

【F-CSNET 通信かわら版】

【表題：テレワークにおけるサイバーセキュリティ対策】

中小事業者の皆様へ

新型コロナウイルス感染症の拡大による緊急事態宣言の対象地域に福岡県が追加されるに伴い、テレワークの再開・拡大を検討されている事業者の皆様へ、テレワークにおけるサイバーセキュリティ対策についてご案内します。

- 1 情報セキュリティの基本（5か条） ～テレワーク時でも必ず実施を
 - ① OSやソフトウェアは常に最新の状態にしよう！
 - ② ウイルス対策ソフトを導入しよう！
 - ③ パスワードを強化しよう！
 - ④ 共有設定を見直そう！
 - ⑤ 脅威や攻撃の手口を知ろう！

- 2 テレワークを始める前に実施すること
 - テレワークで使用するパソコン等について、家族等との共用パソコンを使用する際は業務用のユーザアカウントを別途作成する（テレワーク専用のパソコンが理想）
 - Web会議などのサービスを利用する際は、事前に初期設定の内容を確認し、セキュリティ機能を積極活用する

- 3 テレワークを行う場所は？
 - 自宅の場合
 - ・ 自宅ルータの管理者パスワードは初期設定（工場出荷時）から確実に変更する
 - ・ 自宅のルータは、メーカーのサイトを確認のうえ、ソフトウェアを更新するなど最新の状態を保つ
 - 公共の場で行う場合
 - ・ パソコンの画面を覗かれない（盗み見られない）ように注意
 - ・ Web会議を行う際は内容を聞かれないように注意
 - ・ 公衆Wi-Fi利用時は、パソコンのファイル共有機能をOFFにする
 - ・ 公衆Wi-Fi利用時は、必要に応じてVPNサービスを利用する
 - ・ パソコンだけではなく、紙媒体の取り扱いにも注意を

参考URL（独立行政法人情報処理推進機構HP）

<https://www.ipa.go.jp/files/000055516.pdf>

<https://www.ipa.go.jp/security/announce/telework.html>

- ★ F-CSNET は、公的機関（九州経済産業局地域経済部情報政策課、福岡県警察本部生活安全部サイバー犯罪対策課、福岡県商工部中小企業振興課）と、4つの中小事業者支援団体とが連携し、県内中小事業者を対象に、サイバー犯罪の被害防止等に的確に対応することを目的として発足したネットワークです。
- ★ 福岡県警察サイバー犯罪対策課では、随時情報をホームページに掲載していますので、是非ご覧ください。

<https://www.police.pref.fukuoka.jp/seian/cyber/index.html>