

テレワークのセキュリティについて

令和2年10月
サイバーセキュリティタスクフォース事務局

テレワークにおけるセキュリティ対策の強化

- 総務省では従来から「**テレワークセキュリティガイドライン**」を策定し、**セキュリティ対策の考え方**を示している。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、**実践的かつ具体的で分かりやすい内容のチェックリスト**を作成し、2020年9月に公表。
- またチェックリスト策定と併せ、**セキュリティ対策**に関する**実態調査**と**専門的な相談対応**を実施中。

チェックリストの策定

テレワークセキュリティガイドライン

(2018年4月 第4版)

2004年12月初版
2006年4月第2版
2013年3月第3版



【想定読者像】

- ✓ システム管理者のほか経営層や利用者を幅広く対象
- ✓ 専任の担当や部門が存在
- ✓ 基本的なIT用語は仕組みとして理解しているレベル
- ✓ 基本的なシステム設定作業は、補助解説なく実施可能

追加

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)

(2020年9月 初版)

【想定読者像】

- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本的なIT用語は聞いたことがあるレベル
- ✓ 基本的なシステム設定作業は検索しながら実施可能



テレワーク方式を特定し、その方式に**対応するチェックリスト**を確認

チェックリストは**最低限のセキュリティ**を確実に確保してもらうためのものに限定

テレワーク用ソフトについて、**設定解説資料**を作成し具体的設定を解説

2020年度内に改定予定

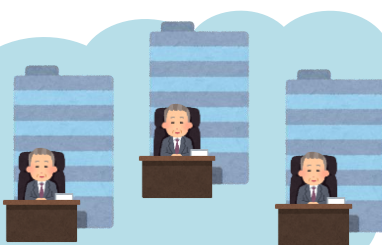
2020年内を目途に実態調査の結果等を踏まえて改定予定

実態調査／専門相談対応

テレワーク導入企業が拡大しており、セキュリティ等の実態や課題について調査（結果はチェックリスト策定にもフィードバック）



テレワーク導入企業



テレワーク導入時・導入後におけるセキュリティ対策の専門的な相談

公表先

相談申込先



https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワークセキュリティに関する手引き（チェックリスト）

- 総務省では従来より「**テレワークセキュリティガイドライン**」を策定し、セキュリティ対策の考え方を示している。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、**実践的かつ具体的で分かりやすい内容**の資料が求められている。

→ テレワークにおける**最低限のセキュリティを確実に確保**してもらうための**手引き（チェックリスト）**を作成。

【手引き(チェックリスト)の想定読者像】

- ✓ セキュリティの**専任担当がい**ないような中小企業等における、**システム管理担当者**
- ✓ 専門的なIT用語（例：VPN）は聞いたことがあるが、**仕組みを理解できていないレベル**

- 平行して実施した実態調査※の結果を踏まえて**年内に改定版（第2版）を作成・公表予定**。

※ 全国の3万事業者に対して本年8月に調査を実施。テレワークを導入している約1,500社から回答。

		ガイドラインの想定読者像	手引き（初版）の想定読者像
対象属性		システム管理者のほか 経営層や利用者を幅広く対象	システム管理担当者
セキュリティ 予算		外部委託コストは必要に 応じて捻出するレベル	外部委託コストの捻出は難しいレベル
セキュリティ 推進体制		専任の担当・担当部門が存在する	専任は存在しない
セキュリティ リテラシ		「適切に…」 「レベルに応じて…」等の読者に解釈をゆだねるような抽象的な要求に対して、対応内容を検討・判断し、対策を実行できる	「適切に…」 「レベルに応じて…」等の読者に解釈をゆだねるような抽象的な要求だけでは、対応すべき内容がわからない
ITリテラシ		VPN・フィルタリング・アンチウイルス等の基本的なIT用語は仕組みとして理解しているレベル システム設定作業は、基本的な内容であれば、無理なく行うことができる	VPN・フィルタリング・アンチウイルス等の基本的なIT用語は聞いたことがあり、利用シーンがイメージできるレベル システム設定作業は、基本的な内容であれば、インターネット検索によって調べながら行うことができる

※第2版では、IT用語で利用シーンのイメージができないレベルやシステム設定作業も手順書がないと実施できないレベルにも対応を目指す

手引きの構成とチェックリスト作成に当たっての考え方

- 手引きは、主に第1部・第2部から構成。
 - ✓ **第1部**で、本手引きの読者は自分の組織が採用する**テレワーク方式を確認・特定**
 - ✓ **第2部**では、第1部で特定した**テレワーク方式に対応するチェックリストを確認**
- チェックリストについては、セキュリティ確保を図る上で**優先対応すべきものがわかりやすいよう配慮**
 - ✓ セキュリティ**重要度が高く**、対策**実施が易い**ものは「◎」、**それ以外**を「○」として、優先順位をつけて整理
 - ✓ セキュリティ**重要度が低い**ものや、対策**実施が難しい**ものは、チェックリスト**対象外**として整理
- テレワークで**広く使われているソフトウェア**については、具体的な設定例として、**設定解説資料を作成**※
 - ※ 手引きの初版では、オンライン会議システムとして、Microsoft Teams、Cisco WebEx Meeting、Zoomの3製品分の解説資料を作成（第2版に向けて、順次拡張していく予定）

第1部

第2部

参考

手引きの構成

- 1 はじめに
- 2 **テレワーク方式の確認**
- 3 テレワーク方式の解説
- 4 テレワーク環境で想定される脅威の解説

読者の行動

- 自社に適合しているテレワーク方式の確認・特定
- 自社のテレワーク環境において想定される脅威の理解

- 1 **テレワーク方式ごとのセキュリティ対策チェックリスト**
- 2 セキュリティ対策チェックリストの設定例一覧
→補足文書として**設定解説資料**を用意
- 3 テレワーク環境のセキュリティ対策と想定脅威一覧

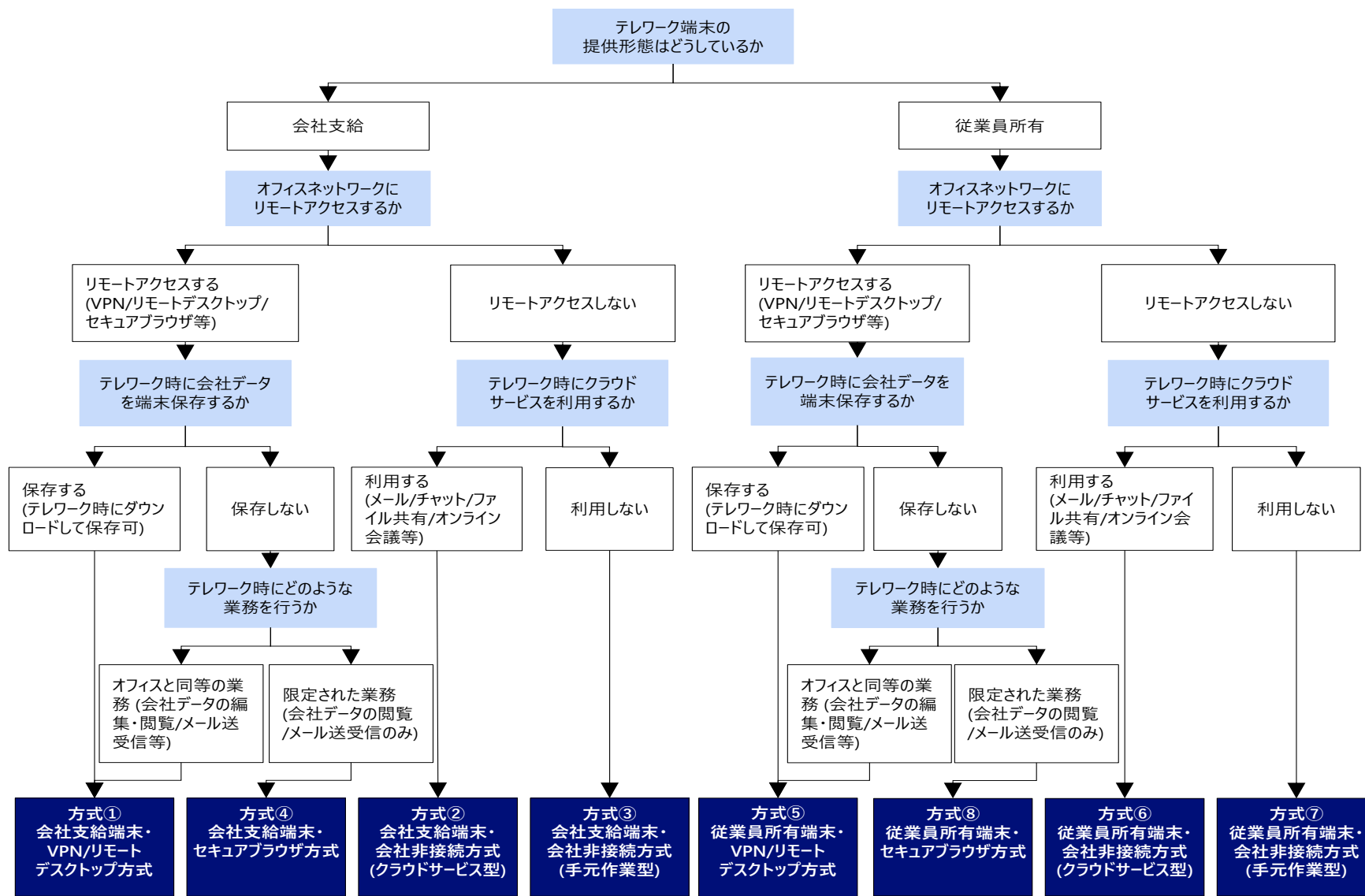
- 第1部で特定したテレワーク方式に対応したチェックリストの特定
- 当該チェックリスト記載のセキュリティ対策実施
- 各セキュリティ対策に紐づく脅威の確認

- 用語集
- テレワークセキュリティに関する参考情報

- （下記を必要に応じて実施）
- 本書記載の用語の理解
 - 参考文献等の閲覧
 - 困った場合の問合せ先

(参考) 手引きにおけるテレワーク方式

- 中小企業等において利用が想定するテレワーク環境のパターン（8方式）を手引きの対象として検討。
- フローチャートを活用して、手引きの読者となる組織がどのテレワーク方式に該当するか特定できるよう配慮。



(参考) セキュリティチェックリストの例 (方式①)

優先度：◎の項目

(全 10 項目)

No.	対策分類	対策内容	想定脅威
2-1	マルウェア対策	☐ テレワーク端末にウィルス対策ソフトをインストールし、リアルタイムスキャンが有効になる設定としている。またウィルス対策ソフトの定義ファイルを自動更新する設定、もしくは手動で最新に更新するルールを作成している。	マルウェア感染
3-1	アクセス制御（論理）	☐ システムによるアクセス制御や重要情報そのものに対するパスワード設定等により、重要情報は許可された人のみが利用できるようにしている。	不正アクセス
4-1	アクセス制御（物理）	☐ テレワーク端末に対して覗き見防止フィルタを貼付し、離席時にはスクリーンロックをかけるようルール化している。	情報の盗聴
5-1	脆弱性管理	☐ テレワーク端末はメーカーサポート切れとなるバージョンのOSやアプリケーションソフトウェアは利用していない。	不正アクセス
(以下略)			

優先度：○の項目

(全 21 項目)

No.	対策分類	対策内容	想定脅威
2-2	マルウェア対策	☐ 不審なメールの開封や、そのメールに記載されているURLのクリック、添付ファイルを開かないように注意喚起をしている。また利用しているメール製品に不審なメールを除外する機能がある場合は有効化している。（クラウドサービス（Webメール）の利用が無い場合は対象外）	マルウェア感染
2-3	マルウェア対策	☐ テレワーク端末（スマートデバイス）へのアプリのインストールは、安全であることが確認できる方法（公式アプリケーションストアの利用等）によるインストールに限定する。	マルウェア感染
3-2	アクセス制御（論理）	☐ インターネット経由で社内システムにアクセスする際に必要なポートやIPアドレス以外からのアクセスを、社内ネットワークとインターネットの境界線に設置されているファイアウォールやルーター等にて遮断している。	不正アクセス
(以下略)			

テレワークのセキュリティに関する相談対応

- 総務省では従来から、**テレワークに関する幅広い相談**について、**テレワークマネージャー相談事業**により対応。
- 今般、中小企業等においてもテレワーク利用が急速に広まっており、適切かつ十分なセキュリティ対策がとられていない可能性もあることから、**セキュリティに関する不安**、具体的な**セキュリティ対策方法**、ルール作りや自社の実施状況の適切性の**コンサルティング**などを**相談できる窓口を開設**しています。
- **セキュリティの専門家**に対して、**無料**で気軽に相談可能ですので、是非ご利用を検討ください。

導入前のお悩み

私物のパソコンを従業員に使わせても問題ないの？

これからテレワークの仕組みを作りたいけど、セキュリティは何をすればいいの？

アクセス制限が必要と聞いたけど、何をどう設定すればいいの？



導入後のお悩み

とりあえずテレワークの仕組みは作ったけれど、セキュリティ的に大丈夫なの？

情報漏えいが心配だけど、従業員への教育は必要？何をすればいいの？

情報セキュリティのルールづくりで考慮すべきポイントは何？

相談費用

無料

相談対応期間

2021年3月まで

相談対応方法

申込の後、相談者の希望に応じて、電話・メール・Web会議により対応します。

相談の申込先

<https://www.lac.co.jp/telework/security.html>

※本事業は、総務省が株式会社ラックに委託し、実施しています。
セキュリティ専門企業の同社の専門家が相談対応に当たります。



テレワークセキュリティガイドラインの概要

- テレワークを導入しようと考えている企業において、**情報セキュリティ対策に関する検討の参考としてもらうことを目的**として、総務省にて策定・公表。
- 2018年4月、社会や技術の変化（クラウドサービスやSNSの普及等）、新たなセキュリティ上の脅威（無線LANの脆弱性、ランサムウェアや標的型攻撃の登場等）などを踏まえた改定（第4版）を実施。



テレワークセキュリティガイドライン
(2018年4月 第4版)

2004年12月初版
2006年4月第2版
2013年3月第3版

テレワークセキュリティガイドライン（第4版）構成

はじめに

✓ セキュリティ対策の必要性や本ガイドラインの位置付け等を記載

1. テレワークにおける情報セキュリティの考え方

- (ア) 「ルール」「人」「技術」のバランスがとれた対策の実施
- (イ) テレワークの方法に応じた対策の考え方
- (ウ) 経営者、システム管理者及びテレワーク勤務者それぞれの立場

✓ 私用端末利用(BYOD)やクラウドサービス利用の留意点を追加

2. テレワークセキュリティ対策のポイント

- (ア) 経営者が実施すべき対策
- (イ) システム管理者が実施すべき対策
- (ウ) テレワーク勤務者が実施すべき対策

✓ 経営者・システム管理者・テレワーク勤務者という類型ごとに実施すべき対策を記載
✓ 第3版で33項目だったものを、計43項目に再編（無線LANの脆弱性対策(VPNの利用、https接続等)やSNS利用の留意事項等を追加)

3. テレワークセキュリティ対策の解説

- (ア) 情報セキュリティ保全対策の大枠
- (イ) マルウェアに対する対策
- (ウ) 端末の紛失・盗難に対する対策
- (エ) 重要情報の盗聴に対する対策
- (オ) 不正アクセスに対する対策
- (カ) 外部サービスの利用に対する対策

✓ 「2. テレワークセキュリティ対策のポイント」で明示した内容について、対策分野ごとに詳細に解説
✓ 「実施すべき基本的な対策」(基本的対策事項)と、「実施することが望ましい対策」(推奨対策事項)に分けて解説
✓ 「トラブル事例や対策」や「コラム」を追加

用語集

参考リンク集

テレワークセキュリティに関する実態調査①

➤ 企業等におけるテレワークに関するセキュリティ等の実態を把握するための調査をWebアンケートにより実施。
 (地域:全国 期間:2020.7.29-8.24 手法:調査票郵送・Web回答 対象数:30,000(従業員10名以上) 回答数:5,433(テレワーク実施企業1,569))

スクリーニング設問

※スクリーニング設問は5,433社が回答

- S-1 テレワークの導入状況
- S-2 テレワークの導入時期
- S-3 新型コロナ収束後のテレワーク活用予定
- S-4 新型コロナ収束後にテレワークを活用しない理由
- S-5 テレワークの全従業員に対する利用割合
- S-6 導入しているテレワークの形態
- S-7 テレワークを導入しない理由
- S-8 テレワークで行っている具体的な業務・実施方法
- S-9 新たにテレワーク化・テレワーク利用拡大したい業務・実施方法

1 情報セキュリティ管理体制

※これ以降の設問はテレワーク導入済みの1,569社が回答

- 1-1 情報セキュリティ管理体制
- 1-2 昨年度のIT投資予算
- 1-3 今年度のテレワーク推進の予算
- 1-4 セキュリティに予算を割くことへの理解

2 テレワークの使用端末・構成方式

- 2-1 テレワークに使用しているPC端末
- 2-2 「会社支給のPC端末」の具体的な使用方法
- 2-3 「従業員所有のPC端末」へのデータ保存に関する対応
- 2-4 テレワークに使用しているモバイル端末
- 2-5 「会社支給のモバイル端末」へのデータ保存に関する対応
- 2-6 「従業員所有のモバイル端末」へのデータ保存に関する対応
- 2-7 使用している会社所有の端末(PC端末・モバイル端末)の種類
- 2-8 テレワーク用のPC端末から社内のシステムや情報にアクセスする場合の接続方法
- 2-9 テレワーク用のモバイル端末から社内のシステムや情報にアクセスする場合の接続方法

3 その他のテレワーク利用製品

- 3-1 テレワークで利用しているウイルス対策製品
- 3-2 テレワークで利用しているデバイス管理製品・サービス
- 3-3 テレワークで利用しているセキュアブラウザ
- 3-4 テレワークで通常利用しているブラウザ
- 3-5 テレワークで利用しているVPN製品
- 3-6 テレワークで利用しているリモートデスクトップ製品
- 3-7 テレワークで利用しているWEB会議システム
- 3-8 テレワークで利用しているメールサービス
- 3-9 テレワークで利用しているチャットツール
- 3-10 テレワークで利用しているストレージサービスの製品
- 3-11 テレワークで利用しているクラウドアクセス用のネットワークセキュリティ製品
- 3-12 テレワークで利用している仮想デスクトップ方式の製品
- 3-13 テレワークで利用しているアプリケーション・ラッピング方式の製品

4 セキュリティ対策の状況

- 4-1 「テレワークセキュリティガイドライン」の認知度
- 4-2 テレワークセキュリティガイドラインの活用により役立った点
- 4-3 テレワークセキュリティガイドラインを活用しなかった理由
- 4-4 テレワーク導入検討に当たり時間や労力を費やした点
- 4-5 情報セキュリティの管理体制等に関する対策の実施状況
- 4-6 各種サイバー攻撃に関する対策の実施状況

5 その他

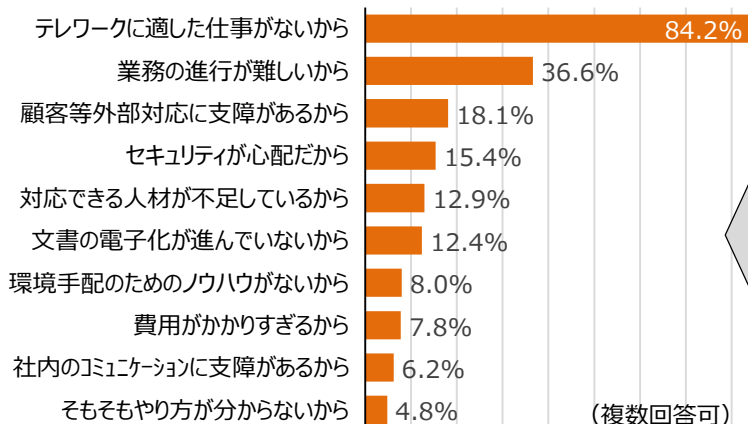
- 5-1 テレワーク導入目的
- 5-2 テレワーク導入目的に対しての効果
- 5-3 テレワークの導入により働き方で大きく変革した点
- 6-1 テレワークの導入にあたっての課題
- 6-2 セキュリティ確保への具体的な課題
- 7-1 テレワークを導入する際に必要を感じた支援
- 7-2 テレワークを有効活用する上で利用したい支援

テレワークセキュリティに関する実態調査②

➤ 企業等におけるテレワークに関するセキュリティ等の実態を把握するための調査をWebアンケートにより実施。
(地域:全国 期間:2020.7.29-8.24 手法:調査票郵送・Web回答 対象数:30,000(従業員10名以上) 回答数:5,433(テレワーク実施企業1,569))

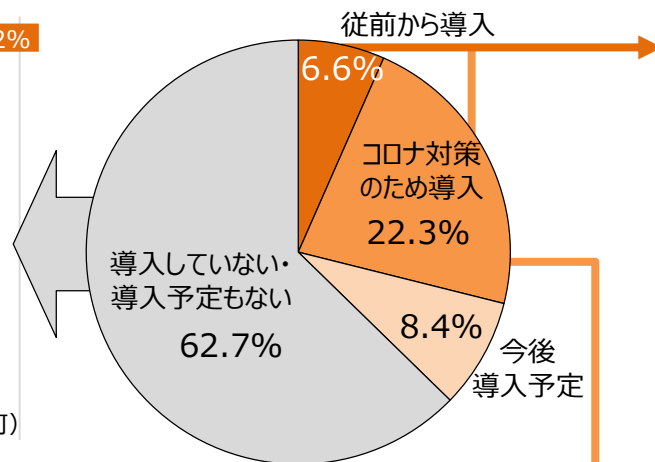
テレワークを導入しない理由

(n=3,406:テレワーク未導入企業)



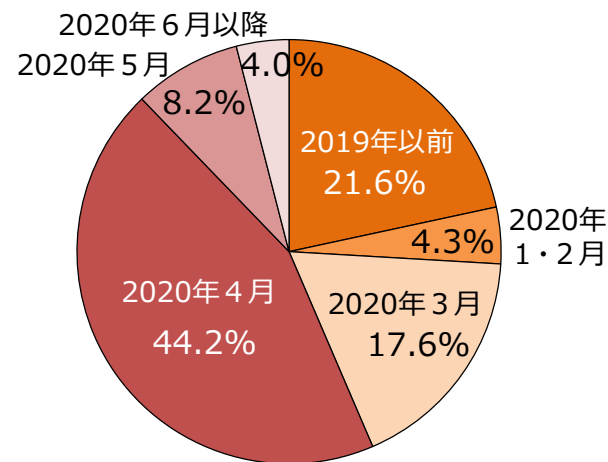
テレワークの導入状況

(n=5,433)



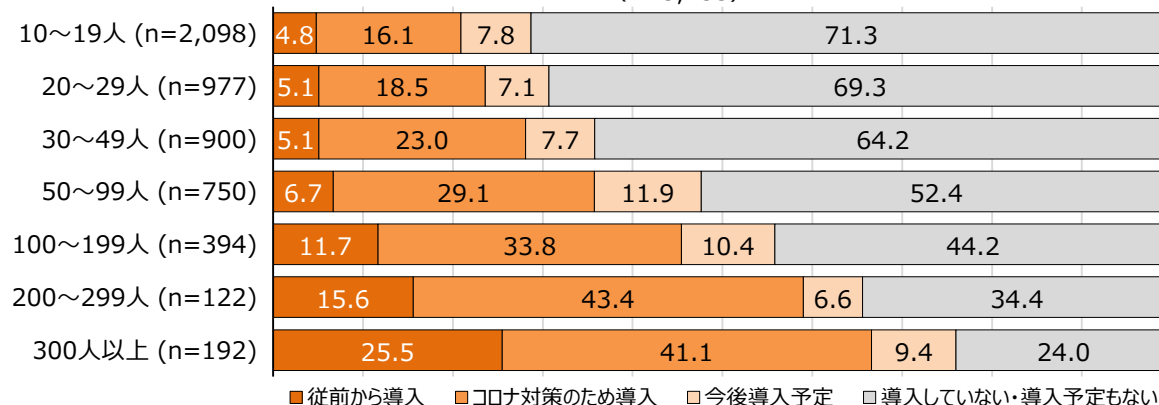
テレワークの導入時期

(n=1,569:テレワーク導入企業)



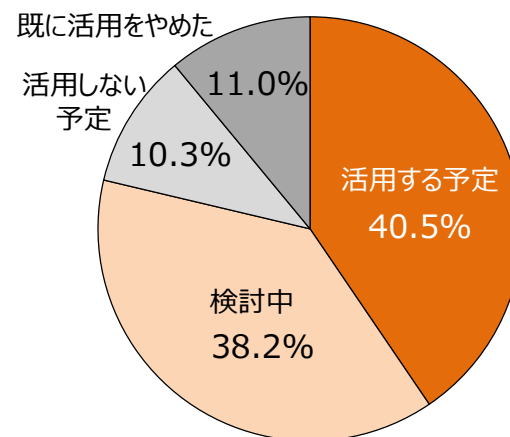
テレワークの導入状況(従業員規模別)

(n=5,433)



新型コロナ収束後のテレワーク活用予定

(n=1,209:コロナ対策のためテレワーク導入した企業)

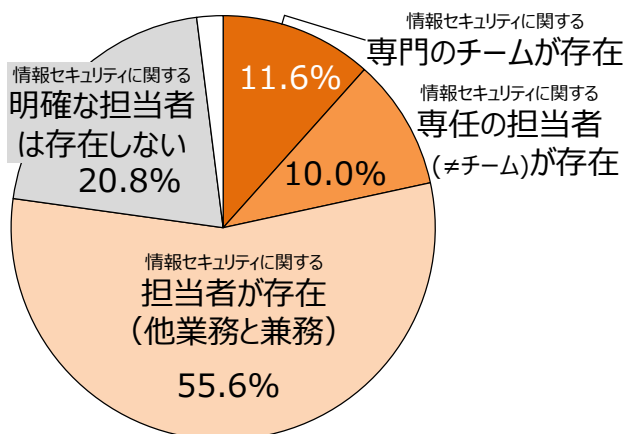


テレワークセキュリティに関する実態調査③

- テレワーク実施企業等におけるセキュリティ等の実態のほか、テレワークセキュリティガイドラインの認知度・活用方法等について調査。

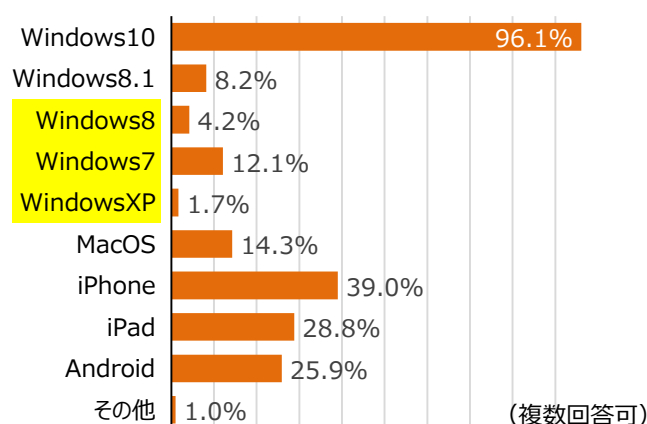
情報セキュリティ管理体制

(n=1,569：テレワーク導入企業)



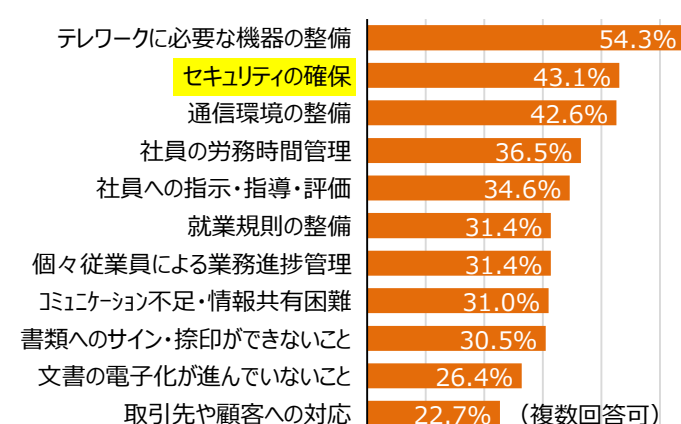
使用している会社所有の端末の種類

(n=1,569：テレワーク導入企業)



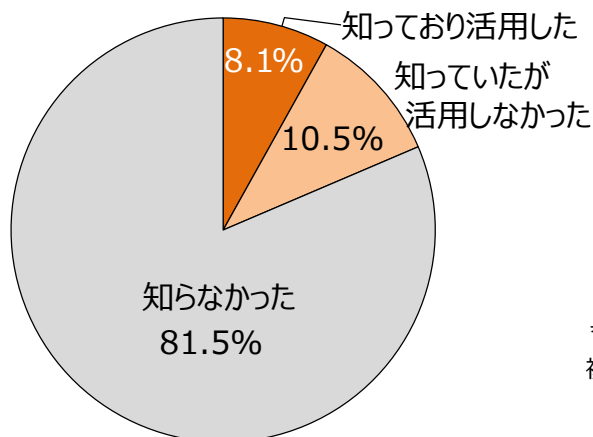
テレワークの導入に当たっての課題

(n=1,569：テレワーク導入企業)



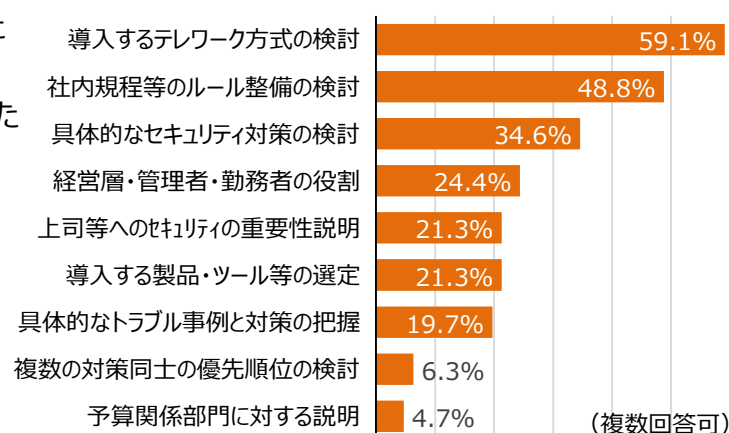
テレワークセキュリティガイドラインの認知度

(n=1,569：テレワーク導入企業)



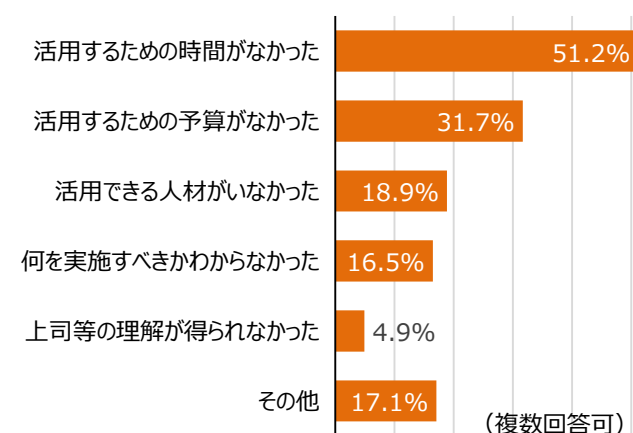
ガイドラインの活用により役立った点

(n=127：テレワーク導入企業&ガイドライン活用)



ガイドラインを活用しなかった理由

(n=164：テレワーク導入企業&ガイドライン非活用)



テレワークセキュリティに関する実態調査④

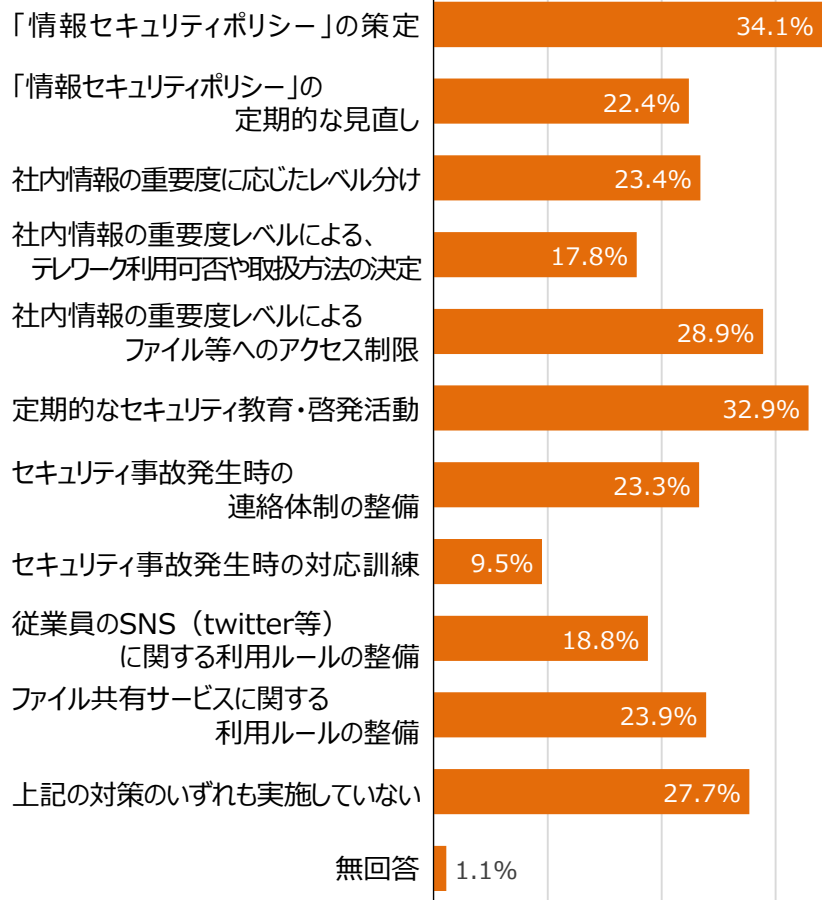
12

➤ テレワークセキュリティガイドラインに記載の主要なセキュリティ対策について、テレワーク導入企業における対策の実施状況についても調査。

情報セキュリティの管理体制等に関する対策の実施状況

(n=1,569：テレワーク導入企業) (複数回答可)

0% 10% 20% 30%



各種サイバー攻撃に関する対策の実施状況

(n=1,569：テレワーク導入企業) (複数回答可)

0% 10% 20% 30% 40% 50% 60%

