資料４－１

令和 6 年 6 月 7 日
内閣サイバーセキュリティセンター

重要インフラを取り巻く情勢について

重要インフラは、豊かで便利な国民社会を支えている。機能性、コストなどの観点から重要インフラの IT 依存度は年々高まってきている。その一方で、重要インフラを取り巻く国際情勢、サイバー情勢、技術動向は時々刻々変化してきており、重要インフラの機能保証を確保していくためには、重要インフラを取り巻く情勢を把握し、関係者間で共有し、論点、価値観の共有が重要である。また、日々発生するサイバーインシデントを分析して得られた結果を共有することは、重要インフラの強靭性を高める観点から重要である。

このため、四半期ごとの重要インフラを取り巻く情勢分析と情報提供されたインシデント分析結果から得られた知見を共有する。

添付資料

資料４－２

サイバーセキュリティを取り巻く情勢(2023 年度第 4 四半期)

【目的】

サイバーセキュリティ技術の急速な進展により、重要インフラを取り巻く情勢は急速な変化を続けている反面、変化に追随することは容易とは言えなくなってきました。

本報告は、サイバーセキュリティに係る国外政策、国内外情勢、技術動向及びリスク関連動向に関して、2023 年度第 4 四半期(1 月～3 月)の主な公開情報をまとめたものであり、サイバーセキュリティを取り巻く情勢の把握の一助とすることを目的に編纂したものです。

【注意事項】

本報告は、公開情報をもとに作成したものである特性から、情報の真偽について保証するものではありません。御活用の際は御留意ください。

1. 国外サイバーセキュリティ政策

1.1. 米国

1.1.1. 上下水道セクターのサイバーインシデント対応ガイド

- ○ 2024 年 1 月 18 日、サイバーセキュリティ・インフラセキュリティ庁(CISA)、連邦捜査局(FBI)、環境保護庁(EPA)が、上下水道(WWS)セクター向けのインシデント対応ガイドを発表 [1]。WWS セクターへの継続的な侵害や障害は、重要インフラ全体に連鎖的な影響が及ぶ可能性があるとし、WWS セクターのサイバーセキュリティ強化を目指す。
- ○ 本ガイドでは、サイバーインシデントのライフサイクルの各段階において、特定の連邦機関との協力の適合性と手段について WWS セクターの事業者に対して助言する。事業者は本ガイドを利用することにより、サイバーインシデント発生前、発生中、発生後の各段階において、インシデント対応計画を補強することができる。

1.1.2. NIST サイバーセキュリティフレームワーク 2.0

- ○ 2024 年 2 月 26 日、米国国立標準技術研究所(NIST)は、NIST サイバーセキュリティフレームワーク(CSF)2.0 を公表 [2]。
- ○ CFS は企業や組織が行うべき施策を機能毎に整理。従来の Identify(識別)、Protect(防御)、Detect(検知)、Respond(対応)、Recover(回復)に加え、

---

[1] *CISA「Water and Wastewater Sector – Incident Response Guide(2024/1/18)」、https://www.cisa.gov/resources-tools/resources/water-and-wastewater-sector-incident-response-guide-0 (2024/5/10 閲覧)*

[2] *NIST「NIST Releases Version 2.0 of Landmark Cybersecurity Framework(2024/2/26)」、https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework (2024/3/18 閲覧)*

CSF2.0 で新たに Govern（ガバナンス）を追加。

○ また、ガイダンスの対象範囲を「重要インフラ」から「全ての組織」に拡大し、サイバーセキュリティが財務等の他のリスクと共に考慮すべきであることを強調。クイックスタートガイド、成功した導入事例、参考文献が検索できるカタログを追加。

1.1.3. 港湾のサイバーセキュリティ強化策

○ 2024 年 2 月 21 日、バイデン大統領は、米国の船舶、港湾及び臨海施設の保護に関する規則の改正に関する大統領令 [3]に署名し、海上のサイバー脅威に直接対処する国土安全保障省(DHS)の権限を強化 [4]した。この大統領令でサイバーインシデントの報告義務を制定し、DHS 傘下の沿岸警備隊は、サイバー脅威をもたらす船舶の移動の管理や船舶・施設を検査できる権限を有する。

○ 沿岸警備隊は、中国製の船舶対陸上クレーンに対するサイバーリスク管理措置に関する海上保安指令を発行予定であり、海上輸送システムにおける国際基準及び業界基準を満たす最低限のサイバーセキュリティ要件を定める規則案を公表。

○ バイデン政権は、今後 5 年間で港湾インフラへ 200 億ドルを投資し、米国の港湾クレーン生産能力を再構築する意向。

1.1.4. 中国国家が主導するサイバー活動への注意喚起

○ 2024 年 2 月 7 日、CISA、NSA、FBI 及びパートナーは、中国国家に支援された攻撃グループ「Volt Typhoon」に関する勧告を発表 [5]。米国との重大な危機や紛争が発生した際に、米国の重要インフラを中断・破壊するサイバー攻撃に備えて、IT ネットワークに事前に侵入し準備していると評価し、重要インフラ組織に警告。

○ 2024 年 3 月 19 日、CISA、NSA、FBI 及びパートナーは、共同ファクトシート「中華人民共和国の国家支援を受けたサイバー活動：重要インフラのリーダ

---

[3] *THE WHITE HOUSE「Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States(2024/2/21)」、https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/21/executive-order-on-amending-regulations-relating-to-the-safeguarding-of-vessels-harbors-ports-and-waterfront-facilities-of-the-united-states/（2024/3/18 閲覧）*

[4] *THE WHITE HOUSE「FACT SHEET: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports(2024/2/21)」、https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/（2024/3/18 閲覧）*

[5] *CISA「PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure(2024/2/7)」、https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a（2024/5/28 閲覧）*

ーのための行動」を発表 [6]。重要インフラ企業のリーダーに対し、「Volt Typhoon」の脅威から組織を守るために、共同ファクトシートで提供されているガイダンスを読むよう強く求めている。

1.1.5. 中国の攻撃グループ「APT31」に対する制裁

- 2024 年 3 月 25 日、米国政府は、米国を標的としたサイバー攻撃に関与したとして、中国政府と関連する「APT31」に対する一連の制裁措置を実施 [7]。
- 財務省外国資産管理局は、中国の企業 1 社と同社に所属する個人 2 人を金融制裁対象に指定 [8]。英国の外務・英連邦・開発省(FCDO)と共同で実施 [9]。
- 司法省は、上記個人 2 人を含む中国籍 7 人を、コンピュータ侵入の共謀及び電信詐欺の共謀の罪で起訴 [10]。
- 国務省は、APT31 と被告に関する情報に対して、最高 1,000 万ドルの司法報奨金を提供すると発表。

1.2. 中国

1.2.1. データセキュリティに関する 3 か年計画

- 2024 年 1 月 4 日、中国政府は、生産要素としてのデータ利用を促進し、経済・社会の発展を推進する上でデータがより重要な役割を果たすための 3 か年行動計画を発表 [11]。同計画では、2024 年からの 3 年間で、データの高度応用の促進、データ供給の質の確保、データ流通環境の改善、データセキュリティ強化のための取組を実施。
- 2024 年 2 月 26 日、中国工業情報省は、「産業分野におけるデータセキュリティ能力の向上に関する実施計画(2024～2026 年)」を発表 [12]。同計画では、製造企業のデータ保護、データセキュリティの規制、データセキュリティ産業

---

[6] *CISA「PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders(2024/3/19)」、https://www.cisa.gov/resources-tools/resources/prc-state-sponsored-cyber-activity-actions-critical-infrastructure-leaders（2024/5/28 閲覧）*

[7] *U.S. department of State「U.S. Takes Action to Further Disrupt PRC Cyber Activities(2024/3/25)」、https://www.state.gov/u-s-takes-action-to-further-disrupt-prc-cyber-activities/（2024/5/21 閲覧）*

[8] *U.S. department of the treasury「Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure（2024/3/25)」、https://home.treasury.gov/news/press-releases/jy2205（2024/5/21 閲覧）*

[9] *GOV.UK「UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity(2024/3/25)」、https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity（2024/5/21 閲覧）*

[10] *U.S. department of justice「Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians(2024/3/25)」、https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived（2024/5/10 閲覧）*

[11] *中华人民共和国中央人民政府「《"数据要素×"三年行动计划(2024—2026 年)》发布(2024/1/4)、https://www.gov.cn/lianbo/bumen/202401/content_6924380.htm（2024/5/21 閲覧）*

[12] *中华人民共和国中央人民政府「工业领域数据安全能力提升实施方案（2024—2026 年）重点问应(2024/2/26)、https://www.gov.cn/zhengce/202402/content_6934385.htm（2024/5/16 閲覧）*

の支援の 3 つの能力を向上させるための 11 の実施項目を指定。

1.2.2. 政府の IT 機器から米国製半導体・OS を排除

- ○ 2024 年 3 月 24 日、政府機関が使用する PC とサーバーから、米国半導体大手 Intel 社及び Advanced Micro Devices 社の CPU を段階的に排除することを定めた IT 機器調達指針を導入したと報じられた[13]。
- ○ 同指針は、Microsoft 社の Windows OS や外国製のデータベースソフトウェアについても、国産製品に置き換えるように求めている。

2. 国外におけるサイバーセキュリティをめぐる情勢

2.1. 重要インフラ関連

2.1.1. レバノンのラフィク・ハリリ国際空港へのサイバー攻撃

- ○ 2024 年 1 月 7 日、レバノンの首都ベイルートのラフィク・ハリリ国際空港がサイバー攻撃を受け、フライト情報表示画面に、レバノンのキリスト教徒グループ「Soldiers of God」を騙り、イランが支援するレバノンを拠点とする過激派組織ヒズボラを批判するメッセージが表示されたと報じられた[14]。乗客の手荷物検査システムは一時的に混乱したが、フライトスケジュールに影響はなかった。
- ○ 同グループは、ソーシャルメディアで関与を否定、イスラエルが関与している可能性が高いとの見方もある。

2.1.2. 米国及び英国の水道分野へのランサムウェア攻撃

- ○ 2024 年 1 月 19 日、米国大手水道会社 Veolia North America 社は、都市水道部門でランサムウェア攻撃による被害が発生したと公表[15]。オンライン請求書支払いシステムで一部遅延が発生、上下水道処理業務に影響はなかったが、個人情報漏えいの可能性がある顧客への通知を実施。
- ○ 2024 年 2 月 12 日、英国大手水道会社 Southern Water 社は、IT システムに不正侵入されサーバーの一部からデータが窃取されたと公表[16]。1 月 22 日、ダークウェブに同社のデータが掲載されたことを受け、1 月 23 日に不審な活動を検知し調査を開始している旨を公表[17]。サービスへの影響はなかった。

---

[13] *FINANCIAL TIMES「China blocks use of Intel and AMD chips in government computers(2024/3/24)」、https://www.ft.com/content/7bf0f79b-dea7-49fa-8253-f678d5acd64a（2024/5/27 閲覧）*

[14] *The Record「Hackers disrupt Beirut airport with anti-Hezbollah message(2024/1/9)」、https://therecord.media/beirut-airport-hack-information-screens-baggage-screening（2024/5/10 閲覧）*

[15] *Veolia「Veolia Responds To Cyber Incident(2024/1/19)」、https://mywater.veolia.us/veolia-responds-cyber-incident（2024/5/21 閲覧）*

[16] *Southern Water「Cyber attack – update for customers(2024/2/12)」、https://www.southernwater.co.uk/latest-news/cyber-attack-update-for-customers-1/（2024/5/21 閲覧）*

[17] *Southern Water「Cyber investigation(2024/1/23)」、https://www.southernwater.co.uk/latest-news/cyber-investigation/（2024/5/21 閲覧）*

2.1.3. 米国 AT&T の大規模通信障害

- 2024 年 2 月 22 日、米国通信大手 AT&T 社で通信障害が発生し、全米で長時間にわたり、電話やメッセージ、インターネット、緊急通報サービスが利用できなくなった [18]。連邦通信委員会(FCC)の公共安全・国土安全保障局が調査を実施 [19]、警察・消防機関が緊急通報サービスに関する情報を SNS で周知 [20]。
- 2024 年 2 月 25 日、AT&T 社は、ネットワーク拡張作業の手順の誤りが原因であり、通信障害により影響を受けた可能性のある顧客に対し、1 日あたりの平均料金に相当する金額を返金すると発表 [21]。

2.1.4. 米国 Change Healthcare 社へのランサムウェア攻撃

- 2024 年 2 月 21 日、米国の医療保険・医療サービス大手 UnitedHealth グループ傘下の Change Healthcare 社が、「BlackCat」ランサムウェアグループによるサイバー攻撃を受け、米国の医療及び請求・支払いのシステムに影響 [22]。
- 2024 年 2 月 12 日、漏えいした認証情報を悪用して、同社が使用する多要素認証が設定されていない Citrix ポータルから侵入、9 日後にランサムウェアが展開された。
- 2024 年 4 月 22 日、主要なプラットフォーム及び製品の約 80%の機能が復旧 [23]、5 月 7 日、インシデント対応が完了。

2.2. 国家支援等を受けたとされる攻撃グループの概況

2.2.1. 中国関連

- 2024 年 1 月、「BlackWood」について、中国、日本及び英国の個人や企業に対して、正規ソフトウェアのアップデートを悪用して、高度なインプラントである NSPX30 を配布する標的型攻撃を行っていると ESET 社が報告 [24]。
- 2024 年 2 月、「i-Soon 社」について、同社から漏えいしたデータから、中国と

---

[18] *AT&T「Network Update(2024/2/22)」、https://about.att.com/pages/network-update (2024/5/27 閲覧)*

[19] *X「The FCC の投稿(2024/2/23)」、https://twitter.com/FCC/status/1760737935178256756 (2024/5/27 閲覧)*

[20] *X「San Francisco Fire Department Media の投稿(2024/2/22)」、https://twitter.com/SFFDPIO/status/1760618741422072177 (2024/5/27 閲覧)*

[21] *AT&T「Addressing the February 22 outage(2024/2/25)」、https://about.att.com/ecms/dam/snrdocs/network-employee-letter.pdf (2024/5/21 閲覧)*[22] *UnitedHealth Group「Frequently Asked Questions: What can you tell us about the ransomware attack?」、https://www.unitedhealthgroup.com/ns/changehealthcare/faq.html (2024/21 閲覧)*

[22] *UnitedHealth Group「Frequently Asked Questions: What can you tell us about the ransomware attack?」、https://www.unitedhealthgroup.com/ns/changehealthcare/faq.html (2024/21 閲覧)*

[23] *UnitedHealth Group「UnitedHealth Group Updates on Change Healthcare Cyberattack(2024/4/22)」、https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html (2024/5/21 閲覧)*

[24] *ESET「NSPX30: A sophisticated AitM-enabled implant evolving since 2005(2024/1/24)」、https://www.welivesecurity.com/en/eset-research/nspx30-sophisticated-aitm-enabled-implant-evolving-since-2005/ (2024/2/16 閲覧)*

つながりのある APT 攻撃キャンペーンとの関連性が発見されたと Palo Alto Networks 社が報告[25]。

- 2024 年 3 月、「Stately Taurus」について、ASEAN-オーストラリア特別サミット中に日本や ASEAN 加盟国の組織を標的としたマルウェア攻撃を行ったと Palo Alto Networks 社が報告[26]。

2.2.2. ロシア関連

- 2024 年 1 月、「Midnight Blizzard」について、Microsoft 社及び Hewlett Packard Enterprise 社が同社の電子メールへの不正アクセスを報告[27、28]。
- 2024 年 2 月、「NoName057(16)」等が、日本の企業や組織に対する攻撃を示唆する内容を Telegram に投稿。2024 年 3 月、「NoName057(16)」が運営する DDoSia プロジェクトについて、Sekoia.io 社が 2024 年の活動概要を報告[29]。
- 2024 年 3 月、「Sandworm」について、ウクライナ侵攻開始時に使用された破壊型マルウェア AcidRain の新しい亜種 AcidPour を確認したと SentinelOne 社が報告[30]。

2.2.3. 北朝鮮関連

- 2024 年 1 月、「APT37」による報道機関や北朝鮮問題の専門家を標的とするキャンペーンについて、SentinelOne 社が報告[31]。将来の攻撃でサイバーセキュリティ関連の組織や個人を標的とする可能性が高いと指摘。
- 2024 年 2 月、ドイツ連邦憲法擁護庁(BfV)と韓国国家情報院(NIS)は、北朝鮮の攻撃グループによる防衛部門に対するサイバー攻撃についての勧告を発

---

[25] Palo Alto Networks「Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaign (2024/2/23)」、https://unit42.paloaltonetworks.com/i-soon-data-leaks/ (2024/3/4 閲覧)

[26] Palo Alto Networks「ASEAN Entities in the Spotlight: Chinese APT Group Targeting (2024/3/26)」、https://unit42.paloaltonetworks.com/chinese-apts-target-asean-entities/ (2024/4/19 閲覧)

[27] Microsoft「Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard(2024/1/19)」、https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/ (2024/2/5 閲覧)

[28] SEC「FORM 8-K, HEWLETT PACKARD ENTERPRISE COMPANY(2024/1/19)」、https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/1645590/000164559024000009/hpe-20240119.htm (2024/2/5 閲覧)

[29] sekoia「NoName057(16)'s DDoSia project: 2024 updates and behavioural shifts(2024/3/1)」、https://blog.sekoia.io/Noname05716-Ddosia-project-2024-updates-and-behavioural-shifts/ (2024/3/15 閲覧)

[30] SentinelOne「AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine(2024/3/21)」、https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/ (2024/4/22 閲覧)

[31] SentinelOne「ScarCruft | Attackers Gather Strategic Intelligence and Target Cybersecurity Professionals (2024/1/22)」、https://www.sentinelone.com/labs/a-glimpse-into-future-scarcruft-campaigns-attackers-gather-strategic-intelligence-and-target-cybersecurity-professionals/ (2024/2/1 閲覧)

表 [32、33]。一部は、「Lazarus」によるキャンペーン Operation Dream Job に関連。

- ○ 2024 年 3 月、「Kimsuky」に関連するマルウェア BabyShark の亜種と考えられる新たなマルウェア ToddlerShark について、Kroll 社が報告 [34]。攻撃者は、ConnectWise ScreenConnect の脆弱性を悪用して ToddlerShark を展開。

3. 国内におけるサイバーセキュリティをめぐる情勢

3.1. 重要インフラ関連

3.1.1. 能登半島地震における通信サービスへの影響

- ○ 2024 年 1 月 1 日 16 時 10 分頃、石川県能登地方で最大震度 7 を観測する地震が発生 [35]し、一部エリアで通信サービスが利用できない、又は利用しづらい状況が発生。
- ○ 2024 年 1 月 6 日、NTT ドコモと KDDI は、共同で船舶上に携帯電話基地局の設備を設置した「船上基地局」の運用を開始 [36、37]。NTT と KDDI は 2020 年に社会課題の解決に取り組む社会貢献連携協定を締結しており、本運用はその一環。
- ○ 2024 年 1 月 15 日、KDDI は、土砂崩れなどによる進入困難箇所を除き、移動基地局の搬入や、基地局への衛星ブロードバンド Starlink を活用したアンテナの設置により応急復旧 [38]。
- ○ 2024 年 1 月 17 日、NTT ドコモも、進入困難箇所を除き応急復旧 [39]。2024 年 3 月 21 日、舳倉島(石川県輪島市)を除くエリアにおいてサービスが復旧 [40]。

---

[32] *BfV「Warning of North Korean cyber threats targeting the Defense Sector(2024/2/19)」、https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?_blob=publicationFile&v=2（2024/3/4 閲覧）*

[33] *NIS「韓獨 정보기관, 북한의 방산기술 사이버위협에 경고(2024/2/19)」、https://www.nis.go.kr/CM/1_4/view.do?seq=282（2024/3/4 閲覧）*

[34] *Kroll「TODDLERSHARK: ScreenConnect Vulnerability Exploited to Deploy BABYSHARK Variant(2024/3/5)」、https://www.kroll.com/en/insights/publications/cyber/screenconnect-vulnerability-exploited-to-deploy-babyshark（2024/4/8 閲覧）*

[35] *気象庁「令和6年能登半島地震の地震活動と防災事項ポータルサイト」、https://www.data.jma.go.jp/kanazawa/shosai/notojishinportal.html（2024/5/21 閲覧）*

[36] *NTT ドコモ「令和 6 年能登半島地震に伴う「船上基地局」運用の実施について -NTT ドコモ、KDDI 共同で海上から通信を復旧-(2024/1/6)」、https://www.docomo.ne.jp/info/news_release/detail/20240106_00_m.html（2024/5/21 閲覧）*

[37] *KDDI「令和 6 年能登半島地震に伴う「船上基地局」運用の実施について(2024/1/6)」、https://newsroom.kddi.com/news/detail/6.html（2024/5/21 閲覧）*

[38] *KDDI「令和 6 年能登半島地震による通信ネットワークの復旧経過状況について(2024/1/16)」、https://newsroom.kddi.com/news/detail/kddi_pr-1092.html（2024/5/21 閲覧）*

[39] *NTT ドコモ「令和 6 年能登半島地震の影響による通信サービスの復旧状況について(2024/1/17)」、https://www.docomo.ne.jp/info/news_release/2024/01/17_00.html（2024/5/21 閲覧）*

[40] *NTT ドコモ「【復旧】令和 6 年能登半島地震の影響により、一部エリアで携帯電話サービスがご利用できない、またはご利用しづらい状況について(2024/1/1)」、https://www.docomo.ne.jp/info/network/kanto/pages/240101_00_m.html（2024/5/21 閲覧）*

舳倉島でのサービス復旧時期は未定。

3.1.2. 埼玉県健康づくり事業団へのランサムウェア攻撃

- 2024 年 1 月 31 日、埼玉県内で健康診断業務等を行う公益財団法人埼玉県健康づくり事業団は、X 線画像読影システムがランサムウェアに感染し、個人情報が漏えいした可能性がある旨を公表[41]。2024 年 12 月までに新たな X 線画像読影システムを構築する予定[42]。
- インターネットに接続している VPN 経由で偵察活動が行われた後、ランサムウェアに感染。フォレンジック調査により、情報漏えいの痕跡は確認されなかったが、データ窃取の有無を完全に断定することはできないと報告。
- 被害を受けた機器に保存されていた個人情報は、約 94 万人分の X 線画像、超音波画像、モアレ検査画像及び画像に付帯する情報(氏名、年齢、生年月日、問診、所見と判定、学校名等)。埼玉県[43]を含む複数の自治体及び事業者[44]は、本事案の影響を受けた旨を公表。

3.1.3. 国分生協病院へのランサムウェア攻撃

- 2024 年 2 月 27 日、鹿児島県霧島市の国分生協病院の画像管理サーバーがランサムウェアに感染し、サーバー内に保存された診療記録のファイルの一部が暗号化され、救急及び一般外来の受け入れを制限、病院全体でインターネット接続を停止[45]。
- 2024 年 3 月 18 日、画像管理サーバーの仮復旧作業が完了、救急及び一般外来の受入を再開[46]。
- 原因は、病院内に設置されたネットワーク機器が、病院内のコンピュータに外部から認証なしでリモートデスクトップ接続が可能な設定になっており、更に感染サーバーにはマルウェア対策ソフトが設定されていなかったと報告。

3.2. その他

3.2.1. うるう年に関連するシステム障害

- 2024 年 2 月 29 日、新潟県、神奈川県、岡山県、愛媛県警察が運営する運

---

41 埼玉県健康づくり事業団「X 線画像読影システムへの不正アクセスについて(2024/1/31)」、https://www.saitama-kenkou.or.jp/pdf/news_20240131.pdf (2024/5/21 閲覧)

42 埼玉県健康づくり事業団「X 線画像読影システムへの不正アクセスについて(2024/3/28)」、https://www.saitama-kenkou.or.jp/pdf/news_20240328.pdf (2024/5/21 閲覧)

43 埼玉県「業務委託先事業者への不正アクセスについて(2024/5/2)」、https://www.pref.saitama.lg.jp/a0710/news/page/news2024050201.html (2024/5/21 閲覧)

44 結核予防会 総合健診推進センター「委託医療機関(公益財団法人埼玉県健康づくり事業団)の X 線画像読影システムへの不正アクセス攻撃に関するご報告とお詫びについて(2024/5/9)」、https://www.ichiken.org/information/2704-20240509/ (2024/5/21 閲覧)

45 鹿児島県医療生活協同組合 国分生協病院「「画像管理サーバー」の障害発生について(2024/3/4)」、https://kokubu-seikyo.jp/2024/03/04/post-1537/ (2024/5/15 閲覧)

46 鹿児島県医療生活協同組合 国分生協病院「「画像管理サーバー」の仮復旧 及び 救急・一般外来の受入再開について(2024/3/18)」、https://kokubu-seikyo.jp/2024/03/18/post-1545/ (2024/5/21 閲覧)

転免許センターでシステム障害が発生し、運転免許証の更新や新規取得の手続きが停止。報道によると、「免許作成機のプログラムにおいて、うるう年を西暦で設定すべきところを和暦に設定していたため」と県警から説明があった[47]。

- 2024 年 2 月 29 日、スギ薬局グループにおいて、全国の約 1,300 ある調剤ができる店舗で、うるう日が原因とみられるシステム障害が発生し、処方箋の登録や会計が一時停止したと報じられた[48]。
- 国外においても、ニュージーランドのガソリンスタンドでの障害、スウェーデンの大手食料品小売店のカード決済の障害が報じられている[49]。また、Citrix 社や Sophos 社の製品においても、うるう年が原因とみられるソフトウェアの不具合が発生。

[47] *日経×TECH「運転免許センターで同時発生した「うるう年」の不具合、和暦設定が引き金に(2024/4/12)」、https://xtech.nikkei.com/atcl/nxt/column/18/00001/09151/（2024/5/21 閲覧）*

[48] *NHK「スギ薬局グループ システム障害が復旧 「うるう日」が原因か(2024/2/29)」、https://www3.nhk.or.jp/news/html/20240229/k10014374401000.html（2024/5/21 閲覧）*

[49] *BleepingComputer「Citrix, Sophos software impacted by 2024 leap year bugs(2024/2/29)」、https://www.bleepingcomputer.com/news/software/citrix-sophos-software-impacted-by-2024-leap-year-bugs/（2024/5/21 閲覧）*

資料４－３

重要インフラにおける情報共有件数について(2023 年度)

「重要インフラのサイバーセキュリティに係る行動計画」に基づき、内閣官房(NISC)、関係省庁、関係機関及び重要インフラ事業者等との間で行われた情報共有の実施状況は以下のとおり。

（単位:件）

実施形態	FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	FY2023 2Q	FY2023 3Q	FY2023 4Q	FY2023 計
重要インフラ事業者等からNISCへの情報連絡(※)	269	309	407	302	99	53	63	57	272
関係省庁・関係機関からのNISCへの情報共有	16	16	6	2	0	7	3	9	19
NISCからの情報提供	38	64	91	83	25	37	34	31	127

（※）重要インフラ事業者等からNISCへの情報連絡は以下のとおり。

1. 事象別内訳

事象の類型			FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	FY2023 2Q	FY2023 3Q	FY2023 4Q	FY2023 計
未発生の事象		予兆・ヒヤリハット	12	28	25	28	9	1	2	0	12
発生した事象	機密性を脅かす事象	情報の漏えい	13	23	29	17	9	4	4	3	20
	完全性を脅かす事象	情報の破壊	11	12	20	15	5	6	3	4	18
	可用性を脅かす事象	システム等の利用困難	158	157	181	145	56	31	30	31	148
	上記につながる事象	マルウェア等の感染	9	18	46	38	2	4	8	6	20
		不正コード等の実行	5	3	2	1	1	0	1	1	3
		システム等への侵入	14	26	24	22	6	2	1	4	13
		その他	47	42	80	36	11	5	14	8	38

2. 原因別類型（複数選択）

原因の類型		FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	FY2023 2Q	FY2023 3Q	FY2023 4Q	FY2023 計
意図的な原因	不審メール等の受信	13	9	47	39	4	0	3	0	7
	ユーザＩＤ等の偽り	12	9	7	7	4	0	0	3	7
	DDoS攻撃等の大量アクセス	20	10	19	28	16	6	2	8	32
	情報の不正取得	8	13	13	10	5	2	3	0	10
	内部不正	0	0	1	1	0	1	1	0	2
	適切なシステム等運用の未実施	11	23	15	8	2	0	3	2	7
偶発的な原因	ユーザの操作ミス	6	18	10	12	4	0	3	3	10
	ユーザの管理ミス	6	13	14	7	4	0	0	4	8
	不審なファイルの実行	7	7	22	26	1	0	1	0	2
	不審なサイトの閲覧	5	3	6	4	4	1	4	2	11
	外部委託先の管理ミス	39	56	107	49	14	12	19	5	50
	機器等の故障	62	39	38	43	8	12	7	11	38
	システムの脆弱性	16	38	32	12	11	6	15	3	35
	他分野の障害からの波及	4	7	10	7	1	2	2	0	5
環境的な原因	災害や疾病等	13	9	3	5	0	1	0	0	1
その他の原因	その他	33	35	48	29	14	10	10	7	41
	不明	53	68	79	62	21	6	8	16	51

3. サイバー攻撃による事象の種別内訳（情報連絡を基にNISC重要インフラ防護担当において分析・再集計）

サイバー攻撃の類型		FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	FY2023 2Q	FY2023 3Q	FY2023 4Q	FY2023 計
総計		87	100	174	143	52	18	26	27	123
	ランサムウェア攻撃	8	13	46	30	8	5	14	9	36
	ランサムウェアを除くマルウェア感染	11	8	29	27	2	1	0	1	4
	DDoS攻撃等の大量アクセス	14	4	15	25	10	6	3	9	28
	その他	54	75	84	61	32	6	9	8	55

（注）FY:年度、Q:四半期

資料４－４

最近のインシデントから得られた教訓(2023 年度第４四半期)

1　趣旨

重要インフラサービスに関連したインシデント情報は、重要インフラ所管省庁を通じて内閣サイバーセキュリティセンターに集約されているが、これらの情報から教訓を案出し共有を図る等、これらの情報の有効活用を促進していくことを考えている。なお、説明を簡潔にするため、複雑な状況を簡易に整理しており、一部具体性に欠ける記載がある旨を御承知置きいただきたい。

2　インシデントから得られた教訓

VPN 機器の脆弱性を突かれランサムウェアに感染した事例、DDoS 攻撃とみられる大量アクセスを受けた事例などにより、サービスの提供に支障が生じた事例が報告された。外部ネットワークに接続するネットワーク機器や内部ネットワークの構成については、攻撃があることを想定した上で提供するサービスの重要度に応じたものとするとともに、脆弱性対応など適切に管理することが重要。

○ ネットワーク接続に係る資産管理及び不正アクセスを前提とした多層防御が必要

ランサムウェアに感染したことによりサービスの提供に支障が出た事例が複数あり、中にはグループ会社にまで感染が拡大した事例もあった。リモートメンテナンス用の VPN 機器や委託先が管理・運用する VPN 機器が侵入口となっており、外部のネットワークと接続する機器の管理の重要性について再認識することが必要。

○ 適切な脆弱性への対応が必要

古いバージョンのままネットワーク機器を使用していたことが原因で不正アクセスを許す事例があった。また、脆弱性について認識していたが修正プログラムが公開されていなかったため特段の対応をせず使用を継続した事例や、緩和策を適用したものの当該緩和策の留意点の検討不足や継続的なネットワーク監視の必要性の認識の欠如していたことから、侵害を受けた事例があった。

○ 提供サービスの重要度に応じたシステム設計と適切な広報の実施が必要

DDoS 攻撃とみられる大量アクセスを受けた事例が複数あり、広報用ウェブサイトの閲覧障害だけでなく、ウェブサイトを活用したサービスの提供に支障が出た事例があった。サービス重要度に応じた DDoS 攻撃への耐性向上に加え、障害発生時の代替手段の確保と適切な広報などの事前の備えが必要。

○ 障害対応時における対応の事前準備が必要

障害の把握から経営層への報告を経て対策本部設置まで数分で対応した事例があった一方で、メンテナンス作業に伴う障害であるにもかかわらず、障害把握に数時間を要した上、対応策の実施の判断にも更に数時間を要した結果、長時間にわたりサービスの提供に影響が出た事例があった。障害発生時における初動対応、連絡体制の確立が必要。

（以上）