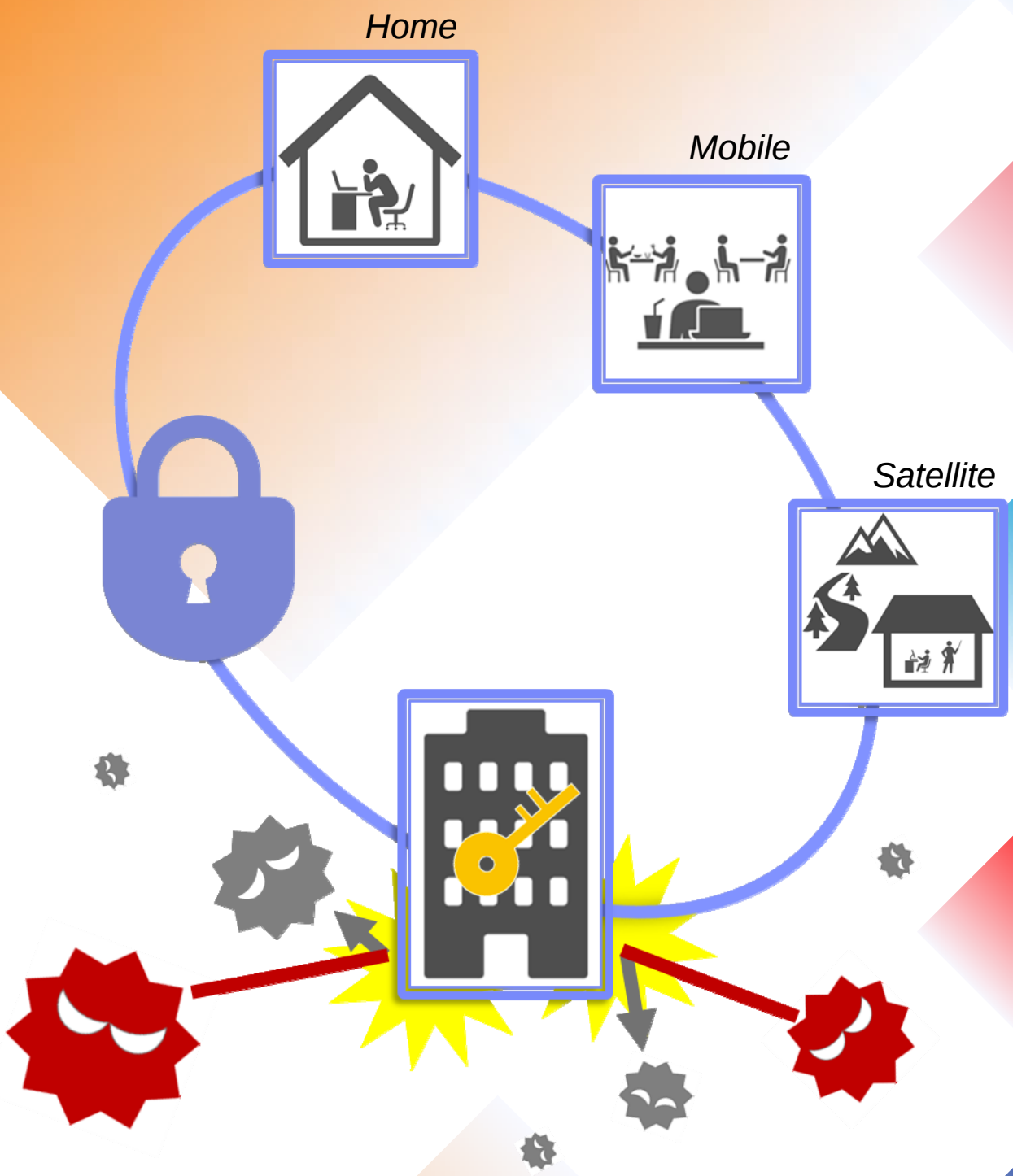
別紙3

テレワークセキュリティガイドライン
第4版



平成30年4月

総務省

全体目次

本ガイドラインで示す対策の区分について

２２ページ以降に示す対策は、重要度に応じて次の２種類に区別しています。

基本対策事項（オレンジ色の枠囲み）

テレワークに関わるすべての関係者が実施すべき、基本的な対策です。

推奨対策事項

はじめてセキュリティ対策を導入する場合などは後回しにしても構いませんが、安全なテレワーク環境を実現するためには実施することが望ましい対策です。

用途別目次

＜テレワーク勤務者が参照すべき項目の一覧＞

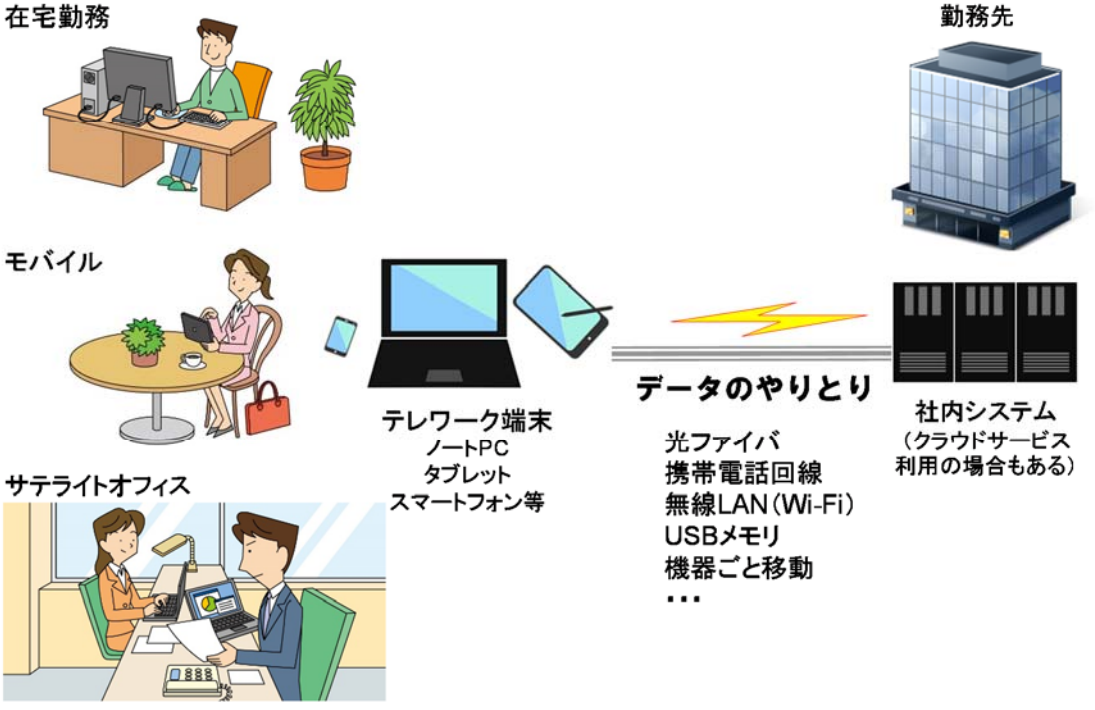
＜テレワークトラブル事例と対策一覧＞

はじめに

最近、社会のいろいろな場面において、「テレワーク」（下記囲み参照）の活用が進んでいます。テレワークにより時間や場所を有効に活用した就労・作業形態は、企業にとっての競争力強化のみならず、新しいビジネスの創出や労働形態の改革、事業継続の向上をもたらすとともに、多様化する個々人のライフスタイルに応じた柔軟かつバランスのとれた働き方の実現に寄与しています。テレワークは、少子・高齢化対策、経済再生、雇用創出、地域振興、防災・環境対策などの様々な目的でも効果があることが認められており、テレワークが今後いっそう普及することで、より創造的な能力を効率的に発揮し得る社会の実現が期待されます。

テレワークとは

情報通信技術（ICT）の利用により時間・空間を有効に活用する多様な就労・作業形態をいい、本ガイドラインでは以下の３つの形態の総称として使用します。



こうしたテレワークを効率的に実施するためには、ICTの活用が欠かせません。自宅や外出先で作成したファイルをインターネットを通じてすぐにオフィスに送ったり、テレワーク勤務者同士でビデオ会議をすることで、オフィスで働いているのとほぼ等しい効率で仕事を進めることができるようになっています。以前は、オフィスの外で仕事を行うというと、必要な資料が手元に用意できないため不便であるとか、情報が外部に漏洩する恐れがあって危険であるなどと考えられていましたが、インターネットの高速化や、暗号化などの情報セキュリティ技術の活用などにより、こうした問題も障害ではなくなっています。日本に限らず世界中の企業で在宅勤務などのテレワークを認めていることが、それを裏付けています。情報セキュリティ対策をしっかり行った上でテレワークを実施することが、今後の企業価値を高めることや経営戦略にとって重要な企業の社会的責任（CSR）の見える化に繋がるものと期待されます。

本ガイドラインは、こうした背景をもとに、これからテレワークを導入しようと考えている企業において、情報セキュリティ対策に関する検討の参考としてもらうことを目的として策定されたものです。オフィスの外で仕事を行う際には、その形態に応じて様々なリスクがありますが、そのリスクについての対策もそれぞれに用意されています。そうした対策をどのように選び、継続的に安全を確保していくかについての基本的な考え方を、本ガイドラインを通じて身につけてください。なお本ガイドラインに書かれている対策は、企業に所属しない個人事業主などの立場でテレワークをされている方にとっても、参考にできるように書かれています。この場合、本ガイドラインにおいて「経営者向け」「システム管理者向け」として書かれている内容についても考慮することが望まれます。

本ガイドラインは、多くの企業にとって参考としやすいように、我が国の企業の多くで採用されている情報セキュリティ対策の考え方をベースとして対策を説明しています。また、これまで業務でインターネットを活用していなかった企業にとっても、内容が簡単に分かり、どのような対策をすればよいかを判断しやすいものとするための工夫を行いました。具体的には、まずテレワークにおける情報セキュリティ対策のポイントを一通り示した上で、具体的な対策の考え方について紹介するという構成としています。

なお、本ガイドラインで示した内容は、あくまでも基本的なテレワーク形態において想定される危険性を前提に、モデルケースとしての対策等を例示するものであり、様々な形で実施されるテレワークのすべてにおいて、ここに示したような情報セキュリティ対策を行わなければならないというものではありません。テレワークの実施方法によっては対策が不要であったり、追加的な対策が必要になることがあります。9ページに示す「テレワークの方法に応じた対策の考え方」を参考にする等して、自らの企業・組織にあった対策を検討してください。

1.　テレワークにおける情報セキュリティ対策の考え方

（ア）「ルール」「人」「技術」のバランスがとれた対策の実施

テレワークとオフィスでの仕事との、情報セキュリティの面での違いは何でしょうか。それは、従業員同士で情報をやりとりするのにも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すること等が挙げられます。

企業で管理する紙文書、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パソコン等の端末で利用されます。そのため、インターネットを経由した攻撃を防御する対策がなされたオフィスとは異なり、情報資産はウイルス・ワーム等の感染、テレワーク端末や記録媒体の紛失・盗難、通信内容の盗聴等の「脅威」にさらされやすいといえます。このとき、端末やその設定や使い方に、脅威に対する「脆弱性」（情報セキュリティ上の欠陥のこと。用語集参照）が存在すると、情報漏えいや情報の消失など実際の事故の発生につながります。テレワークにおける代表的な脅威と脆弱性の例を図１に示します。

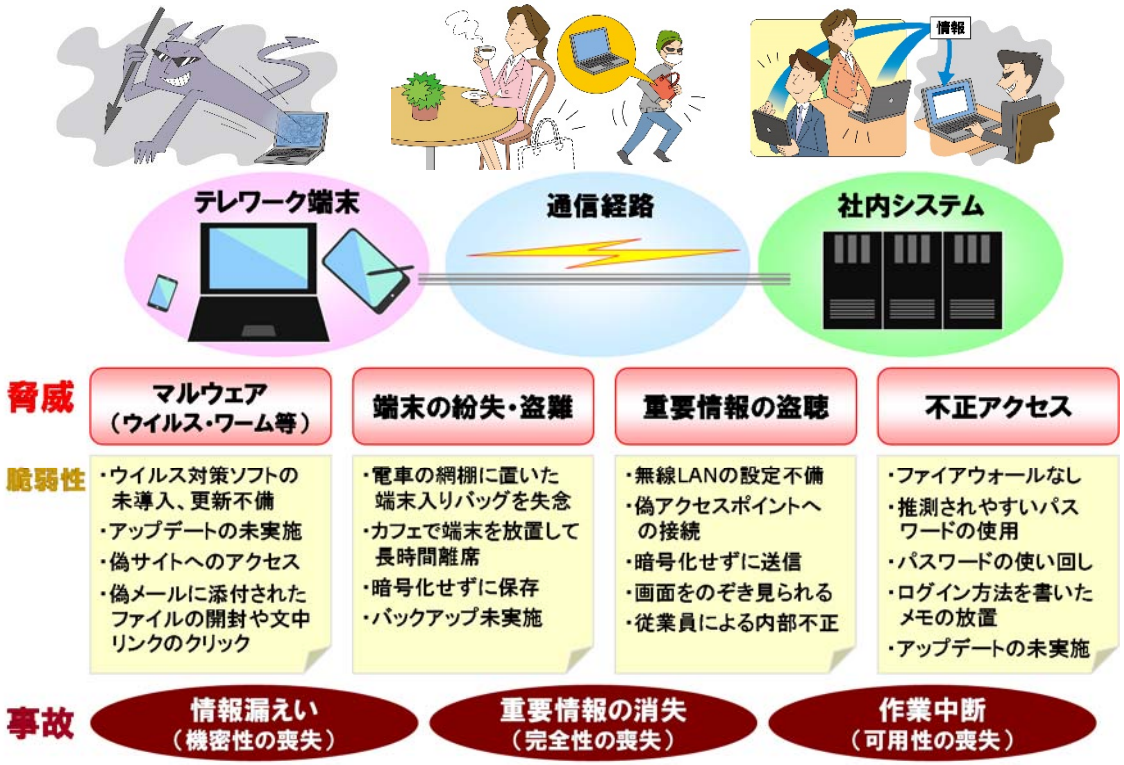


図 1　テレワークにおける脅威と脆弱性について

企業が情報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、認識したうえで、重要度に応じた情報のレベル分けを行い、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、情報セキュリティ対策には「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。下図の容器に水を入れる例からもわかるように、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。そこで、情報資産を守るためには、「ルール」・「人」・「技術」の三位一体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ポイントとなります（図2）。

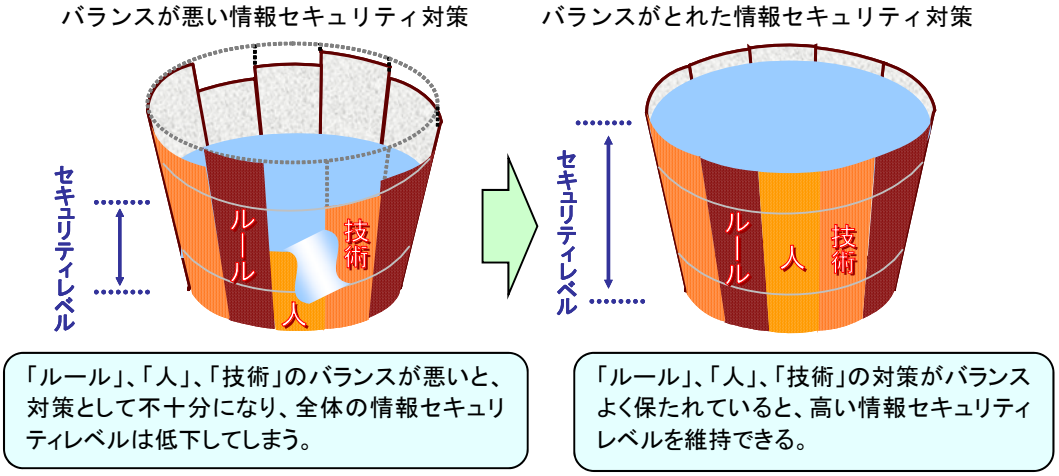


図 2　情報セキュリティ対策におけるバランスの考え方

【コラム】中小企業の情報セキュリティ対策を支援する取組

中小企業がテレワークの導入に併せて情報セキュリティ対策を整備しようとするとき、現状でどのような問題があるのか、今後どのような対策をすべきかを自ら検討するのは困難です。以下に例示する取組はこうした悩みの解決に役立ちます。

① SECURITY ACTION（独立行政法人情報処理推進機構（IPA））

IPA が公開している「中小企業の情報セキュリティ対策ガイドライン」に基づき次の取組を行う旨の自己宣言をすると、SECURITY ACTION 各ロゴマークを自社サイト等に掲示することができ、自社のアピールにつながります。

「情報セキュリティ５か条」の実践･･･★一つ星
「自社診断シート」に基づくセキュリティポリシーの策定・公開･･･★★二つ星

② 情報セキュリティ理解度チェック（NPO日本ネットワークセキュリティ協会）

「電子メールに関する知識」「インターネットの利用法」「ウイルスに関する知識」「パスワードの管理」など、テレワークを行う上でも重要なセキュリティ知識を従業員がどの程度理解しているかの自己チェック環境を提供しています。

このほか、一定の専門知識を備えた専門家の登録制度として、「IT コーディネータ制度」や「情報処理安全確保支援士制度」があります。上記①②を含む制度の詳細については、本ガイドライン末尾の参考リンク集（P61）をご覧ください。

「ルール」・「人」・「技術」とは

（「ルール」について）

業務を進めるにあたって、情報セキュリティの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の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仕事を行うことになるため、そのセキュリティ確保のために新たなルールを定める必要があります。そこで、組織としてどのようなルールを定め、守っていけばよいかについて留意する必要があります。

（「人」について）

情報セキュリティ対策の「ルール」・「人」・「技術」のうち、実施が最も難しいのは「人」の部分です。ルールを定めても、実際にテレワーク勤務者やシステム管理者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・組織が確認するのが難しいことに留意する必要があります。したがって、ルールを定着させるには、関係者への教育や自己啓発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情報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。

（「技術」について）

技術的対策は「ルール」や「人」では対応できない部分を補完するものです。技術的対策は種々の脅威に対して「認証」、「検知」、「制御」、「防御」を自動的に実施するものであり、テレワーク先の環境の多様性を考慮して、それぞれの環境での情報セキュリティ維持のために適切に対策を講じておく必要があります。

（イ）テレワークの方法に応じた対策の考え方

テレワークの方法にはテレワークで行う作業の内容や予算等によって、様々なパターンが考えられます。ここでは、「テレワーク端末への電子データの保存の有無」「オフィスで利用する端末との関係」と「クラウドサービスを利用するかどうか」をもとに、次のような６種類のパターンに分類します。

表 1　テレワークの６種類のパターン

	パターン①	パターン②	パターン③	パターン④	パターン⑤	パターン⑥
	リモートデスクトップ方式	仮想デスクトップ方式	クラウド型アプリ方式	セキュアブラウザ方式	アプリケーションラッピング方式	会社PCの持ち帰り方式
概要	オフィスにある端末を遠隔操作	テレワーク用の仮想端末を遠隔操作	クラウド上のアプリーションを社内外から利用	特別なブラウザを用いて端末へのデータの保存を制限	テレワーク端末内への保存を不可とする機能を提供	オフィスの端末を持ち帰りテレワーク端末として利用
テレワーク端末に電子データを保存するか？	保存しない	保存しない	どちらも可	保存しない	保存しない	保存する
オフィスの端末と同じ環境を利用するか？	同じ	テレワーク専用の環境	クラウド型アプリに関しては同じ	ブラウザ経由で利用するアプリに関しては同じ	テレワーク専用の環境	同じ
クラウドサービスを利用するか？	しない	しない	する	する	する／しない どちらも可	する／しない どちらも可
私用端末の利用（BYOD）との親和性	一定の条件のもとで可	一定の条件のもとで可	一定の条件のもとで可	一定の条件のもとで可	一定の条件のもとで可	－
高速インターネット回線の必要性	必須	必須	望ましい	望ましい	望ましい	不要
備考	－	－	－	－	－	紙媒体で持ち出す場合も本パターンに相当

それぞれの方法と対策の特徴は次の通りです。なお、このうちパターン①～④のいずれかを用いた上で、テレワーク端末上に電子データを保存しないで済むように運用する方式のことを「シンクライアント方式」と呼ぶこともあります。

- パターン①（リモートデスクトップ方式）
  オフィスに設置されたPC等の端末のデスクトップ環境を、テレワーク端末から遠隔操作したり閲覧したりする方法です。おもな利点として、オフィスで利用しているのと同じ環境が利用できるので、オフィスで実施していた作

業を自然な形でテレワーク環境でも継続して行えることが挙げられます。また、作業結果を保存する場合もオフィス側に保存され、テレワーク環境で利用する端末に電子データを残さないようにすることができますので、テレワーク端末として私用端末を使うことも可能です。一方欠点として、テレワーク端末とオフィスを接続するインターネット回線で十分な速度が確保できなければ、操作性が低下することに留意する必要があることが挙げられます。

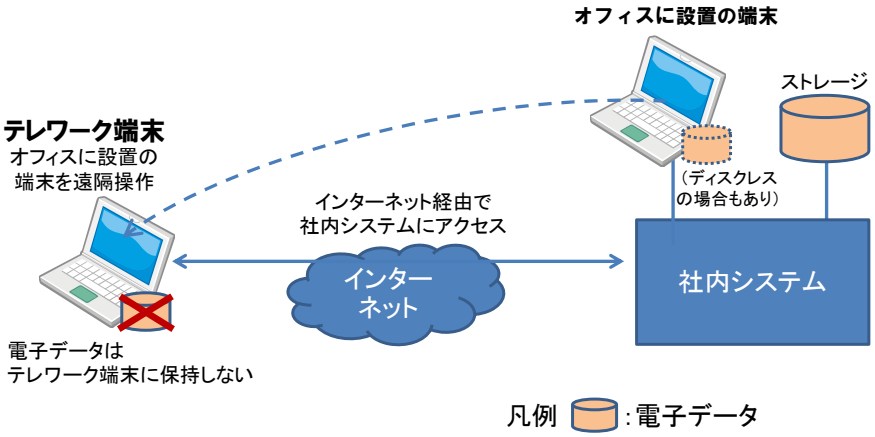


図 3　リモートデスクトップ方式

- パターン②（仮想デスクトップ方式）
  オフィスのサーバ上で提供される仮想デスクトップ基盤（VDI）に、テレワーク端末から遠隔でログインして利用する方法です。テレワーク端末に電子データを残さない点ではパターン①と同様ですが、オフィスに端末を用意しておく必要がありません。仮想デスクトップの環境はシステム管理者が一括して管理することができ、均質的なセキュリティ対策を実施することができます。テレワーク端末とオフィスを接続するインターネット回線の速度がテレワーク端末の操作性を左右する点については、パターン①と同様です。

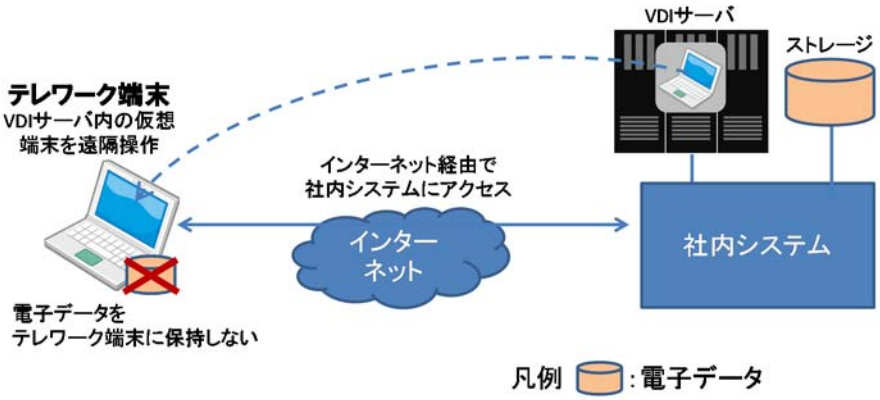


図 4　仮想デスクトップ方式

- パターン③（クラウド型アプリ方式）
  オフィスかテレワーク環境かどうかを問わず、インターネットで接続されている環境からクラウドサーバ上で提供されるアプリケーションにアクセスすることにより、作業を行う方法です。アプリケーションで作成したデータの保存先は、クラウド上とローカル環境のどちらも選択可能であるため、テレワーク勤務者がテレワーク端末に業務に関するデータを保存してしまうとその管理の問題が生じます。パターン①②と比較すると、テレワーク端末とクラウドサーバ間のインターネットの速度が作業の操作性に及ぼす影響は限定的です。

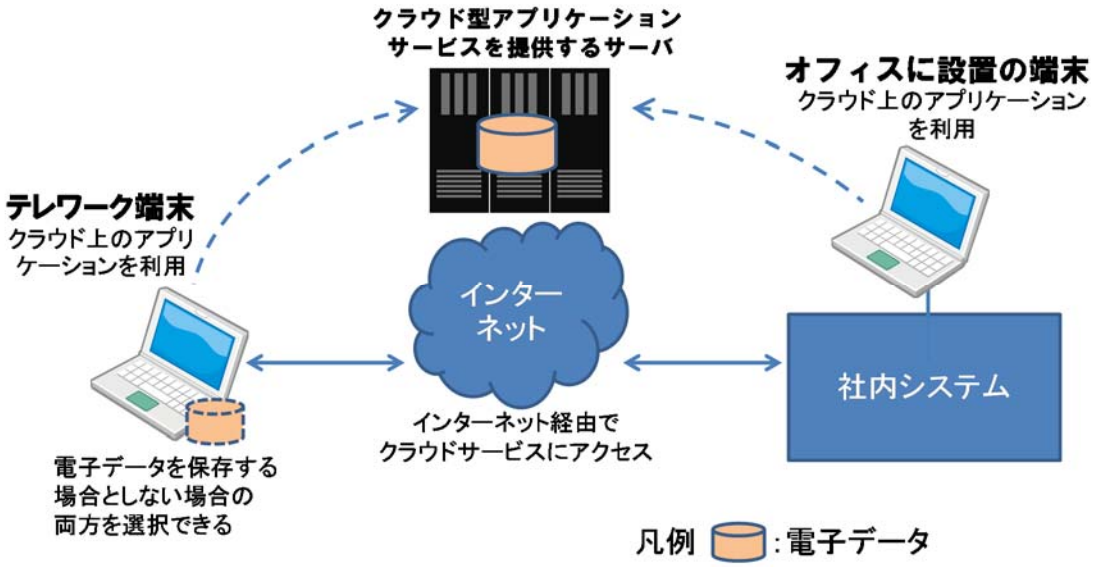


図 5　クラウド型アプリ方式

- パターン④（セキュアブラウザ方式）
  パターン③（クラウド型アプリ方式）の安全性を高めた方式です。特別なインターネットブラウザを用いることで、ファイルのダウンロードや印刷などの機能を制限し、テレワーク端末に業務で利用する電子データを保存しないようにすることが可能です。このようにして安全性が高まる反面、テレワーク端末上で利用できるアプリケーションは、この特別なインターネットブラウザ経由で利用できるものに限られます。インターネットの速度の影響に関してはパターン③と同じです。

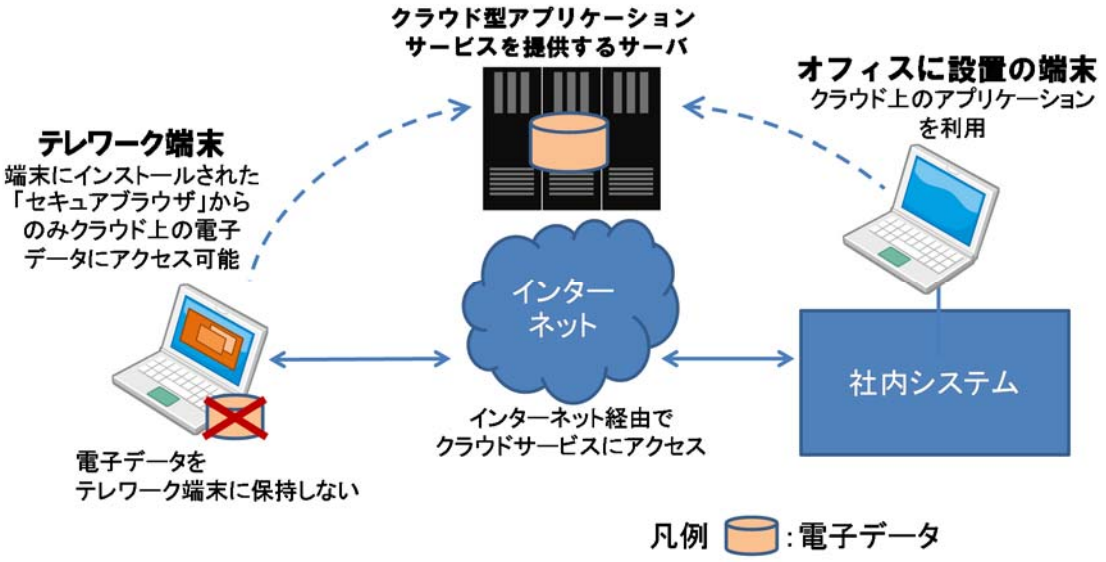


図 6　セキュアブラウザ方式

- パターン⑤（アプリケーションラッピング方式）
  テレワーク端末内に「コンテナ」と呼ばれる、ローカルの環境とは独立した仮想的な環境を設けて、その中でテレワーク業務用のアプリケーションを動作させる方式です。コンテナ内で動作するアプリケーション（文書作成、インターネットブラウザ等）からローカル環境にアクセスすることができないため、テレワーク端末内に電子データを残さない利用が可能です。一方、コンテナ内で動作させるOSやアプリケーションはローカルPCにインストールされたものを利用しますので、インターネットの速度の影響を受けにくい利点もあります。

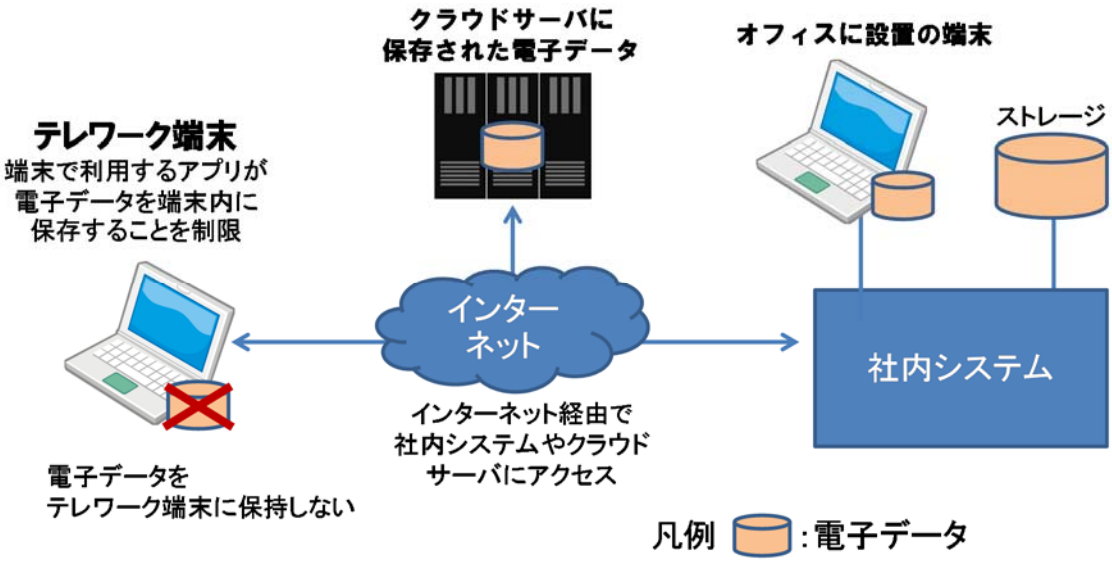


図 7　アプリケーションラッピング方式

- パターン⑥（会社PCの持ち帰り方式）
  オフィスで用いている端末をテレワーク先に持ち出して作業を行う方法です。ネットワーク経由でオフィスにアクセスする必要がある場合は、インターネットの経路上での情報漏えい対策としてVPNで接続することが前提となります。テレワーク環境とオフィスとの間のインターネット回線の速度が操作性に影響しないため、交通機関など通信が安定しない環境でも安定した作業を行うことができます。反面、在宅でテレワークを行うためには毎回オフィスから端末を持ち帰る必要があるほか、持ち帰っていない状態ではテレワークを行うことができないため、気象条件等に応じて急遽テレワークを行うといった場面での利用には不向きです。また、テレワーク端末に電子データを保存することが前提のため、６種類のパターンの中で最も厳格な情報セキュリティ対策を端末に対して行う必要があります。

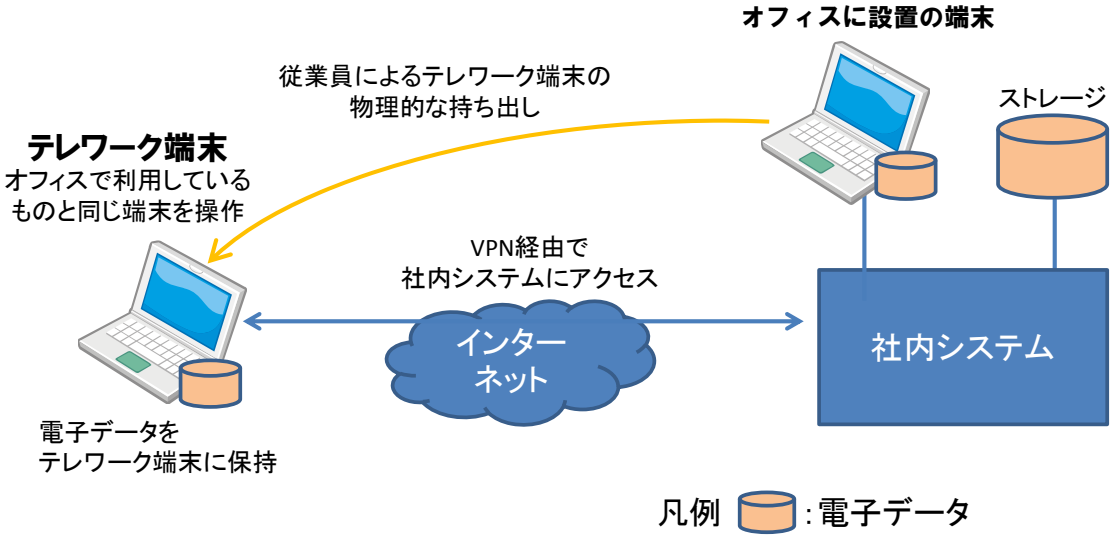


図 8　会社 PC の持ち帰り方式

以上説明したテレワークの方法に関するこうした違いは、おもに「技術」に関する対策に影響します。これ以後の説明部分に対象となるパターンを明示していますので、自社で行うテレワークの方法に応じて参考としてください。特に対象を明示していない場合、すべてのパターンが対象となります。

（自社にふさわしいテレワークの方式の検討）

テレワークの方式は上述のとおり、大きく６種類のパターンに分類されます。さらに、私用端末の利用を認めるかどうかでも、実施すべきセキュリティ対策が変わってきます。私用端末の利用を認めることでテレワークの導入コストを抑制することができますが、反面、管理が不十分になる恐れがあるため、経営者は、自社にふさわしいテレワークの方式について、セキュリティリスクと導入コストの両面から慎重に検討する必要があります。

前述のテレワークの方式のうち、私用端末の利用と相性がよいのは「①リモートデスクトップ方式」「②仮想デスクトップ方式」「④セキュアブラウザ方式」「⑤アプリケーションラッピング方式」の４種類です。これらの方式ではテレワーク端末に電子データを保存しないため、私用端末の管理が仮に不十分であっても事故につながりにくいのです。一方、「③クラウド型アプリ方式」では私用端末に電子データを保存することも可能なため、私用端末だからといって対策がおろそかなままでは事故に直結してしまいます。

私用端末利用の場合、導入コストが低く抑えられると考えられがちですが、実際には私用端末を採用することによる追加の情報セキュリティ対策のコスト（初期導入時と運用期間中の双方）の増加、情報セキュリティレベルの低下による事故発生による損失の可能性等と合わせて考えると、必ずしも期待するようなコストダウンになるとは限りません。企業から端末を貸与するほうがトータルで割安になることもあり得ます。

（クラウドサービスの利用について）

さらに、現在、大規模・高速なコンピュータ資源を低価格で利用する手段として、クラウドコンピューティングサービス（以下、「クラウドサービス」と呼びます。）が注目を集めています。クラウドサービスとは、ネットワークに接続された情報システムや記録装置などのサービス事業者が提供する資源を、ネットワークを経由して必要な分だけ利用できるようなサービスのことです。クラウドサービスの利用者のニーズに応じて、ネットワーク上の資源をレンタルサーバとして提供する、リモートディスクとして提供する、アプリケーションとして提供する等の種類があります。クラウドサービスは規模の拡大に応じてスケールメリットが働くため、自組織でサーバを設置して同様のサービスを運用するのと比較して、一般に割安になります。中小企業にとっても、こうしたコスト面での利点に加え、オフィス内にサーバ管理の担当者を配置しなくてよくなるというメリットがあるため、オフィス内にサーバを置くのを止めて、クラウドサービスに移行する企業が増えています。

テレワークの観点からも、クラウドサービスへの移行にはメリットがあります。オフィス内に設置したサーバにテレワーク先からのアクセスを許可する場合、インターネットとの接続地点に設置するファイアウォールにおいて、外部から内部にアクセスするための一種の「穴」をあける必要がありますが、これは攻撃に悪用される恐れがあり、注意深く設定しなければなりません。オフィス内のサーバをクラウドサービスに移行することでこうした「穴」をあける必要がなくなり、ファイアウォール等のセキュリティ対策設備の管理が楽になります。したがってクラウドサービスの利用は、テレワークの導入によりオフィスのネットワークに及ぶ危険を小さく抑えるために有益です。さらに11ページで紹介したパターン④（セキュアブラウザ方式）でテレワークを行うようにすると、テレワークで利用する電子データの保存場所をクラウドサービス上のみとすることができるため、守りやすくなる利点が得られます。

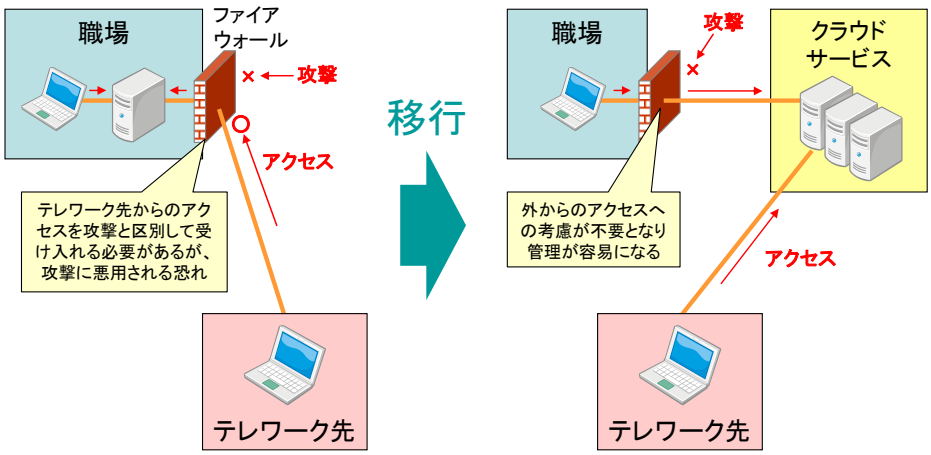


図 9　クラウドサービスへの移行

しかし他方、クラウドサービスは、「プライベートクラウド」と呼ばれる外部から直接アクセスできないものを除き、それ自体広くインターネットからのアクセスを前提とするものであるため、外部からの攻撃を受けやすいことに留意する必要があります。クラウドサービスで用いるパスワード、暗号鍵等は、簡単に推測されないものにするとともに、外部に漏洩することのないように厳格な管理をすべきです。可能であれば、多要素認証の利用や、電子証明書の併用などにより、利用者の認証におけるセキュリティ対策を強化することが望まれます。また、クラウドサービスの情報セキュリティ対策には、クラウドサービスの利用者が自らの責任で行わなければならないものが多く含まれます。クラウドサービスにおいて生じている情報漏えいなどの事故は、利用者の設定ミスにより、秘匿すべき情報に対するアクセス制御が講じられていなかったり、不適切であったりすることが原因であることが多いのです。

なお、最近は無料で使えるクラウドサービス（Ｗｅｂメールやグループウェア、ＳＮＳ等）のアカウントを個人で取得して、テレワークに活用するケースも増えています。実用上十分な性能と安全性を提供しているものもあり、業務利用を一概に禁止する必要はありませんが、以下のことに注意して利用すべきです。

- 個人アカウントでクラウドサービスを利用することで、プライベート用のＰＣに業務情報が意図せずに同期されてしまったり、無関係の第三者と共有されたりしてしまう危険性を、予め十分に把握しておく必要があります。
- 悪意の第三者による乗っ取り、なりすましの防止のため、個人で取得したアカウントであっても上述のような厳格なパスワード管理を行う必要があります。
- 無料であることの代償として、書き込まれた内容に応じた広告が表示されたり、クラウドサービスの利用状況を統計的に分析した結果をクラウド事業者がマーケティング情報として販売したりすることがあります。こうした状況を避けたいのであれば有料サービスの利用を検討して下さい。
- クラウド事業者の提供するクラウドサービスを利用する場合、データを預けることになりますので、クラウド事業者が信用に足る事業者かどうかに注意する必要があります。

以上の点を踏まえて、経営者は、テレワークにおけるクラウドサービス利用の情報セキュリティ上のメリットを考慮して、その活用について検討します。

（ウ）経営者、システム管理者及びテレワーク勤務者それぞれの立場

テレワーク実施において、経営者、システム管理者及びテレワーク勤務者それぞれの立場からテレワークセキュリティの保全に関してどのようにすべきかを認識する必要があります。

＜経営者＞

（ア）において、ルールづくりの重要性について触れました。経営者はこのルールを作る立場にあり、ルールづくりを積極的に推進します。業務におけるICT利活用が進展した現在、テレワークを含む業務を通じて情報セキュリティ上の事故が生じた場合、経営に直結した被害が生じることを自覚し、その防止のために必要な対策をルールとして定めていくことが求められます。さらに、大局的な立場からテレワークセキュリティ保全の全般に関して、経営者の立場でなければできないことを認識します。具体例として、実施すべき情報セキュリティ対策を定めた上で、その導入・運用に必要な人材・費用を確保することが挙げられます。その他、経営者が考えるべき事項については、経済産業省が公表している「サイバーセキュリティ経営ガイドライン」（61ページ「参考リンク集」参照）が参考になります。

＜システム管理者＞

社内システムには企業にとって守るべき電子データが数多く存在します。テレワーク端末から社内システムにアクセスできるようにする等、外部とのやりとりを可能とすることは、社内システムへの不正侵入・不正アクセスの可能性を高めることにもつながります。また、社内システムからウイルスを蔓延させてしまう脅威等に対しても十分な対策を行う必要があります。これらの脅威を踏まえて、システム全体を管理するシステム管理者として実施すべきことを認識します。

＜テレワーク勤務者＞

実際にテレワークを行う勤務者にとって、気をつけなければならないことは多くあります。不審なメールが届いたとき、オフィスであれば、「このメールはおかしくないですか？」と近くの人に相談することが簡単にできますが、テレワーク勤務者の場合は相談しづらい場合もあります。また、テレワーク端末は、オフィス内の端末と比べると、システム管理者が自ら管理のための操作を行うことが難しいことから、テレワーク勤務者が自身で管理することの重要性を自覚した上で、実施すべき対策を理解することが望まれます。

2.　テレワークセキュリティ対策のポイント

テレワークにおける情報セキュリティ対策として、重要と考えられる事項を挙げると次のとおりとなります。それぞれの説明は２２ページ以降をご覧下さい。なお、情報セキュリティ対策は、想定するリスクの種類や程度に応じて様々なものがあり、実際に作成する対策は、個々のリスクを検討の上、これら項目から取捨選択、加除修正していく必要があります。

なおこのリストは、自組織におけるセキュリティ対策がどの程度実施されているかを自己点検するためのセルフチェックリストとしても有用です。これら以外に自社独自のルールを設けている場合は、それらもリストに追加して下さい。

（ア）経営者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1	経営者は、テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、その内容に応じて見直しを行う。	22 ページ
2	社内で扱う情報について、その重要度に応じたレベル分けを行った上で、テレワークでの利用可否と利用可の場合の取扱方法を定める。	25 ページ
3	テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、定期的に教育・啓発活動を実施させる。	27 ページ
4	情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を整えるとともに、事故時の対応についての訓練を実施させる。	29 ページ
5	テレワークにおける情報セキュリティ対策に適切な理解を示した上で、必要な人材・資源に必要な予算を割り当てる。	30 ページ

（イ）システム管理者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1	システム全体を管理する重要な立場であることを自覚し、情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。	22 ページ
2	情報のレベル分けに応じて、電子データに対するアクセス制御、暗号化の要否や印刷可否などの設定を行う。	25 ページ

3	テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、定期的に教育・啓発活動を実施する。	27 ページ
4	情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を確認するとともに、事故時の対応についての訓練を実施する。	29 ページ

（悪意のソフトウェアに対する対策）

5	フィルタリング等を用いて、テレワーク勤務者が危険なサイトにアクセスしないように設定する。	31 ページ
6	テレワーク勤務者が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申請させ、情報セキュリティ上の問題がないことを確認した上で認める。	33 ページ
7	貸与用のテレワーク端末にウイルス対策ソフトをインストールし、最新の定義ファイルが適用されているようにする。	35 ページ
8	貸与用のテレワーク端末のＯＳ及びソフトウェアについて、アップデートを行い最新の状態に保つ。	37 ページ
9	私用端末をテレワークに利用させる際は、その端末に必要な情報セキュリティ対策が施されていることを確認させた上で認める。	38 ページ
10	ランサムウェアの感染に備え、重要な電子データのバックアップを社内システムから切り離した状態で保存する。	39 ページ
11	金融機関や物流業者からの事務連絡を装うなどの不審なメールが迷惑メールとして分類されるよう設定する。	40 ページ

（端末の紛失・盗難に対する対策）

12	台帳等を整備し、貸与するテレワーク端末の所在や利用者等を管理する。	43 ページ

（重要情報の盗聴に対する対策）

13	テレワーク端末において無線 LAN の脆弱性対策が適切に講じられるようにする。	46 ページ

（不正侵入・踏み台に対する対策）

14	社外から社内システムへアクセスするための利用者認証について、技術的基準を明確に定め、適正に管理・運用する。	48 ページ
15	テレワーク勤務者がインターネット経由で社内システムにアクセスする際のアクセス方法を定める。また、社内システムとインターネットの境界線にはファイアウォールやルータ等を設置し、アクセス状況を監視するとともに、不必要なアクセスを遮断する。	49 ページ
16	社内システムへのアクセス用のパスワードとして、強度の低いものを用いることができないように設定する。	51 ページ

（外部サービスの利用に対する対策）

17	メッセージングアプリケーションを含むＳＮＳに関する従業員向けの利用ルールやガイドラインを整備し、その中でテレワーク時の利用上の留意事項を明示する。	54 ページ

18	ファイル共有サービス等のパブリッククラウドサービスの利用ルールを整備し、情報漏えいにつながる恐れのある利用方法を禁止する。	56 ページ

（ウ）テレワーク勤務者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1	テレワーク作業中は、利用する情報資産の管理責任を自らが負うことを自覚し、情報セキュリティポリシーが定める技術的・物理的及び人的対策基準に沿った業務を行い、定期的に実施状況を自己点検する。	22 ページ
2	テレワークで扱う情報について、定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。	25 ページ
3	定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組むことで、情報セキュリティに対する認識を高めることに務める。	27 ページ
4	情報セキュリティ事故の発生に備えて、直ちに定められた担当者に連絡できるよう連絡体制を確認するとともに、事故時に備えた訓練に参加する。	29 ページ

（悪意のソフトウェアに対する対策）

5	マルウェア感染を防ぐため、ＯＳやブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにはアクセスしない。	31 ページ
6	アプリケーションをインストールする際は、システム管理者にその旨を申請し、許可を受けたアプリケーションのみをインストールする。 （私用端末利用の場合）テレワークで利用する端末にインストールするアプリケーションは、安全性に十分留意して選択する。	33 ページ
7	作業開始前に、テレワーク端末にウイルス対策ソフトがインストールされ、最新の定義ファイルが適用されていることを確認する。	35 ページ
8	作業開始前に、テレワーク端末のＯＳ及びソフトウェアについて、アップデートが適用され最新の状態であることを確認する。	37 ページ
9	テレワークにはルールに定められた情報セキュリティ対策が適用されているものを使用し、スマートフォン、タブレット等に関しては不正な改造（脱獄、root 化等）を施さない。	38 ページ
10	テレワーク作業中にマルウェアに感染した場合、その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、電子メールの添付ファイルの開封やリンク先のクリックに一層の注意を払う。	40 ページ

（端末の紛失・盗難に対する対策）

11	オフィス外に情報資産を持ち出すとき、その原本を安全な場所に保存しておく。	42 ページ

12	機密性が求められる電子データを極力管理する必要が無いように業務の方法を工夫する。やむを得ない場合は必ず暗号化して保存するとともに、端末や電子データの入った記録媒体（ＵＳＢメモリ等）等の盗難に留意する。	43 ページ

（重要情報の盗聴に対する対策）

13	機密性が求められる電子データを送信する際には必ず暗号化する。	45 ページ
14	無線 LAN 利用に伴うリスクを理解し、テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する。	46 ページ
15	第三者と共有する環境で作業を行う場合、端末の画面にプライバシーフィルターを装着したり、作業場所を選ぶ等により、画面の覗き見防止に努める。	47 ページ

（不正侵入・踏み台に対する対策）

16	社外から社内システムにアクセスするための利用者認証情報（パスワード、ＩＣカード等）を適正に管理する。	48 ページ
17	インターネット経由で社内システムにアクセスする際、システム管理者が指定したアクセス方法のみを用いる。	49 ページ
18	テレワークで使用するパスワードは、使い回しを避け、一定以上の長さで他人に推測されにくいものを用いるように心がける。	51 ページ

（外部サービスの利用に対する対策）

19	メッセージングアプリケーションを含むＳＮＳをテレワークで利用する場合、社内で定められたＳＮＳ利用ルールやガイドラインに従って利用するようにする。	54 ページ
20	テレワークでファイル共有サービス等のパブリッククラウドサービスを利用する場合、社内ルールで認められた範囲で利用する。	56 ページ

3.　テレワークセキュリティ対策の解説

（ア）情報セキュリティ保全対策の大枠

経営者 1	経営者は、テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、その内容に応じて見直しを行う。
管理者 1	システム全体を管理する重要な立場であることを自覚し、情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。
勤務者 1	テレワーク作業中は、利用する情報資産の管理責任を自らが負うことを自覚し、情報セキュリティポリシーが定める技術的・物理的及び人的対策基準に沿った業務を行い、定期的に実施状況を自己点検する。

＜経営者＞**基本対策事項**

- 情報セキュリティ対策を行う上で、最も基本となるルールが自社の「情報セキュリティポリシー」です。これは、自社における「情報セキュリティに関する方針や行動指針」をまとめた文書であり、これを作ることで組織として統一のとれた情報セキュリティレベルを確保することができます。
- 情報セキュリティポリシーは、次ページ図10の通り、①全体の根幹となる「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「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「実施内容」の３つの階層で構成されています。これらの内容は、その企業の企業理念、経営戦略、企業規模、保有する情報資産、業種・業態等により異なってくるため、自社の企業活動に合致した情報セキュリティポリシーを定める必要があります。
- 基本方針は名の通り基本的な内容なので、テレワークの有無によって内容を変える必要はありませんが、対策基準や実施内容については、テレワークを考慮したものとする必要があります。たとえば、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責任をどちらが負うのかをあらかじめ定めておく必要があります。

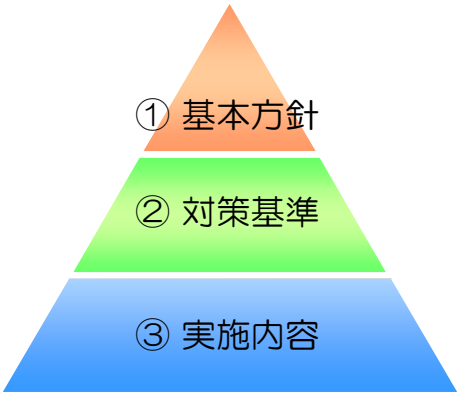


図 10　情報セキュリティポリシーの構成

＜経営者＞**推奨対策事項**

こうした情報セキュリティポリシーは一度策定すればよいというものではありません。「PDCAサイクル」と呼ばれる４つの段階を通じて、ルールを最新の状況に見直すと共に、情報セキュリティ対策のレベルを向上させていくことが重要です（図9）。

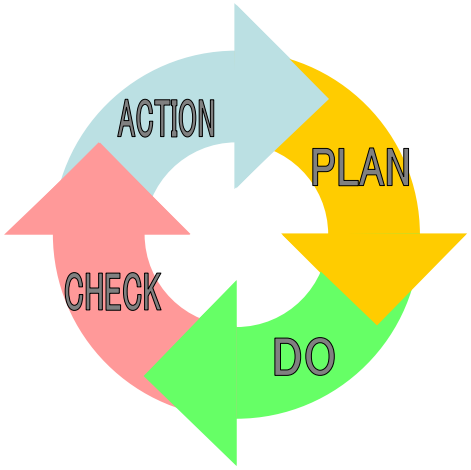


図 11　情報セキュリティに関するＰＤＣＡサイクル

また、自社の従業員であっても、些細なミスや内部不正行為が大きな企業損失に拡大することもあります。テレワークは、様々な環境で業務を行うことが可能になることから、機密情報の外部流出を防ぐためのルール（電子データの持ち出しに当たっては暗号化等の対策等がきちんとされていることについてチェックし、許可を得ること等）を設けるとともに、抑止効果として就業規則等にこれらのルールに違反した場合の罰則規定を設けることも有効です。

＜システム管理者＞**推奨対策事項**

システム管理者はシステム全体を管理する重要な立場であることから、情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じ、定期的にその実施状況を監査する必要があります。

また、経営者がルールを決める際に必要な情報を提供します。

＜テレワーク勤務者＞**推奨対策事項**

オフィスには、情報セキュリティに関する管理責任者がいるのが普通ですが、テレワークを行っている間は、テレワーク勤務者自身がその場所における管理責任者です。特に、情報資産を持ち出して仕事をしている場合は、持ち出している間のその情報資産に関する管理責任は、テレワーク勤務者にあります。定められたルール（重要情報の暗号化、安全な通信経路の利用等）を守って作業をしていれば、仮に作業中に事故が発生して情報が漏洩したり、情報が失われてもテレワーク勤務者が責任を問われることはありませんが、ルールを守っていなかったり、重大な過失があった場合は、テレワーク勤務者が事故の責任を負わなければなりません。テレワークでは上司の目が届きにくいからといって、ルールを守らずに作業することは、結果的に本人にとって重大な損失を招きかねないことを理解しておくことが必要です。

経営者 2	社内で扱う情報について、その重要度に応じたレベル分けを行った上で、テレワークでの利用可否と利用可の場合の取扱方法を定める。
管理者 2	情報のレベル分けに応じて、電子データに対するアクセス制御、暗号化の要否や印刷可否などの設定を行う。
勤務者 2	テレワークで扱う情報について、定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。

＜経営者・システム管理者＞**基本対策事項**

- 社内の情報資産を「機密情報」「業務情報」「公開情報」等３つ程度に分類し、「公開情報」以外の情報資産についての取扱い方法を定めます。
  - 機密情報には、個人情報（自社従業員に関するものも含む）、顧客から預かった非公開情報、機微情報、営業秘密、自社の経営に関する情報などが該当します。
  - 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：社内打合せ資料、勤務管理簿、研修教材等）が該当します。
  - 情報資産の持ち出しを伴うテレワークでは、それらの持ち出された情報（電子データ、紙）が外部に漏えいするリスクが高まることから、「業務情報」と「公開情報」のみを持ち出し可能とすることが考えられます。
- 情報資産の利用者が、それぞれのレベル分けを識別できるようにします。
  - 電子データ：フォルダによる区別、ファイル名への【機密】の追加など
  - 紙媒体：紙面欄外余白部への「機密」表記、ファイルの背表紙への記載など

＜経営者・システム管理者＞**推奨対策事項**

情報資産を社内のファイルサーバなどで管理する場合、電子データを保存するフォルダにアクセス制限を設定することで、機密情報を閲覧・編集する必要のない利用者や端末からアクセスできないようにすることができます。前述のテレワークの方法で示したいずれの方式を選択しても、情報資産に対するアクセス制限を行うことは可能ですが、上述のように、機密情報の持ち出しには大きなリスクを伴います。

テレワークで機密情報を扱う必要がある場合には、「リモートデスクトップ方式」や「仮想デスクトップ方式」を採用した上で、情報資産の重要度と利用者の権限に基づくアクセス制限を行うことで、機密情報の保護と利用の両立が可能になります。

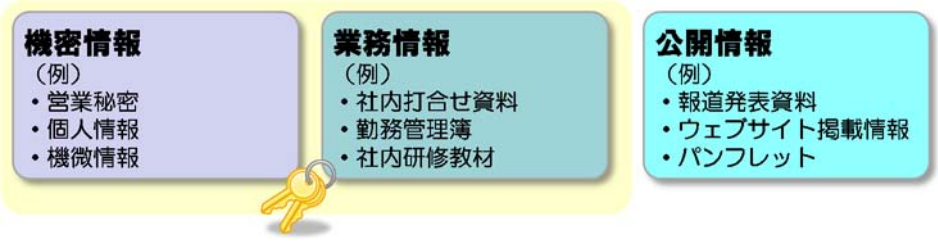


図 12　情報のレベル分け

テレワークトラブル事例と対策〈1〉
～情報のレベル分けに関するトラブル事例～

トラブル事例

社外からも社内と同じように、社内システム内の全てのファイルにアクセスできるようにしていたところ、従業員が外出先でテレワーク中に顧客の秘密情報が表示された状態で作業画面を放置してしまい、秘密情報が盗み見され、ネット上の匿名掲示板に書き込まれてしまったことで、顧客から取引停止を申し渡された。

対策例

このようなトラブルは、8 ページに示した「ルール」「人」「技術」それぞれに関わる問題点を認識した上での対策が必要です。モバイル環境でのテレワークにおいては、周囲に様々な人がいる環境で仕事することもあります。このため、部外者の立入のない執務室では考えにくい端末画面の盗み見等による情報漏えいのリスクについて考慮する必要があります。

具体的な対策としては、まず「ルール」として、経営者が示す方針のもとでシステム管理者においてあらかじめ情報のレベル分けを行い、それぞれの取扱方法を定めます。さらに「技術」的対策として重要情報については社外からのアクセスを不可となるように設定することが考えられます。ただし、テレワーク端末からアクセスする必要がある情報については、この方法は使えません。そこで「人」に関する対策として、重要情報を扱うときに画面を放置することの危険性を伝えるなど、テレワーク勤務者の意識を高めることで未然防止を図ることが求められます。

【コラム】紙媒体での情報の持ち出し

テレワークの際には、暗号化などの対策が容易になることから、業務に必要な情報を電子データとして管理するペーパーレス化を行うことが推奨されます。しかし、多くの企業では、全ての情報が電子化されているわけではなく、やむを得ず紙媒体で情報を持ち出すケースもあるのが実態です。

日本ネットワークセキュリティ協会「セキュリティインシデントに関する調査報告書セキュリティインシデントに関する調査報告書」(2017 年 6 月 14 日)によると、情報漏えい媒体・経路のうち、紙媒体が 47.0%となり、約半数を占めるという結果が出ています。紙による情報持ち出しを認める場合には、資料の紛失・盗難等による情報漏えいのリスクを認識し、これらを踏まえたルールを定める必要があります。具体的には、持ち出し可能な資料の範囲を定める、書類の破棄方法を規定する、資料を持ち出す際には管理表への記載を義務付ける等の対策が考えられます。

また、コワーキングスペース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多いようですので、十分留意してください。

経営者 3	テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、定期的に教育・啓発活動を実施させる。
管理者 3	テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、定期的に教育・啓発活動を実施する。
勤務者 3	定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組むことで、情報セキュリティに対する認識を高めることに務める。

＜経営者・システム管理者＞**基本対策事項**

- テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、教育・啓発活動は欠かすことができません。情報セキュリティ教育・啓発活動は一過性のものではなく、日々の活動及び定期的な実施が重要です（図13）。
- 例えば、次ページ図14のような分かりやすい「メッセージ」を作成し、イントラネット内で通知したり、テレワーク勤務者が目をとめやすいところにポスターとして掲示すること等により、常に意識させることも効果的です。また、テレワーク先で緊急事態が発生した場合の連絡先等は、名刺サイズのカードの形で印刷して配布することで、テレワーク勤務者に常に携帯してもらうことができます。
- また、テレワーク先では、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管理者が確認することは容易ではありません。就業規則等にテレワーク時の機密保持とその違反時の罰則に関する規定を定めるとともに、ルール遵守のメリットを理解してもらうようにします。

＜テレワーク勤務者＞**基本対策事項**

- 定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組み、日頃から情報セキュリティに対する認識を高めることに務めることが重

図 13　情報セキュリティ教育

図 14　イントラネットやポスターによる啓発

＜経営者・システム管理者＞**推奨対策事項**

前述した内容のほか、テレワーク勤務者向けに、自分が適切なテレワークを実施しているかどうかを簡単に確認できるようにする手段も必要です。自己点検項目はこうした確認のツールとして活用できます。内部監査に相当するものとして、年１回程度を目安に定期的に実施すべきです。遵守できていない事項がある場合は、その改善に向けて企業が支援することをあらかじめ示すことで、テレワーク勤務者が実態を偽った回答を行うことを防ぐようにします。

経営者 4	情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を整えるとともに、事故時の対応についての訓練を実施させる。
管理者 4	情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を確認するとともに、事故時の対応についての訓練を実施する。
勤務者 4	情報セキュリティ事故の発生に備えて、直ちに定められた担当者に連絡できるよう連絡体制を確認するとともに、事故時に備えた訓練に参加する。

＜経営者・システム管理者・テレワーク勤務者＞**基本対策事項**

- 万一の情報セキュリティ事故の発生に備えて、迅速な対応策をとれるように連絡体制を整え、常に確認できるようにすることが重要です。早期発見／早期対応することにより、情報セキュリティ事故の影響を最小限に抑えることが可能です。
- また、情報セキュリティ事故の原因を分析し、再発防止に努めることは、組織全体での情報セキュリティ事故の発生を減らすのに有効に作用します。

＜経営者・システム管理者・テレワーク勤務者＞**推奨対策事項**

非常時の連絡体制は、事前に決めておくだけでは本当に非常事態が生じたときにうまく機能するかどうかわかりません。可能な範囲（たとえば年１回）で、「インターネット全体で新種のマルウェアが蔓延し、マヒ状態になった」等の条件を想定した訓練（予行演習）を行い、非常時の連絡体制を実際に使ってみることが重要です。

経営者 5	テレワークにおける情報セキュリティ対策に適切な理解を示した上で、必要な人材・資源に必要な予算を割り当てる。

＜経営者＞**基本対策事項**

- テレワークは新しい働き方であり、こうした働き方をこれまで実施していなかった職場で無理なく安全に導入するためには、オフィス環境における防犯対策に費用が必要なように、テレワーク環境における情報セキュリティ対策にも適切な投資を行うことが必要です。これは、通信や情報セキュリティ対策に必要な機器・設備の購入だけでなく、その運用・管理を行う人的資源の確保も含みます。
- テレワーク向けの情報セキュリティ対策は単に多額の投資を行えばよい、というものではありません。自社のテレワークにおいて何を実現し、何を守るべきかを明確にした上で、その実現に適した方法を選び、その方法に必要な投資を行うことが重要です。

（イ）マルウェアに対する対策

管理者 5	フィルタリング等を用いて、テレワーク勤務者が危険なサイトにアクセスしないように設定する。
勤務者 5	マルウェア感染を防ぐため、ＯＳやブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにはアクセスしない。

＜テレワーク勤務者＞**基本対策事項**

- 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ウイルスやワームの脅威に備えることが重要です。テレワーク中の社外ウェブサイトへのアクセスは必要最小限にとどめ、かつアクセスする前にOSやウェブブラウザ、Flash PlayerやAcrobat Readerなど関連するアプリケーションのアップデートを済ませるようにします。

＜システム管理者＞**推奨対策事項**

危険なサイトには、そもそもテレワーク勤務者がアクセスしないように、システム管理者がフィルタリング等の設定を行うことも有効な対策の一つです。

テレワークトラブル事例と対策〈2〉
～マルウェア感染に関するトラブル事例～

トラブル事例

社内で普段使っているノートパソコンを社外に持ち出しテレワークを行っていた。業務上必要な情報収集をおこなうため、海外のウェブサイト（情報のまとめサイト）を閲覧したところ、そのサイトを通じてパソコンがランサムウェアに感染し画面がロックされてしまった。復旧の期間、作業をストップしなければならなくなり、納期遅延が発生した。

対策例

ウェブサイトの中には閲覧するだけで、マルウェアや悪意あるソフトウェアをインストールしようとするものが存在します。もしインストール前に、画面上に何かの表示が出た場合は、何がインストールされるのかよく読みましょう。その他、以下のような複数の対策をとることで安心・安全なテレワーク環境の構築につながります。

＜テレワーク勤務者における対策＞

- ＰＣ等のテレワーク端末へのウイルス・マルウェアの対策ソフトウェアの導入
- OS やアプリケーションのアップデート
- 危険なウェブサイト等へのアクセスを禁止するフィルタリングソフトの導入

＜システム管理者における対策＞

- サーバ用ウイルス対策ソフトの導入　等

管理者 6	テレワーク勤務者が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申請させ、情報セキュリティ上の問題がないことを確認した上で認める。
勤務者 6	アプリケーションをインストールする際は、システム管理者にその旨を申請し、許可を受けたアプリケーションのみをインストールする。
	（私用端末利用の場合）テレワークで利用する端末にインストールするアプリケーションは、安全性に十分留意して選択する。

＜システム管理者＞**推奨対策事項**

テレワーク勤務者が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申請させ、情報セキュリティ上の問題がないことを確認した上で、使用を認めるようにします。テレワーク勤務者の独断でインストールさせないように注意します。

＜テレワーク勤務者＞**推奨対策事項**

テレワーク端末として用いる端末には、業務用に支給されたアプリケーション以外はダウンロード及びインストールしないようにします。どうしてもインストールが必要な場合は、システム管理者にその旨を申請し、許可を受けたアプリケーションのみをインストールするようにします。

テレワークトラブル事例と対策〈3〉
～ウイルス対策ソフトに関するトラブル事例～

トラブル事例

社内で利用を許可していなかったアプリケーション（海外製の動画ダウンロード用ツール）をインストールしたところ、マルウェアも一緒にインストールされてしまった。端末の画面上に、見慣れない海外の広告等が表示されるようになってしまった。広告が画面を覆うように表示されるため、作業効率を低下させている。マルウェアをアンインストールしたいができない。

対策例

- テレワークで用いる端末への新たなアプリケーションのインストール禁止。プリインストールされたアプリケーション以外は利用できないようにする。
- もしくは、事前に安全性が認められたアプリケーションのみリストアップし、社内で共有する。テレワーク実施者は、リストにあげられたアプリケーションであればインストール可とする。

上記の場合、いずれもシステム管理者側でルールを定めた後、社内での周知も徹底しましょう。せっかく、安全なアプリケーションをリストにまとめても、その在り処をテレワーク勤務者が認知していなければ意味がありません。

また、システム管理者はテレワーク勤務者が端末にどのようなアプリケーションをインストールしているか把握できるようにしましょう。テレワーク利用端末へのＩＣＴ資産管理ソフトウェアの導入も検討するとよいでしょう。

管理者 7	貸与用のテレワーク端末にウイルス対策ソフトをインストールし、最新の定義ファイルが適用されているようにする。
勤務者 7	作業開始前に、テレワーク端末にウイルス対策ソフトがインストールされ、最新の定義ファイルが適用されていることを確認する。

＜システム管理者＞**基本対策事項**

- パソコン等の情報セキュリティ対策（ウイルス定義ファイル更新やアップデート適用等）は、ひとりひとりが対応するには困難な場合があるため、自社の情報セキュリティ管理者やシステム管理者等の指示のもとで一斉に実施することができるよう、自動的に適用されるような設定ができる製品を選択することが効果的です。実施漏れがあるとそこが組織の脆弱性となります。また、重要な更新についてはテレワーク勤務者にアナウンスすることも考えられます。

＜テレワーク勤務者＞**基本対策事項**

- 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ウイルスやワームの脅威に備えることが重要です。テレワーク勤務者は、作業開始前に毎回テレワーク端末におけるウイルス対策ソフトについて、有効期限切れでないことと、最新のパターンファイル（ウイルスチェックリスト）に更新されているなど、オフィスと同じ対策レベルが確保されていることを確認する必要があります。
- 更新頻度は毎日が理想ですが、少なくとも週１回以上は必要です。

テレワーク**トラブル事例**と**対策**〈4〉

～アプリケーション利用に関するトラブル事例～

トラブル事例

端末にインストールしたセキュリティ対策ソフトのパターンファイルの更新を忘れてテレワークを行っていた。気がつくといつの間にかマルウェアに感染してしまった。

対策例

テレワーク勤務者において、次のような対策を常に励行すべきです。

- セキュリティ対策ソフトの定義ソフトに新しいものが配布されていないか（最新の状態か）を確認してからテレワークを開始
- 定義ファイルが自動更新されるようにソフトウェアを設定。

大きな被害をもたらすようなマルウェアや悪意のあるソフトウェアが流行している場合、報道機関や情報処理推進機構（IPA）等から情報発信がされます。日ごろからセキュリティに関する情報収集を行うように心がけましょう。

【コラム】次世代ウイルス対策ソフト

最近の標的型攻撃に用いられるマルウェアは、標準的なウイルス対策ソフトでは検出されないものがほとんどです。これは、標的型攻撃の場合、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、少数の攻撃対象に向けてウイルス対策ソフトで検出されないように工夫した新種のマルウェアを用いて攻撃を行うため、ウイルス対策ソフトのベンダにおいて検出用のパターンファイルを準備できないことによります。

そこで、こうした状況に対応するため、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のではなく、PC 等において動作するアプリケーションすべてを監視し、そのうちマルウェアに似た挙動のアプリケーションを見つけ、警告を表示したりそのマルウェアの動作止めたりする次世代のウイルス対策ソフトが各社から発売されています。海外から送られてくる電子メールの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については、こうした次世代ウイルス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。

管理者 8	貸与用のテレワーク端末のＯＳ及びソフトウェアについて、アップデートを行い最新の状態に保つ。
勤務者 8	作業開始前に、テレワーク端末のＯＳ及びソフトウェアについて、アップデートが適用され最新の状態であることを確認する。

＜システム管理者＞**基本対策事項**

- システム管理者は、OSだけでなく、主要なアプリケーションやミドルウェアについてもアップデートを実施する必要があります。アップデートを行わないと、脆弱性が残ったままとなり、外部からの攻撃が成功する可能性が高まります。

＜テレワーク勤務者＞**基本対策事項**

- テレワーク勤務者はウイルス対策ソフトと同様、OSやソフトウェアのアップデートの状態についても、自ら確認すべきです。

テレワーク**トラブル事例**と**対策**〈5〉

～アップデートに関するトラブル事例～

トラブル事例

専用の PC を使用して、年に数回程度テレワークを実施していた。久しぶりにパソコンを開いてみると、OS やインストールしているアプリケーションがアップデートされていなかったが、急いでいたのでそのままテレワークを行い、インターネット検索をしながら調査資料の作成を行った。そのときは異常を感じなかったが、次回その PC を起動すると、「この PC はウイルスに感染しています。除去用の製品購入が必要です」という偽セキュリティ対策ソフトウェアの広告がしつこく表示されるようになり、作業効率が大幅に低下してしまった。

対策例

テレワーク勤務者において、たまにしか利用しない PC を起動した直後は脆弱な状態であることに留意する必要があります。業務着手に先立ち、OS やアプリケーションのアップデートを行う必要があります。ただしこうしたアップデート作業には長い時間がかかることもあるため、効率的な作業の実施のためには定期的に PC のアップデートを行っておくことが考えられます。また、仮想デスクトップ方式においては、こうした更新作業が不要なディスクレスの端末を用いることもできるので、こうした方法を採用することも検討すべきです。

管理者 9	私用端末をテレワークに利用させる際は、その端末に必要な情報セキュリティ対策が施されていることを確認させた上で認める。
勤務者 9	テレワークにはルールに定められた情報セキュリティ対策が適用されているものを使用し、スマートフォン、タブレット等に関しては不正な改造（脱獄、root 化等）を施さない。

＜システム管理者＞**推奨対策事項**

テレワーク勤務者が私用端末をテレワークに利用する（Bring Your Own Device:BYOD）際は、その端末に必要な情報セキュリティ対策が施されていることをテレワーク勤務者に確認させた上で使用を認めます。

＜テレワーク勤務者＞**推奨対策事項**

私用端末をテレワークに用いる場合、端末が適切に管理されていないと、悪意のソフトウェアに感染したり、不正アクセスの入口として利用されたりすることで、その端末が企業全体の情報漏えいの原因となる恐れがあります。近年のテレワークではパソコンのほか、スマートフォンやタブレット端末も利用されるようになっていますが、不正改造（スマートフォン等では、俗に、端末の「脱獄」や「root化」とも呼ばれます。）を施した端末を、テレワーク端末として業務に使用しないようにします。テレワークにおける私用端末の利用が許可されている場合でも、必ずその利用に関するルールが定められていますので、遵守するようにしてください。

また、テレワークのために貸与された端末を、本来の業務と異なる用途に使用することは、企業の資産の目的外利用として不適切なばかりでなく、悪意のソフトウェアの感染等の原因になります。また、自分で留意するだけでなく、不特定多数の出入りがある環境で作業する場合には、端末を他人に利用されないようにすることも重要です。

管理者10	ランサムウェアの感染に備え、重要な電子データのバックアップを社内システムから切り離した状態で保存する。

＜システム管理者＞**推奨対策事項**

ランサムウェアとは、マルウェアの一種ですが、データを外部に漏えいさせるのではなく、感染したPC等からアクセス可能なデータを暗号化することで使えなくしてしまうところに特徴があります。暗号化されたデータを復号するための鍵は攻撃者しか知らないため、データが使えなくなって困った利用者が攻撃者の言いなりに金銭を支払ってしまう被害が生じています。ただし、言われた通りに金銭を払っても復号されなかった例もあり、攻撃者に対して金銭を払うことは推奨されません。

テレワーク トラブル事例 と 対策〈6〉
～ランサムウェアに関するトラブル事例～

トラブル事例

従業員の利用するテレワーク端末を介して社内システムがランサムウェアに感染してしまい、重要情報が閲覧できなくなるだけでなく、攻撃者から多額の金銭の要求を受けた。重要情報のデータを再び閲覧できるようにするため、やむなく攻撃者の言うとおりに金銭を支払ったが、データを復号するための鍵は送られなかった。

対策例

社内の重要情報については、システム管理者においてバックアップデータをとり、ネットワーク経由でアクセスできない場所や、書き換えのできない場所に保存することで、ランサムウェアによる被害を防ぐことができます。例えば次のような方法が考えられます。

- USB メモリ、取り外し可能なハードディスクや SSD に記録し、機器から取り外して施錠保管
- 書き換え不可能なメディア（例：DVD-R）に記録して保管
- 感染の可能性のある PC のあらゆるユーザでは、書き換えや削除が不可能な状態に設定されたサーバ上の領域で保管。

管理者 11	金融機関や物流業者からの事務連絡を装うなどの不審なメールが迷惑メールとして分類されるよう設定する。
勤務者 10	テレワーク作業中にマルウェアに感染した場合、その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、電子メールの添付ファイルの開封やリンク先のクリックに一層の注意を払う。

＜テレワーク勤務者＞**基本対策事項**

- テレワーク勤務時に留意すべき点として、マルウェアによる標的型攻撃やフィッシング等の脅威が挙げられます。こうした脅威はオフィスで作業をしている時にも発生するのですが、オフィスでは不自然なメールが届いた場合に、「このメールはおかしくないですか？」と近くの人に相談することが簡単にできます。これに対してテレワークでは気軽に相談する相手がいない上に、電子メールを使ってやりとりをすることが多いために、届いたフィッシングメールをつい開いてしまいがちです。特に、知り合いのメールアドレスを騙って送付されてくる電子メールはテレワークにおいては最も危険です。おかしいと思ったら、そのメールを開かずに隔離することを心がけるようにしましょう。また、信頼できないウェブサイトでリンクを開く場合も同様です。

＜システム管理者＞**推奨対策事項**

テレワーク勤務者が誤って不審なメールを開封しないように、迷惑メールとして分類されるように設定する等することにより、可能な限り危険性を未然に防ぐようにします。ただし、最近の標的型攻撃に用いられる電子メールは非常に巧妙になっており、発信者に不自然な点が見られないものもあるため、完全に防ぐことは困難なことも理解しておく必要があります。

＜テレワーク勤務者＞**推奨対策事項**

テレワーク中にマルウェアに感染した場合、またはその恐れがあると感じた場合、部署の責任者やシステム管理者などへの報告を迅速に行うようにします。報告をしなかったり、報告が遅れたりするとテレワーク端末を経由してマルウェアが社内全体に感染し、被害が大きくなる恐れがあります。「報告するとしばらく作業ができなくなるなど弊害があるのでやりたくない」という気持ちになりがちですが、放置することで会社全体がマヒしてしまうなど、会社全体に損害を与えてしまう可能性も考えて判断すべきです。

【コラム】社内 SNS の利用

テレワークを行う際には、コミュニケーション手段として、電子メールを活用する頻度が高まると想定されます。これに加えて、不自然なメールが届いても相談できる相手が近くにいないため、フィッシングやなりすまし等の被害にあいやすいことが懸念されます。

このような被害を防ぐため、従業員間の連絡には、電子メールを利用せずに、社内 SNS 等のメール以外のコミュニケーション手段を活用する企業も増えています。セキュリティを向上させるだけでなく、コミュニケーションの活性化やファイルが簡単に共有できることによる業務効率化等の効果も期待されます。

テレワーク トラブル事例 と 対策〈7〉

～不審メールに関するトラブル事例～

トラブル事例

テレワーク中に勤務先の電子メールアドレスに「クレジットカード請求額のご連絡」という件名の電子メールが届いた。所有しているクレジットカードと同じ会社からの電子メールだったが、最近カードで買い物をしていないので誤請求かどうか確認しようと思い、電子メール本文に示されたリンク先にアクセスし、指示されたとおりにカード番号や有効期限等の情報を入力したところ、後日カードの不正利用をされてしまった。冷静に考えてみると、クレジットカード会社には勤務先の電子メールアドレスを伝えていなかったので、不審メールと気付くことはできたはずだった。

対策例

不審な電子メールを「迷惑メール」として通常の受信ボックスとは別の場所に保存したり、削除したりしてしまうことができます。これには次の３種類の方法があります。

＜テレワーク勤務者による対策＞

- 電子メールアプリケーションの迷惑メール対策機能を使う

＜システム管理者による対策＞

- テレワーク端末におけるマルウェア検知や異常な挙動等の脅威を一括で把握できるようなセキュリティ対策ツールの導入
- 勤務先等に設置されたメールサーバ上で一定の条件（日本語以外、実行形式の添付ファイル付、等）を満たす電子メールを分離
- インターネットサービスプロバイダが提供する迷惑メール対策機能を使う

（ウ）端末の紛失・盗難に対する対策

勤務者 11	オフィス外に情報資産を持ち出すとき、その原本を安全な場所に保存しておく。
【対象】パターン⑥（会社 PC の持ち帰り方式）	

＜テレワーク勤務者＞推奨対策事項

情報漏えいのリスクという観点からは、原本であっても複製であっても危険性は変わりません。しかしながら、例えば、ウイルス感染による電子データの改ざんや電子データの破壊に対する最終的な防御方法は、パソコン等の端末から取り外せる記録装置（外付けのハードディスク、SSD、USBメモリ等）にバックアップとしての複製を用意しておくことです。原本が残されていれば、電子データを復旧することが可能になります。

また、複製を用いることによって、ウイルス感染に限らず、人為的なミスによる電子データの消去やコンピュータの故障、紛失への対策にもなります。業務用資料の電子データを操作したり、プログラム開発、ホームページ制作等の業務を行ったりする端末においては、重要なセキュリティ対策と言えます。

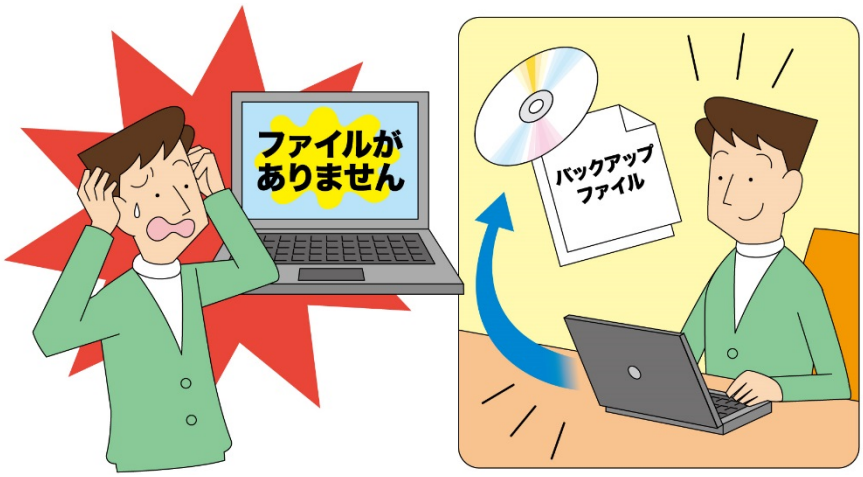


図 15　電子データのバックアップの重要性

管理者12	台帳等を整備し、貸与するテレワーク端末の所在や利用者等を管理する。
勤務者12	機密性が求められる電子データを極力管理する必要が無いように業務の方法を工夫する。やむを得ない場合は必ず暗号化して保存するとともに、端末や電子データの入った記録媒体（ＵＳＢメモリ等）等の盗難に留意する。

＜システム管理者＞**推奨対策事項**

テレワーク端末を企業側から貸し出す場合においては、あらかじめ許可を受けた従業員以外が利用することのないよう、適切な貸し出し管理を行う必要があります。あるテレワーク端末が今どこにあるか、状況がわかるような台帳等を整備します。これにパッチの適用作業の実施状況等を記入する欄を設けておくと、すぐに貸し出しができる状態かどうかを確認できるため便利です。また、私用端末を利用する場合においても、同様に台帳等を整備することは有効と考えられます。

さらに、テレワークで使用した端末やUSBメモリ等を廃棄・譲渡する場合、データをゴミ箱フォルダに捨てたり、ゴミ箱フォルダを空にするだけではデータは完全に削除されるとは限らない点に注意する必要があります。消去専用ソフトウェアを使用したり、ハードディスクを物理的に破壊したりする等の対策が必要です。

＜テレワーク勤務者＞**推奨対策事項**

テレワーク端末は、様々な場所での利用が想定され、その分、悪意の第三者が近づきやすい環境にさらされることもあります。そうしたリスクを自覚し、テレワークにおいて、機密性が求められる電子データを扱わなくて済むように業務のやり方を工夫すべきです。それでもやむを得ず管理する場合は、テレワーク端末内の電子データを暗号化する等して、他人によるテレワーク端末の不正操作を防ぐとともに、電子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。保存されているデータに関する暗号化の方法としては、ドライブやUSBメモリ全体を暗号化する方法とファイル単位の暗号化する方法の２通りがあり、情報の機密性の高さや利用方法に応じて選択します。極めて重要な情報の場合は両方を併用することも考えられます。

喫茶店や交通機関、待合室等の第三者と共有する環境でテレワーク作業を行う場合、テレワーク端末を他者に利用されないようにするためには、パスワードのほか、指紋や顔認証等によるユーザ認証、操作画面の自動ロック（無操作の状態が一定時間経過すると画面がロックされる）等の設定が必要です。鉄道や公共の待合室等で離席する場合、端末を一緒に持ち運ぶのが望ましいのですが、難しいときは画面の確実なロック、盗難防止用のワイヤーの設置などの対策が考えられます。

また、テレワークで使用した私用端末やUSBメモリ等を廃棄・譲渡する場合にも、上記＜システム管理者＞で記載した事項に注意する必要があり、勤務者が確実に行うことが難しい場合はシステム管理者が実施することも考えられます。

テレワーク トラブル事例 と 対策〈8〉
～端末の紛失に関するトラブル事例～

トラブル事例

ローカルディスクに取引実績を含む得意先リストを収納した端末を、移動中の電車内に収納していたカバンごと置き忘れた。後日それに気付いて鉄道会社に問い合わせてみたものの、落とし物としての届出はなかった。数ヶ月後、得意先から「御社にしか知らせていない電話番号にセールスの電話が来る」との苦情が寄せられるようになり、営業担当者全員で謝罪に奔走することとなった。

対策例

持ち運ぶ機会が多く、盗難や紛失の恐れがある端末については、システム管理者において端末内に情報を保持しない端末を用意し、テレワーク勤務者に使ってもらうことが最も適切な対策となります（テレワークの方式における「リモートデスクトップ方式」「仮想デスクトップ方式」「クラウド型アプリ方式」に相当）。ただし、そのような端末は携帯電話等の電波が届かない場所では利用できないため、それでは困る場合、端末内のハードディスクやSSD内の業務情報を暗号化しておき、その復号のための鍵（解除用のパスワード）を端末内に保存しないようにします。

携帯端末などでリモートワイプ（遠隔で端末内の情報を消去できる機能）があるものについては、テレワーク勤務者において日頃から有効にしておくことが望まれます。ただし意図的に情報を盗むことを目的として盗難にあった場合、電波の届かない場所で起動された場合にはリモートワイプは機能しないことも認識しておく必要があります。

（エ）重要情報の盗聴に対する対策

勤務者13	機密性が求められる電子データを送信する際には必ず暗号化する。

＜テレワーク勤務者＞**基本対策事項**

- インターネットにおいては、悪意の第三者が通信内容を傍受している可能性があります。公衆無線LAN(Wi-Fi)を利用する際にも特に注意が必要です（※）。
- 機密情報かどうかに関わらず、オフィスと電子データのやりとりを行う場合は、VPN等、通信経路を暗号化した状態でやりとりできる経路を用いるのが安全です。なお、インターネット経由での電子メールのやりとりにおいては、特に指定しない限り、暗号化は行われませんので注意してください。

（※）詳細については、総務省「Wi-Fi利用者向け簡易マニュアル」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html
を参照してください。

テレワークトラブル事例と対策〈9〉
～公衆無線 LAN 利用に関するトラブル事例～

トラブル事例

公衆無線 LAN を使って電子メールの送受を行っていたところ、添付したファイルに書かれていた秘密情報が、いつの間にか競合企業に知られてしまっていた。

対策例

次項でも説明するように、パスワードの設定されていない公衆無線 LAN や、ホテルに設置されたインターネット回線等においては、同時に利用している他者に通信内容を傍受される恐れがあります。また、パスワードが設定されていてもそのパスワードが不特定対象に公開されている場合は、なりすましの偽アクセスポイントを設置されることで同様に通信内容を傍受される可能性があります。こうした環境でテレワーク勤務者が秘密情報を送受する必要がある場合、あらかじめ秘密情報を格納したファイルを暗号化したり、暗号化機能を備えた電子メールアプリケーションを利用したりするか、VPN のような通信経路を暗号化するサービスを利用することが適切です。なお、暗号化に用いたパスワードを別のメールで送っても対策にはなりません。電話やショートメッセージ等で送るなどの工夫が必要です。

管理者 13	テレワーク端末において無線 LAN の脆弱性対策が適切に講じられるようにする。
勤務者 14	無線 LAN 利用に伴うリスクを理解し、テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する。

＜テレワーク勤務者＞**基本対策事項**

- 無線LAN（Wi-Fi）を自宅で利用する場合、次の２点に留意する必要があります。
  - 無線LANルーターでWPA2による通信経路の暗号化が行われるように設定した上で、外部から推測されにくいパスワードを設定します。
  - テレワーク端末のアップデートを行い、無線LANに関する既知の脆弱性が存在しないように対策しておきます。
- 外出先などで不特定利用者を対象とする無線LANのアクセスポイントを利用する場合は、上記の脆弱性対策を行った上で、以下のいずれかの条件を満たすような方法で利用します。
  - VPNを経由した利用。
  - URLが"https:"で接続されるようなウェブサービスに限定した利用。
  - 信頼できるアプリケーション（PC、スマートフォン、タブレット）の利用。
  - 漏えいしても問題が生じるおそれのない用途に限った利用（例：地図や経路の検索）

＜テレワーク勤務者＞**推奨対策事項**

無線LAN（Wi-Fi）に関しては暗号化していないアクセスポイントを通じた情報の盗聴の恐れがあることはいうまでもありませんが、暗号化されていてもパスワードが公然に知られているアクセスポイント（ホテルやコワーキングスペースで提供されているものを含みます）について、アクセスポイントのなりすましによる情報漏えいのリスクがあります。したがって暗号化しているから安全と考えるのではなく、VPNを用いるなどの多重的な安全対策を行うことが望まれます（図16）。

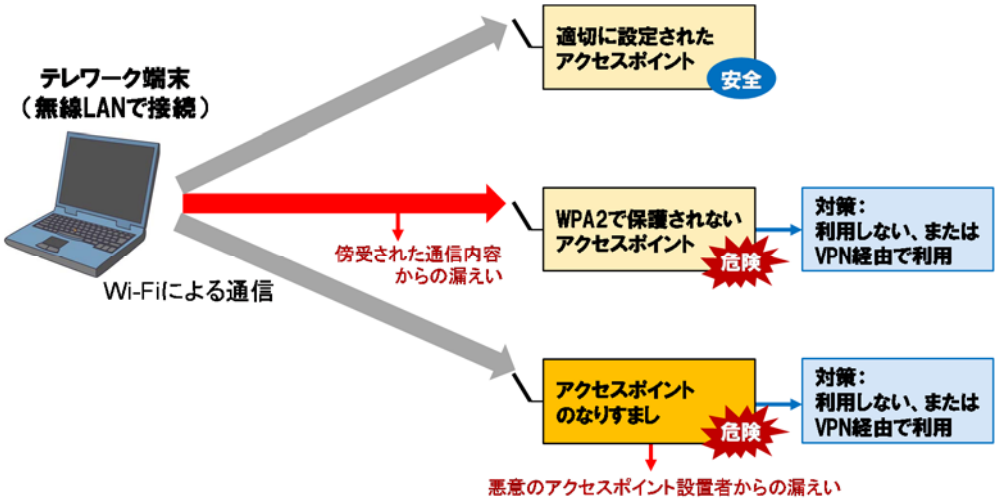


図 16　無線 LAN 利用上のリスク

勤務者15	第三者と共有する環境で作業を行う場合、端末の画面にプライバシーフィルターを装着したり、作業場所を選ぶ等により、画面の覗き見防止に努める。

＜テレワーク勤務者＞**推奨対策事項**

カフェやコワーキングスペース、交通機関、待合室等の第三者と共有する環境でテレワーク作業を行う場合、第三者による作業内容の覗き見に注意する必要があります。プライバシーフィルターをテレワーク端末の画面に装着することで、自分の横に着席している人からの覗き見を防ぐことができます。また、座席を自由に選べる場合は、自分の背中側が壁になっている席を選ぶと安心です。しかしながら、こうした工夫をしても外部の視線を完全に防ぐことはできません。こうした環境においては、第三者の視線にさらされることが望ましくない情報の閲覧や編集は避けるべきです。あらかじめこうした環境での作業が避けられないとわかっている場合は、資料から固有名詞などの機密情報を除いておくことで、漏えい時の被害を限定的にするなどの対策が考えられます。

テレワーク**トラブル事例**と**対策**〈10〉
～画面の覗き見に関するトラブル事例～

トラブル事例

出張中の新幹線の車内で未発表の新製品に関するプレゼンテーション資料を作成していたところ、その内容を何者かに「某社の新製品に関する流出情報！」としてSNSに投稿されてしまった。

対策例

テレワーク勤務者が他人の視線のある環境でテレワーク作業を行う場合、端末にプライバシーフィルターを装着することで内容を把握されにくくなります。ただし、プレゼンテーション用のスライド資料のように文字サイズが大きな文書を編集する場合、プライバシーフィルターを装着していても隣の席などから読めてしまうことがあるため、そうした資料は他人の視線のある環境では参照したり作成したりしないようにしましょう。

（オ）不正アクセスに対する対策

管理者 14	社外から社内システムへアクセスするための利用者認証について、技術的基準を明確に定め、適正に管理・運用する。
勤務者 16	社外から社内システムにアクセスするための利用者認証情報（パスワード、ＩＣカード等）を適正に管理する。
【対象】パターン①（リモートデスクトップ方式）、パターン②（仮想デスクトップ方式）、パターン⑤（アプリケーションラッピング方式）、パターン⑥（会社PCの持ち帰り方式）	

＜システム管理者＞**基本対策事項**

- テレワーク先から社内システムにアクセスする経路は、第三者に悪用された場合、社内システムへの不正侵入のための経路となる恐れがあります。したがって、テレワーク勤務者からの社内システムにアクセスするための利用者認証について、多要素認証方式を用いたり、電子証明書を併用したりするなどの技術的基準を明確に定め、適正に管理・運用する必要があります。
- また、テレワークで「リモートデスクトップ方式」や「仮想デスクトップ方式」を用いる場合、テレワーク先で見えるのは「データに関する画面イメージ（グラフィックデータ）」のみであり、電子データの実体ではありません。したがって、仮にテレワーク端末を盗まれたとしても、端末の中に電子データの実体は存在しないので、情報漏えい等の被害が生じないという利点があります。ただし、社内システムに接続するためのアカウントとパスワードが端末とともに漏れてしまうと、悪意の第三者がテレワーク勤務者になりすまして社内システムにアクセスし、さまざまな操作をすることができてしまいますので、端末にパスワード等、認証に関する情報を保存しないようにする等、適切な保護措置を講じる必要があります。

＜テレワーク勤務者＞**推奨対策事項**

社外から社内システムにアクセスするための利用者認証情報（パスワード、ＩＣカード等）が漏えいすると、第三者がなりすまして重要情報にアクセスする等、多くの重要情報が危険にさらされますので、適正に管理する必要があります。

管理者 15	テレワーク勤務者がインターネット経由で社内システムにアクセスする際のアクセス方法を定める。また、社内システムとインターネットの境界線にはファイアウォールやルータ等を設置し、アクセス状況を監視するとともに、不必要なアクセスを遮断する。
勤務者 17	インターネット経由で社内システムにアクセスする際、システム管理者が指定したアクセス方法のみを用いる。

＜システム管理者＞**基本対策事項**

- 悪意の第三者が、テレワーク端末を経由して情報システムの脆弱性を探し、社内システムへ不正に侵入したり、アカウント保持者になりすまして社内システムへ不正にアクセスしたりする場合があります。インターネットと社内システムや社内の守るべき情報資産との境界線にファイアウォール等を設置することで不正侵入を防止する対策や、本人であることを厳密に確認する認証を行ったり、アクセスするためのパスワードとしてワンタイムパスワード等を利用し、認証機能を強化したりすること等により、情報資産へのアクセスを制御し不正アクセスを防止する対策を行う必要があります。

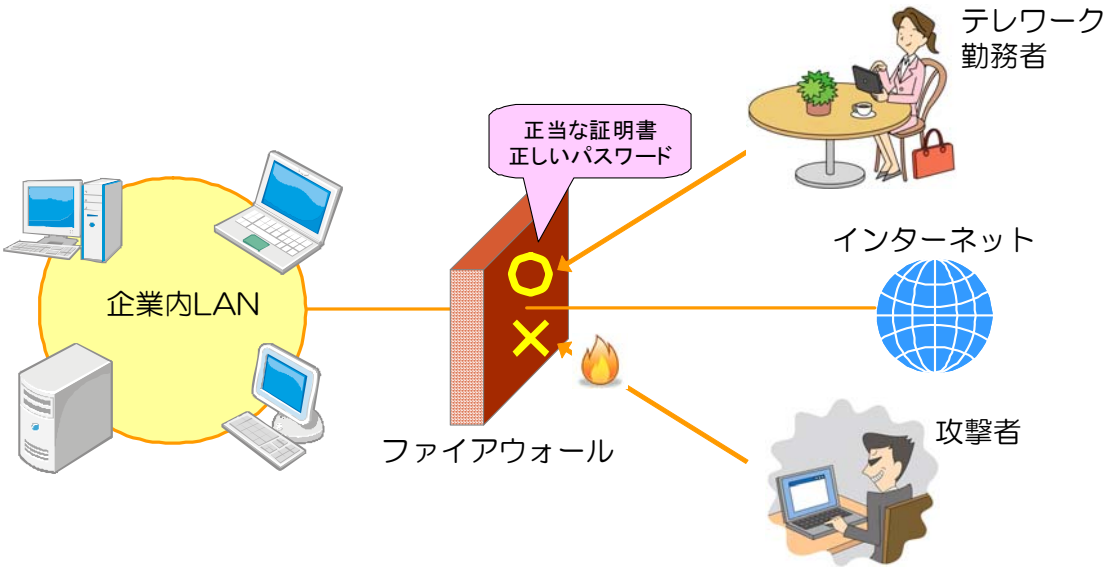


図 17　ファイアウォールの設置

＜システム管理者＞**推奨対策事項**

社内システムがウイルスやワームに感染すると、多数のテレワーク端末も感染し、ひいては社会全体に大きな影響を与えてしまう可能性があります。蔓延防止策は技術的にも運用的にも困難を伴いますが、「早期発見・早期対応」と「検知・制御」を考慮した対策を行う必要があります。

このように、不正侵入・不正アクセスによる情報漏えいを即座に検知・制御することは困難ですが、社内システムの利用状況についてアクセスログを収集することで、不正侵入・不正アクセスによる情報漏えいの調査追跡が可能となります。

＜テレワーク勤務者＞**推奨対策事項**

テレワークでは、インターネットを利用した電子データの送受をすることが想定されることから、電子データの盗聴、窃取、改ざん等の可能性があるため、暗号化された通信等、安全性の高い通信経路を確保する必要があります。このような点を考慮して、システム管理者が指定した通信手段を遵守する必要があります。

また最近ではスマートフォンから無線LANが利用されることも増えており、無線LANの適切な利用が重要になってきています。無線LANの情報セキュリティの具体的施策については、次の資料（※）を参照して下さい。

（※）総務省「Wi-Fi利用者向け簡易マニュアル」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html

さらに、テレワーク端末が「踏み台」となって、社内システムに接続されたり、第三者に対して危害を加えたりする危険性があることから、攻撃対象とならないような対策を端末に施すことにより、つねに適正な状態にしておく必要があります。

テレワーク トラブル事例 と 対策〈11〉
～「踏み台」に関するトラブル事例～

トラブル事例

自社の社内システムとインターネットの境界にファイアウォールを設置し、インターネットから社内システムへのアクセスは従業員が利用するテレワーク端末のみに制限していた。しかし、１台のテレワーク端末がマルウェアに感染したことで攻撃者に乗っ取られたことで「踏み台」にされてしまい、社内システムに侵入され、顧客情報が流出してしまった。

対策例

テレワーク端末が「踏み台」となることを防ぐためには、テレワーク勤務者において行う端末のセキュリティ対策が重要です。ウイルス対策ソフトを導入して最新の状態を保つだけでなく、端末のファイアウォール機能を有効にするなどして、外部からの侵入を防ぐ対策が求められます。
また、システム管理者においてテレワーク端末から社内システムへのアクセスログを分析することで、不自然なアクセスから攻撃者の踏み台にされた可能性を推測することができます。

管理者16	社内システムへのアクセス用のパスワードとして、強度の低いものを用いることができないように設定する。
勤務者18	テレワークで使用するパスワードは、使い回しを避け、一定以上の長さで他人に推測されにくいものを用いるように心がける。

＜システム管理者＞**基本対策事項**

- パスワードの管理に気をつける必要があることは、テレワークに限ったことではありません。しかしながら、インターネット経由で誰でもアクセスできる環境においてパスワードが漏えいすることで、第三者がなりすまして重要情報にアクセスすることに成功してしまうと、多くの重要情報が漏えいの危険にさらされてしまいます。このことから、テレワークで用いるパスワードの管理には特に注意すべきです。他の用途（ネットショッピング、ネットバンキング等）で用いているパスワードとの共用を避けるとともに、他人が推測しにくいものにするように心がけます。

＜システム管理者＞**推奨対策事項**

社内システムへのアクセスに用いるパスワードとして、次に示すような条件にあてはまるものを用いることを禁止します。

- 他のシステムやプライベートで利用しているパスワードと同じもの
- 短いもの（一般に８文字未満）
- 単純なもの（例："11111111"、"ABCDEDGH", "password"など）
- ユーザIDと同じ文字列や、ユーザIDに1文字加えただけのもの
- 辞書に載っている単語そのままやその組み合わせ（例："telework"）

このうち、短いものや単純なものについては、システムの機能として禁止することが可能な場合が多いので、こうした機能を活用することが適切です。

＜テレワーク勤務者＞**推奨対策事項**

サイト毎に異なるパスワードを使うようにすると覚えておくのが難しくなるため、覚えられないものはメモしておいても構いません。ただし、メモをテレワーク端末と同じカバン等に入れて持ち歩かないようにすることを心がける必要があります。どうしても一緒に持ち運ぶ必要がある場合は、パスワードをそのまま書くのではなく、自分だけがわかるルール（数文字抜いたり、順番を入れ替えたりする）

を決めて、メモ通り入力してもログインできないようにするとよいでしょう。

なお、パスワードを頻繁に変更する必要はありませんが、信用できない誰かに手元を見られたり、自分が所有していない端末でログインしたりした後は、できるだけ早めにパスワードを変更すべきです。

図 18　アカウントのパスワード管理

【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が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。

負担を軽減する管理方法として、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や数字を追加する方法が挙げられます。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くと良いでしょう。万が一、追加分の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。このような手法をとることで、簡単に安全なパスワード管理をすることが可能です。

（例）

マスターパスワード：telesec1794

サービスＡのパスワード：telesec1794Se1

サービスＢのパスワード：telesec1794k4O

サービスＣのパスワード：telesec17942R3

テレワークトラブル事例と対策〈12〉
～パスワード管理に関するトラブル事例～

トラブル事例

自社略称と誕生日を組み合わせたものをファイルサーバのパスワードとして設定していたところ、何者かに推測され不正ログインが成功した形跡が見つかった。当該ファイルサーバには顧客の個人情報が保存されており、情報漏えいの疑いのある顧客全員にお詫びを行う事態を招いてしまった。

プライベートで利用していたネットショップと同じパスワードをテレワークでも仕様していたところ、そのネットショップでパスワードの流出事故が発生し、流出したパスワードで勤務先にも不正アクセスされてしまった。

対策例

テレワーク勤務者においてテレワークで用いるパスワードは、こうした不正アクセスを防ぐために次の条件を満たすように作成することが必要です。具体的な作成方法は前ページのコラムを参考にして下さい。

- 他人に容易に推測されないような文字列を選ぶ
- 他のサービス等で用いているパスワードと異なる文字列を選ぶ
- 辞書等に記載されている単語等とは異なる文字列を選ぶ

【コラム】ID・パスワードを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、ブラウザに ID・パスワードを記憶させる機能を持つものがあります。ID・パスワードを入力する負担を軽減することができる便利な機能ですが、利用の際には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。このため、ID・パスワードが記憶された状態で、端末がマルウェア等に感染してしまうと、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。

（カ）外部サービスの利用に対する対策

管理者 17	メッセージングアプリケーションを含むＳＮＳに関する従業員向けの利用ルールやガイドラインを整備し、その中でテレワーク時の利用上の留意事項を明示する。
勤務者 19	メッセージングアプリケーションを含むＳＮＳをテレワークで利用する場合、社内で定められたＳＮＳ利用ルールやガイドラインに従って利用するようにする。

＜システム管理者＞基本対策事項

- Facebook、Twitter、InstagramなどのSNSは、いつ、どんな場所にいてもインターネット経由で簡単に情報を共有できることから、テレワーク勤務者にとって特に便利なサービスといえます。しかしながら、便利だからとSNSで業務に関する内容までやりとりすると業務内容の漏えいにつながる恐れがあります。
- SNSでは情報の公開範囲を「友達のみ」などに制限することができますが、友達として承認している人数が多くなると、本来送るべきでない相手にまで情報が届いてしまうことがあります。
- あらかじめSNSの利用に関して次のような内容を定めたルールやガイドラインを整備し、テレワーク勤務者に周知しておくことが望まれます。
  - 業務上の守秘義務が課せられている内容を扱わない。
  - 法律や倫理に反する発言や、事実に基づかない発言を行わない。

＜システム管理者・テレワーク勤務者＞推奨対策事項

- 特定の相手だけにメッセージを送ることを前提としたSNS（LINE、Facebook Messenger等。ここではメッセンジャー系SNSと呼びます）の場合、基本対策事項に示したようなSNSと比較すると発言内容を制限する必然性は弱まりますが、送るべき相手を間違えることで、トラブルになる可能性があります。とくにテレワークに自宅の私用端末を利用していて、その端末からメッセージを送る場合、勤務先とプライベートの知人などが混在しやすいので注意しましょう。
- テレワーク端末上でSNSを利用している場合、その端末で行った作業（ネットショッピングなど）が友達に伝わってしまうことがあります。こうした副作用が好ましくない場合、テレワーク端末ではSNSにログインしないのが安全です。

テレワークトラブル事例と対策〈13〉
～SNS 利用に関するトラブル事例～

トラブル事例

テレワーク中に勤務先から情報提供の依頼メールが来たので、SNS 上の業務用グループＸに書き込むことでそれに答えたつもりが、うっかり趣味の話題で盛り上がっていた公開のグループに書き込んでしまい、しかもそれに気付かずに放置してしまった。数時間後、外部からの指摘で初めて気付いて削除したが、書き込んだ内容の関係者への謝罪に回る羽目になり、それから３日間仕事にならなかった。

対策例

ひとつの SNS で業務上の連絡とプライベートでの交流を共用するのはこうした情報流出の事故の原因となります。対策としては以下のような方法が想定されます。

＜テレワーク勤務者による対策＞

- SNS への書き込みを行う場合、公開範囲に細心の注意を払う

＜システム管理者による対策＞

- 業務目的での SNS 利用を禁止する
- SNS の業務利用に関するガイドラインを定め、テレワーク勤務者に遵守させる
- SNS に投稿された内容に自社に関するものがないか、定期的に監視する

管理者 18	ファイル共有サービス等のパブリッククラウドサービスの利用ルールを整備し、情報漏えいにつながる恐れのある利用方法を禁止する。
勤務者 20	テレワークでファイル共有サービス等のパブリッククラウドサービスを利用する場合、社内ルールで認められた範囲で利用する。

＜システム管理者＞基本対策事項

- テレワーク勤務者が顧客とデータをやりとりする場合、勤務先のVPNを経由して送受するよりも、インターネット上のファイル共有サービスやファイル受渡サービスを使った方が手軽な場合がしばしばあります。こうしたデータの授受がテレワーク勤務者の上司やシステム管理者が知らない状況で、暗号化などの対策が不備な形でなされることで、情報漏えい等の事故につながる恐れがあります。
- そこで、テレワーク利用者向けにファイル共有サービス等を利用する場合のルールやガイドラインとして次のような内容を整備し、テレワーク勤務者に周知しておくことが望まれます。
  - あらかじめ指定したサービスのみを利用する。
  - ファイルをアップロードする際は、あらかじめファイルを暗号化しておく。
  - 相手のダウンロードが完了したら、ファイルを速やかに削除する。

＜テレワーク勤務者＞推奨対策事項

- 業務で用いるデータをパブリッククラウド上に保存しておくと、どこからでもアクセスできるので便利ですが、パブリッククラウドはインターネットに直結していることが前提のサービスですので、攻撃対象にもなりやすいことに留意する必要があります。パスワードや電子証明書を用いることで、アクセス権限を有する利用者のみがデータにアクセスできるようにできますが、次のような場合はデータが危険にさらされる恐れがあります。
  - パブリッククラウドで用いているシステムに脆弱性が発見された場合。
  - パブリッククラウド上のあるデータにアクセスする権限をもった利用者のうちいずれかのパスワード等の認証情報が漏えいした場合。
- 一部のパブリッククラウドでは、セキュリティ機能の強化を付加価値として提供（セキュアクラウドソリューション等）しているため、どうしてもインターネット上でのデータの共有を継続的に行わなければならない場合はこうしたサービスを利用することが考えられます。

テレワークトラブル事例と対策〈14〉
～パブリッククラウド利用に関するトラブル事例～

トラブル事例

あるプロジェクトでパブリッククラウド上に業務ファイルを保存し、外部委託先を含めた関係者で共有していたが、設定ミスでアクセス制御がかかっておらず、誰でもアクセスできる状態になっていた。この結果、競合他社に先駆けるメリットが失われてしまい、プロジェクトの中止に至った。

対策例

クラウドサービスに関するトラブルとして、設定ミスによる情報漏えいが多発しています。クラウドサービスを利用したファイルの安全な共有のためには、システム管理者、テレワーク勤務者それぞれにおいて、次の各点に留意することが必要です。

- 重要な情報を保存する用途に利用する前に、アクセスを許可していない ID ではアクセスできないようになっていることを確認する。
- アクセス可能なアクセス元 IP アドレスまたはドメインを制限する。
- 脆弱性対策が速やかに行われるなど、セキュリティを重視している事業者が提供するクラウドサービスを利用する
- クラウドサービスへのアクセスに用いる ID とパスワード、電子証明書等を厳正に管理する
- あらかじめファイルを暗号化した上でクラウド上に移送するなど、多重の安全対策を講じる

用語集

英字	OS (Operating System)	メモリやハードディスクの管理やキーボードなどの入出力機能など、パソコン等に基本的な動作をさせるために必要なソフトウェア。
	SSD（Solid State Drive）	半導体メモリを用いた記録装置であり、ハードディスクと同様のディスクドライブとしての利用を前提としたものをいう。
	USB メモリ	USB コネクタに接続して利用する、持ち運び可能な記録媒体。
	VDI（Virtual Desktop Infrastructure）	サーバ上に仮想の PC を複数台用意し、サーバ端末の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。シンクライアントの実現方式のひとつ。
	VPN（Virtual Private Network）	インターネット等の公衆回線網上で、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。
あ	アカウント	ネットワーク及び社内システムにログインする際の権利（ユーザ ID 等）。
	アクセスポイント	端末からインターネットに接続する際に中継を行う機器で、端末とは無線で、インターネットとは有線で通信を行うもの。
	アクセスログ	サーバやルータの動作を記録したもの。アクセス元及びアクセス先の情報を記録し、実施された操作の分析や事故発生時の原因特定などに用いられる。
	アップデート	ソフトウェアにおける不具合の部分を、安全対策を施したものに置き換えたり、ソフトウェアの機能を強化するためにソフトウェアを追加したりするための電子データ及びその操作のこと。
	安全な領域	守るべき重要な情報資産が、危害や損傷などを受けずに正常な状態でいられる領域のこと。情報セキュリティの三大要素である機密性、完全性、可用性が適切に確保されている必要があり、耐震設備や入退出管理設備などの「物理的」なものだけでなく、アクセス制御や認証など「論理的」な情報セキュリティ対策も含めて検討すべきである。
	ウイルス	マルウェアの一種。ワームと異なり自ら感染のための活動を行うことはないが、感染している PC やスマートフォンに保存されているファイルを書き換えることによって自分のコピーを保存し、そのファイルがネットワークや記録装

		置を通じて流通することで感染が拡大する。
さ	サテライトオフィス	本来の勤務先とは別に設置されるオフィス形態の施設のこと。特定の企業専用に設けるものや、複数の企業で共有するものなどがある。
	情報セキュリティポリシー	情報セキュリティに関する①「基本方針」のみを指す場合も、①「基本方針」と②「対策基準」の2つを指す場合も、①「基本方針」、②「対策基準」、③「実施内容」のすべてを指す場合もある。しかし、本ガイドラインにおいては、①②③のすべてを含む概念として情報セキュリティポリシーという用語を用いている。
	シンクライアント	パソコンやスマートフォン、タブレット端末に専用のアプリケーションをインストールしたり、周辺機器（USB メモリに似た形状のものが主流です。）を接続することで、遠く離れた社内システムに接続し、社内システム内の電子データを手元にコピーせずに閲覧や編集を行うことができるサービスにおける、端末側の機能のこと。
	脆弱性	ICT 機器・システムやその利用環境における情報セキュリティ上の欠陥のこと。機器やシステムの設計や開発・実装の過程において意図せずに作り込まれてしまう欠陥と、システムの利用時における設定ミスや不注意によって生じる欠陥の両方を含む。
た	定義ファイル	ウイルスやワーム等の特徴を収録したファイルのこと。ウイルスやワーム等を検出する際に使われる。
	テレワークセンター	テレワーク勤務者の作業場所として提供されるオフィス形態の施設のこと。サテライトオフィスとも呼ばれる。
	トロイの木馬	マルウェアの一種。有用なソフトウェアを装うことで PC やスマートフォン等の機器に取り込まれるが、ソフトウェアの一部として悪意に基づく動作を行う機能を有しており、機器の所有者にとって有害な活動を行う。
は	パーソナルファイアウォール	パソコンにインストールすることで、そのパソコンへの不正アクセス等を遮断する機能を提供するソフトウェア。
	パッチ	ソフトウェアを改善・改良するためのプログラムで、修正箇所についてのみ記述されたもの。
	標的型攻撃	ウイルスやワームのように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、発信者を詐称した電子メール等を用いて行う攻撃のこと。
	ファイアウォール	インターネット経由の不正アクセスから、内部ネットワークに接続されたサーバ等の機器を保護するための機器のこと。
	フィッシング	実在する正規のアドレスからの電子メールや Web サイトを装って、クレジット番号などの秘密情報の入力を促したり、ウイルスに感染させようとする攻撃手法のこと。

	踏み台	利用者が気付かないうちに第三者に乗っ取られ、不正アクセスや迷惑メール配信の中継地点として利用されるコンピュータのこと。
ま	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 やスマートフォンなどの機器において、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。
	ミドルウェア	ＯＳとアプリケーションの中間的な処理を行うソフトウェア。
ら	ランサムウェア	感染した PC から利用可能な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 PC の利用者に対し復号の見返りに金銭等を要求して利益を得る。
	ルータ	ネットワークに接続された機器間の通信経路の制御を行う機器のこと。
わ	ワーム	マルウェアの一種。PC やスマートフォン等の機器において活動し、ネットワークを通じて他の機器に自らのコピーを送出し、感染させる機能を有する。
	ワンタイムパスワード	一度限りしか使えないパスワードを生成することを可能にした認証方式のこと。

参考リンク集

- **テレワークではじめる働き方改革** テレワークの導入・運用ガイドブック（厚生労働省）
  http://work-holiday.mhlw.go.jp/material/pdf/category7/01_01.pdf
  厚生労働省と総務省による 3 年間の実証事業を通じて得られた知識、ノウハウをもとに、テレワークによる効果、テレワークを導入した場合の労務管理の仕方や労務管理ツールの利用方法、セキュリティを確保した ICT システム・ツールの選択方法等やその手順を紹介しています。

- **サイバーセキュリティ経営ガイドライン**（経済産業省）
  http://www.meti.go.jp/policy/netsecurity/mng_guide.html
  サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3 原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」をまとめたものです。

- **中小企業の情報セキュリティ対策ガイドライン**（独立行政法人情報処理推進機構）
  https://www.ipa.go.jp/security/keihatsu/sme/guideline/
  中小企業にとって重要な情報を漏えいや改ざん、喪失などの脅威から保護することを目的とする情報セキュリティ対策の考え方や実践方法について説明するもので、本編 2 部構成と、「5 分でできる！情報セキュリティ自社診断シート」を含む 7 種類の付録で構成されています。

- **SECURITY ACTION**（独立行政法人情報処理推進機構）
  https://www.ipa.go.jp/security/security-action/index.html
  上述の「中小企業の情報セキュリティガイドライン」の付録に示されている情報セキュリティ対策に取り組むことを自己宣言することで、「SECURITY ACTION」ロゴマークを自社の名刺、封筒、会社案内、ウェブサイト等に表示させることができ、自社の取組を対外的にアピールすることができます。

- **情報セキュリティ理解度チェック**（NPO 日本ネットワークセキュリティ協会）
  http://slb.jnsa.org/eslb/
  自社の従業員における情報セキュリティの理解度がどの程度かを把握する仕組みを提供しています。チェックの対象は「電子メールに関する知識」「インターネットの利用法」「ウイルスに関する知識」「パスワードの管理」などテレワークでも有用な知識を幅広く扱っています。基本的な機能の利用は無料ですが、機能強化した有料版もあります。

- **経営と IT 化相談窓口**（NPO IT コーディネータ協会）
  https://www.itc.or.jp/management/diagnosis/
  中小企業が抱える経営課題の解決支援のため、中小企業支援に関する専門知識や豊富な実績を有する人材として資格認定された IT コーディネータを紹介する窓口です。

- **情報処理安全確保支援士制度**（独立行政法人情報処理推進機構）
  https://www.ipa.go.jp/siensi/index.html
  サイバーセキュリティに関する専門的な知識・技能を有する人材である情報処理安全確保支援士の登録制度が平成 29 年度に開始されました。上記ウェブサイトにて登録された情報処理安全確保支援士の得意分野や連絡先等の情報を参照することができます。