愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R6-20号
組織向け

長期休暇前後のセキュリティ対策

前

連絡体制の確認

・セキュリティインシデント発生時の連絡先の更新

不測の事態に備えて、緊急連絡体制や対応手順を明確にしましょう！

利用機器の対策

・休暇中使用しない機器は電源を落とす
・ファームウェアを更新

不正アクセスを防止しましょう！

ソフトウェアの脆弱性対策

・セキュリティパッチの適用
・バージョンアップ

犯人が狙う侵入口（セキュリティの穴）を塞ぎましょう！

バックアップの対策

・重要な情報のバックアップをとり外部媒体に保存

ランサムウェアの攻撃により、同一ネットワーク上にあるバックアップデータは暗号化されてしまいます！

前後

各種ログの確認

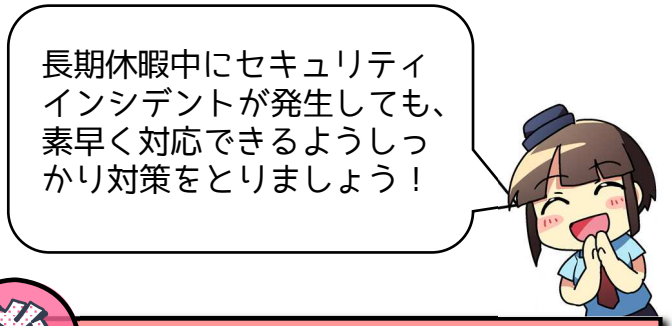
・不審なアクセスがないか、VPN、ファイアーウォール等のログを確認

攻撃の準備をしているかもしれません！
不審なログは早急に調査しましょう！

アクセス制御の設定

・本人認証強化
・外部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

インシデント発生の機会を減らしましょう！



後

持ち出した機器や記録媒体の確認

・不正プログラム感染の確認や、紛失、盗難による情報漏えい等の被害が発生しないように管理

電子メール対策

・不審な添付ファイルを開いたり、リンク先にアクセスしない

休暇明けにたまったメールを確認する作業も慎重に。なりすましメールに注意してください！