安心安全テレワーク施設
ガイドライン
（第 2 版）

2025 年 4 月

一般社団法人日本テレワーク協会

一般社団法人セキュア IoT プラットフォーム協議会

目次

はじめに

【背景】

新型コロナ感染症対策として拡大したテレワークによる働き方、学び方、イベント開催等は、場所が離れていても実施可能なものとして社会的に受け入れられてきている。例えばオンラインでの打ち合わせ、授業、イベントなどは相当に一般化したと言える。一方で日本、特に大都市圏などの住宅事情では自宅等に執務専用のスペースを確保することが難しい上に、家族等への配慮からも、在宅では効率的に働けない、オンオフの切り替えが難しい、心身の健康維持管理面などの課題も分かってきた。また都市の中心部にあるオフィスに日々全社員等が毎日通勤して集まって働くことや、単身赴任などの見直しも進みつつある。そういった状況下で、シェアオフィス、サテライトオフィス、レンタルオフィス、サービスオフィス、コワーキングスペース等（以下テレワーク施設）は、近年大都市圏を中心に大量に供給され、利用者も増加する傾向が続いている。2021年3月に発行した「共同利用型オフィス等で備えたいセキュリティ対策について（第2版）（以下第2版）」では、テレワーク施設におけるサイバーセキュリティ等情報セキュリティの脅威と対策を示してきた。第2版をガイドラインとした「共同利用型オフィス等セキュリティ認証プログラム」については、大手テレワーク施設提供事業者や、首都圏の独立系施設、地方のホテル、旅館等に併設されるテレワーク施設などで認証取得が進んでおり、施設運営事業者は利用者のセキュリティニーズが高いことを認識し、そのニーズに応えることが必要と考えていることが判明した。

以上を踏まえこの第2版の更新版である「安心安全テレワーク施設ガイドライン」では、テレワーク施設に係る情報セキュリティ対策について見直すとともに、作業環境面と施設環境面での安心安全を確保する上での脅威と対策についても取り上げることで、働く場所としての総合的な安心安全を目指すこととした。さらに具体的な対策事例も示すことで、より対策の導入や脅威への対応の取り組み易さへも配慮した。

【利用目的】

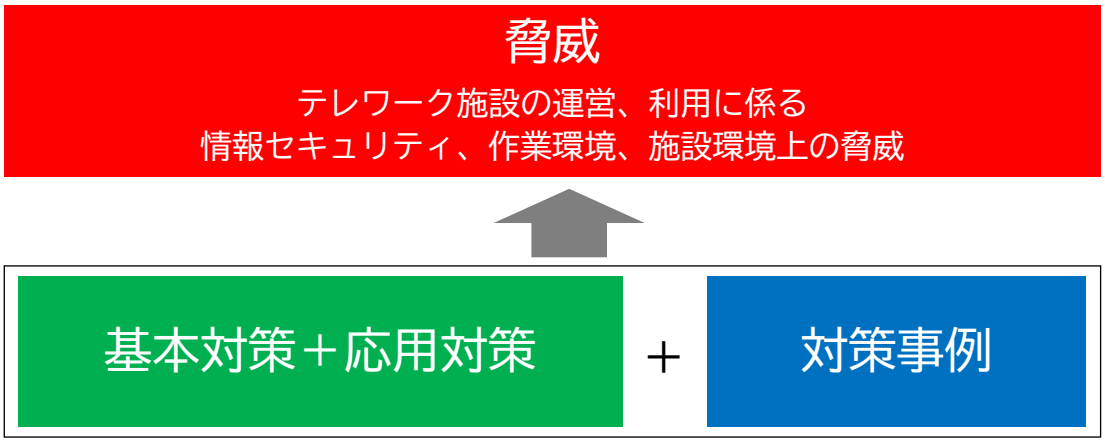
テレワーク施設運営事業者に対して、情報セキュリティ、作業環境、施設環境上の課題と解決策を解説するとともに、安心安全なテレワーク施設を設営・運営するために対応が必要な要件を示す。

また、テレワーク施設の利用者、企業等に対しても、施設を選択する上での参考として利用いただくことを目的としている。

【構成】

テレワーク施設の運営に対して、情報セキュリティ、作業環境、施設環境の観点で考えられる「脅威」と、それに対して備えるべき最低限必要な事項を「基本対策」とし、状況に応じて更に望まれる事項を「応用対策」、対策の具体例を「対策事例」として示し、全体を構成している。

安全なテレワーク施設とする上では、「基本対策」の要件を満たすことを必須と位置づけている。加えて人的、資金的な資源が必要となる、システム的対策や、より高度な管理体制の構築については「応用対策」と位置づけ、より利便性が高く安心安全な環境を整備する上での要件を示した。



【テレワーク施設の定義】

本ガイドラインにおいて対象とする「テレワーク施設」は以下の通りである。

○ 地方公共団体、各種団体、企業等が運営するサテライトオフィス、コワーキングスペース、レンタルオフィス、シェアオフィス、フレキシブルオフィス（フレックスオフィス）、サービスオフィス、テレワークボックス（個室型ワークボックス）等、テレワークの利用に供する施設。

セキュリティ、作業環境、施設環境の課題と対策

第１章. セキュリティ管理体制の構築

【脅威】

- 情報セキュリティ対策が明文化されておらず、人的、運用面でのミス、対応の属人化や順守状況の未把握により、セキュリティ事故が発生する。
- 定期的な対策の改善や是正ができておらず、対策の有効性が低減し、セキュリティ事故が発生する。

【基本対策】

対策①：情報セキュリティポリシーの策定

テレワーク施設における情報セキュリティに関する考え方や責任体制などを明文化したポリシー（基本方針）を策定し、テレワーク施設の会員等利用者（以下「利用者」という）に示す。またポリシーで規定した対策を実施し、情報セキュリティの脅威に変化が発生した場合は見直す。

対策事例①を参照。

対策②：利用規約の策定・利用者の同意

施設の利用規約を策定し、利用申請や登録時に利用者が規約に同意したことを確認し、記録する。

対策事例②を参照。

対策③：施設の保有する情報（データ）の保護

テレワーク施設の運営・管理上の業務（バックオフィス業務）で取り扱う情報が、漏えいや改ざん、不正利用等されないよう保護するために必要な対策を実施する。

対策の内容については、情報の機密性、完全性、可用性※の確保を考慮する。

※コラム「情報の機密性・完全性・可用性」を参照。

対策④：セキュリティ事故発生対応マニュアルの策定

セキュリティ事故発生時の具体的対応を記したマニュアルを策定する。

また、マニュアルに基づき、利用者には事前に利用規約等で、サービス上の不具合やマルウェア感染、情報漏えい等の疑いが発生した場合の連絡方法を明示する。

対策事例③を参照。

対策⑤：セキュリティ教育、研修、訓練の実施

テレワーク施設の経営者を含む全従業員（以下「従業員」という）に対し、「情報セキュリティポリシー」及び「セキュリティ事故発生対応マニュアル」等の重要事項について内容周知を行い、定期的に教育や研修、マルウェア感染等を想定した訓練等を実施し理解度を確認する。

また、実施した活動を記録に残す。

対策⑥：最新の情報セキュリティ情報や関連法令の確認

サイバー攻撃やマルウェア感染等は年々高度化・複雑化していることから、情報セキュリティに関する最新の脅威動向や個人情報保護法等の関連法令の情報を定期的に確認し、把握しておく。

☝対策事例④を参照。

【対策事例】

事例①：情報セキュリティポリシーの内容

テレワーク施設で策定する情報セキュリティポリシー（基本方針）には以下の項目を含める。ここで示す項目は例示であって、施設の用途・運営環境により追加等修正が必要な場合がある。

- 目的
- 法令遵守
- 組織体制
- 情報セキュリティ対策　※対策内容の概要を記載
- 教育・訓練
- 事業継続
- 違反・事故措置
- 継続的改善
- 制定日、改訂日、事業代表者氏名

事例②：利用規約の内容

テレワーク施設で策定する利用規約には以下の項目を含める。ここで示す項目は例示であって、施設の用途・運営環境により追加等修正が必要な場合がある。

- 利用者に発行する入館カード、認証用ID、パスワード等を許可無く他人へ貸与することの禁止。
- 手荷物の常時携行。
- 利用者は持ち込むPC、スマートフォン、タブレット等の端末（以下、「端末」という）

について、ウイルス対策ソフトのインストール、定義ファイルの自動更新、リアルタイムスキャン、定期的にフルスキャンを実施すること。
- 端末のOS、ファームウェア、アプリケーションの最新化。
- 不審なメールやサイトへのアクセス禁止。
- 不正な改造を行っている端末の使用禁止。
- マルウェア感染等の情報セキュリティ事件・事故の疑いがある場合の報告。
- （レンタルPCが有る場合）貸与された端末の設定変更や許可されたアプリケーション以外のインストール禁止。

また、Wi-Fiの利用に関する項目については、総務省「公衆Wi-Fi提供者向け セキュリティ対策の手引き」（令和7年2月版）※を参考すること。
- Wi-Fiルーター（アクセスポイント）の適切な運用
- Wi-Fiルーター（アクセスポイント）の設定の定期的な確認
- 業務用ネットワークの分離
- 利用者情報の適切な確認
- アクセスログの記録・保存
-

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

<u>事例③：セキュリティ事故発生対応マニュアルの内容</u>

テレワーク施設で策定するセキュリティ事故発生マニュアルには以下の項目を含める。ここで示す項目は例示であって、施設の用途・運営環境により追加等修正が必要な場合がある。

- 事故発生時の連絡先（テレワーク施設の管理者等のメールアドレス、電話番号）
- 関係当局の連絡先（所轄警察署、個人情報保護委員会（PPC）等）
- 関係する外部組織の連絡先
  - A） ネットワークベンダ（保守業者等）
  - B） インターネットプロバイダ
  - C） セキュリティ専門ベンダ（調査会社等）
  - D） 弁護士
- 原因調査※・対応手順（情報漏えい、荷物の紛失、ネットワークトラブル等）
- 報告書式（事象・対応経緯、原因、対策・是正項目等。時系列でまとめる）

※ 原因調査にあたっては、セキュリティ事故が発生した場合の証跡として、裁判官の発付する令状に従って、アクセスログを含め、犯人を特定するための情報提供を警察から求められる場合がある。

<u>事例④：最新の情報セキュリティ情報の収集先</u>

国内セキュリティ関連機関や個人情報保護委員会等から発信される各情報を参照する。なお、ネットワーク等システム構築委託先事業者に情報提供を依頼する方法もある。

- 独立行政法人情報処理推進機構（IPA）
  https://www.ipa.go.jp/
- 内閣サイバーセキュリティセンター（NISC）
  https://www.nisc.go.jp/
- 一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）
  https://www.jpcert.or.jp/
- 個人情報保護委員会（PPC）
  https://www.ppc.go.jp/

第２章. 個人情報・利用者管理

【脅威】

- 本人の許可・同意が無いままに、個人情報を取得・提供することで、事件・事故が発生する。
- 利用目的外の個人情報取得・提供など法令違反により罰則を課せられ、利用者や社会からの信頼を失う。

【基本対策】

対策①：個人情報保護ポリシーの策定

利用者及び従業員から取得する個人情報の保護対策や責任体制などを明文化したポリシー（基本方針）を策定し、利用者及び従業員に示す。利用目的の変更等、内部外部における状況変化があった場合は見直す。

☝対策事例①を参照。

対策②：個人情報の適切な管理

利用者及び従業員の個人情報がポリシーの利用目的に基づいて適切に取得・提供されているか、利用終了とともに速やかにかつ適正に廃棄されているか、定期的に確認を行う。

また、取得・提供された個人情報は台帳管理を行い、テレワーク施設の管理者等によって棚卸（例：年1回）※を実施する。

※　第3章「入退出管理」対策②も参照。

対策③：テレワーク施設が提供するWebサイトの適切な管理

提供するWebサイトにおいて、利用登録や問い合わせ等の個人情報を入力・送信させる場合は、TLS（https）通信の設定を実施する。また、Webサイト構築・運用に当たっては、脆弱性への対応を実施する。

☝対策事例②③を参照。

対策④：利用ログの取得・管理

個人情報の漏えいやセキュリティ事故発生時に原因調査を行うために、提供するWebサイトの利用ログ（利用者、利用時間、利用リソース等）を取得する。

また、取得した利用ログは許可無く利用されないようにかつ外部に漏えいしないように適切に保存・管理を行う。

【対策事例】

事例①：個人情報保護ポリシーの内容例

テレワーク施設で制定する個人情報保護ポリシー(基本方針)には以下の項目を含める。ここで示す項目は例示であって、施設の用途・運営環境により追加等修正が必要な場合がある。

- 利用目的（範囲およびインプット情報含めた取得・提供内容に関する事）
- 法令遵守
- 安全管理措置（組織的、人的、物理的、技術的対策の概要）
- 開示等の請求に応じる手続き
- 苦情および相談の対応、申し出先
- 制定日、改訂日、事業者の氏名または名称、住所、連絡先、代表者氏名

事例②：Webサイト構築・運用

Webサイトの構築・運用における脆弱性への対策として、「OWASP Top 10 2021の紹介※1」にある攻撃手法や、「安全なウェブサイトの作り方※2」及び「TLS暗号設定ガイドライン※3」に対応する。

※1 https://owasp.org/Top10/ja/

※2 https://www.ipa.go.jp/security/vuln/websecurity/about.html

※3 https://www.ipa.go.jp/security/crypto/guideline/ssl_crypt_config.html

事例③：Webサイトの脆弱性対策（脆弱性診断）

個人情報を入力する機能（フォーム等）を提供するWebサイトにおいては、セキュリティ脆弱性が原因で発生する情報漏えいや掲載情報（ソースコード）の改ざん被害に合わないために、定期的に第三者の専門家※による脆弱性診断（Webアプリケーション診断等）を実施し、客観性評価による脆弱性の把握と是正による対策強化が推奨される。

※ IPAでは経済産業省が策定した「情報セキュリティサービス基準」に適合する脆弱性診断サービスの提供事業者を公開している。
情報セキュリティサービス基準適合サービスリスト
https://www.ipa.go.jp/security/service_list.html

第３章. 入退室管理

【脅威】

- 許可されていない利用者や身元不明者が入場し、盗難、ネットワークへの不正侵入や情報漏えい等の事件・事故が発生する。
- 利用者になりすました入場、利用が発生する。

【基本対策】

対策①：利用者の本人確認

利用しようとする者に対して、写真付き身分証明書（マイナンバーカード、運転免許証、パスポート等）によって、本人確認を行った上でテレワーク施設の利用登録（許可）を行う。

また、利用登録（許可）をした者以外は原則入場・利用ができないようにする。

会員制のテレワーク施設においては、会員のゲスト（一時的な利用者、打ち合わせ等で会員を訪問した者等）についても、本人確認に加えて、入室可能なエリアやネットワーク接続時の制限事項など個別の利用規約を示す。

対策②：入退室記録・ログの取得・管理

利用者の入場時は、1人ずつ入場を確認し、入場記録がない場合は、身元及びその理由を確認できるまで、退場を許可しない。

また入退室記録又は電子的ログ（利用者、利用時間、利用リソースなど）を取得し、適切に一定期間保存（例：1年間）・管理する。

対策③：入退出管理システム等の管理者パスワード設定

入退室管理を行うPC等機器やシステムには、それを管理する者だけが知るパスワード（管理者パスワード）を設定する。工場出荷時のデフォルト値は変更する。紙ベースで管理する場合は、管理者だけが持つ鍵で施錠する。

管理者パスワードは定期的に更新する必要はないが、アルファベット（大文字、小文字）、数字、記号を組み合わせた十分な長さの文字列で、第三者に推測されにくい複雑なパスワードに変更する。

また、パスワードや鍵の共有範囲は業務上必要な最小限の範囲に止める。管理者の従業員が異動・退職する際には、速やかにパスワードを変更し、鍵を回収する。

【応用対策】

対策④：入退出管理システムの導入

ICカード型やスマートフォンアプリ型会員証など電子的に入退出の管理ができるシス

テムや静脈認証、指紋認証、顔認証など生体情報を使った認証システムを導入することで、利用者を特定でき、記録漏れとなりすましを抑止できる仕組みを導入する。

☝対策事例①を参照。

【対策事例】

事例①：入退室管理システムにおける認証強化

ICカードや生体情報を利用した認証システムにおいては、有効期間の設定、定期的な更新、紛失時に即座に失効する仕組みや、利用者が記憶する暗証番号の入力など鍵となる要素を組み合わせる多要素認証とすることで、セキュリティ対策を強化する。

（組み合わせ可能な鍵の例）

- 物理キー（ICカード、USBドングル等）
- パスワード（暗証番号等）
- 生体情報
- SMS通知やスマホアプリによるワンタイムパスワード

第４章．ネットワークセキュリティ

【脅威】

・ ルーターや無線 LAN アクセスポイント等のネットワーク機器や、複合機、防犯カメラ等のネットワーク接続機器（以下「ネットワーク機器等」という）の管理が不十分で、マルウェア感染、情報漏えい、機能停止、サイバー攻撃等のセキュリティ事故が発生する。

【基本対策】

対策①：セキュリティアップデートの実施

ネットワーク構築、運用にあたって、セキュリティ上の脅威が発生しないように、機器のOSやファームウェア、アプリケーション等が最新化されるよう、定期的に状態を確認し、更新する。自動的にアップデートする機能がある場合には、それを有効にする。

最新化できない場合はその理由と、他の方法による対策の検討、今後の対応計画及び進捗状況についてまとめ、記録する。

メーカーサポートや保守が終了しているネットワーク機器等は使用しない。

対策②：初期設定の変更

ネットワーク機器等が、家庭や同一組織内での利用を想定した初期設定（デフォルト値）は、テレワーク施設での利用にあたって適切なパラメータ設定となるよう変更する。

また、NTP (Network Time Protocol)による自動的な時刻合わせが可能な機器についてはその設定を実施する。

対策③：管理者パスワードの適切な設定

ネットワーク機器等のパラメータを変更するための管理者パスワードは、工場出荷時の値から変更する。

管理者パスワードは定期的に更新する必要はないが、アルファベット（大文字、小文字）、数字、記号を組み合わせた十分な長さの文字列で、第三者に推測されにくい複雑なパスワードに変更する。

また、パスワードの共有範囲は業務上必要な最小限の範囲に止める。パスワードを知る従業員が異動・退職する際には、速やかに変更する。

対策④：無線LANアクセスポイントの適切な設定

無線LANアクセスポイントを提供する場合、セキュリティ方式としてWPA2（適切にアップデートされたもの）又はWPA3を設定し、暗号化方式はAES（CCMP）とする。なお、WEP及びWPAは脆弱性があるため使用しない。

また、テレワーク施設の境界から外に漏れる無線電波が最小限となるよう留意する。

対策⑤：無線LANアクセスポイントの利用者接続パスワード設定と管理

利用者に配付する接続パスワードは、管理者パスワードとは全く別のものを設定し、利用しない者がパスワードを知りうる機会を抑制するため、定期的（年1回以上）に変更する。

☝対策事例②を参照。

対策⑥：利用者の端末間通信の禁止設定

利用者が別の利用者の端末にアクセスできないように、無線LANアクセスポイントの設定において「ネットワーク分離機能」や「プライバシーセパレーター機能」を有効化する。

また、複数の無線LANアクセスポイントを利用している場合や有線LANでネットワークアクセスを提供している場合には、それらが接続されるスイッチやルーターにおいて、特定のポート間通信の禁止等を設定する。

なお、利用者の端末間通信を禁止しつつ、複合機等特定のネットワーク接続機器やポートを利用する場合には、安全な利用が確保できるよう適切に設定する。

対策⑦：業務用ネットワークとの分離

利用者が利用するネットワークから、テレワーク施設事業者の業務システム等のネットワークにアクセスできないようにするため、利用者に提供するネットワークは、接続回線を別にするなど、業務システム等とは独立して設置するか、安全に分離する。

対策⑧：アクセス制御

ルーターのWAN側ポートを除いて、ネットワーク機器等にはインターネット側からアクセスできないようにする。特に複合機は原則として外部ネットワーク（インターネット）に接続しない。ベンダのリモート保守等で接続する必要性がある場合にも、ファイアウォール等を設置した上で、接続IPアドレスやポートを制限するなど、厳重なセキュリティ対策を実施する。

対策⑨：アクセスログの適切な管理

個人情報の漏えいやセキュリティ事故発生時に原因調査を行うために、ネットワーク機器等でNTPによる自動的な時刻合わせが可能な機器についてはその設定を実施し、アクセスログ（接続日時、回数、接続位置、接続先、端末情報等）を取得する。

また、取得したアクセスログは、高い機密性を持つ情報であることから、業務上の必要性に応じた最小限の記録と利用範囲に留め、許可無くマーケティング利用や第三者提供されないようにアクセスを制限する。さらにセキュリティ事故発生時の原因調査に必要な証跡となることから一定期間保管する。ネットワーク機器の運用を事業者に委託している場合は、アクセスログもその委託先事業者において記録・保存されているため、その記録内容や保存期間等を把握し、問い合わせがあった場合の対応方法を委託先事業者と確認する。

☝アクセスログの取り扱いについては「第１章セキュリティ管理体制の構築」対策事例③も参照。

対策⑩：複合機に蓄積されたデータの消去

複合機で入出力したデータは、複合機の内蔵記録装置（ハードディスク等）に保存されることがあるため、この保存されたデータの「暗号化」や「自動消去」機能がある場合には有効にする。機能が無い場合には、定期的に手動で消去する。

対策⑪：複合機の出力管理

複合機から出力した書類や原本書類の第三者による持ち去りや、放置を禁止する事項を利用規約に含めるとともに、注意喚起を行う。

☝対策事例⑤を参照。

対策⑫：レンタルPC

PC、タブレット等の端末をサービス貸与する場合、OSの最新化やウイルス対策ソフトのインストール、定義ファイルの自動更新、リアルタイムスキャンの設定等の対策を行う。

☝対策事例④を参照。

【応用対策】

対策⑬：高度なセキュリティの導入

- 無線LANアクセスポイントと接続する端末等について、電子証明書等を活用して相互に認証を行い、無線LANアクセスポイントのなりすましや許可されていない端末の接続を制限する。
- テレワーク施設から業務で利用するサーバ等へアクセスする場合は、アカウント管理を厳重に行うとともに、多要素認証の仕組み（電子証明書を活用したクライアント認証など）を導入するなど、不正アクセスのリスクを軽減する。
- ネットワークへの接続状況を監視するシステムを導入し、接続機器を保護する。
- 年1回以上の定期的な脆弱性診断の実施。

☝対策事例①⑥を参照。

対策⑭：複合機の媒体接続制限

許可無く複合機に利用者が所有するUSBメモリ等の外部記憶媒体を接続させないことが望ましい。差し込みポート（インターフェイス）がある場合は、無効化（設定および物理的封印等）する。

なお、許可する場合は、申請式にしてログを残す、ウイルススキャンを実行させるなど対策を実施すること。

☝対策事例⑤を参照。

【対策事例】

事例①：ネットワーク機器等の脆弱性診断

ネットワーク機器等はOSやファームウェアが最新化されていないことによって生じる既知の脆弱性を悪用されて、不正アクセスやサイバー攻撃に発展する場合がある。国内セキュリティ関連機関等※から発信される脆弱性情報の確認や専門ツール等を利用した情報収集を行う。また、定期的に第三者の専門家による脆弱性診断（ネットワーク診断、Wi-Fi診断、セグメンテーションテスト等）を実施し、客観性評価により脆弱性を把握し是正する。

※ 独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/vuln/

※ JVN iPedia 脆弱性対策情報データベース
https://jvndb.jvn.jp/

事例②：無線LANアクセスポイントの利用者接続パスワード配付方法

利用者に配付する接続パスワードは、利便性を損なうことなく利用者のみが知ることができる方法で案内することが推奨される。

- 利用受付の際に、本人確認した上で接続パスワードを伝える。
- 会員に限定し通知を受けることができる方法で公開する。
  - 登録されたメールアドレスへ送信
  - 会員しかログインできない管理サイトでの公開

事例③：マルウェア検知

利用者がマルウェアに感染した端末をネットワークに接続した場合や、ネットワーク利用中に感染した場合に備えて、マルウェアのふるまいを検知するツール等を導入する。これにより感染の把握や対応を迅速化し、影響を最小限にとどめることができる。

事例④：レンタルPCの運用・管理対策

PC等端末を貸与する場合、以下の対応を標準化する。

- 利用者アカウントには管理者権限を付与しない。
- 利用者アカウントにはパスワードを設定しない。
- サポート切れのOSやファームウェア、アプリケーション等は使用しない。
- OSやファームウェア、アプリケーション等は常に最新の状態で貸し出しを行う。
- 適切な環境設定を維持した上で貸し出しを行う。返却時には設定が維持されている

か確認する。
- 利用者によるアプリケーションやソフトのインストールを原則許可しない。
- OS標準のセキュリティ設定（例：ファイアウォール、マルウェア検知等）について、貸出前に適切に設定する。
- ウイルス対策ソフトのインストール、定義ファイルの自動更新、リアルタイムスキャンの実施。
- 液晶モニタには、のぞき見防止フィルタを付ける。

事例⑤：複合機の出力管理

複合機からの印刷出力は下記のような出力制御を行い、第三者による持ち去りへの対策を行う。
- IDカード認証
- パスワード入力
- QR等の認証コードによる読み取り
- コインベンダ（現金投入することによってコピーやプリントができる仕組み）の導入

事例⑥：ネットワークの可視化

ネットワークへの接続状況の可視化については、以下の機能を有するシステムを利用する。
- 接続される機器の正当性の確認
- 新しい機器が接続された時に通知し、許可していない機器は接続を切断
- マルウェア感染のおそれがあるサイトやフィッシングサイトへのアクセスを制限
- 不審な通信の監視

第５章. 物理セキュリティ

【脅威】

- 端末の画面が、覗き見られることで、重要な情報が漏えいする。
- 端末やUSBメモリ等の外部記憶媒体（以下「記憶媒体」という）、書類等を放置する、記憶媒体や重要書類を利用可能な状態で廃棄することにより情報の盗難や不正利用が発生する。
- 電話やオンライン（Web）会議の会話が、漏れ聞こえることで、重要な情報が漏えいする。

【基本対策】

対策①：オンライン（Web）会議等への対策

オンライン（Web）会議等で音声を発すること（以下「音声利用」という）を許可する場合は、会議室や専用の個室型ブース等を設置し、音漏れへの対策を整備する。

また、ラウンジ等共有の場で音声利用を行うことによるリスク等について、利用者の注意を喚起する。

対策②：手荷物の管理

離席時の手荷物等を放置することによるリスク等について、利用者の注意を喚起する。

対策③：シュレッダー、溶解BOXの導入

記憶媒体や重要書類を一般ゴミに捨てることによるリスク等について、利用者の注意を喚起する。また復元処理が困難なセキュリティ性の高いシュレッダー（例：マイクロカット等）や中身の取り出し防止機能の付いた溶解BOXを設置する。溶解サービス等利用可能な状態で廃棄する場合は、廃棄完了証明書等で適切に処理したことを証明できる廃棄事業者を選択する。

☝対策事例①を参照。

対策④：サーバや端末の廃棄

テレワーク施設事業者が保有するサーバや端末を廃棄または返却する際は物理破壊や信頼性の高い消去専用ソフトウェアによる消去等を実施し、確実にデータを消去する。

☝対策事例①を参照。

対策⑤：ネットワーク機器の設置場所

ネットワーク機器等は、施錠できるラック等に施錠管理する。アクセスポイントは利用者が直接触れにくい天井の高い位置に設置するなど、許可の無い不正操作を抑止する対策を行う。

また、電源やLANケーブル等においても、断線や接続不良等を防止するために保護および整線（ケーブル等をまとめること）する。

☝対策事例②を参照。

【応用対策】

対策⑥：サウンドマスキングの導入

物理的設備で十分な防音を期待できない場合、サウンドマスキングシステムを導入することが望ましい。

対策⑦：施錠ロッカーの導入

安全に手荷物を管理できるように、また作業空間の確保や通路に置くことによるつまずきなどを抑止する目的で、施錠可能なロッカーを設置することが望ましい。

【対策事例】

事例①：安全な情報(データ)の消去方法

サーバや端末の廃棄が、情報漏えいの原因となることがある。安全に廃棄するためには、次に例示する消去方法により消去する。複数の方法を組み合わせて消去する場合もある。

- 穴をあける等物理破壊する
- シュレッダー（記憶媒体が対象）
- 溶解処理
- 専用消去ソフトウェアによる消去
- 磁気消去（HDDが対象）

事例②：安全なネットワーク機器の設置方法

サーバやネットワーク機器等は、取り扱いや電源コンセントとの接続方法等によって漏電、断線、火災の原因となることがある。安全を確保する上で次の注意事項に対処することで事故の発生を抑止し、また定期的な点検を実施する。

- 水気のある場所には設置しない（漏電事故）。
- 傷んだ電源コードや曲がった状態のコンセントプラグは使用しない（断線、過熱事

故)。

- タコ足配線は定格電力をオーバーして使用しやすいため注意する(過熱、火災事故)。
- チリや埃がたまらないように完全に電源プラグをコンセントに差し込む(火災事故)。
- 電源コードをくぎやホチキスで固定しない。下敷きにされた状態にしない(断線、過熱事故)。
- 電源コードを束にしない、ねじらない。(断線、過熱事故)。

第６章. 作業環境管理

【脅威】

- 作業環境（作業空間、机、椅子、照明、空調、音、整理整頓等）が悪く、利用者の安全と健康が損なわれるおそれがある。

【基本対策】

対策①：空気環境の確保

定期的な換気の実施、または換気用設備の設置等により空気の入れ換えを行い、利用者が不快と感じることのないような空気環境を確保する。

喫煙室を設ける場合は、室外に煙が流出しない措置を行う、標識の掲示を行うなど健康増進法に基づく対策を行う。

対策②：室温・湿度の確保

温度調整、湿度調整ができる空調設備の設置等により、快適な室温・湿度を確保する。

対策③：視環境の確保

作業に適した明るさを確保する。また、明暗の対照が著しくなく、まぶしさを生じさせないような室内照明の選定・設置をする。

太陽光が差し込む場合は、窓にブラインドを設置するなどの対策を実施する。

☝対策事例③を参照。

対策④：騒音の低減措置

外部や情報機器または周辺機器から不快な騒音が発生する場合は、騒音の低減措置をする。また、低騒音型の情報機器を選定・設置する。

対策⑤：作業空間の確保

手足を伸ばせるなど、作業に支障のない十分なスペースを各利用者が確保できるようにする。

対策⑥：事務作業に適した椅子、机の設置

事務作業に適した椅子（キャスター付、肘掛け付、座面の高さ・背もたれの調整機能付等）、机（情報機器作業に必要なもの（キーボード、書類、マウス等）が適切に配置できる広さ、足が窮屈でない大きさ、高さ調整機能付等）を設置している。

☝対策事例①②を参照。

対策⑦：水分補給できる環境の確保

容易に水分補給ができるようにする。

☝対策事例④を参照。

対策⑧：定期的な清掃による清潔・安全な環境の確保

定期的に清掃する仕組みを設け、テレワーク施設運営事業者のスペースを含め施設全体の清潔を保つ。また、通路や棚に物が山積して、転倒や物の落下が生じる事態とならないよう整理整頓する。

地震の際などに物の落下や家具の転倒が起こらないよう、必要な措置を講じる。

電気コード、プラグ、コンセント、配電盤は良好な状態で、配線に損傷が生じている箇所がないようにする。

対策⑨：救急用具の設置

利用者の万が一の負傷に備え、救急用具及び材料を備えている。

対策⑩：便所の確保

利用者の人数や性別に応じた一定数の便所を確保する。

【応用対策】

対策⑪：休憩室の設置

利用者の疲労解消等のため、休憩やストレッチのできるスペースを設ける。

対策⑫：点検リストの作成および定期点検の実施

上記【基本対策】に掲げた項目を満たしているかを確認するための点検リストを作成し、定期的に点検を行う。

対策⑬：衛生管理の知識の習得

利用者の快適な作業環境の確保のため、衛生推進者養成講習の受講など衛生管理の知識を習得する。

【対策事例】

事例①：事務用机、椅子の導入

事務機器メーカーが事務所用に提供する机や椅子で、座面の高さ・背もたれの調整機能が容易に行えるものを導入する。

事例②：事務用機器等の設置又は貸出サービスの導入

作業に適した環境の確保のため、事務用機器（外付けディスプレイ（輝度又はコントラストの調整機能付、ブルーライトカット機能付、位置・向きの調整機能付、目的に応じたサイズ)、外付けキーボード、マウス、パームレスト、テンキー入力機器、パソコンスタンド、充電ケーブル、アダプタ、Webカメラ、スピーカーマイク等）の設置、または貸出サービスを導入する。

より作業を快適に行えるようクッション、ひざ掛け等の設置、または貸出サービスを導入する。

事例③：照度の確認、グレアの抑止等

事務用机やオンライン（Web）会議室等の作業面の照度を測定し、照度の不足やグレアが生じている場合は、照明器具の見直し、間接照明の設置、窓にブラインドを設置するなどの対策をする。

事例④：ウォーターサーバー等の導入

水分補給ができるようウォーターサーバー、自動販売機等を設置する。

第７章. 施設環境管理

【脅威】

- 通信、会議室、電話・オンライン（Web）会議ブース、ワークスペースが利用しにくい、快適でない等、安心して働ける環境として不備がある。
- 休憩できる場所がない、利用しにくい、清潔でない等、適切な休憩を確保できる環境として不備がある。
- 利用者に施設の利用ルールが明示されておらず、不安や不満感が生じる。
- 利用者への適度な声掛けやアンケートなど、意向を聞く、相談を受付ける仕組みに不備があり、不安や不満感が生じる。
- 災害等緊急事態にあたって、施設内待機、施設からの退去、施設閉鎖、避難誘導、必要な物品の整備等、事業継続計画（BCP）に係る手順や周知に不備がある。

【基本対策】

対策①：災害等緊急事態対応方針の整備

災害等緊急事態に対処するための方針を決め、対策を文書化・周知する。最寄りの警察署等の緊急連絡先を従業員に周知する。利用者の急病時の対応方針を従業員に周知する。

☝対策事例①④を参照

対策②：高速通信の確保

時間帯や場所を問わずスピードテストでビデオ通信に適するレベルの速度を確保する。

対策③：通信へのアクセスが容易かつセキュア

通信へのアクセス手順が容易であるとともに、セキュリティも適切に確保する。

対策④：利用者とのコミュニケーション

利用者へのアンケートやコミュニケーションを適時実施し、利便性や快適性などに対する意見やクレームを収集し、その結果と対策状況を利用者に明示する。混雑状況や利用者の意見をもとに、適切な施設整備、会員数、利用者数となるよう運営する。

☝対策事例①②③を参照

対策⑤：目的によるスペースの分離

作業を目的としたスペースと、交流兼休憩を目的としたスペースとを分離し、それぞれ適切な環境を整備する。イベント開催用のスペースは作業を目的としたスペースと分離するか、事前にイベント開催の情報を利用者へ周知する運用を確立する。

☝対策事例⑤を参照

対策⑥：利用ルールの策定、周知

通話の可否、食事の可否等、空間の利用ルールを策定し掲示等で周知する。

☝対策事例⑤を参照

【応用対策】

対策⑦：BCP策定、周知、対処

BCPに係る施設の対応方針が文書化され、利用者、従業員に適切に周知されており、方針に沿った対処が可能となっている。

☝対策事例①を参照

【対策事例】

事例①：従業員教育、処遇

適切に利用者対応ができるよう従業員の教育内容を工夫し実施するとともに、従業員が習得すべきスキルを明示し、習得できた場合には適切に処遇する。

事例②：室内状況の計測・可視化と、基準の明示

温湿度計、CO2モニタ等を設置して空間の状況を計測・可視化するとともに、施設としての基準値を明示し、空間を基準値の範囲に保つ。

事例③：衛生用品の設置

ハンドソープ、除菌スプレー等、利用者の衛生を保つための備品を設置する。

事例④:従業員の健康管理

勤務前に検温と健康観察と行い、体調不良の場合は勤務を見送るよう従業員へ周知する。また、従業員が急遽欠勤しても代替要員を配置できるよう人員計画を行う。

事例⑤：会議室、電話・オンライン（Web）会議ブースの確保

利用者同士の作業音が気にならないよう、防音やサウンドマスキング等の対策をとる。

コラム

無線LANのセキュリティ方式

無線LANのセキュリティ方式には、「WEP」「WPA」「WPA2」「WPA3」があり、それぞれ以下の特徴があります。

	WEP※	WPA※	WPA2	WPA3
安全性	×	×	○	◎
推奨内容	容易に解読されてしまう方式のため、利用を控えてください。	短時間で解読する方法が発見されている方式のため、利用を控えてください。	WPAより強固な方式ですが、脆弱性も発見されています。この脆弱性は、無線LANアクセスポイントのファームウェアをアップデートすることで安全性を確保できます。	WPA2よりも更に安全性を高めた方式で現在最も推奨されます。今後、無線LANアクセスポイントを導入される場合には、WPA3に対応する機器を導入されることを推奨します。
暗号鍵の配布方法	同一SSID内のAP及び全接続端末で同じWEPキーを使用	同一SSID端末内で、同一の事前共有鍵(PSK)を共有する「パーソナル」とIEEE 802.11X認証サーバから端末ごとに個別のキーを配布する「エンタープライズ」モードの2種類が存在		
暗号方式	WEP(RC4)	TKIP(RC4)必須 AES (CCMP)オプション	AES (CCMP)必須 TKIP(RC4)オプション	AES/CNSA (CCMP)
鍵長	40/104bit	104bit	128bit	128/192bit

無線LANアクセスポイントを利用する場合には、WPA2（ソフトウェアアップデートが適切に行われているもの）を利用するか、大幅にセキュリティが向上しているWPA3に対応したものを導入し、利用することを徹底してください。

※ WEP：Wired Equivalent Privacy

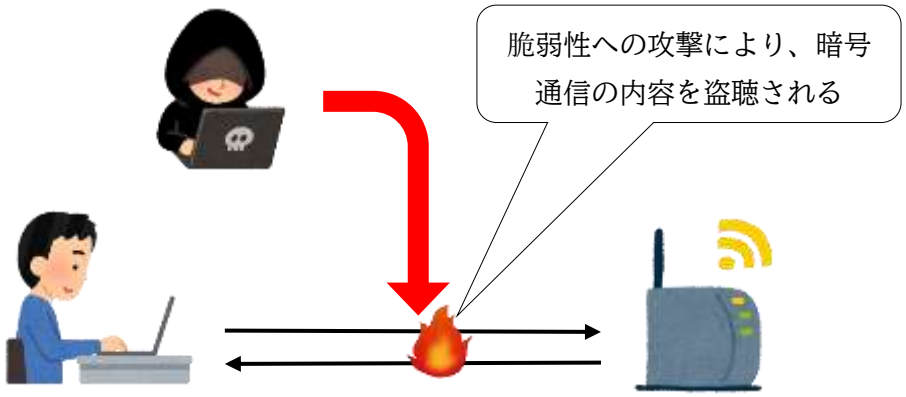
※ WPA：Wi-Fi Protected Access

WPA2の脆弱性

WPA2は広く利用されている無線LANのセキュリティ方式ですが、2018年10月16日に、暗号鍵を特定されるなど複数の脆弱性が公開されました。この脆弱性に対応するソフトウェアアップデートがされないまま利用を続けると、同じ無線LANアクセスポイントの通信範囲内にいる第三者により、不正アクセスによる情報の盗聴が行われる可能性があります。

（不正アクセス方法の一例）

- ツールを用いた暗号化方式のクラッキング
- デフォルトでのSSIDに含まれる、無線APの機器名・バージョン情報等からの脆弱性、初期パスワード等の攻撃者にとって有益な情報の入手
- 無線AP機器にはWPS(Wi-Fi保護セットアップ)機能の無断利用
- MACアドレスフィルタリングを実施している場合の不正アクセス



この脆弱性の対策には、無線LANアクセスポイントのベンダから提供されている最新のファームウェアを適用（更新）することが必要です。発売されて時間の経過した、古い無線LANアクセスポイントを利用している場合には、ファームウェアが提供されていないことがありますので、その際には最新のものへ入れ替えてください。

また無線LANに関する規格を策定する業界団体であるWi-Fi Allianceにより、2018年6月25日に新規格である「WPA3」が発表されました。WPA3では大幅にセキュリティが強化されています。

今後、新たに無線LANアクセスポイントを設置・入替する際には、適切なファームウェエアアップデートがされたWPA2かWPA3に対応した機器を選択してください。

ネットワーク分離機能

ネットワーク分離機能（プライバシーセパレーターとも言う）は、無線LANアクセスポイント（以下「AP」といいます。）に接続している端末同士のアクセス（例：共有フォルダへのアクセス）を禁止することができる機能です。利用者のセキュリティ保護のため、この機能を使用してください。

ただし、複数のAPがある場合において、片方のAPに接続している端末から、別のAPに接続している端末に対しての通信は禁止できません。

電子証明書の活用（IEEE802.1x認証）

電子証明書を活用したIEEE802.1x認証は、無線LANを利用するクライアントと、無線LANアクセスポイントの双方でIEEE802.1xにおける認証プロトコルを使用し、認証にはRADIUS（Remote Authentication Dial-In User Service）サーバを利用することで、無線LANの利用において認証機能を付加する方式です。802.1x認証や、1x認証という言い方をする場合もあります。

RADIUSサーバで認証の許可や拒否を行うことで、未認証のクライアントからの不正アクセスを排除することが可能なため、電子証明書を利用したIEEE802.1x認証を行うことを推奨します。

認証方式	EAP-TLS	EAP-TTLS	EAP-PEAP
概要	電子証明書を用いるため、セキュリティ強度が強い	ID/パスワードを用いるため、認証情報を類推、詐取される可能性がある	ID/パスワードを用いるため、認証情報を類推、詐取される可能性がある
端末側の認証	電子証明書	ID/パスワード	ID/パスワード
サーバ側の認証	電子証明書	電子証明書	電子証明書

ゼロデイ脆弱性を利用した攻撃

脆弱性（セキュリティホール）とは、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを言います。サイバー攻撃においては、この脆弱性を利用した、情報の盗難、機器の利用停止、情報の改ざんなどが行われます。脆弱性を利用した攻撃を実行するためのツールはインターネット上で容易に手に入り、特別な知識がなくても攻撃は可能です。脆弱性と対応策は以下に分類されます。

名称	概要	対策の提供	情報の公開	攻撃手法及び対応
ゼロデイ脆弱性	脆弱性のうち、開発元などによる対策方法や修正プログラムなどが未だ提供されていないものです。	無し	無し	一部の開発者や攻撃者は知っているが、一般ユーザーは脆弱性があることを知ることができず、対応は不可能です。
			有り	対策方法や修正プログラムなどが提供されない段階で、脆弱性の存在が公表されると、攻撃手法が広く知られる一方で、ユーザーは対策が難しい状態となり、非常に危険な状態となります。ユーザーは対策が可能になるまで、その機器やソフトウェアの利用を一時的に取りやめるなど、負担の大きな対応が必要になります。
Nデイ脆弱性	脆弱性が発見された何らかのシステムに対して、提供された修正プログラムのリリースと、その修正プログラムが適用されるまでの時間に存在する脆弱性のことです。	有り	有り	既知の脆弱性を悪用した攻撃ですが、修正プログラムが適用される前に仕掛けられる攻撃のため、ソフトウェア管理が不適切な組織が標的となりやく、修正プログラムからより詳細な脆弱性情報を入手できるため、攻撃ツール作成の難易度が下がり、攻撃者がNデイ脆弱性を利用する頻度は高くなります。修正プログラムが公開された場合、速やかに対応する必要があります。

パスワード強度

安全且つ推測されにくいパスワードを作成するためには、以下のような考え方が参照いただけます。

1. ランダムパスワード

   スマホアプリ、Webアプリ等のツールを利用してランダムに生成させるパスワードです。桁数、文字種等の条件を指定すれば、推測されにくいパスワードをツールが自動的に生成します。

   ただし、機械的に無意味な文字列を作りますので、使用頻度の少ないものを多数覚えるのは非常に難しいです。一時的に設定し、初回ログイン後にすぐ変更する、初期パスワード等に向いています。

2. パスフレーズ

   「パスワード」の一種で、一般的には、文字数が多いものを「パスフレーズ」といいます。「パスフレーズ」は、自分が覚えやすい文章をアルファベットにして、パスワードを作ることで、覚えやすく、見破られにくいパスワードを作ります。例えば、「Jiro is my dog」のような文章から、「JiroIsMyDog」というパスフレーズを作成します。

   ただし、「thankyouverymuch」等の一般的な文章は利用してはいけません。また、特殊文字や数字が必要な場合には、空白部分を特殊文字にしたり、数字を付加したりする等して対応します。例えば、「JiroIsMyDog#65」等

3. コアパスフレーズ

   自分の趣味や興味のあること等から決めたフレーズを基に、任意の変換ルールを適用して、憶えやすく、強度の高いパスワードを作成します。これを全てのパスワードに共通して使用する「コアパスワード」とし、更にフレーズを付加して、パスワードを生成します。

   例えば、[2.パスフレーズ]を、フレーズとしてコアフレーズを作成した場合、「Jimd#APlOO」になります。これは、パスフレーズの単語の先頭文字のみつなげて、「#」の後ろに機器を識別する任意のコードと番号を組み合わせしたものです。

【参考：内閣サイバーセキュリティセンター インターネットの安全･安心ハンドブックP10 パスワードの安全性を高める】https://security-portal.nisc.go.jp/guidance/pdf/handbook/NISC_handbook_general.pdf

情報の機密性・完全性・可用性

情報セキュリティとは情報の機密性・完全性・可用性を維持することであると定義されています。

個人情報やネットワーク機器等の情報資産を扱うには、機密性・完全性・可用性を確保しないとセキュリティ事故の原因になります。機密性・完全性・可用性には、それぞれ以下の特徴があります。

	機密性（Confidentiality）	完全性（Integrity）	可用性（Availability）
観点	漏れてはいけない	変更されてはいけない	止まってしまってはいけない
脅威	情報の漏えい・流出・盗聴・盗難、システムの不正利用・侵入など	情報の改ざん・混入、サーバの誤処理、許可の無いシステムの改変・改造など	情報の損失・破壊、サーバやシステムの停止、環境的要因（火災等）による事業の停止
脅威の例	利用者情報（氏名、電話番号、クレジットカード情報等）が大量に外部漏えいする	利用者情報を許可なく変更することで、利用者本人がテレワーク施設を突然利用できなくなる	回線障害、機器の故障、マルウェア感染等で、サービスや施設が利用できなくなる

事務所衛生基準規則

厚生労働省が2021年3月に公表した「テレワークの適切な導入及び実施の推進のためのガイドライン」（以下「厚労省テレワークガイドライン」といいます。）の事業者向けチェックリストの「3.作業環境」「(1)サテライトオフィス型）「労働安全衛生規則や事務所衛生基準規則の衛生基準と同等の作業環境となっていることを確認した上でサテライトオフィス等のテレワーク用の作業場を選定しているか。」に記載のある「事務所衛生基準規則（以下「事務所則」といいます。）」は、労働安全衛生法に基づき事務所の衛生基準について定めた厚生労働省令です。この事務所則の内、テレワーク施設に関係の深い項目について下表に抜粋してご紹介します。

詳細は事務所衛生基準規則をご参照ください。

項目			基準
環境管理	空気環境	気積	10立方メートル/人以上とすること
		空気調和設備	一酸化炭素：10ppm以下 二酸化炭素：1,000ppm以下　とすること 気温　　：18℃以上28℃以下になるよう努めること 相対温度　：40％以上70％以下になるよう努めること
		燃焼器具	排気筒、換気扇その他の換気のための設備を設けること
	採光・照明	照度	300ルクス以上とすること
		採光・照明	明暗の対照を少なくすること（局所照明と全般照明を併用） まぶしさをなくすこと
清潔	便所		① 男性用と女性用に区分すること ② 男性用大便所は、60人以内毎に1個以上とすること ③ 男性用小便所は、30人以内毎に1個以上とすること ④ 女性用便所は、20人以内毎に1個以上とすること
休養	休養室等		50人以上又は女性30人以上の労働者を使用する場合は、休養室又は休養所を男性用と女性用に区別して設けること
救急用具			負傷者の手当に必要な救急用具及び材料を備え、その備付け場所及び使用方法を労働者に周知すること

情報機器作業における労働衛生管理のためのガイドライン

厚労省テレワークガイドラインの「自宅等でテレワークを行う際の作業環境整備の留意点」に記載のある「情報機器作業における労働衛生管理のためのガイドライン（以下「情報機器作業ガイドライン」といいます。)」は、事務所において行われるパソコンやタブレットなど情報機器を使って作業を行う労働者の健康を守るためのガイドラインです。この情報機器作業ガイドラインの内、テレワーク施設に関係の深い項目について下表に抜粋して紹介します（一部分かりやすく改変)。
詳細は情報機器作業ガイドラインをご参照ください。

項目	基準
照明及び採光	・ 室内は、できる限り明暗の対照が著しくなく、かつ、まぶしさを生じさせないようにすること ・ ディスプレイを用いる場合の書類上及びキーボード上における照度は 300 ルクス以上とし、作業しやすい照度とすること ・ ディスプレイ画面に直接又は間接的に太陽光等が入射する場合は、必要に応じて窓にブラインド又はカーテン等を設け、適切な明るさとなるようにすること ・ 間接照明等のグレア防止用照明器具を用いること
情報機器	・ ディスプレイは、輝度やコントラストの調節機能があること。また、画面の位置、前後の傾き、左右の向きの等の調整機能があること ・ キーボードは、ディスプレイから分離して、その位置が作業者によって調整できること ・ 数字を入力する作業が多い場合は、テンキー入力機器を利用できるようにすること
椅子	・ 安定しており、かつ、容易に移動できること ・ 床からの座面の高さは、作業者の体形に合わせて、適切な状態に調整できること ・ 適当な背もたれを有していること。また、背もたれは、傾きを調整できること ・ 必要に応じて適当な長さの肘掛けを有していること
机又は作業台	・ 作業面は、キーボード、書類、マウスその他情報機器作業に必要なものが適切に配置できる広さであること ・ 作業者の脚の周囲の空間は、情報機器作業中に脚が窮屈でない大きさのものであること ・ 床からの高さは作業者の体形にあった高さに調整できること

騒音の 低減措置	情報機器及び周辺機器から不快な騒音が発生する場合には、騒音の低減措置を講じること

テレワーク施設における端末の同時接続台数

テレワーク施設の利用者は１人でパソコン・スマートフォン・タブレットなどの端末を複数台数 Wi-Fi 接続をすることが多くあります。従いまして、同時に利用する人数の最大想定人数の３倍程度の台数が同時に接続しても耐えられるように設計する必要があります。共有ワークスペースにおいて、Wi-Fi の速度が遅くなったり不安定になったりする原因として、回線の通信速度の問題ではなく、ルーターやアクセスポイントの推奨接続台数を超えた機器が接続されていることも考えられます。通信上の不安定さを無くすためにも、例えば 30 名程度収容の施設であれば、100 台程度は端末が同時接続できる仕様の機器を用意したいところです。

（参考）チェックシート

要件	基本対策	応用対策
１．セキュリティ管理体制の構築		
対策①：情報セキュリティポリシーの策定		
テレワーク施設における情報セキュリティに関する考え方や責任体制などを明文化したポリシー（基本方針）を策定していますか？	Y / N	
利用者に対してポリシーを明示していますか？	Y / N	
ポリシーで定めた対策を実施し、情報セキュリティの脅威に変化が発生した場合は見直していますか？	Y / N	
対策②：利用規約の策定・利用者の同意		
テレワーク施設の利用規約を策定していますか？	Y / N	
利用申請や登録時に利用者が規約に同意したことを確認し、記録していますか？	Y / N	
対策③：施設の保有する情報（データ）の保護		
テレワーク施設の運営・管理において取り扱う情報は、漏えいや改ざん、不正利用等から保護するために、必要な対策を実施していますか？	Y / N	
対策は情報の機密性、完全性、可用性の確保を考慮できていますか？	Y / N	
対策④：セキュリティ事故発生対応マニュアルの策定		
セキュリティ事故発生時の具体的対応を記したマニュアルを策定していますか？	Y / N	
マニュアルに基づき、利用者には事前に利用規約等で、サービス上の不具合やマルウェア感染、情報漏えい等の疑いが発生した場合の連絡、対応方法を明示していますか？	Y / N	
対策⑤：セキュリティ教育、研修、訓練の実施		
テレワーク施設の経営者を含む全従業員に対し、「情報セキュリティポリシー」及び「セキュリティ事故発生対応マニュアル」等の重要事項について内容周知していますか？	Y / N	
定期的に教育や研修、マルウェア感染等を想定した訓練等を実施し、その活動を記録に残していますか？	Y / N	

対策⑥：最新の情報セキュリティ情報の収集・確認		
サイバー攻撃やマルウェア感染等、情報セキュリティに関する最新の脅威動向や個人情報保護法等の関連法令の情報を定期的に確認し、把握していますか？	Y / N	

２．個人情報・利用者管理		
対策①：個人情報保護ポリシーの策定		
利用者及び従業員から取得する個人情報の保護対策や責任体制などを明文化したポリシー（基本方針）を策定し、利用者及び従業員に明示していますか？	Y / N	
利用目的の変更等、内部外部における状況変化があった場合に見直しをしていますか？	Y / N	
対策②：個人情報の適切な管理		
個人情報保護ポリシーの利用目的に基づいて、個人情報が適切に取得・提供されているか、利用終了とともに速やかに情報が廃棄されているか、定期的に確認できていますか？	Y / N	
取得・提供した個人情報は台帳等によって管理され、テレワーク施設の管理者等によって棚卸し（例：年１回）されていますか？	Y / N	
対策③：テレワーク施設が提供する Web サイトの適切な管理		
提供する Web サイトにおいて、利用登録や問い合わせ等の個人情報を入力・送信させる場合は、TLS（https）通信の設定を実施していますか？	Y / N	
Web サイト構築・運用に当たって、脆弱性への対応を実施していますか？	Y / N	
対策④：利用ログの取得・管理		
個人情報の漏えいやセキュリティ事故発生時に原因調査を行うために、提供するWebサイトの利用ログ（利用者、利用時間、利用リソース等）を取得していますか？	Y / N	
取得した利用ログは許可無く利用されないようにかつ外部に漏えいしないように適切に保存・管理できていますか？	Y / N	

3. 入退室管理		
対策①：利用者の本人確認		
利用しようとする者に対して、写真付き身分証明書（マイナンバーカード、運転免許証、パスポート等）によって、本人確認を行った上でテレワーク施設の利用登録（許可）を行っていますか？	Y / N	
利用登録（許可）された者以外は原則入場・利用ができないようにしていますか？	Y / N	
会員制のテレワーク施設においては、会員のゲスト（一時的な利用者、打ち合わせ等で会員を訪問した者等）についても、本人確認に加えて、入室可能なエリアやネットワーク接続時の制限事項など個別の利用規約を示していますか？	Y / N	
対策②：入退室記録・ログの取得・管理		
利用者の入場時は、1 人ずつ入場を確認し、入場記録がない場合は、身元及びその理由を確認できるまで、退場を許可しないようにしていますか？	Y / N	
入退室記録又は電子的ログ（利用者、利用時間、利用リソースなど）を取得し、適切に一定期間保存（例：1 年間）・管理していますか？	Y / N	
対策③：入退出管理システム等の管理者パスワード設定		
入退室管理を行う PC 等機器やシステムには、それを管理する者だけが知るパスワード（管理者パスワード）を設定していますか？	Y / N	
紙ベースで管理する場合は、管理者だけが持つ鍵で施錠していますか？	Y / N	
管理者パスワードは定期的に更新する必要はないが、アルファベット（大文字、小文字）、数字、記号を組み合わせた十分な長さの文字列で、第三者に推測されにくい複雑なパスワードに変更していますか？	Y / N	
パスワードや鍵の共有範囲は業務上必要な最小限の範囲に止め、管理者の従業員が異動・退職する際には、速やかにパスワードを変更し、鍵を回収していますか？	Y / N	

対策④：電子的・生体認証による入退出管理システムの導入		
IC カード型やスマートフォンアプリ型会員証など電子的に入退出の管理ができるシステムや静脈認証、指紋認証、虹彩認証など生体情報を使った認証システムを導入し、利用者を特定でき、記録漏れとなりすましを抑止できる仕組みを導入していますか？		Y / N

4. ネットワークセキュリティ		
対策①：セキュリティアップデートの実施		
ネットワーク構築、運用にあたって、セキュリティ上の脅威が発生しないように、機器のOSやファームウェア、アプリケーション等が最新化されるよう、定期的に状態を確認し、更新していますか？	Y / N	
自動的にアップデートする機能がある場合には、それを有効にしていますか？	Y / N	
最新化できない場合はその理由と、他の方法による対策の検討、今後の対応計画及び進捗状況についてまとめ、記録していますか？	Y / N	
メーカーサポートが終了したネットワーク機器等を使用しないようにしていますか？	Y / N	
対策②：初期設定の変更		
ネットワーク機器等が、家庭や同一組織内での利用を想定した初期設定（デフォルト値）となっている場合、テレワーク施設での利用にあたって、適切なパラメータ設定となっているか確認し、変更していますか？	Y / N	
NTP による自動的な時刻合わせが可能な機器については、その設定を実行していますか？	Y / N	
対策③：管理者パスワードの適切な設定		
ネットワーク機器等のパラメータ設定を変更するための管理者パスワードは、工場出荷時の値から変更していますか？	Y / N	
管理者パスワードはアルファベット（大文字、小文字）、数字、記号を組み合わせた十分な長さの文字列で、第三者に推測されにくい複雑なパスワードに変更していますか？	Y / N	
管理者パスワードの共有範囲は最小限にし、管理者パスワードを知る者が異動・退職する場合は速やかに変更していますか？	Y / N	
対策④：無線 LAN アクセスポイントの適切な設定		
無線LANアクセスポイントを提供する場合、セキュリティ方式としてWPA2（適切にアップデートされたもの）又はWPA3を設定し、暗号化方式はAES（CCMP）にしていますか？	Y / N	
WEP及びWPAは脆弱性があるため使用しないようにしていますか？	Y / N	
テレワーク施設の境界から外に漏れる無線電波が最小限となるよう留意していますか？	Y / N	

対策⑤：無線 LAN アクセスポイントの利用者接続パスワード設定と管理		
利用者に配付する接続パスワードは、管理者パスワードとは全く別のものを設定し、利用しない者がパスワードを知りうる機会を抑制するため、定期的（年1回以上）に変更していますか？	Y / N	
対策⑥：利用者の端末間通信の禁止設定		
利用者が別の利用者の端末にアクセスできないように、無線 LAN アクセスポイントの設定において「ネットワーク分離機能」や「プライバシーセパレーター機能」を有効化していますか？	Y / N	
複数の無線 LAN アクセスポイントを利用している場合や有線 LAN でのアクセスを提供している場合、接続されるスイッチやルーターの特定ポート間通信を禁止するなど設定していますか？	Y / N	
利用者の端末間通信を禁止し、特定のネットワーク機器等やポートを利用する場合には、安全な利用が確保できるよう適切に設定していますか？	Y / N	
対策⑦：業務用ネットワークとの分離		
利用者が利用するネットワークから、テレワーク施設事業者の業務システム等のネットワークにアクセスできないようにするため、利用者に提供するネットワークは、業務システム等とは独立して設置するか、安全に分離していますか？	Y / N	
対策⑧：アクセス制御		
ルーターの WAN 側ポートを除いて、ネットワーク機器等にはインターネット側からアクセスできないようにし、複合機は原則として外部ネットワーク（インターネット）に接続できないようにしていますか？	Y / N	
ベンダのリモート保守等で接続する必要性がある場合は、ファイアウォール等を設置した上で、接続 IP アドレスやポートを制限するなど、セキュリティ対策を実施していますか？	Y / N	
対策⑨：アクセスログの適切な管理		
個人情報の漏えいやセキュリティ事故発生時に原因調査を行うために、ネットワーク機器等でNTPによる自動的な時刻合わせが可能な機器についてはその設定を実施し、アクセスログ（接続日時、回数、接続位置、接続先、端末情報等）を取得していますか？	Y / N	

取得したアクセスログは、高いプライバシー性を持つ情報であることから、業務上の必要性に応じた最小限の記録と利用範囲に留め、許可無くマーケティング利用や第三者提供されないようにアクセスを制限していますか？	Y / N	
アクセスログは、セキュリティ事故発生時の原因調査に必要な証跡となることから一定期間保管していますか？	Y / N	
ネットワーク機器の運用を事業者に委託している場合は、アクセスログもその委託先事業者において記録・保存されているため、その記録内容や保存期間等を把握し、問い合わせがあった場合の対応方法を委託先事業者と確認していますか？	Y / N	
対策⑩：複合機に蓄積されたデータの消去		
複合機で入出力したデータが内蔵記録装置（ハードディスク等）に保存され続けないように「暗号化」や「自動消去」機能を有効、または定期的に手動で消去するなど対策していますか？	Y / N	
対策⑪：複合機の出力管理		
複合機から出力した書類や原本書類の第三者による持ち去りや、放置を禁止する事項を利用規約に含めるとともに、注意喚起を行っていますか？	Y / N	
対策⑫：レンタル PC		
PC、タブレット等の端末をサービス貸与する場合、OSの最新化やウイルス対策ソフトのインストール、定義ファイルの自動更新、リアルタイムスキャンの実施等の対策を行っていますか？	Y / N	
対策⑬：高度なセキュリティの導入		
無線 LAN アクセスポイントと接続端末等について、電子証明書等を活用して相互に認証を行い、無線 LAN アクセスポイントのなりすましや許可されていない端末の接続を制限していますか？		Y / N
テレワーク施設から業務で利用するサーバ等へアクセスする場合は、アカウント管理を厳重に行うとともに、多要素認証の仕組み（クライアント証明書など）を導入するなど、不正アクセスのリスクを軽減できるようにしていますか？		Y / N
ネットワーク接続状況を監視するシステムを導入して、接続機器を保護していますか？		Y / N
年 1 回以上の定期的な脆弱性診断を実施していますか？		Y / N

対策⑭：複合機の媒体接続制限		
許可無く複合機に利用者が所有するUSBメモリ等の外部記憶媒体を接続させないように、差し込みポート（インターフェイス）がある場合は、無効化（設定および物理的封印等）していますか？		Y / N
複合機に USB メモリ等の外部記憶媒体を接続許可する場合は、申請式にして利用ログを残すことやウイルススキャンを実行させるなど対策を行っていますか？		Y / N

5. 物理セキュリティ		
対策①：オンライン（Web）会議等への対策		
オンライン（Web）会議を許可する場合は、会議室や専用の個室型ブース等の設置等、音漏れへの対策を実施していますか？	Y / N	
ラウンジ等共有の場で音声利用を行うことによるリスク等について、利用者への注意喚起を行っていますか？	Y / N	
対策②：手荷物の管理		
離席時の手荷物等を放置することによるリスク等について、利用者に注意喚起を行っていますか？	Y / N	
対策③：シュレッダー、溶解 BOX の導入		
重要書類や記憶媒体等を一般ゴミに捨てることによるリスク等について、利用者に注意喚起するとともに、復元処理が困難なセキュリティ性の高いシュレッダー（例：マイクロカット等）や中身の取り出し防止機能の付いた溶解 BOX を設置していますか？	Y / N	
溶解ボックス等、利用可能な状態で廃棄する場合は、廃棄完了証明書等で、適切に処理したことを証明できる事業者選択定していますか？	Y / N	
対策④：サーバ端末の廃棄		
テレワーク施設が保有するサーバや端末を廃棄または返却する際は、物理破壊や信頼性の高い専用ソフトウェアや磁気方式を採用し確実にデータ削除を行っていますか？	Y / N	
対策⑤：ネットワーク機器の設置場所		
ネットワーク機器等は、施錠できるラック等に施錠管理し、アクセスポイントは利用者が直接触れにくい天井の高い位置に設置するなど、許可の無い不正操作を防止する対策を実施していますか？	Y / N	
電源や LAN ケーブル等は、断線や接続不良等を防止するために保護および整線を実施していますか？	Y / N	
対策⑥：サウンドマスキングの導入		
物理的設備で十分な防音を期待できない場合、サウンドマスキングシステムを導入していますか？		Y / N
対策⑥：施錠ロッカーの導入		
安全に手荷物を管理できるように、また作業空間の確保や通路に置くことによるつまずきなどを回避する目的で、施錠可能なロッカーを設置していますか？		Y / N

要件	基本対策	応用対策
６．作業環境管理		
対策①：空気環境の確保		
定期的な換気の実施、または換気用設備の設置等により空気の入れ換えを行い、利用者が不快と感じることのないような空気環境を確保されていますか？	Y / N	
喫煙室を設ける場合は、室外に煙が流出しない措置を行う、標識の掲示を行うなど健康増進法に基づく対策を行っていますか？	Y / N	
対策②：室温・湿度の確保		
温度調整、湿度調整ができる空調設備の設置等により、快適な室温・湿度を確保していますか？	Y / N	
対策③：視環境の確保		
作業に適した明るさを確保していますか？	Y / N	
明暗の対照が著しくなく、まぶしさを生じさせないような室内照明の選定・設置をしていますか？	Y / N	
明暗の対照が著しい、またはまぶしさが生じている場合で、その照明の変更が難しい場合は、間接照明の設置により改善対策をしていますか？	Y / N	
太陽光が差し込む場合は、窓にブラインドやカーテンを設置するなど、作業に適した環境にしていますか？	Y / N	
対策④：騒音の低減措置		
外部や情報機器または周辺機器から不快な騒音が発生する場合は、騒音の低減措置をしていますか？	Y / N	
低騒音型の情報機器を選定・設置していますか？	Y / N	
対策⑤：作業空間の確保		
各利用者に、手足を伸ばせるなど作業に支障のない十分なスペースを確保していますか？	Y / N	
対策⑥：事務作業に適した椅子、机の設置		
事務作業に適した椅子（キャスター付、肘掛け付、座面の高さ・背もたれの調整機能付等）、机（情報機器作業に必要なもの（キーボード、書類、マウス等）が適切に配置できる広さ、足が窮屈でない大きさ、高さ調整機能付等）を設置していますか？	Y / N	

対策⑦：水分補給できる環境の確保		
容易に水分補給ができるようしていますか？	Y / N	
対策⑧：定期的な清掃による清潔・安全な環境の確保		
定期的に清掃する仕組みを設け、事業者のスペースを含め施設内の清潔を保っていますか？	Y / N	
通路や棚に物が山積し、転倒や物の落下が生じる事態とならないよう整理整頓されていますか？	Y / N	
地震の際などに物の落下や家具の転倒が起こらないよう、必要な措置を講じていますか？	Y / N	
電気コード、プラグ、コンセント、配電盤は良好な状態で、配線に損傷が生じている個所などはないか？	Y / N	
対策⑨：救急用具の設置		
利用者の万が一の負傷に備え、救急用具及び材料を備えていますか？	Y / N	
対策⑩：便所の確保		
利用者の人数や性別に応じた一定数の便所を確保していますか？	Y / N	
対策⑪：休憩室の設置		
利用者の疲労解消等のため、休憩やストレッチのできるスペースを設けていますか？		Y / N
対策⑫：点検リストの作成および定期点検の実施		
【基本対策】に掲げた項目を満たしているかを確認するための点検リストを作成していますか？		Y / N
作成した点検リストに基づき、定期的に点検を行っていますか？		Y / N
対策⑬：衛生管理の知識の習得		
利用者の快適な作業環境の確保のため、衛生推進者養成講習の受講など衛生管理の知識を習得していますか？		Y / N

要件	基本対策	応用対策
７．施設環境		
対策①：災害等緊急事態対応方針の整備		
災害等緊急事態に対処するために方針が決まっており、対策が文書化され周知されていますか？	Y / N	
最寄りの警察署等の緊急連絡先が従業員に周知されていますか？	Y / N	
利用者の急病時の対応方針が従業員に周知されていますか？	Y / N	
対策②：高速通信の確保		
時間帯や場所を問わずスピードテストでビデオ通信に適するレベルの速度が確保できていますか？	Y / N	
対策③：通信へのアクセスが容易かつセキュア		
通信へのアクセス手順が容易であるとともに、セキュリティも適切に確保できていますか？	Y / N	
対策④：利用者とのコミュニケーション		
適度な声掛けやアンケートによる利用者の意向や、相談を受付ける仕組みができていますか？	Y / N	
対策⑤：目的によるスペースの分離		
作業するスペースと、交流兼休憩を目的としたスペースとが分かれていますか？	Y / N	
イベント開催用のスペースが作業を目的としたスペースと分かれているか、事前にイベント開催の情報を利用者へ周知する運用が確立していますか？	Y / N	
対策⑥：利用ルールの策定・周知		
施設の利用ルールが初めての利用者にもわかりやすく明示されていますか？	Y / N	
対策⑦：BCP 策定、周知、対処		
BCP に係る施設の対応方針が文書化され、利用者、従業員に適切に周知されており、方針に沿った対処が可能となっていますか？		Y / N