資料４

令和７年６月２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

参考資料

資料４－１

サイバーセキュリティを取り巻く情勢(2024 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、2024 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. ホワイトハウスが、U.S. Cyber Trust Mark の開始を公表

- ○ 2025 年 1 月 7 日、ホワイトハウスは、IoT 製品がサイバーセキュリティの脅威に対して適切に保護されているか否か、米国の消費者が簡単に確認することができる U.S. Cyber Trust Mark の開始を公表[1][2]。
- ○ 本ラベルは、米国で販売される同プログラムのサイバーセキュリティ基準を満たしたホームセキュリティカメラ、スマート家電、ガレージドアオープナー及びベビーモニターなどの IoT 製品に表示される。
- ○ 本ラベルには QR コードが添付され、消費者がスキャンすることで、製品のサポート期間、ソフトウェア・パッチ、セキュリティ・アップデートの自動更新の有無など、セキュリティ情報を確認することが可能。
- ○ この自主プログラムは、米国連邦通信委員会（FCC）が監督し、承認された第三者のサイバーセキュリティ・ラベル管理者が製品申請の評価、ラベル使用の承認及び消費者向け普及啓発などの活動を実施[3]。

---

[1] *The White House「White House Launches "U.S. Cyber Trust Mark", Providing American Consumers an Easy Label to See if Connected Devices are Cybersecure（2025/1/7）」、https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure/（2025/5/14 閲覧）*

[2] *FCC「U.S. Cyber Trust Mark（2025/1/7）」、https://www.fcc.gov/CyberTrustMark(2025/5/14 閲覧）*

[3] *FCC「FCC CREATES VOLUNTARY CYBERSECURITY LABELING PROGRAM FOR SMART PRODUCTS（2024/3/14）」、https://web.archive.org/web/20240316143613/https://docs.fcc.gov/public/attachments/DOC-401201A1.pdf(2025/5/14 閲覧）*

1.1.2. NIST が、NICE フレームワーク v2.0.0 を公表

- 2025 年 3 月 5 日、米国国立標準技術研究所（NIST）は、NICE フレームワーク v2.0.0 を公表 [4]。
- サイバーセキュリティに関する人材育成を推進するイニシアティブである NICE が提供する本フレームワークは、サイバーセキュリティ業務とその完了に必要な知識とスキルを説明するための共通言語を提供しており、官民や業界を問わず、キャリアの発見、教育と訓練、雇用及び人材育成に活用することが可能。
- v2.0.0 では、職務分類や作業内容の追加・更新、コンピテンシー分野の更新、重複又は冗長な TKS（タスク・知識・スキル）ステートメントの削除など、進化する業界のニーズとの整合性を確保 [5]。

1.1.3. ODNI が、年次脅威評価を公表

- 2025 年 3 月 25 日、米国国家情報長官室（ODNI）は、2025 年の年次脅威評価を公表 [6]。これは、米国インテリジェンス・コミュニティが公式に、米国国民、米国本土、そして世界における米国の利益に対する様々な脅威について評価したもの。
- 本報告書では、ロシア、中国、イラン及び北朝鮮が、個別又は集団により、他国を攻撃・脅迫し、米国の利益に挑戦していると詳述。
- サイバー犯罪については、金銭的な動機から医療システムや地方自治体など、米国の国民や経済に広範な影響を及ぼす可能性のある、防御が不十分な米国の標的狙い続けており、水道インフラについても、より一般的な標的となっていると指摘。

1.2. 英国

1.2.1. 英国政府が、AIのサイバーセキュリティに関する行動規範を公表

- 2025 年 1 月 31 日、英国政府は AI システムをサイバー攻撃から保護する新たな任意規範として AI サイバーセキュリティ行動規範を公表 [7]。
- 本行動規範は、システムに対する脅威の評価とリスク管理、システムオペレーターに対する適切な試験・評価の実施、サプライチェーンの保護及び定期的なセキュリティ・アップデートなど 13 の基本原則で構成さ

---

[4] *NIST「NICE FRAMEWORK RESOURCE CENTER」、https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center（2025/5/14 閲覧）*

[5] *NICE「NICE Framework Components v2.0.0 Summary of Changes（2025/3/5）」、https://www.nist.gov/system/files/documents/2025/03/10/NICE Framework V2 Summary of Changes %28March 2025%29_508compliant.pdf（2025/5/15 閲覧）*

[6] *ODNI「ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY（2025/3/25）」、https://www.odni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf（2025/5/15 閲覧）*

[7] *GOV.UK「Code of Practice for the Cyber Security of AI（2025/1/31）」、https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice/code-of-practice-for-the-cyber-security-of-ai（2025/5/15 閲覧）*

れており、これらの原則により、従来からのサイバーセキュリティの懸念と AI 特有の課題の両方に対処する包括的なフレームワークを形成。

○ 本行動規範のための実施ガイドも同時に公表し、企業が遵守すべきガイダンスと手続きをまとめて提供し、サイバー防衛の強化を支援。

1.3. フランス

1.3.1. ANSSI が、サイバー脅威の概要 2024 を公表

○ 2025 年 3 月 10 日、フランスサイバーセキュリティ庁（ANSSI）が、2024 年 1 月 1 日から 12 月 31 日までの期間のサイバーセキュリティの脅威や発生した重要なインシデントなどについてまとめたサイバー脅威の概要 2024 を公表[8]。

○ 2024 年、ANSSI に報告されたインシデントは、2023 年と比較して 15%の増加。特にオリンピックの聖火がフランスに到着する 5 月から、パラリンピックの閉会式が行われる 9 月までの期間において増加。

○ パリオリンピック・パラリンピックは、メディアへの露出など攻撃者にとって大きな機会を提供。ANSSI は恐喝やスパイ活動を目的とした攻撃に加え、ハクティビストによる攻撃も観察。ただ、これらの攻撃はいずれもオリンピックの円滑な運営に顕著な影響は与えていない。

○ その他、攻撃者による暗号化ネットワークの利用、サプライチェーン攻撃、ランサムウェア攻撃が継続的に行われていると指摘。

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. 米国のニューヨーク血液センターへのランサムウェア攻撃

○ 2025 年 1 月 26 日、ニューヨーク血液センター（NYBCe）のシステム上で不審な活動を検知[9]。調査の結果、ランサムウェア攻撃であることを確認し、特定のシステムをオフライン化するなどの措置とともに、復旧に向けた取組を実施。

○ これにより NYBCe の全ての事業部門が影響を受けたが、2025 年 2 月 3 日、ドナーセンターの運営やコミュニティの献血活動など、全ての活動を再開。

2.1.2. 英国の水道供給業者のランサムウェア攻撃による被害額を公表

○ 2025 年 2 月 26 日、英国の南部地域の 270 万人の顧客に水道サービスと

---

[8] *ANSSI「CYBER THREAT OVERVIEW 2024（2025/3/10）」、https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-004.pdf（2025/5/15 閲覧）*

[9] *New York Blood Center Enterprises「New York Blood Center Enterprises Cybersecurity Incident Update（2025/2/3）」、https://www.nybce.org/news/articles/cyber/（2025/5/16 閲覧）*

470 万人の顧客に下水サービスを提供している水道事業者の Southern Water が、2024 年 2 月に発生したランサムウェア攻撃により、年間を通じて 450 万ポンド（約 8 億 5 千万円）の費用が発生したことを明らかにした[10]。

- ○ 本インシデントは、システムのサーバーの一部データが、外部からの不正な侵入により盗まれたが、運用、財務システム及び顧客向けシステムには影響はなかった。
- ○ 費用は、インシデントへの対処として、外部のサイバーセキュリティ専門家や法律顧問の雇用、また、個人情報が漏えいした可能性のある顧客への連絡などに要したもの。

2.1.3. マレーシアのクアラルンプール国際空港のサイバー攻撃

- ○ 2025 年 3 月 25 日、国家サイバーセキュリティ庁（NACSA）及び空港を管理・運営する管理会社のマレーシア・エアポートは、共同声明により、2025 年 3 月 23 日に、マレーシアのクアラルンプール国際空港（KLIA）の特定のシステムに影響を与えるサイバー攻撃があったと公表[11]。
- ○ 同共同声明では、空港の運営には影響はないとしているが、10 時間以上、フライト情報の表示やチェックインウンター、手荷物取扱サービスに影響があり、航空会社と空港スタッフは手動操作に頼らざるを得なくなったとの報道もある。

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. 福岡県の税務システムの障害

- ○ 2025 年 1 月 30 日、福岡県において、県税の課税及び納税情報を管理している税務システムの障害により、県税の支払いや納税証明書等の発行の一部が不可となる事象が発生。
- ○ 税務システムのサーバを構成する機器の一部の部品交換をした際、必要なソフトウェアの設定変更を行わなかったことが原因。これにより、バックアップデータの接続に障害が生じ、情報の参照や更新ができない状況が発生したもの[12]。

---

[10] *Southern Water「Annual Report and Financial Statements 2023-2024」、https://www.southernwater.co.uk/media/mmcogsam/southern-water-annual-report-2023-24.pdf（2025/5/16 閲覧）*

[11] *MALAYSIA AiIRPORTS「JOINT STATEMENT BY NATIONAL CYBER SECURITY AGENCY (NACSA) AND MALAYSIA AIRPORTS（2025/3/25）」、https://www.malaysiaairports.com.my/en/media-centre/news/1562（2025/5/16 閲覧）*

[12] *福岡県「税務システムの障害について（2025/1/31）」、https://www.pref.fukuoka.lg.jp/contents/zeishisu-info.html（2025/5/16 閲覧）*

○ 2025 年 2 月 3 日、通常どおり納税証明書の発行等の業務を再開 [13]。

3.1.2. 宇都宮セントラルクリニックのランサムウェア感染

○ 2025 年 2 月 18 日、宇都宮セントラルクリニックは、同病院のサーバーがランサムウェア攻撃を受けたことに伴う情報漏えいの可能性と業務制限について公表 [14]。

○ システム障害が発生したのは 2025 年 2 月 10 日、ランサムウェア攻撃を確認後、サーバーをインターネットや院内ネットワークから遮断する措置を講じたことで、院内システムが使用できなくなり、当面の間、診察及び健診業務の制限を実施。

○ 調査の結果、患者の氏名、生年月日、住所、電話番号、メールアドレス、診療に関する情報及び健康診断に関する情報など、最大で約 30 万人分の個人情報が漏えいした可能性があることが判明。

○ 2025 年 5 月 14 日、通常の全ての診察及び健診業務を再開 [15]。

3.1.3. 保険見直し本舗グループのランサムウェア感染

○ 2025 年 2 月 25 日、約 50 社の提携保険会社の販売代理店である保険見直し本舗は、同社グループのランサムウェア被害について公表 [16][17]。

○ 被害が確認されたのは、2025 年 2 月 16 日。直ちに、関連するサーバーをネットワークから切り離すなどの緊急措置を講じた上で、外部専門家の協力のもと、原因及び影響範囲等の調査を実施。

○ 2025 年 4 月 30 日、調査の結果、データサーバの一部で保管しているファイルがランサムウェアにより暗号化されており、そのデータには、保険契約に関する個人情報や協業先企業から受託した業務に関わる個人情報が含まれ、約 510 万件の個人情報が漏えいした可能性があると公表 [18]。

3.1.4. NTT コミュニケーションズへの不正アクセス

○ 2025 年 3 月 5 日、NTT コミュニケーションズは、不正アクセスにより、同社社

---

[13] *福岡県「税務システムの障害の復旧について（2025/2/2）」、https://www.pref.fukuoka.lg.jp/contents/zeimusisutemushougainofukkyu.html（2025/5/16 閲覧）*

[14] *宇都宮セントラルクリニック「クリニックからのお知らせ（2025/2/18）」、https://ucc.or.jp/2025/02/17259（2025/5/16 閲覧）*

[15] *宇都宮セントラルクリニック「クリニックからのお知らせ（2025/5/14）」、https://ucc.or.jp/2025/05/17495（2025/5/16 閲覧）*

[16] *保険見直し本舗グループ「当社グループの委託先保険代理店におけるランサムウェア被害による個人情報漏えいのおそれについて（2025 年 2 月 25 日）」、https://www.nissay.co.jp/news/2024/pdf/20250225.pdf（2025/5/16 閲覧）*

[17] *保険見直し本舗グループ「当社グループにおけるランサムウェア被害に関しまして（2025 年 2 月 25 日）」、https://mhompo.co.jp/news/20250225/pdf/5bb59a05.pdf（2025/5/16 閲覧）*

[18] *保険見直し本舗グループ「当社グループにおけるランサムウェア被害に関しまして（第2報）（2025/4/30）」、https://mhompo.co.jp/news/20250430/pdf/20250430.pdf（2025/5/16 閲覧）*

内システムのオーダ情報流通システム（サービスの開通や変更に関わる情報を管理するシステム）に格納されていた法人向けサービスの情報の一部が外部に流出した可能性があることを公表[19]。

- ○ 2025 年 2 月 5 日に不正アクセスを発見、初動措置を実施し、2 月 15 日に不正アクセスを受けた装置を遮断する措置を実施。
- ○ 流出した可能性のある情報は、約 18,000 社の契約番号、契約名、担当者名、電話番号、メールアドレス、住所及びサービスの利用に係る情報。

3.1.5. 北陸電力の電気料金システムの不具合に伴う電気の誤停止

- ○ 2025 年 3 月 24 日、北陸電力において、48 件の顧客の送電を誤って停止する事案が発生[20]。
- ○ 本事案は、電気料金システムのメンテナンスで不具合が生じ、2025 年 3 月 22 日から 23 日における電気料金の入金を確認できなかったことにより、誤って送電を停止したもの。
- ○ 送電を停止した 48 件の顧客には、2025 年 3 月 25 日までに個別に連絡をして送電を完了。

---

[19] *NTT コミュニケーションズ株式会社「当社への不正アクセスによる情報流出の可能性について（2025/3/5）」、https://www.ntt.com/about-us/press-releases/news/article/2025/0305_2.html?msockid=3cd7a310d87e67dc0ed5b6d2d98c6682（2025/5/16 閲覧）*

[20] *北陸電力株式会社「電気料金システムの不具合に伴う電気の誤停止について（2025/3/26）」、https://www.rikuden.co.jp/press/attach/25032601.pdf?1742968941（2025/5/16 閲覧）*

資料４－２

重要インフラにおける情報共有件数について(2024 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	FY2020 計	FY2021 計	FY2022 計	FY2023 計	FY2024 1Q	FY2024 2Q	FY2024 3Q	FY2024 4Q	FY2024 計
重要インフラ事業者等からNISCへの情報連絡(※)	309	407	302	272	68	102	103	65	338
関係省庁・関係機関からのNISCへの情報共有	16	6	2	19	6	5	6	4	21
NISCからの情報提供	64	91	83	127	22	15	36	18	91

（※）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			FY2020 計	FY2021 計	FY2022 計	FY2023 計	FY2024 1Q	FY2024 2Q	FY2024 3Q	FY2024 4Q	FY2024 計
未発生の事象		予兆・ヒヤリハット	28	25	28	12	3	3	0	1	7
発生した事象	機密性を脅かす事象	情報の漏えい	23	29	17	20	9	13	6	2	30
	完全性を脅かす事象	情報の破壊	12	20	15	18	4	4	7	5	20
	可用性を脅かす事象	システム等の利用困難	157	181	145	148	28	46	66	40	180
	上記につながる事象	マルウェア等の感染	18	46	38	20	10	1	1	2	14
		不正コード等の実行	3	2	1	3	0	3	0	0	3
		システム等への侵入	26	24	22	13	5	20	10	5	40
		その他	42	80	36	38	9	12	13	10	44

2. 原因別類型（複数選択）

原因の類型		FY2020 計	FY2021 計	FY2022 計	FY2023 計	FY2024 1Q	FY2024 2Q	FY2024 3Q	FY2024 4Q	FY2024 計
意図的な原因	不審メール等の受信	9	47	39	7	0	0	1	2	3
	ユーザＩＤ等の偽り	9	7	7	7	1	3	6	0	10
	DDoS攻撃等の大量アクセス	10	19	28	32	2	9	29	12	52
	情報の不正取得	13	13	10	10	4	11	6	1	22
	内部不正	0	1	1	2	1	1	1	0	3
	適切なシステム等運用の未実施	23	15	8	7	3	3	2	3	11
偶発的な原因	ユーザの操作ミス	18	10	12	10	4	6	6	3	19
	ユーザの管理ミス	13	14	7	8	6	4	2	2	14
	不審なファイルの実行	7	22	26	2	0	0	0	3	3
	不審なサイトの閲覧	3	6	4	11	4	1	3	1	9
	外部委託先の管理ミス	56	107	49	50	12	21	17	12	62
	機器等の故障	39	38	43	38	5	14	9	8	36
	システムの脆弱性	38	32	12	35	2	9	2	6	19
	他分野の障害からの波及	7	10	7	5	0	0	2	0	2
環境的な原因	災害や疾病等	9	3	5	1	0	2	0	0	2
その他の原因	その他	35	48	29	41	10	13	11	7	41
	不明	68	79	62	51	18	20	16	13	67

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		FY2020 計	FY2021 計	FY2022 計	FY2023 計	FY2024 1Q	FY2024 2Q	FY2024 3Q	FY2024 4Q	FY2024 計
総計		100	174	143	123	27	59	57	27	170
	ランサムウェア攻撃	13	46	30	36	13	5	11	2	31
	ランサムウェアを除くマルウェア感染	8	29	27	4	1	1	0	1	3
	DDoS攻撃等の大量アクセス	4	15	25	28	2	10	29	9	50
	その他	75	84	61	55	11	43	17	15	86

（注）FY:年度、Q:四半期

最近のインシデントから得られた教訓(2024 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

DDoS 攻撃が複数報告された。被害を抑えるための対策と被害を想定した対策を行うこと等によるサイバー攻撃への備えが必要。また、システム更新時等の作業ミスによるシステム障害や動作確認の不足によるシステム障害が複数報告された。全ての関係者が適切に関与して作業にあたることやリリース前の動作確認を行うことが必要。

○ DDoS 攻撃に対するシステム対策や適切な広報・連絡体制等の備えが必要

IoT ボットネット等を用いた DDoS 攻撃（UDP フラッド攻撃、HTTP フラッド攻撃等）が複数あった。被害を抑えるための対策（同一 IP アドレスの大量のリクエストを遮断、DDoS 攻撃対策専用アプライアンス製品等を導入、サーバ等の設定の見直し等）を行うことや、被害を想定した対策（システムの重要度に応じた対応方針の策定ソーリーページ等の設定、通報先・連絡先一覧作成など発生時の対策マニュアルの策定等）を行うこと等の備えが必要。

○ システム更新時等における作業手順書の確認やリリース前の動作確認が必要

システムの更新等の作業時における手順ミスや設定ミスに加えて、リリース前の検証不足に起因するシステム障害により、サービスの提供時に支障が出た事例が複数あった。事前の検討から作業後の確認まで全ての関係者が適切に関与するとともに、作業手順を確認したのち作業にあたることやシステム更新等を行った際のリリースにあたっては、可能な限り実際の運用に近い状況での動作確認を行うことが必要。

○ サーバやネットワーク等の適切な設定や脆弱性への対応が必要

公開しているサーバが踏み台にされた事例やソフトウェアやウェブアプリケーションの脆弱性を悪用され不正アクセスされたことでウェブサイトが改ざんされる事例が複数あった。また、その際の攻撃対象に委託先が含まれる事例もあった。サーバやネットワーク等の適切な設定やシステムの重要性に応じた脆弱性診断・対応が必要。

○ 公開されているウェブサイトの適切な設計が必要

同一の送信元 IP アドレスから問い合わせフォーム等を用いて大量の通知が送信された事例が複数あった。また、外部から管理者用ページにアクセス可能であったためウェブサイトを改ざんされた事例や登録フォームにアップロードできるファイル形式を設定していなかったことから不正プログラムがアップロードされシステムが改ざんされた事例があった。公開されているウェブサイトの構築段階からの適切な設計が必要。

○ 従業員のリテラシー向上に加えシステム的な対策が必要

ウェブサイト閲覧中に偽サポートからのアラートが表示され、記載の連絡先に架電し、遠隔操作される事例やメールに添付されている不審な添付ファイルを開いてしまったことによるマルウェア感染等の被害が複数あった。従業員のリテラシーの向上に向けた研修等を定期的に行うことが重要。加えて、閲覧ページの制限、広告ブロック等のウェブブラウザにおけるフィルタリングの設定等の対策を行うことが必要。

以上

参考資料１

サイバーセキュリティを取り巻く情勢(2024 年度第 3 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、2024 年度第 3 四半期(10 月～12 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. DHS が、重要インフラにおける AI の役割と責任の枠組みを公表

- ○ 2024 年 11 月 14 日、国土安全保障省（DHS）は、重要インフラにおける人工知能（AI）の役割と責任のフレームワークを公表 [1]。
- ○ 本フレームワークでは、重要インフラにおける AI の安全・セキュリティの脆弱性について、AI を利用した攻撃、AI システムを標的とした攻撃及び設計・実装の失敗という 3 つの主要カテゴリーを特定。
- ○ これらの脆弱性に対処するため、AI 開発者、重要インフラの所有者と運営者、大学、研究機構、AI の安全・安心の問題に携わる消費者擁護団体を含む市民社会、連邦・州政府などの公共組織といった主要な関係者に向け、それぞれ推奨される行動を提示 [2]している。

1.1.2. CISA、NSA、FBI 及び国際パートナーが、通信インフラの可視性の強化及び堅牢化ガイダンスを公表

- ○ 2024 年 12 月 3 日、サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）、国家安全保障局（NSA）、連邦捜査局（FBI）及び国際パートナーは、

---

[1] *DHS「Roles and Responsibilities Framework for Artifical Intelligence in Crirtical Infrastructure」(2024/11/14)、https://www.dhs.gov/publication/roles-and-responsibilities-framework-artificial-intelligence-critical-infrastructure（2025/2/25 閲覧）*

[2] *DHS「Groundbreaking Framework for the Safe and Secure Deployment of AI in Critical Infrastructure Unveiled by Department of Homeland Security（2024/11/14）」、https://www.dhs.gov/archive/news/2024/11/14/groundbreaking-framework-safe-and-secure-deployment-ai-critical-infrastructure（2025/2/25 閲覧）*

世界の主要な通信プロバイダのネットワークを侵害した中国関連の脅威アクターから保護するためのベストプラクティスを提供する、通信インフラの可視性の強化及び堅牢化ガイダンスを公表[3]。

- ○ ネットワーク内のアクティビティを監視、検出及び理解するといった可視性を高めることにより、ネットワークトラフィック、ユーザーアクティビティ及びデータフローを把握し、ネットワーク防御者が脅威や脆弱性を迅速に特定することが可能となる。
- ○ 本ガイダンスで提示したベストプラクティスに従うことで、中国関連及びその他のサイバー脅威の潜在的な侵入ポイントを制限することが可能となるとしている。

1.1.3. CISA と EPA は、インターネットに露出したインターフェースが WWS 分野にもたらすリスクに関する共同ファクトシートを公表

- ○ 2024 年 12 月 13 日、CISA と環境保護庁（EPA）は、インターネットに露出したヒューマンマシンインターフェイス（HMI）が、上下水道システム（WWS）にサイバーセキュリティ上のリスクをもたらす可能性があることを述べた共同ファクトシートを公表[4]。
- ○ 本共同ファクトシートは、上下水道システム施設に対し、人間と機械の間で情報をやり取りする際に伝達を担う HMI のインターネットへの露出を制限し、悪意のあるサイバー活動から HMI を保護するための推奨事項を提供している。
- ○ EPA と CISA は、WWS 分野の組織が HMI への遠隔アクセスに関するセキュリティを強化するために、本ファクトシートに記載されている緩和策を検討し、実施することを強く推奨[5]している。

1.1.4. DHS は、海底ケーブルのセキュリティと強靭性に関するレポートを公表

- ○ 2024 年 12 月 18 日、米国国土安全保障省（DHS）は、戦略・政策・計画局（PLCY）及び CISA を通じて、情報コミュニティの代表者グループなどを招集し、海底通信ケーブルセクターの業界関係者との一連の協議を開催し、海底ケーブルのセキュリティと強靭性に関するレポートを公表[6]。

---

[3] *CISA「Enhanced Visibility and Hardening Guidance for Communications Infrastructure（2024/12/3）」、https://media.defense.gov/2024/Dec/03/2003596322/-1/-1/1/JOINT-GUIDANCE-ENHANCED-VISIBILITY-HARDENING-GUIDE-FOR-COMMS-INFRASTRUCTURE.PDF（2025/2/25 閲覧）*

[4] *CISA「CISA and EPA Release Joint Fact Sheet Detailing Risks Internet-Exposed HMIs Pose to WWS Sector（2024/12/13）」、https://www.cisa.gov/news-events/alerts/2024/12/13/cisa-and-epa-release-joint-fact-sheet-detailing-risks-internet-exposed-hmis-pose-wws-secto（2025/2/25 閲覧）*

[5] *CISA「Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems（2024/12/13）」、https://www.cisa.gov/resources-tools/resources/internet-exposed-hmis-pose-cybersecurity-risks-water-and-wastewater-systems（2025/2/25 閲覧）*

[6] *DHS「Priorities for DHS Engagement on Subsea Cable Security & Resilience（2024/12/18）」、https://www.*

○ 本レポートでは、海底通信ケーブルの故障の主な要因は、自然災害、事故及び故意の破壊活動に分類され、海底ケーブル故障のうち、約3分の2は漁業活動や船のいかりを引きずった際などに伴う事故となっているが、現在は悪意を持った人為的な破壊リスクが高まっている。
○ 海底通信ケーブルに関する諸課題を受けて、本レポートでは、以下、①～③のとおり、優先すべき取り組みを整理している。
① 官民連携メカニズムを強化
② 米国における海底通信ケーブルの許認可及び規制プロセスの合理化
③ 緊急管理と事案対応における連邦政府の役割と責任の明確化

1.2. 豪州

1.2.1. ACSC が、重要インフラ組織向けの OT サイバーセキュリティの原則に関するガイダンスを公表

○ 2024 年 10 月 2 日、オーストラリアサイバーセキュリティセンター(ACSC)は、オペレーショナル・テクノロジー(OT)サイバーセキュリティの原則に関するガイダンスを公表[7]。本ガイダンスについては、内閣官房セキュリティセンター（NISC）及び警察庁を含む、9 か国の各組織が共同署名。
○ 本ガイダンスは、重要インフラ組織が OT 環境の設計、実装及び管理に関する意思決定を行うことを支援する以下の 6 つの原則を提示。
○ ①安全が第一、②ビジネスの知識が重要、③OT データは極めて重要であり、保護する必要あり、④OT を他の全てのネットワークから分離・隔離する、⑤サプライチェーンは安全でなければならない、⑥OT のサイバーセキュリティには人材が不可欠。

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. 米最大の上下水道ユーティリティ、American Water Works へのサイバー攻撃

○ 2024 年 10 月 3 日、米ニュージャージー州カムデンに拠点を置き、1,400 万人以上に飲料水と廃水のサービスを提供するアメリカンウォーターワークス（American Water Works Company）は、コンピュータネットワーク及びシステム内での不正な活動を発見したと公表[8]。

---

dhs.gov/sites/default/files/2024-12/24_1218_scrc_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf（2025/2/25 閲覧）

[7] *ASD「Principles of operational technology cyber security（2024/10/2）」、https://www.cyber.gov.au/sites/default/files/2024-10/principles_of_operational_technology_cyber_security.pdf（2025/2/25 閲覧）*

[8] *UNITED STATES SECURITIES AND EXCHANGE COMMISSION「Form 8-k American Water Works Compa*

- 特定のシステムを遮断し、非アクティブ化するなど、システムとデータを保護するための措置を講じた。
- 現在までのところ、本インシデントにより悪影響を受けた上下水道施設や事業はないとされている。

2.1.2. メキシコの空港運営会社（OMA）へのサイバー攻撃

- 2024 年 10 月 18 日、メキシコの中央及び北部地域の 9 州にある 13 の国際空港を運営及び管理しているメキシコの空港運営会社 Grupo Aeroportuario del Centro Norte（OMA）で、サイバーインシデントが発生 [9]。
- OMA が管理する空港のスクリーンがダウン。代替システムとバックアップシステムを通じて空港の運営は継続。
- 2024 年 11 月 5 日、本インシデントはランサムウェア攻撃によるもので、一部、情報漏えいがあった旨を公表 [10]。

2.1.3. 米ペンシルベニア州ピッツバーグ地域交通局（PRT）へのランサムウェア攻撃

- 2024 年 12 月 19 日、米ペンシルバニア州ピッツバーグ地域交通局（PRT）が、ランサムウェア攻撃を検出し、PRT のカスタマーサービスセンターなどの乗客サービスが影響を受けた [11]。
- インシデントの発覚後実施した調査により [12]、PRT はサイバー犯罪者がネットワークから特定の個人情報のデータを盗んだと判断し、被害の影響を受けた個人に対して通知を実施。盗まれたデータの中には、PRT 従業員及び PRT の求職者に関連する社会保障番号と運転免許証番号が含まれている。
- また、PRT は被害の影響を受けた個人以外で、影響を受ける可能性のある個人について、金融口座などを注意深く監視し、被害が生じた場合には、法執行機関に報告、個人情報を保護するための適切な措置を講じることを奨励している。

---

ny,Inc（2024 年 10 月 7 日）」、https://www.sec.gov/Archives/edgar/data/1410636/000119312524233300/d869346d8k.htm?7194ef805fa2d04b0f7e8c9521f97343（2025/2/25 閲覧）

[9] *OMA「OMA Informa Sobre Incidente de Ciberseguridad（2024/10/18）」、https://www.oma.aero/assets/005/6312.pdf（2025/2/25 閲覧）*

[10] *OMA「OMA Proporciona Information Adicional Sobre Incidente de Ciberseguridad（2024/11/5）」、https://noticias.oma.aero/news/oma-proporciona-informacion-adicional-sobre-incidente-de-ciberseguridad-39779-5f19f.html（2025/2/25 閲覧）*

[11] *Pittsburgh Regional Transit「Pittsburgh Regional Transit to Cybersecurity Incident（2024/12/23）」、https://www.rideprt.org/siteassets/inside-the-pa/media-center/press-releases/2024/12232024cyber.pdf（2025/2/25 閲覧）*

[12] *Pittsburgh Regional Transit「Pittsburgh Regional Transit to Cybersecurity Incident（2024/12/23）」、https://www.rideprt.org/siteassets/inside-the-pa/media-center/press-releases/2025/01072025cyberincident.pdf（2025/2/25 閲覧）*

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. 奈良県斑鳩町町立図書館におけるランサムウェア感染

- 2024 年 10 月 3 日、同月 1 日から運用開始を予定していた斑鳩町立図書館システムについて、ランサムウェアに感染したことを公表 [13]。図書館システムと外部とのネットワークを遮断するとともに、図書館システムの運用停止に伴い、図書館のホームページ及びシステムによる蔵書検索なども停止した。
- 2024 年 10 月 25 日、当該システムのサーバ内に含まれている、図書館利用者の個人情報（21,994 人分）について、専門業者によるフォレンジック調査の結果、データの漏洩は確認されなかった旨、公表。
- 本インシデントは、システムの導入作業時において、構築中のサーバへのアクセス設定に不備があったため、ログイン ID 及びパスワードが解析され、外部からの不正アクセスが発生したが原因 [14]。

3.1.2. 年末年始にかけての航空事業者及び金融機関等に対するサイバー攻撃

- 2024 年 12 月末から 2026 年 1 月の年末年始にかけて、航空分野、金融分野等へのサイバー攻撃が相次いだ。
- 2024 年 12 月 26 日7時 24 分から日本航空（JAL）において、社内外を繋ぐネットワーク機器でサイバー攻撃を受け、社外システムと通信しているシステムで不具合が発生 [15]。国内線及び国際線に遅延が発生したが、 同日 13 時 20 分頃、システムが復旧し、当日フライト分の販売も再開された。なお、顧客データ流出やウイルス被害なし。
- また、2024 年 12 月 26 日 15 時頃から三菱 UFJ 銀行において、外部から大量のデータが送られ、インターネットバンキングをスマートフォンのアプリなどから利用する際にログインできない事象が発生 [16]。顔認証や指紋認証のシステムにも不具合が生じたが、翌 27 日夜にはほぼ復旧。なお、預金の抜き取りや不正送金、顧客情報の流出は確認されていない。

---

[13] *奈良県斑鳩町「図書館システム構築業務におけるコンピュータウイルスの発生事案について（2024 年 10 月 3 日）」、https://www.town.ikaruga.nara.jp/0000002914.html（2025 年 2 月 25 日閲覧）*

[14] *奈良県斑鳩町「図書館システム構築業務におけるコンピュータウイルスの発生事案について（最終報）（2024 年 10 月 25 日）」、https://www.town.ikaruga.nara.jp/0000002943.html（2025 年 2 月 25 日閲覧）*

[15] *JAL（日本航空）「ネットワーク障害による運航への影響について（終報）（2024/12/26）」、https://www.jal.co.jp/jp/ja/info/2024/other/241226-2（2024/12/26 閲覧）*

[16] *三菱 UFJ 銀行（MUFG）「ネットワーク不具合による各種サービスの影響について（12 月 26 日 18 時 45 分時点）（2024/12/26）」、https://www.bk.mufg.jp/emeg/10_1513.html(2024/12/26 閲覧)*

3.2. その他

3.2.1. 浦添市の小学校、児童など約 700 人分の個人情報が流出の恐れ

- 2024 年 11 月 20 日、浦添市内の小学校において、児童及び卒業生とその保護者などの個人情報の漏洩の恐れがある事案が発生 [17]。
- 教諭1名が校務用パソコンにてインターネット閲覧中に、偽のセキュリティ警告に従い、遠隔操作ツールをインストールし、当該ツールが起動していた約 10 分の間、当該パソコンから個人情報等が保存されている USB メモリ及び校内ファイルサーバーにアクセスできる状態にあったことが原因。
- 当該端末を含め、及び全校務用 PC のウイルス対策ソフトのスキャンを実施したが、ウイルス等は確認されなかった。

3.2.2. Salesforce で発生した日本を含む世界的なシステム障害

- 2024 年 11 月 15 日から 16 日にかけて、クラウドサービスを提供する Salesforce において、日本を含むアジア太平洋地域及び北米地域の一部に影響を及ぼすシステム障害が発生。データベースのメンテナンス作業が原因。
- 本事案により、日本国内においても、政府、独法、地方公共団体、金融機関等、多くの組織において、サービスのログインができない、閲覧ができないといった障害が発生。

3.2.3. 北朝鮮を背景とするサイバー攻撃グループ TraderTraitor によるサイバー攻撃

- 2024 年 12 月 24 日、警察庁、FBI及び米国国防省サイバー犯罪センターは、北朝鮮当局の下部組織のラザルスグループの一部とされるサイバー攻撃グループ「TraderTraitor」が、2024 年 5 月、暗号資産関連事業者である（株）DMM ビットコインから約 482 億円相当の暗号資産を窃取したと評価し、合同で文書を公表 [18]。
- 今回の日米合同のパブリックアトリビューションを受け、警察庁、内閣官房セキュリティセンター（NISC）及び金融庁の連名で、攻撃グループの手口例及び緩和策に関する文書を公表 [19]。これは、標的となる事業者に、直面するサイバー空間の脅威を認識し、必要な対策を講じてもらうこととしたもの。

---

[17] *沖縄県浦添市「市内小学校にて発生した情報漏洩のおそれがある事案の調査結果について」（2025 年 1 月 8 日）」、https://www.city.urasoe.lg.jp/doc/2025010700199/（2025 年 2 月 25 日閲覧）*

[18] *警察庁「北朝鮮を背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について（2024 年 12 月 24 日）」、https://www.npa.go.jp/bureau/cyber/pdf/020241224_pa.pdf（2025 年 2 月 25 日閲覧）*

[19] *警察庁、内閣サイバーセキュリティセンター、金融庁「北朝鮮背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について（注意喚起）（2024 年 12 月 24 日）」、https://www.npa.go.jp/bureau/cyber/pdf/20241224_caution.pdf（2025 年 2 月 25 日閲覧）*

参考資料２

最近のインシデントから得られた教訓(2024 年度第３四半期)

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

DDoS 攻撃の事例が多数あり、SNS への攻撃を示唆する投稿を伴うものと、無いものとがあった。サービスの重要度や実際の攻撃手法を踏まえた適切な対策が必要。また、委託先におけるランサムウェア感染により、多数の事業者の個人情報漏えいが発生したとみられる事例が複数あった。委託先におけるセキュリティ対策の確認が重要。

○　攻撃を想定したシステム設計と障害発生時における適切な広報の実施が必要

複数種類の攻撃手法を組み合わせた DDoS 攻撃や、事業者が管理する IP アドレスレンジ全体を攻撃対象とした事例があった。サービスの重要度及び実際の攻撃手法を踏まえた DDoS 攻撃への技術的観点での耐性向上に加え、障害発生時における適切な形での広報手段などの組織的観点での対応の備えが必要。

○　サプライチェーン全体でのサイバーセキュリティ向上の取組が必要

委託先における VPN 機器等の管理・運用の不十分さを起因とするランサムウェア感染により、多数の重要インフラ事業者で情報漏えいが発生したとみられる事例が複数あった。脆弱性への適切な対応や ID/パスワードの設定・管理の必要性を認識しつつ、委託する業務の重要度を踏まえた選定基準の設定と評価、責任分解点の明確化などが重要。

○　サーバやネットワークなどの適切な設定や脆弱性への対応が必要

漏えいした ID/パスワードや攻撃者が想定しやすいアカウント名を悪用され、VPN 機器から内部ネットワークへの侵入を許した事例が複数あった。また、Web サイトが、意図しない種別のファイルをアップロード可能な状態となっている脆弱性を悪用され改ざんされた事例があった。サーバ、ネットワーク及びネットワーク機器の適切な設計・設定が必要。

○　認証の強化に加えて認証情報の適切な管理・運用が必要

クラウドサービスのアカウント、メールアカウント及び SNS アカウントなど、初期状態や何らかの形で漏えいした ID/パスワードを用いて悪用されたと考えられる事例も複数あった。容易に想像しにくい ID/パスワードの設定や多要素認証の有効化による認証強化に加えて、管理者アカウントの厳格な管理・運用が必要。

○　作業手順書の確認など適切な事前準備が必要

システムの変更や更新などの作業時における手順のミスや設定ミス、事前の検証不足に起因するシステム障害及び作業後の確認作業不足により、サービスの提供に支障が出た事例が複数あった。事前の検討から作業後の確認まで、作業対象機器の影響を受けるシステムの担当者を含む全ての関係者の適切な関与が必要。