サイバーだより

令和２年４月１４日

長野県警察本部
サイバー犯罪捜査課

テレワーク勤務のサイバーセキュリティ

新型コロナウイルス感染拡大防止のため、テレワーク勤務が推奨されています。勤務先がテレワーク専用のシステムを導入していれば、セキュリティ対策は考慮されているはずですが、急遽テレワーク勤務することになった場合、対策が十分とは言えません。

１　悪意のあるソフトウェア対策

○　ウィルス対策ソフトの導入。
○　OS、アプリケーションを最新状態に保つ。
○　不要、電子署名されていないソフトウェアはインストールしない。
○　電子メールの添付ファイル、リンク先に一層の注意を払う。

標的型メールの脅威

件名　Web会議の開催
下記URLから参加願います。

２　盗聴対策

○　機密データを送信する際は暗号化する。
○　無線LANは必ず暗号化して利用。
　公衆無線LANで機密情報を扱わない。
○　公共の場所でパソコンを使用する際は、のぞき見に注意。

脅威（盗聴）
不正なFree-Wifi

３　外部サービスの利用

○SNSは、社内等でルールを定めてから利用。
○ファイル共有（クラウドサービス）では必ずファイルを暗号化。
　相手のダウンロードが完了した時点で、速やかに削除。
○パスワードの使い回しを避け、短いものや単純なのもは使用しない。

【被害に遭わないために】

テレワークにはリスクも生じます。リスクを認識した上で社内ルールを定め、大切な情報資産を守って下さい。

【参考】　総務省　テレワークセキュリティガイドライン（第4版）
https://www.soumu.go.jp/main_content/000545372.pdf