2020 年 12 月 23 日

年末年始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)

年末年始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。

1. 概要

重要インフラ事業者等においては、例年の年末年始休暇に伴うセキュリティリスクへの対応に加えて、新型コロナウイルス感染症対応の長期化に伴う対応が求められています。

長期休暇中の監視体制の不備、休暇明けのメールの大量処理に加え、長期休暇中を利用したシステムの更改等に伴うリスクを的確に把握し、管理することが重要です。

昨今発生しているサイバー攻撃やトラブル事例を踏まえ、障害発生時の回復手段の事前準備等の「レジリエンス」(障害回復力)を確保するため、長期休暇に伴う関係者や判断者の連絡体制の確保など、システム障害に備えた対応態勢の整備や連絡手段の確保が必要です。

2. 年末年始休暇等に伴うセキュリティリスク

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での対応が進む中、在宅勤務等によって組織が管理していないネットワークからのアクセスの増加、自宅等の職場外での業務情報の取扱い、業務プロセスの急な変更、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引き続き必要です。

過去にはクリスマス[1]や新年の挨拶[2]を題材としたマルウエア付きメールが送信される事例も確認されており、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年末年始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 最近の脆弱性に関するセキュリティリスク
④ システム更改時等の作業誤り等に関するセキュリティリスク

---

[1] *IPA「サイバー情報共有イニシアティブ(J-CSIP)2014 年度 活動レポート 別冊 添付資料「X」による攻撃メール一覧(2015/5/27)」、https://www.ipa.go.jp/files/000046020.pdf (2020/12/22 閲覧)*

[2] *IPA「【注意喚起】潜伏しているかもしれないウイルスの感染検査を今すぐ!(2015/6/29)」、https://www.ipa.go.jp/security/ciadr/vul/20150629-checkpc.html (2020/12/22 閲覧)*

⑤ 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
⑥ 長期休暇中に発見・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
⑦ 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
⑧ 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

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、不要なポートやプロトコルを外部に開放しない等の対策を講じているか改めて確認することが必要です。クラウドサービスを利用している場合、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、クラウドサービスの管理者権限の認証情報の管理などについて再確認することが必要です。テレワークや年末年始休暇等に関連して、たとえば、職場から持ち出したPCを職場のLANに接続する前に、自職場のＩＴ環境に応じたリスクを的確に評価し、その結果を踏まえ、検疫を行うなどの対処が必要です。

(2) 最近のマルウエアに関するセキュリティリスク

昨今、ランサムウエアを含むマルウエアによる攻撃が活発になっています。

特に、ランサムウエアによるサイバー攻撃の高度化・巧妙化、攻撃活動が活発になっており、本年度に入ってから、我が国及び関連する海外の組織でランサムウエアの感染による業務支障が報道されています。ランサムウエアによるサイバー攻撃については、重要インフラ事業者等があらかじめ、予防策、感染した場合の緩和策、対応策などを検討しておくための注意喚起[3]を当センターから公開しているため、活用してください。メール経由で感染を試みるマルウエアについても、注意が必要です。攻撃に用いられるメールとして、請求書を騙ったもの、システム管理者を装ったもの、「新型コロナウイルス感染症」等の時事や季節に関する事柄を題材にしたもの、マルウエア「Emotet」[4]や「IcedID」[5]のように感染したPCから窃取したメールの件名等を引用したなりすましメール等、様々なパターンがあることに留意することが必要です。

(3) 最近の脆弱性に関するセキュリティリスク

標的型攻撃等では、インターネット接続の有無に関わらず、PC、サーバー、ネットワーク機器等ネットワーク全体の脆弱性が攻撃対象となります。インターネットに接続している機器はもちろんのこと、インターネットに接続していない機器についても、

---

[3] *NISC「ランサムウエアによるサイバー攻撃について【注意喚起】(2020/11/26)」、https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf (2020/12/22 閲覧)*
[4] *IPA「「Emotet」と呼ばれるウイルスへの感染を狙うメールについて(2020/9/2)」、https://www.ipa.go.jp/security/announce/20191202.html (2020/12/22 閲覧)*
[5] *JPCERT/CC(Twitter)「Analysis Center(@jpcert_ac)の投稿(2020/11/6)」、https://twitter.com/jpcert_ac/status/1324561915738091522 (2020/12/22 閲覧)*

パッチ適用の必要性やパッチが適用できない場合の管理策などを十分検討し、システムの状況を踏まえた適切な管理を実施することが必要です。

特に、最近では、先日、当センターからも注意喚起を行った脆弱性を含む以下の脆弱性への対応について、留意することが必要です。

- ドメインコントローラーの深刻な脆弱性(CVE-2020-1472)[通称：Zerologon][6]
- Fortinet 製の VPN 機器の脆弱性(CVE-2018-13379)[7]
- Oracle WebLogic Server の脆弱性(CVE-2020-14750)[8]

(4) システム更改時等の作業誤り等に関するセキュリティリスク

一般に、システムの更改は、年末年始や大型連休等長期休暇のタイミングに実施することが多く、これらの作業に起因したシステム障害が発生し、長期休暇後にサービスに支障が生じることがあります[9]。

最近、システムの重要機器故障時の自動切り替え機能が、サプライヤーの仕様変更の連絡不徹底により設計どおりに動作しない事例、クラウドサービス上に構築したシステムを更改した際、クラウド事業者側の仕様変更の連絡不徹底により、クラウドに保存した機密情報が外部に公開される状態となる事例など、不十分なサプライチェーン管理によってもたらされるトラブルが散見されています。

参考 URL

- 年末年始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/alert20201217.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
- 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
- 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

---

[6] *IPA「更新:Microsoft 製品の脆弱性対策について(2020 年 8 月)(2020/9/28)」、https://www.ipa.go.jp/security/ciadr/vul/20200812-ms.html (2020/12/22 閲覧)*

[7] *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 (2020/12/22 閲覧)*

[8] *JPCERT/CC「2020 年 10 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起(2020/11/4)」、https://www.jpcert.or.jp/at/2020/at200040.html (2020/12/22 閲覧)*

[9] *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 (2020/12/22 閲覧)*