IPAより

多くの人が長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。このような状況でセキュリティインシデントが発生した場合は、対応に遅れが生じたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生したり、長期休暇後の業務継続に影響が及ぶ可能性があります。

これらのような事態とならないよう、(1)個人の利用者、(2)企業や組織の利用者、(3)企業や組織の管理者、のそれぞれの対象者に対して取るべき対策をまとめています。また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

■長期休暇における情報セキュリティ対策

https://www.ipa.go.jp/security/measures/vacation.html

■日常における情報セキュリティ対策

https://www.ipa.go.jp/security/measures/everyday.html

※上記リンク先において、対象者毎に参照すべき範囲は以下のとおりです。

(1)個人の利用者　　　：個人向けの対策（3.）

(2)企業や組織の利用者：個人及び企業・組織のシステム利用者向けの対策（2-2. / 3.）

(3)企業や組織の管理者：個人、企業・組織のシステム利用者及び管理者向けの対策（2-1. / 2-2. / 3.）

 被害に遭わないためにもこれらの対策の実施をお願いします。

■ゴールデンウィーク等の長期休暇における情報セキュリティ対策（IPA）

https://www.ipa.go.jp/security/anshin/heads-up/alert20240422.html

【企業や組織の方々へ】

企業や組織のネットワークとインターネットとの境界に設置されるセキュリティ製品の脆弱性を悪用する攻撃が継続して確認されています。本件に関連する対策情報として、2023年5月に経済産業省より「ASM（Attack Surface Management）導入ガイダンス」が公開され、また8月にはIPAからネットワーク貫通型攻撃、10月にはオンラインストレージの脆弱性に関する注意喚起を行っております。

現状ではランサムウェア攻撃のみならずネットワーク貫通型攻撃に関連する脅威が持続しており、昨今の国際情勢も踏まえ留意が必要と考えられる状況となっています。また、標的型攻撃メールを用いた攻撃も継続していることから、従来対策及び本件の追加的対策の双方が必要といえます。

以下のページも参考に、日々の確認および平時の備えなどの対策について再度確認をしてください。

■アタックサーフェスの Operational Relay Box 化を伴うネットワーク貫通型攻撃について～Adobe ColdFusion の脆弱性（CVE-2023-29300）を狙う攻撃～

https://www.ipa.go.jp/security/security-alert/2024/alert\_orb.html

お問い合わせ先

標的型攻撃に関するご相談及び情報提供先

■J-CRAT 標的型サイバー攻撃特別相談窓口

E-mail：tokusou@ipa.go.jp

URL：https://www.ipa.go.jp/security/todokede/tokubetsu.html

被害情報の届出先

■コンピュータウイルス・不正アクセスに関する届出窓口

URL：https://www.ipa.go.jp/security/todokede/crack-virus/about.html

一般的な情報セキュリティ（主にウイルスや不正アクセス）や相談先に迷う場合は以下までお問い合わせください。

■情報セキュリティ安心相談窓口

E-mail：anshin@ipa.go.jp

URL：https://www.ipa.go.jp/security/anshin/about.html

あわせて、不審な動き等を検知した場合は、速やかに所管省庁、セキュリティ関係機関等状況に応じた関係先への情報提供や警察へのご相談もご検討ください。

今一度、サイバーセキュリティの確保に努めていただくとともに長期休暇期間がサイバーセキュリティに与えるリスクに鑑み、団体会員の皆様におかれましては所属企業や取引先等の中小企業の皆様にも周知いただけますと幸いです。