

テレワーク勤務のサイバーセキュリティ対策

新型コロナウイルスの感染拡大を受け、テレワークが注目を集めています。

必要なセキュリティ対策を怠ればマルウェアに感染したり、情報漏洩が発生するなど業務に大きな影響を与えることが予想されます。

以下の点に注意しながら万全のセキュリティ対策であなたやあなたの会社の大事な情報を守りましょう！

注意すべきポイント！

- ◎ テレワークで使用するパソコン等（タブレット、スマートフォン）
 - 毎日の業務開始前に、使用するパソコン等のOS、ウィルス対策ソフト、アプリケーションを最新状態にする
 - データを暗号化して保存する
 - ファイル共有機能をオフにする
- ◎ パスワード
 - テレワーク専用のものを作成する
 - 他人に推測されにくい複雑なものを作成する
- ◎ 自宅Wi-Fiルータ
 - ファームウェアを最新の状態にアップデートする
 - IDとパスワードを初期のまま使用しない
- ◎ Wi-Fiスポット（公衆無線LAN）
 - 偽のWi-Fiスポットに注意
 - セキュリティが不十分な公衆無線LANで重要な情報のやり取りをしない
- ◎ 電子メール
 - Wordファイル等のマクロ機能を安易に起動しない
 - 取引先から身に覚えのないメールが送られてきたら、電話で確認

マルウェアって？

あなたのパソコンに入り込み不正かつ有害な動作を行わせるものだよ

どんな被害があるの？

パソコン等からあなたの大切な個人情報や、会社の重要な顧客情報などを抜き取ったり、勝手に外部に送って流出させるよ

