

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3版

令和4年5月



総務省

早引きインデックス

テレワークセキュリティの疑問と本書の対応ページ

Q

テレワークセキュリティの疑問

A

対応ページ

- 最短の手順で対策をチェックしたい。

下記  マーカー部分の2ステップを行ってください。
Step1で方式確認(p.10)→Step2で対策チェック(p.25~p.57)

- 何から始めればよいかわからない。
- 自社のテレワーク方式を確認したい。

Step1 (1ページだけです)

第1部 2. あなたのテレワーク方式はどれ？

フローチャートで自組織のテレワーク方式を確認できます。

p.10

- 各テレワーク方式の特徴をきちんと理解したい。

第1部 4. テレワーク方式の解説

各方式の特徴について図を交えながら解説します。

p.14
|
p.24

- 現在の対策状況を把握したい。
- 実施すべき対策を洗い出したい。

Step2 (3~4ページだけです)

第2部 1. テレワークセキュリティ 対策チェックリスト

自組織のテレワーク方式に対応するチェックリストで
対策状況をチェックできます。

p.25
|
p.57

- 対策の必要性を社内に訴えたい。

参考 1. テレワーク環境を狙う脅威

テレワーク環境で想定される脅威について解説します。

p.65
|
p.69

- 具体的な対策内容を知りたい。

参考 2. テレワークに有効なセキュリティ対策

リスクを最小化するための対策について解説します。

p.70
|
p.87

- テレワークセキュリティに関する
各種ガイドラインや情報を知りたい。

参考 5. リンク集

テレワークセキュリティに関連して参考となる文献や
Webサイト等をご紹介します。

p.100
|
p.101

※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3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。

※本書に記載されている会社名・商品名は、それぞれ各社の商標・登録商標です。

目次

早引きインデックス

テレワークセキュリティの疑問と本書の対応ページ	3
-------------------------------	---

はじめに

1. 本書の目的	6
2. 本書の想定読者	6
3. 本書の使い方	7

第1部

1. テレワークの形態	9
2. あなたのテレワーク方式はどれ?	10
3. テレワーク方式の全体概要	11
会社支給の端末／方式①～方式④	12
個人所有の端末／方式⑤～方式⑧	13
4. テレワーク方式の解説	14
方式① 会社支給端末：VPN/リモートデスクトップ方式	15
方式② 会社支給端末：クラウドサービス方式	17
方式③ 会社支給端末：スタンドアロン方式	18
方式④ 会社支給端末：セキュアブラウザ方式	19
方式⑤ 個人所有端末：VPN/リモートデスクトップ方式	20
方式⑥ 個人所有端末：クラウドサービス方式	22
方式⑦ 個人所有端末：スタンドアロン方式	23
方式⑧ 個人所有端末：セキュアブラウザ方式	24

第2部

1. テレワークセキュリティ 対策チェックリスト	25
方式① 会社支給端末：VPN/リモートデスクトップ方式	26
方式② 会社支給端末：クラウドサービス方式	30
方式③ 会社支給端末：スタンドアロン方式	34
方式④ 会社支給端末：セキュアブラウザ方式	38
方式⑤ 個人所有端末：VPN/リモートデスクトップ方式	42
方式⑥ 個人所有端末：クラウドサービス方式	46
方式⑦ 個人所有端末：スタンドアロン方式	50
方式⑧ 個人所有端末：セキュアブラウザ方式	54
2. 対策チェックリストの設定例一覧	58
3. セキュリティ対策一覧	59

1. テレワーク環境を狙う脅威	65
(1) マルウェア感染	66
(2) 不正アクセス	67
(3) 端末の紛失・盗難	68
(4) 情報の盗聴	69
2. テレワークに有効なセキュリティ対策	70
(1) 資産・構成管理	71
(2) マルウェア対策	72
(3) アクセス制御・認可	74
(4) 物理セキュリティ	76
(5) 脆弱性管理	77
(6) 通信暗号化	79
(7) インシデント対応・ログ管理	80
(8) データ保護	82
(9) アカウント・認証管理	84
(10) 特権管理	86
3. 知っておきたいキーワード集	88
MDM	88
各種連絡体制(インシデント発生時)	89
管理者権限	90
時刻同期	91
システムによるアクセス制御	92
重要情報	94
対応手順(インシデント対応手順)	95
パスワード強度	96
4. 用語集	98
5. リンク集	100

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、このガイドラインを補うものとして作成されました。具体的には、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がテレワークを導入・活用する際に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、本書で示す対策の実施を目標とすることで、テレワーク環境でも効果的にセキュリティを確保できます。

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む)を対象としています。具体的には次の読者像を念頭に、必要な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
セキュリティ 予算	外部委託コストの捻出が難しいレベルの組織	外部委託コストを必要に応じて捻出するレベルも含めた幅広い組織
セキュリティ 推進体制	<u>専任の担当・担当部門が存在しない</u> 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	読者に解釈を委ねるような <u>抽象的な要求だけでは、対応内容がわからない</u>	読者に解釈を委ねるような抽象的な要求でも、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用語について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
	基本的なシステム設定作業であれば、インターネット検索等により調べながら行える	基本的なシステム設定作業であれば、問題なく行える

^{※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. 本書の使い方

本書は、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ご活用ください。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。既にテレワーク方式が明らかな場合は読み飛ばして構いません。

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し、必要なセキュリティ対策を実施してください。

さらに、セキュリティ対策への理解を深めるために有効な資料として、「[参考 1. テレワーク環境を狙う脅威\(p.65～\)](#)」、「[参考 2. テレワークに有効なセキュリティ対策\(p.70～\)](#)」を必要に応じてご活用ください。

また、従業員向けのコンテンツとして、「従業員向けハンドブック」と「緊急時対応カード(シール)」を作成していますので、ご活用ください。

構成	概要
■ 早引きインデックス	テレワークセキュリティに関する疑問に対する本書の対応ページを示しています。
■ 目次	本書の詳細目次です。
■ はじめに	本書の目的や想定読者像を明らかにした上で、全体構成及び活用方法を説明しています。
第 1 部	
■ 1. テレワークの形態	業務を行う場所に応じた働き方の分類を示しています。
■ 2. あなたのテレワーク方式はどれ？	テレワークの利用シーンを想定し、導入(または予定)しているテレワーク方式をフローチャートで確認できます。
■ 3. テレワーク方式の全体概要	本書で取り扱うテレワーク方式の概要を解説しています。
■ 4. 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 2 部	
■ 1. テレワークセキュリティ 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。
■ 2. 対策チェックリストの設定例一覧	テレワークでよく利用される製品の設定・利用方法について解説した「設定解説資料」を紹介しています。
■ 3. セキュリティ対策一覧	「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

1. テレワーク環境を狙う脅威	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。
2. テレワークに有効なセキュリティ対策	テレワーク環境における脅威を回避するための効果的なセキュリティ対策について解説しています。
3. 知っておきたいキーワード集	テレワークセキュリティ 対策チェックリストに登場するセキュリティ対策の重要なキーワードについて、図解を用いて詳しく解説しています。
4. 用語集	本書で用いている主な用語を解説しています。
5. リンク集	対策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。

付録(別紙)

従業員向けハンドブック	テレワークを行う従業員が常に反復して気を付けるべきことやもしもの時の連絡先等を記載しています。テレワークを実施する従業員に配布して活用してください。
緊急時対応カード(シール)	テレワークを行う従業員が困った際にどういった行動を最優先にすべきか記載しています。テレワークを実施する従業員に配布し、パソコン等のテレワーク端末に貼付して活用してください。

第1部

1. 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ます。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。

移動時間を要しないため、時間を有効に活用できます。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とも言えます。



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(シェアオフィスやコワーキングスペースを含む、メインのオフィス以外に設けられたオフィス)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えます。また、都心部にあるサテライトオフィスは、移動時間の合い間に立ち寄って業務を行えるため、業務の効率化を図ることも可能です。



③ モバイル勤務

ノート PC やタブレット、スマートフォン等を活用して時間や場所の制約なく業務を行う働き方です。自由に働く場所を選択できるだけでなく、外勤における移動時間を利用できるため、業務の効率化を図ることが可能です。



第1部

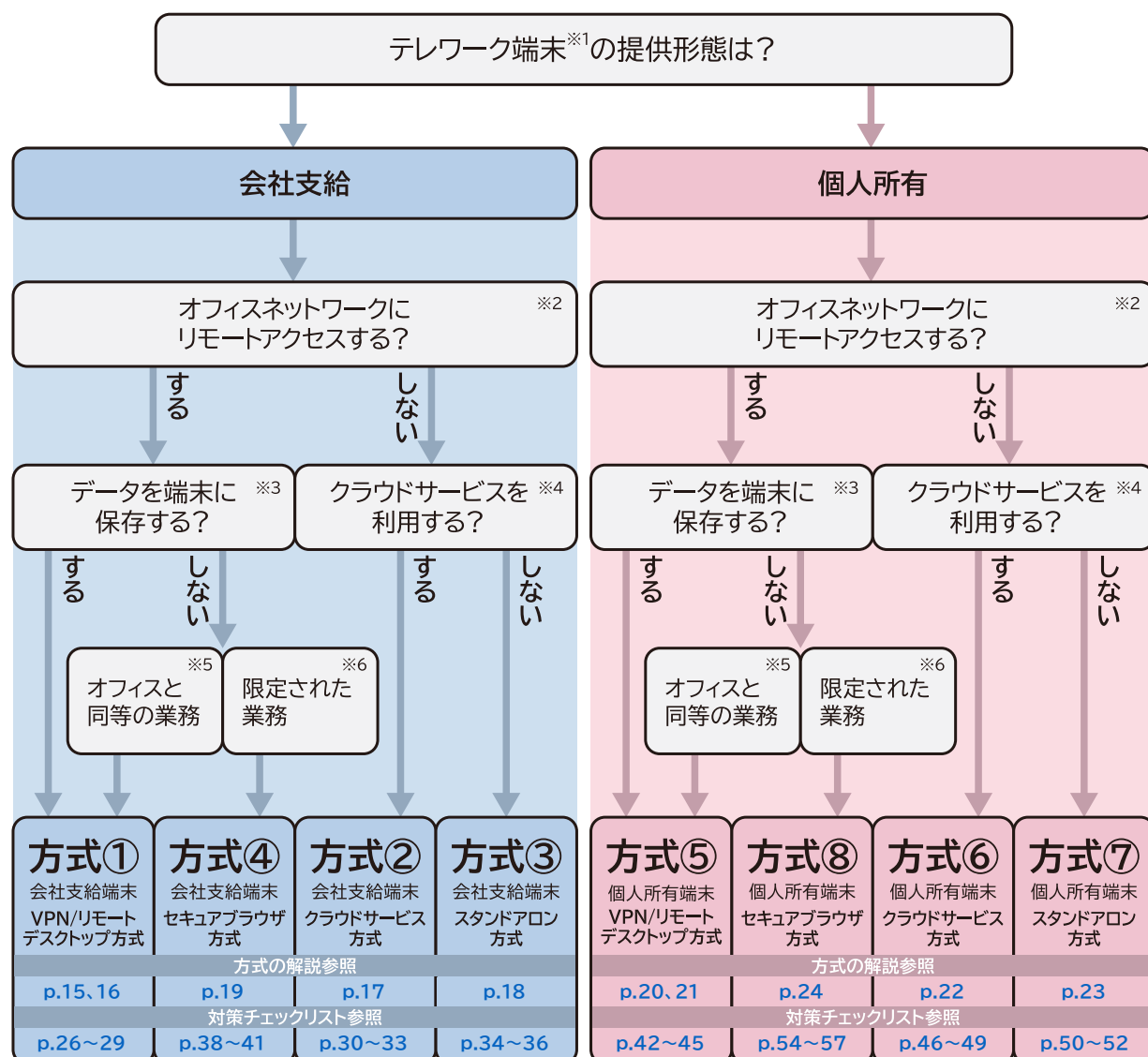
2. あなたのテレワーク方式はどれ？

次のフローチャートで、皆様の組織で導入している(導入を予定している)テレワーク方式を確認できます。既に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、PC やスマートフォン等の複数の環境を併用して業務を行っており、それぞれ利用形態が異なる場合は、環境ごとに方式を確認します。

各方式の詳細な説明については、「第1部 4. テレワーク方式の解説(p.14~)」をご覧ください。

あなたが該当するテレワーク方式を確認し、チェックリストの対策を実施しよう！



※1 テレワークのために従業員が使用するPCやタブレット、スマートフォンが該当する。 ※2VPN/リモートデスクトップ/セキュアブラウザ等を使用してリモートアクセスする。 ※3 テレワーク時にデータを端末保存する ※4 テレワーク時にメール/チャット/ファイル共有/オンライン会議等のクラウドサービスを利用する。 ※5 テレワーク時に会社データの編集・閲覧/メール送受信等のオフィスと同等の業務を行う。 ※6 テレワーク時に会社データの閲覧/メール送受信のみの限定された業務を行う。

第1部

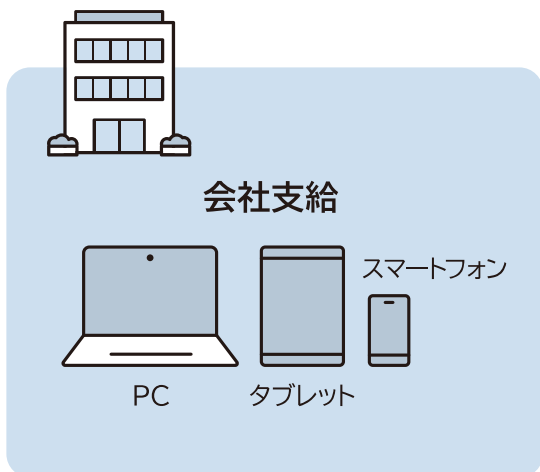
3. テレワーク方式の全体概要

テレワークを実現するためのシステム構成には、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種別等により、複数の方式が存在します。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、まずは、皆様の組織で導入している(導入を予定している)テレワーク方式を明らかにする必要があります。

本書では、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しています。さらに、次の表に示すとおり、会社支給端末の場合は方式①～方式④、個人所有端末の場合は方式⑤～方式⑧のいずれかに分類できます。

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。



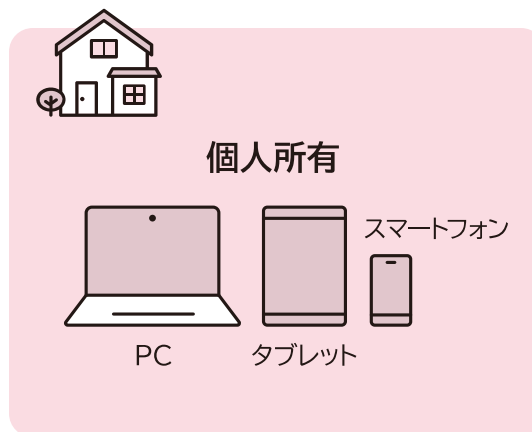
オフィスネットワークへの接続方式の種別等により

方式①～方式④に分類

方式解説 → [p.15～p.19](#)

個人所有の端末

テレワークのために従業員が使用する、個人所有の PC やスマートフォン等が該当します。

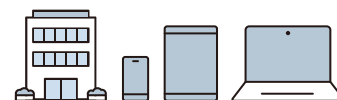


オフィスネットワークへの接続方式の種別等により

方式⑤～方式⑧に分類

方式解説 → [p.20～p.24](#)

なお、各方式の解説に登場する共通的な用語については、「用語集(p.98～p.99)」にまとめてありますので、必要に応じてご参照ください。



方式① 会社支給端末：VPN/リモートデスクトップ方式

概要	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。		
テレワーク端末へのデータ保存	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		
オフィスネットワークへの接続方式	VPN、 リモートデスクトップ等	クラウドサービス利用	利用する/利用しない どちらも含む
参照ページ	方式解説 → p.15、p.16	対策チェックリスト → p.26～p.29	

方式② 会社支給端末：クラウドサービス方式

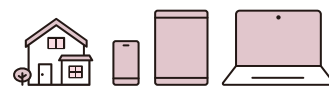
概要	会社支給のテレワーク端末からインターネット上のクラウドサービスに接続して業務を行う方式。		
テレワーク端末へのデータ保存	保存する/保存しないどちらも含む		
オフィスネットワークへの接続方式	接続しない	クラウドサービス利用	利用する
参照ページ	方式解説 → p.17	対策チェックリスト → p.30～p.33	

方式③ 会社支給端末：スタンドアロン方式

概要	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む)、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。		
テレワーク端末へのデータ保存	保存する		
オフィスネットワークへの接続方式	接続しない	クラウドサービス利用	利用しない
参照ページ	方式解説 → p.18	対策チェックリスト → p.34～p.36	

方式④ 会社支給端末：セキュアブラウザ方式

概要	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。		
テレワーク端末へのデータ保存	保存しない		
オフィスネットワークへの接続方式	セキュアブラウザ	クラウドサービス利用	利用する
参照ページ	方式解説 → p.19	対策チェックリスト → p.38～p.41	



方式⑤ 個人所有端末：VPN/リモートデスクトップ方式

概要	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。		
テレワーク端末へのデータ保存	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		
オフィスネットワークへの接続方式	VPN、 リモートデスクトップ等	クラウドサービス利用	利用する/利用しない どちらも含む
参照ページ	方式解説 → p.20、p.21	対策チェックリスト → p.42～p.45	

方式⑥ 個人所有端末：クラウドサービス方式

概要	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。		
テレワーク端末へのデータ保存	保存する/保存しないどちらも含む		
オフィスネットワークへの接続方式	接続しない	クラウドサービス利用	利用する
参照ページ	方式解説 → p.22	対策チェックリスト → p.46～p.49	

方式⑦ 個人所有端末：スタンドアロン方式

概要	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保存し、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。		
テレワーク端末へのデータ保存	保存する		
オフィスネットワークへの接続方式	接続しない	クラウドサービス利用	利用しない
参照ページ	方式解説 → p.23	対策チェックリスト → p.50～p.52	

方式⑧ 個人所有端末：セキュアブラウザ方式

概要	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。		
テレワーク端末へのデータ保存	保存しない		
オフィスネットワークへの接続方式	セキュアブラウザ	クラウドサービス利用	利用する
参照ページ	方式解説 → p.24	対策チェックリスト → p.54～p.57	

第1部

4. テレワーク方式の解説

ここからは、方式①～⑧までの8つのテレワーク方式^{※1}について一つずつ解説します。フローチャートで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を確認するためにも、解説をご活用ください。

なお、各方式の解説に当たって登場する共通的な用語については、巻末の「用語集(p.98～p.99)」にまとめてあり解説していますので、必要に応じてご参照ください。

※1 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

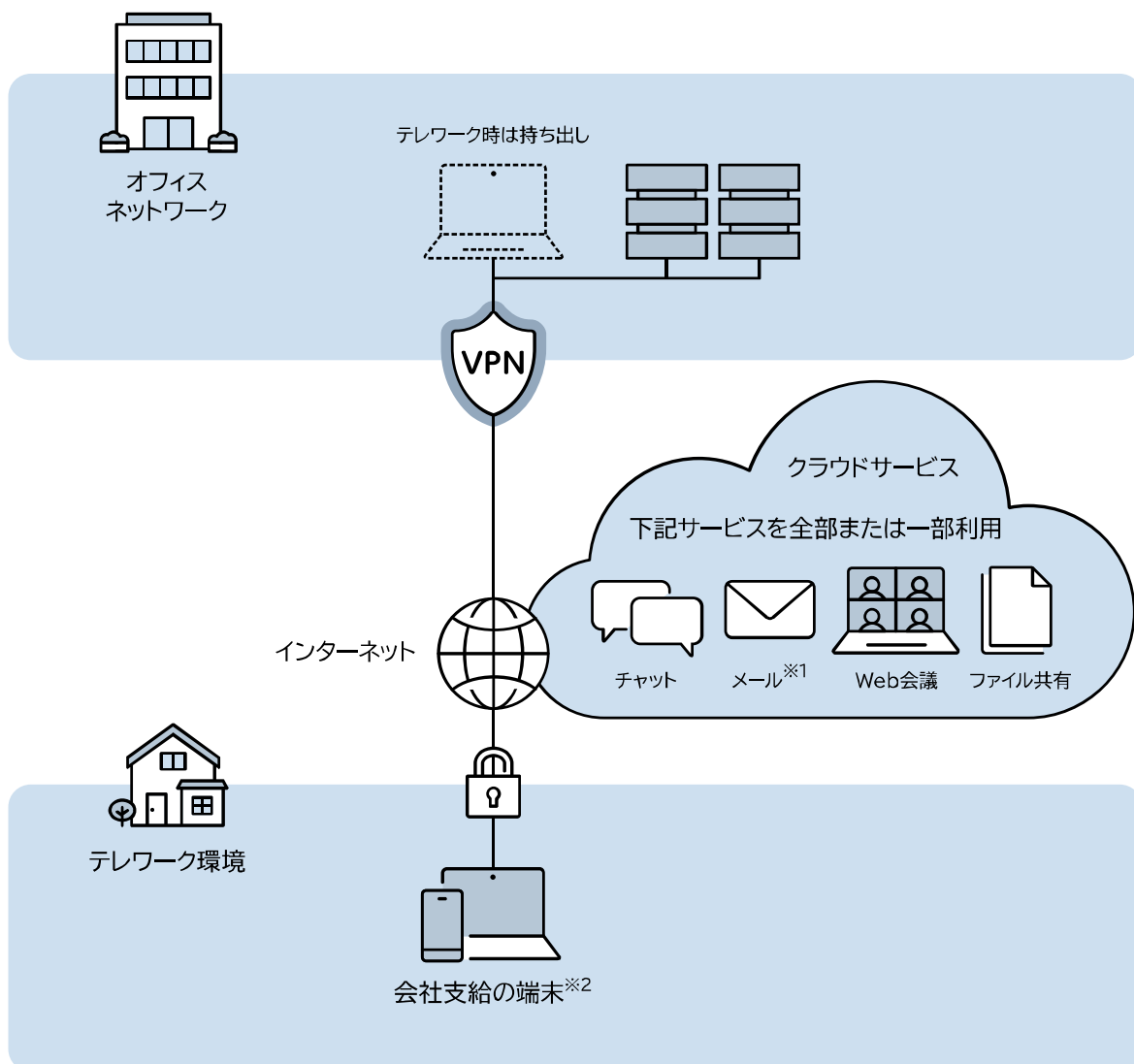
方式① テレワーク方式の解説

会社支給端末：VPN/リモートデスクトップ方式

この方式には、VPN方式とリモートデスクトップ方式の2つが該当します。

[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接続して業務を行います。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行う場合も含まれます。オフィスと同等の業務環境を実現できるのが特徴です。



対策チェックリスト参照: [p.26~p.29](#)

※1 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。

※2 タブレットやスマートフォンを使う場合に、アプリケーション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。

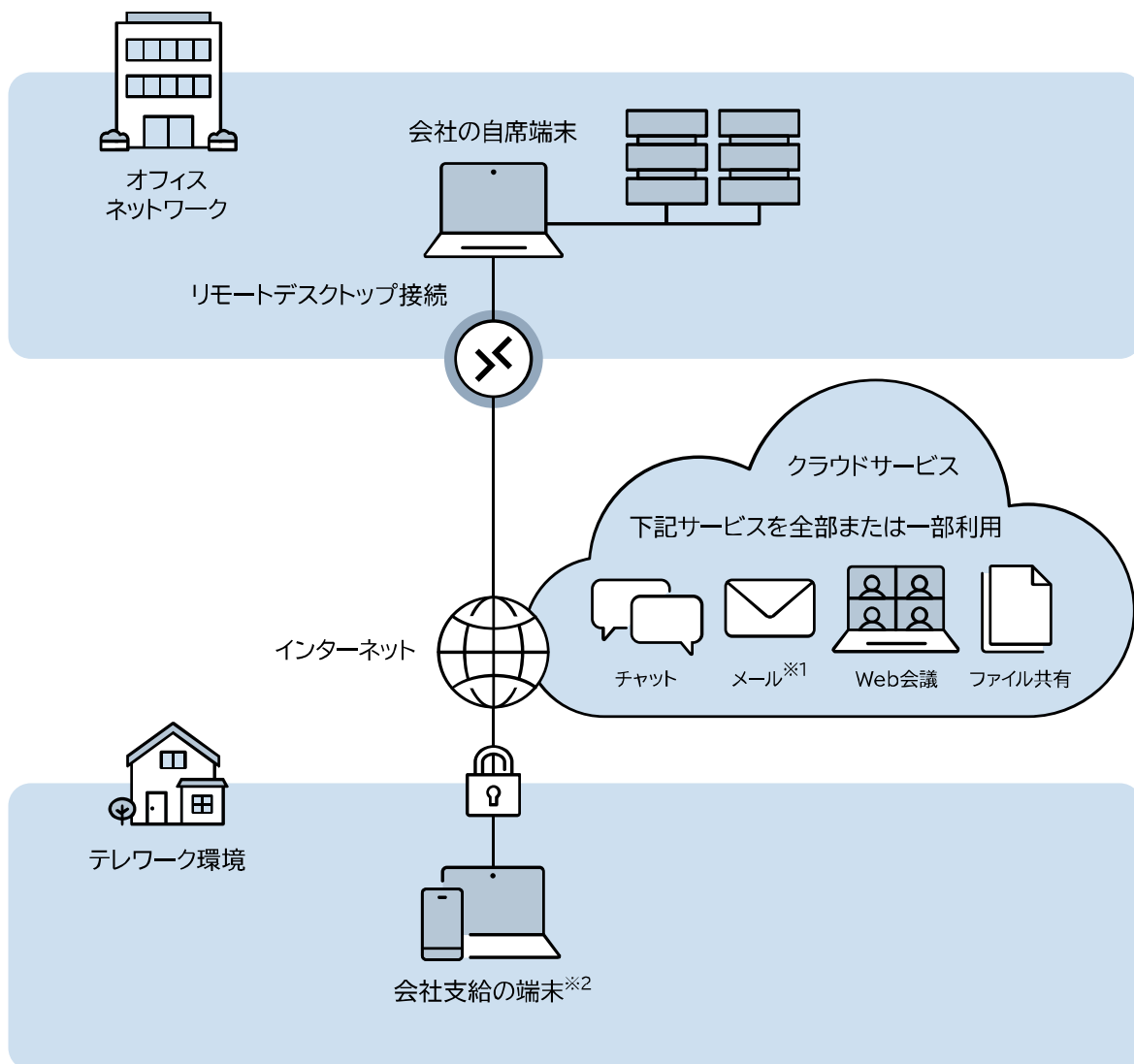
方式① テレワーク方式の解説

会社支給端末：VPN/リモートデスクトップ方式

この方式には、VPN方式とリモートデスクトップ方式の2つが該当します。

【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(遠隔操作)して業務を行います。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行う場合も含まれます。オフィスと同等の業務環境を実現できるのが特徴です。



対策チェックリスト参照: [p.26~p.29](#)

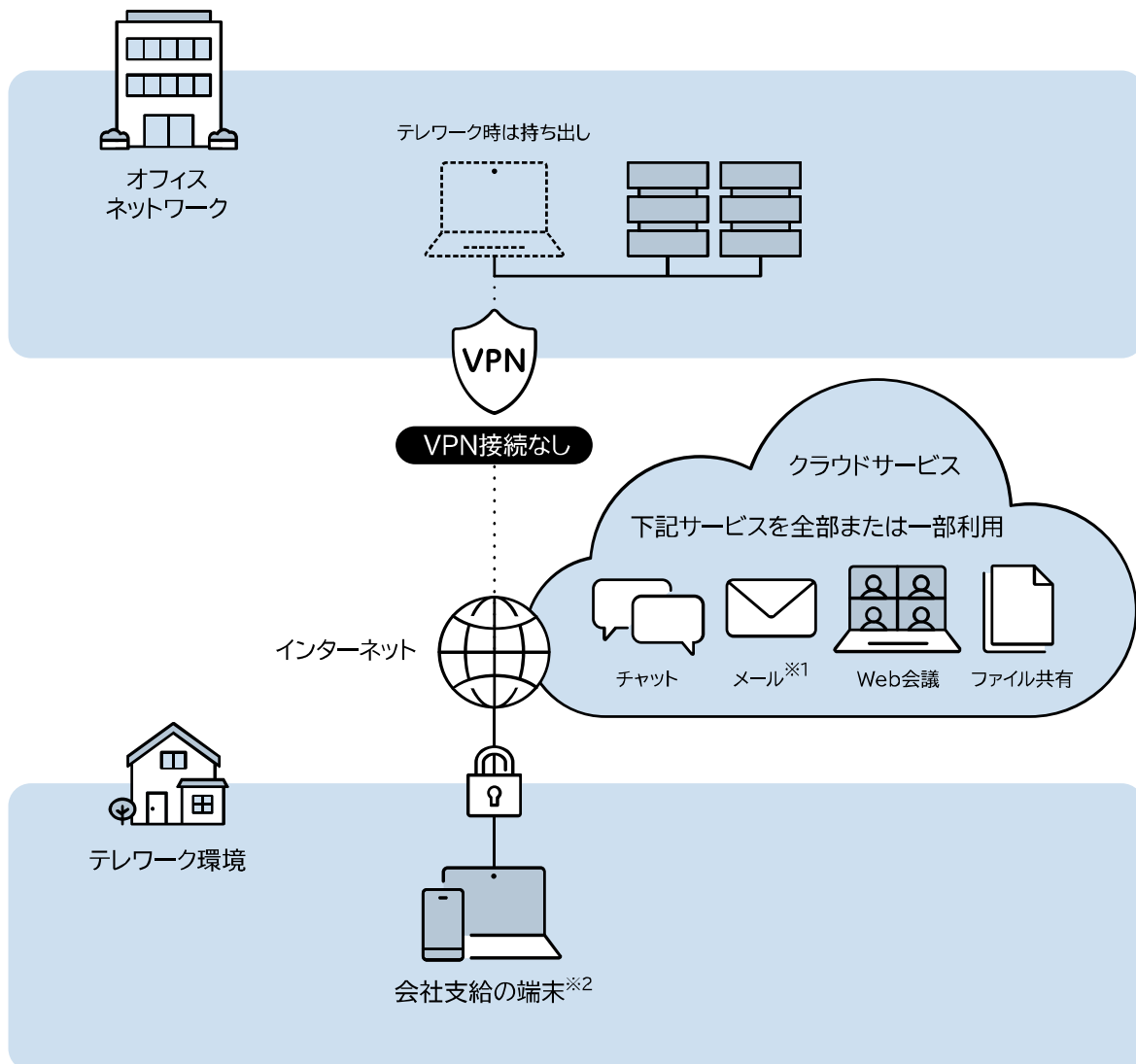
※1 プロバイダー提供のメール利用もクラウドサービスに該当。

※2 タブレットやスマートフォンを使う場合に、アプリケーション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 テレワーク方式の解説

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。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、スタンドアロン方式のようにテレワーク端末上で業務を行う場合も含まれます。オフィスネットワークに接続しないのが特徴です。



対策チェックリスト参照: [p.30~p.33](#)

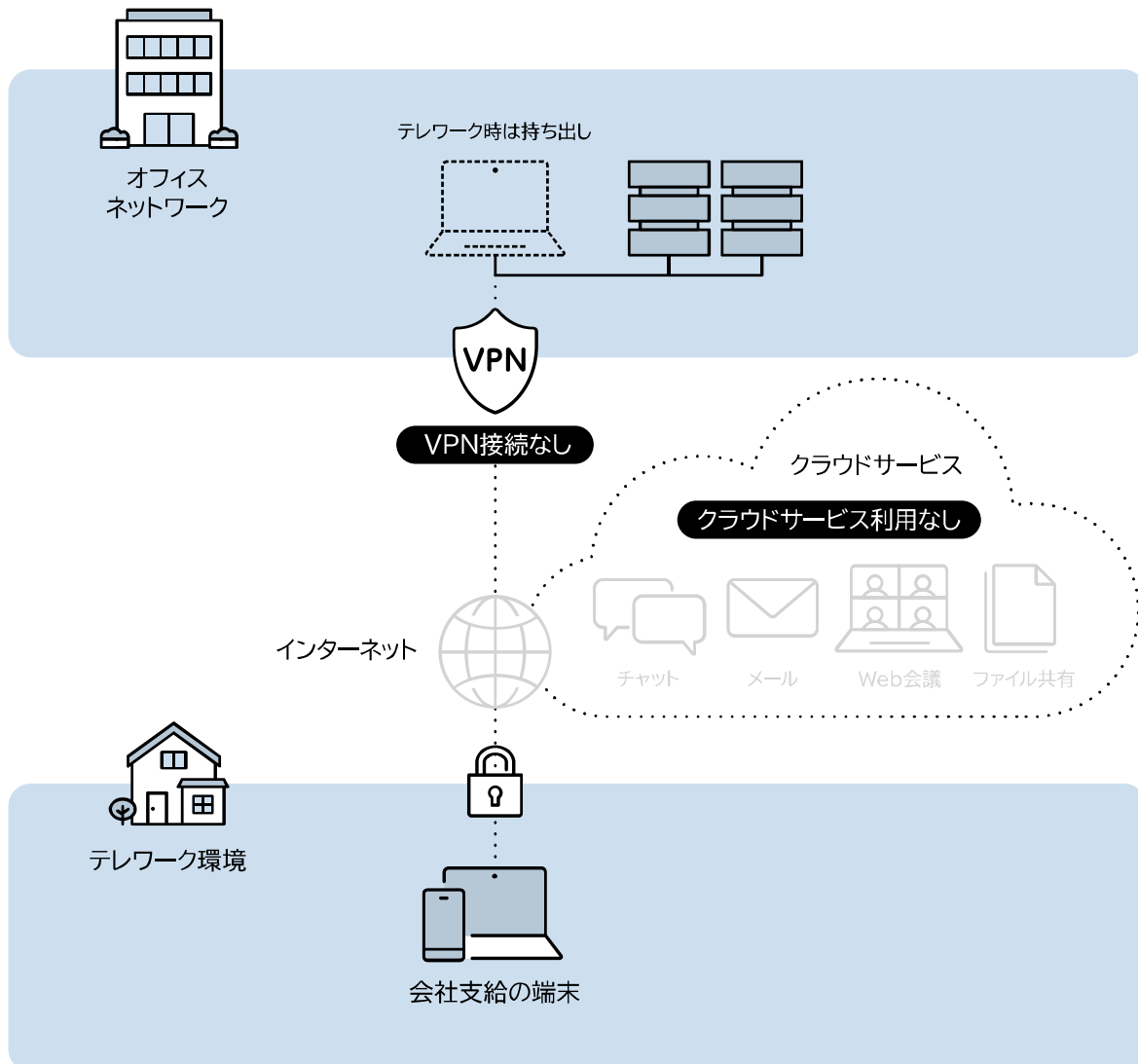
※1 プロバイダー提供のメール利用もクラウドサービスに該当。

※2 タブレットやスマートフォンを使う場合に、アプリケーション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 テレワーク方式の解説

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む)、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います。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のが特徴です。

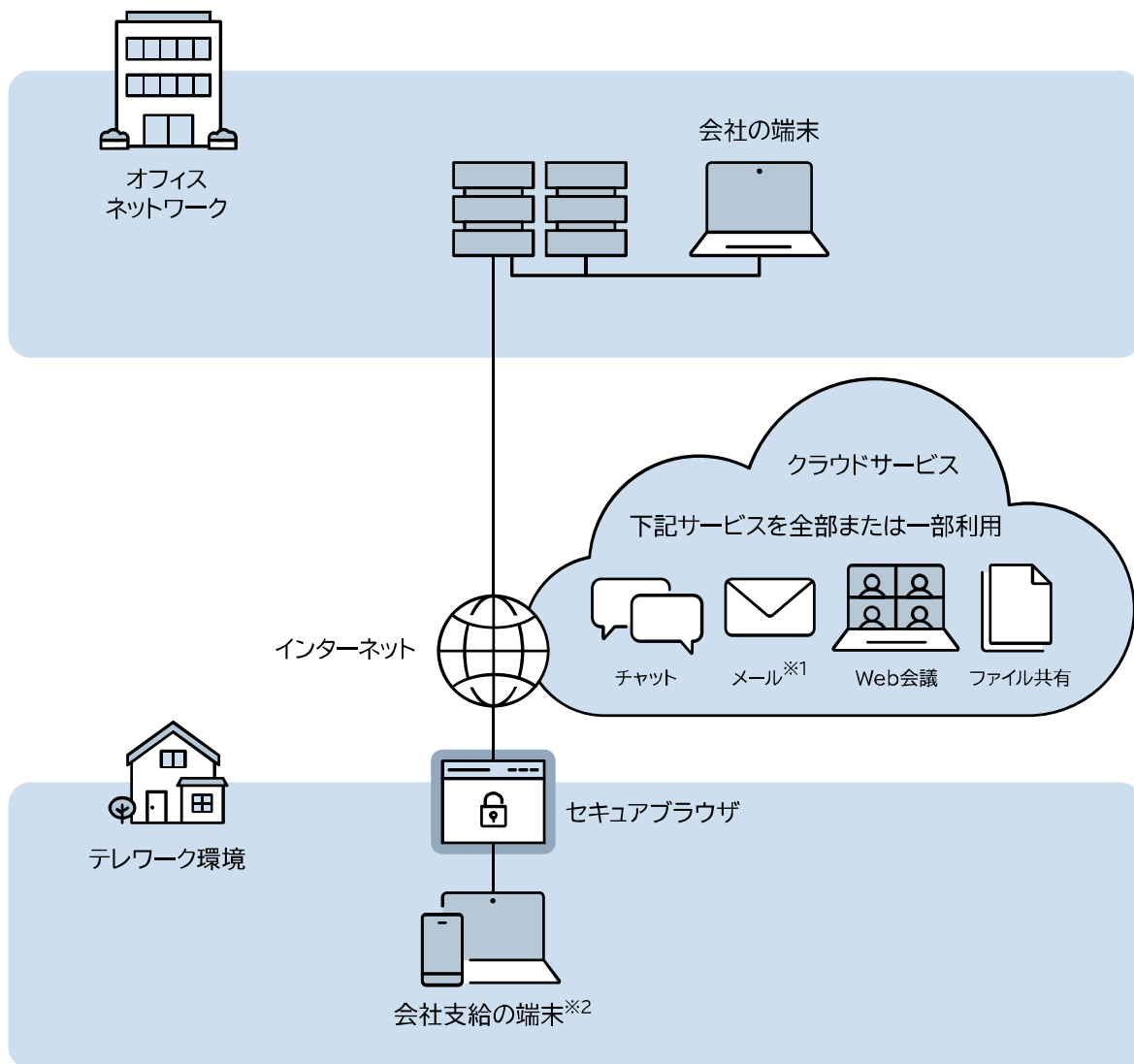


対策チェックリスト参照: [p.34~p.36](#)

方式④ テレワーク方式の解説

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 Web 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行います。端末へのデータ保存を行わず、セキュアブラウザに対応した業務のみを限定的にテレワークで行うのが特徴です。



対策チェックリスト参照: [p.38~p.41](#)

※1 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。

※2 タブレットやスマートフォンを使う場合に、アプリケーション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。

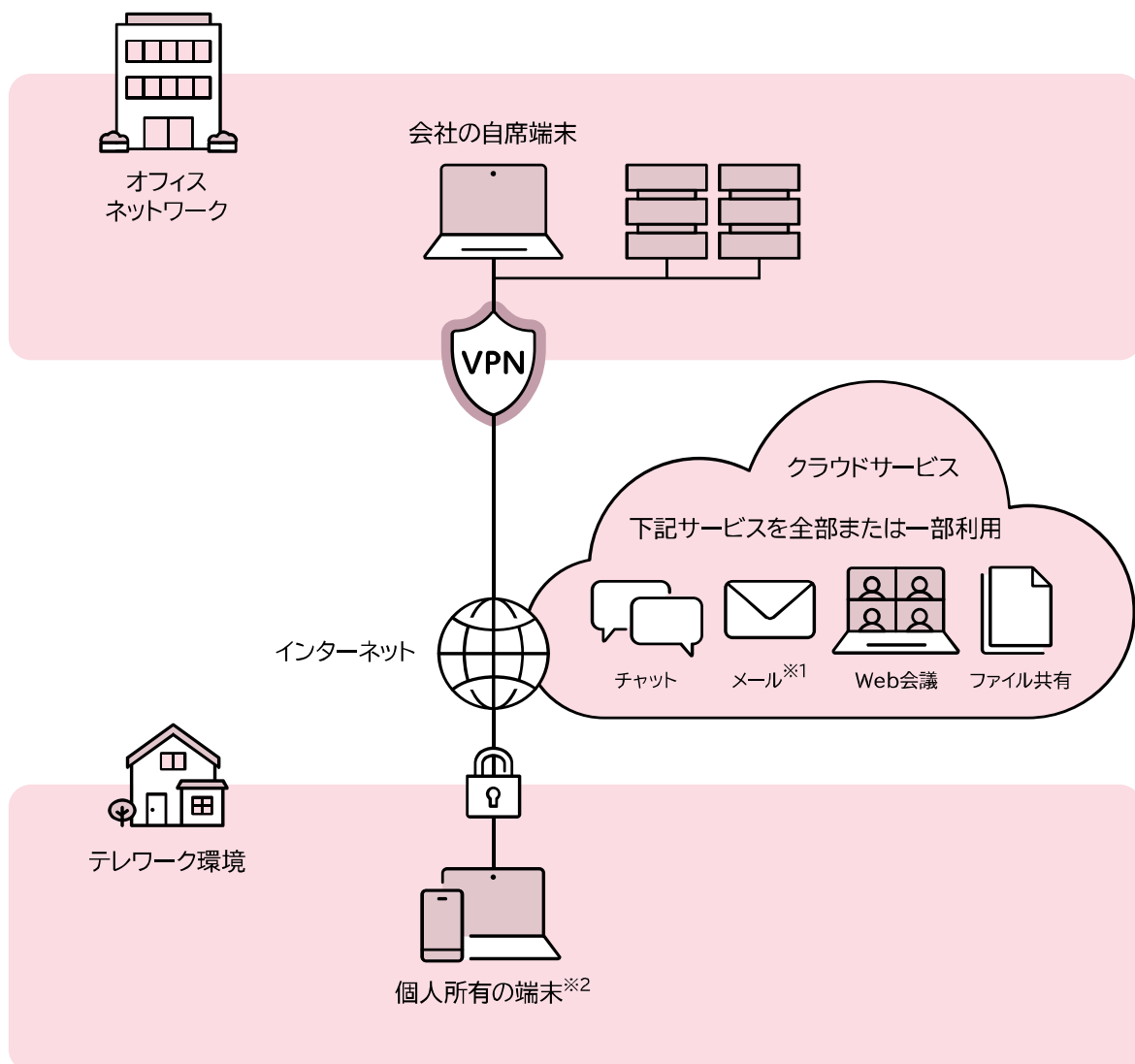
方式⑤ テレワーク方式の解説

個人所有端末：VPN/リモートデスクトップ方式

この方式には、VPN方式とリモートデスクトップ方式の2つが該当します。

[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接続して業務を行います。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行う場合も含まれます。オフィスと同等の業務環境を実現できるのが特徴です。



対策チェックリスト参照: [p.42~p.45](#)

※1 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。

※2 タブレットやスマートフォンを使う場合に、アプリケーション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。

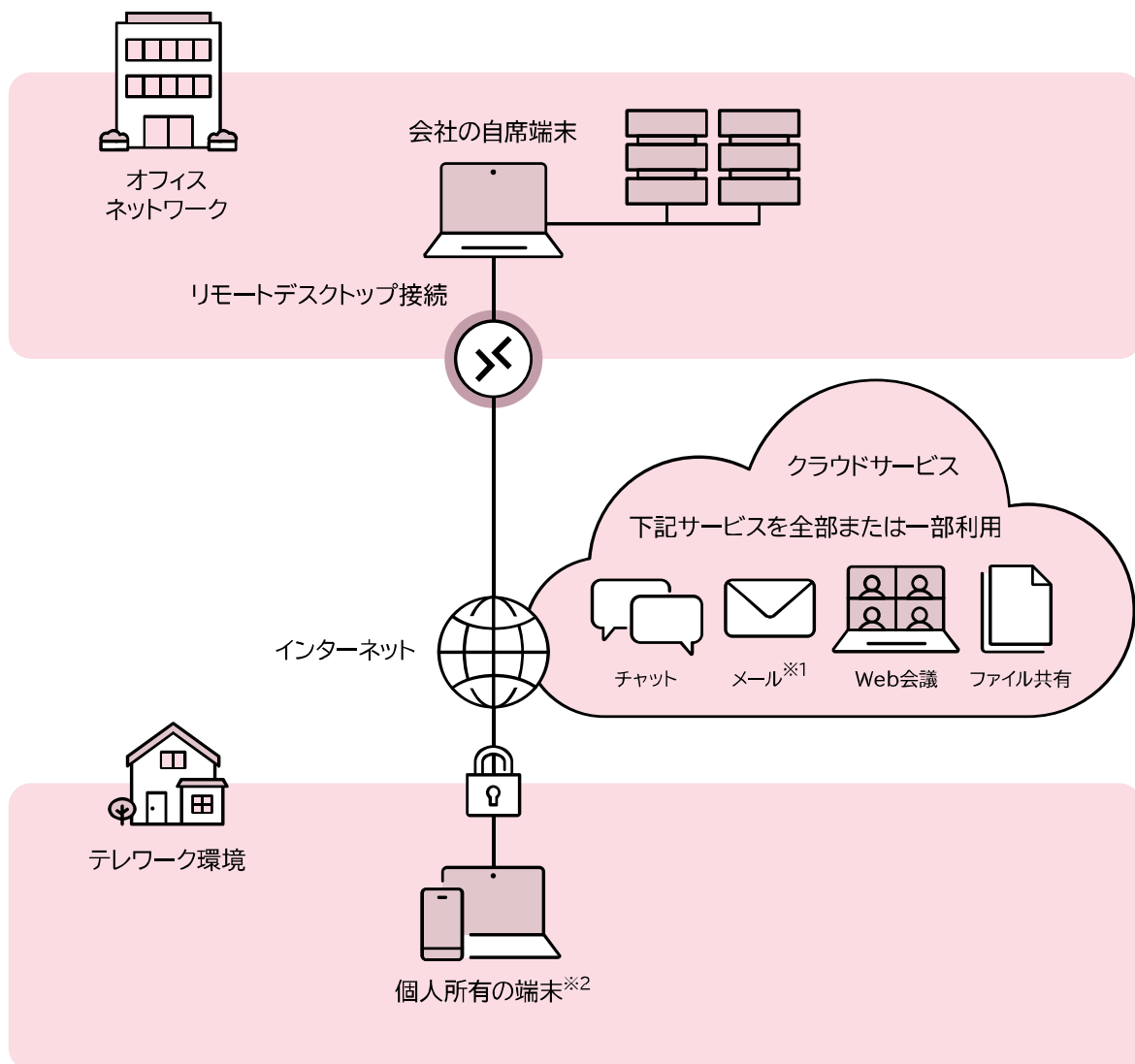
方式⑤ テレワーク方式の解説

個人所有端末：VPN/リモートデスクトップ方式

この方式には、VPN方式とリモートデスクトップ方式の2つが該当します。

[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行います。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行う場合も含まれます。オフィスと同等の業務環境を実現できるのが特徴です。



対策チェックリスト参照: [p.42~p.45](#)

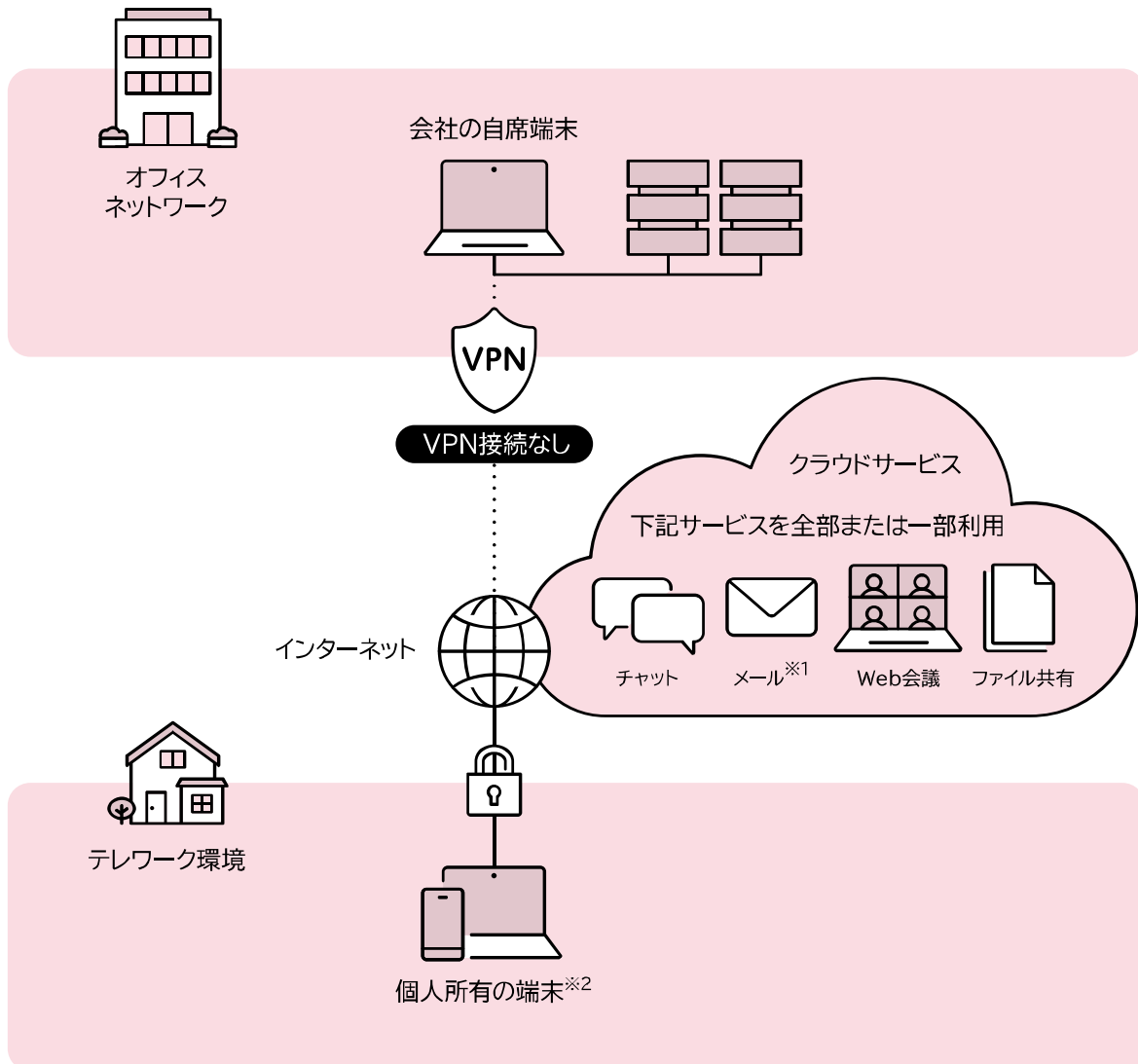
※1 プロバイダー提供のメール利用もクラウドサービスに該当。

※2 タブレットやスマートフォンを使う場合に、アプリケーション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 テレワーク方式の解説

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行います。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、スタンドアロン方式のようにテレワーク端末上で業務を行う場合も含まれます。オフィスネットワークに接続しないのが特徴です。



対策チェックリスト参照: [p.46~p.49](#)

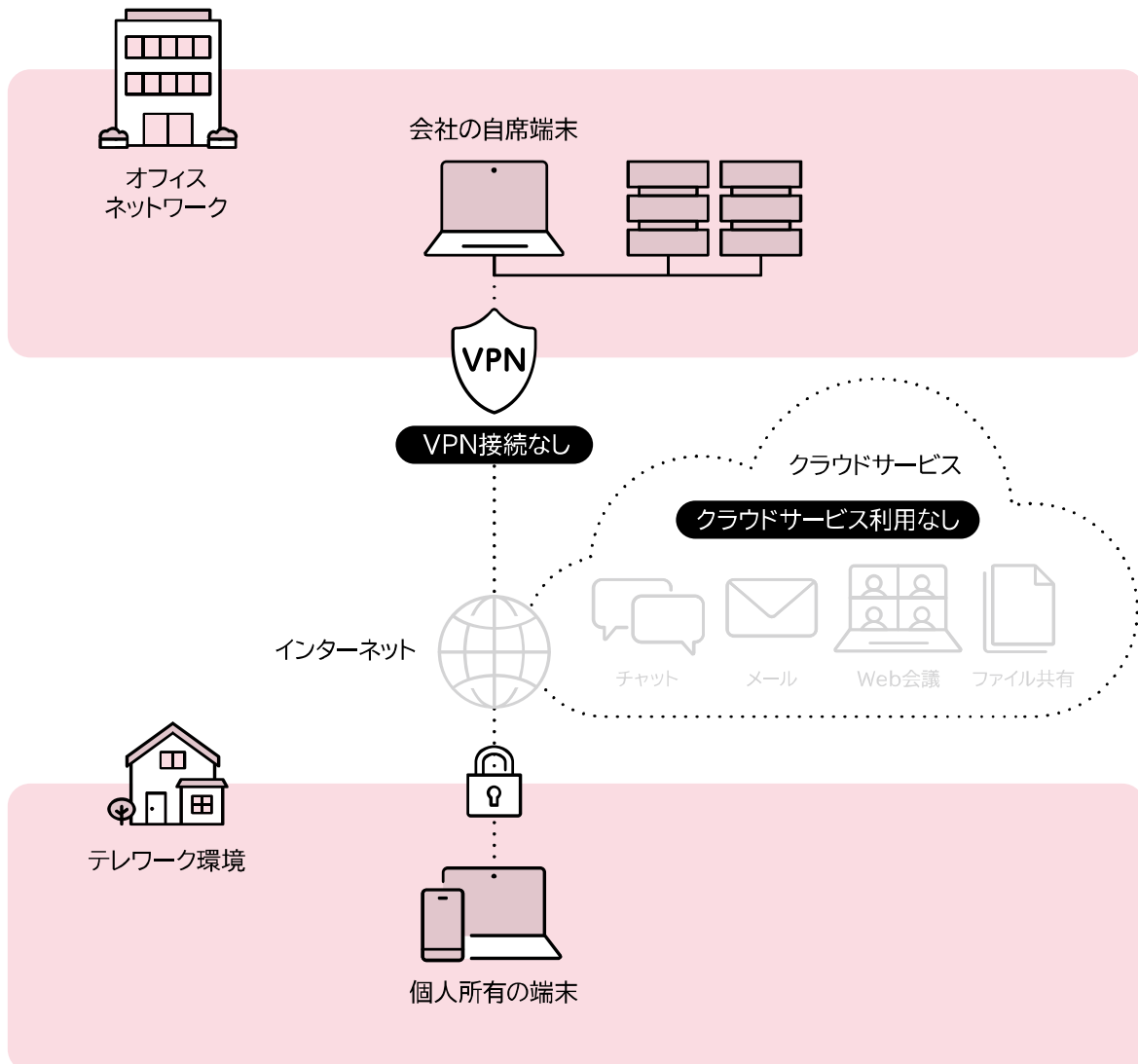
※1 プロバイダー提供のメール利用もクラウドサービスに該当。

※2 タブレットやスマートフォンを使う場合に、アプリケーション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 テレワーク方式の解説

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进行处理することで業務を行います。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のが特徴です。

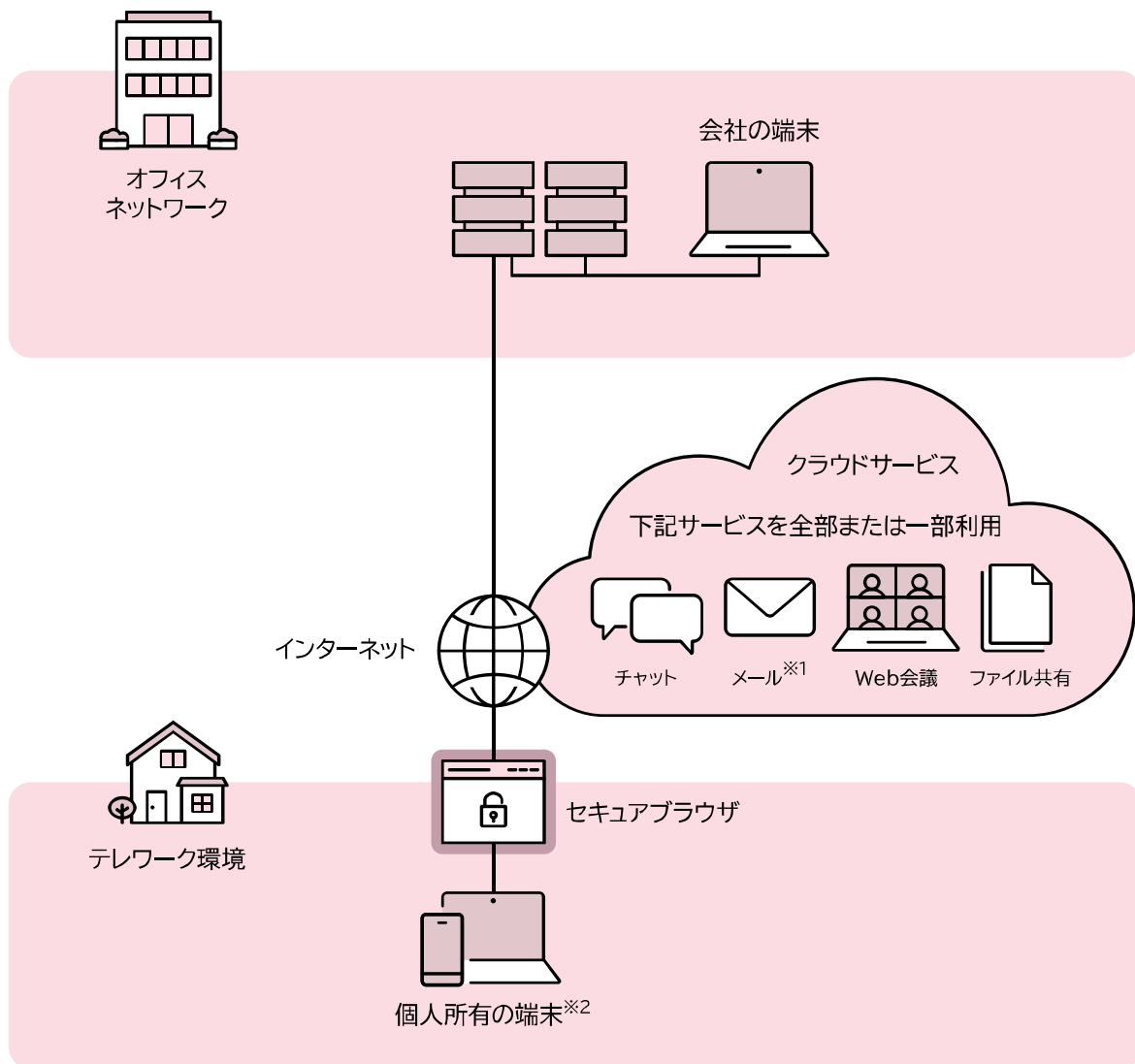


対策チェックリスト参照: [p.50~p.52](#)

方式⑧ テレワーク方式の解説

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Web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行います。端末へのデータ保存を行わず、セキュアブラウザに対応した業務のみを限定的にテレワークで行うのが特徴です。



対策チェックリスト参照: [p.54~p.57](#)

※1 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。


※2 タブレットやスマートフォンを使う場合に、アプリケーション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。

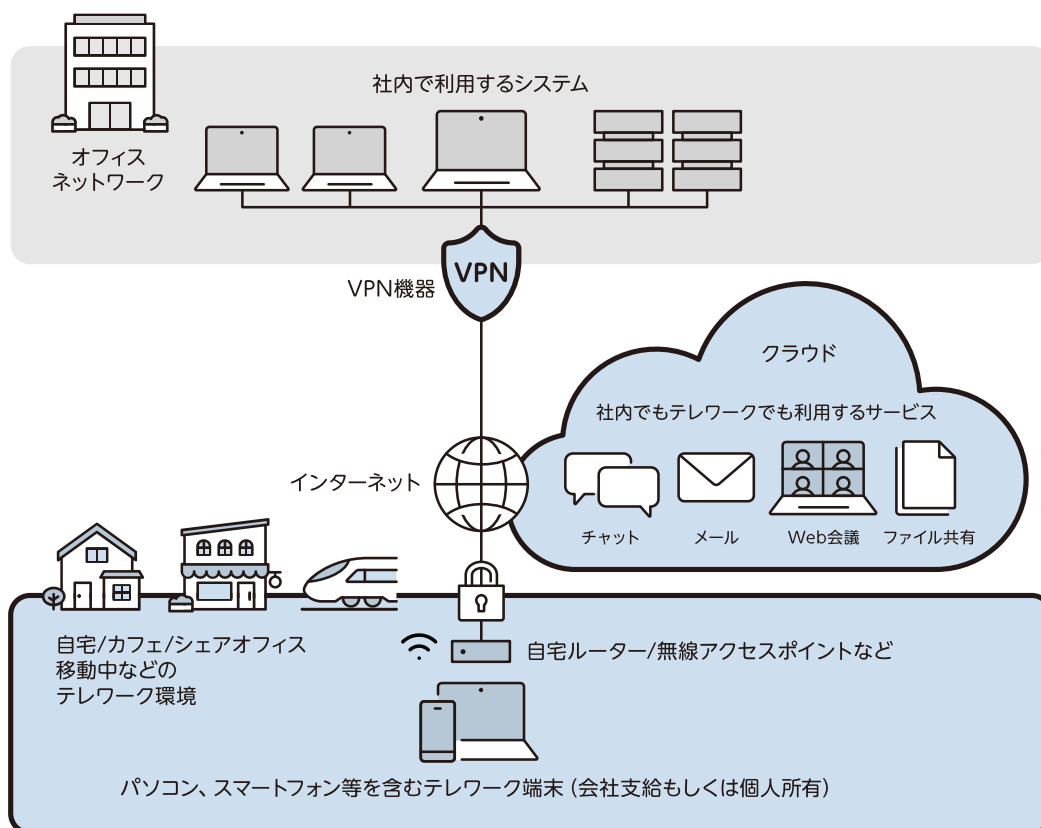
第2部

1. テレワークセキュリティ 対策チェックリスト

中小企業等の担当者がテレワークの導入や利用を進めるに当たり、必要なセキュリティ対策をテレワーク方式ごとに確認できるよう、対策チェックリストをご用意しました。また、効率的に着手・実施できるよう、各対策事項の優先度を示しています。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く(効果が高く)、かつ実施難易度が低いもの(専門知識、追加コストの観点で懸念が小さい)。
優先度: ○	セキュリティ対策の重要性が高く(効果が高く)、かつ実施難易度が中程度のもの(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)。もしくは、セキュリティ対策の重要性が中程度で(ある程度の効果が期待できる)、かつ実施難易度が低いもの(専門知識、追加コストの観点で懸念が小さい)。

なお、本対策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^{※1}、具体的には下図の  で示した範囲です。



※1 テレワークの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、対策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 テレワークセキュリティ 対策チェックリスト(1/4)

会社支給端末：VPN/リモートデスクトップ方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
1-1	資産・構成管理 → p.71	テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。	<input type="checkbox"/>	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 → p.71	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する。	<input type="checkbox"/>	不正アクセス 情報の盗聴
2-1	マルウェア対策 → p.72、73	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を有効にする※1。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にするか、手動で更新するルールを作成する。	<input type="checkbox"/>	マルウェア感染
2-2	マルウェア対策 → p.72、73	不審なメールを開封し、メールに記載されている URL をクリックしたり、添付ファイルを開いたりしないよう周知する。	<input type="checkbox"/>	マルウェア感染
3-1	アクセス制御・ 認可 → p.74、75	許可された人のみが重要情報を利用できるよう、システムによるアクセス制御やファイルに対するパスワード設定等を行う。	<input type="checkbox"/>	不正アクセス
4-1	物理セキュリティ → p.76	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	<input type="checkbox"/>	情報の盗聴
4-2	物理セキュリティ → p.76	テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。	<input type="checkbox"/>	情報の盗聴
5-1	脆弱性管理 → p.77、78	テレワーク端末にはメーカーサポートが終了した OS やアプリケーションを利用しないよう周知する。	<input type="checkbox"/>	不正アクセス
5-2	脆弱性管理 → p.77、78	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するよう周知する。	<input type="checkbox"/>	不正アクセス
5-4	脆弱性管理 → p.77、78	テレワーク端末から社内にリモートアクセスするための VPN 機器等には、メーカーサポートが終了した製品を利用せず、最新のセキュリティアップデートを適用する。	<input type="checkbox"/>	不正アクセス
7-1	インシデント 対応・ログ管理 → p.80、81	セキュリティインシデントの発生時や、そのおそれがある状況に備えて、対応手順及び関係者への各種連絡体制を定め、従業員に緊急連絡先を周知する。	<input type="checkbox"/>	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。

方式① テレワークセキュリティ 対策チェックリスト(2/4)

会社支給端末：VPN/リモートデスクトップ方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
8-1	データ保護 → p.82, 83	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<input type="checkbox"/>	盗難・紛失
9-1	アカウント・ 認証管理 → p.84, 85	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パスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。	<input type="checkbox"/>	不正アクセス
9-2	アカウント・ 認証管理 → p.84, 85	テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。	<input type="checkbox"/>	不正アクセス

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
2-3	マルウェア対策 → p.72, 73	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おく。	<input type="checkbox"/>	マルウェア感染
2-4	マルウェア対策 → p.72, 73	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<input type="checkbox"/>	マルウェア感染
3-2	アクセス制御・ 認可 → p.74, 75	インターネット経由で社内システムにアクセスがあった際には、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不要なIPアドレスからの通信を遮断する。	<input type="checkbox"/>	不正アクセス
3-3	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。	<input type="checkbox"/>	情報の盗聴
3-4	アクセス制御・ 認可 → p.74, 75	オンライン会議に参加するためのパスワードの設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。	<input type="checkbox"/>	情報の盗聴
3-5	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。	<input type="checkbox"/>	情報の盗聴

方式① テレワークセキュリティ 対策チェックリスト(3/4)

会社支給端末：VPN/リモートデスクトップ方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
5-3	脆弱性管理 → p.77, 78	テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新の ファームウェア を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
6-1	通信暗号化 → p.79	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のクラウドサービスを利用する場合(特に ID・ パスワード 等の入力を求められる場合)は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。	<input type="checkbox"/>	情報の盗聴
6-2	通信暗号化 → p.79	無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、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にする。	<input type="checkbox"/>	情報の盗聴
7-2	インシデント 対応・ログ管理 → p.80, 81	テレワーク端末と接続先の各システムの 時刻を同期 させる。	<input type="checkbox"/>	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 → p.80, 81	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 を収集する。	<input type="checkbox"/>	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 → p.82, 83	テレワーク端末の紛失時に備えて MDM 等を導入し、リモートからのデータ消去、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する。	<input type="checkbox"/>	盗難・紛失
8-3	データ保護 → p.82, 83	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、端末に内蔵されたハードディスクや フラッシュメモリ 等の記録媒体の暗号化を実施する ※2。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	盗難・紛失
8-4	データ保護 → p.82, 83	テレワーク端末には原則として重要情報を保管しないよう周知する。万一その必要性が生じた場合 ※3 には、 パスワード の設定やファイルの暗号化を実施し、一時的な保管のみを許可する。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	不正アクセス 盗難・紛失

※2 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。

※3 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。

方式① テレワークセキュリティ 対策チェックリスト(4/4)

会社支給端末：VPN/リモートデスクトップ方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
8-5	データ保護 → p.82, 83	オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対してはパスワードの設定や期間指定の自動削除等を実施するよう周知する。 また、上記ルールは可能な限り設定を強制する。	<input type="checkbox"/>	情報の盗聴
9-3	アカウント・ 認証管理 → p.84, 85	テレワーク端末やテレワークで利用する各システムに対して一定回数以上パスワードを誤入力した場合、それ以上のパスワード入力を受け付けないよう設定する。	<input type="checkbox"/>	不正アクセス
9-4	アカウント・ 認証管理 → p.84, 85	テレワークで利用する各システムへのアクセスには、多要素認証を求めるよう設定する。	<input type="checkbox"/>	不正アクセス
10-1	特権管理 → p.86, 87	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、業務上必要な最小限の人に付与する。	<input type="checkbox"/>	不正アクセス
10-2	特権管理 → p.86, 87	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する。	<input type="checkbox"/>	不正アクセス
10-3	特権管理 → p.86, 87	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する。	<input type="checkbox"/>	不正アクセス

方式② テレワークセキュリティ 対策チェックリスト(1/4)

会社支給端末：クラウドサービス方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↵		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
1-1	資産・構成管理 → p.71	テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。	<input type="checkbox"/>	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 → p.71	テレワークで利用しているシステムや取り扱い <u>重要情報</u> を把握する。	<input type="checkbox"/>	不正アクセス 情報の盗聴
2-1	マルウェア対策 → p.72、73	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を有効にする ^{※1} 。 ウイルス対策ソフトの <u>定義ファイル</u> を自動更新する設定にするか、手動で更新するルールを作成する。	<input type="checkbox"/>	マルウェア感染
2-2	マルウェア対策 → p.72、73	不審なメールを開封し、メールに記載されている URL をクリックしたり、添付ファイルを開いたりしないよう周知する。	<input type="checkbox"/>	マルウェア感染
3-1	アクセス制御・ 認可 → p.74、75	許可された人のみが重要情報を利用できるよう、システムによる <u>アクセス制御</u> やファイルに対する <u>パスワード</u> 設定等を行う。	<input type="checkbox"/>	不正アクセス
4-1	物理セキュリティ → p.76	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	<input type="checkbox"/>	情報の盗聴
4-2	物理セキュリティ → p.76	テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。	<input type="checkbox"/>	情報の盗聴
5-1	脆弱性管理 → p.77、78	テレワーク端末にはメーカーサポートが終了した <u>OS</u> やアプリケーションを利用しないよう周知する。	<input type="checkbox"/>	不正アクセス
5-2	脆弱性管理 → p.77、78	テレワーク端末の <u>OS</u> やアプリケーションに対して最新の <u>セキュリティアップデート</u> を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
7-1	インシデント 対応・ログ管理 → p.80、81	セキュリティインシデントの発生時や、そのおそれがある状況に備えて、 <u>対応手順</u> 及び関係者への <u>各種連絡体制</u> を定め、従業員に緊急連絡先を周知する。	<input type="checkbox"/>	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 → p.82、83	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<input type="checkbox"/>	盗難・紛失

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。

方式② テレワークセキュリティ 対策チェックリスト(2/4)

会社支給端末：クラウドサービス方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
9-1	アカウント・ 認証管理 → p.84, 85	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 <u>パスワード</u> には、「長く」「複雑な」 <u>パスワード</u> を設定するようルール化する。また、可能な限り <u>パスワード強度</u> の設定を強制する。	<input type="checkbox"/>	不正アクセス
9-2	アカウント・ 認証管理 → p.84, 85	テレワーク端末のログイン <u>パスワード</u> や、テレワークで利用する各システムの初期 <u>パスワード</u> は必ず変更するよう設定する。	<input type="checkbox"/>	不正アクセス

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
2-3	マルウェア対策 → p.72, 73	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おく。	<input type="checkbox"/>	マルウェア感染
2-4	マルウェア対策 → p.72, 73	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<input type="checkbox"/>	マルウェア感染
3-3	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。	<input type="checkbox"/>	情報の盗聴
3-4	アクセス制御・ 認可 → p.74, 75	オンライン会議に参加するための <u>パスワード</u> の設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。	<input type="checkbox"/>	情報の盗聴
3-5	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。	<input type="checkbox"/>	情報の盗聴
5-3	脆弱性管理 → p.77, 78	テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新の <u>ファームウェア</u> を適用するよう周知する。	<input type="checkbox"/>	不正アクセス

方式② テレワークセキュリティ 対策チェックリスト(3/4)

会社支給端末：クラウドサービス方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
6-1	通信暗号化 → p.79	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のクラウドサービスを利用する場合(特に ID・ <u>パスワード</u> 等の入力を求められる場合は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。	<input type="checkbox"/>	情報の盗聴
6-2	通信暗号化 → p.79	無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、無線の暗号化 <u>パスワード</u> は第三者に推測されにくいものにする。	<input type="checkbox"/>	情報の盗聴
7-2	インシデント 対応・ログ管理 → p.80、81	テレワーク端末と接続先の各システムの <u>時刻を同期</u> させる。	<input type="checkbox"/>	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 → p.82、83	テレワーク端末の紛失時に備えて <u>MDM</u> 等を導入し、リモートからのデータ消去、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する。	<input type="checkbox"/>	盗難・紛失
8-3	データ保護 → p.82、83	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、端末に内蔵されたハードディスクや <u>フラッシュメモリ</u> 等の記録媒体の暗号化を実施する ※2。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	盗難・紛失
8-4	データ保護 → p.82、83	テレワーク端末には原則として重要情報を保管しないよう周知する。万一その必要性が生じた場合 ※3 には、 <u>パスワード</u> の設定やファイルの暗号化を実施し、一時的な保管のみを許可する。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	不正アクセス 盗難・紛失
8-5	データ保護 → p.82、83	オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対しては <u>パスワード</u> の設定や期間指定の自動削除等を実施するよう周知する。また、上記ルールは可能な限り設定を強制する。	<input type="checkbox"/>	情報の盗聴

※2 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。

※3 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。

方式② テレワークセキュリティ 対策チェックリスト(4/4)

会社支給端末：クラウドサービス方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
9-3	アカウント・ 認証管理 → p.84, 85	テレワーク端末やテレワークで利用する各システムに対して一定回数以上 <u>パスワード</u> を誤入力した場合、それ以上の <u>パスワード</u> 入力を受け付けられないよう設定する。	<input type="checkbox"/>	不正アクセス
9-4	アカウント・ 認証管理 → p.84, 85	テレワークで利用する各システムへのアクセスには、多要素認証を求めよう設定する。	<input type="checkbox"/>	不正アクセス
10-1	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、業務上必要な最小限の人に付与する。	<input type="checkbox"/>	不正アクセス
10-2	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限のパスワード</u> には、強力な <u>パスワード</u> ポリシーを適用する。	<input type="checkbox"/>	不正アクセス
10-3	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、必要な作業時のみ利用する。	<input type="checkbox"/>	不正アクセス

方式③ テレワークセキュリティ 対策チェックリスト(1/3)

会社支給端末：スタンドアロン方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↵		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
1-1	資産・構成管理 → p.71	テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。	<input type="checkbox"/>	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 → p.71	テレワークで利用しているシステムや取り扱う <u>重要情報</u> を把握する。	<input type="checkbox"/>	不正アクセス 情報の盗聴
2-1	マルウェア対策 → p.72、73	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を有効にする ^{※1} 。 ウイルス対策ソフトの <u>定義ファイル</u> を自動更新する設定にするか、手動で更新するルールを作成する。	<input type="checkbox"/>	マルウェア感染
3-1	アクセス制御・ 認可 → p.74、75	許可された人のみが重要情報を利用できるよう、システムによる <u>アクセス制御</u> やファイルに対する <u>パスワード</u> 設定等を行う。	<input type="checkbox"/>	不正アクセス
4-1	物理セキュリティ → p.76	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	<input type="checkbox"/>	情報の盗聴
4-2	物理セキュリティ → p.76	テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。	<input type="checkbox"/>	情報の盗聴
5-1	脆弱性管理 → p.77、78	テレワーク端末にはメーカーサポートが終了した <u>OS</u> やアプリケーションを利用しないよう周知する。	<input type="checkbox"/>	不正アクセス
5-2	脆弱性管理 → p.77、78	テレワーク端末の <u>OS</u> やアプリケーションに対して最新の <u>セキュリティアップデート</u> を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
7-1	インシデント 対応・ログ管理 → p.80、81	セキュリティインシデントの発生時や、そのおそれがある状況に備えて、 <u>対応手順</u> 及び関係者への <u>各種連絡体制</u> を定め、従業員に緊急連絡先を周知する。	<input type="checkbox"/>	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 → p.82、83	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<input type="checkbox"/>	盗難・紛失

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。

方式③ テレワークセキュリティ 対策チェックリスト(2/3)

会社支給端末：スタンドアロン方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
9-1	アカウント・ 認証管理 → p.84, 85	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 <u>パスワード</u> には、「長く」「複雑な」 <u>パスワード</u> を設定するようルール化する。また、可能な限り <u>パスワード強度</u> の設定を強制する。	<input type="checkbox"/>	不正アクセス
9-2	アカウント・ 認証管理 → p.84, 85	テレワーク端末のログイン <u>パスワード</u> や、テレワークで利用する各システムの初期 <u>パスワード</u> は必ず変更するよう設定する。	<input type="checkbox"/>	不正アクセス

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
2-4	マルウェア対策 → p.72, 73	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<input type="checkbox"/>	マルウェア感染
5-3	脆弱性管理 → p.77, 78	テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新の <u>ファームウェア</u> を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
6-2	通信暗号化 → p.79	無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、無線の暗号化 <u>パスワード</u> は第三者に推測されにくいものにする。	<input type="checkbox"/>	情報の盗聴
7-2	インシデント 対応・ログ管理 → p.80, 81	テレワーク端末と接続先の各システムの <u>時刻を同期</u> させる。	<input type="checkbox"/>	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 → p.82, 83	テレワーク端末の紛失時に備えて <u>MDM</u> 等を導入し、リモートからのデータ消去、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する。	<input type="checkbox"/>	盗難・紛失
8-3	データ保護 → p.82, 83	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、端末に内蔵されたハードディスクや <u>フラッシュメモリ</u> 等の記録媒体の暗号化を実施する ※2。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	盗難・紛失

※2 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。

方式③ テレワークセキュリティ 対策チェックリスト(3/3)

会社支給端末：スタンドアロン方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
8-4	データ保護 → p.82, 83	テレワーク端末には原則として重要情報を保管しないよう周知する。万一その必要性が生じた場合 ※ ³ には、 <u>パスワード</u> の設定やファイルの暗号化を実施し、一時的な保管のみを許可する。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	不正アクセス 盗難・紛失
9-3	アカウント・ 認証管理 → p.84, 85	テレワーク端末やテレワークで利用する各システムに対して一定回数以上 <u>パスワード</u> を誤入力した場合、それ以上の <u>パスワード</u> 入力を受け付けないよう設定する。	<input type="checkbox"/>	不正アクセス
9-4	アカウント・ 認証管理 → p.84, 85	テレワークで利用する各システムへのアクセスには、多要素認証を求めよう設定する。	<input type="checkbox"/>	不正アクセス
10-1	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、業務上必要な最小限の人に付与する。	<input type="checkbox"/>	不正アクセス
10-2	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> の <u>パスワード</u> には、強力な <u>パスワード</u> ポリシーを適用する。	<input type="checkbox"/>	不正アクセス
10-3	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、必要な作業時のみ利用する。	<input type="checkbox"/>	不正アクセス

※³ 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。

- Memo -

方式④ テレワークセキュリティ 対策チェックリスト(1/4)

会社支給端末：セキュアブラウザ方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↵		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
1-1	資産・構成管理 → p.71	テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。	<input type="checkbox"/>	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 → p.71	テレワークで利用しているシステムや取り扱い <u>重要情報</u> を把握する。	<input type="checkbox"/>	不正アクセス 情報の盗聴
2-1	マルウェア対策 → p.72、73	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を有効にする ^{※1} 。 ウイルス対策ソフトの <u>定義ファイル</u> を自動更新する設定にするか、手動で更新するルールを作成する。	<input type="checkbox"/>	マルウェア感染
2-2	マルウェア対策 → p.72、73	不審なメールを開封し、メールに記載されている URL をクリックしたり、添付ファイルを開いたりしないよう周知する。	<input type="checkbox"/>	マルウェア感染
3-1	アクセス制御・ 認可 → p.74、75	許可された人のみが重要情報を利用できるよう、システムによる <u>アクセス制御</u> やファイルに対する <u>パスワード</u> 設定等を行う。	<input type="checkbox"/>	不正アクセス
4-1	物理セキュリティ → p.76	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	<input type="checkbox"/>	情報の盗聴
4-2	物理セキュリティ → p.76	テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。	<input type="checkbox"/>	情報の盗聴
5-1	脆弱性管理 → p.77、78	テレワーク端末にはメーカーサポートが終了した <u>OS</u> やアプリケーションを利用しないよう周知する。	<input type="checkbox"/>	不正アクセス
5-2	脆弱性管理 → p.77、78	テレワーク端末の <u>OS</u> やアプリケーションに対して最新の <u>セキュリティアップデート</u> を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
7-1	インシデント 対応・ログ管理 → p.80、81	セキュリティインシデントの発生時や、そのおそれがある状況に備えて、 <u>対応手順</u> 及び関係者への <u>各種連絡体制</u> を定め、従業員に緊急連絡先を周知する。	<input type="checkbox"/>	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 → p.82、83	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<input type="checkbox"/>	盗難・紛失

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。

方式④ テレワークセキュリティ 対策チェックリスト(2/4)

会社支給端末：セキュアブラウザ方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
9-1	アカウント・ 認証管理 → p.84, 85	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パスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。	<input type="checkbox"/>	不正アクセス
9-2	アカウント・ 認証管理 → p.84, 85	テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。	<input type="checkbox"/>	不正アクセス

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
2-3	マルウェア対策 → p.72, 73	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おく。	<input type="checkbox"/>	マルウェア感染
2-4	マルウェア対策 → p.72, 73	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<input type="checkbox"/>	マルウェア感染
3-2	アクセス制御・ 認可 → p.74, 75	インターネット経由で社内システムにアクセスがあった際には、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不要な IP アドレスからの通信を遮断する。	<input type="checkbox"/>	不正アクセス
3-3	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。	<input type="checkbox"/>	情報の盗聴
3-4	アクセス制御・ 認可 → p.74, 75	オンライン会議に参加するためのパスワードの設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。	<input type="checkbox"/>	情報の盗聴
3-5	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。	<input type="checkbox"/>	情報の盗聴
5-3	脆弱性管理 → p.77, 78	テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新のファームウェアを適用するよう周知する。	<input type="checkbox"/>	不正アクセス

方式④ テレワークセキュリティ 対策チェックリスト(3/4)

会社支給端末：セキュアブラウザ方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
6-1	通信暗号化 → p.79	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のクラウドサービスを利用する場合(特に ID・ <u>パスワード</u> 等の入力を求められる場合は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。	<input type="checkbox"/>	情報の盗聴
6-2	通信暗号化 → p.79	無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、無線の暗号化 <u>パスワード</u> は第三者に推測されにくいものにする。	<input type="checkbox"/>	情報の盗聴
7-2	インシデント 対応・ログ管理 → p.80, 81	テレワーク端末と接続先の各システムの <u>時刻を同期</u> させる。	<input type="checkbox"/>	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 → p.80, 81	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 <u>アクセスログ</u> を収集する。	<input type="checkbox"/>	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 → p.82, 83	テレワーク端末の紛失時に備えて <u>MDM</u> 等を導入し、リモートからのデータ消去、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する。	<input type="checkbox"/>	盗難・紛失
8-5	データ保護 → p.82, 83	オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対しては <u>パスワード</u> の設定や期間指定の自動削除等を実施するよう周知する。 また、上記ルールは可能な限り設定を強制する。	<input type="checkbox"/>	情報の盗聴
9-3	アカウント・ 認証管理 → p.84, 85	テレワーク端末やテレワークで利用する各システムに対して一定回数以上 <u>パスワード</u> を誤入力した場合、それ以上の <u>パスワード</u> 入力を受け付けられないよう設定する。	<input type="checkbox"/>	不正アクセス
9-4	アカウント・ 認証管理 → p.84, 85	テレワークで利用する各システムへのアクセスには、多要素認証を求めるよう設定する。	<input type="checkbox"/>	不正アクセス

方式④ テレワークセキュリティ 対策チェックリスト(4/4)

会社支給端末：セキュアブラウザ方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
10-1	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、業務上必要な最小限の人に付与する。	<input type="checkbox"/>	不正アクセス
10-2	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限のパスワード</u> には、強力な <u>パスワード</u> ポリシーを適用する。	<input type="checkbox"/>	不正アクセス
10-3	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、必要な作業時のみ利用する。	<input type="checkbox"/>	不正アクセス

方式⑤ テレワークセキュリティ 対策チェックリスト(1/4)

個人所有端末：VPN/リモートデスクトップ方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↵		
No.	分類 [p.70～87]	対策内容	対応済	想定脅威 [p.65～69]
1-1	資産・構成管理 → p.71	テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。	<input type="checkbox"/>	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 → p.71	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する。	<input type="checkbox"/>	不正アクセス 情報の盗聴
2-1	マルウェア対策 → p.72、73	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を有効にする※1。 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にするか、手動で更新するルールを作成する。	<input type="checkbox"/>	マルウェア感染
2-2	マルウェア対策 → p.72、73	不審なメールを開封し、メールに記載されているURLをクリックしたり、添付ファイルを開いたりしないよう周知する。	<input type="checkbox"/>	マルウェア感染
3-1	アクセス制御・ 認可 → p.74、75	許可された人のみが重要情報を利用できるよう、システムによるアクセス制御やファイルに対するパスワード設定等を行う。	<input type="checkbox"/>	不正アクセス
4-1	物理セキュリティ → p.76	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	<input type="checkbox"/>	情報の盗聴
4-2	物理セキュリティ → p.76	テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。	<input type="checkbox"/>	情報の盗聴
5-1	脆弱性管理 → p.77、78	テレワーク端末にはメーカーサポートが終了したOSやアプリケーションを利用しないよう周知する。	<input type="checkbox"/>	不正アクセス
5-2	脆弱性管理 → p.77、78	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するよう周知する。	<input type="checkbox"/>	不正アクセス
5-4	脆弱性管理 → p.77、78	テレワーク端末から社内にリモートアクセスするためのVPN機器等には、メーカーサポートが終了した製品を利用せず、最新のセキュリティアップデートを適用する。	<input type="checkbox"/>	不正アクセス
7-1	インシデント 対応・ログ管理 → p.80、81	セキュリティインシデントの発生時や、そのおそれがある状況に備えて、対応手順及び関係者への各種連絡体制を定め、従業員に緊急連絡先を周知する。	<input type="checkbox"/>	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。

方式⑤ テレワークセキュリティ 対策チェックリスト(2/4)

個人所有端末：VPN/リモートデスクトップ方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
8-1	データ保護 → p.82, 83	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<input type="checkbox"/>	盗難・紛失
9-1	アカウント・ 認証管理 → p.84, 85	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パスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。	<input type="checkbox"/>	不正アクセス
9-2	アカウント・ 認証管理 → p.84, 85	テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。	<input type="checkbox"/>	不正アクセス

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
2-3	マルウェア対策 → p.72, 73	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おく。	<input type="checkbox"/>	マルウェア感染
2-4	マルウェア対策 → p.72, 73	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<input type="checkbox"/>	マルウェア感染
3-2	アクセス制御・ 認可 → p.74, 75	インターネット経由で社内システムにアクセスがあった際には、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不要なIPアドレスからの通信を遮断する。	<input type="checkbox"/>	不正アクセス
3-3	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。	<input type="checkbox"/>	情報の盗聴
3-4	アクセス制御・ 認可 → p.74, 75	オンライン会議に参加するためのパスワードの設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。	<input type="checkbox"/>	情報の盗聴
3-5	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。	<input type="checkbox"/>	情報の盗聴

方式⑤ テレワークセキュリティ 対策チェックリスト(3/4)

個人所有端末：VPN/リモートデスクトップ方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
5-3	脆弱性管理 → p.77, 78	テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新の ファームウェア を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
6-1	通信暗号化 → p.79	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のクラウドサービスを利用する場合(特に ID・ パスワード 等の入力を求められる場合)は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。	<input type="checkbox"/>	情報の盗聴
6-2	通信暗号化 → p.79	無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、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にする。	<input type="checkbox"/>	情報の盗聴
7-2	インシデント 対応・ログ管理 → p.80, 81	テレワーク端末と接続先の各システムの 時刻を同期 させる。	<input type="checkbox"/>	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 → p.80, 81	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 を収集する。	<input type="checkbox"/>	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 → p.82, 83	テレワーク端末の紛失時に備えて MDM 等を導入し、リモートからのデータ消去、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する。	<input type="checkbox"/>	盗難・紛失
8-3	データ保護 → p.82, 83	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、端末に内蔵されたハードディスクや フラッシュメモリ 等の記録媒体の暗号化を実施する ※2。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	盗難・紛失

※2 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。

方式⑤ テレワークセキュリティ 対策チェックリスト(4/4)

個人所有端末：VPN/リモートデスクトップ方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
8-4	データ保護 → p.82, 83	テレワーク端末には原則として重要情報を保管しないよう周知する。万一その必要性が生じた場合 ※3 には、 <u>パスワード</u> の設定やファイルの暗号化を実施し、一時的な保管のみを許可する。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	不正アクセス 盗難・紛失
8-5	データ保護 → p.82, 83	オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対しては <u>パスワード</u> の設定や期間指定の自動削除等を実施するよう周知する。 また、上記ルールは可能な限り設定を強制する。	<input type="checkbox"/>	情報の盗聴
9-4	アカウント・ 認証管理 → p.84, 85	テレワークで利用する各システムへのアクセスには、多要素認証を求めるよう設定する。	<input type="checkbox"/>	不正アクセス
10-1	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、業務上必要な最小限の人に付与する。	<input type="checkbox"/>	不正アクセス
10-2	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限のパスワード</u> には、強力な <u>パスワード</u> ポリシーを適用する。	<input type="checkbox"/>	不正アクセス

※3 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。

方式⑥ テレワークセキュリティ 対策チェックリスト(1/4)

個人所有端末：クラウドサービス方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
1-1	資産・構成管理 → p.71	テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。	<input type="checkbox"/>	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 → p.71	テレワークで利用しているシステムや取り扱う <u>重要情報</u> を把握する。	<input type="checkbox"/>	不正アクセス 情報の盗聴
2-1	マルウェア対策 → p.72、73	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を有効にする ^{※1} 。 ウイルス対策ソフトの <u>定義ファイル</u> を自動更新する設定にするか、手動で更新するルールを作成する。	<input type="checkbox"/>	マルウェア感染
2-2	マルウェア対策 → p.72、73	不審なメールを開封し、メールに記載されている URL をクリックしたり、添付ファイルを開いたりしないよう周知する。	<input type="checkbox"/>	マルウェア感染
3-1	アクセス制御・ 認可 → p.74、75	許可された人のみが重要情報を利用できるよう、システムによる <u>アクセス制御</u> やファイルに対する <u>パスワード</u> 設定等を行う。	<input type="checkbox"/>	不正アクセス
4-1	物理セキュリティ → p.76	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	<input type="checkbox"/>	情報の盗聴
4-2	物理セキュリティ → p.76	テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。	<input type="checkbox"/>	情報の盗聴
5-1	脆弱性管理 → p.77、78	テレワーク端末にはメーカーサポートが終了した <u>OS</u> やアプリケーションを利用しないよう周知する。	<input type="checkbox"/>	不正アクセス
5-2	脆弱性管理 → p.77、78	テレワーク端末の <u>OS</u> やアプリケーションに対して最新の <u>セキュリティアップデート</u> を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
7-1	インシデント 対応・ログ管理 → p.80、81	セキュリティインシデントの発生時や、そのおそれがある状況に備えて、 <u>対応手順</u> 及び関係者への <u>各種連絡体制</u> を定め、従業員に緊急連絡先を周知する。	<input type="checkbox"/>	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 → p.82、83	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<input type="checkbox"/>	盗難・紛失

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。

方式⑥ テレワークセキュリティ 対策チェックリスト(2/4)

個人所有端末：クラウドサービス方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70～87]	対策内容	対応済	想定脅威 [p.65～69]
9-1	アカウント・ 認証管理 → p.84, 85	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パスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。	<input type="checkbox"/>	不正アクセス
9-2	アカウント・ 認証管理 → p.84, 85	テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。	<input type="checkbox"/>	不正アクセス

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70～87]	対策内容	対応済	想定脅威 [p.65～69]
2-3	マルウェア対策 → p.72, 73	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おく。	<input type="checkbox"/>	マルウェア感染
2-4	マルウェア対策 → p.72, 73	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<input type="checkbox"/>	マルウェア感染
3-3	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。	<input type="checkbox"/>	情報の盗聴
3-4	アクセス制御・ 認可 → p.74, 75	オンライン会議に参加するためのパスワードの設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。	<input type="checkbox"/>	情報の盗聴
3-5	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。	<input type="checkbox"/>	情報の盗聴
5-3	脆弱性管理 → p.77, 78	テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新のファームウェアを適用するよう周知する。	<input type="checkbox"/>	不正アクセス

方式⑥ テレワークセキュリティ 対策チェックリスト(3/4)

個人所有端末：クラウドサービス方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↵		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
6-1	通信暗号化 → p.79	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のクラウドサービスを利用する場合(特に ID・ パスワード 等の入力を求められる場合は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。	<input type="checkbox"/>	情報の盗聴
6-2	通信暗号化 → p.79	無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、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にする。	<input type="checkbox"/>	情報の盗聴
7-2	インシデント 対応・ログ管理 → p.80, 81	テレワーク端末と接続先の各システムの 時刻を同期 させる。	<input type="checkbox"/>	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 → p.82, 83	テレワーク端末の紛失時に備えて MDM 等を導入し、リモートからのデータ消去、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する。	<input type="checkbox"/>	盗難・紛失
8-3	データ保護 → p.82, 83	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、端末に内蔵されたハードディスクや フラッシュメモリ 等の記録媒体の暗号化を実施する ^{※2} 。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	盗難・紛失
8-4	データ保護 → p.82, 83	テレワーク端末には原則として重要情報を保管しないよう周知する。万一その必要性が生じた場合 ^{※3} には、 パスワード の設定やファイルの暗号化を実施し、一時的な保管のみを許可する。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	不正アクセス 盗難・紛失
8-5	データ保護 → p.82, 83	オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対しては パスワード の設定や期間指定の自動削除等を実施するよう周知する。また、上記ルールは可能な限り設定を強制する。	<input type="checkbox"/>	情報の盗聴

※2 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。

※3 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。

方式⑥ テレワークセキュリティ 対策チェックリスト(4/4)

個人所有端末：クラウドサービス方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
9-4	アカウント・ 認証管理 → p.84, 85	テレワークで利用する各システムへのアクセスには、多要素認証を求めるよう設定する。	<input type="checkbox"/>	不正アクセス
10-1	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、業務上必要な最小限の人に付与する。	<input type="checkbox"/>	不正アクセス
10-2	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> の <u>パスワード</u> には、強力な <u>パスワード</u> ポリシーを適用する。	<input type="checkbox"/>	不正アクセス

方式⑦ テレワークセキュリティ 対策チェックリスト(1/3)

個人所有端末：スタンドアロン方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
1-1	資産・構成管理 → p.71	テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。	<input type="checkbox"/>	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 → p.71	テレワークで利用しているシステムや取り扱う <u>重要情報</u> を把握する。	<input type="checkbox"/>	不正アクセス 情報の盗聴
2-1	マルウェア対策 → p.72、73	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を有効にする ^{※1} 。 ウイルス対策ソフトの <u>定義ファイル</u> を自動更新する設定にするか、手動で更新するルールを作成する。	<input type="checkbox"/>	マルウェア感染
3-1	アクセス制御・ 認可 → p.74、75	許可された人のみが重要情報を利用できるよう、システムによる <u>アクセス制御</u> やファイルに対する <u>パスワード</u> 設定等を行う。	<input type="checkbox"/>	不正アクセス
4-1	物理セキュリティ → p.76	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	<input type="checkbox"/>	情報の盗聴
4-2	物理セキュリティ → p.76	テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。	<input type="checkbox"/>	情報の盗聴
5-1	脆弱性管理 → p.77、78	テレワーク端末にはメーカーサポートが終了した <u>OS</u> やアプリケーションを利用しないよう周知する。	<input type="checkbox"/>	不正アクセス
5-2	脆弱性管理 → p.77、78	テレワーク端末の <u>OS</u> やアプリケーションに対して最新の <u>セキュリティアップデート</u> を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
7-1	インシデント 対応・ログ管理 → p.80、81	セキュリティインシデントの発生時や、そのおそれがある状況に備えて、 <u>対応手順</u> 及び関係者への <u>各種連絡体制</u> を定め、従業員に緊急連絡先を周知する。	<input type="checkbox"/>	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 → p.82、83	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<input type="checkbox"/>	盗難・紛失

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。

方式⑦ テレワークセキュリティ 対策チェックリスト(2/3)

個人所有端末：スタンドアロン方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
9-1	アカウント・ 認証管理 → p.84, 85	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 <u>パスワード</u> には、「長く」「複雑な」 <u>パスワード</u> を設定するようルール化する。また、可能な限り <u>パスワード強度</u> の設定を強制する。	<input type="checkbox"/>	不正アクセス
9-2	アカウント・ 認証管理 → p.84, 85	テレワーク端末のログイン <u>パスワード</u> や、テレワークで利用する各システムの初期 <u>パスワード</u> は必ず変更するよう設定する。	<input type="checkbox"/>	不正アクセス

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
2-4	マルウェア対策 → p.72, 73	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<input type="checkbox"/>	マルウェア感染
5-3	脆弱性管理 → p.77, 78	テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新の <u>ファームウェア</u> を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
6-2	通信暗号化 → p.79	無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、無線の暗号化 <u>パスワード</u> は第三者に推測されにくいものにする。	<input type="checkbox"/>	情報の盗聴
7-2	インシデント 対応・ログ管理 → p.80, 81	テレワーク端末と接続先の各システムの <u>時刻を同期</u> させる。	<input type="checkbox"/>	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 → p.82, 83	テレワーク端末の紛失時に備えて <u>MDM</u> 等を導入し、リモートからのデータ消去、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する。	<input type="checkbox"/>	盗難・紛失
8-3	データ保護 → p.82, 83	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、端末に内蔵されたハードディスクや <u>フラッシュメモリ</u> 等の記録媒体の暗号化を実施する ※2。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	盗難・紛失

※2 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。

方式⑦ テレワークセキュリティ 対策チェックリスト(3/3)

個人所有端末：スタンドアロン方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
8-4	データ保護 → p.82, 83	テレワーク端末には原則として重要情報を保管しないよう周知する。万一その必要性が生じた場合 ※ ³ には、 <u>パスワード</u> の設定やファイルの暗号化を実施し、一時的な保管のみを許可する。ただし、端末に会社のデータを保管しない場合を除く。	<input type="checkbox"/>	不正アクセス 盗難・紛失
9-4	アカウント・ 認証管理 → p.84, 85	テレワークで利用する各システムへのアクセスには、多要素認証を求めよう設定する。	<input type="checkbox"/>	不正アクセス
10-1	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、業務上必要な最小限の人に付与する。	<input type="checkbox"/>	不正アクセス
10-2	特権管理 → p.86, 87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限のパスワード</u> には、強力な <u>パスワード</u> ポリシーを適用する。	<input type="checkbox"/>	不正アクセス

※³ 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。

- Memo -

方式⑧ テレワークセキュリティ 対策チェックリスト(1/4)

個人所有端末：セキュアブラウザ方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↵		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
1-1	資産・構成管理 → p.71	テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。	<input type="checkbox"/>	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 → p.71	テレワークで利用しているシステムや取り扱う <u>重要情報</u> を把握する。	<input type="checkbox"/>	不正アクセス 情報の盗聴
2-1	マルウェア対策 → p.72、73	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を有効にする ^{※1} 。 ウイルス対策ソフトの <u>定義ファイル</u> を自動更新する設定にするか、手動で更新するルールを作成する。	<input type="checkbox"/>	マルウェア感染
2-2	マルウェア対策 → p.72、73	不審なメールを開封し、メールに記載されている URL をクリックしたり、添付ファイルを開いたりしないよう周知する。	<input type="checkbox"/>	マルウェア感染
3-1	アクセス制御・ 認可 → p.74、75	許可された人のみが重要情報を利用できるよう、システムによる <u>アクセス制御</u> やファイルに対する <u>パスワード</u> 設定等を行う。	<input type="checkbox"/>	不正アクセス
4-1	物理セキュリティ → p.76	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	<input type="checkbox"/>	情報の盗聴
4-2	物理セキュリティ → p.76	テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。	<input type="checkbox"/>	情報の盗聴
5-1	脆弱性管理 → p.77、78	テレワーク端末にはメーカーサポートが終了した <u>OS</u> やアプリケーションを利用しないよう周知する。	<input type="checkbox"/>	不正アクセス
5-2	脆弱性管理 → p.77、78	テレワーク端末の <u>OS</u> やアプリケーションに対して最新の <u>セキュリティアップデート</u> を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
7-1	インシデント 対応・ログ管理 → p.80、81	セキュリティインシデントの発生時や、そのおそれがある状況に備えて、 <u>対応手順</u> 及び関係者への <u>各種連絡体制</u> を定め、従業員に緊急連絡先を周知する。	<input type="checkbox"/>	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 → p.82、83	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	<input type="checkbox"/>	盗難・紛失

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。

方式⑧ テレワークセキュリティ 対策チェックリスト(2/4)

個人所有端末：セキュアブラウザ方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：◎		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
9-1	アカウント・ 認証管理 → p.84, 85	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パスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。	<input type="checkbox"/>	不正アクセス
9-2	アカウント・ 認証管理 → p.84, 85	テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。	<input type="checkbox"/>	不正アクセス

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
2-3	マルウェア対策 → p.72, 73	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おく。	<input type="checkbox"/>	マルウェア感染
2-4	マルウェア対策 → p.72, 73	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	<input type="checkbox"/>	マルウェア感染
3-2	アクセス制御・ 認可 → p.74, 75	インターネット経由で社内システムにアクセスがあった際には、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不要な IP アドレスからの通信を遮断する。	<input type="checkbox"/>	不正アクセス
3-3	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。	<input type="checkbox"/>	情報の盗聴
3-4	アクセス制御・ 認可 → p.74, 75	オンライン会議に参加するためのパスワードの設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。	<input type="checkbox"/>	情報の盗聴
3-5	アクセス制御・ 認可 → p.74, 75	オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。	<input type="checkbox"/>	情報の盗聴

方式⑧ テレワークセキュリティ 対策チェックリスト(3/4)

個人所有端末：セキュアブラウザ方式

※対策内容の下線付き用語については、p.88 以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↘		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
5-3	脆弱性管理 → p.77, 78	テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新の ファームウェア を適用するよう周知する。	<input type="checkbox"/>	不正アクセス
6-1	通信暗号化 → p.79	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のクラウドサービスを利用する場合(特に ID・ パスワード 等の入力を求められる場合)は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。	<input type="checkbox"/>	情報の盗聴
6-2	通信暗号化 → p.79	無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、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にする。	<input type="checkbox"/>	情報の盗聴
7-2	インシデント 対応・ログ管理 → p.80, 81	テレワーク端末と接続先の各システムの 時刻を同期 させる。	<input type="checkbox"/>	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 → p.80, 81	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 を収集する。	<input type="checkbox"/>	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 → p.82, 83	テレワーク端末の紛失時に備えて MDM 等を導入し、リモートからのデータ消去、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する。	<input type="checkbox"/>	盗難・紛失
8-5	データ保護 → p.82, 83	オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対しては パスワード の設定や期間指定の自動削除等を実施するよう周知する。 また、上記ルールは可能な限り設定を強制する。	<input type="checkbox"/>	情報の盗聴
9-4	アカウント・ 認証管理 → p.84, 85	テレワークで利用する各システムへのアクセスには、多要素認証を求めるよう設定する。	<input type="checkbox"/>	不正アクセス

方式⑧ テレワークセキュリティ 対策チェックリスト(4/4)

個人所有端末：セキュアブラウザ方式

※対策内容の下線付き用語については、p.88以降で解説しています。

優先度：○		A3 見開きで印刷して、問題なければ✓チェックしましょう。↴		
No.	分類 [p.70~87]	対策内容	対応済	想定脅威 [p.65~69]
10-1	特権管理 → p.86、87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限</u> は、業務上必要な最小限の人に付与する。	<input type="checkbox"/>	不正アクセス
10-2	特権管理 → p.86、87	テレワーク端末やテレワークで利用する各システムの <u>管理者権限のパスワード</u> には、強力な <u>パスワード</u> ポリシーを適用する。	<input type="checkbox"/>	不正アクセス

第2部

2. 対策チェックリストの設定例一覧

対策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した「設定解説資料」を作成しています。

● テレワークツール設定解説資料【総務省】

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

- Cisco Webex Meetings
- Microsoft Teams
- Zoom
- Windows
- Mac
- iOS
- Android
- LanScope An
- Exchange Online
- Gmail
- Teams_chat
- LINE
- OneDrive
- Googleドライブ
- Dropbox
- YAMAHA VPNルーター
- Cisco ASA
- 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

※設定解説資料については、特定の製品の利用を促したり、避けるよう勧めたりするものではありません。

第2部

3. セキュリティ対策一覧

「第2部 1. テレワークセキュリティ 対策チェックリスト(p.25～)」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。

※対策内容の下線付き用語については、p.88以降で解説しています。

※各方式のチェック欄で、「/」は対象外です。

No.	分類	対策内容	想定脅威	対策を怠った場合の影響	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	テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。	マルウェア感染 不正アクセス 盗難・紛失	セキュリティ対策を実施していない端末が存在し、マルウェア感染のリスクが高まるほか、端末の盗難や紛失時に被害状況を把握できない。	◎		✓	✓	✓	✓	✓	✓	✓	✓
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い <u>重要情報</u> を把握する。	不正アクセス 情報の盗聴	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かどうか把握できない。	◎		✓	✓	✓	✓	✓	✓	✓	✓
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を有効にする※1。ウイルス対策ソフトの <u>定義ファイル</u> を自動更新する設定にするか、手動で更新するルールを作成する。	マルウェア感染	ウイルス定義ファイルが最新でないために、テレワーク端末がマルウェアに感染するリスクが高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。

No.	分類	対策内容	想定脅威	対策を怠った場合の影響	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
2-2	マルウェア対策	不審なメールを開封し、メールに記載されているURLをクリックしたり、添付ファイルを開いたりしないよう周知する。	マルウェア感染	悪意あるサイトに誘導され、マルウェアに感染したり、重要情報にアクセスするための認証情報等が窃取されたりするリスクが高まる。	◎	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	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おく。	マルウェア感染	悪意あるサイトに誘導され、マルウェアに感染したり、重要情報にアクセスするための認証情報等が窃取されたりするリスクが高まる。	○	クラウドサービス（Web メール）の利用無しの場合は対象外	✓	✓	△	✓	✓	✓	△	✓
2-4	マルウェア対策	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。	マルウェア感染	安全性が確認できない方法でインストールすると、正規のアプリケーションを模したマルウェアに感染するリスクが高まる。	○		✓	✓	✓	✓	✓	✓	✓	✓
3-1	アクセス制御・認可	許可された人のみが重要情報を利用できるよう、システムによる アクセス制御 やファイルに対する パスワード 設定等を行う。	不正アクセス	本来アクセス権限が必要で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で、重要情報が流出するリスクが高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓
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があった際には、 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不要なIPアドレスからの通信を遮断する。	不正アクセス	脆弱性を突いた攻撃やアカウントのなりすまし等の悪意のある攻撃により不正アクセスされるリスクが高まる。	○	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、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。	情報の盗聴	不適切な利用者が不正に参加していることに気づかず、情報漏えいのリスクが高まる。	○	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	オンライン会議に参加するための パスワード の設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。	情報の盗聴	不適切な利用者が不正に参加し、情報漏えいにつながるリスクが高まる。	○	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	✓	✓	△	✓	✓	✓	△	✓

No.	分類	対策内容	想定脅威	対策を怠った場合の影響	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
3-5	アクセス制御・認可	オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。	情報の盗聴	不適切な利用者が不正に参加していることに気づかず、情報漏えいのリスクが高まる。	○	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	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	情報の盗聴	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高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓
4-2	物理セキュリティ	テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。	情報の盗聴	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高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓
5-1	脆弱性管理	テレワーク端末にはメーカーサポートが終了したOSやアプリケーションを利用しないよう周知する。	不正アクセス	セキュリティアップデートが行えないため、製品の脆弱性を突いた攻撃により不正アクセス等のリスクが高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓
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するよう周知する。	不正アクセス	製品の脆弱性を突いた攻撃により不正アクセス等のリスクが高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓
5-3	脆弱性管理	テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新のファームウェアを適用するよう周知する。	不正アクセス	ファームウェアの脆弱性を突いた攻撃により不正アクセス等のリスクが高まる。	○		✓	✓	✓	✓	✓	✓	✓	✓
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ためのVPN機器等には、メーカーサポートが終了した製品を利用せず、最新のセキュリティアップデートを適用する。	不正アクセス	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口となるため、ファームウェアの脆弱性を突いた攻撃により不正アクセス等のリスクが高まる。	◎		✓	△	△	△	✓	△	△	△
6-1	通信暗号化	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のクラウドサービスを利用する場合(特にID・パスワード等の入力求められる場合は、暗号化されたHTTPS通信であること、接続先のURLが正しいことを確認するよう周知する。	情報の盗聴	通信内容を盗み見られ、情報漏えいのリスクが高まる。	○	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、セキュリティ方式として「WPA2」又は「WPA3」を利用し、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にする。	情報の盗聴	通信内容を盗み見られ、情報漏えいのリスクが高まる。	○		✓	✓	✓	✓	✓	✓	✓	✓

No.	分類	対策内容	想定脅威	対策を怠った場合の影響	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
7-1	インシデント対応・ログ管理	セキュリティインシデントの発生時や、そのおそれがある状況に備えて、 対応手順 及び関係者への 各種連絡体制 を定め、従業員に緊急連絡先を周知する。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴	セキュリティインシデントが発生した事実の把握や被害拡大の早期防止ができず、被害が拡大するリスクが高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓
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 時刻を同期 させる。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴	セキュリティインシデントの原因調査において、原因や被害状況の特定、絞り込みの難易度が高まる。結果として適切な対応が遅れ、被害が拡大するリスクが高まる。	○		✓	✓	✓	✓	✓	✓	✓	✓
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 を収集する。	マルウェア感染 不正アクセス 盗難・紛失 情報の盗聴	セキュリティインシデントの原因調査において、原因や被害状況の特定、絞り込みの難易度が高まる。結果として適切な対応が遅れ、被害が拡大するリスクが高まる。	○	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	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	盗難・紛失	紛失時の早期発見が困難となり、端末を取得した悪意のある第三者が不正にアクセスし、情報漏えいにつながるリスクが高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓
8-2	データ保護	テレワーク端末の紛失時に備えて MDM 等を導入し、リモートからのデータ消去、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する。	盗難・紛失	端末を取得した悪意のある第三者が不正にアクセスし、情報漏えいにつながるリスクが高まる。	○		✓	✓	✓	✓	✓	✓	✓	✓
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、端末に内蔵されたハードディスクや フラッシュメモリ 等の記録媒体の暗号化を実施する <small>※2</small> 。ただし、端末に会社のデータを保管しない場合を除く。	盗難・紛失	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できるため、保存している情報の漏えいリスクが高まる。	○	端末に会社のデータを保管しない場合は対象外	✓	✓	✓		✓	✓	✓	

※2 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。

No.	分類	対策内容	想定脅威	対策を怠った場合の影響	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
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ないよう周知する。万一その必要性が生じた場合 ※3 には、 <u>パスワード</u> の設定やファイルの暗号化を実施し、一時的な保管のみを許可する。ただし、端末に会社のデータを保管しない場合を除く。	不正アクセス 盗難・紛失	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、情報漏えいのリスクが高まる。	○	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	オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対しては <u>パスワード</u> の設定や期間指定の自動削除等を実施するよう周知する。 また、上記ルールは可能な限り設定を強制する。	情報の盗聴	共有する予定ではない画面情報を誤操作で共有してしまったり、会議の録画ファイルが不適切な第三者に参照されたりして、情報漏えいのリスクが高まる。	○	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	✓	✓	△	✓	✓	✓	△	✓
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 <u>パスワード</u> には、「長く」「複雑な」 <u>パスワード</u> を設定するようルール化する。また、可能な限り <u>パスワード強度</u> の設定を強制する。	不正アクセス	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のリスクが高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓
9-2	アカウント・認証管理	テレワーク端末のログイン <u>パスワード</u> や、テレワークで利用する各システムの初期 <u>パスワード</u> は必ず変更するよう設定する。	不正アクセス	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のリスクが高まる。	◎		✓	✓	✓	✓	✓	✓	✓	✓
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に対して一定回数以上 <u>パスワード</u> を誤入力した場合、それ以上の <u>パスワード</u> 入力を受け付けないよう設定する。	不正アクセス	悪意のある第三者がパスワードを容易に試行できるため、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のリスクが高まる。	○	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へのアクセスには、多要素認証を求めるよう設定する。	不正アクセス	悪意のある第三者にパスワードが流出しやすくなるだけでなく、なりすましによる不正アクセスのリスクが高まる。	○		✓	✓	✓	✓	✓	✓	✓	✓

※3 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。

No.	分類	対策内容	想定脅威	対策を怠った場合の影響	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
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の 管理者権限 は、業務上必要な最小限の人に付与する。	不正アクセス	悪意のある第三者が不正に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や、誤操作による情報漏えいのリスクが高まる。	○		✓	✓	✓	✓	✓	✓	✓	✓
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する。	不正アクセス	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のリスクが高まる。	○		✓	✓	✓	✓	✓	✓	✓	✓
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する。	不正アクセス	管理者権限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高まるだけでなく、管理者権限の利用情報等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。	✓	✓	✓	✓				

参考

1. テレワーク環境を狙う脅威

ここでは、テレワーク環境における脅威について理解を深めるために、代表的な脅威の概要に加え、脅威が顕在化する流れや業務への影響を3つのステップに分けて解説しています。

また、「[第2部 1. テレワークセキュリティ 対策チェックリスト\(p.25～\)](#)」の各対策項目がいずれのステップで有効かについても併せて記載しています。セキュリティ対策を講じるに当たり、システム担当者等が対策の重要性や必要性について組織内の理解を促すためにお役立てください。

(1) マルウェア感染

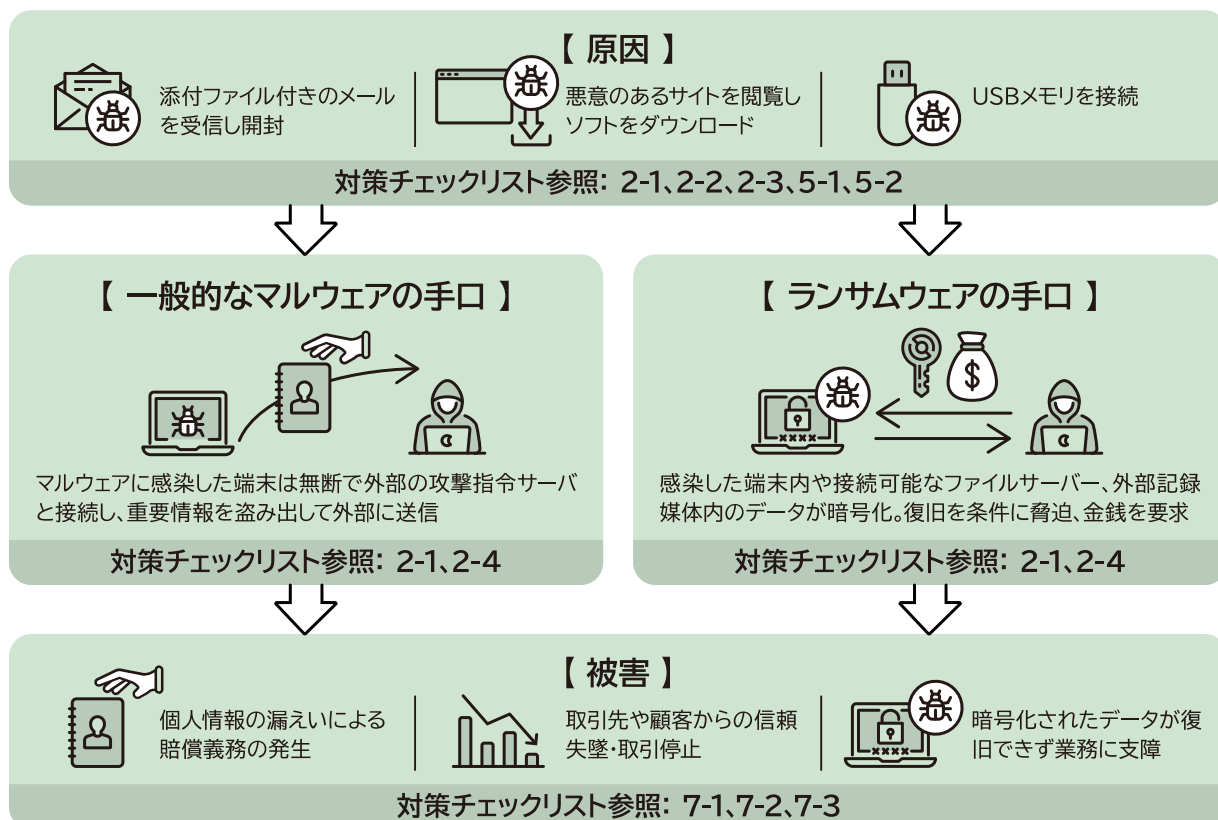


「マルウェア」とは、不正かつ有害な動作を行う目的で作成された悪意のあるソフトウェアや悪質なプログラムの総称です。一般的に「コンピュータウイルス」と呼ばれるものもマルウェアの一種です。昨今話題になっているランサムウェアもマルウェアの一種で、感染した端末をロックしたり、端末上のデータを暗号化して使用不能にしたりします。

このような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「マルウェア感染」と呼びます。マルウェアによる攻撃は高度化しているため、ここで紹介する添付ファイルの開封やソフトウェア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。

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」等につながるだけでなく、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」となる可能性もあります。

一方、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することにより「業務停止」につなが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替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。

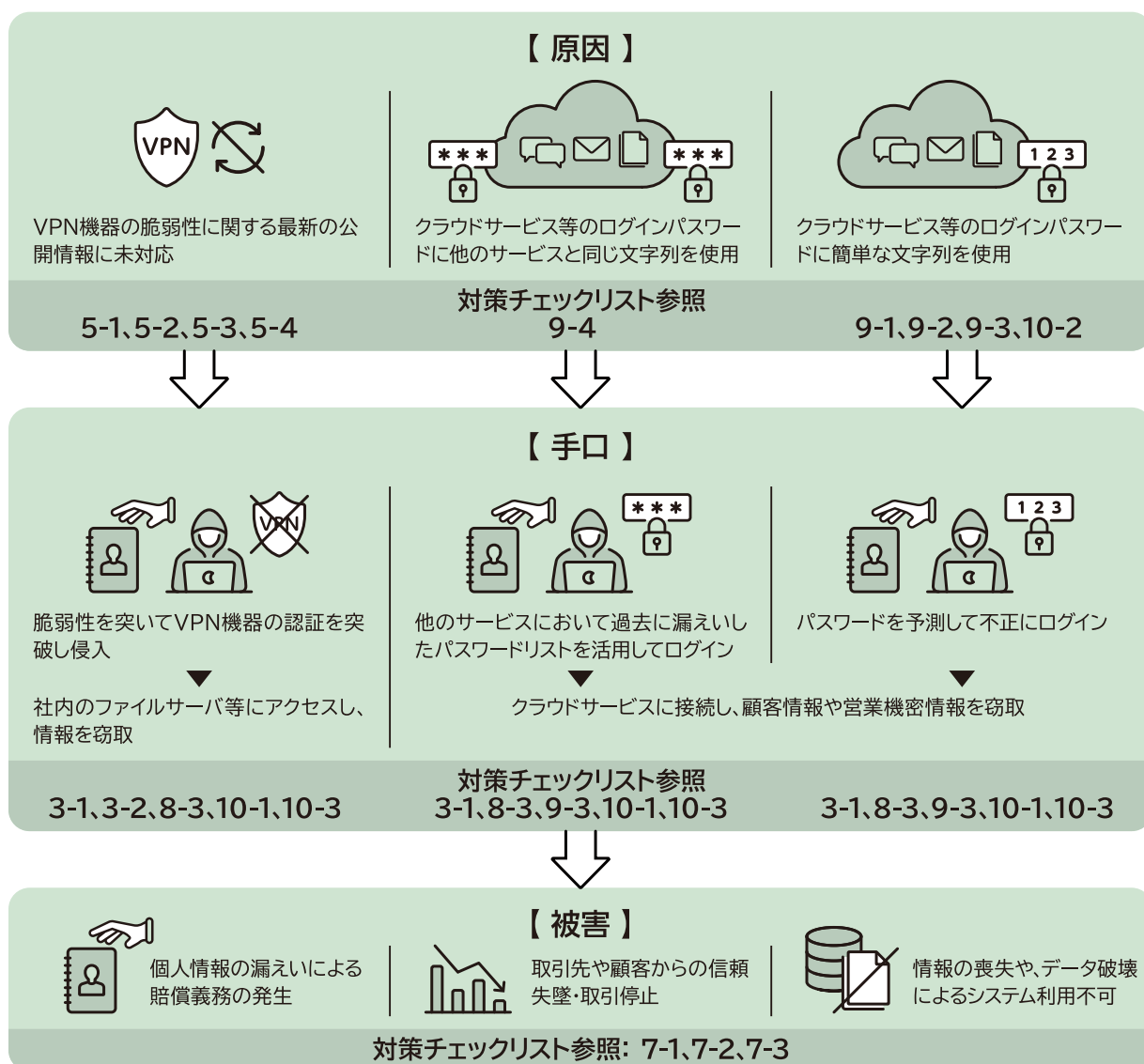




(2) 不正アクセス

「不正アクセス」とは、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、本人の許可を得ずに他人の ID 及びパスワードでログインし、利用者に提供されているサービスを受ける行為のことで、

不正アクセスを確認した場合は、「情報漏えい」の発生や、情報漏えいに伴う「賠償責任」の発生、データ破壊によるシステム利用の不可、さらには、取引先や顧客からの「信頼失墜」や「取引停止」につながる可能性があります。

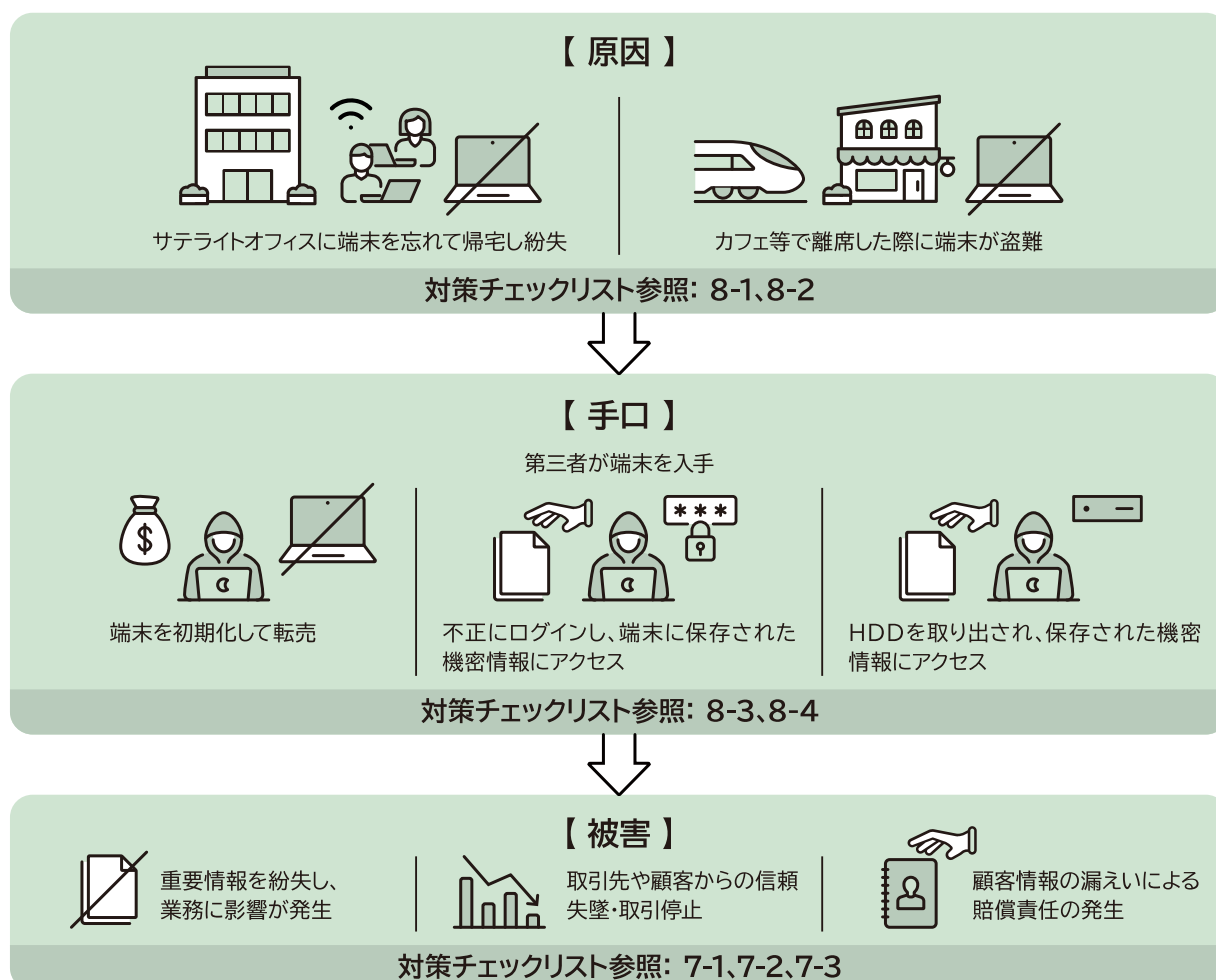




(3) 端末の紛失・盗難

「端末の紛失・盗難」とは、テレワーク端末を紛失したり、物理的に第三者に盗まれたりすることです。

紛失・盗難時には、「情報漏えい」の発生や、情報漏えいに伴う「賠償責任」の発生、さらには、取引先や顧客からの「信頼失墜」や「取引停止」につながる可能性があります。

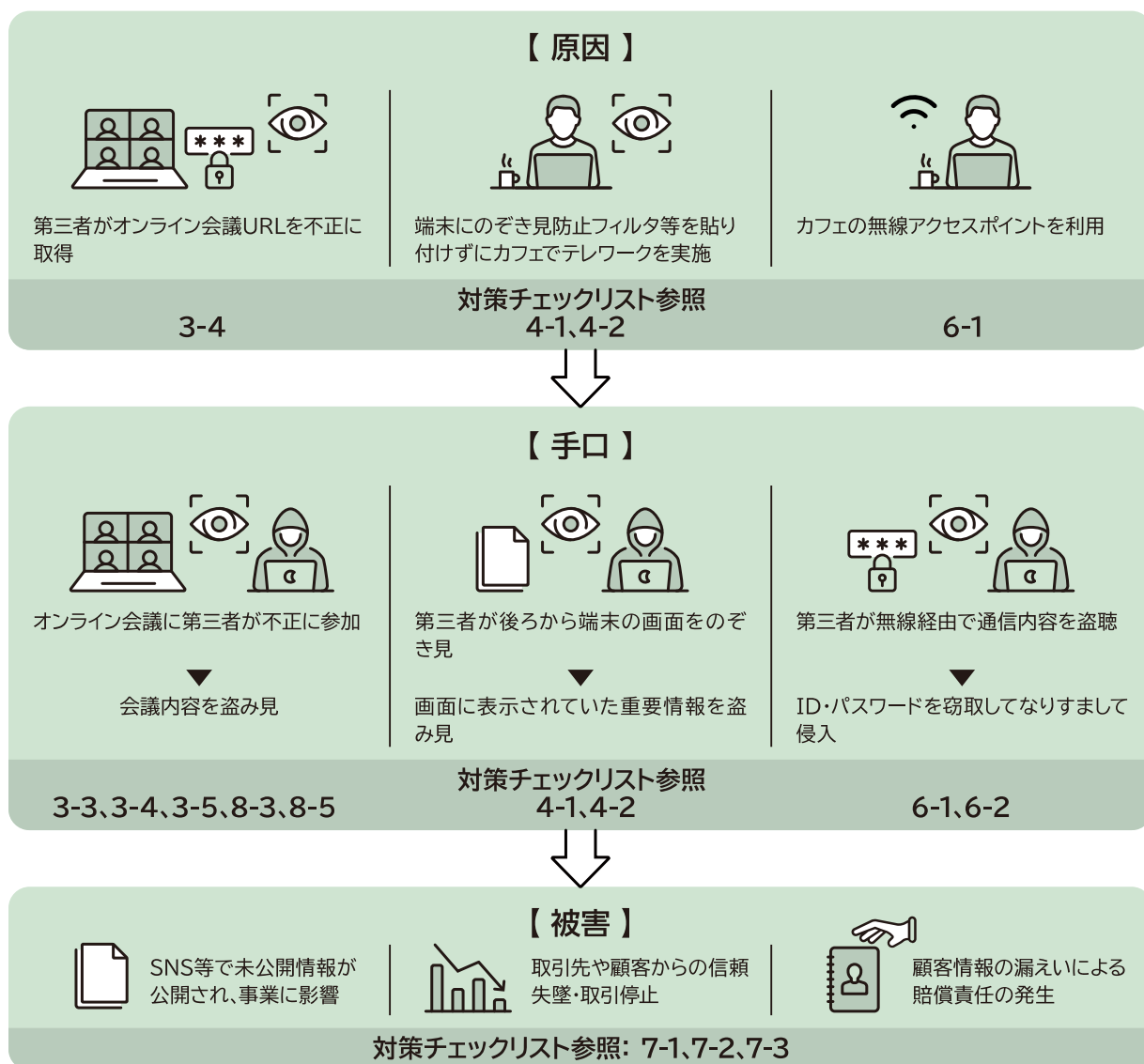




(4) 情報の盗聴

「情報の盗聴」とは、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たり、端末をのぞき見られたりすることです。

情報が盗聴された場合には、「情報漏えい」の発生や、情報漏えいに伴う「賠償責任」の発生、さらには、取引先や顧客からの「信頼失墜」や「取引停止」につながる可能性があります。



参考

2. テレワークに有効なセキュリティ対策

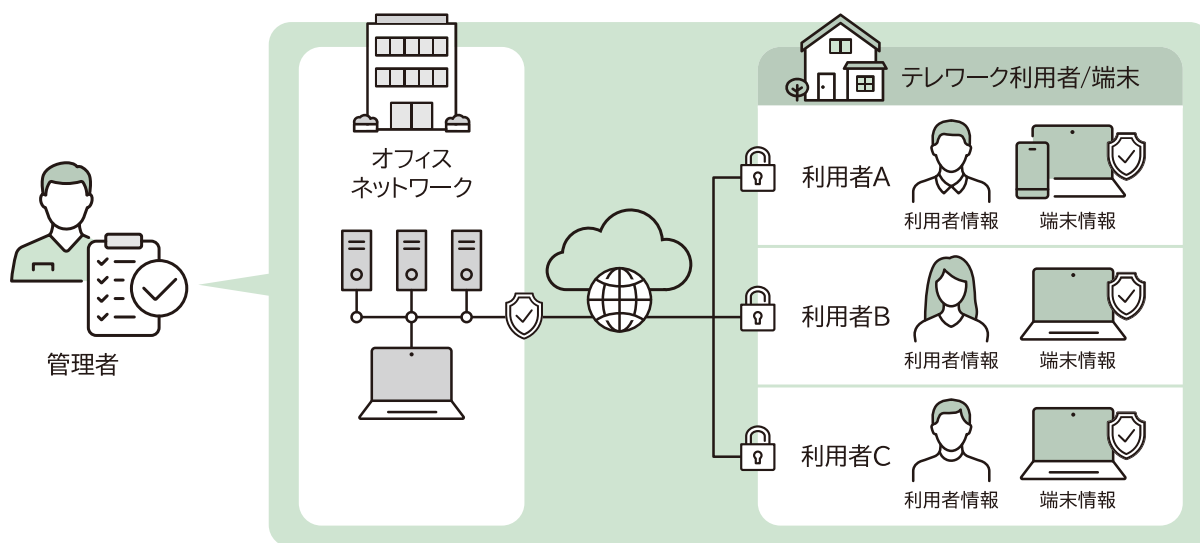
ここでは、テレワーク環境における脅威を回避するための効果的なセキュリティ対策について理解を深めるために、代表的なセキュリティ対策の概要と具体策、さらには対策を怠った場合の影響について解説しています。





「[第2部 1. テレワークセキュリティ 対策チェックリスト\(p.25~\)](#)」、「[第2部 3. セキュリティ対策一覧\(p.59~\)](#)」の各対策項目が、それぞれどのような脅威を回避するためのものなのかを知り、組織のテレワーク環境の実態に応じた適切な対策を講じるためにお役立てください。



(1) 資産・構成管理

テレワークで利用するハードウェアやソフトウェア等の把握や、その管理を行います。IT 資産そのものの管理が直接的な対策になるわけではなく、その他のさまざまなセキュリティ対策を実施する際の前提となる対策です。

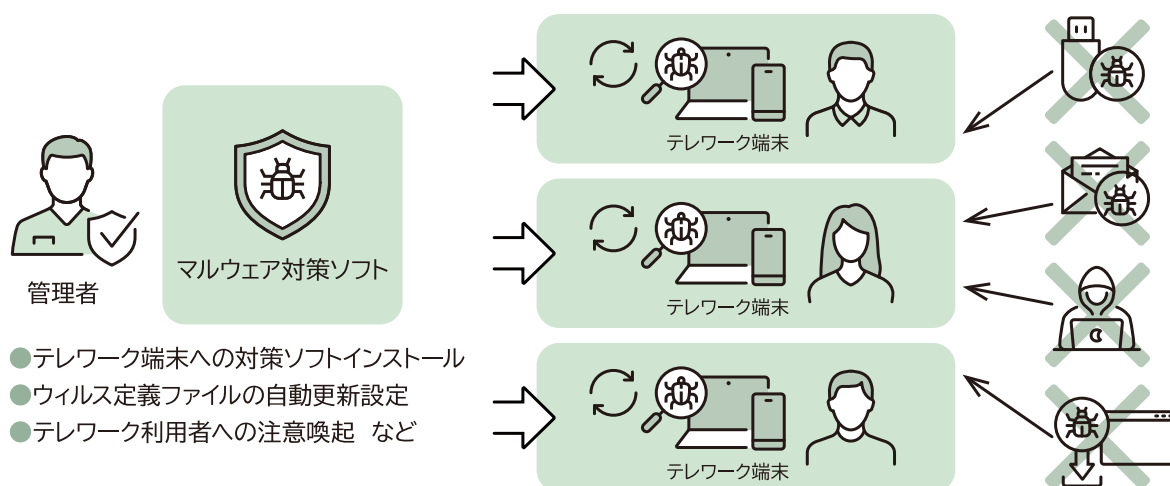






 対策	<p>対策1 セキュリティ対策一覧参照: 1-1 → p.59</p> <p>テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。</p>
 影響	<p>対策を怠った場合の影響</p> <p>セキュリティ対策を実施していない端末が存在し、マルウェア感染のリスクが高まるほか、端末の盗難や紛失時に被害状況を把握できない。</p>
 対策	<p>対策2 セキュリティ対策一覧参照: 1-2 → p.59</p> <p>テレワークで利用しているシステムや取り扱う重要情報を把握する。</p>
 影響	<p>対策を怠った場合の影響</p> <p>システムを適正な利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かどうか把握できない。</p>



(2) マルウェア対策

マルウェアの感染防止や検出、エンドポイントセキュリティに関する対策です。テレワークにおいてはインターネットを利用する機会が多く、特にインターネット経由の感染例が多いマルウェアの脅威に備える必要があります。



 対策	<h3>対策1</h3> <p>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を有効にする ^{※1}。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にするか、手動で更新するルールを作成する。</p>	<p>セキュリティ対策一覧参照: 2-1 → p.59</p>
 影響	<h3>対策を怠った場合の影響</h3> <p>ウイルス定義ファイルが最新でないために、テレワーク端末がマルウェアに感染するリスクが高まる。</p>	
 対策	<h3>対策2</h3> <p>不審なメールを開封し、メールに記載されている URL をクリックしたり、添付ファイルを開いたりしないよう周知する。</p>	<p>セキュリティ対策一覧参照: 2-2 → p.60</p>
 影響	<h3>対策を怠った場合の影響</h3> <p>悪意あるサイトに誘導され、マルウェアに感染したり、重要情報にアクセスするための認証情報等が窃取されたりするリスクが高まる。</p>	

※1 Windows 製品に標準搭載されたウイルス対策ソフト(Windows Defender)を利用する場合、公式アプリケーションストアを利用する等の安全な方法でインストールしたアプリのみを利用している場合は、ウイルス対策ソフトのインストール作業は不要。また、iOS 製品においてはウイルス対策ソフトのインストールは不要。



対策

対策 3

セキュリティ対策一覧参照: 2-3 → [p.60](#)

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おく。



影響

対策を怠った場合の影響

悪意あるサイトに誘導され、マルウェアに感染したり、重要情報にアクセスするための認証情報等が窃取されたりするリスクが高まる。



対策

対策 4

セキュリティ対策一覧参照: 2-4 → [p.60](#)

スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は、公式アプリケーションストアを利用するよう周知する。



影響

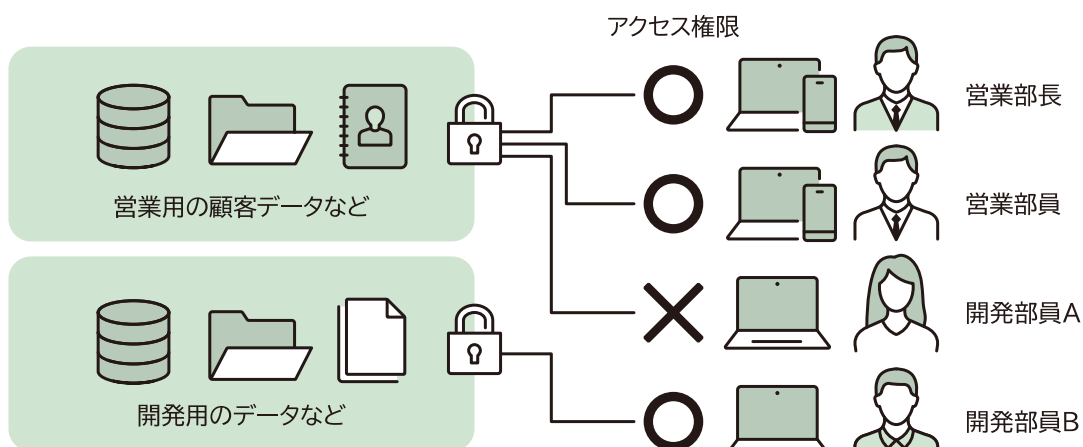
対策を怠った場合の影響





安全性が確認できない方法でインストールすると、正規のアプリケーションを模したマルウェアに感染するリスクが高まる。



(3) アクセス制御・認可

データやサービスへのアクセスを、必要最小限かつ正当な権限を有する者のみに制限することに関する対策です。制限をかいこぐって不審なアクセスが発生していないか、オフィスネットワークとインターネットとの間の通信を監視することで、セキュリティインシデントの早期発見につなげることができます。



 対策	<p>対策1 セキュリティ対策一覧参照: 3-1 → p.60</p> <p>許可された人のみが重要情報を利用できるよう、システムによるアクセス制御やファイアールに対するパスワード設定等を行う。</p>
 影響	<p>対策を怠った場合の影響</p> <p>本来アクセス権限が必要で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ことで、重要情報が流出するリスクが高まる。</p>
 対策	<p>対策2 セキュリティ対策一覧参照: 3-2 → p.60</p> <p>インターネット経由で社内システムにアクセスがあった際には、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不要なIPアドレスからの通信を遮断する。</p>
 影響	<p>対策を怠った場合の影響</p> <p>脆弱性を突いた攻撃やアカウントのなりすまし等の悪意のある攻撃により不正アクセスされるリスクが高まる。</p>



対策

対策 3

セキュリティ対策一覧参照: 3-3 → p.60

オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。



影響

対策を怠った場合の影響

不適切な利用者が不正に参加していることに気づかず、情報漏えいのリスクが高まる。



対策

対策 4

セキュリティ対策一覧参照: 3-4 → p.60

オンライン会議に参加するための[パスワード](#)の設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。



影響

対策を怠った場合の影響

不適切な利用者が不正に参加し、情報漏えいにつながるリスクが高まる。



対策

対策 5

セキュリティ対策一覧参照: 3-5 → p.61

オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。



影響

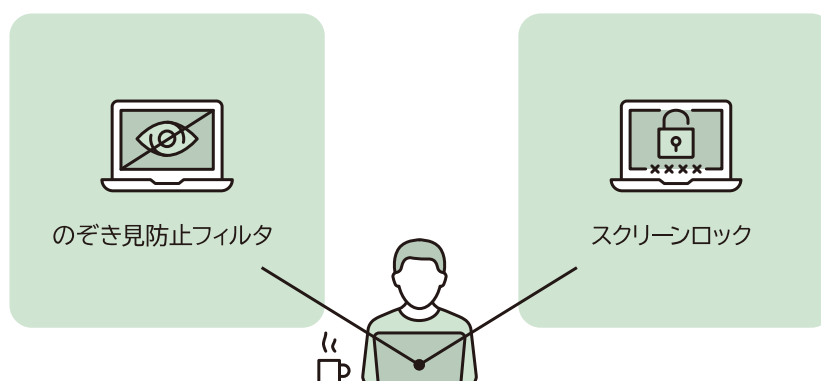
対策を怠った場合の影響





不適切な利用者が不正に参加していることに気づかず、情報漏えいのリスクが高まる。



(4) 物理セキュリティ

テレワーク環境は、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することが比較的容易な環境にあります。そうした懸念を払しょくするための対策です。

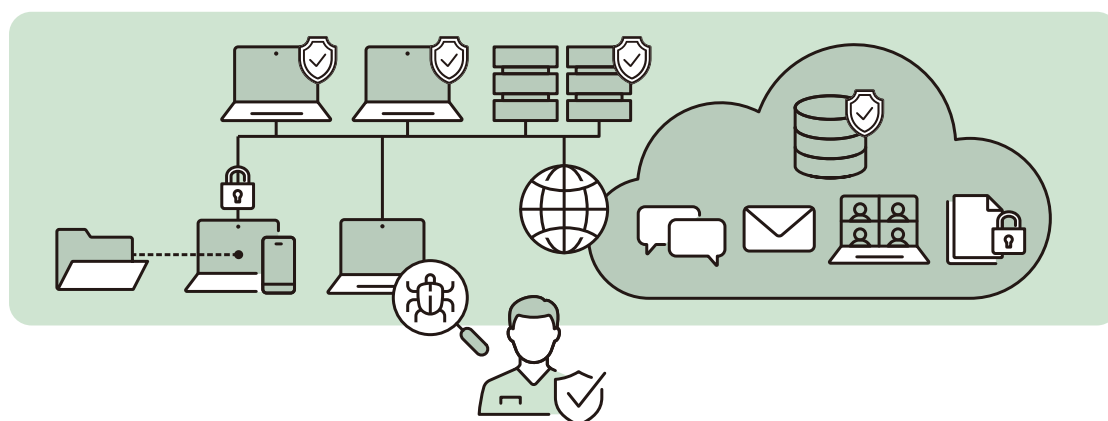






 対策	対策1 セキュリティ対策一覧参照: 4-1 → p.61 テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。
 影響	対策を怠った場合の影響 テレワーク端末越しの情報漏えいや不正利用のリスクが高まる。
 対策	対策2 セキュリティ対策一覧参照: 4-2 → p.61 テレワーク端末から離れる際には、スクリーンロックをかけるよう周知する。
 影響	対策を怠った場合の影響 テレワーク端末越しの情報漏えいや不正利用のリスクが高まる。



(5) 脆弱性管理

テレワーク環境で利用しているハードウェアやソフトウェアに潜む脆弱性を管理します。脆弱性を放置していると、外部からの攻撃が成功する可能性が高まります。このような事態を防ぐためにも、脆弱性管理の実施が必要です。



 対策	<p>対策1 セキュリティ対策一覧参照: 5-1 → p.61</p> <p>テレワーク端末にはメーカーサポートが終了した OS やアプリケーションを利用しないよう周知する。</p>
 影響	<p>対策を怠った場合の影響</p> <p>セキュリティアップデートが行えないため、製品の脆弱性を突いた攻撃により不正アクセス等のリスクが高まる。</p>
 対策	<p>対策2 セキュリティ対策一覧参照: 5-2 → p.61</p> <p>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するよう周知する。</p>
 影響	<p>対策を怠った場合の影響</p> <p>製品の脆弱性を突いた攻撃により不正アクセス等のリスクが高まる。</p>



対策

対策 3

セキュリティ対策一覧参照: 5-3 → p.61

テレワークで利用するネットワーク機器には、メーカーサポートが終了した製品を利用せず、最新の[ファームウェア](#)を適用するよう周知する。



影響

対策を怠った場合の影響

ファームウェアの脆弱性を突いた攻撃により不正アクセス等のリスクが高まる。



対策

対策 4

セキュリティ対策一覧参照: 5-4 → p.61

テレワーク端末から社内にリモートアクセスするための [VPN](#) 機器等には、メーカーサポートが終了した製品を利用せず、最新の[セキュリティアップデート](#)を適用する。



影響

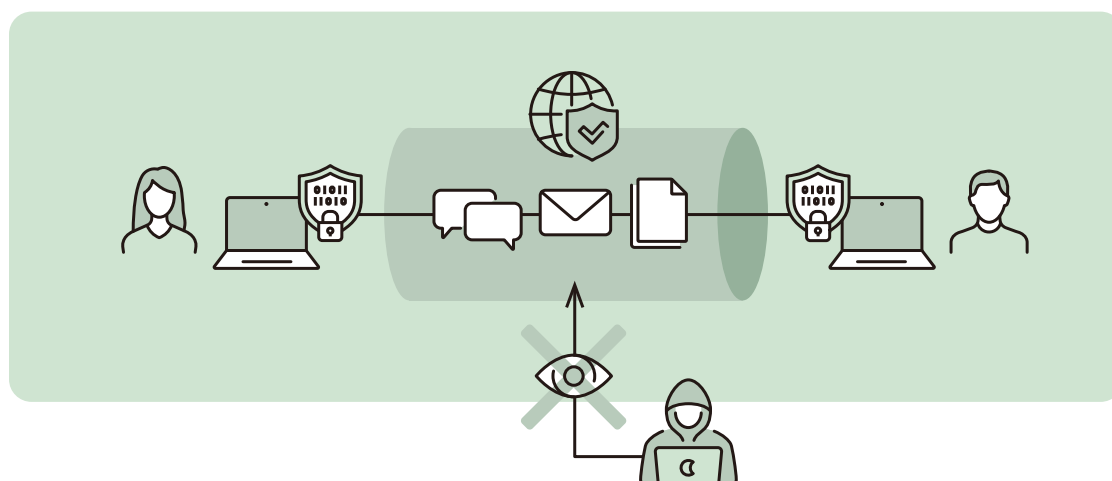
対策を怠った場合の影響





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口となるため、ファームウェアの脆弱性を突いた攻撃により不正アクセス等のリスクが高まる。



(6) 通信暗号化

通信中におけるデータの機密性や可用性の確保に関する対策です。インターネット経由でデータの送受信をする場合、通信経路上に第三者が介在し、情報をのぞき見されるおそれもあります。そのため、通信経路を暗号化して、データを保護することが必要です。

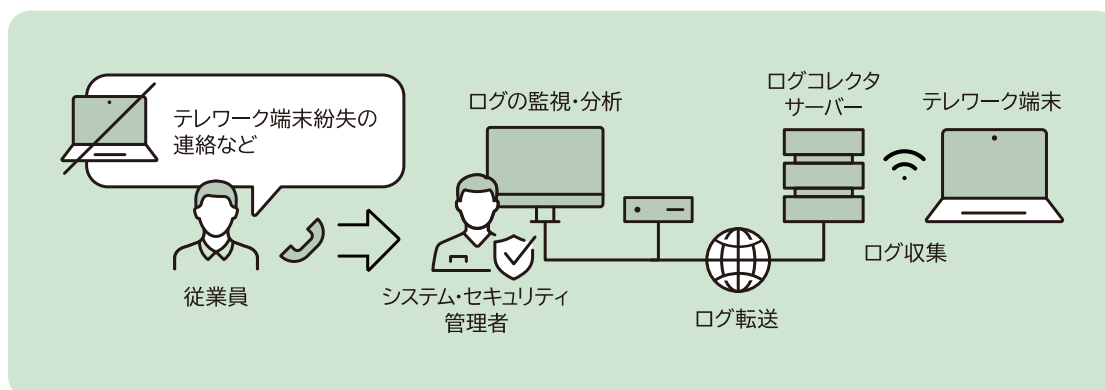






 対策	対策1	セキュリティ対策一覧参照: 6-1 → p.61
 影響	対策を怠った場合の影響 通信内容を盗み見られ、情報漏えいのリスクが高まる。	
 対策	対策2	セキュリティ対策一覧参照: 6-2 → p.61
 影響	対策を怠った場合の影響 通信内容を盗み見られ、情報漏えいのリスクが高まる。	



(7) インシデント対応・ログ管理

セキュリティインシデントへの迅速な対応と、ログの取得や調査に関する対策です。万一の際に迅速かつ確かな意思決定を行うためには、平時のうちに対応計画を整備しておくことが重要です。



 対策	対策1	セキュリティ対策一覧参照: 7-1 → p.62
 影響	対策を怠った場合の影響 セキュリティインシデントが発生した事実の把握や被害拡大の早期防止ができず、被害が拡大するリスクが高まる。	
 対策	対策2	セキュリティ対策一覧参照: 7-2 → p.62
 影響	対策を怠った場合の影響 セキュリティインシデントの原因調査において、原因や被害状況の特定、絞り込みの難易度が高まる。結果として適切な対応が遅れ、被害が拡大するリスクが高まる。	



対策

対策 3

セキュリティ対策一覧参照: 7-3 → p.62

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](#)を収集する。



影響

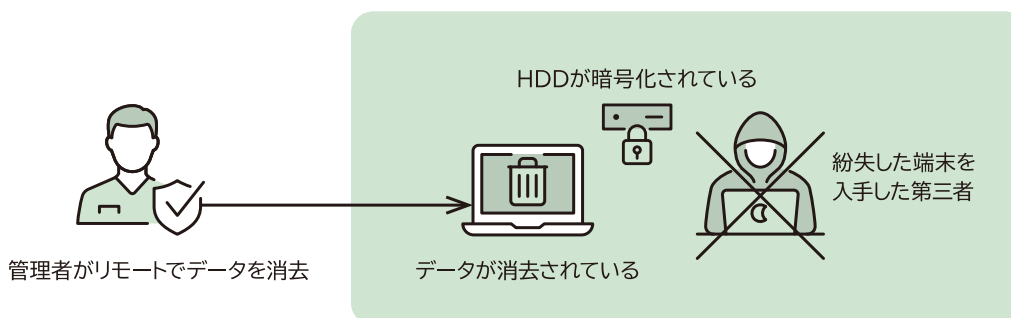
対策を怠った場合の影響





セキュリティインシデントの原因調査において、原因や被害状況の特定、絞り込みの難易度が高まる。結果として適切な対応が遅れ、被害が拡大するリスクが高まる。



(8) データ保護

保護すべきデータの特定や保存されているデータの機密性・可用性の確保に関する対策です。テレワーク環境においては情報資産をオフィスから持ち出す必要があることから、持ち出された情報がテレワーク端末の紛失や盗難により外部に漏えいするリスクが高まるため、重要情報を適切に保護する仕組みが必要です。



 対策	<p>対策1 セキュリティ対策一覧参照: 8-1 → p.62</p> <p>スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。</p>
 影響	<p>対策を怠った場合の影響</p> <p>紛失時の早期発見が困難となり、端末を取得した悪意のある第三者が不正にアクセスし、情報漏えいにつながるリスクが高まる。</p>
 対策	<p>対策2 セキュリティ対策一覧参照: 8-2 → p.62</p> <p>テレワーク端末の紛失時に備えて MDM 等を導入し、リモートからのデータ消去、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する。</p>
 影響	<p>対策を怠った場合の影響</p> <p>端末を取得した悪意のある第三者が不正にアクセスし、情報漏えいにつながるリスクが高まる。</p>



対策

対策 3

セキュリティ対策一覧参照: 8-3 → p.62

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、端末に内蔵されたハードディスクやフラッシュメモリ等の記録媒体の暗号化を実施する^{※2}。ただし、端末に会社のデータを保管しない場合を除く。



影響

対策を怠った場合の影響

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できるため、保存している情報の漏えいリスクが高まる。



対策

対策 4

セキュリティ対策一覧参照: 8-4 → p.63

テレワーク端末には原則として重要情報を保管しないよう周知する。万一その必要性が生じた場合^{※3}には、パスワードの設定やファイルの暗号化を実施し、一時的な保管のみを許可する。ただし、端末に会社のデータを保管しない場合を除く。



影響

対策を怠った場合の影響

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、情報漏えいのリスクが高まる。



対策

対策 5

セキュリティ対策一覧参照: 8-5 → p.63

オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対してはパスワードの設定や期間指定の自動削除等を実施するよう周知する。また、上記ルールは可能な限り設定を強制する。



影響

対策を怠った場合の影響

共有する予定ではない画面情報を誤操作で共有してしまったり、会議の録画ファイルが不適切な第三者に参照されたりして、情報漏えいのリスクが高まる。

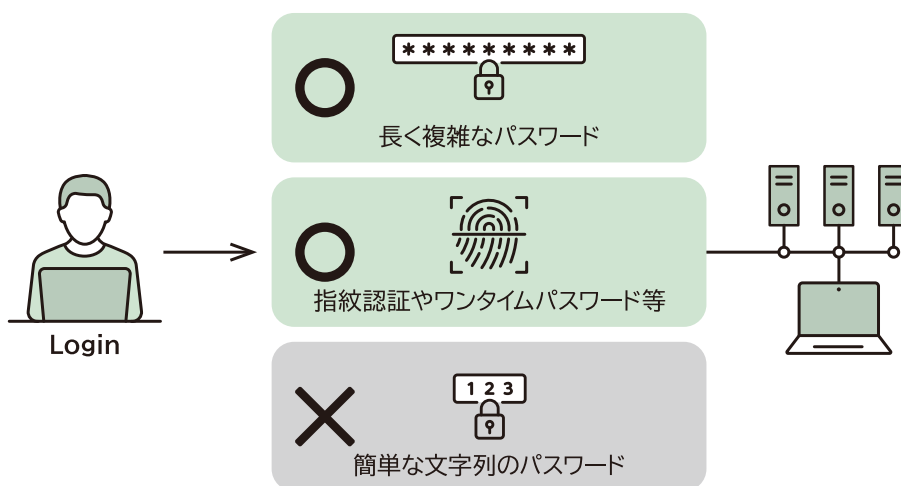
※2 iOS 製品については初期状態で暗号化されているため対応不要。





※3 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。



(9) アカウント・認証管理

情報システムにアクセスするためのアカウント管理や認証手法に関する対策です。利用者を識別するために ID やパスワードを適切に管理するとともに、アクセス権限に応じた適切なアカウントを付与します。パスワードの設定では、複数のサービス間で同じパスワードを使いまわさないことも重要です。



 対策	対策1	セキュリティ対策一覧参照: 9-1 → p.63
 影響	対策を怠った場合の影響 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のリスクが高まる。	
 対策	対策2	セキュリティ対策一覧参照: 9-2 → p.63
 影響	対策を怠った場合の影響 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のリスクが高まる。	



対策

対策 3

セキュリティ対策一覧参照: 9-3 → p.63

テレワーク端末やテレワークで利用する各システムに対して一定回数以上パスワードを誤入力した場合、それ以上のパスワード入力を受け付け不要設定する。



影響

対策を怠った場合の影響

悪意のある第三者がパスワードを容易に試行できるため、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のリスクが高まる。



対策

対策 4

セキュリティ対策一覧参照: 9-4 → p.63

テレワークで利用する各システムへのアクセスには、多要素認証を求めるよう設定する。



影響

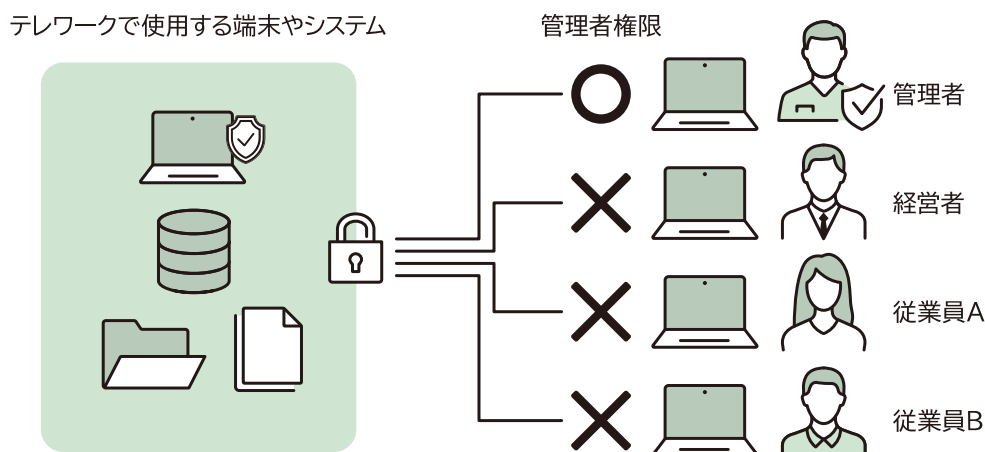
対策を怠った場合の影響

悪意のある第三者にパスワードが流出しやすくなるだけでなく、なりすましによる不正アクセスのリスクが高まる。



(10) 特権管理

不正アクセス等に備えたシステム管理者権限の保護に関する対策です。管理者権限が不適切に使用されると、より大きな被害につながります。特権を有するアカウントを適切に管理することは、悪意のある第三者による攻撃はもちろん、内部による不正を防ぐためにも重要です。



対策

対策1

セキュリティ対策一覧参照: 10-1 → p.64

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、業務上必要な最小限の人に付与する。



影響

対策を怠った場合の影響

悪意のある第三者が不正に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や、誤操作による情報漏えいのリスクが高まる。



対策

対策2

セキュリティ対策一覧参照: 10-2 → p.64

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する。



影響

対策を怠った場合の影響

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のリスクが高まる。



対策

対策 3

セキュリティ対策一覧参照: 10-3 → [p.64](#)

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する。



影響

対策を怠った場合の影響

管理者権限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高まるだけでなく、管理者権限の利用情報等から不正アクセスの懸念を発見することが困難になる。

3. 知っておきたいキーワード集

MDM

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です。

MDMを導入する必要性

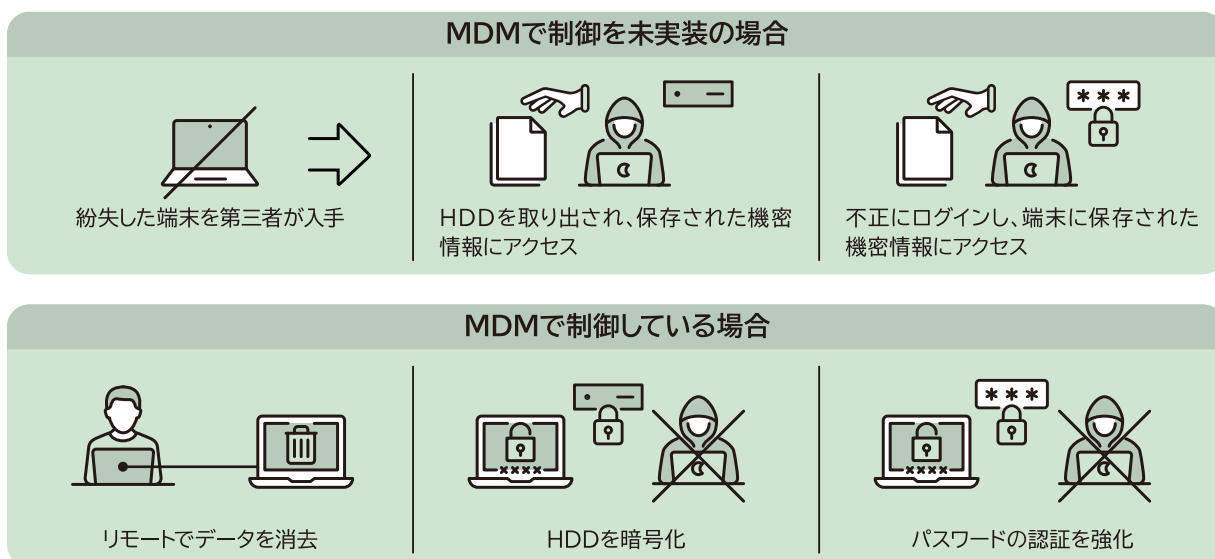
MDMを導入することで、テレワーク端末に対してセキュリティ設定等を強制できるため、テレワーク環境におけるセキュリティ統制の強化に役立ちます。また、テレワーク端末の紛失・盗難時には、端末内に保存されているデータの保護等を通じて、情報漏えいを防止できます。

なお、製品によって、セキュリティ設定等の強制範囲が異なるため、製品選定の際には求めている機能が利用可能かどうかを確認する必要があります。

MDMの機能例

MDMの機能としては次のようなものがあります。

- 内蔵記録装置(HDD等)の暗号化: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に、データを暗号化して漏えいを防ぎます。
- 遠隔操作によるデータ消去:テレワーク端末の紛失・盗難時に、遠隔操作で端末のデータを消去して漏えいを防ぎます。
- 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、パスワードの設定方法等のルールを定めて適用(強制)します。



各種連絡体制(インシデント発生時)

インシデント発生時にしかる場所に連絡をすべき理由と、連絡先および連絡内容は、次のとおりです。

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かないと、緊急時に適切な報告、連絡、相談等ができなくなり、被害が拡大す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。

- 連絡すべき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

システム・セキュリティ管理者は、従業員に対して、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)を事前に周知しておく必要があります。



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。

- 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
- 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
- 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

管理者権限とは、システムの設定やプログラムの実行・インストール等、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を実行できるため、攻撃者の標的になりやすいとされています。

そのため、管理者権限の付与は業務上必要な担当者に限定するとともに、必要なときだけ利用させることや、強力なパスワード設定等により保護することが重要です。

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 Linux の root	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
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

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です。

時刻同期の必要性

サーバやネットワーク機器等のように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きます。

時刻同期をしていない場合、ログを取得した時刻が正確でない可能性があり、実際に行われた操作との因果関係がわからず、調査が行えないこともあります。

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のが一般的です。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サーバとして指定している場合はあえて変更する必要はありません。ただし、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るため、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、あえて設定変更の必要がないこともあります。

システムによるアクセス制御

「システムによるアクセス制御」とは、利用者によるシステムやデータ等への接続や、接続先での閲覧・作成・実行等に制限をかけることです。

その実施方法のパターンと各方法で実現できることは、次のとおりです。

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は、守るべき情報について、業務上必要のない者が閲覧、改ざん、持出し等を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、本来必要のない人がアクセス可能な状態となっている場合は、不正アクセスやマルウェア感染等が発生した際の影響や被害の拡大につながります。したがって、適切なアクセス制御を実施する必要があります。

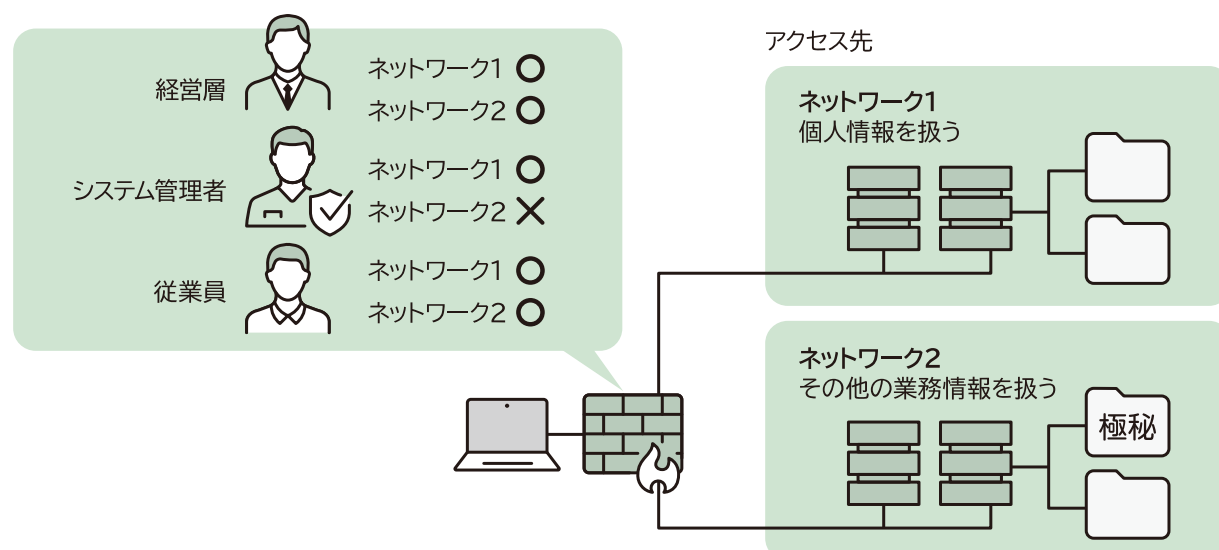
アクセス制御の方法として3つの例を示します。自組織に適用できる場合は参考にしてください。

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たアクセス制御を実施できます。

例えば、社内に「個人情報扱うネットワーク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により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。



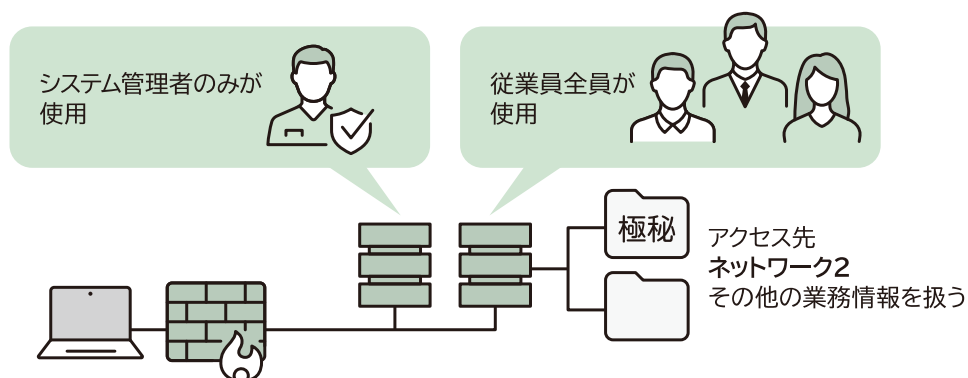
例2 サーバのファイアウォール機能によって制御する場合

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といったように、アクセス制御レベルの異な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。

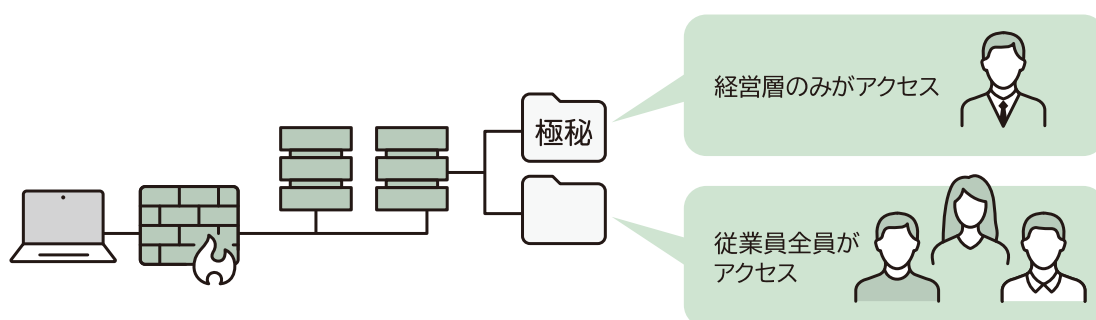
例えば、下図のネットワーク②において、管理者のみが使用するサーバと、全従業員が使用するファイルサーバがあるとします。この場合、端末からのアクセス制御は、ファイアウォールだけでは十分に行うことができません。そのため、管理者のみが使用するサーバに対して、例えば管理者用端末に割り振られたIPアドレスからの通信のみ許可するといったアクセス制御を実施する必要があります。

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

1台のファイルサーバの中で、例えば「経営層のみがアクセスできるフォルダ」と「全従業員がアクセスできるフォルダ」といったように、役職や関係者ごとにアクセス制御レベルを分けたい場合は、フォルダ単位でアクセス制御を実施できます。



重要情報

本書における「重要情報」とは、営業秘密のように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のように管理責任を伴う情報のことです。

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、情報漏えいの発生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の影響や被害の程度を想定した上で、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必要があります。

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、取引先の関連企業等、間接的な接点を持つセキュリティ対策の弱い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る新規事業を停止、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)	社内システムへの不正アクセスによるシステム停止、機会損失
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ることによる情報漏えい 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)

本書における「対応手順」とは、インシデントが発生した際に、どのような順でどのようなことを実施すべきかを示したものです。

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、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、オフィスでの業務とテレワークでの業務におけるシステム環境は異なることがあります。したがって、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しておくことが重要です。

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ないように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、該当のユーザがアクセスしたかどうかを確認します。また、情報漏えいの可能性の有無を確認します。
ウイルス対策ソフトによるスキャン	ウイルス対策ソフトによるスキャンを実施し、マルウェア感染の検知・駆除の可能性を確認します。
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	他の従業員を同様の被害から守るため、同一の操作を行わないように注意喚起を行います。また、既に行ってしまった場合を想定して対応策も案内します。

パスワード強度

「パスワード強度」とは、パスワードの安全性が高いかどうかを図る尺度のことです。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^{※1}や辞書攻撃^{※2}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、適切なパスワードを設定することが重要です。

また、パスワードを複数のサービスで使い回していると、ある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ことになりかねないため、様々なサービスで同一のパスワードを使用しないようにします。

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:tHkh84Lp9Ck4O
サービスCのパスワード:tHkh84Lp9C2R3

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。

※1 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。

※2 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。

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。

参考

4. 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。代表的なものに、Windows、iOS、Android 等がある。
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、自宅や外出先などから安全にオフィスネットワークに接続できる技術。
アクセスログ	アクセス元及びアクセス先の情報等、サーバやネットワーク機器の動作を記録したもの。実施された操作の分析や事故発生時の原因特定等に用いられる。
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ないが、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で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する。
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る。ここには、プロバイダーが提供するメールサービスの利用も含む。
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。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む。
セキュアブラウザ	端末側にデータを残さずに利用できる特殊Webブラウザ。閲覧した情報を端末に保存できないようにする機能のほか、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る。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る。
セキュリティアップデート	ソフトウェアの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のこと。

用語	解説
定義ファイル	ウイルスの特徴を収録したファイル。「シグニチャ」「パターンファイル」等とも呼ばれ、ウイルスの検出時に使用される。
ファイアウォール	ネットワーク上の通信を遮断する機能。サーバ上のソフトウェアにファイアウォール機能が実装されている場合と、専用のハードウェアに機能が実装されている場合の両方がある。
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。
フラッシュメモリ	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」のこと。電源を落としてもデータを保持することが可能な記録媒体。
マルウェア	ウイルス、ワーム、トロイの木馬等の悪意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、それらの所有者が気付かないうちに感染させ、機器本来の動作の妨害やデータの破壊、データの窃盗等、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上にある 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、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。

参考

5. リンク集

本書に関連して参考となる文献やWebサイト等をご紹介します。情報収集および理解の促進にお役立てください。

- **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、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。

- **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。

- **サイバーセキュリティお助け隊サービス【(独)情報処理推進機構】**

<https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html>

中小企業向けのセキュリティサービスが満たすべき基準「サイバーセキュリティお助け隊サービス基準」(「サービス基準」)を示し、サービスを登録・公表する制度です。

(ユーザ向けウェブサイト) <https://www.ipa.go.jp/security/otasuketai-pr/>

- **テレワーク関連ツール一覧【日本テレワーク協会】**

<https://japan-telework.or.jp/wordpress/wp-content/uploads/2021/05/Tools-V6.0s-20210531.pdf>

テレワーク導入時に検討すべきネットワーク及び各種ツール(ソフトウェア・サービス等)を概算費用と合わせて、テレワーク推進担当者向けに示したものです。

- **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、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。

- 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/index.html>
インターネットを利用する際の一般的な留意点をまとめたものです。
- みんなで使おう サイバーセキュリティ・ポータルサイト【内閣サイバーセキュリティセンター】
<https://security-portal.nisc.go.jp/>
サイバーセキュリティの普及啓発や人材育成に関する公的機関などの様々な施策や取り組みを集約して紹介したポータルサイトです。
- 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
企業の経営者が、サイバーセキュリティ対策を推進していく上で重要な項目をまとめたものです。
- 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>
テレワークの導入に当たり、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。

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/