支給されている(されていた)人はテレワーク実施経験者の82.4%に及ぶ。

個人所有のPCが社外だけでなく、社内でも利用されている。社外からのウイルス等の持ち込み、移動時の盗難防止などに注意が必要である。

14. 自宅からのネットワーク接続は 個人所有機器の利用が6割

自宅からのネットワーク接続機器(複数回答)(n=1800)



自宅からネットワークに接続する際に利用する機器は、個人所有の機器の利用がテレワーク実施経験者の64.6%に及ぶ。

適切な設定・管理が盗聴、不正アクセスなどから守るための対策が必要である。

参考【注意喚起】家庭内における無線LANのセキュリティ設定の確認を

<https://www.ipa.go.jp/security/topics/alert270612.html>

- ◆ 企業でのテレワーク導入は緊急事態宣言により急激に加速した。オンライン会議も増え、コミュニケーションの取り方には大きな変化が生じている。このような変化に対してセキュリティの不安を感じている人も少なくない。
- ◆ 企業ではテレワークでのセキュリティ対策についてルールの見直しや実施をすすめる必要がある。（対策についてはIPAのサイトでも紹介している）
 - 「テレワークを行う際のセキュリティ上の注意事項」
<https://www.ipa.go.jp/security/announce/telework.html>
 - 「Web会議サービスを使用する際のセキュリティ上の注意事項」
<https://www.ipa.go.jp/security/announce/webmeeting.html>

調査は継続しており、企業編の調査結果についても公開予定。

◆ 本資料は以下でダウンロードできます。

- <https://www.ipa.go.jp/security/fy2020/reports/scrm/index.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

2021年1月28日 BYODの利用実態を追加(13. 14.)
問い合わせ先メールアドレスの誤り修正