

滋賀県警察からのお知らせ

夏季休暇に備えたセキュリティ対策



夏季休暇の時期は、システム管理者が不在等、通常とは異なる状況になりやすく、企業等を狙ったサイバー攻撃やウイルス感染等の不測の事態が発生した場合、対処が遅れてしまいがちです。

特にこの夏は、マイクロソフト社がセキュリティアップデートを公開する8月15日が、お盆と重なるため注意が必要です。

不測の事態に備えて、夏季休暇の時期には、以下のセキュリティ対策を実施してください。

夏季休暇の前には

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ください。

使用しない機器の電源 OFF

休暇中に使用しないサーバ等の機器は電源を OFF にしてください。

基本的なセキュリティ対策の実施

OS やアプリケーションの脆弱性を解消したり、セキュリティ対策ソフトを更新したり、基本的なセキュリティ対策が漏れなく実施できているか確認してください。
また、ランサムウェア対策として、重要データはバックアップをとっておくようにして下さい。

夏季休暇明けには

サーバ等における各種ログの確認

サーバ等機器に対する不審なアクセスがないか、各種ログを確認してください。



業務開始前のセキュリティ更新プログラムの適用

業務を開始する前にセキュリティ更新プログラムを適用し、ぜい弱性を解消するようにしてください。

休暇中に届いたメールも安易に添付ファイルを開かないよう注意が必要です。