


長期休暇前後のサイバーセキュリティは ココに注意!!



年末年始などの**長期休暇の時期**は、企業・組織のシステム管理者が不在となることが多く、**セキュリティに関する問題が発生した場合の対応が遅れ、被害が拡大する可能性があります。**

長期休暇前と**長期休暇後**の基本的なサイバーセキュリティ対策を徹底しましょう。

長期休暇前の対策

企業・組織のシステム管理者の対策

- ☆ セキュリティ問題発生時の**連絡体制**や**対応手順**を確認しておく
- ☆ **重要なデータはバックアップ**しておき、**ネットワークから切り離して保管**しておく



社員・職員の対策

- ◇ セキュリティ問題発生時の**連絡先**を確認しておく
- ◇ 業務で使用する機器(パソコン、スマートフォンなど)やデータを**社外に持ち出す場合は、ルールを確認、遵守**する



共通の対策

- ◎ 業務で使用する機器
 - ▷ OSやソフトウェアを**最新の状態**にしておく
 - ▷ ウイルス対策ソフトの**定義ファイル**を**最新の状態**にしておく
- ◎ 休暇中に**使用しない機器の電源**を切っておく

長期休暇後の対策

企業・組織のシステム管理者の対策

- ☆ 休暇中のサーバへの**不審なアクセスの有無**などについて**各種ログを確認**する
- ☆ Webサーバで公開している**コンテンツの改ざんの有無**を確認する



社員・職員の対策

- ◇ 持ち出していた**機器やUSBメモリなどのウイルスチェック**を実施する
- ◇ 休暇中にたまったメールは、**不審なメールに注意**し、安易に添付ファイルを開いたり、リンク先にアクセスせず、**内容をよく確認**する



共通の対策

- ◎ 休暇中に**使用していなかった機器**
 - ▷ OSやソフトウェアを**最新の状態**にする
 - ▷ **ウイルス対策ソフトの定義ファイル**を**最新の状態**にする

