# サイバー攻撃対策通信

令和６年12月20日
令和６年度第５号
栃木県警察本部
警備部警備第一課

## 年末年始における
## 情報セキュリティに関する注意喚起

**長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。
思わぬ被害が生じないために、以下の対策を実施して下さい。**

### －長期休暇前の対策－

#### １．緊急連絡体制の確認

**不測の事態が発生した場合に備えて、委託先企業を含めた緊急連絡体制や対応手順等が明確になっているか確認して下さい。**

#### ２．社内ネットワークへの機器接続ルールの確認と遵守

**ウイルス感染したパソコンや外部記録媒体等を社内ネットワークに接続することで、ウイルスをネットワーク内に拡散してしまう恐れがあります。長期休暇中にメンテナンス作業などで社内ネットワークへ機器を接続する予定がある場合は、社内の機器接続ルールを事前に確認し厳守して下さい。**

#### ３．使用しない機器の電源OFF

**長期休暇中に使用しないサーバ等の機器は電源をOFFにして下さい。**

### －長期休暇明けの対策－

#### １．修正プログラムの適用

**長期休暇中にＯＳや各種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ります。修正プログラムの有無を確認し、必要な修正プログラムを適用して下さい。**

#### ２．定義ファイルの更新

**長期休暇中に電源を切っていたパソコンは、セキュリティソフトの定義ファイルが古い状態のままになっています。電子メールの送受信やウェブサイトの閲覧等を行う前に定義ファイルを更新し、最新の状態にして下さい。**

#### ３．サーバ等における各種ログの確認

**サーバ等の機器に対する不審なアクセスが発生していないか、各種ログを確認して下さい。もし何らかの不審なログが記録されていた場合は、早急に詳細な調査、警察への通報等の対応を行って下さい。**

TPCCAT
Tochigi Police Counter Cyber Attack Team

**※参照　IPA（情報処理推進機構）ホームページ　https://ipa.go.jp/security/anshin/heads-up/alert20241217.html**