岐阜県警察からのお知らせ

サイバー犯罪
対策課

「長期休暇前後のｾｷｭﾘﾃｨ対策のｽｽﾒ」の巻

長期休暇に向けてセキュリティ対策を再確認！

長期休暇の時期は、システム管理者が不在となることも多く、問題が発生した際の対応遅れや、休暇明けに急いでメールを確認してしまう等、セキュリティの問題が発生する可能性が高くなります。特にセキュリティ対策が手薄となりがちな長期休暇前後の時期は、企業、個人問わずセキュリティ対策の再確認をし、被害防止、被害拡大防止に努めましょう。

長期休暇「前」の対策

組　織

1　問題発生時の緊急連絡体制の確認
2　使用しない機器の電源 OFF（サーバ、PC 等）
3　機器やデータの持ち出しルールの確認と遵守（紛失、情報の暗号化、外部から社内へのリモートアクセス時の ID・PW 管理等）
4　社内ネットワークへの機器接続ルールの確認と遵守（感染端末から社内への感染を防ぐ）

個　人

1　旅行前、旅行中の SNS 投稿に注意（不在を公表しているのと同じ）
2　相談窓口が休止している場合が多いので注意

長期休暇「後」の対策

組　織

1　修正プログラムの適用（OS、ソフトウェア、アプリケーション、IoT 機器等）
2　定義ファイルの更新（セキュリティソフト）
3　サーバ等における各種ログの確認（不審なアクセスの有無）
4　持出機器のウイルスチェック（PC、USB メモリ等）
5　メールの開封、リンクへのアクセスに警戒（感染のおそれ有り）

個　人

1　修正プログラムの適用（OS、ソフトウェア、アプリケーション等）
2　定義ファイルの更新（セキュリティソフト）

参考：IPA（情報処理推進機構）

警戒が薄れる長期休暇明けの時期を狙って攻撃される可能性が高いため、休暇明けは特に注意してください!!

本件問い合わせ先：岐阜県警察本部サイバー犯罪対策課　058-271-2424