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.21
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。

年末年始におけるセキュリティ
「警戒の空白」を生まない対策を推進しましょう。

年末年始等の長期休暇は、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。
サイバー攻撃に対する警戒に空白がないように意識をしておくことが重要です。

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「年末年始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/alaert20201217.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。）

~Sophos Firewallの脆弱性（2022年12月1日公表）~

Sophos社が、「Sophos Firewall」について、リモートコード実行等が可能になる７つの脆弱性に対応する修正パッチをリリースし、その適用を呼びかけています。当該製品を利用されている方は、セキュリティパッチの適用、またはアップグレードを実施してください。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）
・Sophos Firewall	OSコマンドインジェクションの脆弱性、管理者がSSL VPN設定のアップロードを介してコード実行できる可能性があるなど	CVE-2022-3226（CVSSスコア7.2） 等	修正プログラムの適用 アップグレードの実施

参照：SOPHOS セキュリティアドバイザリ https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0

«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。

«CS情報SHIG@»年末年始のネットショッピングは慎重に。詐欺サイトに騙されないでください。

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 →

https://www.pref.shiga.lg.jp/police/seikatu/304409/index.html