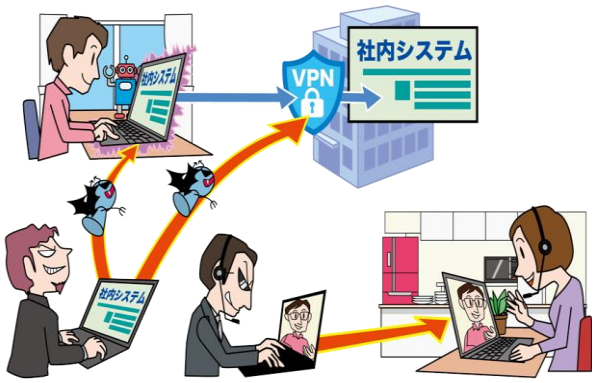
セキュリティ対策を講じて、安全にテレワークを

テレワーク（telework）とは ICT（情報通信技術）を活用した時間や場所にとらわれない柔軟な働き方の意味で、「tele（離れた所）」と「work（働く）」を組み合わせた造語です。新型コロナウイルス感染症の世界的な蔓延により、テレワーク等の新しい働き方が注目されています。テレワークは政府が推進する働き方改革の重要な取組のひとつにもなっていますが、このような働き方の変化に伴い、テレワーク用PCのウイルス感染に伴う情報の流出、通信内容の盗み見、Wi-Fiルータの不正利用など様々な問題が発生する可能性があります。安全にテレワークを活用するためには、**PCやインターネットのセキュリティ対策を講じること**が重要です。

○ **テレワークを活用する際のリスク**

- 使用している端末のウイルス感染
- ウイルス感染に伴う情報の流出
- キーロガー（キーボードで入力した文字を記録する悪意のあるプログラム）による通信内容の盗み見
- 通信が暗号化されていないことによる通信内容の盗み見
- フリーWi-Fi の利用に伴う通信内容の盗み見
- 自宅 Wi-Fi ルーターの管理用IDとパスワードが初期設定から変更されていないことによる外部からの不正利用



（出典　IPA 独立行政法人情報処理推進機構）

対策

- **ウイルス対策の徹底**
  OS、ソフトウェア及びウイルス対策ソフトは、アップデートにより、最新の状態を保つ。
- **不特定多数の人が利用する端末でテレワークをしない**
  インターネットカフェや公共の場所に設置されているコンピュータなど、不特定多数の人が利用する端末では、キーロガー等の悪意のあるプログラムにより通信内容が盗み見られることがあるため、テレワークでは不特定多数の人が利用する端末を利用しない。
- **VPNサービスの利用**
  VPNサービスを利用することにより、通信を暗号化し、情報の盗み見を防止する。
  ※　VPN製品の脆弱性を悪用されないようにするため、更新プログラムは確実に適用する。
- **フリーWi-Fi を利用する際のセキュリティ対策の徹底**
  暗号化されているフリーWi-Fi を利用することや、データが暗号化されている「https」で URL が始まるサイトにアクセスする。また、なりすましアクセスポイントへの接続を避けるため、Wi-Fi の自動接続設定を OFF にする。
- **自宅 Wi-Fi ルーターの不正利用対策の徹底**
  ファームウェア（内蔵されている制御のためのソフトウェア）を最新のものにアップデートするとともに、管理用IDとパスワードを変更する。また、WEPやWPAの暗号化方式は、解読されるおそれがあるため使わない。

岩手県警察本部サイバー犯罪対策課の公式ツイッターは QR コードから！！サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための情報をお知らせしています。

@Iwate_cyber

岩手県警察本部生活安全部サイバー犯罪対策課

令和3年7月1日発行