テレワーク セキュリティ ルールブック

株式会社エスケイワード
コンサルティング事業部

2020.05.26 公開

はじめに

テレワーク　利用者のルールについて

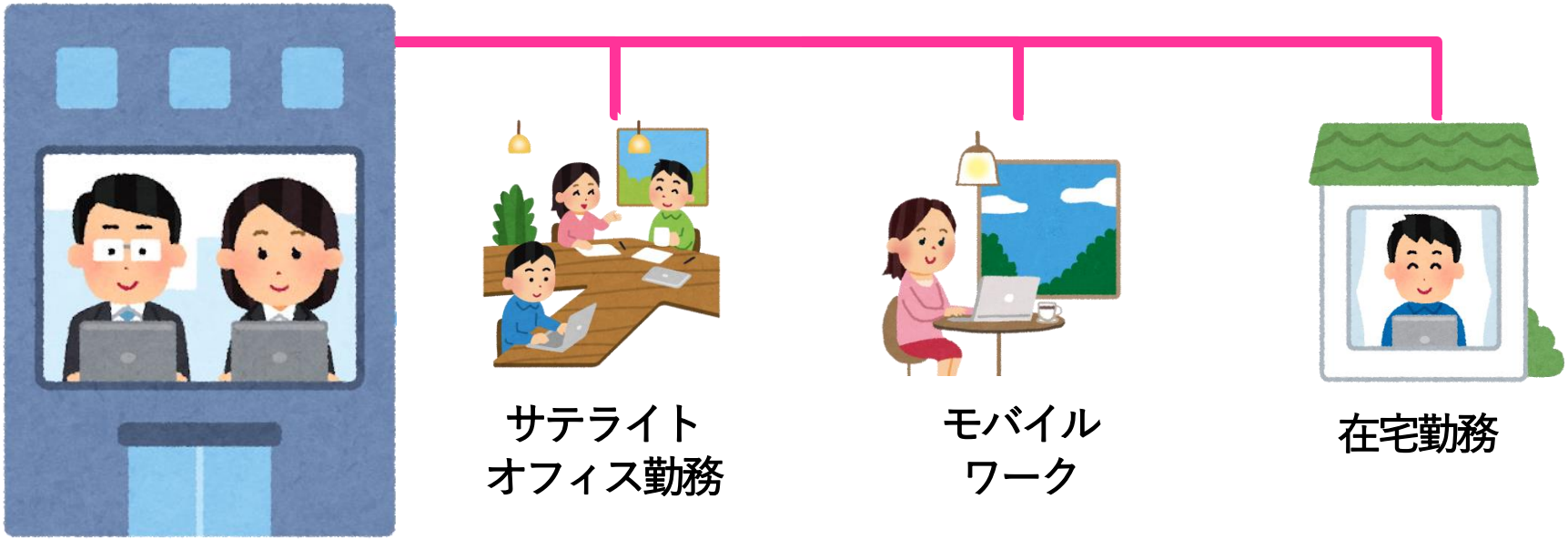
テレワーク勤務の方は、会社・組織が定めたルールをよく理解し、それに従ってください。
本ルールブックは、**テレワーク利用者**に向けたセキュリティ上の注意事項をご案内します。

目次

テレワークとは？

テレワークとは「会社以外で仕事をすること」です。

- 勤務先以外のオフィススペースで仕事をする「サテライトオフィス勤務」
- 客先や喫茶店等移動先で仕事をする「モバイルワーク」
- そして、家で仕事をする「在宅勤務」



※私物の専用PC・家族との共用PC・会社のPCを使用する場合でリスクが異なります

1. コンピューターウイルス対策

日々、多くのコンピューターウイルスが誕生しています。
コンピューターウイルス感染のリスクを減らすための重要な対策です。

- ウイルス対策ソフトの導入と定義ファイルの更新
- OS（オペレーティングシステム）は常に、最新の状態を保つ
  （Windowsアップデート、又はMicrosoftアップデート）
- 見知らぬ相手から届いた不審なメールの添付ファイルは開かずに削除する
- 知り合いから届いたメールの場合でも、不審な添付ファイルが添付されている場合には、送信元に問い合わせる
- スパムメールなどに記載されたリンクは開かない（URLはクリックしない）
- 作業前に、ウイルス対策ソフトが最新の状態になっているか確認する

2. 盗難・紛失対策

機密情報の入ったPCや端末を盗難・紛失すると
情報漏洩となります。

<u>持ち運び途中での盗難・紛失に注意する</u>

- ◘ 無人の車中に放置しない
- ◘ 飲食店等の公衆の場所で、端末や媒体（紙含む）を置きっぱなしにしない

3. パスワード対策

使いまわされたパスワードは「マスターキー」のようなもの。
一つ流出すれば他のログインに使われることも。

- パスワードの使い回し禁止
- パスワードは業務用と私用（プライベート）を必ず分ける
- ツールごとにパスワードを分ける
- 覚えやすくわかりにくいパスワードにする

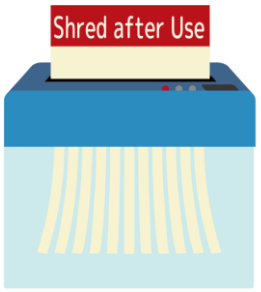
  ※例えばコアのパスワードとクラウドサービスの頭文字2文字を組み合わせるやり方などがある
- パスワードが記載してある紙やメモ等を、第三者が容易に閲覧できる状態にしない

4. 書類の管理

原本、コピー、プリントした書類はどうしていますか？
自宅でも紙の廃棄ルールは社内と同じにすること。

<u>廃棄不備による漏えい(原本・コピー・プリントアウト)</u>

- ◘ 機密性の高いものや、個人情報の記載されたものは全てシュレッダー処理とする
- ◘ パスワードなど機密性の高い情報をそのまま廃棄しない
- ◘ 同居の方にも見られないようにしておく
- ◘ 自宅でも紙の廃棄ルールは社内と同じにする



5. ネットワーク＆無線LAN

Wi-fiの接続設定を制限しましょう。

外部での無線LAN使用について

- 無線LAN使用時は、リスクを理解して無料の無線LAN（フリーWIFI）等に接続しない
- HTTPSのサイトを利用する
- 接続先は、毎回確認する

自宅作業でのネットワーク環境（無線LAN含む）設定について

- 原則有線ネットワークケーブルで接続する。
- 無線LAN機器設定時は以下を考慮する。

① WPA2以上による暗号化形式の機器を選ぶ（通信しているデータを読み取らせない）
※新規購入時は　WPA３やWIFI6対応の機種を選ぶようにすること。

② ANY拒否・ESS-IDステルス（親機の名前を他人に見られないようにする）
SSIDステルス （無線LANアクセスポイントが自分のSSID（ESSID）を教えなくなる機能）
ANY接続拒否 （接続先が空欄もしくは「Any」になっている接続を拒否する機能）

③ MACアドレス・フィルタリング（親機を不正に使わせない）
Wi-Fiルーターに特定の機器のみを接続させることを目的とした機能

6. データ対策

データを失うリスクを意識しましょう。

社外に持ち出す端末は、紛失時にデータを失うリスクがある

- バックアップ先にデータを保管する
- 外部移動時・端末紛失等によりデータの流出を防ぐ為、原則機密性の高い情報を端末に保存しない
- 成果物を会社に提出後、業務で得た素材やデータは自宅PCから削除する

7. クリアデスク・クリアスクリーン

自宅で作業する際にも
2S（整理・整頓）の徹底を心掛けましょう。

クリアスクリーン

- 端末はロック付のスクリーンセーバーを必ず設定する
- 在宅勤務特でも、離席する場合には、以下のいずれかの処置を徹底する
  - （ａ）ログオフ
  - （ｂ）時間制限付きパスワード付きスクリーンセーバーの設定

クリアデスク（在宅業務をする場合の整理・整頓のルール）

- 業務終了時には卓上には、不要な書類等は置かない
- 機密性の高い物に関しては、定められた場所に置く（鍵付きの引き出し等）

8. 社外使用時の注意

周囲からの盗み見・盗み聞き対策として、
業務上知り得た情報は許可なく公言しない（見せない）こと。

- 社外（飲食店や打ち合わせ場所等）で作業をする場合は、
  盗難や、他者、のぞき見などに十分に注意を払う
- 自宅で作業を実施している場合でも、離席する場合にはPCにロックをかける
- 業務上知り得た情報は、社外では口外は禁止
  （※業務上知り得た情報を部外者（友人・知人等）に口外したり、業務以外の目的で使用しないこと。特に喫煙所・飲食店・乗り物の中・廊下・エレベーター等での「なにげない会話」に注意すること。就業時間終了後も同様に注意すること。自宅でも機密情報は話さないこと）
- 外部でクライアント名・個人名は伏字にして話す
  （※また、同業者、ライバル会社等の情報を話さない、また見えないように注意すること）

9. 端末廃棄時の注意

データはゴミ箱で削除しただけでは
完全に削除できません。

<u>データ完全廃棄について</u>

- 端末廃棄時は必ずデータ消去ソフトを使用する
- データはゴミ箱に削除では完全に削除できないため、機密性の高い情報は完全消去ソフト等を使用してデータ削除する

10. 緊急時、有事の際の対応

報告先と対応のルールを守りましょう。

環境変更時とサービス変更時の対応

- ◘ 緊急時の連絡先と対応のルールを学ぶ
  （メールの誤送信・データの誤削除・ウイルスに感染・PCを壊した・インターネットにつながらない・PCを紛失した…など。ネット環境がない場合の連絡先も確保すること）
- ◘ 社外のネットワークサービスを利用する場合には、契約書、利用規約等に記載された情報セキュリティ面での状況を確認し、管理者に相談する
- ◘ 自分の作業環境に変更があった場合は、管理者に報告をする
- ◘ 情報セキュリティの事故発生時は、速やかに会社へ連絡をする
- ◘ 端末からのアラート通知があった場合には、その内容を確認し、報告する

紛失時について

- ◘ 社外受信端末を紛失、もしくは漏洩等の事故があった場合は速やかに管理者へ報告する

テレワークセキュリティ構築の6ステップ

STEP 01 テレワーク基本方針の作成

STEP 02 リスク分析・対策検討支援①
情報セキュリティルールブック作成支援

STEP 03 リスク分析・対策検討支援②
情報システム管理規程作成支援

STEP 04 テレワークユーザー様への教育

STEP 05 運用点検レクチャー
運用方法レクチャー

STEP 06 運用開始

テレワークセキュリティを始めるには？

まずはこの基本方針の作成から始めましょう。

テレワーク・情報セキュリティ対策支援

株式会社エスケイワードでは、「テレワークセキュリティ対策支援」や「情報セキュリティ対策支援」を行っています。ご依頼・お問い合わせはこちらへ（https://www.sk-con.jp/）

テレワークセキュリティ構築支援

現場のニーズに合わせて、テレワーク・セキュリティの体制構築を実施致します。プライバシーマークやISO27001（ISMS）構築実績のある専門のコンサルタントが御社の業務内容をヒアリングし、テレワーク運用に伴い、ご担当者様と一緒セキュリティルールを作り上げます。コースは現状調査からルール策定、教育、運用監査を実施する事により、実用的なルール策定が可能です。

構築期間：標準4～5ヶ月
訪問回数：4～6回
費用　　：400,000円～

テレワークセキュリティ現状チェックサービス

現在すでに、テレワークを導入しているが、セキュリティ対策はどこから手を付ければよいか、難しい所です。その場合は、まずはこちらのテレワークセキュリティ診断を実施してください。情報セキュリティの「ISO27001」の規格を元に、コンサルタントがセキュリティ診断をいたします。

構築期間：標準1～5ヶ月
オンラインコンサルティング：2回
費用　　：150,000円～

スポット支援

「今のところ順調に自社運営が出来ている様子だが、困った時の相談先がいなくて、問題を解決できそうもない。」
「一度専任のコンサルタントに相談に乗って欲しい。」
担当コンサルタントが御社に訪問し、課題の解決をサポートいたします。

訪問回数：1回
費用　　：50,000円～（※1）

※1：価格は、標準的なケースでの参考価格です。お客様の状況によって異なる場合があります。