あなたの会社のテレワークは大丈夫ですか？

～会社外の情報セキュリティ対策について～

働き方の多様化や災害などの緊急時に備え、テレワークを実施又は計画している企業もあるかと思います。

BCP（事業継続計画）においても重要な考え方で、導入を推奨されていますが、自宅等で業務を行うには事前に規則を決めるほか、情報セキュリティ対策をしっかりと行う必要があります。

おろそかにすると、個人情報や機密情報の漏えい等のセキュリティインシデントが発生し、損害賠償や信用失墜につながる恐れがあります。

次に挙げる注意点を参考に、安全なテレワークを実施して下さい。

使用するパソコンの注意点

会社が準備しているパソコンを自宅で使用するのであれば、会社の情報セキュリティ基準を満たしているはずですが、従業員所有のパソコンを使用する場合は注意が必要です。

会社として従業員に対し次の点を指導・確認しましょう！

○　サポート期限の切れたOSやアプリの使用を禁止する。
　※　Windows7は2020年1月14日で既にサポート終了
○　セキュリティ対策ソフトを導入させる。
○　OSやアプリのアップデートを適切に実施させる。
○　会社から持ち出せるデータ（情報）を定め、適切に管理させる。
　※　USBメモリなどでデータを管理する場合は、紛失に備えて暗号化やパスワードの設定などを行う。

使用する回線の注意点

会社でVPN回線を使用している場合は、テレワークでもその回線を使用すれば安全ですが、多くの場合は通常のインターネットを使って会社とやりとりをしています。

会社として従業員に対し次の点を指導しましょう！

○　Wi-Fiルータ等の情報通信機器を初期設定のままで使用させない。
○　店舗等が提供しているWi-Fiスポットに注意させる。
　※　セキュリティのレベルが事業者によって異なります。

被害に遭った場合は速やかに警察へ相談しましょう！

警察の相談窓口

・警察本部警察安全相談窓口
　TEL 098-863-9110(又は、プッシュ回線等から#9110)
・各警察署の警察安全相談窓口