テレワークのセキュリティ

テレワークセキュリティガイドライン

1. テレワークにおける情報セキュリティ対策の考え方
   - 「ルール」「人」「技術」のバランスがとれた対策の実施 .
   - テレワークの方法に応じた対策の考え方
   - 経営者、システム管理者及びテレワーク勤務者それぞれの立場

2. テレワークセキュリティ対策のポイント
   - 経営者が実施すべき対策
   - システム管理者が実施すべき対策
   - テレワーク勤務者が実施すべき対策

3. テレワークセキュリティ対策の解説
   - 情報セキュリティ保全対策の大枠
   - マルウェアに対する対策
   - 端末の紛失・盗難に対する対策
   - 重要情報の盗聴に対する対策
   - 不正アクセスに対する対策
   - 外部サービスの利用に対する対策

（総務省　テレワークセキュリティガイドライン　第４版　別紙３より）

東京オリンピック・パラリンピックや、新型肺炎の感染リスクを少なくするためにテレワークが叫ばれておりますが、その実施の際必ず気を付けなければいけないのが、IT セキュリティです。
そうした中、これからテレワークを導入しようと考えている企業が、どのような情報セキュリティ対策を講じるべきかを検討する参考として、総務省よりテレワークセキュリティガイドラインが Web 上でも公開されています。
このガイドラインから、テレワークを実施する上でのセキュリティに関するポイントをまとめてみます。
テレワークを効率的に実施するためには、ICT の活用が欠かせません。時間・空間を有効に活用する多様な就労・作業形態として、ICT の利用により、在宅勤務、モバイル、サテライトオフィスから、会社とのデータのやり取りを可能にして、社外からでも業務を行うことができるのがテレワークです。
情報セキュリティにおいて、テレワークとオフィスでの仕事との違いは、会社関係者同士での情報をやりとりするのにインターネットを利用する必要があったり、第三者が立ち入る場所で業務作業を行うリスクがあったりすることなどが挙げられます。
企業が情報セキュリティ対策を行う際は、保護すべき情報資産を洗い出し、どのような脅威や脆弱性、リスクがあるのかを十分に把握し、体系的な対策を実施することになりますが、情報セキュリティ対策には「最も弱いところが全体のセキュリティレベルになる」という特徴があることを認識する必要があります。だからこそ、どこか１箇所に弱点があれば、他の対策をいくら強化しても全体のセキュリティレベルの向上にはつながらないため、情報資産を守るためには、「ルール」・「人」・「技術」の三位一体のバランスがとれた対策を実施し、全体のレベルを落とさないようにすることがポイントとなります。
テレワークには様々なパターンがあり、「テレワーク端末への電子データの保存の有無」、「オフィスで利用する端末との関係」と「クラウドサービスを利用するかどうか」をもとに分類し、適切な対策をとります。
そして、テレワークにの実施においては、経営者、システム管理者、及びテレワーク勤務者のそれぞれの立場からテレワークセキュリティの保全に関してどのようにすべきかを認識し、対策をとります。
企業は、このガイドラインをもとに、企業の推進するテレワークに合わせたセキュリティ対策を講じる必要があります。