テレワークのセキュリティ対策

テレワークに必要なセキュリティの考え方

① ルールによるセキュリティ対策
- セキュリティガイドラインの策定
- セキュリティルール・情報管理ルールの策定
- ガイドラインとルールの遵守・浸透

② 技術的なセキュリティ対策
- アクセスの管理・制限
- 暗号による管理
- 運用のセキュリティ
- ネットワークのセキュリティ

③ 物理的なセキュリティ対策

（参照元： 厚生労働省　テレワークではじめる働き方改革　テレワークの導入・運用ガイドブック）

厚生労働省が公開している「テレワークではじめる働き方改革 テレワークの導入・運用ガイドブック」には、実践編として安全なテレワークのためのセキュリティ対策が掲載されています。
テレワークを実施するためには、ルールによるセキュリティ対策に加え、技術的、物理的な側面からも総合的にセキュリティ対策を行う必要があります。

① ルールによるセキュリティ対策
- 企業のセキュリティポリシーに従い、テレワーク導入後の運用に即した、組織として統一のとれた情報セキュリティに関する基本方針や行動指針を明文化する「セキュリティガイドライン」を作成します。
- 自宅における作業環境、PC の保管及び管理方法や、社内の紙媒体資料の持ち出しに関するルールの設定など、テレワーク特有の行動のルールを決定するため、セキュリティルール・情報管理ルールの策定をします。
- セキュリティガイドラインやルールを、テレワーク実施者に遵守するよう求める必要があるため、研修などを通じて従業員に理解してもらい、浸透させることが重要です。

② 技術的なセキュリティ対策
- システム及びアプリケーションへのアクセスが従業員本人によるものであることを認証することや、あらかじめ登録されている端末からのみのアクセスを許可することなどの措置を講じるアクセスの管理・制限が必要です。
- たとえ PC が紛失してしまったり、盗難に遭った場合でも、すぐに情報が漏えいするリスクを防ぐため暗号による管理をします。
- 電子データの原本保存やウイルス対策ソフトなど、脅威に備えた運用のセキュリティが必要です。
- より安全な回線を選択し、正規のサーバ証明書なども取得して、ネットワークのセキュリティが重要です。

③ 物理的なセキュリティ対策
- 監視カメラや入退出管理といった盗難防止策や、施錠棚やシュレッダーによる情報漏えいの防止策などの物理的なセキュリティ対策が必要です。

安全なテレワークを実施するために、こうした３つの総合的なセキュリティ対策は、企業にとって最重要事項です。