資料２

令和 5 年 12 月 20 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

サイバーセキュリティを取り巻く情勢(2023 年度第 2 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 2 四半期(7 月～9 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 米国国家サイバーセキュリティ戦略実施計画

- 2023 年 7 月 13 日、ホワイトハウスは、同年 3 月に公表した国家サイバーセキュリティ戦略に対する実施計画を公表[1]。
- 国家サイバーセキュリティ戦略の 27 の戦略目標ごとに、18 の担当省庁に割当てられ、完了までのタイムラインを整理。
- 国家サイバー局長室(ONCD)が実施状況に関し大統領及び議会に報告、行政管理予算局(OMB)と協力して予算要求が実施計画と整合的であるかを確認する。

1.1.2 CISA サイバーセキュリティ 2024-2026 会計年度戦略計画

- 2023 年 8 月 4 日、米国サイバーセキュリティ・インフラセキュリティ庁(CISA)は、同庁の取組の指針として 3 つの目標と 9 つの目的を示す CISA サイバーセキュリティ 2024-2026 会計年度戦略計画を公表[2]。
- CISA のリソースは有限であることから、米国にとって最大限の効果を得るため、連邦政府機関、標的になりやすいが対応リソースの乏しい組織、重要インフラ、キーテクノロジー・サイバーセキュリティ企業等の 4 つの組織を重視。

---

[1] *The White House「National Cybersecurity Strategy Implementation Plan(2023/7/13)」、https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf (2023/8/22 閲覧)*

[2] *CISA「CISA Cybersecutity Strategic Plan FY2024-2026(2023/8/4)」、https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf (2023/9/4 閲覧)*

1.1.3　サイバーインシデント報告協議会報告書

○ 2023 年 9 月 19 日、米国国土安全保障省(DHS)は、重要インフラのためのサイバーインシデント報告法(CIRCIA:the Cyber Incident Reporting for Critical Infrastructure Act)に基づき設置されたサイバーインシデント報告協議会が「連邦政府へのサイバーインシデント報告の調和」と題する報告書を公表[3]。

○ 報告では、サイバーインシデントの報告を合理化するために、重複するインデント報告のリスト、重複する報告要件を調和するための課題・措置、そのための推奨事項を報告。

1.2.　中国

1.2.1　中国政府機関職員の iPhone の業務使用等禁止報道

○ 中国は中央政府機関の職員に対し、米アップルの iPhone やその他の海外メーカーのデバイスの業務使用及び職場への持ち込みを禁止した旨報道。

○ 外国のテクノロジーへの依存を減らし、サイバーセキュリティを強化するという中国政府の方針を示す最新の事例であり、中国国外への機密情報の流出を懸念しているものと推測[4]。なお、中国外務省報道官は当該報道について否定している。

1.2.2　中国地震センターが海外攻撃グループに攻撃されたと発表

○ 2023 年 7 月 26 日、中国武漢市危機管理局は、地震監視センターの一部のネットワーク機器に対し海外組織からサイバー攻撃を受けた旨を発表。

○ 中国共産党系メディアの「環球時報」は、地震の強度のデータが盗まれたなどと報じた。また、環球時報や国営テレビ局である CCTV が運営するソーシャルメディアアカウントなどの中国国営メディアは、攻撃は政府支援で米国からのものと主張[5]。

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　米国医療サービス企業における患者情報の漏えい

○ 2023 年 7 月 10 日、米国を本拠とする米国及び英国の医療施設を運営する HCA Healthcare は、推定 1,100 万人の個人情報がハッキングフォーラムに

---

[3] *DHS「Harmonization of Cyber Incident Reporting to the Federal Government(2023/9/19)」、https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government（2023/10/17 閲覧）*

[4] *日経新聞「中国政府 iPhone 禁止　米紙報道、機密流出懸念か(2023/9/6)」、https://www.nikkei.com/article/DGXZQOCB06A1G0W3A900C2000000/（2023/12/1 閲覧）*

[5] *REUTERS「China says Wuhan earthquake centre attacked by overseas hackers(2023/7/27)」、https://www.reuters.com/world/china/china-says-wuhan-earthquake-centre-attacked-by-overseas-hackers-2023-07-26/（2023/12/1 閲覧）*

公開されている旨を公表。

- ○ 漏えいした情報は、患者の氏名、居住市・州・郵便番号、メールアドレス、生年月日、電話番号等であり、臨床情報、口座情報等の機密性の高い情報は含まない[6]。

2.1.2 英国航空管制システム障害 国内外の空港で多数が足止め

- ○ 2023 年 8 月 28 日、英国の航空管制システム(NATS)にシステム障害が発生し、28 日当日は約 1,500 便を超えるフライトがキャンセル、英国領空を運航した約 5,500 便のうち、約 575 便が遅延した。この日は英国の祝日であるほか、周辺国の一部でも学校が休校となる繁忙期であり、空港では多くの利用客が足止めとなった。
- ○ 同じ名称であるが実際には別である2つの航路上の地点を含む、非常に稀な飛行計画について、システム上で処理ができず、プライマリシステムとバックアップシステムの両方が停止してまったことが原因[7]。

2.1.3 アイルランド銀行におけるシステム障害

- ○ 2023 年 8 月、アイルランド銀行で、システムの設定ミスが原因で、口座に残高のない顧客でもATMから現金を引き出せる状態になり、同国内のATMに大行列ができる混乱となり、警察が出動する事態が発生[8]。

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

- ○ 2023 年 7 月「Storm-0058」について、政府機関を含む複数の電子メールアカウントに対する不正アクセスを行っていると Microsoft 社が報告[9]。
- ○ 2023 年 9 月、「BlackTeck」について、警察庁と NISC が NSA、FBI、CISA と合同の注意喚起を発出[10]。

---

[6] *Bleepingcomputer「HCA confirms breach after hacker steals data of 11 million patients(2023/7/11)」、https://www.bleepingcomputer.com/news/security/hca-confirms-breach-after-hacker-steals-data-of-11-million-patients/（2023/12/1 閲覧）*

[7] *NATS「NATS report into air traffic control incident details root cause and solution implemented(2023/9/6)」、https://www.nats.aero/news/nats-report-into-air-traffic-control-incident-details-root-cause-and-solution-implemented/（2023/12/1 閲覧）*

[8] *gigazine「銀行で「口座がスッカラカンでもATMからお金を引き出せる」障害が発生、街中のATMに大行列ができて警察が出動する事態に(2023/8/16)」、https://gigazine.net/news/20230816-ireland-bank-atm-access-to-cash/（2023/12/1 閲覧）*

[9] *Microsoft「Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email(2023/7/11)」、https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/(2023/8/8 閲覧）*

[10] *内閣サイバーセキュリティセンター「中国を背景とするサイバー攻撃グループ BlackTech によるサイバー攻撃について(2023/9/27)」、https://www.nisc.go.jp/pdf/press/20230927NISC_press.pdf（2023/10/2 閲覧）*

2.2.2 ロシア関連

- 2023 年 7 月、「Trula」が、新しい.NET バックドア CAPIBAR を使用して情報を窃取 [11]。
- 2023 年 8 月、「Sandworm Team」が、ウクライナ軍の Android 端末を標的としたスパイマルウェア Infamous Chisel を配布、米国連邦機関等が共同アドバイザリーを発出 [12]。
- 2023 年 9 月、「APT28」がウクライナのエネルギー施設へフィッシング攻撃、システムへの侵入は失敗 [13]。

2.2.3 北朝鮮関連

- 2023 年 7 月、JumpCloud 社は、北朝鮮が支援する攻撃グループによる攻撃を受けたと報告。Mandiant 社は、本事案が攻撃グループ「UNC4899」によるものと指摘し、同グループが北朝鮮 RGB 傘下で暗号資産窃取にフォーカスしていると評価 [14]。
- 2023 年 8 月、韓国の京畿南部警察庁は、米韓合同軍事演習である乙支フリーダムシールドが開始する前日の 8 月 20 日に、米韓合同軍事演習のシミュレーションセンターを狙ったサイバー攻撃に発表。いくつかの根拠を基に、攻撃グループ「Kimsuky」による攻撃と判断 [15]。
- 2023 年 9 月、北朝鮮政府の支援を受ける攻撃グループが、脆弱性の研究開発を専門とするセキュリティ研究者を攻撃。攻撃者は少なくとも 1 つのゼロデイ脆弱性を悪用 [16]。

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 鹿児島県志布志市のふるさと納税サイトに不正アクセス

- 2023 年 6 月 22 日、鹿児島県志布志市は、同市のふるさと納税特設サイトが

---

[11] *CERT-UA「Targeted attacks Turla (UAC-0024, UAC-0003) using CAPIBAR and KAZUAR malware (CERT-UA#6981)(2023/7/18)」、https://cert.gov.ua/article/5213167 (2023/8/21 閲覧)*

[12] *SSU「SBU exposes russian intelligence attempts to penetrate Armed Forces' planning operations system(2023/8/8)」、https://ssu.gov.ua/en/novyny/sbu-exposes-Russian-intelligence-attempts-to-penetrate-armed-forces-planning-operations-system (2023/9/13 閲覧)*

[13] *CERT-UA「Кібератака APT28: msedge як завантажувач, TOR та сервіси mockbin.org/website.hook як центр управління (CERT-UA#7469)(2023/9/4)」、https://cert.gov.ua/article/5702579 (2023/10/3 閲覧)*

[14] *JumpCloud「Incident Details(2023/7/12)」、https://jumpcloud.com/blog/security-update-incident-details (2023/8/22 閲覧)*

[15] *경기남부경찰청「(보도자료) 한미연합연습 노린 북 '김수키' 소행 사이버 공격 확인(2023/8/20)」、http://www.ggpolice.go.kr/main/bbsview.do (2023/9/4 閲覧)*

[16] *Google「Active North Korean campaign targeting security researchers(2023/9/7)」、https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/ (2023/9/27 閲覧)*

不正アクセスを受け、クレジットカード情報が 910 件漏えいした可能性があることを公表。

- ○ 調査の結果、7 月 22 日、同市は同サイトにおいて会員登録を行った者及び当サイトを通じて本市に寄附をした者の最大で 2,280 人の個人情報が漏えいした恐れがある旨公表[17]。

3.1.2 福岡徳洲会病院における不正アクセス

- ○ 2023 年 7 月 28 日、福岡徳洲会病院は、第三者から不正アクセスを受け、データベースに保存されている個人情報及び患者情報が外部から閲覧可能な状態になっていた旨を公表。
- ○ 漏えいした可能性ある情報は、患者情報(氏名、住所、生年月日、投薬内容、病名、検査値)最大 48,983 件のほか職員、学生、研修生の情報[18]。

3.1.3 法人向けインターネットバンキング AnserBizSOL のシステム障害

- ○ 2023 年 8 月 31 日、法人向けインターネットバンキングサービス「AnserBizSOL」でシステム障害が発生、AnserBizSOL を利用する銀行と信用組合の一部で法人向けインターネットバンキングが利用できなくなった。
- ○ 午前 9 時 10 分に発生し、午前 11 時 47 分に復旧、影響を受けたのは、NTT データが支援するシステム共同センター「MEJAR」に参画している横浜銀行、七十七銀行、北陸銀行、北海道銀行、東日本銀行や、複数の信用組合[19]。

3.2. その他

3.2.1 名古屋港へのランサムウェア攻撃

- ○ 2023 年 7 月 4 日早朝、名古屋港運協会(名古屋市)は、NUTS(名古屋港統一ターミナルシステム)に障害が発生し、名古屋港全ターミナルの作業を停止したと発表。
- ○ 7 月 6 日 18 時には全ターミナルで作業を再開。障害の原因は、リモート機器の脆弱性を突かれた不正アクセスにより、ランサムウェアに感染し、データセンター内の NUTS の全サーバーが暗号化された可能性[20]。

---

[17] *志布志市「本市が運営する「志布志市ふるさと納税特設サイト」への外部の第三者からの不正アクセスによる個人情報漏えいに関するお詫びとお知らせ(第 2 報)(2023/7/20)」、https://www.city.shibushi.lg.jp/soshiki/5/22558.html (2023/12/1 閲覧)*

[18] *福岡徳洲会病院「不正アクセスによる個人情報流出の可能性についてお知らせとお詫び(2023/7/28)」https://www.f-toku.jp/news/detail.php?id=226 (2023/12/1 閲覧)*

[19] *日経クロステック「NTT データの法人向けインターネットバンキングで障害、2 時間半で復旧(2023/8/31)」、https://xtech.nikkei.com/atcl/nxt/news/18/15843/ (2023/12/1 閲覧)*

[20] *名古屋港協会「NUTS システム障害の経緯報告(2023/7/26)」、https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf (2023/12/1 閲覧)*

資料２関連

豪州サイバーセキュリティ戦略の公表について

2023年11月、豪州政府は「2023-2030年 豪州サイバーセキュリティ戦略」を公表した。
豪州をサイバーセキュリティ分野における世界的リーダーとするための2030年までのビジョンを示しており、重要インフラ防護を含む6層のサイバーシールドを官民の連携により強化し、国家のサイバーレジリエンスを構築するとした。
https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

	（サイバーシールド）	（主な取組）
1	**強固な企業と市民** 市民と企業は、サイバー脅威から保護され、サイバー攻撃から迅速に回復することができる。	①中小企業のサイバーセキュリティ支援　②サイバー脅威からの国民の保護 ③豪州へのサイバー攻撃の阻止④官民連携によるランサムウェアビジネスの打破 ⑤企業へのガイダンス提供　⑥インシデント対応支援　⑦IDの保護
2	**安全なテクノロジー** 豪州の国民は、デジタル製品やサービスが安全で目的に適合していることを信頼できる。	⑧信頼できるデジタル製品とソフトウェア ⑨最も価値のあるデータセットの保護 ⑩新興技術の安全な利用の促進
3	**世界最高水準の脅威共有・ブロック** 豪州は、リアルタイム脅威情報にアクセスでき、大規模な脅威をブロックすることができる。	⑪経済全体にわたる脅威インテリジェンスネットワークの構築 ⑫サイバー攻撃阻止のための大規模な脅威ブロック機能
4	**重要インフラ防護** 我々の重要インフラや不可欠な政府システムは、サイバー攻撃に耐え、立ち直ることができる。	⑬重要インフラ規制のスコープ明確化 ⑭重要インフラのサイバーセキュリティ義務と遵守の強化 ⑮政府のサイバーセキュリティ強化　⑯脆弱性特定のための負荷テスト
5	**主権能力** 豪州は、多様で専門的なサイバー人材により、サイバー産業を繁栄させる。	⑰国家サイバー人材の育成と専門化 ⑱ローカルのサイバー産業、研究、技術革新の加速
6	**強靭な地域とグローバルリーダーシップ** 豪州の地域は、サイバー強靭性を増し、デジタル経済によって繁栄する。国際法や規範を遵守し、共通の利益に適った国際基準を作る。	⑲パートナーとして選ばれるための地域におけるサイバー強靭性の支援 ⑳国際的なサイバールール、規範、基準の形成、支持、擁護

重要インフラにおける情報共有件数について(2023 年度第 2 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	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(※1)	269	309	407	302	99	53	―	―	152
関係省庁・関係機関からのNISCへの情報共有	16	16	6	2	0	0	―	―	0
NISCからの情報提供	38	64	91	83	15	28	―	―	43

(※1) 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	―	―	10
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	―	―	13
	完全性を脅かす事象	情報の破壊	11	12	20	15	5	6	―	―	11
	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	―	―	87
	上記につながる事象	マルウェア等の感染	9	18	46	38	2	4	―	―	6
		不正コード等の実行	5	3	2	1	1	0	―	―	1
		システム等への侵入	14	26	24	22	6	2	―	―	8
		その他	47	42	80	36	11	5	―	―	16

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	―	―	4
	ユーザＩＤ等の偽り	12	9	7	7	4	0	―	―	4
	DDoS攻撃等の大量アクセス	20	10	19	28	16	6	―	―	22
	情報の不正取得	8	13	13	10	5	2	―	―	7
	内部不正	0	0	1	1	0	1	―	―	1
	適切なシステム等運用の未実施	11	23	15	8	2	0	―	―	2
偶発的な原因	ユーザの操作ミス	6	18	10	12	4	0	―	―	4
	ユーザの管理ミス	6	13	14	7	4	0	―	―	4
	不審なファイルの実行	7	7	22	26	1	0	―	―	1
	不審なサイトの閲覧	5	3	6	4	4	1	―	―	5
	外部委託先の管理ミス	39	56	107	49	14	12	―	―	26
	機器等の故障	62	39	38	43	8	12	―	―	20
	システムの脆弱性	16	38	32	12	11	6	―	―	17
	他分野の障害からの波及	4	7	10	7	1	2	―	―	3
環境的な原因	災害や疾病等	13	9	3	5	0	1	―	―	1
その他の原因	その他	33	35	48	29	14	10	―	―	24
	不明	53	68	79	62	21	6	―	―	27

3. サイバー攻撃による事象の種別内訳(情報連絡を元に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(※2)	FY2020 計(※2)	FY2021 計(※2)	FY2022 計(※2)	FY2023 1Q	FY2023 2Q	FY2023 3Q	FY2023 4Q	FY2023 計
総計	87	100	174	143	52	18	―	―	70
ランサムウェア攻撃	8	13	46	30	8	5	―	―	13
ランサムウェアを除くマルウェア感染	11	8	29	27	2	1	―	―	3
DDoS攻撃等の大量アクセス	14	4	15	25	10	6	―	―	16
その他	54	75	84	61	32	6	―	―	38

(※2) 件数は今後の精査により修正の可能性がある

(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(2023 年度第２四半期)

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

海外グループ会社経由の不正アクセスを許し情報漏えいに至ってしまった事例の他、ランサムウェア感染や DDoS 攻撃などのサイバー攻撃の被害の報告もあった。委託先を含め多層防御の必要がある。また、システム障害では、引き続き、設定ミス、手順ミスなどを起因とするものが複数寄せられており、適切な事前準備が求められる。

○ ネットワークの適切なセグメント分けとアクセス制御、監視が必要

海外グループ会社を経由した不正アクセスによる情報漏えいが発生した事例があった。一方で、侵害にあったネットワークと基幹系ネットワークが分離されていたため、主要なサービスへの影響が限定的であった事例があった。グループ企業間でセキュリティに関する運用の水準が異なる場合があることも踏まえ、組織内でのマルウェアの感染拡大を防ぐための措置が必要。

また、認証情報が漏えいした場合も想定し、事後の不正アクセスを防ぐために多要素認証などの認証強化が必要。

○ 委託先を含み、適切なネットワーク接続部分の資産管理及び脆弱性管理が必要

閉鎖的なネットワーク環境での運用を前提としていたシステムについて、委託先がインターネットに接続したことによりランサムウェアに感染した事例があった。また、VPN 機器に関して、適切なアクセス制限をしておらず、かつ、既知の脆弱性への修正プログラムが未適用であったことにより、ランサムウェアが侵入したと考えられる事例があった。

○ 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

DDoS 攻撃とみられる大量のアクセスを受けた事例が複数あった。サービスの重要度に応じた DDoS 攻撃への耐性向上のための対策に加え、障害発生時における代替手段の用意と適切な広報など事前の備えが必要。

○ ウェブサイト作成のためのソフトウェアの適切な管理が必要

ウェブサイトに無関係な海外のサイトへのリンクが設定された事例や、既知の脆弱性への修正プログラムが未適用だったことを原因としたウェブサイトの改ざん事例があった。作成したいウェブサイトに応じたソフトウェアの選択と、機能拡張のために追加したソフトウェアを含めた適切な脆弱性管理が必要。また、復旧に長期間要した事例もあり、ウェブサイトの停止や再構築の手順を確立しておくなどの事前準備が必要。

○ 作業手順書の確認など適切な事前準備が必要

システムメンテナンスの際の設定ミス、データの誤削除といった作業ミスによるシステム障害や、テスト環境から本番環境へ移行する際の確認不足によるウェブサイトの誤表示など、適切な事前準備により防げるインシデントが複数あった。

○ リスクアセスメントを踏まえた IT-BCP が必要

機器の故障に起因したシステム障害が多数あった。故障自体を防ぐことは困難であることから、提供するサービスの重要度も踏まえた冗長化等を検討することが必要。また、冗長化していたはずのシステムが適切に機能せず、サービスの提供に影響が出た事例も複数あった。機器故障が起きた場合を想定した影響の検討や、それを踏まえた対応手順の確立などの準備が必要。

以上