長期休暇における情報セキュリティ対策の実施について

（平成30年４月25日作成）

長期休暇期間中は、セキュリティの問題が発生した場合の発見が遅れ、場合によっては関係者に対して被害が及ぶ可能性があります。
このような事態とならないよう、下記の対策の実施をお願いします。

記

１　組織のコンピュータ管理者向け
（1）　長期休暇前の対策
ア　緊急連絡体制の確認（休日・夜間の対応体制・連絡手順等の確認）
・　ホームページ等を外部委託している場合は、委託業者の連絡先確認
イ　使用しない機器の電源OFF（稼働する機器は必要最小限に）
ウ　重要なデータのバックアップ
（2）　長期休暇明けの対策
ア　修正プログラムの適用、ウイルス定義ファイルの更新
イ　ホームページが改ざんされていないか確認
・　ホームページサーバ内に不審なファイルが置かれていないかのチェック

２　組織のコンピュータ利用者向け
（1）　長期休暇前の対策
ア　機器やデータの持ち出しルール等の確認・遵守
・　パソコンやデータを持ち出す場合は、社内ルールを事前に確認願います
イ　使用しない機器の電源OFF（稼働する機器は必要最小限に）
（2）　長期休暇明けの対策
ア　ウィンドウズアップデートやウイルス定義ファイル等のアップデートの実施
イ　持ち出した機器（パソコンやＵＳＢメモリ等）のウイルスチェック
ウ　実在の企業などを騙ったばらまき型メールに注意（添付ファイルを開かない、リンク先にアクセスしないなど）

※　詳しくは、次のWebページも参考にしてください。
・　IPAによる注意喚起
https://www.ipa.go.jp/security/measures/vacation.html
・　JPCERTによる注意喚起
https://www.jpcert.or.jp/pr/2018/pr180001.html

連絡先　沖縄県警察本部サイバー犯罪対策課
(メール hitech@police.pref.okinawa.jp)