

サイバーセキュリティ パートナーシップだより



R5-28

年末年始のセキュリティ対策

長期休暇の時期は、システム管理者の長期不在により、いつもと違う状況になりやすく、コンピュータウイルス感染等の事案発生時の対処が遅くなる
ことが懸念されるため、以下の点に注意して被害を未然に防止しましょう。



管理者の方へ

(IPA (情報処理推進機構) ホームページから引用)

休暇の前に！

- ① 緊急連絡先の確保～連絡体制や対応手順の確認をしておきましょう
- ② 社内ネットワークへの機器接続ルールの確認と厳守
- ③ 使わない機器の電源を OFF にする

休暇が終わり、勤務が始まったら！

- ① 修正プログラムの適用～修正の有無を確認し、必要な更新をしましょう
- ② セキュリティソフト定義ファイルの更新
- ③ サーバ等の各種ログの確認～不審なアクセスが発生していないか確認

業務でPC等を利用する方へ

休暇の前に！

- ① 社内ネットワークへの機器接続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！！
- ② 使わない機器の電源を OFF にする

気を付けて！



休暇が終わり、勤務が始まったら！

- ① 不審なメールに注意！！
※ 実在する企業・団体を騙る不審メールが送られているかも！？
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！
- ② 持ち出した機器等のウイルスチェックを行う

個人でPC等を利用する方へ

- ① 行楽等の外出先でのSNS投稿に注意！～居場所や個人情報にはアップしない
- ② 偽のセキュリティ警告に注意！～警告画面の電話番号には電話しない！
- ③ 不審なショートメッセージに注意！
～文中URLからはアクセスしない！※フィッシングサイト等誘導の可能性あり



山口県警察サイバー犯罪相談窓口
入力フォーム



県警ホームページにて広報資料
や動画を公開中です。
(詳しくはQRコード参照)

