TLP:WHITE【全分野】

別紙

2021 年 12 月 15 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

# 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)

重要インフラ事業者等においては、ランサムウエア被害や情報漏えいが多数発生しています。被害の予防、緩和のためには、リスクを把握し、管理することが重要です。長期休暇に伴う重要インフラ所管省庁を含めた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に努めてください。

取り分け最近は、Emotet の活動再開や、攻撃者が、管理が不十分な機器から侵入して、ランサムウエアによるサイバー攻撃が多数発生しています。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加え、次に掲げるリスク要因を含めることが必要です。

① ランサムウエアに関するセキュリティリスク
② 新たに確認された脆弱性に関するセキュリティリスク
③ Emotet の活動再開のリスク
④ サプライチェーンに起因するリスク
⑤ 長期休暇に伴うリスク

長期休暇中に緊急時の対応が出来る態勢になっているか、重要インフラ所管省庁を含めた連絡ルートの確認や、連絡先が最新であるか確認してください。

なお、基本的なアカウント保護対策としての、ID やパスワードを流用しないこと、長く複雑なパスワードを設定すること、多要素認証を導入すること等の基本的対策についても、こうした機会を活用して確認することが肝要です。

## 1. ランサムウエアに関するセキュリティリスク

ランサムウエアの具体的な予防策、感染した場合の緩和策、対応策等の具体例については当センターの注意喚起[1]を参考にしてください。

企業情報、個人情報の窃取や金銭の要求を目的としたランサムウエアによる攻撃が多数発生しています。重要インフラ事業者等においては、情報窃取やデータの暗号化等の被害は、経済・社会に大きな影響を与えることを踏まえ、予防策、感染した場合の緩和策、対応策等を検討してください。

国内のランサムウエア感染事例において、バックアップも暗号化されて、復旧できない事例が発生しています。こうしたことを防ぐため、当センターがこれまで発出した注意喚起において、一般的なグッドプラクティスの例(321 ルールによるバックアップ)を紹介してきましたが、こうした対策がなされていれば、防止できたものでした。

[1] *NISC「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(2021/4/30)」、https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf (2021/12/14 閲覧)*

このため、改めて、321 ルールを応用したランサムウエア対策のバックアップ手法の例を説明します。図に示すとおり、①データを 3 つ保存する、②バックアップファイルを異なる 2 種類の媒体に保存する、③1 つをオフラインに保管する方法です。この手法はランサムウエア被害を受けた場合の迅速な復旧対策の一例です。このほかにも対策手法が提案されていますので、自組織の実情とデータの重要度に応じ、適切な対策を検討し、実施してください。


図 バックアップの 321 ルールを応用したランサムウエア対策の例

## 2. 新たに確認された脆弱性に関するセキュリティリスク対応

ソフトウエアは、日々新しい脆弱性が発見されており、ソフトウエアの導入後に適切な管理を行う必要があります。長年使用されずにネットワークに設置したままの機器、海外拠点の機器に対してセキュリティパッチの適用等の脆弱性管理がなされているか確認してください。シャドウ IT 等の管理が不十分な機器から侵害される例がみられており、IT 資産管理を徹底してください。

当センターは、以下の脆弱性について注意喚起を行っているところですが、改めて対応状況について再確認してください。

- Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）[2]
- Movable Type の深刻な脆弱性(CVE-2021-20837)[3]
- Apache HTTP Server のパストラバーサルの脆弱性(CVE-2021-41773)[4]
- Ivanti(旧 Pulse Secure)製の VPN 機器の脆弱性(CVE-2021-22937)[5]

米国 CISA は、公表されている脆弱性のうち、攻撃が観測されている注意すべき脆弱性について Web で公開[6]していますので、参考にしてください。

## 3. Emotet の活動再開のリスク

マルウエア Emotet が、2021 年 11 月から活動再開し、国内においても攻撃メールが確認されています。従来の添付ファイルから感染させる攻撃手法に加え、Adobe 製ソフ

---

[2] *JPCERT/CC「Apache Log4j の任意のコード実行の脆弱性(CVE-2021-44228)に関する注意喚起(2021/12/11)、https://www.jpcert.or.jp/at/2021/at210050.html (2021/12/14 閲覧)」*

[3] *JPCERT/CC「Movable Type の XMLRPC API における脆弱性(CVE-2021-20837)に関する注意喚起(2021/10/20)」、https://www.jpcert.or.jp/at/2021/at210047.html (2021/12/14 閲覧)*

[4] *JPCERT/CC「Apache HTTP Server のパストラバーサルの脆弱性(CVE-2021-41773)に関する注意喚起(2020/10/8)」、https://www.jpcert.or.jp/at/2021/at210043.html (2021/12/14 閲覧)*

[5] *NIST「CVE-2021-22937 Detail(2021/8/16)」、https://nvd.nist.gov/vuln/detail/CVE-2021-22937 (2021/12/10 閲覧)*

[6] *CISA「KNOWN EXPLOITED VULNERABILITIES CATALOG(2021/11/3)」、https://www.cisa.gov/known-exploited-vulnerabilities-catalog (2021/12/10 閲覧)*

トウエアを装った不正な Windows アプリのインストールを促し、感染させる新たな手法[7]が確認されています。

セキュリティポリシーによって、あらかじめ感染に繋がる OS やアプリケーションの機能等の制限や、感染源となるファイルが個人に配信される前に隔離・駆除又は無害化する組織的な対策に加え、メールの本文中の URL や添付ファイルを安易に開かない個人の取組を行う必要があります。

## 4. サプライチェーンに起因するリスク

サプライチェーンに起因する重要インフラサービス障害の連鎖に係るリスクに関して、考慮する必要があります。例えば、CDN やクラウドサービス等の連携先システム障害に起因する可用性のリスクがあります。外部調達や外部サービス等を利用する際は、それらがダウンした際も重要インフラサービスの提供に問題がないか確認してください。

## 5. 長期休暇に伴うリスク

長期休暇明けに多数のメールを確認する際、不審な添付ファイルを開いたり、リンク先にアクセスしたりしないようにしてください。メールを利用したフィッシング攻撃が起点となり、侵害される事例が多数発生しています。Web メールサービス等のアカウントを標的としたフィッシングや Emotet 等、攻撃は常に変化しているため、継続的な対策が必要です。

参考 URL

- 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
- ランサムウェア対策に関する注意喚起(医療 ISAC)
  https://www.m-isac.jp/2021/12/02/recommend01/
- Reducing the Significant Risk of Known Exploited Vulnerabilities (CISA)
  https://cyber.dhs.gov/bod/22-01/
- 【注意喚起】マルウェア Emotet が 10 カ月ぶりに活動再開、日本も攻撃対象に(LAC)
  https://www.lac.co.jp/lacwatch/alert/20211119_002801.html
- 「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて攻撃活動再開後の状況／被害相談の例（2021 年 12 月 9 日 追記）(IPA)
  https://www.ipa.go.jp/security/announce/20191202.html#L17
- CDN が原因で世界規模のネット障害(日経クロステック)
  https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800012/071500144/
- Web メールサービスのアカウントを標的としたフィッシングに関する注意喚起(JPCERT/CC)
  https://www.jpcert.or.jp/at/2021/at210049.html

[7] *Bleeping Computer「Emotet now spreads via fake Adobe Windows App Installer packages(2021/12/1)」、https://www.bleepingcomputer.com/news/security/emotet-now-spreads-via-fake-adobe-windows-app-installer-packages/ (2021/12/14 閲覧)*