参考資料２－１

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）
（初版）

総務省
Ministry of Internal Affairs and Communications

令和２年９月 11 日（ver.1.0）

テレワークセキュリティに関する Q&A と本書の対応ページ

Q1. まず何から始めればよいか知りたい。また、チェックリストを手早く確認したい。

A1. まず**第 1 部 2.「テレワーク方式の確認」**で自社のテレワークの方式を確認してください。
次に、**第 2 部 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」**で自社の方式に対応するチェックリストでセキュリティ対策状況を確認してください。

Q2. 各テレワーク方式がどういうものか、より具体的に知りたい。

A2. **第 1 部 3.「テレワーク方式の解説」**で各方式の特徴について、表や図を用いて解説しているので確認してください。

Q3. チェックリストの対策の必要性を知りたい。社内へ説明する理由がほしい。

A3. **第 1 部 4.「テレワーク環境で想定される脅威の解説」**には、チェックリストの対策を実施しなかった場合の脅威や業務影響について解説しています。各対策はこれらの脅威や業務影響のリスクを軽減できるように考えられています。

Q4. チェックリストの対策を実施するために、具体的な製品の設定方法を知りたい。

A4. **第2部 2.「セキュリティ対策チェックリストの設定例一覧」**では、よく利用されるテレワーク製品について、チェックリストの要求内容を実現するための設定例を解説しています。

Q5. テレワーク方式ごとではなく、チェックリスト全体を一覧的に確認したい。

A5. **第 2 部 3.「テレワーク環境のセキュリティ対策と想定脅威一覧」**には、チェックリストの内容を一覧表として整理しています。

第 1 部

第 2 部

目次

第１部

本書は、総務省の令和２年度「テレワークセキュリティに係るチェックリスト策定に関する調査研究」事業（受託者：NRI セキュアテクノロジーズ株式会社）により作成したものです。

第 1 部

1　はじめに

(ア) 本書の目的

本書は、**中小企業等の担当者の皆様がテレワーク導入や利用を進める**に当たり、中小企業等が考慮すべきセキュリティリスクを踏まえ、**実現可能性が高く優先的に実施すべきセキュリティ対策を簡潔に示した**ものです。

そのため、本書で示すセキュリティ対策は、**必ずしも網羅的ではありませんが、基本的かつ重要な（最低限必要となる）対策**になります。まずは、本書で示す対策を実施することを目標とすることで、効率的にセキュリティ対策を進めることができます。

なお、本書とは別に公表している『**テレワークセキュリティガイドライン（第 4 版）**』については、企業等を幅広く（規模等の区別なく）対象としてセキュリティの考え方や対策を整理しているものですが、**本書は予算や社内のセキュリティ体制が必ずしも十分ではない中小企業等を対象に作成しています**。（次ページの「(ウ) 本書の想定読者」もご確認ください。）

(イ) テレワークとは

本書が想定するテレワークとは、情報通信技術（ICT）の利活用により、時間・空間を有効に活用する多様な就労・作業形態を指し、本書では具体的に以下の 3 つの形態の総称として使用します。

①在宅勤務
②モバイルワーク
③サテライトオフィス勤務

在宅勤務

モバイルワーク

サテライトオフィス勤務

なお、ICT 技術の進歩によって、テレワーク環境においても、オフィス環境と全く同等とまでは言えないものの、オフィス環境と大きな遜色ない程度に業務の生産性を維持できるようになってきている傾向があります。また、こうしたテレワークには、一般に次に挙げるようなメリットがあると言われています。

・通勤時間節約や通勤ストレスからの解放
・仕事と育児・介護・治療との両立
・事業継続性の確保（Business Continuity Plan, BCP）

一方で、テレワークは全職種、全従業員を対象として一律に導入することが必ずしも期待する効果につながらない可能性もあります。テレワーク導入そのものを目的とはせずに、自社がテレワークを導入することによってどのようなメリットを享受したいかを整理した上でテレワーク導入を推進することを推奨します。

その上で、テレワークの導入や利用に当たり、最低限必要なセキュリティ対策を実施するために、本書を御活用願います。

(ウ) 本書の想定読者

本書は、中小企業等のセキュリティ管理担当者やシステム管理担当者（担当者ではないがこれらに準ずる役割を担っている方を含みます。）を読者として想定しています。具体的には次のとおり想定しており、これを念頭に用語や解説を付加して作成しています。

属性	本書の想定読者像	(参考)テレワークセキュリティガイドラインの想定読者像
セキュリティ予算の考え方	外部委託コストの捻出は難しい	外部委託コストは必要に応じて捻出しうる
セキュリティ推進体制	専任担当は存在しない	専任担当又は担当部門が存在する
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だけでは、対応すべき内容がわからない	「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
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 用語は聞いたことがあり、利用シーンがイメージできるレベル	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、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	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

(エ) 本書の活用方法

本書は、下表のとおり、主に 2 部構成で作成されています。

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・特定し、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できるようにしています。

本書の全体構成

構成		概要
第 1 部	1 はじめに	本書を活用するための、目的、想定するテレワーク、活用方法を説明しています。
	2 テレワーク方式の確認	テレワークの利用シーンを想定して、導入している（導入を予定している）テレワーク方式の確認手順を示しています。
	3 テレワーク方式の解説	テレワーク方式の詳細を解説しています。
	4 テレワーク環境で想定される脅威の解説	テレワーク環境において想定される脅威の概要を解説しています。
第 2 部	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	テレワーク方式ごとに実施すべきセキュリティ対策を確認できる「チェックリスト」です。
	2 セキュリティ対策チェックリストの設定例一覧	チェックリストの対策内容の実現方法の参考として、設定例の解説を行っている製品の一覧です。
	3 テレワーク環境のセキュリティ対策と想定脅威一覧	テレワーク環境におけるセキュリティ対策の「対策内容」「優先度」「想定脅威」「方式ごとの対策要否」を示しています。
参考	用語集	本書で用いている主な用語を説明しています。
	テレワークセキュリティに関する参考情報	チェックリストを実施するうえで参考となる文献や Web サイトなどを示しています。

第 1 部では、「2 テレワーク方式の確認」を参照して、自社のテレワークでの業務内容、利用する端末などの状況を基に、該当するテレワーク方式を確認してください。そのうえで、「3 テレワーク方式の解説」を参照して、自社のテレワーク方式の詳細を理解し、該当する方式に応じたチェックリストを選択してください。

第 2 部では、「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」を参照して、該当する方式に応じたセキュリティ対策を実施してください。

また、チェックリストの内容を具体的な環境で実施する際の参考としていただくために、一部の製品については設定解説資料を用意しています。「2 セキュリティ対策チェックリストの設定例一覧」では、設定解説の対象となっている製品を一覧として記載していますので、必要に応じて参照してください。

なお、セキュリティ対策を進めるに当たり、対策の重要性や必要性について組織内や経営層から説明を求められている場合など、セキュリティ対策への理解を深めてもらうために活用可能な資料として、第１部の「４　テレワーク環境において想定される脅威の解説」を作成しています。

2 テレワーク方式の確認

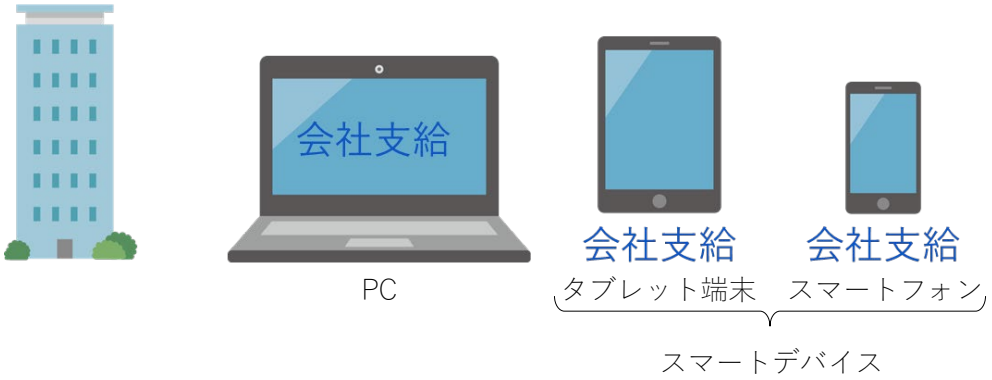
テレワークには、活用するシステム・環境などにより複数の方式が存在します。具体的には、テレワークで利用する端末種別、オフィスネットワークへの接続方式、テレワーク端末※へのデータ保存の有無などにより方式を分類することができ、各方式により考慮すべきセキュリティ対策も変わります。

ここでは、皆様の組織において導入している（導入を予定している）テレワーク方式を確認することを目的として、自社のテレワークでの業務内容、利用する端末などの状況を基に、該当するテレワーク方式を選択します。組織内で複数の方式の利用が想定される場合は、該当する複数の方式についてそれぞれご確認ください。

テレワーク端末の例

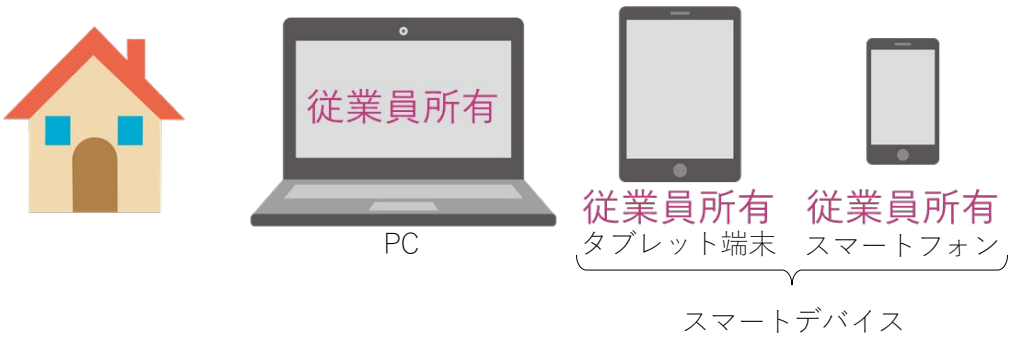
会社支給の端末：

オフィスから持ち出して使用する PC やスマートデバイス（タブレット端末・スマートフォン）が該当



従業員所有の端末：

従業員が所有しており、業務に利用する PC やスマートデバイス（タブレット端末・スマートフォン）が該当



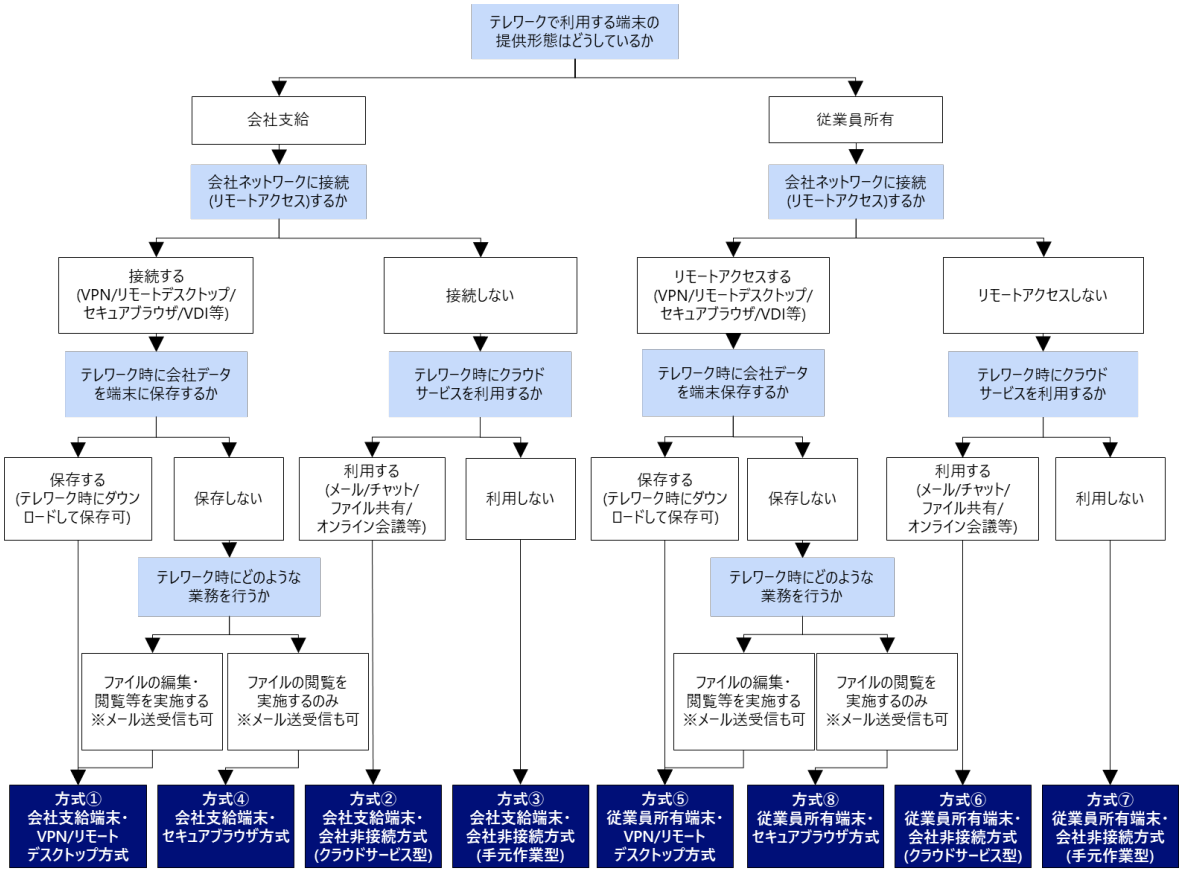
(ア) テレワーク方式の確認手順

下図のフローチャートを活用し、各設問について、自社の環境にあてはまるものを選択肢から選んでいくことで、該当する方式が確認できます。

各方式の詳細な説明については、「3 テレワーク方式の解説」をご覧ください。

また、該当する方式におけるセキュリティ対策に関するチェックリストは、「第２部　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」に方式ごとに整理しています。なお、複数の方式が該当する場合は、該当する全ての方式のチェックリストを確認してください。

テレワーク方式確認のフローチャート



※PC やスマートデバイス等の複数の環境を併用しており、環境ごとに利用形態が異なる場合は、環境ごとに上記のフローチャートで方式を確認してください。

3 テレワーク方式の解説

前ページのフローチャートにおける各テレワーク方式について、具体的に解説します。

皆様の組織において導入している（導入を予定している）として選択したテレワーク方式が、適切に選択できているかの確認にもご活用下さい。

また、チェックリストは方式ごとに「第２部　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」に整理しています。なお、複数の方式が該当する場合は、該当する全ての方式のチェックリストを確認してください。

なお、各方式の解説に当たって共通的な用語については、下表に解説していますので、参照ください。

用語	解説
VPN	Virtual Private Network の略。あたかも自社ネットワーク内部の通信のように、自宅や外出先などの遠隔の場所から安全に社内ネットワークにアクセスが行える技術のことです。
リモートデスクトップ	社内ネットワークに置いてある PC の画面をネットワーク経由で手元 PC（テレワーク端末）に転送して表示し、遠隔から社内ネットワーク上の PC を操作する技術のことです。
セキュアブラウザ	社内システムやクラウドサービス上に保管された情報を閲覧する際に利用する専用ソフトウェアで、情報閲覧時に手元の端末にデータが保存されない（できない）機能があるものです。製品によっては、スクリーンショット、テキストのコピー&ペースト、アクセス可能なページの制限を行えるものもあります。
クラウドサービス	従来は、PC やサーバで管理・利用していたようなソフトウェアやデータ等を、インターネット等のネットワークを通じて利用できるようにした様々なサービスの総称。本書では、メール、チャット、オンライン会議、ファイル共有などのクラウドサービスを想定しています。また、プロバイダーが提供するメールサービスの利用も含みます。
テレワーク端末へのデータ保存	テレワークの際に、社内サーバやクラウドサービスにデータを保存するのではなく、テレワーク環境で利用する（持ち出して利用する）端末にデータを保存する場合をさします。データの保存場所がよくわからない場合は、テレワーク端末がネットワーク（社内ネットワークやインターネット）に接続していない状態でも該当データにアクセスできる場合は、テレワーク端末にデータが保存されていると考えることができます。

(ア) テレワーク方式の概要

各テレワーク方式について、テレワーク端末として「会社支給の端末」と「従業員所有の端末」のそれぞれを活用する場合に分けて、その概要を説明します。

① テレワーク端末として会社支給の端末を活用する場合

方式	オフィスネットワークへの接続方式	クラウドサービス利用	テレワーク端末へのデータ保存	概要	該当ページ
方式① 会社支給端末・VPN/リモートデスクトップ方式	VPN、リモートデスクトップ等	利用する/利用しないどちらも含む	保存する ※リモートデスクトップ接続の場合は「保存しない」場合も含む	会社支給のテレワーク端末からオフィスネットワークにVPN 接続し、業務を行う方式。 または、会社支給のテレワーク端末からオフィスネットワークにリモートデスクトップ接続し、業務を行う方式。 いずれの場合も手元端末上で作業をするケースも含む。	方式解説 p.14~15 チェックリスト p.33～
方式② 会社支給端末・会社非接続方式（クラウドサービス型）	接続しない	利用する	保存する/保存しないどちらも含む	会社支給の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アクセスし、業務を行う方式。手元端末上で作業を実施するケースも含む。	方式解説 p.16 チェックリスト p.37～
方式③ 会社支給端末・会社非接続方式（手元作業型）	接続しない	利用しない	保存する	会社支給のテレワーク端末をテレワーク環境に持ち出して、あらかじめ保存しておいたファイルの編集・閲覧作業のみを手元端末上で実施し、業務を行う方式。	方式解説 p.17 チェックリスト p.41～
方式④ 会社支給端末・セキュアブラウザ方式	セキュアブラウザ	利用する	保存しない	会社支給のテレワーク端末から、特殊なセキュアブラウザ（手元端末へのデータ保存制限等）を活用し、社内システムやクラウドサービスのアプリケーションソフトウェアにアクセスし、業務を行う方式。	方式解説 p.18 チェックリスト p.45～

②　テレワーク端末として従業員所有の端末を活用する場合

方式	オフィスネットワークへの接続方式	クラウドサービス利用	テレワーク端末へのデータ保存	概要	該当ページ
方式⑤ 従業員所有端末・VPN/リモートデスクトップ方式	VPN、リモートデスクトップ等	利用する/利用しないどちらも含む	保存する ※リモートデスクトップ接続の場合は「保存しない」場合も含む	従業員所有のテレワーク端末からオフィスネットワークにVPN 接続し、業務を行う方式。手元端末上で作業を実施するケースも含む。 または、従業員所有のテレワーク端末からオフィスネットワークにリモートデスクトップ接続し、業務を行う方式。いずれの場合も手元端末上で作業をするケースも含む。	方式解説 p.19~20 チェックリスト p.49～
方式⑥ 従業員所有端末・会社非接続方式（クラウドサービス型）	接続しない	利用する	保存する/保存しないどちらも含む	従業員所有の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アクセスし、業務を行う方式。手元端末上で作業をするケースも含む。	方式解説 p.21 チェックリスト p.53～
方式⑦ 従業員所有端末・会社非接続方式（手元作業型）	接続しない	利用しない	保存する	従業員所有のテレワーク端末をテレワーク環境に持ち出して、あらかじめ保存しておいたファイルの編集・閲覧作業のみを手元端末上で実施し、業務を行う方式。	方式解説 p.22 チェックリスト p.57～
方式⑧ 従業員所有端末・セキュアブラウザ方式	セキュアブラウザ	利用する	保存しない	従業員所有のテレワーク端末から、特殊なセキュアブラウザ（手元端末へのデータ保存制限等）を活用し、社内システムやクラウドサービスのアプリケーションソフトウェアにアクセスし、業務を行う方式。	方式解説 p.23 チェックリスト p.60～

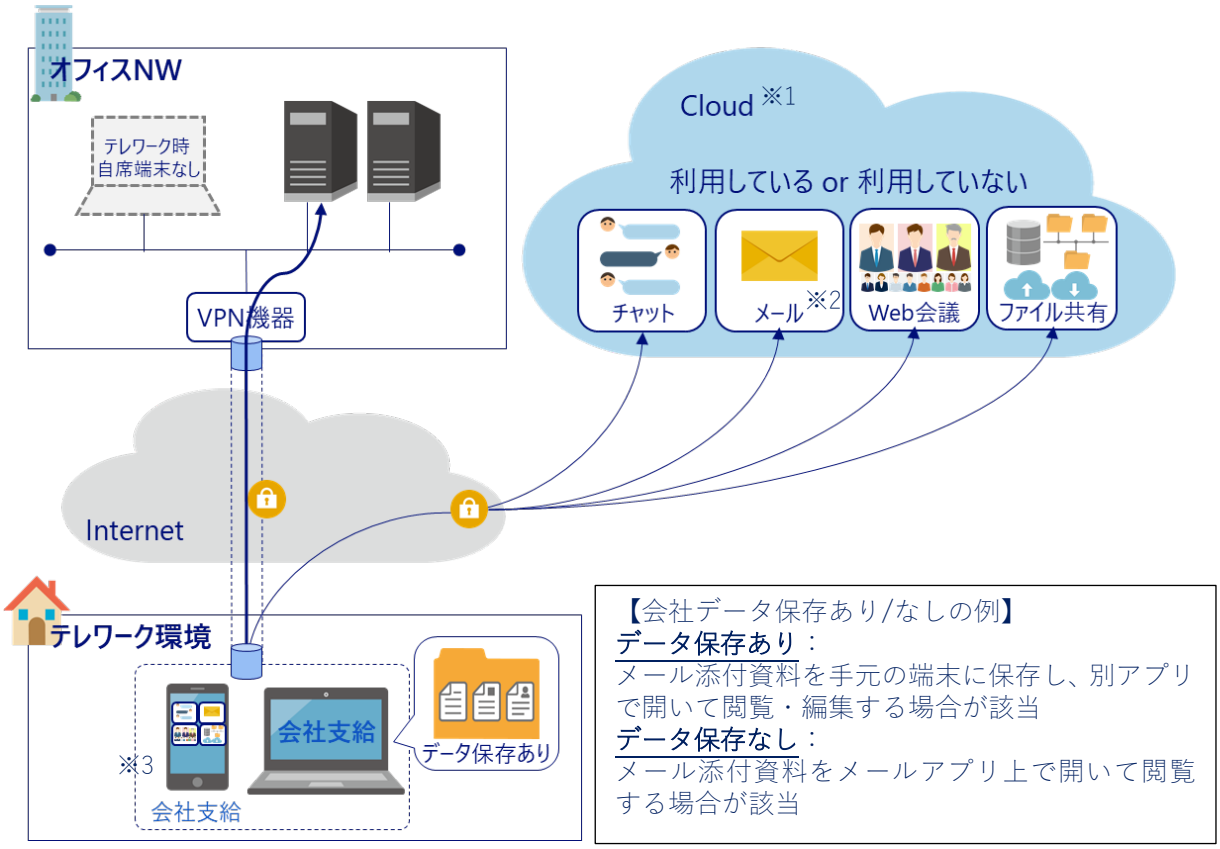
(イ) テレワーク方式の詳細

各テレワーク方式の詳細な具体的説明について、図解とともに説明します。

① 会社支給端末・VPN/リモートデスクトップ方式

以下の(1)と(2)に示す 2 パターンの接続方式が該当します。

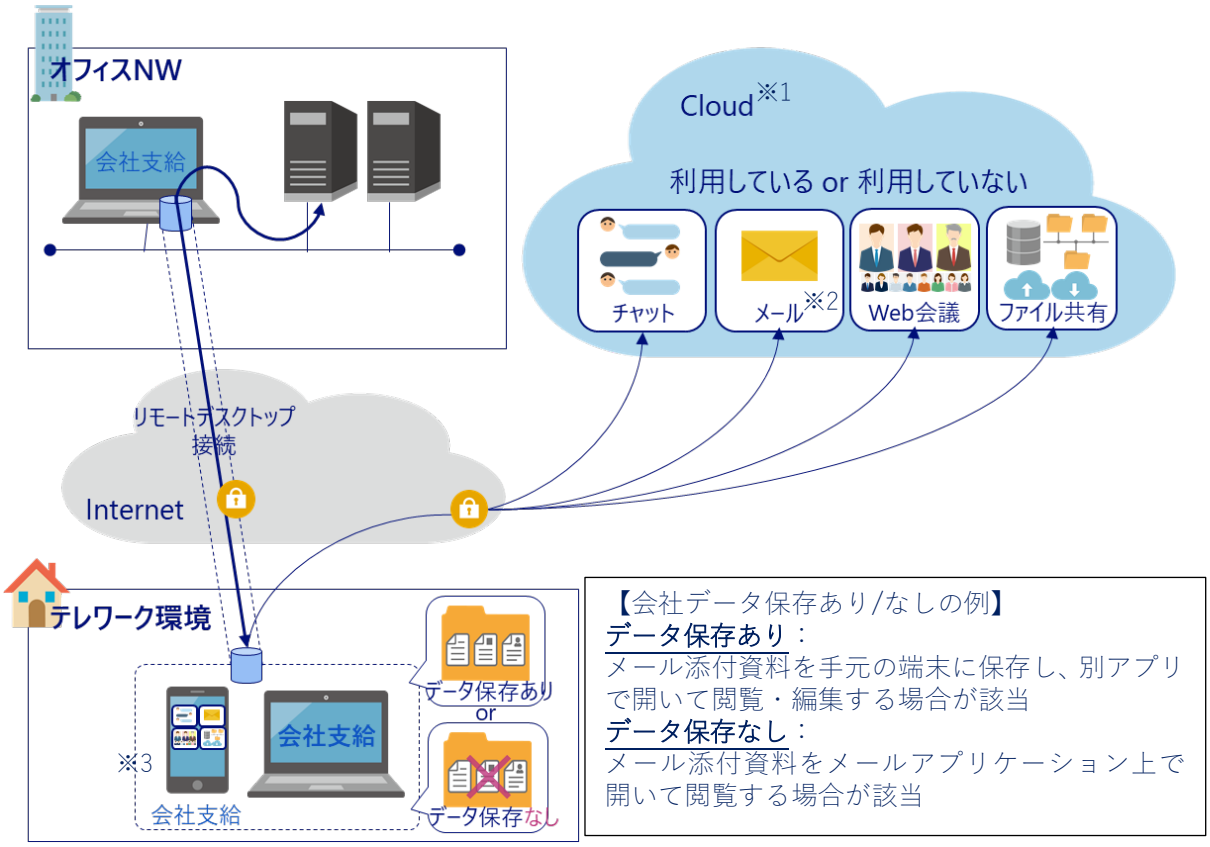
(1) 会社支給のテレワーク端末からオフィスネットワークへ VPN 接続して業務を実施します。オフィスと同等の業務環境を実現することが可能です。手元のテレワーク端末上で作業を併せて実施するケースも含みます。



【会社データ保存あり/なしの例】
データ保存あり：
メール添付資料を手元の端末に保存し、別アプリで開いて閲覧・編集する場合が該当
データ保存なし：
メール添付資料をメールアプリ上で開いて閲覧する場合が該当

※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

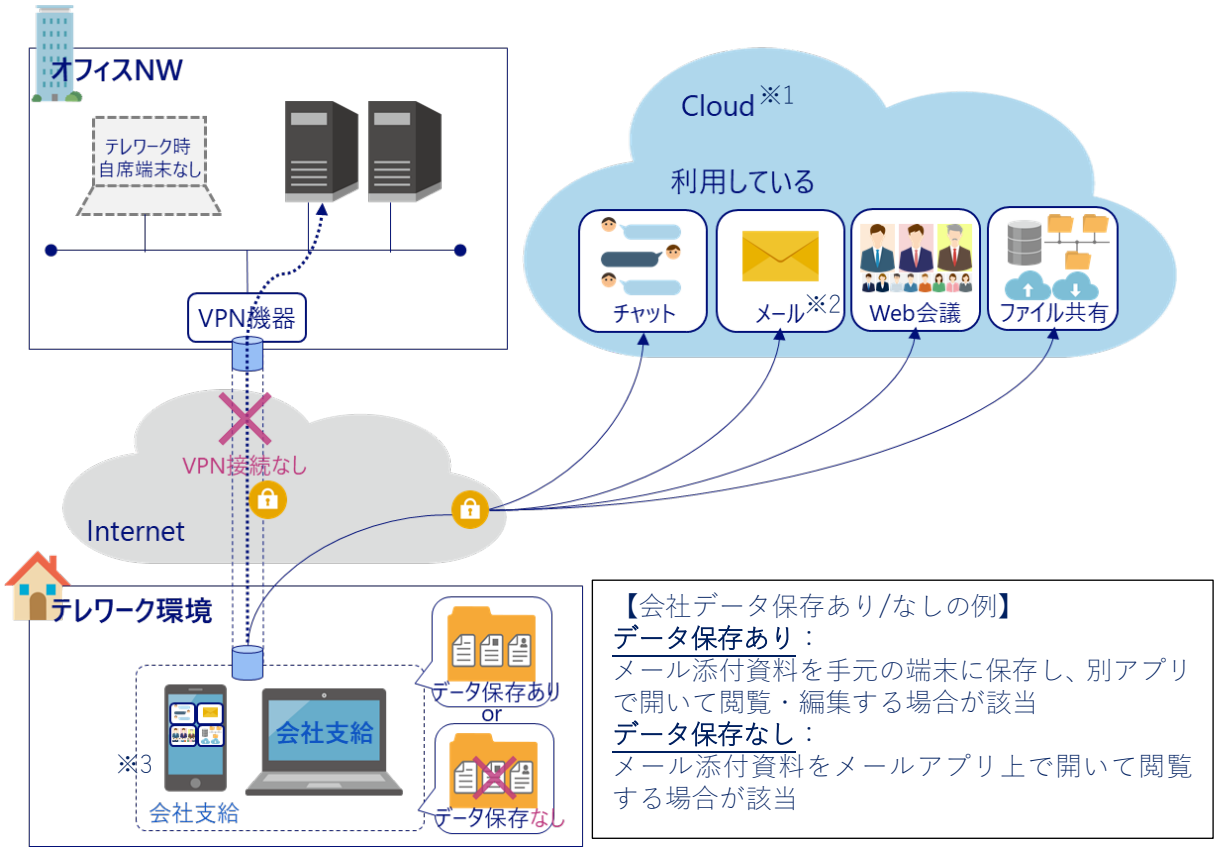
(2) 会社支給のテレワーク端末からオフィスネットワークにある会社支給の端末へリモートデスクトップ接続して業務を実施します。オフィスと同等の業務環境を実現することが可能です。手元のテレワーク端末上で作業を併せて実施するケースも含みます。



※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

②　会社支給端末・会社非接続方式（クラウドサービス型）

会社支給の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アクセスして業務を実施します。オフィスネットワークに接続しないのが特徴であり、クラウドサービスの活用により、オフィスと同等の業務環境を実現しうる可能性があります。手元のテレワーク端末上で作業を併せて実施するケースも含みます。

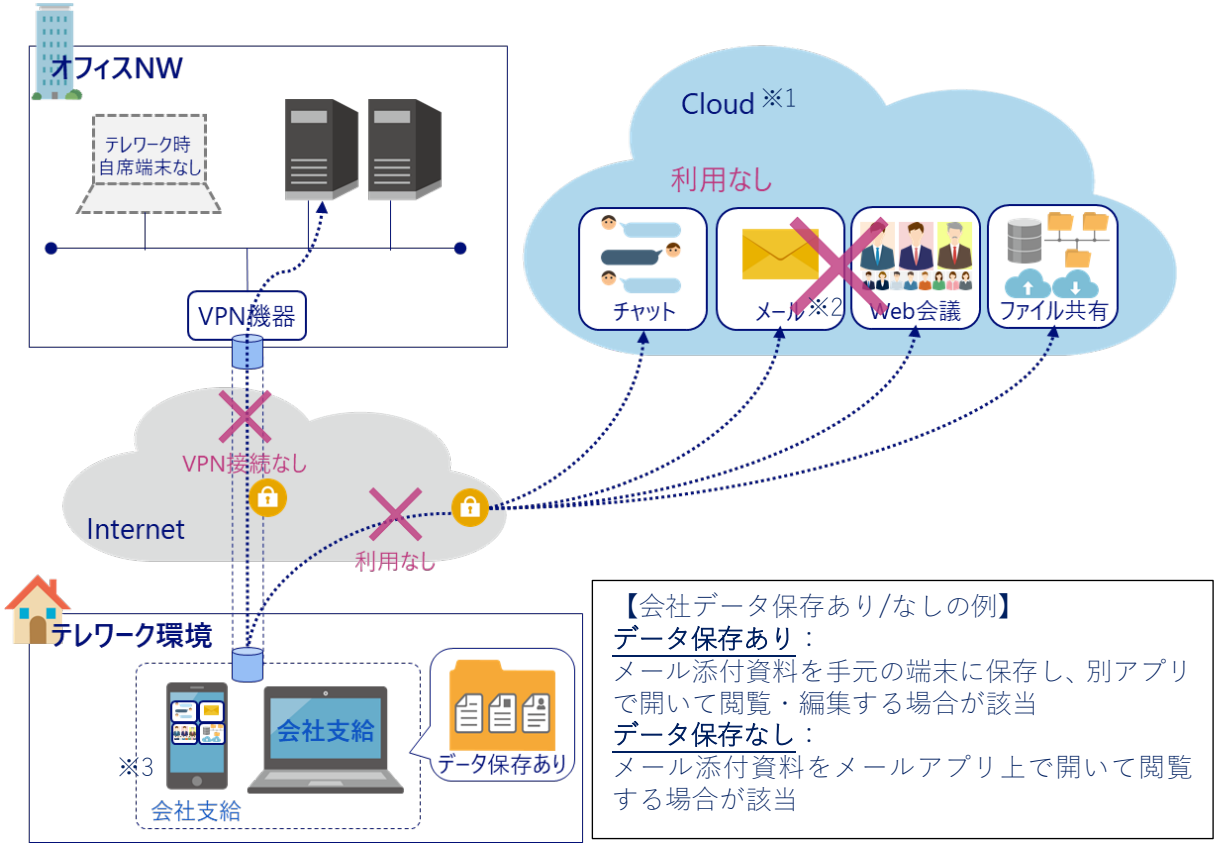


【会社データ保存あり/なしの例】
データ保存あり：
メール添付資料を手元の端末に保存し、別アプリで開いて閲覧・編集する場合が該当
データ保存なし：
メール添付資料をメールアプリ上で開いて閲覧する場合が該当

※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

③　会社支給端末・会社非接続方式（手元作業型）

会社支給のテレワーク端末をテレワーク環境に持ち出して、あらかじめ端末へ保存しておいたデータを編集・閲覧することで業務を実施します。オフィスネットワークに接続しないことに加え、クラウドサービスを利用しないことが特徴であり、限定業務のみを実施します。

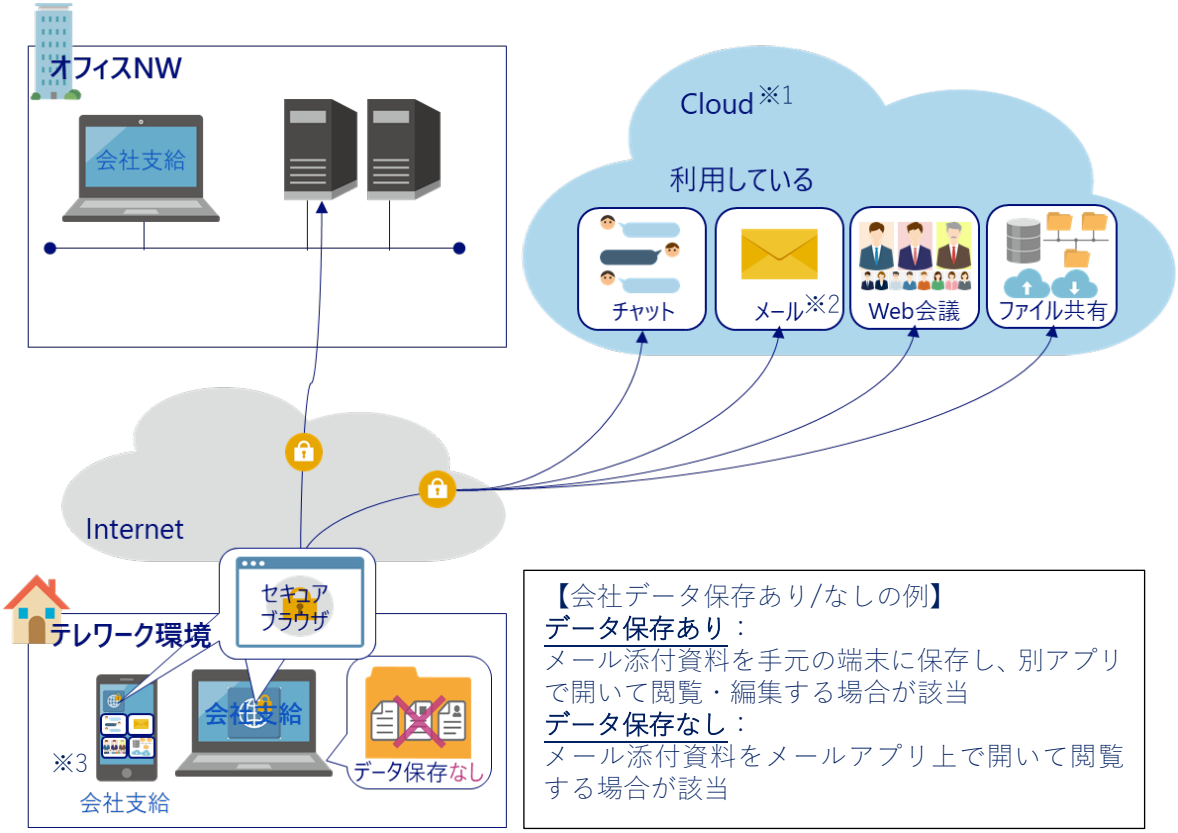


【会社データ保存あり/なしの例】
データ保存あり：
メール添付資料を手元の端末に保存し、別アプリで開いて閲覧・編集する場合が該当
データ保存なし：
メール添付資料をメールアプリ上で開いて閲覧する場合が該当

※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

④　会社支給端末・セキュアブラウザ方式

会社支給のテレワーク端末から特別なインターネットブラウザ（セキュアブラウザ）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て業務を実施します。端末へのデータ保存をしないことが特徴であり、限定業務のみを実施します。



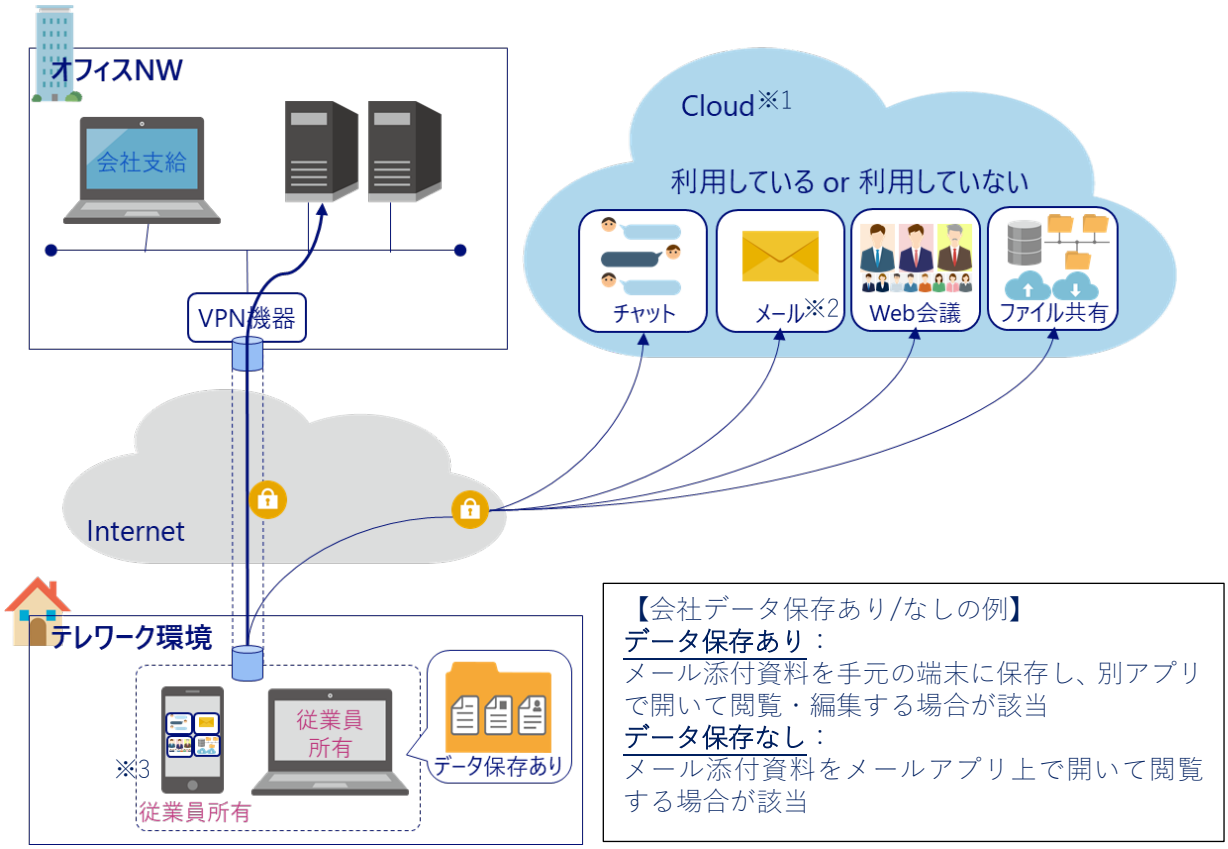
【会社データ保存あり/なしの例】
データ保存あり：
メール添付資料を手元の端末に保存し、別アプリで開いて閲覧・編集する場合が該当
データ保存なし：
メール添付資料をメールアプリ上で開いて閲覧する場合が該当

※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

⑤　従業員所有端末・VPN/リモートデスクトップ方式

以下の(1)と(2)に示す 2 パターンの接続方式が該当します。

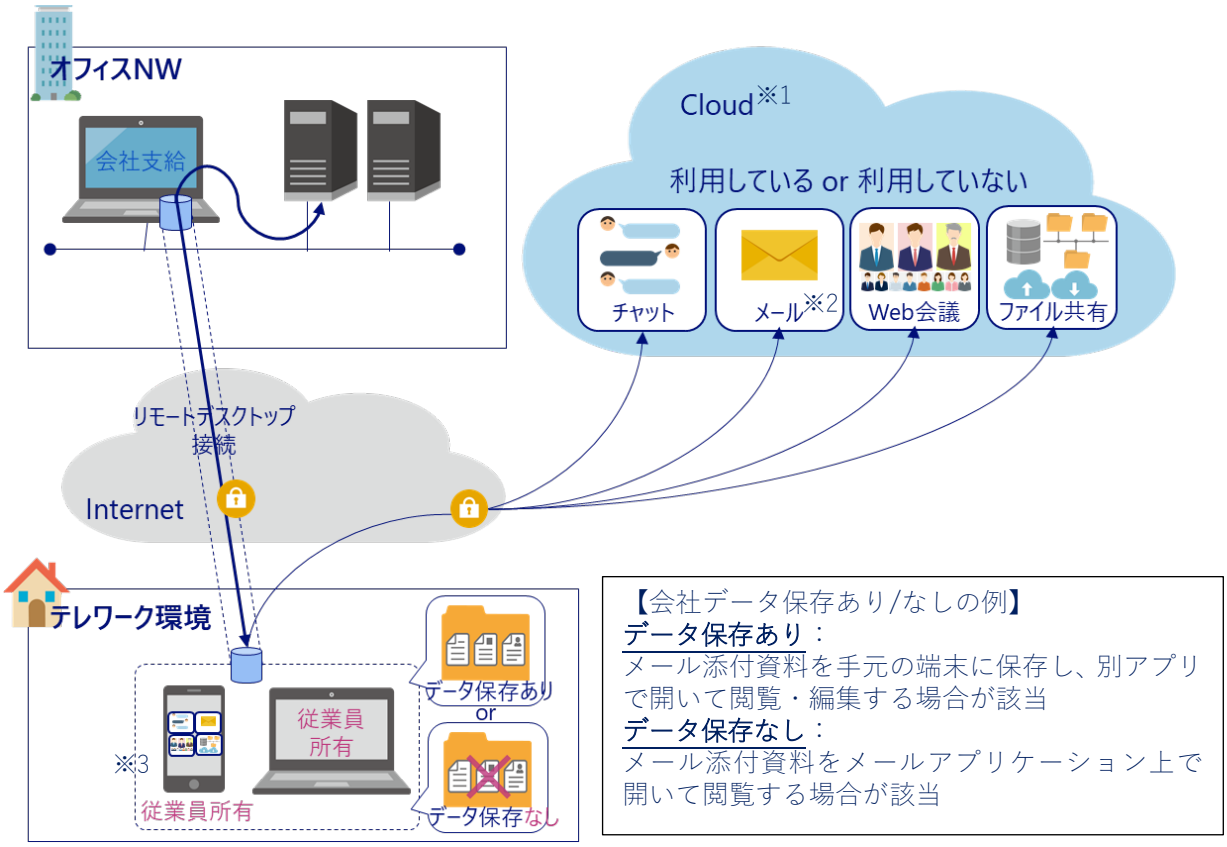
(1) 従業員所有のテレワーク端末からオフィスネットワークへ VPN 接続して業務を実施します。オフィスと同等の業務環境を実現することが可能です。手元のテレワーク端末上で作業を併せて実施するケースも含みます。



【会社データ保存あり/なしの例】
データ保存あり：
メール添付資料を手元の端末に保存し、別アプリで開いて閲覧・編集する場合が該当
データ保存なし：
メール添付資料をメールアプリ上で開いて閲覧する場合が該当

※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

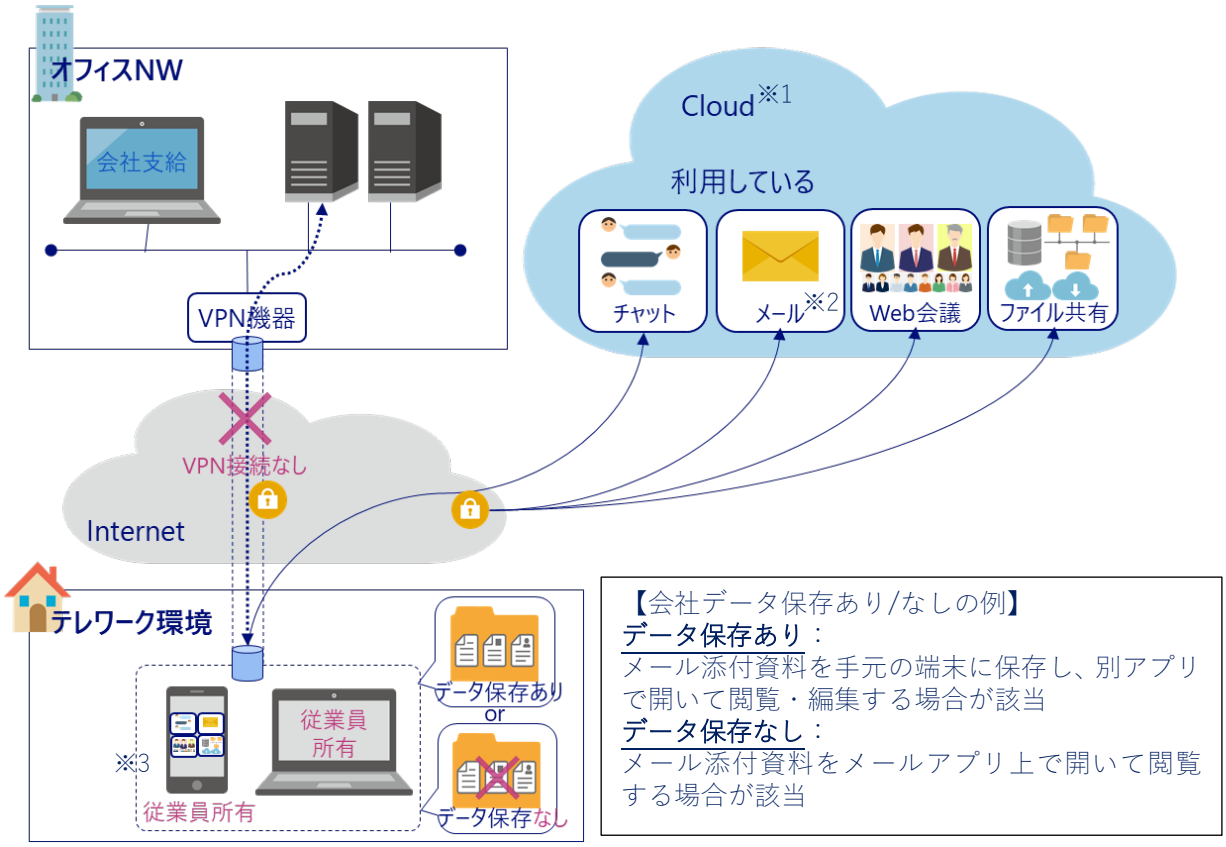
(2) 従業員所有のテレワーク端末からオフィスネットワークにある会社支給の端末へリモートデスクトップ接続して業務を実施します。オフィスと同等の業務環境を実現することが可能です。手元のテレワーク端末上で作業を併せて実施するケースも含みます。



※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

⑥　従業員所有端末・会社非接続方式（クラウドサービス型）

従業員所有の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接続して業務を実施します。オフィスネットワークに接続しないのが特徴であり、クラウドサービスの活用により、オフィスと同等の業務環境を実現しうる可能性があります。手元のテレワーク端末上で作業を併せて実施するケースも含みます。

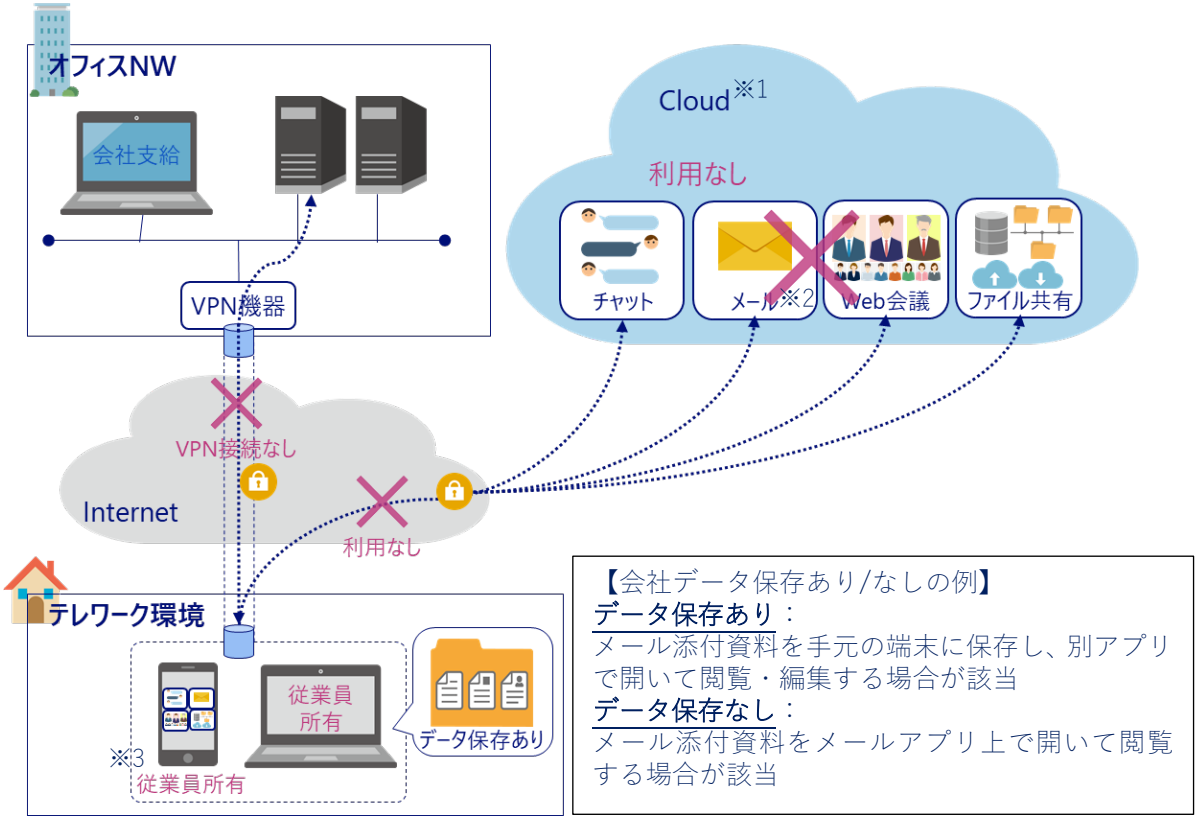


【会社データ保存あり/なしの例】
データ保存あり：
メール添付資料を手元の端末に保存し、別アプリで開いて閲覧・編集する場合が該当
データ保存なし：
メール添付資料をメールアプリ上で開いて閲覧する場合が該当

※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

⑦　従業員所有端末・会社非接続方式（手元作業型）

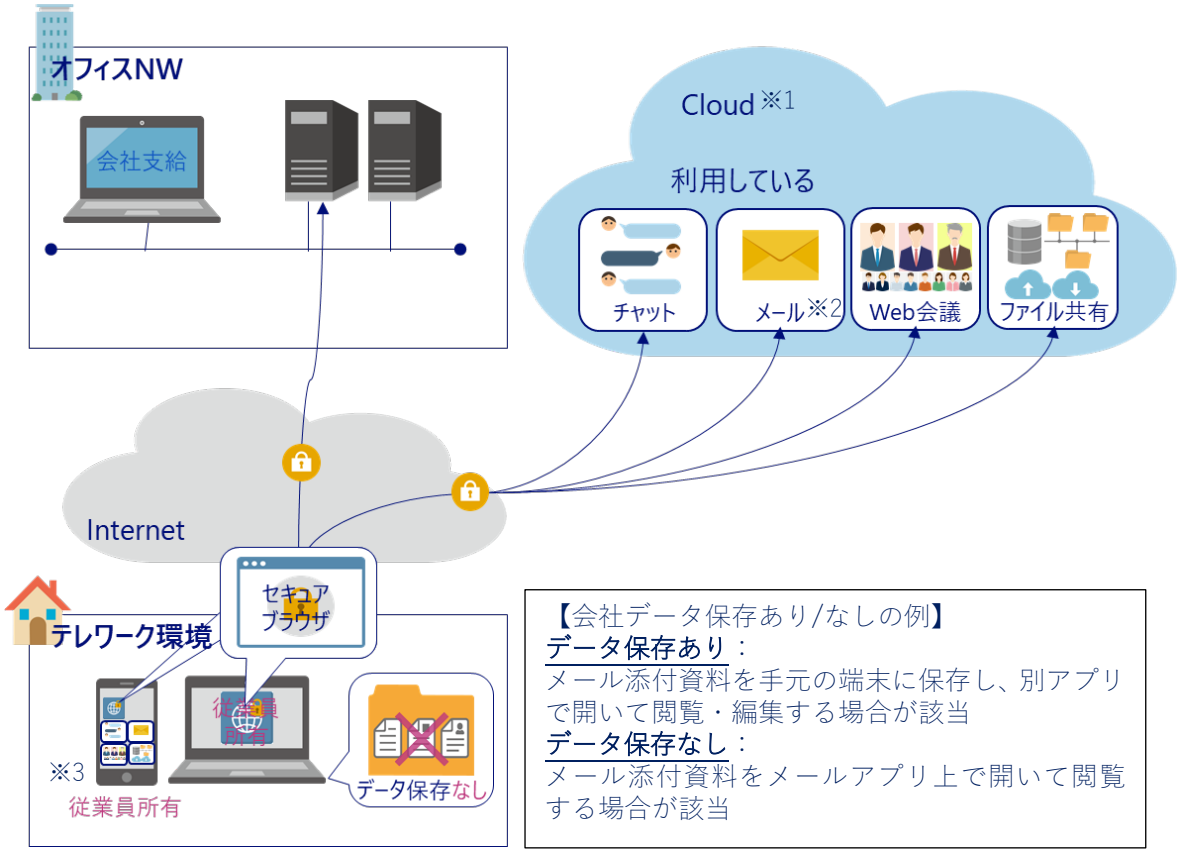
従業員所有のテレワーク端末をテレワーク環境に持ち出して、あらかじめ端末へ保存しておいたデータを編集・閲覧することで業務を実施します。オフィスネットワークに接続しないことに加えクラウドサービスを利用しないことが特徴であり、限定業務のみを実施します。



※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

⑧　従業員所有端末・セキュアブラウザ方式

従業員所有のテレワーク端末から特別なインターネットブラウザ（セキュアブラウザ）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て業務を実施します。端末へのデータ保存をしないことが特徴であり、限定業務のみを実施します。



【会社データ保存あり/なしの例】
データ保存あり：
メール添付資料を手元の端末に保存し、別アプリで開いて閲覧・編集する場合が該当
データ保存なし：
メール添付資料をメールアプリ上で開いて閲覧する場合が該当

※1：「クラウドサービスを利用している」は全部又は一部を利用しているケースが該当
※2：プロバイダー提供のメール利用もクラウドサービスに該当
※3：タブレット端末やスマートフォンのアプリを用いてメール等を使用している場合も「クラウドサービスを利用している」に該当

4　テレワーク環境で想定される脅威の解説

テレワーク環境において想定される脅威について、中小企業等の皆様の理解を深めるために、各脅威の概要に加え、顕在化の流れや顕在化による業務影響を簡潔に解説しています。解説の作成に当たっては、セキュリティ対策を進めるに当たり、対策の重要性や必要性をシステム担当者等が組織内に理解してもらうために活用することができるようにしています。

各脅威は、典型的な攻撃手法や増加傾向・注目度が高い攻撃手法、脅威から想定される各種被害について、起因・過程・被害の 3 つのステップに分けて図解します。

また、「第 2 部　1 チェックリスト方式ごとのセキュリティ対策チェックリスト」のチェックリストの各対策が、起因・過程・被害のいずれのステップで有効な対策であるかを、図解中の「関連するチェックリストの対策」に示しています。

(ア) 脅威の解説　マルウェア感染

①　マルウェア感染とは

マルウェアとは、不正かつ有害な動作を行う目的で作成された悪意のあるソフトウェアや悪質なコードの総称です。一般的に「コンピュータウイルス」と呼ばれるものも、マルウェアの一種に該当します。

また、昨今話題になっているランサムウェアもマルウェアの一種で、感染した端末をロックしたり、端末上のデータを暗号化して使用不能にしたりします。

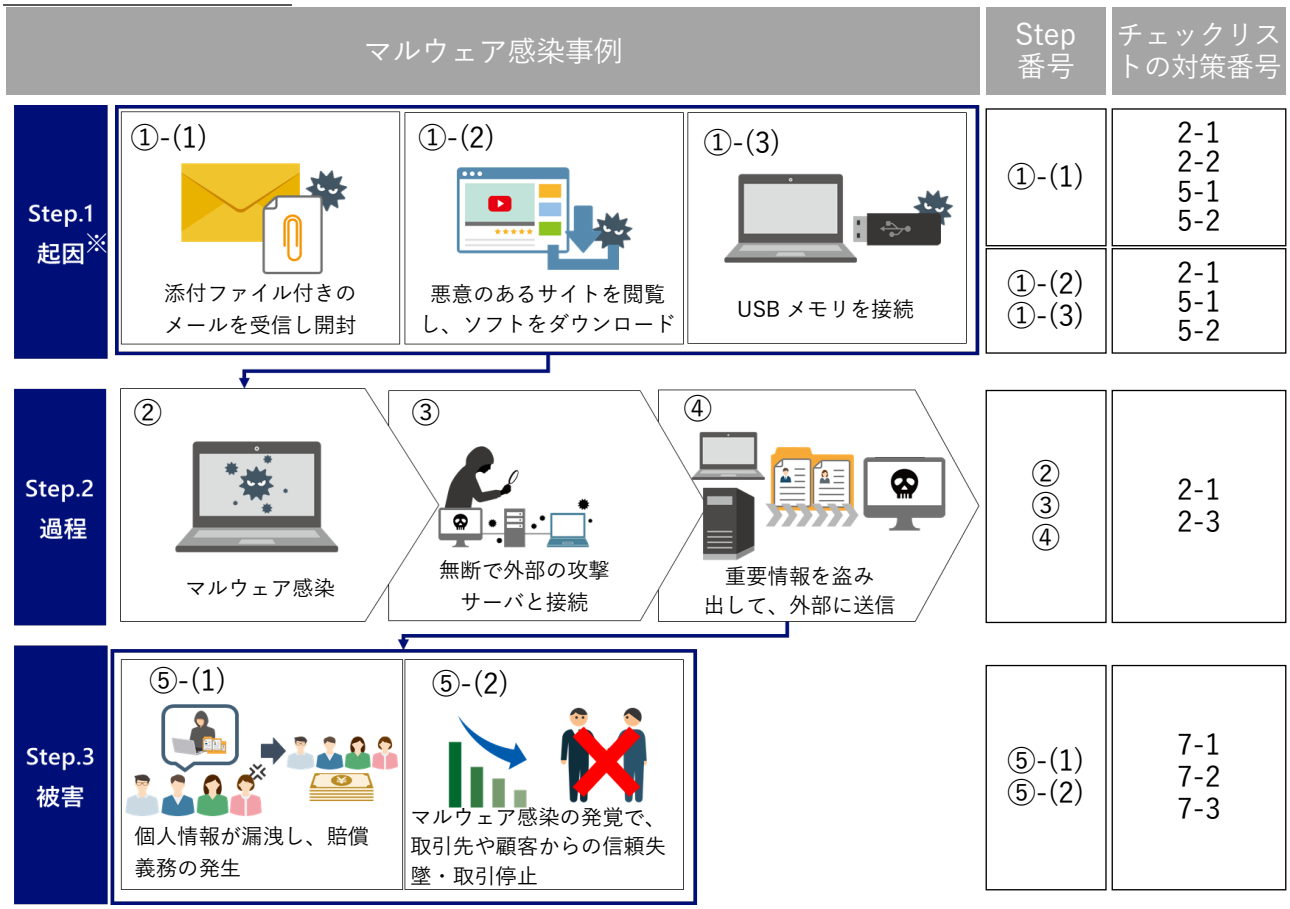
マルウェア感染とは、悪意あるソフトウェアや悪質なコードがソフトウェアに組み込まれることを指します。

一般的なマルウェアに感染した場合、機器本来の動作の妨害や、データの破壊による「業務停止」、データの外部送信による「情報漏洩」、また、自組織の機器が他の攻撃に悪用された場合、「攻撃の加害者」となる可能性があります。

ランサムウェアに感染した場合、感染した端末にあるデータや、当該端末を通じて社内のファイルサーバや外付けハードディスクなどの外部記憶媒体に保管されているファイルを暗号化されることにより「業務停止」が発生する可能性があります。この際に攻撃者は、元に戻すことと引き換えに金銭などを要求しますが、金銭を支払っても復旧されない可能性があることや、金銭を支払うことで攻撃者が更なる攻撃を行うメリットを与えてしまうことなどから、支払いに応じることは推奨されません。

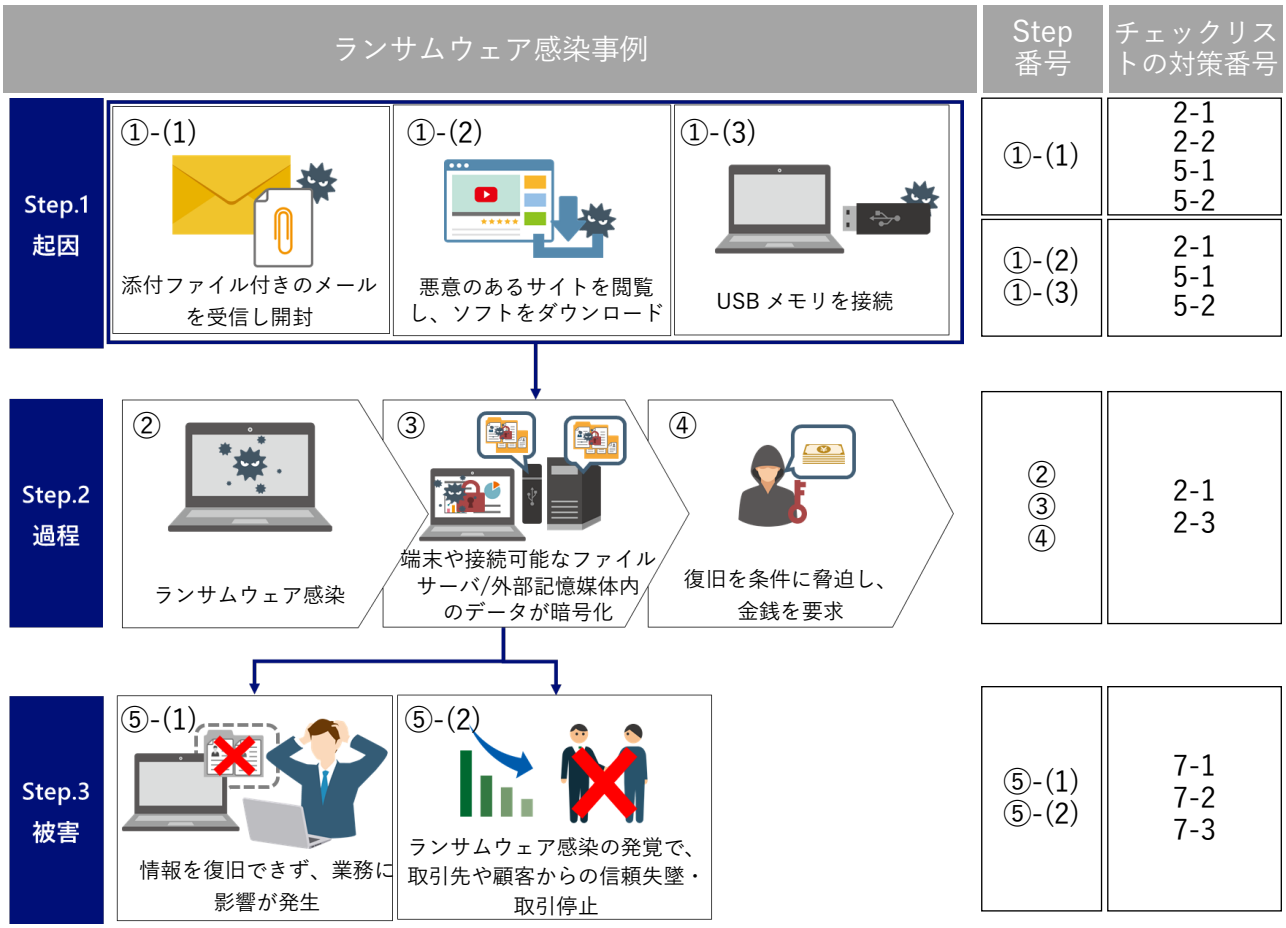
② マルウェア感染の事例

○ 一般的なマルウェア



※攻撃は日々多様化しているため、本事例紹介で掲載している添付ファイルの開封やソフトウェアのダウンロード等の操作を実施しない場合でも、マルウェアに感染する場合があります。

○ ランサムウェアの事例


ランサムウェア感染事例
Step番号
チェックリストの対策番号
Step.1 起因
①-(1)
添付ファイル付きのメールを受信し開封
①-(2)
悪意のあるサイトを閲覧し、ソフトをダウンロード
①-(3)
USB メモリを接続
①-(1)
2-1 2-2 5-1 5-2
①-(2) ①-(3)
2-1 5-1 5-2
Step.2 過程
②
ランサムウェア感染
③
端末や接続可能なファイルサーバ/外部記憶媒体内のデータが暗号化
④
復旧を条件に脅迫し、金銭を要求
② ③ ④
2-1 2-3
Step.3 被害
⑤-(1)
情報を復旧できず、業務に影響が発生
⑤-(2)
ランサムウェア感染の発覚で、取引先や顧客からの信頼失墜・取引停止
⑤-(1) ⑤-(2)
7-1 7-2 7-3

(イ) 脅威の解説　不正アクセス

①　不正アクセスとは

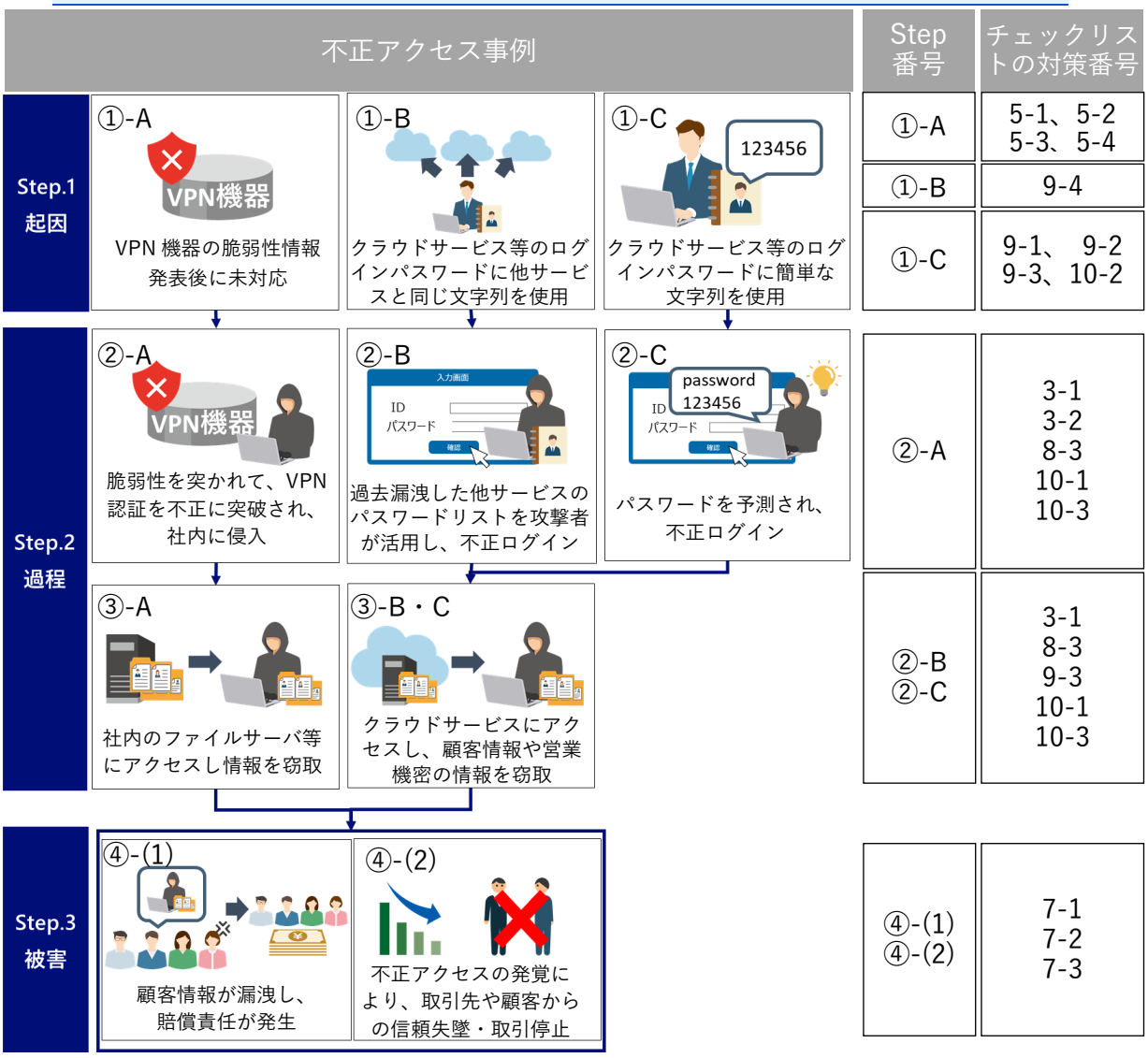
不正アクセスとは、以下のような行為を指します。

・コンピュータの OS やアプリケーションソフトウェア、ハードウェアに存在する脆弱性を悪用し、アクセスする権限を持たない第三者が内部に侵入する行為。

・ID 及びパスワードを利用者の許可を得ずに利用し、利用者に提供されているサービスを受ける行為。

不正アクセスをされた場合、「情報漏洩」の発生や、そちらに伴う「賠償責任」の発生、また、取引先や顧客からの「信頼失墜」や「取引停止」となる可能性があります。

②　不正アクセスの事例



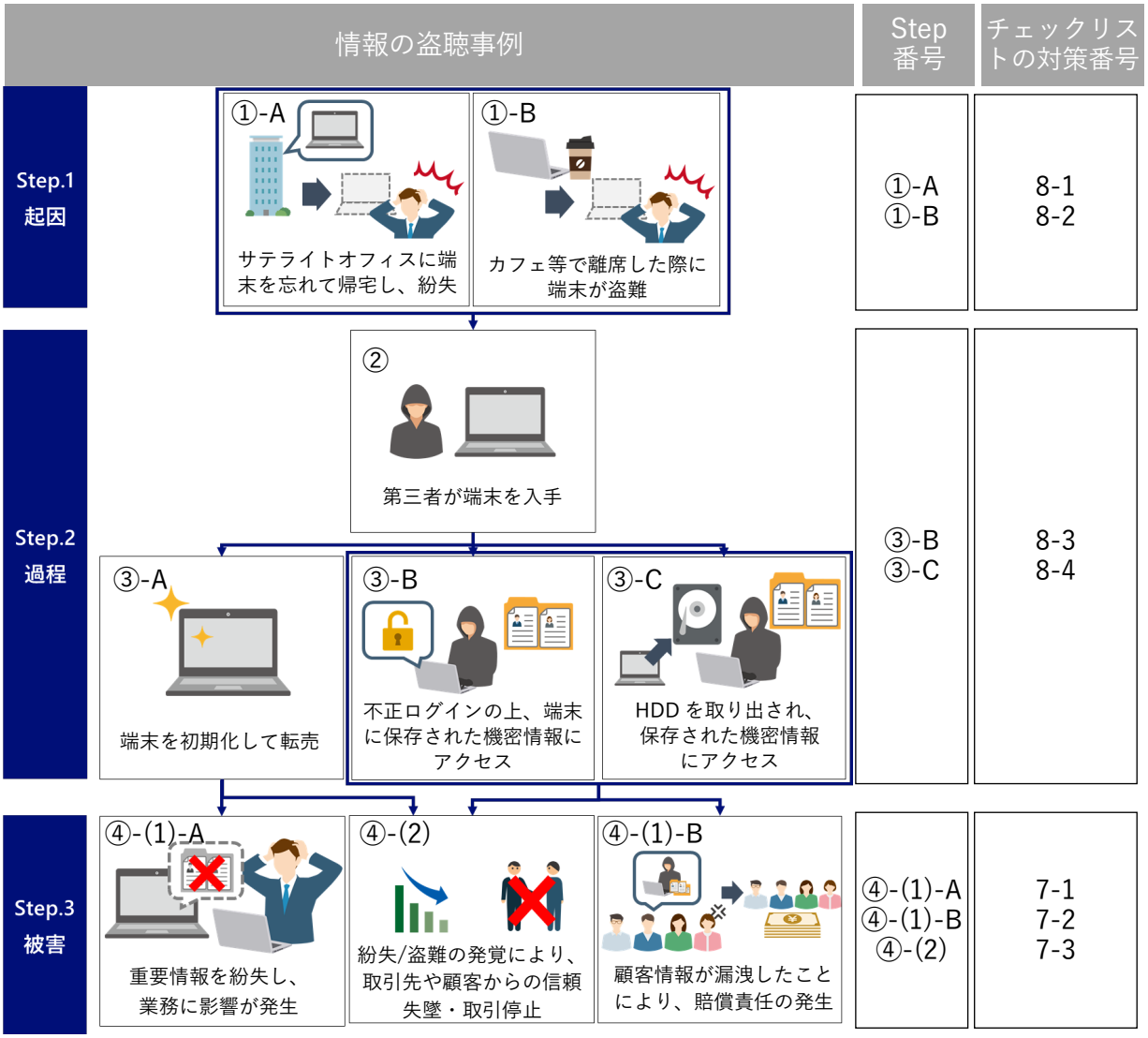
(ウ) 脅威の解説　端末の紛失・盗難

①　端末の紛失・盗難とは

端末など、物理的な機器を第三者に盗まれること、又はなくしてしまうことを指します。

盗難・紛失にあった場合、「情報漏洩」の発生や、それに伴う「賠償責任」の発生、また、取引先や顧客からの「信頼失墜」や「取引停止」となる可能性があります。

②　端末の紛失・盗難の事例



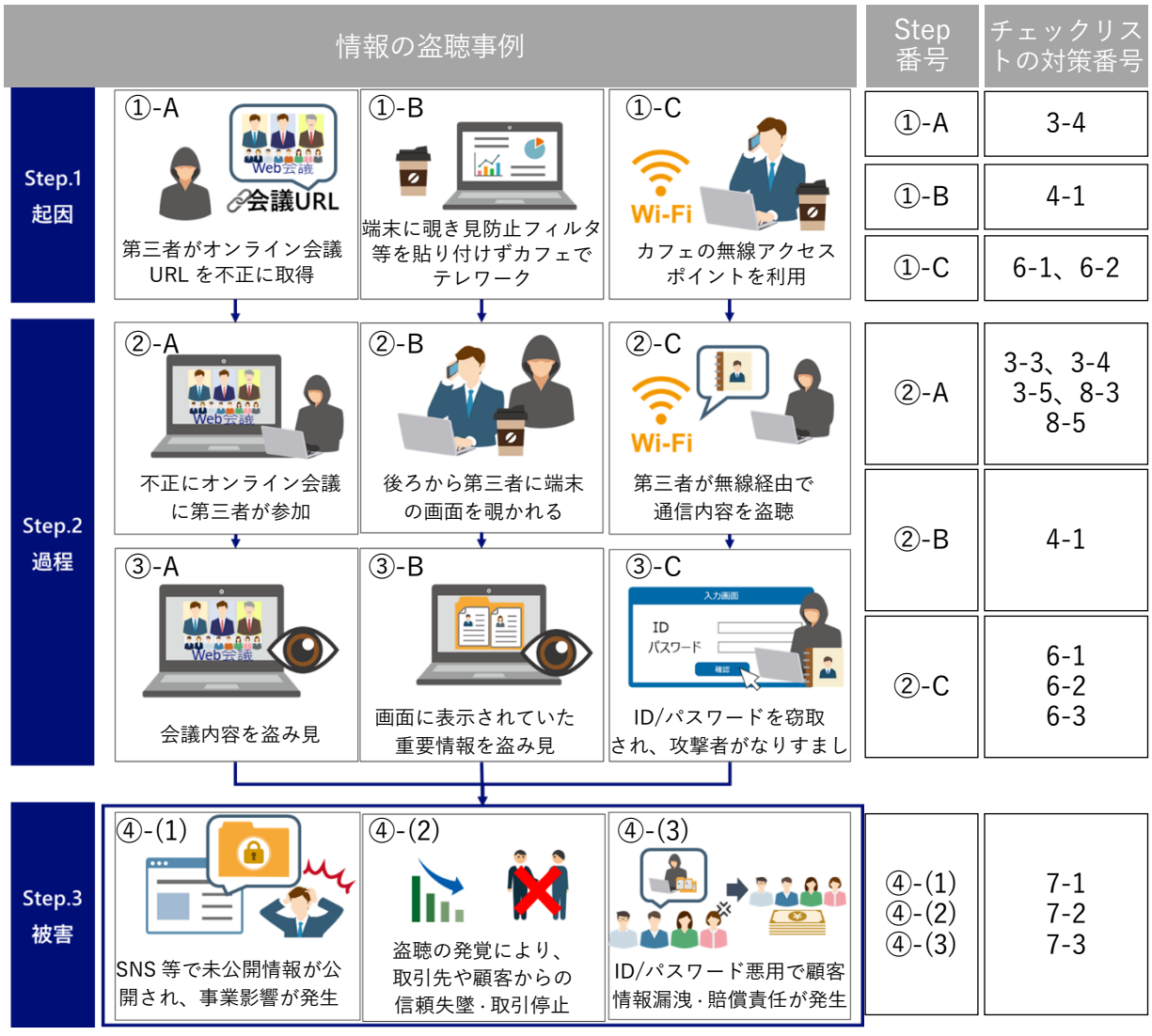
(エ) 脅威の解説　情報の盗聴

①　情報の盗聴とは

ネットワーク上でやり取りされているデータを盗み見られることや、端末を覗き見られることを指します。

情報の盗聴にあった場合、「情報漏洩」の発生や、それに伴う「賠償責任」の発生、また、取引先や顧客からの「信頼失墜」や「取引停止」となる可能性があります。

②　情報の盗聴の事例



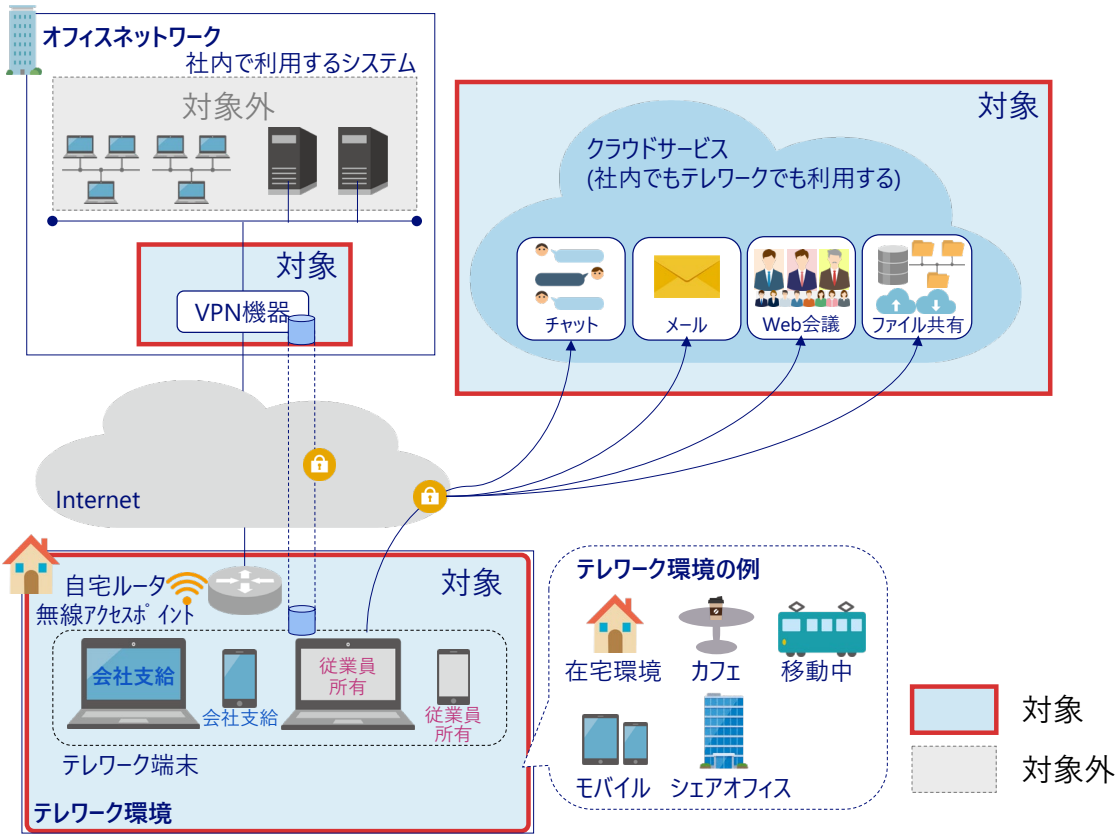
第２部

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

中小企業等の皆様がテレワーク導入や利用を進めるに当たり、テレワーク方式ごとに実施すべきセキュリティ対策を確認できるように、チェックリストとして対策内容を具体的に示しています。また、効率的にセキュリティ対策を進められるように、各対策内容に優先度を付けています。

(ア) セキュリティ対策の対象範囲

チェックリストにおけるセキュリティ対策の対象範囲は、テレワークの導入や利用のために必要となるシステムや機器です。



前ページの図としては、

・テレワーク環境

・クラウドサービス（社内でもテレワークでも利用する環境）

・オフィスネットワークのうち、社外から社内にアクセスするための VPN 機器が対象となります。一方、テレワークの導入有無に関わらず社内で利用するシステム（オフィスネットワーク）等についてはチェックリストの対象範囲としては考慮されていないため、別途セキュリティ対策を検討していていただくことを推奨します。

(イ) 優先度の考え方

各対策内容の優先度を以下の通り定義します。優先度の高い対策から順に着手・実施することを推奨します。

優先度：◎

- セキュリティ重要性が高い（対策実施による効果が高い）、かつ、実施難易度が低い（専門知識、追加コストの観点で懸念が小さい）

優先度：〇

- セキュリティ重要性が高い（対策実施による効果が高い）、かつ、実施難易度が高くない（IT セキュリティに関する知識が必要であるが、実装困難ではない）
- セキュリティ重要性が中程度（対策実施による効果がある程度期待できる）、かつ、対策難易度が低い（専門知識、追加コストの観点で懸念が小さい）

(ウ) セキュリティ対策チェックリスト

①会社支給端末・VPN/リモートデスクトップ方式

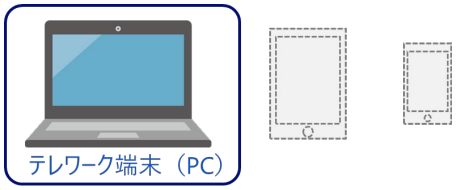
本チェックリスト内で取り扱う用語の中で、「テレワーク端末」については、以下の3つで使い分けを実施しています。

テレワーク端末：

テレワークで利用するPCやスマートデバイス（タブレット端末やスマートフォン）が該当します。

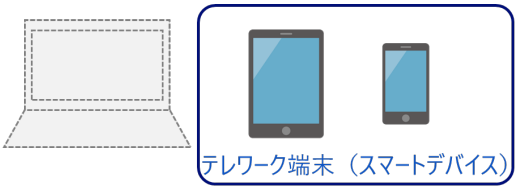
テレワーク端末（PC）：

テレワークで利用するPCが該当します。



テレワーク端末（スマートデバイス）：

テレワークで利用するスマートデバイス（タブレット端末やスマートフォン）が該当します。



◆前提となる対策

No.	対策分類	対策内容	想定脅威
1-1	資産管理	□ 会社で許可したテレワーク端末のみをテレワークに使用しており、使用している端末とその利用者を把握している。	マルウェア感染 不正アクセス 盗難・紛失
1-2	資産管理	□ テレワークで利用しているシステムや取り扱う重要情報※を把握している。 ※ 営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報	不正アクセス 情報の盗聴

※対策分類「資産管理」の対策に関しては、情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策となります。

優先度：◎の項目

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イ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※。またウイ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。 ※ Windows 製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、また iOS 製品で、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）でインストールしたアプリのみを利用している場合は、インストール作業は不要	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
5-2	脆弱性管理	□ テレワーク端末の OS やアプリケーションソフトウェアに対して最新のセキュリティアップデートを適用している。	不正アクセス
5-4	脆弱性管理	□ テレワーク端末から社内にリモートアクセスする際に利用する VPN 機器や、会社端末のリモートデスクトップアプリケーション等について、メーカーサポート切れの製品は利用せず、最新のセキュリティアップデートを適用している。	不正アクセス
7-1	インシデント対応・管理	□ 情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や懸念がある状況（不審なメールを開封した場合等）における対応方針を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-1	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に端末の位置情報を検出できるようにしている。	盗難・紛失
9-1	認証	□ テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス
9-2	認証	□ テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス

◆優先度：〇の項目

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
3-3	アクセス制御（論理）	□ オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-4	アクセス制御（論理）	□ オンライン会議にアクセスするための URL や会議参加のパスワードを不要なメンバーに伝えないようにしている。また会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-5	アクセス制御（論理）	□ オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
5-3	脆弱性管理	□ テレワークで利用する自宅の Wi-Fi ルーターやモバイル Wi-Fi 等は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス
6-1	通信暗号化	□ テレワークでクラウドサービス（Web メール、チャット、オンライン会議、クラウドストレージ等）を利用する場合は、HTTPS 通信でかつ、接続先の URL が正しいことを確認している。（クラウドサービスを利用していない場合は対象外）	情報の盗聴
6-2	通信暗号化	□ クラウドサービスに接続する際や、ID・パスワード等の情報を入力するサービスに接続する際には、暗号化されている HTTPS 通信であることを確認してから使用している。	情報の盗聴
6-3	通信暗号化	□ 自宅の Wi-Fi ルーター等の機器を利用する場合は、Wi-Fi のセキュリティ方式として「WPA2」を利用して、パスワードは第三者に推測されにくいものを利用している。	情報の盗聴
7-2	インシデント対応・管理	□ テレワーク端末とアクセス先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴

No.	対策分類	対策内容	想定脅威
7-3	インシデント対応・管理	□ テレワーク端末から社内システムにアクセスする際のアクセスログを収集している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-2	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に MDM※等を導入し、リモートからのデータの消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用している。 ※ Mobile Device Management の略称で、スマートフォン等のスマートデバイスを一元的に管理・運用すること、又はその機能を提供するソフトウェア	盗難・紛失
8-3	データ保護	□ テレワーク端末の盗難・紛失時に情報が漏えいしないように、ハードディスクやフラッシュメモリ※等の内蔵された記憶媒体の暗号化を実施している※※。（端末に会社のデータを保管しない場合は対象外） ※ ハードディスクとは異なる記憶媒体の一つで、「不揮発性の半導体メモリ」をさす。電源をおとしてもデータを保持することが可能な記憶媒体 ※※ iOS 製品については初期状態で暗号化されているため対応不要	盗難・紛失
8-4	データ保護	□ テレワーク端末には原則として重要情報を保管しておらず、もし重要情報を保管しなければならない場合※には、ファイルの暗号化（パスワード設定等）を実施している。（端末に会社のデータを保管しない場合は対象外） ※ テレワーク端末のローカルにファイル保存するケースであり、ファイルサーバやクラウドストレージ、各種クラウドサービスのシステム内に保存するケースは対象外	不正アクセス 盗難・紛失
8-5	データ保護	□ オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。 上記のルールを強制することが可能な場合は、強制するように設定する。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
9-3	認証	□ テレワーク端末やテレワークで利用する各システムのアカウントが一定回数以上パスワードを誤入力した場合、パスワード入力ができなくなるように制限している。	不正アクセス
9-4	認証	□ テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定している。	不正アクセス
10-1	特権管理	□ テレワーク端末やテレワークで利用する各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス
10-2	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス
10-3	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用している。	不正アクセス

② 会社支給端末・会社非接続（クラウドサービス型）

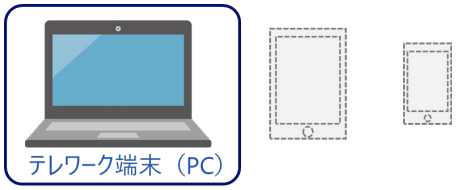
本チェックリスト内で取り扱う用語の中で、「テレワーク端末」については、以下の3つで使い分けを実施しています。

テレワーク端末：

テレワークで利用するPCやスマートデバイス（タブレット端末やスマートフォン）が該当します。

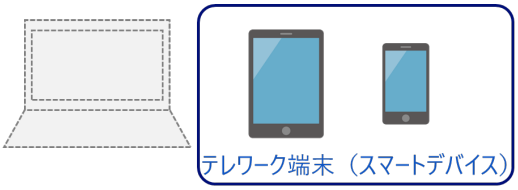
テレワーク端末（PC）：

テレワークで利用するPCが該当します。



テレワーク端末（スマートデバイス）：

テレワークで利用するスマートデバイス（タブレット端末やスマートフォン）が該当します。



◆前提となる対策

No.	対策分類	対策内容	想定脅威
1-1	資産管理	□ 会社で許可したテレワーク端末のみをテレワークに使用しており、使用している端末とその利用者を把握している。	マルウェア感染 不正アクセス 盗難・紛失
1-2	資産管理	□ テレワークで利用しているシステムや取り扱う重要情報※を把握している。 ※ 営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報	不正アクセス 情報の盗聴

※対策分類「資産管理」の対策に関しては、情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策となります。

優先度：◎の項目

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イ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※。またウイ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。 ※ Windows 製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、また iOS 製品で、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）でインストールしたアプリのみを利用している場合は、インストール作業は不要	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
5-2	脆弱性管理	□ テレワーク端末の OS やアプリケーションソフトウェアに対して最新のセキュリティアップデートを適用している。	不正アクセス
7-1	インシデント対応・管理	□ 情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や懸念がある状況（不審なメールを開封した場合等）における対応方針を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-1	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に端末の位置情報を検出できるようにしている。	盗難・紛失
9-1	認証	□ テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス
9-2	認証	□ テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス

◆優先度：〇の項目

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
3-3	アクセス制御（論理）	□ オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-4	アクセス制御（論理）	□ オンライン会議にアクセスするための URL や会議参加のパスワードを不要なメンバーに伝えないようにしている。また会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-5	アクセス制御（論理）	□ オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
5-3	脆弱性管理	□ テレワークで利用する自宅の Wi-Fi ルーターやモバイル Wi-Fi 等は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス
6-1	通信暗号化	□ テレワークでクラウドサービス（Web メール、チャット、オンライン会議、クラウドストレージ等）を利用する場合は、HTTPS 通信でかつ、接続先の URL が正しいことを確認している。（クラウドサービスを利用していない場合は対象外）	情報の盗聴
6-2	通信暗号化	□ クラウドサービスに接続する際や、ID・パスワード等の情報を入力するサービスに接続する際には、暗号化されている HTTPS 通信であることを確認してから使用している。	情報の盗聴
6-3	通信暗号化	□ 自宅の Wi-Fi ルーター等の機器を利用する場合は、Wi-Fi のセキュリティ方式として「WPA2」を利用して、パスワードは第三者に推測されにくいものを利用している。	情報の盗聴
7-2	インシデント対応・管理	□ テレワーク端末とアクセス先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴

No.	対策分類	対策内容	想定脅威
8-2	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に MDM※等を導入し、リモートからのデータの消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用している。 ※ Mobile Device Management の略称で、スマートフォン等のスマートデバイスを一元的に管理・運用すること、又はその機能を提供するソフトウェア	盗難・紛失
8-3	データ保護	□ テレワーク端末の盗難・紛失時に情報が漏えいしないように、ハードディスクやフラッシュメモリ※等の内蔵された記憶媒体の暗号化を実施している※※。（端末に会社のデータを保管しない場合は対象外） ※ ハードディスクとは異なる記憶媒体の一つで、「不揮発性の半導体メモリ」をさす。電源をおとしてもデータを保持することが可能な記憶媒体 ※※ iOS 製品については初期状態で暗号化されているため対応不要	盗難・紛失
8-4	データ保護	□ テレワーク端末には原則として重要情報を保管しておらず、もし重要情報を保管しなければならない場合※には、ファイルの暗号化（パスワード設定等）を実施している。（端末に会社のデータを保管しない場合は対象外） ※ テレワーク端末のローカルにファイル保存するケースであり、ファイルサーバやクラウドストレージ、各種クラウドサービスのシステム内に保存するケースは対象外	不正アクセス 盗難・紛失
8-5	データ保護	□ オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。 上記のルールを強制することが可能な場合は、強制するように設定する。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
9-3	認証	□ テレワーク端末やテレワークで利用する各システムのアカウントが一定回数以上パスワードを誤入力した場合、パスワード入力ができなくなるように制限している。	不正アクセス
9-4	認証	□ テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定している。	不正アクセス
10-1	特権管理	□ テレワーク端末やテレワークで利用する各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス
10-2	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス
10-3	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用している。	不正アクセス

③ 会社支給端末・会社非接続方式（手元作業型）

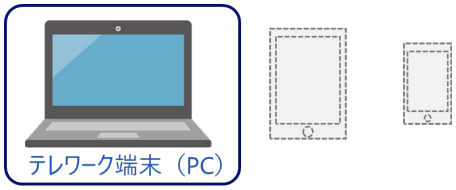
本チェックリスト内で取り扱う用語の中で、「テレワーク端末」については、以下の3つで使い分けを実施しています。

テレワーク端末：

テレワークで利用するPCやスマートデバイス（タブレット端末やスマートフォン）が該当します。

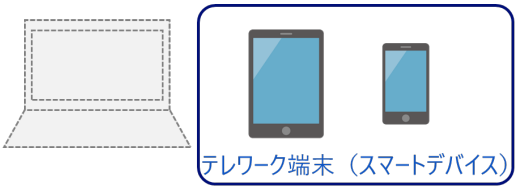
テレワーク端末（PC）：

テレワークで利用するPCが該当します。



テレワーク端末（スマートデバイス）：

テレワークで利用するスマートデバイス（タブレット端末やスマートフォン）が該当します。



◆前提となる対策

No.	対策分類	対策内容	想定脅威
1-1	資産管理	□ 会社で許可したテレワーク端末のみをテレワークに使用しており、使用している端末とその利用者を把握している。	マルウェア感染 不正アクセス 盗難・紛失
1-2	資産管理	□ テレワークで利用しているシステムや取り扱う重要情報※を把握している。 ※ 営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報	不正アクセス 情報の盗聴

※対策分類「資産管理」の対策に関しては、情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策となります。

優先度：◎の項目

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イ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※。またウイ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。 ※ Windows 製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、また iOS 製品で、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）でインストールしたアプリのみを利用している場合は、インストール作業は不要	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
5-2	脆弱性管理	□ テレワーク端末の OS やアプリケーションソフトウェアに対して最新のセキュリティアップデートを適用している。	不正アクセス
7-1	インシデント対応・管理	□ 情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や懸念がある状況（不審なメールを開封した場合等）における対応方針を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-1	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に端末の位置情報を検出できるようにしている。	盗難・紛失
9-1	認証	□ テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス
9-2	認証	□ テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス

◆優先度：〇の項目

No.	対策分類	対策内容	想定脅威
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
5-3	脆弱性管理	□ テレワークで利用する自宅の Wi-Fi ルーターやモバイル Wi-Fi 等は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス
6-2	通信暗号化	□ クラウドサービスに接続する際や、ID・パスワード等の情報を入力するサービスに接続する際には、暗号化されている HTTPS 通信であることを確認してから使用している。	情報の盗聴
6-3	通信暗号化	□ 自宅に設置している Wi-Fi ルーター等の機器を利用する場合は、Wi-Fi のセキュリティ方式として「WPA2」を利用して、パスワードは第三者に推測されにくいものを利用している。	情報の盗聴
7-2	インシデント対応・管理	□ テレワーク端末とアクセス先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-2	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に MDM※等を導入し、リモートからのデータの消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用している。 ※ Mobile Device Management の略称で、スマートフォン等のスマートデバイスを一元的に管理・運用すること、又はその機能を提供するソフトウェア	盗難・紛失
8-3	データ保護	□ テレワーク端末の盗難・紛失時に情報が漏えいしないように、ハードディスクやフラッシュメモリ※等の内蔵された記憶媒体の暗号化を実施している※※。（端末に会社のデータを保管しない場合は対象外） ※ ハードディスクとは異なる記憶媒体の一つで、「不揮発性の半導体メモリ」をさす。電源をおとしてもデータを保持することが可能な記憶媒体 ※※ iOS 製品については初期状態で暗号化されているため対応不要	盗難・紛失
8-4	データ保護	□ テレワーク端末には原則として重要情報を保管しておらず、もし重要情報を保管しなければならない場合※には、ファイルの暗号化（パスワード設定等）を実施している。（端末に会社のデータを保管しない場合は対象外） ※ テレワーク端末のローカルにファイル保存するケースであり、ファイルサーバやクラウドストレージ、各種クラウドサービスのシステム内に保存するケースは対象外	不正アクセス 盗難・紛失
9-3	認証	□ テレワークで利用する端末や各システムのアカウントが一定回数以上パスワードを誤入力した場合パスワード入力できないように制限している。	不正アクセス

No.	対策分類	対策内容	想定脅威
9-4	認証	□ テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定する。	不正アクセス
10-1	特権管理	□ テレワークで利用する端末や各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス
10-2	特権管理	□ テレワークで利用する端末や各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス
10-3	特権管理	□ テレワークで利用する端末や各システムの管理者権限は必要な作業時のみ利用している。	不正アクセス

④ 会社支給端末・セキュアブラウザ方式

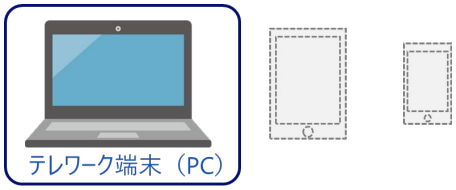
本チェックリスト内で取り扱う用語の中で、「テレワーク端末」については、以下の3つで使い分けを実施しています。

テレワーク端末：

テレワークで利用するPCやスマートデバイス（タブレット端末やスマートフォン）が該当します。

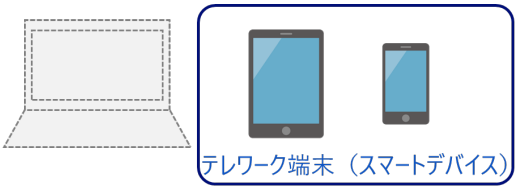
テレワーク端末（PC）：

テレワークで利用するPCが該当します。



テレワーク端末（スマートデバイス）：

テレワークで利用するスマートデバイス（タブレット端末やスマートフォン）が該当します。



◆前提となる対策

No.	対策分類	対策内容	想定脅威
1-1	資産管理	□ 会社で許可したテレワーク端末のみをテレワークに使用しており、使用している端末とその利用者を把握している。	マルウェア感染 不正アクセス 盗難・紛失
1-2	資産管理	□ テレワークで利用しているシステムや取り扱う重要情報※を把握している。 ※ 営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報	不正アクセス 情報の盗聴

※対策分類「資産管理」の対策に関しては、情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策となります。

優先度：◎の項目

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イ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※。またウイ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。 ※ Windows 製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、また iOS 製品で、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）でインストールしたアプリのみを利用している場合は、インストール作業は不要	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
5-2	脆弱性管理	□ テレワーク端末の OS やアプリケーションソフトウェアに対して最新のセキュリティアップデートを適用している。	不正アクセス
7-1	インシデント対応・管理	□ 情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や懸念がある状況（不審なメールを開封した場合等）における対応方針を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-1	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に端末の位置情報を検出できるようにしている。	盗難・紛失
9-1	認証	□ テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス
9-2	認証	□ テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス

◆優先度：〇の項目

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
3-3	アクセス制御（論理）	□ オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-4	アクセス制御（論理）	□ オンライン会議にアクセスするための URL や会議参加のパスワードを不要なメンバーに伝えないようにしている。また会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-5	アクセス制御（論理）	□ オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
5-3	脆弱性管理	□ テレワークで利用する自宅の Wi-Fi ルーターやモバイル Wi-Fi 等は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス
6-1	通信暗号化	□ テレワークでクラウドサービス（Web メール、チャット、オンライン会議、クラウドストレージ等）を利用する場合は、HTTPS 通信でかつ、接続先の URL が正しいことを確認している。（クラウドサービスを利用していない場合は対象外）	情報の盗聴
6-2	通信暗号化	□ クラウドサービスに接続する際や、ID・パスワード等の情報を入力するサービスに接続する際には、暗号化されている HTTPS 通信であることを確認してから使用している。	情報の盗聴
6-3	通信暗号化	□ 自宅の Wi-Fi ルーター等の機器を利用する場合は、Wi-Fi のセキュリティ方式として「WPA2」を利用して、パスワードは第三者に推測されにくいものを利用している。	情報の盗聴

No.	対策分類	対策内容	想定脅威
7-2	インシデント対応・管理	□ テレワーク端末とアクセス先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
7-3	インシデント対応・管理	□ テレワーク端末から社内システムにアクセスする際のアクセスログを収集している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-2	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に MDM※等を導入し、リモートからのデータの消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用している。 ※ Mobile Device Management の略称で、スマートフォン等のスマートデバイスを一元的に管理・運用すること、又はその機能を提供するソフトウェア	盗難・紛失
8-5	データ保護	□ オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。 上記のルールを強制することが可能な場合は、強制するように設定する。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
9-3	認証	□ テレワーク端末やテレワークで利用する各システムのアカウントが一定回数以上パスワードを誤入力した場合、パスワード入力ができなくなるように制限している。	不正アクセス
9-4	認証	□ テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定している。	不正アクセス
10-1	特権管理	□ テレワーク端末やテレワークで利用する各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス
10-2	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス
10-3	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用している。	不正アクセス

⑤ 従業員所有端末・VPN/リモートデスクトップ方式

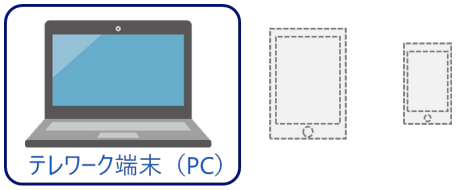
本チェックリスト内で取り扱う用語の中で、「テレワーク端末」については、以下の3つで使い分けを実施しています。

テレワーク端末：

テレワークで利用するPCやスマートデバイス（タブレット端末やスマートフォン）が該当します。

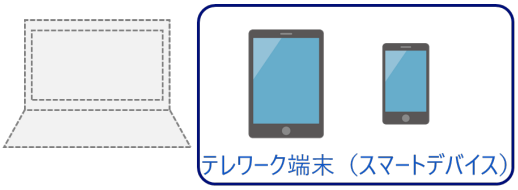
テレワーク端末（PC）：

テレワークで利用するPCが該当します。



テレワーク端末（スマートデバイス）：

テレワークで利用するスマートデバイス（タブレット端末やスマートフォン）が該当します。



◆前提となる対策

No.	対策分類	対策内容	想定脅威
1-1	資産管理	□ 会社で許可したテレワーク端末のみをテレワークに使用しており、使用している端末とその利用者を把握している。	マルウェア感染 不正アクセス 盗難・紛失
1-2	資産管理	□ テレワークで利用しているシステムや取り扱う重要情報※を把握している。 ※ 営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報	不正アクセス 情報の盗聴

※対策分類「資産管理」の対策に関しては、情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策となります。

優先度：◎の項目

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イ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※。またウイ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。 ※ Windows 製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、また iOS 製品で、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）でインストールしたアプリのみを利用している場合は、インストール作業は不要	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
5-2	脆弱性管理	□ テレワーク端末の OS やアプリケーションソフトウェアに対して最新のセキュリティアップデートを適用している。	不正アクセス
5-4	脆弱性管理	□ テレワーク端末から社内にリモートアクセスする際に利用する VPN 機器や、会社端末のリモートデスクトップアプリケーション等について、メーカーサポート切れの製品は利用せず、最新のセキュリティアップデートを適用している。	不正アクセス
7-1	インシデント対応・管理	□ 情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や懸念がある状況（不審なメールを開封した場合等）における対応方針を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-1	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に端末の位置情報を検出できるようにしている。	盗難・紛失
9-1	認証	□ テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス
9-2	認証	□ テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス

◆優先度：〇の項目

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
3-3	アクセス制御（論理）	□ オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-4	アクセス制御（論理）	□ オンライン会議にアクセスするための URL や会議参加のパスワードを不要なメンバーには伝えないようにしている。また会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-5	アクセス制御（論理）	□ オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
5-3	脆弱性管理	□ テレワークで利用する自宅の Wi-Fi ルーターやモバイル Wi-Fi 等は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス
6-1	通信暗号化	□ テレワークでクラウドサービス（Web メール、チャット、オンライン会議、クラウドストレージ等）を利用する場合は、HTTPS 通信でかつ、接続先の URL が正しいことを確認している。（クラウドサービスを利用していない場合は対象外）	情報の盗聴
6-2	通信暗号化	□ クラウドサービスに接続する際や、ID・パスワード等の情報を入力するサービスに接続する際には、暗号化されている HTTPS 通信であることを確認してから使用している。	情報の盗聴
6-3	通信暗号化	□ 自宅の Wi-Fi ルーター等の機器を利用する場合は、Wi-Fi のセキュリティ方式として「WPA2」を利用して、パスワードは第三者に推測されにくいものを利用している。	情報の盗聴

No.	対策分類	対策内容	想定脅威
7-2	インシデント対応・管理	□ テレワーク端末とアクセス先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
7-3	インシデント対応・管理	□ テレワーク端末から社内システムにアクセスする際のアクセスログを収集している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-2	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に MDM※等を導入し、リモートからのデータの消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用している。 ※ Mobile Device Management の略称で、スマートフォン等のスマートデバイスを一元的に管理・運用すること、又はその機能を提供するソフトウェア	盗難・紛失
8-3	データ保護	□ テレワーク端末の盗難・紛失時に情報が漏えいしないように、ハードディスクやフラッシュメモリ※等の内蔵された記憶媒体の暗号化を実施している※※。（端末に会社のデータを保管しない場合は対象外） ※ ハードディスクとは異なる記憶媒体の一つで、「不揮発性の半導体メモリ」をさす。電源をおとしてもデータを保持することが可能な記憶媒体 ※※ iOS 製品については初期状態で暗号化されているため対応不要	盗難・紛失
8-4	データ保護	□ テレワーク端末には原則として重要情報を保管しておらず、もし重要情報を保管しなければならない場合※には、ファイルの暗号化（パスワード設定等）を実施している。（端末に会社のデータを保管しない場合は対象外） ※ テレワーク端末のローカルにファイル保存するケースであり、ファイルサーバやクラウドストレージ、各種クラウドサービスのシステム内に保存するケースは対象外	不正アクセス 盗難・紛失
8-5	データ保護	□ オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。 上記のルールを強制することが可能な場合は、強制するように設定する。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
9-4	認証	□ テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定している。	不正アクセス
10-1	特権管理	□ テレワーク端末やテレワークで利用する各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス
10-2	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス

⑥ 従業員所有端末・会社非接続方式（クラウドサービス型）

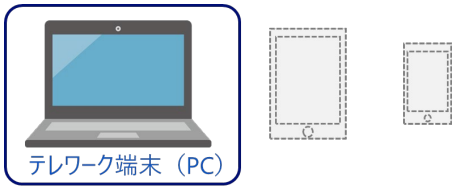
本チェックリスト内で取り扱う用語の中で、「テレワーク端末」については、以下の3つで使い分けを実施しています。

テレワーク端末：

テレワークで利用するPCやスマートデバイス（タブレット端末やスマートフォン）が該当します。

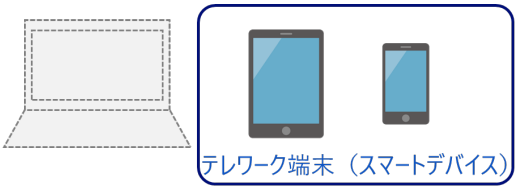
テレワーク端末（PC）：

テレワークで利用するPCが該当します。



テレワーク端末（スマートデバイス）：

テレワークで利用するスマートデバイス（タブレット端末やスマートフォン）が該当します。



◆前提となる対策

No.	対策分類	対策内容	想定脅威
1-1	資産管理	□ 会社で許可したテレワーク端末のみをテレワークに使用しており、使用している端末とその利用者を把握している。	マルウェア感染 不正アクセス 盗難・紛失
1-2	資産管理	□ テレワークで利用しているシステムや取り扱う重要情報※を把握している。 ※ 営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報	不正アクセス 情報の盗聴

※対策分類「資産管理」の対策に関しては、情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策となります。

優先度：◎の項目

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イ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※。またウイ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。 ※ Windows 製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、また iOS 製品で、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）でインストールしたアプリのみを利用している場合は、インストール作業は不要	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
5-2	脆弱性管理	□ テレワーク端末の OS やアプリケーションソフトウェアに対して最新のセキュリティアップデートを適用している。	不正アクセス
7-1	インシデント対応・管理	□ 情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や懸念がある状況（不審なメールを開封した場合等）における対応方針を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-1	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に端末の位置情報を検出できるようにしている。	盗難・紛失
9-1	認証	□ テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス
9-2	認証	□ テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス

◆優先度：〇の項目

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
3-3	アクセス制御（論理）	□ オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。	情報の盗聴
3-4	アクセス制御（論理）	□ オンライン会議にアクセスするための URL や会議参加のパスワードを不要なメンバーに伝えないようにしている。また会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-5	アクセス制御（論理）	□ オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。	情報の盗聴
5-3	脆弱性管理	□ テレワークで利用する自宅の Wi-Fi ルーターやモバイル Wi-Fi 等は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス
6-1	通信暗号化	□ テレワークでクラウドサービス（Web メール、チャット、オンライン会議、クラウドストレージ等）を利用する場合は、HTTPS 通信でかつ、接続先の URL が正しいことを確認している。（クラウドサービスを利用していない場合は対象外）	情報の盗聴
6-2	通信暗号化	□ クラウドサービスに接続する際や、ID・パスワード等の情報を入力するサービスに接続する際には、暗号化されている HTTPS 通信であることを確認してから使用している。	情報の盗聴
6-3	通信暗号化	□ 自宅の Wi-Fi ルーター等の機器を利用する場合は、Wi-Fi のセキュリティ方式として「WPA2」を利用して、パスワードは第三者に推測されにくいものを利用している。	情報の盗聴
7-2	インシデント対応・管理	□ テレワーク端末とアクセス先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴

No.	対策分類	対策内容	想定脅威
8-2	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に MDM※等を導入し、リモートからのデータの消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用している。 ※ Mobile Device Management の略称で、スマートフォン等のスマートデバイスを一元的に管理・運用すること、又はその機能を提供するソフトウェア	盗難・紛失
8-3	データ保護	□ テレワーク端末の盗難・紛失時に情報が漏えいしないように、ハードディスクやフラッシュメモリ※等の内蔵された記憶媒体の暗号化を実施している※※。（端末に会社のデータを保管しない場合は対象外） ※ ハードディスクとは異なる記憶媒体の一つで、「不揮発性の半導体メモリ」をさす。電源をおとしてもデータを保持することが可能な記憶媒体 ※※ iOS 製品については初期状態で暗号化されているため対応不要	盗難・紛失
8-4	データ保護	□ テレワーク端末には原則として重要情報を保管しておらず、もし重要情報を保管しなければならない場合※には、ファイルの暗号化（パスワード設定等）を実施している。（端末に会社のデータを保管しない場合は対象外） ※ テレワーク端末のローカルにファイル保存するケースであり、ファイルサーバやクラウドストレージ、各種クラウドサービスのシステム内に保存するケースは対象外	不正アクセス 盗難・紛失
8-5	データ保護	□ オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。 上記のルールを強制することが可能な場合は、強制するように設定する。	情報の盗聴
9-4	認証	□ テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定している。	不正アクセス
10-1	特権管理	□ テレワーク端末やテレワークで利用する各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス
10-2	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス

⑦ 従業員所有端末・会社非接続方式（手元作業型）

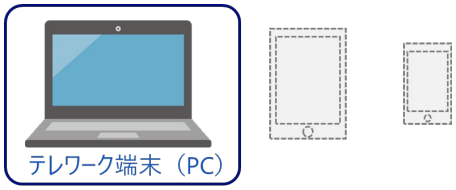
本チェックリスト内で取り扱う用語の中で、「テレワーク端末」については、以下の3つで使い分けを実施しています。

テレワーク端末：

テレワークで利用するPCやスマートデバイス（タブレット端末やスマートフォン）が該当します。

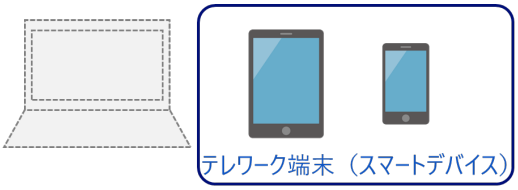
テレワーク端末（PC）：

テレワークで利用するPCが該当します。



テレワーク端末（スマートデバイス）：

テレワークで利用するスマートデバイス（タブレット端末やスマートフォン）が該当します。



◆前提となる対策

No.	対策分類	対策内容	想定脅威
1-1	資産管理	□ 会社で許可したテレワーク端末のみをテレワークに使用しており、使用している端末とその利用者を把握している。	マルウェア感染 不正アクセス 盗難・紛失
1-2	資産管理	□ テレワークで利用しているシステムや取り扱う重要情報※を把握している。 ※ 営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報	不正アクセス 情報の盗聴

※対策分類「資産管理」の対策に関しては、情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策となります。

優先度：◎の項目

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イ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※。またウイ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。 ※ Windows 製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、また iOS 製品で、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）でインストールしたアプリのみを利用している場合は、インストール作業は不要	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
5-2	脆弱性管理	□ テレワーク端末の OS やアプリケーションソフトウェアに対して最新のセキュリティアップデートを適用している。	不正アクセス
7-1	インシデント対応・管理	□ 情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や懸念がある状況（不審なメールを開封した場合等）における対応方針を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-1	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に端末の位置情報を検出できるようにしている。	盗難・紛失
9-1	認証	□ テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス
9-2	認証	□ テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス

◆優先度：〇の項目

No.	対策分類	対策内容	想定脅威
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
5-3	脆弱性管理	□ テレワークで利用する自宅の Wi-Fi ルーターやモバイル Wi-Fi 等は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス
6-2	通信暗号化	□ クラウドサービスに接続する際や、ID・パスワード等の情報を入力するサービスに接続する際には、暗号化されている HTTPS 通信であることを確認してから使用している。	情報の盗聴
6-3	通信暗号化	□ 自宅の Wi-Fi ルーター等の機器を利用する場合は、Wi-Fi のセキュリティ方式として「WPA2」を利用して、パスワードは第三者に推測されにくいものを利用している。	情報の盗聴
7-2	インシデント対応・管理	□ テレワーク端末とアクセス先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-3	データ保護	□ テレワーク端末の盗難・紛失時に情報が漏えいしないように、ハードディスクやフラッシュメモリ※等の内蔵された記憶媒体の暗号化を実施している※※。（端末に会社のデータを保管しない場合は対象外） ※　ハードディスクとは異なる記憶媒体の一つで、「不揮発性の半導体メモリ」をさす。電源をおとしてもデータを保持することが可能な記憶媒体 ※※　iOS 製品については初期状態で暗号化されているため対応不要	盗難・紛失
8-4	データ保護	□ テレワーク端末には原則として重要情報を保管しておらず、もし重要情報を保管しなければならない場合※には、ファイルの暗号化（パスワード設定等）を実施している。（端末に会社のデータを保管しない場合は対象外） ※　テレワーク端末のローカルにファイル保存するケースであり、ファイルサーバやクラウドストレージ、各種クラウドサービスのシステム内に保存するケースは対象外	不正アクセス 盗難・紛失
8-5	データ保護	□ オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。 上記のルールを強制することが可能な場合は、強制するように設定する。	情報の盗聴
9-4	認証	□ テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定している。	不正アクセス
10-1	特権管理	□ テレワーク端末やテレワークで利用する各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス
10-2	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス

⑧ 従業員所有端末・セキュアブラウザ方式

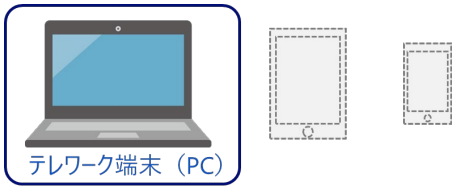
本チェックリスト内で取り扱う用語の中で、「テレワーク端末」については、以下の3つで使い分けを実施しています。

テレワーク端末：

テレワークで利用するPCやスマートデバイス（タブレット端末やスマートフォン）が該当します。

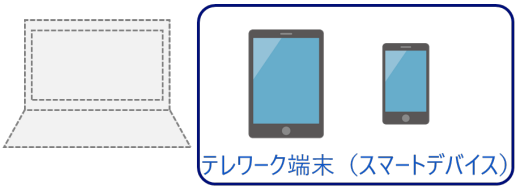
テレワーク端末（PC）：

テレワークで利用するPCが該当します。



テレワーク端末（スマートデバイス）：

テレワークで利用するスマートデバイス（タブレット端末やスマートフォン）が該当します。



◆前提となる対策

No.	対策分類	対策内容	想定脅威
1-1	資産管理	□ 会社で許可したテレワーク端末のみをテレワークに使用しており、使用している端末とその利用者を把握している。	マルウェア感染 不正アクセス 盗難・紛失
1-2	資産管理	□ テレワークで利用しているシステムや取り扱う重要情報※を把握している。 ※ 営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報	不正アクセス 情報の盗聴

※対策分類「資産管理」の対策に関しては、情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策となります。

優先度：◎の項目

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イ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※。またウイ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。 ※ Windows 製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、また iOS 製品で、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）でインストールしたアプリのみを利用している場合は、インストール作業は不要	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
5-2	脆弱性管理	□ テレワーク端末の OS やアプリケーションソフトウェアに対して最新のセキュリティアップデートを適用している。	不正アクセス
7-1	インシデント対応・管理	□ 情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や懸念がある状況（不審なメールを開封した場合等）における対応方針を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-1	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に端末の位置情報を検出できるようにしている。	盗難・紛失
9-1	認証	□ テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス
9-2	認証	□ テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス

◆優先度：〇の項目

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
3-3	アクセス制御（論理）	□ オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-4	アクセス制御（論理）	□ オンライン会議にアクセスするための URL や会議参加のパスワードを不要なメンバーに伝えないようにしている。また会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
3-5	アクセス制御（論理）	□ オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
5-3	脆弱性管理	□ テレワークで利用する自宅の Wi-Fi ルーターやモバイル Wi-Fi 等は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス
6-1	通信暗号化	□ テレワークでクラウドサービス（Web メール、チャット、オンライン会議、クラウドストレージ等）を利用する場合は、HTTPS 通信でかつ、接続先の URL が正しいことを確認している。（クラウドサービスを利用していない場合は対象外）	情報の盗聴
6-2	通信暗号化	□ クラウドサービスに接続する際や、ID・パスワード等の情報を入力するサービスに接続する際には、暗号化されている HTTPS 通信であることを確認してから使用している。	情報の盗聴
6-3	通信暗号化	□ 自宅の Wi-Fi ルーター等の機器を利用する場合は、Wi-Fi のセキュリティ方式として「WPA2」を利用して、パスワードは第三者に推測されにくいものを利用している。	情報の盗聴

No.	対策分類	対策内容	想定脅威
7-2	インシデント対応・管理	□ テレワーク端末とアクセス先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
7-3	インシデント対応・管理	□ テレワーク端末から社内システムにアクセスする際のアクセスログを収集している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴
8-2	データ保護	□ テレワーク端末（スマートデバイス）の紛失時に MDM※等を導入し、リモートからのデータの消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用している。 ※ Mobile Device Management の略称で、スマートフォン等のスマートデバイスを一元的に管理・運用すること、又はその機能を提供するソフトウェア	盗難・紛失
8-5	データ保護	□ オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。 上記のルールを強制することが可能な場合は、強制するように設定する。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴
9-4	認証	□ テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定している。	不正アクセス
10-1	特権管理	□ テレワーク端末やテレワークで利用する各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス
10-2	特権管理	□ テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス

2 セキュリティ対策チェックリストの設定例一覧

チェックリストに記載されている各対策内容を実現するための参考として活用いただくために、テレワークでよく利用される一部の製品を対象として、具体的な製品の設定・利用方法について設定例と併せて解説を行った「設定解説資料」を作成しています。

テレワークツール設定例（設定解説資料）一覧

No.	ドキュメント名	製品種別	製品名
1	設定解説資料 （Cisco WebEx Meeting）	オンライン会議システム	Cisco WebEx Meeting
2	設定解説資料 （Microsoft Teams）	オンライン会議システム	Microsoft Teams
3	設定解説資料 （Zoom）	オンライン会議システム	Zoom

上表の設定解説資料について、次の URL で公開しています。
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

設定解説資料については、今後、テレワークでの利用が多い製品について順次作成していく予定です。

なお、設定解説資料については、特定の製品の利用を促し又は避けるよう勧めるものではありません。

3 テレワーク環境のセキュリティ対策と想定脅威一覧

テレワーク環境におけるセキュリティ対策を実施するうえで参考となる「対策内容」「優先度」「想定脅威」「方式ごとの対策要否」を、次ページ以降に示します。各対策内容における想定脅威の詳細を解説していますので、必要に応じて参考としてください。

No.	分類	対策内容	想定脅威（概要）	想定脅威（詳細）	優先度	備考	方式①	方式②	方式③	方式④	方式⑤	方式⑥	方式⑦	方式⑧
1-1	資産管理	会社で許可したテレワーク端末のみをテレワークに使用しており、使用している端末とその利用者を把握している。	マルウェア感染 不正アクセス 盗難・紛失	テレワークで利用している機器とその利用者を把握できていない場合、機器に対する各種セキュリティ対策が未実施の端末が存在するリスクが増加する。 また、シリアルナンバー等の端末固有の情報を把握していない場合ことで、端末の盗難や紛失時にその実態を把握することが困難であるなどのリスクが増加する。	―		✓	✓	✓	✓	✓	✓	✓	✓
1-2	資産管理	テレワークで利用しているシステムや取り扱う重要情報※1を把握している。 ※1　営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報	不正アクセス 情報の盗聴	テレワークで実施している業務や利用しているシステム、取扱う重要情報を把握していない場合、利用システムや重要情報の取り扱いに関する各種セキュリティ対策が未実施の懸念が増加する。	―		✓	✓	✓	✓	✓	✓	✓	✓
2-1	マルウェア対策	テレワーク端末にウイ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※2。またウイ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。 ※2　Windows 製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、また iOS 製品で、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）でインストールしたアプリのみを利用している場合は、インストール作業は不要	マルウェア感染	最新化されたウイルス定義ファイルであれば駆除できていたマルウェアの駆除ができないため、テレワークで利用している端末のマルウェアに感染するリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓
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	不審なメールに記載されている URL をアクセスすることで悪意のあるサイトに誘導され、マルウェアの感染や、重要情報にアクセスするための認証情報等が取得されるリスクが増加する。 不審な添付ファイルを開くことでマルウェアに感染するリスクが増加する。	○	クラウドサービス（Web メール）の利用無しの場合は対象外	✓	✓	×	✓	✓	✓	×	✓
2-3	マルウェア対策	テレワーク端末（スマートデバイス）へのアプリケーションのインストールは、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	公式アプリケーションストア上からアプリケーションをインストールしていない場合、正規のアプリケーションを模したマルウェアをインストールし、マルウェアに感染するリスクが増加する。	○		✓	✓	✓	✓	✓	✓	✓	✓

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	重要情報へのアクセスを業務上必要な人のみに制限するように、重要情報を保管しているシステムやツールによるアクセス制御や重要情報そのものにパスワードを設定する等の制限を実施していない場合、本来アクセス権限が必要ではない人のアカウントを不正利用された場合や、利用者の不作為（操作ミス等）により重要情報を流出するというリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓	✓
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	社内システムへのインターネット経由でのアクセスに必要なポート以外のポートやIPアドレスからの通信がファイアウォールやルーターで遮断されていない場合、本来不要である許可ポートを利用した悪意のある攻撃（脆弱性を突いた攻撃やアカウントのなりすまし等）により不正アクセスされるリスクが増加する。	○	社内NWに接続しない場合は対象外	✓	×	×	✓	✓	×	×	✓
3-3	アクセス制御（論理）	オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴	オンライン会議の開始時や途中参加者発生時に本人確認を実施しないことにより、会議に不適切なユーザーが不正に参加していることに気付くことができずに、会議を通じた情報漏洩のリスクが増加する。 尚、オンライン会議においては、本人と対面しないため、参加者がシステム上に表示されている名前の本人であることをカメラによるビデオ映像や音声等の方法による確認する必要があります。	○	クラウドサービス（オンライン会議）利用無しの場合は対象外	✓	✓	×	✓	✓	✓	×	✓
3-4	アクセス制御（論理）	オンライン会議にアクセスするためのURLや会議参加のパスワードを不要なメンバーに伝えないようにしている。また会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴	オンライン会議の参加のためのパスワードやURLを不要なメンバーに伝えることで、会議に不適切なユーザーが不正に参加することで会議を通じた情報漏洩のリスクが増加する。 また、パスワードの設定や強度をしない（できない）場合は、ユーザーによるパスワード未設定や容易に推測可能なパスワードを設定することにより、会議への不正参加のリスクが増加する。 尚、会議の不正参加の防止については、URLやパスワードの秘匿以外に、会議開始時の本人確認の徹底などにより代替することが可能。	○	クラウドサービス（オンライン会議）利用無しの場合は対象外	✓	✓	×	✓	✓	✓	×	✓
3-5	アクセス制御（論理）	オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴	オンライン会議において、不適切な参加者が確認された場合に物理的な退出処理はできないため、主会議催者による強制退出が実施できない場合、適切な業務の遂行が実施できないリスクが増加する。	○	クラウドサービス（オンライン会議）利用無しの場合は対象外	✓	✓	×	✓	✓	✓	×	✓
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	テレワークの作業環境は、オフィス環境に比べて、家族を含む不適切な人物が物理的にテレワーク端末を覗き見（ショルダーハッキング）が比較的容易な環境であることが懸念されます。 そのため、覗き見防止フィルタの貼付や、離席時のスクリーンロックの実施を行わない場合、テレワーク端末越しの情報漏洩や不正利用のリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓	✓

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は利用していない。	不正アクセス	テレワーク端末の OS やアプリケーションとしてメーカーサポート切れの製品を利用している場合、製品としてセキュリティアップデートが行わないため、製品の脆弱性に対する攻撃により不正アクセス等のリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓
5-2	脆弱性管理	テレワーク端末の OS やアプリケーションに対して最新のセキュリティアップデートを適用している。	不正アクセス	テレワーク端末の OS やアプリケーションとし最新のセキュリティアップデートを適用していない場合、製品の脆弱性に対する攻撃により不正アクセス等のリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓
5-3	脆弱性管理	テレワークで利用する自宅の Wi-Fi ルーターやモバイル Wi-Fi 等は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス	テレワークで利用している自宅に設置している Wi-Fi ルータ等において、メーカーサポート切れや古いファームウェアの状態で利用している場合、該当ファームウェアの脆弱性に対する攻撃による不正アクセス等のリスクが増大します。	○		✓	✓	✓	✓	✓	✓	✓	✓
5-4	脆弱性管理	テレワーク端末から社内にリモートアクセスする際に利用する VPN 機器や、会社端末のリモートデスクトップアプリケーション等について、メーカーサポート切れの製品は利用せず、最新のセキュリティアップデートを適用している。	不正アクセス	テレワークを実施するために社内に設置している VPN 機器は、利用目的の特性としてインターネットからの通信を許可することになる。そのため、メーカーサポート切れや古いファームウェアの状態で利用している場合、インターネット外部から該当ファームウェアの脆弱性に対する攻撃による不正アクセス等のリスクが増大します。	◎		✓	×	×	×	✓	×	×	×
6-1	通信暗号化	テレワークでクラウドサービス（Web メール、チャット、オンライン会議、クラウドストレージ等）を利用する場合は、HTTPS 通信でかつ、接続先の URL が正しいことを確認している。（クラウドサービスを利用していない場合は対象外）	情報の盗聴	テレワーク勤務者がインターネット経由でクラウドサービスへアクセスする場合は、オフィス環境からのアクセスに比べて無線 LAN の利用等による通信を傍受される可能性が高いと推測される。定常的に利用する暗号化されていない通信を利用するオンライン会議システムを利用する場合、悪意のある第三者による通信の傍受により情報漏洩するリスクが増加する。	○	クラウドサービスを利用していない場合は対象外	✓	✓	×	✓	✓	✓	×	✓
6-2	通信暗号化	クラウドサービスに接続する際や、ID・パスワード等の情報を入力するサービスに接続する際には、暗号化されている HTTPS 通信であることを確認してから使用している。	情報の盗聴	テレワーク勤務者が利用する公共の無線 LAN が、機器の脆弱性や使用している暗号強度等、セキュリティ面で懸念があるため非暗号化された通信を使用する場合、悪意のある第三者による通信の傍受により情報漏洩するリスクが増加する。	○		✓	✓	✓	✓	✓	✓	✓	✓
6-3	通信暗号化	自宅の Wi-Fi ルーター等の機器を利用する場合は、Wi-Fi のセキュリティ方式として「WPA2」を利用して、パスワードは第三者に推測されにくいものを利用している。	情報の盗聴	テレワーク勤務者が利用する公共の無線 LAN や自宅設置の Wi-Fi ルータにおいて、暗号強度の弱いセキュリティ方式（WPA2 以外）や推測しやすいパスワードを利用している場合、悪意のある第三者による通信の傍受により情報漏洩するリスクが増加する。	○		✓	✓	✓	✓	✓	✓	✓	✓

7-1	インシデント対応・管理	情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や懸念がある状況（不審なメールを開封した場合等）における対応方針を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴	情報セキュリティインシデント発生時の対応方針や、関係者への連絡体制が定められていない場合、セキュリティインシデントの発生自体の把握や被害拡大の早期防止等ができずに、セキュリティインシデント全般の発生時の被害が増大するリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓
7-2	インシデント対応・管理	テレワーク端末とアクセス先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴	テレワーク端末とアクセス先の各システムの時刻がずれている場合、情報セキュリティインシデント発生時の原因調査において各種システムログを利用した原因や被害状況の特定や絞り込みの難易度が高くなり、その結果、インシデントによる被害拡大防止のための適切な対応を実施することができずにセキュリティインシデント全般の発生時の被害が増大するリスクが増加する。	○		✓	✓	✓	✓	✓	✓	✓	✓
7-3	インシデント対応・管理	テレワーク端末から社内システムにアクセスする際のアクセスログを収集している。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴	テレワーク端末から社内システムにアクセスする際のアクセスログを収集していないことで、情報セキュリティインシデント発生時の原因調査において原因や被害状況の特定や絞り込みが困難になり、その結果、インシデントによる被害拡大防止のための適切な対応を実施することができずにセキュリティインシデント全般の発生時の被害が増大するリスクが増加する。	○	社内 NW に接続しない場合は対象外	✓	×	×	✓	✓	×	×	✓
8-1	データ保護	テレワーク端末（スマートデバイス）の紛失時に端末の位置情報を検出できるようにしている。	盗難・紛失	テレワーク環境においては、オフィス等で業務を実施する場合に比べて、テレワーク端末の紛失による悪意のある第三者に物理的に取得される可能性が高い懸念がある。テレワーク端末の位置情報を検出するためのアプリケーションソフトウェアを導入していない場合、紛失時の早期発見が困難となることで悪意のある第三者の取得による不正なデータアクセス等の情報漏洩のリスクが増加する。	◎	スマートフォンのみ対象	×	×	×	✓	×	×	×	✓
8-2	データ保護	テレワーク端末（スマートデバイス）の紛失時に MDM※3 等を導入し、リモートからのデータの消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用している。 ※3　Moblie Device Management の略称で、スマートフォン等のスマートデバイスを一元的に管理・運用すること、又はその機能を提供するソフトウェア	盗難・紛失	テレワーク環境においては、オフィス等で業務を実施する場合に比べて、テレワーク端末の紛失による悪意のある第三者に物理的に取得される可能性が高い懸念がある。リモートからデータ削除を行う機能や、ログイン時の認証ポリシーやハードディスクの暗号間等を強制していない場合、紛失時に悪意のある第三者が取得することによる不正なデータアクセス等の情報漏洩のリスクが増加する。	○	スマートフォンのみ対象	×	×	×	✓	×	×	×	✓

8-3	データ保護	テレワーク端末の盗難・紛失時に情報が漏えいしないように、ハードディスクやフラッシュメモリ※4等の内蔵された記憶媒体の暗号化を実施している※5。（端末に会社のデータを保管しない場合は対象外） ※4　ハードディスクとは異なる記憶媒体の一つで、「不揮発性の半導体メモリ」をさす。電源をおとしてもデータを保持することが可能な記憶媒体 ※5　iOS 製品については初期状態で暗号化されているため対応不要	盗難・紛失	テレワーク環境においては、オフィス等で業務を実施する場合に比べて、紛失や盗難などによりテレワーク端末のハードディスクを悪意のある第三者が物理的に取得する可能性が高い懸念がある。ハードディスクの暗号化を実施していない場合、取得されたハードディスクの読み取りが可能な装置に接続することで、アカウントの認証無しにデータにアクセスされることが可能であり、保存している情報を漏えいするリスクが増加する。	○	端末に会社のデータを保管しない場合は対象外	✓	✓	✓	×	✓	✓	✓	×
8-4	データ保護	テレワーク端末には原則として重要情報を保管しておらず、もし重要情報を保管しなければならない場合※6には、ファイルの暗号化（パスワード設定等）を実施している。（端末に会社のデータを保管しない場合は対象外） ※6　テレワーク端末のローカルにファイル保存するケースであり、ファイルサーバやクラウドストレージ、各種クラウドサービスのシステム内に保存するケースは対象外	不正アクセス 盗難・紛失	テレワーク環境においては、オフィス等で業務を実施する場合に比べて、紛失や盗難などによりテレワーク端末のハードディスクを悪意のある第三者が物理的に取得する可能性が高い懸念がある。 テレワーク端末に保管された重要情報に対してパスワード設定等の暗号化を実施していない場合、ハードディスクの盗難時やマルウェア等による不正アクセス時にテレワーク端末に保存されている重要情報にアクセスされた場合の情報漏洩のリスクが増加する。	○	端末に会社のデータを保管しない場合は対象外	✓	✓	✓	×	✓	✓	✓	×
8-5	データ保護	オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。 上記のルールを強制することが可能な場合は、強制するように設定する。 （クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴	オンライン会議に関する、適切なルールを作成していないことにより、本来、共有する必要が無い情報を共有してしまう懸念があります。具体的には、公開されている会議そのものの情報（会議のタイトル等）に重要情報を含めてしまう、会議中に共有する予定ではないデスクトップ画面情報やビデオ画面や音声等の不作為による共有、会議の録画ファイルが不適切な第三者に参照される、等による情報漏洩のリスクが増加する。 また、上記のルールをシステム的に強制できない場合、利用者がルールを守らないことによる情報漏洩リスクの増加が発生します。	○	クラウドサービス（オンライン会議）利用無しの場合は対象外	✓	✓	×	✓	✓	✓	✓	×	✓
9-1	認証	テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス	従業員が利用する端末のログインアカウントや、テレワークで利用するシステムのアカウントのパスワードが破られやすい容易なパスワードに設定している場合、悪意のある第三者にパスワードが把握されやすくなり、なりすましによる不正アクセスが行われれるリスクが増加します。	◎		✓	✓	✓	✓	✓	✓	✓	✓	✓

9-2	認証	テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス	従業員が利用する端末のログインアカウントや、テレワークで利用するシステムのアカウントの初期パスワードを変更していない場合、悪意のある第三者にパスワードが把握されやすくなり、なりすましによる不正アクセスが行われれるリスクが増加します。	◎		✓	✓	✓	✓	✓	✓	✓	✓	✓
9-3	認証	テレワーク端末やテレワークで利用する各システムのアカウントが一定回数以上パスワードを誤入力した場合、パスワード入力ができなくなるように制限している。	不正アクセス	テレワークで利用する端末や各システムのアカウントが一定回数以上パスワードを誤入力した場合パスワード入力できないように制限していない場合、悪意のある第三者によるパスワード試行が容易に実行できるためパスワードが把握されやすくなり、なりすましによる不正アクセスが行われれるリスクが増加します。	○	従業員所有端末については業務用途以外にも利用されていることが前提のため対象外とする。	✓	✓	✓	✓	×	×	×	×
9-4	認証	テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定している。	不正アクセス	テレワークで利用する各システムへのアクセスに対して多要素認証を設定せずに ID/Password のみで認証を行うことで、悪意のある第三者にパスワードが流出された場合に、なりすましによる不正アクセスが行われれるリスクが増加します。	○		✓	✓	✓	✓	✓	✓	✓	✓	✓
10-1	特権管理	テレワーク端末やテレワークで利用する各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス	テレワークで利用する端末や各システムにおいて、業務上不要に人に対して管理者権限を与えている場合、悪意のある第三者による不正アクセスにより重要情報にアクセスできる可能性が高くなり、重要情報の漏洩のリスクの増加や、ユーザーの不作為による情報漏洩のリスクが増加します。	○		✓	✓	✓	✓	✓	✓	✓	✓	✓
10-2	特権管理	テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス	テレワークで利用する端末や各システムの管理者権限のパスワードに、強力なパスワードポリシーを適用していない場合、ユーザーが破られやすい容易なパスワードに設定することで、悪意のある第三者にパスワードが把握されやすくなり、なりすましによる不正アクセスが行われれるリスクが増加します。	○		✓	✓	✓	✓	✓	✓	✓	✓	✓
10-3	特権管理	テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用している。	不正アクセス	管理者権限が必要な作業時以外で管理者権限を利用することで、管理者権限の利用情報などから不正アクセスの懸念を発見する等が困難になったり、ユーザーの不作為による情報漏洩のリスクが増加します。	○	従業員所有端末については業務用途以外にも利用されていることが前提のため対象外とする。	✓	✓	✓	✓	×	×	×	×

参考

1 用語集

用語	解説
OS（Operating System）	メモリやハードディスクの管理やキーボードの入出力機能等、PC やスマートデバイスに基本的な動作をさせるため必要なソフトウェア。
USB メモリ	USB コネクタに接続して利用する、持ち運び可能な記憶媒体。
VPN	Virtual Private Network の略。あたかも自社ネットワーク内部の通信のように、自宅や外出先などの遠隔の場所から安全に社内ネットワークにアクセスが行える技術のことです。
WPA2	無線 LAN のセキュリティ方式の一つで、現在主流として利用されているもの。これよりセキュリティが弱い方式として WPA や WEP という方式がありますが、利用の際は WPA2 を利用することが推奨されます。
アカウント	ネットワーク及び社内システムにログインする際の権利（ユーザ ID 等）。
アクセスログ	サーバやルーターの動作を記録したもの。アクセス元及びアクセス先の情報を記録し、実施された操作の分析や事故発生時の原因特定などに用いられます。
ウイルス	マルウェアの一種。ワームと異なり自ら感染のための活動を行うことはありませんが、感染している PC やスマートフォンに保存されているファイルを書き換えることによって、自分のコピーを保存し、そのファイルがネットワークや記録装置を通じて流通することで感染が拡大します。
クラウドサービス	従来は、PC やサーバで管理・利用していたようなソフトウェアやデータ等を、インターネット等のネットワークを通じて利用できるようにした様々なサービスの総称。本書では、メール、チャット、オンライン会議、ファイル共有などのクラウドサービスを想定しています。また、プロバイダーが提供するメールサービスの利用も含みます。
サテライトオフィス	本来の勤務先とは別に設置されるオフィス形態の施設のこと。特定の企業専用に設けるものや、複数の企業で共有するものなどがある。
シリアルナンバー	「シリアル番号」とも呼ばれる識別情報。PC などの製品などに付与される番号で PC の種類ではなく端末固有に割り当てられる番号。
スマートデバイス	iPhone、Android OS が搭載されたスマートフォンや、iPad などのタブレットの総称。

脆弱性	ICT 機器・システムやその利用環境における情報セキュリティ上の欠陥のこと。機器やシステムの設計や開発･実装の過程において意図せずに作り込まれてしまう欠陥と、システムの利用時における設定ミスや不注意によって生じる欠陥の両方を含みます。
セキュアブラウザ	社内システムやクラウドサービス上に保管された情報を閲覧する際に利用する専用ソフトウェアで、情報閲覧時に手元の端末にデータが保存されない（できない）機能があるものです。製品によっては、スクリーンショット、テキストのコピー&ペースト、アクセス可能なページの制限を行えるものもあります。
セキュリティアップデート	ソフトウェアにおけるセキュリティに関する不具合の部分を、安全対策を施したものに置き換えること。または置き換えるために使用する修正プログラムそのものをさします。
セキュリティ方式	無線ルーターなどの機器によって「暗号化 Protocol」や「暗号化」「セキュリティ」と呼ばれる無線ルーターの接続方式。
定義ファイル	「シグニチャ」「パターンファイル」等とも呼ばれる、ウイルスの特徴を収録したファイルのこと。ウイルスを検出する際に使用されます。
テレワーク端末	テレワークを実施するためにオフィス以外の環境に持ち出して作業を行う PC やスマートフォン等の機器を指します。
テレワーク端末へのデータ保存	テレワークの際に、社内サーバやクラウドサービスにデータを保存するのではなく、テレワーク環境で利用する（持ち出して利用する）端末にデータを保存する場合をさします。データの保存場所がよくわからない場合は、テレワーク端末がネットワーク（社内ネットワークやインターネット）に接続していない状態でも該当データにアクセスできる場合は、テレワーク端末にデータが保存されていると考えることができます。
のぞき見防止フィルタ	PC やスマートフォンの利用者以外の第三者が、画面をのぞき込んだ際に内容が読み取りにくくすることを目的として、画面に貼付するフィルタ。
ハードディスクの暗号化	物理的にハードディスクが盗難にあった場合、他の端末に接続して中身を見られたりしないように暗号化する機能。Windows10 のデフォルトである BitLocker などが本機能に該当します。
ファイアウォール	ネットワーク上を流れる通信を遮断する機能を持つソフトウェア。
ファームウェア	コンピュータやルーターのような電子機器のハードウェアに密接に連携して組み込まれるソフトウェア。
リモートデスクトップ	社内ネットワークに置いてある PC の画面をネットワーク経由で手元 PC（テレワーク端末）に転送して表示し、遠隔から社内ネットワーク上の PC を操作する技術のことです。
ルーター	ネットワークに接続された機器間の通信経路の制御を行う機器のことです。

2 テレワークセキュリティに関する参考情報

本書に関連して参考となる文献や Web サイトなどを示します。規格やガイドラインは改定されますので、適宜に最新版を参照してください。

○テレワークセキュリティガイドライン（第 4 版）【総務省】
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用いただくために、テレワークの導入に当たってのセキュリティ対策についての考え方や対策例を示したものです。

○インターネットの安全・安心ハンドブック【内閣サイバーセキュリティセンター】
https://www.nisc.go.jp/security-site/handbook/
インターネットの利用に当たっての一般的な留意点をハンドブックとして示したものです。

○サイバーセキュリティ経営ガイドライン Ver2.0【経済産業省/独立行政法人情報処理推進機構】
https://www.meti.go.jp/policy/netsecurity/mng_guide.html
企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するための観点からとりまとめた資料です。

○中小企業の情報セキュリティ対策ガイドライン【独立行政法人情報処理推進機構】
https://www.ipa.go.jp/security/keihatsu/sme/guideline/
中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順を示したものです。

○テレワークではじめる働き方改革　テレワークの導入・運用ガイドブック【厚生労働省】
https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/H28hatarakikatakaikaku.pdf
主として労務・人事の観点からテレワークの導入・運用についてまとめられたものです。

○テレワーク実施者の方へ【内閣サイバーセキュリティセンター】
https://www.nisc.go.jp/security-site/telework/
○テレワークを実施する際にセキュリティ上留意すべき点について【内閣サイバーセキュリティセンター】
https://www.nisc.go.jp/active/general/pdf/telework20200414.pdf
○テレワーク等への継続的な取組に際してセキュリティ上留意すべき点について【内閣サイバーセキュリティセンター】
https://www.nisc.go.jp/active/general/pdf/telework20200611.pdf
○テレワークを行う際のセキュリティ上の注意事項【独立行政法人情報処理推進機構】
https://www.ipa.go.jp/security/announce/telework.html
関係機関から、テレワークを行う際のセキュリティ上の留意点等について周知が行われています。

テレワークのセキュリティで困ったときは

総務省では、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無料で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が対応いたしますので、是非ご活用ください。

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？

〇相談費用

無料

〇相談対応期間

2021 年 3 月まで

〇相談方法

次の URL から申込の後、相談者の希望に応じて、電話・メール・Web 会議により対応

〇相談申込先

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。

本書に対する御意見等をお寄せください。
第２版に向けた改定作業の参考とさせていただきます。
なお、個別のシステムおよび環境に関する御質問をいただいても回答・返信ができない場合があります。

本書に関する問い合わせ先

総務省 サイバーセキュリティ統括官室

Email telework-security@ml.soumu.go.jp

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