資料３

令和 4 年 9 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(2022 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、2022 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 サイバー政策の動向、サイバーセキュリティ関係予算要求

- ○ ロシアによるウクライナ侵攻を受け、米国・欧州各国はロシアに対する経済制裁を発動、ロシア政府が実現可能なサイバー攻撃の選択肢を模索しているという情報に基づき、バイデン大統領は国家のサイバーセキュリティに関する声明を発表[1]。
- ○ 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、潜在的なロシアのサイバー攻撃に備え、重要インフラ事業者と電話会議を実施[2]。
- ○ 米国司法省(DOJ)は、重要インフラを標的とした 2 つの歴史的なサイバー攻撃を実施した 4 人のロシア政府職員の起訴状を公表[3]。
- ○ 米国財務省外国資産管理局(OFAC)は、ロシアのダークネット市場と暗号資産取引所を制裁対象リストに追加、DOJ、連邦捜査局(FBI)、麻薬取締局、内国歳入庁及び国土安全保障省が参加した共同イニシアチブによる制裁を実施、ドイツ連邦警察と連携し、ダークネット市場から 2,500 万ドル相当のビット

---

[1] *THE WHITE HOUSE「Statement by President Biden on our Nation's Cybersecurity(2022/3/21)」、https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/ (2022/5/11 閲覧)*

[2] *CISA「READOUT OF CISA CALL WITH CRITICAL INFRASTRUCTURE PARTNERS ON POTENTIAL RUSSIAN CYBERATTACKS AGAINST THE UNITED STATES(2022/3/22)」、https://www.cisa.gov/news/2022/03/22/readout-cisa-call-critical-infrastructure-partners-potential-russian-cyberattacks (2022/5/11 閲覧)*

[3] *U.S. Department of Justice「Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide(2022/3/24)」、https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical (2022/5/13 閲覧)*

コインを押収[4]。

- バイデン政権は、2023 年度の米国サイバーセキュリティ予算として、民生部門で 108.9 億ドルを提案し 2022 年度から約 10.7%増加、CISA への大幅な増額となり、要求額は 25 億ドル、2022 年度から約 18%増加[5]。
- 2022 年 4 月 4 日、米国国務省は、新たにサイバースペース・デジタル政策局(CDP)が正式に運用を開始したことを発表[6]。

1.1.2 バイデン政権の実施した首脳会合等

- 2022 年 5 月、バイデン政権は、米・ASEAN 特別サミットを皮切りに、EU 米国貿易技術評議会(TTC)、米韓首脳会談、日米首脳会談、インド太平洋経済枠組み(IPEF)の立上げに関する首脳会談、日米豪印「Quad(クアッド)」首脳会合と、各会合・首脳会談を精力的に実施。
- 米国・ASEAN 特別サミットでは、サイバーセキュリティ能力の向上、デジタルリテラシーとインクルージョンの促進、効率性・イノベーション・通信・インターネットの安全かつ公平な利用・経済の繁栄を促進する枠組みや政策の強化について合意[7]。
- EU 米国貿易技術評議会(TTC)では、人工知能(AI)に関して、信頼できる AI とリスク管理のための評価及び測定ツールに関するロードマップを作成することに合意したほか、第三国における情報通信技術・サービス(ICTS)サプライチェーンへの資金提供に関するタスクフォースの設置、デジタルプラットフォームに関する新しい協力フレームワークについて合意し、中小企業向けサイバーセキュリティのベストプラクティスに関するガイドラインを公開[8]。
- 日米首脳会談では、サイバー及び宇宙領域並びに新興技術の分野における協力を加速させることを決定し、サイバーセキュリティ及び情報保全が緊密な同盟協力の基盤を形成しており、今後も日米の協力の焦点であり続けるとの認識を共有[9]。

---

[4] *US.DEPARTMENT OF THE TREASURY「Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex(2022/4/5)」、https://home.treasury.gov/news/press-releases/jy0701 (2022/5/16 閲覧)*

[5] *THE WHITE HOUSE「Budgetof the U.S.GovernmentFISCAL YEAR 2023(2022/3)」、https://www.whitehouse.gov/wp-content/uploads/2022/03/budget_fy2023.pdf (2022/5/16 閲覧)*

[6] *DOS「Establishment of the Bureau of Cyberspace and Digital Policy(2022/4/4)」、https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/ (2022/5/11 閲覧)*

[7] *THE WHITE HOUSE「ASEAN-U.S. Special Summit 2022, Joint Vision Statement(2022/5/13)」、https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/13/asean-u-s-special-summit-2022-joint-vision-statement/ (2022/6/6 閲覧)*

[8] *Cirabc「EU-U.S. Joint Statement of the Trade and Technology Council 16 May 2022 Paris-Saclay, France(2022/5/16)」、https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/14bf0332-62ee-411b-8c74-bea38cd79efb/details (2022/6/7 閲覧)*

[9] *外務省「日米首脳共同声明「自由で開かれた国際秩序の強化」」(2022/5/23)」、https://www.mofa.go.jp/mofaj/files/100347254.pdf (2022/6/2 閲覧)*

○ 日米豪印「Qaud(クアッド)」首脳会合では、脅威情報の共有を通じた各国の重要インフラ防護の強化、デジタル製品及び半導体のサプライチェーンリスクの特定・評価、政府調達における基本的なソフトウエアセキュリティ基準との整合にコミット、サイバー人材育成・能力構築等に係る協調などについて合意[10]。

1.1.3 国家サイバーインフォームドエンジニアリング戦略

○ 2022 年 6 月 15 日、米国エネルギー省(DOE)サイバーセキュリティ、エネルギーセキュリティ及び緊急対応局(CESER)は、国家サイバーインフォームドエンジニアリング(CIE:The Cyber-Informed Engineering)戦略を公表[11]。

○ 国家 CIE 戦略では、エネルギーインフラに関し、エンジニアリングシステムの設計段階から、サイバーセキュリティ対策を行うべきとするとともに、CIE が適用されたインフラに対するインセンティブの導入も提案[12]。

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. 政府機関関連

2.1.1 重要インフラに対するロシアの国家支援・犯罪的なサイバー脅威

○ 2022 年 4 月 20 日、米国・オーストラリア・カナダ・ニュージーランド・英国のサイバーセキュリティ当局等は、共同でセキュリティアドバイザリー「重要インフラに対するロシアの国家支援・犯罪的なサイバー脅威」を公開[13]。

○ 米国及びその同盟国等に関係する重要インフラ組織が、悪意あるサイバー活動の増加にさらされる可能性があることを警告。

○ 重要インフラ組織が、ロシアの国家支援及び犯罪的なサイバー脅威から、速やかに重要インフラを守るために実施すべき措置を提示。

2.1.2 CISA が公表した日常的に悪用される脆弱性 TOP15(2021 年)

○ 2022 年 4 月 28 日、CISA は NSA、FBI、ACSC(オーストラリア)、CCCS(カナダ)、NZ NCSC(ニュージーランド)、NCSC-UK(英国)と合同で 2021 年に日常的に悪用された脆弱性に関する共同アドバイザリー(CSA)を公表[14]。

---

[10] *外務省「日米豪印首脳会合共同声明(2022/5/24)」、https://www.mofa.go.jp/mofaj/fp/nsp/page1_001188.html (2022/6/3 閲覧)*

[11] *DOE「National Cyber-Informed Engineering Strategy(2022/6/15)」、https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document (2022/7/1 閲覧)*

[12] *GovernmentCIO Magazine「DOE Will Release National Cyber-Informed Engineering Strategy Next Week(2022/6/6)」、https://governmentciomedia.com/doe-will-release-national-cyber-informed-engineering-strategy-next-week (2022/7/6 閲覧)*

[13] *CISA「Alert (AA22-110A)Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure(2022/4/20)」、https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (2022/5/23 閲覧)*

[14] *CISA「Alert (AA22-117A) 2021 Top Routinely Exploited Vulnerabilities(2022/4/27)」、https://www.cisa.gov/uscert/ncas/alerts/aa22-117a (2022/6/1 閲覧)*

- ○ CSA に記載された脆弱性 TOP15 の多くにおいて、情報開示から 2 週間以内に概念実証(PoC)コードが公開されていることを指摘。
- ○ 脆弱性が残存するシステムがインターネット上に少なからず残存していることを指摘。
- ○ CISA は悪意のあるサイバー攻撃者による侵害のリスクを低減するために、システムに適時パッチを適用すること、及び集中パッチ管理システムを導入することを推奨。

2.1.3 中国が支援するサイバー攻撃者による脆弱性の悪用

- ○ 2022 年 6 月 24 日、NSA、CISA、FBI は、共同セキュリティアドバイザリー「中国が支援するサイバー攻撃者によるネットワークデバイス及びネットワークプロバイダの悪用」を公開 [15]。
- ○ 中国の国家支援を受けたサイバー攻撃者が悪用する一般的な脆弱性等を説明。
- ○ 重要インフラ事業者等に、緩和策等を実行することにより防御体制を強化し、悪質なサイバー攻撃者が重要ネットワークに影響を及ぼすリスクの低減を勧奨。

2.2. その他

2.2.1 サイバー空間からみた侵攻開始後のウクライナ情勢

- ○ ウクライナ侵攻開始以後もマルウエア等を用いたサイバー攻撃活動が継続しており、重要インフラ事業者等が攻撃対象となる事例も多数発生 [16]。
- ○ 偽情報を拡散し社会的動揺を誘うインフルエンスオペレーションも確認 [17]。
- ○ 衛星通信サービスのシステムがサイバー攻撃を受け通信障害が発生、障害影響が多数の顧客に波及 [18]。

2.2.2 国内のシステム開発委託における北朝鮮の IT 労働者問題

- ○ 自治体の防災アプリのシステム開発外注において北朝鮮の IT 労働者が関与 [19]。

---

[15] *CISA「Alert (AA22-158A) People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices(2022/6/10)」、https://www.cisa.gov/uscert/ncas/alerts/aa22-158a (2022/7/15 閲覧)*

[16] *CyberPeace Institute「UKRAINE: Timeline of Cyberattacks(2022/5/12)」、https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/ (2022/5/23 閲覧)*

[17] *MOTERBARD「Hacked News Channel and Deepfake of Zelenskyy Surrendering Is Causing Chaos Online(2022/3/17)」、https://www.vice.com/en/article/93bmda/hacked-news-channel-and-deepfake-of-zelenskyy-surrendering-is-causing-chaos-online (2022/5/23 閲覧)*

[18] *Viasat「KA-SAT Network cyber attack overview(2022/3/20)」、https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/ (2022/5/23 閲覧)*

[19] *神戸新聞「北朝鮮籍のIT技術者 兵庫県防災アプリの修正業務に関与(2022/5/19)」、https://www.kobe-np.co.jp/news/sougou/202205/0015313333.shtml (2022/6/1 閲覧)*

○ 過去には、ミサイルの研究データが北朝鮮側に流出した疑い[20]。
○ 北朝鮮の IT 労働者が北朝鮮国民ではない者を装って就職しようとする試みに対し、米国国務省、財務省、FBI が共同で北朝鮮の IT 労働者に対するガイダンスを公開[21]。
○ 経済安全保障上の観点から業務の委託先、再委託先組織における仲介サイトを使った雇用や報酬の支払い方法について適切に把握することが重要。

2.2.3 攻撃グループ Lazarus によるサイバー攻撃

○ 攻撃グループ「Lazarus」による金融機関や暗号資産取引所を標的としたサイバー攻撃が活発化しており、FBI、CISA、米国財務省が警告を発出[22]。
○ 金融分野以外にも、化学分野を標的としたスパイ活動を確認[23]。
○ 初期の攻撃手口としては、ソーシャルエンジニアリングの利用が多くみられることから、ソーシャルエンジニアリング攻撃に対する従業員への教育が重要。

2.2.4 海外におけるランサムウエアの動向

○ 2022 年 3 月に引き続き、4 月、5 月はランサムウエアグループ Lockbit が最も活発に活動、Conti は大幅に活動を縮小[24]。
○ 2022 年 5 月 6 日、米国国務省(DOS)はランサムウエアグループ Conti の主要な指導的立場にある個人の特定や所在につながる情報等に対して、最高 1,000 万ドル(約 13.5 億円)の報奨金を支払うと発表[25]。
○ セキュリティ企業 AdvancedIntel の調査によると、Conti はインフラを大規模に停止、Conti ブランド廃止の可能性があり、Conti 内部の人材が小規模なランサムウエアグループなどへ移行する可能性[26]。
○ ランサムウエアグループは、被害者から身代金を受け取るため、脅迫の初

---

[20] *PRESIDENT Online「なぜ「防衛庁のミサイル研究データ」は北朝鮮側に渡ったのか…元国家安全保障局長が解説する"流出経路"(2022/5/31)」、https://president.jp/articles/-/57672?page=1（2022/6/1 閲覧）*
[21] *U.S. DEPARTMENT of STATE「Guidance on the Democratic People's Republic of Korea Information Technology Workers(2022/5/16)」、https://www.state.gov/guidance-on-the-democratic-peoples-republic-of-korea-information-technology-workers/（2022/6/1 閲覧）*
[22] *CISA「North Korean State-Sponsored APT Targets Blockchain Companies(2022/4/18)」、https://www.cisa.gov/uscert/ncas/alerts/aa22-108a（2022/6/20 閲覧）*
[23] *Broadcom「Lazarus Targets Chemical Sector(2022/4/14)」、https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical（2022/6/20 閲覧）*
[24] *Malwarebytes「Ransomware: May 2022 review(2022/6/3)」、https://blog.malwarebytes.com/threat-intelligence/2022/06/ransomware-may-2022-review/（2022/6/14 閲覧）*
[25] *U.S. Department of State「Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice(2022/5/6)」、https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/（2022/6/15 閲覧）*
[26] *AdvIntel「DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape(2022/5/21)」、https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape（2022/6/17 閲覧）*

期段階で企業名を伏せる、被害企業の Web サイトに脅迫メッセージを表示する、サーフェイスウェブに窃取したデータを公開するなど、様々な手法を試み[27]。

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. 政府機関関連

3.1.1 重要インフラのサイバーセキュリティに係る行動計画の決定

- 2022 年 6 月 17 日、サイバーセキュリティ戦略本部第 34 回会合において、重要インフラサービスの安全かつ持続的な提供に向けた基本的な枠組みとして、「重要インフラのサイバーセキュリティに係る行動計画」が決定[28]

3.2. 重要インフラ関連

3.2.1 つるぎ町立半田病院におけるランサムウエア被害と調査報告書

- 2021 年 10 月 31 日、つるぎ町立半田病院がランサムウエア攻撃を受け、電子カルテをはじめとするシステムが停止し、救急や新規患者の受け入れを停止。
- 2022 年 1 月 4 日、つるぎ町立半田病院は、電子カルテシステムが再稼働、通常診療を再開。
- 2022 年 6 月 16 日、つるぎ町立半田病院は、同院が設置した有識者会議による調査報告書を公表[29]。
- 2022 年 5 月、6 月には、安江病院と鳴門山上病院で、サイバー攻撃により電子カルテシステムなどが一時停止するも、すぐにバックアップからシステムを復旧[30]。

3.3. その他

3.3.1 フィッシングに関する動向

- フィッシング対策協議会によると、フィッシングの報告数は、2017 年から 2021 年にかけて増加し続け、2021 年は 2020 年と比較して 2 倍以上増加[31]。
- 日本国内におけるフィッシングのターゲットは、従前より狙われていた銀行に関する情報から、クレジットカード情報や各種 EC サイトのアカウント情報へと

---

[27] *Krebs on Security「Ransomware Group Debuts Searchable Victim Data(2022/6/14)」、https://krebsonsecurity.com/2022/06/ransomware-group-debuts-searchable-victim-data/（2022/6/20 閲覧）*

[28] *サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る行動計画(2022/6/17)」、https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf（2022/7/7 閲覧）*

[29] *つるぎ町立半田病院「徳島県つるぎ町立半田病院 コンピュータウイルス感染事案有識者会議調査報告書について(2022/6/16)」、https://www.handa-hospital.jp/topics/2022/0616/index.html（2022/7/4 閲覧）*

[30] *医療法人久仁会 鳴門山上病院「2022 年 6 月 21 日 サイバー攻撃による被害について(第 2 報)(2022/6/21)」、https://kyujinkai-mc.or.jp/info/20220621/（2022/7/4 閲覧）*

[31] *フィッシング対策協議会「フィッシングレポート 2022(2022/6/1)」、https://www.antiphishing.jp/report/phishing_report_2022.pdf（2022/7/26 閲覧）*

変遷[32]。

- 2021 年 12 月以降、フィッシング対策協議会は、情報通信分野、鉄道分野、水道分野など、重要インフラ分野関連のサービスを装うフィッシングについて注意喚起[33]。
- 2021 年 9 月、Microsoft は、大規模なフィッシングを可能とする PHaaS(Phishing as a Service)について報告し、攻撃の増加を懸念[34]。
- 米セキュリティ企業 coveware によると、2022 年第 1 四半期(2022 年 1 月～3 月)において、ランサムウエアの攻撃経路はメールフィッシングがトップ[35]。

3.3.2 Oracle Java の署名検証の脆弱性(CVE-2022-21449)

- 2022 年 4 月、Oracle は Java の署名検証の脆弱性(CVE-2022-21449)を修正[36]。
- ECDSA 署名の検証アルゴリズムの実装に脆弱性があり、攻撃者が作成した偽の署名を正規の署名として処理し、不正にデータにアクセスされる脅威が存在[37]。
- Java は広く導入されているため、攻撃手法が確立される前に、早急にパッチを適用するなどの対策が重要。

3.3.3 F5 製 BIG-IP の任意コード実行の脆弱性(CVE-2022-1388)

- 2022 年 5 月、ネットワーク機器大手 F5 はロードバランサーBIG-IP の任意コード実行の脆弱性(CVE-2022-1388)を公開[38]。
- 同機器には認証処理に脆弱性があり、特定のリクエストを送信すると認証情報無しで特権ユーザーとして、不正にアクセスされる脅威が存在。
- 本脆弱性の実証コード(PoC コード)の存在が確認されたため、修正パッチを早急に適用することや、適用前の侵害の有無を確認することが重要[39]。

---

[32] *日本サイバー犯罪対策センター「フィッシングターゲットの変遷(2022/2/4)」、https://www.jc3.or.jp/threats/topics/article-430.html (2022/5/9 閲覧)*

[33] *フィッシング対策協議会「緊急情報 一覧」、https://www.antiphishing.jp/news/alert/ (2022/5/17 閲覧)*

[34] *Microsoft「Catching the big fish: Analyzing a large-scale phishing-as-a-service operation(2021/9/21)」、https://www.microsoft.com/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/ (2022/5/13 閲覧)*

[35] *Coveware「Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting(2022/5/3)」、https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting (2022/5/16 閲覧)*

[36] *Oracle「Oracle Critical Patch Update Advisory - April 2022(2022/4/19)」、https://www.oracle.com/security-alerts/cpuapr2022.html (2022/7/29 閲覧)*

[37] *Neil Madden「CVE-2022-21449: Psychic Signatures in Java(2022/4/19)」、https://neilmadden.blog/2022/04/19/psychic-signatures-in-java/ (2022/7/25 閲覧)*

[38] *F5「K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388(2022/5/4)」、https://support.f5.com/csp/article/K23605346 (2022/6/8 閲覧)*

[39] *CISA「Threat Actors Exploiting F5 BIG-IP CVE-2022-1388(2022/5/18)」、https://www.cisa.gov/uscert/ncas/alerts/aa22-138a (2022/6/14 閲覧)*

3.3.4　ゼロデイ脆弱性の脅威と対策

- ○ 2022 年 5 月、Microsoft はサポート診断ツールに関する脆弱性(CVE-2022-30190)を公開[40]。
- ○ 2022 年 6 月、Atlassian はコラボレーションツール Confluence に関する脆弱性(CVE-2022-26134)を公開[41]。
- ○ 両社はゼロデイ脆弱性の情報公開後、修正パッチの提供前に悪用を確認。
- ○ 脆弱性の影響を緩和するためには、アクセス制御や、脅威情報を把握し、自組織への影響を確認して対策を検討することが重要[42]。

以上

---

[40] *Microsoft「CVE-2022-30190 マイクロソフト サポート診断ツールの脆弱性に関するガイダンス(2022/5/30)」、https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability-jp/（2022/7/19 閲覧）*

[41] *Atlassian「Confluence Server and Data Center – CVE-2022-26134 – Critical severity unauthenticated remote code execution vulnerability(2022/6/2)」、https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html（2022/7/19 閲覧）*

[42] *ENISA「Zero-Day(2017/5/29)」、https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/zero-day（2022/7/19 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 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	FY2018 計	FY2019 計	FY2020 計	FY2021 計	FY2022 1Q	2Q	3Q	4Q	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	—	—	—	78
関係省庁・関係機関からのNISCへの情報共有	7	16	16	6	0	—	—	—	0
NISCからの情報提供	43	38	64	91	18	—	—	—	18

(※) 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	2Q	3Q	4Q	計
未発生の事象		予兆・ヒヤリハット	27	12	28	25	15	—	—	—	15
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	6	—	—	—	6
	完全性を脅かす事象	情報の破壊	17	11	12	20	5	—	—	—	5
	可用性を脅かす事象	システム等の利用困難	97	158	157	181	30	—	—	—	30
	上記につながる事象	マルウェア等の感染	17	9	18	46	15	—	—	—	15
		不正コード等の実行	4	5	3	2	0	—	—	—	0
		システム等への侵入	14	14	26	24	2	—	—	—	2
		その他	34	47	42	80	9	—	—	—	9

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

(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 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

引き続き、Emotet に起因する事例が複数寄せられた。またランサムウエアに関連した報告ではサービスの停止やデータの消失などがあった一方で、バックアップ等の対応策をとっていたことで被害範囲を抑えた事例もあり、事前準備の有無が業務継続への影響を二分した。また、システムの更新・設定の不具合に起因するサービス障害等の事例が依然として発生している。

経営層及び戦略マネジメント層を含めた組織全体でのリスク管理や多層的対応を進めるとともに、昨今のインシデントから改善すべき対応策を速やかに検討・導入し、サイバーセキュリティの確保に努めることが重要である。

○　攻撃傾向の把握と対策の技術的有効性にかかる継続的な評価が必要

マルウエア Emotet 感染により、個人情報が流出し、自組織を騙る不審メールに利用される事例が多数あった。また委託先が感染したことで、複数の組織において同時期に不審メールが確認された事例があった。

○　バックアップの重要性の再認識と IT-BCP の策定と点検が必要

ランサムウエ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複数あった。また二重脅迫を目的とした窃取活動により、内部情報の一部が外部へ流出した可能性があった。海外拠点に設置された製品の脆弱性が悪用されたことでネットワークへ侵入された事例もあった。

○　換金性のある情報を取り扱うサービスに対する攻撃耐性の点検が必要

リスト型攻撃による不正ログインを受け、その後の認可の手続きも十分ではなかったことから、顧客情報の不正な閲覧やサービスの不正利用につながる事例が発生した。

○　前例に過度にとらわれ過ぎない事前準備及び対応策が必要

システムメンテナンス時における設定不備や考慮漏れ、認識の誤りといった不注意によってシステムに不具合が発生し、サービス提供への影響又はデータの一部が消失する事例が発生した。

○　現場の運用状況を踏まえた更新計画が必要

動作することを優先して対応が行われたために残存していたサポート期限の切れた旧式のソフトウエアについて、軽微な不具合を通じて利用していた事実が発覚した。

以上