# サイバー防犯通信

https://www.police.pref.hyogo.lg.jp/cyber/

令和７年３５号

兵庫県警察サイバーセンター
サイバー情報発信室

# 長期休暇に向けた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

### 対処手順・連絡体制

休暇前 重要

・ 不測の事態の発生に備えて、緊急連絡体制や対処手順等が明確になっているか確認する。

・ 連絡フローが現在の組織体制に沿っているか。
・ 各担当者の電話番号は変わっていないか　etc.

休暇中にインシデントを認知したが対応が休暇明けとなり、被害が拡大した事例も…

### バックアップ

休暇前 休暇後 重要

・ 重要なデータや機器設定ファイルに対するバックアップ対策を実施する。
・ バックアップデータは、ネットワークから切り離し、変更不可とするなどの対策を検討する。

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も…

### アクセス制御

休暇前 休暇後

・ アクセス制限の確認、多要素認証の利用不要なアカウントの削除等により本人認証を強化する。
・ 利用者にパスワードが単純ではないか確認させる。
・ 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。

### ソフトウェアの脆弱性対策

休暇前

・ 脆弱性対策の状況を確認し、必要に応じてセキュリティパッチの適応やソフトウェアのバージョンアップを行う。
・ 長期休暇期間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。

### 利用機器に関する対策

休暇前

・ 機器（サーバ、パソコン等、通信回線装置、特定用途機器（防犯カメラ等）等）のファームウェアを最新にアップデートする。
・ 長期休暇期間中に使用しない機器の電源を落とす。

### 電源を落としていた機器に対する対策

休暇後

・ 長期休暇期間中に電源を落としていた機器は、端末起動後、一番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する。
・ 最新の状態になっていない場合は、更新してから利用を開始する。

### ソフトウェアの脆弱性対策

休暇後

・ 長期休暇期間中における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応や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。

### 不正プログラム感染の確認

休暇後

・ 長期休暇期間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、不正プログラム対策ソフトウェア等で確認する。

### 各種ログの確認

休暇前 休暇後

・ サーバ等の機器に対する不審なアクセスがないか、VPN、ファイアーウォール、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、早急に詳細な調査等を行う。

## 情報システム利用職員向け

### 機器やデータの持ち出しルールの確認と遵守

休暇前 休暇後

・ 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（持ち出し・持ち込みに関する内規の遵守等）を徹底する。
・ 持ち出し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。

### 利用機器に関する対策

休暇前

・ 不正アクセスを防止するため、長期休暇期間中に使用しない機器の電源を落とす。

### 電子メール

休暇前 休暇後

・ 電子メールを確認する前に利用機器のOS・アプリケーションに対する修正プログラムの適応や不正プログラム対策ソフトウェア等の定義ファイルの更新等を実施する。
・ 不審な添付ファイルを開いたり、リンク先にアクセスしない。
・ 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。

## サイバーセンター公式「X」(旧Twitter)

兵庫県警察サイバーセンターではX（旧Twitter）で、サイバー犯罪やサイバーセキュリティの情報をいちはやくお届けしています。

https://x.com/HPP_c3division