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）

第２版

（令和３年５月）

総務省

テレワークセキュリティの疑問と本書の対応ページ

Q. まず何から始めればよいか知りたい。チェックリストを手早く確認したい。

A. まず「第1部1. テレワーク方式の確認」で自組織のテレワークの方式を確認してください。
次に、「第2部1. セキュリティ対策チェックリスト」で自組織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。

Q. 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。

A.「第1部2. テレワーク方式の解説」で各方式の特徴について、図等を用いて解説しているので確認してください。

Q. チェックリスト項目の必要性を知りたい。社内へ説明する理由がほしい。

A.「第1部3. 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。

Q. 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。

A.「第2部2. 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。

Q. 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。

A.「第2部3. 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。

※本書を周知する場合は、次のURLを周知願います。
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

※本書は、総務省の令和2年度事業「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」（受託者：NRIセキュアテクノロジーズ株式会社）の調査研究結果を踏まえ、総務省において作成したものです。

目次

0．はじめに

(1)　本書の目的

総務省では、従来から、テレワークを業務に活用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・活用するための指針として「テレワークセキュリティガイドライン」を策定[1]してきました。

本書は、この「テレワークセキュリティガイドライン」を補うものとして、予算やセキュリティ体制等が必ずしも十分ではない中小企業等の担当者を対象としたものです。具体的には、中小企業等の担当者がテレワークを導入し、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、**中小企業等においても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**を具体的に示しています。

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**です。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、効果的にテレワークセキュリティを確保することができます。

(2)　本書の想定読者

本書は、中小企業等においてシステム・セキュリティ管理を行う担当者（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。具体的には次の読者像を想定し、これを念頭に用語や解説を付加して作成しています。

	本書の想定読者像	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	外部委託コストの捻出は難しいレベルの組織	外部委託コストは必要に応じて捻出しうるレベルも含めた幅広い組織
セキュリティ推進体制	専任のセキュリティ担当が存在しないような組織	専任の担当・担当部門が存在する場合も含めた幅広い組織
セキュリティリテラシ	「適切に…」等の読者に解釈を委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…」等の読者に解釈を委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	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
	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

[1] 初版：平成16(2004)年12月／第２版：平成18(2006)年４月／第３版：平成25(2013)年３月／第４版：平成30(2018)年４月／第５版：令和３(2021)年５月

(3)　テレワークの形態

テレワークとは、情報通信技術（ICT：Information and Communication Technology）を活用し、場所や時間を有効に活用できる柔軟な働き方のことです。

テレワークの形態は、業務を行う場所に応じて、在宅勤務、サテライトオフィス勤務、モバイル勤務に分類され、本書ではいずれの形態も対象としています。

①　在宅勤務

自宅で業務を行う働き方です。

通勤等の移動時間を要しないことから、時間を有効に活用することが可能です。また、例えば育児休業明けの労働者が短時間勤務等と組み合わせて勤務することや、保育所の近くで働くこと等が可能となるため、仕事と家庭生活との両立に資する働き方です。

②　サテライトオフィス勤務

自宅の近くや通勤途中の場所等に設けられたサテライトオフィス（メインのオフィス以外に設けられたオフィス。シェアオフィスやコワーキングスペースを含みます。）で業務を行う働き方です。

通勤時間を短縮しつつ、在宅勤務やモバイル勤務以上に環境の整った場所で業務を行うことができます。また、都心部にあるサテライトオフィスは、移動時間に立ち寄って業務を行うことが可能なことから、業務効率化を図ることも可能です。

③　モバイル勤務

ノートPC等を活用して臨機応変に選択した場所で業務を行う働き方です。

自由に働く場所を選択できる、外勤における移動時間を利用できるなど、働く場所を柔軟に運用することで業務の効率化を図ることが可能です。

ICT技術の進歩により、テレワーク環境は、オフィス環境と全く同等とは言えないものの、大きな遜色のない程度に業務を実施できるようになってきています。また、テレワークの実施には、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・療養との両立、事業継続性（BCP）の確保等のメリットがあります。

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することなく、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、テレワークを導入するようにしましょう。

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。

(4)　本書の構成（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。

まず、第１部（「第１部１．テレワーク方式の確認」（p.8～））で、テレワークでの業務内容や利用する端末等の状況を基に、該当するテレワーク方式を確認・特定してください。テレワーク方式が既に明らかな場合には、第１部は読み飛ばして構いません。

その上で、第２部（主に「第２部１．セキュリティ対策チェックリスト」（p.29～））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し、そのチェックリストをもとにセキュリティ対策をお願いします。

構成	概要
０．はじめに	本書の目的や想定読者像を明らかにした上で、全体構成（活用方法）を説明しています。
第1部	
第１部１．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、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ための手順を示しています。
第１部２．テレワーク方式の解説	本書で取り扱う各テレワーク方式の詳細を解説しています。
第１部３．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解説しています。
第2部	
第２部１．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項目を「チェックリスト」の形で示しています。
第２部２．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、具体的な製品の設定例について触れています。
第２部３．セキュリティ対策と想定脅威一覧	「チェックリスト」を一覧形式で示すとともに、それぞれのセキュリティ対策項目における想定脅威の詳細を示しています。
参考	
参考１　用語集（キーワード解説）	本書で用いている主な用語を説明しています。また、重要なキーワードについても解説します。
参考２　テレワークセキュリティに関する参考情報	チェックリストを活用する上で参考となる文献やWebサイト等を示しています。

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３．テレワーク環境で想定される脅威の解説」（p.23～）を作成しています。御活用ください。

第１部１．テレワーク方式の確認

テレワークの実現するためのシステム構成には複数の方式が存在します。例えば、テレワークで利用する端末の種別、オフィスネットワークへの接続方式の別等により方式を分類することができ、方式によって考慮すべきセキュリティ対策も変わります。

そのため、皆様の組織で導入している（導入を予定している）テレワーク方式をまずは明らかにする必要があります。次ページに、テレワークでの業務内容、利用する端末等の状況をもとに、該当する選択肢を選ぶことでテレワーク方式を確認できるフローチャートを示していますので活用してください。テレワーク方式が明らかな場合は、第２部に進んでください。

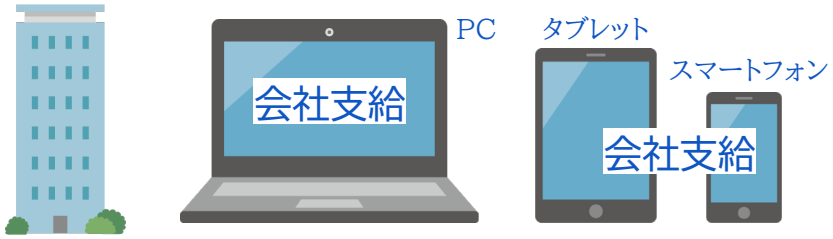
なお、組織内で複数のテレワーク方式が利用されていることもありますので、その場合は該当する複数の方式についてそれぞれご確認ください。

また、各方式の詳細な説明については、「第１部２．テレワーク方式の解説（p.10～）」をご覧ください。

＜テレワーク端末の例＞

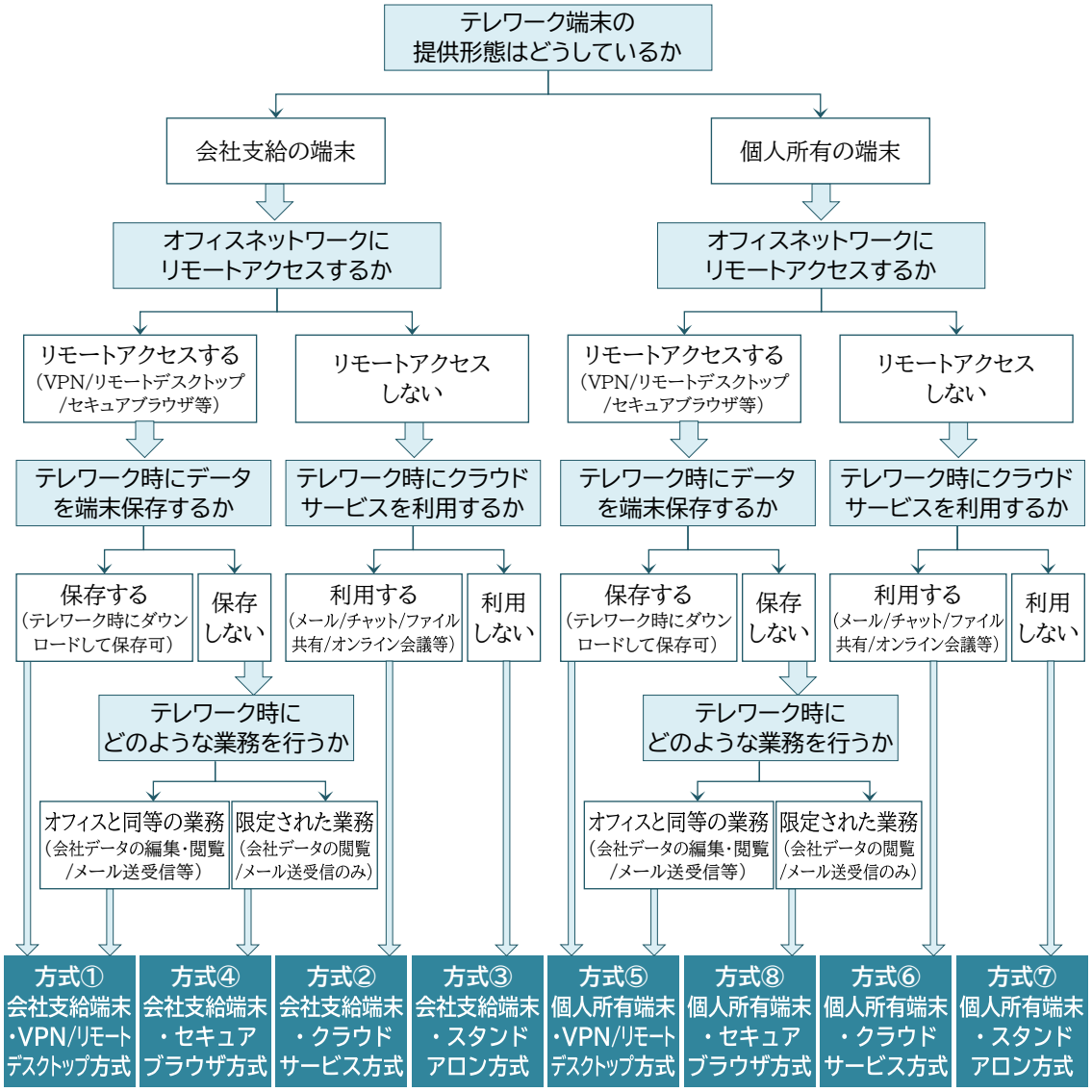
会社支給の端末

テレワークのために、オフィスから持ち出して使用するPCやスマートフォン等が該当します。テレワーク専用端末を会社から支給される場合もこちらに該当します。



個人所有の端末

従業員が個人所有しており、テレワークに利用するPCやスマートフォン等が該当します。



PCやスマートフォン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、環境ごとにフローチャートで方式を確認してください。

第１部２．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８つのテレワーク方式[2]について解説します。フローチャートによって選択したテレワーク方式が、導入している（導入を予定している）ものと合致しているかどうかの確認のためにも、解説を御活用ください。

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の略称。あたかもオフィスネットワーク内部にいるかのように、自宅や外出先などの遠隔の場所から安全にオフィスネットワークに接続可能な技術のことです。
クラウドサービス	従来は、オフィスネットワーク内のPCやサーバで保存・管理していたようなソフトウェアやデータを、オフィスネットワーク内ではなくインターネット上で保存・管理し、利用者は、インターネットを通じていつでもどこでも利用できるようにしたサービス。 本書では、メール、チャット、オンライン会議、ファイル共有等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。
セキュアブラウザ	特殊なインターネットブラウザで、端末側にデータを残さずに利用することができます。閲覧した情報を端末に保存できないようにする機能や、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、接続先制限を行えるものもあります。 クラウドサービスやオフィスネットワーク上のシステムに接続する際に利用することで、情報漏えい等に備えたデータ管理が容易になります。
リモートデスクトップ	オフィスネットワークに置いてあるPCの画面を、インターネット経由でテレワーク端末のPCに転送して表示した上で、テレワーク端末のPCからオフィスネットワークに置いてあるPCを遠隔操作する技術。

[2] テレワークセキュリティガイドラインと比較した場合、本書では次の違いがあります。
・中小企業等には導入が難しい「仮想デスクトップ（VDI）方式」「セキュアコンテナ方式」を除外
・テレワーク端末が「会社支給」であるか「個人所有」であるかにより、別方式として取扱い
・「VPN方式」と「リモートデスクトップ方式」は、本書でのセキュリティ対策が同じであるため統合
・「クラウドサービス方式」を併用する場合、別方式とせず併用先方式に包含して取扱い

テレワーク方式の全体概要

テレワーク方式について、テレワーク端末が「会社支給」であるか「個人所有」であるかにより大別（会社支給端末：方式①～方式④／個人所有端末：方式⑤～方式⑧）しています。

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へVPN接続して業務を行う方式。 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ある端末（PC）へリモートデスクトップ接続して業務を行う方式。 いずれの場合も、ダウンロードしたデータを用いてテレワーク端末上で業務を実施するケースも含みます。	方式解説 p.13～ チェックリスト p.30～
方式② 会社支給端末・クラウドサービス方式	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に接続して業務を行う方式。 クラウドサービスからダウンロードしたデータを用いて、テレワーク端末上で業務を行う場合も含みます。	方式解説 p.15～ チェックリスト p.33～
方式③ 会社支給端末・スタンドアロン方式	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にデータを保存しておき（外部記録媒体で持ち運ぶ場合を含みます。）、テレワーク中は保存しておいたデータを処理することで業務を行う方式。	方式解説 p.16～ チェックリスト p.36～
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セキュアブラウザを利用し、オフィスネットワーク内の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に接続して業務を行う方式。	方式解説 p.17～ チェックリスト p.38～

方式⑤ 個人所有端末・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	個人所有のテレワーク端末からオフィスネットワークへVPN接続して業務を行う方式。 または、個人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端末(PC)へリモートデスクトップ接続して業務を行う方式。 いずれの場合も、ダウンロードしたデータを用いてテレワーク端末上で業務を実施するケースも含みます。	方式解説 p.18～ チェックリスト p.41～
方式⑥ 個人所有端末・クラウドサービス方式	接続しない	利用する	保存する/保存しないどちらも含む	個人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に接続して業務を行う方式。 クラウドサービスからダウンロードしたデータを用いて、テレワーク端末上で業務を行う場合も含みます。	方式解説 p.20～ チェックリスト p.44～
方式⑦ 個人所有端末・スタンドアロン方式	接続しない	利用しない	保存する	個人所有のテレワーク端末に外部記録媒体等でデータを持ち運び、テレワーク中は保存しておいたデータを処理することで業務を行う方式。	方式解説 p.21～ チェックリスト p.47～
方式⑧ 個人所有端末・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	個人所有のテレワーク端末からセキュアブラウザを利用し、オフィスネットワーク内の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に接続して業務を行う方式。	方式解説 p.22～ チェックリスト p.49～

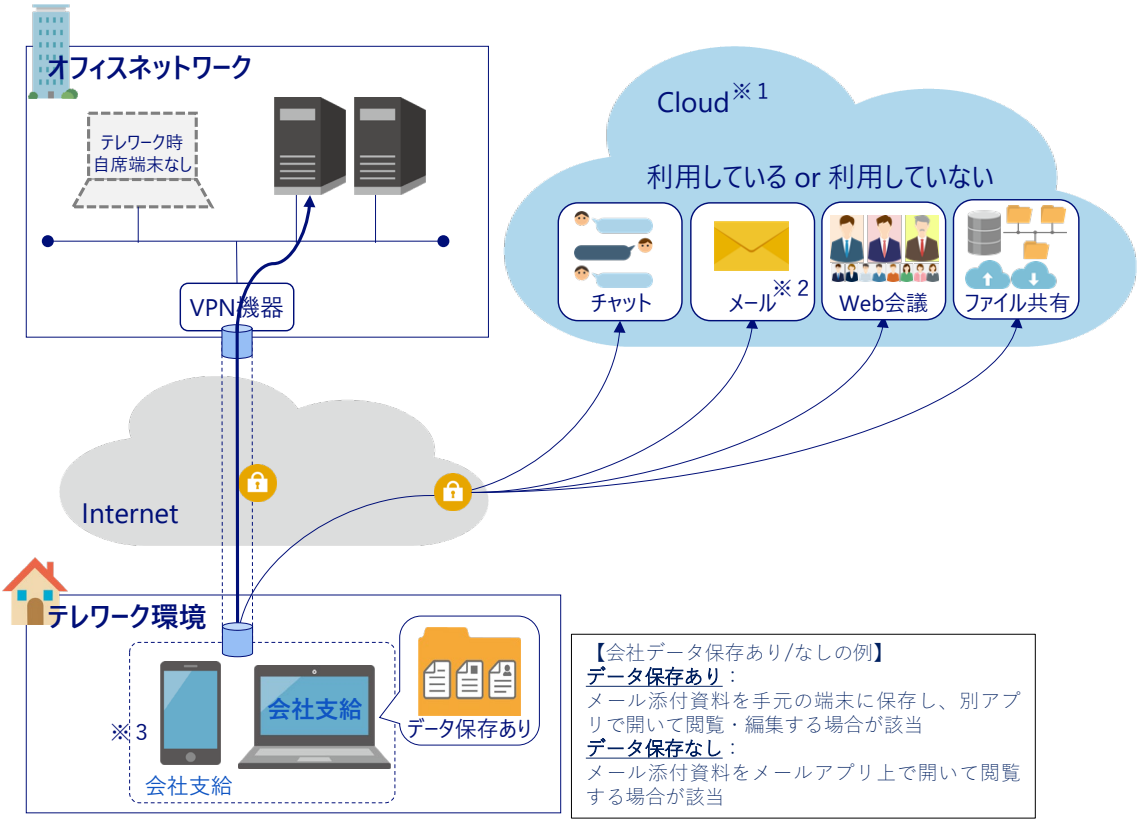
方式①　会社支給端末・VPN/リモートデスクトップ方式

次に示す２つのパターン（VPN方式とリモートデスクトップ方式）が該当します。

［VPN方式］

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。ダウンロードしたデータを用いてテレワーク端末上で業務を実施するケースも含みます。

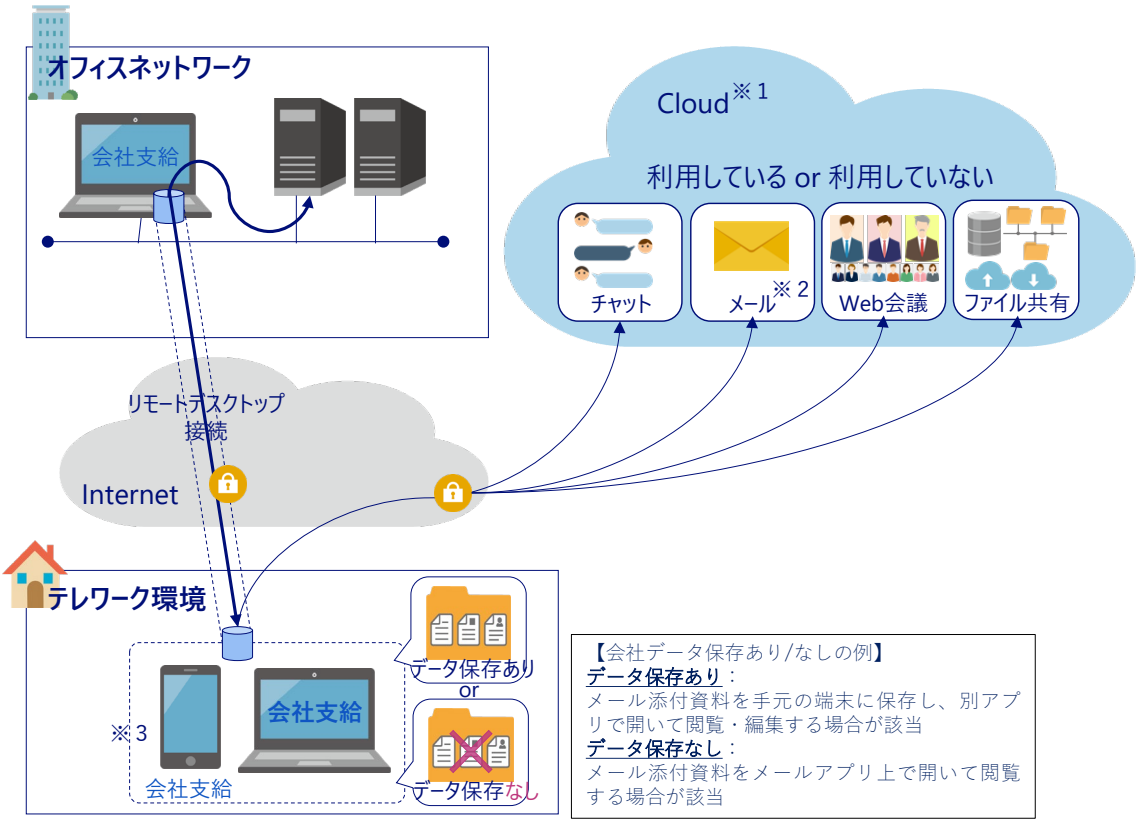


※１「クラウドサービスを利用」は全部又は一部を利用しているケースが該当
※２ プロバイダー提供のメール利用もクラウドサービスに該当
※３ タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

［リモートデスクトップ方式］

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端末（PC）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。ダウンロードしたデータを用いてテレワーク端末上で業務を実施するケースも含みます。

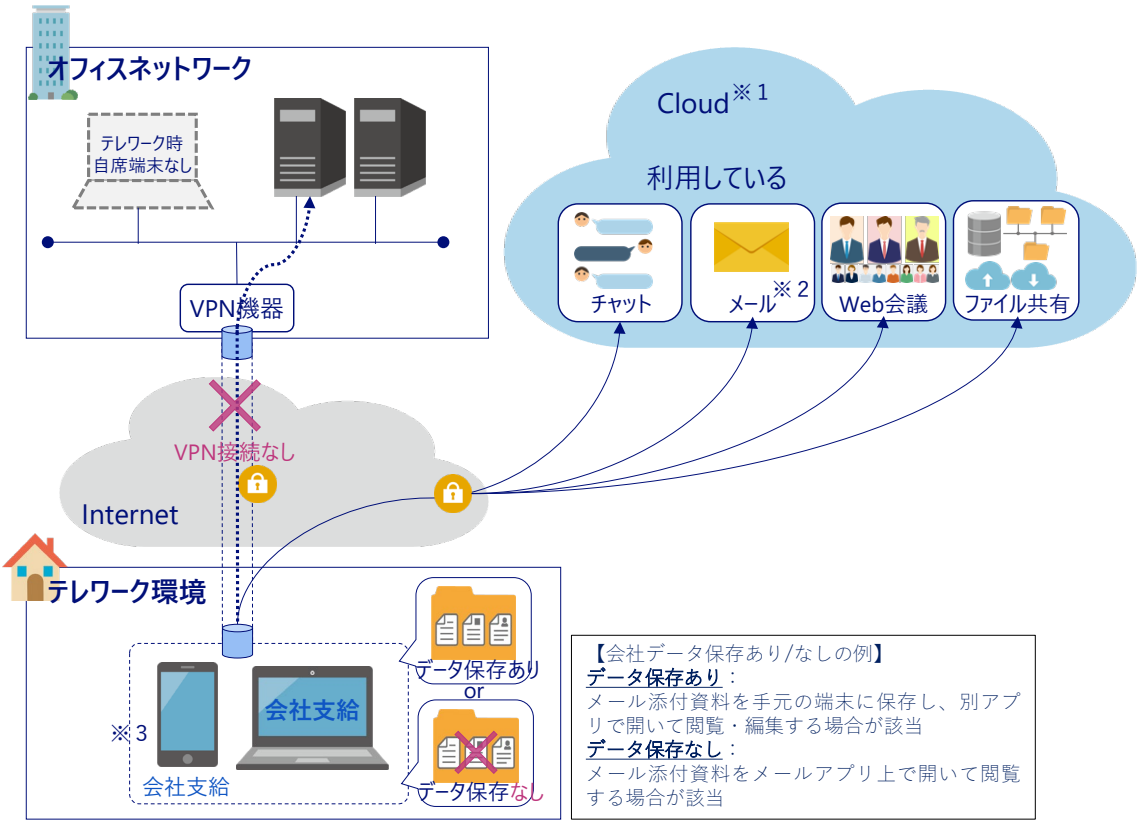


※1 「クラウドサービスを利用」は全部又は一部を利用しているケースが該当
※2 プロバイダー提供のメール利用もクラウドサービスに該当
※3 タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

方式②　会社支給端末・クラウドサービス方式

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す。クラウドサービスからダウンロードしたデータを用いて、テレワーク端末上で（スタンドアロン方式のように）業務を実施する場合も含みます。

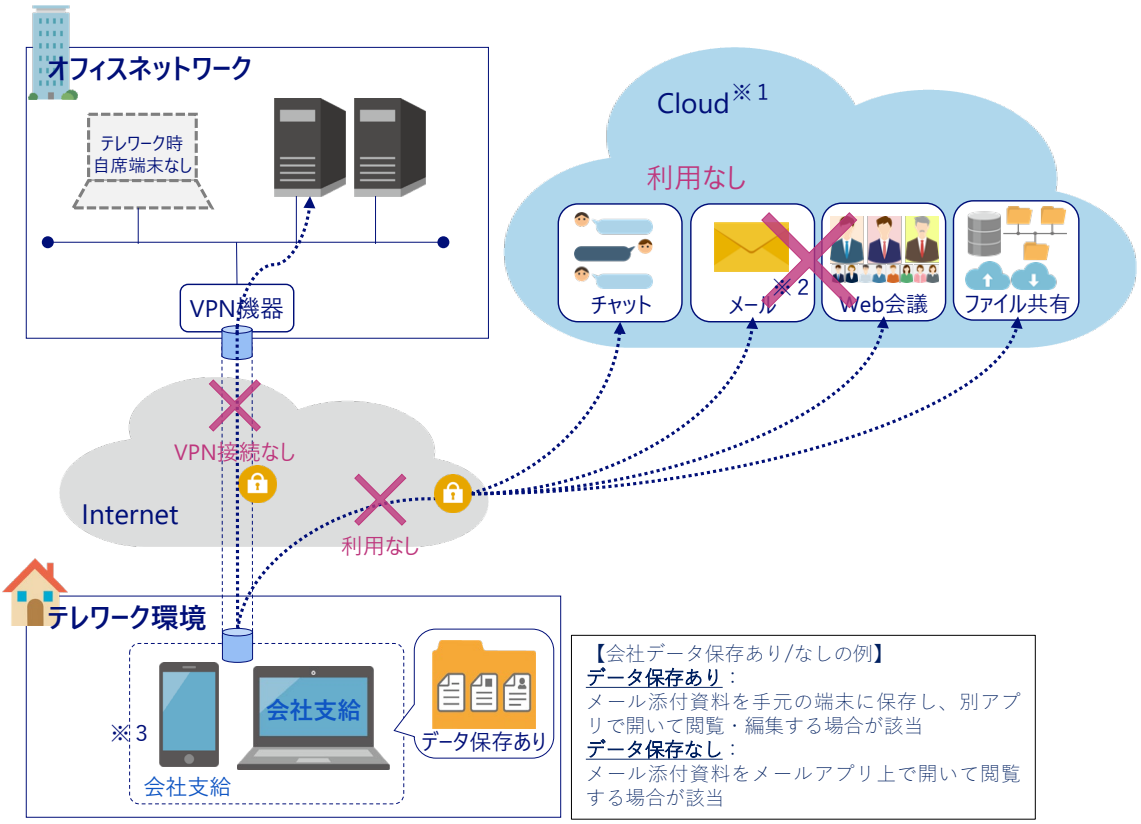


※1 「クラウドサービスを利用」は全部又は一部を利用しているケースが該当
※2 プロバイダー提供のメール利用もクラウドサービスに該当
※3 タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

方式③　会社支給端末・スタンドアロン方式

会社支給のテレワーク端末にデータを保存しておき（外部記録媒体で持ち運ぶ場合を含みます。）、テレワーク中は保存しておいたデータを処理することで業務を実施します。

スタンドアロン方式では、ネットワークに接続しないことから、オフィスネットワークに接続せず、クラウドサービスも利用しないことが特徴です。

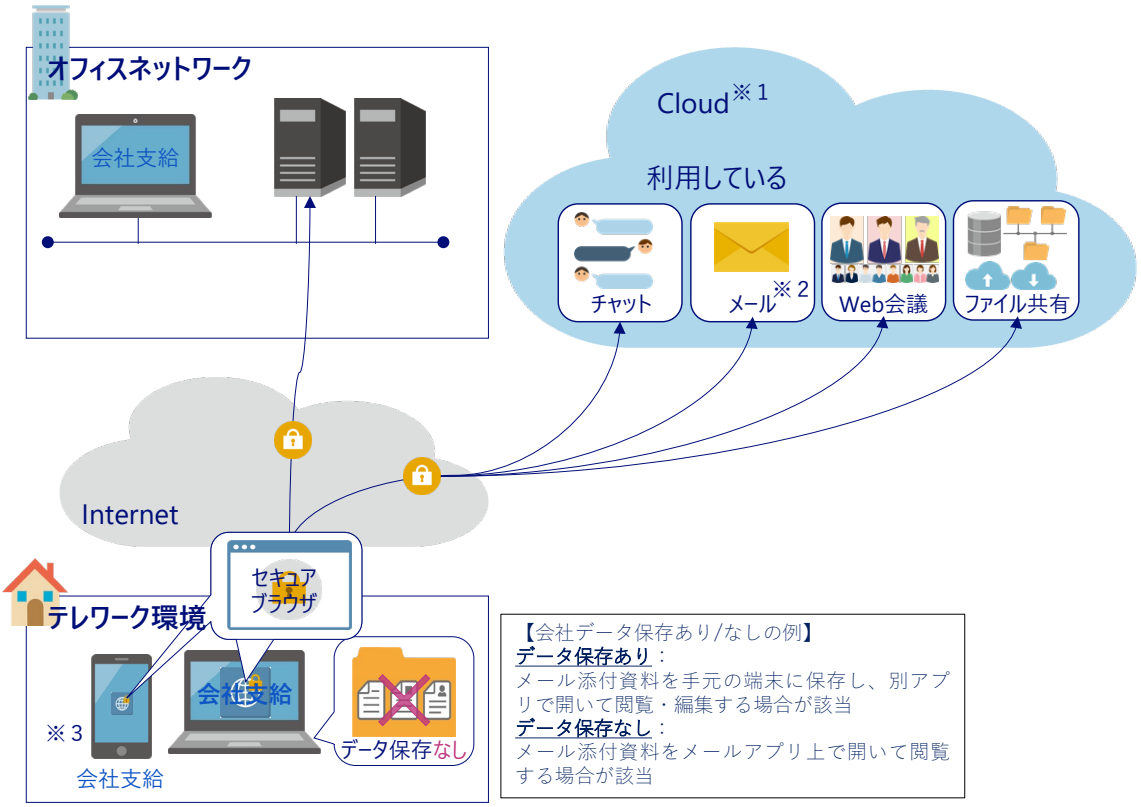


※1 「クラウドサービスを利用」は全部又は一部を利用しているケースが該当
※2 プロバイダー提供のメール利用もクラウドサービスに該当
※3 タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

方式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、オフィスネットワーク内の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に接続して業務を実施します。

セキュアブラウザ方式では、端末へのデータ保存をしないことが特徴です。また、セキュアブラウザに対応した限定された業務のみをテレワークで実施します。



※1 「クラウドサービスを利用」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 タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

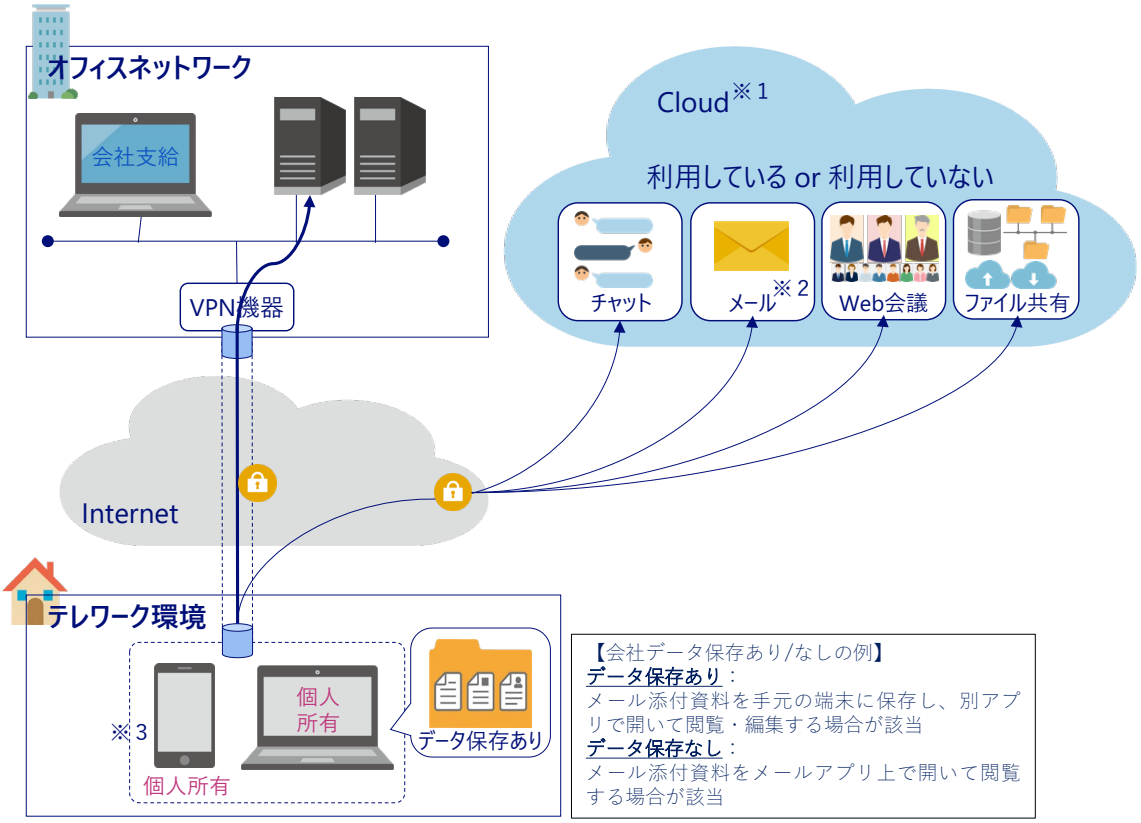
方式⑤　個人所有端末・VPN/リモートデスクトップ方式

次に示す２つのパターン（VPN方式とリモートデスクトップ方式）が該当します。

［VPN方式］

個人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。ダウンロードしたデータを用いてテレワーク端末上で業務を実施するケースも含みます。

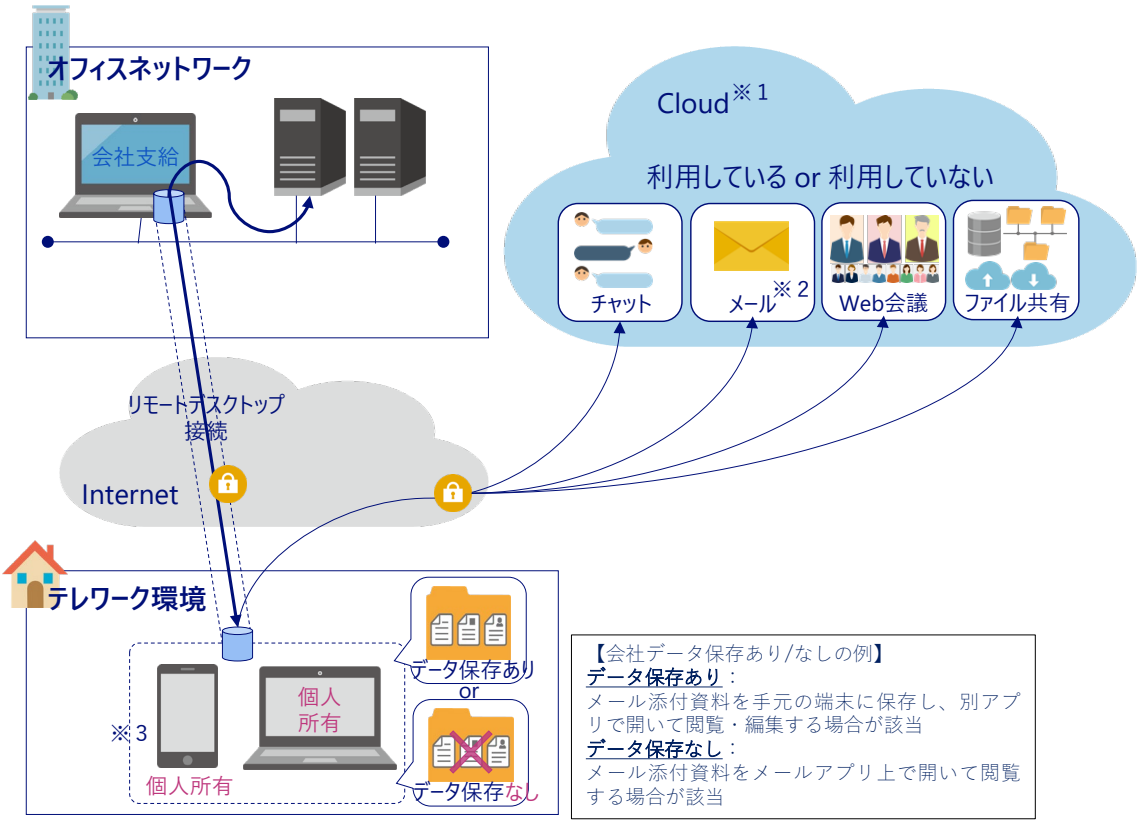


※１「クラウドサービスを利用」は全部又は一部を利用しているケースが該当
※２ プロバイダー提供のメール利用もクラウドサービスに該当
※３ タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

［リモートデスクトップ方式］

個人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端末（PC）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。ダウンロードしたデータを用いてテレワーク端末上で業務を実施するケースも含みます。

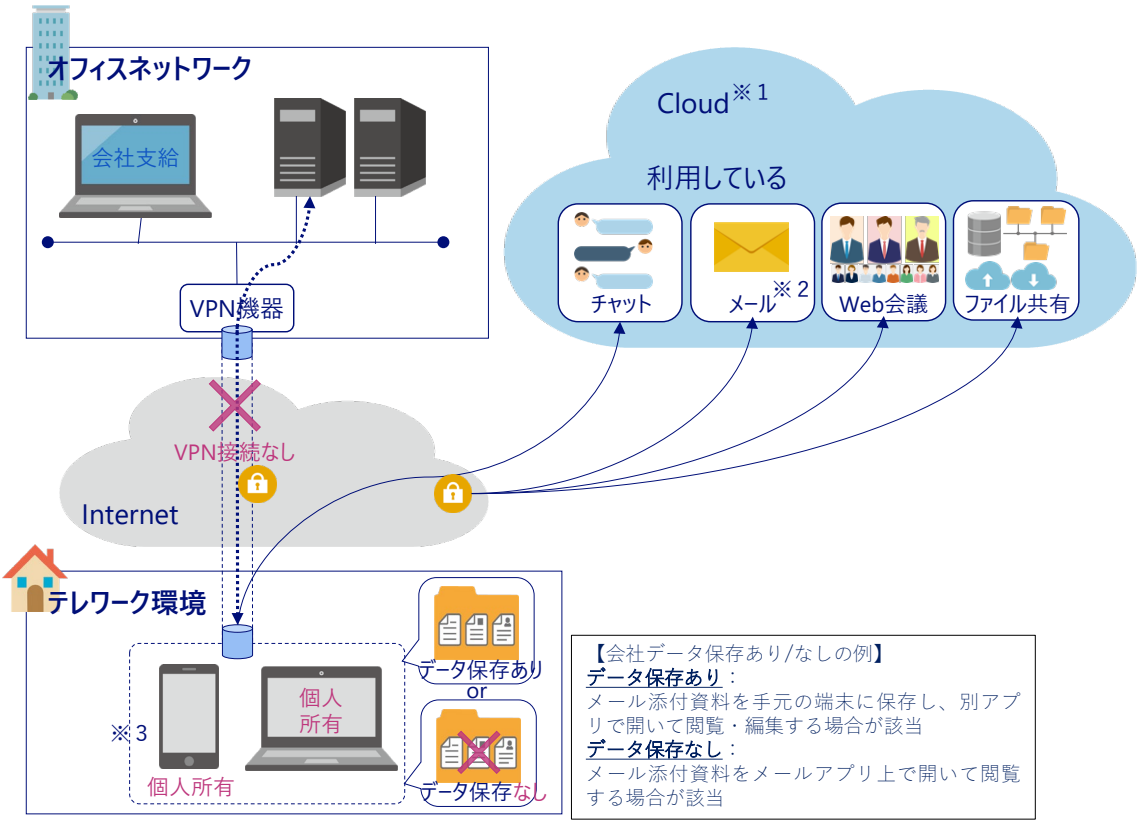


※1 「クラウドサービスを利用」は全部又は一部を利用しているケースが該当
※2 プロバイダー提供のメール利用もクラウドサービスに該当
※3 タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

方式⑥　個人所有端末・クラウドサービス方式

個人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す。クラウドサービスからダウンロードしたデータを用いて、テレワーク端末上で（スタンドアロン方式のように）業務を実施する場合も含みます。

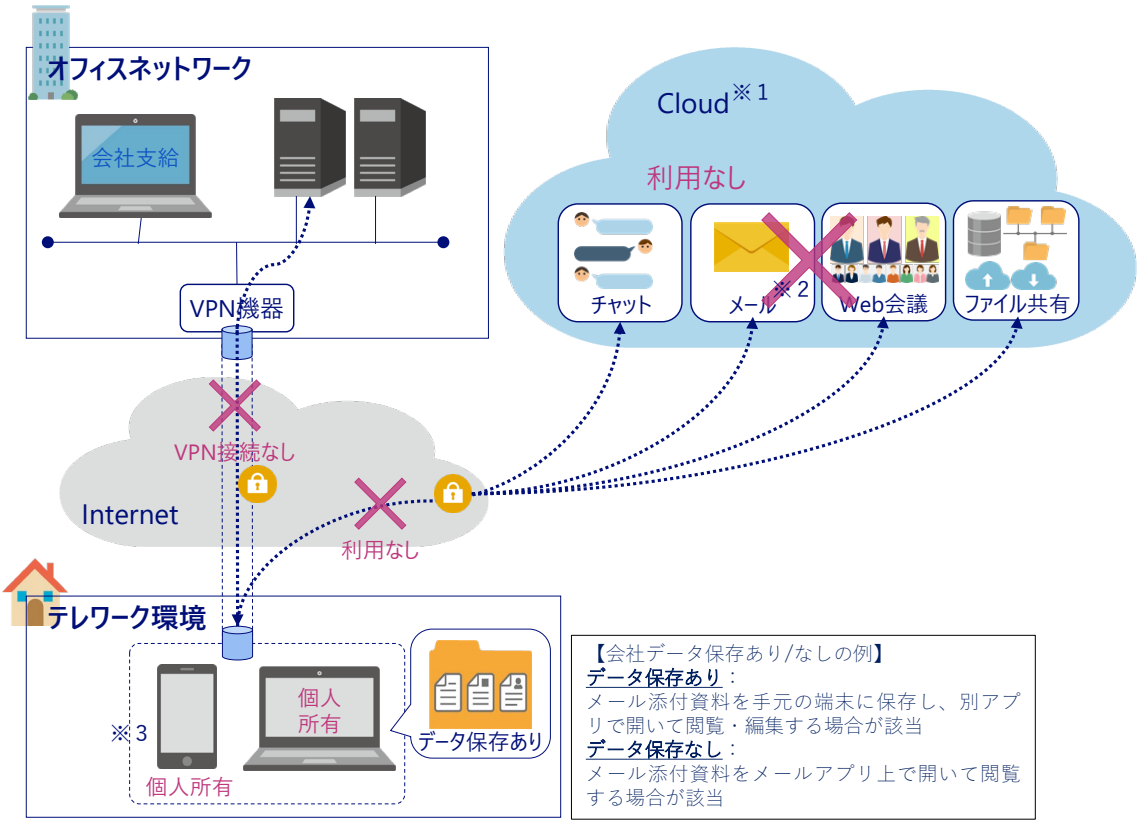


※1 「クラウドサービスを利用」は全部又は一部を利用しているケースが該当
※2 プロバイダー提供のメール利用もクラウドサービスに該当
※3 タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

方式⑦　個人所有端末・スタンドアロン方式

個人所有のテレワーク端末に外部記録媒体等でデータを持ち運び、テレワーク中は保存しておいたデータを処理することで業務を実施します。

スタンドアロン方式では、ネットワークに接続しないことから、オフィスネットワークに接続せず、クラウドサービスも利用しないことが特徴です。

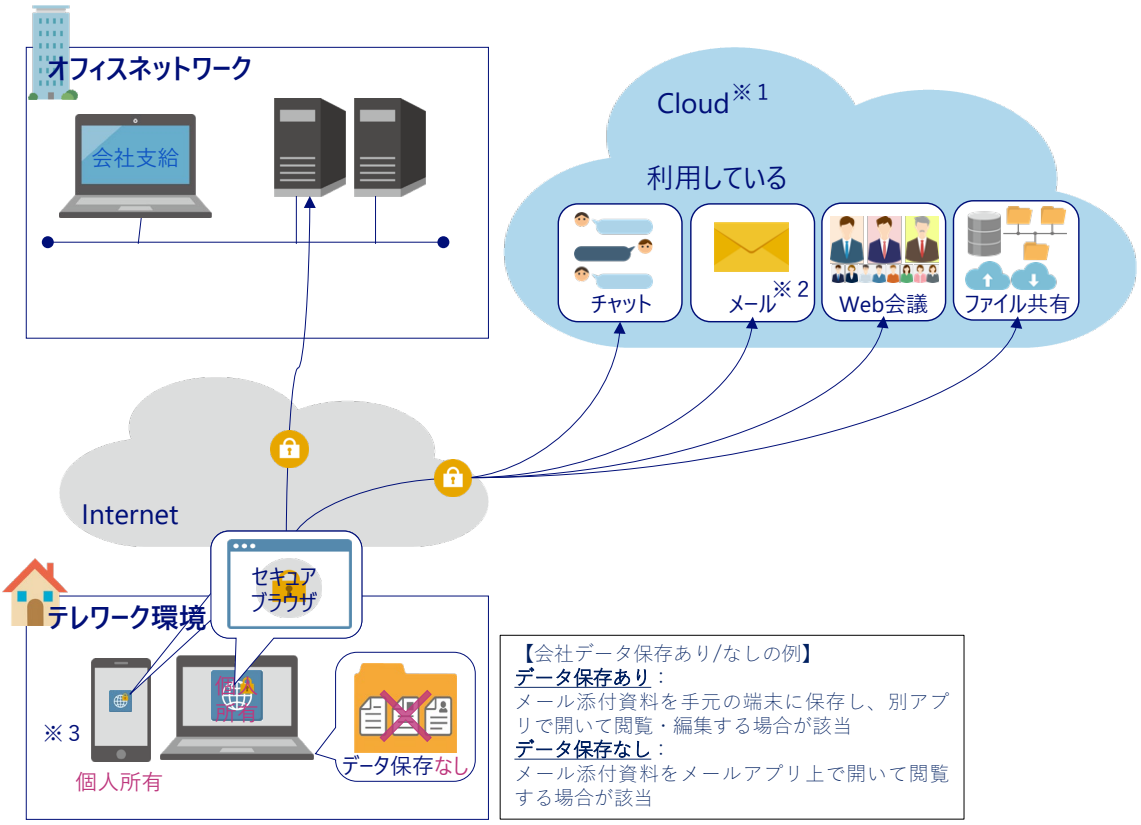


※1 「クラウドサービスを利用」は全部又は一部を利用しているケースが該当
※2 プロバイダー提供のメール利用もクラウドサービスに該当
※3 タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

方式⑧　個人所有端末・セキュアブラウザ方式

個人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、オフィスネットワーク内の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に接続して業務を実施します。

セキュアブラウザ方式では、端末へのデータ保存をしないことが特徴です。また、セキュアブラウザに対応した限定された業務のみをテレワークで実施します。



※1 「クラウドサービスを利用」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 タブレットやスマートフォンのアプリでメール等を利用する場合も「クラウドサービスを利用」に該当

第１部３．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理解を深めるために、各脅威の概要に加え、脅威が顕在化する流れや顕在化による業務影響を解説しています。なお、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いやすいような記載としています。

各脅威は、典型的な攻撃手法を例として、起因・過程・被害の３つのステップに分けて解説しています。また、「第２部１．セキュリティ対策チェックリスト」（p.29～）に示すチェックリストの各対策項目が、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についても併せて記載しています（特定のステップの場合のみに有効な対策については、当該ステップを括弧書きで記載しています。）。

(1) マルウェア感染

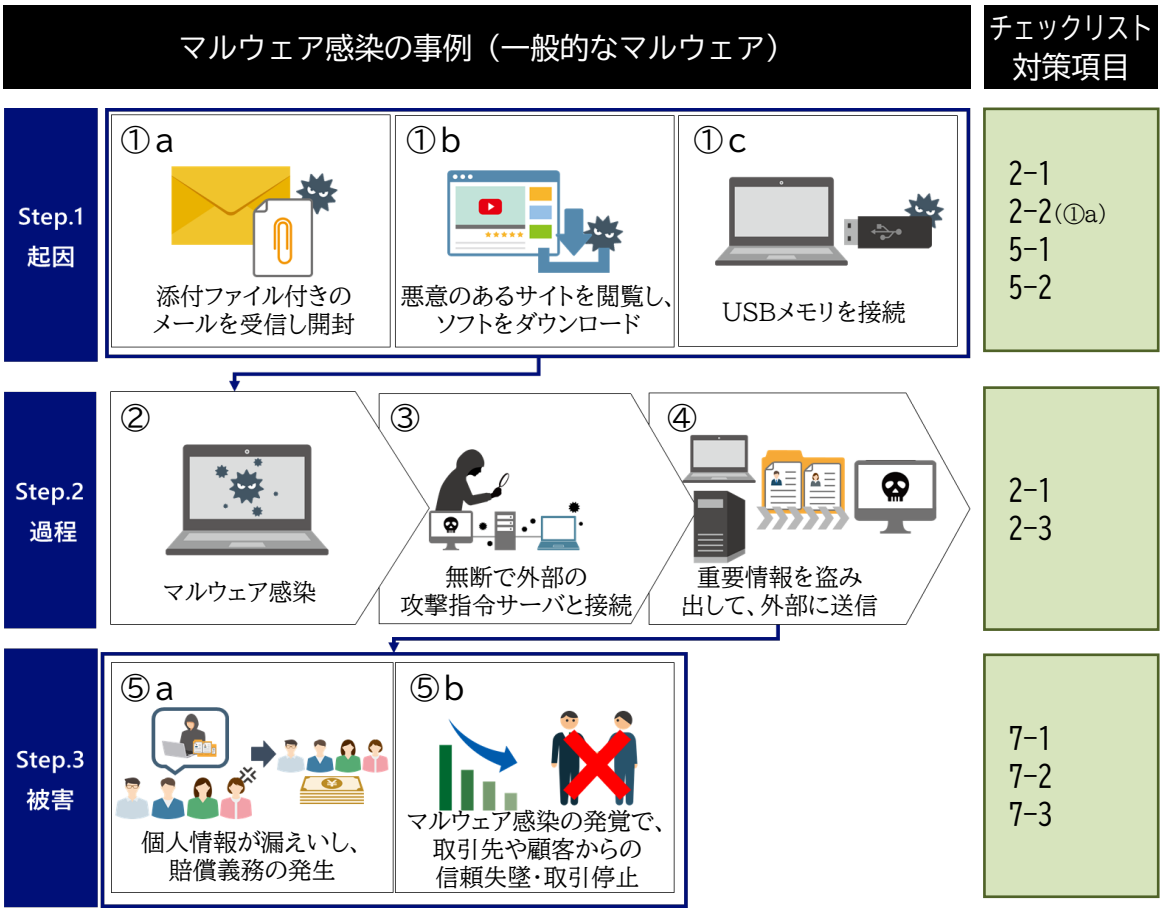
マルウェアとは、不正かつ有害な動作を行う目的で作成された悪意のあるソフトウェアや悪質なプログラムの総称です。一般的に「コンピュータウイルス」と呼ばれるものもマルウェアの一種に該当します。

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。

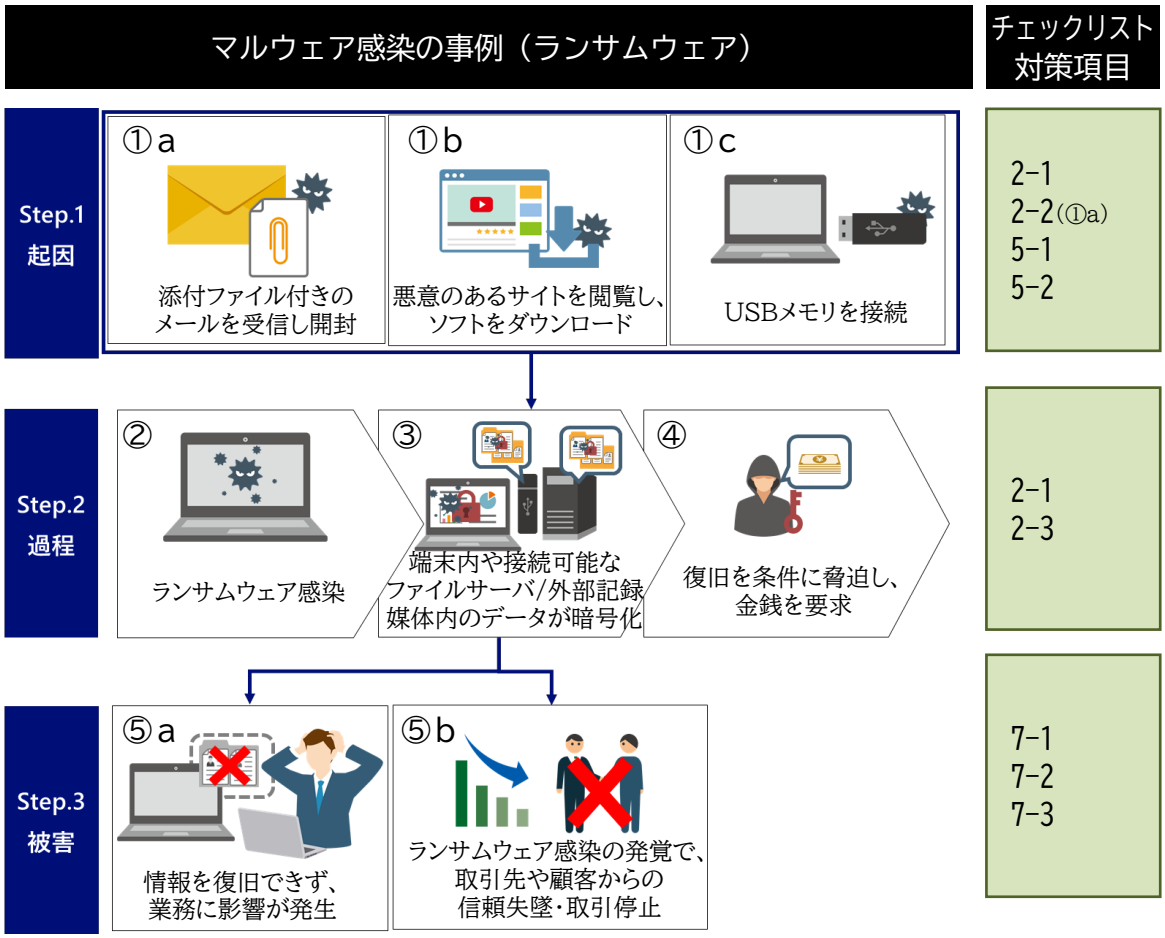
マルウェア感染とは、悪意あるソフトウェアや悪質なプログラムが、使用している端末やソフトウェアに組み込まれることを指します。

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「情報漏えい」、また、自組織の機器が第三者に対する攻撃に悪用されることで、「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、当該端末を通じてファイルサーバや外付けハードディスク等の外部記録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の身代金を要求しますが、身代金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犯罪者に利益供与を行ったと見なされてしまうこともあるため、支払いに応じることは推奨されません。



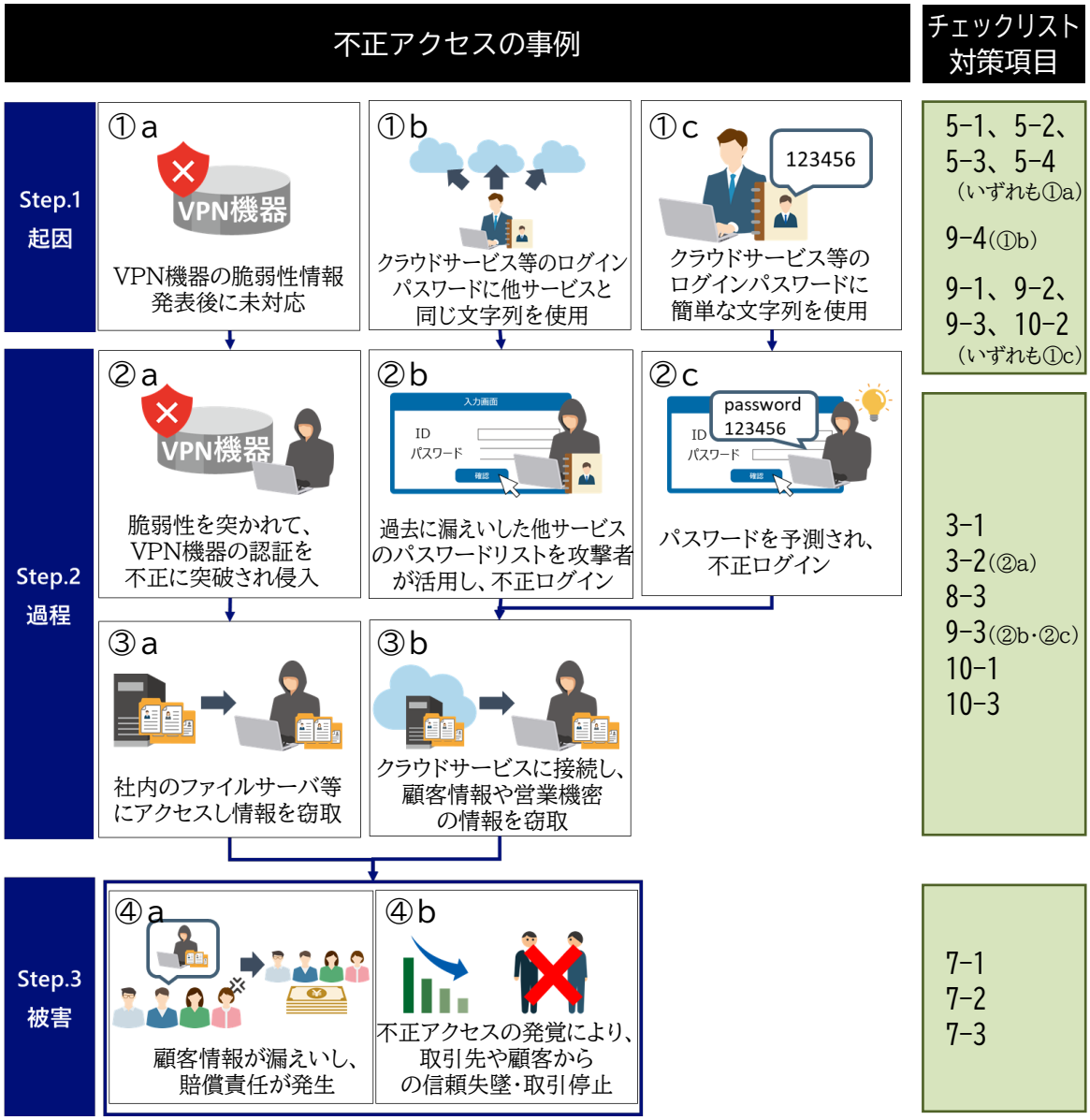
マルウェアによる攻撃は高度化しているため、本事例で紹介している方法である、添付ファイルの開封やソフトウェアのダウンロード等の操作を明示的にしていない場合であっても、マルウェアに感染する場合があります。


マルウェア感染の事例（ランサムウェア）
チェックリスト
対策項目
Step.1
起因
①a
添付ファイル付きの
メールを受信し開封
①b
悪意のあるサイトを閲覧し、
ソフトをダウンロード
①c
USBメモリを接続
2-1
2-2(①a)
5-1
5-2
Step.2
過程
②
ランサムウェア感染
③
端末内や接続可能な
ファイルサーバ/外部記録
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
2-1
2-3
Step.3
被害
⑤a
情報を復旧できず、
業務に影響が発生
⑤b
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
7-1
7-2
7-3

(2) 不正アクセス

不正アクセスは、コンピュータのOSやアプリケーション、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や、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が該当します。

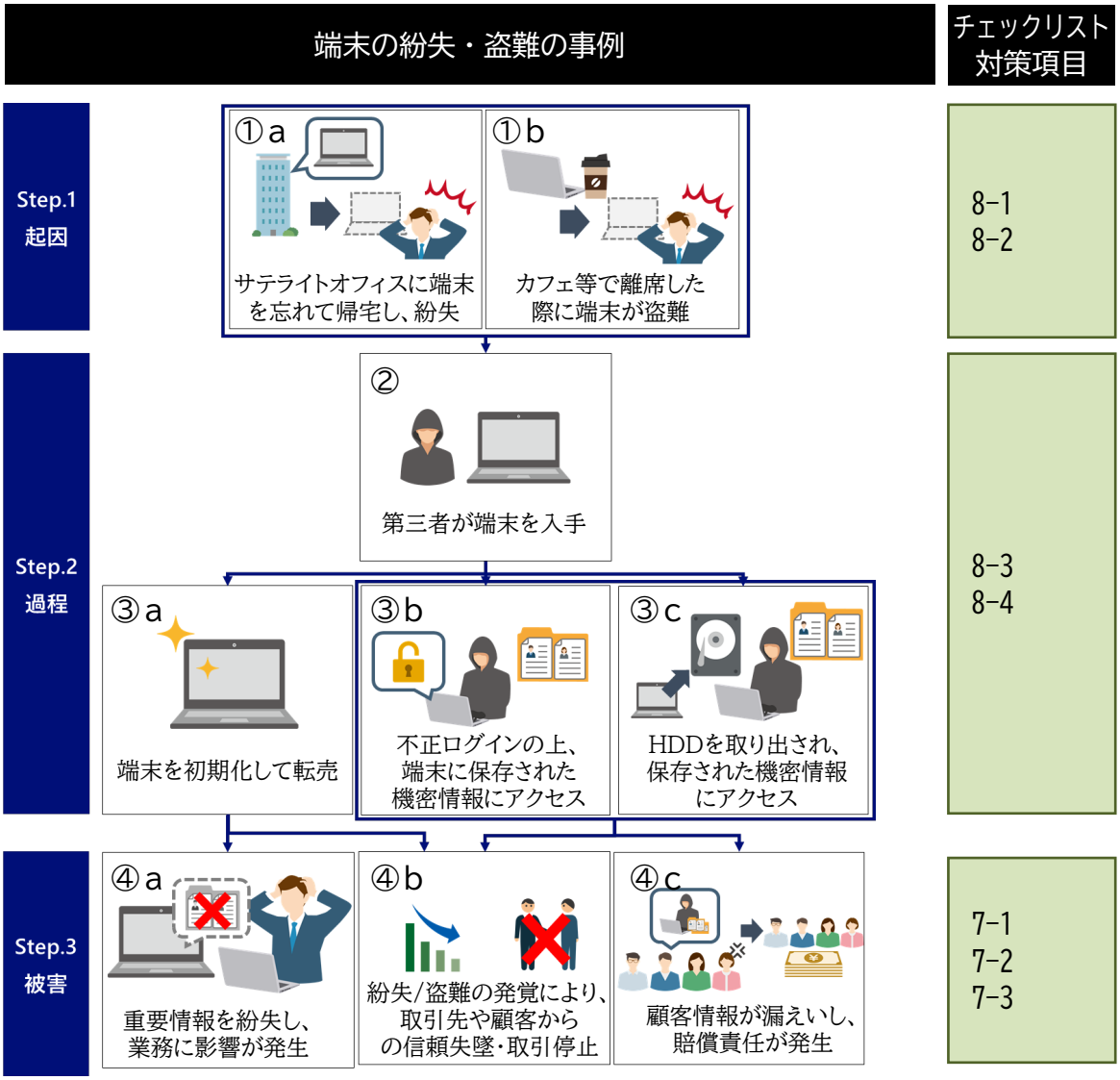
不正アクセスをされた場合、「情報漏えい」の発生や、情報漏えいに伴う「賠償責任」の発生、また、取引先や顧客からの「信頼失墜」や「取引停止」となる可能性があります。



(3) 端末の紛失・盗難

テレワーク端末をなくしてしまうこと、又は物理的に第三者に盗まれることを指します。

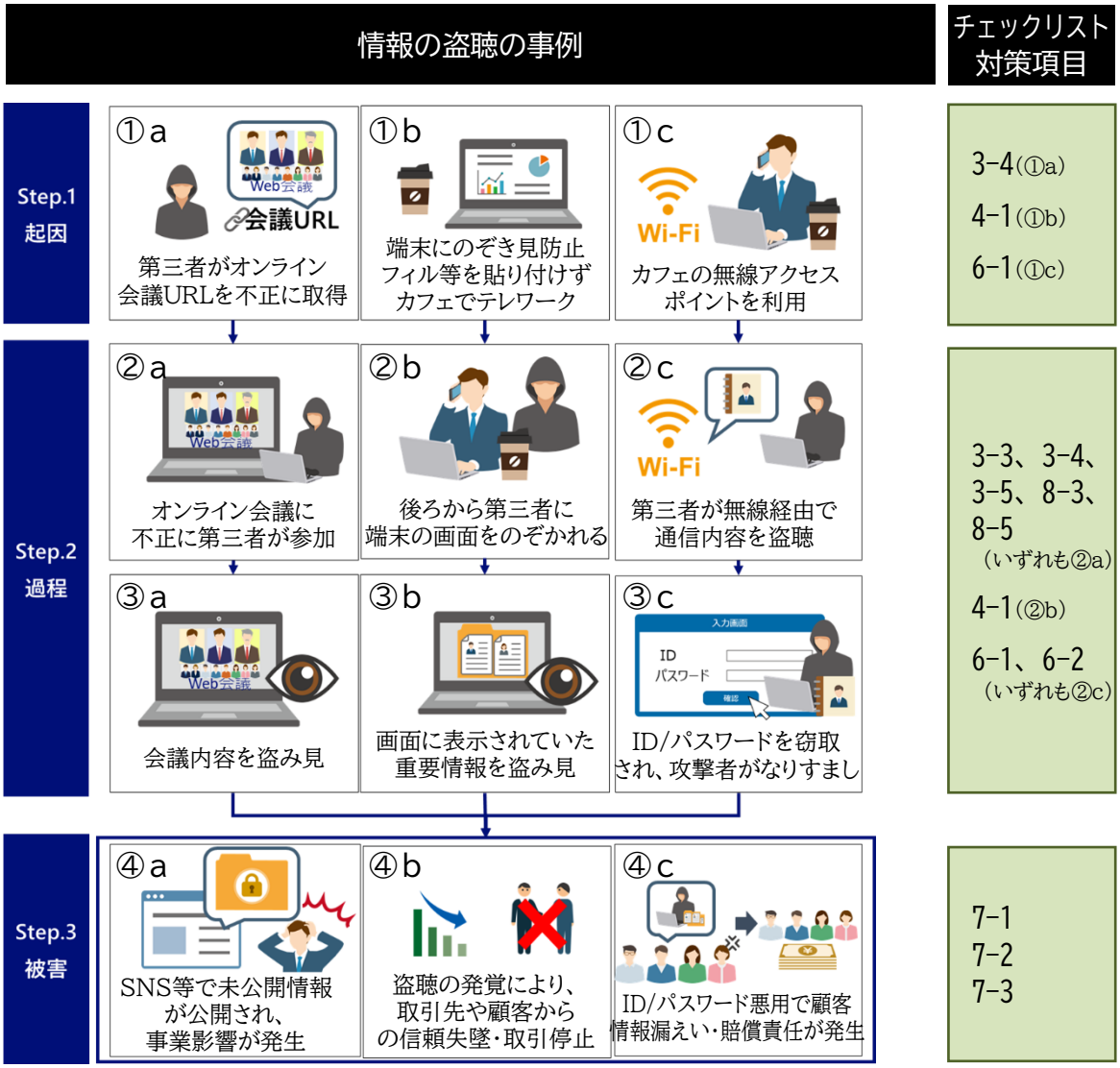
盗難・紛失にあった場合、「情報漏えい」の発生や、情報漏えいに伴う「賠償責任」の発生、また、取引先や顧客からの「信頼失墜」や「取引停止」となる可能性があります。



（4） 情報の盗聴

インターネット等の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、端末をのぞき見られることを指します。

情報の盗聴にあった場合、「情報漏えい」の発生や、情報漏えいに伴う「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。



第２部１．セキュリティ対策チェックリスト

中小企業等の担当者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、次ページ以降に、チェックリストとしてセキュリティ対策事項を具体的に示しています。

また、セキュリティ対策について、優先度の高いものから効率的に着手・実施できるよう、優先度ごとにチェックリストを示します。優先度の区分は次のとおりです。

優先度：◎

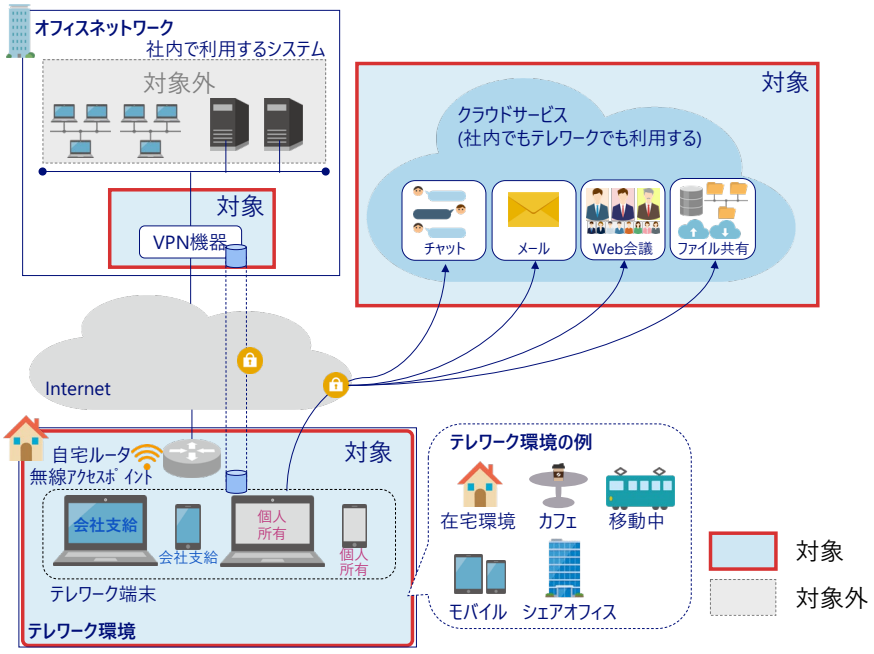
セキュリティ対策の**重要性が高い**（実施することによる効果が高い）もののうち、**実施難易度が低い**（専門知識、追加コストの観点で懸念が小さい）もの。

優先度：○

セキュリティ対策の**重要性が高い**（実施することによる効果が高い）もののうち、**実施難易度が中程度**（ITセキュリティに関する知識が必要であるが、実施困難ではない）のもの。

また、セキュリティ対策の**重要性が中程度**（実施することによりある程度の効果が期待できる）もののうち、**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）ものも対象です。

なお、本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[3]で、具体的には下図のとおりです。



[3] テレワークの導入有無に関わらず利用するシステム（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いないため、別途セキュリティ対策を検討していただくことを推奨します。

方式①　会社支給端末・VPN/リモートデスクトップ方式

優先度：◎の事項

No.	分類	対策内容	想定脅威
1-1	資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク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・構成管理	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　営業秘密等の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等の管理責任を伴う情報	不正アクセス 情報の盗聴
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、又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
3-1	アクセス制御・認可	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	物理セキュリティ	テレワーク端末に対してのぞ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・ログ管理	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、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、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（スマートフォン等）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	アカウント・認証管理	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	アカウント・認証管理	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：〇の事項

No.	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し、メールに記載されているURLをクリックしたり、添付されているファイルを開いたりしないよう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（スマートフォン等）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
3-2	アクセス制御・認可	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、社内ネットワークとインターネットの境界に設置されているファイアウォールやルーター等において、不要なポートへの通信や必要なIPアドレス以外からの通信を遮断している。	不正アクセス
3-3	アクセス制御・認可	オンライン会議の主催者はミーティングの開始時及び途中参加者がいる場合に、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・認可	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必要なメンバーだけに伝えるようにしている。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・認可	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無線LANルーター等のネットワーク機器は、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	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（特にID・パスワード等を入力するとき）は、暗号化されている（HTTPS通信である）ことと、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	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化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・ログ管理	テレワーク端末と接続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・ログ管理	テレワーク端末からオフィスネットワークに接続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（スマートフォン等）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　Mobile Device Managementの略称で、スマートフォン等を一元的に管理・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※4等の内蔵された記録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録媒体の一つで、「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録媒体 ※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
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サービス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	アカウント・認証管理	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、それ以上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	アカウント・認証管理	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

方式②　会社支給端末・クラウドサービス方式

優先度：◎の事項

No.	分類	対策内容	想定脅威
1-1	資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク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・構成管理	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　営業秘密等の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等の管理責任を伴う情報	不正アクセス 情報の盗聴
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、又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
3-1	アクセス制御・認可	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	物理セキュリティ	テレワーク端末に対してのぞ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・ログ管理	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、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、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（スマートフォン等）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	アカウント・認証管理	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	アカウント・認証管理	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：○の事項

No.	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し、メールに記載されているURLをクリックしたり、添付されているファイルを開いたりしないよう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（スマートフォン等）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
3-3	アクセス制御・認可	オンライン会議の主催者はミーティングの開始時及び途中参加者がいる場合に、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・認可	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必要なメンバーだけに伝えるようにしている。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・認可	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無線LANルーター等のネットワーク機器は、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	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（特にID・パスワード等を入力するとき）は、暗号化されている（HTTPS通信である）ことと、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	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化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・ログ管理	テレワーク端末と接続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（スマートフォン等）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 Mobile Device Managementの略称で、スマートフォン等を一元的に管理・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※4等の内蔵された記録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録媒体の一つで、「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録媒体 ※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
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サービス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	アカウント・認証管理	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、それ以上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	アカウント・認証管理	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

方式③　会社支給端末・スタンドアロン方式

優先度：◎の事項

No.	分類	対策内容	想定脅威
1-1	資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク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・構成管理	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　営業秘密等の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等の管理責任を伴う情報	不正アクセス 情報の盗聴
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、又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
3-1	アクセス制御・認可	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	物理セキュリティ	テレワーク端末に対してのぞ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・ログ管理	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、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、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（スマートフォン等）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	アカウント・認証管理	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	アカウント・認証管理	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：○の事項

No.	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（スマートフォン等）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
5-3	脆弱性管理	テレワークで利用する自宅の無線LANルーター等のネットワーク機器は、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	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化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・ログ管理	テレワーク端末と接続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（スマートフォン等）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　Mobile Device Managementの略称で、スマートフォン等を一元的に管理・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※4等の内蔵された記録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録媒体の一つで、「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録媒体 ※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
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サービス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	アカウント・認証管理	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、それ以上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	アカウント・認証管理	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

方式④　会社支給端末・セキュアブラウザ方式

優先度：◎の事項

No.	分類	対策内容	想定脅威
1-1	資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク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・構成管理	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　営業秘密等の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等の管理責任を伴う情報	不正アクセス 情報の盗聴
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、又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
3-1	アクセス制御・認可	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	物理セキュリティ	テレワーク端末に対してのぞ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・ログ管理	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、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、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（スマートフォン等）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	アカウント・認証管理	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	アカウント・認証管理	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：〇の事項

No.	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し、メールに記載されているURLをクリックしたり、添付されているファイルを開いたりしないよう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（スマートフォン等）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
3-2	アクセス制御・認可	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、社内ネットワークとインターネットの境界に設置されているファイアウォールやルーター等において、不要なポートへの通信や必要なIPアドレス以外からの通信を遮断している。	不正アクセス
3-3	アクセス制御・認可	オンライン会議の主催者はミーティングの開始時及び途中参加者がいる場合に、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・認可	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必要なメンバーだけに伝えるようにしている。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・認可	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無線LANルーター等のネットワーク機器は、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	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（特にID・パスワード等を入力するとき）は、暗号化されている（HTTPS通信である）ことと、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	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化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・ログ管理	テレワーク端末と接続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・ログ管理	テレワーク端末からオフィスネットワークに接続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（スマートフォン等）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　Mobile Device Managementの略称で、スマートフォン等を一元的に管理・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	アカウント・認証管理	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、それ以上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	アカウント・認証管理	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

方式⑤　個人所有端末・VPN/リモートデスクトップ方式

優先度：◎の事項

No.	分類	対策内容	想定脅威
1-1	資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク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・構成管理	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　営業秘密等の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等の管理責任を伴う情報	不正アクセス 情報の盗聴
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、又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
3-1	アクセス制御・認可	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	物理セキュリティ	テレワーク端末に対してのぞ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・ログ管理	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、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、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（スマートフォン等）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	アカウント・認証管理	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	アカウント・認証管理	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：〇の事項

No.	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し、メールに記載されているURLをクリックしたり、添付されているファイルを開いたりしないよう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（スマートフォン等）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
3-2	アクセス制御・認可	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、社内ネットワークとインターネットの境界に設置されているファイアウォールやルーター等において、不要なポートへの通信や必要なIPアドレス以外からの通信を遮断している。	不正アクセス
3-3	アクセス制御・認可	オンライン会議の主催者はミーティングの開始時及び途中参加者がいる場合に、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・認可	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必要なメンバーだけに伝えるようにしている。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・認可	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無線LANルーター等のネットワーク機器は、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	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（特にID・パスワード等を入力するとき）は、暗号化されている（HTTPS通信である）ことと、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	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化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・ログ管理	テレワーク端末と接続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・ログ管理	テレワーク端末からオフィスネットワークに接続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（スマートフォン等）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　Mobile Device Managementの略称で、スマートフォン等を一元的に管理・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※4等の内蔵された記録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録媒体の一つで、「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録媒体 ※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
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サービス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	アカウント・認証管理	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

方式⑥　個人所有端末・クラウドサービス方式

優先度：◎の事項

No.	分類	対策内容	想定脅威
1-1	資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク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・構成管理	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　営業秘密等の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等の管理責任を伴う情報	不正アクセス 情報の盗聴
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、又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
3-1	アクセス制御・認可	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	物理セキュリティ	テレワーク端末に対してのぞ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・ログ管理	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、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、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（スマートフォン等）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	アカウント・認証管理	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	アカウント・認証管理	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：○の事項

No.	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し、メールに記載されているURLをクリックしたり、添付されているファイルを開いたりしないよう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（スマートフォン等）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
3-3	アクセス制御・認可	オンライン会議の主催者はミーティングの開始時及び途中参加者がいる場合に、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・認可	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必要なメンバーだけに伝えるようにしている。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・認可	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無線LANルーター等のネットワーク機器は、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	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（特にID・パスワード等を入力するとき）は、暗号化されている（HTTPS通信である）ことと、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	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化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・ログ管理	テレワーク端末と接続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（スマートフォン等）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 Mobile Device Managementの略称で、スマートフォン等を一元的に管理・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※4等の内蔵された記録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録媒体の一つで、「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録媒体 ※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
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サービス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	アカウント・認証管理	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

方式⑦　個人所有端末・スタンドアロン方式

優先度：◎の事項

No.	分類	対策内容	想定脅威
1-1	資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク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・構成管理	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　営業秘密等の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等の管理責任を伴う情報	不正アクセス 情報の盗聴
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、又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
3-1	アクセス制御・認可	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	物理セキュリティ	テレワーク端末に対してのぞ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・ログ管理	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、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、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（スマートフォン等）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	アカウント・認証管理	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	アカウント・認証管理	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：○の事項

No.	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（スマートフォン等）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
5-3	脆弱性管理	テレワークで利用する自宅の無線LANルーター等のネットワーク機器は、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	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化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・ログ管理	テレワーク端末と接続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（スマートフォン等）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　Mobile Device Managementの略称で、スマートフォン等を一元的に管理・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※4等の内蔵された記録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録媒体の一つで、「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録媒体 ※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
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サービス内に保存するケースは対象外	不正アクセス 盗難・紛失
9-4	アカウント・認証管理	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

方式⑧　個人所有端末・セキュアブラウザ方式

優先度：◎の事項

No.	分類	対策内容	想定脅威
1-1	資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク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・構成管理	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　営業秘密等の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等の管理責任を伴う情報	不正アクセス 情報の盗聴
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、又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
3-1	アクセス制御・認可	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	物理セキュリティ	テレワーク端末に対してのぞ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・ログ管理	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、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、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（スマートフォン等）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	アカウント・認証管理	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	アカウント・認証管理	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：〇の事項

No.	分類	対策内容	想定脅威	方式⑧
2-2	マルウェア対策	不審なメールの開封し、メールに記載されているURLをクリックしたり、添付されているファイルを開いたりしないよう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（スマートフォン等）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	✓
3-2	アクセス制御・認可	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、社内ネットワークとインターネットの境界に設置されているファイアウォールやルーター等において、不要なポートへの通信や必要なIPアドレス以外からの通信を遮断している。	不正アクセス	✓
3-3	アクセス制御・認可	オンライン会議の主催者はミーティングの開始時及び途中参加者がいる場合に、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・認可	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必要なメンバーだけに伝えるようにしている。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・認可	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無線LANルーター等のネットワーク機器は、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	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（特にID・パスワード等を入力するとき）は、暗号化されている（HTTPS通信である）ことと、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	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化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・ログ管理	テレワーク端末と接続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・ログ管理	テレワーク端末からオフィスネットワークに接続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（スマートフォン等）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　Mobile Device Managementの略称で、スマートフォン等を一元的に管理・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	アカウント・認証管理	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	✓

第２部２．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次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

- ○ CiscoWebexMeetings
- ○ Microsoft Teams
- ○ Zoom
- ○ Windows
- ○ Mac
- ○ iOS
- ○ Android
- ○ LanScope An
- ○ Exchange Online
- ○ Gmail
- ○ Teams_chat
- ○ LINE
- ○ OneDrive
- ○ Googleドライブ
- ○ Dropbox
- ○ YAMAHA VPNルータ
- ○ CiscoASA
- ○ Windowsリモートデスクトップ接続
- ○ Chromeリモートデスクトップ
- ○ Microsoft Defender
- ○ ウイルスバスター ビジネスセキュリティサービス

設定解説資料は次のURLで掲載します。
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

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。

第２部３．セキュリティ対策と想定脅威一覧

「第２部１．セキュリティ対策チェックリスト」（p.29～）でテレワーク方式ごとに示したセキュリティ対策を一覧表の形で示します。「対策内容」「想定脅威」「優先度」「方式ごとの対策要否」のほか、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・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク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	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。 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、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・構成管理	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　営業秘密等の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等の管理責任を伴う情報	不正アクセス 情報の盗聴	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。 テレワークで実施している業務やその際に利用しているシステム、そして、テレワークで取り扱う重要情報について把握していない場合、システムを適正な利用者が利用しているのか、またデータ管理等に関する各種セキュリティ対策が十分であるかといった懸念が増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓
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、又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。	◎		✓	✓	✓	✓	✓	✓	✓	✓

53

2-2	マルウェア対策	不審なメールの開封し、メールに記載されているURLをクリックしたり、添付されているファイルを開いたりしないよう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に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窃取されるリスクが増加する。 また、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（スマートフォン等）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が含まれている可能性があるため、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・認可	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が不正利用されたり、利用者が操作ミスをしたりすることにより重要情報が流出するリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓	✓
3-2	アクセス制御・認可	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、社内ネットワークとインターネットの境界に設置されているファイアウォールやルーター等において、不要なポートへの通信や必要なIPアドレス以外からの通信を遮断している。	不正アクセス	不要なポートや必要なIPアドレス以外からの通信が遮断されていない場合、それらを狙った悪意のある攻撃（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。	○	オフィスネットワークに接続しない場合は対象外	✓	×	×	✓	✓	×	×	✓
3-3	アクセス制御・認可	オンライン会議の主催者はミーティングの開始時及び途中参加者がいる場合に、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がいる場合に本人確認を実施しないことにより、会議に不適切な利用者が不正に参加していることに気付くことができず、情報漏えいのリスクが増加する。 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	✓	✓	×	✓	✓	✓	×	✓
3-4	アクセス制御・認可	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必要なメンバーだけに伝えるようにしている。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URLやパスワードを、必要ない利用者に伝えることで、会議に不適切な利用者が不正に参加し、会議を通じた情報漏えいのリスクが増加する。 また、パスワードの設定を強制しない（できない）場合は、利用者がパスワードを未設定にしたり、容易に推測可能なパスワードを設定したりすることにより、会議への不正参加のリスクが増加する。	○	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	✓	✓	×	✓	✓	✓	×	✓
3-5	アクセス制御・認可	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、会議主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	物理セキュリティ	テレワーク端末に対してのぞ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、家族を含む業務と関係ない人物が、物理的にテレワーク端末をのぞき見（ショルダーハッキング）することが比較的容易な環境であることが懸念される。のぞ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えいや不正利用のリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓	✓

54

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無線LANルーター等のネットワーク機器は、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	自宅に設置する無線LANルーター等のネットワーク機器について、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加する。	○		✓	✓	✓	✓	✓	✓	✓	✓
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、インターネットに常時接続され、オフィスネットワークへの入り口となる。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、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加する。	◎		✓	×	×	×	✓	×	×	×
6-1	通信暗号化	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（特にID・パスワード等を入力するとき）は、暗号化されている（HTTPS通信である）ことと、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	無線LANを利用したり、自宅外でテレワークを行ったりするときに、通信内容が暗号化されていない場合、悪意のある第三者による通信の傍受により情報漏えい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	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化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	公衆無線LANや自宅設置の無線LANのセキュリティ方式としてWPA2やWPA3以外（WEP・WPA）を利用している場合、悪意のある第三者が通信の傍受することで、通信内容を盗み見られ、情報漏えいするリスクが増加する。 無線LAN使用時のセキュリティ確保（セキュリティ方式の詳細を含む。）については、総務省が公表している、「無線LAN（Wi-Fi）のセキュリティに関するガイドライン」を参考にしてください。 https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/	○		✓	✓	✓	✓	✓	✓	✓	✓
7-1	インシデント対応・ログ管理	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、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、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手順や、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。 また、迅速な初動を行うため、インシデントが発生したとわかったときだけでなく、そのおそれがあるときから、積極的に情報連絡を行うことを周知しておく必要がある。	◎		✓	✓	✓	✓	✓	✓	✓	✓
7-2	インシデント対応・ログ管理	テレワーク端末と接続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	テレワーク端末と接続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。	○		✓	✓	✓	✓	✓	✓	✓	✓

55

7-3	インシデント対応・ログ管理	テレワーク端末からオフィスネットワークに接続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オフィスネットワークに接続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。	○	オフィスネットワーク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（スマートフォン等）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や盗難のリスクが高い。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えいのリスクが増加する。	◎	スマートフォン等のみ対象	✓	✓	✓	✓	✓	✓	✓	✓
8-2	データ保護	テレワーク端末（スマートフォン等）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 Mobile Device Managementの略称で、スマートフォン等を一元的に管理・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や盗難のリスクが高い。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えいのリスクが増加する。	○	スマートフォン等のみ対象	✓	✓	✓	✓	✓	✓	✓	✓
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等の内蔵された記録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録媒体の一つで、「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録媒体 ※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、テレワーク端末の紛失や盗難のリスクが高い。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サービス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、テレワーク端末の紛失や盗難のリスクが高い。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えい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	オンライン会議について、適切なルールを遵守しないと、公開情報（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等を誤操作による共有してしまう、会議の録画ファイルが不適切な第三者に参照される、等による情報漏えい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えいリスクの増加が発生する。	○	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	✓	✓	×	✓	✓	✓	×	✓

56

9-1	アカウント・認証管理	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るリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓
9-2	アカウント・認証管理	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るリスクが増加する。	◎		✓	✓	✓	✓	✓	✓	✓	✓
9-3	アカウント・認証管理	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、それ以上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ときにパスワード入力がそれ以上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るリスクが増加する。	○	個人所有端末については業務用途以外にも利用されるため対象外とする。	✓	✓	✓	✓	×	×	×	×
9-4	アカウント・認証管理	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・パスワード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るリスクが増加する。	○		✓	✓	✓	✓	✓	✓	✓	✓
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、業務上必要でないにも関わらず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、重要情報の漏えいリスクの増加や、誤操作による情報漏えいのリスクが増加する。	○		✓	✓	✓	✓	✓	✓	✓	✓
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、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るリスクが増加する。	○		✓	✓	✓	✓	✓	✓	✓	✓
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に管理者権限を利用することで、管理者権限でマルウェア感染することで重要情報に直接アクセスされてしまうなど、誤操作による情報漏えいのリスクが増加する。また、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ことが困難になる。	○	個人所有端末については業務用途以外にも利用されるため対象外とする。	✓	✓	✓	✓	×	×	×	×

57

参考１　用語集（キーワード解説）

用語集

用語	解説
OS	Operating Systemの略称。PCやスマートフォン等を動作させる基本的なソフトウェア。（例：Windows、iOS、Android）
VPN	Virtual Private Networkの略称。あたかもオフィスネットワーク内部にいるかのように、自宅や外出先などの遠隔の場所から安全にオフィスネットワークに接続可能な技術のことです。
アクセスログ	サーバやネットワーク機器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、オフィスネットワーク内のPCやサーバで保存・管理していたようなソフトウェアやデータを、オフィスネットワーク内ではなくインターネット上で保存・管理し、利用者は、インターネットを通じていつでもどこでも利用できるようにしたサービス。 本書では、メール、チャット、オンライン会議、ファイル共有等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。
脆弱性 （ぜいじゃくせい）	機器やシステム等におけるセキュリティ上の欠陥のこと。機器やシステム等の設計や開発・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	特殊なインターネットブラウザで、端末側にデータを残さずに利用することができます。閲覧した情報を端末に保存できないようにする機能や、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、接続先制限を行えるものもあります。 クラウドサービスやオフィスネットワーク上のシステムに接続する際に利用することで、情報漏えい等に備えたデータ管理が容易になります。
セキュリティアップデート	ソフトウェアのうち、セキュリティに関して不具合のある部分を、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。

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。
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。サーバ上のソフトウェアでファイアウォールの機能が実装されている場合や、専用の機器（ハードウェア）で機能が実装されている場合のいずれもがあります。
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。
マルウェア	ウイルス、ワーム、トロイの木馬等の悪意のあるソフトウェアの総称。PCやスマートフォン等の機器において、それらの機器所有者による認知のないままに感染し、機器本来の動作の妨害やデータの破壊、データの外部への送出等、機器所有者の望まない活動を行う。
リモートデスクトップ	オフィスネットワークに置いてあるPCの画面を、インターネット経由でテレワーク端末のPCに転送して表示した上で、テレワーク端末のPCからオフィスネットワークに置いてあるPCを遠隔操作する技術。
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。

「MDM」について

MDMとは、Mobile Device Managementの略称で、スマートフォン等を一元的に管理・運用すること、又はその機能を提供するソフトウェアのことを指します。

MDMを導入する必要性

MDMを導入することで、セキュリティ設定等を強制することが可能となるため、テレワーク端末に対するセキュリティ統制の強化に役立ちます。また、テレワーク端末の紛失・盗難時においても、端末内に保存されているデータを保護等し、データ漏えい防止に役立ちます。

なお、MDMでどこまでセキュリティ設定等の強制が可能かといった点は、製品によって異なりますので、製品選定の際には求めている機能が利用可能か確認する必要があります。

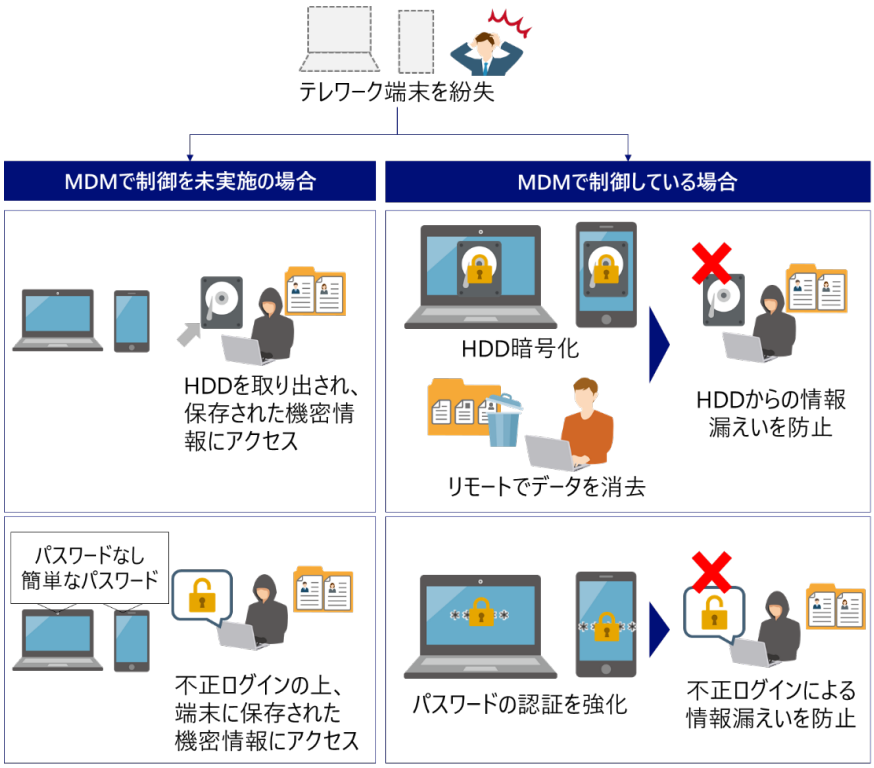
MDMの機能例

MDMの機能として次のようなものがあります。

〇内蔵記録装置（HDD等）暗号化：紛失・盗難等によりテレワーク端末が第三者に渡ってしまった場合でも、データの漏えいを防ぐことができます。

〇遠隔操作によるデータ消去：紛失・盗難等があった場合に、遠隔操作で端末のデータを消去することができるため、データの漏えいを防ぐことができます。

〇認証ポリシーの強制：端末にログインする際の認証について、ルール（パスワード設定方法等）を定めて適用（強制）することができます。



「各種連絡体制（インシデント発生時）」について

インシデント発生時に連絡をすべき連絡先と連絡内容について解説します。

連絡体制を整備する必要性

インシデントが発生した際に連絡すべき場所や内容を事前に連絡体制として確定しておくことが必要です。連絡体制を事前に定めていない場合、緊急時に適切な報告、連絡、相談などができなくなるおそれがあります。

事前に整理をすべき内容の例

事前に整理をしておく内容としては、以下のようなものがあります。

・連絡を取る必要がある組織内の関連部門や組織外の関係者
・法令で公的機関に報告を行う必要がある場合はその基準や内容
・連絡の際に報告すべき事項や連絡時のフォーマット
・連絡先（固定電話番号、緊急用電話番号等）

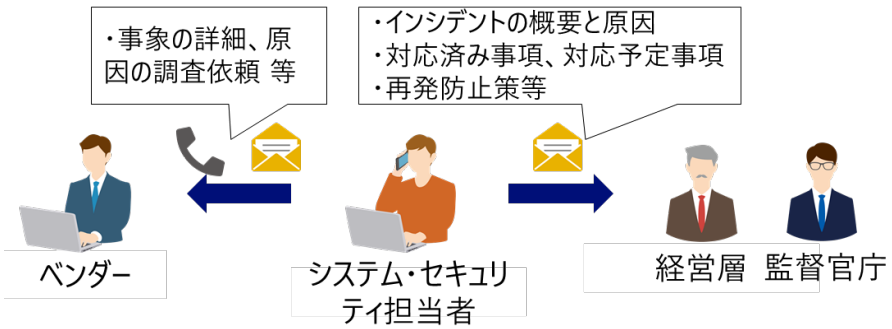
従業員が行うべき連絡の例

従業員が連絡すべき内容（氏名・部署名、発生事象、直前に実施した作業内容等）については、システム・セキュリティ管理者から従業員に対して、事前に周知を行っておくことが必要です。

システム・セキュリティ管理者が行うべき連絡の例

多様な関係者への報告を遅滞なく行うため、あらかじめ報告内容を整理しておく必要があります。

〇経営層への報告内容例：発生日時、漏えいした情報の内容・件数等、その他被害内容、発生原因、対応済み・対応予定事項、再発防止策
〇システムベンダーへの報告内容例：発生日時、漏えいした情報の内容・件数等、原因の調査依頼、対応済み・対応予定事項
〇監督官庁への報告内容例：企業名、発生日時、被害内容（漏えいした情報の内容・件数等）、発生原因、対応済み・対応予定事項、再発防止策



「管理者権限」について

管理者権限は、一般権限と比較してシステム上でより多くの操作を実行可能な権限のことを指します。システムの設定やプログラムの実行・インストールなどが可能です。

管理者権限を守る必要性

管理者権限は、各種システムの設定変更、アカウントの追加や権限変更、不正操作履歴の削除等の多くの操作が実行可能なことから、攻撃者の標的になりやすいです。

そのため、管理者権限の付与を業務上必要な担当者に限定し、必要なときだけ利用することや、強力なパスワード設定等により保護することが重要となります。

管理者権限の例

管理者権限と実施可能な操作内容の例は、次の通りです。

管理者権限の例	管理者権限で実施可能な内容
Active Directoryの管理者アカウント	ドメインに所属するユーザアカウントの追加・削除 ドメインに所属するユーザ端末のセキュリティ設定等の変更
WindowsのAdministrators	端末上のセキュリティ設定変更やアプリケーションのインストール等
Linuxのroot	
VPN機器のAdmin権限	VPNユーザアカウントの追加・削除 VPNユーザのアクセスルールの変更

「時刻同期」について

時刻同期とは、サーバやネットワーク機器等の内蔵時計を正しく合わせておくことをいいます。

時刻同期の必要性

サーバやネットワーク機器等などのアクセスログ等を取得しているシステムについては、時刻同期を行っておく必要があります。

時刻同期をしていない場合、ログを取得していたとしても、そのログの時刻が信用できないため、実際に行われた操作との因果関係がわからず、調査が行えない可能性があります。

時刻同期の方法

時刻同期には、NTPという専用のプロトコルを用いることが一般的です。設定項目でNTPサーバを設定できる場合は、信頼できるNTPサーバ（例えば独立行政法人情報通信研究機構（NICT）が提供している「ntp.nict.jp」）を指定しましょう。

なお、組織内の特定サーバをNTPサーバとして既に指定している場合はあえて変更する必要はありません。テレワーク環境では従来参照していたNTPサーバにアクセスできなくなっていることもありますので、注意が必要です。

また、Windowsの場合、初期状態ではMicrosoftが提供するNTPサーバを参照する設定になっているのが一般的であり、あえて設定変更は必要ないこともあります。

「システムによるアクセス制御」について

「システムによるアクセス制御」とは、利用者がシステムやデータ等に接続をしてもよいか、また、接続先で閲覧・作成・実行等を実施してよいかの制限をかけることを指します。

「システムによるアクセス制御」の実施方法のパターンと、各方法で実現できることを解説します。

システムによるアクセス制御を実施する必要性

アクセス制御が適切に設定されていない場合、守るべき情報について、業務上アクセスする必要のない者が閲覧、改ざん、持出し等が行える状態になっている可能性があります。

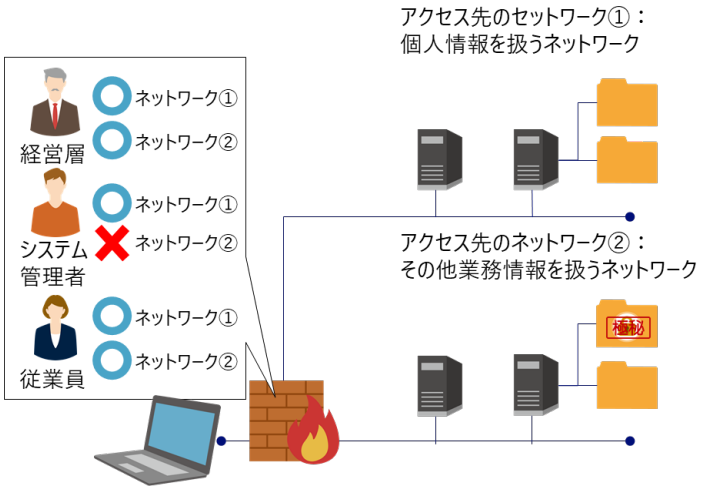
企業によっては、外部に送信・公開する情報の管理は適切に行われていても、オフィスネットワーク内に保管している情報については、厳密にアクセス制御がされていないこともあります。オフィスネットワーク内の情報であっても、本来アクセスすべきでない人がアクセス可能な状態となっている場合、仮に不正アクセスやマルウェア感染等が発生した際に、影響や被害の拡大につながるおそれがあることから、適切に制御を実施する必要があります。

アクセス制御の方法として３つの例を示します。自組織に適用できる場合は参考にしてください。

例１：ファイアウォールによってネットワーク間の通信を制御する場合

ネットワーク単位で、取り扱う情報レベルを分けて保管している場合には、各ネットワークの境界となるファイアウォールでIPアドレスや通信プロトコル等に基づいて、アクセス制御を実施することができます。

例えば、社内に「個人情報を扱うネットワーク①」と「その他の業務に用いる情報を扱うネットワーク②」というように複数のネットワークが存在する場合、各ネットワークの境界に設置されているファイアウォールの設定でアクセス制御を実施できます。



なお、同一ネットワーク内にアクセス制御レベルの異なるデータを複数持っている

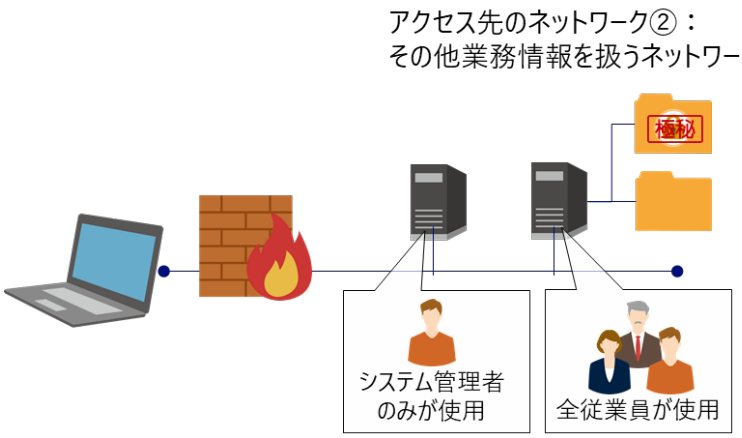
場合は、この例では完全には制御しきることができません。

例２：サーバのファイアウォール機能によって制御する場合

アクセス制御レベルの異なるサーバ（例えば管理者のみが使用するサーバと組織内全員が使用するサーバ）が同一ネットワーク上にある場合には、ファイアウォールによる通信制御だけでは十分に対応できません。

この場合には、サーバが持つファイアウォール機能を使い、IPアドレスや通信プロトコル等に基づいて制御することが可能です。

例えば、下図のネットワーク②において、管理者のみが使用するサーバと、全従業員が使用するファイルサーバがあるとします。この場合、端末からのアクセス制御は、ファイアウォールだけでは十分に行うことができません。そのため、管理者のみが使用するサーバに対して、例えば管理者用端末に割り振られたIPアドレスからの通信のみ許可するといたアクセス制御を実施することが必要となります。

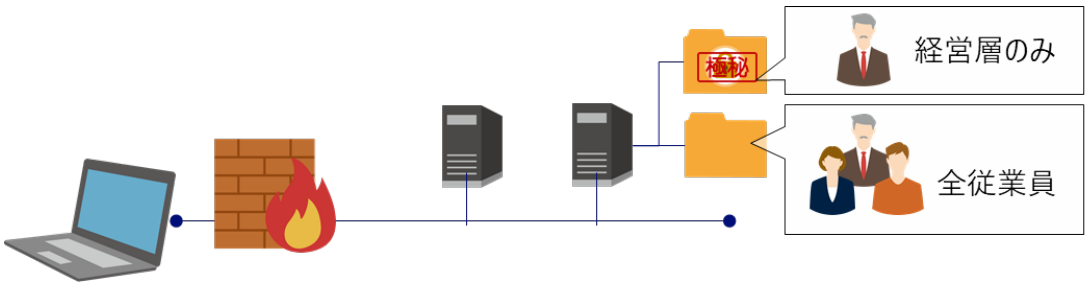


なお、同一のサーバ内に、アクセス制御レベルの異なるファイルやフォルダがある場合は、この例では完全に制御しきることができません。

例３：フォルダによって制御する場合

ファイルサーバの中で、役職や関係者単位でアクセス制御レベルを分けたい場合は、フォルダごとでのアクセス制御を実施することが可能です。

例えば、「経営層のみにアクセス許可するフォルダ」と「全従業員がアクセスできるフォルダ」というように様々な権限のフォルダが存在する場合、フォルダの設定でアクセス制御を実施できます。



「重要情報」について

本書において「重要情報」とは、営業秘密等の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等の管理責任を伴う情報を指します。

重要情報を管理する必要性

個人情報に該当しない場合でも、情報漏えい時に甚大な被害をもたらす情報もあります。そのため、自社における重要情報が何であるかを定義し、その情報が漏えいした際に、どの程度の損害が発生しうるかを想定した上で、組織内で保有している重要情報について事前に整理を行うことが必要となります。

自組織内で所有する情報だけで重要か否かを判断するのではなく、親会社や取引先等から間接的に受領したり、一時的に保有したりしている情報も含め情報の重要性を判断することが大切です。

攻撃者の中には、セキュリティ対策が堅牢な大企業を直接狙うのではなく、取引として関連のある企業等、セキュリティ対策の弱い間接的に接点のある環境を狙って侵害を計画するケースもあります。他組織に関する情報にも十分注意しましょう。

重要情報と情報漏えい時の影響例

重要情報とその情報が漏えいした際の影響例は、次の通りです。

重要情報の例	情報漏えい時の影響例
顧客の個人情報（例：氏名・住所・クレジットカード情報）	顧客から損害賠償を請求されることによる金銭被害の発生
自組織の機密情報（例：新規サービスの開発情報）	機密情報が漏えいしたことにより新規事業が停止し、売り上げの減少
自組織の従業員の認証情報（例：管理者権限のログイン情報）	社内システムへ不正アクセスされ、システム停止により機会損失の発生
親会社の機密情報や親会社に接続する際の認証情報（例：親会社に接続するための認証情報）	自社の環境を介して親会社の顧客情報にアクセスされ情報が漏えい 顧客や親会社から損害賠償等を請求されることによる金銭被害の発生

「対応手順（インシデント対応手順）」について

インシデントが発生した際に、対応手順としてどのようなことを実施すべきかを解説します。

対応手順を作成する必要性

インシデント対応手順を事前に定めていない場合、緊急時にどのような対応を実施すべきかわからず適切に対応ができないこととなります。これは、対応の遅れにつながり、ひいては被害が拡大することにもつながります。

なお、オフィスでの業務実施時とテレワーク時の業務におけるシステムの環境は異なることがあります。この場合、オフィスでの業務実施時を想定したインシデント対応手順では適切な対応が行えない可能性があるため、テレワーク時に合わせた対応手順を整備することが重要です。

テレワーク端末のマルウェア感染の例

対応手順の概略例として、テレワーク端末へのマルウェア感染の場合を示します。

実施内容	必要性
（端末をVPN接続している場合） 端末のVPN接続状態を切断	端末のマルウェア感染の可能性を考慮し、被害拡大を防ぐため、端末をVPN接続から切断します。
直近で実施した作業のヒアリング	マルウェア感染が疑われるような操作を行ったか、該当端末の利用者に確認します。 （例：直前に添付ファイルを開封した）
（端末をVPN接続している場合） アカウントの無効化	アカウント情報（ID、パスワード）を窃取されている場合、社内ネットワークに不正アクセスされるおそれがあることから、アカウントを無効化します。
影響範囲の確認（アクセス履歴のあったデータとその件数の特定等）	重要情報の保管されているサーバ、クラウドサービス等に対して、該当のユーザからアクセスした痕跡があるかを確認します。また、情報漏えいの可能性の有無に関しても確認します。
ウイルス対策ソフトによるスキャン	マルウェア感染の場合、ウイルス対策ソフトによるスキャンで検知・駆除できる可能性があるため実施します。
端末の初期化	マルウェア感染が断定できる場合や、原因が特定できず打ち手が他に無い場合は端末を初期化します。
ウイルス対策ソフトの最新化	既存のマルウェアへの感染を防ぐため、ウイルス対策ソフトを最新化します。
注意喚起	他の従業員が同様のインシデントの被害にあわないようにするために、同一の操作を行わないよう注意喚起を行います。（既に行ってしまった場合も想定して対応策も案内します。）

「パスワード」について

パスワードの安全性が高いかどうかを図る尺度のことを「パスワード強度」といいます。パスワードの文字数や使用できる文字の種類（数字、英字の大文字・小文字、記号）により、パスワード強度は変化します。

強いパスワードを利用する必要性

パスワード強度が弱いパスワードを使用した場合、総当たり攻撃[4]や辞書攻撃[5]等により、パスワードが解読され、不正アクセスを受けるおそれがあります。そのため、適切にパスワードを設定することが求められます。

また、パスワードを複数のサービスで使い回していると、どこかのサービスでパスワードが漏えいした場合に、他のサービスまで攻撃を受けてしまう状態となりますので、同一のパスワードを様々なサービスで使用することは推奨されません。

パスワードとして使用を推奨しないものの例

パスワードとして使用を推奨しないものの例は、次の通りです。

・名前や生年月日
・他サイトと同様のログイン情報
・辞書に載っている単語（１文字変えるといった対応でも同じです。）
・推測されやすい単語

マスターパスワードの活用

他者から秘匿したマスターパスワードとなる文字列を一つ作り、サービスごとのパスワードは、マスターパスワードに続けて文字列を追加する方法が挙げられます。なお、追加する文字列についても容易に推測されないようにする必要があります。

（例）　マスターパスワード：tHkh84Lp9C
　　サービスＡのパスワード：tHkh84Lp9CSe1
　　サービスＢのパスワード：tHkh84Lp9Ck40
　　サービスＣのパスワード：tHkh84Lp9C2R3

この際、パスワードを忘れてしまった場合に備えて、追加分のみをメモや電子ファイルとして保存しておけば、万が一、メモが漏えいした場合であっても、マスターパスワードは秘匿されているため、不正アクセスのリスクを抑えることができます。

パスフレーズ

パスワード長を長くするために「パスフレーズ」を利用することも有効です。パスフレーズは、複数の単語を組み合わせたもの（フレーズ）を指し、より長い文字列での作成が可能であることから、ブルートフォース攻撃（総当たり攻撃）への対策として有効です。また、ランダムな記号ではなく単語をベースに作成を行うため、通常のパスワードよりも忘れにくくなります。

---

[4] ブルートフォース攻撃とも呼ばれます。１つずつ文字を変えながら、しらみつぶしにパスワード入力を試していく攻撃手法です。
[5] よく使われるパスワードを順次試していく攻撃手法です。

参考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サイト等を示します。

○テレワークセキュリティガイドライン（第５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まとめたものです。

○サイバーセキュリティ経営ガイドライン【経済産業省/(独)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ものです。

○中小企業の情報セキュリティ対策ガイドライン【(独)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/

テレワークを行う際のセキュリティ上の留意点等について周知したものです。

○テレワークを行う際のセキュリティ上の注意事項【(独)情報処理推進機構】

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

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したものです。

○テレワークの適切な導入及び実施の推進のためのガイドライン【厚生労働省】

https://www.mhlw.go.jp/content/000759469.pdf

労務管理を中心に、労使双方にとって留意すべき点等を明らかにしたものです。

○テレワーク総合情報サイト【総務省】

https://telework.soumu.go.jp/

テレワークの導入事例や、導入に当たって活用可能な支援策をまとめたサイトです。

［修正履歴］
2021年５月31日　第２版策定
2021年６月２日　方式確認のフローチャートの文字サイズ等変更

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 （迷惑メール防止のため「@」を「×」と表記しています。）
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/