資料２

令和 3 年 10 月 25 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 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、2020 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. 世界的なサプライチェーン動向

1.1.1 半導体のサプライチェーン動向

- ○ 相次ぐ自然災害や工場火災、需要予測の誤り等により世界的に半導体が不足し、自動車生産等へ影響[1]。
- ○ 各国政府は自国の半導体生産の能力を向上させる方向で対応を実施[2]。

1.2. 米国

1.2.1 バイデン大統領の就任

- ○ 2021 年 1 月 20 日、米国第 46 代大統領にバイデン氏が就任[3]。
- ○ バイデン大統領は、就任日に 15 件の大統領令に署名、その後「パリ協定」に正式復帰、主要国首脳との電話会談で自由主義諸国の結束の重要性を強調[4]。
- ○ 2021 年 4 月 12 日、バイデン大統領は、米国サイバーセキュリティにかかわ

---

[1] *Bloomberg「台湾の水不足深刻化、非常警報も発令-TSMC はタンクローリー活用(2021/3/25)」、https://www.bloomberg.co.jp/news/articles/2021-03-25/QQH76ZT0AFB501 (2021/4/14 閲覧)*

[2] *日経新聞「バイデン氏、半導体の国内増産に意欲 産業界と意見交換(2021/4/13)」、https://www.nikkei.com/article/DGXZQOGN12CJ80S1A410C2000000/ (2021/4/18 閲覧)*

[3] *NHK「アメリカ バイデン新大統領 就任演説(2021/1/25)」、https://www3.nhk.or.jp/news/special/presidential-election_2020/report/about_joe-biden/about_joe-biden_08.html (2021/2/16 閲覧)*

[4] *BBC「バイデン氏、大統領令に次々署名 「パリ協定」復帰など(2021/1/21)」、https://www.bbc.com/japanese/55746524 (2021/2/9 閲覧)*

る 3 人のトップリーダーの候補者を指名[5]。

1.2.2 米国のサイバーセキュリティ強化、米中外交会談の実施

- ○ 米国の大統領選挙や、SolarWinds のソフトウエアの脆弱性をついた政府機関等が標的とされた大規模なサイバー攻撃が発生[6]。
- ○ バイデン大統領は、米国のサイバーセキュリティ強化に取り組む姿勢を表明[7]。
- ○ 2021 年 3 月 18 日、米中外交会談で、米国へのサイバー攻撃を含めた幅広い分野で意見交換を実施[8]。

1.2.3 日米首脳会談と共同声明

- ○ 2021 年 4 月 16 日、日米首脳会談が開催され、共同声明を発表[9]。
- ○ 今回の共同声明では、1969 年の日米首脳会談の共同声明以来、「台湾」に言及[10]。

1.3. 中国

1.3.1 中国によるワクチン外交の展開

- ○ 新型コロナウイルス感染症において、感染拡大初期のマスク外交に続き、中国製ワクチンによる途上国向けワクチン外交を展開、入手困難とされるワクチン等を外交カードにアジアや世界における影響力を拡大[11]。

---

[5] *THE WHITE HOUSE「President Biden Announces His Intent to Nominate 11 Key Administration Leaders on National Security and Law Enforcement(2021/4/12)」、https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/12/president-biden-announces-his-intent-to-nominate-11-key-administration-leaders-on-national-security-and-law-enforcement/（2021/4/20 閲覧）*

[6] *US-CERT「Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations(2020/12/17)」、https://us-cert.cisa.gov/ncas/alerts/aa20-352a（2021/3/26 閲覧）*

[7] *THE WHITE HOUSE「Executive Order on Improving the Nation's Cybersecurity(2021/5/12)」、https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/（2021/5/13 閲覧）*

[8] *U.S. DOS「Secretary Antony J. Blinken, National Security Advisor Jake Sullivan, Director Yang And State Councilor Wang At the Top of Their Meeting(2021/3/18)」、https://www.state.gov/secretary-antony-j-blinken-national-security-advisor-jake-sullivan-chinese-director-of-the-office-of-the-central-commission-for-foreign-affairs-yang-jiechi-and-chinese-state-councilor-wang-yi-at-th/（2021/3/25 閲覧）*

[9] *外務省「日米首脳会談(2021/4/16)」、https://www.mofa.go.jp/mofaj/na/na1/us/page1_000951.html（2021/4/21 閲覧）*

[10] *外務省「日米首脳共同声明「新たな時代における日米グローバル・パートナーシップ」(2021/4/16)」、https://www.mofa.go.jp/mofaj/files/100177719.pdf（2021/4/21 閲覧）*

[11] *ハンギョレ新聞「中国、ASEAN 相手に「ワクチン外交」、ベトナムだけ除外(2021/1/18)」、http://japan.hani.co.kr/arti/international/38876.html（2021/2/8 閲覧）*

1.3.2　中国海警法の成立及び施行とその後の動向

- ○ 2021 年 1 月 22 日、中国の国家主権、安全及び海洋権益の保護を目的に、海上警備にあたる中国海警局の任務や権限を規定した中国海警法が成立[12]。
- ○ 2021 年 2 月 1 日、中国海警法が施行されたが、日本政府は、その問題点を内外に情報発信し、中国を念頭とした「自由で開かれたインド太平洋」の実現に向けた取組を強化[13]。

1.3.3　第 13 期全国人民代表大会第 4 回会議の概要

- ○ 2021 年 3 月 5 日、全国人民代表大会第 4 回会議が開幕し、「第 14 次 5 か年計画」、「2035 年までの長期目標」が採択、香港の統治に関し、民主派を排除する選挙制度の変更を決定[14]。
- ○ 中国では、表現や言論自由・基本的人権・法の支配といった普遍的価値をめぐり国際社会との衝突を繰り返しており、香港の選挙制度改革、新疆ウイグル自治区や中国海警法等の中国の動きに対し、国際社会の対応が注目[15]。

1.3.4　香港における選挙制度改正について

- ○ 2021 年 3 月 11 日、第 13 期全国人民代表大会第 4 回会議において、愛国者を主体とする「香港人による香港支配」を確保するため、香港の選挙制度改正を決定[16]。
- ○ 2021 年 3 月 30 日、全人代常務委員会は、香港の行政長官を選ぶ選挙委員会の権限拡充や、事前に候補者を審査する「資格審査委員会」を新設するため、中華人民共和国香港特別行政区基本法附属書Ⅰ及びⅡを改正[17]。

---

[12] *中华人民共和国主席令「中华人民共和国海警法(2021/1/22)」、http://www.npc.gov.cn/npc/c30834/202101/58620cba3bba46f0832b9acd98657f83.shtml（2021/9/20 閲覧）*

[13] *外務省「日米安全保障協議委員会(日米「2＋2」)（概要)(2021/3/16)」、https://www.mofa.go.jp/mofaj/na/st/page1_000942.html（2021/3/17 閲覧）*

[14] *朝日新聞「全人代、香港の選挙制度改変採択して閉幕 民主派排除へ(2021/3/11)」、https://www.asahi.com/articles/ASP3C6RTCP3CUHBI01G.html（20201/3/16 閲覧）*

[15] *Sankei Biz「茂木外相、香港やウイグルに深刻懸念 国連人権理会合で表明(2021/2/24)」、https://www.sankeibiz.jp/macro/news/210224/mca2102240640008-n1.htm（2021/3/18 閲覧）*

[16] *全国人民代表大会「全国人大高票通过关于完善香港特别行政区选举制度的决定(2021/3/11)」、http://www.npc.gov.cn/npc/kgfb/202103/d594abc2c8cf47a4b9c853e39f6c19ca.shtml（2021/4/12 閲覧）*

[17] *日経新聞「香港選挙制度変更を可決 全人代常務委(2021/3/30)」、https://www.nikkei.com/article/DGXZQOGM305UN0Q1A330C2000000/（2021/4/16 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 各国の法執行機関によるサイバー攻撃への対応

- 2021 年 1 月 27 日、欧州刑事警察機構(Europol)は、国際連携の結果、マルウエア「Emotet」の攻撃インフラを制御下に置くことに成功[18]。
- 2021 年 2 月下旬以降、警察庁、総務省、ICT-ISAC 及び ISP が連携し、Emotet に感染した端末に対する通知を開始[19]。
- 2021 年 1 月以降、ランサムウエアの「Netwalker」、「Fonix」、「Ziggy」等が相次いで活動を停止[20]。

2.1.2 Microsoft Exchange Server の深刻な脆弱性

- 2021 年 3 月 2 日、マイクロソフトは、「Microsoft Exchange Server」の脆弱性について、悪用確認済の脆弱性 4 件を含む緊急性が高い 7 件を修正するセキュリティ更新プログラムを定例外で公開[21]。
- 複数の脆弱性を組み合わせることで、Microsoft Exchange Server が稼働しているデバイス上で、リモートから任意のコードを実行することが可能[22]。
- 本脆弱性を悪用し、機密情報の窃取やランサムウエアの感染を試みる攻撃が発生[23]。

2.2. 重要インフラ関連

2.2.1 米国フロリダ州の浄水処理施設へのサイバー攻撃について

- 米国フロリダ州の浄水処理システムがサイバー攻撃を受け、浄水処理に用いる苛性ソーダの注入量設定値が変更される事案が発生[24]。

---

[18] *Europol「WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION (2021/1/27)」、https://www.europol.europa.eu/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action (2021/3/2 閲覧)*

[19] *警察庁「マルウエアに感染している機器の利用者に対する注意喚起の実施について(2021/2/19)」、https://www.npa.go.jp/cyber/policy/mw-attention.html (2021/3/2 閲覧)*

[20] *BleepingComputer「Ziggy ransomware shuts down and releases victims' decryption keys(2021/2/7)」、https://www.bleepingcomputer.com/news/security/ziggy-ransomware-shuts-down-and-releases-victims-decryption-keys/ (2021/3/1 閲覧)*

[21] *マイクロソフト「On-Premises Exchange Server Vulnerabilities Resource Center - updated March 25, 2021 (2021/3/25)」、https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/ (2021/4/6 閲覧)*

[22] *マイクロソフト「オンプレミス Exchange Server の脆弱性の調査や修復に対応する方向けのガイダンス(2021/3/18)」、https://msrc-blog.microsoft.com/2021/03/18/20210319_exchangeoob_guidance/ (2021/4/6 閲覧)*

[23] *マイクロソフト「Analyzing attacks taking advantage of the Exchange Server vulnerabilities(2021/3/25)」、https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/ (2021/4/16 閲覧)*

[24] *Pinellas County Sheriff's Office 「21-015 Detectives Investigate Computer Software Intrusion at Oldsma*

○ 米国 CISA は、注意喚起を行い技術的な緩和策や奨励事項を提示[25]。
○ 浄水処理のような産業用制御システム(ICS)のセキュリティ確保に関して、保安体制を踏まえた対応が必要[26]。

2.2.2 ネットワーク機器やセキュリティ機器等の深刻な脆弱性

○ 2020 年 12 月 23 日、セキュリティ会社 EYE が、Zyxel 製のファイアウォール等に、第三者が管理者権限でログイン可能なバック ドア アカウントの存在を報告[27]。
○ 2021 年 1 月 22 日、SonicWall は、同社の一部のリモートアクセス製品にゼロデイ脆弱性が存在し、その脆弱性を悪用したとみられる不正アクセスの確認を報告[28]。
○ 2021 年 1 月 10 日にニュージーランド準備銀行(RBNZ)が、同年 1 月 25 日にオーストラリア証券投資委員会(ASIC)が、同年 2 月 1 日にワシントン州監査局(SAO)が、Accellion 製ファイル転送機器に関連した不正アクセスをそれぞれ公表[29]。

2.3. その他

2.3.1 セキュリティ研究者を標的にしたサイバー攻撃キャンペーン

○ 2021 年 1 月 25 日、グーグルとマイクロソフトは、様々な企業や組織のセキュリティ研究者を標的にしたサイバー攻撃キャンペーンについて警告[30]。
○ 攻撃グループは、ソーシャルメディア等を利用してセキュリティ研究者と信頼関係を構築後、悪意ある Web サイトや共同研究を装って送付したファイルを通じてシステムへマルウエアを感染[31]。

---

r's Water Treatment Plant(2021/2/8)」、https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant（2021/3/17 閲覧）

[25] *CISA「Alert (AA21-042A)Compromise of U.S. Water Treatment Facility(2021/2/11)」、https://us-cert.cisa.gov/ncas/alerts/aa21-042a（2021/3/17 閲覧）*

[26] *NIST「SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security(2015/5)」、https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final（2021/9/19 閲覧）*

[27] *EYE「Undocumented user account in Zyxel products(CVE-2020-29583)(2020/12/23)」、https://eye.security/en/blog/undocumented-user-account-in-zyxel-products-cve-2020-29583（2021/5/6 閲覧）*

[28] *SonicWall「SonicWall Publishes Additional SMA 100 Series 10.x and 9.x Firmware Upgrades(2021/2/19)」、https://www.sonicwall.com/blog/2021/01/security-notice-update-on-sma-100-series-product-investigation/（2021/5/6 閲覧）*

[29] *BleepingComputer「Data breach exposes 1.6 million Washington unemployment claims(2021/2/1)」、https://www.bleepingcomputer.com/news/security/data-breach-exposes-16-million-washington-unemployment-claims/（2021/4/16 閲覧）*

[30] *Google Threat Analysis Group「New campaign targeting security researchers(2021/1/25)」、https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/（2021/2/1 閲覧）*

[31] *マイクロソフト「ZINC attacks against security researchers(2021/1/28)」、https://www.microsoft.com/securit*

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 新型コロナウイルス感染症に関するサイバー事案

- 2021 年 1 月 21 日、緊急事態宣言に伴う対応を記載したメール等を装い、マルウエア「Emotet」に感染させようとする攻撃を国内で確認 [32]。
- 2021 年 1 月 26 日、英国の国民保健サービス(NHS)が、新型コロナウイルス感染症のワクチン接種の希望を確認するフィッシングメールを確認し、注意喚起を実施 [33]。
- 2021 年 1 月、地方自治体が、メールの誤送信等により、新型コロナウイルス感染症に関する陽性者情報を外部に漏えい等したことを相次いで公表 [34]。

3.1.2 地方自治体等におけるランサムウエアの被害の拡大

- 2019 年頃から米国を始めとする海外で、地方自治体及び関係機関におけるランサムウエアの被害が拡大、2020 年 11 月には国内でもカプコンの被害が大きく報道 [35]。
- 2021 年 2 月、地方自治体向けコンサルティング会社のサーバーがランサムウエアに感染し、200 を超える取引先の地方自治体等の個人情報が流出の可能性と報道 [36]。
- 地方自治体に限らず、被害の拡大が懸念されるため、引き続き注意が必要 [37]。

3.1.3 クラウドサービス利用時のセキュリティ上の課題

- 2020 年 12 月 25 日、クラウドサービス事業者のセールスフォース・ドットコムは、同社の顧客関係ソリューション「Salesforce」において、設定が適切に行

---

y/blog/2021/01/28/zinc-attacks-against-security-researchers/ (2021/2/1 閲覧)

[32] *浅間商事「【注意喚起】Emotet(エモテット)感染拡大のお知らせ(2021/1/22)」、https://www.asama-shoji.co.jp/blog/topics/6057/ (2021/1/28 閲覧)*

[33] *NHS(Twitter)「NHS(@NHSuk)の投稿(2021/1/26)」、https://twitter.com/NHSuk/status/1353751565518123015 (2021/1/28 閲覧)*

[34] *日経 xTECH「コロナ感染者の個人情報を「うっかり流出」、地方自治体で相次ぐ事故の理由(2021/1/26)」、https://xtech.nikkei.com/atcl/nxt/column/18/00138/012200715/ (2021/5/31 閲覧)*

[35] *朝日新聞「カプコン脅迫、犯罪グループがファイル公開 機密情報か(2020/11/11)」、https://www.asahi.com/articles/ASNCC4GB1NCCULZU005.html (2020/12/16 閲覧)*

[36] *日経新聞「200 超の自治体情報流出か コンサルにサイバー攻撃(2021/4/1)」、https://www.nikkei.com/article/DGXZQOUE01BUY0R00C21A4000000/ (2021/4/6 閲覧)*

[37] *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)*

われていない場合、Salesforce 上の一部の情報が第三者から閲覧できると発表[38]。

- 2020 年 12 月以降、Salesforce における設定不備により、意図しない情報が外部から参照された可能性があると公表する組織が相次ぎ、特に、2021 年 2 月以降、国内の複数の地方自治体が同様の可能性を発表[39]。
- 2021 年 2 月 20 日、Amazon Web Services(AWS)が提供するクラウドサービスの一部に障害が発生、これに伴い、2 月 22 日午前 5 時 55 分頃から午前 10 時 50 分頃まで、気象庁の Web サイトで一部コンテンツ(最新の気象データ、地震等)の閲覧障害が発生[40]。

3.1.4 相次ぐ国内の IT 関連のシステムトラブル

- みずほ銀行の複数のシステム、新型コロナウイルス接触確認アプリ「COCOA」、マイナンバーカードの健康保険証利用、NTT ドコモのオンライン専用料金プラン「ahamo」など、国内の複数の IT システム関連の障害が発生[41]。
- 障害の原因は、機器の故障やプログラムの不具合、処理リソースの不足など、個々の事案で差異を確認[42]。
- 想定していない障害の発生を抑え、収束させるためには、経営層を含めた組織全体の対応が必要[43]。

3.2. その他

3.2.1 LINE による利用者データの保護管理について

- 2021 年 3 月、国内の LINE 利用者のデータに対し、国外からアクセスできる状態にあったとの報道[44]。
- LINE は規約でそのような状況を十分説明しておらず、対応に不備があったと

---

[38] *ITmedia「楽天、PayPay の情報漏えい、原因はセールスフォース製品の設定ミス？(2020/12/28)」、https://www.itmedia.co.jp/business/articles/2012/28/news051.html (2021/3/2 閲覧)*

[39] *日経 xTECH「9 つの自治体で不正アクセスの可能性が明らかに、セールスフォース「設定不備」問題(2021/2/12)」、https://xtech.nikkei.com/atcl/nxt/news/18/09644/ (2021/3/5 閲覧)*

[40] *ITmedia「AWS 障害、5 時間でほぼ復旧 気象庁 Web サイトなどに影響(2021/2/20)」、https://www.itmedia.co.jp/news/articles/2102/20/news021.html (2021/3/9 閲覧)*

[41] *みずほフィナンシャルグループ、みずほ銀行「株式会社みずほ銀行におけるシステム障害に係る対応状況について(2021/4/5)」、https://www.mizuho-fg.co.jp/release/pdf/20210405_2release_jp.pdf (2021/4/13 閲覧)*

[42] *みずほフィナンシャルグループ、「株式会社みずほ銀行におけるシステム障害にかかる原因究明・再発防止について(2021/6/15)」、https://www.mizuho-fg.co.jp/release/pdf/20210405_2release_jp.pdf (2021/9/22 閲覧)*

[43] *経済産業省「サイバーセキュリティ経営ガイドライン Ver 2.0(2017/11/16)」、https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf (2021/9/22 閲覧)*

[44] *朝日新聞「日本の LINE 利用者の画像・動画全データ、韓国で保管(2021/3/17)」、https://www.asahi.com/articles/ASP3K64ZCP3KUHBI01W.html (2021/4/6 閲覧)*

判断し、個人情報保護委員会及び総務省に報告する一方、調査のための第三者委員会を立ち上げ、運用の見直しに着手[45]。

3.2.2　インサイダースレットについて

- ○ 2021 年 3 月、ソフトバンク及び松井証券に関するインサイダースレット(内部からの脅威)に係る事案を発表[46]。
- ○ 事案の共通点として、「自身の業務及び情報へのアクセス権限の範囲内で不正行為を行っていた」「不正行為をいち早く検知する仕組みが機能していなかった」ことなどが挙げられた[47]。
- ○ セキュリティ対策としては、システムの管理に加え、「人の管理」の視点も重要[48]。

以上

---

[45] *LINE「ユーザーの個人情報に関する一部報道について(2021/3/17)」、https://linecorp.com/ja/pr/news/ja/2021/3675（2021/4/6 閲覧）*

[46] *松井証券「業務委託先元従業員の逮捕について(2021/3/24)」、https://www.matsui.co.jp/parts/pdf-view/web/viewer.html?file=/company/ir/press/pdf/pr210324.pdf（2021/4/7 閲覧）*

[47] *情報処理推進機構「「企業における営業秘密管理に関する実態調査 2020」報告書について(2021/3/18)」、https://www.ipa.go.jp/security/fy2020/reports/ts_kanri/index.html（2021/4/7 閲覧）*

[48] *ソフトバンク「訪問販売代理店でのお客さま情報の不正取得について(2021/3/4)」、https://www.softbank.jp/corp/news/press/sbkk/2021/20210304_01/（2021/4/7 閲覧）*

サイバーセキュリティを取り巻く情勢(2021 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、2021 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 サイバーセキュリティに関する米国大統領令

- ○ 2021 年 2 月 24 日、バイデン大統領は、経済的繁栄及び国家安全保障の確保と国際的な緊急事態への対応能力の向上を目的に、米国のサプライチェーンの強靭性を強化するための大統領令に署名[1]
- ○ 2021 年 5 月 12 日、バイデン大統領は、米国へのサイバー攻撃などに対応すべく、サイバーセキュリティ分野で連邦政府機関と契約する情報通信サービス企業との間で官民連携を深めることを趣旨とする大統領令に署名[2]。

1.1.2 米国のサイバーセキュリティに関する取組

- ○ 2021 年 6 月 2 日、Anne Neuberger 大統領副補佐官(サイバー・新興技術担当)は、企業経営者やビジネスリーダーに対し、ランサムウエア攻撃から身を守るためのセキュリティ対策について書簡を送付[3]。

---

[1] *THE WHITE HOUSE「Executive Order on America's Supply Chains(2021/2/24)」、https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/ (2021/5/11 閲覧)*

[2] *THE WHITE HOUSE「Executive Order on Improving the Nation's Cybersecurity(2021/5/12)」、https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (2021/5/18 閲覧)*

[3] *THE WHITE HOUSE「What We Urge You To Do To Protect Against The Threat of Ransomware(2021/6/2)」、https://www.spencerfane.com/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf (2021/6/8 閲覧)*

○ 2021 年 6 月 8 日、大規模なサイバー攻撃が進行中又は差し迫っている場合の対応と復旧のために、公的機関や民間企業を直接支援することが可能な法律を含む「2021 年米国イノベーション・競争法」が連邦議会上院で可決[4]。

1.1.3 2022 年度連邦政府サイバーセキュリティ予算要求

○ 2021 年 5 月 28 日、米国行政管理予算局は、2022 年度の予算教書を連邦議会に提出[5]。

○ 2022 年度予算教書では、サイバーセキュリティを含む安全保障について、中国の脅威への対抗やロシアの不安定な行動の抑止を優先[6]。

○ 2022 年度のサイバーセキュリティに係る予算要求について、サイバーセキュリティ・インフラセキュリティ庁(CISA)は 21 億 3400 万ドル、エネルギー省(DOE)は 6 億 4200 万ドル、国防総省(DOD)は 104 億ドルを計上[7]。

1.2. 中国

1.2.1 一帯一路をめぐる動向、中国の海洋侵出をめぐる動向

○ 一帯一路に関して、ASEAN 諸国で計画が進む中、オーストラリア連邦政府は、ビクトリア州政府が中国と締結した「一帯一路」構想に関する協定破棄を公表[8]。

○ 2021 年 6 月 13 日、イタリアは、中国と一帯一路に参加する覚書について、見直しを含めて考えていることを表明[9]。

○ 2021 年 4 月 29 日、全人代常務委員会は、海上交通を担う海事局の権限を強化する改正海上交通安全法を可決(2021 年 9 月 1 日施行)[10]。

○ 2021 年 4 月 26 日、中国は尖閣諸島の地形調査報告書を発表、日本政府は

---

[4] *Senate Democrat「The United States Innovation and Competition Act of 2021」、https://www.democrats.senate.gov/imo/media/doc/USICA%20Summary%205.18.21.pdf（2021/6/15 閲覧）*

[5] *Reuters「米 22 年度予算案、歳出 6 兆ドル要求 インフラ投資など重点(2021/5/29)」、https://jp.reuters.com/article/usa-biden-budget-idJPKCN2D92BV（2021/7/6 閲覧）*

[6] *JETRO「バイデン米政権、予算教書を議会に提出、2022 年度は 6 兆ドル規模の歳出を要求(2021/6/3)」、https://www.jetro.go.jp/biznews/2021/06/054bf78f18d7c3c1.html（2021/7/13 閲覧）*

[7] *Office of Management and Budget「BUDGET OF THE U.S. GOVERNMENT FISCAL YEAR 2022」、https://www.whitehouse.gov/wp-content/uploads/2021/05/budget_fy22.pdf（2021/7/13 閲覧）*

[8] *オーストラリア政府外務省「Decisions under Australia's Foreign Arrangements Scheme(2021/4/21)」、https://www.foreignminister.gov.au/minister/marise-payne/media-release/decisions-under-australias-foreign-arrangements-scheme（2021/5/16 閲覧）*

[9] *Reuters「対中で率直な意見表明が必要、一帯一路見直しも＝伊首相(2021/6/14)」、https://jp.reuters.com/article/g7-summit-china-italy-idJPKCN2DQ06Y（2021/8/15 閲覧）*

[10] *全国人民代表大会「中华人民共和国海上交通安全法(2021/4/29)」、http://www.npc.gov.cn/npc/c30834/202104/9dfede4d82aa4fc1ae8ca22e987e025b.shtml（2021/8/8 閲覧）*

外交ルートを通じて中国へ抗議[11]。

1.2.2　相次ぐ法整備の動き、G7 首脳宣言での中国への言及

- 2021 年 6 月 10 日、全国人民代表大会常任委員会において、中国に対して制裁を発動した外国に対抗措置を取ることを可能とする中国反外国制裁法や中国データセキュリティ法等が成立[12]。
- 2021 年 6 月 13 日、英国で開催された G7 サミットの首脳宣言では中国の強硬なふるまいに対し、G7 首脳は連携して反対の姿勢を表明[13]。

1.3.　国連

1.3.1　サイバーセキュリティに関する第 6 会期国連政府専門家会合について

- 2021 年 5 月 24 日、サイバーセキュリティに関する第 6 会期国連政府専門家会合(GGE)最終会合が開催され、サイバー空間における責任ある国家の行動に関する報告書が採択[14]。
- 今後、この報告書は、2021 年 9 月の第 76 回国連総会に提出される見通し[15]。

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　VPN 機器の脆弱性を悪用したサイバー攻撃の発生

- 日本企業の調査によれば、2021 年 1 月から 3 月にランサムウエアの被害を受けたシステムに共通する特徴として、VPN 機器の修正パッチが未適用、パスワードが推測可能等のものが存在、VPN 機器の運用管理が重要[16]。
- 2021 年 4 月 13 日、カプコンは、同社に対するサイバー攻撃の調査結果を公表、新型コロナ禍におけるネットワーク負荷増大を考慮し予備機に保有して

---

[11] *nippon.com「尖閣諸島の地形図公表、外交ルート通じ中国に抗議=加藤官房長官(2021/4/27)」、https://www.nippon.com/ja/news/reu20210427KBN2CE05H/（2021/5/14 閲覧）*

[12] *読売新聞「対中制裁に対抗措置、中国が「反外国制裁法」など可決(2021/6/10)」、https://www.yomiuri.co.jp/world/20210610-OYT1T50187/（2021/8/17 閲覧）*

[13] *外務省「G7 コーンウォール・サミット 首脳コミュニケ(2021/6/13)」、https://www.mofa.go.jp/mofaj/files/100200083.pdf（2021/6/15 閲覧）*

[14] *外務省「サイバーセキュリティに関する国連政府専門家会合最終会合における報告書の採択(2021/5/29)」、https://www.mofa.go.jp/mofaj/press/release/press24_000114.html（2021/6/14 閲覧）*

[15] *外務省「GGE 報告書の主要なポイント(速報版)」、https://www.mofa.go.jp/mofaj/files/100195724.pdf（2021/6/14 閲覧）*

[16] *ラック「2021 年も増加傾向のランサムウェア、被害に関する共通点とは(2021/4/5)」、https://www.lac.co.jp/lacwatch/report/20210405_002585.html（2021/8/23 閲覧）*

いた旧型の VPN 機器を経由して攻撃者が組織内に不正侵入したと説明[17]。

○ 2021 年 5 月 6 日、米国 CISA は、VPN 機器のゼロデイ脆弱性を悪用し、新種のランサムウエア「FiveHands」に感染する事例が確認されたとして注意喚起を公開[18]。

2.1.2 ランサムウエアに対する脅威の高まり

○ 2021 年 4 月以降、国内企業や海外子会社におけるランサムウエアの被害が複数発生[19]。

○ 国外では、米国の石油パイプライン企業 Colonial Pipeline 等の重要インフラに係る組織等でランサムウエアの被害が相次ぎ発生[20]。

○ セキュリティ企業の調査によれば、2020 年におけるランサムウエアの影響を修復するための費用の平均額は前年の 2 倍[21]。

2.1.3 最近のマルウエアに係る動向

○ 2021 年 3 月以降、メールやブラウザ等の認証情報を窃取する等の機能を有するマルウエア「IcedID」に感染させようとする不正なメールを多数確認[22]。

○ 2021 年 4 月 22 日、米国 CISA は、Web シェル「SUPERNOVA」による攻撃の分析レポートを公開、攻撃者がこの Web シェルを埋め込むことで、攻撃対象環境に対するアクセスの永続性を確立[23]。

2.2. その他

2.2.1 ソフトウエアのサプライチェーンに対する攻撃

○ 米国の多数の政府機関や企業等で導入されている IT 監視・管理ソフトウエア「SolarWinds Orion」にバックドアが含まれていたことが公表[24]。

---

[17] *カプコン「不正アクセスに関する調査結果のご報告【第 4 報】(2021/4/13)」、https://www.capcom.co.jp/ir/news/html/210413.html（2021/8/23 閲覧）*

[18] *CISA「Analysis Report (AR21-126A) FiveHands Ransomware(2021/5/6)」、https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a（2021/8/23 閲覧）*

[19] *KADOKAWA「海外子会社サーバーへの不正アクセスについて(2021/6/4)」、https://group.kadokawa.co.jp/documents/topics/20210604_f3dmp.pdf（2021/6/7 閲覧）*

[20] *ITmedia「ランサムウェア攻撃を受けた JBS、約 12 億円の身代金をビットコインで支払い(2021/6/10)」、https://www.itmedia.co.jp/news/articles/2106/10/news112.html（2021/8/23 閲覧）*

[21] *Sophos「ランサムウェアの現状 2021 年版(2021/4)」、https://secure2.sophos.com/ja-jp/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf（2021/8/23 閲覧）*

[22] *トレンドマイクロ「「EMOTET」後のメール脅威状況：「IcedID」および「BazarCall」が 3 月に急増(2021/4/28)」、https://blog.trendmicro.co.jp/archives/27732（2021/8/23 閲覧）*

[23] *CISA「Analysis Report (AR21-112A) CISA Identifies SUPERNOVA Malware During Incident Response(2021/4/29)」、https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112a（2021/8/23 閲覧）*

[24] *Solarwinds「SolarWinds Security Advisory(2021/4/6)」、https://www.solarwinds.com/ja/sa-overview/security*

○ ソフトウエア開発支援のツール「Codecov」に対する攻撃が発生 [25]。
○ 2021 年 4 月、米国 CISA は、ソフトウエアのサプライチェーン攻撃に対する防御に関するガイダンスを発行 [26]。
○ 2021 年 5 月 12 日、バイデン大統領は、ソフトウエアのサプライチェーンに関する対応策を含む大統領令(EO14028)に署名この大統領令に基づき、米国 NIST などがガイドライン等を発表 [27]。

2.2.2 世界各地の大規模な Web サイトのアクセス障害

○ 2021 年 6 月 8 日、CDN 大手 Fastly のシステム障害により、日本の政府機関等を含む世界各地の Web サイトにおいて、アクセス障害が発生 [28]。
○ 2021 年 6 月 17 日、CDN 世界最大手 Akamai テクノロジーズのシステム障害により、米国やオーストラリアの航空会社や金融機関、証券取引所等の Web サイトにおいて、アクセス障害が発生 [29]。

2.2.3 MITRE ATT&CK について

○ MITRE ATT&CK は、実際のサイバー攻撃の手法を体系化し、攻撃者の攻撃方法や行動、目的を明文化したもので、それについて概説 [30]。
○ ATT&CK では、セキュリティ運用、脅威インテリジェンス、セキュリティアーキテクチャなど様々な形で利用例を紹介 [31]。
○ ATT&CK を活用することで、攻撃を検知して対応するアプローチが実現可能 [32]。

---

advisory（2021/9/18 閲覧）

[25] *Codecov「Bash Uploader Security Update（2021/4/29)」、https://about.codecov.io/security-update/（2021/6/18 閲覧）*

[26] *CISA「Codecov Releases New Detections for Supply Chain Compromise(2021/4/30)」、https://us-cert.cisa.gov/ncas/current-activity/2021/04/30/codecov-releases-new-detections-supply-chain-compromise（2021/6/18 閲覧）*

[27] *NIST「 Improving the Nation's Cybersecurity: NIST's Responsibilities under the Executive Order（2021/5/12)」、https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity（2021/8/13 閲覧）*

[28] *日経新聞「大規模システム障害、世界数千件に影響 1500 億円損失も(2021/6/9)」、https://www.nikkei.com/article/DGXZQOGN08FC50Y1A600C2000000（2021/9/15 閲覧）*

[29] *CNN「ネットでまた大規模障害、航空会社や銀行などのサイトが一時ダウン(2021/6/18)」、https://www.cnn.co.jp/tech/35172578.html（2021/9/15 閲覧）*

[30] *MITRE「ATT&CK Matrix for Enterprise」、https://attack.mitre.org/（2021/5/26 閲覧）*

[31] *MITRE「MITRE ATT＆CK:Design and Philosophy(2020/3)」、https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf（2021/5/20 閲覧）*

[32] *MITRE「Frequently Asked Questions」、https://attack.mitre.org/resources/faq/（2021/9/20 閲覧）*

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 英国の国際戦略研究所の「サイバー能力と国力」に関するレポート

- 2021 年 6 月 28 日、英国のシンクタンク国際戦略研究所(IISS: International Institute for Strategic Studies)は、「サイバー能力と国力」と題するレポートを発表[33]。
- 日本の評価について、インターネット関連技術などに強みがあるとしているが、日本国憲法上の理由から軍事的なサイバー攻撃能力の開発や情報収集活動が制限されており、企業の経営層においてサイバー防衛への理解不足があるとし、3 段階の区分で一番低い「Tier 3」と区分。

3.1.2 外交青書について

- 2021 年 4 月 27 日、外務省は、令和 3 年版外交青書を公表[34]。
- 令和 3 年版外交青書では、中国を「日本を含む地域と国際社会の安全保障上の強い懸念」と、また、竹島を「日本固有の領土」と記述。
- これらに対し、中国及び韓国は、それぞれ抗議[35]。

3.2. 重要インフラ関連

3.2.1 新型コロナウイルスワクチン接種予約システムに関する様々なトラブル

- 新型コロナウイルスワクチン接種予約について、65 歳以上の高齢者を優先に始まった件で、複数自治体におけるワクチン予約システムの障害が発生[36]。
- 東京都の医療従事者等向けのワクチン接種予約システムでは、個人情報が閲覧可能な状態になっていた可能性があり、改修完了まで Web サイトでのワクチン予約を中止[37]。
- 2021 年 5 月 17 日、自衛隊大規模接種センターにおける新型コロナウイルスワクチンの接種予約の受付開始後、予約情報の入力チェックや特定条件下での操作ができなくなる問題が判明し予約システムを改修[38]。

---

[33] *IISS「Cyber Capabilities and National Power: A Net Assessment(2021/6/28)」、https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power（2021/7/7 閲覧）*

[34] *外務省「令和 3 年版外交青書」、https://www.mofa.go.jp/mofaj/files/100181433.pdf（2021/5/18 閲覧）*

[35] *中国外交部「報道官定期記者会見(2021/4/27)」、https://www.fmprc.gov.cn/web/fyrbt_673021/jzhsl_673025/t1871962.shtml（2021/5/18 閲覧）*

[36] *日経 xTECH「新型コロナワクチン接種の予約、複数自治体がシステム障害で相次ぎ停止(2021/4/16)」、https://xtech.nikkei.com/atcl/nxt/news/18/10128（2021/8/23 閲覧）*

[37] *東京都「ワクチン接種予約システムの不具合について(2021/4/27)」、https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/04/28/20.html（2021/8/23 閲覧）*

[38] *日経 xTECH「防衛省が大規模接種センターの予約サイトを改修、自治体コードに入力チェック追加(2021/5/24)」、https://xtech.nikkei.com/atcl/nxt/news/18/10445/（2021/8/23 閲覧）*

3.2.2　中央銀行デジタル通貨と暗号資産の動向

- ○ 日本では、他国に先んじて暗号資産の制度整備を行い、2021 年 4 月には日本銀行が中央銀行デジタル通貨の実証実験の初期段階を開始[39]。
- ○ 米国では、FRB が米国の中央銀行デジタル通貨を発行する可能性に特に焦点を当てたディスカッションペーパーを 2021 年夏に発行する予定[40]。
- ○ 中国では、デジタル人民元の実証実験を進行[41]。
- ○ 暗号資産について、米国では 1 万ドル相当以上の移転に内国歳入庁への報告を義務付ける方針を公表するなど規制を強化、米 Facebook では独自の暗号資産「Diem」発行に向けた準備を進行[42]。

3.3.　その他

3.3.1　最近の不正アクセスによる情報流出事案

- ○ 2021 年第 1 四半期、ネットマーケティングやユピテル、弥生、中日新聞社等が不正アクセスより、1 万件以上のクレデンシャル情報や個人情報が流出した可能性等を発表[43]。
- ○ ネットマーケティングの事案では、マッチングアプリ Omiai の会員登録時に使用する年齢確認用の運転免許証等の画像データが最大 171 万件分の情報が流出した可能性を発表[44]。
- ○ ユピテルの事案では、2017 年 10 月の不正アクセスの覚知から 3 年半以上過ぎ、情報流出を受け発表[45]。

以上

---

[39] *日本銀行「中央銀行デジタル通貨に関する実証実験の開始について(2021/4/5)」、https://www.boj.or.jp/announcements/release_2021/rel210405b.pdf（2021/6/15 閲覧）*

[40] *米国連邦準備制度理事会「Federal Reserve Chair Jerome H. Powell outlines the Federal Reserve's response to technological advances driving rapid change in the global payments landscape(2021/5/21)」、https://www.federalreserve.gov/newsevents/pressreleases/other20210520b.htm（2021/6/15 閲覧）*

[41] *Foresight「「遅くても 2022 年までに」実用化秒読みに入ったデジタル人民元(2021/3/5)」、https://www.fsight.jp/articles/-/47782（2021/6/15 閲覧）*

[42] *Diem 協会「Diem Announces Partnership with Silvergate and Strategic Shift to the United States(2021/5/12)」、https://www.diem.com/en-us/updates/diem-silvergate-partnership/（2021/6/15 閲覧）*

[43] *中日新聞「お客さま情報の流出の可能性に関するお知らせとお詫び(2021/6/24)」、https://static.chunichi.co.jp/pdf/article/afb5552138202fb23d968567c0311468.pdf（2021/7/5 閲覧）*

[44] *ネットマーケティング「不正アクセスによる会員様情報流出に関するお詫びとお知らせ(2021/5/21)」、https://www.net-marketing.co.jp/news/5873/（2021/6/8 閲覧）*

[45] *ユピテル「My Yupiteru 会員様情報の一部流出のお詫びとお知らせ(2021/6/7)」、https://www.yupiteru.co.jp/corp/important/210607.html（2021/7/2 閲覧）*

重要インフラにおける情報共有件数について(2021 年度第 2 四半期)

「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	FY2017 計	FY2018 計	FY2019 計	FY2020 計	FY2021 1Q	FY2021 2Q	FY2021 3Q	FY2021 4Q	FY2021 計
重要インフラ事業者等からNISCへの情報連絡(※)	388	223	269	309	109	79	－	－	188
関係省庁・関係機関からのNISCへの情報共有	19	7	16	16	4	1	－	－	5
NISCからの情報提供	54	43	38	64	17	24	－	－	41

（※）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			FY2017 計	FY2018 計	FY2019 計	FY2020 計	FY2021 1Q	FY2021 2Q	FY2021 3Q	FY2021 4Q	FY2021 計
未発生の事象		予兆・ヒヤリハット	80	27	12	28	5	2	－	－	7
発生した事象	機密性を脅かす事象	情報の漏えい	15	13	13	23	11	5	－	－	16
	完全性を脅かす事象	情報の破壊	20	17	11	12	4	7	－	－	11
	可用性を脅かす事象	システム等の利用困難	143	97	158	157	62	41	－	－	103
	上記につながる事象	マルウェア等の感染	65	17	9	18	6	7	－	－	13
		不正コード等の実行	13	4	5	3	0	0	－	－	0
		システム等への侵入	17	14	14	26	5	8	－	－	13
		その他	35	34	47	42	16	9	－	－	25

2.原因別類型（複数選択）

原因の類型		FY2017 計	FY2018 計	FY2019 計	FY2020 計	FY2021 1Q	FY2021 2Q	FY2021 3Q	FY2021 4Q	FY2021 計
意図的な原因	不審メール等の受信	89	36	13	9	3	0	－	－	3
	ユーザＩＤ等の偽り	4	3	12	9	3	0	－	－	3
	DDoS攻撃等の大量アクセス	31	17	20	10	3	4	－	－	7
	情報の不正取得	16	10	8	13	5	0	－	－	5
	内部不正	4	1	0	0	0	1	－	－	1
	適切なシステム等運用の未実施	15	14	11	23	4	3	－	－	7
偶発的な原因	ユーザの操作ミス	23	10	6	18	5	1	－	－	6
	ユーザの管理ミス	13	6	6	13	5	2	－	－	7
	不審なファイルの実行	42	16	7	7	1	0	－	－	1
	不審なサイトの閲覧	20	4	5	3	2	0	－	－	2
	外部委託先の管理ミス	41	29	39	56	25	29	－	－	54
	機器等の故障	32	27	62	39	11	6	－	－	17
	システムの脆弱性	36	19	16	38	5	7	－	－	12
	他分野の障害からの波及	10	6	4	7	4	2	－	－	6
環境的な原因	災害や疾病等	0	1	13	9	0	3	－	－	3
その他の原因	その他	29	29	33	35	21	4	－	－	25
	不明	57	46	53	68	23	25	－	－	48

（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(2021 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

○　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

ランサムウエア感染により、データが暗号化され、長時間にわたりサービスを提供できなかった事例が多数あった。

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。また、業務委託先のランサムウエア感染により、同先に格納される自社データが被害に遭うことがあることに留意。なお、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)。

○　委託先を含めたシステム開発環境や API 連携先の不正アクセス対策の確認が必要

システム開発環境や API 連携サービスへの不正アクセスにより、機密情報が漏えいした事例が複数あった。

○　リスト型攻撃対策は依然必要

顧客マイページへのリスト型攻撃による不正アクセスにより、顧客情報が不正に閲覧された事例が複数あった。

複数アドレスからの分散した検知されにくい時間をかけた（low & slow の）リスト型攻撃が行われることがあることに留意。

○　SNS の活用等による BCP における複数情報公開手順の確保が必要

外部サービスである CDN(Contents Delivery Network)の障害により、この CDN を利用している複数事業者が同時多発的にウェブサービスを提供できなくなった事例があった。

以上

最近のインシデントから得られた教訓(2021 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

○　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

ランサムウエア感染により、データが暗号化され、長時間にわたりサービスを提供できなかった事例が多数あった。

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。また、業務委託先のランサムウエア感染により、同先に格納される自社データが被害に遭うことがあることに留意。なお、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)。

○　サプライチェーン管理の徹底や設定どおりの稼働の確保が必要

一時的なシステム障害の際、冗長化したシステムが設定どおりには予備系に切り替わらず、長時間にわたりサービスを提供できなかった事例が多数あった。

○　リスクに応じた外部サービスの利用が必要

利用する外部サービスの停止によりシステムに不具合が発生し、長時間にわたりサービスが提供できなかった事例が多数あった。

○　SNS の活用等による BCP における複数情報公開手順の確保が必要

外部サービスである CDN(Contents Delivery Network)の障害により、この CDN を利用している複数事業者が同時多発的にウェブサービスを提供できなくなった事例があった。

以上