情報セキュリティ白書

Information Security White Paper

2023

進む技術と未知の世界：新時代の脅威に備えよ

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

「情報セキュリティ白書2023」の刊行にあたって

2022 年を振り返ると、2 月に発生したロシアのウクライナ侵攻は、近隣諸国や支援国、そして食料やエネルギー等の経済的つながりを持つ国々にまで影響を及ぼしました。この紛争は武力戦にサイバー空間を含む情報戦を加えたハイブリッド戦と呼ばれるものとなり、関係各国はランサムウェアを始めとするサイバー攻撃や、世論誘導を意図する虚偽情報拡散等の対応に追われました。米国では CISA、FBI 等によりサイバー攻撃への注意喚起が繰り返されました。日本では、9 月に政府機関や企業のホームページ等を標的とした DDoS 攻撃と思われるサービス不能攻撃により、業務継続に影響のある事案も発生したほか、国家等が背景にあると考えられる攻撃者による暗号資産取引事業者等を狙ったサイバー攻撃や、一定の集団によるものとみられる学術関係者等を標的としたサイバー攻撃も明らかとなり、国民の誰もがサイバー攻撃の懸念に直面することとなりました。政府からも関係省庁等々の合同による注意喚起が多数出されました。

この間、国内では、ランサムウェア攻撃による大きな被害が報告されました。2 月には自動車部品工場が攻撃を受け、出荷先の工場が稼働停止しました。10 月には自治体の医療センターのサーバーが取引先の給食提供業者を経由した攻撃を受け、電子カルテシステムが利用できなくなりました。サプライチェーン全体のセキュリティ対策、事業継続計画、インシデント対応等の重要性が再認識されました。

一方政策面では、「サイバーセキュリティ 2022」「重要インフラのサイバーセキュリティに係る行動計画」「国家安全保障戦略」 等が公表され、サイバー警察局、サイバー特別捜査隊等の設置等が実施されました。6 月に閣議決定された「デジタル社会の実現に向けた重点計画」では、利便性の向上とサイバーセキュリティ確保の両立に向け、官民の緊密な連携を進めていくことが示されました。

そして、2022 年は AI への注目が集まった年でもありました。特に生成系 AI の技術的な発展は目覚ましく、ビジネスにおける業務革新等への期待が高まる一方、AI の利用による人権、プライバシー、知的財産権等の保護が課題として顕在化しました。更にウクライナ侵攻では、虚偽情報生成に AI が利用され、情報の信頼性に対する課題が深刻化しました。このような AI の課題に対して EU では、AI の安全で遵法的な利用に関する規則が策定されました。また米国も「AI 権利章典」を公開して人権や安全に配慮した AI の利用を宣言しました。

AI 利用を起点とする IT 環境の革新は、確かに大きな可能性があるようですが、セキュリティやプライバシーの脅威も大きくなると思われます。では、私達はどうすればよいのでしょうか。

まずはリスクを正しく知ることから始めましょう。何が重大なリスクなのかを特定した上で、変化に対応してセキュリティ対策の基本を継続的に実践していくとともに、未知の脅威に対しては情報共有し、適切な利用について議論を重ね、安全、安心なデジタル社会の実現を目指していくことが重要です。

本白書が、多くの方々に広く利用され、技術の進展とそれに伴う未知の脅威、リスクに対する備えを実践するための一助となることを祈念します。

2023年7月

独立行政法人情報処理推進機構（IPA）

理事長 齋藤 裕

目次

コラム

2023

情報セキュリティ白書

序章

2022年度の情報セキュリティの概況

2022 年はウクライナ侵攻による安全面や経済面の不安が継続する一方、生成系 AI の急激な普及等で IT 環境の革新を予感させる年となった。国内では、企業・団体におけるランサムウェア被害が増え続けた。攻撃の手口では、窃取したデータを暴露する「二重の脅迫」に加え、被害組織への DDoS 攻撃や、被害の事実を被害組織の顧客や利害関係者に連絡する等の脅迫手法も確認されている。ここ数年で被害が急増している要因として、ランサムウェア攻撃をサービスとして提供する「RaaS（Ransomware as a Service）」の普及や、攻撃者の組織化・分業化が挙げられる。2022 年 2 月の自動車部品会社へのランサムウェア攻撃では、部品供給先である自動車工場の稼働が 1 日停止した。同年 10 月の大阪市の医療センターへのランサムウェア攻撃では、VPN でつながる給食提供業者から侵入され、サーバーを介して医療センターの電子カルテシステムに障害が及んだ。同システムはバックアップが保管されていたが復旧に 2 ヵ月を要した。これらの事案から、サプライチェーン全体での脆弱性対策、データ保護、復旧計画の必要性等が再認識された。

情報漏えいの被害について、調査会社の調査によれば、漏えい・紛失事故を公表した社数、事故件数はともに 2 年連続で最多となった。2022 年 6 月には、地方自治体の業務委託先の従業員が、46 万人余りの個人情報を含む USB メモリーを紛失した。USB メモリーは回収され、漏えいの痕跡はないとされたが、記録媒体管理の重要性を再認識させられる事案であった。

個人を狙ったフィッシング等の被害については、2022 年度は通信事業者をかたる偽 SMS が減少した一方、宅配便業者や公的機関をかたる偽 SMS が増加、または新たに出現した。また、パソコン利用者に対する偽のセキュリティ警告について IPA に寄せられた相談件数は過去 4 年間で最多となった。

海外においても、様々なサイバー攻撃の脅威がより深刻になっている。米国連邦捜査局（FBI）の年次報告書によると、2022 年に報告されたビジネスメール詐欺の被害総額は、前年比約 15% 増の約 27 億 4,200 万ドルであった。セキュリティベンダーが 2022 年上半期に全世界で確認した DDoS 攻撃は、過去最多となる約 602 万回で、前年同期比で 205% であった。ランサムウェア攻撃も世界中で起きており、イタリアでは地方行政機関の通信インフラのサービスが全面中断し、フランスでは病院が被害を受け手術の中止や入院患者の移送等、生活や治療に影響を及ぼす被害が報告されている。

セキュリティ政策面では、国内ではサイバー警察局、サイバー特別捜査隊等の体制面の強化、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の公開、業界ごとのサイバー・フィジカル・セキュリティ対策ガイドラインの公開等で、より実践的な対策を推進した。また、経済安全保障推進法や安全保障関連 3 文書の中でもサイバーセキュリティ対策強化の方向性が示された。

世界的には、2022 年 2 月のウクライナ侵攻以降、安全保障面の緊張、エネルギー・食料不足等で予断を許さない状況が続いている。ウクライナでの戦いは、国家間の武力攻撃とサイバー攻撃のハイブリッド戦、及びサイバー空間での情報宣伝戦が特徴となっている。サイバー攻撃について、米国はサイバー軍による諜報面のウクライナ支援、国内におけるサイバー攻撃注意喚起、大統領令 14028 に基づくサプライチェーン防御強化等を継続した。また EU は、重要インフラの統一セキュリティ規格である「NIS 2」を 2022 年 11 月に成立させた。

情報宣伝戦について、ロシアは虚偽情報を多用したが、ウクライナも SNS 等で情報を発信して対抗した。技術面では、生成系 AI の急速な発展や広告配信等の IT 基盤の普及により、虚偽情報の容易な生成・配信が可能となった。虚偽情報の識別は難しく、拡散にどう対応するかは今後の課題である。AI の関連政策として、EU は、AI の安全で遵法的な利用に関する規則「Artificial Intelligence Act」（AI 法）を公表、2023 年 6 月には生成系 AI の利用や学習に関する規制を追加した修正案を採択した。米国は 2022 年 10 月、「AI 権利章典」を公開した。欧米それぞれで人権や安全に関する AI の不適切な利用への対処に進展が見られた。

2022年度の情報セキュリティの概況

	主な情報セキュリティインシデント・事件	主な情報セキュリティ政策・イベント
2022年 4月	● CISA、ロシアのウクライナに対するサイバー攻撃情報開示（2.2.2）	● IPA、「組織における内部不正防止ガイドライン」第5版を公開（2.8.1） ● 警察庁にサイバー警察局、関東管区警察局にサイバー特別捜査隊を新設（2.1.5）
5月		● 「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案」成立（2.1.1） ● 第28回日EU定期首脳協議開催、デジタルパートナーシップ合意（2.2.1）
6月	● 地方自治体の業務委託先が個人情報を保存したUSBメモリーを紛失（1.2.9） ● イタリアの地方行政機関がランサムウェア攻撃でサービス停止（3.1.1）	● G7エルマウサミット開催（2.2.1） ● 「デジタル社会の実現に向けた重点計画」が閣議決定（2.1.1） ● NISC、「重要インフラのサイバーセキュリティに係る行動計画」公開（2.1.1）
7月	● ENISA、ランサムウェア脅威実態を報告（2.2.3）	
8月		● 総務省、「ICTサイバーセキュリティ総合対策2022」公開（2.1.4）
9月	● 親ロシア系攻撃集団、国内組織にDDoS攻撃（1.2.4） ● 家具製造小売業の持株会社が不正アクセスを受け、約13万2,000アカウント分の個人情報が流出（1.2.9）	● IPA、ビジネスメール詐欺の特設ページを開設（1.2.3） ● EU、デジタル製品の「サイバーレジリエンス法案」公開（2.2.3） ● ISMAP-LIU運用開始（2.7.3）
10月	● 大阪府の病院にランサムウェア攻撃、電子カルテシステムに障害が発生（1.2.1） ● 入力フォーム支援サービス事業者のサービスが不正アクセスを受け、入力情報が流出（1.2.9）	● 米国、「AI権利章典」公開（2.2.3）
11月	● IPA、学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について注意喚起（1.2.2） ● 厚生労働省、医療機関等のサイバーセキュリティ対策で注意喚起（2.1.1） ● オーストラリアの保険会社の個人情報970万人分が漏えい（1.1.1）	● 経済産業省、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」公開（2.1.3） ● EUの重要インフラの統一セキュリティ規格「NIS 2」が成立（2.2.3） ● EU、AI法修正案を公開（2.2.3）
12月	● フランスの病院がランサムウェア攻撃により患者を緊急移送（3.1.1）	● 安全保障関連3文書が閣議決定（2.1.1） ● 米国、国防授権法2023成立（2.2.2）
2023年 1月	● 保険会社の委託先に不正アクセス、顧客情報が流出（1.2.9） ● 米国ソーシャルテクノロジー企業にGDPR違反で3億9,000万ユーロの制裁金（2.2.3）	● 経済産業省、「クレジットカード決済システムのセキュリティ対策強化検討会 報告書」公開（2.1.3）
2月		● 日米豪印の4ヵ国（QUAD）で連携したサイバーセキュリティ月間実施（2.1.1）
3月	● IPA、Emotetの攻撃活動再開を観測（1.2.6）	● 経済産業省、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」公開（2.1.1、2.1.3） ● IPA、「サイバーセキュリティ経営ガイドライン」改訂（2.1.3） ● 米国、新サイバーセキュリティ戦略を公開（2.2.2）

※ 2022年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。ランサムウェア攻撃、標的型攻撃、ビジネスメール詐欺、DDoS攻撃、Web改ざん、フィッシング等の被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照されたい。

第3章
個別テーマ

本章では個別テーマとして、制御システム、IoT、クラウドのセキュリティについて、インシデントや攻撃の実態、脆弱性や脅威の動向、国の施策や対策状況等を解説する。また、米国大統領選挙の妨害活動や新型コロナウイルスのインフォデミック、ウクライナ侵攻に関連したサイバー情報戦等における、Disinformation やフェイクニュースといった虚偽情報の生成と拡散について、事例や脅威、その対策を取り上げた。

3.1 制御システムの情報セキュリティ

制御システム（ICS：Industrial Control System）は、電力、ガス、水道、輸送・物流、製造ライン等、我々の生活を支える重要インフラ※1を管理し、制御するシステムである。従来、制御システムの多くは独立したネットワーク、固有のプロトコル、事業者ごとに異なる仕様で構築・運用されており、外部からサイバー攻撃を行うことは困難と考えられていた。しかし、近年、ネットワーク化やオープン化（標準プロトコル・汎用製品の利用）が進んだこと、10 ～ 20 年に及ぶライフサイクルの長さ故に、外部との接続やサイバー攻撃を想定していない制御システムが今なお多数稼働していること、攻撃者にとって価値の高い標的であること、地政学的緊張の高まり等から、制御システムに対するサイバー脅威は年々高まっている。また、実際に社会経済活動に大規模な被害が出たインシデントが世界各地で相次いで発生している。

本節では、制御システムのセキュリティの動向と主な取り組みについて述べる。

3.1.1 インシデントの発生状況と動向

調査会社による制御システムユーザー等へのアンケート調査において、2021 年同様、2022 年も制御システムへの侵入や運用障害が発生したという回答が一定数以上あった。

例えば、米国、ドイツ、日本の製造、電力、石油・ガス業界の従業員 1,000 人以上の組織に所属する IT 及び制御・運用技術（OT：Operational Technology）の専門家 900 名を対象とした調査結果では、回答者の 89% が、過去 12 ヵ月間にサイバー攻撃によって生産またはエネルギー供給が影響を受けた、と回答している。そのうち 56% が、制御システム及び OT システムの運用が 4 日以上停止する被害に至った、と回答している※2。米国、欧州 12 ヵ国、オーストラリアの政府、製造、エネルギー、通信、建設、農業、医療等の様々な分野の IIoT（Industrial Internet of Things）及び OT 担当者 800 名を対象とした調査結果では、回答者の 94% が、過去 12 ヵ月間にセキュリティインシデントを経験し、そのうちの 87% は、1 日以上業務が影響を受けた、と回答している※3。

2022 年に公になった重要インフラ分野のインシデントには、ロシアのウクライナ侵攻に伴うサイバー攻撃、重要インフラの制御システムを侵害した攻撃、生産や重要サービスに影響を与えたサイバー攻撃、政府や自治体を標的とした攻撃、医療機関への攻撃、ウイルス※4に感染した USB メモリーやパソコンを接続することによる侵害、という六つの特徴が見られた。以下、この六つの特徴について述べる。

（1）ロシアのウクライナ侵攻に伴うサイバー攻撃

2022 年 2 月 24 日のロシアのウクライナ侵攻に伴い、両国及び支援国におけるサイバー攻撃が増加した。

侵攻初日、米国の大手衛星通信事業者 Viasat, Inc. の通信衛星 KA-SAT の消費者向け衛星ブロードバンドサービスがサイバー攻撃を受け、欧州全土の多くのユーザーがインターネットにアクセスできなくなった※5。攻撃者は、VPN 機器の設定ミスを悪用して地上の管理ネットワークに侵入し、多くの住宅用モデムに対して破壊的な管理コマンドを実行した※6。結果として何万台ものモデムが KA-SAT ネットワークから切断され、再接続できなくなった。また、この障害によって、ドイツの Enercon GmbH 製風力タービン 5,800 基の遠隔監視及び制御に障害が

発生した※7。

全球測位衛星システム（GNSS：Global Navigation Satellite System）信号に対する妨害も増加した。欧州航空安全機関（EASA：European Union Aviation Safety Agency）が2022年3月17日に発行した安全情報公報によると、カリーニングラード地域、バルト海周辺及び近隣諸国、フィンランド東部、黒海、東地中海地域で、GNSSのスプーフィング（なりすまし）やジャミング（電波妨害）が増加した※8。エストニアの首都タリンからフィンランド南東部のサヴォンリンナへの航空機は、3日間運行できなくなった※9。

(2) 重要インフラの制御システムが侵害された事例

2022年も引き続き、重要インフラの制御システムが侵害されたインシデントが世界各地で発生した。

2022年6月27日、イランの鉄鋼会社3社がサイバー攻撃を受けた。被害企業の一つであるKhouzestan Steel Companyでは、Siemens AGのプロセス制御システムSIMATIC PCS7が侵害され、攻撃者は、工場の床に溶鋼が噴出した監視カメラの映像、及び制御システムのスクリーンショットをSNSに投稿した。同社の生産ラインは数日間停止した※10。

2022年8月15日、英国イングランド中部の小規模水道事業者South Staffordshire Water PLCの親会社South Staffordshire PLCが、ランサムウェア攻撃グループによる攻撃を受けた※11。セーフティシステムや配水システムは正常に稼働し続け、160万人に毎日3億3,000万リットル供給している水の供給と品質には影響はなかったが、攻撃者は同社業務を監視・制御するために使用されているSCADA（Supervisory Control And Data Acquisition）システムの文書及び2枚のスクリーンショットを公開し、水道水の化学物質のレベルを操作できた、と主張した。

また、2022年9月、イスラエルの複数組織で使用されているBerghof Automation GmbHのPLC（Programmable Logic Controller）55台が侵害された。攻撃者は、PLCの管理パネルへのログインに成功したことを示す動画と、PLCの遮断を含む攻撃の一部の段階を示すHMI（Human Machine Interface）画面のスクリーンショットを公開した。管理パネルからはプロセスにある程度影響を与えることは可能であるが、実際のプロセス設定は管理パネルからだけでは不可能であった。攻撃者はデフォルトの認証情報を使用して、PLCの管理パネルにアクセスしたと考えられており、この事例は、インターネットへの資産の公開を禁止し、パスワードポリシーの徹底、特にデフォルトのログイン情報を変更することで防ぐことが可能であった※12。

(3) 生産や重要サービスに影響を与えたサイバー攻撃の事例

制御システムにおいて最も重要視される「可用性（Availability）」に影響を与えたインシデントも、世界中で相次いだ。

表3-1-1に、2022年に公にされた、生産や重要サービ

被害企業	発生国	発生年月（報道年月）	内容・影響・被害
大手農業機械メーカー	米国	2022年5月	ランサムウェアによる攻撃を受け、一部の生産施設が影響を受けた※13。
航空会社	インド	2022年5月	ランサムウェアによる攻撃を受け、一部のシステムが影響を受け、航空機の運行に遅延が発生した※14。
電子機器受託生産大手	メキシコ	2022年5月	生産施設の一つがランサムウェアによる攻撃を受け、停止した※15。
自動車用ホース製造会社	米国	2022年6月	ランサムウェアによる攻撃を受け、ネットワーク及び生産管理システムが停止した※16。
新聞社	ドイツ	2022年10月	ランサムウェアによる攻撃を受け、印刷システムが機能しなくなったため、紙の新聞を発行できず、電子版を発行した※17。
鉄道会社	デンマーク	2022年11月	鉄道会社にITサービスを提供しているプロバイダーがサイバー攻撃を受け、サーバーをシャットダウンした。運転士に制限速度や鉄道のメンテナンス等の運行上重要な情報を提供しているソフトウェアが使用できなくなった※18。
複数の消防署を運営する会社	オーストラリア	2022年12月	サイバー攻撃を受け、予防措置としてネットワーク全体をシャットダウンした。「広範囲なIT機能停止」が発生し、メール、電話、及び消防士の仕事を自動化する緊急通報システムが影響を受けた※19。
鉱業会社	カナダ	2022年12月	本社オフィスのITシステムがランサムウェアによる攻撃を受け、制御システムへの影響を判断するための予防措置として、鉱山の操業を停止した※20。

■表3-1-1　2022年に公にされた、生産や重要サービスに影響を与えたサイバー攻撃のインシデント事例

スに影響を与えたサイバー攻撃のインシデント事例を示す。

(4) 政府や自治体が標的となった事例

政府や自治体を標的としたサイバー攻撃も、世界中で相次いだ。攻撃によって、重要なサービスの機能停止や情報の漏えいといった影響が発生している。

表 3-1-2 に、2022 年に公にされた、政府や自治体が標的となったインシデント事例を示す。

(5) 医療機関が標的となった事例

医療機関を標的としたサイバー攻撃も、世界中で相次いだ。医療機関のコンピューターがランサムウェアに感染すると、保有している情報資産（データ等）が暗号化され、電子カルテシステムが利用できなくなり診療に支障が生じたり、患者の個人情報が窃取されたりする等の深刻な被害をもたらす可能性がある。最悪の場合は、人命に関わる（国内の事例については「1.2.1 (2) (b) 医療機関における被害事例」参照）。

インシデントの一例としては、2022 年 12 月、フランスの病院 Hospital Centre of Versailles がランサムウェアによる攻撃を受け、コンピューターシステムがダウンした。手術が中止され、患者 6 名（集中治療室の 3 名、新生児室の 3 名）が他の病院に移送された※31。

米国の医療機関の IT 及びセキュリティ担当者 641 名を対象に実施した調査によると、調査対象組織の 89% が過去 12 ヵ月間に平均 43 回と、ほぼ 1 週間に 1 回の割合でサイバー攻撃を受けていた。また、最も一般的な 4 種類の攻撃（クラウドの侵害、ランサムウェア攻撃、サプライチェーン攻撃、ビジネスメール詐欺（BEC）／スプーフィング／フィッシング）にあった組織の 20% 以上が、患者の死亡率の上昇を経験していた※32。

国内では、厚生労働省が、「医療情報システムの安全管理に関するガイドライン 第 5.2 版」を 2022 年 3 月に策定した※33。また、医療機関等におけるサイバーセキュリティ対策の強化について、2022 年 11 月に注意喚起を行っている※34（「2.1.1 (2) 国民が安全で安心して暮らせるデジタル社会の実現」参照）。

(6) ウイルスに感染した USB メモリーやパソコンを接続することによる侵害

業務用に持ち込んだ USB メモリーやパソコンを接続することによるウイルス感染も、継続して発生している。

Honeywell International Inc. のレポート「Industrial Cybersecurity USB Threat Report 2022※35」によると、USB メモリーを悪用する脅威は、同社が世界中の生産施設で検知・ブロックした脅威のうち 52% を占め、2021 年の 37% から増加している。また、SANS Institute のレポート「The State of ICS/OT Cybersecurity in 2022 and Beyond※36」によると、制御システム及び OT のセキュリティインシデントにおける最初の攻撃手段で最

発生国・地域	発生年月（報道年月）	内容・影響・被害
フィンランド	2022 年 4 月	国防省と外務省の Web サイトが DoS 攻撃を受けてダウンし、1 時間後に復旧した※21。
イタリア	2022 年 6 月	シチリア州の州都パレルモの行政機関においてランサムウェアによる攻撃によりデータセンターの情報通信インフラが影響を受け、サービスが全面中断した※22。
ノルウェー	2022 年 6 月	政府の公共サービスポータルが DDoS 攻撃を受け、重要な Web サイトやオンラインサービスの一部がアクセス不能となった※23。
アルバニア	2022 年 7 月	政府の電子サービスがランサムウェア及びデータを破壊するワイパー型ウイルスによる攻撃を受け、首相と議会の Web サイト、及び政府の電子サービスポータルサイトがオフラインとなった※24。
モンテネグロ	2022 年 8 月	政府のデジタルインフラがサイバー攻撃を受け、公共サービス提供会社（電力・ガス・水道等）、交通機関（国境通過、空港を含む）、通信分野が影響を受けた※25。
台湾	2022 年 8 月	総統府、外務省、その他の政府ポータルの Web サイトが DDoS 攻撃を受け、断続的に機能が停止した※26。
チリ	2022 年 9 月	政府機関が運用する Microsoft Windows サーバー及び Linux VMware ESXi マシンがランサムウェアによる攻撃を受け、政府機関の業務及びオンラインサービスが影響を受けた※27。
バヌアツ	2022 年 11 月	ランサムウェアによる攻撃を受け、政府のサーバー及び Web サイトがダウンした※28。
ニュージーランド	2022 年 12 月	マネージドサービスプロバイダーがランサムウェアによる攻撃を受け、複数の政府機関や公的機関を含む国内の数十の組織が影響を受けた※29。
ベルギー	2022 年 12 月	アントワープ市の行政ソフトウェアを提供する企業のサーバーがランサムウェアによる攻撃を受け、市のデジタルサービスが影響を受け、パスポートや ID カード情報を含むデータ 557GB が窃取された※30。

■表 3-1-2　2022 年に公にされた、政府や自治体が標的となったインシデント事例

も多かったのは「IT の侵害」(40.8%) だったが、次いで多かったのが「リムーバブルメディアを介した侵害」(36.7%) だった。

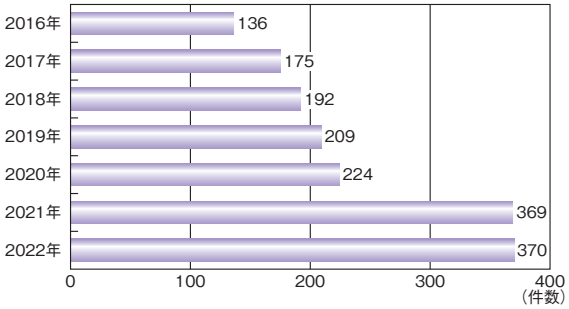
組織は、外部から持ち込む情報端末・機器や媒体に対する明確なセキュリティポリシーを確立し、管理策を策定し、継続的に取り組むことが重要である。

3.1.2 脆弱性及び脅威の動向

本項では、2022 年に見られた、制御システムの脆弱性及び脅威の動向について述べる。

(1) 脆弱性の動向

2022 年も、制御システムの脆弱性が多く公開された。制御システムの脆弱性情報を収集・公開している代表的な組織である米国国土安全保障省 (DHS: Department of Homeland Security) の NCCIC (National Cybersecurity and Communications Integration Center) が、2022 年に公開したアドバイザリーは 370 件で、2021 年の 369 件から横ばいであった (図 3-1-1)。一方で、アドバイザリーで特定された共通脆弱性識別子 CVE (Common Vulnerabilities and Exposures) の件数は 613 件から 778 件へと増加しており、分野別に見ると、基幹製造業に影響を与える可能性があるものが最も多く、次いで、エネルギー、上下水道、医療、交通システムだった※37。



■図 3-1-1 NCCIC が公開した脆弱性アドバイザリーの件数 (2016～2022 年)
(出典) NCCIC の公開情報※38 を基に IPA が作成

非常に影響の大きい脆弱性及び脆弱性を悪用した攻撃手法も発見されている。以下では、それらについて解説する。

(a) Access:7

Axeda Corporation (現、Parametric Technology Corporation (以下、PTC 社) の一部門) の医療機器及び IoT 機器の遠隔管理ツール Axeda に七つの深刻な脆弱性「Access:7」が発見された。Axeda は、機器の機械やセンサー等のネットワークに接続された機器に製造業者が遠隔でアクセスし、管理できるように設計されている。これらの脆弱性を悪用すると、標的となる機器にネットワーク経由でアクセスできる攻撃者が、遠隔でコードを実行したり、ファイルシステムにアクセスしたり、システム設定を変更したりすることが可能となる。これらの脆弱性によって、100 社以上のベンダーの 150 種以上の機器が影響を受け、それらの機器のベンダーの大半は医療分野 (55%) で、次いで、IoT (24%)、IT (8%)、金融サービス (5%)、製造業 (4%) となっている。Axeda は製造終了となっているが、PTC 社は修正プログラム及び緩和策や回避策を公開している※39 (脆弱性の詳細については「3.2.3 (1) (b) Access:7」参照)。

(b) OT:ICEFALL

米国のサイバーセキュリティ企業 Forescout Technologies, Inc. は、世界的なメーカー 10 社の OT システムに、56 件の脆弱性を発見した※40。「OT:ICEFALL」と総称されたこれらの脆弱性は、世界中の同社顧客の OT 機器だけで、少なくとも 3 万台以上の機器、324 の組織に影響するという。56 件の脆弱性のうち、38% はユーザーのログイン認証情報を侵害するために悪用される可能性があり、21% は悪用された場合、不正侵入者がファームウェアを操作でき、14% は遠隔でのコード実行が可能になる。これらの脆弱性の中には、共通脆弱性評価システム CVSS (Common Vulnerability Scoring System) の深刻度スコア (最大値 10.0) が 9.8 と高いものもある。影響を受ける機器は、石油・ガス、化学、原子力、発電・配電、製造、水処理・配水、鉱業、建築、オートメーション等の重要インフラで使用されており、悪用されると、電気や水道の停止、食糧供給の停止、成分の比率が変更されて有毒な混合物が生成される等の可能性がある。

(c) Evil PLC 攻撃

イスラエルのサイバーセキュリティ企業 Claroty Ltd. は、PLC を武器化し、エンジニアリングワークステーションに最初の足場を築き、OT ネットワークに侵入する新たな攻撃手法に関する研究論文を発表した※41。「Evil PLC」と名付けられたこの攻撃は、まず攻撃者が、インターネットに接続された PLC に故意に誤動作を誘発する。これに対処するエンジニアは、エンジニアリングワー

クステーション（EWS）ソフトウェアをトラブルシューティングツールとして使用し、侵害されたPLCに接続する。エンジニアが既存のPLCロジックの作業コピーを取得するためにアップロード操作を行うと、攻撃者はEWSソフトウェアの脆弱性を悪用して、ワークステーション上で悪意のあるコードを実行し、OTネットワーク上の他の機器（他のPLCを含む）にアクセスする。同社は、この攻撃で悪用される脆弱性のあるEWSソフトウェアのベンダー7社に報告し、ほとんどのベンダーは修正プログラム、パッチ、または緩和策を公開した。

(2) 脅威の動向

2022年の脅威の動向としては、2021年に引き続き、ランサムウェアによる攻撃の増加が挙げられる。

米国のサイバーセキュリティ企業Dragos, Inc.（以下、Dragos社）が2022年に追跡調査した、産業組織に対するランサムウェア攻撃は605件で、2021年から87%増加している[※42]。攻撃の72%が製造分野、9%が食品及び飲料分野、5%がエネルギー分野、4%が医薬品分野、3%が石油・天然ガス分野を標的としていた。

ランサムウェアの脅威への対策として、基本的なウイルス対策、通信制御による対策、重要なデータのバックアップが適切に実施されているかの確認等、感染や脅迫に備えたリスク管理対策を徹底することが推奨される。

また、2022年には、制御システムを標的とする新たなウイルスが二つ確認された。

(a) Industroyer2

スロバキアのサイバーセキュリティ企業ESET, spol. s r.o.が、ウクライナのコンピューター緊急対応チーム（CERT-UA）と共同で、ウクライナのエネルギー企業に対する2022年4月の攻撃を分析したところ、ワイパー型ウイルスとともに、2016年にウクライナで大規模停電を引き起こした、制御システムを標的としたウイルス「Industroyer」（「Crash Override」とも呼ばれる）[※43]をカスタマイズした新バージョン「Industroyer2」を発見した[※44]。攻撃者はウクライナの高圧変電所に「Industroyer2」を展開しようとしていたが、同社とCERT-UAはこの攻撃を阻止した。

(b) Pipedream/Incontroller

米国の連邦捜査局（FBI：Federal Bureau of Investigation）、DHSのサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA：Cybersecurity and Infrastructure Security Agency）、米国家安全保障局（NSA:National Security Agency）、及びエネルギー省（DOE：Department of Energy）は、複数の制御システム及びSCADA機器へフルアクセスできる攻撃ツールセットに関する共同サイバーセキュリティアドバイザリーを2022年4月13日に発表した[※45]。このツールセットをDragos社は「Pipedream」[※46]、脅威情報及びインシデント対応企業Mandiant, Inc.は「Incontroller」[※47]と命名した。「Pipedream/Incontroller」は、モジュール式の制御システム攻撃フレームワークとカスタムメイドの攻撃ツールセットで、低スキルのサイバー攻撃者が、高度なスキルを持った攻撃者を模倣した操作を実施することを可能にする。こうした攻撃から制御システム及びSCADA機器を保護するための対策として、制御システムのネットワークへのリモートアクセスに多要素認証を導入すること、制御システム及びSCADA機器とシステムのデフォルトパスワードを変更すること、OT監視ソリューションを使って悪意のある行動や攻撃の指標を検知すること等が推奨されている。

3.1.3 海外の制御システムのセキュリティ強化の取り組み

本項では、海外における制御システムを含む、重要インフラサービスのセキュリティ強化に関する取り組みについて述べる。

(1) 米国CISAの取り組み

重要インフラ部門にサイバーセキュリティインシデントや身代金の支払いをCISAに報告することを義務付ける規則を、CISAが策定し実施するよう指示した法律「Cyber Incident Reporting for Critical Infrastructure Act of 2022（CIRCIA）[※48]」が、2022年3月に制定された。CISAは規則の策定にあたって、2022年9月12日から11月14日までパブリックコメントを募集した。

米国のJoseph Biden大統領が2021年7月に署名した、重要インフラの制御システムのためのサイバーセキュリティの改善に関する国家安全保障に関する覚書[※49]では、CISAが米国国立標準技術研究所（NIST：National Institute of Standards and Technology）及び省庁間コミュニティと連携して、すべての重要インフラ部門に一貫性のあるサイバーセキュリティの基本パフォーマンス目標を策定することを要求しており、これに応じて、CISAは「Cross-Sector Cybersecurity Performance Goals（CPGs）」を2022年11月に発表した[※50]。CPGsは、重要インフラ部門全体の最も一般的で影響の大きい

いくつかのサイバーリスクを軽減することを目的としており、明確に定義され、簡単に実施でき、取り掛かりやすい、優先順位付けされたセキュリティプラクティスを提供している。

(2) 米国 Biden 政権の取り組み

米国の Biden 政権は、重要インフラ事業者と政府の連携を推進する「産業用制御システムサイバーセキュリティイニシアティブ」を 2021 年 7 月に立ち上げ、米国内の 16 の重要インフラ部門において、1 部門ずつサイバー対策を強化する 100 日間の取り組みを実施している。これまで電力、石油・ガス部門を対象に実施してきたが、2022 年 1 月 27 日に水道部門※51、2022 年 10 月 26 日に化学部門を対象とした取り組みを開始した※52。

NIST は、産業用制御システム環境のサイバーセキュリティを向上させる支援に焦点を当てたガイダンス SP1800-10「Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector」を 2022 年 3 月に公開した※53。本ガイダンスは、一般的な攻撃シナリオを説明し、破壊的なウイルス、内部脅威、不正なソフトウェア、不正なリモートアクセス、異常なネットワークトラフィック、履歴データの損失、不正なシステム変更等から制御システムを保護するために、製造業者が実施可能なソリューションの例を示している※54。

NIST の National Cybersecurity Center of Excellence（NCCoE）は、ハイブリッド衛星ネットワーク向けのサイバーセキュリティフレームワークプロファイルを 2022 年 11 月に公開した※55。本プロファイルは、PNT（Positioning, Navigation and Timing：測位、ナビゲーション、タイミング）、リモートセンシング、気象観測、画像処理のための衛星ベースのシステム等のサービスを提供するハイブリッド衛星ネットワークのサイバーセキュリティ体制を評価する手法を識別することを目的としている。

DOE は、エネルギー業界と電力網へのサイバー脅威に対するエンジニアリング、トレーニング、ツール、実践の枠組みの提供に焦点を当てた戦略「National Cyber-Informed Engineering Strategy（CIE）」を 2022 年 6 月 15 日に発表した。この新戦略は、認識、教育、開発、現在のインフラ、将来のインフラの五つの柱で構成されている※56。

運輸保安庁（TSA：Transportation Security Administration）は、旅客・貨物鉄道事業者に対し、パフォーマンスベースの対策に重点を置いてサイバーセキュリティのレジリエンスを強化するよう求めるサイバーセキュリティ指令を、2022 年 10 月 18 日に発表した（10 月 24 日から 1 年間有効）※57。本指令は、CISA や運輸省（DOT：Department of Transportation）の連邦鉄道局（FRA：Federal Railroad Administration）等、業界関係者や連邦政府のパートナーからの幅広い意見に従って作成された。

(3) 欧州連合（EU）の取り組み

欧州議会（European Parliament）は、「ネットワークと情報システムのセキュリティに関する指令（NIS 指令）」（NIS Directive：Network and Information Systems Directive）を置き換える新たなサイバーセキュリティ指令（NIS 2）を 2022 年 11 月に採択した※58。本指令は、重要な分野で活動する中・大規模組織を対象とし、公共電子通信サービス、デジタルサービス、廃水・廃棄物管理、重要製品の製造、郵便・宅配便サービス、医療、行政等のプロバイダーが含まれている。また、新たな条項には、重大なインシデントの認知から 24 時間以内に、欧州連合（EU：European Union）全体に「早期警告」を提出し、その後 72 時間以内にインシデント通知を行う義務、ソフトウェアの脆弱性にパッチを当てること、リスク管理策を準備すること、が含まれている。更に、より厳格な実施要件を設け、加盟国間の制裁体制を一致させることも目的としており、重要なサービスを提供する事業者は、これに従わなかった場合、制裁金を科される。本指令は、欧州委員会（European Commission）でも正式に採択された。この後、加盟国は 21 ヵ月以内に新しい要件を国内法に反映させる必要がある（「2.2.3 (3) (a) 重要インフラのセキュリティ規格改定」参照）。

(4) 英国政府の取り組み

英国デジタル・文化・メディア・スポーツ省（DCMS：Department for Digital, Culture, Media & Sport）は、ブロードバンド及び携帯通信事業者に対し、サイバー攻撃に対するネットワークセキュリティの強化を求める新たな規則を、2022 年 8 月に発表した※59。この規則は 3 年以上かけて策定され、ネットワークの構築と運用だけでなく、その上で実行されるサービスも対象とする包括的なものである。新しい要件は、公衆電気通信ネットワーク及びサービスのプロバイダーがインフラやサービスを調達する方法（及び調達先）、活動やアクセスを監視する方法、セキュリティやデータ保護への投資とそれを監視する方法、データ漏えいやネットワーク停止の結果を関

係者に通知する方法等を対象としている。違反した場合、年間収益の最大 10% の罰金が、違反が続くと 1 日あたり 10 万ポンド（約 1,600 万円）の罰金が科されるとしている。通信規制当局の英国情報通信庁（Ofcom：Office of Communications）は、英国サイバーセキュリティセンター（NCSC：National Cyber Security Centre）と協力して、新たな規制と実践規範を策定し、それを執行し罰金を科す。この規則は 2022 年 10 月から導入され、通信事業者は 2024 年 3 月までに新しい手続きを完全に実施することが求められている。

(5) オーストラリア政府の取り組み

オーストラリア連邦議会は、重要インフラ部門のセキュリティとレジリエンス力を強化し、オーストラリア国民が依存する重要なサービスを物理的、サプライチェーン、サイバー、人的な脅威から保護するための法律「Security Legislation Amendment（Critical Infrastructure Protection）Bill 2022」（SLACIP 法）を 2022 年 3 月 31 日に可決し、同法律は 2022 年 4 月 2 日に施行された[※60]。本法律によって、重要インフラ資産の所有者と運営者がリスク管理プログラムを作成・維持する義務と、国家的な重要性を有するシステムまたは重要インフラ資産の運用者に求められるサイバーセキュリティ義務強化のための新たな枠組みが導入される。SLACIP 法は、「重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）」改正の第 2 部にあたるもので、第 1 部は「Security Legislation Amendment（Critical Infrastructure）Bill 2021」として制定され、2021 年 12 月 2 日に施行された。

3.1.4 国内の制御システムのセキュリティ強化の取り組み

本項では、制御システムを含む、重要インフラサービスのセキュリティ強化に関する国内の主な取り組みの概要を紹介する。

(1) 日本政府の取り組み

包括的な重要インフラのセキュリティ政策については、「2.1.1 政府全体の政策動向」及び「2.1.3 経済産業省の政策」で取り上げているので、そちらを参照されたい。ここでは特に、制御システムのセキュリティ強化に関連する取り組みについて触れる。

内閣官房情報セキュリティセンター（NISC：National Information Security Center）が、2021 年度における我が国を取り巻くサイバーセキュリティに関する情勢、及び自由、公正かつ安全なサイバー空間実現のために取り組む施策の実施状況等をまとめた「サイバーセキュリティ 2022（2021 年度年次報告・2022 年度年次計画）[※61]」を 2022 年 6 月に発表した。NISC の重要インフラグループは、重要インフラの情報セキュリティ対策を推進するため、2018 年策定の「サイバーセキュリティ戦略」及び 2017 年策定の「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[※62]」に基づき、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化、の五つの施策を進めており、「重要インフラのサイバーセキュリティに係る行動計画[※63]」を 2022 年 6 月に発表した。

経済産業省は、業界団体や企業が自らの工場を取り巻く環境を整理し、必要な工場のセキュリティ対策を企画・実行していく際に役立つガイドライン「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0」を 2022 年 11 月に策定した[※64]。

経済産業省と IPA 産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）は、米国政府（CISA、DOE、国務省（DOS: United States Department of State）、アイダホ国立研究所（INL：Idaho National Laboratory））及び EU 政府（欧州委員会通信ネットワーク・コンテンツ・技術総局）と連携し、2022 年 10 月 24 ～ 28 日まで、日米 EU の専門家による制御システムのサイバーセキュリティに関する人材育成イベント「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施した[※65]（「2.2.1 (5) (d) インド太平洋地域に向けたサイバー演習」参照）。2018 年に開始され、4 回目となるこのイベントでは、インド太平洋地域の重要インフラ事業者や国の CSIRT（Computer Security Incident Response Team）における OT・IT のサイバーセキュリティ担当者や、関連する政府機関の政策担当者を対象として、ハンズオン演習が行われた。

「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）」が 2022 年 5 月 11 日に成立し、同月 18 日に公布された[※66]（「2.1.1 (5) 経済安全保障推進法の制定」参照）。本法律は四つの柱で構成され、その一つとして、電気、ガス、水道、通信、鉄道等の基幹インフラサービスが安定的に提供されるよう、重要インフラ企業のサイバーセキュリティを確保するための制度が導入される。例えば、重要インフラ企業は、インフラサービスの提供に重要なシステム

（ハードウェア・ソフトウェア）を導入する場合、事前に政府に届け出て審査を受ける必要がある。2024 年 2 月までに本制度の適用が開始される予定となっている。

(2) IPA の取り組み

2022 年度、IPA では制御システムのセキュリティに関して、大きく三つの取り組みを行った。

(a) 制御システムのセキュリティリスクアセスメント普及活動

制御システムに対するセキュリティリスクアセスメントの普及を目的として、「制御システムのセキュリティリスク分析ガイド」（以下、リスク分析ガイド）※67 を用いてリスク分析手法を解説するオンラインセミナーを、2022 年 6 ～ 9 月と 2022 年 12 月～ 2023 年 3 月の 2 回開催した。同セミナーでは、約 500 社・団体の受講者が、リスク分析ガイドを解説した合計約 3 時間の講義動画の視聴や、電子メールによる質疑応答を行った。

また、国内の重要インフラ業界のセキュリティ対策の支援を目的として、「スマート工場のセキュリティリスク分析調査」調査報告書を 2022 年 6 月に公開した※68。本調査は、IoT 機器（LPWA（Low Power Wide Area）、Wi-Fi 等の無線を含む）、クラウド、AI・ビッグデータ活用等により、生産性、設備稼働率、品質及び保守性等の向上を図る「スマート工場化」を検討中または実施中の企業が、スマート工場化に伴って発生するセキュリティリスクを正しく把握し、対策しやすくすることを目的として実施された。

(b) 制御システム向け侵入検知製品の実装技術の調査報告書の公開

制御システムを保有する事業者のセキュリティ対策支援を目的として、「産業用制御システム向け侵入検知製品の実装技術の調査」調査報告書を 2022 年 9 月に公開した※69。本報告書は、制御システムに侵入検知製品導入を検討しようとしている事業者において円滑な導入方法や有効な運用方法等、導入に役立つ情報を提供している。

(c) 制御システムのサイバーセキュリティ人材の育成

ICSCoE では、模擬プラントを用いた演習や、攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析等を通じて、社会インフラ・産業基盤のサイバーセキュリティリスクに対応する人材の育成を支援している（「2.3.3 (2) 産業サイバーセキュリティ人材育成のための活動」参照）。

3.2 IoTの情報セキュリティ

IoT（Internet of Things）技術の普及とともに、セキュリティ設定が不十分なまま、あるいは脆弱性を有したままインターネットに接続されたコンピューター以外の機器（IoT機器）が増大することにより、サイバー攻撃の対象となる脅威が拡大傾向にある。2022年2月24日に開始されたロシアによるウクライナ侵攻の前後において、ウクライナ及びロシア双方のWebサイトへのDDoS（Distributed Denial of Service）攻撃が観測されているが、本攻撃にIoT機器によるボットネットが悪用されていることが報告されている※70。日本国内においても、2022年4月以降、韓国製DVR/NVR（Digital Video Recorder/Network Video Recorder）のウイルス感染の急増が観測されている※71。

本節では、「IoTに対するセキュリティ脅威の動向」「進化の止まらないIoTウイルスの動向」「IoTセキュリティのサプライチェーンとEOLのリスク」「脆弱なIoT機器のウイルス感染と感染機器悪用の実態」「各国のセキュリティ対策強化の取り組み」について述べる。

なお、本節で記載される脆弱性のうち、脆弱性データベースの登録IDを記載しているものについては、表3-2-1に記載の各データベースで検索することによって、概要、詳細情報、関連情報へのリンク等を確認できる。

登録IDの表記例	登録先データベース
CVE-20xx-xxxxx	NVD※72
JVNDB-20xx-xxxxxx	JVN iPedia※73
EDB-ID: xxxxx	Exploit Database※74

■表3-2-1　脆弱性の登録IDの表記例と登録先データベース

3.2.1 IoTに対するセキュリティ脅威の動向

2022年はルーター、DVR/NVRに加えて、NAS（Network Attached Storage）に対する脅威が多く観測された。本項では、サイバー攻撃対象のIoT機器及びそれらにより構成されるシステムの観点から、2022年に観測されたセキュリティ脅威の動向を紹介する。

(1) NASに対する脅威

NASの脆弱性を狙い、ランサムウェアの感染を試みる脅威が増加した。ベンダーとエンドユーザーの両方に身代金を要求する悪質なケースも発生している。

(a) QNAP社製NASに対する脅威

QNAP Systems, Inc.（威聯通科技股份有限公司。以下、QNAP社）は、同社製NASを狙う脅威に対して積極的にサポートを提供し、2022年をとおして対応に追われた。表3-2-2に主な脅威とその対応を示す。

月日	脅威と対応
1/7	QNAP社がインターネットに接続されたNASを保護するための設定手順を説明※75
1/26	QNAP社がランサムウェアDeadBoltによるゼロデイ攻撃対策として、セキュリティ設定とファームウェア更新を推奨※76
2/14	QNAP社が一部の生産終了モデルのテクニカルサポートとセキュリティ更新の延長を発表※77
3/14	QNAP社がLinuxカーネルの脆弱性Dirty Pipe※78（CVE-2022-0847）に対するアドバイザリーを公表※79
3/29	QNAP社がOpenSSLの無限ループの脆弱性（CVE-2022-0778（JVNDB-2022-001476））に対するアドバイザリーを公表※80
4/20	QNAP社がApache HTTP Serverの複数の脆弱性（CVE-2022-22719、CVE-2022-22720、CVE-2022-22721、CVE-2022-23943（JVNDB-2022-001478～001481））に対するアドバイザリーを公表※81
4/25	QNAP社がNetatalkの複数の脆弱性に対するアドバイザリーを公表※82
6/17	QNAP社がランサムウェアDeadBoltの新たなキャンペーンに対するアドバイザリーを公表※83
6/18	ランサムウェアeCh0raixがQNAP社製NASを再び標的としているとBleeping Computerが報道※84
6/22	QNAP社がPHPのリモートコード実行の脆弱性（CVE-2019-11043（JVNDB-2019-011337））に対するアドバイザリーを公表※85
7/7	QNAP社が新しいランサムウェアCheckmateに対するアドバイザリーを公表※86
9/3	QNAP社がアプリケーションPhoto Stationのランサムウェア DeadBolt対策としてアドバイザリーを公表※87
10/29	Group-IBがランサムウェアDeadBoltの活動（QNAP社製NASのゼロデイ脆弱性を悪用して、QNAP社とエンドユーザーの両方を脅迫）を報告※88

■表3-2-2　2022年QNAP社製NASに発生した主な脅威と対応

(b) ASUSTOR社製NASに対する脅威

2022年2月24日、ASUSTOR Inc.（華芸科技股份有限公司。以下、ASUSTOR社）製NASのゼロデイ脆弱性を狙うランサムウェア「DeadBolt」の攻撃が報告された※89。同月21日の時点でASUSTOR社からファームウェアの更新が公開されている※90。

(c) TerraMaster 社製 NAS に対する脅威

2022 年 3 月 7 日、TerraMaster Technology Co., Ltd.（深圳市图美电子技术有限公司。以下、TerraMaster 社）製 NAS 用のオペレーティングシステム TOS の脆弱性（CVE-2022-24989、CVE-2022-24990）を悪用した非認証のリモートコード実行で感染を試みるランサムウェア DeadBolt の活動が報告された※91。同月 1 日の時点で TerraMaster 社からファームウェアの更新が公開されている※92。

(d) Western Digital 社製 NAS に対する脅威

2022 年 3 月 24 日、Western Digital Corporation（以下、Western Digital 社）は、同社製 NAS のファームウェアである My Cloud OS 5 のアップデートを公開した※93。VFS（Virtual File System）モジュール vfs_fruit を使用する samba にヒープ範囲外の読み取り／書き込みの脆弱性（CVE-2021-44142（JVNDB-2022-001296））が存在し、攻撃者が管理者権限で任意のコード実行できる可能性があった。

(e) Synology 社製 NAS に対する脅威

2022 年 4 月 28 日、Synology Inc.（群暉科技股份有限公司。以下、Synology 社）は、同社製 NAS のオペレーティングシステムに含まれる、AFP（Apple Filing Protocol）によるファイルサーバー機能を提供するオープンソースソフトウェアである Netatalk の複数の脆弱性（CVE-2022-0194、CVE-2022-23121 ～ 23125）に関するアドバイザリーを公開した※94。攻撃者によるリモートコード実行と機密情報の窃取の可能性があった。

(f) バッファロー社製 NAS に対する脅威

2022 年 8 月 31 日、株式会社バッファローは、同社製 NAS における AFP の脆弱性とその対処方法（ファームウェアの更新または AFP 機能の無効化）を公開した※95。

(g) Zyxel 社製 NAS に対する脅威

2022 年 9 月 6 日、Zyxel Networks Corporation（合勤科技股份有限公司。以下、Zyxel 社）は、同社製 NAS のリモートコード実行の脆弱性（CVE-2022-34747）に関するアドバイザリーを公開した※96。

(2) ルーターに対する脅威

ウイルス感染させた機器を乗っ取り、第三者への攻撃に悪用する目的で、ルーターの脆弱性を狙う脅威が継続している。

(a) D-Link 社製ルーターに対する脅威

2022 年 1 月、D-Link Corporation（友讯科技股份有限公司。以下、D-Link 社）製ルーターのコマンドインジェクション脆弱性（CVE-2015-2051）を狙った攻撃が多く観測された※97。

2022 年 8 月上旬、D-Link 社製ルーターの下記の 4 種類の脆弱性を狙う Mirai の亜種 Moobot の攻撃が観測された※98。

- CVE-2015-2051（JVNDB-2015-001591）
- CVE-2018-6530（JVNDB-2018-002681）
- CVE-2022-26258（リモートコマンド実行の脆弱性）
- CVE-2022-28958（リモートコード実行の脆弱性）

(b) MikroTik 社製ルーターに対する脅威

2022 年 3 月 16 日、SIA Mikrotīkls（以下、MikroTik 社）製ルーターを C&C サーバー※99 のプロキシーとして悪用するウイルス TrickBot の活動が報告された※100。また、これらの攻撃に対するフォレンジックを行うためのオープンソースのツール RouterOS Scanner が公開された※101。

(c) ASUS 社製ルーターに対する脅威

2022 年 3 月 17 日、ASUSTeK Computer Inc.（華碩電脑股份有限公司。以下、ASUS 社）製ルーターがロシアの国家支援型ボットネット「Cyclops Blink」の攻撃対象となっていることが報告された※102。同月 25 日、ASUS 社はアドバイザリーを公開した後、4 月 1 日に更新ファームウェアの提供を開始した※103。

(d) DrayTek 社製ルーターに対する脅威

2022 年 8 月 3 日、DrayTek Corporation（居易科技中国分公司。以下、DrayTek 社）製ルーターの非認証のリモートコード実行の脆弱性（CVE-2022-32548）が発見された※104。この時点では、世界中で 20 万台以上の該当機器がインターネットに接続されていることが確認されており、翌 4 日、DrayTek 社は更新ファームウェアを含むアドバイザリーを公開した※105。

(e) NETGEAR 社製ルーターに対する脅威

2022 年 9 月 15 日、NETGEAR, Inc.（以下、NETGEAR 社）製ルーターで用いられているサードパーティ（Xiamen Xunwang Network Technology Co.,

Ltd.）製のゲーム高速化モジュール FunJSQ の脆弱性（任意のコード実行の可能性、CVE-2022-40619、CVE-2022-40620）が報告された※106。同月 8 日の時点で、NETGEAR 社からアドバイザリーが公開されている※107。

同年 12 月 2 日、NETGEAR 社製 Nighthawk RAX30（AX2400）ルーターにおいて、IPv4 トラフィックに適用されるアクセス制限が IPv6 トラフィックに適用されない誤設定と思われる脆弱性（CVE-2022-4390）が報告された※108。同月 1 日の時点で NETGEAR 社から Hot Fix が公開されているが、脆弱性の詳細は非公開であった※109。

(f) 各社製ルーターに対する脅威

2022 年 6 月 28 日、ASUS 社、Cisco Systems, Inc.（以下、Cisco 社）、DrayTek 社、NETGEAR 社等の SOHO（Small Office Home Office）ルーターに感染するウイルス「ZouRAT」の情報が公開された※110。ZouRAT は、Mirai を大幅に変更した亜種と考えられている。

(3) DVR/NVR に対する脅威

ルーターと同様に、ウイルス感染させた機器を乗っ取り、第三者への攻撃に悪用する目的で、DVR/NVR の脆弱性を狙う脅威が継続している。

(a) QNAP 社製ビデオ監視システムに対する脅威

2022 年 5 月 6 日、QNAP 社は、ビデオ監視システム QVR が動作する同社製 NVR のコマンドインジェクションの脆弱性（CVE-2022-27588（JVNDB-2022-001795））について、アドバイザリー（更新ファームウェアを含む）を公開した※111。

(b) 韓国製 DVR/NVR に対する脅威

2022 年 4 月以降、国内において韓国製 DVR/NVR のウイルス感染が急増した（「3.2.4 (2) 国内における感染急増」参照）。

(4) コネクテッドカーに対する脅威

自動車をインターネットと接続して付加価値を提供するコネクテッドカー技術に対する脅威が発生している。

(a) Honda 社のリモートキーレスエントリーシステムに対する脅威

2022 年 3 月、本田技研工業株式会社（以下、Honda 社）製の一部自動車のリモートキーレスエントリーシステムの脆弱性（CVE-2022-27254）を研究者が公開した※112。中間者攻撃で得た RF（Radio Frequency）信号を基にリプレイ攻撃を行うことで、ロック解除やエンジン始動が可能であるという。

同年 7 月、Honda 社製のほぼすべて（2012 ～ 2022 年製）の自動車のリモートキーレスエントリーシステムの脆弱性（CVE-2021-46145（JVNDB-2021-017766））を悪用して、ロック解除やエンジン始動を可能とする Rolling-PWN Attack を研究者が公開した※113。

(b) トヨタ自動車の T-Connect に関する情報漏えいの脅威

2022 年 10 月、トヨタ自動車株式会社（以下、トヨタ自動車）は、同社のコネクテッドサービス T-Connect のユーザーサイトのソースコードの一部が誤って GitHub 上で公開された結果、ソースコード中のデータベースへのアクセスキーを悪用することで、サービス契約者のメールアドレスと顧客管理番号が漏えいした可能性があることを発表して謝罪した※114。開発委託先企業におけるソースコードの不適切な取り扱いが原因とされている。

(c) GPS トラッカーに対する脅威

2022 年 7 月 19 日、169 ヵ国で約 150 万台の自動車に搭載されている Shenzhen Micodus Electronic Technology Co., Ltd.（以下、MiCODUS 社）製 GPS（Global Positioning System）トラッカー MV720 の以下に示す 5 種類の脆弱性が報告された※115。

- CVE-2022-2107（ハードコードされた認証情報の使用の脆弱性）
- CVE-2022-2141（不適切な認証の脆弱性）
- CVE-2022-2199（クロスサイトスクリプティングの脆弱性）
- CVE-2022-34150（ユーザー制御の鍵による認証回避の脆弱性）
- CVE-2022-33944（ユーザー制御の鍵による認証回避の脆弱性）

通常、GPS トラッカーはリアルタイムで位置と速度、過去のルートを監視し、盗難が発生した場合にリモートで燃料を遮断する。しかし、攻撃者が当該脆弱性を悪用すると、搭載車両に対する不正な追跡に加えて、不正に SMS（Short Message Service）でコマンドを送信し、搭載車両を突然停止させる攻撃が可能となる。同社製 GPS トラッカーは、欧米の政府機関・軍隊・法執行機関・重要インフラ事業者等で用いられており、国家安全保障

上の影響が大きい。発見者と米国 DHS 傘下の CISA は MiCODUS 社と情報共有しようと繰り返し試みたが無視された※115。同日、CISA は ICS アドバイザリーを公開した※116。

(5) その他の IoT 機器に対する脅威

様々な IoT 機器に対する脆弱性、及びそれらの脆弱性を狙う脅威が報告されている。

(a) 医療機器に対する脅威

2023 年 3 月 2 日、スマート輸液ポンプ（ネットワーク接続機能を有する輸液ポンプ）のセキュリティ調査結果が報告された※117。医療機関のネットワークに接続された 20 万台以上のスマート輸液ポンプをスキャンした結果、その 75% において、約 40 種類存在する既知の脆弱性のいずれかを有すること、あるいは、約 70 種類存在する既知の IoT 機器のセキュリティアラートの対象となっていることが確認された。スキャンされた輸液ポンプにおいて発見された脆弱性の上位 10 種類を表 3-2-3 に示す。

順位	脆弱性 ID	該当比率
同率 1 位	CVE-2019-12255（JVNDB-2019-007841）	52.11%
	CVE-2019-12264（JVNDB-2019-007544）	
同率 3 位	CVE-2016-9355（JVNDB-2016-008012）	50.39%
	CVE-2016-8375（JVNDB-2016-008011）	
5 位	CVE-2020-25165（JVNDB-2020-009572）	39.54%
6 位	CVE-2020-12040（JVNDB-2020-007531）	17.83%
同率 7 位	CVE-2020-12047（JVNDB-2020-007458）	15.23%
	CVE-2020-12045（JVNDB-2020-007457）	
	CVE-2020-12043（JVNDB-2020-007456）	
	CVE-2020-12041（JVNDB-2020-007455）	

■表 3-2-3　スマート輸液ポンプで発見された上位 10 種類の脆弱性
（出典）パロアルトネットワークス株式会社「医療機関にセキュリティを：調査対象輸液ポンプの 75% に脆弱性かアラート※117」を基に IPA が編集

(b) UPS に対する脅威

2022 年 3 月、Schneider Electric SE（以下、シュナイダー社）の APC Smart-UPS の下記 3 種類の脆弱性が発見され、TLStorm と名付けられた※118。

- CVE-2022-22806（TLS 認証バイパスの脆弱性）
- CVE-2022-22805（TLS バッファーオーバーフローの脆弱性）
- CVE-2022-0715（JVNDB-2022-001579）

脆弱性の原因は、Mocana Corporation（以下、Mocana 社）製の組み込み用 TLS（Transport Layer Security）である NanoSSL ライブラリの誤用である。シュナイダー社の APC ブランドの UPS（Uninterruptible Power System：無停電電源装置）は全世界で 2,000 万台以上提供されており、これらの脆弱性を悪用してリモートから完全な乗っ取りが可能であると指摘された。

(c) ビデオ会議デバイスに対する脅威

2022 年 6 月 3 日、Owl Labs 製ビデオ会議デバイス Meeting Owl Pro 及び Whiteboard Owl の脆弱性（CVE-2022-31459 ～ 31463）が報告された※119。これらの脆弱性を攻撃して Wi-Fi ネットワーク上の不正なアクセスポイントとすることで、利用者のネットワークに対するバックドアとして悪用可能であった。同月 6 日及び 23 日、Owl Labs は二回に分けて更新ファームウェアを公開した※120。

(d) 産業用位置情報デバイス／システムに対する脅威

2022 年 8 月 15 日、産業用位置情報システム RTLS（Real-Time Locating Systems）及びそのデバイスのゼロデイ脆弱性が報告された※121。中間者攻撃によって位置情報を改ざんすることで、追跡タグを装備した作業員を危険なエリアに誘導すること等が可能であった。この脆弱性を報告した研究者らは、Sewio Networks s.r.o. 製 Indoor Tracking RTLS UWB Wi-Fi kit 及び Avalue Technology Incorporation（安勤科技股彬有限公司）製 Renity Artemis Enterprise kit を用いて実証実験を行い、攻撃可能性を検証した。

(e) 航空機内インターネット接続に対する脅威

2022 年 9 月、株式会社コンテック（以下、コンテック社）製の航空機内インターネット接続用無線 LAN アクセスポイント FLEXLAN FX3000/2000 シリーズの脆弱性（CVE-2022-36158 ～ 36159（JVNDB-2022-002346））が報告された※122。非公開の開発用 Web 設定ページが残存したまま出荷されており、データの窃取・改ざん、システムの破壊及び任意のコマンド実行が可能となっていた。同月、コンテック社は、更新ファームウェア及び回避策を公開した※123。

(f) IP 電話機に対する脅威

2022 年 12 月 8 日、Cisco 社は、同社製 IP 電話機 Cisco IP Phone 7800/8800 シリーズのスタックオーバーフローの脆弱性（CVE-2022-20968）に関するアドバイザリーを公開した※124。2023 年 1 月、同社はファームウェ

アの更新を公開した。

(g) スマートスピーカーに対する脅威

2022 年 12 月 26 日、Google LLC（以下、Google 社）製スマートスピーカー Google Home シリーズの脆弱性情報が公開された[※125]。2021 年 1 月に発見された脆弱性により、遠隔操作用バックドアアカウントを作成し、盗聴や内部データの読み書きが可能であった。発見者は Google 社から 10 万 7,500 ドルの報奨金を受け取った。

3.2.2 進化の止まらないIoTウイルスの動向

前項で述べたように、IoT 機器やシステムにおいて、次々と新たな脆弱性が発見されており、これらを狙うウイルスによる攻撃手段としての取り込みが続いている。本項では、ウイルスの進化の観点から、2022 年に観測された脅威の動向を紹介する。

(1) Mirai とその亜種

2016 年 9 月に出現し、同月末にソースコードが公開された「Mirai」は、2022 年も新たな亜種が発生して感染活動を継続している。

(a) Spring4Shell の脆弱性を狙う Mirai の亜種

2022 年 4 月、前日にアドバイザリーが公開されたばかりの Java アプリケーションのオープンソースフレームワーク Spring Framework のゼロデイ脆弱性「Spring4Shell」（CVE-2022-22965（JVNDB-2022-001498））を感染拡大に悪用する Mirai の亜種が観測された[※126]。

(b) RapperBot

2022 年 8 月 3 日、6 月中旬から観測されている Mirai の亜種「RapperBot」の活動が報告された[※127]。従来の Mirai の典型的な亜種と異なり、以下に示す特徴を有する。

- パスワード認証を受け入れるように設定された SSH（Secure Shell）サーバーに対してブルートフォース攻撃を仕掛ける。このため、ウイルス内部に SSH 2.0 クライアント機能が実装されている。
- ブルートフォース攻撃に用いる認証情報のリストは、当初はウイルス内部に保持していたが、7 月以降は C&C サーバーのポート番号 4343 ～ 4345 から最新のリストを取得するように変更された。
- 感染後、SSH サーバーに攻撃者の SSH 公開鍵をコピーしたり、管理者権限のユーザー「suhelper」を追加したりすることで、機器の再起動後やウイルス削除後も SSH 経由で感染機器の乗っ取り継続を試みる。
- 自分自身を識別する文字列をウイルス内部に含まず、亜種の特定を回避しようと試みる。

1 ヵ月半の間に RapperBot の感染拡大活動と思われる 3,500 以上の IP アドレスが観測された。その国・地域別分布を表 3-2-4 に示す。

順位	国／地域	全体に占める割合
同率 1 位	台湾	18%
	米国	18%
3 位	韓国	16%
4 位	ドイツ	8%
5 位	日本	6%
6 位	中国	5%
同率 7 位	オーストラリア	3%
	メキシコ	3%
	カナダ	3%
	ロシア	3%

■表 3-2-4　感染活動が確認された RapperBot の国・地域別分布
（出典）Fortinet, Inc.「So RapperBot, What Ya Bruting For? [※127]」を基に IPA が作成

(2) EnemyBot

2022 年 3 月、IoT 機器を含む Linux が実装された機器を感染対象とする新たなボットネットが発見され、ウイルスのダウンロード URL の一部文字列から「EnemyBot」と名付けられた[※128]。同年 4 月 12 日、EnemyBot は主に Gafgyt のソースコードから派生して Mirai のソースコードから複数のモジュールを流用していること、接続経路を匿名化する Tor（The Onion Router）ネットワーク上の C&C サーバーに接続することでボットネットの停止（テイクダウン）を困難としていること等、詳細な分析結果が報告された[※129]。同年 5 月 26 日、EnemyBot の新たな亜種が発見され、様々な機器や Web サーバーの脆弱性（次ページ表 3-2-5）を攻撃する 24 種類のエクスプロイトを含む Web スキャン機能が追加されていた[※130]。

(3) その他の新たなウイルス

既存のウイルスの技術（ソースコードの一部や脆弱性の悪用方法等）を流用しつつ、新たなウイルスを開発する試みが継続している。

脆弱性 ID	影響を受ける機器とその脆弱性
CVE-2021-44228 CVE-2021-45046 （JVNDB-2021-005429）	Apache Log4J RCE※131
CVE-2022-1388	F5 BIG-IP RCE
EDB-ID: 50781	Adobe ColdFusion 11 RCE
CVE-2020-7961 （JVNDB-2020-003135）	Liferay Portal 信頼性のないデータのデシリアライゼーションの脆弱性
EDB-ID: 50872	PHP Scriptcase 9.7 RCE
CVE-2021-4039	Zyxel NWA-1100-NH コマンドインジェクションの脆弱性
EDB-ID: 50865	Razer Sila コマンドインジェクションの脆弱性
CVE-2022-22947	Spring Cloud Gateway コードインジェクションの脆弱性
CVE-2022-22954	VMWare Workspace One RCE
CVE-2021-36356 （JVNDB-2021-011319） CVE-2021-35064 （JVNDB-2021-009127）	Kramer VIAware RCE
EDB-ID: 50844	WordPress Video Sync PDF plugin ローカルファイルインクルードの脆弱性
EDB-ID: 50775	DbItek GoIP ローカルファイルインクルードの脆弱性
EDB-ID: 50843	WordPress Cab fare calculator plugin ローカルファイルインクルードの脆弱性
EDB-ID: 50665	Archeevo 5.0 ローカルファイルインクルードの脆弱性
CVE-2018-16763 （JVNDB-2018-009581）	Fuel CMS 1.4.1 RCE
CVE-2020-5902 （JVNDB-2020-007318）	F5 BIG-IP RCE
EDB-ID: 46150	ThinkPHP 5.X RCE
EDB-ID: 43055	Netgear DGN1000 1.1.00.48 'Setup.cgi' RCE
CVE-2022-25075	TOTOLINK A3000RU コマンドインジェクションの脆弱性
CVE-2015-2051 （JVNDB-2015-001591）	D-Link HNAP SOAP Action-Header コマンドインジェクションの脆弱性
CVE-2014-9118 （JVNDB-2014-008410）	Zhone zNID GPON 2426A ルーター ファームウェア S3.0.501 未満 RCE
CVE-2017-18368 （JVNDB-2017-014439）	Zyxel P660HN 非認証のコマンドインジェクションの脆弱性
CVE-2020-17456 （JVNDB-2020-010180）	Seowon SLR 120 ルーター RCE
CVE-2018-10823 （JVNDB-2018-013710）	D-Link DWR シリーズ コマンドインジェクションの脆弱性

■表 3-2-5　EnemyBot の新たな亜種が攻撃する脆弱性
（出典）AT&T Inc.「Rapidly evolving IoT malware EnemyBot now targeting Content Management System servers and Android devices※130」を基に IPA が編集

(a) B1txor20

2022 年 3 月 15 日、Apache Log4j の脆弱性※132 を狙う新たなウイルスの活動が観測され、「B1txor20」と名付けられた※133。B1txor20 は、ARM 及び X64 アーキテクチャの Linux 搭載機器を感染対象としており、C&C サーバーとの通信に DNS（Domain Name System）トンネリングを用いていることを特徴とする。

(b) Fodcha

2022 年 4 月 13 日、インターネット上で急速に拡散している DDoS ボットネットの情報が公開され、「Fodcha」と名付けられた※134。Fodcha は、主に以下に示す脆弱性と Telnet/SSH の脆弱なパスワードを感染拡大に悪用する。

- EDB-ID: 39328
  （Android ADB Debug Server リモートペイロード実行の脆弱性）
- CVE-2021-22205（JVNDB-2021-006131）
  （GitLab CE/EE の不適切な入力確認の脆弱性）
- CVE-2021-35394（JVNDB-2021-010965）
  （Realtek Jungle SDK のコマンドインジェクション及び境界外書き込みの脆弱性）
- EDB-ID: 41471
  （MVPower DVR のシェルコマンド実行の脆弱性）
- LILIN DVR のコマンドインジェクションの脆弱性等※135
- EDB-ID: 37770
  （TOTOLINK ルーターのバックドアの脆弱性）
- CVE-2014-9118（JVNDB-2014-008410）
  （Zhone zNID GPON 2426A ルーターファームウェア S3.0.501 未満のリモートコマンド実行の脆弱性）

同年 3 月 29 日から 4 月 10 日までに 6 万 2,000 台以上の感染が観測されており、中国国内に 1 万台以上のアクティブな感染機器（ボット）が存在し、毎日 100 を超える被害者が DDoS 攻撃を受けていた。

同年 10 月 31 日、Fodcha の新しいバージョンの活動が報告された※136。ファイル及びトラフィックレベルでの検出を回避するために機密リソースとネットワーク通信が暗号化されており、C&C サーバーはプライマリとバックアップのデュアル C2 スキームが採用されていた。6 万台以上のアクティブな感染機器、40 台以上の C&C サーバーから成り、1Tbps を超える DDoS 攻撃能力を有していること、1 日平均 100 以上の標的を攻撃し、10 月 11 日には 1,396 の標的に対する DDoS 攻撃が観測された。標

的の大半は、中国及び米国である。6月29日から10月21日までの週に観測された攻撃対象の国と標的数の上位10ヵ国は、中国（標的数156,440、全体比率78.2%（以下同様））、米国（19,992、10.0%）、シンガポール（4,274、2.1%）、日本（3,176、1.6%）、ロシア（2,832、1.4%）、ドイツ（2,032、1.0%）、フランス（1,938、1.0%）、英国（1,718、0.9%）、カナダ（1,624、0.8%）、オランダ（1,496、0.7%）であった。

(c) Shikitega

2022年9月6日、Linux搭載端末及びIoT機器を感染対象とする、新たなウイルス「Shikitega」の情報が公開された[※137]。Shikitegaは、使用する度に異なる符号化結果を生成するポリモーフィックエンコーダーであるSGN（Shikata Ga Nai）[※138]を用いてウイルスを段階的に配信することで、パターンマッチング方式によるウイルス検知を回避する。また、脆弱性CVE-2021-4034（JVNDB-2021-018119）及びCVE-2021-3493（JVNDB-2021-005708）を悪用して管理者権限を取得し、crontabを用いた永続性を実現しつつ、最終的に暗号資産Moneroのマイニングプログラム XMRigをダウンロードして実行する。

(d) Chaos

2022年9月28日、プログラミング言語Goで記述された新たなウイルス「Chaos」の情報が公開された[※139]。Chaosは、WindowsまたはLinuxが動作するSOHOルーターからエンタープライズサーバーまで広範囲の機器を感染対象とする。ウイルス内部に中国語の文字列を含み、中国国内のインフラストラクチャーがC&Cサーバーに悪用されている。感染機器から窃取したRSA秘密鍵の悪用、典型的なパスワードのリストを悪用したブルートフォース攻撃、または既知の脆弱性（Huawei HG532ルーターにおける任意のコード実行の脆弱性（CVE-2017-17215（JVNDB-2017-013014））やZyxel Firewallにおける非認証のリモートコマンドインジェクションの脆弱性[※140]（CVE-2022-30525））を感染拡大に悪用する。6月中旬から7月中旬に数百台の感染、イタリアを中心とした欧州、米国及び中国での分布、様々な事業体を標的とするDDoS攻撃の実施が確認されている。

3.2.3 IoTセキュリティのサプライチェーンとEOLのリスク

IoT機器の開発に用いられる共通コンポーネントや標準プロトコルに起因する脆弱性（IoT機器のサプライチェーンリスク）、サポートが終了したEOL（End-of-life）ステータスにあるIoT機器における脆弱性の発見（EOLのリスク）が引き続き発生している。本項では、これらのリスク事例を紹介する。

(1) サプライチェーンのリスク

複数のIoT機器の開発に用いられている共通のソフトウェアコンポーネントやハードウェア部品（チップセットやSoC（System on a Chip））において、引き続き脆弱性が発見されており、広範囲にわたる影響やセキュリティ対策の困難性が生じている。

(a) KCodes NetUSBの脆弱性

2022年1月11日、KCodes Corporation（盈碼科技股彬有限公司。以下、KCodes社）製NetUSBのカーネルモジュールにおけるリモートコード実行の脆弱性（CVE-2021-45608（JVNDB-2021-017175））が開示された[※141]。NetUSBは、ルーターのUSBポートに接続した機器をネットワーク上からローカルのUSBポートに接続されているかのようにアクセス可能とする（USB Over IP）製品であり、以下に示す各社のルーターで採用されている。

- NETGEAR社
- TP-Link Technologies Co., Ltd.（普联技术有限公司。以下、TP-Link社）
- Shenzhen Tenda Technology Co., Ltd.（深圳市吉祥腾达科技有限公司。以下、Tenda社）
- Edimax Technology Co., Ltd.（訊舟科技股份有限公司）
- D-Link社
- Western Digital社

なお、2021年9月20日以降、発見者からKCodes社への脆弱性情報開示後、同年11月19日までにKCodes社から各ベンダーにパッチを送信済みであり、同年12月20日までに各ベンダーは更新ファームウェアをリリースした。

(b) Access:7

2022年3月8日、PTC社が提供するAxeda agent及びAxeda Desktop Server等に7種類の脆弱性（次ページ表3-2-6）が報告され、「Access:7」と名付けられた[※142]。Axedaのソリューションは、IoT機器の製造業者による遠隔管理機能を提供しており、ヘルスケア分野・

金融サービス・製造業等において用いられており、100社以上のベンダーが提供する150種以上の機器が影響を受けるとされている（「3.1.2(1)(a)Access:7」参照）。

脆弱性ID	脆弱性の概要
CVE-2022-25249（JVNDB-2022-001521）	Axeda Agentにおけるパストラバーサルの脆弱性
CVE-2022-25250（JVNDB-2022-001520）	Axeda Agentにおける重要な機能に対する認証の欠如の脆弱性
CVE-2022-25251（JVNDB-2022-001519）	Axeda Agentにおける重要な機能に対する認証の欠如の脆弱性
CVE-2022-25246（JVNDB-2022-001525）	Axeda Desktop Serverにおけるハードコードされた認証情報の使用の脆弱性
CVE-2022-25248（JVNDB-2022-001523）	ERemoteServer（Agent構成時にベンダーが使用するツール）における情報漏えいの脆弱性
CVE-2022-25247（JVNDB-2022-001524）	ERemoteServerにおける重要な機能に対する認証の欠如の脆弱性
CVE-2022-25252（JVNDB-2022-001528）	Axeda Agent及びAxeda Desktop Server（で用いられるxBase39ライブラリ）における例外に対する不適切なチェックの脆弱性

■表3-2-6　Access:7の脆弱性
（出典）Forescout Technologies, Inc.「Access:7 - How Supply Chain Vulnerabilities Can Allow Unwelcomed Access to Your Medical and IoT Devices※142」を基にIPAが編集

同日、CISAはアドバイザリー（ICSA-22-067-01※143）を、PTC社はアドバイザリー及びサポート情報※144を公開した。

(c) TLStorm 2.0

2022年5月、Aruba Networks（現、Hewlett Packard Enterprise Co.の一部門）及びAvaya Inc.のネットワーク事業部門（現、Extreme Networks, LLCの一部門）製のネットワークスイッチにおける下記5種類の脆弱性が発見され、TLStorm 2.0と名付けられた※145。TLStorm※118（「3.2.1(5)(b)UPSに対する脅威」参照）同様、脆弱性の原因の一部は、Mocana社製NanoSSLライブラリの誤用である。

- Aruba
  - CVE-2022-23677（NanoSSL誤用に起因するリモートコード実行の脆弱性）
  - CVE-2022-23676（RADIUSクライアントのメモリ破壊の脆弱性）
- Avaya
  - CVE-2022-29860（CVE-2022-22805と同様）
  - CVE-2022-29861（HTTPヘッダ解析におけるスタックオーバーフロー）
  - CVE未採番（HTTP POSTリクエスト処理におけるヒープオーバーフロー）

(d) uClibc DNSの脆弱性

2022年5月2日、組み込みLinuxシステム開発用C言語ライブラリ「uClibc※146」及び「uClibc-ng※147」のDNS実装における、DNS requestのtransaction IDパラメータを予測可能な脆弱性（CVE-2022-30295（JVNDB-2022-001736））が報告された※148。攻撃者が偽造したDNS responseを送信して不正なDNSキャッシュを登録させることで、ユーザーを悪意のあるサイトへ誘導するDNSキャッシュポイズニング攻撃が可能となる。

uClibcは、Linksys Holdings, Inc.、NETGEAR社、Axis Communications AB（2010年の製品まで）等のベンダーのルーターで使用されているが、2012年5月15日以降は更新が停止されている。

uClibc-ngは、様々なルーターで用いられている組み込みシステム用Linuxディストリビューション OpenWrtで採用されている。2022年5月20日、脆弱性を修正したversion 1.0.41が公開された※147。

(e) スマートフォン用チップセットの脆弱性

2022年6月2日、Unisoc (Shanghai) Technologies Co., Ltd.（紫光展锐（上海）科技有限公司。以下、UNISOC社）製スマートフォン用チップセットにおける脆弱性（CVE-2022-20210）が報告された※149。NAS（非アクセス層）メッセージ処理において長さチェックが省略されているため、ヒープオーバーフロー攻撃が可能となっており、リモートからのサービス停止（DoS：Denial of Services）やコード実行を引き起こす。UNISOC社のチップセットは低価格であるため、アフリカやアジアを中心に世界4位（2022年の市場占有率：9～11%）のシェアを占めており、多くのAndroid機器に影響を与えた。UNISOC社製チップセットに関しては、同年3月にも遠隔制御可能な脆弱性（CVE-2022-27250）が発見されている。

(f) Realtek社製SoC及びSDKの脆弱性

2022年3月25日、Realtek Semiconductor Corp.（瑞昱半導體股份有限公司。以下、Realtek社）は、

同社製RTL819x SoC及びeCos SDK（Software Development Kit）を用いたルーターのバッファーオーバーフローの脆弱性（CVE-2022-27255）に関するアドバイザリーを公開した※150。同年8月12日、DEF CON 30カンファレンスにおいて、発見者が攻撃コード（PoC※151）を含む技術的な詳細を公開した※152。

(2) EOLのリスク

サポートが終了して更新ソフトウェアが提供されないIoT機器や共通コンポーネントにおいて、新たな脆弱性が発見されている。特に共通コンポーネントの場合は、サプライチェーンのリスクも生じ、深刻な影響を与えることとなる。

(a) 家庭用ゲーム機の周辺機器のEOL

2022年7月20日、任天堂株式会社は、2005年及び2008年に発売した「ニンテンドー Wi-Fi USBコネクタ」「ニンテンドー Wi-Fi ネットワークアダプタ」の使用中止を呼びかけた※153。無線LANの暗号化方式としてWEP（Wired Equivalent Privacy）のみをサポートしているため、通信データの改ざんや漏えい、ネットワークの乗っ取りや不正アクセスの恐れが存在し、市販のネットワーク機器への切り替えを要望した。同年8月1日、ニンテンドー Wi-Fi ネットワークアダプタには、以下に示す脆弱性（JVNDB-2022-000056）が存在することも追加公開された。

- CVE-2022-36293（バッファーオーバーフローの脆弱性）
- CVE-2022-36381（OSコマンドインジェクションの脆弱性）

家庭用ゲーム機の周辺機器として販売されたこれらの製品は、発売から10年以上を経過しても使用し続けられており、機器提供者の対応の難しさを象徴する例となった。

(b) Cisco社製EOLルーターのゼロデイ脆弱性

2022年9月7日、Cisco社は、同社製中小企業向けルーターRV110W、RV130、RV130W及びRV215WのIPsec VPNサーバー認証機能における認証バイパスの脆弱性（CVE-2022-20923）の存在を公表した※154。同社は、これらが2019年9月2日にEOLを表明し、同年12月2日に販売を終了した製品※155であることから、更新ファームウェアを提供しないこと、及び回避策が存在しないことを宣言した。近年、Cisco社はEOL製品に対する脆弱性が発見されても更新ファームウェアを提供しない傾向があることが指摘されている※156。

(c) Boa Web Server

2022年11月22日、同年1～2月にインドの配電網に対して実施されたサイバー攻撃において、組み込み用オープンソースのWebサーバーBoaを実装したIoT機器を標的としていたことが報告された※157。Boaは2005年2月23日を最後に開発中止となっていたが、依然として様々なIoT機器や組み込み用SDKで実装されており、既知の脆弱性（CVE-2009-4496（JVNDB-2010-003631）等）が攻撃者によって狙われて、サプライチェーン及びEOLのリスクが生じている。

3.2.4 脆弱なIoT機器のウイルス感染と感染機器悪用の実態

IoT機器／システムに対する脅威が継続・拡大傾向にある中、脆弱なIoT機器とウイルス感染の実態はどうなっているのか。サイバー攻撃によって感染機器はどのように悪用されているのか。本項では、セキュリティ対策強化の取り組みやセキュリティベンダーによる公開情報から、これらの実態について考察する。

(1) 国内における実態調査と注意喚起

総務省及び国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）は、2019年2月20日以降、インターネット接続事業者と連携し、サイバー攻撃に悪用される恐れのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取り組み「NOTICE（National Operation Towards IoT Clean Environment）※158」を継続中である（NOTICEについては「2.1.4(2)(b)IoTにおけるサイバーセキュリティの確保」参照）。2022年2月22日以降は、HTTP(S)に対するポートスキャンに加えて、HTTP(S)上のパスワードを入力可能な機器に対して容易に推測可能なID・パスワードを入力し、サイバー攻撃に悪用される恐れのある機器の特定を開始した。2023年3月の時点で、NOTICE参加インターネットサービスプロバイダー（ISP：Internet Service Provider）は75社、調査対象IPアドレスは約1.12億アドレスである。2022年1月以降の取り組み結果を表3-2-7（次ページ）に示す。

- 「NOTICE注意喚起」（ログイン可能機器利用者への注意喚起）は、2022年6月以降に大幅な増加が見られるが、これは調査対象プロトコル（HTTP(S)）の追加によるものであり、実態として一年間をとおして大きな変化はないと考えられる。

年月	NOTICE 注意喚起（ログイン可能機器）	NICTER 注意喚起（ウイルス感染機器）
2022 年 1 月	1,665 件	平均 198 件／日
2 月	1,686 件	平均 231 件／日
3 月	1,664 件	平均 193 件／日
4 月	1,585 件	平均 376 件／日
5 月	1,564 件	平均 1,025 件／日
6 月	4,504 件	平均 2,489 件／日
7 月	4,506 件	平均 2,250 件／日
8 月	4,381 件	平均 1,550 件／日
9 月	4,394 件	平均 1,023 件／日
10 月	4,327 件	平均 817 件／日
11 月	4,430 件	平均 560 件／日
12 月	4,416 件	平均 670 件／日
2023 年 1 月	4,254 件	平均 772 件／日
2 月	4,136 件	平均 650 件／日
3 月	4,176 件	平均 516 件／日

■表 3-2-7　国内における注意喚起の取り組みの実施結果
（出典）NOTICE サポートセンター「実施状況※159」を基に IPA が作成

- 「NICTER 注意喚起」（ウイルス感染機器利用者への注意喚起）は、2022 年 4 月下旬以降急増し、6 月 6 日に過去最大値（3,288 件／日）を記録した。同年 6 ～ 7 月をピークに減少に転じたものの、2022 年 3 月以前と比較して約 3 ～ 4 倍という高い値が継続している。これは、Mirai の亜種の活動活発化の影響を受けて、国内の脆弱な機器（主に DVR/NVR）の感染が拡大したと考えられる（同時期の国内における感染急増については次項を参照）。

(2) 国内における感染急増

2022 年 4 月 24 日以降、国内における Mirai の亜種に感染した IoT 機器の急増が観測され、Pinetron Co., Ltd（파인트론。現、파인티앤에스。以下、Pinetron 社）製の DVR/NVR が 300 台以上感染していることが判明した※160。5 月 11 日、更なる感染拡大が観測され、約 800 台の感染 DVR/NVR 中、約 600 台が Pinetron 社製であった※161。

6 月に入ると、FOCUS H&S Co., Ltd.（주식회사 포커스에이치엔에스。以下、FOCUS H&S 社）製 DVR/NVR の感染急増が観測された※162。当該機器には、パスワード変更や無効化ができないバックドアアカウントの脆弱性（CVE-2022-35733）が存在しており、国内の販売代理店であるユニモテクノロジー株式会社は 2022 年 1 月に更新ファームウェアを提供していた※163が、適用されていない多くの機器が存在したと考えられる。最も多かった 6 月 28 日には、5,137 台の IoT 機器の感染が観測されており、4 月の感染拡大時には Pinetron 社に加えて CTRing Co., Ltd.、6 月の感染拡大時には FOCUS H&S 社に加えて Rifatron Co., Ltd.（이화트론）と、韓国製 DVR/NVR の感染増加が確認された※71。

(3) 国内における攻撃の観測

株式会社インターネットイニシアティブが国内における攻撃の観測情報及び分析結果による月次観測レポートを公開している※164。2022 年 1 ～ 12 月の報告内容から IoT 関連で観測された攻撃を抽出した結果を表 3-2-8 に示す。

年月	観測された主な攻撃
2022 年 1 月	D-Link ルーターの脆弱性を狙った攻撃※97
2 月	Mozi の感染活動、NETGEAR ルーターや MVPower DVR の脆弱性を悪用した通信※165
3 月	MVPower DVR の Wget コマンドインジェクション脆弱性を悪用した通信※166
4 月	Wget コマンドインジェクション脆弱性を悪用した通信※167
5 月	Mozi の感染活動、NETGEAR ルーターや MVPower DVR の脆弱性を悪用した通信※168
7 月	Netis ルーターや Netcore ルーターの脆弱性を狙った攻撃※169
8 月	Netis ルーターや Netcore ルーターの脆弱性を悪用した通信※170
10 月	Netis ルーターや Netcore ルーターの脆弱性を狙った攻撃※171
11 月	Netis ルーターや Netcore ルーターの脆弱性を狙った攻撃※172
12 月	Realtek Jungle SDK の脆弱性を狙った攻撃※173

■表 3-2-8　国内において観測された主な攻撃
（出典）株式会社インターネットイニシアティブ「wizSafe Security Signal 観測レポート※164」を基に IPA が作成

(4) 感染機器のサイバー攻撃への悪用の実態

IoT 機器に感染する「機器乗っ取り型ウイルス※174」は、ウイルス感染した機器を、主に第三者へのサイバー攻撃に悪用する傾向がある。ここでは、具体的な悪用事例を紹介する。

(a) DDoS 攻撃への悪用

2022 年 6 月 27 日、ウイルス感染したルーター、ネットワークカメラ、侵害されたサーバー等、180 ヵ国以上（大半は米国、インドネシア、ブラジル）の約 17 万の異なる IP アドレスからなるボットネットによる中国の電気通信会社への DDoS 攻撃が発生した※175。攻撃者は HTTP/2 多

重化リクエストを用いて、平均 180 万 RPS（リクエスト／秒）、最大 390 万 RPS の攻撃を実施し、4 時間で合計 253 億のリクエストを送信し、当該事業者に対して DDoS 緩和ソリューションを提供しているセキュリティ会社の過去最大の記録となった。

同年 10 月 12 日、インターネットセキュリティサービス事業者による 2022 年第 3 四半期 DDoS 脅威レポートが公開された※176。Mirai の亜種のボットネットによるオンラインゲームサーバーへの最大 2.5Tbps の DDoS 攻撃が観測され、UDP フラッドと TCP フラッドのマルチベクトル攻撃によるものであった。

同年 12 月 15 日、クロスプラットフォームで構成されるボットネット「MCCrash」の観測が報告された※177。このボットネットはまず、違法な Windows ライセンス取得を目的とした悪意のクラッキングツールのインストールによって Windows パソコンに感染した後、SSH 対応の Linux ベースの機器（IoT 機器を含む）にデフォルト認証情報の辞書攻撃を仕掛けることで感染を拡大する。感染機器の大半がロシアに存在しており、他にカザフスタン、ウズベキスタン、ウクライナ、ベラルーシ、チェコ、イタリア、インド、インドネシア、ナイジェリア、カメルーン、メキシコ及びコロンビアで発見されている。米国を中心として世界各国に存在するプライベートのオンラインゲームサーバーに対して DDoS 攻撃を行うことを目的としており、サーバーをクラッシュさせるための内部コマンド名 ATTACK_MCCRASH から MCCrash と命名された。

(b) プロキシーとしての悪用

2022 年 8 月 18 日、FBI は、サイバー犯罪者による米国企業に対するクレデンシャル・スタッフィング攻撃※178 において、プロキシーの悪用について警告した※179。攻撃者の発信元を隠蔽し、または特定地域から発信のブロックによる防御を回避するために、residential proxy（ウイルス感染によりプロキシーサーバーとして悪用されている IoT 機器、または悪用されることを承知の上で個人が提供するプロキシーサーバー）が用いられている、と指摘した。

同年 12 月 1 日、サイバー犯罪者に提供することを目的とした、大規模なプロキシーサービス「BlackProxies」が発見された※180。世界中の 100 万以上の residential proxy を提供可能と主張しており、2022 年秋の時点で 18 万以上の IP アドレスのプールが表示されている。

(c) 標的型攻撃や OT に対する攻撃への悪用

2022 年 5 月 2 日、サイバー攻撃者集団 UNC3524（その後の調査により、同年 11 月、ロシアが支援する集団 APT29 と同一と判定）によるスパイ活動において、セキュリティ対策が不十分なネットワーク機器、IoT 機器及び OT 機器に対する攻撃と悪用が報告された※181。これらの機器にバックドアを設置することで検知を困難とし、C&C サーバーには、ウイルス感染させた LifeSize, Inc. 製会議室カメラシステムや D-Link 社のネットワークカメラを悪用していることが確認されている。

2022 年 6 月 1 日、ネットワークカメラや NAS 等の IoT 機器を侵入口として、IT ネットワーク（リモートデスクトップサービスの動作する Windows パソコンやドメインコントローラー、Windows サーバー）に横展開した後、OT 機器に対して DoS 攻撃を仕掛けるランサムウェアの活動「R4IoT」が報告された※182。

(d) 中国の国家支援型サイバー攻撃への悪用

2022 年 6 月 7 日、CISA、NSA 及び FBI は、中国が支援するサイバー攻撃者の活動に関して、共同でサイバーセキュリティアドバイザリーを公開した※183。2020 年以降、攻撃者は SOHO ルーターや NAS の既知の脆弱性を悪用して、C&C サーバーへの通信をルーティングするためのアクセスポイントとして追加し、他へ侵入するための攻撃拠点としている。攻撃者によって悪用された上位の脆弱性を、表 3-2-9（次ページ）に示す。

(5) P2P ボットネットの現状

2022 年 11 月 3 日、P2P（Peer-to-Peer）プロトコルを用いるボットネットの現状が報告された※184。Linux ベースの IoT 機器を感染対象とするウイルス Hajime、Mozi、Pink の現状を以下に示す。

- Hajime※185 は、2018 年 5 月以降は更新が停止したと考えられているが、依然として 2 万台前後の感染が継続している。感染台数上位国は、イラン、中国、インド、ロシア、ブラジル、ベネズエラ、インドネシア、イタリア、英国、パレスチナである。
- Mozi※186 は、2021 年 7 月の作者逮捕後も活動が継続しており、2 万 8,000 台以上の感染が確認されている。感染台数上位国は、中国、インド、ロシア、パキスタン、ボリビア、イラン、モロッコ、アルゼンチン、ベネズエラ、ブラジルである。
- Pink※187 は、そのほとんど（98.1%）が中国内の IoT 機器に感染しているウイルスである。ピーク時には 160

ベンダー名	脆弱性 ID	脆弱性の概要
Cisco	CVE-2018-0171	RCE
	CVE-2019-15271	
	CVE-2019-1652	
Citrix	CVE-2019-19781	RCE
DrayTek	CVE-2020-8515	RCE
D-Link	CVE-2019-16920	RCE
Fortinet	CVE-2018-13382	認証バイパスの脆弱性
MikroTik	CVE-2018-14847	認証バイパスの脆弱性
NETGEAR	CVE-2017-6862	RCE
Pulse	CVE-2019-11510	認証バイパスの脆弱性
	CVE-2021-22893	RCE
QNAP	CVE-2019-7192	権限昇格の脆弱性
	CVE-2019-7193	リモートインジェクションの脆弱性
	CVE-2019-7194	XML ルーティング迂回攻撃の脆弱性
	CVE-2019-7195	
Zyxel	CVE-2020-29583	認証バイパスの脆弱性

■表 3-2-9　中国の国家支援型サイバー攻撃で悪用された上位の脆弱性
（出典）CISA「People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices※183」を基に IPA が編集

万台以上の感染が確認されていたが、2020 年 7 月以降、機器ベンダーのクリーンアップの取り組みの結果、14 万 5,881 台（7 月 12 日）から 2 万 9,956 台（8 月 20 日）へと大幅に減少した。

3.2.5 各国のセキュリティ対策強化の取り組み

これまで述べたように、脆弱性を有したままインターネットに接続された IoT 機器はサイバー攻撃の対象となり、機器の利用者や第三者に被害を及ぼすこととなる。場合によっては、国家間の戦争に悪用される恐れもあり、IoT 機器のセキュリティ対策強化は必須となっている。本項では、対策を検討・推進する上で参考となるセキュリティガイドラインや手引き等の発行状況や国内外の取り組みについて紹介する。

(1) IoT 関連のガイドラインや手引き等の改訂・新規発行

これまでに公開された IoT セキュリティに関するガイドラインや手引き等の改訂版、新たなガイドライン等が引き続き公開されている。2022 年以降に国内及び海外で公開されたガイドラインや手引き等を、表 3-2-10（次ページ）と表 3-2-11（次ページ）に示す。

(2) IoT 製品のセキュリティラベリング

一定のセキュリティ基準を満たす IoT 製品に対して、各国政府及びその傘下の認証機関がお墨付きを与えるセキュリティラベリングは、欧米を中心に検討・導入が進められており、各国間の協調も始まりつつある。国内でも制度構築に向けた検討会が開始された。

(a) ドイツにおける対象製品拡大

2022 年 5 月 6 日、ドイツ連邦政府・情報セキュリティ庁（BSI：Bundesamt für Sicherheit in der Informationstechnik）は、2021 年 5 月 7 日に承認された IT セキュリティ法 2.0（IT-Sicherheitsgesetz 2.0）において消費者保護を目的として導入された IT セキュリティラベル（IT-Sicherheitskennzeichen）制度の対象製品の拡大を発表した※188。2021 年 11 月からブロードバンドルーターと電子メールサービスの二つのカテゴリで申請受付を開始していたが、新たにスマートカメラ、スマートスピーカー、スマート掃除機及びガーデニングロボット、スマートトイ、スマートテレビを対象に追加した。

(b) 共通ガイドラインに基づく国際間の協調

2022 年 10 月 20 日、ドイツ BSI とシンガポール首相官邸傘下の CSA（Cyber Security Agency of Singapore）は、IT セキュリティラベリングの相互承認に関する二国間協定に署名したと発表した※189。これは、両国のラベリング制度が、ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）が制定した欧州標準 ETSI EN 303 645（CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements）※190 に基づいていることによる。

(c) 国内における適合性評価制度構築に向けた検討開始

2022 年 11 月 1 日、経済産業省が主催する産業サイバーセキュリティ研究会ワーキンググループ 3（サイバーセキュリティビジネス化）傘下の「IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会」の第 1 回会合が開催された※191。IoT 製品の安全性確保のため、製品ベンダーにおけるセキュリティ対策の取り組みは必要不可欠であるが、既存制度では取り組み状況を調達者や消費者にアピールすることができず、対策コストを製品価格に反映することは困難である。そこで、「一定のセキュリティ要求基準に対するセキュリティ対策の適合性を評価しその結果を利用者や調達者が分かる形で可視化する制度（適合性評価制度）」を構築すべく、現状の

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
IPA	IoT 開発におけるセキュリティ設計の手引き（2023 年 3 月版）※193	IoT 開発におけるセキュリティ設計担当者	具体的な設計手法（脅威分析、対策検討、脆弱性対策）	2023 年 3 月
	ETSI EN 303 645 V2.1.1（2020-06）サイバーセキュリティ技術委員会（CYBER）；民生用 IoT 機器のサイバーセキュリティ：ベースライン要件［翻訳版］※194	コンシューマ向け IoT 機器の開発者・製造者	ETSI EN 303 645※190 の日本語訳	2023 年 3 月
一般社団法人日本クラウドセキュリティアライアンス（CSA-JC：Cloud Security Alliance Japan Chapter）	CSA IoT Controls Matrix v3 ガイド※195	IoT システムの設計者、開発者、評価者	フレームワークスプレッドシートを用いた IoT システムの評価・実装方法	2022 年 4 月（英語版）2022 年 6 月（日本語版）
	CSA IoT Controls Matrix v3（EXCEL）※196		IoT システムの評価・実装に利用可能なセキュリティコントロール	
一般社団法人セキュア IoT プラットフォーム協議会（SIOTP：Secure IoT Platform Consortium）	IoT セキュリティ手引書 Ver2.0※197	IoT 機器の製造事業者、IoT システムの提供に関わる事業者	IoT 機器に求められるセキュリティ対策について、製品ライフサイクルの各分類における業界基準の解釈と検証結果	2022 年 1 月

■表 3-2-10　2022 年以降に国内で新規公開・改訂された IoT 関連のガイドラインや手引き等
（出典）各団体の公開情報を基に IPA が作成

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
NIST（National Institute of Standards and Technology：米国国立標準技術研究所）	NISTIR 8349 (Draft): Methodology for Characterizing Network Behavior of Internet of Things Devices※198	IoT 機器の製造者及び開発者、ネットワーク管理者、脆弱性研究者	IoT 機器のネットワーク通信動作を MUD（Manufacturer Usage Description）仕様に基づいて文書化する方法	2022 年 1 月
	NISTIR 8425: Profile of the IoT Core Baseline for Consumer IoT Products※199	IoT 機器の製造者、小売業者、インテグレーター、試験・認証機関	消費者向け IoT 機器のセキュリティ機能のコアとなるベースライン	2022 年 9 月
	NISTIR 8431: Workshop Summary Report for “Building on the NIST Foundations: Next Steps in IoT Cybersecurity”※200	IoT 機器の製造者、セキュリティアーキテクト、テスト・評価の専門家、市場関係者	IoT 製品のサイバーセキュリティ基準に関する NIST Cybersecurity for IoT プログラムの作業に寄せられたフィードバック	
	NIST SP 1800-36 (Draft): Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security (Preliminary Draft)※201	IoT 機器の利用者	組織が IoT 機器とネットワークの両方を保護する方法	2023 年 5 月
DSCI（Data Security Council of India）	IoT Security Guidebook※202	IoT セキュリティの関係者全般	IoT に関する幅広い技術的な視点、包括的なアドバイス	2022 年 8 月
	IoT Security Best Practices Document※203		消費者向け IoT セキュリティ、産業用 IoT セキュリティ及びクラウド IoT セキュリティのベストプラクティス	

■表 3-2-11　2022 年以降に海外で新規公開・改訂された IoT 関連のガイドラインや手引き等
（出典）各団体の公開情報を基に IPA が作成

課題、制度構築の目的、構築すべき制度等について議論を開始した。

(3) ボットネットの解体

2022 年 6 月 16 日、米国司法省（United States Department of Justice）は、ドイツ・オランダ・英国の法執行機関のパートナーとともに、世界中の数百万台のハッキングされたコンピューターや電子機器で構成されたボットネット「RSOCKS」を解体したと発表した※192。RSOCKS は、ロシアのサイバー犯罪組織により運営されており、当初は産業用制御システムの構成機器、タイムレコーダー、ルーター、オーディオビデオストリーミング機器、

スマートガレージオープナー等の様々な IoT 機器を標的として構築を開始し、その後、Android 端末やコンピューターに感染を拡大していた。解体には、脅威インテリジェンスの民間企業 Black Echo LLC も協力し、官民連携のもとで実施された。

COLUMN

情報セキュリティポリシー見直しのススメ ～「とりあえずセキュリティ」からの脱却～

日本において、「情報セキュリティポリシー」という言葉が企業や組織に認知され始めたのは、2002 年に ISMS 適合性評価制度が正式にスタートして以降でしょう。ISMS 認証登録数は、2016 年に 5,000 件を超え、2022 年には 7,000 件を超えていますので、多くの企業や組織において、情報セキュリティポリシーが策定され、基本方針に基づく対策基準や実施手順が整備されていると考えられます。情報セキュリティポリシーは、どのような情報資産をどのような脅威からどのように守るのかといった「基本方針」、情報セキュリティを確保するための体制や具体的な規則を示す「対策基準」、対象者や用途によって必要な規程や手続き等を明確にした「実施手順」の 3 階層で構成されるのが一般的です。

さて、この「情報セキュリティポリシー」ですが、皆さんの組織では適切に見直されていますでしょうか。昨今の DX 推進やクラウドファーストという流れがある中で、セキュリティ規程が足かせとなって、DX が進まない、クラウドサービスを利用したくても利用できない、組織内の IT 関連申請の手続きが煩雑で業務効率が下がっている、というような悩みを抱えている組織がかなりあるという声が聞こえてきます。本来、業務を安全・安心に進めて、企業としての利益や組織の成果に貢献することが目的であるはずのセキュリティが、業務改革の妨げになったり、業務効率を下げるようなことになっているとすれば、それは残念なことです。

このような組織でよく見られることは、「とりあえずセキュリティ」という考え方です。例えば、ISMS 認証に登録するためには、「適用宣言書」という自組織に適用するセキュリティ対策の項目と、除外する項目及び除外理由を記した文書を作成する必要がありますが、除外項目が多いと審査の際に不利になるのではないかとか、適切な除外理由が見当たらないのでとりあえず採用した方がよいのではないかということで、セキュリティ対策を決定し、それに関する規程や手続きを整備し、運用しているケースがあるのではないでしょうか。セキュリティポリシーを運用する組織に所属する人は、万一のことを考えて、どうしてもセキュリティが目的になってしまいがちです。そうなると、「とりあえず禁止する」「とりあえず許可制にする」「とりあえず記録を残す」といった「とりあえずセキュリティ」が横行する可能性が高まります。

それでは、自組織内で、この「とりあえずセキュリティ」が見られる場合、どうしたらよいのでしょうか。もちろん、「対策基準」や「実施手順」を見直すことが必要なのですが、その前に「基本方針」を見直すことをお勧めします。昔作られた「基本方針」は、とにかく「守る」ことに主眼がおかれたものが多いはずです。これを、IT 活用や情報資産活用、ひいては業務改革・改善を目的としたものに変えることで、経営者の意思として、「攻めの」セキュリティの基本的な考え方を示すことができます。これが「とりあえずセキュリティ」から脱却するための近道になるのではないでしょうか。

3.3 クラウドの情報セキュリティ

クラウドサービス（SaaS：Software as a Service、PaaS：Platform as a Service、IaaS：Infrastructure as a Service 等）の利用は、その利便性の高さから、年々増加の傾向にある。一般社団法人日本情報システム・ユーザー協会（JUAS：Japan Users Association of Information Systems）の「企業 IT 動向調査報告書 2022[※204]」によれば、1,132 社を対象とする調査において、「パブリッククラウド（SaaS）」を「導入済み」と回答した企業が 53.6%、「パブリッククラウド（IaaS、PaaS）」を「導入済み」と回答した企業が 44.6% であり、多くの企業がクラウドサービスを導入している。

クラウドサービスは、オンプレミスのシステムに比べて、導入が容易であり、必要な機能を必要なだけ利用できることがメリットである。しかし、オンプレミスのシステムと異なり、クラウドサービスでは利用者側がカスタマイズできることには制限がある。セキュリティ対策の検討や実装についてはクラウドサービス事業者（以下、事業者）が主体的に実施するため、クラウドサービス利用者（以下、利用者）の求める強度の対策がとられていなかったり、詳細な対策内容を利用者が容易に確認できないため十分であるか判断がしにくかったりというデメリットがある。安全、安心にクラウドサービスを利用するためには、利用の成功事例・課題解決事例や事業者が公開している情報を収集したり、セキュリティ対策に必要な情報を事業者に問い合わせる等、利用者側の積極的な活動も必要となる。

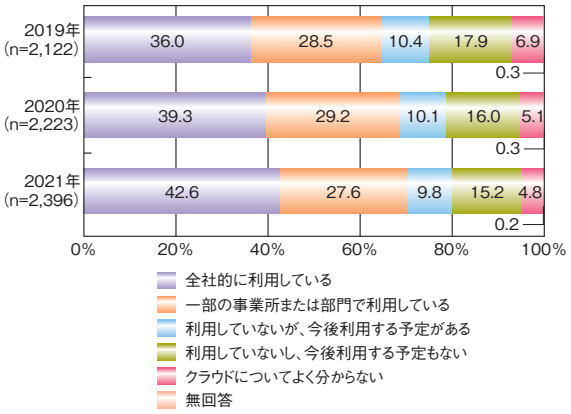
クラウドサービスの導入が増加する一方で、利用者の設定ミスにより、第三者から情報が閲覧可能な状態となっていたり、不正にアクセスされて情報が漏えいしたりというインシデントも後をたたない。Fortinet, Inc. が 2022 年 3 月に、全世界 823 人のサイバーセキュリティの専門家を対象にした調査結果によると、パブリッククラウド環境のセキュリティ対策状況について回答者の 95% が「懸念がある」と回答した（「中程度に懸念」「非常に懸念」「極めて強い懸念」の合計）。また、最も懸念しているクラウドセキュリティの脅威については、62% が「クラウドの設定ミス／セットアップの間違い」であると回答した[※205]。

総務省からも「クラウドサービス利用・提供における適切な設定のためのガイドライン」（「3.3.4 クラウドサービスの情報セキュリティに対する政府・関連団体の取り組み」参照）が公開されており、クラウドサービスを利用する上での適切な設定が促進され利用者が安全、安心にクラウドサービスを利用できることが望まれる。

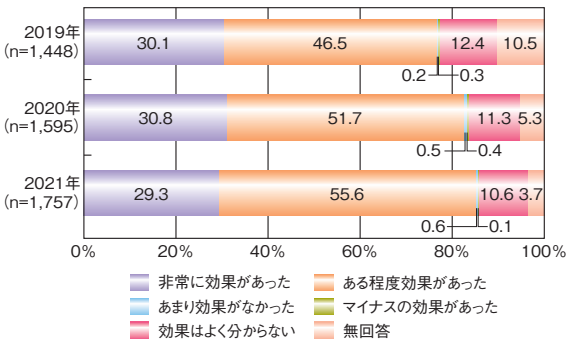
本節では、クラウドサービスの設定ミスを中心にクラウドサービスの利用の現状、インシデント被害、課題と対策、セキュリティの政策等について述べる。

3.3.1 クラウドサービスの利用状況

総務省の「令和 3 年 通信利用動向調査報告書（企業編）[※206]」によれば、従業員 100 人以上の企業 2,396 社について、クラウドサービスを利用していると回答した割合は 70.2%、2020 年の 68.5% より 1.7 ポイント増加した（図 3-3-1）。更にサービス利用の効果について「非常に効果があった」または「ある程度効果があった」と回答した企業は 2020 年の 82.5% より 2.4 ポイント増加した（図 3-3-2）。クラウサービスの利用状況及び利用効果は堅調に推移しており、今後もクラウドサービスの利用は増加していくと考えられる。

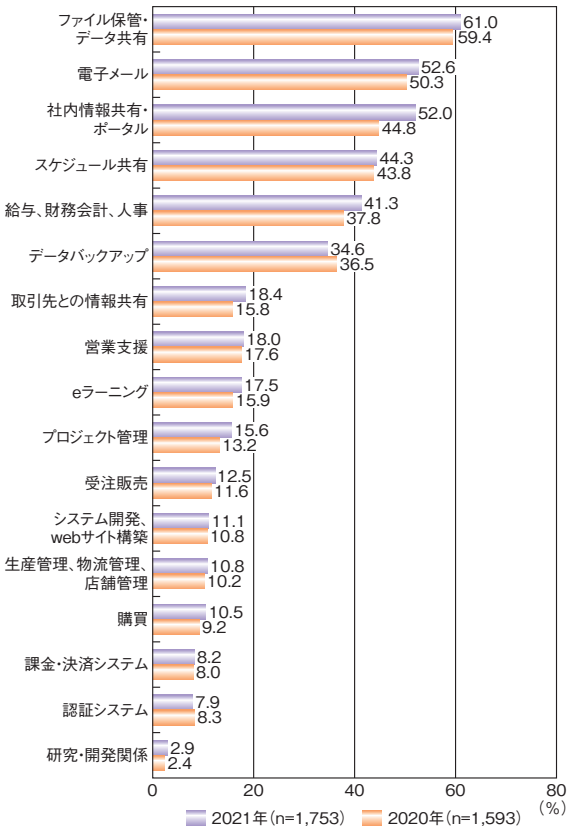


■図 3-3-1　クラウドサービスの利用状況の推移
（出典）総務省「令和 3 年 通信利用動向調査報告書（企業編）」を基に IPA が編集



■図 3-3-2　クラウドサービスの効果の推移
（出典）総務省「令和 3 年 通信利用動向調査報告書（企業編）」を基に IPA が編集

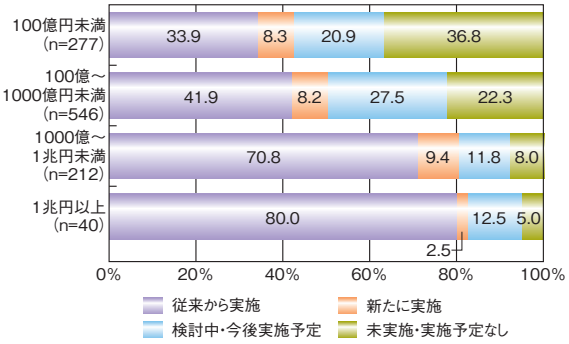
総務省の「令和 4 年版 情報通信白書※207」によると、クラウドで利用しているサービスの種類は「ファイル保護・データ共有」(61.0%)が最も高く、「電子メール」(52.6%)、「社内情報共有・ポータル」(52.0%)と続く。回答した半数以上の企業が日常業務で必須となるデータの共有や電子メールにクラウドサービスを活用しており、企業活動において、クラウドサービスが重要な役割を果たしていることが見て取れる(図 3-3-3)。



■図 3-3-3　クラウドサービスの利用内訳
(出典)総務省「令和 4 年版 情報通信白書※207」を基に IPA が編集

JUAS の「企業 IT 動向調査報告書 2022」によると、SaaS を 2021 年度より前から利用している企業の割合は「1 兆円以上」(80%)、「1000 億～1 兆円未満」(70.8%)、「100 億円～ 1000 億円未満」(41.9%)、「100 億円未満」(33.9%) となっており、売上高規模が大きい企業程、先行して活用している状況が確認された。クラウドサービスの利用料は従量制のため、企業規模によらずクラウドの恩恵を大いに受け、サービスを速やかに効率的に提供／利用できるはずだが、既存のシステムがある企業ではクラウドサービスに移行するためのリソースやコスト等がボトルネックとなり、クラウドサービスの活用を進められない状況が推察されると報告している(図 3-3-4)。

IDC Japan 株式会社によると、日本のパブリッククラウドサービス市場は、2021 年は 1 兆 5,879 億円（前年比 28.5%増）となっており※208-1、「令和 4 年版 情報通信白書※208-2」によれば、新型コロナウイルス感染症（以下、新型コロナウイルス）の感染拡大を契機としたオフィスの移転・縮小に伴うクラウドへの移行や、DX、データ駆動型ビジネスを進めるためにクラウドを活用した ICT 基盤の強化が進むこと等によって今後も拡大が予想されるという。



■図 3-3-4　売上高別 SaaS 活用状況
(出典)JUAS「企業 IT 動向調査報告書 2022」を基に IPA が編集

3.3.2 クラウドサービスのインシデント事例

2022 年も 2021 年に引き続き、クラウドサービスの利用者の設定ミスに起因するインシデントが多く見られた。原因の特定や対策が速やかに行えているように見える一方、発覚の経緯が外部からの連絡である事案が多く見られた。

この項では、クラウドサービスのインシデント発生状況及び主に 2022 年に発生したクラウドサービスに関連するインシデント事例について紹介する。

(1) クラウドサービスのインシデント状況

Sophos Ltd. が、IaaS を利用している 31 ヵ国の中堅・中小企業(SMB：Small and Medium Business)の IT 担当者 4,984 名に対して実施したクラウドセキュリティに関する調査※209 によると、2022 年に経験したサイバー攻撃に次のような変化があったという。

- 56% のユーザーが、組織に対する攻撃の量が増加したと回答
- 59% のユーザーが、組織に対する攻撃がより複雑になっていると回答
- 53% のユーザーが、組織に対する攻撃の影響が増加したと回答
- 67% のユーザーが、自社がランサムウェアの被害を受

けたと回答

このように半数以上の回答者が攻撃の増加、複雑化、組織への影響の増加を感じ、ランサムウェアの被害を受けている。しかし、IaaS の保護に不正侵入防止システム（IPS：Intrusion Prevention System）を導入していると回答した人の割合は 40%、Web アプリケーションと API（Application Programming Interface）の保護に WAF（Web Application Firewall）を使用していると回答した人の割合は 44% となっており、対策が十分でないことが分かった。また、IaaS のリソースの設定ミスを追跡・検出していると回答した人の割合は 37%、IaaS のリソースのソフトウェア脆弱性を定期的にスキャンしていると回答した人の割合は 47% にとどまり、設定ミスや脆弱性の放置により、攻撃されやすい環境になっていることが分かった。

トレンドマイクロ株式会社の「2022 年上半期サイバーセキュリティレポート※210」によると、2022 年上半期には Web やクラウドのシステムからの情報漏えいは 38 件確認され、公表内容等から漏えい情報の件数を合計すると全体で 430 万件の情報が漏えいした可能性があり、これらの事例の発生原因としては、約 7 割が脆弱性であったという。

これらの調査結果から、クラウドサービスにおいても多くのインシデントが発生しており、その原因として設定ミスや脆弱性が挙げられていること、そして、その対策が十分でないことが読み取れる。設定ミスに起因するインシデントは、社内で設定ミスを事前に発見すれば防止できたものである。例えばクラウドサービスを利用した情報管理を行う際には公開範囲の設定が適切であるか十分注意を払う必要がある。

(2) 設定ミスに起因するインシデント

ゲームコンテンツ、情報サイト、EC サイト等の企画・開発・運営を行う IT 企業である株式会社エイチームにおいて、2022 年 4 月 7 日、採用に関する情報がインターネット上で閲覧可能になっているとの指摘がエイチーム監査役から社長室長、管理部長、IT システム部門マネージャーに報告された。調査の結果、一部の個人情報がインターネット上で最長 6 年以上閲覧可能な状態にあったことが発覚した※211。

閲覧可能となっていた個人情報は新卒採用イベントやインターンシップに参加した学生 4,588 名の氏名、学校名等、グループ従業員 161 名分の氏名、所属部署、顔写真等、2016 ～ 2017 年に実施した中途採用イベントの参加者 30 名の氏名、メールアドレス、職業等、2017 年 8 月～ 2021 年 10 月に面接等の交通費を支給した 1,078 名の氏名、振込先口座番号等であった。2022 年 5 月 16 日の時点で、個人情報を閲覧できる状態は解消したこと、また不正使用等の被害は確認されていないことを発表している。

クラウドサービスを利用して作成した個人情報を含むファイルに対して、閲覧範囲の公開設定を「このリンクを知っているインターネット上の全員が閲覧できます」としたことが原因であり、個人情報を含むすべてのファイルに閲覧制限を実施したとしている。

更に同社は、本件に関して個人情報保護委員会へ報告するとともに、クラウドサービスを利用したファイルのアクセス範囲設定の見直し、個人情報を含むすべてのデータへのアクセスの制限を実施した。今後は、個人アカウントを用いてクラウドサービス上に作成したファイルの業務での利用を禁止し、法人アカウントでクラウドサービス上に作成したファイルのみ業務で利用可能にするという。加えて、社内でのチェック体制の強化、個人情報に関する管理体制の強化、情報管理に関する規程やルール等の見直し及び社内周知の徹底等の再発防止に努めるとしている。

一般社団法人シェアリングエコノミー協会において、同協会が主催するイベントの申込者の個人情報が、2022 年 7 月 1 日～同月 20 日 11 時 53 分ごろまでの間、第三者が閲覧可能となっていたことが判明した※212。

2022 年 7 月 1 日、同協会が主催するイベントの申込フォームを Web ページに掲載したところ、7 月 20 日 10 時 24 分に申込者から他人の申込情報を閲覧できるとのメールを受信、同メールの状況を 11 時 53 分に確認した。直ちに第三者が他人の申込情報を閲覧できないようイベントシステムの設定を変更、16 時 30 分に個人情報漏えいの可能性に関するお知らせとお詫びのお知らせを Web ページで公表した。2022 年 7 月 20 日時点で、漏えいによる被害の発生は確認できていないとしている。

本イベントの申し込みに利用した Google フォームの設定ミスにより、106 名の申し込み情報（氏名、電話番号、メールアドレス等）が第三者から閲覧できる状態になっていたことが原因であった。

同社は、2022 年 7 月 20 日に個人情報保護委員会に報告するとともに、個人情報が漏えいした可能性のある申込者 106 名へメールによる連絡を実施し、再発防止対策として、申込フォーム公開時のチェック体制の強化、

事務局に対するセキュリティ研修を実施するとしている。

このほか、2022 年 6 月にもライフイズテック株式会社で Google フォームの設定ミスにより個人情報が閲覧可能であったというインシデントが発生している※213。

(3) 委託先の設定ミスに起因するインシデント

2020 年 6 月 4 日、ヘルスケアサービス関連事業を行うケアプロ株式会社（以下ケアプロ社）において、同社の委託先のデータベース上で管理されている顧客情報が第三者から閲覧できる状態になっていたことが判明した※214。

第三者から参照可能となっていた情報は 2012 年 1 月 18 日から 2019 年 12 月 20 日までに同社でイベントを開催した顧客の情報（イベント開催場所、物品配送情報、物品受渡担当者名等 622 件）であった。

ケアプロ社の物流委託先のアカウントの一つが不正利用された可能性があると、委託先が利用する Amazon Web Services（AWS）から連絡を受けて調査を行った結果、委託先の自社サーバーから AWS サーバーへの移行時に、AWS のストレージに同社のデータをバックアップとして保管しており、委託先がストレージの設定を公開設定としたため、第三者に閲覧可能となっていたことが判明した。AWS と委託先の調査によれば不正利用の形跡はなかったという。2020 年 1 月 9 日、警視庁渋谷警察署生活安全課保安係サイバー担当に経緯を相談し対応策の指示を受け、対応を行ったとしている。

ケアプロ社の委託先では、再発防止策としてクラウドサービス利用者のアカウント・パスワードが適切に管理されていること（使いまわしの見直し、アカウント削除を含む ID 管理の徹底等）の確認、すべてのパソコンから重要情報が漏えいしないよう、ハードディスクの暗号化や、セキュリティソフトの導入を確認するとともに、AWS サポートと連携し、不正利用覚知の迅速化のため、海外で利用されていないかを利用履歴により継続的に確認することとした。

またケアプロ社は、二次被害等が発生した場合は、関係官庁や警察機関との連携を取りながら対応を進めるとしている。

3.3.3 クラウドサービスのセキュリティの課題と対策

企業・組織ではクラウドサービスが事業活動で利用されるだけでなく、企業・組織の基幹システムとして利用されることも多くなっている。そのため、クラウドサービスに関連するシステムの停止や脆弱性はビジネスへの影響が大きくなってきている。本項では、クラウドサービスのセキュリティの課題と対策について述べる。

(1) クラウドサービスのセキュリティの課題と対策

オンプレミスのセキュリティ対策とは異なるクラウド特有のセキュリティ対策が求められる。その代表が事業者と利用者がそれぞれに責任を分担し、全体としてセキュリティを確保する責任共有モデルの考え方である。総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）※215」でも取り挙げられ、SaaS における管理と責任共有については、「情報セキュリティ白書 2022※216」の「3.3.3 クラウドサービスのセキュリティの課題と対策」にも記載した。概念は浸透しつつあると考えられるが実践する上での課題はいくつか残っている。

「3.3.1 クラウドサービスの利用状況」に述べたようにクラウドサービスの利用は拡大しており、1 社が複数のクラウドサービスを組み合わせて利用し、管理が複雑になっていることが推定される。このような状況では、設定ミスを発見したり、脆弱性の有無を判断して対応したりといった対策を人手で実施することは限界があるため、管理ツールやサービスの利用が有効である。サイバー攻撃の手口等は日々変化をしているので、ツールやサービスの検討には利用しているクラウドサービスの内容やビジネス環境も考慮し、守るべきものが何か、最もリスクが高まっているのはどこかを見極めることが重要である。

ツールやサービスの利用により設定ミスや脆弱性が検知されれば対策も取りやすくなることが期待されるが、最終的に人が判断する側面は残っており、またそもそも、何を検知する、何に対応するというルールは人が策定すべきである。SaaS の場合は、責任範囲がデータとアプリケーションの利用者アカウント管理に限定されることから、保守体制を持たない、あるいは、利用部門が管理することも多くなる。そのため、クラウドのセキュリティ対策について十分な知識がなく、また対策が十分であるかを確認できないまま利用せざるを得ないことが懸念される。「3.3.2 (2) 設定ミスに起因するインシデント」に挙げた事例でも、情報の開示範囲は利用者が設定し、サービス開始後も開示範囲を確認することが求められていた。しかし、結果として公開された状態で放置されてしまっていた。

対策としては、オンプレミスのシステムを利用していたときと同様に、情報システム部門の管理下でのみ利用を認めるという方法も有効である。しかし、企業、組織内の体制見直しがクラウド導入の理由であったり、利用部門からの様々なクラウド利用要望が拡大したりといった状況

においては、特定の部門の管理下に制限するよりも、社内のどの組織においても、安全・安心にクラウドが利用できるように明確なルールを定め、そのルールを順守できるよう従業員を教育することが求められる。ルールには導入する際に事業者に確認するべきことや利用時に問題を発見したときの報告先等を最低限含めるべきである。

(a) 事業継続上のリスクへの対応

クラウドサービスにおける責任分担モデルでは、セキュリティを確保する責任は利用者に残っている。インシデントが発生した際の事業継続についても、クラウドサービスを利用していたからと言って、自社の責任を免れるものではない。クラウドサービスを利用していたからと言って、自社の責任を免れるものではない。

クラウドサービス事業者はあらかじめ責任範囲や補償範囲、SLA（Service Level Agreement：サービス品質保証）等を詳細に規定しており、クラウドサービス利用者にどのような被害、影響があったとしても、この規定の範囲でしか補償を行わない。2022 年 7 月、Microsoft Corporation が提供する Microsoft Teams 等のサービス群において障害が発生し、同サービスを利用できない事態が続くというインシデントが発生した※217。この障害は復旧までに約 5 時間を要した。サービスが停止した約 5 時間は Microsoft Corporation が事前に告知していた SLA 99.99% の補償範囲内であるため、利用できなかったことに対して利用者への損害賠償等はされなかった。SLA の補償範囲内であろうと業務時間内にサービスが停止した場合、どのような影響が見込まれるのか、代替手段はあるのか、そこでの営業損失等は容認可能なものか、事業継続の観点からも検討が必要となる。

(b) 海外データ保管のガバナンスリスクへの対応

クラウドサービスを利用することで新たに考慮すべき事象を含めたセキュリティ対策要件の検討が必要である。例えば、自社内で保管していたデータをクラウドサービス上に保管する際、保管先が国内のデータセンターとは限らない。個人情報保護法 28 条では、「個人情報取扱事業者は外国にある第三者に個人データを提供する場合、これについての本人の同意が必要」と規定している。利用したいサービスに個人データが含まれるか、クラウドサービス事業者が個人データを取り扱うサービスについて本人の同意を得ているのか等、あらかじめ確認すべきことがある。クラウドサービスで個人情報を扱う場合は、個人情報保護委員会が公開している法令、ガイドライン及び「『個人情報の保護に関する法律についてのガイドライン』に関する Q&A※218」等を確認することが必要である。また、個人情報の有無にかかわらず、データセンター所在国の法規制が適用されることも考慮する必要がある。米国、英国、中国等では政府、あるいは規制当局による閲覧や差し押さえが起こり得る。2009 年には米国で FBI が調査のためにデータセンターの機材をすべて押収し、顧客約 50 社が電子メールやデータベースにアクセスできなくなる事案が発生している※219。

事業者側には約款や利用規則、SLA を順守する責任はあるが、それが利用者の求めるセキュリティ強度を満たしているのかは、利用者が判断しなければならない。もしも、使いたいクラウドサービスのセキュリティ対策が、自社の求めるレベルに至っていなければ、そのサービスを利用しない、対策を追加で実施する、あるいはそのサービスを使うリスクを許容する、等を判断しなければならない。

(2) 安全・安心にクラウドを利用するために

「3.3.2 クラウドサービスのインシデント事例」で述べたように、設定ミスがクラウドサービスのインシデント原因として注目されているが、利用者の設定ミスは、利用者の認識不足や知識不足によるところも大きい。安全・安心にクラウドサービスを利用するためには、事業者が適切な情報を開示し、利用者がその情報を利用して必要な行動をとることが必要である。情報開示と利用のポイントを IPA の調査結果を基に述べる。

(a) クラウドサービスの情報開示、情報利用の実態

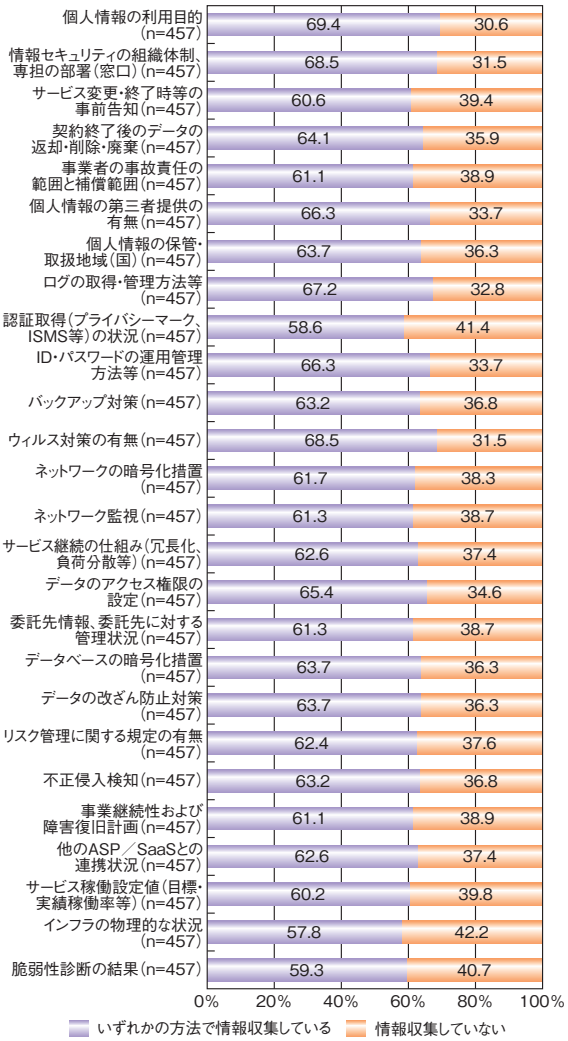
パブリッククラウドのサービスでは、事業者が用意したサービスのメニューから利用者が利用したいものを選択してそのまま利用する。通常は利用者ごとのカスタマイズはできない。クラウドサービスを選定するために必要な情報は利用者が公開情報から入手したり、事業者のカタログやパンフレットを読んだり、営業担当者の話を聞いたり、事業者に問い合わせをしたりといった方法によって利用者自らが収集する必要がある。

総務省は、クラウドサービスの安全・信頼性を向上させるため、利用者によるクラウドサービスの比較・評価・選択等に資する情報の開示項目を示した「クラウドサービスの安全・信頼性に係る情報開示指針」（以下、情報開示指針）を公表している※220。

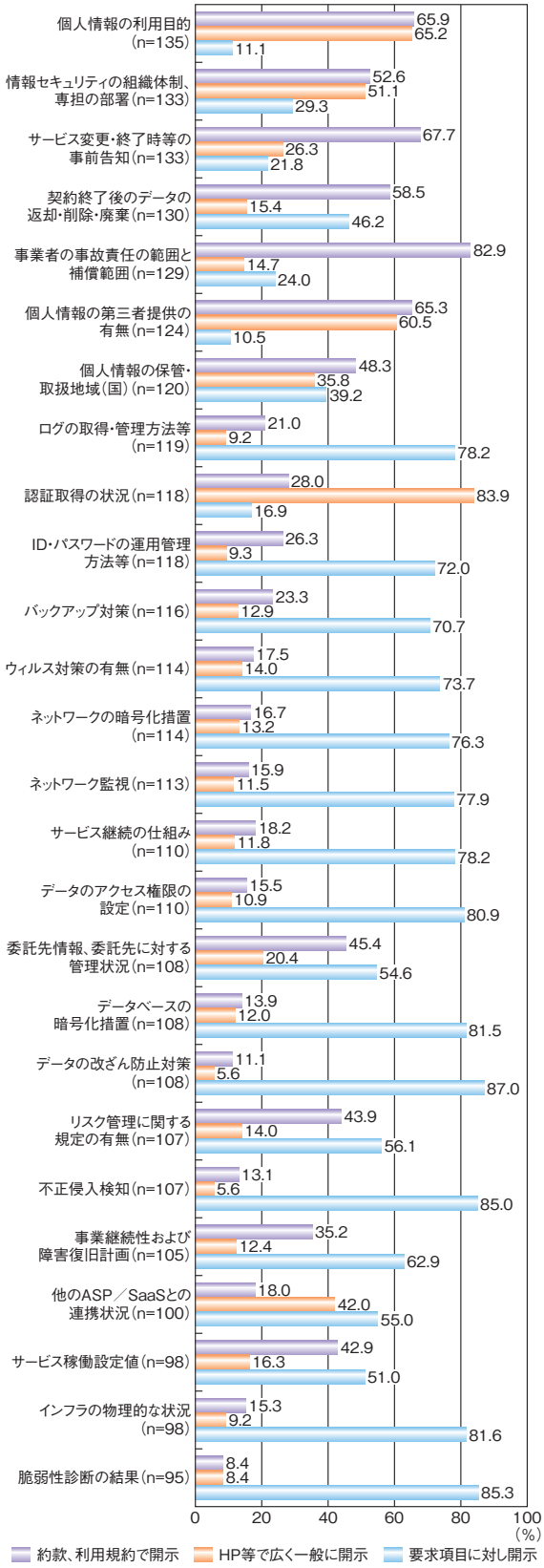
IPA は 2022 年に「クラウドサービス（SaaS）のサプライチェーンリスクマネジメント実態調査※221」（以下、2022

年クラウド調査）で、事業者の情報開示、利用者の情報入手の項目や方法について調査した。情報開示指針から、IPA が選定した 26 情報について、企業・組織で 2020 年 4 月以降クラウドサービスの選定や運用に携わった経験のある利用者に契約前（選定時）に情報を収集・利用しているかを質問した。各情報について 57.8 ～ 69.4% の範囲で収集していると回答した（図 3-3-5）。

事業者に対しても同様の情報について情報開示の状況を質問したところ、66.0 ～ 98.8% の範囲で情報開示をしていると回答した。事業者の情報開示は、約款や利用規約、Web ページ等で誰でも閲覧できるようにしている場合（公開情報による対応）と、チェックリストや質問票、問い合わせ等により情報提供を要求された場合に個別に対応する場合（個別要求への対応）があり、情報によってそのどちらかあるいは両方を行っていることが分かった（図 3-3-6）。



■図 3-3-5　契約前（選定時）の情報収集・利用状況（利用者）
（出典）IPA「クラウドサービス（SaaS）のサプライチェーンリスクマネジメント実態調査」を基に編集



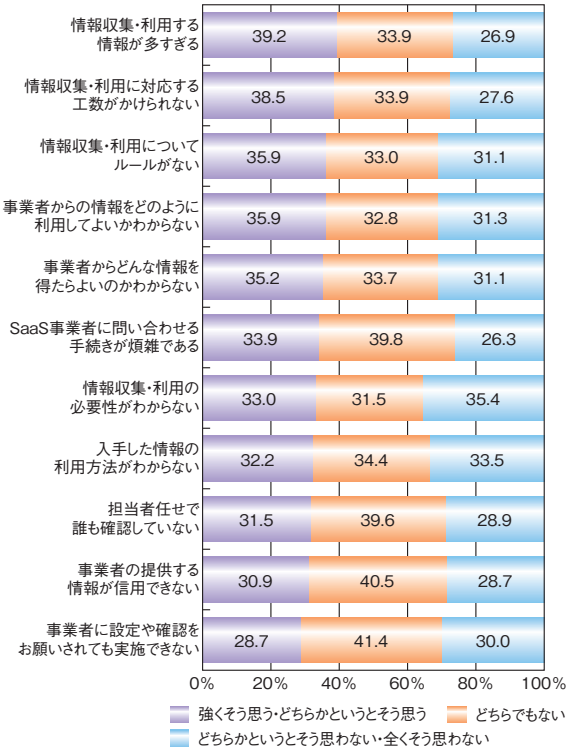
■図 3-3-6　契約前（選定時）の情報開示の方法（事業者）
（出典）IPA「クラウドサービス（SaaS）のサプライチェーンリスクマネジメント実態調査」を基に編集

「公開情報による対応」を行っている代表的な情報には、「個人情報の利用目的」「情報セキュリティの組織体制、専担の部署」「個人情報の第三者提供の有無」等、個人情報の取り扱い上法律やガイドラインで公表が求められる情報、「認証取得の状況」等サービスの信頼性をアピールできる情報、「サービス変更・終了時等の事前告知」「契約終了後のデータの返却・削除・廃棄」「事業者の自己責任の範囲と補償範囲」等、事業者の責任範囲を明示する情報があった。また、「個別要求への対応」を行っている情報には、データ、ネットワーク、インフラ等の技術的対策が多く含まれていた。利用者に開示する情報にはセキュリティ対策上やビジネス上で機密性の高い情報が含まれることがある。そのため事業者は、情報が攻撃に悪用されたり、ビジネス上の不利益を生じたりすることがないように、情報ごとに開示の可否や方法を変えていることが分かった。

2022 年クラウド調査で事業者に、セキュリティに関する情報を開示することにより、攻撃を受けやすくなると思うか質問したところ、「全くそう思わない、どちらかというとそう思わない」と回答した割合が28.4% であるのに対し、「強くそう思う」「どちらかというとそう思う」と回答した割合の合計は 46.1% に達し、17.7 ポイントも差があった。情報開示に起因したサイバー攻撃を懸念する回答が多かったことに対して、攻撃につながるような情報は出す必要がない、その上で公開は企業のセキュリティへの姿勢を示すもので大切だ、といった有識者からの意見もあった。

一方、選定時にどのような方法で前述の 26 情報を入手しているのかを利用者に質問したところ、「約款、利用規約」から入手していると回答したのは最大で 52.7%、「HP 等の公開情報」から入手していると回答したのは最大で 37.5%、「要求して収集」していると回答したのは最大で 20.3% であった。図 3-3-6（前ページ）に示したように、事業者が公開している情報は利用されている可能性が高いが、個別に要求されなければ開示しない技術的な対策について、利用者は十分な情報を入手していない可能性がある。

2022 年クラウド調査で、利用者の情報収集、情報利用の課題について質問したところ、「強くそう思う・どちらかというとそう思う」割合は、「情報収集・利用する情報が多すぎる」が 39.2% と最も高く、「情報収集・利用に対応する工数がかけられない」（38.5%）、「情報収集・利用についてルールがない」（35.9%）、「事業者からの情報をどのように利用してよいかわからない」（35.9%）、「事業者からどんな情報を得たらよいのかわからない」



■図 3-3-7　SaaS の情報収集・利用における課題（利用者 n=457）
（出典）IPA「クラウドサービス（SaaS）のサプライチェーンリスクマネジメント実態調査」を基に編集

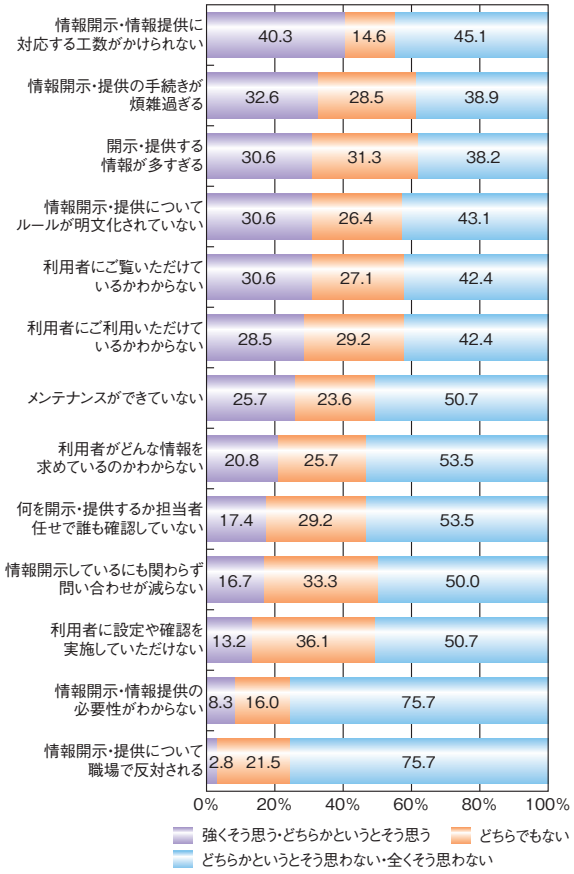
（35.2%）が続いた（図 3-3-7）。

事業者の情報開示の課題について同様に質問したところ、「強くそう思う・どちらかというとそう思う」割合は、「情報開示・情報提供に対応する工数がかけられない」が 40.3% と最も高く、「情報開示・提供の手続きが煩雑すぎる」（32.6%）、「開示・提供する情報が多すぎる」（30.6%）、「情報開示・提供についてルールが明文化されていない」（30.6%）、「利用者にご覧いただけているかわからない」（30.6%）、「利用者にご利用いただけているかわからない」（28.5%）が続いた（次ページ図 3-3-8）。

調査の結果から、利用者、事業者ともに対応工数、情報量、ルールについての課題が上位であることが分かった。また事業者の課題は、利用者が何を見て、どう利用しているのか分かっていない、情報の送り手としての実態把握ができていないことであることが分かった。利用者の課題は何を得て、どう利用したらよいか分かっていない、情報の受け手としての知識が不足していることであることが分かった。

(b) クラウドサービスのセキュリティチェック項目

IPA の 2022 年クラウド調査で、利用者に選定時に収集する情報について参照しているガイドラインがあるかを質問したところ、「他社の事例や、コンサルタントなどの



■図 3-3-8　SaaS の情報収集・利用における課題（事業者 n=144）
（出典）IPA「クラウドサービス（SaaS）のサプライチェーンリスクマネジメント実態調査」を基に編集

情報を参考にしている」（37.9%）、「総務省の情報開示指針」（21.2%）、「情報開示指針以外の基準・ガイド・チェックリスト」（1.3%）（複数回答可）という結果であった。同調査で事業者に情報開示・情報提供を行う内容を決定する際に参照しているガイドラインがあるかを質問したところ、「他社が開示している情報を参考にしている」（53.5%）、「総務省の情報開示指針」（44.4%）、「参照するものはなく担当者の判断で行っている」（25.0%）、「情報開示指針以外の基準・ガイド・チェックリスト」（15.3%）（複数回答可）という結果であった。つまり、どんな情報を収集、開示するかについては利用者も事業者も他社の様子をうかがいながら判断しているという回答が最も多いが、総務省の情報開示指針を参照している割合が、他の基準・ガイド等を参照している割合より多いということが分かった。まずは現在収集、開示している項目が情報開示指針の項目を含んでいるかを確認することが利用者、事業者ともに推奨される。

事業者は約款や利用規約、あるいは、インターネット上に情報を開示し、いつでも、誰でも内容が確認できることが望ましい。ここで、機密性の高いセキュリティ対策の詳細やセキュリティの設定情報等、攻撃等に悪用される恐れがある項目は実施の有無程度の記載にとどめる、あるいは、個別の問い合わせがあった場合の回答のルールを決めておくこと等が重要である。

利用者は公開情報だけでは、自社に必要なセキュリティ対策が実施されていることを確認できないことがある。そのような場合は、チェックリスト等により事業者に直接問い合わせる方法がよく利用される。チェックリストは複数の候補に対して同じ観点で比較ができることから、調達の手順の中にチェックリストの利用を規定し、自社のセキュリティポリシーやクラウド利用方針に基づくチェックリストを用意することは有効である。ただし、チェックリストは共通的な確認項目だけでなく、利用したいクラウドサービスに固有のセキュリティ要件について項目を付加したり、より詳細な回答を求めたりといった運用をすることが必要である。

チェックリストの作成でも参考にされることが多い情報セキュリティマネジメントシステムの国際規格である ISO/IEC 27001 は 2022 年 10 月 25 日に改訂され、「A.5.23 クラウドサービス利用のための情報セキュリティ」が追加された。この新しい管理基準では組織固有の情報セキュリティ要件に関連し、クラウドサービスの取得、使用、管理、及び終了に必要なプロセスを概説している。2022 年 10 月以降のチェックリスト見直しにおいてぜひ参考にしていただきたい。

また IPA では 2023 年 4 月 26 日、「中小企業の情報セキュリティ対策ガイドライン」を第 3.1 版に改訂した※222。同ガイドラインではクラウドサービスを安全に利用するための留意事項を示すとともに、付録として新たに「中小企業のためのクラウドサービス安全利用の手引き※223」を追加した。サプライチェーンの弱点を突いた攻撃で中小企業が狙われる恐れがあり、対策の強化が望まれる。中小企業に向けた支援策については「2.4.2 中小企業に向けた情報セキュリティ支援策」を参照いただきたい。

3.3.4 クラウドサービスの情報セキュリティに対する政府・関連団体の取り組み

クラウドサービスのセキュリティ対策向上のため、政府や団体が 2022 年度に公表・改訂したガイドラインやクラウドサービスの選定時に利用者が参考にできる認証・認定制度について主なものを述べる。なお、その他にも多数のクラウドサービスに関連する国内外の制度・ガイドラインが発行、改訂されている※224。

(1) クラウドに関する主なセキュリティガイドライン

2022年6月「デジタル社会の実現に向けた重点計画」の中で、「政府情報システムのためのセキュリティ評価制度(ISMAP)において、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みを、令和4年(2022年)中に策定し、当該仕組みを利用したクラウドサービスの申請受付を開始するなど、クラウド・バイ・デフォルトの拡大を推進する」ことが閣議決定した。この施策の一環として、2022年11月NISC、デジタル庁、総務省、経済産業省は「ISMAP-LIUクラウドサービス登録規則※225」を発行した。

総務省は、2022年10月「クラウドサービス利用・提供における適切な設定のためのガイドライン」(以下、設定ガイドライン)を公表した※226。設定ガイドラインは、2021年9月に総務省が改訂した「クラウドサービス提供における情報セキュリティ対策ガイドライン(第3版)」をベースに「クラウドサービスの設定」に特化し、事業者、利用者それぞれに対して、実施することが望ましい対策を記載している。設定ガイドラインの公表により、今後クラウドサービスの適切な設定の促進が図られることが期待される。また、設定ガイドラインの公表と同時に「ASP・SaaSの安全・信頼性に係る情報開示指針(ASP・SaaS編)」も第3版に改訂された。総務省が2007年から推進している情報開示指針の策定活動の一環である。サービスの種類別にこれまで8種類の情報開示指針が公表されている※220。

(2) クラウドに関連する認定制度

2022年11月、上記「ISMAP-LIUクラウドサービス登録規則」の発行と同時に「ISMAP-LIU」(イスマップ・エルアイユー:ISMAP for Low-Impact Use)の運用が開始された※227。ISMAPは2020年10月に運用を開始した制度で、対象はクラウドサービス全般に及ぶが、ISMAP-LIUはセキュリティリスクが低い業務や情報の処理に使うSaaSに限定した認定制度である(「2.7.3 政府情報システムのためのセキュリティ評価制度(ISMAP)」参照)。政府調達においては、ISMAPに登録されていることが条件となるが、登録されるサービスは政府だけでなく、企業や組織でも利用可能なものであり、機密性の高い情報を取り扱う業務等においては、ISMAPの登録の有無を選定の際の参考情報として利用できる。

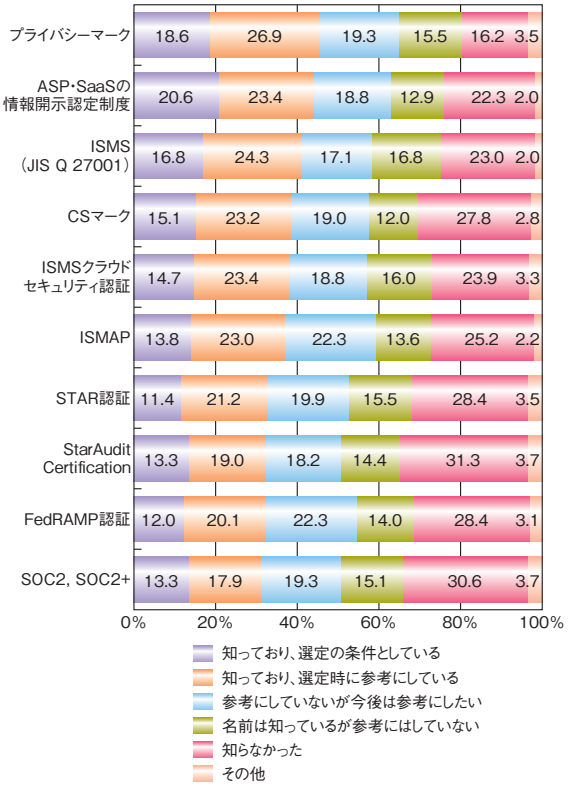
一般社団法人日本クラウド産業協会(ASPIC※228)は、総務省等が定めた各種ガイドライン、情報開示指針を基に、ASP・SaaS等、クラウドサービスの活用を考えている企業や地方公共団体等が、事業者やサービスを比較、評価、選択する際に必要な安全・信頼性に係る情報を適切に開示し、かつ一定の要件を満たすサービスを認定する情報開示認定制度を運営している。2022年7月には累積認定数が300サービスを越えた※229。認定されたサービスは、ASPICのサイト上に事業者名、サービス名及び申請内容が公開されている※230。申請内容は情報開示指針を基にしているので選定の際の参考情報として利用することができる。

CSA Security, Trust & Assurance Registry(以下、STAR認証)はCloud Security Alliance(CSA)が事業者のセキュリティ対応の透明性を確保するために行っている活動である※231。事業者は、CSAが提供しているCAIQ(Consensus Assessments Initiative Questionnaire)に基づいて、チェックリスト形式でCSAの提供するクラウド統制表(CCM:Cloud Control Matrix)に準拠しているかを自己評価し、そのレポートを公開している。CAIQの評価項目は日本語で読むことができ、登録情報も英語だけでなく、日本語の登録も可能となっている。2023年4月には「グローバルプロバイダが日本語CAIQ評価レポートを登録する方法」が公開された※232。グローバルにクラウドサービスの選定を行う際に、チェックリストとして参考にしたり、評価レポートを見比べたりすることができる。

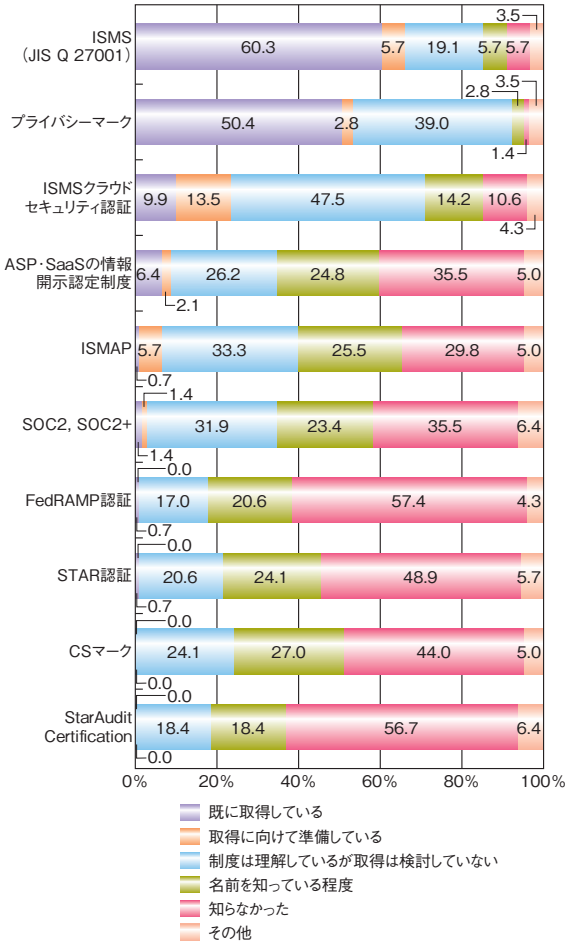
2022年クラウド調査によると、利用者のSaaSに関連する認定・認証制度の参照度合いは図3-3-9(次ページ)のとおりである。選定の条件としているという回答が最も多かったのはASPICが行っている「ASP・SaaSの情報開示認定制度」(20.6%)であり、その他は20%未満と低いことが分かった。しかし、「知っており、選定時に参考にしている」と「参考にしていないが今後は参考にしたい」を合計するといずれも50%を超えており、徐々に選定での利用が進むことが期待される。

事業者のSaaSに関連する認定・認証制度の取得状況は図3-3-10(次ページ)のとおりである。「ISMS(JIS Q 27001)」と「プライバシーマーク」については半数以上の事業者が取得済みであり、全体的に「取得に向けて準備している」という回答は少ない。ISMSやプライバシーマークは必要最低限取得したほうがいいが、その他の制度については様子を見ているように見受けられる。

認定・認証制度については、利用者側からは今後いろいろな制度も選定に利用していきたいという意識が見られたが、事業者側はISMSとプライバシーマーク以外は検討もされていないようである。認定・認証は、ある基



■図 3-3-9　SaaS に関連する認定・認証制度の参照度合い（利用者 n=457）
（出典）IPA「クラウドサービス（SaaS）のサプライチェーンリスクマネジメント実態調査」を基に編集



■図 3-3-10　SaaS に関連する認定・認証制度の取得度合い（事業者 n=141）
（出典）IPA「クラウドサービス（SaaS）のサプライチェーンリスクマネジメント実態調査」を基に編集

準に対する準拠度合いを示すものとして有効であり、特にセキュリティの知識が事業者程ない利用者にとっては、安心・安全なクラウドサービス選定の一助となる。事業者も利用者も魅力的なサービスの一項目としてセキュリティをとらえ、ガイドラインや認定・認証制度を活用することで、より安心、安全にクラウドサービスを利用できることが期待される。

3.4 虚偽情報拡散の脅威と対策の状況

ネット上の虚偽情報、あるいは真偽不明な情報の生成・拡散（特定の意図による拡散を含む）による社会の混乱や分断、対立は、近年その深刻さを増している。この脅威について、2010 年代前半までは意図的または自然発生的なデマ、差別・犯罪助長等の有害情報、詐欺的な購買行動への誘導等が問題視されてきた。2016 年の米国大統領選挙以降は、世界各国で世論誘導や選挙における中傷・扇動、新型コロナウイルス対策に関する混乱、ウクライナ侵攻におけるサイバー情報戦等の脅威が連続して発生し、虚偽、あるいは真偽不明な情報の生成・拡散にどう対応すべきか、課題となっている。

更に近年、生成系 AI（Generative AI）と呼ばれる AI によるコンテンツ生成技術が急速に向上し、事実に見せかけた架空のコンテンツ、あるいは不正確なコンテンツが容易に作れる事態となり、生成系 AI の利用の在り方の議論も始まっている。本項ではこうした虚偽あるいは真偽不明な情報の生成・拡散について、その脅威と対応の状況を述べる。

3.4.1 虚偽情報とは

「虚偽情報」とは何だろうか。単純な意味では事実と異なる、あるいは不正確な情報を指すが、近年、特にネット上で意図的に広められる当該情報が「Disinformation」あるいは「フェイクニュース（Fake news）」と呼ばれている。以下では虚偽情報の整理を試みる。なお、私怨等の個人的な理由で他者・組織を貶める虚偽情報は除外する。

(1) 虚偽情報の類型

虚偽情報に関連して用いられる用語を以下に整理する。

- Disinformation
  意図的に広められる虚偽情報。ここで意図とは、特定の組織・個人に利益または不利益をもたらすことが想定され、特に政治的な主張や攻撃、対立扇動の意図がある場合に Disinformation が用いられることが多い。国家安全保障に関わる虚偽情報にこの用語を用いるべき、との意見もある※233。
- フェイクニュース
  Disinformation と同様に意図的に広められる虚偽情報であるが、国内ではこの用語が定着している。ニュースの体裁は必要なく、SNS 上の個人の言説もフェイクニュースとなり得る。政治的意図はないが、内容がセンセーショナルで話題性や経済的利益を狙った虚偽情報もフェイクニュースと呼ばれることがある※234。
- Misinformation
  誤解・誤認・伝聞等による誤り、あるいは不正確な情報を指す。拡散意図は無関係とされる※235 が、国内ではその拡散を「デマ」と呼び、自然発生的であることが多い。ただし、Disinformation・フェイクニュースを正しいと信じ込み、自身の思いを付け加えた Misinformation を拡散する場合、結果として Disinformation・フェイクニュース拡散の一端を担ってしまう。
- Malinformation
  差別、権利侵害、犯罪助長等、倫理的に許されない情報や、危害を与える情報、誤解を招くような情報を指す。武器作成手法、プライバシー暴露等、虚偽でない情報も含まれる。国内でこれに近い言葉に「有害情報」がある。Disinformation の中には、例えば他者を差別、抑圧する言説で Malinformation とみなされるものもある。

上記のように各用語のカテゴリは重なり合っており、実際の虚偽情報拡散では各カテゴリの言説が混ざり合うことが想定される。そこで本項では、虚偽情報を特定カテゴリに絞ることはせず、Disinformation、フェイクニュースと呼ばれる情報を主体とするが、それらの拡散で派生的に生まれる Misinformation、Malinformation も包含する言葉として議論を進める※236。

なお情報の「虚偽性」については、以下の類型があると考えられる。

- 内容が事実でない、あるいは不正確なこと
  最も単純な虚偽である。
- 内容を拡大解釈、誇張すること
  宣伝、他者攻撃等でよく用いられる。
- 飛躍した論理で情報を関係させること
  無関係な事実や虚偽を並べ、推定に過ぎないストーリーを正しいストーリーに見せる、等。これは、「ナラティブ（Narrative）」と呼ばれる共感を呼びやすいストーリーに基づいた拡散手法として用いられる。

- 情報伝達の意図を誤らせること
  情報の本来の意図を錯誤させる。最も端的な例は宣伝を宣伝に見せずに人を誘導すること（ステルスマーケティング等）である。

(2) 脅威の類型

以下では、虚偽情報拡散による脅威の類型を整理する。

- 事実の捏造による他者攻撃・評価棄損
  最も直接的な形の脅威である。虚偽情報の内容は時々のイベントに基づき、イベントに関わった組織・個人の評価を棄損するコンテンツが捏造される。棄損の影響は時間的には限定される。報道機関やSNS事業者、第三者監視機関等のファクトチェックで対応可能と思われるが、2017年、Deepfake技術によるBarack Obama前大統領の虚偽動画のデモンストレーション※237が公開されて以降、対象コンテンツは動画・音声に及ぶこととなった。その真贋を一般利用者が判定することは難しく、一定の割合でそれを信用する利用者が出るリスクがある。
- 根拠不明な主張の浸透による対立・分断
  正しさの根拠を明らかにしない主張、誇張を含む主張は即座に虚偽と判定しにくいが、組織的・継続的に行うことで支持に至ることがある。2020年11月の米国大統領選挙において、Donald Trump大統領は選挙で不正が行われたと根拠を示さないまま繰り返した。Trump支持派は裁判所に選挙無効を訴え、すべて却下されたにもかかわらず、共和党支持者の多くが選挙不正を信じる結果となり、米国世論の分断は深まった。
  このように、対立構造が明快な問題について、根拠不明瞭な主張はプロパガンダに利用され、浸透するリスクがある。
- 虚偽情報の連鎖による行動の暴発
  一定の支持者を得る虚偽情報がSNS上で拡散し、それが新たな虚偽情報を連鎖的に発生させ、大きな流れを作ることがある。2016年、民主党大統領候補だったHillary Clinton氏が「小児性愛者グループの中心だ」という中傷がTwitterで拡散し、その「証拠」とされる情報が続々と投稿され、小児性愛のナラティブが作り上げられた末、Clinton派と関係があるとされたピザ店が市民の襲撃を受けた（ピザゲート事件）※238。
  このように、特定のナラティブに共感するSNSグループで虚偽情報の連鎖がエスカレートし、暴発することがある。ピザゲート事件の場合は極右団体QAnonの陰謀論※239と結びついたとされる。
- 災害時等の対応混乱・不安拡大
  災害・パンデミック等の社会不安が発生した場合、不安を解消するため、その要因を根拠なく特定して排除または攻撃する虚偽情報が拡散することがある。2020年の新型コロナウイルスの拡大期には、医学的に根拠のない対症療法等がSNS上で拡散された。また、2020年後半からのワクチン接種について、これに強く反発する団体等から「殺人ワクチン」等の主張とともに反対運動が起こった。これらの影響は限定的だったと見られるが、災害・パンデミック時の虚偽情報拡散は生命に関わることがあり、拡散の程度によらず注意すべきとの意見もある※240。
- 戦争における宣伝戦のエスカレート
  ウクライナ侵攻では、2種類のサイバー空間の戦いが現実のものとなった。一つはウクライナの重要ITインフラに対するサイバー攻撃と防御、もう一つがネット上での虚偽情報拡散を含む宣伝戦（認知空間の戦い）である。後者について、ロシアは多くの虚偽情報による宣伝戦を仕掛けた。Joseph Biden大統領は、米国のインテリジェンス情報を開示して対抗した。ウクライナも、Volodymyr Zelenskyy大統領が首都キーウから逃亡した等の虚偽情報に対抗してSNSで「自分はここにいる」と表明※241、影響を封じた。
  ロシアはまた、宣伝戦に前述のナラティブの手法を用いた。ナラティブは「人々に強い感情・共感を生み出す、真偽や価値判断が織り交ざる伝播性の高い物語」と定義され※242、例えば陰謀論「Aの元凶はB」もナラティブである。ウクライナ侵攻の場合「ロシアとウクライナは歴史的に不可分」「ウクライナ政府はネオナチ」がナラティブである。戦争や国家間の紛争においては、ナラティブと虚偽情報を交えた認知空間の戦いがエスカレートすることとなる。

3.4.2 虚偽情報生成・拡散の事例

本項では、2016年以降に起きた虚偽情報拡散の大規模事案を参考に、関係組織、情報生成及び拡散の仕組みを整理する。

(1) 2016年米国大統領選挙の妨害活動

2016年米国大統領選挙の妨害活動事案の内容、関係組織、手口、影響について述べる。

- 事案の内容
  2016 年 11 月の米国大統領選挙において、民主党へのサイバー攻撃による情報窃取・暴露、Clinton 民主党候補の中傷を含む Disinformation による選挙介入工作があったとされる。
- 関係組織
  米 国 ODNI（Office of the Director of National Intelligence）は、ロシア政府と Internet Research Agency（IRA）等の親ロシア系宣伝・情報操作企業による工作があったと断定した※243。IRA と関係者は 2018 年、選挙妨害により米国で起訴された。また、民間選挙コンサルティング企業の工作関与も報じられた（後述）。
- 手口
  IRA 等による情報操作では、Facebook 等の SNS アカウントを用いたインフルエンサーへのなりすまし、「Troll」と呼ばれる炎上投稿、政治広告出稿等があったという※244。また、SNS 拡散を効率化するボット※245も活用されたという※246。
  上記とは別に、選挙コンサルティング企業 Cambridge Analytica Ltd. による選挙介入工作が発覚した。2018 年 4 月、同社のデータアナリストが選挙工作のために Facebook, Inc.（現、Meta Platforms, Inc.）の個人情報 8,700 万人分を不正流用したことを認めた※247。Facebook 利用者の政治志向等を分析してメッセージを送るため、マイクロターゲティングと呼ばれる個人を特定した広告手法が活用されたという。同社へのロシア、Trump 陣営の関与も報じられたが、Trump 陣営の選挙介入工作への関与は明らかではない。
- 影響
  情報の暴露や中傷等の工作により Clinton 候補は打撃を受け、Trump 候補に有利に働いたとされる。一方、マイクロターゲティングによる工作はどの程度あったか、実際に効果はあったかは明らかでない※248。
  副次的な影響としては、デジタルによる選挙干渉が安全保障の問題と認識され、米国・欧州では敵対国家とその支援勢力の情報工作を規制する法制整備につながった。また SNS 事業者もファクトチェック等の規制を強めた。2018 年 11 月の米国中間選挙においては、米国サイバー軍（U.S. Cyber Command）が IRA の不正アクセスを遮断、選挙妨害を防いだとされる※249。

(2) Brexit に関わるポスト真実政治言説

Brexit に関わるポスト真実政治言説事案の内容、関係組織、手口、影響について述べる。

- 事案の内容
  2016 年 6 月 23 日の国民投票により、英国の EU 離脱（Brexit）が決定、2020 年 12 月 31 日に離脱が完了した。この間、残留派・離脱派による自派擁護・他派攻撃等の虚偽情報が蔓延した。客観的事実よりも個人の感情・信条に訴える政治的言説は「ポスト真実政治（Post truth politics）」と呼ばれた。
- 関係組織
  2017 年 11 月の時点で、欧州全体においてロシアによる虚偽情報を用いた工作は Brexit に関するものも含め拡大した、とされた※250。しかし、2020 年 7 月の英国議会情報セキュリティ委員会（Intelligence and Security Committee of Parliament）の報告では、Brexit に関するロシアの妨害活動を特定できなかった※251。虚偽情報の多くは英国内の残留派・離脱派によるポスト真実政治言説だったと思われる。
- 手口
  SNS を中心に虚偽情報が拡散された。虚偽情報には、3 年前の画像を現在の画像に見せる投稿、根拠のない離脱賛否情報を含む動画等、ファクトチェックで検知可能なものが多かった。また、「EU に巨額のお金を貢ぐのをやめ、自国で使おう」「Johnson 首相は EU との妥協なしの Brexit を実施、金融事業者と利益を得ることを画策」等のナラティブも発生、関連する虚偽情報が拡散した※252。
- 影響
  虚偽情報そのものの影響は自明ではないが、上記のポスト真実政治への傾向が強まったと思われる。実際、EU に対する英国政府の支出は全支出の 1% に過ぎない、という事実は説得力を持たなかった※253。こうした事実軽視、自身の信条に近い主張の選好は 2020 年の米国大統領選挙や 2022 年のウクライナ侵攻等でも世界的に見られる、との分析もある※254。

(3) 新型コロナウイルスのインフォデミック

新型コロナウイルスのインフォデミック事案の内容、関係組織、手口、影響について述べる。

- 事案の内容
  2020 年 1 月に新型コロナウイルスが中国で蔓延してから、2021 年末までの約 2 年間、新型コロナウイルス関連の虚偽情報が SNS、報道等で拡散し続けた。主な虚偽情報・不確定情報の類型は以下のようになる。
  ①発生源・感染主体に関する不確定情報

発生源は中国武漢市の市場あるいはウイルス研究所である可能性が高いとの西側メディアの報道が2023年4月時点も継続している※255。中国政府は強く否定している。感染主体については「アジア系の人々が感染を起こした」とのナラティブがヘイトスピーチとなって欧米で急拡散し、市民の暴力行為に発展した。インドではイスラム系の人々へのヘイトスピーチも拡散した。

②感染対処法に関するデマ

発生直後、根拠不明の多くの対処法が拡散した。多くがデマであったと考えられ、これらを否定する情報も拡散した。国内調査によれば、情報に接した多くの人がこれを疑ったが、一定の割合で信じてしまった人もいた※256。

③対策に関する詐欺情報

発生直後から、世界各国で詐欺情報が横行した。具体的には、関係省庁の注意喚起を装うフィッシングメール、マスク・新薬・ワクチン接種等に関する金銭詐欺、給付金支給に関する個人情報詐取等様々であった※257。

④ワクチン接種に関する不正確な主張

新型コロナウイルスワクチン接種に反対する人々は、医学的合理性が確認されていない「ワクチンによって死亡者が出た」等の言説によって反対運動を展開した。国内の反ワクチン運動については、政府のワクチン政策に対する不信がある、との分析もなされた※258。

- 関係組織

「コロナ禍は○○のせい」「ワクチンは陰謀」等のナラティブに共鳴したグループは、SNS等で虚偽情報の増幅・拡散を行ったと思われる。2021年4月、EUは、中国・ロシアが欧米のワクチン接種のリスクに関する虚偽情報をオンライン上で拡散しているとの見解を示した※259が、確証はない。

- 手口

デマ・詐欺情報の多くはSNSによる拡散であり、状況に応じて自然発生的に生じたと考えられる。ただし、ヘイトスピーチの拡散ではボットの利用が確認され※260、共鳴するグループが組織的に拡散したケースがあることがうかがわれる。各国は特定の発信源を統制するという対策を取れず、ファクトチェック・注意喚起が対策の柱となった。

- 影響

世界同時的な社会不安の発生に伴い、虚偽情報・根拠不明情報の同時蔓延も生じ、インフォデミック（Infodemic）という言葉が生まれた。便乗詐欺、ヘイトスピーチの標的となった人々には影響が出た。一方で、国内調査では、根拠不明な情報の拡散について多くのSNS利用者がこれを冷静に受け取ったとの結果もある※256。

なお、虚偽情報により、例えばワクチン忌避者の増加に影響があったか等は明らかでない。

(4) 2020年米国大統領選挙の不正選挙キャンペーン

2020年米国大統領選挙の不正選挙キャンペーン事案の内容、関係組織、手口、影響について述べる。

- 事案の内容

2020年11月の米国大統領選挙において、郵便投票に集計等の不正があったとTrump大統領が主張したことにより、関連する根拠不明な主張、虚偽情報が拡散した。Trump陣営は選挙結果が無効であるとしてミシガン州連邦地方裁判所等に提訴したが、根拠不十分で棄却され、更に最高裁判所に上告した接戦4州についても棄却された※261。選挙不正を信じるTrump支持派ではこれらの結果に対する不満が高まり、2021年1月6日、一部支持者が連邦議会を占拠、その鎮圧において死者5名が出る異常事態となった※262。

選挙不正を訴える主張は報道にも及び、保守系メディアのFox Newsの報道に対して、カリフォルニア州ロサンゼルス郡で使用された投票システムを納入した企業Smartmatic Corp.、ジョージア州で使用された電子投票機を製造した企業Dominion Voting Systems Corp.が、報道内容は虚偽であり名誉棄損であるとして提訴した。Fox NewsはDominion Voting Systems Corp.に関する報道の誤りを認め、2023年4月18日、同社に和解金7億8,750万ドルを支払うことで合意した※263。

- 関係組織

2020年9月、DHSは郵便投票の不正に関するロシアの虚偽情報拡散（結果としてTrump大統領支持）を警告した※264。しかし、2016年大統領選挙に比較するとロシアによる工作の影響は小さく、政府やSNS事業者のIRA監視等の対策がある程度有効だったと見られる※265。情報拡散の主体となったのは「盗まれた選挙」ナラティブに共鳴したTrump支持派であった。

- 手口

Trump 大統領の Twitter 発信を起点とする SNS 利用が中心だが、前述のように保守系メディアの報道にもファクトチェックがずさんな例があった。

なお、「盗まれた選挙」ナラティブは、投票用紙を封入した郵便物の紛失や配達遅延等、各州の郵便投票制度に不備があったことも説得力を持った一因とされる。民主党や非保守系メディアが各州の郵便投票制度の不備に触れずに「盗まれた選挙」を虚偽と決めつけたことも問題をエスカレートさせたとの見方がある※266。

- 影響

「盗まれた選挙」ナラティブを信じた共和党員と虚偽であるとした民主党員の亀裂は大きく、米国世論を分断する状況を深めてしまったと思われる。また、ナラティブが QAnon のような過激主義と結びついた場合に暴力が発生してしまうこと、SNS はその増幅器となってしまうことも明らかになった。

一方で、本事案への対応は言論の自由と規制の問題も提起した。Fox News の報道への提訴について、Fox News は当初言論の自由を盾に「報道する価値があるものに対する提訴は無効」と主張したが、提訴を受け司会者の降板等を行った。また SNS 事業者はファクトチェック等の不正コンテンツ規制対策を既に実践していたが、連邦議会占拠事案の発生により、Twitter, Inc.（現、X Corp.）は Trump 大統領のアカウントを停止、同大統領の情報発信を事実上封じた。この結果、Trump 大統領発信による虚偽情報による混乱は収束したが、報道提訴や民間企業の判断によるアカウント停止等がどのような場合に許されるのか、課題として残った。2022 年 11 月 19 日、Twitter, Inc. のオーナーとなった Elon Musk CEO は「言論の自由を守る」として Trump 氏のアカウントを復活した※267。

(5) ウクライナ侵攻におけるサイバー情報戦

ウクライナ侵攻におけるサイバー情報戦の内容、関係組織、手口、影響について述べる。

- 情報戦の内容

2022 年 2 月 24 日のウクライナ侵攻の準備、及び侵攻後のサイバー情報戦として、ロシアはナラティブや虚偽情報拡散による宣伝戦・サイバー攻撃を仕掛けた。対象は主としてウクライナだが、報道機関・SNS 等による世界的な宣伝・情報工作も行われた。これらの総体は、ロシアの安全保障政策に基づくサイバー情報戦の一環であり、2014 年のクリミア併合時点から継続している※268。ウクライナからロシアに対するサイバー情報戦も活発に行われているが、ここではロシアの活動に注目する。

- 関係組織

ロシアのサイバー情報戦の主体は政府、ロシア軍、RT（旧称、Russia Today）や SPUTNIK 等の親ロシア系報道機関、既出の IRA 等の親ロシア系宣伝・情報操作企業、親ロシア系ハッカーとされる。親ロシア系の第三国からの拡散もあるという※269。

- 手口

Web サイトハッキングによる情報改ざん・偽サイトによる拡散を始め、様々な媒体を通じた工作が行われている。ウクライナ侵攻で特徴的な活動としては以下がある。

①世界的なサイバーインフルエンス工作

Microsoft Corporation の調査によると、ロシアは国内・ウクライナ・西側諸国・非同盟国それぞれに、SNS 等に事前に配置した宣伝メッセージを一斉に拡散、自国・ウクライナ・非同盟国からの支持強化、及び西側諸国の分断誘発を図った※270。

②ウクライナ政府の評価を棄損する虚偽情報

宣伝メッセージにおいて、「ウクライナ政府はネオナチ」とする中傷、Zelenskyy ウクライナ大統領の虚偽動画、「同大統領が首都キーウを脱出」等の虚偽情報が用いられた。ただし、容易に見破れる内容が多く、Zelenskyy 政権の機敏な対応で直後に虚偽と判明した情報もある。

③偽旗作戦（False Flag Operation）

侵攻以前から「ウクライナ東部のロシア系住民が迫害された」「親ロシア勢力が攻撃された」等の情報が SNS 等で拡散した※271。米国はこれを、侵攻を正当化するロシアの「偽旗作戦」と断じ、Biden 大統領が公表するという異例の措置を取った※272 が、侵攻は防げなかった。

④ SNS「Telegram」の主戦場化

Telegram はロシアで誕生した守秘性の高い SNS であり、ロシア・ウクライナ双方で多くの人が利用している。2013 年のサービス開始以来、監視等の機能がないために極右・過激主義・反体制集団等が宣伝を行っていたが、政府の規制は免れていた※273。2022 年以降、Telegram はロシア、ウクライナ双方の政府及び政府支援グループが虚偽情報拡散・宣伝を行う主戦場となった。ロシア国民は自国に加え、ウクライナ及び西側諸国の拡散情報を自由に見ることができる※274。ロシア政府には Telegram 規

制が自国に有利でない、という判断があると思われる。Telegram 上では相手国政府にサイバー攻撃を行う「サイバー義勇軍」の勧誘も行われたという。

- 影響

ロシア政府の情報戦は、自国民の支持強化には成功した。肝心な対ウクライナについて、侵攻当初、ロシア政府は大半のウクライナ国民が支持または無関心の態度を取ると想定したと見られるが、彼らは反ロシアに回った。ウクライナに対する情報戦は失敗であったといえる。西側諸国の分断に対しても、ロシア政府の思惑は外れた※275。これらの誤算については、ウクライナ政府の SNS 等による情報戦が巧みであったこと、2014 年のクリミア侵攻の成功でロシアに楽観が生まれたこと、等が指摘されている。一方で、西側諸国や中国・ロシア陣営に与しないグローバルサウス諸国の支持については一定の効果があったものと見られる。

(6) 台湾における中国の情報工作

台湾における中国の情報工作事案の内容、関係組織、手口、影響について述べる。

- 事案の内容

台湾政府の政策実施を妨害し選挙に介入する、あるいは台湾政府・関係者の評価を棄損する虚偽情報の拡散が大量に行われている。台湾・日本・米国政府は台湾統一を目指す中国の情報戦の一環であるとしている。2022 年 8 月の Pelosi 米国下院議長の台湾訪問では、台湾近海での軍事演習に加え、Pelosi 議員及び台湾政府に対する誹謗や台湾からの中国人退去、中国国営メディア CCTV の記者による「中国軍機が台湾海峡横断」とのブログ投稿※276 等の虚偽情報が大量に拡散した。

- 関係組織

情報工作の主体は、中国共産党中央宣伝部、中国共産主義青年団、中国人民解放軍、中国ネット民（Chinese netizen）、政治関連のコンテンツファーム※277 等であるとされる※278。

- 手口

SNS が主体であるが、ロシアの情報戦のやり方を参考にしているといわれる。台湾の半導体企業に関する米国報道を曲解し、台湾政府与党が企業を米国に売ったという虚偽情報が大量に拡散された等の調査例がある※279。また 2019 年以降は、YouTube 動画を含む Facebook を利用した拡散が増えている※278。2022 年の Pelosi 米国下院議長訪問時の拡散では YouTube と掲示板型ソーシャルニュースサイトの Reddit を使った拡散が確認されており、複数の SNS を使用することでコンテンツを一斉に削除されないようにしている、との見方がある※280。

- 影響

2022 年 11 月の台湾統一地方選挙では、中国との対決姿勢を前面に出した与党・民進党は敗北し、蔡英文総統は党首を辞任した※281。中国の情報戦の影響は明らかではないが、工作に勢いがつくことが予想される。台湾は世界で最も虚偽情報の拡散に晒されているとされ※282、市民は SNS 上で正しい情報を得ることは難しくなったと感じるという。

もう一つの影響として、日本への虚偽情報拡散がある。台湾海峡の力による現状変更に反対し続ける日本にも中国は情報戦を仕掛けているとされ、例えば在日米軍基地を抱えて世論が分断しやすい沖縄での工作、あるいは台湾有事における日本の介入について日本国内を分断する工作等が懸念されている※283。

3.4.3 虚偽情報生成・拡散の流れ

以上の事例を基に、虚偽情報の生成・拡散の流れを整理した結果を図 3-4-1（次ページ）に示す。

(1) 生成・拡散の流れ

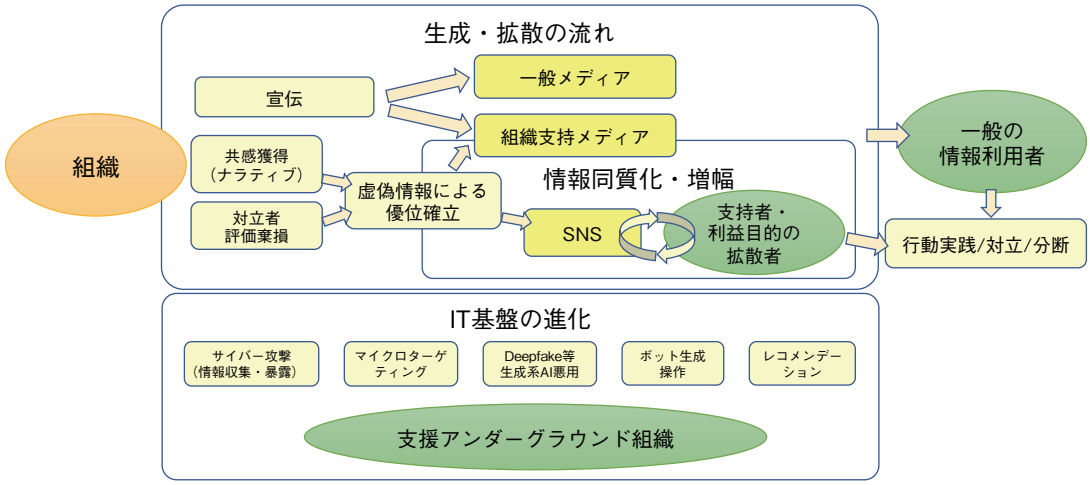
組織が自身の主張を基に優位を確立するため、宣伝、あるいは虚偽を含む情報拡散を行う。共感を得やすいナラティブがあると、それと虚偽情報を組み合わせる。共感した支持者、あるいはアクセス数や広告収入増加等の利益（アテンションエコノミー）を意図した第三者が増幅・拡散を行う。虚偽情報単独での拡散は限定的だが、ナラティブと結びついて共感性が増すと、少なくとも共感した支持者は拡散情報の事実性を重視しなくなると考えられる。

(2) 流れを加速する IT 基盤の進化

近年の IT 基盤の進化は、2016 年以降の虚偽情報の生成・拡散のコストを大幅に削減する機能を結果的に担っている。虚偽情報を拡散したい組織を支援するアンダーグラウンド組織は、この基盤を活用して生成・拡散エコシステムを形成している。技術面では、以下の要素が高度化・自動化したことが重要である。

- 情報窃取・悪意の拡散

サイバー攻撃による不正アクセス等で評価棄損対象と



■図 3-4-1　虚偽情報生成・拡散の流れ

する組織・個人の情報を窃取する。また大量のボットにより、虚偽情報拡散を自動化する。

- コンテンツ生成
  生成系 AI による「事実とは似て非なるコンテンツ」の生成は、政治家のフェイク動画拡散等で悪用が懸念されている。2020 年以降急速に普及している大規模言語モデル（LLM：Large Language Model）を用いた対話型 AI では、例えばナラティブと虚偽を交えたコンテンツが簡単に作れる、等のリスクが考えられるが、詳細はまだ明らかでない。
- 広告関連機能による拡散・増幅
  マイクロターゲティング技術の悪用は、個人を特定した虚偽情報生成・配信を容易にする。また、検索エンジン等で用いられるレコメンデーションアルゴリズムは、特定志向を持つグループに彼らが好む情報ばかりを提示し、虚偽情報の増幅（エコーチェンバー現象※284）を容易にする。この結果、情報の同質化が進む。

3.4.4 日本国内の状況

2023 年 4 月時点で、日本国内に世論を二分するような対立はなく、付随する虚偽情報の大規模拡散はないと見られる。しかし、災害や政治的事件に関する虚偽情報、特定集団や個人に対する差別・ヘイト情報等の拡散等が SNS 上で続いている。以下では、「生成・配信の方法が不適切」とみなされた事例も含め、国内の状況を説明する。

(1) 2016 年以降の虚偽情報拡散の傾向

米国大統領選挙の行われた 2016 年以降、国内でも虚偽情報拡散に対する関心は急速に高まった。2016 年には、特定ジャンルの情報を整理するキュレーションサイトにおける虚偽の医療情報配信が問題となった。配信時のファクトチェックがずさんであり、サイト運営者である株式会社ディー・エヌ・エーはメディア事業者として内容に責任を持つべき、とされた※285。同サイトは著作権の取り扱い等についても問題を起こしており、2016 年 12 月に閉鎖に追い込まれた※286。

総務省のプラットフォームサービスに関する研究会では、2020 年に拡散された虚偽情報の分析結果が報告されている※287。それによると、新型コロナウイルス対策のフェイクニュースについては、調査対象者の 58.9% が偽情報と気づいている。一方、国内政治関連のフェイクニュースについては、偽情報と気づいた人は 18.8% にとどまった。新型コロナウイルス関連の虚偽情報は一般にも知られていたために多くの人が疑ったと思われる。

(2) 政治的な虚偽情報拡散

2018 年 9 月、米軍基地をめぐる対立構造が明確な沖縄県知事選挙において、選挙関連サイトや SNS 上で立候補者や前知事を貶めるような情報が多数配信された。沖縄県の新聞社である沖縄タイムスは、候補者の「フェイクニュース」を報道したと認め、その経緯を検証している※288。更に、2022 年 9 月の沖縄県知事選挙に関しても組織的と思われる虚偽情報・ミスリードを誘発する情報の拡散が報じられた。報道機関のファクトチェックによると、虚偽情報には 4 年前の沖縄県知事選挙の動画転用、等が含まれていた。こうした沖縄県における虚偽情報拡散については、琉球帰属論※289 等に基づいて世論分断を図る中国の工作の影響が懸念されている※233。

2020年米国大統領選挙の不正選挙ナラティブについては、日本国内でもこれに共感し、不正選挙やTrump支持を訴える人々が一定の割合で出現した。米国のTrump支持派が組織的に日本で拡散したわけではなく、むしろアクセス増による広告収入増等の動機で拡散された情報が、ボトムアップ的に共感を得たものと見られる。また、こうした組織的でない拡散はコロナ禍やウクライナ侵攻に関する虚偽情報についても同様に観察された※290。ウクライナ侵攻時には、在日ロシア大使館のTwitterが虚偽情報拡散の中心となり、その後国内で共感者が拡散したと見られる※291。

(3) 個人を対象とする誹謗中傷・虚偽情報

国内の虚偽情報拡散で特徴的なのは、組織ではなく個人を対象とする誹謗中傷が報じられる点である。2020年4～5月、SNS上である人物への誹謗中傷投稿が集中、炎上し、被害者の自殺事件が発生した。ここではナラティブと呼ぶような共感を呼ぶ仕掛けがない代わりに、SNS利用者の「正義感」が多くの誹謗中傷を招いた、と分析された※287。こうした誤った「正義感」は、コロナ禍のような社会不安状況下では「自粛警察」のようなレッテル貼り、差別に結びついてしまうリスクがある※292。

3.4.5 虚偽情報の対応状況

虚偽情報の拡散抑制や影響の低減に向けた民間事業者、政府の対応について以下に整理する。

(1) ファクトチェックの強化

ファクトチェックは、配信される情報が事実に基づいているか、法規・倫理規定に違反しないものであるか等を調査し、結果を公表することとされ、虚偽情報対策の基本である。報道機関は自身の報道の検証手段として、また米国のPolitiFact.com※293等の第三者機関はSNS上の政治的言説のチェックを実施してきたが、2016年以降、SNS事業者自身も含め、対応が強化されている。例えばMeta Platforms, Inc.は、Facebook、Instagramの投稿(写真・動画・音声を含む)について、虚偽の引用、虚偽に基づく主張、陰謀論、不正サイト参照、虚偽または誤解を招く捏造・改変・一部削除、誤解を招く風刺等をチェックする、としている。このプロセスは、利用者フィードバックによるフェイクニュース(虚偽情報)特定、ファクトチェック、審議、コンテンツラベリング、利用者への周知、配信制限へと進む。ファクトチェックは、国際的なファクトチェックネットワーク(IFCN:The International Fact-Checking Network)※294が認定した80以上の第三者機関と提携し、60以上の言語について実施している※295。しかし、新型コロナウイルスワクチンに関する医療ジャーナル記事がFacebookで虚偽と誤判定され、正規のアクセスが制限された※296等、虚偽情報の急増に対応できていないという指摘もある。

Twitterは、新オーナーのMusk CEOが公共政策チームの解雇を続けており、民主主義・人権等の観点からのファクトチェック機能の弱体化が懸念されている※297。一方で、Musk CEOはクラウドベースツールCommunity Notesの試験導入を進めている。Community Notesは誤解を招くと思われるツイートに対して違う視点からのメモを追加できる機能で、効果的だとするファクトチェック専門家もいる※298。

急増する音声・動画のファクトチェックも課題である。YouTubeは近年ニュースソースとして一定の位置を占めているが、2022年1月、80以上のファクトチェック団体がYouTubeに対し、「コロナ禍や大統領選挙関連を含むデマと誤報の温床になっており、コンテンツ削除や常習犯対策等の改善を求める」と連名で主張、AIを用いた虚偽情報対策にも言及した※299。音声・動画のファクトチェックには、AIを用いた認識・言語化※300、虚偽動画等の自動検知※301が試みられている。AI利用による効率化への期待が大きい反面、精度向上等には時間が必要と思われる。この間、生成系AIの普及によりチェックが必要なコンテンツが爆発的に増えてしまうと、対応が非常に難しくなる可能性がある。

(2) 配信の統制強化

組織的拡散への対策の柱として、拡散の中心となる組織や個人の配信を制限する方法がある。顕著な例として、2020年米国大統領選挙におけるTrump大統領のTwitterアカウント停止は不正選挙キャンペーンの混乱を一気に収束させ、2022年のウクライナ侵攻におけるRT、SPUTNIK及び関連事業者に対する配信停止措置は、米欧におけるロシアの情報工作妨害に効果があったとされる※302。なお、ロシア政府も2022年3月4日にフェイクニュース法を成立させ、国内独立系報道機関、西側報道機関の活動を厳しく規制した※303。ただし、Telegramを介した西側報道へのアクセスは可能であり、徹底したものではない(「3.4.2(5)ウクライナ侵攻におけるサイバー情報戦」参照)。

配信停止措置は、「3.4.2(4)2020年米国大統領選挙

の不正選挙キャンペーン」で述べたように、個人の私権や表現の自由を制限する側面があるため、法律や規定に基づく、等の慎重な対応が必要である。個人のレベルでは、通常のSNS投稿が倫理規定に反したとしてアカウントを停止される、等でトラブルになるケースがある。

(3) アンダーグラウンド組織の諜報・攻撃対策

米国大統領選挙やウクライナ侵攻で見られたように、国家レベルの虚偽情報拡散では対象組織の情報収集、効率的な拡散インフラ構築等が組み合わされ、実施される。これを支援するアンダーグラウンド組織の活動監視・サイバー攻撃防御は虚偽情報拡散対策としても重要である。

(4) 政府の虚偽情報関連政策

米欧の西側諸国は、以前から旧ソ連・ロシアの情報宣伝戦に対峙し、2022年以降は親ロシア報道機関のコンテンツ配信停止等でも連携しているが、自国内から発信されたネット上の虚偽情報対策に関してはアプローチが異なる。米国ではプラットフォーム事業者の自主規制に任されてきたが、2016年以降、選挙への介入も含めた選挙セキュリティが政府の重要課題となった。テキサス、カリフォルニアの2州は選挙妨害目的のDeepfake動画利用を禁じた※304ものの、連邦政府レベルでは強い規制はまだなく、CISAが選挙セキュリティ対策として州政府への支援等を行っている。2022年3月、CISAは選挙虚偽情報対策の政府機関・関係事業者向けガイドラインを示した※305が、NISTの選挙関連の規格化は電子投票システム関係にとどまっている。外国政府が関与している選挙介入にはサイバー軍も出動する一方、国内発の情報の規制には連邦政府は慎重なスタンスであることがうかがわれる。

一方欧州は、政府の統制が前面に出ている。EUでは、欧州デジタル市場の安全な利用に関する統制の一環としてデジタルサービス法（DSA：Digital Services Act）※306を策定、プラットフォーム事業者（gatekeeper）に対して違法コンテンツ対応義務を明確化した（「2.2.3(3)(d) データ利用とガバナンスに関する規格策定」参照）。EUはまた、2024年に完全施行予定のAIの安全な利用に関する規則案（「2.2.3(3)(e) AI法の策定」参照）について、生成系AI利用システムに関する追加規定を審議し、2023年6月には生成系AIの生成物であることの表示や、学習等に用いたコンテンツの情報公開を義務化する規制を追加した修正案を採択した※307。

(5) 日本国内の対応

以下では、日本国内の官民による虚偽情報拡散防止の対応状況についてまとめる。

- プラットフォームサービスに関する検討会

  総務省の同検討会は2018年10月、プラットフォーム事業者の利用者情報の適切な管理を検討する場として設置されたが、2020年以降は誹謗中傷、Deepfake等の虚偽画像・フェイクニュースの拡散に対して取るべき施策も議論され、2023年度も継続中である※308。国内の違法・有害情報流通の実態調査※309等の報告もなされ、事業者の監視・統制と通信の秘密・表現の自由との兼ね合い等が議論されている。事業者が申告した取り組み事例によれば、普及啓発・注意喚起がメインであり、ファクトチェックは目立っていない※310。また、配信規制のような厳しい統制には言及されていない。

  なお総務省の情報通信審議会情報通信政策部会が2023年5月2日に公表した「『2030年頃を見据えた情報通信政策の在り方』部会報告書（原案）」には、偽情報・誤情報対策が明記された※311。

- Disinformation対策フォーラム

  同フォーラムは、プラットフォームサービスに関する研究会の検討結果を受け、一般社団法人セーファーインターネット協会が設置した会議体で、ファクトチェック機能強化・虚偽情報リテラシーの強化を二本柱とする対策を検討、2022年3月に報告書を公開した※312。なお、議論開始の時期がウクライナ侵攻前であったため、報告書には侵攻関連の知見は含まれない。

- ファクトチェック機関の活動

  2017年6月、有志による特定非営利活動法人ファクトチェック・イニシアティブ（FIJ：FactCheck Initiative Japan）※313が発足し、2017年の総選挙ファクトチェックプロジェクト、国内SNS事業者との連携、支援システムの開発、海外ファクトチェック機関との連携等を推進する等、国内のファクトチェック活動を先導している。また2022年10月、日本ファクトチェックセンター※314が発足、動画・音声を含むSNS等のファクトチェック結果を公開している。ただし、こうした活動は海外（韓国、台湾を含む）に比べ十分でなく、資金面、人材面に課題があるとされる※315。日本ファクトチェックセンターは学生を採用し、ファクトチェック人材育成をスコープとしているが、AI利用によるチェック効率化等、課題は多いと思われる。

- 消費者庁の活動

ネット上のインフルエンサーが報酬をもらい、虚実を交えて行うステルスマーケティングは、その情報が広告勧誘目的であると認識しない利用者を欺くものとして問題視されてきたが、国内では規制が遅れていた。2022年9月、消費者庁はステルスマーケティングに関する検討会を開催し※316、同検討会はこれを規制すべきとの提言を取りまとめた※317。これらを踏まえて消費者庁は2023年3月28日に景品表示法の不当表示を改訂、同年10月から実施することとした。違反した広告依頼事業者には公表措置が、悪質な場合は懲役または罰金が科されることとなる※318。

- 生成系AIへの対応

2023年4月25日、政府は生成系AIについて「規制は避け、産業界の応用に向けた環境整備を行う」方針を示した※319。民間からは、ビジネスや業務の在り方、開発の在り方を変えるゲームチェンジャーとしての期待とともに、虚偽情報の拡散、情報漏えい、プライバシー侵害、知財権侵害等のリスクについて懸念の声が上がっている。知財権侵害については、日本の著作権法が機械学習によるコンテンツ解析を無条件に認めている点が懸念事項とされている※320。大学等からは生成系AIの研究・教育への利用に関し意見が公開されている※321。総じて「強い規制はせず、課題を明らかにしつつ正しく利用する方法を見出すべき」という意見が多い。ただし、虚偽情報・AI利用に関するリテラシー教育プログラムは国内ではまだ整備されていない。また、米国Biden政権の「AI権利章典」のような、人権・プライバシーに配慮した開発原則は、2023年4月時点で政府は公表していない（AI権利章典については「2.2.3 (3) (e) AI法の策定」参照）。

2023年4月30日、高崎市にて開催されたG7技術・デジタル大臣会合の閣僚宣言に「責任あるAIとAIガバナンスの推進」が明記され、生成系AIについてG7あるいはOECD（Organisation for Economic Cooperation and Development）等で議論の場を持つことが合意された※322。政府の統制を強めたいEUと、民間の自主規制にとどめたい米・日とのすり合わせが注目される。

- 国家安全保障戦略

2022年12月16日に公表された国家安全保障戦略※323において、日本を取り巻く環境では偽情報の拡散等を通じた情報戦等が恒常的に生起しているとし、偽情報等の拡散を含め認知領域における情報戦への対応能力を強化するため、外国による偽情報等に関する情報の集約・分析、対外発信の強化、政府外の機関との連携の強化等のための新たな体制を政府内に整備するとされた（「2.1.1 (6) 安全保障関連3文書の改訂」参照）。

3.4.6 まとめと今後の見通し

ここまで、虚偽情報拡散の脅威の現状と対策をみてきた。本項ではこれをまとめ、虚偽情報拡散対策の今後の見通しについて検討する。

(1) 状況のまとめ

虚偽情報拡散は国家レベルの組織的・政治的なもの、陰謀論・差別・偏見等、社会に根強くあるナラティブの威を借りて虚偽のストーリーが作られるもの、災害・パンデミック・金融不安等の社会不安を契機とする突発的なもの、更にこれらの組み合わせや、これらによって経済的利益を得ようとするもの、等が確認できる。拡散を容易にしてしまうのが現在のITプラットフォームで、SNS・ターゲティング・レコメンデーション等による情報同質化（フィルターバブル）と増幅（エコーチェンバー現象）が懸念される。

ITサービス提供者の側では、過度のビジネス重視による不正コンテンツ放置が問題化し、ファクトチェック強化やEUによる規制強化が進んでいるが、生成系AI等による真偽不明なコンテンツの急増は新たな懸念となる。中心的な拡散力のある組織・個人の配信規制は沈静化に有効であるが、法的な裏付け等、慎重な運用が必要である。

ITサービス利用者の側では、真偽不明情報の拡散についての意識向上が求められる。アクセス数・広告収入増加等を目当てに虚偽と思われる情報を拡散した結果、一定の割合でそれを信じる人が現われたと報告されている※324。また国内においては、過剰な正義感あるいは使命感がナラティブとなって、他者の人権を否定、あるいは誹謗中傷する言説を拡散する傾向が見られる。こうした虚偽情報や拡散抑制に関するリテラシーについて、官民の教育プログラムは十分に整備されていない。

(2) 今後の見通し

虚偽情報の拡散は、社会の分断や対立を求める力が働く限り、今後も継続すると思われる。検討されている対応策を整理すると、以下のようになる。

- ファクトチェック機能強化
  急増するコンテンツのチェック自動化等の技術支援が必要と思われる。また、「この話題は虚偽情報が確認されている」というリスク情報の開示も、利用者への注意喚起のために重要と思われる。
- 配信元の規制
  犯罪目的・武力行使正当化・差別等の情報拡散については火急の対応が必要である。一方で、憲法で保障されている表現の自由と配信規制の折り合いについては継続的な議論が必要と思われる。
- 利用者のリテラシー向上
  教育プログラムの拡充が必要である。例えば、以下の情報を周知することは意味があると考えられる。
  - 虚偽情報拡散の流れと、増幅する仕組みの問題点
  - ファクトチェックの重要性
  - 特定の情報ソースに依存しないことの重要性
  - あるナラティブに共感するか、関連する真偽不明情報を興味本位で利用すると、誰でも拡散に加担する可能性があることのリスク
  - 各人が持っている価値観での「正義感」による拡散は要注意であり、かえって悪意を増長する可能性があることのリスク
- 生成系 AI の利用ルール策定
  現在は人権への配慮が注目されているが、虚偽情報を激増させない生成・利用ルールの早期の策定も望まれる。生成系 AI はそのメリットも大きいため、一律規制ではない対応が重要である。
- ナラティブに基づく拡散対応
  あるナラティブ（A は B のせいだ、等）に共感してしまうと関連情報の事実性が重視されなくなることが確認されており、ファクトチェックが機能しないリスクがある。拡散されたナラティブに対する有効な対応は難しく、中長期的な課題と考えられる。
- アンダーグラウンド組織への対応
  IT プラットフォームのサイバーセキュリティ確保が重要な対策であることは言うまでもないが、拡散を支援するアンダーグラウンド組織が AI 技術を悪用した場合、この対処は非常に難しくなると予想される[※325]。AI 技術の悪用を防止し、当該組織の活動をいかに抑止するかが重要課題となる。

※1　NISC が重要インフラの運営を担う事業者と、そこで行われるセキュリティ対策を支援する所管省庁が参照すべき指針として公表している「重要インフラの情報セキュリティ対策に係る行動計画」では、「重要インフラ」として 14 分野が定義されている。
NISC：重要インフラグループ　https://www.nisc.go.jp/policy/group/infra/index.html〔2023/5/19 確認〕
※2　トレンドマイクロ株式会社：Whitepaper: The State of Industrial Cybersecurity　https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html〔2023/5/19 確認〕
※3　Barracuda Networks, Inc.：The State of Industrial Security in 2022　https://assets.barracuda.com/assets/docs/dms/NetSec_Report_The_State_of_IIoT_final.pdf〔2023/5/19 確認〕
※4　「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※5　MENAFN：Thousands without internet after massive 'Cyber attack' in Europe　https://menafn.com/qn_news_story_s.aspx?storyid=1103810157&title=Thousands-without-internet-after-massive-Cyber-attack-in-Europe&source=30〔2023/5/19 確認〕
※6　Viasat, Inc.：KA-SAT Network cyber attack overview　https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/〔2023/5/19 確認〕
※7　REUTERS：Satellite outage knocks out thousands of Enercon's wind turbines　https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/〔2023/5/19 確認〕
※8　EASA：EASA publishes SIB to warn of intermittent GNSS outages near Ukraine conflict areas　https://www.easa.europa.eu/newsroom-and-events/news/easa-publishes-sib-warn-intermittent-gnss-outages-near-ukraine-conflict〔2023/5/19 確認〕
※9　FLYING：Pilots In Eastern Finland Warned Of GPS Interference Near Russian Border　https://www.flyingmag.com/pilots-in-eastern-finland-warned-of-gps-interference-near-russian-border/〔2023/5/19 確認〕
※10 CyberScoop：Iranian steel facilities suffer apparent cyberattacks　https://cyberscoop.com/iran-cyberattack-israel-hacktivist-steel-ics/〔2023/5/19 確認〕
Cyber Law Toolkit：Predatory Sparrow operation against Iranian steel maker (2022)　https://cyberlaw.ccdcoe.org/wiki/Predatory_Sparrow_operation_against_Iranian_steel_maker_(2022)〔2023/5/19 確認〕
※11 Bleeping Computer：Hackers attack UK water supplier but extort wrong company　https://www.bleepingcomputer.com/news/security/hackers-attack-uk-water-supplier-but-extort-wrong-company/〔2023/5/19 確認〕
SCADAfence：Understanding The South Staffordshire Water Cyber Attack　https://blog.scadafence.com/south-staffs-water-attack〔2023/5/19 確認〕
Forescout Technologies, Inc.：Analysis of Clop's Attack on South Staffordshire Water – UK　https://www.forescout.com/blog/analysis-of-clops-attack-on-south-staffordshire-water-uk/〔2023/5/19 確認〕
※12 Security Affairs：Pro-Palestinian group GhostSec hacked Berghof PLCs in Israel　https://securityaffairs.co/wordpress/135656/hacktivism/ghostsec-hacked-berghof-plcs-israel.html〔2023/5/19 確認〕
OTORIO Ltd.：Pro-Palestinian Hacking Group Compromises Berghof PLCs in Israel　https://www.otorio.com/blog/pro-palestinian-hacking-group-compromises-berghof-plcs-in-israel/〔2023/5/19 確認〕
※13 Security Affairs：US agricultural machinery manufacturer AGCO suffered a ransomware attack　https://securityaffairs.co/wordpress/131058/cyber-crime/agco-suffered-ransomware-attack.html〔2023/5/19 確認〕
※14 Bleeping Computer：SpiceJet airline passengers stranded after ransomware attack　https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/〔2023/5/19 確認〕
※15 Bleeping Computer：Foxconn confirms ransomware attack disrupted production in Mexico　https://www.bleepingcomputer.com/news/security/foxconn-confirms-ransomware-attack-disrupted-production-in-mexico/〔2023/5/19 確認〕
※16 Help Net Security：Automotive hose manufacturer hit by ransomware, shuts down production control system　https://www.helpnetsecurity.com/2022/06/23/nichirin-ransomware/〔2023/5/19 確認〕
株式会社ニチリン：当社米国子会社への不正アクセス発生について
https://www.nichirin.co.jp/news/20220622.pdf〔2023/5/19 確認〕
※17 Bleeping Computer：Ransomware attack halts circulation of some German newspapers　https://www.bleepingcomputer.com/news/security/ransomware-attack-halts-circulation-of-some-german-newspapers/〔2023/5/19 確認〕
※18 Cybernews：Cyberattack paralyzed Danish Railways for hours　https://cybernews.com/news/cyberattack-paralyzed-danish-railways/〔2023/5/19 確認〕
※19 The Record：Australian fire service operating 85 stations shuts down network after cyberattack　https://therecord.media/australian-fire-service-operating-85-stations-shuts-down-network-after-cyberattack/〔2023/5/19 確認〕
※20 Security Affairs：Canadian Copper Mountain Mining Corporation (CMMC) shut down the mill after a ransomware attack　https://securityaffairs.com/140282/cyber-crime/canadian-cmmc-ransomware-attack.html〔2023/5/19 確認〕
Industrial Cyber：Copper Mountain Mining resumes operational production, following ransomware attack　https://industrialcyber.co/critical-infrastructure/copper-mountain-mining-resumes-operational-production-following-ransomware-attack/〔2023/5/19 確認〕
※21 The Register：Finnish govt websites knocked down as Ukraine President addresses MPs　https://www.theregister.com/2022/04/09/dos_attacks_finland_russia/〔2023/5/19 確認〕
※22 BankInfoSecurity：Palermo Municipality Cyberattack Still Affecting Citizens　https://www.bankinfosecurity.com/palermo-municipality-cyberattack-still-affecting-citizens-a-19226〔2023/5/19 確認〕
IT Pro：Palermo ransomware attack: Vice Society claims responsibility as city details recovery strategy　https://www.itpro.co.uk/security/ransomware/368266/vice-society-ransomware-palermo-details-recovery-strategy〔2023/5/19 確認〕
※23 Bleeping Computer：Russian hacktivists take down Norway govt sites in DDoS attacks　https://www.bleepingcomputer.com/news/security/russian-hacktivists-take-down-norway-govt-sites-in-ddos-attacks/〔2023/5/19 確認〕
※24 GovInfoSecurity：Cyberattack Affects Albanian Government E-Services: Report　https://www.govinfosecurity.com/cyberattack-affects-albanian-government-e-services-report-a-19582〔2023/5/19 確認〕
※25 Security Affairs：Unprecedented cyber attack hit State Infrastructure of Montenegro　https://securityaffairs.co/wordpress/134900/cyber-warfare-2/montenegro-cyber-attack.html〔2023/5/19 確認〕
U.S. Embassy in Montenegro：Security Alert - Montenegro　https://me.usembassy.gov/security-alert-montenegro-august-26-2022/〔2023/5/19 確認〕
※26 Infosecurity Magazine：DDoS Attacks Pepper Taiwanese Government Sites　https://www.infosecurity-magazine.com/news/ddos-attacks-pepper-taiwanese/〔2023/5/19 確認〕
※27 Bleeping Computer：New ransomware hits Windows, Linux servers of Chile govt agency　https://www.bleepingcomputer.com/news/security/new-ransomware-hits-windows-linux-servers-of-chile-govt-agency/〔2023/5/19 確認〕
※28 SC Media：Government of Vanuatu offline since early November in suspected ransomware attack　https://www.scmagazine.com/news/ransomware/the-government-of-vanuatu-offline-since-early-november-in-suspected-ransomware-attack〔2023/5/19 確認〕
※29 The Record：Multiple government departments in New Zealand affected by ransomware attack on IT provider　https://therecord.media/multiple-government-departments-in-new-zealand-affected-by-ransomware-attack-on-it-provider/〔2023/5/19 確認〕
Te Whatu Ora：Cyber incident　https://www.tewhatuora.govt.nz/whats-happening/cyber-incident/〔2023/5/19 確認〕
※30 Bleeping Computer：Antwerp's city services down after hackers attack digital partner　https://www.bleepingcomputer.com/news/security/antwerps-city-services-down-after-hackers-attack-digital-partner/〔2023/5/19 確認〕
※31 The Record：French hospital complex suspends operations, transfers patients after ransomware attack　https://therecord.media/french-hospital-complex-suspends-operations-transfers-critical-patients-after-ransomware-attack/〔2023/5/19 確認〕

※ 32 HIT Consultant：Report: How Cyberattacks Hurts Patient Care and Mortality Rates https://hitconsultant.net/2022/09/13/cyberattacks-hurts-patient-care-and-mortality-rates/〔2023/5/19 確認〕
Proofpoint, Inc.：Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care https://www.proofpoint.com/us/cyber-insecurity-in-healthcare〔2023/5/19 確認〕
※ 33 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 第 5.2 版（令和 4 年 3 月）https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html〔2023/5/23 確認〕
※ 34 厚生労働省：医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起） https://www.mhlw.go.jp/content/10808000/001011666.pdf〔2023/5/19 確認〕
※ 35 https://www.honeywellforge.ai/us/en/campaigns/industrial-cybersecurity-threat-report-2022〔2023/5/19 確認〕
※ 36 https://www.nozominetworks.com/downloads/US/SANS-Survey-2022-OT-ICS-Cybersecurity-Nozomi-Networks.pdf〔2023/5/19 確認〕
※ 37 https://mysecuritymarketplace.com/mp-files/ot-iot-security-report-2022-2h-review.pdf〔2023/5/19 確認〕
※ 38 ICS-CERT の Web サイトで暦年（1/1 ～ 12/31）ごとに公開された ICSA Advisories の件数をカウントした。ただし、ICSMA（医療機器の脆弱性）は除く。カウントは公表日ベースとした（公表日が 2022 年なら、採番年度が 2021（ICSA-2021-xxx-x）でも 2022 年でカウント）。
CISA：Cybersecurity Alerts & Advisories https://www.cisa.gov/news-events/cybersecurity-advisories〔2023/5/19 確認〕
※ 39 SecurityWeek：Medical, IoT Devices From Many Manufacturers Affected by 'Access:7' Vulnerabilities https://www.securityweek.com/medical-iot-devices-many-manufacturers-affected-access7-vulnerabilities〔2023/5/19 確認〕
Forescout Technologies, Inc.：Access:7 https://www.forescout.com/research-labs/access7/〔2023/5/19 確認〕
PTC 社：Security vulnerabilities identified in the Axeda agent and Axeda Desktop Server https://www.ptc.com/en/support/article/CS363561〔2023/5/19 確認〕
CISA：PTC Axeda agent and Axeda Desktop Server (Update C) https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-01〔2023/5/19 確認〕
※ 40 The Register：CISA and friends raise alarm on critical flaws in industrial equipment, infrastructure https://www.theregister.com/2022/06/21/56_vulnerabilities_critical_industrial/〔2023/5/19 確認〕
Forescout Technologies, Inc.：OT:ICEFALL https://www.forescout.com/resources/ot-icefall-report/〔2023/5/19 確認〕
※ 41 Industrial Cyber：Evil PLC Attack weaponizes PLCs to exploit engineering workstations, breach OT and enterprise networks https://industrialcyber.co/vulnerabilities/evil-plc-attack-weaponizes-plcs-to-exploit-engineering-workstations-breach-ot-and-enterprise-networks/〔2023/5/19 確認〕
Claroty Ltd.：Evil PLC Attack: Using a Controller as Predator Rather than Prey https://claroty.com/team82/blog/evil-plc-attack-using-a-controller-as-predator-rather-than-prey/〔2023/5/19 確認〕
※ 42 Dragos 社：Dragos ICS/OT Cybersecurity Year in Review 2022 https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Report-2022.pdf?hsLang=en〔2023/5/19 確認〕
※ 43 IPA：制御システム関連のサイバーインシデント事例 2 ～ 2016 年 ウクライナ マルウェアによる停電 https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000076756.pdf〔2023/5/19 確認〕
※ 44 ESET, spol. s r.o.：ウクライナに大規模停電をもたらした「Industroyer」マルウェアの新バージョン「Industroyer2」確認 https://www.eset.com/jp/blog/welivesecurity/industroyer2-industroyer-reloaded/〔2023/5/19 確認〕
※ 45 CISA：APT Cyber Tools Targeting ICS/SCADA Devices https://www.cisa.gov/uscert/ncas/alerts/aa22-103a〔2023/5/19 確認〕
※ 46 Dragos 社：PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems https://hub.dragos.com/whitepaper/chernovite-pipedream〔2023/5/19 確認〕
Dragos 社：Analyzing PIPEDREAM: Results from Runtime Testing https://www.dragos.com/blog/analyzing-pipedream-results-from-runtime-testing/〔2023/5/19 確認〕
※ 47 Mandiant, Inc.：INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool〔2023/5/19 確認〕
※ 48 https://www.cisa.gov/circia〔2023/5/19 確認〕
※ 49 The White House：National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/〔2023/5/19 確認〕
※ 50 CISA：Cross-Sector Cybersecurity Performance Goals https://www.cisa.gov/cross-sector-cybersecurity-performance-goals〔2023/5/19 確認〕
※ 51 The White House：Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/〔2023/5/19 確認〕
※ 52 Axios：Exclusive: Biden admin launching new chemical sector cyber strategy https://www.axios.com/2022/10/26/biden-admin-chemical-sector-cyber-strategy〔2023/5/19 確認〕
The White House：FACT SHEET: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Chemical Sector https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/26/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-chemical-sector/〔2023/5/19 確認〕
※ 53 NIST：SP 1800-10 -Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector https://csrc.nist.gov/publications/detail/sp/1800-10/final〔2023/5/19 確認〕
※ 54 SecurityWeek：NIST Releases ICS Cybersecurity Guidance for Manufacturers https://www.securityweek.com/nist-releases-ics-cybersecurity-guidance-manufacturers〔2023/5/19 確認〕
※ 55 Industrial Cyber：NCCoE rolls out cybersecurity profile for hybrid satellite networks https://industrialcyber.co/critical-infrastructure/nccoe-rolls-out-cybersecurity-profile-for-hybrid-satellite-networks/〔2023/5/19 確認〕
NIST：Now Available! Final Annotated Outline: Cybersecurity Framework Profile for Hybrid Satellite Networks https://www.nccoe.nist.gov/news-insights/now-available-final-annotated-outline-cybersecurity-framework-profile-hybrid〔2023/5/19 確認〕
※ 56 DOE：National Cyber-Informed Engineering Strategy https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf〔2023/5/19 確認〕
※ 57 Industrial Cyber：New TSA security directive for railroad carriers focuses on performance-based measures https://industrialcyber.co/transport/new-tsa-security-directive-for-railroad-carriers-focuses-on-performance-based-measures/〔2023/5/19 確認〕
TSA：Security Directive 1580-21-01A - Enhancing Rail Cybersecurity https://www.tsa.gov/sites/default/files/sd-1580-21-01a.pdf〔2023/5/19 確認〕
※ 58 JD Supra：European Parliament Adopts "NIS2" Cybersecurity Directive https://www.jdsupra.com/legalnews/european-parliament-adopts-nis2-2527500/〔2023/5/19 確認〕
欧州議会：Cybersecurity: Parliament adopts new law to strengthen EU-wide resilience https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience〔2023/5/19 確認〕
※ 59 TechCrunch：UK mobile and broadband carriers face fines of $117K/day, or 10% of sales, if they fail to follow new cybersecurity rules https://techcrunch.com/2022/08/30/uk-mobile-and-broadband-carriers-face-fines-of-117k-day-or-10-of-sales-if-they-fail-to-follow-new-cybersecurity-rules/〔2023/5/19 確認〕
Legislation.gov.uk：Telecommunications (Security) Act 2021 https://www.legislation.gov.uk/ukpga/2021/31/enacted〔2023/5/19 確認〕
GOV.UK：Proposals for new telecoms security regulations and code of practice - government response to public consultation https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/outcome/proposals-for-new-telecoms-security-regulations-and-code-of-

practice-government-response-to-public-consultation〔2023/5/19確認〕
※60 Industrial Cyber：Australia passes SLACIP Act to build security, resilience of nation's critical infrastructure sector https://industrialcyber.co/threats-attacks/australia-passes-slacip-act-to-build-security-resilience-of-nations-critical-infrastructure-sector/〔2023/5/19確認〕
Department of Home Affairs：Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022〔2023/5/19確認〕
※61 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022.pdf〔2023/5/19確認〕
※62 https://www.nisc.go.jp/pdf/policy/infra/infra_rt4.pdf〔2023/5/19確認〕
※63 https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf〔2023/5/19確認〕
※64 経済産業省：工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html〔2023/5/19確認〕
※65 経済産業省：「インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク」を実施しました https://www.meti.go.jp/press/2022/10/20221031001/20221031001.html〔2023/5/19確認〕
※66 内閣府：経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）（令和4年法律第43号）https://www.cao.go.jp/keizai_anzen_hosho/index.html〔2023/5/19確認〕
経済産業省：経済安全保障推進法 https://www.meti.go.jp/policy/economy/economic_security/index.html〔2023/5/19確認〕
※67 IPA：制御システムのセキュリティリスク分析ガイド 第2版 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html〔2023/5/19確認〕
※68 IPA：「スマート工場のセキュリティリスク分析調査」調査報告書 https://www.ipa.go.jp/security/reports/vuln/controlsystem-smartplant.html〔2023/5/19確認〕
※69 IPA：「産業用制御システム向け侵入検知製品の実装技術の調査」調査報告書 https://www.ipa.go.jp/security/controlsystem/icsidsreport.html〔2023/5/19確認〕
※70 Qihoo 360 Technology Co., Ltd.：Some details of the DDoS attacks targeting Ukraine and Russia in recent days https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/〔2023/5/19確認〕
※71 NICT：NICTER観測統計 - 2022年4月～6月 https://blog.nicter.jp/2022/08/nicter_statistics_2022_2q/〔2023/5/19確認〕
※72 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔2023/5/19確認〕
※73 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp/〔2023/5/19確認〕
※74 OffSec Services Limited：Exploit Database https://www.exploit-db.com/〔2023/5/19確認〕
※75 QNAP社：Take Immediate Actions to Secure QNAP NAS https://www.qnap.com/en/security-news/2022/take-immediate-actions-to-secure-qnap-nas〔2023/5/19確認〕
※76 QNAP社：Take Immediate Actions to Stop Your NAS from Exposing to the Internet, and Update QTS to the latest available version. Fight Against Ransomware Together https://www.qnap.com/en/security-news/2022/take-immediate-actions-to-stop-your-nas-from-exposing-to-the-internet-and-update-qts-to-the-latest-available-version-fight-against-ransomware-together〔2023/5/19確認〕
※77 QNAP社：QNAP Extends Security Updates for EOL Products https://www.qnap.com/en/news/2022/qnap-extends-security-updates-for-eol-products〔2023/5/19確認〕
※78 CM4all GmbH：The Dirty Pipe Vulnerability https://dirtypipe.cm4all.com/〔2023/5/19確認〕
※79 QNAP社：Local Privilege Escalation Vulnerability in Linux (Dirty Pipe) https://www.qnap.com/ja-jp/security-advisory/qsa-22-05〔2023/5/19確認〕
※80 QNAP社：Infinite Loop Vulnerability in OpenSSL https://www.qnap.com/en-in/security-advisory/qsa-22-06〔2023/5/19確認〕
※81 QNAP社：Multiple Vulnerabilities in Apache HTTP Server https://www.qnap.com/en-in/security-advisory/qsa-22-11〔2023/5/19確認〕
※82 QNAP社：Multiple Vulnerabilities in Netatalk https://www.qnap.com/en-in/security-advisory/qsa-22-12〔2023/5/19確認〕
※83 QNAP社：DeadBolt Ransomware https://www.qnap.com/en-in/security-advisory/qsa-22-19〔2023/5/19確認〕
※84 Bleeping Computer：QNAP NAS devices targeted by surge of eCh0raix ransomware attacks https://www.bleepingcomputer.com/news/security/qnap-nas-devices-targeted-by-surge-of-ech0raix-ransomware-attacks/〔2023/5/19確認〕
※85 QNAP社：PHP Vulnerability https://www.qnap.com/en-in/security-advisory/qsa-22-20〔2023/5/19確認〕
※86 QNAP社：Checkmate Ransomware via SMB Services Exposed to the Internet https://www.qnap.com/en-in/security-advisory/qsa-22-21〔2023/5/19確認〕
※87 QNAP社：DeadBolt Ransomware https://www.qnap.com/en/security-advisory/qsa-22-24〔2023/5/19確認〕
※88 Group-IB Global Private Limited：DeadBolt ransomware: nothing but NASty https://www.group-ib.com/blog/deadbolt-ransomware-decryption〔2023/5/19確認〕
※89 The Hacker News：Warning - Deadbolt Ransomware Targeting ASUSTOR NAS Devices https://thehackernews.com/2022/02/warning-deadbolt-ransomware-targeting.html〔2023/5/19確認〕
※90 ASUSTOR社：ADM リリースノート ADM 4.0.6.REG2 (2023-02-20) https://www.asustor.com/service/release_notes#adm4〔2023/5/19確認〕
※91 Octagon Networks, Inc.：CVE-2022-24990: TerraMaster TOS unauthenticated remote command execution via PHP Object Instantiation https://octagon.net/blog/2022/03/07/cve-2022-24990-terrmaster-tos-unauthenticated-remote-command-execution-via-php-object-instantiation/〔2023/5/19確認〕
※92 TerraMaster社：TOS 4.2.30 is released for update! https://forum.terra-master.com/en/viewtopic.php?f=28&t=3030〔2023/5/19確認〕
※93 Western Digital社：My Cloud OS 5 Firmware 5.21.104 https://www.westerndigital.com/support/product-security/wdc-22006-my-cloud-os5-firmware-5-21-104〔2023/5/19確認〕
※94 Synology社：Synology-SA-22:06 Netatalk https://www.synology.com/en-us/security/advisory/Synology_SA_22_06〔2023/5/19確認〕
※95 株式会社バッファロー：【更新】NAS商品における AFP の脆弱性とその対処方法 https://www.buffalo.jp/news/detail/20230410-01.html〔2023/5/19確認〕
※96 Zyxel社：Zyxel security advisory for format string vulnerability in NAS https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-format-string-vulnerability-in-nas〔2023/5/19確認〕
※97 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022年1月観測レポート https://wizsafe.iij.ad.jp/2022/02/1348/〔2023/5/19確認〕
※98 Palo Alto Networks, Inc.：Mirai Variant MooBot Targeting D-Link Devices https://unit42.paloaltonetworks.com/moobot-d-link-devices/〔2023/5/19確認〕
パロアルトネットワークス株式会社：D-Linkの機器を狙うMirai亜種MooBot https://unit42.paloaltonetworks.jp/moobot-d-link-devices/〔2023/5/19確認〕
※99 C&Cサーバー：Command and Controlサーバーの略。ウイルス等により乗っ取ったコンピューター等に対し、遠隔から命令を送り制御するサーバー。
※100 Microsoft Corporation：Uncovering Trickbot's use of IoT devices in command-and-control infrastructure https://www.microsoft.com/en-us/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/〔2023/5/19確認〕
※101 Microsoft Corporation：microsoft / routeros-scanner https://github.com/microsoft/routeros-scanner〔2023/5/19確認〕
※102 Trend Micro Incorporated：Cyclops Blink Sets Sights on Asus Routers https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html〔2023/5/19確認〕
※103 ASUS社：ASUS Product Security Advisory https://www.asus.com/content/asus-product-security-advisory/〔2023/5/19確認〕
※104 Musarubra US LLC：Unauthenticated Remote Code Execution in a Wide Range of DrayTek Vigor Routers https://www.trellix.com/en-us/about/newsroom/stories/research/rce-in-dratyek-routers.html〔2023/5/19確認〕
Musarubra Japan株式会社：複数のDrayTek製Vigorルーターに認証なしのリモートコード実行が可能な脆弱性 https://blogs.trellix.jp/rce-

in-dratyek-routers〔2023/5/19 確認〕
※ 105 DrayTek 社：Security Advisory: DrayTek Router unauthenticated remote code execution vulnerability (CVE-2022-32548) https://www.draytek.co.uk/support/security-advisories/kb-advisory-aug2022-cve-2022-32548〔2023/5/19 確認〕
※ 106 ONEKEY GmbH：Security Advisory: NETGEAR Routers FunJSQ Vulnerabilities https://onekey.com/blog/security-advisory-netgear-routers-funjsq-vulnerabilities/〔2023/5/19 確認〕
※ 107 NETGEAR 社：Security Advisory for Vulnerabilities in FunJSQ on Some Routers and Orbi WiFi Systems, PSV-2022-0117 https://kb.netgear.com/000065132/Security-Advisory-for-Vulnerabilities-in-FunJSQ-on-Some-Routers-and-Orbi-WiFi-Systems-PSV-2022-0117〔2023/5/19 確認〕
※ 108 Tenable, Inc.：NETGEAR Nighthawk WiFi6 Router Network Misconfiguration https://www.tenable.com/security/research/tra-2022-36〔2023/5/19 確認〕
※ 109 NETGEAR 社：RAX30 Firmware Version 1.0.9.90 - Hot Fix https://kb.netgear.com/000065411/RAX30-Firmware-Version-1-0-9-90-Hot-Fix〔2023/5/19 確認〕
※ 110 Lumen Technologies, Inc.：ZuoRAT Hijacks SOHO Routers To Silently Stalk Networks https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/〔2023/5/19 確認〕
※ 111 QNAP 社：Vulnerability in QVR https://www.qnap.com/en/security-advisory/qsa-22-07〔2023/5/19 確認〕
※ 112 HackingIntoYourHeart / Unoriginal-Rice-Patty https://github.com/HackingIntoYourHeart/Unoriginal-Rice-Patty〔2023/5/19 確認〕
nonamecoder/CVE-2022-27254：https://github.com/nonamecoder/CVE-2022-27254〔2023/5/19 確認〕
※ 113 Rolling Pwn Attack https://rollingpwn.github.io/rolling-pwn/〔2023/5/19 確認〕
※ 114 トヨタ自動車：お客様のメールアドレス等の漏洩可能性に関するお詫びとお知らせについて https://global.toyota/jp/newsroom/corporate/38095972.html〔2023/5/19 確認〕
※ 115 BitSight Technologies, Inc.：BitSight Discovers Critical Vulnerabilities in Widely Used Vehicle GPS Tracker https://www.bitsight.com/blog/bitsight-discovers-critical-vulnerabilities-widely-used-vehicle-gps-tracker〔2023/5/19 確認〕
※ 116 CISA：MiCODUS MV720 GPS tracker (Update A) https://www.cisa.gov/news-events/ics-advisories/icsa-22-200-01〔2023/5/19 確認〕
※ 117 Palo Alto Networks, Inc.：Know Your Infusion Pump Vulnerabilities and Secure Your Healthcare Organization https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/〔2023/5/19 確認〕
パロアルトネットワークス株式会社：[2022-03-04 14:30 PST の内容を反映] 医療機関にセキュリティを：調査対象輸液ポンプの 75% に脆弱性かアラート https://unit42.paloaltonetworks.jp/infusion-pump-vulnerabilities/〔2023/5/19 確認〕
※ 118 Armis Security Ltd.：TLStorm 2.0 https://www.armis.com/research/tlstorm/〔2023/5/19 確認〕
※ 119 modzero AG：Meeting Owl – Security Disclosure Report https://www.modzero.com/static/meetingowl/Meeting_Owl_Pro_Security_Disclosure_Report_RELEASE.pdf〔2023/5/19 確認〕
※ 120 Owl Labs：Meeting Owl Pro Software Release Notes https://support.owllabs.com/s/knowledge/Meeting-Owl-Pro-Software-Release-Notes〔2023/5/19 確認〕
Owl Labs：Whiteboard Owl Software Release Notes https://support.owllabs.com/s/knowledge/Whiteboard-Owl-Software-Release-Notes〔2023/5/19 確認〕
※ 121 Nozomi Networks Inc.：Nozomi Networks Researchers Reveal Zero-Day RTLS Vulnerabilities at Black Hat 22 https://www.nozominetworks.com/blog/nozomi-networks-researchers-reveal-zero-day-rtls-vulnerabilities-at-black-hat-22/〔2023/5/19 確認〕
Nozomi Networks Inc.：UWB Real Time Locating Systems: How Secure Radio Communications May Fail in Practice https://www.nozominetworks.com/downloads/US/Nozomi-Networks-WP-UWB-Real-Time-Locating-Systems.pdf〔2023/5/19 確認〕
※ 122 NeroTeam Security Labs S.A.S.：[CVE-2022-36158 / CVE-2022-36159] Contec FLEXLAN FXA2000 and FXA3000 series vulnerability report. https://neroteam.com/blog/contec-flexlan-fxa2000-and-fxa3000-series-vulnerability-repo〔2023/5/19 確認〕
※ 123 コンテック社：FLEXLAN FX3000 および FX2000 シリーズの脆弱性と対策について https://www.contec.com/-/media/Contec/jp/support/security-info/contec_security_flexlan_ja_220901.pdf〔2023/5/19 確認〕
※ 124 Cisco 社：Cisco IP Phone 7800 and 8800 Series Cisco Discovery Protocol Stack Overflow Vulnerability https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U〔2023/5/19 確認〕
※ 125 Matt's internet home：Turning Google smart speakers into wiretaps for $100k https://downrightnifty.me/blog/2022/12/26/hacking-google-home.html〔2023/5/19 確認〕
※ 126 Qihoo 360 Technology Co., Ltd.：What Our Honeypot Sees Just One Day After The Spring4Shell Advisory https://blog.netlab.360.com/what-our-honeypot-sees-just-one-day-after-the-spring4shell-advisory-en/〔2023/5/19 確認〕
※ 127 Fortinet, Inc.：So RapperBot, What Ya Bruting For? https://www.fortinet.com/blog/threat-research/rapperbot-malware-discovery〔2023/5/19 確認〕
フォーティネットジャパン合同会社：RapperBot の脅威とは https://www.fortinet.com/jp/blog/threat-research/rapperbot-malware-discovery〔2023/5/19 確認〕
※ 128 Securonix, Inc.：Detecting EnemyBot – Securonix Initial Coverage Advisory https://www.securonix.com/blog/detecting-the-enemybot-botnet-advisory/〔2023/5/19 確認〕
※ 129 Fortinet, Inc.：Enemybot: A Look into Keksec's Latest DDoS Botnet https://www.fortinet.com/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet〔2023/5/19 確認〕
フォーティネットジャパン合同会社：Enemybot：Keksec による最新の DDoS ボットネットの外観 https://www.fortinet.com/jp/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet〔2023/5/19 確認〕
※ 130 AT&T Inc.：Rapidly evolving IoT malware EnemyBot now targeting Content Management System servers and Android devices https://cybersecurity.att.com/blogs/labs-research/rapidly-evolving-iot-malware-enemybot-now-targeting-content-management-system-servers〔2023/5/19 確認〕
※ 131 RCE：Remote Code Execution の略。リモートコード実行の脆弱性を表す。
※ 132 Apache Log4j の脆弱性の詳細に関しては、「情報セキュリティ白書 2022」の「3.1.2（1）（a）Log4Shell」（p.168）を参照。
※ 133 Qihoo 360 Technology Co., Ltd.：New Threat: B1txor20, A Linux Backdoor Using DNS Tunnel https://blog.netlab.360.com/b1txor20-use-of-dns-tunneling_en/〔2023/5/19 確認〕
※ 134 Qihoo 360 Technology Co., Ltd.：Fodcha, a new DDos botnet https://blog.netlab.360.com/fodcha-a-new-ddos-botnet/〔2023/5/19 確認〕
※ 135 「情報セキュリティ白書 2021」の「3.2.1（4）LILIN 社製 DVR のゼロデイ脆弱性を狙う攻撃」（p.199）を参照。
※ 136 Qihoo 360 Technology Co., Ltd.：Fodcha Is Coming Back, Raising A Wave of Ransom DDoS https://blog.netlab.360.com/fodcha-is-coming-back-with-rddos/〔2023/5/19 確認〕
※ 137 AT&T Inc.：Shikitega - New stealthy malware targeting Linux https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux〔2023/5/19 確認〕
※ 138 Mandiant, Inc.：Shikata Ga Nai Encoder Still Going Strong https://www.mandiant.com/resources/blog/shikata-ga-nai-encoder-still-going-strong〔2023/5/19 確認〕
※ 139 Lumen Technologies, Inc.：Chaos Is A Go-Based Swiss Army Knife Of Malware https://blog.lumen.com/chaos-is-a-go-based-swiss-army-knife-of-malware/〔2023/5/19 確認〕
※ 140 Rapid7 Inc.：CVE-2022-30525 (FIXED): Zyxel Firewall Unauthenticated Remote Command Injection https://www.rapid7.com/blog/post/2022/05/12/cve-2022-30525-fixed-zyxel-firewall-unauthenticated-remote-command-injection/〔2023/5/19 確認〕
※ 141 SentinelOne, Inc.：CVE-2021-45608 ¦ NetUSB RCE Flaw in Millions of End User Routers https://www.sentinelone.com/labs/cve-2021-45608-netusb-rce-flaw-in-millions-of-end-user-routers/〔2023/5/19 確認〕
※ 142 Forescout Technologies, Inc.：New Supply Chain Vulnerabilities Impact Medical and IoT Devices https://www.forescout.com/blog/access-7-vulnerabilities-impact-supply-chain-component-in-medical-and-iot-device-models/〔2023/5/19 確認〕
Forescout Technologies, Inc.：Access:7 - How Supply Chain Vulnerabilities Can Allow Unwelcomed Access to Your Medical and IoT Devices https://www.forescout.com/resources/access-

7-supply-chain-vulnerabilities-can-allow-unwelcomed-access-to-your-medical-and-iot-devices/〔2023/5/19 確認〕
※ 143 CISA:PTC Axeda agent and Axeda Desktop Server (Update C) https://www.cisa.gov/news-events/ics-advisories/icsa-22-067-01〔2023/5/19 確認〕
※ 144 PTC 社：Axeda Public Advisory https://www.ptc.com/en/documents/security/coordinated-vulnerability-disclosure/axeda-public-advisory〔2023/5/19 確認〕
PTC 社：CS363561- Security vulnerabilities identified in the Axeda agent and Axeda Desktop Server https://www.ptc.com/en/support/article/CS363561〔2023/5/19 確認〕
※ 145 Armis Security Ltd.：TLStorm 2 - NanoSSL TLS library misuse leads to vulnerabilities in common switches https://www.armis.com/blog/tlstorm-2-nanossl-tls-library-misuse-leads-to-vulnerabilities-in-common-switches〔2023/5/19 確認〕
Armis Security Ltd.：TLStorm 2.0 - A set of critical vulnerabilities for Aruba and Avaya switches that can break network segmentation https://www.armis.com/wp-content/uploads/2022/05/TLStorm2-WP.pdf〔2023/5/19 確認〕
※ 146 Erik Andersen：uClibc https://www.uclibc.org/〔2023/5/19 確認〕
※ 147 uClibc-ng - Embedded C library:https://www.uclibc-ng.org/〔2023/5/19 確認〕
※ 148 Nozomi Networks Inc.：Nozomi Networks Discovers Unpatched DNS Bug in Popular C Standard Library Putting IoT at Risk https://www.nozominetworks.com/blog/nozomi-networks-discovers-unpatched-dns-bug-in-popular-c-standard-library-putting-iot-at-risk/〔2023/5/19 確認〕
※ 149 Check Point Software Technologies Ltd.：VULNERABILITY WITHIN THE UNISOC BASEBAND OPENS MOBILE PHONES COMMUNICATIONS TO REMOTE HACKER ATTACKS https://research.checkpoint.com/2022/vulnerability-within-the-unisoc-baseband/〔2023/5/19 確認〕
※ 150 Realtek 社：Vulnerability Report - Realtek AP-Router SDK Advisory (CVE-2022-27255) https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2022-27255.pdf〔2023/5/19 確認〕
※ 151 PoC（Proof of Concept）：発見された脆弱性を実証するために公開されたプログラムコード。
※ 152 Faraday Security：New research findings from Faraday goes to DEF CON https://faradaysec.com/blog-new-research-from-faraday-goes-to-def-con/〔2023/5/19 確認〕
DEF CON ON YOUTUBE：DEF CON 30 - Octavio Gianatiempo, Octavio Galland - Hidden Attack Surface of OEM IoT devices https://www.youtube.com/watch?v=veicfLvqc0s〔2023/5/19 確認〕
※ 153 任天堂株式会社：「ニンテンドー Wi-Fi USB コネクタ」および「ニンテンドー Wi-Fi ネットワークアダプタ」使用中止のお願い https://www.nintendo.co.jp/support/information/2022/0720.html〔2023/5/19 確認〕
※ 154 Cisco 社：Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers IPSec VPN Server Authentication Bypass Vulnerability https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-vpnbypass-Cpheup90〔2023/5/19 確認〕
※ 155 Cisco 社：End-of-Sale and End-of-Life Announcement for the Cisco Small Business RV Series Routers (selected models) https://www.cisco.com/c/en/us/products/collateral/routers/small-business-rv-series-routers/eos-eol-notice-c51-742771.pdf〔2023/5/19 確認〕
※ 156 Bleeping Computer：Cisco won't fix authentication bypass zero-day in EoL routers https://www.bleepingcomputer.com/news/security/cisco-won-t-fix-authentication-bypass-zero-day-in-eol-routers/〔2023/5/19 確認〕
※ 157 Microsoft Corporation：Vulnerable SDK components lead to supply chain risks in IoT and OT environments https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/〔2023/5/19 確認〕
※ 158 https://notice.go.jp/〔2023/5/19 確認〕
※ 159 https://notice.go.jp/status〔2023/5/19 確認〕
※ 160 NICTER 解析チーム：https://twitter.com/nicter_jp/status/1519583257670479872〔2023/5/19 確認〕
※ 161 NICTER 解析チーム：https://twitter.com/nicter_jp/status/1524640416938659840〔2023/5/19 確認〕
※ 162 NICTER 解析チーム：https://twitter.com/nicter_jp/status/1534722508729229312〔2023/5/19 確認〕
※ 163 ユニモテクノロジー株式会社：UDR-JA1004/JA1008/JA1016 ファームウエアを更新しました http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1643590226-637355〔2023/5/19 確認〕
※ 164 株式会社インターネットイニシアティブ：wizSafe Security Signal https://wizsafe.iij.ad.jp/〔2023/5/19 確認〕
※ 165 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022年2月 観測レポート https://wizsafe.iij.ad.jp/2022/03/1370/〔2023/5/19 確認〕
※ 166 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022年3月 観測レポート https://wizsafe.iij.ad.jp/2022/04/1380/〔2023/5/19 確認〕
※ 167 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022年4月 観測レポート https://wizsafe.iij.ad.jp/2022/05/1393/〔2023/5/19 確認〕
※ 168 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022年5月 観測レポート https://wizsafe.iij.ad.jp/2022/06/1407/〔2023/5/19 確認〕
※ 169 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022年7月 観測レポート https://wizsafe.iij.ad.jp/2022/08/1443/〔2023/5/19 確認〕
※ 170 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022年8月 観測レポート https://wizsafe.iij.ad.jp/2022/09/1455/〔2023/5/19 確認〕
※ 171 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022 年 10 月 観測レポート https://wizsafe.iij.ad.jp/2022/11/1479/〔2023/5/19 確認〕
※ 172 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022 年 11 月 観測レポート https://wizsafe.iij.ad.jp/2022/12/1489/〔2023/5/19 確認〕
※ 173 株式会社インターネットイニシアティブ：wizSafe Security Signal 2022 年 12 月 観測レポート https://wizsafe.iij.ad.jp/2023/01/1499/〔2023/5/19 確認〕
※ 174 IoT 機器に感染するウイルスの分類については、「情報セキュリティ白書 2020」の「表 3-2-1 IoT 機器に感染するウイルスの分類」（p.166）を参照。
※ 175 Imperva, Inc.：Record 25.3 Billion Request Multiplexing DDoS Attack Mitigated by Imperva https://www.imperva.com/blog/record-25-3-billion-request-multiplexing-attack-mitigated-by-imperva/〔2023/5/19 確認〕
※ 176 Cloudflare, Inc.：Cloudflare DDoS threat report 2022 Q3 https://blog.cloudflare.com/cloudflare-ddos-threat-report-2022-q3/〔2023/5/19 確認〕
Cloudflare, Inc.：Cloudflare DDoS 脅威レポート 2022 年第 3 四半期 https://blog.cloudflare.com/ja-jp/cloudflare-ddos-threat-report-2022-q3-ja-jp/〔2023/5/19 確認〕
※ 177 Microsoft Corporation：MCCrash: Cross-platform DDoS botnet targets private Minecraft servers https://www.microsoft.com/en-us/security/blog/2022/12/15/mccrash-cross-platform-ddos-botnet-targets-private-minecraft-servers/〔2023/5/19 確認〕
※ 178 クレデンシャル・スタッフィング攻撃：侵害された、または漏えいしたユーザー認証情報を悪用して、他のサービスへの大規模な不正ログインを試みる攻撃手法。
※ 179 FBI：Proxies and Configurations Used for Credential Stuffing Attacks on Online Customer Accounts https://www.ic3.gov/Media/News/2022/220818.pdf〔2023/5/19 確認〕
※ 180 DomainTools, LLC：Purpose Built Criminal Proxy Services and the Malicious Activity They Enable https://www.domaintools.com/resources/blog/purpose-built-criminal-proxy-services-and-the-malicious-activity-they-enable/〔2023/5/19 確認〕
※ 181 DARKReading（Informa PLC Informa UK Limited）：How APTs Are Achieving Persistence Through IoT, OT, and Network Devices https://www.darkreading.com/attacks-breaches/how-apts-are-achieving-persistence-through-iot-ot-and-network-devices〔2023/5/19 確認〕
※ 182 Forescout Technologies, Inc.：R4IoT: When Ransomware Meets the Internet of Things https://www.forescout.com/blog/r4iot-when-ransomware-meets-the-internet-of-things/〔2023/5/19 確認〕
Forescout Technologies, Inc.：R4IoT: When Ransomware Meets IoT and OT https://www.forescout.com/research-labs/r4iot/〔2023/5/19 確認〕
※ 183 CISA：People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices https://www.cisa.gov/uscert/ncas/current-activity/2022/06/07/peoples-republic-

china-state-sponsored-cyber-actors-exploit〔2023/5/19 確認〕
CISA：People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices https://www.cisa.gov/uscert/ncas/alerts/aa22-158a〔2023/5/19 確認〕
※ 184 Qihoo 360 Technology Co., Ltd.：P2P Botnets: Review - Status - Continuous Monitoring https://blog.netlab.360.com/p2p-botnets-review-status-continuous-monitoring/〔2023/5/19 確認〕
※ 185 Hajimeの詳細に関しては、「情報セキュリティ白書2018」の「3.1.1（1）IoT 機器の Mirai 等の感染に対抗する『Hajime』」（p.162）、「情報セキュリティ白書 2020」の「3.2.1（2）機器保護型ウイルスの動向」（p.176）を参照。
※ 186 Moji の詳細に関しては、「情報セキュリティ白書 2020」の「3.2.1（1）（n）Mozi」（p.175）、「情報セキュリティ白書 2022」の「3.2.1（3）（b）Gafgyt の亜種『Mozi』」（p.175）を参照。
※ 187 Qihoo 360 Technology Co., Ltd.：Pink, a botnet that competed with the vendor to control the massive infected devices https://blog.netlab.360.com/pink-en/〔2023/5/19 確認〕
※ 188 BSI：IT-Sicherheitskennzeichen jetzt auch für smarte Verbraucherprodukte (archiviert) https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220504_IT-SiK-Erweiterung.html〔2023/5/19 確認〕
※ 189 BSI：BSI and Singapore Cyber Security Agency Mutually Recognise Cyber Security Labels https://www.bsi.bund.de/EN/Service-Navi/Presse/Pressemitteilungen/Presse2022/221020_IT-SiK-Singapur.html〔2023/5/19 確認〕
※ 190 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf〔2023/5/19 確認〕
※ 191 経済産業省：第 1 回 産業サイバーセキュリティ研究会 ワーキンググループ 3 IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/001.html〔2023/5/19 確認〕
※ 192 United States Attorney's Office：Russian Botnet Disrupted in International Cyber Operation https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation〔2023/5/19 確認〕
※ 193 IPA：「IoT 開発におけるセキュリティ設計の手引き」を公開 https://www.ipa.go.jp/security/iot/iotguide.html〔2023/5/19 確認〕
※ 194 IPA：欧州規格 ETSI EN 303 645 V2.1.1 (2020-06) の翻訳 https://www.ipa.go.jp/security/controlsystem/etsien303645.html〔2023/5/19 確認〕
※ 195 https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2022/06/Guide-to-the-CSA-IoT-Controls-Matrix-v3_J.pdf〔2023/5/19 確認〕
※ 196 https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2022/06/CSA-IoT-Controls-Matrix-v3_J.xlsx〔2023/5/19 確認〕
※ 197 一般社団法人セキュア IoT プラットフォーム協議会：「IoT セキュリティ手引書 Ver2.0」をリリース ～IoTビジネスに関わる事業者向けにセキュリティの課題と対応策のガイドラインを提示～ https://www.secureiotplatform.org/release/2022-01-31〔2023/5/19 確認〕
※ 198 https://csrc.nist.gov/publications/detail/nistir/8349/draft〔2023/5/19 確認〕
※ 199 https://csrc.nist.gov/publications/detail/nistir/8425/final〔2023/5/19 確認〕
※ 200 https://csrc.nist.gov/publications/detail/nistir/8431/final〔2023/5/19 確認〕
※ 201 https://csrc.nist.gov/publications/detail/sp/1800-36/draft〔2023/5/19 確認〕
※ 202 https://www.dsci.in/content/iot-security-guidebook〔2023/5/19 確認〕
※ 203 https://www.dsci.in/content/iot-security-best-practices-document〔2023/5/19 確認〕
※ 204 https://juas.or.jp/cms/media/2022/04/JUAS_IT2022.pdf〔2023/5/25 確認〕
※ 205 フォーティネットジャパン合同会社：2022 年クラウドセキュリティ レポート https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/ja_jp/report-2022-cloud-security.pdf〔2023/5/25 確認〕
※ 206 https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR202100_002.pdf〔2023/5/25 確認〕
※ 207 総務省：令和 4 年版 情報通信白書 データ集（第 3 章第 6 節） https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nf306000.html〔2023/5/25 確認〕
※ 208-1 IDC Japan 株式会社：国内パブリッククラウドサービス市場予測を発表 https://www.idc.com/getdoc.jsp?containerId=prJPJ48986422〔2023/5/25 確認〕
※ 208-2 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/01honpen.pdf〔2023/5/25 確認〕
※ 209 Sophos Ltd.：SMB におけるクラウドセキュリティの現状 2022 年版 https://news.sophos.com/ja-jp/2022/11/29/the-reality-of-smb-cloud-security-in-2022-jp/〔2023/5/25 確認〕
※ 210 https://resources.trendmicro.com/rs/945-CXD-062/images/m506-2022 年上半期サイバーセキュリティレポート .pdf〔2023/5/25 確認〕
※ 211 株式会社エイチーム：採用活動における個人情報漏えいの可能性に関するご報告とお詫び https://www.a-tm.co.jp/news/29297/〔2023/5/25 確認〕
※ 212 一般社団法人シェアリングエコノミー協会：個人情報漏えいの可能性に関するお知らせとお詫び（※ 7 月 28 日追記） https://sharing-economy.jp/ja/20220720〔2023/5/25 確認〕
※ 213 ライフイズテック株式会社：お客様情報の一部が閲覧可能な状態にあったことへのお知らせとお詫び https://life-is-tech.com/news/wp-content/uploads/2022/06/453a575d0d32d7f2e6d0b3273ca54140.pdf〔2023/5/25 確認〕
※ 214 ケアプロ株式会社：個人情報閲覧の可能性に関するお詫びとご報告 https://carepro.co.jp/about/yobou_news_20200604.pdf〔2023/5/25 確認〕
※ 215 https://www.soumu.go.jp/main_content/000771515.pdf〔2023/5/25 確認〕
※ 216 https://www.ipa.go.jp/publish/wp-security/sec-2022.html〔2023/5/25 確認〕
※ 217 NHK NEWS WEB：マイクロソフト「チームズ（Teams）」障害 アクセスできないなど https://www3.nhk.or.jp/news/html/20220721/k10013729031000.html〔2023/5/25 確認〕
NHK NEWS WEB：マイクロソフト チームズ（Teams）「サービス大部分が復旧」 発表 https://www3.nhk.or.jp/news/html/20220721/k10013729211000.html〔2023/5/25 確認〕
※ 218 個人情報保護委員会：法令・ガイドライン等 https://www.ppc.go.jp/personalinfo/legal/〔2023/5/25 確認〕
※ 219 総務省：参考資料 https://www.soumu.go.jp/main_content/000067990.pdf〔2023/5/25 確認〕
※ 220 総務省：「クラウドサービスの安全・信頼性に係る情報開示指針」における「AI を用いたクラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS 編）」の追加 https://www.soumu.go.jp/menu_news/s-news/01ryutsu06_02000306.html〔2023/5/25 確認〕
※ 221 https://www.ipa.go.jp/security/reports/economics/scrm/cloud2022.html〔2023/5/25 確認〕
※ 222 IPA：中小企業の情報セキュリティ対策ガイドライン https://www.ipa.go.jp/security/guide/sme/about.html〔2023/5/25 確認〕
※ 223 https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf〔2023/5/25 確認〕
※ 224 一般財団法人日本情報経済社会推進協会：クラウドサービスに関連する国内外の制度・ガイドラインの紹介 https://www.jipdec.or.jp/library/sqau0900000055at-att/JIP-ISMS201-1.1.pdf〔2023/5/25 確認〕
※ 225 https://www.ismap.go.jp/csm/sys_attachment.do?sys_id=383d21a4dbf965106e6cb915f396192d〔2023/5/25 確認〕
※ 226 総務省：「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）に対する意見募集の結果と「クラウドサービス利用・提供における適切な設定のためのガイドライン」及び「ASP・SaaS の安全・信頼性に係る情報開示指針（ASP・SaaS 編）第 3 版」の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00149.html〔2023/5/25 確認〕
※ 227 経済産業省：「ISMAP ー LIU」の運用を開始しました https://www.meti.go.jp/press/2022/11/20221101002/20221101002.html〔2023/5/25 確認〕
※ 228 ASPIC：日本クラウド産業協会への名称変更のお知らせ https://www.aspicjapan.org/pdf/20220401.pdf〔2023/5/25 確認〕
※ 229 ASPIC：情報開示認定300サービス突破記念表彰及び表彰式ライブ配信のお知らせ https://www.aspicjapan.org/nintei/pdf/news/221110.pdf〔2023/5/25 確認〕
※ 230 ASPIC：クラウドサービスの安全・信頼性に係る情報開示認定制度とは https://www.aspicjapan.org/nintei/〔2023/5/25 確認〕
※ 231 一般社団法人日本クラウドセキュリティアライアンス（CSA ジャパン）：STAR https://www.cloudsecurityalliance.jp/site/?page_id=429〔2023/5/25 確認〕
※ 232 一般社団法人日本クラウドセキュリティアライアンス（CSA ジャパン）：グローバルプロバイダが日本語 CAIQ 評価レポートを登録する方法 https://cloudsecurityalliance.jp/newblog/author/mmorozum/

〔2023/5/25 確認〕
※ 233 長迫智子：今日の世界における「ディスインフォメーション」の動向――“Fake News”から”Disinformation”へ https://www.spf.org/iina/articles/nagasako_01.html〔2023/5/23 確認〕
※ 234 総務省：フェイクニュースを巡る動向 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd114400.html〔2023/5/23 確認〕
※ 235 Dictionary.com：“Misinformation” vs. “Disinformation”：Get Informed On The Difference https://www.dictionary.com/e/misinformation-vs-disinformation-get-informed-on-the-difference/〔2023/5/23 確認〕
※ 236 Malinformation は情報の虚偽性に加えて、有害性や倫理・法制の議論が必要となるが、本項では除外する。
※ 237 BBC News：Fake Obama created using AI video tool https://www.youtube.com/watch?v=AmUC4m6w1wo〔2023/5/23 確認〕
Supasorn Suwajanakorn, Steven M. Seitz, and Ilra Kemelmacher-Shlizerman：Synthesizing Obama: Learning Lip Sync from Audio https://grail.cs.washington.edu/projects/AudioToObama/〔2023/6/19 確認〕
※ 238 ニューズウィーク日本版:偽ニュース、小児性愛、ヒラリー、銃撃 ... ピザゲートとは何か https://www.newsweekjapan.jp/stories/world/2016/12/post-6501.php〔2023/5/23 確認〕
※ 239 Britannica：QANON https://www.britannica.com/topic/QAnon〔2023/5/23 確認〕
REUTERS：What is QAnon and how are social media sites taking action on it? https://jp.reuters.com/article/us-socialmedia-qanon-factbox/what-is-qanon-and-how-are-social-media-sites-taking-action-on-it-idUKKBN26203M〔2023/5/23 確認〕
※ 240 NII Today：「SNS によるデマ拡散」問題の本質とは https://www.nii.ac.jp/today/89/4.html〔2023/5/23 確認〕
※ 241 USA Today：Ukrainian President Volodymyr Zelenskyy shares a message from Kyiv https://www.youtube.com/watch?v=tLv9IqcoNe8〔2023/5/23 確認〕
※ 242 SYNODOS：ウクライナ戦争と「ナラティブ優勢」をめぐる戦い https://synodos.jp/opinion/international/28156/〔2023/5/23 確認〕
※ 243 Office of the Director of National Intelligence：Background to “Assessing Russian Activities and Intentions in Recent US Elections”：The Analytic Process and Cyber Incident Attribution https://www.dni.gov/files/documents/ICA_2017_01.pdf〔2023/5/23 確認〕
※ 244 HUFFPOST：ロシアの「フェイクニュース工場」は米大統領選にどう介入したのか https://www.huffingtonpost.jp/entry/russia-fakenews_jp_5c5b77b4e4b0faa1cb67da06〔2023/5/23 確認〕
※ 245 ボット：「ロボット（Robot）」を省略した「ボット（Bot）」から転じた、作業を自動化するプログラムの総称。ここでは、SNS に自動的に投稿するプログラムを指す。
※ 246 笹原和俊、デジタル影響工作に対する計算社会科学のアプローチ、一田和樹他、ネット世論操作とデジタル影響工作、原書房、2023 年 3 月 20 日
※ 247 The Guardian：‘I made Steve Bannon’s psychological warfare tool’：meet the data war whistleblower https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump〔2023/5/23 確認〕
日本経済新聞社：フェイスブック、情報流用 8700 万人規模に拡大 https://www.nikkei.com/article/DGXMZO29021990V00C18A4000000/〔2023/6/19 確認〕
※ 248 東洋経済：ネットの検索結果が「投票」に及ぼす恐ろしい影響 https://toyokeizai.net/articles/-/447766〔2023/5/23 確認〕
※ 249 REUTERS：U.S. disrupted Russian trolls on day of November election: report https://jp.reuters.com/article/us-usa-trump-russia/u-s-disrupted-russian-trolls-on-day-of-november-election-report-idUSKCN1QF26Q〔2023/5/23 確認〕
※ 250 日本経済新聞：ロシア、SNS 工作拡大か 欧州社会分断あおる https://www.nikkei.com/article/DGXMZO23567000W7A111C1FF2000/〔2023/5/23 確認〕
※ 251 The Guardian：Russia report reveals UK government failed to investigate Kremlin interference https://www.theguardian.com/world/2020/jul/21/russia-report-reveals-uk-government-failed-to-address-kremlin-interference-scottish-referendum-brexit〔2023/5/23 確認〕
※ 252 FIRST DRAFT：Brexit: The false, misleading and suspicious claims CrossCheck has uncovered so far https://firstdraftnews.org/articles/brexit-the-false-misleading-and-suspicious-claims-crosscheck-has-uncovered/〔2023/5/23 確認〕
※ 253 公益財団法人 NIRA 総合研究開発機構：ポスト・トゥルースの時代とは https://www.nira.or.jp/paper/my-vision/2017/post-30.html〔2023/5/23 確認〕
※ 254 水谷瑛嗣郎、ポスト・トゥルース 陰謀論の時代における「リアル」な政治を求めて、駒村圭吾編：Liberty2.0 自由論のバージョンアップはありうるのか?、弘文堂、2023 年 2 月 28 日
※ 255 The Wall Street Journal：Lab Leak Most Likely Origin of Covid-19 Pandemic, Energy Department Now Says https://www.wsj.com/articles/covid-origin-china-lab-leak-807b7b0a〔2023/5/23 確認〕
※ 256 総務省：新型コロナウイルス感染症に関するフェイクニュースや偽情報 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd125110.html〔2023/5/23 確認〕
※ 257 独立行政法人国民生活センター：これまでに寄せられた新型コロナウイルス関連の消費者トラブル https://www.kokusen.go.jp/soudan_now/data/coronavirus_jirei.html〔2023/5/23 確認〕
※ 258 米国・欧州等においては、ワクチン接種の可否は個人が決定すべきであり、政府の指示によるべきでないとの考えもある。
※ 259 REUTERS：中国とロシア、偽情報で欧米ワクチンの不信感植え付け＝EU https://jp.reuters.com/article/health-coronavirus-disinformation-idJPKBN2CF2MR〔2023/5/23 確認〕
※ 260 笹原和俊、デジタル影響工作に対する計算社会科学のアプローチ、一田和樹他、ネット世論操作とデジタル影響工作、原書房、2023 年 3 月 20 日
※ 261 REUTERS：U.S. Supreme Court dumps last of Trump's election appeals https://www.reuters.com/article/us-usa-court-election-idUSKBN2B01LE〔2023/5/23 確認〕
REUTERS：米最高裁、激戦 4 州の結果無効化の訴え退ける トランプ氏に打撃 https://jp.reuters.com/article/usa-election-trump-idJPKBN28M084〔2023/6/19 確認〕
※ 262 The Washington Post：How one of America’s ugliest days unraveled inside and outside the Capitol https://www.washingtonpost.com/nation/interactive/2021/capitol-insurrection-visual-timeline/?utm_campaign=wp_graphics&utm_medium=social&utm_source=twitter〔2023/5/23 確認〕
※ 263 Bloomberg：Fox’s $787.5 Million Settlement Doesn’t End Its Liability Over 2020 Election Fraud Claims https://www.bloomberg.com/news/articles/2023-04-18/fox-agrees-to-settle-dominion-lawsuit-over-election-fraud-claims?leadSource=uverify%20wall〔2023/5/23 確認〕
※ 264 日本経済新聞：ロシア、米大統領選で郵便投票標的か 偽情報に米警戒 https://www.nikkei.com/article/DGXMZO63427550U0A900C2FF8000/〔2023/5/23 確認〕
※ 265 CNN：フェイスブック、ロシア発の選挙工作を阻止 FBI の情報受け https://www.cnn.co.jp/tech/35159056.html〔2023/5/23 確認〕
※ 266 一般社団法人日本戦略研究フォーラム：アメリカ大統領選が揉めた最大の理由とは https://www.jfss.gr.jp/article/1397〔2023/5/23 確認〕
※ 267 The New York Times：Elon Musk Reinstates Trump’s Twitter Account https://www.nytimes.com/2022/11/19/technology/trump-twitter-musk.html〔2023/5/23 確認〕
※ 268 佐々木孝博、ロシアによるデジタル影響工作、一田和樹他、ネット世論操作とデジタル影響工作、原書房、2023 年 3 月 20 日
※ 269 U.S. Department of State：GEC Special Report: August 2020 Pillars of Russia’s Disinformation and Propaganda Ecosystem https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf〔2023/5/23 確認〕
※ 270 Microsoft Corporation：ウクライナの防衛：サイバー戦争の初期の教訓 https://news.microsoft.com/ja-jp/2022/07/04/220704-defending-ukraine-early-lessons-from-the-cyber-war/〔2023/5/23 確認〕
※ 271 朝日新聞：ロシアの偽情報作戦、ソ連時代から「お家芸」 ウクライナ危機の深層 https://digital.asahi.com/articles/ASQ2S7H84Q2SUHBI03X.html〔2023/5/23 確認〕
※ 272 The New York Times：Russia has been laying groundwork online for a ‘false flag’ operation, misinformation researchers say. https://www.nytimes.com/2022/02/19/business/russia-has-been-laying-groundwork-online-for-a-false-flag-operation-misinformation-researchers-say.html〔2023/5/23 確認〕
※ 273 藤村厚夫、世界のメディアの変容、一田和樹他、ネット世論操作とデジタル影響工作、原書房、2023 年 3 月 20 日
※ 274 The Wall Street Journal：ロシアで SNS「テレグラム」急成長の理由 https://jp.wsj.com/articles/telegram-thrives-amid-russias-media-crackdown-11647826301〔2023/5/23 確認〕
※ 275 University of Cambridge：The failure of Russian propaganda

https://www.cam.ac.uk/stories/donbaspropaganda〔2023/5/23 確認〕
※ 276 公安調査庁：内外情勢の回顧と展望（令和５年度版）特集３サイバー空間の広がりに伴う脅威の拡散　https://www.moj.go.jp/content/001386269.pdf〔2023/5/23 確認〕
※ 277 コンテンツファーム：広告収入を目的として質の高くない Web コンテンツを大量に作成・配信する企業・サービス。
※ 278 Brookings Institute：Disinformation in Taiwan, in Impact of disinformation on democracy in Asia　https://www.brookings.edu/wp-content/uploads/2022/12/FP_20221216_democracy_asia_disinformation.pdf〔2023/5/23 確認〕
※ 279 NHK：サイカル journal 情報戦　https://www3.nhk.or.jp/news/special/sci_cul/2023/01/special/taiwan-2/〔2023/5/23 確認〕
※ 280 The Diplomat：China's Changing Disinformation and Propaganda Targeting Taiwan　https://thediplomat.com/2022/09/chinas-changing-disinformation-and-propaganda-targeting-taiwan/〔2023/5/23 確認〕
※ 281 REUTERS：Taiwan president quits as party head after China threat bet fails to win votes　https://www.reuters.com/world/asia-pacific/taiwan-votes-local-elections-amid-tensions-with-china-2022-11-26/〔2023/5/23 確認〕
※ 282 Varieties of Democracy (V-Dem)：Democracy Report 2023　https://www.v-dem.net/〔2023/5/23 確認〕
※ 283 公益財団法人日本国際問題研究所：台湾有事におけるディスインフォメーションの脅威と対策のあり方　https://www.jiia.or.jp/research-report/security-fy2021-01.html〔2023/5/23 確認〕
※ 284 山本龍彦、大統領選挙後のアメリカ社会　SNS とフェイクポピュリズム、外交、Vo.66　Mar./Apr. 2021
※ 285 東洋経済：DeNA、第３者委報告書が明かした「構造問題」https://toyokeizai.net/articles/-/162628?page=2〔2023/5/23確認〕
※ 286 日経クロステック：DeNA が WELQ 事件受けキュレーション９サイトを閉鎖、守安社長「心よりお詫び」　https://xtech.nikkei.com/it/atcl/news/16/120103594/〔2023/5/23 確認〕
※ 287 山口真一：わが国における誹謗中傷・フェイクニュースの 実態と社会的対処　https://www.soumu.go.jp/main_content/000745067.pdf〔2023/5/23 確認〕
※ 288 藤代裕之：フェイクニュース検証記事の制作過程 ～ 2018 年沖縄県知事選挙における沖縄タイムスを事例として～　http://www.ssi.or.jp/journal/pdf/Vol8No2_10.pdf〔2023/5/23 確認〕
※ 289 琉球帰属論：「琉球は明・清の冊封国であったが、19 世紀に日本が武力で強制的に併合した」との考え方。
※ 290 読売新聞大阪本社社会部、情報パンデミック、あなたを惑わすものの正体　第２章 発信者を追う、中央公論社、2022 年 11 月 10 日
※ 291 読売新聞：SNS で「被害はウクライナの自作自演」拡散、陰謀論に次々傾倒のワナ…浮かぶ共通点　https://www.yomiuri.co.jp/national/20220414-OYT1T50064/〔2023/5/23 確認〕
※ 292 法務省：自粛警察と誤った正義感　https://www.moj.go.jp/JINKEN/jinken05_00055.html〔2023/5/23 確認〕
※ 293 POLITIFACT:https://www.politifact.com/〔2023/5/23 確認〕
※ 294 IFCN：Commit to transparency　— sign up for the International Fact-Checking Network's code of principles　https://ifcncodeofprinciples.poynter.org/〔2023/5/23 確認〕
※ 295 Meta Platforms, Inc.：Facebook のファクトチェックについて　https://www.facebook.com/business/help/2593586717571940〔2023/5/23 確認〕
※ 296 The bmj：Covid-19：Researcher blows the whistle on data integrity issues in Pfizer's vaccine trial　https://www.bmj.com/content/375/bmj.n2635/rr-80〔2023/5/23 確認〕
※ 297 Forbes：Elon Musk's Twitter Quietly Fired Its Democracy And National Security Policy Lead　https://www.forbes.com/sites/thomasbrewster/2023/02/24/elon-musk-twitter-democracy-and-human-rights-layoffs/?sh=e902f4f6b97e〔2023/5/23 確認〕
※ 298 Poynter.：Elon Musk keeps Birdwatch alive — under a new name　https://www.poynter.org/fact-checking/2022/elon-musk-keeps-birdwatch-alive-under-a-new-name/〔2023/5/23 確認〕
※ 299 Gigazine：YouTube が誤情報やデマの温床と化していると 80 以上のファクトチェック団体が抗議　https://gigazine.net/news/20220113-fact-checkers-urge-youtube-fight-disinformation/〔2023/5/23 確認〕
Poynter.：An open letter to YouTube's CEO from the world's fact-checkers　https://www.poynter.org/fact-checking/2022/an-open-letter-to-youtubes-ceo-from-the-worlds-fact-checkers/〔2023/5/23 確認〕
※ 300 論座:動画や音声までも対象とする「ファクトチェック自動化」は、フェイクニュースの解決策となるか　https://webronza.asahi.com/business/articles/2022072800007.html?page=1〔2023/5/23 確認〕
※ 301 DeepFake Detection　https://paperswithcode.com/task/deepfake-detection〔2023/5/23 確認〕
※ 302 佐々木孝博、ロシアによるデジタル影響工作、一田和樹他、ネット世論操作とデジタル影響工作、原書房、2023 年３月 20 日
川口貴久、権威主義国家によるデジタル影響工作と民主主義、一田和樹他、ネット世論操作とデジタル影響工作、原書房、2023 年３月 20 日
※ 303 民放オンライン:ロシアでフェイクニュース法　各国メディアが報道・取材活動中止　https://minpo.online/article/post-91.html〔2023/5/23 確認〕
※ 304 湯淺墾道：アメリカ選挙法におけるディープフェイク規制の動向　https://www.spf.org/iina/articles/harumichi_yuasa_01.html〔2023/5/23 確認〕
※ 305 CISA：Rumor Control Start-Up Guide　https://www.cisa.gov/resources-tools/resources/rumor-control-start-guide〔2023/5/23 確認〕
※ 306 European Commission：The Digital Services Act: ensuring a safe and accountable online environment　https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en〔2023/5/23 確認〕
※ 307 REUTERS：欧州議会、AI規則案の修正を採択　https://jp.reuters.com/article/tech-ai-eu-idJPKBN2Y01WN〔2023/6/27 確認〕
※ 308 総務省：プラットフォームサービスに関する検討会　https://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/index.html〔2023/5/23 確認〕
※ 309 総務省：誹謗中傷等の違法・有害情報への対策に関するワーキンググループ（第１回）インターネット上の違法・有害情報に関する 流通実態アンケート調査　https://www.soumu.go.jp/main_content/000853886.pdf〔2023/5/23 確認〕
※ 310 総務省：プラットフォームサービスに関する検討会　偽情報対策に係る取組集　https://www.soumu.go.jp/main_content/000868124.pdf〔2023/5/23 確認〕
※ 311 総務省：「2030 年頃を見据えた情報通信政策の在り方」二次答申（案）に関する意見募集　https://www.soumu.go.jp/menu_news/s-news/01ryutsu20_02000001_00003.html〔2023/5/23 確認〕
※ 312 一般社団法人セーファーインターネット協会：Disinformation 対策フォーラム　https://www.saferinternet.or.jp/anti-disinformation/〔2023/5/23 確認〕
※ 313 https://fij.info/〔2023/5/23 確認〕
※ 314 日本ファクトチェックセンター：https://factcheckcenter.jp/〔2023/5/23 確認〕
※ 315 総務省　プラットフォームサービスに関する研究会：日本におけるファクトチェック活動の現状と課題　https://www.soumu.go.jp/main_content/000861267.pdf〔2023/5/23 確認〕
※ 316 消費者庁：ステルスマーケティングに関する検討会　https://www.caa.go.jp/policies/policy/representation/meeting_materials/review_meeting_005/〔2023/5/23 確認〕
※ 317 日本経済新聞：「ステマ」法規制へ　消費者庁、広告主を行政処分　https://www.nikkei.com/article/DGXZQOUE260PX0W2A221C2000000/〔2023/5/23 確認〕
※ 318 日本経済新聞：「ステマ」10 月から規制へ　消費者庁、不当表示に追加　https://www.nikkei.com/article/DGXZQOUE274V00X20C23A3000000/〔2023/5/23 確認〕
※ 319 JIJI.COM：「生成 AI」活用へ環境整備　日本語アプリの開発促進―政府　https://www.jiji.com/jc/article?k=2023042500953&g=pol〔2023/5/23 確認〕
※ 320 日本経済新聞：日本は生成 AI 天国か　著作物「学び放題」に危機感も　https://www.nikkei.com/article/DGXZQOCD072460X00C23A4000000/〔2023/5/23 確認〕
※ 321 東京大学：生成系 AI（ChatGPT, BingAI, Bard, Midjourney, Stable Diffusion 等）について　https://utelecon.adm.u-tokyo.ac.jp/docs/20230403-generative-ai〔2023/5/23 確認〕
東洋大学：生成系 AI に関する INIAD の見解　https://www.toyo.ac.jp/news/academics/faculty/iniad/20230414/〔2023/5/23 確認〕
※ 322 G7 群馬高崎デジタル・技術大臣会合：「G7 群馬高崎デジタル・技術大臣会合」の開催結果　https://g7digital-tech-2023.go.jp/topics/topics_20230430.html〔2023/5/23 確認〕
※ 323 内閣官房：国家安全保障戦略について　https://www.cas.go.jp/jp/siryou/221216anzenhoshou.html〔2023/5/23 確認〕
※ 324 読売新聞社大阪本社社会部、情報パンデミック　あなたを惑わすものの正体　第２章 発信者を追う　なぜ広めるのか、中央公論社、2022 年 11 月 10 日
※ 325 ニューズウィーク日本版：2023 年は AI が生成したフェイクニュースが巷にあふれる ..... インフォカリプス（情報の終焉）の到来　https://www.newsweekjapan.jp/ichida/2023/01/2023ai.php〔2023/5/23 確認〕

付録

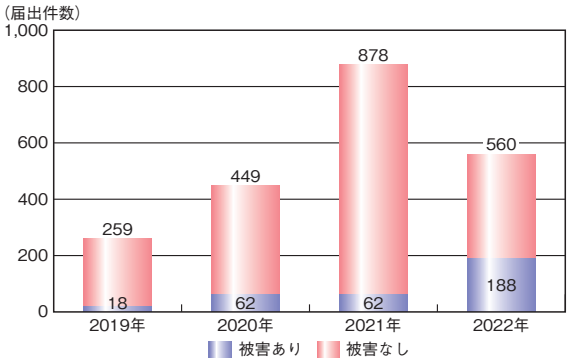
資料

資料A　2022年のコンピュータウイルス届出状況

IPA が 2022 年 1 月から 12 月の期間に受け付けたコンピュータウイルス（以下、ウイルス）届出の集計結果について述べる。

A.1　届出件数

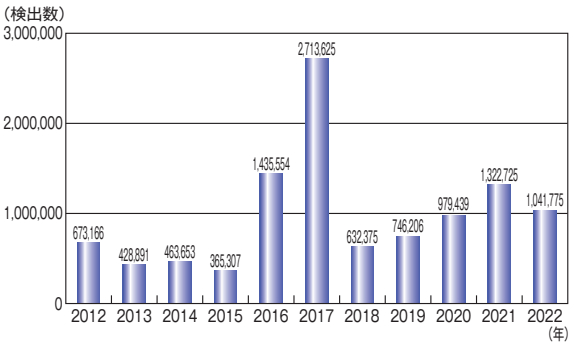
2022 年の年間届出件数は、前年の 878 件より 318 件（36.2%）少ない 560 件であった（図 A-1）。そのうち、ウイルス感染の実被害があった届出は 188 件であった。



■図 A-1　ウイルス届出件数推移（2019～2022 年）

A.2　届出のあったウイルス等検出数

2022 年に寄せられたウイルス等の検出数は、前年の 132 万 2,725 個より 28 万 950 個（21.2%）少ない 104 万 1,775 個であった（図 A-2）。



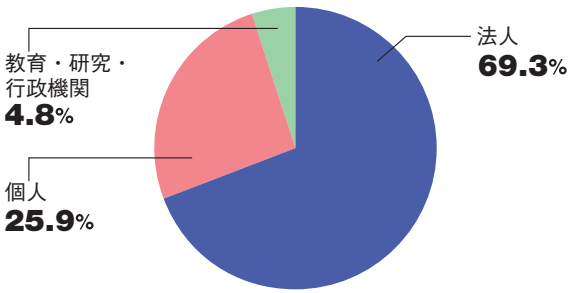
■図 A-2　ウイルス等検出数推移（2012～2022 年）

A.3　届出者の主体別届出件数

2022 年は前年と比較すると、全体の届出件数は減少した一方で、「法人」からの届出は増加した。届出者の主体別の比率では「法人」からの届出が 69.3%（388 件）と最も多かった（表 A-1、図 A-3）。

届出者の主体	2020 年	2021 年	2022 年
法人	232	284	388
個人	188	578	145
教育・研究・行政機関	29	16	27
合計（件）	449	878	560

■表 A-1　ウイルス届出者の主体別届出件数（2020～2022 年）



■図 A-3　ウイルス届出者の主体別届出件数の比率（2022 年）

A.4　傾向

2022 年でウイルス感染の実被害に遭った届出 188 件のうち、145 件が Emotet に感染した被害であり、半数以上を占めた。特に 3 月においては 42 件の被害の届出があり、これは IPA が 2 月に「Emotet の攻撃活動の急増」として、注意喚起を行った時期と一致する。これらの届出件数の詳細は、下記の資料を参照いただきたい。また、本白書では「1.2.6 ばらまき型メールによる攻撃」にて、メールを介してウイルスを感染させる攻撃手口や対策について詳しく述べているので、ぜひこちらも一読いただきたい。

参照

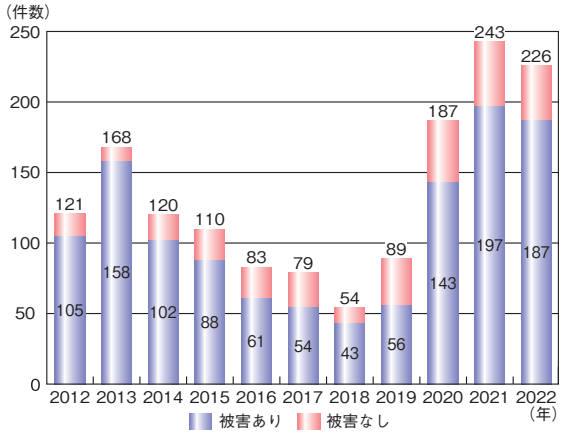
■コンピュータウイルス・不正アクセスの届出状況［2022年（1月～12月）］
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108005.pdf

資料B　2022年のコンピュータ不正アクセス届出状況

IPA が 2022 年 1 月から 12 月の期間に受け付けたコンピュータ不正アクセス（以下、不正アクセス）届出の集計結果について述べる。

B.1　届出件数

2022 年の年間届出件数は、前年の 243 件より 17 件（7.0%）少ない 226 件であった（図 B-1）。そのうち、実被害があった届出は 187 件であった。



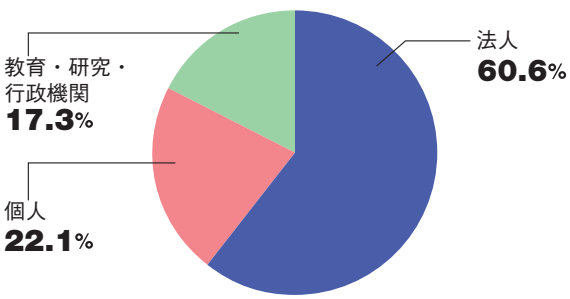
■図 B-1　不正アクセス届出件数推移（2012 年～2022 年）

B.2　届出者の主体別届出件数

2022 年は前年と比較すると、「法人」からの届出件数が減少しているが、届出者の主体別の比率では「法人」からの届出が 60.6%（137 件）と最も多かった（表 B-1、図 B-2）。

届出者の主体	2020 年	2021 年	2022 年
法人	114	156	137
個人	57	46	50
教育・研究・行政機関	16	41	39
合計（件）	187	243	226

■表 B-1　不正アクセス届出者の主体別届出件数（2020～2022 年）

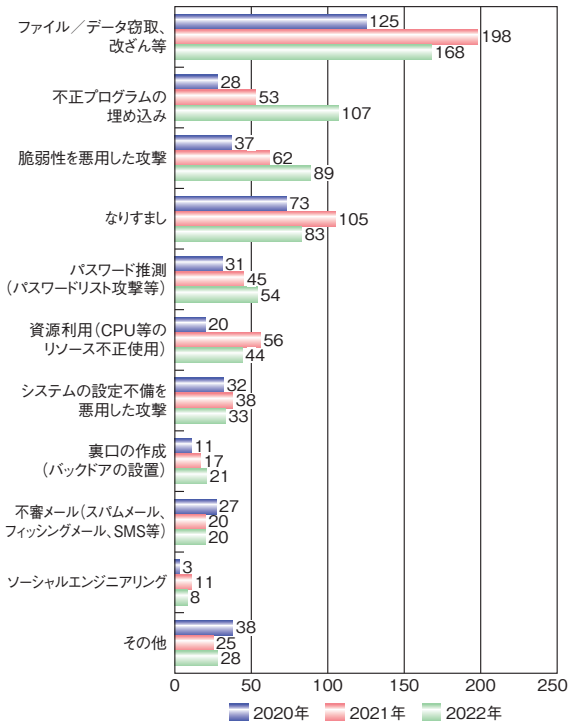


■図 B-2　不正アクセス届出者の主体別届出件数の比率（2022 年）

B.3　手口別件数

届出を攻撃行為（手口）により分類した件数を図 B-3 に示す。なお、以降の分類も含め、届出 1 件につき、複数の分類項目が該当する場合がある。その場合は該当する項目のそれぞれにカウントした。

2022 年の届出において最も多く見られた手口は、前年と同様に「ファイル／データ窃取、改ざん等」の 168 件であり、次いで「不正プログラムの埋め込み」が 107 件、「脆弱性を悪用した攻撃」が 89 件であった。



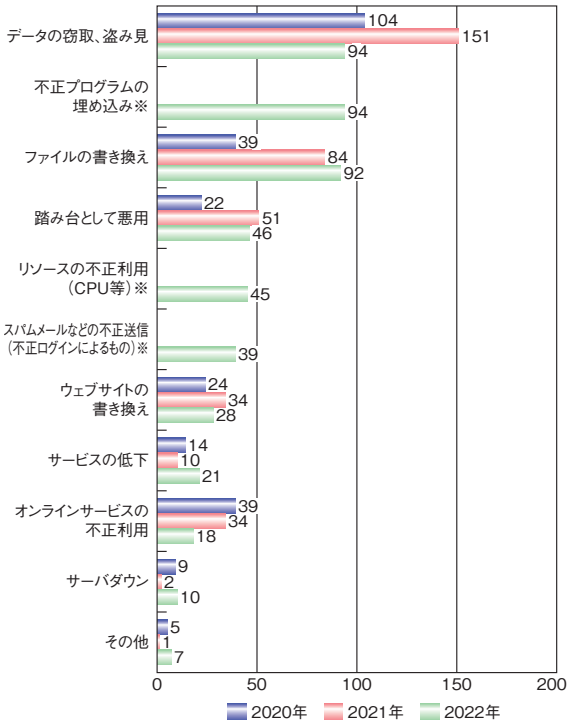
■図 B-3　不正アクセス手口別件数の推移（2020～2022 年）

B.4　被害内容別件数

届出のうち、実際に被害に遭った届出について、被害内容により分類した件数を図 B-4 に示す。2022 年の届出において最も多く見られた被害は、「データの窃取、盗み見」と「不正プログラムの埋め込み」の 94 件であった。次いで「ファイルの書き換え」が 92 件、「踏み台として悪用」が 46 件であった。

なお、具体的な被害事例については、「コンピュータウイルス・不正アクセスに関する届出について」（https://www.ipa.go.jp/security/todokede/crack-virus/about.

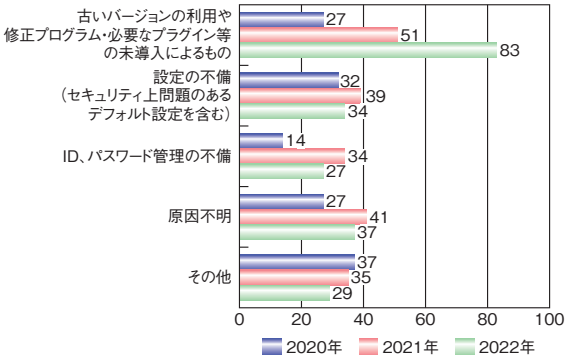
html）において「コンピュータウイルス・不正アクセスの届出事例［2022 年上半期（1 月～ 6 月）］」及び「コンピュータウイルス・不正アクセスの届出事例［2022 年下半期（7 月～ 12 月）］」を紹介している。そちらも、ぜひ参考にしていただきたい。



■図 B-4　不正アクセス被害内容別件数の推移（2020～2022 年）
※被害内容が多様化したため、2022 年から項目を細分化した。

B.5 原因別件数

実際に被害に遭った届出について、不正アクセスの原因となった問題点／弱点で分類した件数を図 B-5 に示す。2022 年の届出において最も多く見られた原因は、前年と同様に「古いバージョンの利用や修正プログラム・必要なプラグイン等の未導入によるもの」であり 83 件であった。次いで「設定不備（セキュリティ上問題のあるデフォルト設定を含む）」が 34 件、「ID、パスワード管理の不備」が 27 件であった。



■図 B-5　不正アクセス原因別件数の推移（2020～2022 年）

B.6 傾向と対策

不正アクセス被害の傾向と対策について述べる。

(1) 企業・組織の被害の傾向と対策

2022 年は Web サイト（EC サイトを含む）の脆弱性や設定不備を悪用した不正アクセスに関する被害が多く見られた。また、VPN 装置の脆弱性やリモートデスクトップサービスの設定不備を悪用した不正侵入に関する被害も依然として多く確認されている（「1.2.5 (1) VPN 製品の脆弱性を対象とした攻撃」「1.2.1 ランサムウェア攻撃」参照）。

対策としては、Web サイトや VPN 装置等に限らず、利用している機器やソフトウェアに関する脆弱性情報の収集と修正プログラムの適用、設定の見直しといった基本的なセキュリティ対策を実施することが重要である。更に、Web アプリケーションの脆弱性診断の実施等も含めて、着実に脆弱性や設定不備を解消していく必要がある。

(2) システム利用者の被害の傾向と対策

2022 年も引き続き、パスワードリスト攻撃や総当たり攻撃により、認証が突破されたことで、メールアカウント等が不正利用されたとする被害が依然として見られた。

システム利用者においては、他者に推測されにくい複雑なパスワードを設定する、パスワードの使いまわしをしないといった基本的な対策を実施することに加えて、多要素認証等のセキュリティオプションを積極的に採用する等、自身が所有するアカウントが適切に管理できているか今一度見直していただきたい。

参照

■コンピュータウイルス・不正アクセスの届出状況［2022年（1月～12月）］
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108005.pdf

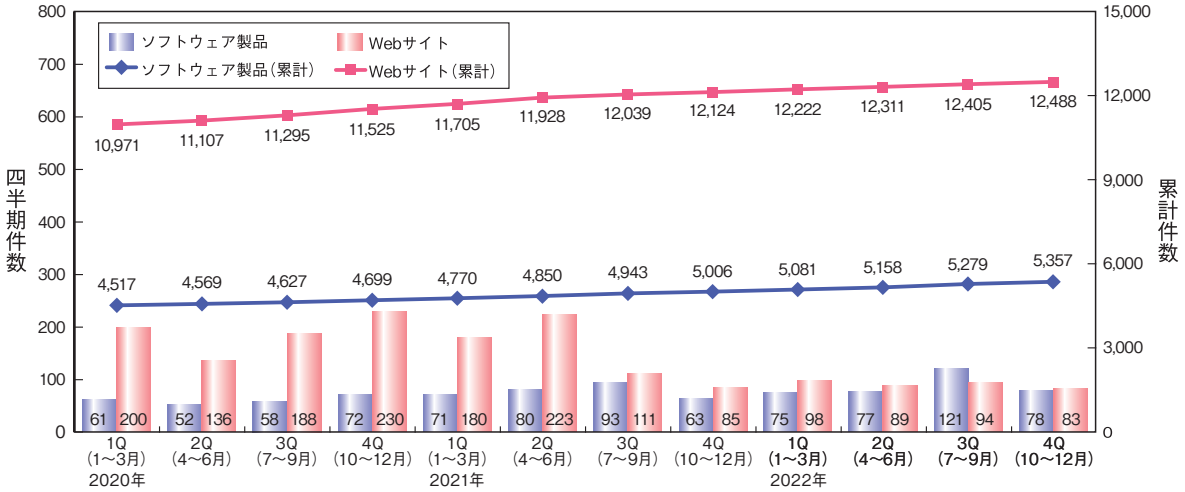
資料C　ソフトウェア等の脆弱性関連情報に関する届出状況

IPA が受け付けた脆弱性関連情報に関する届出は、2022 年末までに 1 万 7,845 件に達した。

C.1　脆弱性の届出概況

2022 年末時点で、届出受付開始（2004 年 7 月 8 日）からの累計は、ソフトウェア製品に関するもの 5,357 件、Web サイトに関するもの 1 万 2,488 件、合計 1 万 7,845 件で、Web サイトに関する届出が全体の 70.0% を占めている（図 C-1）。

表 C-1 に示すように、届出受付開始から各四半期末時点までの就業日 1 日あたりの届出件数は、2022 年第 4 四半期末時点で 3.97 件となっている。



■図 C-1　脆弱性関連情報の届出件数の四半期別推移

2020年1Q（1~3月）	2020年2Q（4~6月）	2020年3Q（7~9月）	2020年4Q（10~12月）	2021年1Q（1~3月）	2021年2Q（4~6月）	2021年3Q（7~9月）	2021年4Q（10~12月）	2022年1Q（1~3月）	2022年2Q（4~6月）	2022年3Q（7~9月）	2022年4Q（10~12月）
4.04	4.03	4.03	4.04	4.04	4.06	4.05	4.02	4.01	3.99	3.98	3.97

■表 C-1　就業日 1 日あたりの届出件数（届出受付開始から各四半期末時点）

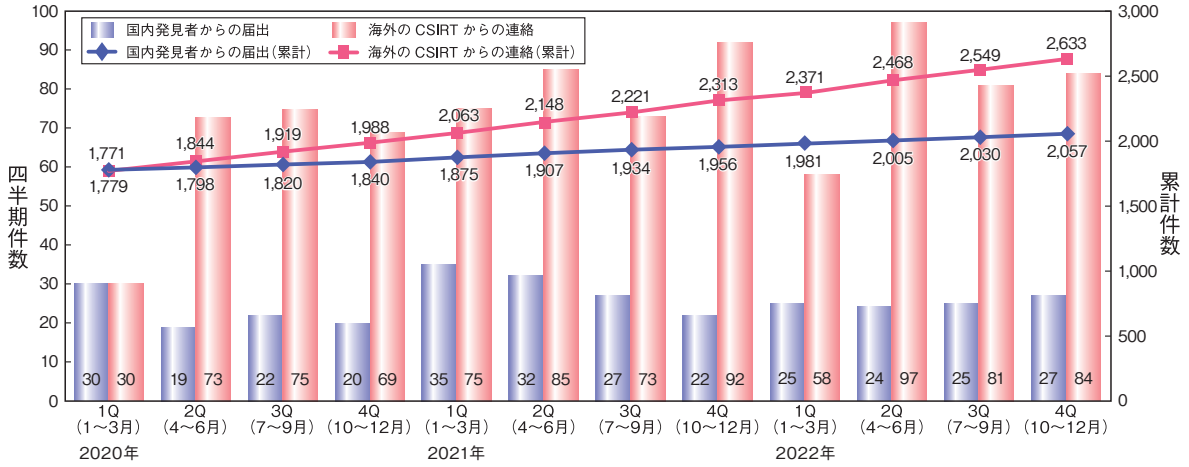
C.2　ソフトウェア製品の脆弱性の処理の終了状況

2022 年末時点のソフトウェア製品に関する脆弱性の処理状況は、JPCERT/CC が調整を行い、製品開発者が脆弱性の修正を完了し、JVN で対策情報を公表したものは 2,488 件、JVN で公表せず製品開発者が個別対応を行ったものは 40 件、製品開発者が脆弱性ではないと判断したものは 108 件、告示で定める届出の対象に該当せず不受理としたものは 521 件で、処理の終了件数の合計は 3,157 件に達した（表 C-2）。

このほか、海外の CSIRT から JPCERT/CC が連絡を受けた 2,633 件を JVN で公表した。これらの脆弱性対策情報の公表件数の期別推移を図 C-2 に示す。なお、複数の届出についてまとめて 1 件の脆弱性対策情報として公表する場合があるため、表 C-2 の「公表済み」の件数と図 C-2 の公表件数は異なっている。

分類		累計件数
修正完了	公表済み	2,488件
	個別対応	40件
脆弱性ではない		108件
不受理		521件
合計		3,157件

■表 C-2　ソフトウェア製品の脆弱性の処理終了件数



■図 C-2　ソフトウェア製品の脆弱性対策情報の公表件数

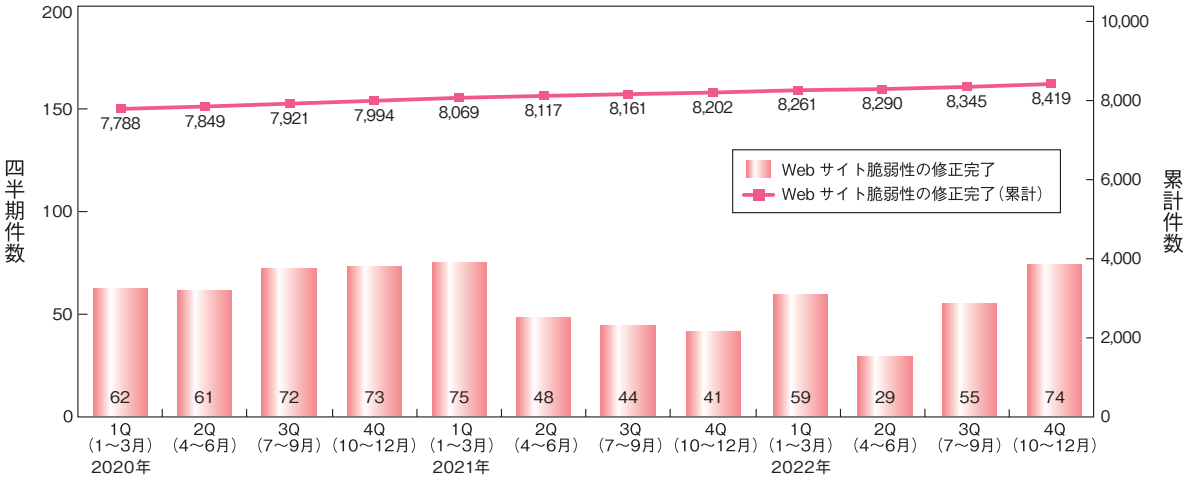
C.3 Webサイトの脆弱性の処理の終了状況

2022 年末時点の Web サイトに関する脆弱性の処理状況は、IPA が通知を行い Web サイト運営者が修正を完了したものは 8,419 件、IPA が注意喚起等を行った後に処理を終了したものは 1,130 件、IPA 及び Web サイト運営者が脆弱性ではないと判断したものは 732 件、Web サイト運営者と連絡が不可能なもの、または IPA が対応を促しても修正完了した旨の報告をしない、修正を拒否する等、Web サイト運営者の対応により取り扱いが不能なものが 232 件、告示で定める届出の対象に該当せず不受理としたものは 286 件で、処理の終了件数の合計は 1 万 799 件に達した（表 C-3）。

これらのうち、修正完了件数の期別推移を図 C-3 に示す。

分類	累計件数
修正完了	8,419件
注意喚起	1,130件
脆弱性ではない	732件
取扱不能	232件
不受理	286件
合計	10,799件

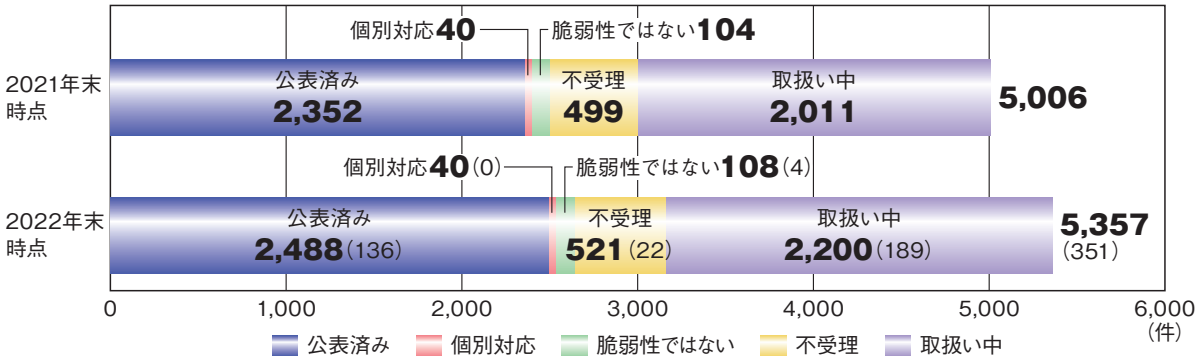
■表 C-3　Web サイトの脆弱性の終了件数



■図 C-3　Web サイトの脆弱性の修正完了件数

C.4 ソフトウェア製品の脆弱性の届出の処理状況

ソフトウェア製品の脆弱性関連情報の届出について処理状況を図 C-4 に示す。2022 年に JVN で「公表済み」となったソフトウェア製品の件数は 136 件で累計 2,488 件となった。また、「取扱い中」の届出は 189 件増加し、2,200 件となった。「処理終了」した届出は、162 件増加し、累計 3,157 件となった。

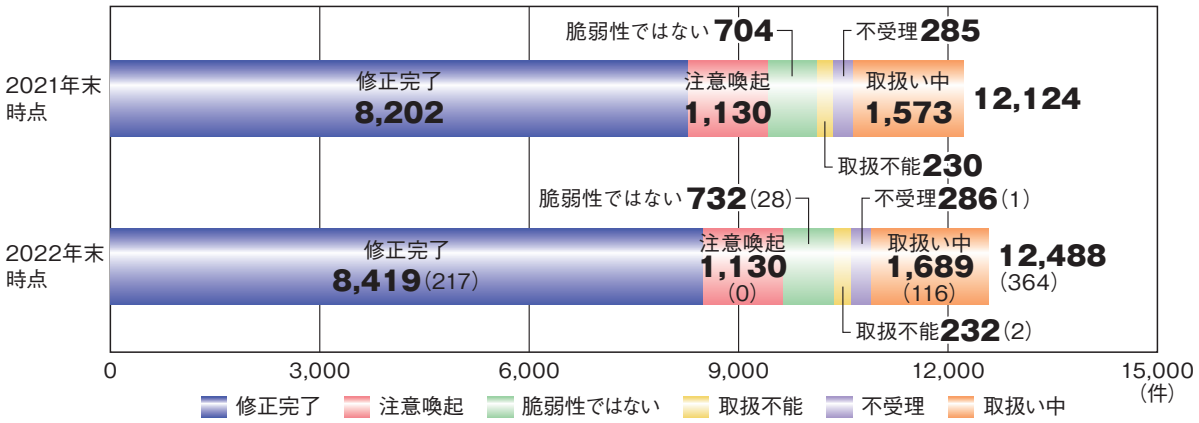


※( )内の数値は 2021 年末時点と 2022 年末時点の差分

■図 C-4　ソフトウェア製品の脆弱性関連情報の届出の処理状況の推移

C.5 Webサイトの脆弱性の届出の処理状況

Web サイトの脆弱性関連情報の届出について処理状況を図 C-5 に示す。2022 年に「修正完了」した Web サイトの件数は 217 件で累計 8,419 件となった。また、「取扱い中」の届出は 116 件増加し、1,689 件となった。「処理終了」した届出は、248 件増加し、累計 10,779 件となった。



※( )内の数値は 2021 年末時点と 2022 年末時点の差分

■図 C-5　Web サイトの脆弱性関連情報の届出の処理状況の推移

参照

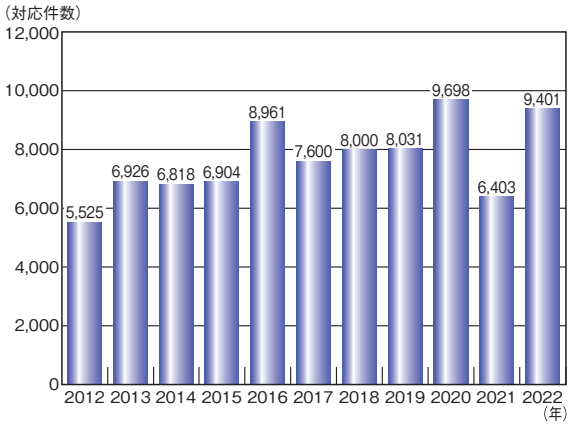
■ソフトウェア等の脆弱性関連情報に関する届出状況［2022年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/reports/vuln/software/2022q4.html

資料D　2022年の情報セキュリティ安心相談窓口の相談状況

IPA が 2022 年 1 月から 12 月の期間に対応した、相談状況の集計結果について述べる。

D.1　相談対応件数

2022 年の年間相談対応件数は 9,401 件となり、2021 年の相談対応件数 6,403 件より 2,998 件（46.8%）の増加となった（図 D-1）。



■図 D-1　相談対応件数推移（2012～2022 年）

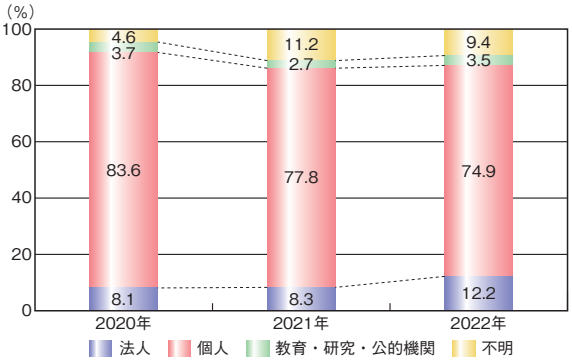
D.2　相談者の主体別相談件数

2022 年は個人からの相談が 7,043 件（74.9%）と最も多かった。

相談者の主体別相談比率の推移では、法人からの相談比率が 2 年連続で前年を上回り、2022 年は 1,145 件（12.2%）に達した（表 D-1、図 D-2）。

相談者の主体	2020 年	2021 年	2022 年
法人	782	530	1,145
個人	8,110	4,984	7,043
教育・研究・公的機関	359	170	330
不明	447	719	883
合計（件）	9,698	6,403	9,401

■表 D-1　情報セキュリティ安心相談窓口の主体別相談対応件数（2020～2022 年）



■図 D-2　情報セキュリティ安心相談窓口の主体別相談件数の比率推移（2020～2022 年）

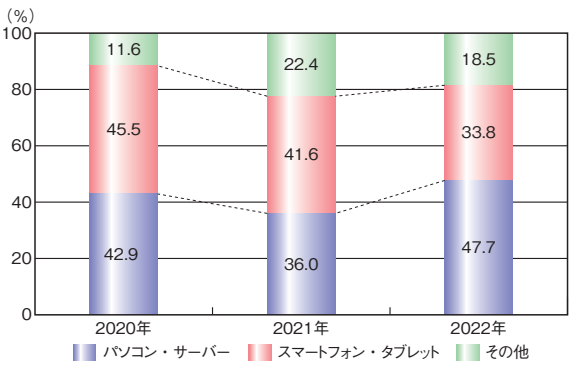
D.3　相談者の機器種別相談件数

2022 年は「パソコン・サーバー」に関する相談が 4,487 件（47.7%）と最も多かった。

相談者の機器種別相談比率の推移では、「スマートフォン・タブレット」に関する相談が減少する一方で、「パソコン・サーバー」に関する相談は大幅に増加した（表 D-2、図 D-3）。「Emotet 関連」についての相談増加が、要因の一つと考えられる。

機器種別の主体	2020 年	2021 年	2022 年
パソコン・サーバー	4,163	2,304	4,487
スマートフォン・タブレット	4,411	2,666	3,173
その他	1,124	1,433	1,741
合計（件）	9,698	6,403	9,401

■表 D-2　情報セキュリティ安心相談窓口の機器種別相談件数（2020～2022 年）

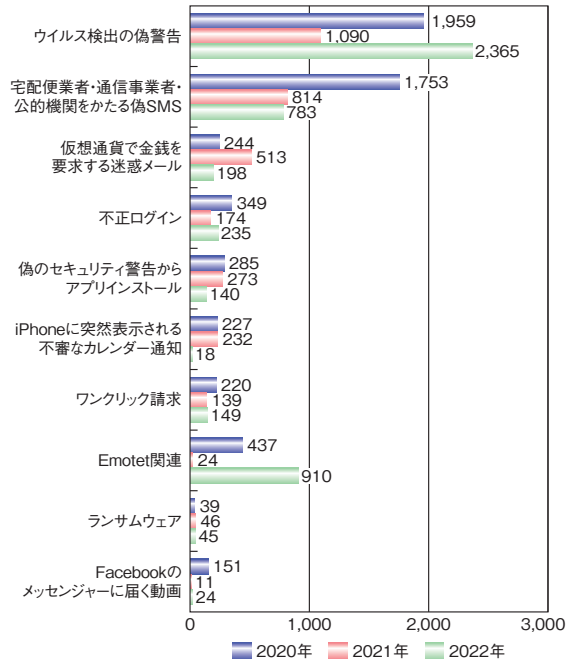


■図 D-3　情報セキュリティ安心相談窓口の機器種別相談件数の比率推移（2020～2022 年）

D.4 手口別相談件数

主な手口ごとの相談件数を図 D-4 に示す。2022 年の相談で最も多く寄せられたのは、「ウイルス検出の偽警告」に関する相談で2,365 件（25.2%）であった。次いで、「Emotet 関連」についての相談が 910 件（9.7%）、「宅配便業者・通信事業者・公的機関をかたる偽 SMS」に関する相談が 783 件（8.3%）であった。上位三つの手口による相談件数の合計は 4,058 件で、全相談件数（9,401 件）の 43.2% であった。

問い合わせの多い手口については、情報セキュリティ安心相談窓口の発行する「安心相談窓口だより」や、「手口検証動画」で注意喚起を行っている。ぜひ参考にしてほしい。



■図 D-4　主な手口別相談件数の推移（2020～2022 年）

参照

■安心相談窓口だより
https://www.ipa.go.jp/security/anshin/attention/index.html
■手口検証動画シリーズ
https://www.ipa.go.jp/security/anshin/measures/verificationmov.html

IPAコンクール応援隊長「まもるくん」

第18回 IPA「ひろげよう情報モラル・セキュリティコンクール」2022 受賞作品

IPAは、子どもたちがインターネットにまつわる課題に自ら向き合い、解決策を見出すきっかけとして、全国の小学生・中学生・高校生・高専生を対象とするコンクールを開催しています。

ここでは、全61,962点の応募作品の中から、受賞した作品の一部をご紹介いたします。なお、すべての受賞作品は下記のWebサイトで公開しています。

[https://www.ipa.go.jp/security/hyogo/]

最優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

話すのは
ネット上でも
人と人

北海道 北海道帯広柏葉高等学校 2年 **小沼 裕詞郎**さん

〈ポスター部門〉

青森県 弘前大学教育学部附属中学校 2年 **橋本 和香**さん

〈4コマ漫画部門〉

沖縄県 沖縄市立沖縄東中学校 2年
安慶田 ひよりさん

優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

だいじだよ　ぼくのぶんしん　パスワード

東京都　世田谷区立東玉川小学校　1年
加藤 佑悟さん

ネットだと　ついつい緩む　心の扉

福岡県　福岡市立那珂中学校　3年
柳瀬 優月さん

鍵はした?　家もスマホも　一緒だよ

兵庫県　神戸学院大学附属高等学校　3年
森岡 泰椛さん

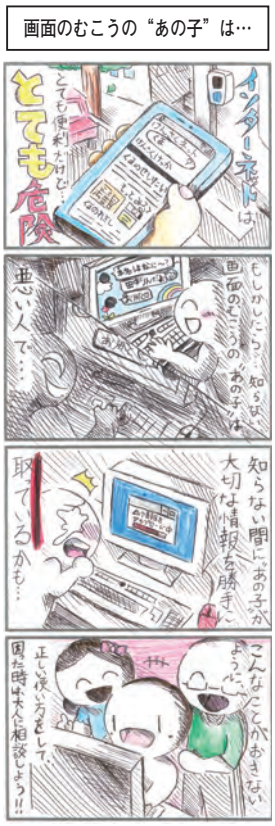
〈ポスター部門〉

愛知県 知立市立知立小学校 5年
石川 花凛さん

埼玉県 越谷市立千間台中学校 2年
北村 汐月さん

長崎県 長崎県立長崎工業高等学校 2年
藤本 佳穂さん

〈4コマ漫画部門〉



山梨県 山梨学院小学校 6年
大代 花凛さん

奈良県 香芝市立香芝北中学校 3年
内海 花菜さん

佐賀県 佐賀県立白石高等学校 1年
髙岸 孝仁さん

IPAの便利なツールとコンテンツ

情報セキュリティ対策ベンチマーク
https://security-shien.ipa.go.jp/diagnosis/benchmark/index.html?bm_id=1

診断

用途・目的	自組織のセキュリティレベルを診断
利用対象者	情報セキュリティ担当者
特 長	• 他組織と比較した自組織のセキュリティレベルが判る • 自組織に不足しているセキュリティ対策が判る

概要

「セキュリティ対策の取り組み状況に関する評価項目」27 問と「企業プロフィールに関する評価項目」19 問、計 46 問に回答すると以下の診断結果を表示します。

■提供される診断結果
- セキュリティレベルを示したスコア(最高点 135 点、最低点 27 点)と度数分布状況と偏差値
- 情報セキュリティリスクの指標の分布と企業規模、業種、情報資産数等が自組織と近い他組織と比較し、自組織の位置が示された散布図
- 自組織の過去診断結果との比較や従業員数別での比較を含む 4 種類のレーダーチャート
- 結果に応じた推奨される取り組み

※ベンチマークに使用する診断データは 2022 年 3 月に Ver.5.1 にアップデート

脆弱性体験学習ツール「AppGoat」
https://www.ipa.go.jp/security/vuln/appgoat/

学習

用途・目的	脆弱性の基礎的な知識の学習
利用対象者	• アプリケーション開発者 • Web サイト管理者
特 長	脆弱性の概要や対策方法等、脆弱性に関する基礎的な知識を実習形式で体系的に学べるツール

概要

SQL インジェクション、クロスサイト・スクリプティング等 12 種の Web アプリケーションに関連する脆弱性について学習できるツールです。
利用者は学習テーマ毎の演習問題に対して、埋め込まれた脆弱性の発見、プログラミング上の問題点の把握、対策手法を学べます。

■活用方法例
- Web アプリケーション用学習ツール(個人学習モード)を利用した、自宅等での個人学習
- Web アプリケーション用学習ツール(集合学習モード)を利用した、学校の講義や組織内のセミナー等における複数人での学習

脆弱性対策情報データベース「JVN iPedia」
https://jvndb.jvn.jp/

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	国内外のソフトウェア製品の公開された脆弱性対策情報が掲載されたキーワード検索可能なデータベース

概要

■掲載情報例
- 脆弱性の概要
- 脆弱性がある製品名とそのベンダー名
- 共通脆弱性識別子 CVE
- 脆弱性の深刻度 CVSS 基本値
- 本脆弱性に関わる製品ベンダー等のリンク

■活用方法例
- ネット記事等に記載された CVE 番号を JVN iPedia で検索し、脆弱性の詳細を確認
- 自組織で使用している製品名で検索し、脆弱性の詳細を確認

MyJVN バージョンチェッカ for .NET
https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

対策

用途・目的	パソコンにインストールされたソフトウェア製品が最新バージョンかどうかを確認
利用対象者	パソコン利用者全般
特 長	インストールされている対象製品が最新バージョンかどうかとインストールされているバージョン等を一括確認できる

概要

■判定対象ソフトウェア製品

- Adobe Reader
- Mozilla Firefox
- Lunascape
- VMware Player
- JRE
- Mozilla Thunderbird
- Becky! Internet Mail
- Google Chrome
- Lhaplus
- iTunes
- OpenOffice.org
- LibreOffice

■活用方法例

毎朝 MyJVN バージョンチェッカを実行して、使用しているソフトウェアが最新かどうかをチェックし、最新でなければそのソフトウェアを更新

■動作環境・必須ソフトウェア

- Windows 10、11
- .NET Framework

注意警戒情報サービス
https://jvndb.jvn.jp/alert/

対策

用途・目的	脆弱性対策に必要な最新情報の収集
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	日本で広く利用され、脆弱性が悪用されると影響の大きいサーバー用オープンソースソフトウェアのリリース情報と IPA が発信する「重要なセキュリティ情報」を提供

概要

■掲載情報例

- Apache HTTP Server
- BIND
- WordPress
- Apache Struts
- Joomla!
- 重要なセキュリティ情報
- Apache Tomcat
- OpenSSL

■活用方法例

定期的に自組織で使用しているオープンソースソフトウェアのリリース情報や IPA が発信する「重要なセキュリティ情報」が公表されているかどうかを確認し、公表されていれば内容の確認、必要に応じ対応を行う

サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

対策

用途・目的	IPA が発信する「重要なセキュリティ情報」のリアルタイム取得
利用対象者	• システム管理者 • サービスの保守を担う担当者 • 個人利用者
特 長	Web ページに HTML タグを埋め込むと、IPA が発信する「重要なセキュリティ情報」とリアルタイムに同期した情報を表示させる

概要

■「重要なセキュリティ情報」発信例

- 利用者への影響が大きい製品の脆弱性情報
- サイバー攻撃への注意喚起
- 広く使われる製品のサポート終了情報

■活用方法例

icat を自組織の従業員がよくアクセスする Web ページ（イントラページ等）に表示させ、ソフトウェア更新等の対策を促す

MyJVN 脆弱性対策情報フィルタリング収集ツール（mjcheck4）
https://jvndb.jvn.jp/apis/myjvn/mjcheck4.html

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	JVN iPedia に登録されている脆弱性対策情報をフィルタリングして自社システムに関連する脆弱性情報を効率よく収集

概要

■フィルタリング例
• 製品名　　• CVSSv3　　• 公開日　等

■活用方法例
• 自組織が利用しているオープンサーバーソフトウェア製品の脆弱性対策情報収集
• 情報システム部門が運用しているシステムの脆弱性対策情報の収集

■動作環境・必須ソフトウェア
• Windows 10、11

Web サイトの攻撃兆候検出ツール「iLogScanner」
https://www.ipa.go.jp/security/vuln/ilogscanner/

診断

用途・目的	Web サイトに対する攻撃の痕跡、攻撃の可能性を検出
利用対象者	Web サイト運営者
特 長	Web サイトのアクセスログ、エラーログ、認証ログを解析し、攻撃の痕跡や攻撃に成功した可能性があるログを解析結果レポートに表示

概要

■アクセスログ、エラーログから検出可能な項目例
• SQL インジェクション　　• OS コマンド・インジェクション
• ディレクトリ・トラバーサル　　• クロスサイト・スクリプティング

■認証ログ（Secure Shell、FTP）から検出可能な項目例
• 大量のログイン失敗　　• 短時間の集中ログイン
• 同一ファイルへの大量アクセス　　• 認証試行回数

■活用方法例
定期的に iLogScanner を実行し、自組織の Web サイトを狙った攻撃が行われているか確認

5 分でできる！情報セキュリティ自社診断
https://security-shien.ipa.go.jp/diagnosis/selfcheck/

診断

用途・目的	自社の情報セキュリティ対策状況を診断
利用対象者	中小企業・小規模事業者の経営者、管理者、従業員
特 長	• 設問に答えるだけで自社のセキュリティ対策状況を把握することができる • 診断後は、診断結果に即した推奨資料やツールが確認できる

概要

「5 分でできる！情報セキュリティ自社診断」は、情報セキュリティ対策のレベルを数値化し、問題点を見つけるためのツールです。
オンライン版では、25 の質問に答えるだけで診断することができ、過去の診断結果や同業他社との比較もできます。また、診断結果に合わせてお薦めする資料、ツールが紹介されるため、今後どのような対策に取り組むべきかを把握することができます。

情報セキュリティ・ポータルサイト「ここからセキュリティ！」

学習 診断 対策

https://www.ipa.go.jp/security/kokokara/

用途・目的	• 情報セキュリティや情報リテラシーに関する情報収集 • 国内の主なレポート、ガイドライン、学習・診断等のツール等の利用
利用対象者	• インターネットの一般利用者（小学生～大人） • 企業の管理者／一般利用者
特 長	情報セキュリティ関連の民間及び公的な団体が公開する無償の資料、情報、ツールを網羅的に掲載。目的別、用途別、役割別に情報を選択し利用が可能

概要

• セキュリティベンダー、公的機関、政府等から発信される注意喚起や、資料・動画・ツール等のコンテンツを網羅的に掲載したポータルサイト
• コンテンツを「被害に遭ったら」「対策する」「教育・学習」「セキュリティチェック」「データ＆レポート」に分類。必要な情報が見つけやすい
• セキュリティレベルを診断するクイズを「小学生」「中高生・ホームユーザ」「社会人」というカテゴリー別に紹介。楽しみながら学べる

サイバーセキュリティ経営ガイドライン実施状況の可視化ツール

診断

https://www.ipa.go.jp/security/economics/checktool.html

用途・目的	セキュリティ対策の実施状況のセルフチェック
利用対象者	主に従業員 300 名以上の企業の CISO 等、サイバーセキュリティ対策の実施責任者
特 長	サイバーセキュリティ経営ガイドラインに準拠したセキュリティ対策の実施状況を成熟度モデルで自己診断し、レーダーチャートで可視化

概要

経営者がサイバーセキュリティ対策を実施する上で責任者となる担当幹部（CISO 等）に指示すべき“重要 10 項目”が、適切に実施されているかどうかを 5 段階の成熟度モデルで自己診断し、その結果をレーダーチャートで可視化するツールです。
診断結果は、経営者への自社のセキュリティ対策の実施状況の説明資料として利用できます。経営者が対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定や適切なセキュリティ投資の検討、投資家等ステークホルダとのコミュニケーション等に役立てることができます。

■提供される主な機能
・重要 10 項目の実施状況の可視化
・診断結果と業種平均との比較
・対策を実施する際の参考事例
・グループ企業同士の診断結果の比較

5 分でできる！情報セキュリティポイント学習

学習

https://security-shien.ipa.go.jp/learning/

用途・目的	自社の情報セキュリティ教育の実施
利用対象者	中小企業の経営者、管理者、従業員等
特 長	• 自社診断の質問を 1 テーマ 5 分で学べる • インストール不要、無料の学習ツール

概要

情報セキュリティについて e-Learning 形式で学習できるツールです。
身近にある職場の日常の 1 コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら適切な対処法を学ぶことができます。
また、利用者登録をしていただくと、学習の中断・再開ができ、これまでの学習進捗状況を表形式で確認することができます。

安心相談窓口だより
https://www.ipa.go.jp/security/anshin/attention/index.html

学習 対策

用途・目的	最新の「ネット詐欺」等の手口を知り被害防止につなげる
利用対象者	スマートフォン、パソコンの一般利用者
特 長	実際に相談窓口に寄せられる、よくある相談内容に関して「手口」と「被害にあった場合の対処」「被害にあわないための対策」を学べる

概要

IPA 情報セキュリティ安心相談窓口では、寄せられる相談に関して手口を実際に検証し、そこで得られた知見をその後の相談対応にフィードバックするとともに、注意喚起等、情報発信にも活かしています。
「安心相談窓口だより」では中でも多く相談が寄せられる相談内容の「手口」「対処」「対策」について、パソコンやスマートフォンの操作等にあまり詳しくない人でも理解できるように分かりやすく説明を行っています。
記事は不定期に公開されますので、「安心相談窓口だより」を定期的に確認することで、最新のネット詐欺等の手口や対策を知り、被害の未然防止に役立てることができます。
手口に関する内容以外にも、被害にあわないための日ごろから気を付けるポイントについての記事も公開しています。

映像で知る情報セキュリティ　各種映像コンテンツ
https://www.ipa.go.jp/security/videos/list.html

学習

用途・目的	動画の視聴により、情報セキュリティの脅威、手口、対策等を学ぶ
利用対象者	スマートフォンやパソコンを使用する一般利用者 組織の経営者、対策実践者、啓発者、従業員等
特 長	組織内の研修等で利用できる10 分前後の動画を公開。情報セキュリティ上の様々な脅威・手口、対策をドラマ等の動画を通じで学べる

概要

「標的型サイバー攻撃」「ワンクリック請求」「偽警告」等の脅威をテーマにした動画のほか、「中小企業向け情報セキュリティ対策」「スマートフォンのセキュリティ」「新入社員向け」といった訴求対象者別の動画を公開しています。動画の視聴により、スマートフォン・パソコンを使用する際に利用者に求められる振舞いや対策を身に付けることができます。
情報セキュリティの自己研さんを目的とした個人の視聴のほか、組織内の研修用としての利用が可能です。

■動画のタイトル例
- 今そこにある脅威　組織を狙うランサムウェア攻撃
- What' s BEC ？～ビジネスメール詐欺 手口と対策～
- 妻からのメッセージ ～テレワークのセキュリティ～
- あなたのパスワードは大丈夫？～インターネットサービスの不正ログイン対策～

索引

さ

た

な

は

ま

ら

わ

著作・製作　独立行政法人情報処理推進機構（IPA）

編集責任　高柳 大輔　小山 明美　涌田 明夫　白石 歩　小川 隆一

執筆者

IPA

和泉 隆平	板垣 寛二	伊藤 彰朗	伊藤 吉史	内海 百葉
大島 尚	大友 更紗	小川 隆一	奥田 美幸	小幡 宗宏
甲斐 成樹	金子 成徳	神谷 健司	亀田 恭史	唐亀 侑久
河合 真吾	神田 雅透	木下 弦	小山 明美	佐川 陽一
佐藤 栄城	柴本 憲一	清水 碩人	白石 歩	菅 大豪
竹内 智子	武智 洋	田島 威史	丹野 菜美	近澤 武
辻 宏郷	中島 健児	中島 尚樹	楢原 龍史	西尾 秀一
西村 奏一	野村 春佳	橋本 徹	長谷川 智香	平尾 謙次
福岡 尊	福原 聡	冨士 愛恵里	古居 敬大	松島 伸彰
松田 琳花	宮本 冬美	森 淳子	安田 進	湯澤 凱貴
横山 美晴	吉野 和博	吉本 賢樹	與那嶺 崇	渡邉 祥樹
藁科 綾子				

株式会社日立製作所　相羽 律子
サイバーセキュリティ国際会議 CODE BLUE　発起人　篠田 佳奈
国立研究開発法人情報通信研究機構　中尾 康二
デジタル庁　戦略・組織グループ　セキュリティ危機管理チーム　満塩 尚史
国立研究開発法人情報通信研究機構　横山 輝明
一般社団法人 JPCERT コーディネーションセンター　米澤 詩歩乃
情報規格調査会 JTC 1 ／ SC 27 ／ WG 5 小委員会

協力者

IPA

板橋 博之	伊藤 真一	井上 佳春	江島 将和	小沢 理康
加賀谷 伸一郎	亀山 友彦	菅野 和弥	栗原 史泰	桑名 利幸
小杉 聡志	塩田 英二	柴田 直	白鳥 悦正	高見 穣
高柳 大輔	田口 聡	土屋 正	遠山 真	西原 栄太郎
日向 英俊	前島 肇	前田 祐子	松田 修平	宮崎 卓行
渡辺 貴仁				

国立研究開発法人情報通信研究機構　井上 大介
一般社団法人 JPCERT コーディネーションセンター　江田 佳領子
長崎県立大学　島 成佳
三井物産セキュアディレクション株式会社　増田 聖一
明治大学　湯淺 墾道
経済産業省商務情報政策局サイバーセキュリティ課
経済産業省貿易経済協力局安全保障貿易管理課

おわりに

新型コロナウイルス感染症の拡大防止対策は結果としてテレワークやDXの推進を加速させ、ニューノーマルと呼ばれる大きな変化をもたらしました。そして、2022年2月に勃発したロシアによるウクライナ侵攻では、国同士の武力による衝突に、 サイバー攻撃や情報戦という新しい戦いが重大な要素として含まれるようになりました。2022年後半は生成系AIが話題となり身近なツールとして誰もがAIを利用できるようになりました。こんなに急激で大きな技術、環境の変化は経験したことがありません。本白書のサブタイトルの「進む技術と未知の世界 新時代の脅威に備えよ」には、このような大きな変化に潜む脅威に対しても基本を見失わず、連携して対処しなければならないという思いを込めています。

本白書は多岐にわたるサイバーセキュリティに関する国内外の事象や動向を調査・分析し、分かりやすい解説を心掛け、IPA職員だけでなく外部有識者の協力を得て作成しています。なお、IPAのWebサイトから本白書のPDF版が無料でダウンロードいただけます。 冊子、PDF版ともに、皆さまのサイバーセキュリティ対策の検討・実践の一助となれば幸いです。

編集子

情報セキュリティ白書 2023

進む技術と未知の世界：新時代の脅威に備えよ

2023 年 7 月 25 日　第 1 版発行

企画・著作・制作・発行　**独立行政法人情報処理推進機構（IPA）**

〒 113-6591
東京都文京区本駒込2丁目 28 番8号
文京グリーンコートセンターオフィス 16 階
URL　https://www.ipa.go.jp/
電話　03-5978-7503
E-Mail spd-book@ipa.go.jp

表紙デザイン／本文DTP・編集　**伊藤 千絵、久磨 公治、涌田 明夫、北林 俊平**