在宅勤務者のセキュリティ注意点

在宅勤務者のセキュリティポイント

- セキュリティポリシーに沿った業務の遂行
- 利用する情報資産の管理責任者であることの自覚
- セキュリティルールに従って作業すれば責任は問われない
- 定期的なセキュリティ対策実施状況の自己点検
- 情報セキュリティ事故発生時に備え、連絡体制の確認
- 業務で使用する PC やデバイスは安全な場所で使用・管理
- 第三者による不正アクセスや、画面ののぞき見を防ぐ
- VPN 通信など信頼できるネットワークを使用
- 情報資産の暗号化、およびセキュアなバックアップ
- 許可されたアプリ以外のインストール禁止
- 業務に関係のないサイトへのアクセスをしない
- セキュリティ対策ソフトや、OS を最新にする
- 利用者認証管理情報の厳格な管理と運用

テレワークによって、在宅勤務を行う人は、会社で実施している情報セキュリティ対策に関する行動指針に加え、更に気を付けるべきポイントが増えます。
これは、堅牢なセキュリティシステムに守られた会社内での業務とは違い、ネットワーク越しで社外からの業務活動を行うことになるため、脅威のレベルが当然上がるからです。よって、テレワークを実施するためには、従来のセキュリティーポリシーを見直し、在宅勤務者用のセキュリティルールを定めることが前提となります。
在宅勤務者は、会社で定めたセキュリティポリシーを遵守し、自宅で取り扱う会社の情報資産の管理責任者であることを自覚する必要があります。会社で定めたテレワークに適したセキュリティルールに従って業務作業を遂行している限りにおいては、原則責任は問われません。
そのためにも、ルールに従ったセキュリティ対策実施状況を自己点検して、万が一情報セキュリティ事故が発生したときに備え、連絡体制の確認が必要です。
業務で使用する PC やモバイル端末は、盗まれたりしないよう家の中で安全な場所で使用し、管理します。その際、家族も含め、第三者が不正に利用したり、業務作業中の画面をのぞき見されないよう注意が必要です。家庭内の Wi-Fi を家族で共有しているときなど、不正に会社のデータがアクセスできないように、VPN を使用したり、ディスク上のデータを暗号化して、安全なバックアップを実施しておくことも大切です。
また、ゲームなど許可されていないアプリをインストールしたりすることはもちろん禁止ですし、誰もまわりに居ないからとつい普段家で使っている Web サイトを見てしまいがちですが、マルウェア侵入等のセキュリティリスクがあるため業務に関係ない Web サイトへのアクセスは絶対ダメな行いだと認識すべきです。
セキュリティ対策にとって当たり前な、OS のアップデートやアンチウィルスソフトの定義ファイルの更新などは、VPN で繋いだ場合の回線が遅いからと後回しにしてしまいがちです。OS のアップデートなどは、業務時間外にスケジュール設定するなど、忘れないように対処が必要です。そして、ID やパスワードなど、絶対に家族や第三者に知られないよう会社にかいる時以上に気をつけて、管理と運用をすることが重要になります。
セキュリティルールを守り、事故がない安心安全な在宅勤務を継続するため、普段からの心がけが大切です。