テレワークセキュリティガイドライン

第５版

（令和３年５月）

総務省

本ガイドラインの構成

本ガイドラインは次のとおり構成されています。最初から順に読むことを期待していますが、自組織にとって特に必要な章を確認する際の参考にしてください。

第１章　はじめに（p.5～）

本ガイドラインの背景や目的、テレワークの形態、想定読者等を示しています。

第２章　テレワークにおいて検討すべきこと（p.10～）

テレワークにおけるセキュリティ対策を進めるに当たり、「ルール」・「人」・「技術」のバランスのとれた対策を行う必要性や、「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」の適切な役割分担の重要性と、各立場の役割を具体的に示しています。

また、近年のテレワークを取り巻く環境やセキュリティ動向の変化を踏まえ、クラウドサービスの活用やゼロトラストセキュリティに関する考え方も示しています。

第３章　テレワーク方式の解説（p.24～）

テレワーク方式を７種類に整理した上で、各方式について、基本的構成に加えて派生的な構成を示しているほか、各方式特有のセキュリティ上の留意点等について示しています（各方式共通のセキュリティ対策は第４章・第５章）。

また、テレワークによって実現しようとする業務の内容やセキュリティ統制の容易性等を踏まえ、適した方式を選定する際の参考となるよう、フローチャートや、各方式の特性比較表を示しています。

第４章　テレワークセキュリティ対策一覧（p.55～）

「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」の立場ごとに、テレワークにおけるセキュリティ対策として一般的に普及しており、基本的に取り組むことが求められる「基本対策」と、一定の予算や組織体制が整備されていないと実施が困難なセキュリティ対策であるものの、実施により更なるセキュリティの向上が見込める「発展対策」をそれぞれ掲載しています。

また、各セキュリティ対策は、13個の対策分類に分け整理しています。

第５章　テレワークセキュリティ対策の解説（p.66～）

第４章に記載の各セキュリティ対策について、詳細解説を示しています。

第６章　テレワークにおけるトラブル事例と対策（p.91～）

テレワークセキュリティに関するトラブル事例を具体的に紹介した上で、セキュリティ上の留意点や、本ガイドライン内のどのセキュリティ対策が有効であるかを示しています。

※本ガイドラインを周知する場合は、次のURLを周知願います。
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

※本ガイドライン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

第１章　はじめに

１．本ガイドラインの背景

テレワークは、場所や時間を有効に活用できる柔軟な働き方です。近年の情報通信技術（ICT：Information and Communication Technology）の進歩により、テレワークによってオフィス[1]環境と同等程度の業務を実施することも可能となってきていることから、企業等における導入・活用が進んでいます。

テレワークのメリット[2]として、移動時間等を有効に活用できるという業務の効率化があるほか、働き方改革に寄与する手段としても注目を集めています。テレワークを積極的に活用することにより、育児・介護と仕事を両立するというような多様で柔軟な働き方を後押しするとともに、通勤時間の節約や通勤ストレスからの解放といった従業員のワーク・ライフ・バランスの向上にも貢献することができます。

また、テレワークは、災害発生やパンデミックといった緊急事態発生時における企業等の事業継続性の確保に貢献する手段としても活用が期待されます。実際に令和２(2020)年に流行した感染症に対応するため、多くの企業等において急速にテレワークの導入や活用が進みました。

従来のテレワークの導入・活用は、業務の効率化や働き方改革等を目的として、企業等の「一部」の従業員が利用する、業務・勤務形態の例外的な選択肢の一つに留まっている状況でした。しかしながら、感染症対応を契機として、企業等の従業員が一斉かつ長期にわたってテレワークを利用している状況も多く見受けられるようになり、テレワークはもはや企業等における標準的・一般的な業務・勤務形態の一つになりつつあります。

このように急速に普及したテレワークですが、この実現を後押しした背景として、テレワークを実現するための多様な製品やサービスが充実してきたことも挙げられます。このような新たな製品やサービスを活用し、テレワークを推進していく姿勢は重要ですが、結果としてシステム構成や利用形態が多様化し、従来から整備してきた情報システムのセキュリティ対策や情報セキュリティ関連規程が十分に対応できていない状況も想定されます。

例えば、インターネットとオフィスネットワークの境界部分では厳重なセキュリティ対策が実施されることが一般的ですが、テレワークにクラウドサービスを活用し、オフィスネットワークを経由することなくインターネットに直接アクセスする場合には、そ

[1] 本ガイドラインにおいて「オフィス」は、企業等の物理的な所在地である場所、いわゆる職場を指します。

[2] 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、そのために必要となるテレワーク方式やセキュリティ対策を検討した上で、テレワークを導入するようにしましょう。

のようなセキュリティ対策は機能しません。また、企業等が管理するPCは、セキュリティ対策ソフトを通常は導入し管理していますが、テレワークで自宅のPCや自身のスマートフォン等を利用する場合には、そのようなセキュリティ対策もそのままでは機能しません。

テレワーク環境を含む情報システムに対するサイバー攻撃についても、正規のメールと容易に区別がつかないような不審メールによるマルウェア感染（例：Emotet）の広まりや、特定の企業等を徹底的に狙った標的型攻撃の発生など、高度化・複雑化し続けています。

既知の攻撃手法への防御を念頭に構成されたセキュリティ対策だけでは十分な防御が難しくなってきており、オフィスネットワーク内に攻撃者が侵入することを前提にセキュリティ対策の在り方を再検証するゼロトラストという考え方に注目が集まっています。この考え方は、前述したような多様化するシステム構成や利用形態に対するセキュリティの向上という観点からも注目されています。

このように、テレワークを取り巻く環境やセキュリティ動向が変化してきていることから、これに対応するため、平成30(2018)年４月[3]に公表した本ガイドライン（第４版）について全面的な改定を行い、第５版として策定するものです。

[3] 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

2．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、本ガイドラインではいずれの形態も対象としています。それぞれの概要及び特徴は次のとおりです。

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。

このほか、テレワーク等を活用し、リゾート地や温泉地、国立公園等、普段のオフィスとは異なる場所で余暇を楽しみつつ仕事を行う、いわゆる「ワーケーション」についても、情報通信技術を利用して仕事を行う場合には、サテライトオフィス勤務又はモバイル勤務の一形態として分類することができます。

3．本ガイドラインの目的

本ガイドラインは、前述したテレワークを取り巻く環境やセキュリティ動向の変化を踏まえた上で、テレワークの導入を検討しようとしている企業等のみならず、既にテレワークを導入している企業等においても、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なるよう策定しています。

テレワークで業務を実施するに当たっては、テレワーク特有のセキュリティ上のリスクがあります。こうしたリスクは、特定の担当者や特定の対策を実施するだけで対応できるものではなく、企業等の組織全体で適切な役割分担を行いながら、複数の対策を重層的に採ることが必要となります。

本ガイドラインを通じて、そのような役割や対策を把握した上で、これからテレワークを導入しようとしている企業等にあっては、導入に当たってガイドラインに沿ったテレワーク環境が構築されるようにし、既にテレワークを導入している企業等にあっては、自らのテレワーク環境がガイドラインに沿ったものであるか検証を行い、必要に応じて、ガイドラインに沿ったものとなるよう対応を行っていくことを期待しています。

なお、本ガイドラインは、テレワークを導入・活用するために必要となるセキュリティ対策等について示しています。しかしながら、企業等の業務はテレワークだけに限らないことから、企業等が実施すべきセキュリティ対策の全てを本ガイドラインで網羅的に示しているわけではないことに留意してください。

また、本ガイドラインで示したセキュリティ対策については、一般的なテレワーク環境を想定したものです。実際のテレワークは様々な形で実施されていることから、環境によっては対策が不要となる場合も、追加的な対策が必要となる場合[4]も考えられます。

[4] 取り扱う情報の機密性や重要性が高い場合等は、リスクマネジメントを適切に行い、必要なセキュリティ対策を十分に検討するようにしてください。また、業界標準（業界ガイドライン）等において厳格なセキュリティ対策を求められている場合は、それも十分に参照するようにしてください。

4．本ガイドラインの想定読者像

総務省では、本ガイドラインとは別に「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）」（以下本節で「チェックリスト」といいます。）を公表しており、それぞれの想定読者像は次のとおりです

	本ガイドラインの想定読者像	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）の想定読者像
対象属性	システム・セキュリティ管理者のほか経営者やテレワーク勤務者も幅広く対象	システム・セキュリティ管理者
セキュリティ予算	外部委託コストは必要に応じて捻出しうるレベルも含めた幅広い組織	外部委託コストの捻出は難しいレベルの組織
セキュリティ推進体制	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	専任のセキュリティ担当が存在しないような組織
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に対して、対応内容を検討・判断し、対策を実行できる	「適切に…」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
ITリテラシ	VPN・フィルタリング・アンチウイルス等の基本的なIT用語は仕組みとして理解している	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
	システム設定作業は、基本的な内容であれば、無理なく行うことができる	システム設定作業は、基本的な内容であれば、インターネット検索によって調べながら行うことができる

チェックリストでは、システム・セキュリティ管理者が優先的に実施すべき基本的なセキュリティ対策のみに焦点をあて、具体的かつ平易な表現で説明しています。

一方、本ガイドラインでは、テレワークを導入しようとしている又は導入済みの全ての企業等を幅広く対象として、システム・セキュリティ管理者に加えて、経営者やテレワーク勤務者の立場で実施すべきセキュリティ対策[5]や、一定の費用や組織体制が必要になるなど実施難易度が高いセキュリティ対策についても示しています。

そのため、本ガイドラインのセキュリティ対策事項は、チェックリストのセキュリティ対策事項を包含していることから、本ガイドラインの内容について適切な検討・実施ができる場合は、チェックリストを参照する必要はありません。

一方で、本ガイドラインに記載の内容について、理解や検討が難しい場合は、チェックリストの内容を参考にしてください。

[5] 本ガイドラインのセキュリティ対策は、企業等に所属しない個人事業主等の立場でテレワークをされている方も活用できます。この場合、本ガイドラインにおける「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」のそれぞれの立場を全て兼ねることに留意してください。

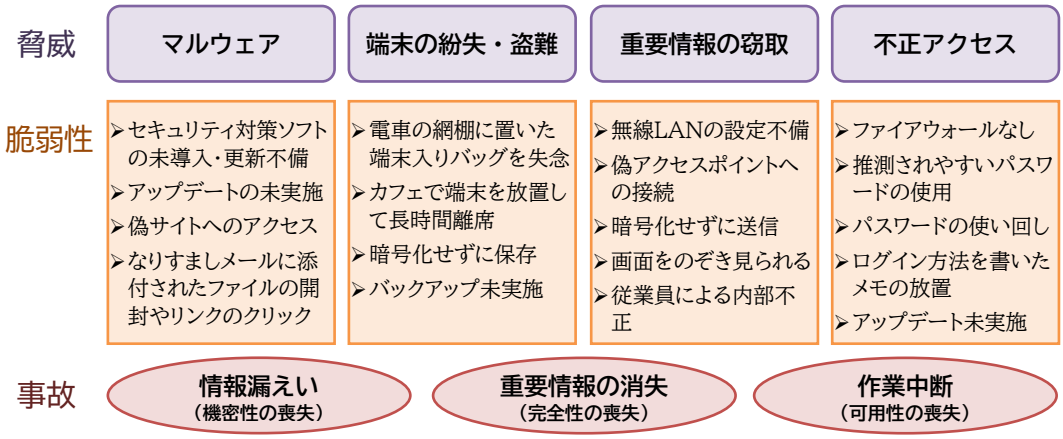
第２章　テレワークにおいて検討すべきこと

１．「ルール」「人」「技術」のバランスがとれた対策

従来のオフィス環境と比較して、テレワーク環境では、従業員同士で情報をやりとりする場合にインターネットを利用する必要があったり、従業員以外の第三者が立ち入る可能性のある場所で作業を行ったりといった、セキュリティ的な観点から環境が異なることがあります。

企業等で管理する紙文書、電子データ、情報システム等をまとめて、その企業等の「情報資産」と呼びます。多くの場合、情報資産はオフィスの中で管理され、外部の目に触れることはありませんが、テレワークを行う場合は、インターネット上を流れたり、持ち運びが容易なノートPC等の端末で利用されたり、第三者が近くにいる状況下で画面に表示されたりします。そのため、セキュリティ対策が十分に施されたオフィス環境とは異なり、テレワーク環境では、情報資産はマルウェア（ウイルス）等の感染やインターネット経由でのサイバー攻撃、テレワーク端末や記録媒体の紛失・盗難、通信内容の窃取やのぞき見等の「脅威」にさらされやすいといえます。

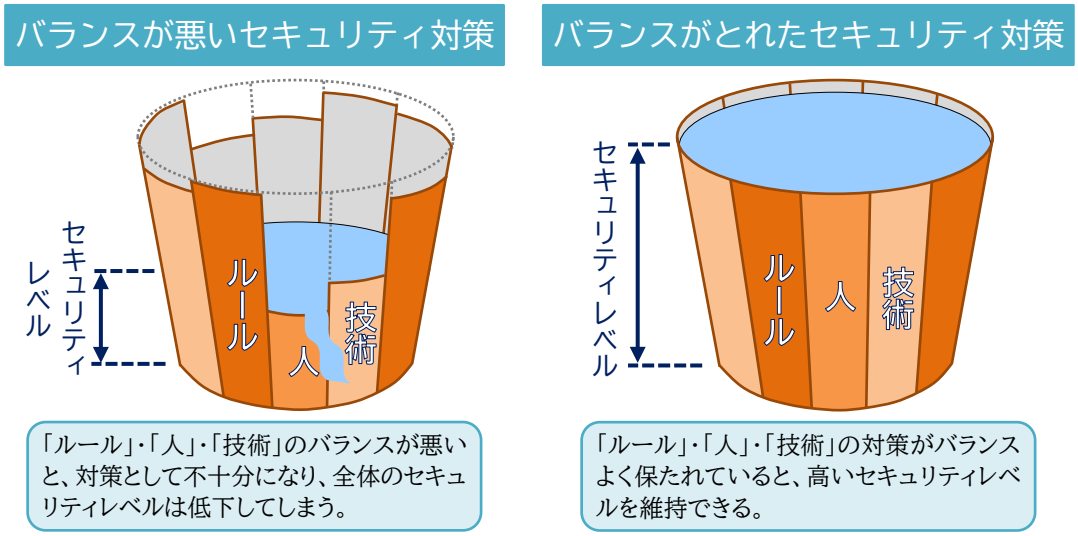
このとき、テレワーク端末の設定や管理の不備といった、脅威に対する「脆弱性」（セキュリティ上の欠陥）が存在すると、情報漏えいや情報の消失等実際の事故の発生につながります。



企業等がセキュリティ対策を効率的に行うには、保護すべき情報資産を洗い出し、どのような脅威や脆弱性（リスク）があるのかを把握、認識した上で、重要度に応じたレベル分けを行い、レベル分けに応じた体系的な対策を実施することが重要です。

このとき、セキュリティ対策は、「最も弱いところが全体のセキュリティレベルになる」という特徴があります。容器に水を入れる例（次ページの図を参照）で示されるように、どこか１箇所に弱点があれば、他の対策をいくら強化しても全体のセキュリティレベルの向上にはつながりません。

情報資産を守るためには、「ルール」・「人」・「技術」のバランスがとれた対策を実施し、全体のレベルを落とさないようにすることが重要です。



①　「ルール」について

業務を進めるに当たって、セキュリティ面で安全かどうかをその都度判断して必要な対策を講じていくことは必ずしも効率的ではなく、また、専門家でなければ適切な判断を行うこともできません。そこで「こうやって仕事をすれば安全を確保できる」という仕事のやり方をルールとして定めておけば、従業員はルールを守ることだけを意識することで、安全に仕事を進めることができます。

テレワークを行う場合、オフィスとは異なる環境で業務を行うことから、そのセキュリティ確保のためには、通常、新たなルールを定める必要があります。

②　「人」について

セキュリティ対策の「ルール」・「人」・「技術」のうち、最も実施が難しいのは「人」の部分です。ルールを定めても、実際に従業員がそれを守らなければ、ルールによる効果が発揮されることはありません。

特にテレワーク勤務者はオフィスから目の届きにくいところで作業をすることになるため、ルールが守られているかどうかを企業等が確認することは容易ではありません。したがって、ルールを定着させるには、教育や啓発活動を通じてルールの趣旨を自ら理解し、ルールを遵守することが自分にとってメリットになることを自覚してもらうことが重要です。また、テレワーク勤務者がセキュリティに関する必要な知識を習得していれば、フィッシングや標的型攻撃等の被害を受けにくくなります。

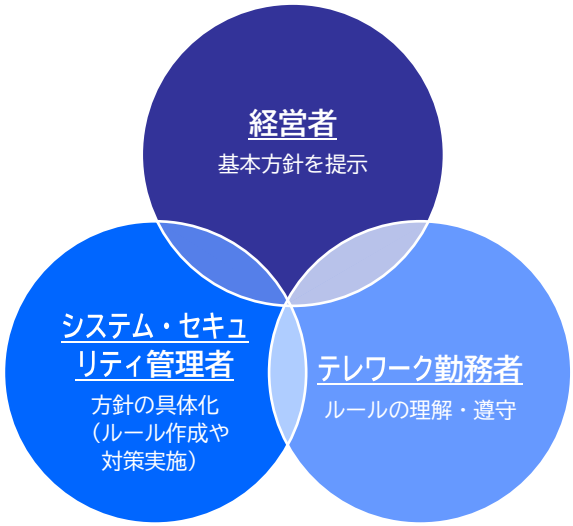
③　「技術」について

「技術」面の対策は「ルール」や「人」では対応できない部分を補完するものです。

技術的な対策を実施する際には、導入するテレワーク方式の特徴や、テレワークの活用方法を踏まえつつ、利便性とセキュリティのバランスをとったものとする必要があります。

２．組織の立場に応じた重要な役割

テレワークの実施に当たっては、「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」がそれぞれの立場からセキュリティの確保に関して必要な役割を認識し、適切に担っていくことが重要です。



本ガイドラインでは、「経営者」は、いわゆる経営層と呼ばれ経営の意思決定に参画できる方を指し、代表権の有無等に限定されません。また、「経営者」や「システム・セキュリティ管理者」が、テレワークを実施する立場になった場合は「テレワーク勤務者」としての役割も期待されるなど、同一人物が複数の立場を兼ねる場合があります。

本節では、「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」のそれぞれの立場について、期待される役割を示した上で、具体的に実施すべき事項を示しています。

記載内容についても、例えば、「経営者」については、経営者として実施すべき事項の全体像が把握できるよう、「システム・セキュリティ管理者」・「テレワーク勤務者」については、特に重要な事項の全体像が把握できるよう、それぞれ系統立てて概略のみを整理して記載しています。

なお、技術的対策を含めたセキュリティ対策の具体については、「第４章　テレワークセキュリティ対策一覧」（p.55～）に示します。

(1) 経営者の役割

経営者の基本的な役割は、事業の効率的かつ健全な発展と、当該事業に影響を及ぼすセキュリティリスクへの対応という両側面から、組織としてのあるべき姿を検討し、その方針を示し、システム・セキュリティ管理者に作業を指示することです。大局的な立場からの判断は、経営者でないとできないと認識しておくことも必要です。また、重要な事項については、テレワーク勤務者に直接示すことも有効です。

事業へのテレワーク活用という観点では、業務効率化、事業継続性の確保、働き方改革等の様々な検討事項がありますが、企業等の活動においてICT利活用が進展した現代では、セキュリティに関する事故が生じた場合、経営に直結した被害が生じうるため、セキュリティの確保も重要な検討事項です。

セキュリティに関するリスクマネジメントを適切に実施するとともに、自組織内におけるセキュリティポリシー(基本方針)やセキュリティ責任者を定める必要があります。また、セキュリティ対策等の実施に支障がないよう予算や人員の確保も必要です。そして、これらのセキュリティ対策に関する取組が、自組織内だけで完結するものではなく、委託先や関連会社を含めて取り組むべきことを理解し実践していくことも必要です。

具体的には、経営者において、上記の役割を踏まえ、次の事項を実施していくことが重要です[6]。なお、「指示する」との記載は、本来は経営者が実施すべき事項であるものの、その具体的作業をシステム・セキュリティ管理者に任せることを意図しています。そのため、権限や予算等を適切に付与し、指示の結果を確認するようにしましょう。

① テレワークセキュリティに関する脅威と事業影響リスクの認識

テレワークはオフィス以外で業務を行うことや、情報の持ち出しが発生すること等から、テレワークの実施に当たってはセキュリティ上の脅威があることを認識するとともに、これにより事業影響リスクが生じうることを認識する。これにより、セキュリティ対策を実施する必要性について、経営者自身が理解する必要がある。

② テレワークに対応したセキュリティポリシーの策定

テレワークの実施に当たり、業務で利用する情報システムや連絡体制が変わることで、従来のセキュリティポリシー（基本方針）で前提としていた状況にも変化が生じる可能性があるため、その見直し（未策定の場合は、策定）を指示する。また、見直し後は、テレワーク勤務者にその内容を周知し、方針の共有を行う。

③ テレワークにおける組織的なセキュリティ管理体制の構築

テレワークの実施に当たり、業務環境が変わるほか、新たな製品・サービスの導入や既存システムの設定変更等により、セキュリティ上のリスクが懸念される。こうしたセキュリティリスクを管理し、必要なセキュリティ対策を実施する責任を組織体制としてどこが負うのか明確にする。また、企業等の意思決定に参加できる経営層レベルの責任者である、最高情報セキュリティ責任者（CISO）を明確にする。

---

[6] 経営者が考えるべき事項は、次のガイドラインも参考になります。
「サイバーセキュリティ経営ガイドライン」（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

④　テレワークでのセキュリティ確保のための資源（予算・人員）確保

テレワークの導入に際しては、従来のシステムとテレワーク環境用のシステムの両方の管理が必要となったり、オフィス外での端末の挙動や情報の取扱いにも注意する必要があったりするなど、従来に比べシステム・セキュリティ管理者の負担が増えることも想定される。そのため、テレワークにおけるセキュリティ確保が適切に実施されるよう、セキュリティ対策に関する予算や人員等の確保を行う。

⑤　テレワークにより生じるセキュリティリスクへの対応方針決定と対応計画策定

テレワークの実施に当たり、守るべき情報を明確にした上で、具体的なセキュリティリスクの特定を指示する。特定されたリスクについて、企業等の戦略と照らし合わせた対応（低減・回避・移転・保有）の方針を示した上で対応計画の策定を指示する。

⑥　テレワークにより対応が必要となるセキュリティ対策のための体制構築

セキュリティリスクへの対応方針や対応計画に従い、セキュリティ対策をとることとなったものについて、そのセキュリティ対策を実施するための体制を構築する。体制構築の際は専門性に応じた適切な人材を割り当て、必要に応じ外部委託も検討する。

⑦　情報セキュリティ関連規程やセキュリティ対策の継続的な見直し

テレワークを狙ったサイバー攻撃が発生するなど、セキュリティリスクは常に変化している。このため、情報セキュリティ関連規程やセキュリティ対策について、継続的に見直しを行うことを指示し、その状況を定期的に確認する。また、こうしたプロセスを仕組みとして整備し、PDCAサイクルが継続的にまわるようにする。

⑧　テレワーク勤務者に対するセキュリティ研修の実施と受講の徹底

テレワークでは、オフィス以外で業務を行うためセキュリティ面での統制が及びにくく、加えて業務とプライベートの区切りも曖昧になりセキュリティ意識も薄れがちである。そのため、組織全体でセキュリティへの理解と意識の向上を図る必要があり、セキュリティ研修の実施を指示するとともに、テレワーク勤務者に対して研修の受講を呼びかける。

⑨　セキュリティインシデントに備えた計画策定や体制整備

テレワークにおいてセキュリティインシデントが発生した場合、オフィスに比べコミュニケーションが制限されるなど従来とは異なる対応を求められることになる。こうした場合も想定したインシデント対応計画を策定するよう指示する。また、インシデント発生の連絡受付や対応に当たって迅速な対応がとれるような体制となっているか確認し、必要に応じて体制の再構築を行う。

⑩　サプライチェーン全体での対策状況の把握

自組織のセキュリティが保護されていたとしても、委託先や関連会社等におけるセキュリティが脆弱であると、預けた情報の漏えいや取引の停滞等により、結果的に自組織にも被害が及ぶ可能性がある。そのため、委託先や関連会社等を含めたサプライチェーン全体で適切なセキュリティ対策が実施されるよう、取引時等にセキュリティ対策状況を確認するなどの必要な対策を行う。特にテレワークの実施に当たって、情報システムの構成や情報のやりとり方法が変更されることもあり、注意が必要である。

(2) システム・セキュリティ管理者の役割

システム・セキュリティ管理者の基本的な役割は、経営者が示した方針や指示を具体化していくことです。情報セキュリティに関するルール（情報セキュリティ関連規程）を作成し、当該ルールを従業員に遵守させる役割を担うとともに、当該ルールに沿った対策の企画や実施も役割として担います。

具体的には、システム・セキュリティ管理者において、上記の役割を踏まえ、次の事項を実施していくことが重要です。

① テレワークに対応した情報セキュリティ関連規程やセキュリティ対策の見直し

自組織が用いるテレワーク方式に応じたセキュリティリスクを評価・把握し、情報セキュリティ関連規程を策定（見直し）するとともに、セキュリティ対策を計画し実施する。また、定期的にセキュリティリスクを再評価するとともに、研修の結果やインシデント発生状況等を踏まえ、情報セキュリティ関連規程やセキュリティ対策の見直しについて検討を行い、必要に応じた変更を実施する。

② テレワークで使用するハードウェア・ソフトウェア等の適切な管理

テレワーク勤務者が使用するテレワーク端末、オフィスネットワークに設置するテレワーク設備、テレワークで利用するソフトウェア・サービス等の一覧を作成し、資産管理を徹底する。また、これらについて最新のセキュリティ状態を保つようアップデートを行うとともに、設定漏れ・設定ミスがないか確認するなど、適切に管理する。

③ テレワーク勤務者に対するセキュリティ研修の実施

テレワーク勤務者に対し、情報セキュリティ関連規程の内容や最新のセキュリティ動向を把握してもらうため、セキュリティ研修等を定期的に実施する。

④ セキュリティインシデントに備えた準備と発生時の対応

テレワーク勤務者においてセキュリティインシデントが発生した場合や、システム・セキュリティ管理者がテレワークだった場合等も想定したインシデント対応計画を策定し、セキュリティインシデント発生時に速やかに対応・復旧ができるようにする。また、対応訓練を実施し、その結果を踏まえ、必要に応じてインシデント対応計画を見直す。

⑤ セキュリティインシデントや予兆情報の連絡受付

テレワーク勤務者がセキュリティインシデントだけでなく、予兆情報（不審情報）を含めて速やかに報告連絡ができるよう、テレワーク時も利用可能な連絡窓口を設け広く周知する。なお、テレワーク勤務者は周囲と気軽に相談しづらい状況も考えられるため、不審な状況があれば幅広く連絡するよう併せて周知する。

⑥ 最新のセキュリティ脅威動向の把握

業界団体や地域のセキュリティコミュニティに参画したり、インターネット上のセキュリティ情報を収集したりするなど、最新のセキュリティ脅威動向を把握し、自組織のセキュリティ対策へ反映する。

(3) テレワーク勤務者の役割

テレワーク勤務者の基本的な役割は、システム・セキュリティ管理者が作成した「ルール」を認識・理解し、これを遵守することです。ルールや対策が適切に整備されたとしても、そのルールが遵守されていない場合、対策が有効に働きません。テレワーク勤務者がルールの重要性を理解し、遵守することがセキュリティの確保につながります。

具体的には、テレワーク勤務者において、上記の役割を踏まえ、次の事項を実施していくことが重要です。

① 情報セキュリティ関連規程の遵守

テレワーク中に利用している情報資産を管理する責任を有していることを理解し、情報セキュリティ関連規程で定められた事項を遵守する。特にテレワークの実施に当たってシステム・セキュリティ管理者が求めるセキュリティ対策について、自身が適切に実施しているかを確認する。

② テレワーク端末の適切な管理

テレワークで使用するPCやスマートフォン等の端末には、機密性の高い情報が含まれうるため、紛失や盗難が発生しないようにするとともに、最新のセキュリティ状態を保つようアップデートを行い、適切に管理する。

③ 認証情報（パスワード・ICカード等）の適切な管理

認証に用いるパスワードの漏えいやICカードの紛失等が発生すると、悪意ある第三者による不正アクセス等に利用されるおそれがあるため、そうした認証情報を適切に管理する。また、パスワードは、第三者に推測されにくい複雑なものを用いる。

④ 適切なテレワーク環境の確保

第三者からののぞき見（ショルダーハッキング）や大声でのオンライン会議による情報漏えい、機器の盗難等が起きないよう、テレワークに適した環境で作業する。また、自宅等においては、無線LAN機器やルーター等のセキュリティ対策を適切に行う。

⑤ セキュリティ研修への積極的な参加

情報セキュリティ関連規程の内容や最新のセキュリティ動向を把握するため、システム・セキュリティ管理者が開催するセキュリティ研修等に積極的に参加する。

⑥ セキュリティインシデントに備えた連絡方法の確認

セキュリティインシデントが発生した際に、どこに対してどのような内容を報告し、自身はどのような行動を取ればよいのか、あらかじめ確認する。特に、連絡先についてはテレワーク実施中であっても確実に連絡が取れるよう確認・記録しておく。

⑦ セキュリティインシデント発生時の速やかな報告

テレワークで使用する端末を紛失した場合、不審なメールやファイルを受信した場合、端末の挙動に不審な点を感じた場合等には、あらかじめ確認しておいた連絡先に速やかに報告し、必要な対応をとる。報告の要否に迷うような事象も幅広く報告することが望ましい。

【コラム】情報漏えい

情報漏えいの傾向

日本ネットワークセキュリティ協会が実施した調査[7]によると、情報漏えいの媒体・経路のうち、インターネットと電子メールが48%と約半数を占めており、年々比率が増加しています。

また、同調査によれば、情報漏えいの原因は、「紛失・置き忘れ」「誤操作」「不正アクセス」が三大要因であり、その３つで約70%を占めています。

情報漏えい対策の必要性

営業情報や個人情報等の情報が漏えいすると、

・漏洩した情報に対する損害賠償請求
・関連企業等との取引停止
・競合他社との競争力の低下
・信頼の失墜（評判の悪化；レピュテーションリスク）

等、企業等に対して大きな影響を及ぼします。実際に、大阪商工会議所が実施した調査結果[8]によると、「取引先がもしサイバー攻撃を受け、その被害が自社にも及んだ場合、採り得る対処」として、「損害賠償請求」（47%）や「取引停止」（29%）が挙げられています。

このような状況を回避するためにも、情報漏えいの対策は重要となります。

必要となる情報漏洩対策

テレワーク用端末にセキュリティ対策ソフトを導入し、最新のバージョンが適用されるよう更新を行う、電子メールに添付されたオフィス文書等を安易に開かないといった基本的な対策が重要となります。

また、電子メール等の誤送信による情報漏えいに対応するため、外部に添付ファイル等を送信する際には二重チェックを実施したり、誤送信防止用のアプリケーションを活用したりといった対策も有効です。

さらに、コワーキングスペース等で紙資料を用いて作業や打合せを行う場合、カフェなどと比べてオフィスに近い環境のため、つい気が緩んで紙資料を置き忘れる例がありますので、十分留意してください。

---

[7] 「2018年 情報セキュリティインシデントに関する調査報告書（速報版）」（令和元(2019)年６月10日）
https://www.jnsa.org/result/incident/2018.html

[8] 「「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」結果について」（令和元(2019)年５月10日）
https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190510sc.pdf

３．クラウドサービスの活用の考え方

(1)　クラウドサービスとは

クラウドサービスとは、ネットワークに接続されたコンピュータ資源（計算能力、記録装置、情報システム等）を、ネットワーク（インターネット）を介して必要なときに必要な分だけ利用できるようなサービスを指します[9]。従来のように企業等が自組織内でサーバ等の構築・運用するオンプレミス環境とは異なり、サーバ等を自ら保有する必要がありません。

クラウドサービスには、クラウドサービス事業者が利用者に提供する資源の範囲（レベル）によって、SaaS・PaaS・IaaSという分類があります。

①　SaaS（Software as a Service）

電子メールやスケジュール管理、文書作成等のソフトウェア（アプリケーション）レベルの資源（機能）を提供するサービスです。

利用者はソフトウェア（アプリケーション）が提供する各種機能を、すぐに利用することが可能です。

②　PaaS（Platform as a Service）

データベース、開発フレームワーク等のアプリケーションを開発や実行するためのプラットフォームレベルの資源（機能）を提供するサービスです。

利用者はプラットフォームが提供する各種機能を使って、必要なアプリケーションを開発する必要があります。

③　IaaS（Infrastructure as a Service）

サーバや記録領域（ストレージ）等のハードウェアレベルの資源を提供するサービスです。

利用者は、提供されたハードウェアを利用するため、自分でOS（オペレーティングシステム）をはじめとする必要なソフトウェアを導入する必要があります。

SaaS＞PaaS＞IaaSの順に、クラウドサービス事業者が提供する資源の範囲が小さくなります。つまり、SaaS＞PaaS＞IaaSの順にクラウドサービス事業者がセキュリティ確保に責任を持つ範囲が小さくなり、その分、利用者がセキュリティ確保に責任を持つ範囲が大きくなります。

例えば、OSのセキュリティ管理は、通常、IaaSでは利用者の責任範囲となり、PaaSや

[9] クラウドサービスは、クラウドサービス事業者が管理するコンピュータ資源に、インターネットを介してアクセスし、複数の企業等が当該資源を部分的に利用していく「パブリッククラウドサービス」と、企業等が自組織内で管理するコンピュータ資源を、自組織の各部署や関連会社等が部分的に利用していく「プライベートクラウドサービス」の２つの形態に大きく分けることができます。本ガイドラインでは、主に「パブリッククラウドサービス」を指して「クラウドサービス」と呼びます。

SaaSではクラウドサービス事業者の責任範囲となります。

テレワークの実施に当たっては、SaaSを活用する場合が増えています。これは、通常の企業等のシステムは、自組織内向けにサービスを提供することを想定して構築されており、インターネット経由でサービスを提供するためには、インターネット対応のための大規模な改修を実施する必要がありますが、SaaSで提供されるサービスを利用することで、この改修を大きく抑えることが見込まれるためです。

なお、SaaSにより提供されるサービスの例は次のとおりです。

① メールサービス

テキスト（文字）によりコミュニケーションを取りたい場合に便利です。オフィス環境と異なり、SaaSで提供されるメールサービスでは、専用アプリケーションと合わせて提供されることも多いことからスマートフォン等での利用との親和性が高く、移動中や自宅にいる場合にも連絡や確認が可能です。

② チャットサービス

細かい情報を往復させながら実施するコミュニケーションにたけているため、高頻度に意思疎通をしたい場合や、テキスト（文字）により内容を確認しながらコミュニケーションを取りたい場合に便利です。スマートフォン等でも連絡が可能なため、移動中や自宅にいる場合にも連絡や確認が可能です。また、音声会話がはばかられる場面での連絡に有効です。

③ オンライン会議サービス

映像・音声もやりとり可能であるため、限りなく対面に近い形でのコミュニケーションをとりたい場合に便利です。複数名による同時コミュニケーションや、会話中の資料共有等も可能です。

ただし、オンライン会議での会話音量が大きいと意図せず会議の内容が第三者に漏えい（音漏れ）してしまったり、また、周囲の会話音がオンライン会議に入り込んでしまったりすることもありますので、周囲の環境等に注意が必要です。

④ ファイル共有サービス

インターネットに接続した様々な端末から、情報の参照や共有が可能です。また、機能や設定によっては、企業等の内と外の間でのファイル共有手段としても注目されています。

なお、ファイル共有のためのURL（リンク）を共有の都度送付する形のファイル共有サービスでは、当該URLを無効化することで共有後のファイル削除が可能となる機能を提供しているサービスも多く、この場合は誤送信のリスクも一部軽減することが可能です[10]。

[10] URLの無効化前に受信側でファイルをダウンロードした場合には削除することはできません。

(2) テレワークにおけるクラウドサービスの有効性

テレワークの導入検討に際して、クラウドサービス（SaaS）を活用することで、システム構築･管理に関する課題に対して､次のような点で有効であると期待されています。

① セキュリティ管理対象の軽減

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

② システム導入の迅速性

オンプレミス環境に新たなシステムを導入する場合、既存システムとの互換性や、ネットワーク環境の再設計が必要になることから時間を要する場合があります。一方、クラウドサービス（SaaS）では、HTTPS等のWeb技術を基本としたサービスが中心であるため、多くの場合、既存システムに大きな変更を加えることなく、速やかにシステム導入が可能となります。

また、クラウドサービス上でシステムを構築する場合、オンプレミス環境と比較して､サーバやネットワーク機器等を物理的に調達し構築する時間を大幅に削減できるため、その点からも迅速なシステム導入が可能となります。

③ システム拡張・縮退の容量柔軟性

オンプレミス環境に新たなテレワーク向けのシステムを導入する場合､あらかじめ利用者数や通信量等を予測して､需要に該当する仕様に適合した製品や通信回線を選定する必要があります。もし、予測より実需要が大きかった場合には、システムの追加や大容量のものへの更改が必要になります。これを回避するために、将来需要等の安全率を見込んだ容量の製品や通信回線を導入することが通常行われており､コストも余分にかけざるを得ない状況です。

一方、クラウドサービスでは想定外の需要が発生したとしても、容量の上限を特に気にすることなく拡張が可能です。また、クラウドサービスでは、利用途中での容量の縮退や、短期間だけの利用にも対応がしやすいという特徴があります。例えば、３ヵ月だけテレワークシステムを試用し、有用であれば利用を継続し、有用でなければ容量を減らして利用したり、利用を取りやめたりすることが可能です。

④ 運用コストの低減

クラウドサービスは､クラウドサービス事業者によって大量のサーバ等を集中的に管理するため、一般的にスケールメリットが働くことから、その構築や運用に係るコストがオンプレミス環境より割安になります。また、運用監視のための人員についても削減することが可能な場合があります。

(3) テレワークへのクラウドサービス活用の考慮事項

テレワークにおいて、クラウドサービス（SaaS）を活用する場合には、セキュリティ確保の観点から次の点について考慮するようにしましょう。

① クラウドサービスやクラウドサービス事業者の信頼性確認

クラウドサービスには、機密性のある情報を保存する場合や、安定したシステム稼働を前提にした業務で利用する場合等が想定されます。そのため、情報を預け、システム運用の一部を担うことになるクラウドサービスやクラウドサービス事業者について、その信頼性を確認することが重要です。

② クラウドサービスのセキュリティ責任境界の確認

クラウドサービスは、例えばSaaSという分類の中でも様々なサービスが存在し、クラウドサービス事業者と利用者との責任の境界（責任分界）はサービス間で一様ではないため、利用するサービスごとに自組織が担うべき責任範囲を確実に確認することが重要です[11]。実際に、クラウドサービスが複雑化し、本来企業等が行うべき対策が不完全であったことによるセキュリティインシデントが増えています。

③ 情報の重要度定義とクラウド保管情報の管理

クラウドサービスは、インターネットを介してアクセスすることが前提となっているため、インターネットを介した攻撃を受けるリスクがあります。クラウドサービス事業者もセキュリティ対策を強化しており、適切なセキュリティ対策がなされていれば、セキュリティリスクは低減させることが可能ですが、リスクをゼロにすることはできないため、業務で取り扱う情報の機密レベルを定義するとともに、クラウドサービス上で取り扱うことができる機密レベルを定め、クラウド上の情報を適切に管理することが重要です。

④ 適切なアクセス制御の実施

主にファイル共有サービスを提供するクラウドサービスにおいて、アクセス制御設定に不備があり、誤ってインターネットに機密情報を公開してしまうケースが発生しています。適切な利用者のみがアクセスできるようにするとともに、設定可能であればIPアドレス制限等により、アクセス制御を強化することを推奨します。

⑤ 厳格な認証情報の管理と認証手法の強化

④のように、適切な利用者のみがアクセスできる設定を実施していたとしても、正規の利用者のアカウント情報（認証情報等）を窃取して、クラウドサービスへ不正アクセスを試みる攻撃が近年増加しています。そのため、各利用者が用いるパスワードを厳格に管理（第三者に推測されにくいものを設定する、使い回しをしない等）するとともに、パスワード漏えい時に備え、多要素認証等の強力な認証手法の活用を検討することが重要です。

---

[11] クラウドサービスには無償や安価なプランを備えている場合もありますが、そのような場合にはセキュリティに関する機能が制限されていたり、利用状況（挙動）をクラウドサービス事業者がマーケティング情報として活用したりすることもあるため、利用に当たって十分に注意してください。

4．ゼロトラストセキュリティの考え方

(1) ゼロトラストセキュリティとは

近年、サイバー攻撃の高度化等に伴い、新たなセキュリティに対する考え方として、「ゼロトラストセキュリティ」というものが注目されています。

ゼロトラストセキュリティとは、外部ネットワーク（インターネット）と、内部ネットワーク（LAN）との境界による防御（境界型セキュリティ）には限界があり、内部ネットワーク内にも脅威が存在しうるという考えのもと、データや機器等の単位でのセキュリティ強化をうたった考え方を指します。

従来の境界型セキュリティの前提が、「信ぜよ、されど確認せよ」であるとすると、それと対比して、ゼロトラストセキュリティは、「決して信頼せず、必ず確認せよ」であるといえます。

ゼロトラストセキュリティを実現するための要件については、参考文献[12]により諸説あるものの、いずれにおいても次のような考え方が特徴的です。

① ネットワークの内部と外部を区別せず、
　データや機器等の最小単位でセキュリティを考える
② 強固な利用者認証と厳密なアクセス管理
③ セキュリティ対策に関して環境（場所・端末等）の制約を設けない

「政府情報システムにおけるゼロトラスト適用に向けた考え方（政府CIO補佐官等ディスカッションペーパー）」の記載を参考に作成したそれぞれの定義は次のとおり。

＜境界型セキュリティ＞

境界線で内側と外側を遮断して、外部からの攻撃や内部からの情報流出を防止しようとする考え方。境界型セキュリティでは、「信頼できないもの」が内部に入り込まない、また内部には「信頼できるもの」のみが存在することが前提となる。防御対象の中心はネットワーク。

＜ゼロトラストセキュリティ＞

「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という「性悪説」に基づいた考え方。利用者を疑い、端末等の機器を疑い、許されたアクセス権でも、なりすまし等の可能性が高い場合は動的にアクセス権を停止する。防御対象の中心はデータや機器等の資源。

[12] ゼロトラストセキュリティの考え方について言及された文献等
1）Zero Trust Architecture（NIST SP800-207）
2）BeyondCorp（Google）
3）Zero Trust eXtended（ZTX）Ecosystem Providers（Forrester）
4）政府情報システムにおけるゼロトラスト適用に向けた考え方（政府CIO補佐官等ディスカッションペーパー）

(2) ゼロトラストセキュリティの有効性（注目される背景）

ゼロトラストセキュリティが注目される背景としては、サイバー攻撃の高度化をはじめとした次のような課題があり、ゼロトラストセキュリティがこれに対する一つの解として有効であると期待されているためです。なお、ゼロトラストセキュリティは、境界型セキュリティに代わるものではなく、両者を組み合わせて複合的に防御することが期待されています。

① サイバー攻撃の高度化

近年、サイバー攻撃はますます高度化・複雑化してきています。例えば、一般に認知された既知の攻撃手法ではなく、「ゼロデイ攻撃[13]」といわれる未知の攻撃手法によるサイバー攻撃も活発に行われています。また、一見すると不審な点のないメールを、取引先を偽って特定の組織に対して送り、セキュリティ意識の甘い従業員を標的としてマルウェア感染させる「標的型攻撃」等の手法もあります。

このような攻撃手法は、境界型セキュリティの考え方のように完全に防御することは困難であり、内部に侵入されることを念頭においた対策が重要になっています。

② マルウェア感染後の検知の難しさ

「標的型攻撃」では、攻撃初期に比較的防御の弱い端末を乗っ取り、当該端末からアクセス可能な範囲の情報や権限を活用して長期的に情報収集を行い、より高い権限を持つアカウントを順次乗っ取っていくという水平展開型の攻撃が行われます。

自組織の利用者の正規の権限を一旦でも奪取されると、境界型セキュリティの考え方では正規ユーザにしか見えず、その後の検知は困難です。そのため、自組織内に攻撃者が存在することを念頭に置き、水平展開による攻撃が容易に行われないように、ネットワーク全体を一律の権限で取り扱うのではなく、データ等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（最小権限の原則）や、対策に不備のあるPCや不審な振る舞いをする利用者等によるアクセスついてはブロックすること（動的なアクセス権制御）などを行うことが重要になっています。

③ ネットワーク構成の多様化に伴う境界の複雑化

情報通信技術の発展に伴い、大容量のデータ活用が進んでいることから、オフィスやデータセンター等の特定の拠点を介したネットワーク構成では、トラフィック集中によるボトルネックが発生し、業務の障害となるケースが増えてきています。こうした状況を受け、テレワーク端末からWebページ閲覧等をする場合に、オフィスネットワークやデータセンター等の拠点を介することなく、テレワーク端末から直接インターネットへアクセスする「ローカルブレイクアウト」というネットワーク構成が注目され、導入が進んでいます。

ローカルブレイクアウトの普及とあわせて、クラウドサービスの普及や個人所有の端末を業務に用いるBYODの活用等も進んでおり、特定の拠点を防御する境界型セキュリティだけでは対応が難しくなっています。データや機器等を防御の中心としていくことが重要になっています。

---

[13] 未修正・未発表のセキュリティ上の脆弱性を悪用した攻撃。

第３章　テレワーク方式の解説

テレワーク方式（システム構成方式）は様々なパターンが考えられますが、本ガイドラインでは、基本的なテレワーク方式として次の７種類に整理しています。なお、各方式の詳細な説明については、本章の「２．テレワーク方式の詳細解説と考慮事項」（p.28～）を参照してください。また、複数のテレワーク方式の併用については本章の「３．テレワーク方式の併用」（p.52～）を参照してください。

①　VPN方式

テレワーク端末からオフィスネットワークに対してVPN接続を行い、そのVPNを介してオフィスのサーバ等に接続し業務を行う方法

②　リモートデスクトップ方式

テレワーク端末からオフィスに設置された端末（PC等）のデスクトップ環境に接続を行い、そのデスクトップ環境を遠隔操作し業務を行う方法

③　仮想デスクトップ（VDI）方式

テレワーク端末から仮想デスクトップ基盤上のデスクトップ環境に接続を行い、そのデスクトップ環境を遠隔操作し業務を行う方法

④　セキュアコンテナ方式

テレワーク端末にローカル環境とは独立したセキュアコンテナという仮想的な環境を設け、その環境内でアプリケーションを動かし業務を行う方法

⑤　セキュアブラウザ方式

テレワーク端末からセキュアブラウザと呼ばれる特殊なインターネットブラウザを利用し、オフィスのシステム等にアクセスし業務を行う方法

⑥　クラウドサービス方式

オフィスネットワークに接続せず、テレワーク端末からインターネット上のクラウドサービスに直接接続し業務を行う方法

⑦　スタンドアロン方式

オフィスネットワークには接続せず、あらかじめテレワーク端末や外部記録媒体に必要なデータを保存しておき、その保存データを使い業務を行う方法

このテレワーク方式のうち、企業等が自組織に適したものを検討・選定する際の参考となるよう、フローチャートや各方式の特性比較を本章の「１．テレワーク方式の選定」（p.26～）に示しています。

また、テレワーク方式にかかわらず共通的に実施すべきセキュリティ対策は、「第４章　テレワークセキュリティ対策一覧」（p.55～）及び「第５章　テレワークセキュリ

ティ対策の解説」（p.66～）に示していますが、各方式に特有のセキュリティ上の考慮事項がある場合には、本章の「２．テレワーク方式の詳細解説と考慮事項」（p.28～）に示しています。

なお、本ガイドライン（第５版）におけるテレワーク方式と、旧版（第４版）におけるテレワーク方式との対応は次のとおりです。

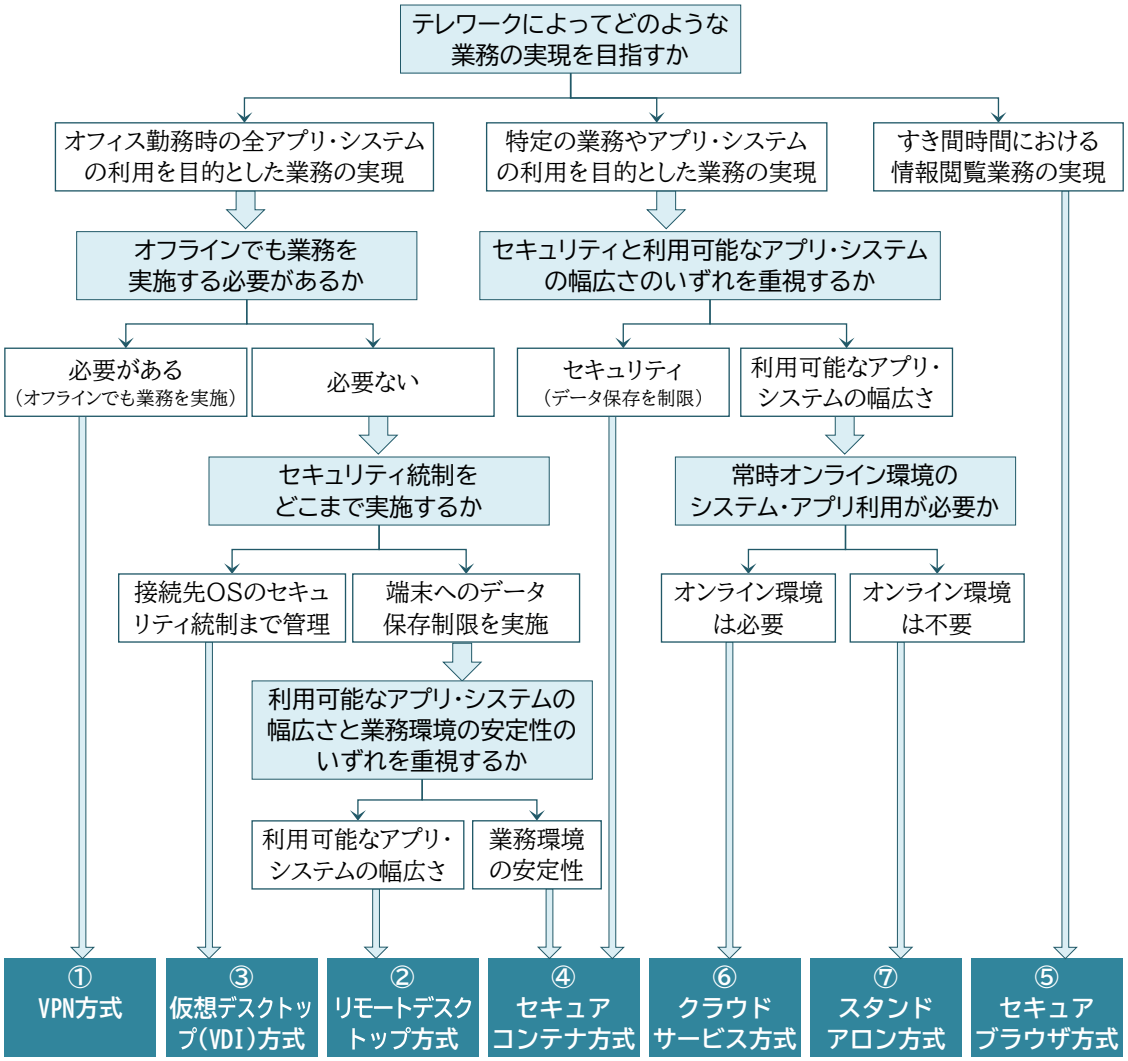
本ガイドライン（第５版）のテレワーク方式	第４版で対応するテレワーク方式
① VPN方式	会社PCの持ち帰り方式
② リモートデスクトップ方式	リモートデスクトップ方式
③ 仮想デスクトップ（VDI）方式	仮想デスクトップ方式
④ セキュアコンテナ方式	アプリケーションラッピング方式
⑤ セキュアブラウザ方式	セキュアブラウザ方式
⑥ クラウドサービス方式	クラウド型アプリ方式
⑦ スタンドアロン方式	会社PCの持ち帰り方式

第４版において「会社PCの持ち帰り方式」としていたものについて、VPN接続を行う場合とスタンドアロンで業務を行う場合とで、セキュリティ上の考慮事項が異なることから分類を細分化したほか、一部の名称についてより理解しやすい方式名に変更しています。

1．テレワーク方式の選定

(1)　フローチャート

実施しようとする業務等を基に、各テレワーク方式のうちどれが適しているかの検討・選定の参考となるよう、フローチャートを次のとおり整理しています。



(2) テレワーク方式の特性比較

各テレワーク方式について、どの方式が適しているかの検討・選定の参考となるよう、各方式の特性を「オフィス業務の再現性[14]」「通信集中時の影響度[15]」「システム導入コスト」「システム導入作業負荷」「セキュリティ統制の容易性[16]」の５軸により、次のとおり整理しています。

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

特性比較の評価は、特性軸ごとに、次の５段階で行っています。

Ｓ：効果や影響が標準よりも相対的に優れている
Ａ：効果や影響が標準よりも相対的にやや優れている
Ｂ：効果や影響が標準的である
Ｃ：効果や影響が標準よりも相対的にやや劣っている
Ｄ：効果や影響が標準よりも相対的に劣っている

評価に当たり、各テレワーク方式は一般的な構成[17]を想定しています。そのため、使用する製品やサービス、具体的なシステム構築方法や構築規模によっては、評価が前後する場合があります。

[14] 物理的な業務（紙媒体の利用・押印等）は考慮していません。
[15] テレワーク用設備に対して通信が集中した時の対応能力を示します。
[16] 端末やクラウド上でのデータ保存に関する制限の容易性や、テレワーク端末やテレワーク関連設備へのシステムアップデートの強制適用の容易性等を示します。
[17] 使用する端末としては、「企業等からの支給端末」と「個人所有端末（BYOD）」の両方を想定しています。ただし、①VPN方式、⑥クラウドサービス方式、⑦スタンドアロン方式については、メリットが大きい「企業等からの支給端末」を想定しています。

２．テレワーク方式の詳細解説と考慮事項

本節では、７種類のテレワーク方式について、それぞれ次の内容について解説をしています。

(a)　基本構成の解説

各方式の基本的な構成について説明しています。

(b)　派生構成の解説

基本構成とは別の派生的な構成について説明しています。

(c)　主なメリット

各方式におけるメリットについて説明しています。

(d)　主なデメリット

各方式におけるデメリットについて説明しています。

(e)　考慮事項

各方式特有のセキュリティ上の留意点のほか、各方式において特に留意すべき考慮事項について説明しています。

なお、テレワーク方式にかかわらず共通的に実施すべきセキュリティ対策は、「第４章　テレワークセキュリティ対策一覧」（p.55～）及び「第５章　テレワークセキュリティ対策の解説」（p.66～）に示しています

(f)　BYOD利用について

各方式において、個人所有端末（BYOD）利用に特化した考慮事項について説明しています。

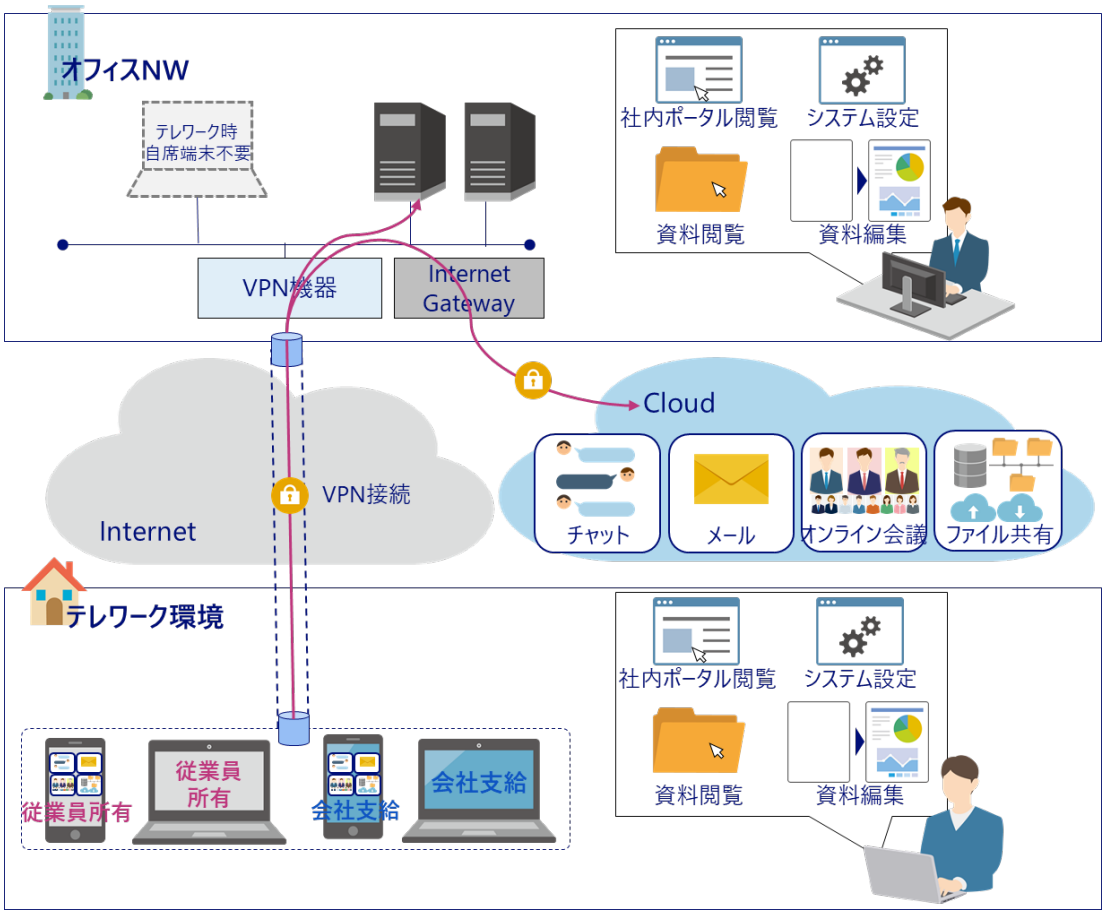
(1)　VPN方式

(a)　VPN方式：基本構成の解説

テレワーク端末からオフィスネットワークにVPN接続を行い、オフィスネットワーク内のファイルサーバやクラウドサービス等に接続し業務を行う方法です。テレワーク端末が物理的にオフィス内にある場合と同じように業務が可能です。

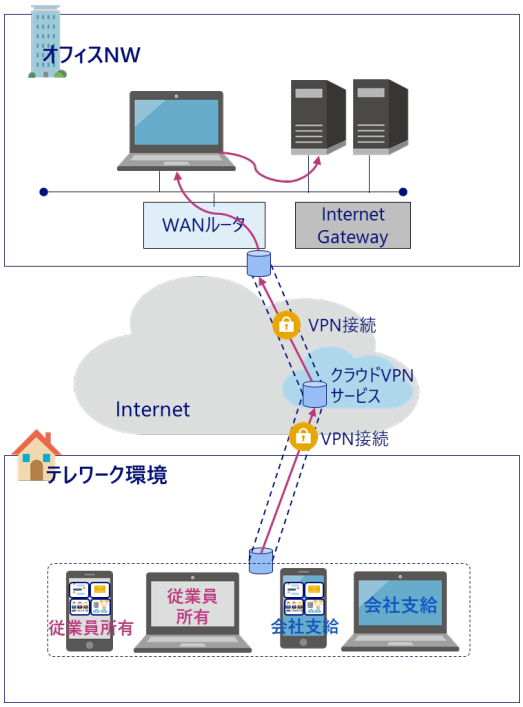
テレワーク端末から外部のクラウドサービス等を利用する際にも、オフィスネットワーク内に設置されたセキュリティ機器を介して接続を行うこととなるため、オフィス内にいるときと同等のセキュリティレベルを確保することができます。加えて、テレワーク端末上にデータの保存が可能です。そのため、通信が不安定になった場合でも、テレワーク端末上に保存されたデータを用いて業務の継続が可能となります。

一方で、情報の持ち出しのリスクや、端末の紛失や盗難による情報漏えいのリスクがあるデメリットがあります。



(b)　VPN方式：派生構成の解説

VPN方式は、次の派生的な構成があります。



①　クラウド型サービスを利用する構成

オフィスネットワーク内にVPN機器を設置するのではなく、クラウド型のVPNサービスを経由して、オフィスネットワークに接続する構成です。

VPN機器の処理能力による同時接続数の上限の問題はなくなりますが、VPNサービスとオフィスネットワークとの間を接続する通信回線の帯域について、必要十分な量が確保されているか考慮する必要があります。

また、クラウドサービスのため、テレワーク勤務者の増減に応じて拡張や縮小が柔軟に可能です。

(c)　VPN方式：主なメリット

・　オフィス内と同等の業務が可能

オフィスネットワークへ接続することにより、物理的にオフィスにいる場合と同じシステムやアプリケーションをテレワーク端末上で利用することができます。そのため、オフィス業務の再現性が高く、オフィスにいる場合と同等の業務が可能です。

ただし、テレワーク端末が支給端末ではなく個人所有端末（BYOD）の場合、業務で利用するシステムやアプリケーションがインストールされていないため、当該メリットを享受できない場合があります。

・　オフィス内と同等のセキュリティレベルの確保が可能

テレワーク端末から外部のクラウドサービス等を利用する際にも、オフィスネットワーク内に設置されたセキュリティ機器を介して接続を行うこととなる（ローカルブレイクアウト時は除く。）ため、オフィス内にいるときと同等のセキュリティレベルを確保することができます。

・　通信回線の影響を受けるがテレワーク端末上での作業で回避可

テレワーク端末上にあらかじめデータを保存しておくことで、通信回線の帯域が不足したり、VPN機器の能力を超える数の接続が行われたりするなどして通信が不安定な場合においても、テレワーク端末上での作業を継続することが可能です。

(d) VPN方式：主なデメリット

・ テレワーク端末のデータ管理とセキュリティ統制が必要

テレワーク端末でデータ処理を行う必要があることから、テレワーク端末へのデータ保存の制限が困難です。そのため、情報の持ち出しのリスクや端末の紛失・盗難等による情報漏えいのリスクへの対応が必要となります。

(e) VPN方式：考慮事項

テレワーク端末上にデータの保存が可能であるため、端末の紛失や盗難による情報漏えいリスクがあります。そのため、テレワーク端末の内蔵記録装置（HDD・SSD等）の暗号化やデータの遠隔消去等の対策が重要となります。

(f) VPN方式：BYOD利用について

個人所有端末（BYOD）を利用する場合、業務で利用するシステムやアプリケーションが利用可能であるか確認が必要なほか、オフィスネットワーク内の環境と異なる環境での業務となるため、利用するテレワーク端末を適切に把握しておくことが重要です。

また、個人所有端末を使用する場合、個人所有端末上にデータ保存が可能であることや、マルウェア対策ソフト等のインストールを強制できないなど、十分なセキュリティ統制が取れません。そのため、セキュリティインシデントが発生しうるリスクを認識し、このリスクが受容可能か評価をした上で、BYOD利用の可否を決定する必要があります。

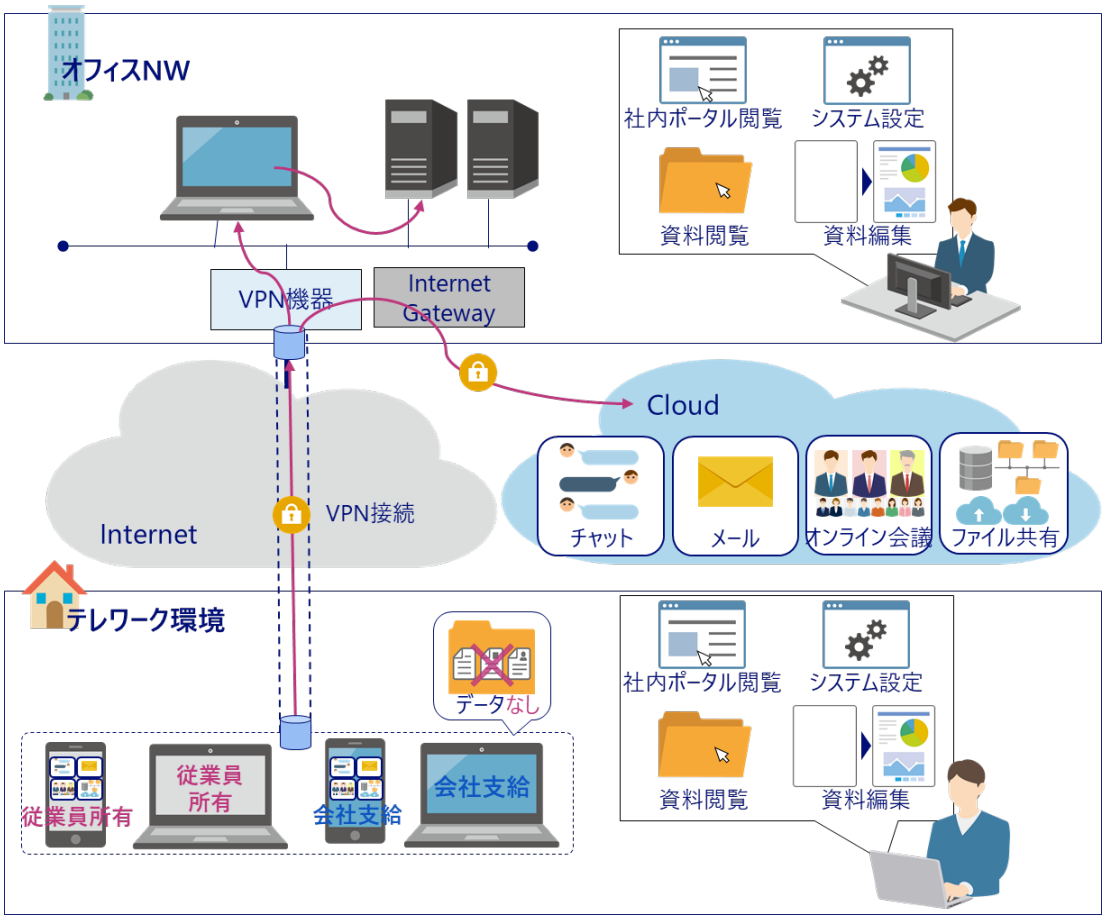
(2)　リモートデスクトップ方式

(a)　リモートデスクトップ方式：基本構成の解説

テレワーク端末から、オフィスネットワーク内に設置されたPC等の端末のデスクトップ環境に接続し、当該デスクトップ環境を遠隔操作することで業務を行う方法です。実際にデータ処理を行うのは、遠隔操作されるオフィスネットワーク内に設置されている端末であるため、オフィス内にいる場合と同じように業務が可能です。

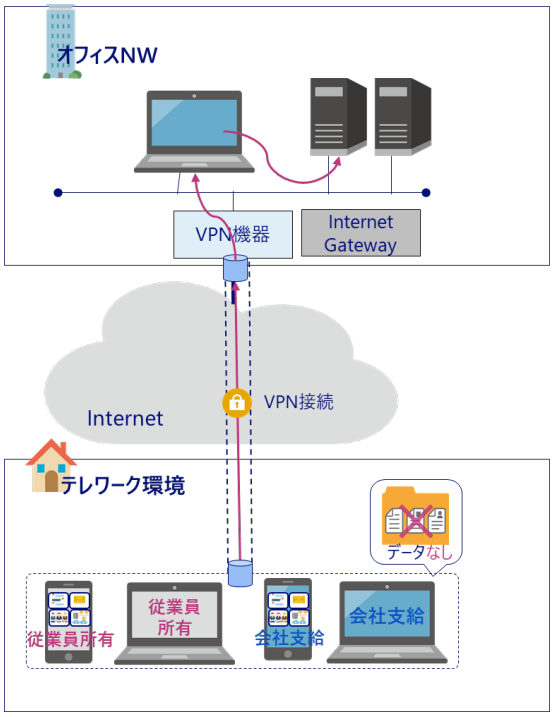
テレワーク端末から外部のクラウドサービス等を利用する際にも、オフィスネットワーク内に設置されたセキュリティ機器を介して接続を行うこととなるため、オフィス内にいるときと同等のセキュリティレベルを確保することができます。加えて、テレワーク端末上へのデータ保存を制限することができるため、データ管理が容易です。

一方で、テレワーク勤務者全員がオフィスネットワークに常時接続して通信を行うことになるため、通信回線の帯域が不足するなどの問題が発生する可能性があります。また、遠隔操作画面をテレワーク端末へ転送することになるため、頻繁にデータの送受信が発生し、通信遅延の影響を大きく受けるデメリットがあります。



(b)　リモートデスクトップ方式：派生構成の解説

リモートデスクトップ方式は、次の派生的な構成があります。

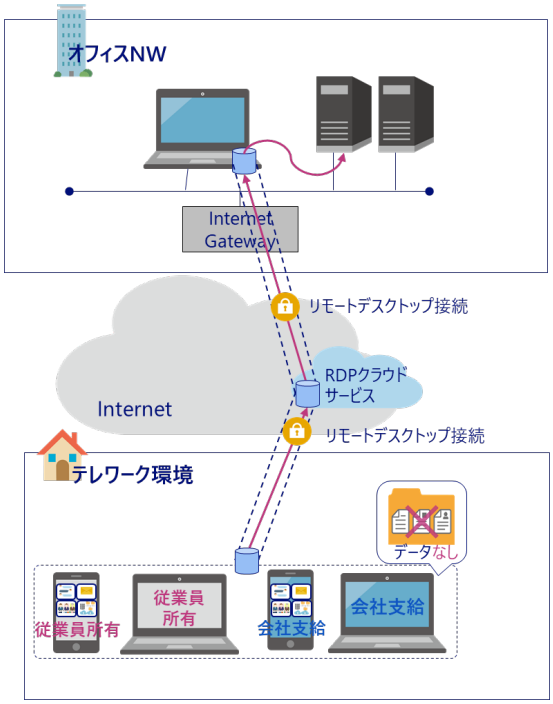


①　VPN接続後にOS標準の「リモートデスクトップ接続」でアクセスする構成

オフィスネットワークにVPN接続を行い、OS標準の「リモートデスクトップ接続」を使用して接続する構成です。

OSに標準として搭載されている機能のため、製品等を別途導入せずに利用が可能です。

また、この方式ではリモートデスクトップ接続時の通信暗号化のためにVPN接続を行っているものの、テレワーク端末にデータを保存しないという点で「(1)　VPN方式」とは異なることから、「リモートデスクトップ方式」として整理しています。

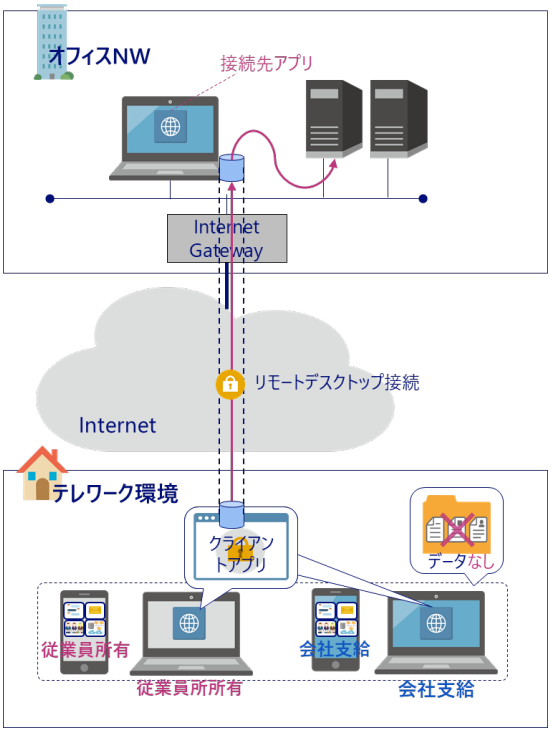


②　クラウド型サービスを利用する構成

オフィスネットワーク内に設置したPCをあらかじめクラウドサービスと同期させ、クラウドサービスを介してテレワーク端末からオフィスネットワーク内に設置したPCに接続する構成です。

VPN接続が必要ないため、オフィスネットワーク内にVPN環境を整備する必要がありません。

また、クラウドサービスのため、テレワーク勤務者の増減に応じて拡張や縮小が柔軟に可能です。



③　オフィスネットワーク内のPCに専用アプリケーションをインストールする構成

オフィスネットワーク内に設置したPC等の端末とテレワーク端末のそれぞれに専用アプリケーションをインストールし、当該アプリケーションを介して接続する構成です。

専用アプリケーションのインストールが必要となるため、導入に時間を要します。

(c)　リモートデスクトップ方式：主なメリット

・　オフィスと同等の業務が可能

オフィスネットワーク内に設置されたPC等の端末を遠隔操作する方式であるため、オフィスネットワーク内にいる場合と同等の業務が可能です。

また、「VPN方式」と異なり、テレワーク端末に業務で利用するシステムやアプリケーションがインストールされている必要がない（遠隔操作先であるオフィスネットワーク内に設置された端末にインストールされていればよい）ため、テレワーク端末が支給端末でもBYODでも、業務の再現性に違いは生じません。

・　オフィス内と同等のセキュリティレベルの確保が可能

テレワーク端末から外部のクラウドサービス等を利用する際にも、オフィスネットワーク内に設置されたセキュリティ機器を介して接続を行うこととなる（ローカルブレイクアウト時は除く。）ため、オフィス内にいるときと同等のセキュリティレベルを確保することができます。

・　テレワーク端末へのデータ保存制限によりデータ管理が容易

設定によりテレワーク端末へのデータ保存の制限が可能なため、テレワーク端末上にデータを保存させないことができ、データ管理が容易です。

(d)　リモートデスクトップ方式：主なデメリット

・　通信回線の影響を受けやすい

テレワーク勤務者全員がオフィスネットワークに常時接続して通信を行うことに

なるため、通信回線の帯域が不足するなどの問題が発生する可能性があります。

また、遠隔操作画面をテレワーク端末へ転送することになるため、頻繁にデータの送受信が発生し、通信遅延の影響を大きく受けてしまいます。

(e) リモートデスクトップ方式：考慮事項

通信回線の帯域に十分考慮する必要があります。そのため、テレワークを導入する前に、通信環境の確認が必要な場合があります。

また、遠隔操作画面をテレワーク端末へ転送することになるため、頻繁にデータの送受信が発生し、通信環境が悪い場合、画面上の操作に遅延が発生し、操作性が著しく低下するおそれがあります。この操作性の低下が著しく業務に影響を及ぼす場合があるため、テレワークを検討している業務が実施可能か業務適性を確認しておく必要があります。

加えて、リモートデスクトップの接続先となるオフィスに設置した端末については、不正な持出し等がなされないような対策（ワイヤーロック等）を検討しておくことも重要です。

(f) リモートデスクトップ方式：BYOD利用について

個人所有端末を利用する場合、個人所有端末へのデータ保存を制限・禁止する必要があります。また、あらかじめBYOD利用に当たってのルールの策定や、端末に必要なセキュリティ対策が施されていることの確認、BYODで利用する端末の管理を行う必要があります。

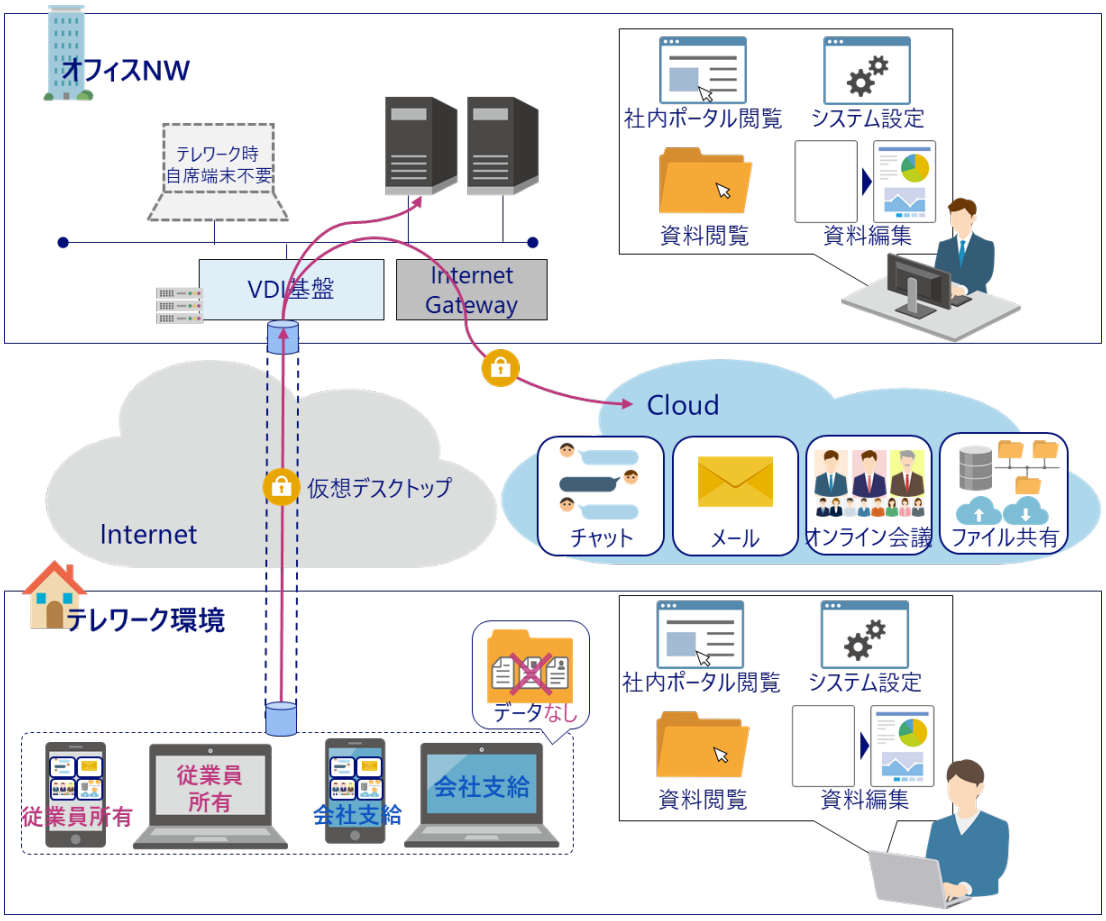
(3) 仮想デスクトップ（VDI）方式

(a) 仮想デスクトップ（VDI）方式：基本構成の解説

テレワーク端末からオフィスネットワーク内に設置された仮想デスクトップ（VDI）基盤に接続し、当該基盤上のデスクトップ画面を通じて業務を行う方法です。前述の「リモートデスクトップ方式」がオフィスネットワーク内に設置されている端末に接続するのに対し、本方式では接続するデスクトップ環境を仮想デスクトップ（VDI）基盤（専用サーバ等）に集約させたものです。

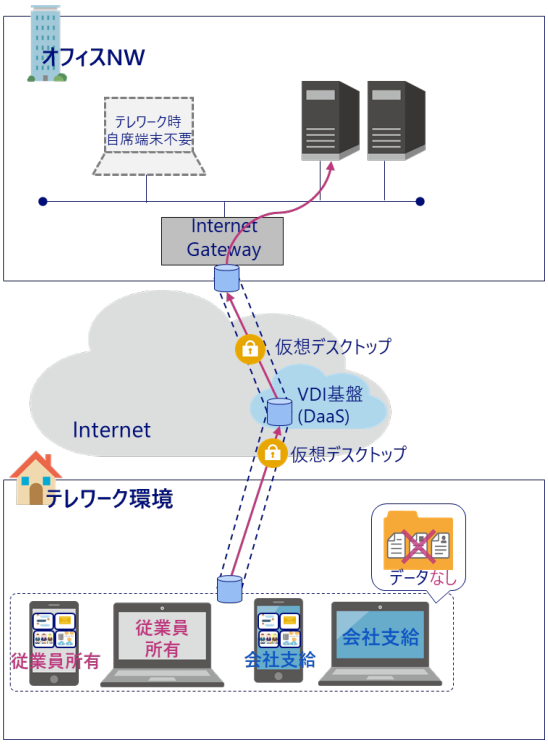
テレワーク端末から外部のクラウドサービス等を利用する際にも、オフィスネットワーク内に設置されたセキュリティ機器を介して接続を行うこととなる（ローカルブレイクアウト時は除く。）ため、オフィス内にいるときと同等のセキュリティレベルを確保することができます。加えて、テレワーク端末上へのデータ保存を制限することができるため、データ管理が容易です。さらに仮想デスクトップ（VDI）環境はシステム・セキュリティ管理者が一括して管理できることから、セキュリティ統制の集中管理が可能となります。

一方で、テレワーク勤務者全員がオフィスネットワークに常時接続して通信を行うことになるため、通信回線の帯域が不足するなどの問題が発生する可能性があります。また、遠隔操作画面をテレワーク端末へ転送することになるため、頻繁にデータの送受信が発生し、通信遅延の影響を大きく受けるデメリットがあります。



(b)　仮想デスクトップ（VDI）方式：派生構成の解説

仮想デスクトップ（VDI）方式は、次の派生的な構成があります。



①　クラウド上に仮想デスクトップ（VDI）基盤を構築する構成

クラウド上に仮想デスクトップ（VDI）基盤を構築し、当該基盤を介してオフィスネットワークに接続する構成です。

仮想デスクトップ（VDI）基盤の管理には高度な技術が必要となりますが、クラウドサービスを利用することで、基盤上のサーバ障害等の対応はクラウドサービス提供事業者に任せることが可能です。

また、クラウドサービスのため、テレワーク勤務者の増減に応じて拡張や縮小が柔軟に可能です。

(c)　仮想デスクトップ（VDI）方式：主なメリット

・　オフィスと同等の業務が可能

オフィスネットワーク内に設置された仮想デスクトップ（VDI）基盤上のデスクトップ画面を遠隔操作する方式であるため、仮想デスクトップ（VDI）基盤上に適切に環境を構築しておくことで、オフィスネットワーク内にいる場合と同等の業務が可能です。

また、「VPN方式」と異なり、テレワーク端末に業務で利用するシステムやアプリケーションがインストールされている必要がない（遠隔操作先である仮想デスクトップ（VDI）基盤上にインストールされていればよい）ため、テレワーク端末が支給端末でもBYODでも、業務の再現性に違いは生じません。

・　オフィス内と同等のセキュリティレベルの確保が可能

テレワーク端末から外部のクラウドサービス等を利用する際にも、オフィスネットワーク内に設置されたセキュリティ機器を介して接続を行うこととなる（ローカルブレイクアウト時は除く。）ため、オフィス内にいるときと同等のセキュリティレベルを確保することができます。

・　テレワーク端末へのデータ保存制限によりデータ管理が容易

設定によりテレワーク端末へのデータ保存の制限が可能なため、テレワーク端末上にデータを保存させないことができ、データ管理が容易です。

・　セキュリティ統制の集中管理が可能

「リモートデスクトップ方式」では、遠隔操作対象の端末はオフィス内で通常使用している端末でしたが、本方式では遠隔操作対象が仮想デスクトップ（VDI）環境に集約されているため、そのセキュリティ統制について管理者が一括して集中管理することが可能です。

(d)　仮想デスクトップ（VDI）方式：主なデメリット

・　通信回線の影響を受けやすい

テレワーク勤務者全員がオフィスネットワークに常時接続して通信を行うことになるため、通信回線の帯域が不足するなどの問題が発生する可能性があります。

また、遠隔操作画面をテレワーク端末へ転送することになるため、頻繁にデータの送受信が発生し、通信遅延の影響を大きく受けてしまいます。

・　大きな環境変更を伴うシステム導入が必要

仮想デスクトップ（VDI）環境の構築や、使用者ごとにデスクトップ環境の構築が必要となるため、大規模な環境変更が必要です。

(e)　仮想デスクトップ（VDI）方式：考慮事項

通信回線の帯域に十分考慮する必要があります。そのため、テレワークを導入する前に、通信環境の確認が必要な場合があります。

また、遠隔操作画面をテレワーク端末へ転送することになるため、頻繁にデータの送受信が発生し、通信環境が悪い場合、画面上の操作に遅延が発生し、操作性が著しく低下するおそれがあります。この操作性の低下が著しく業務に影響を及ぼす場合があるため、テレワークを検討している業務が実施可能か業務適性を確認しておく必要があります。

(f)　仮想デスクトップ（VDI）方式：BYOD利用について

個人所有端末を利用する場合、個人所有端末へのデータ保存を制限・禁止する必要があります。また、あらかじめBYOD利用に当たってのルールの策定や、端末に必要なセキュリティ対策が施されていることの確認、BYODで利用する端末の管理を行う必要があります。

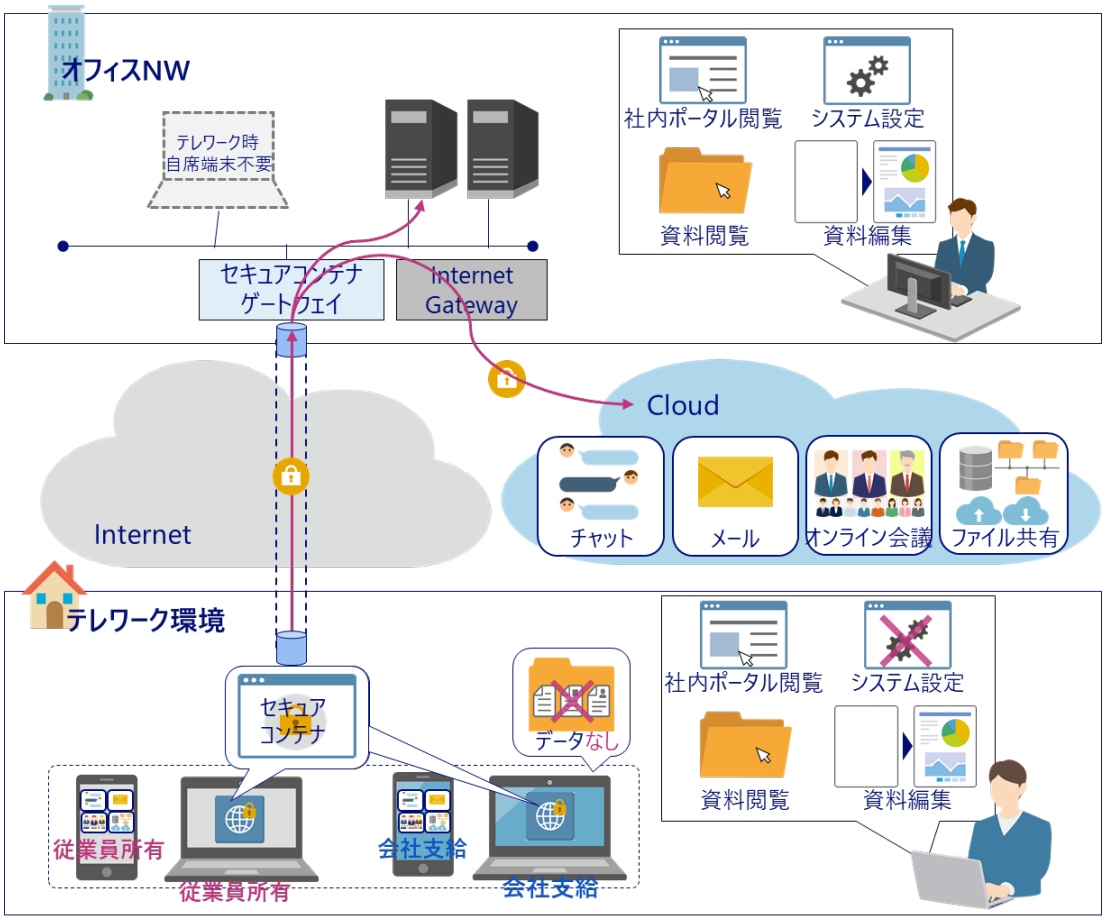
(4)　セキュアコンテナ方式

(a)　セキュアコンテナ方式：基本構成の解説

テレワーク端末上に、ローカル環境（テレワーク端末を通常使っている環境）とは独立したセキュアコンテナという仮想的な環境を設け、その仮想環境内でアプリケーションを動作させ業務を行う方法です。

セキュアコンテナ上で動作するアプリケーションはローカル環境に接続ができないことから、テレワーク端末上にデータを残さずに利用することが可能なため、データ管理が容易です。また、データを処理するアプリケーションはテレワーク端末上（セキュアコンテナ上）で動作しており、その処理に必要なデータをオフィスネットワークとの間で送受信するだけでよいため、インターネットの通信回線の影響を受けにくいです。

一方で、セキュアコンテナ上で動作するアプリケーションに業務が限定されるデメリットがあります。



(b) セキュアコンテナ方式：派生構成の解説

派生的な構成は特にありません。

(c) セキュアコンテナ方式：主なメリット

・ 利用アプリケーション制限によりデータ管理が容易

特定のアプリケーションのみに利用を制限できることから、不必要なデータアクセスを統制することができます。

・ テレワーク端末へのデータ保存制限によりデータ管理が容易

セキュアコンテナ上で動作するアプリケーションはローカル環境に接続ができないことから、テレワーク端末上にデータを残さずに利用することが可能なため、データ管理が容易です。

・ 通信回線の影響を受けるがテレワーク端末上での作業で回避可

セキュアコンテナ上で動作させるアプリケーションはテレワーク端末で動作しているため、通信回線の影響を受けにくく、通信が不安定な場合にもローカルでの作業が可能です。

(d) セキュアコンテナ方式：主なデメリット

・ 特定のアプリケーションに業務が限定

セキュアコンテナ上で動作するアプリケーション（Officeアプリケーションによる文書作成等）に業務が限定されます。そのため、導入予定の製品でどのような業務が実施可能か確認する必要があります。

(e) セキュアコンテナ方式：考慮事項

テレワーク端末上に、ローカル環境（テレワーク端末を通常使っている環境）とは独立した仮想的な環境（暗号化された安全な領域）を設け、その仮想環境内でアプリケーションを動作させるという性質上、特定のアプリケーションに利用が制限されます。

利用可能なアプリケーション例は以下の通り。

アプリケーション種別	操作内容
Officeアプリケーション 例：PowerPoint、Excel、Word	・ファイルの閲覧・編集
ファイルサーバ 例：Windowsファイルサーバ	・ファイルの閲覧・編集
クラウドストレージ 例：Box	・ファイルの閲覧・編集
グループウェア 例：Garoon	・スケジュールの登録・閲覧 ・ワークフロー承認等

実際に対応しているアプリケーションについてはセキュアコンテナ製品によって異なるため、導入予定の製品でどのような業務が実施可能か確認する必要があります。

また、アプリケーションを利用する際に、通常のオフィスでの操作性とセキュアコンテナ上での操作性（反応速度や画面構成等）が異なる場合があるため、操作性についても期待する要件を満たしているか確認してから導入することが望ましいです。

(f) セキュアコンテナ方式：BYOD利用について

個人所有端末を利用する場合、あらかじめBYOD利用に当たってのルールの策定や、端末に必要なセキュリティ対策が施されていることの確認、BYODで利用する端末の管理を行う必要があります。

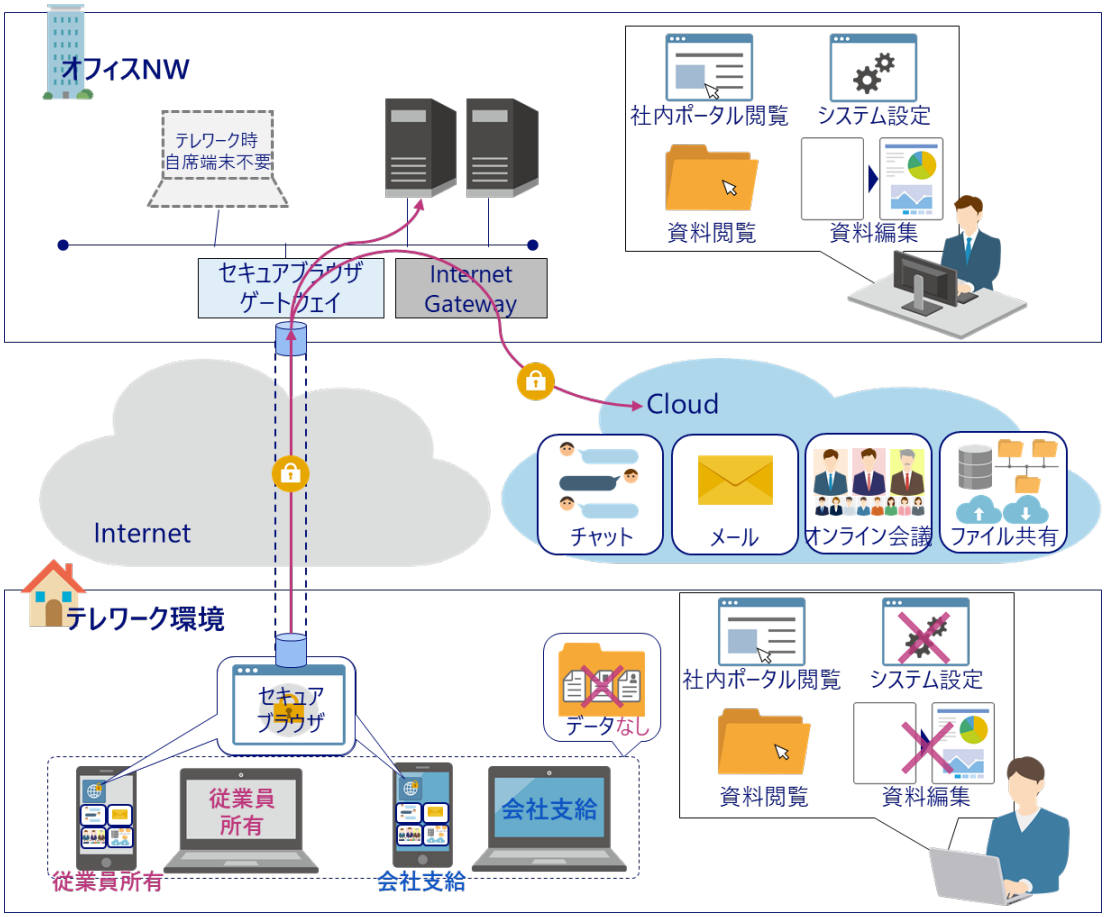
(5)　セキュアブラウザ方式

(a)　セキュアブラウザ方式：基本構成の解説

テレワーク端末上で、セキュアブラウザと呼ばれる特別なインターネットブラウザを利用し、オフィスネットワーク内で利用されるシステム（社内システム）やクラウドサービスで提供されるアプリケーションにアクセスし業務を行う方法です。

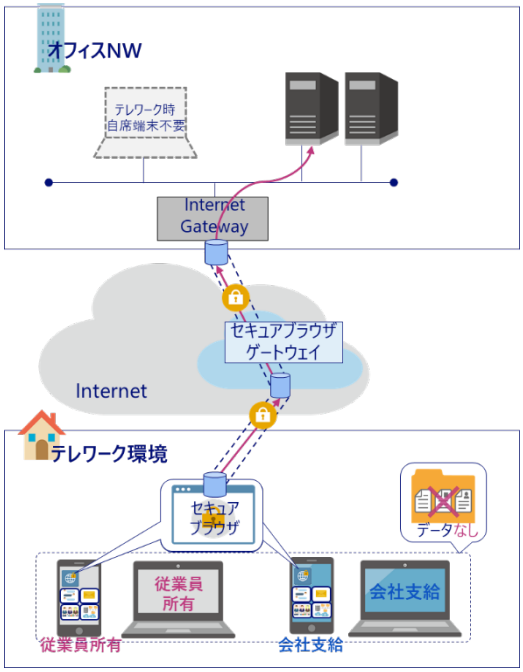
セキュアブラウザを利用することで、ファイルのダウンロードや印刷等の機能を制限することができます。また、テレワーク端末上へのデータ保存を制限することができるため、データ管理が容易です。加えて、セキュアブラウザは、テレワーク端末上で動作しているため、ブラウザ表示に必要なデータをオフィスネットワークとの間で送受信するだけでよいため、常時接続が必要な「リモートデスクトップ方式」や「仮想デスクトップ（VDI）方式」に比べて、インターネットの通信回線の影響が小さいです。

一方で、セキュアブラウザ上で動作するアプリケーションに業務が限定されるデメリットがあります。



(b)　セキュアブラウザ方式：派生構成の解説

セキュアブラウザ方式は、次の派生的な構成があります。



①　クラウド上にセキュアブラウザゲートウェイを構築する構成

クラウド上に設置したセキュアブラウザゲートウェイを介し、オフィスネットワーク内で利用される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する構成です

(c)　セキュアブラウザ方式：主なメリット

- **利用アプリケーション制限によりデータ管理が容易**

特定のアプリケーションのみに利用を制限できることから、不必要なデータアクセスを統制することができます。

- **テレワーク端末へのデータ保存制限によりデータ管理が容易**

特殊なセキュアブラウザ上で業務を実施するため、ファイルのダウンロードや印刷等の機能を制限することができ、テレワーク端末へのデータ保存を制限するなど、データ管理が容易です。

- **通信回線の影響を受けにくい**

「リモートデスクトップ方式」や「仮想デスクトップ（VDI）方式」での画面転送方式と異なり、常時接続して通信を行っているわけではないため、通信回線の影響が小さいです。

(d)　セキュアブラウザ方式：主なデメリット

- **特定のアプリケーションに業務が限定**

セキュアブラウザ上で動作するアプリケーション（資料・メールの閲覧やメールの作成等）に業務が限定されます。そのため、導入予定の製品でどのような業務が実施可能か確認する必要があります。

・ 通信回線の影響を受ける場合がある

セキュアブラウザでの画面表示においても(「セキュアコンテナ方式」と比べると)一定の通信があるため、通信回線の帯域が不足するなどの問題が発生する可能性があります。

(e) セキュアブラウザ方式：考慮事項

セキュアブラウザと呼ばれる特別なインターネットブラウザを利用するという性質上、特定のアプリケーション（資料・メールの閲覧やメールの作成等）に利用が制限されます。そのため、導入予定の製品でどのような業務が実施可能か確認する必要があります。

また、一般的に広く使用されているインターネットブラウザとは操作性が異なる可能性があることに留意が必要です。

(f) セキュアブラウザ方式：BYOD利用について

個人所有端末を利用する場合、あらかじめBYOD利用に当たってのルールの策定や、端末に必要なセキュリティ対策が施されていることの確認、BYODで利用する端末の管理を行う必要があります。

また、セキュアブラウザ方式を実現する製品によってデータが削除されるタイミングが異なり、従業員の利用の仕方によっては、意図せずデータが端末に残るおそれがあります。そのため、個人所有端末を使用する場合、導入するセキュアブラウザ製品の仕様に十分留意する必要があります。

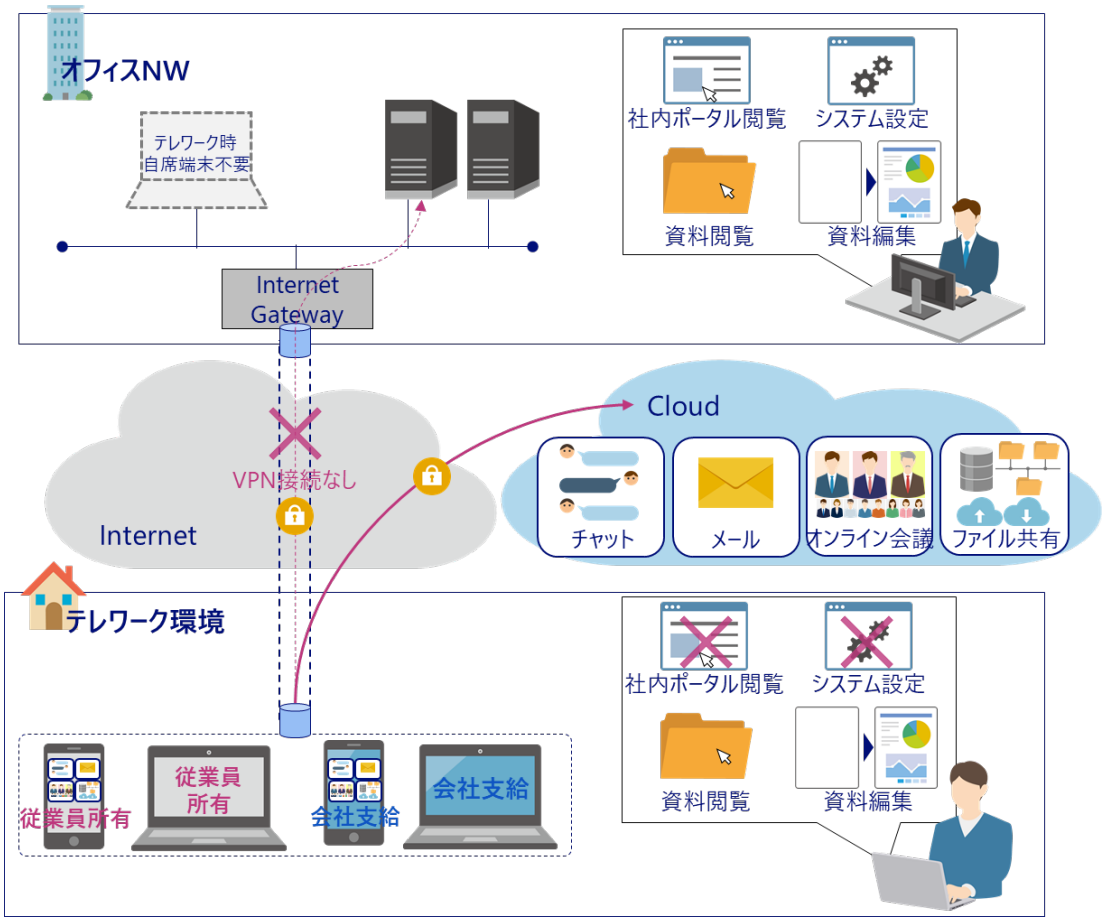
(6)　クラウドサービス方式

(a)　クラウドサービス方式：基本構成の解説

オフィスネットワークに接続せず、テレワーク端末からインターネット上のクラウドサービスに直接接続し業務を行う方法です。

テレワーク勤務者はオフィスネットワークを経由せず、クラウドサービスへ直接接続を行うため、オフィスネットワーク内等にあるテレワークシステムに通信が集中して混雑してしまうといった問題を回避可能です。

一方で、企業等のクラウドサービス導入状況により業務の実現可能な範囲が異なるほか、そもそもクラウドサービスに対応している業務でなければテレワークが実施できないため、どのような業務が実施可能か確認する必要があります。また、クラウドサービスからテレワーク端末上にデータの保存が可能であるため、情報の持ち出しのリスクや、端末の紛失や盗難による情報漏えいのリスクがあります。加えて、オフィスネットワークを経由せず、直接クラウドサービスへ接続するため、利用状況等の把握が困難になるというデメリットがあります。



(b) クラウドサービス方式：派生構成の解説

派生的な構成は特にありません。なお、プロバイダーが提供するメールサービスも、クラウドサービスに該当します。

(c) クラウドサービス方式：主なメリット

・ 必要な数量のみで利用可能

クラウドサービスを利用する従業員に応じて、必要な規模を容易に調達可能です。

・ 比較的軽微な環境変更で利用可能

クラウドサービスはWeb閲覧等と同じ技術を用いている場合が多いため、オフィスネットワーク内の既存システムについて、比較的軽微な環境変更で利用が可能です。

・ オフィスネットワークに接続しないため通信回線の影響なし

オフィスネットワークに接続せず、テレワーク勤務者は直接クラウドサービスに接続して業務を実施するため、テレワーク勤務者が増えても、オフィスネットワークの通信回線の帯域が不足するような問題は生じません。

(d) クラウドサービス方式：主なデメリット

・ 対応しているクラウドサービスに限定

企業等の通常業務において、既にクラウドサービスが導入されている場合は、テレワークによる実現も容易です。

既存の業務をクラウド化する場合は、実施しようとする業務がクラウドサービスとして提供されているものでなければテレワークが実施できないため、どのような業務が実施可能か確認する必要があります。

・ テレワーク端末のデータ管理に加えクラウド分散データ管理が必要

クラウドサービスからテレワーク端末上にデータの保存が可能であるため、情報の持ち出しのリスクや、端末の紛失や盗難による情報漏えいのリスクへの対応が必要です。

また、オフィスネットワークを経由せず、直接クラウドサービスへ接続するため、企業等で定めているサービス以外のクラウドサービスの利用の把握等、管理が困難となります。

(e) クラウドサービス方式：考慮事項

クラウドサービスを利用する際の通信は、オフィスネットワークを経由せず直接インターネットに接続されていることから、オフィスネットワーク上に設置されたセキュリティ機器等による対策ができません。そのため、クラウドプロキシやCASB[18]の導入を検討する必要があります。また、マルウェア対策機能や不正サイトへの接続をブロックす

[18] Cloud Access Security Brokerの略称。クラウドサービスの利用を可視化・制御するためのツール。

る機能を備えたセキュリティ対策ソフトを利用することも重要となります。

また、テレワーク端末上にデータの保存が可能であることから、端末の紛失や盗難による情報漏えいリスク低減のため、テレワーク端末の内蔵記録装置（HDD・SSD等）の暗号化やデータの遠隔消去の対策が重要となります。

加えて、テレワーク端末において処理したデータをクラウドサービス上にアップロードすることも可能であることから、テレワーク端末とクラウドサービスのそれぞれに、どのような情報が保存されているかを管理することも重要です。

さらに、クラウドサービスの利用時はその仕様等を十分に把握した上で利用することが必要であり、設定不備や設定ミス等により、意図せず情報を公開してしまわないよう十分な注意が求められます。同時に、クラウドサービスへのアクセス権限の管理も重要となります。

そして、セキュリティインシデントに備え、クラウドサービスへのアクセスログや操作ログを取得し、それらのログに異常がないか定期的に確認するようにしましょう。テレワーク端末についても、必要なログを取得するなどの対応を実施しましょう。

(f)　クラウドサービス方式：BYOD利用について

個人所有端末を使用する場合、個人所有端末上にデータ保存が可能であることや、マルウェア対策ソフト等のインストールを強制できないなど、十分なセキュリティ統制が取れません。そのため、セキュリティインシデントが発生しうるリスクを認識し、このリスクが受容可能か評価をした上で、BYOD利用の可否を決定する必要があります。

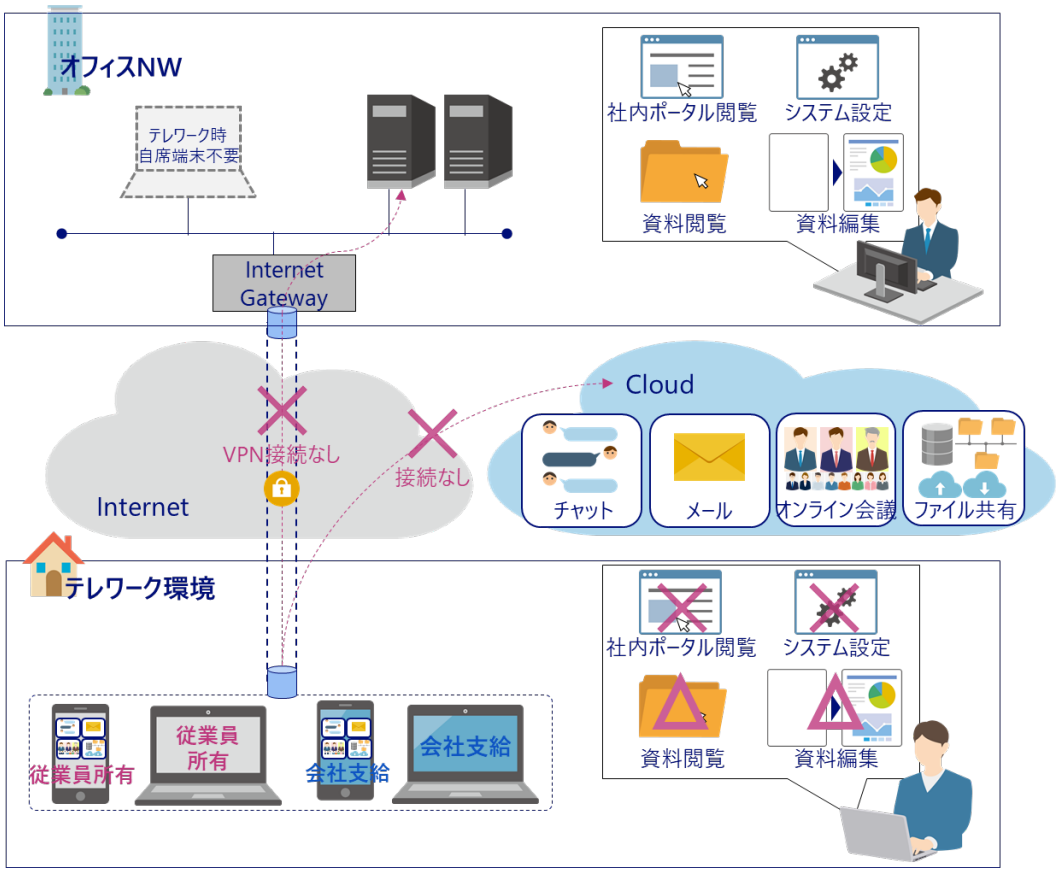
(7) スタンドアロン方式

(a) スタンドアロン方式：基本構成の解説

テレワーク時にオフィスネットワークには接続せず、あらかじめテレワーク端末等へ保存していたデータの編集や閲覧をすることで業務を行う方法です。

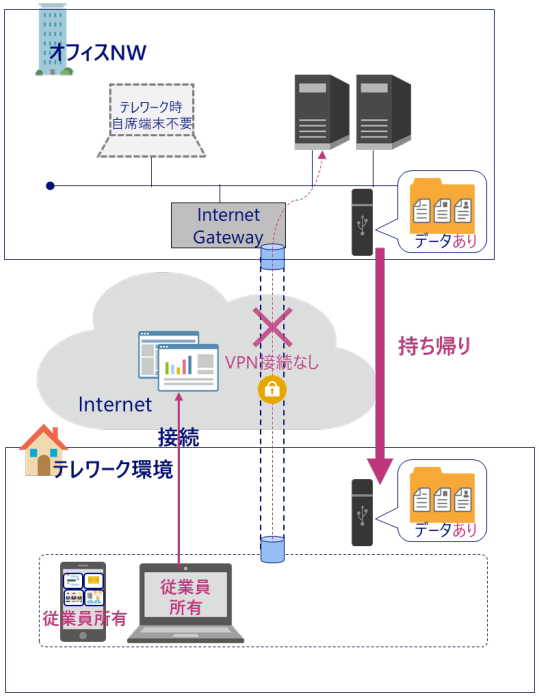
支給端末や個人所有端末をそのまま利用するだけであるため、機器等を新設・増設せずに導入が可能です。また、テレワーク環境からオフィスネットワークへの通信もないため、テレワーク利用に伴う通信集中等の問題も生じません。

一方で、事前に保存したデータを用いた業務に業務内容が限定され、処理したデータをオフィスネットワーク上に反映することもできないため、オフィスから長期間離れて作業するようなテレワーク形態には適合しません。また、テレワーク端末等へ直接データを保存するため、情報の持ち出しのリスクや、端末等の紛失や盗難による情報漏えいのリスクがあります。



(b)　スタンドアロン方式：派生構成の解説

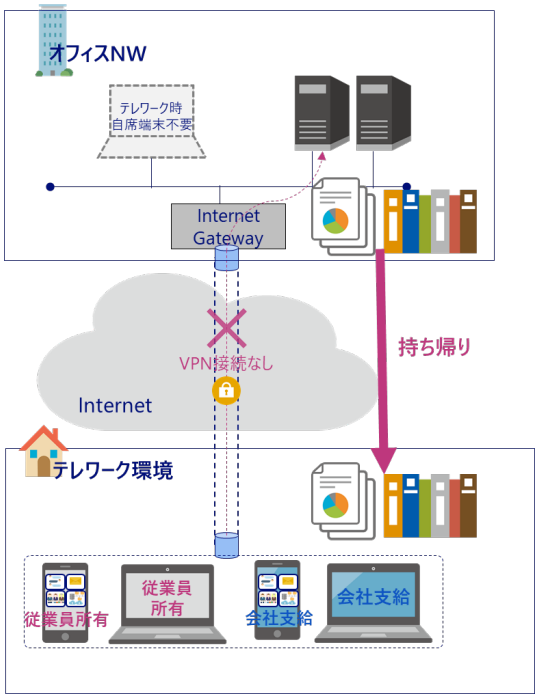
スタンドアロン方式は、次の派生的な構成があります。



①　外部記録媒体でデータを持ち帰り個人所有端末で作業する方式

業務で利用するデータを、テレワーク端末ではなく、USBメモリ等の外部記録媒体に保存して持ち運び、個人所有端末等に接続し業務を行う構成です。

外部記録媒体は通信機能を持たないため、紛失や盗難時に所在地の確認や遠隔からのデータ消去等が行えず、データ管理上のリスクが高いです。また、個人所有端末では、通常、オフィスネットワークと同等のセキュリティ対策ができていないため、マルウェア感染等のリスクもあります。さらに、マルウェアが外部記録媒体（作業後のデータ）を経由してオフィスネットワーク内に持ち込まれるリスクもあります。外部記録媒体は暗号化等のセキュリティ対策を検討しましょう。



②　紙媒体のデータを持ち帰り作業する方式

テレワーク端末と紙媒体（書類等）を持ち出して業務を行う構成です。

紙媒体が電子化されていなくても業務が可能になりますが、紙媒体ではデータの暗号化ができず、加えて紛失や盗難時にデータの所在地を追跡することができないため、情報漏えい等のリスクがあります。

(c) スタンドアロン方式：主なメリット

・ システム構築等が不要

従来使用をしていた端末をテレワーク端末とすることで対応可能なため、新たにシステム構築等を行う必要はありません。

・ 通信をしない通信回線の影響なし

オフィスネットワークに接続せず、テレワーク勤務者はテレワーク端末等に保存されているデータをもとに業務を実施するため、オフィスネットワークの通信回線の帯域が不足するような問題は生じません。

(d) スタンドアロン方式：主なデメリット

・ 保存されたデータで実施できる業務に限定

オフィスネットワークに接続しないため、あらかじめテレワーク端末等に保存したデータを使用した業務に限定されます。また、作業したデータをオフィスネットワーク側に反映することもできません。そのため、長期間オフィスに出勤しないような場合には適合しません。

・ テレワーク端末上のデータ管理とセキュリティ統制が必要

テレワーク端末等へデータを保存し業務等を実施するため、情報の持ち出しのリスクや、端末の紛失や盗難による情報漏えいのリスクへの対応が必要です。

また、調べ物等を行うためインターネットに通常のブラウザ経由で接続することも考えられます。テレワーク端末からインターネット利用が可能な場合は、マルウェアや不正アクセスへの対策等のセキュリティ対策を検討する必要があります。

(e) スタンドアロン方式：考慮事項

テレワーク端末等にデータを保存することから、端末の紛失や盗難による情報漏えいリスク低減のため、テレワーク端末の内蔵記録装置（HDD・SSD等）等の暗号化やデータの遠隔消去の対策が重要となります。

あらかじめテレワーク端末等に保存したデータを使用した業務に限定されますが、情報漏えいリスクを考慮して、必要最低限のデータに絞って持ち出しを行うことが重要です。

加えて、テレワーク端末からインターネット利用を行う可能性がある場合は、マルウェアや不正アクセスへの対策等のセキュリティ対策が必要となります。

(f) スタンドアロン方式：BYOD利用について

個人所有端末を使用する場合、個人所有端末上にデータ保存が可能であることや、マルウェア対策ソフト等のインストールを強制できないなど、十分なセキュリティ統制が取れません。そのため、セキュリティインシデントが発生しうるリスクを認識し、このリスクが受容可能か評価をした上で、BYOD利用の可否を決定する必要があります。

また、USBメモリ等の外部記録媒体を介して支給端末と個人所有端末との間でデータの授受を行う場合、十分にセキュリティ対策がとられていない個人所有端末がマルウェアに感染していると、その外部記録媒体を介して支給端末もマルウェアに感染するおそれがあります。オフィスネットワークのマルウェア感染を防止するために、オフィスへデータを持ち帰る際には外部記録媒体のマルウェアスキャンを実施する必要があります。

さらに、データ移行に利用する外部記録媒体については紛失や盗難のリスクもあるため、外部記録媒体の管理や暗号化が必要となります。

３．テレワーク方式の併用

テレワークの実施に当たって、１つの方式のみを利用する場合だけでなく、複数の方式を併用して利用する場合も想定されます。

実務でよく使用される代表的な例として、ローカルブレイクアウトを併用する方式と、PCとスマートフォン等を併用する方式についてそれぞれ解説します。

(1) ローカルブレイクアウトとの併用

テレワークの実現に当たって、「VPN方式」や「リモートデスクトップ方式」に代表されるように、オフィスネットワークに接続し、業務に必要となる全ての通信をオフィスネットワーク経由でやりとりする方法が広く利用されています。この方法では、テレワーク端末からインターネット（クラウドサービス等）に対する通信も含めて、全ての通信がオフィスネットワークを経由します。そのため、オフィスネットワーク内に設置されたセキュリティ機器を介することとなり、セキュリティ統制が容易となります。

一方で、感染症対応等により従業員がオフィスに出勤することが制限されるような状況では、テレワークの利用に頼るほかなく、多数の従業員が同時にテレワークを実施することとなります。この場合、大量の通信がテレワークを実現するためのシステムに集中することから、これに対応するためにシステムの拡張・増設や通信回線の帯域増加等が必要になり、多くの費用が掛かることが一般的です。

こうした状況に対応するため、オフィスネットワークに接続する方式であっても、インターネットへのアクセスに関しては、オフィスネットワークを介さず、テレワーク端末からインターネットに直接接続させる「ローカルブレイクアウト[19]」という方式が注目されています。

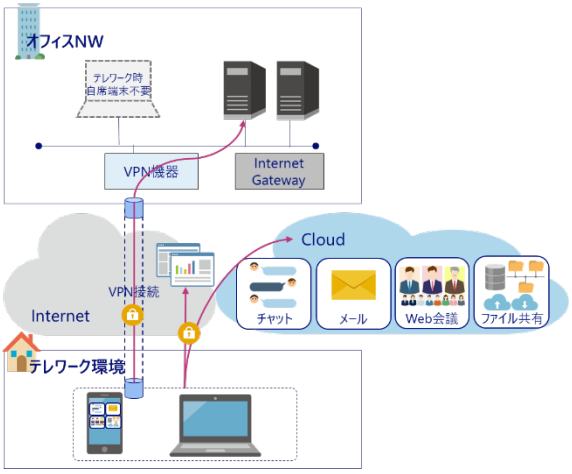
ローカルブレイクアウトを活用する場合、当然ながら、オフィスネットワーク内に設置されたセキュリティ機器を介さず接続することになるため、許可していないクラウドサービスの利用やマルウェア感染等[20]についてセキュリティ統制が難しいという課題があります。そのため、クラウド環境に置かれたプロキシサービス等を経由させるなど、オフィスネットワーク内と同等のセキュリティ統制をかけた上でクラウドサービスを使用することが重要になります。

次ページに、「クラウドサービス方式」をローカルブレイクアウトとして併用する例を示します。

---

[19] インターネットブレイクアウトとも呼ばれます。インターネット向けの通信の全てを直接接続させる方法のほか、特定のドメインや特定のクラウドサービスだけを直接接続させ、それ以外の通信は通常通りオフィスネットワーク経由とする方法もあります。本ガイドラインではこれらをまとめて「ローカルブレイクアウト」と呼称します。なお、セキュリティ統制の観点からは、ローカルブレイクアウトの対象を限定することが効果的です。

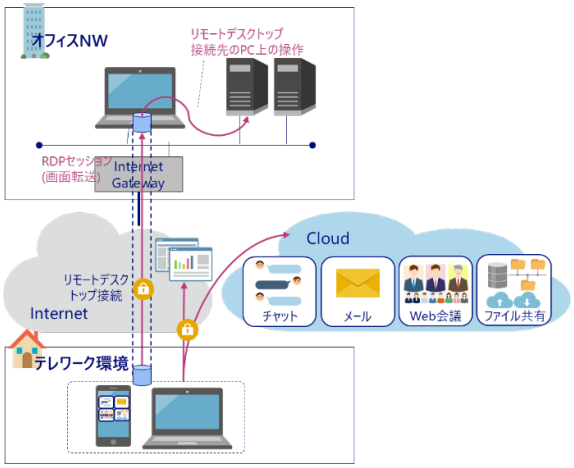
[20] テレワーク勤務者がクラウドサービスを直接利用する場合だけでなく、マルウェア感染した場合に攻撃者が遠隔制御や情報の持ち出しに利用する攻撃指令（C&C）サーバとの通信制限も難しくなります。



① 「VPN方式」とローカルブレイクアウトによる「クラウドサービス方式」の併用

オフィスネットワークには「VPN方式」で接続を行い、クラウドサービスはローカルブレイクアウトとしてテレワーク端末からインターネットに直接接続する方式です。

「VPN方式」については、もともと端末にデータを保存することを前提にしている方式であるため、ローカルブレイクアウトでクラウドサービスを利用したとしても、データ管理上の取扱いは同様です。



② 「リモートデスクトップ方式」とローカルブレイクアウトによる「クラウドサービス方式」の併用

オフィスネットワークには「リモートデスクトップ方式」で接続を行い、クラウドサービスはローカルブレイクアウトとしてテレワーク端末からインターネットに直接接続する方式です。

「リモートデスクトップ方式」は、テレワーク端末上に情報を保存せず、データ管理を容易にする効果があります。そのため、ローカルブレイクアウトでクラウドサービスを利用する場合、クラウドサービス上からテレワーク端末への情報の持ち出しを統制できないというリスクが新たに生じてしまいます。これに対応する方法として、データのダウンロードができないクラウドサービス（例：オンライン会議サービスでテレワーク端末へ情報のダウンロードができない場合）に限り使用を認める方法があります。

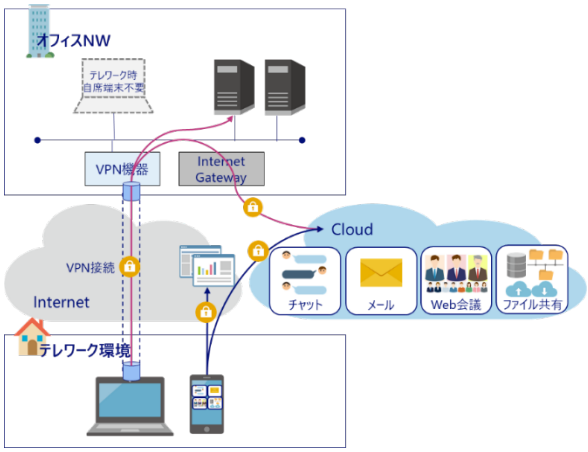
(2)　テレワーク端末としてPCとスマートフォン等の併用

スマートフォン等は、持ち運びがしやすく、移動中といった隙間時間にPCを立ち上げることなく作業も可能であるため、この特徴を活かし、PCとスマートフォン等を併用してテレワークを行う機会も多くなっています。

PCとスマートフォン等を併用する場合、PCへの情報漏えい対策等を積極的に実施していても、スマートフォン等に対する対策が行き届いていない場合も見受けられることから、スマートフォン等に対しても十分なセキュリティ対策を実施することが必要です。

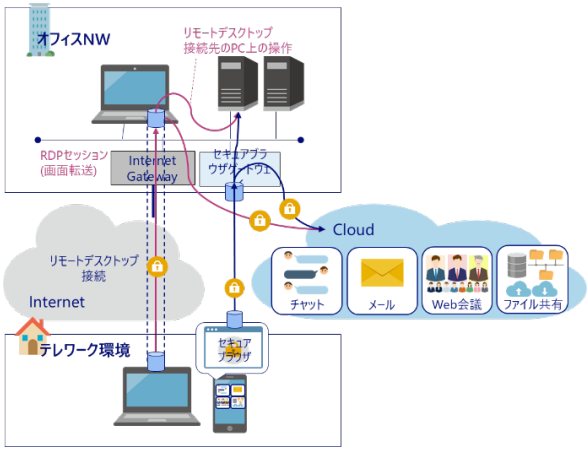
特に、どこでも使用が可能であるというスマートフォンの特徴は、持ち歩く頻度が高く紛失や盗難の可能性が高くなることにもつながることから、MDM（Mobile Device Management）ソリューション等を導入し、データの暗号化や遠隔でのデータ消去等の対策が重要です。

また、スマートフォン等は使用可能なアプリケーション等の制限もあり、PCとは異なるテレワーク方式でスマートフォン等が併用されることも一般的になっています。この場合の代表的な例を以下に示しますが、いずれの場合でも、PCとスマートフォン等とのそれぞれにおいて、適切なセキュリティ対策を実施することが重要です。



①　「VPN方式」のPCと「クラウドサービス方式」のスマートフォン等の併用

通常時にはPCから「VPN方式」で接続して業務を行い、移動時間等にスマートフォン等を活用して「クラウドサービス方式」によって業務を行う方式です。



②　「リモートデスクトップ方式」のPCと「セキュアブラウザ方式」のスマートフォン等の併用

通常時にはPCから「リモートデスクトップ方式」で接続して業務を行い、移動時間等にスマートフォン等を活用して「セキュアブラウザ方式」によって業務を行う方式です。

PCもスマートフォン等も、いずれも端末にデータ残さないテレワーク方式を活用し、データ管理に優れています。

第４章　テレワークセキュリティ対策一覧

テレワーク方式にかかわらず共通的に実施すべきセキュリティ対策について、「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」の立場ごとに一覧として整理しています。なお、テレワーク方式に特有のセキュリティ上の考慮事項については、「第３章　テレワーク方式の解説　２．テレワーク方式の詳細解説と考慮事項」（p. 28～）に示しています。

本ガイドラインではセキュリティ対策を整理するため、次の13個の対策分類[21]に分けています。

	対策分類	説明
A	ガバナンス・リスク管理	テレワークの実施に当たってのリスクマネジメントや、情報セキュリティ関連規程（ルール）の整備等に関する対策。
B	資産・構成管理	テレワークで利用するハードウェアやソフトウェア等の資産の特定や、その管理に関する対策。
C	脆弱性管理	ソフトウェアのアップデート実施等による既知の脆弱性の排除に関する対策。
D	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。
E	データ保護	保護すべき情報（データ）の特定や保存されているデータの機密性・可用性の確保に関する対策。
F	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。
G	通信の保護・暗号化	通信中におけるデータの機密性や可用性の確保に関する対策。
H	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。
I	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。
J	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。
K	物理的セキュリティ	物理的な手段による情報漏えい等からの保護に関する対策。
L	脅威インテリジェンス	脅威動向、攻撃手法、脆弱性等に関する情報の収集に関する対策。
M	教育	テレワーク勤務者のセキュリティへの理解と意識の向上に関する対策。

また、セキュリティ対策は、実施に当たっての優先度の参考として、次のとおり、実施困難度を指標とした「基本対策」と「発展対策」に区分しています。

基本対策	テレワークにおけるセキュリティ対策として一般的に普及しており（実施が比較的容易であり）、基本的に取り組むことが求められるもの。
発展対策	一定の予算や組織体制が整備されていないと実施が困難なセキュリティ対策であるものの、実施により更なるセキュリティの向上が見込めるもの。

なお、各セキュリティ対策において「テレワーク端末」は、PCだけでなくスマートフォン等を含みます。

[21] セキュリティ対策がどの対策分類に対応しているかわかりやすいよう、セキュリティ対策の番号には対応する対策分類のＡ～Ｍの記号を付しています。

1．経営者が実施すべき対策

ガバナンス・リスク管理（詳細解説はp.66～）	
経営者 A-1 基本対策	テレワーク実施に当たって生じる環境変化を踏まえ、セキュリティポリシー（基本方針）の策定や見直し（システム・セキュリティ管理者にその指示をする。）を行い、見直し後は、テレワーク勤務者にその内容を周知し、方針の共有を行う。
経営者 A-2 基本対策	テレワーク実施に伴うセキュリティ対策の重要性を認識し、セキュリティ対策実施に必要となる組織・人材の組成と予算の確保を行う。
データ保護（詳細解説はp.73～）	
経営者 E-1 基本対策	業務で取り扱う情報について、情報の柔軟かつ有効な活用による事業上のメリットと、情報漏えい等が発生した場合の事業影響等を総合的に勘案し、情報取扱いに関する重要度の方針を定める。
インシデント対応・ログ管理（詳細解説はp.86～）	
経営者 J-1 基本対策	セキュリティインシデント発生時に迅速な対応を可能とするため、事業影響レベルを考慮した対応体制と対応優先度を明確としたインシデント対応計画を策定する（システム・セキュリティ管理者に指示する。）。
教育（詳細解説はp.90～）	
経営者 M-1 基本対策	組織全体でセキュリティへの理解と意識の向上を図るため、セキュリティ研修を実施する（システム・セキュリティ管理者に指示する。）とともに、テレワーク勤務者に対して研修の受講を呼びかける。

2．システム・セキュリティ管理者が実施すべき対策

ガバナンス・リスク管理（詳細解説はp.66～）	
管理者 A-1 基本対策	経営者とともにセキュリティポリシー（基本方針）を策定するほか、テレワークのセキュリティを確保するための情報セキュリティ関連規程（対策基準や実施内容）を定め、テレワーク勤務者に周知するとともに、定期的に実施状況を把握・改善する。
管理者 A-2 発展対策	ルールに明文化されていない利用方法や、ルールの改善についてテレワーク勤務者から問い合わせがあった場合、対応方針を検討する。
管理者 A-3 基本対策	テレワーク実施に伴ってクラウドサービス（例：ファイル共有サービス）を利用する場合、情報漏えい等を防止するための利用ルールを整備する。
管理者 A-4 発展対策	クラウドサービスを選定する際には、セキュリティに関する第三者認証を取得しているものや、十分な稼働実績を有しサービス終了のリスクが低いもの、セキュリティ機能強化を継続的に行っているもの等を選定する。
資産・構成管理（詳細解説はp.69～）	
管理者 B-1 基本対策	テレワーク端末を管理する台帳を整備する。また、管理対象となるテレワーク端末について、利用状況（シリアルナンバー、OS種別・バージョン情報、使用アプリケーション、パッチ適用状況、利用者、所在等）を必要に応じて管理・把握する。
管理者 B-2 発展対策	テレワーク端末の利用状況（シリアルナンバー、OS種別・バージョン情報、使用アプリケーション、パッチ適用状況、利用者、所在等）について、資産管理ツールを活用し、常に最新の状態を把握できるようにする。
管理者 B-3 基本対策	テレワーク端末で業務上利用可能なハードウェアやソフトウェア、クラウドサービス等を定め、ルールとしてテレワーク勤務者に周知する。ルール上許可されていないものの利用については、利用者に事前の申請を求め、セキュリティ上の問題がないことを確認できたもののみ利用を許可する。
管理者 B-4 発展対策	テレワーク端末で利用可能なアプリケーションについて、端末管理ツールを活用し、未許可のアプリケーションのインストールを制限・警告する。
管理者 B-5 基本対策	インストールが許可されたアプリケーションについて、定められた場所（公式アプリケーションストア、ベンダーの公式HP等）からのみインストールするようテレワーク勤務者に周知する。
脆弱性管理（詳細解説はp.71～）	
管理者 C-1 基本対策	テレワーク端末におけるOSをはじめとしたソフトウェアについて、アップデートやパッチ適用を定期的に行い最新の状態に保つようテレワーク勤務者に周知する。
管理者 C-2 基本対策	オフィスネットワークにアクセスする際に必要となるVPN機器やリモートデスクトップアプリケーション等について、最新のアップデートやパッチ適用を定期的に行う。

管理者 C-3 基本対策	テレワークで利用する端末やソフトウェアについて、メーカーサポートが終了しているものを利用しないようにテレワーク勤務者に周知する。
管理者 C-4 基本対策	テレワーク勤務者が所有する無線LANルーター等の機器についても、ファームウェアを最新版にするよう、テレワーク勤務者に周知する。
特権管理（詳細解説はp.72～）	
管理者 D-1 基本対策	テレワーク勤務者に貸与するテレワーク端末は必要最小限の権限（例：ユーザ権限）を付与する。
管理者 D-2 発展対策	[Windows利用の場合]テレワーク勤務者に付与するテレワーク端末のアカウント権限はActive DirectoryのGPO（Group Policy Object）にて管理し、User権限を適用する。Administrators権限の適用は業務上必要な機能ごと（例：WindowsUpdate等）に行い、Local Admin権限を適用しない。
管理者 D-3 基本対策	テレワークで利用する製品（VPN機器等）やクラウドサービス等に対する管理者権限は、業務上必要な最小限の人にのみ適用し、アクセス経路も限定（IPアドレス制限等）する。
管理者 D-4 基本対策	テレワーク端末の管理者権限や、テレワークで利用する製品（VPN機器等）やクラウドサービス等に対する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。
データ保護（詳細解説はp.73～）	
管理者 E-1 基本対策	経営者が定める情報取扱いに関する重要度の方針に従い、具体的な情報管理レベルを定めるとともに、テレワークでの利用可否と利用可の場合の取扱方法（利用者・保管場所・利用可能なシステム環境の要件等）を整理してテレワーク勤務者に周知する。
管理者 E-2 発展対策	取り扱う情報の情報管理レベルに照らして、アクセス可能なテレワーク勤務者やテレワーク端末を制限し（認証を実施し）、必要最小限のアクセス権限を適用する。
管理者 E-3 基本対策	テレワークで利用する機密性を有する情報を特定し、保存場所を把握する。
管理者 E-4 基本対策	テレワーク勤務者によるリムーバブルメディア（USBメモリ、CD、DVD等）の使用は、業務上の必要性が認められたものに限定し、ルールで規定する。
管理者 E-5 基本対策	重要情報のバックアップについては、オフィスネットワーク上の共有フォルダ等のほかに、オフィスネットワークから切り離した環境（ネットワークに接続しない記録媒体やクラウドサービス等）にも保管する等、複数の環境でバックアップを保管する。
管理者 E-6 基本対策	テレワーク端末を廃棄する場合は、内蔵されるHDDやSSDについて、データ消去専用ソフトウェアの使用や物理破壊等を行い、データが完全に復元不可能な状態とする。また、テレワーク業務で使用するUSBメモリ等を廃棄する場合も同様に対応する。

管理者 E-7 基本対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルで暗号化を実施するようにテレワーク勤務者に周知する。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。
管理者 E-8 発展対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルでの暗号化を強制し、テレワーク勤務者で設定を変更できないようにする。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。
管理者 E-9 基本対策	テレワーク端末の紛失・盗難に備え、MDM（Mobile Device Management）ソリューション等を導入し、有事の際の遠隔制御でのデータ・アカウント初期化、ログイン時のパスワード認証の強制、ハードディスクの暗号化等の機能を有効化する。
管理者 E-10 基本対策	テレワーク端末の紛失時に端末の位置情報を検知するためのアプリケーションやサービス等を導入する。
マルウェア対策（詳細解説はp.76～）	
管理者 F-1 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
管理者 F-2 基本対策	セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能等を用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
管理者 F-3 発展対策	テレワーク端末にEDR（Endpoint Detection and Response）ソリューションを導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。
管理者 F-4 発展対策	テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるようにする。
通信の保護・暗号化（詳細解説はp.78～）	
管理者 G-1 基本対策	クラウドサービス接続時やデータ送受信を行う際は、通信経路が暗号化された方法（VPN、TLS等）を利用するようテレワーク勤務者に周知する。また、暗号化に際しては危殆化していない暗号アルゴリズム（CRYPTRECを参照するとよい。）が使用されるようにする。
管理者 G-2 発展対策	利用者同士が通信を行うサービスについては、通信相手までの間（E2E：エンドツーエンド）で常時暗号化に対応しているもののみ利用を許可する。
管理者 G-3 基本対策	テレワーク勤務者が無線LANルーター等の機器を利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用し、暗号化のためのパスワード（パスフレーズ）は第三者に推測されにくいものを利用するようテレワーク勤務者に周知する。また、無線LANルーター等の管理者パスワード（設定変更のログイン画面等で必要となるパスワード）についても、第三者に推測されにくいものとすることを併せて周知する。

管理者 G-4 発展対策	オフィスネットワークに接続してテレワークを実施する場合、テレワーク勤務者の最大同時接続数を見込み、その処理が可能な製品やサービスを選定するとともに、必要となる回線帯域やソフトウェアライセンス等を確保する。
アカウント・認証管理（詳細解説はp.81～）	
管理者 H-1 基本対策	テレワーク時にアクセスする社内システムやクラウドサービスへのアクセスで必要となる利用者認証機能について、技術的な基準（多要素認証方式の利用、パスワードポリシーの規定等）を明確に定める。
管理者 H-2 基本対策	社内システムやクラウドサービスへのアクセス時の利用者認証機能として、可能な限り多要素認証を強制する。
管理者 H-3 基本対策	テレワーク端末がオフィスネットワークやクラウドサービスに接続する際は、接続先のサーバの正当性（サーバ証明書等）と、接続元のテレワーク端末の正当性（パスワードやクライアント証明書）を相互に認証する仕組みを備えたものとする。
管理者 H-4 基本対策	テレワーク端末へのログインパスワードや、オフィスネットワークやクラウドサービスにアクセスする際のパスワードは、強力なパスワードポリシーの適用を強制する。
管理者 H-5 基本対策	テレワーク端末やアプリケーションの初期パスワードが強制的に変更されるか、十分な強度のある個別のパスワードが個々に設定されるようにする。
管理者 H-6 基本対策	利用者認証に一定回数失敗した場合、テレワーク端末の一定時間ロックや、テレワーク端末上のデータ消去を行うよう設定する。
管理者 H-7 基本対策	異動や担当変更等を適切に把握し、不要なアカウントの削除やアカウント権限の更新等を実施する。
アクセス制御・認可（詳細解説はp.84～）	
管理者 I-1 基本対策	テレワーク端末においてファイアウォール（パーソナルファイアウォール）を有効にし、適切な設定を施す。
管理者 I-2 基本対策	オフィスネットワークやクラウドサービス等への接続について、接続IPアドレスの制限や、不要ポートの閉鎖を行い、インターネットへの露出を最小限とする。
管理者 I-3 基本対策	データに対するアクセス制御に際して、オフィスネットワーク上の共有フォルダやクラウドサービスに対するアクセス権限設定、ファイアウォール設定等により、機密情報を閲覧・編集する必要のないテレワーク端末やテレワーク勤務者からのアクセスを制御する。
管理者 I-4 発展対策	データに対するアクセス制御に際して、テレワーク勤務者の職務や役割、テレワーク端末の種類やそのセキュリティ対策状況を考慮した動的なアクセス制御を実装する。
管理者 I-5 発展対策	テレワーク勤務者がオフィスネットワークを介さずインターネットに接続を実施することができる構成（ローカルブレイクアウト等）を採るときは、クラウドプロキシによる認証とアクセス制御を実施する。

管理者 I-6 発展対策	オフィスネットワークとインターネットとの通信において、不審なアクセス状況がないか監視する。
管理者 I-7 基本対策	オンライン会議にアクセスするためのURLを正規の参加者以外に公開せず、出席者の確認をするなどして、第三者が会議に参加することのないよう、テレワーク勤務者に周知する。また、会議参加時のパスワード設定や、待機室機能が有効化できる場合には、可能な限り設定するよう併せて周知する。
インシデント対応・ログ管理（詳細解説はp.86～）	
管理者 J-1 基本対策	オフィスネットワークやクラウドサービスの接続に問題が生じた場合や、テレワーク端末に不具合が生じた場合のほか、セキュリティインシデントが疑われる場合に、テレワーク勤務者が対応や連絡を適切に実施できるよう、対応手順や連絡窓口（電話番号を含む。）を整備する。なお、テレワーク勤務者にとって、セキュリティインシデントが不具合と認識される場合があることに留意する。
管理者 J-2 基本対策	セキュリティインシデントの発生に備えて、迅速な対応がとれるよう、インシデント対応計画をあらかじめ策定するほか、自組織内に加え顧客、取引先、監督官庁等に対する連絡体制を整備する。
管理者 J-3 基本対策	セキュリティインシデントが発生した場合、事故発生の原因を分析し、再発防止（必要に応じて追加のセキュリティ対策）に努める。
管理者 J-4 発展対策	セキュリティインシデントの発生に備え、発生を想定した訓練（予行演習）を年１回程度実施する。また、訓練結果を踏まえ、インシデント対応計画等の見直しを行う。
管理者 J-5 基本対策	不正アクセス等のセキュリティインシデントが発生した際に原因調査が可能となるよう、オフィスネットワーク内に設置されたテレワーク関連機器（VPN装置やVDI機器等）へのアクセスログ、テレワーク関連機器やクラウドサービスにログインした後の認証ログや操作ログ、テレワーク端末の操作ログやイベントログ等）について、ログを取得する。
管理者 J-6 基本対策	取得したログについて、保存容量を十分に確保する。過去に遡った調査も必要になることがあるため、可能な限り１年以上保存可能とする。
管理者 J-7 基本対策	テレワーク端末のほか、オフィスネットワーク内の各機器やクラウドサービス上のシステムの時刻が正しく設定（同期）されるように設定する。
管理者 J-8 発展対策	取得ログの検索を容易にするとともに、不正アクセス時のログ改ざんを防止するため、Syslog等を活用し、ログ保存・管理用のサーバを設置する。
管理者 J-9 発展対策	管理者権限の使用状況や、重要情報へのアクセス履歴については、平時から定期的にログの確認を実施する。
管理者 J-10 発展対策	不審なログが記録された際に、自動的にアラートが通知されるようにする。
脅威インテリジェンス（詳細解説はp.89～）	

管理者 L-1 基本対策	セキュリティ関連機関（JPCERT/CC、IPA、NISC等）からセキュリティに関する最新の脅威動向・脆弱性情報を収集する。
管理者 L-2 発展対策	最新の脅威動向・脆弱性情報を把握するために、業界団体や地域のセキュリティコミュニティに加入する。なお、関連するISAC（Information Sharing and Analysis Center）がある場合は、可能な限り加入するようにする。
教育（詳細解説はp.90～）	
管理者 M-1 基本対策	テレワーク勤務者のセキュリティへの理解と意識の向上を図るために、定期的に研修等を実施する。また、テレワーク勤務者に対して最低限求めるセキュリティ対策を定め、テレワーク勤務者に周知する。
管理者 M-2 基本対策	不審メール情報や緊急アップデートの適用等、重要なセキュリティ情報については、組織内のポータルサイトへの掲載、テレワーク勤務者への一斉メールによるアナウンス等、テレワーク勤務者の目にとまりやすい方法で注意喚起を実施する。
管理者 M-3 基本対策	テレワーク勤務者が自ら実施するセキュリティ対策が適切かどうかを確認する機会を年１回程度設け、その結果を把握する。

3．テレワーク勤務者が実施すべき対策

ガバナンス・リスク管理（詳細解説はp.66～）	
勤務者 A-1 基本対策	情報セキュリティ関連規程を確認し、規定に沿った業務を行う。
勤務者 A-2 基本対策	クラウドサービスの利用に際して、定められた利用ルールの範囲で利用する。
勤務者 A-3 発展対策	ルール上明文化されておらず、技術的に可能な利用方法について、暗黙的に許可されていると解釈せず、利用是非についてシステム・セキュリティ管理者に確認する。
資産・構成管理（詳細解説はp.69～）	
勤務者 B-1 基本対策	テレワーク端末が企業等として守るべき情報資産に該当することを認識して適切に管理し、盗難・紛失防止に努める。
勤務者 B-2 基本対策	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際は、ルールで許可されたもの（システム・セキュリティ管理者に申請し許可を受けたものを含む。）のみをインストールする。
勤務者 B-3 基本対策	インストールが許可されたアプリケーションについて、定められた場所（公式アプリケーションストア、ベンダーの公式HP等）からのみインストールする。
脆弱性管理（詳細解説はp.71～）	
勤務者 C-1 基本対策	テレワーク端末におけるOSをはじめとしたソフトウェアについて、自動アップデートを有効にするなどアップデートを適切に実施する（Windows7やFlash Player等のサポートが終了した製品を使用しない。）。
勤務者 C-2 基本対策	テレワーク勤務者が所有する無線LANルーター等の機器についても、ファームウェアを最新版に更新する。
勤務者 C-3 基本対策	テレワーク端末のうち、特にスマートフォンやタブレットに関して、不正な改造（いわゆる脱獄（jailbreak）、root化等）を実施しない。
データ保護（詳細解説はp.73～）	
勤務者 E-1 基本対策	テレワークで取り扱う情報は、定められた取扱方法（利用者・保管場所・利用可能なシステム環境の要件等）に従って取り扱う。
勤務者 E-2 基本対策	リムーバブルメディア（USBメモリ、CD、DVD等）は、業務上必要であり、ルールで許可されている場合のみ利用する。
勤務者 E-3 基本対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルで暗号化を実施する。

マルウェア対策（詳細解説はp.76～）	
勤務者 F-1 基本対策	少しでも不審を感じたメール（添付ファイルやURLリンク等を含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
勤務者 F-2 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
通信の保護・暗号化（詳細解説はp.78～）	
勤務者 G-1 基本対策	クラウドサービス接続時やデータ送受信を行う際は、通信経路が暗号化された方法（VPN、TLS等）を利用する。
勤務者 G-2 基本対策	無線LANルーター等の機器を利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用し、暗号化のためのパスワード（パスフレーズ）は第三者に推測されにくいものを利用する。
勤務者 G-3 基本対策	クラウドサービス（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、接続先のURLが正しいこと（偽サイトでないこと）を確認した上で利用する。
アカウント・認証管理（詳細解説はp.81～）	
勤務者 H-1 基本対策	テレワークに必要となる利用者認証情報（パスワード、ICカード等）を無断貸与や紛失等しないよう、適正に管理する。
勤務者 H-2 基本対策	パスワードは、第三者に推測されにくいものを設定する。多くの文字数を設定できる場合は、複数の単語を組み合わせるなどして文字数が長いもの（パスフレーズ）を設定する。
勤務者 H-3 基本対策	複数のサービス間で同じパスワード使い回さない。また、使用するパスワードが第三者に知られた可能性がある場合は、早急にパスワードを変更する。
アクセス制御・認可（詳細解説はp.84～）	
勤務者 I-1 基本対策	オフィスネットワークやクラウドサービスへの接続は、システム・セキュリティ管理者が指定した方法とし、許可なく設定等を変更しない。
勤務者 I-2 基本対策	テレワーク端末において業務上必要のない無線機能（例：Bluetooth機能、アドホックモード等）は無効化する。
勤務者 I-3 基本対策	複数人でデータを共有可能な場所（オフィスネットワーク上の共有フォルダ、ファイル共有サービス等）に機密情報を保存する場合、情報を閲覧・編集する権限が誰にあるか確認し、適切な設定を実施（テレワーク勤務者で設定できない場合はシステム・セキュリティ管理者に相談）する。
勤務者 I-4 基本対策	オンライン会議にアクセスするためのURLを正規の参加者以外に公開せず、出席者の確認をするなどして、第三者が会議に参加することのないようにする。また、会議参加時のパスワード設定や、待機室機能が有効化できる場合には、可能な限り設定する。

インシデント対応・ログ管理（詳細解説はp.86～）	
勤務者 J-1 基本対策	セキュリティインシデントの発生に備えて、連絡先と対応手順をあらかじめ確認しておく。テレワーク端末が操作不能になることも考えられることから、連絡先は電話番号等も確認するようにしておく。
勤務者 J-2 基本対策	テレワーク端末の紛失やマルウェア感染等のセキュリティインシデントが発生した場合（発生のおそれがある場合を含む。）定められた連絡先へ速やかに報告する。動作が不審であるなど、セキュリティインシデントかどうかわからない場合も速やかに報告する。
物理的セキュリティ（詳細解説はp.88～）	
勤務者 K-1 基本対策	操作画面の自動ロック設定やプライバシーフィルターの貼付等を行うほか、周囲にいる組織外の人の挙動に注意を払う。自宅等で家族がいる場合についても、不注意により意図せず情報漏えい等が起きる可能性があるため注意する。
勤務者 K-2 基本対策	オンライン会議を実施するときは、音漏れや画面を介した情報漏洩が起きないよう注意する。オフィス内であっても、同じ場所で複数人が別のオンライン会議を実施等する場合の音漏れに注意する。
教育（詳細解説はp.90～）	
勤務者 M-1 基本対策	セキュリティに関する研修等を受講し、セキュリティに対する認識を高めるとともに、自らが実施しているセキュリティ対策を確認する。

第５章　テレワークセキュリティ対策の解説

本章では、「第４章　テレワークセキュリティ対策一覧」（p.55～）に示したセキュリティ対策について、対策分類ごとに再掲し、実施に当たっての詳細解説を示しています。

１．ガバナンス・リスク管理

本節では「ガバナンス・リスク管理」として、テレワークの実施に当たってのリスクマネジメントや、情報セキュリティ関連規程（ルール）の整備等に関する対策を示しています。

経営者が実施すべき対策	
経営者Ａ-１ 基本対策	テレワーク実施に当たって生じる環境変化を踏まえ、セキュリティポリシー（基本方針）の策定や見直し（システム・セキュリティ管理者にその指示をする。）を行い、見直し後は、テレワーク勤務者にその内容を周知し、方針の共有を行う。
経営者Ａ-２ 基本対策	テレワーク実施に伴うセキュリティ対策の重要性を認識し、セキュリティ対策実施に必要となる組織・人材の組成と予算の確保を行う。
システム・セキュリティ管理者が実施すべき対策	
管理者Ａ-１ 基本対策	経営者とともにセキュリティポリシー（基本方針）を策定するほか、テレワークのセキュリティを確保するための情報セキュリティ関連規程（対策基準や実施内容）を定め、テレワーク勤務者に周知するとともに、定期的に実施状況を把握・改善する。
管理者Ａ-２ 発展対策	ルールに明文化されていない利用方法や、ルールの改善についてテレワーク勤務者から問い合わせがあった場合、対応方針を検討する。
管理者Ａ-３ 基本対策	テレワーク実施に伴ってクラウドサービス（例：ファイル共有サービス）を利用する場合、情報漏えい等を防止するための利用ルールを整備する。
管理者Ａ-４ 発展対策	クラウドサービスを選定する際には、セキュリティに関する第三者認証を取得しているものや、十分な稼働実績を有しサービス終了のリスクが低いもの、セキュリティ機能強化を継続的に行っているもの等を選定する。
テレワーク勤務者が実施すべき対策	
勤務者Ａ-１ 基本対策	情報セキュリティ関連規程を確認し、規定に沿った業務を行う。
勤務者Ａ-２ 基本対策	クラウドサービスの利用に際して、定められた利用ルールの範囲で利用する。
勤務者Ａ-３ 発展対策	ルール上明文化されておらず、技術的に可能な利用方法について、暗黙的に許可されていると解釈せず、利用是非についてシステム・セキュリティ管理者に確認する。

＜情報セキュリティ関連規程＞

○　企業等においてセキュリティ対策を行う上で、最も基本となるルールが「情報セキュリティ関連規程」です。これは、「情報セキュリティに関する方針や行動指針」をまとめた文書であり、これを作ることで組織として統一のとれたセキュリティレベルを確保することができます。

○　情報セキュリティ関連規程は、

①　セキュリティポリシー（基本方針）

全体の根幹となる文書

② セキュリティスタンダード（対策基準）

基本方針に基づき実施すべきことや守るべきことを規定する文書

③ セキュリティプロシージャ（実施内容）

対策基準で規定された事項を具体的に実行するための手順を示す文書

の３つの階層で構成されます。これらの内容は、企業等の理念、経営戦略、事業規模、保有する情報資産、業種・業態等により異なってくるため、企業等自身の活動に合致した情報セキュリティ関連規程を定めることが必要です。

○ 情報セキュリティ関連規程の３つの階層について、「①セキュリティポリシー（基本方針）」は経営者が定め（案文策定作業はシステム・セキュリティ管理者が行う場合であっても、制定者は経営者とすべきです。）、セキュリティに関する理念や方針を表明します。また、「②セキュリティスタンダード（対策基準）」及び「③セキュリティプロシージャ（実施内容）」はシステム・セキュリティ管理者が定めることが想定されます。

○ 情報セキュリティ関連規程は、テレワークを考慮したものにする必要があります。例えば、テレワークで用いる端末の運用管理部署とテレワーク勤務者の所属する部署とが別であれば、テレワーク中に事故が起きた場合の役割をどちらが担うのかをあらかじめ定めることが必要です。また、いずれのテレワーク方式を選択した場合であっても十分なセキュリティ対策が講じられるようにし、テレワークの提供に関するシステムの管理についても定めておくことが必要です。【経営者Ａ－１、管理者Ａ－１】

○ 情報セキュリティ関連規程を策定して運用するには、責任者を明確にして、策定に携わる適切な人材を確保して組織化すること、必要な予算を確保することがいずれも必要です。【経営者Ａ－２】

○ 情報セキュリティ関連規程は、運用を開始した後も、役職員の要求や社会状況の変化、新たな脅威の発生などに応じて、定期的な見直しが必要です。見直しを継続的に繰り返すことが、セキュリティ対策の向上に役立ちます。

○ 情報セキュリティ関連規程については、企業等に所属する全員に対してセキュリティ教育を実施して、自分の役割は何か、具体的にどのように情報セキュリティ関連規程を守る必要があるのかを周知して、遵守を徹底することが必要です。そのためには、ルールを渡したり、伝えたりするだけではなく、情報セキュリティに関する同意書にサインしてもらう、違反時の規定を設けるなどの方法で、情報セキュリティ関連規程を意識させる仕組みも考えられます。【管理者Ａ－１、勤務者Ａ－１】

○ 情報セキュリティ関連規程に基づき実施しているセキュリティ対策について、定期的（月次や半期ごと等）に実施状況を点検し、システム・セキュリティ管理者から経営者に定期的に報告させ、進捗や対策の効果を把握することが必要です。

＜クラウドサービス利用＞

○ 近年、クラウドサービスの利用が幅広く進んでいますが、これに伴いクラウドサービスにおける情報漏えい等の事例も報告されています。このような状況を極力防ぐためには、自組織内におけるクラウドサービスの利用ルールを定めることが重要です。【管理者Ａ－３、管理者Ａ－４、勤務者Ａ－２】

○ クラウドサービスの利用は、これまで独自に構築していたサービスや業務システ

ムを利用する場合と比較すると、その特性に応じたセキュリティ対策が要求されます。そのため、既存の情報セキュリティ関連規程において、クラウドサービス利用や、テレワーク環境でのクラウドサービスの利用が想定されていない場合、セキュリティ対策が不十分となることから、見直しが必要です。

○　クラウドサービスを安全に利用するためには、クラウドサービスを選定する際の確認事項を明確にし、信頼できるクラウドサービス（クラウドサービス事業者）を選定し、クラウドサービス利用時に必要なセキュリティ対策を明確にし、そしてクラウドサービス利用する際のIDやパスワード等のアカウント情報や保存するデータを適切に管理することが必要です。

○　クラウドサービスの利用の際のセキュリティルールは、情報セキュリティ関連規程と同様に、運用を開始した後も、定期的な見直しが必要です。

○　クラウドサービスを選定する際には、クラウドサービスのセキュリティ対策の実施状況について、第三者認証（第三者の専門家による監査を伴う認証）を取得しているサービスを選定することが、選択の目安となります。なお、クラウドに関する主な第三者認証として、政府情報システムのためのセキュリティ評価制度(ISMAP)[22]、ISO/IEC27001:2013、ISO/IEC 27018:2014、Service and Organization Controls 2（SOC 2）等があります。【管理者Ａ-４】

○　クラウドサービス事業者側での障害や運用の不備等が原因で、クラウドサービス上のデータが消失したり、サービス自体が使えなくなったりという事態も発生しています。そのため、データが消失した場合のことも想定してバックアップを取得したり、サービスが使えなくなった時のために代替手段やサービスを用意したりしておくことも有効です。

[22] 政府機関におけるクラウドサービス調達におけるセキュリティ水準の確保を図るため、内閣官房・総務省・経済産業省が連携して運営しているものです。制度概要や登録されたクラウドサービスについては、制度運用に係る実務及び評価に係る技術的な支援を行っているIPAのWebページを確認願います。
https://www.ipa.go.jp/security/ismap/

2．資産・構成管理

本節では「資産・構成管理」として、テレワークで利用するハードウェアやソフトウェア等の資産の特定や、その管理に関する対策を示しています。

システム・セキュリティ管理者が実施すべき対策	
管理者B-1 基本対策	テレワーク端末を管理する台帳を整備する。また、管理対象となるテレワーク端末について、利用状況（シリアルナンバー、OS種別・バージョン情報、使用アプリケーション、パッチ適用状況、利用者、所在等）を必要に応じて管理・把握する。
管理者B-2 発展対策	テレワーク端末の利用状況（シリアルナンバー、OS種別・バージョン情報、使用アプリケーション、パッチ適用状況、利用者、所在等）について、資産管理ツールを活用し、常に最新の状態を把握できるようにする。
管理者B-3 基本対策	テレワーク端末で業務上利用可能なハードウェアやソフトウェア、クラウドサービス等を定め、ルールとしてテレワーク勤務者に周知する。ルール上許可されていないものの利用については、利用者に事前の申請を求め、セキュリティ上の問題がないことを確認できたもののみ利用を許可する。
管理者B-4 発展対策	テレワーク端末で利用可能なアプリケーションについて、端末管理ツールを活用し、未許可のアプリケーションのインストールを制限・警告する。
管理者B-5 基本対策	インストールが許可されたアプリケーションについて、定められた場所（公式アプリケーションストア、ベンダーの公式HP等）からのみインストールするようテレワーク勤務者に周知する。
テレワーク勤務者が実施すべき対策	
勤務者B-1 基本対策	テレワーク端末が企業等として守るべき情報資産に該当することを認識して適切に管理し、盗難・紛失防止に努める。
勤務者B-2 基本対策	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際は、ルールで許可されたもの（システム・セキュリティ管理者に申請し許可を受けたものを含む。）のみをインストールする。
勤務者B-3 基本対策	インストールが許可されたアプリケーションについて、定められた場所（公式アプリケーションストア、ベンダーの公式HP等）からのみインストールする。

＜資産台帳の整備＞

○　自組織内で使用されているハードウェアやソフトウェアの所在、利用者、バージョン、パッチの適用状況が明確でない場合、どれにどのようなセキュリティ対策が必要になるのか、また、どれがセキュリティ対策を実施済みでどれがセキュリティ対策を未実施なのかが不明確になります。こうした事態を防ぐために、台帳を整備し、ハードウェアやソフトウェアに関する各種情報を常に最新化しておくことが重要です。【管理者B-１】

＜導入ソフトウェア等の管理＞

○　許可していないハードウェアやソフトウェア、クラウドサービス等が勝手に利用される（いわゆるシャドーIT）と、守るべき業務情報等について、管理者によるセキュリティ統制が行えなくなり、情報漏えいのリスクが増加します。したがって、テレワーク端末にインストールされているソフトウェアや、インストール方法等を管理し、把握していないソフトウェアのインストールや、把握していないクラウドサービスの利用がないようにすることが重要です。【管理者B-３、勤務者B-２】

○　許可しているソフトウェアは、公式ストア、ベンダーの公式HP、自組織内のファイルサーバ等の安全な場所からのみインストールできるように周知することが必

要です。【管理者Ｂ-５、勤務者Ｂ-３】

○　ソフトウェアのインストールに関しては、攻撃者によるマルウェアのインストールが行われるケースもあります。ルールによるソフトウェアの利用統制には強制力がないため、ファイル実行やWebアクセス等をトリガーにインストールされるマルウェア感染等を防ぐことはできませんが、資産管理ツールによる統制を行うことにより、マルウェア感染のリスクを低減させることができます。【管理者Ｂ-２】

○　テレワーク端末を一括管理して運用を自動化するための仕組みとして、端末管理ツールを導入し、遠隔操作やソフトウェア管理などの機能により各端末のセキュリティを強化することは、有効な対策の一つです。【管理者Ｂ-４】

3．脆弱性管理

本節では「脆弱性管理」として、ソフトウェアのアップデート実施等による既知の脆弱性の排除に関する対策を示しています。

システム・セキュリティ管理者が実施すべき対策	
管理者C-1 基本対策	テレワーク端末におけるOSをはじめとしたソフトウェアについて、アップデートやパッチ適用を定期的に行い最新の状態に保つようテレワーク勤務者に周知する。
管理者C-2 基本対策	オフィスネットワークにアクセスする際に必要となるVPN機器やリモートデスクトップアプリケーション等について、最新のアップデートやパッチ適用を定期的に行う。
管理者C-3 基本対策	テレワークで利用する端末やソフトウェアについて、メーカーサポートが終了しているものを利用しないようにテレワーク勤務者に周知する。
管理者C-4 基本対策	テレワーク勤務者が所有する無線LANルーター等の機器についても、ファームウェアを最新版にするよう、テレワーク勤務者に周知する。
テレワーク勤務者が実施すべき対策	
勤務者C-1 基本対策	テレワーク端末におけるOSをはじめとしたソフトウェアについて、自動アップデートを有効にするなどアップデートを適切に実施する（Windows7やFlash Player等のサポートが終了した製品を使用しない。）。
勤務者C-2 基本対策	テレワーク勤務者が所有する無線LANルーター等の機器についても、ファームウェアを最新版に更新する。
勤務者C-3 基本対策	テレワーク端末のうち、特にスマートフォンやタブレットに関して、不正な改造（いわゆる脱獄（jailbreak）、root化等）を実施しない。

＜セキュリティアップデートの実施＞

○　脆弱性が存在しているハードウェアやソフトウェアを使用していると、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、OSをはじめとしたソフトウェア（インターネットブラウザやその拡張機能を含みます。）のアップデートやパッチ適用の定期的な実施を始めとする脆弱性管理の実施が必要です。【管理者C-1、管理者C-2、管理者C-4、勤務者C-1、勤務者C-2】

○　発売されて一定の期間が経過された製品やサービスは、サポートが終了し、セキュリティ対策が行われていないものもあります。こうした製品やサービスでは明らかとなった脆弱性にも対応していない場合があるため、攻撃者の標的にされやすくなることから利用は危険です。【管理者C-3】

＜OS改造の禁止＞

○　テレワークで利用するハードウェアのうち、特にスマートフォンやタブレットについて、OSの改造（Jailbreakやroot化）を実施するとセキュリティ機能が低下したり、不正プログラムへの感染を助長したりすることになるため、必ず禁止することが必要です。【勤務者C-3】

４．特権管理

本節では「特権管理」として、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を示しています。

システム・セキュリティ管理者が実施すべき対策	
管理者D-１ 基本対策	テレワーク勤務者に貸与するテレワーク端末は必要最小限の権限（例：ユーザ権限）を付与する。
管理者D-２ 発展対策	［Windows利用の場合］テレワーク勤務者に付与するテレワーク端末のアカウント権限はActive DirectoryのGPO（Group Policy Object）にて管理し、User権限を適用する。Administrators権限の適用は業務上必要な機能ごと（例：WindowsUpdate等）に行い、Local Admin権限を適用しない。
管理者D-３ 基本対策	テレワークで利用する製品（VPN機器等）やクラウドサービス等に対する管理者権限は、業務上必要な最小限の人にのみ適用し、アクセス経路も限定（IPアドレス制限等）する。
管理者D-４ 基本対策	テレワーク端末の管理者権限や、テレワークで利用する製品（VPN機器等）やクラウドサービス等に対する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。

＜管理者権限の制限＞

○　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であるため、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。したがって、管理者権限の利用者は最低限とし、IPアドレス制限等により限られた環境からしか使えないように設定する等の対策が重要です。【管理者D-１、管理者D-３】

○　管理者権限のパスワードは、一般権限より更に強力なパスワードポリシー（ランダム文字列の利用等）を適用することが必要です。【管理者D-４】

＜Active Directory＞

○　Windowsにおいて、Local管理者やDomain管理者の権限を適用すると、テレワーク端末へのアプリケーションのインストールやアンインストール、Windows Defenderやファイアウォールといったセキュリティに関わる設定が可能です。こうした状況で設定変更が行われてしまうと、セキュリティ侵害のリスクが高まる上、攻撃者も極めて高い権限を有してしまいます。そのため、テレワーク端末で利用するユーザには、User権限を設定して、利用を制限することが必要です。【管理者D-２】

（Local管理者：Administratorsというグループに所属している者。端末を管理できるAdministrators権限を有する。）

（Domain管理者：Domain Adminsというグループに所属している者。Domain内の全ての端末のAdministrators権限を持っており、ドメイン内の全ての端末の管理をする事ができる非常に強力な権限を有する。）

5．データ保護

本節では「データ保護」として、保護すべき情報（データ）の特定や保存されているデータの機密性・可用性の確保に関する対策を示しています。

経営者が実施すべき対策	
経営者E-1 基本対策	業務で取り扱う情報について、情報の柔軟かつ有効な活用による事業上のメリットと、情報漏えい等が発生した場合の事業影響等を総合的に勘案し、情報取扱いに関する重要度の方針を定める。
システム・セキュリティ管理者が実施すべき対策	
管理者E-1 基本対策	経営者が定める情報取扱いに関する重要度の方針に従い、具体的な情報管理レベルを定めるとともに、テレワークでの利用可否と利用可の場合の取扱方法（利用者・保管場所・利用可能なシステム環境の要件等）を整理してテレワーク勤務者に周知する。
管理者E-2 発展対策	取り扱う情報の情報管理レベルに照らして、アクセス可能なテレワーク勤務者やテレワーク端末を制限し（認証を実施し）、必要最小限のアクセス権限を適用する。
管理者E-3 基本対策	テレワークで利用する機密性を有する情報を特定し、保存場所を把握する。
管理者E-4 基本対策	テレワーク勤務者によるリムーバブルメディア（USBメモリ、CD、DVD等）の使用は、業務上の必要性が認められたものに限定し、ルールで規定する。
管理者E-5 基本対策	重要情報のバックアップについては、オフィスネットワーク上の共有フォルダ等のほかに、オフィスネットワークから切り離した環境（ネットワークに接続しない記録媒体やクラウドサービス等）にも保管する等、複数の環境でバックアップを保管する。
管理者E-6 基本対策	テレワーク端末を廃棄する場合は、内蔵されるHDDやSSDについて、データ消去専用ソフトウェアの使用や物理破壊等を行い、データが完全に復元不可能な状態とする。また、テレワーク業務で使用するUSBメモリ等を廃棄する場合も同様に対応する。
管理者E-7 基本対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルで暗号化を実施するようにテレワーク勤務者に周知する。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。
管理者E-8 発展対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルでの暗号化を強制し、テレワーク勤務者で設定を変更できないようにする。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。
管理者E-9 基本対策	テレワーク端末の紛失・盗難に備え、MDM（Mobile Device Management）ソリューション等を導入し、有事の際の遠隔制御でのデータ・アカウント初期化、ログイン時のパスワード認証の強制、ハードディスクの暗号化等の機能を有効化する。
管理者E-10 基本対策	テレワーク端末の紛失時に端末の位置情報を検知するためのアプリケーションやサービス等を導入する。
テレワーク勤務者が実施すべき対策	
勤務者E-1 基本対策	テレワークで取り扱う情報は、定められた取扱方法（利用者・保管場所・利用可能なシステム環境の要件等）に従って取り扱う。
勤務者E-2 基本対策	リムーバブルメディア（USBメモリ、CD、DVD等）は、業務上必要であり、ルールで許可されている場合のみ利用する。
勤務者E-3 基本対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルで暗号化を実施する。

＜情報の分類と取扱方針＞

○　保護すべき情報の分類が明確に規定されていないと、非効率あるいは不十分な対策が実施されることにつながります。このような事態を防ぐために、企業等における情報資産を３つ程度（例えば「機密情報」「業務情報」「公開情報」等）に分類し、

公開してもかまわない情報以外の情報資産についての情報管理レベルや取扱方法を定める必要があります。また、経営者はこれらに関する基本的な方針を定める必要があります。【経営者Ｅ-１、管理者Ｅ-１】

※上記の例において、「機密情報」には、個人情報、顧客から預かった非公開情報、機微情報、営業秘密、企業等の経営に関する重要な情報などが該当します。また、「業務情報」には、「機密情報」には該当しないが、公開を前提としない情報（例：打合せ資料、勤務管理簿、研修教材等）が該当します。

○　機密性を有する情報として個人情報に注目しがちですが、例えば、経営に関する重要な情報（事業運営の根幹となる情報）やオフィスネットワークの特権ID情報等については、個人情報以上に厳重に取り扱うべき場合もあり得ることから、各情報の取扱いに関して、情報漏えい等が発生した場合の事業影響等も勘案し、重要度を定めることが必要です。【経営者Ｅ-１、管理者Ｅ-１】

○　情報の取扱方法は、テレワーク勤務者がわかりやすいように例を示すことが重要です。例えば、テレワーク業務で使用するデータは、テレワーク端末自体ではなくオフィスネットワーク上やクラウドサービス上に保存すること、USBメモリ等に業務データを保存する場合は、記録媒体の暗号化を実施すること等が考えられます。【管理者Ｅ-１】

○　情報の取扱方法は、電磁的情報だけではなく、紙媒体についても定めておく必要があります。例えば、データを自宅等において出力することの可否や、紙文書の持ち出しや電子化における制限等が考えられます。【管理者Ｅ-１】

＜記録媒体の暗号化・廃棄＞

○　テレワークでは、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外部に漏えいするリスクが高まりますが、情報管理レベルが高い情報を直ちに利用できなくするのではなく、システム環境を整えることにより、情報漏えいのリスクを軽減しながら利用することも可能です。例えば、テレワーク端末やUSBメモリ等に業務データを保存する場合は、記録媒体レベルでの暗号化[23]を実施することで、データの窃取及びテレワーク端末等の紛失・盗難を通じた情報漏えいを防止することができます。【管理者Ｅ-４、管理者Ｅ-７、勤務者Ｅ-２】

○　端末管理ツールを導入し、テレワーク端末やUSBメモリ等の記録媒体の自動暗号化を行ったり、文書管理システムや暗号化ソリューションを利用してファイルを強制的に暗号化して保存したりすることで、テレワーク勤務者が意図的に設定を変更できないようにすることも重要です。【管理者Ｅ-８】

○　テレワーク端末等の廃棄が適切でないと、悪意ある第三者にテレワーク端末上の情報が窃取されるおそれがあります。これを防ぐために、適切な手順でテレワーク端末等の廃棄を実施することが重要です。なお、通常のフォーマットや初期化をしただけでは、専門技術により復元可能であることに注意してください。【管理者Ｅ-６、勤務者Ｅ-３】

[23] EFS（Encrypting File System）等によりフォルダ等の単位で自動暗号化を行い、正当な権限のない者が復号できないようにする方式も含みます。

＜バックアップの保管＞

○　端末の盗難や故障等によって、重要なデータが使用できなくなり、業務の継続が困難になる可能性があります。このような事態を防ぐために、オフィスネットワーク上の共有フォルダ等にバックアップを保管しておくことが重要です。また、ランサムウェアの感染等のリスクに備えるため、ネットワークに接続しない記録媒体やクラウドサービス等にも保管するなど、複数の環境にバックアップを保管しておくことが重要です。【管理者Ｅ-５】

＜MDMの導入＞

○　テレワーク端末を紛失した際に、悪意のある第三者に拾われデータが漏えいすることを防ぐため、遠隔から端末の位置情報を把握し、テレワーク端末上のデータ等を削除したり、端末を初期化したりできるようにしておくことが重要です。例えば、スマートフォンでは、通信キャリアが提供しているMDMソリューションを利用することで、遠隔から端末を初期化することが可能です。【管理者Ｅ-９、管理者Ｅ-10】

6．マルウェア対策

本節では「マルウェア対策」として、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を示しています。

システム・セキュリティ管理者が実施すべき対策	
管理者Ｆ-１ 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
管理者Ｆ-２ 基本対策	セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能等を用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
管理者Ｆ-３ 発展対策	テレワーク端末にEDR（Endpoint Detection and Response）ソリューションを導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。
管理者Ｆ-４ 発展対策	テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるようにする。
テレワーク勤務者が実施すべき対策	
勤務者Ｆ-１ 基本対策	少しでも不審を感じたメール（添付ファイルやURLリンク等を含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
勤務者Ｆ-２ 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。

＜セキュリティ対策ソフト等の導入＞

○　テレワークにおいては、インターネットを利用する場合が多く、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、セキュリティ対策ソフト（ウイルス対策ソフト）を導入し、適切な設定のもと運用していくことが重要です。また、危険なWebサイト等へのアクセスを禁止するフィルタリングについても同様に実施することが需要です。【管理者Ｆ-１、管理者Ｆ-２、勤務者Ｆ-２】

○　セキュリティ対策ソフト（ウイルス対策ソフト）は、定義ファイルが自動更新されるように設定することが必要です。また、フィルタリングソフトについても、定期的にフィルタリングするサイトを更新することが必要です。【管理者Ｆ-１、管理者Ｆ-２、勤務者Ｆ-２】

＜EDRの導入＞

○　テレワーク端末において攻撃検知と対応を適切に行うためのセキュリティ対策製品として、EDR（Endpoint Detection and Response）の導入も有効な対策の一つです。EDRを導入することで、未知のマルウェアを含めた不審な挙動の検知や、検知した情報に基づく迅速な対応が可能になります。【管理者Ｆ-３】

＜一元管理機能の導入＞

○　マルウェア対策は、１人でも定義ファイルの更新を怠るとマルウェアに感染するリスクが高まるため、複数台の端末を一元管理して、定義ファイルの更新漏れを回避することが重要です。【管理者Ｆ-４】

【コラム】次世代セキュリティ対策ソフト（EDR）

背景

近年、特定の企業等に対して、長期間にわたり攻撃を継続的に実施する標的型攻撃という攻撃手法が増加傾向にあります。この標的型攻撃に用いられるマルウェアは、標準的なセキュリティ対策ソフト（ウイルス対策ソフト）では検出されないものも多い状況です。

これは、従来型の攻撃と異なり、攻撃者がマルウェアを広範囲に拡散させようとせず、攻撃対象に絞った狭い範囲に、新種のマルウェアを用いて攻撃を行うためです。これにより、セキュリティ対策ソフトのベンダーが、そもそもマルウェアを入手することが難しくなり、結果的に検出用の定義ファイルを準備できないことになります。

セキュリティ対策ソフトが検知しないという状況は、そもそもマルウェアに感染しているということを把握できないということになり、侵入防御策を展開していくことが難しい状況です。

次世代セキュリティ対策ソフト（EDR）

こうした状況に対応するため、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにするEDR（Endpoint Detection and Response）という防御手法が注目されています。

これは、従来のように、既知のマルウェアの特徴をパターンファイルとして保持し、そのパターンとの一致状況をもって検知を行うという仕組みではありません。EDRでは、PC等において動作するOSやアプリケーションの挙動を監視し、その挙動をもとにマルウェアに似た挙動（悪意のある攻撃を示す異常な挙動や活動の兆候）を検知します。そのため、未知のマルウェアに対しても有効です。また、EDRではマルウェア感染後の対応（マルウェアの隔離やシステム停止、被害拡大防止や検証・復旧作業等[24]）の迅速化にも有効です。

対策の重要性

不特定多数から送信される電子メールや海外から送られてくる電子メールについて添付ファイルを確認しなければならないなど、比較的リスクの高い業務に用いる端末や、重要な情報を取り扱う端末については、EDRのようなセキュリティ対策ソフトを導入することで、対策の多重化を図ることが考えられます。

セキュリティインシデントの兆候を検知し未然に発生を防ぐことは重要ですが、サイバー攻撃が高度化している現在、全ての攻撃を完全に防御することは困難となってきています。そのため、セキュリティインシデントが発生する前提での対策がより重要となってきます。

[24] EDRの導入に当たっては、必要とする機能への対応を確認するようにしてください。また、その際には、取得・分析しようとするログ（OSの動作やそれによって発生するファイル操作やレジストリ変更等）について確認することも有効です。

7．通信の保護・暗号化

本節では「通信の保護・暗号化」として、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を示しています。

システム・セキュリティ管理者が実施すべき対策	
管理者G-1 基本対策	クラウドサービス接続時やデータ送受信を行う際は、通信経路が暗号化された方法（VPN、TLS等）を利用するようテレワーク勤務者に周知する。また、暗号化に際しては危殆化していない暗号アルゴリズム（CRYPTRECを参照するとよい。）が使用されるようにする。
管理者G-2 発展対策	利用者同士が通信を行うサービスについては、通信相手までの間（E2E：エンドツーエンド）で常時暗号化に対応しているもののみ利用を許可する。
管理者G-3 基本対策	テレワーク勤務者が無線LANルーター等の機器を利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用し、暗号化のためのパスワード（パスフレーズ）は第三者に推測されにくいものを利用するようテレワーク勤務者に周知する。また、無線LANルーター等の管理者パスワード（設定変更のログイン画面等で必要となるパスワード）についても、第三者に推測されにくいものとすることを併せて周知する。
管理者G-4 発展対策	オフィスネットワークに接続してテレワークを実施する場合、テレワーク勤務者の最大同時接続数を見込み、その処理が可能な製品やサービスを選定するとともに、必要となる回線帯域やソフトウェアライセンス等を確保する。
テレワーク勤務者が実施すべき対策	
勤務者G-1 基本対策	クラウドサービス接続時やデータ送受信を行う際は、通信経路が暗号化された方法（VPN、TLS等）を利用する。
勤務者G-2 基本対策	無線LANルーター等の機器を利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用し、暗号化のためのパスワード（パスフレーズ）は第三者に推測されにくいものを利用する。
勤務者G-3 基本対策	クラウドサービス（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、接続先のURLが正しいこと（偽サイトでないこと）を確認した上で利用する。

＜暗号化の必要性＞

○　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。【管理者G-1、勤務者G-1】

○　特に電子メールについては、メールサーバとクライアント（端末）との間の通信プロトコルとして以前に一般的に用いられていたもの（POP、SMTP、IMAP等）は暗号化されていないため、暗号化されたプロトコル（POP over TLS、SMTP over TLS、IMAP over TLS等）を使う必要があります[25]。【管理者G-1、勤務者G-1】

○　暗号化には様々なアルゴリズム（暗号化方法）がありますが、簡単な解読方法が見つかるなどして十分な安全性を保てなくなった（危殆化した）アルゴリズムを使い続けることは危険です。適切な暗号アルゴリズムの選定等については、CRYPTREC（https://www.cryptrec.go.jp/）の「CRYPTREC暗号リスト」や各種ガイドライン[26]

[25] なお、メールサーバ間の通信についても、同様に暗号化されていない場合があるため、暗号化が可能なものを検討することが効果的です。また、電子メールをS/MIME等の暗号化及び電子署名の技術を利用して保護することも電子メールの盗聴及び改ざんを防止する観点から効果的ですが、この場合は相手側もS/MIMEに対応している必要があることに留意する必要があります。

[26] 例えば、Webサイトに利用するTLS（現在SSLは推奨されていません。）については、「TLS暗号設定ガイドライン」をCRYPTRECが発行し、その参考資料として設定参考ガイド等をIPAが公開しています。

を参考にするようにしましょう。【管理者G-１】

○　利用者同士が通信を行うサービス（チャットサービス、オンライン会議サービス等）については、https（TLS）で暗号化した通信をしているように見えても、実際に暗号化されているのは自分の端末からサービス提供事業者のサーバまでの間に限られ、サービス提供事業者のシステム上で一度暗号化が解除された状態になっている場合もあります。機密性の高い情報を取り扱う場合等は、自分の端末から通信相手までの間（E2E：エンドツーエンド）での暗号化が担保されたサービス[27]を利用することで、サービス提供事業者にも通信内容が把握できないようにすることが可能です。【管理者G-２】

＜無線LANのセキュリティ確保＞

○　無線LAN使用時のセキュリティ確保については、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
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
を参考にしてください。【管理者G-３、勤務者G-２】

＜偽サイトへの誘導回避＞

○　クラウドサービスを真似た偽サイト等へのアクセスを防止するため、例えば、オンライン会議の案内送付元のメールアドレスや案内されたオンライン会議のURLが正しいことを確認した上で利用することが必要です。【勤務者G-３】

＜可用性の確保＞

○　多数のテレワーク勤務者が一斉にテレワークを使用する場合、VPN等の同時接続数が不足し、オフィスネットワークにアクセスできないことのないように可用性を確保することが必要です。特に、業務上、同時アクセスが集中する時間帯や、一時的に大量のデータが流れるアプリケーションの利用等を考慮した設計や有事の際の回避策を検討することが必要です。【管理者G-４】

---

https://www.cryptrec.go.jp/op_guidelines.html
https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

[27] 米国国家安全保障局（NSA）において、一部のクラウドサービスのE2E暗号への対応状況をまとめた資料を公表しています。
https://media.defense.gov/2020/Aug/14/2002477667/-1/-1/0/CSI_%20SELECTING_AND_USING_COLLABORATION_SERVICES_SECURELY_FULL_20200814.PDF

【コラム】ファイルの暗号化（PPAP方式）

機密性のあるファイルを相手方に送る場合に、暗号化ファイル（パスワード付きZipファイル）を作成し、その暗号化ファイルをメールで送付した後、パスワードもメールで送付する方式（いわゆるPPAP方式）が一部で用いられています。

しかしながら、この方式では（暗号化ファイルとパスワードを別メールで送信したとしても）、メールに添付された暗号化ファイルを通信経路上で窃取可能な攻撃者は、パスワードを記載したメールも窃取可能であると推測されることから、通信経路上での情報窃取に対するセキュリティ対策としての効果が疑問視されています。なお、これは暗号化ファイルを使わず、ファイル共有サービスを使い、そのURLとパスワードを同じ通信経路（メール）で送る場合についても同様です。

また、暗号化されたファイルに対しては、メールサーバや端末におけるセキュリティ対策ソフト（ウイルス対策ソフト）によって中身のファイルの検知ができないため、セキュリティ対策上デメリットが生じるという点にも留意が必要です。

ファイルを安全に送付するには、パスワードをあらかじめ取り決めた上で暗号化する方法のほか、クラウドストレージ等のファイル共有サービス（当該サービスへのアクセスに当たって認証を行うものや別経路でパスワード送付を行うもの）を活用する方法等が考えられます。求められる機密性やリスク等を考慮の上、適切な手法を利用することが必要です。

8．アカウント・認証管理

本節では「アカウント・認証管理」として、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を示しています。

システム・セキュリティ管理者が実施すべき対策	
管理者H-1 基本対策	テレワーク時にアクセスする社内システムやクラウドサービスへのアクセスで必要となる利用者認証機能について、技術的な基準（多要素認証方式の利用、パスワードポリシーの規定等）を明確に定める。
管理者H-2 基本対策	社内システムやクラウドサービスへのアクセス時の利用者認証機能として、可能な限り多要素認証を強制する。
管理者H-3 基本対策	テレワーク端末がオフィスネットワークやクラウドサービスに接続する際は、接続先のサーバの正当性（サーバ証明書等）と、接続元のテレワーク端末の正当性（パスワードやクライアント証明書）を相互に認証する仕組みを備えたものとする。
管理者H-4 基本対策	テレワーク端末へのログインパスワードや、オフィスネットワークやクラウドサービスにアクセスする際のパスワードは、強力なパスワードポリシーの適用を強制する。
管理者H-5 基本対策	テレワーク端末やアプリケーションの初期パスワードが強制的に変更されるか、十分な強度のある個別のパスワードが個々に設定されるようにする。
管理者H-6 基本対策	利用者認証に一定回数失敗した場合、テレワーク端末の一定時間ロックや、テレワーク端末上のデータ消去を行うよう設定する。
管理者H-7 基本対策	異動や担当変更等を適切に把握し、不要なアカウントの削除やアカウント権限の更新等を実施する。
テレワーク勤務者が実施すべき対策	
勤務者H-1 基本対策	テレワークに必要となる利用者認証情報（パスワード、ICカード等）を無断貸与や紛失等しないよう、適正に管理する。
勤務者H-2 基本対策	パスワードは、第三者に推測されにくいものを設定する。多くの文字数を設定できる場合は、複数の単語を組み合わせるなどして文字数が長いもの（パスフレーズ）を設定する。
勤務者H-3 基本対策	複数のサービス間で同じパスワード使い回さない。また、使用するパスワードが第三者に知られた可能性がある場合は、早急にパスワードを変更する。

＜適切な管理ルールの設定＞

○　インターネット上から業務上必要な情報にアクセスできるテレワークのシステムは、不正アクセスの方法として攻撃者に狙われやすいといえます。したがって、テレワーク勤務者がオフィスネットワーク上のシステムやクラウドサービスに接続するための利用者認証について、多要素認証方式や電子証明書の利用等の技術的基準やパスワードポリシー（長いパスフレーズの利用、使いまわしの禁止等）を明確に定め、適正に管理・運用することが必要です。【管理者H-１、管理者H-４】

○　不正アクセスの試行が行われうることを前提として、利用者認証に一定回数失敗した場合の技術的対応を定めるとともに、異動や担当者変更等に際して権限がなくなるべき者に権限が残ったままにならないよう運用する必要があります。【管理者H-６、管理者H-７】

＜パスワードの設定＞

○　パスワードに第三者が推測しにくいものを設定する必要があります。名前や辞書に載っているような単語を少し変えただけのようなパスワードでは、突破されてし

まうと考えましょう。パスワードの文字数制限が緩い場合は、パスフレーズ（コラム参照）を設定することも有効です。【管理者H-４、管理者H-５、勤務者H-２】

○　パスワードを使い回していると、サービス提供事業者側がサイバー攻撃を受けるなどしてパスワードが流出してしまった場合に、同じパスワードを利用している全てのサービスが不正アクセスを受けかねない状態になります。パスワードの使い回しはやめ、サービスごとに異なるものを設定する必要があります。【勤務者H-３】

○　パスワードの定期的な変更を強制することで、第三者に推測されやすい規則性をもったパスワードを設定する例（例えば特定のキーワードの後に年月を６桁の数字で入れる等）が発生したり、変更を繰り返すことで利用者自身が管理しきれなくなったりするため、パスワードの定期変更は原則不要です。ただし、パスワードが第三者に知られてしまうかそのおそれがあるときや、共有アカウント等を利用している場合であって利用メンバーに変更があったとき等は速やかに変更するようにしましょう。【管理者H-７、勤務者H-３】

＜多要素認証＞

○　クラウドサービスは、その特性上、不特定多数の利用者がアクセス可能であり、利用手順も周知であるため、クラウドサービスの利用者認証情報（ユーザIDやパスワード）が流出した場合に不正アクセスを受けやすいといえます。そのため、可能な限り多要素認証を利用するなどして、利用者認証情報が漏洩しても、ただちに不正アクセスを受けないようにする対策が必要です。また、社内システムへの接続についても、接続時の利用者情報が流出した事例等が報告されていることから、同様に、可能な限り多要素認証を利用することが求められます。【管理者H-２】

＜相互認証＞

○　パスワードといった利用者認証情報は、提供者側（接続先）から見て利用者が正しい利用者であるかを確認するためのものですが、偽サイト・偽サービスへの誤誘導を回避するためには、利用者側（接続元）から見て提供者が正しい提供者であるかを確認（アクセスしようとする先が本来のアクセス先であるか確認）するため、相互認証を行うことが必要です。【管理者H-３】

【コラム】ID・パスワードをインターネットブラウザに記憶させても大丈夫？

インターネットブラウザの中には、ID・パスワードを記憶（保存）させる機能を持つものがあります。これは、入力の負担を軽減することができる便利な機能です。

一方、セキュリティ上のリスクも認識しておく必要があります。ブラウザにID・パスワードを記憶すると、その情報は端末のハードディスクに保存されます。この端末がマルウェア等に感染したり、脆弱性をつかれて攻撃を受けたりしてしまうと、ハードディスクに保存されたID・パスワードが漏えいする可能性があります。

重要なサービスのID・パスワードはブラウザに記憶させずに、面倒でも自ら入力することが奨励されます。

【コラム】パスワードの管理方法

異なるサービス間でパスワードを使いまわすことは望ましくありませんが、サービスごとに異なるパスワードを設定していくうちに、パスワード管理の負担が増えてしまいます。そのため、負担を軽減する管理方法をいくつかご紹介します。

マスターパスワードの活用[28]

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。

パスワードマネージャー

Webサイトやクラウドサービスにログインする際のパスワードを管理するためのツールにパスワードマネージャーがあります。パスワードマネージャーでは、パスワードの自動生成やパスワードの一元管理等が可能です。パスワードマネージャー側でアカウント情報を暗号化して管理をしてくれるため、パスワードマネージャーを起動させる際のIDとパスワードのみを覚えておけば、その他のサービスのアカウント情報を全て覚えておく必要がなくなります。

ただし、パスワードマネージャーの信頼性に注意するとともに、重要なサービスのID・パスワードは記憶させないことも必要です。

[28] マスターパスワードについては、共通の文字列部分や、他のサービスで使用しているパスワードが漏えいした場合に、ブルートフォース攻撃（総当たり攻撃）により設定したパスワードを特定されるリスクがあります。また、本来、パスワード認証は本人だけが知っている知識認証であるため、パスワードの一部であっても他者が知りうるメモという形で保管することは好ましくありません。一方で、あまり重要度の高くないサービスへのログイン認証等において、セキュリティ上のリスクを認識した上で、利便性とのバランスを鑑みた方法として、有効な手法の一つであることから、本コラムで紹介しています。

9．アクセス制御・認可

本節では「アクセス制御・認可」として、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を示しています。

システム・セキュリティ管理者が実施すべき対策	
管理者Ⅰ-1 基本対策	テレワーク端末においてファイアウォール（パーソナルファイアウォール）を有効にし、適切な設定を施す。
管理者Ⅰ-2 基本対策	オフィスネットワークやクラウドサービス等への接続について、接続IPアドレスの制限や、不要ポートの閉鎖を行い、インターネットへの露出を最小限とする。
管理者Ⅰ-3 基本対策	データに対するアクセス制御に際して、オフィスネットワーク上の共有フォルダやクラウドサービスに対するアクセス権限設定、ファイアウォール設定等により、機密情報を閲覧・編集する必要のないテレワーク端末やテレワーク勤務者からのアクセスを制御する。
管理者Ⅰ-4 発展対策	データに対するアクセス制御に際して、テレワーク勤務者の職務や役割、テレワーク端末の種類やそのセキュリティ対策状況を考慮した動的なアクセス制御を実装する。
管理者Ⅰ-5 発展対策	テレワーク勤務者がオフィスネットワークを介さずインターネットに接続を実施することができる構成（ローカルブレイクアウト等）を採るときは、クラウドプロキシによる認証とアクセス制御を実施する。
管理者Ⅰ-6 発展対策	オフィスネットワークとインターネットとの通信において、不審なアクセス状況がないか監視する。
管理者Ⅰ-7 基本対策	オンライン会議にアクセスするためのURLを正規の参加者以外に公開せず、出席者の確認をするなどして、第三者が会議に参加することのないよう、テレワーク勤務者に周知する。また、会議参加時のパスワード設定や、待機室機能が有効化できる場合には、可能な限り設定するよう併せて周知する。
テレワーク勤務者が実施すべき対策	
勤務者Ⅰ-1 基本対策	オフィスネットワークやクラウドサービスへの接続は、システム・セキュリティ管理者が指定した方法とし、許可なく設定等を変更しない。
勤務者Ⅰ-2 基本対策	テレワーク端末において業務上必要のない無線機能（例：Bluetooth機能、アドホックモード等）は無効化する。
勤務者Ⅰ-3 基本対策	複数人でデータを共有可能な場所（オフィスネットワーク上の共有フォルダ、ファイル共有サービス等）に機密情報を保存する場合、情報を閲覧・編集する権限が誰にあるか確認し、適切な設定を実施（テレワーク勤務者で設定できない場合はシステム・セキュリティ管理者に相談）する。
勤務者Ⅰ-4 基本対策	オンライン会議にアクセスするためのURLを正規の参加者以外に公開せず、出席者の確認をするなどして、第三者が会議に参加することのないようにする。また、会議参加時のパスワード設定や、待機室機能が有効化できる場合には、可能な限り設定する。

＜必要最小限のアクセス開放・アクセス権限＞

○　不正アクセスを防止するために、ファイアウォールによるアクセス制御、接続IPアドレス制限、不要ポート閉鎖等の、ネットワークにおけるセキュリティ対策を徹底することが有効です。【管理者Ⅰ-1、管理者Ⅰ-2】

○　また、制限をかいく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。【管理者Ⅰ-6】

○　業務に必要ないBluetooth機能、アドホックモード等の無線接続が有効になっていると、本来意図していない第三者による不正アクセスが行われる可能性があります。したがって、このような不要な無線接続が実施されないよう対策を実施するこ

とが重要です。【勤務者Ⅰ-２】

○　保存されている機密情報について、閲覧・編集権限を与えるべき対象を明確にし、権限の必要ないテレワーク端末やテレワーク勤務者からのアクセスを制御することが重要です。また、継続的にアクセス権限設定等の見直し（点検）を行うとともに、クラウドサービスのサービス内容変更がないか、設定誤りがないか、不必要になった権限が放置されていないか等を確認することも重要です。【管理者Ⅰ-３、勤務者Ⅰ-３】

＜オンライン会議システム＞

○　テレワーク環境におけるオンライン会議システムの使用が増えていますが、セキュリティ対策が不十分な状態でオンライン会議を実施すると、情報漏えいをはじめとするリスクが顕在化する可能性があります。そのため、会議参加者の本人確認の実施をはじめ、会議パスワード設定、待機室（ロビー）での参加者確認、参加者の事前登録、参加者名の設定、二要素認証等の各種対策の徹底が重要です。【管理者Ⅰ-７、勤務者Ⅰ-４】

＜データに対する動的なアクセス制御＞

○　セキュリティ対策が十分に実施されていないテレワーク端末がオフィスネットワーク内のデータにアクセス可能になっていると、その端末を起点にして情報漏えいが発生する可能性があります。したがって、テレワーク勤務者の職務権限やテレワーク端末のセキュリティ対策状況を考慮し、リスクに応じて動的にアクセスをコントロールできるようなデータに対するアクセス基準を検討し、適切な製品やサービスを導入してその基準を実現することが必要です。【管理者Ⅰ-４】

＜ローカルブレイクアウトの考慮＞

○　テレワーク勤務者がオフィスネットワークやクラウドサービスにアクセスする際に、インターネットへのアクセスに関してのみオフィスネットワークを介さず直接接続を行うローカルブレイクアウトは、通信帯域の分散化の観点から有効です。一方で、全てのインターネット上のWebサイトに直接アクセスできる状態になるため、オフィスネットワーク内で不審サイトをプロキシで検知していた場合等は、その恩恵に預かれなくなることから、データの情報漏えいやマルウェア感染等のリスクが高まります。そのため、クラウドプロキシを導入する等の適切なセキュリティ対策を実施することが必要です。【管理者Ⅰ-５】

10. インシデント対応・ログ管理

本節では「インシデント対応・ログ管理」として、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を示しています。

経営者が実施すべき対策	
経営者Ｊ-１ 基本対策	セキュリティインシデント発生時に迅速な対応を可能とするため、事業影響レベルを考慮した対応体制と対応優先度を明確としたインシデント対応計画を策定する（システム・セキュリティ管理者に指示する。）。
システム・セキュリティ管理者が実施すべき対策	
管理者Ｊ-１ 基本対策	オフィスネットワークやクラウドサービスの接続に問題が生じた場合や、テレワーク端末に不具合が生じた場合のほか、セキュリティインシデントが疑われる場合に、テレワーク勤務者が対応や連絡を適切に実施できるよう、対応手順や連絡窓口（電話番号を含む。）を整備する。なお、テレワーク勤務者にとって、セキュリティインシデントが不具合と認識される場合があることに留意する。
管理者Ｊ-２ 基本対策	セキュリティインシデントの発生に備えて、迅速な対応がとれるよう、インシデント対応計画をあらかじめ策定するほか、自組織内に加え顧客、取引先、監督官庁等に対する連絡体制を整備する。
管理者Ｊ-３ 基本対策	セキュリティインシデントが発生した場合、事故発生の原因を分析し、再発防止（必要に応じて追加のセキュリティ対策）に努める。
管理者Ｊ-４ 発展対策	セキュリティインシデントの発生に備え、発生を想定した訓練（予行演習）を年１回程度実施する。また、訓練結果を踏まえ、インシデント対応計画等の見直しを行う。
管理者Ｊ-５ 基本対策	不正アクセス等のセキュリティインシデントが発生した際に原因調査が可能となるよう、オフィスネットワーク内に設置されたテレワーク関連機器（VPN装置やVDI機器等）へのアクセスログ、テレワーク関連機器やクラウドサービスにログインした後の認証ログや操作ログ、テレワーク端末の操作ログやイベントログ等）について、ログを取得する。
管理者Ｊ-６ 基本対策	取得したログについて、保存容量を十分に確保する。過去に遡った調査も必要になることがあるため、可能な限り１年以上保存可能とする。
管理者Ｊ-７ 基本対策	テレワーク端末のほか、オフィスネットワーク内の各機器やクラウドサービス上のシステムの時刻が正しく設定（同期）されるように設定する。
管理者Ｊ-８ 発展対策	取得ログの検索を容易にするとともに、不正アクセス時のログ改ざんを防止するため、Syslog等を活用し、ログ保存・管理用のサーバを設置する。
管理者Ｊ-９ 発展対策	管理者権限の使用状況や、重要情報へのアクセス履歴については、平時から定期的にログの確認を実施する。
管理者Ｊ-10 発展対策	不審なログが記録された際に、自動的にアラートが通知されるようにする。
テレワーク勤務者が実施すべき対策	
勤務者Ｊ-１ 基本対策	セキュリティインシデントの発生に備えて、連絡先と対応手順をあらかじめ確認しておく。テレワーク端末が操作不能になることも考えられることから、連絡先は電話番号等も確認するようにしておく。
勤務者Ｊ-２ 基本対策	テレワーク端末の紛失やマルウェア感染等のセキュリティインシデントが発生した場合（発生のおそれがある場合を含む。）定められた連絡先へ速やかに報告する。動作が不審であるなど、セキュリティインシデントかどうかわからない場合も速やかに報告する。

＜セキュリティインシデントへの迅速な対応＞

○　セキュリティインシデント発生時に迅速かつ的確な対応を実施するためには、平時のうちにインシデント対応計画や各種手順を整備しておくことが重要です。【経営者Ｊ-１、管理者Ｊ-２】

○　セキュリティインシデントが発生した場合や発生のおそれがある場合に、適切な初動対応ができるよう、最低限実施すべきことを記録したチェックリストや、組織内外における緊急連絡先・伝達ルートを整備して、常時携帯して確認できる状態にしておくことが必要です。【管理者Ｊ-１、勤務者Ｊ-１】

○　セキュリティインシデントの疑いが少しでもあればためらわず連絡するよう、テレワーク勤務者へ十分周知し、ハードルを下げることが重要です。【勤務者Ｊ-２】

＜セキュリティインシデント収束後の対応＞

○　セキュリティインシデントは、マルウェア駆除やシステム復旧といった対応だけで終わらせず、再発防止のため、事故原因を丁寧に分析することが重要です。技術的に防止できる点があれば追加のセキュリティ対策を実施したり、運用に問題があればルールの周知徹底やルール改善を実施したりすることまで行い、セキュリティインシデントを契機にPDCAサイクルを回すようにしましょう。【管理者Ｊ-３】

＜インシデント対応訓練の実施＞

○　インシデント対応計画等の適切性を確認するために、定期的に訓練（予行演習）を実施することが効果的です。また、訓練の結果、必要に応じてインシデント対応計画等を見直すことが必要です。【管理者Ｊ-４】

＜ログの取得・保存＞

○　セキュリティインシデント発生時の原因分析に、ログは必須となるため、次のような各種ログを取得・保存しておくことが重要です。【管理者Ｊ-５】
- ・アクセスログ（サーバや機器へ誰がいつアクセスしたかという履歴）
- ・認証ログ（各システムやアプリケーションへのログイン試行履歴）
- ・操作ログ（利用者の操作内容履歴）
- ・イベントログ（システム上の重要な（又は異常な）事象の発生履歴）
- ・特権ログ（管理者権限等の特権IDに関する各種ログ）

○　実際のサイバー攻撃（標的型攻撃等）では、最初の攻撃から認知まで１年近くを要する場合もあることから、原因究明を適切に行うため、ログは十分な期間保存しておくことが必要です。また、Syslogサーバ等を活用することで、効率的なログの保管・管理が可能となります。【管理者Ｊ-６、管理者Ｊ-８】

○　機器等の時刻が正確でなく、結果としてログに記載された時刻が正確でないと、セキュリティインシデントの原因調査に支障を来します。NTP[29]サーバと時刻同期をさせるなど、常に正しい時刻が設定されていることが重要です。【管理者Ｊ-７】

＜ログの確認＞

○　ログの効率的な確認のためには、攻撃者の探索活動を検知するため、アクセスログのうち拒否ログや、管理者権限等の特権IDに対するログイン失敗の履歴を定期的に確認することが効果的です。【管理者Ｊ-９】

○　特権IDの利用や重要情報へのアクセス、エンドポイント上で不審な挙動、通常発生しない宛先への通信等、予め検知するログや条件を定義するとともに、アラート通知時の調査手順を整備しておくことが必要です。【管理者Ｊ-10】

[29] Network Time Protocolの略。サーバや端末等の各種機器の時刻同期に用いられるプロトコル。

11. 物理的セキュリティ

本節では「物理的セキュリティ」として、物理的な手段による情報漏えい等からの保護に関する対策を示しています。

テレワーク勤務者が実施すべき対策	
勤務者K-1 基本対策	操作画面の自動ロック設定やプライバシーフィルターの貼付等を行うほか、周囲にいる組織外の人の挙動に注意を払う。自宅等で家族がいる場合についても、不注意により意図せず情報漏えい等が起きる可能性があるため注意する。
勤務者K-2 基本対策	オンライン会議を実施するときは、音漏れや画面を介した情報漏洩が起きないよう注意する。オフィス内であっても、同じ場所で複数人が別のオンライン会議を実施等する場合の音漏れに注意する。

＜周囲環境への注意＞

○　テレワークは自宅以外にも、サテライトオフィスやカフェ等の場で実施することが考えられ、このような多数の人々が出入りする場所でテレワークを実施する場合は、のぞき見等により情報漏えいが起きないよう注意しましょう。また、そもそも外出先で業務や自組織に関する情報を話さないようにする等、第三者の関心をひかないよう注意を払いながら業務を実施することが重要です。【勤務者K-1】

○　テレワークを自宅で実施する場合でも、離席中に子どもが意図せず操作したり、家族が撮影した室内写真に情報が写り込んだりすることも考えられることから、十分に注意しましょう。【勤務者K-1】

＜オンライン会議での声や画面＞

○　オンライン会議では、機密性のある情報を扱う場合、自分が発する音声、相手の音声ともに、周囲の第三者に漏れ聞こえないように注意しましょう。オフィス内であっても、同じ場所で複数人が別のオンライン会議を実施している場合や、オンライン会議場所の周囲で通常業務を実施している場合は、オンライン会議に音声が入り込み、意図せぬ情報漏えいにつながらないよう注意しましょう。【勤務者K-2】

○　オンライン会議で、画面共有機能を使用する際に、デスクトップ等が意図せず共有されないよう注意するとともに、共有されても問題ないようデスクトップや起動するアプリケーションは整理しておきましょう。また、画面の撮影・録画について注意しましょう。機能的にスクリーンショット撮影や録画を制限していたとしても、スマートフォンのカメラ等で撮影されることまでは制限できません。そのため、対面の場合と異なり、一時的に提示した情報が撮影・録画されるリスクがあることを念頭に入れ、共有しても問題ない情報に留めることも検討する必要があります。【勤務者K-2】

12. 脅威インテリジェンス

本節では「脅威インテリジェンス」として、脅威動向、攻撃手法、脆弱性等に関する情報の収集に関する対策を示しています。

システム・セキュリティ管理者が実施すべき対策	
管理者Ｌ-１ 基本対策	セキュリティ関連機関（JPCERT/CC、IPA、NISC等）からセキュリティに関する最新の脅威動向・脆弱性情報を収集する。
管理者Ｌ-２ 発展対策	最新の脅威動向・脆弱性情報を把握するために、業界団体や地域のセキュリティコミュニティに加入する。なお、関連するISAC（Information Sharing and Analysis Center）がある場合は、可能な限り加入するようにする。

＜脅威動向・脆弱性情報の収集＞

○　セキュリティに関する脅威動向・脆弱性情報は日々変化しているため、定期的に収集し、自組織のセキュリティ対策に反映していくことが重要です。情報の入手先としては、JPCERT/CC（一般社団法人JPCERTコーディネーションセンター）、IPA（独立行政法人情報処理推進機構）、NISC（内閣官房内閣サイバーセキュリティセンター）等、セキュリティに関する情報発信を定常的に実施している組織が挙げられます。【管理者Ｌ-１】

＜セキュリティコミュニティへの所属＞

○　業界団体や地域のセキュリティコミュニティに加入し、コミュニティ内で相互に情報共有を実施することで、より実際に近い最新の脅威動向・脆弱性情報が把握できます。また、セキュリティ担当者同士の人間関係等が構築されることで、何かあった場合の相談相手ができることも、コミュニティに所属するメリットとなります。【管理者Ｌ-２】

○　自組織が属する業界に関連するISAC（Information Sharing and Analysis Center）がある場合はこれに加入することで、業界に特化した脅威動向等を入手することも有効です。【管理者Ｌ-２】

13. 教育

本節では「教育」として、テレワーク勤務者のセキュリティへの理解と意識の向上に関する対策を示しています。

経営者が実施すべき対策	
経営者M-１ 基本対策	組織全体でセキュリティへの理解と意識の向上を図るため、セキュリティ研修を実施する（システム・セキュリティ管理者に指示する。）とともに、テレワーク勤務者に対して研修の受講を呼びかける。
システム・セキュリティ管理者が実施すべき対策	
管理者M-１ 基本対策	テレワーク勤務者のセキュリティへの理解と意識の向上を図るために、定期的に研修等を実施する。また、テレワーク勤務者に対して最低限求めるセキュリティ対策を定め、テレワーク勤務者に周知する。
管理者M-２ 基本対策	不審メール情報や緊急アップデートの適用等、重要なセキュリティ情報については、組織内のポータルサイトへの掲載、テレワーク勤務者への一斉メールによるアナウンス等、テレワーク勤務者の目にとまりやすい方法で注意喚起を実施する。
管理者M-３ 基本対策	テレワーク勤務者が自ら実施するセキュリティ対策が適切かどうかを確認する機会を年１回程度設け、その結果を把握する。
テレワーク勤務者が実施すべき対策	
勤務者M-１ 基本対策	セキュリティに関する研修等を受講し、セキュリティに対する認識を高めるとともに、自らが実施しているセキュリティ対策を確認する。

＜研修等の実施＞

○　テレワーク勤務者のセキュリティへの理解と意識向上を図るには、研修等によるセキュリティ教育を定期的に実施することが欠かせません[30]。【経営者M-１、管理者M-１、勤務者M-１】

○　テレワーク環境では、テレワーク勤務者が定められたルールを守っているかどうかをシステム・セキュリティ管理者が確認することは容易ではありません。テレワークにおける機密保持と違反時の対応をルール化するとともに、研修等においてルール遵守のメリットを理解してもらうようにします。【経営者M-１、管理者M-１】

＜セキュリティ情報に関する注意喚起＞

○　教育・啓発活動は一過性のものではなく、日々の継続した活動が重要です。例えば、自組織内向けのポータルサイトのトップページでお知らせしたり、チャットツールやメールで通知したりすること等により、セキュリティ情報を意識させることが効果的です。また、重要な情報とそうでない情報を区分して通知することで、重要な情報が埋もれてしまわないよう注意することも必要です。【管理者M-２】

＜セキュリティ対策状況の確認＞

○　テレワーク勤務者におけるセキュリティ対策の遵守状況については、定期的（年１回程度）に確認を行い、その結果を把握した上で、教育内容やセキュリティ対策内容の見直しに活用していくことが重要です。【管理者M-３】

[30] 内部不正対策についても、適切な教育を実施することが必要です。適切な教育を実施していないと管理責任を問われることや、不正行為を犯した場合の責任を追及できないことがあります。

第６章　テレワークにおけるトラブル事例と対策

テレワークセキュリティ対策の必要性について理解を深めるため、本章では、テレワークセキュリティに関するトラブル事例と、当該事例に関連した対策について示します。トラブル事例ごとに、次の３項目に整理しています。

①　具体的な動向

具体的なトラブル事例（実際に発生したサイバー攻撃事例や、セキュリティ対策に関する脅威例）

②　テレワークセキュリティへの示唆

セキュリティ上注意すべきであった点

③　有効な対策

本ガイドラインに示した対策のうち、トラブル事例に対して有効であるもの

１．VPN機器の脆弱性の放置

①　具体的な動向

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

2019年には、この脆弱性を悪用する攻撃が既に発生しており、該当のVPN機器の製造ベンダー側でファームウェアの修正が行われていますが、ファームウェアを最新にアップデートしていない機器が攻撃を受けました。

②　テレワークセキュリティへの示唆

脆弱性への対応スピードが他の国と比較して日本は低いという調査結果があります。その調査の中では、米国、英国、ドイツ等の諸外国では、脆弱性公表から最初の１週間で２～５割の製品がアップデートされている中、日本ではアップデートの実施割合が１割にも満たないこと、また脆弱性公表から７カ月たった2020年３月下旬の時点でも、対応率が低いままとなっているという結果が出ています。脆弱性を悪用した攻撃は日々発見され、攻撃者は攻撃の機会を伺っています。そのため、脆弱性対応を放置するのではなく、即時対応を行うことが重要です。

また、テレワークの急激な拡大に対応するため、過去に使用していて運用から外しておいたVPN機器を、設備増強用としてそのまま臨時稼働させたところ、脆弱性が潜んでいたために攻撃を受けたという企業もありました。このように、過去に使用していた機器を再利用する場合には、ファームウェアを最新の状態にして、既知の脆弱性が残っていない状態で使用することが重要です。

③　有効な対策

脆弱性管理（詳細解説はp.71～）	
管理者C-2 基本対策	オフィスネットワークにアクセスする際に必要となるVPN機器やリモートデスクトップアプリケーション等について、最新のアップデートやパッチ適用を定期的に行う。
管理者C-3 基本対策	テレワークで利用する端末やソフトウェアについて、メーカーサポートが終了しているものを利用しないようにテレワーク勤務者に周知する。

２．個人情報保護の強化

①　具体的な動向

2018年５月にEU一般データ保護規則（GDPR）が施行されました。個人データの処理と移転に関する規制であり、EU外の拠点においても規制への考慮が必要となります。また、違反企業に対して、高額な制裁金が課せられるということで注目を集めました。（制裁金は、最大で全世界の年間売上の４％又は2000万ユーロ）

日本においても、2020年６月に、「個人情報の保護に関する法律等の一部を改正する法律」が成立し、2022年４月に個人情報漏えい時に個人情報保護委員会への報告と被害者への通知が義務化されるほか、罰則が引き上げられました。

②　テレワークセキュリティへの示唆

個人情報保護規制の強化の動きに伴い、テレワークでの個人情報の取扱いについて、より一層適切に管理・把握する必要性が高くなっています。

テレワーク勤務者がアクセス可能な個人情報の有無、個人情報にアクセス可能な利用者・端末、個人情報の保管場所（テレワーク端末自身への保存可否を含みます。）等について検討し、対応を強化していく必要があります。

③　有効な対策

データ保護（詳細解説はp.73～）	
経営者E-1 基本対策	業務で取り扱う情報について、情報の柔軟かつ有効な活用による事業上のメリットと、情報漏えい等が発生した場合の事業影響等を総合的に勘案し、情報取扱いに関する重要度の方針を定める。
管理者E-1 基本対策	経営者が定める情報取扱いに関する重要度の方針に従い、具体的な情報管理レベルを定めるとともに、テレワークでの利用可否と利用可の場合の取扱方法（利用者・保管場所・利用可能なシステム環境の要件等）を整理してテレワーク勤務者に周知する。
管理者E-2 発展対策	取り扱う情報の情報管理レベルに照らして、アクセス可能なテレワーク勤務者やテレワーク端末を制限し（認証を実施し）、必要最小限のアクセス権限を適用する。
管理者E-3 基本対策	テレワークで利用する機密性を有する情報を特定し、保存場所を把握する。
勤務者E-1 基本対策	テレワークで取り扱う情報は、定められた取扱方法（利用者・保管場所・利用可能なシステム環境の要件等）に従って取り扱う。

３．アクセス権限の設定不備

①　具体的な動向

2020年12月、電子決済サービスを提供する企業において、情報へのアクセス権限の設定不備により、加盟店に関する情報をまとめたデータベースに対して不正アクセスを受ける事件が発生しました。この攻撃により、加盟店の名称、住所、代表者名等、最大2000万件以上の情報流出の可能性がある事態となりました。

サーバのメンテナンスを実施した際に、アクセス権限の変更を実施し、外部からもアクセス可能な状態になっていたことが、不正アクセスの原因と言われています。

②　テレワークセキュリティへの示唆

アクセス権限の適切な設定やその管理が継続的に行われていない場合、不正アクセスや情報漏えいにつながるおそれがあります。メンテナンス作業等でアクセス権限を変更する際は、不必要な許可ルールが誤って追加されていないか、また、既に必要のなくなった許可ルールが残留していないか等の観点で入念にチェックを行い、必要最小限のアクセス権限設定が行われるようにすることが重要です。

また、クラウドサービス事業者側が実施する機能追加等のアップデートに際し、初期設定値が変更されたり、設定値の意味するところが変更となったりすることもありえるため、仕様を都度確認し、意図しない設定となっていないことを確認することも大切です。

③　有効な対策

アクセス制御・認可（詳細解説はp.84～）	
管理者Ⅰ-3 基本対策	データに対するアクセス制御に際して、オフィスネットワーク上の共有フォルダやクラウドサービスに対するアクセス権限設定、ファイアウォール設定等により、機密情報を閲覧・編集する必要のないテレワーク端末やテレワーク勤務者からのアクセスを制御する。
管理者Ⅰ-4 発展対策	データに対するアクセス制御に際して、テレワーク勤務者の職務や役割、テレワーク端末の種類やそのセキュリティ対策状況を考慮した動的なアクセス制御を実装する。
勤務者Ⅰ-3 基本対策	複数人でデータを共有可能な場所（オフィスネットワーク上の共有フォルダ、ファイル共有サービス等）に機密情報を保存する場合、情報を閲覧・編集する権限が誰にあるか確認し、適切な設定を実施（テレワーク勤務者で設定できない場合はシステム・セキュリティ管理者に相談）する。

４．マルウェア感染

①　具体的な動向

2020年５月、グループ会社の従業員がフリーメールに添付されたファイルを開封し、PC１台がマルウェアに感染する事件が発生しました。マルウェア検知システムは導入していたものの、メールに添付されたファイルに仕込まれたマルウェアが新種であったためにマルウェア検知が遅れ、氏名やメールアドレス等を含む個人情報１万件以上が漏えいしました。

②　テレワークセキュリティへの示唆

フリーメールのように、業務で利用する正規アプリケーション以外のアプリケーションをテレワーク端末上で利用している場合、マルウェアの感染防止・検知等の統制が適切に機能せず、マルウェア感染のリスクが高まります。

テレワーク端末で利用を許可するアプリケーションについては、情報セキュリティ関連規程等のルールにおいて明確に定めることや、業務上必要のないアプリケーションの利用や、不審なサイトへのアクセスを制限するソリューションを導入することで、こうしたリスクは軽減することができます。また、テレワーク環境においては、オフィスネットワークを経由せずにインターネットに直接接続する場合も考えられますが、この場合は、セキュリティ対策ソフト（ウイルス対策ソフト）の定義ファイルをリアルタイムで更新したり、EDR等の高度なソリューションを導入したりすることについて検討が望ましいです。

③　有効な対策

マルウェア対策（詳細解説はp.76～）	
管理者Ｆ-１ 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
管理者Ｆ-２ 基本対策	セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能等を用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
管理者Ｆ-３ 発展対策	テレワーク端末にEDR（Endpoint Detection and Response）ソリューションを導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。
管理者Ｆ-４ 発展対策	テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるようにする。
勤務者Ｆ-１ 基本対策	少しでも不審を感じたメール（添付ファイルやURLリンク等を含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
勤務者Ｆ-２ 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
インシデント対応・ログ管理（詳細解説はp.86～）	
勤務者Ｊ-２ 基本対策	テレワーク端末の紛失やマルウェア感染等のセキュリティインシデントが発生した場合（発生のおそれがある場合を含む。）定められた連絡先へ速やかに報告する。動作が不審であるなど、セキュリティインシデントかどうかわからない場合も速やかに報告する。

5．ランサムウェア

① 具体的な動向

2017年５月、ランサムウェア「WannaCry」による攻撃が流行し、日本を含む150か国以上で発生し、30万台を超えるPCで被害が確認されました。

「WannaCry」はWindowsの脆弱性を利用して感染するランサムウェアであり、セキュリティパッチを適用していない端末に感染し被害が拡大したと考えられます。

② テレワークセキュリティへの示唆

ランサムウェアとは、感染したPC上に保存しているファイル（PCからアクセス可能なネットワーク上のファイルも含みます。）を暗号化して使用ができない状態にし、復旧させることと引き換えに身代金を要求するマルウェアです。ただし、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。

そのため、通常のマルウェア感染対策を実施するとともに、仮にランサムウェアに感染した場合でも、業務継続が可能なようバックアップを適切に取得し復旧できる状態にしておくことが重要です。

③ 有効な対策

脆弱性管理（詳細解説はp.71～）	
管理者C-1 基本対策	テレワーク端末におけるOSをはじめとしたソフトウェアについて、アップデートやパッチ適用を定期的に行い最新の状態に保つようテレワーク勤務者に周知する。
管理者C-3 基本対策	テレワークで利用する端末やソフトウェアについて、メーカーサポートが終了しているものを利用しないようにテレワーク勤務者に周知する。
勤務者C-1 基本対策	テレワーク端末におけるOSをはじめとしたソフトウェアについて、自動アップデートを有効にするなどアップデートを適切に実施する（Windows7やFlash Player等のサポートが終了した製品を使用しない。）。
勤務者C-3 基本対策	テレワーク端末のうち、特にスマートフォンやタブレットに関して、不正な改造（いわゆる脱獄（jailbreak）、root化等）を実施しない。
データ保護（詳細解説はp.73～）	
管理者E-5 基本対策	重要情報のバックアップについては、オフィスネットワーク上の共有フォルダ等のほかに、オフィスネットワークから切り離した環境（ネットワークに接続しない記録媒体やクラウドサービス等）にも保管する等、複数の環境でバックアップを保管する。
マルウェア対策（詳細解説はp.76～）	
管理者F-1 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
管理者F-2 基本対策	セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能等を用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
管理者F-3 発展対策	テレワーク端末にEDR（Endpoint Detection and Response）ソリューションを導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。
管理者F-4 発展対策	テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるようにする。

勤務者Ｆ-１ 基本対策	少しでも不審を感じたメール（添付ファイルやURLリンク等を含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
勤務者Ｆ-２ 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
インシデント対応・ログ管理（詳細解説はp.86～）	
勤務者Ｊ-２ 基本対策	テレワーク端末の紛失やマルウェア感染等のセキュリティインシデントが発生した場合（発生のおそれがある場合を含む。）定められた連絡先へ速やかに報告する。動作が不審であるなど、セキュリティインシデントかどうかわからない場合も速やかに報告する。

【コラム】様々なランサムウェア

ランサムウェアの中には、様々なタイプのものが存在します。

侵入経路が特殊なランサムウェア

「Phobos」と呼ばれるランサムウェアは、RDP経由で侵入するという特徴があります。インターネット上に開放されているRDPポートを探し当て、総当たり攻撃などを通じてRDPアカウントのパスワードを解析して不正ログインを行い、攻撃対象のネットワークに侵入します。そして、管理者権限への昇格を果たした後に、ファイル暗号化や他端末への感染等を実行するといったランサムウェアです。

RDPポートを不用意にインターネットに公開している場合、標的となるおそれがあるため、不要なポートは閉じておくことが重要です。

２段階脅迫型のランサムウェア

2020年11月、ランサムウェアによる攻撃を受け、氏名・住所などを含む個人情報、最大35万件が流出した可能性があるという事件が発生しました。本事件で攻撃者は、データの暗号化とデータの公開という２段階の脅迫を実施しました。具体的には、最初にデータの復旧と引き換えに身代金を要求しますが、その要求に応じない場合、インターネット上にデータを入手していることを公表し、そのデータの削除と引き換えに身代金の支払いを要求しました。

この場合のように、バックアップの適切な取得を行っているだけでは対策として不十分な場合が考えられます。より高度な攻撃があることを念頭に入れ、最新の攻撃手法の情報収集を行い、対応可能な検知ソリューションの導入やセキュリティ監視体制の強化等について検討する必要があります。

6．フィッシングメール

①　具体的な動向

2020年４月～６月にかけて、感染症拡大防止に伴う外出自粛や店舗休業等の影響から、インターネットショッピング利用者が増加しました。これに伴い、インターネットショッピングサイトや宅配便の不在通知等を装うフィッシングメールが多数発生しました。

②　テレワークセキュリティへの示唆

テレワークで個人所有端末を利用している場合は、業務と関係のないメールを受信する可能性もあります。オンラインショッピングサイト等を偽ったフィッシングメールをテレワークで利用している個人所有端末で受信し、記載されたURLへアクセスすることでマルウェアに感染してしまうリスクもあります。

個人所有端末の業務利用に当たってはセキュリティ対策をテレワーク勤務者任せにせず、組織として適切なセキュリティ対策を実施する必要があります。また、攻撃手法や脅威動向の情報を積極的に収集し、被害の増えている攻撃手法については典型例とあわせて注意喚起を行う等の対策も重要です。

③　有効な対策

マルウェア対策（詳細解説はp.76～）	
管理者Ｆ-２ 基本対策	セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能等を用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
勤務者Ｆ-１ 基本対策	少しでも不審を感じたメール（添付ファイルやURLリンク等を含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
教育（詳細解説はp.90～）	
管理者Ｍ-１ 基本対策	テレワーク勤務者のセキュリティへの理解と意識の向上を図るために、定期的に研修等を実施する。また、テレワーク勤務者に対して最低限求めるセキュリティ対策を定め、テレワーク勤務者に周知する。
管理者Ｍ-２ 基本対策	不審メール情報や緊急アップデートの適用等、重要なセキュリティ情報については、組織内のポータルサイトへの掲載、テレワーク勤務者への一斉メールによるアナウンス等、テレワーク勤務者の目にとまりやすい方法で注意喚起を実施する。
管理者Ｍ-３ 基本対策	テレワーク勤務者が自ら実施するセキュリティ対策が適切かどうかを確認する機会を年１回程度設け、その結果を把握する。
勤務者Ｍ-１ 基本対策	セキュリティに関する研修等を受講し、セキュリティに対する認識を高めるとともに、自らが実施しているセキュリティ対策を確認する。

7．ビジネスメール詐欺（BEC）

①　具体的な動向

偽の電子メールを送り付け、従業員をだまして資金を窃取する「ビジネスメール詐欺（＝BEC）」が、財務部門の従業員等、セキュリティ意識の甘い末端の個人を標的に増加しています[31]。

また、IPAが提供している「サイバー情報共有イニシアティブ（J-CSIP）運用状況[2020年７月～９月]」[32]の中で、BECの事例の１つとして、実在するCEOを詐称し、「出張中であるが、企業買収について協力して欲しいことがある」といった内容で連絡を取るようなものが紹介されています。

②　テレワークセキュリティへの示唆

従来、BECは経営層が標的の中心となっていました。しかし、テレワークの普及に伴い、対面での確認がしづらい状況が増加していることを狙って、財務部門等の従業員を標的にBEC被害が増加傾向にあります。企業等において財務や経理等を担当する従業員に対しては特に注意を促すことが重要です。

③　有効な対策

マルウェア対策（詳細解説はp.76～）	
管理者Ｆ-２ 基本対策	セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能等を用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
勤務者Ｆ-１ 基本対策	少しでも不審を感じたメール（添付ファイルやURLリンク等を含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
教育（詳細解説はp.90～）	
管理者Ｍ-１ 基本対策	テレワーク勤務者のセキュリティへの理解と意識の向上を図るために、定期的に研修等を実施する。また、テレワーク勤務者に対して最低限求めるセキュリティ対策を定め、テレワーク勤務者に周知する。
管理者Ｍ-２ 基本対策	不審メール情報や緊急アップデートの適用等、重要なセキュリティ情報については、組織内のポータルサイトへの掲載、テレワーク勤務者への一斉メールによるアナウンス等、テレワーク勤務者の目にとまりやすい方法で注意喚起を実施する。
管理者Ｍ-３ 基本対策	テレワーク勤務者が自ら実施するセキュリティ対策が適切かどうかを確認する機会を年１回程度設け、その結果を把握する。
勤務者Ｍ-１ 基本対策	セキュリティに関する研修等を受講し、セキュリティに対する認識を高めるとともに、自らが実施しているセキュリティ対策を確認する。

[31] 「Business Email Compromise (BEC) Attacks Rise in 75% of Industries According to Abnormal Security Research」(Abnormal Security)
https://abnormalsecurity.com/blog/announcements/q3-bec-report/

[32] サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/J-CSIP/

8．USBメモリの紛失

① 具体的な動向

2020年６月、ある教育機関で児童や関係者延べ3000人以上の氏名や住所、電話番号等を含む個人情報を記録したUSBメモリを紛失する事故が発生しました。テレワークを実施するため、USBメモリを外部に持ち出した際に紛失が発生したとのことで、当該教育機関は、関係者に向け謝罪を表明しています。

② テレワークセキュリティへの示唆

テレワークの実施により、通常の業務を行う場所からPCやUSBメモリ等を持ち出す機会が増加することから、これらを紛失してしまうリスクが高まっています。

そのため、持ち出しを許可する情報を必要最小限に留めることや、万が一PCやUSBメモリ等を紛失してしまった際の対策として、データの暗号化や遠隔からのデータ消去等の対策を実施することが重要です。

③ 有効な対策

データ保護（詳細解説はp.73～）	
管理者E-4 基本対策	テレワーク勤務者によるリムーバブルメディア（USBメモリ、CD、DVD等）の使用は、業務上の必要性が認められたものに限定し、ルールで規定する。
管理者E-7 基本対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルで暗号化を実施するようにテレワーク勤務者に周知する。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。
管理者E-8 発展対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルでの暗号化を強制し、テレワーク勤務者で設定を変更できないようにする。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。
管理者E-9 基本対策	テレワーク端末の紛失・盗難に備え、MDM（Mobile Device Management）ソリューション等を導入し、有事の際の遠隔制御でのデータ・アカウント初期化、ログイン時のパスワード認証の強制、ハードディスクの暗号化等の機能を有効化する。
管理者E-10 基本対策	テレワーク端末の紛失時に端末の位置情報を検知するためのアプリケーションやサービス等を導入する。
勤務者E-2 基本対策	リムーバブルメディア（USBメモリ、CD、DVD等）は、業務上必要であり、ルールで許可されている場合のみ利用する。
勤務者E-3 基本対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルで暗号化を実施する。
アカウント・認証管理（詳細解説はp.81～）	
管理者H-6 基本対策	利用者認証に一定回数失敗した場合、テレワーク端末の一定時間ロックや、テレワーク端末上のデータ消去を行うよう設定する。

９．無線LAN利用通信の窃取

①　具体的な動向

公衆無線LANを利用した攻撃の中には、「Darkhotel」と呼ばれる、ホテルの無線LANネットワークを乗っ取り、無線LANを利用した宿泊者から情報を窃取するという攻撃があります。

また、「偽アクセスポイント」や「APフィッシング」と呼ばれる正規の無線LANのアクセスポイントを装ったアクセスポイントを設置し、誤って接続した端末からネットワークへの不正アクセスを試みる攻撃もあります。

②　テレワークセキュリティへの示唆

テレワークでは無線LANの利用が大変便利ですが、公衆無線LANの多くは、利用者側から公衆無線LANに対する認証が十分にできず、利用している無線LANが正規のものかどうかの確認が困難なものがあります。そのため、接続してきた利用者を標的として通信を傍受し、ログインするため認証情報や、秘匿性の高い情報を窃取する等の攻撃が想定されます。

公衆無線LANを利用する場合は、相互認証されたサービスの利用や、暗号化された通信プロトコル（TLSやIPsec[33]）を利用した通信だけに留める等の注意が必要です。

③　有効な対策

通信の保護・暗号化（詳細解説はp.78～）	
管理者G-1 基本対策	クラウドサービス接続時やデータ送受信を行う際は、通信経路が暗号化された方法（VPN、TLS等）を利用するようテレワーク勤務者に周知する。また、暗号化に際しては危殆化していない暗号アルゴリズム（CRYPTRECを参照するとよい。）が使用されるようにする。
管理者G-2 発展対策	利用者同士が通信を行うサービスについては、通信相手までの間（E2E：エンドツーエンド）で常時暗号化に対応しているもののみ利用を許可する。
管理者G-3 基本対策	テレワーク勤務者が無線LANルーター等の機器を利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用し、暗号化のためのパスワード（パスフレーズ）は第三者に推測されにくいものを利用するようテレワーク勤務者に周知する。また、無線LANルーター等の管理者パスワード（設定変更のログイン画面等で必要となるパスワード）についても、第三者に推測されにくいものとすることを併せて周知する。
勤務者G-1 基本対策	クラウドサービス接続時やデータ送受信を行う際は、通信経路が暗号化された方法（VPN、TLS等）を利用する。
勤務者G-2 基本対策	無線LANルーター等の機器を利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用し、暗号化のためのパスワード（パスフレーズ）は第三者に推測されにくいものを利用する。
勤務者G-3 基本対策	クラウドサービス（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、接続先のURLが正しいこと（偽サイトでないこと）を確認した上で利用する。

[33] Security Architecture for IPの略。インターネットプロトコル（IP）のパケット単位で暗号化を行うプロトコル。

10. 第三者による画面閲覧

① 具体的な動向

従来、業務環境はオフィス等、周囲にいる人間が自組織内の関係者等に限定される環境でした。しかし、テレワークを活用し、在宅勤務やモバイル勤務、サテライトオフィス勤務を行う場合、家族を含む、業務に関係のない第三者に囲まれた環境で業務を行うことが想定されます。

そのため、第三者にPCの画面が見られてしまうことや、家族が偶然撮影しSNS等に投稿した写真にPCの画面が映りこんでしまう等、意図しない情報漏えいにつながるリスクが高まります。

② テレワークセキュリティへの示唆

テレワークにより、家族を含む、業務に関係のない第三者に囲まれた環境で業務を行うことが予想されます。そこで、機密性の高い情報を整理し、家族を含む第三者に見られないようにするというルールの策定や、プライバシーフィルター等の活用により第三者に見せないという対策の徹底が重要です。

また、テレワークの導入によりオンライン会議の利用が促進されていますが、オンライン会議の画面共有機能を使用する際にも注意が必要となります。機能的にスクリーンショット撮影や録画を制限していたとしても、スマートフォンのカメラ等で撮影されることまでは制限できません。そのため、対面の場合と異なり、一時的に提示した情報が撮影・録画されるリスクがあることを念頭に入れ、共有しても問題ない情報に留めることも検討する必要があります。

③ 有効な対策

物理的セキュリティ（詳細解説はp.88～）	
勤務者K-1 基本対策	操作画面の自動ロック設定やプライバシーフィルターの貼付等を行うほか、周囲にいる組織外の人の挙動に注意を払う。自宅等で家族がいる場合についても、不注意により意図せず情報漏えい等が起きる可能性があるため注意する。
勤務者K-2 基本対策	オンライン会議を実施するときは、音漏れや画面を介した情報漏洩が起きないよう注意する。オフィス内であっても、同じ場所で複数人が別のオンライン会議を実施等する場合の音漏れに注意する。
データ保護（詳細解説はp.73～）	
管理者E-1 基本対策	経営者が定める情報取扱いに関する重要度の方針に従い、具体的な情報管理レベルを定めるとともに、テレワークでの利用可否と利用可の場合の取扱方法（利用者・保管場所・利用可能なシステム環境の要件等）を整理してテレワーク勤務者に周知する。
勤務者E-1 基本対策	テレワークで取り扱う情報は、定められた取扱方法（利用者・保管場所・利用可能なシステム環境の要件等）に従って取り扱う。
アクセス制御・認可（詳細解説はp.84～）	
管理者Ⅰ-7 基本対策	オンライン会議にアクセスするためのURLを正規の参加者以外に公開せず、出席者の確認をするなどして、第三者が会議に参加することのないよう、テレワーク勤務者に周知する。また、会議参加時のパスワード設定や、待機室機能が有効化できる場合には、可能な限り設定するよう併せて周知する。
勤務者Ⅰ-4 基本対策	オンライン会議にアクセスするためのURLを正規の参加者以外に公開せず、出席者の確認をするなどして、第三者が会議に参加することのないようにする。また、会議参加時のパスワード設定や、待機室機能が有効化できる場合には、可能な限り設定する。

11. テレワーク端末の踏み台化

① 具体的な動向

2020年５月、リモートアクセスを利用した個人所有端末から正規のアカウントとパスワードを盗まれ、オフィスネットワークに不正アクセスされた案件が発生しました。仮想デスクトップ（VDI）によるリモートアクセスシステムを利用していたものの、個人所有端末自体が攻撃者の踏み台として乗っ取られていたために、VDIサーバ経由で自組織内のファイルサーバを閲覧されたおそれがあり、180社以上の顧客に影響が出るおそれがあると発表をされています。

② テレワークセキュリティへの示唆

テレワーク端末が「踏み台」となることで、オフィスネットワークへのアクセスを許すことや被害拡大を防ぐためには、テレワーク端末のセキュリティ対策が重要となります。

一般にVDI等のリモートアクセスシステムを利用している場合、接続元となるテレワーク端末を介した直接的なデータの持出しは制限できるとされていますが、閲覧による情報流出を防ぐことはできません。VDIを利用しているからと言って、接続元のテレワーク端末の対策が一切不要になるわけではなく、マルウェア感染対策等は必要になります。

特に個人所有端末を活用してテレワークを実施する際には、支給端末と比較してセキュリティ統制が取りづらくなることから、より一層の注意が必要となります。

③ 有効な対策

アクセス制御・認可（詳細解説はp.84～）	
管理者Ⅰ-1 基本対策	テレワーク端末においてファイアウォール（パーソナルファイアウォール）を有効にし、適切な設定を施す。
管理者Ⅰ-2 基本対策	オフィスネットワークやクラウドサービス等への接続について、接続IPアドレスの制限や、不要ポートの閉鎖を行い、インターネットへの露出を最小限とする。
管理者Ⅰ-5 発展対策	テレワーク勤務者がオフィスネットワークを介さずインターネットに接続を実施することができる構成（ローカルブレイクアウト等）を採るときは、クラウドプロキシによる認証とアクセス制御を実施する。
管理者Ⅰ-6 発展対策	オフィスネットワークとインターネットとの通信において、不審なアクセス状況がないか監視する。
勤務者Ⅰ-1 基本対策	オフィスネットワークやクラウドサービスへの接続は、システム・セキュリティ管理者が指定した方法とし、許可なく設定等を変更しない。

12. パスワードの使い回し

① 具体的な動向

他サービス等から漏えいしたIDとパスワードのアカウントリストを使って不正ログインを試みる、「リスト型アカウントハッキング攻撃」が増加傾向にあります。最近でも、大手を含め多くの企業等で被害が発生しています。

時期	業種	被害
2019年５月	製造業	オンラインストアに46万件超の不正ログイン被害が発生し、一部にクレジットカード情報も含まれていた。
2019年８月	小売業	顧客管理システムにおいて不正ログインが発生。被害件数は最大で約４万件、40万ポイント以上が不正に利用された可能性あり。
2019年８月	金融業	会員向けスマートフォン用アプリケーションにおいて、顧客のID情報が最大で１万6,000件超が不正侵入を受けた可能性あり。
2020年６月	製造業	Webサイトへの攻撃で、約30万件の情報流出が確認。
2020年６月	小売業	顧客情報最大40万件が流出した可能性あり。一部の顧客についてはポイントの不正利用等も確認。
2020年９月	旅客鉄道業	サービス利用者の会員アカウント1,000件超に不正ログインが発生。一部アカウントについてポイントの不正利用が確認。

② テレワークセキュリティへの示唆

用途やアクセス経路等が全く異なるサービスであっても、業務で利用するサービスと同様又は類似のIDやパスワードを使用していると、どこかからIDとパスワードが漏えいした場合、リスト型アカウントハッキング攻撃により、不正アクセスをされるおそれがあります。そのため、パスワードの使いまわしをしない等、より一層パスワード管理の重要性が高まります。

また、多要素認証を設定しているアカウントはそうでない場合と比較して、99.9%被害確率が低いというMicrosoft社の調査結果[34]もあることから、パスワード管理の徹底に加え、多要素認証の導入も推奨されます。

③ 有効な対策

アカウント・認証管理（詳細解説はp.81～）	
管理者H-１ 基本対策	テレワーク時にアクセスする社内システムやクラウドサービスへのアクセスで必要となる利用者認証機能について、技術的な基準（多要素認証方式の利用、パスワードポリシーの規定等）を明確に定める。
管理者H-２ 基本対策	社内システムやクラウドサービスへのアクセス時の利用者認証機能として、可能な限り多要素認証を強制する。
管理者H-６ 基本対策	利用者認証に一定回数失敗した場合、テレワーク端末の一定時間ロックや、テレワーク端末上のデータ消去を行うよう設定する。
勤務者H-３ 基本対策	複数のサービス間で同じパスワード使い回さない。また、使用するパスワードが第三者に知られた可能性がある場合は、早急にパスワードを変更する。

[34] 「One simple action you can take to prevent 99.9 percent of attacks on your accounts」 https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

13. クラウドサービスの設定ミス

① 具体的な動向

クラウド環境の設定ミスに起因した情報漏えい事故が数多く発生しています。また、一般の企業等のみならず、クラウド事業者でも設定ミスによる情報漏えい事故が発生しています。

時期	業種	被害
2020年１月	クラウド事業者	アクセス制御設定のミスにより、カスタマーサポート情報2.5億件が漏えい。
2020年10月	クラウド事業者	未公開のものを含む、同社公式ブログのデータが漏えい。

② テレワークセキュリティへの示唆

クラウドサービスは、オンプレミス環境のように明示的にインターネットからのアクセスを許可しなくても、インターネットを介して利用することが前提になっており、設定ミスにより意図せず情報が露呈する状態となりやすくなっています。

テレワーク導入にあわせて利用をはじめたクラウドストレージ等で、不適切な設定がないかを確認したり、設定確認の一環として、契約の期限や更新時期についても確認を行い期限切れにも気をつけたりするなど、クラウドサービス特有の状況を理解し認識しておく必要があります。

③ 有効な対策

ガバナンス・リスク管理（詳細解説はp.66～）	
管理者Ａ-３ 基本対策	テレワーク実施に伴ってクラウドサービス（例：ファイル共有サービス）を利用する場合、情報漏えい等を防止するための利用ルールを整備する。
管理者Ａ-４ 発展対策	クラウドサービスを選定する際には、セキュリティに関する第三者認証を取得しているものや、十分な稼働実績を有しサービス終了のリスクが低いもの、セキュリティ機能強化を継続的に行っているもの等を選定する。
アクセス制御・認可（詳細解説はp.84～）	
管理者Ｉ-２ 基本対策	オフィスネットワークやクラウドサービス等への接続について、接続IPアドレスの制限や、不要ポートの閉鎖を行い、インターネットへの露出を最小限とする。

14. クラウドサービスの障害

① 具体的な動向

近年、クラウドサービスにて大規模障害が発生し、多くのサービスに影響が出るという事態が起きています。様々なサービスでクラウドサービスが活用されていることから、クラウドサービスによる障害の影響が広範になってきています。

時期	被害
2019年８月	データセンターの冷却システム故障に起因して一部のサーバとデータベースが停止。広範な国内サービスに影響を及ぼした。
2019年11月	スパム対策機能更新に起因し、終日、メール・グループウェア・メッセージングサービスが利用不可となった。
2020年12月	アカウント認証システムの移行作業に起因し、認証管理システムがダウン。認証が必要なサービスをはじめ多くのサービスがエラー状態となった。

② テレワークセキュリティへの示唆

クラウドサービスでも障害の発生可能性はゼロではありません。近年、様々なサービスやアプリケーションへのアクセスの前提となる認証基盤をクラウドサービスが担うケースも出てきており、クラウドサービスの障害に伴い、多くの業務が停止することも起こりえます。どんなに稼働率の高いクラウドサービスであっても、オンプレミス同様、障害が発生しうるということに変わりはありません。

テレワークでクラウドを利用する際には、クラウドサービスへの依存度に応じて、クラウド障害が発生した際に備えた事前準備や、実際に障害が発生した場合の対応手順等を予め整理しておくことが重要です。

③ 有効な対策

ガバナンス・リスク管理（詳細解説はp.66～）	
管理者Ａ-３ 基本対策	テレワーク実施に伴ってクラウドサービス（例：ファイル共有サービス）を利用する場合、情報漏えい等を防止するための利用ルールを整備する。
管理者Ａ-４ 発展対策	クラウドサービスを選定する際には、セキュリティに関する第三者認証を取得しているものや、十分な稼働実績を有しサービス終了のリスクが低いもの、セキュリティ機能強化を継続的に行っているもの等を選定する。
データ保護（詳細解説はp.73～）	
管理者Ｅ-５ 基本対策	重要情報のバックアップについては、オフィスネットワーク上の共有フォルダ等のほかに、オフィスネットワークから切り離した環境（ネットワークに接続しない記録媒体やクラウドサービス等）にも保管する等、複数の環境でバックアップを保管する。

15. サプライチェーン

① 具体的な動向

2020年12月に、業務委託先であるマネージド・サービス・プロバイダ（MSP：コンピュータやネットワーク等の運用・保守・監視等を行う事業者）事業者経由でサーバに不正アクセスされ、複数の端末がマルウェアに感染しました。

MSPが提供するソフトウェアの脆弱性が原因ですが、短期間に感染が拡大した原因として、MSPが有するサーバと委託元事業者との間にファイアウォールが存在せず、通信を最小限に制限できていなかったことがあります。

② テレワークセキュリティへの示唆

自組織のセキュリティが保護されていたとしても、委託先や関連会社等におけるセキュリティが脆弱であると、預けた情報の漏えいや取引の停滞等により、結果的に自組織にも被害が及ぶ可能性があります。そのため、委託先や関連会社等を含めたサプライチェーン全体で適切なセキュリティ対策が実施されるよう、取引時等にセキュリティ対策状況を確認するなどの必要な対策を行います。

攻撃者はセキュリティの一番弱いところを狙ってきます。サプライチェーンも含めてセキュリティ対策を適切に実施していない場合、業務委託元組織への攻撃の足がかりとして業務委託先が狙われるおそれがあります。

③ 有効な対策

業務委託先の従業員は直接的な従業員ではないものの、従業員に準ずる位置づけの者として対策を実施することが望まれます。

教育（詳細解説はp.90～）	
管理者M-1 基本対策	テレワーク勤務者のセキュリティへの理解と意識の向上を図るために、定期的に研修等を実施する。また、テレワーク勤務者に対して最低限求めるセキュリティ対策を定め、テレワーク勤務者に周知する。
勤務者M-1 基本対策	セキュリティに関する研修等を受講し、セキュリティに対する認識を高めるとともに、自らが実施しているセキュリティ対策を確認する。

用語集

BYOD	Bring Your Own Devicesの略称。個人所有端末を業務に利用すること。
EDR	Endpoint Detection and Responseの略称。詳細はコラム（p.77）参照。
ISAC	Information Sharing and Analysis Centerの略称。セキュリティに関する情報共有体制の一つ。特定の業界の企業等によって構成される組織であり、当該業界のセキュリティに関する最新の脅威動向やあるべきセキュリティ施策等について分析・共有を実施する。
MDM	Mobile Device Managementの略称。スマートフォン等のセキュリティ設定を統合的に管理するためのツール。
VDI	Virtual Desktop Infrastructureの略称。サーバ上に仮想のPCを複数台用意し、サーバに接続した利用者からはあたかも個別にPCが用意されているような使い勝手で利用できるようにする環境。
VPN	Virtual Private Networkの略称。主にインターネット上で、認証技術や暗号化等の技術を利用し、保護された仮想的な専用線環境を構築する仕組み。
サプライチェーン	システム・サービス等の企画・設計・製造・流通・運用等の一連の流れ、またその一連の流れに関わる企業等のこと。
情報セキュリティ関連規程	企業等における「情報セキュリティに関する方針や行動指針」をまとめた文書。①全体の根幹となる「セキュリティポリシー（基本方針）」、②基本方針に基づき実施すべきことや守るべきことを規定する「セキュリティスタンダード（対策基準）」、③対策基準で規定された事項を具体的に実行するための手順を示す「セキュリティプロシージャ（実施内容）」の３つの階層で構成される。
脆弱性（ぜいじゃくせい）	ICT機器・システムやその利用環境におけるセキュリティ上の欠陥のこと。設計・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。
セキュリティポリシー	情報セキュリティ関連規程のうち、全体の根幹となる基本方針に相当するもの。
ゼロトラストセキュリティ	第２章の「４．ゼロトラストセキュリティの考え方」（p.22～）を参照。
多要素認証	知識認証（例：パスワード、秘密の質問）、物理認証（例：ICカード、SMS認証）、生体認証（例：指紋認証、顔認証）のうち異なる複数の要素を用いる認証方式。
定義ファイル	マルウェア等の特徴を収録したファイルのこと。
パッチ	ソフトウェアを改善・改良するためのプログラム。
標的型攻撃	不特定多数を攻撃するのではなく、特定の組織や利用者に対象を絞って行う攻撃のこと。
フィッシング	詐称した電子メール等で偽のWebサイトに誘導し、クレジット番号等の情報の入力をおこなわせ窃取する攻撃手法のこと。
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。
ランサムウェア	感染した端末上のデータを勝手に暗号化してしまうマルウェア。攻撃者はその端末の利用者に対し暗号化を解除する見返りに金銭等を要求して利益を得る。
リモートデスクトップ	自らの手元にある機器から、ネットワークを経由して他の端末を操作するための仕組みのこと。
ローカルブレイクアウト	オフィスネットワークやデータセンター等の拠点を介することなく、端末から直接インターネットへアクセスするネットワーク構成のこと。

（参考）本ガイドラインの検討経緯

本ガイドラインは、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。また、当該調査研究において次の有識者から構成される調査検討会を開催し、本ガイドラインについて検討を行っています。

＜構成員（五十音順 敬称略）＞

鵜澤　純子　株式会社テレワークマネジメント
小豆川裕子　常葉大学 准教授
田宮　一夫　一般社団法人日本テレワーク協会 専務理事
山田　達司　株式会社エヌ・ティ・ティ・データ
吉岡　克成　横浜国立大学 環境情報研究院 准教授
（座長）渡辺　研司　名古屋工業大学 教授

＜オブザーバー＞

総務省　サイバーセキュリティ統括官室
経済産業省　商務情報政策局　サイバーセキュリティ課
内閣官房　内閣サイバーセキュリティセンター

本ガイドライン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/