サイバーセキュリティ岐阜

No.21 令和２年４月

岐阜県警察本部
サイバー犯罪対策課

「テレワーク」セキュリティは大丈夫？

セキュリティ対策を再確認！

自宅のパソコン等を使用してテレワークを実施する場合、サイバーセキュリティ対策を怠るとパソコンがウイルスに感染して業務が行えなくなることや、重要なデータが流出し、業務に大きな影響を与えることが考えられます。セキュリティ対策を再確認し、被害防止、被害拡大防止に努めましょう。

テレワークで使用するパソコン等

1　サポートが終了しているOSのパソコンを使用しない
2　ウイルス対策ソフトを必ず導入する
3　業務を始める前に、パソコン等のOS、ウイルス対策ソフト、アプリケーションから最新の状態か確認する
（修正プログラムを適用し、脆弱性を解消する）
4　テレワークで使用するパソコンは、自分以外使用させない
5　ファイル共有機能をオフにする
（公衆無線LAN等のネットワークでは他のパソコンからアクセスされる恐れがあります）

自宅のWi-Fiルータを使用する場合

1　ルータのファームウェアを最新にアップデートする
2　管理用IDとパスワードを購入したままの状態で使用しない
（自宅のWi-Fiが勝手に使われてしまう恐れがあります）

電子メールを利用する場合

1　受信したメールの送信者を確認する
2　受信したメールに添付されたWord等のマクロ機能を安易に起動しない
3　メール本文中のURLに安易にアクセスしない

その他

1　USBメモリ等の外部記録媒体は、テレワーク専用のものを使用する
2　勤務先のシステムへログインするときは、定められた手順・方法で行う

万全のセキュリティ対策で情報や資産を守り、安全にテレワークを活用しましょう!!