令和 2 年 12 月 24 日

教職員・学生　各位

最高情報セキュリティ責任者
個人情報総括保護責任者
水光　正仁

冬季休暇中における情報セキュリティインシデント発生の防止及び緊急時の対応（注意喚起）

冬季休暇中における情報セキュリティインシデント発生の防止及び緊急時の対応について、下記の点に留意頂きますようお願い致します。

なお、宮崎大学では情報セキュリティインシデント対応チーム（CSIRT）を設置しておりますので、インシデントが発生した場合は直ちに緊急連絡先にご連絡下さい。

※情報システム操作やアプリケーション操作等の問い合わせはご遠慮下さい。

（緊急連絡先）

情報セキュリティインシデント対応チーム（CSIRT）

電話　　0985-58-2544

メール　　csirt@cc.miyazaki-u.ac.jp

記

（休暇期間前の対応）

- 休暇中に利用しないパソコンやプリンタなどのネットワーク接続機器は電源を切るようにして下さい。
- 部局、センター等で定めた要保護情報が保存されているパソコンや USB メモリ等の外部記録媒体を持ち出すことは、控えてください。ただし、必要があって持ち出す際は、事前に所属する学部長等に届け出るとともに、パソコンのログインパスワードの設定やファイルにパスワードを設定するなど適正に管理して下さい。
  ※容易に推測されないパスワード（数字とアルファベット、特殊文字を絡ませた 8 文字以上）を設定して下さい。
- パソコンやスマートフォンの OS やアプリケーションに最新のセキュリティ更新プロ

グラムが適用されているか確認して下さい。適用されていない場合は休暇前に必ず更新プログラムを適用して下さい。

- ウイルス対策ソフトが最新の定義ファイルである事を確認の上、フルスキャンを行って下さい。

（休暇期間後の対応）

- 休暇中にセキュリティ更新プログラムが公開されていた場合は速やかに更新プログラムを適用して下さい。
- 出勤後に直ちにウイルス対策ソフトを最新の定義ファイルに更新してフルスキャンを実施して下さい。
- 休暇中に受信したメールの中には標的型攻撃メールが含まれている可能性もあるため、安易に開封しないで下さい。同様にメール本文に記載されている不審な URL にも安易にアクセスしないようにして下さい。

（休暇期間中に情報セキュリティインシデントが発生した場合の対応）

- 以下に示すインシデントが発生した可能性がある場合は、直ちに CSIRT 緊急連絡先にご連絡下さい。
  （1） 情報システムへの不正侵入
  （2） サーバの乗っ取り
  （3） Web ページの改ざん
  （4） 情報機器へのマルウェア（ウイルス）の感染
  （5） 情報システムの設定不備による情報漏洩
  （6） 不正アクセスによる情報漏洩
  （7） 記憶媒体の紛失による情報漏洩
  （8） サイバー攻撃によるサービスダウン
  （9） その他、学内外の情報セキュリティを脅かす事象

以上

照会先　：情報基盤センター基盤システム係
内線番号：7818　（清武からは 927818）
E-Mail：query@cc.miyazaki-u.ac.jp