資料２

令和 4 年 1 月 26 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(2021 年度第 2 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 2 四半期(7 月～9 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 半導体サプライチェーンめぐる動向

○ 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 重要インフラサイバーセキュリティへの取組

○ 2021 年 7 月 28 日、バイデン大統領は、重要インフラ制御システム(ICS)のサイバーセキュリティの改善に関する国家安全保障覚書 5(NSM-5)を発行し、「重要インフラ制御システム(ICS)に対するサイバーセキュリティ行動計画」の推進及び重要インフラセキュリティ目標の策定を要求[3]。

---

[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] *THE WHITE HOUSE「National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems(2021/7/28)」、https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (2021/8/13 閲覧)*

○ 2021 年 9 月 21 日、米国サイバーセキュリティ・インフラセキュリティ庁(CISA)と米国標準技術研究所(NIST)は、「重要インフラの制御システムのサイバーセキュリティパフォーマンスの目標と目的」の文書を公表[4]。

○ 2021 年 9 月 21 日、NIST は、米国エネルギー省(DOE)以外による重要インフラ分野のサイバーセキュリティへの取組として、分散エネルギー(DER)をサイバー脅威から保護する方法に関する SP1800-32「産業用 IoT の安全性確保、分散型エネルギー源のサイバーセキュリティ(草案)」を発表等[5]。

1.2.2 サイバーセキュリティに係る官民連携の取組

○ 2021 年 8 月 5 日、米国 CISA は、官民が連携し、重要インフラ等をサイバーセキュリティ上の脅威から防護するための国家のサイバー防衛計画の策定を主導することを目的として、「Joint Cyber Defense Collaborative(JCDC)」の設立を発表し、国家の強靭性を促進[6]。

○ 2021 年 8 月 25 日、バイデン大統領は、民間企業や教育機関等のリーダーとの会合で、米国の重要インフラ等のサイバーセキュリティの改善を支援するよう要請し、出席者は、バイデン政権のサイバーセキュリティ体制を強化する取組を発展させる新たな取組を発表[7]。

1.2.3 インド太平洋地域における新たな枠組

○ 2021 年 9 月 24 日、日米豪印によるインド太平洋地域の安全保障や経済問題を協議する戦略的枠組「Quad(クアッド)」の首脳会談を開催し、対中国を念頭に置いた議題で、サプライチェーン問題からサイバーセキュリティや宇宙などに至るまでを議論[8]。

○ 2021 年 9 月 15 日、米英豪によるインド太平洋の安全と安定の維持を目的とした軍事的枠組「AUKUS(オーカス)」を発表し、オーストラリアへの原子力潜水艦に関連した取引、サイバーセキュリティや人工知能(AI)の分野の協力推進、産業基盤とサプライチェーン統合強化を推進[9]。

---

[4] *CISA「CRITICAL INFRASTRUCTURE CONTROL SYSTEMS CYBERSECURITY PERFORMANCE GOALS AND OBJECTIVES(2021/9/21)」、https://www.cisa.gov/control-systems-goals-and-objectives (2021/9/27 閲覧)*

[5] *NCCoE「Securing the Industrial Internet of Things」、https://www.nccoe.nist.gov/projects/use-cases/energy-sector/iiot (2021/11/2 閲覧)*

[6] *CISA「JOINT CYBER DEFENSE COLLABORATIVE」、https://www.cisa.gov/jcdc (2021/9/7 閲覧)*

[7] *THE WHITE HOUSE「FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity(2021/8/25)」、https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/ (2021/9/6 閲覧)*

[8] *外務省「Joint Statement from Quad Leaders(2021/9/24)」、https://www.mofa.go.jp/mofaj/files/100238179.pdf (2021/10/15 閲覧)*

[9] *THE WHITE HOUSE「Joint Leaders Statement on AUKUS(2021/9/15)」、https://www.whitehouse.gov/briefin*

1.3. 中国

1.3.1 中国共産党創立 100 周年祝賀大会

○ 中国共産党は、2021 年 7 月 1 日、創立 100 周年を記念する祝賀大会を開催し、習近平総書記が、百年目標について、ややゆとりのある社会に対して歴史的な絶対的貧困問題を解決、近代的社会主義強国に対して、全面完成に向けてまい進していると演説[10]。

1.3.2 APT40 に関する声明文

○ 英国、米国等は、2021 年 7 月 19 日、中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等に関して声明文を公表。これに対し、日本は強く支持する一方、中国は強く反論[11]。

1.3.3 中国のサイバーセキュリティに関する規定整備の動向

○ 2021 年 7 月 12 日、ネットワーク製品のセキュリティ脆弱性管理に関する規定を、2021 年 8 月 20 日、個人情報保護法を整備[12]。

○ 2021 年 8 月 17 日、通信など重要情報インフラ施設のデータ保護を目的とした「重要情報インフラ施設安全保護条例」を 2021 年 9 月 1 日施行と発表[13]。

1.3.4 デジタル人民元、暗号資産

○ 中国人民銀行は、2021 年 7 月 16 日、ホワイトペーパー「中国におけるデジタル人民元の研究開発の進展」を公表[14]。

○ 中国では、2021 年 9 月 24 日、暗号資産関連事業を全面禁止する旨公表、デジタル人民元正式導入に向けた準備が着々と進行[15]。

---

g-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/（2021/10/19 日閲覧）

[10] 駐日中国大使館「中国共産党創立100周年祝賀大会における 習近平総書記の演説全文(2021/7/2)」、http://www.china-embassy.or.jp/jpn/zt/zggcdcl100zn/t1889124.htm（2021/8/24 閲覧）

[11] 内閣サイバーセキュリティセンター「中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について(注意喚起)(2021/7/19)」、https://www.nisc.go.jp/press/pdf/20210719NISC_press.pdf（2021/8/24 閲覧）

[12] 中国全国人民代表大会「中华人民共和国个人信息保护法(2021/8/20)」、http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml（2021/8/24 閲覧）

[13] 中華人民共和国「关键信息基础设施安全保护条例(2021/8/17)」、http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm（2021/9/25 閲覧）

[14] 中国人民銀行「Progress of Research & Development of E-CNY in China(2021/7/16)」、http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/index.html（2021/20/20 閲覧）

[15] 中国人民銀行「关于进一步防范和处置虚拟货币交易炒作风险的通知(2021/9/15)」、http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4348521/index.html（2021/10/20 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 Kaseya の「VSA」の利用組織に対するランサムウエア攻撃

- 2021 年 7 月 2 日、米国の IT 企業 Kaseya は、同社の IT 管理ソフトウエア「VSA」に対するサイバー攻撃を公表、全ての顧客に VSA サーバーをシャットダウンするよう通知[16]。
- VSA を利用した IT 資産のリモート監視サービスを提供するマネージドサービスプロバイダ(MSP)が、サイバー攻撃を受け、MSP の顧客の PC が REvil に感染、データが暗号化される等の被害が発生[17]。
- 2021 年 7 月 22 日、Kaseya は復号鍵を入手、影響を受けた顧客にツールとして提供し、データの復元を支援すると発表[18]。

2.2. その他

2.2.1 Windows に関する深刻な脆弱性の相次ぐ公開

- Microsoft は、2021 年 6 月以降、Windows Print Spooler に関する複数の脆弱性(CVE-2021-1675、CVE-2021-34527 等)を公表、一部の脆弱性は、セキュリティ研究者が脆弱性の実証コード(PoC コード)を公開[19]。
- Microsoft は、2021 年 7 月 21 日に Windows の特権昇格の脆弱性(CVE-2021-36934)、2021 年 7 月 23 日に Windows LSA におけるなりすましの脆弱性(CVE-2021-36942)を公表、迅速なパッチ適用等の適切な対応策の実施が必要[20]。
- Microsoft は、2021 年 9 月 8 日に Microsoft MSHTML のリモートでコードが実行される脆弱性(CVE-2021-40444)の悪用が確認されているとして、脆弱性の緩和策及び回避策を公表、2021 年 9 月 15 日にセキュリティ更新プログラムを公開[21]。

---

[16] *Kaseya「Kaseya Responds Swiftly to Sophisticated Cyberattack, Mitigating Global Disruption to Customers(2021/7/6)」、https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/（2021/7/28 閲覧）*

[17] *ZDNet Japan「ランサムウェア攻撃を受けた Kaseya、脆弱性を修正した「VSA」のアップデートをリリース」、https://japan.zdnet.com/article/35173796/（2022/1/4 閲覧）*

[18] *Kaseya「Updates Regarding VSA Security Incident(2021/7/26)」、https://www.kaseya.com/potential-attack-on-kaseya-vsa/（2021/7/28 閲覧）*

[19] *JPCERT/CC「Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起(2021/7/5)」、https://www.jpcert.or.jp/at/2021/at210029.html（2022/1/4 閲覧）*

[20] *JPCERT/CC「2021 年 8 月マイクロソフトセキュリティ更新プログラムに関する注意喚起(2021/8/11)」、https://www.jpcert.or.jp/at/2021/at210034.html（2022/1/4 閲覧）*

[21] *IPA「Microsoft Windows 製品の Microsoft MSHTML の脆弱性対策について(CVE-2021-40444)(2021/9/8)」、https://www.ipa.go.jp/security/ciadr/vul/20210908-ms.html（2022/1/4 閲覧）*

2.2.2 Microsoft Exchange Server の深刻な脆弱性「ProxyShell」

- 2021 年 8 月 5 日、セキュリティカンファレンス「Black Hat USA 2021」で、Microsoft Exchange Server の深刻な脆弱性(CVE-2021-31207、CVE-2021-34473、CVE-2021-34523)[通称:ProxyShell]の技術的詳細が発表 [22]。
- Microsoft や CISA は、これらの脆弱性の組合せにより、リモートから任意のコード実行が可能となることから、セキュリティ更新プログラムの適用を呼びかけ [23]。
- Microsoft は、2021 年 9 月 8 日に Microsoft MSHTML のリモートでコードが実行される脆弱性(CVE-2021-40444)の悪用が確認されているとして、脆弱性の緩和策及び回避策を公表、2021 年 9 月 15 日にセキュリティ更新プログラムを公開 [24]。

2.2.3 IoT 機器のセキュリティに関する動向

- 2021 年 5 月、日本発の IoT 製品・システムを安全に実装するための国際規格、「ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes」が国際標準規格として成立 [25]。
- この ISO/IEC 30147:2021 は、NISC による「安全な IoT システムのためのセキュリティに関する一般的枠組み」を基にしたもの [26]。
- 米国 NIST は、IoT システムのセキュリティに関する文書、「SP 800-213 連邦政府向け IoT デバイスサイバーセキュリティ要件の確立」、「SP 800-213A 連邦政府向け IoT デバイスサイバーセキュリティガイダンス:IoT デバイスサイバーセキュリティ要件のカタログ」のほか、2つの関連文書(NISTIR 8259B、8259C)を公表 [27]。

---

[22] *Sophos「Microsoft Exchange における ProxyShell の脆弱性と対策(2021/9/6)」、https://news.sophos.com/ja-jp/2021/09/06/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do-jp/ (2022/1/4 閲覧)*

[23] *CISA「Urgent: Protect Against Active Exploitation of ProxyShell Vulnerabilities(2021/8/21)」、https://us-cert.cisa.gov/ncas/current-activity/2021/08/21/urgent-protect-against-active-exploitation-proxyshell (2021/9/1 閲覧)*

[24] *IPA「Microsoft Windows 製品の Microsoft MSHTML の脆弱性対策について(CVE-2021-40444)(2021/9/8)」、https://www.ipa.go.jp/security/ciadr/vul/20210908-ms.html (2022/1/4 閲覧)*

[25] *IEC「ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes(2021/5/28)」、https://webstore.iec.ch/publication/62644 (2022/1/12 閲覧)*

[26] *内閣サイバーセキュリティセンター「安全な IoT システムのためのセキュリティに関する一般的枠組(2016/8/26)」、https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf (2022/1/12 閲覧)*

[27] *NIST「SP800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements(2020/12/15)」、https://csrc.nist.gov/publications/detail/sp/800-213/final (2022/1/12 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. 重要インフラ関連

3.1.1 みずほ銀行の相次ぐシステム障害

- ○ みずほ銀行では、これまで 2002 年 4 月及び 2011 年 3 月に、大きなシステム障害が発生[28]。
- ○ 2021 年 2 月以降 9 月まで、8 回のシステム障害が相次いで発生[29]。
- ○ 金融庁は、一連のシステム障害を受け、業務改善命令を発出[30]。

3.1.2 ランサムウエア「LockBit2.0」等によるサイバー攻撃の増加

- ○ 2021 年 5 月以降、複数の Ransomware as a Service(RaaS)が相次いで活動を停止、その後、RaaS のブランド名を変更(リブランド)するなどして活動を再開[31]。
- ○ ランサムウエア「LockBit2.0」について、2021 年 6 月頃から活動が確認され、2021 年 7 月以降、攻撃が急増、日本企業やその海外子会社でも被害を多数確認[32]。
- ○ 全国の自治体から公共事業の施工管理などを請け負っている建設コンサルタント会社が LockBit2.0 のサイバー攻撃を受け、業務の関連データが流出したおそれがあると報道[33]。

3.2. その他

3.2.1 東京 2020 オリンピック・パラリンピック競技大会に係るサイバー関連事象

- ○ 過去の大会では、特に開会式がサイバー攻撃の標的になったことを踏まえ、東京 2020 大会では、NISC は、関連企業など 350 組織での情報共有態勢を整えるなど各組織がサイバー攻撃へ備えた取組を実施[34]。

---

[28] *みずほフィナンシャルグループ「システム障害特別調査委員会の調査報告書の受領について(2021/6/15)」、https://www.mizuho-fg.co.jp/release/20210615release_jp.html（2021/9/22 閲覧）*

[29] *日経 xTECH「業務改善命令からわずか 8 日後、「8 度目」障害で不透明さ増すみずほ銀行の当面の課題(2021/10/6)」、https://xtech.nikkei.com/atcl/nxt/column/18/00001/06112/（2021/11/1 閲覧）*

[30] *金融庁「みずほ銀行及びみずほフィナンシャルグループに対する行政処分について(2021/9/22)」、https://www.fsa.go.jp/news/r3/ginkou/20210922.html（2021/9/22 閲覧）*

[31] *RecordedFuture「Darkside ransomware gang says it lost control of its servers & money a day after Biden threat(2021/5/14)」、https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/（2021/9/14 閲覧）*

[32] *トレンドマイクロ「「LockBit 2.0」のランサムウェア攻撃が拡大中。日本にも被害を及ぼす攻撃活動を解説(2021/8/25)」、https://blog.trendmicro.co.jp/archives/28572（2021/9/7 閲覧）*

[33] *NHK「建設コンサルタントにサイバー攻撃 公共事業データ盗まれたか(2021/8/24)」、https://www3.nhk.or.jp/news/html/20210824/k10013219561000.html（2021/9/6 閲覧）*

[34] *産経新聞「サイバー攻撃情報を350組織で共有 東京五輪・パラへ態勢強化(2021/7/7)」、https://www.sankei.com/article/20210707-NTDMIID54FLQDHKFJBYZHFA64A/（2021/8/23 閲覧）*

○ 2019 年秋頃から、ロシア政府の支援を受ける攻撃グループ等による、世界ドーピング防止機関や東京 2020 大会の関連組織等に対するサイバー攻撃を確認[35]。

○ 2020 年 4 月下旬、日本オリンピック委員会(JOC)事務局がランサムウエア攻撃を受け、感染した可能性のある PC、サーバー等の 7 割を交換、内部情報の流出の痕跡はなかったとして、被害を不公表[36]。

○ 組織委員会の Web サイトが、2021 年 7 月 23 日深夜、DNS の障害やオフィシャルオンラインショップにアクセス集中等で一時閲覧不能、7 月 28 日 20 時半頃、東京電力中東京変電所への落雷の影響で埼玉県川越市のゴルフ競技会場が停電等の事象が発生したが、大会運営・競技運営に影響を与えるようなインシデントは不発生[37]。

以上

---

[35] *Microsoft「New cyberattacks targeting sporting and anti-doping organizations(2021/10/28)」、https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/（2021/8/17 閲覧）*

[36] *NHK「JOC サイバー攻撃受けるも公表せず 去年 4 月 一時業務できず(2021/6/25)」、https://www3.nhk.or.jp/news/html/20210625/k10013103001000.html（2021/8/16 閲覧）*

[37] *NTT「東京 2020 オリンピック・パラリンピック競技大会における NTT の貢献 ～通信サービス with サイバーセキュリティの観点から～(2021/10/21)」、https://group.ntt/jp/newsrelease/2021/10/21/211021a.html（2021/11/1 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 3 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	2Q	3Q	4Q	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	95	－	283
関係省庁・関係機関からのNISCへの情報共有	19	7	16	16	4	1	1	－	6
NISCからの情報提供	54	43	38	64	17	24	28	－	69

（※）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	2Q	3Q	4Q	計
未発生の事象		予兆・ヒヤリハット	80	27	12	28	5	2	4	－	11
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	2	－	18
	完全性を脅かす事象	情報の破壊	20	17	11	12	4	7	5	－	16
	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	41	－	144
	上記につながる事象	マルウェア等の感染	65	17	9	18	6	7	4	－	17
		不正コード等の実行	13	4	5	3	0	0	2	－	2
		システム等への侵入	17	14	14	26	5	8	7	－	20
		その他	35	34	47	42	16	9	30	－	55

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	2Q	3Q	4Q	計
意図的な原因	不審メール等の受信	89	36	13	9	3	0	4	－	7
	ユーザＩＤ等の偽り	4	3	12	9	3	0	2	－	5
	DDoS攻撃等の大量アクセス	31	17	20	10	3	4	1	－	8
	情報の不正取得	16	10	8	13	5	0	3	－	8
	内部不正	4	1	0	0	0	1	0	－	1
	適切なシステム等運用の未実施	15	14	11	23	4	3	3	－	10
偶発的な原因	ユーザの操作ミス	23	10	6	18	5	1	1	－	7
	ユーザの管理ミス	13	6	6	13	5	2	2	－	9
	不審なファイルの実行	42	16	7	7	1	0	3	－	4
	不審なサイトの閲覧	20	4	5	3	2	0	0	－	2
	外部委託先の管理ミス	41	29	39	56	25	29	31	－	85
	機器等の故障	32	27	62	39	11	6	15	－	32
	システムの脆弱性	36	19	16	38	5	7	16	－	28
	他分野の障害からの波及	10	6	4	7	4	2	3	－	9
環境的な原因	災害や疾病等	0	1	13	9	0	3	0	－	3
その他の原因	その他	29	29	33	35	21	4	13	－	38
	不明	57	46	53	68	23	25	10	－	58

（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 3 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ものの、サイバー攻撃によりサービス提供に重大な影響が及ぶものが目立つ傾向にあった。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)。

○　脆弱性対応を含めた資産管理の厳格化が必要

CMS(Contents Management System)などの脆弱性への対応遅れにより不正アクセスを外部から受け、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。

○　情報公開手段の多様化が必要

ウェブサイトが改ざんされ、ウェブサービスを提供できなくなったほか、ウェブサイトを通じた情報発信ができなくなった事例があった。

○　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。

○　広報対応を含めた障害発生を想定した事前準備が必要

システムに不具合が発生した際、システムの特性を踏まえた復旧手順の認識不足により、長時間にわたりサービスが提供できなかったほか、利用者に対する適時・適格な情報発信の欠如により、障害に係る情報が錯そうした事例があった。

○　特殊ケースにおける例外措置の認識と確認が必要

年末年始の特殊ケースにおける例外措置に対する対応漏れにより、システムに不具合が発生し、サービスが提供できなかった事例があった。

以上