情報セキュリティ白書

Information Security White Paper

2024

変革の波にひそむ脅威：リスクを見直し対策を

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2024」の刊行にあたって

「情報セキュリティ白書」は、2008 年以来、サイバーセキュリティ分野における、政策や脅威の動向、インシデントや被害の実態等をまとめ、皆様のセキュリティ対策の推進、学習・研鑽等にお役立ていただくという趣旨で発刊し、産業界、学界、一般の方に広く愛読されてきました。

昨今のサイバー空間の動向を振り返ってみると、新型コロナウイルスのパンデミックは収束し、経済・社会活動の回復とともに、働き方改革、デジタル化が大きく進展し、更には生成 AI の登場により変革の兆しが見えます。他方、2022 年 2 月に始まったロシア・ウクライナ戦争の長期化等、現下の厳しい国際情勢下において、重要インフラの機能停止、国民の情報や知的財産の窃取、民主プロセスへの干渉等のサイバー攻撃が顕在化し、サイバー空間が、地政学的緊張を反映した国家間の争いの場の一部ともなってきています。今後 AI の悪用によるサイバー攻撃の激化や高度化も懸念されるところです。

国内では、ランサムウェア被害が引き続き多数発生しています。2023 年 6 月の社会保険労務士向けクラウドサービスが被害を受けた事案や、同年 7 月の港湾コンテナターミナル内のシステム停止をもたらした事案等が発生しました。また、国民情報や知的財産の窃取を目的としたサイバー攻撃も顕在化し、とりわけ、ネットワーク境界の脆弱性を突いた攻撃が多数発生する等、攻撃に一層の巧妙化・高度化が見られます。今後、人手不足解消のための自動化等、デジタルライフラインにおける AI や IoT システムの社会実装が進み、サイバーリスクが、更に増大していくことが予想されます。このようなリスクに対処していくためには、サイバー空間を巡る、変容するリスクを国際的、経済的、地政学的側面から把握・分析し、リスクへの予見性を高めていくこと、そして、サプライチェーンやサイバーやフィジカルが融合した環境を前提として、システムの設計段階から脆弱性を取り除いていく、セキュア・バイ・デザインのアプローチが重要になっています。

各国においては、こうしたサイバー空間を巡る状況変化を踏まえ、セキュリティ対策の見直しが進められています。国内では 2023 年 7 月に政府機関等のサイバーセキュリティ対策のための統一基準群が全面改定、米国でも 2024 年 2 月にサイバーセキュリティフレームワーク（CSF）が 10 年ぶりに大きく改訂され、欧州では 2024 年の期限に向けて各国が NIS 指令及び EU サイバーレジリエンス法案の実装に取り組んでいます。また、AI に関する制度化、ガイドライン等の整備、法制化も進んでいます。2023 年 12 月には G7 において広島 AI プロセス包括的政策枠組みが示されました。我が国でも、AI の安全性に対する国際的な関心の高まりを踏まえ、AI の安全性の評価手法の検討等を行う機関として、2024 年 2 月、IPA に AI セーフティ・インスティテュートを設置しました。

本白書は、2023 年に生じた事柄を中心に、サイバー空間における脅威や技術の動向、それに対応する内外の政策的対応等について、包括的に記載をしています。本白書が多くの方々に利用され、サイバーセキュリティに関わる最新状況の把握と、それに伴う脅威や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。

2024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

2024

情報セキュリティ白書

序章

2023年度の情報セキュリティの概況

2023 年度は、国内では新型コロナウイルス感染症の 5 類移行により、停滞していた社会活動や経済活動に活気が戻ってきた。一方で、コロナ禍を一つの契機として業務のデジタル化が進み、事業の IT 依存度やシステム・サービス障害による影響が大きくなった。

企業・組織等が受けたサイバー攻撃の件数や被害金額は世界的に増加している。特に、国家の関与が疑われるネットワーク貫通型の攻撃は巧妙かつ執拗で、長期かつ広範囲に及ぶこともあるため深刻な被害を与えている。例えば、「Volt Typhoon」と呼ばれる組織による攻撃は 2021 年ごろから継続し、2023 年 5 月、2024 年 2 月には複数の国家のセキュリティ関係機関が連名で注意喚起を行っている。また、利用者が多いシステム・サービスの脆弱性への攻撃も続いている。企業向けファイル転送ソフトウェア MOVEit Transfer の脆弱性を狙った攻撃では、2024 年 3 月の時点で、全世界の 2,768 組織が被害を受けたという。激化するランサムウェア攻撃に対しては、国際協力により摘発や攻撃用ネットワークの破壊も行われている。2024 年 2 月のランサムウェア攻撃グループ「LockBit」の摘発では、約 10 ヵ国の捜査当局が連携した。

2023 年は、生成 AI の利用が急速に進み、悪用や誤用による脅威やリスクが注目され始めた。具体的には選挙等の政治的な宣伝戦、ロシア・ウクライナ戦争やイスラエル・ハマスの武力衝突等において生成 AI による偽・誤情報が拡散しているとの報道が続いた。国内でも偽・誤情報の生成・拡散の事例が確認されている。生成 AI は真実でないコンテンツを簡単に生成できるため、偽・誤情報の拡散に注意することが大切である。

国内では、2023 年 6 月に社会保険労務士向けクラウドサービスの事業者がランサムウェア攻撃を受け、約 1 ヵ月サービスが停止し、約 3,400 ユーザーの大半に影響が出た。2023 年 7 月には、「LockBit」のランサムウェア攻撃により名古屋港のコンテナターミナル内のシステムが 2 日半停止し、コンテナの搬出・搬入作業に大きな影響があった。サイバー攻撃によるシステムやサービスの停止により、物流のような社会インフラにも影響が出ることが再認識された。一方で、国内の個人情報漏えい、紛失事故の発生件数、流出した個人情報数は増加傾向にあり、過去最多となった。2023 年は内部不正による大量の情報漏えいも報告され、大手通信事業者のグループ企業の内部不正では、2 社で合わせて 1,500 万件を超える顧客情報漏えいが報告された。内部不正は組織の社会的信用を損なう恐れがあり、経営課題として対策に取り組む必要がある。

国外のセキュリティ政策としては、2024 年 2 月、米国 NIST がサイバーセキュリティフレームワーク（CSF）2.0 版を公開した。10 年ぶりとなる大きな改訂で、重要インフラにとどまらないすべての組織におけるサイバーセキュリティ対策の枠組みを示すものとして注目されている。また、2023 年 12 月に米国は「SBOM 管理のための推奨事項」を公表した。政府調達において取引先への SBOM 整備の義務化が進められている。欧州では、重要インフラに関し「NIS 指令」及び「EU サイバーレジリエンス法案」の実装を中心に取り組んでいる。EU 加盟国は 2024 年 10 月までに、自国の規定を NIS2 指令に準拠させるよう求められており、準備が進められている。

国内のセキュリティ政策としては「サイバーセキュリティ 2023」に基づき、対策の強化を進めている。2023 年 7 月には政府機関等のサイバーセキュリティ対策のベースラインとなる統一基準群の全面的な改定がされた。また、同時に「重要インフラのサイバーセキュリティに係る安全基準等策定指針」、更に 2024 年 3 月には「重要インフラのサイバーセキュリティに係る行動計画」の改定版を公表し、重要インフラのサイバーセキュリティ確保に向けた取り組みを示した。

2023 年度は AI の利用拡大に伴い、AI の安全性に関する政策面の取り組みも各国で進んだ。米国、英国、日本等において、AI の安全性に取り組む AI セーフティ・インスティテュートが各々設置される等、各国で短期間に法制化やガイドラインの整備、体制強化が進んでいる。日本は、2023 年 5 月に開催された G7 広島サミットにおいて「広島 AI プロセス」を発表し、AI の安全な利用に関する国際ルール作りに貢献している。

2023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
2023 年　4 月	Wi-Fi ルーターで任意のコード実行を可能とする脆弱性が公開され、Mirai の亜種による悪用も観測（3.5.1）	
5 月	自動車メーカー子会社のデータがクラウド環境の設定ミスにより公開されていたことを公表（3.6.2） 国家の支援が疑われる攻撃者グループによるゼロデイ脆弱性を悪用した攻撃の観測を発表（1.2.2）	G7 広島サミットで官民が連携したサイバー攻撃対策を推進（2.1.1、2.2.1） CISA を含む各国の政府機関「Volt Typhoon」に関する合同のサイバーセキュリティ勧告を発表（2.2.2）
6 月	社会保険労務士向けクラウドサービスがランサムウェアによる不正アクセスを受けサービス停止（1.2.1） ファイル転送ソフトウェアに対するゼロデイ攻撃により情報漏えいやランサムウェア被害が発生（1.2.5）	「不正競争防止法等の一部を改正する法律」成立。ビッグデータ等を念頭にした限定提供データと、営業秘密の一体的な情報管理が可能に（2.1.3）
7 月	名古屋港のコンテナターミナルで利用しているシステムがランサムウェア攻撃を受けて停止（1.2.1） 顧客情報約 596 万件の不正持ち出しを大手通信会社が公表（1.2.8） 国家が支援する攻撃者グループによる、ネットワーク貫通型攻撃による不正アクセスを公表（1.2.2）	NISC「サイバーセキュリティ 2023」、「政府機関等のサイバーセキュリティ対策のための統一基準群」改定版、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」改定版公開（2.1.1）
8 月	福島第一原発処理水放出に関する偽・誤情報拡散（4.1.3）	総務省「ICT サイバーセキュリティ総合対策 2023」公表（2.1.4） EU「デジタルサービス法（Digital Services Act）」発効（2.2.3）
9 月	米国フロリダ州の市が、建設業者を装ったビジネスメール詐欺に遭い約 120 万ドルを送金（1.2.3）	警察庁、NISC、米国諸機関は中国を背景とする攻撃グループ「BlackTech」に関する注意喚起を発出（1.2.2、2.1.5）
10 月	元派遣社員による顧客情報約 928 万件の不正持ち出しを大手通信会社グループ企業が公表（1.2.8） イスラエル・ハマス間の武力衝突勃発、フェイク画像拡散（2.2.1、4.1.3）	経済産業省、IPA「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」開催（2.2.1） 米国、AI に関する大統領令 14110 発布（2.2.2）
11 月	生成 AI を使用した岸田首相の偽動画拡散（3.1.2）	英国「AI 安全性サミット（AI Safety Summit）」開催（2.2.1）
12 月	総合 IT 企業、約 94 万件の個人情報を含むファイルが閲覧可能な状態にあったと公表（1.2.8、3.6.2） 国際刑事警察機構、2023 年 7 月から 12 月にかけて 34 ヵ国が参加した国際的な取り締りを主導（1.2.3）	「広島 AI プロセス包括的政策枠組み」G7 首脳承認（2.2.1） EU サイバーレジリエンス法承認（2.2.3） 米国「SBOM 管理のための推奨事項」公表（2.2.2）
2024 年　1 月	能登半島地震が発生、SNS で偽･誤情報拡散（3.1.2、4.1.3） 台湾総統選挙に関連する偽・誤情報拡散（2.2.2、4.1.3） 米国大統領選挙の予備選において、Biden 大統領のディープフェイク音声拡散（4.1.3）	デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」改訂（2.1.2）
2 月	約 10 ヵ国の捜査当局、LockBit テイクダウンを実施（2.1.5、2.2.3）	AISI Japan 設立（4.1.4）。USAISI 設立（2.2.2） 「Volt Typhoon」に関する再度の合同のサイバーセキュリティ勧告を発表（2.2.2） NIST「サイバーセキュリティフレームワーク（CSF）2.0 版」公開（2.2.2）
3 月		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」改定（2.1.1） IoT 製品のセキュリティラベリング最終取りまとめ公表（2.1.3、3.2.1、3.5.5） 欧州議会「AI 法」承認（2.2.3）

※ 2023 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。ランサムウェア被害、標的型攻撃、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や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していただきたい。

第3章
情報セキュリティ対策強化や取り組みの動向

2023 年度は企業の内部不正事案が多く報道され、抑止の難しさが再認識された。本章では、組織・個人向けの情報セキュリティの対策強化策や取り組み、対策状況の実態、各種認証制度、及び暗号技術の動向について解説する。そのほか各国で検討が進んでいる一定のセキュリティ基準を満たす IoT 製品への認証制度、IoT、制御システム、クラウドのセキュリティ動向、国内外のインシデントの発生状況、対策等についても解説する。

3.1 組織・個人に向けた情報セキュリティ対策の普及活動

組織や個人に向けた情報セキュリティ対策の普及活動について述べる。

3.1.1 組織における情報セキュリティの取り組みと支援策

組織における情報セキュリティの実態と対策状況、及び組織に向けた情報セキュリティ支援策と支援ツールについて述べる。

(1) 組織の情報セキュリティの実態と対策状況

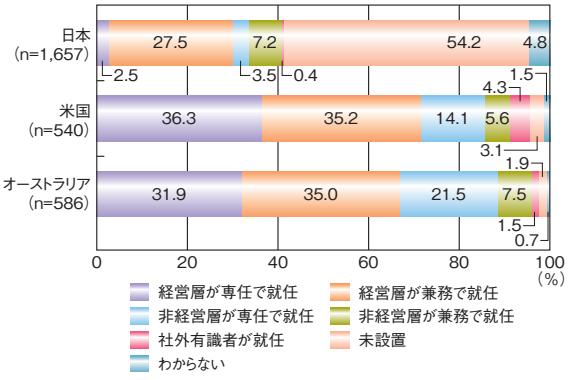
企業のセキュリティ対策・統制状況について、企業や IPA が行った実態調査に基づいて述べる。

(a) セキュリティ管理体制の構築状況

最高情報セキュリティ責任者(CISO:Chief Information Security Officer)は、経営層とセキュリティ担当者をつなぎ、有効なセキュリティ対策の立案から実践に至るまでの責任を負う存在である。NRI セキュアテクノロジーズ株式会社(以下、NRI セキュア社)の「NRI Secure Insight 2023[※1]」(日本 1,657 社、米国 540 社、オーストラリア 586 社の企業を対象に調査。以下、NRI セキュア社調査)によると、CISO を設置している企業の割合(図 3-1-1 において「経営層が専任で就任」「経営層が兼務で就任」「非経営層が専任で就任」「非経営層が兼務で就任」「社外有識者が就任」のいずれか)は、米国・オーストラリアともに 95% 以上であるのに対し、日本は 41.1% にとどまっている。

また、CISO が専任で就任している企業の割合(図 3-1-1 の「経営層が専任で就任」と「非経営層が専任で就任」の合計)は、米国・オーストラリアともに 50% 以上であるのに対し、日本は 6.0% である。「社外有識者が就任」の割合についても米国が 4.3% であるのに対して、オーストラリアが 1.5%、日本が 0.4% と差がついている。

NRI セキュア社調査では、CISO はセキュリティ対策の実施に不可欠であるため、CISO の役割を果たすチームを編成し対応することも考えられるとしている。

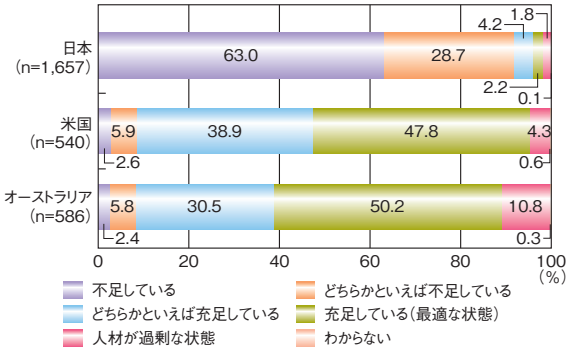


■図 3-1-1　CISO を設置している企業の割合
(出典)NRI セキュア社「NRI Secure Insight 2023」を基に IPA が編集

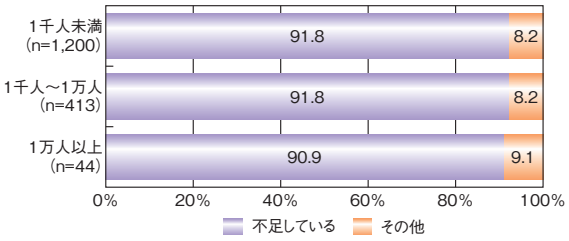
(b) セキュリティ人材の充足状況

NRI セキュア社調査によると、セキュリティ人材が不足している企業の割合は、米国の 8.5%、オーストラリアの 8.2% に対し、日本は 91.7% である(次ページ図 3-1-2)。また、日本企業を従業員数別に見ると、セキュリティ人材が不足している割合は、どの従業員規模でも 90% を超えている(次ページ図 3-1-3)。このことから、日本企業におけるセキュリティ人材不足は、企業規模によらない共通の課題となっているという。

IPA が SECURITY ACTION 宣言事業者(主に中小企業である事業者)を対象に実施した調査[※2]においても、情報セキュリティ対策を進める上での問題点をた



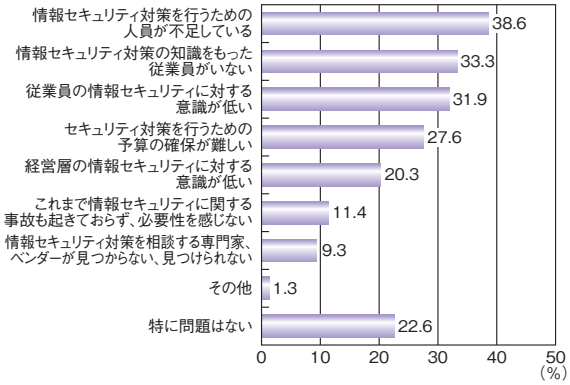
■図 3-1-2　セキュリティ対策に従事する人材の充足状況
(出典)NRI セキュア社「NRI Secure Insight 2023」を基に IPA が編集



※不足している:図3-1-2で「不足している」「どちらかといえば不足している」のいずれかを回答

■図 3-1-3　日本企業の従業員数別セキュリティ人材充足状況
(出典)NRI セキュア社「NRI Secure Insight 2023」を基に IPA が編集

ずねたところ、「情報セキュリティ対策を行うための人員が不足している」と回答した割合が 38.6% と最も高く、次いで「情報セキュリティ対策の知識をもった従業員がいない」が 33.3% であった(図 3-1-4)。



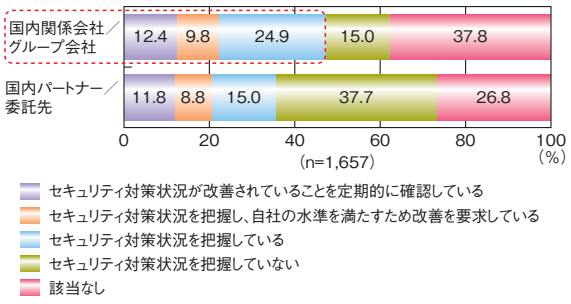
■図 3-1-4　情報セキュリティ対策を進める上での問題点(複数回答、n=5,577)
(出典)IPA「2023 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実施調査」を基に編集

セキュリティ人材の確保・育成については、「サイバーセキュリティ経営ガイドライン※3」(以下、経営ガイドライン)の付録である「サイバーセキュリティ体制構築・人材確保の手引き 第 2.0 版※4」を参照していただきたい。

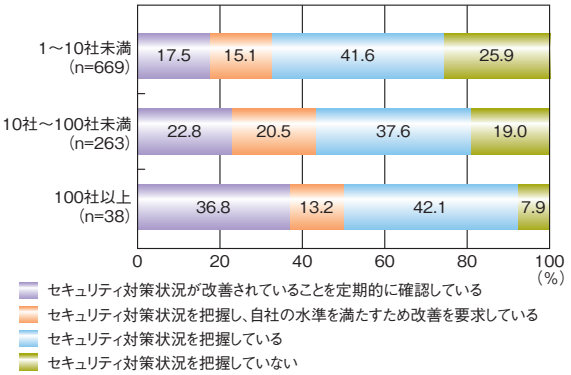
(c) サプライチェーンのセキュリティ対策把握状況

NRI セキュア社調査による、日本企業のサプライチェーン統制状況を図 3-1-5 に示す。国内関係会社／グループ会社に対するセキュリティ対策状況の把握率(図 3-1-5 の赤色の点線部分)は 47.1%、未把握率(「セキュリティ対策状況を把握していない」と回答した割合)は 15.0% となっている。一方、国内パートナー／委託先のセキュリティ対策状況の未把握率は 37.7% であり、これは国内関係会社／グループ会社の未把握率と比較して 22.7% 高い値である。この要因としては、委託先管理においての対象数の多さや、対策状況を把握するための手続きが複雑であり、手間がかかるため実施しにくい等が考えられるという。また、委託先は外部組織であるため、国内関係会社／グループ会社と比較して統制が容易ではない点や、委託元としてセキュリティ対策状況を把握した後の改善活動の促進が難しい点等も、要因として考えられるという。

把握率について、グループ会社数別に見ると、グループ会社数が多い程、把握率が高くなっている(図 3-1-6)。海外等を含めて多くのグループ会社を持つ企業は、攻撃対象領域(アタックサーフェス)が広がっていることから、サプライチェーンリスクへの意識が高いことがうかが



■図 3-1-5　日本企業のサプライチェーンの統制状況(n=1,657)
(出典)NRI セキュア社「NRI Secure Insight 2023」を基に IPA が編集



■図 3-1-6　グループ会社数別の国内関係会社／グループ会社の統制状況
(出典)NRI セキュア社「NRI Secure Insight 2023」を基に IPA が編集

えるという。

日本のサプライチェーンセキュリティ対策の強化については、官民連携で取り組みの検討や推進を行っている（「3.1.1 (2) 組織に向けた情報セキュリティ支援策と支援ツール」参照）。これらの取り組みにより、日本のサプライチェーン全体のセキュリティ対策強化が期待される。

(d) 情報セキュリティの技術的対策状況

NRI セキュア社調査によると、日本企業が EDR（Endpoint Detection and Response）を導入済みである割合は 27.8% であり、2022 年の 18.9%※5 から大きく上昇した。背景としては、サイバー攻撃の増加や新しい働き方の浸透等に要因があるという。

社内ネットワークのトラフィックを可視化する NDR（Network Detection and Response）を導入済みである割合は、11.9% と EDR に次いで高い割合となった。また、NDR の導入について検討中・関心があると回答した割合は 32.0% と最も高かった。これは、リモートデスクトップや VPN 機器を経由した攻撃への対応が要因として考えられるという。

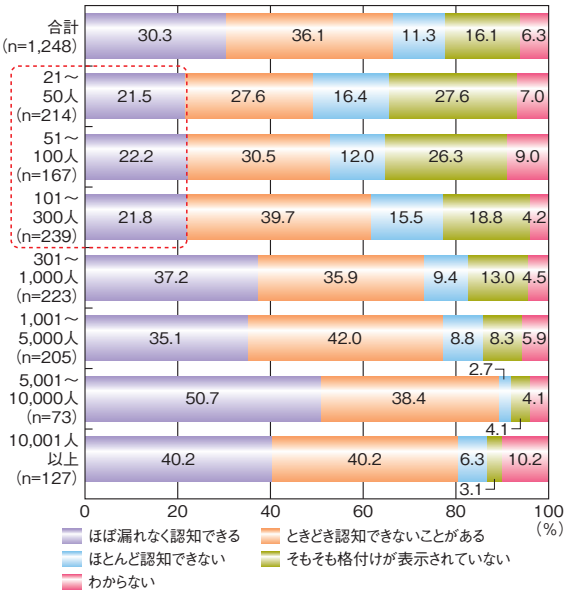
日本企業が EDR や NDR を包括するサービスである XDR（Extended Detection and Response）を導入済みである割合は 6.5% にとどまったが、EDR の運用負荷の高まりに対応するため、XDR を導入する企業も今後増加していくと考えられるという。

(e) 中小企業等の内部不正防止対策状況

IPA が 2023 年度に実施した「内部不正防止対策・体制整備等に関する中小企業等の状況調査※6」（国内企業に所属し、情報セキュリティ・リスク管理・経営等に関与する 1,248 名へのアンケート調査、国内企業 8 社と有識者 4 名へのインタビュー調査等）に基づき、中小企業等における内部不正防止対策や体制についての状況を述べる。IPA では 2013 年に「組織における内部不正防止ガイドライン※7」を公開し、以後継続的に改訂を行い内部不正防止に関する啓発を行っている。しかしながら、報道されているだけでも内部不正に起因する情報セキュリティインシデントは継続的に発生している。同調査で収集した事例情報から、2020 年 4 月以降に国内で発生し、報道された情報漏えいに関する事例を抽出したところ 257 件が観測され、そのうち故意による内部不正を原因とした情報漏えいが 69 件、不注意・ミスに起因する情報漏えいが 62 件であった。

同調査に先行して 2022 年度に IPA で実施した「企業の内部不正防止体制に関する実態調査※8」でも中小企業等の体制整備が進んでいないことが懸念点として明らかになっていた。2023 年度の同調査においては、現状を改善するための対策の方向性を提示することを目的とし、企業経営者の問題意識や基本方針の策定状況、教育・リテラシーの構築の進捗状況と、対策が進んでいると目される中小企業の好事例等の調査を実施した。以降では、中小企業の現状に関して着目すべきアンケート結果を 2 点挙げる。

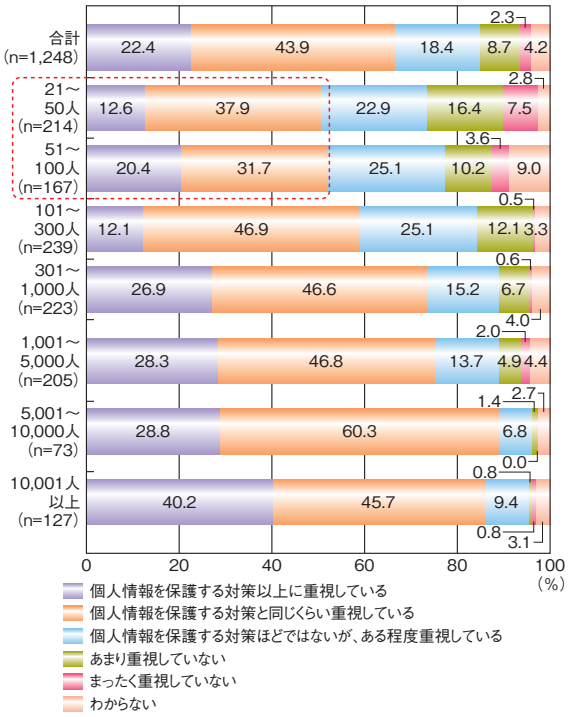
個人情報以外の秘密情報について、格付け表示等によってほぼ漏れなく秘密情報であることを認知できるかどうか尋ねたところ、「ほぼ漏れなく認知できる」と回答した割合は、中小企業では 22% 前後にとどまっていた（図 3-1-7 の赤色の点線部分）。中小企業では秘密情報の格付け表示が実効性を持って実施されている割合が全体平均と比べて低く、従業員が秘密情報か否かを認識できる状況とは言い難いことが見て取れる。まずは個人情報以外の秘密情報の特定を行い、格付けの全社基準に基づくシステム上の分離保管（フォルダで仕分けし、アクセス権限を格付けに合わせて設定）の導入等が現実的な対応であると考えられる。



■図 3-1-7　格付け表示等による秘密情報の周知状況
（出典）IPA「内部不正防止対策・体制整備等に関する中小企業等の状況調査」を基に編集

個人情報保護だけでなく、それ以外の秘密情報（営業秘密、重要なデータ等）を保護する対策を重視しているか尋ねた結果を図 3-1-8（次ページ）に示す。営業秘密等の秘密情報を保護する対策を個人情報と同等以上に重視している割合（「個人情報を保護する対策以上に

重視している」と「個人情報を保護する対策と同じくらい重視している」の合計）は従業員数が小さくなる程、下がる傾向が見て取れた。特に、従業員数が 100 人以下の中小企業では格段に低く、同等以上に重視している中小企業は約半数にとどまっている（図 3-1-8 の赤色の点線部分）。製造業のサプライヤーのように、中小企業であっても技術情報等の営業秘密の重要性が高い企業も多くあると考えられるため、更に全体的な底上げが図られることが望ましい。



■図 3-1-8　秘密情報（営業秘密、重要なデータ等）を保護する対策の重視状況
（出典）IPA「内部不正防止対策・体制整備等に関する中小企業等の状況調査」を基に編集

調査の結果得られた知見を、特に中小企業について改善すべき観点ごとにまとめる。

- 経営課題の改善
  - 経営意識改革途上の企業では、まず内部関係者が主な脅威となる内部不正の防止を経営課題としてとらえ、技術と組織の両面から総合的な対策を行うサイバーセキュリティとの違いを理解した上で、内部不正の防止策を実施すべきである。
  - ISMS 適合性評価制度※9、技術情報管理認証制度※10 等の認証取得、業界全体での取り組み等をきっかけとして、経営者自身が率先して秘密情報管理や内部不正防止の重要性を学ぶことが望ましい。
  - 経営層の意識やリーダーシップが持つ影響力が中小企業では特に大きいことを、経営者自身が強く認識すべきである。
- 重要な秘密の特定と取り扱いの改善
  中小企業の場合は経営者が自ら機動的に重要な秘密を特定し、格付けすることが可能である。ただし、経営層が過負荷にならないように留意が必要である。
- 組織体制・連携に関する課題の改善
  内部不正を所掌するリスク管理の体制を整える必要がある。内部不正を所掌するリスク管理の専門部門がない場合でも、情報システム部門やセキュリティ部門が内部不正対策の IT 技術面をカバーし、総務・人事部門が内部不正対策の組織・人員面をカバーすることで、内部不正防止に特化した体制を作る必要がなくなる。また、5 人程度の幹部で構成する情報管理委員会等を設けている事例があり、小規模で機動的な組織体制の参考にすることができる。
- 社員教育とリテラシー構築に関する課題の改善
  中小規模ならではの実施可能な全社集会等を活用して、経営者が自分の言葉で全従業員に自分の経営方針や、学習し蓄積した知見を直接伝えることが望ましい。
- 対策に関する課題の改善
  サイバーセキュリティ対策でカバーできない内部不正に特化した対策等を既存のサイバーセキュリティ対策に上乗せして措置することが効率的かつ効果的である。これを進めるためには、まず秘密情報漏えいや内部不正の防止には組織に何が必要とされるか、サイバーセキュリティとは分けて認識することが必要である。

以上に留意し、各組織で必要性の高い内部不正対策を把握し、推進することが望まれる。IPA では、こうした内部不正対策に役立つ教育用の動画を 2024 年 3 月に公開している※11。併せて参考にされたい。

(2) 組織に向けた情報セキュリティ支援策と支援ツール

組織に向けた情報セキュリティ支援策と支援ツールについて紹介する。

(a) サプライチェーン・サイバーセキュリティ・コンソーシアム

IPA が公開している「情報セキュリティ 10 大脅威※12」の組織編において「サプライチェーンの弱点を悪用した攻撃」は 6 年連続上位に位置しており、サプライチェー

ン全体で堅固なサイバーセキュリティ対策を実施し、協力体制を築くことが不可欠になっている。そのような取り組みが進む中で、2020年に産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的として、「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3: Supply-Chain Cybersecurity Consortium）※13」が設立され、2023年度もIPAが事務局となり、サプライチェーン全体のサイバーセキュリティ対策強化に向けた取り組みの検討や推進を行った。

SC3においては、総会、運営委員会のもとWG（Working Group）が運営されており、2023年10月の運営委員会では国をまたがるサプライチェーンセキュリティに関する課題や注力すべき分野について議論するために新たに国際WGの設置が決定された。

- 総会
  2023年11月にSC3総会が開かれ、中溝和孝内閣審議官による「最近のサイバー空間の動向を踏まえた取組状況について」と題した基調講演や、一般社団法人日本自動車工業会による取り組み事例の紹介が行われた。当日の決議として、会長・副会長の再任と、2022年に設置されたSC3運営検討準備会の継続が成立した。
- 運営委員会
  新規WG設置の検討や2024年度以降のSC3の在り方や運営方針について議論するための企画・調整室の設置を行った。
- 中小企業対策強化WG
  2022年度の業界ガイドライン共通項抽出事業を踏まえ、2023年度はセキュリティガイドラインが未整備の業界団体に対して、業界ガイドラインの策定支援及び導入の手引き等の作成支援事業を行った。同事業では、セキュリティ専門家が策定支援を行い、この支援をモデルケースになるよう実証し、この実証の結果を業界セキュリティガイドラインの導入手引き等としてまとめた。この導入手引き等は、セキュリティガイドラインが未整備の業界団体で活用されることが期待される。
  2022年度、攻撃動向分析・対策WGでは、少人数の懇談会形式で、経営者のサイバーセキュリティに関する悩み事やニーズを尋ねる取り組みを行ってきた。2023年度は、この取り組みを継承し、商工会議所協力のもと、サイバーセキュリティ懇談会を各地で8回開催し、地域のセキュリティ専門家が「お悩み相談」を行うとともに、その相談の中から中小企業のサイバー攻撃被害事例を収集した。収集した被害事例の中から中小企業のセキュリティ対策の啓発に資する事例を選定し、個別取材を行い、被害事例のコンテンツを作成した。広く経営者に対してサイバーセキュリティ対策の重要性を訴えるため、被害事例のコンテンツをSC3ホームページに掲載している※14。
  また、2024年2月には「やるなら今!業界・地域におけるサイバーセキュリティの取組み」と題して中小企業の経営者及び管理者に対してウェビナーを開催した※15。
- 攻撃動向分析・対策WG
  2023年度は活動を停止しており、中小企業対策強化WGが活動を引き継ぐ形になった。
- 産学官連携WG
  2022年度には産業側と人材育成・教育側の要件にあった別々の基準を組み合わせ、雇用側と教育機関が連携する仕組みを議論し、セキュリティ人材に求められる知識・スキル・能力の定義において参照・活用可能な共通語彙集の試案を作成した。2023年度には共通語彙集の試案を基に、民間企業・教育機関にて評価・検証を行うことでセキュリティ人材に必要なスキル・知識の見える化を試みた。この取り組みを基に、今後、共通語彙集の改良や実務活用を見据えた検討を行い、産学への普及・展開等を図っていく。
- 地域SECUNITY形成促進WG
  2023年度も地域に根付いたセキュリティ・コミュニティの形成促進のため地域SECUNITY形成促進WGを通じて活動を行った。全国に向けたワークショップの開催と中部経済産業局、近畿経済産業局、九州経済産業局と連携した特定地域でのワークショップを開催し、地域間の情報共有を促進するとともに、共通課題の解決に向けた取り組みを検討・推進した。
- 国際WG
  サプライチェーンが日本国内にとどまらず国際的に展開していることから、海外企業も含めたサプライチェーンセキュリティの向上を図るための議論の場として2023年10月に新たに設置された。
  国をまたがるサプライチェーンセキュリティに関する課題や注力すべき分野をSC3会員からのインプットも踏まえて整理し、成果についてはSC3会員に対して情報発信を行い、問題意識や共通課題、対処法等を共有していく。

(b) サイバーセキュリティお助け隊サービス制度

IPA では中小企業等を狙ったサイバー攻撃への対処として不可欠なサービスを効果的かつ安価に、確実に提供することをコンセプトとして 2021 年度より「サイバーセキュリティお助け隊サービス制度※16」を運営している。サービス要件として相談窓口、異常の監視、緊急時の対応支援、簡易サイバー保険等の各種サービスをワンパッケージで安価に提供する「サイバーセキュリティお助け隊サービス基準」を満たした民間のセキュリティ事業者のサービスを「サイバーセキュリティお助け隊サービス」として登録しており、2024 年 4 月 1 日時点で 40 事業者、57 サービスが登録されている。セキュリティ対策推進枠等の IT 導入補助金を申請することが可能なため、中小企業・小規模事業者にとって利用しやすいサービスとなっている。

2023 年度はお助け隊サービスの提供にあたり、サービス内容の拡充をした「お助け隊サービス 2 類」（以下、2 類サービス）の基準※17 を公開した。2 類サービスは価格が制約条件となり十分にサービスを提供できないという提供事業者からの意見を基に価格要件を緩和したものであり、現行のお助け隊サービスのコンセプトは維持しながら、現行サービスをベースに監視機能の強化や定期的なコンサルティングの実施等の拡充、及び重大サイバー攻撃に関する情報の IPA への共有等を要件として、サービス基準の改定を実施した。個々のお助け隊サービス提供事業者から共有された重大サイバー攻撃に関する情報は、IPA 内で集約・分析等を行い、他のお助け隊サービス提供事業者へ情報共有することで、中小企業における効果的な被害拡大防止等が期待される。改定された基準に沿った 2 類サービスの適合性審査の受付を 2024 年度中に開始予定である。

(c) SECURITY ACTION

「SECURITY ACTION※18」は IPA が運用している中小企業が自発的に情報セキュリティ対策に取り組むことを自己宣言する制度であり、2024 年 3 月末時点では宣言数が 33 万件を超えている。「中小企業の情報セキュリティ対策ガイドライン※19」の実践をベースとして 2 段階の取り組み目標を用意しており、同制度で宣言を行うと、取り組み目標に応じて「★」（一つ星）と「★★」（二つ星）のロゴマークを利用できるようになる（図 3-1-9）。

自己宣言をすることが、経済産業省が実施する IT 導入補助金や事業再構築補助金（サプライチェーン強靭化枠）等の申請要件となっているほか、省庁のみならず都道府県等においても補助金や助成金の申請要件として活用されている。

■図 3-1-9 「SECURITY ACTION」ロゴマーク

IPA は、SECURITY ACTION 宣言事業者に対する施策の優先度を判断し、より有効性の高い活動につなげるために 2018 年度以来 5 年ぶりとなる「SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査」を実施し、2024 年 4 月に調査報告書※20 を公開した。同調査では、SECURITY ACTION を宣言した事業者の継続的な情報セキュリティ対策に対する意識の向上やセキュリティ対策を進める上での問題点や制度上の課題を取りまとめており、SECURITY ACTION 制度を運用していく上で、実効性の向上に資することが期待される。

(d) 経営者向けインシデント対応机上演習・リスク分析ワークショップ

近年のサイバー攻撃によって、企業は事業規模や業種を問わず脅威に晒されている。IPA では地域のセキュリティ・コミュニティや中小企業に対してセキュリティに関するセミナー開催支援を行っているが、2023 年度は中小企業の経営者層や IT 担当者、セキュリティ担当者を対象にセキュリティの意識向上、対策の促進を図るための机上演習及びワークショップを開催した。

「経営者向けインシデント対応机上演習※21」は中小企業の経営層を対象に、セキュリティインシデントが発生した場合を想定し、「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の付録 8「中小企業のためのセキュリティインシデント対応の手引き※22」（次ページ図 3-1-10）を参考に、インシデント対応の基本ステップ（検知・初動対応、報告・公表、復旧・再発防止）の一連の流れを体験するものであり、2023 年度は全国で 10 回開催した。経営者は自社でセキュリティインシデントが発生した場合、被害とその影響を最小限に抑えて事業継続を確保する必要がある。同演習を通じて、サイバー攻撃によるセキュリティインシデントについて経営者が適切に対応するため

■図 3-1-10　中小企業のためのセキュリティインシデント対応の手引き

のポイントや事前の備えを学ぶことにより、平時の具体的な対応手順の整備と、インシデント発生時の的確な対応を行うことが期待できる。

「IT・セキュリティ担当者向けリスク分析ワークショップ※23」では、中小企業の IT・セキュリティ担当者を対象に、自社の情報資産の洗い出し、リスク値の算定、対策の検討といった詳細リスク分析について「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の付録 7「リスク分析シート※24」や「制御システムのセキュリティリスク分析ガイド 第 2 版※25」（図 3-1-11）を用いて演習を行った。2023 年度には全国で 12 回、同ワークショップを開催した。中小企業では、事業内容や取り扱う情報、職場環境、IT 利用状況等によってリスクが異なる。同ワークショップを受講した IT・セキュリティ担当者が、自社に対する詳細なリスク分析を行い、リスクの高い項目を特定し、優先順位付けしたリスク対策計画を立てることで、セキュリティ対策の効率的な実施とセキュリティ水準の向上が見込まれる。

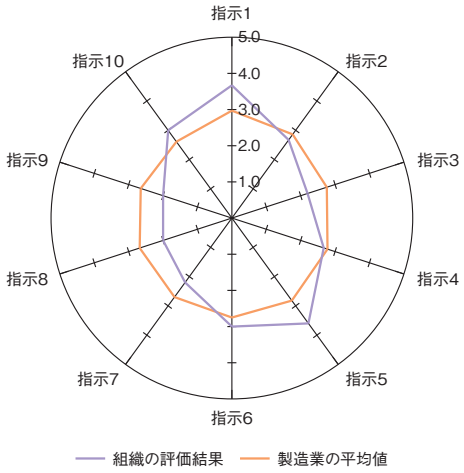
今後、経営者層・IT・セキュリティ担当者向けにセキュリティ対策に資するツールとして、演習で使用した資料を公開予定である。

■図 3-1-11　制御システムのセキュリティリスク分析ガイド

(e) サイバーセキュリティ経営可視化ツール・プラクティス集

IPA は、経営ガイドラインに基づくサイバーセキュリティ対策の実践状況を可視化する「サイバーセキュリティ経営可視化ツール※26」（以下、可視化ツール）と、経営ガイドラインを事例集として補完する「サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集※27」（以下、プラクティス集）を提供している。

可視化ツールは、経営ガイドラインに掲載されている、経営者が CISO 等に対し指示すべきサイバーセキュリティ経営の「重要 10 項目」（指示 1 ～ 10）の実践状況を自己評価し、その結果をレーダーチャートで表示する（図 3-1-12）。評価は、成熟度モデルに基づく 5 段階（最高レベル 5 に 5 ポイント、最低レベル 1 に 1 ポイント）によって行う（表 3-1-1）。また同業種の平均値との比較等も可



指示1:サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示2:サイバーセキュリティリスク管理体制の構築
指示3:サイバーセキュリティ対策のための資源（予算、人材等）確保
指示4:サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示5:サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示6:PDCAサイクルによるサイバーセキュリティ対策の継続的改善
指示7:インシデント発生時の緊急対応体制の整備
指示8:インシデントによる被害に備えた事業継続・復旧体制の整備
指示9:ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
指示10:サイバーセキュリティに関する情報の収集、共有及び開示の促進

■図 3-1-12　重要 10 項目の実践状況のレーダーチャート表示例

成熟度	定義
レベル 1	実施していない又は部分的である
レベル 2	一部で実施されている
レベル 3	全体で実施されている
レベル 4	定期的に実施内容が評価されている
レベル 5	継続的に実施内容が改善されている

■表 3-1-1　成熟度モデルによるレベル定義

能であり、サイバーセキュリティ体制の更なる強化につなげることが期待できる。

プラクティス集には、経営ガイドラインの「重要 10 項目」実践時に参考となる考え方やヒント、実施手順や実施事例が記載されている（表 3-1-2）。プラクティス集におけるリスクマネジメントの実践事例は、企業が自社のセキュリティ課題について対策を行う上で、有用な情報である。

2023 年 12 月 22 日に開催された「第 26 回コラボレーション・プラットフォーム」では、サイバーセキュリティ経営の普及啓発を目的に、可視化ツールを体験してもらう対面形式のワークショップを開催した（「2.1.3 (1) (c) WG3（サイバーセキュリティビジネス化）」参照）。

受講者は個人ワークにて実際に可視化ツールを用い、自社の現状の問題点の把握と解決策の策定を行った。その後グループに分かれて、ツールの使い方や自社の課題・解決策の策定等について意見交換し、その成果について班ごとに発表することで可視化ツールへの理解を深めた。

(f) セキュリティ対応組織の教科書

日本セキュリティオペレーション事業者協議会（ISOG-J：Information Security Operation providers Group Japan）では、企業において一般的にセキュリティ対応を行う SOC（Security Operation Center）や CSIRT（Computer Security Incident Response Team）等の組織において求められる共通的なカテゴリーやサービスを包括的に記載し、効果的な組み合わせや幅広い知見をまとめることにより、経営者から現場担当者まで、幅広く活用可能な「セキュリティ対応組織（SOC/CSIRT）の教科書[※28]」を作成している。

同教科書ではセキュリティ対応組織の構築、運用について持つべきセキュリティ機能が分類されているほか、行うべき対応の優先度が記載されており、2023 年 10 月に第 3.1 版が公開された。

第 3.1 版ではより理解しやすいよう表現の変更や図や補足説明を追加し、付録として「サービスポートフォリオシート」が追加された。同付録を活用することにより不足しているサービスや既存サービスのレベルを体系的に把握し、現状評価を行い、その結果を基に、セキュリティ対応における運用の改善を効果的に実施することができるようになる。

(g) セキュリティ対策ソリューションガイド

特定非営利活動法人日本ネットワークセキュリティ協会（JNSA:Japan Network Security Association）[※29]は、2024 年 2 月に、「インシデント損害額調査レポート 第 2 版[※30]」を公表した。同レポートでは、2017 年 1 月から

	実践のプラクティス
1	1-1. 経営者がサイバーセキュリティリスクを認識するための、他社被害事例の報告 1-2. 最新の脅威によるリスクに対応するための、セキュリティポリシーの改訂・共同管理 1-3. 海外拠点における情報保護に関するコンプライアンスを拠点別チェックリストで担保
2	2-1. サイバーセキュリティリスクに対応するための、兼任のサイバーセキュリティ管理体制の構築
3	3-1. サイバーセキュリティ対策のための、予算の確保 3-2. 経営層やスタッフ部門等の役割に応じた、リテラシーにとどまらないセキュリティ教育実践 NEW 3-3. サイバーセキュリティ対策のための、必要なサイバーセキュリティ人材の定義・育成
4	4-1. 経営への重要度や脅威の可能性を踏まえたサイバーセキュリティリスクの把握と対応 4-2.『サイバーセキュリティ経営可視化ツール』を用いたリスク対策状況の把握と報告 NEW
5	5-1. 多層防御の実施 5-2. サイバーセキュリティ対策において委託すべき範囲の明確化とその管理 NEW 5-3. IT サービスの委託におけるセキュリティ対策を契約と第三者検証で担保 NEW 5-4. セキュリティバイデザインを標準とする、クラウドベースの開発プロセスの励行 5-5. 事業部門による DX 推進をセキュリティ確保の観点から支える仕組みづくり NEW 5-6. アクセスログの取得
6	6-1. PDCA サイクルの検証と、演習・訓練を通じた評価・改善プロセスの強化 6-2. 一律のルール適用が困難なビジネスにおけるセキュリティ KPI を用いたリスク管理 6-3. ステークホルダーの信頼を高めるための、サイバーセキュリティ関連情報発信の工夫
7	7-1. 司令塔としての CSIRT の設置 7-2. 従業員の初動対応の規定 7-3. 想定されるインシデントについてのセキュリティ分析計画の事前策定 7-4. CSIRT 業務の属人化回避も兼ねたインシデントや脅威に関する情報の共有・蓄積 NEW 7-5. 無理なく実践するインシデント対応演習 NEW 7-6. インシデント発生時の優先度に応じた顧客への通知・連絡・公表手順
8	8-1. インシデント対応時の危機対策本部との連携 8-2. 組織内外の連絡先の定期メンテナンス
9	9-1. サイバーセキュリティリスクのある委託先の特定と対策状況の確認 9-2. サプライチェーンで連携する各社が『自社ですべきこと』を実施する体制の構築 NEW
10	10-1. 情報共有活動への参加による信頼獲得と、収集した知見の社内への還元 10-2.『情報の共有・公表ガイダンス』を参考に CSIRT と社内外関係者との連携推進 NEW 10-3. 業界団体を活用したセキュリティ対策に関する情報共有活動

※NEW は、第 4 版で追加されたプラクティス

■表 3-1-2　経営ガイドライン実践のプラクティス
（出典）IPA のプラクティス集

2022 年 6 月までにサイバー攻撃の被害を受けた国内の約 1,300 組織を対象として、インシデントが発生した際の具体的な対応、アウトソーシング先、実際に生じるコスト（損害額・損失額）をまとめた。同レポートによれば、セキュリティ被害を受けたのは大企業が 30%、団体等が 23%、中小企業が 47% であった。また、サイバー攻撃が行われた際の被害金額の平均が、ランサムウェア感染については 2,386 万円、Emotet 感染については 1,030 万円、Web サイトからの情報漏えいについてはクレジットカードの情報漏えいが含まれる場合は 3,843 万円（個人情報のみの漏えいについては 2,955 万円）となっており、金銭的な影響も非常に大きいことが分かった。

そのような中、JNSA は、同法人の会員企業が取り扱うネットワークセキュリティ等に関するサービス、イベント、セミナーを検索できるサービス「JNSA ソリューションガイド※31」を 2023 年 10 月に更新した。同サービスの更新により、導入事例や、課題解決、対応したいトピックから、セキュリティ製品やサービスを調べることができるようになった。特に、トピックについては、IPA が公表している「情報セキュリティ 10 大脅威」の各脅威や「5 分でできる!情報セキュリティ自社診断※32」の診断項目に加えて、中小企業が抱えるサイバーセキュリティ対策の課題解決といった観点から検索することができる等、利用者のニーズや関心に沿って調べることができるようになっている。

3.1.2 情報セキュリティの普及啓発活動

本項では、インターネット利用にまつわる不適切な事例の紹介と、その解決に向けたネットリテラシー向上のための啓発活動について述べる。

(1) 生成 AI に関する啓発活動と注意点

近年、高精度な文章や画像等を生成する AI（生成 AI：Generative Artificial Intelligence）が、急速に発展しており、個人でも生成 AI を簡単に利用できるようになってきている。その反面、生成 AI を利用した虚偽情報が拡散される危険性や、インターネット上に公開された情報を生成 AI が学習することで、新たに生成された画像やイラスト等が、著作権を侵害する恐れも指摘されている。

また、生成 AI に入力した情報がその生成 AI の学習に使われる可能性もあり、その情報が他の利用者への回答内容に使われる情報漏えい等のセキュリティ面でのリスクも考えられる※33。

(a) 生成 AI に関する啓発活動

2023 年 11 月ごろ、岸田文雄首相の偽動画がインターネット上で拡散し話題となった※34。この偽動画も生成 AI を使用して作成されていた。

個人情報保護委員会では、2023 年 6 月に「生成 AI サービスの利用に関する注意喚起等について※35」を発出し、一般の利用者が生成 AI を利用する際の留意点として、①入力した個人情報等が他の情報と結び付けられ、正確または不正確な内容で出力されるリスクの認識、②出力される応答結果に不正確な内容の個人情報が含まれるリスクの認識、③サービスの利用規約やプライバシーポリシーについて十分な確認を行うことが挙げられている。

文部科学省は、教育場面での生成 AI 活用の適否を判断する際のガイドライン※36 を公開し、生成 AI が生成する回答を鵜呑みにせず、「あくまでも参考の一つ」として、「自分で判断する」ことが必要だとしている。

なお、生成 AI については「4.2 AI のセキュリティ」も参照いただきたい。

(b) 今後の生成 AI 利用上の注意点

生成 AI が個人でも容易に利用できるようになり、様々な情報を収集、整理したり、文章や画像等のコンテンツをより効率的に制作したりすることができるようになっている一方で、生成 AI によって利用者の個人情報が本人の意図に関係なく学習されたり、生成された情報の正確性を利用者が確かめることなく発信したりするリスクが高まってきている。利用者としては、自分自身のプライバシーが漏えいしたり、他人のプライバシーを侵害しないよう配慮してデータを入力し、出力された回答も正確であるかどうか確認する等して、生成 AI を適切に利用していくことが重要である。

また、生成 AI から出力された情報を正しい方法で活用していくことも重要になる。本項でもインターネット上の真偽不明な情報について言及しているが、真偽不明な情報には、生成 AI から出力された画像・動画が組み合わされた、真偽を判断することが難しい虚偽情報が含まれる可能性がある。世間にあふれる情報について、真実性があるのか、事実に基づいたものかを注意して判断した上で、受容する必要性がますます高まってきている。そして、真偽不明な情報を不用意に転載・転送したり、アップロードすることがないように注意しなければならない。

生成 AI サービスを始めとして、IT 技術は日々高度

化が進み、処理できる情報量も増加を続け、それに応じてITの利便性はますます高まってきている。そのような中で、私達は、情報にまどわされて適正な判断ができなくなることのないよう、AI等の新しい技術にも対応したネットリテラシーを身に付けていくことが重要である。

(2) インターネット上の真偽不明な情報に関する啓発活動

インターネット上には真偽が不確かな情報も少なからず存在する。2024年1月に能登半島地震が発生した際、SNS上で実在しない地名を挙げて救助を求める投稿や、東日本大震災の津波の動画を加工したと見られる映像を、今回の地震による津波のように紹介する投稿が相次いだ。これらの虚偽情報の投稿が第三者によって拡散されたことにより、救助活動が妨げられる事態も発生した※37。

2022年にロシアがウクライナに軍事侵攻を開始した際にも、「ウクライナのゼレンスキー大統領は国外に逃亡した」という虚偽情報が発信・拡散された。首都キーウが陥落寸前だと印象付け、ウクライナの兵士や国民におけるロシアへの抵抗の意志をくじく狙いであったと見られる※38。

日本ファクトチェックセンターでは2023年に公開したフェイクニュース（誤情報・虚偽情報）の検証記事や動画のうち、社会に対する影響が大きく、注目を集めたものを「2023年10大フェイクニュース」として2023年12月に公表している※39。

総務省は、メディア情報リテラシー向上施策の現状と課題等に関する調査を実施するとともに、偽・誤情報に関する啓発教育教材等を公開し、その中で「情報の真偽が分からない場合は拡散しないことが重要」としている※40。

なお、虚偽情報の拡散については「4.1 虚偽を含む情報拡散の脅威と対策の動向」も参照いただきたい。

(3) 闇バイト防止のための啓発活動

近年、SNS上でいわゆる闇バイトの募集が行われていることが問題となっている。2023年6月に、広域強盗事件で「ルフィ」と名乗っていた指示役が逮捕され話題となった。この事件では、強盗の実行役を募集する際にSNSを使用していたとされている※41。

警察庁では、2023年1月から7月末までに特殊詐欺で検挙した被疑者を対象に受け子等になった経緯を集計したところ「SNSから応募」が46.9%と最も高い割合を占めていることが分かった※42。

闇バイトに応募し、一度個人情報を提供してしまうと、途中で辞めたくなっても個人情報をもとに脅迫されるため、逮捕されるまで辞められない。このように実行役をSNS上で集め、捨て駒として利用していたとされている。

警視庁は、このような状況を背景に、闇バイト防止啓発動画を公開し、「闇バイトに応募してしまうと、詐欺の受け子や出し子、強盗の実行犯等、犯罪組織の手先として利用され、犯罪者となってしまう」と注意を呼びかけている（図3-1-13）。動画は「警視庁公式チャンネル※43」で視聴できる。

■図3-1-13　闇バイト防止啓発動画
（出典）警視庁公式チャンネル「闇バイトは犯罪です※44」

また、富山県警察は、「富山県警察公式チャンネル※45」で、闇バイトの危険性をドラマ形式で説明した「注意喚起動画『STOP 闇バイト・裏バイト』※46」を公開した。ほかに、福岡県警察※47や奈良県警察※48等でも動画を公開し、注意を喚起している。

(4) 迷惑動画に関する啓発活動

迷惑行為を撮影した動画がSNSで拡散され、問題となっている。回転寿司店内でしょうゆさしに直接、口をつけたように見える動画を撮影し、SNS上に投稿した者は、威力業務妨害等の罪に問われ、執行猶予付きの有罪判決を言い渡された※49。

情報をインターネットで一度公開してしまうと、消すことは困難になり、その結果、「デジタルタトゥー」としてネット上に残り続けることとなる。迷惑動画を見て転載したり、投稿者の身元を特定したりする行為も、その内容しだいでは罪に問われる可能性があるため、注意が必要である※50。

文部科学省は、不適切な写真をSNSに投稿することの問題点と、そのことにより社会や自分の将来へ及ぼす影響について考えさせることをとおして、インターネット上に情報を発信する際の責任を理解させ、インターネットを

適切に利用しようとする態度を身に付けさせることを目的とした動画教材※51を「文部科学省 /mextchannel※52」で公開している。

IPAが公開している映像コンテンツ「あなたの書き込みは世界中から見られてる −適切なSNS利用の心得−※53」では、インターネットは誰もが広く世界中に情報発信できる反面、いたずら写真や悪口の書き込み等で他人や自分を傷つける道具にもなりかねないことを理解した上でSNSを利用するよう呼びかけている。動画は「IPA Channel※54」で視聴できる。

(5)その他の啓発活動

内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）は毎年2月1日から3月18日を「サイバーセキュリティ月間」と定め、「#サイバーセキュリティは全員参加」というキャッチフレーズのもと、中央省庁のほか、民間企業でも様々な啓発イベントを実施している。2023年度はサイバーセキュリティの最新の事例を基に、経営層が知っておくべきサイバーセキュリティのリスクを紹介する経営層向けセミナーを開催した※55。

また、内閣府大臣官房政府広報室は、「巧妙化するフィッシングから身を守るには※56」を公開し、電子メールやSMS内のリンクは安易にタップせず、携帯電話会社等が提供するセキュリティ設定を活用する等の対策を徹底するよう呼びかけている（手口や対処の詳細については「1.2.6個人を狙うSMS・メールを悪用した手口」参照）。このほか、「サポート詐欺」に巻き込まれる前に手口を知り、警告画面が出てきた場合の対策を紹介した動画「PCやスマホに警告画面が出ても慌てないで!『サポート詐欺』にご注意※57」も公開している（手口や対処の詳細については「1.2.7（1）偽のセキュリティ警告（サポート詐欺）」参照）。

総務省も、Webサイト「上手にネットと付き合おう! 安心・安全なインターネット利用ガイド※58」を運営しており、2023年度は、子供達がデジタル技術の利用を通じて、社会に積極的に参加できることを目指して「家庭で学ぶデジタル・シティズンシップ※59」を公開した。また、「インターネットトラブル事例集2023年版※60」（図3-1-14）をまとめ、インターネット利用上の様々なトラブルと回避策について解説している。

■図3-1-14　インターネットトラブル事例集2023年版
（出典）総務省「悪ふざけなどの不適切な投稿※61」

警視庁は、シニア層を対象とする「スマホ防犯教室※62」を2023年に開催し、スマホを狙った様々な詐欺被害の疑似体験情報の提供や、個別相談会を実施した。「スマホ防犯教室」オンライン講座では、スマホの防犯について、再現ドラマを交え解説した動画で被害に遭わないための対策を紹介している（図3-1-15）。動画は「警視庁公式チャンネル」で視聴できる。

■図3-1-15　スマホ防犯教室
（出典）警視庁公式チャンネル「スマホ防犯教室　オンライン型講座　架空料金請求詐欺編※63」

3.2 製品・サービス認証制度の動向

IPA では情報セキュリティ対策の実現に向けて、国民に向けた情報提供や啓発活動、企業・組織に対するセキュリティ施策の促進とともに、政府機関や独立行政法人等が IT 製品やクラウドサービス等を安全に調達及び利用するために活用できる制度の運営を行っている。

本節では、政府機関等で使用される IT 製品のセキュリティ機能を評価する「IT セキュリティ評価及び認証制度（JISEC）」、政府機関等のシステムに組み込まれる暗号アルゴリズム実装の確認及び暗号モジュールの安全性を試験する「暗号モジュール試験及び認証制度（JCMVP）」、及び政府が求めるセキュリティ要求を満たしているクラウドサービスを評価・登録する「政府情報システムのためのセキュリティ評価制度（ISMAP）」の動向について報告する。

3.2.1 IT セキュリティ評価及び認証制度

サイバーセキュリティ戦略本部が発行している「政府機関等のサイバーセキュリティ対策のための統一基準（令和 5 年度版）[※64]」（以下、政府統一基準）では府省庁及び独立行政法人等が遵守すべき情報セキュリティ対策を定めている。この中では、システムを構成する市販の IT 製品の調達及び運用についてもセキュリティ要件を策定し、確認することを調達者に求めている。

IT 製品がセキュリティ要件を満たすことを確認する仕組みとして、セキュリティ評価制度が欧米諸国を中心に発展し、セキュリティ評価基準が国際規格として策定された。日本でも、このセキュリティ評価基準を用いて IT 製品を評価する「IT セキュリティ評価及び認証制度（JISEC：Japan Information Technology Security Evaluation and Certification Scheme）」を IPA が運営し、政府機関等の IT 製品調達に活用されている。

(1) 政府の IT 製品調達セキュリティ要件

政府統一基準では、府省庁及び独立行政法人等の情報システムセキュリティ責任者に対し、情報システムを構成する IT 製品を調達する場合、経済産業省が発行している「IT 製品の調達におけるセキュリティ要件リスト[※65]」（以下、調達要件リスト）を参照し、想定されるセキュリティ上の脅威に対抗するためのセキュリティ要件を策定することを遵守事項として定めている。調達要件リストには、利用者情報を扱うシステムの基盤となり、攻撃の対象となり得る以下の 11 の製品分野が指定されている。今後も対象製品分野は、拡大される予定である。

- デジタル複合機（MFP）
- ファイアウォール
- 不正侵入検知 / 防止システム（IDS/IPS）
- OS（サーバ OS に限る）
- データベース管理システム（DBMS）
- スマートカード（IC カード）
- 暗号化 USB メモリ
- ルータ／レイヤ 3 スイッチ
- ドライブ全体暗号化システム
- モバイル端末管理システム
- 仮想プライベートネットワーク（VPN）ゲートウェイ

調達要件リストでは、これらの製品分野の IT 製品がセキュリティ要件を満たすことを確認する方法として、国際標準に基づく第三者認証製品を活用する方法と、各組織で個別に確認する方法があることを示している。JISEC は、IT 製品のセキュリティ評価の国際標準である ISO/IEC 15408 に基づく第三者認証制度であり、JISEC で認証されたセキュリティ要件を満たす IT 製品を調達することで、政府統一基準の要求を満たすことができる。

調達要件リストの中でも特に、構築時に受け入れ検査を行う情報システムとは独立して調達されることの多いデジタル複合機の調達、国策としてセキュリティ対策が重要となる旅券やマイナンバーカード等のスマートカードの調達で JISEC の認証制度は活用されている。

(2) 認証制度の国際連携

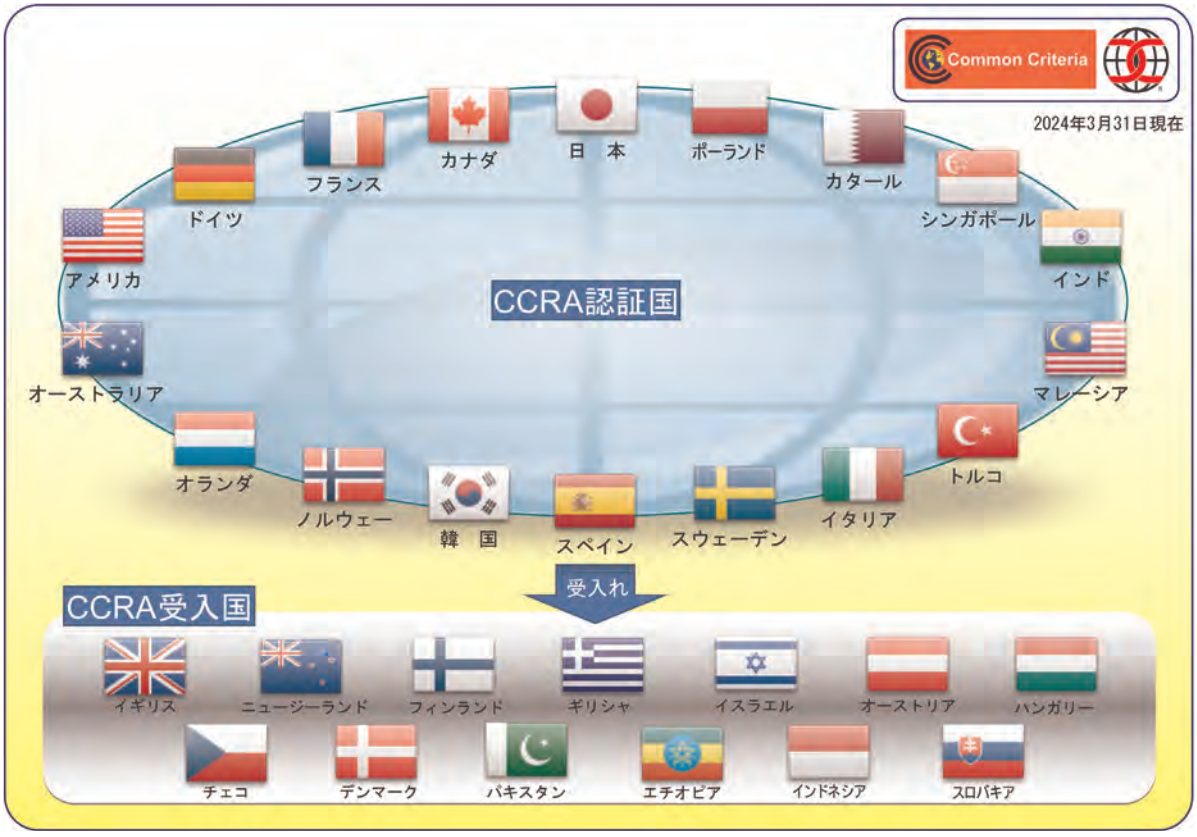
JISEC でも採用しているセキュリティ評価基準である ISO/IEC 15408 は、欧米 6 ヵ国によるコモンクライテリア（共通基準）プロジェクトの成果をベースに開発された。また、同一製品に対し調達国ごとに重複する評価を行うコストを低減するため、これらの国々を代表する公的機関が運営する制度でコモンクライテリアを用いて評価された結果については相互に認め合うという相互承認協定が締結された。その後、相互承認協定には多くの国が加盟して CCRA（Common Criteria Recognition Arrangement）と呼ばれるようになり、JISEC を運営す

る日本も 2003 年に CCRA に加盟している。これにより日本のベンダーは、製品を CCRA 加盟国の調達対象とするために、JISEC を活用することで、日本語の開発資料をそのまま使用して認証を取得することができるようになった。CCRA では、自国で認証制度を運営している「認証国」と、認証制度を有しないが政府調達要件として認証結果を受け入れる「受入国」があり、2024 年 3 月末現在、CCRA 加盟国は認証国 18 ヵ国、受入国 13 ヵ国の計 31 ヵ国に上る（図 3-2-1）。近年は東ヨーロッパやアフリカの国が受入国として加盟、2023 年にはポーランドとカタールが受入国から認証国へ移行している一方、2019 年には英国、2022 年にはニュージーランドが認証国から受入国に移行している。

(3) セキュリティ要件の共通化

コモンクライテリアでは、IT 製品が具備すべきセキュリティ要件を、規定された形式に従って記述する。例えば、アクセス制御機能の要件では、対象となるオブジェクトやサブジェクトのリスト、セキュリティ属性、それらを用いたアクセス方針をコモンクライテリアで規定された形式で記述する。これにより、調達者が必要としている IT 製品のセキュリティ要件仕様を、あいまいさを排除して製品開発者に伝えることを可能とする。このコモンクライテリア形式で表された調達要件仕様書を「プロテクションプロファイル（PP：Protection Profile）」と呼び、CCRA 加盟国での IT 製品の政府調達に利用されている。加盟国の調達部門は、調達する IT 製品のセキュリティ要件をプロテクションプロファイルとして作成し、調達要件として公開している。これらのプロテクションプロファイルのうち汎用的なものは、CCRA のポータルサイト[※66] にも掲載され、他の機関も同様の分野の製品を調達する際に調達要件として指定することができる。日本においても、調達要件リストでは製品分野ごとにこれらのプロテクションプロファイルを指定しており、また、独自の製品を調達する機関は、プロテクションプロファイルを自ら作成し[※67]、調達を実施している。

同じ製品分野の IT 製品調達で、似たような調達仕様が調達者ごとに提示されることは、開発者にとっては負荷となる。そこで CCRA では、加盟国の認証機関が中心となり、いくつかの製品分野で共通的に用いるプロテクションプロファイルの策定を行っている。このプロテクションプロファイルは、「cPP（collaborative Protection Profile）」と呼ばれ、CCRA 加盟国は、該当する製品分野の調達には、この cPP を用いてセキュリティ要件を

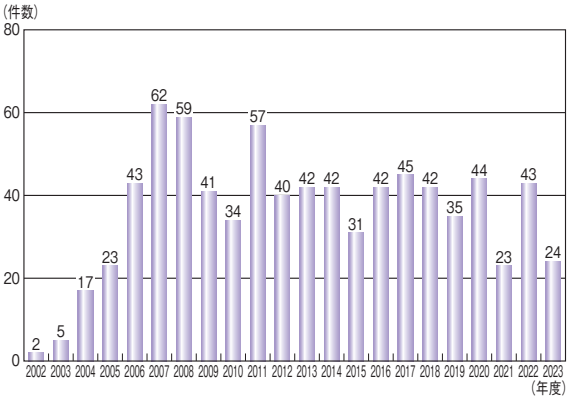


■図 3-2-1　CCRA 加盟国

指定することもある。既にファイアウォール、ドライブ全体暗号化システム、ネットワークデバイス、バイオメトリクス認証、データベース管理システムやデジタル複合機等の製品分野について cPP が策定され、CCRA ポータルサイトで公開されている。

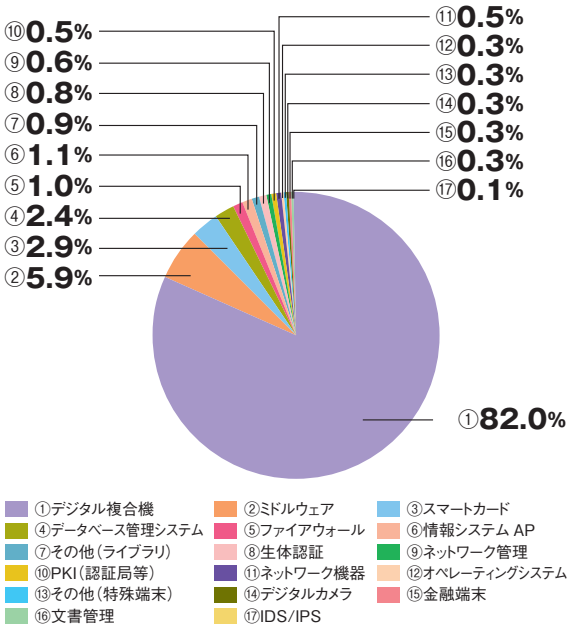
(4) 認証の状況

2023 年度までの JISEC における認証発行件数の推移を図 3-2-2 に示す。認証発行件数は、リーマンショックの影響による 2009 年度の減少と 2011 年度のリバウンド後、毎年 25 ～ 45 件前後で推移している。



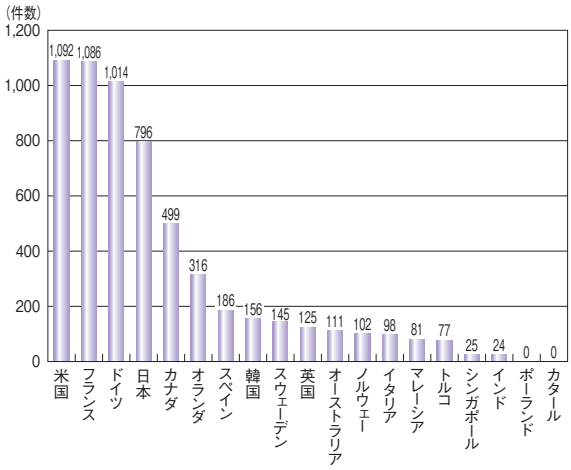
■図 3-2-2　JISEC の認証発行件数の推移

JISEC が認証発行した製品の分野の内訳を図 3-2-3 に示す。認証製品分野としては、デジタル複合機が圧倒的に多い。これは日本のデジタル複合機ベンダーが国際的にも高いシェアを有し、CCRA 加盟国においても政府調達の対象となっているからである。また、それ以外の製品分野の認証が JISEC で少ないのは、セキュリティ製品全般において日本のベンダーの国際的な競争力が弱いこと、ファイアウォールやネットワーク管理製品等はシステム構築の中で組み込まれてテストされ納入されることが多いため、製品単品での調達要件の対象とならないこと等が理由である。JISEC が毎年発行している認証のほとんどはデジタル複合機の新機種リリースによるものである。



■図 3-2-3　JISEC の認証発行の製品分野内訳

CCRA 加盟各国の認証機関が公開している認証発行件数の 2023 年度における累計を図 3-2-4 に示す。日本の認証発行件数は、米国、フランス、ドイツに次いで 4 番目に多い。これら 4 ヵ国は、政府調達に認証製品を活用しているのに加えて、国内に IT 製品の製造ベンダーを多く持つ国々である。英国のように、セキュリティ評価の歴史が長い国でも、国内の製造ベンダーの減少による制度維持コストの削減を理由に認証国から受入国に移行している国もある。韓国では、国際的に大きな市場を持つ製造ベンダーが、製品仕向地によりモバイル製品は米国で、スマートカード関連製品はヨーロッパで認証を取得しているため、国内制度での認証発行件数は少ない。



■図 3-2-4　CCRA 各国の認証件数

(5) 2023 年度のトピック

トピックとして、2023 年度に実施された制度変更や制度運営の検討について紹介する。

(a) CC:2022/CEM:2022 への移行

JISEC でも採用しているセキュリティ評価基準であるコモンクライテリア（ISO/IEC 15408）について、全面的に改訂した新規格（CC:2022/CEM:2022）が 2022 年に発行された。JISEC でも新規格の採用のため、日本語規

格の整備を進め、2023 年 11 月 1 日に CC:2022/CEM:2022 日本語翻訳版を公開※68 し、同日に、CC:2022/CEM:2022 を使用した認証申請の受付も開始された。

旧規格を使用した認証申請については、CCRA の移行ポリシー及び JISEC の規程に従い、新旧規格の並立期間を設定した上で、一部例外を除き、2024 年 5 月に受付を終了している。ただし、JISEC で認証発行の多いデジタル複合機分野のプロテクションプロファイルを含む、厳格な適合を求めるプロテクションプロファイルに適合する製品については、例外的に 2025 年 11 月末まで旧規格での認証申請を受け付ける予定である。

(b) 手続きの電子化推進

JISEC における手続きの電子化を推進するため、以下のとおり関連する規程類の一部を改正し、2023 年 11 月 1 日に施行した※69。

- IPA が発行する認証書及び認証報告書は、電子署名した電子データによる発行とした。申請者がこれまでどおりの書面による発行を希望する場合は、別途申請に応じて対応する。
- IPA と申請者との間で締結する秘密保持契約は、IPA にて導入している電子契約による契約とした。申請者の電子契約による対応が困難な場合は、これまでどおり書面による契約にも対応する。
- 申請者及び評価機関から IPA へ提出する申請書類の提出において、電子署名した電子データによる提出を認め、書面による提出を必須としないことにした。

(c) 認証有効期限の設定及び延長

JISEC において CCRA 文書に準拠することを目的に、認証有効期限の設定及び延長の仕組みの導入をするため、以下のとおり関連する規程類の一部を改正し、2023 年 12 月 15 日に施行した※70。

- 2021 年 9 月 30 日に、認証書の有効期限に関する要求事項が定められている CCRA 文書「認証書の有効性：運用手順 v1.0※71」が発行された。当該 CCRA 文書に基づき、IPA が発行する認証書に有効期限（認証日より 5 年間）の記載を追加した。認証有効期限が満了した認証書は、有効であるとはみなされない。
- 2023 年 3 月 9 日に、保証継続の枠組みを定めた CCRA 文書が更新され、「保証継続：CCRA 要求事項 v3.0※72」が発行された。保証継続とは、「認証済み IT 製品やその環境が変更された場合、適用可能な過去の評価結果を再利用するために、認証維持及び再評定を定義し、以前の評価を承認する枠組み」であり、「認証維持」と「再評定」がある。具体的には、認証維持とは主にアップデートした製品（後継製品）に対して認証を継続するため、「認証済み IT 製品に対する変更があったものの、その変更が初回認証時に評価されたセキュリティ事項への影響が小さいと判断された場合、変更された IT 製品に対して認証を維持する仕組み」である。認証維持の申請期限について、以前は認証日から 2 年後までであったが、認証有効期限の 3 ヵ月前までに変更した。更に、認証書の有効期限の導入に伴い、その有効期限を延長できるようにするため、当該 CCRA 文書に基づき、再評定の仕組みを新たに導入した。再評定とは、「認証済み IT 製品は変更されていないが、当該 IT 製品に対する攻撃に関わる各種状況の変化を評価して、当該 IT 製品が初回に認証されたときと同じレベルの耐性に達しているかを確認すること」である。再評定の仕組みを用いて問題がないと確認されると、認証有効期限を更に 5 年間延長することができる。

(d) JISEC の制度運営の検討

JISEC の制度運営の継続性を高めるため、認証制度の活性化に向けた検討を行った。

その結果、認証取得の目的を以下の四つに整理し、各々の目的に応じた水準での認証を可能とすべく制度改善を図ることとした。

①国の安全保障に資する IT 製品の高度な信頼性確保
②政府調達に必須とされる IT 製品の信頼性確保
③IT 製品の国際競争力強化を視野に入れた認証
④ISO/IEC 15408 による認証よりも低コスト・短期間での取得可能な軽量認証

このうち、①～③については、昨今の国内外の情勢を踏まえ、IT 製品のセキュリティの信頼性確保が重要課題となる中で、認証済み IT 製品の政府調達を推進すべく、政府レベルの関与を強めた認証としても活用できる体制への整備を検討していくこととなった。併せて、認証作業の効率化の検討も行っている。④については、経済産業省が検討していた「IoT 製品に対するセキュリティ適合性評価制度」との統合に向けた検討を進め※73、2024 年 3 月に最終的に取りまとめられた制度構築方針案のパブリックコメントが実施された※74。JISEC と並立した形で、同パブリックコメントの結果を反映した新たな制度が 2024 年度中にスタートする計画である。

3.2.2 暗号モジュール試験及び認証制度

「暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）」とは、利用者が暗号モジュールの信頼性を客観的に把握できるように設けられた第三者認証制度である。

同制度に基づく認証を取得することにより、暗号アルゴリズムが適切に実装され、暗号鍵等の重要情報を適切に保護している暗号モジュールであることをアピールできる。

同制度は、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）とカナダのCCCS（Canadian Centre for Cyber Security）により運営されているCMVP（Cryptographic Module Validation Program）※75と同等の制度であり、IPAが認証機関として運営している※76。本項では、JCMVPの最新動向について述べる。

(1) 政府機関等におけるJCMVPの活用

「政府機関等のサイバーセキュリティ対策のための統一基準（令和5年度版）」における暗号・電子署名の遵守事項（7.1.5節）に対する基本対策事項として、「政府機関等の対策基準策定のためのガイドライン（令和5年度版）※77」（2023年7月4日一部改定版）では「情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。」として、五つの例が挙げられている。その中の一つに、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択することが挙げられている。また、2019年2月に公開された「行政手続におけるオンラインによる本人確認の手法に関するガイドライン※78」において、JCMVPにより認証されたハードウェアトークンに対して当人認証保証の最高レベル3を与えるとされている。

(2) 発行・申請書類の電子化対応

同制度において、従来は紙で発行していた暗号モジュール認証書及び暗号アルゴリズム確認書を電子署名付きの電子データとして発行する運用を2024年4月に試行的に開始している。2024年中に以下を含む電子化対応の本格運用を始める予定である。

従来どおり紙の暗号モジュール認証書及び暗号アルゴリズム確認書を希望する申請者には、有償で対応することで利用者のニーズに柔軟に対応する。

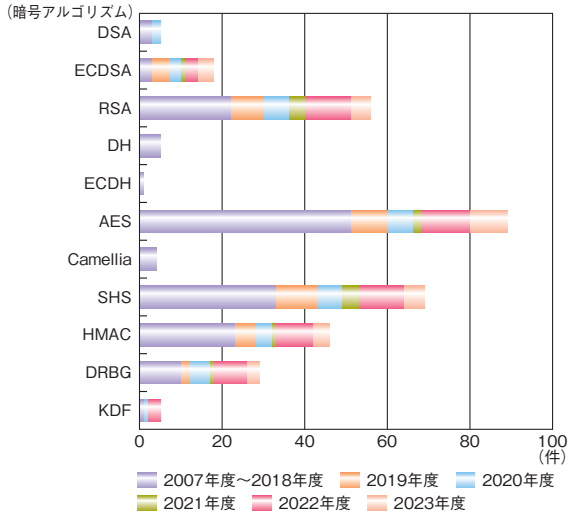
更に、申請者からの書類についても、申請者の組織名義を用いた電子署名が付与された電子データであれば受け付けることで、双方向での電子化を推進している。

これによりペーパーレス化が進み、暗号アルゴリズム確認書に関する発行コスト及び保管コストが削減され、社会のデジタル化に寄与することが期待される。

(3) ITセキュリティ評価及び認証制度（JISEC）との連携

IPAが運営する評価認証制度には、JISECとJCMVPの二つがある。JISECが2016年に発行、2024年3月に改定したガイドライン※79によって、JCMVPの活用方針が示されている（JISECの活動については「3.2.1 ITセキュリティ評価及び認証制度」参照）。

例えば、この活用方針に関連するデジタル複合機のプロテクションプロファイル「Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015※80」では、信頼できるツールを用いた暗号アルゴリズム実装のテストを求めている。JISECでは、このテストにJCMVPの暗号アルゴリズム実装試験ツール（JCATT：Japan Cryptographic Algorithm implementation Testing Tool）を活用して認証を行っている。2023年度は、このプロテクションプロファイルに基づく認証が14件完了している。このような連携を通じて、図3-2-5に示すように、JCATTを使って確認された暗号アルゴリズム実装の実績は順調に伸びている。



■図3-2-5　JCATTにより確認された暗号アルゴリズム実装の実績
（出典）IPAの公開情報を基に作成

3.2.3 政府情報システムのためのセキュリティ評価制度（ISMAP）

2020年6月3日、内閣官房、総務省、経済産業省

は「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：通称、ISMAP（イスマップ））」の開始をアナウンスした※81。本項では、ISMAPの概要や運用等について紹介する。

(1) ISMAPの概要

ISMAPは、政府が求めるセキュリティ要件を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。

従来、政府調達にあたっては、個々のクラウドサービスが実施していると表明する情報セキュリティ対策の実施状況を、調達者が直接確認することが必要であったが、同制度により、この確認を省略でき負担を軽減できる。

(2) ISMAP制度制定と制度改善の経緯

2018年6月に公開された「政府情報システムにおけるクラウドサービスの利用に係る基本方針※82」（2021年3月30日付けでISMAPに関する記述が追記されている）では、「クラウド・バイ・デフォルト原則」が掲げられた。

これを踏まえ、経済産業省と総務省は、2018年8月から「クラウドサービスの安全性評価に関する検討会※83」を発足させ、適切なセキュリティ要件を満たすクラウドサービスを導入するために必要な評価方法等を検討し、2020年1月に「クラウドサービスの安全性評価に関する検討会とりまとめ※84」が公開された。また、同月のサイバーセキュリティ戦略本部会合において「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて※85」が決定された。

上記検討会において、2019年6月から、政府情報システム調達に応募するクラウド事業者が遵守すべきセキュリティ管理基準（ISMAP管理基準）の検討が行われた。ISMAP管理基準は、国際規格をベースに「政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版）※86」「NIST SP800-53 rev.4」を参照して作成された。国際規格としては、情報セキュリティに関してはJIS Q 27001（ISO/IEC 27001）、JIS Q 27002（ISO/IEC 27002）とクラウドサービスの情報セキュリティに関するJIS Q 27017（ISO/IEC 27017）が参考にされた。また、ISMAP管理基準の検討には、これらの国際規格に準拠して編成された「クラウド情報セキュリティ管理基準（平成28年度版）」が参考にされ、そこに含まれるガバナンス基準についてJIS Q 27014（ISO/IEC27014）が参考にされた。

一方、ISMAP制定後も、ISMAPの対象となっている主に「機密性2情報※87」を扱う情報システムのうち、SaaSについては、提供されるサービスが多様であり、用途や機能が極めて限定的なサービスや、「機密性2情報」の中でも比較的重要度が低い情報のみを取り扱うサービス等もある。

このため、ISMAPの枠組みをベースとして、リスクの小さな業務・情報の処理に用いるSaaSを対象にした仕組みである「ISMAP-LIU（ISMAP for Low-Impact Use：イスマップ・エルアイユー）」を新たに設け、2022年11月1日から運用を開始した。これにより、クラウド・バイ・デフォルトの更なる推進と拡大が期待される。

更にISMAP-LIU登録促進のため、2023年5月19日より「ISMAP-LIU登録促進のための特別措置」を開始した（2025年3月末までの約2年間を予定）※88。同措置では、ISMAP-LIUクラウドサービスリストに登録申請を予定し、かつ一定の基準を満たすSaaSサービスは、各政府機関におけるSaaSサービスの調達時に参照される特別措置サービスリスト（一般には非公開）に登録される。特別措置サービスリストに登録されたサービスは、特別措置期間中、ISMAP-LIUクラウドサービスリストへの登録に係る提出物の一部等を免除することが可能になるほか、特別措置期間中の外部監査の対象を一部免除することが可能になる。これによって、ISMAP-LIUの登録を促進するとともに、政府機関等における安全なSaaSサービスの利用拡大を目指す。

また、ISMAPは2020年6月の運用開始から4年が経過し、政府機関等がクラウドサービスを調達する際のセキュリティ・信頼性を評価する制度として定着する一方で、運用を通じた課題も明らかになってきた。これを受けて、ISMAPの信頼性・安定性の保持を前提としつつ、制度運用を合理化・明確化するため、2022年10月より「ISMAP制度改善の取組み」を継続して実施している。2023年10月からは、「外部監査の負担軽減」や「審査の迅速化・効率化」等の諸課題について改善した枠組みによる本格運用が開始された※89。

(3) ISMAPのフロー

同制度においては、政府機関等が調達するクラウドサービスに要求される基本的な情報セキュリティ管理・運用の基準を満たすセキュリティ対策を実施していることが確認されたクラウドサービスが、ISMAPクラウドサービ

スリスト（以下、サービスリスト）に登録される。

また、同制度における監査を実施できる監査機関は、当該監査に求められる要求事項を満たすことが確認された後、同制度が公表するISMAP監査機関リスト（以下、監査機関リスト）に登録される。

同制度のフローを図3-2-6に示す。クラウドサービス事業者は、監査機関リストに登録された機関による監査を受け、ISMAP運用支援機関であるIPAを通じてISMAP運営委員会にサービス登録申請を行う。申請を受けたISMAP運営委員会は審査を行い、承認されたサービスがサービスリストに掲載される。府省庁の調達者はサービスリストを使って調達先候補を選ぶ。

なお、同制度の運用に係る実務及び評価に係る技術的な支援はIPAが行い、そのうち、監査機関の評価及び管理に関する業務については、IPAから特定非営利活動法人日本セキュリティ監査協会（JASA：Japan Information Security Audit Association）に委託している。

(4) ISMAPの運用

同制度は、2020年6月に内閣官房（NISC、情報通信技術（IT）総合戦略室）、総務省、経済産業省の所管で運用が開始され、2024年3月時現在の所管は、NISC、デジタル庁、総務省、経済産業省である。最高意思決定機関としてISMAP運営委員会を設置し、事務局をNISCに置き、運用支援はIPAが担当している。

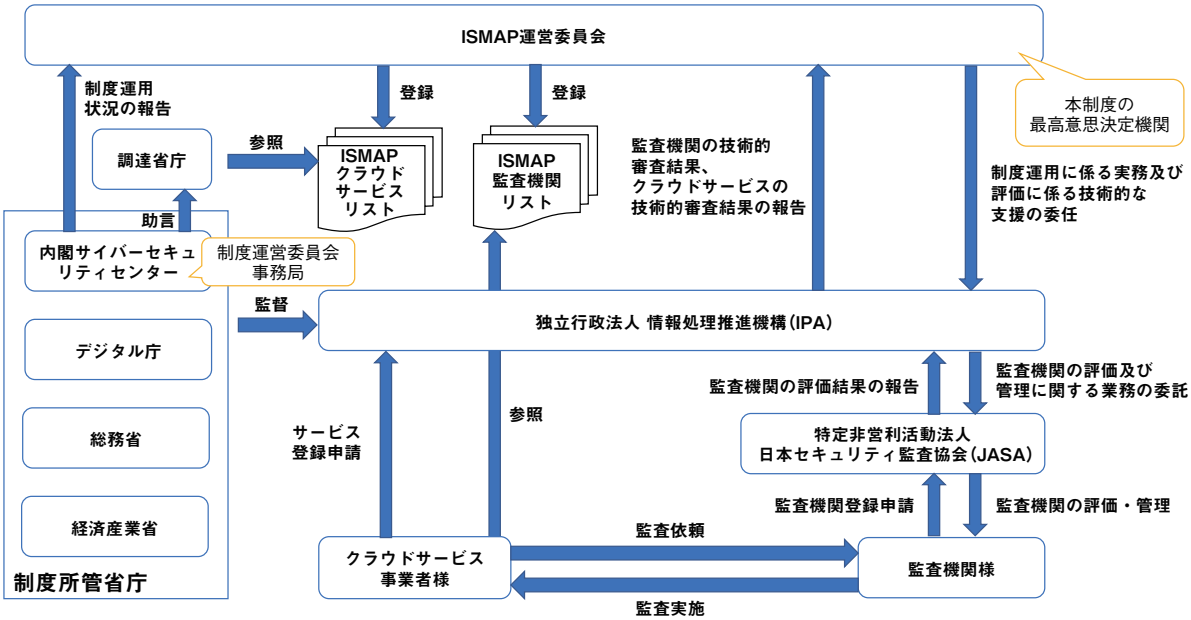
制度の概要、基準規程類、監査機関リスト、及びサービスリストは、2021年5月に開設されたISMAPポータルサイト※91で公開されており、2022年1月には同制度の登録について、ポータルサイトでの電子申請の受付を開始している。2024年5月1日現在、登録されている監査機関は5機関、クラウドサービスは69サービスである。

(5) セキュアなクラウド利用に向けて

IPAは、クラウドサービス事業者がサービスリストへの登録を行うにあたり、セキュリティ対策の進め方及び管理基準の理解の一助となることを目的として、「ISMAP管理基準マニュアル」を作成している※92。

また、2023年7月4日に発行されたNISCの「重要インフラのサイバーセキュリティに係る安全基準等策定指針※93」は、「事業環境の変化を捉え、インターネットを介したサービス（クラウドサービス等）を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。」としており、国内の評価制度としてはISMAPが該当すると考えられる。ISMAPで公開されるクラウドサービスリスト等が、重要インフラ分野を始めとする民間においても参照されることで、クラウドサービスの適切な活用の推進が期待される。

「クラウドサービスの安全性評価に関する検討会とりまとめ」にも記載されたように、情報システムのセキュリティ確保の責任は、一義的に当該システムの調達者または利用者が負うものである。同制度に登録されたクラウド



（注）制度運用に係る実務及び評価に係る技術的な支援をIPAが行い、うち、監査機関の評価及び管理に関する業務についてJASAに再委託する。

■図3-2-6　クラウドサービスの安全性評価の制度のフロー
（出典）ISMAP「ISMAP概要※90」

サービスを利用したとしても、それだけでは情報システム全体のセキュリティが十分に確保されることにはならない。調達者は、利用するクラウドサービスについて適切な設定を行うことに加えて、情報システム全体のセキュリティリスクを分析し、適切な対策を行うことが求められる。

COLUMN

「情報セキュリティ監査制度」創設20周年を迎えて

経済産業省により「情報セキュリティ監査制度」が作られたのは 2003 年のことで、2023 年には制度創設 20 周年を迎えました。もちろん、それ以前から情報セキュリティ監査は行われていましたが、何を基準に監査するのかが監査を行う企業・組織によってまちまちだったため、監査結果が適切かどうかの判断が難しいという問題がありました。しかし、情報セキュリティ監査制度によって「情報セキュリティ監査基準」と「情報セキュリティ管理基準」が示され、あいまいだった監査の基準が明確になりました。制度がスタートしてしばらくは、情報セキュリティ監査が世の中に普及したとは言い難い状況でしたが、ここ 5 年程の間に、地方自治体、中央官庁、独立行政法人等の公的機関や、電力等の重要インフラ事業者、クラウド事業者等が、各セグメントにおけるセキュリティ対策の基準を明確化したことから、情報セキュリティ監査が再び注目されています。

情報セキュリティ監査とは、組織の重要な情報資産に対する情報セキュリティ対策が適切に整備・運用されているか否かを、独立かつ専門的な立場から検証・評価を行い、保証あるいは助言を与えることとされています。監査結果に対して、何らかの保証を与えるのは「保証型監査」、助言を与えるのは「助言型監査」と呼ばれます。現在実施されているほとんどは助言型監査ですが、情報セキュリティ監査制度の黎明期において、監査人・被監査主体双方にとって比較的ハードルの低い助言型監査が普及してきたことは自然な流れといえます。しかし、制度創設 20 周年を迎えた中、この助言型監査についていくつか疑問が湧いてきているのも事実です。

まず、監査人には被監査主体との独立性が求められていますが、監査結果に対する「助言」はコンサルティングと何が違うのかという疑問です。助言はあくまで助言であって、発見事項に対してどのように対処すべきかの選択や判断は被監査主体にある、というのが建前となっていますが、監査を受けた側からしてみたら、実際にどう対処したらよいかを知りたいわけで、限りなくコンサルティングと同様の助言が監査人に期待されるでしょう。監査における助言の位置付けをより明確にする必要があるのではないでしょうか。次に、助言型監査にありがちなのが、監査が予定調和的になっているのではないかということです。助言型監査においては限られた工数でできるだけ効率の良い監査を実施するために、監査人はあらかじめ予備調査等によって、何ができていて何ができていないかという監査結果を想定して監査を実施することがよいとされています。しかしこれが行き過ぎると被監査主体が自分で「できていない」と分かっていることが監査人によって「できていない」と追認されるだけの監査になってしまう可能性があります。もちろん第三者に「できていない」と指摘されることで、組織内で対策の重要性が認識されるという効果はありますが、本来の監査の目的はそれだけではないでしょう。

制度創設 20 周年を過ぎた今こそ、助言型監査の在り方について見直すとともに、ある程度セキュリティマネジメントの成熟度が高い企業や組織に対しては、監査の本来の目的である「保証型監査」を普及させるためにはどうしたらよいかを考える時期に来ているのではないでしょうか。

3.3 暗号技術の動向

電子政府推奨暗号の安全性の評価・監視等を行っているCRYPTRECの動向と、暗号技術に関する研究動向について述べる。

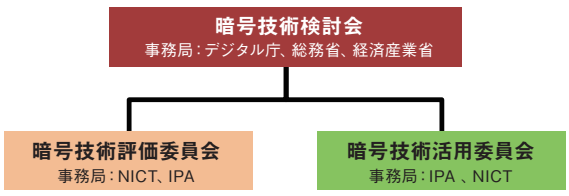
3.3.1 CRYPTRECの動向

政府等が利用するシステム（電子政府システム）におけるセキュリティを確保するため、デジタル庁、総務省、経済産業省、国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）、及びIPAは安全性と実用性に優れた暗号技術を選び出すことを目的に、CRYPTREC（Cryptography Research and Evaluation Committees）を組織している。CRYPTRECでは、電子政府システムでの利用を推奨する暗号アルゴリズム（「CRYPTREC暗号リスト※94」）の安全性を評価、監視し、暗号技術の適切な実装法や運用法を調査、検討している。また、電子政府システムの調達・開発にあたって、調達要件や開発要件として採用すべき「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準※95」（以下、強度要件設定基準）も提供している。

(1) 2023年度の体制

CRYPTRECは、デジタル庁と総務省、経済産業省が運営し、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する「暗号技術検討会」、及びNICTとIPAが運営し、主に技術的な評価を実施する委員会とで構成されている。

委員会には、暗号技術の安全性評価を中心とした技術課題を主に担当する「暗号技術評価委員会」と、セキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する「暗号技術活用委員会」が設置されている（図3-3-1）。



■図3-3-1　CRYPTRECの体制

暗号技術検討会と両委員会の主な役割は以下のとおりである。

- 暗号技術検討会
  CRYPTREC活動計画の承認、委員会が作成する各種成果物の承認等、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する。
- 暗号技術評価委員会
  暗号技術に対する攻撃技術動向の調査や安全性評価等、暗号技術の技術的信頼性に関する検討を担当する。傘下には、量子コンピューターが実用化されても安全性が保てると期待される「耐量子計算機暗号（PQC：Post-Quantum Cryptography）」に関するガイドラインを作成する「暗号技術調査ワーキンググループ（耐量子計算機暗号）」が設置されている。
- 暗号技術活用委員会
  セキュリティ対策の推進、暗号技術の利用促進等に寄与する運用ガイドラインの整備を中心とした、暗号利用に関する課題の検討を担当する。傘下には、2020年度に公開した「暗号鍵管理システム設計指針（基本編）※96」のガイダンスを作成する「暗号鍵管理ガイダンスワーキンググループ」が設置されている。

(2) 2023年度の主な活動

2023年度の暗号技術検討会及び各委員会の主な活動内容・成果について以下に述べる。

(a) 暗号技術検討会

2023年度には、各委員会の2023年度活動計画、及び活動報告の審議が行われ、承認された。更に、各委員会で作成していた以下のガイドラインについて審議が行われ、承認された。

- CRYPTREC暗号技術ガイドライン（軽量暗号）
- TLS暗号設定ガイドライン

(b) 暗号技術評価委員会

CRYPTREC暗号リストに掲載されている暗号技術の安全性と実装性に関わる監視活動のほか、2023年度の主な活動内容・成果は以下のとおりである。

- CRYPTREC暗号技術ガイドライン（軽量暗号）の更新
  2023年度はNIST Lightweightコンペティション※97

にて最終選考されたAsconについて、実装性能及び標準化動向について外部評価を実施した。また、2021年度から2023年度にかけて実施した外部評価結果に基づき、2016年度版「CRYPTREC暗号技術ガイドライン（軽量暗号）」に新規情報の追加・更新を行い、2023年度版ガイドライン[※98]として公開した。

- 暗号技術調査ワーキンググループの活動
  PQCに関するガイドライン[※99]及び研究動向調査報告書[※100]を2022年度に公開したが、NISTのPQC標準化において第4ラウンドが進行中であることや、PQCの技術開発や標準化活動が引き続き世界的に活発であるため、「暗号技術調査ワーキンググループ（耐量子計算機暗号）」を引き続き設置し、各種動向を今後2年間かけて調査・把握し、同ガイドラインの改定及び研究動向調査報告書の新規作成を行うこととした。2023年度は、PQCがベースとする数学的な問題ごとに、主要な暗号国際会議を中心に、研究動向や開発・標準化動向について調査した。
  このほか、主要な公開鍵暗号（RSA暗号、楕円曲線暗号）の安全性の根拠となる「素因数分解問題」と「離散対数問題」の困難性に関して、CRYPTRECが公開している「予測図[※101]」の改訂も行った。

(c) 暗号技術活用委員会

2023年度の主な活動内容・成果は以下のとおりである。

- TLS暗号設定ガイドライン改訂の検討
  「TLS暗号設定ガイドライン[※102]」は、主にWebサーバーの構築者・管理者向けにサーバーでの適切なTLS（Transport Layer Security）暗号設定方法を解説したものである。2020年7月に同ガイドラインを公開して以降、CRYPTREC暗号リストの改定、強度要件設定基準の策定が行われた。また、最近のTLSに関するRFC（Request For Comments）規格や技術環境の変化への対応も必要になったことから、公開後の3年間の動向を踏まえて、同ガイドラインの改訂を行った。
  具体的には、安全性の基準としての「鍵長」による推奨要件を、強度要件設定基準にて導入された「ビットセキュリティ」による推奨要件へと変更した。これにより、取り扱い方法があいまいであった、「X25519の楕円曲線」が明確に許容されることとなった。また、「セキュリティ例外型」では「推奨セキュリティ型」への速やかな移行を明確に促す観点から、移行期限を明記した表現が取り入れられた。現在のセキュリティ例外型の設定内容は、2029年度を目途とした改訂時に終了する予定である。
- 暗号鍵管理ガイダンスワーキンググループの活動
  情報を安全に取り扱うためには、通信データや保管情報の暗号化に使う暗号アルゴリズムに注意を払うだけでは不十分であり、暗号アルゴリズムに用いられる暗号鍵の管理が適切に行われる必要がある。このため、暗号鍵管理システムにおいて検討すべき要求項目を網羅し、それらを解説したガイダンスの作成を進めており、「暗号鍵管理システム設計指針（基本編）」を2020年に、「暗号鍵管理ガイダンス 第1版[※103]」を2023年5月にそれぞれ公開した。
  2023年度は、同ガイダンスの第1版では記載を見送った解説部分の拡充を行うため、暗号鍵管理ガイダンスワーキンググループを引き続き設置し、「システムの設計原理と運用ポリシー」及び「デバイスへのセキュリティ対策」の要求項目に対する解説・考慮点を整理した。2024年度には、残る「システムのオペレーション対策」の要求項目に対する解説・考慮点を整理した上で、これらを取りまとめて拡充部分の解説内容を執筆し、同ガイダンスの追補を完成させる計画である。

(d) CRYPTREC シンポジウム 2023 の開催

CRYPTRECの活動成果を広く知らしめ、暗号技術に関する最新動向を紹介することで、社会全体のセキュリティ向上に役立てるため、2023年7月26日に「CRYPTREC シンポジウム 2023[※104]」を開催した。同シンポジウムは、現地会場とオンライン会場のハイブリッド形式で開催された。

3.3.2 暗号関連の技術動向

本項では2023年度における、共通鍵暗号、公開鍵暗号、軽量暗号及び実装攻撃に関する研究動向についてそれぞれ解説する。

(1) 共通鍵暗号に関する研究動向

2023年度は、共通鍵暗号の解読について大きな進展はなかったものの、既存の暗号アルゴリズムへの攻撃について、攻撃に必要な計算量の削減等の進展があった。ここでは主な発表を紹介する。

AES[※105]について、Eurocrypt 2023[※106]にて、特定の差分を持つように選択した二つの平文(A, B)を暗号化して暗号文(C, D)を作り、それらに特定の差分を

加えた別の暗号文 (E, F) にしてから平文 (G, H) に復号して得られる平文・暗号文の組 [(A, B, G, H), (C, D, E, F)] を大量に使って秘密鍵を推定するブーメラン攻撃の新手法が報告された。切詰差分解析と呼ばれる中間データの一部のビットの差分のみに着目する解析法をブーメラン攻撃に適用することによって、256 ビット鍵の場合の AES の仕様である 14 段中、6 段に対する解読計算量が従来の約千分の一である 2^{61} に削減された。また、Crypto 2023[※107] にて、攻撃者が平文に加えて秘密鍵を自由に操作することができる前提で秘密鍵を求める新たな関連鍵攻撃手法が報告された。具体的には、平文側と暗号文側の両方からそれぞれ求めたデータが中間段において一致するような鍵候補を絞り込む中間一致攻撃と差分攻撃を組み合わせた差分中間一致攻撃という解読手法により、解読可能段数が 10 段から 12 段に更新された。更に、128 ビット鍵の場合の AES に対しては、FSE 2023[※108] にて、特定の差分を持つように選択した平文・暗号文のペアを大量に使って秘密鍵を求める差分攻撃の中でも、より現実に近い汎用的な攻撃モデルでの新手法が提案され、従来と同じ 7 段に対する解読が可能（解読計算量 $2^{110.2}$）であると報告された。

また、ストリーム暗号 ChaCha[※109] についての攻撃論文がいくつか報告されている。特に FSE 2023 では、複数の入出力差分を組み合わせる攻撃手法により、仕様である 20 段中、6 段に対する解読計算量を従来の $1/2^{40}$ となる $2^{99.48}$ に削減した結果が示された。また、Crypto 2023 では、加算、ローテーション、XOR（排他的論理和）の基本構造に対して大きな相関特性を持つ「良い PNB（probabilistic neutrality bit）」と呼ばれるビットの集合を見つける効率的な手法が提案された。この手法を適用して、最後の XOR とローテーションを行わない 7.5 段に対する攻撃（解読計算量 $2^{242.9}$）が初めて報告された。上記のように、2023 年度も AES、ChaCha に対する暗号解析の進展が見られたが、セキュリティマージンはまだ十分にあり、安全性に直ちに影響を与えるものではない。

(2) 公開鍵暗号に関する研究動向

公開鍵暗号に関する暗号解析では、NIST による耐量子計算機暗号（PQC）の標準化プロセス[※110] に関連して、重要な攻撃報告がなされている。

2022 年度に行われた NIST 4th PQC Standardization Conference[※111] において候補であった、同種写像を用いた鍵カプセル化メカニズムである SIKE（Supersingular Isogeny Key Encapsulation）はもはや安全ではないことが、SIKE の開発者チームから発表された。これは Wouter Castryck 氏と Thomas Decru 氏によって、SIKE の提案パラメータのすべてにおいて秘密鍵を求めることができる攻撃が査読前論文（Eurocrypt 2023 にて採録）として報告されたことによる。また Eurocrypt 2023 にて、Castryck-Decru の手法とは独立に考案された Luciano Maino 氏らによる手法を組み合わせて、開始曲線の自己同型環が分かっている場合の攻撃の一般化や、開始曲線を変更した場合への攻撃の一般化がなされている。このように、SIKE のパラメータを変更した場合に対する攻撃や、その亜種に対する攻撃も盛んに研究されている状況であり、SIKE と同じ分類となる同種写像に基づく公開鍵暗号の安全性評価に与える影響が注目される。

2022 年 7 月に、NIST は、PQC の公開鍵暗号及び鍵確立アルゴリズムとして CRYSTALS-Kyber を、署名アルゴリズムに関しては CRYSTALS-Dilithium、FALCON、SPHINCS+ を最終選考アルゴリズムとして発表していた[※112]。2023 年度は、これに続いて、ドラフト規格を作成中である。また、2023 年度より、格子ベースではない追加の署名アルゴリズムを募る新たなラウンドを開始している。

(3) 軽量暗号の標準化に関する動向

NIST Lightweight コンペティション[※97] において、2023 年 2 月に Ascon が最終選考アルゴリズムとして発表されていた[※113]。2023 年度はこれに続いて、2023 年 6 月に NIST IR（Internal Report）の発行、及びワークショップが開催された。2024 年 3 月末時点でドラフト規格を NIST が作成中である。

(4) 実装攻撃に関する動向

デジタル署名アルゴリズムである DSA（Digital Signature Algorithm）及び ECDSA[※114] では、署名生成時に nonce と呼ばれるランダムな値を使用する。nonce の扱いには注意が必要で、サイドチャネル攻撃等の手段によって nonce の情報が部分的に漏えいしている場合に適用できる攻撃が知られており、Lattice Attack と呼ばれている。CHES 2023[※115] において、従来の限界を超える Lattice Attack の改良が発表された[※116]。2022 年度にも Lattice Attack の改良が報告されていたが、そのときと比較して攻撃成功率が向上している。また、従来は攻撃不可能と考えられていた、nonce の漏えいが 1 ビットであるケースについても、112 ビッ

トのECDSAに対する攻撃に成功したことが報告された。現状では112ビット以下の楕円曲線は使用されていないので、この攻撃による現実的な脅威は生じないが、今後もこの攻撃の研究とその進展に注意する必要があり、DSA、ECDSAの実装におけるサイドチャネル情報からのnonceの漏えい対策の重要性が増している。

また、サイドチャネル攻撃に関して、算術加算処理中の繰り上がりに注目した手法の提案があり、鍵付きハッシュ関数によるメッセージ認証アルゴリズムの一つであるHMAC-SHA-2の純粋なハードウェア実装に対する攻撃に成功したことが発表された※117。HMAC-SHA-2へのサイドチャネル攻撃に関しては、従来はソフトウェア実装にのみ適用可能であるものや、部分的な分析にとどまるものしか知られておらず、HMAC-SHA-2の純粋なハードウェア実装はサイドチャネル攻撃に対しては対策を特に施さなくても十分安全と考えられることもあった。しかし、この新しい攻撃手法により、もはやそうとは言えず、純粋なハードウェア実装にあたっても適切な攻撃対策が必要になったと言える。

3.4 制御システムのセキュリティ

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※118を管理し、制御するシステムである。従って、制御システムのセキュリティインシデントは、社会経済活動に大きな影響を与える。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。

本節では、制御システムのセキュリティの動向とセキュリティ強化の主な取り組みについて述べる。

3.4.1 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、2022年同様、2023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、世界の制御・運用技術（OT：Operational Technology）の専門家570名を対象とした調査結果では、回答者の組織の74%が過去1年間に少なくとも1回の侵入を経験し、32%がランサムウェアによる攻撃の被害を受けていた※119。米国、ドイツ、アラブ首長国連邦、日本のIT及びOTセキュリティの意思決定者405名を対象にした調査結果では、回答者の97%が過去1年間にOTに影響を与えたITセキュリティインシデントを経験したと回答し、47%がランサムウェアによる攻撃のインシデントを経験したと回答している※120。

以下では、2023年に公になった重要インフラ分野のインシデントのうち、水道の制御システムが侵害された事例、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、エネルギーインフラへの大規模サイバー攻撃の事例、港湾施設が標的となった事例、GPSスプーフィング攻撃の事例、政府や自治体が標的となった事例、医療機関が標的となった事例について述べる。

(1) 水道の制御システムが侵害された事例

2023年も引き続き、重要インフラの制御システムが侵害されるインシデントが世界各地で発生した。

2023年11月24日、米国ペンシルベニア州アリキッパの水道局の、水圧を維持し水流を調整するポンプがある郊外の施設が、親イラン派の攻撃グループ「Cyber Av3ngers」による攻撃を受けた※121。この施設で使用されている、イスラエルのUnitronics（1989）（RG）Ltd.製のPLC（Programmable Logic Controller）が標的となり、作業員はPLCをオフラインにし、バックアップツールを使用して水圧を維持した。このPLCは主ネットワークから切り離された独自のコンピューターネットワーク上にあったため、水処理施設そのものには影響はなく、飲料水には影響はなかった。同グループはイラン政府のイスラム革命防衛隊の傘下で、政治的動機によってイスラエル製品やイスラエルと関係のある組織を攻撃することを公言しており、11月22日以降、米国内の上下水道施設を含む複数の施設の同PLCに、デフォルトのパスワードでアクセスしていた可能性がある※122。米国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）は、同PLCを使用している上下水道分野の組織に対して、デフォルトのパスワード「1111」が使用されていないことを確認して変更すること、OTネットワークへのすべてのリモートアクセスに多要素認証を要求すること等のアラートを公表した※123。更に、機器メーカーに対して、デフォルトのパスワードの廃止を勧告するアラートを公表した※124。

また、2023年12月初旬には、アイルランド西海岸メイヨー県エリスの民間の水道事業者のシステムも、イスラエルのUnitronics (1989) (RG) Ltd.製のツールを使用していることを理由に、同一の攻撃グループによる攻撃を受けた。この攻撃によって、2日間にわたって約160世帯が断水した※125。

(2) 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3-4-1（次ページ）に、2023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を示す。

被害企業・組織	発生国	発生年月	内容・影響・被害
工具・部品メーカー	カナダ	2023年1月	サイバー攻撃を受け、インシデント調査のために一部のコンピューターシステムをオフラインにしたため、三つの生産施設が影響を受けた※126。
郵便配達サービス企業	英国	2023年1月	サイバーインシデントが発生し、国外への郵便サービスを停止した※127。
半導体装置メーカー	米国	2023年2月	ランサムウェアによる攻撃を受け、生産関連システムを含む特定のビジネスシステムが影響を受け、封じ込めの一環として、生産施設の一部で一時的に操業を停止した※128。
農業・食品企業	米国	2023年2月	ランサムウェアによる攻撃を受け、北米全域のシステムを停止したため、生産工場の操業及び出荷が停止した※129。
国営郵便企業	イスラエル	2023年4月	サイバー攻撃を受け、予防措置としてコンピューターシステムの一部を停止したため、荷物の配送、宅配便の受付等のサービスが停止した※130。
電子機器メーカー	フランス	2023年5月	ランサムウェアによるものと考えられるサイバー攻撃を受け、フランス、ドイツ、チュニジアの三つの施設の生産を停止した※131。
製薬会社	日本	2023年6月	ランサムウェアによる攻撃を受け、複数のサーバーが暗号化された。物流に関連するシステムを含む国内外の一部の社内システムをサーバーから切り離した※132。
鉄道会社	ポーランド	2023年8月	ハッカーが、列車を停止させる信号を発信したため、少なくとも20の列車が停止し、数時間運行が麻痺した※133。
通信事業者	チリ	2023年10月	ランサムウェアによる攻撃を受け、データセンター、インターネットアクセス、VoIP（Voice-over-IP）等多数のサービスに影響が出た※134。
通信事業者	ウクライナ	2023年12月	サイバー攻撃を受け、携帯電話サービス及びインターネットが利用できなくなった※135。

■表3-4-1　2023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

(3) エネルギーインフラへの大規模サイバー攻撃の事例

2023年5月、デンマークで、重要インフラを標的とした、同国史上最大規模のサイバー攻撃が発生した。2023年5月11日から30日間の二波にわたる攻撃で、同国の多くの重要インフラ事業者が使用している台湾のZyxel Networks製ファイアウォールのゼロデイ脆弱性を悪用して、デンマークのエネルギーインフラを運営する22社のネットワークが侵害された。この攻撃について2023年11月、デンマークの重要インフラ分野のCSIRTであるSektorCERTは、詳細なレポートを公表した。

攻撃の第一波は5月11日に開始され、その後しばらく休止した後、5月22日に第二波が始まった※136。SektorCERTのセンサーネットワークがすぐに攻撃を検知し、インシデント対応チームを編成して対応したが、攻撃者は複数の企業の産業用制御システムにアクセスし、いくつかの企業がインターネットへの接続を切断したアイランドモードに追い込まれたと報告されている。これらの攻撃は、ロシア連邦軍参謀本部情報総局が関与しているとされるAPT攻撃グループ「Sandworm」によるものとされていたが、ForeScout Technologies, Inc.は、第二波は単に修正プログラムが適用されていないファイアウォールに対する大規模な攻撃キャンペーンの一部であり、「Sandworm」や他の国家支援の攻撃者による標的型攻撃の一部ではないことを示唆している※137。

(4) 港湾施設が標的となった事例

港湾施設がサイバー攻撃を受け、物流に直接大きな影響を与えたインシデントが日本とオーストラリアで発生した。

2023年7月4日、総取扱貨物量日本一の名古屋港の、コンテナターミナルを管理する中央システム「名古屋港統一ターミナルシステム（NUTS：Nagoya United Terminal System）」がランサムウェア攻撃を受けて停止し、トレーラーを使用するターミナルでのコンテナ搬出入作業がすべて中止された。同システムは7月6日に復旧した※138（詳細については「1.2.1(2)(a)港湾事務所における被害事例」参照）。

2023年11月には、オーストラリアの港湾運営会社DP World Australiaがサイバー攻撃を受けた。11月10日、四つの港（シドニー、メルボルン、ブリスベン、フリーマントル）のコンテナターミナルの陸上業務及びトラックの移動を管理するシステムで不正な活動を検知し、すぐにシステムへのアクセスを遮断し、インターネットへの接続を切断した。そのため、これら四つの港のコンテナターミナルの操業がすべて停止した。同社は、システムの完全性を確実にするためのテストを11月12日に実施し、11月13日朝に操業を再開した。これら四つのコンテナターミナルは、オーストラリアの貿易の約40%を取り扱っており、操業停止となったことで、約3万個ものコンテナが立往生する事態となった※139。

(5) GPS スプーフィング攻撃の事例

パイロットと航空技術者の国際的なグループOPSGROUPによると、スプーフィング（なりすまし）攻撃によって民間航空機のナビゲーション（航行）システムが機能しなくなるインシデントが、2023年9月以降、中東上空で何十件も発生した※140。9月下旬、イラン近郊で複数の民間航空機のナビゲーションシステムが機能しなくなり、航路を誤った。これらの航空機は、システムを欺き、実際の位置から何マイルも離れた場所を飛行していると思わせるスプーフィングされたGPS信号を受信した。そのうちの1機は、許可なくイラン領空に侵入するところだった。この攻撃活動はバグダッド、カイロ、テルアビブの三つの地域に集中していた。OPSGROUPは11月に、過去5週間で50件以上のインシデントを追跡し、三つの異なる種類のナビゲーションスプーフィングのインシデントを識別したと公表した。原因がはっきりしないこの問題に対する解決策は今のところないという※141。

(6) 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、2022年同様、世界中で発生した。

2023年2月8日、米国カリフォルニア州オークランド市の自治体が、ランサムウェア攻撃グループ「Play」による攻撃を受けた※142。影響を受けたシステムをインターネットから切り離したため、市民にサービスを提供しているシステムが使用できなくなった※143。復旧できない状態が1週間続き、2月14日、同市は非常事態宣言を発令した※144。この宣言により、同市はインフラとサービスの復旧のために、機器や資材の調達を迅速化し、必要に応じて緊急作業員を派遣することができるようになった。攻撃グループは、身代金が支払われなかったため、3月1日に同市から窃取したとするデータのリストを公開し、3月4日には10GBのデータを公開した※142。このデータには、個人情報、金融情報、身分証明文書、パスポート情報、及び2010年7月から2022年1月の間に市に在職していた職員の情報等が含まれていた。同市は、侵害の影響を受けた約1万3千人に通知した。4月末に、ようやくほとんどのシステムが復旧した※145。また、5月末時点で、同インシデントによって被害を受けたとして、同市に対して4件の法的訴訟と1件の集団訴訟が起こされている※146。

2023年12月8日、イタリアのクラウドサービスプロバイダーWestpole SPAが、ランサムウェア攻撃グループ「LockBit 3.0」による攻撃を受けた。この攻撃は、同社の顧客であり、540の地方自治体を含む1,300の行政機関に行政向けデジタルサービスを提供するイタリア政府の子会社PA Digitale社が主要な標的であった。影響を受けた行政機関・自治体は、サービスの提供を手作業に頼らざるを得なくなった。イタリアの国家サイバーセキュリティ庁が、影響を受けた行政機関･自治体のデータ復旧に取り組んだ※147。

(7) 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。

2023年11月23日、米国の6州で30の病院と200以上の介護施設を運営する医療サービスプロバイダーArdent Health Servicesが、ランサムウェアによる攻撃を受けた。同事業者は、すぐにネットワークをオフラインにし、サーバー、臨床プログラムを含むITアプリケーションへのすべてのユーザーアクセスを停止した※148。影響を受けた病院は、緊急でない処置の一部を一時的に停止し、緊急治療を必要とするすべての患者を、その地域の他の病院に移送した。移送先となった病院は、増大した患者に対応するために、スタッフを増員しなければならなかった。また、予約や手術の再スケジュールが必要な患者には、病院が直接連絡した。電子カルテプラットフォームや、その他の臨床及びビジネスの中核システムが12月6日に復旧し、患者ポータルの一部機能は12月21日に、全機能は2024年1月9日に復旧した※149。

医療分野で働く14ヵ国のIT及びサイバーセキュリティ専門家233人を対象に実施した調査レポートによると、ランサムウェア攻撃を受けたと回答した割合は2022年の66%から60%に減少しているが、ランサムウェア攻撃によってデータが暗号化された割合は73%で、過去3年間で最も高かった。データが暗号化された攻撃の37%では、データも窃取されており、「二重の脅迫」が一般化していることを示唆している。また、医療分野におけるランサムウェア攻撃の根本原因は、認証情報の侵害（32%）が最も多く、次いで脆弱性の悪用（29%）であった※150。

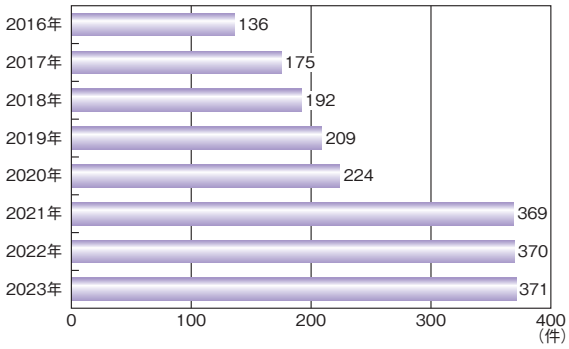
3.4.2 脆弱性及び脅威の動向

本項では、2023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

2023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 CISA が、2023 年に公開した制御システムの脆弱性に関するアドバイザリー（ICS Advisory）は 371 件で、2022 年の 370 件から横ばいであった（図 3-4-1）。



■図 3-4-1　CISA が公開した制御システムの脆弱性に関するアドバイザリーの件数（2016 ～ 2023 年）
（出典）CISA の公開情報※151 を基に IPA が作成

2023 年は、悪用する際に認証を必要とする脆弱性の数が大幅に増加した。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）のうち、悪用する際に認証を必要とする脆弱性の割合が 2022 年は 22% だったが、2023 年は 34% だった。これには、研究開発中のデバイスやプロトコルに認証を取り入れるものが増えていること、認証が必要なルートキットの悪用の増加等、いくつかの要因が考えられる※152。

影響の大きな脆弱性も発見されている。以下では、それらについて解説する。

(a) Crit.IX

米国のセキュリティベンダー Armis Inc. が、米国 Honeywell International Inc.（以下、Honeywell 社）の発電所、化学プラント、自動車製造、農業生産等の工場で稼働する自動制御システムである DCS（Distributed Control System）プラットフォーム製品 Experion に 9 件の脆弱性を発見し、これらの脆弱性を「Crit.IX」と名付けた※153。Crit.IX は、無認可のリモートコード実行（RCE: Remote Code Execution）を可能にする脆弱性で、攻撃者はデバイスを乗っ取り、DCS コントローラーの動作を変更する権限を持ちながら、コントローラーを管理するエンジニアリングワークステーションからはその変更を隠すことができる。Armis Inc. と Honeywell 社は協力して修正プログラムを作成し、顧客に通知した。また、CISA は、この問題に関する独自のアドバイザリーを 2023 年 7 月 13 日に公表し、Honeywell 社が発行した修正プログラムを適用するよう顧客に促した※154。

(b) TETRA:BURST

世界中の緊急（救急）サービスで使用されている無線通信プロトコル Terrestrial Trunked Radio（TETRA）に、攻撃者が通信を盗聴したり操作したりすることを可能にする深刻なゼロデイ脆弱性が研究者らによって発見された。1995 年に欧州電気通信標準化機構（ETSI：European Telecommunications Standards Institute）が発表した TETRA は、特に法執行機関向けに最も広く使われている業務用移動無線規格の一つで、警察、消防隊、軍隊等の緊急（救急）サービスや一部の産業環境で、約 30 年にわたって継続的に使用されている。研究者らは TETRA に五つの脆弱性を発見し、「TETRA: BURST」と総称している。攻撃者がこれらの脆弱性を悪用すると、警察や軍の通信を盗聴したり、彼らの動きを追跡したり、TETRA で伝送される重要インフラのネットワーク通信を操作したりすることが可能になる※155。

(c) CODESYS V3 ソフトウェア開発キットの 15 の脆弱性

Microsoft Corporation（以下、Microsoft 社）が、CODESYS V3 ソフトウェア開発キット（SDK：Software Development Kit）の 15 の脆弱性を発見し、世界中の産業環境で使用されている数百万台の PLC が、リモートコード実行やサービス拒否（DoS：Denial of Services）攻撃を受けるリスクに晒されている、と警告した。500 社以上のデバイスメーカーが、IEC 61131-3 規格に準拠している 1,000 種類以上の PLC のプログラミングに同 SDK を使用しており、ユーザーはカスタムオートメーションシーケンスを開発することができる。Microsoft 社は 2022 年 9 月に、開発元であるドイツの CODESYS GmbH に報告し、同社はセキュリティ更新プログラムを 2023 年 4 月にリリースした。Microsoft 社は、リスク認識を高め、修正プログラム適用のペースが上がるよう、8 月 10 日に詳細についてのブログ記事を投稿した※156。

(2) 脅威の動向

2023 年の脅威の動向としては、2022 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。

Dragos, Inc. によると、2023 年に産業組織に影響を与えたランサムウェア攻撃グループは 50 グループで、2022 年から 28% 増加している。また、同社に報告された、産業組織に影響を与えたランサムウェア・インシデン

トは 905 件で、2022 年から 49.5% 増加している※152。

世界の重要インフラのコンポーネントを所有、運用、またはサポートする企業に勤務する IT 及び OT のセキュリティ専門家 1,100 人を対象とした調査結果では、過去 1 年間に 75% の組織がランサムウェア攻撃を経験しており、過去 2 年間で 10% 増加している。そのうち 37% が IT/OT 両環境が影響を受けており、17% が OT 環境のみ影響を受けていた※157。

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※158 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、2023 年には、制御システムを標的とする新たなウイルスが確認された。その概要を以下に示す。

米国のサイバーセキュリティ企業 Mandiant, Inc. が、送電・配電設備を停止させるために設計された新たなウイルス「CosmicEnergy」を発見した※159。このウイルスは、ヨーロッパ、中東、アジアの送電・配電業務で一般的に使用されている IEC 60870–5-104（以下、IEC-104）規格準拠のリモートターミナルユニット（RTU：Remote Terminal Unit）を特に標的としていた。分析の結果、CosmicEnergy は 2016 年 12 月と 2022 年 4 月にウクライナのエネルギープロバイダーを標的とした攻撃に使われた「Industroyer」や「Industroyer.V2」といった過去の OT ウイルスに類似していることが明らかになった。更に、「IronGate」「Triton」「Incontroller」等の制御システムを標的とした他のウイルスと同様に、Python ベースで、OT プロトコル実装にオープンソースライブラリを使用している。Industroyer 同様、破壊ツール「PIEHOP」を使用して侵害した Microsoft SQL サーバーを介して標的の OT システムにアクセスする可能性が高い。被害者のネットワークに侵入すると、攻撃者は悪意のあるツール Lightwork を介して IEC-104 の「ON」または「OFF」コマンドを発行することにより、RTU をリモートで管理することができる。Mandiant, Inc. は、今回発見されたウイルスは、ロシアのサイバーセキュリティ企業 Rostelecom-Solar（旧 Solar Security）が主催する模擬停電攻撃演習におけるレッドチーム用ツールとして、請負業者が開発したものである可能性があると見ている。

3.4.3 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

2023 年 2 月 24 日、米国コンピューター緊急事態対策チーム（US-CERT：United States Computer Emergency Readiness Team）と産業制御システムサイバー緊急事態対応チーム（ICS-CERT：Industrial Control Systems Cyber Emergency Response Team）が廃止され、CISA に統合された※160。

CISA は、情報システムがランサムウェア攻撃者に悪用される可能性のある脆弱性を露出していることを、重要インフラ事業者に警告する新たな取り組み「Ransomware Vulnerability Warning Pilot（RVWP）」を 2023 年 1 月 30 日に開始した※161。RVWP では、CISA が重要インフラ事業者のネットワークをスキャンし、インターネットに接続されたシステムの脆弱性を発見して、組織がハッキングされる前に脆弱性を修正できるよう支援する。

2023 年 3 月、CISA は 2022 年 11 月に発表した「Cross-Sector Cybersecurity Performance Goals（CPGs）」を、重要インフラコミュニティから寄せられたフィードバックに応えて更新した※162。この更新では、NIST のサイバーセキュリティフレームワーク（CSF：Cyber Security Framework）の機能と密接に連携し、組織が CPGs を使用して、CSF を中心に構築された幅広いサイバーセキュリティプログラムの一部として投資の優先順位を決定できるように、整理、順序変更、番号付けが行われている。

2023 年 7 月、CISA は重要インフラパートナー（以下、パートナー）の IT と OT の両方を分野横断的にリアルタイム監視することを目的としたプログラム「CyberSentry」を発表した※163。このプログラムは、IT/OT ネットワークに影響を及ぼす既知・未知の悪意ある活動を監視することで、電力・水道、銀行・金融機関、医療等の国家の重要な機能を支える米国の重要インフラネットワークの運用者を防衛する国家的取り組みを支援することを目的としている。

2023 年 11 月、CISA と連邦緊急事態管理庁（FEMA: Federal Emergency Management Agency）は、米国の重要インフラのセキュリティとレジリエンス力を高めるための持続的な全国キャンペーン「Shields Ready」を開始した※164。同キャンペーンは、重要インフラが潜在的な脅威に備えてどのように準備するか、また、危機やインシデントが発生する前に行動を起こすことで、システム、施設、プロセスのレジリエンス力をどのように強化するか

について、より広範かつ戦略的に焦点を当てている。「Shields Ready」は重要インフラ事業者に対し、インフラのレジリエンス力を高めるための四つのステップ（①重要な資産を識別し、依存関係をマッピングする、②リスクのアセスメントをする、③計画を立て、演習を実施する、④演習の結果やアセスメントに基づいて、対応・復旧計画を定期的に評価し、更新する）に集中することを奨励している。

(2) 米国 Biden 政権の取り組み

米国のBiden政権は、2023年3月2日に国家サイバーセキュリティ戦略「National Cybersecurity Strategy」を発表した※165。同戦略には、米国が直面する課題や脅威、それらに対処するための優先順位が詳細に記されている。また、五つの柱である①重要インフラを守る、②脅威アクターを妨害し、解体する、③セキュリティとレジリエンスを向上させるために市場の力を形成する、④レジリエンスの未来に投資する、⑤共通の目標を追求するための国際的なパートナーシップを構築する、を掲げている。2018年の国家サイバーセキュリティ戦略からの大きな変更点として、重要インフラ分野の組織は、一定の基本的なサイバーセキュリティ要件を満たすことが求められている。更に政府はソフトウェアやハードウェアの商業的な販売者や開発者が、セキュアな開発手法を通じて、自社の製品をセキュアに保つ責任を負うことを望んでいる。

2023年7月13日には、国家サイバーセキュリティ戦略の実施計画「National Cybersecurity Strategy Implementation Plan（NCSIP）」を発表した※166-1。この計画には、連邦政府機関の65以上の取り組みが定められており、それぞれの期限内に達成する必要がある。官民パートナーシップの拡大が、同戦略が求めているサイバースペースにおける責任の「根本的な転換」における中心的な焦点で、「ランサムウェアのエコシステム」のプレイヤーに対する積極的な破壊及び解体作戦に、民間セクターのパートナーを参加させるよう求めている。また、サプライチェーンリスクを軽減するために、サードパーティーベンダーに適用されるソフトウェア部品表（SBOM：Software Bill of Materials）標準の策定に、政府が更に関与することを求めている。NCSIPは、新たなサイバー脅威に対応していつでも更新できるように設計されており、2024年5月に第2版が公開された※166-2。

Joseph Biden大統領は、2023年11月を「重要インフラのセキュリティとレジリエンス月間」とし、「本月間において、重要インフラを強化し、我々の集団的セキュリティと経済的繁栄を損なう脅威に対して警戒を怠らないことを再確認しよう」と宣言した※167。CISAは、「この月間は、重要インフラが国家の健全性に果たす重要な役割と、重要インフラのセキュリティとレジリエンスを強化することがなぜ重要なのかについて、政府のあらゆるレベル、インフラの所有者と運用者、そして米国民を教育し、関与させることに重点を置いている」と声明で述べている。

NISTは、CSF 2.0を2024年2月26日に公開した※168。フレームワークの対象範囲が、あらゆる分野、あらゆる規模の組織に拡大された。正式名称も、「重要インフラのサイバーセキュリティを改善するためのフレームワーク」から「サイバーセキュリティフレームワーク」に変更されている。CSFは、組織がサイバーセキュリティ態勢を改善し、安全に活動するための組織意識を向上させるための、一連のベストプラクティス及び推奨事項である。CSF 2.0では、コアの五つの機能（識別（Identify）、防御（Protect）、検知（Detect）、対応（Respond）、復旧（Recover））に、六つ目の機能として、組織のミッションと利害関係者の期待に照らして、他の五つの機能の成果を達成し、優先順位をつけるために組織が何をすべきかを示すアウトプットを提供する「統治（Govern）」が追加された。

NISTのNational Cybersecurity Center of Excellence（NCCoE）は、LNG（液化天然ガス）業界と、LNGの包括的な液化プロセス、輸送、流通をサポートする補助的な機能向けのCSFプロファイルのガイダンスNIST IR 8406「Cybersecurity Framework Profile for Liquefied Natural Gas」を2023年6月8日に発表した※169。同ガイダンスは、サイバーセキュリティ活動を管理し、LNGプロセス全体にわたるサイバーリスクを低減するための、自主的でリスクベースのアプローチを提供している。LNG CSFプロファイルは、既存のサイバーセキュリティガイダンスや方針に取って代わるものではなく、LNG業界が既に使用している現行のサイバーセキュリティ基準、規制、業界ガイドラインを補足するものであり、LNG組織が提供する推奨事項の優先順位付けを利害関係者が支援することで、既存のベストプラクティスを補完することを意図している。

NCCoEは、ハイブリッド衛星ネットワーク（HSN：Hybrid Satellite Network）のためのCSFプロファイル「NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks（HSN）」の最終版を2023年9月に公開した※170。HSN CSFプロファイルを

使用することで、組織はHSNに関連するシステム、資産、データ、リスクを識別でき、自己アセスメントを実施し、サイバーセキュリティ原則を遵守することによりHSNサービスを保護することができる。またHSNサービスやデータのサイバーセキュリティに関連した妨害や破損を検出することができ、タイムリーで有効かつレジリエンス力のある方法でHSNサービスやデータの異常に対応することができる。更に、サイバーセキュリティインシデント後にHSNを適切な動作状態に回復することができる。

(3) EUの取り組み

欧州連合（EU：European Union）の欧州委員会（European Commission）は、2022年9月に同委員会が提案した「EUサイバーレジリエンス法案（EU Cyber Resilience Act）」について、欧州議会（European Parliament）及び欧州理事会（European Council）との間で政治的合意に達した、と2023年12月1日に発表した※171。同法律は既存の法律、特に2022年に採択された「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（NIS2指令）」を補完するもので、オープンソースソフトウェアや、医療機器、航空機器、自動車等、既存の規則で既に対象になっているサービス等、特定の除外項目以外の、他のデバイスやネットワークに直接または間接的に接続されるすべての製品に適用される。同法案の重要な要素は、製品のライフサイクル全体をカバーすることであり、特に、製造業者と開発者に対して、製品が使用されると予想される期間を反映したサポート期間を定め、その期間中にセキュリティアップデートを提供する義務を規定している。今回の合意は、欧州議会と欧州理事会の正式な承認が必要となり、承認されれば、同法律は官報に掲載されてから20日目に発効する（2024年初頭発効予定）（欧州の政策については「2.2.3 (2) サイバーセキュリティ政策」参照）。

(4) オーストラリア政府の取り組み

オーストラリアのCyber and Infrastructure Security Centre（CISC）は、重要インフラの責任主体及び直接の利害関係者の義務を簡素化し、運用のレジリエンスを向上させ、複雑さを軽減することを目的とした「重要インフラ資産クラス定義ガイダンス」を2023年5月に公開した※172。同ガイダンスでは、2018年の「重要インフラ安全保障法（Security of Critical Infrastructure Act：SOCI Act）※173」及びSOCI定義規則（LIN 21/039）※174で重要インフラ資産が定義されているので、自らの資産が重要インフラ資産かどうかを判断する際に、これらを参照するよう資産所有者及び運用者に呼びかけている。

3.4.4 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について述べる。

(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。

NISCが、2022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をまとめた「サイバーセキュリティ2023（2022年度年次報告・2023年度年次計画）」を2023年7月に発表した※175。また同月、NISCの重要インフラグループは、2022年6月に策定した「重要インフラのサイバーセキュリティに係る行動計画」に基づき、各重要インフラの安全基準等の策定・改定を支援するために策定された「重要インフラのサイバーセキュリティに係る安全基準等策定指針」を発表した※176。

NISC、総務省、経済産業省は、2023年8月にベトナム・ハノイにて「重要インフラ防護ワークショップ」を開催し、「重要インフラ防護」をテーマとした研究開発の動向や、クラウド環境におけるセキュリティリスク、セキュリティ成熟度に関する知見や官民の取り組み等に関する情報交換を行った※177。

経済産業省及び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、国務省）及びEU政府（通信ネットワーク・コンテンツ・技術総局）と連携し、2023年10月9日から13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イベントを東京にて4年ぶりに対面開催した※178。インド太平洋地域（ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾）から招聘した35名の政府機関・産業界の実務者が、ハンズオン演習及び専門家によるサイバーセキュリティセミナーに参加した（「2.2.1 (3) (e) 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」参照）。

（2）IPA の取り組み

2023 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分析普及活動

制御システムのセキュリティリスク分析は、制御システム分野や重要インフラに関わる多くの事業者にとって、セキュリティレベルの抜本的な向上と継続的な維持見直しの達成に必要不可欠である。IPA は、制御システムのセキュリティリスク分析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）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、2023 年 6 ～ 9 月と、2023 年 12 月～ 2024 年 3 月の 2 回開催した。同セミナーでは、約 420 の企業・団体が参加した。

（b）調査報告書等の公開

制御システムのネットワークのオープン化、制御機器の OS のオープン化に伴い、産業用制御システムにおいてもセキュリティ対策強化のために侵入検知製品の導入が検討されるようになった。IPA は、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に、「産業用制御システム向け侵入検知製品等の導入手引書」を 2023 年 6 月に公開した※ 179。同手引書は、侵入検知製品等の基礎知識から導入にあたって検討すべきこと、そして具体的な導入の進め方について、実際に侵入検知製品を利用している事業者への聞き取り調査を基に紹介している。

2023 年 7 月には、工場における具体的な対策への指針を提供するため、先進的なスマート工場の事例を調査して対策項目を整理した「スマート工場化でのシステムセキュリティ対策事例 調査報告書」を公開した※ 180。同報告書は、工場設備のセキュリティ管理責任者等が、スマート工場の生産システムにおけるセキュリティ対策を実施する際の参考書として利用されることを想定している。別紙には「セキュリティ対策内容の一覧と各種ガイドラインとの対応」を掲載しており、経済産業省による「サイバー・フィジカル・セキュリティ対策フレームワーク※ 181」や「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 付録 E※ 182」の実践を検討する際に利用できる。

また、「3.4.3（1）米国 CISA の取り組み」で前述した、米国 CISA が 2023 年 3 月に発行した「Cross-Sector Cybersecurity Performance Goals Ver.1.0.1（2023-03）」を翻訳し、2023 年 8 月に公開した※ 183。

（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に対応する人材の育成を支援している（「2.3.3（2）産業システムセキュリティ人材育成のための活動」参照）。

3.5 IoTのセキュリティ

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）へのサイバー攻撃が後を絶たない。ウイルス感染したIoT 機器のボットネットによるDDoS（Distributed Denial of Service）攻撃に、日本国内のウイルス感染したIoT 機器も悪用されており、国内のIoT 機器への感染拡大攻撃が観測されている。

本節では、「IoTに対するセキュリティ脅威の動向」「進化を続ける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（End-of-Life）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、本節では脆弱性情報の詳細を省略しているが、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3-5-1 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※184
JVNDB-20xx-xxxxxx	JVN iPedia※185
EDB-ID: xxxxx	Exploit Database※186

■表3-5-1　脆弱性の登録ID の表記例と登録先データベース

3.5.1 IoTに対するセキュリティ脅威の動向

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、2023 年に観測されたセキュリティ脅威の動向を紹介する。

(1) ルーターに対する脅威

ウイルス感染させて機器を乗っ取り、第三者への攻撃に悪用する目的に合致するルーターに対して、その脆弱性を狙う脅威が継続している。

(a) Synology 社製ルーターに対する脅威

2022 年12 月22 日、Synology Inc.（群暉科技股份有限公司。以下、Synology 社）は、同社製ルーター用オペレーティングシステムSynology Router Manager において、任意のコマンド実行やDoS（Denial of Service）状態、任意のファイル読み取りに至る恐れがある、以下に示す脆弱性に関するアドバイザリーを公開し、2023 年1 月6 日及び5 月16 日に更新して脆弱性の詳細を追加した※187。

- CVE-2023-32956
- CVE-2022-43932（JVNDB-2022-004427）
- CVE-2023-32955
- CVE-2023-0077（JVNDB-2023-001518）

(b) TP-Link 社製ルーターに対する脅威

2023 年1 月17 日、TP-Link Technologies Co., Ltd.（普联技术有限公司。以下、TP-Link 社）製ルーターTL-WR710N V1（ファームウェアバージョン151022）及びArcher C5 V2（ファームウェアバージョン160201）において、リモートコード実行等を引き起こす可能性がある、以下に示す脆弱性が報告された※188。

- CVE-2022-4498（JVNDB-2023-001959）
- CVE-2022-4499（JVNDB-2023-001965）

2023 年4 月24 日、TP-Link 社製Wi-Fi ルーターArcher AX21 において、管理者権限で任意のコード実行を可能とする脆弱性（CVE-2023-1389（JVNDB-2023-005522））のアドバイザリーが公開された※189。TP-Link 社は、3 月17 日の時点で更新ファームウェアを公開していた※190。4 月11 日以降、Mirai の亜種による同脆弱性の悪用が観測されている※191。

2023 年5 月16 日、欧州の外交機関を狙った中国の国家支援型※192APT（Advanced Persistent Threat）グループ「Camaro Dragon」によるサイバー攻撃において、悪意のあるコード（リモートシェル機能、ファイル転送機能、SOCKS トンネリング機能等）を追加されたファームウェアに書き換えられたTP-Link 社製ルーターWR940N 等が用いられていることが報告された※193。ファームウェアの改変方法やその悪用方法は不明である。

(c) NetComm 製ルーターに対する脅威

2023 年1 月17 日、NetComm Wireless Limited（現在はCasa Systems, Inc. の一部門）製ルーターNF20MESH／NF20／NL1902 において、未認証のリモート攻撃者による任意のコード実行に至る可能性がある、以下に示す脆弱性が報告された※194。

- CVE-2022-4873
- CVE-2022-4874

(d) Cisco 社製ルーター等に対する脅威

2023 年 2 月 1 日、Cisco Systems, Inc.（以下、Cisco 社）製の産業用アプライアンス（ルーターやゲートウェイ、ワイヤレスアクセスポイント等）において、認証済みリモート攻撃者によるコマンドインジェクションを可能とする、以下に示すゼロデイ脆弱性の情報が公開された※195。また、Cisco 社の緩和策を回避し、再起動やファームウェア更新後も悪意のあるコードが残留し続けることが指摘された。

- CVE-2023-20076（JVNDB-2023-004067）
- Cisco バグ ID：CSCwc67015

同日、Cisco 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※196。

2023 年 10 月 16 日、Cisco 社は、同社製ルーターやスイッチで採用されている Linux ベースのオペレーティングシステム IOS XE の Web インターフェースにおけるゼロデイ脆弱性（CVE-2023-20198（JVNDB-2023-004217））を公開した※197。翌 17 日、インターネット上で同インターフェースを使用している 6 万 7,445 台の機器が特定されて、うち 3 万 4,140 台が侵害を受けてバックドアを設置されていた※198。同月 20 日、Cisco 社は、もう一つのゼロデイ脆弱性（CVE-2023-20273）を追加公開した。二つの脆弱性を組み合わせた悪用が大規模侵害の要因と考えられており、同月 22 日に Cisco 社は更新ファームウェアを公開した。

(e) NETGEAR 社製ルーターに対する脅威

2023 年 5 月 11 日、NETGEAR, Inc.（以下、NETGEAR 社）製ルーター Nighthawk RAX30 において、非認証のリモートコード実行、コマンドインジェクション、認証バイパスに至る恐れがある、以下に示す脆弱性の情報が公開された※199。

- CVE-2023-27357
- CVE-2023-27367
- CVE-2023-27368
- CVE-2023-27369
- CVE-2023-27370

(f) ASUS 社製ルーターに対する脅威

2023 年 6 月 19 日、ASUSTeK Computer Inc.（華碩電脑股份有限公司。以下、ASUS 社）製ルーター 18 機種において、以下に示す脆弱性を含むセキュリティ修正の更新ファームウェアが公開された※200。

- CVE-2023-28702（JVNDB-2023-007784）
- CVE-2023-28703（JVNDB-2023-007783）
- CVE-2023-31195（JVNDB-2023-000048）
- CVE-2022-46871（JVNDB-2022-003994）
- CVE-2022-38105（JVNDB-2022-004975）
- CVE-2022-35401（JVNDB-2022-005048）
- CVE-2018-1160（JVNDB-2018-014397）
- CVE-2022-38393（JVNDB-2022-004974）
- CVE-2022-26376（JVNDB-2022-014335）

2023 年 9 月 5 日、ASUS 社ルーター RT-AX55、RT-AX56U_V2、RT-AC86U における、以下に示す脆弱性が公開された※201。

- CVE-2023-39238（JVNDB-2023-011977）
- CVE-2023-39239（JVNDB-2023-011976）
- CVE-2023-39240（JVNDB-2023-011975）

これらの脆弱性を悪用されると、リモートコード実行、サービス中断、機器上での任意の操作に至る恐れがある※202。

(g) MikroTik RouterOS の脆弱性

2023 年 7 月 25 日、SIA Mikrotīkls 製ルーターの MikroTik RouterOS において、管理者から特権管理者への権限昇格を可能とする脆弱性（CVE-2023-30799（JVNDB-2023-023345））が報告された※203。2022 年 10 月に更新ファームウェアが提供されているが、インストールされていないルーターが数多く存在し、Shodan※204 を用いた検索によって、Web ベースの管理インターフェース経由でアクセス可能な約 50 万台、MikroTik 管理ツール Winbox 経由で接続可能な約 90 万台の存在が確認されている。また、サンプルとして調査された 5,500 台のうちの 60% 近くが、同脆弱性を悪用したブルートフォース攻撃の標的となり得る初期設定の管理者アカウント「admin」を使用していることが報告された。

(h) Sierra Wireless 社製ルーターに対する脅威

2023 年 12 月 6 日、Sierra Wireless, Inc.（現在は Semtech Corporation の一部門）製 OT/IoT 向けセルラールーター※205AirLink シリーズにおける 21 種類の脆弱性が発見され、「Sierra:21」と名付けられた※206。イ

ンターネット上に 8 万 6,000 台以上の接続が検出され、2019 年以降に発見された脆弱性に対応する修正プログラムが適用されていたのは 10% 未満であった。

(i) バッファロー社製 VPN ルーターに対する脅威

2023 年 12 月 25 日、株式会社バッファローは、同社製 VPN ルーター VR-S1000 において、任意のコマンド実行や機密情報の窃取に至る恐れがある、以下に示す脆弱性の情報と更新ファームウェアを公開した※207。

- CVE-2023-45741※208（JVNDB-2023-000125）
- CVE-2023-46681※208（同上）
- CVE-2023-46711※208（同上）
- CVE-2023-51363※209（同上）

(2) NAS に対する脅威

2022 年に続いて、NAS（Network Attached Storage）の脆弱性を狙う脅威の増加傾向が続いている。

(a) QNAP 社製 NAS に対する脅威

2023 年 1 月 30 日、QNAP Systems, Inc.（威聯通科技股份有限公司。以下、QNAP 社）は、同社製 NAS において、リモート攻撃者による悪意のコード挿入を可能とする脆弱性（CVE-2022-27596（JVNDB-2023-002361））と更新ファームウェアの情報を含むアドバイザリーを公開した※210。同月 31 日、影響を受けるバージョンのファームウェアを搭載した 2 万 9,968 台の NAS がインターネット上に接続されていることが報告された※211。

2023 年 3 月 30 日、QNAP 社は、同社製 NAS で用いられているオペレーティングシステム QTS、QuTS hero、QuTScloud、QVP において、機密データへのアクセスを可能として、最終的に任意のコード実行に至る恐れがある、以下に示す脆弱性と更新ファームウェアの情報を含むアドバイザリーを公開した※212。

- CVE-2022-27597（JVNDB-2022-022069）
- CVE-2022-27598（JVNDB-2022-022070）

2023 年 11 月 4 日、QNAP 社は、同社製 NAS で用いられているオペレーティングシステム QTS、QuTS hero、QuTScloud において、リモートコード実行に至る恐れがある、以下に示す脆弱性と更新ファームウェアの情報を含むアドバイザリーを公開した※213。

- CVE-2023-23368（JVNDB-2023-016900）
- CVE-2023-23369（JVNDB-2023-016901）

(b) Western Digital 社製 NAS に対する脅威

2023 年 6 月 13 日、Western Digital Corporation（以下、Western Digital 社）は、同社製 NAS における以下に示す脆弱性に対応する更新用ファームウェアを公開するとともに、ファームウェアを更新していない NAS による同社のクラウドサービス MyCloud への接続を拒否すると表明した※214。

- CVE-2022-36326（JVNDB-2022-024385）
- CVE-2022-36327（JVNDB-2022-024376）
- CVE-2022-36328（JVNDB-2022-024384）
- CVE-2022-29840（JVNDB-2022-024334）
- CVE-2023-22814（JVNDB-2023-017273）

2023 年 8 月 9 日、Western Digital 社製 MyCloud PR4100 NAS における以下に示す脆弱性を悪用し、同社製 NAS になりすましてクラウドサービス MyCloud に接続することによって、同サービスに接続されたすべての NAS へのアクセスやリモートコード実行が可能であることが報告された※215。

- CVE-2022-36331（JVNDB-2022-024074）
- CVE-2022-36328（JVNDB-2022-024384）
- CVE-2022-29841（JVNDB-2022-024333）
- CVE-2022-36327（JVNDB-2022-024376）

Western Digital 社は、2022 年 12 月 21 日、2023 年 1 月 10 日、同年 5 月 15 日に更新ファームウェアを含むアドバイザリーを公開済みであった※216。

(c) Zyxel 社製 NAS に対する脅威

2023 年 6 月 20 日、Zyxel Networks Corporation（合勤科技股份有限公司。以下、Zyxel 社）製は、同社製 NAS326、NAS540、NAS542 における、リモートコマンド実行に至る恐れがある、コマンドインジェクション脆弱性（CVE-2023-27992（JVNDB-2023-010595））と更新ファームウェアの情報を含むアドバイザリーを公開した※217。

2023 年 11 月 30 日、Zyxel 社は、同社製 NAS326、NAS542 における、OS コマンド実行に至る恐れがある、以下に示す脆弱性と更新ファームウェアの情報を含むアドバイザリーを公開した※218。

- CVE-2023-35137
- CVE-2023-35138
- CVE-2023-37927
- CVE-2023-37928
- CVE-2023-4473

- CVE-2023-4474

(d) Synology 社製 NAS に対する脅威

2023 年 8 月 9 日、Synology 社製 NAS DS920+ における以下に示す脆弱性を悪用し、同社製 NAS になりすましてクラウドサービス QuickConnect に接続しておき、クラウドサービス利用者を攻撃者の管理下にある NAS にリダイレクトすることによって、認証情報の窃取を行い、最終的に利用者データへのアクセス、リモートコード実行が可能であることが報告された※219。

- CVE-2024-0860
- CVE-2024-27769
- CVE-2024-27770
- CVE-2024-27771
- CVE-2024-27768

2023 年 10 月 17 日、Synology 社製 NAS に搭載されている Linux ベースのオペレーティングシステム DiskStation Manager（DSM）において、管理者パスワード生成時、Web ブラウザー上のセキュアでない疑似乱数生成（PRNG：Pseudo Random Number Generator）関数を用いており、実際の悪用は困難であるものの、パスワードを推定される恐れがある脆弱性（CVE-2023-2729）が報告された※220。

(3) DVR/NVR に対する脅威

同一機種や同等機種が世界中に散在する傾向のある DVR/NVR（Digital Video Recorder/Network Video Recorder）の脆弱性を狙う脅威が継続している。

(a) TBK Vision 社製 DVR に対する脅威

2023 年 5 月 1 日、TBK Vision 社製 DVR である TBK-DVR4104 及び TBK-DVR4216 において、5 年前に発見された認証バイパス／管理者権限取得の脆弱性（CVE-2018-9995（JVNDB-2018-004376））を悪用する攻撃の試みが観測され、最大 5 万以上の侵入防止システム（IPS：Intrusion Prevention System）において検出された※221。TBK Vision 社の製品は、世界各国の銀行・小売業・政府機関等において 60 万台以上のカメラ、5 万台以上のレコーダーが設置されている上、様々なブランドの OEM（Original Equipment Manufacturer）製品としても販売されており、公開済みの PoC（Proof of Concept）※222 コードと組み合わせて容易に攻撃可能なため、攻撃者の格好の標的となっている。

(b) QNAP 社製 NVR に対する脅威

2023 年 12 月 9 日、QNAP 社は、同社製 VioStor NVR の脆弱性情報と更新ファームウェアの適用方法を含むアドバイザリーを公開した（「3.5.2 (1) (g) InfectedSlurs」参照）※223。

(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引き続き発生している。

(a) コネクテッドカーにおける API の脆弱性

2024 年 1 月 3 日、約 20 社の自動車メーカー及び自動車サービスのテレマティクスシステム、オートモーティブ API、それらをサポートするインフラストラクチャを調査した結果、リモートからのロック／ロック解除、エンジン始動／停止、ヘッドライトの点滅、正確な位置の特定等を可能とする脆弱性を発見したことが公開された※224。

(b) テスラ社製電気自動車のインフォテインメントシステムの脆弱性

2023 年 8 月 9 日、BlackHat USA 2023 において、Tesla, Inc.（以下、テスラ社）製自動車で採用されているインフォテインメントシステムを制御する MCU（Media Control Unit）上の AMD（Advanced Micro Devices, Inc.）製プロセッサ（MCU-Z）の脆弱性を悪用し、管理者権限で任意のソフトウェアを実行可能とする「Tesla Jailbreak」の有効化や、テスラ社の内部サービスネットワークで車両の認証・認可に用いられる車両固有の RSA 暗号鍵の抽出が可能であることが発表された※225。

(c) Syrus 4G IoT ゲートウェイの脆弱性

2023 年 12 月 8 日、Digital Communications Technologies LLC（以下、DCT 社）製の車載用テレマティクスゲートウェイ Syrus 4G IoT Gateway において、搭載車両の遠隔操作に加えて、サーバー経由で他の搭載車両への攻撃に悪用可能な脆弱性（CVE-2023-6248（JVNDB-2023-018248））が報告された※226。49 ヵ国以上で 11 万 9,000 台以上の自動車に搭載されており、米国及びラテンアメリカ全土で 4,000 台以上の車両がリアルタイムでサーバーに接続されていることが確認された。同脆弱性は、2023 年 4 月、発見者によって DCT 社に報告されたが、同社の対応は遅く、更新ファームウェアは未提供のため、情報が開示された。

(5) IP 電話機に対する脅威

インターネットを介して電話機能を提供する IP 電話機に対する脅威が発生している。

(a) Cisco 社製 IP 電話機に対する脅威

2023 年 3 月 1 日、Cisco 社は、同社製 IP 電話機 6800/7800/8800 シリーズの Web ベース管理インターフェースにおける、非認証のリモート攻撃者による任意のコード実行や DoS 攻撃に至る恐れがある、以下に示す脆弱性と更新ファームウェアの情報を含むアドバイザリーを公開した※227。

- CVE-2023-20078（JVNDB-2023-003782）
- CVE-2023-20079（JVNDB-2023-003789）

(b) AudioCodes 社製 IP 電話機に対する脅威

2023 年 8 月 10 日、BlackHat USA 2023 において、Zoom の ZTP（Zero Touch Provisioning）機能※228 及び同機能を実装した AudioCodes Ltd.（以下、AudioCodes 社）製 IP 電話機 C450HD における脆弱性を悪用し、盗聴や電話機の遠隔制御、企業内ネットワークへの侵入拠点としての使用が可能であることが報告された※229。

(6) 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) シュナイダー社製 UPS に対する脅威

2024 年 4 月 11 日、Schneider Electric SE（以下、シュナイダー社）は、同社製 APC UPS 用の設定・管理用ツール（APC Easy UPS Online Monitoring Software）において、悪意の Web コードの実行や機器の機能停止に至る恐れがある、以下に示す脆弱性に関するセキュリティ通知を公開し、ソフトウェアの更新を呼びかけた※230。

- CVE-2023-29411（JVNDB-2023-008892）
- CVE-2023-29412（JVNDB-2023-008891）
- CVE-2023-29413（JVNDB-2023-008890）

(b) キヤノン製ネットワークプリンターに対する脅威

2023 年 7 月 31 日、キヤノン株式会社は、同社製インクジェットプリンターの Wi-Fi 接続設定に関する機密情報が通常の初期化処理では削除できない場合があるため、修理・貸与・廃棄等、プリンターが第三者に渡る可能性がある場合の脆弱性軽減策及び修復策を公開した※231。

(c) D-Link 社製 Wi-Fi 中継器に対する脅威

2023 年 10 月 9 日、D-Link Corporation（以下、D-Link 社）製 Wi-Fi 中継器（Mesh Range Extender）DAP-X1860 における、リモートコマンドインジェクションの脆弱性（CVE-2023-45208（JVNDB-2023-014619））の情報が報告された※232。2024 年 1 月 3 日、D-Link 社は更新ファームウェアを公開した。

(d) Zyxel 社ファイアウォール／アクセスポイントに対する脅威

2023 年 11 月 28 日、Zyxel 社は、同社製ファイアウォール及びアクセスポイントにおける、以下に示す脆弱性と更新ファームウェアの情報を含むアドバイザリーを公開した※233。

- CVE-2023-35136（JVNDB-2023-018208）
- CVE-2023-35139（JVNDB-2023-018209）
- CVE-2023-37925（JVNDB-2023-018206）
- CVE-2023-37926（JVNDB-2023-018207）
- CVE-2023-4397（JVNDB-2023-018204）
- CVE-2023-4398（JVNDB-2023-018205）
- CVE-2023-5650（JVNDB-2023-018516）
- CVE-2023-5797（JVNDB-2023-018515）
- CVE-2023-5960（JVNDB-2023-018118）

3.5.2 進化を続ける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、IoT ウイルスによる攻撃手段としての悪用例が後を絶たない。本項では、ウイルスの進化の観点から、2023 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、2023 年も既存の亜種が進化するとともに新たな亜種が発生し、感染活動を継続している。

(a) Medusa

2023 年 2 月 3 日、2015 年から存在するボットネット「Medusa」に関して、Mirai のソースコードをベースとした新しいバージョンの発見が報告された※234。従来版が持っていた DDoS 攻撃機能に加えて、暗号資産マイニ

ング MaaS（Malware as a Service）機能※235 やランサムウェア機能を備えている。

(b) V3G4

2023 年 2 月 15 日、Mirai の新たな亜種「V3G4」の観測結果が報告された※236。2022 年 7 ～ 12 月の活動において、以下に示す様々な脆弱性を感染拡大に悪用していたことが観測されている。

- CVE-2012-4869（JVNDB-2012-004164）
- EDB-ID: 18393
- CVE-2014-9727
- EDB-ID: 15807
- CVE-2017-5173（JVNDB-2017-004263）
- CVE-2019-15107（JVNDB-2019-008300）
- Spree Commerce の任意のコマンド実行の脆弱性
- EDB-ID: 42788
- CVE-2020-8515（JVNDB-2020-001735）
- CVE-2020-15415（JVNDB-2020-007241）
- CVE-2022-36267（JVNDB-2022-014384）
- CVE-2022-26134（JVNDB-2022-011115）
- CVE-2022-4257（JVNDB-2022-022187）

(c) Moobot

2023 年 3 月 29 日、Mirai の亜種「Moobot」※237 の活動が継続しており、以下に示す脆弱性を悪用して感染拡大を試みていることが報告された※238。

- Realtek 社製無線機器向け Jungle SDK の脆弱性※239（CVE-2021-35394（JVNDB-2021-010965））
- CVE-2022-46169（JVNDB-2022-022114）

(d) Zyxel 社製ファイアウォールへの攻撃

2023 年 5 月 19 日、Zyxel 社製ファイアウォールにおけるコマンドインジェクションの脆弱性（CVE-2023-28771（JVNDB-2023-009227））は、同年 4 月 25 日に Zyxel 社から修正プログラムの適用を促すアドバイザリー※240 が公開されたが、インターネット上に約 4 万 2,000 のインスタンスが存在することが警告された※241。同年 5 月 28 日、Mirai の亜種による同脆弱性の積極的な悪用が観測されている※242。同年 7 月 19 日、Mirai の亜種 Dark.IoT を含む複数のボットネットでこの脆弱性が悪用されていることが観測されている※243。

(e) IZ1H9

2023 年 4 月 10 日、Mirai の亜種「IZ1H9※244」の活動が観測された※245。以下に示す脆弱性を悪用し、インターネット上のサーバーやネットワーク機器を感染対象としている。

- CVE-2023-27076（JVNDB-2023-006940）
- CVE-2023-26801（JVNDB-2023-006313）
- CVE-2023-26802（JVNDB-2023-006314）
- Zyxel 社製 DSL（Digital Subscriber Line）製品 CPE シリーズのリモートコード実行及び DoS の脆弱性※246

2023 年 10 月 9 日、IZ1H9 が新たに複数の IoT 機器等の脆弱性（表 3-5-2）を感染拡大に悪用していることが報告された※247。

影響を受ける機器等	脆弱性ID
D-Link 社製ルーター等	CVE-2015-1187 （JVNDB-2015-007962） CVE-2016-20017 （JVNDB-2022-019711） CVE-2020-25506 （JVNDB-2020-015749） CVE-2021-45382 （JVNDB-2021-018599）
Netis Technology Co., Ltd.（网是科技股份有限公司）製ルーター Netis WF2419	CVE-2019-19356 （JVNDB-2019-014562）
Sunhillo SureLine	CVE-2021-36380 （JVNDB-2021-011031）
Geutebrück GmbH 製 IP カメラ G-Cam E2、G-Code	CVE-2021-33544 等、 合計 8 種類の脆弱性 （JVNDB-2021-002023）
Yealink Network Technology Co., Ltd.（廈門億聯網絡技術股分有限公司）製 デバイス管理（DM）	CVE-2021-27561 （JVNDB-2021-013849） CVE-2021-27562 （JVNDB-2021-007536）
TP-Link 社製ルーター Archer AX21	CVE-2023-1389 （JVNDB-2023-005522）
Korenix Technology（現 Beijer Electronics, Inc.）製 JetWave Wi-Fi AP	CVE-2023-23295 （JVNDB-2023-004598）
TOTOLINK（台灣吉翁電子股份有限公司）製 ルーター	CVE-2022-40475 （JVNDB-2022-018076） CVE-2022-25080 （JVNDB-2022-006253） 等、合計 12 種類の脆弱性
Prolink（Fida International（S）Pte Ltd.）製ルーター PRC2402M	CVE-2021-35401 ただし、攻撃コードが不完全

■表 3-5-2　IZ1H9 が新たに悪用する脆弱性と影響を受ける機器等
（出典）Fortinet, Inc.「IZ1H9 Campaign Enhances Its Arsenal with Scores of Exploits※247」を基に IPA が作成

(f) 亜種名のない Mirai の亜種

2023 年 6 月 22 日、D-Link 社、Zyxel 社、NETGEAR 社等の IoT 機器における 22 種類の脆弱性を用いて、感染拡大と DDoS 攻撃への悪用を試みる Mirai の亜種の活動が報告された※248。2023 年 3 月から活動が活発化したこの亜種は、特定を回避するためなのか、亜種名を示す文字列が含まれていない。

(g) InfectedSlurs

2023 年 11 月 21 日、2 種類のリモートコード実行に至るゼロデイ脆弱性を悪用してルーターや NVR に感染し、DDoS 攻撃用ボットネットを構築するウイルスの発見が報告され、C&C サーバー※249 の名前や内部の文字列から「InfectedSlurs」と名付けられた※250。Mirai の亜種の一つである JenX※251 から派生したと考えられている。

同年 12 月 6 日、ベンダーが更新ファームウェアとアドバイザリーを公開したことから、影響を受けるルーターが FXC 株式会社の情報コンセント対応型無線 LAN ルーター AE1021/AE1021PE であること、脆弱性が OS コマンドインジェクション脆弱性（CVE-2023-49897（JVNDB-2023-009966））であることが明らかになった※252。

同年 12 月 14 日、更新ファームウェアは 2014 年 6 月 21 日に公開済みであり、ベンダーがアドバイザリーを公開したことを受けて、影響を受ける NVR が QNAP 社の VioStor（ファームウェアバージョン 5.0.0 以前）であること、脆弱性が OS コマンドインジェクション脆弱性（CVE-2023-47565（JVNDB-2023-014789））であることが公開された※253。

(2) その他の IoT ウイルス

Mirai 等の既存ウイルスの技術（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。

(a) Hinata

2023 年 3 月 16 日、Go 言語で記述されており、DDoS 攻撃に焦点を当てた新たなウイルス「Hinata」の発見が報告された※254。最盛期の Mirai と比較して非常に攻撃能力が高く、理論上 1 万ノード（ピーク時の Mirai ボットネットの約 6.9% の規模）で 3.3Tbps 以上（UDP フラッド攻撃）、約 27Gbps ／約 20.4Mrps（HTTP フラッド攻撃）を実現可能と推測されている。これは、1% 未満のリソースで Mirai の最大級の攻撃に匹敵するトラフィックを生成可能であることを意味する※255。

(b) ShellBot

2023 年 3 月 29 日、Perl で開発された「ShellBot」（別名、PerlBot）の活動が継続しており、Moobot 同様（「3.5.2 (1) (c) Moobot」参照）の脆弱性を悪用して感染拡大を試みていることが報告された※238。ShellBot については 3 種類の異なる亜種が観測されている。

(c) AndoryuBot

2023 年 5 月 8 日、Ruckus Wireless, Inc.（現在は CommScope Holding Company, Inc. の一部門）製 Wi-Fi アクセスポイントの脆弱性（CVE-2023-25717（JVNDB-2023-004133））を悪用して感染拡大を試みる新たなボットネット「AndoryuBot」の発見が報告された※256。「Project Andoryu」と称して、DDoS 代行サービスを販売する Telegram 上のチャンネルも発見されている。

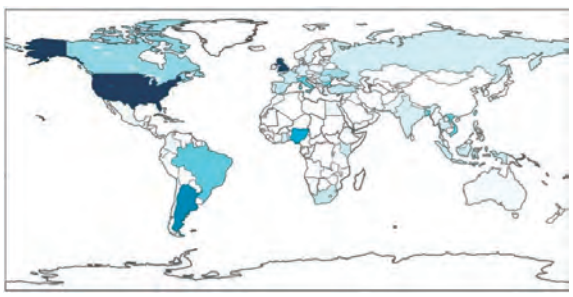
(d) GobRAT

2023 年 5 月 29 日、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）は、同年 2 月に実行された Go 言語で記述されたウイルス「GobRAT」による日本国内の Linux ベースのルーターに対する感染活動を報告した※257。

(e) AVrecon

2023 年 7 月 12 日、SOHO（Small Office/Home Office）ルーターを感染対象とし、7 万台以上に感染して 20 ヵ国以上にまたがって 4 万以上の IP アドレスを永続的に保持するボットネット「AVrecon」の活動が報告された※258（図 3-5-1）。

同月 25 日、AVrecon に感染した機器の悪用目的が residential proxy※259 であり、ウイルス感染機器を用いてプロキシーサービス（Proxy as a Service）を提供し



■図 3-5-1　AVrecon 感染機器（ボット）の世界的分布
（出典）Lumen Black Lotus Labs「Routers From The Underground: Exposing AVrecon※258」（2023 年 7 月 12 日公開）

ているとの疑いがある SocksEscort に結び付いている、との調査結果が報告された※260。

3.5.3 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。また、IoT 機器の廃棄時のリスクに関する調査結果が報告されている。本項では、これらのリスク事例を紹介する。

(1) 共通コンポーネントの脆弱性

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における脆弱性の発見は、広範囲にわたる影響やセキュリティ対策の困難性を生じている。

(a) Looney Tunables

2023 年 10 月 3 日、Fedora、Ubuntu、Debian 等の Linux の主要なディストリビューションで用いられている GNU C ライブラリの ld.so ダイナミックローダーにおける、ローカル攻撃者の管理者権限昇格に至る恐れがある脆弱性（CVE-2023-4911（JVNDB-2023-013913））が報告された※261。実行時のライブラリ動作を変更するための環境変数 GLIBC_TUNABLES の処理にバッファオーバーフローの脆弱性が存在することに起因することから、「Looney Tunables」と名付けられた。

(b) pfSense

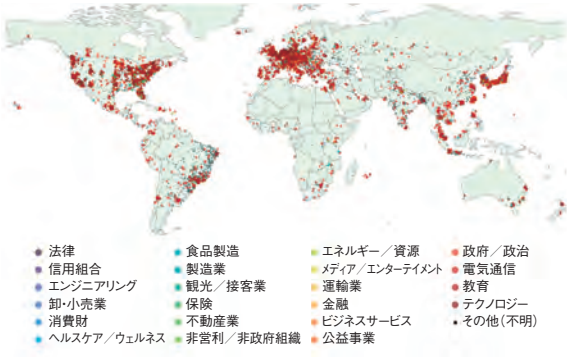
2023 年 12 月 11 日、Rubicon Communications, LLC（Netgate）が開発したオープンソースのファイアウォール／ルーター用ソフトウェア pfSense において、任意のリモートコード実行に至る恐れがある、以下に示す脆弱性と修正プログラム適用バージョンの情報が公開された※262。

- CVE-2023-42325（JVNDB-2023-016897）
- CVE-2023-42327（JVNDB-2023-016898）
- CVE-2023-42326（JVNDB-2023-017429）

(2) 標準プロトコルの脆弱性

2023 年 4 月 25 日、LAN 内のアプリケーションに動的構成メカニズムを提供するためのインターネット標準プロトコル SLP（Service Location Protocol）において、最大 2,200 倍の増幅率の大規模 DoS 増幅攻撃を可能とする恐れがある脆弱性（CVE-2023-29552（JVNDB-2023-001760））が報告された※263。同年 2 月の時点において、2,000 以上の世界中の組織で 670 種類以上の製品、5 万 4,000 以上の実装の存在が確認されている（図 3-5-2）。

同 4 月 25 日、CISA は警告を公開した※264。



■図 3-5-2　確認された SLP の実装の国・地域・事業分野別分布
（出典）BitSight Technologies, Inc.「New high-severity vulnerability (CVE-2023-29552) discovered in the Service Location Protocol (SLP)※263」を基に IPA が編集

(3) 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 機器において、新たな脆弱性が発見されている。

(a) Cisco 社製 EOL ルーターの脆弱性

2023 年 1 月 11 日、Cisco 社は、2016 年 5 月 5 日及び 2021 年 1 月 29 日にソフトウェアメンテナンスサポートを終了した同社製 VPN ルーター RV016、RV042、RV042G、RV082、RV320、RV325 において、任意のコマンド実行に至る恐れのある以下の脆弱性を公開し、更新ファームウェアを提供しないことを表明した※265。

- CVE-2023-20025（JVNDB-2023-002344）
- CVE-2023-20026（JVNDB-2023-002358）
- CVE-2023-20118（JVNDB-2023-008395）

同月 20 日には、インターネット上に約 2 万台の当該ルーターが残されていることが報告された※266。

(b) Cisco 社製電話アダプターの脆弱性

2023 年 5 月 3 日、Cisco 社は、2020 年 6 月 1 日に脆弱性対策及びセキュリティのサポートを終了した電話アダプター（アナログ電話機を VoIP ネットワークに接続するためのアダプター）SPA112 の Web ベース管理インターフェースにおいて、非認証のリモート攻撃者による任意のコード実行に至る恐れのある脆弱性（CVE-2023-20126（JVNDB-2023-009752））を公開し、更新ファームウェア

を提供しないことを表明した※267。

(c) Socomec 社製 UPS に対する脅威

2023 年 9 月 7 日、CISA は、SOCOMEC Group S.A.（以下、Socomec 社） 製 UPS MODULYS GP（MOD3GP-SY-120K）における、以下の脆弱性に関するアドバイザリーを公表した※268。

- CVE-2023-38582（JVNDB-2023-012762）
- CVE-2023-39446（JVNDB-2023-012760）
- CVE-2023-41965（JVNDB-2023-012905）
- CVE-2023-41084（JVNDB-2023-012894）
- CVE-2023-40221（JVNDB-2023-012895）
- CVE-2023-39452（JVNDB-2023-012759）
- CVE-2023-38255（JVNDB-2023-012892）

Socomec 社は、同製品が 2014 年に生産終了した EOL であることから、現行製品への移行を推奨している。

(4) IoT 機器の廃棄時のリスク

2023 年 4 月 18 日、スロバキアのサイバーセキュリティ企業 ESET, spol. s r.o. が廃棄されて二次市場で流通している企業向けルーター 16 台を入手して調査した結果、56% 以上（9 台）に企業の機密データが残存していたことが報告された※269。顧客データ、第三者によるネットワーク接続を可能とする情報、他のネットワークに接続するための資格情報、ルーター間の認証用暗号鍵、IPsec または VPN の認証情報、ハッシュ化された管理者パスワード、以前の所有者・使用者を特定するための情報等が含まれており、IoT 機器のライフサイクルの最終段階（廃棄フェーズ）のセキュリティ対策が十分に実施されていないことが露呈した。

3.5.4 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 NICT 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）※270」を継続中である。2024 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 83 社、調査対象 IP アドレスは約 1.12 億アドレスである。2023 年 1 月以降の取り組み結果を表 3-5-3 に示す。

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）
2023 年 1 月	4,254 件	1日平均 772 件
2023 年 2 月	4,136 件	1日平均 650 件
2023 年 3 月	4,176 件	1日平均 516 件
2023 年 4 月	4,685 件	1日平均 388 件
2023 年 5 月	4,888 件	1日平均 533 件
2023 年 6 月	5,063 件	1日平均 571 件
2023 年 7 月	5,122 件	1日平均 702 件
2023 年 8 月	5,055 件	1日平均 1,088 件
2023 年 9 月	5,162 件	1日平均 808 件
2023 年 10 月	5,162 件	1日平均 817 件
2023 年 11 月	5,181 件	1日平均 1,438 件
2023 年 12 月	5,190 件	1日平均 672 件
2024 年 1 月	5,443 件	1日平均 939 件
2024 年 2 月	5,492 件	1日平均 964 件
2024 年 3 月	5,402 件	1日平均 1,111 件

■表 3-5-3　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「最近の観測状況※271」を基に IPA が作成

- 「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 月の調査対象プロトコル（HTTP(S)）の追加によって大幅に増加した後、参加 ISP の増加（2022 年 12 月時点の 74 社から、2024 年 3 月時点では 83 社に増加）に伴う微増が見られるものの、実態として 1 年間をとおして大きな変化はないと考えられる。
- 「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 月下旬以降の国内の脆弱な機器（主に DVR/NVR）の感染拡大による増加が継続しており、更に 2023 年 10 月中旬以降、Mirai の亜種の活動活発化の影響による増加（2023 年 10 月 23 日に過去最大値 6,300 件／日を記録）が見られる。

(2) 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※272。2023 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 3-5-4 に示す。

年月	観測された主な攻撃
2023 年 1 月	MVPower DVR※273、NETGEAR ルーター※274、Realtek Jungle SDK（「3.5.2（1）（c）Moobot」参照）の脆弱性を狙った感染拡大攻撃※275
2 月	Realtek Jungle SDK、MVPower DVR、NETGEAR ルーターの脆弱性を狙った感染拡大攻撃※276
3 月	Realtek Jungle SDK、MVPower DVR、NETGEAR ルーター、組み込み Linux ZeroShell の脆弱性を狙った感染拡大攻撃※277
5 月	Realtek Jungle SDK の脆弱性を狙った感染拡大攻撃※278
6 月	同上※279
7 月	MVPower DVR、NETGEAR ルーターの脆弱性を狙った感染拡大攻撃※280
10 月	Cisco IOS XE の脆弱性を狙った侵害攻撃※281（「3.5.1（1）（d）Cisco 社製ルーター等に対する脅威」参照）

■表 3-5-4　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※272」を基に IPA が作成

(3) 感染機器のサイバー攻撃への悪用の実態

ウイルス感染させた IoT 機器に関する攻撃者による悪用方法の傾向を紹介する。

(a) DDoS 攻撃への悪用

DDoS 攻撃対策サービス（保護・軽減）を提供するネットワークセキュリティ事業者がウイルス感染した IoT 機器を悪用した DDoS 攻撃の実態を報告している。

- 2023 年第一四半期（1 ～ 3 月）には、南米の通信事業者を狙い、約 2 万台規模の Mirai 亜種のボットネットを含む攻撃において、DNS（Domain Name System）と UDP（User Datagram Protocol）の攻撃トラフィックを含むマルチベクトル攻撃が実行され、わずか 1 分程度であったが 1.3Tbps が観測された※282。
- 第二四半期（4 ～ 6 月）には、米国の ISP を狙い、約 1 万 1,000 台規模の Mirai 亜種ボットネットからの ACK フラッド攻撃が実行され、ピーク時に 1.4Tbps が観測された※283。
- 第三四半期（7 ～ 9 月）には、Mirai 亜種のボットネットによる UDP フラッド攻撃によって、ピーク時に 2.6Tbps が観測された※284。
- 第四四半期（10 ～ 12 月）には、欧州のクラウドサービス提供者を狙い、約 1 万 8,000 台規模の Mirai 亜種ボットネットからの五種類以上のマルチベクトル攻撃が実行され、ピーク時に 1.9Tbps が観測された※285。

2023 年 9 月 21 日に公開されたセキュリティベンダーの報告書によると、2023 年上半期にダークウェブ上で 700 以上の DDoS 攻撃サービスの広告が配信されているという※286。サービス価格は、攻撃対象の防御力等、攻撃の複雑さを決定する多数の要因によって左右され、1 日あたり 20 ドルから 1 ヵ月あたり 1 万ドルの間で設定されている。

(b) 暗号資産のマイニングへの悪用

2023 年 6 月 22 日、インターネットに接続された Linux ベースのシステム及び IoT 機器を標的とする攻撃の観測が報告された※287。最終的に、Hiveon OS（Lunix ベースのオープンソース OS）用にカスタマイズされたウイルスをダウンロードして、暗号資産（仮想通貨）のマイニング、すなわちクリプト・ジャッキングに悪用することを目的としている。

2023 年 7 月 26 日、Mirai の亜種のボットネットによる、DDoS 攻撃及び暗号資産マイニングへの悪用を目的とした Apache Tomcat サーバーへの攻撃の観測が報告された※288。

(c) 国家支援型 APT への悪用

2023 年 12 月 13 日、APT 攻撃者による秘密データ転送を目的としたボットネット KV-botnet の追跡結果が報告された※289。KV-botnet は、Cisco RV320 シリーズ、DrayTek Vigor、NETGEAR ProSAFE 等の SOHO ルーターで構成されていたが、同年 11 月 29 ～ 30 日以降は Axis Communications AB. 製の IP カメラ M1045-LW、M1065-LW、p1367-E 等の悪用開始が観測された。

KV-botnet の活動は、2022 年 7 月から 2023 年 2 月にかけて中国の国家支援型 APT グループ「Volt Typhoon」によって侵害されたネットワークの中継ノードとして機能する NETGEAR ProSAFE と共通点があり、「将来の有事の際に米国とアジア地域間の重要な通信インフラを混乱させる能力の開発を追求している」と評価されている同グループの関与が疑われている※290。

3.5.5 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、国家支援型 APT 攻撃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)法規制の強化

IoT 製品のセキュリティを規制する法律の制定・発効が各国で進められている。

(a)英国 PSTI レジーム

2023 年 4 月 29 日、英国政府は、2022 年 12 月 7 日に成立した「製品セキュリティ及び通信インフラストラクチャ法規制（Product Security and Telecommunication Infrastructure Bill）」（通称 PSTI 法）に基づいて実施される、インターネットに接続するすべての消費者向け製品に適用される最低セキュリティ基準制度「Product Security and Telecommunications Infrastructure（Product Security）Regime」の 1 年後の発効を告知した。2024 年 4 月 29 日、同制度は発効された※291。

2024 年 1 月 26 日、英国政府は同制度に関するガイダンスを更新した※292。制度へ準拠するための、考慮すべき主要条項が紹介されている。

(b)EU サイバーレジリエンス法案

2022 年 9 月 15 日に草案が発表された「EU サイバーレジリエンス法案（EU Cyber Resilience Act）」に関して、2023 年 12 月 1 日、欧州委員会は、欧州議会と欧州理事会が政治的合意に達したと発表した※293。同月 20 日、同法案（欧州議会案）が欧州理事会から欧州議会へ提出された※294（「3.4.3(3)EU の取り組み」参照）。

(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認証を与えるセキュリティラベリングの検討・導入が進んでいる。

(a)国内における適合性評価制度構築

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※73」において、現状の課題、適合性評価制度構築の目的、構築すべき適合性評価制度等について、議論を行ってきた。2023 年 5 月 15 日に中間取りまとめを公開した。同年 8 月 9 日から「IoT 製品のセキュリティ適合性評価制度における基準等の策定に向けたプレ検討委員会」を開催し、構築する適合性評価制度において求めるべきセキュリティ要件案、適合基準案、評価手順案を議論・策定し、これらに基づき実際の製品に対する適合性評価の検証を行った。2024 年 3 月 15 日に最終取りまとめを公開して、構築すべき IoT 製品に対するセキュリティ適合性評価制度の方向性について示した。

(b)米国政府の U.S. Cyber Trust Mark 発表

2023 年 7 月 18 日、米国政府は、消費者向けスマートデバイスのセキュリティラベリングとして、U.S. Cyber Trust Mark プログラムを発表した※295。NIST が発行する特定のサイバーセキュリティ基準に基づき、連邦通信委員会（FCC：Federal Communications Commission）は 2024 年にプログラムを開始予定である（「2.2.2(2)(a)(ア) U.S. Cyber Trust Mark プログラムについて」参照）。

(c)シンガポールの CLS 更新

2023 年 9 月 26 日、シンガポール首相官邸傘下の CSA（Cyber Security Agency of Singapore）は、消費者向けスマートデバイスの Cybersecurity Labelling Scheme（CLS）を更新した※296。各セキュリティ規定の要件を明確化するために、新規ドキュメント「Assessment Methodology」が追加されており、同月 22 日から有効とされている。

(3)日米の共同勧告

2023 年 9 月 27 日、日米のサイバーセキュリティ機関及び法執行機関である、NISC と警察庁、米国国家安全保障局（NSA：National Security Agency）、米国連邦捜査局（FBI:Federal Bureau of Investigation）、CISA は、共同で中国の国家支援型 APT グループ「BlackTech」の活動に関してサイバーセキュリティアドバイザリーを公開した※297。BlackTech は、ルーターのファームウェアを改ざんし、ルーターのドメイン信頼関係を悪用して、海外子会社から標的である日本や米国の本社に侵入する能力を有しており、この活動を検知して BlackTech のバックドアから機器を保護するための緩和策の実施を推奨している。

(4) IoT 機器向け軽量暗号の選定

2023 年 2 月 7 日、NIST は、IoT 機器等で利用可能な軽量暗号として、ASCON ファミリーを標準化することを決定した[※ 298]。同年 6 月 16 日、NIST は標準化プロセスの最終ラウンドに関する報告書を公開した[※ 299]。

(5) 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。2023 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 3-5-5 と表 3-5-6（次ページ）に示す。

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
経済産業省	IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド[※ 300]	IoT 機器を開発する中小企業の経営者、セキュリティ担当者・開発担当者・品質管理者	IoT 機器開発の各ライフサイクルフェーズにおけるセキュリティ対策、最初に検討すべき技術的対策	2023 年 6 月
総務省	ICT サイバーセキュリティ総合対策 2023[※ 301]	IoT セキュリティ関係者	情報通信ネットワークの安全性・信頼性の確保、サイバー攻撃への自律的な対処能力の向上、国際連携の推進、普及啓発の推進を目的として推進すべき施策	2023 年 8 月
IPA	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］[※ 302]	コンシューマー向け IoT 機器の開発者・製造者	ETSI EN 303 645 の日本語訳	2023 年 3 月
	IoT 開発におけるセキュリティ設計の手引き（2024 年 3 月版）[※ 303]	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）	2024 年 3 月
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 Ver3.0[※ 304]	カメラ付き小型 IoT 機器の製造・販売・運用・採用・廃棄に関わる各事業者	カメラ付き小型 IoT 機器に想定されるセキュリティ対策、製品ライフサイクルの各フェーズで注意すべきポイント	2023 年 9 月

■表 3-5-5　2023 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）	NIST SP 800-216: Recommendations for Federal Vulnerability Disclosure Guidelines ※305	連邦政府機関のセキュリティ担当者、情報システムを機関に提供する請負業者とその下請け業者	連邦政府内の情報システム（IoT 機器を含む）の脆弱性開示を管理するためのガイドライン	2023 年 5 月
	NIST SP 1800-36A (2nd Preliminary Draft): Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management - Enhancing Internet Protocol-Based IoT Device and Network Security - Volume A: Executive Summary ※306	IoT 機器の利用者	IP ベースの IoT 機器とネットワークのセキュリティ強化の方法（エグゼクティブサマリー）	2023 年 9 月
	同上 - Volume D: Functional Demonstrations ※306		同上（機能デモンストレーション）	
	同上 - Volume B: Approach, Architecture, and Security Characteristics ※306		同上（アプローチ、アーキテクチャ、セキュリティの特徴）	2023 年 10 月
	同上 - Volume C: How-To Guides ※306		同上（利用ガイド）	
	同上 - Volume E: Risk and Compliance Management ※306		同上（リスクとコンプライアンスの管理）	
	NIST Cybersecurity Framework 2.0 ※307	サイバーセキュリティ・プログラムの策定と指導の責任者	産業界、政府機関、その他の組織がサイバーセキュリティ・リスクを管理するためのガイダンス	2024 年 2 月

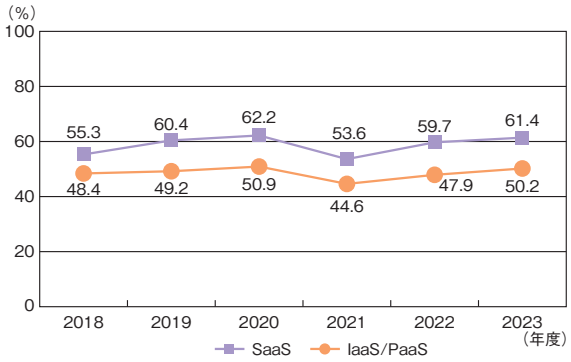
■表 3-5-6　2023 年以降に海外で新規公開・改訂された IoT 関連のガイドラインや手引き等
（出典）各団体の公開情報を基に IPA が作成

3.6 クラウドのセキュリティ

2010 年ごろを境に、もっぱらインターネットを経由してサービスを利用できる形態のソフトウェアや、ハードウェアに代わるプラットフォームが普及するようになり、今や主流となっている。これがクラウドサービス（SaaS：Software as a Service、PaaS：Platform as a Service、IaaS：Infrastructure as a Service 等）である。本節ではクラウドサービスの利用状況を俯瞰しつつ、各種のインシデントを取り上げ、クラウドサービスに関し特に注意を払うべきセキュリティ上の課題と対策を述べる。

3.6.1 クラウドサービスの利用状況

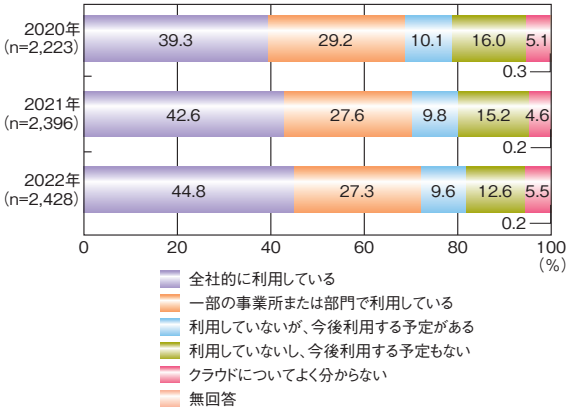
JUAS の過去 5 年間の「企業 IT 動向調査報告書[※308]」によれば、各種のクラウドサービスを「導入済み」と回答した企業の比率は図 3-6-1 のように推移している。



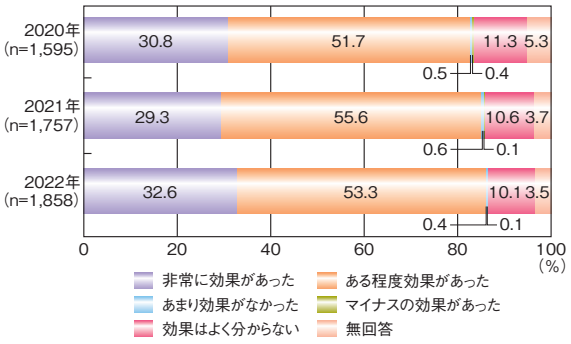
■図 3-6-1　クラウドサービスの導入状況の推移（2018～2023 年度）
（出典）JUAS「企業 IT 動向調査報告書」を基に IPA が作成

調査結果の変動はあるが、SaaS の導入企業は一貫して過半数を占め、クラウドサービスの利用はもはや特別な選択肢ではなく、定着しつつあると思われる。このことは、総務省の「令和 4 年 通信利用動向調査報告書（企業編）[※309]」において、利用している・利用予定がある企業が 7 割を超え（図 3-6-2）、実際に導入した企業では 8 割以上が効果を実感していることからもうかがわれる（図 3-6-3）。

実際にどのような用途で SaaS が利用されているかは、同じく「令和 4 年 通信利用動向調査報告書（企業編）」によって概観できる（次ページ図 3-6-4）。



■図 3-6-2　クラウドサービスの利用状況の推移（2020～2022 年）
（出典）総務省「令和 4 年 通信利用動向調査報告書（企業編）」を基に IPA が編集

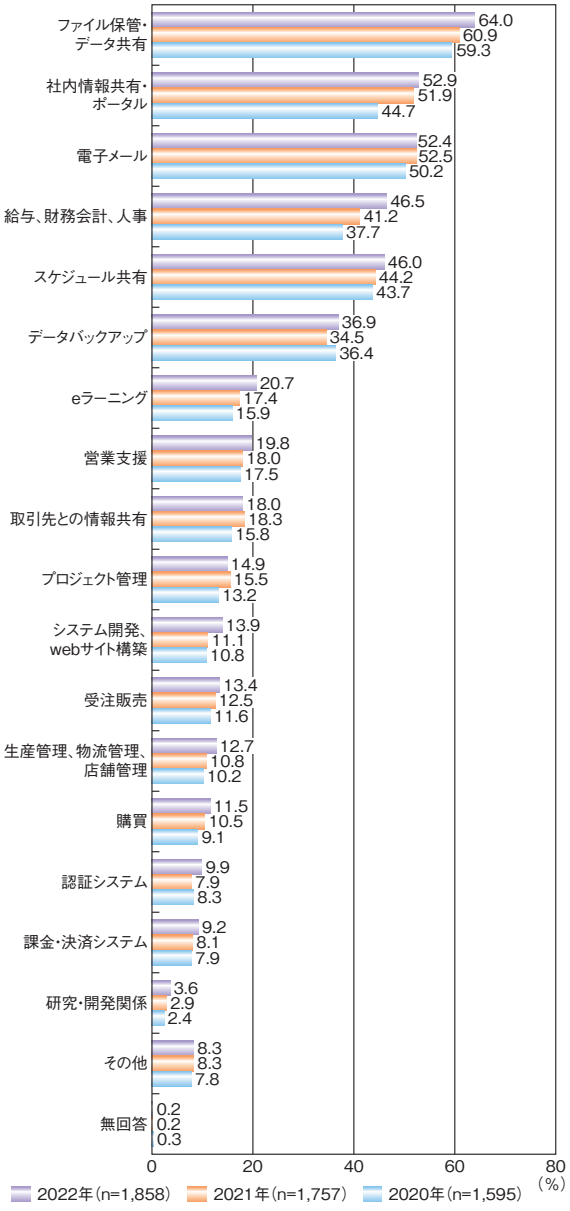


■図 3-6-3　クラウドサービスの効果の推移（2020～2022 年）
（出典）総務省「令和 4 年 通信利用動向調査報告書（企業編）」を基に IPA が編集

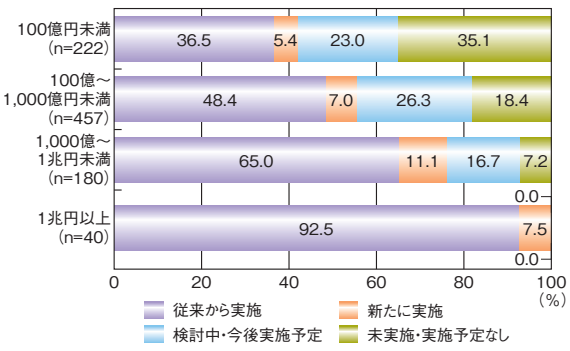
各種データの保管、共有、コミュニケーション支援を中心に活用されていることが読み取れる。これらは組織的活動をデジタルツールによって支援する際の土台であることから、SaaS が様々な組織の IT 基盤として重要な役割を果たしていると言える。

SaaS の積極的な導入は一部大企業だけに見られる動きではなく、様々な規模の企業において積極的に実施・検討される選択肢でもある。JUAS の「企業 IT 動向調査報告書 2024[※310]」では、売上高別の SaaS 活用状況を図 3-6-5（次ページ）のとおりにまとめている。

既に導入済みであるか検討中である企業（「従来から実施」「新たに実施」「検討中・今後実施予定」の合計）の割合は売上規模によらず 6 割を超えている。



■図 3-6-4　具体的に利用しているクラウドサービスの推移（複数回答、2020～2022 年）
（出典）総務省「令和 4 年 通信利用動向調査報告書（企業編）」を基に IPA が編集



■図 3-6-5　売上高別 SaaS 活用状況（2023 年）
（出典）JUAS「企業 IT 動向調査報告書 2024」を基に IPA が編集

3.6.2 クラウドサービスのインシデント事例

クラウドサービスの利用には何らかのネットワーク経由でのアクセスが欠かせない。このことはネットワークに関連するセキュリティ上の配慮が必要になるという性質を示唆し、実際にそのようなインシデントが発生している。以下では 2023 年度中に発生した事例を振り返りつつ、クラウドサービスの注目すべきセキュリティ上の特性を示す。

(1) 設定ミスによるインシデント事例

導入が容易であっても、クラウドサービスを安全に使えるかどうかは別問題である。2023 年度にも、設定ミスによる情報漏えいが発生している。

(a) SaaS 利用時の設定ミス

2023 年 12 月 7 日、インターネット関連の多様な事業を手掛ける株式会社エイチームは、クラウドサービスの設定ミスにより一部の個人情報が公開状態となっていたことを公表した※311。対象となったクラウドサービスは Google LLC（以下、Google 社）の提供する Google ドライブであり、ドライブ上のデータの公開範囲を「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」と設定していた。調査結果※312 によれば、同社サービスの利用者、取引先企業、新卒・中途採用の候補者、インターンシップに参加した一部の学生、退職者を含む従業員ら約 94 万人分の、氏名、住所、電話番号、メールアドレス等が 2017 年 3 月から 2023 年 11 月にかけて公開状態となっていた。

上記事例の背後には、社内のセキュリティ担当の目の届かないところでも容易に導入できてしまう SaaS の手軽さがあると推察される。また、クラウドサービスの性質上、サービスの機能やデータには一般にインターネットを経由したアクセスが可能であるため、これが漏えいの可能性とも結び付く。加えて、SaaS ではサービスを実行するソフトウェア本体がサービス事業者の管理するインフラ上で動くため、公開されてしまったデータに第三者からどのようなアクセスがあったのかをサービス利用者が直接に調べることが困難である。結果として、設定ミスによる情報漏えいは、その可能性が強く推認されるにとどまり、被害範囲を具体的に特定できないことが多い。

(b) IaaS/PaaS 利用時の設定ミス

2023 年 5 月 12 日、トヨタ自動車株式会社の委託を受け、トヨタコネクティッド株式会社が管理していたデータの

一部（車載端末 ID、車台番号、車両の位置情報、時刻）が、クラウド環境の設定ミスにより公開状態となっていたことが公表された※313。また、その後の同社が管理するすべてのクラウド環境を含めた調査※314によって、国内向けサービスにおける車載端末 ID、更新用地図データ、更新用地図データ作成年月の一部、及び海外（日本を除くアジア、オセアニア）向けサービスにおける顧客の住所、氏名、電話番号、メールアドレス、顧客 ID、車両登録ナンバー、車台番号の一部が、外部の第三者によりアクセス可能となっていたことが追加で判明した。該当期間は 2013 年 11 月ごろから問題公表の直前である 2023 年 5 月ごろまでに及び、実際にどの程度の不正アクセスがあったのかは定かでない。本件はその後、個人情報保護委員会による行政指導の対象となっており、漏えいの恐れのあった個人データの件数は約 230 万人分に上ることが明らかにされている※315。

2023 年 10 月 21 日、スマートフォン用の位置共有アプリ「NauNau」において 230 万人以上の位置情報と会話が外部から参照可能な状態にあったと報道された※316。その 2 日後には同アプリの開発・運営企業 Suishow 株式会社の親会社である株式会社モバイルファクトリーが報道を認め※317、同年 12 月 7 日には調査結果が公表された※318。その内容によれば、2022 年 9 月の終わりごろから 2023 年にかけて、同アプリ上で利用される最大 380 万人分の多種多様なデータが、クラウド環境の設定ミスによって外部から参照可能な状態にあった。その中には、サービス利用者の位置情報、生年月日、アプリ上での会話内容等が含まれていた。ただし、当該モバイルアプリを解析し背後のクラウドサービスを呼び出すデータを組み立てなければ不正アクセスを行うことはできず、第三者機関による調査では情報流出の事実を確認できなかったとしている。

NauNau の事例について注意すべきは、多くのモバイルアプリがクラウドサービスの一種だということである。モバイルアプリはインターネットからアクセス可能なサーバーが提供する機能やデータを基に動作することがほとんどであり、IaaS/PaaS がシステム基盤となっていることが多い。本件もそれに該当する。

(2) サイバー攻撃によるインシデント事例

クラウドサービスはインターネット越しに利用できるという性質上、インターネット経由でのサイバー攻撃を受ける対象ともなる。以下では 2023 年度に発生したクラウドサービス向けのサイバー攻撃事例をいくつか紹介する。

(a) パスワードリスト攻撃

情報漏えいは様々なサービスにおいて発生しており、Facebook や、X（旧 Twitter）といった、世界的な SNS も例外ではない。そして、漏えいした情報にサービス利用者の ID やパスワードといったアカウント情報が含まれる場合、当該のサービス利用者が同じ ID とパスワードで利用している他のサービスにも漏えいしたアカウントでアクセスできることになる。この点を突いて、不正に入手したアカウント情報を、他のサービスへのログインに用いるのがパスワードリスト攻撃である。

2023 年 3 月 20 日から 27 日にかけて、エン・ジャパン株式会社が運営する転職支援サービスに対し大量の不正ログインが発生した※319。不正ログインの対象となったのは、同サービスに登録された Web 履歴書のうち、25 万 5,765 名分である。不正ログインが特定のアクセス元（IP アドレス群）から行われていたことから、同社は当該通信をブロックした。

2023 年 5 月 14 日には、株式会社セシール（以下、セシール社）の運営するオンラインショップにおいてパスワードリスト攻撃と見られる不正アクセスが発生した※320。発生した不正アクセスは 10 回であり、結果として 3 件の不正ログインが成功し、顧客情報 2 名分が漏えいしたと見られる。しかし、その時点で直ちにアクセス元からの通信をブロックし、被害は限定された。

なお、特定のアクセス元からの通信ブロックだけでパスワードリスト攻撃に対処することは難しい。セシール社の事例では同サービスが 2018 年にも同様の攻撃を経験していた※321 ことが迅速な対応と被害の限定につながった可能性があるが、その際のアクセス元は 200 ヵ所以上に分散しており、容易には遮断できなかったことも報告されている。

(b) ランサムウェア攻撃の事例

2023 年 6 月 5 日、株式会社エムケイシステムがランサムウェア攻撃を受け、同社の提供する社会保険労務士向けの業務支援 IT サービスが利用できなくなった※322。被害範囲は同社の展開する主力サービスを含む広範囲に及んだ。この攻撃では、システム基盤の管理者アカウントがパスワードリスト攻撃によって乗っ取られ、サービスを提供しているサーバー群の管理者権限を奪われたと推測される。一部のサービスを再開できたのは 6 月 30 日となり、同社のサービスが大きな市場シェアを持っていることから、国内の多数の社労士事務所に多大な影響を及ぼす事例となった（詳細については「1.2.1 (2) (b) クラウ

ドサービス事業者における被害事例」参照）。一般に、高度な攻撃のすべてを予防することは困難である一方で、パスワード管理やバックアップの徹底により、こうした被害の発生を防ぐ余地がある。

(c) 業務委託先経由のサイバー攻撃の事例

2023 年 11 月 27 日、LINE ヤフー株式会社は、同社サービス利用者の個人データ、取引先等に関する個人データ、従業者等に関する個人データが不正アクセスにより漏えいしたことを公表した※323。2024 年 2 月 14 日の調査完了時点では、同社サービス利用者の個人データ約 30 万 3,000 件、取引先等に関する個人データ約 8 万 6,000 件、従業者等に関する個人データ約 13 万件が漏えいした可能性があると公表した※324。これらの個人データに対する不正アクセスは、同社の関係会社である韓国 NAVER Cloud Corp. のウイルス感染が起点となっている。ウイルス対策の不備もさることながら、関係先とは言え委託先企業からのアクセスを許容するセキュリティ設定となっていたことが致命傷となった。更に本件の調査過程では更に別件の同社システムへの不正アクセスが発覚し、従業者等の約 5 万 8,000 件の個人データが、委託先企業のアカウントの不正利用により漏えいしたことが判明した※325。同社の前身となる LINE 株式会社は、かねてより国境を越えての個人データ管理に問題のあることを個人情報保護委員会から指摘されており、その対応※326 を進めている最中での立て続けの問題発生となった。

クラウドサービスを提供するサービス事業者のシステムは膨大な量の個人データ等を含み、サイバー犯罪者にとっては高い経済価値を伴う格好の的である。他方で、サイバー攻撃への有効性の高い対策は、ネットワークの分離やウイルス対策ソリューションの導入、多要素認証の導入等複数存在する。しかし、あらゆる技術的対策を適用することは現実的ではなく、優先順位を踏まえて適切な組み合わせを検討し、かつ、組織全体で取り組むことが必要である。

(3) 広域インフラ障害のインシデント事例

クラウドサービスはいくつもの機材がつながった広域ネットワークを基盤とする。この巨大なシステムの維持・管理は困難であり、過年度中にも大きな障害が複数発生した。

(a) グローバル IaaS/PaaS の大規模障害

2023 年 1 月 25 日の午後 4 時から最大約 5 時間半にわたり、Microsoft 社の提供する各種のクラウドサービスがほぼ全世界で利用できなくなる大規模障害が発生した。Microsoft 社では自社の提供するクラウドサービスの障害情報を開示するサイトを設けており、そこでの説明によると、クラウドサービス基盤となっているネットワークに対して行われた設定変更が失敗し、全世界に影響を及ぼしたという※327。複数のネットワーク機器が混在する環境下での設定変更に対し、ネットワーク機器によって異なる挙動を示すことを事前に把握できていなかったことと、そのような状況も想定した入念なチェックプロセスが適切に運用されなかったことが原因であるとしている。

2023 年 6 月 14 日午前 4 時過ぎから午前 7 時過ぎにかけて、Amazon Web Services, Inc. のクラウドサービスである AWS（Amazon Web Services）クラウドが提供する複数のサービスが動作障害を起こした※328。AWS クラウドは世界最大手のグローバルクラウドサービスであり、ニューヨーク州都市交通局では列車やバスの運行情報を Web サイトやアプリ上で表示できなくなり、サウスウエスト航空でも Web サイトへのアクセスに問題を生じたほか※329、海を隔てた日本でも、一部のスマート家電が動かなくなるといった影響があった※330。この障害の原因は、アクセス負荷の増大に伴いインフラ構成の自動調整機能が作動した際に、それまでは実際に作動したことのなかった未検証のプログラムが動作し、不具合が顕在化したものであった※331。

上記の AWS クラウドの障害について注目すべきは、AWS の米国バージニアのリージョン（クラウドの分割区域）の障害により、日本のスマート家電にも影響が発生したことである。米国内の障害で日本にも影響が出た理由としては、AWS のリージョンは東京、大阪にも存在する一方で、リージョンごとに利用価格や機能が異なり、必ずしも地理的に近いリージョンだけを利用するとは限らないというクラウド利用の特性が関わっていると考えられる。

2023 年 4 月 26 日、フランス・パリにある Google 社のデータセンターで冷却システムの水道管から水漏れが発生し、これが原因となった火災が発生した。この浸水と火災により、欧州向けの Google サービスが一部利用できなくなる広域大規模障害に発展した※332。本件障害は一時的に全世界に波及したが、問題を起こしたリージョンを切り離す等することで数時間以内に影響範囲は限定された。欧州におけるクラウドサービスの復旧にはおよそ 27 時間を要した。

(b) 通信障害

インターネット等の通信障害もまた、クラウドサービスの利用に影響を与える。2023 年 4 月 3 日の朝には、西日本電信電話株式会社（以下、NTT 西日本）の提供する通信サービス「フレッツ光」等が 1 時間 39 分にわたって利用できない、または利用しづらくなるという大規模障害が西日本の広い範囲で発生した[※333]。この障害は、東日本電信電話株式会社の通信サービスでもほぼ同時に発生しており、最大 35.9 万回線の光アクセスサービス等が利用できない、または利用しづらくなるという同様の問題が発生した[※334]。報道によれば、これらの障害の原因は、ネットワーク機器が想定外の挙動を示したことであった。ただし、当該機器は 2018 年から利用していた機器の後継機であり、まったく利用ノウハウのない機種を不用意に導入したものではないという[※335]。後に、この挙動は通信機器メーカーでも把握していなかった不具合であることが特定されている。

2023 年 2 月上旬には、台湾本島と馬祖列島をつなぐ海底ケーブル 2 本が切断されるインシデントが発生した。これが攻撃によるものか、事故かは不明だが、馬祖列島におけるクラウドサービス等の利用に問題を生じた。台湾当局では安全保障上の懸念も踏まえた上で、海底ケーブル以外に利用できる衛星通信路の確保等にも取り組んでいる[※336]。国境を越えたインターネット回線網の構築において海底ケーブルは主役の立場にあり、通信インフラが持つ安全保障上の重要性も指摘されている[※337]。

2024 年 1 月 1 日に能登半島を襲った地震は多大な被害を地域にもたらした。NTT 西日本の 2024 年 1 月のニュースリリース一覧[※338]には、地震発生直後から設備が非常用電源に切り替わった様子や、電源が枯渇して後に長い復旧作業に着実に取り組んできた様子が生々しく残る。更にこの一覧を 2023 年にさかのぼれば、沖縄を台風が襲った際の通信への影響も垣間見える。これらの事例は、自然災害の影響がクラウドサービスの利用において無視できない要素であることを示している。

3.6.3 クラウドサービスのセキュリティの課題と対策

クラウドサービス利用にあたっては、サービス利用者とサービス事業者の間でそれぞれにどこまでを責任範囲とするかを整理する必要があり、これを「責任共有モデル[※339]」と呼ぶ。責任共有モデルについては「情報セキュリティ白書 2022[※340]」の「3.3.3 (2) (a) 責任共有モデルの実践」を参照されたい。その上で、利用形態に応じて個別の対策を導入することになる。例えば、ネットワークに対するファイアウォールの導入、関連機器・ソフトウェアの脆弱性へのパッチ適用、アクセス権限の適正な設定・管理等がこれに該当する。また、それらに関する近年の新しいアプローチ、例えばゼロトラストセキュリティ、SSVC[※341]、EPSS[※342]、KEV[※343] 等も参照・活用の検討対象となる。クラウドサービスを念頭においたセキュリティの考え方については、NISC が 2021 年 11 月末に「クラウドを利用したシステム運用に関するガイダンス[※344]」を公表しており、その他の参考資料も含め全体を俯瞰する起点として利用できる。以下では、クラウドのサービス利用者とサービス事業者という切り口から、クラウドセキュリティに関連する、上記以外の論点に目を向ける。

(1) サービス利用者側での対策

「3.6.2 クラウドサービスのインシデント事例」では、設定ミス、サイバー攻撃と、広域インフラ障害を取り上げた。近年発展してきているクラウドサービス利用者向けの技術的対策に目を向けると、設定ミスについてはクラウド環境設定の検証・是正を支援する CSPM（Cloud Security Posture Management）が、不正アクセスについてはサービスアクセス全般を監視・制御する CASB（Cloud Access Security Broker）等がある。これらに加え、重要性が高く、導入の技術的な敷居が比較的低い対策には、以下の二つがある。

(a) パスキー認証の利用

大多数のクラウドサービスは、ID とパスワードの組によってサービス利用者を識別する。パスワードは長くて複雑なものをサービスごとに使い分ける方が安全であるが、実際には覚えやすいものを使いまわすことも多いと考えられ、これがパスワードリスト攻撃の被害を助長する一因にもなっていると見られる。

パスワード認証の欠点を克服する技術として急速に導入が進むのがパスキー認証[※345]である。技術的な詳細は後述するが、スマートフォンで読み取れる指紋や顔等の情報も活用し、ID とパスワードに代えて、容易には盗用できない情報でサービス利用者の識別・アクセス許可を行う。ID とパスワードの盗用はパスワードリスト攻撃だけでなくフィッシングでも発生し、時にはその他のサイバー攻撃にも転用されるが、パスキー認証であればサーバーから盗み出した情報だけでは認証ができないため、これらの攻撃に対して極めて有効性の高い対策になると期待されている。

サービス利用者の観点からは、パスキー認証に対応しているクラウドサービスを選定し、認証手段としてパスキー認証を選ぶだけでよい。通常はスマートフォンがあれば簡単な手順で利用を開始できるため、導入の敷居は低く、それでいてセキュリティの着実な向上が望める。既に世界中のクラウドサービスが着々と対応を進めており※346、クラウドサービスにおける認証手段の主流になると見込まれる。

(b) インフラ障害への備え

クラウドサービスの利用に当たっては、アクセス手段であるネットワーク環境の多重化も検討すべきである。例えばインターネット接続回線については複数の回線事業者との契約が想定し得る。

クラウドサービスを利用する場合でもデータの管理責任は利用者にある。サービス利用者側で定期的なバックパップを取ることは、ランサムウェアによる被害発生時の復旧にも役立ち、強く推奨される。なお、バックアップデータを同一のクラウドサービス上に保存すると耐障害性の点で問題があるため、別のクラウドサービスを利用したり、手元のハードディスクドライブを利用したりするといった別の場所へのバックアップ保管が望ましい。

どれだけ手を尽くしたとしても、クラウドサービスが利用できなくなり、通常業務の遂行に著しく支障をきたす恐れはある。事実、社労士向け事務支援 IT サービスがランサムウェア被害を受けた事例では、サービス復旧までに 1 ヵ月近い時間がかかっている。中途段階にある様々な業務・処理を緊急時に迅速かつ安全に停止する方策や、バックアップ等から速やかに最低限の業務進行状態を回復する手順の整理を行っておくと、被害を限定できる。事業継続計画（BCP：Business Continuity Plan）の策定がこれにあたる。

上記の対策を網羅的に導入することは容易ではなく、特に中小規模の企業では、コストや人材の面で課題となることも考えられる。リスクアセスメントの実施によって、優先的に対処すべき課題を明らかにし、取り組みの効果を見積もることができる。具体的な手引きとしては、IPA の「中小企業の情報セキュリティ対策ガイドライン」がある。また、情報セキュリティに限らない一般のリスクアセスメント手法については、JIS Q 31010「リスクマネジメント−リスクアセスメント技法」が代表的なもののカタログとなっている。JIS Q 31010 については、日本産業標準調査会（JISC：Japanese Industrial Standards Committee）の Web サイト※347 で利用者登録をすると、無償で参照できる。

(2) サービス事業者側での対策

クラウドサービス利用者が導入すべき対策はサービス事業者にもそのまま当てはまる。以下では、サービス利用者とは異なるサービス事業者ならではの課題と対策に目を向ける。

(a) パスキー認証の導入

技術的には、パスキー認証は公開鍵暗号とチャレンジ・レスポンス認証の組み合わせを中核とする。スマートフォン等の端末内でアクセス先サービスごとに生成・保存した公開鍵を使い、サービス側サーバーとの間でチャレンジ・レスポンス認証を行う。端末のセンサーを用いた指紋認証や顔認証は秘密鍵へのアクセス許可の過程で行われ、サービスへのアクセス認証そのものには直接は関係しない。

サービス側でパスキー認証に対応するには、上記のチャレンジ・レスポンス認証のプロトコル処理をサーバー側に実装するのに加え、端末側で動作するクライアントアプリケーションにも対応実装を導入する必要がある。スマートフォンアプリであれば Android OS や iOS といった代表的なプラットフォームが提供する API を用いればよく、Web ブラウザーからのアクセスについては、WebAuthn※348 が該当仕様として策定されている。より簡便な方法としては、パスキー認証に対応している他のサービスとの ID 連携（OpenID Connect）で対応することもできる。準拠すべき規格は FIDO Alliance によって管理されている※349。

2023 年 12 月 8 日、パスキーに関する規格策定と導入推進を担う FIDO Alliance と FIDO ジャパンワーキンググループは報道陣向けの説明会を実施し、パスキー認証の概要と現状を示した。報道によれば、名だたるサービスが既にパスキー認証に対応しているという※350。パスキーを利用可能なアカウント数は既に 70 億以上となっている上に、実際に導入した企業でサービス向上という成果が見られるという。例えば、ニュージーランド航空では Web サイトへの初訪問から 24 時間以内のユーザー登録率が 30% に向上し、ユーザー登録完了までにかかる時間が約 5 分の 1 になり、離脱率も半減した。更に、Google 社では Google アカウントへのログイン成功率が 14% から 64% に大幅向上し、国内の大手サービスであるメルカリでも認証時間を 20.5 秒削減でき、82.5% の高い認証成功率につながった。これらは、セキュリティ対策としてだけでなく、サービス向上策としても、パスキー

認証の導入効果が大きいことを示唆している。

(b)クラウドセキュリティ標準への準拠

クラウドサービス事業の多くは、AWS や Google Cloud Platform（GCP）、Microsoft Azure といったグローバルクラウドの IaaS/PaaS を土台として、その上に自社製の SaaS を構築・運用していると推測される。これらのサービス事業者はクラウドサービスの担い手であると同時にサービス利用者でもある。このため、サービス利用者としては設定ミス等のないよう IaaS/PaaS を適切に運用する必要があるとともに、自社のサービスに SaaS としての十分な品質を確保することが求められる。その際の道標として役立つのが、各種のクラウドセキュリティ標準である。これらの標準は認証制度と一体に規定されており、認証の取得過程を通じてクラウドセキュリティの課題と対策を把握・実践できるとともに、自社のサービスが一定の品質を確立していることを外部に示す手段となる。代表的なものを以下に例示する。

ISMS クラウドセキュリティ認証※351 は ISMS（ISO/IEC 27000 ファミリー）認証を基礎とするアドオン認証制度であり、よく知られた国際標準である ISMS 認証を取得済みの組織が追加で審査を受けられる。ISMS 規格との差分は ISO/IEC 27017（JIS Q 27017）※352 にまとめられている。同認証制度ではクラウドサービスのサービス利用者（クラウドサービスカスタマー）またはサービス事業者（クラウドサービスプロバイダー）のどちらであるかを表明して審査を受ける。他社の提供する IaaS/PaaS の上に自社の SaaS を構築・運用する場合には、カスタマーかつプロバイダーであるものとして扱う。

SOC（Service Organization Control）2 は米国公認会計士協会（AICPA：American Institute of Certified Public Accountants）の策定したクラウドセキュリティ標準であり、監査報告書の一種としてクラウドサービスの構築・運用状況を開示する文書である。なお、SOC 1 は財務統制の報告書で、SOC 3 は SOC 2 の内容を一般の人々に向けて分かりやすく翻案したものを指す。SOC 2 における評価事項は「Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy」（通称、トラストサービス規準）という名称で整理されており、これを日本語に訳したものが日本公認会計士協会によって公開されている※353。SOC 2 のレポートについては Google 社等世界中の大手クラウドサービスプロバイダーによるものが公表されており容易に参照できる。このため、トラストサービス規準が実際の取り組みや SOC 2 報告書にどのように反映されるのかということを具体的に確認できる。なお、SOC 2 はある時点での監査報告をまとめた Type 1 と、一定期間にわたっての持続的な管理策の運用を示す Type 2 の 2 種類に分かれている。

CSA STAR（Security, Trust & Assurance Registry）認証は非営利の民間団体である米国 CSA（Cloud Security Alliance）の策定した認証制度であり、レベル 1 から 3 に認証の水準が分かれている※354。レベル 1 は自己評価に基づき、レベル 2 はある時点での第三者評価、レベル 3 は認証取得後の継続的モニタリングの実施に対応する。いずれの場合も CSA の Web サイト上で情報が公開され、クラウドサービスのサービス利用者による参照が容易となっている。審査基準にあたる情報は CCM（Cloud Control Matrix）としてまとめられており、更に、表形式となっている CCM の内容をチェックリスト形式に簡素化した CAIQ（Consensus Assessment Initiative Questionnaire）がある。レベル 1 では CAIQ に基づいて自己評価を行う。これらの資料は原文との対応関係が確認できる形で日本語版が用意されている※355。

前述の三つの認証制度以外にも類似するものは多数あり、一般財団法人日本情報経済社会推進協会（JIPDEC）がそれらを広く紹介するレポートをまとめている※356。

※ 1　https://www.nri-secure.co.jp/download/insight2023-report〔2024/4/23 確認〕
※ 2　IPA：「2023 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査」報告書について　https://www.ipa.go.jp/security/reports/sme/sa-survey2023.html〔2024/4/23 確認〕
※ 3　経済産業省：サイバーセキュリティ経営ガイドラインと支援ツール　https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔2024/4/23 確認〕
※ 4　https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf〔2024/4/23 確認〕
※ 5　NRI セキュア社：NRI Secure Insight 2022　https://www.nri-secure.co.jp/download/insight2022-report〔2024/4/23 確認〕
※ 6　IPA：2023 年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書　https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html〔2024/6/3 確認〕
※ 7　https://www.ipa.go.jp/security/guide/insider.html〔2024/4/19 確認〕
※ 8　IPA：「企業の内部不正防止体制に関する実態調査」報告書　https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html〔2024/4/19 確認〕
※ 9　一般社団法人情報マネジメントシステム認定センター：ISMS 適合性評価制度　https://isms.jp/isms.html〔2024/4/19 確認〕
※ 10　経済産業省：「技術情報管理認証制度（トップページ）」　https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html〔2024/4/19 確認〕
※ 11　IPA：今、そこにある脅威～内部不正による情報流出のリスク～　https://www.youtube.com/watch?v=YVBHBIf23gA〔2024/4/19 確認〕
※ 12　https://www.ipa.go.jp/security/10threats/index.html〔2024/4/19 確認〕
※ 13　https://www.ipa.go.jp/security/sc3/〔2024/4/19 確認〕
※ 14　IPA：サイバーセキュリティ対策に関する個別インタビュー集　https://www.ipa.go.jp/security/sc3/activities/chushoWG/content/〔2024/4/19 確認〕
※ 15　IPA：SC3 中小企業対策強化ワーキンググループ主催ウェビナー（オンラインセミナー）「やるなら今!業界・地域におけるサイバーセキュリティの取組み」　https://www.ipa.go.jp/security/sc3/activities/chushoWG/11_seminar.html〔2024/4/19 確認〕
※ 16　https://www.ipa.go.jp/security/sme/otasuketai-about.html〔2024/4/19 確認〕
※ 17　IPA：サイバーセキュリティお助け隊サービス基準（2.0 版）　https://www.ipa.go.jp/security/sme/otasuketai/nq6ept000000faii-att/000092713.pdf〔2024/4/19 確認〕
※ 18　https://www.ipa.go.jp/security/security-action/index.html〔2024/4/19 確認〕
※ 19　https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf〔2024/4/19 確認〕
※ 20　IPA：2023 年度宣言事業者における情報セキュリティ対策の実態調査 - 調査報告書 -　https://www.ipa.go.jp/security/reports/sme/m42obm000000488h-att/sa-survey2023.pdf〔2024/4/19 確認〕
※ 21　https://www.ipa.go.jp/security/seminar/sme/ttx-e.html〔2024/4/19 確認〕
※ 22　https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf〔2024/4/19 確認〕
※ 23　https://www.ipa.go.jp/security/seminar/sme/riskassesmentws.html〔2024/4/19 確認〕
※ 24　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〔2024/4/19 確認〕
※ 25　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〔2024/4/19 確認〕
※ 26　https://www.ipa.go.jp/security/economics/checktool.html〔2024/4/19 確認〕
※ 27　https://www.ipa.go.jp/security/economics/csm-practice.html〔2024/4/19 確認〕
※ 28　https://isog-j.org/output/2023/Textbook_soc-csirt_v3.1.pdf〔2024/4/19 確認〕
※ 29　https://www.jnsa.org〔2024/4/19 確認〕
※ 30　https://www.jnsa.org/result/incidentdamage/202402.html〔2024/4/19 確認〕
※ 31　https://sg.jnsa.org〔2024/4/19 確認〕
※ 32　https://www.ipa.go.jp/security/guide/sme/5minutes.html〔2024/4/19 確認〕
※ 33　日本経済新聞：生成 AI のリスクとは　誤情報拡散や情報漏洩が課題　https://www.nikkei.com/article/DGXZQOCB041NJ0U3A500C2000000/〔2024/4/19 確認〕
※ 34　NHK：番組に似せた岸田首相の偽動画拡散 日本テレビが注意呼びかけ　https://www3.nhk.or.jp/news/html/20231104/k10014247171000.html〔2024/4/19 確認〕
※ 35　https://www.ppc.go.jp/files/pdf/230602_kouhou_houdou.pdf〔2024/4/19 確認〕
※ 36　文部科学省：初等中等教育段階における生成 AI の利用に関する暫定的なガイドライン　https://www.mext.go.jp/content/20230710-mxt_shuukyo02-000030823_003.pdf〔2024/4/19 確認〕
※ 37　読売新聞オンライン：能登地震、偽情報がSNSで拡散…架空の地名で「助けて下さい」・原因は「人工地震」　https://www.yomiuri.co.jp/politics/20240103-OYT1T50054/〔2024/4/19 確認〕
朝日新聞デジタル：SNS の偽・誤情報、有識者会議で対策議論　被災地では偽の救助要請　https://www.asahi.com/articles/ASS1T6K1ZS1TULFA01K.html〔2024/4/19 確認〕
※ 38　NHK 解説委員室：偽情報がもたらす脅威～情報戦への備えを　https://www.nhk.jp/p/ts/4V23PRP3YR/episode/te/21V4RR3N4L/〔2024/4/19 確認〕
※ 39　日本ファクトチェックセンター：AI、処理水、陰謀論 ...、JFC が検証した 2023 年 10 大フェイクニュース 史上最大の選挙の年に備えを　https://www.factcheckcenter.jp/explainer/others/10-biggest-fakenews-2023/〔2024/4/19 確認〕
※ 40　総務省：【啓発教育教材】インターネットとの向き合い方～ニセ・誤情報に騙されないために～　https://www.soumu.go.jp/use_the_internet_wisely/special/nisegojouhou/〔2024/4/19 確認〕
※ 41　朝日新聞デジタル：広域強盗、関連する事件は 50 件以上と判明　すでに 60 数人逮捕　https://www.asahi.com/articles/ASR283G90R28UTIL004.html〔2024/4/19 確認〕
※ 42　警察庁：令和5年における特殊詐欺の認知・検挙状況等について（暫定値版）　https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2023.pdf〔2024/4/19 確認〕
※ 43　https://www.youtube.com/@MPD_koho〔2024/4/19 確認〕
※ 44　https://www.youtube.com/watch?v=0_GGmZDXUqY〔2024/4/19 確認〕
※ 45　https://www.youtube.com/@user-ee2hu8vk3x〔2024/4/19 確認〕
※ 46　https://www.youtube.com/watch?v=rsqF8RnoscA〔2024/4/19 確認〕
※ 47　福岡県警察：動画「闇バイトは暴力団の使い捨て」の制作について　https://www.police.pref.fukuoka.jp/boutai/sotai/konnnahazujyanakatta/yamibaitodouga.html〔2024/4/19 確認〕
※ 48　奈良県警察：絶対にダメ!!闇バイト　https://www.police.pref.nara.jp/0000005779.html〔2024/4/19 確認〕
※ 49　NHK：くら寿司 “しょうゆさしに口” 迷惑動画などの被告に有罪判決　https://www3.nhk.or.jp/news/html/20231013/k10014224531000.html〔2024/4/19 確認〕
※ 50　日経 BP：教育と ICT online 第 112 回　なぜ若者は迷惑動画を投稿してしまうのか　https://project.nikkeibp.co.jp/pc/atcl/19/08/28/00031/032200125/〔2024/4/19 確認〕
※ 51　文部科学省：教材⑩ 軽はずみな SNS への投稿（全編）　https://www.youtube.com/watch?v=WCx-RMKRT60&list=PLGpGsGZ3lmbAOd2f-4u_Mx-BCn13GywDI&index=32〔2024/4/19 確認〕
※ 52　https://www.youtube.com/@mextchannel〔2024/4/19 確認〕
※ 53　https://www.youtube.com/watch?v=tVZSuGkmnGQ〔2024/4/19 確認〕
※ 54　https://www.youtube.com/@ipajp〔2024/4/19 確認〕
※ 55　https://security-portal.nisc.go.jp/cybersecuritymonth/2024/seminar/index.html〔2024/4/19 確認〕
※ 56　https://www.gov-online.go.jp/tokusyu/phishing/〔2024/4/19 確認〕
※ 57　https://www.gov-online.go.jp/prg/prg27221.html〔2024/4/19 確認〕
※ 58　https://www.soumu.go.jp/use_the_internet_wisely/〔2024/4/19 確認〕
※ 59　https://www.soumu.go.jp/use_the_internet_wisely/parent-teacher/digital_citizenship/〔2024/4/19 確認〕
※ 60　総務省：インターネットトラブル事例集ダウンロードページ　https://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/jireishu.html〔2024/4/19 確認〕
※ 61　https://www.soumu.go.jp/use_the_internet_wisely/trouble/case/case18.html〔2024/4/19 確認〕
※ 62　警視庁：あなたのスマホが狙われている!?「スマホ防犯教室」　https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/sumaho_bouhan.html〔2024/4/19 確認〕
※ 63　https://www.youtube.com/watch?v=yL9rZl2qmFc〔2024/

4/19 確認〕
※ 64 https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf〔2024/4/19 確認〕
※ 65 https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf〔2024/4/19 確認〕
※ 66 Common Criteria：https://www.commoncriteriaportal.org〔2024/4/19 確認〕
※ 67 IPA：評価・認証プロテクションプロファイルリスト https://www.ipa.go.jp/security/jisec/pps/certified-pps/〔2024/4/19 確認〕
※ 68 IPA：セキュリティ評価基準（CC/CEM） https://www.ipa.go.jp/security/jisec/about/kijun.html〔2024/4/19 確認〕
※ 69 JISEC の「規程集」ページ（https://www.ipa.go.jp/security/jisec/shinsei/kitei.html〔2024/4/19 確認〕）の「IT セキュリティ評価及び認証制度に係る規程の改正（2023 年 11 月施行）」参照。
※ 70 JISEC の「規程集」ページ（https://www.ipa.go.jp/security/jisec/shinsei/kitei.html〔2024/4/19 確認〕）の「IT セキュリティ評価及び認証制度に係る規程の改正（2023 年 12 月施行）」参照。
※ 71 https://www.ipa.go.jp/security/jisec/shinsei/doe3um00000098cg-att/Cvv1.0_20210930-j.pdf〔2024/4/19 確認〕
※ 72 https://www.ipa.go.jp/security/jisec/shinsei/cdk3vs00000023xp-att/Acv3.0_20230309-J.pdf〔2024/4/19 確認〕
※ 73 経済産業省：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/index.html〔2024/4/19 確認〕
※ 74 経済産業省：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最終とりまとめを公表し、制度構築方針案に対する意見公募を開始しました https://www.meti.go.jp/press/2023/03/20240315005/20240315005.html〔2024/4/19 確認〕
※ 75 NIST：Cryptographic Module Validation Program https://csrc.nist.gov/projects/cryptographic-module-validation-program〔2024/4/19 確認〕
※ 76 IPA：暗号モジュール試験及び認証制度（JCMVP） https://www.ipa.go.jp/security/jcmvp/index.html〔2024/4/19 確認〕
※ 77 https://www.nisc.go.jp/pdf/policy/general/guider5.pdf〔2024/4/19 確認〕
※ 78 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/f1be078e/20220422_resources_standard_guidelines_guideline_07.pdf〔2024/4/19 確認〕
※ 79 IPA、JISEC：「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン 第 1.9 版 https://www.ipa.go.jp/security/jisec/shinsei/cdk3vs000000260p-att/guidelineforHCD-PP_1.9.pdf〔2024/4/19 確認〕
※ 80 https://www.ipa.go.jp/en/security/jisec/pps/certified-cert/c0553_it7627.html〔2024/4/19 確認〕
※ 81 内閣官房、総務省、経済産業省：「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用開始 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00071.html〔2024/4/19 確認〕
※ 82 https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf〔2024/4/19 確認〕
※ 83 総務省、経済産業省：クラウドサービスの安全性評価に関する検討会について https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/001_02_00.pdf〔2024/4/19 確認〕
※ 84 https://www.soumu.go.jp/main_content/000666496.pdf〔2024/4/19 確認〕
※ 85 https://www.nisc.go.jp/pdf/policy/general/wakugumi2021.pdf〔2024/4/19 確認〕
※ 86 NISC：「政府機関等のサイバーセキュリティ対策のための統一基準群」 https://www.nisc.go.jp/policy/group/general/kijun.html〔2024/4/19 確認〕
※ 87 機密性 2 情報：行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害されまたは行政事務の遂行に支障を及ぼす恐れがある情報を指す。
※ 88 https://www.digital.go.jp/policies/security/ismap-liu/#special_measures〔2024/4/19 確認〕
※ 89 NISC、デジタル庁、総務省、経済産業省：ISMAP 制度改善の取組み https://www.ismap.go.jp/sys_attachment.do?sys_id=be1ce75c4713b5103f0f6befe16d4355〔2024/4/19 確認〕
※ 90 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005〔2024/4/19 確認〕
※ 91 https://www.ismap.go.jp〔2024/4/19 確認〕
※ 92 「ISMAP 管理基準マニュアル」は、JIS 規格である JIS Q 27014:2015（ISO/IEC 27014:2013）と JIS Q 27017:2016（ISO/IEC 27017:2015）の両方を購入している場合のみ閲覧することができる。
ISMAP：管理基準 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028&sys_kb_id=6ce589cac305821032713201150131d5&spa=1〔2024/4/19 確認〕
※ 93 https://www.nisc.go.jp/pdf/policy/infra/shishin202307.pdf〔2024/4/19 確認〕
※ 94 https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf〔2024/4/19 確認〕
※ 95 https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf〔2024/4/19 確認〕
※ 96 https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf〔2024/4/19 確認〕
※ 97 NIST：Lightweight Cryptography https://csrc.nist.gov/Projects/lightweight-cryptography〔2024/4/19 確認〕
※ 98 CRYPTREC：CRYPTREC 暗号技術ガイドライン（軽量暗号）2023 年度版 https://www.cryptrec.go.jp/report/cryptrec-gl-2006-2023.pdf〔2024/4/19 確認〕
※ 99 CRYPTREC：CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号） https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf〔2024/4/19 確認〕
※ 100 CRYPTREC：CRYPTREC 耐量子計算機暗号の研究動向調査報告書 https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2022.pdf〔2024/4/19 確認〕
※ 101 NICT、IPA：CRYPTREC Report 2023 https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2023.pdf〔2024 年 7 月公開予定〕
※ 102 CRYPTREC：CRYPTREC TLS 暗号設定ガイドライン https://www.cryptrec.go.jp/report/cryptrec-gl-3001-3.1.0.pdf〔2024/6/20 確認〕
※ 103 https://www.cryptrec.go.jp/report/cryptrec-gl-3004-1.0.pdf〔2024/4/19 確認〕
※ 104 CRYPTREC：CRYPTREC シンポジウム 2023 https://www.cryptrec.go.jp/events/cryptrec_symposium2023_presentation.html〔2024/4/19 確認〕
※ 105 AES（Advanced Encryption Standard）：米国で NIST により標準化された共通鍵暗号。
※ 106 Eurocrypt 2023：2023 年 4 月 23 日～ 4 月 27 日にフランスで行われた学会。
International Association for Cryptologic Research：Eurocrypt 2023 https://eurocrypt.iacr.org/2023/〔2024/4/19 確認〕
※ 107 Crypto 2023：2023 年 8 月 19 日～ 8 月 24 日にアメリカで行われた学会。
International Association for Cryptologic Research：Crypto 2023 https://crypto.iacr.org/2023/〔2024/4/19 確認〕
※ 108 FSE 2023：2023 年 3 月 20 日～ 3 月 24 日に中国で行われた学会。
International Association for Cryptologic Research：FSE 2023 https://fse.iacr.org/2023/〔2024/4/19 確認〕
※ 109 ChaCha:Daniel J. Bernstein によって開発されたストリーム暗号。ChaCha20 は ChaCha を基にした 20 ラウンドのストリーム暗号であり、これとメッセージ認証子である Poly1305 とを組み合わせた ChaCha20-Poly1305 は、CRYPTREC の電子政府推奨暗号リストに含まれている。
※ 110 NIST：Post-Quantum Cryptography Standardization https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization〔2024/4/19 確認〕
※ 111 NIST：Fourth PQC Standardization Conference https://csrc.nist.gov/events/2022/fourth-pqc-standardization-conference〔2024/4/19 確認〕
※ 112 NIST：PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4〔2024/4/19 確認〕
※ 113 NIST：Lightweight Cryptography Standardization Process: NIST Selects Ascon https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon〔2024/4/19 確認〕
※ 114 ECDSA（Elliptic Curve Digital Signature Algorithm）：楕円曲線暗号を用いたデジタル署名アルゴリズム。
※ 115 CHES 2023:2023 年 9 月 10 ～ 14 日にチェコで行われた学会。
International Association for Cryptologic Research：CHES 2023 https://ches.iacr.org/2023/〔2024/4/19 確認〕
※ 116 Luyao Xu, Zhengyi Dai, Baofeng Wu and Dongdai Lin：Improved Attacks on (EC)DSA with Nonce Leakage by Lattice Sieving with Predicate https://tches.iacr.org/index.php/TCHES/article/view/10294〔2024/4/19 確認〕
※ 117 Yaacov Belenky, Ira Dushar, Valery Teper, Vadim

Bugaenko, Oleg Karavaev, Leonid Azriel and Yury Kreimer：Carry-based Differential Power Analysis (CDPA) and its Application to Attacking HMAC-SHA-2 https://tches.iacr.org/index.php/TCHES/article/view/10955〔2024/4/19 確認〕
※ 118 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 15 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〔2024/4/23 確認〕
※ 119 Fortinet, Inc.：2023 State of Operational Technology and Cybersecurity Report https://www.fortinet.com/demand/gated/report-state-ot-cybersecurity〔2024/4/23 確認〕
※ 120 TXOne Networks：The Crisis of Convergence: OT/ICS Cybersecurity 2023 https://www.txone.com/security-reports/ot-ics-cybersecurity-2023/〔2024/4/23 確認〕
※ 121 The Record：Pennsylvania water authority hit with cyberattack allegedly tied to pro-Iran group https://therecord.media/water-authority-pennsylvania-cyberattack-pro-iran-group〔2024/4/23 確認〕
※ 122 Dark Reading：Pro-Iran Attackers Access Multiple Water Facility Controllers https://www.darkreading.com/ics-ot-security/Pro-Iran-Attackers-Access-Multiple-Water-Facility-Controllers〔2024/4/23 確認〕
※ 123 CISA：ALERT - Exploitation of Unitronics PLCs used in Water and Wastewater Systems https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems〔2024/4/23 確認〕
※ 124 CISA：Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords https://www.cisa.gov/resources-tools/resources/secure-design-alert-how-manufacturers-can-protect-customers-eliminating-default-passwords〔2024/4/23 確認〕
※ 125 The Record：Two-day water outage in remote Irish region caused by pro-Iran hackers https://therecord.media/water-outage-in-ireland-county-mayo〔2024/4/23 確認〕
※ 126 IT World Canada：Canadian tool manufacturer hit by cyber attack https://www.itworldcanada.com/article/canadian-tool-manufacturer-hit-by-cyber-attack/523620〔2024/4/23 確認〕
※ 127 The Guardian：Royal Mail overseas post badly disrupted after cyber incident https://www.theguardian.com/business/2023/jan/11/royal-mail-services-suffer-severe-disruption-after-cyber-incident〔2024/4/23 確認〕
※ 128 IDG Communications, Inc.：MKS Instruments falls victim to ransomware attack https://www.csoonline.com/article/3687098/mks-instruments-falls-victim-to-ransomware-attack.html〔2024/4/23 確認〕
※ 129 Security Affairs：Ransomware attack on food giant Dole Food Company blocked North America production https://securityaffairs.com/142726/cyber-crime/dole-food-company-ransomware-attack.html〔2024/4/23 確認〕
※ 130 CTECH：Cyberattacks strike Israel Post, irrigation systems https://www.calcalistech.com/ctechnews/article/hj000lsgm3〔2024/4/23 確認〕
※ 131 Security Affairs：Lacroix Group shut down three facilities after a 'targeted cyberattack' https://securityaffairs.com/146335/cyber-crime/lacroix-group-ransomware-attack.html〔2024/4/23 確認〕
※ 132 Bleeping Computer：Japanese pharma giant Eisai discloses ransomware attack https://www.bleepingcomputer.com/news/security/japanese-pharma-giant-eisai-discloses-ransomware-attack/〔2024/4/23 確認〕
エーザイ株式会社：ランサムウェア被害の発生について https://www.eisai.co.jp/news/2023/news202341.html〔2024/4/23 確認〕
※ 133 Security Affairs：POLAND'S AUTHORITIES INVESTIGATE A HACKING ATTACK ON COUNTRY' S RAILWAYS https://securityaffairs.com/149952/hacking/hacking-attack-polan-railways.html〔2024/4/23 確認〕
※ 134 Bleeping Computer：Chilean telecom giant GTD hit by the Rorschach ransomware gang https://www.bleepingcomputer.com/news/security/chilean-telecom-giant-gtd-hit-by-the-rorschach-ransomware-gang/〔2024/4/23 確認〕
※ 135 Dark Reading：Kyivstar Mobile Attack Plunges Millions in Ukraine Into Comms Blackout https://www.darkreading.com/ics-ot-security/kyivstar-mobile-attack-ukraine-comms-blackout〔2024/4/23 確認〕
The Record：Hackers damaged some infrastructure of Ukraine's Kyivstar telecom company https://therecord.media/hackers-damaged-kyivstar-functions-ukraine-telecom-cyberattack〔2024/4/23 確認〕
※ 136 Security Affairs：Danish critical infrastructure hit by the largest cyber attack in Denmark's history https://securityaffairs.com/154156/apt/denmark-critical-infrastructure-record-attacks.html〔2024/4/23 確認〕
SektorCERT：The attack against Danish, critical infrastructure https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf〔2024/4/23 確認〕
※ 137 Industrial Cyber：Forescout publishes critical analysis of recent energy sector cyberattacks in Denmark, Ukraine https://industrialcyber.co/industrial-cyber-attacks/forescout-publishes-critical-analysis-of-recent-energy-sector-cyberattacks-in-denmark-ukraine/〔2024/4/23 確認〕
Forescout Technologies, Inc.：Clearing the Fog of War - A Critical Analysis of Recent Energy Sector Attacks in Denmark and Ukraine https://www.forescout.com/resources/clearing-the-fog-of-war/〔2024/4/23 確認〕
※ 138 Bleeping Computer：Japan's largest port stops operations after ransomware attack https://www.bleepingcomputer.com/news/security/japans-largest-port-stops-operations-after-ransomware-attack/〔2024/4/23 確認〕
Internet Watch：名古屋港のランサムウェア感染事件、港運協会らが詳細な経緯と今後の対応を報告 https://internet.watch.impress.co.jp/docs/news/1521097.html〔2024/4/23 確認〕
Internet Watch：「日本の重要インフラに影響を及ぼした」～名古屋港へのランサムウェア攻撃をトレンドマイクロが解説 https://internet.watch.impress.co.jp/docs/news/1520831.html〔2024/4/23 確認〕
※ 139 The Maritime Executive：DP World Australia Resumes Terminal Ops After "Serious" Cyber Incident https://maritime-executive.com/article/dp-world-australia-resumes-terminal-ops-after-serious-cyber-incident〔2024/4/23 確認〕
※ 140 OPSGROUP：Flights Misled Over Position, Navigation Failure Follows https://ops.group/blog/gps-spoof-attacks-irs/〔2024/4/23 確認〕
※ 141 VICE：Commercial Flights Are Experiencing 'Unthinkable' GPS Attacks and Nobody Knows What to Do https://www.vice.com/en/article/m7bk3v/commercial-flights-are-experiencing-unthinkable-gps-attacks-and-nobody-knows-what-to-do〔2024/4/23 確認〕
OPSGROUP：GPS Spoofing Update: Map, Scenarios And Guidance https://ops.group/blog/gps-spoofing-update-08nov2023/〔2024/4/23 確認〕
※ 142 Security Week：Ransomware Operators Leak Data Allegedly Stolen From City of Oakland https://www.securityweek.com/ransomware-operators-leak-data-allegedly-stolen-from-city-of-oakland/〔2024/4/23 確認〕
※ 143 Security Week：City of Oakland Hit by Ransomware Attack https://www.securityweek.com/city-of-oakland-hit-by-ransomware-attack/〔2024/4/23 確認〕
City of Oakland：City of Oakland Targeted by Ransomware Attack, Work Continues to Secure and Restore Services Safely https://www.oaklandca.gov/news/city-of-oakland-targeted-by-ransomware-attack-core-services-not-affected〔2024/4/23 確認〕
※ 144 Security Affairs：City of Oakland issued a local state of emergency after recent ransomware attack https://securityaffairs.com/142295/cyber-crime/city-of-oakland-emergency-ransomware.html〔2024/4/23 確認〕
※ 145 Government technology：Oakland Reports 'Outstanding' Headway in Ransomware Recovery https://www.govtech.com/security/oakland-reports-outstanding-headway-in-ransomware-recovery〔2024/4/23 確認〕
City of Oakland：City of Oakland Targeted by Ransomware Attack, Work Continues to Secure and Restore Services Safely https://www.oaklandca.gov/news/city-of-oakland-targeted-by-ransomware-attack-core-services-not-affected〔2024/4/23 確認〕
City of Oakland：City of Oakland Restores and Recovers Systems Affected by Ransomware Attack https://www.oaklandca.gov/news/city-of-oakland-restores-and-recovers-systems-affected-by-ransomware-attack〔2024/4/23 確認〕
※ 146 The Oaklandside：Oakland gets sued after ransomware

hack https://oaklandside.org/2023/05/30/oakland-sued-after-ransomware-hack/〔2024/4/23 確認〕
※ 147 Security Affairs：The ransomware attack on Westpole is disrupting digital services for Italian public administration https://securityaffairs.com/156090/cyber-crime/westpole-ransomware-attack.html〔2024/4/23 確認〕
Cubic Lighthouse：LockBit Ransomware Disrupts Public Digital Services in Italy https://cubic-lighthouse.com/2023/12/22/lockbit-ransomware-disrupts-public-digital-services-in-italy/news/〔2024/4/23 確認〕
※ 148 Bleeping Computer：Ardent hospital ERs disrupted in 6 states after ransomware attack https://www.bleepingcomputer.com/news/security/ardent-hospital-ers-disrupted-in-6-states-after-ransomware-attack/〔2024/4/23 確認〕
※ 149 FIERCE Healthcare：UPDATE: Ardent Health restores access to Epic EHR two weeks after ransomware attack https://www.fiercehealthcare.com/health-tech/ardent-health-struggles-get-systems-back-online-hospitals-reopen-emergency-rooms〔2024/4/23 確認〕
Ardent Health Services：Cybersecurity Incident https://ardenthealth.com/cybersecurityincident〔2024/4/23 確認〕
※ 150 Sophos Ltd.：The State of Ransomware in Healthcare 2023 https://news.sophos.com/en-us/2023/08/10/the-state-of-ransomware-in-healthcare-2023/〔2024/4/23 確認〕
※ 151 CISA の Web サイトで暦年（1/1 ～ 12/31）ごとに公開された ICS Advisory の件数をカウントした。ただし、ICS Medical Advisory（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 2023 年なら、採番年度が 2022（ICSA-2022-xxx-x）でも 2023 年でカウント）。
CISA：Cybersecurity Alerts & Advisories https://www.cisa.gov/news-events/cybersecurity-advisories〔2024/4/23 確認〕
※ 152 Dragos, Inc.：OT Cybersecurity: The 2023 Year in Review https://www.dragos.com/ot-cybersecurity-year-in-review/〔2024/4/23 確認〕
※ 153 ARMIS：Crit.IX: 9 vulnerabilities discovered in Honeywell's Experion Platforms for Distributed Control Systems (DCS) https://www.armis.com/blog/critix-9-vulnerabilities-discovered-in-honeywells-experionplatforms-for-distributed-control-systems-dcs/〔2024/4/23 確認〕
※ 154 The Record：Honeywell, CISA warn of 'Crit.IX' vulnerabilities affecting manufacturing tools https://therecord.media/honeywell-cisa-warn-of-vulnerabilities-affecting-manufacturing-tools〔2024/4/23 確認〕
CISA：ICS ADVISORY - Honeywell Experion PKS, LX and PlantCruise https://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06〔2024/4/23 確認〕
※ 155 Dark Reading：Zero-Day Vulnerabilities Discovered in Global Emergency Services Communications Protocol https://www.darkreading.com/vulnerabilities-threats/zero-day-vulnerabilities-disclosed-in-global-emergency-services-communications-protocol〔2024/4/23 確認〕
※ 156 Microsoft 社：Multiple high severity vulnerabilities in CODESYS V3 SDK could lead to RCE or DoS https://www.microsoft.com/en-us/security/blog/2023/08/10/multiple-high-severity-vulnerabilities-in-codesys-v3-sdk-could-lead-to-rce-or-dos/〔2024/4/23 確認〕
※ 157 Claroty Ltd.：The Global State of Industrial Cybersecurity 2023 https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity-2023〔2024/4/23 確認〕
※ 158 本白書では文献引用上の正確性を期す必要がない場合、表記の統一のため、悪意のあるプログラム、マルウェア等を総称して「ウイルス」と表記する。
※ 159 Mandiant, Inc.：COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response〔2024/4/23 確認〕
※ 160 CISA：US-CERT and ICS-CERT Transition to CISA https://www.cisa.gov/news-events/alerts/2023/02/24/us-cert-and-ics-cert-transition-cisa〔2024/4/23 確認〕
※ 161 Bleeping Computer：CISA now warns critical infrastructure of ransomware-vulnerable devices https://www.bleepingcomputer.com/news/security/cisa-now-warns-critical-infrastructure-of-ransomware-vulnerable-devices/〔2024/4/23 確認〕
CISA：Ransomware Vulnerability Warning Pilot (RVWP) https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot〔2024/4/23 確認〕
※ 162 Industrial Cyber：CISA CPGs reorganized, reordered, renumbered to align with NIST CSF functions, following industry feedback https://industrialcyber.co/cisa/cisa-cpgs-reorganized-reordered-renumbered-to-align-with-nist-csf-functions-following-industry-feedback/〔2024/4/23 確認〕
CISA：Cross-Sector Cybersecurity Performance Goals https://www.cisa.gov/cross-sector-cybersecurity-performance-goals〔2024/4/23 確認〕
※ 163 BANK INFO SECURITY：CISA's New 'CyberSentry' Program to Tighten ICS Security https://www.bankinfosecurity.com/cisas-new-cybersentry-program-to-tighten-ics-security-a-22435〔2024/4/23 確認〕
CISA：CyberSentry Program https://www.cisa.gov/resources-tools/programs/cybersentry-program〔2024/4/23 確認〕
※ 164 CyberWire：CISA, FEMA, and Shields Ready. https://thecyberwire.com/stories/a4d21db2db0b4d2fb0fab6ce989e088f/cisa-fema-and-shields-ready〔2024/4/23 確認〕
FEMA：DHS Unveils New Shields Ready Campaign to Promote Critical Infrastructure Security and Resilience https://www.fema.gov/press-release/20231107/dhs-unveils-new-shields-ready-campaign-promote-critical-infrastructure〔2024/4/23 確認〕
※ 165 GOV INFO SECURITY：White House Unveils Biden's National Cybersecurity Strategy https://www.govinfosecurity.com/white-house-unveils-bidens-national-cybersecurity-strategy-a-21349〔2024/4/23 確認〕
The White House：FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/〔2024/4/23 確認〕
U.S. Department of State：Announcing the Release of the Administration's National Cybersecurity Strategy https://www.state.gov/announcing-the-release-of-the-administrations-national-cybersecurity-strategy/〔2024/4/23 確認〕
※ 166-1 CPO MAGAZINE：White House Cybersecurity Strategy Implementation Plan Released: 65 Mandatory Initiatives, Increased Public-Private Partnerships https://www.cpomagazine.com/cyber-security/white-house-cybersecurity-strategy-implementation-plan-released-65-mandatory-initiatives-increased-public-private-partnerships/〔2024/4/23 確認〕
The White House：FACT SHEET: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/〔2024/4/23 確認〕
※ 166-2 The White House：NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION PLAN https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf〔2024/6/11 確認〕
※ 167 MSSP Alert：November is Critical Infrastructure and Resilience Month https://www.msspalert.com/news/biden-declares-november-2023-critical-infrastructure-and-resilience-month〔2024/4/23 確認〕
The White House：A Proclamation on Critical Infrastructure Security and Resilience Month, 2023 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/31/a-proclamation-on-critical-infrastructure-security-and-resilience-month-2023/〔2024/4/23 確認〕
CISA：CISA Launches Critical Infrastructure Security and Resilience Month 2023 https://www.cisa.gov/news-events/news/cisa-launches-critical-infrastructure-security-and-resilience-month-2023〔2024/4/23 確認〕
CISA：Critical Infrastructure Security and Resilience Month https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-security-and-resilience-month〔2024/5/16 確認〕
※ 168 The Register：NIST updates Cybersecurity Framework after a decade of lessons https://www.theregister.com/2024/02/27/nist_cybersecurity_framework_2/〔2024/4/23 確認〕
NIST：NIST Releases Version 2.0 of Landmark Cybersecurity Framework https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework〔2024/4/23 確認〕
※ 169 Industrial Cyber：NCCoE publishes LNG Cybersecurity

Framework Profile based on prioritized mission objectives https://industrialcyber.co/mining-oil-gas/nccoe-publishes-lng-cybersecurity-framework-profile-based-on-prioritized-mission-objectives/〔2024/4/23 確認〕
NIST：NCCoE Publishes Final NIST IR 8406, Cybersecurity Framework Profile for Liquefied Natural Gas https://www.nccoe.nist.gov/news-insights/nccoe-publishes-final-nist-ir-8406-cybersecurity-framework-profile-liquefied-natural〔2024/4/23 確認〕
※ 170 Industrial Cyber：NCCoE releases final NIST IR 8441 HSN Profile document for enhanced space cybersecurity https://industrialcyber.co/nist/nccoe-releases-final-nist-ir-8441-hsn-profile-document-for-enhanced-space-cybersecurity/〔2024/4/23 確認〕
NIST：NIST IR 8441 Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN) https://csrc.nist.gov/pubs/ir/8441/final〔2024/4/23 確認〕
※ 171 Industrial Cyber：EU Cyber Resilience Act reaches political consensus to strengthen cybersecurity standards for products https://industrialcyber.co/threats-attacks/eu-cyber-resilience-act-reaches-political-consensus-to-strengthen-cybersecurity-standards-for-products/〔2024/4/23 確認〕
※ 172 Industrial Cyber：Australia releases comprehensive guide on critical infrastructure asset class definition https://industrialcyber.co/regulation-standards-and-compliance/australia-releases-comprehensive-guide-on-critical-infrastructure-asset-class-definition/〔2024/4/23 確認〕
Cyber and Infrastructure Security Centre：Critical Infrastructure Asset Class Definition Guidance https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-asset-class-definition-guidance.pdf〔2024/4/23 確認〕
※ 173 Federal Register of Legislation：Security of Critical Infrastructure Act 2018 https://www.legislation.gov.au/Details/C2022C00160〔2024/4/23 確認〕
※ 174 Federal Register of Legislation：Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 https://www.legislation.gov.au/Series/F2021L01769〔2024/4/23 確認〕
※ 175 NISC：サイバーセキュリティ 2023（2022 年度年次報告・2023 年度年次計画） https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023.pdf〔2024/4/23 確認〕
※ 176 NISC：重要インフラのサイバーセキュリティに係る安全基準等策定指針 https://www.nisc.go.jp/pdf/policy/infra/shishin202307.pdf〔2024/4/23 確認〕
※ 177 経済産業省：第 16 回 日 ASEAN サイバーセキュリティ政策会議の結果（4）重要インフラ防護に関する取り組みの推進 https://www.meti.go.jp/press/2023/10/20231006009/20231006009.html〔2024/4/23 確認〕
※ 178 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/2023/10/20231016002/20231016002.html〔2024/4/23 確認〕
※ 179 IPA：産業用制御システム向け侵入検知製品等の導入手引書 https://www.ipa.go.jp/security/controlsystem/icsidshandbook.html〔2024/4/23 確認〕
※ 180 IPA：スマート工場化でのシステムセキュリティ対策事例 調査報告書 https://www.ipa.go.jp/security/controlsystem/securityreport-smartfactory-2023.html〔2024/4/23 確認〕
※ 181 経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその展開 https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html〔2024/4/23 確認〕
※ 182 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〔2024/4/23 確認〕
※ 183 IPA：米 CISA 発行 Cross-Sector Cybersecurity Performance Goals Ver.1.0.1(2023-03)の翻訳 https://www.ipa.go.jp/security/controlsystem/cisacpgs.html〔2024/4/23 確認〕
※ 184 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov〔2024/4/23 確認〕
※ 185 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp〔2024/4/23 確認〕
※ 186 OffSec Services Limited：Exploit Database https://www.exploit-db.com〔2024/4/23 確認〕
※ 187 Synology 社：Synology-SA-22:25 SRM https://www.synology.com/en-us/security/advisory/Synology_SA_22_25〔2024/4/23 確認〕
※ 188 CERT Coordination Center：Vulnerabilities in TP-Link routers, WR710N-V1-151022 and Archer C5 V2 https://kb.cert.org/vuls/id/572615〔2024/4/23 確認〕
※ 189 Zero Day Initiative：(Pwn2Own) TP-Link Archer AX21 merge_country_config Command Injection Remote Code Execution Vulnerability https://www.zerodayinitiative.com/advisories/ZDI-23-451/〔2024/4/23 確認〕
※ 190 TP-Link 社：Download for Archer AX21 V3 https://www.tp-link.com/us/support/download/archer-ax21/v3/〔2024/4/23 確認〕
※ 191 Zero Day Initiative：TP-LINK WAN-SIDE VULNERABILITY CVE-2023-1389 ADDED TO THE MIRAI BOTNET ARSENAL https://www.zerodayinitiative.com/blog/2023/4/21/tp-link-wan-side-vulnerability-cve-2023-1389-added-to-the-mirai-botnet-arsenal〔2024/4/23 確認〕
※ 192 中国の国家支援型サイバー攻撃への IoT 機器の悪用は、2022 年にも発生。詳細は、「情報セキュリティ白書 2023」（https://www.ipa.go.jp/publish/wp-security/2023.html〔2024/4/23 確認〕）の「3.2.4（4）(d) 中国の国家支援型サイバー攻撃への悪用」(p.200) を参照。
※ 193 Check Point Software Technologies Ltd.：THE DRAGON WHO SOLD HIS CAMARO: ANALYZING CUSTOM ROUTER IMPLANT https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/〔2024/4/23 確認〕
※ 194 CERT Coordination Center：New Netcomm router models NF20MESH, NF20, and NL1902 vulnerabilities https://kb.cert.org/vuls/id/986018〔2024/4/23 確認〕
※ 195 Musarubra US LLC：When Pwning Cisco, Persistence is Key - When Pwning Supply Chain, Cisco is Key https://www.trellix.com/blogs/research/when-pwning-cisco-persistence-is-key-when-pwning-supply-chain-cisco-is-key/〔2024/4/23 確認〕
※ 196 Cisco 社：Cisco IOx Application Hosting Environment Command Injection Vulnerability https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL〔2024/4/23 確認〕
※ 197 Cisco 社：Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z〔2024/4/23 確認〕
※ 198 Censys, Inc.：CVE-2023-20198 – Cisco IOS-XE ZeroDay https://censys.com/cve-2023-20198-cisco-ios-xe-zeroday/〔2024/4/23 確認〕
※ 199 Claroty Ltd.：Pwn2Own Toronto 22: Exploit Netgear Nighthawk RAX30 Routers https://claroty.com/team82/research/chaining-five-vulnerabilities-to-exploit-netgear-nighthawk-rax30-routers-at-pwn2own-toronto-2022〔2024/4/23 確認〕
※ 200 ASUS 社：ASUS Product Security Advisory https://www.asus.com/content/asus-product-security-advisory/〔2024/4/23 確認〕
※ 201 TWCERT/CC（台灣電腦網路危機處理暨協調中心）：ASUS RT-AX55、RT-AX56U_V2、RT-AC86U - Format String - 1, 2, 3 https://www.twcert.org.tw/newepaper/cp-151-7354-4e654-3.html〔2024/4/23 確認〕
https://www.twcert.org.tw/tw/cp-132-7355-0ce8d-1.html〔2024/4/23 確認〕
https://www.twcert.org.tw/tw/cp-132-7356-021bf-1.html〔2024/4/23 確認〕
※ 202 Bleeping Computer：ASUS routers vulnerable to critical remote code execution flaws https://www.bleepingcomputer.com/news/security/asus-routers-vulnerable-to-critical-remote-code-execution-flaws/〔2024/4/23 確認〕
※ 203 VulnCheck Inc.：Exploiting MikroTik RouterOS Hardware with CVE-2023-30799 https://vulncheck.com/blog/mikrotik-foisted-revisited〔2024/4/23 確認〕
※ 204 SHODAN：インターネットに接続された機器を探索・調査可能な検索エンジン。
https://www.shodan.io〔2024/4/23 確認〕
※ 205 OT/IoT 向けセルラールーター：3G や 4G 等のセルラー接続を介して重要なローカルネットワークをインターネットに接続するためのルーター。政府機関や商業施設、緊急サービス、エネルギー、交通、上下水道システム、製造業、医療等、複数の重要インフラ分野で使用されている。
※ 206 Forescout Technologies, Inc.：Sierra:21 - Supply Chain Vulnerabilities in IoT/OT routers https://www.forescout.com/research-labs/sierra21/〔2024/4/23 確認〕
Forescout Technologies, Inc.：Sierra:21 – Living on the Edge – Supply Chain Vulnerabilities in OT/IoT Routers https://www.

forescout.com/resources/sierra21-vulnerabilities〔2024/4/23 確認〕
※ 207 株式会社バッファロー：VR-S1000 における複数の脆弱性とその対処方法 https://www.buffalo.jp/news/detail/20231225-01.html〔2024/4/23 確認〕
※ 208 NeroTeam Security Labs S.A.S.：Buffalo VPN VR-S1000 - Vulnerability Report https://neroteam.com/blog/buffalo-vpn-vr-s1000-vulnerability-report〔2024/4/23 確認〕
※ 209 株式会社ラック：【注意喚起】バッファロー製 VR-S1000 における複数の脆弱性（CVE-2023-51363）、早急な対策を https://www.lac.co.jp/lacwatch/alert/20240122_003661.html〔2024/4/23確認〕
※ 210 QNAP 社：Security ID：QSA-23-01, Vulnerability in QTS and QuTS hero https://www.qnap.com/en/security-advisory/qsa-23-01〔2024/4/23 確認〕
※ 211 Censys, Inc.：CVE-2022-27596: The Next Ransomware Target? https://censys.com/cve-2022-27596/〔2024/4/23 確認〕
※ 212 QNAP 社：Security ID：QSA-23-06, Vulnerabilities in QTS, QuTS hero, QuTScloud, and QVP https://www.qnap.com/en/security-advisory/qsa-23-06〔2024/4/23 確認〕
※ 213 QNAP 社：Security ID：QSA-23-31, Vulnerability in QTS, QuTS hero, and QuTScloud https://www.qnap.com/en/security-advisory/qsa-23-31〔2024/4/23 確認〕
QNAP 社：Security ID：QSA-23-35, Vulnerability in QTS, Multimedia Console, and Media Streaming add-on https://www.qnap.com/en/security-advisory/qsa-23-35〔2024/4/23 確認〕
※ 214 Western Digital 社：Western Digital My Cloud OS 5, My Cloud Home and SanDIsk ibi Firmware Update https://www.westerndigital.com/support/product-security/wdc-23009-western-digital-my-cloud-os-5-my-cloud-home-and-sandisk-ibi-firmware-update〔2024/4/23 確認〕
※ 215 Claroty Ltd.：A Pain in the NAS: Exploiting Cloud Connectivity to PWN your NAS: WD PR4100 Edition https://claroty.com/team82/research/a-pain-in-the-nas-exploiting-cloud-connectivity-to-pwn-your-nas-wd-pr4100-edition〔2024/4/23 確認〕
※ 216 Western Digital 社：Western Digital My Cloud OS 5, My Cloud Home and SanDisk ibi Firmware Update https://www.westerndigital.com/support/product-security/wdc-22020-my-cloud-os-5-my-cloud-home-ibi-firmware-update〔2024/4/23 確認〕
Western Digital 社：My Cloud Firmware Version 5.26.119 https://www.westerndigital.com/en-il/support/product-security/wdc-23002-my-cloud-firmware-version-5-26-119〔2024/4/23 確認〕
Western Digital 社：My Cloud Firmware Version 5.26.202 https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202〔2024/4/23 確認〕
※ 217 Zyxel 社：Zyxel security advisory for pre-authentication command injection vulnerability in NAS products https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-pre-authentication-command-injection-vulnerability-in-nas-products〔2024/4/23 確認〕
※ 218 Zyxel 社：Zyxel security advisory for authentication bypass and command injection vulnerabilities in NAS products https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-authentication-bypass-and-command-injection-vulnerabilities-in-nas-products〔2024/4/23 確認〕
※ 219 Claroty Ltd.：A Pain in the NAS: Exploiting Cloud Connectivity to PWN your NAS: Synology DS920+ Edition https://claroty.com/team82/research/a-pain-in-the-nas-exploiting-cloud-connectivity-to-pwn-your-nas-synology-ds920-edition〔2024/4/23 確認〕
※ 220 Claroty Ltd.：Synology NAS DSM Account Takeover: When Random is not Secure https://claroty.com/team82/research/synology-nas-dsm-account-takeover-when-random-is-not-secure〔2024/4/23 確認〕
※ 221 Fortinet, Inc.：TBK DVR Authentication Bypass Attack https://fortiguard.fortinet.com/outbreak-alert/tbk-dvr-attack〔2024/4/23 確認〕
※ 222 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。
※ 223 QNAP 社：Security ID：QSA-23-48, Vulnerability Affecting Legacy VioStor NVR https://www.qnap.com/en/security-advisory/qsa-23-48〔2024/4/23 確認〕
※ 224 Sam Curry：Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More https://samcurry.net/web-hackers-vs-the-auto-industry/〔2024/4/23 確認〕
※ 225 BlackHat USA 2023：Jailbreaking an Electric Vehicle in 2023 or What It Means to Hotwire Tesla's x86-Based Seat Heater https://www.blackhat.com/us-23/briefings/schedule/#jailbreaking-an-electric-vehicle-in--or-what-it-means-to-hotwire-teslas-x-based-seat-heater-33049〔2024/4/23 確認〕
※ 226 SOCRadar：Syrus4 IoT Gateway Vulnerability Could Allow Code Execution on Thousands of Vehicles, Simultaneously (CVE-2023-6248) https://socradar.io/syrus4-iot-gateway-vulnerability-could-allow-code-execution-on-thousands-of-vehicles-simultaneously-cve-2023-6248/〔2024/4/23 確認〕
※ 227 Cisco 社：Cisco IP Phone 6800, 7800, and 8800 Series Web UI Vulnerabilities https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP〔2024/4/23 確認〕
※ 228 ZTP（Zero Touch Provisioning）機能：認定ハードウェアの自動プロビジョニングをサポートする機能。
※ 229 BlackHat USA 2023：Zero-Touch-Pwn: Abusing Zoom's Zero Touch Provisioning for Remote Attacks on Desk Phones https://www.blackhat.com/us-23/briefings/schedule/#zero-touch-pwn-abusing-zooms-zero-touch-provisioning-for-remote-attacks-on-desk-phones-31341〔2024/4/23 確認〕
※ 230 シュナイダー社：Security Notification - SEVD-2023-101-04 Easy UPS Online Monitoring Software https://www.se.com/il/en/download/document/SEVD-2023-101-04/〔2024/4/23 確認〕
※ 231 キヤノン株式会社：CP2023-003 Vulnerability Mitigation/Remediation for Inkjet Printers (Home and Office/Large Format) https://psirt.canon/advisory-information/cp2023-003/〔2024/4/23 確認〕
※ 232 RedTeam Pentesting GmbH：D-Link DAP-X1860: Remote Command Injection https://www.redteam-pentesting.de/en/advisories/rt-sa-2023-006/-d-link-dap-x1860-remote-command-injection〔2024/4/23 確認〕
※ 233 Zyxel 社：Zyxel security advisory for multiple vulnerabilities in firewalls and APs https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-aps〔2024/4/23 確認〕
※ 234 Cyble Inc.：New Medusa Botnet Emerging Via Mirai Botnet Targeting Linux Users https://cyble.com/blog/new-medusa-botnet-emerging-via-mirai-botnet-targeting-linux-users/〔2024/4/23 確認〕
※ 235 Bleeping Computer：Medusa botnet returns as a Mirai-based variant with ransomware sting https://www.bleepingcomputer.com/news/security/medusa-botnet-returns-as-a-mirai-based-variant-with-ransomware-sting/〔2024/4/23 確認〕
※ 236 Palo Alto Networks, Inc.：Mirai Variant V3G4 Targets IoT Devices https://unit42.paloaltonetworks.com/mirai-variant-v3g4/〔2024/4/23 確認〕
パロアルトネットワークス株式会社：IoT デバイスを狙う Mirai の亜種「V3G4」 https://unit42.paloaltonetworks.jp/mirai-variant-v3g4/〔2024/4/23 確認〕
※ 237 Moobot の詳細に関しては、「情報セキュリティ白書 2020」（https://www.ipa.go.jp/publish/wp-security/sec-2020.html〔2024/4/23 確認〕）の「3.2.1（1）（h）Moobot」（p.172）を参照。
※ 238 Fortinet, Inc.：Moobot Strikes Again - Targeting Cacti And RealTek Vulnerabilities https://www.fortinet.com/blog/threat-research/moobot-strikes-again-targeting-cacti-and-realtek-vulnerabilities〔2024/4/23 確認〕
※ 239 詳細は、「情報セキュリティ白書 2022」（https://www.ipa.go.jp/publish/wp-security/sec-2022.html〔2024/4/23 確認〕）の「3.2.2（h）Realtek 社製無線機器向け SDK の脆弱性」（p.180）を参照。
※ 240 Zyxel 社：Zyxel security advisory for OS command injection vulnerability of firewalls https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls〔2024/4/23 確認〕
※ 241 Rapid7 Inc.：AKB - CVE-2023-28771 https://attackerkb.com/topics/N3i8dxpFKS/cve-2023-28771/rapid7-analysis〔2024/4/23 確認〕
※ 242 infosec.exchange：The Shadowserver Foundation https://infosec.exchange/@shadowserver/110442626213838177〔2024/4/23 確認〕
※ 243 Fortinet, Inc.：DDoS Botnets Target Zyxel Vulnerability CVE-2023-28771 https://www.fortinet.com/blog/threat-research/ddos-botnets-target-zyxel-vulnerability-cve-2023-28771〔2024/4/23 確認〕
※ 244 「IH1Z9」の活動は 2018 年 12 月にも観測されている。詳細は、「情報セキュリティ白書 2019」（https://www.ipa.go.jp/archive/

publish/wp-security/sec-2019.html〔2024/4/23確認〕)の「3.2.1(1)(i)Miori／IZ1H9／APEP」(p.165)を参照。
※245 Palo Alto Networks, Inc.：Old Wine in the New Bottle: Mirai Variant Targets Multiple IoT Devices https://unit42.paloaltonetworks.com/mirai-variant-iz1h9/〔2024/4/23 確認〕
パロアルトネットワークス株式会社：新しい瓶に古い酒：Mirai 亜種が複数の IoT デバイスを標的に https://unit42.paloaltonetworks.jp/mirai-variant-iz1h9/〔2024/4/23 確認〕
※246 Zyxel 社：Zyxel security advisory for remote code execution and denial-of-service vulnerabilities of CPE https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-code-execution-and-denial-of-service-vulnerabilities-of-cpe〔2024/4/23 確認〕
※247 Fortinet, Inc.：IZ1H9 Campaign Enhances Its Arsenal with Scores of Exploits https://www.fortinet.com/blog/threat-research/Iz1h9-campaign-enhances-arsenal-with-scores-of-exploits〔2024/4/23 確認〕
※248 Palo Alto Networks, Inc.：IoT Under Siege: The Anatomy of the Latest Mirai Campaign Leveraging Multiple IoT Exploits https://unit42.paloaltonetworks.com/mirai-variant-targets-iot-exploits/〔2024/4/23 確認〕
パロアルトネットワークス株式会社：沈黙の IoT: 複数の IoT エクスプロイトを悪用する最新 Mirai キャンペーンの解剖 https://unit42.paloaltonetworks.jp/mirai-variant-targets-iot-exploits/〔2024/4/23 確認〕
※249 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。
※250 Akamai Technologies, Inc.：InfectedSlurs Botnet Spreads Mirai via Zero-Days https://www.akamai.com/blog/security-research/new-rce-botnet-spreads-mirai-via-zero-days〔2024/4/23 確認〕
※251 「JenX」の詳細は、「情報セキュリティ白書 2019」(https://www.ipa.go.jp/archive/publish/wp-security/sec-2019.html〔2024/4/23 確認〕)の「3.2.1(1)(b)JenX ／ Jennifer」(p.163)を参照。
※252 Akamai Technologies, Inc.：Actively Exploited Vulnerability in FXC Routers: Fixed, Patches Available https://www.akamai.com/blog/security-research/zero-day-vulnerability-spreading-mirai-patched〔2024/4/23 確認〕
※253 Akamai Technologies, Inc.：Actively Exploited Vulnerability in QNAP VioStor NVR: Fixed, Patches Available https://www.akamai.com/blog/security-research/qnap-viostor-zero-day-vulnerability-spreading-mirai-patched〔2024/4/23 確認〕
※254 Akamai Technologies, Inc.：Uncovering HinataBot: A Deep Dive into a Go-Based Threat https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet〔2024/4/23 確認〕
※255 Dark Reading：Mirai Hackers Use Golang to Create a Bigger, Badder DDoS Botnet https://www.darkreading.com/vulnerabilities-threats/mirai-hackers-golang-bigger-badder-ddos-botnet〔2024/4/23 確認〕
Miraiの最盛期の攻撃に関しては、「情報セキュリティ白書2017」の「3.2.1(1)Mirai による DDoS 攻撃の脅威」(p.174)を参照。
※256 Fortinet, Inc.：AndoryuBot – New Botnet Campaign Targets Ruckus Wireless Admin Remote Code Execution Vulnerability (CVE-2023-25717) https://www.fortinet.com/blog/threat-research/andoryubot-new-botnet-campaign-targets-ruckus-wireless-admin-remote-code-execution-vulnerability-cve-2023-25717〔2024/4/23 確認〕
※257 JPCERT/CC:Linux ルーターを狙った Go 言語で書かれたマルウェア GobRAT https://blogs.jpcert.or.jp/ja/2023/05/gobrat.html〔2024/4/23 確認〕
※258 Lumen Black Lotus Labs：Routers From The Underground: Exposing AVrecon（2023 年 7 月 12 日公開） https://blog.lumen.com/routers-from-the-underground-exposing-avrecon/〔2024/4/23 確認〕
※259 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。同様の事例としては、「情報セキュリティ白書2023」(https://www.ipa.go.jp/publish/wp-security/2023.html〔2024/4/23 確認〕)の「3.2.4(4)(b)プロキシーとしての悪用」(p.200)を参照。
※260 Krebs on Security：Who and What is Behind the Malware Proxy Service SocksEscort? https://krebsonsecurity.com/2023/07/who-and-what-is-behind-the-malware-proxy-service-socksescort/〔2024/4/23 確認〕
※261 Qualys, Inc.：CVE-2023-4911: Looney Tunables – Local Privilege Escalation in the glibc' s ld.so https://blog.qualys.com/vulnerabilities-threat-research/2023/10/03/cve-2023-4911-looney-tunables-local-privilege-escalation-in-the-glibcs-ld-so〔2024/4/23 確認〕
※262 SonarSource SA：pfSense Security: Sensing Code Vulnerabilities with SonarCloud https://www.sonarsource.com/blog/pfsense-vulnerabilities-sonarcloud/〔2024/4/23 確認〕
※263 BitSight Technologies, Inc.：New high-severity vulnerability (CVE-2023-29552) discovered in the Service Location Protocol (SLP) https://www.bitsight.com/blog/new-high-severity-vulnerability-cve-2023-29552-discovered-service-location-protocol-slp〔2024/4/23 確認〕
※264 CISA：Abuse of the Service Location Protocol May Lead to DoS Attacks https://www.cisa.gov/news-events/alerts/2023/04/25/abuse-service-location-protocol-may-lead-dos-attacks〔2024/4/23 確認〕
※265 Cisco 社：Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers Vulnerabilities https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5〔2024/4/23 確認〕
※266 Bleeping Computer：Over 19,000 end-of-life Cisco routers exposed to RCE attacks https://www.bleepingcomputer.com/news/security/over-19-000-end-of-life-cisco-routers-exposed-to-rce-attacks/〔2024/4/23 確認〕
※267 Cisco 社：Cisco SPA112 2-Port Phone Adapters Remote Command Execution Vulnerability https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-unauth-upgrade-UqhyTWW〔2024/4/23 確認〕
※268 CISA：ICS ADVISORY - Socomec MOD3GP-SY-120K https://www.cisa.gov/news-events/ics-advisories/icsa-23-250-03〔2024/4/23 確認〕
※269 ESET, spol. s r.o.：ESET Discovers Corporate Secrets and Data on Recycled Company Routers https://www.eset.com/int/about/newsroom/press-releases/research/eset-discovers-corporate-secrets-and-data-on-recycled-company-routers/〔2024/4/23 確認〕
※270 https://notice.go.jp〔2024/4/23 確認〕
※271 https://notice.go.jp/status〔2024/5/13 確認〕
※272 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/〔2024/4/23 確認〕
※273 MVPower 社製 DVR TV-7104HE の脆弱性(EDB-ID：41471)については以下を参照。
OffSec Services Limited：MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution (Metasploit) https://www.exploit-db.com/exploits/41471〔2024/4/23 確認〕
※274 NETGEAR 社製ルーター DGN1000 の脆弱性（EDB-ID: 43055)については以下を参照。
OffSec Services Limited：Netgear DGN1000 1.1.00.48 - 'Setup.cgi' Remote Code Execution (Metasploit) https://www.exploit-db.com/exploits/43055〔2024/4/23 確認〕
※275 株式会社インターネットイニシアティブ：wizSafe Security Signal 2023年1月 観測レポート https://wizsafe.iij.ad.jp/2023/02/1524/〔2024/4/23 確認〕
※276 株式会社インターネットイニシアティブ：wizSafe Security Signal 2023年2月 観測レポート https://wizsafe.iij.ad.jp/2023/03/1537/〔2024/4/23 確認〕
※277 株式会社インターネットイニシアティブ：wizSafe Security Signal 2023年3月 観測レポート https://wizsafe.iij.ad.jp/2023/04/1546/〔2024/4/23 確認〕
※278 株式会社インターネットイニシアティブ：wizSafe Security Signal 2023年5月 観測レポート https://wizsafe.iij.ad.jp/2023/06/1568/〔2024/4/23 確認〕
※279 株式会社インターネットイニシアティブ：wizSafe Security Signal 2023年6月 観測レポート https://wizsafe.iij.ad.jp/2023/07/1576/〔2024/4/23 確認〕
※280 株式会社インターネットイニシアティブ：wizSafe Security Signal 2023年7月 観測レポート https://wizsafe.iij.ad.jp/2023/08/1588/〔2024/4/23 確認〕
※281 株式会社インターネットイニシアティブ：wizSafe Security Signal 2023 年 10 月 観測レポート https://wizsafe.iij.ad.jp/2023/11/1625/〔2024/4/23 確認〕
※282 Cloudflare, Inc.：DDoS threat report for 2023 Q1 https://blog.cloudflare.com/ddos-threat-report-2023-q1/〔2024/4/23 確認〕
※283 Cloudflare, Inc.：DDoS threat report for 2023 Q2 https://blog.cloudflare.com/ddos-threat-report-2023-q2/〔2024/4/23 確認〕

※ 284 Cloudflare, Inc. : DDoS threat report for 2023 Q3 https://blog.cloudflare.com/ddos-threat-report-2023-q3/〔2024/4/23 確認〕
※ 285 Cloudflare, Inc. : DDoS threat report for 2023 Q4 https://blog.cloudflare.com/ddos-threat-report-2023-q4/〔2024/4/23 確認〕
※ 286 AO Kaspersky Lab : Kaspersky releases overview of IoT-related threats in 2023 https://usa.kaspersky.com/about/press-releases/2023_kaspersky-releases-overview-of-iot-related-threats-in-2023〔2024/4/23 確認〕
AO Kaspersky Lab : Overview of IoT threats in 2023 https://securelist.com/iot-threat-report-2023/110644/〔2024/4/23 確認〕
※ 287 Microsoft Corporation : IoT devices and Linux-based systems targeted by OpenSSH trojan campaign https://www.microsoft.com/en-us/security/blog/2023/06/22/iot-devices-and-linux-based-systems-targeted-by-openssh-trojan-campaign/〔2024/4/23 確認〕
※ 288 Aqua Security Software Ltd. : Tomcat Under Attack: Exploring Mirai Malware and Beyond https://www.aquasec.com/blog/tomcat-under-attack-investigating-the-mirai-malware/〔2024/4/23 確認〕
※ 289 Lumen Technologies, Inc. : Routers Roasting On An Open Firewall: The KV-Botnet Investigation https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/〔2024/4/23 確認〕
※ 290 Joint Cybersecurity Advisory : People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF〔2024/4/23 確認〕
Microsoft Corporation : Volt Typhoon targets US critical infrastructure with living-off-the-land techniques https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/〔2024/4/23 確認〕
※ 291 GOV.UK : Starting gun fired on preparations for new product security regime https://www.gov.uk/government/news/starting-gun-fired-on-preparations-for-new-product-security-regime〔2024/5/21 確認〕
※ 292 GOV.UK : The UK Product Security and Telecommunications Infrastructure (Product Security) regime https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime〔2024/4/23 確認〕
※ 293 European Commission : Commission welcomes political agreement on Cyber Resilience Act https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168〔2024/4/23 確認〕
※ 294 Council of the European Union : Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 - Letter sent to the European Parliament https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_17000_2023_INIT〔2024/4/23 確認〕
※ 295 The White House : Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/〔2024/4/23 確認〕
※ 296 Cyber Security Agency of Singapore : Cybersecurity Labelling Scheme (CLS) - Updates https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/updates〔2024/4/23 確認〕
※ 297 Cybersecurity Advisory : People's Republic of China-Linked Cyber Actors Hide in Router Firmware https://www.ic3.gov/Media/News/2023/230927.pdf〔2024/4/23 確認〕
※ 298 NIST : Lightweight Cryptography Standardization Process: NIST Selects Ascon https://csrc.nist.gov/news/2023/lightweight-cryptography-nist-selects-ascon〔2024/4/23 確認〕
※ 299 NIST : NIST IR 8454: Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process https://csrc.nist.gov/pubs/ir/8454/final〔2024/4/23 確認〕
※ 300 https://www.meti.go.jp/policy/netsecurity/chusyosecurityguide.pdf〔2024/4/23 確認〕
※ 301 https://www.soumu.go.jp/main_content/000895981.pdf〔2024/4/23 確認〕
※ 302 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〔2024/4/23 確認〕
※ 303 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〔2024/4/23 確認〕
※ 304 一般社団法人セキュア IoT プラットフォーム協議会 : セキュア IoT プラットフォーム協議会が「IoT セキュリティ手引書 Ver3.0」をリリース https://www.secureiotplatform.org/release/2023-09-26〔2024/4/23 確認〕
※ 305 https://csrc.nist.gov/pubs/sp/800/216/final〔2024/4/23 確認〕
※ 306 https://csrc.nist.gov/pubs/sp/1800/36/2prd〔2024/4/23 確認〕
※ 307 NIST : Cybersecurity Framework https://www.nist.gov/cyberframework〔2024/4/23 確認〕
※ 308 JUAS : 企業 IT 動向調査 https://juas.or.jp/library/research_rpt/it_trend/〔2024/5/2 確認〕
※ 309 https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR202200_002.pdf〔2024/5/2 確認〕
※ 310 JUAS : 企業 IT 動向調査報告書 2024 https://juas.or.jp/cms/media/2024/04/JUAS_IT2024.pdf〔2024/5/2 確認〕
※ 311 株式会社エイチーム : 個人情報漏えいの可能性に関するお知らせ https://www.a-tm.co.jp/news/43858/〔2024/5/2 確認〕
※ 312 株式会社エイチーム : 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/44238/〔2024/5/2 確認〕
※ 313 トヨタ自動車株式会社 : クラウド環境の誤設定によるお客様情報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/39174380.html〔2024/5/2 確認〕
※ 314 トヨタ自動車株式会社 : クラウド設定によるお客様情報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/39241571.html〔2024/5/2 確認〕
※ 315 個人情報保護委員会 : トヨタ自動車株式会社による個人データの漏えい等事案に対する個人情報の保護に関する法律に基づく行政上の対応について https://www.ppc.go.jp/files/pdf/230712_01_houdou.pdf〔2024/5/2 確認〕
※ 316 NHK : 「NauNau」230 万人以上 位置情報など外部から閲覧可能な状態に https://www3.nhk.or.jp/news/html/20231021/k10014232891000.html〔2024/5/2 確認〕
※ 317 株式会社モバイルファクトリー : Suishow 株式会社に関する報道について https://www.mobilefactory.jp/newsrelease/2023/20231023/〔2024/5/2 確認〕
※ 318 Suishow 株式会社 : 当社運営の「NauNau」をご利用いただいているお客様への重要なお知らせとお詫びについて https://www.mobilefactory.jp/wp-content/uploads/2023/12/c97ba9d2edf12d1a16fef3806bea77f2-1.pdf〔2024/5/2 確認〕
※ 319 エン・ジャパン株式会社 : 「エン転職」への不正ログイン発生に関するお詫びとお願い https://corp.en-japan.com/newsrelease/2023/32484.html〔2024/5/2 確認〕
※ 320 株式会社ディノス・セシール : 弊社「セシールオンラインショップ」への“なりすまし”による不正アクセスについて https://www.cecile.co.jp/fst/information/cecile_20230516.pdf〔2023/5/20 確認〕
株式会社サイバーセキュリティ総研 : 第三者による不正ログインでユーザー情報流出か「セシールオンラインショップ」 https://cybersecurity-info.com/news/cecile-online-shop-unauthorized-login/〔2024/5/2 確認〕
ScanNetSecurity : 不正ログイン成功3件にとどまる、「セシールオンラインショップ」へのなりすましによる不正アクセス https://scan.netsecurity.ne.jp/article/2023/05/25/49412.html〔2024/5/17 確認〕
※ 321 株式会社ディノス・セシール : 弊社「セシールオンラインショップ」への不正アクセスとお客様情報流出の可能性に関するお詫びとお知らせ https://www.cecile.co.jp/fst/information/c_20180606.pdf〔2024/5/2 確認〕
※ 322 株式会社エムケイシステム : 【お詫び】弊社製品障害に関するご報告 https://www.mks.jp/company/topics/20230605〔2024/5/2 確認〕
株式会社エムケイシステム : 第三者によるランサムウェア感染被害のお知らせ https://contents.xj-storage.jp/xcontents/AS97180/bc464498/fb3c/479a/ad33/51ec0cd39818/140120230606596742.pdf〔2024/5/2 確認〕
※ 323 LINE ヤフー株式会社 : 不正アクセスによる、情報漏えいに関するお知らせとお詫び https://www.lycorp.co.jp/ja/ir/news/auto_20231127594672/main/0/link/Notice and apology regarding information leakage due to unauthorized access_JP.pdf〔2024/5/2 確認〕
※ 324 LINE ヤフー株式会社 : 不正アクセスによる、情報漏えいに関するお知らせとお詫び（2024/2/14 更新） https://www.lycorp.co.jp/ja/news/announcements/007712/〔2024/5/2 確認〕
※ 325 LINE ヤフー株式会社 : 委託先 2 社のアカウントを利用した不正アクセスによる、従業者等の情報漏えいに関するお知らせとお詫び

https://www.lycorp.co.jp/ja/news/announcements/007711/〔2024/5/2 確認〕
※ 326 LINE 株式会社：個人情報保護委員会からの個人情報の取扱い等に係る報告および当社における今後の方針について https://linecorp.com/ja/pr/news/ja/2021/3682〔2024/5/2 確認〕
LINE ヤフー株式会社：LINE のデータ移転に関するご説明 https://www.lycorp.co.jp/ja/news/announcements/000823/〔2024/5/2 確認〕
※ 327 以下の Web ページで「Post Incident Review (PIR) – Azure Networking – Global WAN issues（Tracking ID: VSG1-B90）」を参照した。
Microsoft 社：Azure status history https://azure.status.microsoft/en-us/status/history/〔2024/5/2 確認〕
※ 328 Amazon Web Services, Inc.：Service health https://health.aws.amazon.com/health/status〔2024/5/2 確認〕
※ 329 CNN：アマゾンのクラウドサービスに大規模障害 トランプ氏出廷の報道にも影響 https://www.cnn.co.jp/tech/35205182.html〔2024/5/2 確認〕
※ 330 日本経済新聞：AWS、一時大規模障害 スマホで家電など操作できず https://www.nikkei.com/article/DGXZQOGN140DN0U3A610C2000000/〔2024/5/2 確認〕
※ 331 Amazon Web Services, Inc.：Summary of the AWS Lambda Service Event in Northern Virginia (US-EAST-1) Region https://aws.amazon.com/jp/message/061323/〔2024/5/2 確認〕
※ 332 Google 社：Google Cloud Service Health > Incidents > Multiple Google Cloud services in the europe-west9-a zone are impacted https://status.cloud.google.com/incidents/dS9ps52MUnxQfyDGPfkY〔2024/5/2 確認〕
※ 333 NTT 西日本：2023 年 4 月 3 日に発生した通信サービスへの影響について https://www.ntt-west.co.jp/brand/20230428_1/〔2024/5/2 確認〕
※ 334 東日本電信電話株式会社:2023 年 4 月 3 日に発生した通信サービスへの影響について https://www.ntt-east.co.jp/corporate/20230428.html〔2024/5/2 確認〕
※ 335 ITmedia：NTT 東西の「フレッツ光」大規模障害、原因は特定のサーバから届いた“特殊なパケット”だった https://www.itmedia.co.jp/news/articles/2304/03/news168.html〔2024/5/2 確認〕
※ 336 読売新聞オンライン：海底ケーブル切断で電話やネット遮断、中国船関与か…台湾本島で同様の事態懸念 https://www.yomiuri.co.jp/world/20230302-OYT1T50368/〔2024/5/2 確認〕
※ 337 NHK：知られざる海底ケーブルの世界 https://www3.nhk.or.jp/news/html/20230620/k10014104331000.html〔2024/5/2 確認〕
※ 338 NTT 西日本：ニュースリリース https://www.ntt-west.co.jp/news/〔2024/3/4 確認〕
※ 339 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） https://www.soumu.go.jp/main_content/000771515.pdf〔2024/5/2 確認〕
※ 340 https://www.ipa.go.jp/publish/wp-security/qv6pgp0000000vgi-att/000100472.pdf〔2024/5/2 確認〕
※ 341 CISA：Stakeholder-Specific Vulnerability Categorization (SSVC) https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc〔2024/5/2 確認〕
※ 342 Forum of Incident Response and Security Teams, Inc.：Exploit Prediction Scoring System (EPSS) https://www.first.org/epss/〔2024/5/2 確認〕
※ 343 CISA：Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog〔2024/5/2 確認〕
※ 344 https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html〔2024/5/2 確認〕
※ 345 FIDO Alliance：Passkeys (Passkey Authentication) https://fidoalliance.org/passkeys/〔2024/5/2 確認〕
※ 346 1Password：Passkeys.directory（パスキー認証に対応する大手クラウドサービスの一覧） https://passkeys.directory/〔2024/5/2 確認〕
※ 347 JISC：https://www.jisc.go.jp/index.html〔2024/5/2 確認〕
※ 348 MDN：ウェブ認証 API – Web API https://developer.mozilla.org/ja/docs/Web/API/Web_Authentication_API〔2024/5/2 確認〕
※ 349 FIDO Alliance：Get Started on Your Passwordless Journey https://fidoalliance.org/implement-passkeys-overview/〔2024/5/2 確認〕
※ 350 ケータイ Watch：パスワードレス認証でフィッシング被害にも効果あり! パスキーを展開する「FIDO アライアンス」の現況とこれから https://k-tai.watch.impress.co.jp/docs/news/1553203.html〔2024/5/2 確認〕
※ 351 情報マネジメントシステム認定センター（ISMS-AC）：ISMS クラウドセキュリティ認証 https://isms.jp/isms-cls.html〔2024/5/2 確認〕
※ 352 ISO：ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services https://www.iso.org/standard/43757.html〔2024/5/2 確認〕
※ 353 日本公認会計士協会（JICPA）：AICPA「セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関する Trust サービス規準」の翻訳の公表について https://jicpa.or.jp/specialized_field/ITI/2022/20221228tzq.html〔2024/5/2 確認〕
※ 354 CSA（Cloud Security Alliance）：CSA の認証制度：STAR 認証について https://cloudsecurityalliance.jp/newblog/2021/10/07/csa の認証制度について /〔2024/5/2 確認〕
※ 355 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）：CCM WG https://www.cloudsecurityalliance.jp/site/?page_id=2048#ccm〔2024/5/2 確認〕
※ 356 JIPDEC：「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」改訂版 公開 https://www.jipdec.or.jp/news/news/20220531.html〔2024/5/2 確認〕

付録

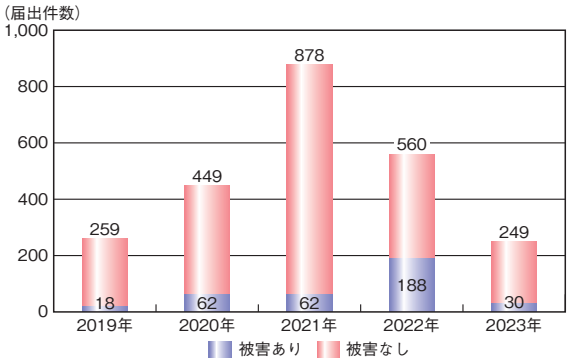
資料

資料A　2023年のコンピュータウイルス届出状況

IPA が 2023 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

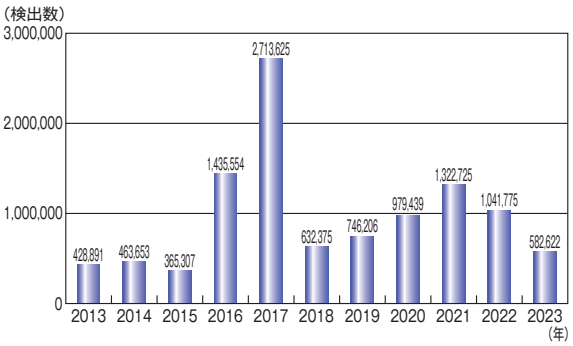
2023 年の年間届出件数は、前年の 560 件より 311 件（55.5%）少ない 249 件であった（図 A-1）。そのうち、ウイルス感染の実被害があった届出は 30 件であった。



■図 A-1　ウイルス届出件数推移（2019～2023 年）

A.2　届出のあったウイルス等検出数

2023 年に寄せられたウイルス等の検出数は、前年の 104 万 1,775 個より 45 万 9,153 個（44.1%）少ない 58 万 2,622 個であった（図 A-2）。



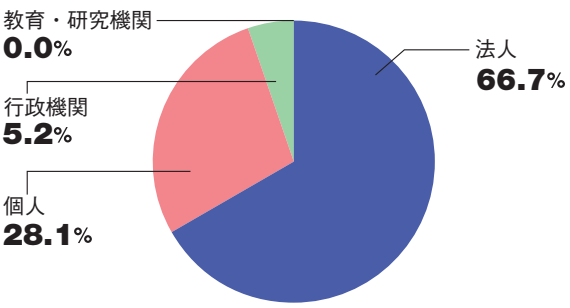
■図 A-2　ウイルス等検出数推移（2013～2023 年）

A.3　届出者の主体別届出件数

2023 年の主体別届出件数は前年と比較すると、全体的に減少した。主体別の比率では「法人」からの届出が 66.7%（166 件）と最も多かった（表 A-1、図 A-3）。

届出者の主体	2021 年	2022 年	2023 年
法人	284	388	166
個人	578	145	70
行政機関	15	18	13
教育・研究機関	1	9	0
合計（件）	878	560	249

■表 A-1　ウイルス届出者の主体別届出件数（2021～2023 年）



■図 A-3　ウイルス届出者の主体別届出件数の比率（2023 年）

A.4　傾向

2023 年でウイルス感染の実被害に遭った届出 30 件のうち、ランサムウェアの感染被害が 11 件あった。また、Emotet の感染被害も同じく 11 件あり、2022 年で実被害に遭った届出 188 件のうち、Emotet の感染被害が 145 件であったことに比べると大幅に減少したものの届出はされている。なお、Emotet に関しては不定期に休止・再開を繰り返しており、今後、再び大規模な攻撃活動が開始される可能性もあるため、引き続き警戒をしていただきたい。

これらの届出件数の詳細は、下記の資料から参照可能であり、ランサムウェアの攻撃手口や対策に関しては、本白書の「1.2.1 ランサムウェア攻撃」にて詳しく述べているので、ぜひそちらを一読いただきたい。

参照

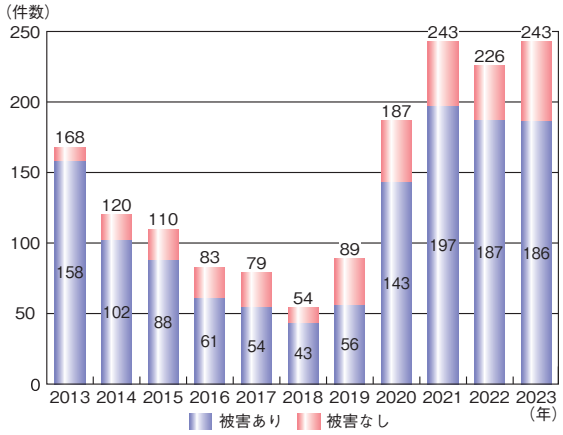
■コンピュータウイルス・不正アクセスの届出状況［2023年（1月～12月）］
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-report.pdf

資料B　2023年のコンピュータ不正アクセス届出状況

IPA が 2023 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

2023 年の年間届出件数は、前年の 226 件より 17 件（7.5%）多い 243 件であった（図 B-1）。そのうち、実被害があった届出は 186 件であった。



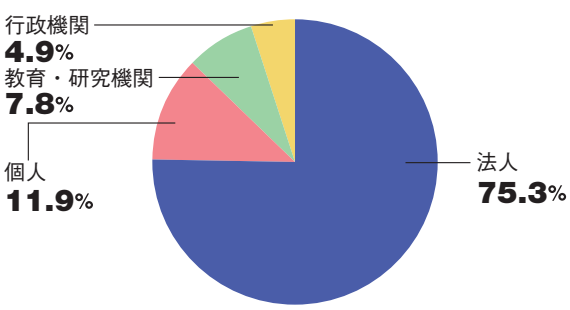
■図 B-1　不正アクセス届出件数推移（2013 年～2023 年）

B.2　届出者の主体別届出件数

2023 年は前年と比較すると、「法人」からの届出件数が増加した一方で、その他の届出件数は減少している。届出者の主体別の比率で見ると「法人」からの届出が 75.3%（183 件）と最も多かった（表 B-1、図 B-2）。

届出者の主体	2021 年	2022 年	2023 年
法人	156	137	183
個人	46	50	29
教育・研究機関	22	21	19
行政機関	19	18	12
合計（件）	243	226	243

■表 B-1　不正アクセス届出者の主体別届出件数（2021～2023 年）

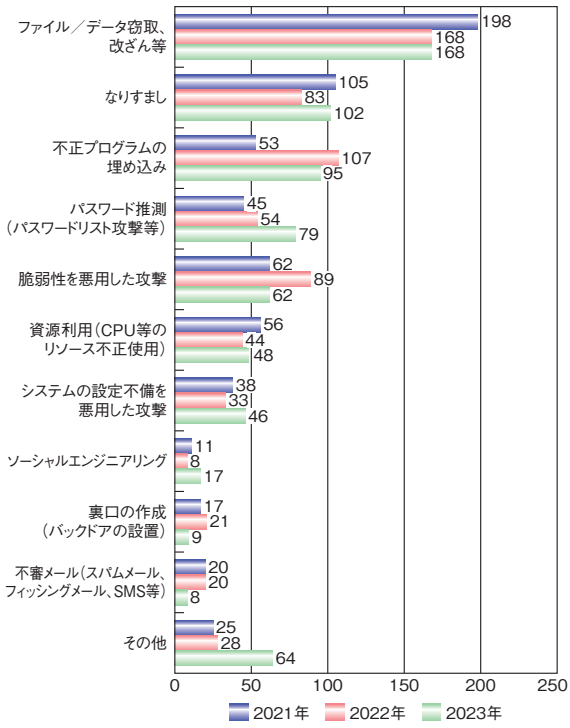


■図 B-2　不正アクセス届出者の主体別届出件数の比率（2023 年）

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。

2023 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「なりすまし」が 102 件、「不正プログラムの埋め込み」が 95 件であった。



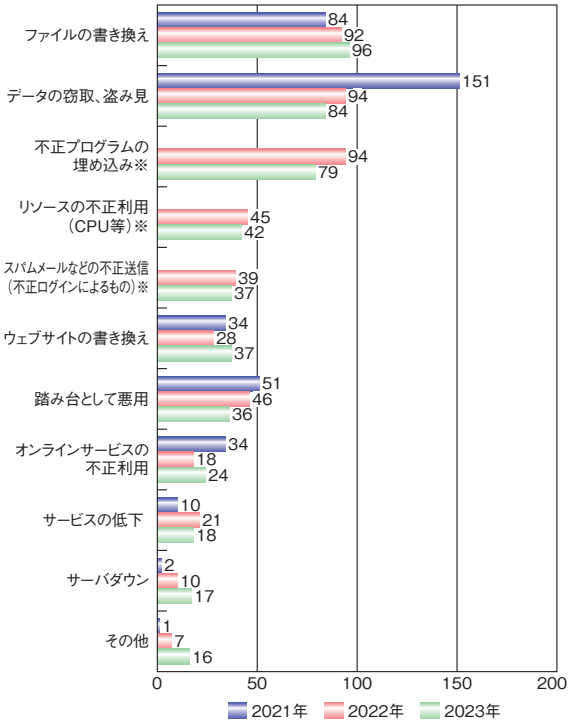
■図 B-3　不正アクセス手口別件数の推移（2021～2023 年）

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。2023 年の届出において最も多く見られた被害は、「ファイルの書き換え」の 96 件であった。次いで「データの窃取、盗み見」が 84 件、「不正プログラムの埋め込み」が 79 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［2023 年上半期（1 月～ 6 月）］」及び「コン

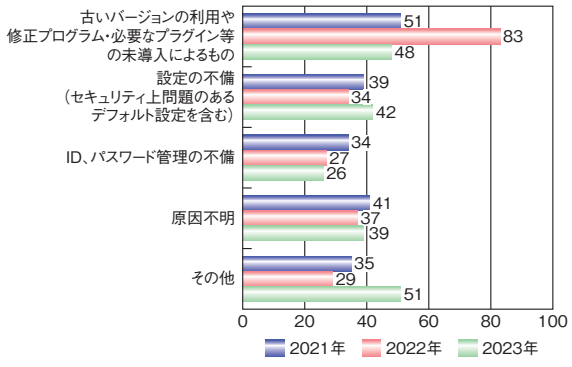
ピュータウイルス・不正アクセスの届出事例［2023 年下半期（7 月～ 12 月）］」を紹介している。そちらも、ぜひ参考にしていただきたい。



■図 B-4　不正アクセス被害内容別件数の推移（2021～2023 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。2023 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 48 件であった。次いで「設定の不備（セキュリティ上問題のあるデフォルト設定を含む）」が 42 件、「ID、パスワード管理の不備」が 26 件であった。



■図 B-5　不正アクセス原因別件数の推移（2021～2023 年）

B.6 傾向と対策

不正アクセスの傾向と対策について述べる。

(1) 傾向

図 B-1 に示した 2023 年に届出された 243 件について、不正アクセス（被害なしも含む）の傾向を分析したところ、「Web サイトの脆弱性や設定不備の悪用に関する不正アクセス」が 65 件、「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ランサムウェア攻撃に関する不正アクセス」が 52 件確認された。また、「パスワードリスト攻撃や総当たり攻撃で、認証を突破されたことによる、メールアカウント等の不正アクセス」が 44 件あった。

(2) 対策

(1)で示した脆弱性や設定不備の対策としては、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や修正プログラムの適用、設定の定期的な見直しといった、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。企業・組織においては、脆弱性診断やペネトレーションテスト等を行い、確実に脆弱性や設定不備を解消することが望まれる。なお、ソフトウェア等の脆弱性対策に関しては、本白書の「1.2.5 ソフトウェアの脆弱性を悪用した攻撃」も参照していただきたい。

メールアカウント等の不正アクセスに関する対策としては、企業・組織やシステム利用者に限らず、他者に推測されにくい複雑なパスワードを設定する、パスワードの使い回しをしない等の基本的な対策を実施することに加え、利用しているシステムで多要素認証等のセキュリティオプションが用意されている場合には積極的に採用する等、今一度、アカウントが適切に管理できているか見直すことを勧める。

参照

■コンピュータウイルス・不正アクセスの届出状況［2023年（1月～12月）］
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-report.pdf

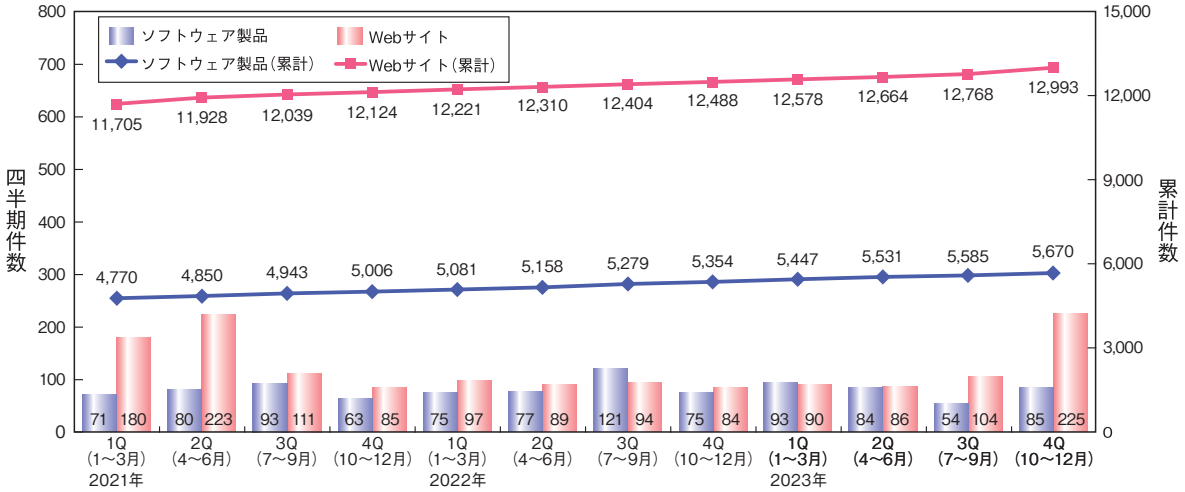
資料C　ソフトウェア等の脆弱性関連情報に関する届出状況

IPA が受け付けたソフトウェア製品や Web サイトの脆弱性の情報について、届出件数や処理の状況を述べる。

C.1　脆弱性の届出概況

2023 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 5,670 件、Web サイトに関するもの 1 万 2,993 件、合計 1 万 8,663 件で、Web サイトに関する届出が全体の 69.6% 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、2023 年第 4 四半期末時点で 3.93 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

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）	2023年1Q（1~3月）	2023年2Q（4~6月）	2023年3Q（7~9月）	2023年4Q（10~12月）
4.04	4.06	4.05	4.02	4.01	3.99	3.98	3.97	3.95	3.94	3.92	3.93

■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）

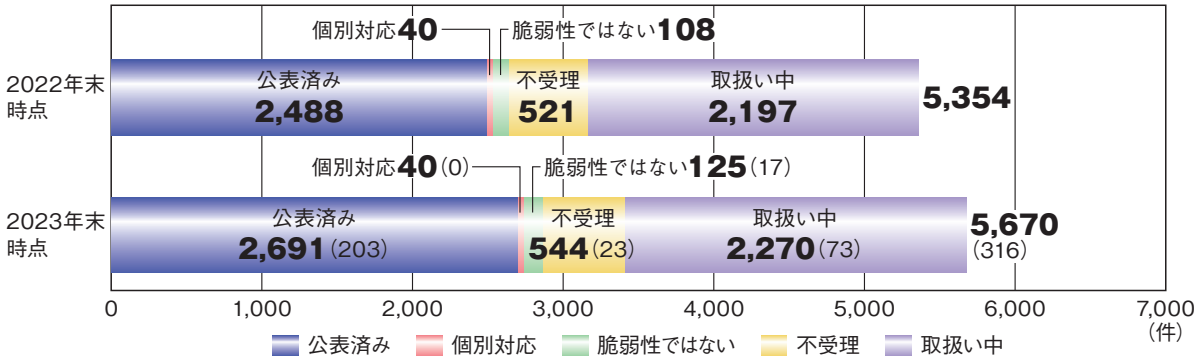
C.2　ソフトウェア製品の脆弱性届出の処理状況

ソフトウェア製品に関する脆弱性届出の 2023 年における処理件数及び 2023 年末時点での処理状況別の累計件数について図 C-2 に示す。

2023 年の届出のうち、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「公表済み」のものは 203 件で累計 2,691 件、JVN で公表せず製品開発者が「個別対応」を行ったものは 0 件で累計 40 件、製品開発者が「脆弱性ではない」と判断したものは 17 件で累計 125 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 23 件で累計 544 件となり、これらをまとめた「処理の終了」件数は 243 件で累計 3,400 件に達した。また、「取扱い中」の届出は 73 件増加して 2,270 件となり、ソフトウェア製品に関する届出は累計 5,670 件となった。

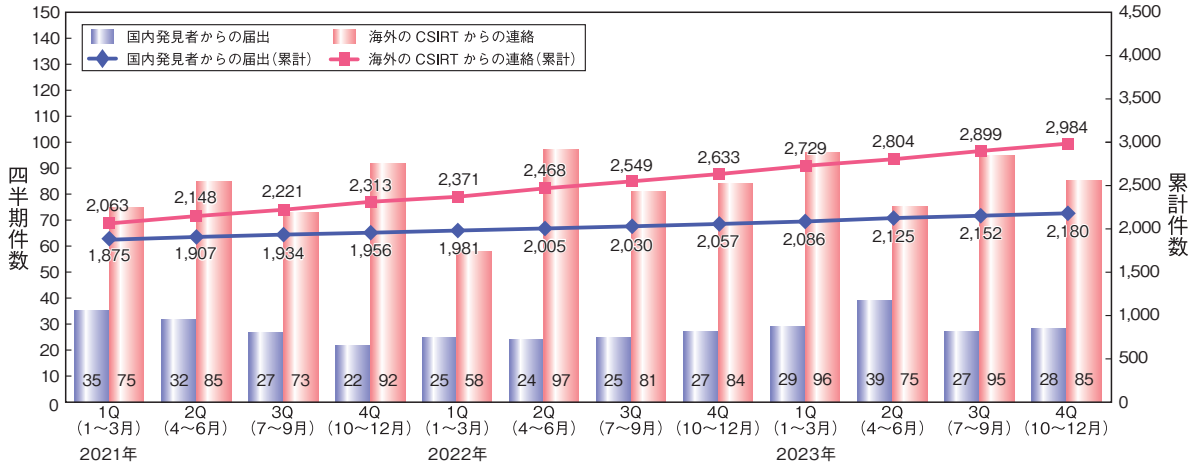
ソフトウェア製品の脆弱性対策情報の公表件数の累計は、国内発見者からの届出を公表したものが 2,180 件、海外の CSIRT から JPCERT/CC が連絡を受けたものを JVN で公表したものが 2,984 件となった。これらソフトウェア製品の脆弱性対策情報の公表件数の期別推移を図 C-3 に示す。

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、図 C-2 の「公表済み」の件数と図 C-3 の公表件数は異なっている。



※( )内の数値は 2022 年末時点と 2023 年末時点の差分

■図 C-2　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



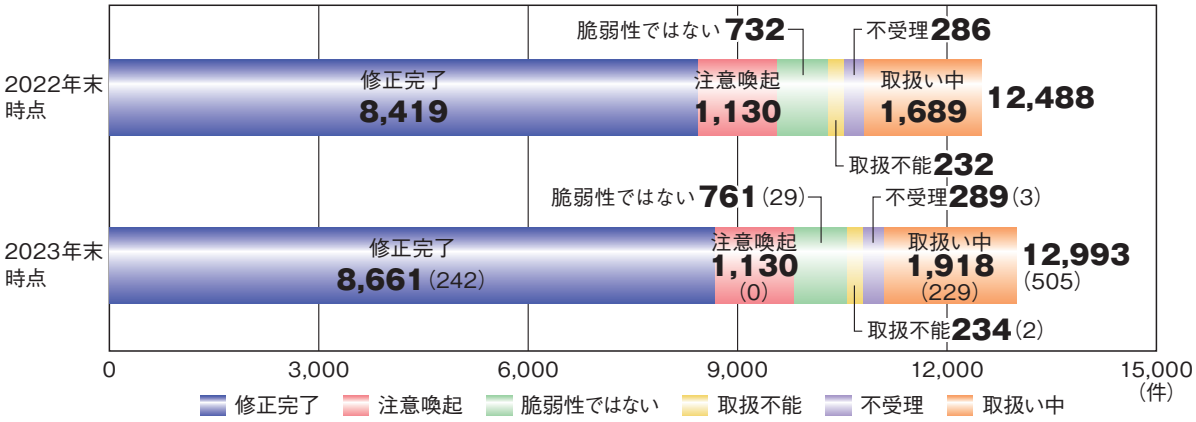
■図 C-3　ソフトウェア製品の脆弱性対策情報の公表件数

C.3 Webサイトの脆弱性届出の処理状況

Web サイトに関する脆弱性届出の 2023 年における処理件数及び 2023 年末時点での処理状況別の累計件数について図 C-4 に示す。

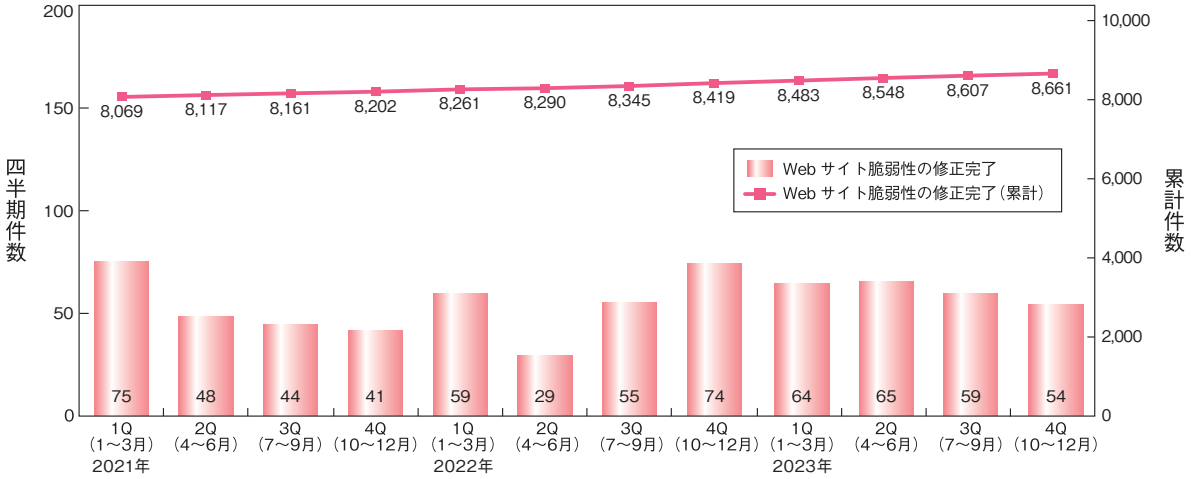
2023 年の届出のうち、IPA が通知を行い Web サイト運営者が「修正完了」としたものは 242 件で累計 8,661 件、IPA が「注意喚起」等を行った後に処理を終了したものは 0 件で累計 1,130 件、IPA 及び Web サイト運営者が「脆弱性ではない」と判断したものは 29 件で累計 761 件、Web サイト運営者と連絡が不可能なもの、または IPA が対応を促しても修正完了した旨の報告をしない、修正を拒否する等、Web サイト運営者の対応により「取扱不能」なものは 2 件で累計 234 件、告示で定める届出の対象に該当せず「不受理」としたものは 3 件で累計 289 件となり、これらをまとめた「処理の終了」件数は 276 件で累計 1 万 1,075 件に達した。また、「取扱い中」の届出は 229 件増加して 1,918 件となり、Web サイトに関する届出は累計 1 万 2,993 件となった。

これらのうち、「修正完了」件数の期別推移を図 C-5 に示す。



※( )内の数値は 2022 年末時点と 2023 年末時点の差分

■図 C-4　Web サイトの脆弱性関連情報の届出の処理状況の推移



■図 C-5　Web サイトの脆弱性の修正完了件数

参照

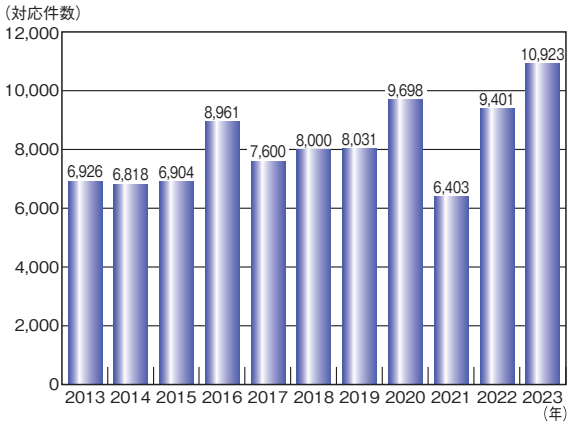
■ソフトウェア等の脆弱性関連情報に関する届出状況［2023年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/reports/vuln/software/2023q4.html

資料D　2023年の情報セキュリティ安心相談窓口の相談状況

IPA が 2023 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

2023 年の年間相談対応件数は 10,923 件となり、2022 年の相談対応件数 9,401 件より 1,522 件（16.2%）の増加となった（図 D-1）。



■図 D-1　相談対応件数の推移（2013～2023 年）

D.2　相談者の主体別相談件数

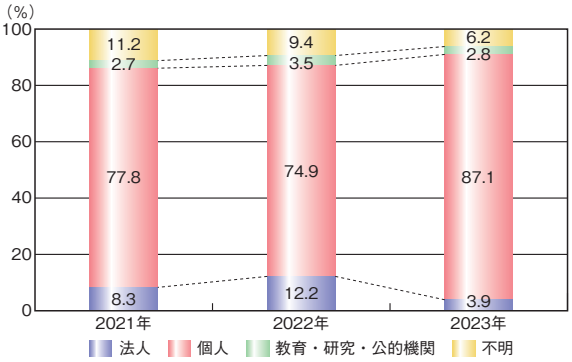
相談者の主体別では、2023 年も個人からの相談が 9,514 件（87.1%）と最も多かった。

主体別相談比率の推移では、法人からの相談比率は 2022 年と比較して 8.3% 減少した一方、個人からの相談比率は 12.2% 増加した（表 D-1、図 D-2）。

法人については、2022 年に多かった「Emotet 関連」の相談の減少が、要因の一つと考えられる。また個人については、「ウイルス警告の偽警告」についての相談の増加が要因の一つと考えられる（「D.4 手口別相談件数」参照）。

相談者の主体	2021 年	2022 年	2023 年
法人	530	1,145	427
個人	4,984	7,043	9,514
教育・研究・公的機関	170	330	308
不明	719	883	674
合計（件）	6,403	9,401	10,923

■表 D-1　情報セキュリティ安心相談窓口の主体別相談件数（2021～2023 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（2021～2023 年）

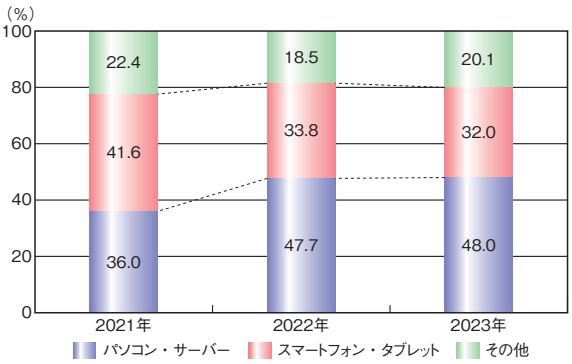
D.3　相談者の機器種別相談件数

相談機器種別では、2023 年は「パソコン・サーバー」に関する相談が 5,240 件（48.0%）と最も多かった。

相談者の機器種別相談比率は、2022 年と比較して同じ水準で推移しており、大きな変化はなかった（表 D-2、図 D-3）。

相談機器種別の主体	2021 年	2022 年	2023 年
パソコン・サーバー	2,304	4,487	5,240
スマートフォン・タブレット	2,666	3,173	3,492
その他	1,433	1,741	2,191
合計（件）	6,403	9,401	10,923

■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（2021～2023 年）

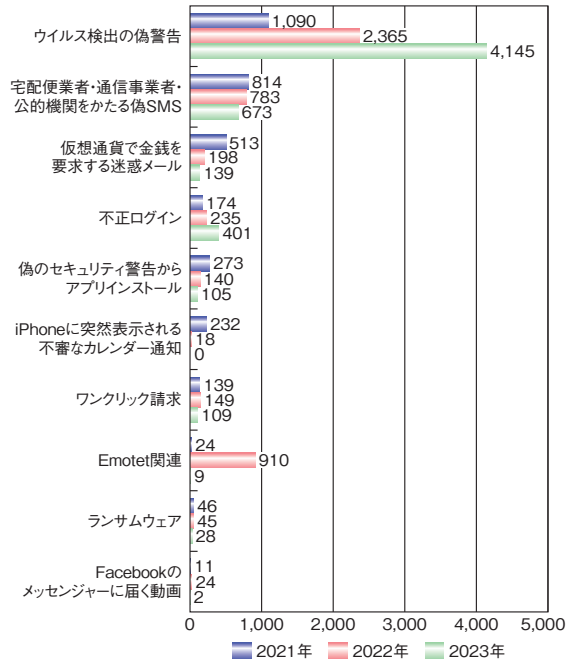


■図 D-3　情報セキュリティ安心相談窓口の機器種別相談件数の比率推移（2021～2023 年）

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。2023 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4,145件(37.9%)であった。次いで、「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 673 件 (6.2%)、「不正ログイン」に関する相談が 401 件(3.7%)であった。上位三つの手口による相談件数の合計は 5,219 件で、全相談件数(10,923 件)の 47.8% 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（2021～2023 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

第19回 IPA「ひろげよう情報セキュリティコンクール」2023 受賞作品

ひろげよう情報セキュリティコンクールは、情報セキュリティをテーマとした作品制作を通じて、全国における児童・生徒等の情報セキュリティに関する意識醸成と興味喚起を図ることを目的として開催しています。ここでは、全53,312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。

最優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

それでいい？
使いまわしの
パスワード

大阪府 大阪市立大淀小学校 5年 **今岡 陽菜歌**さん

〈ポスター部門〉

扱いに注意！君の味方は敵にもなる

神奈川県 神奈川県立神奈川工業高等学校 3年 **村石 琉音**さん

〈4コマ漫画部門〉

フィッシング

兵庫県 西宮市立鳴尾中学校 3年
奥埜 和花さん

優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

信じるの　知らない人の　その言葉

大阪府　堺市立南八下小学校　4年
市ノ瀬 瑚珀さん

セキュリティ　「面倒くさい」が　命とり

大阪府　大阪教育大学附属平野中学校　1年
稲垣 敢太さん

詐欺メール「緊急」「至急」疑おう

大阪府　東大谷高等学校　1年
小倉 結子さん

〈ポスター部門〉

フィッシングに注意！

兵庫県 雲雀丘学園小学校 6年
オストハイダ 真紋さん

“Fake” Wi-Fi

愛媛県 松山市立勝山中学校 3年
渡辺 梨緒さん

兵庫県 兵庫県立姫路工業高等学校 2年
川上 心優さん

〈4コマ漫画部門〉

なぞかけ

岡山県 岡山市立御津南小学校 5年
北山 穂風さん

「まぁ、いっか。」の結末は…。

広島県 呉市立東畑中学校 3年
長尾 妃芽さん

こわ〜い話

広島県 広島県立呉商業高等学校 3年
井上 心彩さん

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://www.ipa.go.jp/security/sec-tools/benchmark.html

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）
- 情報セキュリティリスクの指標と企業規模、業種が自組織と近い他組織について診断項目別に比較
- 結果に応じた推奨される取り組み

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	脆弱性に関する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 の 12 種類の 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

■動作環境・必須ソフトウェア
Windows 10、11

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	国内外で公開されたソフトウェア製品の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のバージョンが最新かどうかの確認
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をまとめて確認できる

概要

■判定対象ソフトウェア製品

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

■動作環境・必須ソフトウェア

Windows 10、11

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	国内で広く利用され、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
- Apache Struts
- Apache Tomcat
- BIND
- Joomla!
- OpenSSL
- WordPress
- 重要なセキュリティ情報

■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、Web ページから IPA が発信する「重要なセキュリティ情報」を配信

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
- 広く使われる製品のサポート終了情報
- サイバー攻撃への注意喚起

■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ソース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する

5 分でできる！情報セキュリティ自社診断
https://www.ipa.go.jp/security/guide/sme/5minutes.html

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、診断結果に即した対策が確認できる

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。
25 の質問に答えるだけで診断することができ、解説編を参照することで、診断編にある設問の内容を自社で対応していない場合に生じる情報セキュリティへのリスクと、今後どのような対策を設ける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！」
https://www.ipa.go.jp/security/kokokara/

学習 診断 対策

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
• 教育学習は対象者を細分化し、それぞれに適した教育学習コンテンツを紹介

サイバーセキュリティ経営可視化ツール
https://www.ipa.go.jp/security/economics/checktool.html

診断

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	原則として、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 Ver3.0 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
https://www.ipa.go.jp/security/sec-tools/5mins_point.html

学習

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。

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

「サイバー攻撃」「内部不正」「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」「新入社員向け」「保護者／小学生／中高生向け」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～
- 今そこにある脅威～内部不正による情報流出のリスク～
- What' s BEC ？～ビジネスメール詐欺 手口と対策～
- 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

J

L

M

N

O

P

R

S

T

U

V

W

あ

か

さ

た

な

は

ま

ら

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　井上 佳春
小川 隆一

執筆者　IPA
浅見 侑太　板垣 寛二　伊藤 彰朗　伊東 麻子　伊藤 吉史
井上 佳春　内海 百葉　大久保 直人　大友 更紗　小川 賢一
小川 隆一　小幡 宗宏　甲斐 成樹　金山 栄一　金子 成徳
神谷 健司　唐亀 侑久　河合 真吾　神田 雅透　黒岩 俊二
小杉 聡志　小山 明美　小山 祐平　佐川 陽一　佐藤 栄城
篠塚 耕一　白石 歩　白鳥 悦正　新保 淳　銭谷 謙吾
高塚 光幸　竹内 智子　武智 洋　田島 威史　田島 凛
丹野 菜美　近澤 武　辻 宏郷　長迫 智子　中島 健児
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
藤井 明宏　古居 敬大　松島 伸彰　宮本 冬美　森 淳子
安田 進　山下 恵一　吉野 和博　吉原 正人　吉本 賢樹
渡邉 祥樹

株式会社日立製作所　相羽 律子
三菱電機株式会社　神余 浩夫
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
株式会社 KDDI 総合研究所　三宅 優
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
和泉 隆平　板橋 博之　伊藤 真一　江島 将和　大澤 淳
釜谷 誠　亀山 友彦　岸野 照明　北村 弘　栗原 史泰
桑名 利幸　古明地 正俊　塩田 英二　清水 碩人　瀬光 孝之
高見 穣　高柳 大輔　田口 聡　田村 智和　土屋 正
遠山 真　中島 尚樹　中野 美夏　西原 栄太郎　日向 英俊
松田 修平　真鍋 史明　宮崎 卓行

一般社団法人 JPCERT コーディネーションセンター　石寺 桂子
Trend Micro Incorporated　木村 仁美
長崎県立大学　島 成佳
国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所
経済産業省 商務情報政策局 サイバーセキュリティ課

おわりに

ロシア・ ウクライナ戦争の収束の兆しが見えないところに、イスラエル・ ハマス間の武力衝突が勃発した2023年。 戦場での戦闘とサイバー戦に加え、生成AIの進化や台頭によって精巧に加工された虚偽情報を用いた情報戦が繰り広げられているといいます。 一方、私達の身の回りにも本物の画像を細工したフェイクニュースや詐欺目的と思われる虚偽情報がSNS等で数多く飛び交っています。 本白書では新たに設けた「第4章　注目のトピック」に、前年に引き続き、虚偽情報拡散に関する節を設け、多くの事例について解説しています。 これに加え、AIのセキュリティについても第4章に節を設けました。IPAには2024年2月、AIを安全に利用し、 利便性を享受できるよう、AIの安全性に関する評価手法や基準の検討等を行うAIセーフティ・インスティテュート（AISI）が設置されました。今後、本白書においてもAIに関する記述は欠かせないものになりそうです。

編集子

情報セキュリティ白書 2024

変革の波にひそむ脅威：リスクを見直し対策を

2024 年 7 月 30 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**