テレワークセキュリティガイドライン

（第３版）

平成２５年３月

総務省

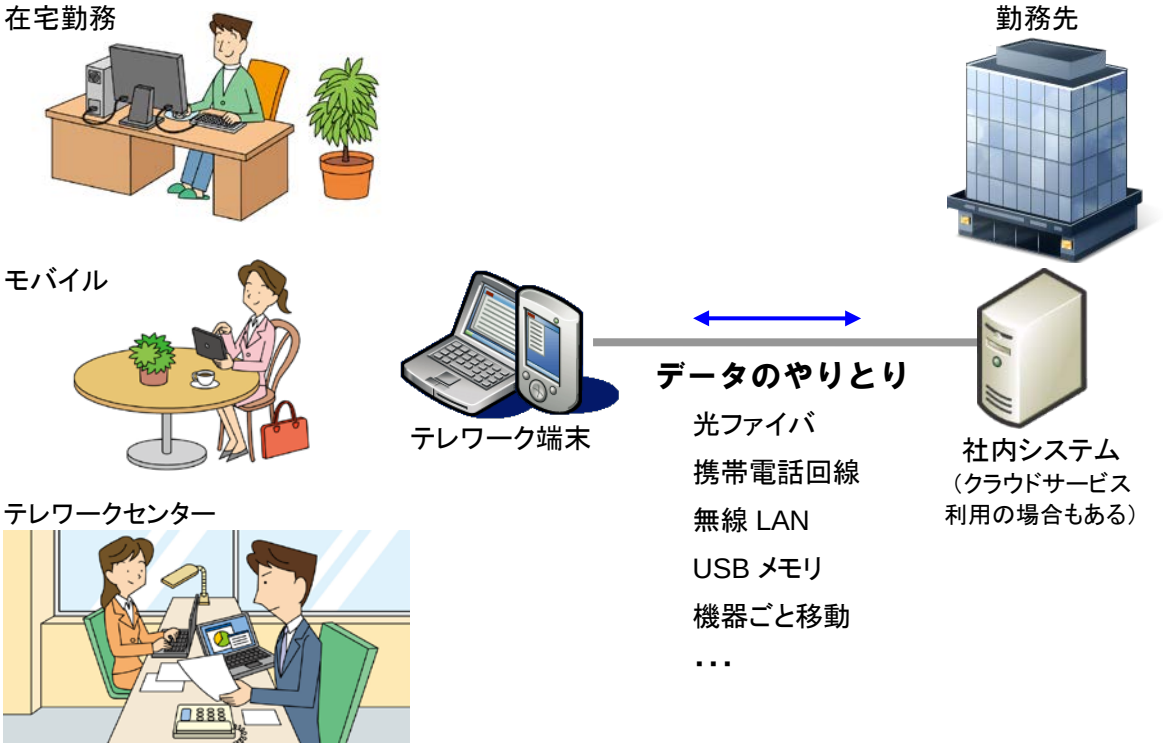
目　次

はじめに

現在、新しい働き方として「テレワーク」（下記コラム参照）が社会的に注目されています。テレワークによる時間・場所にとらわれない就労・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、事業継続能力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する可能性を秘めています。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・環境対策等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・空間的束縛から解放された多様な就労・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職場に送ったり、テレワーク勤務者同士でビデオ会議をすることで、職場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、職場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、暗号化等の情報セキュリティ技術の活用等により、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等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。

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。職場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。

本ガイドラインは、情報セキュリティマネジメントのためのベストプラクティス集として国際標準化されているJIS Q 27002規格における考え方をベースとしています。ただし、本ガイドラインはこの規格の完全な遵守を求めるのではなく、情報セキュリティ対策について不慣れな方にとっても、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ことに重きを置いて作成されています。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に関して押さえるべきポイントを示した上で、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。8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

テレワークと職場での仕事との、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。通常、情報資産は職場の中で管理され、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職場とは異なり、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、端末やその利用者に、脅威に対する「脆弱性」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。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行うにあたっては、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十分に把握、認識したうえで、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）。

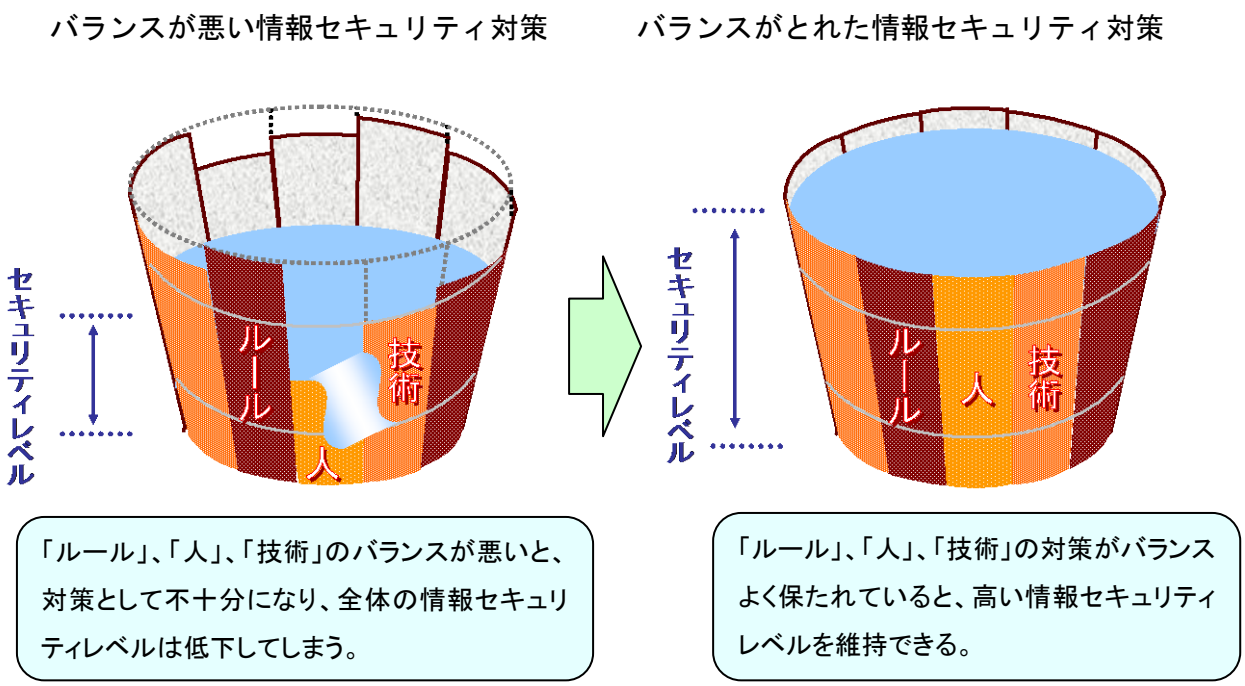


図 2　情報セキュリティ対策におけるバランスの考え方

「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、職場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職場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」と「インターネット経由で社内システムにアクセスするかどうか」をもとに、次のような３つのパターンに分類します。

表 1　テレワークの３つのパターン

	パターン①	パターン②	パターン③
	オフライン持ち出し型	オンライン持ち出し型	シンクライアント型
テレワーク端末に電子データを保存するか？	保存する	保存する	保存しない
テレワークを行う際、インターネット経由で社内システムにアクセスするか？	しない	する	する
代表的なテレワーク作業例	・職場のパソコン等の端末に電子データを入れて持ち出す ・USB メモリに電子データを保存して持ち出す	・テレワーク端末から社内システムに接続し、電子データを手元にコピーしてから作業を行う	・テレワーク端末から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
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、パターン②と③の違いは、「テレワーク端末に電子データの実体が一時的にでも存在するかどうか」です。各パターンにおいて想定される脅威と対策の考え方については、本ガイドラインの解説書で説明しています。

- パターン①（オフライン持ち出し型）
  USBメモリやパソコン等に電子データを格納して、テレワーク先まで従業員が移送することで作業を行う方法です。テレワーク先でインターネットを利用する場合でも、社内システムへのアクセスにインターネットを使わなければこの方法に該当します。テレワーク端末内に電子データがあるため、災害等で社内システムが止まってしまうような状況でもテレワーク先では作業することができますが、テレワーク先における電子データの安全確保のための対策と、移送中の安全確保のための対策がそれぞれ必要となります。

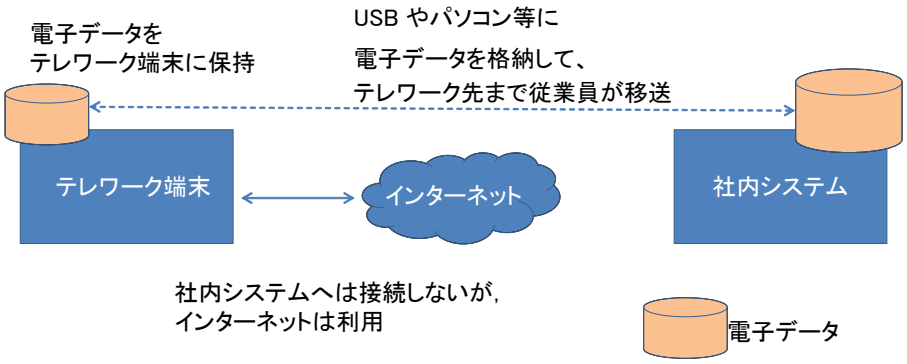


図 3　オフライン持ち出し型

- パターン②（オンライン持ち出し型）
  インターネット等を用いて電子データをテレワーク端末にコピーした上で、その電子データを用いて作業を行う方法です。①と同様、社内システムの稼働状況に関わらず作業をすることができますが、テレワーク先における電子データの安全確保のための対策と、ネットワーク上での安全確保のための対策がそれぞれ必要となります。

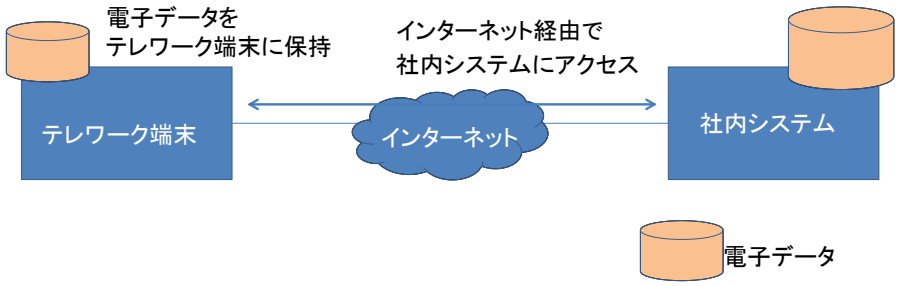


図 4　オンライン持ち出し型

- パターン③（シンクライアント型）
  シンクライアントと呼ばれる専用のアプリケーション（USBインタフェースに接続する機器の場合もあります）を用いることで、テレワーク端末に電子データの実体を持ち出すことなくテレワーク先での作業を可能とする方法です。パターン①と②に比べて、テレワーク先での安全確保のための対策が少なくて済みます。一方で、社内システムが停止してしまうと、テレワーク先から社内システムにアクセスすることができなくなりますので、テレワーク先での作業環境を維持するには社内システムを稼働し続けることが必要です。

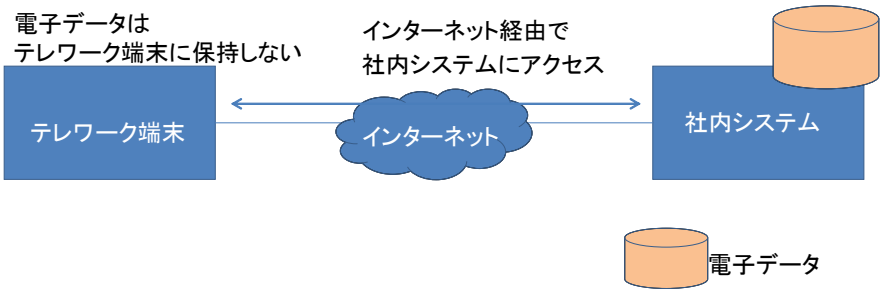


図 5　シンクライアント型

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３種類のパターンに分類されます。さらに、私物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。私物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、管理が不十分にならざるを得ないデメリットがあるため、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。

私物利用の場合、導入コストが低く抑えられると考えられがちですが、これは従業員が業務遂行に必要な性能のパソコン等の端末を所有している場合に限ります。この条件があてはまらない場合、事故の発生可能性等を考慮すると、企業から端末を貸与するという選択肢も考えられます。

（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。中小企業にとっても、コスト面での利点に加え、職場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、職場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。職場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テレワーク用の一種の「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。職場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。こうした意味では、クラウドサービスはテレワークと相性がよいと言えます。

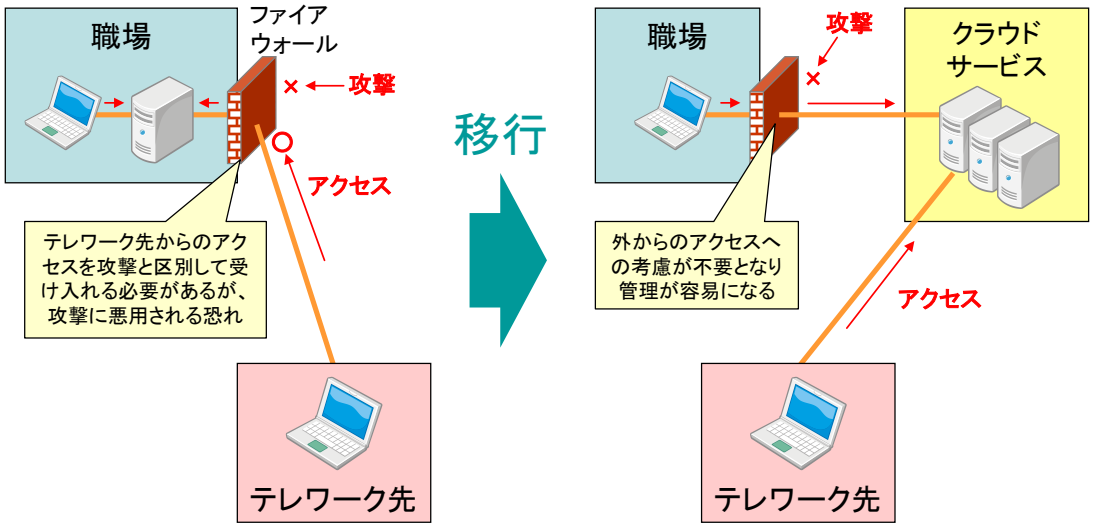


図 6　クラウドサービスへの移行

一方で、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、インターネットに接続されることが前提であるため、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。

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。

- 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。その他、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。

＜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、職場であれば、「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、職場内の端末と異なり、情報セキュリティ対策に関して「管理しづらい」または「管理できない」状況に陥りやすく、様々な脅威にさらされやすい状況にあります。このような状況で、いかに情報セキュリティを確保しながらテレワークを行うかについて意識する必要があります。

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17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、こうした項目を取捨選択、加除修正していく必要があります。

（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。	17 ページ
2	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・啓発活動を実施させる。	19 ページ
3	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。	21 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。	17 ページ
2	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。	19 ページ
3	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。	21 ページ

（悪意のソフトウェアに対する対策）

4	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。	21 ページ
5	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。	22 ページ
6	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。	22 ページ

7	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。	23 ページ
8	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。	23 ページ

（端末の紛失・盗難に対する対策）

9	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。	25 ページ

（不正侵入・踏み台に対する対策）

10	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。	27 ページ
11	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通信手段を指定する。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。	27 ページ
12	社内システム内にある重要な電子データを、安全な領域に格納する。	29 ページ
13	パスワードに有効期限を設け、テレワーク勤務者にパスワードを適宜変更させるようにする。	29 ページ
14	不審なメールを迷惑メールとして分類されるよう設定する。	30 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。	17 ページ
2	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。	19 ページ
3	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。	21 ページ

（悪意のソフトウェアに対する対策）

4	マルウェア配布等が報告されている危険なサイトにはアクセスしない。	21 ページ
5	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。	22 ページ

6	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。	22 ページ
7	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。	23 ページ
8	テレワークには必要な情報セキュリティ対策が講じら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を施さない。	23 ページ

（端末の紛失・盗難に対する対策）

9	職場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。	24 ページ
10	機密性が求められる電子データを保存する際には必ず暗号化し、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。	25 ページ

（重要情報の盗聴に対する対策）

11	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。	26 ページ
12	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。	26 ページ

（不正侵入・踏み台に対する対策）

13	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。	27 ページ
14	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通信手段のみを用いる。	27 ページ
15	テレワークで使用するパスワードは、使い回しを避け、他人に推測されにくいものを用いるように心がけ、定められたルールに従って適宜変更する。	29 ページ
16	テレワーク作業中はマルウェアによる標的型攻撃やフィッシング等の標的になりやすいことを自覚し、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。	30 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＞

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。

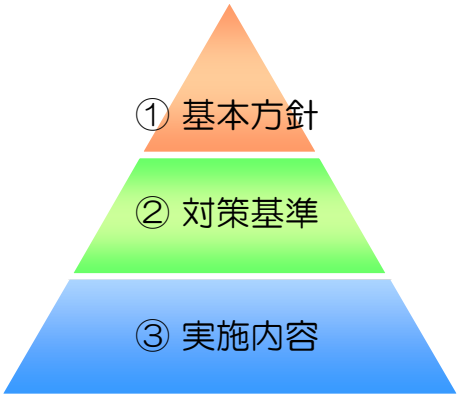


図 7　情報セキュリティポリシーの構成

情報セキュリティポリシーは、図7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。

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8）。

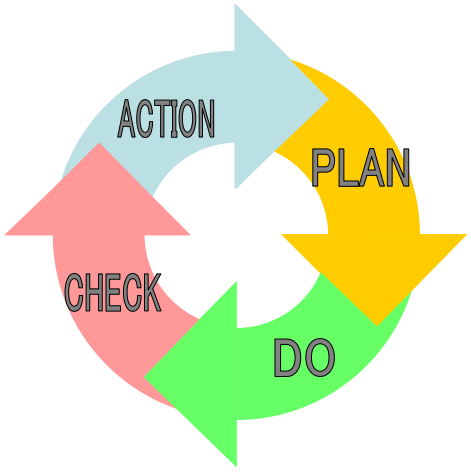


図 8　情報セキュリティに関するＰＤＣＡサイクル

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機密保持規定（電子データの持ち出しに当たっては暗号化等の機密保持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＞

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＞

職場には、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	**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・啓発活動を実施させる。**
管理者 2	**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 2	**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＞

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9）。

例えば、次ページのような分かりやすい「ポスター」を作成し、テレワーク勤務者が目をとめやすいところに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（図10）。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。

一方で、テレワーク勤務者に、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。

＜テレワーク勤務者＞

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要です。

図 9　情報セキュリティ教育

図 10　ポスターによる啓発

経営者 3	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。
管理者 3	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。
勤務者 3	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。

＜経営者・システム管理者・テレワーク勤務者＞

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とともに、訓練（予行演習）をしたりしておくことが重要です。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。

（イ）悪意のソフトウェアに対する対策

管理者 4	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 4	マルウェア配布等が報告されている危険なサイトにはアクセスしない。

＜システム管理者＞

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。

＜テレワーク勤務者＞

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。テレワークに用いる端末から、マルウェア配布等が報告されている危険なサイトにはアクセスしないようにします。

管理者5	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5	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。

＜システム管理者＞

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＞

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ソフトウェア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。

管理者6	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6	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＞

なお、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。

＜テレワーク勤務者＞

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）に更新されていることを確認する必要があります。

管理者7	**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7	**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＞

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＞

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。

管理者8	**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8	**テレワークには必要な情報セキュリティ対策が講じら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を施さない。**

＜システム管理者＞

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＞

私物の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物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。

（ウ）端末の紛失・盗難に対する対策

勤務者 9	職場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①（オフライン持ち出し型）、パターン②（オンライン持ち出し型）	

＜テレワーク勤務者＞

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。

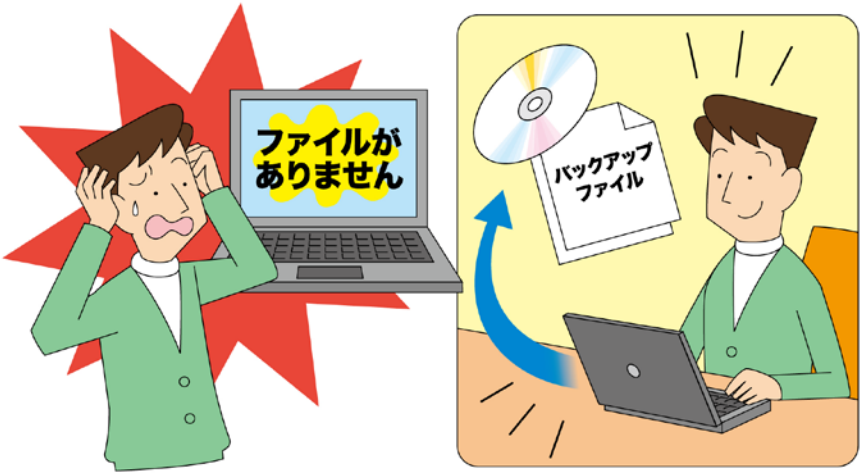


図 11　　電子データのバックアップの重要性

管理者 9	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 10	機密性が求められる電子データを保存する際には必ず暗号化し、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＞

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、私物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＞

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。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。

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、テレワーク作業中の離席にも十分な注意が必要です。鉄道や公共の待合室等で離席する場合は、できれば端末を一緒に持ち運ぶようにするほうがよいでしょう。

また、テレワークで使用した私物端末や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、勤務者自身が行うのではなくシステム管理者が確実に実施することが望ましいと考えられます。

（エ）重要情報の盗聴に対する対策

勤務者 11	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＞

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、職場と電子データのやりとりを行う場合は、VPN等、暗号化した状態で通信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「無線LANを安心して利用するための手引書」

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security.html

を参照してください。

勤務者 12	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＞

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、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。第三者の視線にさらされることが望ましくない情報を編集せざるを得ない場合は、あらかじめ企業のロゴを外したり、重要情報の書かれている部分の背景を文字と同じ色にして見えなくする等により、多少覗かれても実害がないようにすることも検討すべきです。

（オ）不正侵入・踏み台に対する対策

管理者10	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13	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②（オンライン持ち出し型）、パターン③（シンクライアント型）	

＜システム管理者＞

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、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、テレワークでシンクライアントを用いる場合、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＞

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11	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通信手段を指定する。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14	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通信手段のみを用いる。

＜システム管理者＞

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。

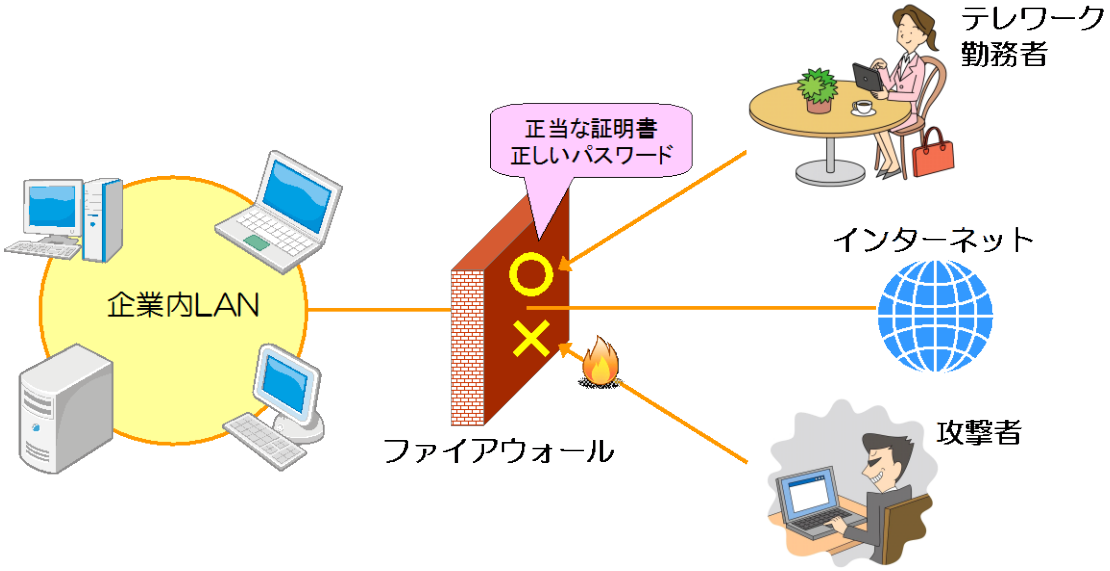


図 12　　ファイアウォールの設置

なお、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＞

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、「一般利用者が安心して無線LANを利用するために（総務

省）」を参照して下さい。

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、テレワーク端末のOSが提供するファイアウォール機能を利用するか、パーソナルファイアウォールをインストールする等して、端末を適正な状態にしておく必要があります。

管理者12	**社内システム内にある重要な電子データを、安全な領域に格納する。**

＜システム管理者＞

システムやアプリケーションの脆弱性を完全に無くすことはできないため、ネットワークに接続している限り、不正侵入・不正アクセスからの被害を完全に防ぐことはできません。きわめて重要な電子データについては、アクセスする必要があるときのみネットワークに接続し、それ以外の場合はネットワークから切り離すことも検討すべきです。

管理者13	**パスワードに有効期限を設け、テレワーク勤務者にパスワードを適宜変更させるようにする。**
勤務者15	**テレワークで使用するパスワードは、使い回しを避け、他人に推測されにくいものを用いるように心がけ、定められたルールに従って適宜変更する。**

＜システム管理者＞

パスワードに有効期限を設け、テレワーク勤務者にパスワードを適宜変更させるようにし、長期間同一のパスワードをテレワーク勤務者に使わせないようにします。

＜テレワーク勤務者＞

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。

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。

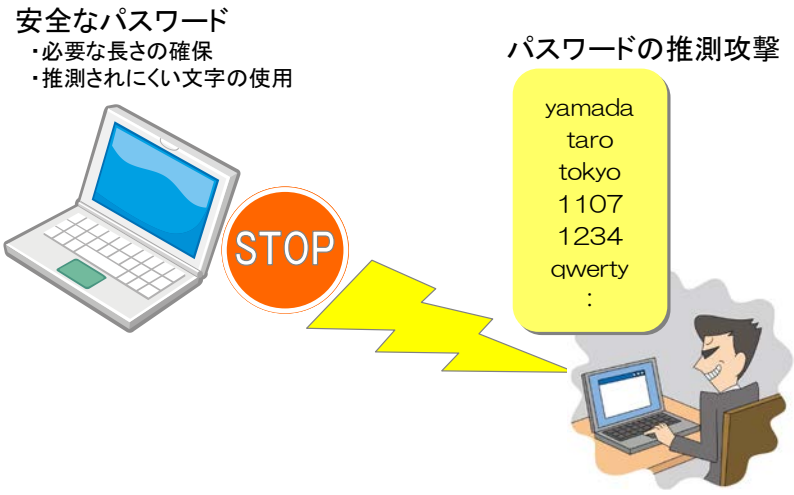


図 13　アカウントのパスワード管理

管理者 14	**不審なメールを迷惑メールとして分類されるよう設定する。**
勤務者 16	**テレワーク作業中はマルウェアによる標的型攻撃やフィッシング等の標的になりやすいことを自覚し、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。**

＜システム管理者＞

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。

＜テレワーク勤務者＞

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。こうした脅威は職場で作業をしている時にも発生するのですが、職場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。

用語集

英字	JIS Q 27002	情報セキュリティにおけるベストプラクティスをまとめ、基本的な管理項目を規定するために 2005 年に ISO と IEC により国際標準化された規格（ISO/IEC 27002）。2006 年にその日本語版をもとに JIS 規格化された。
	OS (Operating System)	メモリやハードディスクの管理やキーボード等の入出力機能等、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。
	VPN	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等に用いられる。
	アップデート	プログラム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、危害や損傷等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等の「物理的」なものだけでなく、アクセス制御や認証等「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	悪意のあるソフトウェアの一種。
さ	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。
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	悪意のあるソフトウェアの一種。
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、クレジット番号等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。
	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	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	悪意のあるソフトウェアの一種。
	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。