河上 聖志

差出人: JASPO事務局
送信日時: 2023年4月27日木曜日 13:56
件名: 【ご連絡】IPA SC3事務局からのお知らせ：【注意喚起】春の大型連休に向けて実施いただきたい対策について

一般社団法人日本スポーツ用品工業協会
会員　各位
（ＢＣＣにてお送りいたします）

いつもお世話になっております。
日頃より弊協会の活動にご理解とご協力を賜り誠にありがとうございます。

IPA（独立行政法人　情報処理機構）より下記のお知らせを頂きましたので
ご連絡申し上げます。
内容をご確認の上、ご参考になれば幸甚です。
ご査収ください。

＞＞＞
SC3 会員及び関係者各位

平素より大変お世話になっております。SC3 事務局でございます。
主題の件につきまして、ご案内です。

昨今のサイバー攻撃事案のリスクの高まりを踏まえ、政府から昨年 12 月には、
年末年始休暇において実施いただきたい対策などの注意喚起が行われましたが、
その後もランサムウェアによるサイバー攻撃被害が国内外の様々な企業・
団体等で続いています。このように依然として厳しい情勢下で春の大型連休を
迎えるにあたり、4 月 24 日に経済産業省から改めて注意喚起が公表されています
（総務省、警察庁、内閣官房内閣サイバーセキュリティセンター同時発表）。
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、団体会員の
皆様におかれては、所属企業の皆様にもぜひ注意喚起いただけますと幸いです。

■春の大型連休に向けて実施いただきたい対策について（注意喚起）

昨年 12 月の関係府省庁連名による注意喚起の発出後も、ランサムウェアによる
サイバー攻撃被害が国内外で続いており、また、エモテットと呼ばれる
マルウェアへの感染を狙う攻撃メールも本年 3 月に活動再開とその新たな手口を

確認しており、国内の企業・団体等へ広く感染の被害が広がっていると考えられます。
さらに、日本の政府機関・自治体や企業のホームページ等を標的としたDDoS攻撃と
思われるサービス不能攻撃により、業務継続に影響のある事案も発生し、国民の誰もが
サイバー攻撃の懸念に直面することとなっています。
このような情勢下にあって、特に大型連休中は通常と異なる体制等により予期しない
事象が生じることが懸念されるとともに、連休明けは電子メールの確認の量が増える
ことで偽装のチェックなどがおろそかになるといった感染リスクの高まりも予想されます。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、
大型連休における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、
セキュリティ対策実施責任者、及び情報システムを用いる職員等それぞれにおいて
下記の観点の対策を講じていただくよう改めてお願いいたします。

◆セキュリティ対策の実施に関する責任者における実施事項

１．長期休暇期間前の対策
・長期休暇期間中のセキュリティインシデントを認知した際の対処手順及び
　連絡体制の確認
・利用機器・外部サービスに関する対策
・ソフトウェアに関する脆弱性対策の実施
・バックアップ対策の実施
・アクセス制御に関する対策
・職員等への注意喚起の実施

２．長期休暇期間明けの対策
・サーバ等における各種ログの確認
・ソフトウェアに関する脆弱性対策の実施
・不正プログラム感染の確認
・長期休暇期間中に電源を落としていた機器に関する対策

◆情報システムを利用する職員等における実施事項

１．長期休暇期間前の対策
・利用機器に関する対策
・機器やデータの持ち出しルールの確認と遵守

２．長期休暇期間明けの対策
・利用機器のOS/アプリケーションへの修正プログラムの適用及び
　定義ファイルの更新
・不審メールへの注意

各実施事項の詳細については、下記の注意喚起をご確認ください。
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に対して情報提供いただくとともに、
警察にもご相談ください。

■経済産業省からの注意喚起の発表
（総務省、警察庁、内閣官房内閣サイバーセキュリティセンター同時発表）
春の大型連休に向けて実施いただきたい対策について（注意喚起）
https://www.meti.go.jp/press/2023/04/20230424002/20230424002.html

■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/alert20230420.html

■「中小企業の情報セキュリティ対策ガイドライン」を改訂

「中小企業の情報セキュリティ対策ガイドライン」は、中小企業の経営者や
実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理する
ための具体的な手順等を示したガイドラインです。2019年3月に第3版を公表して以降、
新型コロナウイルス感染防止策によるテレワークの普及や、DX 推進の両輪としての
情報セキュリティ対策といった社会動向の変化などを踏まえ、具体的な対応策を
盛り込むための改訂を行いました。

本ガイドラインは、本編2部と付録で構成されています。第1部に経営者が認識すべき
「3原則」、経営者が実行すべき「重要7項目の取組」を記載し、第2部では
実務担当者向けに情報セキュリティ対策の具体的な進め方を説明しています。
さらに、「情報セキュリティ基本方針」や「情報セキュリティ関連規程」などの
ひな形を付録として備えています。今回の改訂の主なポイントは以下のとおりです。

1.テレワークを安全に実施するためのポイントを具体的な方策として追加
2.セキュリティインシデント発生時の対応を具体的な方策として追加
3.「中小企業のためのセキュリティインシデント対応の手引き」を付録に追加

本ガイドラインおよび「SECURITY ACTION」制度の活用によって、ITを利活用している
中小企業が情報セキュリティ対策に取り組み、経済社会全体のサイバーリスク低減に
つながることを期待しています。
ご一読いただけますようお願いいたします。

■中小企業の情報セキュリティ対策ガイドライン（IPA）
https://www.ipa.go.jp/security/guide/sme/about.html

□■IPA━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
独立行政法人情報処理推進機構　(IPA)
セキュリティセンター　企画部　中小企業支援グループ
SC3 事務局
sc3-info@ipa.go.jp
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━IPA■□

◆IPA を騙った偽メールにご注意ください◆
IPA からお送りするメールニュースには、電子署名を付与しております。
（電子署名以外のファイルを添付して送付することは一切ありません。）
不審なメールを受信した場合は、自社の担当部署にご確認ください。
＞＞＞
＞＞＞＞＞＞

以上　宜しくお願いいたします。
□□□□□□□□□□□□□□□□□□□
一般社団法人　日本スポーツ用品工業協会
事務局
TEL:03-3219-2041
E-mail: jaspo_sgi@sgi-jaspo.org
□□□□□□□□□□□□□□□□□□□