# サイバーニュース

H31年第4号
奈良県警察本部
サイバー犯罪対策課

## 長期休暇におけるセキュリティ対策【企業編】

ゴールデンウイークや年末年始などの長期休暇の時期は、システム管理者が不在になることも多いため、ウイルス感染や不正アクセス等のトラブルが発生した場合に対処が遅れていまい、被害が拡大する恐れがあります。
このような事態とならないよう、以下の対策を実施することが重要です。

### 長期休暇の「前」の対策

✓ ソフトウェアを最新の状態に！

休暇中や休暇明けのリスクを軽減することができますので、OS・ウイルス対策ソフトウェア・インストールプログラムを更新し、最新の状態にしましょう！


✓ 緊急連絡体制の確認！

万が一、トラブルが発生した場合に備えて、代理担当者や保守委託先企業を含めた、緊急連絡体制や対応手順を再確認しておきましょう！

✓ 不必要な機器等の停止！

外部からの攻撃を受けるリスクを軽減するため、休暇中使用しないパソコンやサーバ等の機器は電源をOFFにし、サーバの不必要なサービスは停止しておきましょう！


✓ データのバックアップ！

システムの不具合やランサムウェア等のウイルスによるデータ破壊に備えて、社内の重要なデータについては、外部記録媒体等へバックアップを行いましょう！

### 長期休暇の「後」の対策

✓ ソフトウェアの更新！

休暇中に修正プログラムや定義ファイルが公開されている場合がありますので、ウェブサイトの閲覧等を行う前に、OS・ウイルス対策ソフトウェア・インストールプログラムを更新しましょう！

✓ 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。不審なログが記録されていた場合は、早急に調査を行うことが重要です。

✓ ウイルスのチェック！

長期休暇中に持ち出していたパソコンや各種デバイスについては、ウイルスチェックを行い、安全を確認してから使用しましょう。


✓ 不審なメールに注意！

休暇明けには、休暇中に受信したメールが大量に溜まっていることが想定できます。誤って不審なメールの添付ファイルを開くことがないよう注意しましょう！


連休前後は、業務も忙しくふとしたミスが大きなセキュリティ事故に繋がる可能性があります。特に連休後のメールの確認では、うっかり添付ファイルを開いてしまうとウイルスに感染し、情報を窃取される恐れがあります。また、メールに記載のURLをクリックするとフィッシングサイト等に誘導される恐れもあります。

**不審なメールの添付ファイルなどは絶対に開かないよう注意してください!!**

【参考】独立行政法人情報処理推進機構IPA「長期休暇における情報セキュリティ対策」
https://www.ipa.go.jp/security/measures/vacation.html