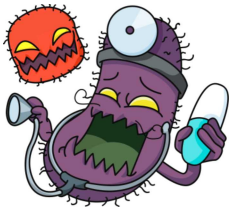
テレワークにおけるセキュリティ対策

現在、新型コロナウイルス感染症の影響から、テレワークが注目されています。
しかし、様々な場所で会社の情報を取り扱うことが出来るようになると、そのセキュリティの脆弱性を狙った攻撃者の標的や、ウイルス感染などによる情報漏えいのきっかけになってしまうこともあります。

☆　テレワーク時の具体的セキュリティ対策

○　コンピュータウイルスへの感染を防ぐ対策をしましょう。



利用するパソコンのOSやウイルス対策ソフトは、常に最新の状態に更新してから、作業を実施しましょう。
悪意のあるメールによってウイルスなどに感染しないように、メール閲覧、添付ファイルの開封やメールに記載されているリンクをクリックする際は十分に注意しましょう。
また、機密性の高い情報を取り扱う際には、暗号化して保存するなどの対策も検討しましょう。

○　公衆無線LANは安全なアクセスポイントを利用しましょう。

不特定多数が接続できるWi-Fiスポットは、通信が暗号化されていないなどセキュリティ対策が十分でないものや、盗聴を目的としたなりすましWi-Fiスポットなどの危険なものもあります。
利用する際は、SMS連携方式、SNSアカウントを利用した認証方式、メール認証方式などの利用者認証をしているなど、公衆無線LANのセキュリティ対策が確実に行われているものを利用しましょう。

○　職場のセキュリティポリシーに従った利用をしましょう。

個人のパソコン等をテレワークに用いる場合は、会社から許可されたソフトウェアのみの使用を心掛け、コンピュータウイルス感染や不正アクセスによる情報漏えい等の被害に遭わないように注意しましょう。

○　その他にも・・・

テレワークで使用するパスワードは使い回しを避けて、一定以上の長さ、複雑さで他人に推測されにくいものにしましょう。
ファイル共有サービスなどのクラウドサービスを利用する場合は、会社のルールなどで認められた範囲で利用しましょう。

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利用しましょう。

【参考】
総務省「テレワークセキュリティガイドライン(第４版)」「テレワークセキュリティガイドライン(第４版)におけるセキュリティ対策のポイント」
https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000200.html
国民のための情報セキュリティサイト　「Wi-Fi(無線LAN)の安全な利用について」
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html
情報セキュリティ・ポータルサイト(管理者:独立行政法人 情報処理推進機構)「気をつけたい、テレワーク時のセキュリティ７つの落とし穴(LAC)」
https://www.ipa.go.jp/security/kokokara/study/company.html#telework

福島県警察本部生活安全部生活環境課
サイバー犯罪対策室
情報提供メール：fp-hitec@police.pref.fukushima.jp

福島県警サイバー
防犯キャラクター
ダ メ ポ チ く ん