2020 年 5 月 25 日

在宅勤務・テレワークでの注意事項

ＪａＧｒａプライバシーマーク審査センター
業務室長　斎藤　成
（東京グラフィックス専務理事）

新型コロナウイルスへの対応で会員各社では、在宅勤務・テレワークを実践されている事業所も多くございます。本日（5 月 25 日）政府は緊急事態宣言を解除いたしましたが、未だ気を緩めることはできません。そこでＪａＧｒａとして、テレワークに際して個人情報保護、営業の秘密保護の観点から注意事項を以下に掲載いたします。重複する項目もありますが、参考になさってください。
なお引用は、ＪａＧｒａ「個人情報保護ガイドブック第 6 版」をはじめ、（独法）情報処理推進機構（ＩＰＡ）:「日常における情報セキュリティ対策」、また営業の秘密情報管理については、経済産業省知的財産政策室：「テレワーク時の秘密情報管理のポイント」等の最新の資料から抜粋します。

JISの要求事項とJaGraガイドブックから

まず、個人情報保護については、ＪＩＳ　Q15001　2017 年版　附属書Ｃでは、
【テレワーキング】管理策：テレワーキングの場所でアクセス、処理及び保存される個人情報を保護するために、方針及び支援するセキュリティ対策を実施することが望ましい。と規定されています。プライバシーマーク付与事業所では、方針と対策を立て、実施なさってください。
次に、ＪａＧｒａの個人情報保護ガイドライン第 6 版「安全対策基準」では、テレワーク等で社外へのＰＣ持ち出し利用について、以下のように規定しています。
◆社外へのＰＣ持ち出し利用について
①　ＰＣの社外持ち出しは、原則禁止とする。
②　業務上やむを得ない事情がある場合は、以下の措置を実施する。

・持ち出す際は、事前に使用するＰＣや周辺機器、使用者名、使用期間、使用目的につき業務責任者の承認を得て、情報システム責任者へ申請し貸与を受ける。
・情報システム責任者は、持ち出し用のセキュリティ対策を施したＰＣや周辺機器を用意する（ＰＣは暗号化、周辺機器はパスワード保護を原則とし、いずれもウイルスチェックを済ませることとする）。
・使用者は、持ち出したＰＣが盗難されないよう、気を配り、電車等の網棚に載せたり、社用車に放置したりすることなく、自分の身から離さないようにする。また酒席へ持ち込むこ

とのないようにする。
・使用者は、持ち出すＰＣに保管する情報を必要最小限とし、原則として機密データは保管しない。リスクを分散するため、機密データは周辺機器に保管することを原則とし、持ち出すＰＣに機密データを保管する必要がある場合は、機密データの漏えいを防ぐため、暗号化やアクセス制御等の対策を講じる。
・使用者は、持ち出したＰＣにおける機密データの使用を必要最小限にとどめる。
・使用者は、持ち出した情報システム機器を使用後、ＰＣや周辺機器内のデータを消去し、速やかに返却する。
・情報システム責任者は、貸出台帳に貸出及び返却記録を残し、定期的に棚卸を実施し、未返却や逸失した情報システム機器がないかどうか確認する。

IPA「日常における情報セキュリティ対策」

（独法）情報処理推進機構　2019 年 4 月 2 日更新

◆組織のシステム管理者向け

1.情報持ち出しルールの徹底

業務用パソコン等の機器やデータを組織外に持ち出す場合のルールを明確にし、関係者に周知徹底してください。また、そのルールに則り適切に運用されているかを確認してください。ルールの例としては、関係者に機器を貸し出しする際は、機器内に不必要なデータが保存されていないか事前に確認する、紛失した場合に備えて、持ち出す機器や USB メモリ等の外部記憶媒体には適切な暗号化を施す、等があります

2.社内ネットワークへの機器接続ルールの徹底

ウイルス感染したパソコンや外部媒体等を社内ネットワークに接続することで、ウイルスをネットワーク内に拡散してしまうおそれがあります。普段は社内ネットワークに接続していないパソコン等の機器を社内ネットワークに接続する場合のルールを明確にし、関係者に周知徹底してください。 接続する機器の脆弱性対策やウイルスチェックなどが適切に実施されているかを確認してください。

3.修正プログラムの適用

管理するサーバやパソコン等の OS（オペレーティングシステム）、ルータやスイッチ等のファームウェア、各種ソフトウェアに修正プログラムを適宜適用し、最新のバージョンに更新、維持するようにしてください。

4.セキュリティソフトの導入および定義ファイルの最新化

管理するサーバやパソコン、スマートフォン等にセキュリティソフトを導入するとともに、

セキュリティソフトの定義ファイル（パターンファイル）が常に最新の状態になるように設定し、最新の状態になっているか定期的に確認してください。

5.定期的なバックアップの実施

システムの不具合やランサムウェア等のウイルスによるデータ破壊に備えて、定期的に外部記憶媒体等へバックアップを行ってください。特に重要なデータは必ずバックアップを行ってください。

6.パスワードの適切な設定と管理

システム管理等で使用するパスワードは可能な範囲で複雑な長い文字列を設定してください。大小英字、数字および記号を混在させて、最低でも 8 文字にしてください。他のシステムやインターネットサービスで同じパスワードを使い回さないでください。また、パスワードを初期設定のままで利用していないか確認してください。

7.不要なサービスやアカウントの停止または削除

外部から接続できるサーバで稼働している不要なサービスや、管理する機器やシステムに存在する不要なユーザアカウントは、停止または削除してください

テレワークを行う際のセキュリティ上の注意事項

ＩＰＡ　2020 年 5 月 20 日更新

https://www.ipa.go.jp/security/measures/everyday.html#section2

1. 修正プログラムの適用
2. セキュリティソフトの導入および定義ファイルの最新化
3. パスワードの適切な設定と管理
4. 不審なメールに注意
5. ＵＳＢメモリ等の取り扱いの注意
6. 社内ネットワークへの機器接続ルールの遵守
7. ソフトウェアをインストールする際の注意
8. パソコン等の画面ロック機能の設定

テレワークを始める前に

テレワークで使用するパソコン等は、できる限り他人と共有して使わないようにしてください。共有で使わざるを得ない場合は、業務用のユーザアカウントを別途作成してください。ウェブ会議のサービス等を新たに使い始める際は、事前にそのサービス等の初期設定の内容を確認してください。特にセキュリティ機能は積極的に活用してください。

自宅で行う場合

自宅のルータは、メーカーのサイトを確認のうえ、最新のファームウェアを適用（ソフトウェア更新）してください。

公共の場で行う場合

カフェ等の公共の場所でパソコン等を使用するときはパソコンの画面をのぞかれないように注意してください。

公共の場所でウェブ会議を行う場合は、話し声が他の人に聞こえないように注意してください。

公衆Ｗｉ－Ｆｉを利用する場合は、パソコンのファイル共有機能をオフにしてください。

公衆Ｗｉ－Ｆｉを利用する場合は、必要に応じて信頼できるＶＰＮサービスを利用してください。

デジタルデータ／ファイルだけではなく、紙の書類等の管理にも注意してください。

◆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」

2020 年 5 月 7 日更新

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

●企業内部で保管していた営業秘密の持ち帰り作業の対応

テレワークへの切り替えにあたって、改めて、秘密情報の管理の態様や諸規程の整備 状況を確認し、必要に応じて見直しを図ることが有用と考えられます。

具体的には、

① 営業秘密管理規程や情報取扱規定、セキュリティ規定等の社内規程がテレワークに即した内容になっているかの確認・改訂

②当該諸規程について従業員（派遣労働者も含みます。）への周知徹底（メールによるリマインドやｅ－ラーニングの実施等）

③ 情報の性質に応じた当該情報への適切なアクセス権者の設定

④ 「㊙」（ マル秘）・「社内限り」といった秘密であることの表示の付記

⑤ ＩＤ・パスワードの設定――― といった対応をとることが考えられます。

不正競争防止法が求めている営業秘密該当性の３要件＊のうち、テレワークへの切り替えにあたっては、特に、秘密管理性要件をどのように確保するかについて、この秘密管理性要件の趣旨は、「企業が秘密として管理しようとする 対象（情報の範囲）が、従業員等に対し

て明確化されることによって、従業員等の予見可能性、ひいては経済活動の安定性を確保する」ことにあります。

＊不正競争防止法「営業秘密」の保護　3 要件

①　秘密として管理されていること（秘密管理性）

②　有用な技術上又は営業上の情報であること（有用性）

③公然と知られていないこと（非公知性）

そこで、まず、会社として、自社が保有している情報のうち秘密として管理しようとする情報の範囲を明確にするとともに、当該情報に対する従業員の予見可能性を確保するために、どのような措置（秘密管理措置）を実施するかを検討する必要があります。

例えば、営業秘密管理規程や情報取扱規程、セキュリティ規程等を設けている場合、「秘密として管理しようとする情報」が当該規程上の「秘密情報」等に含まれるかを確認することが有用です。
また、各種情報取扱規程等との関係では、テレワークの実施にあたり、秘密情報等の社外への持ち出しを認めることが予想されますが、一方で、各種情報取 扱規程等において、「秘密情報の社外への持ち出し禁止」などとのみ規定されている場合には、テレワークの実施によって、当該規程等が形骸化することになり、ひいては、従業員の予見可能性を減退させる可能性も出てきます。

そこで、各種情報取扱規程等の関連規程を改めて見直し、通常勤務における情報の取り扱いに関する規定に加えて、テレワークの実施を念頭に、必要な場合には秘密情報の社外への持ち出しを認めつつ、その場合のルール（秘密管理措置）を定めること（各種情報取扱規程等の見直しも含みます。）が考えられます。

その他、テレワーク開始にあたって、改めて、従業員の予見可能性を確保するために、情報の性質に応じた当該情報への適切なアクセス権者の設定、秘密情報が含まれる媒体への「㊙」（マル秘）・「社内限り」といった秘密であることの表示の付記、ＩＤ・パスワードの設定等の措置（各種情報取扱 規程等におけるルールの設定状況及び実施状況）を再確認し、必要に応じ追加的措置をとることも有用です。

なお、テレワーク実施の過程で上長等への申請や許可の取得を求めるべきケースも想定されますが、テレワークの実効性を確保するため、申請・許可を伝統的な「捺印」では なく、「電子的方法」によることができるよう、また、申請等の履歴データを残すという 意味でも、必要に応じて関連規程の確認・見直しをすることも考えられます。

●秘密情報（重要書類）の保護

テレワークの実施にあたって、通常、企業内部において紙媒体で保存している秘密情報（重要書類）を、自宅等に持ち帰ったとしても、直ちに営業秘密としての法的保護を失うわけではありません。 以下のポイントを押さえた管理を意識することで、万が一の場合でも、営業秘密として不正競争防止法による法的保護を受けられる可能性があります。

秘密管理性要件の趣旨は、前述のとおり、「企業が秘密として管理しようとする 対象（情報の範囲）が、従業員等に対して明確化されることによって、従業員等の予見可 能性、ひいては経済活動の安定性を確保する」ことにあります。

したがって、例えば、持出しをする秘密情報が紙媒体の場合、当該書面に「㊙」（マル 秘）・「社内限り」等の秘密であることの表示を付すことによって、従業員の予見可能性を確保するといった方法が考えられます。

この他、必ずしも営業秘密として保護されるために必須の要件ではありませんが、秘密情報の保護に役立つ手法として、以下のような秘密情報（重要書類）を社外に持ち出すに当たってのルールを整備することも考えられます。

・持ち出しを認める書類を厳選する
・持ち出しにあたって上長等の事前許可を必要とする
・持ち出しをした者・書類・期間を一覧で管理する
・持ち出しをした際の管理方法を徹底させる（書類を机上に放置しない等）
・業務上の必要がなくなった場合には、返却を義務付ける。あるいはシュレッダーで裁断するなどの秘密保持に資する安全な方法による廃棄を義務付ける 等

また、テレワーク中に従業員による書類のコピーやファイルの印刷を認める場合もあるかもしれません。その場合には、上記と同様に、以下のようなファイルをコピー等するに あたってのルールを整備することも考えられます。

・コピー等をした際に当該書面に「㊙」（マル秘）・「社内限り」等の秘密であることの 表示が付されるように設定をしておく
・コピー等を認めるファイルを厳選する
・コピー等にあたって上長等の事前許可を必要とする
・コピー等をした者・書類を一覧で管理する
・コピー等をした際の管理方法を徹底させる（書類を机上に放置しない等）
・業務上の必要がなくなった場合には返却を義務付ける、あるいはシュレッダーで裁断するなどの秘密保持に資する安全な方法による廃棄を義務付ける 等

これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程等の関連規定の内容を再確認（場合に より見直し）するとともに、その実施状況の確認をすることが有用です。

なお、紙媒体は、技術的に複製を制限することや、第三者への提供等を制限すること が困難ですので、中長期的には、可能な範囲でペーパーレス化を進めることも、有用です。

秘密情報の保護に役立つ手法として、以下のようなローカルフォルダへの保存にあたっての ルールを整備することも考えられます。

・ローカルフォルダへの保存を認めるデータを厳選する
・保存にあたって上長等の事前許可を必要とする
・できる限り私物端末機器ではなく勤務先貸与端末機器を使用させる
・勤務先貸与端末機器には勤務先が承認していないソフトをインストールしない（勤 務先貸与端末機器に技術的な設定変更制限が可能であれば設定する）
・私用・家族との共用を許可しない
・保存をする勤務先貸与端末機器には勤務先所定のウイルス対策ソフトのインストー ルを徹底する等十分なセキュリティ対策を行う
・保存をした者・ファイル・期間を一覧で管理する
・業務上の必要がなくなった場合の廃棄を義務付ける 等

そこで、万が一の事態に備えて、以下のような手立てを講じておくことも考えられます。

（未然の防止策）

①営業秘密へのアクセス権者の設定範囲を改めて確認し、当該営業秘密にアクセスする必要のない従業員がアクセスできないようにすること。

②社内教育の実施や社内規程の周知等を通じて、秘密情報管理の重要性に関する従業員の理解を深め漏えいに対する危機意識を高めること。

③情報漏えい行為を実施しにくい状況を作り出すための工夫として例えば以下のような対策を行うこと。

・メールの転送制限
・メールへのファイル添付の制限
・メールを送信する際に上長の承認を必要とする設定
・メールを送信する際に上長が常にＣＣに追加される設定
・遠隔操作によりＰＣ内のデータを消去できるツールの利用
・社用ＰＣにＵＳＢやスマートフォンを接続できないようにする設定
・コピー防止用紙やコピーガード付きの記録媒体等の利用

・プリントアウトの制限 等

また、以下のような対策を講じることによって、万が一、情報漏えいが起きた場合でも、開示先等による営業秘密へのアクセスを制限したり、営業秘密の流出元・流出先を把握することが可能になると考えられます。

（事後的な対応を可能とするための対策）

・データの暗号化による閲覧制限

・ＰＣのシンクライアント化

・従業員による営業秘密へのアクセスやダウンロードのログの保存

・一定回数、パスワード認証に失敗すると秘密情報を消去できるツールの利用 等

以　上