令和5年 Vol.6

Ksisnetだより

Ksisnet
Kyoto Small and Medium Enterprises Information Security Support Network
京都中小企業情報セキュリティ支援ネットワーク

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】

- 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が出ています！

休暇前 アクセス制御

- アクセス権限の確認、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。

休暇前 ソフトウェアの脆弱性対策

- 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。

休暇前 利用機器に関する対策

- 機器（サーバ、パソコン等、通信回線装置、特定用途機器（防犯カメラなど）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。

休暇後 電源を落としていた機器に関する対応

- 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、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。

休暇後 ソフトウェアの脆弱性対策

- 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用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。

休暇後 不正プログラム感染の確認

- 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。

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

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（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 利用機器に関する対策

- 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。

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。

京都の事業者 Incident Zero

Twitter（京都府警察サイバーセンター公式ツイッター）

京都府警察では、「京都府警察サイバーセンター（@KPP_cyber）」のTwitterアカウントで、サイバー犯罪被害防止に関する等の情報発信を行っています。