資料３

令和５年９月７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１四半期) ····· 2
・重要インフラにおける情報共有件数について(2023 年度第１四半期) ····· 9
・最近のインシデントから得られた教訓(2023 年度第１四半期) ····· 10

サイバーセキュリティを取り巻く情勢(2023 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、2023 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 世界最大級の不正マーケット Genesis Market への制裁・一斉摘発

- 2023 年 4 月 5 日、米国財務省外国資産管理局(OFAC)は、デバイスの認証情報や関連する機密情報の窃盗と販売に関与しているとして、世界最大級の不正なマーケットの一つである Genesis Market を金融制裁の対象に指定[1]。
- 2023 年 4 月 4 日から 5 日にかけ、米国司法省(DOJ)は、米国連邦捜査局(FBI)及び欧州刑事警察機構(ユーロポール)をはじめとした国際パートナーと連携し、Operation Cookie Monster(クッキーモンスター作戦)と呼ばれる Genesis Market の一斉摘発を実施[2]。

1.1.2 米国国防総省サイバー戦略

- 2023 年 5 月 26 日、米国国防総省(DOD)は、機密扱いの 2023 年米国国防総省サイバー戦略を議会に伝達したことを公表した[3]。
- 本戦略は、2022 年の国家防衛戦略で定められたサイバー空間の概念と防衛目標を運用するための指示をDODに与えるものであり、米国民を保護し、

---

[1] *US.DOT「Treasury Sanctions Illicit Marketplace Genesis Market(2023/4/5)」、https://home.treasury.gov/news/press-releases/jy1388 (2023/3/24 閲覧)*

[2] *DOJ「Criminal Marketplace Disrupted in International Cyber Operation(2023/4/5)」、https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation (2023/5/11 閲覧)*

[3] *DOD「DOD Transmits 2023 Cyber Strategy(2023/5/26)」、https://www.defense.gov/News/Releases/Release/Article/3408707/dod-transmits-2023-cyber-strategy/ (2023/6/16 閲覧)*

米国の防衛上の優先事項を推進するために、DOD がサイバー空間において又はサイバー空間を通じてどのように活動するかを定めたもの。

○ 本戦略は実世界の経験に基づくものであり、2018 年の前戦略以降、DOD は、前方防衛(defending forward)政策を通じて数多くの重要なサイバー空間作戦を実行し、米国本土に影響を与える前に、悪意のあるサイバー活動を積極的に妨害した知見等を反映。

1.1.3 米国サイバー空間ソラリウム委員会 2.0 報告書

○ 2023 年 6 月 7 日、米国サイバー空間ソラリウム委員会(以下「CSC」)は、米国の重要インフラ防護のための官民連携の見直し(Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure)と題した報告書を公表[4]。

○ 現在の重要インフラ防護のための官民連携政策は時代遅れとなり、今日の需要を満たすことができなくなっており、政府機関の組織、資金、焦点も不十分。官民関係の現状を評価し、今後の国家安全保障を改善するために官民関係を再構築することが必要と評価。

○ しかしながら、規制・インセンティブ付与・協力のバランスをとるアプローチに軸足を置くコンセプトが、官民を調整する最良の方法であることに変わりはないと結論。

1.1.4 米国国防総省、政府調達局及び航空宇宙局における TikTok 禁止

○ 2023 年 6 月 2 日、米国国防総省(DOD)、政府調達局(GSA)及び航空宇宙局(NASA)は、請負事業者も含めた政府システムに接続するデバイスにおける TikTok の保有及び使用を禁止する暫定規則「Federal Acquisition Regulation: Prohibition on a ByteDance Covered Application」を発表[5]。

○ 暫定規則では、2023 年 6 月 2 日以降に全ての政府機関が公示する調達に関して適用され、また、同日以前に公示された調達は、7 月 3 日までにこの暫定規則に準拠した内容に修正し、再公示することが求められる。

○ 暫定規則の適用対象は、米国行政管理予算局(OMB)覚書による例外を除き、政府が所有もしくは管理する情報技術、又は請負事業者によって使用もしくは提供される情報技術(請負事業者の従業員が提供する機器を含む)の全てに適用。

---

[4] *CSC2.0「Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure(2023/6/7)」、https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure/ (2023/7/14 閲覧)*

[5] *FEDERAL REGISTER「Federal Acquisition Regulation: Prohibition on a ByteDance Covered Application(2023/6/2)」、https://www.federalregister.gov/documents/2023/06/02/2023-11756/federal-acquisition-regulation-prohibition-on-a-bytedance-covered-application (2023/7/18 閲覧)*

1.2. 中国

1.2.1 中華人民共和国反間諜法

- 2023 年 4 月 26 日、中国全国人民代表大会(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」)の改正案が可決[6]、7 月 1 日同法は施行。
- スパイ組織及びその代理人による、中国の国家安全に危害を及ぼすとみなされる活動について、国内外を問わず適用。
- 国家秘密、インテリジェンス及びその他国家の安全と利益に関わる文書、データ、資料、物品の窃取等のほか、国家機関や重要情報インフラ等へのサイバー攻撃もスパイ行為と規定。

1.2.2 中国、米マイクロンの半導体を調査、調達停止

- 2023 年 4 月 31 日、中国国家インターネット情報弁公室(CAC)は、米半導体大手マイクロン・テクノロジーが中国で販売している製品のサイバーセキュリティについて調査すると表明[7]。
- 2023 年 5 月 21 日、中国の国家インターネット情報弁公室は、マイクロン・テクノロジーについて、サイバーセキュリティ審査を通過できなかったと発表[8]。
- 審査を通過できなかった理由は、同社製品には重大なサイバーセキュリティ上の隠れたリスクが存在しており、中国の重要情報インフラのサプライチェーンにとって大きなリスクとなり、国家の安全に影響するためと説明。

1.2.3 米国国務省、中国は米重要インフラへのサイバー攻撃能力を有すると警告

- 2023 年 5 月 25 日、米国国務省は、中国は米国の石油・ガスパイプラインや鉄道システムなどの重要インフラに対してサイバー攻撃を仕掛けることが可能だと警告[9]。
- 米国国務省のミラー報道官は記者会見において、米国情報機関は、中国がほぼ確実に、米国内の石油・バスパイプラインや鉄道システム等、重要インフラサービスを混乱させるサイバー攻撃を行う能力があると評価している旨発言[10]。

---

[6] *The Record「China revises law to include certain cyberattacks as 'acts of espionage'(2023/4/27)」、https://therecord.media/china-beijing-cyberespionage-law-revised (2023/8/23 閲覧)*

[7] *Reuters「中国、米マイクロンの半導体を調査 サイバーリスク阻止と説明(2023/4/31)」、https://jp.reuters.com/article/china-cybersecurity-micron-idJPKBN2VX1FB (2023/8/23 閲覧)*

[8] *JETRO「中国、米マイクロン製品の調達停止、サイバーセキュリティー審査を通過できず(2023/5/24)」、https://www.jetro.go.jp/biznews/2023/05/fad9cf500b30a3f1.html (2023/8/23 閲覧)*

[9] *https://jp.reuters.com/article/usa-china-cyber-idJPL4N37M4DJ*

[10] *DOS「Department Press Briefing - May 25, 2023(2023/5/25)」、https://www.state.gov/briefings/department-press-briefing-may-25-2023/ (2023/8/23 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 米国テキサス州ダラス市に対するランサムウェア攻撃

- 2023 年 5 月 3 日、米国テキサス州ダラス市は、Royal ランサムウェアグループによるランサムウェア攻撃を受け、IT システムの一部を停止し、市警察及び消防の通信・IT システムが停止した旨を公表 [11]。
- ダラス市の全ての地方裁判所が休業したほか、緊急通報システムが停止した警察及び消防は電話や手書きで対応する等の影響。水道料金のオンライン支払システム、図書館予約システムが停止する等の影響 [12]。

2.1.2 米国運輸省の交通費給付システムにおける個人情報流出

- 2023 年 5 月 12 日、Reuters は、米国運輸省(DOT)の交通費支給システム TRANServe が侵害を受け、23.7 万人の連邦政府の現職及び元職員の個人情報が流出したと報道 [13]。
- TRANServe は、米国の交通渋滞と大気汚染問題に対処するため、エネルギー効率の高い公共交通機関の利用を促進するため、1991 年に DOT において設立され、2005 年以降連邦政府機関の全ての従業員を対象として実施 [14]。
- DOT は、この侵害では輸送の安全システムには影響はないが、安全が確保されるまで、TRANServe システムへのアクセスを凍結すると公表 [15]。

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 5 月、「Volt Typhoon」が、米国の重要インフラを標的とした攻撃を実行。ステルス性を重視した攻撃手法が用いられていることから、攻撃の検出が困難になる可能性を Microsoft 社は懸念。
- 2023 年 6 月、「Earth Preta」が、2023 年から新たな攻撃手法を用いて活発な活動を行っていると Trend Micro 社が報告。
- 2023 年 6 月、「UNC4841」が、Barracuda 社のメールセキュリティゲートウェイ

---

[11] *The Record「Dallas city government confirms ransomware attack affecting police and other services(2023/5/4)」、https://therecord.media/dallas-confirms-ransomware-attack-affecting-police-website（2023/6/13 閲覧）*

[12] *KERA「Dallas is still under a ransomware attack. Here's what's impacted(2023/6/1)」、https://www.keranews.org/government/2023-06-01/dallas-ransomware-attack-cyberattack-whats-impacted（2023/8/23 閲覧）*

[13] *Reuters「Data of 237,000 US government employees breached(2023/5/12)」、https://www.reuters.com/world/us/data-237000-us-government-employees-breached-2023-05-12/（2023/6/13 閲覧）*

[14] *DOT「About TRANServe」、https://www.transportation.gov/transerve/about-transerve（2023/6/13 閲覧）*

[15] *DOT「FAQs on TRANServe System Unavailability」、https://www.transportation.gov/transerve/step-step-transit-benefit-application-guide（2023/6/13 閲覧）*

(ESG)のゼロデイ脆弱性を悪用するため、全世界の多数の組織に悪意のある添付ファイルを含む電子メールを送信したと Mandiant 社が報告。

2.2.2 ロシア関連

- 2023 年 4 月、ロシアの NTC Vulkan 社の企業機密文書が流出し、SEKOIA.IO 社、Mandiant 社が分析結果を公表。ロシア軍部や情報機関のために設計したデータベース、サイバー攻撃や演習システムなどの技術情報やマニュアルが記載。
- 2023 年 4 月、「APT28」による、Cisco 社製ルーターの脆弱性 CVE-2017-6742 を悪用した攻撃について、米国と英国が共同アドバイザリーを公表。ウクライナ CERT-UA から、「Windows Update」を騙るフィッシングキャンペーンについて報告。
- 2023 年 5 月、米国 FBI は、ロシア連邦保安庁が使用する情報窃取マルウェア Snake の無効化に成功。

2.2.3 北朝鮮関連

- 2023 年 4 月、2023 年 3 月下旬頃から発覚し始めた 3CX サプライチェーン攻撃について、多数のセキュリティ企業が分析結果を報告。3CX 社の開発環境が侵害され、同社ソフトウェアのインストーラーがトロイの木馬化された。このインストーラーを介した、情報窃取型マルウェアやバックドアの配布を確認。帰属に関して、攻撃グループ「Lazarus」や「UNC4736」などと分析。
- 2023 年 5 月、「Bluenoroff」が macOS を対象とするマルウェア RustBucket を使用。同グループによる macOS を対象とした攻撃を初観測。また、日本の金融機関などを装う複数のドメインを発見。
- 2023 年 6 月、米国及び韓国は、攻撃グループ「Kimsuky」によるソーシャルエンジニアリングに関するセキュリティ勧告を発表。実在する人物を装うスピアフィッシングメールなどに言及。SentinelOne 社は、同様の手法を使用して Google アカウントの認証情報などの窃取を狙う「Kimsuky」のキャンペーンを報告。マルウェア ReconShark を展開するケースも確認。

2.3. その他

2.3.1 ビジネスメール詐欺をめぐるサイバー犯罪活動の巧妙化

- 2023 年 5 月、Microsoft 社はビジネスメール詐欺をめぐるサイバー犯罪活動の急増に焦点を当てたサイバーシグナルの第 4 版をリリース [16]。
- 大規模にビジネスメール詐欺を行う犯罪プラットフォームの存在や、メールア

[16] *Microsoft「Cyber Signails May 2023(2023/5/19)」、https://aka.ms/CyberSignalsReport-4 (2023/6/19 閲覧)*

カウントの侵害をシステムで検知するための手法である「あり得ない移動」を回避する新たな手法が使われる等、サイバー犯罪活動が巧妙化

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 富士通 Japan 社製コンビニ交付システムによる証明書誤交付事案

- 2023 年 3 月以降、富士通 Japan 製コンビニ交付システムを利用する地方公共団体において証明書の誤交付が相次いで発生。
- 横浜市の事案では高負荷時の処理誤り、足立区の住民記録システムとコンビニ交付システムの連携誤り等、原因は多様。
- 事案を受け、総務省やデジタル庁はシステムの点検等を要請、個人情報保護委員会は個人情報保護法等に基づく報告徴収や資料提供を要求。

3.1.2 全日本空輸(ANA)の国内線システム障害

- 2023 年 4 月 3 日、全日本空輸(ANA)は、国内線でシステム障害が起こり、航空券の予約や販売、搭乗手続きなどのサービスが一時的にできなくなったと発表、羽田―福岡など計 55 便が欠航、約 6,700 人に影響し、遅延も多数発生[17]。
- 4 月 7 日、ANA は、システム不具合の原因と再発防止策を発表、原因は、予約管理業務のために特定のデータを抽出する日常の処理において、ソフトウェアのバグを起因とするエラーが発生し、データベースサーバーが一時的に高負荷状態となり、その結果、データ処理が滞り、サーバー2 台が同時に停止したことによるもの。
- 再発防止に向け、(1)データ抽出方法の変更、(2)データベースサーバーが 2 台同時に停止しないための制御プログラムの強化の 2 点を実施。今後、システム障害が発生した場合に備え、バックアップシステムへの迅速な切りかえ、訓練の実施などの対策も実施[18]。

3.1.3 約 90 の自治体が利用する議会 Web システムに不正アクセス

- 2023 年 4 月、(株)フューチャーインが約 90 の自治体に提供している議会関連 Web サービスのサーバーが不正アクセスを受け、同社は一時サービスを停止[19]。

---

[17] *読売「全日空システム障害、6700人に影響…振り替え便も欠航の女性「親族の手術でどうしても帰りたい」(2023/4/3)」、https://www.yomiuri.co.jp/economy/20230403-OYT1T50202/（2023/8/24 閲覧）*

[18] *CNET.Japan「4 月 3 日の ANA の障害、原因はソフトウェアのバグ--国内線 55 便が欠航、データ流出は無し(2023/4/10)」、https://japan.cnet.com/article/35202379/（2023/8/24 閲覧）*

[19] *Security-next「自治体向け「議会運営サービス」にサイバー攻撃(2023/4/14)」、https://www.security-next.com/145404（2023/8/23 閲覧）*

○ 議会中継や登庁管理、会議録検索など、自治体の議会運営を支援するサービスで、9 日頃より外部から大量のアクセスが発生、11 日に ID やパスワードの総当り攻撃を受け、一部サーバーが不正侵入された形跡が確認。
○ 原因はシステムにログインするための ID とパスワードの総当たり攻撃を受け、ID とパスワードが不正に窃取され、侵入されたもの [20]。

3.1.4 JR 東日本における電源工事に起因するシステム障害

○ 2023 年 6 月 24 日、JR 東日本において、電源工事の影響により、Web サイト、ビューカードシステム、モバイル Suica システム、えきねっと・旅行業システムへの電源供給が停止し、ハード故障やデータ不整合が発生し、サービスが一時利用不可 [21]。
○ 原因は、屋内の電源工事にあたって、計画と異なる盤内にあるブレーカーを「切」にしたことで、システムサーバーの電源が遮断されたため。具体的には、①工事の操作手順書に誤りがあったことと、②現地操作時にその誤りに気付かず操作をしたこと。

[20] *日経クロステック「全国約 90 の自治体議会 Web システムが停止、事業者サーバーが不正アクセス被害(2023/4/14)」、https://xtech.nikkei.com/atcl/nxt/news/18/14994/（2023/8/23 閲覧）*

[21] *東日本旅客鉄道株式会社「システム不具合による影響及び原因と対策について(2023/6/26)」、https://www.jreast.co.jp/info/2023/20230626_ho04.pdf（2023/8/23 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 1 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	―	―	―	99
関係省庁・関係機関からのNISCへの情報共有	16	16	6	0	0	―	―	―	0
NISCからの情報提供	38	64	91	83	15	―	―	―	15

(※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	―	―	―	9
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	―	―	―	9
	完全性を脅かす事象	情報の破壊	11	12	20	15	5	―	―	―	5
	可用性を脅かす事象	システム等の利用困難	158	157	181	145	56	―	―	―	56
	上記につながる事象	マルウェア等の感染	9	18	46	38	2	―	―	―	2
		不正コード等の実行	5	3	2	1	1	―	―	―	1
		システム等への侵入	14	26	24	22	6	―	―	―	6
		その他	47	42	80	36	11	―	―	―	11

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

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	―	―	―	52
ランサムウェア攻撃	8	13	46	30	8	―	―	―	8
ランサムウェアを除くマルウェア感染	11	8	29	27	2	―	―	―	2
DDoS攻撃等の大量アクセス	14	4	15	25	10	―	―	―	10
その他	54	75	84	61	32	―	―	―	32

(※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

リモートアクセス経路の脆弱性を突かれたランサムウェア攻撃や、DDoS 攻撃含むウェブサイトへの様々な攻撃などサイバー攻撃によりサービス提供に影響が及んだ事例が複数あった。また、引き続き、システム障害が多数発生しており十分なリスクアセスメントを踏まえた上でのシステム構築が求められるとともに、委託先を含む適切な管理が求められる。

○ ネットワーク接続にかかる資産・脆弱性管理及び不正侵入を前提とした多層防御が必要

ランサムウェアの感染により、サービスの提供に支障が出た事例、特に、委託先の感染により影響を受けた事例が複数あった。中には、スタンドアローンで運用している機器のリモートメンテナンス時に感染した事例があり、適切なセキュリティの確保が必要。また、データの暗号化まで至らなかったものの、ランサムウェア攻撃を実行しようとした痕跡及び認証情報を窃取するツールが実行された痕跡が発見された事例があった。今後の攻撃を踏まえ監視強化が必要。

○ ウェブサイト等の公開されているサーバに係る適切な設計と脆弱性等の適切な管理が必要

ウェブサイト等が改ざんされ他の無関係なサイトへのリンクが設定されたり、ウェブの管理機能等の脆弱性をつかれスパムメール送信の踏み台となってしまった事例が複数あった。中には、ブルートフォース攻撃により管理画面の認証情報を窃取された事例もあり、適切な認証・認可の仕組みやアカウントロックアウトの設定など基本的な対策が必要。

○ 攻撃を想定したシステム設計と障害発生時における適切な広報の実施が必要

DDoS 攻撃とみられる大量のアクセスを受けた事例が多数あった。中には、複数の組織が利用するクラウドの DNS に対するランダムサブドメイン攻撃により、当該複数組織のウェブサイトの閲覧やメールの送受信に影響した事例もあった。障害発生時における広報については、代替手段の確保含め適切な対応が必要。

○ ユーザーのリテラシー向上に加えウェブブラウザにおける対策が必要

ウェブサイト閲覧中に偽のサポートからアラートが表示され、記載の連絡先に架電し、遠隔操作される事例が複数あった。組織内システムのユーザーのリテラシー向上と、閲覧ページの制限、広告ブロック等の、ウェブブラウザにおける対策が必要。

○ システムの設計・実装時やメンテナンス時における適切なリスクアセスメントが必要

想定されるリスクの評価を誤ったことに起因するシステム障害が多数発生した。既知のバグについて発生頻度等から影響はないと判断していた結果、予期せぬエラーによりサービス提供に支障が生じた事例や、連休明けのソフトウェアアップデートの通信量の見誤りによりシステム障害が起きた事例などがあった。

○ 委託先を含み、作業手順書の確認など適切な事前準備や管理が必要

作業時における手順のミスや設定ミスに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出た事例が引き続きあった。また、委託先で起きている事例も多数あり、作業の重要度や、作業するシステムに障害が発生した場合のインパクトなどを踏まえて適切に管理を行うことが必要。

以上

資料３関連

報道資料

令和５年８月４日
内閣官房内閣サイバーセキュリティセンター

内閣サイバーセキュリティセンターの電子メール関連システムからのメールデータの漏えいの可能性について

今般、内閣サイバーセキュリティセンター（NISC）の電子メール関連システムに対し、不正通信があり、個人情報を含むメールデータの一部が外部に漏えいした可能性があることが判明しました。

これは、メーカーにおいて確認できていなかった電子メール関連システムに係る機器の脆弱性を原因とするものであると考えられ、同様の事案は国外においても確認されています。

NISC における本事案の経緯及び講じた措置は以下のとおりです。

・６月 13 日　電子メール関連システムに係る不正通信の痕跡を発見。
・６月 14～15 日　当該システムの状況を確認するため、速やかに運用を停止。不正通信の原因と疑われる機器を交換するとともに、他の機器等に異常がないことの確認や、内部監視の強化等の対策を実施の上で、当該システムを再稼働。
・６月 21 日　保守運用事業者の調査により、不正通信が当該機器の脆弱性を原因とするものであることを示す証跡を発見（本事案について個人情報保護委員会に報告）。

これを受けて、外部専門機関等による調査を行った結果、現時点までに、NISC が令和４年 10 月上旬から令和５年６月中旬までの間にインターネット経由で送受信した個人情報を含むメールデータの一部が外部に漏えいした可能性があることが判明したところです。

NISC においては、本事案により、メールアドレス等の個人情報が漏えいした可能性を排除できない方に対して個別に通知するとともに、事案の公表を行うこととしたところです。関係者の皆様には、ご迷惑をおかけすることになり、お詫び申し上げます。

なお、現時点で、具体的な個人情報の漏えい等は不明であり、個人情報の悪用等の被害は確認されていませんが、今後 NISC を装った不審なメールが送付される等の可能性は否定できませんので、ご注意ください。

NISC では、引き続きセキュリティ対策の強化に努めるとともに、セキュリティ関係機関等とも連携しながら、一層の状況把握に努めてまいります。

【お問い合わせ先】
内閣サイバーセキュリティセンター
〇本事案の概要について
基本戦略第１グループ：電話番号 03-6910-0365
〇本事案による個人情報の漏えいの可能性に係るご不明点等について
基本戦略総括グループ：電話番号 03-3581-3768