



## 連休前後はセキュリティ対策の確認を！



### ～ 連休 前 ～



- ☐ **緊急連絡体制の確認** [管理者]  
春先の異動などを踏まえ、緊急時の連絡体制が現時点の組織体制に沿っているか、担当者の連絡先に変更はないかを確認！
- ☐ **アクセス制御の確認** [管理者]  
アクセス権限の確認、多要素認証の有効化等本人認証の強化、パスワードが複雑かを確認！
- ☐ **使用しない機器は電源OFF** [管理者] [利用者]  
休暇中に使用しないサーバ等の機器は電源OFFを！
- ☐ **機器やデータの持ち出しルールの確認** [利用者]  
休暇中に社外に機器やデータ等を持ち出す場合は持ち出しルールを確認！
- ☐ **ソフトウェアの脆弱性対策** [管理者]  
サーバやパソコン、プリンター等各種IT機器の最新のファームウェアへの更新を！
- ☐ **データのバックアップの実施** [管理者]  
ランサムウェアなどサイバー攻撃に備え、重要データのバックアップを！



### ～ 連休 明 け ～

- ☐ **修正プログラムの確認** [管理者] [利用者]  
休暇中にOSやソフトウェアの修正プログラムが公開されている場合があるのでまず確認！
- ☐ **定義ファイル更新** [管理者] [利用者]  
電子メールの送受信やウェブの閲覧前にウイルス対策関連の定義ファイルの更新を！
- ☐ **各種ログのチェック** [管理者]  
サーバ等の機器に不審なアクセスがないかログをチェック！
- ☐ **不審なメールに注意** [利用者]  
休暇明けはメールが溜まっている場合が多く、中には実在の企業等を騙った悪意のあるメールが届いていることもあることから、不審なメールの添付ファイルは開かず、URLもクリックしない！
- ☐ **持ち出した機器のウイルスチェック** [利用者]  
休暇中に持ち出した機器等はウイルスが混入していないか利用前にウイルスチェックを！



昨年末にも同じような内容  
出してなかったっけ…？

長期休暇中はセキュリティ対策が  
甘くなり、攻撃者から狙われやす  
くなるから改めて確認しましょう！



**注意**

CAUTION

休暇後の5月14日は、  
「パッチチューズデー」  
(各社が定例アップデートを公開する日)  
の予定があるので忘れずに要チェック！

