

大型連休に向けて、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

- 長期休暇期間中の**監視体制**を確認する。
- 必要に応じ、システムアラート等の監視体制を強化する。
- セキュリティインシデントの**対処手順**を確認し、**連絡体制を更新**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

バックアップ°

重要

休暇後

- 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**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が出ています！

休暇前

休暇後

各種脆弱性対策

- 利用中の**ソフトウェア**や**機器等**の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用**や**バージョンアップ**を行う。
- 長期休暇期間中に公表された脆弱性情報を確認し、必要に応じて対応する。

休暇後

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**がないか、VPN、ファイアウォール、監視装置等の**ログやアラートを確認**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

休暇前

休暇後

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**（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

休暇後

電子メール

- 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用**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。

埼玉県警察本部サイバー局サイバー対策課
S.P.P Cyber Bureau Cybercrime Countermeasures Division

緊急時はこちら！

最寄りの警察署又は全国统一サイバー犯罪メール相談窓口

<https://www.npa.go.jp/bureau/cyber/soudan.html>

