資料２

令和 4 年 12 月 22 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(2022 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、2022 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 ウクライナとの協力

○ 2022 年 7 月 22 日、米国 CISA は、CISA とウクライナ国家特殊通信情報保護局(SSSCIP)が共通のサイバーセキュリティの優先事項に関する協力を強化するための覚書(MOC)に署名したことを公表[1]。

1.1.2 JCDC の成果に係るコメント

○ CISA は、2021 年 8 月に設立した、政府機関と民間セクターとの共同サイバー防御協力に係る取組である JCDC(JOINT CYBER DEFFENSE COLLABORATIVE)の過去 1 年間の成果を総括したコメントを公表[2]。

○ 2021 年 12 月の Log4j の脆弱性への対応や、2022 年 2 月に Daxin マルウエアが発見された際の対応でのコラボレーション、ウクライナ情勢を受けた Shields-Up キャンペーン立ち上げ等の成果に言及。

1.1.3 ソフトウエア・サプライチェーン・ガイダンス

○ 2022 年 9 月 1 日、米国国家安全保障局(NSA)、米国サイバーセキュリティ・

---

1 CISA「UNITED STATES AND UKRAINE EXPAND COOPERATION ON CYBERSECURITY(2022/7/27)」、https://www.cisa.gov/news/2022/07/27/united-states-and-ukraine-expand-cooperation-cybersecurity (2022/8/18 閲覧)

2 CISA「CONNECTING THE DOTS TO DRIVE DOWN CYBER RISK TOGETHER: THE SUPERHEROES BEHIND THE NATION'S JCDC(2022/8/12)」、https://www.cisa.gov/blog/2022/08/12/connecting-dots-drive-down-cyber-risk-together-superheroes-behind-nations-jcdc (2022/9/16 閲覧)

インフラセキュリティ庁(CISA)及び国家情報長官室(ODNI)は、ソフトウエア・サプライチェーン攻撃から保護するための開発者向けガイダンス Software Supply Chain Guidance for Developers を公表[3]。

○ 「SolarWinds」や「Log4j」等の事案を受け、ソフトウエア・サプライチェーンの強化に向けセキュリティ基準への適合等について策定する、開発者向け、サプライヤー向け、ソフトウエアを購入した顧客向けの 3 つのガイドラインのうちの第一弾。

1.1.4 サイバーインシデント報告法の報告要件に関する RFI

○ 2022 年 9 月 9 日、CISA は、2022 年 3 月にバイデン大統領が署名した「重要インフラのためのサイバーインシデント報告法(the Cyber Incident Reporting for Critical Infrastructure Act)」に従い、サイバーインシデントの報告要件について、一般の意見を求める情報提供要請(Request For Information(RFI))を実施する旨公表。

○ RFI では、「網羅的ではない」と前置きした上で、情報提供を要請する対象について、主なものとして、「規制対象の定義、基準及び範囲」、「報告内容と提出方法」、「その他のインシデント報告要件と脆弱性情報の共有」、「追加のポリシー、手順及び要件」を記載[4]

○ サイバーインシデントの報告要件については、法の制定から 24 か月以内に草案を公表し、そこから 18 か月以内に最終規則を発行することとなっている。

1.2. 中国

1.2.1 データ域外移転安全評価弁法

○ 2022 年 9 月 1 日、中国国家インターネット情報弁公室は、中国国内での事業運営を通じて収集・生成した重要データや個人情報を域外に提供する際の安全評価手続きを定めた「データ域外移転安全評価弁法」を施行[5]。

○ 重要データや個人情報等を域外に提供する際、事業者が所在する省のネットワーク情報部門を通じ、国家ネットワーク情報部門にデータ域外移転安全評価の審査を申請することを義務付け[6]。

---

3 NSA, CISA, ODNI「NSA, CISA, ODNI Release Software Supply Chain Guidance for Developers(2022/9/1)」、https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3146465/nsa-cisa-odni-release-software-supply-chain-guidance-for-developers/ (2022/9/30 閲覧)

4 CISA「CISA WELCOMES INPUT ON NEW CYBER INCIDENT REPORTING REQUIREMENTS(2022/9/9)」、https://www.cisa.gov/news/2022/09/09/cisa-welcomes-input-new-cyber-incident-reporting-requirements (2022/10/14 閲覧)

5 国家互联网信息办公室「国家互联网信息办公室令第 11 号(2022/7/7)」、http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm (2022/12/8 閲覧)

6 JETRO「データ域外移転安全評価弁法、9 月 1 日から施行、安全評価の審査対象が明確に(2022/7/12)」、https://www.jetro.go.jp/biznews/2022/07/d98b4f5993babebd.html (2022/12/8 閲覧)

1.2.2 インターネット利用者の管理を強化する新たな規定

○ 2022 年 8 月 1 日、中国国家インターネット情報弁公室は、SNS 運営事業者に対し、利用者のアカウント管理を強化するよう求める「インターネット加入者アカウント情報管理規定」を施行 [7]。

○ 規定では、利用者の実名登録の義務付け、登録情報が事実と異なる等法律に違反した場合のアカウント閉鎖や新たなアカウントの作成の禁止、規制当局への報告等について規定 [8]。

1.2.3 サイバーセキュリティ法の改正案に係る意見募集

○ 2022 年 9 月 12 日、中国国家インターネット情報弁公室は、2017 年のサイバーセキュリティ法施行以降の情勢変化に対応した行政処罰法、データセキュリティ法、個人情報保護法等の法改正・制定を受け、サイバーセキュリティ法の改正案を公表、意見募集を実施 [9]。

○ 主に、違反した企業に対して科す過料について、現行法では 100 万元以下と定めているが、改正案では「5,000 万元以下」又は「前年度の売上高の 5%以下」(いずれも「情状が特に重大な場合」)まで引き上げ。個人(直接責任を負う主管人員とその他直接責任者)に対する過料は、現行法の 10 万元以下から 100 万元以下に引き上げ [10]。

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 カナダの通信事業者 Rogers で大規模障害

○ カナダ大手通信事業者の Rogers Communications において、2022 年 7 月 8 日(金)朝 5 時～7 月 8 日(金)夜の約 19 時間、通信障害が発生 [11]。

○ カナダ全土で広範囲に障害が発生し、緊急通報を含む固定電話や携帯電話、インターネットやテレビ等の様々なサービスに影響。同社の 1000 万人以上の顧客に電話不通とインターネット接続断の影響 [12]。

---

7 国家互联网信息办公室「国家互联网信息办公室发布《互联网用户账号信息管理规定》(2022/6/27)」、http://www.cac.gov.cn/2022-06/26/c_1657868775333429.htm (2022/12/8 閲覧)

8 NHK「中国 "ネット利用者の管理強化"新指針施行 党大会前に統制か(2022/8/1)」、https://www3.nhk.or.jp/news/html/20220801/k10013747001000.html (2022/12/8 閲覧)

9 国家互联网信息办公室「关于修改《中华人民共和国网络安全法》的决定(征求意见稿)(2022/9/12)」、http://www.cac.gov.cn/2022-09/14/c_1664781649609823.htm (2022/12/8 閲覧)

10 JETRO「サイバーセキュリティー法の改正案公表、過料引き上げなど罰則規定を整備(2022/9/29)」、https://www.jetro.go.jp/biznews/2022/09/a0501adfc0d197eb.html (2022/12/8 閲覧)

11 CTVNews「What we know about the network system failure that led to the Rogers outage(2022/7/12)」、https://www.ctvnews.ca/business/what-we-know-about-the-network-system-failure-that-led-to-the-rogers-outage-1.5982790 (2022/12/7 閲覧)

12 The verge「Rogers restores service for 'vast majority' of customers after massive outage(2022/7/10)」https://www.theverge.com/2022/7/9/23201678/rogers-communications-restores-service-vast-majority-customers-widespread-outage (2022/12/7 閲覧)

○ 金曜日早朝に実施したコアネットワークをアップデートするためのメンテナンス時に失敗が発生したことが原因。コアルーターの一部が誤作動し、それによりトラフィックの過負荷が発生。その結果、システム全体がシャットダウン [13]。

2.1.2 犯罪者グループが英国水道会社にサイバー攻撃を主張

○ 「Clop」と呼ばれるサイバー犯罪者グループが英国の大手水道会社である Thames Water 社の IT システムにアクセスしたとリーク Web サイトで主張 [14]。
○ しかし、Thames Water 社はこのサイバー犯罪者グループの主張に対して公式に反論し、Clop が同社のネットワークを侵害したという報告はデマであり、同社の業務はフル稼働していると声明を発表。
○ 他方で、リークされた情報は、South Staff Water 社及び South Staffordshire Water 社のものであるという指摘もあるが、同社は顧客への安全な水の供給に影響はないことを確認したと声明を発表。

2.1.3 パリ郊外の病院、サイバー攻撃被害に

○ パリ南部の南部、エッソンヌ県の病院がサイバー攻撃に遭い、病院の活動に影響 [15]。
○ 攻撃は 8 月中旬の週末に始まり、緊急手術のみ行い、その他の手術や治療は他病院へ患者を誘導したり延期するなどの事態 [16]。
○ 診療予約、患者のカルテも見られず、MRI やレントゲンの画像保存にも支障が起きており、カルテや処方箋などのデータも全て手書きで対応。

2.1.4 北京の地下鉄防疫システムに障害

○ 9 月 13 日、北京の地下鉄全駅の改札口で、新型コロナウイルスの感染リスクを乗客ごとに点検するシステムに障害が発生し、駅に入れない人々で大混雑する騒ぎが発生 [17]。
○ 濃厚接触者ではないことなどを証明するスマホアプリが読み取れなくなり、

---

13 CP24「Some Ontario residents still left without service after Rogers outage(2022/7/9)」、https://www.cp24.com/news/some-ontario-residents-still-left-without-service-after-rogers-outage-1.5981251 (2022/12/7 閲覧)

14 Bleepingcomputer「Hackers attack UK water supplier but extort wrong company(2022/8/16)」、https://www.bleepingcomputer.com/news/security/hackers-attack-uk-water-supplier-but-extort-wrong-company/ (2022/12/7 閲覧)

15 Antennefrance「ハッカーがパリ地方病院へのサイバー攻撃終了に 1,000 万ドルを要求(2022/8/23)」、https://www.antennefrance.com/internet/cyber-attack-on-paris-regional-hospital/ (2022/12/7 閲覧)

16 Ovninavi「パリ郊外の病院、サイバー攻撃被害に。犯人は 1000 万ドルの「rançongisiel」要求。(2022/8/23)」、https://ovninavi.com/%e3%83%91%e3%83%aa%e9%83%8a%e5%a4%96%e3%81%ae%e7%97%85%e9%99%a2%e3%80%81%e3%82%b5%e3%82%a4%e3%83%90%e3%83%bc%e6%94%bb%e6%92%83%e8%a2%ab%e5%ae%b3%e3%81%ab%e3%80%82/ (2022/12/7 閲覧)

17 共同通信「北京の地下鉄防疫システムに障害 駅に入れない人々で大混雑(2022/9/13)」、https://nordot.app/942313069829292032 (2022/12/7 閲覧)

係員が一人一人のスマホを目視で点検した。当局は午前中に復旧したと説明。

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

- 2022 年 8 月、APT41(Winnti, Wicked Panda)について、2021 年に米国・台湾等の 13 の組織を標的としたサイバー攻撃キャンペーンが実施された旨、セキュリティ企業が報告 [18]
- 2022 年 9 月、BlackTech について、F5 BIG-IP の脆弱性(CVE-2022-1388)を悪用した攻撃活動に関連していると推測される旨、JPCERT/CC が報告 [19]

2.2.2 ロシア関連

- 2022 年 7 月、主にウクライナ及びウクライナを支援する国家の政府機関、重要インフラ(エネルギー企業)及び国民を標的とした DDoS 攻撃、マルウエアの送付、フィッシングキャンペーンがセキュリティ企業等により多数報告 [20] (XakNet、Trickbot グループ、Killnet、UAC-0056、Turla、Gamaredon、BERSERK BEAR 等)。
- 2022 年 8 月、Killnet がウクライナに HIMARS を提供するロッキード・マーチン社への DDoS 攻撃について犯行声明。このほか、スペイン、ラトビア、エストニア、モルドバ、フィンランド、モンテネグロ等の政府機関・企業等を標的とした DDoS 攻撃、マルウエア送付が、セキュリティ企業等から多数報告 [21]。
- 2022 年 8 月、サイバー攻撃を受けたモンテネグロに対し、フランス(国家情報システムセキュリティ庁(ANSSI))や米国(連邦捜査局(FBI)サイバーアクションチーム(CAT))が支援 [22]。

2.2.3 北朝鮮関連

- 2022 年 7 月、医療及び公衆衛生部門の組織を標的としたランサムウエア「Maui」の攻撃について CISA から警告が発出 [23]。

---

18 Group-IB「APT41 World Tour 2021 on a tight schedule(2022/8/18)」、https://blog.group-ib.com/apt41-world-tour-2021 (2022/9/6 閲覧)

19 JPCERT/CC「攻撃グループ BlackTech による F5 BIG-IP の脆弱性(CVE-2022-1388)を悪用した攻撃(2022/9/15)」、https://blogs.jpcert.or.jp/ja/2022/09/bigip-exploit.html (2022/10/3 閲覧)

20 CNN「Russian hackers allegedly target Ukraine's biggest private energy firm(2022/7/5)」、https://edition.cnn.com/2022/07/01/politics/russia-ukraine-dtek-hack/index.html (2022/8/16 閲覧)

21 LIFE「"Спонсор мирового терроризма": Хакеры объявили о запуске атаки на производителя HIMARS(2022/8/1)」、https://life.ru/p/1513325 (2022/9/7 閲覧)

22 Databreachtoday「Cuba Ransomware Gang Takes Credit for Attacking Montenegro(2022/8/30)」、https://www.databreachtoday.com/cuba-ransomware-gang-takes-credit-for-attacking-montenegro-a-19938 (2022/9/13 閲覧)

23 Databreachtoday「Cuba Ransomware Gang Takes Credit for Attacking Montenegro(2022/8/30)」、https://

○ 2022 年 9 月、Lazarus について、2022 年 2 月から 7 月にかけてカナダ、米国、及び日本のエネルギー企業に対して攻撃を実施した旨、Cisco Systems 社の Talos が公表[24]。

○ 2022 年 9 月、ZINC について、2022 年 4 月下旬から 9 月中旬にかけて、米国、英国、インド、ロシアのメディア、防衛、航空宇宙、IT サービス等の複数の業界の組織の従業員を標的とするソーシャルエンジニアリングを実施した旨、Microsoft 社が報告[25]。

2.3. その他

2.3.1 米国司法省が北朝鮮の攻撃者から約 50 万ﾄﾞﾙの身代金を押収)

○ 2022 年 7 月、FBI が米国カンザス州の医療センターから支払われた身代金及び捜査の過程で新たに発覚した被害組織の身代金を押収し、被害組織へ返還した旨公表[26]。

○ 同医療センターで発生したランサムウエア攻撃に関し、医療サービス継続のため被害組織が 10 万ドルの身代金を支払っていた(2021 年 5 月)[27]。

○ 米国政府としては身代金の支払い要求に応じることに強く反対する立場を表明しており、HPH の組織に対する注意喚起により「Maui」ランサムウエアに対する対策内容を周知[28]。

2.3.2 サイバーセキュリティ安全審査委員会(CSRB)の報告書

○ 2022 年 7 月 14 日、DHS は、2021 年 12 月に発見された Log4j の脆弱性に係るサイバーセキュリティ安全審査委員会(CSRB)の報告書を公表。本報告書では、本脆弱性は継続中であるとし、継続的なリスクへの対処等 4 つの推奨事項を提示[29]。

---

www.databreachtoday.com/cuba-ransomware-gang-takes-credit-for-attacking-montenegro-a-19938 (2022/9/13 閲覧)

24 Cisco Talos「Lazarus and the tale of three RATs (2022/9/8)」、https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html (2022/9/29 閲覧)

25 Microsoft 「ZINC weaponizing open-source software (2022/10/21)」、https://www.microsoft.com/security/blog/2022/09/29/zinc-weaponizing-open-source-software/ (2022/10/18 閲覧)

26 DOJ「Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside(2022/6/7)」、https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (2022/8/4 閲覧)

27 DOJ「Deputy Attorney General Lisa O. Monaco Delivers Keynote Address at International Conference on Cyber Security (ICCS) 2022(2022/7/19)」、https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-keynote-address-international-conference (2022/8/1 閲覧)

28 CISA「Alert (AA22-187A) North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector(2022/7/6)」、https://www.cisa.gov/uscert/ncas/alerts/aa22-187a (2022/7/28 閲覧)

29 CISA「Review of the December2021 Log4j Event(2022/7/11)」、https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf (2022/8/5 閲覧)

2.3.3　米国下院議長訪台に伴うサイバー事案

○ 8 月 2 日からのペロシ米国下院議長による台湾訪問に伴い、台湾では、DDoS 攻撃、デジタルサイネージ改変、偽情報流布など、様々なサイバー関連事象が発生 [30]。

2.3.4　Hikvision 社製ネットワークカメラの脆弱性「CVE-2021-36260」

○ 2022 年 8 月 24 日、Cyfirma 社が 100 か国以上で 80,000 台を超える Hikvision 社(本社:中国)製のネットワークカメラが脆弱性「CVE-2021-36260」に対して保護されていない状態でインターネット接続されていると報告、修正にはファームウエアのアップデートが必要 [31]。

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　大規模な通信サービス障害(2022 年 7 月～9 月)

○ 2022 年 7 月 2 日、KDDI の通信サービスで大規模な通信障害が発生し、同社は電気通信事業法上の重大な事故として総務省に報告 [32]。

○ 2022 年 8 月 25 日には NTT 西日本、9 月 4 日には楽天モバイルで重大な事故に該当する通信障害が発生 [33]。

○ 通信サービスを利用出来ないことで、QR コード決済等の様々なサービスが利用できなくなり、国民生活や社会経済に影響 [34]。

3.1.2　5 地銀で一時システム障害

○ 2022 年 8 月 8 日、北海道銀行、横浜銀行、七十七銀行、東日本銀行及び北陸銀行の 5 つの地方銀行でシステム障害が一時発生。ATM やインターネットバンキングで他行への振り込みが一部できなくなったが、9 日午前までに復旧。5 行は NTT データの共通システム「MEJAR」を利用 [35]。

○ 原因は、MEJAR に参加している銀行の店舗情報を変更する際、NTT データの設定に不具合。

---

30 フォーカス台湾「ペロシ氏訪台/桃園空港に脅迫状 ペロシ氏の台湾訪問阻止を狙う 警察が保安検査強化(2022/8/2)」、https://news.yahoo.co.jp/articles/9a072a075bc8cdc6bcce661bb73a613dcfed1f5d (2022/9/16 閲覧)

31 Cyfirma「Thousands of Hikvision Cameras are still vulnerable and can be potentially exploited(2022/8/24)」、https://www.cyfirma.com/wp-content/uploads/2022/08/HikvisionSurveillanceCamerasVulnerabilities.pdf (2022/9/6 閲覧)

32 KDDI「7 月 2 日に発生した通信障害について(2022/7/29)」、https://www.kddi.com/important-news/20220729_01/ (2022/10/21 閲覧)

33 楽天モバイル「2022 年 9 月 4 日に発生した通信障害について(2022/10/4)」、https://network.mobile.rakuten.co.jp/information/news/other/2136/ (2022/10/21 閲覧)

34 大垣共立銀行「ATM 通信障害の発生しについて(2022/7/2)」、https://www.okb.co.jp/archive/2022/20220702-03.html (2022/10/21 閲覧)

35 時事通信「5地銀で一時システム障害　振り込み一部できず(2022/8/9)」、https://www.jiji.com/jc/article?k=20220809003628g=eco (2022/12/7 閲覧)

3.1.3　日銀決済システム、長時間不具合

- ○ 2022 年 9 月 14 日、日本銀行と民間金融機関を接続し、資金や国債の決済などに使う日本銀行の電子決済システム「日銀ネット」で不具合が発生。外国為替取引や日銀との国債のやりとりで遅れが発生[36]。
- ○ 不具合は 14 日午前 9 時頃発生し、同日夕、原因となった機器を交換し、不具合は解消。

3.2.　その他

3.2.1　海外ハッカー集団による日本への攻撃の宣言

2022 年 9 月 6 日から 17 日にかけ、Killnet、MIRAI 及び PHOENIX は、日本の政府機関等へのサイバー攻撃を示唆する内容を Telegram に投稿した。その際、行政及び民間企業等が運営する Web サイトの閲覧障害が発生。DDoS 攻撃とみられる事象も見受けられた。

- ○ 9 月 6～8 日、Killnet による日本への攻撃示唆と宣戦布告[37]。
- ○ 9 月 6 日以降、日本の行政サービス及び民間企業等の Web サイトの閲覧障害発生[38]。
- ○ 9 月 10～17 日、MIRAI による日本への攻撃示唆[39]。
- ○ 9 月 11～13 日、PHOENIX による日本への攻撃示唆[40]。

---

*36 日経新聞「日銀決済システム、長時間「不具合」 外為決済に遅れ(2022/9/14)」、https://www.nikkei.com/article/DGXZQOUB142YU0U2A910C2000000/（2022/12/7 閲覧)H^*

37 Telegram「WE ARE KILLNET@killnet_reservs の投稿」、https://t.me/s/killnet_reservs（2022/10/19 閲覧）

38 Twitter「デジタル庁@digital_jpn の投稿(2022/9/6)」、https://twitter.com/digital_jpn/status/1567120572043395076（2022/10/17 閲覧）

39 Telegram「MIRAI@QBOTDDOS の投稿」、https://t.me/s/QBOTDDOS（2022/10/19 閲覧）

40 Telegram「PHOENIX@phoenixinform の投稿」、https://t.me/s/phoenixinform（2022/10/19 閲覧）

重要インフラにおける情報共有件数について(2022 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	FY2018 計	FY2019 計	FY2020 計	FY2021 計	FY2022 1Q	FY2022 2Q	FY2022 3Q	FY2022 4Q	FY2022 計
重要インフラ事業者等からNISCへの情報連絡(※)	223	269	309	407	78	83	―	―	161
関係省庁・関係機関からのNISCへの情報共有	7	16	16	6	0	0	―	―	0
NISCからの情報提供	43	38	64	91	18	18	―	―	36

(※) 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			FY2018 計	FY2019 計	FY2020 計	FY2021 計	FY2022 1Q	FY2022 2Q	FY2022 3Q	FY2022 4Q	FY2022 計
未発生の事象		予兆・ヒヤリハット	27	12	28	25	15	2	―	―	17
発生した事象	機密性を脅かす事象	情報の漏えい	13	13	23	29	5	5	―	―	10
	完全性を脅かす事象	情報の破壊	17	11	12	20	5	4	―	―	9
	可用性を脅かす事象	システム等の利用困難	97	158	157	181	29	37	―	―	66
	上記につながる事象	マルウェア等の感染	17	9	18	46	13	15	―	―	28
		不正コード等の実行	4	5	3	2	0	0	―	―	0
		システム等への侵入	14	14	26	24	2	5	―	―	7
		その他	34	47	42	80	9	15	―	―	24

2. 原因別類型 (複数選択)

原因の類型		FY2018 計	FY2019 計	FY2020 計	FY2021 計	FY2022 1Q	FY2022 2Q	FY2022 3Q	FY2022 4Q	FY2022 計
意図的な原因	不審メール等の受信	36	13	9	47	19	12	―	―	31
	ユーザＩＤ等の偽り	3	12	9	7	2	2	―	―	4
	DDoS攻撃等の大量アクセス	17	20	10	19	8	6	―	―	14
	情報の不正取得	10	8	13	13	3	2	―	―	5
	内部不正	1	0	0	1	0	0	―	―	0
	適切なシステム等運用の未実施	14	11	23	15	2	0	―	―	2
偶発的な原因	ユーザの操作ミス	10	6	18	10	2	6	―	―	8
	ユーザの管理ミス	6	6	13	14	2	2	―	―	4
	不審なファイルの実行	16	7	7	22	14	10	―	―	24
	不審なサイトの閲覧	4	5	3	6	0	1	―	―	1
	外部委託先の管理ミス	29	39	56	107	11	14	―	―	25
	機器等の故障	27	62	39	38	7	11	―	―	18
	システムの脆弱性	19	16	38	32	4	3	―	―	7
	他分野の障害からの波及	6	4	7	10	3	3	―	―	6
環境的な原因	災害や疾病等	1	13	9	3	2	2	―	―	4
その他の原因	その他	29	33	35	48	8	5	―	―	13
	不明	46	53	68	79	11	20	―	―	31

(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(2022 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からの情報連絡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

管理ミスを原因としたサービスの利用停止の事例が複数報告され、広範囲かつ長時間にわたる障害により、他の重要インフラ分野にも影響を及ぼす事例もあった。また、ウェブサイト等に対するサービス不能攻撃とみられる大量のアクセスや、これを要因としたウェブサイトの閲覧障害やサービスの提供に影響を及ぼす事例が複数発生した。更に、同じ分野の複数の事業者が利用する同一の委託先のサービス等のシステム障害により、当該複数事業者全てに影響を及ぼした事例も報告された。

取引先や委託先等のサプライチェーンを含めた管理が必要であり、インシデント発生時には、システム・サービスの復旧に加えて適切な広報の実施も含めた、迅速な対応が求められる。

○　ベンダー等関係者との情報連携や手順書の確認など適切な事前準備が必要

メンテナンス作業時などにおける作業手順書の確認不足や設定不備、ベンダーとユーザーとの認識の齟齬を起因とするシステム障害によりサービスの提供に支障が生じた事例が複数あった。障害発生時の適切な広報の実施のため、経営層による判断・対応、広報部門との連携も重要。

○　所与のサービスが利用不可となった場合を想定した BCP の策定と点検が必要

利用を前提としているサービスについて、障害により利用不可となった際に自組織が提供するサービスにも影響を及ぼした事例があった。

○　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や、これを要因とした自組織のウェブサイトの閲覧障害、サービス提供にも影響を及ぼした事例が発生した。

○　外部サービスの不具合を前提とした多重化・多様化等による代替手段の確保が必要

複数の事業者が利用する同一の委託先のサービス等について、当該委託先のシステム障害等により、同時期に多数の事業者のサービスの提供に影響が生じた事例が複数あった。

○　多重防御に加え、ネットワーク接続にかかる資産管理の重要性の再認識が必要

ランサムウェアにより業務上必要となるデータの暗号化が行われたことで、サービスの提供に支障が出た事例があった。他方で、海外子会社の一部のシステムにおいてランサムウェアの被害にあったものの、国内含めその他のシステムには影響が無かった事例があった。

以上