滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R４年度 No.10
今、注目のサイバーセキュリティに関する情報をお届けします。

夏休み（長期休暇）におけるセキュリティ

夏休み等の長期休暇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。

長期休暇の「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。

長期休暇の「後」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定義ファイル（パターンファイル）が古くなっている場合があります。また、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ので、必ず確認してください。

サーバ等の各種ログの確認

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。

不審なメールに注意

長期休暇明けは、メールが溜まっていることが想定されますので、注意してメールチェックを行って下さい。

・添付ファイルは安易に開かない。
・本文中のURLにアクセスしない。

参照：IPA「夏休みにおける情報セキュリティに関する注意喚起」 https://www.ipa.go.jp/security/topics/alaert20220803.html

脆弱性情報（緊急性、重要性の高い脆弱性情報等をピックアップしてご紹介します。）

～VMwareの認証管理製品等の脆弱性（2022年8月2日公表）～

VMware社が、複数の製品でシステムの認証を管理する機能等を有するVMware Identity Manager (vIDM)等複数の製品について、重要な脆弱性情報を公表しています。

脆弱性は、認証を回避してアクセスし、管理者権限を取得することができるというもので、修正パッチの適用を呼びかけています。

詳細は、必ず、公式サイト及びIPA、JVN、JPCERT/CC等の脆弱性情報提供サイトを確認してください。

サービス名、機器名（影響を受けるソフトウェア）	脆弱性の概要（悪用された場合の影響等）	CVE（共通脆弱性識別子）	対策（修正プログラムの公開情報等）
・Workspace ONE Access ・VMware Identity ・Manager (vIDM) 等	当該脆弱性を悪用して当該製品を導入しているシステムの制御を奪取することが可能となる。	CVE-2022-31656 （CVSSスコア9.8） 等	修正パッチの適用（公開中）

参照：Vmware「Vmwareセキュリティアドバイザリ」https://www.vmware.com/security/advisories/VMSA-2022-0021.html

«Windows8.1のサポートが令和5年1月10日に終了»

サポートを終了したソフトウェアは、原則、脆弱性が発見されても更新されません。

ウイルス感染被害に遭う可能性も高まります。

対象のOSを利用されている場合は、最新版への移行等の対策をお願いします。早めに実施することをお勧めします。

«CS情報SHIG@»偽ショッピングサイトの見分け方→「.top」「.xyz」等のドメインに注意しましょう。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表） 詳細は県警webページで →