滋賀県警からのサイバーセキュリティに関するお知らせ

ゴールデンウイーク中におけるサイバーセキュリティ対策

システム担当者が不在となりやすいゴールデンウイーク等の長期休暇中や、業務に追われがちな長期休暇明けは、いつもとは違う状況になりやすく、企業等を狙ったサイバー攻撃やウイルス感染など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。

このような事態に備えて、長期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。

長期休暇「前」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

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。

長期休暇「明け」は？

セキュリティソフトの更新

電源が OFF になっていた PC は、セキュリティソフトの更新をおこなってから、使用するようにしてください。

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ください。何らかの不審なログが記録されていた場合は、早急に詳細な調査等の対応を行ってください。

参考：独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/measures/vacation.html

５月１日改元「令和」への移行

改元に便乗した「サイバー攻撃」に注意

「令和」への改元に伴い、システムの変更やアプリケーション等の更新が必要となり、準備が大詰めとなっていますが、改元に便乗するサイバー攻撃の発生も懸念されます。システムの動作確認やアプリケーションの更新を実施するとともに、セキュリティ面も不備がないかを確認するようにお願いします。

改元に便乗した「詐欺」に注意

また、「改元によってシステムの更新費用やアプリケーションの購入費用が必要」などという理由をつけ、金銭を騙し取る詐欺が発生するおそれがあります。 実際に更新費用等が発生する場合もありますので、十分、確認をするようにお願いします。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）