内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

2021 年 4 月 26 日

内閣官房内閣サイバーセキュリティセンター

大型連休等に伴うセキュリティ上の留意点について

2021 年 4 月 26 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、大型連休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。

本件は、新型コロナウイルス感染症対応の長期化に伴い、引き続き、これらに乗じたとみられるサイバー攻撃が確認されていることに加え、大型連休がサイバーセキュリティに与えるリスクを踏まえ、適切な管理策が必要となることに鑑み、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：大型連休等に伴うセキュリティ上の留意点について(注意喚起)

本件に対する問い合わせ先
内閣サイバーセキュリティセンター(NISC)
電話：03-5253-2111(代表)
重要インフラ第 2 グループ

2021 年 4 月 26 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

大型連休等に伴うセキュリティ上の留意点について(注意喚起)

大型連休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に努めてください。

新型コロナウイルス感染症対応の長期化に伴い、引き続き、これらに乗じたとみられるサイバー攻撃が確認されています。大型連休がサイバーセキュリティに与えるリスクを踏まえ、適切な管理策が必要となります。

1. 大型連休等に伴うセキュリティリスク

昨年来、新型コロナウイルス感染症対策として、新しい生活様式が組み込まれており、大型連休に際し、重要インフラ事業者等においては、次のようなリスクを含め対応策の検討が必要です。

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 新たに確認された脆弱性に関するセキュリティリスク
④ システム更改等の作業に起因するリスク
⑤ 長期休暇に伴うリスク

2. 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

新型コロナウイルス感染症対策の一環として、テレワークが大幅に普及してきていますが、テレワークの利用拡大に伴うネットワーク負荷増大への対応として利用した旧型の VPN 装置が起因となって、機密情報の窃取やランサムウエアの感染につながる事案が発生しています。

チェックポイント

- インターネット等の外部ネットワークからアクセス可能な機器については、セキュリティパッチを迅速に適用する、管理機能、不要なポートやプロトコルを外部に開放しない等の管理策等、IT 資産管理を改めて確認する。
- 必要な監視強化や、攻撃を受けた場合の対応策をあらかじめ確認しておく。
- クラウドサービスを利用している場合は、設定ミスや不十分なアクセス制御、多要素認証不採用などによる脆弱な認証などを考慮し、管理者権限の認証情報を適切に管理する。

- テレワーク等に関連し、職場から持ち出したPCについて、休暇中に長期間、十分な管理下になかったPCを職場で再び利用する際は、パッチの適用やウイルススキャンの実施など必要に応じて実施する。

(2) 最近のマルウエアに関するセキュリティリスク

最近では、マルウエア「Emotet」に代わり、マルウエア「IcedID」による攻撃が活発になってきています。IcedIDは、Emotet同様、返信を装ったなりすましメールや料金の請求を装ったメールを用いる等、様々な手口で感染を試みます。海外では、新型コロナウイルス感染症のワクチン接種に関連するフィッシングメールが確認されています。

チェックポイント

- ランサムウエアによるサイバー攻撃について、予防策、感染した場合の緩和策・対応策などについてあらかじめ検討しておく。
- 海外同様、我が国でも、人の不安や心理的な手口を利用したマルウエアによる攻撃が行われる可能性があることに留意する。

(3) 新たに確認された脆弱性に関するセキュリティリスク

標的型攻撃等では使用しているソフトウエアや機器等の脆弱性が利用されます。最近明らかになった脆弱性について、既に攻撃が確認されています。

チェックポイント

- 必要な管理策やセキュリティパッチの適用等を講じる。
- Fortinet製Virtual Private Network(VPN)装置の脆弱性（CVE-2018-13379）[1]
- Ivanti製VPN装置「Pulse Connect Secure」の脆弱性（CVE-2021-22893、CVE-2020-8260、CVE-2020-8243、CVE-2019-11510）[2]
- Windowsのドメインコントローラの脆弱性（CVE-2020-1472）[通称:Zerologon][3]
- Microsoft Exchange Serverの脆弱性（CVE-2021-26855等）[4]

(4) システム更改等の作業に起因するリスク

大型連休等のタイミングでシステム更改などの変更作業を実施する場合には、これらの作業に起因したシステム障害が発生することがあり留意が必要です[5]。また、自組織で変更がない場合でも、利用している外部サービスやクラウドサービスでの連休期間中の変更等が意図しない動作につながる可能性があります。

---

[1] *NISC「Fortinet製VPNの脆弱性(CVE-2018-13379)に関する重要インフラ事業者等についての注意喚起の発出について(2020/12/3)」、https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf (2021/4/26閲覧)*

[2] *Ivanti「Pulse Connect Secure Security Update(2021/4/20)」、https://blog.pulsesecure.net/pulse-connect-secure-security-update/ (2021/4/26閲覧)*

[3] *Microsoft「CVE-2020-1472 Netlogon の特権の昇格の脆弱性(2021/2/9)」、https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2020-1472 (2021/4/26閲覧)*

[4] *Microsoft「On-Premises Exchange Server Vulnerabilities Resource Center(2021/3/25)」、https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/ (2021/4/26閲覧)*

[5] *IPA「情報システムの障害状況 2019年前半データ(2019/9/20)」、https://www.ipa.go.jp/files/000077486.pdf (2021/4/26閲覧)*

(5) 長期休暇に伴うリスク

その他、長期休暇に伴う以下のリスクについて、必要な管理策の実施が必要です。

チェックポイント

- 長期休暇明けに行われる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
- 長期休暇中に確認・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が遅延するリスク
- 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
- 長期休暇中に発生したインシデント等が適切に担当者に伝達されないリスク

参考 URL

- ゴールデンウィークにおける情報セキュリティに関する注意喚起(IPA)
  https://www.ipa.go.jp/security/topics/alert20210421.html
- 2021 年 1 月から 3 月を振り返って(JPCERT/CC)
  https://www.jpcert.or.jp/newsflash/2021041501.html
- 最近のサイバー攻撃の状況を踏まえた経営者への注意喚起(経済産業省)
  https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf
- 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(NISC)
  https://www.nisc.go.jp/active/general/pdf/telework20200414.pdf
- Salesforce の製品の設定不備による意図しない情報が外部から参照される可能性について(NISC)
  https://www.nisc.go.jp/active/infra/pdf/salesforce20210129.pdf
- ランサムウエアによるサイバー攻撃について【注意喚起】(NISC)
  https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf
- Fortinet 製 VPN の脆弱性(CVE-2018-13379)に関する重要インフラ事業者等についての注意喚起の発出について(NISC)
  https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf
- 【注意喚起】事業継続を脅かす新たなランサムウエア攻撃について(IPA)
  https://www.ipa.go.jp/security/announce/2020-ransom.html