茨城県警察からのお知らせ　　令和８年８月７日

サイバーセキュリティ対策に関する情報提供について

長期休暇前後のサイバーセキュリティ対策に関する注意喚起をお送りします。

長期休暇の時期は、システム担当者や管理者が長期間不在になる場合も多く、いつもとは違う状況になりがちです。このような状況でセキュリティインシデントが発生した場合は、対応が遅れたり想定していなかった事象へと発展する等、思わぬ被害が発生します。

最近では、インターネットに接続された機器・装置類の脆弱性を悪用する攻撃が相次いでいます。また、それにより不正な通信の中継点とされてしまう可能性もあります。

攻撃を受けた場合、保有情報の漏洩や改ざん、ランサムウェアへの感染に加え、意図せずに他組織等への攻撃に加担することにも繋がります。

長期休暇の前後に講ずるべき対策をまとめましたので、以下の対応を検討してください。

１．長期休暇前

〇対処手順や連絡体制の確認

休暇中にインシデントが発生した場合に備え、委託先企業を含めた緊急連絡体制や対処手順を再確認しておきましょう。

〇使用しない機器の電源 OFF

・長期休暇中に使用しないサーバ等の機器は電源を OFF にしましょう。

・電源を切っていたパソコンは、セキュリティソフトの定義ファイル（パターンファイル）が古い状態のままになっています。電子メールやウェブサイトの閲覧をする前に定義ファイルを更新しましょう。

〇バックアップの取得

重要データのバックアップを取得し、必要な場合にはバックアップからの復元が可能なことを確認しておくことが重要です。また、バックアップデータの保管場所についても検討し、ネットワークから切り離した安全な場所に保存するようにしましょう。

〇アクセス制御

・アクセス権限が適切か、不要なアカウントがないか確認しましょう。

・VPN 等、外部からアクセス可能な機器の設定も確認しましょう。

〇ソフトウェアの脆弱性対策

・ソフトウェアのセキュリティパッチ適用やバージョンアップなど、脆弱性への対策を実施しましょう。

・休暇中に脆弱性が発表された場合の対応についても決めておきましょう。

〇利用機器に関する対策

・IT 機器のファームウェアを更新し、脆弱性への対策を実施しましょう。

・休暇中に使用しない機器は、シャットダウンして不正アクセスやマルウェア感染などのリスクを軽減しましょう。

２．長期休暇後

〇メールへの対処

不正なリンクや添付ファイルを含むメールに注意する必要があります。特に、送信元が不審なメールについては開封せず、報告して組織内で情報共有をしましょう。

３．その他

詳細は下記の URL から、IPA（独立行政法人情報処理推進機構）が掲示している「2026 年度夏休みにおける情報セキュリティに関する注意喚起」をご確認ください。

https://www.ipa.go.jp/security/anshin/heads-up/alert20260730.html

【本件の問合せ先】
茨城県警察本部サイバー企画課
電話：029-301-0110