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 7 月 21 日

内閣官房内閣サイバーセキュリティセンター

夏季休暇等に伴うセキュリティ上の留意点について

2021 年 7 月 21 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。

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ることに加え、2020 年東京オリンピック・パラリンピック競技大会に乗じたサイバー攻撃が確認される恐れがあることに鑑み、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 7 月 21 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)

本格的な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。また、2020 年東京オリンピック・パラリンピック競技大会(以下「東京 2020 大会」)に乗じたサイバー攻撃が確認される恐れがあります。夏季休暇や東京 2020 大会等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. 夏季休暇等に伴うセキュリティリスク

夏季休暇等に際し、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 ランサム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 東京 2020 大会に関するセキュリティリスク
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

昨今、セキュリティ対応が不十分な VPN 装置が起因となり、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

- 管理する IT 資産のうち、インターネット等外部ネットワークからアクセス可能な機器については、外部ネットワーク公開の必要性を精査し、外部からの管理機能や、これに関連するポート(137(TCP/UDP)、138(UDP)、139(TCP)、445(TCP/UDP)、3389(TCP/UDP)など)、プロトコルを必要なものに限定し、使用する場合は、セキュリティパッチの迅速な適用等を改めて確認する。
- 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) ランサムウエアに関するセキュリティリスク

ランサムウエア攻撃が活発になっており、日本国内では、日本企業や海外子会社で攻撃者にデータが公開される事例が増加、海外では、重要インフラに関わる事業者がランサムウエアに感染、サービスの供給に支障が生じた事例やマネージドサービスプロバイダー(MSP)を介してMSPの顧客がランサムウエアに感染した事例が発生しています。

チェックポイント

- 当センターから公開している「ランサムウエアによるサイバー攻撃に関する注意喚起について」等を参照し、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・対応策などをあらかじめ検討しておく。
- 米国CISAによるランサムウエア対策(参考URL参照)を参考に、具体的対策を講じる。

(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

標的型攻撃やランサムウエア攻撃等では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の中には、悪用が報告されているものがあり、注意が必要です。

チェックポイント

- ソフトウエアや機器等の脆弱性については、悪用が報告されているものを含む以下の脆弱性に十分留意する。
  - 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]
  - Citrix製「Citrix Application Delivery Controller」「Citrix Gateway」「Citrix SD-WAN WANOP」の脆弱性(CVE-2019-19781)[3]
  - 「Microsoft Exchange Server」の脆弱性(CVE-2021-26855等)[4]
  - F5 Networks製「BIG-IP」製品の脆弱性(CVE-2020-5902)[5]
  - 「SonicWall Secure Mobile Access 100シリーズ」の脆弱性(CVE-2021-20016)[6]

---

[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 (2021/7/21 閲覧)*

[2] *Ivanti「Pulse Connect Secure Security Update(2021/4/20)」、https://blog.pulsesecure.net/pulse-connect-secure-security-update/ (2021/7/21 閲覧)*

[3] *Citrix「CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance(2020/10/23)」、https://support.citrix.com/article/CTX267027 (2021/7/21 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/ (2021/7/21 閲覧)*

[5] *F5 Networks「K52145254: TMUI RCE vulnerability CVE-2020-5902(2021/5/3)」、https://support.f5.com/csp/article/K52145254 (2021/7/21 閲覧)*

[6] *SonicWall「CONFIRMED ZERO-DAY VULNERABILITY IN THE SONICWALL SMA100 BUILD VERSION 10.X(2021/2/4)」、https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001 (2021/7/21 閲覧)*

- 「Microsoft Windows Print Spooler」の脆弱性
  (CVE-2021-34481[7]、CVE-2021-34527[8])
- 「Microsoft Windows」のドメインコントローラーの脆弱性(CVE-2020-1472 等)[9]

(4) 東京 2020 大会に関するセキュリティリスク

平時と同様、ランサムウエアを含むマルウエア、DDoS 攻撃、脆弱性への対応やシステム障害の発生に備えた対応策の実施に加え、以下について考慮が必要です。

チェックポイント

- 東京 2020 大会の関係者を騙ったメールや Web サイト(フィッシングサイト)によるサイバー攻撃が発生するリスク
- 重要インフラサービスに関連する内部、外部で発生した事案に対する連絡体制・対処体制の確認(所管省庁への連絡体制を含む)

(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

---

[7] *Microsoft「Windows Print Spooler Elevation of Privilege Vulnerability CVE-2021-34481(2021/7/15)」、https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481 (2021/7/21 閲覧)*

[8] *Microsoft「Windows Print Spooler Remote Code Execution Vulnerability CVE-2021-34527(2021/7/16)」、https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527 (2021/7/21 閲覧)*

[9] *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 (2021/7/21 閲覧)*

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
- 2021 年 4 月から 6 月を振り返って(JPCERT/CC)
  https://www.jpcert.or.jp/newsflash/2021070801.html
- 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
- ランサムウエアによるサイバー攻撃に関する注意喚起について(NISC)
  https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.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
- 中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について(注意喚起)(NISC)
  https://www.nisc.go.jp/press/pdf/20210719NISC_press.pdf
- 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
- 複数の SSL VPN 製品の脆弱性に関する注意喚起(JPCERT/CC)
  https://www.jpcert.or.jp/at/2019/at190033.html
- 【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について(IPA)
  https://www.ipa.go.jp/security/announce/2020-ransom.html
- Stop Ransomware(CISA)
  https://www.cisa.gov/stopransomware
- CISA and MS-ISAC Release Ransomware Guide(CISA)
  https://us-cert.cisa.gov/ncas/current-activity/2020/09/30/cisa-and-ms-isac-release-ransomware-guide