資料３

令和 4 年 3 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から得られた知見を共有する。

サイバーセキュリティを取り巻く情勢(2021 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、2021 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。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 サイバー攻撃に対する取組

○ 米国のサイバーセキュリティ政策の「ランサムウエア攻撃への対応」について、被害企業に身代金を安易に支払わせない取組等、多面的な政策を実施[1]。

○ バイデン政権は、2021 年 10 月 13 日、14 日、30 か国以上の国々と、ランサムウエアの脅威に対処するための国際会議を開催し、犯罪者グループを撲滅するための対策をまとめた共同声明を発表[2]。

○ バイデン大統領は、ロシア系とされるサイバー犯罪集団に関する情報提供へ報奨金を支払うなど、サイバーセキュリティに係る中国、ロシアに対する積極的な対応を実施[3]。

○ 米国政府は、2021 年 12 月 15 日、重要インフラのサイバーセキュリティ強化を目的とした新たなセキュリティガイダンス「CISA Insights:潜在的なサイバー

---

[1] *DEPARTMENT OF THE TREASURY「Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments(2021/9/21)」、https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (2021/11/9 閲覧)*

[2] *THE WHITE HOUSE「Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021(2021/10/14)」、https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/ (2021/11/9 閲覧)*

[3] *U.S. DEPARTMENT of STATE「Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice(2021/11/4)」、https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/ (2021/12/14 閲覧)*

脅威の準備と軽減」を発行[4]。

1.1.2 対中国関連動向等

- ○ 米国議会の超党派諮問機関「米中経済安全保障調査委員会(USCC)」は、2021 年 11 月 17 日、年次報告書で、中国人民解放軍は台湾に侵攻する能力を有しているか、又は近いうちに有することを指摘、中国の台湾攻撃に対する米国の抑止力が低下していることに危機感を表明[5]。
- ○ 米国のバイデン大統領と中国の習近平国家主席は、2021 年 11 月 15 日、米中首脳会談を開催[6]。
- ○ バイデン大統領は、2021 年 12 月 6 日、2022 年 2 月の北京オリンピック・パラリンピック競技大会に外交官や公式代表を派遣しない「外交的ボイコット」を発表、その後、2021 年 12 月 9 日、10 日に民主主義のためのサミットを開催[7]。
- ○ バイデン大統領は、2021 年 11 月 11 日、「中国通信機器排除法」に、12 月 23 日、中国の新疆ウイグル自治区からの物品輸入を原則禁止とする「ウイグル強制労働防止法案」に署名[8]。

1.1.3 2022 会計年度国防権限法の成立等

- ○ 2021 年 12 月 27 日、米国国防予算の大枠と国防政策の方針を含む 2022 会計年度の国防権限法(NDAA2022)が成立[9]。
- ○ 米国議会は、米国政府への資金調達を行う 2022 年度の歳出法が成立されておらず、今後の米国のサイバーセキュリティ政策に影響を及ぼす可能性[10]。

---

[4] *CISA「PREPARING FOR AND MITIGATING POTENTIAL CYBER THREATS(2021/12/15)」、https://www.cisa.gov/sites/default/files/publications/CISA_INSIGHTS-Preparing_For_and_Mitigating_Potential_Cyber_Threats-508C.pdf（2022/1/18 閲覧）*

[5] *U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION「2021 Annual Report to Congress(2021/11/17)」、https://www.uscc.gov/annual-report/2021-annual-report-congress（2021/12/7 閲覧）*

[6] *THE WHITE HOUSE「Readout of President Biden's Virtual Meeting with President Xi Jinping of the People's Republic of China(2021/11/16)」、https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/16/readout-of-president-bidens-virtual-meeting-with-president-xi-jinping-of-the-peoples-republic-of-china/（2021/11/18 閲覧）*

[7] *THE WHITE HOUSE「Press Briefing by Press Secretary Jen Psaki, December 6, 2021(2021/12/6)」、https://www.whitehouse.gov/briefing-room/press-briefings/2021/12/06/press-briefing-by-press-secretary-jen-psaki-december-6-2021/（2021/12/7 閲覧）*

[8] *THE WHITE HOUSE「Bill Signed: H.R. 3919(2021/11/11)」、https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/11/bill-signed-h-r-3919/（2021/12/14 閲覧）*

[9] *THE WHITE HOUSE「Bill Signed: S. 1605(2021/12/27)」、https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/27/bill-signed-s-1605/（2022/1/26 閲覧）*

[10] *House Committee on Appropriations「Government Funding Update: Republicans Must Negotiate」、https://appropriations.house.gov/government-funding-update（2022/1/25 閲覧）*

1.2. 中国

1.2.1 中国共産党の 100 年奮闘の重大成果と歴史的経験に関する決議の採択

○ 中国共産党の第 19 期中央委員会第 6 回全会は、2021 年 11 月 11 日、中国共産党の 100 年の歩みを総括する歴史決議「党の 100 年奮闘の重大成果と歴史的経験に関する決議」を採択、毛沢東氏、鄧小平氏の時代に続く第 3 の歴史決議[11]。

○ 習近平総書記は、毛沢東氏、鄧小平氏と並ぶ権威を確立し、2022 年秋の第 20 回中国共産党大会での 3 期目を目指す布石[12]。

1.2.2 第 14 次 5 か年計画の商務発展計画・外資利用発展計画

○ 中国商務部は、2021 年 7 月 8 日、「第 14 次 5 か年計画の商務発展計画」を公表[13]。

○ 中国商務部は、2021 年 10 月 22 日、「第 14 次 5 か年計画期間の外資利用発展計画」を公表[14]。

1.2.3 2022 年北京オリンピック・パラリンピック競技大会開催等

○ 2022 年北京大会は、2022 年 2 月 4 日から開催が予定される中、外交的ボイコットやスマホアプリの個人情報漏えいリスクが懸念[15]。

○ 中国工業情報化部は、Alibaba Cloud が、Apache Log4j に対する脆弱性の報告を行わなかったことに対し、ネットワークセキュリティ脅威及び脆弱性情報共有プラットフォームの参加資格を 6 か月停止[16]。

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 米国国防総省におけるサプライチェーン関する取組:CMMC2.0

○ 2021 年 11 月 4 日、米国国防総省(DoD)は、調達先に求めるサイバーセキュ

---

[11] 中华人民共和国中央人民政府「中共中央关于党的百年奋斗重大成就和历史经验的决议(全文)(2021/11/16)」、http://www.gov.cn/zhengce/2021-11/16/content_5651269.htm (2021/11/17 閲覧)

[12] NHK「中国共産党「歴史決議」意義を強調 習主席 3 期目目指す布石か(2021/11/12)」、https://www3.nhk.or.jp/news/html/20211112/k10013345871000.html (2022/2/12 閲覧)

[13] 中国商務部「商务部关于印发《"十四五"商务发展规划》的通知(2021/7/8)」、http://www.mofcom.gov.cn/article/zwgk/gztz/202107/20210703174101.shtml (2021/12/15 閲覧)

[14] 中国商務部「商务部关于印发《"十四五"利用外资发展规划》的通知(2021/10/22)」、http://www.mofcom.gov.cn/article/ghjh/202110/20211003210174.shtml (2021/12/15 閲覧)

[15] Reuters「Olympics-China's Games app has security flaws, researchers say(2022/1/19)」、https://jp.reuters.com/article/us-olympics-2022-app-idCAKBN2JS1JR (2022/1/28 閲覧)

[16] 壹讀「羅 Sir 說—合規 | 安全漏洞砸中, 阿里雲再遭點名(2021/12/24)」、https://read01.com/B22E66B.html#.YeTyNP7P2Ul (2022/1/17 閲覧)

リティの取組に関する規則「CMMC 2.0」を発表[17]。

- ○ CMMC とは、サプライチェーンにおけるセキュリティ強化を目的とした認証制度のことで、調達先における保護が必要となる管理すべき重要情報（CUI: Controlled Unclassified Information）の保護に重きを置いたもの。
- ○ CMMC2.0 では、CMMC1.0（2020 年 11 月発効）の課題を改善し、レベル区分をこれまでの 5 階層から 3 階層に簡素化し、一部のレベルではセルフアセスメントを可能にするなど、より現実的なアプローチを採用。

2.1.2 サイバーレジリエントシステムの開発:システムセキュリティエンジニアリングアプローチの改訂版(SP800-160 Vol.2 Rev.1)の改訂

- ○ 米国国立標準技術研究所（NIST）は、2021 年 12 月、「サイバーレジリエントシステムの開発:システムセキュリティエンジニアリングアプローチ」の改訂版(NIST SP800-160 Vol.2 Rev.1)を公開[18]。
- ○ SP800-160 Vol.2 Rev.1 でサイバーレジリエンスとは、システムが、負荷、攻撃、侵害などの不利な条件下において、状況を予期、耐性、回復、適応するための能力(強靭性)を持つことと定義。
- ○ 改訂は、サイバーレジリエンスエンジニアリングのためのフレームワークとその使用概念及びシステムライフサイクルにおけるサイバーレジリエンスの実装のための考慮事項を提示。

2.2. その他

2.2.1 攻撃グループ NOBELIUM によるクラウドサービスプロバイダ等を介したサイバー攻撃

- ○ 2021 年 10 月 24 日、Microsoft は、攻撃グループ NOBELIUM によるクラウドサービスプロバイダ等を介した標的型攻撃について発表[19]。
- ○ NOBELIUM は、ロシア由来の攻撃グループとしており、2020 年の SolarWinds や 2021 年 5 月の欧米の政府機関等への攻撃に関与が疑われているとのこと。
- ○ この攻撃に対する対策として、多要素認証の有効化、ログの確認、不要な管

---

[17] *米国国防総省「Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program(2021/11/4)」、https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/ (2022/3/2 閲覧)*

[18] *NIST「SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach(2021/12)」、https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final (2022/3/2 閲覧)*

[19] *Microsoft「New activity from Russian actor Nobelium(2021/10/24)」、https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/ (2022/3/2 閲覧)*

理者権限の削除など、いくつかの具体的な推奨事項を指示[20]。

2.2.2 マルウエア「Emotet」の活動再開

- ○ 2021 年 11 月、マルウエア「Emotet」に関する攻撃活動が再開され、複数の組織が Emotet の感染拡大を試みる不正なメールを確認[21]。
- ○ 攻撃者は、従来の攻撃手法に加え、メールで URL リンクにアクセスさせオンラインストレージ上の PDF ファイルを参照するために、URL 先で Adobe 製ソフトウエアを装った不正な Windows アプリをインストールするよう促して感染を拡大[22]。
- ○ 組織による効果的な対策を講じることに加え、メールの添付ファイルのマクロ有効化や、URL 先でのソフトウエアのインストールを安易に実施しないよう個人が意識することが重要[23]。

2.2.3 ロギングライブラリ「Log4j」の脆弱性

- ○ 2021 年 12 月、Java アプリケーションに広く使われているロギングライブラリ「Log4j」の脆弱性が公開され、世界中の組織が対応[24]。
- ○ 修正パッチリリース後に新たな脆弱性がみつかり、2021 年の年末にかけて緊急対応が継続[25]。
- ○ 侵害等の被害報告は少ないが、継続的な警戒が必要[26]。

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 NTT ドコモにおける大規模な通信障害とサービスへの影響

- ○ 2021 年 10 月 14 日午後 5 時頃から 15 日午後 10 時まで、NTT ドコモの通信回線で障害が発生し、音声通話・データ通信サービスが利用しづらい状況が

---

[20] *Microsoft「New activity from Russian actor Nobelium(2021/10/24)」、https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/（2022/3/2 閲覧）*

[21] *JPCERT/CC「マルウェア Emotet の感染拡大に関する注意喚起(2022/2/10)」、https://www.jpcert.or.jp/at/2022/at220006.html（2022/3/1 閲覧）*

[22] *IPA「「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて 攻撃活動再開後の状況／被害相談の例(2021/12/9)」、https://www.ipa.go.jp/security/announce/20191202.html#L17（2022/3/1 閲覧）*

[23] *JPCERT/CC「マルウェア Emotet の感染に関する注意喚起(2019/11/27)」、https://www.jpcert.or.jp/at/2019/at190044.html（2022/3/1 閲覧）*

[24] *JPCERT/CC「Apache Log4j の任意のコード実行の脆弱性(CVE-2021-44228)に関する注意喚起(2021/12/11)」、https://www.jpcert.or.jp/at/2021/at210050.html（2022/3/1 閲覧）*

[25] *JPCERT/CC「2021 年 12 月に公表された Log4j の脆弱性について(2021/12/24)」、https://www.jpcert.or.jp/newsflash/2021122401.html（2022/3/1）*

[26] *警察庁「Java ライブラリ「Apache Log4j」の脆弱性(CVE-2021-44228)を標的とした攻撃の観測について(2021/12/14)」、https://www.npa.go.jp/cyberpolice/important/2021/202112141.html（2022/3/1 閲覧）*

継続、音声通話約 460 万人、データ通信 830 万人以上に影響[27]。

- ○ ネットワーク工事の切り戻しに伴う IoT 機器の位置登録信号の増大によるネットワーク輻輳が原因[28]。
- ○ NTT ドコモ、ahamo、NTT ドコモ回線を利用する仮想移動体通信事業者(MVNO)、タクシーや郵便局におけるクレジットカードでの支払い等に影響[29]。
- ○ 総務省は、2021 年 10 月 19 日、この大規模な通信障害を電気通信事業法の定める「重大な事故」に当たると判断し、11 月 26 日、行政指導を実施[30]。

3.1.2 医療機関のサイバー攻撃被害

- ○ 2021 年 10 月 31 日、徳島県つるぎ町立半田病院において、サイバー攻撃により、救急や新規患者の受入れ中止する等の被害[31]。
- ○ 医療機関へのサイバー攻撃被害は、増加傾向、データのバックアップやセキュリティアップデート等の情報セキュリティ対策を確実に実施[32]。

3.1.3 サプライチェーンリスクが顕在化した事例

- ○ 2021 年 12 月 2 日、スマートフォン決済「楽天ペイ」において、楽天銀行との連携に不具合で、口座から引き落としがされたが、決済やチャージができなかった障害[33]。
- ○ 2021 年 12 月 22 日、AWS の北バージニアリージョンの電力消失により、複数の Web サービスで障害が発生[34]。
- ○ 複数自治体で外部委託事業者の計算システムの算出誤りが原因で国民健康保険料に誤りが発生[35]。

---

[27] *NTTドコモ「重要なお知らせ(通信障害等):【お詫び/回復】音声通話・データ通信サービスがご利用しづらい事象について(2021/10/14)」、https://www.nttdocomo.co.jp/info/network/kanto/pages/211014_00_m.html (2021/11/15 閲覧)*

[28] *NTTドコモ「通信障害の対応状況に関する説明会(2021/11/10)」、http://ngt.idc.nttdocomo.co.jp/20211110_10.pdf (2021/11/15 閲覧)*

[29] *朝日新聞「「届け先がわからない!」ドコモ通信障害にウーバー配達員も悲鳴(2021/10/15)」、https://www.asahi.com/articles/ASPBH6DRRPBHULFA00K.html (2021/11/15 閲覧)*

[30] *総務省「株式会社 NTTドコモに対する電気通信事故に関する適切な対応について(指導)(2021/11/26)」、https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000233.html (2021/11/28 閲覧)*

[31] *日経新聞「ランサム攻撃でカルテ暗号化 徳島の病院、インフラ打撃(2021/11/12)」、https://www.nikkei.com/article/DGXZQOUE071OK0X01C21A1000000/ (2021/12/2 閲覧)*

[32] *厚生労働省「医療情報システムの安全管理に関するガイドライン改定について(2021/12/17)」、https://www.mhlw.go.jp/content/10808000/000868532.pdf (2022/2/3 閲覧)*

[33] *産経新聞「楽天ペイ、決済エラーでも引き落とし 銀行システム障害(2021/12/3)」、https://www.sankei.com/article/20211203-JYMK5JPIZBLJ7LOIN7SDYBXIE4/ (2022/1/6 閲覧)*

[34] *ITmedia「AWS で一時障害、原因はデータセンターの電力消失 Slack や Trello にも影響か(2021/12/23)」、https://www.itmedia.co.jp/news/articles/2112/23/news076.html (2022/1/6 閲覧)*

[35] *Densan「当社提供システムの不具合発生に関するお詫び(2021/12/2)」、https://www.ndensan.co.jp/informatio*

3.2. その他

3.2.1 ニップングループへのサイバー攻撃

- ○ 2021 年 7 月 7 日未明から、株式会社ニップンがサイバー攻撃により、販売管理や財務会計などの基幹業務のグループシステムで大規模なシステム障害が発生[36]。
- ○ 同社グループの情報ネットワーク上の大半のサーバーが同時に暗号化、本社や全事業拠点とバックアップが被害に遭い、災害を想定したシステム障害の事業継続計画(BCP)想定を大きく上回る約 9 割のシステムに影響[37]。
- ○ ニップンでは、システム障害の早期復旧が見込めず影響が長期化することから、企業内容等の開示に関する内閣府令第 17 条の 15 の 2 第 1 項に規定された第 1 四半期、第 2 四半期、第 3 四半期の報告書の提出期限を延長[38]。

4. 重要インフラの次期行動計画改定への方向性の提言

- ○ 2021 年 10 月 25 日、重要インフラ専門調査会において、第 4 次行動計画における有効な取組は継続しつつ、障害対応体制強化の在り方を抜本的な見直すこと、将来の環境変化を先取りしサプライチェーン等を含め包括的な対応することを柱とする政策部会からの提言を了承[39]

以上

---

n/1503.html（2022/1/20 閲覧）

[36] *ニップン「システム障害発生のお知らせ(続報)(2021/8/16)」、https://www.nippn.co.jp/topics/detail/_icsFiles/afieldfile/2021/08/16/20210816.pdf（2021/12/7 閲覧）*

[37] *ニップン「2022 年 3 月期第 1 四半期報告書の提出期限延長に関する承認申請書提出のお知らせ(2021/8/16)」、https://www.nippn.co.jp/topics/detail/_icsFiles/afieldfile/2021/08/16/20210816-1.pdf（2021/12/7 閲覧）*

[38] *ニップン「2022 年 3 月期第 3 四半期報告書の提出期限延長に関する承認申請書承認のお知らせ(2022/2/14)」、https://www.nippn.co.jp/topics/detail/_icsFiles/afieldfile/2022/02/14/20220214-2.pdf（2022/2/28 閲覧）*

[39] *重要インフラ専門調査会第 26 会合資料 5「重要インフラ行動計画改定への提言(2021/10/25)」https://www.nisc.go.jp/conference/cs/ciip/dai26/pdf/26shiryou05.pdf(2022/2/11 閲覧）*