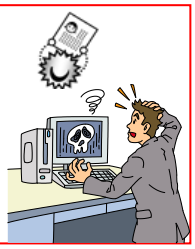
TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2020年 第9号

安全なテレワークのためのサイバーセキュリティ対策

テレワークでは、オフィスのサイバーセキュリティの環境と異なり、勤務先のシステム等に外部からアクセスするため、マルウェア（ウイルス）に感染するリスクが高まります。今回、基本的な注意点と対策について紹介します。

コンピュータの注意点

Web サイトやアプリケーションを介してコンピュータウイルスに感染し、情報を盗まれることがあります。



対策

OS やウイルス対策ソフトは、常に最新の状態に更新し、利用前及び定期的にウイルススキャンを確実に実施しましょう。

自宅で使うWi-Fiルータの注意点

Wi-Fiルータに欠陥がある場合や、管理用IDとパスワードが初期設定のままの場合、外部から不正アクセスされるおそれがあります。

対策

Wi-Fiルータのファームウェアは最新のものにアップデートし、IDやパスワードは推測されにくいものに今すぐ変更しましょう。

公共のWi-Fiスポットの注意点（1）

公共のWi-Fiスポットの中には、セキュリティが不十分なものがあり、通信内容を傍受されるおそれがあります。

対策

信頼できるVPNサービスを利用して、通信経路を暗号化しましょう。
重要な情報のやりとりはやめましょう。

公共のWi-Fiスポットの注意点（2）

悪意ある者が設置した、実在するSSIDと同じ名称とする偽のWi-Fiスポットに接続してしまい、情報を盗み見られるおそれがあります。

対策

偽の可能性を考慮し、たとえ漏えいしても支障のない情報に留める。

その他にも、
- 各種パスワードは使い回しを避け、長くて複雑なものにする。
- テレワークについての相談先を先に確認しておき、何かあれば対処する。
- 第三者の盗み見に注意する。
- 持ち出すコンピュータや資料にも注意する。

などがあります。

重要な情報や資産を守りながら、安全にテレワークを活用しましょう。