



サイバーセキュリティ対策通信

大阪府警察本部サイバーセキュリティ対策課

令和8年版 長期休暇に向けて、セキュリティ対策は万全ですか？

セキュリティ対策責任者・システム担当者向け

休暇前 対処手順・連絡体制

重要

- 万が一の事態に備えて、委託先を含めた**緊急連絡体制**を最新にする。
- インシデント発生時の具体的な**対処手順**を確認する。

長期休暇期間中に認知したインシデントの対応が休暇明けとなり、被害が拡大した事例も！

休暇前 休暇後 バックアップ

重要

- ランサムウェアによるデータ全滅を防ぐため、重要データの**バックアップは必ずネットワーク**から切り離して**保管**する。
- バックアップから**正常に復元できるか**を一部だけでもテストする。

ランサムウェア攻撃により、大切なバックアップも暗号化されてしまう被害が出ています！

休暇前 休暇後 アクセス制御

- アクセス権限の確認、利用者にパスワードが単純でないかの確認、パスキーなどの**フィッシング耐性のある多要素認証**へ移行、不要なアカウントの削除等により、**本人認証を強化**する。
- 外部ネットワークからアクセス可能な**機器へのアクセスは必要なものに限定**する。

休暇前 休暇後 機器・ソフトウェアの脆弱性対策

- 機器（**VPN**、サーバ、パソコン等、防犯カメラ等）を**必ず最新の状態にアップデート**する。
- 休暇中に公表された**重要な脆弱性情報に対応するための体制を整える**。
- 使用しない機器の**電源を落とし**、不要な外部接続は無効化する。

休暇後 電源を落としていた機器・持ち出した機器に関する対応

- 休暇中に電源を落としていた機器は、端末起動後、**最初に不正プログラム対策ソフトウェア等の定義ファイルを確認し、最新の状態に更新**してから、利用を開始する。
- 持ち出しが行われていたパソコン等が、不正プログラムに感染していないか確認する。

休暇前 休暇後 各種ログの確認

- **不審なアクセス**がないか、VPN、ファイアウォール、監視装置等ログやアラートで確認する。
- 不審なログが記録されていた場合は、早急に**保全して**詳細な調査等を行う。

情報システム利用職員向け

休暇前 機器やデータの持ち出しルールの確認と遵守

- 端末や外部記録媒体等の持ち出しは、**組織内の安全基準等に則った適切な対応**を徹底する。
- 持ち出した機器の**不正プログラム感染や、紛失、盗難による情報漏えい等の被害が発生しないように管理**する。

休暇前 使用しない機器の電源オフ

- 不正アクセスを防止するため、休暇中に使用しない機器の**電源を落とす**。

休暇前 休暇後 巧妙ななりすましへの対策

- **生成AIを利用した上司等へのなりすまし**に警戒し、不審なメールや金銭要求には**別の電話等で本人確認**を行うルールを設定しておく。

休暇前 休暇後 ソフトウェアの脆弱性対策

- 業務を始める前に、脆弱性情報を確認し、必要に応じて**セキュリティパッチの適用や各種ソフトウェアのバージョンアップ**を行う。
- 直ちに実施することが困難な場合は、リスク緩和策を講じる。

休暇後 不正プログラム感染の確認

- 休暇中に持ち出しが行われていたパソコン等が不正プログラムに感染していないか、**最新に更新した不正プログラム対策ソフトウェア等で確認**する。

休暇前 休暇後 電子メール

- **不審な添付ファイルを開いたり、リンク先にアクセスしたりしない**。
- 不審な点があれば、電子メールを開封する前に、**電話等、別の手段で確認**する。



大阪府警察ウェブサイト

その他サイバー犯罪対策に関する事は
大阪府警察のウェブサイトやXを確認ください



大阪府警察サイバーセキュリティ対策情報 X