資料２

令和 6 年 2 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(2023 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、2023 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 人工知能の安全、安心、信頼できる開発と利用に関する大統領令

○ 2023 年 10 月 30 日、バイデン政権は、人工知能(AI)の安全、安心、信頼できる開発と利用に関する大統領令に署名[1]。

○ 大統領令では、サイバーセキュリティに関連する主な内容として、AI の安全性とセキュリティに関するガイドライン・標準・ベストプラクティスの開発、 安全で信頼性の高い AI の確保、 重要インフラ及びサイバーセキュリティにおける AI の管理等について、それぞれ各政府機関が、いつまでに、何をするのかを具体的に規定[2]。

1.1.2 CISA が人工知能導入のためのロードマップを発表

○ 2023 年 11 月 14 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)は、人工知能導入のためのロードマップ(Roadmap for Artificial Intelligence Adoption)を公表[3]。

---

[1] *The White House「Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence(2023/10/30)」、https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (2023/11/6 閲覧)*

[2] *The White House「FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence(2023/10/30)」、https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ (2023/11/7 閲覧)*

[3] *CISA「CISA Releases Roadmap for Artificial Intelligence Adoption(2023/11/14)」、https://www.cisa.gov/new*

○ 本ロードマップは、10 月 30 日にバイデン政権が署名した人工知能の安全、安心、信頼できる開発と利用に関する大統領令を受けたもので、CISA は、サイバーセキュリティ能力を強化するための AI の利用促進、AI システムのサイバー空間における脅威からの確実な保護、重要インフラを脅かす AI の悪用の抑止を推進。

1.1.3 「重大な」サイバーセキュリティインシデントに関する SEC 開示規則が発効

○ 2023 年 12 月 18 日、米国証券取引委員会(SEC)の、上場企業によるサイバーセキュリティのリスク管理、戦略、ガバナンス、重大なサイバーセキュリティインシデントに関する開示を強化・標準化するための新しい規則が施行[4]。

○ 上場企業は、インシデントの発見後、遅延なくその重要性を判断し、インシデントが重要であると判断された場合、その判断から通常 4 営業日以内に規則で定める様式での開示が必要。

○ このほか、サイバー脅威による重大なリスクを評価・特定・管理するためのプロセス、企業に重大な影響を与えたか・可能性があるかどうか、取締役会の監督・経営陣の役割と専門知識についても開示が必要。

1.2. 中国

1.2.1 習国家主席がバイデン米大統領と会談

○ 2023 年 11 月 15 日、米中首脳は、約 1 年ぶりの対面での会談を実施、会談では、両首脳は、米中政府間協議を通じて、高度な AI システムのリスクに対処し、AI の安全性を向上させる必要性を確認。バイデン大統領は、貿易や投資を不当に制限することなく、米国の先端技術が自国の国家安全保障を損なうために利用されるのを防ぐために必要な措置をとり続けることを強調[5]。

○ 習国家主席は、今回の会談を契機として打ち立てるべき「5 つの柱」として、共同で(1)正確な認知を打ち立てる、(2)意見の違いを効果的に管理・コントロールする、(3)互恵的協力を推進する、(4)大国としての責任を負う、(5)人的・文化的交流を促進するという 5 点を列挙[6]。

1.2.2 中国、改正反スパイ法のビジネス環境への影響懸念に反論、米国の手法

---

s-events/alerts/2023/11/14/cisa-releases-roadmap-artificial-intelligence-adoption（2023/12/12 閲覧）

[4] *SEC「FACT SHEET Public Company Cybersecurity Disclosures; Final Rules(2023/12/18)」、https://www.sec.gov/files/33-11216-fact-sheet.pdf（2024/1/19 閲覧）*

[5] *The White House「Readout of President Joe Biden's Meeting with President Xi Jinping of the People's Republic of China（2023/11/15)」、https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/15/readout-of-president-joe-bidens-meeting-with-president-xi-jinping-of-the-peoples-republic-of-china-2/（2024/2/7 閲覧）*

[6] *JETRO「習国家主席がバイデン米大統領と会談、軍事関連の意思疎通再開、AI などで協力も(2023/11/17)」、https://www.jetro.go.jp/biznews/2023/11/c093b204909a187c.html（2024/2/7 閲覧）*

を非難

- 2023 年 12 月 7 日、中国国家安全部はメッセンジャーアプリ「微信」上の公式アカウントで、「改正反スパイ法」が対中投資を萎縮させているとの見方に反論[7]。反スパイ法の強化は世界各地で行われている正当な措置だと主張。
- また、いくつかの国は「安全保障」を政治問題化、武器化して中国の正常な経済・貿易活動と発展の権利を押さえつけようとしているとし、米国はこれまで 1,500 以上の中国の事業体や個人に対して制裁を行い、市場経済のルールにそむき、中国企業の生存と発展に重大な影響を与えていると非難。

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 ドイツ西部でランサムウェア攻撃が原因で 70 の自治体がサービス提供を一時停止

- 2023 年 10 月 30 日、ドイツの南ヴィストファーレン IT 社がランサムウェア攻撃を受け、感染拡大防止のため、サービスを提供する主にノルトライン・ヴェストファーレン州の 70 以上の自治体に対し、自社インフラに対するアクセスを制限。その結果、自治体サービスが著しく制限[8]。
- ドイツのサイバーセキュリティ専門家は、地方自治体は通常月末に金融取引を行うため、給与、社会扶助、介護基金からの送金などの支払が影響を受ける可能性があると指摘。

2.1.2 オーストラリア第2位の通信企業オプタスの通信障害

- 2023 年 11 月 7 日、オーストラリア第2位の通信企業オプタスで通信障害が発生し、人口の 40%に当たる約 1,000 万人が、一日のほとんどの時間スマートフォン、インターネット、固定電話を使用できなくなり、決済、交通、医療システムに混乱[9]。
- 障害の原因は、ソフトウェアのアップグレードの際に、全国の拠点に設置されたルーターがネットワークから切断され、スタッフが物理的にルーターの再接続・再起動を行う必要があり復旧に時間を要したこと。サイバー攻撃や顧客情報の漏えいの兆候は無し[10]。

---

[7] *JETRO「中国、改正反スパイ法のビジネス環境への影響懸念に反論、米国の手法を非難(2023/12/11)」、https://www.jetro.go.jp/biznews/2023/12/344178b19820affc.html（2024/2/7 閲覧）*

[8] *The Record「Massive ransomware attack hinders services in 70 German municipalities(2023/11/2)」、https://therecord.media/massive-cyberattack-hinders-services-in-germany（2024/2/7 閲覧）*

[9] *Reuturs「Optus outage causes chaos in Australia before services restored(202311/7)」、https://www.reuters.com/technology/australias-optus-hit-by-national-network-outage-2023-11-07/（2024/2/7 閲覧）*

[10] *Optus「We're very sorry for the outage」、https://www.optus.com.au/notices/outage-response（2024/2/7 閲覧）*

2.1.3　米国ペンシルベニア州水道局へのサイバー攻撃

- ○ 2023 年 11 月下旬、イラン政府イスラム革命防衛隊（IRGC）傘下の攻撃グループ「Cyber Av3ngers」が米国ペンシルベニア州の Aliquippa 水道局のイスラエル製制御システムに侵入。同水道局ではシステムをネットワークから遮断し、手動による操作へ切り替え、飲料水など給水への影響は無し[11]。
- ○ 米国 CISA は、同じ制御システムが複数の州で利用されていることを踏まえ、パスワードの変更や多要素認証の採用を含めた緩和策を実施するよう注意喚起[12]。

2.1.4　米医療サービス大手 Ardent 社へのランサムウェア攻撃

- ○ 2023 年 11 月 23 日、米ナッシュビルに本拠を置く、全米で 37 の医療施設を運営する医療サービス大手 Ardent 社がランサムウェア攻撃を受け、複数の州にわたり、病院の救急業務などに支障[13]。
- ○ 傘下の医療施設で治療中の患者への対応は継続。システムが復旧するまでの間、緊急性のない手術等のスケジュールを変更し、救急外来患者の一部を他の地域の病院に振り分けし対応[14]。

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

- ○ 2023 年 10 月、「ISLANDDREAMS」による WinRAR の脆弱性(CVE-2023-38831)の悪用について、Google 社が報告[15]。
- ○ 2023 年 12 月、「UNC4841」について、Barracuda 社のメールセキュリティゲートウェイ(ESG)の脆弱性を悪用した攻撃を行ったと同社が報告[16]。

---

[11] *The Record「Pennsylvania water authority hit with cyberattack allegedly tied to pro-Iran group(2023/11/28)」、https://therecord.media/water-authority-pennsylvania-cyberattack-pro-iran-group（2024/2/7 閲覧）*

[12] *CISA「IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities(2023/12/1)」、https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a（2024/2/7 閲覧）*

[13] *The Record「Multiple hospitals divert ambulances after ransomware attack on parent company(2023/11/28)」、https://therecord.media/ardent-health-services-ransomware-hospitals-divert-ambulances（2024/2/8 閲覧）*

[14] *Ardent HEALTH SERVICES「Cybersecurity Incident」、https://ardenthealth.com/cybersecurityincident（2024/2/8 閲覧）*

[15] *Google「Government-backed actors exploiting WinRAR vulnerability(2023/10/18)」、https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/（2023/11/7 閲覧）*

[16] *Barracuda「Barracuda Email Security Gateway Appliance (ESG) Vulnerability(2023/12/24)」、https://www.barracuda.com/company/legal/esg-vulnerability（2024/1/9 閲覧）*

2.2.2 ロシア関連

- 2023 年 10 月、「Sandworm」がウクライナの電気通信プロバイダを攻撃 [17]。
- 2023 年 10 月、「APT28」、「Sandworm」等が WinRAR の脆弱性 CVE-2023-38831 を悪用 [18]。
- 2023 年 11 月、ウクライナの NCCC は、2023 年 9 月に「APT29」が WinRAR の脆弱性 CVE-2023-38831 を悪用し、主にアゼルバイジャンとイタリアにフィッシング攻撃を実施した旨を報告 [19]。
- 2023 年 12 月、ウクライナの電気通信事業者 Kyivstar がサイバー攻撃により通信障害が発生したと The Record が報道 [20]、その後、Kyivstar を装ったフィッシングメールが確認されたと CERT-UA が報告 [21]。

2.2.3 北朝鮮関連

- 2023 年 11 月、Microsoft 社は、CyberLink 社の正規ソフトを悪用するサプライチェーン攻撃を観測し、高い確度で攻撃グループ「Lazarus」に帰属。一部、日本でも影響を確認 [22]。
- 2023 年 11 月、北朝鮮の関与が疑われる、求職活動を装う 2 つのキャンペーンを発見。一方は高い確度で北朝鮮に帰属され、北朝鮮の IT 労働者に関連する可能性あり [23]。
- 2023 年 12 月、攻撃グループ「Lazarus」による新たなキャンペーン Operation Blacksmith を観測したと Cisco 社が報告。このキャンペーンに関連する、D 言語で書かれた複数のマルウェアを確認 [24]。

---

[17] *CERT-UA「Особливості деструктивних кібератак у відношенні українських провайдерів (CERT-UA#7627)(2023/10/15)」、https://cert.gov.ua/article/6123309 (2023/11/20 閲覧)*

[18] *Google「Government-backed actors exploiting WinRAR vulnerability(2023/10/18)」、https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/ (2023/11/15 閲覧)*

[19] *NCCC「APT29 ATTACKS EMBASSIES USING CVE-2023-38831(2023/11/14)」、https://www.rnbo.gov.ua/en/Diialnist/6708.html (2023/12/12 閲覧)*

[20] *The Record「Hackers damaged some infrastructure of Ukraine's Kyivstar telecom company(2023/12/13)」、https://therecord.media/hackers-damaged-kyivstar-functions-ukraine-telecom-cyberattack (2024/1/23 閲覧)*

[21] *CERT-UA「"Заборгованість Київстар", "Запит СБУ": нова атака UAC-0050 з використанням RemcosRAT (CERT-UA#8338)(2023/12/21)」、https://cert.gov.ua/article/6276824 (2024/1/23 閲覧)*

[22] *Microsoft「Diamond Sleet supply chain compromise distributes a modified CyberLink installer(2023/11/22)」、https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/ (2023/11/27 閲覧)*

[23] *Palo Alto Networks「求職戦線異状あり: 北朝鮮の国家支援型 APT 脅威アクターの特徴をもつ 2 つの求人・求職ハック キャンペーン(2023/11/21)」、https://unit42.paloaltonetworks.jp/two-campaigns-by-north-korea-bad-actors-target-job-hunters/ (2023/11/28 閲覧)*

[24] *Cisco「Operation Blacksmith: Lazarus targets organizations worldwide using novel Telegram-based malware written in DLang(2023/12/11)」、https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/*

2.3. その他

2.3.1 Okta 社のサポートケース管理システムへの不正アクセス

- 2023 年 10 月、ID プロバイダの Okta 社は同社のサポートケース管理システムが不正アクセスを受け、一部の顧客の情報が漏えいしたことを公開[25]。
- 影響を受けた顧客企業として Cloudflare 社や 1Password 社が情報漏えいによる自社への影響や対応状況を公開[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 全銀システムのシステム障害

- 2023 年 10 月 10 日から 11 日にかけて、一般社団法人全国銀行資金決済ネットワークが運営する全国銀行データ通信システム(全銀システム)に障害が発生し、10 の金融機関における 566 万件の内国為替取引に影響。
- 原因は、中継コンピュータ(RC)の移行作業におけるプログラム不具合、全銀ネットはベンダーマネジメントの向上等を再発防止策として公表[27]。

3.1.2 日本カードネットワークのシステム障害

- 2023 年 11 月 11 日、日本カードネットワークが運営する決済ネットワーク「CARDNET」にシステム障害が発生し、約 80 万件のクレジットカードの決済が利用できない等の影響[28]。
- 原因は、13 日に予定していたシステム更改の準備作業であるデータ同期処理によるシステムへの過負荷[29]。

3.1.3 中津市民病院にサイバー攻撃

- 2023 年 11 月 21 日、中津市民病院は、財務会計システムのサーバがランサムウェアに感染し、取引先事業者に関する情報が流出した可能性がある旨を公表[30]。

(2024/1/10 閲覧)

[25] *Okta「Unauthorized Access to Okta's Support Case Management System: Root Cause and Remediation (2023/10/20)」、https://sec.okta.com/harfiles (2023/11/21 閲覧)*

[26] *CloudFlare「How Cloudflare mitigated yet another Okta compromise(2023/10/21)」、https://blog.cloudflare.com/how-cloudflare-mitigated-yet-another-okta-compromise/ (2023/11/21 閲覧)*

[27] *一般社団法人全国銀行資金決済ネットワーク「全国銀行データ通信システムの障害について(2023/12/1)」、https://www.zengin-net.jp/announcement/pdf/announcement_20231201.pdf (2023/12/1 閲覧)*

[28] *https://www.nikkei.com/article/DGXZQOUB112N50R11C23A1000000/*

[29] *CARTNET「11 月 11 日 CARDNET センターの障害について(11/24 更新)」、https://www.cardnet.co.jp/release/20231111_1.html (2024/2/8 閲覧)*

[30] *中津市民病院「財務会計システムへの不正アクセスによる情報流出の可能性について(2023/11/21)」、https:/*

○ 被害が生じた財務会計システムは、電子カルテシステムをはじめとする他ネットワークへと接続していないため、患者情報の流出はなく、診療業務への影響も無し。

3.2. その他

3.2.1 QR コードを使用したフィッシング

○ 複数のセキュリティ企業が、QR コードを使用したフィッシング(Quishing)について相次いで報告。

○ Microsoft アカウントの認証情報を窃取しようとする大規模な Quishing キャンペーンが 2023 年 5 月頃に開始。日本の組織でも該当するフィッシングメールを受信した事例あり[31]。

○ 2023 年 9 月に Quishing の観測数が急増し、10 月もこの傾向が継続[32]。

3.2.2 マルウェア Mirai の亜種 InfectedSlurs

○ マルウェア Mirai の亜種である InfectedSlurs による、ルーターや NVR 製品のゼロデイ脆弱性を悪用した拡散を観測。主に日本で使用されている製品の脆弱性も悪用[33]。

○ 2023 年 12 月時点で InfectedSlurs の感染数は 1 万以上と考えられており、その多くは中国やインドだが、日本でも感染を確認。

○ InfectedSlurs のボットネットを使用した DDoS 攻撃は様々な国の IP アドレスを対象に行われており、DDoS 攻撃代行サービスのインフラとして利用されている可能性あり。

/www.city-nakatsu.jp/hospital/info/info2023/pdf/tpc_20231121.pdf (2024/2/8 閲覧)

[31] *Cofense「Major Energy Company Targeted in Large QR Code Phishing Campaign(2023/8/16)」、https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/ (2023/11/14 閲覧)*

[32] *Perception Point「QR Code Phishing (Quishing) Attacks Have More Than Quadrupled In Just One Month(2023/10/23)」、https://perception-point.io/blog/qr-code-phishing-quishing-attacks-have-more-than-quadrupled-in-just-one-month/ (2023/11/13 閲覧)*

[33] *IIJ「Mirai 亜種 InfectedSlurs の活動状況(2023/12/20)」、https://sect.iij.ad.jp/blog/2023/12/mirai-infectedslurs/ (2024/1/16 閲覧)*

重要インフラにおける情報共有件数について(2023 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	FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	2Q	3Q	4Q	計
重要インフラ事業者等からNISCへの情報連絡(※1)	269	309	407	302	99	53	63	―	215
関係省庁・関係機関からのNISCへの情報共有	16	16	6	2	0	0	0	―	0
NISCからの情報提供	38	64	91	83	15	28	21	―	64

(※1) 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			FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	2Q	3Q	4Q	計
未発生の事象		予兆・ヒヤリハット	12	28	25	28	9	1	2	―	12
発生した事象	機密性を脅かす事象	情報の漏えい	13	23	29	17	9	4	4	―	17
	完全性を脅かす事象	情報の破壊	11	12	20	15	5	6	3	―	14
	可用性を脅かす事象	システム等の利用困難	158	157	181	145	56	31	30	―	117
	上記につながる事象	マルウェア等の感染	9	18	46	38	2	4	8	―	14
		不正コード等の実行	5	3	2	1	1	0	1	―	2
		システム等への侵入	14	26	24	22	6	2	1	―	9
		その他	47	42	80	36	11	5	14	―	30

2. 原因別類型(複数選択)

原因の類型		FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	2Q	3Q	4Q	計
意図的な原因	不審メール等の受信	13	9	47	39	4	0	3	―	7
	ユーザＩＤ等の偽り	12	9	7	7	4	0	0	―	4
	DDoS攻撃等の大量アクセス	20	10	19	28	16	6	2	―	24
	情報の不正取得	8	13	13	10	5	2	3	―	10
	内部不正	0	0	1	1	0	1	1	―	2
	適切なシステム等運用の未実施	11	23	15	8	2	0	3	―	5
偶発的な原因	ユーザの操作ミス	6	18	10	12	4	0	3	―	7
	ユーザの管理ミス	6	13	14	7	4	0	0	―	4
	不審なファイルの実行	7	7	22	26	1	0	1	―	2
	不審なサイトの閲覧	5	3	6	4	4	1	4	―	9
	外部委託先の管理ミス	39	56	107	49	14	12	19	―	45
	機器等の故障	62	39	38	43	8	12	7	―	27
	システムの脆弱性	16	38	32	12	11	6	15	―	32
	他分野の障害からの波及	4	7	10	7	1	2	2	―	5
環境的な原因	災害や疾病等	13	9	3	5	0	1	0	―	1
その他の原因	その他	33	35	48	29	14	10	10	―	34
	不明	53	68	79	62	21	6	8	―	35

3. サイバー攻撃による事象の種別内訳(情報連絡を元にNISC重要インフラ防護担当において分析・再集計)

サイバー攻撃の類型	FY2019 計(※2)	FY2020 計(※2)	FY2021 計(※2)	FY2022 計(※2)	FY2023 1Q	2Q	3Q	4Q	計
総計	87	100	174	143	52	18	26	―	96
ランサムウェア攻撃	8	13	46	30	8	5	14	―	27
ランサムウェアを除くマルウェア感染	11	8	29	27	2	1	0	―	3
DDoS攻撃等の大量アクセス	14	4	15	25	10	6	3	―	19
その他	54	75	84	61	32	6	9	―	47

(※2) 件数は今後の精査により修正の可能性がある

(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(2023 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

システムの更改やメンテナンスに際してのリスクについて、影響範囲などの想定が十分にできていなかったことや、その対応についての管理が不十分であったことなどから、システム障害に至った事例が複数あった。自組織の情報資産の把握、リスクの特定、分析及び評価といった一連のリスクアセスメントと、それを踏まえたリスク対応などリスクマネジメントの継続的な向上が重要である。

○ システム更改時などにおける適切なリスクアセスメントが必要

システム更改時などにおけるリスクに関して、本番環境への影響を十分に想定できず大規模障害に発展してしまった事例や、一つのシステム障害が複数のサービスに影響を及ぼした事例など、リスクアセスメントが不足していたと考えられる事例が多数あった。

○ 委託先を含み、適切な事前準備やシステム管理が必要

システムメンテナンス時の設定誤りを起因とするシステム障害や、障害発生時における代替手段の実施に際しマニュアルどおりに対応しなかったことにより、サービスの提供に支障が出た事例が引き続きあった。また、アプリケーションのライセンス更新漏れ、システムに使用している機器の不具合情報に係る委託先内における共有漏れなど、情報共有不足によるシステム障害も発生している。

○ 認証情報の適切な管理が必要

システム開発の委託先が発行したアクセスキーが漏えいし悪用された事例や、サポート詐欺やフィッシングメールなどの手法により認証情報が漏えいしリークサイトに公開された事例、漏えいした認証情報により迷惑メールの発信に悪用された事例などがあった。委託先を含め、認証情報の適切な管理が求められる他、漏えいしてしまうことも想定した多要素認証の導入も重要。

○ 組織間の連携・情報共有が必要

SoC などの関係機関と連携し、ウェブサイトへの攻撃を試行する通信を検知・遮断するなどにより、インシデントを未然に防止できた事例があった。また、インシデントの発生を速やかにグループ企業間で共有し、被害拡大防止につなげている事例もあった。グループ企業・関係機関との連携・情報共有は重要であり継続的な取組が必要。

○ 廃止済のドメインについて適切な管理が必要

閉鎖したウェブサイトのドメインが第三者に取得される事例が複数あり、偽サイトが公開されている事例もあった。他方、ウェブサイト閉鎖後、一定期間組織で保持し、保持期間終了後も当該ドメインについてモニタリングし、第三者に取得されている旨を公表するなど適切にリスク管理をしている事例もあった。ドメインの廃止に関しては、顧客への影響を踏まえた適切な対応が求められる。

以上