サイバーセキュリティパートナーシップだより

R7-29

年末年始のセキュリティ対策

長期休暇の時期は、システム管理者が長期不在になるなど、いつもと違う状況になりやすく、セキュリティインシデントが発生した場合は、対応に遅れが生じたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生し、長期休暇後の業務継続に影響が及ぶ可能性があります。このような事態にならないよう、以下の対策を実施してください。

企業や組織向けチェックリスト

システムを管理する方へ

休暇前

☑ **緊急連絡体制の確認**
→ 連絡フローが現在の体制になっているか
担当者の電話番号が変わっていないか

☑ **社内ネットワークへの機器接続ルールの確認と厳守**
→ パソコンや外部記録媒体をネットワークに接続する前に確認を

☑ **使用しない機器の電源ＯＦＦ**
→ サーバやルーターなど、侵入経路となり得る機器は電源ＯＦＦ

休暇明け

☑ **修正プログラムの適用**
→ ＯＳや各種ソフトウェアの必要な更新

☑ **セキュリティソフトの定義ファイルを最新のものに更新**
→ 社員がメールの確認やウェブサイトを閲覧する前に最新の状態に

☑ **サーバ等における各種ログの確認**
→ 不審なアクセスが発生していないか確認

業務でパソコン等を利用する方へ

休暇前

☑ **機器やデータの持ち出しルールの確認と厳守**
→ 持ち出したＰＣやデータは厳重に管理しましょう！

☑ **使用しない機器の電源ＯＦＦ**
→ パソコンやネットワークプリンターなどは電源ＯＦＦ

休暇明け

☑ **修正プログラムの適用と定義ファイルの更新**
→ ＯＳや各種ソフトウェアの必要な更新を行い、
セキュリティソフトの定義ファイルを最新の状態に

☑ **不審なメールに注意**
→ たまったメールの開封は慎重に！添付ファイルや文中ＵＲＬに注意！
実在する企業・団体を騙る不審なメールが送られているかも！？

☑ **持ち出した機器等のウイルスチェックを実施**
→ ネットワークに接続する前にチェック

引用：IPA独立行政法人情報処理推進機構ホームページより

サイバー犯罪相談事例
対処法と対策・相談窓口

山口県警サイバー課ＬＩＮＥ友達募集中！
サイバー犯罪に関する防犯情報を配信中です

山口県警察本部 サイバー犯罪対策課