サイバーだより

栃木県警察
サイバー対策センター
令和７年１２月

長期休暇に向けたセキュリティ対策！

しっかりと対策して有意義な長期休暇を送りましょう!

⚡対処手順・連絡体制

- ☐長期休暇期間中の監視体制を確認する。
- ☐必要に応じ、システムアラート等の監視体制を強化する。
- ☐セキュリティインシデントの対処手順を確認し、連絡体制を更新する。

⚡ソフトウェアの脆弱性対策

- ☐脆弱性対策の状況を確認し、必要に応じて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を行う。
- ☐長期休暇期間中に公表された重要な脆弱性情報に対応するための体制を整える。
- ☐直ちに実施することが困難な場合は、リスク緩和策を講じる。

⚡利用機器に関する対策

- ☐機器（サーバ、パソコン等、通信回線装置、特定用途機器（防犯カメラなど））等のファームウェアを最新にアップデートする。
- ☐不正アクセス等を防止するため、長期休暇期間中に使用しない機器の電源を落とす。
- ☐長期休暇期間中に電源を落としていた機器は、端末起動後、最初に不正プログラム対策ソフトウェア等の定義ファイルを確認する。
- ☐最新の状態になっていない場合は、更新してから、利用を開始する。

⚡バックアップ

- ☐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対策を実施する。
- ☐バックアップデータはネットワークから切り離し、変更不可とするなどの対策を検討する。

⚡アクセス制御

- ☐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り、本人認証を強化する。
- ☐利用者にパスワードが単純でないか確認させる。
- ☐外部ネットワークからアクセス可能な機器へのアクセスは必要なものに限定する。

⚡不正プログラム感染の確認

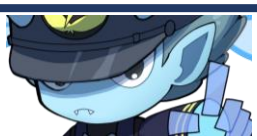
- ☐長期休暇期間中に持ち出しが行われていたパソコン等が不正プログラムに感染していないか、不正プログラム対策ソフトウェア等で確認する。

セルフチェックでしっかり確認!

⚡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ないか、VPN、ファイアーウォール、監視装置等のログやアラートで確認する。
- ☐不審なログが記録されていた場合は、早急に詳細な調査等を行う。

栃木県警察サイバー対策センター
TOCHIGI POLICE
CYBERCRIME CONTROL CENTER



栃木県警察HP(サイバーだより)
https://www.pref.tochigi.lg.jp/keisatu/n14/seikatu/cyber_cyber_dayori.html