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2章
情報セキュリティを支える基盤の動向

2023年5月に新型コロナウイルス感染症が5類感染症に分類され、国際間でも対面での人材育成や国際会議等が再開された。重要インフラや産業システムのセキュリティ対策について、世界各国は喫緊の課題として法制、制度、人材育成の取り組みを進めている。米国では2023年12月に「SBOM管理のための推奨事項」が、2024年2月に大幅に改訂されたサイバーセキュリティフレームワーク2.0版が公開された。国内では、深刻化するDDoS攻撃への対処として、脆弱なIoT機器の調査継続が決定した。また、IoT機器の信頼性を開発段階から検証するため「情報セキュリティサービス基準」に「機器検証サービス」が追加された。本章では、情報セキュリティに関する国内外の政策、国際標準化の動向、人材育成の取り組みについて解説する。

2.1 国内の情報セキュリティ政策の状況

本節では、政府が推進する情報セキュリティ政策の状況について述べる。

2.1.1 政府全体の政策動向

政府全体のサイバーセキュリティ政策は、3年ごとに改定される「サイバーセキュリティ戦略※1」に基づき、各年度の年次計画が逐次文書化される。本項では、2023年度に発行された年次計画「サイバーセキュリティ2023※2」（以下、年次計画）に基づく主な取り組みと、経済安全保障関連施策の状況について述べる。

(1) 年次計画が注力する政策課題

「サイバーセキュリティ戦略」では、サイバーセキュリティ政策の方向性について、「①デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進」「②公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」「③安全保障の観点からの取組強化」の3点が示されている。年次計画では、更に国家の支援を受けた組織等によるサイバー攻撃の深刻化・巧妙化が指摘され、安全保障分野で欧米に比肩しうる対応能力の向上、実効的な対策強化のための政策課題として、①各主体による対策の強化・対処能力の向上、②政府による支援等の充実・強化、③国際連携・協力の強化が挙げられている。また、2022年度に引き続き、注力項目として「経済社会の活力の向上及び持続的発展」「国民が安全で安心して暮らせるデジタル社会の実現」「国際社会の平和・安定及び我が国の安全保障への寄与」等に関わる施策を推進するとしている。以下では、この記載に基づき、2023年度に行った取り組みを概観する。

(2) 経済社会の活力の向上及び持続的発展

年次計画では、サイバー攻撃被害のリスクが高まる状況においても、サイバーセキュリティ対策への経営者の関与が高まらず、経営層とIT部門やDX推進部門との認識ギャップが存在するとし、経営層にサイバーセキュリティに関する意識改革のための「気づき」を与えることが重要であるとしている。経営層の意識改革については、経済産業省とIPAが2023年3月に改訂した「サイバーセキュリティ経営ガイドライン Ver 3.0※3」の活用を促進するとし、これに基づきIPAは2023年10月、「サイバーセキュリティ経営ガイドライン Ver 3.0実践のためのプラクティス集 第4版※4」を発行した。なお、2023月7月には、「サイバーセキュリティ経営ガイドライン Ver 3.0」の「付録A-2」に対応したサイバーセキュリティ経営可視化ツールについても業界平均値比較機能の追加を行った（「2.1.3 (1) (b) WG2（経営・人材・国際）」「3.1.1 (2) (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」参照）。

また年次計画では、2022年度に引き続き「サイバーセキュリティ対策情報開示の手引き※5」を踏まえた民間の取り組みを支援し、官民の障害対応体制を強化するため、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」を改定するとした。これに基づき内閣

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2023年7月、同指針を改定し、「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※6」として公開した。

更に年次計画は、特に中小企業の対策の充実が求められるとしている。これについては2022年度に引き続き、経済産業省における「サイバーセキュリティお助け隊サービス※7」の拡充やサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3：Supply-Chain Cybersecurity Consortium）※8との連携が「特に強力に取り組む施策」に選出されている。また総務省・経済産業省において、引き続き、地域SECUNITY※9におけるセミナーやインシデント演習等のコミュニティの自発的な運営に向けた取り組みを支援するとしている（「3.1.1（2）（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」「3.1.1（2）（b）サイバーセキュリティお助け隊サービス制度」参照）。

サプライチェーンセキュリティについては、業界ごとのプラクティスの横展開や産学官の結節点となる基盤の整備、サイバーとフィジカル双方に対応したフレームワーク作成等の取り組みが重要であるとしている。特に2023年度は、オープンソースソフトウェア（OSS：Open Source Software）の利用に伴うソフトウェアサプライチェーンリスクへの懸念から、脆弱性管理で重要なSoftware Bill of Materials（SBOM）※10に関わる活動が含められた。経済産業省は、SBOMの活用促進に関するドキュメント整備と普及啓発に取り組んでおり、その一貫として2023年7月、「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」を策定した※11（「2.1.3（1）（a）（イ）分野横断SWG」参照）。また総務省は、代表的な通信システムのSBOMを作成・評価する等、通信分野のSBOM導入に向けた実証事業を実施した※12。

このほか年次計画では、2022年度に引き続き、経済産業省の情報セキュリティサービス審査登録制度※13に「機器検証サービス」を追加し、信頼性のある検証事業者を確認する仕組みを構築するほか、開発段階のIoT機器の脆弱性検証による検証済製品ラベルの仕組みの構築に向けた検討を進めるとしている。また、2024年4月更新の「情報セキュリティサービス基準 第4版※14」に「ペネトレーションテスト（侵入試験）サービス」が追加された（「2.1.3（4）情報セキュリティサービス審査登録制度」参照）。

「サイバーセキュリティ戦略」が掲げる「誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着」の取り組みとして、年次計画は、総務省がWi-Fiの利用と提供に必要なセキュリティ対策のガイドライン類の改定を検討するとしている。総務省はこの一環として2024年3月、無線LAN（Wi-Fi）のセキュリティに関するガイドラインの改定を行った※15。

また年次計画は、子供達の安全なインターネット利用に関する周知啓発の取り組みとして、文部科学省と協力し、「e-ネットキャラバン※16」等の啓発講座の必要な内容更新、及び実施を行うとしている。更に情報モラル教育については2022年度に引き続き、教員等へのオンラインセミナーによる指導力向上を図るとしている。2023年度のe-ネットキャラバンは協力企業の支援のもとに、2,166件の講座が実施された※17。

(3) 国民が安全で安心して暮らせるデジタル社会の実現

年次計画では、本項目の取り組みを、以下の項目ごとにまとめている。

(a) 国民・社会を守るためのサイバーセキュリティ環境の提供

年次計画は、関係政府機関（主体）ごとに取り組みを整理している。まず警察庁は、サイバー警察局、サイバー特別捜査隊による国内外関係機関との連携による重大サイバー事案への対処を行うとしている。この一環として2023年12月、警察庁はランサムウェアLockBitによって暗号化されたデータの復号化ツールを欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）に提供※18、国際的攻撃者集団の摘発に貢献した（「2.1.5（2）（b）（ア）ランサムウェアに対する対処」参照）。

また総務省は、国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）が実施している脆弱なIoT機器の調査事業NOTICE（National Operation Towards IoT Clean Environment）※19の継続・拡充に関する法改正を行うとし、2023年12月に「国立研究開発法人情報通信研究機構法の一部を改正する等の法律の施行に伴う関係政令の整備及び経過措置に関する政令」が成立した※20。年次計画はまた、NICTが運営する「サイバーセキュリティネクサス（CYNEX：Cybersecurity Nexus）※21」による情報共有推進、更に2022年に策定された「5Gセキュリティガイドライン※22」

の普及推進等を行うとしている（その他の取り組みについては「2.1.4 総務省の政策」参照）。

また厚生労働省では、2023 年 5 月に策定された「医療情報システムの安全管理に関するガイドライン第 6.0 版※23」の普及啓発を行うとしている。なお、年次計画で求められた「水道分野における情報セキュリティガイドライン」の改訂は、2024 年 4 月に国土交通省に移管され、継続検討されている※24。

更に経済産業省は、2022 年度に引き続き、フィッシングサイトの閉鎖依頼等を実施するとともに、増加傾向にあるフィッシング詐欺の攻撃手法分析、対応力向上を図る。また、ソフトウェア製品開発者が配慮すべきセキュリティ上の事項の普及、脆弱性情報への対処に関わる情報提供、製品開発者の体制や、サプライチェーン等の脆弱性調整に影響する項目についての啓発等を実施するとしている。

（b）デジタル庁の施策に基づくサイバーセキュリティ確保

デジタル庁では、2022 年度に「誰一人取り残されない、人にやさしいデジタル化」実現のためのセキュリティ基盤構築施策として、政府情報システムにおけるセキュリティ・バイ・デザインやセキュリティリスク分析のガイドライン、ゼロトラストアーキテクチャ等に関する技術レポート等、九つのドキュメントを公開している。年次計画では、2023 年度に上記のドキュメントのデジタル庁システムへの活用、及び技術動向に応じた改訂を行うとした（「2.1.2 デジタル庁の政策」参照）。

また制度運用面では、「政府情報システムのためのセキュリティ評価制度（ISMAP）」について、審査業務の実施と業務効率化の改善検討、SaaS（Software as a Service）を対象とする ISMAP-LIU の普及施策に取り組むとした（「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）」参照）。

マイナポータルについては、利用者視点に立った UI・UX の改善等を継続するとしている。これらの一環として、2024 年 1 月以降、医療保険情報取得 API 等が公開され※25、2024 年 3 月 24 日にはマイナポータルのトップページが更新された※26。

（c）経済社会基盤を支える主体の取り組み

年次計画は、政府機関等、重要インフラ事業者、大学・教育研究機関の主体ごとに取り組みを整理している。

（ア）政府機関等の各主体の取り組み

年次計画ではまず、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「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」を 2023 年度に改定し、同改定を踏まえ、「政府機関等における情報システム運用継続計画ガイドライン」「SBD（Security By Design）マニュアル」等の統一基準適用個別マニュアルの改定について検討を行うとしている。この改定作業は NISC が担い、2023 年 7 月、全面的に改定された基準群を公開した※27。改定のポイントとして以下が挙げられ、各府省庁が実施することとなる。

- 米国国立標準技術研究所（NIST：National Institute of Standards and Technology）の対策を参考にしたサプライチェーン対策の強化
- ISMAP の活用や認証強化によるクラウドサービス利用における対策強化（ISMAP については「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）」参照）
- 重要ソフトウェアの設定確認や教育、脆弱性診断等、ソフトウェア利用における対策強化
- サイバー攻撃に対するレジリエンスや脅威・技術動向を踏まえての対策強化
- 組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保

また年次計画は、安全性・透明性の検証が可能なセンサーを政府端末に導入、収集したログ情報を前掲の CYNEX にて集約、NICT が蓄積するサイバーセキュリティ情報と横断的に解析し、結果を関係機関で共有する事業（CYXROSS※28）を開始するとしている。

（イ）重要インフラの各主体の取り組み

サイバーセキュリティ戦略本部が 2022 年に「重要インフラのサイバーセキュリティに係る行動計画※29」を策定した。年次計画では、2022 年度の上記行動計画の実施状況はおおむね順調であるとされ、2023 年度も引き続き行動計画に沿った以下の施策を行うとした。

- 障害対応体制の強化：重要インフラ事業者の組織統治の在り方を「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」において規定化する等の実施。
- 安全基準等の整備及び浸透：安全基準等の継続改善と自主的な取り組みの推進。この一環で、2023 年 7 月、NISC は改訂した「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」を公開した。

- 情報共有体制の強化：IPA、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）等との連携を含めた、官民を挙げた共有体制の継続強化。重要インフラ事業者の自律的な組織であるセプターカウンシルの活性化支援（「2.1.3 (5) J-CSIP（サイバー情報共有イニシアティブ」参照）。
- リスクマネジメントの活用：重要インフラ事業者等におけるリスクマネジメントの継続強化。この一環で、2023年7月、NISCは「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書※30」を発行した。
- 防護基盤の強化：2022年度に実施した「分野横断的演習」の継続拡充、及び重要インフラ内演習の促進。分野横断的演習は2023年12月に開催され、重要インフラ事業者以外の組織も参加した※31。

(ウ) 大学・教育研究機関等の主体の取り組み

文部科学省は2022年度、各大学（主体）等で規定したサイバーセキュリティ対策等基本計画の実践状況についてフォローアップを行った。また各主体のセキュリティ担当者の役割に応じた層別研修、情報システムの脆弱性診断等を実施した。

年次計画では2023年度、これらの調査・実践を基に、セキュリティ対策の共通課題の検討を進め、各主体の対策強化を促すとしている。また各主体の担当者向け研修は、実践に利用できる知識を習得できるよう充実を図り、情報システムに対する脆弱性診断やペネトレーションテストを引き続き実施するとしている。更に、2022年度に発足した国立情報学研究所（NII：National Institute of Informatics）ストラテジックサイバーレジリエンス研究開発センター※32の活動を中心に、国立大学間のサイバー攻撃情報共有・研修・脅威解析手法の開発を推進するとしている。

(d) 情報共有・連携と東京2020オリンピック・パラリンピック競技大会の知見活用

サイバーセキュリティ基本法に基づき、行政機関、重要インフラ事業者、サイバー関連事業者等が早期の段階でサイバーセキュリティ情報を迅速に共有する会議体として、2019年にサイバーセキュリティ協議会※33が設立された。年次計画では、サイバーセキュリティ協議会の2022年度活動について、迅速な対策情報の公開に至った案件が30件あった等により一定の評価を示した。また、東京2020オリンピック・パラリンピック競技大会におけるサイバー脅威・対策の知見・ノウハウを、G7広島サミット※34や大阪・関西万博等の国際イベントの対策に活用する民間企業のリスクマネジメントの取り組み等について、一定の評価が与えられた。年次計画では、2023年度もこれらの取り組みを継続し、国際イベントの万全な開催を確保するとしている。こうした準備の結果、2023年5月のG7広島サミット、及び4～5月の関係閣僚会合ではサイバー攻撃による大きな被害は発生しなかった。

(e) 大規模サイバー攻撃等の対処態勢の強化

年次計画では、2022年度は、内閣官房による重要インフラへの攻撃を想定した大規模サイバー攻撃事態等対処訓練、警察庁によるインシデント対応訓練や観測強化、個人情報保護委員会による情報漏えい事案の連携検討、金融庁によるインシデント対応連携等の事例を紹介し、一定の評価を与えた。2023年度も引き続き、大規模サイバー攻撃事態の演習、各主体の取り組みを継続するとしている。

この一環として、NISCは2023年12月、重要インフラサービスの継続が脅かされるケースを想定した分野横断的演習を実施した※35。また2024年2月、警視庁は重要インフラ事業者や半導体関連事業者と合同で、サイバー攻撃対応訓練を実施した※36。

(4) 国際社会の平和・安定及び我が国の安全保障への寄与

年次計画では、本項目の取り組みを、以下の項目ごとにまとめている。

(a)「自由・公正かつ安全なサイバー空間」の確保

政府は、サイバー空間における法の支配の推進について、首脳・閣僚級協議や東南アジア諸国連合（ASEAN: Association of Southeast Asian Nations）等との多国間協議、14ヵ国と継続的に実施している二国間サイバー協議、サイバーセキュリティに関する国連オープン・エンド作業部会等を通じ、関係各国との連携・議論の深化を進めている。年次計画では2023年度も、サイバー空間における国際法の適用、自由、公正かつ安全なサイバー空間の確保等の議論に寄与するとしている。また日本がG7議長国であることから、サイバー犯罪捜査に対する国際連携の強化に貢献するとしている。

こうした連携の一環として、NISC、経済産業省、総

務省は2023年10月、「第16回 日ASEANサイバーセキュリティ政策会議※37」を開催し、ASEAN諸国とのサイバーセキュリティ政策・重要インフラ防護に関する事例共有・能力構築・演習等に関する連携の在り方を協議した(「2.2.1(2)(b)日本ASEAN友好協力50周年の取り組み」参照)。

(b)我が国の防御力・抑止力・状況把握力の強化

国家の防御能力の確保・強靭化について、サイバーセキュリティの重要性が増す中、政府は2022年度、各自衛隊の防護システムやネットワークインフラの強化、防衛調達におけるセキュリティを担保する「防衛産業サイバーセキュリティ基準」の導入準備等を実施した。また2022年12月に閣議決定された「国家防衛戦略※38」等を踏まえ、敵対的勢力の「サイバー空間の利用を妨げる能力」等に対する抜本的な防衛力強化を図るため、ASEAN地域フォーラム(ARF:ASEAN Regional Forum)等の枠組みで国際連携を深めた。また、関係政府機関によるサイバー脅威情報の収集にも努め、北朝鮮が支援する攻撃者集団の攻撃について暗号資産関連事業者への注意喚起等を行った。

年次計画では、2023年度も引き続き、国家安全に対するサイバー攻撃防御・抑止・状況把握の取り組みを強化するとしている。この一環として、「防衛産業サイバーセキュリティ基準」の防衛調達契約への適用が2023年度から開始された※39。また2023年7月に開催された第30回ASEAN地域フォーラム(ARF)閣僚会合では、ウクライナ情勢、南シナ海に関する行動規範、北朝鮮の弾道ミサイル発射、ミャンマー情勢等に対するASEANと日本の協力強化が表明された※40。

(c)国際協力・連携

「2.1.1(4)(a)『自由・公正かつ安全なサイバー空間』の確保」で述べたとおり、政府は自由・公正かつ安全なサイバー空間の確保のために、二国間のサイバー協議、ASEAN諸国等との多国間政策会議や演習・能力構築イベントに加え、ネットワーク監視に関する国際会議※41参加等の連携の取り組みを実施している。年次計画では、これらの取り組みが成果を挙げ、同盟国・同志国との信頼構築に貢献したとし、インド太平洋地域への連携拡大が必要としている。また、2023年度はこれらの取り組みを継続し、米国・英国・オーストラリア等の主要同盟国・同志国との連携に加え、友好協力50周年を迎えるASEANとの協力強化や能力構築の更なる推進、大洋州島しょ諸国への支援拡大等に取り組むとしている。これに基づき2023年度に実施されたイベントについては、「2.2.1 国際社会と連携した取り組み」を参照されたい。

(5)横断的施策

年次計画は、「横断的施策」を「研究開発の推進」「人材の確保、育成、活躍促進」「全員参加による協働、普及啓発」の三つに整理している。以下では、「研究開発の推進」について取り上げる。

「研究開発の推進」では、「国際競争力の強化と産学官エコシステムの構築」「実践的な研究開発の推進」「中長期的な技術トレンドを視野に入れた対応」の3点について取り組みが進められている。

国際競争力の強化において、2023年度の特徴と思われるのは、内閣府の「経済安全保障重要技術育成プログラム(K Program)※42」の推進である。同プログラムは2022年度より内閣府、文部科学省、経済産業省により、府省横断的に経済安全保障上重要な先端技術の研究開発を推進する事業として開始され、第一次の研究開発ビジョンでは海洋、宇宙・航空、領域横断・サイバー空間、バイオの4領域が明示された※43。また2022年度に第1次、2023年度に第2次の研究開発構想が示され、サイバーセキュリティ関係では以下の5件が公開されている。

- 「サプライチェーンセキュリティに関する不正機能検証技術の確立(ファームウェア・ソフトウェア)※44」
- 「人工知能(AI)が浸透するデータ駆動型の経済社会に必要なAIセキュリティ技術の確立※45」
- 「先進的サイバー防御機能・分析能力強化※46」
- 「偽情報分析に係る技術の開発※47」
- 「セキュアなデータ流通を支える暗号関連技術(高機能暗号)※48」

これらの研究開発構想にAIによる防御、AIによる脅威、が含まれているのが注目される。このうちサプライチェーンセキュリティに関する構想は2023年7月、AIセキュリティに関する構想は同年11月に国立研究開発法人科学技術振興機構(JST:Japan Science and Technology Agency)が公募を行い、研究が開始されることとなった。

また経済安全保障関連の中長期の研究開発において、セキュリティ分野では量子暗号が含まれる。これについて年次計画は、内閣府、文部科学省による「戦略的

イノベーション創造プログラム（SIP）第3期」課題※49の推進、及びデジタル庁、経済産業省、総務省による政府調達暗号評価プロジェクトCRYPTREC※50における現行暗号への影響分析を行うとしている（CRYPTRECについては「3.3.1 CRYPTRECの動向」参照）。

(6) 経済安全保障関連施策の状況

2022年5月、経済活動に関して国家及び国民の安全を損なう行為を防ぐための経済安全保障推進法が成立した※51。本項では、同法に基づく施策の整備状況を述べる。

(a) 経済安全保障推進法の整備状況

経済安全保障推進法では、以下の4項目について制度を創設するとし、公布から6ヵ月～2年以内の段階的施行が規定されている。

①重要物資の安定的供給
②基幹インフラ役務の安定的提供
③先端的な重要技術の開発支援
④特許出願の非公開

上記項目のうち①と③は2022年9月に基本指針が決定され、③については「2.1.1 (5) 横断的施策」で述べたK Program実践等の運用が始まっている。また②と④については2023年4月に基本指針が決定され、④については同年8月、特許出願非公開の対象となる技術分野及び付加要件が、また12月には非公開に関する適正管理措置のガイドラインが公開された※52。

なお国土交通省は2024年1月、経済安全保障推進法に基づく事前審査の対象となる「基幹インフラ」に港湾運送事業を追加する方針を示した※53。同時に、港湾分野の安全ガイドラインの整備を行い、これらに基づき、「重要インフラのサイバーセキュリティに係る行動計画」は2024年3月に改定され、港湾分野が15番目の重要インフラとして明記された※54。

(b) セキュリティ・クリアランス制度の整備状況

「セキュリティ・クリアランス制度」は、安全保障上重要な情報にアクセスが必要な者の信頼性を政府が確認する制度である。経済安全保障分野における同制度の検討は、経済安全保障推進法の成立を機に、2023年2月から内閣官房の有識者会議にて進められた※55。経済安全保障分野では、政府が指定する「重要経済安保情報」の詳細、民間事業者が保有する情報へのアクセス、調査におけるプライバシーや労働法制との調整等が懸案事項となる。有識者会議の検討結果は2024年1月に取りまとめられ、同制度創設に関する「重要経済安保情報の保護及び活用に関する法律案※56」が第213回国会に提出された。同法案は衆議院内閣委員会にて、政府による「重要経済安保情報」の指定や解除、及びクリアランス調査の運用状況を国会に報告する等の修正が行われた後、2024年4月9日、衆議院本会議にて可決された※57。

(7) AI戦略に基づく取り組みの状況

2019年6月、内閣府の統合イノベーション戦略推進会議は「AI戦略2019※58」を決定した。AI戦略2019は「人間尊重」「多様性」「持続可能」の三つの理念を掲げ、これらの理念を実装する四つの戦略目標（人材、産業競争力、技術体系、国際）を設定した。そして、戦略目標達成に向け、「未来への基盤作り」「産業・社会の基盤作り」「倫理」に関する取り組みが行われた。2021年6月、「AI戦略2019『フォローアップ』」として、各取り組みはおおむね計画どおり進捗しているが、社会実装につながる実感が出ていないとして、「AI戦略2021」が決定された※59。更に、2022年4月、「AI戦略2022※60」では五つ目の戦略目標として「差し迫った危機への対処」を設定し、パンデミックや大規模災害等に対する取り組みが具体化された。

2023年5月、「AI戦略会議（イノベーション政策強化推進のための有識者会議）」は、生成AIの普及や各国の取り組み状況等の急激な変化や広島AIプロセスを踏まえて「AIに関する暫定的な論点整理※61」を公表した。同会議は2023年～2024年度に8回にわたり、広島AIプロセスの進め方、AI事業者ガイドライン等の行動規範の履行確保及びAI利用の促進の検討等の議論を重ねた※62（広島AIプロセスについては「2.2.1 (2) (a) G7広島サミットとAI関連の国際連携」、AI事業者ガイドラインについては「2.1.3 (2) (a) AI事業者ガイドライン検討会」、AIセキュリティについては「4.2 AIのセキュリティ」参照）。

また、AIの安全性に対する国際的な意識の高まりを踏まえ、AIの安全性の評価手法の検討等を行う機関として、米国や英国等に続き、日本も「AIセーフティ・インスティテュート」を2024年2月に設立した。同機関は、関係10省庁（内閣府（科学技術・イノベーション推進事務局）、国家安全保障局、NISC、警察庁、デジタル庁、総務省、外務省、文部科学省、経済産業省、防衛省）、

関係4機関（NICT、国立研究開発法人理化学研究所、NII、独立行政法人産業技術総合研究所）の協力のもと、IPAに設置され、諸外国の機関とも連携して、AIの安全性評価に関する基準や手法の検討等を進めていく[※63]。

2.1.2 デジタル庁の政策

デジタル庁では、デジタル庁及び各府省庁におけるサービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理についての手続き・手順や、各種技術標準等に関する共通ルールや参考ドキュメントである「デジタル社会推進標準ガイドライン」群をまとめている。そのうちセキュリティに関するドキュメントとしては、九つのドキュメント（ガイドライン、適用方針、エンタープライズアーキテクチャ、技術レポート）を公開している[※64]。

（1）「デジタル社会推進標準ガイドライン」群におけるセキュリティに関するドキュメントの改訂

デジタル庁では、「デジタル社会推進標準ガイドライン」群のセキュリティに関するドキュメントを2022年及び2023年に公開してきた。ドキュメント公開後に寄せられた関係者や有識者の意見等の反映や2023年7月にサイバーセキュリティ戦略本部で決定された「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）[※65]」に関連する修正等を行い、以下の三つのドキュメントの改訂を行った。

（a）「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」の改訂

情報システムに対して効率的にセキュリティを確保するためには、情報システムの企画から運用まで一貫したセキュリティ対策（セキュリティ・バイ・デザイン）を実施する必要がある。「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[※66]」では、システムライフサイクルにおけるセキュリティ対策を俯瞰的にとらえるため、各工程でのセキュリティ実施内容、要求事項、関係者の役割の定義が記載されている。2024年1月に実施された改訂の主なポイントは以下のとおりである。

- 各工程での実施内容や構成を見直して品質強化、実用的なセキュリティ対策のポイントを拡充し、使いやすさを向上
- リスク管理体制整備の重要性、具体的な体制整備に関連する内容の見直し
- システム利用者や開発者／運用者等の「人に起因するセキュリティ脅威、対策の必要性、対策の考え方」を追記
- 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）等が策定し、日本も共同署名した「Secure by Design[※67]」の改訂案におけるセキュア・バイ・デザイン、セキュア・バイ・デフォルト原則の内容を踏まえて更新
- 2023年9月に改訂された「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針[※68]」に基づき、クラウド・バイ・デフォルトを前提としたクラウドベースの記載を拡充

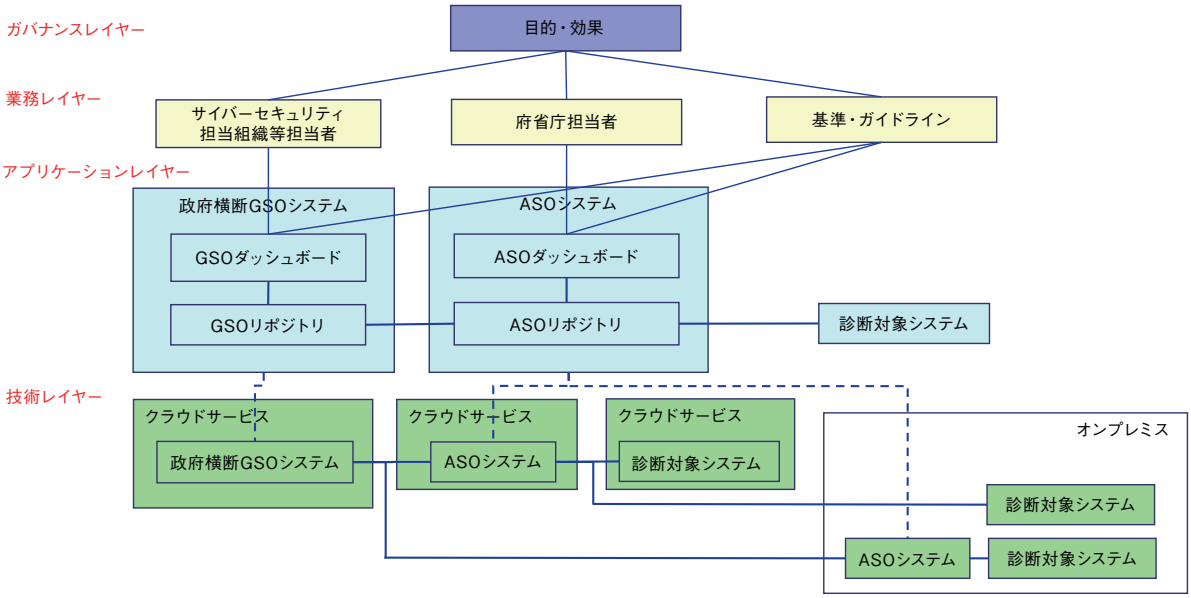
（b）「常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）」の改訂

ゼロトラストアーキテクチャの環境下において、安定かつ安全なサービス提供を実現するためには、政府全体のサイバーセキュリティリスクを早期に検知し、低減することが必要となる。「常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）[※69]」には、この活動を継続的に実施するための、情報収集・分析を目的としたプラットフォームのアーキテクチャが記載されている。2024年1月に実施された改訂の主なポイントは以下のとおりである。

- CRSA（Continuous Risk Scoring & Action：常時リスク診断・対処）の概要及び目的と効果について明示
- EA（Enterprise Architecture）に関する説明であることを明示して、タイトル、本文及びエンタープライズアーキテクチャ全体図を修正（修正された全体図については次ページ図2-1-1参照）
- 各政府機関の情報システムから統計情報を収集することについて言及
- 診断対象領域と診断対象について明示

（c）「政府情報システムにおける脆弱性診断導入ガイドライン」の改訂

政府情報システムにおいてサイバーレジリエンスを確保するためには、脆弱性診断を実施することが重要である。「政府情報システムにおける脆弱性診断導入ガイドライン[※70]」では、最適な脆弱性診断を選定、調達できるようにするための、脆弱性診断導入に関する基準とその指針について記載されている。2024年1月と2月に



■図 2-1-1　CRSA のエンタープライズアーキテクチャ全体図
（出典）デジタル庁「常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）」

実施された改訂の主なポイントは以下のとおりである。

- 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群（令和 5 年度版）の改定に伴い記載を変更
- Web API（Web Application Programming Interface）の診断に関する記載を追加
- 「OWASP Mobile Application Security Verification Standard（MASVS）※71」の改定に伴い記載を変更
- セキュリティベンダーの脆弱性検出能力を測る手段として、国内外の脆弱性届出制度や開発者等への報告及び調整実績を記載
- 脆弱性の深刻度評価における CVSS（Common Vulnerability Scoring System）のバージョン指定を廃止
- 各機関が保有するインベントリーの見直し方法に ASM（Attack Surface Management）を追加
- 定期診断を実施する際の留意点を追加
- 検出した脆弱性の深刻度評価に際し、CVSS の評価根拠の明記を求める旨を追加
- 診断を実施するセキュリティベンダーに求める要件及び選定手段として、経済産業省の「情報セキュリティサービス基準 第 3 版※72」（「2.1.3（4）情報セキュリティサービス審査登録制度」参照）を記載

（2）「デジタル社会推進標準ガイドライン」群におけるセキュリティ等に関するドキュメントの策定

「デジタル社会推進標準ガイドライン」群の中から、2023 年度に策定したセキュリティ等に関する二つのドキュメントについて紹介する。

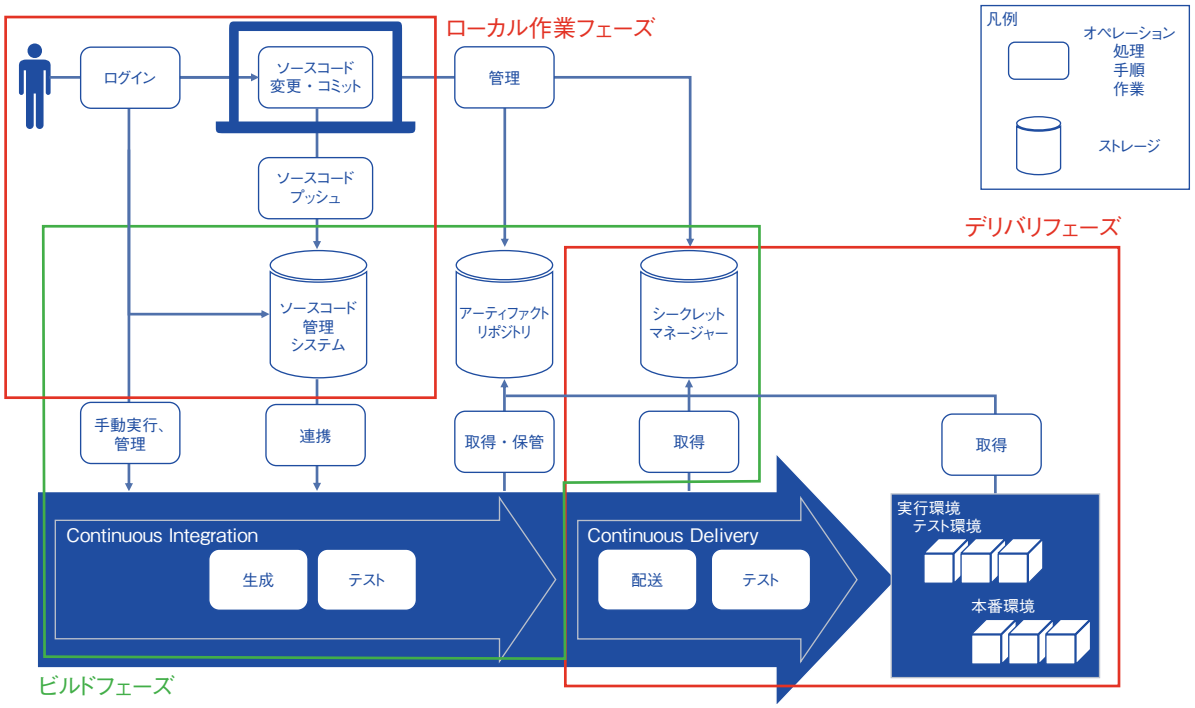
（a）「CI／CD パイプラインにおけるセキュリティの留意点に関する技術レポート」の策定

昨今のモダン技術を基に構築されたモダンアプリケーションにおいて、開発のサイクルを自動化する CI/CD パイプラインは、開発プロセスやセキュリティ対策を最適化させる上で欠かせない情報システム・コンポーネントである。攻撃者はコードを直接変更し、ビルドやデリバリまでを自動的に行ってしまうことに着目し、標的にし始めている。「CI ／ CD パイプラインにおけるセキュリティの留意点に関する技術レポート※73」では、CI/CD パイプラインをセキュリティの観点から解説し、保護策を検討する際のポイントについて説明している。

図 2-1-2（次ページ）に CI/CD パイプライン概要図を示す。

同技術レポートでは、CI/CD パイプラインについて、ローカル作業フェーズ、ビルドフェーズ、デリバリフェーズに分けて、セキュリティ対策を整理している。

- 全フェーズに共通した対策
  資産管理、脆弱性管理を含む運用・保守、環境への対策（シークレットの保護、アカウント管理・アクセス制御、ログの取得・管理、CI/CD パイプラインをとおした信頼性の確保）
- ローカル作業フェーズの保護
  利用者やエンドポイントにおける対策、ソースコード管



■図 2-1-2　CI/CD パイプライン概要図
（出典）デジタル庁「CI／CD パイプラインにおけるセキュリティの留意点に関する技術レポート」

理システム及びブランチの保護、ソースコード管理システムの公私共用なユーザーアカウントの管理、ソースコードと作業者の紐付き、ソースコード管理システムに対するシークレットの記録予防

- ビルドフェーズの保護
  ビルド上での実行範囲の制限、シークレット情報の漏えい予防、ソースコード・成果物の信頼性の担保、依存物の安全性の担保、ストレージ内の成果物の保護
- デリバリフェーズの保護
  デリバリ時に利用するシークレットの保護、信頼できる成果物をデリバリするための保護、デリバリ時の証跡

(b)「安全保障等の機微な情報等に係る政府情報システムの取扱い」の策定

「安全保障等の機微な情報等に係る政府情報システムの取扱い※74」では、安全保障等の機微な情報等を扱う情報システムについて、注意が必要とされるリスクとその対応策、クラウド化の検討、データ連携における留意点といった、利用者が検討すべき観点をまとめている。

同ドキュメントでは、「安全保障、公共の安全・秩序の維持といった機微な情報及び当該情報になり得る情報を扱う情報システムにおいては、情報システムの停止や情報漏えい等による社会的影響は計り知れないため、そうした情報を扱う者自らの説明責任が特に強く求められている。そのため、情報システムの利用に当たっては、機器構成や設置場所、運用体制等を利用者自らが把握できることや運用面のガバナンスを利かせられること等、利用者にとっての高度な自律性が重視される。」との基本的な考え方が示されている。

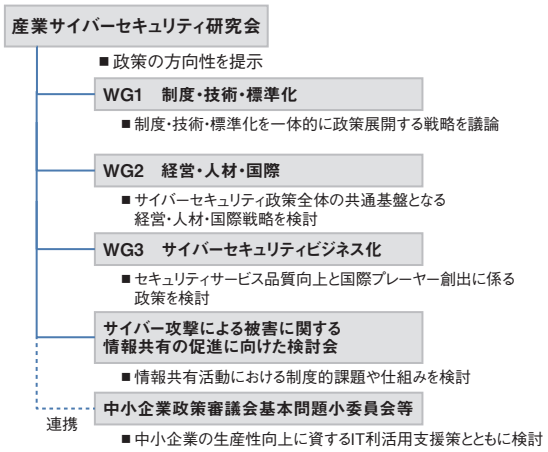
注意が必要なリスクとその対応策としては、構成要素を「データ、運用、ソフトウェア、ハードウェア、データセンタ・通信」に分類し、講じる対策の観点を整理している。また、クラウド化の検討、データ連携における留意点も記載されている。

2.1.3 経済産業省の政策

経済産業省は、サイバー空間とフィジカル空間を統合したサプライチェーン全体にわたるセキュリティ対策の強化に向け、制度、標準化、経営、人材、ビジネス等、様々な観点から施策を検討・実施している。

(1) 産業サイバーセキュリティ研究会

2017 年 12 月、経済産業省は我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進するため、産業界を代表する経営者、インターネット関連の学識経験者等から構成される「産業サイバーセキュリティ研究会」を設置した。図 2-1-3（次ページ）



■図 2-1-3　産業サイバーセキュリティ研究会及び WG の全体構成
（出典）経済産業省「産業分野におけるサイバーセキュリティ政策※75」を基に IPA が編集

に同研究会の構成を示す。

2019 年 4 月、同研究会のワーキンググループ 1（WG1）等での議論を踏まえ、経済産業省は Society 5.0 における産業社会でのセキュリティ対策のフレームワークとして「サイバー・フィジカル・セキュリティ対策フレームワーク※76」（以下、CPSF）を策定した。同研究会では、CPSF を軸として、各種ガイドラインや対策ツール等を整備している（図 2-1-4）。

同研究会では 2024 年 4 月 5 日に第 8 回会合を開催し、以下の四つの柱のもとで推進している産業界におけるサイバーセキュリティ対策強化に向けた取り組みの進捗状況、及び今後の産業サイバーセキュリティ政策について議論した。

①サプライチェーン全体での対策強化
②国際連携を意識した認証・評価制度等の立ち上げ
③政府全体でのサイバーセキュリティ対応体制の強化
④新たな攻撃を防ぎ、守るための研究開発の促進

以下では、本研究会で合意された四つの柱の取り組み方針に基づいた各ワーキンググループ（以下、WG）の 2023 年度の活動について述べる。

（a）WG1（制度・技術・標準化）

WG1 では、産業サイバーセキュリティに関する制度・技術・標準化を一体として政策に展開する戦略を議論している。CPSF に基づいて、産業分野別サブワーキンググループ（以下、SWG）と分野横断 SWG が設置され、各分野の特性に応じたセキュリティ対策の検討を行っている※78（次ページ図 2-1-5）。

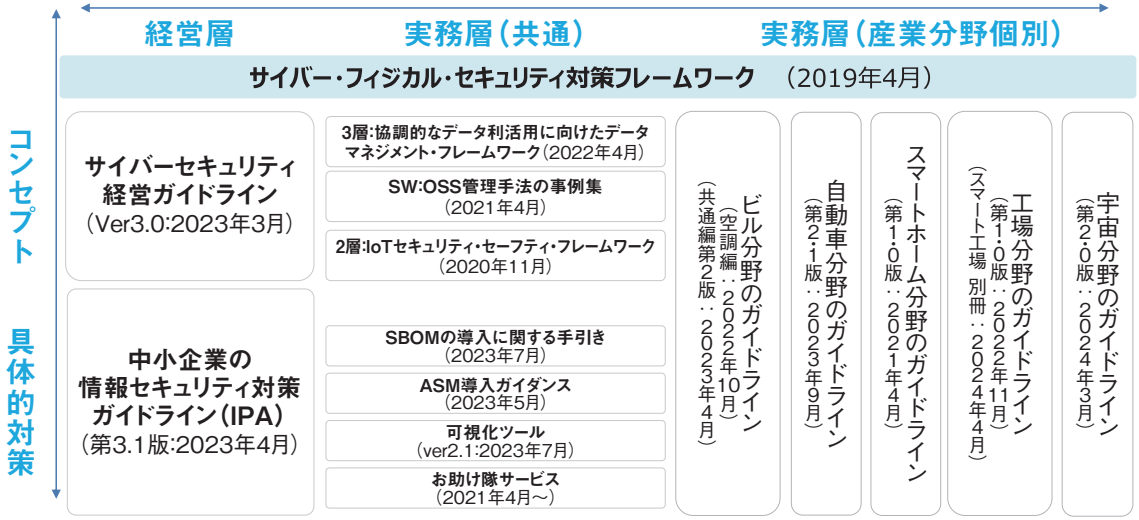
（ア）産業分野別 SWG

産業分野別 SWG として、ビル、電力、防衛産業、自動車産業、スマートホーム、宇宙産業、工場の七つの産業分野の SWG が活動している。

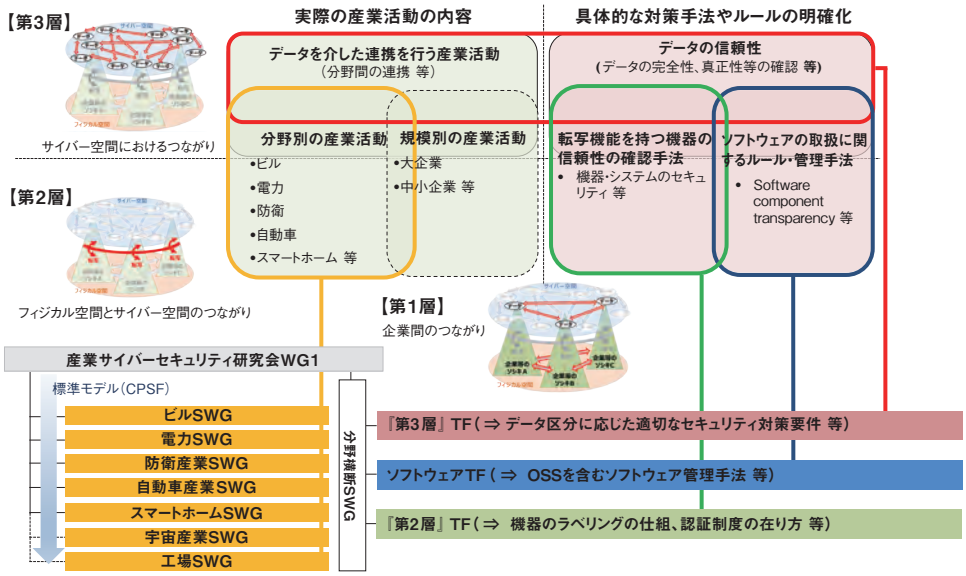
ビル SWG は、2023 年 11 月 30 日に第 16 回会合※80 を開催し、IPA を中心に設置が検討されているコンソーシアムにビル SWG が合流すること等について議論した。

電力 SWG は、2024 年 2 月 1 日に第 16 回会合※81 を開催し、電力制御システムにおけるサプライチェーン・リスク、電力システムにおけるサイバーセキュリティリスク点検ツール等について議論した。

防衛産業 SWG と連携する防衛装備庁情報セキュリティ官民検討会は、NIST SP800-171 に対応した防衛産業サイバーセキュリティ基準の適用を 2023 年度の契



■図 2-1-4　CPSF を基にした各種ガイドラインと対策ツール
（出典）経済産業省「第8回 産業サイバーセキュリティ研究会 事務局説明資料※77」



■図 2-1-5　タスクフォースの構成
（出典）経済産業省「サプワーキンググループ、タスクフォース等の検討状況※79」

約より始めた※39。

自動車産業 SWG と連携する一般社団法人日本自動車工業会総合政策委員会は、2023 年 9 月に「自工会／部工会・サイバーセキュリティガイドライン 2.1 版※82」を公開した。

宇宙産業 SWG は、2023 年 3 月に公開した「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver1.1※83」について、スコープの拡大、セキュリティ関連規程の雛形の追加、具体的な対策内容に関する改訂を行い、2024 年 4 月に「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver2.0※84」を公開した。

工場 SWG は、2022 年 11 月公表「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 Ver1.0※85」の別冊として、工場のスマート化に伴う対策のポイントをまとめた「別冊：スマート化を進める上でのポイント Ver1.0※86」を 2024 年 4 月に公開した。

（イ）分野横断 SWG

分野横断 SWG では、CPSF の実装を促進するべく、各層に焦点を絞った層別タスクフォースである「『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース（『第 2 層』TF）」、及び「『第 3 層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース（『第 3 層』TF）」が活動している。

また、OSS 等のソフトウェアの活用・脆弱性管理手法を検討する「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討 TF（ソフトウェア TF）」も活動している。ソフトウェア TF は、2023 年 7 月 28 日に「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引き Ver1.0※11」を公開した。同手引きは、主にソフトウェアサプライヤー向けに、SBOM を導入するメリットや実際に導入するにあたって認識・実施すべきポイントをまとめている。2024 年 2 月 28 日に第 12 回会合※87 を開催し、SBOM 取引モデル等を拡充した「ソフトウェア管理に向けた SBOM の導入に関する手引き Ver2.0（案）」、及び SBOM の普及展開策について議論した。

（b）WG2（経営・人材・国際）

WG2 では、サイバーセキュリティ政策全体の共通基盤となる経営者の参画と人材育成、中小企業の対策、国際連携に関する政策を議論している。

2024 年 3 月 25 日に第 10 回会合※88 を開催し、サプライチェーン対策として取り組むべき課題、及びセキュリティ人材の育成・活用について議論した。

「サイバーセキュリティ経営ガイドライン Ver3.0※89」の普及・定着に向けて、IPA を通じて 2023 年 7 月に自己診断結果と業種平均値の比較機能を追加した「サイバーセキュリティ経営可視化ツール Ver2.1※90」、及び 2023 年 10 月に「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 第 4 版」を公開した（「3.1.1 (2) (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」参照）。

サプライチェーン上の中小企業支援に関して、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）では、2023年11月に国際WGを新設し、国をまたがるサプライチェーンサイバーセキュリティの強化を推進するため、国外の機関や団体と連携して実施すべき取り組みについて検討・推進した（「3.1.1(2)(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」参照）。

地域SECUNITY形成促進WGでは、全国ワークショップ（2回）及び地域でのワークショップ（中部、九州、近畿）を実施した。地域関連事業では、IPAを通じて経営者のリーダーシップによるセキュリティ対策の推進（机上演習開催※91：11件）、担当者のスキルの底上げを通じた対策実装の推進（リスク分析ワークショップ開催※92-1：12件）、及び地域の中小企業支援組織と連携した効率的かつ効果的な普及啓発活動の推進（セミナー開催支援：31件、講師派遣：104件）等の活動を実施した※92-2。

サイバーセキュリティお助け隊サービス※93では、現行（1類）は価格上限があるため実態上、従業員10人前後の中小企業への提供がメインであることから、中規模以上の中小企業のニーズにも応えるサービスとなるよう、お助け隊サービスの新たな類型（2類）を創設した。価格要件を緩和しつつ、監視機能の強化や定期的なコンサルティング実施等の新たなセキュリティサービスの追加、IPAへの重大サイバー攻撃に関する情報の共有等を要件とした「サイバーセキュリティお助け隊サービス基準2.0版」を公開した※94（「3.1.1(2)(b)サイバーセキュリティお助け隊サービス制度」参照）。

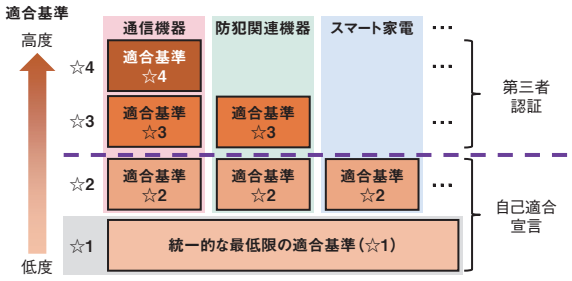
国際連携に関しては、日本のサイバー対処能力の強化や国際競争力強化の観点から、サイバー分野におけるルール作りを主導する欧米等の議論に参画し、国内制度との相互運用性の担保に向けて議論した。また、日本企業のサプライチェーン上重要なインド太平洋地域のサイバー対策の能力構築を推進し、幅広い有志国との協議等で国際連携を深めた（「2.2.1国際社会と連携した取り組み」参照）。

(c) WG3（サイバーセキュリティビジネス化）

WG3では、セキュリティサービス品質向上と国際的なプレイヤー創出に関わる政策を検討している。

IoT機器等のセキュリティ検証を行う検証事業者の信頼性可視化のため、情報セキュリティサービス審査登録制度に「機器検証サービス」を追加し、2023年度より検証事業者の登録及び「情報セキュリティサービス基準適合サービスリスト※95」への掲載を開始した。更に2024年4月、同制度に「ペネトレーション（侵入検査）サービス」を追加し、2024年9月ごろより登録申請の募集を開始する（「2.1.3(4)情報セキュリティサービス審査登録制度」参照）。

IoT製品の脆弱性を狙ったサイバー脅威が高まっていることを踏まえ、経済産業省では、2022年11月に「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」を設置し、2024年3月15日に最終取りまとめを公表した※96。「IoT製品に対するセキュリティ適合性評価制度」は、IoT製品共通の最低限の脅威に対応するための基準（☆1）及びIoT製品類型ごとの特徴に応じた基準（☆2、☆3及び☆4）を定め、求められるセキュリティ水準に応じた複数の適合性評価レベルを用いる方針である。☆1は、2024年度中に制度の開始を目指す（図2-1-6）。また、現行の「ITセキュリティ評価及び認証制度（JISEC）※97」と一体となった枠組みで運用する方針である。



■図2-1-6　適合性評価レベルのイメージ図
（出典）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 構築方針案※98」

WG3では、ニーズとシーズのマッチングの場として2018年からコラボレーション・プラットフォームを開催してきた。2023年度にはコロナ禍明けの新たなスタートとしてハイブリッド形式にて、以下の三つのテーマで実施された※99。

- 第25回「ポストPPAPのメールセキュリティ」（2023年9月22日）
  パスワード付きのZIPファイルとパスワードを別メールで送るという手法の危険性が顕在化している中、その対応策を各分野の識者により、講演とパネルディスカッション形式により広く議論を行った。
- 第26回「『サイバーセキュリティ経営ガイドライン』に基づく対策実施状況の可視化」（2023年12月22日）
  経営層がサイバーリスクを経営上の重要課題として把握して適切な投資判断を促すことを目的として、経済産業省が公開している「サイバーセキュリティ経営ガイドライン」について、ポイントの解説とIPAが公開して

いる可視化ツールに関するワークショップを開催した。

- 第 27 回「サイバー・フィジカル・セキュリティ：工場を守るセキュリティ対策とは」（2024 年 2 月 26 日）
  あらゆるものがインターネットにつながる IoT 時代を迎え、いかなる工場もサイバー攻撃を受ける可能性がある現在、サイバーとフィジカルという二つの面からどのような対策が有効か実例を交えながら、講演及びパネルディスカッション形式により議論を深めた。

（d）サイバー攻撃による被害に関する情報共有の促進に向けた検討会

同検討会では、「サイバー攻撃被害に係る情報の共有・公表ガイダンス※100」で主なスコープとしていた被害組織自身による情報共有ではなく、被害組織を直接支援する専門組織間での情報共有の促進を主なスコープとして、検討を実施している。

同検討会は、2023 年 11 月に「サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書」を、2024 年 3 月に「攻撃技術情報の取扱い・活用手引き」「秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文」を公開した※101。同報告書では、被害者の同意を個別に得ることなく速やかな情報共有が可能な情報の考え方を整理した。具体的には、通信先情報やマルウェア（ウイルス※102）情報、脆弱性関連情報等の「攻撃技術情報」から被害組織が推測可能な情報を非特定化加工した情報が対象となり得ると提言した。更に、どのような形で非特定化加工を行えばよいか等専門組織として取るべき具体的な方針について同手引きにて整理した。同モデル条文では、ユーザー組織と専門組織が共通の認識を持ち、専門組織が非特定化加工済みの攻撃技術情報を共有したことに基づく法的責任を原則として負わないことを合意するための条文を提示した。

サイバー攻撃が高度化する中、単独組織による攻撃の全容解明は困難となっている。攻撃の全容の把握や被害の拡大を防止する等の観点からサイバー攻撃に関する情報共有の更なる促進が求められる。

（2）その他の検討会の活動

他の検討会等における活動について述べる。

（a）AI 事業者ガイドライン検討会

2023 年 10 月、経済産業省は「人間中心の AI 社会原則※103」の実装に向けて、統一的で分かりやすい事業者向けガイドラインを検討するため「AI 事業者ガイドライン検討会」を設置した。

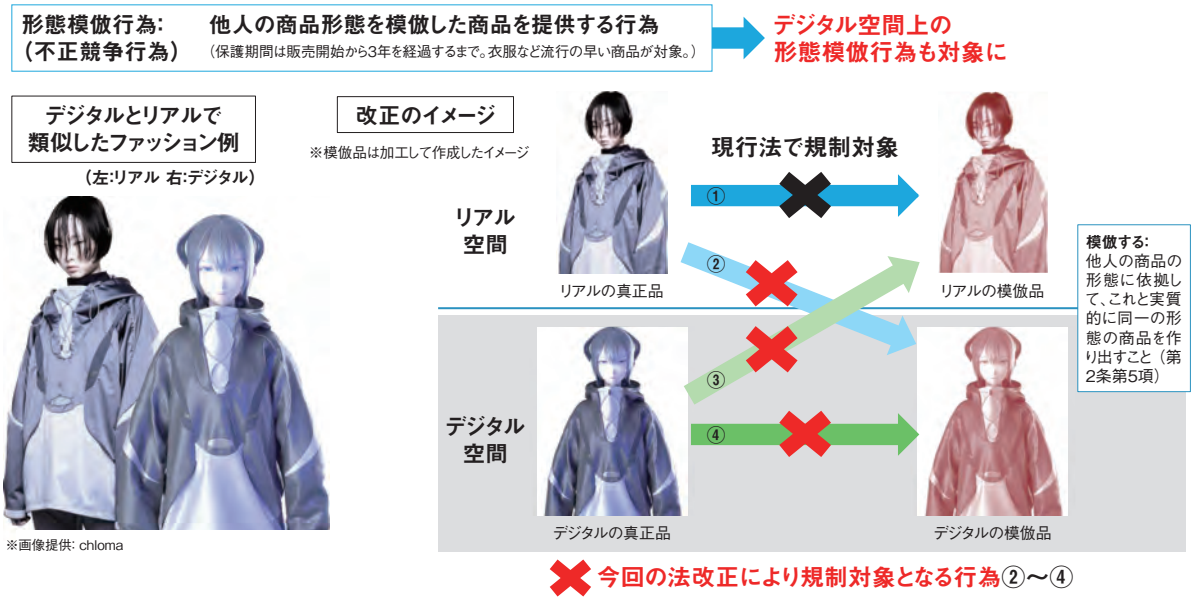
同検討会は、既存の三つのガイドライン（総務省の「国際的な議論のための AI 開発ガイドライン案※104」と「AI 利活用ガイドライン※105」、経済産業省の「AI 原則実践のためのガバナンス・ガイドライン Ver.1.1※106」）について、統合・見直しを行いつつ、国内外の動向を反映し、2024 年 4 月に「AI 事業者ガイドライン 第 1.0 版」を公開した※107。同ガイドラインは、AI に関するリスクをステークホルダー（「AI 開発者」「AI 提供者」「AI 利用者」）にとって受容可能な水準で管理しつつ、そこからもたらされる便益が最大化するよう、我が国における AI ガバナンスの統一的な指針を示している。

AI 技術の利用拡大に伴い、知的財産権の侵害や偽情報、誤情報の生成・発信等、社会的リスクが増大している。AI 活用（開発・提供・利用）に取り組むすべての事業者（政府・自治体等の公的機関を含む）が、同ガイドラインを参考の一つにしながら、具体的な取り組みを推進することが重要である（「4.2 AI のセキュリティ」参照）。

（b）不正競争防止法の改正

2023 年 6 月の通常国会で「不正競争防止法等の一部を改正する法律※108」が成立し、2024 年 4 月 1 日に施行された。不正競争防止法の改正では、デジタル化に伴う事業活動の多様化を踏まえたブランド・デザイン等の保護強化、及び国際的な事業展開に関する制度整備が行われた。主な改正内容について述べる。

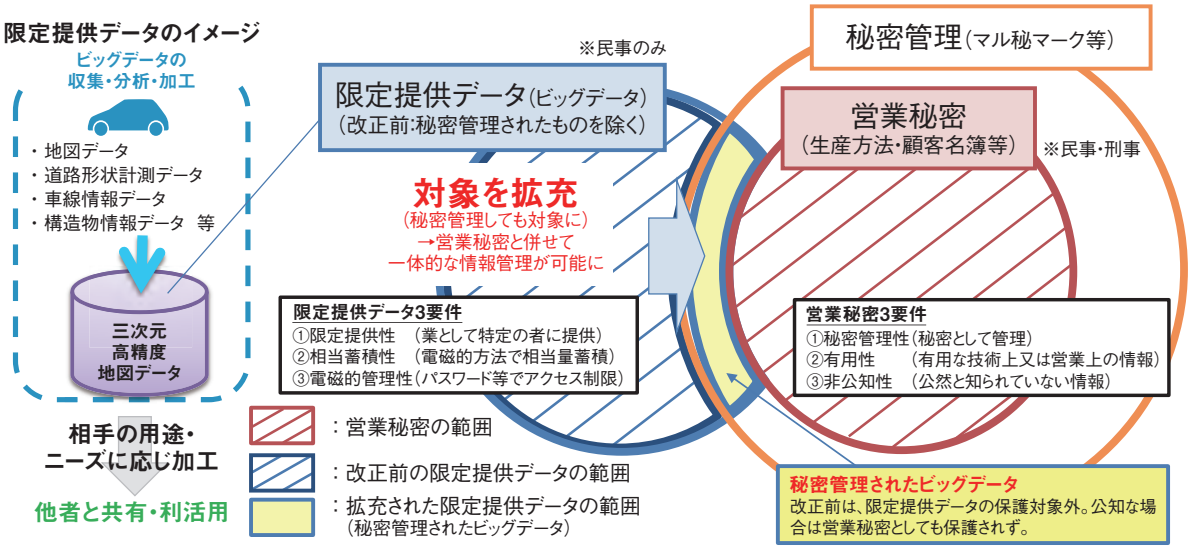
- デジタル空間における形態模倣品提供行為の防止
  改正前の不正競争防止法（以下、改正前不競法）では、形態模倣品提供行為について有体物の商品を想定していた。近年、デジタル空間上で精巧な衣服や小物等のデジタルの商品の経済取引が活発化していることから、デジタル空間上でのデジタル商品の形態模倣品提供行為（電気通信回線を通じて提供する行為）も規律の対象とし、デジタル空間上の商品の保護が強化された※109（次ページ図 2-1-7）。
- 限定提供データの定義の明確化
  改正前不競法のビッグデータ等を念頭にした「限定提供データ」を保護する制度では、「秘密管理されていないビッグデータ」を保護対象としていた。近年の企業実務では、自社で秘密管理しているビッグデータであっても他社に提供することがあることから、保護対象を「電磁的方法により管理されているビッグデータ」（営業秘密を除く）」に拡充した※110。これにより、営



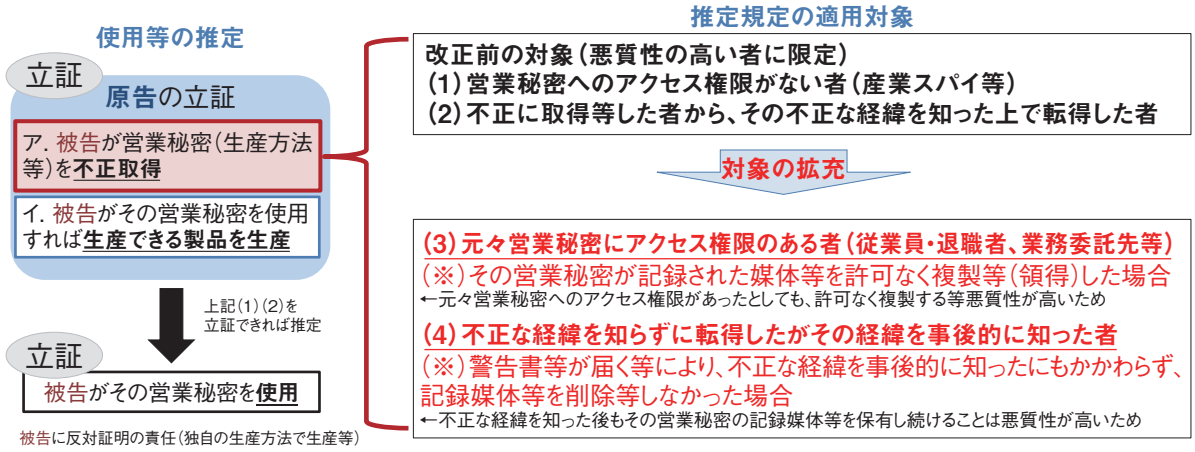
■図 2-1-7　デジタル空間における形態模倣行為の防止のイメージ
(出典)経済産業省・特許庁「令和 5 年不正競争防止法等改正説明会テキスト」を基に IPA が編集

業秘密でも限定提供データでも保護を受けることができない「隙間」が解消されるとともに、実務上は「限定提供データ」と「営業秘密」の一体的な情報管理が可能となった(図 2-1-8)。

- 使用等の推定規定の拡充
  改正前不競法では、被告が「技術上の秘密」を不正取得し、かつ、「その技術上の秘密」を使用すれば生産できる製品を生産している場合には、被告が「その技術上の秘密」を使用等したと推定する規定が設けられており、その適用対象は、産業スパイ等の悪質性の高い者に限定していた。オープンイノベーション・雇用の流動化を踏まえ、前記の推定規定の適用対象を、「元々営業秘密にアクセス権限のある者(従業員・退職者、業務委託先等)」や「不正な経緯を知らずに転得したがその経緯を事後的に知った者」についても、同様に悪質性が高いと認められる場合に限り拡大・拡充した(次ページ図 2-1-9)。これにより、「元々営業秘密にアクセス権限のある者」が許可なく複製すれば悪質性が高いとして適用できるようになり、営業秘密の保護が強化された。
- 外国公務員贈賄に対する罰則の強化・拡充
  「国際商取引における外国公務員に対する贈賄の防



■図 2-1-8　営業秘密・限定提供データの範囲のイメージ
(出典)経済産業省「不正競争防止法等の一部を改正する法律【知財一括法】の概要」を基に IPA が編集



■図 2-1-9　使用等の推定規定の拡充のイメージ
（出典）経済産業省「不正競争防止法等の一部を改正する法律【知財一括法】の概要」を基に IPA が編集

止に関する条約」をより高い水準で実施するため、外国公務員贈賄罪に対する法定刑を、国内の経済犯罪の中で最も重い水準に引き上げた。更に、日本企業の外国人従業者が当該日本企業の業務に関し、単独で国外において外国公務員等に対する贈賄行為に及んだ場合について、当該外国人従業者を処罰対象とし、当該日本企業も処罰し得ることを明確化した。

- 国際的な営業秘密侵害事案における手続きの明確化
これまで、日本国内で事業を行う企業の営業秘密が海外で侵害された場合の民事訴訟について、日本国内の裁判所で日本の法律に基づき起訴できるのか、事案によって不明確であった。このため、日本国内において事業を行う営業秘密保有者の営業秘密であって、日本国内において管理されているもの（当該営業秘密が専ら日本国外の事業の用に供されるものである場合を除く）に関する訴えについて、日本の裁判所において裁判を行うことができるという国際裁判管轄に関する規定（19 条の 2 第 1 項）及び、改正前不競法 2 条 1 項 4 号、5 号、7 号及び 8 号に掲げる不正競争を日本国外において行う場合についても日本の不競法を適用する、という適用範囲に関する規定（19 条の 3）を新設した。

(c) ASM 導入ガイダンス

経済産業省は、2023 年 5 月 29 日に「ASM 導入ガイダンス※111」を公開した。組織の外部（インターネット）からアクセス可能な IT 資産を把握・評価し、攻撃の初期段階でサイバー攻撃から守るための手法である ASM（Attack Surface Management）について、基本的な考え方や特徴、留意点等の基本情報とともに取り組み事例等をまとめている。クラウド利用の拡大やテレワークの拡大によってサイバー攻撃の起点が増加する中、自社のセキュリティ戦略に ASM を組み込むことで、IT 資産を適切に管理しリスクを洗い出すことが期待される。

(d) クレジット取引セキュリティ対策協議会

同協議会は、クレジットカード取引に関わる事業者が実施すべきセキュリティ対策を定めたガイドラインを改訂し、「クレジットカード・セキュリティガイドライン 5.0 版」を 2024 年 3 月 15 日に公開した※112。改訂内容には、2025 年 4 月以降、すべての EC 加盟店は、「セキュリティ・チェックリスト」記載の脆弱性対策等のセキュリティ対策を実施すること等が盛り込まれた。

(3) 技術情報管理認証制度

経済産業省は「産業競争力強化法等の一部を改正する法律」に基づき、2018 年 9 月から「技術情報管理認証制度」を開始している※113。これは、事業者の技術等の情報管理について、国が示す認証基準に適合していることを、事業所管大臣及び経済産業大臣が認定した認証機関が認証を付与する制度である。認証機関を目指す組織に対して、独立行政法人中小企業基盤整備機構や IPA が情報提供支援を実施し、2024 年 2 月現在 8 事業者が認証機関として認定を受けている。認証を取得しようとする企業・団体等に対しては、経済産業省が専門家を派遣して認証取得に向けた情報セキュリティ体制構築の無償支援を行う事業を行っており、2023 年度は 2023 年 5 月～ 2024 年 2 月の期間に実施した※114。これまで情報セキュリティ対策に取り組んだ経験がない事業者等に向けて、技術情報管理認証制度

の基準に基づく自己チェックリストが公開されている。引き続き機密性の高い技術情報等を保持する中小企業や業界団体等による同制度の活用が期待される。

(4) 情報セキュリティサービス審査登録制度

情報セキュリティサービスを安心して活用できる環境を醸成するべく、経済産業省は「情報セキュリティサービス基準」（以下、本サービス基準）及び「情報セキュリティサービスに関する審査登録機関基準」を策定し、2018年2月に公表した※115。2024年4月4日には、両基準に基づく情報セキュリティサービス審査登録制度の一層の普及を図るべく、本サービス基準の第4版※116を公開し、併せて、見直し要望の高い項目に対応した「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示」の第3版を公開した※117。

本サービス基準では、従来の分類に2023年4月より新たに「機器検証サービス」を加えた。更に2024年4月からは「脆弱性診断サービス」のオプションとして「ペネトレーションテスト（侵入試験）サービス」の基準を満たすサービスを提供可能である旨の表示を可能とするため、「脆弱性診断サービス」を「脆弱性診断サービス及びペネトレーションテスト（侵入試験）サービス」とした。これらの見直しにより、本サービス基準では、情報セキュリティサービスを以下の五つに分類している。

- 情報セキュリティ監査サービス
- 脆弱性診断サービス及びペネトレーションテスト（侵入試験）サービス
- デジタル・フォレンジックサービス
- セキュリティ監視・運用サービス
- 機器検証サービス

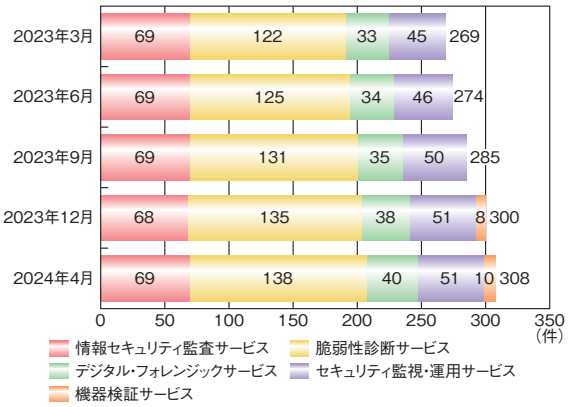
情報セキュリティサービス審査登録制度は、本サービス基準に照らして、情報セキュリティサービスについて一定の品質の維持・向上が図られているか否かを第三者が客観的に判断し、結果を公開することで、利用者が必要なセキュリティサービスを容易に選定できるようにする枠組みである。

IPAはこの枠組みに基づき、2018年7月から、審査登録機関※118による審査の結果、本サービス基準に適合すると認められ、当該機関の登録台帳に登録され、かつIPAに誓約書を提出した事業者の情報セキュリティサービスを「情報セキュリティサービス基準適合サービスリスト※95」（以下、本リスト）として公開している。

本リストは、NISCの「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）※119」において、以下のケースにおける外部委託先選定に活用できるように参照されている。

- 監査業務の外部委託先選定
- 脆弱性診断の外部委託先選定
- インシデントレスポンス業務の外部委託先選定
- セキュリティ監視業務の外部委託先選定

本リストのサービス登録数は堅調に推移しており、2024年4月に308件に達した（図2-1-10）。



■図2-1-10　情報セキュリティサービス登録数の推移

「政府情報システムのためのセキュリティ評価制度（ISMAP）」において、評価を実施する監査機関として登録申請する場合、本リストに「情報セキュリティ監査サービス」として登録されていることが要求事項の一つになっている（「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）」参照）。

本リストの活用がより一層進むことで、情報セキュリティサービスの品質向上に加え、情報セキュリティサービス市場の活性化にもつながることが期待される。

(5) J-CSIP（サイバー情報共有イニシアティブ）

経済産業省の協力のもと、IPAでは2011年10月から、官民連携による高度なサイバー攻撃対策を目的として、サイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan）を運用している。

J-CSIPは、日本の基幹産業を担う企業を中心に、サイバー攻撃等に関する情報を相互に共有し、サイバー攻撃の防御とその被害の低減を目指している。2024年3月末現在、IPAを情報の中継・集約点（情報ハブ）として15の業界から292の企業や業界団体（以下、参

加組織）が J-CSIP に参加している。

参加の形態としては、IPA と参加組織との間で個別に秘密保持契約（NDA：Non-Disclosure Agreement）を締結して情報共有を行う業界単位のグループ（SIG※120）と、規約を基に業界の情報共有活動を支援するための枠組みである「情報連携体制」が存在する（図 2-1-11）。

また、J-CSIP は IPA を通じて、経済産業省やセプターカウンシル※121 の C⁴TAP、JPCERT/CC 等とも連携している。

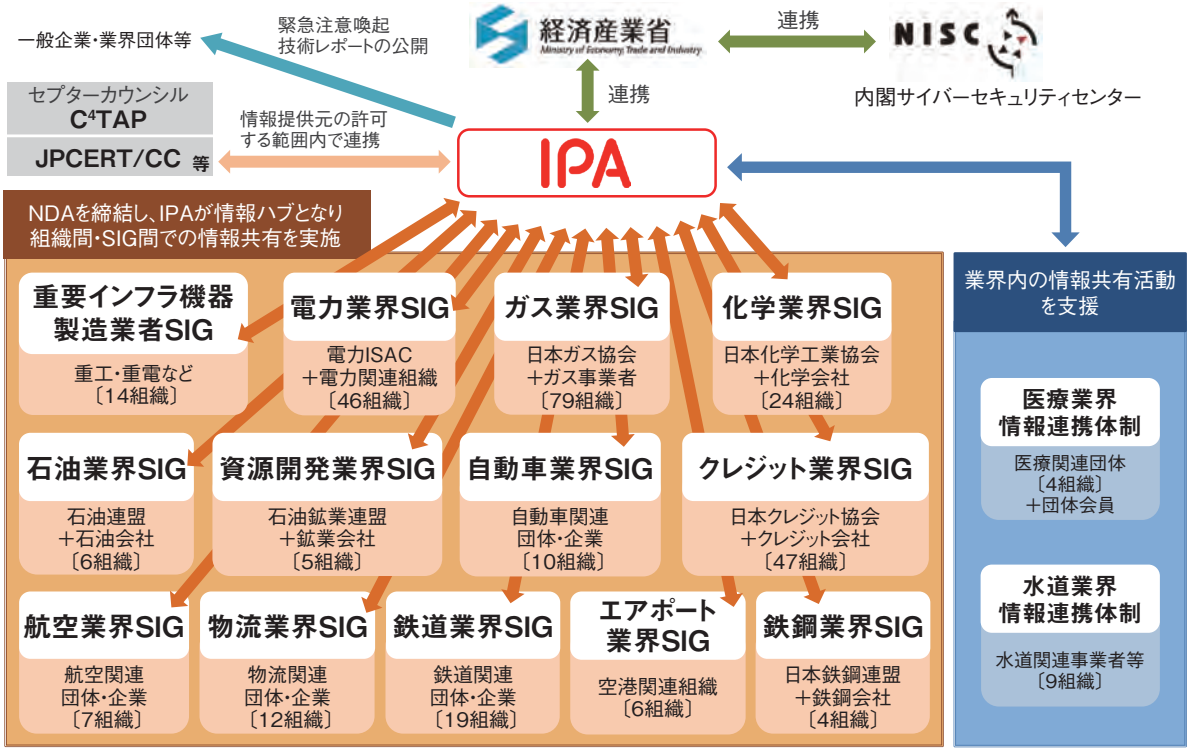
J-CSIP では、IPA と参加組織との間でサイバー攻撃に関する手口や被害の情報、標的型攻撃メール等に関する情報共有を行っている。なお、J-CSIP の中で共有される情報は、提供元が明らかにならないよう、情報提供者の固有の情報を除去するルールがある。

2023 年度も、VPN 装置等のインターネット境界に設置された装置に対するサイバー攻撃（ネットワーク貫通型攻撃）が問題となった（ネットワーク貫通型攻撃については「1.2.2 標的型攻撃」参照）。J-CSIP 参加組織からも、この攻撃に関連する情報の提供があり、不正通信先の IP アドレス等の情報を参加組織に共有し※123、同様の攻撃発見に役立てた。

J-CSIP では、無作為に送信される不審メールやウイルスメール（ばらまき型メール）については、一般的に脅威の度合いが低いと考えられることから、原則として情報の提供依頼や共有の対象とはしていない。しかし、広くばらまかれているメールであっても、セキュリティ製品による検知をすり抜けるテクニックが複数用いられたもの等、特に注意を要する手口については、情報共有の対象とし、参加組織に警戒を促した※123。ばらまき型メールと見なせる攻撃であっても、かつて標的型攻撃で使われていたような巧妙な手口が取り入れられている傾向があり、状況に応じ、今後も情報共有を図っていく必要があると思われる。

ビジネスメール詐欺に関しては、2022 年度までと同様、複数の情報提供を受けた。企業間の取り引きのメールに介入したり、CEO（Chief Executive Officer：最高経営責任者）になりすましたりする等、基本的な騙しの手口は変わらない。ただし、役員の声に似せた電話の併用や、文書の偽造等、巧妙な騙しの手口を使用する事例が確認されている（「1.2.3 ビジネスメール詐欺（BEC）」参照）。これらの詳しい情報を J-CSIP 内で共有するとともに、情報提供元の許可が得られた範囲で、事例の一般公開も行った※124。

このほか、情報提供元の組織をかたったフィッシングメールとフィッシングサイトが確認された事例や、日本の企業を装ったウイルス付きのメール等の情報提供があり、



■図 2-1-11　J-CSIP の体制全体図
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023 年 10 月～ 12 月］※122」

それぞれ共有を行った。

前述したとおり、ネットワーク境界にある機器のゼロデイ脆弱性を悪用した高度な標的型攻撃が複数確認されている。ネットワーク境界にある機器を侵害されると、攻撃者が目標としている組織の情報資産等に直接アクセスすることが可能となる恐れがあり、一層の注意が必要と思われる。一方で、特定の業界や組織を標的としたメールによる攻撃も引き続き観測されており※125、警戒が必要である。

情報共有活動は、攻撃の痕跡や手口の情報を基に、防御側で連携して対抗するための重要な施策の一つであり、IPA は引き続き J-CSIP の運用を継続していく。

(6) J-CRAT(サイバーレスキュー隊)

経済産業省の協力のもと、IPA は 2014 年 7 月に J-CRAT (Cyber Rescue and Advice Team against targeted attack of Japan:サイバーレスキュー隊) を発足させた。J-CRAT の目的を以下に示す。

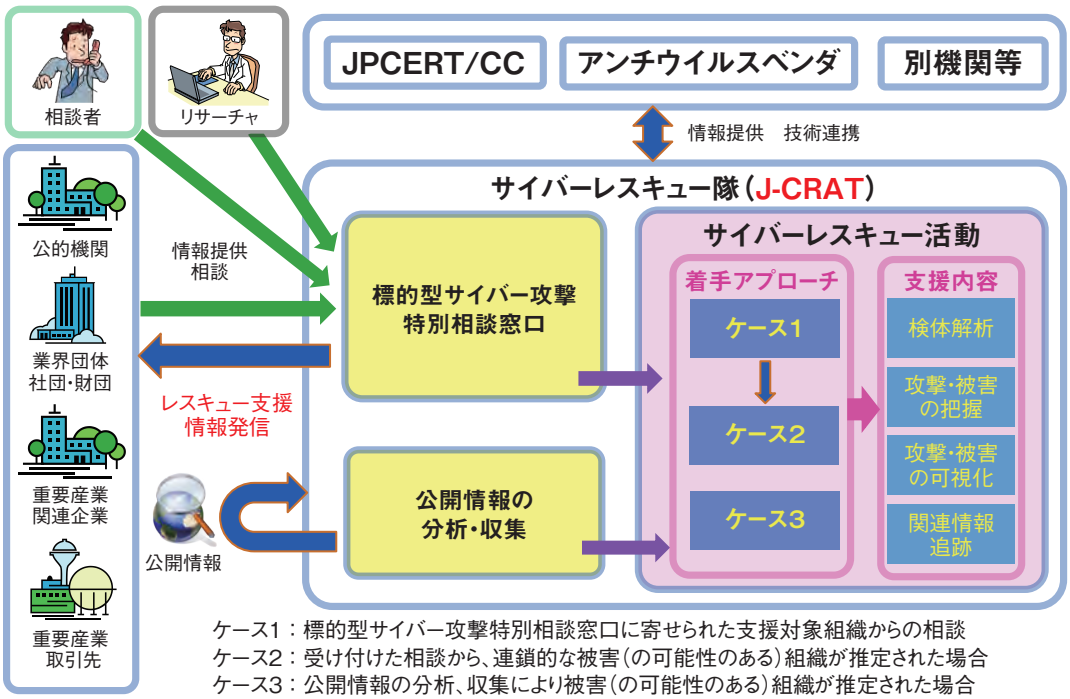
- 攻撃に気付いた組織における被害拡大と再発の抑止・低減
- 標的型攻撃による諜報活動等の連鎖の遮断

J-CRAT では、常時「標的型サイバー攻撃特別相談窓口」(以下、窓口)の運営と「公開情報の分析・収集」の二つの活動を実施している。

窓口では、主に公的機関等の組織から、標的型攻撃メールに関する情報提供や相談を受け付けている※126。「公開情報の分析・収集」では、日々公開されるインターネット上の情報等から、各種ウイルス情報等を収集している。また、これまでの活動実績から、地政学や国際政治、国際経済や科学技術等に関する動向との関連が明らかになったため、それらの情報収集を幅広く行っている。

標的型攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等サプライチェーンを構成する組織に対して、被害実態の確認と認知の支援、被害緩和の暫定対応に関する助言を「サイバーレスキュー活動」として実施している※127。また、窓口における対応の結果、必要があると判断した組織に対して、攻撃の期間・内容、感染範囲、想定被害等をヒアリングし、早急な対策着手が行えるよう、民間セキュリティ事業者への移行を前提とした助言を行っている(図 2-1-12)。

J-CRAT では、情報収集活動や支援活動から得られた結果を基に、注意喚起情報や技術レポートを随時公開している。これらの取り組み等を通じ、被害組織のセキュリティインシデントに対する速やかな対応力向上や、平時における標的型攻撃への対策力向上に資する活動を行っている。また、活動を通じて組織のセキュリティ人材の育成、標的型攻撃の連鎖の解明、及び攻撃の連



■図 2-1-12　J-CRAT の活動の全体像とスキーム
(出典)IPA「サイバーレスキュー隊 J-CRAT(ジェイ・クラート)について※127」を基に編集

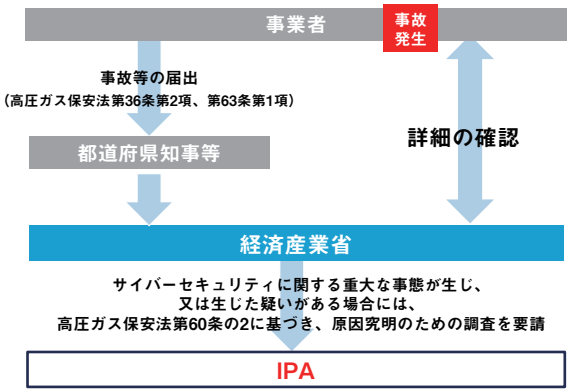
鎖を遮断することによる被害の低減を推進していく。

(7) 重要インフラ業界のサイバーインシデントに係る事故調査事業

近年、重要インフラや社会基盤を狙ったサイバー攻撃のリスクが懸念されており、プラント等で事故が発生した場合に、サイバーインシデントの観点からの原因の究明が可能な機能を整備することが必要となっている。

そのような背景から、日本では2023年12月に「高圧ガス保安法等の一部を改正する法律（令和4年法律第74号）」が施行され、電力、ガス、高圧ガス分野のプラント等で重大な事故等が発生し、保安に係るサイバーセキュリティに関する重大な事態が生じた場合、またはその疑いがある場合に原因究明の調査を行うことが規定された[※128]（図2-1-13）。

事故の調査は、経済産業省からの要請を受けて、IPA産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）の調査分析部サイバーインシデント調査室[※129]が実施する。同調査室は産業界や中核人材育成プログラム（「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）の修了者と連携して、サイバー攻撃に起因する事故かどうかを調査し、経済産業省へ報告する。同調査室が国内初のサイバーセキュリティに関する事故原因の調査機関として機能し、事故原因が明らかになることで、重要インフラ業界におけるサイバーリスクへの対応方針の検討やガイドラインの策定等が可能になり、防護力の向上につながることが期待される。



■図2-1-13　サイバー事故調査のフロー

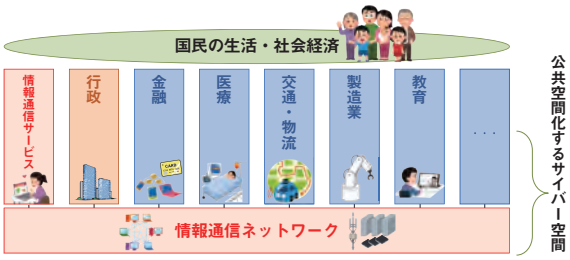
2.1.4 総務省の政策

総務省は「ICTサイバーセキュリティ総合対策2023[※130]」（以下、総合対策2023）を2023年8月に公表した。総合対策2023は前年に公表された「ICTサイバーセキュリティ総合対策2022[※131]」（以下、総合対策2022）の策定後、国際情勢の緊迫化を含めたサイバー攻撃リスクの拡大等の状況変化を踏まえた議論、及びIoT機器を狙ったサイバー攻撃が多く発生している状況等に対応するため、「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」で2023年1月から行った議論を経て必要な改定を行ったものである。

その際、総務省はサイバーセキュリティについて、総合対策2022と同様に以下のように整理した。

- サイバー空間は、あらゆる主体が利用する公共空間であり、その根幹は情報通信ネットワークである（図2-1-14）。
- サイバー攻撃等により情報通信ネットワークの機能停止や情報の漏えい等が生ずれば、国民の生活や我が国の経済社会に甚大な影響が発生する恐れがある。

その上で「社会経済活動を支える情報通信ネットワークの安全を確保し、サイバー空間を利用するすべての国民のサイバーセキュリティの向上を図ること」を総務省の役割とした。

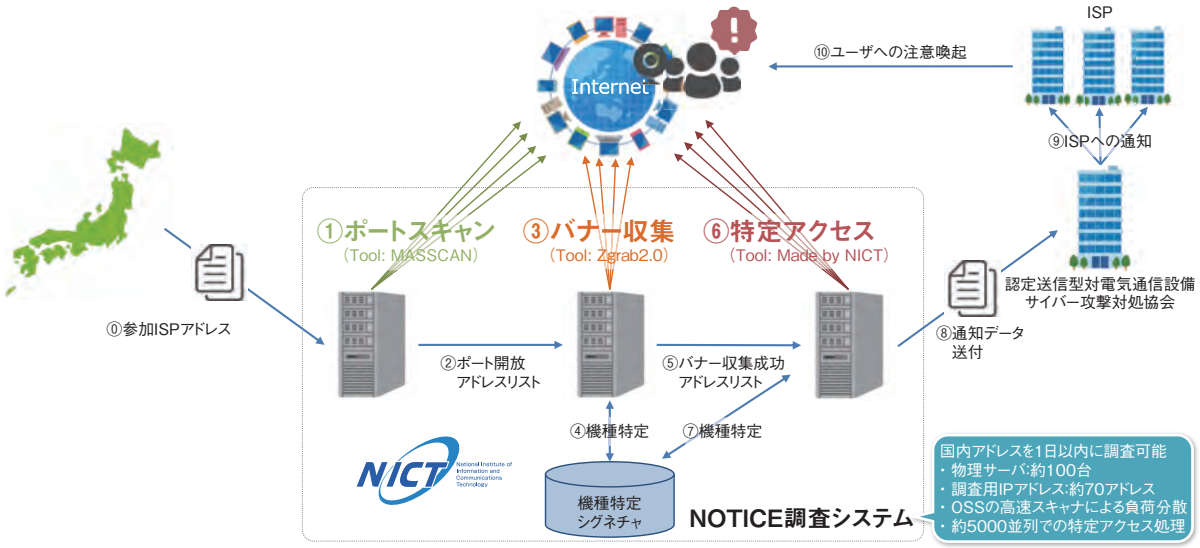


■図2-1-14　サイバーセキュリティと総務省の役割
（出典）総合対策2023を基にIPAが編集

以下では、総合対策2023に基づき「総合的なIoTボットネット対策の推進」と「電気通信事業者による積極的サイバーセキュリティ対策の推進」等について述べる。なお、総務省における人材育成に関する施策については、「2.3.3(1)(b)NICTにおける人材育成」に記載している。

(1) 総合的なIoTボットネット対策の推進

2023年1月、サイバーセキュリティタスクフォースのもとに、総合的なIoTボットネット対策の実現に向けて「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」が設置された[※132]。同分科会は、端末（IoT機器）側、ネットワーク側それぞれについて今後取り組むべき対策について検討するため、2023年6月まで毎月1回開



■図 2-1-15　ID、パスワードに脆弱性がある IoT 機器の調査の概要
(出典)付録 4

催された※133。その検討結果は、総合対策 2023 の「付録 4 情報通信ネットワークにおけるサイバーセキュリティ対策分科会とりまとめ」(以下、付録 4)として公表された。付録 4 に基づいて、IoT ボットネット対策について述べる。

(a) NOTICE における端末(IoT 機器)側の調査

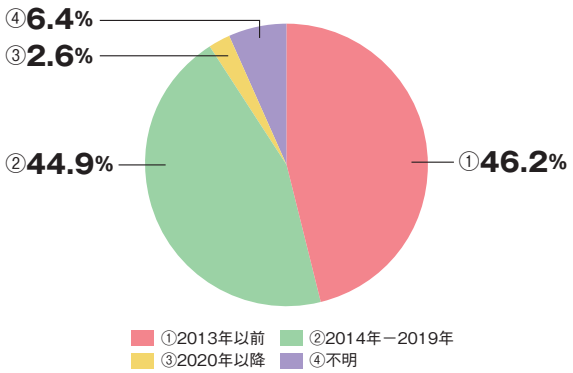
総務省所管の NICT が推進する IoT ボットネット対策は、以下の二つがある。

- NOTICE (National Operation Towards IoT Clean Environment):ID、パスワードに脆弱性のある IoT 機器を検知し、注意喚起する取り組み(図 2-1-15)
- NICTER (Network Incident analysis Center for Tactical Emergency Response):ウイルスに感染している IoT 機器を検知し、注意喚起する取り組み

注意喚起は一般社団法人 ICT-ISAC を通じ、インターネットサービスプロバイダー (ISP:Internet Service Provider、以下 ISP 事業者)に通知する。ISP 事業者はそれを受け、個別に利用者に注意喚起を行う。

NOTICE は ISP 事業者の自主的な協力を基本としており、開始当初の参加 ISP 事業者数は 24 社であったが、2024 年 2 月現在 83 社の参加手続きが完了している。また、調査対象となる IP アドレスの総数は 1.12 億個となっている。

ISP 事業者にとって、自網内の IoT ボットネットから自網外に送信される攻撃通信は、外部から自網へ向けての攻撃通信と比べ、通信を遮断した場合に正常な通信も遮断してしまう恐れがあるため、一般的に対策が困難とされている。そのため、IoT ボットネットとボットネット化の恐れがある IoT 機器をあらかじめ、可能な限り減らす取り組みがポイントとなる。NOTICE の取り組みの結果、ID、パスワードに脆弱性のあるボットネット化の恐れがある IoT 機器の削減にはある程度成果が上がっているものの、現在でも一定数残存しているという。特に注意喚起対象になった機器のうち、10 年以上前に発売された機器が 4 割以上を占めていることが明らかになり(図 2-1-16)、IoT 機器のライフサイクルの長さによる対策の難しさをうかがわせた。



■図 2-1-16　注意喚起対象となった IoT 機器の発売年の割合
(総数 27,925 台、2022 年 11 月〜2023 年 4 月)
(出典)付録 4 を基に IPA が編集

他方、NICTER によりウイルス感染による感染通信が検知され、注意喚起対象となった IoT 機器の数は 2022 年春以降高止まっているという(注意喚起の実施結果については「3.5.4 (1) 国内における実態調査と注意喚起」参照)。

付録 4 では、今後の対応策として以下の 3 点が示されている。

①脆弱性等のある IoT 機器の調査の延長・拡充

観測能力の維持・強化の観点、及びサイバー攻撃の手法の多様化への対応のため、2024 年度以降の調査の延長、拡充を実施する。

②利用者への注意喚起等の実効性の向上

メーカーやシステムインテグレーター（以下、SIer）と連携し、脆弱性のある IoT 機器のリスク、不利益について一般利用者への周知を強化する。更に、感染通信を発している IoT 機器や脆弱性のある IoT 機器に対して利用者が注意喚起等に応じない場合に、ISP 事業者が接続を拒否する具体的要件や手続き等の妥当性について示す「端末設備の接続に関するガイドライン（仮称）」を策定する。

③メーカーや SIer 等、幅広い関係者との連携による総合的な対処

利用者への注意喚起以外に関係事業者と連携を進め、総合的な脆弱性の対処を推進する（表 2-1-1）。

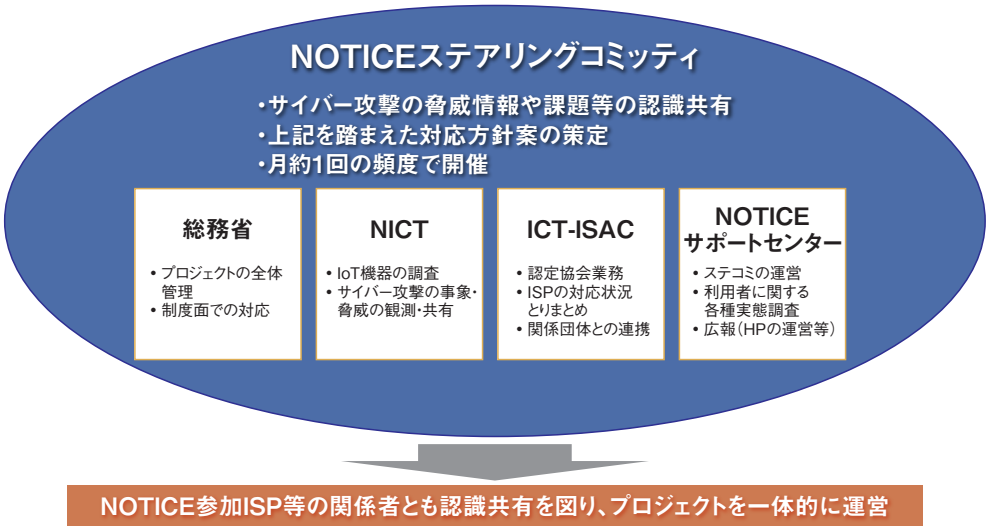
連携例	対処例
ISP 事業者との連携	レンタルサービス等を通じて機器が ISP 事業者によって管理されている場合、利用者に直接対処を求めることなく ISP 事業者側で一括して対処する。
メーカーとの連携	注意喚起対象となった製品について、利用者への情報提供、ファームウェアの改修・更新や新製品の機能改善等必要な対処を促す。
SIer との連携	法人利用者等、機器の設置・管理に SIer が関与している場合、SIer を通じて機器の ID・パスワードの設定等やファームウェアの更新等必要な対処を促す。

■表 2-1-1　IoT 機器に対する利用者への注意喚起以外の対処例
（出典）付録 4 を基に IPA が編集

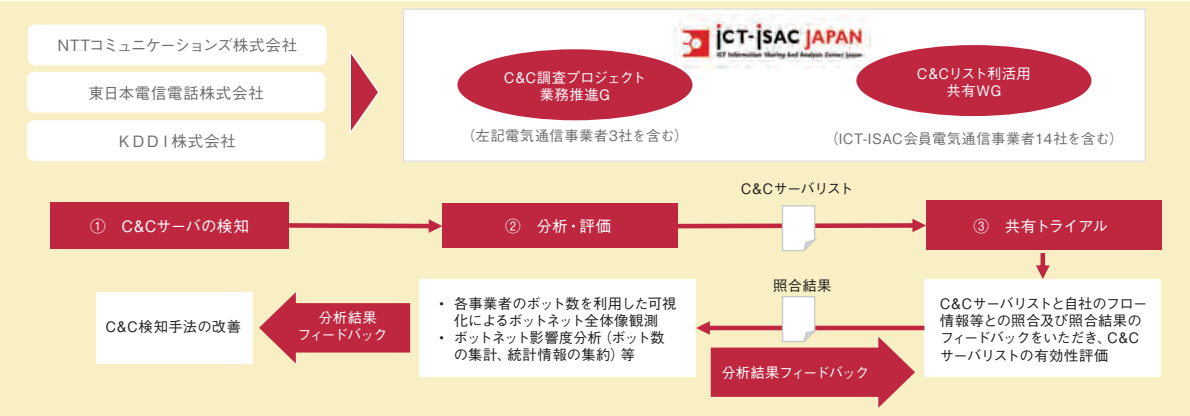
①～③を効果的に実施するため、NOTICE の運営体制の強化が求められる。NOTICE の柔軟かつ効率的な運営に取り組むため、司令塔としての役割を担う「NOTICE ステアリングコミッティ」が 2023 年 5 月に立ち上げられた。その役割は、サイバー攻撃の事象、脅威の認識共有を行った上で通信サービスへのリスクを評価し、そのリスクレベルに応じて IoT 機器の調査や利用者への注意喚起、周知啓発等を機動的に実施するというものである（図 2-1-17）。また、取り組みの前提となる脆弱性等のある IoT 機器の調査には、必要に応じ外部関係者との連携を一層推進するという。なお、NOTICE は当初、2024 年 3 月末までの時限措置として、2019 年 2 月に開始された。その後、2023 年 12 月に公布された「国立研究開発法人情報通信研究機構法の一部を改正する等の法律」の施行に伴い、時限設定が解除され、NOTICE 事業が継続されることになった※134。これに伴い、IoT 機器におけるパスワードの設定不備以外の脆弱性として、ファームウェアの脆弱性を有する機器の調査、及び NICTER を活用した既感染端末の探索も調査対象となった※135。

(b) ネットワーク側やその他における対策

一般社団法人 ICT-ISAC は 2022 年 11 月に「C2 リスト利活用共有 -WG」を立ち上げた※136。そして 2022 年度から 2023 年度にかけて「電気通信事業者におけるフロー情報分析による C&C サーバ検知に関する調査」



■図 2-1-17　NOTICE ステアリングコミッティの概要
（出典）付録 4



■図 2-1-18 「電気通信事業者におけるフロー情報分析による C&C サーバ検知及び共有に関する調査」概要
（出典）一般社団法人 ICT-ISAC「別紙1．本調査の概要※140」

（図 2-1-18）を実施した※137。同調査の目的は「未知の C&C サーバ検知」と「C&C サーバリストの有効性評価のためのボットネットの調査」である。NTT コミュニケーションズ株式会社、KDDI 株式会社、東日本電信電話株式会社の 3 社（以下、電気通信事業者 3 社）が IP アドレス等のフロー情報※138 から特定した「C&C サーバリスト」を共有し、電気通信事業者の情報と照合するという※139。その結果、既存手法より早期に検知されたケース、特定の電気通信事業者のみが検知したケースがあり、事業者間連携による多くの検知や、影響度の高い C&C サーバーの特定が期待される。

一方、リアルタイムに検知データが活用できるよう、「C&C サーバリスト」の共有の仕組み、共有すべきデータの検討、具体的利用シーンの整理、検知手法の共有が課題として指摘されている。

今後の対応策としては、以下が挙げられている。

- NICT その他関係機関との連携等による C&C サーバーのさらなる検知精度の向上
- 検知・評価作業の短縮化
- C&C サーバーの死活監視を通じ、活動状況の逐次観測、収集データのリアルタイム性の確保
- 「C&C サーバリスト」の迅速かつ効果的な共有・利活用に向けた具体的な枠組み、ルールの策定
- ISP 事業者間での検知手法の情報共有の促進

加えて、IoT ボットネットの全体像の可視化に向け、観測網である「統合分析対策センター（仮称）」の立ち上げが予定されている※141。可視化により個々の IoT ボットネットの状況に応じた効果的な対策を実現し、IoT ボットネットの縮小を目指すとしている。

(2) 電気通信事業者による積極的サイバーセキュリティ対策の推進

2023 年度には、電気通信事業者による積極的なサイバーセキュリティ対策に関する総合実証として以下の三つが実施された。

- 自動巡回による機械的処理を活用した、フィッシングサイト等の悪性 Web サイトの検知技術・共有手法の検討・実証
- ネットワーク側の対策としての平時におけるフロー情報の収集・蓄積・分析による C&C サーバーの検知に係る技術実証（「2.1.4 (1) (b) ネットワーク側やその他における対策」参照）
- RPKI（Resource Public-Key Infrastructure）※142 や DNSSEC（DNS Security Extensions）※143、DMARC（Domain-based Message Authentication Reporting and Conformance）※144 等のネットワークセキュリティ技術について、技術的な課題にとどまらない普及方策の検討

上記の実証を踏まえ、2024 年度は収集・分析した悪性 Web サイトの情報をセキュリティサービス等に活用した際の効果検証、悪性 Web サイト対策のガイダンスを作成するとしている。また、RPKI、DNSSEC、DMARC 等のネットワークセキュリティ技術については普及促進に向けたガイドライン案を作成するとしている。

(3) ICT サイバーセキュリティ政策分科会

2024 年 2 月にサイバーセキュリティタスクフォースのもとに「ICT サイバーセキュリティ政策分科会」を開催することが発表された※145。総務省が中長期的に取り組むべきサイバーセキュリティ施策の方向性を検討するため、

主に以下 3 点を検討するという。

- 重要インフラ分野におけるサイバーセキュリティ対策強化の在り方
- サイバーセキュリティの基盤となる人材育成及び研究開発の在り方
- サイバーセキュリティの確保に向けた国際連携及び普及啓発の在り方

第 1 回の会合は同年 2 月 9 日に行われ、3 月末までに 4 回開催された。サイバーセキュリティの最近の状況、我が国を取り巻くサイバーセキュリティの情勢、通信分野におけるサイバーセキュリティ対策の取り組み等が議題として挙げられた。

(4) 地方自治体に向けたサイバーセキュリティ対策強化

2024 年 3 月 1 日、総務省が地方自治体に対し、サイバー攻撃に対処するための基本方針の策定と公表を義務付ける、地方自治体法改正案が閣議決定され、国会に提出された※146。「地方自治法の一部を改正する法律案の概要」によれば DX の進展を踏まえた対応の一つとして、地方自治体がサイバーセキュリティの確保の方針を定め、必要な措置を講じることが示されている。そしてその方針の策定等の指針を総務大臣が示すという※147。総務省は方針策定の参考となるガイドラインを新たに作成する予定で、これが指針となる。地方自治体はこの法改正を受け、2026 年 4 月 1 日までに基本方針の策定が求められ、方針に基づいた各種対策を講じる必要がある。

2.1.5 警察によるサイバー空間の安全確保の取り組み

2021 年 9 月に閣議決定されたサイバーセキュリティ基本法に基づき、警察庁は、2022 年 4 月に「警察におけるサイバー戦略※148」を改定した。

そこでは、サイバー空間の安全･安心を確保するため、深刻化する脅威に対処できる態勢の整備、国内外の多様な主体との連携強化、社会全体でのサイバーセキュリティ向上に向けた取り組みの推進強化を掲げ、同戦略に基づき「サイバー重点施策について※149」（以下、重点施策）も併せて改定した。

重点施策では、上記戦略に基づき 2022 年からの 3 年間の取り組みを掲げている。具体的には、「①体制及び人的・物的基盤の強化」としてサイバー空間の脅威に対処するための警察庁及び都道府県警察における体制構築や優秀な人材の確保及び育成、警察における情報セキュリティの確保等、「②実態把握と社会変化への適応力の強化」として通報・相談への対応強化による実態把握の推進や実態解明と実効的な対策の推進等が挙げられている。そのほか「③部門間連携の推進」「④国際連携の推進」「⑤官民連携の推進」も併せた五つの施策が推進されている。

本項では、2023 年度の重点施策への取り組み状況とサイバー攻撃、犯罪の情勢等について、主に「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について※150」及び「令和 5 年版 警察白書※151」等に基づいて述べる。

(1) 警察における主な取り組み

2023 年の警察における主な取り組みとして、組織基盤強化、実態把握と社会変化への適応力の強化、国際連携、官民連携等の四つについて述べる。なお、2022 年度以前より継続している人材育成の取り組みについては、「情報セキュリティ白書 2023※152」の「2.1.5(1)(b) 警察における人材育成の取り組み」を参照いただきたい。

(a) 警察における組織基盤の更なる強化

警察庁では、サイバー空間をめぐる脅威に対処するため、2022 年 4 月に「サイバー警察局※153」を、関東管区警察局に「サイバー特別捜査隊※154」を新設した。

サイバー警察局は、警察庁内各局や国内外の様々な主体と連携し、人材育成等の基盤整備、各国との情報交換、サイバー事案の捜査指揮、不正プログラム等の解析への技術支援等のサイバー政策の推進における中心的な役割を担うものである。一方、サイバー特別捜査隊は、国の捜査機関として国や国民に深刻な影響を及ぼす重大なサイバー事案への対処等を担うものである。その発足後に国内では特殊詐欺の被害金が暗号資産でマネーロンダリングされた形跡を解析、国外では海外の捜査機関と連携し、ランサムウェアの犯人を訴追する等の成果を上げてきたことから、警察庁は 2024 年度の組織改正要求でサイバー特別捜査隊を「サイバー特別捜査部」に格上げすることを明記※155 し、2024 年 4 月 1 日にサイバー特別捜査部が発足した。

警察庁並びに都道府県警察における情報セキュリティの確保も喫緊の課題である。脆弱性情報等情報セキュリティインシデントに発展し得る情報の早期把握を目的とした

最高情報セキュリティ責任者（CISO：Chief Information Security Officer）を中心とした情報セキュリティ体制と、サイバー部門の間で円滑な情報共有が行われる体制の整備と組織内の情報セキュリティインシデントの適切な対処のためにサイバー部門が連携した実効的なCSIRT体制も構築するとしている。

このほかの2022年度以前より継続している組織基盤強化の取り組みについては、「情報セキュリティ白書2023」の「2.1.5 (1) (a) 警察における組織基盤の更なる強化」を参照いただきたい。

(b) 実態把握と社会変化への適応力の強化

急速に変化するサイバー事案の脅威の情勢に対処するために、次のような施策を実施している（具体的な事例については「2.1.5 (2) (b) サイバー攻撃に対する警察の取り組み事例」等で詳述）。

(ア) 通報・相談への対応強化による実態把握の推進

サイバー警察局及び都道府県警察では、被害通報を促進するための広報・啓発活動に取り組むとともに、民間事業者とも連携して、通報・相談が適切になされるような気運の醸成や環境整備を行うとしている。また、サイバー部門に遅滞なく伝達する手順を確立する等、部門間連携に加え、より適切かつ円滑な対応を可能とするための相談対応の充実や官民連携の強化も推進している。更に、サイバー犯罪の被害企業等における業務の早期復旧等に配慮した初動捜査を推進している。

(イ) 実態解明と実効的な対策の推進

サイバー警察局にサイバー関連情報の分析を担う体制を構築し、警察内のサイバー関連情報に加え、関係機関・団体や事業者から提供される情報等の多様な情報の分析を推進している。また、サプライチェーンの複雑化等へ対処するため、平時から関係機関・団体や事業者等と連携した分析評価を推進している。更に情報窃取の標的となる恐れの高い先端技術を有する事業者等との情報交換を積極的に推進している。一方、サイバー事案の捜査や通報・相談等を通じて事案を把握した場合は、一つの事案のみに着目するのではなく、事案に関係する情勢を俯瞰的にとらえ、攻撃者につながる可能性のある情報や、その他の広範な関連情報を総合的に収集・分析・評価する。それにより、特定の攻撃グループ、国家機関等が関与していることを明らかにする等、より広い範囲での実態解明を進めるとしている。特に、ランサムウェアについては、多業種にわたって甚大な影響を及ぼしていることから、関係行政機関、団体等が連携してサイバー事案の分析を行い、被害の再発や未然防止・拡大防止に向けた取り組みを推進している。

事案対処に際しては、被疑者の検挙のみならず、犯行手口等の実態解明や被害の拡大防止等にも努めるとしている。そのためには、関係省庁等と連携し、解明された情報の適切な公表等を推進するとともに重要インフラ事業者等との実践的な共同対処訓練も実施する。実態解明のための分析・解析にあたっては、ウイルスの多様化・耐解析機能の実装等に対処していくため、機械学習の活用等を進めて解析態勢を強化し、解析の効率化・高度化を図る。また、インターネット上の脅威情報等の収集及び分析の高度化を狙い、児童ポルノや規制薬物広告、自殺誘引情報等の違法・有害情報に厳正に対処するため、インターネット・ホットラインセンターからの通報及びサイバーパトロール等を通じて把握した情報を端緒として、削除依頼等を積極的に推進している。

更にインターネット上の脅威情報を収集・分析するリアルタイム検知ネットワークシステムについて、能動的に犯罪の端緒等を検知・発見する等、情報収集・分析を高度化するとしている。

(c) 国際連携の推進

警察庁は、国際共同捜査への積極的な参画に向けた環境を整備するとともに、国境を越えたサイバー事案に対処するため、外国捜査機関等との信頼関係を構築し、互恵的な関係の構築を図っている。

具体的な連携活動として、2004年から開催され13回目となるASEAN＋3国際犯罪閣僚会議が、ASEAN10ヵ国に日本、中国及び韓国を加え、2023年8月22日に開催された。日本とASEANとの間で2013年から開催され8回目となる日･ASEAN国際犯罪閣僚会議も、同日に開催された。両会議とも各国間の国際連携強化を目的としている。

両会議に出席した谷公一国家公安委員会委員長は、サイバー犯罪対策、特殊詐欺対策、テロ対策等における各国の連携強化の重要性について述べるとともに、北朝鮮による拉致問題の即時解決に向けた協力を要請した。特に谷国家公安委員会委員長が共同議長を務めた日・ASEAN国際犯罪閣僚会議では、特殊詐欺の深刻な被害についてASEAN諸国と懸念を共有し、犯罪組織に対峙するため、捜査協力等を強化することを改めて確認した[※156]。

(d) 官民連携の推進

警察では、次のような官民連携施策を推進している。

- 民間事業者等と連携した犯罪インフラ対策の推進
  データ通信用SIMカード契約、SMS認証、インターネットバンキング、eコマースにおけるクレジットカード利用等、新たなサービスや技術の悪用を防止する観点からのサービス仕様の見直しや事後追跡可能性の確保等、民間事業者等による必要な対策推進に向けた被害実態の情報提供等の働き掛けを推進している。
- 地域において活動する多様な主体との連携
  都道府県警察は、サイバー保険を取り扱う損害保険会社等と連携する等※157、中小企業等に対する広報・啓発活動を推進している。また、サイバー事案の潜在化防止や再発防止を目的とした共同対処協定を広範な業界の企業や商工会等の産業組織と締結することを推進している。更に最近注目度が高まっている経済安全保障の観点から、サイバー事案により様々な情報が窃取されるリスクやサプライチェーンを構成する企業が打撃を受けるリスクがあることについて、注意喚起を行っている。
- 警察庁サイバー警察局とIPAとの連携
  2023年12月にサイバー事案の未然防止や事案発生時の被害拡大防止を図るためにサイバー警察局とIPAは連携協定を締結した※158。同協定に基づき、サイバー事案被害等が発生したときに、都道府県警察が一般的な技術支援・助言を通報・相談者から求められた場合、IPAが運営する情報セキュリティ安心相談窓口を紹介する。また、平時においては、広報啓発セミナーの開催や注意喚起の情報発信等で連携する。
  なお、サイバー警察局では、警察庁の注意喚起情報を集約して公開している※159。

官民連携の推進については、「2.1.5 (2) (a) サイバー空間の脅威の情勢」のランサムウェアやフィッシングに関する記述の中でも事例を挙げている。

このほかの2022年度以前より継続している官民連携の取り組みについては、「情報セキュリティ白書2023」の「2.1.5(1)(d)官民連携の推進」を参照いただきたい。

(2) 2023年のサイバー攻撃の情勢と警察の取り組み

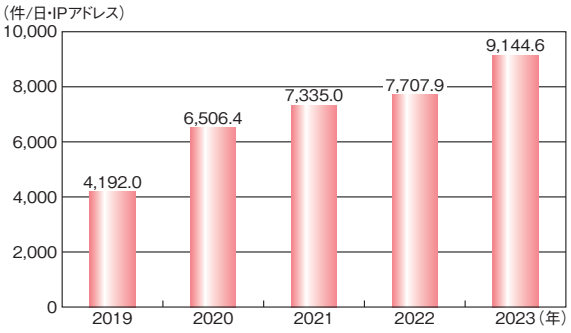
2023年におけるサイバー空間の脅威の情勢と、その脅威に対し、安心・安全を確保するための警察の主な取り組みについて述べる。

(a) サイバー空間の脅威の情勢

2023年におけるサイバー空間の脅威の情勢について述べる。

(ア) センサーにおいて検知したアクセスの概況

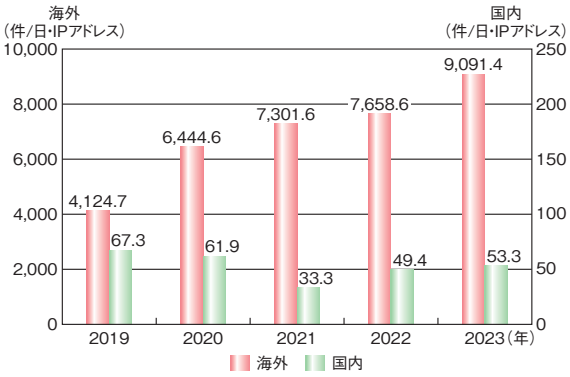
警察庁では、インターネット上にセンサーを設置し、不特定多数のIPアドレスに対して無差別に送られてくる通信パケットを収集し、分析することで、インターネットに接続された各種機器の脆弱性の探索行為等を観測している※150。これにより、脆弱性を悪用した攻撃、ウイルスに感染したコンピューターの動向等、インターネット上で発生している各種事象を把握することができる。2023年に同センサーが検知したアクセス件数は、1日・1IPアドレスあたり9,144.6件と前年を18.6%上回り、2011年以降、増加の一途をたどっている(図2-1-19)。アクセス件数が増加している背景として、IoT機器の普及により攻撃対象が増加していることや技術の進歩により攻撃手法が高度化していること等が想定されるとのことである。



■図2-1-19　センサーが検知したアクセス件数の推移(2019～2023年)
(出典)警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」を基にIPAが編集

2023年に検知したアクセスの送信元を分析すると、国内を送信元とするアクセスが1日・1IPアドレスあたり53.3件であるのに対して、海外を送信元とするアクセスが9,091.4件と大部分を占めている(次ページ図2-1-20)。依然、海外が高い割合を占めており、海外からの脅威への対処が引き続き重要であることは明白である。

2023年においては、IoT機器に対するMirai等のウイルス感染拡大を狙ったと思われるアクセスも多数観測されている。国内を送信元とするMiraiボットの特徴を有するアクセスを宛先ポート別に分析すると、宛先ポート52869/TCPに対するアクセスが2023年5月中旬ごろから増加していたという※125。



■図 2-1-20　検知したアクセスの送信元で比較した 1 日・1IP アドレス当たりの件数の推移(2019～2023 年)
(出典)警察庁「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

また、脆弱性を有する VPN 機器等を探索する目的と想定される複数種類のアクセスも断続的に観測された。VPN 機器等の脆弱性を悪用されてネットワークに侵入された場合は、情報の窃取やランサムウェアの感染によるデータの暗号化等の被害に遭う可能性がある(「1.2.5 (1) VPN 製品の脆弱性を対象とした攻撃」参照)。

(イ)ランサムウェア被害の情勢

2023 年の企業・団体等におけるランサムウェア被害の報告件数は 197 件であった。2022 年よりは減少したものの、依然として高い水準で推移している(ランサムウェアの被害状況については「1.1.2 (3) ランサムウェアによる被害」「1.2.1 (1) (a)被害件数」参照)。

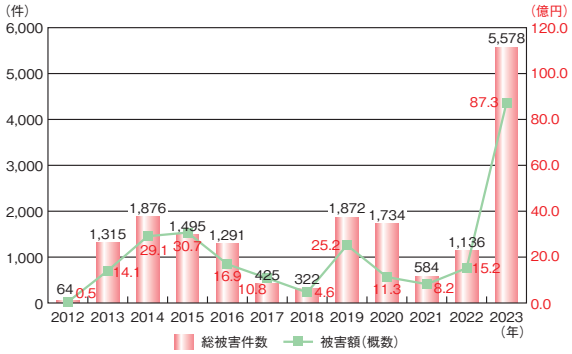
最近のランサムウェア被害の主な特徴として、以下が挙げられている。

- 二重恐喝(ダブルエクストーション)の被害は 130 件であり、手口を確認できたランサムウェア被害(175 件)の 74%[※150]、約 4 分の 3 と高い割合を占めている。
- 企業・団体等のネットワークに侵入し、データを暗号化する(ランサムウェアを用いる)ことなくデータを窃取した上で、企業・団体等に対価を要求する手口である「ノーウェアランサム攻撃」による被害が出てきている(「1.2.1 (1) (d)暗号化を伴わない攻撃手口」参照)。
- 身元が特定されにくい暗号資産による支払い要求が 87% を占めている。

(ウ)フィッシング等に伴う被害の情勢等

2023 年のフィッシング報告件数は、フィッシング対策協議会によれば、119 万 6,390 件となり、前年比で 22 万 7,558 件増加したという。

フィッシングによる主な犯罪の一つであるインターネットバンキングによる不正送金事犯の 2023 年における発生件数は過去最多の 5,578 件、被害総額は約 87 億 3,130 万円と報告されており、2023 年の悪化が著しい(図 2-1-21)。



■図 2-1-21　インターネットバンキングに係る不正送金事犯におけるフィッシングの推移(2012～2023 年)
(出典)警察庁「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

(b)サイバー攻撃に対する警察の取り組み事例

サイバー攻撃に対する警察の主な取り組み等について述べる。

(ア)ランサムウェアに対する対処

警察はランサムウェアに対処するため、以下のような取り組みを実施している。

- サイバー事案の被害潜在化防止
  ランサムウェア被害が被害者自身に対する社会的評価の悪化の懸念等から警察への通報・相談そのものがためらわれる傾向にある[※150]。警察庁では、「サイバー事案の被害の潜在化防止に向けた検討会」を開催し、業界、セキュリティ関係団体、法曹界、学術界の有識者による議論を取りまとめ、2023 年 4 月に報告書を公表した[※160]。
- 医療機関等との連携強化
  医療機関におけるランサムウェアによる被害が発生していることを踏まえ、2023 年 4 月、公益社団法人日本医師会と覚書を締結[※161]するとともに、2023 年 5 月、四病院団体協議会及び各国公私立大学病院に対して連携強化に関する依頼を行った。
- VPN 機器の脆弱性に関する広報啓発
  警察庁 Web サイト、警察庁 X(旧 Twitter)等の様々な媒体の活用や各都道府県警察が関係機関・団体等と構築する協議会等を通じて、ランサムウェア被害の主たる要因となる VPN 機器の脆弱性について情報発信を行う等、積極的な広報活動を実施した。
- リークサイト上において売買されるアクセス権の把握等

ダークウェブ上のリークサイトでは、国内の事業者等のID・パスワード等のアクセス権が掲載されるケースがある。当該リークサイトにおいて売買されるアクセス権等を監視し、都道府県警察を通じて、当該事業者等に対してID・パスワード等が漏えいしていることを示した上で、必要な対策を講じるよう求めた。

- 国際連携の強化

  欧州各国の捜査機関との緊密な連携を図るため、2022年6月から、サイバー事案に専従する連絡担当官として警察職員をEuropolに初めて常駐させた。更に、2023年2月から連絡担当官を増員し、国際共同捜査への参画に向けて各国捜査機関との更なる連携強化を推進している。この連携強化の具体的な成果として、複数国の捜査機関が協働してランサムウェア攻撃グループ「LockBit」の一員と見られる被疑者の検挙、及び関連インフラのテイクダウン（停止）を実施した※162。

  また、警察庁とNISCは米国諸機関と連携し、中国を背景とするサイバー攻撃グループ「BlackTech」によるサイバー攻撃に関する注意喚起を発出した※163。

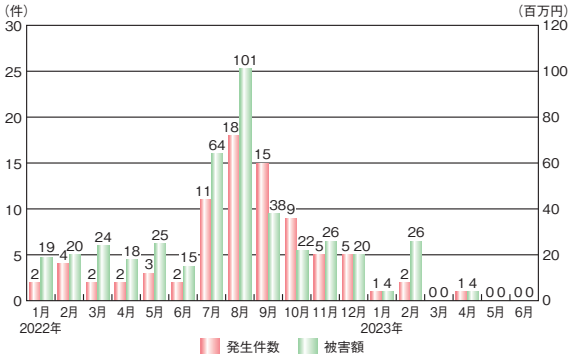
- サイバー特別捜査隊による捜査及び実態解明

  サイバー特別捜査隊が、ランサムウェアが用いられた事案の捜査及び実態解明を推進してきた結果、侵入時、侵入後、攻撃実行時の各段階で共通して見られる攻撃者の手口の解明も進んだ。

（イ）フィッシングによる不正送金等への対処

警察は急増しているフィッシングによる不正送金に対処するため、以下のような取り組みを実施している。

- 金融庁及び一般社団法人全国銀行協会等に対し、インターネットバンキングの不正送金の被害状況等の提供を実施した。
- 金融庁、一般社団法人全国銀行協会及び一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）と連携し、メールやSMSに記載されたリンク先サイトにID及びワンタイムパスワード・乱数表等のパスワードを入力しないよう2023年8月、12月に注意喚起を行った※164-1。
- SIMスワップによる不正送金事案が増加していた状況を踏まえ、2022年9月、総務省と連携し、携帯電話事業者に対して、携帯電話機販売店における本人確認の強化を要請した。2023年2月までに同対応が完了した結果、2023年におけるSIMスワップによる不正送金の被害が激減した（図2-1-22）。



■図2-1-22　SIMスワップに係る不正送金発生状況
（2022年1月～2023年6月）
（出典）警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」を基にIPAが編集

（ウ）家庭用ルーターの不正利用に関する注意喚起

家庭用ルーターがサイバー攻撃に悪用され、従来の対策のみでは十分ではないことから、2023年3月、警察庁及び警視庁において、複数の関係メーカーと協力し、注意喚起を行った※164-2。具体的には、各家庭で所有するルーターについて、初期設定のID・パスワードの変更やソフトウェアの最新バージョンへのアップデート等のほか、見覚えのない設定変更がなされていないか確認するよう呼び掛けた。

（エ）重要インフラ事業者等に対する注意喚起

2023年には、特定の情報通信機器の脆弱性に関して全国に注意喚起を実施した。更に、海外の関係機関・団体等からサイバー攻撃等に関する情報を入手した場合は個別に注意喚起を行う等、サイバー攻撃による重要インフラ事業者等の被害の未然防止・拡大防止を図った。

（オ）C2サーバーのテイクダウン

サイバー攻撃で使用されたウイルスの解析等を通じて把握したC2サーバー（C&Cサーバーとも呼ばれる）に対し、不正な機能を停止（テイクダウン）するよう、サーバーを管理する事業者等に依頼する等の対策を継続的に実施した。

（カ）サイバーインテリジェンス情報共有ネットワーク

サイバーインテリジェンス情報共有ネットワークは、警察及び先端技術を有する等の理由により情報窃取の標的となる恐れのある全国約8,600の事業者等（2023年12月末現在）から構成されている。この枠組みを通じて、事業者等から提供される標的型攻撃メールを始めとする情報窃取を企図したと見られるサイバー攻撃に関する各

種情報を集約するとともに、これらの情報を総合的に分析して、事業者等に対し、分析結果に基づく注意喚起を行っている。

(キ)共同対処訓練の実施

2023年においても、継続的に自治体、電力事業者、金融機関等の幅広い分野の重要インフラ事業者等を対象に、標的型攻撃メールを題材とした訓練や警察との連携を確認するための現場臨場訓練等の実践的な共同対処訓練を約700回実施し、警察との連携強化や各事業者等のサイバー攻撃に対する対処能力の向上を図った。

(ク)DDoS攻撃に関する注意喚起

2023年5月、NISCと連名で、重要インフラ事業者等のWebサイトへのDDoS攻撃に関する注意喚起を行った※164-3。この注意喚起では、2022年9月に発生した国内の政府関連や重要インフラ事業者等のWebサイトに対する一連のDDoS攻撃に関する分析結果を示して、同事案で確認されたDDoS攻撃の主な手口のほか、攻撃元のIPアドレスの99%が海外に割り当てられたものであること等が特徴として示された。DDoS攻撃への対策として、これら海外に割り当てられたIPアドレスからの通信の遮断、同一IPアドレスからのアクセス回数の制限等のサーバー設定の見直し等の対策を示した。そのほか、システムの重要度に基づく選別・分離、通報先・連絡先一覧を含む対策マニュアルの策定等、リスク低減に向けたセキュリティ対策の実施を呼び掛けた。

(ケ)G7広島サミットにおけるサイバー攻撃対策

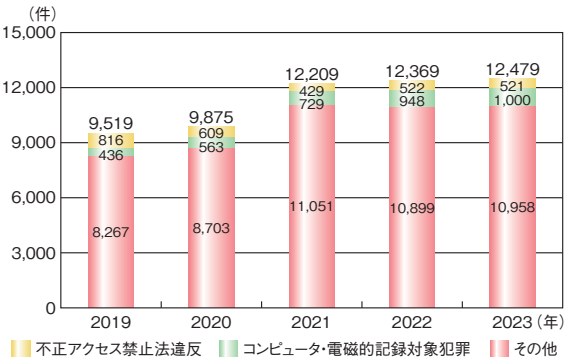
G7広島サミットでは、開催地を管轄する広島県警察を中心に、警察庁及び各都道府県警察が、推進態勢の確立、情報収集・分析の強化、管理者対策の徹底、事案対処態勢の充実等の各種取り組みを推進した。具体的な取り組みとしては、G7広島サミット及び関連行事の主催府省庁、電力、空港等の重要インフラ事業者等に対するサイバーセキュリティ対策状況の確認及び助言を行った。また、関係施設の事業者、重要インフラ事業者等とのサイバー攻撃の発生を想定した共同対処訓練、関係事業者が管理するサーバーやネットワーク機器等に対する脆弱性試験、関連Webサイトの改ざんや閲覧障害を早期に検知するための観測強化等のサイバー攻撃対策を行った。サミット期間中、広島市Webサイトにおいて DDoS攻撃によるものと見られる閲覧障害が発生する等、G7広島サミット開催の機会を狙ったサイバー攻撃が発生したものの、こうした取り組みの成果として、サイバー攻撃によるサミット等の進行への影響を防ぐことができた。

(3)2023年のサイバー事案の検挙状況等

2023年における警察が検挙したサイバー事案の状況について述べる。

(a)サイバー犯罪の検挙状況

サイバー犯罪の検挙件数は2020年まで年間、1万件以下で推移していたが、2021年は一気に2割以上増加の1万2,209件に跳ね上がった。2022年は微増にとどまり、2023年もその傾向に変動はなかった(図2-1-23)。



■図2-1-23　サイバー犯罪の検挙件数(2019～2023年)
(出典)警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」を基にIPAが編集

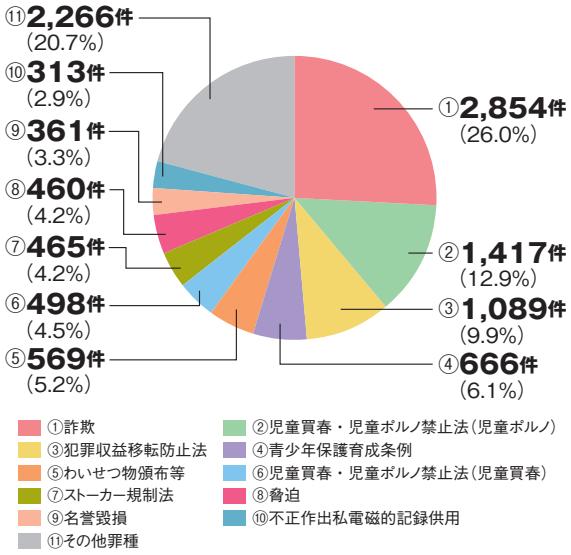
2023年に検挙されたサイバー犯罪で9割近くを占める「その他」1万958件のうち、「詐欺」がほぼ4分の1を占め、「児童買春・児童ポルノ禁止法(児童ポルノ)」違反が続いている(次ページ図2-1-24)。

(b)不正アクセス禁止法違反の情勢

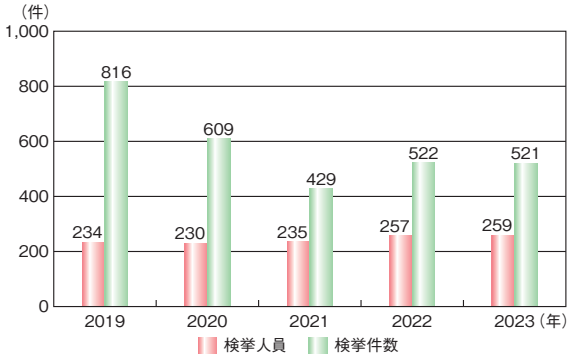
2023年に検挙されたサイバー犯罪の中で、不正アクセス禁止法違反の検挙件数は521件で前年から横ばいとなった(次ページ図2-1-25)。

521件のうち9割以上を占める475件が認証情報を悪用する手口である識別符号窃用型となっており、その中で「利用権者のパスワードの設定・管理の甘さに付け込んで入手」が最多の203件で、全体の42.7%となっている(次ページ図2-1-26)。

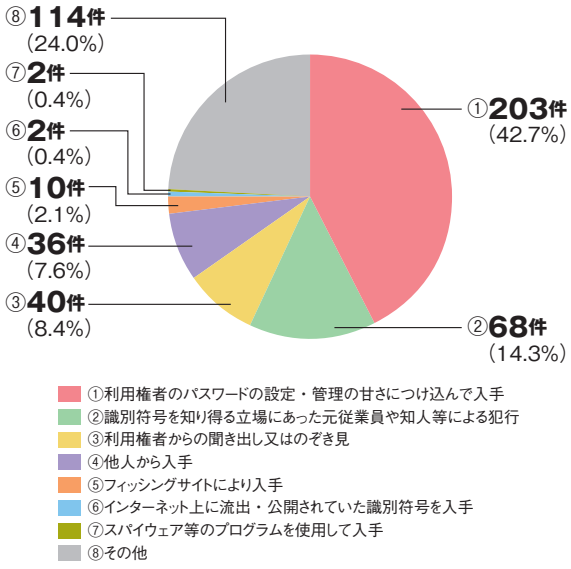
一方、識別符号窃用型の不正アクセス行為の検挙数(475件)を、不正に利用されたサービス別に見ると、「オンラインゲーム・コミュニティサイト」が最多の234件と、



■図 2-1-24　その他の検挙状況(2023 年、n=10,958 件)
(出典)警察庁「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

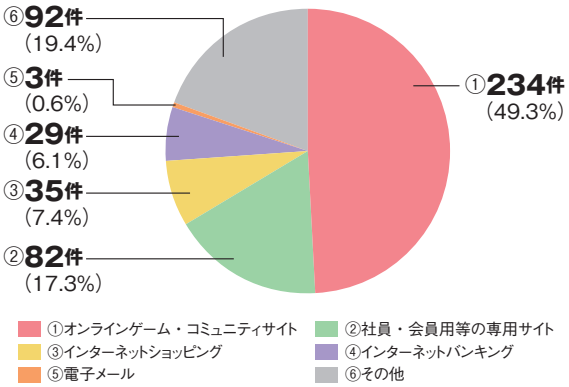


■図 2-1-25　不正アクセス禁止法違反の検挙件数(2019～2023 年)
(出典)警察庁「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 2-1-26　不正アクセス行為(識別符号窃用型)に係る手口別検挙数
(2023 年、n=475 件)
(出典)警察庁「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

身近なエンターテインメントがほぼ半数を占めている(図 2-1-27)。

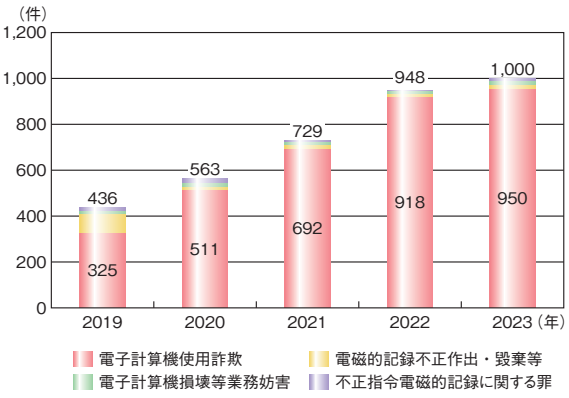


■図 2-1-27　不正に利用されたサービス別検挙件数(識別符号窃用型)
(2023 年、n=475 件)
(出典)警察庁「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

(c)コンピュータ・電磁的記録対象犯罪の検挙件数と特徴

2023 年におけるコンピュータ・電磁的記録対象犯罪の検挙件数は 1,000 件と初めて 4 桁に乗り、前年と比べて 52 件増加した。

また、総検挙件数のうち、「電子計算機使用詐欺」が 950 件と圧倒的多数を占めている。同詐欺が 90% 以上を占める傾向は 2020 年から続いている(図 2-1-28)。



■図 2-1-28　コンピュータ・電磁的記録対象犯罪の検挙件数の推移
(2019～2023 年)
(出典)警察庁「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

重要な社会経済活動が営まれる公共空間へと変貌を遂げているサイバー空間において、国民が安全・安心に生活できるデジタル社会の実現に向け、警察には引き続き、その脅威に事前予防的に対処していくことが期待されている。

2.2 国外の情報セキュリティ政策の状況

サイバー攻撃は国境を問わず、あらゆる国・地域の脆弱なシステムに対して仕掛けられる。また、IT 化した社会サービスやそれを支えるサプライチェーンは国境を越えてつながり合い、他国におけるサイバー脅威が自国に深刻な影響を与える可能性がある。更に近年、国家の支援を受けた攻撃者による他国へのサイバー攻撃や虚偽情報流布等の脅威が現実になっている。こうした状況に国や地域が単独で対処することは難しく、国際連携が不可避である。本節では、国際連携に向けた状況理解のために、各国・各地域における情報セキュリティ政策について述べる。

2.2.1 国際社会と連携した取り組み

国際社会の概況、及び我が国と各国の首脳・外相等の連携協議を中心に取り組みを述べる。なお、国際間のサイバーセキュリティ連携の基盤となる安全保障に関する協議・連携状況も含める。

(1) 国際社会の概況

2020 年から世界中で猛威を振るった新型コロナウイルス感染症に対する各国の対策、ワクチン開発が進み、感染拡大防止対策として行われてきた制限は徐々に解除された。日本でも、2023 年 5 月 8 日より、5 類感染症に位置付けられ※165、外出自粛等の制限が解除されたことで経済活動は活発になってきている。一方、2022 年 2 月に発生したロシアによるウクライナ侵攻から 2 年以上経過したが、未だに解決には至らない※166。また、2023 年 10 月にはイスラエル・パレスチナをめぐる情勢が悪化し、武装勢力による攻撃で多数の死者が出る等、緊迫した状況が継続している※167。

新しい技術としては人工知能（AI：Artificial Intelligence）が注目されている。2022 年 11 月に OpenAI, Inc. がリリースした生成 AI「ChatGPT」は、公開 2 ヵ月でユーザーが 1 億人を突破する等、AI が身近なツールとして利用されるようになった。その反面、AI 利用の安全性について各方面で議論されており、ルールや規制の整備も進んでいる。

(a) イスラエル・パレスチナ情勢に対する国際社会の対応

2023 年 12 月、国連安全保障理事会（以下、安保理事会）において、ガザ地区への人道支援の拡大及び監視に関する決議案が賛成多数で採択された※168。その後、安保理事会では、停戦等を求める決議案が提出される都度、米国が拒否権を 4 回にわたり行使した※169が、2024 年 3 月 25 日、イスラエルとイスラム組織ハマスとのパレスチナ自治区ガザでの戦闘の即時停戦と人質全員の即時かつ無条件の解放を求める決議案を賛成多数で採択した。全 15 理事国のうち 14 ヵ国が賛成し、米国は棄権した※170。

この軍事衝突をめぐっては、SNS でイスラエルとパレスチナのそれぞれを支持する立場から非難し合う様子が見られ、偽の動画等を拡散しているものもあるという※171。これに対し欧州連合（European Union）の Thierry Breton 欧州委員（産業政策担当）は 2023 年 10 月、SNS 経営者 Elon Musk、Mark Zuckerberg 両氏に対し、2023 年 8 月発効のデジタルサービス法（Digital Services Act）を遵守し、それぞれが提供する X（旧 Twitter）と Facebook、Instagram におけるデマの拡散に対処するよう要請した※172（「4.1.3 (1) イスラエル・ハマス間の武力衝突」参照。デジタルサービス法については「2.2.3 (2) (d) データガバナンスに関する規格の運用状況」参照）。

(b) AI の軍事利用や安全性に関する国際的な議論

AI は多方面での利活用に期待がある一方、軍事利用による脅威が懸念されている。2023 年 2 月、オランダで開催された「軍事領域における責任ある AI 利用（REAIM：Responsible Artificial Intelligence in the Military Domain）」サミットでは、AI の責任ある軍事利用について国際的な理解を深めることを目的に議論が行われた。REAIM 宣言では、AI の安全保障上のメリットのみならず課題への理解を深めることの必要性や、将来の議論の継続、及び多様なステークホルダーによる議論の重要性をアピールしつつ、国際法上の義務に従い、国際的な安全保障、安定、説明責任を損なわない、責任ある軍事利用が重要であるとする内容が盛り込まれた※173。米国は、同サミットにおいて、AI の責任ある軍事利用の更なる促進に向けた、国際的な規範形成を目

的とした「AIと自律性の責任ある軍事利用に関する政治宣言」構想を発表し、2023年11月にはBonnie Jenkins米国国務次官(軍備管理・国際安全保障担当)主催により、同政治宣言の初会合を行った。同政治宣言には、日本を含む46ヵ国が参加を表明した※174。

2023年12月、国連総会において、AIが人間の判断を介さずに敵を殺傷する「自律型致死兵器システム(LAWS: Lethal Autonomous Weapon Systems)」※175について、世界の安全保障に与える影響を懸念し、対応が急務だとする決議を日米等152ヵ国の賛成多数で採択した。LAWSに関する総会決議はこれが初めてであり、各国でAIを利用した兵器システムの開発が進む中、具体的な規制につながるか注目される※176。また2024年3月には、スイス・ジュネーブでLAWSの規制を目指す「自律型致死兵器システム(LAWS)に関する政府専門家会合」が開催された。今後3年間で規制対象兵器や法的拘束力等を検討し、成果文書の採択を目指すとしている※177。

軍事利用の議論が進む一方、生成AIの急速な技術革新と普及に伴い、汎用AI技術の安全な開発と使用についても国際的な検討が進んでいる。2023年11月、英国で「AI安全性サミット(AI Safety Summit)」が開催され※178、最先端AIのリスクの理解の促進を図り、国際的に協調した行動を通じて、リスクを軽減する方途等について議論された。Kamala Harris米国副大統領、Ursula von der Leyen欧州委員会委員長、Giorgia Meloni イタリア首相、Justin Trudeau カナダ首相を始めとするG7を含む各国首脳・閣僚級のほか、国際機関、主要なAI企業、有識者等が参加した。岸田文雄首相もオンラインで参加し、2023年5月のG7広島サミットで主導した「広島AIプロセス」の計画について、生成AIを含む高度なAI開発者向けの「広島プロセス国際指針」と「広島プロセス国際行動規範」に合意したことを述べた※179。更に、2024年3月、国連総会においてAIの安全性や信頼性をめぐる決議案が採択された。同決議案は、米国が取りまとめ、日本等120ヵ国以上が共同提案国となった。決議案は、すべての国連加盟国に対し、AI技術の安全性や信頼性を確保するため、規制や管理の枠組み作りに協力して取り組むよう求めているほか、AI技術の利用で各国間の格差を是正するため、途上国を支援すること等を求めている※180。AIの安全性はセキュリティと密接な関係にある。AIの安全性とセキュリティについては「4.2 AIのセキュリティ」を参照いただきたい。

(c)サイバー犯罪に関する国際協力

サイバー犯罪は、犯罪行為の結果が国境を越えて広範な影響を及ぼし得ることから、その防止及び抑制のために国際的に協調して有効な手段を取る必要がある。2021年11月、欧州評議会閣僚委員会は、容易に国境を越えるサイバー犯罪対策のため、他の締約国からより迅速かつ円滑な手続きによる電子的形態の証拠収集を可能にすること等を目的とした「協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書」を採択した。2023年8月、日本も同議定書を受諾した。「ドメイン名の登録情報の開示」「インターネット・サービス・プロバイダが保有する情報の開示」「緊急事態における相互援助及びコンピュータ・データの迅速な開示」等が含まれている※181。

サイバー犯罪に対する国際協力としては、ランサムウェア攻撃グループ「LockBit」の被疑者検挙において、警察庁サイバー特別捜査隊等がEuropolの主導する作戦に参加し、外国捜査機関との国際共同捜査を推進した結果、被疑者逮捕、テイクダウン(同グループが使用するサーバー等の機能停止)が実施された※150「2.1.5(2)(b)(ア)ランサムウェアに対する対処」「2.2.3(2)(c)欧州におけるサイバー脅威と対策の状況」参照)。

(2)日本の国際協力

2023年は、G7広島サミットと日本ASEAN(Association of South East Asian Nations:東南アジア諸国連合)友好協力50周年記念という日本のリーダーシップが問われる節目の年であった。それぞれの概要について述べる。

(a)G7広島サミットとAI関連の国際連携

2023年度のサミットは、5月19～21日、広島にて開催された※182。日本、イタリア、カナダ、フランス、米国、英国、ドイツの7ヵ国首脳並びに欧州理事会議長及び欧州委員会委員長が出席した。そのほか、豪州、ブラジル、コモロ(アフリカ連合議長国)、クック諸島(太平洋諸島フォーラム議長国)、インド(G20議長国)、インドネシア(ASEAN議長国)、韓国、ベトナムの8ヵ国の首脳と国連、国際エネルギー機関(IEA:International Energy Agency)、国際通貨基金(IMF:International Monetary Fund)、経済協力開発機構(OECD:Organisation for Economic Cooperation and Development)、世界銀行、世界保健機関(WHO:World Health Organization)、世界貿易機関(WTO:World Trade Organization)の七つの国際機関の長が招待された。また、21日には

Volodymyr Zelenskyy ウクライナ大統領が訪日し、ウクライナに関するセッションに参加した※183。

2023年5月、「G7広島首脳コミュニケ※184」において、生成AIに関する議論を年内に行うための枠組み「広島AIプロセス」を立ち上げるよう関係閣僚に指示がなされた。2023年12月、G7デジタル・技術担当大臣並びにOECD及びAIに関するグローバル・パートナーシップ（GPAI：Global Partnership on AI）※185は、広島AIプロセスG7デジタル・技術閣僚声明において、「広島AIプロセス包括的政策枠組み」及び「広島AIプロセスを前進させるための作業計画」を取りまとめた。G7首脳はこれらの成果を承認した。そして、AIライフサイクルに関わるあらゆる主体に対して「すべてのAI関係者向けの広島プロセス国際指針」に適宜従うことを奨励し、特に、高度なAIシステムを開発する組織に対して「高度なAIシステムを開発する組織向けの広島プロセス国際行動規範」の履行にコミットすることを求めた※186。

(b) 日本ASEAN友好協力50周年の取り組み

2023年は日本ASEAN友好協力50周年を迎え、日本とASEANの友好関係を更に強固なものとすべく、年間をとおして、日本とASEANの双方において、様々な記念事業や交流事業を実施した※187。

2023年6月には、タイ・バンコクの日・ASEANサイバーセキュリティ能力構築センター（AJCCBC：ASEAN-Japan Cybersecurity Capacity Building Centre）において、国際協力機構（JICA：Japan International Cooperation Agency）の技術協力プロジェクト「サイバーセキュリティとデジタルトラストサービスに関する日ASEAN能力向上プログラム強化プロジェクト」の初回研修の記念セレモニーが開催され、日本から、石月英雄外務省総合外交政策局審議官兼サイバー政策担当大使のほか、総務省、JICAの関係者が、タイから、ティラウット・ワィタヤコーン国家サイバーセキュリティ局副長官がそれぞれ出席した※188。このプロジェクトは、ASEAN地域のサイバーセキュリティ対応能力の強化を図るため、AJCCBCにおけるサイバーセキュリティ・トレーニング、若年層向けサイバーセキュリティ人材開発プログラムの拡大、第三者機関協力によるセミナー等の開催、情報収集・分析能力の強化を図るものである（「2.3.3(1)(d) AJCCBC」参照）。

2023年10月、NISCは、「日ASEANサイバーセキュリティ官民共同フォーラム」を東京で開催した。同フォーラムは、日ASEAN友好50周年を祝し、サイバーセキュリティ関係者のための記念式典として企画された。個々の成果を称える「功労者表彰」と、ASEAN諸国の民間協会団体との連携を強化する「MOU締結式典」等、ASEANの官民協力の価値を共有する場となった※189。

2023年12月、日本ASEAN友好協力50周年特別首脳会議が東京で開催された。岸田首相と2023年のASEAN議長国であるインドネシアのJoko Widodo大統領が共同議長を務め、特別首脳会議の成果文書として、日本ASEAN友好協力に関する共同ビジョン・ステートメント及びその実施計画を採択した※190。共同ビジョン・ステートメントには、「デジタル化、ICTソリューション及びAIに関する協力の推進」や「サイバーセキュリティ並びにテロ、国境を越える犯罪及び偽情報対策等の分野における協力を強化」が記された※191。

これらの記念事業とは別に、2009年より継続している日ASEANサイバーセキュリティ政策会議も2023年10月に開催された。ASEAN加盟国のサイバーセキュリティ関係省庁及び情報通信関係省庁、ASEAN事務局、日本の内閣官房、総務省、外務省、経済産業省の関係者が出席した。第16回となるこの政策会議では、一年間の各国のサイバーセキュリティ政策について意見交換を行ったほか、重要インフラ防護に関する事例の共有、共同意識啓発、能力構築、産学官連携、サイバー演習等の協力活動の実施を確認し、今後の更なる協力活動の在り方についても議論した※37。また、日本ASEAN友好協力50周年記念活動の結果も確認した。

(3) その他の各国・地域との連携強化

日本と二国間、あるいは多国間で行われたその他の連携強化について述べる。

(a) 日米豪印4ヵ国の連携強化

2023年12月、東京で、第3回日米豪印上級サイバーグループ対面会合を行い、日米豪印がサイバー分野で確認した諸原則（国際法の適用、「日米豪印サイバーセキュリティ・パートナーシップ：共同原則※192」等）に対する支持を表明し、「日米豪印上級サイバーグループ共同プレスリリース※193」を行った※194。日本から市川恵一国家安全保障局次長兼内閣官房副長官補、オーストラリアからHamish Hansford内務次官補（サイバー・インフラセキュリティ担当）、インドからMU Nair国家サイバーセキュリティ調整官（中将）、米国からAnne Neuberger国家安全保障担当大統領次席補佐官（サイバー・新興技術担当）が参加した。

(b) 日米の連携強化

2023 年 5 月、外務省で第 8 回日米サイバー対話を開催した。日米両国の政府横断的な取り組みの必要性を踏まえ、日米双方の幅広い関係者が、両国におけるサイバー政策、国際場裡における協力及び二国間協力等、サイバーに関する日米協力について幅広く議論した[※195]。日本から、石月外務省総合外交政策局審議官兼サイバー政策担当大使、外務省、国家安全保障局、NISC、警察庁、公安調査庁、総務省、経済産業省、防衛省を含む関係者が、米国から、Nathaniel Fick 国務省サイバー・デジタル政策局サイバー大使、国務省、国防省を含む関係者がそれぞれ出席した。

(c) 日・NATO の連携強化

2023 年 11 月、ベルギーのブリュッセルで、第 1 回日・NATO サイバー対話を開催し、日本と北大西洋条約機構（NATO：North Atlantic Treaty Organization）の双方のサイバー政策、サイバー分野における今後の協力等の幅広い論点について意見交換を行った[※196]。石月外務省総合外交政策局審議官兼サイバー政策担当大使と David van Weel NATO 事務総長補が共同議長を務め、日本から、外務省、NISC、防衛省の関係者が出席した。

(d) 日・EU の連携強化

2023 年 11 月、ベルギーのブリュッセルで、第 5 回日・EU サイバー対話を開催し、日本と EU の双方のサイバーセキュリティ戦略・政策、日・EU 間及び国連等の多国間の協力、能力構築支援等の幅広い論点について意見交換を行った[※197]。石月外務省総合外交政策局審議官兼サイバー政策担当大使と Joanneke Balfoort 欧州対外活動庁共通安全保障・防衛政策危機管理総局次長が共同議長を務め、日本から、外務省、NISC、警察庁、総務省、経済産業省、防衛省、JPCERT/CC の関係者が、EU から、欧州対外活動庁、欧州委員会及び Europol の関係者がそれぞれ出席した。

(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

2023 年 10 月、米国政府・EU 政府と連携した制御システムのサイバーセキュリティ対策に関するキャパシティビルディングプログラム「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[※198]」を経済産業省と IPA の共催で開催した。これまで新型コロナウイルス感染症の影響によりリモート形式で実施していたが、2023 年度は 4 年ぶりに対面形式で開催した。同プログラムではインド太平洋地域の研修生に対して、工業用プラント等で用いられる水位調整を行う制御システムの模擬プラントや AI を活用したロボットアームを用いて、サイバー攻撃の手口やそれによって起きる事象、攻撃の対処法等を学ぶハンズオン演習を提供した。また、サプライチェーンのリスクマネジメントをテーマにしたセミナーでは、中核人材育成プログラムの修了者が米国の専門家とともにパネルディスカッションに登壇して知見を共有した。

(f) 大洋州島しょ国向けサイバーセキュリティ能力構築演習

政府が掲げる「自由で開かれたインド太平洋」の実現に向けた取り組みの一環として、総務省は、インフラ構築やデジタル化が進み、地理的に重要な位置を占めている大洋州島しょ国（パラオ、ミクロネシア連邦、マーシャル諸島、ナウル、キリバス）からサイバーセキュリティ対策に従事する政府職員及び通信事業者等の重要インフラ事業者の職員を招聘し、2024 年 2 月、米国のグアムにてサイバーセキュリティに関する基礎知識の習得を目的とした研修と実践的サイバー防御演習（CYDER）を含んだサイバーセキュリティ能力構築演習を実施した[※199]（「2.3.3 (1) (b) (イ) CYDER」参照）。

(g) その他の二国間での連携強化

2023 年 6 月、テレビ会議方式で、第 1 回日・ヨルダン・サイバーセキュリティ協議を開催し、両国のサイバーセキュリティ政策、脅威認識等について議論した[※200]。日本から、西永知史外務省中東アフリカ局参事官及び山口勇 NISC 参事官ほかが、ヨルダンからは、Mohammad Khasawneh 王宮府国家政策会議局長ほかが出席した。

2023 年 9 月、外務省で、第 5 回日・インド・サイバー協議を開催し、両国のサイバー政策やサイバーセキュリティ戦略、両国が直面しているサイバー空間の脅威、5G・オープン RAN（Open Radio Access Network）技術の発展について意見交換を行うとともに、能力構築支援関連の二国間協力や国連、日米豪印における協力についても議論した[※201]。日本から、石月外務省総合外交政策局審議官兼サイバー政策担当大使、国家安全保障局、サイバー安全保障体制整備準備室、NISC、警察庁、公安調査庁、総務省、経済産業省、防衛省、JPCERT/CC 等から代表者が、インドから、Muanpuii Saiawi 外務省サイバー外交担当局長、内務省、国家

安全保障会議事務局、電子情報技術省、電気通信局、国家重要情報インフラ保護センター、CERT-In、防衛研究開発機構、国防省、在京インド大使館の代表者が出席した。

2023 年 11 月、フランスで、第 7 回日仏サイバー協議を開催し、両国のサイバーセキュリティ戦略や政策、二国間及び国連等の多国間での協力、能力構築支援等の幅広い論点について意見交換を行った※202。日本から、石月外務省総合外交政策局審議官兼サイバー政策担当大使、外務省、NISC、警察庁、総務省、経済産業省、JPCERT/CC 等の関係者が、フランスから、Henri Verdier 欧州・外務省デジタル大使、欧州・外務省、国家情報システムセキュリティ庁、軍事省、及び内務省の関係者がそれぞれ出席した。

2023 年 12 月、東京で、第 5 回日豪サイバー政策協議を開催し、両国のサイバーセキュリティ戦略や政策、二国間及び国連等の多国間での協力、能力構築支援等の幅広い論点について意見交換を行った※203。日本から、石月外務省総合外交政策局審議官兼サイバー政策担当大使、外務省、NISC、警察庁、総務省、経済産業省、防衛省、JPCERT/CC 等の関係者が、オーストラリアから、Brendan Dowling 外務貿易省サイバー問題・重要技術担当大使、外務貿易省、内務省、豪州通信情報局サイバーキュリティセンターの関係者がそれぞれ出席した。

2.2.2 米国の政策

米国にとって、2023 年は中間選挙と大統領選挙の谷間の年であった。前年の中間選挙では当初予想より共和党の躍進はなく、健闘した民主党は下院の過半数を押さえた。これにより、上院で過半数を占める共和党との間でねじれが発生し、民主党の Joseph Biden 大統領は引き続き、難しい政権運営を強いられている。

そのような中、2023 年 10 月に AI の安全、安心、信頼できる開発と使用に関する大統領令を Biden 大統領が発令したことは、米国のみならず、全世界の IT セキュリティ業界に大きな影響を与えた。

一方、米国の外に目を移すと 2022 年 2 月に始まったロシア・ウクライナ戦争は 2 年以上が経過して膠着状態が深まり、終わりが見えない状況に陥る一方、中東地域ではイスラム組織ハマスによるイスラエル大規模攻撃が勃発する等、グローバル規模での地政学的不安定さが増した。

本項では、これらのグローバルな政治的リスクを見据えながら、かじ取りの困難さが増した 2023 年の米国の政策について述べる。

(1) AI を主とした国家サイバーセキュリティ政策

OpenAI, Inc. が開発した Chat GPT 等の生成 AI の一般利用は 2023 年に急速に拡大した。しかし、その一方で、生成 AI を悪用したフェイクニュース、画像、動画のディープフェイク等が世の中を騒がせた※204。2024 年は今後の世界の動向を左右するような大型選挙が目白押しであり、また、各地での紛争激化も続く見込みであることから AI 利用による偽情報の拡散増大がますます懸念される。

事実、2024 年 1 月 13 日の台湾総統選挙では、AI を悪用した偽動画が拡散した等の報道が相次いだ※205。11 月に控えている米国の大統領選挙等でも国内外からの妨害には予断を許さない。

一方、選挙が AI の偽情報等で妨害されるのを防ぐために Microsoft Corporation、Google LLC、TikTok Ltd. 等 20 社は自主的に連携していくことを合意し、2024 年 2 月、ドイツで開かれたミュンヘン安全保障会議において連名で発表した※206。

以下では、サイバーセキュリティでも注目されている生成 AI 対策を中心に 2023 年 1 月～ 2024 年 2 月に各政府機関で実施された施策、及び Biden 政権が新たに発令した施策について述べる。

(a) 新たな大統領令

2023 年 10 月 30 日、Biden 大統領は AI に関する大統領令である EO 14110（Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence）※207 を発令した。これは、AI を扱うものとしては、Donald Trump 大統領時代の EO 13859※208 と EO 13960※209 に続く、3 番目の大統領令である。同大統領令は、AI 産業における競争の促進、市民の自由と国家安全保障に対する AI 対応の脅威の防止、AI 分野における米国の国際競争力の確保等を規定しており、法的拘束力のある行政措置である。

同大統領令の特徴の一つに、主要な連邦政府機関に対し、最高 AI 責任者（CAIO：Chief AI Officer）の設置を義務付けていることが挙げられる。

また、この大統領令が発令された背景の一つには、生成 AI が誤った情報を拡散することにより、差別を助長したり、場合によっては国家安全保障を損なうケースさ

え発生させたことが挙げられる。一方、米国がAIから潜在的な恩恵を獲得するための規定も含まれる。米国は、これまでのクラウド基盤、各種アプリケーションサービスや情報機器の提供等において世界のIT分野を牽引してきたが、それにAIも加えて、米国の優位性を維持していきたいとの強い意向があり、本大統領令の主な政策目標として、次のような項目を挙げている。

- AI作業における競争とイノベーションの促進
- 公民権と労働者の権利擁護による、AIによる危害からの消費者とそのプライバシーの保護
- AIの調達と使用を管理する連邦政策の特定
- AI生成コンテンツの電子透かしシステム開発による知的財産の盗難の回避
- AIのグローバルリーダーとしての地位を維持

また、同大統領令により、米国商務省（DOC：U.S. Department of Commerce）のNISTは、既存の「AIリスクマネジメントフレームワーク（AI RMF：AI Risk Management Framework）※210」を補完するために、安心かつ安全で信頼できるAIシステムの開発導入に関わる基準やベストプラクティスを策定するよう求められている。

そのほか、同大統領令で注目された具体的内容には、次のようなものがある。

- デュアルユース基盤モデル（dual-use foundation model）の開発者等に対する報告義務
  同モデルは、化学・生物・放射線・核兵器の開発や深刻なサイバー攻撃等、国家安全保障に関わるようなリスクを内包したAIモデルのことである。同モデルの安全性、確実性、信頼性を確保するために、開発者に対し、レッドチームによる一般公開前の安全性テストの結果を連邦政府と共有する義務を課す。
- 生成AIのラベリング等に関するガイダンスの策定
  生成AIのリスクを踏まえながら、AIが生成したコンテンツを識別する能力を高めるため、デジタルコンテンツ承認（digital content authentication）及び生成コンテンツの電子透かしによるラベリング（digital watermarking）等に関するガイダンスを作成することを求める。
- プライバシーの保護
  すべての米国国民のプライバシー保護を強化するため、同大統領令では、プライバシー強化技術（PETs: Privacy Enhancing Technologies）の開発等を連邦政府が支援することを求めている。なお、PETsには、通信経路を隠すためのTor（The Onion Router/Onion Routing）、集計対象となった要素の値や性質を集計結果から推察されにくくする「差分プライバシー」、情報自体は伝えず情報が満たす性質を証明する「ゼロ知識証明」等、広範な分野が含まれる。

（b）AI利用推進の新イニシアティブ

2023年11月1日、Harris副大統領はEO 14110に基づき、「AIの安全かつ、責任ある利用を推進する新イニシアティブ※211」を発表した。その中では、透明性、プライバシー、説明責任、消費者保護等、民主的な価値と利益を反映したAIに関するルールと規範を同盟国やパートナー国とともに確立することをうたい、次の項目に取り組むことを示した。

- 米国AIセーフティ・インスティテュート
  Biden政権はDOCを通じて、NIST内に米国AIセーフティ・インスティテュート（USAISI：U.S. AI Safety Institute）※212を設立する。USAISIは、AIの危険性を評価・軽減するためのガイドライン、ツール、ベンチマーク、ベストプラクティスを作成し、AI利用におけるリスクを特定・軽減する評価を行うことで、NISTのAI RMFを運用する。また、英国のAIセーフティ・インスティテュート等の類似機関との情報共有や研究協力を行い、民間、学界、産業界の外部専門家と連携する。
- AI利用に関する政策指針案
  Biden政権は、米国行政管理予算局（OMB：Office of Management and Budget）を通じて、連邦政府によるAI利用に関する初の政策指針（ガイダンス）案※213をパブリックコメント用に公表した。この政策指針案には、連邦政府における責任あるAIイノベーションの推進、透明性と説明責任の確保、連邦職員の保護、AIの利用時の便益とコストによるリスク管理等の内容が盛り込まれている。
  同政策指針案では、米国政府機関がAIを活用して政府サービスを向上させ、米国国民により公平にサービスを提供できるようにするための取り組みの概要が述べられており、CIO.Govという組織は、その中でも米国の技術系高官向けに最重要ポイントを挙げた「連邦政府テクノロジー・リーダーがOMBのAI政策ドラフトについて知っておくべきことトップ10※214」を公表している。
- AIと自律性の責任ある軍事利用に関する政治宣言
  米国国務省（DOS：U.S. Department of State）は2023年2月に「AIと自律性の責任ある軍事利用に関

する政治宣言（Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy[※215]）」を発表した。本宣言は、世界中の責任ある国家が、自国の軍事・防衛施設への自律的な機能やシステムの導入を含め、責任ある合法的な方法で AI 能力の活用や軍事 AI 能力の責任ある開発・配備・使用に関する規範を確立するためのものである。

- 公益のための AI を推進する資金提供
  米国は、Harris 副大統領の主導のもと、AI 分野において慈善団体との取り組みも推進する。これには、労働者、消費者、地域社会、歴史的に疎外されてきた人々の利益のために設計され、利用される AI を推進するための慈善寄付の構想が含まれている。

(c) 新たなサイバーセキュリティ戦略

Biden 政権は 2023 年 3 月 2 日、「国家サイバーセキュリティ戦略（National Cybersecurity Strategy[※216]）」を公表した。2021 年に発生したランサムウェアによる燃料パイプライン運営会社への攻撃等、重要インフラをターゲットとした事案が後を絶たない中、同政権は安心・安全な社会を実現するための施策の一環として、サイバーセキュリティ戦略を強化してきた。今回の戦略の冒頭では「サイバーセキュリティは経済の基盤的機能、重要インフラの運営、民主主義と民主的制度の強靭さ、個人のデータと通信のプライバシー、国家防衛に不可欠なもの」とうたい、以下の五つの柱を掲げた。

- 重要インフラの防衛
  重要インフラとそれが提供する重要なサービスの可用性とレジリエンスについて、次のような施策により、米国国民に信頼感を与える。
  国家の安全保障と公共の安全を確保するために、重要なセクターにおけるサイバーセキュリティの最小要件の適用を拡大し、規制を調和させてコンプライアンスの負担を軽減する。
  重要インフラと重要なサービスを守るために必要なスピードと規模での官民協働を可能にする。
  連邦ネットワークの防御と近代化、連邦事故対応ポリシーを更新する。
- 脅威ある行動者の破壊と解体
  国力のあらゆる手段を用いて、悪意のあるサイバー攻撃者を、次のような方針で米国の国家安全保障や公共の安全を脅かすことができないようにする。
  敵対者を混乱させるために、あらゆる国力の手段を戦略的に使用しながら、スケーラブルなメカニズムを通じて、民間部門を破壊活動に参加させる。
  ランサムウェアの脅威に対して、連邦政府の包括的なアプローチと国際的なパートナーとの連携により対処する。
- セキュリティとレジリエンスを達成するための市場の力の形成
  デジタルエコシステムをより信頼できるものにするために、リスクを低減し、サイバーセキュリティの不備がもたらす結果を最も脆弱な人々から遠ざけるために、デジタルエコシステム内の最適な立場にある人々に責任を負わせる。そのためには、プライバシー保護や個人データの安全性保護を促進する。また、ソフトウェア製品やサービスに対する責任を転換し、安全な開発慣行を促進し、連邦政府の補助金プログラムが、安全でレジリエンスに優れた新しいインフラへの投資を促す。
- レジリエンスな未来への投資
  戦略的な投資と協調的な行動を通じて、米国は、安全でレジリエンスに優れた次世代技術やインフラの革新において、世界をリードし続ける。インターネットの基盤やデジタルエコシステム全体におけるシステム的な脆弱性を低減し、国境を越えたデジタル抑圧に対するレジリエンスを向上させる。対象分野として、ポスト量子暗号、デジタル ID ソリューション、クリーンエネルギーインフラ等、次世代技術に対するサイバーセキュリティ研究開発を優先する。そのために、多様で強固な国家サイバー人材の育成を行う。
- 共通の目標を達成するための国際的パートナーシップの構築
  米国は、サイバー空間における国家の責任ある行動が期待・強化され、無責任な行動を取る国家、組織は国際社会から孤立し、コストがかかるような世界を求めている。志を同じくする国同士の国際連合やパートナーシップを活用し、共同の準備、対応、コスト賦課を通じて、我々のデジタルエコシステムへの脅威に対抗する。平時と有事の両方で、サイバー脅威から自らを守るためにパートナーの能力を向上させる。情報通信技術や運用技術に関する製品・サービスのグローバルなサプライチェーンを安全、確実、信頼できるものにするために、同盟国やパートナーと協力する。

(d) NIST の施策

NIST は計測を中心とした技術的な標準化とともに、米国政府機関向け規格の策定についても重要な役割を

担っている。ここでは、EO 14110 への対応とサイバーセキュリティフレームワークの改訂について述べる。

（ア）AI に対する米国のスタンスについて

Biden 大統領は EO 14110 の中で「AI は我々の世代を定義する技術であり、我々は AI の力を善のために活用する一方で、そのリスクから人々を守る義務がある。大統領令の一環として、DOC は産業界、学界、市民社会等からの意見を募集し、AI の安心、安全で信頼できる業界標準を策定することで、米国がこの急速に進化する技術の責任ある開発と利用において世界をリードし続けることができるようにする」と明言している。

すなわち、NIST は、幅広い利害関係者が参加するオープンで透明性の高いプロセスを通じてガイダンスを策定すること等により、AI の安心、安全で信頼できる業界標準を策定することを目指している。そこには、「AI と自律性の責任ある軍事利用に関する政治宣言」に示されているように、急速に進化する技術の責任ある開発と利用においても米国が世界を牽引し続けることができるようにしたいという DOS の意向が示されている（「2.2.2（1）（b）AI 利用推進の新イニシアティブ」参照）。

また、EO 14110 では NIST に対し、AI の評価や実際の攻撃者と同じ条件で攻撃を実施するレッドチーム等のガイドラインを策定し、コンセンサスに基づく標準の開発を促進することにより、AI システムの評価のためのテスト環境を提供するよう指示している。そこで、NIST は 2023 年 12 月に情報提供要請書（RFI：Request for Information）※217 を発行した。

NIST では、これらのガイドラインとインフラは、AI の安全で信頼できる開発と責任ある利用において、AI コミュニティを支援するリソースとなると想定している。

（イ）サイバーセキュリティフレームワークの改訂

2024 年 2 月 26 日、NIST はサイバーセキュリティフレームワーク（CSF：Cyber Security Framework）2.0 版を公開した※218。これまで、1.0 版を 2014 年、1.1 版を 2018 年に公開しており、大きな改訂としては 10 年ぶりとなる。主な改訂は以下のとおりである。

- 対象を重要インフラにとどまらないすべての規模や業種の組織での利用に拡大
- 機能（識別（Identify）、防御（Protect）、検知（Detect）、対応（Respond）、復旧（Recover））にあらたに「統治（Govern）」を追加
- サイバーサプライチェーンリスク管理の強化
- 他フレームワークとの整合と実装ガイダンスの紐付け※219
- 実装事例の充実と分野別フレームワークの包含
- CSF に基づく評価事例の充実

CSF は法律や国際標準のような強制力はないが、サイバーセキュリティ対策の枠組みとして多くの組織やガイドライン等で参照されている。今回の改訂で、対象が重要インフラだけでないことが明確に示されたことで、更に利用が拡大することが予想される。

（e）CISA の施策

CISA は EO 14110 を含む Biden 政権のサイバーセキュリティ政策の実装、普及を主導しているが、ここ数年の重点テーマである重要インフラへの攻撃対策、ウクライナへの親ロシア勢力によるサイバー攻撃対策に加え、2023 年は AI も重要テーマとして取り上げられている。

（ア）Roadmap for AI について

2023 年 11 月 14 日、CISA は EO 14110 に基づき、セキュリティ向上のための AI の利用促進や重要インフラ組織への AI 導入支援に関する取り組みを示したドキュメント「CISA Roadmap for Artificial Intelligence※220」（以下、Roadmap for AI）を発表した。

CISA によると、AI システムは従来のソフトウェアとは異なるものの、基本的なセキュリティ慣行は同じように適用され、そのロードマップは、既存のサイバーセキュリティ及びリスク管理プログラムを基礎としている。

Roadmap for AI では、AI を有効活用することによるサイバーセキュリティ能力の強化や、AI システムそのものの脅威からの防御、AI の目標の統一・加速に向けた CISA の次の五つの取り組みも述べられている。

- 責任ある AI の使用
- AI ベースの Secure by Design ソフトウェアの採用
- AI 悪用からの重要インフラの保護
- AI の取り組みに関するパートナーとの協力
- AI ベースのソフトウェアのシステムと技術に関する従業員の教育

（イ）セキュア・バイ・デザインについて

2023 年 10 月 16 日、CISA は日本の NISC 等 17 ヵ国のサイバーセキュリティ組織と共同で、セキュア・バイ・デザインの原則とアプローチに関するガイダンス「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default※221」

の更新版を公開した。

同ガイダンスは、2023年に公表された米国国家サイバーセキュリティ戦略の具体化施策の一つである。

同ガイダンスの公開は、製品セキュリティラベリング制度（「2.2.2 (2) (a) (ア) U.S. Cyber Trust Mark プログラムについて」参照）の国家間相互認証の観点から、製品セキュリティに関する各国の歩調を合わせることを意図している。そして、同ガイダンス更新版の内容は、「EU サイバーレジリエンス法案（EU Cyber Resilience Act）※222」のように製品のセキュリティ確保に向けた各国の国内法令に今後反映される可能性がある。

今回の更新版では、2023年4月に公開された初版における「顧客のセキュリティ課題に当事者意識を持つ」「徹底的な透明性と説明責任を積極的に受容」「経営層のリーダーシップ」の3原則をより詳しく展開しており、すべてのAIシステムに適用できるよう拡張されている。

また、同ガイダンスは、ソフトウェア製造者とその顧客を対象として、それぞれの製品に関して技術的な脆弱性の影響を低減し、組織的な競争力を向上させることを目的に製品セキュリティにおいて講じるべき戦略や方策を提示しており、組織のセキュリティ体制としてあるべき姿が示されている。

なお、CISAの取り組みについては「3.4.3（1）米国CISAの取り組み」も参照されたい。

(2) 米国のその他の国家セキュリティ政策

2023年のセキュリティ関連トピックの中ではAIの存在感が大きかったが、それ以外にも様々な施策が遂行されてきた。ここでは、AI関連以外の2023年を中心とした米国の重要施策の状況を述べる。

(a) EO 14028の実装状況

EO 14028は、2021年5月に発令された「国家のサイバーセキュリティ向上に関する大統領令」であり、本項では同大統領令に基づいて2023年に実施された内容等を紹介する。

(ア) U.S. Cyber Trust Mark プログラムについて

U.S. Cyber Trust Mark プログラム※223は、同大統領令に基づき、2023年7月に発表された。

具体的には、米国人がより安全でサイバー攻撃に対する脆弱性の少ないスマート機器をより簡単に選択できるよう、サイバーセキュリティ認証とラベリングを行うためのプログラムであり、2024年中に開始される見込みである。その一環として、NISTが定めるセキュリティ基準を満たすIoT製品には「U.S. Cyber Trust Mark」が付与される。

なお、当該プログラムを推進することをコミットした企業の中には、LG Electronics U.S.A.やSamsung Electronicsのような製造業者のほか、Amazon.com, Inc.やBest Buyといった流通業者等も含まれている。

(イ) SBOM管理のための推奨事項について

2023年12月、米国の国家安全保障局（NSA：National Security Agency）が「SBOM管理のための推奨事項（Recommendations for Software Bill of Materials（SBOM）Management※224）」を公表した。SBOMは、日本ではソフトウェア部品表とも称され、製品を含むソフトウェアを構成するコンポーネントや互いの依存関係、ライセンスデータ等をリスト化した一覧表である。同表は、オープンソースソフトウェアのライセンス管理や脆弱性の管理、ソフトウェアのサプライチェーンのリスク管理等の用途で活用される。また、大統領令EO 14028において、政府調達におけるSBOM活用の検討指示が明記されたことから、米国規制当局を中心とした取引組織へのSBOM整備の義務化等が進められてきた。

今回の推奨事項は、国家安全保障システム（National Security Systems）を対象に、適切にSBOM管理機能を組み込むことを支援する目的で作成されたものであるが、一般の企業やソフトウェア開発者等にとっても参考になる内容となっている。最新版は2024年1月4日に更新された。

(b) 国防総省のセキュリティ施策

サイバー領域も、陸・海・空・宇宙と並んで米国の防衛を担う米国国防総省（DoD：U.S. Department of Defense）が守るべき領域の一つである。本項では2023年を中心とした同省の施策を述べる。

(ア) サイバー戦略2023について

2023年9月、DoDは「2023年国防総省サイバー戦略（2023 DOD Cyber Strategy）」の要約である「SUMMARY 2023 CYBER STRATEGY of The Department of Defense※225」を公表した。

米国がこれまで実施してきたサイバー作戦の中から得られた教訓に加え、ロシア・ウクライナ戦争でサイバー技術がどのように利用されたかを観察した結果に基づい

て、同戦略が作られたことが示されている。また、同戦略では、同盟国、パートナー、産業界と緊密に協力し、紛争を抑止すること、抑止が失敗した場合でも戦いを続け、勝利するために、適切なサイバー能力、サイバーセキュリティ、サイバーレジリエンスを確保する必要性があることに言及している。

更に国防総省自身のサイバーネットワークとインフラの防御、可用性、信頼性、レジリエンスを確保することに加え、国防総省以外の機関の関連する役割を支援し、防衛産業基盤を保護するための国防総省の行動を強調している。

(イ) CYBERCOM の Under Advisement について

米国サイバー軍（CYBERCOM：U.S. Cyber Command）は、米国軍のサイバー戦を担当する統合軍のことであり、同軍が 2023 年 6 月に発表したアンダーアドバイズ（Under Advisement[※226]）では、民間セクターとの提携による外国の脅威に関する技術情報の共有の拡大が示された。

具体的には、CYBERCOM の活動において発見された新種のマルウェアや IoC（Indicator of Compromise：侵害指標）を民間企業や関係する省庁と迅速に共有し、脅威が米国ネットワークに到達する前に防御の強化につなげること等が挙げられる。関係する省庁には、NSA のサイバーセキュリティコラボレーションセンターや国土安全保障省（DHS：Department of Homeland Security）のサイバー防衛共同体等が含まれる。

(c) 対外施策について

本項では、2023 年のサイバーセキュリティに関する米国の主な対外施策を二つ取り上げる。

(ア) EU- 米国データプライバシーフレームワークについての動き

2023 年 7 月、欧州委員会（EC：European Commission）は、EU から米国への個人データの移転に関し、「EU- 米国データプライバシーフレームワーク（EU-U.S. Data Privacy Framework）」の十分性を認定した[※227]。同フレームワークは、「GDPR（General Data Protection Regulation：EU 一般データ保護規則）[※228]」に基づいており、これにより、EU から同フレームワークに参画する米国企業に、追加のデータ保護措置を講じる必要なく、安全に個人データを移転することができるようになった。

それまで、欧州委員会は米国に対し、GDPR 運用についての十分性認定はしておらず、「プライバシー・シールド」と呼ばれる代替措置を導入していた。しかしながら、EU 司法裁判所は 2020 年 7 月、米国に移転された個人データの米国国内法による保護が不十分として、「プライバシー・シールド」を無効と判断した。これを受け、EU と米国は、「プライバシー・シールド」に代わる新たな枠組みに関する協議を開始した経緯がある。

(イ) 国防権限法

Biden 大統領は 2023 年 12 月 22 日、2024 年の米国議会上院・下院で可決された国防権限法（National Defense Authorization Act for Fiscal Year 2024：NDAA 2024[※229]）に署名した。同法は、米国国防予算の大枠を決めるものであるが、特筆される内容として、アジアで米国軍の態勢強化を目的とする予算は前年度より 3 割近く増やしたことが挙げられる。この背景には長期的に最大の競争相手と見なす中国への対処に重点を置いていることがある。

中国から統一の圧力を受け続けてきた上に、2024 年 1 月 13 日の総統選を控えていた台湾では、同法の可決を受け、外交部は「バイデン米大統領の署名により成立した国防権限法（NDAA2024）では、台湾軍の訓練、指導、組織のキャパシティ・ビルディング構築などを支援する計画や、台湾軍と米軍によるサイバーセキュリティ分野での協力強化など、台湾支援に関する条文が盛り込まれた。これは、安全保障上の台米連携強化を支持するという米国の高いコミットメントと揺るぎない立場を示すものだ。米議会が繰り返し実際の行動をもって、台米安全保障連携の強化と台湾の国防全体の強靭性のために法的根拠や政策のツールを提供していることに外交部は強く感謝する。」とのニュースリリースを発行したという[※230]。

また同法では、地政学上の安定を企図し、インド太平洋地域を対象に地上発射型ミサイルの配備戦略の推進やウクライナやイスラエル支援も引き続き、進めていくことも規定されている。

(ウ) Volt Typhoon に関するサイバーセキュリティ勧告

CISA、NSA、米国連邦捜査局（FBI：Federal Bureau of Investigation）を含む各国の政府機関は、中国の支援を受けたサイバー攻撃者「Volt Typhoon」に関する合同のサイバーセキュリティ勧告（CSA：Cybersecurity Advisory）を 2023 年 5 月 24 日と 2024 年 2 月 7 日に発

表した※231。Volt Typhoon は米国内の重要インフラに侵入することにより、将来の米国との有事の際に重要インフラの機能を妨害することを狙っているという。2月7日に発表された CSA では、Volt Typhoon の活動を軽減するために取るべき行動として、公開されている脆弱性に対する修正プログラムの適用、多要素認証の実装、ログの保管、メーカーのサポート終了への対応計画が挙げられている。

2.2.3 欧州の政策

2023 年度の欧州は、ロシア･ウクライナ戦争の長期化、10 月のイスラエル・ハマス間の武力衝突の勃発による安全保障の課題、経済停滞の深刻化、欧州各国での右翼勢力の台頭等、政治的に不安定な状況となっている。以下ではこのような状況下において、英国と EU 諸国のセキュリティ・データ保護に関する動向について述べる。

(1) 主要国の経済的・社会的混迷

英国では、経済の低迷やルワンダへの不法移民者強制移送を骨子とする移民削減政策への反発※232 により、Rishi Sunak 政権の支持が低迷している。2023 年 8 月、英国のシンクタンクは、EU 離脱による欧州大陸市場との隔絶、ロシア・ウクライナ戦争の影響等が同国に 5 年にわたる「失われた経済成長」をもたらし、富裕層と貧困層の格差を広げていると警告した※233。Sunak 首相には就任当初、経済手腕が期待され、日本が主導する環太平洋パートナーシップ協定（TPP 協定：Trans-Pacific Partnership Agreement）に 2023 年 7 月正式参加※234 する等の独自政策に取り組んでいるが、Brexit による市場分断と地域紛争の影響は長引いている。

フランスでは 2023 年 6 ～ 7 月、警官によるアフリカ系の少年射殺事件を契機として各地で暴動が発生、Emmanuel Macron 大統領は訪独の予定を中止した※235。同事案は、移民労働者を中心とする貧困層の経済格差、差別が背景にあるとされる。更に 2024 年 3 月のイスラム過激派勢力「イスラム国（IS：Islamic State）」によるモスクワ銃撃事件※236 以降、欧州で行われる大規模スポーツイベント（UEFA チャンピオンズリーグ、パリ 2024 オリンピック競技大会等）へのテロ行為に対する不安が大きくなっている※237。

ドイツでは世界的なインフレ、需要低迷の影響から 2023 年度 GDP は前年度比でマイナス 0.3% となった。また 2024 年度の成長見通しも大幅に下方修正され、低迷は長期化する懸念がある※238。こうした中、経済や移民政策に対する Olaf Scholz 政権への不満から、右翼政党 Alternative für Deutschland（AfD）の台頭が懸念されている。「ホロコースト犠牲者を想起する国際デー」にあたる 2024 年 1 月 27 日に Scholz 首相は、台頭する極右過激派による人種主義や反ユダヤ主義再燃への懸念を表明した※239。ドイツはホロコーストの反省から、イスラエル国民への支援を責務としてきたが、現行の反ユダヤ主義の台頭は過去に例を見ないと懸念されている。

反ユダヤ主義は 2023 年 10 月 7 日のイスラエル・ハマス間の武力衝突勃発以降、欧米各国で高まっている。EC は同年 11 月 6 日、「反ユダヤ主義と戦う特使と調整官の共同声明※240」を公表、各国政府・市民にユダヤ人コミュニティを守るよう呼びかけたが、英国の慈善団体によれば、2023 年の反ユダヤヘイト事件は 4,103 件で 2022 年の約 2.5 倍となり、その 3 分の 2 が 10 月 7 日以降であった※241。

以上のように欧州は、地域紛争・経済停滞・差別等による国家・民族間の対立が鮮明となり、不安定な状況となりつつある。こうした対立を扇動する偽情報の拡散や、敵対的国家・組織に支援される勢力によるサイバー攻撃の激化が懸念される。

(2) サイバーセキュリティ政策

欧州のサイバーセキュリティ政策は、欧州ネットワーク・情報セキュリティ機関（ENISA：The European Union Agency for Cybersecurity）が主導し、重要インフラに関する「NIS 指令（Network and Information Systems Directive）※242」の実装、デジタル要素を備えた製品の開発におけるセキュリティ規格「EU サイバーレジリエンス法案※243」の実装を中心として進められている。以下では、これらの施策の最新動向について述べる。

(a) NIS 指令の改訂と実装

EU 域内の重要インフラシステムの統一セキュリティ規格である NIS 指令は、改訂作業が 2022 年中に完了、改訂版は 2023 年 1 月 16 日に NIS2 指令として正式に発効した。NIS2 指令では、重要インフラシステムの多様化、リスク管理の効率化・厳格化等に関して以下のような拡張が行われている。

- 重大エンティティ（essential entity）と呼ぶ基幹サービス分野に行政、下水道、宇宙を追加
- 重要エンティティ（important entity）と呼ぶ分野に郵便、廃棄物処理、化学、食品、製造等を追加

- インシデント等の報告義務の強化
- 違反行為に対する統合的な罰則の強化
- 規則適用対象に関する統一ルールと各国独自拡張ルールの規定
- 金融等の業界規則との整合

EU 加盟国は 2024 年 10 月 17 日までに、国内規定を NIS2 指令に準拠させるよう求められる。

ENISA は、NIS 指令の適用対象となる重大サービス運用者（OES：Operators of Essential Services）、デジタルサービスプロバイダー（DSP：Digital Service Providers）のセキュリティ投資や管理体制について調査を継続しており、2023 年 11 月に報告書の最新版を発行した※244。同報告書では EU 加盟 27 ヵ国の 1,080 社の OES/DSP 企業（各国 40 社）のデータを集計しており、2023 年のセキュリティへの投資が 7.1%であり、前年に比べ 0.4%増加したこと、技術分野ではデータプライバシーへの投資が大きいこと（米国、アジア太平洋地域における投資と比較しての特徴）、運輸セクターの OES の 55% が NIS 指令に基づき投資を強化したこと、OES/DSP 経営層の 81% がサイバーリスク管理手法の承認に関わったこと等の結果が得られている。NIS2 指令による対策拡張の効果については、2024 年度の報告が待たれる。

(b) EU サイバーレジリエンス法案の修正

EC は 2022 年 9 月 15 日、デジタル製品のライフサイクル全般におけるセキュリティ規格「EU サイバーレジリエンス法案（CRA：EU Cyber Resilience Act）」を発表した※243。IoT 機器を含むハードウェア製品、ソフトウェア製品の製造・利用における脆弱性の排除、利用者の製品選定における十分なセキュリティ情報の提供について製造者・配給者の責任を規定するもので、提案は以下の内容を含んでいる。

- デジタル要素を含み、ネットワークに接続されるあらゆる製品が対象であるが、医療・航空・自動車等、既存の法制で要件が規定されている製品は除く。
- デジタル製品のセキュリティリスクレベルを「重要デジタル製品：クラスⅡ（高リスク）」「重要デジタル製品：クラスⅠ（低リスク）」「それ以外の製品」の 3 レベルに分け、レベルに応じたセキュリティ適合性評価を行う。高リスク製品には OS、CPU、産業用ファイアウォール等、低リスク製品にはルーター、VPN 等、それ以外の製品には HDD、スマートアシスタント、ゲーム機等、市場の 90%の製品が含まれるとされる※245。
- 重要デジタル製品のクラスⅡ全製品、クラスⅠの一部製品には第三者による適合性評価（第三者認証）を必須とする。適合性評価機関（認証機関）の選定と監査は加盟国が行う。
- 設計・製造時のセキュリティリスク評価、顧客への情報提供、脆弱性対応支援を必須とし、サプライチェーン上の関係者とその役割を分担する。
- 製品に、積極的に悪用された脆弱性が発覚した場合は 24 時間以内に ENISA に報告する。
- 法案の運用は、加盟国が指定する市場監視局が監視する。市場監視局は、重大なセキュリティリスクが想定される製品の適合性評価を実施し、要件を満たさない製品の是正、回収措置等を命じる。対応によっては製造者に制裁金が課される※246。
- 重要デジタル製品リストの更新、法案の実装における詳細項目等の規定は EC が代行する。後者の詳細規定には、SBOM の利用等を含む。

同法案は「あらゆる重要なデジタル製品」が対象であり、IoT 関連製品・サービスに関する様々な分野に影響を及ぼし得るため、欧州の消費者団体が賛同の意見を表明※247した一方、製品・サービス分野ごとの適合性評価の設計とコスト、加盟国の準備体制等に対する懸念も想定された。上流工程の OSS 開発者が下流の（他で開発された）OSS の脆弱性対応や製造責任・賠償責任を負うという CRA の要求に対して、特に OSS コミュニティは「手弁当でメンテナンスしている開発者を悪者にする」「OSS 開発を制限しかねない」といった懸念や、多くの反対意見を表明した※248。

EC もこれに配慮し、CRA の修正を行った。主要な点は「商用のオープンソース開発においてもセキュリティに対し相応の責任を持つ」という責任分担の考え方、体制上はセキュリティ責任を担保する OSS 管理者という主体（非営利団体を含む）の導入である。OSS 管理者は最終的なデジタル製品製造者ではなく、商用の OSS がセキュアかつ機能的であることを維持管理する役割を負う。その役割には OSS の脆弱性管理・修正プログラム更新、CRA のセキュリティ要件遵守が含まれる。

OSS 管理者の存在を前提とする修正 CRA 法案は 2023 年 12 月 1 日、欧州議会（European Parliament）で承認された※249。また OSS コミュニティ 7 団体も 2024 年 4 月、CRA を支持し、CRA の求めるセキュリティ基準に沿った開発プロセスのベストプラクティスの共通化で

協力すると表明した※250。欧州議会・ECによる最終承認・施行は2024年夏、事業者の対応完了(完全実施)は36ヵ月後の2027年夏と想定される。改正されたCRAはOSSコミュニティの反発にかなり配慮した内容となったが、OSSコミュニティやサプライチェーンのセキュリティ対策にどのような影響があるか、未知の部分がある。今後のデジタル製品開発者の対応が注目される。

(c)欧州におけるサイバー脅威と対策の状況

2023年10月、ENISAはサイバーセキュリティ脅威の概況に関する年報を公開した※251。2022年後半から2023年前半までの主要な脅威として以下が挙げられている。

- 暗号化、情報窃取等の多重脅迫(multiple extortion)の手法によるランサムウェア攻撃が最大で、ENISAの分析対象事案の31.3%(約1,480件)を占める。
- ランサムウェアの攻撃者としてロシア系の攻撃グループ「LockBit」が突出し、欧州のランサムウェア分析事案の56.6%を占める。日本国内でも2023年7月の名古屋港のランサムウェア被害※252はLockBitによるとされている※253(「1.2.1(2)(a)港湾事務所における被害事例」参照)。
- 他の主要な脅威としてDoS攻撃(分析事案の21.4%、約1,010件)、データ窃取・漏えい(分析事案の20.1%、約950件)が続く。
- 攻撃の巧妙化(正規ツールの悪用等)・複合化、サービス化が進んでいる。初期侵入の手口としてフィッシングが再度用いられている。
- 一方で地政学的理由(ロシア・ウクライナ戦争等)による攻撃が増えている。必ずしも攻撃に巧妙さはなく、虚偽情報を交えた情報戦が多くなっている。
- 生成AIによる虚偽情報拡散が新たな懸念となっている(虚偽情報の脅威については「4.1 虚偽を含む情報拡散の脅威と対策の動向」、AIセキュリティについては「4.2 AIのセキュリティ」参照)。

以上の脅威のうちランサムウェアについて、Europolは国際連携活動(No More Ransom※254)を主導してきたが、2024年2月、ランサムウェア攻撃グループ「LockBit」に対する一斉摘発を行った※255。この摘発では約10ヵ国が捜査に協力し、サーバー34台を差し押さえたほかLockBitのメンバー2名を逮捕、200口座以上、1万4,000以上のアカウントを閉鎖した。LockBitはこれで大きな打撃を受けたかに見えたが、直後に病院を攻撃する等のしたたかさを見せている※256。ランサムウェアには引き続き警戒と対策が必要である。

(d)データガバナンスに関する規格の運用状況

ECのデジタルデータ戦略では、欧州がデータ駆動型社会をリードし、域内の自由なデータ流通、公平・公正なデータアクセスによる単一デジタルデータ市場を確立するとしている※257。これに基づきECは、デジタルデータの保護と公平・公正な流通のための規格として、以下のような法制を整備している。

- 公平なデータへのアクセス及び利用実現のためのデータ法(Data Act)※258。2024年1月11日に施行された。
- 公共団体の保有する一部データの機密性・プライバシーを保護し、研究開発等における安全な再利用を規定するデータガバナンス法(Data Governance Act)※259。2022年6月23日に発効、猶予期間を経た2023年9月24日に施行された。
- 大規模オンラインプラットフォーム事業者(以下、gatekeeper)の商慣行を公平・公正な競争の視点で規制するデジタル市場法(Digital Markets Act、以下DMA)※260。2022年11月1日に発効、2023年5月2日に施行された。
- gatekeeperのコンテンツ配信、情報開示、契約の透明性等に対する責任を規定するデジタルサービス法(DSA:Digital Services Act)※261。2023年8月末から一部の大規模gatekeeperに対して施行され、2024年2月17日から全面的に施行された。DSAは虚偽情報等の配信に対する規制となるため、サイバーセキュリティ対策との関わりが深い。

これらの法制は、それまでgatekeeperが独占的に決定していたデジタル市場の参入・統制の枠組みを再編するものである。gatekeeperに指定されたプラットフォーム事業者には厳しい要請や罰則が課され、ECがこれらの制度をどこまで厳格に運用するのかが注目される。2024年4月時点で、以下のような制度適用例が公開されている。

- Xの違法コンテンツ拡散等に対する調査
  2023年12月18日、ECはリスク管理、投稿監視、透明性等に関するDSA違反の疑いでX Corp.(以下、X社)への正式調査を開始した※262。ECは、同社のSNSサービスXにおいて、ハマスのイスラエル攻撃に関する違法コンテンツ拡散等への対応、情報操作対抗機能(Community Notes)の有効性、プ

ラットフォームへのアクセスの透明性等が不十分な可能性があるとし、調査対象とした。EC の X 社への事前調査は 2023 年 9 月時点で始まっていたが、ハマスのイスラエル攻撃に関する虚偽情報拡散もこれに重なった。

- TikTok の子供の保護等に関する調査
  2024 年 2 月 19 日、EC は子供の保護、透明性、データアクセス等に関する DSA 違反の疑いで TikToK Pte. Ltd.（以下、TikTok 社）への正式調査を開始した[※263]。EC は、動画 SNS サービス TikTok において、サービスの推奨アルゴリズムによって過激なコンテンツを子供が視聴し続けてしまうこと（ウサギの穴効果）の負の影響、年少者に対する年齢チェック機能の有効性、子供のプライバシー保護対応、プラットフォームへのアクセスの透明性等が不十分な可能性があるとし、調査対象とした。TikTok はプラットフォームを利用する若者の安全を守るために引き続き専門家や業界と協力するとしている[※264]。しかし EC は 2024 年 4 月 22 日、TikTok の視聴者に報酬を与える新サービス TikTok Lite が未成年には「中毒性がある」とし、サービス停止の可能性を含め調査を開始するとし[※265]、規制を強めている（子供の個人情報保護については「2.2.3（3）（b）高額な制裁事案の傾向」参照）。
- gatekeerper の DMA 違反に関する調査
  2024 年 3 月 25 日、EC は gatekeeper である Alphabet Inc.、Apple Inc.、Meta Platforms, Inc.（以下、Meta 社）に対して DMA 違反の疑いで調査を開始するとした[※266]。調査内容は、Alphabet Inc. については Google 検索の結果が自社サービスに有利に利用される（self-preference）点、Apple Inc. については iOS 利用者がアプリ選択や設定変更を容易に行えない点、Meta 社については、サービス間で個人情報を統合する場合の利用者の同意の取り方に不公平がある点等に関するものである。
  域内市場の公平・公正なサービス提供について、EU は DMA に先立ち、gatekeeper の反トラスト行為・不正競争行為を EU 競争法に基づき監視してきた。例えば EC は 2024 年 3 月 4 日、Apple Inc. に対して、iOS 上の音楽ストリーム配信ビジネスにおける優越的な立場を乱用し、公正な競争を妨害したとして 18 億ユーロを超える制裁金を課した[※267]。EU 競争法と DMA は一見重複するように感じられるが、EU 競争法は事後対応で IT サービスの変化に合わない、無償というデジタルサービスの特性に合わない[※268] 等の問題があり、DMA はいち早くこれに対応したとされる。今後の適用が注目される。

（e）AI 法の成立と実装準備

2021 年以来、EC が提案・修正を重ねてきた AI の安全で遵法的な利用に関する規則（Artificial Intelligence Act、以下 AI 法）[※269] は、2024 年 3 月 13 日、欧州議会にて承認された[※270]。当初は 2023 年中の承認が想定されたが、2023 年に急速に普及した生成 AI の規制方針、過度の規制は米国に対して不利になるとする民間事業者・団体、加盟国との調整等が難航し、2023 年 12 月に 3 日間の議論を経て暫定合意された[※271] 後、2024 年 3 月に以下の修正が加えられ、最終承認となった。

- 汎用目的 AI（GPAI：General-purpose artificial intelligence）の規定
- 法執行機関のリアルタイム生体識別利用に関する制限
- 利用禁止 AI のカテゴリ追加（インターネット・監視カメラ映像からの顔認証等）
- AI 利用者の権限の拡張（苦情申し立て、説明を受ける権利等）

このうち GPAI の規定は、実質的に生成 AI の規定である。GPAI のリスクが AI 法の規定する「ハイリスク」（人の安全、人権、経済等の被害をもたらすリスクで、AI サービスベンダーにリスク低減の義務が生じる）であるか、特に影響が広範囲に波及する GPAI モデル（ChatGPT 等）のリスクをどう見るかが焦点となった。その結果としては、一段下の「限定リスク」（AI サービスベンダーに AI を利用していることを開示する義務が生じる）の規定である透明性の要件を課し、リスクが広範囲に及ぶことが想定される GPAI については追加の要件を課すこととなった。この透明性には訓練データのサマリー情報の開示、EU 著作権法の遵守、生成コンテンツが AI によることを示すラベル付与（フェイク利用の抑止）等が含まれる。すべての訓練データのサマリー情報作成の実行可能性、コンテンツラベル付与の方式や有効性（ラベル削除の困難性等）は未知数であり、更なる検討が必要と思われる。なお、AI 法のリスクベースモデル（四つのリスクレベルと対応する規定）の概要は、「情報セキュリティ白書 2023」の「2.2.3（3）（e）AI 法の策定」を参照されたい。

一方、安全性の問題（公平性・人権等の問題を含む）がサービスバリューチェーン全体に広範囲に波及するリスク（systemic risk）のある GPAI モデルについては、当該リスクのアセスメントと低減、GPAI モデルの評価テス

ト実施、インシデント監視等の規定が追加された。また systemic risk の分類については、フランスが厳しい要件を緩和するよう主張した結果、毎年見直されることとなった。

実装の問題に関連して、EC は 2024 年 1 月、AI 法の実施を統括する機関として欧州 AI 事務所（European AI Office）を設置した※272。同事務所は EU における信頼に足る AI（Trustworthy AI）実装のセンターであり、加盟国における AI 法実践を統括する。GPAI 関連規定の実践については GPAI モデル開発者を監督し、必要な制裁も行うとしている※273。米国、英国、日本等では、信頼に足る AI 実装のため、AI の安全性を開発者側から統制する AI セーフティ・インスティテュート（AISI：AI Safety Institute）の設置発表が相次いでいる※274（「4.2 AI のセキュリティ」参照）。EC の欧州 AI 事務所の設置、及び同時期に発表した AI 関連のスタートアップ・中小企業の支援イニシアティブ「GenAI4EU」の設置※275 は、AISI と同様な目的であると見られるが、欧州 AI 事務所は法的強制力を持ち、EU 全体の GDPR の実施状況を監督する欧州データ保護委員会（EDPB：European Data Protection Board）のような位置付けになると想定される。

欧州議会で承認された AI 法は、今後加盟各国及び欧州評議会（European Council）の承認を経て 2024 年中に正式発効、24 ヵ月後（2026 年）に完全運用が見込まれる。なお、禁止される AI（政府による個人の格付け、高齢・障害等による個人の脆弱性の搾取等、リスク分類で「許容できない AI」に区分される AI）の規制は発効の 6 ヵ月後に運用が開始される等、一部の規制の運用は実施が早まるとされている※276。

(3) GDPR の運用状況

GDPR は 2022 年より厳格な運用が開始され、2023 年もそれが継続している。

(a) GDPR 違反の概況

国際法律事務所 DLA Piper の調査によれば、2023 年 1 月 28 日から 2024 年 1 月 17 日までの GDPR 違反の制裁金総額は約 17.8 億ユーロで、2022 年 1 月 28 日から 2023 年 1 月 25 日の間の制裁金総額の 14% 増であった※277。2022 年から、EU 各国のデータ保護機関（DPA：Data Protection Authority）が高額制裁に躊躇しなくなり、2021 年から総額は 1.5 倍に跳ね上がった。2023 年は引き続き高止まり傾向にあるといえる。制裁の根拠は合法性・公平性・透明性等の GDPR の基本原則違反が最も多い。

国別の制裁金額では、2022 年度に引き続きプラットフォーマー（gatekeeper）等の EU 拠点が多いアイルランドが首位、ルクセンブルクが続いている。アイルランドデータ保護機関 Data Protection Commission（DPC）は GDPR の主要な高額制裁を科す主体となっているが、アイルランド、EU 双方で控訴に持ち込まれる未解決事案が増えている。違反届出件数については、2023 年 1 月 28 日 ～ 2024 年 1 月 27 日は 1 日平均 335 件で、2022 年～ 2023 年の同時期の 1 日平均 328 件とほぼ同等である。国別ではドイツ、オランダ、ポーランドの順に多い。

(b) 高額な制裁事案の傾向

2023 年の高額な制裁事案としては以下がある。

- 2023 年 1 月 4 日、アイルランド DPC は、Meta 社に対し、Facebook、Instagram におけるターゲティング広告に関する個人データ利用の同意手続きが不透明である等の不備が GDPR 違反にあたるとして合計 3 億 9,000 万ユーロの制裁金を科し、更に同社の業務プロセスを 3 ヵ月以内に改善するよう命じた※278。
- 2023 年 4 月 4 日、英国データ保護機関 Information Commissioner's Office（ICO）は、TikTok 社に対し、13 歳以下の 100 万人以上の子供が親の同意を得ずに TikTok を利用し、それらのデータを削除する機能を提供していないこと、また利用者データの収集・利用に関する情報を提供していないことが GDPR 違反にあたるとして、1,450 万ユーロの制裁金を科した※279。
- 2023 年 5 月 12 日、アイルランド DPC は Meta 社に対し、欧州から米国への個人データ移転に伴う Meta 社独自の追加保護処理が米国国内法の不備を補填できておらず GDPR 違反にあたるとして、12 億ユーロの制裁金を科した※280。制裁金額はアイルランド DPC の監督機関である EDPB の「被害の深刻さに合わせる」との要請で修正され、GDPR 違反としては過去最高額である。Meta 社は、他の個人データ移転を行う事業者と同等の欧州標準契約条項（SCC：Standard Contractual Clause）に準拠しているのに制裁は不適切・不公平であると反論、提訴するとした※281。こうした厳しい制裁は、米国諜報機関の移転データに対する監視への不安が背景にあると考えられる。
- 2023 年 6 月 15 日、フランスデータ保護機関

Commission Nationale de l'Informatique et des Libertés（CNIL）は、コマースマーケティング企業 Criteo S.A. に対し、同社のクッキーを用いた個人向け追跡広告を利用するパートナーによるインターネット利用者からのデータトラッキング許諾ができていない、Criteo S.A. のプライバシーポリシーや顧客情報利用規定が不十分である、利用者のデータ削除要請に対応できていない等が GDPR 違反にあたるとして、4,000 万ユーロの制裁金を科した※282。

- 2023 年 9 月 1 日、アイルランド DPC は、TikTok 社に対し、TikTok の子供の投稿や個人情報の開示制限、開示した情報の利用に関する情報提供に不備がある、プライバシーが保護されない操作への誘導（ダークパターン）がある等が GDPR 違反にあたるとして 3 億 4,500 万ユーロの制裁金を科した※283。また、3 ヵ月以内に TikTok の処理を GDPR に準拠させるよう命じた。前掲のとおり、TikTok の子供の利用に関しては ICO も制裁を課し、EC が中毒性があるとして TikTok Lite サービス停止の可能性を含めた調査を開始する等、厳しい対応が続いている。

以上のように、高額な GDPR 違反制裁は先のデジタルデータガバナンス法制運用とともに、gatekeeper の市場独占による公平性の問題を排除し、EU 市民の権利と EU 事業者の競争力を確保する手段としての利用が鮮明になりつつある。欧州のサイバーセキュリティ政策、AI 法の運用もこの流れの中に位置付けて見ていく必要がある。

2.2.4 アジア太平洋地域でのCSIRTの動向

インシデント対応や脅威情報の伝達・公開等、情報セキュリティ対策活動の向上に取り組む各国の National CSIRT（以下、CSIRT）は、あらゆるサイバー攻撃の脅威に備えて自国におけるインシデント対応の迅速化や効率化、サイバーセキュリティ人材の能力構築、情報連携の強化等、様々な課題に取り組んでいる。それに加えて、国外のパートナーとの脅威情報の共有や技術交流を行う等、国際連携を通じた地域のサイバーセキュリティ能力の強化に取り組んでいる。本項では、主にアジア太平洋地域における CSIRT の機能強化やインシデント対応への取り組み、CSIRT 間の相互連携の実態について述べる。

(1) CSIRT の機能強化の動き

アジア太平洋地域における各国・地域の CSIRT の機能強化やインシデント対応への取り組みについて述べる。

(a) オーストラリア

2023 年 11 月 22 日、オーストラリア連邦政府が「2023 ～ 2030 年サイバーセキュリティ戦略（2023-2030 Australian Cyber Security Strategy）※284」と「実施計画（Action Plan）※285」を発表した。同戦略は、2030 年までにサイバーセキュリティ分野において自らが世界のリーダーになるというビジョンを実現するための道筋を、企業及び市民のサイバーセキュリティ能力強化、技術分野のセキュリティ強化、世界水準の脅威情報共有と防御等の六つのテーマごとに示している。企業及び市民のサイバーセキュリティ能力強化の項目では、インシデント対応に関して、企業がインシデント報告を単一のポータルサイトで簡潔に行える仕組みを整えることや、政府へ報告されたインシデント情報の用途を明確にする等、企業の不安を払しょくし、官民の迅速な情報共有と対応支援を促進するための規則作りを検討することを具体的な目標として挙げている。これらのインシデント対応強化の取り組みは、内務省（Home Affairs）が主導し、National CSIRT の機能を担う ACSC（Australian Cyber security Centre：オーストラリアサイバーセキュリティセンター）の上位組織である ASD（Australian Signals Directorate：オーストラリア信号局）等多数の政府機関が携わり進めていくとしている。また、目標の一つに企業向けサイバーセキュリティガイダンスの提供を挙げており、ACSC 等が連携して、サイバーセキュリティ関連の義務要件を分かりやすくまとめるとしている。そのほか、大規模なインシデント発生後にインシデント対応の評価を行うサイバーインシデント審議委員会を新設し、同委員会での議論により得られた教訓を社会に広く共有することで、国の脅威情報共有やインシデント対応、サイバー意識向上プログラムの改善等につなげていくとしている。

(b) ニュージーランド

2023 年 8 月 31 日、GCSB（Government Communications Security Bureau：政府通信保安局）が、CERT NZ（Computer Emergency Response Team New Zealand：ニュージーランドコンピュータ緊急対応チーム）を NCSC（National Cyber Security Centre：国家サイバーセキュリティセンター）に統合すると発表した※286。両組織の統合は、数年かけて段階的

に行われる。CERT NZはビジネス・イノベーション・雇用省傘下のサイバーセキュリティ機関として2017年に設置されて以来、国内の企業や個人等にセキュリティ関連情報を提供し、インシデント対応のサポートを行ってきた。一方、NCSCは情報機関であるGCSB傘下に置かれ、政府最高情報セキュリティ責任者(GCISO:Government Chief Information Security Officer)を擁する組織であり、重要組織への脅威の検出や対応、予防的対策の助言、機密情報の保護等、幅広いサイバーセキュリティ業務を担っている。発表によれば、CERT NZがNCSCに統合された後も、両組織の現行の機能とサービスは継続されるが、単一のサイバーセキュリティ機関として、今後双方の専門知識を活用し、あらゆる脅威レベルのインシデントに対応するための体制と能力の強化を目指すとしている。

(c)インド

2023年6月30日、CERT-In(Indian Computer Emergency Response Team:インドコンピュータ緊急対応チーム)が「政府機関に向けた情報セキュリティの実践に関するガイドライン(Guidelines on Information Security Practices for Government Entities)」を発表した※287。同ガイドラインは、政府機関及びその関連組織内におけるサイバーセキュリティ対策と管理に必要な基本的要件を実装するための指針を示している。例えば、組織の上級管理者はCISOを任命する必要があること、CISOはIT運用チームやインフラストラクチャの構築チームとは別に専任のサイバーセキュリティチームを設置する必要があること、また専任チームが担うインシデント対応やセキュリティポリシーの策定等の役割を定めている。サイバーセキュリティ対策の要件については、ネットワークセキュリティ、アプリケーションセキュリティ、データセキュリティ、及び脆弱性とセキュリティ修正プログラムの管理等の項目ごとに要件が整理されている。そのほか、ガイドラインで提示しているセキュリティ要件を満たしているか確認するためのチェックリストが付録に含まれており、内部や外部の監査人を含む監査チームが、組織のセキュリティ体制を評価する際に役立つものとなっている。また、日々変化する脅威状況を踏まえ、CERT-Inが内容の見直しと更新を行うとしている。

(d)シンガポール

2023年10月17日、SingCERT(Singapore Computer Emergency Response Team:シンガポールコンピュータ緊急対応チーム)を管轄するCSA(Cyber Security Agency of Singapore:シンガポールサイバーセキュリティ庁)が、サイバーセキュリティ人材を育成するプログラムSG Cyber Associatesを立ち上げたと発表した※288。同プログラムを立ち上げた背景には、急速なデジタル化と増大するサイバーセキュリティの脅威に対応するスキルの向上が求められている一方で、スキルや対応体制が不十分な産業セクターや中小企業が依然として存在している現状がある。このギャップを埋めるため、サイバーセキュリティの専門家以外の人々に対し、仕事に関連したサイバーセキュリティスキルを身につけることができる、基礎的かつ特定のテーマに焦点を当てたトレーニングを提供するとしている。基礎的なトレーニングに関しては、入門レベルのサイバーセキュリティ関連認定資格の取得を希望する者を対象としたプログラムを、サイバーセキュリティ専門家のトレーニングと資格認定を専門とする非営利組織ISC2(International Information System Security Certification Consortium:国際情報システムセキュリティ認定コンソーシアム)と連携して提供し、サイバーセキュリティに携わる人材の幅を広げ、サイバーセキュリティ労働力の全体的な能力を向上させることを目指す。また、対象を絞った特定のテーマに関するトレーニングに関しては、法律の専門家や監査人等に、サイバーリスク及びデータセキュリティ等の問題について理解を深めてもらうプログラムを提供することで、ランサムウェア等のサイバー犯罪に対応する企業のリスク管理支援に携わる専門家の能力を強化したいとしている。また、IT及びソフトウェア分野のプロジェクトマネージャーや開発者等に、開発の初期段階から安全な製品やサービスをつくるためのサイバーセキュリティスキルを身につけてもらうプログラムを提供するとしている。こうした特定のテーマに関するトレーニングは、CSAがIES(Institution of Engineers Singapore:シンガポール技術者協会)等の専門機関と協力し、特定のニーズを満たすカスタマイズされたプログラムを開発し、提供するとしており、まずは、IES会員向けにIoTセキュリティ等の技術領域に関するコースを開発することを計画している。CSAは、今後より多くの専門機関やパートナーと協力し、SG Cyber Associatesのトレーニングプログラムを拡大していくと述べている。

(e)台湾

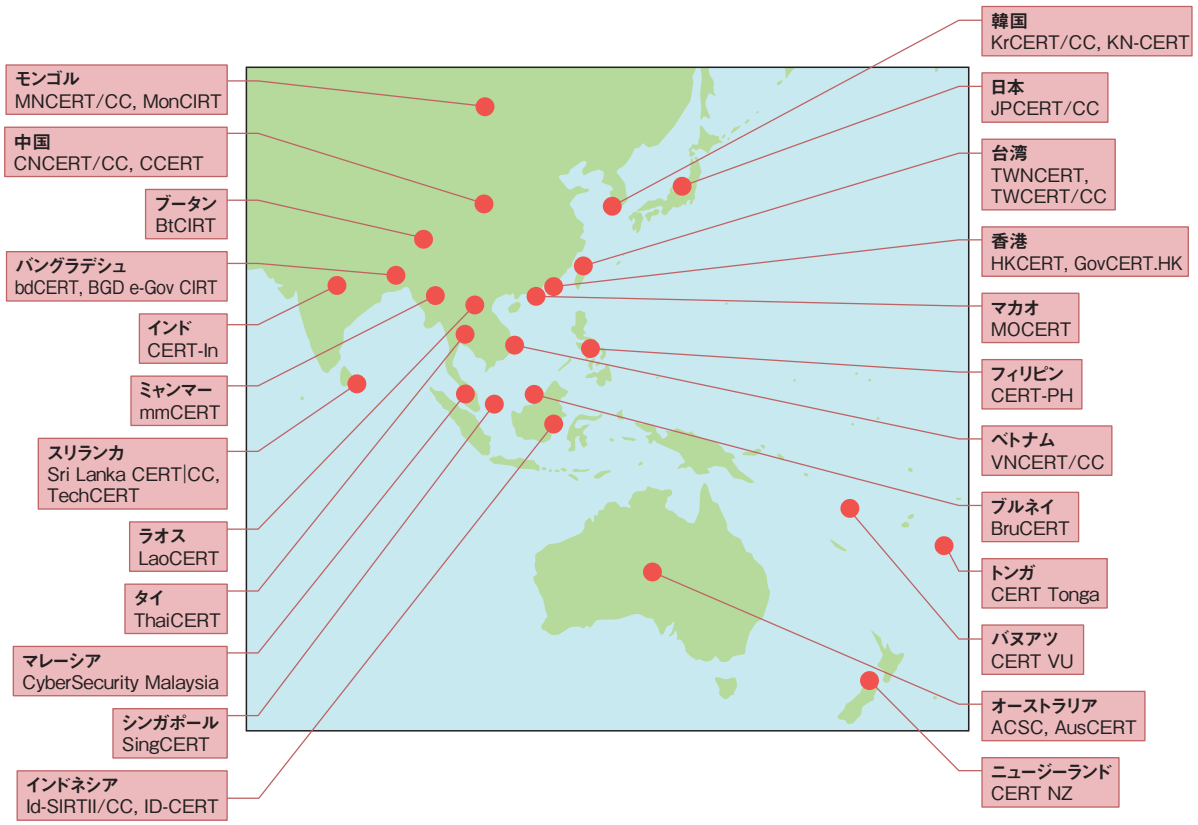
2023年1月1日、MODA(Ministry of Digital Affairs:デジタル発展省)傘下に、台湾のサイバーセキュリティ関連業務を担う行政法人NICS(National

Institute of Cyber Security：国家サイバーセキュリティ研究院）が設立された※289。台湾のサイバーセキュリティ政策の策定を担うMODAと、政策の推進を担うACS（Administration for Cyber Security：サイバーセキュリティ管理局）とともに、サイバーセキュリティ技術機関としてサイバーセキュリティ対策の強化を目指す。組織を紹介する資料※290によるとNICSの主な役割として、台湾における情報セキュリティ技術の研究開発及び普及、政府機関や重要インフラにおける重大なセキュリティインシデントの対応支援及び防護、セキュリティ人材の育成、国際的な技術交流・協力の推進等が挙げられている。また、CSIRT組織のインシデント報告の仕組みを統合し、インシデント報告と対応の効率化を図ることが組織の中期発展計画に盛り込まれている。台湾には政府機関のインシデント対応を行うTWNCERT（Taiwan National Computer Emergency Response Team）と民間組織のインシデント対応を行うTWCERT/CC（Taiwan Computer Emergency Response Team/Coordination Center）があり、今後これらの組織は、組織編制や運用の改善を行っていくと見られる。同年1月10日に行われた開所式には、蔡英文総統（当時）やオードリー・タンデジタル発展相（当時）が出席し、蔡総統はその場でNICSは産業界や学術研究機関から最も優秀な人材を集めたセキュリティ研究機関として、全力で情報セキュリティ技術の研究開発や、重要インフラと情報システムの防護能力の向上に努めることになっていると述べている※291。

(2) アジア太平洋地域のCSIRT間連携

アジア太平洋地域全体のCSIRTからなるコミュニティとして、APCERT（Asia Pacific Computer Emergency Response Team:アジア太平洋コンピュータ緊急対応チーム）※292があり、地域内で発生したインシデント対応における連携の円滑化や、サイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。2003年の設立当初、参加メンバーは12の国･経済地域の15チームだったが、地域内でCSIRTの立ち上げが進んだことや、CSIRTコミュニティへの参加を通じた情報共有等の重要性が高まったことから年々メンバーが増えている。2024年3月末現在、24の国･経済地域の33チームが、オペレーショナルメンバーとなっている（図2-2-1）。

JPCERT/CCは、2003年のAPCERT設立当初から事務局を務め、運営委員会の一員として組織運営を支えている。APCERTの主な活動は、年次サイバー演習の実施、年次報告書の発行及び年次会合の開催である。



■図2-2-1　APCERTオペレーショナルメンバー（2024年3月末現在）
（出典）APCERT「Member Teams※293」を基にIPAが編集

2023年のサイバー演習は、「Digital Supply Chain Redemption（デジタルサプライチェーンの救済）」をテーマに実施された※294。同演習には、APCERTのオペレーショナルメンバーのうち合計21の国・経済地域から24チームが参加した。年次報告書は、APCERT全体の活動に加えて各チームの組織概要や、対応したインシデント統計等をまとめた文書で、Webサイトで公開されている※295。2023年のAPCERT年次会合は、前回に引き続き11月にオンラインで開催された。韓国のKrCERT/CC※296が議長に、マレーシアのCyberSecurity Malaysia※297が副議長に、JPCERT/CCが事務局に、CyberSecurity Malaysia、Sri Lanka CERT| CC（Sri Lanka Computer Emergency Readiness Team | Coordination Centre）※298、JPCERT/CCが運営委員にそれぞれ再選された。

APCERTでは能力開発の取り組みとして、電話会議システムを利用して、インシデント対応に関するノウハウを教えるオンライントレーニングを2014年以来継続している。こうしたオンラインで連携する取り組みを継続することで、加盟組織間の交流を深めている。更に、脆弱性情報の調整や公表に関して各国CERT間のノウハウ共有や能力構築を目的としたワーキンググループ（Coordinated Vulnerability Disclosure WG）が新たに設立され、JPCERT/CCがリード役を務めている。

そのほか、この地域におけるCSIRT間連携については、2023年12月17日に日本ASEAN友好協力50周年特別首脳会議※190で採択された「日本ASEAN友好協力に関する共同ビジョン・ステートメント2023」の実施計画※299に「ASEANサイバーセキュリティ協力戦略2021-2025に沿ってコンピュータ緊急対応チーム（CERT）の連携促進」を行うとの記載があり、地域のサイバーセキュリティ分野における協力を強化する取り組みの一環として、CSIRT間連携の促進が盛り込まれている。

このように、アジア太平洋地域の各国におけるCSIRTの機能強化に加えて、APCERTやASEAN等の国際的な団体が、CSIRTの活動を後押しする取り組みを進めている。2023年は各国で新型コロナウイルス感染症収束によって渡航制限が解除され、国際会合やイベントがリモート開催から現地開催に戻りつつあり、対面での密なコミュニケーションが再び行えるようになった。今後も引き続き、オンラインと対面それぞれのメリットを活かした地域のCSIRT間の交流と連携が推進されることで、地域全体のサイバーセキュリティ能力の更なる強化や進展につながることが期待される。

2.3 情報セキュリティ人材の現状と育成

国内のサイバーセキュリティに関わる人材は質的にも量的にも不足しており、人材育成は各界が協力して解決すべき問題である。教育の充実、高度な人材の育成・確保、セキュリティ人材が将来にわたって活躍できる社会環境の整備等、様々な課題が挙げられている。本節では、産学官における人材育成の取り組みについて述べる。

2.3.1 デジタル人材としての情報セキュリティ人材の状況

DX 推進のためにデジタル人材の育成が求められる中、2023 年 8 月、経済産業省より改訂版の「デジタルスキル標準 ver.1.1」が公開された※300。デジタルスキル標準は、働き手一人ひとりが DX に参画する際の学びの指針となる「DX リテラシー標準（DSS-L）」と、DX を推進する人材の役割や習得すべき知識・スキルを示す「DX 推進スキル標準（DSS-P）」の二つで構成される。デジタルスキル標準は、様々な企業や教育関連組織において採用されている。また、経済産業省と IPA が運営するデジタル人材育成プラットフォーム「マナビ DX※301」のデジタル実践講座には 2024 年 5 月末時点で 62 のセキュリティに関連する講座が登録される等、情報セキュリティ人材の育成支援が進められている。

しかしながら、セキュリティ人材は依然として不足している。ISC2, Inc. が発行した「ISC2 Cybersecurity Workforce Study 2023※302」の調査によると、日本国内のサイバーセキュリティ人材は 2023 年現在約 48 万人存在し、約 11 万人が不足しているという。また、2024 年 3 月に公開された株式会社リクルートの調査※303では、2023 年のサイバーセキュリティ関連求人数は 2014 年比で 24.3 倍に増加しているが、サイバーセキュリティ関連転職者数は 2014 年の 3.62 倍にとどまっている。

このように、人材育成の支援が進められているにも関わらず、人材不足は解消されていない。状況を改善するためには、人材育成を充実させる施策に加えて、セキュリティ人材を効率的に活用していくことも重要である。本節では、人材不足の背景にある状況と対応について述べる。

(1) 人材不足の背景

セキュリティ人材充足の課題には様々なステークホルダーが存在し、社会的な状況も関係するため、考慮すべき点すべてを列挙することは難しい。以下ではいくつかの項目を取り上げる。

(a) 情報セキュリティのカバーする技術領域の広がり

あらゆるビジネスがデジタル世界とつながって展開される状況が広がり、情報セキュリティはビジネスにおいて不可欠な前提となりつつある。それに伴い、情報セキュリティのカバーする範囲がますます広がっている状況にある。

DSS-P のサイバーセキュリティ人材類型は、サイバーセキュリティ、各種法や規制への遵守に加えて、プライバシー保護を含むものとなっている。2023 年には、それらに加え、サプライチェーンセキュリティ、AI システムとそのセキュリティ対応が求められており、カバーすべき技術領域が広がっている。

求められる技術領域の広がりに合わせ、デジタルスキル標準においても、生成 AI 利用時に求められるリテラシーを補記する形で 2023 年 8 月に DSS-L の改訂が実施されている。また、DSS-P についても、現在、生成 AI 時代の人材育成をテーマに検討が進められている※304。

生成 AI のみならず、新しい技術領域に対応できる人材の育成は必要であり、それに効率良く追従していくための人材育成方法、人材育成システムの整備が望まれる。

(b) セキュリティ人材が求められる社会領域の広がり

民間企業でのセキュリティ人材の需要が拡大していることに加えて、それ以外の分野でのセキュリティ人材需要が大きくなってきていることも、セキュリティ人材不足に影響すると予想される。

民間企業においては、世の中のデジタル化とともに DX を推進する動きが加速する中で、IT・セキュリティベンダー等の専門的なセキュリティ人材、企業情報システム部門等のセキュリティ人材に加えて、DX 推進における「プラス・セキュリティ※305 人材」が求められている。2027 年までに、サイバーセキュリティ機能の 30% をサイバーセキュリティの専門家以外のユーザーが所有、直接利用するようになると Gartner, Inc. は予想している※306。

政府は 2022 年 12 月に、いわゆる「安保 3 文書」（国家安全保障戦略、国家防衛戦略、防衛力整備計画）を決定した。この中の防衛力整備企画において、2027

年までに自衛隊のサイバー専門部隊の隊員（コア要員）を約 4,000 人に増員し、サイバー関連分野の業務に従事する隊員を含む総サイバー要員を約 2 万人体制にするとしている※307。また、それに呼応する形で、民間事業者がサイバー安全保障人材育成を支援するために、一般社団法人サイバー安全保障人材基盤協会※308 が設立されている。

警察庁は、サイバー犯罪増加、ランサムウェア感染被害の拡大の状況から、2022 年にサイバー警察局を新設するとともに、警察学校教養体系の運用、検定制度の運用、人材育成基盤装置の整備等を推進し、サイバー捜査官の拡充を進めている※148。

民間企業のみならず様々な社会領域でセキュリティ人材が求められている状況は、今後の人材不足にも影響するものと予想される。

(c) 需要と供給のミスマッチ

IPA による「デジタル時代のスキル変革等に関する調査（2022 年度）全体報告書※309」（以下、スキル変革調査）は、IT 人材の適材化を阻む問題として「学びの方向性を定めることが難しい」ことを挙げ、また、適所化については、採用において「IT 人材のスキルを適切に評価できていない」ことを挙げている。スキル変革調査は IT 人材に関する調査であるが、セキュリティ人材にも同様の状況があると推測される。

SC3 産学官連携 WG の調査※310 では、複数企業のセキュリティ関連の職務記述の表現の比較と、求人票の比較をしている。同じ名称の求人票でも会社によって要件がまったく異なり、各項目も一致していないことを確認している。現状、企業ごとでサイバーセキュリティに関する業務やそれを束ねた役割・職務の内容が不統一で、属性の項目名等の記述方法にも共通性がないことが見て取れるとしている。求人においては組織のセキュリティ対応体制やそこで実施する業務が明確でないことや、そのために必要な知識・技術を特定できていないことから、非常に高いレベルの要件や定性的であいまいな表現となり、応募者とのミスマッチが生じ、求人が多いにもかかわらず応募者が少ない結果となっていると考えられる※302、311。つまり、企業においては、組織内で必要とする情報セキュリティに関わる人材や職務を正確に表現ができておらず、人材の適材化／適所化がうまくできてないといえる。

(2) 人材不足への対応

前項では、人材不足の背景として、セキュリティ人材がカバーする技術領域の広がり、セキュリティ人材を求める社会領域の拡大、需要と供給のマッチングの問題を取り上げた。本項では、それらへの対応をいくつか紹介する。

(a) セキュリティ業務の整理

スキル変革調査の「調査から導き出される問題のまとめと施策の方向性」では、「組織に必要な人材を定義し、必要なスキルを提示する」ことを施策の方向性としている。スキルを提示するためには、組織としての業務と、その業務を行う役割（ロール）を明確にする必要がある。DSS-P では、業務の違いによって区分したロールごとにスキルを定めている。業務・ロールを各組織で検討し、実際にどのような業務・ロールが必要とされているのかを整理することで、対応するスキルを特定することができる。

一般企業においては、「プラス・セキュリティ人材」が必要であると言われる。しかし、プラス・セキュリティ人材を効率良く育成していく具体的な方法は検討が重ねられている状況である。前述したスキル変革調査を踏まえると、一般企業に共通する職種について業務内容をきめ細かく明らかにし、必要となるセキュリティ関連のスキル・知識を業務内容別に標準化することが、取り組み範囲を限定できるという点で、プラス・セキュリティ人材の育成支援になり得ると期待される。一方で、業種・業態によって求められる技術・知識・経験が異なることから、ここで言う標準化も業種・業態別に検討する必要があると考えられる。

業種別での活動例としては金融業界での取り組みがある。セキュリティに特化したものではないが、2024 年 1 月に特定非営利活動法人金融 IT 協会※312（以下、金融 IT 協会）が、金融業界横断での IT 利活用、デジタル人材育成を目的に活動を開始している。また、2024 年 4 月 5 日に開催された経済産業省「産業サイバーセキュリティ研究会」では、規模や業種等サプライチェーンの実態に応じて企業の適切なセキュリティ対策レベルを評価し、可視化する仕組みを検討するとの方向性が示された※313。この仕組みにより組織全体のセキュリティ対策レベルを細目にわたって把握することは、従業員に求められるセキュリティ関連のスキル・知識を見定める上でも参考になると期待される。

(b) 人材のスキル評価の共通化

スキル変革調査の「IT 人材の活躍を阻む環境のまとめ（適所化の問題）」では「IT 人材のスキルを適切に評価できていない」としている。同調査によれば、IT 人材の採用や評価において、スキルのアセスメントをするための体系的な基準を設けて行っている企業は少ない。企業、教育機関等それぞれの組織において、必要となるきめ細かさでの人材評価が共通的基準で実施できれば、人材の適材化・適所化は容易になると考えられる。

共通的な基準としては IPA の IT スキル標準（ITSS）の 7 段階のレベル評価がある。しかし、個々のスキル・知識を確認することのできる細目に及ぶ共通的な基準はない。IPA の ITSS+（プラス）「セキュリティ領域※314」においても、企業のセキュリティ関連業務を 17 分野に整理しているが、評価レベルについては規定していない※315。

金融 IT 協会では、「金融 IT 検定」を立ち上げた。同検定は金融機関における IT・デジタル活用に必要な知識を問うもので、業界で必要とされる技術・知識・業務等を共通化し、ベンダー等との意思疎通がスムーズに行える環境を整えることを目的としている。

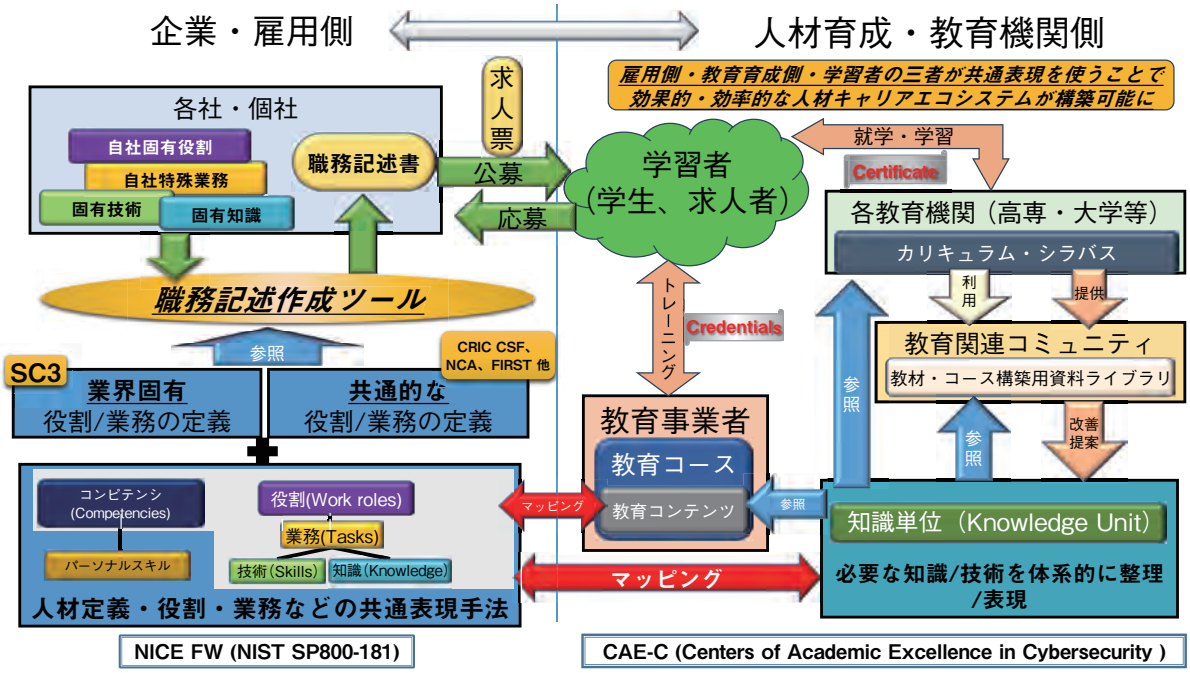
(c) ビジネス環境へのセキュリティ機能の組み込み

ノーコードやレスコードの普及等により、事業担当部門自身がアプリケーションを実行する環境を維持管理してアジャイルにビジネス展開することが今後当たり前になってくる。事業実施において、事業実務者がビジネスアプリケーションを開発することや、デジタルなビジネス環境を運用する場面が多くなることが想定される。そのような状況においては、事業実務者が事業環境のセキュリティ対策を確実に構築、運用を行うことができ、セキュリティ対策で時間と工数を取られることなく、スピード感を持ってビジネス展開できることが求められる。更に、企業全体のセキュリティ管理としては、すべての事業環境におけるセキュリティ対策が統一的に管理されていることが求められる。そのためには、作業する人員が意識することなくセキュアに業務が行えるように、全社として業務基盤に対策を統一的に組み込むことが重要である。これにより、一般的なビジネス環境における新たなセキュリティ対応の需要の増大を予防的に抑え込むことが容易となり、セキュリティ人材不足の解消にも効果が期待できる。

(3) 今後の方向性

デジタルセキュリティ人材を生かしていく施策の背景と対応の一部として、セキュリティ業務の整理、人材のスキル評価の共通化、ビジネス環境へのセキュリティ機能の組み込みを取り上げた。これらの対応を扱う一例として、SC3 産学官連携 WG の「SC3 セキュリティ人材育成フレームワーク」を説明する（図 2-3-1）。

米国では、企業等のサイバーセキュリティ人材育成向けに NICE（National Initiative for Cybersecurity



■図 2-3-1　SC3 セキュリティ人材育成フレームワーク
（出典）SC3 事務局「SC3 第 8 回産学官連携 WG 令和 5 年度 WG 活動報告【抜粋】※310」の図を SC 産学官連携 WG 丹康雄座長へのインタビューに基づき IPA が編集

Education） が「Workforce Framework for Cybersecurity（NICE Framework）※316」（以下、NICE フレームワーク）を推進し、サイバーセキュリティの業務に関する記述を共通化するための NIST SP800-181※317 を規定して、開発・改善を続けている。「SC3 セキュリティ人材育成フレームワーク」は、NICE フレームワークをベースに人材定義・役割・業務等の共通表現手法として用いている。これに、一般企業での共通的な役割／業務の定義※318 と業界固有の役割／業務の定義※319 を加えてテンプレートとしている。自組織のセキュリティ業務を検討する際には、それらのテンプレートをベースとすることで、一から記述する必要がなくなる。各社固有の役割／業務／技術／知識を検討した後、それらを職務記述作成ツールのインプットとすれば、自組織に特化した職務記述書を生成できる。これにより、セキュリティ業務の整理が容易に行える道具立てを提供している。

スキル評価の共通化について、「SC3 セキュリティ人材育成フレームワーク」では直接支援する形にはなっていない※320 が、学習者（学生、求人者等）に人材育成・教育機関で共通知識単位に基づいた修了証あるいは認定証をデジタルバッジで発行することを想定している。これによりスキル評価の共通化を実現しようとしている。

今後もデジタルセキュリティ人材の需要増加に応えていくために、人材育成環境を充実させていくことに加え、育成された人材を生かしていく環境を整えることが更に重要になってくる。一例として「SC3 セキュリティ人材育成フレームワーク」を取り上げたが、このような検討が今後進むことが望まれる。

2.3.2 情報セキュリティ人材育成のための国家試験、国家資格制度

本項では、情報セキュリティ人材の育成や確保を目的とした国家試験や国家資格制度に関する動向を紹介する。

(1) 情報セキュリティマネジメント試験

企業・組織においては、組織が定めた情報セキュリティポリシーを部門内に周知して遵守を促し、部門の情報管理を実施する等、情報セキュリティ対策を推進する人材（情報セキュリティマネジメント人材）が必須である。こうした人材を育成するために、2016 年度春期より「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が実施されている。2020 年度から CBT（Computer Based Testing）方式※321 に移行した同試験は、2023 年 4 月からは年間を通じて随時※322 CBT 方式により実施され、2023 年度は応募者数 3 万 9,824 人（前年比約 1.27 倍）、合格者数 2 万 6,398 人（前年比約 1.64 倍）であった※323。

(2) 情報処理安全確保支援士制度

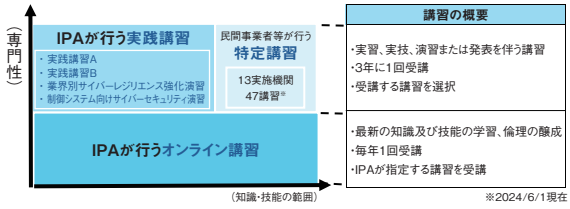
最新の知識・技能を備え、サイバーセキュリティ対策を推進する人材の育成と確保を目指し、2016 年 10 月に「情報処理の促進に関する法律」の改正法が施行され、国家資格「情報処理安全確保支援士」制度が創設された。

情報処理安全確保支援士（以下、登録セキスペ）はサイバーセキュリティ分野初の国家資格であり、情報処理安全確保支援士試験合格者等が登録を申請し、登録簿に登録されることにより資格を取得できる。試験は年 2 回実施され、2023 年度は応募者数 3 万 7,697 人（前年比約 1.08 倍）、合格者数 5,678 人（前年比約 1.16 倍）であった※323。登録セキスペは 2024 年 4 月 1 日時点で 2 万 2,692 人※324 となった。

登録セキスペは、3 年ごとの登録更新が義務付けられている。登録セキスペには登録証（カード型）が交付され、初回登録時は帯の色がグリーン、1 回目の更新時はブルー、2 回目の更新時以降はゴールドに変わる。2023 年 10 月 1 日にゴールド登録証が初めて発行された。登録証のカラーパターンを図 2-3-2 に示す。

■図 2-3-2 登録証のカラーパターン

また、登録更新には計 4 回の法定講習の受講が必要である※325。法定講習の全体像を図 2-3-3 に示す。



■図 2-3-3 法定講習の全体像

法定講習の「オンライン講習」では、登録セキスペに期待される情報セキュリティの実践に必要な知識・技能・倫理について学習することを目的として、IPA が指定す

る講習を毎年1回受講する。

また、実習、実技、演習または発表等を通じて具体的な技術や手法を学ぶことを目的として、3年に1回、「IPAが行う実践講習」あるいは「民間事業者等が行う特定講習」から任意の講習を選択して受講する。

「IPAが行う実践講習」のうち、主に登録後3年目までの登録セキスペを対象とした「実践講習A」は、インシデント対応等の演習を通じて情報セキュリティ対応実践のための具体的な技術や手法を習得するカリキュラムで、2023年度は892名が受講した。また、主に登録後4年目以降の登録セキスペを対象とした「実践講習B」は、想定企業において新規事業を立ち上げる際のセキュリティ上の助言を検討するカリキュラムで、2023年度は3,389名が受講した。このほかに、専門的な知識・技術修得を望む登録セキスペを対象として「業界別サイバーレジリエンス強化演習(CyberREX)※326」と「制御システム向けサイバーセキュリティ演習(CyberSTIX)※327」の選択も可能となっている(「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)。

「民間事業者等が行う特定講習」は、「IPAが行う実践講習」と同等以上の効果を有する講習として経済産業大臣が定める講習※328であり、個々の登録セキスペが目指すキャリアパスに応じた講習を幅広い分野から選択できる。2023年度には13実施機関40講習であったものが、2024年度には13実施機関47講習(2024年6月1日時点)と対象が増加した。

サイバーセキュリティ対策の現場で活躍している登録セキスペからは「オンライン講習ではサイバーセキュリティに関する知識やトレンドのほか、情報収集の仕方や直近の法改正の内容等を学ぶことができる。実践講習・特定講習では実践的なトレーニングを受けることもできる。また、信頼のある資格保有者であることで、開発段階から安心して業務を依頼していただけた」(ITベンダー企業経営者)との声※329が聞かれた。今後一層、企業・組織のセキュリティ対策推進に登録セキスペの活躍が期待され、大きな役割を果たしていくと考えられる。

2.3.3 セキュリティ人材育成のための活動

情報セキュリティ人材を育成するための活動について述べる。

(1)情報セキュリティ人材育成のための活動

情報セキュリティの人材育成を行う関係機関の活動について述べる。

(a)セキュリティ・キャンプ

「セキュリティ・キャンプ」は、若年層の情報セキュリティ意識の向上、並びに将来第一線で活躍できる高度な情報セキュリティ人材を発掘・育成する場として、一般社団法人セキュリティ・キャンプ協議会(以下、セキュリティ・キャンプ協議会)とIPAにより運営されている。セキュリティ・キャンプ協議会とIPAが開催しているプログラム・イベントについて以下で紹介する。

- セキュリティ・キャンプ全国大会
  年1回、主に夏休み期間中に4泊5日の合宿形式の勉強会としてセキュリティ・キャンプのメインイベントである「セキュリティ・キャンプ全国大会」(以下、全国大会)を開催してきた。20回目となる2023年度の「全国大会2023」は8月7日から11日の5日間で開催した。448名の応募があり、選考を通過した79名が参加した※330。
- セキュリティ・ネクストキャンプ
  過去の全国大会を修了、または同等以上のスキルを持つ25歳以下の学生等を対象に、更なる育成の場として「セキュリティ・ネクストキャンプ2023」を全国大会と同時に開催した。5回目の開催となる同プログラムでは62名の応募があり、選考を通過した10名が参加した※331。
- セキュリティ・ジュニアキャンプ
  15歳以下の生徒を対象に「セキュリティ・ジュニアキャンプ」を全国大会と同時に開催した。2022年度まで全国大会の一部として「ジュニアゼミ」を開催していたが、小中学生でもプログラミングの教育が行われるようになったことを受けて、セキュリティを学ぶ機会を増やすために、2023年度より一つの大会として独立させたものである。同プログラムでは25名の応募があり、選考を通過した5名が参加した※332。
- セキュリティ・ミニキャンプ
  25歳以下の学生、生徒、児童を対象に各地域で専門性の高い技術的な教育を提供する専門講座のほか、情報セキュリティのリテラシー向上を企図した参加資格を限定しない一般講座を開催している※333。
  セキュリティ・キャンプ協議会等と地域の組織・団体との共催により1日または2日にわたり行われるプログラムで2023年度は全国各11ヵ所の地域で開催した※334。東京(2023年5月)、三重(2023年7月)、宮崎(2023年8月)、沖縄(2023年10月)、北海道(2023年11

月）では専門講座のみ開催した。新潟（2023年9月）、山梨（2023年9月）、徳島（2023年10月）、広島（2023年11月）、石川（2023年12月）、大阪（2024年3月）では一般講座と専門講座が開催された。

- Global Cybersecurity Camp
  「Global Cybersecurity Camp（GCC）」は「国籍・人種を超えた専門知識のあるグローバル人材の育成」と「国境を越えた友情とゆるやかなコミュニティの形成」を目的としたイベントである。セキュリティに興味を持つ25歳以下の若者がともに学び、友好を深める場として2018年度より日本を含むアジア太平洋地域4ヵ国で開始し、6回目となる2023年度の「GCC 2024 タイ」は9ヵ国の関連団体・大学により開催された。日本からは選考を通過した5名が参加し、参加者はグループワークをとおして各国の受講生、講師等と交流を行い、最終日にその成果を発表した※335。

（b）NICTにおける人材育成

NICTが運営するサイバーセキュリティ研究所には「サイバーセキュリティネクサス（CYNEX）」「ナショナルサイバートレーニングセンター」「サイバーセキュリティ研究室」「セキュリティ基盤研究室」「ナショナルサイバーオブザベーションセンター」という五つの機能・役割があり、研究開発と人材育成に大別される。本項ではNICTが実施している各種人材育成の活動について述べる。

（ア）CYNEX

サイバーセキュリティネクサス（CYNEX：Cyber Security NEXUS）は、産学官連携の結節点（ネクサス）となる先端的基盤の構築のため、2021年4月に組織された。ナショナルサイバートレーニングセンターとサイバーセキュリティ研究室の活動から得られるサイバー攻撃の膨大なデータと人材育成ノウハウを活用し、社会全体でサイバーセキュリティ人材を育成するための共通基盤を共有することで、日本のサイバーセキュリティの対応能力向上を目指している。

CYNEXでは「Co-Nexus A（Accumulation & Analysis）」「Co-Nexus S（Security Operation & Sharing）」「Co-Nexus E（Evaluation）」「Co-Nexus C（CYROP）」の四つのサブプロジェクトが並行して推進されており、人材育成に関連するのはCo-Nexus SとCo-Nexus Cである。

- Co-Nexus S
  Co-Nexus Sでは、高度SOC（Security Operation Center）人材の育成と国産脅威情報の生成・提供・情報発信を行っている。CYNEXの解析チームに参画組織から育成人材を受け入れ、研修と実務を通じて高度SOC人材を育成している。2023年度は4期生として16名が参加した。
- Co-Nexus C
  Co-Nexus Cでは、国内のセキュリティ人材育成事業を活性化させることを目的に、サイバーセキュリティ演習基盤や人材育成教材のオープン化を行っている。サイバーセキュリティ演習基盤として教材と実機の演習環境からなる「CYROP（CYber Range Open Platform）」は、Co-Nexus Cにおけるサイバーセキュリティ演習基盤として、2022年2月にオープン化し、教育機関や民間企業にライセンスの提供を開始した※336。教材・コンテンツ等についてはCo-NEXUS A、S、Eからのフィードバックによるサイバー演習の継続的な最新化、社会的な需要に応じた開発・拡充を行っている。2023年度は29種類の演習教材を提供し、3組織で商用演習サービスの利用を開始した。

NICTは2023年10月、CYNEXの活動を本格始動させる「CYNEXアライアンス」の発足を発表した※337。CYNEXアライアンスでは民間企業、政府機関、教育機関が四つのCo-Nexusに参画し、各Co-Nexusの活動を深化させ、Co-Nexusへの参加組織がアクセスできるサイバーセキュリティ情報の拡充を進める。具体的には「セキュリティ情報融合基盤CURE（Cybersecurity Universal REpository）」を参加組織に開放すると2023年10月に発表した。2024年2月末現在、参加組織は60に達した。

（イ）CYDER

実践的サイバー防御演習（CYber Defense Exercise with Recurrence：CYDER）は、サイバー攻撃を受けた際の一連の対応を、パソコンを操作しながらロールプレイ形式で学ぶことができる演習である。2013年に総務省の実証実験としてスタートし、現在はNICTのナショナルサイバートレーニングセンターによって開発・実施されている。初級（Aコース）、中級（Bコース）、準上級（Cコース）からなる集合演習と、オンライン入門コース、プレCYDERからなるオンライン演習がある。2023年度の集合演習では、初級（Aコース）69回、中級（Bコース）34回、準上級（Cコース）4回を実施した※338。また2023年度、オンライン演習のプレCYDERは国の機関、地方公共団体

のみを受講対象とし※339、2023年12月5日から2024年1月31日に※340実施した。

総務省は2024年2月18～26日にグアムでCYDERを活用し、大洋州島しょ5ヵ国（パラオ、ナウル、マーシャル諸島、ミクロネシア連邦、キリバス）の通信インフラの安全を守るための人材育成を支援する目的で演習を実施した。この演習では、NICTが観測した最新の攻撃情報が活用されている。総務省が島しょ国地域を対象にCYDERを使用し演習を行うのは初めてである※341。

（ウ）CIDLE

総務省は2023年8月、2025年日本国際博覧会（以下、大阪・関西万博）関連組織のサイバーセキュリティ強化のため、万博向けサイバー防御講習「CIDLE（シードル）」を2023年9月から実施すると発表した※342。CIDLEでは、NICTのナショナルサイバートレーニングセンターの大規模仮想ネットワーク環境等を活用し、大阪・関西万博関連組織の情報システム担当者等向けにインシデント対応演習等を実施予定である。

（エ）SecHack365

社会を脅かすサイバーセキュリティ上の課題を分析研究し、解消するアイデアの創出と解決策を実装する力を持った人材が強く求められている。こうした問題意識からNICTのナショナルサイバートレーニングセンターでは、25歳以下を対象に、「セキュリティイノベーター」として様々な課題にアイデアを持って切り込める、次の四つの能力を身に付けた人材の育成を目指す「SecHack365」プログラムを2017年度から実施している※343。

- サイバーセキュリティの課題に関する分析力
- 新たな発想で課題解決に挑むアイデアを多産し研究やシステム等に昇華できる力
- 自ら開発するサービスやプロダクト、システムを安全なものにするスキルや能力
- サイバーセキュリティの課題を解消するストーリーを作りそれを分かりやすく表現できる力

年6回のイベントと通年（365日）のオンライン指導で参加者の研究・開発を支援する仕組みで、「表現駆動」「学習駆動」「開発駆動」「思索駆動」「研究駆動」の5種類のコースが用意されている。2023年度の6回のイベントはオフライン、オンライン各3回ずつが交互に行われ、2024年3月2日にオフラインで成果発表会が行われた。

（c）SECCON

SECCON（SECURITY CONTEST）は、情報セキュリティをテーマにした多様な競技を開催する情報セキュリティコンテストイベントである。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）内に設置されたSECCON実行委員会が運営している※344。SECCONは年間を通じ複数のプログラムを行っており、技術の実践の提供、実践的情報セキュリティ人材の発掘・育成に貢献している。各プログラムの2023年度の実施内容について紹介する。

- SECCON CTF
  CTF（Capture the Flag）は攻撃・防御両者の視点を含むセキュリティの総合力を競うハッキングコンテストである。2023年度は本大会として、オンラインで実施される予選大会「SECCON CTF 2023 Quals」が2023年9月16～17日に、国際決勝と国内決勝の二つの大会で構成される決勝大会「SECCON CTF 2023 Finals」が東京で同年12月23～24日に開催された。国際決勝の出場条件は予選大会の全体順位が10位以内であること、国内決勝は予選大会の日本国内順位が10位以内であること等が定められている※345。
- SECCON Beginners
  SECCON Beginnersは、CTF未経験者やCTFを目指す人向けの勉強会である。初級向けのCTFの実践だけでなく、問題解説やワークショップが併催されている。2023年度はオンライン、オフライン含め合計5回開催された※346。
- CTF for GIRLS
  CTF for GIRLSでは、情報セキュリティ技術に興味がある女性を対象にコミュニティ形成の一環として、情報セキュリティ技術について学ぶワークショップやCTFイベントを開催している。2023年9月にオンラインでワークショップを行ったほか、CTF for GIRLSの発足10年目を記念したイベントが2023年12月に開催された※347。
- SECCON Workshop
  SECCON Workshopは、セキュリティ技術をハンズオンで学ぶワークショップである。2023年7月には東京で「Moving Target Defense」「IoTセキュリティ」をテーマに、9月には札幌で「IoTセキュリティ」をテーマに開催された。10月には福岡で「XDPで作って学ぶファイアウォールとロードバランサー」と題して開催された※348。

(d) AJCCBC

日 ASEAN サイバーセキュリティ能力構築センター（Asean Japan Cybersecurity Capacity Building Centre：AJCCBC）は、ASEAN 域内のサイバーセキュリティ能力の底上げを行うため、タイのバンコクに 2018 年 9 月に設立された人材育成プロジェクトである※349。

2023 年 6 月 19 日、国際協力機構（Japan International Cooperation Agency：JICA）の技術協力プロジェクト「サイバーセキュリティとデジタルトラストサービスに関する日 ASEAN 能力向上プログラム強化プロジェクト」の第 1 回の研修開催を記念し、オープニングセレモニーが AJCCBC で行われた。同プロジェクトは 2023 年 3 月から 4 年間の予定で AJCCBC の運営を支援する※350。

また、2023 年 6 ～ 12 月に ASEAN 加盟国の政府・重要インフラ企業の役職員向けに各種体験型のサイバーセキュリティ演習を 4 回開催した※351。

(e) 産学情報セキュリティ人材育成交流会

産学情報セキュリティ人材育成交流会は、JNSA が情報セキュリティ分野の人材不足の状況を踏まえ、JNSA 産学情報セキュリティ人材育成検討会を 2012 年に発足し、「教育機関における産学連携の支援」と「会員企業における採用を支援する取り組み」の実行を宣言したことに始まる※352。同交流会はインターンシップに興味を持つ学生に対し、受け入れ企業と交流できる場を提供し、長期インターンシップに関わる不安等を解消する目的で実施している。2023 年度の同交流会は 12 月 2 日に定員 60 名で、東京大学本郷キャンパスで開催され、インターンシップの実施を予定する企業と学生が、セキュリティ業界、サイバーセキュリティの仕事、働き方等について情報交換を行った※353。

(f) サイバーセキュリティ経営戦略コース

サイバーセキュリティ経営戦略コースは、東京工業大学の環境・社会理工学院 技術経営専門職学位課程において社会人アカデミーのプログラムとして行っている、技術経営（Management of Technology：MOT）に関する 14 種類あるプログラム（Career up MOT：CUMOT）のうちの一つである。サイバーセキュリティ経営及び経営立案に求められる知識・能力を備え、企業・組織を先導する人材を育成することが目的である※354。2023 年度は 11 月から 3 月の毎週木曜日にオンライン講義形式で開催された※355。

(g) KOSEN Security Educational Community

KOSEN Security Educational Community は、独立行政法人国立高等専門学校機構が実施しているサイバーセキュリティ人材育成事業である。高等専門学校（以下、高専）には、IT の最新ハードウェアやソフトウェアに触れる環境があり、在校生は早い段階から専門教育を受けていることから、サイバーセキュリティ分野において将来、社会に貢献できるポテンシャルがある。当該事業は木更津高専と高知高専が拠点校となり、その他全国の高専のうち 8 校を 5 ブロックに分け、協力校として拠点校と連携して人材育成を推進している※356。2023 年度には、サマースクール、演習、講習会、コンテスト等のサイバーセキュリティに関する技術を習得するための多様なイベントが開催された※357。

(2) 産業システムセキュリティ人材育成のための活動

IPA の産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）では、重要インフラや産業基盤のサイバー攻撃に対する防御力を強化するための人材育成事業に取り組んでいる。具体的にはセキュリティの観点から企業等の経営層と現場担当者を繋ぐ人材（中核人材）を対象とした「中核人材育成プログラム」、セキュリティ対策を統括する経営層や部課長クラス等向けの「責任者向けプログラム」、制御システムのサイバーセキュリティ担当者向けの「実務者向けプログラム」を実施している。

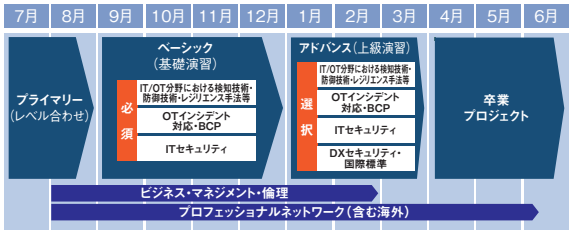
本項では 2023 年度に実施した事業について述べる。

(a) 中核人材育成プログラム

ICSCoE は、2017 年 7 月から制御技術（OT：Operational Technology）と情報技術（IT）、マネジメント、ビジネス分野を総合的に学び、サイバーセキュリティ対策の中核となる人材を育成する「中核人材育成プログラム」を実施している。同プログラムでは、OT 及び IT 知識のレベル合わせからハイレベルな演習までを 1 年間のフルタイムで実施する（次ページ図 2-3-4）。第 1 期から第 6 期までに 370 名の修了者を輩出し、2023 年 7 月に開講した第 7 期では、電力・ガス・鉄鋼・石油・化学・自動車・鉄道・放送・通信・建築・産業用制御システムのベンダー等の幅広い業界から 65 名が参加した。

カリキュラムは以下の 3 領域を基軸とした構成となっている。

- 「IT/OT 分野における検知技術・防衛技術・レジリ



■図 2-3-4　第 7 期中核人材育成プログラムの年間スケジュール

エンス手法等」（模擬プラントを用いた攻撃と防御の両面を学ぶパープルチーム演習、制御システムを含んだセキュリティリスク評価、攻撃に対する防衛技術の理解等）

- 「OT インシデント対応・BCP」（安全性と事業継続性を両立する OT インシデント対応、制御システム BCP 対応の演習等）
- 「IT セキュリティ」（制御システムセキュリティ実現のための IT 設計、IT インシデント対応、体制整備等）

また、専門家によるビジネスマネジメントに関する講義や米国・欧州等の先進事例を学び現地トップレベル機関との人的ネットワークの構築を目的とする海外派遣演習、国内で制御システムの現場を見学するフィールドワーク等を含んでいる。

2024 年 4 月には、第 7 期受講者が海外派遣演習として英国及びフランスを訪問した。英国では、港湾都市に所在するプリマス大学 Cyber-SHIP Lab を訪問し、船舶システムの模擬プラント等を見学したほか、英国科学・イノベーション・技術省にて英国におけるサイバーセキュリティ政策の紹介を受けた後、サイバーセキュリティ分野のスタートアップを支援する Cyber Runway 等を訪問し、意見交換を行った。フランスでは、サイバーセキュリティにおける先進的な技術開発等が行われている研究機関 Institut Mines-Télécom 及び IRT System X を訪れ、技術開発の現場を見学した。

国内においても、発電プラントや化学プラント等制御システムが稼働する現場を見学した。

カリキュラムの総まとめの「卒業プロジェクト」では、受講者自身が課題を設定してグループワークで成果物を作成する。第 6 期では 22 件の成果物が作成され、受講者の取り組みの一端を紹介するため、機密性等の観点から公開可能な 6 件を Web サイトで公開した※ 358。

中核人材育成プログラムの修了者コミュニティである「叶会※ 359」は、2018 年夏以降、同プログラムを通じて培った人脈の活用、知見やノウハウの共有を目指し、地域活動や技術をテーマにする複数の部会を設置する等、活動している。

2023 年 11 月には修了年次をまたがる縦のつながりの形成、最新情報及びノウハウ共有を目的とした叶会総会の第 6 回を開催した。

叶会には第 1 期から第 6 期までの修了者に加え、2024 年 6 月に修了した第 7 期生も参加しており、今後もコミュニティとしての規模を拡大しながら、お互いの顔が見える縦横の人的つながりを形成し、産業サイバーセキュリティに関する適時、適切な情報共有活動を継続することが期待される。

また、修了者へのフォローアップの一環として、リカレント教育の機会を設けている。2023 年度は 7 月から 8 月の間で 4 コース 4 回のプログラムを提供し、それぞれ希望者が参加した。知識・スキルのアップデートや修了者間のネットワークの維持、構築の場になっている。

(b) 責任者向けプログラム

責任者向けプログラムでは、「サイバー危機対応机上演習（CyberCREST）」「業界別サイバーレジリエンス強化演習（CyberREX）」「サイバーセキュリティ企画演習（CyberSPEX）」の三つのプログラムを実施した。

- サイバー危機対応机上演習（CyberCREST）
  「サイバー危機対応机上演習（CyberCREST：Cyber Crisis REsponse Table top exercise）※ 360」は、制御システムを有する企業・団体においてサイバーセキュリティ対策を統括する責任者や SOC（Security Operation Center）の責任者、サイバーセキュリティ対策部門の管理職を対象としたプログラムである。
  2024 年 1 月に同演習を東京で実施した。同演習では、世界情勢の不確実性を背景に高まるサイバー攻撃の脅威に備え、組織の責任者層に不可欠なサイバーセキュリティの知識やスキルを学ぶため、OT 環境へのサイバー攻撃の脅威やインシデントへの対処についての講義や、イスラエルの有識者による講演及び質疑、更に国家脅威アクターによるサプライチェーン攻撃のシナリオを使った机上演習を行った。
- 業界別サイバーレジリエンス強化演習（CyberREX）
  「業界別サイバーレジリエンス強化演習（CyberREX：Cyber Resilience Enhancement eXercise by industry）※ 326」は、電力、ガス、ビル、金属、石油、化学、自動車（製造）、ファクトリーオートメーション、情報通信、鉄道、物流、航空、船舶業界において、CISO に相当する役割を担う人材や IT 部門、生産

部門等の責任者・マネージャークラスの人材を対象としたプログラムである。登録セキスペの「実践講習」としても参加可能になっている。

2023年5月と9月に東京、11月に大阪で同演習を実施した。同演習は、部署・部門のサイバーセキュリティに関するインシデント対応力・回復力を強化するため、仮想企業を想定し、業界の最新動向、業界別に考慮すべきセキュリティ要件、安全性要件を織り込んだシナリオ形式による実践演習を中心に進められた。受講者に加え、サイバーセキュリティの専門家や関連省庁の関係者も参加した形式でグループ演習を行った。

- サイバーセキュリティ企画演習（CyberSPEX）

「サイバーセキュリティ企画演習（CyberSPEX：Cyber Security Planning Exercise※361）」は、組織のサイバーセキュリティを推進する責任者（マネジメント）層として必要な企画立案スキルを習得するためのプログラムである。2023年度より新規開講し、2024年1月から2月にかけて東京で計4日間実施した。同演習では責任者層として知るべきサイバーセキュリティの知識を獲得する講義やワークショップ、経営層を説得する考え方やロジカルシンキングを習得する提言シミュレーション演習を行った。提言シミュレーション演習では、仮想企業を用いてサイバーセキュリティの企画を立案し、模擬的な役員会において経営経験者の講師に対して提言を行い、実践的なフィードバックを得て知見を深めた。参加者からは、「グループワーク形式で他受講者の意見も大変参考になった」「経営向け提案のストーリー作成のイメージがつかめた」といった反応があった。

(c) 実務者向けプログラム

実務者向けプログラムでは、「制御システム向けサイバーセキュリティ演習（CyberSTIX：Cyber SecuriTy practIcal eXercise for industrial control system）※327」を実施している。同演習は、制御システムのサイバーセキュリティを担当する、または今後担当予定の技術者を対象として実施したプログラムである。登録セキスペの「実践講習」としても参加可能になっている。

2023年5月に札幌、9月に東京、2024年2月に福岡で同演習を実施した。同演習は、制御システムのサイバーセキュリティを理解するための導入的な演習に位置付けられている。制御システムへの攻撃手法、及び制御システムのサイバーセキュリティ対策の基礎を、簡易模擬システムを用いた実機演習（ハンズオン演習）で体験し、制御システムのセキュリティについて実践的に理解することを目的としている。

2.4 国際標準化活動

国際標準とは、製品や技術を、国境を越えて利用するために制定される国際的な共通規格であり、国際規格とも呼ばれる。本節では、日本の標準化活動を含む様々な標準化団体の活動及び国際標準化の動向としてISO、IEC、ITU-Tのセキュリティ分野の活動を紹介する。

2.4.1 様々な標準化団体の活動

日本の標準化活動への取り組みと、作成プロセスや作成組織の違いから見た標準の分類、及びセキュリティに関連する分野の主な標準化団体の概要を示す。

(1) 日本の標準化活動推進の取り組み

主要国では、自国に有利な標準化を目指し、官民を挙げて標準化活動に取り組んでいる。日本でも「市場創出に資する経営戦略上の標準化活動(戦略的活動)」に積極的に取り組むことが、これまでの基盤的活動の維持に加えて重要であるとして、2022年4月より経済産業省日本産業標準調査会基本政策部会にて、日本の標準化活動の在るべき姿や課題・取り組み事項の整理を行い、2023年6月「日本型標準加速化モデル」を公表した※362。「日本産業標準調査会 基本政策部会 取りまとめ※363」では「人材の育成・確保」「経営戦略と標準化」「研究開発と標準化」「標準加速化を支える環境整備・各種取組」をポイントに挙げ、上記モデルの実現に向けた課題と施策を述べている。

(2) 標準の分類

国際標準には、公的な標準化団体により所定の手続きを経て作成される「デジュール標準(de jure standard)」、いくつかの企業や団体等が協力して自主的に作成する「フォーラム標準(forum standard)」、公的な標準化団体を介さず、市場や業界において広く採用された結果として事実上標準化される「デファクト標準(de facto standard)」がある。

デジュール標準では、幅広くステークホルダーを集めて議論をとおして合意形成を行う。次項で紹介するISO、IEC、ITU-Tが作成する国際規格やJIS等の国家規格が該当し、策定プロセスが規定されており、様々な規制等に用いられることも多い。合意形成のために複数の検討段階が設定されており、正式に発行するまでに時間がかかる(ISO/IECは約3年)。

フォーラム標準は業界団体等、共通の関心を持つ企業等が集まって議論し、業界ルール等限定的な範囲で合意される標準である。作成スピードは速く、業界の特性が反映されていることから該当する業界内では利用が促進されやすい。次項で紹介するIEEE、IETF、TCGが発行する標準が該当する。コンソーシアム標準と呼ばれることもある。業界のフォーラム標準が、その後、国際標準化団体に提案され、時間をかけてデジュール標準となる場合もある。

電気製品やIT製品等、開発サイクルの短い分野では、その時点の市場で一般的な規格としてデファクト標準が採用される傾向にある。例えばWindowsのようなOSやGoogleのような検索エンジン等、グローバルなIT企業の製品・サービスが事実上の国際標準となる傾向があり、合意形成プロセスは存在しない。

(3) 情報セキュリティ分野に関する標準化団体

情報セキュリティに関連するデジュール標準やフォーラム標準の策定を行っている主な国際標準化団体を以下に示す。

- ISO(International Organization for Standardization:国際標準化機構)/IEC(International Electrotechnical Commission:国際電気標準会議)JTC 1(Joint Technical Committee 1:第一合同技術委員会)※364:情報セキュリティを含む情報技術の国際規格を策定している。コンピューターや情報分野を扱う国際標準化団体としてISO、IECはそれぞれ独立に存在しているが、扱う領域の競合を避けるために双方が連携し、JTC1が設立された。日本国内の標準化団体としては、日本産業標準調査会(JISC:Japanese Industrial Standards Committee)がISO、IEC双方のメンバーであり、JTC 1でも活動している※365。
- ITU-T(International Telecommunication Union Telecommunication Standardization Sector:国際電気通信連合 電気通信標準化部門):
  電気通信技術に関わる国際規格を策定している。情報セキュリティに関してはSG(Study Group)17が設置され※366、ISOや後述するIETFとともにネットワークやID管理等に関する標準化活動を行っている。策定した標準はITU-T勧告として定められる。

また、情報セキュリティ分野に関するフォーラム標準を策定する代表的な組織として、以下がある。

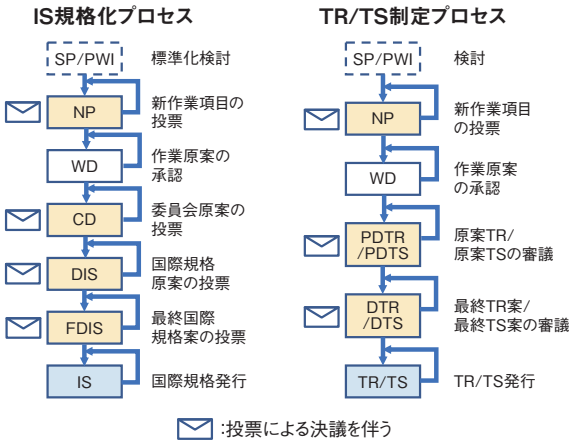
- IEEE（The Institute of Electrical and Electronics Engineers, Inc.）：
  電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織である IEEE-SA（Standards Association）が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoT セキュリティ等の広範な領域で標準化を行っている。
- IETF（Internet Engineering Task Force）：
  インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメーリングリストに登録することで誰でも議論に参加できる。情報セキュリティについては、インターネット上のセキュアなプロトコル、暗号、署名、認証、セキュリティ情報連携（セキュリティオートメーション）等の方式の標準化を行っている※367。標準化した技術文書は RFC（Request For Comments）として参照できる。
- TCG（Trusted Computing Group）：
  信頼できるコンピューティング環境（埋め込み機器、パソコン／サーバー、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダーやシステムインテグレーターがメンバーとなり、中国、日本に regional forum がある※368。

2.4.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）

ISO/IEC JTC 1/SC 27（以下、SC 27）は、ISO 及び IEC の合同専門委員会（ISO/IEC JTC 1）において、情報セキュリティに関する国際標準化を行う分科委員会（SC：Subcommittee）である。SC 27 は、テーマ別に以下の五つの作業グループ（WG）で構成される。

WG 1：情報セキュリティマネジメントシステム
WG 2：暗号とセキュリティメカニズム
WG 3：セキュリティの評価・試験・仕様
WG 4：セキュリティコントロールとサービス
WG 5：アイデンティティ管理とプライバシー技術

ISO/IEC における標準化作業は、策定する仕様の完成度によって図 2-4-1 のような作成段階があり、それぞれ各国の投票によって次の段階へ進む。なお、ISO において、技術が未成熟である、またはガイダンス等の標準仕様ではないが重要であるとされたものは、技術報告書または技術仕様書として発行する。



■図 2-4-1　ISO/IEC JTC 1/SC 27 における文書の作成段階
（出典）JISC「ISO/IEC 規格の開発手順※369」を基に IPA が作成

図 2-4-1 の各文書の作成段階と略号は以下のとおりである。

SP：研究期間（Study Period）
PWI：予備業務項目（Preliminary Work Item）
※SP と PWI のどちらを実施するかは WG によって異なる。
NP：新作業項目（New work item Proposal）
WD：作業原案（Working Draft）
CD：委員会原案（Committee Draft）
DIS：国際規格原案（Draft International Standard）
FDIS：最終国際規格案（Final Draft International Standard）
IS：国際規格（International Standard）
PDTR：予備技術報告原案（Preliminary Draft Technical Report）
PDTS：予備技術仕様書原案（Preliminary Draft Technical Specification）
DTR：技術報告書原案（Draft Technical Report）
DTS：技術仕様書原案（Draft Technical Specification）
TR：技術報告書（Technical Report）
TS：技術仕様書（Technical Specification）

以下に、各 WG の活動概要を述べる。なお本文中では略号を使用する。

（1）WG 1（情報セキュリティマネジメントシステム）

WG 1 では、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）に関する国際規格として、ISO/IEC 27001（ISMS 要求事項）及び ISO/IEC 27002（情報セキュリティ管理策及

び実施の手引き）を中心に、ISO/IEC 27001 が示す ISMS 要求事項に関する手引きや指針を提供する規格、ISO/IEC 27001 及び ISO/IEC 27002 を土台とする分野別規格、及びその他トピックスに関する ISO/IEC 27000 ファミリー規格の国際標準化活動を実施している。

(a) ISO/IEC 27001:2022 及び ISO/IEC 27002:2022 発行に伴う他規格への影響

2022 年には、ISO/IEC 27001 の本文と ISO/IEC 27002 の構成の大きな変更を伴う改訂がされた。この改訂に伴い、これら規格を引用、参照している規格には見直しが発生している。

ISO/IEC 27002 に基づきセクター固有のガイドラインを提供する規格は、改訂への対応が比較的早く、ISO/IEC 27011（ISO/IEC 27002 に基づく電気通信組織のための情報セキュリティマネジメント指針）は、既に改訂を終えて、2024 年 3 月に改訂版が発行された。ISO/IEC 27019（エネルギーユーティリティ工業のための情報セキュリティ制御）は現在 DIS の段階、ISO/IEC 27017（ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）は CD の段階である。

その他のガイドライン規格においても、改訂が開始されている。ISO/IEC 27003（情報セキュリティマネジメントシステム－手引）、ISO/IEC 27004（情報セキュリティマネジメント－測定）、ISO/IEC TS 27008（セキュリティ技術－情報セキュリティ管理策の監査員のための指針）は、いずれも、改訂が開始され、WD の段階である。ISO/IEC 27013（情報セキュリティ，サイバーセキュリティ，プライバシー保護－ ISO/IEC 27001 及び ISO/IEC 20000-1 の統合的実施の手引）については、改訂は行われず、追補版を発行予定で作業が行われている。

検討が開始されている新規規格としては、ISO/IEC 27028（ISO/IEC 27002:2022 の属性の利用及び作成に関する手引）がある。ISO/IEC 27002:2022 で新たに取り込まれた属性について、その利用や作成に関する手引きを示す規格である。ISO/IEC 27002 では、93 個の管理策が次の 4 箇条に分けて示されている。

- 組織的管理策（37 個）
- 人的管理策（8 個）
- 物理的管理策（14 個）
- 技術的管理策（34 個）

属性は、これらの管理策を、更に分類しやすくするためのものであり、規格では表 2-4-1 の五つの属性が示されているが、組織がこれ以外の新たな属性を作成することもできる。

属性	属性値
管理策のタイプ	予防、検知、是正
情報セキュリティ特性	機密性、完全生、可用性
サイバーセキュリティ概念	識別、防御、検知、対応、復旧
運用機能	ガバナンス、資産管理、情報保護、人的資源のセキュリティ、物理的セキュリティ、システム及びネットワークセキュリティ、アプリケーションのセキュリティ、セキュリティを保った構成、識別情報及びアクセスの管理、脅威及び脆弱性の管理、継続、供給者関係のセキュリティ、法及び順守、情報セキュリティ事象管理、情報セキュリティ保証
セキュリティドメイン	ガバナンス及びエコシステム、保護、防御、対応力

■表 2-4-1　ISO/IEC 27002 の属性
（出典）ISO・IEC「ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls※370」を基に執筆者が作成

(b) その他の ISO/IEC 27000 ファミリー規格の国際標準化活動

ISO/IEC 27001:2022 及び ISO/IEC 27002:2022 の改訂と直接関係のない、その他の規格の動向について述べる。

ISO/IEC 27016（情報セキュリティマネジメント－組織経済学（Organizational Economics））については、改訂検討が開始され、PWI にある。また、サイバーセキュリティに関するガイドラインである ISO/IEC TR 27103（サイバーセキュリティと ISO 及び IEC 規格）は改訂中であり、WD の段階である。

(2) WG 2（暗号とセキュリティメカニズム）

WG 2 では、暗号プリミティブ（暗号アルゴリズム）や、デジタル署名技術、鍵共有のような汎用的かつ基本的な暗号プロトコル等の標準化を行っている。2023 年度は、新しい規格である ISO/IEC 4922-1（秘密マルチパーティ計算 第 1 部：総論）と ISO/IEC 4922-2（秘密マルチパーティ計算 第 2 部：秘密分散に基づくメカニズム）の 2 件、及び既存規格 2 件の改訂版（追補）が発行された。このほかの主な活動内容について以下に示す。

(a) 耐量子計算機暗号の規格化作業停滞

ドイツより、耐量子計算機暗号 FrodoKEM の標準化が提案され、1 年半での規格の発行を目指し、ISO/

IEC 18033-2（暗号アルゴリズム 第2部：非対称暗号）の追補として2023年に規格化作業が開始された。この追補に掲載候補として挙げられているアルゴリズムは、FrodoKEM、CRYSTALS-Kyber、Classic McElieceである。

ただ、WG内の議論では、耐量子計算機暗号の規格内容の考え方に様々な見解が出ているため、コンセンサスが得られておらず、進捗は停滞気味である。中間会合を増やして議論を加速する予定である。

(b) 完全準同型暗号の規格化作業再開

完全準同型暗号はISO/IEC 18033-8（暗号アルゴリズム 第8部）として2021年に規格化を開始したが、様々なタイプのアルゴリズムがあるため、規格化作業の進捗は芳しくなかった。

2023年に、完全準同型暗号を単独の規格とし、アルゴリズムタイプごとに各部に分けることが提案され、ISO/IEC 28033として規格化作業を開始することが承認された。ISO/IEC 28033-1（完全準同型暗号 第1部:総論）、ISO/IEC 28033-2（完全準同型暗号 第2部：BGV/BFV系）、ISO/IEC 28033-3（完全準同型暗号 第3部:CKKS系）、ISO/IEC 28033-4（完全準同型暗号 第4部：CGGI系）という構成で議論を進めている。

(3) WG3（セキュリティの評価・試験・仕様）

WG3では、セキュリティの評価・試験手法の標準化を行っている。本項においては、WG3において開発され、2023年度に発行された以下の三つの国際標準に関して概説する。

(a) ISO/IEC 23837 “Information security - Security requirements, test and evaluation methods for quantum key distribution”

ISO/IEC 23837は、量子鍵配送（Quantum key distribution）のセキュリティ要件、及び評価・テスト手法を規定した国際標準である。量子鍵配送とは、暗号鍵を含む鍵情報を光子に載せ、量子力学的な性質を活用して鍵情報を守りつつ、送信者と受信者で暗号鍵を共有する仕組みである。もし盗聴者が光子に載せた鍵情報を盗み見ると、光子の量子力学的な状態が変化したことを検知できる。検知されずに鍵情報を盗聴することが不可能であることが理論上証明されている。盗聴されずに交換された暗号鍵のみを用いて暗号通信を行うことで、量子コンピューターを含むいかなる計算機でも暗号解読が不可能な暗号通信を実現できる。

量子鍵配送は理論上の安全性が量子情報理論によって証明されているが、理論と実装との著しい差異や、不適切な仕様、バグ等があればその限りではない。そのため、量子鍵配送システムが正しく設計・実装されていることを確認するためのセキュリティ評価やテストが必要となる。量子鍵配送システムは、その特性を光学測定器によって定量的に評価すること、測定結果と安全性理論とがリンクしていること等の特徴があることから、従来の暗号システムとは大きく異なる評価手法・テスト手法が必要となる。ISO/IEC 23837は、安全な量子鍵配送システムが順守すべきセキュリティ機能要件をPart1に、量子鍵配送システムのセキュリティを検証するためのテスト詳細をPart2に、それぞれ記載している。

(b) ISO/IEC TS 9569 “Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045”

ISO/IEC TS※371 9569は、開発者がセキュアな更新プログラムを開発するために順守すべきセキュリティ要件等を定めている。

欧州議会においてEUCC Implementation Act※372が承認され、EUCC※373と呼ばれるISO/IEC 15408に基づくIT製品のセキュリティ評価・認証制度の設立が欧州において進行している。ISO/IEC 15408に基づくセキュリティ評価・認証制度としては、古くから存在するCCRA※374と呼ばれるグローバルな枠組みがあったが、EUCCにおいてはCCRAにはなかった新たな評価・認証プロセスが追加されている。その一つが、既に評価・認証されたIT製品に更新プログラムが適用された場合のレビュープロセスである。EUCC Implementation Actは、IT製品開発者に更新プログラムの開発・適用プロセスの手順を明確化し、評価機関にそのプロセスを評価することを求めているが、どのような更新プログラムの開発・適用プロセスを実施すべきかに関する詳細を記述していない。ISO/IEC TS 9569は、もともとEUCCへの適用を念頭に開発され、開発者がセキュアな更新プログラムを開発するために順守すべき更新プログラムに関する要件や、攻撃者により改変された更新プログラムが適用されることを防ぐためIT製品が満たすべきセキュリティ要件等を定めており、今後まず欧州においてISO/IEC TS 9569に基づく更新プログラムの開発・適

用プロセスの評価が開始されるものと思われる。

(c) ISO/IEC 17825 “Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules”

ISO/IEC 17825 は、暗号モジュールに対する非侵襲攻撃（サイドチャネル攻撃等、暗号モジュールへの物理的侵入を伴わない攻撃）の評価手法に関する国際標準である。ある研究者から技術的な指摘※375 を受けたため、それらの指摘に対応するため 2020 年より改訂が開始され、2024 年 1 月に改訂版が発行された。

(4) WG 4（セキュリティコントロールとサービス）

WG 4 では、WG 1 が対象とする ISMS を実施・運用する際に必要となる具体的なセキュリティ対策、及びセキュリティサービスの標準化を行っている。以下に、WG 4 における 2023 年度の主な成果、活動を紹介する。

(a) IoT のセキュリティとプライバシーのための標準化活動

WG 4 では、IoT のセキュリティとプライバシーに関わる標準化として、以下の四つの活動を進めている。

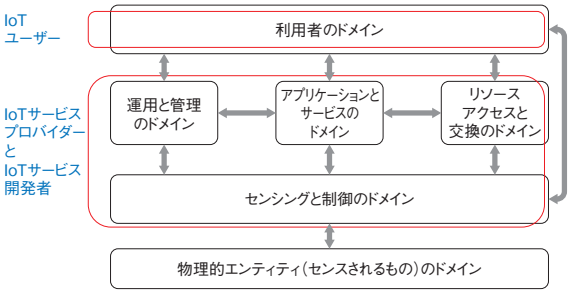
- ISO/IEC 27400: Cybersecurity – IoT security and privacy – Guidelines
- ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements
- ISO/IEC 27403: Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics
- ISO/IEC 27404: Cybersecurity – IoT security and privacy – Cybersecurity labelling framework for consumer IoT

(ア) ISO/IEC 27400: Cybersecurity – IoT security and privacy – Guidelines

同規格は、IoT 推進コンソーシアムが策定した「IoT セキュリティガイドライン※376」に基づき、日本から規格案が提案され、2022 年 6 月に発行された。

同規格における IoT システムは、IoT ユーザー、IoT サービス開発者（機器の開発者を含む）、IoT サービスプロバイダーの三つの利害関係者によって構成され、第 5 章では利害関係者と IoT 参照体系との関係を図 2-4-2 で示すように整理している。

第 6 章では、IoT システムにおけるリスク源（リスクソース）について言及している。



■図 2-4-2　ドメインに基づく参照モデル
（出典）ISO・IEC「ISO/IEC 27400:2022 Cybersecurity – IoT security and privacy – Guidelines※377」を基に執筆者が翻訳

第 7 章では、セキュリティ対策、及びプライバシー対策が、IoT サービス開発者／ IoT サービスプロバイダー、IoT ユーザーのそれぞれの立場での対策内容、目的、導入ガイドといったガイドライン的表現で記載されている。第 7 章に記載されているセキュリティ対策としては、IoT セキュリティポリシー、IoT を保有する組織のセキュリティ、IoT システムのセキュアな設計原則、安全な開発環境と手順、IoT 機器やシステム設計の検証、IoT システムのための適切なネットワークの利用、安全な IoT 機器の設定と構成管理、IoT ユーザー及び機器の認証、ソフトウェア／ファームウェアのアップデート提供、ライフサイクルに適応したセキュリティ対策、脆弱な機器の管理、IoT ユーザーのためのサポートサービス、IoT ユーザーのための機器やサービスの初期設定、IoT 機器の安全な廃棄または再利用等が含まれており、広範囲な対策群が提供されている。

同規格は、ガイドラインの位置付けであるため、IoT ユーザーや IoT サービス開発者等に対する強制力はないものの、それぞれの IoT システムにおける利害関係者が同規格に基づき、IoT システムの設計、運用、管理を実施することが推奨されており、IoT セキュリティ及びプライバシーの規範となるものと考えられている。更に、同規格は、他の進行中の IoT 関連の規格（ISO/IEC 27402、ISO/IEC 27404 等）からも参照されている。

(イ) ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements

同規格は、NIST 及び ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）の既存のガイドラインを下敷きに米国主導で規格案が作成され、2023 年 11 月に発行された。

同規格の位置付けは、図 2-4-3（次ページ）にあるように、同規格の基本要求事項が水平方向の基本ベースラ

インとなり、その上に垂直市場（健康、金融サービス、産業、家電、輸送等）や様々なセクター（民間／工業、公共、防衛、国家安全保障等）のアプリケーションで想定されるIoT機器の使用とリスクに対する追加要件を構築できるというものになっている。

■図 2-4-3　特定セクターや垂直市場による潜在的な追加要件との関係
（出典）ISO・IEC「ISO/IEC 27402:2023 Cybersecurity – IoT security and privacy – Device baseline requirements[※378]」を基に執筆者が翻訳

同規格の枠組み等の詳細については「情報セキュリティ白書2023」の「2.6.2（4）（a）（イ）ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements」を参照いただきたい。

（ウ）ISO/IEC 27403: Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

同規格は、2019年4月、テルアビブ会議において、中国からNPとして提案され、同年10月のパリ会議では、NPの承認がなされ、2022年10月にDISに進むことが決定し、2024年3月の時点ではFDISの段階にある。「IoT-domotics」とは、娯楽、機器制御、監視等の用途として、居住環境（ホームオートメーション等）で利用するIoTサービスをいう。同規格は、ISO/IEC 27400との棲み分けが難しい部分が多いものの、IoT-domoticsの特性を抽出し、ISO/IEC 27400の枠組みに沿ってIoT-domoticsの視点からセキュリティとプライバシーに関するガイドラインを整理している。

同規格は、ISO/IEC 27400のセキュリティ対策、及びプライバシー対策に基づき、IoT-domoticsの視点から追加的なガイダンスを提供しているが、IoTユーザーのための簡単なIoT機器の設定、フェイルセーフ、子供への考慮等のIoT-domoticsとして特徴的な内容が含まれており、IoT-domoticsを構成するサブシステムやIoTゲートウェイのためのセキュリティ、及びプライバシーのガイドラインを提供している。

（エ）ISO/IEC 27404: Cybersecurity – IoT security and privacy – Cybersecurity labelling framework for consumer IoT

同規格案は、2021年10月にシンガポールから提案されたもので、ユーザーが活用するIoT機器にセキュリティラベルを付与し、機器にどの程度セキュリティ機能が装備されているかを、IoT機器のユーザーが把握できるようにする目的で検討が開始された。

現在、WDの審議を終え、第1版CDの段階にある。以下に同規格案の概要を示す。

- 規格案のスコープ

  同規格案は、消費者向けIoT製品のサイバーセキュリティラベリングプログラムを開発・実施するためのサイバーセキュリティラベリングフレームワークを定義し、以下のトピックに関するガイダンスを含む。

  - 消費者向けIoT製品に関連するリスクと脅威
  - 利害関係者、役割、責任
  - 関連規格とガイダンス文書
  - 適合性評価の選択肢
  - ラベリング発行及び保守要件
  - 相互承認の考慮事項

  同規格の対象範囲は、複数の機器が接続されるIoTゲートウェイ、基地局、ハブ、スマートカメラ、テレビ、スピーカー、ウェアラブル機器、コネクテッド煙探知機、ドアロック、窓センサー、コネクテッドホームオートメーション、アラームシステム、洗濯機や冷蔵庫等のコネクテッド家電、スマートホームアシスタント、コネクテッド子供用玩具及びベビーモニター等の消費者向けIoT製品に限定される。消費者向けではない製品は、この規格から除外される。除外される機器の例としては、主に製造、ヘルスケア、その他の産業用途を目的としたものがある。

  同規格案は、消費者、開発者、サイバーセキュリティラベル発行機関、独立試験機関に適用される。

- 同規格案策定の背景

  脅威状況、必要性等の背景は以下のとおりである。

  - IoTの脅威状況

    世界的に、IoT製品の数が加速度的に増加している。消費者向けIoT製品は、市場投入までの期間が短く、陳腐化も早いことが多い。消費者向け製品は価格帯が低く、利益率も低いため、サイバーセキュリティ対策が十分に施された状態で設計・製造されていないことが多い。このようなIoT製品に

は、根本的なセキュリティ上の弱点や一般的な欠陥がしばしば見受けられる。IoT 製品が普及するにつれて、IoT 製品にサイバーセキュリティのための十分な対策が施されていないことが、広範な攻撃対象領域（アタックサーフェス）を生み出し、サイバーセキュリティのリスクを増大させ、ウイルスや侵入テストツールを悪用したサイバー攻撃の影響を受けやすくなっている。

－ラベリングの枠組みの必要性

消費者向け IoT ラベリング制度は、特定の地域や市場におけるサイバーセキュリティの懸念に対応するために個別に策定されているため、ラベリングされた製品を比較することが難しくなり、国際市場に混乱をもたらす可能性がある。そのため、各消費者向け IoT サイバーセキュリティラベルが示すサイバーセキュリティ要件の整合を図るためのサイバーセキュリティラベリングの枠組みが必要とされている。

－枠組み（フレームワーク）の意義

サイバーセキュリティのラベリングフレームワークは、既存の広く使用されている規格（例えば、ETSI EN 303 645、TS 103 701、NIST IR 8259、NIST IR 8259A、NIST IR 8425、ISO/IEC 27400、ISO/IEC 27402）からのサイバーセキュリティ要件を整合させる。このフレームワークに基づいて消費者向け IoT サイバーセキュリティラベリングスキームを実装することで、相互認証とそのプロセスを簡素化することができる。更に、追加の特殊性（テストケースや能力等）を提供するサイバーセキュリティラベリングスキームの実装は、このフレームワークを補完するものである。

- 成果達成の側面

サイバーセキュリティラベリングの枠組みは、以下の側面で成果を達成することを目指している。

－消費者 - 透明性：消費者向け IoT 製品のサイバーセキュリティの提供は、一般消費者には不透明である。サイバーセキュリティのラベリングを利用することで、消費者は消費者向け IoT 製品を購入する際に十分な情報を得た上で選択できる。

－開発者 - ブランディング：サイバーセキュリティのラベリングは、開発者が製品を差別化し、ブランドの質を高めることで、より積極的で持続可能な産業を育成できる。また、開発者にとっては、より安全な製品を製造し、製品にサイバーセキュリティを提供するために費やした努力を収益化するインセンティブとなる。

－経済／エコシステム - 相互承認：デジタル経済の成長に伴い、サイバーセキュリティのラベリングに互換性を持たせることで、国境を越えた重複したテストの必要性を減らし、開発者のコンプライアンスにかかるコストを削減して市場アクセスを向上させ、ラベリングの推進により各国間で相互承認する道を開くことができる。

- 保証の限界

消費者向け IoT 製品のサイバーセキュリティラベリングは、正式なセキュリティ保証を提供するものではない。消費者向け IoT 製品は、そのラベリング状況に関係なく、悪意のある攻撃者によって侵害される可能性がある。より高いセキュリティ保証を求めるユーザー（企業、製造業、産業アプリケーション、ヘルスケア等）は、正式な評価・認証スキーム（ISO/IEC 15408-1:2022 に記載されているもの等）で認証された製品の導入を検討することを強く推奨している。

同規格案は、2025 年を目途に規格化を完了する予定である。

(b) 人工知能システムのセキュリティ脅威に対処するためのガイダンス（ISO/IEC 27090: Cybersecurity – Artificial Intelligence – Guidance for addressing security threats to artificial intelligence systems）

本項では、AI システムのセキュリティ脅威に対処するためのガイダンスを提供する新しい規格である ISO/IEC 27090 について解説する。

（ア）規格の背景

AI システムに対するセキュリティ上の脅威にタイムリーに対処することは、AI システムを使用または開発する組織の信頼性を向上させるだけでなく、AI システムに対する信頼性を向上させることにもつながる。テクノロジーが速いペースで進歩・革新し続ける中、AI システムで生まれる新たなセキュリティの脆弱性を加味し、セキュリティ目標を継続的に評価（見直し）する必要がある。

AI システムにおいては、次の「（イ）AI システムに対する攻撃の例」で記載するような AI 固有の攻撃（脅威）が存在するが、脆弱性を用いた悪用・攻撃等、以前からあるサイバー空間における脅威についても、十分な対策を講じることが必要となる。

AI システムは、組織がデジタルトランスフォーメーション

を採用するにつれて普及し、その結果、これらのシステムに対するサイバー攻撃の可能性が高まっており、AIシステムに対する攻撃の事例が既に報告されている（例えば、電子メール保護システムに対する回避攻撃等）。更に、AIシステムが多目的かつ広範囲に使用されている結果、特にセキュリティが重要視される状況では、サイバー攻撃の結果が深刻なものとなり、場合によっては個人の身体的・精神的被害につながることも考えられる。

AIシステムには、その開発方法とデータへの強い依存性により、従来の情報処理システムと比較して、更なる脆弱性が存在する。このような新たな脅威の状況に対する認識と理解は、敵対的攻撃からAIシステムを保護するために不可欠である。この認識と理解により、AIシステムへの特有の攻撃を軽減することに加え、従来のソフトウェアや情報システムを保護するために使用されている既存のセキュリティ対策もAIシステムに適用することができる。

また、AIシステムにおけるセキュリティ上の脅威や脆弱性は、情報セキュリティ上の危害や、安全性への影響を含むAIシステムの意図しない危険性をもたらす可能性がある。様々な攻撃は、個人への危害をもたらすだけでなく、金銭的な面に加え非金銭的な面でもビジネスに望ましくない影響を与える可能性がある。

（イ）AIシステムに対する攻撃の例

本項では、データポイズニング攻撃とモデルインバージョン攻撃を紹介する。

データポイズニング攻撃は、学習データに不要なデータを注入する攻撃のことで、望ましくない学習結果を引き起こす可能性がある。一般に情報セキュリティの確保を行うためには、ISO/IEC 27001で確立されたベストセキュリティプラクティスを順守することが推奨されるが、AI/ML（Machine Learning：機械学習）対応の作業、データ、及び制御フローには、いくつかの追加的な対応が適切な場合がある。具体的には、アクセス制御のような既存の対策は、許可されたユーザーのみがトレーニングデータにアクセスできることを保証するために使用することができるが、使用されるデータが期待される性能を提供することを保証するためには、更なる対策が必要である。データポイズニングの検出は、このような対策に必要なものとしているが、このような脅威の検知を行うことはしばしば困難である。

モデルインバージョン攻撃は、学習データの再構成により情報漏えい等を促す攻撃である。モデルへの正当なクエリ（query）によって成立するため、従来の効果的な情報セキュリティ対策が実施されている場合でも、モデルや知的財産が盗まれる可能性等があり、従来の情報セキュリティ対策ではリスクが軽減されない。脅威の検知は課題であるが、情報の流出を効果的に軽減するための対策が不可欠になる。

AIの脅威を軽減するために使用される対策には、組織の資産を保護するために複数のセキュリティ対策を活用する多層防御（Defense in depth）の手段を使用することができる。検証されていないデータをトレーニングに使用した場合、データポイズニングやMLのデータや制御フローを調整する攻撃に関連するリスクが高まる可能性がある。

（ウ）規格のスコープと目次

上記の背景に基づき、同規格案のスコープは「1. Scope」において「本規格は、組織が人工知能（AI）システムに特有のセキュリティ上の脅威及び障害に対処するためのガイダンスを提供するものである。本ガイダンスは、AIシステム特有のセキュリティ脅威が、そのライフサイクル全体を通じてどのような結果をもたらすか、また、そのような脅威を検知し緩和する方法について、組織がよりよく理解できるようにするための情報を提供することを目的としている。

また、本規格は、AIシステムを開発または使用する、公共及び民間の企業、政府機関、非営利団体を含む、あらゆる種類及び規模の組織に適用可能である。」と規定されている。

同規格案の内容は、以下の目次で構成される。

1. Scope
2. Normative References
3. Terms and definitions
4. Abbreviated terms
5. Application of information security
6. Threats to AI systems
6.1 General
6.2 Data poisoning attack
6.3 Evasion attack
6.4 Membership inference
6.5 Model exfiltration
6.6 Model inversion
6.7 Scaling attacks
7. Systemic considerations for multiple concurrent mitigations

7.1 Overview
7.2 Conflicting interactions of mitigations
7.3 Continuity of mitigations across the AI life cycle

なお、同規格案は現在 CD 1 の段階にあるが、最新の AI 技術の高度化への追随作業等、更なる規格案の改善が必要と考えられている。

(c) サイバーフィジカルシステム (CPS) のためのセキュリティの枠組み

同プロジェクトは、経済産業省で構築した「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)[※78]」に基づいて、日本の提案により 2020 年 4 月に PWI 5689 として議論を開始した。規格策定に貢献する国の数が不足していることが理由で1度目の投票は否決されたが、タイトルを「Security frameworks and use cases for cyber physical systems (サイバーフィジカルシステムのためのセキュリティの枠組とユースケース)」として、再度 PWI の審議を行い、2023 年 10 月に NP が承認され、現在 WD 1 として審議を進めている段階である。

(d) WG 4 に関連するその他の規格群

WG 4 では、前述の IoT、AI、CPS に関連する課題以外についても、多数の重要な審議を進めている。

以下にその審議課題項目、規格の番号、及び審議状況を示す。

- ビジネス継続のための ICT 準備技術 (27031) : 現在は FDIS の段階
- インターネットセキュリテイガイドライン (27032) : 規格化完了
- ネットワークセキュリティ (27033-7) : ネットワーク仮想化セキュリティのガイドライン。規格化完了
- インシデントマネジメント (27035) : パート 1、パート 2、パート 3 は規格化完了。また、パート 4 (Coordination) は、DIS の段階
- サプライヤー関連セキュリティ (27036) : パート 3 の改版作業は完了
- デジタルエビデンスの識別、収集、確保、保全 (27037) : 改版作業なし
- リダクション (墨消し技術) (27038) : 改版作業なし
- IDPS (侵入検知システム) (27039) : 改版作業なし
- ストレージセキュリティ (27040) : 規格化完了
- 仮想化サーバーの設計／実装のためのセキュリティガイドライン (21878) : 改版作業なし
- 産業用インターネット基盤のためのセキュリティ参照体系 (24392) : 規格化完了
- 仮想化された信頼のルートのためのセキュリティ要件 (27070) : 規格化完了
- 機器とサービス間の信頼接続の構築のためのセキュリティ推奨 (27071) : 規格化完了
- 公開鍵基盤における実践とポリシーの枠組み (27099) : 規格化完了
- データの起源―参照モデル (データ追跡のため) (5181) : 現在は WD 3 の段階
- ビッグデータセキュリティ・プライバシー、データセキュリティマネジメントの枠組みのためのガイドライン : 中国による NP 提案中
- ビッグデータセキュリティ・プライバシー、実施のためのガイドライン : 現在は CD 1 の段階

(5) WG 5 (アイデンティティ管理とプライバシー技術)

WG 5 では、アイデンティティ管理、プライバシー、バイオメトリクスの標準化を行っている。2023 年度の主な活動を紹介する。

(a) アイデンティティ管理

2011 年に初版が発行され、2019 年に改訂された ISO/IEC 24760-1 (アイデンティティ管理のフレームワーク パート 1 : 用語と概念) は、日本が新たに加えるよう提案した「authoritative identifier」を含むいくつかの用語を加えて、2023 年 1 月に追補 (Amendment) が発行された。2016 年に発行された ISO/IEC 24760-3 (アイデンティティ管理のフレームワーク パート 3 : 実践) は、パート 1 及び ISO/IEC 24760-2 (アイデンティティマネジメントの枠組み パート 2 : 参照アーキテクチャ及び要求事項) を踏まえて実務プロセスの指針を整理するものであり、これら別パートの更新状況を反映し、不明瞭であるとされている問題を改善するための追補が 2023 年 2 月に発行された。なお、ISO/IEC 24760-4 (アイデンティティ管理のフレームワーク パート 4 : 認証器、クレデンシャル及びユーザー認証) が 2022 年 7 月に NP として承認され、現在、WD の段階にある。

2016 年に初版が発行された ISO/IEC 29146 (アクセス管理のためのフレームワーク) は、近年のアクセス制御技術に合わせるための改訂を日本が提案し、2024 年 1 月に発行された。

(b)プライバシー

ISO/IEC 29100（プライバシーフレームワーク）の初版が発行された2011年当時は、「引用規格（Normative references）」は任意要素（引用規格がなければ記載しなくてもよい要素）であったが、「ISO/IEC 専門業務用指針 第2部」の改訂（第7版（2016年版））によって引用規格が強制要素となった。引用規格を盛り込むこと、及び間違った記載を修正した追補を本文に反映することにより、無償で取得可能なISO/IEC 29100のみで正しいテキストが分かるようISO/IEC 29100改訂の必要性を日本が訴えたため、改訂されることとなった。日本の﨑村夏彦主査がエディターを務め改訂作業を行い、2024年2月、第2版が発行された。

ISO/IEC 27701は、2019年に初版が発行された。同規格は、SC27 WG 1が開発した国際規格であるISO/IEC 27001及びISO/IEC 27002に、プライバシー対策に関する要求事項及びプラクティスを加えて拡張することにより、組織によるプライバシー情報マネジメントシステム（PIMS：Privacy Information Management System）の構築を支援することを目的としている。2022年2月にISO/IEC 27002:2022が発行されたことに伴い、主にISO/IEC 27002:2022に整合させることに特化した改訂のみを行う予定であったが、ISO中央事務局より、ISO/IEC 27701はタイプA（要求事項を提供する）マネジメントシステム規格（MSS）であるため、Annex SL（マネジメントシステム規格を調和させるアプローチ）に則った構成に書き換えるよう指示があり、2024年4月の国際会議でDISのコメントの処理が行われた。

(c)バイオメトリクス

モバイル機器上でのバイオメトリクスを使った認証に対するセキュリティ要件を定めるプロジェクトISO/IEC 27553は、バイオメトリック照合結果に関する情報以外はモバイル機器から外に出ないパート1（Local modes）が2022年11月に発行され、モバイル機器間やリモートサービスも含めてバイオメトリック照合する場合を扱うパート2（Remote modes）が、現在DISの段階にある。

2.4.3 情報通信技術、電気通信に関わるセキュリティ規格の標準化（ITU-T SG17）

ITU-Tにおいてセキュリティを担当するSG17は、以下の五つの作業グループ（WP：Working Party）で構成され、各WPは2～3の小グループ（課題：Question）を持っている。

- WP1：セキュリティ戦略と連携
  - Q1：セキュリティ標準化戦略と連携
  - Q15：量子技術のセキュリティを含む新興テクノロジーのための、または、新興テクノロジーによるセキュリティ
- WP2：5G、IoT、ITS セキュリティ
  - Q2：セキュリティアーキテクチャとネットワークセキュリティ
  - Q6：電気通信サービスとIoTのためのセキュリティ
  - Q13：ITSセキュリティ
- WP3：サイバーセキュリティとセキュリティ管理
  - Q3:電気通信のための情報セキュリティ管理とセキュリティサービス
  - Q4：サイバーセキュリティとスパム対策
- WP4：サービスとアプリケーションのセキュリティ
  - Q7：安全なアプリケーションサービス
  - Q8：クラウドコンピューティングとビッグデータ基盤のセキュリティ
  - Q14：分散台帳技術（DLT）のセキュリティ
- WP5：基本的なセキュリティ技術
  - Q10：ID管理とテレバイオメトリクスのアーキテクチャ/メカニズム
  - Q11：アプリケーションの安全性を確保するための一般的な技術（ディレクトリ、PKI、形式記述言語、OID等）

ITU-Tの標準化作業（勧告作成作業）は、新たな勧告作成のためのWI（Working Item）立ち上げ提案から開始し、WIで作成されたドラフト文書に対してITU-Tのメンバーが修正・追記提案を寄書として提出し、議論の結果をエディターが編集してドラフト文書が更新される。ドラフト文書の作成が完了した段階で承認手続きに進み、承認されれば勧告として発行される。承認手続きにはTAP（Traditional Approval Process：伝統的承認手続）とAAP（Alternative Approval Process：代替承認手続）の2種類がある。AAPは2008年に制定され、迅速な勧告発行が可能となる主要な承認手続きとなっている。会合で勧告発行が合意された後に各国に照会が行われ、コメントがなければ勧告発行となる。TAPは主に規制や政策に関する事項を含む勧告案の承認に適用され、会合での勧告発行合意後、英語以外の5ヵ国語に翻訳され、各国に対して協議を依頼する。次回の会合直前まで投票を受け付け、返答の70%以上の賛同が得られて会合で反対がなければ勧告として発行される

ことになる※379。

ITU-T では勧告のほかに、勧告文書に対して補助的な情報を提供する「補足文書」、仕様ではないが技術的な情報を含む「テクニカルレポート」等が作成されている。

以下に、活動概要と 2023 年度に注目された主な活動について述べる。

(1) WP1 (セキュリティ戦略と連携)

WP1 は、SG17 内、ITU-T 内、及び外部の団体との連携と SG17 全体の戦略を検討する Q1 と、量子技術を含む新しい技術に対するセキュリティ検討を行う Q15 から構成されている。

(a) 量子鍵配送 (QKD) に関する状況 (Q15)

ITU-T では量子鍵配送 (QKD : Quantum Key Distribution) に関わる標準化活動を積極的に進めており、SG13 (Future networks and emerging network technologies) においてフレームワーク技術について、SG17 においてセキュリティ関連の技術について勧告化を進めている。Q15 では日本の研究機関、及び企業が積極的に寄書を提出し、勧告作成をリードしている。2023 年までに、SG17 では以下の勧告を作成した。

- X.1710: Security framework for quantum key distribution networks
- X.1712: Security requirements and measures for quantum key distribution networks – key management
- X.1714: Key combination and confidential key supply for quantum key distribution networks
- X.1715: Security requirements and measures for integration of quantum key distribution network (QKDN) and secure storage network

更に、5 件の新たな勧告作成が進められている。

(b) 新興テクノロジーのための、または、新興テクノロジーによるセキュリティ (Q15)

セキュリティが必要とされる分野は広いため、各課題に属さない新しい技術分野のセキュリティ検討を即座に着手できるようにするため、Q15 ではどの課題 (Q) でも研究項目となっていない分野の寄書作成を提案可能となっている。以下は、2023 年に開始した勧告案作成作業の一部である。

- X.so-sap: Guidelines for security orchestration of service access process
- X.gcspcc: Guidelines of developing of cybersecurity simulation platform based on cloud computing
- X.SecaaS: Security threats to be identified in the domain of security as a service
- X.dtns: Guidelines of using digital twin of network for network security
- X.sr-ai: Security requirements for AI systems

対象となる分野は多岐にわたっているが、2023 年度は AI とサプライチェーンのセキュリティに関するワークショップを SG17 として開催したため、これらに関する勧告作成提案が行われた。AI セキュリティに関しては、X.sr-ai の勧告作成が開始されたが、この勧告案では、AI システムのライフサイクルを六つのステージに分け、ライフサイクルに基づいた AI システムモデルを示すとともに、ライフサイクルの各段階に責任を持つ利害関係者を特定し、ライフサイクルの六つの段階を考慮したセキュリティ上の脅威を提示する。そして、関連する利害関係者を支援するために、一連のセキュリティ要件を提供することとしている。

(2) WP2 (5G、IoT、ITS セキュリティ)

WP2 は、各種のネットワークに関するセキュリティを取り扱う。

5G への進化により、モバイルとインターネットの融合が進むとともに、ネットワークへの新たな機能の追加、及び仮想化等のネットワークインフラの変化が進み、4G 世代に比べて大きな変化が見られている。このため、セキュリティについても注目され、ITU-T においても 5G ネットワークの全体的な視点からセキュリティの検討を行っている。

「5G セキュリティ (Q2)」では、2023 年においては、総務省が作成した「5G セキュリティガイドライン」をベースに日本が主導的に作成を進めてきた勧告 X.1818 (Security controls for operation and maintenance of IMT-2020/5G network systems) の承認手続きが進められている。

(3) WP3 (サイバーセキュリティとセキュリティ管理)

WP3 は、ネットワークに対する攻撃の検知・防御を行うためのサイバーセキュリティと、ISMS に基づいたテレコムサービスを対象としたセキュリティ管理を取り扱う。

(a) STIX/TAXII (Q4)

サイバー攻撃活動の情報を交換するための仕組みとして、国際的な標準化団体であるOASIS (Organization for the Advancement of Structured Information Standards Group) で規格化されているSTIX (Structured Threat Information eXpression)、TAXII (Trusted Automated eXchange of Indicator Information) のITU-T勧告化が進められているが、ロシアからのコメント対応のため勧告成立が遅れている。

(b) サプライチェーンセキュリティ (Q4)

2023年2月の会合より、ソフトウェアのサプライチェーンセキュリティに関する勧告作成を開始した。現在、以下の3件の勧告作成が進められている。

- X.ssc-sra: Guidelines for software supply chain security audit
- X.st-ssc: Security threats of software supply chain
- X.rm-sup: Risk management on the security of software supply-chain for telecommunication organizations

(4) WP4 (サービスとアプリケーションのセキュリティ)

「Distributed Ledger Technology (DLT) (Q14)」では、ブロックチェーンのコア技術として使われている分散台帳技術 (DLT) について、DLT自体のセキュリティ検討、及びDLTを利用したセキュリティ対策の検討が行われている。これまでに、DLTのセキュリティフレームワーク、DLTの脅威分析に関する勧告が発行されるとともに、DLTを利用したオンライン支払い、オンライン投票等、13件の勧告が作成されている。2023年においては、異なるDLTシステムを相互運用するためのDLTゲートウェイシステム (X.DLT-dgi: Security requirements of DLT gateway for interoperability) の議論を開始した。

(5) WP5 (基本的なセキュリティ技術)

「ID管理に関連するデファクト標準の勧告化 (Q10)」では、ID管理についてデファクト標準で利用されている仕様の勧告化を積極的に行っている。標準化のための業界団体であるFast Identity Online Alliance (FIDO) が作成したUAF (Universal Authentication Framework)、U2F (Universal Second Factor) はX.1277.2、X.1278.2として勧告化された。また、ID管理エコシステムの構成要素間のシームレスな接続を可能にするオープンスタンダードなインターフェース (API) セットであるOSIA Version 6.1.0をITU-T勧告とし、「X.1281: APIs for interoperability of identity management systems」として2023年に発行が承認された。

2.4.4 制御システム関連のセキュリティ規格の標準化 (IEC TC 65/WG 10)

近年の制御システムは、情報システム同様に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) が進んだことで、サイバー攻撃の脅威に晒されるようになった。こうした動向に伴い、制御システムにおいてもリスク分析に基づくセキュリティ対策が喫緊の課題となっている。これについて、日米欧各国の政府機関・業界団体が取り組みを進めているが、本項では制御システムのセキュリティの国際標準について述べる。

(1) ISA/IEC 62443シリーズの概要

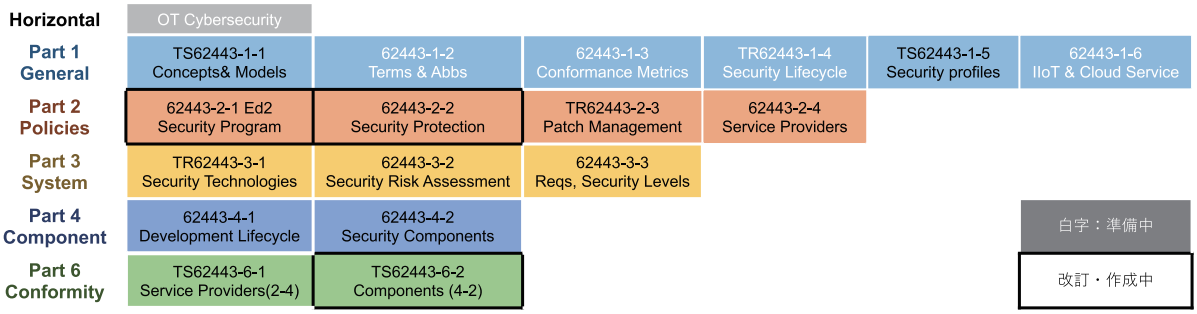
制御システムのセキュリティを包括的に網羅した国際標準「工業通信ネットワーク - ネットワーク及びシステムセキュリティ (ISA/IEC 62443)」は、ISA (International Society of Automation：国際自動制御学会) 99 Committee※380とIEC Technical Committee 65 Working Group10 (TC 65/WG 10)※381により作成されているため、ISA/IEC 62443-X-Yと記載される。

ISA/IEC 62443は大別して五つのグループに分類され、発行済みと策定・準備中のものを合わせて17の規格が存在する (次ページ図2-4-4)。

ISA/IEC 62443は、産業制御システムをサイバー攻撃から守るために開発された。規格の議論を始めた2002年頃は、市販OSや汎用プロトコルが狙われやすいとして、それらの対策方針について検討された。しかし、2011年になって各社独自技術を用いた制御システムやコントローラーがサイバー攻撃を受けるようになり※384、制御システム全般のサイバー脅威への基本的概念から分析と対策の手順、マネジメントや機器機能等、幅広い要求を扱うようになった。同規格を参照して、鉄道や機械等の分野規格の開発も進んでおり、産業システムのサイバーセキュリティの基本規格として位置付けられている。

(2) 各グループの概要と状況

ISA/IEC 62443のグループごとの概要と2023年度の検討状況について紹介する。



■図 2-4-4　ISA/IEC 62443 シリーズ文書の発行・改定状況（概要）
（出典）星野浩志、藤田淳也、神余浩夫「IEC 62443 制御システムセキュリティ規格の現状※382」（「制御システムセキュリティカンファレンス 2023※383」講演資料）を基に執筆者が編集

(a) ISA/IEC 62443-1 グループ（一般）

ISA/IEC 62443 の中で用いられる用語の解説や、制御システムのセキュリティ動向、地理的に分散したフィールド機器を遠隔から集中監視制御する SCADA※385 モデルの一般論等を規定している。このグループは、事業者やシステムインテグレーター、機器ベンダー等、すべての関係者が共通して参照する規格である。2023 年 9 月に「1-5 分野別プロファイル作成のためのガイド」が発行された。新たに「1-6 IIoT とクラウドシステム」が準備中である。

(b) ISA/IEC 62443-2 グループ（ポリシーと手順）

事業者や運用者等の組織を対象とした、主にマネジメントに関連するセキュリティ要求事項等を規定した規格であり、組織としてのセキュリティマネジメントシステムの確立や、パッチ管理等の運用に関連する事項が記載されている。「2-4 サービスプロバイダーへの要求」が 2023 年 12 月に発行、「2-1 制御システム設備オーナーへの要求」の改訂版が近く発行の見込みである。

(c) ISA/IEC 62443-3 グループ（システム）

複数の機器や製品を組み合わせて運用する制御システムを対象とした規格である。

ISA/IEC 62443-3-3 は、ISA/IEC TS 62443-1-1 で規定される基礎的要求事項（FR：Foundational Requirement）に対応する形で、システムの技術的なセキュリティ要求事項を規定している。要求事項は、システム要件（SR：System Requirement）と強化策（RE：Requirement Enhancement）から構成され、各要求事項にセキュリティレベル（SL：Security Level）が割り当てられている。SL は、それぞれの要求事項を満たした場合に、どのような攻撃からシステムを保護できるかを示すものである。4 段階の SL が規定されており、最も高度な要求事項を満たすものをレベル 4 としている。

(d) ISA/IEC 62443-4 グループ（コンポーネント）

制御システムを構成する個別コンポーネント（機器や装置）を対象とした規格であり、主にコンポーネントのライフサイクルの各フェーズにおけるセキュリティ要求事項や、搭載されるセキュリティ機能等に関する事項が記載されている。

(e) ISA/IEC 62443-6 グループ（コンフォーミティ）

製品等の規格適合性評価の方法を開発する IECEE（IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components）※386 のワーキンググループから IEC TC 65/WG 10 へ依頼されたことをきっかけに基準作成を行っている。IEC 62443 要件準拠の基準や基準を満たすことのエビデンスの確認方法について具体化している。

(3) ISA/IEC 62443 の活用

2023 年度は、様々な業界での ISA/IEC 62443 の活用が進展し、電力、化学、石油、ビル、鉄道等におけるセキュリティ標準の開発が進んでいる。また各国での第三者評価・認証（ISASecure※387、IECEE の ISA/IEC 62443 関係認証）での活用を見据えての評価認証におけるセキュリティ評価手法の開発も進んでいる。重要インフラや産業システムのサイバーセキュリティ対策は、各国の緊急課題であり、法整備や制度開発が急がれる。

COLUMN

デジタル署名が付いたウイルスの広がり

デジタル署名は、暗号技術を利用して情報の完全性を電子的に保証するための技術です。この技術は、プログラムやモジュール、ドライバー等が製造時から改変されていないことを製造ベンダーが証明するためにも利用され、このような使われ方をした場合は特に「コード署名」と呼ばれます。そのため、正当なコード署名が付いたプログラムであれば、多くの場合、OS は正しいプログラムとして利用者の確認を求めることなく自動的に実行します。逆に言えば、もしコード署名が悪用され、ウイルスに「正しいと判定される」コード署名が付いていた場合、OS はウイルスを正しいプログラムと誤認して実行してしまいます。実際、2010 年代には、国家が支援している（と思われる）組織により、「正しいと判定される」コード署名付きのウイルス（Stuxnet や Flame 等）が標的型攻撃ツールとして敵対国に送り込まれたことがあります。

ただ、今までは標的型攻撃ツール以外でコード署名を付けたウイルスはあまり検知されていませんでした。その理由として考えられるのは、コード署名をするときに使った署名鍵の「所有者情報」が、当該署名を検証するために使う「証明書」に記載されていることです。このことは、攻撃者にとって自らの身元を晒すということであり、コード署名を悪用することのハードルになっていたと思われます。そのため、もし攻撃者が身元を隠したままコード署名を悪用しようとすれば、一番考えられる方法は何らかの理由で漏えいした署名鍵を使ってコード署名をすることでした。もっともこのケースでは、漏えいした署名鍵と対応する証明書を失効させればそれ以降は「正しいと判定される」コード署名は作れなくなるし、そもそも署名鍵が漏えいしないようにハードウェア的な対策も進んでいるので、このケースのリスクは今後、更に低減していくものと思われます。

ところが、トレンドマイクロ株式会社の調査[i]によれば、最近になってコード署名を付けたウイルスが少しずつ広がりを見せています。その要因の一つとして、何らかの理由で攻撃者が施したコード署名が「正しいと判定される」ような「不正な証明書が発行」されたケースの存在が挙げられます。例えば、英語圏で一般人を狙ってサイバー犯罪グループが利用しているウイルス QAKBOT（クアックボット）に、複数の一般企業の証明書によって「正しいと判定される」コード署名を付けて配布していることが確認されています。この事例では、気付かれずに「正当な一般企業」になりすまして、当該企業の証明書を不正取得した形跡がありました。

クラウドでのリモート署名サービスに「不正アクセスしてリモート署名を行う」ケースも存在します。本来は漏えいしないようにハードウェア的な対策が取られているはずの署名鍵を利用したコード署名を付けたウイルスも断続的に観測されています。こちらは、ハードウェア内にしか存在しないはずの署名鍵に攻撃者がリモートでアクセスできることを意味しています。

なりすまされた企業は被害者といえますが、対外的には当該企業が作成したウイルスと認識されて、信用に関わる問題となる恐れがあります。また、どのケースも、もとをたどると「なりすまし」に起因すると考えられるので、特に企業では、証明書の管理者やコード署名を作成できる利用者のアカウント管理を強化する必要があります。

i　トレンドマイクロ株式会社：Attack Signals Possible Return of Genesis Market, Abuses Node.js, and EV Code Signing
https://www.trendmicro.com/en_us/research/23/k/attack-signals-possible-return-of-genesis-market.html〔2024/5/31 確認〕

※ 1　https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf〔2024/5/2 確認〕
※ 2　サイバーセキュリティ戦略本部：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〔2024/5/2 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」を改訂しました　https://www.meti.go.jp/press/2022/03/20230324002/20230324002.html〔2024/5/2 確認〕
※ 4　IPA：サイバーセキュリティ経営ガイドライン Ver 3.0 実践のためのプラクティス集　https://www.ipa.go.jp/security/economics/csm-practice.html〔2024/5/2 確認〕
※ 5　https://www.soumu.go.jp/main_content/000630516.pdf〔2024/5/2 確認〕
※ 6　https://www.nisc.go.jp/pdf/policy/infra/shishin202307.pdf〔2024/5/2 確認〕
※ 7　IPA：サイバーセキュリティお助け隊サービス制度　https://www.ipa.go.jp/security/sme/otasuketai/index.html〔2024/5/2 確認〕
※ 8　IPA：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）とは　https://www.ipa.go.jp/security/sc3/about/〔2024/5/2 確認〕
※ 9　経済産業省：地域 SECUNITY（セキュリティ・コミュニティ）　https://www.meti.go.jp/policy/netsecurity/secunity.html〔2024/5/2 確認〕
※ 10 Software Bill of Materials（SBOM）：ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト。
※ 11 経済産業省：「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」を策定しました　https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html〔2024/5/2 確認〕
※ 12 KDDI 株式会社、株式会社 KDDI 総合研究所、富士通株式会社、日本電気株式会社、株式会社三菱総合研究所：サイバーセキュリティーの強化を目的に通信分野への SBOM 導入に向けた実証事業に着手　https://news.kddi.com/kddi/corporate/newsrelease/2023/08/01/6897.html〔2024/5/2 確認〕
※ 13 https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html〔2024/5/2 確認〕
※ 14 https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun4.pdf〔2024/5/2 確認〕
※ 15 総務省：無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について　https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/〔2024/5/2 確認〕
※ 16 https://www3.fmmc.or.jp/e-netcaravan/〔2024/5/2 確認〕
※ 17 一般財団法人マルチメディア振興センター：e- ネットキャラバンとは　https://www3.fmmc.or.jp/e-netcaravan/about/〔2024/5/2 確認〕
※ 18 警察庁：ランサムウェア LockBit による暗号化被害データに関する復号ツールの開発について　https://www.npa.go.jp/news/release/2024/release2.pdf〔2024/5/2 確認〕
※ 19 https://notice.go.jp〔2024/5/2 確認〕
※ 20 e-gov 法令検索：令和六年政令第二十六号　https://elaws.e-gov.go.jp/document?lawid=506CO0000000026_20240401_000000000000000〔2024/5/2 確認〕
※ 21 https://cynex.nict.go.jp〔2024/5/2 確認〕
※ 22 総務省：5G セキュリティガイドライン第 1 版　https://www.soumu.go.jp/main_content/000812253.pdf〔2024/5/2 確認〕
※ 23 厚生労働省：医療情報システムの安全管理に関するガイドライン第 6.0 版（令和 5 年 5 月）　https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html〔2024/5/2 確認〕
※ 24 国土交通省：水道分野におけるサイバーセキュリティ対策　https://www.mlit.go.jp/mizukokudo/watersupply/stf_seisakunitsuite_bunya_topics_bukyoku_kenkou_suido_kikikanri_sisin.0005.html〔2024/5/2 確認〕
厚生労働省：「生活衛生等関係行政の機能強化のための関係法律の整備に関する法律」の公布について（通知）　https://www.mhlw.go.jp/content/10900000/001100963.pdf〔2024/5/2 確認〕
※ 25 デジタル庁：マイナポータル API 仕様公開サイト　https://myna.go.jp/html/api/index.html〔2024/5/2 確認〕
※ 26 デジタル庁：マイナポータルのトップページが新しくなりました　https://services.digital.go.jp/mynaportal/news/20240324-01/〔2024/5/2 確認〕
※ 27 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〔2024/5/2 確認〕
※ 28 総務省：政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業（CYXROSS）　https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00381〔2024/5/2 確認〕
※ 29 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　https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf〔2024/5/2 確認〕
※ 30 NISC：重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書　https://www.nisc.go.jp/pdf/policy/infra/rmtebiki202307.pdf〔2024/5/2 確認〕
※ 31 一般社団法人日本シーサート協議会、NISC 分野横断的演習実行委員会：2023 年 NISC/NCA 連携分野横断的演習 開催報告　https://www.nca.gr.jp/activity/event/2024/2023_niscnca_1/〔2024/5/2 確認〕
※ 32 NII：ストラテジックサイバーレジリエンス研究開発センター　https://www.nii.ac.jp/research/centers/cyberresilience/〔2024/5/2 確認〕
※ 33 NISC：サイバーセキュリティ協議会　https://www.nisc.go.jp/council/cs/kyogikai/index.html〔2024/5/2 確認〕
※ 34 外務省：G7 広島サミット 2023　https://www.mofa.go.jp/mofaj/gaiko/summit/hiroshima23/〔2024/5/2 確認〕
※ 35 電波新聞デジタル：重要インフラに迫るサイバー攻撃の脅威に備える　官民が大規模な合同演習　https://dempa-digital.com/article/502932〔2024/5/2 確認〕
※ 36 JIJI.COM：サイバー攻撃対処、官民で訓練　インフラ事業者が参加―警視庁　https://www.jiji.com/jc/article?k=2024020500600&g=soc#goog_rewarded〔2024/5/2 確認〕
※ 37 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　https://www.meti.go.jp/press/2023/10/20231006009/20231006009.html〔2024/5/2 確認〕
※ 38 防衛省：国家防衛戦略について　https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy.pdf〔2024/5/2 確認〕
※ 39 防衛装備庁：防衛産業サイバーセキュリティ基準の整備について　https://www.mod.go.jp/atla/cybersecurity.html〔2024/5/2 確認〕
※ 40 外務省：第 30 回 ASEAN 地域フォーラム（ARF）閣僚会合　https://www.mofa.go.jp/mofaj/a_o/rp/page1_001769.html〔2024/5/2 確認〕
※ 41 例えば International Watch and Warning Network（IWWN）、Forum of Incident Response and Security Teams（FIRST）。
※ 42 内閣府：経済安全保障重要技術育成プログラム　https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html〔2024/5/2 確認〕
※ 43 内閣府：経済安全保障重要技術育成プログラムに係る研究開発ビジョン（第一次）　https://www8.cao.go.jp/cstp/anzen_anshin/1_vision_gaiyou.pdf〔2024/5/2 確認〕
※ 44 内閣府、文部科学省：「サプライチェーンセキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）」に関する研究開発構想（個別研究型）　https://www8.cao.go.jp/cstp/anzen_anshin/20230310_mext_2.pdf〔2024/5/2 確認〕
※ 45 内閣府、文部科学省：「人工知能（AI）が浸透するデータ駆動型の経済社会に必要な AI セキュリティ技術の確立」に関する研究開発構想（個別研究型）　https://www8.cao.go.jp/cstp/anzen_anshin/20221021_mext_3.pdf〔2024/5/2 確認〕
※ 46 内閣府、経済産業省：「先進的サイバー防御機能・分析能力強化」に関する研究開発構想（プロジェクト型）　https://www8.cao.go.jp/cstp/anzen_anshin/02-06_20231020_meti_4.pdf〔2024/5/2 確認〕
※ 47 内閣府、経済産業省：「偽情報分析に係る技術の開発」に関する研究開発構想（個別研究型）　https://www8.cao.go.jp/cstp/anzen_anshin/02-07_20231020_meti_5.pdf〔2024/5/2 確認〕
※ 48 内閣府、文部科学省：「セキュアなデータ流通を支える暗号関連技術（高機能暗号）」に関する研究開発構想（個別研究型）　https://www8.cao.go.jp/cstp/anzen_anshin/4_20231225_mext.pdf〔2024/5/2 確認〕
※ 49 国立研究開発法人量子科学技術研究開発機構：SIP 第 3 期「先進的量子技術基盤の社会課題への応用促進」課題に係る公募について　https://www.qst.go.jp/site/collaboration/sip-230512.html〔2024/5/2 確認〕
※ 50 CRYPTREC：CRYPTREC とは　https://www.cryptrec.go.jp/about.html〔2024/5/2 確認〕
※ 51 内閣府：経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）　https://www.cao.go.jp/keizai_anzen_hosho/〔2024/5/2 確認〕
※ 52 内閣府：特許出願の非公開に関する制度　https://www.cao.go.jp/keizai_anzen_hosho/patent.html〔2024/5/2 確認〕
※ 53 日本経済新聞：経済安保法、基幹インフラに港湾事業追加　国交省方針　https://www.nikkei.com/article/DGXZQOUA2489C0U4A120C2000000/〔2024/5/2 確認〕
※ 54 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）　https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf〔2024/5/2 確認〕
※ 55 内閣官房：経済安全保障分野におけるセキュリティ・クリアランス

制度等に関する有識者会議　https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/index.html〔2024/5/2 確認〕
※ 56 内閣官房：重要経済安保情報の保護及び活用に関する法律案 https://www.cas.go.jp/jp/houdou/pdf/20240227_siryou.pdf〔2024/5/2 確認〕
※ 57 NHK：「セキュリティークリアランス」法案 衆議院本会議で可決 https://www3.nhk.or.jp/news/html/20240409/k10014416721000.html〔2024/5/2 確認〕
※ 58 https://www8.cao.go.jp/cstp/ai/aistratagy2019.pdf〔2024/5/2 確認〕
※ 59 内閣府統合イノベーション戦略推進会議：「AI戦略 2021 ～人・産業・地域・政府全てにAI～（「AI戦略 2019」フォローアップ）」 https://www8.cao.go.jp/cstp/ai/aistrategy2021_honbun.pdf〔2024/5/2 確認〕
※ 60 https://www8.cao.go.jp/cstp/ai/aistrategy2022_honbun.pdf〔2024/5/2 確認〕
※ 61 https://www8.cao.go.jp/cstp/ai/ronten_honbun.pdf〔2024/5/2 確認〕
※ 62 内閣府：AI戦略会議　https://www8.cao.go.jp/cstp/ai/ai_senryaku/ai_senryaku.html〔2024/5/2 確認〕
※ 63 内閣府 科学技術・イノベーション推進事務局、IPA AI セーフティ・インスティテュート：AI セーフティ・インスティテュート（AISI）の今後の活動について　https://www8.cao.go.jp/cstp/ai/aisi/siryo2.pdf〔2024/5/2 確認〕
AI セーフティ・インスティテュート：https://aisi.go.jp〔2024/5/2 確認〕
※ 64 デジタル庁：デジタル社会推進標準ガイドライン　https://www.digital.go.jp/resources/standard_guidelines/〔2024/5/1 確認〕
※ 65 https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf〔2024/5/1 確認〕
※ 66 https://www.digital.go.jp/resources/standard_guidelines/#ds200〔2024/5/1 確認〕
※ 67 https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf〔2024/5/1 確認〕
※ 68 https://www.digital.go.jp/resources/standard_guidelines/#ds310〔2024/5/1 確認〕
※ 69 https://www.digital.go.jp/resources/standard_guidelines/#ds211〔2024/5/1 確認〕
※ 70 https://www.digital.go.jp/resources/standard_guidelines/#ds221〔2024/5/1 確認〕
※ 71 https://mas.owasp.org/MASVS/〔2024/5/1 確認〕
※ 72 https://www.meti.go.jp/press/2022/03/20230330002/20230330002-1.pdf〔2024/5/1 確認〕
※ 73 https://www.digital.go.jp/resources/standard_guidelines/#ds202〔2024/5/1 確認〕
※ 74 https://www.digital.go.jp/resources/standard_guidelines/#ds910〔2024/5/1 確認〕
※ 75 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/001_05_00.pdf〔2024/5/1 確認〕
※ 76 https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html〔2024/5/1 確認〕
※ 77 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/008_03_00.pdf〔2024/5/1 確認〕
※ 78 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〔2024/5/1 確認〕
※ 79 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/006_05_00.pdf〔2024/5/1 確認〕
※ 80 経済産業省：第 16 回産業サイバーセキュリティ研究会ワーキンググループ 1 ビルサブワーキンググループ　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/016.html〔2024/5/1 確認〕
※ 81 経済産業省：第 16 回 産業サイバーセキュリティ研究会ワーキンググループ 1（制度・技術・標準化）電力サブワーキンググループ　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/016.html〔2024/5/1 確認〕
※ 82 一般社団法人日本自動車工業会：自動車産業サイバーセキュリティガイドライン　https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html〔2024/5/1 確認〕
※ 83 経済産業省：産業サイバーセキュリティ研究会 ワーキンググループ 1（制度・技術・標準化）宇宙産業サブワーキンググループ 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/20230331_report.html〔2024/5/1 確認〕
※ 84 経済産業省：産業サイバーセキュリティ研究会 ワーキンググループ 1（制度・技術・標準化）宇宙産業サブワーキンググループ 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/20240328_report.html〔2024/5/1 確認〕
※ 85 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〔2024/5/1 確認〕
※ 86 https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_appendix.pdf〔2024/5/1 確認〕
※ 87 経済産業省：第 12 回 サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/012.html〔2024/5/1 確認〕
※ 88 経済産業省：第 10 回 産業サイバーセキュリティ研究会 ワーキンググループ 2（経営・人材・国際）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/010.html〔2024/5/1 確認〕
※ 89 https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔2024/5/1 確認〕
※ 90 IPA：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〔2024/5/1 確認〕
※ 91 IPA：経営者向けインシデント対応机上演習　https://www.ipa.go.jp/security/seminar/sme/ttx-e.html〔2024/5/1 確認〕
※ 92-1 IPA：IT・セキュリティ担当者向けリスク分析ワークショップ https://www.ipa.go.jp/security/seminar/sme/riskassesmentws.html〔2024/5/1 確認〕
※ 92-2 経済産業省：第 10 回 産業サイバーセキュリティ研究会 ワーキンググループ2（経営・人材・国際）事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/010_03_00.pdf〔2024/06/07 確認〕
※ 93 IPA：サイバーセキュリティお助け隊サービス制度　https://www.ipa.go.jp/security/sme/otasuketai-about.html〔2024/5/1 確認〕
※ 94 IPA：お知らせ：サイバーセキュリティお助け隊サービスに新たな類型（2類）を創設しました　https://www.ipa.go.jp/pressrelease/2023/press20240315.html〔2024/5/1 確認〕
※ 95 https://www.ipa.go.jp/security/service_list.html〔2024/5/1 確認〕
※ 96 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〔2024/5/1 確認〕
※ 97 IPA：IT セキュリティ評価及び認証制度（JISEC）　https://www.ipa.go.jp/security/jisec/index.html〔2024/5/1 確認〕
※ 98 https://www.meti.go.jp/press/2023/03/20240315005/20240315005-3r.pdf〔2024/5/1 確認〕
※ 99 IPA：コラボレーション・プラットフォームについて　https://www.ipa.go.jp/security/seminar/collapla.html〔2024/5/1 確認〕
※ 100 経済産業省：「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」に対する意見募集の結果及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の公表　https://www.meti.go.jp/press/2022/03/20230308006/20230308006.html〔2024/5/1 確認〕
※ 101 経済産業省：産業サイバーセキュリティ研究会 サイバー攻撃による被害に関する情報共有の促進に向けた検討会 報告書等　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/20231122_report.html〔2024/5/1 確認〕
※ 102 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。
※ 103 https://www8.cao.go.jp/cstp/aigensoku.pdf〔2024/5/1 確認〕
※ 104 総務省：国際的な議論のための AI 開発ガイドライン案（AI 開発ガイドライン）　https://www.soumu.go.jp/main_content/000499625.pdf〔2024/5/1 確認〕
※ 105 総務省：AI 利活用ガイドライン　https://www.soumu.go.jp/main_content/000809595.pdf〔2024/5/1 確認〕
※ 106 経済産業省：AI 原則実践のためのガバナンス・ガイドライン https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_1.pdf〔2024/5/1 確認〕
※ 107 経済産業省：「AI 事業者ガイドライン（第 1.0 版）」を取りまとめました　https://www.meti.go.jp/press/2024/04/20240419004/20240419004.html〔2024/5/1 確認〕
総務省：「AI 事業者ガイドライン」掲載ページ　https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html〔2024/5/1 確認〕
※ 108 経済産業省：不正競争防止法 直近の改正（令和5年）　https://www.meti.go.jp/policy/economy/chizai/chiteki/kaisei_recent.html〔2024/5/1 確認〕

※ 109 経済産業省：不正競争防止法等の一部を改正する法律【知財一括法】の概要　https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/r5kaisei06.pdf〔2024/5/1 確認〕
※ 110 経済産業省：限定提供データに関する指針　https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf〔2024/5/1 確認〕
※ 111 経済産業省：「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」を取りまとめました　https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html〔2024/5/1 確認〕
※ 112 経済産業省：「クレジットカード・セキュリティガイドライン」が改訂されました　https://www.meti.go.jp/press/2023/03/20240315002/20240315002.html〔2024/5/1 確認〕
※ 113 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〔2024/5/1 確認〕
※ 114 経済産業省：技術情報管理認証制度 専門家派遣事業のご案内　https://r4.outreach.go.jp/tics-haken.html〔2024/5/1 確認〕
※ 115 経済産業省：情報セキュリティサービス審査登録制度　https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html〔2024/5/1 確認〕
※ 116 経済産業省：情報セキュリティサービス基準第 4 版　https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun4.pdf〔2024/5/1 確認〕
※ 117 経済産業省：情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示 第 3 版　https://www.meti.go.jp/policy/netsecurity/shinsatouroku/reiji3.pdf〔2024/5/1 確認〕
※ 118 審査登録機関：「情報セキュリティサービスに関する審査登録機関基準」に適合すると IPA が確認した機関。なお、申請事業者が「情報セキュリティサービス基準」に適合するか否かの審査・判定は、各審査登録機関がその責任において実施する。
※ 119 https://www.nisc.go.jp/pdf/policy/general/guider5.pdf〔2024/5/1 確認〕
※ 120 SIG（Special Interest Group）：「特定の分野（各業界におけるサイバー攻撃に関する情報）について、情報を交換するグループ」という意味で、J-CSIP では各業界の参加組織の集合体を SIG と呼んでいる。
※ 121 セプターカウンシル：重要インフラのセキュリティ対策向上を図るために、各重要インフラ分野（セプター）の代表から構成された協議会で、政府機関等から独立した、分野横断的な情報共有体制。
※ 122 https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q3-report.pdf〔2024/5/31 確認〕
※ 123 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023 年 7 月～ 9 月］　https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q2-report.pdf〔2024/5/1 確認〕
※ 124 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023 年 4 月～ 6 月］　https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q1-report.pdf〔2024/5/1 確認〕
※ 125 警察庁：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf〔2024/5/1 確認〕
※ 126 IPA：J-CRAT 標的型サイバー攻撃特別相談窓口　https://www.ipa.go.jp/security/todokede/tokubetsu.html〔2024/5/1 確認〕
※ 127 IPA：サイバーレスキュー隊 J-CRAT（ジェイ・クラート）について　https://www.ipa.go.jp/security/j-crat/about.html〔2024/5/1 確認〕
※ 128 経済産業省：「高圧ガス保安法等の一部を改正する法律案」が閣議決定されました　https://www.meti.go.jp/press/2021/03/20220304004/20220304004.html〔2024/5/1 確認〕
経済産業省：認定高度保安実施事業者制度の運用を開始し、燃料電池自動車等の規制の一元化を実施しました　https://www.meti.go.jp/press/2023/12/20231221003/20231221003.html〔2024/5/1 確認〕
※ 129 IPA：調査分析部サイバーインシデント調査室　https://www.ipa.go.jp/jinzai/ics/ciil/index.html〔2024/5/1 確認〕
※ 130 https://www.soumu.go.jp/main_content/000895981.pdf〔2024/5/1 確認〕
※ 131 https://www.soumu.go.jp/main_content/000829941.pdf〔2024/5/1 確認〕
※ 132 総務省：「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」の開催　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00155.html〔2024/5/1 確認〕
※ 133 総務省：サイバーセキュリティタスクフォース　https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/index.html〔2024/5/1 確認〕
※ 134 総務省：国立研究開発法人情報通信研究機構法の一部改正について　https://www.soumu.go.jp/main_content/000920260.pdf〔2024/5/1 確認〕
※ 135 NICT：より安全な IoT 環境の実現に向けて ― NOTICE 事業 5 年間の総括と今後の取り組み ―　https://www2.nict.go.jp/csri/nict_cyber2024/pdf/ 講演 2_ より安全な IoT 環境の実現に向けて _NOTICE 事業 5 年間の総括と今後の取り組み .pdf〔2024/5/1 確認〕
※ 136 一般社団法人 ICT-ISAC：組織概要　https://www.ict-isac.jp/outline/〔2024/5/1 確認〕
※ 137 総務省により「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ」が 2021 年 11 月に策定されたことを受け実施された。
一般社団法人 ICT-ISAC：電気通信事業者におけるフロー情報分析による C&C サーバ検知に関する調査について（C&C サーバリスト共有トライアルの実施）　https://www.ict-isac.jp/news/news20230825.html〔2024/5/1 確認〕
※ 138 フロー情報：通信トラフィックデータのうち、IP アドレス、ポート番号等ヘッダー情報、ルーターでヘッダー情報を抽出する際に付与されるタイムスタンプ等の情報であり、通信の内容は含まれない。
※ 139 一般社団法人 ICT-ISAC：電気通信事業者におけるフロー情報分析による C&C サーバ検知に関する調査について（C&C サーバリスト共有トライアルの実施）（更新）　https://www.ict-isac.jp/news/news20231113.html〔2024/5/1 確認〕
※ 140 https://www.ict-isac.jp/news/news20230825/ 別紙1．本調査の概要 .pdf〔2024/5/1 確認〕
※ 141 日本経済新聞：サイバー攻撃、官民連携の分析センター設置 総務省検討　https://www.nikkei.com/article/DGXZQOUA268O80W3A620C2000000/〔2024/5/1 確認〕
※ 142 RPKI（Resource Public-Key Infrastructure）：自立ネットワークの IP アドレスや AS（Autonomous System）番号を電子証明書で検証し、通信経路の乗っ取り等を防止する技術。
※ 143 DNSSEC（DNS Security Extensions）：ドメインネームと IP アドレスの紐付けを電子証明書で検証し、サーバーのなりすまし等を防止する技術。
※ 144 DMARC（Domain-based Message Authentication Reporting and Conformance）：電子メールの送信元ドメインの正しさを検証し、なりすまし等の場合、自動的に処理する技術。
※ 145 総務省：「ICT サイバーセキュリティ政策分科会」の開催　https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00269.html〔2024/5/1 確認〕
※ 146 日本経済新聞：自治体にサイバー対策公表義務付け　週内にも法案決定　https://www.nikkei.com/article/DGXZQOUA276RN0X20C24A2000000/〔2024/5/1 確認〕
総務省：国会提出法案　https://www.soumu.go.jp/menu_hourei/k_houan.html〔2024/5/1 確認〕
※ 147 総務省：地方自治法の一部を改正する法律案の概要　https://www.soumu.go.jp/main_content/000931798.pdf〔2024/5/1 確認〕
※ 148 警察庁：警察におけるサイバー戦略について（依命通達）　https://www.npa.go.jp/bureau/cyber/pdf/202204_senryaku.pdf〔2024/5/1 確認〕
※ 149 警察庁：サイバー重点施策について（通達）　https://www.npa.go.jp/bureau/cyber/pdf/202204_jyuten.pdf〔2024/5/1 確認〕
※ 150 警察庁：令和 5 年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf〔2024/5/1 確認〕
※ 151 警察庁：令和 5 年版 警察白書　https://www.npa.go.jp/hakusyo/r05/index.html〔2024/5/1 確認〕
※ 152 https://www.ipa.go.jp/publish/wp-security/2023.html〔2024/5/1 確認〕
※ 153 警察庁：サイバー警察局　https://www.npa.go.jp/bureau/cyber/index.html〔2024/5/1 確認〕
※ 154 関東管区警察局：サイバー特別捜査隊　https://www.kanto.npa.go.jp/about/syoukai10.html〔2024/5/1 確認〕
※ 155 警察庁：令和 6 年度予算　概算要求の概要　https://www.npa.go.jp/policies/budget/r6/gaisanyokyu/r6tousyoyosan.pdf〔2024/5/1 確認〕
※ 156 警察庁：ASEAN+3国際犯罪閣僚会議及び日・ASEAN国際犯罪閣僚会議の開催について　https://www.npa.go.jp/bureau/soumu/kokusai/ammtc2023.html〔2024/5/1 確認〕
※ 157 警察庁、あいおいニッセイ同和損害保険株式会社：サイバー事案に係る被害の未然防止や拡大防止等に向け、警察庁サイバー警察局とあいおいニッセイ同和損保が連携協定を締結　https://www.aioinissaydowa.co.jp/corporate/about/news/pdf/2023/news_2023111001245.pdf〔2024/5/1 確認〕
※ 158 警察庁：サイバー事案の対処に関する協定書　https://www.ipa.go.jp/news/2023/announce/nq6ept0000001aua-att/keisatsucho_20231222.pdf〔2024/5/1 確認〕
※ 159 警察庁：サイバー警察局注意喚起　https://www.npa.go.jp/

bureau/cyber/koho/caution.html〔2024/5/1 確認〕
※ 160 警察庁：有識者会議　https://www.npa.go.jp/bureau/cyber/what-we-do/csmeeting.html〔2024/5/1 確認〕
※ 161 公益社団法人日本医師会：日本医師会及び警察庁サイバー警察局の連携に関する覚書締結等について　https://www.med.or.jp/nichiionline/article/011146.html〔2024/5/1 確認〕
※ 162 警察庁：ランサムウェア被疑者の検挙及び関連犯罪インフラのテイクダウンに関するユーロポールのプレスリリースについて　https://www.npa.go.jp/news/release/2024/release1.pdf〔2024/5/1 確認〕
※ 163 警察庁：中国を背景とするサイバー攻撃グループ BlackTech によるサイバー攻撃について（注意喚起）　https://www.npa.go.jp/bureau/cyber/pdf/20230927press.pdf〔2024/5/1 確認〕
※ 164-1 警察庁：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）　https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf〔2024/5/1 確認〕
警察庁：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）　https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf〔2024/5/1 確認〕
※ 164-2 警察庁：家庭用ルーターの不正利用に関する注意喚起について　https://www.npa.go.jp/bureau/cyber/pdf/20230328_press.pdf〔2024/5/1 確認〕
※ 164-3 警察庁、NISC：DDoS 攻撃への対策について　https://www.npa.go.jp/bureau/cyber/pdf/20230501.pdf〔2024/5/1 確認〕
※ 165 厚生労働省：新型コロナウイルス感染症の5類感染症移行後の対応について　https://www.mhlw.go.jp/stf/corona5rui.html〔2024/5/1 確認〕
※ 166 外務省：ウクライナ情勢に関する対応　https://www.mofa.go.jp/mofaj/erp/c_see/ua/page3_003225.html〔2024/5/1 確認〕
※ 167 外務省：ガザ情勢　https://www.mofa.go.jp/mofaj/me_a/me1/palestine/page22_001217.html〔2024/5/1 確認〕
※ 168 外務省：ガザ地区に対する人道支援の拡大と監視に関する国連安保理決議の採択について（外務報道官談話）　https://www.mofa.go.jp/mofaj/press/danwa/pageit_000001_00144.html〔2024/5/1 確認〕
※ 169 NHK：アメリカが拒否権行使し否決 ガザ停戦決議案 国連安保理　https://www3.nhk.or.jp/news/html/20240221/k10014365741000.html〔2024/5/1 確認〕
※ 170 Reuters：国連安保理、ガザ即時停戦決議案を採択　米は棄権　https://jp.reuters.com/world/us/GRUZHHQYPJJ3DOOKRMLIRMYCGY-2024-03-25/〔2024/5/1 確認〕
※ 171 NHK：イスラエルとハマスの衝突 100 万回以上見られた偽動画 など 33 に　https://www3.nhk.or.jp/news/html/20231107/k10014250371000.html〔2024/5/1 確認〕
※ 172 Reuters：アングル：イスラエル・ハマス紛争、氾濫する偽情報で世論歪む恐れ　https://jp.reuters.com/economy/JWD5O7OHIJKTTKBNLFGDGENHUM-2023-10-18/〔2024/5/1 確認〕
※ 173 外務省：軍事領域における責任ある AI 利用（REAIM）イニシアチブ　https://www.mofa.go.jp/mofaj/gaiko/arms/page23_004201.html〔2024/5/1 確認〕
※ 174 外務省：「AI と自律性の責任ある軍事利用に関する政治宣言」への我が国の参加　https://www.mofa.go.jp/mofaj/press/release/press5_000156.html〔2024/5/1 確認〕
※ 175 外務省：自律型致死兵器システム（LAWS）について　https://www.mofa.go.jp/mofaj/dns/ca/page24_001191.html〔2024/5/1 確認〕
※ 176 NHK：“AI 兵器 対応急がれる” 国連総会で決議を採択　https://www3.nhk.or.jp/news/html/20231224/k10014298431000.html〔2024/5/1 確認〕
※ 177 外務省：特定通常兵器使用禁止制限条約自律型致死兵器システムに関する政府専門家会合の開催（2024 年 3 月）　https://www.mofa.go.jp/mofaj/dns/ca/pagew_000001_00431.html〔2024/5/1 確認〕
NHK：AI 使った「自律型兵器システム」の規制を目指す国際会議始まる　https://www3.nhk.or.jp/news/html/20240305/k10014379161000.html〔2024/5/1 確認〕
※ 178 GOV.UK：AI SAFETY SUMMIT　https://www.aisafetysummit.gov.uk/〔2024/5/1 確認〕
※ 179 外務省：岸田総理大臣の英主催 AI 安全性サミットへの参加について（結果概要）　https://www.mofa.go.jp/mofaj/ecm/ec/page5_000484.html〔2024/5/1 確認〕
※ 180 NHK：“AI 技術に安全性や信頼性確保を” 初の決議案が採択 国連総会　https://www3.nhk.or.jp/news/html/20240322/k10014398891000.html〔2024/5/1 確認〕
※ 181 外務省：協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書　https://www.mofa.go.jp/mofaj/ila/st/page24_002143.html〔2024/5/1 確認〕
※ 182 外務省：G7 広島サミット（令和 5 年 5 月 19 日～ 21 日）https://www.mofa.go.jp/mofaj/ms/g7hs_s/page1_001673.html〔2024/5/1 確認〕
※ 183 外務省：G7 広島サミット（ゼレンスキー・ウクライナ大統領の訪日）https://www.mofa.go.jp/mofaj/ecm/ec/page4_005892.html〔2024/5/1 確認〕
※ 184 外務省：G 7広島首脳コミュニケ（2023年5月20日）　https://www.mofa.go.jp/mofaj/files/100507034.pdf〔2024/5/1 確認〕
※ 185 OECD：The Global Partnership on AI (GPAI)　https://oecd.ai/en/gpai〔2024/5/1 確認〕
※ 186 総務省：広島 AI プロセス G7 デジタル・技術閣僚声明（2023年12 月 1 日）　https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document02.pdf〔2024/5/1 確認〕
総務省：広島AIプロセスについて　https://www8.cao.go.jp/cstp/ai/ai_senryaku/7kai/11hiroshimaaipurosesu.pdf〔2024/5/1 確認〕
※ 187 外務省：日本 ASEAN 友好協力 50 周年事業　https://www.mofa.go.jp/mofaj/a_o/rp/page23_003946.html〔2024/5/1 確認〕
※ 188 外務省：石月英雄サイバー政策担当大使の「日・ASEAN サイバーセキュリティ能力構築センター（AJCCBC）」研修オープニングセレモニー出席　https://www.mofa.go.jp/mofaj/press/release/press5_000050.html〔2024/5/1 確認〕
※ 189 ASEAN-CBP：日 ASEAN サイバーセキュリティ官民共同フォーラム (IC-AJCC)　https://asean-cbp.org/ic-ajcc-jp/〔2024/5/1 確認〕
※ 190 外務省：日本 ASEAN 友好協力 50 周年特別首脳会議（概要）https://www.mofa.go.jp/mofaj/a_o/rp/pageit_000001_00111.html〔2024/5/1 確認〕
※ 191 日本 ASEAN 友好協力に関する共同ビジョン・ステートメント―信頼のパートナー　https://www.mofa.go.jp/mofaj/files/100601311.pdf〔2024/5/1 確認〕
※ 192 https://www.mofa.go.jp/mofaj/files/100347891.pdf〔2024/5/1 確認〕
※ 193 https://www.mofa.go.jp/mofaj/fp/es/pageit_000001_00084.html〔2024/5/1 確認〕
※ 194 外務省：第 3 回日米豪印上級サイバーグループ対面会合の開催（結果）　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_00062.html〔2024/5/1 確認〕
※ 195 外務省：第 8 回日米サイバー対話の開催　https://www.mofa.go.jp/mofaj/press/release/press4_009685.html〔2024/5/1 確認〕
※ 196 外務省：第 1 回日・NATO サイバー対話の開催（結果）https://www.mofa.go.jp/mofaj/press/release/press4_009859.html〔2024/5/1 確認〕
※ 197 外務省：第 5 回日・EU サイバー対話の開催（結果）　https://www.mofa.go.jp/mofaj/press/release/press4_009860.html〔2024/5/1 確認〕
※ 198 IPA：2023 年度「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　https://www.ipa.go.jp/jinzai/ics/global/ics20231016.html〔2024/5/1 確認〕
※ 199 総務省：大洋州島しょ国向けサイバーセキュリティ能力構築演習を実 施　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00190.html〔2024/5/1 確認〕
※ 200 外務省：第 1 回日・ヨルダン・サイバーセキュリティ協議の開催 https://www.mofa.go.jp/mofaj/me_a/me1/jo/page7_000032.html〔2024/5/1 確認〕
※ 201 外務省：第 5 回日・インド・サイバー協議の開催　https://www.mofa.go.jp/mofaj/press/release/press4_009785.html〔2024/5/1 確認〕
※ 202 外務省：第 7 回日仏サイバー協議の開催（結果）　https://www.mofa.go.jp/mofaj/press/release/press5_000160.html〔2024/5/1 確認〕
※ 203 外務省：第 5 回日豪サイバー政策協議の開催（結果）　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_00040.html〔2024/5/1 確認〕
※ 204 Reuters：Deepfaking it: America's 2024 election collides with AI boom　https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30/〔2024/5/1 確認〕
※ 205 NHK：台湾総統選挙 AI 悪用とみられる不審アカウントや偽動画 広がる　https://www3.nhk.or.jp/news/html/20231223/k10014297431000.html〔2024/5/1 確認〕
※ 206 NHK：米 IT 大手など 20 社が協定 選挙での AI 偽動画や音声対策へ連携　https://www3.nhk.or.jp/news/html/20240217/k10014361881000.html〔2024/5/1 確認〕
※ 207 The White House：Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/〔2024/5/1 確認〕
※ 208 Federal Register：Maintaining American Leadership in Artificial Intelligence https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence〔2024/5/1 確認〕
※ 209 Federal Register：Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government〔2024/5/1 確認〕
※ 210 NIST：AI Risk Management Framework https://www.nist.gov/itl/ai-risk-management-framework〔2024/5/1 確認〕
※ 211 The White House：FACT SHEET: Vice President Harris Announces New U.S. Initiatives to Advance the Safe and Responsible Use of Artificial Intelligence https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/fact-sheet-vice-president-harris-announces-new-u-s-initiatives-to-advance-the-safe-and-responsible-use-of-artificial-intelligence/〔2024/5/1 確認〕
※ 212 NIST：U.S. Artificial Intelligence Safety Institute https://www.nist.gov/artificial-intelligence/artificial-intelligence-safety-institute〔2024/5/1 確認〕
※ 213 The White House：Proposed Memorandum for the Heads of Executive Departments and Agencies https://www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf〔2024/5/1 確認〕
※ 214 CIO.GOV：The Top 10 Things Federal Technology Leaders Should Know About OMB's Draft AI Policy https://www.cio.gov/ai-policy/〔2024/5/1 確認〕
※ 215 https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/〔2024/5/1 確認〕
※ 216 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf〔2024/5/1 確認〕
※ 217 Federal Register：Request for Information (RFI) Related to NIST's Assignments Under Sections 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence (Sections 4.1, 4.5, and 11) https://www.federalregister.gov/documents/2023/12/21/2023-28232/request-for-information-rfi-related-to-nists-assignments-under-sections-41-45-and-11-of-the〔2024/5/1 確認〕
※ 218 NIST：The NIST Cybersecurity Framework (CSF) 2.0 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf〔2024/5/1 確認〕
※ 219 紐付けられたフレームワーク、ガイドラインには以下が含まれる。
・NIST プライバシーフレームワーク
・NIST AI 100-1：AI リスクマネジメントフレームワーク（AI-RMF）
・NIST SP800-218 v1.1：NIST セキュアソフトウェア開発フレームワーク（SSDH）
・CIS Critical Security Controls
※ 220 CISA：CISA Roadmap for Artificial Intelligence https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdf〔2024/5/1 確認〕
※ 221 https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf〔2024/5/1 確認〕
※ 222 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〔2024/5/1 確認〕
※ 223 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/?_ga=2.173443239.506610032.1709268239-234130803.1702622199&_fsi=0DwKYWiz〔2024/5/1 確認〕
※ 224 https://media.defense.gov/2023/Dec/14/2003359097/-1/-1/0/CSI-SCRM-SBOM-Management-v1.1.PDF〔2024/5/1 確認〕
※ 225 DoD：2023 DOD Cyber Strategy Summary https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF〔2024/5/1 確認〕
※ 226 CYBERCOM：CYBERCOM's "Under Advisement" to increase private sector partnerships, industry data-sharing in 2023 https://www.cybercom.mil/Media/News/Article/3444464/cybercoms-under-advisement-to-increase-private-sector-partnerships-industry-dat/〔2024/5/1 確認〕
※ 227 EC：Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721〔2024/5/1 確認〕
※ 228 EUR-Lex：Regulation - 2016/679 - EN - gdpr - EUR-Lex https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679〔2024/5/1 確認〕
※ 229 Library of Congress：Text - H.R.2670 - 118th Congress (2023-2024): National Defense Authorization Act for Fiscal Year 2024 https://www.congress.gov/bill/118th-congress/house-bill/2670/text〔2024/5/1 確認〕
※ 230 Taiwan Today：バイデン米大統領が国防権限法に署名、外交部は台湾支援強化に感謝 https://jp.taiwantoday.tw/news.php?unit=148,149,150,151,152&post=246482〔2024/5/1 確認〕
※ 231 CISA、NSA、FBI 等：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〔2024/5/1 確認〕
CISA、NSA、FBI 等：PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a〔2024/5/1 確認〕
※ 232 Reuters：英政府が移民受け入れ削減計画、人手不足に拍車と反発も https://jp.reuters.com/world/europe/DMKXXX2VNBIXTEEID4ZRA3ARZM-2023-12-05/〔2024/5/1 確認〕
※ 233 BBC：Spending power to surge in London but plunge in other regions https://www.bbc.com/news/business-66436792〔2024/5/1 確認〕
※ 234 日本経済新聞：TPP 初の新規加入、英国加盟を正式承認　計 12 カ国体制に https://www.nikkei.com/article/DGXZQOUA13CVN0T10C23A7000000/〔2024/5/1 確認〕
※ 235 Reuters：Sporadic violence, but calmer night in France after family buries teenager https://www.reuters.com/world/europe/france-deploys-45000-police-armored-vehicles-amid-riots-2023-07-01/〔2024/5/1 確認〕
※ 236 Reuters：Moscow concert hall attack: what we know about shooting in Russia https://www.reuters.com/world/europe/what-we-know-about-shooting-concert-venue-near-moscow-2024-03-22/〔2024/5/1 確認〕
※ 237 BBC：France beefs up security as Paris Olympics approach https://www.bbc.com/news/world-europe-68772589〔2024/5/1 確認〕
※ 238 Reuters：German economy dodges recession despite shrinking 0.3% in 2023 https://www.reuters.com/markets/europe/german-economy-contracted-03-2023-stats-office-2024-01-15/〔2024/5/1 確認〕
※ 239 BBC：Germany: Scholz warns against rise of neo-Nazi networks https://www.bbc.com/news/world-europe-68117813〔2024/5/1 確認〕
※ 240 EC：Joint Statement of Special Envoys and Coordinators Combating Antisemitism https://ec.europa.eu/newsroom/just/newsletter-archives/48763〔2024/5/1 確認〕
※ 241 BBC：UK antisemitic hate incidents hit new high in 2023, says charity https://www.bbc.com/news/uk-68288727〔2024/5/1 確認〕
※ 242 ENISA：NIS Directive https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new〔2024/5/1 確認〕
※ 243 EC：Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act〔2024/5/1 確認〕
※ 244 ENISA：NIS Investments Report 2023 https://www.enisa.europa.eu/publications/nis-investments-2023〔2024/5/1 確認〕
※ 245 Cyber Risk GmbH：The European Cyber Resilience Act (CRA) https://www.european-cyber-resilience-act.com/?_fsi=6wxbpuJp〔2024/5/1 確認〕
※ 246 JETRO：欧州委、デジタル製品のサイバーセキュリティー対応を義務付ける法案発表 https://www.jetro.go.jp/biznews/2022/09/27fcc2dec113fddc.html〔2024/5/1 確認〕
※ 247 BEUC：Position papers Cyber Resilience Act proposal https://www.beuc.eu/position-papers/cyber-resilience-act-proposal

〔2024/5/1 確認〕
※ 248 クラウド Watch：オープンソース業界に広がる懸念　欧州で導入予定のサイバーレジリエンス法　https://cloud.watch.impress.co.jp/docs/column/infostand/1497776.html〔2024/5/1 確認〕
※ 249 EC：Commission welcomes political agreement on Cyber Resilience Act　https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168〔2024/5/1 確認〕
※ 250 TechCrunch：Open source foundations unite on common standards for EU's Cyber Resilience Act　https://techcrunch.com/2024/04/02/open-source-foundations-unite-on-common-standards-for-eus-cybersecurity-resilience-act/〔2024/5/1 確認〕
※ 251 ENISA：ENISA Threat Landscape 2023　https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023〔2024/5/1 確認〕
※ 252 名古屋港運協会、名古屋コンテナー委員会、ターミナル部会：NUTS システム障害の経緯報告　https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf〔2024/5/1 確認〕
※ 253 トレンドマイクロ株式会社：ランサムウェア「LockBit」の概要と対策～名古屋港の活動停止を引き起こした犯罪集団　https://www.trendmicro.com/ja_jp/jp-security/23/h/securitytrend-20230823-01.html〔2024/5/1 確認〕
※ 254 https://www.nomoreransom.org〔2024/5/1 確認〕
※ 255 Europol：Law enforcement disrupt world's biggest ransomware operation　https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation〔2024/5/1 確認〕
Reuters：ハッカー集団ロックビットを摘発、米英など 10 カ国の共同捜査で　https://jp.reuters.com/world/security/DN37JXQJZRKTPJCJ2TR2TRXGIY-2024-02-21/〔2024/5/1 確認〕
※ 256 The Asahi Shimbun：Expert: LockBit ransomware group to keep hitting hospitals　https://www.asahi.com/ajw/articles/15205662〔2024/5/1 確認〕
※ 257 EC：European data strategy　https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en〔2024/5/1 確認〕
※ 258 EC：Data Act　https://digital-strategy.ec.europa.eu/en/policies/data-act〔2024/5/1 確認〕
※ 259 EC：European Data Governance Act　https://digital-strategy.ec.europa.eu/en/policies/data-governance-act〔2024/5/1 確認〕
※ 260 EC：Digital Markets Act　https://digital-markets-act.ec.europa.eu/index_en〔2024/5/1 確認〕
※ 261 EC：The Digital Services Act　https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en〔2024/5/1 確認〕
※ 262 EC：Commission opens formal proceedings against X under the Digital Services Act　https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709〔2024/5/1 確認〕
※ 263 EC：Commission opens formal proceedings against TikTok under the Digital Services Act　https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926〔2024/5/1 確認〕
※ 264 Reuters：EU, TikTok の正式調査開始　デジタルサービス法違反の恐れ　https://jp.reuters.com/business/technology/BBBCLC6RCRLS3LO2YALRT4OGFI-2024-02-20/〔2024/5/1 確認〕
※ 265 The Guardian：EU threatens TikTok Lite with ban over reward-to-watch feature　https://www.theguardian.com/technology/2024/apr/22/eu-threatens-to-ban-tiktok-lite-over-reward-to-watch-feature〔2024/5/1 確認〕
※ 266 EC：Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act　https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689〔2024/5/1 確認〕
※ 267 EC：Commission fines Apple over €1.8 billion over abusive App store rules for music streaming providers　https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161〔2024/5/1 確認〕
※ 268 日本経済新聞：EU、巨大 IT に新規制　デジタル寡占抑止へ「超独禁法」　https://www.nikkei.com/article/DGXZQOGN060E40W4A300C2000000/〔2024/5/1 確認〕
※ 269 EC：REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS　https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN〔2024/5/1 確認〕
※ 270 European Parliament：Artificial Intelligence Act: MEPs adopt landmark law　https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law〔2024/5/1 確認〕
Reuters：Europe one step away from landmark AI rules after lawmakers' vote　https://www.reuters.com/technology/eu-lawmakers-endorse-political-deal-artificial-intelligence-rules-2024-03-13/〔2024/5/1 確認〕
※ 271 Reuters：Europe agrees landmark AI regulation deal　https://www.reuters.com/technology/stalled-eu-ai-act-talks-set-resume-2023-12-08/〔2024/5/1 確認〕
JETRO：EU、AI を包括的に規制する法案で政治合意、生成型 AI も規制対象に　https://www.jetro.go.jp/biznews/2023/12/8a6cd52f78d376b1.html〔2024/5/1 確認〕
※ 272 EC：Commission Decision Establishing the European AI Office　https://digital-strategy.ec.europa.eu/en/library/commission-decision-establishing-european-ai-office〔2024/5/1 確認〕
※ 273 EC：European AI Office　https://digital-strategy.ec.europa.eu/en/policies/ai-office〔2024/5/1 確認〕
※ 274 NIST：U.S. Artificial Intelligence Safety Institute　https://www.nist.gov/artificial-intelligence-safety-institute〔2024/5/1 確認〕
GOV.UK：AI SAFETY INSTITUTE　https://www.gov.uk/government/organisations/ai-safety-institute〔2024/5/1 確認〕
AISI Japan:AI Safety Institute　https://aisi.go.jp/〔2024/5/1 確認〕
※ 275 EC：Commission launches AI innovation package to support Artificial Intelligence startups and SMEs　https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383〔2024/5/1 確認〕
※ 276 European Parliament：Artificial Intelligence Act: MEPs adopt landmark law　https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law〔2024/5/1 確認〕
One Asia Lawyers：EU・AI 法の成立 – 来るべき AI 規制への備え –　https://oneasia.legal/12675〔2024/5/1 確認〕
※ 277 DLA Piper：DLA Piper GDPR Fines and Data Breach Survey: January 2024　https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024〔2024/5/1 確認〕
※ 278 CMS：GDPR Enforcement Tracker ETid1543　https://www.enforcementtracker.com/ETid-1543〔2024/5/1 確認〕
※ 279 CMS：GDPR Enforcement Tracker ETid1730　https://www.enforcementtracker.com/ETid-1730〔2024/5/1 確認〕
※ 280 CMS：GDPR Enforcement Tracker ETid1844　https://www.enforcementtracker.com/ETid-1844〔2024/5/1 確認〕
※ 281 BBC：Meta: Facebook owner fined €1.2bn for mishandling data　https://www.bbc.com/news/technology-65669839〔2024/5/1 確認〕
※ 282 CMS：GDPR enforcement Tracker ETid1912　https://www.enforcementtracker.com/ETid-1912〔2024/5/1 確認〕
※ 283 CMS：GDPR Enforcement Tracker ETid2032　https://www.enforcementtracker.com/ETid-2032〔2024/5/1 確認〕
※ 284 Australian Government：2023-2030 Australian Cyber Security Strategy　https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy〔2024/5/1 確認〕
※ 285 Australian Government：2023-2030 Australian Cyber Security Strategy Action Plan　https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy-action-plan.pdf〔2024/5/1 確認〕
※ 286 GCSB：New Zealand takes the first step in creating a lead operational cyber security agency　https://www.gcsb.govt.nz/news/new-zealand-takes-the-first-step-in-creating-a-lead-operational-cyber-security-agency/〔2024/5/1 確認〕
※ 287 Ministry of Electoronics & IT：CERT-In issues "Guidelines on Information Security Practices" for Government Entities for Safe & Trusted Internet　https://www.pib.gov.in/PressReleasePage.aspx?PRID=1936470〔2024/5/1 確認〕
※ 288 CSA:New Cyber Talent Programme to Provide Foundational and Targeted Cybersecurity Training For Non-Cybersecurity Professionals　https://www.csa.gov.sg/News-Events/Press-Releases/2023/new-cyber-talent-programme-to-provide-foundational-and-targeted-cybersecurity-training-for-non-cybersecurity-professionals〔2024/5/1 確認〕
※ 289 NICS：About Us　https://www.nics.nat.gov.tw/en/about/introduction/〔2024/5/1 確認〕

※ 290 NICS：National Institute of Cyber Security　https://download.nics.nat.gov.tw/UploadFile/attachfilenew/1_NICS Intro（核定版）_1120626.pdf〔2024/5/1 確認〕
※ 291 中華民国総統府：國家資通安全研究院揭牌　總統：全力推動前瞻資安科技　為全民打造一個安全、安心及安穩的數位環境　https://www.president.gov.tw/News/27301〔2024/5/1 確認〕
※ 292 https://www.apcert.org/〔2024/5/1 確認〕
※ 293 APCERT: Member Teams　https://www.apcert.org/about/structure/members.html〔2024/5/1 確認〕
※ 294 APCERT：APCERT CYBER DRILL 2023 “DIGITAL SUPPLY CHAIN REDEMPTION”　https://www.apcert.org/documents/pdf/APCERTDrill2023PressRelease.pdf〔2024/5/1 確認〕
※ 295 APCERT：Documents　https://www.apcert.org/documents/index.html〔2024/5/1 確認〕
※ 296 https://krcert.or.kr〔2024/5/1 確認〕
※ 297 https://www.cybersecurity.my/en/index.html〔2024/5/1 確認〕
※ 298 https://www.cert.gov.lk〔2024/5/1 確認〕
※ 299 外務省：日 ASEAN 友好協力に関する共同ビジョン・ステートメント 2023 信頼のパートナー 実施計画（仮訳）　https://www.mofa.go.jp/files/100601230.pdf〔2024/5/1 確認〕
※ 300 経済産業省：デジタルスキル標準　https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/main.html〔2024/5/1 確認〕
※ 301 https://manabi-dx.ipa.go.jp〔2024/5/1 確認〕
※ 302 ISC2, Inc.：ISC2 Cybersecurity Workforce Study 2023　https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e〔2024/5/1 確認〕
※ 303 株式会社リクルート：サイバーセキュリティー関連求人、2014 年比で 24.3 倍に増加　https://www.recruit.co.jp/newsroom/pressrelease/assets/20240315_work_01.pdf〔2024/5/1 確認〕
※ 304 IPA：生成 AI 時代の人材育成に関する座談会　https://www.ipa.go.jp/jinzai/skill-standard/dss/zadankai.html〔2024/5/1 確認〕
※ 305 「プラス・セキュリティ」とは、自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身に付けること、あるいは身に付けている状態のこと。
経済産業省：「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）をとりまとめました　https://www.meti.go.jp/policy/netsecurity/tebiki_taisei_jinzai.html〔2024/5/1 確認〕
※ 306 Gartner, Inc.：Gartner Unveils Top Eight Cybersecurity Predictions for 2024　https://www.gartner.com/en/newsroom/press-releases/2024-03-18-gartner-unveils-top-eight-cybersecurity-predictions-for-2024〔2024/5/1 確認〕
※ 307 防衛省：防衛力整備計画　https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/plan.pdf〔2024/5/1 確認〕
※ 308 https://cstia.or.jp〔2024/5/1 確認〕
※ 309 https://www.ipa.go.jp/jinzai/chousa/ps6vr7000000z6cc-att/skill-henkaku2022-zentai.pdf〔2024/5/1 確認〕
※ 310 SC3 事務局：SC3 第 8 回産学官連携WG 令和 5 年度 WG 活動報告【抜粋】　https://www.ipa.go.jp/security/sc3/activities/sangakukanWG/images/8th_siryou_abs.pdf〔2024/5/1 確認〕
※ 311 米国では 10 年ほど前から、採用条件を見直し「スキルファースト」で人材採用するアプローチを取る企業も出てきている。
DIAMOND ハーバード・ビジネス・レビュー：リーダーはどのように企業のテクノロジー活用を牽引すべきか　https://dhbr.diamond.jp/articles/-/10211?page=2〔2024/5/1 確認〕
※ 312 https://fita.or.jp〔2024/5/1 確認〕
※ 313 経済産業省：第 8 回「産業サイバーセキュリティ研究会」を開催しました　https://www.meti.go.jp/press/2024/04/20240405003/20240405003.html〔2024/5/1 確認〕
※ 314 https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/security.html〔2024/5/1 確認〕
※ 315 セキュリティ関連知識・スキルの内容は、「情報処理安全確保支援士試験（レベル 4）シラバス」（https://www.ipa.go.jp/shiken/syllabus/ps6vr7000000i97q-att/syllabus_sc_ver2_0.pdf〔2024/5/1 確認〕）を参照することになっている。17 分野の一部には主導できるレベル（情報処理安全確保支援士試験レベル）、コミュニケーションが取れるレベル（情報セキュリティマネジメント試験レベル）が示されているが、企業等によって、レベルの付し方の変更や、知識・スキル項目の追加・削除・詳細化が必要とされている。
※ 316 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf〔2024/5/1 確認〕
※ 317 Workforce Framework for Cybersecurity (NICE Framework)　https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final〔2024/5/1 確認〕
※ 318 一般企業における共通的な役割／業務は CRIC CSF の人材定義リファレンスの改訂版、また、インシデント対応の役割／業務は NCA、FIRST 等のガイドラインを活用することが検討されている。
※ 319 SC3 業界連携 WG で検討することが考えられている。
※ 320 NICE FW ではコンピタンシーには評価基準を項目として設定するように定められているが、評価基準自身は各組織で設定することになっている。
※ 321 CBT（Computer Based Testing）方式：試験会場に設置されたコンピューターを利用して実施する試験方式のこと。受験者はコンピューターに表示された試験問題に対して、マウスやキーボードを用いて解答する。
※ 322 このほかに、身体の不自由等により CBT 方式の受験ができない方を対象とした筆記試験を、春期 4 月 16 日及び秋期 10 月 8 日に実施した。
※ 323 IPA：情報処理技術者試験 情報処理安全確保支援士試験 統計資料 令和 5 年度試験 全試験区分版　https://www.ipa.go.jp/shiken/reports/hjuojm000000liyb-att/toukei_r05.pdf〔2024/5/1 確認〕
※ 324 IPA：国家資格「情報処理安全確保支援士」2024 年 4 月 1 日付新規登録者 1,345 名の内訳　https://www.ipa.go.jp/jinzai/riss/reports/data/20240401newriss.html〔2024/5/1 確認〕
※ 325 IPA：講習の目的と概要　https://www.ipa.go.jp/jinzai/riss/forriss/koushu/overview.html〔2024/5/1 確認〕
※ 326 IPA：責任者向けプログラム 業界別サイバーレジリエンス強化演習（CyberREX）　https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberrex/index.html〔2024/5/1 確認〕
※ 327 IPA：実務者向けプログラム 制御システム向けサイバーセキュリティ演習（CyberSTIX）　https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberstix/index.html〔2024/5/1 確認〕
※ 328 経済産業省：情報処理安全確保支援士特定講習　https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html〔2024/5/1 確認〕
※ 329 IPA：登録セキスペインタビュー　https://www.ipa.go.jp/jinzai/riss/interview/riss.html#section13〔2024/5/1 確認〕
※ 330 IPA：セキュリティ・キャンプ全国大会 2023 ホーム　https://www.ipa.go.jp/jinzai/security-camp/2023/zenkoku/index.html〔2024/5/1 確認〕
※ 331 IPA：セキュリティ・ネクストキャンプ 2023 ホーム　https://www.ipa.go.jp/jinzai/security-camp/2023/next/index.html〔2024/5/1 確認〕
※ 332 IPA：セキュリティ・ジュニアキャンプ 2023 ホーム　https://www.ipa.go.jp/jinzai/security-camp/2023/junior/index.html〔2024/5/1 確認〕
※ 333 セキュリティ・キャンプ協議会：地方大会　https://www.security-camp.or.jp/minicamp/〔2024/5/1 確認〕
※ 334 セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 東京 2023　https://www.security-camp.or.jp/minicamp/tokyo2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 三重 2023　https://www.security-camp.or.jp/minicamp/mie2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 宮崎 2023　https://www.security-camp.or.jp/minicamp/miyazaki2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 新潟 2023　https://www.security-camp.or.jp/minicamp/niigata2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 山梨 2023　https://www.security-camp.or.jp/minicamp/yamanashi2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 徳島 2023　https://www.security-camp.or.jp/minicamp/tokushima2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 沖縄 2023　https://www.security-camp.or.jp/minicamp/okinawa2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 北海道 2023　https://www.security-camp.or.jp/minicamp/hokkaido2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 広島 2023　https://www.security-camp.or.jp/minicamp/hiroshima2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 石川 2023　https://www.security-camp.or.jp/minicamp/ishikawa2023.html〔2024/5/1 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 大阪 2024　https://www.security-camp.or.jp/minicamp/osaka2024.html〔2024/5/1 確認〕
※ 335 セキュリティ・キャンプ協議会：GCC 2024 Thailand - Global

Cybersecurity Camp 2024 Thailand https://www.security-camp.or.jp/event/gcc_Thailand2024.html〔2024/5/1 確認〕
※ 336 NICT：サイバーセキュリティ演習基盤 CYROP のオープン化トライアルを開始 https://www.nict.go.jp/press/2022/02/03-1.html〔2024/5/1 確認〕
※ 337 NICT:日本のサイバーセキュリティの結節点“CYNEX アライアンス”を発足 https://www.nict.go.jp/press/2023/10/02-1.html〔2024/5/1 確認〕
※ 338 NICT：CYDER 開催スケジュール https://cyder.nict.go.jp/course/schedule/index.html〔2024/5/1 確認〕
※ 339 NICT：プレ CYDER の募集を開始しました https://cyder.nict.go.jp/news/2023/post_36.html〔2024/5/1 確認〕
※ 340 NICT：開催スケジュール オンラインコース https://cyder.nict.go.jp/course/schedule/index.html#cource_c〔2024/5/1 確認〕
※ 341 日本経済新聞：太平洋地域でサイバー防御の初演習 総務省、実施を発表 https://www.nikkei.com/article/DGXZQOUA27A080X20C24A2000000/〔2024/5/1 確認〕
総務省：大洋州島しょ国向けサイバーセキュリティ能力構築演習を実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00190.html〔2024/5/1 確認〕
※ 342 総務省：2025 年日本国際博覧会に向けたサイバー防御講習「CIDLE（シードル）」の実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00175.html〔2024/5/1 確認〕
※ 343 NICT：SecHack365 の目的 https://sechack365.nict.go.jp/document/#p01〔2024/5/1 確認〕
※ 344 SECCON：SECCON 実行委員会／WG メンバー https://www.seccon.jp/2023/seccon/executivecommittee.html〔2024/5/1 確認〕
※ 345 SECCON：SECCON CTF 2023 ルール https://ctf.seccon.jp/rules-ja/〔2024/5/1 確認〕
※ 346 SECCON：SECCON Beginners とは https://www.seccon.jp/2023/beginners/about-seccon-beginners.html〔2024/5/1 確認〕
※ 347 CTF for GIRLS:CTF for GIRLS 10 年目記念イベント開催レポート http://girls.seccon.jp/news31.html〔2024/5/1 確認〕
※ 348 SECCON：SECCON Workshop https://www.seccon.jp/2023/seccon-workshop/〔2024/5/1 確認〕
※ 349 総務省：日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）における新プロジェクトの開始 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00166.html〔2024/5/1 確認〕
※ 350 JICA：日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）における第 1 回研修オープニングセレモニー：ASEAN 各国のサイバーセキュリティ専門人材の育成に貢献 https://www.jica.go.jp/information/press/2023/20230619_42.html〔2024/5/1 確認〕
※ 351 日本電気株式会社:NEC、ASEAN 加盟国向けのサイバーセキュリティ人材を育成する演習業務を受託 https://jpn.nec.com/cybersecurity/topics/2023/PR003_AJCCBC.html〔2024/5/1 確認〕
※ 352 JNSA：JNSA 産学情報セキュリティ人材育成検討会とは？ https://www.jnsa.org/internship/jinzai.html〔2024/5/1 確認〕
※ 353 JNSA：交流会に参加しよう！ー「産学情報セキュリティ人材育成交流会」 https://www.jnsa.org/internship/event.html〔2024/5/1 確認〕
※ 354 東京工業大学：環境・社会理工学院 技術経営専門職学位課程実施 キャリアアップ MOT プログラム CUMOT https://www.academy.titech.ac.jp/cumot/data/cumot_2023.pdf〔2024/5/1 確認〕
※ 355 東京工業大学：キャリアアップ MOT（CUMOT）サイバーセキュリティ経営戦略コース 受講生募集のご案内 https://www.academy.titech.ac.jp/cumot/cy/data/cumot_CY_2023.pdf〔2024/5/1 確認〕
※ 356 独立行政法人国立高等専門学校機構：サイバーセキュリティ人材育成事業 https://k-sec.kochi-ct.ac.jp/promotion-system/index.html〔2024/5/1 確認〕
※ 357 独立行政法人国立高等専門学校機構：Topics & News 一覧 https://k-sec.kochi-ct.ac.jp/topics-news/〔2024/5/1 確認〕
※ 358 IPA：中核人材育成プログラム 卒業プロジェクト https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/index.html〔2024/5/1 確認〕
※ 359 IPA：中核人材育成プログラム修了者コミュニティ「叶会（かなえかい）」 https://www.ipa.go.jp/jinzai/ics/core_human_resource/kanaekai.html〔2024/5/1 確認〕
※ 360 IPA：責任者向けプログラム サイバー危機対応机上演習（CyberCREST） https://www.ipa.go.jp/jinzai/ics/short-pgm/cybercrest/index.html〔2024/5/1 確認〕
※ 361 IPA：責任者向けプログラム サイバーセキュリティ企画演習（CyberSPEX） https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberspex/index.html〔2024/5/1 確認〕
※ 362 経済産業省：日本産業標準調査会基本政策部会「取りまとめ」（日本型標準加速化モデル）を公表しました。 https://www.meti.go.jp/policy/economy/hyojun-kijun/jisho/seisaku.html〔2024/5/1 確認〕
※ 363 https://www.meti.go.jp/policy/economy/hyojun-kijun/jisho/pdf/20230620tori.pdf〔2024/5/1 確認〕
※ 364 ISO：ISO/IEC JTC 1 https://www.iso.org/committee/45020.html〔2024/5/1 確認〕
※ 365 JISC：JISC について https://www.jisc.go.jp/jisc/index.html〔2024/5/1 確認〕
※ 366 ITU：SG17: Security https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔2024/5/1 確認〕
※ 367 IETF：Security Area https://trac.ietf.org/trac/sec/wiki〔2024/5/1 確認〕
※ 368 TCG：Welcome to Trusted Computing Group https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔2024/5/1 確認〕
※ 369 https://www.jisc.go.jp/international/iso-prcs.html〔2024/5/1 確認〕
※ 370 https://www.iso.org/standard/75652.html〔2024/5/2 確認〕
※ 371 Technical Specification（TS）：現時点では技術的に未成熟等の理由により、国際標準として発行するのは妥当ではない文書。
※ 372 EC：Cybersecurity – security requirements for ICT product certification https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification_en〔2024/5/1 確認〕
※ 373 European cybersecurity certification scheme（EUCC）：欧州で創立が進められている、ISO/IEC 15408 に基づく IT 製品のセキュリティ評価・認証制度。
※ 374 Common Criteria Recognition Arrangement（CCRA）：日本、米国のほか、欧州各国を含む計 31 ヵ国が加盟している、ISO/IEC 15408 に基づく IT 製品のセキュリティ認証の国際相互承認の枠組み。「3.2.1 IT セキュリティ評価及び認証制度」参照。
※ 375 A Critical Analysis of ISO 17825 (‘Testing methods for the mitigation of non-invasive attack classes against cryptographic modules’), Carolyn Whitnall & Elisabeth Oswald, at ASIACRYPT 2019, LNCS, vol 11923.
※ 376 IoT 推進コンソーシアム、総務省、経済産業省：IoT セキュリティガイドライン ver 1.0 https://www.soumu.go.jp/main_content/000428393.pdf〔2024/5/7 確認〕
※ 377 https://www.iso.org/standard/44373.html〔2024/5/7 確認〕
※ 378 https://www.iso.org/standard/80136.html〔2024/5/7 確認〕
※ 379 ITU-T の標準化プロセスについては、一般社団法人情報通信技術委員会が「標準化教育コンテンツ」（https://www.ttc.or.jp/activities/sdt_text〔2024/5/1 確認〕）として公開している「標準化教育テキスト（入門編）第 9 版 (2023 年 3 月)」の「2-1 デジュール標準化機関」（https://www.ttc.or.jp/application/files/1816/8360/6916/Standard_text_chapter2-1_v9.0.pdf〔2024/5/1 確認〕）の「2-1-1 ITU」が参考となる。
※ 380 https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99〔2024/5/1 確認〕
※ 381 IEC：TC 65 Scope https://www.iec.ch/dyn/www/f?p=103:14:613850989665891::::FSP_ORG_ID,FSP_LANG_ID:2612,25〔2024/5/1 確認〕
※ 382 https://www.jpcert.or.jp/present/2023/ICSR2023_02_YOKOGAWAElectric.pdf〔2024/5/1 確認〕
※ 383 https://www.jpcert.or.jp/event/ics-conference2023.html〔2024/5/1 確認〕
※ 384 IPA：制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ https://www.ipa.go.jp/security/controlsystem/incident.html〔2024/5/1 確認〕
※ 385 SCADA（Supervisory Control and Data Acquisition）：産業制御システムの一種であり、コンピューターによるシステム監視とプロセス制御を行う。
※ 386 https://www.iecee.org〔2024/5/1 確認〕
※ 387 https://isasecure.org〔2024/5/1 確認〕

付録

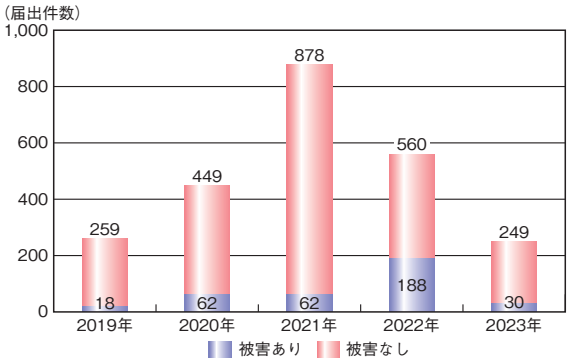
資料

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

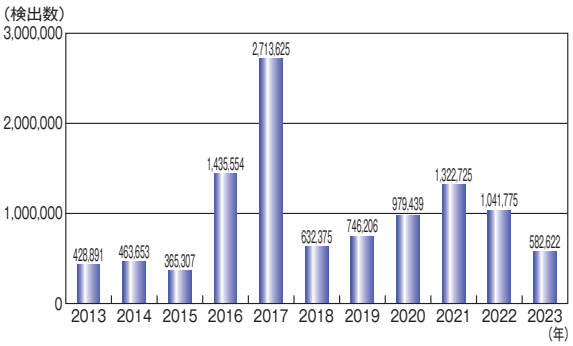
2023 年の年間届出件数は、前年の 560 件より 311 件（55.5%）少ない 249 件であった（図 A-1）。そのうち、ウイルス感染の実被害があった届出は 30 件であった。



■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）。



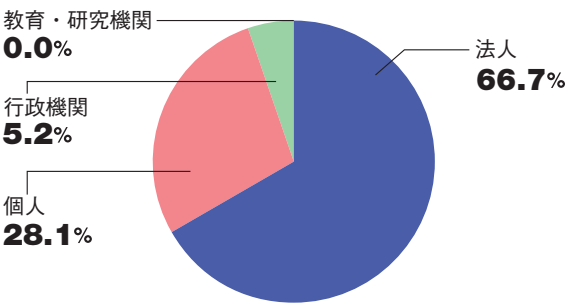
■図 A-2　ウイルス等検出数推移（2013～2023 年）

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

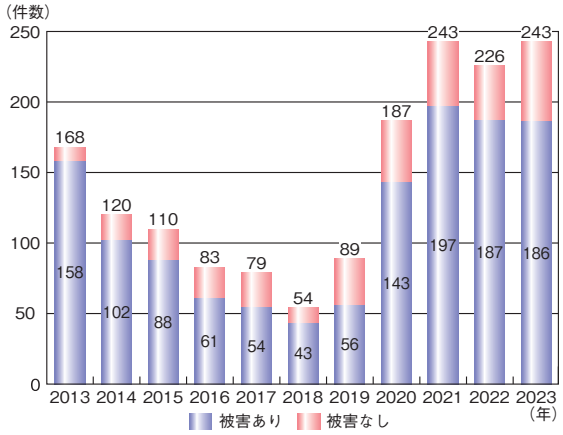
■コンピュータウイルス・不正アクセスの届出状況［2023年（1月～12月）］
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-report.pdf

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。



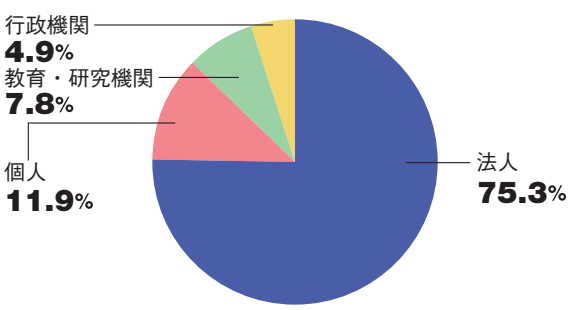
■図 B-1　不正アクセス届出件数推移（2013 年～2023 年）

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）

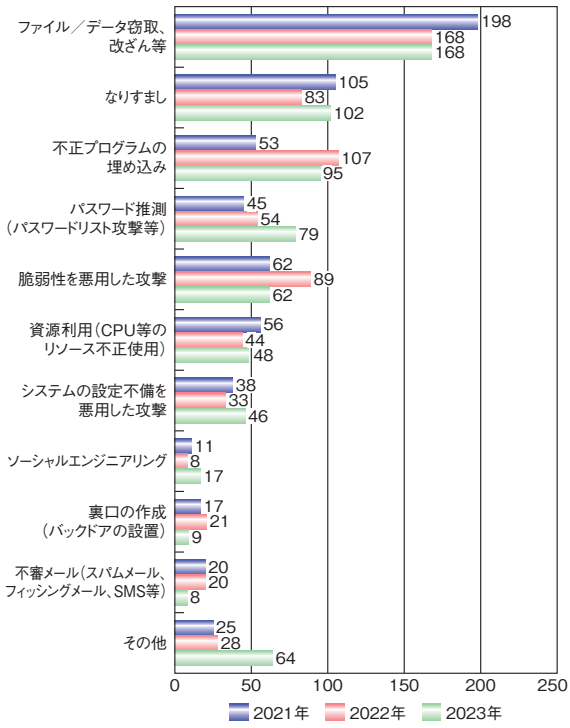


■図 B-2　不正アクセス届出者の主体別届出件数の比率（2023 年）

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。



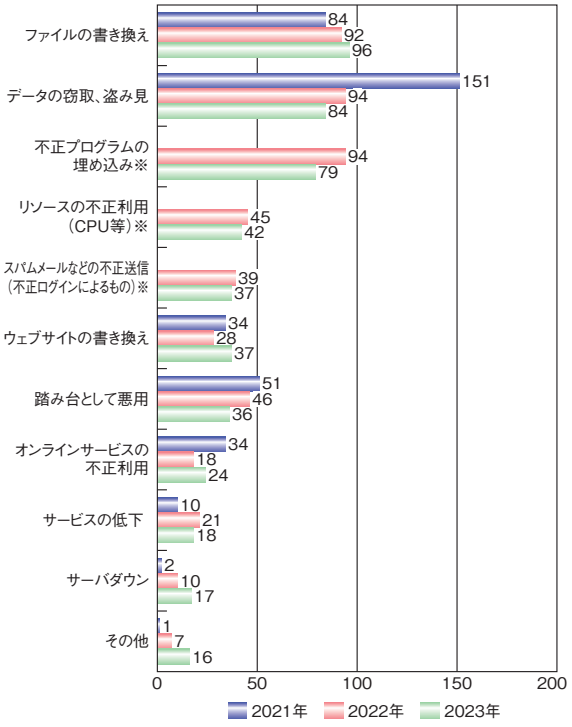
■図 B-3　不正アクセス手口別件数の推移（2021～2023 年）

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

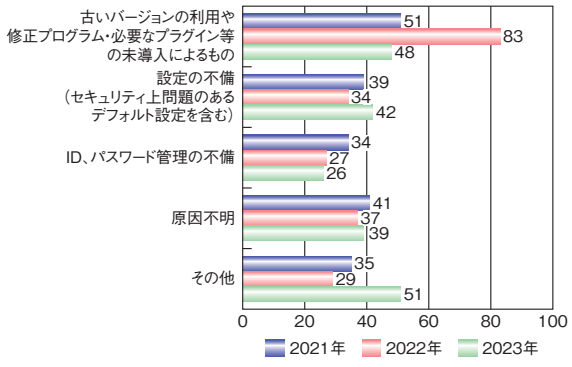
ピュータウイルス・不正アクセスの届出事例［2023 年下半期（7 月～ 12 月）］」を紹介している。そちらも、ぜひ参考にしていただきたい。



■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

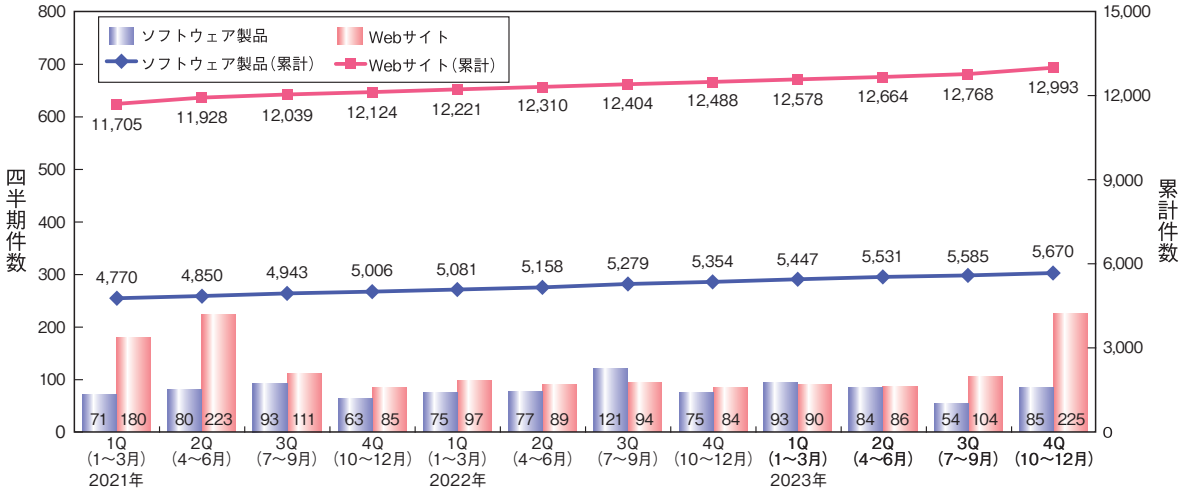
資料C　ソフトウェア等の脆弱性関連情報に関する届出状況

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）

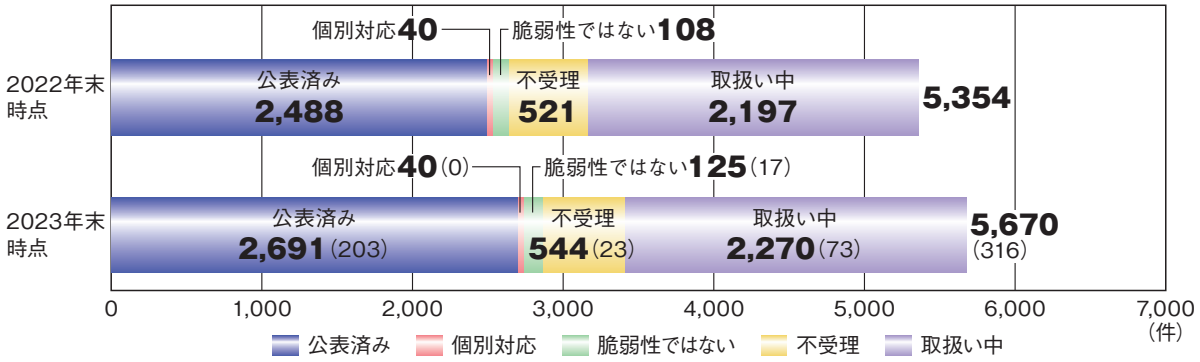
C.2　ソフトウェア製品の脆弱性届出の処理状況

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。

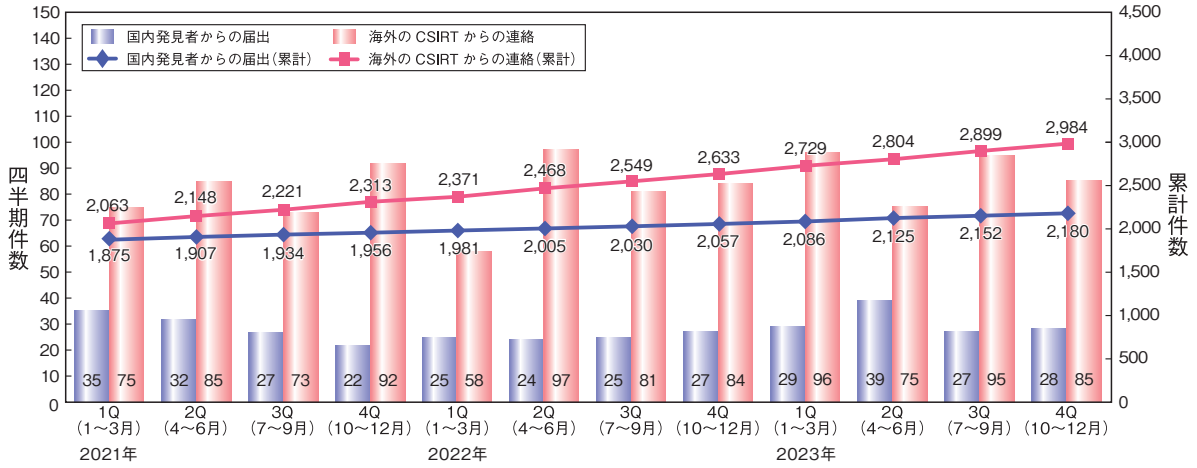
ソフトウェア製品の脆弱性対策情報の公表件数の累計は、国内発見者からの届出を公表したものが 2,180 件、海外の CSIRT から JPCERT/CC が連絡を受けたものを JVN で公表したものが 2,984 件となった。これらソフトウェア製品の脆弱性対策情報の公表件数の期別推移を図 C-3 に示す。

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



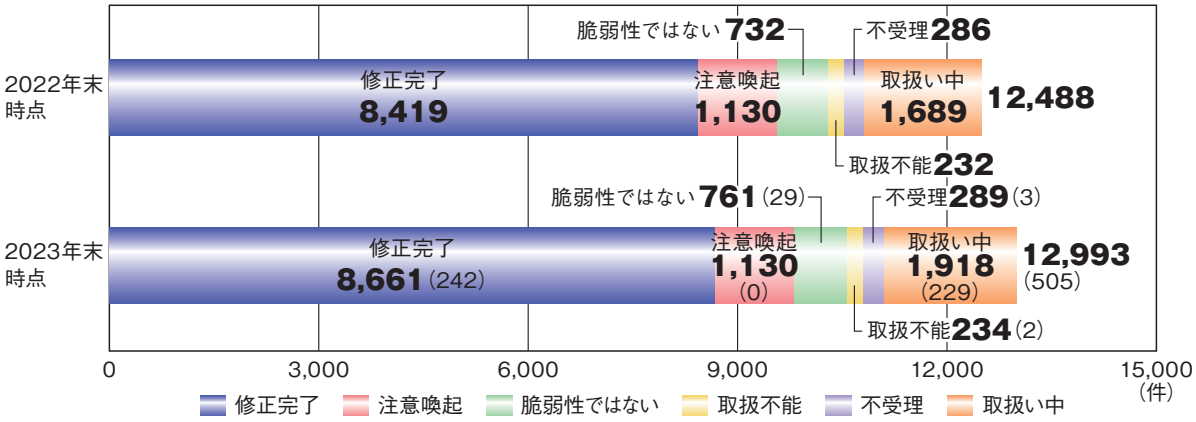
■図 C-3　ソフトウェア製品の脆弱性対策情報の公表件数

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。

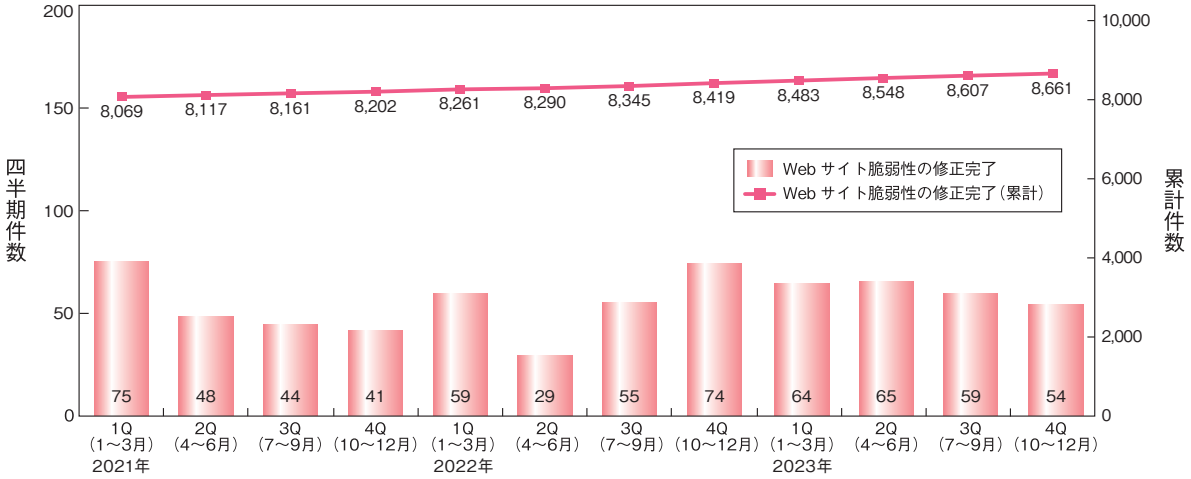
2023 年の届出のうち、IPA が通知を行い Web サイト運営者が「修正完了」としたものは 242 件で累計 8,661 件、IPA が「注意喚起」等を行った後に処理を終了したものは 0 件で累計 1,130 件、IPA 及び Web サイト運営者が「脆弱性ではない」と判断したものは 29 件で累計 761 件、Web サイト運営者と連絡が不可能なもの、または IPA が対応を促しても修正完了した旨の報告をしない、修正を拒否する等、Web サイト運営者の対応により「取扱不能」なものは 2 件で累計 234 件、告示で定める届出の対象に該当せず「不受理」としたものは 3 件で累計 289 件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

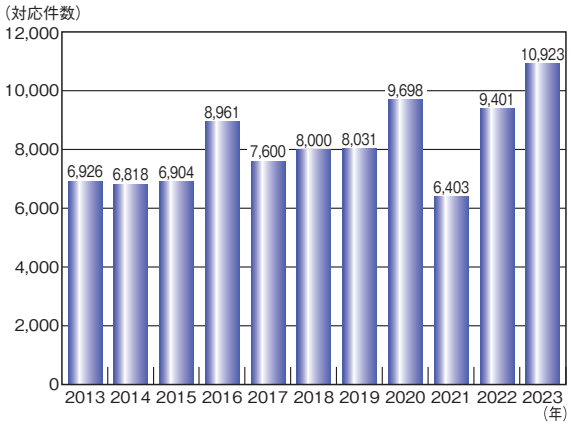
■ソフトウェア等の脆弱性関連情報に関する届出状況［2023年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/reports/vuln/software/2023q4.html

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

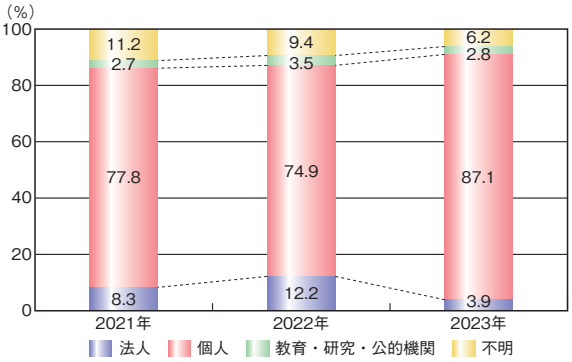
相談者の主体別では、2023 年も個人からの相談が 9,514 件（87.1%）と最も多かった。

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）

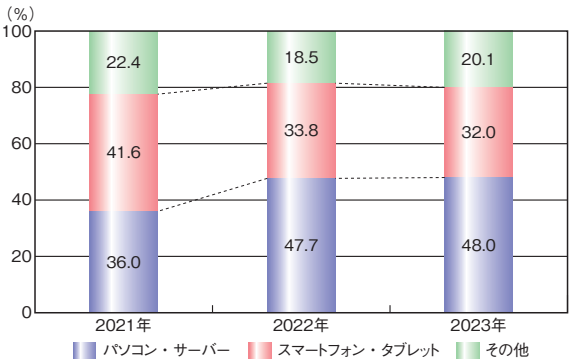
D.3　相談者の機器種別相談件数

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）

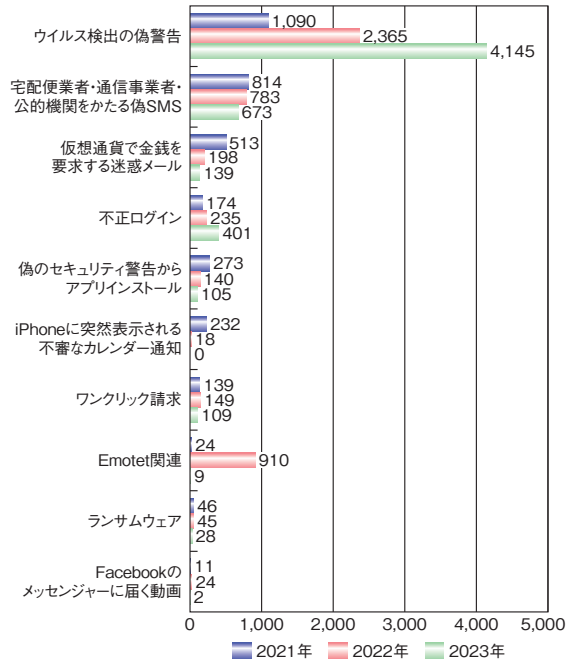


■図 D-3　情報セキュリティ安心相談窓口の機器種別相談件数の比率推移（2021～2023 年）

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

・本白書の引用、転載については、IPA Web サイトの「書籍・刊行物等に関するよくあるご質問と回答」（https://www.ipa.go.jp/publish/faq.html）に掲載されている「2. 引用や転載に関するご質問」をご参照ください。なお、出典元が IPA 以外の場合、当該出典元の許諾が必要となる場合があります。
・本白書は 2023 年度の出来事を主な対象とし、執筆時点の情報に基づいて記載しています。
・電話によるご質問、及び本白書に記載されている内容以外のご質問には一切お答えできません。あらかじめご了承ください。
・本白書に記載されている会社名、製品名、及びサービス名は、それぞれ各社の商標または登録商標です。本文中では、™ または ® マークは明記しておりません。
・本白書に掲載しているグラフ内の数値の合計は、小数点以下の端数処理により、100% にならない場合があります。

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**

Copyright © 2024 Information-technology Promotion Agency, Japan.