Sec01-02-60\_各種ガイドブックの内容要約\_働き方改革関連

1. 改訂履歴
   1. 【2020年4月27日】働き方改革を実現するために有用なITツールの種類と活用事例の内容要約
   2. 【2020年4月27日】ゼロから学べるテレワーク導入完全ガイド【V-CUBE】の内容要約
   3. 【2020年4月23日】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】の内容要約
   4. 【2020年4月21日】原本をMindManagerへ移行
   5. 【2020年4月21日】Sec01-02から働き方改革関連を分離
2. ファイル種別
   1. MindManager→html版

ドキュメントを参照: [Page not found &middot; GitHub Pages](https://bluemoon55.github.io/Sharing_Knowledge/MindManager/Sec01-02-60_各種ガイドブックの内容要約_働き方改革関連.html)

1. ●情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン【厚生労働省】

ドキュメントを参照: [3003011.pdf](https://www.mhlw.go.jp/file/06-Seisakujouhou-11200000-Roudoukijunkyoku/3003011.pdf)

* 1. ガイドラインの主なポイント
     1. ○ テレワークのメリット
        1. テレワークは労働者が所属する事業場での勤務に比べて、働く時間や場所を柔軟に活用することが可能
           1. 労働者にとってのメリット

・通勤時間の短縮

・業務の効率化･時間外労働の削減

・育児や介護と仕事の両立の一助に

・仕事と生活の調和を図ることが可能 等

* + - * 1. 使用者にとってのメリット

・業務効率化による生産性の向上

・育児･介護等による労働者の離職の防止

・遠隔地の優秀な人材の確保

・オフィスコストの削減 等

* + 1. ○ テレワークの問題や課題
       1. 問題や課題
          1. ・労働時間の管理が難しい
          2. ・仕事と仕事以外の切り分けが難しい
          3. ・長時間労働になりやすい 等
       2. ↓テレワークにおける適切な労務管理の実施は、テレワークの普及の前提 となる重要な要素
    2. ○ 労働基準関係法令の適用
       1. テレワークを行う労働者にも、労働基準法、最低賃金法、労働安全衛生法、労働者災害補償保険法等の労働基準関係法令が適用される
       2. 業務を行う場所に応じたテレワークの特徴
          1. ① 在宅勤務

通勤の必要がないため、時 間を有効に活用することが 可能となり、仕事と家庭生 活との両立に繋がる

* + - * 1. ② サテライトオフィス勤務

自宅近くや通勤途中の場所など に設けられたサテライトオフィ スを利用することで、通勤時間 を短縮しつつ、作業環境の整っ た場所での就労が可能

* + - * 1. ③ モバイル勤務

労働者が自由に働く場所を選 択できる、外勤における移動 時間を利用できる等、業務の 効率化を図ることが可能

* 1. ガイドラインの概要
     1. １趣旨
     2. ２労働基準関係法令の適用及び留意点等
        1. （１）労働基準関係法令の適用
        2. （２）労働基準法の適用に関する留意点
        3. （３）長時間労働対策について
           1. ・テレワークについては、労働者が使用者と離れた場所で勤務をするため、長時間労働を招くおそれがあることも指摘されており、使用者は、長時間労働による健康障害防止を図ることが求められる
           2. ① メール送付の抑制

役職者等から時間外、休日又は深夜におけるメールを送付することの自粛を命ずる

* + - * 1. ② システムへのアクセス制限

外部のパソコン等から深夜・休日はアクセスできないよう設定すること

* + - * 1. ③テレワークを行う際の時間外・休日・深夜労働の原則禁止等

業務の効率化やワークライフバランスの実現の観点から、時間外・休日・深夜労働を原則禁止とすること又は使用者等による許可制とすること

* + - * 1. ④長時間労働等を行う労働者への注意喚起

長時間労働が生じるおそれのある労働者や、休日・深夜労働が生じた労働者に対して、労働時間の記録や、労務管理システムを活用して注意喚起を行うこと

* + - 1. （４）労働安全衛生法の適用及び留意点
      2. （５）労働災害の補償に関する留意点
    1. ３テレワークを適切に導入及び実施するに当たっての注意点
       1. （１）労使双方の共通の認識
       2. （２）業務の円滑な遂行
       3. （３）業績評価等の取扱い
       4. （４）通信費、情報通信機器等のテレワークに要する費用負担の取扱い
       5. （５）社内教育等の取扱い
    2. ４ テレワークを行う労働者の自律
       1. ・労働者においても、勤務する時間帯や自らの健康に十分に注意を払いつつ、作業能率を勘案して自律的に業務を遂行することが求められる

1. ●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】

ドキュメントを参照: [01\_01.pdf](https://work-holiday.mhlw.go.jp/material/pdf/category7/01_01.pdf)

* 1. 目次
     1. はじめに
        1. テレワークは、『ICT（情報通信技術）を活用し、時間や場所を有効に活用できる柔軟な働き方』です。
        2. 近年、スマートフォン、タブレット端末等の情報通信機器が発達するとともに、通信サービスについても、ブロードバンドサービスが普及し、運用コストやセキュリティ確保の課題も解決されつつあり、テレワークを取巻く環境は、飛躍的に変化しています。
        3. 企業にとってのメリット
           1. • 人材の確保・育成
           2. • 業務プロセスの革新
           3. • 事業運営コストの削減
           4. • 非常時の事業継続性（BCP）の確保
           5. •企業内外の連携強化による事業競争力の向上
           6. • 人材の離職抑制・就労継続支援
           7. • 企業ブランド・企業イメージの向上
        4. 従業員にとってのメリット
           1. • ワーク・ライフ・バランスの向上
           2. • 生産性の向上
           3. • 自律・自己管理的な働き方
           4. • 職場との連携強化
           5. •仕事全体の満足度向上と労働意欲の向上
        5. ［本書が想定している読者］
           1. ■経営者

直面する経営課題（生産性向上、グローバル化の推進、オフィスコストの削減、優秀な人材の採用・流出防止、BCP（事業継続性）の確保等）の解決に向け、テレワークがどのように役立つかを理解し、自社の施策として導入・普及拡大を検討するために

* + - * 1. ■テレワークの推進担当者（経営企画担当、人事・総務担当、情報システム担当など）

テレワークの導入、普及拡大に当たり、実務的な知識やノウハウを習得し、実践につなげるために

* + 1. Ⅰ　基礎編
       1. 1.テレワークとは
          1. 在宅勤務（終日在宅勤務）

●従業員のワーク・ライフ・バランスを実現する上で効果的です。

●育児・介護期の従業員がキャリアの継続を図ることができます。また、障がいなどにより通勤が困難な従業員の就労継続にも効果的です。

●静かな環境を整えやすいため、集中して業務を行うことができます。

* + - * 1. モバイルワーク

●営業職など、所属オフィス外での業務が多い職種にとって特に有用です。

●移動時間を有効活用できる、顧客先で迅速に対応できるなどのメリットがあります。

* + - * 1. サテライトオフィス勤務 （施設利用型勤務）

●顧客先に近い施設の利用

顧客先に近い施設を利用することで、迅速な顧客対応、帰社などのための移動時間の削減により、業務を効率化できます。

●従業員の自宅に近い施設の利用

従業員の自宅に近い施設を利用することで、所属するオフィスまで通勤することが困難な人材を活用できます。

●遊休施設や空き家などの活用

遊休施設や空き家などを活用することで、オフィスコストを抑えることができます。

オフィススペースの契約形態

専用型

自社・自社グループ専用として利用され、従業員が営業活動で移動中、あるいは出張中である場合などに立ち寄って就業できるオフィススペースです。事業所とは別にスペースを設置する方法と、各地の事業所内にテレワーク専用のスペースを設ける「スポットオフィス」が存在します。

共用型

複数の企業がシェアして利用するオフィススペースです。最近では、「シェアオフィス」や「コワーキングスペース」ともいい、企業や、フリーランス、起業家が一定の契約のもとにスペースを活用して仕事をしたり、情報交換やイベント開催を行ってビジネスを行うオフィスもあります。

* + - 1. 2.我が国のテレワークを取り巻く現状
      2. 3.テレワークの効果
         1. 企業（経営者・推進担当者）の感じる効果

優秀な人材の確保や雇用継続につながった

資料の電子化や業務改善の機会となった

通勤費やオフィス維持費などを削減できた

非常時でも事業を継続でき、早期復旧もしやすかった

顧客との連携強化、従業員の連携強化になった

離職率が改善し、従業員の定着率向上が図れた

企業のブランドやイメージを向上させることができた

* + - * 1. 従業員（テレワーク実施者）の感じる効果

家族と過ごす時間や趣味の時間が増えた

集中力が増して、仕事の効率が良くなった

自律的に仕事を進めることができる能力が強化された

職場と密に連携を図るようになり、これまで以上に信頼感が強くなった

仕事の満足度が上がり、仕事に対する意欲が増した

* + - * 1. 1　企業にとっての効果

【コラム】業務の見える化

業務の「見える化」とは、成果だけでなく、業務の進捗状況を表やグラフ等にすることで、作業者や上司・同僚がその業務の進み具合を適宜確認できるようにすることです。

例えば、スケジュール共有ツールなどでその日に進める業務の内容を周知する、又は作成する資料を誰でも閲覧可能な共有ファイルに格納することで資料の作成状況を共有するなどの方法があります。

業務の「見える化」をすると、作業者は自身以外の従業員と業務の分担がしやすくなるほか、上司が業務の進み具合を管理しやすくなるメリットがあります。

また、業務に対する評価について、成果のみではなく、どのように業務を進めたかのプロセスも評価対象にすることができます。このプロセス評価は、作業者が業務に取り組んだ労力全体の評価を受けられることから、作業に当たった従業員の仕事に対するモチベーションが向上しやすくなったり、業務の無駄や不手際をチェックすることで次回以降の業務の進め方が改善したりする効果があります。

【コラム】キャリアの継続を可能にするテレワーク利用

A社では、従業員のほとんどが出社せず、終日在宅勤務を行っています。中には、配偶者の転勤に合わせて、所属するオフィスから遠く離れた場所に転居した、高い専門性を持つ技術者もいます。

従業員には、業務遂行が十分に可能なシステムが提供され、顧客との会議や従業員同士の打ち合わせには、Web 会議システムを活用しています。

一方、従業員間の対面でのコミュニケーションも大切にしており、2 か月に 1回は全従業員が本社に集合し、顔を合わせて会議と食事をする会を設けるなどの工夫をしています。

* + - * 1. 2　従業員にとっての効果

ⅰ. ワーク・ライフ・バランスの向上

•通勤時の身体的負担を軽減し、自由に使える時間が増加することで、ワーク・ライフ・バランスを向上させることができる

•生産性の向上によってプライベートの時間をきちんと確保でき、仕事と生活のメリハリがついた

ⅱ. 生産性・創造性の向上

•一人で作業するための空間をつくることで、自分自身の担当業務に集中して取り組むことができるため、生産性・創造性が向上する

ⅲ. 自律・自己管理的な働き方

•目標を定めて業務進捗や業績管理を自律的に行う必要性があるため、セルフマネジメント力が養われる

•ワーク・ライフ・バランスの実現に向けて、仕事と生活との切り分けやバランスをより一層意識するようになり、仕事にメリハリをつけるようになる

ⅳ. 職場との連携強化

•意識的にコミュニケーションを図ろうとする結果、今まで以上にコミュニケーションの回数が増え、上司・同僚との信頼感が高まる

•ツールを介したコミュニケーションがやり取りの気軽さを生み、コミュニケーションの回数が増える

•業務を「見える化」することで、上司と部下が業務の連携を図りやすくなり、信頼関係が向上する

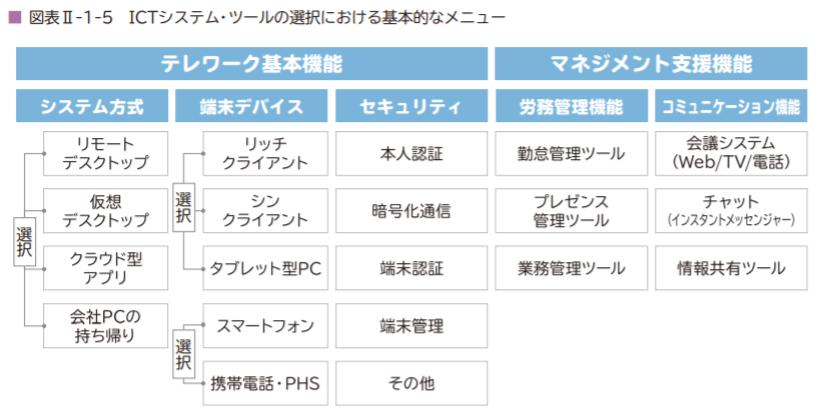
ⅴ.仕事全体の満足度向上・就業意欲の向上

•柔軟な働き方ができるため、ワーク・ライフ・バランスを実現でき、仕事に対する満足度が向上する

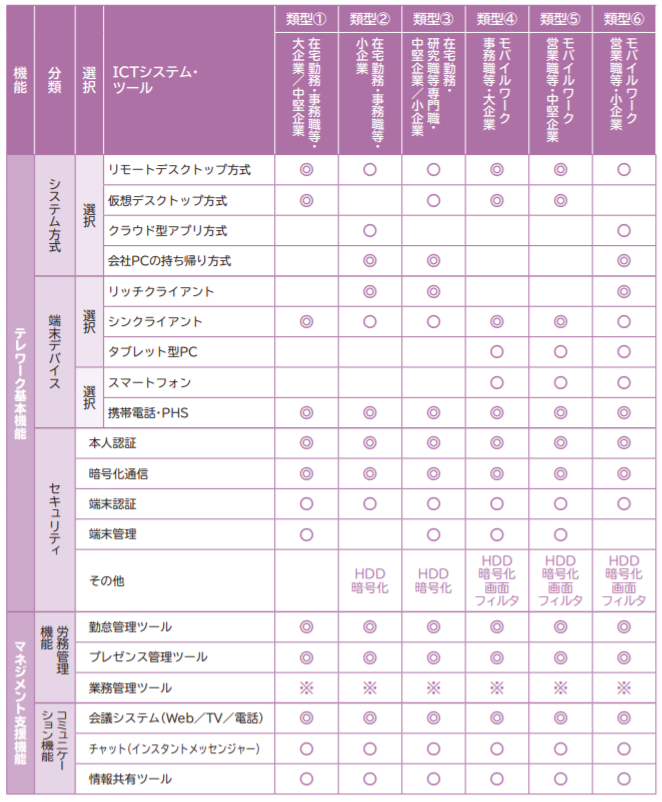
•働きたいという意欲を持ちながらも十分な労働時間を確保できなかった人材にとって、テレワークが労働時間の確保に役立ち、より仕事への意欲がより向上する

* + 1. Ⅱ　実践編
       1. 第1章　モデル類型とは
          1. 1.「テレワークモデル実証事業」の効果
          2. 2.モデル類型における①テレワーク形態、②職種、③企業規模
          3. 3.モデル類型の選択
          4. 4.各モデル類型におけるICTシステム・ツール

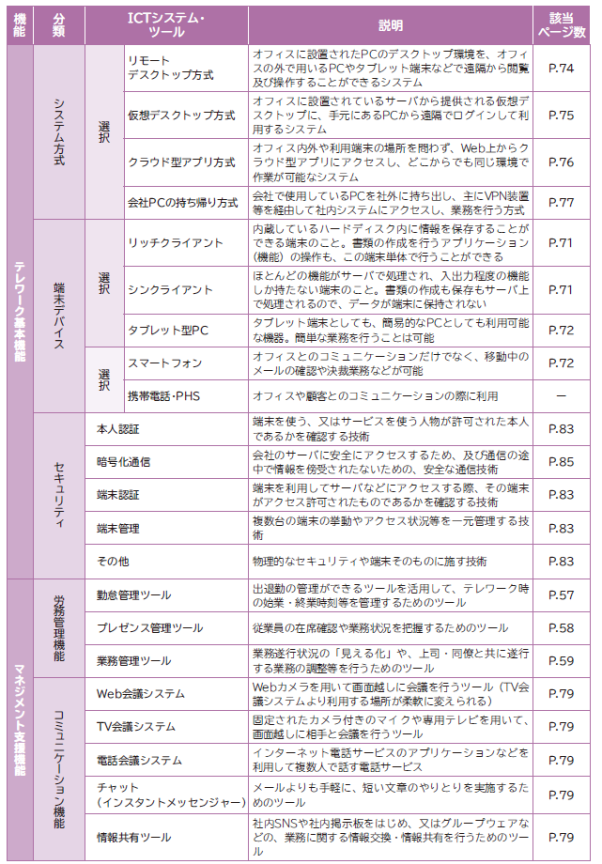
■図表Ⅱ-1-5　ICTシステム・ツールの選択における基本的なメニュー



■図表Ⅱ-1-6　各モデル類型におけるICTシステム・ツールの選択（一覧）



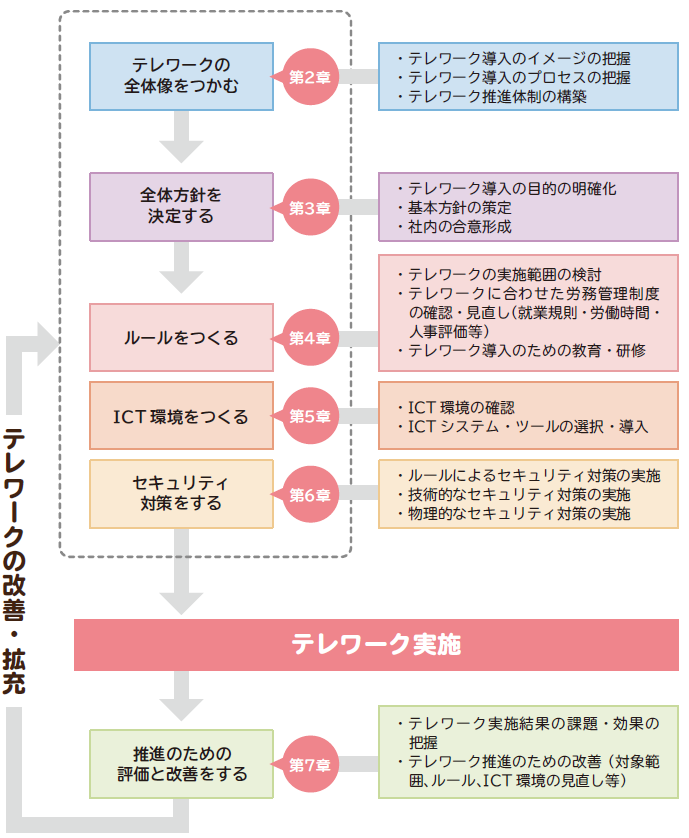
■図表Ⅱ-1-7　各モデル類型におけるICTシステム・ツールの説明



※各モデル類型におけるICTシステム・ツールの説明

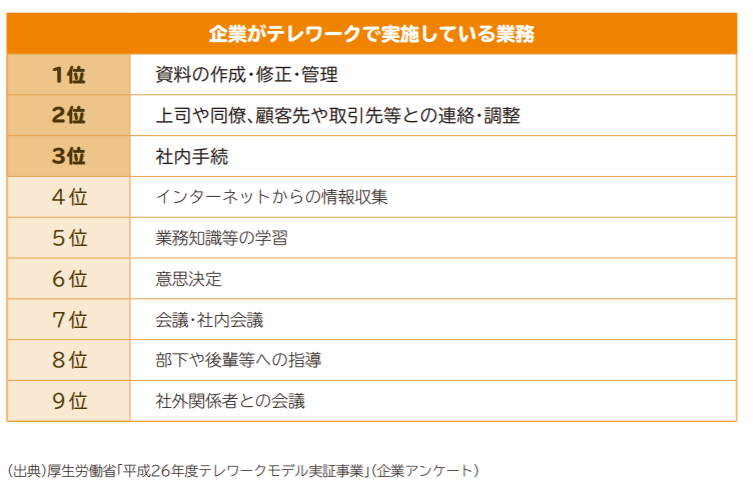
* + - 1. 第２章　テレワーク導入の手順・推進体制
         1. 1.テレワーク導入のイメージ
         2. 2.導入のプロセス

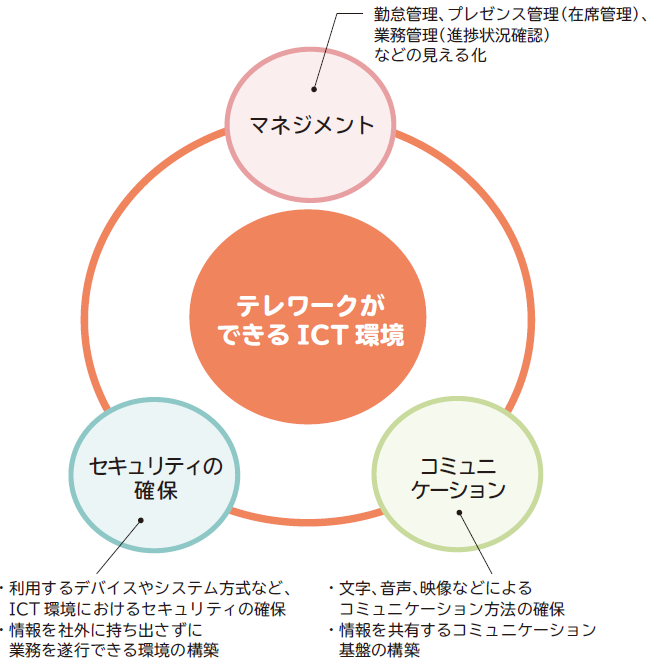
※各モデル類型におけるICTシステム・ツールの説明



* + - * 1. 3.推進体制の構築
      1. 第３章　テレワーク実施のための全体方針の決定
         1. 1.導入目的の明確化
         2. 2.基本方針の策定
         3. 3.社内の合意形成のポイント
      2. 第４章　テレワークのためのルールづくり
         1. 1.テレワーク実施範囲の検討

図表Ⅱ-4-2　企業がテレワークで実施している業務



* + - * 1. 2.労務管理
        2. 3.導入のための教育・研修
    1. 第５章　テレワークのためのICT環境づくり
       1. 図表Ⅱ-5-1 テレワークができるICT環境
          1. 
       2. 1.ICT環境導入のための手順
          1. 導入手順（例）

❶現在のICT環境の確認

❷テレワーク環境の方式選択・各種ツールの選択

❸導入に必要な期間の確認

❹導入中の業務の停滞箇所・要調整の確認

❺導入期間の全社周知（システムの利用に関する従業員向け研修）

❻システム導入～システムの実際の稼動

* + - 1. 2.テレワーク環境の選択
         1. （1） 利用端末の確認

❶リッチクライアント（ファットクライアント）型PC

❷ シンクライアント型PC

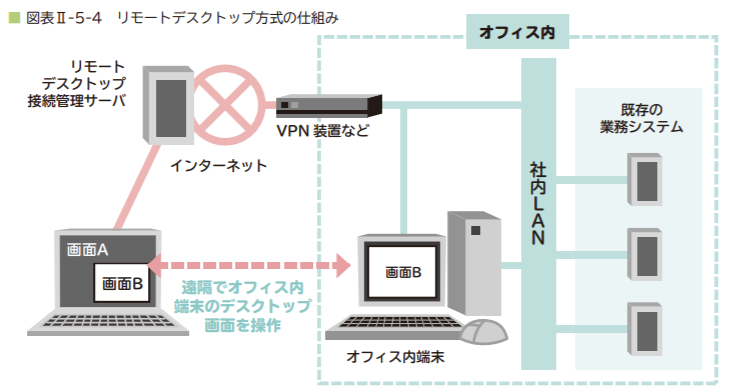
1）リッチクライアントを専用システムでシンクライアント化する方法

2）シンクライアント専用PCを利用する方法

3）リモートデスクトップ接続クライアントを利用する方法

❸ タブレット型PC・スマートフォン

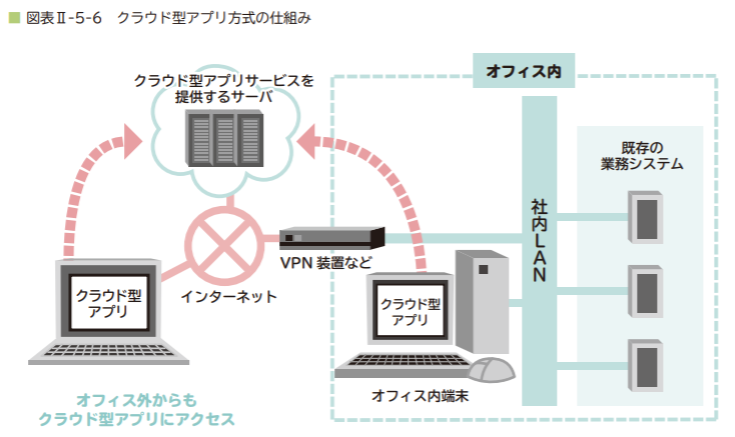
* + - * 1. （2） ネットワーク
        2. （3） サーバ
      1. 3.テレワーク環境におけるシステム方式の選択
         1. （１）リモートデスクトップ方式



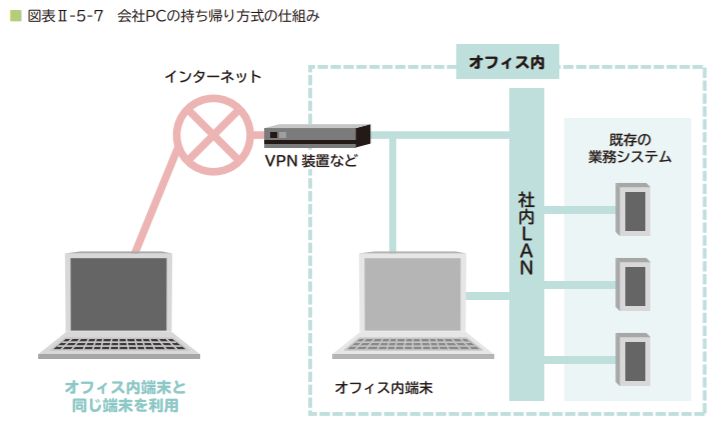
セキュリティ

作業は遠隔操作で実施する。そのため、全ての作業がオフィスの端末で行っている状態と同じで、手元の端末にデータは残らない。また、保存したファイルはオフィスにある端末上に保存される。情報漏えいが起きにくいメリットがある。

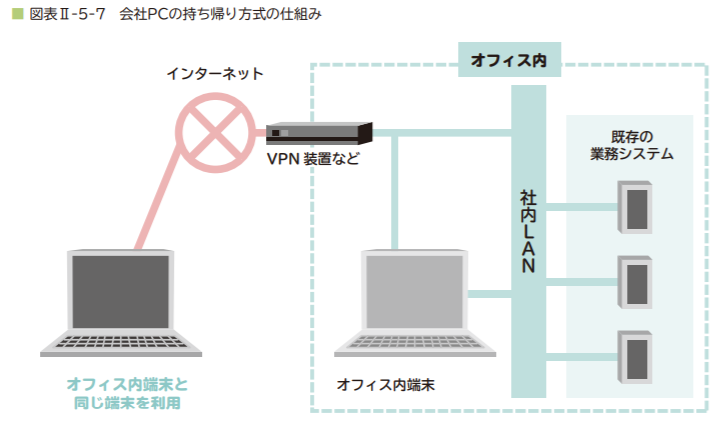
* + - * 1. （２）仮想デスクトップ方式



* + - * 1. （３）クラウド型アプリ方式



* + - * 1. （４）会社PC の持ち帰り方式



* + - 1. 4.労務管理ツール
      2. 5.コミュニケーションツール
         1. ❶ 会議システム
         2. ❷Eメール・チャット（インスタントメッセンジャー）
         3. ❸ 情報共有ツール

1） データ共有ツール

2） グループウェア

* + 1. 第６章　安全なテレワークのためのセキュリティ対策
       1. 図表Ⅱ-6-1　テレワークに必要なセキュリティの考え方
          1. 
       2. 1.ルールによるセキュリティ対策
          1. （1）セキュリティガイドラインの策定

●基本方針：セキュリティ全体の根幹

●対策基準：基本方針をもとに実施すべきことや守るべきことを規定したもの

●実施手順：対策基準の事項を具体的に実行するための手順を示したもの

* + - * 1. （2）セキュリティルール・情報管理ルールの策定

●自宅における作業環境、PC の保管及び管理方法

●自宅における休憩中の PC の取扱い 〔ロックだけでいいのか、保管して鍵をかけるのか〕

●モバイルワークにおけるPCの管理方法 〔体から離さない、ストラップをつける、のぞき見防止フィルターをつける〕

●オフィスから持ち出す PCの管理 〔暗号化、BIOSパスワードなどを義務付け〕

●オフィス以外での情報管理 〔紙情報の管理、共用スペースでの情報管理〕

図表Ⅱ-6-2　セキュリティルール・情報管理ルールの例

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、セキュリティガイドラインが定める技術的・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。

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。

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。また、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。

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）の盗難に留意する。また、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。

* + - * 1. （3）ガイドラインとルールの遵守・浸透
      1. 2.技術的なセキュリティ対策
         1. （1） アクセスの管理・制限

本人認証

端末認証

* + - * 1. （２）暗号による管理

ハードディスク（HDD）暗号化

セキュアコンテナ

携帯電話等にセキュアコンテナ（暗号化された企業用の業務データエリア）を作成するソフト及びサービス

情報漏えい対策付きの USB メモリ

* + - * 1. （３）運用のセキュリティ

電子データの原本保存

情報が改ざんされていない状態を保つためにも、情報の原本を常に意識して保存することはセキュリティ対策にもつながります。

例えばデータを自動バックアップするようにして、デー

タが誤って削除されてしまった場合でもデータの呼び出しや復元ができるようにしたり、データの閲覧記録や作業記録を取ったり、システム内で行われたことを監視や記録するソフトウェアを利用します。

このセキュリティでは、ネットワークやシステムの利用のハードルを上げるものではありません。

より厳密に「改ざんされていないデータ」を得るには、保存した時刻の認証や電子署名、印刷データ電子化・管理による方法も利用できます。

ウイルス対策ソフト

インターネットに接続したり、外付けの記録媒体に接続する可能性がある限り、端末はウイルスに感染するおそれがあります。

ウイルスに感染すると端末が不具合を起こすほか、情報漏えいの危険性が高まります。そこで、事前に端末内にウイルス対策ソフトを導入し、ウイルスの早期検知、検知した場合の駆除を行うことができるようにしておく必要があります。

その機能を果たすソフトが、セキュリティ対策ソフトです。近年は不正アクセス検知や不正プログラム検出など、様々な悪意あるソフトウェアに対して有効な製品が増えています。

ウイルス対策ソフトは端末だけではなく、サーバに対して機能するものもあります。シンクライアント型端末を利用する場合はサーバのセキュリティを確保するために、端末自体よりもサーバに対してウイルス対策ソフトを導入すると効果的、かつコスト面から見ても有用です。

【コラム】導入した対策ソフトを含むソフトウェアを最新の状態にするアップデートの必要性

悪意あるソフトウェア等の手口は日々進化しており、対策ソフトのメーカーもそれに対抗すべく、日々最新の対策を講じています。そのため、導入した対策ソフトを含むソフトウェアを最新の状態にするアップデートを定期的に行うことが重要です。

特に情報システム関連の部署は、最新のソフトウェアがテレワーク実施者の利用しているPCに反映されているか、常に注意が必要です。

例えばリモートデスクトップを採用している職場の場合、オフィス内の PC が常時起動されたまま、再起動によって更新されるソフトウェアがなかなか更新されないことも有ります。

情報システム関連の部署やテレワーク推進部署が適宜メールや掲示板などを用いて事業所内に更新の周知を行い、システム上からも最新バージョンのシステムに切り替わっていないPCがないか、注意しましょう。

また、定期的なウイルスチェック（ウイルススキャン）の徹底も大切です。

* + - * 1. （４）ネットワークのセキュリティ

概要

ネットワークを通じてやり取りされる情報、及びネットワークを支える機器・設備を安全に使い続けるため、ウイルス感染や不正アクセスがされにくいネットワークを用意しましょう。

十分にセキュリティ対策を施していないネットワークを使い続けた結果、情報資産全体に悪影響となり、最悪の場合、事業を一時的に停止しなければならない事態にもなるおそれがあります。

ネットワークのセキュリティは特に、個々のテレワーク実施者よりも組織の情報システムを担当する部署の意識が問われています。

テレワーク実施者が安全なネットワークを利用してアクセスできる環境を提供し、ネットワークからの不正侵入に対して対策をするとともに、日頃から問題が起きていないかをチェックする体制を作りましょう。

より安全な回線の選択

テレワークでは、外部のネットワークを介して、社内ネットワークに通信をすることになります。

そのため、外部のネットワークを利用する場合に、テレワーク実施者が定められたVPN回線に接続してアクセス（暗号化通信）するルールやシステムを導入する、あるいは不正な通過パケットを自動的に発見、もしくは遮断する措置のできるシステムが求められます。

これらは一定期間ごとに記録を管理して不正な動きの有無を確認したり、システムがきちんと稼動しているのかの定期チェックが必要です。

また、モバイルワーク等を実施する際には、ウイルス感染や盗聴の危険性のある公衆Wi-Fiは利用せず、通信キャリアが提供するモバイルルータを利用するといったルールづくりが望まれます。

公衆Wi-Fiを利用する際には、通信路が暗号化されたサービスを利用することが必要です。

やむを得ず、それ以外の公衆 Wi-Fi を利用する際には、全て暗号化された通信のみを利用することで安全性を高めることができますが、意識しないところで通信するソフトなどもあるため注意が必要です。

こうした対策ができない場合には、機密情報は扱わず、公開情報のみを利用する業務に限定するなどの対応が求められます

サーバ証明書

第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施しましょう。

正規のサーバ証明書の取得に加え、紛らわしくないドメイン名を使うこと等により、テレワーク実施者によるサーバ正当性の確認を容易にするとよいでしょう。

【コラム】モバイルワークにおけるセキュリティ対策の注意点等（例）

モバイルワーク時のルール（例）

①オフィス外を移動するときは、必ずPCを鞄に入れて常時携帯する

②PCのローカルエリアにファイルを保存しない

③ハードディスクを暗号化する

④社外環境で印刷出力しない

⑤インターネット接続は会社支給のモバイルルータからのみ可とする

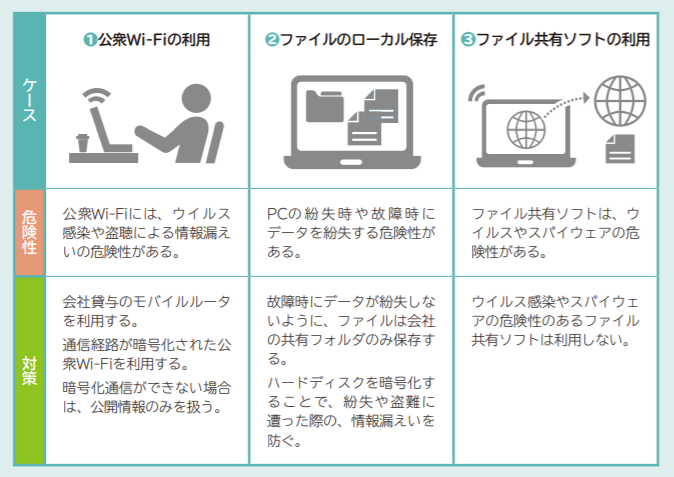
⑥社内環境へは暗号化通信を利用して接続する

⑦のぞき見防止フィルターを必ず装着する

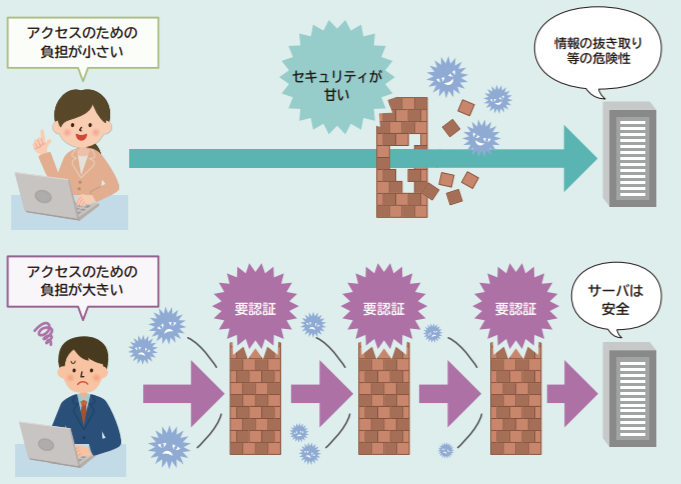
⑧PCを持ち帰る時は、上長にメールで報告する

⑨Web会議等の音声が発せられるときは、周囲に聞かれないよう注意する

危険性と対策について



【コラム】セキュリティ保護と業務効率向上とのジレンマ



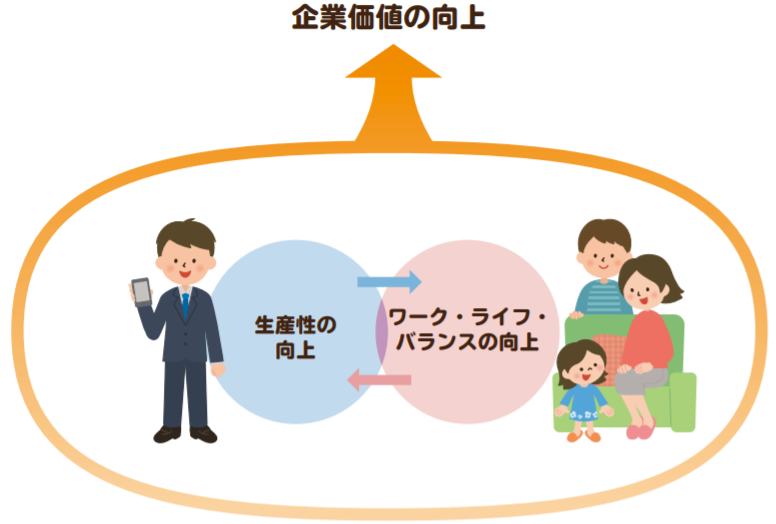
セキュリティの強化は、「情報資産」の保護のために重要かつ、盗難・紛失以外にもオンラインから情報の抜き取り等の危険性がある現代において不可欠なものです。

しかし、セキュリティを強化すればするほどICT環境が複雑になるため、従業員に求める認証作業やICT環境構築を担う情報システム担当者の作業が増えてしまいます。

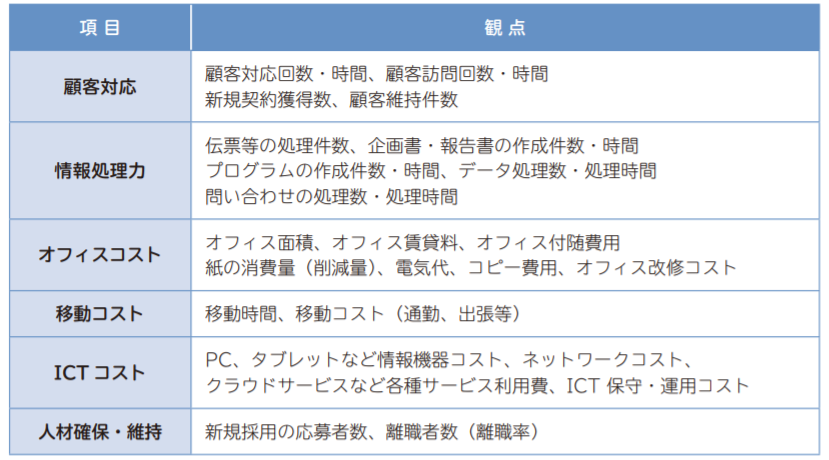
その結果、作業の煩雑さから業務効率が低下する問題が発生し、従業員のテレワーク利用が普及しにくくなるおそれもあります。

企業ごとの業務や風土によって適度なバランスを模索することが必要です。

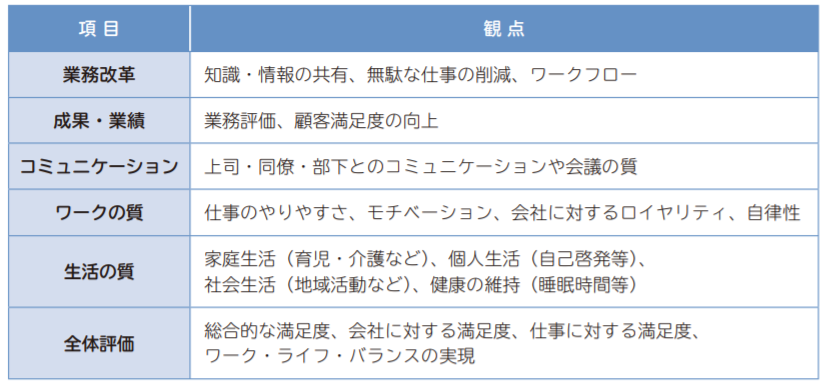
* + - 1. 3.物理的なセキュリティ対策
         1. ルールによるセキュリティ対策と技術的なセキュリティ対策では不十分な場合があります。例えば、盗難やスパイ活動、破壊等の損害など、PCやサーバという実体あるもの（ハードウェア）が危機にさらされる場合です。
         2. そこで「物理的なセキュリティ対策」が必要となってきます。具体的には監視カメラや入退出管理といった盗難防止策や、施錠棚やシュレッダーによる情報漏えいの防止策などが挙げられます。
         3. 物理的なセキュリティはテレワークの導入と同時に厳密に見直す、ということはほとんどありません。しかし、基本的に情報や情報に関する設備のある場所について、例えば「サーバや書類ラックは常に施錠されているか」「入退室の記録が適切な期間保管されているのか」といった確認が重要です。
         4. テレワークでは所属オフィス以外の場所が「オフィス」になります。そのため、新しく執務環境とみなす場所については、オフィス同様の物理的セキュリティ対策をする必要があります。例えば、在宅勤務時には「自宅に会社貸与のPCを施錠管理できる棚があるか」「執務中の家の立ち入りは不特定多数ではないか」などの確認は必要です。これらの確認には、テレワーク利用申請等の申請書類に執務環境を明記させたり、誓約書等を交わすことで十分な注意を約束するように指導するなどの対応が有効です。
         5. また、ペーパーレス化を進めることは、セキュリティ対策にもつながります。資料を全て電子化しておくことで、紙資料をオフィス外に持ち出す必要がなくなるので紛失や盗難が防げるほか、社内での情報整理が簡単になるので、情報の管理がしやすくなります。
    1. 第7章　テレワーク推進のための評価と改善
       1. 1.評価の仕方
          1. 図表Ⅱ-7-1　生産性の向上とワーク・ライフ・バランスの向上による企業価値の向上



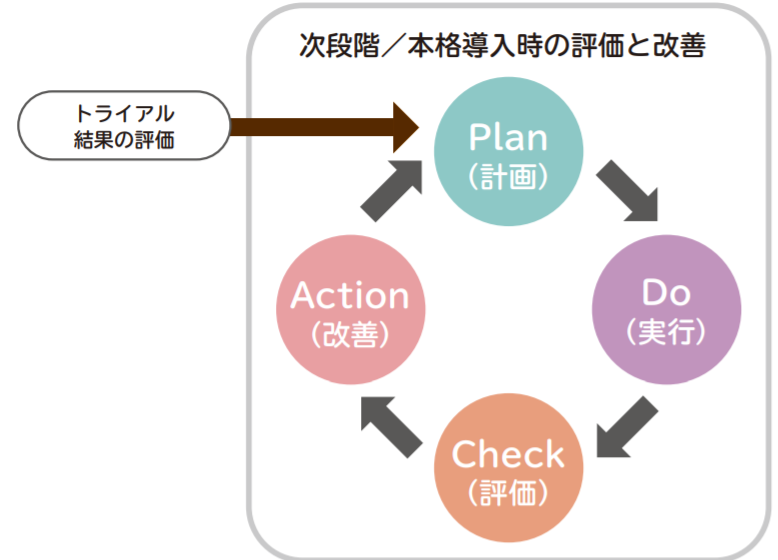
* + - * 1. 図表Ⅱ-7-2　量的評価（例）



* + - * 1. 図表Ⅱ-7-3　質的評価（例）



* + - 1. 2.改善の仕方
         1. 図表Ⅱ-7-4　テレワークの評価によるPDCAサイクルの実践



* + 1. テレワークの活用でよくあるQ&A
       1. 育児や介護など、さまざまなライフイベントに対応したテレワーク
       2. 事業継続性（BCP）の確保
          1. BCP対策として、テレワークが活用できますか？

何十年に一回の大災害に備えるというよりも、台風や大雪など、年に何回か発生する自然災害や、インフルエンザなどが流行した際に、在宅で仕事ができるテレワークは有効といえるでしょう。

* + - 1. 業務特性に応じたテレワーク
      2. マネジメント
      3. セキュリティ
         1. テレワークの場合、社外でのセキュリティは大丈夫ですか？

ルールによるセキュリティ対策に加え、物理的・技術的の側面から総合的にセキュリティ対策を行うことで、より安全にテレワークを実施することができます。

例えば、ルールによる対策には、「公衆回線は利用しない」、

物理的な対策には「貸与したPCは鍵付きの保管場所を用意する」、「第三者からののぞき見を防止する画面フィルタを利用する」、

技術的な対策には「ウイルスの検知・駆除ソフトを利用する」などが挙げられます（詳しくはP.80 ～ 88をご参照ください）。

* + - 1. 遠隔地におけるテレワーク
    1. テレワークお役立ちリンク集
       1. 厚生労働省ホームページ
          1. http://www.mhlw.go.jp/

ドキュメントを参照: [www.mhlw.go.jp](http://www.mhlw.go.jp/)

* + - * 1. ※ホームページ内で「テレワーク普及」と検索。以下の順番に選択しても、ご参照いただけます
      1. テレワーク相談センター
         1. http://www.tw-sodan.jp/

ドキュメントを参照: [www.tw-sodan.jp](http://www.tw-sodan.jp/)

* + - * 1. テレワークの導入や実施時における労務管理上の課題などについて、個別企業からの相談に対応する「テレワーク相談センター」を設置しています。
      1. 情報通信機器を活用した在宅勤務の適切な導入及び実施のためのガイドライン（在宅勤務ガイドライン）
         1. http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou\_roudou/roudoukijun/shigoto/ guideline.html

ドキュメントを参照:  [guideline.html](http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/shigoto/%20guideline.html)

* + - * 1. 在宅勤務に関する労働基準関係法令の適用及びその注意点などについて解説しています。
      1. テレワークセキュリティガイドライン（第４版）

参照: [●テレワークセキュリティガイドライン第４版【総務省】](#a_テレワ_クセキュリティガイドライン第_版_総務省_)

* + - * 1. http://www.soumu.go.jp/main\_content/000545372.pdf

ドキュメントを参照: <http://www.soumu.go.jp/main_content/000545372.pdf>

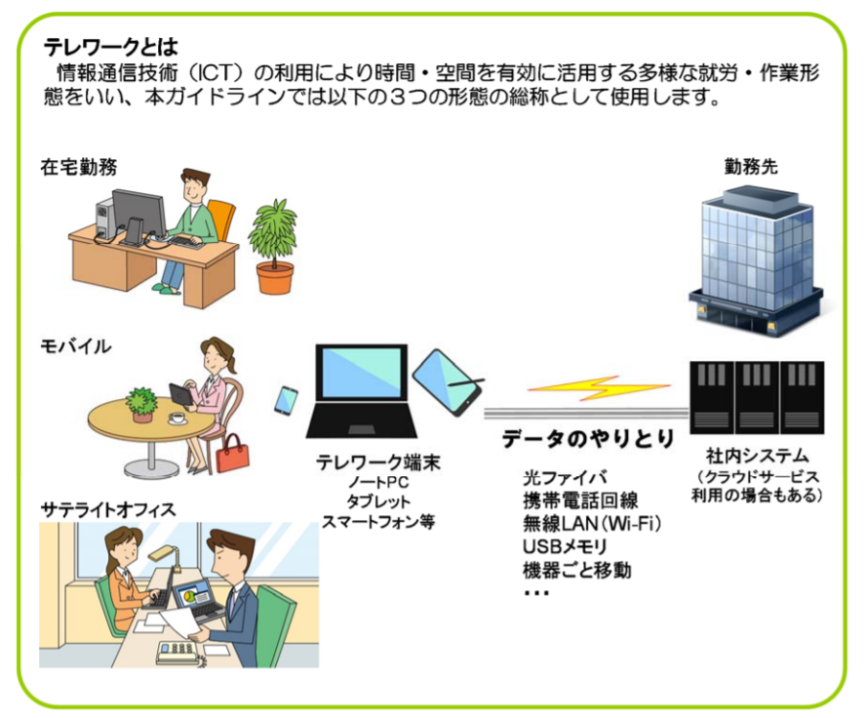
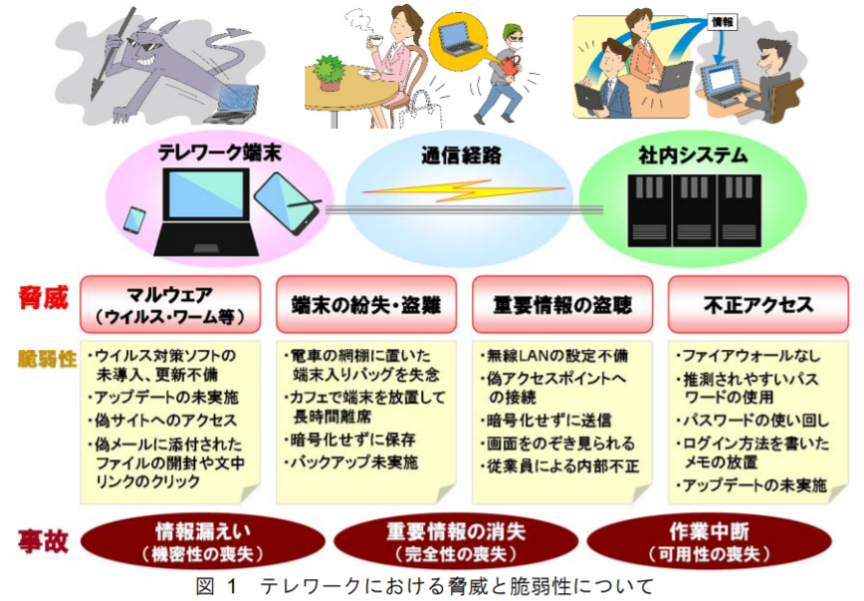
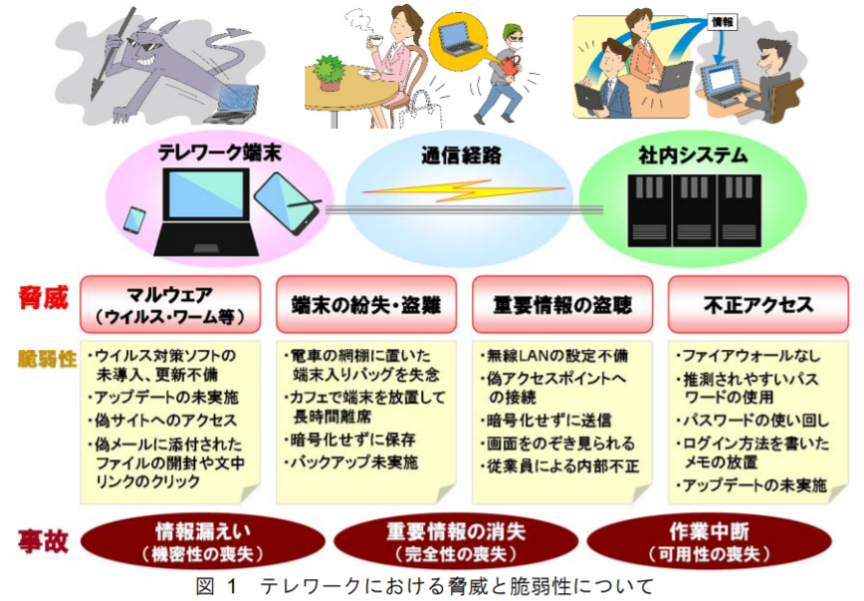
* + - * 1. テレワークにおける情報セキュリティ対策について解説しています。
      1. 職場意識改善助成金（テレワークコース）
         1. http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou\_roudou/roudoukijun/jikan/syokubaisikitelework.html
         2. テレワークを新規で導入する中小企業に対する助成制度です。導入経費の1/2～3/4（上限額：150万円）を助成しています
  1. システム方式
     1. リモートデスクトップ
     2. 仮想デスクトップ
     3. クラウド型アプリ
     4. 会社ＰＣ持ち帰り
  2. 端末デバイス
     1. リッチクライアント
     2. シンクライアント
     3. タブレット型PC
     4. スマートフォン
     5. 携帯電話
  3. セキュリティ
     1. 本人認証
     2. 端末認証
     3. 端末管理
     4. 暗号化通信
     5. ストレージ暗号化

1. ●テレワークセキュリティガイドライン第４版【総務省】

ドキュメントを参照: [000545372.pdf](https://www.soumu.go.jp/main_content/000545372.pdf)

* 1. 全体目次
     1. はじめに
     2. 1. テレワークにおける情報セキュリティ対策の考え方
        1. （ア） 「ルール」「人」「技術」のバランスがとれた対策の実施
        2. （イ） テレワークの方法に応じた対策の考え方
        3. （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
     3. 2. テレワークセキュリティ対策のポイント
        1. （ア） 経営者が実施すべき対策
        2. （イ） システム管理者が実施すべき対策
        3. （ウ） テレワーク勤務者が実施すべき対策
     4. 3. テレワークセキュリティ対策の解説
        1. （ア） 情報セキュリティ保全対策の大枠
        2. （イ） マルウェアに対する対策
        3. （ウ） 端末の紛失・盗難に対する対策
        4. （エ） 重要情報の盗聴に対する対策
        5. （オ） 不正アクセスに対する対策
        6. （カ） 外部サービスの利用に対する対策
     5. 用語集
     6. 参考リンク集
  2. 用途別目次
     1. ＜テレワーク勤務者が参照すべき項目の一覧＞
        1. １．テレワークにおける情報セキュリティ対策の考え方
        2. ２．テレワークセキュリティ対策のポイント
           1. （ウ）テレワーク勤務者が実施すべき対策
        3. ３．テレワークセキュリティ対策の解説
           1. （ア）セキュリティ保全体制の大枠
           2. （イ）マルウェアに対する対策
           3. （ウ）端末の紛失・盗難に対する対策
           4. （エ）重要情報の盗聴に対する対策

（カフェなどモバイル環境でテレワークを行う人が対象）

* + - * 1. （オ）不正アクセスに対する対策
        2. （カ）外部サービスの利用に対する対策
    1. ＜テレワークトラブル事例と対策一覧＞
       1. 1.情報のレベル分けに関するトラブル事例
       2. 2.マルウェア感染に関するトラブル事例
       3. 3.ウイルス対策ソフトに関するトラブル事例
       4. 4.アプリケーション利用に関するトラブル事例
       5. 5.アップデートに関するトラブル事例
       6. 6.ランサムウェアに関するトラブル事例
       7. 7.不審メールに関するトラブル事例
       8. 8.端末の紛失に関するトラブル事例
       9. 9.公衆無線LAN利用に関するトラブル事例
       10. 10.画面の覗き見に関するトラブル事例
       11. 11.「踏み台」に関するトラブル事例
       12. 12.パスワード管理に関するトラブル事例
       13. 13.SNS利用に関するトラブル事例
       14. 14.パブリッククラウド利用に関するトラブル事例
  1. はじめに
     1. テレワークとは？
        1. 在宅勤務
        2. モバイル
        3. サテライトオフィス
        4. 
  2. 1.テレワークにおける情報セキュリティ対策の考え方
     1. （ア）「ルール」「人」「技術」のバランスがとれた対策の実施
        1. 図1テレワークにおける脅威と脆弱性について
           1. 
        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
           1. 
        3. 【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
           1. 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。
           2. 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。

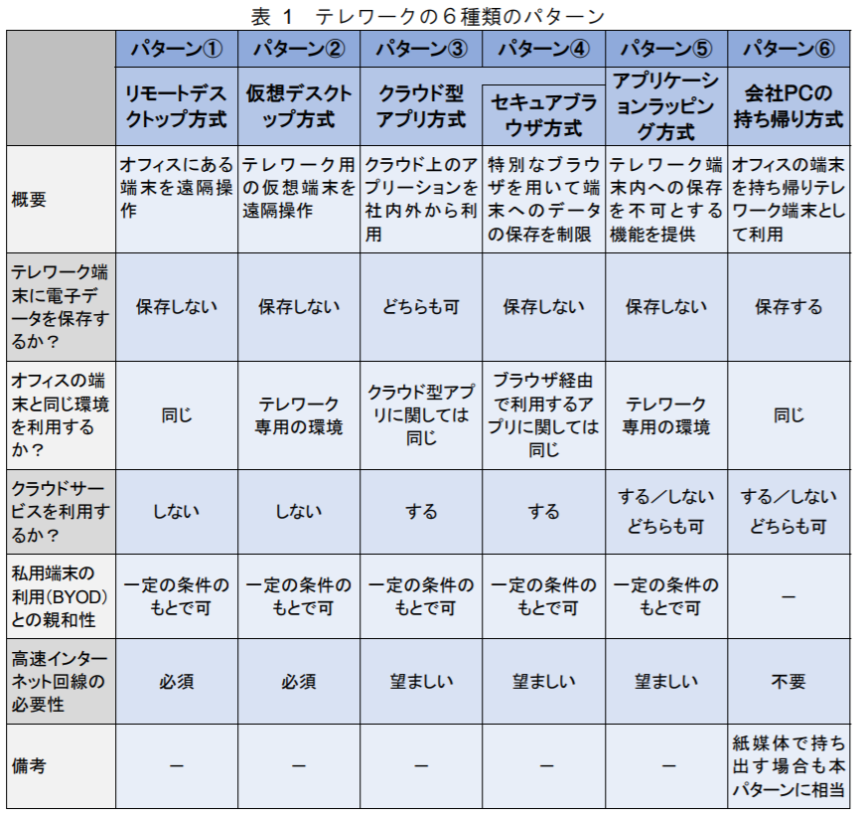
「情報セキュリティ 5 か条」の実践･･･★一つ星

「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

* + - * 1. 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。

* + - 1. 「ルール」・「人」・「技術」とは
         1. （「ルール」について）
         2. （「人」について）
         3. （「技術」について）
    1. （イ） テレワークの方法に応じた対策の考え方
       1. 表1 テレワークの６種類のパターン
          1. 
          2. リモートデスクトップ方式
          3. 仮想デスクトップ方式
          4. クラウド型アプリ方式
          5. セキュアブラウザ方式
          6. アプリケーションラッピング方式
          7. 会社ＰＣの持ち帰り方式
       2. 図3 リモートデスクトップ方式
       3. 図4 仮想デスクトップ方式
       4. 図5 クラウド型アプリ方式
       5. 図6 セキュアブラウザ方式
       6. 図7 アプリケーションラッピング方式
       7. 図8 会社PC の持ち帰り方式
       8. （自社にふさわしいテレワークの方式の検討）
       9. （クラウドサービスの利用について）
       10. 図9 クラウドサービスへの移行
    2. （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
       1. ＜システム管理者＞
       2. ＜テレワーク勤務者＞
  1. 2.テレワークセキュリティ対策のポイント
     1. （ア） 経営者が実施すべき対策
        1. （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。
           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。
           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。
           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。
           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。
     2. （イ）システム管理者が実施すべき対策
        1. （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。
           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。
           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。
           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。
        2. （悪意のソフトウェアに対する対策）
           1. 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。
           2. 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。
           3. 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。
           4. 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。
           5. 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。
           6. 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。
           7. 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。
        3. （端末の紛失・盗難に対する対策）
           1. 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。
        4. （重要情報の盗聴に対する対策）
           1. 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。
        5. （不正侵入・踏み台に対する対策）
           1. 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。
           2. 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。
           3. 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。
        6. （外部サービスの利用に対する対策）
           1. 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。
           2. 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。
     3. （ウ）テレワーク勤務者が実施すべき対策
        1. （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。
           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。
           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。
           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。
        2. （悪意のソフトウェアに対する対策）
           1. 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。
           2. 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。
           3. （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。
           4. 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。
           5. 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。
           6. 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。
           7. 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。
        3. （端末の紛失・盗難に対する対策）
           1. 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。
           2. 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。
        4. （重要情報の盗聴に対する対策）
           1. 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。
           2. 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。
           3. 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。
        5. （不正侵入・踏み台に対する対策）
           1. 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。
           2. 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。
           3. 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。
        6. （外部サービスの利用に対する対策）
           1. 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。
           2. 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。
  2. 3.テレワークセキュリティ対策の解説
     1. （ア）情報セキュリティ保全対策の大枠
        1. １
           1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. ＜経営者＞基本対策事項
        2. 図10情報セキュリティポリシーの構成
        3. ＜経営者＞推奨対策事項
        4. 図11情報セキュリティに関するＰＤＣＡサイクル
      1. ２
         1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. ＜経営者・システム管理者＞基本対策事項
        2. ＜経営者・システム管理者＞推奨対策事項
        3. 図 12 情報のレベル分け
        4. 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～
        5. 【コラム】紙媒体での情報の持ち出し
      1. ３
         1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. ＜経営者・システム管理者＞基本対策事項
        2. ＜テレワーク勤務者＞基本対策事項
        3. 図13 情報セキュリティ教育
        4. 図14イントラネットやポスターによる啓発
        5. ＜経営者・システム管理者＞推奨対策事項
      1. ４
         1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. ＜経営者・システム管理者・テレワーク勤務者＞基本対策事項
        2. ＜経営者・システム管理者・テレワーク勤務者＞推奨対策事項
      1. ５
         1. 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。

* + - * 1. ＜経営者＞基本対策事項
    1. （イ） マルウェアに対する対策
       1. ５
          1. 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。

* + - * 1. 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。

* + - * 1. ＜テレワーク勤務者＞基本対策事項
        2. ＜システム管理者＞推奨対策事項
        3. 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～
      1. ６
         1. 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。

* + - * 1. 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。

* + - * 1. ＜システム管理者＞推奨対策事項
        2. ＜テレワーク勤務者＞推奨対策事項
        3. 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～
      1. ７
         1. 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。

* + - * 1. 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。

* + - * 1. ＜システム管理者＞基本対策事項
        2. ＜テレワーク勤務者＞基本対策事項
        3. 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～
        4. 【コラム】次世代ウイルス対策ソフト
      1. ８
         1. 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。

* + - * 1. 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。

* + - * 1. ＜システム管理者＞基本対策事項
        2. ＜テレワーク勤務者＞基本対策事項
        3. 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～
      1. ９
         1. 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。

* + - * 1. 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。

* + - * 1. ＜システム管理者＞推奨対策事項
        2. ＜テレワーク勤務者＞推奨対策事項
      1. 10
         1. 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。

* + - * 1. ＜システム管理者＞推奨対策事項
        2. 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～
      1. 11
         1. 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。

* + - * 1. 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。

* + - * 1. ＜テレワーク勤務者＞基本対策事項
        2. ＜システム管理者＞推奨対策事項
        3. ＜テレワーク勤務者＞推奨対策事項
        4. 【コラム】 社内SNS の利用
        5. 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～
    1. （ウ） 端末の紛失・盗難に対する対策
       1. 11
          1. 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）

* + - * 1. ＜テレワーク勤務者＞推奨対策事項
      1. 12
         1. 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。

* + - * 1. 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。

* + - * 1. ＜システム管理者＞推奨対策事項
        2. ＜テレワーク勤務者＞推奨対策事項
        3. 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～
    1. （エ） 重要情報の盗聴に対する対策
       1. 13
          1. 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。

* + - * 1. ＜テレワーク勤務者＞基本対策事項
        2. 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～
      1. 13
         1. 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。

* + - * 1. 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。

* + - * 1. ＜テレワーク勤務者＞基本対策事項
        2. ＜テレワーク勤務者＞推奨対策事項
        3. 図16 無線LAN 利用上のリスク
      1. 15
         1. 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。

* + - * 1. ＜テレワーク勤務者＞推奨対策事項
        2. 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～
    1. （オ） 不正アクセスに対する対策
       1. 16
          1. 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。

* + - * 1. 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。

* + - * 1. 【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）
        2. ＜システム管理者＞基本対策事項
        3. ＜テレワーク勤務者＞推奨対策事項
      1. 17
         1. 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。

* + - * 1. 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。

* + - * 1. ＜システム管理者＞基本対策事項

図17 ファイアウォールの設置

* + - * 1. ＜システム管理者＞推奨対策事項
        2. ＜テレワーク勤務者＞推奨対策事項
        3. 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～
      1. 18
         1. 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。

* + - * 1. 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。

* + - * 1. ＜システム管理者＞基本対策事項
        2. ＜システム管理者＞推奨対策事項
        3. ＜テレワーク勤務者＞推奨対策事項

図 18 アカウントのパスワード管理

* + - * 1. 【コラム】 パスワードの管理方法
        2. 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～
        3. 【コラム】ID・パスワードをブラウザに記憶させても大丈夫？
    1. （カ）外部サービスの利用に対する対策
       1. 19
          1. 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。

* + - * 1. 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。

* + - * 1. ＜システム管理者・テレワーク勤務者＞推奨対策事項
        2. 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～
      1. 20
         1. 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。

* + - * 1. 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。

* + - * 1. ＜システム管理者＞基本対策事項
        2. ＜テレワーク勤務者＞推奨対策事項
        3. 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～
  1. 用語集
  2. 参考リンク集
     1. 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）

参照: [●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】](#a_テレワ_クではじめる働き方改革_テレワ_クの導入_運用ガイドブック__厚生労働省_)

* + - 1. http://work-holiday.mhlw.go.jp/material/pdf/category7/01\_01.pdf
      2. 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。
    1. サイバーセキュリティ経営ガイドライン（経済産業省）
       1. http://www.meti.go.jp/policy/netsecurity/mng\_guide.html

ドキュメントを参照: [mng\_guide.html](http://www.meti.go.jp/policy/netsecurity/mng_guide.html)

* + - 1. 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。
    1. 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）
       1. https://www.ipa.go.jp/security/keihatsu/sme/guideline/

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - 1. 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。
    1. SECURITY ACTION （独立行政法人情報処理推進機構）
       1. https://www.ipa.go.jp/security/security-action/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/security-action/index.html)

* + - 1. 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、「SECURITYACTION」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。
    1. 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）
       1. http://slb.jnsa.org/eslb/

ドキュメントを参照: [eslb](http://slb.jnsa.org/eslb/)

* + - 1. 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。
      2. 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。
    1. 経営と IT 化相談窓口（NPO IT コーディネータ協会）
       1. https://www.itc.or.jp/management/diagnosis/

ドキュメントを参照: [diagnosis](https://www.itc.or.jp/management/diagnosis/)

* + - 1. 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。
    1. 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）
       1. https://www.ipa.go.jp/siensi/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/siensi/index.html)

* + - 1. 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。

1. 働き方改革を実現するために有用なITツールの種類と活用事例

ドキュメントを参照: [働き方改革を実現するために有用なITツールの種類と活用事例｜テレワークナビ](https://www.nice2meet.us/the-best-tools-to-implement-work-style-reform-law)

* 1. はじめに
     1. 働き方改革とは
     2. 働き方改革の推進にはIT（ICT）ツールが欠かせない
  2. 1．残業は減少する一方、サービス残業が増える
  3. 2．ジタハラ（時短ハラスメント）
  4. 3．人手不足の解消と生産性向上の課題を克服できない
     1. ITツールの種類にはどのようなものがある？
  5. Web会議システム
     1. サービス名：V-CUBE ミーティング
     2. サービス名：Zoom ミーティング
        1. 価格：無料版と有料版があります。
           1. プロ（小規模チーム向け）：$14.99/月/ホスト
           2. ビジネス（中小企業向け）：$19.99/月/ホスト
           3. 企業（大企業向け）：$19.99/月/ホスト
        2. 特長：
           1. 招待メールをクリックするだけで手軽にWeb会議参加
           2. 同時接続可能拠点数100～1000
           3. ガートナー社より2018 MagicQuadrant会議ソリューション部門レポートでLeader'sQuadrantの評価。2019年に米国NASDAQ上場
        3. 実績：
           1. DropBox、box、Slackなどの大手企業ほか世界75万社以上が導入
        4. 提供元：
           1. Zoom Video Communications, Inc
     3. Skype　 https://www.skype.com/ja/
     4. Google ハングアウト　 https://hangouts.google.com/?hl=ja
  6. ビジネスチャット
     1. Chatwork　 https://go.chatwork.com/ja/
     2. Slack　 https://slack.com/intl/ja-jp/
     3. LINE WORKS　 https://line.worksmobile.com/jp/
     4. Microsoft Teams　 https://products.office.com/ja-jp/microsoft-teams/group-chat-software
  7. オンラインストレージ
     1. Dropbox 　https://www.dropbox.com/ja/
     2. Box　 https://www.box.com/ja-jp/home
     3. Google Drive　 https://www.google.com/intl/ja\_ALL/drive/
     4. Microsoft OneDrive　 https://onedrive.live.com/about/ja-jp/
  8. バーチャルオフィス
     1. Sococo　 https://www.telework-management.co.jp/services/tool/sococo/
     2. Remotty　 https://www.remotty.net/
  9. 勤怠管理システム
     1. ジョブカン勤怠管理　 https://jobcan.ne.jp/
     2. jinjer勤怠　 https://hcm-jinjer.com/
     3. e-就業ASP　 https://www.nds-tyo.co.jp/e-asp/
  10. ERP（Enterprise Resources Planning）
      1. SAP　 https://www.sap.com/japan/index.html
      2. クラウドERP　freee　 https://www.freee.co.jp/cloud-erp/
      3. ORACLE NET SUITE　 http://www.netsuite.co.jp/
  11. まとめ：課題に応じた適切なITツールの選択が重要

1. ゼロから学べるテレワーク導入完全ガイド【V-CUBE】
   1. 第1章テレワークの基礎を学ぼう
      1. 01.そもそもテレワークって何？
      2. 02.テレワークの普及の現状とは？
      3. 03．テレワークが企業にもたらすメリットは？
   2. 第2章テレワークを自社に導入しよう
      1. 01．テレワーク推進チームを作る
      2. 02．導入目的を明確にする
      3. 03．対象範囲と実施業務・期間を設定する
      4. 04．人事・労務環境を整備する
      5. 05．テレワーク実施計画とセキュリティルールを作成する
      6. 06.ICTツールを導入する
      7. 07．研修・セミナーを開催する
      8. 08．トライアル期間を開始する
      9. 09．テレワークの評価・改善をする
      10. 10．本格的なテレワークの運用を開始する
2. モバイルセキュリティ関連
   1. ●MDM導入・運用検討ガイド【経済産業省】

ドキュメントを参照: [MDMGuideV1.pdf](https://www.jssec.org/dl/MDMGuideV1.pdf)

* 1. ●情報セキュリティ対策の基本 スマートフォン編 - IPA【IPA】

ドキュメントを参照: [000059213.pdf](https://www.ipa.go.jp/files/000059213.pdf)

* 1. ●スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン【経済産業省】

ドキュメントを参照: [seccontents\_000142.html](https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000142.html)

* 1. ●私物端末の業務利用におけるセキュリティ要件の考え方【内閣官房】

ドキュメントを参照: [byod.pdf](https://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/byod.pdf)

* 1. ●導入事例　大分県庁　【Soliton】

ドキュメントを参照: [pref-oita.html](https://www.soliton.co.jp/case_study/pref-oita.html)

* 1. NISTガイドライン
     1. Mobile Device Security: Cloud and Hybrid Builds
        1. Executive Summary

ドキュメントを参照: [mds-nist-sp1800-4a-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4a-draft.pdf)

* + - 1. Approach, Architecture, and Security Characteristics

ドキュメントを参照: [mds-nist-sp1800-4b-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4b-draft.pdf)

* + - 1. How-To Guide

ドキュメントを参照: [mds-nist-sp1800-4c-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4c-draft.pdf)