サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和2年
4月15日
Vol.41

テレワークのサイバーセキュリティ対策！

新型コロナウイルス感染拡大を受けテレワーク勤務が推奨されていますが、テレワークは、勤務先のセキュリティ環境とは異なる外部の環境から勤務先のシステムへアクセスするため、リスクが高まります。今回は、テレワークに関するセキュリティ対策ポイントの一部を掲載しています。

詳細については、総務省HP「テレワークセキュリティガイドライン」（https://www.soumu.go.jp/main_content/000545372.pdf）を確認の上、安全なテレワーク勤務を推進しましょう！

～身近に潜むテレワークを狙った脅威～

○　パソコンのOSやウイルス対策ソフトを更新しておらず、ウイルスに感染してしまう。

○　通信が暗号化されていないWi-Fiスポットを利用したことにより、通信内容を傍受されてしまう。

○　簡単なパスワードを使いまわしていたために、不正にアクセスされてしまう。

経営者・管理者が行うべき対策

○　テレワーク勤務を考慮した情報セキュリティーポリシーや、使用する端末・アプリケーションなどの利用ルールを見直す。

※　技術的対策（アクセス制御、暗号による管理など）

※　物理的対策（パソコンの管理、資料の暗号化・システムからの切り離しなど）

○　テレワーク勤務者に対し、教養を行ったり、自己啓発を促したりする。

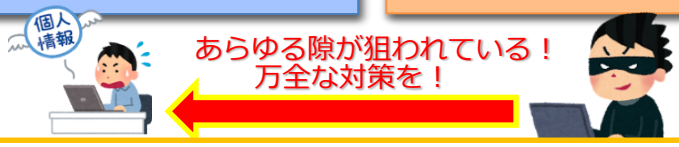
テレワーク勤務者が行うべき対策

○　OSやウイルス対策ソフトを最新状態に更新し、定期的にウイルスチェックを行う。

○　メールの開封やリンクのクリック等は一層の注意を払う。

○　公共の場のWi-Fiスポットを利用する際は、ファイル共有機能をオフにしたり、データを暗号化したりする。

○　自宅のWi-Fiルータを使用する場合は、必ず管理用ID・パスワードを初期設定から変更する。



相談窓口

愛媛県警察本部サイバー犯罪対策課　TEL089-934-0110㈹