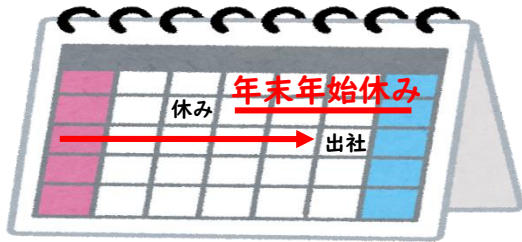




## 年末年始のセキュリティ対策は万全ですか？



長期休暇**前後**のセキュリティ対策について今一度、確認してみましょう！



セキュリティ対策責任者・システム担当者向け

①



☑ データのバックアップは正しく実施しましたか？

重要なデータや機器設定ファイルに対するバックアップの実施。実際に復旧できることを事前に確認しておく◎

②



☑ ソフトウェアに関する脆弱性対策は万全ですか？

セキュリティパッチの適用やソフトウェアのバージョンアップの実施。  
長期休暇明けは、忘れず不正プログラム対策ソフトウェア等の定義ファイルの状態確認。

③



☑ アクセス権限の付与は正しく設定できていますか？

アクセス権限の確認、多要素認証の利用、不要なアカウントの削除等による本人認証の強化。  
パスワードが単純でないかを確認。

④

電源OFF



☑ 長期休暇中に使用しない機器の電源は落とすよう指示しましたか？

外部からの不正なアクセスを防止する観点から、長期間使用しない機器の電源はシャットダウン。使用しない外部サービスの無効化の可否の検討。

⑤



☑ 従業員等へ注意喚起を実施しましたか？

従業員に対して長期休暇前後における各種注意事項を共有。特に、電子メールを確認する際は、不審な添付ファイルは開かない、リンク先にアクセスしないよう指示を徹底。

⑥



☑ 機器やデータの持ち出しルールを確認・共有しましたか？

許可を得て持ち出す機器や媒体の不正プログラム感染、紛失や盗難による情報漏えい等の被害を発生させないような管理、ルールの徹底。



サイバー犯罪被害に遭った場合は、警察への通報・相談を！



警察では、事件捜査に加えて、被害企業等の被害拡大防止や捜査で判明した犯罪手口等の活用による被害の未然防止等の取組を行っています。  
サイバー事案が発生した際は、早期の警察への通報・相談をお願いします！

奈良県警察HP



サイバーセキュリティ対策に関する情報を掲載しています。是非ご覧下さい。