サイバー攻撃対策通信
（令和７年第８号）

令和７年8月4日

福岡県警察本部

夏季長期休暇におけるセキュリティ対策

長期休暇中、システム管理者不在の状況でセキュリティインシデントが発生した場合、対応の遅れや予想外の事象への発展により、業務継続に影響が及ぶ可能性があります。
このような事態とならないよう、**長期休暇の前後に以下の対策を実施**しましょう。

休暇前の対策

管理者向け

- **緊急連絡体制の確保**
  委託先企業を含めた緊急連絡体制や対応手順等が明確になっているか確認しましょう。
- **社内ネットワークへの機器接続ルールの確認と遵守**
  休暇中にメンテナンス作業等で社内ネットワークへ機器を接続する予定がある場合は社内の機器接続ルールを事前に確認し遵守しましょう。
- **使用しない機器の電源OFF**
  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。

利用者向け

- **機器やデータの持ち出しルールの確認と遵守**
  - 休暇中に社外での対応が必要となるPC等の機器やデータ等の情報を持ち出す際は、ルールを事前に確認し遵守しましょう。
  - 持ち出した機器やデータは、ウイルス感染や紛失、盗難等によって情報漏えい等の被害が発生しないよう管理しましょう。
- **使用しない機器の電源OFF**
  休暇中に使用しない機器は、電源をOFFにしましょう。

休暇後の対策

管理者向け

- **修正プログラムの適用**
  休暇中にOSや各種ソフトウェアの修正プログラムが公開されていないかを確認し、必要な修正プログラムを適用しましょう。
- **定義ファイルの更新**
  電子メールの送受信やWebサイトの閲覧等を行う前に、セキュリティソフトの定義ファイルを更新し、最新の状態にしましょう。
- **サーバ等における各種ログの確認**
  サーバ等の機器に対する不審なアクセスが発生していないか、各種ログを確認しましょう。

利用者向け

- **修正プログラムの適用**
  休暇中にOSや各種ソフトウェアの修正プログラムが公開されていないかを確認し、システム担当者の指示に従い、必要な修正プログラムを適用しましょう。
- **定義ファイルの更新**
  電子メールの送受信やWebサイトの閲覧等を行う前に、セキュリティソフトの定義ファイルを更新し、最新の状態にしましょう。
- **持ち出した機器等のウイルスチェック**
  休暇中に持ち出していたPCや外部記録媒体にウイルスが混入していないか、会社内で利用する前にセキュリティソフトでスキャンを行いましょう。
- **不審なメールの確認**
  休暇明けはメールが溜まっていることが想定されますので、特に注意してメールチェックを行いましょう。

【参照/IPA】https://www.ipa.go.jp/security/anshin/heads-up/alert20250801.html

福岡県警察サイバー攻撃対策隊（公安第一課第七係）電話番号：092-641-4141（内線：5986）