テレワークはココに注意!!

サイバーセキュリティ・ニュース
CS-NEWS

サイバー犯罪対策課
令和２年４月

テレワークが急速に普及する中、サイバーセキュリティ対策を怠ると、パソコン等のマルウェア（ウイルス）感染や重要なデータの流出などにより、業務に大きな影響が出ることが考えられます。

サイバーセキュリティ対策を万全にして、情報や資産を守りましょう。

使用するパソコン等（タブレット、スマートフォン）の注意点


ミーポくん

◇ サポートが終了しているＯＳを使用しない
◇ ウイルス対策ソフトを導入する
◇ 業務開始前に〈パソコン等のＯＳ〉〈ウイルス対策ソフト〉〈アプリケーション〉が最新の状態か確認する
◇ テレワークで使用するパソコン等を他人に使用させない
◇ 必要のないファイル共有機能をオフにしておく
◇ 必要があるとき以外は、テレワークで使用するパソコン等をインターネットに接続しない

パスワードの設定・管理についての注意点

◆ 他人に推測されにくい複雑なパスワードを設定する
◆ 他のサービスで設定しているパスワードを使い回さない
◆ パスワードを入力したメモ等をパソコン本体に保存しない

自宅のWi-Fiルータを使用する場合の注意点

★ ファームウェア（Wi-Fiルータ本体を制御するためのソフトウェア）を最新のものにアップデートする
★ 管理用のパスワードを購入したままの状態で使用しない

電子メールを利用する場合の注意点

☆ メールの内容や言葉遣い等に不自然な点があれば差出人に電話等で直接確認する
☆ 安全が確認できなければ、添付ファイルを開かない
☆ 添付ファイル開封時に「コンテンツの有効化」「マクロを有効にする」などと表示されても不用意にクリックしない
☆ メール本文中のリンク（クリックすると他のページに移動する文字など）は不用意にクリックしない

その他

○ 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
○ 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


ミーポくん

※ 今回紹介したのは、テレワークにおけるサイバーセキュリティ対策の一部です。
このほかにも、テレワークの種類（方式）に応じた対策を講じる必要があります。