資料５

令和 3 年 5 月 31 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(2020 年度第 3 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、2020 年度第 3 四半期(10 月～12 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。ご活用の際はご留意ください。

1. 国外サイバーセキュリティ政策

1.1. 米国

1.1.1 米国大統領選挙の結果について

- ○ 2020 年 11 月 3 日に行われた米国大統領選挙は、11 月 7 日、バイデン候補が勝利を宣言。他方、トランプ大統領は敗北を認めず、法廷闘争の構え[1]。
- ○ 2021 年 1 月 7 日、米国連邦議会の上下両院合同会議は、バイデン候補を次期第 46 代米国大統領に選出し、トランプ大統領も「秩序ある政権移行」を約束[2]。
- ○ 2021 年 1 月 20 日、第 46 代米国大統領にバイデン大統領が就任、バイデン政権は国際協調重視の姿勢[3]。

1.1.2 トランプ大統領のアカウント停止と SNS の「表現の自由」について

- ○ 2021 年 1 月、トランプ大統領の SNS 上での言動が 2021 年 1 月 6 日の連邦議会議事堂襲撃事件につながったとの考えから、SNS 各社が大統領のアカ

---

[1] *BBC「米大統領選 2020 トランプ氏、バイデン氏の「勝利」に言及 敗北は認めず(2020/11/16)」、https://www.bbc.com/japanese/54948308 (2020/11/17 閲覧)*

[2] *REUTERS「米議会がバイデン氏勝利認定、大統領「秩序ある政権移行」確約(2021/1/7)」、https://jp.reuters.com/article/biden-congress-idJPKBN29C0Y8 (2021/1/7 閲覧)*

[3] *時事通信「同盟修復、世界に関与 国際協調路線に転換 バイデン米新大統領(2021/1/21)」、https://www.jiji.com/jc/article?k=2021012100427&g=int (2021/1/21 閲覧)*

ウントを停止[4]。

- ○ これについて、「表現の自由」との関連で議論が活発化[5]。
- ○ 仏国においても、インターネット上の誤った情報により教員が殺害されたこと等を受け、ネット規制強化の動き[6]。

1.1.3 米国の重要新興技術分野における国家戦略について

- ○ 2020 年 10 月、米国トランプ政権は、革新的な技術における米国の技術的優位性と競争力を確保するための国家戦略「NATIONAL STRATEGY for CRITICAL AND EMERGING TECHNOLOGIES OCTOBER 2020」を発表、これは 2017 年の国家安全保障戦略「National Security Strategy of the United States of America」に基づくもの[7]。
- ○ 米国の経済成長と安全保障のため、20 の科学技術分野[8]を特定。

1.2. 欧州

1.2.1 米英のサプライチェーンにかかる対中政策について

- ○ バイデン政権の対中政策は、トランプ政権のスタンスとあまり変わらず、むしろ中国にとって脅威となる可能性もあるとの指摘[9]。
- ○ トランプ政権によるファーウエイ製品の締め出しにより、2020 年第 2 四半期のスマートフォン出荷台数は、ファーウエイが前年同期比 21%減となり、首位から 2 位に陥落、他方、Xiami(中国)が約 40%増と出荷を伸ばし、Apple を抜いて 3 位にランク入り[10]。
- ○ 2020 年 11 月 30 日、英国はファーウエイ製品を締め出すための法案及び戦

---

[4] *東京新聞「ツイッター社、トランプ氏のアカウント永久停止 暴力扇動の危険ありと判断(2021/1/9)」、https://www.tokyo-np.co.jp/article/78931 (2021/2/7 閲覧)*

[5] *東京新聞「トランプ氏の SNS 追放は「表現の自由」の侵害か 巨大 IT 企業の支配に懸念相次ぐ(2021/1/13)」、https://www.tokyo-np.co.jp/article/79512 (2021/2/7 閲覧)*

[6] *時事通信「「表現の自由」対応苦慮 教員殺害でネット規制強化―仏(2020/10/22)」、https://www.jiji.com/jc/article?k=2020102100708 (2021/2/5 閲覧)*

[7] *Homeland Security Digital Library「National Strategy for Critical and Emerging Technologies Released(2020/10/15)」、https://www.hsdl.org/c/national-strategy-for-critical-and-emerging-technologies-released/ (2020/5/5 閲覧)*

[8] *高度なコンピューティング、先進的な通常兵器技術、先端工学材料、先進的なものづくり、高度なセンシング、エアロエンジン技術、農業技術、人工知能、自律システム、バイオテクノロジー、CBRN の緩和技術、通信及びネットワーク技術、データサイエンスとストレージ、分散型台帳技術、エネルギー技術、ヒューマン・マシン・インターフェース、医療・公衆衛生に関する技術、量子情報科学、半導体・マイクロエレクトロニクス、宇宙技術*

[9] *Businessinsider「Biden will team up with Europe to be tougher on China than Trump(2020/12/6)」、https://www.businessinsider.com/analysis-biden-could-be-tougher-for-china-than-trump-2020-12 (2020/12/09 閲覧)*

[10] *PC Watch インプレス「Xiaomi が Apple を抜き世界スマホシェア 3 位に(2020/12/2)」、https://pc.watch.impress.co.jp/docs/news/1292518.html (2020/12/9 閲覧)*

略を公表[11]。

1.2.2 巨大 IT 企業への規制強化・対中関係の動向等

- ○ 2020 年 12 月 15 日、欧州委員会は「デジタルサービス法」と「デジタル市場法」を柱とする巨大 IT 企業への規制強化案を公表[12]。
- ○ EU を離脱した英国においても、2020 年 11 月、巨大 IT 企業を監視・規制する専門の新組織を競争・市場庁に設置すると公表[13]。
- ○ また米国議会下院司法委員会は、2020 年 10 月、GAFA(Google、Apple、Facebook、Amazon)が反競争的な方法で市場支配力を拡大しているとの報告書を公表[14]。
- ○ 欧州の対中関係は、特に独国においてスタンスを転換する動きがあるとの指摘[15]。

1.3. 中国

1.3.1 中国共産党「5 中全会」について

- ○ 2020 年 10 月、中国共産党の重要会議である「5 中全会」が開催され、次期 5 ヵ年計画に加え、2035 年までの長期目標を審議・決定[16]。
- ○ また慣例となる最高指導者の後継者人事はなく、異例となる習近平国家主席の第 3 期目続投との見方もあり[17]。
- ○ 中国政府の関与が疑われるスパイ活動による技術情報窃取が相次ぐ中、米

---

[11] *英国政府サイト「Roadmap to remove high risk vendors from telecoms network(2020/11/30)」、https://www.gov.uk/government/news/roadmap-to-remove-high-risk-vendors-from-telecoms-network (2020/12/09 閲覧)*

[12] *European Commission「Europe fit for the Digital Age: Commission proposes new rules for digital platforms(2020/12/15)」、https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347 (2021/1/15 閲覧)*

[13] *英国政府「New competition regime for tech giants to give consumers more choice and control over their data, and ensure businesses are fairly treated(2020/11/27)」、https://www.gov.uk/government/news/new-competition-regime-for-tech-giants-to-give-consumers-more-choice-and-control-over-their-data-and-ensure-businesses-are-fairly-treated (2021/1/15 閲覧)*

[14] *HOUSE COMMITTEE ON THE JUDICIARY「Judiciary Antitrust Subcommittee Investigation Reveals Digital Economy Highly Concentrated, Impacted By Monopoly Power(2020/10/6)」、https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429 (2021/1/15 閲覧)*

[15] *時事ドットコム「ドイツ、中国偏重の政策転換(2020/12/27)」、https://www.jiji.com/jc/p?id=20201226145203-0036530222 (2021/1/15 閲覧)*

[16] *人民日報「中国共産党第 19 期五中全会コミュニケの要点(2020/10/30)」、http://j.people.com.cn/n3/2020/1030/c94474-9775153.html (2020/11/8 閲覧)*

[17] *東京新聞「中国の五中全会 前例破る長期政権懸念(2020/10/30)」、https://www.tokyo-np.co.jp/article/65221/ (2020/11/12 閲覧)*

国は「チャイナ・イニシアチブ」を推進[18]。

○ スパイ活動の背景にある「中国製造 2025」を踏まえた次期 5 ヵ年計画が「5 中全会」で決定されたことを受け、引き続き、各国は警戒[19]。

1.3.2 中国輸出管理法の施行について

○ 米国大統領選でバイデン候補が勝利し、政権移行が進む中、2020 年 12 月 1 日、中国は輸出管理法を施行[20]。

○ 2020 年 12 月 2 日、中国商務省は規制対象となる品目を初めて発表[21]。

○ 今後、中国は政治的、外交的関係が悪化した国に対して、輸出管理法を恣意的に運用する可能性も否定できないとの見方もあり、中国の動向に留意が必要[22]。

1.3.3 香港国家安全維持法の影響、中国国防法の改正について

○ 香港国家安全維持法の施行から半年となる 2021 年 1 月、香港では民主化を求める 53 名が逮捕、同法律の施行以来、一度に逮捕された人数としては最大規模[23]。

○ これについて、2021 年 1 月 9 日、米国、英国、カナダ及びオーストラリアの 4 ヵ国外相は共同声明で「深刻な懸念」を表明[24]。

○ 2020 年 12 月 26 日、宇宙やサイバー空間を新たに軍事活動の対象へ追加するなどした中国国防法の改正案が成立、2021 年 1 月 1 日から施行[25]。

---

[18] *Department of Justice「The China Initiative(2020/9/1)」、https://www.justice.gov/usao-edtx/china-initiative (2020/11/15 閲覧)*

[19] *NHK「米中新冷戦 激化する攻防～産業スパイの実態 (2019/2/6)」、https://www3.nhk.or.jp/news/special/45th_president/articles/column/article/2019-0206-00.html (2020/11/16 閲覧)*

[20] *新華社「聚焦出口管制法:贯彻总体国家安全观(2020/10/17)」、http://www.xinhuanet.com/politics/2020-10/17/c_1126624428.htm (2020/12/14 閲覧)*

[21] *中国商務部、国家暗号管理局、海関総署「商用暗号輸入許可リスト、商用暗号輸出管理リスト及び関連管理措置に関する公告(2020/12/2)」、http://www.mofcom.gov.cn/article/zwgk/zcfb/202012/20201203019733.shtml (2020/12/14 閲覧)*

[22] *エコノミスト Online「中国の輸出管理法で影響も？実は中国依存度が高い輸入品ランキング(2021/1/23)」、https://weekly-economist.mainichi.jp/articles/20210119/se1/00m/020/022000c (2021/1/24 閲覧)*

[23] *東京新聞「香港警察、民主派 53 人を一斉逮捕 国安法違反の疑いで過去最多 弾圧を強化(2021/1/6)」、https://www.tokyo-np.co.jp/article/78303 (2021/1/17 閲覧)*

[24] *英国政府「Foreign Ministers' joint statement on arrests in Hong Kong(2021/1/9)」、https://www.gov.uk/government/news/foreign-ministers-joint-statement-on-arrests-in-hong-kong (2021/1/17 閲覧)*

[25] *日本経済新聞「中国「利益侵害」で軍動員も 国防法改正、米制裁意識か(2020/12/26)」、https://www.nikkei.com/article/DGXZQOGM263M20W0A221C2000000/ (2021/1/17 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. 政府機関関連

2.1.1 多くの米国政府機関を巻き込んだ SolarWinds 事案について

- 2020 年 12 月 13 日、米国 SolarWinds は、同社の IT インフラストラクチャ監視・管理プラットフォーム「Orion Platform」にバックドアが仕掛けられていることを公表[26]。
- バックドアは、Orion Platform の正規アップデートにより仕掛けられ、米国を中心とした米国政府機関を含む最大 18,000 組織に影響[27]。
- 2020 年 12 月 17 日、米国 CISA は、アラートを発するとともに、2021 年 1 月 5 日に FBI、ODNI 及び NSA とともに共同声明を発し、ロシア由来のものと非難[28]。

2.2. 重要インフラ関連

2.2.1 重要インフラ事業者等が保有する脆弱な Fortinet 製 VPN 機器情報の公開

- 2019 年 5 月、Fortinet は、FortiOS の SSL VPN 機能に、外部から当該 VPN 機器内のファイルを読み取ることが可能となる脆弱性(CVE-2018-13379)を公表[29]。
- 攻撃者が本脆弱性を悪用した場合、当該機器のユーザー名やパスワードを平文で窃取できる可能性があり、その場合、攻撃対象組織のネットワークへの侵入が可能。
- 2020 年 11 月 19 日以降、約 5 万件に及ぶ同脆弱性の影響を受ける VPN 機器の IP アドレスを含む情報が公開[30]。
- これを受け、2020 年 12 月 3 日、内閣サイバーセキュリティセンターは公開情報を基に情報収集・分析を行い、確認した重要インフラ事業者等関連の VPN

---

[26] *SolarWinds「SolarWinds Security Advisory」、https://www.solarwinds.com/ja/securityadvisory (2021/1/19 閲覧)*

[27] *SolarWinds「Form 8-K(2020/12/14)」、https://investors.solarwinds.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=14559445 (2021/1/19 閲覧)*

[28] *CISA「JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA) (2021/1/5)」、https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure (2021/1/19 閲覧)*

[29] *Fortinet「FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests(2019/5/24)」、https://www.fortiguard.com/psirt/FG-IR-18-384 (2020/12/7 閲覧)*

[30] *Bleeping Computer「Hacker posts exploits for over 49,000 vulnerable Fortinet VPNs(2020/11/22)」、https://www.bleepingcomputer.com/news/security/hacker-posts-exploits-for-over-49-000-vulnerable-fortinet-vpns/ (2020/12/7 閲覧)*

装置について、 所管省庁に注意喚起を発出[31]。

2.2.2 「Oracle WebLogic Server」の深刻な脆弱性について

- 2020 年 10 月 20 日、Oracle が Web アプリケーションサーバー「Oracle WebLogic Server」の脆弱性(CVE-2020-14882、CVE-2020-14883)を公開[32]。
- 2020 年 11 月 1 日、Oracle は定例外アップデートを実施し、新たに「Oracle WebLogic Server」の脆弱性(CVE-2020-14750)を公開[33]。
- これらの脆弱性は悪用が簡単であり、専門機関等が注意を呼びかけていたが、脆弱性情報の公開から約 1 週間で脆弱性(CVE-2020-14882)を悪用する攻撃が発生[34]。

2.2.3 新型コロナウイルス感染症のワクチン等をめぐるサイバー攻撃

- 2020 年 11 月 13 日、マイクロソフトは、ロシア政府や北朝鮮政府とつながれが疑われるハッカー集団が、新型コロナウイルス感染症のワクチンや治療薬を開発している製薬企業等を標的としたサイバー攻撃について公表[35]。

2.2.4 クラウドサービスにおける責任境界モデルと脅威及び脆弱性

- クラウドサービスの利用が進む中、2019 年に発生した「情報セキュリティ 10 大脅威 2020」に「予期せぬ IT 基盤の障害に伴う業務停止」がランク入り、クラウド固有のリスクが増加[36]。
- 2020 年 1 月、米国国家安全保障局(NSA)はクラウドの脆弱性緩和に関するレポートを公表し、クラウドサービスの脆弱性として、「設定ミス」、「アクセス制御の不備」、「共有テナントの脆弱性」及び「サプライチェーンの脆弱性」を指摘[37]。

---

[31] *内閣サイバーセキュリティセンター「Fortinet 製 VPN の脆弱性(CVE-2018-13379)に関する重要インフラ事業者等についての注意喚起の発出について(2020/12/3)」、https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf (2020/12/7 閲覧)*

[32] *Oracle「Oracle Critical Patch Update Advisory - October 2020(2020/10/20)」、https://www.oracle.com/security-alerts/cpuoct2020.html (2020/12/7 閲覧)*

[33] *Oracle「Oracle Security Alert Advisory-CVE-2020-14750(2020/11/1)」、https://www.oracle.com/security-alerts/alert-cve-2020-14750.html (2020/12/7 閲覧)*

[34] *SANS Technology Institute「PATCH NOW: CVE-2020-14882 Weblogic Actively Exploited Against Honeypots(2020/10/29)」、https://isc.sans.edu/diary/26734 (2020/12/7 閲覧)*

[35] *Microsoft「Cyberattacks targeting health care must stop(2020/11/13)」、https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ (2021/1/6 閲覧)*

[36] *IPA「情報セキュリティ 10 大脅威 2020(2020/8/25)」、https://www.ipa.go.jp/files/000080871.pdf (2020/11/23 閲覧)*

[37] *National Security Agency 「Cybersecurity Information Mitigating Cloud Vulnerabilities(2020/1/22)」、https:/*

○ クラウドサービスでは、一般的に、サービスを提供するクラウド提供者と利用組織の双方がセキュリティを確保するための責任を共有する「責任共有モデル」を採用しており、リスクに適切に対応するため、このモデルを前提とした双方のリスクコミュニケーションが重要[38]。

2.3. その他

2.3.1 セキュリティベンダー各社の 2021 年セキュリティ脅威予測

○ セキュリティーベンダー各社は 2021 年のセキュリティ脅威として、さらなるテレワークの普及に伴うホームネットワークへの攻撃の増加、ランサムウエアの拡大及び新型コロナウイルス感染症に便乗した医療機関へのサイバー攻撃の継続を共通して予測[39, 40, 41, 42]。

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 東京証券取引所におけるシステム障害について

○ 東京証券取引所は、2020 年 10 月 1 日、株式売買システム「arrowhead」の障害により、全銘柄の売買を終日停止。全銘柄の売買終日停止は、1999 年の取引全面システム化以降初[43]。

○ 原因は、冗長化している共有ディスク装置のうち 1 号機が故障の際、設定誤りで 2 号機に切り替わらなかったこと[44]。

/media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF（2021/1/20 閲覧）

[38] *マイクロソフト「クラウドにおける共同責任（2019/10/16）」、https://docs.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility（2021/2/2 閲覧）*
Amazon「責任共有モデル | AWS（amazon.com）」、https://aws.amazon.com/jp/compliance/shared-responsibility-model/（2021/2/2 閲覧）

[39] *カスペルスキー「＜Kaspersky Security Bulletin：2021 年サイバー脅威の動向予測＞ APT 攻撃が新たな脅威の様相と攻撃戦略の変化をみせ、日本を狙う APT 攻撃も進化し増加すると予測（2020/11/19）」、https://www.kaspersky.co.jp/about/press-releases/2020_vir10122020（2021/01/18 閲覧）*

[40] *トレンドマイクロ「トレンドマイクロ、2021 年セキュリティ脅威予測を公開～自宅のテレワーク環境がサイバー攻撃の弱点に～（2020/12/22）」、https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20201222-01.html（2021/01/18 閲覧）*

[41] *シマンテック「シマンテック 2021 年サイバーセキュリティ予測 - 今後の展望（2020/11/21）」、https://symantec-enterprise-blogs.security.com/blogs/japanese/symantec-2021-predictions（2021/01/18 閲覧）*

[42] *FireEye「サイバーセキュリティ動向予測レポート 2021」、https://content.fireeye.com/predictions-jp/rpt-security-predictions-2021-jp（2021/01/18 閲覧）*

[43] *日本取引所グループ「システム障害に係る独立社外取締役による調査委員会の報告書について(2020/11/30)」、https://www.jpx.co.jp/corporate/news/news-releases/0020/20201130-03.html（2021/2/3 閲覧）*

[44] *東京証券取引所「10 月 1 日に株式売買システムで発生した障害について(2020/10/19)」、https://www.jpx.co.jp/corporate/news/news-releases/0060/nlsgeu0000051l46-att/trading_system.pdf（2020/11/18 閲覧）*

○ 東京証券取引所は、2020 年 11 月 30 日、金融庁から業務改善命令を受け、社長が辞任する等、経営問題に発展[45]。

3.1.2 ランサムウエアの感染に伴う被害の拡大について

○ 2020 年 11 月、日本国内の企業において、ランサムウエアに感染し、データの暗号化及び窃取した情報の公開といった 2 段階の圧力をかけて脅迫された事例が公表[46]。

○ 最近のランサムウエアは、既知の各種対策を回避し、検知を困難にさせるなど高度化[47]。

○ 2020 年、米国の教育機関、地方自治体、医療機関及び医療関連会社のシステムがランサムウエアに感染する事例が頻発[48]。

○ 2020 年 11 月 26 日、米国のセキュリティ企業 CrowdStrike は、日本企業の約半数が直近 1 年間でランサムウエアの被害にあったと回答したと報告[49]。

○ 2020 年 11 月 26 日、ランサムウエアによるサイバー攻撃が国内外の様々な組織で確認されていることを踏まえ、内閣サイバーセキュリティセンターは注意喚起を公開[50]。

3.1.3 MSP や海外拠点を攻撃の起点とした不正アクセス

○ 2020 年、MSP(マネージドサービスプロバイダ)や海外拠点を攻撃の起点とした不正アクセスが相次いで発生、同年 12 月 11 日、三菱パワーは、同年 9 月に発生した MSP を経由した同社グループに対する不正アクセスを公表[51]。

○ 2020 年 12 月 28 日、川崎重工は、同年 6 月に発生した同社グループの海外拠点を経由した不正アクセスを公表[52]。

---

[45] *日本取引所グループ「システム障害に係る業務改善命令及び責任の所在の明確化について」、https://www.jpx.co.jp/corporate/news/news-releases/0020/nlsgeu00000553ll-att/nlsgeu00000553mh.pdf (2021/2/3 閲覧)*

[46] *カプコン「不正アクセスによる情報流出に関するお知らせとお詫び(2020/11/16)」、 https://www.capcom.co.jp/ir/news/html/201116.html (2021/4/16 閲覧)*

[47] *三井物産セキュアディレクション「企業名を名指しで脅迫する「Ragnar Locker」ランサムウエアの解析(2020/11/11)」、https://www.mbsd.jp/research/20201111.html (2020/12/8 閲覧)*

[48] *Emsisoft「The State of Ransomware in the US: Report and Statistics 2020(2021/1/18)」、https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/ (2021/4/12 閲覧)*

[49] *日本経済新聞「クラウドストライク、2020 年度版グローバルセキュリティ意識調査結果を発表(2020/11/26)」、https://www.nikkei.com/article/DGXLRSP600746_W0A121C2000000/ (2020/12/9 閲覧)*

[50] *内閣サイバーセキュリティセンター「ランサムウエアによるサイバー攻撃について(注意喚起)(2020/11/26)」、https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf (2020/12/9 閲覧)*

[51] *三菱パワー「当社ネットワークに対するマネージドサービスプロバイダを経由した第三者からの不正アクセスに係る件(2020/12/11)」、https://power.mhi.com/jp/news/20201211.html (2021/1/12 閲覧)*

[52] *川崎重工「当社グループへの不正アクセスについて(2020/12/28)」、https://www.khi.co.jp/pressrelease/news_*

3.1.4　非対面本人確認(eKYC)について

○ ドコモ口座の不正利用に端を発した不正出金問題で話題に上る機会の増えた本人確認(KYC：Know Your Customer)について、現在はスマホ等を用いたオンラインでの非対面本人確認(eKYC：electronic Know Your Customer)が普及され始めており、その活用に注目[53]。

以上

201228-1j.pdf（2021/1/12 閲覧）

[53] *JNSA Press「本人確認手段としての eKYC と今後の発展(2020/1/15)」、https://www.jnsa.org/jnsapress/vol48/JNSA_Press_No48.pdf（2020/11/9 閲覧）*

重要インフラにおける情報共有件数について（2020 年度）

「重要インフラの情報セキュリティ対策に係る第４次行動計画」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	FY2016 計	FY2017 計	FY2018 計	FY2019 計	FY2020 1Q	FY2020 2Q	FY2020 3Q	FY2020 4Q	FY2020 計
重要インフラ事業者等からNISCへの情報連絡(※)	856	388	223	269	61	75	86	87	309
関係省庁・関係機関からのNISCへの情報共有	41	19	7	16	4	6	1	5	16
NISCからの情報提供	80	54	43	38	11	8	21	24	64

※1)重要インフラ事業者等からNISCへの情報連絡の事象別内訳は以下のとおり。

事象の類型			FY2016 計	FY2017 計	FY2018 計	FY2019 計	FY2020 1Q	FY2020 2Q	FY2020 3Q	FY2020 4Q	FY2020 計
未発生の事象		予兆・ヒヤリハット	330	80	27	12	3	4	13	8	28
発生した事象	機密性を脅かす事象	情報の漏えい	30	15	13	13	4	5	4	10	23
	完全性を脅かす事象	情報の破壊	47	20	17	11	4	4	3	1	12
	可用性を脅かす事象	システム等の利用困難	80	143	97	158	39	41	37	40	157
	上記につながる事象	マルウェア等の感染	289	65	17	9	4	4	3	7	18
		不正コード等の実行	10	13	4	5	0	1	1	1	3
		システム等への侵入	26	17	14	14	1	3	11	11	26
		その他	44	35	34	47	6	13	14	9	42

※2)上記事象における原因別類型は以下のとおり。（複数選択）

事象の類型		FY2016 計	FY2017 計	FY2018 計	FY2019 計	FY2020 1Q	FY2020 2Q	FY2020 3Q	FY2020 4Q	FY2020 計
意図的な原因	不審メール等の受信	546	89	36	13	2	4	0	3	9
	ユーザＩＤ等の偽り	1	4	3	12	0	5	2	2	9
	DDoS攻撃等の大量アクセス	23	31	17	20	4	3	1	2	10
	情報の不正取得	14	16	10	8	3	2	4	4	13
	内部不正	0	4	1	0	0	0	0	0	0
	適切なシステム等運用の未実施	19	15	14	11	4	3	7	9	23
偶発的な原因	ユーザの操作ミス	15	23	10	6	4	5	3	6	18
	ユーザの管理ミス	8	13	6	6	3	0	2	8	13
	不審なファイルの実行	243	42	16	7	0	4	1	2	7
	不審なサイトの閲覧	29	20	4	5	0	1	2	0	3
	外部委託先の管理ミス	20	41	29	39	9	12	15	20	56
	機器等の故障	22	32	27	62	10	11	13	5	39
	システムの脆弱性	56	36	19	16	3	3	22	10	38
	他分野の障害からの波及	0	10	6	4	2	2	2	1	7
環境的な原因	災害や疾病等	0	0	1	13	0	7	2	0	9
その他の原因	その他	34	29	29	33	9	9	6	11	35
	不明	92	57	46	53	18	14	18	18	68

（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

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

○　サイバー攻撃対応は引き続き必要であるが、他のリスク源にも注意が必要

システムの更新・設定の不具合、外部委託先の不具合、内部の人的統制の不具合に起因するサービス障害等、外部からのサイバー攻撃以外の要因によるサービス障害の事例のほうが依然として多く発生している。なお、サイバー攻撃は、管理により防げたものが多くあった。

○　ネット接続に係る資産管理及びバックアップの重要性の再認識が必要

委託先クラウドのランサムウエア感染により、複数事業者が、データを暗号化され、長時間にわたりサービスを提供できなかった事例があった。

VPN の重要性の再認識と海外拠点等セキュリティ対策が弱い拠点から侵入されることがあることに留意。なお、最近のランサムウエアは、暗号化に加え機密情報を公開すると身代金を要求されることがある(二重脅迫型)。

○　BYOD(Bring Your Own Device)も含めた資産管理が必要

フィッシングメールにより私有スマホのアカウントが乗っ取られ、クラウドに自動バックアップ保存された機密情報が第三者から閲覧可能となった事例があった。

○　セキュリティ・バイ・デザインの考え方に則ったシステムの企画・設計段階からのセキュリティ確保が必要

システムの設計不備やアクセス集中により、新規立ち上げた予約システムに不具合が発生し、長時間にわたりサービスを提供できなかったほか、個人情報が閲覧可能な状態になった事例が多数あった。

○　キャパシティ(処理能力)管理を含めたバッチ処理の適切なスケジューリングが必要

バッチ処理の遅延により、システムに不具合が発生し、サービスを提供できなかった事例が複数あった。

○　不使用ドメインの一定期間の登録保持が必要

ドメインの不使用による登録解除後の悪意のある第三者による登録により、ウェブサイトにアクセスしたら不正サイトに誘導された事例があった。

以上