資料２－１

令和 6 年 10 月 8 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２－２

サイバーセキュリティを取り巻く情勢(2024 年度第 1 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 1 四半期(4 月～6 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. 飲料水システムに対する注意喚起

- ○ 2024 年 5 月 20 日、米国環境保護庁(EPA)は、地域の飲料水システムに対するサイバーセキュリティの脅威と脆弱性について概説するとともに、飲料水安全法(Safe Drinking Water Act: SDWA)の遵守について注意喚起を実施[1]。国の水関連システムに対する脅威や攻撃について、その頻度と深刻度が増してきており、追加的な対策が不可欠であることから、当該注意喚起を発出。
- ○ また、EPA による最近の査察結果において、査察対象となった水道システムの大部分(70%以上)が SDWA の要件を十分に遵守しておらず、一部のシステムは、デフォルトのままでのパスワードの使用や多要素認証を採用していないなどの重大なサイバーセキュリティの脆弱性があることが判明。
- ○ この注意喚起は、SDWA 第 1433 条に基づく EPA の継続的な検査・取り締まりの重要性を強調するものであり、EPA は、計画的な検査の回数を増やし、必要に応じて民事及び刑事上の強制措置を講じる予定。

[1] *EPA「EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation's Drinking Water(2024/5/20)」、https://www.epa.gov/newsreleases/epa-outlines-enforcement-measures-help-prevent-cybersecurity-attacks-and-protect (2024/8/19 閲覧)*

1.1.2. 医療施設のサイバーセキュリティを強化・自動化するシステムの開発

- 2024 年 5 月 20 日、医療高等研究計画局(ARPA-H)は、5,000 万ドル以上を投資して、IT チームが病院環境のセキュリティを強化するためのツールを開発する Universal PatchinG and Remediation for Autonomous DEfense (UPGRADE)プログラムを開始すると発表[2]。
- デジタルで病院環境のモデルを構築し、ソフトウェアの弱点を探ることで潜在的な脆弱性を事前に評価することを可能にする。脅威が検出されると、パッチなどの改善策が自動的に調達または開発され、モデル環境でテストされ、使用機器の停止を最小限に抑えて展開されることを目指すもの。
- 「脆弱性緩和ソフトウェア・プラットフォームの構築」、「病院設備の忠実度の高いデジタル空間での再現環境の開発」、「脆弱性の自動検出」、「脆弱性に対する拡張防御策の自動開発」の 4 つの技術分野に関する提案を募集。

1.1.3. 米国エネルギー省が「サプライチェーン・サイバーセキュリティ原則」を発表

- 2024 年 6 月 18 日、米国エネルギー省(DOE)は、アイダホ国立研究所と共同で策定した新しい「サプライチェーン・サイバーセキュリティ原則」を発表[3、4]。
- この原則は、エネルギーインフラを支えるサプライチェーンにおけるサイバーセキュリティのベストプラクティスを確立するものであり、エネルギー分野にサービスを提供するサプライヤーやメーカーもこの原則への支持を表明。
- サプライヤー向けとエンドユーザー向けの原則が策定されており、世界中の電力、石油及び天然ガスのシステム管理と運用のために使用される主要技術を強化するための枠組みを構築。

1.1.4. 米国内における Kaspersky 製品の販売等禁止

- 2024 年 6 月 20 日、米国商務省産業安全保障局(BIS)は、ロシアを拠点とする Kaspersky 社について、米国内におけるソフトウェアの販売及びサービスの提供を禁止することを公表[5]。
- 本措置は、米国子会社である Kaspersky Lab, Inc.及びその関連会社、子会社、親会社に適用される。2024 年 9 月 29 日(EDT)午前 12 時以降、米国内での Kaspersky 社のソフトウェア販売や、既に使用されているソフトウェアの

---

[2] *ARPA-H、「ARPA-H announces program to automate cybersecurity for health care facilities(2024/5/20)」、https://arpa-h.gov/news-and-events/arpa-h-announces-program-automate-cybersecurity-health-care-facilities (2024/8/19 閲覧)*

[3] *DOE、「DOE Leads Effort to Improve the Cybersecurity of Energy Supply Chains(2024/6/18)」、https://www.energy.gov/articles/doe-leads-effort-improve-cybersecurity-energy-supply-chains(2024/8/19 閲覧)*

[4] *DOE、「Supply Chain Cybersecurity Principles(2024/6/18)」、https://www.energy.gov/sites/default/files/2024-06/DOE%20Supply%20Chain%20Cyber%20Princples%20June%202024.pdf(2024/8/19 閲覧)*

[5] *BIS「Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers(2024/6/20)」、https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-us-customers(2024/8/19 閲覧)*

アップデートの提供などを禁止。

- ○ 既存の Kaspersky が提供した製品及びサービスを引き続き使用する個人及び企業は、本措置により法的処罰を受けることはないが、機密データなどがさらされないよう速やかに新しいベンダーに移行することを強く推奨。

1.2. 英国

1.2.1. スマートデバイスのセキュリティ強化に関する法律が施行

- ○ 2024 年 4 月 29 日、インターネットに接続されたスマートデバイスが最低限のセキュリティ標準を満たすことを義務付ける Product Security and Telecommunications Infrastructure act（PSTI 法）が施行[6][7]。
- ○ この法律は、メーカーが、全てのスマートデバイスの基本的なサイバーセキュリティ要件（以下）を満たしていることを保証しなければならない。
  - ① オンラインで容易に発見され、共有される可能性のあるデフォルトパスワードを使用するデバイスの提供禁止
  - ② セキュリティ問題が発生した際の報告先の提供
  - ③ 重要なセキュリティアップデートが提供される最短の期間の明示
- ○ ほとんどのスマートデバイスは、英国外で製造されているが、この法律は、英国市場向けに製品を輸入、販売する組織にも適用。これに違反した場合、最大 1,000 万ポンド、又は、全世界での収益の 4%のいずれか高い方の罰金が科される。

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. 英国の血液検査等を実施する病理検査機関へのランサムウェア攻撃

- ○ 2024 年 6 月 3 日、主にロンドン南東部での多くの血液検査を処理する病理検査機関 Synnovis が、ランサムウェアによるサイバー攻撃の被害を受け、Synnovis のほぼ全ての IT システムが影響を受け、多くのサービスが中断[8]。その結果、検査予約や手術が延期されるなど、大きな混乱が生じた[9]。
- ○ 6 月 24 日、サイバー攻撃の犯人と主張するグループがデータをオンラインで

---

[6] *The National Cyber Security Centre「Smart devices: new law helps citizens to choose secure products（2024/4/29）」https://www.ncsc.gov.uk/blog-post/smart-devices-law(2024/8/26 閲覧)*

[7] *GOV.UK「New laws to protect consumers from cyber criminals come into force in the UK（2024/4/29）」https://www.gov.uk/government/news/new-laws-to-protect-consumers-from-cyber-criminals-come-into-force-in-the-uk(2024/8/26 閲覧)*

[8] *「Synnovis「Cyberattack update: 24 June 2024(2004/6/24)」、https://www.synnovis.co.uk/news-and-press/cyberattack-update-24-june-2024(2024/8/26 閲覧)*

[9] *NHS England「Synnovis cyber attack – statement from NHS England(2004/6/21)」、https://www.england.nhs.uk/2024/06/synnovis-cyber-attack-statement-from-nhs-england/(2024/8/26 閲覧)*

公開し、このデータが Synnovis のシステムから盗まれたものであることが確認された旨、公表。

- ○ 7 月 25 日、IT インフラの多くの部分について再構築し、一部の病院との接続は復旧済みであるが、完全復旧に向けて進行中である旨、公表。

2.1.2. スペインのサンタンデール銀行への不正アクセス

- ○ 2024 年 5 月 14 日、スペインに拠点を置く大手銀行グループのサンタンデール銀行が不正アクセスの被害にあった旨を公表[10]。
- ○ 第三者プロバイダーがホストしているデータベースへの不正アクセス。直ちに、当該データベースへのアクセスを遮断し、影響を受ける顧客を保護するため、不正防止策を追加するなどの対策を実施。
- ○ 調査の結果、チリ、スペイン、ウルグアイの顧客、サンタンデールグループの現従業員及び元従業員の情報にアクセスされたことを確認。
- ○ 口座取引を可能にする認証情報や取引データは、当該データベースに含まれておらず、同行の業務やシステムには影響はなかった。

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. 岡山県精神科医療センターへのランサムウェア攻撃

- ○ 2024 年 5 月 19 日、岡山県精神科医療センター及び東古松サンクト診療所において、ランサムウェアによるサイバー攻撃により電子カルテを含めた総合情報システムに障害が発生（紙カルテの運用などにより診療体制は維持）[11]。
- ○ 2024 年 6 月 11 日、患者情報等の流出が確認された旨公表。流出した可能性のある情報は、総合情報システムで職員が業務で作成した資料を保存していた共有フォルダ内の患者情報で、氏名、住所、生年月日及び病名など、最大約 40,000 人分、病棟会議の議事録等[12]。

3.1.2. イセトーへのランサムウェア攻撃

- ○ 2024 年 5 月 26 日、金融機関及び地方公共団体などの情報処理サービスを手がけるイセトー（京都市）は、複数のサーバー、端末内の情報がランサム

---

[10] *Santander Bank「Santander Statement（2024/5/14）」、https://www.santander.com/content/dam/santander-com/en/stories/contenido-stories/2024/statement.pdf(2024/8/26 閲覧)*

[11] *地方独立行政法人 岡山県精神科医療センター「当センターの電子カルテシステムの障害発生について（第2報）(2024/5/21)」、https://www.popmc.jp/home/organization/5w64e269/5bid3p49/9xekkbxz/(2024/8/26 閲覧)*

[12] *地方独立行政法人 岡山県精神科医療センター「患者情報等の流出について（2024/6/11）」、https://www.popmc.jp/home/organization/5w64e269/5bid3p49/zx2nd5xq/(2024/8/26 閲覧)*

ウェアによる被害が発生し、また、同年 6 月 6 日には個人情報の流出のおそれがある旨公表[13]。

- ○ 6 月 18 日、攻撃者グループのリークサイトにおいて、同社から窃取されたと考えられる情報のダウンロード URL が掲載されている旨を確認（7 月 3 日時点では消失）、公開された情報は同社のサーバーから流出したものであること、また流出した情報の中には一部の取引先の顧客の個人情報が含まれていることが判明[14]。
- ○ 多数の金融機関及び地方公共団体などが、本事案を原因とする情報漏えいについて公表。

3.1.3. 九州電力の子会社で、不正アクセスにより個人情報が漏えい

- ○ 2024 年 6 月 3 日、九州電力のグループ会社である株式会社キューヘンの社内ネットワークの一部が、第三者による不正アクセス（ランサムウェア攻撃）を受け、情報が漏えいしたおそれがあることが確認[15]。
- ○ 九州電力において、漏えいしたおそれがある情報はキューヘンに委託している給湯器販売に関する業務で使用する約 4,000 件及び電化機器の PR 業務で使用していた約 20,000 件の個人情報である旨公表。
- ○ キューヘンにおいて、影響を受けたパソコンの停止、パソコン及びデータ保存領域のネットワークからの切り離しを行うなど、被害拡大を防止するための対応を実施し、九州電力のシステムや電力供給への影響はない。

---

[13] *株式会社イセトー「ランサムウェア被害の発生について(2024/5/29)」、https://www.iseto.co.jp/news/news_202405-3.html（2024/8/26 閲覧）*

[14] *株式会社イセトー「ランサムウェア被害の発生について（続報2）(2024/5/29)」、https://www.iseto.co.jp/news/news_202407.html(2024/8/26 閲覧）*

[15] *九州電力株式会社「グループ会社への不正アクセスが発生しました（第2報）（2024/6/13）」、https://www.kyuden.co.jp/press_h240613-1.html（2024/8/26 閲覧）*

資料２－３

重要インフラにおける情報共有件数について(2024 年度第１四半期)

「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	2Q	3Q	4Q	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	－	－	－	68
関係省庁・関係機関からのNISCへの情報共有	16	6	2	19	6	－	－	－	6
NISCからの情報提供	64	91	83	127	22	－	－	－	22

（※）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	2Q	3Q	4Q	計
未発生の事象		予兆・ヒヤリハット	28	25	28	12	3	－	－	－	3
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	－	－	－	9
	完全性を脅かす事象	情報の破壊	12	20	15	18	4	－	－	－	4
	可用性を脅かす事象	システム等の利用困難	157	181	145	148	28	－	－	－	28
	上記につながる事象	マルウェア等の感染	18	46	38	20	10	－	－	－	10
		不正コード等の実行	3	2	1	3	0	－	－	－	0
		システム等への侵入	26	24	22	13	5	－	－	－	5
		その他	42	80	36	38	9	－	－	－	9

2.原因別類型（複数選択）

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

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	2Q	3Q	4Q	計
総計		100	174	143	123	27	－	－	－	27
	ランサムウェア攻撃	13	46	30	36	13	－	－	－	13
	ランサムウェアを除くマルウェア感染	8	29	27	4	1	－	－	－	1
	DDoS攻撃等の大量アクセス	4	15	25	28	2	－	－	－	2
	その他	75	84	61	55	11	－	－	－	11

（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１四半期)

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 機器の脆弱性を突く典型的なランサムウェア攻撃の被害事例が複数報告された。資産管理・脆弱性管理の重要性の再認識が必要。また、複数分野の重要インフラ事業者と取引する事業者において、事業規模の大小に関係なくインシデントが発生した。委託先等サプライチェーンを構成する事業者間における持続的なサイバーセキュリティ向上の取組が重要。

さらに、機器の故障等を原因とするシステム障害も多数報告があり、IT-BCP の策定と適切な運用が重要。

○ 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

委託先におけるランサムウェア感染により、多数の事業者で情報漏洩が発生した事例が複数あった。委託先におけるセキュリティ対策やインシデント発生時の復旧対応の定期的な確認等が必要。ランサムウェア感染については、VPN 機器を侵入口とする典型的な攻撃の被害となった事例が複数あり、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。

○ 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

Web サーバへの DDoS 攻撃とみられる大量アクセスを受けた事例が複数あった。中には、SQL インジェクション攻撃との複合攻撃を受けたが、ウェブサイトが適切に設計されていたことにより回避できた事例もあった。また、攻撃の対象は Web サーバだけでなく、サービス提供に必要となる通信の経路上に存在するインターネットに接続された機器であるケースもあり、サービスの重要度に応じた DDoS 攻撃への耐性向上に加え、障害発生時における適切な形での広報手段など事前の備えも必要。

○ 認証手段の高度化の実施と認証情報の適切な管理・運用が必要

Web サイト管理用アカウント、メールアカウント、SNS アカウントの ID/パスワードが漏洩し悪用されたと考えられる事例が複数あった。多要素認証やアクセス制限など、認証手段の高度化を実施することが必要。

○ ユーザーリテラシー向上に加えシステム的な対策が必要

業務上必要な検索等ウェブサイト閲覧中に、偽警告サイトへ誘導された事例が複数あった。検索結果に実在するブランドそっくりの広告や大手ベンダーのチャットを装う等手段も巧妙化してきている。システム的な対策や職員の教育により問題が起きないようにするだけではなく、仮に問題が起きた際に同僚や上長に素早く相談できる環境の醸成も必要。

以上