



# 年末年始に備えたサイバーセキュリティ対策



長期休暇前後のサイバーセキュリティ対策がおろそかであると、万一インシデントが発生した場合、思わぬ被害が生じたり対応に遅れが生じるなど、業務継続に影響が及ぶ可能性があります。

**下記項目**をしっかりと実践しましょう。



## 連休前

### ■ システム管理者・担当者

- 不測の事態に備え、委託先企業を含めた緊急連絡体制、対応手順の確認
- メンテナンス等の予定がある場合、連休前に組織内ネットワークへの機器接続ルールを確認
- 連休中に使用しないサーバ等の機器は電源をOFF

よし！確認しよう

### ■ 社員、職員など（組織内ユーザー）

- PC等の機器や情報を持ち出す場合、持ち出しルールを確認
- 連休中に使用しない機器は電源をOFF



## 連休後

### ■ システム管理者・担当者

- 連休中に公開された修正プログラムの確認、適用
- ウイルス対策ソフトの定義ファイルの確認、更新
- サーバ等に対する不審なアクセスがないか、各種ログの確認、調査を実施



### ■ 社員、職員など（組織内ユーザー）

- 連休中に公開された修正プログラムの確認
- システム管理者の指示を受け適用
- ウイルス対策ソフトの定義ファイルの確認、更新
- 組織内ネットワーク接続前に持ち出したPC等のウイルスチェックを実施
- 心当たりのないメールの添付ファイルは開かず本文のURLに接続しない
- 休暇中に受信したメールのチェックに注意



【参考】IPA独立行政法人情報処理推進以降「2024年度 年末年始における情報セキュリティにおける注意喚起」

<https://www.ipa.go.jp/security/anshin/heads-up/alert20241217.html>

◆ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などを、ホームページやX（旧Twitter）に掲載していますのでぜひご覧ください。

◆ 万一、被害に遭われた場合は、管轄警察署宛てご一報ください。

【X】



【HP】

