ちょっと待って！

そのテレワーク、セキュリティは大丈夫？

テレワーク＝**時間や場所の有効活用**。でも、サイバー空間には悪意ある犯罪者がたくさん。
テレワーク環境＝コンピュータやインターネットの**セキュリティ対策**をしていますか？

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。

―― 利用するコンピュータのOSやウイルス対策ソフトは常に最新の状態に更新し、必ず利用前及び定期的にウイルススキャンを実施しましょう。

カフェ等のWi-Fiスポットはセキュリティが十分でないものもあり、通信内容を傍受されるおそれがあります。

―― 不特定多数が接続できるWi-Fiスポット（＝公衆無線LAN）は、通信が暗号化されていないものやパスワードが公開されているものなど、そのセキュリティレベルはさまざま。
利用時はファイル共有機能をオフにし、通信経路を暗号化（VPN）するとき以外は、たとえ漏えいしても支障のない情報だけのやりとりに留めましょう。

自宅のWi-Fiルータの管理用IDとパスワード。初期設定のままだとコンピュータ内に侵入されるおそれがあります。

―― そもそも変更した覚えがない…そんな方はルータの管理画面で要確認。
「admin」や「password」等のありがちな初期設定になっていたら危険です。
他人に推測されにくいものに今すぐ変更しましょう。

その他にも・・・

- ☞ 各種パスワードは使い回しを避け、一定以上の長さで他人に推測されにくいものにする。
- ☞ 公共の場では覗き見や盗難のリスクを考え、長時間離席しない、壁際の席に座るなどの配慮をする。
- ☞ テレワークについての相談先を事前に確認しておき、不安なことがあればすぐに対処する。

etc…

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。

警視庁サイバーセキュリティ対策本部