CYBER SECURITY NEWS
栃木県警察
サイバー対策センター
令和８年４月

連休前後のセキュリティ対策

長期休暇中は、監視体制が手薄になりやすく、サイバー攻撃者にとって「狙いやすい時期」になります。
今一度、基本的なセキュリティ対策の徹底をお願いします。

連休前

① 緊急連絡体制の確保
不測の事態に備えて、委託先を含めた緊急連絡体制や対応手順を確認する。

② ソフトウェアの脆弱性対策
各種IT機器が最新のファームウェアに更新されているか確認する。

③ アクセス制御の確認
アクセス権限の確認、多要素認証の利用、パスワードが単純でないか確認する。

④ バックアップの取得
重要データ、機器設定ファイルのバックアップを取得するとともに、バックアップデータはネットワークから切り離す。

⑤ 使用しない機器は電源OFF
不正アクセス等防止のため、休暇中使用しない機器の電源は落とす。

連休後

① 修正プログラムの確認
休暇中にOSやソフトウェアの修正プログラムが公開されていないか確認する。

② 定義ファイルの更新
メールの送受信、ウェブサイトの閲覧前にセキュリティソフトの定義ファイルを更新する。

③ 各種ログの確認
サーバ等の機器に不審なアクセスがないか確認する。

④ 持ち出した機器のウイルスチェック
組織内で利用する前にセキュリティソフトでウイルススキャンの実施をする。

⑤ 不審なメールに注意
休暇明けはメールが溜まっている場合が多く、不用意に添付ファイルは開かず、本文中のURLはクリックしないなど特に注意を払う。