青い森のサイバーセキュリティ

令和２年６月
青森県警察本部保安課
サイバー犯罪対策室

テレワーク時はセキュリティ意識を高く

公衆無線ＬＡＮ(Wi-Fi)の利用はなるべく避ける

公衆無線ＬＡＮ(Wi-Fi)は通信内容が盗み見られる可能性があります。暗号化通信(SSL-VPN等)の利用や会社貸与のモバイルルーターの利用など、信頼のおける手段を確保しましょう。

私物端末利用(BYOD)時はウイルス対策意識を強く持とう

私物の端末は業務端末に比べセキュリティ対策が不足していることが多いものです。ウイルスによる業務資料やビデオ会議画面の盗み見、踏み台にされたことによる会社への不正侵入などを防ぐため、「業務中は不必要なウェブを見ない」「業務にも使う端末は会社のセキュリティポリシーに合わせる」「ＯＳやアプリケーションはこまめにアップデートする」など、利用者としてのセキュリティ意識を高めましょう。

【業務管理者側の対策】

テレワークで業務を始めるためには、セキュリティの確保に関する事前準備が必要です。オンライン会議ツール（ビデオ会議、グループ通話、メーリングリストなど）、データ共有方式（クラウドストレージ、社内サーバなど）、スケジュール管理ツール（グループウェアなど）等、業務ツールとして何を使うかを十分検討し、それに合わせた対策を行って下さい。