資料２

令和 5 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 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、2022 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 サイバーセキュリティパフォーマンス目標(CPGs)

- ○ 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、2022 年 10 月 25 日、全ての重要インフラ分野に適用可能なサイバーセキュリティパフォーマンス目標(CPGs)を発表[1]。
- ○ 同目標は、サイバーセキュリティ対策の全てを網羅したものではなく、重要インフラ事業者が実施すべき最低限のものを経営層にも理解し易いように明確に記載。
- ○ 国立標準技術研究所(NIST)のサイバーセキュリティフレームワーク(CSF)とも整合しており、小規模またはセキュリティ対策の成熟度の低い組織が、セキュリティ投資の優先順位付けが可能。

1.1.2 HPH セクターを標的とする攻撃グループ「Daixin Team」

- ○ 2022 年 10 月 26 日、CISA が、ヘルスケア及び公衆衛生(HPH)セクターを標的にした攻撃として、2022 年 7 月の Maui Ransomware に続き、「Daixin Team」に関する注意喚起を実施[2]。
- ○ 「Daixin Team」は、ランサムウエアを展開するだけでなく被害組織のシステム

---

[1] *CISA「Cross-Sector Baseline Cybersecurity Performance Goals (CPGs)(2022/10/27)」、https://www.cybercoop.com/cisa-performance-goals-operational-technology/ (2022/11/22 閲覧)*

[2] *Cybersecurity and Infrastructure Security Agency「Alert (AA22-294A) #StopRansomware: Daixin Team (2022/10/26)」、https://www.cisa.gov/uscert/ncas/alerts/aa22-294a (2022/10/18 閲覧)*

からデータを窃取し、二重恐喝脅威型のランサムウエア攻撃を実施。

- FBI、CISA 及び米国保健福祉省(HHS)は、HPH 分野の組織に対し、「Daixin Team」の攻撃から保護するため、推奨される緩和策、ランサムウエア攻撃に対する準備、ランサムウエア被害の軽減及び防止策、ランサムウエア被害発生時の推奨する対応について、それぞれ具体的な対策を公表。

1.1.3 CISA が脆弱性管理手法「SSVC」のガイドラインを公開

- 2022 年 11 月 10 日、CISA がステークホルダー別脆弱性分類「SSVC(Stakeholer-Specific Vulnerability Categorization)」のガイドラインを公表[3]。
- ガイドラインでは、「脆弱性の悪用状況」、「技術的な影響」、「攻撃の自動化可否」、「業務に不可欠な機能への影響」、「公共の福祉への影響」の各判断ポイントについて、予め定義された値を選択し、当該脆弱性への対応の優先度を決定する方法を記載。
- CISA では、米国政府機関及び重要インフラ事業者における脆弱性悪用の影響を 3 段階(「High」、「Medium」、「Low」)で評価した上で、独自に定義した決定木を用いて脆弱性に対する優先度を決定。

1.1.4 米国における TikTok 使用禁止等の動き

- 2023 年 12 月、米国各州において、ショートビデオ共有アプリ「TikTok」の利用を規制する動きが活発化[4]。
- サウスダコタ州では、州政府職員や請負業者を対象に、州政府の機器での使用を禁止する知事令(2022 年 11 月 29 日)。
- サウスカロライナ州では、州政府の担当部局が管理する全ての電子機器によるアクセスを禁止要請(2022 年 12 月 5 日)。
- メリーランド州では、中国やロシアの特定企業の製品とプラットフォームを州政府機関での使用を禁止する緊急命令(2022 年 12 月 6 日)。
- テキサス州では、州政府が支給する機器での利用の禁止、個人端末で利用する場合の脆弱性対処の計画策定を指示(2022 年 12 月 7 日)。

1.2. 中国

1.2.1 ネットワーク製品のセキュリティ脆弱性収集プラットフォームの届出管理弁

---

[3] *Cybersecurity and Infrastructure Security Agency「Stakeholer-Specific Vulnerability Categorization Guide (2022/11/10)」、https://www.cisa.gov/sites/default/files/publications/cisa-ssvx-guide%20508c.pdf (2022/12/6 閲覧)*

[4] *JETRO「米州政府で TikTok 使用禁止相次ぐ、メリーランドなど(2022/12/12)」、https://www.jetro.go.jp/biznews/2022/12/4a69e32190c70ef6.html (2023/3/8 閲覧)*

法

- ○ 2022 年 10 月 28 日、中国工業情報化部は「ネットワーク製品のセキュリティ脆弱性収集プラットフォームの届出管理弁法」を発表。弁法は 2023 年 1 月 1 日から施行。
- ○ 2021 年 7 月に、ネットワーク製品の脆弱性の発見・報告・修正・公表等の行為を規範化し、リスクを予防するため、「ネットワーク製品のセキュリティ脆弱性管理規定」を発表。
- ○ 同規定では、組織・個人が設立したネットワーク製品セキュリティ脆弱性収集プラットフォームは政府に届出を行なう旨を定めており、今回の弁法は、脆弱性収集プラットフォームの届出方式や報告内容などを規定[5]。

1.2.2 中華人民共和国反間諜法

- ○ 2022 年 12 月 30 日、全国人民代表大会(全人代)常務委員会において、中華人民共和国反間諜法(いわゆる「反スパイ法」)の改正案が審議[6]。
- ○ 2014 年施行以来初めての改正となり、改正案では、国家安全や利益にかかわる文書、データ、資料、物品をこっそり探ったり、提供したりする行動を「スパイ行為」と規定。
- ○ 重要インフラのサイバーセキュリティにかかる脆弱性を外部に漏らす行為も取り締まりの対象[7]。

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 ドイツの鉄道会社における通信システムトラブル

- ○ 2022 年 10 月 8 日、ドイツ北部で、通信システムの障害で列車の運行がおよそ 3 時間にわたり止まるなど、鉄道網で大規模な混乱が発生。
- ○ 鉄道会社及び政府は通信ケーブルへの破壊工作が原因とみており、警察当局が犯罪捜査に着手。
- ○ 列車の運行に必要な通信システムで障害が発生。運輸・デジタル相は、通信ケーブルが 2 カ所の異なる地点で故意に切断されたとして、破壊工作だった可能性を示唆[8]。

---

[5] *JETRO「「ネットワーク製品のセキュリティー脆弱性収集プラットフォームの届け出管理弁法」を発表(2022/11/17)」、https://www.jetro.go.jp/biznews/2022/11/4a7b08f2b2c19533.html（2023/3/8 閲覧）*

[6] *朝日「中国で新たな「スパイ行為」定義へ　サイバーの欠陥情報漏洩など(2022/12/30)」、https://www.asahi.com/articles/ASQDZ6QB6QDZUHBI00Q.html（2023/2/27 閲覧）*

[7] *日経「中国、スパイ行為の対象拡大　資料やデータに幅広く網(2023/1/3)」、https://www.nikkei.com/article/DGXZQOGM044Y80U3A100C2000000/（2023/2/27 閲覧）*

[8] *日経「ドイツ鉄道で「破壊工作」か　通信障害で一時運休(2022/10/9)」、https://www.nikkei.com/article/DGXZQOGR091O80Z01C22A0000000/（2023/2/28 閲覧）*

2.1.2 オーストラリアの民間医療保険大手メディバンクにサイバー攻撃

- 2022 年 10 月 13 日、オーストラリアの民間医療保険大手のメディバンクは、システムに異常なアクティビティを検知。攻撃者から顧客データの取引について身代金交渉を希望する連絡。
- 攻撃者は 200GB のデータを窃取した旨を主張。調査の結果、攻撃者は全ての顧客データ及び大量の健康保険請求データにアクセス可能であったことが判明。
- メディバンクが身代金を支払わないことを公表した後、攻撃者はダークウェブ上に顧客データを公開[9]。

2.2. 国家支援等を受けたとされる攻撃グループの概況

2.2.1 中国関連

- 2022 年 11 月、「Mustang Panda」について、フィリピン政府組織又は関連組織を標的としていると考えられる活動を確認した旨ラックが、世界中の政府、研究機関、学術機関に対するスピアフィッシングキャンペーンを行った旨 TRENDMICRO 社がそれぞれ報告[10、11]。
- 2022 年 12 月、「MirrorFace」について、日本の政治団体を標的としたスピアフィッシングキャンペーンを行ったと ESET 社が報告[12]。

2.2.2 ロシア関連

- 2022 年 10 月、APT「Iridium(Sandworm Team)」が、エジプトとポーランドの運輸・物流企業を標的として、新しい「Prestige」ランサムウエアを用い攻撃を行ったと Microsoft Threat Intelligence Center(MSTIC)が報告[13]。
- 2022 年 11 月、「APT29」が、Windows Credential Roaming の脆弱性(CVE-2022-30170)を利用した欧州外交機関を攻撃の標的としていると Mandiant 社

---

[9] *Medibank「MEDIBANK CYBER ATTACK – CUSTOMER NOTICE OF ELIGIBLE DATA BREACH AS AT 09 JANUARY 2023」、https://www.medibank.com.au/health-insurance/info/cyber-security/customer-notice/ (2023/2/28 閲覧)*

[10] *ラック「中国圏拠点の Mustang Panda がマルウェア「Claimloader」で標的型攻撃、日本にも影響か(2022/11/17)」、https://www.lac.co.jp/lacwatch/report/20221117_003189.html (2022/12/20 閲覧)*

[11] *TRENDMICRO「Earth Preta Spear-Phishing Governments Worldwide(2022/11/18)」、https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html (2022/12/20 閲覧)*

[12] *ESET「Unmasking MirrorFace: Operation LiberalFace targeting Japanese political entities(2022/12/14)」、https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities (2023/1/10 閲覧)*

[13] *Microsoft Security Threat Intelligence「New "Prestige" ransomware impacts organizations in Ukraine and Poland(2022/10/14)」、https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ (2022/11/28 閲覧)*

が報告[14]。

○ 2022 年 12 月、「Fancy Bear」について、米国の衛星通信ネットワークに数ヶ月にわたり侵入していたと Cyberscoop 社が報告[15]。

2.2.3 北朝鮮関連

○ 2022 年 11 月、「Lazarus」が、ドイツ、ブラジル、インド、イタリア、メキシコ、スイス、サウジアラビア、トルコ、米国の複数分野の組織を標的に「Dtrack」バックドアを使った攻撃を実施していると、Kaspersky が報告[16]。

○ 2022 年 12 月、「Lazarus」が、マルウエア「AppleJesus」を使用して暗号資産の利用者や利用組織を標的に攻撃を実施していると、VOLEXITY 社及び Microsoft 社が報告[17]。

2.3. その他

2.3.1 国連安保理北朝鮮制裁委員会専門家パネル中間報告書

○ 2022 年 10 月 7 日、国連安保理北朝鮮制裁委員会専門家パネルが中間報告書を公表。

○ 軍需工業省や朝鮮人民軍といった北朝鮮関係機関が関与したサイバー攻撃事案について記載。

○ 暗号資産事業者や取引所に対するサイバー攻撃は継続しており、洗練化され、窃取された資金の追跡がより困難化と指摘。

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 大阪急性期・総合医療センターのランサムウエア感染事案

○ 2022 年 10 月 31 日、大阪府立病院機構大阪急性期・総合医療センターが、ランサムウエア攻撃を受け、電子カルテシステムに障害が発生した為、緊急以外の手術や外来診療を一時停止[18]。

---

[14] *MANDIANT「They See Me Roaming: Following APT29 by Taking a Deeper Look at Windows Credential Roaming(2022/11/8)」、https://www.mandiant.com/resources/blog/apt29-windows-credential-roaming（2022/12/5 閲覧）*

[15] *Cyberscoop「CISA researchers: Russia's Fancy Bear infiltrated US satellite network」、https://www.cyberscoop.com/apt28-fancy-bear-satellite/（2023/1/19 閲覧）*

[16] *Kaspersky「DTrack activity targeting Europe and Latin America(2022/11/15)」、https://securelist.com/dtrack-targeting-europe-latin-america/107798/（2022/12/6 閲覧）*

[17] *Volexity「Buyer Beware: Fake Cryptocurrency Applications Serving as Front for AppleJeus Malware(2022/12/1)」、https://www.volexity.com/blog/2022/12/01/buyer-beware-fake-cryptocurrency-applications-serving-as-front-for-applejeus-malware/（2022/12/1 閲覧）*

[18] *大阪急性期・総合医療センター「「電子カルテシステム」の障害発生について(2022/10/31)」、https://www.gh.opho.jp/pdf/info20221031.pdf（2022/12/7 閲覧）*

- 同センターは、10 月 31 日以降、厚生労働省の調査チーム、大阪府警、システムベンダーの支援を得て原因の究明及び復旧対応を実施、12 月 12 日には、電子カルテを含む基幹システムを再稼働、2023 年 1 月 11 日には、通常の診療体制が完全に復旧した旨を公表[19]。
- 同センターは、2023 年 1 月 25 日、外部の有識者による調査委員会を発足、3 月下旬調査報告書公表予定。

3.1.2 尼崎市における USB メモリ紛失事案

- 2022 年 6 月、尼崎市が BIPROGY 株式会社へ委託した臨時特別給付金対応業務において、再々委託先従業員が尼崎市民の個人データを含むUSBメモリを紛失する事案が発生。
- 2022 年 11 月 28 日、尼崎市は調査委員会による調査報告書を公表[20]
- 調査報告書は、委託者による受託者の作業の管理不足や、契約書で禁じられている再委託及び再々委託等を問題点として指摘。

3.1.3 NTTドコモの西日本地域における通信障害

- 2022 年 12 月 17 日、インターネット接続基盤の故障を起因とした異常動作により、故障発生時に自動で待機系に切り替わらないことで、西日本地域の一部の顧客においてインターネット通信（sp モード、ahamo のデータ通信）が利用しづらい事象が発生[21]。
- 2022 年 12 月 20 日、設備増強工事において、作業対象のネットワーク機器特有の手順を考慮せずに工事を行ったため、ネットワーク機器の設定が一部消失したことで、西日本地域の一部の顧客においてインターネット通信（sp モード、ahamo のデータ通信）が利用しづらい事象が発生[22]。
- 2023 年 1 月 16 日に、これら通信サービス障害に関して、総務省に重大な事故報告書を提出[23]。

---

[19] *大阪急性期・総合医療センター「診療体制の復旧について（第9報）(2023/1/10、https://www.gh.opho.jp/pdf/info20230110.pdf（2023/3/10 閲覧）*

[20] *尼崎市「個人情報を含む USB メモリーの紛失事案について(2022/11/28)」、https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html（2022/11/28 閲覧）*

[21] *NTTドコモ「2022 年 12 月 17 日に発生した西日本地域において一部のお客さまが sp モードをご利用しづらい事象について(2023/1/16)」、https://www.docomo.ne.jp/binary/pdf/info/news_release/2023/01/16_00.pdf（2023/2/28 閲覧）*

[22] *NTTドコモ「2022 年 12 月 20 日に発生した西日本地域において一部のお客さまが sp モードをご利用しづらい事象について(2023/1/16)」、https://www.docomo.ne.jp/binary/pdf/info/news_release/2023/01/16_01.pdf（2023/2/28 閲覧）*

[23] *NTTドコモ「2022 年 12 月 17 日および 12 月 20 日の通信サービス障害に関する報告書を提出(2023/1/16)」、https://www.docomo.ne.jp/info/news_release/2023/01/16_02.html（2023/2/28 閲覧）*

米国国家サイバーセキュリティ戦略の公表について

資料２－１

2023年3月2日、米ホワイトハウスは、4年4ヶ月ぶりに改定した「国家サイバーセキュリティ戦略」を公表した。
社会全体のデジタル技術への依存度の高まりや、中国、ロシア、イラン、北朝鮮及び非国家主体の悪意あるサイバー活動による米国の国家安全保障や社会経済活動への影響を踏まえ、以下の5つの柱から構成されている。

（https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/）

第1の柱：重要インフラの防護	第2の柱：脅威主体の阻止と打破	第3の柱：セキュリティ及びレジリエンスを推進する市場原理の形成	第4の柱：レジリエントな未来への投資	第5の柱：共通の目標を追求するための国際協力体制の形成
1. 国家の安全保障や公共の安全を支えるサイバーセキュリティ要件の確立 2. 官民協力の拡大 3. 連邦政府のサイバーセキュリティーセンターの統合 4. 連邦政府のインシデント対応計画及びプロセスの更新 5. 連邦政府の防衛の現代化	1. 連邦政府による阻止活動の統合 2. 敵対勢力阻止のための官民協働の強化 3. インテリジェンス共有及び被害通知の加速と規模拡大 4. 米国を拠点とするインフラの悪用防止 5. サイバー犯罪への対抗とランサムウェアの打倒	1. データ管理者の説明責任 2. 安全なIoTデバイス開発推進 3. 安全性に問題のあるソフトウェア及びサービスに対する法的責任の転嫁 4. 安全を確保した設計に対する連邦政府の補助金及びその他のインセンティブの活用 5. 説明責任を向上させるための連邦政府調達の活用 6. 連邦政府によるサイバー保険の支援	1. インターネットの技術的基盤の安全確保 2. サイバーセキュリティーのための連邦政府における研究開発の活性化 3. ポスト量子に対する備え 4. クリーンエネルギーの将来性の確保 5. デジタル・アイデンティティー・エコシステムの発展支援 6. サイバー人材強化のための国家戦略の策定	1. デジタル・エコシステムに対する脅威に対抗するためのコアリションの形成 2. 国際的パートナーの能力強化 3. 同盟国及び同志国を支援する米国の能力拡大 4. 国家の責任ある行動に関するグローバルな規範強化のためのコアリションの形成 5. ICT及びOT製品及びサービスのグローバルサプライチェーンの安全確保

✓ セキュリティ水準）　重要インフラの防護にあたり、これまでの自主的な取組による進展があったものの、強制的な基準の欠如が不十分かつ首尾一貫しない結果を招いたとして、セクター毎の規制枠組みが不可欠となっている旨明確にし、法的権限のないセクターでは議会との協力が必要とした。セクター毎のサイバーセキュリティに関する最低要件の策定に際しては、CISA※1が発行する重要インフラ各セクター共通のパフォーマンスゴールやNIST※2が発行するサイバーセキュリティフレームワークといった既存のガイダンスを活用することとした。

✓ インシデント報告）　サイバー脅威の標的となった事業者による政府機関への連絡方法や政府機関による支援方法を明確化する必要があるため、国家インシデント対応計画をCISA主導のもと更新するとした。加えて、サイバーインシデント報告法（CIRCIA法)により、対象となるサイバーインシデントを72時間以内にCISAに報告することを義務付け、タイムリーな情報共有を実現し、集団的防御を強化するとした。

※1 米国サイバーセキュリティ・インフラストラクチャーセキュリティ庁　※2 米国国立標準技術研究所

重要インフラにおける情報共有件数について(2022 年度第 3 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	FY2022 2Q	FY2022 3Q	FY2022 4Q	FY2022 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	83	63	―	224
関係省庁・関係機関からのNISCへの情報共有	7	16	16	6	0	0	0	―	0
NISCからの情報提供	43	38	64	91	18	18	30	―	66

(※) 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	FY2022 2Q	FY2022 3Q	FY2022 4Q	FY2022 計
未発生の事象		予兆・ヒヤリハット	27	12	28	25	15	2	5	―	22
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	5	5	4	―	14
	完全性を脅かす事象	情報の破壊	17	11	12	20	5	4	2	―	11
	可用性を脅かす事象	システム等の利用困難	97	158	157	181	29	37	37	―	103
	上記につながる事象	マルウェア等の感染	17	9	18	46	13	15	6	―	34
		不正コード等の実行	4	5	3	2	0	0	0	―	0
		システム等への侵入	14	14	26	24	2	5	7	―	14
		その他	34	47	42	80	9	15	2	―	26

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	FY2022 2Q	FY2022 3Q	FY2022 4Q	FY2022 計
意図的な原因	不審メール等の受信	36	13	9	47	19	12	2	―	33
	ユーザＩＤ等の偽り	3	12	9	7	2	2	1	―	5
	DDoS攻撃等の大量アクセス	17	20	10	19	8	6	2	―	16
	情報の不正取得	10	8	13	13	3	2	1	―	6
	内部不正	1	0	0	1	0	0	1	―	1
	適切なシステム等運用の未実施	14	11	23	15	2	0	5	―	7
偶発的な原因	ユーザの操作ミス	10	6	18	10	2	6	3	―	11
	ユーザの管理ミス	6	6	13	14	2	2	2	―	6
	不審なファイルの実行	16	7	7	22	14	10	1	―	25
	不審なサイトの閲覧	4	5	3	6	0	1	1	―	2
	外部委託先の管理ミス	29	39	56	107	11	14	11	―	36
	機器等の故障	27	62	39	38	7	11	12	―	30
	システムの脆弱性	19	16	38	32	4	3	5	―	12
	他分野の障害からの波及	6	4	7	10	3	3	0	―	6
環境的な原因	災害や疾病等	1	13	9	3	2	2	1	―	5
その他の原因	その他	29	33	35	48	8	5	8	―	21
	不明	46	53	68	79	11	20	13	―	44

(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

ランサムウェアに関連した報告では、長期間・広範囲にわたりサービスが停止した事例があった一方で、重要システムに係る被害の影響を抑えた事例もあり、障害対応への準備等が業務継続への影響を二分した。また、ウェブサーバへの不正アクセスによるウェブサイトの改ざんや情報流出が複数報告された。システム障害においては、設定ミス等によりサービスの可用性に支障をきたした事例が、複数の分野で数多く発生した。

ランサムウェア攻撃に関する報告が相次いでおり、改めて、ネットワーク接続にかかる資産管理・脆弱性管理の重要性の再認識が必要であるとともに、委託先等を含めたサプライチェーン全体の管理が求められる。

○　多層防御に加え、ネットワーク接続にかかる資産管理の重要性の再認識が必要

ランサムウェアにより業務上必要となるデータ等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あった。他方で、重要システムにおける適切な対策を講じ、基幹のサービスについては継続できた事例があった。

○　ウェブサイト等の公開されたサーバに係る脆弱性管理の徹底が必要

脆弱性をつく不正アクセス(SQL インジェクションなど)による認証情報の流出や、サーバのマルウェア感染によるウェブサイトの閲覧障害などの事例があった。

○　外部サービス利用時のリスクについての再認識が必要

外部サービスを提供する組織がサイバー攻撃を受けたことにより、自組織へも影響が及んだ事例があった。十分な対策が取られているはずという思い込みを排除し、リスクを認識した上でのサプライチェーン全体の管理が求められる。

○　認証手段の高度化の検討と認証情報の適切な管理が必要

ウェブサイト管理用、ネットワーク機器管理用の ID・パスワードが流出する事例が複数報告された。多要素認証やアクセス制限など、必要に応じて認証手段の高度化を検討するとともに、認証情報が格納されているサーバについてはより厳格な管理が求められる。

○　作業手順書の確認など適切な事前準備が必要

メンテナンス作業時などにおける作業手順書の確認不足やシステムの設定ミスを起因とするシステム障害により、サービスの提供に支障が生じた事例が複数あった。障害発生時の適切な広報の実施のため、経営層による判断・対応、広報部門との連携も重要。

以上