CONFIDENTIAL

AISEL

セキュリティ ガイドライン

テレワーク版　2025年2月

目次

セキュリティーガイドライン（テレワーク版）

目的

テレワーク時に機密情報を扱う業務を行う上で、情報セキュリティに関する基本指針と行動指針を定め、テレワーク時のセキュリティ事故を防止する。

位置づけと概要

セキュリティーガイドラインの位置づけ

このガイドラインは、ISMS、Pマーク等、情報セキュリティ全般への準拠に加え、テレワークにおけるセキュリティに関する部分での詳細事項をまとめた物です。

※”テレワーク”は在宅勤務を含む組織施設外からの業務を指します。

テレワーク実施時も就業規定に定める服務規律等を遵守する必要があります。

規律及びガイドラインに違反した場合、就業規程により処罰される事があります。

このガイドラインの内容

1. テレワークを行う上で実施すべき事・守るべき事の理由
2. テレワーク中の主な禁止事項
3. インフラと環境としての必要要件と、具体的な対策基準や実行手順

補足：リモートを行う時こそ、コミュニケーションの質と社会人モラルを重視

初めて在宅勤務を実行する時には、「在宅勤務時のセキュリティ遵守に関する誓約書」の事前提出が必要です。（管理部門に確認して下さい）

セキュリティーガイドライン（テレワーク版）

1. テレワークを行う上で実施すべき事・守るべき事の理由

出社して業務をしている中では、気が付かないうちに守られている事が多々あります。
テレワークではそれらを理解した上で自己防衛をしなければなりません。

例えば、

- 家族の画面のぞき見やＰＣ操作により、機密情報が見られる可能性がある
- 自宅の空き巣被害でＰＣを略奪され、情報漏洩に繋がる可能性がある
- 自宅ネットワークの脆弱性により、他のＰＣから侵入等される可能性がある
- リモートの方式によって、社外にデータが持ち出される可能性がある

これらは、お客様からみると、出社時に比べてリスク増加の懸念とも捉えられます。
お客様の情報及び、企業の情報を守る事が基本にあってテレワークが可能となります。

この様なリスクを回避する為にガイドラインを作り、その内容を遵守できる方のみにテレワークが許可（指示）されることになります。

セキュリティーガイドライン（テレワーク版）

2. テレワーク中の主な禁止事項

1. 在宅勤務中は、**自宅以外の場所での業務を禁止**する
2. 公衆やフリーのアクセスポイント等、漏洩リスクの高いネットワークへの接続は禁止する
3. 会社貸与ＰＣ以外へのデータの複製、保存は禁止する
4. スクリーンショットの画像化や印刷、テキストのコピー等の情報複製を禁止する
5. 社員以外の同居人等が、会社貸与ＰＣ及び機密情報に接する行為を禁止する
6. テレワーク勤務における紙資料の持ち出しに関しては原則禁止する
   事前に顧客及び上長に持ち出し許可を得た場合に関しては可とするが、
   持ち出した資料の複製及び第三者の閲覧は禁止する
   ※ 部門に定型の持ち出し管理があればそれに従う事

セキュリティーガイドライン（テレワーク版）

3. 利用する機器やネットワークに関する制限

- ■ 社内情報への接続方法
- ■ 利用するＰＣ機器等
  - 会社貸与ＰＣ、顧客貸与ＰＣ
  - 自己所有機器
- ■ テレワーク場所（自宅）のネットワーク
- ■ テレワークを実行する時の環境への注意
- ■ Microsoft 365を、社外で利用する時の機器制限

セキュリティーガイドライン（テレワーク版）

3. 利用する機器やネットワークに関する制限

■ **社内情報への接続方法**

- **仮想ネットワーク 接続方式**　（Virtual Private Network：以下　ＶＰＮ）
  会社のネットワークに外部から接続する (ネットワークが直接つながる方式)
  ※ 会社貸与ＰＣのみ可 (社内LANに直接つながるため、会社にあるPCと同一扱い)

- **リモートデスクトップ 接続方式**　（Remote View：以下　ＲＶ）
  会社のＰＣ・サーバー画面を遠隔操作 (ネットワークが直接にはつながらない方式)
  ※ 会社貸与ＰＣは可、自宅ＰＣの利用も条件付きで可 (サーバー遠隔制御、保守含む)
  ※ スマホ、タブレットでの利用も可能

- **セキュア・インターネット ログオン方式**
  インターネットに公開されていて、社内管理されているログオンID、パスワードで
  アクセスするシステム（AIPO、MA-EYES(外用)、Microsoft365ブラウザ等）
  ※ 会社貸与ＰＣ及び、自宅ＰＣ可

※どの方式であっても、会社貸与ＰＣ以外への機密データの格納は禁止です

セキュリティーガイドライン（テレワーク版）

3. 利用する機器やネットワークに関する制限

■ **利用するＰＣ機器等**

- **原則として会社から貸与したＰＣからのみ業務が可能**

  業務用のＰＣは会社から貸与します
  ※ 貸与ＰＣの故障や緊急事態で貸与が間に合わない、社内のＰＣやサーバーの画面を直接遠隔で見る保守等の場合では、条件付きで私用ＰＣを認める場合があります

- **会社貸与ＰＣについて**

  HDD/SSDが暗号化されていないものは持ち出し不可
  セキュリティソフトがインストールされている事（AppGuardもしくはESET）
  自己所有のＵＳＢメモリ等の記録媒体をＰＣに接続する事は禁止
  私的利用は禁止（インターネット閲覧・ゲーム等）
  メーラーに私的な個人用アドレスを設定する事を禁止

- **顧客からＰＣを貸与された場合について**

  お客様が定める利用規則等を厳守して業務をする事
  顧客のＰＣには、アイセルのデータを保存する事を禁止する
  自宅ネットワーク等に対して指示が無い場合、会社貸与ＰＣと同一の基準で考える事

セキュリティーガイドライン（テレワーク版）

3. 利用する機器やネットワークに関する制限

■ **利用するＰＣ機器等**

- **自己所有の私用PCについて**
  在宅勤務を行う場合は、会社からPCを借り受けてください

  私用PCでは、リモートデスクトップ方式又は、セキュア・インターネットログオン方式によるWEBブラウザでのみ可とし、アプリ導入や仮想ネットワーク方式は不可とする

  業務で使用する場合は、以下の情報を上長に申請し、許可を受けなければならない

  1. 公衆等フリーの回線ではないインターネット回線を所有し利用することの宣言
  2. セキュリティソフト及び、OSのアップデートを常に有効に設定している事の宣言

- **その他機器について**
  モニター・キーボード・マウス・ヘッドセットは、自己所有物の利用を可とする
  マイク＆カメラに関しては、原則会社から貸与をするが自己所有物の利用も可とする

セキュリティーガイドライン（テレワーク版）

3. 利用する機器やネットワークに関する制限

■ テレワーク場所（自宅）のネットワーク

- 自宅におけるネットワーク（回線、通信機器）は自己所有のもの、集合住宅の場合は住宅共有のものを利用すること
  ※ 時間帯や利用状況によって遅く不安定になる、などの対策は各自で行うこと

- 回線契約が無い、フリーアクセスの公衆無線LAN等でのテレワークは禁止する
  ※ POKET Wi-Fi等、いわゆるキャリアＳＩＭを使った接続は可とする
  （通信量など各自で注意のこと）

- 接続方式については有線を推奨とする
  無線の場合、ルーター及びSSIDに強力なパスワードがかかっていること
  暗号化なしや、WEPなど強度が低い暗号化方式の利用は禁止する
  MACアドレスをネットワークアクセス認証の用途で利用しない事

- 通信機器の脆弱性対応を行う
  自己所有する通信機器のメーカーサポート状況を確認すること
  ◆ 脆弱性対応したファームウェアの更新などがあれば適用すること
  ◆ 修正が提供されない（サポート終了）機器を長期間利用しないよう注意すること

セキュリティーガイドライン（テレワーク版）

3. 利用する機器やネットワークに関する制限

■ **テレワーク場所（自宅）のネットワーク**

- 家族と共用のネットワークを利用する場合は、VPN接続が完了するまでは他のPCから侵入される懸念があるため、原則は同時利用を禁止とする（特にVPN接続するまでの間）

  ※ VPNを稼働していない状態で、自宅ネットワークに接続することは禁止する
  ※ 他のPCが存在する場合、先んじてセキュリティソフトの有効稼働等を確認しておく事

  セグメントを分けるなど相互通信がされないようなルーター設定を推奨する

- 貸与PCに権限設定がない共有フォルダがある場合、自宅ネットワーク接続は禁止する
- スマートフォンなどPC以外の自己所有機器への情報漏洩が無いよう通信制限すること

セキュリティーガイドライン（テレワーク版）

3. 利用する機器やネットワークに関する制限

■ テレワークを実行する時の環境への注意

- 家族や他の人がいる場合、画面が容易に見られない作業場所を確保する事
  スピーカーから音を出す場合やマイクで会話する場合も、安易に聞かれない様にする事
- 全てのアクセス手段（接続方法及びID/PASS等）は、自分以外の人には教えない事、メモを貼らない事、会社貸与や顧客貸与の業務用PCを触らせない事
- 利用中の画面は自分以外が見られないようにし、休憩時を含みPCから離れる時は他の人がそばにいなくても必ず画面をロックする事
- 私用で家の中を撮影する場合など、PCの画面や音声が記録されないように注意する事
- 業務が終了したら速やかにRV・VPNの接続を終了し、PCをログオフする事
- PCを利用しない時には、キャビネット等に保管する事（鍵付きを推奨）

セキュリティーガイドライン（テレワーク版）

災害発生時等の緊急連絡には、Teamsによる連絡・報告を基本とします。
詳細は 事業継続計画 の「災害時緊急連絡網」を参照してください。

3. 利用する機器やネットワークに関する制限

■ **Microsoft365を、社外で利用する時の機器制限**

① 私用機器：利用不可
ローカルにデータを残さない事を重視（ダウンロードも禁止）
スマホは紛失の可能性が高く、かつアプリ版はデータを保持する為、漏洩リスクがある
紛失時の報告を義務付けられない、機種変更と区別がつかない等を鑑み利用不可とする

② 貸与スマホ：制限（条件付き利用可）
紛失報告の問題はないが、アプリ版は漏洩防止強化の為に対象者を制限する
＊責任をもって管理できる（部長職以上と会社が認めたPM、PL等）に限定し、
リモートワイプ、アプリ制限等のMDM機能（Intune）を導入する事を必須とする

＊私用スマホはWEB版のOfficeなら可		Office WEB版	Office アプリ版	理由他
Outlook (メール、スケジュール)	貸与PC	○	○	
	私用PC	○	×	①
	貸与スマホ	○	△	②：要MDM
	私用スマホ	○	×	①
Teams （チームの利用）	貸与PC	○	○	
	私用PC	○	×	①
	貸与スマホ	× 存在しない	△	②：要MDM
	私用スマホ	× 存在しない	× TV会議のみ可	①

（注）ＷＥＢ版とは、ブラウザ上で動作させるもの
アプリ版とは、office.com、各store等からダウンロードし、PCやスマホ等にインストールして使うもの

セキュリティーガイドライン（テレワーク版）

補足：リモートを行う時こそ、コミュニケーションの質と社会人モラルを重視

■ テレワークを含む、リモートでの業務で起こりうるマイナス面を防止する

リモートでの業務は、周りを気にする事や気にされる事が減少し、孤立をも引き起こします
上司部下・メンバー全員が、お互いのメンタルを出社時以上に気にかけねばなりません
顔を見て気がつく事も多く、チーム全員で孤立化やメンバー間のトラブルを防ぎましょう

上司は、偏りがないようにまんべんなく部下に言葉をかけ、メンタル状況を常に見ること
チャットだけではなく、頻繁に人を集めて対面やTV会議で顔を見た会話をすること
（自宅背景は消すなどプライバシー考慮の事）
※ 新卒メンターの方も同様です、又、孤立しがちな一人住まいの方には特に配慮が必要です

チャットの利用は、容易に単発で発言できる為、業務中の会話であることを忘れがちです
顔が見えない、言葉が足りない等、意思疎通に齟齬が生じてトラブルの元になりがちです

提供されるチャットツールは私用ではありません、業務レベルでの発言（文面）をすること
重要な報連相は、顔を見ながらのTV会議や、状況を纏めて説明内容が残る方法で行う事

※ 社会人として適切な運用ができない様であれば、利用を制限する場合があります
チャットの多用により、対外的なメール等の文章作成能力の低下を懸念しています
会社は利用ログを取得していますので、必要に応じて閲覧する場合があります

変更履歴

2020年12月1日	テレワーク業務に伴う、セキュリティガイドライン制定	初版
2022年2月	目次の追加 全体の見直し	目次ページの作成 文体の整理と表記ゆれの修正
2023年2月	目次 M365を利用する機器の制限	リンクの作成 災害時等は「Teams連絡が基本」を追記
2023年10月	位置づけと概要	”テレワーク”の表記ゆれ(リモート勤務)を修正
2024年2月	テレワーク場所のネットワーク	MACアドレスを認証に利用しないよう修正
2025年2月1日	全ページ 3.■ テレワーク場所（自宅）のネットワーク	ロゴマークの更新 自己所有の通信機器のサポート状況確認を追記