資料４

令和５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

サイバーセキュリティを取り巻く情勢(2022 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、2022 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 米国国家サイバーセキュリティ戦略

- 2023 年 3 月 2 日、ホワイトハウスは、4 年 4 か月ぶりに改定した「国家サイバーセキュリティ戦略」を公表[1]。
- 社会全体のデジタル技術への依存度の高まりや、中国、ロシア、イラン、北朝鮮及び非国家主体の悪意あるサイバー活動による米国の国家安全保障や社会経済活動への影響を踏まえ、5 つの柱から構成。
- 米国国家サイバーセキュリティ戦略の公表に関連して、2023 年 3 月 3 日、米国環境保護庁(EPA)は、公共水道システム(PWS)のサイバーセキュリティに関する覚書[2]及びガイダンス[3]を公表、3 月 7 日、米国運輸保安局は、空港及び航空機のオペレーターに係る新たなサイバーセキュリティ規則を公表[4]。
- 2023 年 3 月 9 日、バイデン政権は、国家サイバーセキュリティ戦略を踏まえ

---

[1] *The White House「FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy (2023/3/2)」、https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/ (2023/4/18 閲覧)*

[2] *EPA「Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Proces(2023/3/3)」、https://www.epa.gov/system/files/documents/2023-03/Addressing%20PWS%20Cybersecurity%20in%20Sanitary%20Surveys%20Memo_March%202023.pdf (2023/4/18 閲覧)*

[3] *EPA「Evaluating Cybersecurity During Public Water System Sanitary Surveys(2023/3/3)」、https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf (2023/4/18 閲覧)*

[4] *TSA「TSA issues new cybersecurity requirements for airport and aircraft operators(2023/3/7)」、https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft (2023/4/18 閲覧)*

た 2024 年度予算教書を公表。

1.1.2 DOJ が 13 か国の機関と連携し Hive に対し法的措置を実施

- 2023 年 1 月 26 日、DOJ が、HPH(Healthcare and Public Health:ヘルスケア及び公衆衛生)セクターを含む様々な組織を標的に攻撃を実施してきたランサムウェア攻撃グループ「Hive」に対する法的措置を実施したと公表[5]。
- ランサムウェア攻撃グループ「Hive」は、これまで 80 か国以上の 1,500 人以上の標的に対して攻撃を実施。
- 2022 年 7 月下旬以降、FBI は「Hive」のコンピュータネットワークに侵入し、ランサムウェアの復号化鍵を取得して世界中の被害者に提供。
- DOJ は、「Hive」ランサムウェアの被害者を少なくとも 336 人支援し、1 億 3,000 万ドル以上の身代金の支払いを防いだと公表。
- 合計 13 か国の法執行機関が「Hive」ランサムウェアに対する法的措置を支援[6]。
- 続いて、2023 年 3 月 24 日、DOJ は、サイバー犯罪者が盗まれたデータの取引などをする世界最大級の市場である BreachForums の創設者の逮捕と同フォーラムの閉鎖を公表[7]。

1.1.3 米国における TikTok 使用禁止等の動き

- 2023 年 2 月 27 日、米国行政管理予算局(OMB)は、連邦政府機関に対し、政府支給の携帯電話等から TikTok を削除することを命じた覚書を公表[8]。
- 本覚書の適用対象は、中国バイトダンス社又は同社が所有する事業体が開発・提供するソーシャルネットワーキングサービス TikTok 又は TikTok の後継アプリケーション若しくはサービスを対象とし、全ての行政機関に適用。
- 2023 年 3 月 1 日、米国議会下院議会外交委員会は、下院外交委のマコール委員長(共和党)が提案した TikTok 禁止法案を賛成多数で可決[9]。
- 上院議会では、3 月 7 日、ワーナー上院議員(民主党)及びテューン上院議員

---

[5] *DOJ「U.S. Department of Justice Disrupts Hive Ransomware Variant(2023/1/26)」、https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant（2023/2/13 閲覧）*

[6] *Europol「Cybercriminals stung as HIVE infrastructure shut down(2020/12/18)」、https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down（2023/2/13 閲覧）*

[7] *DOJ「Justice Department Announces Arrest of the Founder of One of the World's Largest Hacker Forums and Disruption of Forum's Operation(2023/3/24)」、https://www.justice.gov/opa/pr/justice-department-announces-arrest-founder-one-world-s-largest-hacker-forums-and-disruption（2023/5/18 閲覧）*

[8] *THE WHITE HOUSE「MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES (2023/2/27)」、https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf（2023/3/8 閲覧）*

[9] *Bloomberg「TikTok 禁止法案、共和党主導の米下院外交委が賛成多数で可決(2023/3/2)」、https://www.bloomberg.co.jp/news/articles/2023-03-02/RQV9RIT0G1KW01（2023/3/10 閲覧）*

(共和党)を筆頭とする 12 人の超党派の上院議員グループが情報通信技術を危険にさらす脅威の発生を制限する法(Restricting the Emergence of Security Threats that RiskInformation and Communications Technology ACT:RESTRICT 法)」を提出[10]。

1.2. 中国

1.2.1 個人情報域外移転標準契約弁法

- 個人情報保護法に基づく個人情報の域外移転の要件のひとつである「標準契約」の締結について定めた「個人情報域外移転標準契約弁法」(以下「標準契約弁法」)が 2023 年 2 月 24 日に公表、同年 6 月 1 日に施行予定[11]。
- 標準契約弁法では、標準契約の締結の対象として、
  - 重要情報インフラ運営者に該当しない
  - 取扱個人情報が 100 万人未満
  - 前年 1 月 1 日から起算して域外に提供した個人情報が累計 10 万人未満
  - 前年 1 月 1 日から起算して域外に提供した機微な個人情報が累計 1 万人未満

  以上のすべてを満たす場合と規定。
- 影響評価の実施、標準契約の締結、契約発効後の当局への届出を規定。

1.2.2 中国国家データ局の設立

- 2023 年 3 月 7 日、中国の第 14 期全国人民代表大会(全人代)第 1 回会議において国務院(内閣)の組織再編が提議され、データ分野では、新たに国家データ局を設立[12]。
- 同局は国家発展改革委員会が管理し、中央ネットワークセキュリティー・情報化委員会からデジタル中国建設プラン策定、公共サービスと社会ガバナンスの情報化推進、スマートシティー建設の推進、情報リソースの業界・部門をまたいだ共有・運用などの業務が移管。
- また、国家発展改革委員会からデジタルエコノミー発展に向けた調整や、国家ビッグデータ戦略の実施、データ要素基本制度の構築、デジタルインフラ配置などの業務を移管。

---

[10] *Gigazine「TikTok などセキュリティリスクがあるアプリや技術の利用を規制する「RESTRICT 法」の法案を超党派グループが提出(2023/3/8)」、https://gigazine.net/news/20230308-restrict-act/ (2023/3/10 閲覧)*

[11] *国家互联网信息办公室「个人信息出境标准合同办法(2023/3/24)」、http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm (2023/5/18 閲覧)*

[12] *国务委员兼国务院秘书长「关于国务院机构改革方案的说明(2023/3/8)」、http://www.gov.cn/guowuyuan/2023-03/08/content_5745356.htm (2023/5/18 閲覧)*

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 米国連邦航空局 NOTAM システム障害

- 2023 年 1 月 11 日、米国連邦航空局(FAA)が運用する、乗務員に安全情報を提供する Notice to Air Missions system (NOTAM システム)に障害が発生し、FAA は同日午前 9 時頃まで、全米各地で航空機の運航を停止させる措置を実施[13]。
- NOTAM システム障害に係る FAA の予備調査では、契約社員がライブのプライマリーデータベースとバックアップデータベース間の同期を修正する作業中に、意図せずファイルを削除してしまったことが判明。

2.1.2 米国Tモバイルに不正アクセス、個人情報流出

- 2023 年 1 月 19 日、米国携帯キャリア T-Mobile は契約者の個人情報が不正アクセスにより流出したと公表。同社が証券取引委員会（SEC）に同日提出した適時開示の報告書によると、約 3700 万人の契約者の情報が流出[14]。
- T-Mobile の発表によると、今回流出した個人情報は、氏名と住所、メールアドレス、電話番号、誕生日、T-Mobile の顧客番号、契約回線数、契約プランの情報などで、犯人は 1 つの API を通じてデータを不正に取得[15]。

2.1.3 ニューヨーク証券取引所のシステム障害

- 2023 年 1 月 24 日、米国ニューヨーク証券取引所で、取引開始直後に多数の銘柄の取引が一時停止、同取引所は 25 日、予備システムの設定ミスが根本的な原因だったと発表、モルガン・スタンレー株やベライゾン・コミュニケーション株など取引中断した 84 銘柄を含む 251 銘柄が影響を受け、計 4341 件の売買が無効[16]。

2.1.4 ルフトハンザ航空でシステム障害、運航混乱

- 2023 年 2 月 15 日、ドイツのルフトハンザ航空で大規模なシステム障害が発生し、ドイツ国内で最も利用客の多いフランクフルト空港に向かう便が欠航、目的地変更などの影響が発生[17]。

---

[13] *FAA「FAA NOTAM Statement」、https://www.faa.gov/newsroom/faa-notam-statement（2023/2/16 閲覧）*

[14] *日経 BP「米 T-Mobile の顧客情報が不正アクセスで再び流出、2018 年以降で 8 回目のインシデント(2023/1/24)」、https://project.nikkeibp.co.jp/idg/atcl/19/00001/00429/?ST=idg-cm-wireless&P=1（2023/5/18 閲覧）*

[15] *T-Mobile「-Mobile Informing Impacted Customers about Unauthorized Activity(2023/1/19)」、https://www.t-mobile.com/news/business/customer-information（2023/5/18 閲覧）*

[16] *日経新聞「NY 証取の一時中断、予備システムの設定ミスが原因(2023/1/25)」、https://www.nikkei.com/article/DGXZQOGN25D9D0V20C23A1000000/（2023/5/18 閲覧）*

[17] *日経新聞「ルフトハンザ航空でシステム障害、運航混乱(2023/2/15)」、https://www.nikkei.com/article/DGXZQ*

○ ドイツテレコムの光ファイバーケーブルを作業員が誤って傷付けたことが原因で、ルフトハンザのITシステムが機能しなくなり、同社の本拠地であるフランクフルトでの業務に障害が発生[18]。

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 2 月、「Mustang Panda」について、欧州を標的とした新しいスピアフィッシング攻撃を行った旨 EclecticIQ 社が、日本やドイツの外交関係者等を標榜しつつブルガリア・オーストラリア・台湾の組織を標的とした攻撃を行っている旨 ESET 社が報告。

○ 2023 年 2 月、「Blackfly（APT 41）」について、Broadcom 社は、アジアを標的とした攻撃を継続しているが、最近ではコングロマリットの2つの子会社の知的財産を標的とするなど、様々な業界の知的財産窃取に重点を置いていると報告。

○ 2023 年 3 月、「Roaming Mantis」について、Android ユーザーを標的とした SMS フィッシング活動の範囲を拡大している旨 TEAM CYMRU 社が報告。

2.2.2 ロシア関連

○ 2023 年 3 月、「APT28」について、脆弱性 CVE-2023-23397 を悪用した攻撃を行っている旨 BleepingComputer 社が報告。

○ 2023 年 1 月、「NoName057」の GitHub アカウントの停止について CyberScoop、SentinelOne 社が報告。デンマークの銀行、チェコ大統領選候補者、リトアニアの物流分野への DDoS 攻撃について、ロイター、SentinelOne 社が報告。

○ 2023 年 2 月、Killnet の関係グループである「Passion」について、親ロシア派のハクティビストに対して DDoS 攻撃ツールの有償提供を開始したと Redware 社が報告。「Killnet」と「Deanon Club」について、ハッカーフォーラム Infinity を設立したと Redware 社が報告。同年 3 月、Killmilk について、民間軍事ハッキング会社 BlackSkills を設立した旨 Flashpoint 社が報告。

2.2.3 北朝鮮関連

○ 2023 年 1 月、「Lazarus」の下部組織の「BlueNoroff」が、Windows OS のセキュリティ保護機能の Mark-of-the-Web(MOTW)を回避する新たな手法を用いた攻撃を実施していると、Kasperusky 社が分析。

OCB15CK20V10C23A2000000/（2023/5/18 閲覧）

[18] *Bloomberg「ルフトハンザ航空が一時運航停止、ケーブル損傷でシステムに障害(2023/2/15)」、https://www.bloomberg.co.jp/news/articles/2023-02-15/RQ493RDWRGG001（2023/5/18 閲覧）*

○ 2023 年 2 月、「Lazarus」について、官民の研究機関、医療研究機関、エネルギー分野の組織及びそれらのサプライチェーンを標的に攻撃を実施していると、WithSecure 社が分析。また、同グループが、アンチフォレンジック技術を使用した攻撃を実施していると AhnLab 社の分析チーム ASEC が公表。さらに、バックドア「WinorDLL64」を使用した攻撃の実施について ESET 社が公表。

○ 2023 年 2 月、米国 NSA、FBI、CISA、HHS 及び韓国の NIS、DSA が共同で、北朝鮮の国家支援を受けた攻撃グループによるランサムウェア活動に対してアドバイザリーを発出。

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 JAL の Web サイトで接続障害

○ 2023 年 3 月 9 日、日本航空は、国内線全路線が片道一律 6,600 円で乗れるキャンペーンの予約受け付けを開始したことにより、同社の Web サイトにアクセスが集中し、航空券の予約や搭乗手続きのページにつながりにくくなったと公表 [19]。

○ 同キャンペーンによる Web サイトへのアクセスが事前想定の 2.5 倍に達し、負荷分散装置が処理性能の限界を超えて停止、予約系基幹システムに連なるサーバーも過負荷となったことによるもの [20]。

3.1.2 「アフラック生命保険」と「チューリッヒ保険」で情報漏えい

○ 2023 年 1 月 10 日、アフラック生命保険とチューリッヒ保険の 2 社は顧客情報の一部が流出したことが判明した旨公表 [21、22]。

○ 2 社とも外部委託先の事業者のサーバーが不正アクセスを受けた可能性を説明している。2 社は同じ米国の事業者へ委託していた旨報道 [23]。

○ チューリッヒによれば、外部委託業者が、2022 年の年末に新たに構築したサーバーを適切なセキュリティ対策を講じない状態で設置した結果、2023 年 1 月 6 日から 8 日にかけて不正アクセス者が当該サーバーからデータを盗んだのち、1 月 8 日から 9 日にかけていわゆるダークウェブサイトにデータを掲

---

[19] *時事通信「JALのHPで接続障害　サイトでの搭乗手続きに影響(2023/3/9)」、https://www.jiji.com/jc/article?k=2023030900602&g=soc（2023/5/18 閲覧）*

[20] *日経クロステック「JAL「6600 円セール」中止を招いたシステム障害の原因判明、負荷は想定の 2.5 倍(2023/3/24)」、https://xtech.nikkei.com/atcl/nxt/column/18/00001/07852/（2023/5/18 閲覧）*

[21] *アフラック生命保険株式会社「個人情報流出に関するお詫びとお知らせ(2023/1/10)」、https://www.aflac.co.jp/news_pdf/2023011001.pdf（2023/5/18 閲覧）*

[22] *チューリッヒ保険会社「個人情報流出に関するお詫びとお知らせ(2023/1/10)」、https://www.zurich.co.jp/-/media/jpz/zrh/pdf/pr/2023/NewsRelease_20230110_ZurichInsuranceCompanyLtd.pdf（2023/5/18 閲覧）*

[23] *NHK「「アフラック生命保険」と「チューリッヒ保険」で情報漏えい(2023/1/10)」、https://www3.nhk.or.jp/news/html/20230110/k10013946151000.html（2023/5/18 閲覧）*

載したもの[24]。

3.1.3 大阪急性期・総合医療センター調査報告書

- 2023 年 3 月 28 日、大阪急性期・総合医療センターは、2022 年 10 月 31 日に同センターにおいて発生したサイバー攻撃事案に係る調査報告書を公表[25]。
- 2023 年 1 月から計 3 回の会合を開催し、フォレンジック調査結果の確認や関係者へのヒアリング調査等を踏まえ、調査報告書を取りまとめ。
- 調査報告書は、インシデントの発生から初動、復旧までを時系列にまとめ、発生要因、実施した技術的な再発防止策を整理。また、病院としての課題と国等への提言をまとめた内容。

3.2. その他

3.2.1 FENICS インターネットサービスの不正通信事案

- 2023 年 2 月 20 日、富士通が、FENICS インターネットサービスに関するネットワーク機器からの不正な通信について調査結果を公表[26]。
- 一部のネットワーク機器に、サービス運用者が機器へログインする際の情報を窃取するプログラムが不正に動作していたことが判明。
- 不正通信が行われたネットワーク機器に、当該機器への認証をバイパスする機能、ログ出力を停止する機能が不正に組み込まれていたことが判明。
- 対処として、不正通信の遮断や監視の強化、不正通信が行われたネットワーク機器の交換等を実施。
- 複数のサービス利用組織が不正通信による情報漏えいの可能性について公表。

---

[24] *チューリッヒ保険会社「個人情報漏えいに関するお詫びとご報告」、https://www.zurich.co.jp/customerdata/（2023/5/18 閲覧）*

[25] *大阪急性期・総合医療センター「情報セキュリティインシデント調査委員会報告書について(2023/3/28)」、https://www.gh.opho.jp/important/785.html（2023/4/18 閲覧）*

[26] *富士通株式会社「FENICS インターネットサービスに関するネットワーク機器からの不正な通信について(調査結果)(2023/2/20)」、https://www.fujitsu.com/jp/services/infrastructure/network/news/2023/0220.html（2023/2/28 閲覧）*

NIST CSF2.0 ディスカッション・ドラフトの公表について

2023年4月24日、米国国立標準技術研究所(NIST)は、サイバーセキュリティフレームワーク(CSF)2.0のディスカッション・ドラフトを公表した。
ディスカッション・ドラフトは、今夏リリース予定であるCSF2.0のドラフトのたたき台として位置づけられるものであり、改定プロセスの中心となりうる「Core」パートにフォーカスして草案を示し、議論の促進をはかることを目的としている。
(https://csrc.nist.gov/publications/detail/white-paper/2023/04/24/discussion-draft-of-the-nist-csf-20-core/draft)

【主なポイント】

- ✓ 重要インフラに特化した文言を削除。普遍的に適用可能なサイバーセキュリティの成果に焦点を移すことで、包括的かつ汎用的なフレームワークを実現。
- ✓ 新たなFunctionとしてGovernを追加。組織的背景、リスク管理戦略、方針と手順、役割と責任を網羅したサイバーセキュリティガバナンス機能を提供。
- ✓ IdentifyのFunctionにおけるSupply Chain Risk ManagementのCategoryについて成果主導のアプローチを重視。
- ✓ IdentifyのFunctionにおける新たなCategoryとしてImprovementを追加。組織のサイバーセキュリティ取組における継続的改善の重要性を強調。
- ✓ ProtectのFunctionにおける全てのCategoryにわたってPeople, Process, Technology(PPT)の組み合わせを活用し、資産を防御。
- ✓ ProtectのFunctionにおける新たなCategoryとしてTechnology Infrastructure Resilienceを追加。インシデントに直面しても重要なシステムやデータを維持することで障害を最小限にとどめ、重要なサービスの継続を保証。
- ✓ RespondとRecoverのFunctionにおける各Categoryを更新。インシデントフォレンジックの重要性を含むサイバーインシデント対応管理を実施。

インシデントの予防

インシデントの検知・対応・復旧

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	**CSF 2.0 Category**	**CSF 2.0 Category Identifier**
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF 2.0 Core の Function と Category

重要インフラにおける情報共有件数について(2022 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	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	63	78	302
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	0	0
NISCからの情報提供	43	38	64	91	18	18	30	17	83

(※) 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	5	6	28
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	4	3	17
	完全性を脅かす事象	情報の破壊	17	11	12	20	5	4	2	4	15
	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	37	42	145
	上記につながる事象	マルウェア等の感染	17	9	18	46	13	15	6	4	38
		不正コード等の実行	4	5	3	2	0	0	0	1	1
		システム等への侵入	14	14	26	24	2	5	7	8	22
		その他	34	47	42	80	9	15	2	10	36

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	2	6	39
	ユーザＩＤ等の偽り	3	12	9	7	2	2	1	2	7
	DDoS攻撃等の大量アクセス	17	20	10	19	8	6	2	12	28
	情報の不正取得	10	8	13	13	3	2	1	4	10
	内部不正	1	0	0	1	0	0	1	0	1
	適切なシステム等運用の未実施	14	11	23	15	2	0	5	1	8
偶発的な原因	ユーザの操作ミス	10	6	18	10	2	6	3	1	12
	ユーザの管理ミス	6	6	13	14	2	2	2	1	7
	不審なファイルの実行	16	7	7	22	14	10	1	1	26
	不審なサイトの閲覧	4	5	3	6	0	1	1	2	4
	外部委託先の管理ミス	29	39	56	107	11	14	11	13	49
	機器等の故障	27	62	39	38	7	11	12	13	43
	システムの脆弱性	19	16	38	32	4	3	5	0	12
	他分野の障害からの波及	6	4	7	10	3	3	0	1	7
環境的な原因	災害や疾病等	1	13	9	3	2	2	1	0	5
その他の原因	その他	29	33	35	48	8	5	8	8	29
	不明	46	53	68	79	11	20	13	18	62

(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 攻撃とみられる大量のアクセスを受けた事例が数多く報告された他、メール機能を悪用した攻撃やランサムウェア攻撃など、サイバー攻撃によるインシデントが報告されており、それぞれに対応する対策を講じるとともに、障害発生時における適切な広報活動が必要。

他方で、システムの更新・設定の不具合、委託先の不具合に起因するサービス障害の事例は引き続き数多く報告されており、サプライチェーンを含め適切な管理が求められる。

○ DDoS 攻撃の手法に応じた緩和策の検討が必要

DDoS 攻撃とみられる大量のアクセスを受けた事例が多数あった。その手法や標的は多様であり、CDN サービスによる緩和策が有効に機能しにくい検索などの動的コンテンツへの大量アクセスや、DNS サーバーへの大量アクセスなどの事例があった。また、ウェブサイトの中でも外部に委託しているコンテンツが標的となった事例もあり、ウェブサイト運営に係る委託先との連携が求められるとともに、障害発生時における代替の広報手段の確保が必要。

○ メール受信におけるシステム対策と継続的な職員のリテラシー教育が必要

正規のメールを模すような巧妙化されたメールを受信する事例が複数あり、マルウェアに感染した事例があった。一方で、不審な添付ファイルをブロックするシステムや職員のリテラシーが高かったことにより感染を回避できた事例があった。

○ ネットワーク接続に係る資産管理及び組織内のネットワーク分離が重要

ランサムウェア攻撃を受けた事例が引き続き複数あったが、情報系システムと基幹系システムのネットワークが分離されていたため、影響が限定的であった事例が複数あった。また、基幹系システムは侵害されたものの、代替措置により主要なサービスを継続できた事例もあり、BCP の重要性について再認識が必要。

○ 海外を含む委託先の適切な管理が必要

海外の委託先が不正アクセスを受けたことにより、個人情報など機密情報が漏洩した事例があった。

○ システム更新等に伴う影響を適切に評価することが必要

軽微な障害に対応する修正プログラムを適用した結果、サービスの提供に支障が出た事例や、顧客からのWeb サイトへのアクセス量を十分に評価できておらず閲覧障害に至った事例があった。

○ 作業手順書の確認など適切な事前準備や管理が必要

作業時における設定のミスや管理不足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出た事例が引き続き複数あった。

以上