2020年7月30日

夏季休暇等に伴うセキュリティ上の留意点について【注意喚起】

2020年7月30日、内閣サイバーセキュリティセンターは、重要インフラ事業者等に向けて夏季休暇等に伴うセキュリティ上の留意点について注意喚起を行いました。

また、本件は、新型コロナウイルス感染症対応の長期化に伴い、サイバーセキュリティリスクの高まりとこれに乗じたサイバー攻撃の兆候がみられていること等を踏まえ、本格的夏季休暇に入る前に、適切なサイバーセキュリティ管理のための注意喚起ですが、広く一般にも活用していただけるよう公開するものです。

資料　夏季休暇等に伴うセキュリティ上の留意点について【注意喚起】

本件に関する連絡先
内閣サイバーセキュリティセンター
電話番号03-5253-2111（代表）
　重要インフラ第２グループ

別紙

2020 年 7 月 30 日

内閣サイバーセキュリティセンター
重要インフラグループ

夏季休暇等に伴うセキュリティ上の留意点について(注意喚起)

新型コロナウイルス感染症対応の長期化に伴い、サイバーセキュリティリスクの高まりとこれに乗じたサイバー攻撃の兆候がみられていること等を踏まえ、本格的夏季休暇に入る前に、重要インフラ事業者等の十全なサイバーセキュリティ確保のための注意喚起です。

1. 概要

重要インフラ事業者等においては、新型コロナウイルス感染症対応の長期化に伴い、急速なテレワークの導入等、必ずしも十分ではない形でのサイバーセキュリティ対応とならざるを得ない状況も見受けられます。また、こうした混乱に乗じたサイバー攻撃の兆候がみられています。

特に本年は世界的な新型コロナウイルス感染症拡大を踏まえ、本格的に夏季休暇の期間に入る前に、例年の夏季休暇に伴うセキュリティリスクへの対応に加えて、こうした状況変化を踏まえて、適切なセキュリティリスクの管理が求められます。

重要インフラ事業者等の使命は、システム障害によりサービスの継続的な供給に支障の無いようにすることですが、その適切な実現方法は、それぞれの分野や組織によって異なり、一律ではありません。本格的夏季休暇を迎えるにあたり、組織ごとによって設置されるサイバーセキュリティを考慮したリスク管理及び危機管理体制、CSIRT 活動等、組織の指揮・管理の下、CISO、システム管理者、システム利用者、関係組織、委託先等を含む組織関係者全体で取り組み、適切なサイバーセキュリティを確保することが求められます。

2. 夏季休暇等に伴うセキュリティリスク

本年の夏季休暇期間においては、当初予定されていた 2020 年東京オリンピック競技大会・東京パラリンピック競技大会は延期となりましたが、引き続き注意が必要です。他方、新型コロナウイルス感染症への対応としての新しい生活様式への移行が進む中、在宅勤務によって組織が管理していないネットワークからの勤務の増加、自宅での業務情報の扱い、Web 会議、業務プロセスの急な変更、通常と異なるプロセスでの組織的な意思決定、十分な選定を経なかった製品やサービスの導入などの背景を踏まえることが必要です。当初数か月程度を見込んでいた対応体制は、長期的に続けなければならない状況になっていると認識する必要があります。

長期休暇中でも世界は動いています。毎年 8 月には「Black Hat USA」、「DEF CON」等のセキュリティカンファレンスが開催され、新たな脆弱性や PoC の発表が多くなるなど、世界の動向変化や関係機関からの注意喚起を迅速に察知するための情報収集、組織内での評価、発信体制に加え、事案発生時に組織内外(関係省庁を含む)の危機対応関係各部署への速やかな伝達、対応方針の検討、事案対応が行えるよう連絡体制の確認について検討することが必要です。

こうした状況認識の下、重要インフラ事業者等においては、例年取り組んでいる夏季休暇等に伴うセキュリティリスクへの対応に、次に掲げるリスク要因を含めることが必要です。

① テレワークに関するセキュリティリスク
② 最近のマルウエアに関するセキュリティリスク
③ 長期休暇明けの大量のメール確認による不注意がマルウエアの感染につながる不審メール等を開封するリスク
④ 長期休暇中に提供された発見・公表された脆弱性、関係機関からの提供情報、OS、ソフトウエア等への対応遅延リスク
⑤ 長期休暇中のインシデントに対して監視の目が届きにくくなるリスク
⑥ 長期休暇中に発生したインシデントが適切に担当者に伝達されないリスク

3. 特に留意すべきセキュリティリスクについて

(1) テレワークに関するセキュリティリスク

テレワークを継続している事業者等においては、この機会にテレワークに関するセキュリティリスクを再確認し、必要な対応が求められます。その際、攻撃者がリモートアクセス環境の脆弱性や設定不備を突き、深刻な被害が発生する事例も発生していることから、リモートアクセス環境を構成する製品に対する迅速なアップデートや適切な設定が必要となります。また、クラウドサービスを利用していることによるリスクとして、設定ミスや不十分なアクセス制限、多要素認証不採用などによる脆弱な認証、クラウドサービスの管理者権限の認証情報の管理なども考慮することが必要です。

テレワークを導入していない事業者等が新たにテレワークを導入する際には、「テレワークを実施する際にセキュリティ上留意すべき点について[1]」等を参照し、適切なテレワーク環境を構築することが必要です。

(2) 最近のマルウエアに関するセキュリティリスク

コロナ禍において、事業者等に対するランサムウエア等を含むマルウエアによる攻撃が活発になっています。マルウエア「Emotet」については、しばらく活動を休止していましたが、2020 年 7 月以降、世界的に活動が再開されたことが確認されています。「Emotet」は、感染端末から窃取したメールの本文や添付ファイルを引用したなりすましメールに加え、請求書を騙ったメールやシステム管理者を装ったメール等、一般的に

[1] *内閣サイバーセキュリティセンター「テレワークを実施する際にセキュリティ上留意すべき点について (資料 2)」(2020/4/14)、https://www.nisc.go.jp/active/general/pdf/telework20200414.pdf*

利用者が開きやすいメールを送信することで、感染を拡大するマルウエアです。その他、ランサムウエア「MAZE」、「EKANS」や、情報窃取マルウエア「LODEINFO」等、マルウエア流行の状況を踏まえた対策が必要です。なお、ランサムウエアの攻撃目的が金銭ではなく破壊活動や企業情報の窃取である可能性があることも考慮すべきです。ランサムウエア対策を講じていても、大規模な被害に発展する事案が世界的に発生しており、重要なデータのバックアップについて、この際確認することが必要です。

参考 URL

・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/measures/vacation.html
・Web 会議サービスを使用する際のセキュリティの注意事項(IPA)
https://www.ipa.go.jp/security/announce/webmeeting.html
・「Emotet」と呼ばれるウイルスへの感染を狙うメールについて(IPA)
https://www.ipa.go.jp/security/announce/20191202.html
・マルウエア Emotet の感染に繋がるメールの配布活動の再開について(JPCERT/CC)
https://www.jpcert.or.jp/newsflash/2020072001.html
・マルウエア LODEINFO の進化(JPCERT/CC)
https://blogs.jpcert.or.jp/ja/2020/06/LODEINFO-2.html