S.P.P Cyber Bureau
Cybercrime
Countermeasures Division

埼玉県警察
サイバーセキュリティレポート

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

対処手順・連絡体制

休暇前

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！

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！

各種脆弱性対策

休暇前
休暇後

- 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。

各種ログの確認

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

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。

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。