テレワークにおけるセキュリティ確保について

総務省　サイバーセキュリティ統括官室
主査
服部　裕史

1. 最新のサイバーセキュリティ動向

2. テレワークにおけるセキュリティ確保

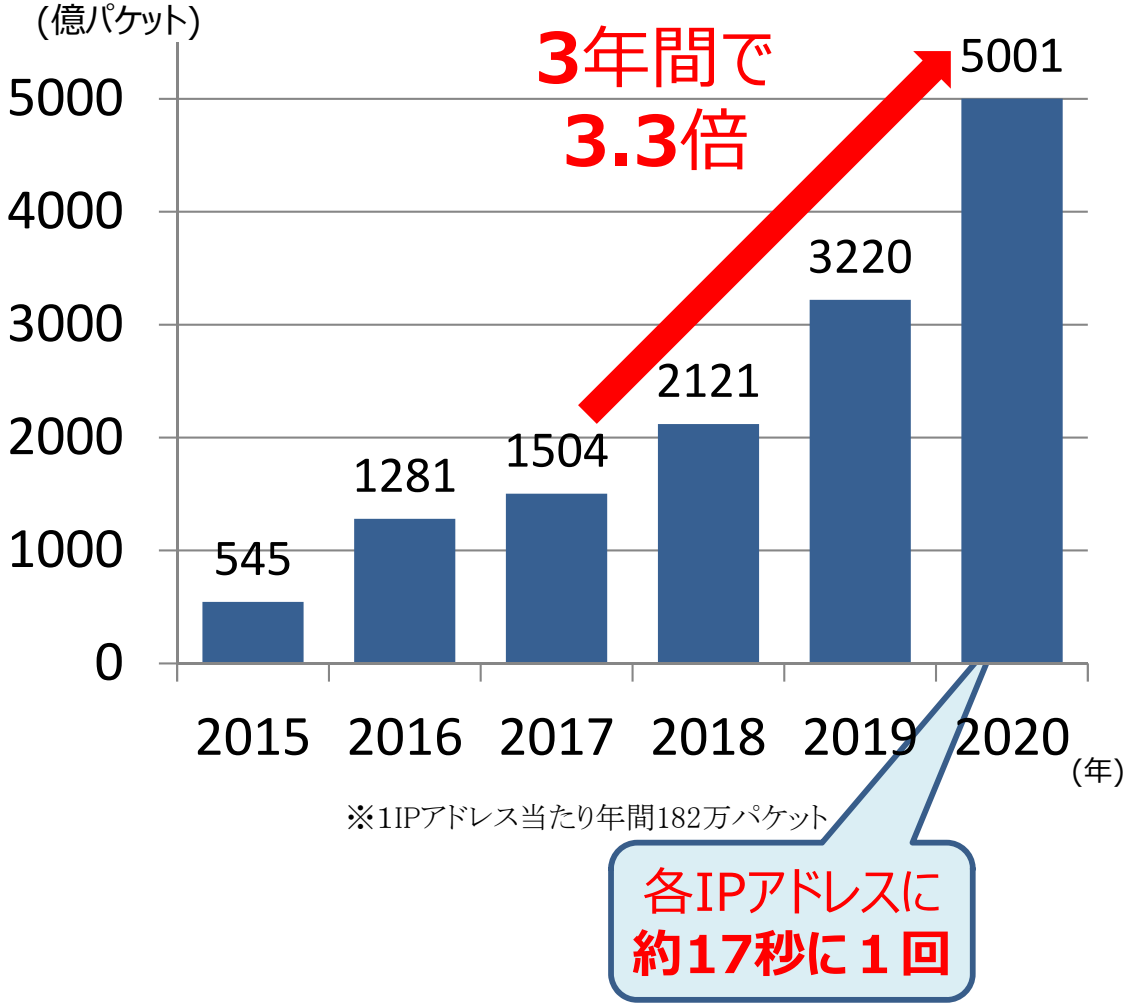
3.（参考）無線LANにおけるセキュリティ確保

１．最新のサイバーセキュリティ動向

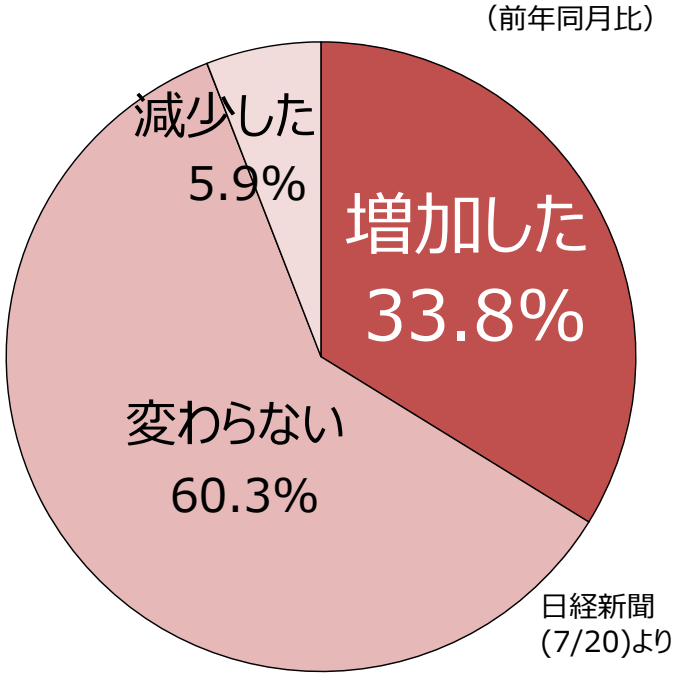
サイバー攻撃の脅威の増加

- 新型コロナへの対応として、テレワークの普及拡大や社会全体のデジタル・トランスフォーメーション（DX）が進みつつある中、サイバー攻撃も増加。

国立研究開発法人情報通信研究機構(**NICT**)において、大規模サイバー攻撃観測網「**NICTER**」を活用し、**サイバー攻撃の状況を常時観測**



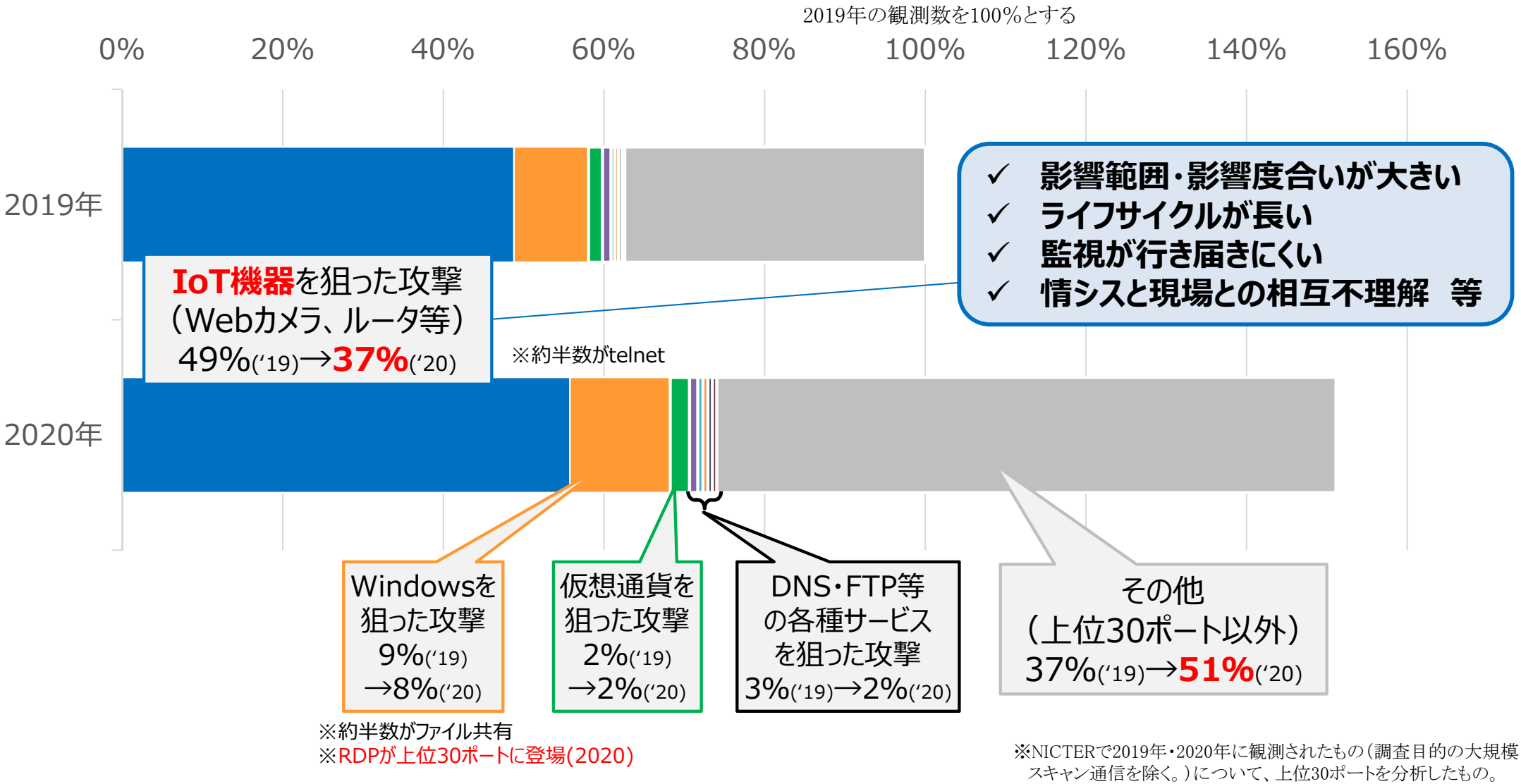
2020年４月以降に受けたサイバー攻撃



社内システム・設備の停止や提供しているサービスの停止といった企業活動そのものに影響する攻撃が増加

大規模サイバー攻撃観測網「NICTER」による観測結果

- NICTERにより観測された通信の内容（上位30ポートの分析）
  - ✓ **IoT機器を狙った攻撃が依然としてトップ**
  - ✓ **攻撃(対象ポート)が年々多様化**

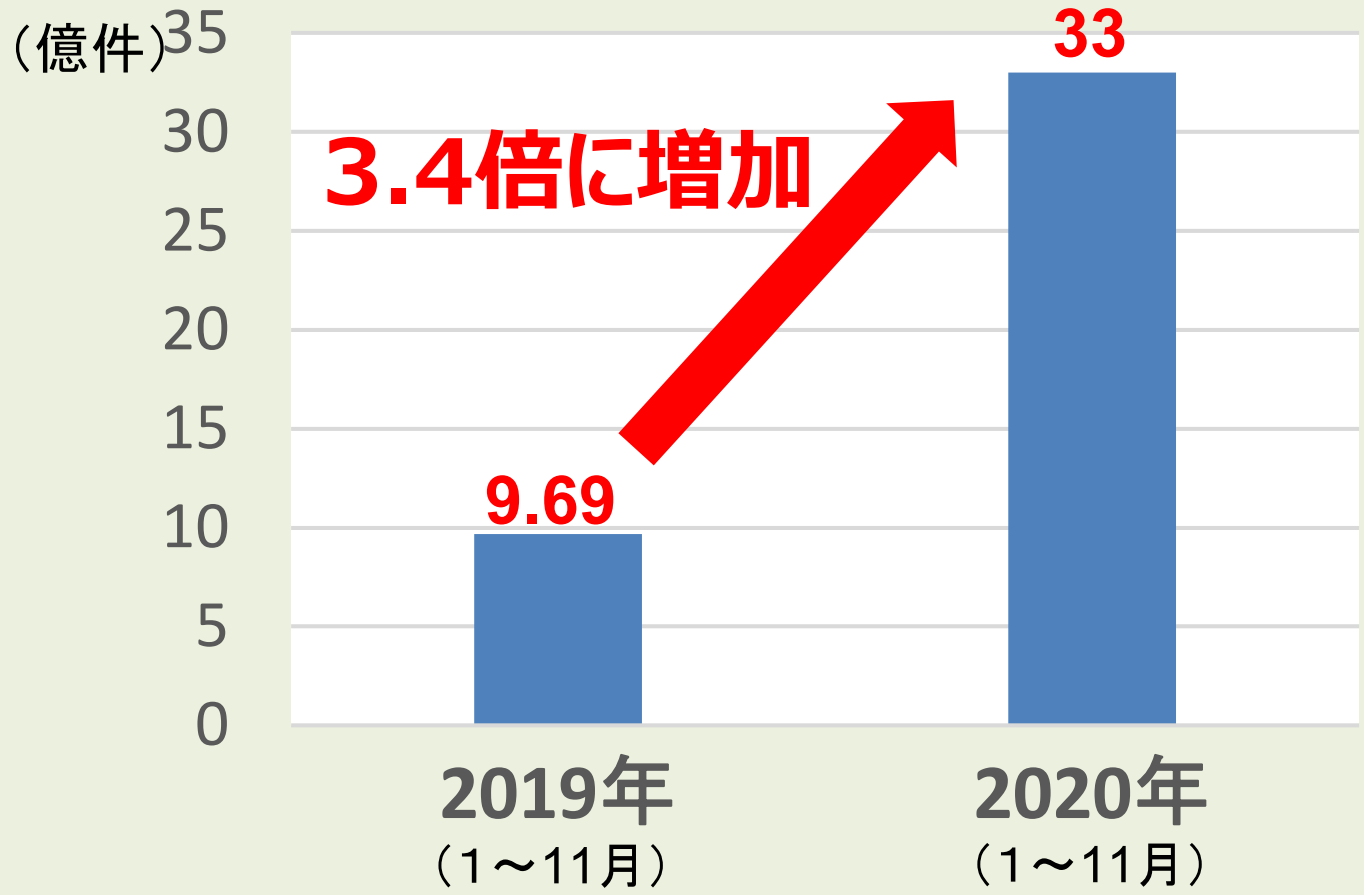


※NICTERで2019年・2020年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位30ポートを分析したもの。

特にテレワーク・・・

テレワーク環境を狙った攻撃*の増加

* リモートデスクトップ（RDP）を狙ったブルートフォース攻撃数
（kaspersky社による検出数（世界））



出典：Kaspersky The story of the year: remote work(10 Dec. 2020)より作成

中小企業に対するサイバー攻撃

- 中小企業であっても実際にサイバー攻撃の標的となっている。
- 大企業のセキュリティ対策が進展するにつれ、取引関係にある中小企業を踏み台にするパターンも。
- 自社には狙われる情報がない、という考え方はもはや通用しない。（他社に迷惑→損害賠償責任も）

【中小企業におけるサイバー攻撃対策に関するアンケート調査】（大阪商工会議所）
（期間：2017年３～６月／回答数：315社／関西の中小企業等）https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf

✓中小企業であっても、**標的型攻撃メールの受信（18%）**や**ランサムウエアによる被害（７%）**にあっている

○具体的な被害例
- ランサムウエアによる感染で、１部署のデータ全て暗号化された
- なりすましメールの添付資料を開いたことで、情報が漏洩した
- 自社ホームページがアクセス不能になり、修復に１カ月ほどかかった
- メールアカウントが乗っ取られた
- ホームページのセキュリティーホールを突かれ、悪意のあるリンクを埋め込まれた

【サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査】（大阪商工会議所）
（期間：2019年２～３月／回答数：118社／全国の従業員100人以上の企業）https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190510sc.pdf

✓「**取引先がサイバー攻撃被害を受け、それが自社に及んだ経験**」がある企業は**４社に１社（25%）**。
その結果、「情報漏洩」（５社）、システムダウン（３社）、データ損壊（３社）など実害も出ている。

✓「**取引先がもしサイバー攻撃を受け、その被害が自社にも及んだ場合**、採り得る対処」としては、「口頭や文書での注意喚起」（51%）、「**損害賠償請求**」（**47%**）、「セキュリティソフト・ハード導入の依頼／要件化」（37%）、「**取引停止**」（**29%**）など。

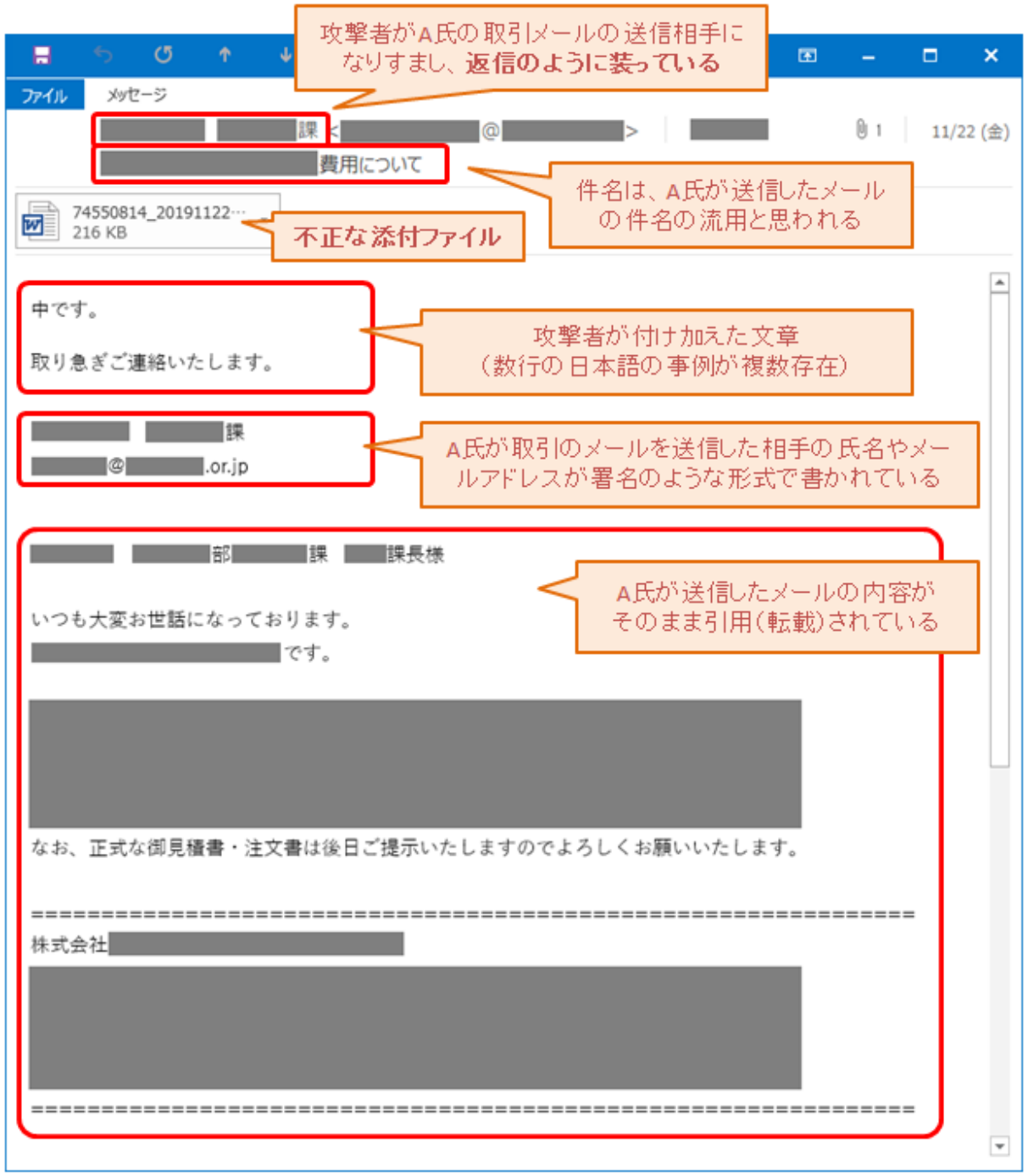
✓「中小企業は今後どうしていくべきか」については、「中小企業自身が自衛すべき」（60%）、「国や自治体が支援すべき」（45%）、「IT企業や損保会社が安価・簡便なセキュリティサービスを提供すべき」（30%）など。

Emotet（エモテット）

Emotet（エモテット）

- ✓ 世界的な被害を出すマルウェアの一種
  （マルウェア＝不正な動きをするソフトウェア）
- ✓ 国内でも2019年から大流行
  （2014年に最初に確認され機能追加）

1. メールの**添付ファイル**か**URLダウンロード**で感染
2. 感染すると攻撃者からの指示を受け様々な悪さをすることが可能
   （ファイルを暗号化したり、情報を漏えいさせたり等）
3. 過去メール、アドレス帳、ログイン情報等を攻撃者が収集
4. なりすましメールが**非常に巧妙**
   ・実在の人からのメール
   ・本人のアカウントから送信されること
   ・実際のやりとりメールも利用

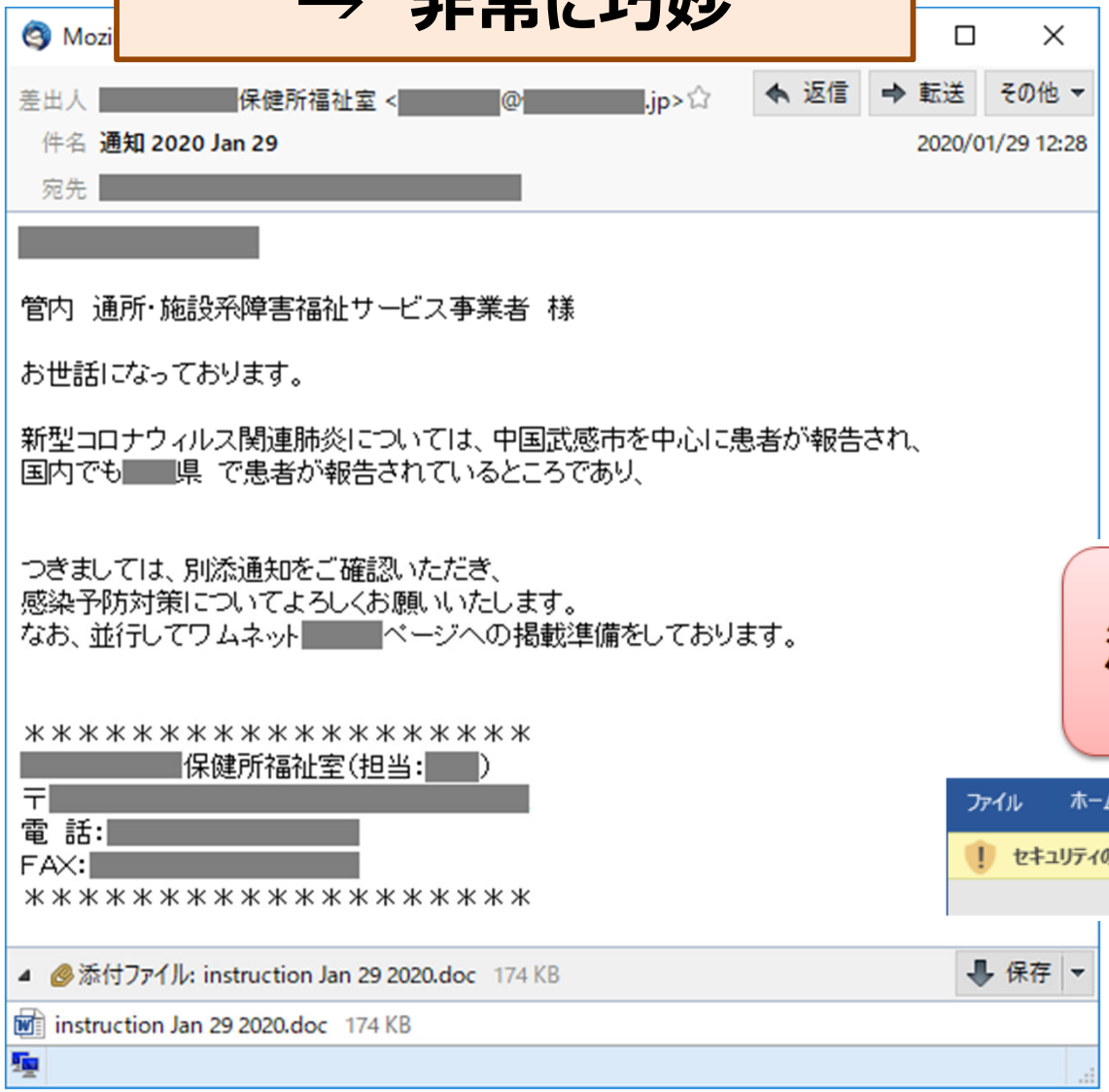


「「Emotet」と呼ばれるウイルスへの感染を狙うメールについて」より引用
https://www.ipa.go.jp/security/announce/20191202.html

Emotet（エモテット）

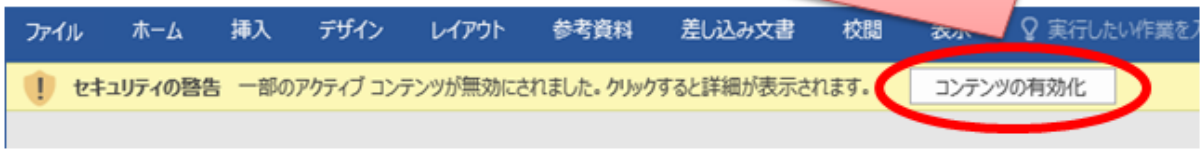
- ✓ コロナの流行当初時にコロナの話題
- ✓ 保健所から、管轄事業者宛を装う

→ **非常に巧妙**



- ✓ Emotetが仕込まれた添付ファイルや ダウンロードさせられたファイルは、 「マクロ」というプログラムが埋め込まれている
- ✓ **マクロを実行せず、送信元に確認を！**

注意！ このパソコン上で、文書ファイルに埋め込まれている マクロ(プログラム)等の実行を許可するという意味の ボタン。このボタンをクリックすると、悪意のあるマクロ が動作し、ウイルスに感染させられてしまう。



「「Emotet」と呼ばれるウイルスへの感染を狙うメールについて」より引用
https://www.ipa.go.jp/security/announce/20191202.html

２．テレワークにおけるセキュリティ確保

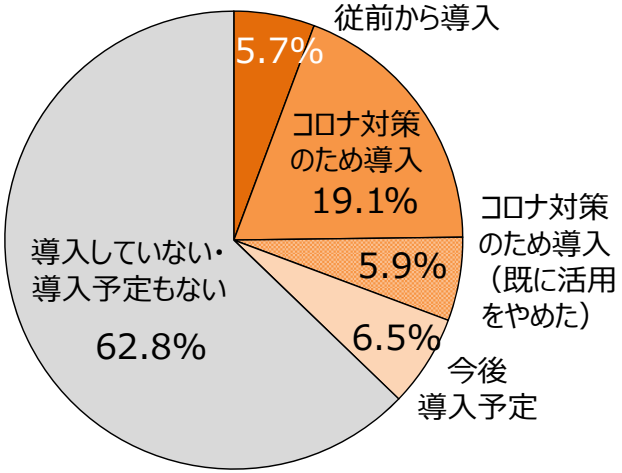
テレワークセキュリティに関する実態調査結果

➢ 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。
手法：調査票郵送・Web回答　地域：全国　対象数：各30,000(従業員10名以上)

調査結果の詳細は「総務省　テレワーク　セキュリティ」で検索

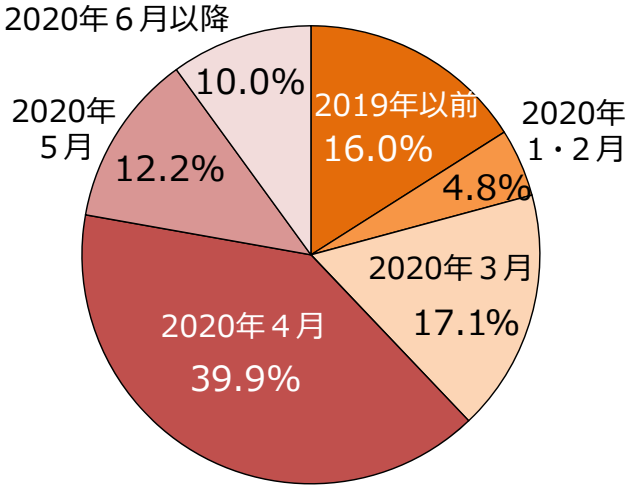
テレワークの導入状況

(n=4,385：全回答者(１次調査対象者を除く))



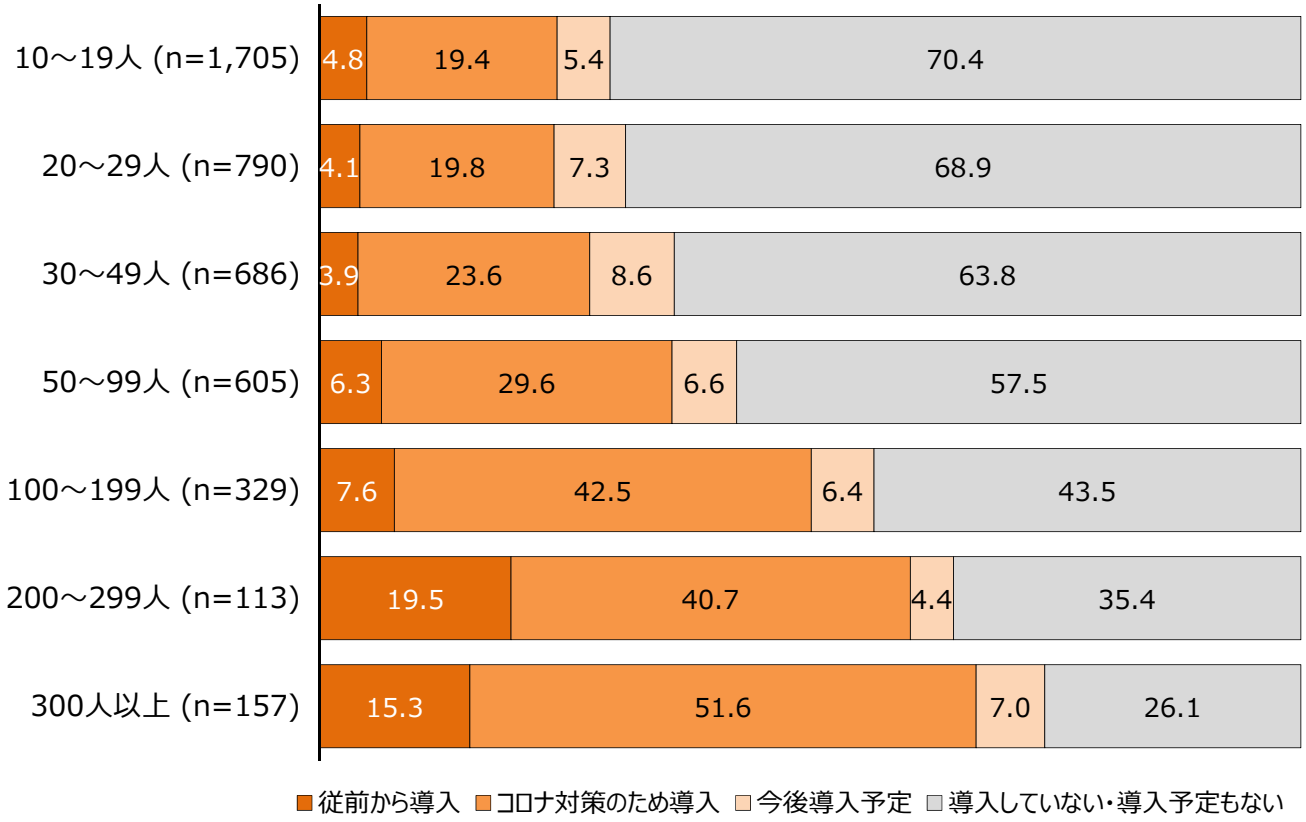
テレワークの導入時期

(n=1,996：テレワーク実施企業)



テレワークの導入状況（従業員規模別）

(n=4,385：全回答者(１次調査対象者を除く))

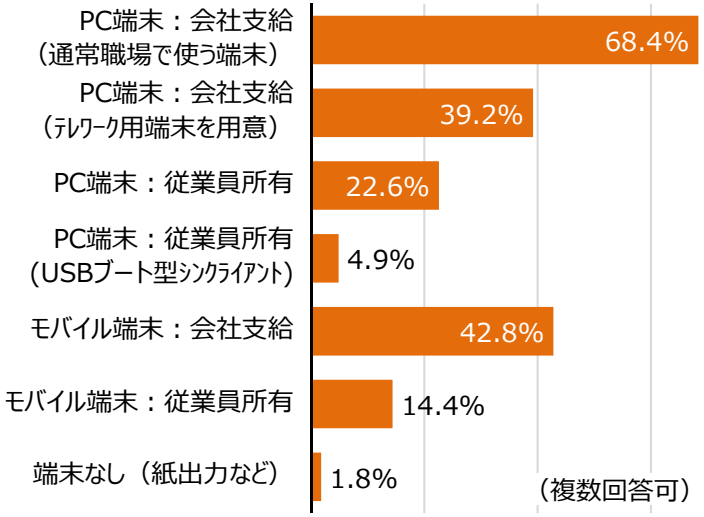


テレワークセキュリティに関する実態調査結果（利用状況・課題）

- テレワークでは会社支給端末や、クラウドサービスが広く利用されている。
- テレワークの導入に当たって、「セキュリティの確保」が最大の課題となっている。

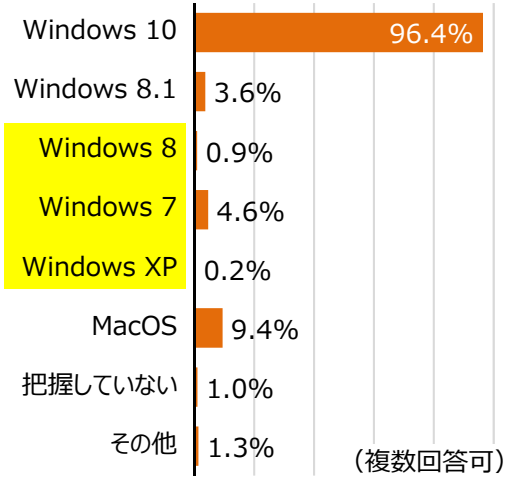
テレワーク利用を許可している端末

（n=1,996：テレワーク実施企業）



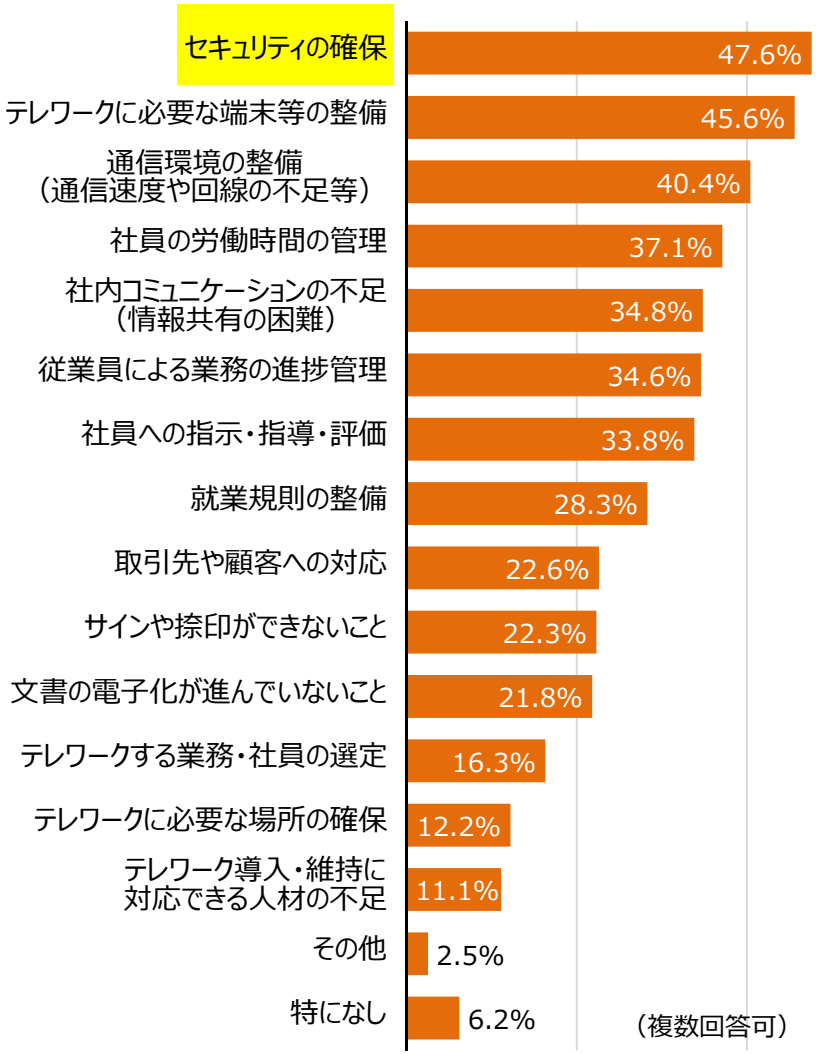
会社支給PC端末のOS

（n=1,735：会社支給PC端末を利用）



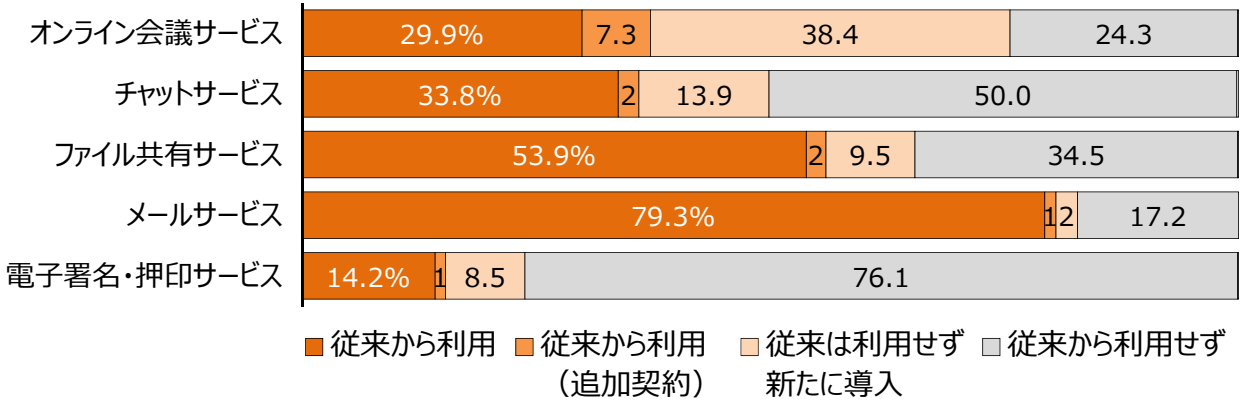
テレワークの導入に当たり課題となった点

（n=1,996：テレワーク実施企業）



クラウドサービスの利用状況

（n=1,996：テレワーク実施企業）



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。
  → テレワークを取り巻く環境やセキュリティ動向の変化に対応するため**2021年５月**に**全面的に改定**
- 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、ガイドラインを補完するものとして、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いても、テレワークを実施する際に**最低限のセキュリティ**を**確実に確保**してもらうための**チェックリスト・設定解説**も策定・公表。

テレワークセキュリティガイドライン

（2021年５月　第５版）

2004年12月初版
2006年４月第２版
2013年３月第３版
2018年４月第４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

ガイドラインに記載の内容について、理解や検討が難しい場合・・・

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)

（2021年５月　第２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

対象とするセキュリティ対策のイメージ		難易度		
		低	中	高
重要度	高	基本	基本	発展
	中	基本	基本	発展
	低	基本	基本	発展

対象とするセキュリティ対策のイメージ		難易度		
		低	中	高
重要度	高	◎	○	－
	中	○	○	－
	低	－	－	－

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**しいものは「◎」、**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**※
  - ※ 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	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	• 用語集 • テレワークセキュリティに関する参考情報
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	• 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	(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

テレワークセキュリティガイドラインの改定

テレワークセキュリティガイドライン
（2021年５月　第５版）

2004年12月初版
2006年４月第２版
2013年３月第３版
2018年４月第４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)
（2021年５月　第２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。
- ✓実施す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構成

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。
（セキュリティ対策は「基本対策」と「発展対策」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98項目に
✓**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

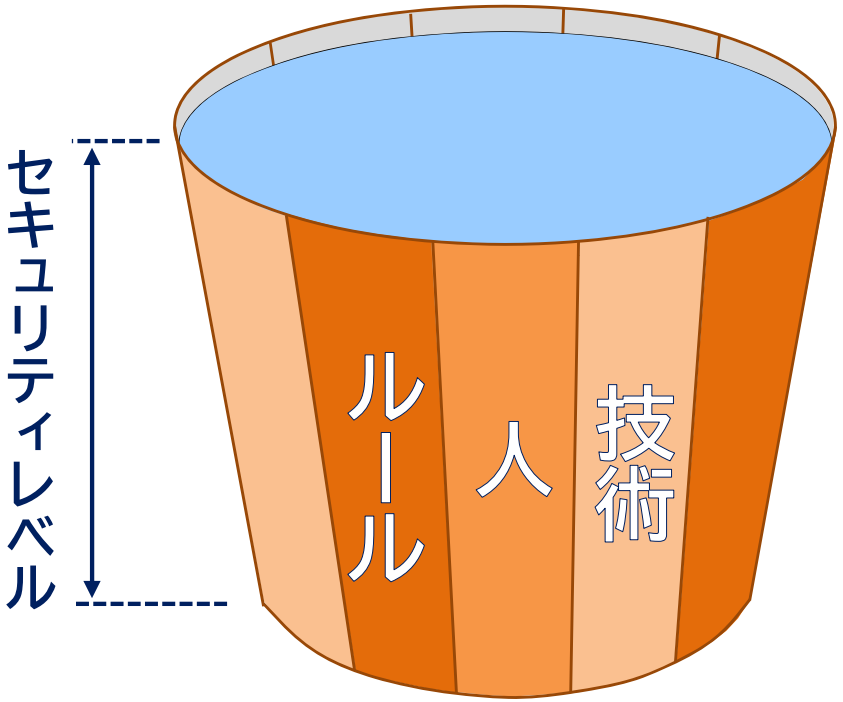
✓第４章で明示した内容について、対策分類ごとに詳細に解説。

第６章 テレワークにおけるトラブル事例と対策

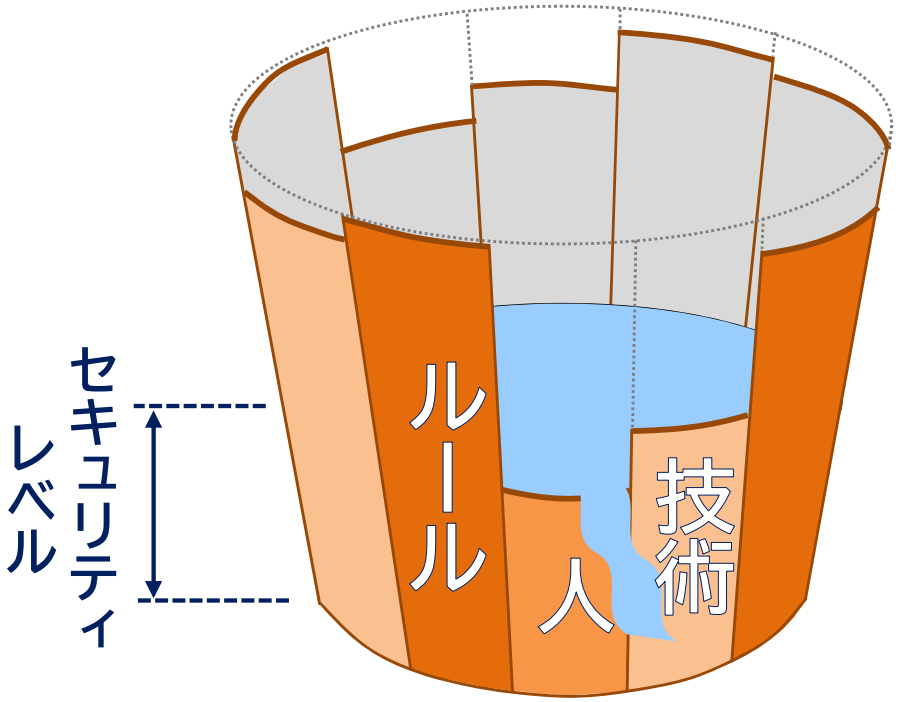
✓**トラブル事例**を具体的に紹介した上で、セキュリティ上留意すべき点や、本ガイドライン内のどの対策が有効であるかを説明。

ルール、人、技術のバランスのとれたセキュリティ対策

バランスがとれた対策

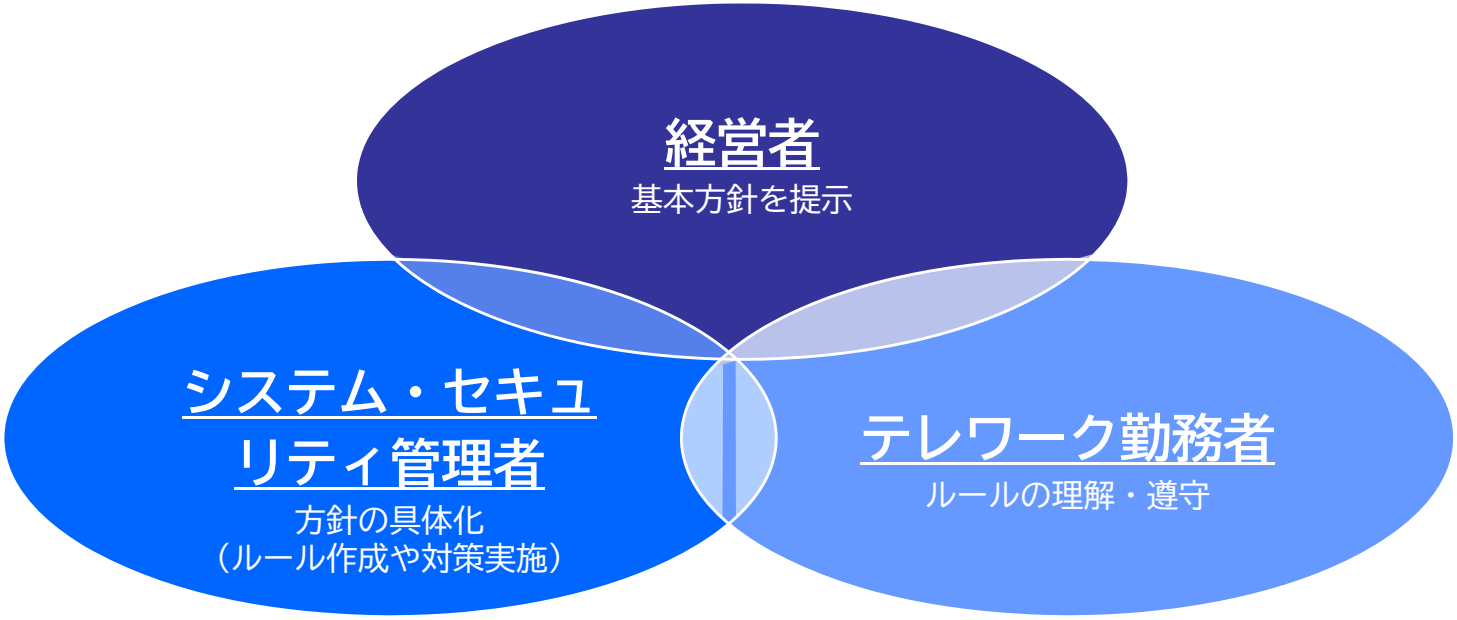


バランスが悪い対策



ルール	人	技術
✓ テレワークでは、オフィスと異なる環境で業務を実施する →セキュリティ確保のためには、通常、新たなルールを定める必要	✓ ルールは守られてこそ効果有 ✓ テレワークでは目が届きにくい ✓ 教育・研修で趣旨を理解し、遵守＝自己メリットを自覚 ✓ 手口を共有することも重要	✓ 「ルール」や「人」では対応できない部分を補完するもの ✓ 利便性とセキュリティのバランスをとったものとする必要

組織の立場に応じた役割



経営者	システム・セキュリティ管理者	テレワーク勤務者
✓ 事業に影響を及ぼすセキュリティリスクの検討や、その対応方針を示す（セキュリティに関する事故が生じた場合、経営に直結した被害が生じうる） ✓ セキュリティ責任者の決定 ✓ 予算・人員の確保 ✓ 委託先や関連会社を含めた取組	✓ 経営者が示した本針や指示を具体化する ✓ 情報セキュリティに関するルールを作成し、当該ルールを従業員に遵守させる ✓ ルールに沿った対策の企画や実施	✓ 「ルール」を認識・理解し、これを遵守する

クラウドサービス

クラウドサービスの有効性

1．セキュリティ管理対象の軽減

- ✓ オンプレミス環境でシステムの導入・運用を行う場合は、物理的セキュリティ、OS等のソフトウェアの脆弱性管理といった多くの点について担当者が適切に管理し、統制する必要
- ✓ 一方、クラウドサービス（SaaS）では、情報・データ、アカウント情報、アクセス権等の管理を適切に行うことができれば、アプリケーションレベル以下の領域の管理負荷を軽減することが可能

2．システム導入の迅速性

- ✓ ハードウェア調達や構築にかかる時間を縮減

3．システム拡張・縮退の容量柔軟性

- ✓ 利用人数が不明確な場合でも柔軟に拡張可能
- ✓ 不要になった場合に対応しやすい
- ✓ 無償や安価なプランの場合は、セキュリティ機能が制限される場合等もあるため注意が必要

4．運用コストの低減

- ✓ クラウド事業者の大量調達によるスケールメリット
- ✓ 運用監視人員も削減可能な場合

クラウドサービス活用時の留意事項

1．サービスや事業者の信頼性確認

- ✓ 機密性の確保や、安定したシステム稼働のための信頼性確認

2．セキュリティ責任境界の確認

- ✓ サービスによって利用者との責任の境界（責任分界）は様々
- ✓ 自組織が担うべき責任範囲を確実に確認することが重要

3．情報の重要度定義とクラウド保管情報の管理

- ✓ クラウドサービスは、インターネットを介してアクセスすることが前提となっているため、インターネットを介した攻撃を受けるリスクがある
- ✓ リスクをゼロにすることはできないため、業務で取り扱う情報の機密レベルを定義し、クラウドサービス上で取り扱うことができるレベルを定め、クラウド上の情報を適切に管理することが重要

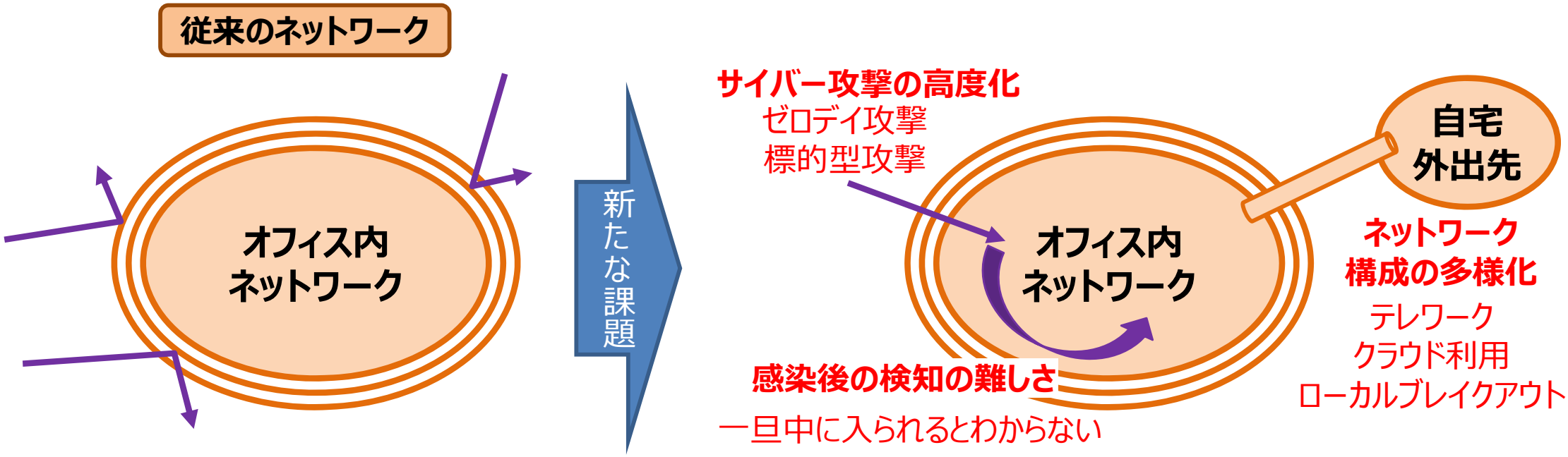
4．適切なアクセス制御の実施

- ✓ アクセス制御設定に不備があり、誤ってインターネットに機密情報を公開してしまうケースが発生している
- ✓ 適切な利用者のみがアクセスできるようしたり、IPアドレス制限等により、アクセス制御を強化することが推奨される

5．厳格な認証情報の管理と認証手法の強化

- ✓ 正規の利用者のアカウント情報（認証情報等）を窃取して、クラウドサービスへ不正アクセスを試みる攻撃者が近年増加
- ✓ パスワードを厳格に管理（第三者に推測されにくいものを設定する、使い回しをしない等）するとともに、多要素認証等の強力な認証手法の活用を検討することが重要

ゼロトラストセキュリティ



境界型セキュリティ	ゼロトラストセキュリティ
✓ 境界線で内側と外側を遮断 ✓ 外部からの攻撃や内部からの情報流出を防止 ✓ 「信頼できないもの」が内部に入り込まない、また内部には「信頼できるもの」のみが存在することが前提 ✓ 防御対象の中心はネットワーク	✓ 「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という「性悪説」に基づいた考え方 ✓ 利用者を疑い、端末等の機器を疑い、許されたアクセス権でも、なりすまし等の可能性が高い場合は動的にアクセス権を停止 ✓ 防御対象の中心はデータ、機器等の資源

ガイドラインにおけるテレワーク方式

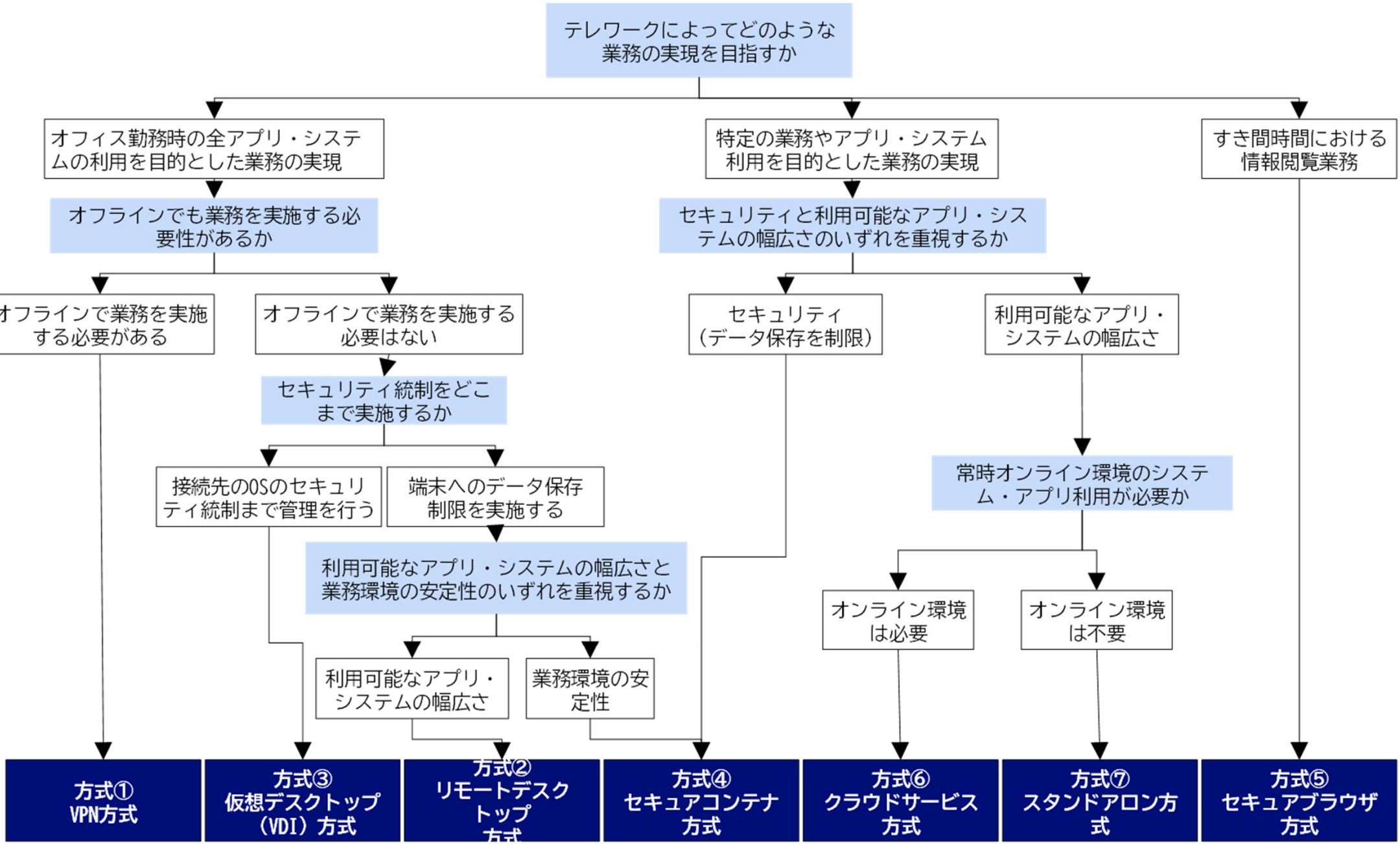
方式名	概要
① VPN方式	テレワーク端末からオフィスネットワークに対してVPN接続を行い、そのVPNを介してオフィスのサーバ等に接続し業務を行う方法
② リモートデスクトップ方式	テレワーク端末からオフィスに設置された端末（PC等）のデスクトップ環境に接続を行い、そのデスクトップ環境を遠隔操作し業務を行う方法
③ 仮想デスクトップ(VDI)方式	テレワーク端末から仮想デスクトップ基盤上のデスクトップ環境に接続を行い、そのデスクトップ環境を遠隔操作し業務を行う方法
④ セキュアコンテナ方式	テレワーク端末にローカル環境とは独立したセキュアコンテナという仮想的な環境を設け、その環境内でアプリケーションを動かし業務を行う方法
⑤ 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殊なインターネットブラウザを利用し、オフィスのシステム等にアクセスし業務を行う方法
⑥ クラウドサービス方式	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に直接接続し業務を行う方法
⑦ スタンドアロン方式	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録媒体に必要なデータを保存しておき、その保存データを使い業務を行う方法

✓各方式について解説図を作成

✓派生的な方式についても記載（例：クラウド型VPNサービスを利用する形式）

✓各方式に特有のセキュリティ上の注意事項についても記載

テレワーク方式の検討フローチャート



テレワーク方式の特性比較

テレワーク方式	オフィス業務の再現性	通信集中時の影響度	システム導入コスト	システム導入作業負荷	セキュリティ統制の容易性	ポイント（想定される使い方）
①VPN方式	**S**（オフィスと同等の業務が可能）	**A**（通信影響を受けるが、端末側(ローカル)作業で一部回避可）	**B**（システム導入が必要）	**B**（環境変更を伴うシステム導入が必要）	**C**（データ管理とセキュリティ統制が必要）	業務再現性が高く、通信集中にも対応したい場合の利用が想定
②リモートデスクトップ方式	**S**（オフィスと同等の業務が可能）	**C**（通信影響を受けやすい）	**B**（システム導入が必要）	**B**（環境変更を伴うシステム導入が必要）	**A**（データ保存を制限でき、データ管理が容易）	業務再現性が高く、セキュリティやコストをバランスする場合の利用が想定
③仮想デスクトップ（VDI）方式	**S**（オフィスと同等の業務が可能）	**C**（通信影響を受けやすい）	**C**（高額なシステム導入が必要）	**C**（大きな環境変更を伴うシステム導入が必要）	**S**（データ保存を制限でき、セキュリティの集中管理が容易）	業務再現性が高く、高度なセキュリティを実現したい場合の利用が想定
④セキュアコンテナ方式	**B**（特定のアプリやシステムでの作業のみ可能）	**A**（通信影響を受けるが、端末側(ローカル)作業で一部回避可）	**B**（システム導入が必要）	**B**（環境変更を伴うシステム導入が必要）	**A**（データ保存を制限でき、データ管理が容易）	セキュリティを確保しつつ通信集中にも対応したい場合の利用が想定
⑤セキュアブラウザ方式	**C**（メールや資料閲覧に限定）	**B**（通信影響を受けるが影響は軽微）	**B**（システム導入が必要）	**B**（環境変更を伴うシステム導入が必要）	**A**（データ保存を制限でき、データ管理が容易）	セキュリティを重視した、特定業務での利用が想定
⑥クラウドサービス方式	**B**（特定のアプリやシステムでの作業のみ可能）	**S**（オフィスネットワークに接続しないため影響なし）	**A**（サービス導入費（使用量に応じた必要最小限）が必要）	**A**（比較的軽微な環境変更で利用可能）	**D**（データ管理に加え、クラウド上でのデータ管理が必要）	拡張性を重視した、特定業務での利用が想定
⑦スタンドアロン方式	**D**（端末に保存したデータのみの作業が可能）	**S**（通信をしないため影響なし）	**S**（追加のシステム・サービス不要）	**S**（システム変更不要）	**C**（データ管理とセキュリティ統制が必要）	コストと導入のしやすさを重視した臨時利用が想定

テレワークセキュリティ対策

対策事項の分類

対策分類	説明
ガバナンス・リスク管理	テレワークの実施に当たってのリスクマネジメントや、情報セキュリティ関連規程（ルール）の整備等に関する対策。
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等の資産の特定や、その管理に関する対策。
脆弱性管理	ソフトウェアのアップデート実施等による既知の脆弱性の排除に関する対策。
特権管理	不正アクセス等に備えたシステム管理者権限の保護に関する対策。
データ保護	保護すべき情報（データ）の特定や保存されているデータの機密性・可用性の確保に関する対策。
マルウェア対策	マルウェアの感染防止や検出、エンドポイントセキュリティに関する対策。
通信の保護・暗号化	通信中におけるデータの機密性や可用性の確保に関する対策。

信頼できるクラウドサービス選定や、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

守るべきデータの特定と暗号化、バックアップ取得や確実な廃棄に言及

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)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

対策分類	説明
アカウント・認証管理	情報システムにアクセスするためのアカウント管理や認証手法に関する対策。
アクセス制御・認可	データやサービスへのアクセスを、必要最小限かつ正当な権限を有する者のみに制限することに関する対策。
インシデント対応・ログ管理	セキュリティインシデントへの迅速な対応と、ログの取得や調査に関する対策。
物理的セキュリティ	物理的な手段による情報漏えい等からの保護に関する対策。
脅威インテリジェンス	脅威動向、攻撃手法、脆弱性等に関する情報の収集に関する対策。
教育	テレワーク勤務者のセキュリティへの理解と意識の向上に関する対策。

攻撃起点となる認証突破対策として、多要素認証に言及

ゼロトラスト観点より、最小権限によるアクセス権統制に言及

完全防御が難しいという前提のもと、インシデント発生後の事後対応に言及

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等)に言及

セキュリティ関連機関が発信する情報の収集やコミュニティ加入の重要性に言及

注意喚起・教育等の重要性に言及

吹き出しは対策項目の見直しに当たって考慮した観点

テレワークにおけるトラブル事例と対策

トラブル事例

1．VPN機器の脆弱性の放置
2．個人情報保護の強化
3．アクセス権限の設定不備
4．マルウェア感染
5．ランサムウェア
6．フィッシングメール
7．ビジネスメール詐欺（BEC）
8．USBメモリの紛失
9．無線LAN利用通信の窃取
10．第三者による画面閲覧
11．テレワーク端末の踏み台化
12．パスワードの使い回し
13．クラウドサービスの設定ミス
14．クラウドサービスの障害
15．サプライチェーン

具体的事例と対策例（VPN機器の脆弱性の放置）

1．VPN機器の脆弱性の放置

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

① 具体的な動向

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。既知の脆弱性を放置したまま運用を続けていた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、この脆弱性を悪用する攻撃が既に発生しており、該当のVPN機器の製造ベンダー側でファームウェアの修正が行われていますが、ファームウェアを最新にアップデートしていない機器が攻撃を受けました。

トラブル事例を防ぐために、留意すべき点を記載

② テレワークセキュリティへの示唆

脆弱性への対応スピードが他の国と比較して日本は低いという調査結果があります。その調査の中では、米国、英国、ドイツ等の諸外国では、脆弱性公表から最初の１週間で２～５割の製品がアップデートされている中、日本ではアップデートの実施割合が１割にも満たないこと、また脆弱性公表から７カ月たった2020年３月下旬の時点でも、対応率が低いままとなっているという結果が出ています。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対応するため、過去に使用していて運用から外しておいたVPN機器を、設備増強用としてそのまま臨時稼働させたところ、脆弱性が潜んでいたために攻撃を受けたという企業もありました。このように、過去に使用していた機器を再利用する場合には、ファームウェアを最新の状態にして、既知の脆弱性が残っていない状態で使用することが重要です。

当該トラブル事例を防ぐために、該当する対策事項を記載

③ 有効な対策

	脆弱性管理（詳細解説はp.74～）
管理者C-2 基本対策	オフィスネットワークにアクセスする際に必要となる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やパッチ適用を定期的に行う。
管理者C-3 基本対策	テレワークで利用する端末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テレワーク勤務者に周知する。

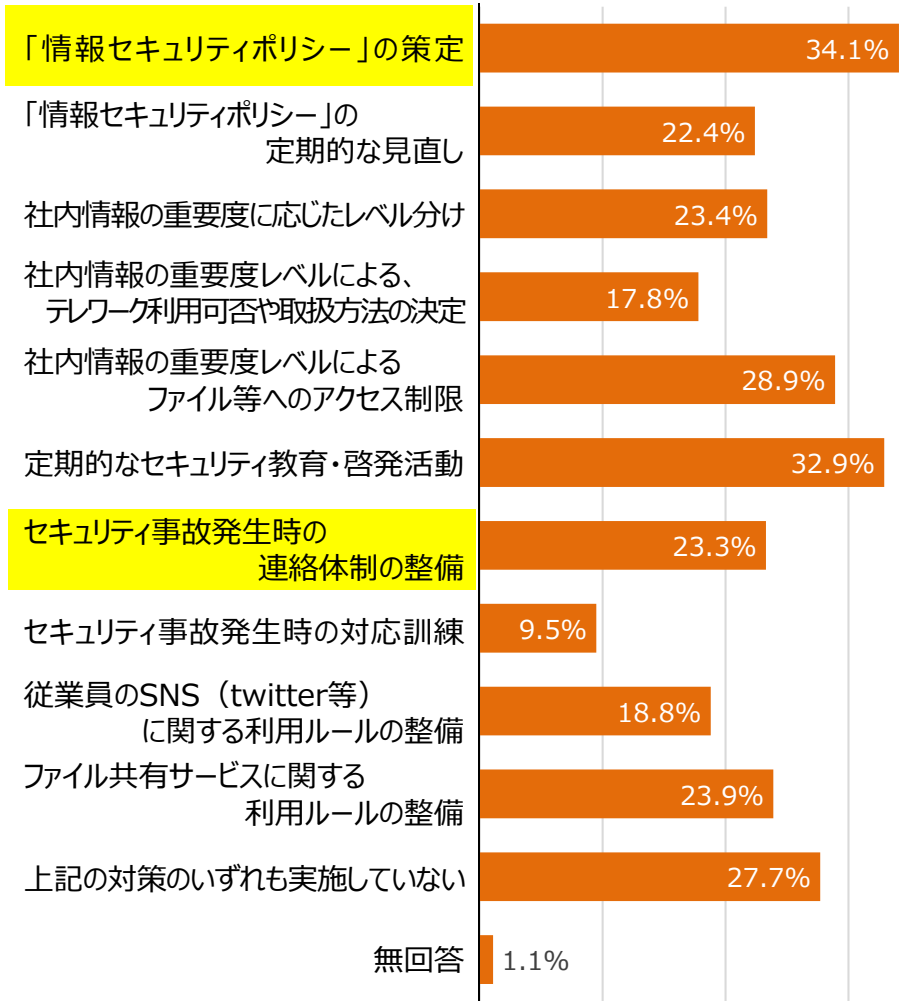
テレワークセキュリティに関する実態調査結果（対策実施状況）

1次調査

- 情報セキュリティポリシーを策定している企業は約３分の１にとどまる。
- セキュリティ対策ソフトが常に最新になるように指示・設定している企業も約３分の２にとどまる。

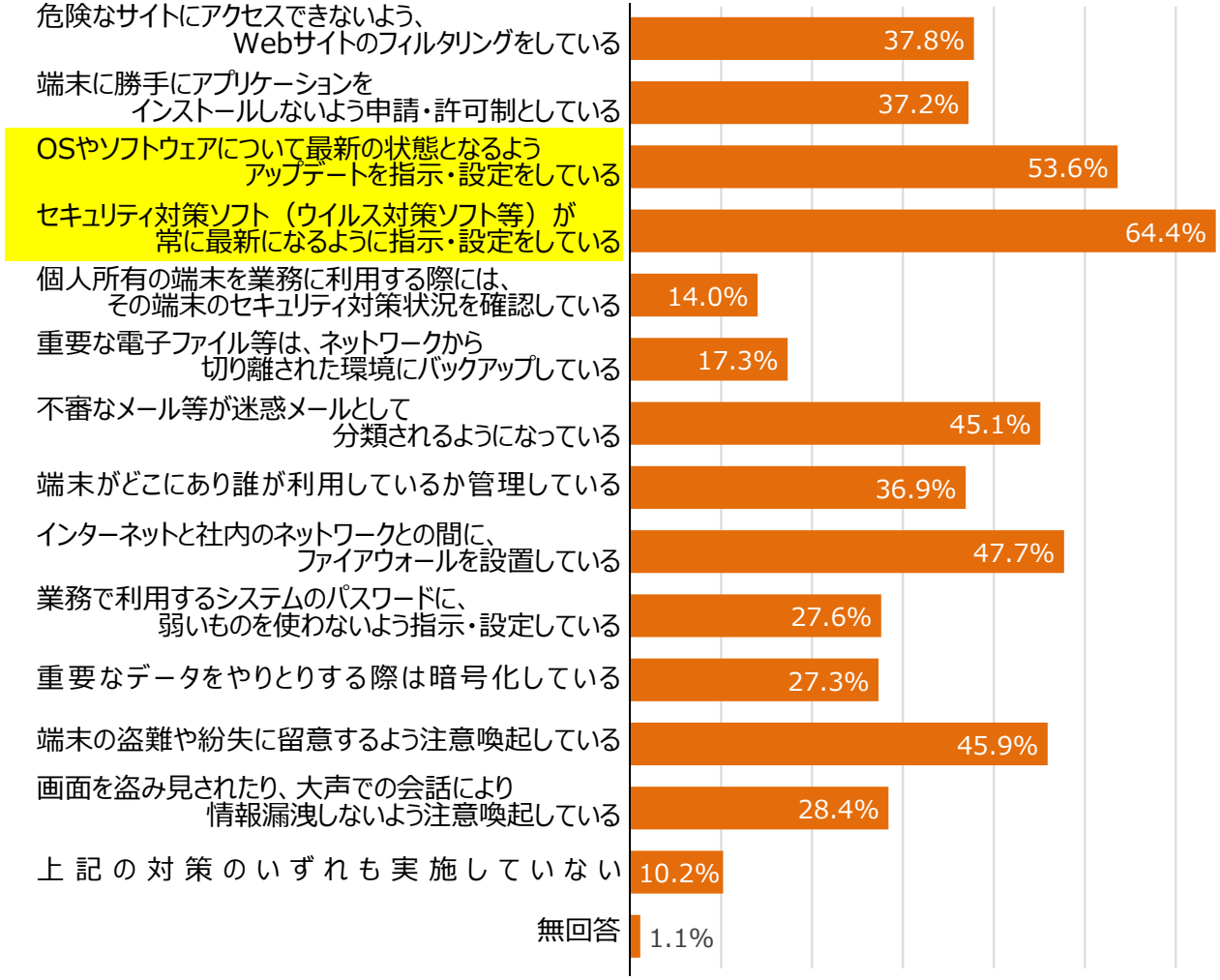
情報セキュリティの管理体制等に関する対策の実施状況

（n=1,569：テレワーク導入企業）　（複数回答可）



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）



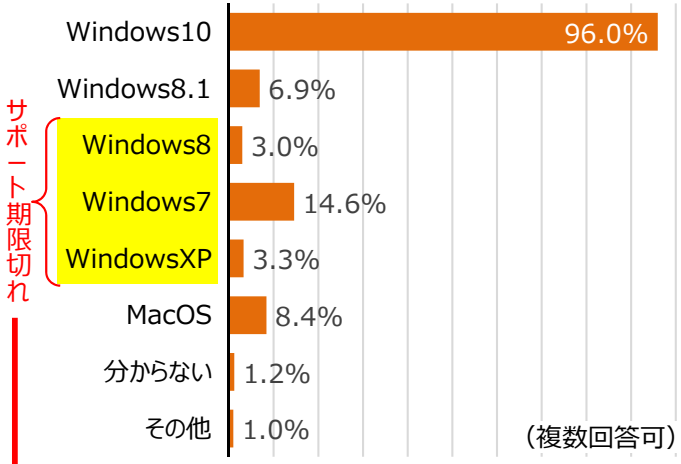
テレワークセキュリティに関する実態調査結果（サポート期限切れOS）

２次調査

- サポート期限切れOSが一部で使用され続けており、製造業や、大規模企業に多い傾向
  →製造装置やシステムに組み込まれており容易に更新できないような場合が想定
- サポート期限切れOSが危険という認識を持っていない場合も見受けられる。

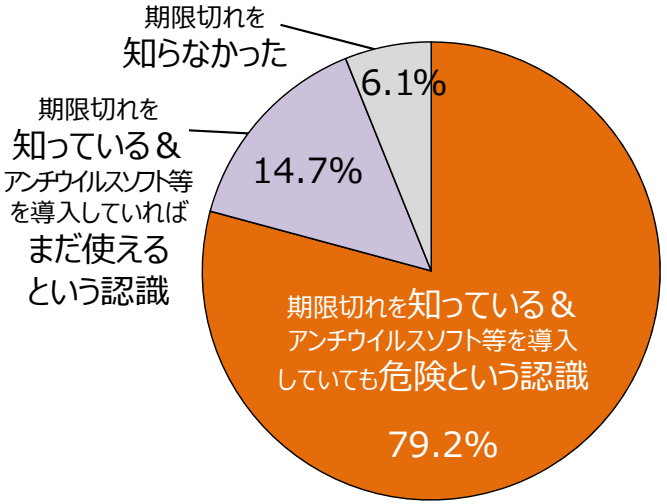
職場・テレワークに関わらず会社所有PC端末のOSの種類

（n=5,037：全回答者）



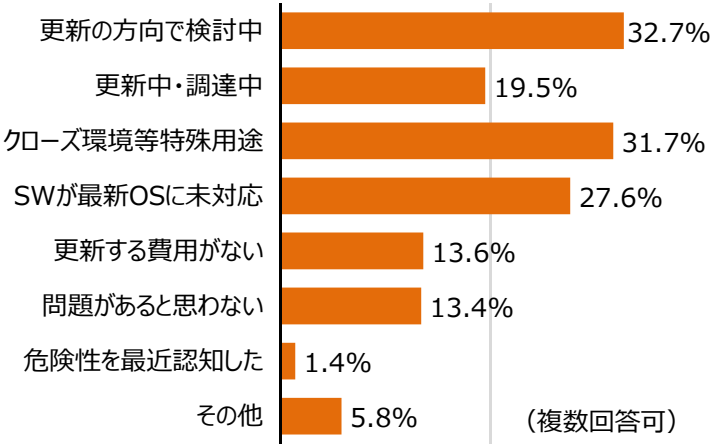
サポート期限切れOSに対する認識

（n=5,037：全回答者）



サポート期限切れOSを使用している理由

（n=851：サポート期限切れOSを使用している者）



(注)自由回答により、ESUを使用している企業も見受けられた
（ESU：Windows 7 拡張セキュリティ更新プログラム（最大で2023年1月まで））

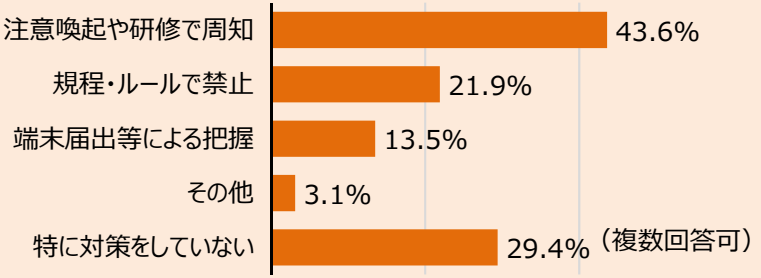
業種別	全回答数	期限切れOS使用	
		数	割合
全体	5,037	851	17 %
建設業	585	59	10 %
製造業	1,023	237	23 %
情報通信業	243	34	14 %
運輸業・郵便業	328	58	18 %
卸売・小売業	1,145	199	17 %
金融・保険業	52	7	13 %
不動産業	105	15	14 %
サービス業、その他	1,556	242	16 %

規模別	全回答数	期限切れOS使用	
		数	割合
全体	5,037	851	17 %
10～19人	1,877	268	14 %
20～29人	903	142	16 %
30～49人	803	130	16 %
50～99人	712	129	18 %
100～199人	401	93	23 %
200～299人	141	31	22 %
300人以上	200	58	29 %

（テレワーク時に従業員所有PCを許可している場合）

サポート期限切れ端末を使用しないようにする対策

（n=482：テレワーク時に従業員所有PC端末の利用を許可している者）



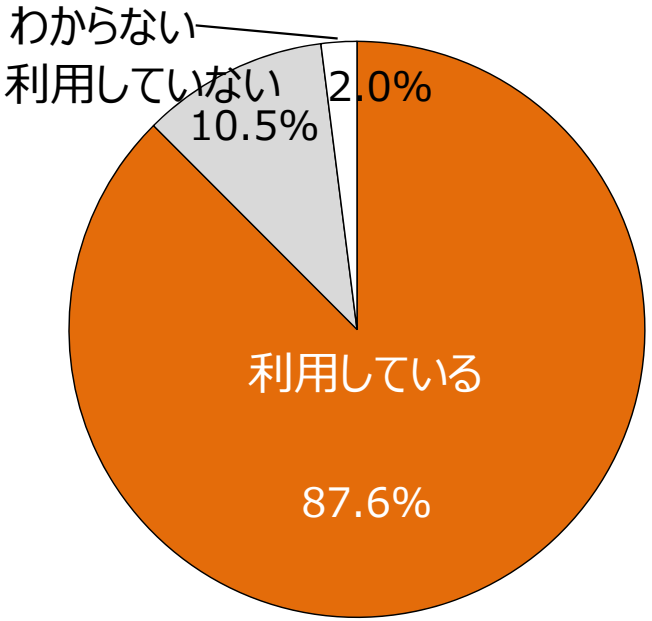
３．（参考）無線ＬＡＮにおけるセキュリティ確保

公衆無線LANの利用状況

➢ 無線LANに対するセキュリティ意識等を把握するための調査をWebアンケートにより実施。
期間：2021.3.16-19　調査数：30,000（うち無線LAN利用者1,000をスクリーニング（性別・年代を「モバイル端末によるインターネット利用者数」により割り付け））

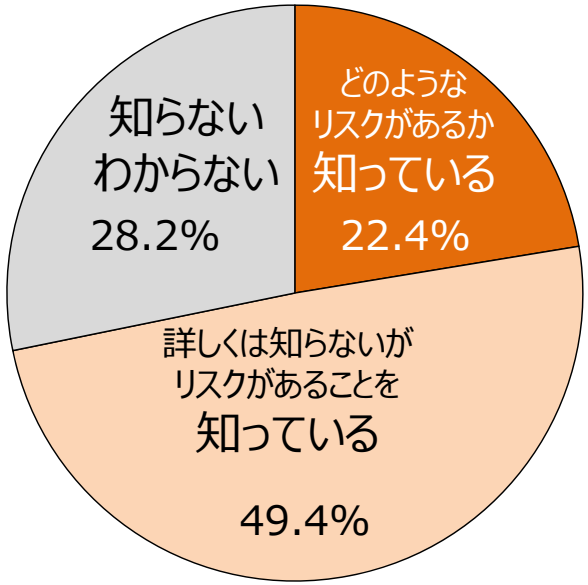
自宅無線LANの利用有無

（n=30,000：全員）



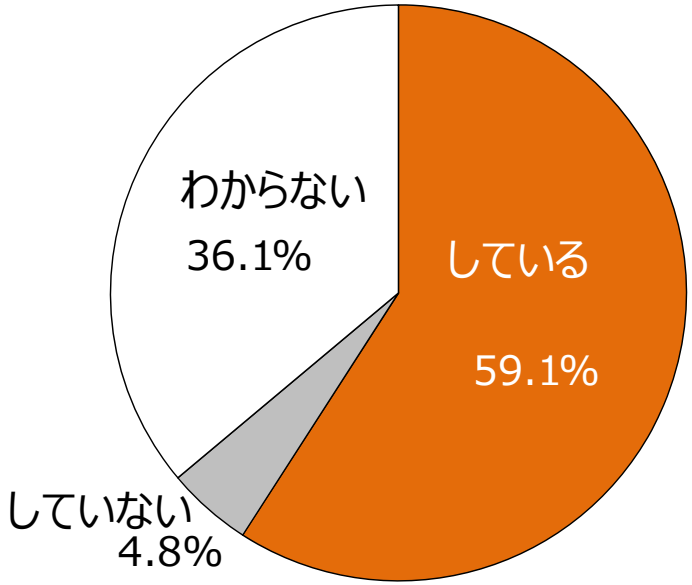
無線LAN利用時における セキュリティ上のリスク認知

（n=30,000：全員）



自宅無線LANの暗号化

（n=962：自宅無線LANの利用者）

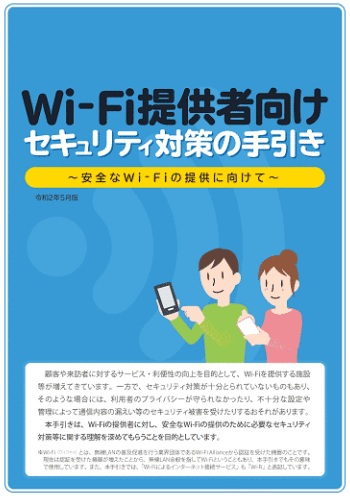


無線LANのセキュリティガイドライン

- 総務省では、無線LANの利用者・提供者向けにガイドラインを作成しており、周知啓発に活用。
- 新技術や最新のセキュリティ動向に対応するため、内容を見直し2020年５月に改定版を公表。
- 改定版については、Wi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に幅広く周知。
  https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

「Wi-Fi利用者向け 簡易マニュアル」(平成27年3月10日版)の見直しポイント

- ✓ セキュリティ対策の訴求点を明確にするため、**セキュリティ対策のポイント**を**整理**
  - ① 接続する**アクセスポイント**をよく**確認**（偽アクセスポイント対策として接続URL等を確認）
  - ② 正しい**URL**で**HTTPS通信**をしているか**確認**（Wi-Fi暗号化等に関わらず通信内容を保護）
  - ③ 自宅に設置している**機器の設定**を**確認**（管理用パスワードの変更やファームウェアアップデート等）
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**



「Wi-Fi提供者向け セキュリティ対策の手引き」(平成28年8月版)の見直しポイント

- ✓ ガイドラインの対象者の明確化（**自店利用者のみへ提供する者も対象**）
- ✓ 近年懸念されている**偽アクセスポイント対策**（認証画面のURLの周知等）を追記
- ✓ 暗号化のための**パスフレーズを公開**している場合解読の**リスクが高まる**ことを明示
- ✓ 状況に応じたセキュリティ対策の選択と**利用者への周知**が必要であることを明確化
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**

「Wi-Fi利用者向け 簡易マニュアル」 概要

1　接続するアクセスポイントをよく確認しよう

- ✓ 接続しようとしているWi-Fiサービスを確認
  - 掲示されているステッカー等で、提供者やサービス内容を確認
  - 提供者が不明なものや不審と感じるものには接続しない
- ✓ 接続先の名前（SSID）を確認
  - SSIDが提供者が提供するものと同じか確認
  - 同じSSIDでも偽アクセスポイントの場合があるため、認証画面が表示された場合はURLとHTTPS通信を確認

Wi-Fiの**利用者**に対し、**安全なWi-Fiの利用**のために必要なセキュリティ対策等に関する理解を深めてもらうことを目的として作成。

2　正しいURLでHTTPS通信をしているか確認しよう

- ✓ URLが「https://」で始まるHTTPS通信により、通信全体の暗号化が可能
- ✓ ブラウザのURL入力欄に鍵マークがあることを確認
  （「！」やエラー表示が出ていないことを確認）
- ✓ URL（特にドメイン部分）を確認して、本物に巧妙に似せた偽URL・偽サイトに騙されない

3　自宅に設置している機器の設定を確認しよう

- ✓ セキュリティ方式は「WPA2」を選択
- ✓ Wi-Fiの暗号化のためのパスワードは第三者に推測されにくいものを設定
- ✓ Wi-Fi機器の管理用パスワードも同様
- ✓ ファームウェアを最新のものに更新

最後に　資料のご案内

紹介した各種文献については、

検索サイトで「**総務省　テレワーク　セキュリティ**」

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

または「**総務省　無線LAN　セキュリティ**」で検索

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/