

長期休暇における情報セキュリティ対策

長期休暇の時期は、システム管理者の長期不在等、いつもとは違う状況になりやすく、セキュリティインシデント発生時の対応の遅れや想定していなかった事象への発展等が懸念されるため、以下の点に注意して被害を未然に防止しましょう。

システム管理者・担当者向け

休暇前 対処手順・緊急連絡体制

- セキュリティインシデントの**対応手順を確認し、連絡体制を確認**する。
- 各担当者の連絡先の見直しをする。

休暇前 機器接続ルールの確認

- メンテナンス作業等で、社内ネットワークへ機器を接続する場合は、**社内の機器接続ルールを確認**する。

休暇前 利用機器に関する対策

- 不正アクセス等を防止するため、長期休暇中に**使用しない機器の電源を落とす**。

休暇後 修正プログラムの更新

- 長期休暇中のオペレーティングシステムや各種ソフトウェアの**修正プログラムの有無を確認し、必要な場合は適用**する。

休暇後 定義ファイルの更新

- 長期休暇中に電源を落としていた機器は、**セキュリティソフトの定義ファイルを最新の状態**にしてから利用を開始する。

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、**各種ログを確認**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。

情報システム利用者向け

休暇前 機器やデータの持ち出しルールの確認と遵守

- 端末やデータ等の情報を持ち出す場合は、**組織内の持ち出しルールを事前に確認**する。

休暇前 利用機器に関する対策

- 不正アクセス等を防止するため、長期休暇中に**使用しない機器の電源を落とす**。

休暇中 機器やデータの厳重な管理

- 自宅等に持ち出したパソコン等の機器やデータはウイルス感染や紛失、盗難等による**情報漏えい等の被害が発生しないよう、厳重に管理**する。

休暇後 修正プログラムの更新

- 長期休暇中のオペレーティングシステムや各種ソフトウェアの**修正プログラムの有無を確認し、必要な場合は適用**する。

休暇後 定義ファイルの更新

- 長期休暇中に電源を落としていた機器は、**セキュリティソフトの定義ファイルを最新の状態**にしてから利用を開始する。

休暇後 ウイルスチェック

- 長期休暇中に持ち出していたパソコンや外部記録媒体等に**ウイルスが混入していないか、組織内で利用する前にセキュリティソフトでウイルススキャン**を行う。

休暇後 不審なメールに注意

- 長期休暇明けはメールが溜まっていることが想定されるため、より注意してメールチェックを行い、**不審な添付ファイルを開いたり、本文中のURLにアクセスしたりしない**。

