



個人情報取扱いに関する事故を起こさないために
【テレワーク時に注意すべきこと】

2022年7月15日

JIPDEC

一般財団法人日本情報経済社会推進協会
プライバシーマーク推進センター



本資料について

- 本資料は、事業者の皆様が従業者に対して行う個人情報保護教育に利用していただくことを目的に作成した参考資料です。
- JIPDECプライバシーマーク推進センターに提出された個人情報の取扱いに関する事故報告書等から、事故の発生状況や原因、再発防止策などを整理し、まとめたものです。
- 個人情報の取扱いに関する事故を起こさないために、自社における個人情報取扱い業務の実態に合わせ、具体的な運用ルール等を追記するなど適宜変更してご利用いただき、ルール等の周知徹底に努めていただければ幸いです。



目次

■はじめに

- テレワークに係る事故事例のご紹介

■テレワーク時に注意すべきこと

- 気をつけましょう、こんなとき・こんなこと

■まとめ

- 当社のルールを確認しましょう
- 緊急事態への対応を確認しましょう

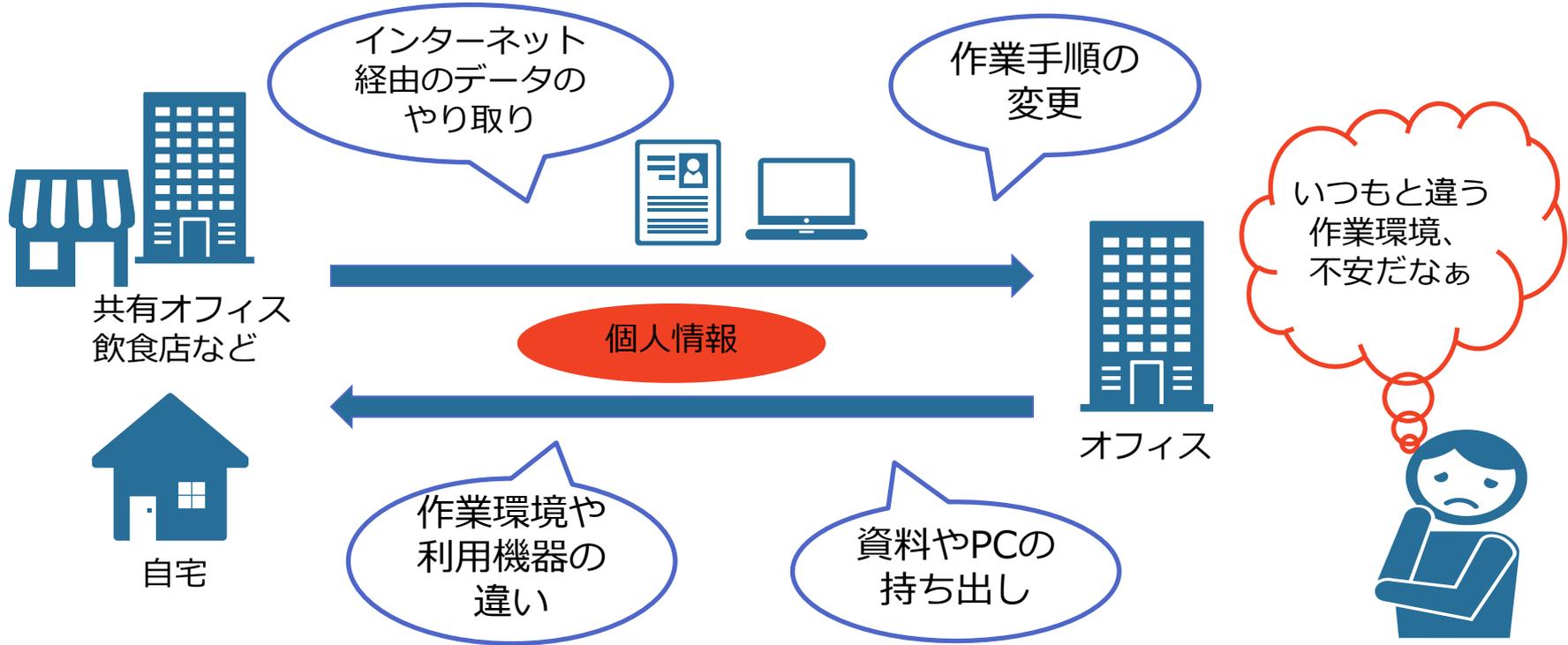
■参考情報

- 参考サイト

はじめに

テレワークを実施するにあたり

■ オフィスと異なる環境での業務

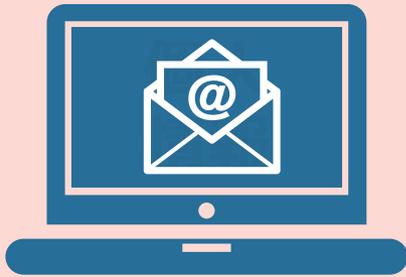


個人情報の取扱いに関する事故発生リスク（不正アクセス・メール誤送信・紛失などによる漏えい・・・）も高まります。

テレワークに係る事故事例のご紹介

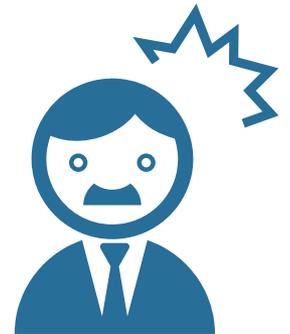
■ 自宅など、オフィス以外での業務中

▶ 不注意や管理の不手際



作業ファイルをメール添付で送付する際、普段オフィスでは2つの画面で確認していたが、自宅でノートPCの小さい画面で作業したところ、見間違えて個人情報が含まれた別のファイルを誤送信してしまった。

オフィスで使用したB社の資料を、ノートPCに保存したまま自宅で作業をしていたところ、A社とのやり取りの際に、A社専用サーバに誤ってB社の資料をアップロードしてしまった。



■ 移動中や共有スペースなどでの業務中

▶ 認識不足・意識の欠如

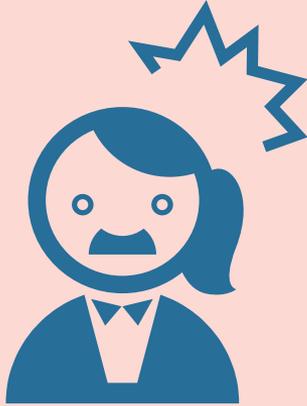


共有スペースでのWeb会議中、会話内容に含まれていた顧客情報が、周囲に漏れ聞こえてしまっていた。

ノートPCで顧客情報ファイルを開いたまま離席し、PCの画面が第三者にのぞき見されてしまった。

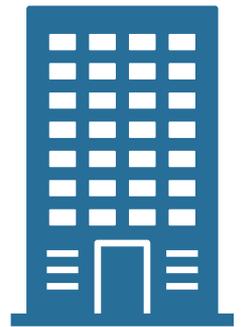
■ テレワークのためオフィスに不在の時

▶ 管理の不手際



退会手続きの書類がオフィスに届いていたが、テレワークのため確認できず、退会手続きをしていなかったため、本来送るべきではない会員向けのメールを送信してしまった。

担当者がテレワーク中に、オフィスの席に置かれた書類が、担当者に渡らず所在不明になった。



■ セキュリティ対策の不備

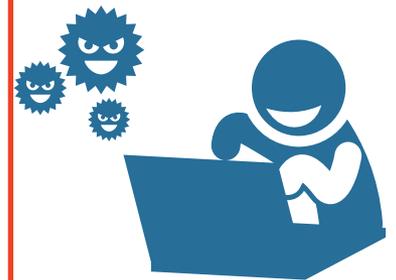
▶ 管理不備・認識不足



自宅のネットワーク環境のセキュリティ対策が不十分で、PCがウイルスに感染した。その際、PCから削除し忘れていた作業データが流出してしまった。

グループ会社の従業員がフリーメールに添付されたファイルを開封し、PC1台がマルウェアに感染した。マルウェア検知システムは導入されていたものの、メール添付されたファイルに仕込まれたマルウェアが新種であったため、マルウェア検知が遅れ、氏名やメールアドレス等を含む個人情報1万件以上が漏えいした。

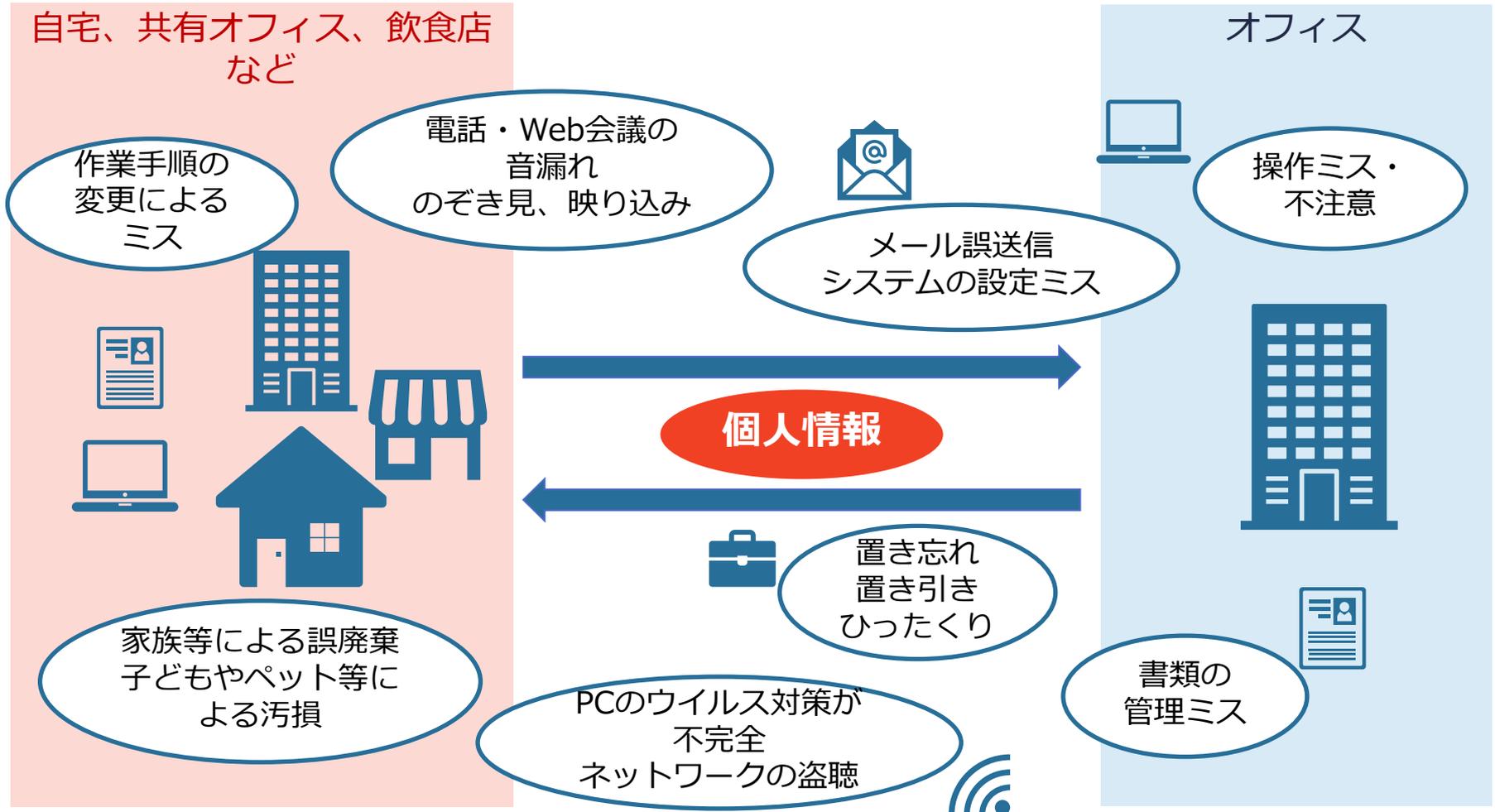
出所：総務省「テレワークセキュリティガイドライン第5版」



テレワーク時に注意すべきこと

気をつけましょう、こんなとき・こんなこと

■ 作業環境や作業手順が変わる時





テレワーク実施の留意点（1）

■ 紛失・盗難防止対策

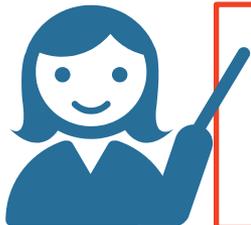
- 持ち出している・オフィスで保管している情報（資料、データ等）、端末等の把握
- 移動中、共有スペースでの作業時の持ち物（ノートPC等の端末、資料等）の管理

■ 盗聴・のぞき見防止対策

- 共有スペースでの作業環境の確認、のぞき見防止フィルター使用など

■ 不正アクセス等への対策

- ID・PW管理の確認
- PCのOS、ソフトウェアのアップデート
- ウィルス対策ソフトの導入、アップデート
- ネットワーク機器の設定確認



取り扱う情報の管理者であるという意識をもって、
自分自身の業務環境を点検・整備しましょう。



テレワーク実施の留意点（2）

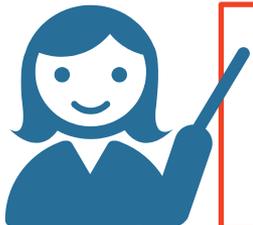
■ ルールの確認・ルールに沿った業務の実施

- 社内規程・ルールを再確認する。
- 不審に感じたメールへの対応手順を確認する。
 - ✓ 添付ファイル、URLリンク等は絶対クリックしない。
 - ✓ システム管理者等への報告 など。
- 報告・相談ルートを再確認する。
 - ✓ PCの動作がおかしいなど、どうしたらいいか分からない場合は、自己判断せずに誰かに相談する。



■ 緊急時対応の確認

- 事故を起こした場合は、定められた手順により速やかに報告を行う。
 - ✓ 早期の対応により被害を最小限にする。

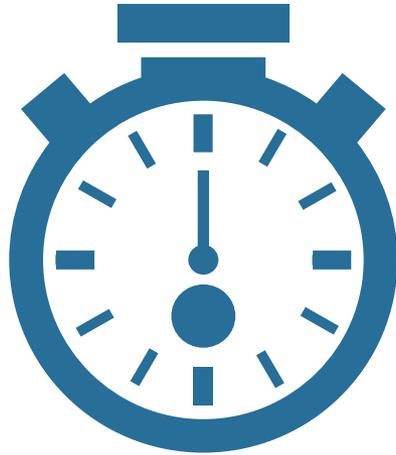


いざという時のため、
緊急時の相談先・連絡先を確認しておきましょう。
(担当者、電話番号、メールアドレスなど)



事故を発生させないためにはどうしたらよいですか？

- 皆さんで考えましょう





個人情報を取り扱うその前に、もう一度

その取扱いは
ルール通りですか？

個人情報を取り扱うのに
適切な環境ですか？



その持ち出しは
本当に必要ですか？

持ち出しているものは

- 必要最小限の情報ですか？
- 会社から承認を受けた情報や
媒体ですか？

まとめ：個人情報取扱いに関する事故
を起こさないために



ルールを理解し、守ることが大切です

事故を起こさない

(未然防止)

事故を起こさないための
体制・対策のルール化

従業者は

定められたルールを
理解し、守る

事故が発生した場合の影響

を最小限に抑える

早期発見、緊急時対応の
ルール化や対策の実施

従業者は

事故発覚・発見時にルー
ルに従って行動する





当社のルール・運用を確認しましょう



緊急事態への対応を確認しましょう

参考情報



参考リンク（1）

■ プライバシーマーク制度サイト

- 【注意喚起】テレワークを実施する際の留意点

<https://privacymark.jp/news/system/2020/0420.html>

- 社内教育用参考資料：個人情報への取扱いに関する事故を起こさないために

「メール誤送信を防ごう」

「紛失・盗難を防ごう」

「日常業務の中で注意すべきこと」

テレワークを行う際の参考情報としても、ご活用ください。

<https://privacymark.jp/system/reference/index.html>

- 付与事業者専用サイト

お役立ちリンク集：国のIT施策・その他関連情報

<https://member.privacymark.jp/>

■ 個人情報保護委員会

- テレワークに伴う個人情報漏えい事案に関する注意事項

https://www.ppc.go.jp/news/careful_information/telework/

■ 経済産業省

- テレワーク時における秘密情報管理のポイントQ&A解説

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf



参考リンク（２）

■ 総務省

- テレワーク総合情報サイト

<https://telework.soumu.go.jp/>

- テレワークにおけるセキュリティ確保

テレワークセキュリティガイドラインが掲載されています。（「テレワーク勤務者が実施すべき対策」参照）

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

- 社員・職員全般の情報セキュリティ対策

外出先で業務用端末を利用する場合の対策や持ち運び可能なメディアや機器を利用する上での危険性と対策について

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_staff.html

厚生労働省

- テレワーク総合ポータルサイト

<https://telework.mhlw.go.jp/>

- テレワークの適切な導入及び実施の推進のためのガイドライン

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/shigoto/guideline.html

■ 独立行政法人情報処理推進機構（IPA）

- 各種テレワーク支援施策

<https://www.ipa.go.jp/action/telework/index.html>