資料28－２

テレワークセキュリティガイドライン等について

サイバーセキュリティタスクフォース事務局

令和３年 ２月８日

テレワークセキュリティガイドラインの改定

- 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**を示してきた。
- 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、**2020年９月**には、**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・公表。
- テレワークを取り巻く環境やセキュリティ動向の変化を踏まえ、「**テレワークセキュリティガイドライン**」の**全面的な改定**作業を行っており、改定案について**意見公募を実施予定**。（2月中旬～3月初旬に実施予定）

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

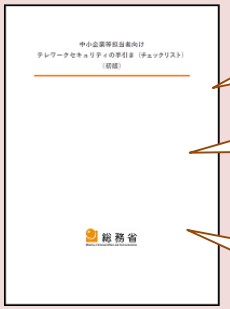
追加

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

全面改定

【テレワーク環境・セキュリティ動向の変化】

- ✓ テレワークは「一部の従業員」が利用するものから、Web会議を含め、一般的な業務・勤務形態に
- ✓ クラウドサービスの普及やスマートフォン等の活用が進むなど、システム構成や利用形態が多様化
- ✓ 標的型攻撃等の高度な攻撃が増え、従来型のセキュリティ対策では十分対応できない状況も発生

【ガイドライン改定の主要なポイント】

- ✓ テレワーク方式を再整理した上で、テレワークによって実現する業務の内容や、セキュリティ統制の容易性等から、適した方式を選定するフローチャートを掲載。
- ✓ 経営者・システム管理者・勤務者の立場それぞれにおける役割を明確化。
- ✓ 執るべきセキュリティ対策の分類や内容を全面的に見直し
- ✓ テレワークセキュリティに関連するトラブルについて、具体的事例を含め全面見直し
  （事例紹介のほか、セキュリティ上留意すべき点や、採るべき対策についても明示）

テレワークセキュリティガイドラインの改定概要

第４版（2018年４月）

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対策の考え方

✓「ルール」「人」「技術」のバランスのとれた対策の必要性を説明。
✓ テレワークの方式を6種類に整理し、その概要と対策の考え方を簡単に説明。
✓ 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。
✓「経営者」「システム管理者」「テレワーク勤務者」のそれぞれの立場について簡単な説明。

2. テレワークセキュリティ対策のポイント

✓「経営者」「システム管理者」「テレワーク勤務者」の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）
✓ 対策事項は、6個の脅威カテゴリに分類。

3. テレワークセキュリティ対策の解説

✓「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。
✓「実施するべき基本的な対策」（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。

※上記のほか、「用語集」「参考リンク集」が、第４版・第５版ともにある。

分割

- テレワーク**環境の変化**（感染症対応）等を追加
- **想定読者（チェックリストとの差異）**の項目を追加
- 経営者・管理者・勤務者の**役割を具体的に列挙**（適切な役割分担の重要性についても強調）
- テレワークやセキュリティの環境変化を踏まえ、
  - **クラウドサービス**の利用上の**考慮事項を追記**
  - サイバー攻撃の高度化を踏まえ、**ゼロトラストセキュリティ**に関する項目を追加
- **方式選定にもガイドラインは活用**されているため、
  - テレワーク方式の解説を章として独立・増強
  - **選定フローチャート**や**特性比較表**を新規作成
- テレワークの利用の広がりに合わせて、
  - **テレワーク方式を７種類に再編**（変更・細分化）
  - **派生的な構成**についても明記
- テレワーク利用の広まりや、サイバー攻撃の深刻化に対応するため、**対策事項を全面見直し**(倍増)
  例）オンライン会議システムのセキュリティ対策や、VPN機器のファームウェアアップデート等を新たに追加
- 対策事項を、13個の対策カテゴリに分類
- 各対策事項の詳細な解説についても、近年の動向を踏まえて全面的に見直し
- トラブル事例の対策に当たっては、複数対策が紐付く場合もあるため、章として独立
- 近年の実事例等を踏まえ、事例を全面更新

第５版（意見募集開始予定）

第１章 はじめに

✓ 背景、目的、テレワークの形態、想定読者等を説明。

第２章 テレワークにおいて検討すべきこと

✓「ルール」「人」「技術」のバランスのとれた対策の必要性を説明。
✓「経営者」「システム・セキュリティ管理者」「テレワーク勤務者」の適切な役割分担の重要性と、各立場の役割を具体的に説明。
✓ テレワークを取り巻く環境変化を踏まえ、クラウドサービスの有効性やセキュリティ上の留意事項に関して説明。
✓ サイバー攻撃が高度化している状況を踏まえ、セキュリティ手法として注目されるゼロトラストセキュリティに関する考え方を説明。

第３章 テレワーク方式の解説

✓ テレワーク方式を7種類に再整理し、各方式について、基本的構成に加えて派生的な構成まで詳細に解説。
✓ 各テレワーク方式に特有のセキュリティ上の留意点について説明（各方式共通の対策は第4・5章）。
✓ 実現しようとする業務内容等を踏まえ、適した方式を選定するフローチャートや、各方式の特性比較表を掲載。

第４章 テレワークセキュリティ対策一覧

✓「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」の役割ごとに、実施すべきセキュリティ対策を記載。（対策事項は「基本対策事項」と「発展対策事項」に区分。）
✓ テレワークが一般的な業務形態となってきたことに対応し、対策項目は94項目【調整中】に倍増
✓ 対策分類は、13個のカテゴリに細分化し、見通しを整理。

第５章 テレワークセキュリティ対策の解説

✓ 第4章で明示した内容について、対策分類ごとに詳細に解説。

第６章 テレワークにおけるトラブル事例と対策

✓ トラブル事例を具体的に紹介した上で、セキュリティ上留意すべき点や、本ガイドライン内のどの対策が有効であるかを説明。

意見募集に向けた最終調整中であり、記載内容は変わる場合があります。

第１章　はじめに

テレワークの形態

第５版で記載を**追記**

- ✓ 本ガイドラインの対象としては、幅広いテレワーク形態を想定
- ✓ ３つの形態に分類して具体的に例示（分類は第４版と同様）
- ✓ ワーケーション※もサテライトオフィス勤務やモバイル勤務の一形態であることを明確化

※テレワーク等を活用し、リゾート地等、普段のオフィスとは異なる場所で余暇を楽しみつつ仕事を行うもの

本ガイドラインの想定読者

第５版で**新規**に記載

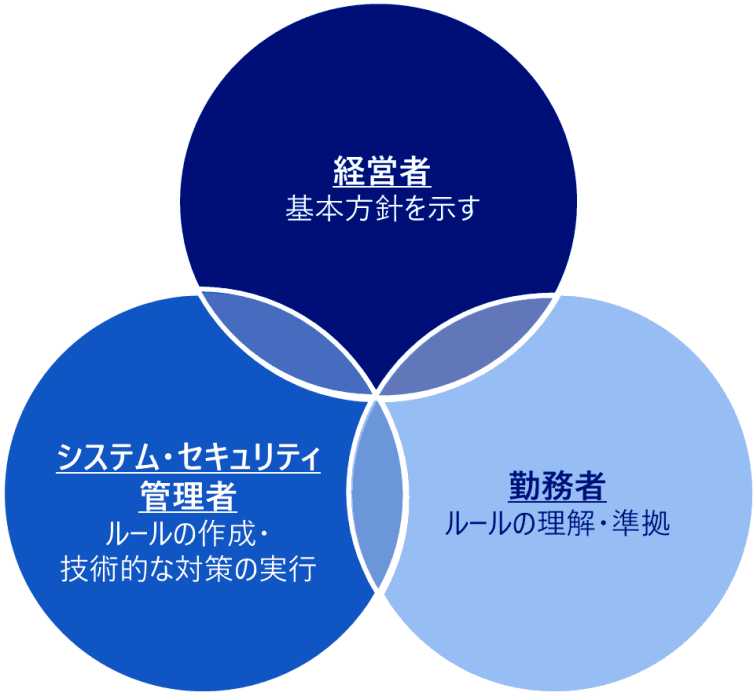
	ガイドラインの想定読者像	手引き（初版）の想定読者像
対象属性	システム・セキュリティ管理者のほか**経営層や利用者を幅広く対象**	システム管理担当者
セキュリティ予算	外部委託コストは**必要に応じて捻出**しうるレベル	外部委託コストの捻出は難しいレベル
セキュリティ推進体制	**専任**の担当・担当部門**が存在する組織も対象**	**専任は存在しない**
セキュリティリテラシ	「適切に…」「レベルに応じて…」等の読者に解釈をゆだねるような**抽象的な要求に対して、対応内容を検討・判断し、対策を実行できる**	「適切に…」「レベルに応じて…」等の読者に解釈をゆだねるような**抽象的な要求だけでは、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	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、**無理なく行うことができる**	**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**

意見募集に向けた最終調整中であり、記載内容は変わる場合があります。

第２章　テレワークにおいて検討すべきこと

経営者、システム・セキュリティ管理者、テレワーク勤務者の役割分担

第５版で記載を**明確化**



経営者については『サイバーセキュリティ経営ガイドライン（経済産業省）』、システム・セキュリティ管理者/テレワーク勤務者については『Telework Essentials Toolkit（米CISA）』等を参考に、**日本企業がテレワーク導入を進める際に、経営者・従業員の立場ごとに特に重要な役割を整理。**

経営者の重要な役割

第５版で**新規**に記載

1.テレワークにおけるセキュリティ脅威と事業影響リスクの特定・整理
2.テレワークにおけるリスクに応じたセキュリティポリシーの策定指示
3.テレワークにおけるセキュリティリスク管理体制の構築
4.テレワークセキュリティ対策のための資源確保
5.テレワークにおけるセキュリティリスクへの対応計画の策定指示
6.テレワークにおけるセキュリティリスク対応策の実施体制の構築
7.セキュリティ教育を実施するための体制の構築
8.セキュリティポリシー及びセキュリティ対策状況の定期的な見直し・修正の指示
9.セキュリティインシデント発生に備えた計画の策定及び体制の構築
10.テレワーク業務に関わるサプライチェーン全体での対策状況の把握

システム・セキュリティ管理者の重要な役割

第５版で**新規**に記載

1.テレワークにおけるセキュリティリスクの把握と対策の定期的な見直し
2.テレワーク下で従業員が用いるデバイス・ソフトウェア等の資産管理
3.ハードウェア・ソフトウェアに対する継続的な脆弱性管理
4.従業員に対する定期的なセキュリティ教育の実施
5.セキュリティインシデント発生時や、発生の可能性がある場合の対応
6.セキュリティインシデントの発生を想定した訓練等の実施
7.テレワークにおける最新のセキュリティ脅威動向の把握

テレワーク勤務者の重要な役割

第５版で**新規**に記載

1.テレワークにおけるセキュリティポリシーの遵守
2.テレワークで使用する資産（PC・スマートフォン等）の適正な管理
3.認証に用いる情報（パスワード・ICカード等）の適正な管理
4.セキュリティ研修への積極的な参加
5.セキュリティインシデント発生時及び発生の恐れがある場合の報告
6.セキュリティインシデント発生時の連絡先及び対応内容の確認

意見募集に向けた最終調整中であり、記載内容は変わる場合があります。

第３章　テレワーク方式の解説①

テレワーク方式　第５版で記載を**再編**

第４版のテレワーク方式
会社PCの持ち帰り方式
リモートデスクトップ方式
仮想デスクトップ方式
アプリケーションラッピング方式
セキュアブラウザ方式
クラウド型アプリ方式

細分化

端末にデータを保存したり、クラウドを使う場合も新たに想定

端末にデータを保存したり、クラウドを使う場合も新たに想定

名称をわかりやすいものに

クラウドを使わない場合も新たに想定

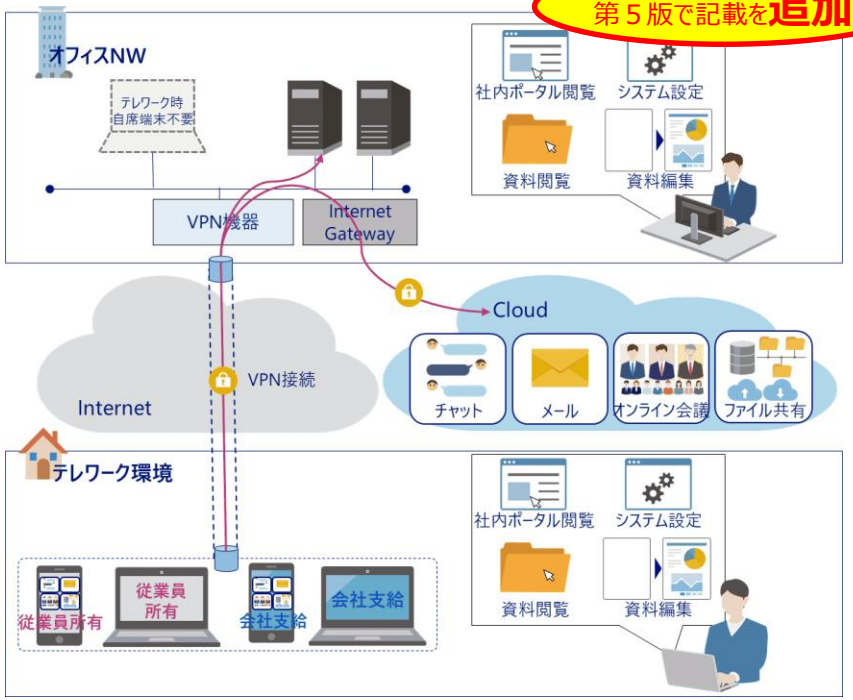
名称の平仄をあわせわかりやすいものに

方式名	概要
VPN方式	テレワーク端末から、オフィスネットワークにVPN接続を行い、社内のファイルサーバやクラウドサービス等に接続し業務を行う方法
リモートデスクトップ方式	テレワーク端末から、オフィスに設置されたPC等の端末のデスクトップ環境に接続し、テレワーク端末からデスクトップ環境を遠隔操作し業務を行う方法
仮想デスクトップ(VDI)方式	テレワーク端末から仮想デスクトップ基盤に接続し、デスクトップ画面を呼び出し業務する方法
セキュアコンテナ方式	テレワーク端末にローカル環境とは独立したセキュアコンテナという仮想的な環境を設け、当該環境内でアプリケーションを動作させ業務を行う方法
セキュアブラウザ方式	テレワーク端末からセキュアブラウザと呼ばれる特別なインターネットブラウザを利用し、社内システムや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法
会社非接続方式(クラウドサービス型)	オフィスネットワークに接続せず、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直接接続し業務を行う方法
会社非接続方式(スタンドアロン型)	オフィスネットワークには接続せず、あらかじめテレワーク端末や外部記憶媒体内へ保存していたデータの編集や閲覧することで業務を行う方法

第３章　テレワーク方式の解説②

テレワーク方式の解説例（VPN方式）

第５版で記載を**追加**



＜派生方式＞

<u>クラウド型VPNサービスを利用する形式</u>

社内ネットワークにVPNアプライアンスを設置するのではなく、クラウド型のVPNサービスを経由して、オフィスネットワークに接続します。

＜考慮事項＞

テレワーク端末内にデータの保存が可能であるため、端末の紛失による情報漏えいリスクがあります。そのため、ハードウェアの暗号化やデータの遠隔消去の対策が重要となります。また、テレワーク勤務者が増加する場合は、回線帯域のキャパシティの上限を超過しないよう考慮する必要があります。

テレワーク方式の派生方式

第５版で**新規**に記載

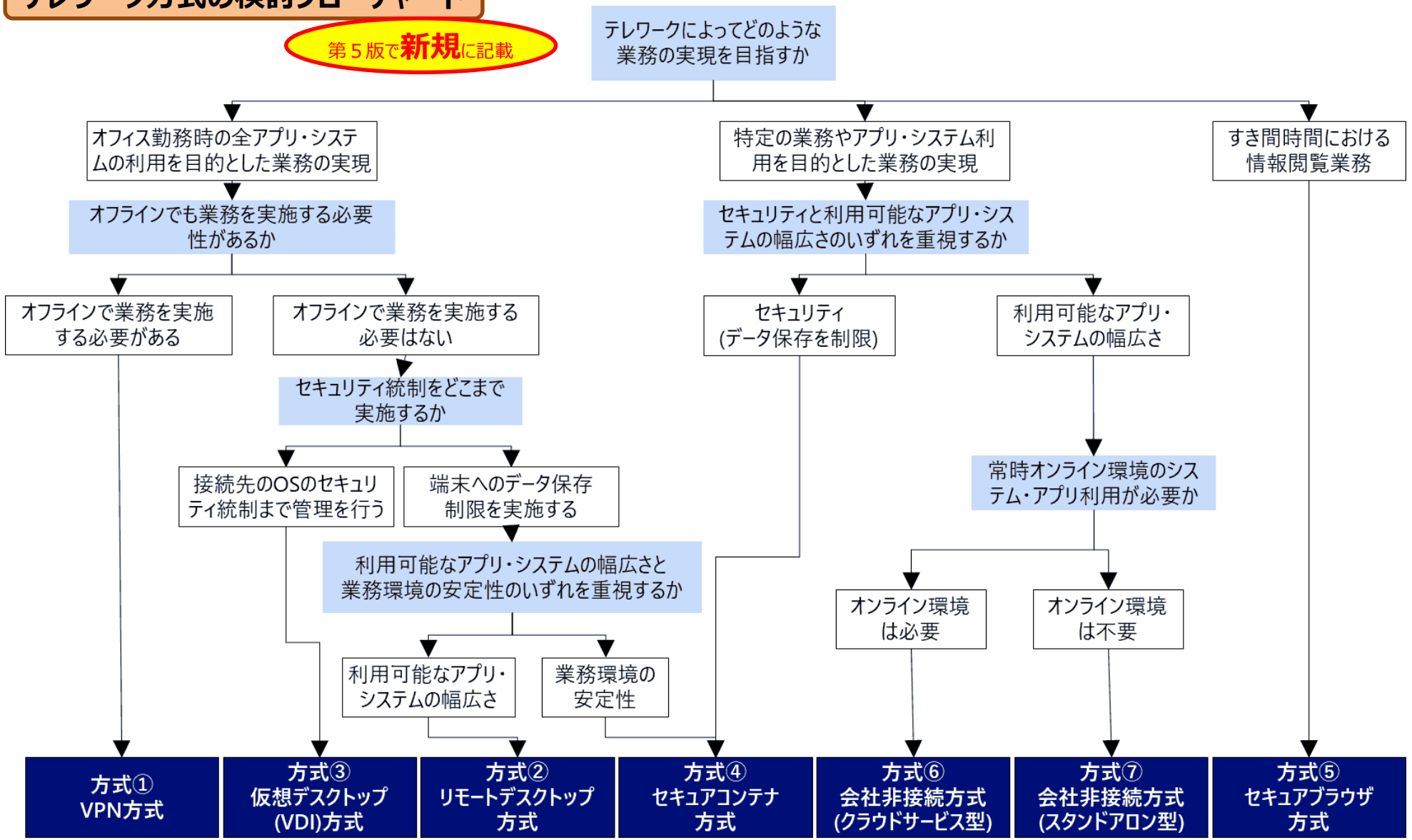
方式	派生方式
VPN方式	クラウド型VPNサービスを利用する形式
リモートデスクトップ方式	VPN接続後にWindows標準の「リモートデスクトップ接続」でオフィスPCにアクセスする形式
	クラウド基盤を介してリモートデスクトップする形式
	社内PCに専用アプリケーションをインストールし社内PCにリモートデスクトップする方式
仮想デスクトップ（VDI）方式	クラウド上に仮想デスクトップする方式
セキュアコンテナ方式	ー
セキュアブラウザ方式	クラウドサービスにアクセスする形式
会社非接続方式（クラウドサービス型）	テレワーク端末から直接クラウド上のメールサービスにアクセス
	テレワーク端末から直接クラウド上のチャットサービスにアクセス
	テレワーク端末から直接クラウド上のオンライン会議サービスにアクセス
	テレワーク端末から直接クラウド上のファイル共有サービスにアクセス
会社非接続方式（スタンドアロン型）	紙媒体のデータを持ち帰り作業する形式
	インターネットに接続し作業する形式
	外部記憶媒体でデータを持ち帰り従業員所有端末で作業する形式

意見募集に向けた最終調整中であり、記載内容は変わる場合があります。

第３章　テレワーク方式の解説③

テレワーク方式の検討フローチャート

第５版で**新規**に記載



意見募集に向けた最終調整中であり、記載内容は変わる場合があります。

第３章　テレワーク方式の解説④

テレワーク方式の特性比較

第５版で**新規**に記載

各特性は、S＞A＞B＞C＞D

No.	方式	コスト	オフィス業務再現性※2	通信キャパシティ影響度	導入負荷	セキュリティ統制の容易性※3	選定ポイント
①	VPN方式	B (システム導入が必要)	S (オフィスと同等の業務が可能)	A (通信影響を受けるがローカル作業で回避可)	B (環境変更を伴うシステム導入が必要)	C (端末のデータ管理とセキュリティ統制が要)	業務再現性に加え、通信不安定時の代替手段確保
②	リモートデスクトップ方式	B (システム導入が必要)	S (オフィスと同等の業務が可能)	C (通信環境の影響を受けやすい)	B (環境変更を伴うシステム導入が必要)	A (端末のデータ保存制限によりデータ管理が容易)	バランス型① (コスト、業務再現性、セキュリティの両立)
③	仮想デスクトップ(VDI)方式	C (高額なシステム導入が必要)	S (オフィスと同等の業務が可能)	C (通信環境の影響を受けやすい)	C (大きな環境変更を伴うシステム導入が必要)	S (端末へのデータ保存統制、セキュリティ集中管理が容易)	セキュリティ重視 (業務再現性に加え、高度セキュリティの実現)
④	セキュアコンテナ方式	B (システム導入が必要)	B (特定アプリ・システムで閲覧・作成業務)	A (通信影響を受けるがローカル作業で回避可)	B (環境変更を伴うシステム導入が必要)	A (端末のデータ保存制限によりデータ管理が容易)	バランス型② (通信安定性とセキュリティの両立)
⑤	セキュアブラウザ方式	B (システム導入が必要)	C (メール・資料閲覧に限定)	B (影響は軽微だが閲覧時に通信影響を受ける)	B (環境変更を伴うシステム導入が必要)	A (端末のデータ保存制限によりデータ管理が容易)	特定業務型① (セキュリティ重視)
⑥	会社非接続方式(クラウドサービス型)	A (必要な数量のみスモール利用可)	B (特定アプリ・システムで閲覧・作成業務)	S (社内未接続のため通信キャパシティ影響なし)	A (軽微な環境変更で利用可能)	D (端末のデータ管理に加え、クラウド分散データ管理が要)	特定業務型② (拡張性重視)
⑦	会社非接続方式(スタンドアロン型)	S (追加システム不要)	D (端末内の保存範囲内の資料閲覧・作成に限定)	S (通信をしないためキャパシティ影響なし)	S (システム変更不要)	C (端末のデータ管理とセキュリティ統制が要)	臨時利用型 (コストと導入しやすさ重視)

※１：BYOD利用の場合も想定しうるが、①VPN方式、⑥会社非接続方式(クラウドサービス型)、⑦会社非接続方式(スタンドアロン型)については、よりメリットを享受することが可能な会社支給端末を想定
※２：物理的な業務(紙媒体の利用、押印等)は考慮していない
※３：端末やクラウド上等データ保存が可能な範囲や、稼働しているシステムのパッチ適用の強制の可否を含む

意見募集に向けた最終調整中であり、記載内容は変わる場合があります。

第４章・第５章　テレワークセキュリティ対策

対策事項の分類

第５版で記載を**見直し**

※第４版では、①情報セキュリティ保全、②マルウェア、③端末の紛失・盗難、④重要情報の盗聴、⑤不正アクセス、⑥外部サービスの利用　の６種類

信頼できるクラウドサービス選定の考え方や、クラウドサービスの利用ルールに言及

セキュリティ対策の実施対象となる資産特定の重要性に言及

クリティカルな攻撃の起点になるVPN基盤等の脆弱性管理の重要性に言及

高度な攻撃で最も狙われる特権防御の重要性に言及

高度な攻撃への効果が期待されるゼロトラストの観点として、守るべきデータの特定と暗号化に言及

攻撃起点になりやすく、検知が難しいエンドポイントセキュリティ強化(EDR)の観点追加

対策分類	説明
ガバナンス・リスク管理	テレワーク実施に伴う事業リスクの特定・対応、及び、リスクに鑑みた全社統一のセキュリティのポリシー、スタンダード、プロシージャなどのルールの管理・周知を行う対策
資産・構成管理	テレワークで利用するハードウェアや、ソフトウェアについて、対象を特定するための情報(ホスト名、シリアルNo.、利用者、利用バージョンなど)や構成を管理する対策。
脆弱性管理	テレワークで利用するハードウェアや、ソフトウェアについて、最新のバージョンが適用され、既知の脆弱性が残存していないことを定期的に確認し、セキュアな状態を維持する対策。
特権管理	データリソースやサービスの正常稼働を担うシステム管理者権限を、不正アクセスによる乗っ取りから守るための対策。
データ保護	守るべきデータリソースやサービスに相当する機密情報の特定、及び、その機密レベルに基づいた重要度定義を実施する対策。また、重要度にあわせた、データの配置ルール、バックアップ、データ暗号化などの対策も含む。
マルウェア対策	エンドポイントにおけるマルウェア感染の防止・検知対策(アンチウィルスなど)や、マルウェア感染経路となりうるWebアクセス、メールなどにおけるセキュリティ対策。
通信の保護・暗号化	守るべきデータリソースやサービスにアクセスする手段である通信に関して、機密性(データ送受信過程の通信暗号化など)や可用性(リモートアクセス基盤の正常稼働など)を確保するための対策。

対策分類	説明
アカウント・認証管理	守るべきデータリソースやサービスにアクセスするアカウントの正当性の認証と、その認証手法に関わる対策
アクセス制御・認可	外部から内部、または内部から内部へのデータリソースやサービスへのアクセスについて、必要最小限のアクセスポリシーの管理と当該ポリシーに則ったアクセス制御の実施(認可)が該当。
インシデント対応・ログ管理	守るべきデータリソースやサービスへの不正な侵害・インシデントが生じた場合を想定し、原因・影響を特定するためのログ取得や管理などの対策
物理的セキュリティ	データリソースやサービスへのアクセス環境に関して、物理的な手段による不正なアクセスが生じうる場合(入室/盗み見/盗み聞き/持出しなど)に、必要最小限のアクセスポリシーを実現するための物理的な制約を実施する対策。
脅威インテリジェンス	守るべきデータリソースやサービスに対する不正な侵害につながりうる、脅威動向、攻撃手法、脆弱性などに関する情報の収集を行う対策。
教育	守るべきデータリソースやサービスを活用する従業員や、セキュリティ対策を実施する管理者などの組織の人材について、セキュリティリテラシ高めるための教育活動、注意喚起、研修参加などの活動を行う対策。

攻撃起点となる認証突破対策として、多要素認証を強調

ゼロトラスト観点より、最小特権によるアク[illegible]

完全防御が難しいという前提のもと、攻撃発生後の事後対応系対策に言及

オンライン会議普及に伴い、在宅環境の物理セキュリティ対策(意図せぬ画面映り込み・音漏れ対策など)の強化

セキュリティ意識のあまり高くない従業員への注意喚起・教育等の重要性に言及

高度な攻撃への効果が期待されるゼロトラストの観点としてEnd-to-Endでのデータ通信の暗号化（通信の保護・暗号化）に言及

吹き出しは対策項目の見直しに当たって考慮した観点

意見募集に向けた最終調整中であり、記載内容は変わる場合があります。

第６章　テレワークにおけるトラブル事例と対策

トラブル事例

第５版で記載を**見直し**

1.VPN機器の脆弱性
2.個人情報保護の強化
3.アクセス権限の設定不備に関するトラブル事例
4.マルウェア感染に関するトラブル事例
5.ランサムウェアに関するトラブル事例
6.不審メールに関するトラブル事例
（フィッシングメール）
7.不審メールに関するトラブル事例
（ビジネスメール詐欺）
8.端末の紛失に関するトラブル事例
9.公衆無線LAN利用に関するトラブル事例
10.画面を介した情報流出に関するトラブル事例
11.踏み台に関するトラブル事例
12.パスワード管理に関するトラブル事例
13.パブリッククラウド利用に関するトラブル事例
（クラウドサービスにおける情報漏えい）
14.パブリッククラウド利用に関するトラブル事例
（クラウドサービスにおける大規模障害）
15.サプライチェーンに関するトラブル事例

具体的事例と対策例（VPN機器の脆弱性）

＜具体的事例＞

2020年8月に、VPN機器のIDやパスワードが世界中から流出する事件が発生しました。脆弱性を修復せずに運用を続けていたVPN機器が攻撃を受け、日本でも40社近くの企業に対して、不正アクセスが行われました。

2019年には、当該脆弱性を悪用する攻撃がすでに発生しており、ベンダー側で修正が行われ対策が可能になっていましたが、脆弱性の修正が未実施の機器が攻撃を受けたというものでした。

各トラブル事例について、具体的なインシデント等の発生動向を記載。

＜テレワークセキュリティへの示唆＞

（略）脆弱性を悪用した攻撃は日々発見され、攻撃者は攻撃の機会を伺っています。そのため、脆弱性対応を放置するのではなく、即時対応を行うことが重要です。

また、テレワークの急激な拡大に伴い、設備を増強するべく、以前利用をしていたVPN機器を再度稼働させたところ、脆弱性が潜んでいたために攻撃を受けた企業もありました。このように、急遽テレワークの導入等に伴い、過去に使用していた機器を再利用する場合には、脆弱性が残っていないかを確認した上で利用することが重要となります。

当該トラブル事例を防ぐために、どのような点に留意すべきかを記載。

＜有効な対策＞

・社内にリモートアクセスする際のVPN機器やリモートデスクトップアプリケーション等について、最新のアップデート及びパッチ適用を定期的に行う。
・テレワークで利用するデバイスやソフトウェアについて、メーカーサポートが終了しているものを利用しないように周知する。

当該トラブル事例を防ぐために、第４・５章に記載された対策事項のうち該当するものを記載

意見募集に向けた最終調整中であり、記載内容は変わる場合があります。

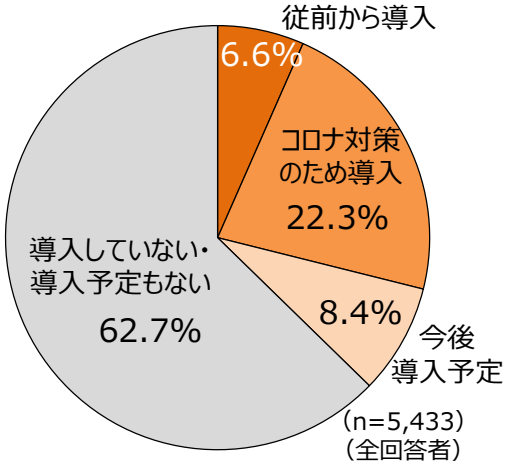
テレワークセキュリティに関する実態調査①

- 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。

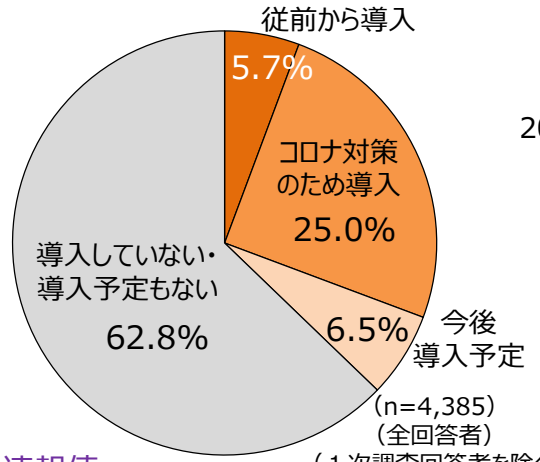
１次調査）　期間：2020.7.29-2020.8.24　　回答数：5,433（うちテレワーク実施企業1,569）
２次調査）　期間：2020.12.16-2021.1.18　　回答数：5,037（うちテレワーク実施企業1,996）
（１・２次共通）地域：全国　手法：調査票郵送・Web回答　対象数：30,000（従業員10名以上／２次調査は１次調査のテレワーク実施企業を含む）

テレワークの導入状況

１次調査（昨夏）

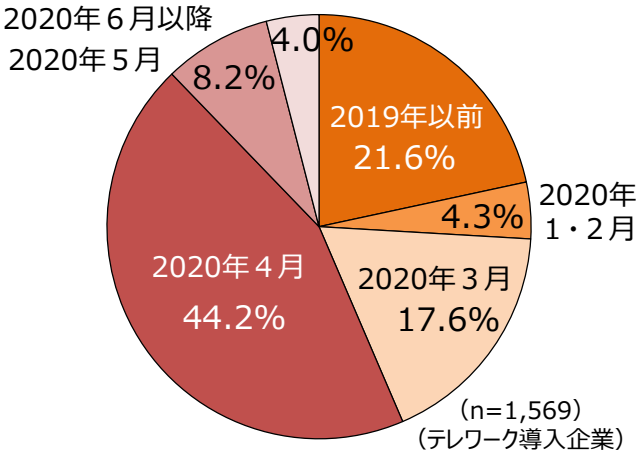


２次調査（今冬）

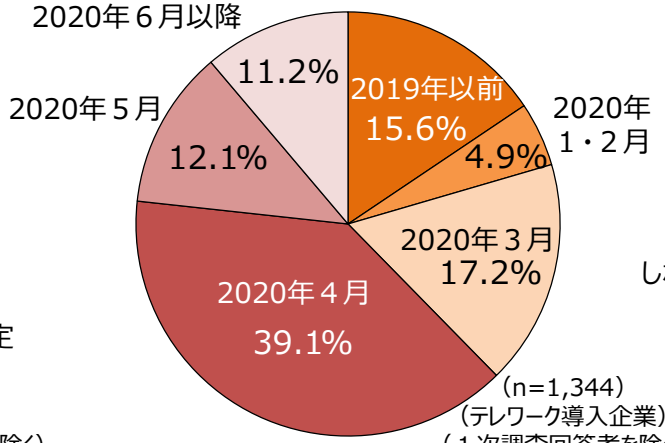


テレワークの導入時期

１次調査（昨夏）

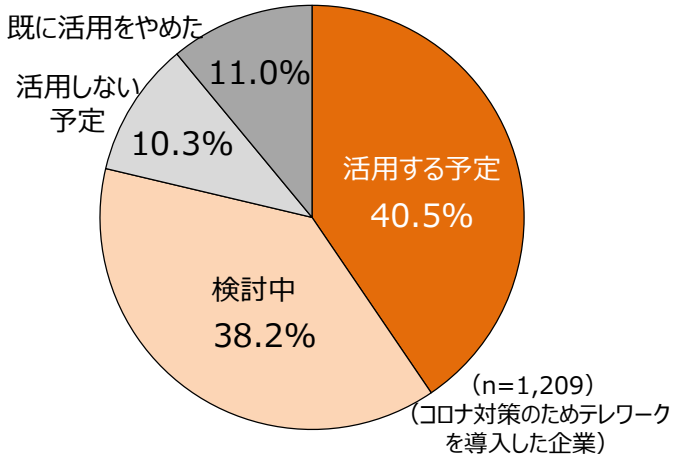


２次調査（今冬）

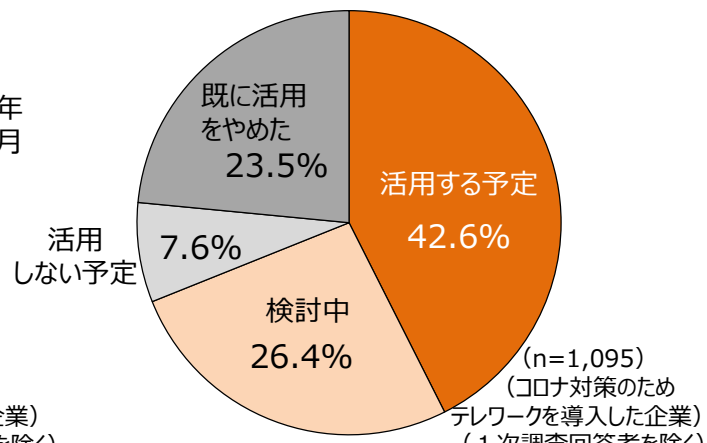


新型コロナ収束後のテレワーク活用予定

１次調査（昨夏）



２次調査（今冬）

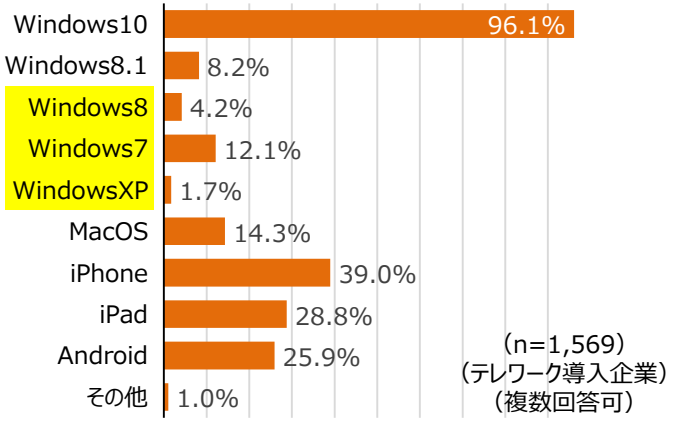


２次調査結果は速報値

テレワークセキュリティに関する実態調査②

1次調査（昨夏）

使用している会社所有の端末の種類



設問　貴社・貴団体において使用している会社所有のPC端末及び会社所有のモバイル端末（スマートフォン/タブレット）の種類をすべてお答えください。

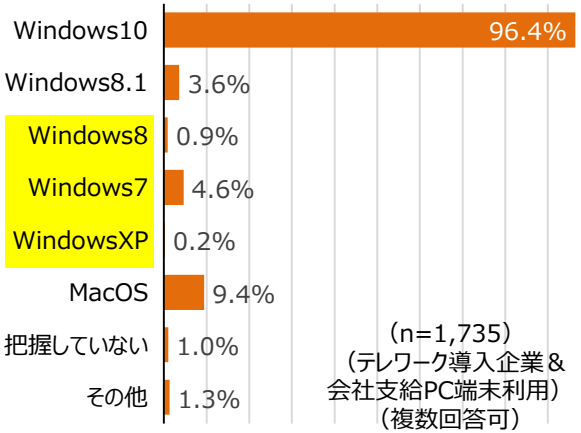
テレワーク使用端末以外（クローズ環境等）と勘違いして、誤って回答しているのではないか？

設問　テレワークで利用する会社支給のPC端末について、利用しているOSの種類を全て教えてください。

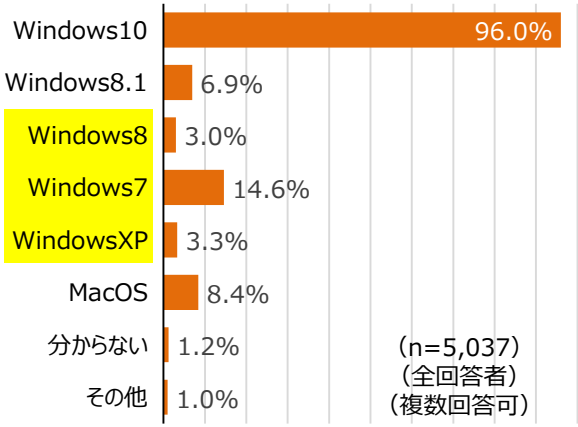
設問　職場利用・テレワーク利用に関わらず、会社所有のPC端末のOSの種類を全て教えてください。

2次調査（今冬）

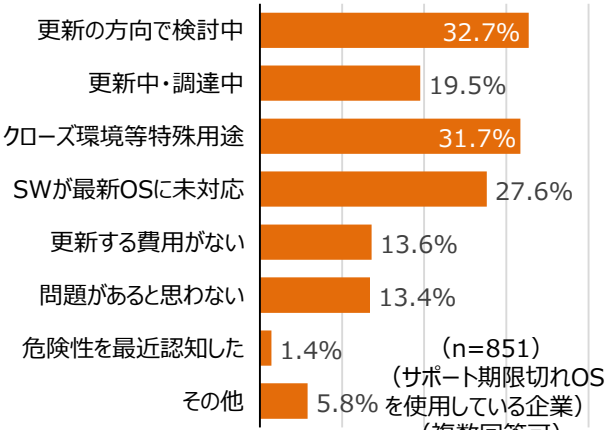
テレワークで使用する会社支給のPC端末の種類



職場・テレワークに関わらず会社所有のPC端末の種類



サポート期限が切れたOSを使用している理由



※自由回答により、ESUを使用している企業も見受けられた

2次調査結果は速報値