情報セキュリティ白書

Information Security White Paper

2025

一変する日常：支える仕組みを共に築こう

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2025」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。

サイバー空間を巡る脅威は年を追うごとに質・量ともに増大しております。2024 年も国内国外を問わず、ランサムウェア攻撃、標的型攻撃、DDoS 攻撃等、様々なサイバー攻撃による脅威に晒されました。また、今般の厳しい国際情勢下において、影響工作を始めとした地政学的背景に起因するサイバー空間のリスクも顕在化しております。サイバー攻撃の手口も、取引先や委託先等のサプライチェーン上でセキュリティ対策が不十分な部分を入口とするものや、複雑なソフトウェアのサプライチェーンの脆弱性を狙ったもの、更には、生成 AI を悪用したもの等、一層高度化・巧妙化しております。

他方、データ駆動型の便利で豊かな社会、Society 5.0 の実現を目指し、サイバー空間とフィジカル空間が融合していく中で、セキュリティ面でのリスクが顕在化してきております。これまでのフィジカル空間での経済社会行動が IoT 機器やロボット等、様々なデバイスとつながることによりデータ化され、ネット上のサイバー空間に集積し、そのビッグデータが生成 AI により解析、最適化されるサイクルの中で、サイバー攻撃を許す隙が増えるとともに、一度インシデントが起きるとその影響が瞬時に広範に伝播し、大規模な情報漏えいやインフラの機能不全をもたらすリスクがますます高まってきております。

こうした中で、国内では、2022 年 12 月に閣議決定された国家安全保障戦略において「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」との目標が掲げられ、2025 年 5 月にはサイバー対処能力強化法及び同整備法が成立し、「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るための能動的なサイバー防御を実施する体制の整備が進められています。

また、経済社会インフラが直面するサイバーリスクへの耐性を確保する観点から、システムの設計段階、すなわち、アーキテクチャーレベルでセキュリティを組み込んでいく、「セキュア・バイ・デザイン」の視点に立った様々な制度整備や取り組み、これらを推進していくための人材や技術等、サイバーセキュリティ供給能力の強化に向けた取り組み等も新たに動き出しております。

本白書が、2024 年度の情勢を踏まえた脅威分析と政策動向の総括を通じ、関係者の皆さまの日々の対策検討や実践に資するものであること、そしてより安全で信頼されるデジタル社会の確立に寄与する一助となることを、心より願っております。

2025年9月

独立行政法人情報処理推進機構（IPA）

理事長 齊藤 裕

目次

コラム

2025

情報セキュリティ白書

序章

2024年度の情報セキュリティの概況

近年、情報セキュリティの脅威は一層深刻化しており、サイバー攻撃の手法も高度化している。2024 年においては、ランサムウェア攻撃や、DDoS 攻撃等のインシデントが相次ぎ、重要インフラや企業の運営に影響を与えた。国内では 2024 年 6 月に、総合エンターテインメント企業がランサムウェア攻撃を受け、動画配信サービスやオンラインショップの障害、出荷遅延等の被害が生じた。また印刷会社に対するランサムウェア攻撃では、約 60 の委託元に影響が及んだ。これらのインシデントは、サービス停止や情報漏えいにより多数の企業・組織及び利用者に被害をもたらし、情報セキュリティ対策の重要性を改めて認識させた。国外では、鉄道、空港、水処理施設等の重要インフラに対してランサムウェア攻撃被害が発生し、安全保障の観点からも対策が急務となっている。

2024 年には、政治的なイベントに関連した DDoS 攻撃が増加し、公共の安全や秩序が脅かされる事態も発生した。2024 年 7 月、8 月にはオリンピック関連のスポンサー、パートナーの Web サイトを標的とした DDoS 攻撃が観測された。また 2024 年は世界各国で重要な選挙が行われ、選挙運動、政党、選挙インフラを対象とした DDoS 攻撃が観測された。米国では、大統領選挙を狙った DDoS 攻撃が 11 月に発生した。日本でも、2024 年 7 月と 10 月に安全保障イベントに関連した DDoS 攻撃が発生した。また、2024 年末から 2025 年初頭にかけて、航空会社、金融機関、携帯通信会社が相次いで DDoS 攻撃を受け被害が発生した。これらの攻撃には IoT ボットネットが利用されている。

2025 年 1 月、警察庁と NISC（現 NCO）は、2019 年ごろから継続していた複数の攻撃キャンペーンについて、国家に支援されたサイバー攻撃グループによるものとして注意喚起を行った。これらの攻撃は、日本の安全保障の棄損や先端技術情報の窃取を目的としており、攻撃手法の公表を通じて被害の拡大防止が呼びかけられた。

国際的には、国家を背景としたサイバー攻撃の激化による被害が発生した。「Salt Typhoon」と呼ばれる攻撃グループによる攻撃では、米国通信事業者 9 社を含む世界中の企業数十社のシステムへの侵入が観測され、広範なスパイ活動及び情報収集が行われたことが確認された。国家を背景とした攻撃グループに対しては複数の国、組織が連携し、情報共有や摘発を行っている。

2024 年は AI の悪用による被害も報告された。前述の選挙妨害においては生成 AI が偽情報の生成に多用されたという。偽情報の流布を利用した情報操作型サイバー攻撃は、社会の混乱や分断、政府機関の信頼失墜等、サイバー領域と認知領域の双方にわたる攻撃手段として，国家の安全保障上の脅威ともとらえられる。今後も警戒が必要である。

このような状況を踏まえ、日本国内においてもサイバーセキュリティ政策の強化が進められた。ランサムウェア攻撃の被害拡大や DDoS 攻撃における IoT 機器の悪用に対して、政府は 2024 年度のサイバーセキュリティ戦略において、サプライチェーン・リスクへの対応と DX 推進・支援の強化を掲げた。経済産業省は「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」「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス」の発行等で、設計段階からセキュリティを考慮するセキュア・バイ・デザインの施策を推進した。また、2025 年 3 月には IoT 製品のセキュリティ評価認証制度として「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の運用が開始された。更に、サプライチェーン強化に向けたセキュリティ対策評価制度の検討等にも取り組んでいる。

サイバー安全保障分野では、「外部からのサイバー攻撃について、被害が発生する前の段階から、その兆候に係る情報その他の情報の収集を通じて探知し、その主体を特定するとともに、その排除のための措置を講ずることにより、国家及び国民の安全を損なうおそれのあるサイバー攻撃の発生並びにこれによる被害の発生及び拡大の防止」を図る「能動的サイバー防御」の実現に向けた検討が進められた。その結果、2025 年 5 月には「重要電子計算機に対する不正な行為による被害の防止に関する法律」及び「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律」が成立した。今後、官民連携の強化、通信情報の利用、攻撃サーバーの無害化等の実践を通じ、サイバー安全保障分野での対応能力向上が期待される。

	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
2024年 4月	● 米国のセキュリティベンダーが提供するファイアウォール用OSに対するゼロデイ攻撃を確認（1.2.4） ● 米国のマルチクラウドデータウェアハウスプラットフォームを利用している複数の組織を標的としたデータ侵害が発生（1.1.1）	● 米国「外国敵対勢力が管理するアプリから米国人を保護する法」成立（4.1.1）
5月	● 国家の支援が疑われるサイバー攻撃グループが、国内の暗号資産関連事業者から約482億円相当の暗号資産を窃取（1.2.2） ● 行政機関等から通知書等の印刷と発送を請け負っていた印刷会社でランサムウェア被害が発生（1.2.1）	● 「重要経済安保情報保護活用法」成立（3.1.1） ● NISCと警察庁が、米国CISAの作成したサイバー脅威緩和に関する国際ガイダンスに共同署名（4.1.1） ● 「AIソウル・サミット」開催（2.1.3）
6月	● 総合エンタメ企業が展開する動画共有サービス等がランサムウェア攻撃を受け、サービス停止（1.2.1）	● 「G7プーリア・サミット」開催（3.1.1）
7月	● 日本・NATOの活動に抗議するDDoS攻撃が発生（1.2.3） ● 米国サイバーセキュリティ会社のシステム障害により世界約850万台のWindowsデバイスに影響が発生（1.1.1） ● パリオリンピック関連のスポンサー、パートナーを標的としたDDoS攻撃が発生（1.1.1）	● NISCと警察庁は、オーストラリアのACSCが作成したAPT40に関する国際アドバイザリーに共同署名（4.1.1） ● NISC「サイバーセキュリティ2024」公表（3.1.1） ● NISTは、生成AIのセキュア開発のためのプロファイルである「SP 800-218A」公開（4.1.2）
8月	● 不動産仲介業の従業員が同業他社に転職する際、不動産登記簿に基づく社内資料を不正に持ち出し（1.2.7） ● 米国の国際空港がランサムウェア攻撃を受け、フライト情報表示等の重要な機能に影響が発生（1.2.5）	● EU「AI Act」発効（2.1.1、2.1.3） ● 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ver 2.0」公表（3.1.3）
9月	● 米国司法省は、国家の支援が疑われる攻撃グループに侵害された20万台超の消費者向け機器からなるボットネットを無害化したと発表（1.2.2） ● 米国の水処理施設にランサムウェア攻撃（1.2.5）	
10月	● ランサムウェア開発者らを欧州刑事警察機構等による共同捜査により逮捕（4.1.1） ● 日米共同統合演習に抗議するDDoS攻撃が発生（1.2.3）	● オーストラリアのACSCは、重要インフラ事業者に向けて策定した「OTサイバーセキュリティの原則」公開（4.1.5）
11月	● 米国大統領選挙で、複数の国家が関与すると見られる影響工作を確認（2.2.3） ● 米国大統領選挙期間中に大規模なDDoS攻撃が数日にわたって発生（1.1.1） ● 国家の支援が疑われる攻撃グループが9社の米国通信事業者、及び世界中の企業数十社を侵害していたことをFBI等が公表（1.1.1、1.2.5）	● IPAとAJCCBCは、オランダのNCSCと協働し、タイで重要情報インフラ保護に関する人材育成プログラムを提供（4.1.1） ● 経済産業省とIPAは、米国政府・EU政府と連携し、「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（4.1.1）
12月	● 米国の地域交通局がランサムウェア攻撃を受け、鉄道の遅延等の一時的な混乱が発生（1.2.5） ● 年末から年始にかけて国内の重要インフラ企業等へ大規模なDDoS攻撃が発生（1.2.3）	● EU「サイバーレジリエンス法」発効（4.1.3） ● 国連総会にて、サイバー犯罪に関する包括的な国際条約である「国連サイバー犯罪条約」採択（4.1.1） ● EUのサイバーセキュリティ能力を強化する「サイバー連帯法」及び「改正サイバーセキュリティ法（CSA）」が成立（4.1.3）
2025年 1月	● 警察庁及びNISCは、安全保障や先端技術に係る情報窃取を目的とした攻撃キャンペーンについて、国家の関与が疑われる組織的なサイバー攻撃活動であるとして注意喚起（1.2.2）	● 「U.S. Cyber Trust Mark」運用開始（4.1.2） ● 米国大統領令14144、ソフトウェアサプライチェーンセキュリティ強化策等を指示（4.1.2） ● EU「デジタルオペレーショナルレジリエンス法」全面適用開始（4.1.3） ● 米国大統領令14179、Biden政権のAI統制施策を棄却（4.1.2）
2月	● 営業秘密にあたる研究データを外国企業に漏えいしたとして国立研究開発法人の元研究員に有罪判決（1.2.7）	● 「AIアクションサミット」開催（2.1.3） ● 「サイバー対処能力強化法案」及び「同整備法案」が閣議決定（3.1.1） ● 米国DHS、CISA等所管機関の活動縮小（4.1.2）
3月	● 地方銀行をかたる自動音声を含む電話による大規模なボイスフィッシング被害が発生（1.1.2）	● 経済産業省「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）」公開（3.1.3） ● IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」運用開始（3.3.1）

※表には、2024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。表中の数字は本白書中に掲載している項目番号である。他のインシデント・事件や、政策・イベント等については本文を参照いただきたい。

第3章
国内の政策及び取り組みの動向

2024 年度以降、我が国のサイバー安全保障分野での対応能力向上を目的とした各種法整備が進み、政府機関等により、これに関連した様々な取り組みが開始された。また、網羅的なセキュリティ対策強化のため、中小企業を含む人材育成の取り組みや機会創出、評価・認証制度の運営、普及啓発活動も進んでいる。本章ではサイバーセキュリティに関する国内の政策、取り組みについて解説する。

3.1 国内のサイバーセキュリティ政策の状況

本節では、政府が推進するサイバーセキュリティ政策の状況について述べる。

3.1.1 政府全体の政策動向

本項では、政府が特に注力している取り組みについて取り上げる。具体的には、サイバー安全保障に関する取り組み、「サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）※1」において特に強力に取り組むとされた施策を紹介する。また、経済安全保障に関する取り組みを紹介する。

(1) サイバー安全保障に関する取り組み（能動的サイバー防御の実現に向けた検討等）

2022 年に閣議決定された「国家安全保障戦略※2」において、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、能動的サイバー防御の導入のため、①官民連携の強化、②通信情報の利用、③攻撃者のサーバー等への侵入・無害化、④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）の発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置等の実現に向け検討を進めるとされた。本項では、これらの実現に向けた検討を行うために開催された有識者会議の提言、及び同提言を踏まえて制定された「重要電子計算機に対する不正な行為による被害の防止に関する法律※3」（以下、サイバー対処能力強化法）、「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律※4」（以下、整備法）の概要を紹介する。

(a) サイバー安全保障分野での対応能力の向上に向けた提言

「国家安全保障戦略」に基づき新たな取り組みの実現に必要となる法制度の整備等の検討のため、「サイバー安全保障分野での対応能力の向上に向けた有識者会議※5」が立ち上げられ、4 回の全体会議、及び以下をテーマとした計 9 回のテーマ別会合で検討を行った。

①官民連携の強化
②通信情報の利用
③アクセス・無害化

その結果、実現すべき具体的な方向性について、上記 3 テーマ及びそれぞれのテーマについて議論を行う中で明らかになった④横断的課題について「サイバー安全保障分野での対応能力の向上に向けた提言※6」を取りまとめた。各テーマについての提言の概要は以下のとおりである。

①官民連携の強化
- 官民双方向の情報共有を促進すべき。
- 技術情報に加え、経営層が判断を下す際に必要な、攻撃の背景や目的等も共有されるべき。
- 特に漏えいにより我が国の安全保障に支障を与えるおそれがある情報等を扱う場合にはセキュリティ・クリアランス制度を活用する等、適切な情報管理と情報共有を両立する仕組みを構築すべき。
- ベンダーとの連携を深めるべき。ベンダーが利用者とリスクコミュニケーションを行うべき旨を法的責務として位置付けるべき。

- 基幹インフラ事業者によるインシデント報告の義務化のほか、その保有重要機器の機種名等の届出を求め、攻撃関連情報の迅速な提供等ができる仕組みを整えるべき。被害組織の負担軽減等のため、報告先や様式の一元化、簡素化等を進めるべき。

②通信情報の利用

- 先進主要国は国家安全保障の観点からサイバー攻撃対策のため事前に対象を特定せず通信情報を収集して分析しており、我が国でも一定の条件下での通信情報の利用を検討すべき。
- 外外通信（国内を経由し伝送される国外から国外への通信）は先進主要国と同等の方法の分析が必要。加えて、外内通信（国外から国内への通信）及び内外通信（国内から国外への通信）についても必要な分析をできるようにしておくべき。
- コミュニケーションの本質的内容に関わる部分は分析の必要があるとは言えない。機械的にデータを選別し検索条件等で絞る等の工夫が必要。
- 通信の秘密であっても公共の福祉のために必要かつ合理的な制限を受ける。取得及び情報処理のプロセスについて独立機関の監督が重要。
- 通信当事者の有効な同意がある場合の通信情報の利用は、同意がない場合とは異なる内容の制度により実施することも可能。
- 性質上非公開とすべき範囲はあるが、適切な情報公開は行われるべき。公開困難な部分を独立機関の監督で補うべき。

③アクセス・無害化

- サイバー攻撃の特徴を踏まえ、被害防止を目的としたアクセス・無害化を行う権限は、緊急性を意識し、事象や状況の変化に応じて臨機応変かつ即時に対処可能な制度にすべき。比例原則を遵守し、必要な範囲で実施されるものとするため、警察官職務執行法を参考としつつ、適正な実施を確保するための検討を行うべき。
- 武力攻撃事態に至らない段階から我が国を全方位でシームレスに守るための制度とすべき。
- 権限の執行主体は、警察や防衛省・自衛隊とし、共同で実効的に措置を実施可能な制度とすべき。
- 措置の対象は、国、重要インフラ、事態発生時等に自衛隊等の活動が依存するインフラ等へのサイバー攻撃に重点を置く一方、必要性が認められる場合には、適切にアクセス・無害化が実施できるような仕組みとすべき。
- 国際法上許容される範囲でアクセス・無害化が行われるような仕組みを検討すべき。

④横断的課題

- サイバーセキュリティ戦略本部の構成等を見直すとともに、NISC の発展的改組にあたり、政府の司令塔として強力な情報収集・分析、対処調整機能を有する組織とすべき。
- 重要インフラに求められるサイバーセキュリティ対策の水準を示し、常に見直しを図る制度とすべき。
- 政府主導での高品質な国産セキュリティ製品、サービス供給の強化を支援すべき。
- 官民の人材交流を強化すべき。
- 中小企業等のセキュリティ対策についての支援拡充やサプライチェーン企業の対策水準を検討すべき。

同提言に基づき、後述のサイバー対処能力強化法及び整備法が制定された。また、サイバーセキュリティ戦略本部は、2025 年 5 月、同提言等を踏まえ、「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項※7」を決定し、現行制度下において喫緊に取り組むべき施策の方向性を取りまとめるとともに、改組後のサイバーセキュリティ戦略本部において 2025 年内を目途に新たな「サイバーセキュリティ戦略」を策定することとした。同決定で示された施策の方向性の概要は以下のとおりである。

- 新たな司令塔機能の確立
  - NISC を我が国におけるサイバーセキュリティの司令塔機能を担う新組織へ発展的に改組する。
  - サイバー脅威に関するすべての利用可能な情報による付加価値の高い分析に基づき、国際連携・官民連携により、政府全体で被害の未然防止・拡大防止を含めた対応を行うため、新組織を中心に、高度な情報収集・分析能力を担う体制・基盤・人材等を総合的に整備する。
- 巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化
  - 新組織を中心に官民連携基盤を整備し、適切な情報保全・管理に基づく政府からの積極的な情報提供及び報告等に係る民間の負担軽減を進め、官民双方向の情報共有を求心力とした、認識共有・信頼醸成に基づく新たな官民連携エコシステムの実現を図る。
  - 政府機関等について、横断的な監視体制を強化・高度化し、セキュリティ対策水準の向上及び実効

性の確保を図る。また、IoT 製品のセキュリティ評価制度である「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」について、政府機関等の調達の選定基準に含める。

- 単独での対策が困難な小規模自治体も念頭に置いた人材確保等の支援や、診療等への影響を最小限にするため、医療機関等に対する初動対応等の支援を推進する。
- 政府機関・重要インフラ等を通じ、官民横断的な対策の強化を図るため、脅威ハンティングの実施拡大や、実践的対応力の強化を推進する。また、重要インフラについては、分野特性を踏まえつつ、分野横断的な新たな基準を策定する。
- 社会全体のセキュリティ確保の強化に向け、セキュアバイデザイン原則等に基づき、IoT 製品等のセキュリティ対策やソフトウェアの透明性確保等に係る取り組みを推進し、普及・浸透を図る。
- 中小企業等を含めたサプライチェーン全体のレジリエンス強化に向け、リスクに応じた対策水準の提示、対策サービスに係る支援、関係法令の適用関係の明確化等、対応力に応じたサイバーセキュリティ対策の実装拡大に向けた取り組みを推進する。

- サイバーセキュリティを支える人的・技術的基盤の整備
  - 官民を通じた人材の育成・確保のため、関係政府機関等における高度人材の確保・育成に向けた民間人材の活用や演習環境の構築の推進とともに、官民共通の「人材フレームワーク」を策定し、官民を通じた実態把握やキャリアパス設計等を進める。
  - サイバーセキュリティ関連技術について、官のニーズを踏まえた研究開発・実証等を通じた技術情報等の提供や、政府機関等による積極的な活用等により、国内産業の育成及び早期の社会実装による新たな技術・サービスを生み出すエコシステムの形成を図るとともに、先端技術について、国際的な動向を踏まえ、AI に係る安全性の確保や耐量子計算機暗号（PQC：Post-Quantum Cryptography）への移行等に関して対応を進める。
- 国際連携を通じた我が国のプレゼンス強化
  - 国際的なルール整備に関し、二国間・多国間関係を強化・進展させるとともに、ASEAN・太平洋島しょ国等に対する能力構築プログラムを提供し、協力関係を強化する。

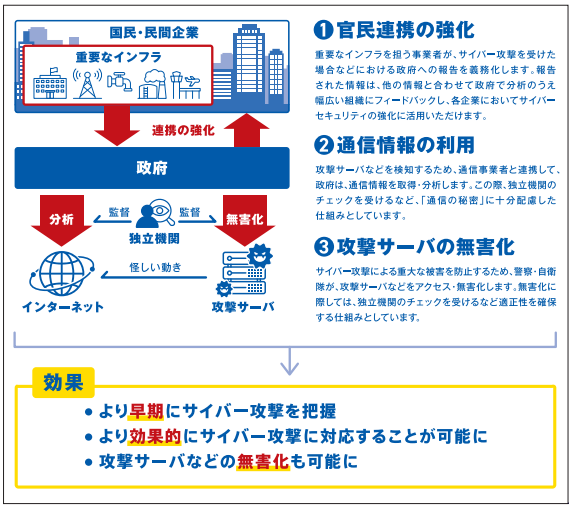
2025 年 7 月 1 日には、NISC が発展的に改組され、サイバー安全保障も含め、官民を通じたサイバーセキュリティの確保に関する司令塔として、内閣サイバー官を長とする国家サイバー統括室（NCO：National Cybersecurity Office）が発足した[※8]。

(b) サイバー対処能力強化法及び整備法

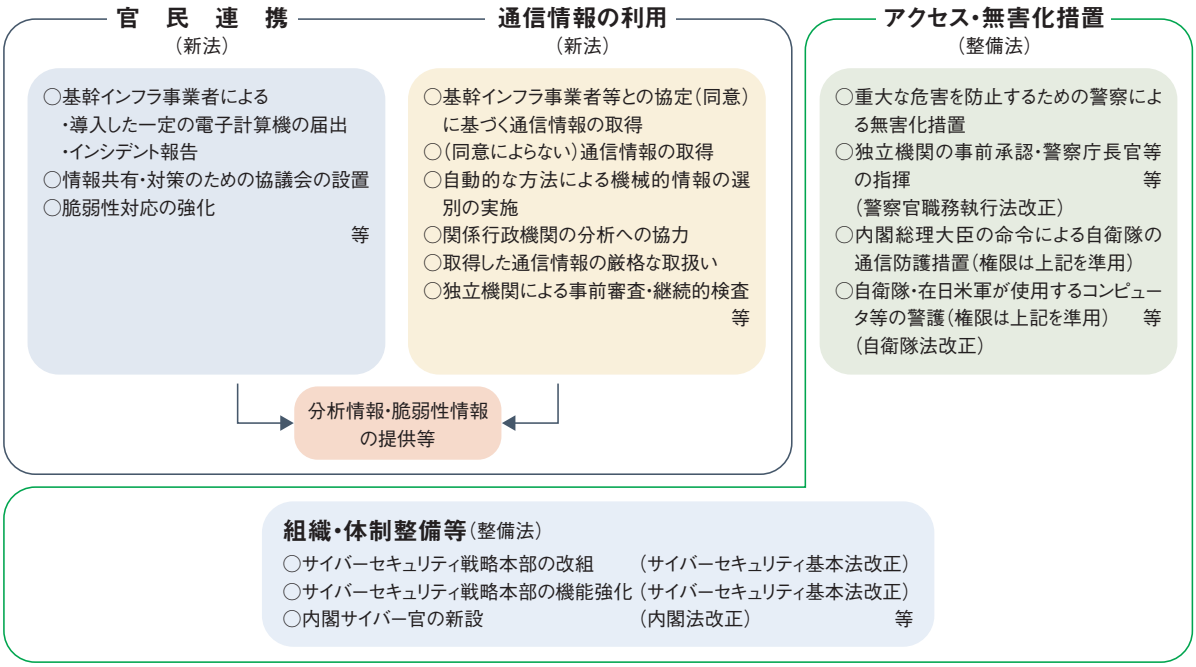
「国家安全保障戦略」及び前述の提言を踏まえて 2025 年 2 月、サイバー対処能力強化法案及び整備法案が閣議決定され、同年 5 月に成立し[※9]、同月、サイバー対処能力強化法及び整備法として公布された[※10]。

両法律の制定の背景としては、上述のとおり「国家安全保障戦略」において能動的サイバー防御の導入に向けた検討が閣議決定されたことに加え、IT 系システムの侵害、有事に備えた重要インフラ等への侵入、機微情報の窃取等のサイバー安全保障に関わる攻撃が巧妙化・深刻化するとともに、サイバー攻撃関連通信や被害数が年々増加傾向にあり、質・量両面でサイバー攻撃の脅威が増大していること、欧米主要国が官民連携や通信情報の利用、アクセス・無害化について先行した取り組みを行っていることが挙げられる[※10]。そこで、国民生活や経済活動の基盤及び国家及び国民の安全をサイバー攻撃から守るため、欧米主要国における取り組みも参考に、能動的サイバー防御を実施する体制を整備するため、両法律が制定された。

サイバー対処能力強化法は①官民連携、②通信情報の利用、③分析情報・脆弱性情報の提供等を規定し、整備法は④アクセス・無害化措置、⑤組織・体制整備等を規定（関係法律の改正）している。図 3-1-1 は、両法律により実現する能動的サイバー防御のポイントを示す図である。また、図 3-1-2（次ページ）は、両法律の概



■図 3-1-1　能動的サイバー防御のポイント
（出典）内閣官房「みんなで備えよう。新・サイバー防御、はじまる。[※11]」



■図 3-1-2　サイバー対処能力強化法（図中の「新法」）及び整備法の概要
（出典）内閣官房「重要電子計算機に対する不正な行為による被害の防止に関する法律案 及び 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律案 概要※12」を基に IPA が編集

要である。

サイバー対処能力強化法及び整備法における①～⑤に係る規定の概要は以下のとおりである。内容が広範にわたるため、詳細については内閣官房の説明資料等を参照されたい※13。

①官民連携の強化

- 基幹インフラ事業者によるインシデント報告等
  - 基幹インフラ事業者※14 が特定重要電子計算機（サイバーセキュリティが害された場合に、特定重要設備の機能が停止し、または低下するおそれがある一定の電子計算機）を導入した際の事業所管大臣への届出
  - 基幹インフラ事業者が特定重要電子計算機のインシデント情報等を認知した際の事業所管大臣・内閣総理大臣への報告
- 情報共有・対策のための協議会の設置
- 電子計算機の使用者に対する情報共有
- 脆弱性対応の強化等
  - 内閣総理大臣・電子計算機等供給事業所管大臣（電子計算機やそれに組み込まれるプログラムの供給を行う事業を所管する大臣。経済産業大臣等※15）が重要電子計算機として用いられる電子計算機やプログラムにおける脆弱性を認知した際の当該電子計算機等の供給者に対する情報提供
  - 脆弱性が基幹インフラ事業者が使用する特定重要電子計算機に用いられる電子計算機等に関連する場合、電子計算機等供給事業所管大臣が、当該電子計算機等の供給者に対し、サイバー攻撃による被害を防止するために必要な措置を講ずるよう要請
- 罰則の整備
  - 行政職員・協議会構成員等による秘密の不正な利用・漏えいの行為に対する罰則
  - 基幹インフラ事業者が、インシデント報告等を行わず、是正命令を受けてもなお対応しない場合、または、インシデント報告等に関連し、資料提出等を求められても対応しない場合の罰則

②通信情報の利用

- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得
  内閣総理大臣は、基幹インフラ事業者等との協定に基づき、通信情報を取得し、取得した通信情報のうち、外内通信に係るものを用いて分析を実施し、当該事業者に必要な分析結果を提供する。
  なお、この場合の通信情報の取得は、協定（同意）に基づくため、通信の秘密に抵触しない。
- （同意によらない）通信情報の取得
  内閣総理大臣は、国外の攻撃インフラ等の実態把握のため必要があると認める場合には、サイバー通

信情報監理委員会（いわゆる 3 条委員会）の承認を受け、外外通信の通信情報を取得することができる。また、内閣総理大臣は、国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要があると認める場合には、サイバー通信情報監理委員会の承認を受け、外内通信または内外通信の通信情報を取得することができる。

- 自動的な方法による機械的情報の選別の実施

  内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、調査すべきサイバー攻撃に関係があると認めるに足りる機械的情報（IP アドレス、指令情報等のコミュニケーションの本質的な内容ではない情報（図 3-1-3））を選別し、それ以外のものを直ちに消去する措置を講ずることとされている。

コミュニケーションの本質的な内容に**当たらない例**	○ 送受信日時 2024.04.01 12:00:04 ○ IPアドレス 103.23.145.84 ○ 通信量 20kB ○ ポート番号 80 ○ コマンド POST/ A3fe e3844A7D35300734D2BA HTTP/1.1 ○ プロトコル（通信方式） HTTP / SSL / SMTP ○ ソフトウェアの種類 Mozilla/4.0(…Trident/7.0;NET4.0c;…)… ○ ドメイン名 cas.go.jp ○ メールアドレス hogehoge@example.com （個人情報保護の観点から、個人を識別することができないように加工することが必要）
コミュニケーションの本質的な内容に**当たる例**	× 電子メールの本文・件名 × 添付ファイルの内容・名称 × IP電話の通話内容 × Webサイトに掲載されている文章、画像

■図 3-1-3　コミュニケーションの本質的な内容ではない情報の例
（出典）内閣官房「サイバー対処能力強化法及び同整備法について※9」を基に IPA が編集

- 独立機関による事前審査・継続的検査

  通信情報の利用の適正確保のため、サイバー通信情報監理委員会を設置し、内閣総理大臣による（同意によらない）国外関係通信の取得に際しての遅滞のない審査・承認、通信情報の取り扱いに対する継続的な検査、無害化措置に際しての審査・承認等の事務等を行わせることとする。

  同委員会は、承認件数等について国会に報告するとともに、その概要を公表しなければならない。

  なお、通信情報の漏えいや盗用については罰則が定められている。

- 罰則の整備
  - 通信情報を取り扱う行政職員による通信情報の不正な利用・漏えいの行為に対する罰則
  - 通信情報を保有する行政機関の管理を侵害して通信情報を取得する行為に対する罰則

③分析情報・脆弱性情報の提供等

内閣総理大臣は、基幹インフラ事業者によるインシデント報告や選別後の通信情報、協議会を通じて得た情報等の整理・分析を行い、整理・分析した情報（分析情報）を、サイバーセキュリティ確保のため、関係行政機関に提供する。必要に応じて、外国政府等にも提供できる。また、事業所管大臣は、必要に応じ、基幹インフラ事業者に対して分析情報を提供できる。

そのほか、前記①で述べたように、脆弱性対応の強化のための関係者への情報提供や、協議会における情報共有等が規定されている（次ページ図 3-1-4）。

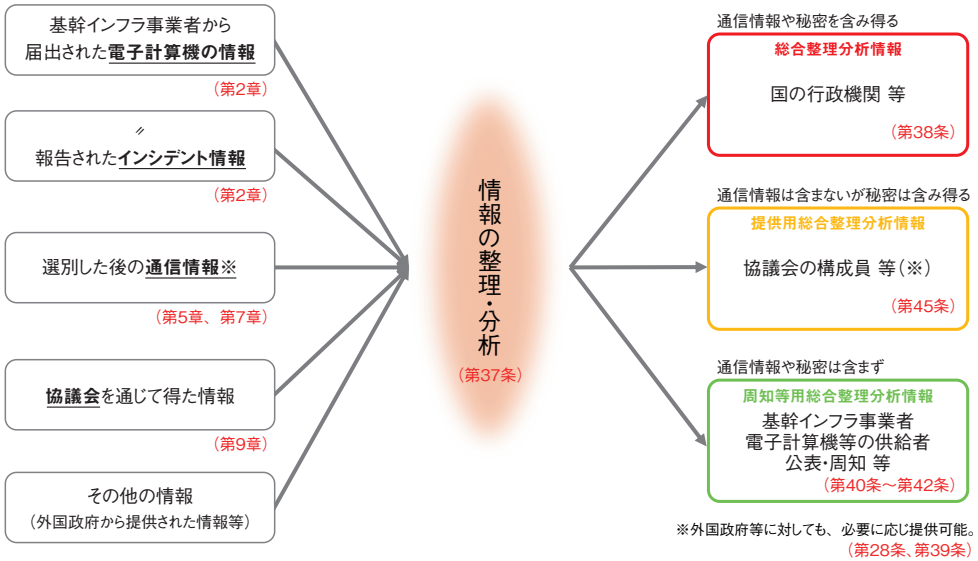
④アクセス・無害化措置

- 警察によるアクセス・無害化措置（警察官職務執行法の改正）

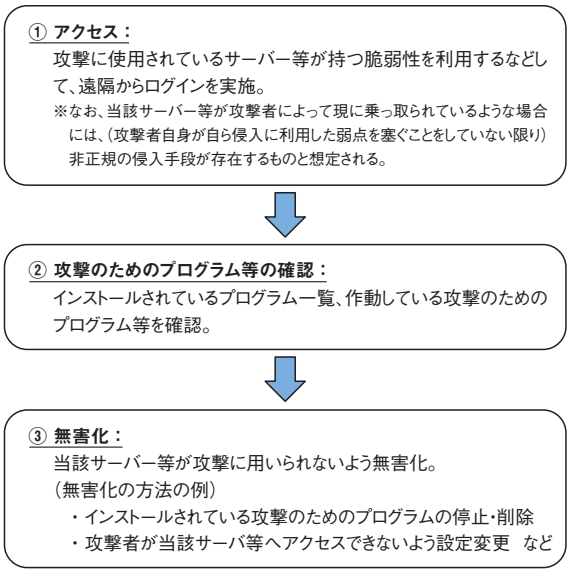
  警察庁長官が指名する警察官（サイバー危害防止措置執行官）は、サイバー攻撃に用いられる通信等を認めた場合であって、そのまま放置すれば重大な危害が発生するおそれがあるため緊急の必要があるときは、サイバー攻撃の送信元等であるサーバー等の管理者等に対し、攻撃のためのプログラムの停止・削除等の措置（当該サーバー等にアクセスし、インストールされた攻撃のためのプログラム等を確認することを含む）を命じ、または自ら当該措置を実施することができる（アクセス・無害化のステップについては、次ページ図 3-1-5 参照）。国外のサーバー等への措置に際しては、外務大臣との事前協議が必要とされている。また、措置に際しては、原則、サイバー通信情報監理委員会の事前の承認が必要である。

- 防衛省・自衛隊によるアクセス・無害化措置（自衛隊法の改正）

  国や基幹インフラ等の重要電子計算機に対する攻撃であり、外国政府を背景とする主体による高度の攻撃と認められるものが行われ、自衛隊が対処する特別の必要があるときは、内閣総理大臣が当該重要電子計算機に対する通信防護措置をとるべき旨を命ずることができる。通信防護措置を命ぜられた部隊等は、警察と共同して当該措置を実施する。その際、改正警察官職務執行法を準用し、サイバー



■図 3-1-4　分析情報・脆弱性情報の提供等のイメージ
（出典）内閣官房「サイバー対処能力強化法及び同整備法について」



■図 3-1-5　アクセス・無害化のステップ（イメージ）
（出典）内閣官房「サイバー対処能力強化法及び同整備法について」を基に IPA が編集

通信情報監理委員会の事前の承認等のもとでアクセス・無害化措置を実施することができる。

また、自衛隊及び在日米軍が使用する電子計算機をサイバー攻撃から職務上警護する自衛官についても、緊急の必要があるときには、同法を準用し、アクセス・無害化措置を実施できる。

なお、アクセス・無害化については、その実施主体が警察及び自衛隊になるが、こうした措置は国家安全保障の観点から整合性の取れた形で行われる必要があり、内閣官房（新組織）が、国家安全保障局とも連携しつつ、その司令塔機能を発揮する必要がある[※10]。

⑤組織・体制整備等（関係法律の改正）

- 政府を挙げた取り組みを推進するための体制整備
  - サイバーセキュリティ戦略本部を、内閣総理大臣を本部長、すべての国務大臣を本部員とする組織に改組するとともに、有識者から構成されるサイバーセキュリティ推進専門家会議を新設
  - サイバーセキュリティ戦略本部の所掌事務に、重要インフラ事業者等のサイバーセキュリティ確保に関する国の施策の基準の作成及び国の行政機関等におけるサイバーセキュリティの確保の状況の評価等を追加し、機能強化
  - 内閣府の所掌事務にサイバー対処能力強化法に基づく官民連携の強化及び通信情報の利用に関する事務を追加するとともに、同府にサイバー通信情報監理委員会を設置。また、サイバー対処能力強化法に係る事務を掌理する内閣府特命担当大臣の設置
  - 内閣官房に、サイバーセキュリティの確保に関する総合調整等の事務を掌理する内閣サイバー官を新設
  - IPA の業務に、情報の整理分析及び被害防止に必要な情報の周知等の事務並びに重要インフラ事業者等のサイバーセキュリティの確保の状況の調査を追加
  - 国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）の業務に、国

等の情報システムに対する不正な活動の監視及び分析に係る事務を追加

サイバー対処能力強化法及び整備法は、一部を除き、公布の日（2025 年 5 月 23 日）から起算して 1 年 6 ヵ月以内（サイバー対処能力強化法のうち、サイバー通信情報監理委員会の設置については公布日から 1 年以内、通信情報の利用については一部を除き 2 年 6 ヵ月以内、整備法のうち、サイバーセキュリティ戦略本部の改組、内閣サイバー官の設置等については、6 ヵ月以内）で政令で定める日から施行される。

今後、サイバー対処能力強化法第 3 条に基づき閣議決定される基本方針に基づき、上記の事項等が具体化される。

(2) 年次計画に基づく取り組み

政府は、「サイバーセキュリティ基本法[※16]」に基づき、3 年程度の間のサイバーセキュリティに係る諸施策の目標及び実施方針を示すサイバーセキュリティ戦略を策定するとともに、同戦略を的確に実施するために、各年度の年次計画を作成し、サイバーセキュリティ施策を推進している。

本項では、2024 年 7 月に策定された「サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）」（以下、年次計画）において「特に強力に取り組む施策」として掲げられているものに関連する取り組みを中心に紹介する。

(a) 政府機関や重要インフラ等の対処能力の向上

年次計画では、国全体のリスクの低減とレジリエンスの向上を図るため、「政府機関や重要インフラ等の対処能力の向上」が必要であり、そのために政府機関におけるサイバーセキュリティ体制の抜本的強化、重要インフラ演習の強化及び個別分野におけるレジリエンス向上、IPA の機能強化及び NICT の取り組み強化を通じたサイバーセキュリティ対策の底上げ等に取り組むこととされた。

- 政府機関におけるサイバーセキュリティ体制の抜本的強化

  政府機関等が講ずるべき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」が 2023 年に令和 5 年度版[※17]に改定されたのを受け、NISC は、2024 年 7 月に「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）」の一部改定[※18]、同年 10 月に「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の改定[※19]を行った。また、NISC は、同年 7 月、政府機関等の情報システムを対象とした横断的アタックサーフェスマネジメント（ASM）事業を開始した[※20]。そのほか、年次計画には、デジタル庁における総合運用・監視システムによる運用監視の開始（「3.1.2 (2) 総合運用・監視システム（COSMOS）の整備」参照）や、安全性や透明性の検証が可能な国産センサーを導入し、得られた情報を集約して分析し、我が国独自にサイバーセキュリティに関する情報の生成を行うこと等が取り組みとして掲げられている。

- 重要インフラ演習の強化及び個別分野におけるレジリエンス向上

  2024 年度、NISC は、2006 年度から重要インフラ事業者等向けに実施してきた「分野横断的演習」を「全分野一斉演習」として実施するとともに、官民間の連携の実践に重点を置いた新たな「官民連携演習」も実施した。重要インフラ事業者等の障害対応体制の有効性検証を目的とする「全分野一斉演習」は、2024 年 12 月 5 日に机上演習形式で行われ、重要インフラ事業者等（情報通信、金融、電力等の 15 分野）、重要インフラ所管省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）、セプター（15 分野 21 セプター）、サイバーセキュリティ関係機関（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））が参加した。同演習では、情報収集については速やかに対応できているものの、関係機関等への情報共有や緊急時における事業継続の対応については手順書の有無の把握や手順書の即座の参照・行動ができていない点が明らかとなった。また、他業種・他組織へ影響が及ぶ脅威を想定して官民連携（連絡体制・情報共有等）の手順を重点的に確認・検証・強化することを目的とした新たな取り組みである「官民連携演習」は、同年 10 月 16 日（予行）及び 2025 年 2 月 13 日（試行）に机上演習形式で行われた。同演習には、NISC、情報通信分野・電力分野の事業者、セプター及び所管省庁、サイバーセキュリティ関係機関が参加した（予行は 16 組織、試行は 21 組織が参加）。同演習を通じて、政府からの注意喚起等を発出する際に事業者に期待するアクションを明らかにすることや、被害組織からの攻撃に関する情報提供、それを踏まえた政府・事業者間でそれぞれ付加価値を付けて情報を回していくことの重

要性が認識された※21。

医療機関に向けた取り組みとして、厚生労働省は、医療法に基づく医療機関に対する立入検査の際に確認するサイバーセキュリティ対策の項目について、医療情報システムの安全管理に関するガイドラインから特に取り組むべき重要な項目を抽出した「令和6年度版 医療機関におけるサイバーセキュリティ対策チェックリスト※22」及びその解説である「令和6年度版 医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～※23」の公表（2024年5月）、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表※24」の公表（同年6月）のほか、「医療機関向けセキュリティ教育支援ポータルサイト※25」を通じて研修やインシデント発生時の初動対応支援を行った。また、同月、総務省、厚生労働省及び経済産業省は、情報セキュリティインシデント予防等の観点から、医療機関及び医療情報システム・サービス事業者が医療情報システムの契約において、役割分担等の協議しておくべき事項を具体化するため「医療情報システムの契約における当事者間の役割分担等に関する確認表※26」を公表した。そのほか、2024年6月に改正された「地方自治法※27」により、地方公共団体は、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とされ、総務大臣は、当該方針の策定等について指針を示すこととされた（当該部分は2026年4月施行）。

- IPAの機能強化及びNICTの取り組み強化を通じたサイバーセキュリティ対策の底上げ

IPAが事務局を務めるAIセーフティ・インスティテュート（AISI：AI Safety Institute）は、2024年9月、AIシステムの開発者や提供者がAIセーフティ評価を実施する際に参照できる基本的な考え方を提示する「AIセーフティに関する評価観点ガイド※28」及びAIセーフティ評価手法の一つであるレッドチーミング手法を解説する「AIセーフティに関するレッドチーミング手法ガイド※29」を公開した（「2.1.3 (2) (b) AIセーフティ評価」参照）。また、経済産業省及びIPAは、2025年3月、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の運用を開始した※30（「3.3.1 セキュリティ要件適合評価及びラベリング制度（JC-STAR）」参照）。更に、IPAは、産業分野のセキュリティ・リスク情報集約のハブとしての機能強化等を行った※31（「3.1.3 (1) (c) 政府全体でのサイバーセキュリティ対応体制の強化」参照）。総務省・NICTと厚生労働省が連携し、医療システムを想定した演習教材を作成し、医療機関向けサイバーセキュリティ演習を試行実施した※32。そのほか、年次計画では、講師人材の育成にも取り組むとされている。

(b) サプライチェーン・リスクへの対応強化とDXを推進・支援する取り組みの強化

年次計画では、「サプライチェーン・リスクへの対応強化とDXを推進・支援する取組の強化」のため、セキュアバイデザイン・セキュアバイデフォルト原則を踏まえたIoT機器・ソフトウェア製品のサイバーセキュリティ対策促進、中小企業のサイバーセキュリティ対策促進等に取り組むこととされた。

- セキュアバイデザイン・セキュアバイデフォルト原則を踏まえたIoT機器・ソフトウェア製品のサイバーセキュリティ対策促進

経済産業省は、2024年8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 ver 2.0※33」を公表したほか、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の「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」において「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス」の策定に向けた検討が行われている※34（「3.1.3 (1) (b) セキュア・バイ・デザインの実践」参照）。また、前述のとおり、2025年3月、JC-STARの運用が開始されたところ、経済産業省は、IoT製品の輸出時の適合性評価に係る負担を軽減するため、シンガポール（Cybersecurity Labelling Scheme）、英国（PSTI法）、米国（U.S. Cyber Trust Mark）、欧州連合（EU：European Union）（Cyber Resilience Act）との相互承認に向け、海外当局との交渉を引き続き進めるとしている※30。

NICTは、2023年に改正された「国立研究開発法人情報通信研究機構法※35」に基づき、2024年度から、「NOTICE（National Operation Towards IoT Clean Environment）」において、ID・パスワードに脆弱性があるIoT機器の調査に加えて、脆弱性があるファームウェア等を搭載しているIoT機器、既にマルウェアに感染しているIoT機器を新たに対象とするサイバーセキュリティ対策助言等業務を新設する※36とともに、IoT機器メーカー等との連携を強化した※37（「3.1.4 (1) (a) IoTボットネットに対する端末側の対策（新NOTICE）」参照）。また、総務省は、2024年度、

「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」として、一般社団法人ICT-ISAC及び電気通信事業者とともに、平時におけるフロー情報分析によるC&Cサーバー※38の疑いがある機器の検知を行い、C&Cサーバーの検知情報等をICT-ISAC会員企業と共有する運用と対策の検討を行った※39（「3.1.4（1）（b）IoTボットネットに対するネットワーク側の対策（C&Cサーバーの検知・対処の推進）」参照）。

- 中小企業のサイバーセキュリティ対策促進
  IPAは、監視機能の強化や定期的なコンサルティングの実施等の拡充を要件としたサイバーセキュリティお助け隊サービスの新たな類型（2類）を創設し、2024年10月に2類の最初の登録を行った※40ほか、経済産業省は、政府広報の活用※41等により同サービスの認知度拡大を図った（「3.4.1（2）（b）サイバーセキュリティお助け隊サービス制度」参照）。IPAは、2024年度に実施した中小企業実態調査を踏まえ、中小企業において効果のある対策として、SECURITY ACTION二つ星の実施や第三者認証の取得・社内セキュリティ体制の整備等を示した※42（「3.4.1（2）（c）SECURITY ACTION」参照）。また、IPAは、地域のセキュリティ専門家である情報処理安全確保支援士（登録セキスペ）と中小企業のマッチングを促す場としてサイバーセキュリティ相談会を2024年度に計6回開催し、相談会を通じて、中小企業等のセキュリティ対策を支援できる登録セキスペをリスト化（中小企業向けサイバーセキュリティ対策支援者リスト）した※43（登録セキスペについては「3.2.2（2）情報処理安全確保支援士制度」参照）。

（c）欧米主要国を始めとする関係国との連携の一層の強化

年次計画では、「自由、公正かつ安全なサイバー空間」を確保するため、「海外のサイバーセキュリティ関係機関との協調・連携及びインド太平洋地域における能力構築支援の推進」「警察におけるサイバー空間の安全・安心の確保に資する取組の推進」等に取り組むこととされた。

- 海外のサイバーセキュリティ関係機関との協調・連携及びインド太平洋地域における能力構築支援の推進
  海外の関係機関との協調・連携の取り組みとして以下を実施した。
  - 2024年5月、NISC及び警察庁による人権保護や民主主義の推進に関与する組織や個人のためのサイバー脅威緩和に関する国際ガイダンスへの共同署名※44
  - 同年7月、NISC及び警察庁によるAPT40グループに関する国際アドバイザリーへの共同署名※45（「3.1.5（2）（b）（ア）国際アドバイザリーへの共同署名」参照）
  - 同年9月、米国で開催され、68ヵ国・機関が参加した「カウンターランサムウェア・イニシアティブ会合」へのNISC、警察庁及び外務省等による参加※46
  - 2025年1月、日米韓3ヵ国政府による北朝鮮による暗号資産窃取及び官民連携に関する共同声明の発出※47
  - 同月、NISCによる英国主導の「サイバーセキュリティ人材に関する国際的な連合」への参画※48

上記のほか、2024年度におけるサイバー分野の外交として、米国（6月）、英国（9月）、EU（11月）等の国・機関とのサイバー対話・協議※49や北朝鮮サイバー脅威に関する日米韓外交当局間作業部会※50等の実施により、関係国との連携を深化した（「4.1.1（3）（b）各国との連携強化」）。

2024年6月のG7プーリア・サミットでは、岸田文雄総理（当時）が、AIは人類の発展にとって大きな可能性を秘める一方、偽情報の拡散やサイバー攻撃を含むリスクも生じさせることを指摘した※51。また、G7サイバーセキュリティ作業部会が新たに設置され、2024年5月※52及び12月※53に会合が開催され、重要インフラ保護、サプライチェーンのセキュリティ確保、AIの安全な方法での活用等について議論された。

インド太平洋地域における途上国の能力構築支援の取り組みとして、NISC、総務省及び経済産業省による日ASEANサイバーセキュリティ政策会議（同年10月）※54、経済産業省及びIPA並びに米国及びEU政府による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（同年11月）※55等が実施された（「4.1.1（3）（b）各国との連携強化」参照）。

- 警察におけるサイバー空間の安全・安心の確保に資する取り組みの推進
  警察庁は、2024年度、ランサムウェア攻撃グループ「Phobos」に対する欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）や米国連邦捜査局（FBI：Federal Bureau of Investigation）との国際共同捜査や、国際刑事警察機構（ICPO：International Criminal

Police Organization、INTERPOLとも呼ばれる）が主導する西アフリカにおける組織的な金融犯罪に対するオペレーション「ジャッカル」における国際共同捜査に参画し、独自の分析結果等を関係国の捜査機関に提供することにより、被疑者の検挙に貢献した※56（「3.1.5(2)(b)(イ)その他国際連携による犯罪捜査等の取り組み」参照）。

(3)経済安全保障関連施策の状況

2024年度は、「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※57」（以下、経済安全保障推進法）が全面的に施行されるとともに、「重要経済安保情報の保護及び活用に関する法律※58」（以下、重要経済安保情報保護活用法）が成立し、公布され、同法の施行に向けた準備が進められた。本節では、両法に関する2024年度の主な動きを紹介する。

(a)経済安全保障推進法

経済安全保障推進法に基づき、①重要物資の安定的な供給の確保に関する制度、②基幹インフラ役務の安定的な提供の確保に関する制度、③先端的な重要技術の開発支援に関する制度、④特許出願の非公開に関する制度の四つの制度が創設された。

このうち、①に関しては、2025年5月時点で12の特定重要物資について124件の供給確保計画が認定されている※59。

③に関しては、「経済安全保障重要技術育成プログラム※60」（通称、K Program）において、サイバーセキュリティに関係が深い技術の研究開発構想が策定されている。2024年度は、個別研究型の「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※61」について4件※62、「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）※63」について4件※64、「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）※65」について5件※66、「偽情報分析に係る技術の開発※67」について1件※68の研究開発課題（テーマ）が新規採択された。またプロジェクト型の「先進的サイバー防御機能・分析能力強化※69」については、4件のテーマが採択された※70。

2024年5月には、②の制度の運用が開始されるとともに、④の制度が開始された。④の制度により、特許出願の明細書等に、公にすることにより外部から行われる行為によって国家及び国民の安全を損なう事態を生ずるおそれが大きい発明が記載されていた場合には、「保全指定」という手続きにより、出願公開や特許査定等の特許手続きが留保されるとともに、発明の内容の開示が原則禁止され、発明の実施も許可制となり、機微な技術の公開や情報流出が防止される。特許出願を非公開にするかどうか（保全指定をするか否か）の審査は、特許庁による第一次審査と内閣府による保全審査（第二次審査）の2段階に分けて行われる。このうち、第一次審査では、特許出願の中から、政令で定められた「特定技術分野※71」に属する発明が記載されている出願を選別して内閣総理大臣（内閣府）に出願書類を送付する。特定技術分野には、サイバーセキュリティと関係が深いものとして、耐タンパ性ハウジングにより計算機の部品等を保護する技術及び通信妨害等に関する技術が含まれている。両技術を含む特定技術分野の一部の技術に関して、2025年3月、内閣府が産業の発達への影響に関する調査結果を発表した※72。

(b)重要経済安保情報保護活用法

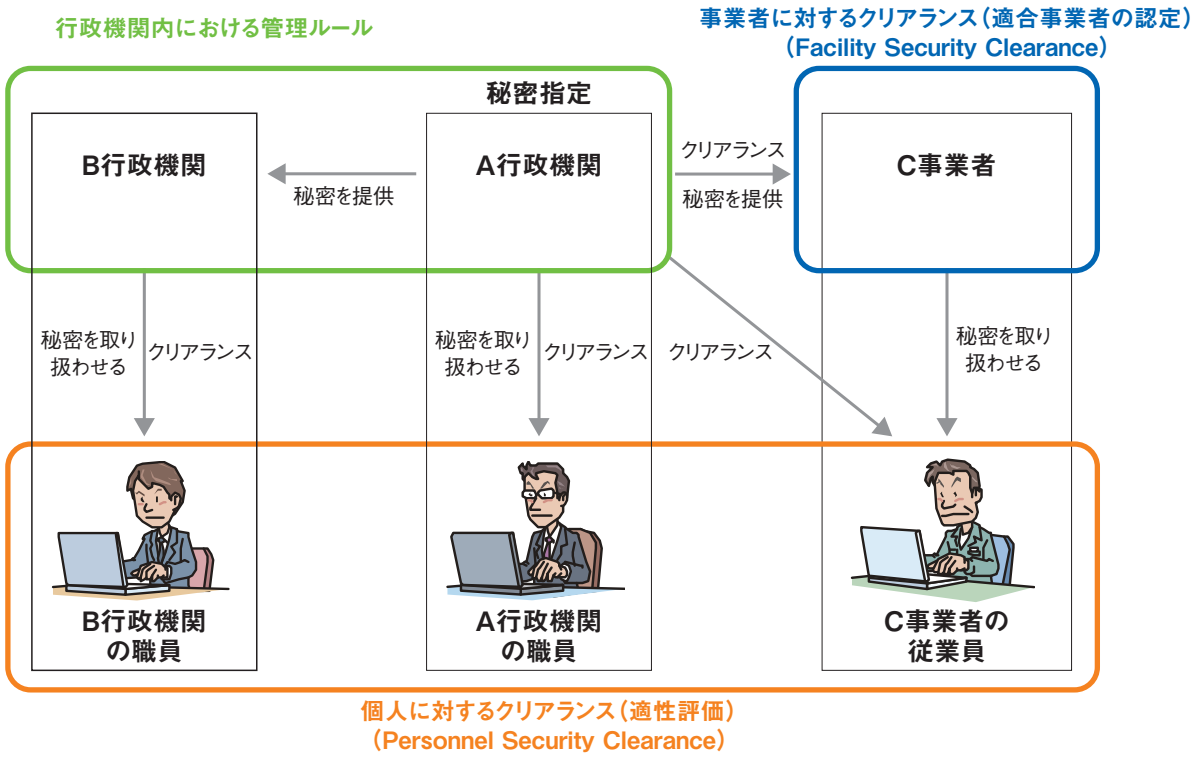
2024年1月に公表された「経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議」の「最終とりまとめ※73」により、経済安全保障分野におけるセキュリティ・クリアランス制度※74の創設が提言された。これを受けて、2024年5月に重要経済安保情報保護活用法が成立し※75、同月公布され、2025年5月に施行された。

図3-1-6（次ページ）は、同法に基づく重要経済安保情報の提供の流れの概略図である。

同法は、①重要経済安保情報の指定、②重要経済安保情報の提供、③重要経済安保情報の取扱者の制限、④適性評価、⑤罰則等を定めている。概要は、以下のとおりである※77。

①重要経済安保情報の指定

行政機関の長は、重要経済基盤（重要なインフラや物資のサプライチェーン）に関する一定の情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に支障を与えるおそれがあるため、特に秘匿する必要があるものを、「重要経済安保情報」として指定する。重要経済安保情報の具体例としては、サイバー脅威・対策等に関する情報や、サプライチェーン上の脆弱性関連情報が想定されている。指定の有効期間は5年以内で、原則30年まで延長可能である。行政機関の長は、重要経済安保情報の取り扱い業務を行わせる職員の範囲を定める等の



■図 3-1-6　重要経済安保情報の提供の流れとそれに対する管理ルールのイメージ
（出典）内閣府「適性評価と重要経済安保情報の提供の流れ※76」を基に IPA が編集

保護措置を講ずることとされている。

②重要経済安保情報の提供

行政機関の長は、必要に応じて他の行政機関等（外国の政府を含む）に重要経済安保情報を提供できる。我が国の安全保障に著しい支障を及ぼすおそれがないと認めるとき等は、国会や裁判所等にも提供できる。また、重要経済基盤の脆弱性の解消等我が国の安全保障の確保に資する活動を促すため、必要があると認めたときは、適合事業者（政令で定める基準に適合する事業者）との契約に基づき、重要経済安保情報を提供することも可能となっている。

③重要経済安保情報の取扱者の制限

重要経済安保情報の取り扱いの業務は、適性評価において重要経済安保情報を漏えいするおそれがないと認められた者に制限される。なお、特定秘密保護法による適性評価において特定秘密の取り扱いの業務を行った場合にこれを漏らすおそれがないと認められた者は、重要経済安保情報の取り扱いの業務を行うことができるとされている。

④適性評価

行政機関の長は、重要経済安保情報の取り扱いの業務を行うことが見込まれる行政機関の職員又は適合事業者の従業員について、本人の同意を得た上で、内閣総理大臣による調査の結果に基づき漏えいのおそれがないことについての評価（適性評価）を行う。適性評価の有効期間は 10 年である。調査内容は、重要経済基盤毀損活動との関係に関する事項、犯罪及び懲戒の経歴に関する事項、情報の取り扱いに係る非違の経歴に関する事項、薬物の濫用及び影響に関する事項、精神疾患に関する事項、飲酒についての節度に関する事項、及び信用状態その他の経済的な状況に関する事項の七つとされている。

なお、評価対象者が他の行政機関の長が直近に実施した適性評価（10 年を経過していないものに限る）において漏えいのおそれがないと認められた者である場合には、改めて調査することなく適性評価を実施可能とされている。

⑤罰則

重要経済安保情報の漏えい時に、5 年以下の拘禁刑若しくは 500 万円以下の罰金またはこれを併科する罰則等が規定されている。

2025 年 1 月、同法第 18 条第 1 項に基づき、「重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定に関し、統一的な運用を図るための基準※78」（運用基準）が閣議決定された。運用

基準は、重要経済安保情報の指定及び解除等、適性評価の実施、適合事業者の認定等について、具体的な判断基準や手順を規定している。また、同法の運用にあたって留意すべき事項として、拡張解釈の禁止並びに基本的人権及び報道・取材の自由の尊重、公文書管理法及び情報公開法の適正な運用が規定された。また、適性評価の実施にあたっての基本的考え方として、基本的な人権の尊重、プライバシーの保護、法定の七つの調査事項以外の調査の禁止、適性評価の結果の目的外利用の禁止が規定された。

3.1.2 デジタル庁の政策

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の策定・改訂や、政府情報システムに係るセキュリティガバナンスの構築・維持に資する情報システムの整備を行っている。

(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策定・改訂

デジタル庁では、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及び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、10 本のドキュメント（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※79。

2024 年には、猛威を振るうサプライチェーン・リスクへの対応や既存ドキュメント利用者のより一層の理解を促進し、政府情報システムのセキュリティ強化に資することを目的として、以下のドキュメントの策定・改訂を行った。

(a)「政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集」の策定

情報システムの構築・運用・保守では、外部事業者（サードパーティー、クラウドサービス、業務委託等）を活用することが多いが、これらはすべてサプライチェーンの一部である。昨今、クラウドサービスの利用等によりサプライチェーンが一層拡大していることもあり、サプライチェーンに起因するセキュリティインシデントも多発している。

「政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理 及び その対策のグッドプラクティス集※80」では、サプライチェーン・リスクを含めた網羅的なセキュリティ対策はこれまでどおり「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※81」（以下、政府統一基準群）をベースラインとしつつ、サプライチェーン・リスクに起因する大規模な攻撃や事故等に備えて、自組織やシステムだけでなく、サプライチェーン全体を考慮したリスクを管理し、対策するための課題整理とその対策のグッドプラクティスを示した。

同グッドプラクティス集では、政府情報システムに想定される主要なサプライチェーン・リスクを、以下のとおり定義している。

- ビジネスサプライチェーン・リスク
  政府情報システムの開発・運用・保守等の業務を請け負う委託先や再委託先（それ以降も同様）に関連する、内部不正による情報漏えいやマルウェア感染等のサイバー攻撃を受けることによる業務停止等のセキュリティリスク
- サービスサプライチェーン・リスク
  政府情報システム等で利用する事業者によって提供されるクラウドサービスに関連する情報漏えい、業務停止等のセキュリティリスク
- 機器・ソフトウェアサプライチェーン・リスク
  政府情報システムで利用するハードウェアやソフトウェアに含まれるバックドアや致命的な脆弱性が悪用され、システムへの不正アクセスやマルウェア感染等のサイバー攻撃を受けることによる、情報漏えい、業務停止等のセキュリティリスク

これらの異なる領域にまたがるサプライチェーン・リスクや、様々なセキュリティリスクを含めた政府情報システムに係るリスク全体に関する総合的なリスクアセスメントを確実に実施することが重要であること、特に、業務委託先やクラウドプロバイダー等の外部の関係者が関与する場合、その相手先でのセキュリティ対策等を適切に把握することが求められることから、委託先、サプライヤー、サービス提供者等との緊密な協力が不可欠であることを、同グッドプラクティス集のグッドプラクティスは示している。

また、サプライチェーン・リスクは動的なものであり、技術の進化や新たな脅威の発生によりリスクの性質や影響範囲が変化することがあることから、初回のリスク評価や対策実施にとどまらず、継続的な監視と再評価を行うことの重要性を示している。

更に、同グッドプラクティス集は、サプライチェーン・リ

スクが顕在化した場合の対応を適切に行うために、あらかじめインシデント対応計画を整備することとし、その対応計画の中でインシデントの検知、報告、対応、復旧の手順を明確に定め、委託先等の関係者との協力体制を整備しておく必要性を説明している。これらの取り組みにより、より堅牢なサプライチェーン・リスク管理体制を構築し、政府情報システムにおけるセキュリティ水準の向上に努めることが期待される。

(b)「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」の改訂

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。「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[※82]」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。

今回、同技術レポートに「別添 . CI/CD パイプラインによる Infrastructure as Code 実装例[※83]」を追加した。同実装例では、AWS（Amazon Web Services）上で稼働する政府情報システムが、その AWS リソースを Infrastructure as Code ツール「Terraform」によって構成管理され、そして CI/CD パイプラインツール「GitHub Actions」を用いて自動適用されている状況を想定した実装例を紹介している。

同実装例では、CI/CD パイプラインのサーバーやネットワーク等のインフラ構成管理と自動化ツールの提供を担当するプラットフォームチームと、アプリケーションのコード開発とテスト、デプロイメントを担当するサービスチームのそれぞれの観点から、具体的なシナリオを基に各要素の実例を示している。

図 3-1-7 にプラットフォームチームの CI/CD パイプライン概要図を示す。

プラットフォームチームの CI/CD パイプラインでは、プラットフォームチームが一元的に管理する Terraform バイナリー及び AWS プロバイダーを、サービスチームに提供できる状態を想定している。これは、複数チームで共通利用されるソフトウェアに対する個別のセキュリティチェックをプラットフォームチームが担うことで、ルールへの準拠がより実行的になる効果を期待している。

図 3-1-8（次ページ）にサービスチームの CI/CD パイプライン概要図を示す。

サービスチームは、AWS リソースの構成を Terraform ファイルに定義し管理する。これを自動化するのがサービスチームの CI/CD パイプラインである。これは、プラットフォームチームの CI/CD パイプラインの成果物であるコンテナイメージと AWS の各種シークレット情報を用いて、Terraform ファイルの内容を AWS に反映している。

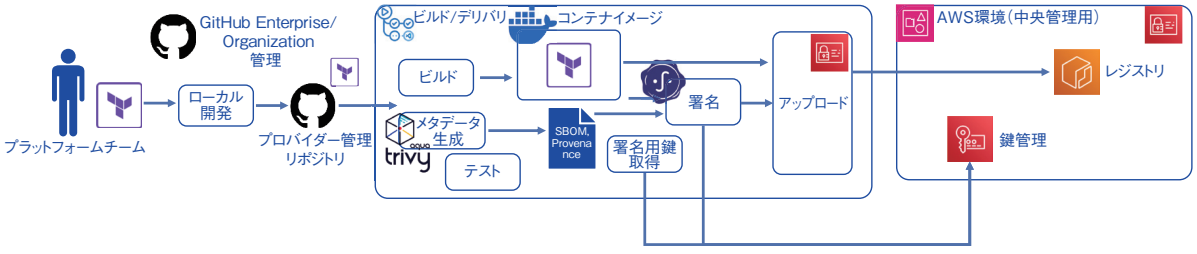
同実装例はあくまで保護策の全体的な実装例であり、実運用環境では、全体的なリスクやパフォーマンス等の機能・非機能要件を基に、保護策の要否、粒度、強度を決定し、ツールを選定することを求めている。

(2) 総合運用・監視システム（COSMOS）の整備

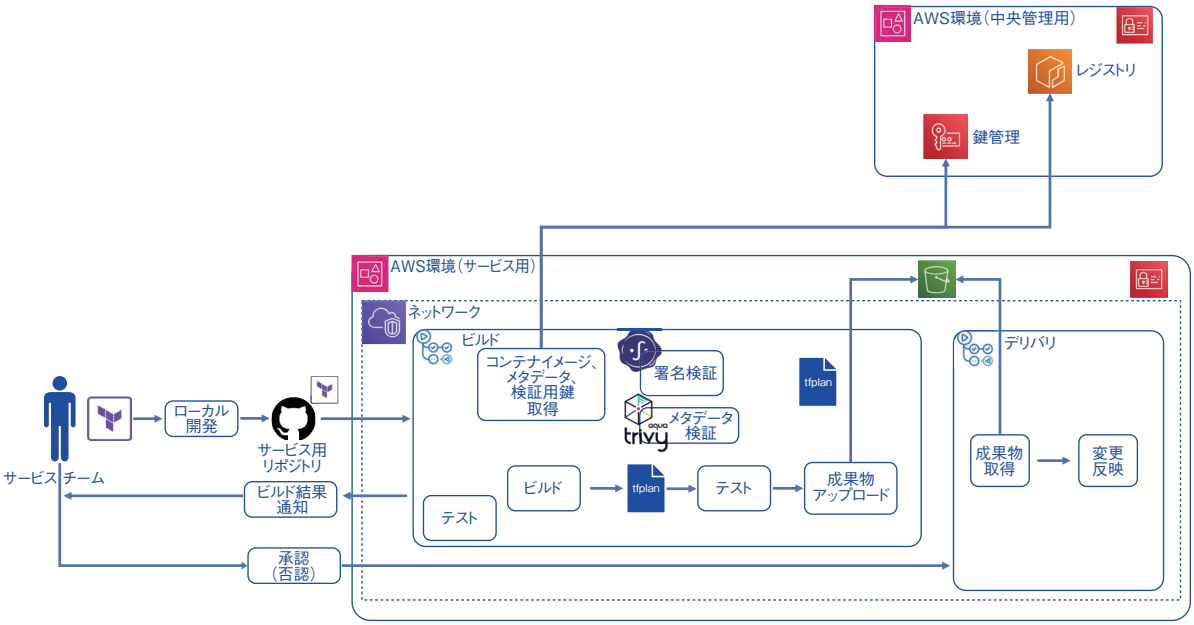
デジタル庁における総合運用監視は、デジタル庁の整備する政府情報システム全体のサービス提供状況の把握を行いつつ、内部監査人協会（IIA：The Institute of Internal Auditors）の 3 ラインモデル[※84] における第 2 ライン及び第 3 ラインの役割から各システムの IT マネジメントを支援する仕組みである。デジタル庁におけるシステム全体のサービス稼働状況を横断して一元的に把握する総合運用・監視システム（COSMOS）を構築・運用することで、デジタル庁の IT ガバナンスの実現を目指す（次ページ図 3-1-9）。

総合運用・監視システムは、デジタル庁が管理する政府情報システムを対象として各システムへの外形監視を行う。総合運用監視の目的・役割について紹介する。

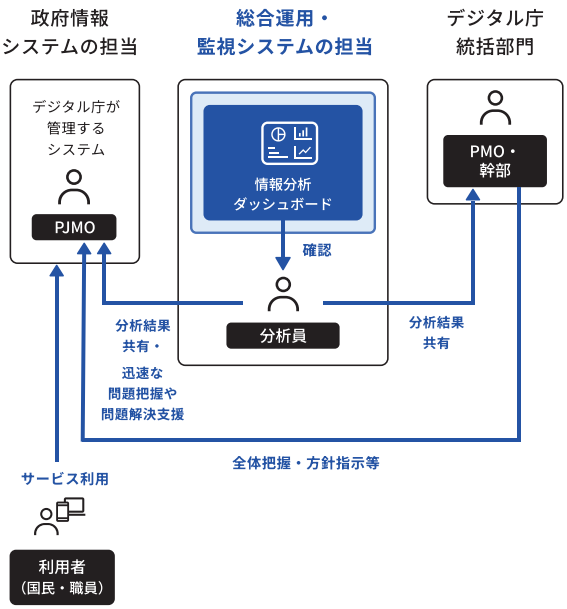
- 総合運用監視によるデジタル庁の IT ガバナンス向上



■図 3-1-7　プラットフォームチームの CI/CD パイプライン概観
（出典）デジタル庁「別添 . CI/CD パイプラインによる Infrastructure as Code 実装例」



■図 3-1-8　サービスチームの CI/CD パイプライン概観
（出典）デジタル庁「別添 . CI/CD パイプラインによる Infrastructure as Code 実装例」



■図 3-1-9　総合運用・監視システム概要図
（出典）デジタル庁「IT ガバナンスを確保するための総合運用監視※85」

政府情報システムの提供サービスが（インターネットや外部サービスを含む）複数のシステムで構成される等、各システムの運用者では提供サービスへの影響が把握しづらい場合に支援できるように、総合的な手法でデジタル庁の異なるシステムの運用状況を全体的・継続的に監視する。

- 利用者視点及び客観的なサービス提供状況の把握
  各システムの運用者は、利用者に対するサービス提供やリスク管理等を担う第 1 ラインとしてのシステム稼働の状況把握をしている。総合運用監視では、システム稼働に加え、利用者視点でのサービス提供の状況を把握する。そのため、総合運用監視は、第 1 ラインを支援する第 2 ライン／第 3 ラインとして各システムの運用者から独立的・客観的にサービス提供の状況を把握する。
- インシデント発生時のデジタル庁全体の対応支援
  インシデント発生時に影響の範囲やシステムの関連性を特定することを支援する。これにより、インシデントが発生した各システムの運用者と連携し、デジタル庁全体としてインシデント対応を迅速かつ効果的に行う。
- 各システムの運用品質のレベルの向上
  独立的・客観的にサービス提供状況を把握し、各システムの運用者に定期的にフィードバックする。サービス提供状況のフィードバックにより、各システムの運用者による運用品質レベルの向上を図る。

(3) 常時リスク診断・対処（CRSA）システムの整備

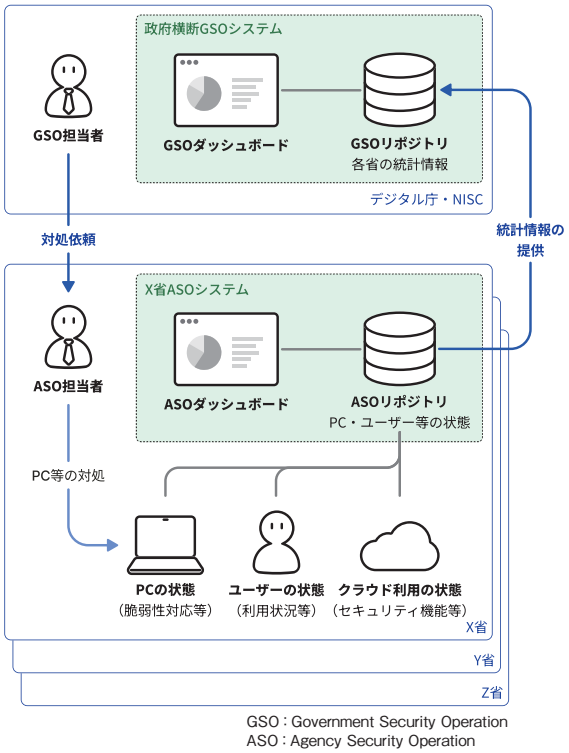
CRSA（Continuous Risk Scoring & Action：常時リスク診断・対処）とは、組織のセキュリティポリシー等に準拠するために情報システムに導入された必要なコントロール（管理策）に関して、以下を実施するものである。

- リスク診断：必要なコントロールと実際の状態とのギャップやリスクを可視化
- 対処：可視化されたギャップやリスクの是正対応

- 常時：ギャップやリスクの可視化と是正対応を継続的に実施

デジタル庁は、2024 年度に CRSA の概念に基づき、組織のネットワークとシステムのサイバーセキュリティを強化するための仕組みを提供する CRSA システムを整備した。

これにより、組織の資産に関する情報を収集し、資産の構成及びソフトウェアコンポーネントに更新を適用するといった潜在的リスクの是正活動を支援し、情報システムの運用等においてセキュリティポリシー等からの逸脱を発見し、適時適切に対処することを可能とする（図 3-1-10）。



■図 3-1-10　CRSA システム概要図
（出典）デジタル庁「常時リスク診断・対処（CRSA）※86」

CRSA システム導入の目的と効果は以下のとおりである。

- 政府統一基準群等に準拠したコントロール（管理策）からの逸脱の迅速な把握と是正対応
  サイバーセキュリティ対策に必要なコントロールの実施状況を継続的にモニタリングし、どこが不適切な状態になっているかを迅速に把握し、是正対応を実施する。
- インシデント発生時のトリアージ等の効果的な対応
  リアルタイムに自組織の資産状況、脆弱性対応状況等を把握し、インシデント発生時の資産等への影響規模や対応の優先度について迅速に判断する。
- リアルタイムデータによるセキュリティ対策実施状況の効率的な報告
  CRSA システムを導入した組織は、リアルタイムな資産状態、アカウントの利用状況、インシデントの発生状況等を把握できる。これにより、サイバーセキュリティ対策状況を客観的かつ効率的に報告可能とする。政府全体としては、各組織のサイバーセキュリティ対策状況を各組織に負担をかけることなく効率的に把握可能とする。
- 脅威やインシデントに対する政府横断的な脆弱箇所の迅速な発見と是正対応
  特定の脅威情報やインシデントに関する情報を基に、影響のある箇所やインシデントの発生する可能性のある箇所を政府横断的に特定し、迅速かつ効果的に対処可能とする。
- ゼロトラストアーキテクチャの運用環境を適切に維持
  ゼロトラストアーキテクチャの具体的な実装・運用において、CRSA システムの診断結果をポリシーエンジンのインプット情報として活用する。

3.1.3 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。同研究会は以下の三つのワーキンググループ（以下、WG）及び「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」によって構成される。また各 WG の配下には、サブワーキンググループ（以下、SWG）または検討会が設置されている※87。

- WG1（実効性強化・国際連携）
  - 分野横断 SWG
  - 電力 SWG
  - 工場 SWG
  - 半導体産業 SWG
  - ビル SWG

- 宇宙産業 SWG
- サプライチェーン強化に向けたセキュリティ対策評価制度に関する SWG

- WG2（地域・中小企業支援）
  - サイバーセキュリティ人材の育成促進に向けた検討会
- WG3（産業振興・人材育成）
  - 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
  - 産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環（仮題）に向けての検討会
- 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

同研究会では2024年4月5日に第8回会合を開催し、今後の産業サイバーセキュリティ政策について議論を行った。2025年5月23日には第9回会合を開催し、施策の進捗状況が確認された※88。以下では、2024年度に同研究会で重点的に取り組んできた活動について述べる。

(a) サプライチェーン全体での対策強化

経済産業省は、半導体関連産業のサイバーセキュリティ対策のため、2024年11月にWG1に「半導体産業SWG」を設置し、我が国の半導体産業におけるサイバーセキュリティの在り方や守るべき対象技術等を議論するとともに、サイバーセキュリティ対策への取り組み、問題意識や事例等、相互に情報共有を行っている※89。

同SWGでは、国内の半導体産業におけるセキュリティ対策状況等を踏まえた工場セキュリティ対策の指針を示すため、「半導体デバイス工場における OT セキュリティガイドライン」の策定に向け議論している。同ガイドラインは、最も高度な攻撃者（国家の支援を受けたグループ）を想定した対策レベルを実現するために、「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）※90」や「The NIST Cybersecurity Framework（CSF）2.0※91」等リスクベースのサイバーセキュリティフレームワークを活用したリスク分析、及び具体的な対策を検討する際等に活用されることが想定される。

また経済産業省は、サプライチェーンに起因するインシデントへの対策を強化するため、2024年7月、WG1に「サプライチェーン強化に向けたセキュリティ対策評価制度に関するSWG※92」を設置し、対策状況を可視化し企業の対策決定を容易・適切なものにする仕組みである「サプライチェーン強化に向けたセキュリティ対策評価制度」の制定を目指し議論を行っている。同SWGは2025年4月14日に「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ※93」を公表し、現状の構想を取りまとめた。同制度は2025年度の実証事業を踏まえた上で、2026年度の運用開始を目指す。

そのほか、WG1の「電力SWG」は、2025年2月4日に第18回会合※94を開催し、サプライチェーン・リスクへの対応、分散型電源のサイバーセキュリティ、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の活用について議論し、サプライチェーン・リスクへの対策に関する手引き文書の策定を目指している。

WG1の「工場SWG」は、2025年3月4日に第8回会合※95を開催し、2022年11月16日に第1.0版が公表された「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※96」の改訂及び、より利用しやすいAppendixの作成を目指し議論を行った（新規Appendixは2025年4月11日に公表）。

(b) セキュア・バイ・デザインの実践

経済産業省は、IoT製品やソフトウェアでのセキュア・バイ・デザインの実践を推進する観点から、以下の検討・取り組みを行っている。

WG3の「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会」では、IoT製品を対象として、一定水準のセキュリティ要件に対するセキュリティ対策の適合性を評価し、その結果を調達者・利用者が分かる形で可視化する制度を策定するため議論を行ってきた。それを踏まえ、2024年8月に経済産業省は「IoT製品に対するセキュリティ適合性評価制度構築方針※97」を公表した。この方針を基にして、IPAは経済産業省の協力のもと、2025年3月より「セキュリティ要件適合評価及びラベリング制度（JC-STAR: Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements）」の運用を開始した（「3.3.1 セキュリティ要件適合評価及びラベリング制度（JC-STAR）」参照）。

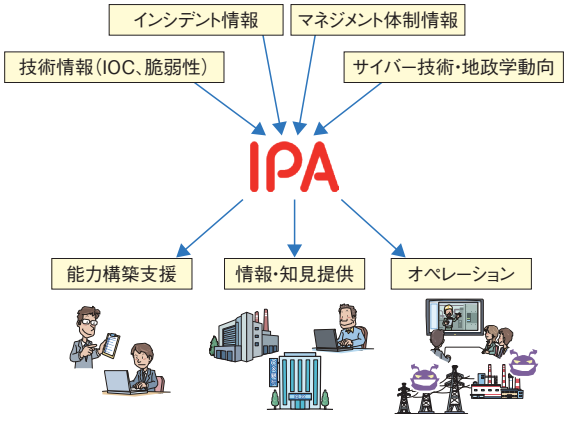
WG1の「分野横断SWG」で活動している「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」（以下、ソフトウェアTF）では、オープンソースソフトウェア（OSS：Open Source Software）等のソフトウェアの活用・脆弱性管理手法を検討している。ソフトウェアTFは、2024年8月29日に「ソフトウェア管理に向けたSBOM（Software Bill of

Materials）の導入に関する手引 ver 2.0」を公開した※98。改訂版となる同手引は、ソフトウェアを供給する企業と調達する企業の双方を想定読者とし、中小企業も含め、あらゆる企業にとって SBOM をより効率的に活用できる方法等として、脆弱性管理プロセスの具体化、SBOM 対応モデル、SBOM 取引モデル等を新たな内容として盛り込んでいる。2025 年 3 月 4 日には第 15 回会合※99を開催し、経済産業省はそこでの議論を基に、ソフトウェアのセキュア開発のための標準である「セキュア・ソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）※100」を組織・プロジェクトの現場に導入するための具体的な方法や手順を示す「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）※101」を提示した。また WG1 は、政府機関等及び重要インフラ事業者を始め広く社会で活用される情報・通信システム、ソフトウェア製品及び ICT サービスを開発し提供する「サイバーインフラ事業者」を対象としたセキュリティガイドラインとして、「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）※102」を提示した。

（c）政府全体でのサイバーセキュリティ対応体制の強化

経済産業省は、「サイバー状況把握力」の強化により国家安全保障戦略に基づく対応を強化すべく、以下の取り組みを行っている。

- IPA が有する産業界とのネットワーク、セキュリティ対策制度を駆使した産業分野のセキュリティ・リスク情報（サイバーインテリジェンス）集約のハブとしての機能強化（図 3-1-11）
- 経済活動に影響を及ぼすサイバーリスクを統合的に分析することによる、産業分野に関する脅威評価のハブとしての機能を追加
- J-CRAT を活用した、防御や抑止対応に資する情報共有／対応支援活動のハブとしての活動推進（「3.1.3（3）（b）J-CRAT（サイバーレスキュー隊）」参照）
- サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携（「3.1.3（4）（c）サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携」参照）



■図 3-1-11　IPA におけるサイバー情報集約・情勢分析能力の強化
（出典）経済産業省「第9回 産業サイバーセキュリティ研究会 事務局説明資料※31」を基に IPA が編集

今後、経済インテリジェンス収集力の強化等によりサイバー情報の集約・情勢分析機能や対処支援能力の一層の強化を図るとともに、第 217 回通常国会で成立したサイバー対処能力強化法に基づく業務への対応により、政府全体のサイバー安全保障体制の強化に貢献していく。

（d）サイバーセキュリティ供給能力の強化

経済産業省は、国内のセキュリティ企業の強化のため、2024 年 7 月、WG3 に「産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環（仮題）に向けての検討会※103」を設置し、サイバーセキュリティビジネスの振興のための方策について議論を行っている。

国産のサイバーセキュリティ製品・サービスが創出される環境を作るための包括的な政策パッケージとして、同検討会での議論を踏まえ、経済産業省は 2025 年 3 月 5 日に「サイバーセキュリティ産業振興戦略※104」を発表した。サイバーセキュリティ産業のマーケットには、国内で活用されるセキュリティ製品の多くを海外製が占めている現状や、導入実績が重視される商慣習、十分に開発投資が行われにくい事業環境といった課題が存在している。「サイバーセキュリティ産業振興戦略」では、政府機関等がスタートアップの製品・サービスを試行的に活用することで製品開発の出口を確保し、技術力・競争力強化の支援やベンダー・SIer 間の共同のための枠組みの構築を行うことにより、国内マーケットを拡大し、安全保障の確保やデジタル赤字の解消を目指す。経済産業省では、今後、予算編成等を踏まえ取り組みの具体化を図る。

また経済産業省は、産業界のサイバーセキュリティ対策の強化のため、2024 年 7 月、WG2 に「サイバーセキュリティ人材の育成促進に向けた検討会※105」を設置し、セキュリティ人材のすそ野を拡大するための施策について議論を行っている。

同検討会ではサイバーセキュリティ人材不足への対応として、特に以下の 3 点について重点的に検討をしてい

る（「3.2.1 サイバーセキュリティ人材の現状と育成状況」参照）。

- セキュリティ・キャンプの拡充
- 情報処理安全確保支援士（登録セキスペ）の活用及び制度の見直し
- 中堅・中小企業等の内部でセキュリティ対策を推進する者の確保に向けた新たな施策

(2) 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※106。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。2024 年 8 月 16 日に「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準※107」が改正され、認証の基準が更新された。この改正により、企業が取り組むべき内容を更新・明確化した。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。

(3) 情報共有・初動対応支援・脆弱性対策の取り組み

IPA では、重大なサイバー攻撃に関する情報共有を行う情報ハブ（集約点）の役割を担う「J-CSIP（サイバー情報共有イニシアティブ）」、重要インフラ事業者等を対象に標的型サイバー攻撃等の初動対応支援を行う「J-CRAT（サイバーレスキュー隊）」、そして脆弱性情報を官民で連携し、適切に流通・対処する仕組みである「情報セキュリティ早期警戒パートナーシップ」を運営している。

(a) 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被害の低減を目指している。参加形態としては、IPA と参加組織との間で情報共有を行う業界単位のグループ（SIG※108）と、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（次ページ図 3-1-12）。

2025 年 3 月には、新たに半導体業界 SIG、同年 4 月には、暗号資産交換業界情報連携体制が発足し、2025 年 7 月 1 日現在、IPA を情報の中継・集約点（情報ハブ）として 17 の業界から 320 の企業や業界団体（以下、参加組織）が J-CSIP に参加している。

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 で共有される情報は、提供元が明らかにならないよう、情報提供者固有の情報を除去するルールがある。

2024 年度の J-CSIP における IPA の活動としては、参加組織から提供された IoC（Indicator of Compromise：侵害指標）等の情報共有に加え、標的型攻撃に関する脅威情報や、サイバー情勢に関する注意喚起等の情報発信を行った。

これらの情報共有の中には、VPN ゲートウェイのようなネットワーク境界にある機器から侵入する「ネットワーク貫通型攻撃」や、以前から観測されている、特定の業界や組織を標的としたメールによる攻撃も含まれている。

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。

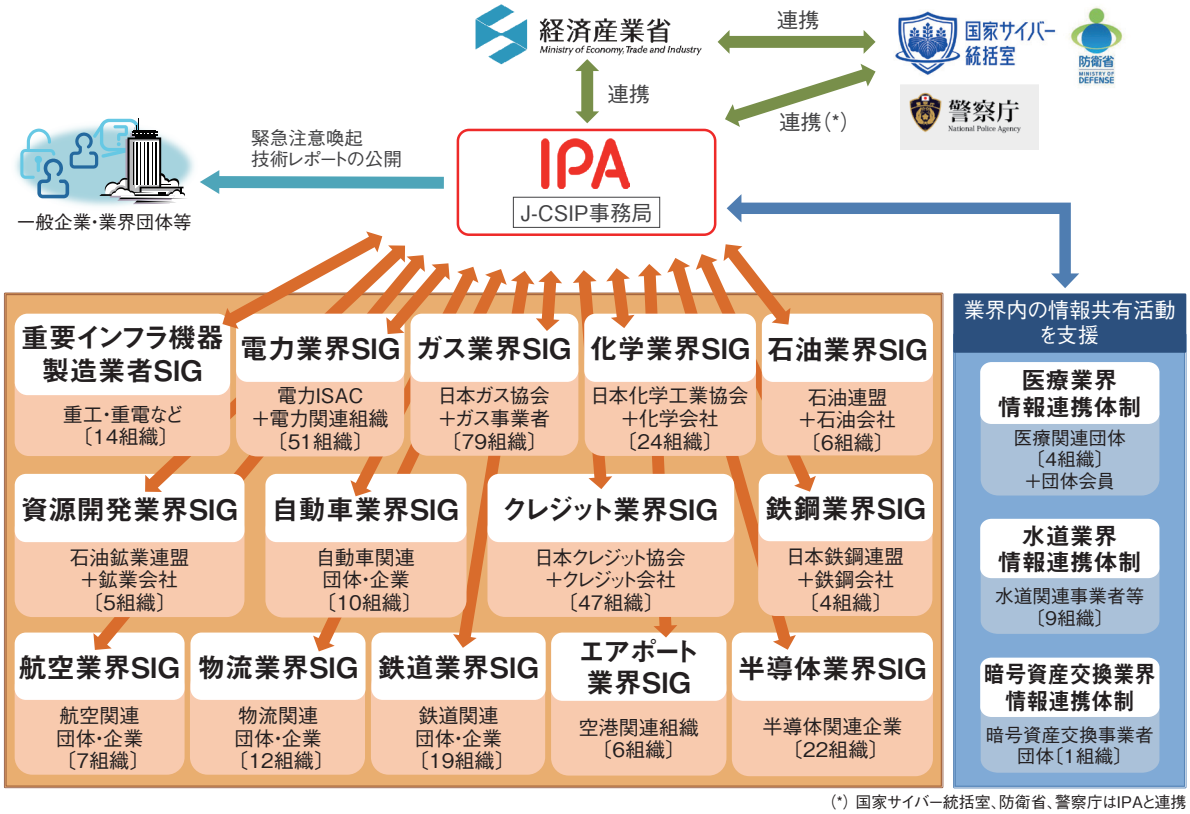
(b) J-CRAT（サイバーレスキュー隊）

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）※110」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※111」（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。「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、各種マルウェア情報等を収集している。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



(*) 国家サイバー統括室、防衛省、警察庁はIPAと連携

■図 3-1-12　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(ジェイシップ)について[※109]」を基に編集

なっているため、それらの情報収集を幅広く行っている。

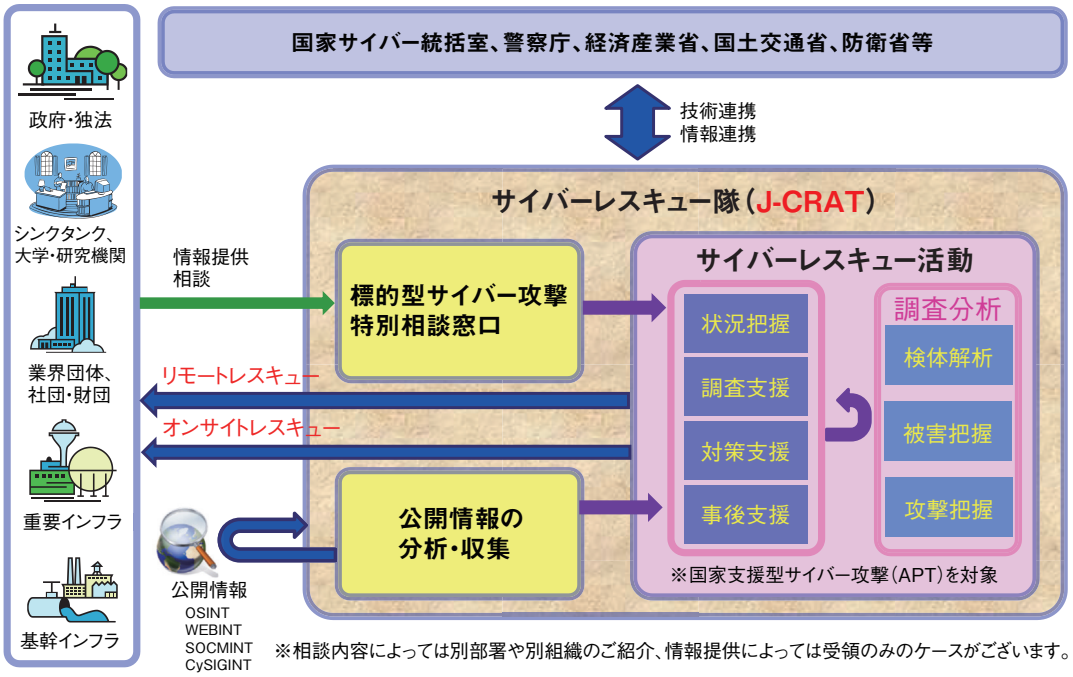
標的型攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等サプライチェーンを構成する組織に対しては、被害実態の確認と認知の支援、被害緩和の暫定対応に関する助言を「サイバーレスキュー活動」として実施している。また、窓口における対応の結果、必要があると判断した組織に対して、攻撃の期間・内容、感染範囲、想定被害等をヒアリングし、早急な対策着手が行えるよう、「リモートレスキュー」や「オンサイトレスキュー」等によって、民間セキュリティ事業者への移行を前提とした助言を行っている（次ページ図3-1-13)。

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、注意喚起情報等を随時公開している。こうした取り組み等を通じ、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、及び攻撃の連鎖を遮断することによる被害の低減を推進している。

(c) 情報セキュリティ早期警戒パートナーシップ

「情報セキュリティ早期警戒パートナーシップ」（以下、パートナーシップ）は、ソフトウェア製品及び Web サイトに関する脆弱性関連情報の円滑な流通、対策の普及を図るため、公的ルールに基づく官民連携体制として、2004 年 7 月に整備された脆弱性関連情報の届出受付制度である。後述する経済産業省の告示のもと、IPA が受付機関、JPCERT/CC が調整機関の役割を担い、運営している。

不正アクセス、マルウェア等による被害発生を抑制するため、脆弱性関連情報が発見された場合に、それらをどのように取り扱うべきかを示した経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」が 2004 年に制定されたことを踏まえ、脆弱性関連情報の適切な流通を実現するため、関係者に推奨する行為を取りまとめたものとして「情報セキュリティ早期警戒パートナーシップガイドライン」の第 1 版が 2004 年 7 月に制定された。同告示は、2017 年に経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程[※112]」となり、2024 年 6 月に改正された。この改正と「情報システム等の脆弱性情報の取扱いに関する研究会」での検討結果を踏まえ、同ガイドラインについても改訂を行い、2024 年 6



■図 3-1-13　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※110」

月に第 13 版が発行されている※113。

同ガイドラインの適用範囲は、脆弱性により不特定または多数の人々に影響を及ぼすもの、具体的には、国内で利用されているソフトウェア製品や、主に日本国内からのアクセスが想定されるサイトで稼働する Web アプリケーション（例えば、主に日本語で記述された Web サイトや、URL のトップレベルドメインが「jp」の Web サイト等）が対象である。

同ガイドラインが対象とする主な関係者と、それぞれがパートナーシップに対応するメリットを表 3-1-1 に示す。

関係者	メリット
発見者	・公的機関を介して製品開発者や Web サイト運営者に脆弱性対応を促すことができる。 ・製品脆弱性の発見者は、脆弱性対策情報の公表時に名前を掲載できる。
製品開発者	・自社製品に影響する未公表の脆弱性を知ることができる。 ・脆弱性の対策方法を利用者に広く周知できる。 ・脆弱性問題に真摯に取り組む姿勢を示すことができる。
Web サイト運営者	・脆弱性の存在が広く知れ渡る前に、修正できる。 ・自分では気付かなかった脆弱性を確認し修正できる。 ・自分の Web サイトの利用者の安全性向上につながる。

■表 3-1-1　主な関係者とパートナーシップに対応するメリット
（出典）IPA「情報セキュリティ早期警戒パートナーシップの紹介※114」を基に編集

関係者がパートナーシップに対応することにより、製品を使用するユーザー（システム構築事業者含む）は、製品に関する脆弱性情報を把握し、対策を行い、その製品に対する攻撃のリスクを低減できるようになる。また、システムの企画や開発・設計等で使用する製品の選定に際して、公表情報を参考として活用できるようになる。

パートナーシップの活動の全体像を図 3-1-14（次ページ）に示す。

2024 年にパートナーシップへ届出された脆弱性の届出状況については、「1.2.4（1）（b）早期警戒パートナーシップにおける脆弱性の届出状況」を参照されたい。

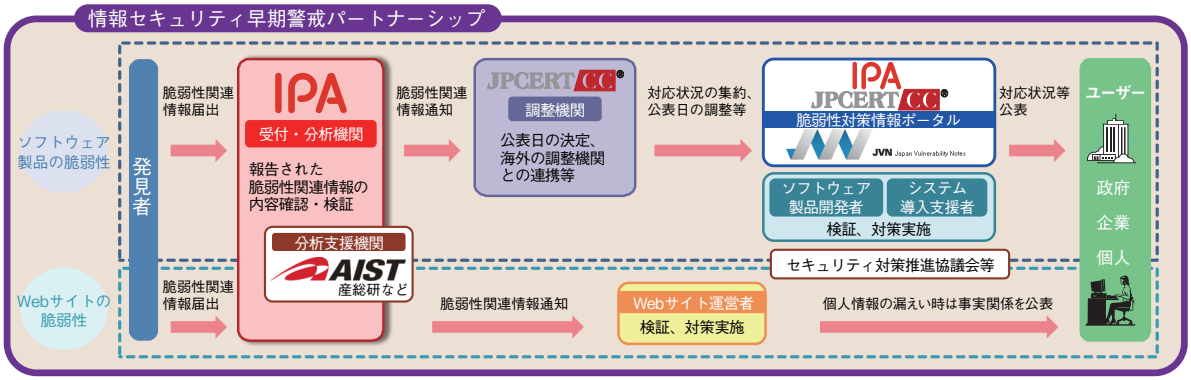
今後も、脆弱性関連情報が関係者の協力のもと、適切に流通、対応、公表されることで、製品利用者や Web サイト運営者が脆弱性を攻撃される可能性を低減することが期待される。

（4）その他の検討会等における活動

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※115」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※116」を設置した。2024 年 10 月より、経済産業省と IPA AI セーフティ・インスティテュートが同検



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

■図 3-1-14　パートナーシップの全体像
（出典）IPA「情報セキュリティ早期警戒パートナーシップの紹介」を基に編集

討会の共同事務局となり運営している。

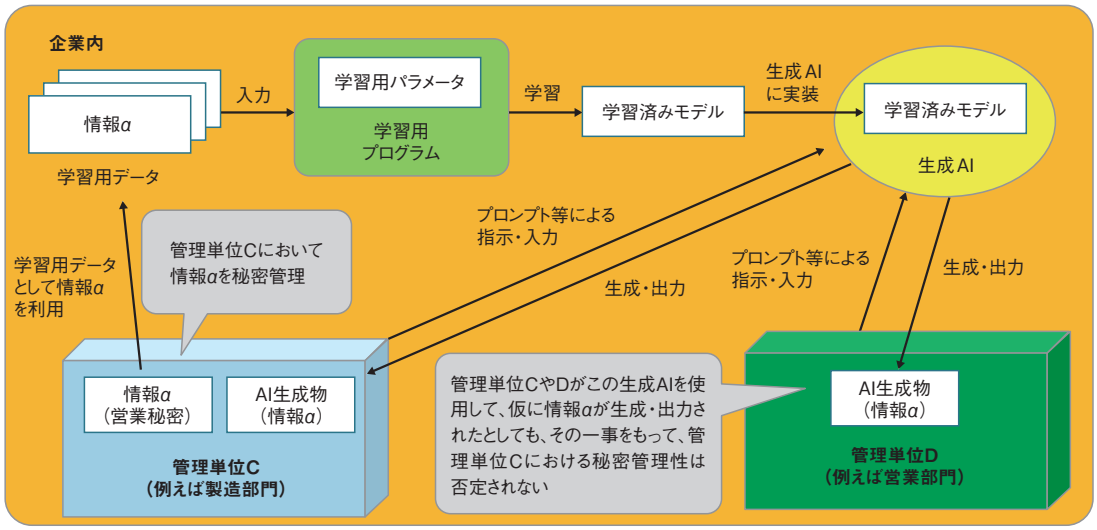
同検討会は、2024 年 4 月に公開された「AI 事業者ガイドライン（第 1.0 版）※117」について、AI をめぐる動向が国際的な議論の進展等目まぐるしく変化する中、AI の安全安心な活用が促進されるよう、改訂を行った。改訂版は、2025 年 3 月に「AI 事業者ガイドライン（第 1.1 版）※118」として総務省と経済産業省から発行された。

(b) 不正競争防止小委員会

経済産業省は、不正競争防止法に関する事項を審議する場として、2017 年 7 月に「産業構造審議会 知的財産分科会 不正競争防止小委員会」を設置し、定期的に議論を行っている※119。

同小委員会は 2025 年 3 月 25 日に第 28 回を開催し、2025 年 3 月 31 日に「営業秘密管理指針※120」を改訂した。営業秘密管理指針は、不正競争防止法により営業秘密として法的保護を受けるために必要となる「最低限の水準の対策」を示すものとして策定された。同指針は、前回改訂である 2019 年 1 月以降の営業秘密を取り巻く環境の変化、及び関連する法制度の見直し、裁判の動向を踏まえて、改訂が行われた。これらの改訂により、クラウド・AI の活用等における営業秘密の要件の解釈が明確化された。以下、営業秘密の 3 要件（秘密管理性、有用性、非公知性）における主な改訂内容を示す。

- 秘密管理性について
  企業における管理実態を踏まえ、秘密管理性及び秘密管理措置について具体化を行った。例えば、営業秘密と他の情報との分別管理を含めた考え方について、「秘密管理措置の程度」の考慮要素の一つに位置付けるとともに、秘密管理措置においては情報セキュリティで求められる措置の程度に達していなくとも、秘密管理措置が認められ得る旨の記載を追記した。また、外部クラウドや生成 AI を利用した具体例についても追記を行った。例えば、企業内で、秘密管理されている情報を生成 AI に利用し、当該情報が同一部門及び別部門において AI 生成物として生成・出力されることがあったとしても、当該情報が秘密管理されているのであれば、そのことの一事をもって秘密管理性が否定されることはないことを明確化した（次ページ図 3-1-15）。
- 有用性の考え方について
  昨今の裁判例を踏まえ、営業秘密の有用性の要件として、当該情報を取得した者がそれを有効に活用できるかどうかに関わらず、事業者の事業活動に使用・利用されているのであれば、有用性の要件が充足されるものであると考えられる旨等を明確化した。
- 非公知性の考え方について
  非公知性の有無の判断についての考え方を明確化した。例えば、第三者からのハッキング等により不正取得された営業秘密が、その後ダークウェブ上に公表されたとしても、その一事をもって直ちに非公知性が喪失するわけではない旨を明確化した。また、AI 学習用データを想定した公知情報を組み合わせたものについて、その組み合わせが知られていなかったり容易に知り得ないため、財産的価値が失われていない場合や、その組み合わせが知られていたり容易であったりしたとしても、取得に要する時間や資金的コストがかかるため財産的価値があるという場合には、非公知と言い得る旨を明確化した。リバースエンジニアリングについては、特殊な技術をもって相当な期間が必要であり、誰でも容易に当該営業秘密を知ることができない場合には、当該製品を市販したことをもって非公知性



■図 3-1-15　生成 AI 利用における秘密管理の参考例
（出典）経済産業省「『営業秘密管理指針』の主な改訂内容一覧※121」

を喪失するとはならないが、誰でもごく簡単に製品を解析することによって営業秘密を取得できるような場合には、当該製品を市販したことによって営業秘密自体を公開したに等しいと考えられることから、非公知性を喪失すると考えられる旨を明確化した。

(c) サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携

防衛省、経済産業省及び IPA は、2024 年 12 月 27 日に、防衛省・自衛隊を含む我が国のサイバー状況把握力、及びサイバー事案への対処能力の強化、並びにサイバー安全保障の確保に資することを目的として、3 者間での連携を強化すべく、包括的な連携協定を締結した※122。同協定に基づき 3 者間がそれぞれに保有する技術的・専門的な知識を相互に共有し、「自衛隊による IPA の取り組みへの参画等を通じた産業界向けセキュリティ支援」「情報提供等を通じた防衛産業との連携強化」「3 者間の新たな協議体（枠組み）の設置」※123 を進めていく。

(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【6.0 版】※124」を 2025 年 3 月 5 日に公開した。改訂内容として、EC 加盟店における、システムや Web サイトの脆弱性対策や、不正利用対策として EMV 3-D セキュア（カード決済時に本人認証を強化するサービス）の導入、及び不正ログイン対策等のセキュリティ対策の実施が盛り込まれた。

3.1.4 総務省の政策

総務省は「ICT サイバーセキュリティ政策の中期重点方針」（以下、中期重点方針）を 2024 年 7 月 31 日に公表した※125。中期重点方針は、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設置された「ICT サイバーセキュリティ政策分科会」により取りまとめられた。同分科会は我が国のサイバーセキュリティをめぐる環境が今後大きく変化していくことが見込まれることを踏まえ、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について集中的に検討を行うために設置された。「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」「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」「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」に関し、総務省が中長期的に取り組むべき施策の方向性が検討され、中期重点方針として「重要インフラ分野等におけるサイバーセキュリティの確保」「サイバー攻撃対処能力の向上と新技術への対応」「地域をはじめとするサイバーセキュリティの底上げに向けた取組」「国際連携の更なる推進」が示された。

以下では、中期重点方針の内容も踏まえつつ、総務省の施策を紹介する。なお、総務省における人材育成に関する施策については、「3.2.3 (2) サイバーセキュリティ人材育成のための活動」を参照いただきたい。

(1) 情報通信ネットワーク・サービスにおけるサイバーセキュリティ確保の取り組み

情報通信ネットワークに大きな影響を及ぼすIoTボットネット対策、安全・安心な通信サービスの利用に向けたスマートフォンアプリのセキュリティ対策、データの改ざんや送信元のなりすまし等を防止する仕組みであるトラストサービス等について2024年度の取り組みを紹介する。

(a) IoTボットネットに対する端末側の対策（新NOTICE）

NOTICE（National Operation Towards IoT Clean Environment）※126は総務省所管のNICTが推進するIoTボットネット対策の一つである。「国立研究開発法人情報通信研究機構法（NICT法）」が2023年12月に改正され※127、新NOTICEでは、従来のIoT機器のパスワードの設定不備を検知、注意喚起する取り組みに加え、ファームウェアに脆弱性を有する機器の調査、感染端末の探索も調査対象となった（「情報セキュリティ白書2024※128」の「2.1.4(1)(a)NOTICEにおける端末（IoT機器）側の調査」参照）。新NOTICEの活動の目的は「IoT機器のセキュリティ対策向上を推進することにより、ボットネットによるサイバー攻撃の発生や被害を未然に防ぐ」ことである。「脆弱なIoT機器の観測能力強化」「IoT機器へのリスクと対策への意識啓発」「メーカーやSIerとの連携強化」の活動を行い、総合的な対処を推進していくという。

2024年度のIoT機器の観測状況を表3-1-2に示す。

種類	件数
容易に推測可能なID・パスワードである機器	18万3,066件
ファームウェアに高リスク脆弱性を有するIoT機器	8万7,005件
マルウェア感染IoT機器検知数	1万5,965件
リフレクション攻撃の踏み台にされうるIoT機器	21万6,852件

■表3-1-2　IoT機器の観測状況（2024年4月～2025年3月）
（出典）NOTICE Webサイト※129を基にIPAが作成

今後は、NOTICEで得られたNICTの知見、ノウハウを活用し、高度な分析情報の提供や重要インフラを対象としたアタックサーフェス（攻撃対象領域）調査に取り組む。

(b) IoTボットネットに対するネットワーク側の対策（C&Cサーバーの検知・対処の推進）

2022～2023年度の2年間のプロジェクトとして、電気通信事業者におけるフロー情報※130の分析によるC&Cサーバー検知技術の有効性検証、及び事業者間の情報共有における課題整理のための実証事業を行った（「情報セキュリティ白書2024」の「2.1.4(1)(b)ネットワーク側やその他における対策」参照）。その結果、分析機能の強化、能動的分析等の新たな手法の導入による、技術的に信頼度の極めて高いC&Cサーバーリストの作成、C&Cサーバーの挙動状況、国別、マルウェアファミリー等の属性の把握等に成功したという。

今後、C&Cサーバーの検出網羅性の向上を目指すためには「迅速かつ精緻なC&Cサーバーリストの作成」「分析事業者の拡大」「統合的な分析」といった取り組みが必要であり、ボットネット縮小を目指すためには、「IoTボットネットの全体像の可視化」「各ボットネットの特性に応じた効果的な対処の実現」が必要であるという。

(c) スマートフォンアプリのセキュリティ対策の推進

スマートフォンに搭載されているアプリについて、利用者の意図しない利用者情報の取り扱いが生じ得る懸念等に対し、2023年度より人気アプリ等を対象に利用者の意図に反したスマートフォンアプリによる情報送信等について技術的な解析を実施し、国内のアプリ解析能力水準に係る課題等の整理が行われた。

また、「スマートフォン利用者情報取扱指針」等を含む「スマートフォン プライバシー イニシアティブ（SPI）」は、2024年11月、セキュリティの確保に係る取り組みの追記等が行われ、「スマートフォン プライバシー セキュリティイニシアティブ（SPSI）」として公表された※131。

(d) データ流通基盤のトラストサービス（eシール）の推進

2024年4月に「eシールに係る指針（第2版）※132」が公表された。同指針ではeシールを以下のように説明している。

- 電子データの出所または起源を示すためのもの
- 電子データについて改変が行われていないかどうかを確認することができるもの

eシールは電子文書等が改ざんされていないことの確認ができ、発行元を証明する。電子署名も電子文書等への暗号化等の措置が行われて以降、当該電子文書等が改ざんされていないことを確認できるという点では同じである。一方、電子署名は自然人※133が電子文書を作成したこと、電子文書に示された意思表示が本人によるものであることを証明するという点で違いがある。テレワーク等の働き方が定着し、官民を問わずあらゆる手

続きを電子的にスムーズに完結させるニーズが増大した。オンライン取引・手続き等において、発行元に関する証明のニーズが高まること等が想定されるため、e シールに係る認証業務の民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた検討を行い、2025 年 3 月に「e シールに係る認証業務の認定に関する規程※134」（令和 7 年総務省告示第 113 号）により国（総務大臣）による認定制度を創設した。

(2) サイバー攻撃対処能力の向上の取り組み

サイバー攻撃対処能力の向上を目指す実証事業、体制強化の取り組みを紹介する。

(a) CYXROSS

「CYXROSS」はサイバーセキュリティ情報の収集、分析等を行う実証事業である。安全性、透明性の検証が可能な NICT 開発のセンサー「CYXROSS Agent」を各省庁の端末に導入し、得られたマルウェア情報等を NICT の「CYNEX」（「3.2.3 (2) (b) CYNEX」参照）で組織横断的な情報分析を行い、デジタル庁、NISC、各省庁等に情報共有する※135（図 3-1-16）。CYXROSS の取り組みの意義は、「自国の健康診断は自国の技術で」行うことにあり、国産技術による政府端末情報収集、複数省庁が連携する横断分析環境の確立、日本の情勢分析能力強化を挙げている。2024 年までに CYXROSS Agent Ver1.0 の実装が完了し、オペレーションルーム「CYXROSS CORE」の運用を開始した。また、総務省の端末への導入を開始し、今後政府全体の端末への導入を拡大する。更に、CYXROSS を GSOC※136 と連携させ、NICT の継続的な実務として取り組むことで、エンドポイントを含む政府システムの一元的な監視体制の構築に貢献する予定である。

(b) 研究開発等を担う NICT の体制強化の取り組み

サイバーセキュリティ分野における研究開発能力の強化に向けて、大きな影響力を有する米国との連携を深化させるため、NICT 内に米国の政府機関や研究組織とのサイバーセキュリティ技術に関する国際的な結節点を形成し、共同研究や人材交流、情報の共有や発信等を戦略的に活性化させる必要があるという。

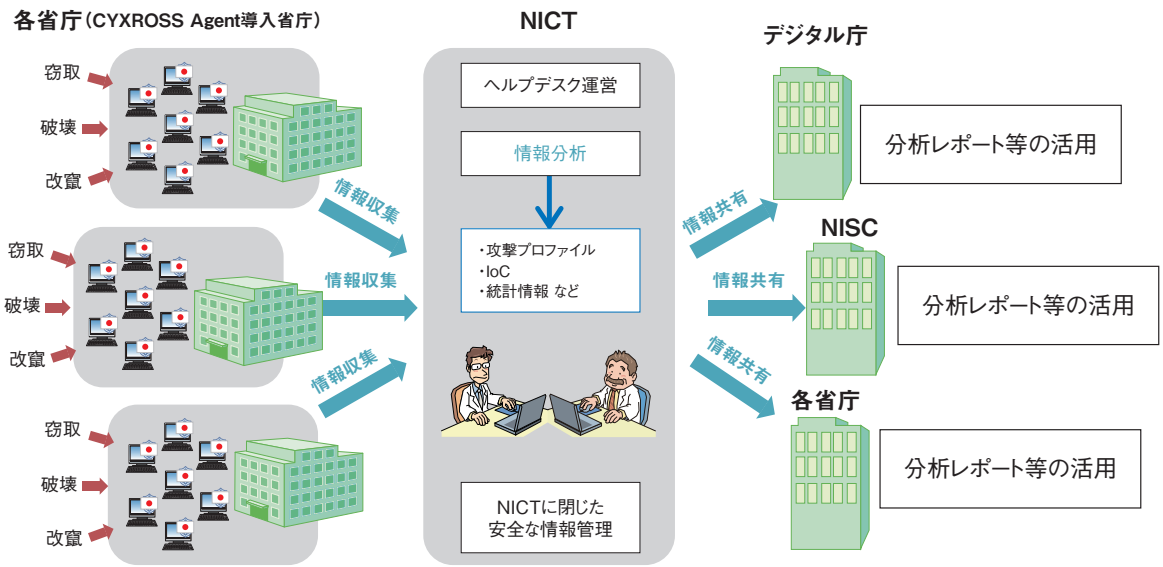
(3) ガイドライン改訂の取り組み

総務省では、日常生活にネットサービスの利用が不可欠な現代社会において、安全にサービスが利用できるよう各種ガイドラインの整備とその普及に努めている。ここでは 2024 年度に改定されたセキュリティに関するガイドラインを紹介する。

(a) スマートシティセキュリティガイドラインの改訂

2024 年 6 月 28 日、「スマートシティセキュリティガイドライン（第 3.0 版）」が公表された※137。同ガイドラインは地域 DX や地域活性化にもつながるスマートシティのセキュリティ確保のため策定されている。目的は以下のとおりである。

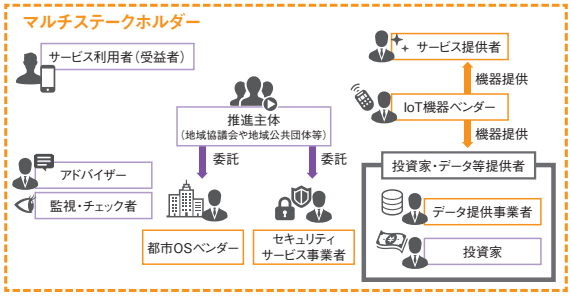
- スマートシティの推進に関わるあらゆる主体において、セキュリティの観点でスマートシティの構造を把握する。



■図 3-1-16　CYXROSS 実証事業の全体イメージ
（出典）NICT「NICT サイバーセキュリティ研究所の取り組み※135」を基に IPA が編集

- 各関係主体が、スマートシティを構成する各要素のセキュリティ上のリスク及び実施すべきセキュリティ対策を把握する。
- 各関係主体が、スマートシティの特徴を踏まえたスマートシティ横断的なセキュリティ上のリスク及び実施すべきセキュリティ対策を把握する。

なお、同ガイドラインでは関係主体を以下の図 3-1-17 のとおり定義し、想定読者を地域協議会、地域公共団体等の推進主体、推進主体と連携しセキュリティ対策の実施が求められるサービス提供者、及び都市 OS ベンダー等としている。



■図 3-1-17　ガイドラインで定義する関係主体のイメージ
（出典）総務省「スマートシティセキュリティガイドライン（第 3.0 版）※138」を基に IPA が編集

(b) 地方公共団体におけるサイバーセキュリティ対策

総務省は、地方公共団体に対し「地方公共団体における情報セキュリティポリシーに関するガイドライン」を示している。直近では、以下のポイントについて改定を行い、「令和 7 年 3 月版」として 2025 年 3 月 28 日に公表した※139。

- マイナンバー利用事務系に係る画面転送の方式について
- 無線 LAN 利用の要件について
- 機器等の調達について
- インシデントの対応について

また、2024 年 6 月に改正された地方自治法において、地方公共団体はサイバーセキュリティを確保するための方針を策定し、その方針に基づき必要な措置を講じることとされた。総務大臣は、方針の策定等について指針を示すこととされている（2026 年 4 月 1 日施行）。

総務大臣の指針案については、2024 年 4 月 1 日に通知され、各地方公共団体は当該指針案を十分に参照して、方針の策定を改正法施行日に行うことになる。更なるサイバーセキュリティの確保・充実が目指される。

3.1.5 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戦略に基づき、警察庁が 2022 年 4 月に改定した「警察におけるサイバー戦略※140」では、2025 年までの 3 年間の警察の取り組みとして、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が掲げられた。

同戦略に基づき「警察におけるサイバー重点施策※141」も併せて改定された。そこでは、「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が挙げられている。また、「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」も併せた五つが重点施策として推進されてきた。

本項では、これらのサイバー空間に対する警察の基本施策のもと、2024 年度を中心とした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 6 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※142」「令和 6 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※56」及び「令和 6 年版 警察白書※143」等に基づいて述べる。

(1) 警察における主な取り組み

2024 年度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、官民連携の推進の三つについて述べる。

(a) 警察における組織基盤の更なる強化

警察では、深刻化する重大サイバー事案の対処を担う国の捜査機関として、関東管区警察局に「サイバー特別捜査隊」を 2022 年 4 月に新設した。2024 年 4 月には、同隊を発展的に改組し、新たに「サイバー特別捜査部※144」が設置されるとともに、そのもとに企画分析課と特別捜査課が置かれた。企画分析課は、重大サイバー事案に関する情報の収集と分析、特別捜査課は、重大サイバー事案に関係した犯罪の捜査を主に担う。

サイバー特別捜査部は、情報技術解析部門の解析

担当職員等の併任者も合わせると総勢約 300 人強の体制となり、犯罪捜査のほかに、重大サイバー事案の対処に必要な情報の収集や整理及び事案横断的な分析等を行う。

これにより、サイバー特別捜査部は、都道府県警察が捜査により得た膨大な情報を集約し、外国捜査機関等との情報交換や独自の捜査で得た情報と併せて高度な分析・解析を行い、犯罪グループの中枢被疑者の特定や実態解明等を一層推進することができるようになった。

(b) 実態把握と社会変化への対応力の強化

日本国内の治安をめぐる情勢は近年目まぐるしく変化を続けており、その中でサイバー空間は社会経済活動が営まれる重要かつ公共性の高い空間へと変貌を遂げ、特に SNS は目覚ましい普及が見られている。

このように我々を取り巻く環境が激変する中において、ますます深刻化するサイバー犯罪の検挙と抑止に向けた警察による実態把握と対応力の強化について述べる。

(ア) 不正アクセスへの対応

警察では、サイバー犯罪の上位を占める不正アクセス行為の犯行手口の分析に基づき、関係機関等とも連携し、広報・啓発等により被害を防止するとともに、毎年、民間企業や行政機関等に対する「不正アクセス行為対策等の実態調査※145」及び「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発状況等に関する調査※146」等を実施し、公表している。

前者は市販のデータベースに掲載された企業、教育機関（国公立、私立の大学等）、医療機関、地方公共団体（県・市区町村等）、独立行政法人及び特殊法人、後者は市販のデータベースに掲載された企業のうち業種分類が「情報・通信」「サービス」「電気機器」または「金融」であるもの、及び国公立・私立大学のうち理工系学部またはこれに準ずるものを設置するものから無作為に抽出し、調査票を郵送で配布し、電子メールまたは郵送により回答を得た結果を取りまとめたものであり、産官学の広い範囲のデータが集約されているといえる。

(イ) インターネットバンキングに係る不正送金への対応

警察では、2023 年から被害が急増しているインターネットバンキングに係る不正送金事犯に対し、関係機関と連携したフィッシング被害の実態把握や、フィッシングサイトに関する分析及び関係事業者への照会等、早期の実態解明と必要な取り締りを推進している。併せて、フィッシング対策に関する Web サイト※147 を開設し、被害防止策や被害に遭った際の対応について周知している。

また、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）※148 等との官民連携の枠組みを通じて、把握したフィッシングサイトの情報をセキュリティソフト事業者等に提供する等の被害防止対策も推進している。

(ウ) インターネット上の違法情報・有害情報への対応

警察庁は、一般財団法人インターネット協会へ業務委託する形で、違法・有害情報の発信に関する情報収集と対処を目的とする団体であるインターネット・ホットラインセンター（IHC：Internet Hotline Center）※149 を 2006 年に開設した。具体的には「児童ポルノ」「覚醒剤等の規制薬物の販売」「犯罪実行者の募集」「集団自殺の呼び掛け」に関する通報を一般のインターネット利用者等から受理して、警察への情報提供、サイト管理者への削除依頼等を行っている。

また、インターネット上の重要犯罪密接関連情報等を収集し、IHC に通報するサイバーパトロールセンター（CPC）も運用している。

(エ) 国際情勢を踏まえた注意喚起

ここ数年、情報窃取を目的としたサイバー攻撃、国家を背景とする暗号資産獲得を目的としたサイバー攻撃事案等が相次ぎ発生していることから、警察庁も積極的に注意喚起情報を発出している。

2019 年から現在に至るまで、警察庁は NISC とともに、「MirrorFace」というサイバー攻撃グループが、日本国内の組織、事業者及び個人に対して、マルウェアを添付したメールの送信等により、情報窃取を目的としたサイバー攻撃を行っていることを確認している。2025 年 1 月、これらのサイバー攻撃が、中国の関与が疑われる組織的なサイバー攻撃活動である可能性があることから、サイバー攻撃の手口や未然防止対策等に関する注意喚起を実施した※150。

(c) 官民連携の推進

警察では、各都道府県警察及び重要インフラ事業者等で構成される「サイバーテロ対策協議会※151」をすべての都道府県に設置しており、重要インフラ事業者等とのサイバー攻撃事案の発生を想定した共同対処訓練等の官民連携による取り組みを実施している。同協議会との連携については、警察庁の Web サイトにサイバー事

案に関する通報・相談・情報提供の統一窓口を設置して、通報・相談の負担軽減も図っている。

その他の取り組みとして、警察及び全国約 8,700 の事業者等からなるサイバーインテリジェンス情報共有ネットワーク（CCI ネットワーク）の枠組みを構築している。ここでは、情報窃取を目的と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、これら情報及びその他の情報を総合的に分析し、事業者等に対し注意喚起を実施している。

(2) 2024 年のサイバー攻撃の情勢と警察の対応

2024 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、世の中の安心・安全を確保するための警察の主な対応について述べる。

(a) サイバー空間の脅威の情勢と検挙状況

2024 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不審なアクセスの概況

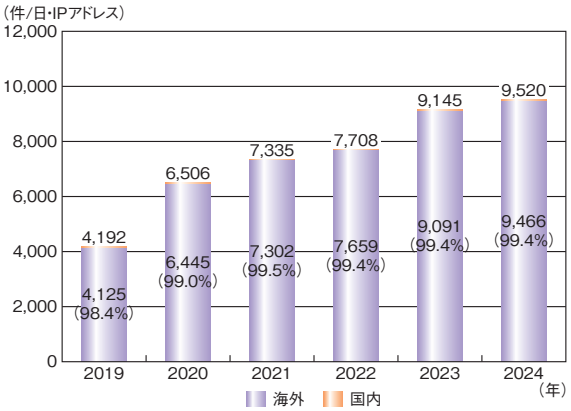
警察では、セキュリティ上の脆弱性に関する情報や標的型攻撃等の犯行手口に関する情報等を把握・分析し、被害を未然防止、拡大防止するための施策の一環として、都道府県警察のサイバー事案対策部門に技術的な面から支援を行う部隊であるサイバーフォース※152 を、警察庁及び全国の情報通信部にそれぞれ設置している。

全国のサイバーフォースの司令塔を担う警察庁のサイバーフォースセンターは、サイバー事案の予兆・実態等を把握することを目的とし、2002 年よりインターネット上にセンサーを設置し、リアルタイム検知ネットワークシステムを通じて、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、分析している。これにより、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、脆弱性を悪用した攻撃、マルウェアに感染したコンピューターの振る舞い等、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。

2024 年に同センサーが検知した不審なアクセス件数は、1 日・1IP アドレスあたり 9,520 件と前年を 4.1% 上回り、2011 年以降、増加の一途をたどっているが、その大部分は海外を発信元とするアクセスが占めている（図 3-1-18）。

(イ) サイバー犯罪・サイバー事案の概況

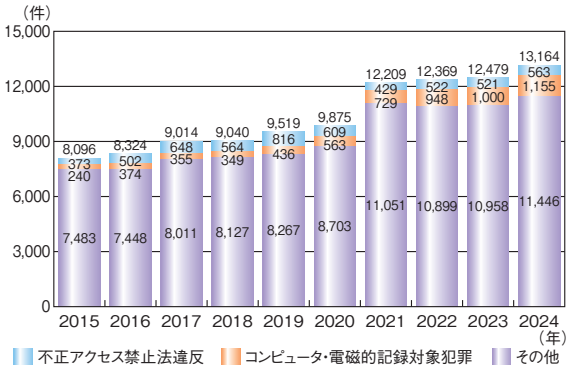
インターネット空間を悪用したサイバー犯罪※153 の検



■図 3-1-18　警察庁が検知した不審なアクセス件数（1 日・1IP アドレスあたり、2019 ～ 2024 年）
（出典）警察庁「令和 6 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

挙件数は 2020 年までは 1 万件／年以下で推移していたが、2021 年に一気に 2 割以上増加の 1 万 2,209 件に跳ね上がって以来、高水準で推移している。2024 年におけるサイバー犯罪の検挙件数は、前年から 5.5% 増の 1 万 3,164 件に上った。

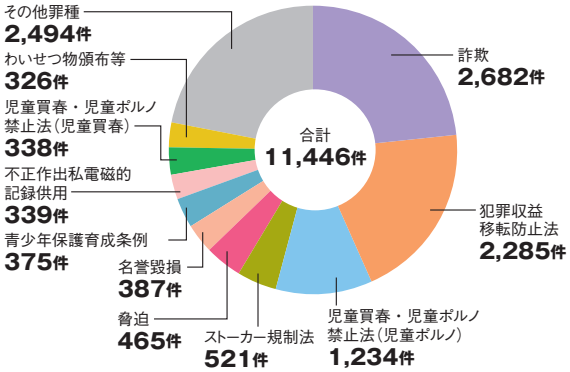
1 万 3,164 件のサイバー犯罪の内訳では、「コンピュータ・電磁的記録対象犯罪」が 1,155 件、「不正アクセス禁止法違反」が 563 件を占める（図 3-1-19）。



■図 3-1-19　サイバー犯罪の検挙件数の推移（2015 ～ 2024 年）
（出典）警察庁「令和 6 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

1 万 1,446 件を占める「その他」の内訳（次ページ図 3-1-20）については、最多を占めているのが「詐欺」であることに変わりはないが、第 2 位の「犯罪収益移転防止法違反」と第 3 位の「児童買春・児童ポルノ禁止法違反」は前年※154 と順位が逆転しているとともに、これら上位の事案全体が占める割合が増加していることは注目される。

2024 年に検挙された不正アクセス禁止法違反 563 件のうち約 9 割を占める 511 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いる。同手口を不

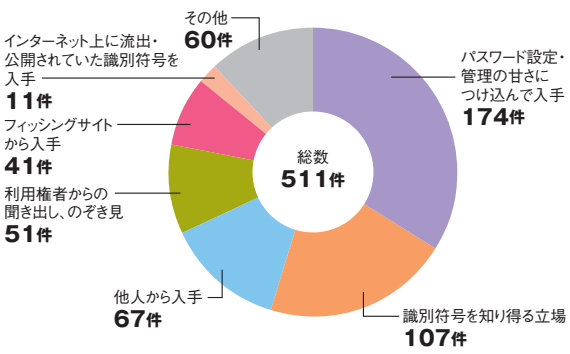


■図 3-1-20　その他の検挙状況(2024 年)
(出典)警察庁「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

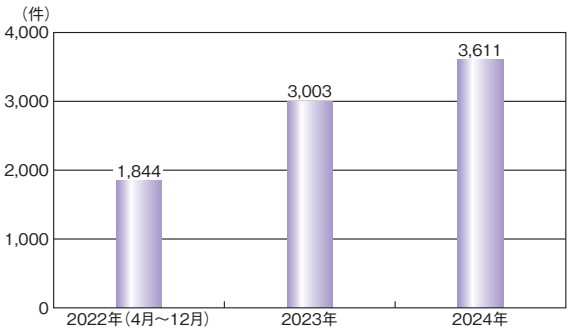
正に利用されたサービス別に見ると、「パスワードの設定・管理の甘さに付け込んで入手」が最多の 174 件、「識別符号を知り得る立場」が 2 番目の 107 件を占め、ユーザー側とサービス提供側双方に起因する事案が半分以上を占めていることが分かる(図 3-1-21)。

サイバー事案※155 の検挙件数は前年より 2 割程度増え 3,611 件に達している(図 3-1-22)。

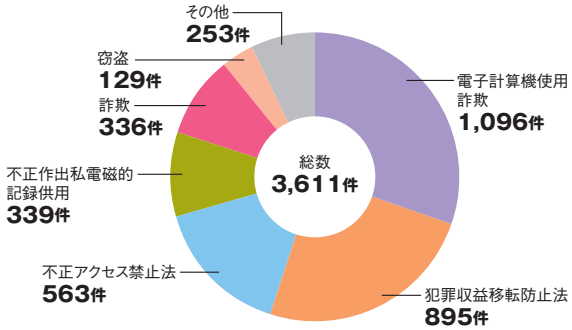
サイバー事案のうち、従業員による着服等の「電子計算機使用詐欺」と、金融機関の口座やキャッシュカードの譲渡・売買等の「犯罪収益移転防止法」に違反した案件が過半を占め(図 3-1-23)、直接的な金銭窃取を目的とした犯罪の多さが浮き彫りになっている。



■図 3-1-21　不正アクセス行為(識別符号窃用型)に係る手口別検挙件数(2024 年)
(出典)警察庁「令和 6 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 3-1-22　サイバー事案の検挙件数の推移(2022 ～ 2024 年)
(出典)警察庁「令和 6 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 3-1-23　サイバー事案の検挙状況(2024 年)
(出典)警察庁「令和 6 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)インターネット空間を悪用した犯罪の概況

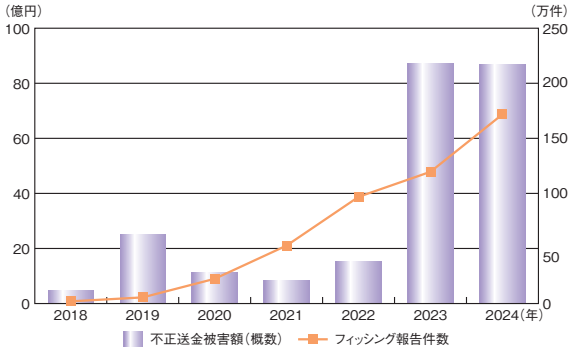
以下、インターネット空間を悪用した主な犯罪の概況を述べる。

- フィッシング

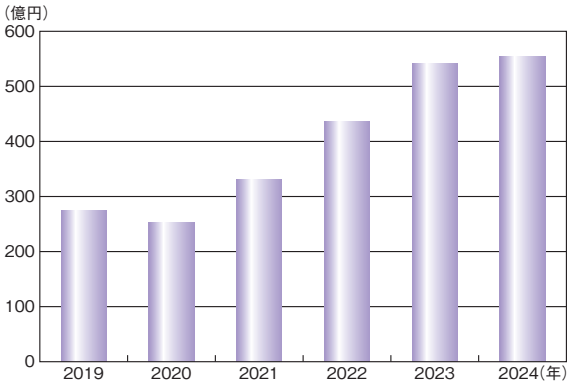
  フィッシング対策協議会によると、2024 年におけるフィッシング報告件数は 171 万 8,036 件であり、前年の 119 万 6,390 件から大きく増加した一方、不正送金の被害額は 86 億 9,000 万円と微減となった(図 3-1-24)。また、一般社団法人日本クレジット協会によると 2024 年のクレジットカードの不正利用被害額は約 555 億円と前年比で 2.6% 増え、過去最多となった(次ページ図 3-1-25)。

- 特殊詐欺

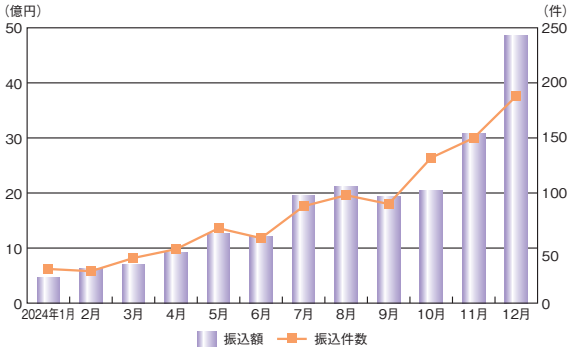
  2024 年の特殊詐欺(被害額 500 万円以上の振り込み型の事案)の被害件数・振込額は、年末に向け、ともに右肩上がりになっている(次ページ図 3-1-26)。2024 年の被害額は約 314 億円であり、そのうちインター



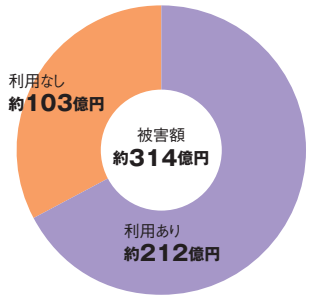
■図 3-1-24　フィッシング報告件数及び不正送金被害額の推移(2018 ～ 2024 年)
(出典)警察庁「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 3-1-25　クレジットカード不正利用被害額の推移(2019～2024 年)
(出典)警察庁「令和 6 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 3-1-26　特殊詐欺におけるインターネットバンキングを利用した振込被害の推移(2024 年 1 ～ 12 月)
(出典)警察庁「令和 6 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 3-1-27　特殊詐欺の被害額に関するインターネットバンキングの利用の有無(2024 年)
(出典)警察庁「令和 6 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

ネットバンキングを利用したものは約 212 億円と約 3 分の 2 を占める(図 3-1-27)。

近年は、匿名・流動型犯罪グループによるものと見られる特殊詐欺が広域的に行われており、同グループはSNSでいわゆる闇バイト等で高額な報酬を示唆して「受け子」等を募集し、犯行に加担させている。また、首謀者、指示役、実行役の間の連絡手段には、匿名性が高く、メッセージが自動的に消去される仕組みを備えた通信手段を使用する等、犯罪の証拠を隠滅しようとする手口が多く見られる。

なお、特殊詐欺の被害拡大防止を目的として、警察庁では 2025 年 1 月にゆうちょ銀行との間で情報連携協定書を締結した※156。

- SNS 型投資・ロマンス詐欺

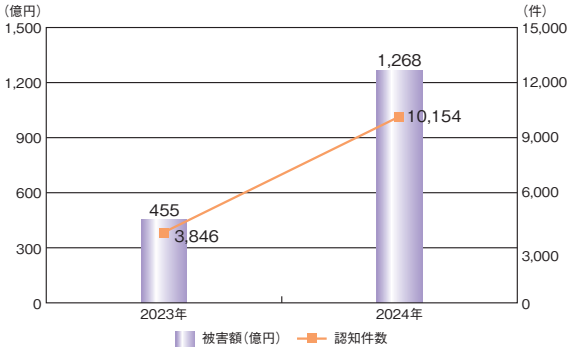
SNS 型投資・ロマンス詐欺は、SNS を通じて対面することなく、交信を重ねる等して関係を深めて信用させ、投資金名目やその利益の出金手数料名目等で金銭を騙し取る、または恋愛感情や親近感を抱かせて金銭を騙し取る等の犯罪である。

SNS の利用が進む中、同詐欺の認知件数、被害額ともに前年比で急増し、被害額が約 1,268 億円と特殊詐欺を大きく上回っていることは注目に値する※157(図 3-1-28)。

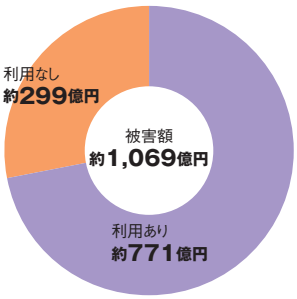
また、同詐欺でも振込が主に使用された事案では、インターネットバンキングが利用された事案の被害額が約 771 億円と 7 割以上の高い比率を占める(図 3-1-29)。

- ランサムウェア

2024 年のランサムウェアの被害報告件数は 222 件、ノーウェアランサムは 22 件であった。ノーウェアランサムの件数は前年比で 8 件減っているものの、ランサム



■図 3-1-28　SNS 型投資・ロマンス詐欺の認知件数・被害額の推移(2023 ～ 2024 年)
(出典)警察庁「令和 6 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 3-1-29　SNS 型投資・ロマンス詐欺(振込が主に使用された事案)の被害額に関するインターネットバンキングの利用の有無(2024 年)
(出典)警察庁「令和 6 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

ウェアは 25 件増えていることから、合算では 17 件増えており、2022 年から高止まりが続いている。なお、最近拡大しつつある手口であるノーウェアランサムとは、データを暗号化することなくデータを窃取した上で対価を要求する手口の呼称である。ランサムウェアについては「1.2.1 ランサムウェア攻撃」を参照されたい。

(b) サイバー攻撃に対する警察の取り組み事例

2024 年に実施した、主なサイバー攻撃に対する具体的な取り組み事例を挙げる。

(ア) 国際アドバイザリーへの共同署名

中国政府を背景とするサイバー攻撃グループといわれている「APT40」は、北米、欧州、豪州等を標的としており、我が国の企業も攻撃の標的になっていたことが確認されている。

2024 年 7 月、警察庁及び NISC は、米国、英国、カナダ、ニュージーランド、ドイツ及び韓国の関係機関とともに、オーストラリア通信情報局（ASD：Australian Signals Directorate）オーストラリアサイバーセキュリティセンター（ACSC：Australian Cyber Security Centre）が作成した国際アドバイザリー「APT40 Advisory PRC MSS tradecraft in action[※158]」の共同署名に加わり、アドバイザリーを公表した。これには、APT40 による過去の攻撃事例に基づく攻撃手法、攻撃の検知や緩和策が示されている。

(イ) その他国際連携による犯罪捜査等の取り組み

ICPO が主導して、西アフリカにおける組織的な金融犯罪を国際共同捜査するオペレーション「ジャッカル」に、日本警察も 2024 年 4 月から参画した。警察庁のサイバー特別捜査部は、SNS 型投資・ロマンス詐欺事案について、関係都道府県警察の横断的な捜査情報の分析や暗号資産追跡を実施し、ナイジェリア人名義の暗号資産アカウントに送金されている事実を突き止めた。同情報をナイジェリア警察に提供したところ、同国内の被疑者の検挙が行われた[※159]。

これを受け、2024 年 7 月、国際的な詐欺の拠点となっているナイジェリアで、ICPO と独立行政法人国際協力機構（JICA：Japan International Cooperation Agency）が開催した、ロマンス詐欺等の捜査力向上を目的とした研修会において、警察庁担当者が資金回収等に使われる暗号資産に関する捜査手法の説明等を行った[※160]。

2024 年にも深刻な被害が発生した DDoS 攻撃への対応については、国際共同捜査を通じ、外国捜査機関から提供を受けた情報を緻密に精査することによって、DDoS 攻撃 Web サービスを利用した者を 3 名検挙した。2024 年 12 月には警察庁 Web サイトにおいて DDoS 攻撃に関する注意を促すメッセージを掲載するとともに、公式 X アカウントや Google の広告機能を活用して周知する取り組みを行った[※161]。

OT（Operational Technology）のサイバーセキュリティ対策に関する国際連携としては、警察庁は NISC とともに、ACSC が策定した文書「OT サイバーセキュリティの原則（Principles of OT Cyber Security）」の共同署名に加わった[※162]。

(ウ) 生成 AI を悪用した事件被疑者の検挙

生成 AI に関する具体的な事案としては、2023 年 3 月、生成 AI を利用し、人が電子計算機で実行した際、ファイルのデータを上書きして破壊する機能を有する不正プログラムを作成したことにより、警視庁は 2024 年 5 月に不正指令電磁的記録作成容疑で無職の男（25 歳）を逮捕した[※163]。

(エ) 合同捜査本部による不正送金事件の捜査

2022 年から 2023 年にかけて発生したインターネットバンキングに関する不正送金事件で、関係都道府県警察により得られた情報をサイバー特別捜査部が集約・分析するとともに、暗号資産の追跡捜査や関係被疑者の SNS アカウントに関する捜査を実施した。

その結果、サイバー特別捜査部や関東管区警察局及び 16 都道府県警察（警視庁、広島、北海道、宮城、茨城、群馬、千葉、静岡、大阪、兵庫、奈良、岡山、愛媛、福岡、長崎、熊本）の合同捜査本部は、同一の犯行グループが SIM スワップという手口を駆使し、組織的に不正送金を実行している実態を解明した。そして最終的に 2024 年 7 月、犯行グループの指示役と見られる男（44 歳）を不正アクセス禁止法違反（不正アクセス行為）で逮捕した[※164]。

合同捜査本部の捜査により、同グループによる被害件数及び被害額は、少なくとも 20 件、1 億 2,000 万円に上ることが明らかになっている。

(オ) 偽情報投稿事案被疑者の検挙等、能登半島地震に関する対応

2024 年 1 月 1 日に発生した能登半島地震においては、被災地の警察が捜索活動等に全力を挙げる中、SNS

上において過去の災害時の画像や虚偽の救助要請が拡散されたこと等により、捜索活動等が妨害される事態が生じていた。そうした状況の中、サイバー特別捜査隊（当時）は、各種情報収集を通じて、被災地の警察と連携しながら、関連アカウントに関する捜査を実施した。

石川県警察は、サイバー特別捜査隊との連携による捜査の結果、地震当日に被災者を装ってSNS上に救助を求める虚偽の内容を投稿し、本来不要な捜索活動等を警察に実施させてその業務を妨害した会社員の男（25歳）を特定し、2024年7月に偽計業務妨害容疑で逮捕した※165。

なお、同地震発生時には、SNS上において、QRコードを利用した義援金を募る送金詐欺も、警察によって確認された。

（カ）警察におけるその他の取り組み

警察庁はSIMスワップによる不正送金対策として、2024年5月、総務省と連携し、携帯電話事業者に対して本人確認の強化を要請した（2022年以降2度目）。SIMスワップは、実在する人物になりすまして店舗に来店し、本人確認資料として偽造した運転免許証等を用い、MNP（携帯電話番号ポータビリティ）またはSIMカードの再発行を行うことで携帯電話番号を乗っ取り、乗っ取った携帯電話番号のスマホを悪用して2段階認証やパスワードの再発行を行うことでインターネットバンキング等のアカウントを乗っ取り、不正送金を行う手口である※166。この手口による被害は、2022年に爆発的に発生した。

国内におけるサイバー保険を名目とした架空料金請求詐欺事件に係る捜査においては、サイバー特別捜査隊（当時）による暗号資産追跡と、その結果の事案横断的な分析により、従来明らかになっていなかった事案相互の関連性が明らかになり、関係警察による関連被疑者の逮捕に貢献した。

このほか、「国民を詐欺から守るための総合対策※167」（2024年6月18日、犯罪対策閣僚会議決定）に基づき、関係機関・団体・民間事業者等の協力を得ながら、各種施策を強力に推進している。

3.2 サイバーセキュリティ人材の現状と育成

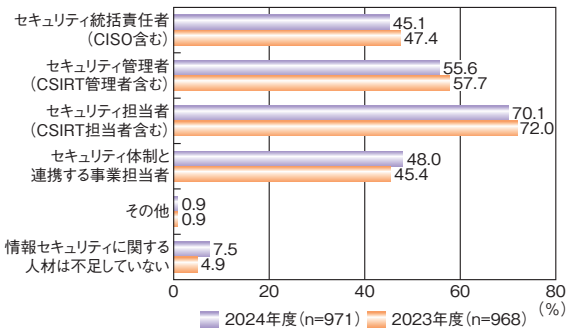
日本におけるサイバーセキュリティ人材は、様々な人材育成施策が行われているものの、不足状態が続き、深刻な問題となっている。官民挙げての新たな育成施策では、多くの課題が浮き彫りになっており、これらに対応する取り組みが行われている。本節では、官民における、サイバーセキュリティ人材育成の取り組みについて述べる。

3.2.1 サイバーセキュリティ人材の現状と育成状況

ISC2, Inc. が発表した「2024 ISC2 Cybersecurity Workforce Study※168」によると、日本のサイバーセキュリティ人材の不足は過去最大に達しており、セキュリティ確保には 16 万 9,603 人の専門家が追加で必要であるとされた。一方、セキュリティ人材の労働力については、堅調に増加しており、前年より 4% 増加しているものの、供給が需要に追い付いていない状況である※169。

一般社団法人日本情報システム・ユーザー協会（JUAS：Japan Users Association of Information Systems）の東証一部上場企業とそれに準じる企業を対象とした「企業 IT 動向調査報告書 2025※170」によると、不足しているセキュリティ人材の職種は、「セキュリティ担当者（CSIRT 担当者含む）」の割合が 70.1% と最も高く、続いて「セキュリティ管理者（CSIRT 管理者含む）」が 55.6% と高い（図 3-2-1）。「セキュリティ体制と連携する事業担当者」を除いて、2023 年度に比べて、すべての職種の人材で不足と回答した割合が若干減少しており、「情報セキュリティに関する人材は不足していない」割合が若干増加しているものの、情報セキュリティ人材の不足の状況に大きな改善は見られない。

また、民間の IT 転職サービス企業であるレバテック株式会社の調査※171 によれば、2024 年 12 月のセキュリティ人材の転職求人倍率が 54 倍と IT 業界における順位が 1 位となっており、深刻な人材不足が浮き彫りとなっている。



■図 3-2-1　情報セキュリティ人材不足の状況
（出典）JUAS「企業 IT 動向調査報告書 2025」を基に IPA が編集

需要の背景には様々なものがあるが、主な要因として AI の普及やデジタル化の急速な拡大や、これに伴うサイバーセキュリティインシデントの増加が考えられる。例えば、IPA が発行した「DX 動向 2024※172」によれば、DX に取り組んでいる日本企業の割合は年々増加しており、2023 年度は 7 割を超えている。また、IDC Japan 株式会社によれば、日本国内における 2024 年の国内エッジインフラ市場の支出額は前年比 12.3% 増の 1 兆 6,000 億円になると推計しており、2024 年以降も年々増加すると予想している※173。一方、警察庁によると、サイバー攻撃の前兆となることもある脆弱性探索行為等の不審なアクセス件数や、ランサムウェアの被害報告件数が前年から増加する等、極めて深刻な情勢が継続しているという※56。

日本政府においては、2024 年 11 月に東京都内で開かれた国際会議「サイバーイニシアチブ東京 2024※174」において、平将明デジタル大臣が、国家及び国民の安全を守る「能動的サイバー防衛」の検討を進めるべく、「自由、公正かつ安全なサイバー空間を確保するために官民が連携し、日本全体で対策を強化することが不可欠だ」と述べ、中谷元防衛大臣は、「サイバー人材の育成・確保こそがサイバー能力の抜本的強化の基盤であり中枢だ」と述べている※175。更に、武藤容治経済産業大臣は、産業界に「サイバーセキュリティを将来の事業活動や成長に不可欠な取り組みとして対策の強化を図ってほしい」と呼びかけている※176。

経済産業省においては、2024 年 7 月に「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）サイバーセキュリティ人材の育成促進に向けた検討会」（以下、人材育成促進に向けた検討会）を発足し、有識者及び IPA とともに、サイバーセキュリティ人材育成を更に加速し、セキュリティ人材を増加させるための検討を行い、2025 年 5 月に施策の方向性を取りまとめた。人材育成促進に向けた検討会では、「①民間企業の 99% 以上を占める中小企業におけるセキュリティ人材」「②企業や IT ベンダー等でセキュリティをリードする登録セキスペ人材」「③未来のサイバーセキュリティを担う学

生等の若年層人材」を対象として検討が進められた。

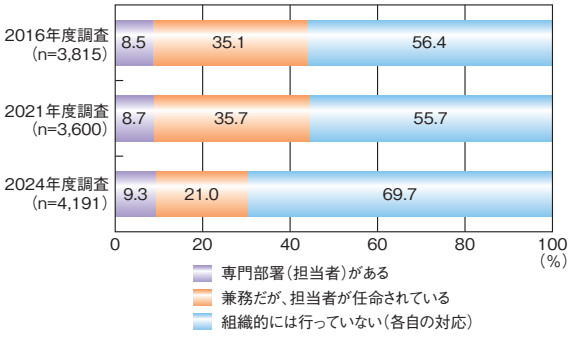
本項では、人材育成促進に向けた検討会での検討対象となっているこれら三つの活動に焦点を当て、それぞれの現状や課題と、今後のセキュリティ人材育成の方向性について述べる。

(1) セキュリティ人材不足の現状

セキュリティ人材不足については、サイバーセキュリティ対策の必要性が十分認知されていないことやコストの問題等、様々な要因により生じているものと考えられる。以下では、人材育成促進に向けた検討会で取り上げられたセキュリティ人材不足の現状を紹介する。

(a) 中小企業のサイバーセキュリティ

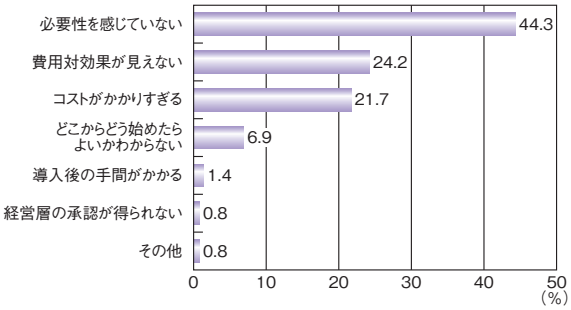
IPA が実施した「2024 年度 中小企業における情報セキュリティ対策に関する実態調査※177」によると、セキュリティの「専門部署（担当者）がある」企業の割合は、2021 年度に行った同様の調査時と比較して、0.6% 増の 9.3% にとどまっている。また、「兼務だが、担当者が任命されている」企業は21.0%に減少、「組織的には行っていない（各自の対応）」企業が 69.7% と大幅に増加している（図 3-2-2）。



■図 3-2-2　中小企業における情報セキュリティ体制
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

パロアルトネットワークス株式会社の調査※178 においても、セキュリティの対策に関与する担当者を「非 IT 担当が兼務」している中小企業が 34%、「担当者不在」の中小企業が 9% であるとの結果が示されている。

更に、「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」によると、情報セキュリティに関する教育を含む過去 3 期の情報セキュリティ投資について、投資していないと回答した中小企業の割合が 2024 年度は 62.6% に上っている。投資していない 1 番の理由として「必要性を感じていない」が 44.3% と最も多く、次いで「費用対効果が見えない」が 24.2%、「コストがかかりすぎる」が 21.7% となっている（図 3-2-3）。



■図 3-2-3　情報セキュリティ対策投資を行わなかった理由（n=2,623）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

以上のことから、中小企業ではセキュリティ人材による組織的な体制の構築が進んでおらず、その背景として情報セキュリティ投資の必要性の認識の不足やコストの問題があることがうかがえる。

(b) 情報処理安全確保支援士（登録セキスペ）の推移

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に係る専門人材の国家資格である（「3.2.2 (2) 情報処理安全確保支援士制度」参照）。登録セキスペの登録者数は、2020 年 5 月に情報処理の促進に関する法律が改正され、登録セキスペの登録更新制度が導入されて以降、2 万人前後と横ばいで推移していた。2024 年には増加に転じたものの、2020 年 4 月の登録者数である 20,413 人と比較すると、2025 年 4 月は 16% 増の 23,751 人にとどまっている。このような登録者数の伸び悩みから、特に中小企業では、登録セキスペの確保が難しくなっている可能性がある。

更に、情報処理安全確保支援士試験合格者のうち 6 割以上は登録セキスペへの登録がされていない。また、登録消除者のアンケート結果によると、「メリットがない」「金銭的な負担が大きい」「転職・異動・業務上不要」というコメントが目立っている。課題として、セキュリティ業務がベンダー側に偏っており、ユーザー企業での活用が進んでいないこと、専業化がされておらず活躍の場が限られていること、資格維持のためのコストが大きいこと（3 年間で 10 万円以上）等が挙げられており※179、維持コストを低減するとともに、登録セキスペの活躍の場とユーザー企業での活用促進が望まれている。

(c)若年層への教育

一般社団法人セキュリティ・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・キャンプ事業※180では、2004年度から2024年度までに「セキュリティ・キャンプ全国大会」を始めとして「セキュリティ・キャンプ　ネクスト」「セキュリティ・キャンプ　ジュニア」「セキュリティ・ミニキャンプ」を実施し、累計3,012名が修了した(「3.2.3(2)(a)セキュリティ・キャンプ」参照)。若年層の優秀なセキュリティ人材の早期発掘と育成という目的に沿って、これまで数多くの将来有望な人材を輩出してきており、情報セキュリティの業界にとどまらず各方面から、高度なIT人材育成の有益なイベントとして認知されている。その一方で、1年間に育成できる人数が限定的であること、また、同全国大会を修了した後の状況を把握できていないのが現状の課題である※181。

(2)セキュリティ人材不足への対応

前項では、セキュリティ人材不足における現状や課題等について取り上げた。本項では、人材育成促進に向けた検討会の検討内容を基に、人材不足への対応の方向性について紹介する。

(a)中小企業へのセキュリティ人材育成

IPAでは、中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示した「中小企業の情報セキュリティ対策ガイドライン※182」を公開している。同ガイドラインは、経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を始め、情報セキュリティ対策の具体的な進め方を分かりやすく説明している。対策は、「情報セキュリティ5か条」等、できるところから始めて段階的にステップアップできる構成としている。同ガイドラインを活用することで、サイバーセキュリティ人材が不足している中小企業においても、対策の必要性を理解した上で組織的対策を行うことが可能になる。

また、人材育成促進に向けた検討会においては、中堅・中小企業等の組織内でセキュリティ対策を推進する者の育成・確保を行うための取り組みとして「実践的方策ガイド」の作成を進めている※183。同ガイドの案には、セキュリティ対策を実施するための最初のステップとして、セキュリティ担当者を配置転換等により兼務であっても1名は確保すること、内部だけで実施が難しい対策については付き合いのあるITベンダーや商工会・商工会議所等の支援機関を活用すること等が盛り込まれている。

(b)登録セキスペの登録者数の拡大

人材育成促進に向けた検討会では、登録セキスペを増やすための施策が検討されている。まず、登録セキスペの活用促進・活躍の場の拡大については、サイバーセキュリティ人材が特に不足している中小企業等(需要側)と登録セキスペ(供給側)をつなぐマッチングの枠組みの整備、スキル強化の機会や講習の拡大等、登録セキスペへの働きかけ、サプライチェーン強化に向けたセキュリティ対策評価制度やIoT製品に対するセキュリティ適合性評価制度である「セキュリティ要件適合評価及びラベリング制度(JC-STAR)」等の活用についての企業側への働きかけ等、多面的な施策が検討されている。例えば、「中小企業向けサイバーセキュリティ対策支援者リスト」の整備が挙げられている。同リストは登録セキスペの得意分野、専門領域等を可視化するものである。中小企業が同リストを活用することにより、登録セキスペによる中小企業のニーズに合ったセキュリティ対策の実装支援、適切なセキュリティ商材の導入支援を可能にすることが期待される。

次に、資格更新コストの低減に関しては、実際に企業等においてサイバーセキュリティ関連業務に従事している等、所定の実務にあたっている登録セキスペについて、資格更新のために同様の内容の講習を受ける負担を軽減すべく、更新講習(一部)のみなし受講制度や、更新講習の一部である「オンライン講習」の一部簡素化が検討されている※184。これらの施策を通じて、現在の登録セキスペ登録人数を2030年までに5万人まで増加させることを目指している。

(c)若年層への教育

前述のセキュリティ・キャンプでの育成人数が限定的であるという課題に関しては、既存事業を修了する人数を増やすのではなく、セキュリティの裾野を広げる観点から、AI等の特定領域の専門性と高度なセキュリティの知見の双方を兼ね備えた人材の育成を目的とする新たなセキュリティ・キャンプ事業を2025年度から実施することで、育成人数を増やす。また、修了生の継続的な知見研鑽、社会還元、活躍状況の共有等を目的としたコミュニティを整備していくことで、修了後の実績等を把握できるようにすることが今後の方向性として示された。

3.2.2 サイバー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、サイバー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

企業や組織では、定めた情報セキュリティポリシーの周知徹底、部門の情報管理等を実施する情報セキュリティマネジメント人材が不可欠である。こうした人材の育成を促進するために、IPA は 2016 年度春期から「情報セキュリティマネジメント試験」を実施している。2020 年度から CBT（Computer Based Testing）方式[※185]に移行した同試験は、2023 年 4 月からは年間を通じて随時[※186] CBT 方式により実施され、2024 年度は応募者数 4 万 5,481 人（前年比約 1.14 倍）、合格者数 2 万 8,731 人（前年比約 1.09 倍）であった[※187]。

(2) 情報処理安全確保支援士制度

サイバーセキュリティ分野初の国家資格である「情報処理安全確保支援士[※188]」（以下、登録セキスペ）は、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、2024 年度は応募者数 4 万 3,597 人（前年比約 1.16 倍）、合格者数 5,384 人（前年比約 0.95 倍）であった[※187]。登録セキスペは 2025 年 4 月 1 日時点で 2 万 3,751 人となった[※189]。

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。登録証のカラーパターンを図 3-2-4 に示す。

■図 3-2-4　登録証のカラーパターン（2025 年 4 月 1 日時点）

また、登録更新には計 4 回の講習の受講が必要である[※190]。講習の種類とその概要を表 3-2-1 に示す。

「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。

講習	講習の概要
実践講習	・実習、実技、演習または発表を伴う講習 ・3 年に 1 回受講 ・IPA または民間事業者等が行う実践的な講習の中から 1 講習を選択して受講
オンライン講習	・最新の知識及び技能の学習、倫理の醸成 ・毎年 1 回受講 ・IPA が指定する講習を受講

■表 3-2-1　講習の全体像

また、「実践講習」では、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 または民間事業者等が行う「実践講習」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修得するカリキュラムで、2024 年度は 1,209 名が受講した。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、企業における新規事業立ち上げを想定し、セキュリティ上の助言を検討するカリキュラムで、2024 年度は 2,506 名が受講した。また、主に登録後 7 年目以降の登録セキスペを対象とした「実践講習 C」を 2025 年 7 月に開始した。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 IPA が行う「業界別サイバーレジリエンス強化演習（CyberREX）[※191]」と「制御システム向けサイバーセキュリティ演習（CyberSTIX）[※192]」という「実践講習」の選択も可能となっている（「3.2.3 (1) 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「実践講習」[※193]は、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。2024 年度には 14 実施機関 48 講習であったものが、2025 年度には 16 実施機関 56 講習と増加した。

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「本資格の取得が会社の信用の大きな裏付けになり、その結果数多くの企業に脆弱性診断を実施できた。」（IT ベンダー企業経営者）[※194]、「本資格が専門性や倫理観の高い人材の証になっていて、また、質の高い学びを継続する取り組み姿勢も評価できることから資格取得を内部表彰の対象としている。」（警察関係者）[※195]との声が聞かれた。今後も、企業・組織のセキュリティ対策推進に登録セキスペが一層活躍し、大きな役割を果たしてくことが期待される。

3.2.3 セキュリティ人材育成のための活動

サイバー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。

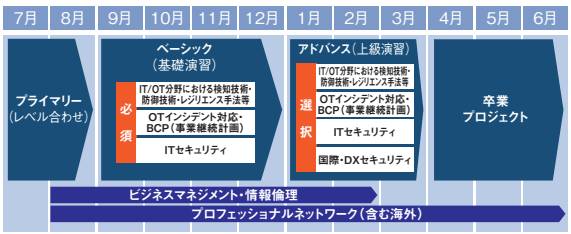
(1) 産業システムセキュリティ人材育成のための活動

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。

本項では 2024 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）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（図 3-2-5）。第 1 期から第 7 期までに 435 名の修了者を輩出し、2024 年 7 月に開講した第 8 期では、電力・鉄鋼・化学・自動車・鉄道・建築・金融・産業機械・産業用制御システムのベンダー等の幅広い業界から 57 名が参加した。



■図 3-2-5　第 8 期中核人材育成プログラムの年間スケジュール

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させる 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）

これらに加えて、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等も行っている。

海外派遣演習として、2025 年 4 月には、第 8 期受講者がフランス及び英国を訪問した。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 SystemX を訪れ、技術開発の現場を見学した。英国では、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、Imperial College London 内の Institute for Security Science and Technology（ISST）によって運営されている産学官共同研究機関 Research Institute in Trustworthy Industrial Control Systems（RITICS）及びサイバーセキュリティ分野のスタートアップ支援や企業間交流等を促進する施設 Plexal を訪問した。

国内においても、発電プラントや機械製造プラント等制御システムが稼働する現場の見学を行った。

カリキュラムの総まとめとなる「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を通じて成果物を作成する。第 7 期では 20 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 15 件を Web サイトで公開した※196。

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※197」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。

2024 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第 7 回叶会総会を開催した。

叶会には第 1 期から第 7 期までの修了者に加え、2025 年 6 月に修了した第 8 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 ICSCoE では、修了者の修了後の知識・スキルのアップデートを目的とした、リカレント教育の機会を設けている。2024 年度は 7 月から 8 月の間で 4 コースのプログラムを提供し、それぞれ希望者が参加した。最新

の技術動向やトレンドを反映した講習だけでなく、修了者間の人的ネットワークの構築、維持の場にもなっている。

(b) 責任者向けプログラム

責任者向けプログラムでは、「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）」「サイバー危機対応机上演習（CyberCREST）」の三つのプログラムを実施した。

- 業界別サイバーレジリエンス強化演習（CyberREX）
  CyberREX（Cyber Resilience Enhancement eXercise by industry）※191 は、実施回ごとに設定する対象業界において、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」としても受講可能になっている。
  2024 年 5 月と 9 月に東京、11 月に大阪で同演習を実施した。同演習では、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・回復力を強化することを目的とし、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実施した。
- サイバーセキュリティ企画演習（CyberSPEX）
  CyberSPEX（Cyber Security Planning Exercise）※198 は、組織のサイバーセキュリティを推進する責任者を対象としたプログラムである。
  2025 年 1 月に東京で同演習を実施した。同演習では、責任者層として必要なセキュリティ企画立案スキルを習得することを目的とし、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実施した。
- サイバー危機対応机上演習（CyberCREST）
  CyberCREST（Cyber Crisis RESponse Table top exercise）※199 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（CISO）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 年度の同演習は、DX 化による OT 領域のリスクと海外拠点のセキュリティ強化に焦点を当て、具体的な軽減策の検討や国際的な OT セキュリティ戦略を強化するために必要な実践的な知識やスキルの習得を目指し、2024 年 12 月から 2025 年 1 月にオンデマンド講習、2 月に講義及び机上演習を東京で実施した。

(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）」「ERAB サイバーセキュリティトレーニング」の二つのプログラムを実施した。

- 制御システム向けサイバーセキュリティ演習（CyberSTIX）
  CyberSTIX（Cyber SecuriTy practIcal eXercise for industrial control system）※192 は、制御システムのサイバーセキュリティを担当する実務者や、今後担当予定の実務者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」としても受講可能になっている。
  2024 年 5 月に大阪、9 月に東京、2025 年 2 月に札幌で同演習を実施した。同演習では、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実践的に理解することを目的とし、簡易模擬システムを用いた実機演習（ハンズオン演習）を中心に実施した。
- ERAB サイバーセキュリティトレーニング
  ERAB サイバーセキュリティトレーニング※200 は、電力小売事業に関わる ERAB（Energy Resource Aggregation Business）事業者において、セキュリティ対策を検討し、立案・実施する実務者等を対象としたプログラムである。
  同演習は、経済産業省の「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver2.0※201」における ERAB 事業者に求められるサイバーセキュリティ対策に関する知識やスキルの習得を目的としている。2024 年 11 月から 12 月にオンデマンド講習、同 12 月に最新動向の講義、グループワーク、実機を用いた実演（デモ）を中心とした演習を東京で実施した。

(2) サイバーセキュリティ人材育成のための活動

サイバー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サイバー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。21回目となる2024年度の全国大会は8月12日から17日の6日間で開催した。497名の応募があり、選考を通過した80名が参加した※202。
- セキュリティ・キャンプ　ネクスト
  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・キャンプ2024　ネクスト」を全国大会と同時に開催した。6回目の開催※203となる本プログラムでは144名の応募があり、選考を通過した10名が参加した※204。
- セキュリティ・キャンプ　ジュニア
  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15歳以下の生徒を対象に「セキュリティ・キャンプ2024ジュニア」を全国大会と同時に開催した。2回目の開催となる本プログラムでは25名の応募があり、選考を通過した6名が参加した※205。
- 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、セキュリティのリテラシー向上を目的とした参加資格を限定しない公開講座を開催している※206。
  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、2024年度は全国12ヵ所の地域で開催した※207。東京（2024年4月）、宮城（2024年6月）、三重（2024年7月）、沖縄、岩手（2024年10月）、北海道、熊本（2024年11月）では専門講座のみ開催した。広島（2024年8月）、愛知（2024年9月）、山梨（2024年9月）、大阪（2025年3月）では公開講座と専門講座が開催された。石川（2024年12月）ではワークショップと称し、専門講座に加えてCTF（Capture The Flag）も開催した。
- セキュリティ・キャンプフォーラム
  過去にセキュリティ・キャンプに参加した修了生同志や講師等との参加年度を超えた交流、及び修了後の活動成果発表を通じた修了生の認知度向上と産業界での活躍に向けたきっかけ等の場の提供を目的として、毎年2～3月のサイバーセキュリティ月間に合わせて開催している。2024年度は2025年3月15日に開催し、特別講演と修了生の活動状況の発表、セキュリティ・キャンプ関係者によるブース展示を実施した※208。
- 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の韓国、台湾、シンガポールの4地域で開始した。7回目となる2024年度は台湾で「GCC 2025」として、11の国と地域の関連団体・大学により開催された。日本からは選考を通過した4名が参加し、参加者は講義を受けるとともに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※209。

(b) CYNEX

「サイバーセキュリティネクサス（CYNEX：Cybersecurity Nexus）※210」は、NICTが運営するサイバーセキュリティ研究所で運営されている。産官学連携の結節点（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、2025年度までが第1期CYNEXとされている※135。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。

2023年10月に発足が発表された「CYNEXアライアンス」は、2024年には本格稼働フェーズに進んだ。CYNEXアライアンスは日本のサイバーセキュリティの産学官中核拠点確立を目指し、2024年12月末時点で既に90組織が参加している。CYNEXアライアンスには四つのサブプロジェクト「Co-Nexus」があり、そのうち人材育成に関係するのはCo-Nexus S（Security Operation & Sharing）、Co-Nexus C（CYROP：Cyber Range Open Platform）である。Co-Nexus Sは高度な解析者の育成とCYNEX独自の脅威情報の生成・発信を行っており、2024年12月末時点で参加組織は18組織であった。Co-Nexus Cはサイバーセキュリティ演習基盤CYROPを民間等に開放し、セキュリティ人材育成のハー

ドルを下げることで、国内のセキュリティ人材育成事業を活性化させる取り組みである。2024 年 12 月末時点の参加組織は 65 組織であった※211。いずれも前年の参加組織数から増加している。

(c) CYDER

「実践的サイバー防御演習（CYDER：Cyber Defense Exercise with Recurrence）」は、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。CYDER では、標的型攻撃、踏み台攻撃、ランサムウェア攻撃等、最近のサイバー攻撃事例に基づいた、リアリティのあるシナリオを使った演習が実施されており、自治体等のネットワーク環境を忠実に再現した仮想空間上で、受講者は実機を操作し、実際に手を動かしながら、ロールプレイ形式でインシデントハンドリングを体験できる。

2024 年度は初級（A コース）69 回、中級（B コース）32 回、準上級（C コース）5 回の集合演習を実施した。また 2023 年度下期より、オンラインによる、個人向け独習型の演習「プレ CYDER」を開講しており、「地方公立病院を襲うランサムウェア編」を 2024 年 5 月 21 日～ 7 月 19 日に※212、「たったひとつの冴えないパスワード編」を 2024 年 10 月 17 日～ 2025 年 1 月 31 日に開講した※213。基礎の基礎から学べ、最短 3 時間で受講が可能なこと、複数回に分けての受講が可能なことが特徴である。

(d) CIDLE

ナショナルサイバートレーニングセンターでは、2023 年度から 2024 年度にかけて、万博向けサイバー防御講習「CIDLE（Cyber Incident Defense Learning for EXPO）」を実施した※214。CIDLE は CYDER や東京 2020 オリンピック・パラリンピック競技大会の関連組織のセキュリティ担当者等を対象とした実践的サイバー演習「サイバーコロッセオ」の知見も活用して構成されたプログラムである※215。2025 年日本国際博覧会（大阪・関西万博）に向け、サイバーセキュリティを強化し安全な開催に資するよう、2023 年 9 月から関連組織の情報システム担当者等を対象として総務省・NICT により実施された。

(e) SecHack365

NICT が主催する「SecHack365」は、25 歳以下を対象に長期にわたるハッカソンによるモノづくりの機会を提供し、「セキュリティイノベーター」としてセキュリティの様々な課題にアイデアで切り込める人材の育成を目指すプログラムである。次の四つの能力を身に付けた人材の育成を目指し 2017 年度から実施している※216。

- 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などに形作る力
- サービスやプロダクト、システムを安全なものにする能力
- 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。2024 年度はキックオフを 6 月にオンラインで行った後、7 月に東京、9 月に広島、11 月に大阪で 2 泊 3 日のオフラインイベントが行われた※217。その後、2025 年 3 月 9 日にオフラインで成果発表会が行われ、6 作品が優秀作品として表彰された※218。

(f) SECCON

「SECCON（SECURITY CONTEST）」は、年間を通じ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。2012 年より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※219。目的は実践的情報セキュリティの人材発掘・育成、技術の実践の場の提供である※220。なお、SECCON の呼称がそれまでの西暦（例：SECCON2023）から連番になることが 2024 年 4 月に発表され※221、2024 年度の呼称は「SECCON 13」となった※222。「SECCON 13」の各プログラムの実施内容について紹介する。

- SECCON CTF
  CTF 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。予選大会「SECCON CTF 13 Quals」は 2024 年 11 月 23 ～ 24 日にオンラインで実施された。その後、国際部門と国内部門の 2 部門で構成される決勝大会「SECCON CTF 13 Finals」が、東京で開催された「SECCON 13 電脳会議※223」の会場において 2025 年 3 月 1 ～ 2 日に行われた。国際部門の出場条件は予選大会の上位 8 チーム、国内部門は日本在住のメンバーで構成されるチームのうち、上位 8 位（ただし、国際部門に出場できるチームを除く）であること等が定められて

いる※224。

- SECCON Beginners
  「SECCON Beginners」は日本国内のCTFプレイヤーを増やし、人材育成とセキュリティ技術の底上げを目的としたCTF未経験者向けの勉強会である。2024年度は初・中級者向けのオンラインCTFが2024年6月15～16日に開催されたほか、国内5ヵ所でワークショップが行われた※225。
- CTF for GIRLS
  「CTF for GIRLS」は、情報セキュリティ技術に興味がある女性を対象に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コミュニティである。2024年は8月にフォレンジック分野、12月にペネトレーション分野のワークショップを行ったほか、「SECCON 13電脳会議」の会場において、CTFのワークショップ、ハンズオン、交流会等を行った※226。
- SECCONCON
  「SECCONCON（SECCON Contests）」は、応募された競技やコンテストの企画案や設計案を実際に行うイベントである。2024年は4回目の開催となり11月にオンラインで行われた※227。

(g) 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※228。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。2024年度の同交流会は6月15日に定員60名で、東京大学本郷キャンパスで開催された※229。

COLUMN

「クラウドサービスのリスク」をどうやって把握する?

最近は、クラウドサービスを利用することが当たり前になってきました。一般的なオンプレミスの情報システムと比較すると、クラウドサービスを活用した場合のほうが、セキュリティ対策が十分行われていることも多い。とは言うものの、クラウドサービスにおいて、セキュリティインシデントや障害は発生していないのでしょうか? また、クラウドサービスのセキュリティ対策は十分であると断言できるでしょうか?

実際、グローバルなクラウドサービスの長時間のサービス停止や、広域での障害は、近年でも発生しています。また、国内や小規模クラウドサービスにおけるセキュリティインシデントも同様に発生しています。こうした現実がある中、クラウドサービスのセキュリティ対策状況を、利用者である我々はどうやって知ることができるのでしょう?

オンプレミスで情報システムを構築する場合のセキュリティ対策状況は、設置場所、建屋、設備、ハードウェア、仮想環境、OS、ミドルウェア、アプリのすべてを対象とし、それらを直接確認する情報セキュリティ監査により把握することができました。一方、クラウドサービス上に情報システムを構築した場合、一般的には、サービスの内部を直接確認することはできません。つまりは、クラウドサービスの中のセキュリティ対策状況は、「ブラックボックス」になっているわけです。

ブラックボックスに対しては、セキュリティ的観点から十分なリスクの判断ができません。これを解消するために、クラウドサービス事業者によっては、自らの情報セキュリティ対策状況を、米国公認会計士協会(AICPA)の標準であるSOC(Service Organization Control)2に基づいたレポートとして提供している場合があります。また、ISMAP(政府情報システムのためのセキュリティ評価制度)で認証されたクラウドサービスにおいては、対応するセキュリティ管理策、リスク評価を行うために必要な情報等が公開されています。

クラウドサービスを活用したシステム構築では、自ら設定・構築するOS、ミドルウェア、アプリは直接確認し、クラウドサービスについてはSOC2レポートやISMAP認証制度の公開情報等を確認して、クラウドサービスを含むセキュリティ対策の状況全体を把握する必要があります。情報セキュリティ監査だけでは、セキュリティインシデントや障害等を防ぐことはできませんが、情報セキュリティ監査を通じて情報システムのリスクを把握することにより、自らのリスクを適切に管理することができます。クラウドサービスの活用にあたっては、クラウドサービスのリスクを把握することが重要です。

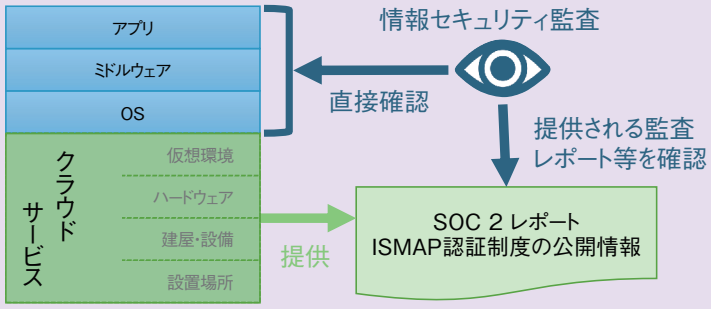


図　クラウドサービスを活用したシステム構築における情報セキュリティ監査

3.3 製品・サービスの評価・認証制度・暗号技術の動向

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

本節では、新たに開始した IoT 製品のセキュリティレベルを可視化する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」、IT 関連製品のセキュリティ機能の適切性・確実性をセキュリティ評価基準の国際標準である ISO/IEC 15408 に基づいて評価する「IT セキュリティ評価及び認証制度（JISEC）」、サプライチェーン強化に向けた対策評価制度構築に向けた検討、及び政府が求めるセキュリティ要求を満たしているクラウドサービスを評価・登録する「政府情報システムのためのセキュリティ評価制度（ISMAP）」の動向について報告する。また、電子政府システムでの利用を推奨する暗号アルゴリズムの安全性の評価・監視等を目的とし、デジタル庁、総務省、経済産業省、NICT、及び IPA が組織する CRYPTREC の動向についても報告する。

3.3.1 セキュリティ要件適合評価及びラベリング制度（JC-STAR）

2025 年 3 月から、IPA では IoT 製品のセキュリティレベルを可視化する「セキュリティ要件適合評価及びラベリング制度（JC-STAR：Labeling scheme based on Japan Cyber-Security Technical Assessment Requirements）※230」の運用を新たに開始した。JC-STAR は、IPA が運営する製品のセキュリティ機能等に対する評価制度としては、「IT セキュリティ評価及び認証制度（JISEC）」「暗号モジュール試験及び認証制度（JCMVP）」に次ぐ、三つ目の評価制度となる。なお、JC-STAR という名称及び同制度のロゴ（図 3-3-1）は、それぞれ第 6839291 号及び第 6910025 号として商標登録されている。

■図 3-3-1　JC-STAR ロゴ

本項では、JC-STAR が発足することとなった背景や制度概要、今後の取り組み等について解説する。

(1) JC-STAR 発足の背景

様々な IoT 製品がインターネットにつながることで便利なサービスが提供されるデジタル社会が実現している。実際、「情報通信白書令和 6 年版※231」に掲載された調査会社の予測によれば、世界の IoT 機器数は 2025 年に 462.9 億台に達すると見込まれている。

一方、IoT 製品を狙ったサイバー攻撃が増加しており、NICT が観測している NICTER（Network Incident analysis Center for Tactical Emergency Response）の観測レポート※232 によれば不審な通信のうち 3 分の 1 以上が IoT 機器を狙った攻撃に分類されている。これらの攻撃の結果として、マルウェアに感染した多くの IoT 機器が乗っ取られてボット化し、DDoS 攻撃によって社会システムを停止させるといった被害が現実化している。

初期の事例では、2016 年 10 月、米国で Twitter（現 X）や Spotify 等の著名なインターネットサービスへのアクセスに大規模な障害を生じさせた DDoS 攻撃が発生し、Mirai というマルウェアに感染した多数の IoT 機器によって構成されたボットネットが使用された攻撃であることが判明した※233。1 台の IoT 機器の攻撃能力はごく限られたものだが、IoT 製品が普及したことにより、多数の IoT 機器がボットネット化されると 500Gbps から 1Tbps に達するトラフィックを発生させ、社会インフラをダウンさせることができると証明された。その後も DDoS 攻撃にはボット化した IoT 機器が使われ続けており、日本でも 2024 年の年末から 2025 年の年始にかけて、航空業界や金融機関等に DDoS 攻撃の被害が出て、社会的な混乱を招いた（「1.2.3 (2) (a) 国内事業者向け攻撃の事例と手口」参照）。IPA の「情報セキュリティ 10 大脅威 2025※234」では、5 年ぶりに DDoS 攻撃がランクインしている。

ここでの問題は、「ボット化した IoT 機器」には、ホームルーター、ビデオレコーダー、ネットワークカメラ、ネット家電等を始めとして、身近で使われている IoT 機器が多く含まれていることである。このことは、IoT 製品の利用者はサイバー攻撃の「被害者」になるだけではなく、知らないうちに利用者自らが社会システムを停止させるサイバー攻撃の「加害者」の片棒を担ぐことになるかもしれない、ということを意味している。実際、マルウェアに感染し、

サイバー攻撃に加担してしまう危険性があるような、セキュリティ対策が十分に行われていない IoT 機器を観測し、注意喚起を行う「NOTICE※235」プロジェクトによれば、容易に推測可能な ID ／パスワードを使っている IoT 機器約 1 万 5,000 台、脆弱性が放置されたままの IoT 機器約 4,000 台、マルウェアに感染していると推定される IoT 機器約 1,000 ～ 1,500 台が発見されている。

本来、IoT 製品の利用者も IoT 製品のセキュリティ確保の役割の一翼を担っており、購入前に「十分なセキュリティ機能があるか」や「購入後のアップデートファイルの提供等のサポート体制がどのようになっているのか」を自ら確認し、利便性や価格だけでなく、セキュリティ対策も施されているかを考慮して IoT 製品を購入することが期待される。更に、購入後もその製品に脆弱性があれば、セキュリティアップデートの適用等への対処が求められる。

しかしこれまでは、IoT 製品の利用者がそのような情報を自ら確認することは難しく、どの IoT 製品のセキュリティ対策が適切なのか判断できなかった。また、セキュリティ対策を行った IoT 製品をベンダーが販売しても、セキュリティ対策の取り組みについて利用者にアピールすることが難しいという課題があった。加えて、最近では、IoT 製品のセキュリティ機能のみならず、サプライチェーン・リスク※236 管理の必要性も高まっている。

このような背景のもと、IoT 製品へのセキュリティ対策を進めるべく、米国、EU、シンガポール、英国等が IoT 製品のセキュリティ対策に関する評価制度の導入を進めており、日本でも経済産業省が 2022 年 11 月から「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※237」を発足させた。この検討会では、共通の物差しで IoT 製品のセキュリティ機能を評価・可視化し、適切なセキュリティ対策が講じられている IoT 製品が広まる仕組みの構築に向けた報告書を取りまとめた。その後、パブリックコメントの結果を踏まえ、2024 年 8 月に「IoT 製品に対するセキュリティ適合性評価制度構築方針※238」が公表された。

IPA では、上記の制度構築方針に基づき、JC-STAR の発足準備を進め、2025 年 3 月 25 日に「★ 1 適合ラベル」取得の申請受付※239 を開始した。その後、「★ 1 適合ラベル」の交付を開始し、同年 5 月 21 日に最初の「適合ラベル取得製品リスト※240」を公開した。なお、「★ 1 適合ラベル」は、IoT 製品共通の最低限の脅威に対応するための基準として設けられた適合基準を満たすことを、ベンダーが自己宣言した IoT 製品に対して交付されるものである。

(2) IoT 製品のセキュリティリスクが放置される理由と対処

インターネットに接続する以上、IoT 製品も IT 製品と同様のセキュリティリスクがある。しかし、以下のような IoT 製品特有の要因によって、セキュリティリスクが放置されたままになってしまうことが考えられる。

- IT 製品と異なり、IoT 製品に備わっているセキュリティ機能とは別のセキュリティ機能を独自に追加して利用することができない。
- IoT 製品が持つリソースが少なく、十分なセキュリティ機能を実装することができない。
- インターネットに簡単につながらないことのほうが利用者の不満に直結しやすいため、簡単にインターネット接続できるように初期設定では簡易なアクセス制御／ログイン管理機能しか提供していない。
- もともとはインターネットに接続することが想定されずに設計・製造されていた製品に対して、オプションとして、あるいは新機能としてインターネットに接続できるようにしたケースでは、インターネットに接続する際のセキュリティリスクに関する検討が不十分な攻撃対象領域（アタックサーフェス）が残ったまま発売されてしまうことがある。
- 利用者が想定しない機能（場合によってはベンダー自身も把握していない機能）が初期設定で有効になっており、想定外のデータのやり取りがあっても分からない。
- 設定ミスやマルウェア感染、不正アクセスといった問題が発生していても、IoT 製品の基本機能（例えば、エアコンなら空調機能、カメラなら撮影機能、テレビなら受信機能）としては正常に動作し、物理的な異常が見られない場合には、そもそも問題が発生していることに気が付きにくい。
- IoT 製品の明確な管理担当者等はおらず、一度設置されると、故障等が生じない限り、長期間メンテナンスされることなく使われ続け、発見された脆弱性に対する修正プログラムさえも適用されない。
- ベンダーがいつまでサポートするのかがはっきりせず、発見された脆弱性に対してアップデートファイルがそもそも作られないことがある。
- サポート期間が終了し、発見された脆弱性に対するアップデートファイルが提供されなくなってもそのまま使われ続ける。
- IoT 製品に記録されたデータの廃棄手順がはっきりしない。

こういったセキュリティリスクに対処するために、ベン

ダーにはIoT製品の設計段階からセキュリティを考慮（セキュア・バイ・デザイン）し、運用・保守フェーズを含むIoT製品のライフサイクルを通じた対策が求められる。例えば、IoT機器を開発する企業向けの「IoT機器を開発する中小企業向け製品セキュリティ対策ガイド※241」が参考になる。

IoT製品のセキュリティがほぼ評価されずに調達されることが多い現状を踏まえ、JC-STARに期待されることは、適切なセキュリティ対策が講じられたIoT製品を適合ラベルの交付により可視化し、それを目印に調達してもらうことでIoT製品のセキュリティ向上を図ることである。

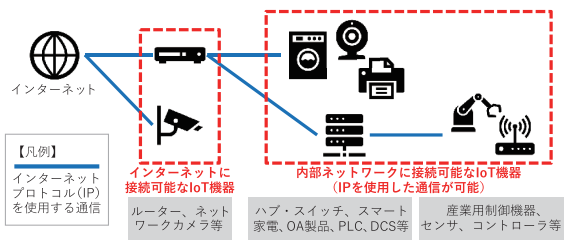
(3) JC-STARの概要

JC-STARは、インターネットと通信が行える幅広いIoT製品を対象として、共通的な物差しでその製品のセキュリティレベルを可視化することを目的としている。

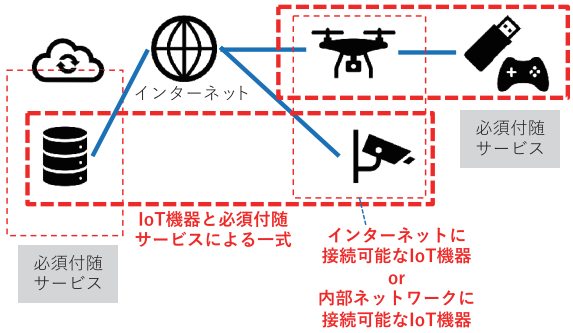
具体的な対象範囲は、以下の4条件を満たすIoT製品である。簡単に言えば、「インターネットの世界とつながり、インターネット側からの通信を受けるIoT製品のうち、その製品のベンダーが提供するセキュリティ機能のみが利用できるIoT製品」ということである（図3-3-2）。

①機器が含まれている（クラウドサービスやソフトウェアといったものは単体では対象外）。
②インターネットプロトコルを使用したデータ送受信（IP通信）ができる機能を有する。
③直接・間接を問わず、インターネットにつながる（可能性がある／否定できない場合を含む）。
④購入時にその IoT 製品に搭載されているセキュリティ機能を利用し、アップデート以外で（調達者・利用者が自らの意志で）後から別のセキュリティ機能を追加することが困難である。

また、IoT製品が意図した目的を提供するために、IoT機器と一体で提供することが必須となるデジタルサービスを「必須付随サービス」と呼び、これも適合ラベルの



■図3-3-2　JC-STARの対象製品例
（出典）IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報※242」



■図3-3-3　JC-STARの対象製品例（必須付随サービスを有するもの）
（出典）IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」

対象となる（図3-3-3）。

パソコン等のように後からセキュリティソフトを入れる等、セキュリティ対策を後から追加できるものについては別途セキュリティ対策を検討してもらえばよいのに対して、IoT製品ではあらかじめその製品が備えるセキュリティ機能を使うしか利用者には選択肢がない以上、必要なセキュリティ機能はベンダーの責任において提供すべきというのが、このような対象範囲を定めた理由である。

一方、セキュリティ機能の提供には相応のコストがかかり、最終的にはベンダーだけでなく購入者にも一定の負担をしてもらう以上、むやみに高いコストをかけられない。そこで、JC-STARでは求められるセキュリティ水準に応じた4段階（「★1」（レベル1）～「★4」（レベル4））の適合基準を設定している。

適合基準を満たしたIoT製品は、その基準に応じた適合ラベルを取得することができる。この適合ラベルは、機器本体やパッケージ、ホームページ等に表示することができ、IoT製品のセキュリティ対策のアピールに利用できる。

(a) 適合基準について

JC-STARでは、適合ラベルを取得するために求められるセキュリティ水準に応じたセキュリティ要件として、以下の合計4段階の適合基準を設けており、レベルが上がる程、高度なセキュリティ要件となる。

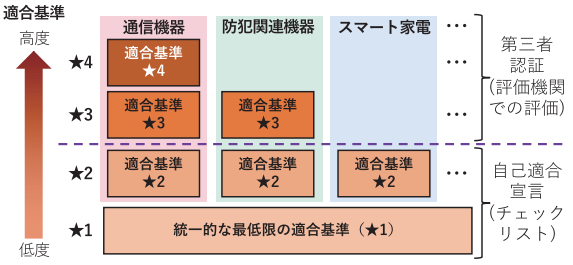
- 最低限の脅威に対抗するための製品共通の適合基準である「★1」
- IoT製品類型ごとの特徴に応じた適合基準である「★2」「★3」「★4」

これらの適合基準は、日本独自に定めたセキュリティ要件に基づく基準となっているが、将来的な相互承認の実現を見据えてETSI EN 303 645※243、NIST IR

8425※244、EU CRA（Cyber Resilience Act※245）等の国内外のセキュリティ要件等とも調和するように配慮している。

具体的には、各レベル・製品類型ごとに想定される脅威や保護すべき情報資産等を考慮し、その脅威に対抗するためにIoT製品のセキュリティ機能として具備すべきセキュリティ要件を設定している。製品類型、想定されるセキュリティ脅威や保護すべき情報資産等の違いにより、求められるセキュリティ要件が異なり、適合基準のレベルが高くなる程、求められるセキュリティ要件のレベルが高くなる。

「★1」と「★2」の適合基準は主に民間の利用を想定しており、「★3」と「★4」の適合基準は主に政府機関や重要インフラ、地方自治体等の高いセキュリティが必要なシステムでの利用を想定している。購入者は、自身が求めるセキュリティ水準に適した適合基準のラベルが交付された製品を優先的に選択することが期待される。なお、高い適合基準を選ぶことが必要、あるいは、最良であるということは必ずしもなく、利用環境や利用目的に応じて、想定すべき脅威が考慮された適切な水準の適合基準を選択することが重要である（図3-3-4、表3-3-1）。



■図3-3-4　適合基準
（出典）IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」

レベル	位置付け
★4	政府機関や重要インフラ事業者、地方公共団体、大企業等の重要なシステムでの利用を想定した製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを独立した第三者が評価して示すもの
★3	
★2	製品類型ごとの特徴を考慮し、「★1」に追加すべき基本的なセキュリティ要件を定め、それを満たすことをベンダーが自ら宣言するもの
★1	製品として共通して求められる最低限のセキュリティ要件を定め、それを満たすことをベンダーが自ら宣言するもの

■表3-3-1　適合基準のレベルとその位置付け

「★1」では、最低限の脅威に対抗するために、主に以下の事項を実現することを目指している。

- マルウェアに感染してボット化するのを防ぐ。とりわけ、感染した機器からの感染拡大を防止する。
- インターネット経由の遠隔攻撃を想定し、スクリプトキディレベル（限定的な専門知識のみを有し、インターネットやダークウェブ等で公開されているクラックツール等を用いてシステムの脆弱性を利用して攻撃するレベル）の攻撃に対して実用的な耐性を持たせる。
- 製品不具合や脆弱性に対する対応・サポート方針を明確化し、適合ラベル有効期間内のサポート（アップデートファイルの提供等）が確実に実施されるようにする。
- 廃棄前に、運用中に生成されたデータを適切に削除することができる。

また、「★1」の適合基準への評価はチェックリストや評価ガイドを用いてベンダーが低コストで自己評価可能なレベルとする一方、海外制度と国際連携可能な要件とすることを踏まえ、表3-3-2（次ページ）に示す16個の適合基準（(1)～(16)）が定められた。

(b) 適合ラベルについて

適合ラベルは、IoT製品があらかじめ備えるセキュリティ機能が定められたセキュリティ要件（適合基準）に適合していることを示す目印として交付される。適合ラベルを取得したIoT製品には、製品本体（筐体）、パッケージ、マニュアル、パンフレット、ホームページ等に適合ラベルを記載・貼付・使用することで、セキュリティ対策の取り組みを購入者にアピールすることができる。

なお、適合ラベルの有効期間は2年を基本とし、延長申請が可能である。また、適合ラベルの有効期間内はアップデートファイルの提供等のサポートが義務付けられている。

適合ラベルには、IoT製品が取得した適合基準のレベルと登録番号のほか、そのIoT製品情報を確認するため、IPAが管理する「適合ラベル取得製品情報ページ」（以下、製品情報ページ）のURLを埋め込んだ二次元コードが組み込まれている（次ページ図3-3-5）。この製品情報ページは登録番号ごとに用意されており、「適合ラベル取得製品リスト」から表示できる。

製品情報ページでは、適合ラベルが交付されたIoT製品に対して、申請者情報、製品情報、適合ラベル情報、セキュリティ情報（アップデート情報や脆弱性情報等）、サポート期間、問い合わせ先情報等を最新の状態に維持しながら、一元的に提供できる仕組みを取り入れている。これにより、いつまでそのIoT製品を安全に使えるかが分かり、またIoT製品利用中のセキュリティ

★1で考慮する主な脅威			脅威に対抗するために★1で求める適合基準			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づくアクセス制御 (2)容易に推測可能なデフォルトパスワードの禁止 (3)パスワード等の認証値の変更機能 (4)ネットワーク経由のユーザ認証に対する総当たり攻撃からの保護	情報提供	(16)ユーザへのセキュアな利用・廃棄方法に関する情報提供(初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等)
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6)ソフトウェアコンポーネントのアップデート機能 (7)容易かつ分かりやすいアップデート手順 (8)アップデート前のソフトウェアの完全性の確認機能 (10)ユーザが製品型番を認識可能とする記載・機能	情報・問合せの受付、情報提供	(5)連絡先・手続き等の脆弱性開示ポリシーの公開 (9)セキュリティアップデートの優先度決定方針の文書化
	③未使用インタフェースの有効化により、		インタフェースへの論理アクセス	(13)不要かつリスクの高いインタフェースの無効化(物理的・論理的な通信ポート等)	―	―
	①～③共通		データ保護	(11)製品に保存される守るべき情報の保護(保存データの暗号化、物理的保護による保存、OSセキュア管理等)	―	―
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12)ネットワーク経由で伝送される守るべき情報の保護(通信の暗号化、保護された通信環境の利用等)	―	―
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15)製品内に保存される守るべき情報の削除機能 ※(11)も含む	情報提供	※(16)に含む
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンス向上	(14)停電・ネットワーク停止等からの復旧時の認証情報やソフトウェア設定の維持(初期状態に戻らないこと)	―	―

■表3-3-2 ★1の適合基準
(出典)IPA「IoT製品のセキュリティ確保に向けて※246」

■図3-3-5 適合ラベルの例

対策やトラブル発生時等の対処がしやすくなることが期待される。

更に、製品情報ページの「適合ラベル情報」の「適合ラベルステータス」では、市場に長期間流通しているIoT製品についても、その時点の適合ラベルの状態をリアルタイムで確認できる(次ページ表3-3-3)。

(c)適合ラベルの取得スキーム

JC-STARでは、適合基準で定めた要件を実際に満たしているかどうかを具体的に判断するための評価手順(評価手法・評価ガイド)が用意されている。適合基準と評価手順は1対1の関係にあり、この評価手順に従って適合基準への適合性を確認する必要がある。

この評価手順を使って、「★1」と「★2」では、ベンダーが自己適合宣言、すなわちチェックリストにより適合性を確認し、すべての要件を満たしていると判定した場合、適合ラベルの申請を行うことができる。その申請がIPAに受理されると、そのIoT製品に対して適合ラベルが交付される。これにより、評価の信頼性はベンダーの信

ステータス	説明
有効	適合ラベルが有効期間内にあり、失効・取り消しに該当する事由がない状態
失効猶予（延長申請中）	適合ラベルの有効期間が満了しているが、有効期間の延長申請手続きが行われている状態
失効（有効期限切れ）	適合ラベルの有効期間が満了した後、有効期間の延長が行われていない状態
失効（自主取下げ）	適合ラベルの有効期間内に、IoT 製品ベンダーからの申し出により、適合ラベルの効力を失効させた状態
取消し	適合ラベルの有効期間内に、適合ラベルの取り消し事由に該当する事象が発生し、定められた期間内にその事由を解消するための是正がなされなかった場合に、IPA が強制的に適合ラベルの効力を停止させた状態

■表 3-3-3　適合ラベルのステータス

頼性に依存することになるが、低コストかつ短期間で適合ラベルを取得することができる。

なお、適合ラベルの交付にあたり、IPA はチェックリストの評価結果の根拠となる証跡の提出は求めておらず、評価結果の内容が正しいかどうかを IPA が自ら確認するものではないことに留意する必要がある。その代わり、適合ラベルの有効期間中は証跡の保管をベンダーに課しており、疑義が生じた場合に、事後的に IPA がサーベイランス（検査）を実施し、証跡等の提出を要求できる。その結果次第で適合ラベルの取り消しもあり得る仕組みを導入することで信頼性のバランスを取っている。

一方、高い信頼性が求められる「★ 3」と「★ 4」では、独立した評価機関が評価手順に従って適合性を評価し、その結果を IPA が認証するという第三者評価・認証方式により、適合ラベルが交付される（図 3-3-6）。「IT セキュリティ評価及び認証制度（JISEC）」に基づくコモンクライテリア認証とほぼ同様の考え方で運営される。

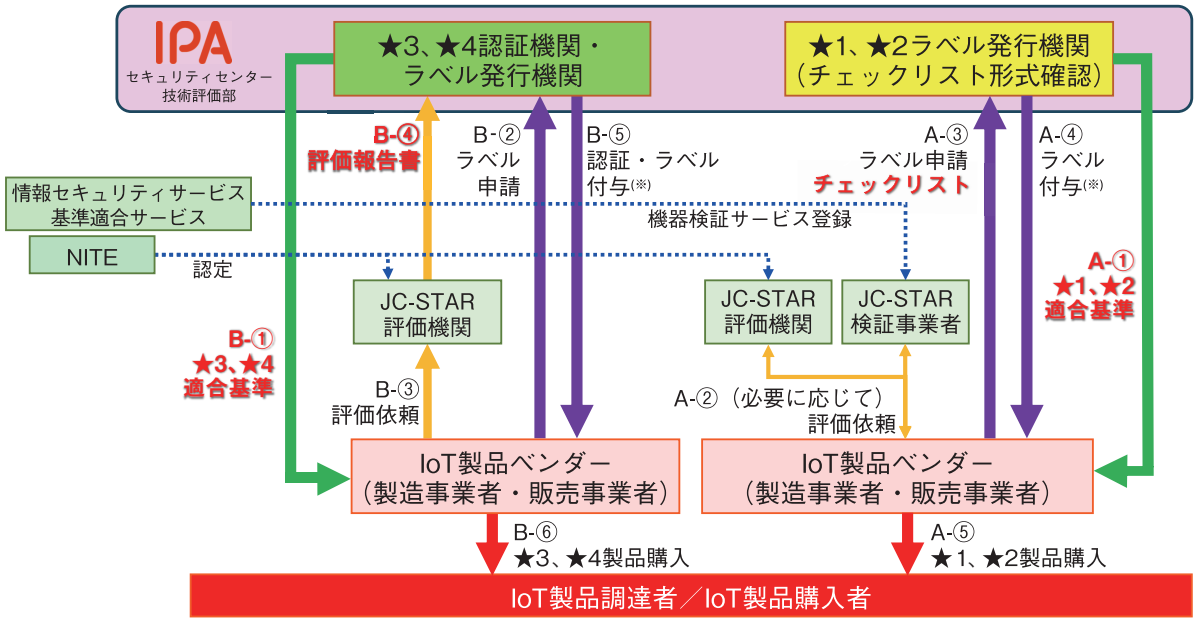
(4) JC-STAR 活用に向けた今後の取り組み

「★ 1 適合ラベル」の交付が始まり、今後もラベルを取得した IoT 製品が「適合ラベル取得製品リスト」に順次追加される。これにより、IoT 製品に求められる「★ 1」のセキュリティ要件を満たしていることを示す「★ 1 適合ラベル」が貼付された IoT 製品が実際に市場投入されることになる。

今後もベンダーが多くの IoT 製品で適合ラベルの取得を望むような環境を整備していくことと併せて、調達者や利用者に対してパンフレット、ポスター等で JC-STAR の意義を分かりやすく伝え、IoT 製品を購入する際は少なくとも「★ 1 適合ラベル」を取得した製品を購入してもらうように賛同団体等とともにプロモーション活動をしていく予定である。

(a) 調達要件での活用に関する調整

政府機関、重要インフラ事業者、地方公共団体等の社会的にセキュリティリスクが高いシステムを扱う組織における IoT 製品の調達要件に、JC-STAR の適合ラベ



(※) IPAは、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスクについて経済産業省を含めた政府関係機関に照会をかけ、その照会結果に基づきラベルを付与する。

■図 3-3-6　JC-STAR 適合ラベルの取得スキーム
（出典）IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」を基に編集

ル取得製品の選定を含めるよう経済産業省等が働きかけている。2025 年 5 月時点で、以下の文書に JC-STAR 活用に関する記載がある。

- 「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）」の一部改定（2024 年 7 月）※18 の「4.3.1 機器等の調達」
- 「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 7 年 3 月版）※247」の第 2 章「6.3. システム開発、導入、保守等」
- 「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver3.0※248」の「3.4. ERAB システムが維持すべきサービスレベル」「3.6. ERAB システムにおけるサイバーセキュリティ対策」

経済産業省はまた、重要インフラ事業者に対する施策として、「重要インフラのサイバーセキュリティに係る行動計画」に基づく「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、調達製品への要求事項の策定及び調達時の確認を明示した上で、「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※249」に詳細な記載を追加する方向で調整を進める予定である。

(b) 適合基準の拡張

IoT 製品類型ごとの特徴に応じたより高度な適合基準（「★ 2」以上）については、政府調達での活用が見込まれるネットワークカメラと通信機器の二つの製品類型を対象に、IPA に設置された適合基準検討ワーキンググループにより整備が進められており、2026 年 1 月以降に当該製品分野の「★ 2」以上の受付を開始する予定である。また、スマートホーム関連機器に対する「★ 2」等、その他の製品類型の「★ 2」以上の適合基準も順次整備し、制度を拡張していく計画である。

(c) 諸外国制度との相互承認に向けた調整

諸外国における IoT 製品の適合性評価制度の動向（表 3-3-4）も踏まえ、各国の制度との連携を図り、相互承認に向けた交渉を経済産業省と IPA は行っている。これにより、IoT 製品を海外に輸出する際に求められる適合性評価にかかるベンダーの負担軽減が期待される。

現在、シンガポール（Cybersecurity Labelling Scheme※250）、英国（PSTI 法※251）、米国（U.S. Cyber

国・地域	シンガポール	英国	米国	EU
制度名	Cybersecurity Labelling Scheme (CLS)	Product Security & Telecommunication Infrastructure Act（PSTI 法）	U.S. Cyber Trust Mark	Cyber Resilience Act（CRA）
マーク	CYBERSECURITY LABEL REGISTRATION ID: CSA/IOTWABCD MORE INFO AT: www.csa.gov.sg/cls	ステッカーのみ	U.S. CYBER TRUST MARK	CE
開始時期	2020 年 10 月開始	2024 年 4 月施行	2025 年より基準策定開始（制度開始時期調整中）	・報告義務 :2026 年 9 月 ・その他 :2027 年 12 月
任意/義務	任意	義務	任意	義務
対象	消費者向け IoT 機器	消費者向け IoT 製品	消費者用無線 IoT 製品	デジタル要素を含む製品
適合基準	・＊1：ETSI EN 303 645 の基準の一部 ・＊2：ETSI EN 303 645 のすべての必須要件に基づく基準 ・＊3及び＊4:＊2の基準に加え、IMDA「IoT Cyber Security Guide」の基準	ETSI EN 303 645の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	NISTIR 8425をベースとした基準となる見込み	・製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」「上市後の積極的に悪用された脆弱性・インシデントの報告」等を義務付ける予定
評価方法	・＊1 及び＊2：自己適合宣言 ・＊3 及び＊4：自己適合宣言及び評価機関による試験	自己適合宣言	第三者認証	・「重要なデジタル製品」以外の製品：自己適合宣言 ・「重要なデジタル製品」のクラスⅠ（EUCC や EN 規格の対象外の製品を除く）及びクラスⅡの製品：第三者認証

■表 3-3-4　諸外国の IoT 適合性評価制度
（出典）IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」を基に編集

Trust Mark[※252])、EU(CRA)等の各国担当機関との間で交渉を行っている。また、日米(首脳級)、日EU(閣僚級)、G7(首脳級)等において、相互承認に向けて取り組む旨を合意している。

進捗状況としては、英国とは具体的な相互承認のやり方を含めた交渉を行っている段階である。それ以外の国・地域についても、基準策定の方針に関する認識合わせなど、相互認証に向けた前向きな協議を進めている。

(d)業界団体・賛同団体との連携

経済産業省は2025年3月、「特定分野システムのIoT製品におけるJC-STAR制度活用ガイド(1.1版)[※253]」を公開した。同ガイドは、特定分野システム(特定の分野や業界において類似の汎用的な構成で利用されるシステム)にて調達・利用されるIoT製品に対して、実質的な業界標準としてのセキュリティ要件を定め、それをJC-STARにおける適合基準として整備することで、適合ラベル取得製品の供給と調達のエコシステム構築を促し、当該分野でのセキュリティの確保に貢献することを目的としている。特定分野システムの例として、スマートホームシステム、工場システム、ビルシステムが挙げられている。

このほかにも、各業界団体やIoT製品ベンダーも参画し、JC-STARとの連携や会員企業への積極的な適合ラベル取得の働きかけを行うことに賛同している「賛同団体」が5団体ある(五十音順)。

- 一般社団法人情報通信ネットワーク産業協会(CIAJ:Communications and Information network Association of Japan)
- 一般社団法人デジタルライフ推進協会(DLPA:Digital Life Promotion Association)
- 一般社団法人電子情報技術産業協会(JEITA:Japan Electronics and Information Technology Industries Association)
- 公益社団法人日本防犯設備協会(JSSA:Japan Security Systems Association)
- 一般社団法人ビジネス機械・情報システム産業協会(JBMIA:Japan Business Machine and Information System Industries Association)

例えば、JBMIAが運営しているBMSec(事務機セキュリティプログラム)については、2025年10月以降JC-STARへ制度統合することが発表されている[※254]。

3.3.2 ITセキュリティ評価及び認証制度(JISEC)

IT製品が政府調達におけるセキュリティ要件を満たすことを確認する仕組みとして、セキュリティ評価制度が欧米諸国を中心に発展し、セキュリティ評価基準が国際標準ISO/IEC 15408として策定された。日本でも、このセキュリティ評価基準を用いてIT製品を評価する「ITセキュリティ評価及び認証制度(JISEC:Japan Information Technology Security Evaluation and Certification Scheme)[※255]」をIPAが運営し、政府機関等のIT製品調達に活用されている。

本項ではJISECの動向や認証制度の国際連携について解説する。

(1)政府のIT製品調達におけるセキュリティ要件

サイバーセキュリティ戦略本部が発行している「政府機関等のサイバーセキュリティ対策のための統一基準(令和5年度版)[※17]」(以下、政府統一基準)では、府省庁及び独立行政法人等の情報システムセキュリティ責任者に対し、情報システムを構成するIT製品を調達する場合、経済産業省が発行している「IT製品の調達におけるセキュリティ要件リスト[※256]」(以下、調達要件リスト)を参照し、想定されるセキュリティ上の脅威に対抗するためのセキュリティ要件を策定することが遵守事項として定められた。

調達要件リストでは、対象製品分野のIT製品がセキュリティ要件を満たすことを確認する方法として、調達時に受け入れテスト等で確認する方法と、国際標準に基づく認証取得を確認する方法があることを示している。JISECは、ISO/IEC 15408に基づく第三者認証制度であり、JISECで認証されたセキュリティ要件を満たすIT製品を調達することで、政府統一基準の要求を満たすことができる。

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

(2)認証制度の国際連携

JISECでも採用しているセキュリティ評価基準であるISO/IEC 15408は、欧米6ヵ国によるコモンクライテリア(共通基準)プロジェクトの成果をベースに開発された。

また、これらの国々を代表する公的機関が運営する制度でコモンクライテリアを用いて評価された結果については相互に認め合うという相互承認協定が締結された。これによりIT製品のベンダーは、調達国ごとに重複したセキュリティ評価や認証を受けることなく、製品を国際的に展開できるようになっている。

相互承認協定は、その後、多くの国が加盟し、現在ではCCRA（Common Criteria Recognition Arrangement）と呼ばれている※257。CCRAでは、自国で認証制度を運営している「認証国」と、認証制度を有しないが政府調達要件として認証結果を受け入れる「受入国」がある。2024年にベルギーとヨルダンが受入国としてCCRAに加盟し、2025年3月末現在、CCRA加盟国は認証国18ヵ国、受入国15ヵ国の計33ヵ国に上る（図3-3-7）。

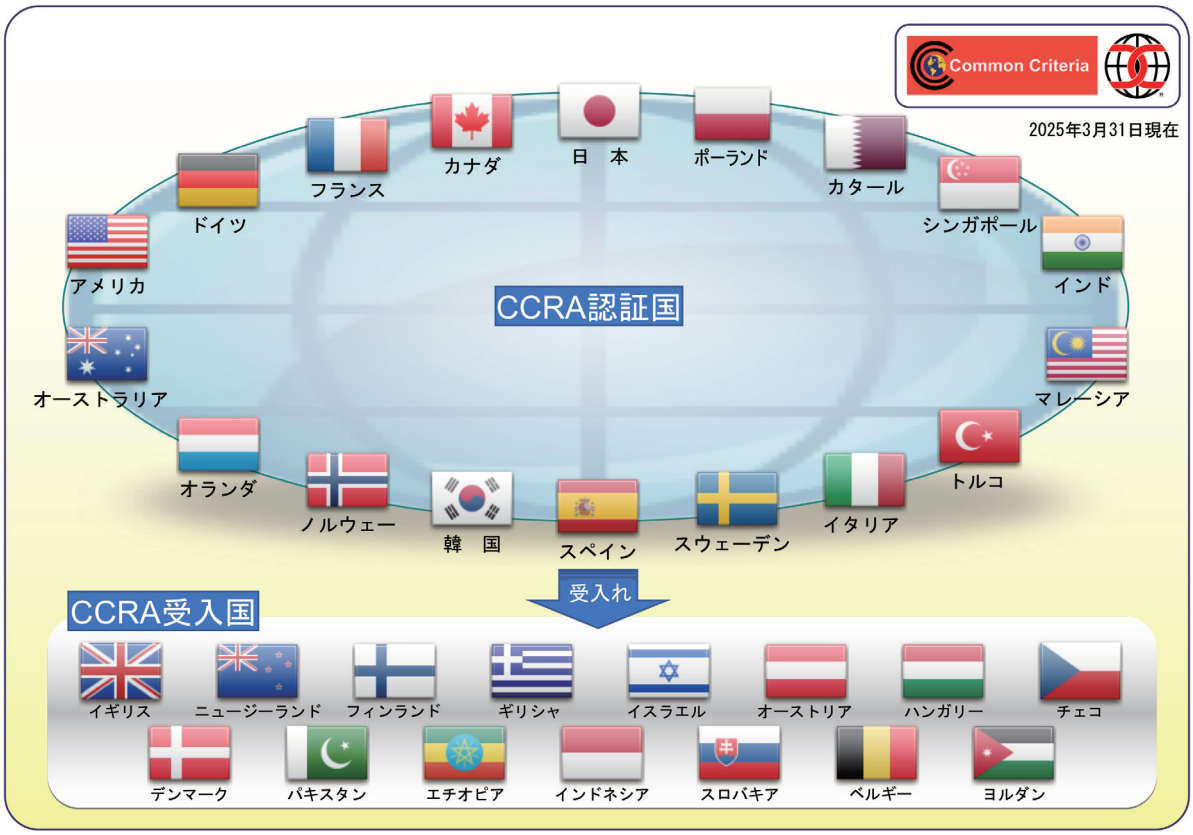
JISECを運営する日本も2003年にCCRAに認証国として加盟している。これにより、日本のベンダーはJISECを活用することで、日本語の開発資料をそのまま使用してIT製品の認証を取得することができ、かつそのIT製品がCCRA加盟国の調達対象として認められるようになっている。

また日本は2025年3月現在、CCRAの管理運営上の重要事項を議論する意思決定機関である運営委員会（MC：Management Committee）の議長国となっており、認証制度の国際連携の推進に努めている。

(3) セキュリティ要件の共通化

コモンクライテリアでは、IT製品が具備すべきセキュリティ要件を、規定された形式に従って記述することを定めている。中でも、アクセス制御機能や監査機能等、必要なセキュリティ機能の要件をテンプレート化して表現することにより、調達者が必要としているIT製品のセキュリティ要件仕様を、あいまいさを排除して製品開発者に伝えることが可能になる。このコモンクライテリア形式で表された調達要件仕様書は「プロテクションプロファイル（PP：Protection Profile）」と呼ばれている。

プロテクションプロファイルはCCRA加盟国でIT製品の政府調達要件として利用されている。プロテクションプロファイルのうち汎用的なものは、CCRAのポータルサイト※258にも掲載され、政府機関以外の機関でも同様の分野の製品を調達する際に調達要件として指定することができる。日本においても、調達要件リストでは製品分野ごとにこれらのプロテクションプロファイルを指定している。また、調達要件リストに含まれていない独自の製品



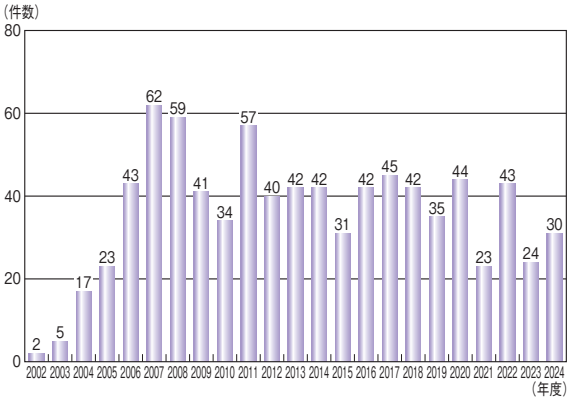
■図3-3-7　CCRA加盟国

を調達する機関は、プロテクションプロファイルを自ら作成し※259、調達を実施することもある。

同じ製品分野のIT製品調達で、複数の調達者から似ているが完全には一致していないプロテクションプロファイルが調達要件として指定されることは、別の認証として取り直す必要があることを意味し、ベンダーにとっては大きな負担となる。また、重複した評価や認証を繰り返す労力を省くというCCRAの目的にも合致しない。そこでCCRAでは、いくつかの製品分野で、加盟国の認証機関が中心となり、対象製品分野のベンダーや有識者を含む国際的な技術コミュニティを組織し、世界共通のプロテクションプロファイル「cPP（collaborative Protection Profile）」の策定を行っている。既にファイアウォール、ドライブ全体暗号化システム、ネットワークデバイス、バイオメトリクス認証、データベース管理システムやデジタル複合機等の製品分野についてcPPが策定され、CCRAポータルサイトで公開されている。

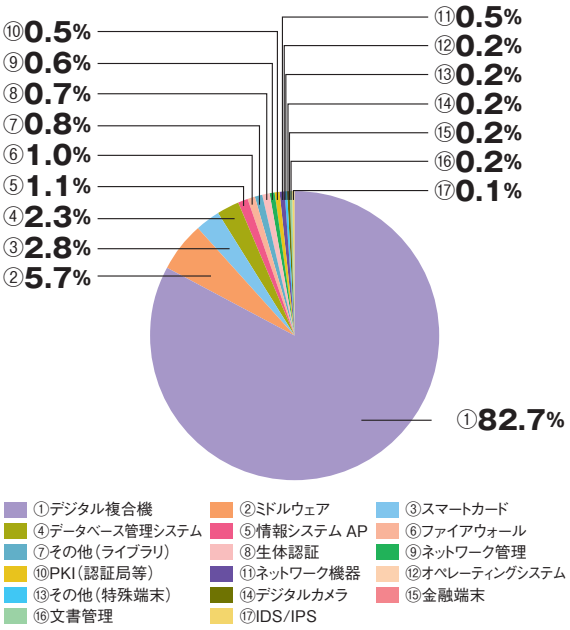
(4) 認証の状況

2024年度までのJISECにおける認証発行件数の推移を図3-3-8に示す。2024年度の認証発行件数は30件であり、2020年以降の年度別の認証発行件数は40件以上または30件以下と、年度によって大きな差がある。2019年以前は認証発行までに1年以上要する製品もあり、年度別で見ると認証発行件数は平準化されていた。近年は短期間での認証発行が実現していることもあり、製品開発サイクルの影響が認証発行件数に表れるようになってきており、年度の違いで認証発行件数が大きく増減する状況が生じている。



■図3-3-8　JISECの認証発行件数の推移

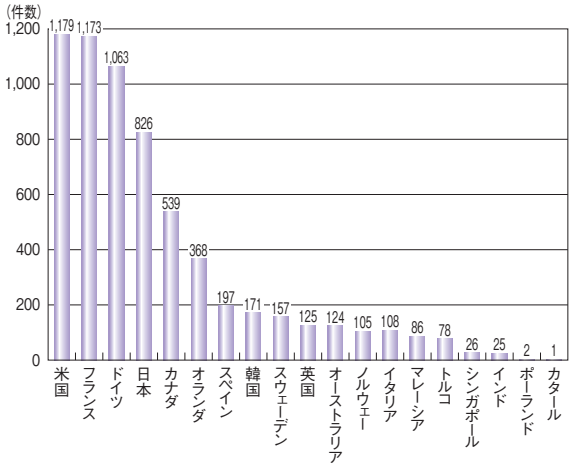
JISECにおける累計の認証発行件数の製品分野別の割合を図3-3-9に示す。認証製品分野としては、デジタル複合機が認証発行件数の8割以上を占め圧倒的に多い。これは日本のデジタル複合機ベンダーが国際的にも高いシェアを有し、CCRA加盟国においても政府調達の対象となっているからである。また、それ以外の製品分野の認証発行件数がJISECで少ないのは、セキュリティ製品全般において日本のベンダーの国際的な競争力が弱いこと、ファイアウォールやネットワーク管理製品等はシステム構築の中で組み込まれてテストされ納入されることが多いため、製品単品での調達要件の対象とならないこと等が理由である。JISECが毎年発行している認証のほとんどはデジタル複合機の新機種リリースによるものである。



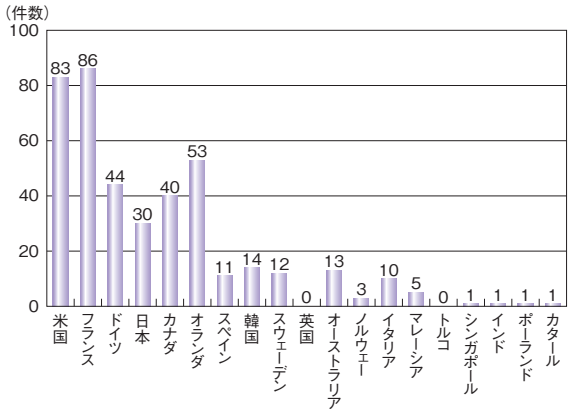
■図3-3-9　JISECの認証発行件数の製品分野別割合

CCRA加盟各国の認証機関が公開している認証発行件数の2024年度までの累計を図3-3-10（次ページ）に示す。日本の累計認証発行件数は、米国、フランス、ドイツに次いで4番目に多い。これら4ヵ国は、政府調達に認証製品を活用しているのに加えて、国内にIT製品の製造ベンダーを多く持つ国々である。近年は、新しい認証機関が設立されたオランダの認証発行件数が大きく増加しており、2024年度のオランダの認証発行件数は、フランス（86件）、米国（83件）に次ぐ3番目の53件となっている（次ページ図3-3-11）。

一方、英国のように、セキュリティ評価の歴史が長い国でも、国内の製造ベンダーの減少による制度維持コストの削減を理由に認証国から受入国に移行している国もある。韓国では、国際的に大きな市場を持つ製造ベンダーが、製品仕向地によりモバイル製品は米国で、スマー



■図 3-3-10　CCRA 各国の累計認証発行件数



■図 3-3-11　CCRA 各国の認証発行件数（2024 年度）

トカード関連製品はヨーロッパで認証を取得しているため、国内制度での認証発行件数は少ない。

(5) 2024 年度のトピック（CCRA 定期審査の受審）

JISEC に対する CCRA の定期審査が 2024 年 12 月 16 日から 12 月 20 日にわたり IPA にて行われた。CCRA では、加盟国の認証機関が CCRA の要求事項を満たしているかを確認するため、各国の認証機関が互いに審査員を派遣し、定期審査が行われることになっている。前回の JISEC に対する定期審査は 2015 年であり、新型コロナウイルスの流行により審査が延期となったこともあり 9 年ぶり 3 回目の定期審査となった。

今回の定期審査は、審査員として米国、マレーシアの認証機関から各 2 名、オブザーバーとしてインド、シンガポールの認証機関から各 2 名、合計 8 名が来日して実施され、認証制度の規程、認証員の技術的能力、運営状況等が CCRA の要求事項に適合していることが確認された。2025 年 3 月の CCRA 会合を経て、CCRA 加盟各国より認証国として継続承認を得た。

3.3.3 サプライチェーン強化に向けた対策評価制度構築に向けた検討

経済産業省が主催する産業サイバーセキュリティ研究会において、現在検討が進められているサプライチェーン強化に向けた対策評価制度について、中間取りまとめ※260 及び経済産業省及び NISC のプレスリリース※261 を基に紹介する。

(1) 制度構築の背景

近年、業務委託先がサイバー攻撃を受け、顧客情報が漏えいしたり、システムが停止したりすることにより、事業継続に大きな影響が及ぶ事案が発生している※262。IPA による「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」では、2023 年度にサイバーインシデントの被害に遭ったと回答した企業のうち、約 7 割がサイバーインシデントにより取引先に影響があったと回答した。大企業のみならず中小企業においても、商流において多くの取引先を持ち、サプライチェーンを形成している。そのうちの 1 社がサイバー攻撃を受けた場合、前述のような被害を他社に及ぼす可能性がある。しかし、業務委託先が適切なセキュリティ対策を講じているのかを委託元が確認することは容易ではない。また、業務委託先では、各社から様々なセキュリティ対策を要求されることが、特にリソースが限られる中小企業では過度な負担となっており、サプライチェーン全体でのセキュリティ向上につながっていないことが課題となっている。

経済産業省及び NISC では、前述の課題解決に向け、産業サイバーセキュリティ研究会において、「サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ」を設置、2024 年 7 月に第 1 回を開催し、2025 年 4 月開催の第 5 回まで議論を重ね、検討を行った※263。この検討の結果は 2025 年 4 月 14 日に「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ※260」として公表された。

(2) 制度の目的

こうした状況の中、前記の中間取りまとめでは、委託元、委託先双方にとって適切なセキュリティ対策の決定及び実施と、実施しているセキュリティ対策の可視化が必要であるとし、サプライチェーンにおいて想定されるリスクに対して、立ち位置に応じた対策を、サプライチェーン強化に向けた対策評価制度で提示することで、企業

のセキュリティ対策の決定を容易、適切なものにすることを目指すとされた。特にサプライチェーンを構成する中小企業が自力でセキュリティ対策強化に取り組むには限界があるため、同制度の活用により、サプライチェーン全体でのセキュリティ対策の適切な実施が促進され、サプライチェーンのみならず、社会全体でのサイバーレジリエンスの強化が期待される。

(3) 基準の考え方

同制度では、求められるセキュリティ対策を「三つ星(★3)」「四つ星(★4)」「五つ星(★5)」の3段階で区分することを検討している。検討においては先行する国内外のガイドラインや制度等[※264]が参考にされた[※265]。

なお、三つの区分は中小企業が自ら情報セキュリティ対策に取り組む宣言を行うSECURITY ACTION[※266]という先行する仕組みにおいて、一つ星、二つ星の区分が存在している中、同制度はそれに続くものとしている(SECURITY ACTIONについては「3.4.1 (2) (c) SECURITY ACTION」参照)。

それぞれの段階で目指す対策としては、三つ星がすべてのサプライチェーン企業が最低限実装すべきセキュリティ対策、四つ星はサプライチェーン企業が標準的に目指すべきセキュリティ対策、五つ星が未知の攻撃も含めた高度なサイバー攻撃を想定する等サプライチェーン企業が到達点として目指すべき対策としている。

なお、各区分の評価スキームは三つ星が社内等の専門家による自己評価、四つ星、五つ星については、評価機関による第三者評価を想定している。

(4) 今後のスケジュール

2024年度の検討を踏まえ、2025年度には制度案の実証及び、制度構築方針の公表を予定しており、経済産業省は2026年度での制度運用開始を目指している。

3.3.4 政府情報システムのためのセキュリティ評価制度(ISMAP)

2020年6月3日、内閣官房、総務省、経済産業省は「政府情報システムのためのセキュリティ評価制度(Information system Security Management and Assessment Program:通称、ISMAP(イスマップ))」の開始をアナウンスした[※267]。本項では、ISMAPの概要や運用等について紹介する。

(1) ISMAPの概要及び制度改善の経緯

ISMAPは、政府が求めるセキュリティ要件を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。政府調達において、ISMAP導入前は、個々のクラウドサービスが実施する情報セキュリティ対策を調達者が直接確認する必要があったが、この制度により確認を省略でき、負担が軽減される。

2018年6月に公開された「政府情報システムにおけるクラウドサービスの利用に係る基本方針[※268]」では、「クラウド・バイ・デフォルト原則」が掲げられた。これを受けて、総務省と経済産業省は2018年8月から「クラウドサービスの安全性評価に関する検討会[※269]」を発足、ISMAP管理基準を制定し、2020年6月に制度の運用を開始した。

また主に「機密性2情報[※270]」を扱うSaaSサービスに関し、リスクの小さい業務に特化した「ISMAP-LIU(ISMAP for Low-Impact Use)」を設け、2022年11月1日から運用を開始した。なお、一定のセキュリティ水準を維持しつつ、登録に必要な提出物や外部監査の対象を一部免除することでISMAP-LIUへの登録を促進することを目的とした「ISMAP-LIU登録促進のための特別措置」は、2023年5月19日に開始され、2025年3月31日に終了した。

ISMAPは2020年6月の運用開始から5年が経過し、政府機関等がクラウドサービスを調達する際のセキュリティ・信頼性を評価する制度として定着している。その一方で、運用を通じた課題も明らかになってきていることから、ISMAPの信頼性・安定性の保持を前提としつつ、制度運用を合理化・明確化するため、2022年10月より「ISMAP制度改善の取組み」を継続して実施している。

2023年10月からは、「外部監査の負担軽減」や「審査の迅速化・効率化」等の諸課題を改善した運用が開始された[※271]。更に、管理基準の解釈を明確化するための「ISMAP管理基準ガイドブック」が2024年5月に作成・公開された[※272]。今後も国際規格の改訂に伴うISMAP管理基準の改定と併せて、ISMAPが担保している安全性・信頼性を保持しつつ、過剰なセキュリティレベルを求めない(合理化)、重複監査の排除、外部監査機関に競争性を持たせる等により、制度運用の合理化・明確化、クラウドサービス事業者の負荷軽減、審査の迅速化・効率化等の改善といった制度の継続的な見

直しを進めていく※273。

また、ISMAP-LIU についても、2025 年 4 月に事前申請及び事前申請に伴う影響度評価の廃止や、対象業務の拡大といった制度改善が実施された※271。

(2) ISMAP のフロー

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

また、同制度における監査を実施できる監査機関は、当該監査に求められる要求事項を満たすことが確認された後、同制度が公表する ISMAP 監査機関リスト（以下、監査機関リスト）に登録される。同制度のフローを図 3-3-12 に示す。

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

(3) ISMAP の運用

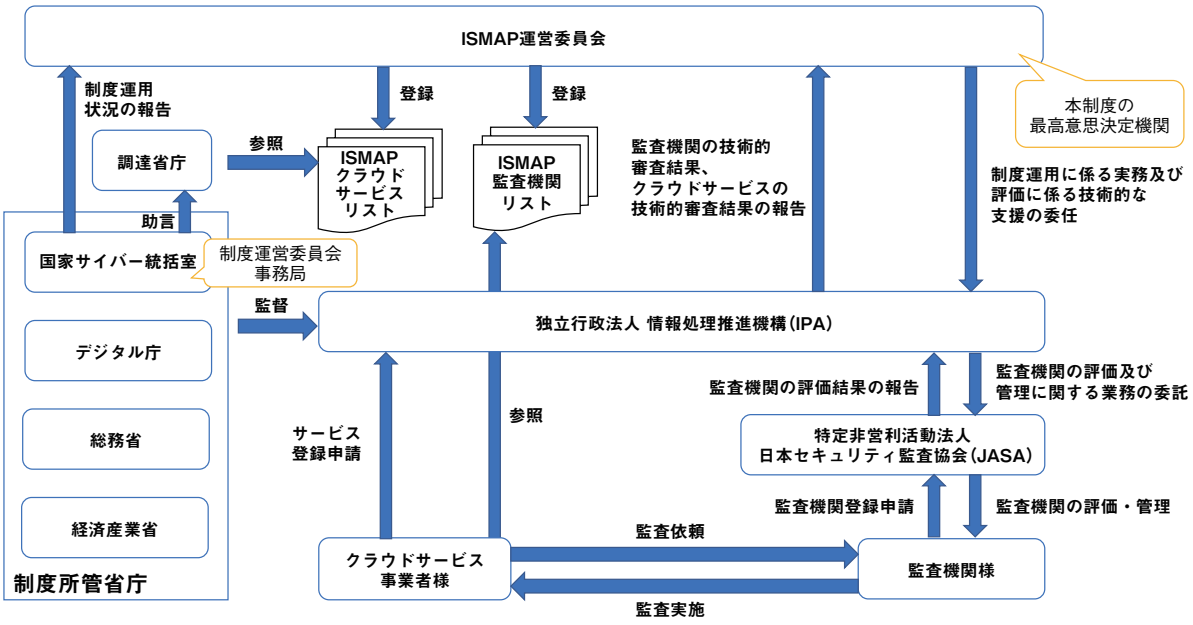
同制度は、2020 年 6 月に内閣官房（NISC、情報通信技術（IT）総合戦略室）、総務省、経済産業省の所管で運用が開始され、2021 年 9 月以降は、NISC（現 NCO）、デジタル庁、総務省、経済産業省の所管で運営されている。最高意思決定機関として ISMAP 運営委員会を設置し、事務局を NCO に置き、運用支援は IPA が担当している。

制度の概要、基準規程類、監査機関リスト、及びサービスリストは、ISMAP ポータルサイト※275 で公開されており、2025 年 4 月末日時点で、登録されている監査機関は 5 機関、クラウドサービスは 78 サービス（うち 1 件は ISMAP-LIU）である。

なお、情報システムのセキュリティ確保の責任は、一義的に当該システムの調達者または利用者が負うものである。このことは「クラウドサービスの安全性評価に関する検討会とりまとめ※276」にも記載されている。同制度に登録されたクラウドサービスを利用したとしても、それだけでは情報システム全体のセキュリティが十分に確保されることにはならない。調達者は、利用するクラウドサービスについて適切な設定を行うことに加えて、情報システム全体のセキュリティリスクを分析し、適切な対策を行うことが求められる。

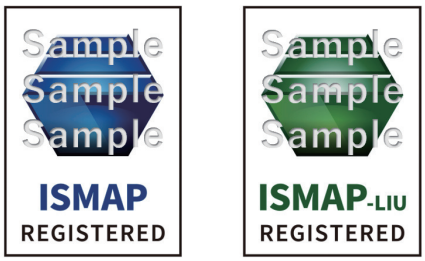
(4) セキュアなクラウド利用に向けて

ISMAP の更なる理解促進と普及に向けて、ISMAP を象徴するロゴマーク（次ページ図 3-3-13）と、ISMAP に登録されているクラウドサービスが使用可能なロゴマーク（次ページ図 3-3-14）を作成し、公開した。また、同制度と類似する海外の制度との比較調査を実施し、調査結果について 2024 年 8 月 27 日に、IPA ホームページ



■図 3-3-12　クラウドサービスの安全性評価の制度のフロー
（出典）ISMAP「ISMAP 概要※274」

■図 3-3-13　ISMAP 制度のロゴマーク（サンプル）



■図 3-3-14　ISMAP に登録されているクラウドサービスが使用可能なロゴマーク（サンプル）

で公開している※277。

そのほかにも、ISMAP に係る各種主体（登録クラウドサービス事業者、クラウドサービス登録申請者、監査機関、制度所管省庁、及び ISMAP 運用支援機関等）の間で、双方向のコミュニケーションを実施・促進している。これに関連した情報発信の一環として、同制度の制度概要を分かりやすくまとめたパンフレット「はじめての ISMAP※278」を 2024 年 4 月に作成・公開した。2025 年 3 月 26 日には、2025 年度以降の ISMAP 制度見直しの具体的な取り組みの工程表を公開している※273。

更に、ISMAP 制度運営側と、登録クラウドサービス事業者及びクラウドサービス登録申請者（以下、登録事業者・申請者）側の双方向でコミュニケーションを図るため、制度運営側から制度改善の取り組み状況について説明会を実施し、改善内容を説明するとともに、登録事業者・申請者側から意見を聴取している。併せて、ISMAP における情報セキュリティインシデントに関する報告について、制度運営側と登録クラウドサービス事業者側双方において速やかな情報連携・共有を図ることを目的に、報告の枠組みを設け、コミュニケーション方法を明確化した※279。

引き続き、制度運営側からの ISMAP に関する情報発信強化、及び ISMAP に係る各種主体間の双方向のコミュニケーション深化によって、同制度が担保している安全性・信頼性を確保しつつ、変化の速いクラウド分野に対応できる制度であるよう変革を進めていく。

3.3.5 CRYPTREC

電子政府のサイバーセキュリティを確保するため、デジタル庁、総務省、経済産業省、NICT、及び IPA は、電子政府システムでの利用を推奨する暗号アルゴリズム（CRYPTREC 暗号リスト※280）の安全性を評価、監視し、その適切な実装方法や運用方法を調査、検討することを目的に、CRYPTREC（Cryptography Research and Evaluation Committees）を組織している。CRYPTREC の体制では、暗号技術検討会のもとに、暗号技術評価委員会と暗号技術活用委員会が設置されている。体制の詳細については CRYPTREC のサイト※281 を参照されたい。ここでは、2024 年度の主な活動内容及び成果をまとめる。

(1) 暗号技術検討会

暗号技術検討会は、CRYPTREC 活動計画の承認、委員会が作成する各種成果物の承認等、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進している。2024 年度には、各委員会で作成した「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024 年度版※282」（以下、耐量子計算機暗号ガイドライン）及び「暗号鍵管理ガイダンス Part 2※283」について審議が行われ、承認された。また、2025 年度の活動として、耐量子計算機暗号（PQC：Post-Quantum Cryptography）に関する対応を速やかに進めることが決定された。

(2) 暗号技術評価委員会

暗号技術評価委員会は、暗号技術に対する攻撃技術の動向調査や安全性評価等、暗号技術の技術的信頼性を検討している。CRYPTREC 暗号リストに掲載されている暗号技術の安全性に関わる監視活動※284 を継続的に実施しているほか、2024 年度の主な活動内容及び成果は以下のとおりである。

- 耐量子計算機暗号ガイドライン及び調査報告書の作成
  暗号技術評価委員会の傘下に設置した WG（Working Group）において、2024 年度版の耐量子計算機暗号ガイドライン及び「CRYPTREC 耐量子計算機暗号の研究動向調査報告書※285」（以下、調査報告書）を作成した。2022 年度に作成した同様のガイドライン及び調査報告書を基に、米国政府標準暗号として規格化された ML-KEM※286、ML-DSA※287、SLH-DSA※288 の各方式や、NIST PQC 標準化プロジェクト※289 において 2022 年から追加募集が行われた PQC 署名方式の評価状況を踏まえて、安全性の根拠とする数学的問題のカテゴリーである格子、符号、多変数多項式、同種写像、ハッシュ関数のそれぞれ

に基づく方式に分類した解説を更新した。

- 量子コンピューターが共通鍵暗号の安全性に及ぼす影響の調査及び評価
  耐量子計算機暗号ガイドライン及び調査報告書において対象としているのは公開鍵暗号や署名方式であり、共通鍵暗号は含まれていない。2019 年度の技術調査報告書「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」を基に、技術の進展を反映した 2024 年度版※290 を作成した。
  2019 年度版からの結論の差異は、量子コンピューターによる攻撃では、ハッシュ関数 SHA-2 及び SHA-3 において衝突攻撃に対する安全性マージンが従来よりも下がることが明らかになったことである。このため、重要な用途に利用するハッシュ関数は、可能であれば、より安全性のマージンが確保できる出力長 384 ビットか 512 ビットのアルゴリズムを採用するのが望ましいとされた。

(3) 暗号技術活用委員会

暗号技術活用委員会は、暗号技術の普及促進、及び安全な利用等に寄与する運用ガイドラインの整備を中心に、暗号利活用に関する課題を検討している。2024 年度の主な活動内容及び成果は以下のとおりである。

- 「暗号鍵管理ガイダンス Part 2」の作成
  暗号技術活用委員会の傘下に設置した WG では、「暗号鍵管理ガイダンス Part 2」を作成した。
  情報を安全に取り扱うためには、暗号鍵の管理を適切に行うことが要求される。2023 年に公開した「暗号鍵管理ガイダンス Part 1※291」及び今回の「暗号鍵管理ガイダンス Part 2」は、暗号鍵管理機能を備えたシステムにおいて検討すべき要求項目を網羅的に解説した「暗号鍵管理システム設計指針（基本編）※292」の理解を促進することを目的として、暗号鍵管理システムのシンプルなモデル（トイモデル）を用いた各要求項目への対応例の提示等をしながら、より詳細に要求項目について解説した。これら二つのガイダンスにより、同設計指針の全要求項目をカバーした。
  「暗号鍵管理ガイダンス Part 2」で解説した内容は、「暗号鍵管理システムの概要設計に関わる項目」「暗号鍵管理デバイスの管理に関わる項目」「暗号鍵管理システムのオペレーション管理に関わる項目」である。このうち、二つ目の項目は暗号鍵管理デバイスを使って暗号鍵の管理及び保管を行うシステムの場合に、三つ目の項目は多層防御や災害・障害復旧対策等を組込むシステムの場合に特に検討が必要となる項目である。
- クラウドサービスにおける鍵管理ガイダンスの検討
  近年は、クラウドサービスを活用して情報システムを構築し、運用することも増えている。しかし、設定不備等によりクラウドサービスに預けた情報が漏えいするリスクも存在する。そこで、クラウドサービスにおける暗号鍵管理システムを適切に選択、構築、運用することを目的として、クラウドサービスにおける暗号鍵管理の仕組みや注意事項を解説したガイダンスを作成すべく、2024 年度から検討を開始した。
  2024 年度は趣旨（目的、想定読者、スコープ）、検討体制、スケジュール等のガイダンス作成方針を議論した。2025 年度から新たな WG を設置して、本格的にガイダンスの作成に着手する予定である。

(4) CRYPTREC シンポジウム 2024 の開催

CRYPTREC の活動成果を周知し、暗号技術に関する最新動向を紹介することで、社会全体のセキュリティ向上に寄与するため、CRYPTREC シンポジウムを開催している。2024 年度は 9 月 2 日に「CRYPTREC シンポジウム 2024※293」を開催し、CRYPTREC の活動報告に加え、第一人者を招いて三つの招待講演（軽量暗号と標準化動向、軽量暗号に対するサイドチャネル攻撃、暗号資産の鍵管理）を行った。

COLUMN

これからは「量子コンピューターに対して安全な暗号」を使わなければいけないの？

量子コンピューター関連技術の発達は目覚ましく、将来的には、現在使っている暗号が量子コンピューターによって解読されてしまう、と聞いたことはありませんか？　他方で、そのような事態に対応するための「量子コンピューターに対して安全な暗号」というものについても聞いたことがあるかもしれません。正式には、「耐量子計算機暗号」や「PQC（Post-Quantum Cryptography）」と呼ばれるものです。このコラムでは、このような話をどれだけ深刻に受け止める必要があるのかをお話しします。

まずは安心できる点から見ていきましょう。幸いにも、現在広く利用されている暗号が、近い将来に量子コンピューターにより解読される可能性は低いと考えられています[i]。これは、現在実現している量子コンピューターと、暗号解読に利用できる水準の量子コンピューターでは、性能に大きな隔たりがあるためです。その隔たりを埋めるためにどのくらいの期間が必要かという議論には、大きな余地があり、誰も確かなことは言えません。10 年で実現すると予想する人もいれば、永遠に実現しないと予想する人もいます。確実なのは、今、暗号解読をするのであれば、量子コンピューターよりもスーパーコンピューターを使う方が圧倒的に確実だということです。

一方で、以下に挙げるようないくつかの懸念点もあります。

一つ目の懸念点は、暗号解読できる量子コンピューターの実現時期について、確かなことは誰にも分からないということは、前述したようにかなり長い期間実現しないとの予想とは反対に、かなり短期間で実現する可能性もゼロだとは言い切れないという点です。

二つ目の懸念点は、現時点では暗号解読ができない情報であっても、遠い将来においては量子コンピューターを利用してその情報が解読されてしまうかもしれないという点です。例えば、患者を特定可能な情報を含む遺伝子疾患に関する医療情報を暗号化して保管してあったとしましょう。その情報の保護期間が 100 年と設定されていたとすると、量子コンピューターによる暗号解読が 100 年以内に実現した場合、このような情報は量子コンピューターによって解読される脅威に晒されることとなります。

三つ目の懸念点は、情報システムで使用されている暗号を変更するためには、様々な作業が発生し、それらを完了するには多くの人が想像する以上に時間がかかる点です。例えば、情報システムで使用される製品の製造事業者が PQC を搭載した製品を開発・供給する、情報システムの構築事業者が PQC を利用できるよう情報システムを更新する（ハードウェア、ソフトウェア、システムの再設計や交換が必要な場合もある）、品質保証・認定基準・監査等の手続きを更新する、更新された基準に基づいて認証を再度取得する等の一連の作業が完了してやっと暗号の変更ができるという場合もあります。これらの作業は、多くの人々が協力して行う必要があるものですが、共通の目標意識を持てなかった場合は、より長い時間がかかることになりかねません。

これらの懸念点があることから、現時点では「暗号解読される可能性が低い」のにもかかわらず、「量子コンピューターに対して安全な暗号に移行すべきだ」といった話が出てきているのです。

COLUMN

以上の背景のもと、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）は PQC の標準化を行い[ii]、それらの暗号をいつごろまでに利用するべきかの計画案を公表しました[iii]。この計画案の中では、PQC への切り替えのタイミングを 2035 年としています。また、産業界においても、これらの標準化された PQC に対応する製品が急ピッチで開発されつつあります。今後は、それらの製品が、徐々に利用されるようになると予想されています。

もっとも、情報システムで使用しているすべての暗号を PQC に置き換えるには、相当なコスト（費用及び期間）が必要となります。そもそも現実的なコストではすべての暗号を一斉に PQC に置き換えることは不可能かもしれません。そのような事情を踏まえると、保護しなければいけない期間が長く、また漏えいした場合のリスクが高い情報から優先して、PQC への置き換えを行うアプローチが効果的だと考えられます。例えば、数十年にわたって秘密裡に保管しなければならないデータは早急に対応しつつ、短期間の保護しか要求されていないデータに対しては今までどおり既存の暗号技術で対応し、長期的には徐々に PQC を利用する割合を増やすといったアプローチです。

ただし、このようなアプローチを実施するためには、対象とする情報システムが、どのようなデータに対して、どのような暗号を利用しているかということを把握していないといけません。つまり、情報システムの管理者が最初に行うべきことは、その情報システムが保護しているデータと、利用する暗号にどのようなものがあるのかを確認することなのです。

i　CRYPTREC：現在の量子コンピュータによる暗号技術の安全性への影響　https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html〔2025/7/10 確認〕
ii　NIST：FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard　https://csrc.nist.gov/pubs/fips/203/final〔2025/7/10 確認〕
NIST:FIPS 204, Module-Lattice-Based Digital Signature Standard　https://csrc.nist.gov/pubs/fips/204/final〔2025/7/10 確認〕
NIST:FIPS 205, Stateless Hash-Based Digital Signature Standard　https://csrc.nist.gov/pubs/fips/205/final〔2025/7/10 確認〕
iii　NIST：IR 8547, Transition to Post-Quantum Cryptography Standards　https://csrc.nist.gov/pubs/ir/8547/ipd〔2025/7/10 確認〕　注：この計画案は、あくまでドラフト段階であり、最終稿ではありません。

3.4 組織・個人に向けたサイバーセキュリティ対策の普及活動

組織や個人に向けたサイバーセキュリティ対策の普及活動について述べる。

3.4.1 組織におけるサイバーセキュリティの取り組みと支援策

組織におけるサイバーセキュリティの実態と対策状況、普及活動及び組織に向けたサイバーセキュリティ支援策と支援ツールについて述べる。

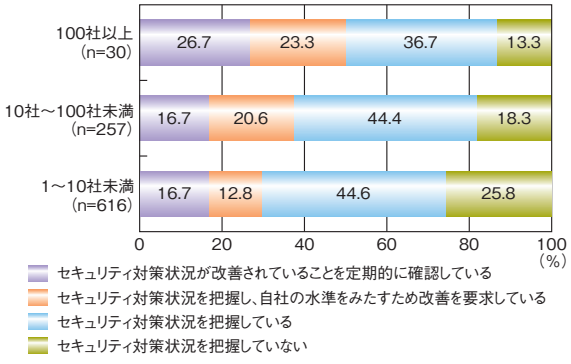
(1) 中小企業におけるセキュリティ管理体制の構築状況

中小企業における企業のセキュリティ対策・統制状況について、以下の資料を基に述べる。

- NRI セキュアテクノロジーズ株式会社（以下、NRI セキュア社）:「NRI Secure Insight 2024[※294]」（日本 1,481 社、米国 507 社、オーストラリア 503 社の企業を対象に調査。以下、NRI セキュア社調査）
- IPA:「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」（全国の中小企業の経営層及び情報システム／情報セキュリティの担当マネージャー 4,191 人を対象に調査。以下、IPA 調査）

(a) サプライチェーンのセキュリティ対策把握状況

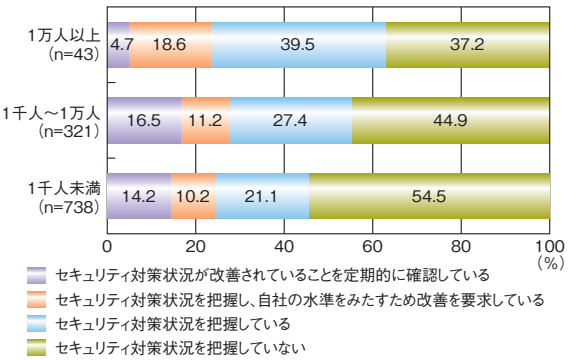
NRI セキュア社調査によると、国内関係会社／グループ会社の統制状況についてグループ会社数別で見た場合の、グループ会社数が 10 社未満である日本企業における、「セキュリティ対策状況を把握していない」の割合は 25.8% であるのに対し、グループ会社数が 100 社以上の企業における「セキュリティ対策状況を把握していない」の割合は 13.3% であった（図 3-4-1）。



■図 3-4-1　グループ会社数別で見た国内関係会社／グループ会社の統制状況
（出典）NRI セキュア社「NRI Secure Insight 2024」を基に IPA が編集

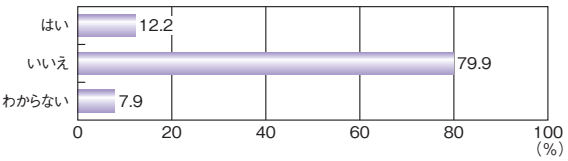
また、国内パートナー／委託先の対策状況について従業員数別で見ると、従業員数が 1 千人未満である企業では「セキュリティ対策を把握していない」の割合は 54.5% であるのに対し、従業員数が 1 万人以上の企業では 37.2% であった（図 3-4-2）。

これらにより、企業規模が大きい程、サプライチェーンにおけるセキュリティ対策状況の把握が進んでいること、また、グループ会社への統制と比較して、委託先への統制は進んでいないことが分かる。



■図 3-4-2　従業員数別で見た国内パートナー／委託先の統制状況
（出典）NRI セキュア社「NRI Secure Insight 2024」を基に IPA が編集

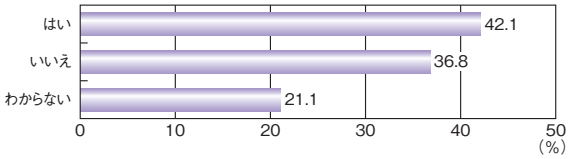
一方、中小企業を対象とした IPA 調査で「発注元企業から情報セキュリティに関する要請を受けた経験はあるか」を尋ねたところ、「はい」が 12.2%、「いいえ」が 79.9%、「わからない」が 7.9% となり、全体の 1 割強が発注元企業から情報セキュリティに関する要請を受けた経験があると回答した（図 3-4-3）。



■図 3-4-3　販売先（発注元企業）から情報セキュリティに関する要請を受けた経験（n=4,191）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

また、このうちの「はい」と答えた企業に「発注元企業から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思うか」を尋ねたところ、「はい」が 42.1% となり、全体の 4 割強となることが分かった。ここから、発注元企業の求めるセキュリティ

対策に応じる、あるいはそういった対策を行っているということは、発注元企業との取り引きにつながる大きな要因になり得るということが分かる（図 3-4-4）。

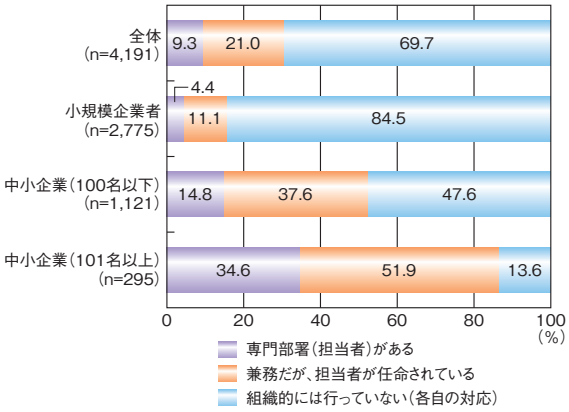


■図 3-4-4　情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因か（n=511）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

(b) 中小企業の情報セキュリティ体制の整備状況

IPA 調査によると、中小企業に情報セキュリティ対策はどのような体制で行われているか、整備状況を尋ねた結果、「組織的には行っていない（各自の対応）」と回答した割合が 69.7% と最も高く、ほぼ 7 割の中小企業において情報セキュリティ体制が整備されていないことが分かる。

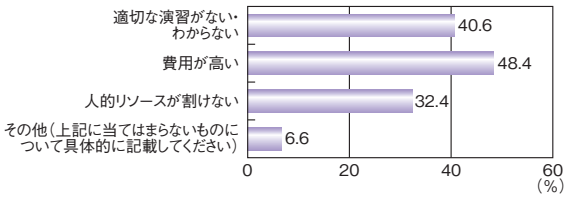
企業規模別に見ると、「小規模企業者」（5 名以下）では「組織的には行っていない（各自の対応）」割合が 84.5% であるのに対し、「中小企業（100 名以下）」では 47.6%、「中小企業（101 名以上）」では 13.6% となっており、企業規模が大きくなるにつれ、セキュリティ体制の整備がなされていることが分かる（図 3-4-5）。



■図 3-4-5　セキュリティ体制の整備状況
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

(c) 中小企業の情報セキュリティ人材の教育状況

IPA 調査では、中小企業のセキュリティ人材の教育に関する調査を行っている。「セキュリティ人材を育成するために外部研修を活用している、または活用する意向があるか」を尋ねた結果、19.8% が「はい」、80.2% が「いいえ」と答えた。「いいえ」と答えた理由について尋ねた結果、「費用が高い」が 48.4%、「適切な演習がない・わからない」が 40.6% との回答があり、コストや適切な演習が分からないといったことが外部研修の活用の障壁になっていることが分かる。また、「人的リソースが割けない」が 32.4% であり、セキュリティ担当として育てる人員を確保する余裕がないことが読み取れる（図 3-4-6）。

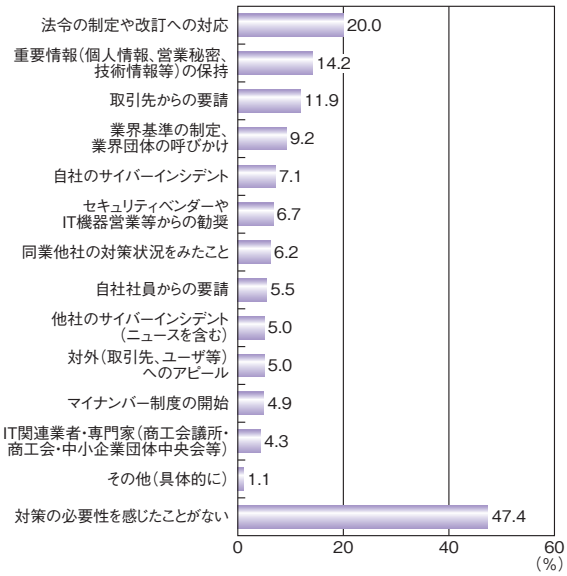


■図 3-4-6　外部研修を活用していないまたは活用する意向がない理由（n=3,361）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

(d) 中小企業の情報セキュリティの技術的対策実施状況

IPA 調査によると、中小企業が情報セキュリティ対策を実施（強化）するきっかけとなった理由について、「法令の制定や改訂への対応」が 20.0% と最も多く、「重要情報（個人情報、営業秘密、技術情報等）の保持」が 14.2%、「取引先からの要請」が 11.9%、「業界基準の制定、業界団体の呼びかけ」が 9.2% と続いている（図 3-4-7）。

自ら重要情報を保持しているとの認識を持って対策を強化するケースも見られるが、外的要因（外部の基準や規程の制定や取引先からの要請）をきっかけとするケー

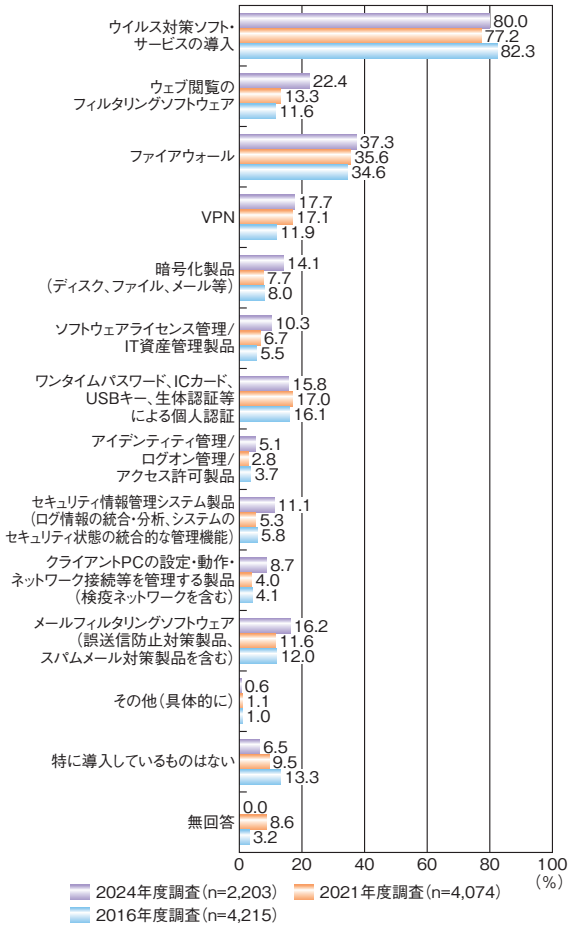


■図 3-4-7　情報セキュリティ対策を実施（強化）するきっかけとなった理由（n=4,191）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

スも多いことがうかがえる。

また、図 3-4-7（前ページ）の設問に「対策の必要性を感じたことがない」以外の回答をした中小企業に対して、導入している情報セキュリティ関連製品やソフトウェアについて尋ねた結果を図 3-4-8 に示す。「ウイルス対策ソフト・サービスの導入」が 80.0% と最も高く、幅広く利用されており、基本的なセキュリティ対策は進んでいることが読み取れる。次いで、「ファイアウォール」が 37.3%、「ウェブ閲覧のフィルタリングソフトウェア」が 22.4% となった。過去 2 回の調査と比較すると、ウイルス対策ソフト・サービスの導入率は 2021 年度の 77.2% と比較して微増している。また、フィルタリングや資産管理製品の導入は拡大しており、これは新たなセキュリティニーズを反映したものであると思われる。クライアント PC の設定等を管理する製品の導入も増えており、2021 年度の 4.0% から 8.7% に増加していることから、ネットワーク管理の重要性が認識されてきていると思われる。

これらのことから、不正アクセスやデータ保護への関心と投資が高まっており、それに伴い様々なセキュリティ製品が導入されつつあることがうかがえる。



■図 3-4-8　情報セキュリティ関連製品やソフトウェアの導入状況
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

(2) 組織に向けたサイバーセキュリティ支援組織・支援策と支援ツール

IPA に関連したサイバーセキュリティ支援組織・支援策と支援ツールについて紹介する。

(a) CRIC SC3

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）※295 は、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的として、2020 年に設立された。設立当初は、IPA が事務局となり、取り組みを進めてきたが、更なる体制強化を行うため、2025 年 1 月に一般社団法人サイバーリスク情報センター（CRIC：Cyber Risk Intelligence Center）※296 と一体的連携を行う形式で法人化を行い、一般社団法人サイバーリスク情報センター 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（CRIC SC3）※297 として活動を開始した。

SC3 は 2020 年の設立当初からサプライチェーン対策の重要性を業界に広め、経営層への情報提供や中小企業向けの対策強化、セキュリティ人材の育成を推進し、「業界連携のプラットフォーム」としての位置付けを確立してきた。しかし、サイバー攻撃の高度化やパンデミックによるリモートワークの普及、DX の進展、生成 AI 等の環境変化に伴い、産業界のサイバーセキュリティへの意識も急速に向上、変化しており、個々の企業による対応に加えて、業種・業態を越えたサプライチェーン全体での課題対応や、産業界と政府間の連携強化の必要性が高まってきた。このような背景から、設立当初からの理念である「産業界主導による業界連携のプラットフォーム」としてサプライチェーン上のステークホルダーとの対話や政策提言を主導し、施策の実効性を高めるために、2024 年 4 月からは企画運営機能の強化、WG の再編を進めた。

業界連携、国際連携、人材育成を推進する方針が 2024 年 6 月の総会で承認されたことから、業界連携 WG、国際 WG、人材教育・育成 WG が設置され、更に WG のもとでよりターゲットを限定した SWG が活動している。業界連携 WG にはサプライチェーンサイバーセキュリティ成熟度モデル検討 SWG や工場セキュリティ共創 SWG が存在する。前者は中小企業を含めたサプライチェーン全体のセキュリティ対策の底上げを目的として、

取引先から対策状況が確認可能になるよう企業ごとに対策レベルを可視化する制度の運用を検討する（「3.3.3 サプライチェーン強化に向けた対策評価制度構築に向けた検討」参照）。後者は工場システムにおけるセキュリティの普及啓発を行うことを目的としている。

一体的連携を行っている CRIC は、セキュリティ産業の供給側であるセキュリティベンダーが活動をする CRIC SQC（セキュリティ品質検討委員会：Security Quality Committee）と、需要側のユーザー企業団体である CRIC CSF（産業横断サイバーセキュリティ検討会：Cross Sectors Forum）を有している。CRIC に、需要側の中小企業を含む団体の SC3 が加わることで、産業界におけるサイバーセキュリティ対策を包括的に議論する組織が CRIC に集約される。これにより、議論が活性化し、産業界のサイバーセキュリティ対策を推進するための様々な取り組みの実現につながることが期待される。

(b) サイバーセキュリティお助け隊サービス制度

IPA は、中小企業等を狙ったサイバー攻撃への対処として不可欠なサービスを効果的かつ安価に提供することをコンセプトとした「サイバーセキュリティお助け隊サービス制度※298」を 2021 年度から運営している（図 3-4-9）。

■図 3-4-9 「サイバーセキュリティお助け隊サービス※299」パンフレット

同制度が提供するサービスの要件（上限価格、相談窓口の設置、異常の監視、緊急時の対応支援、簡易サイバー保険等）は、「サイバーセキュリティお助け隊サービス基準※300」に定められている。これらを満たした民間のセキュリティ事業者のサービスが「サイバーセキュリティお助け隊サービス」として登録され、IPA の Web サイトで公開されている※301。2025 年 4 月 1 日時点で 46 事業者、78 サービスが登録されており、2025 年 3 月時点で約 8,400 の企業に導入されている。同サービスの導入に際しては、IT 導入補助金（セキュリティ対策推進枠）を申請することが可能である。2025 年度は補助の上限金額が 100 万円から 150 万円に、補助率は 2 分の 1 以内から小規模事業者限定で 3 分の 2 以内にそれぞれ引き上げられた。このように、中小企業が導入しやすいサービスとなっている。

2024 年度には、中規模以上の中小企業のセキュリティ対策のニーズに応える、お助け隊サービス 2 類制度が開始された。同制度は、従来のお助け隊サービスのコンセプトを維持しながら、価格要件を緩和したものであり、監視上限台数の拡大、監視機能の強化、定期的なコンサルティング実施等のサービス拡充を行うことが可能となった。

(c) SECURITY ACTION

「SECURITY ACTION※302」は IPA が運営する中小企業向けの情報セキュリティ対策の自己宣言制度であり、2025 年 4 月時点で、40 万件超の宣言が行われている。この制度では「中小企業の情報セキュリティ対策ガイドライン」に基づき 2 段階の取り組み目標を用意しており、取り組み目標に応じた宣言を行うと、「★」（一つ星）と「★★」（二つ星）のロゴマークを利用できるようになる（図 3-4-10）。

■図 3-4-10 「SECURITY ACTION」ロゴマーク

一つ星の取り組み目標は、情報セキュリティの基本的な対策の実施で、具体的には、「情報セキュリティ 5 か条」に取り組むことが求められる。二つ星は、「5 分でできる! 情報セキュリティ自社診断※303」を行い、自社の状況を把握した上で「情報セキュリティ基本方針」を定め、外部に公開することが求められる。自己宣言をすることが、経済産業省が実施する IT 導入補助金等の申請要件となっており、都道府県や市町村が提供する補助金や助成金の申請要件としても活用されている。この制度により、中小企業は情報セキュリティ対策を強化しつつ、経済的

な支援を受けることが可能になる。

(d) セキュリティインシデント対応机上演習教材

中小企業においても、サイバー攻撃によってセキュリティインシデントが発生した場合、被害とその影響範囲を最小限に抑えて事業継続を確保する必要がある。そのためには、あらかじめ対応手順の整備をしておくほか、実際にセキュリティインシデントが発生した際の対応を体験しておくことが重要である。こうしたことを踏まえ、IPAは、初動対応や再発防止策の検討を行う「セキュリティインシデント対応机上演習」を組織内で行うための教材とマニュアルを2025年4月に公開した※304。

同演習は、最初にインシデント対応のポイントを学習した後、付与されたインシデント発生状況を踏まえた対応についてディスカッションを実施し、最後に振り返りを行う流れとなっている（表3-4-1）。演習を通じ、組織の意思決定プロセスを体験する内容となっているため、セキュリティの担当者だけではなく経営層も参加することを推奨している。

演習教材は、一般企業及び医療機関においてランサムウェアに感染した場合を想定したシナリオとなっており、必要に応じて企業の設定やシステム構成等、内容をカスタマイズできる。マニュアルには、実施手順やシナリオの解説等が記載されており、中小企業のセキュリティ担当者等が演習を企画・実施しやすいようになっている。

演習を通じ、組織におけるインシデント対応の課題を発見し、体制や対応ルール等の改善を行うことで、組織のインシデント対応能力を向上させることが可能となる。

時間	内容
0:00～0:05 （5分）	オープニング（主催者挨拶、講師紹介、目的説明等）
0:05～0:25 （20分）	**講習（座学）** 「中小企業のためのセキュリティインシデント対応の手引き」をベースにインシデント対応のポイントを学ぶ。
0:25～1:25 （60分） ※説明、発表時間を含む	**演習1** 発生した事案の初動対応について、グループディスカッションにより対応方針等を検討する。
1:25～1:35 （10分）	（休憩）
1:35～2:35 （60分） ※説明、発表時間を含む	**演習2** 業務・システムの復旧や再発防止、公表等について、グループディスカッションにより対応方針等を検討する。
2:35～2:50 （15分）	振り返り
2:50～3:00 （10分）	質疑応答・クロージング

■表3-4-1　セキュリティインシデント対応机上演習のタイムスケジュール
（出典）IPA「セキュリティインシデント対応机上演習教材※304」

(e) 制御システムのセキュリティリスク分析ガイド

IPAは、制御システムのセキュリティ向上を目的として2017年10月、「制御システムのセキュリティリスク分析ガイド」の第1版を公開し、2018年10月には第2版を公開した。2023年3月に記載誤り等を訂正した最新版を公開している※305。同ガイドは、既存の規格やガイドラインで要求されているリスク分析の手順について事業者が実施できるように解説したガイドブック（手引き書）である。同ガイドの第1版公開後、同ガイドや付随する別冊資料や補足資料の拡充を行っており、2024年は以下の追加公開を行った。

- 2024年3月、同ガイドの補足資料である「制御システム関連のサイバーインシデント事例」シリーズにおいて、「【事例10】2022年 衛星通信網へのサイバー攻撃の事例」「【事例11】2022年 電力網への攻撃の事例」を公開した※306。同シリーズでは、インシデント事例の概要と攻撃の流れ（攻撃ツリー）を紹介しており、制御システム保有事業者が、同ガイドに提唱された「事業被害ベースのリスク分析」を実施する際に活用できる。
- 2024年12月、同ガイドの別冊として「制御システムに対するリスク分析の実施例 第2版 事例2：社外サービスと接続した制御システムに対するリスク分析※307」を公開した。同文書では、外部サービスと接続した制御システムのリスク分析を行い、「外部ネットワークから攻撃者が侵入する脅威」を新たに想定している。
- 2024年12月、同ガイドの補足資料として「『制御システムのセキュリティリスク分析ガイド』と国際規格との比較※308」を公開した。同資料では、リスクアセスメントに言及する国際規格ISO/IEC 27000シリーズ、IEC 62443シリーズやNIST SP 800-30等と同ガイドを比較し、評価項目の類似性や違いを明確にしている。

また2024年10月には「『スマート工場のセキュリティリスク分析調査』調査報告書 第2版※309」を公開した。第2版には、スマート工場化に伴う制御システムの新たな課題を調査する目的で実施された「高度制御を実現する新たな制御システムのスマート化モデル類型細分化と対策の調査」の調査結果が追加された。同調査では、実装モデルに対するリスク分析手法として「制御システムのセキュリティリスク分析ガイド」を用いている。

IPA では、同ガイドや事例シリーズの提供だけなく、効果的なリスク分析を実施するためのセミナーを開催し、セキュリティ対策としてのリスク分析の有効性及びリスク分析手法の理解を深める活動に取り組んでいる※310。

3.4.2 サイバーセキュリティ及びネットリテラシーの普及活動

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

(1) 生成 AI の安全利用に関する啓発活動

近年、高精度な文章や画像等を生成する生成 AI が、急速に発展しており、個人でも生成 AI を簡単に利用できるようになってきている。それに伴い、生成 AI を悪用した犯罪や、情報の漏えい等が問題となっている。

2024 年 5 月、インターネット上で公開されている対話型生成 AI を悪用してマルウェアを作成したとして、川崎市在住の 25 歳の無職の男性が不正指令電磁的記録作成容疑で逮捕された※163。複数の対話型生成 AI に指示を出してマルウェアの設計情報を回答させ、回答内容を組み合わせてマルウェアを作成したという。

また、2025 年 3 月にミャンマーで大地震が発生した際には、AI で作成されたフェイク画像や動画が出回り、各国のメディアが誤って引用してしまう等、混乱を招く事態に陥った※311。

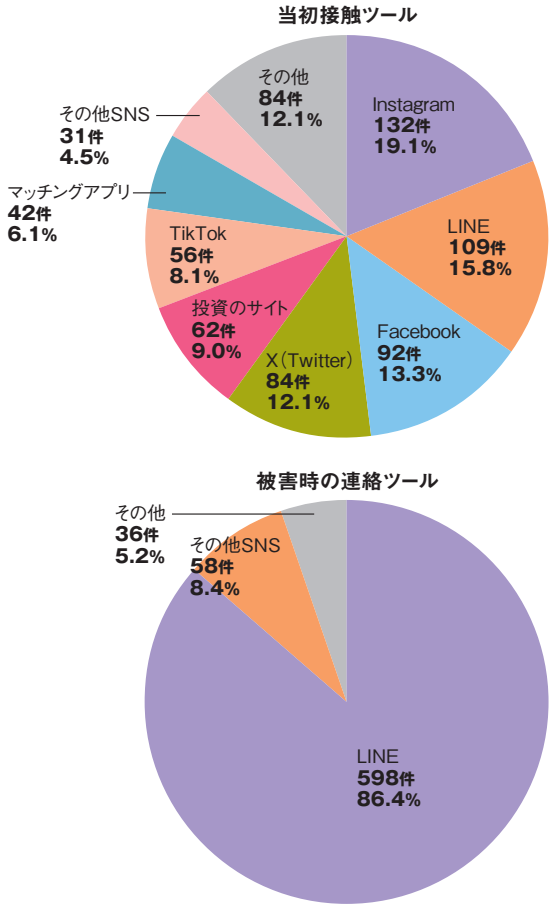
総務省は、生成 AI を活用する上で注意すべきことをクイズ形式で学べる啓発教材「生成 AI はじめの一歩～生成 AI の入門的な使い方と注意点～※312」を公開した。同教材では、生成 AI の活用にあたって注意すべきポイントとして「情報の正確性」「情報流出」「知的財産権の侵害」「活用者としてのモラル」の四つを挙げている。

なお、生成 AI については、「2.1 AI セーフティ実現に向けた取り組み」も参照いただきたい。

(2) SNS を使った詐欺防止に向けた啓発活動

近年、SNS を悪用した詐欺の被害が急増している。2025 年 2 月、60 代の女性が、SNS を通じて嘘の投資話を持ちかけられ、現金 2,200 万円を騙し取られる事件があった※313。

警察庁は「警察庁・SOS47 特殊詐欺対策ページ※314」で、このような SNS 型投資詐欺について、手口と被害の実態や、実際の事例を丁寧に解説している※315。被害の実態については、SNS 等の様々なチャネルから接触を図った後、被害時の連絡ツールとして LINE が使用されるケースが多いことが示されている（図 3-4-11）。事例の紹介では、被害者の年齢や被害金額に加え、「必ず儲かります」「投資用アプリをインストールしてください」といった、詐欺に用いられるキーワードを挙げながら解説している。最後に、気を付けるべきポイントとして「投資先が実在しているか・国の登録業者かどうか」「振込先の口座に不審な点がないか」等を挙げ、注意を促している。



■図 3-4-11　SNS 型投資詐欺の被害の実態（2025 年 1 ～ 2 月、総数 692 件）
（出典）警察庁「SNS 型投資詐欺※315」を基に IPA が編集

また、金融庁では、「詐欺的な投資に関する相談ダイヤル」を開設し、SNS 型投資詐欺による損害を被った場合に限らず、詐欺的な投資勧誘を受けて不審に思った場合や、投資について悩んでいる場合の相談等を受け付けている※316。

2025 年 1 月、50 代の無職の男性が、マッチングアプリで知り合った人物から、SNS を通じたやり取りで「会うためには会員カードを作る必要がある」等と言われ、現金 125 万円を騙し取られる SNS 型ロマンス詐欺の被害に遭った※317。

警察庁はSNS型ロマンス詐欺についても対策ページを公開しており、「実際に会ったことがない人からお金の話をされたら要注意」と呼びかけている※318。

また、2024年12月に岩手県警察はNTT東日本岩手支店、セコム株式会社岩手統括支社と「地域の安全・安心の実現に向けた連携協定」を締結し、特殊詐欺被害防止のための広報啓発活動や、特殊詐欺を認知した際の積極的な通報等に連携して取り組むことを発表した※319。

(3)闇バイト防止のための啓発活動

2024年8月から11月にかけて、1都3県でいわゆる闇バイト※320との関連が疑われる強盗事件が19件発生した※321。これらの事件により逮捕された47人のうち37人が20代以下であり、若年層が闇バイトに応募し犯罪の実行者となるケースが目立っている。2024年9月、さいたま市で起きた事件では、住宅に20代の男らが押し入り、住人女性2人が粘着テープのようなもので拘束され、現金約10万円とキャッシュカード等が奪われた※322。2024年10月には横浜市内で男性高齢者が殺害され、現金や貴金属等が奪われるといった凶悪な事件も起きた※323。

文部科学省は、YouTubeの「文部科学省／mextchannel※324」で、闇バイトの危険性をドラマ形式で説明した「教材㉗情報の真偽を確かめよう! SNS闇バイト編(高校生)※325」を公開した。

警視庁では、闇バイトに申し込んでしまった場合、警視庁総合相談センターまたはヤング・テレホン・コーナー(警視庁少年相談係)に相談するよう呼びかけている※326。

また、LINEヤフー株式会社と国立大学法人静岡大学は、闇バイトの加担リスクを学ぶことを目的とした中学生・高校生向けの情報モラル教材「『闇バイト』を自分ごととして考えてみよう～闇バイトに注意!あなたを犯罪に巻き込む手口～」を公開した※327。同教材では、実際に闇バイトを募集する側に立ち、募集コメントを考える経験を通じて、闇バイトの可能性がある募集の見極め方を学ぶことができる。

(4)誹謗中傷防止のための啓発活動

インターネット上での誹謗中傷は、2024年夏に開催されたパリ2024オリンピック・パラリンピック競技大会でも問題となった。競歩の日本代表2人が混合リレーに専念するため、個人種目を辞退したことをめぐり、誹謗中傷が相次ぎ、選手が自身のSNSで「たくさんの方からの厳しい言葉に傷ついた。このようなことが少しでも減ってほしい」と投稿した※328。公益財団法人日本オリンピック委員会も異例の声明を出し、行き過ぎた内容に対しては警察への通報や法的措置も検討する姿勢を示す事態となった※329。

相次ぐ誹謗中傷に対して、開示請求を行う動きが増えている。芸能事務所の株式会社セント・フォースは2025年2月26日、公式サイトを更新し、所属タレントに対するネット上の誹謗中傷や虚偽の情報の拡散について「弊社はタレントの安全と尊厳を守るため、悪質な誹謗中傷・デマの拡散について、法的措置を含めた厳正な対応を進めてまいります。具体的には、弁護士と連携のもと、発信者情報開示請求を行い、悪質な投稿の発信者に対する適切な措置を講じます」と声明を発表した※330。

総務省では、一般社団法人ソーシャルメディア利用環境整備機構、一般社団法人セーファーインターネット協会及び法務省と共同して、特設サイト「#NoHeartNoSNS※331」を開設し、誹謗中傷に対する相談窓口を紹介している(図3-4-12)。

■図3-4-12　#NoHeartNoSNS
(出典)一般社団法人ソーシャルメディア利用環境整備機構「#NoHeartNoSNS」

法務省はYouTubeの「MOJchannel※332」で、「人権啓発動画『インターネットはヒトを傷つけるモノじゃない。』※333」を公開し、インターネット上の誹謗中傷等の根絶を呼びかけている※334。

(5)ネットリテラシー向上のための啓発活動

NISCは毎年2月1日から3月18日を「サイバーセキュリティ月間」と定め、「#サイバーセキュリティは全員参加」というキャッチフレーズのもと、中央省庁のほか、民間企業でも様々な啓発イベントやコンテンツの公開を実施している※335。

2024 年度の「サイバーセキュリティ月間」にあわせて NISC は、「インターネットの安全・安心ハンドブック Ver 5.10[※336]」を公開した。

内閣府大臣官房政府広報室は、「スマートフォンのセキュリティ対策できていますか? 4 つのポイント[※337]」を公開し、電子メールや SMS 内のリンクは安易にタップせず、携帯電話会社等が提供するセキュリティ設定を活用する等の対策を徹底するよう呼びかけている。

総務省は、インターネットや SNS における利用者の ICT リテラシー向上を目指し、プラットフォーム事業者や通信事業者、IT 企業・団体等とともに官民連携プロジェクト「DIGITAL POSITIVE ACTION[※338]」を開始した。

また、総務省では Web サイト「上手にネットと付き合おう! 安心・安全なインターネット利用ガイド[※339]」を運営しており、2024 年度は、青少年、保護者、シニアを対象に、ICT リテラシーを身に付けるための教材「5 つの分野の ICT リテラシーを学ぼう ～つくろう!守ろう!安心できる情報社会～[※340]」を公開した(図 3-4-13)。

■図 3-4-13　青少年向け啓発教育教材
(出典)総務省「5 つの分野の ICT リテラシーを学ぼう ～つくろう!守ろう!安心できる情報社会～」

COLUMN

セキュリティは「コスト」か「投資」か?

現代社会において、企業や組織が直面するサイバーセキュリティ上の脅威はますます深刻化していますが、脅威に対応するためのセキュリティ対策を「コスト」としてとらえるべきか、積極的な「投資」ととらえるべきかという議論が昔からされてきました。

長年にわたり、セキュリティ対策が直接的な収益を生まないことから「(やむを得ない) コスト」とみなされてきました。例えば、企業がファイアウォールやセキュリティソフトを導入する場合、それらの製品購入費、ライセンス料、保守費用等に加え、専門スタッフの雇用や教育、システムの運用監視のための人的リソースも必要です。これらは目に見える形では利益に直結しないため、「コスト」と感じられるのも無理はありません。特に予算が限られている中小企業にとっては、こうした費用を負担に感じる場合もあることから、セキュリティ対策への出費がなかなか進まなかったという側面があります。

これに対して、2015 年に経済産業省と IPA が「サイバーセキュリティ経営ガイドライン[i]」を発表して、セキュリティ対策は企業活動におけるコストや損失を減らすために必要不可欠な「投資」であると位置付け、経営者に対してセキュリティ対策への出費を促しました。例えば、サイバー攻撃によるシステムダウンが発生すれば、業務停止による機会損失は計り知れません。特に、現代ではデジタル化が進み、オンラインでの取り引きやサービス提供が主流となっています。この環境下でシステムが脆弱であれば、顧客は安心してサービスを利用できず、競争力を失うことになります。逆に、強固なセキュリティをアピールできれば、顧客からの信頼を獲得し、長期的な収益増加につなげられるというわけです。

ところが最近、このセキュリティ対策は「投資」であるという考え方に疑問を持つ声が増えていきています。その理由の一つは、やはりセキュリティ対策の効果は事後的にしか評価できないという点にあります。例えば、新しいマーケティング戦略や設備導入といった投資では、事前に ROI (投資収益率) を予測し、その成果を数値で追跡することが可能ですが、セキュリティ対策の場合、「攻撃が防げた」「被害がゼロだった」といった成果は、実際に何かが起こらなかったことを証明するものであり、具体的な利益として計上することは難しいという特性があるからです。セキュリティ対策の ROI を定義しようという試みもされてきましたが、未だに説得力のある定義はされていません。また、セキュリティや個人情報保護に関する法規制や、サプライチェーンにおける発注元からの要求等、社会的要請への対応や社会的責任を果たすための「必要なコスト」であると考えるべきだとの意見が台頭してきています。

しかしながら、この「コスト」か「投資」という議論は、視点の違いに過ぎません。現状の課題に対応するという視点からは「コスト」と言えるでしょうし、将来起こる可能性がある課題に先んじて対応し企業競争力を高めるという視点からは「投資」と言えるでしょう。いずれにしても大切なことは、セキュリティ対策は、企業の規模や業種を問わず普遍的なものであるということです。リスク評価を行い、自組織にとって最適な対策を見極め、過少でも過度でもない適切な出費を行うことこそが重要であると考えます。

i https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf〔2025/7/10 確認〕

※ 1　https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf〔2025/6/26 確認〕
※ 2　内閣官房：国家安全保障戦略について　https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf〔2025/6/26 確認〕
※ 3　e-Gov 法令検索：重要電子計算機に対する不正な行為による被害の防止に関する法律（令和七年法律第四十二号）　https://laws.e-gov.go.jp/law/507AC0000000042/20271122_000000000000000〔2025/6/26 確認〕
※ 4　内閣府：官報 令和７年５月23日号外第113号（p.75）　https://www.kanpo.go.jp/20250523/20250523g00113/20250523g001130075f.html〔2025/6/26 確認〕
※ 5　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html〔2025/6/26 確認〕
※ 6　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf〔2025/6/26 確認〕
※ 7　https://www.nisc.go.jp/pdf/policy/kihon-s/250529kikkin.pdf〔2025/6/26 確認〕
※ 8　NCO：国家サイバー統括室の設置について　https://www.nisc.go.jp/pdf/press/NCO0701.pdf〔2025/7/2 確認〕
NCO：概要　https://www.nisc.go.jp/about/overview/index.html〔2025/7/2 確認〕
※ 9　国会審議の過程で、衆議院において、サイバー対処能力強化法案に通信の秘密の尊重（第２条の２）等の規定を追加する修正が行われた。衆議院：閣法 第 217 回国会 4 重要電子計算機に対する不正な行為による被害の防止に関する法律案に対する修正案　https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/syuuseian/11_7CD2.htm〔2025/6/26 確認〕
※ 10 内閣官房：サイバー対処能力強化法及び同整備法について　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf〔2025/6/26 確認〕
※ 11 https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/shin_cyber_leaflet.pdf〔2025/6/26 確認〕
※ 12 https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/gaiyou.pdf〔2025/6/10 確認〕
※ 13 内閣官房：サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など）　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html〔2025/6/26 確認〕
※ 14 経済安全保障推進法に基づき指定される、基幹インフラ事業（15事業）を行う者のうち、特定重要設備（役務の安定的な提供のために重要であり、役務の安定的な提供を妨害する行為の手段として使用されるおそれがあるもの）の機能が停止・低下した場合に、役務の安定的な提供に支障が生じ、国家・国民の安全を損なうおそれが大きいものとして主務省令で定める基準に該当する者。2025 年５月時点で 249 者。
内閣官房：サイバー対処能力強化法及び同整備法について　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf〔2025/6/26 確認〕
※ 15 柿沼重志：能動的サイバー防御の導入（立法と調査 474 号）　https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2025pdf/20250414003.pdf〔2025/6/26 確認〕
※ 16 https://laws.e-gov.go.jp/law/426AC1000000104〔2025/6/26 確認〕
※ 17 サイバーセキュリティ戦略本部：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）　https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf〔2025/6/26 確認〕
※ 18 NISC：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）　https://www.nisc.go.jp/pdf/policy/general/guider6.pdf〔2025/6/26 確認〕
※ 19 NISC：「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」　https://www.nisc.go.jp/policy/group/general/sbd_sakutei.html〔2025/6/26 確認〕
※ 20 NISC：横断的アタックサーフェスマネジメント（ASM）事業の運用開始に係るプレスリリース　https://www.nisc.go.jp/pdf/press/20240719NISC_press.pdf〔2025/6/26 確認〕
※ 21 NISC：2024 年度 官民連携演習等 実施結果　https://www.nisc.go.jp/pdf/policy/infra/NISC_enshu_20250527.pdf〔2025/6/26 確認〕
※ 22 https://www.mhlw.go.jp/content/10808000/001262036.pdf〔2025/6/26 確認〕
※ 23 https://www.mhlw.go.jp/content/10808000/001262037.pdf〔2025/6/26 確認〕
※ 24 https://www.mhlw.go.jp/content/10808000/001261299.pdf〔2025/6/26 確認〕
※ 25 https://mist.mhlw.go.jp/〔2025/6/26 確認〕
※ 26 https://www.meti.go.jp/shingikai/mono_info_service/medical_information_system/checklist.html〔2025/6/26 確認〕
※ 27 e-Gov 法令検索：地方自治法（昭和二十二年法律第六十七号）　https://laws.e-gov.go.jp/law/322AC0000000067/20261225_506AC0000000065〔2025/6/26 確認〕
※ 28 AISI：AI セーフティに関する評価観点ガイド（第 1.00 版）　https://aisi.go.jp/assets/pdf/ai_safety_eval_v1.00_ja.pdf〔2025/6/26 確認〕
なお、2025 年３月に、マルチモーダル基盤モデルに対して AI セーフティ評価を行う際に重要となる評価観点及び評価項目例を追記した第 1.10 版が公開されている（AISI:AI セーフティに関する評価観点ガイド（第 1.10 版）　https://aisi.go.jp/assets/pdf/ai_safety_eval_v1.10_ja.pdf〔2025/6/26 確認〕）。
※ 29 AISI：AI セーフティに関するレッドチーミング手法ガイド（第 1.00 版）　https://aisi.go.jp/assets/pdf/ai_safety_RT_v1.00_ja.pdf〔2025/6/26 確認〕
なお、2025 年３月に、画像等のマルチモーダル情報に関する攻撃手法等の追記に加え、新たに作成した詳細解説書やレッドチーミングの成果物例を含めた第 1.10 版が公開されている（AISI：AI セーフティに関するレッドチーミング手法ガイド（第 1.10 版）の公開　https://aisi.go.jp/effort/effort_information/250331_1/〔2025/6/26 確認〕）。
※ 30 経済産業省：IoT 製品に対するセキュリティラベリング制度（JC-STAR）の運用を開始しました　https://www.meti.go.jp/press/2024/03/20250325007/20250325007.html〔2025/6/26 確認〕
※ 31 経済産業省：第9回産業サイバーセキュリティ研究会 事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/009_03_00.pdf〔2025/6/26 確認〕
※ 32 総務省：令和6年度医療分野向けサイバーセキュリティ演習のご案内　https://www.jmha.or.jp/contentsdata/keiei/dx/cynex_sankousiryou.pdf〔2025/6/26 確認〕
※ 33 https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf〔2025/6/26 確認〕
※ 34 2025 年３月に開催された第 15 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において、「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）」（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/015_s01_00.pdf〔2025/6/26 確認〕）が提示された。
※ 35 e-Gov 法令検索：国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）　https://laws.e-gov.go.jp/law/411AC0000000162〔2025/6/26 確認〕
※ 36 NICT：IoT 機器のセキュリティ向上を推進する新しい「NOTICE」を開始　https://www.nict.go.jp/press/2024/03/29-2.html〔2025/6/26 確認〕
※ 37 NOTICE：NOTICE の取り組みに、新たに IoT 機器メーカー・関連団体からも参加いただきました　https://notice.go.jp/news/topic/news20240828_2〔2025/6/26 確認〕
※ 38 C&C サーバー：Command and Control サーバーの略。マルウェア等により乗っ取ったコンピューター等に対し、遠隔から命令を送り制御するサーバー。
※ 39 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（分析事業者の拡大）　https://www.ict-isac.jp/news/news20240625.html〔2025/6/26 確認〕
※ 40 IPA：登録番号 2024-　https://www.ipa.go.jp/security/sme/otasuketai/servicelist/category2/registration-number2024.html〔2025/6/26 確認〕
※ 41 例えば、政府広報ラジオ番組「杉浦太陽・村上佳菜子 日曜まなびより」2月16日（日曜日）放送「備えて安心!中小企業のサイバーセキュリティお助け隊サービス」（https://www.gov-online.go.jp/article/202502/radio-2765.html〔2025/6/26 確認〕）、日経ビジネス広告記事「中小企業のサイバーセキュリティー対策『お助け隊サービス』で中小企業をサイバー攻撃から守る」（https://special.nikkeibp.co.jp/atclh/ONB/25/gov_online0214/〔2025/6/26 確認〕）。
※ 42 経済産業省:第11回産業サイバーセキュリティ研究会WG2（地域・中小企業支援）事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/011_03_00.pdf#page=30〔2025/6/26 確認〕
※ 43 IPA：サイバーセキュリティ相談会・マネジメント指導　https://www.ipa.go.jp/security/seminar/sme/riss-katsuyo.html〔2025/6/26 確認〕
※ 44 NISC、警察庁：人権保護や民主主義の推進に関与する組織や個人のためのサイバー脅威緩和に関する国際ガイダンスへの共同署名について　https://www.nisc.go.jp/pdf/press/press_Mitigating_Threats.pdf〔2025/6/26 確認〕
※ 45 NISC、警察庁：豪州主導の APT40 グループに関する国際アドバイザリーへの共同署名について　https://www.nisc.go.jp/pdf/press/press_APT40Advisory.pdf〔2025/6/26 確認〕

※ 46 NISC、警察庁、外務省：「カウンターランサムウェア・イニシアティブ会合」への参加　https://www.nisc.go.jp/pdf/press/press_cri_statement_20241003.pdf〔2025/6/26 確認〕
※ 47 NISC：北朝鮮による暗号資産窃取及び官民連携に関する共同声明　https://www.nisc.go.jp/pdf/news/press/250114_jointstatement_jpn.pdf〔2025/6/26 確認〕
※ 48 NISC：英国主導の「サイバーセキュリティ人材に関する国際的な連合」への参画について　https://www.nisc.go.jp/pdf/press/2025_International_Coalition_on_Cyber_Security_Workforces.pdf〔2025/6/26 確認〕
※ 49 外務省：日本のサイバー分野での外交　二国間協議・対話等 https://www.mofa.go.jp/mofaj/fp/nsp/page24_000687.html〔2025/6/26 確認〕
※ 50 外務省：第３回北朝鮮サイバー脅威に関する日米韓外交当局間作業部会の開催　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_01135.html〔2025/6/26 確認〕
※ 51 外務省：G7 プーリア・サミット（概要）　https://www.mofa.go.jp/mofaj/ecm/ec/pageit_000001_00752.html〔2025/6/26 確認〕
※ 52 National Cybersecurity Agency：G7 cybersecurity working group　https://www.acn.gov.it/portale/en/w/gruppo-di-lavoro-g7-sulla-cybersicurezza〔2025/6/26 確認〕
※ 53 National Cybersecurity Agency：Press statement of the President of the G7 Cybersecurity Working Group, Bruno Frattasi　https://www.acn.gov.it/portale/en/w/dichiarazione-alla-stampa-del-presidente-del-gruppo-di-lavoro-g7-sulla-cybersicurezza-bruno-frattasi〔2025/6/26 確認〕
※ 54 NISC、総務省、経済産業省：第 17 回　日 ASEAN サイバーセキュリティ政策会議の結果　https://www.nisc.go.jp/pdf/press/17thAJCPM_ja.pdf〔2025/6/26 確認〕
※ 55 経済産業省：「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました　https://www.meti.go.jp/press/2024/11/20241115001/20241115001.html〔2025/6/26 確認〕
※ 56 警察庁：令和6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/R6/R06_cyber_jousei.pdf〔2025/6/26 確認〕
※ 57 https://laws.e-gov.go.jp/law/504AC0000000043〔2025/6/26 確認〕
※ 58 https://laws.e-gov.go.jp/law/506AC0000000027〔2025/6/26 確認〕
※ 59 内閣府：経済安全保障推進法に基づく重要物資の安定的な供給の確保（サプライチェーン強靱化）に関する制度全般や技術流出防止について　https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/supply_chain/doc/sc_gaiyou.pdf〔2025/6/26 確認〕
※ 60 https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html〔2025/6/26 確認〕
※ 61 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 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_next_3.pdf〔2025/6/26 確認〕
※ 62 JST：経済安全保障重要技術育成プログラム（K Program）における新規採択課題の決定について（令和5年度第3回募集 AIセキュリティ）　https://www.jst.go.jp/pr/info/info1712/pdf/info1712.pdf〔2025/6/26 確認〕
※ 63 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_next_2.pdf〔2025/6/26 確認〕
※ 64 JST：経済安全保障重要技術育成プログラム（K Program）における新規採択課題の決定について（令和5年度第2回募集）　https://www.jst.go.jp/pr/info/info1697/pdf/info1697.pdf〔2025/6/26 確認〕
JST：経済安全保障重要技術育成プログラム（K Program）における新規採択課題の決定について（令和5年度第4回募集、令和6年度第3回募集）　https://www.jst.go.jp/pr/info/info1749/pdf/info1749.pdf〔2025/6/26 確認〕
※ 65 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_next.pdf〔2025/6/26 確認〕
※ 66 JST：経済安全保障重要技術育成プログラム（K Program）における新規採択課題の決定について（令和5年度第4回募集、令和6年度第1回募集）　https://www.jst.go.jp/pr/info/info1747/pdf/info1747.pdf〔2025/6/26 確認〕
※ 67 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〔2025/6/26 確認〕
※ 68 NEDO：「経済安全保障重要技術育成プログラム」で偽情報の分析に係る技術の開発に着手 ―複数の根拠から真偽判定を支援する偽情報対策システムの開発を目指す―　https://www.nedo.go.jp/news/press/AA5_101763.html〔2025/6/26 確認〕
※ 69 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〔2025/6/26 確認〕
※ 70 NEDO：「経済安全保障重要技術育成プログラム」で先進的サイバー防御機能・分析能力強化に着手　―自由、公正かつ安全なサイバー空間の確保を目指す―　https://www.nedo.go.jp/news/press/AA5_101762.html〔2025/6/26 確認〕
※ 71 「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施行令（令和四年政令第三百九十四号）」（https://laws.e-gov.go.jp/law/504C00000000394〔2025/6/26 確認〕）の第 12 条第 1 項参照。
※ 72 本文に掲げた技術についての調査結果は、「令和6年度特定技術分野における産業の発達への影響に関する調査　ー耐タンパ性ハウジングにより計算機の部品等を保護する技術ー」（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/patent/doc/patent_sangyou_r6_4.pdf〔2025/6/26 確認〕）及び「令和6年度特定技術分野における産業の発達への影響に関する調査　ー通信妨害等に関する技術ー」（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/patent/doc/patent_sangyou_r6_5.pdf〔2025/6/26 確認〕）として公表された。
※ 73 https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/torimatome.pdf〔2025/6/26 確認〕
※ 74 セキュリティ・クリアランス制度：国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として指定された情報に対して、アクセスする必要がある者のうち、情報を漏らすおそれがないという信頼性を確認した者の中で取り扱うとする制度。
内閣府：いわゆる「セキュリティ・クリアランス」について　https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/sankou_clearance.pdf〔2025/6/26 確認〕
※ 75 国会審議の過程で、衆議院において、内閣総理大臣による「重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定の状況」の国会への報告（第 19 条）等を追加する修正が行われた。
衆議院：閣法 第 213 回国会 24 重要経済安保情報の保護及び活用に関する法律案に対する修正案（自民、立憲、維教、公明、国民、有志）　https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/syuuseian/1_8466.htm〔2025/6/26 確認〕。
※ 76 https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/sankou_hyouka.pdf〔2025/6/26 確認〕
※ 77 内閣府：重要経済安保情報の保護及び活用に関する法律の概要　https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/gaiyo.pdf〔2025/6/26 確認〕
※ 78 内閣府：重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定に関し、統一的な運用を図るための基準の策定について　https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/kijun.pdf〔2025/6/26 確認〕
※ 79 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/〔2025/6/4 確認〕
※ 80 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a547f9a6/20250630_resources_standard_guidelines_technical_report_01.pdf〔2025/7/1 確認〕
※ 81 https://www.nisc.go.jp/policy/group/general/kijun.html〔2025/6/4 確認〕
※ 82 https://www.digital.go.jp/resources/standard_guidelines/#ds202〔2025/6/4 確認〕
※ 83 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/2aa40167/20250630_resources_standard_guidelines_technical_report_02.pdf〔2025/7/1〕
※ 84 IIA（一般社団法人日本内部監査協会訳）：IIA の３ラインモデル https://www.iiajapan.com/leg/pdf/data/iia/2020.07_1_Three-Lines-Model-Updated-Japanese.pdf〔2025/6/4 確認〕
※ 85 https://www.digital.go.jp/policies/security/comprehensive-operational-synthetic-monitoring-system〔2025/6/4 確認〕
※ 86 https://www.digital.go.jp/policies/security/crsa〔2025/6/4 確認〕
※ 87 経済産業省：産業サイバーセキュリティ研究会　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/index.html〔2025/7/1 確認〕
※ 88 経済産業省：第９回 産業サイバーセキュリティ研究会　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/009.

html〔2025/7/1 確認〕
※ 89 経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_semiconductor/pdf/002_06_00.pdf〔2025/7/1 確認〕
※ 90 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　https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html〔2025/7/1 確認〕
※ 91 NIST：The NIST Cybersecurity Framework (CSF) 2.0 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf〔2025/7/1 確認〕
※ 92 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/index.html〔2025/7/1 確認〕
※ 93 https://www.meti.go.jp/press/2025/04/20250414002/20250414002-2.pdf〔2025/7/1 確認〕
※ 94 経済産業省：第 18 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/018.html〔2025/7/1 確認〕
※ 95 経済産業省：第 8 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）工場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_kojo/008.html〔2025/7/1 確認〕
※ 96 https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.0.pdf〔2025/7/1 確認〕
※ 97 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240823_1.pdf〔2025/7/1 確認〕
※ 98 経済産業省：サイバー攻撃への備えを!「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました　https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html〔2025/7/1 確認〕
※ 99 経済産業省：第 15 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/015.html〔2025/7/1 確認〕
※ 100 NIST：Secure Software Development Framework (SSDF) Version 1.1:　https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf〔2025/7/1 確認〕
※ 101 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/015_s01_00.pdf〔2025/7/1 確認〕
※ 102 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/cyber_infrastructure/pdf/202503_g2.pdf〔2025/7/1 確認〕
※ 103 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/enhanced_security/index.html〔2025/7/1 確認〕
※ 104 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/enhanced_security/pdf/20250305_2.pdf〔2025/7/1 確認〕
※ 105 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/index.html〔2025/7/1 確認〕
※ 106 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/〔2025/7/1 確認〕
※ 107 https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/08.pdf〔2025/7/1 確認〕
※ 108 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。
※ 109 https://www.ipa.go.jp/security/j-csip/about.html〔2025/6/4 確認〕
※ 110 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〔2025/6/4 確認〕
※ 111 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〔2025/6/4 確認〕
※ 112 https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf〔2025/7/3 確認〕
※ 113 https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html〔2025/7/3 確認〕
※ 114 https://www.ipa.go.jp/security/guide/ps6vr70000011k4i-att/000059695.pdf〔2025/7/3 確認〕
※ 115 https://www8.cao.go.jp/cstp/aigensoku.pdf〔2025/7/1 確認〕
※ 116 https://www.ipa.go.jp/disc/committee/expert-group-on-aigfb.html〔2025/7/1 確認〕
※ 117 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_1.pdf〔2025/7/1 確認〕
※ 118 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf〔2025/7/1 確認〕
※ 119 経済産業省：不正競争防止小委員会　https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/fusei_kyoso/index.html〔2025/7/1 確認〕
※ 120 https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf〔2025/7/1 確認〕
※ 121 https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/fusei_kyoso/pdf/027_03_01.pdf〔2025/7/1 確認〕
※ 122 経済産業省：サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携に関する協定書　https://www.meti.go.jp/press/2024/12/20241227001/20241227001-1.pdf〔2025/7/1 確認〕
※ 123 防衛省：サイバーセキュリティ分野における経済産業省との連携強化について（サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携）　https://www.mod.go.jp/j/press/news/2024/12/27b_02.pdf〔2025/7/1 確認〕
※ 124 https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_6.0_published.pdf〔2025/7/1 確認〕
※ 125 総務省：「ICT サイバーセキュリティ政策の中期重点方針」（案）に対する意見募集の結果及び「ICT サイバーセキュリティ政策の中期重点方針」の公表　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00219.html〔2025/6/4 確認〕
総務省：ICT サイバーセキュリティ政策の中期重点方針　https://www.soumu.go.jp/main_content/000960379.pdf〔2025/6/4 確認〕
※ 126 https://notice.go.jp〔2025/6/4 確認〕
※ 127 衆議院：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　https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/21220231215087.htm〔2025/6/4 確認〕
※ 128 https://www.ipa.go.jp/publish/wp-security/2024.html〔2025/6/4 確認〕
※ 129 NOTICE：最近の観測状況　https://notice.go.jp/status〔2025/6/4 確認〕
※ 130 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。
ICT サイバーセキュリティ政策分科会：ICT サイバーセキュリティ政策の中期重点方針　https://www.soumu.go.jp/main_content/000960379.pdf〔2025/6/4 確認〕
※ 131 総務省：スマートフォン　プライバシー　https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/smartphone_privacy.html〔2025/6/4 確認〕
※ 132 https://www.soumu.go.jp/main_content/000942602.pdf〔2025/6/4 確認〕
※ 133 自然人：民法上、権利義務の主体となることができる人を指し、法人と自然人が含まれる。自然人は個人のこと。
図解六法：人・者・自然人・法人　https://www.zukairoppo.com/glossary-hito〔2025/6/4 確認〕
※ 134 https://www.soumu.go.jp/main_content/001000541.pdf〔2025/6/4 確認〕
※ 135 総務省：NICT サイバーセキュリティ研究所の取り組み　https://www.soumu.go.jp/main_content/000952545.pdf〔2025/6/4 確認〕
※ 136 GSOC（Government Security Operation Coordination team）：24 時間 365 日、政府横断的な情報収集、攻撃の分析、政府機関への助言等を行うため、NISC に設置された体制。
NISC：別添8 用語解説 GSOC（Government Security Operation Coordination team：ジーソック）　https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024-8.pdf〔2025/6/4 確認〕
※ 137 総務省：「スマートシティセキュリティガイドライン（第 3.0 版）」（案）に対する意見募集の結果及び「スマートシティガイドライン（第 3.0 版）」の公表　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00215.html〔2025/6/4 確認〕
※ 138 https://www.soumu.go.jp/main_content/000955126.pdf〔2025/6/4 確認〕
※ 139 総務省：「地方公共団体における情報セキュリティポリシーに関するガイドライン」等の意見募集の結果及び改定版の公表　https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000355.html〔2025/6/4 確認〕
※ 140 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〔2025/6/4 確認〕
※ 141 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〔2025/6/4 確認〕

※ 142 警察庁：令和６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/R6kami/R06_kami_cyber_jousei.pdf〔2025/6/4 確認〕
※ 143 国家公安委員会、警察庁：令和６年版 警察白書　https://www.npa.go.jp/hakusyo/r06/index.html〔2025/6/4 確認〕
※ 144 警察庁：サイバー特別捜査部とは　https://www.npa.go.jp/bureau/cyber/what-we-do/about_ncu.html〔2025/6/4 確認〕
※ 145 警察庁：不正アクセス行為対策等の実態調査 アクセス制御機能に関する技術の研究開発の状況等に関する調査 調査報告書　https://www.npa.go.jp/bureau/cyber/pdf/R6countermeasures.pdf〔2025/6/4 確認〕
※ 146 警察庁：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況　https://www.npa.go.jp/news/release/2024/20240314.pdf〔2025/6/4 確認〕
※ 147 警察庁：フィッシング対策　https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html〔2025/6/4 確認〕
※ 148 https://www.jc3.or.jp/〔2025/6/4 確認〕
※ 149 https://www.internethotline.jp/〔2025/6/4 確認〕
※ 150 警察庁、NISC：MirrrorFace 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/20250108_caution.pdf〔2025/6/4 確認〕
※ 151 警察庁：サイバーテロ対策協議会　https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/katsudo/cyber/index.html〔2025/6/4 確認〕
※ 152 警察庁：サイバーフォース　https://www.npa.go.jp/bureau/cyber/what-we-do/cyberforce.html〔2025/6/4 確認〕
※ 153 サイバー犯罪：警察庁による定義では「不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪」を指す。
※ 154 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〔2025/6/4 確認〕
※ 155 サイバー事案：警察庁による定義では「サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案」を指す。
※ 156 警察庁:特殊詐欺等の被害拡大防止を目的とした株式会社ゆうちょ銀行との「情報連携協定書」締結について　https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/jyouhourenkei250117.pdf〔2025/6/4 確認〕
※ 157 警察庁：令和６年における特殊詐欺及び SNS 型投資・ロマンス詐欺の認知・検挙状況について（暫定値版）　https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2024.pdf〔2025/6/4 確認〕
※ 158 ACSC：APT40 Advisory PRC MSS tradecraft in action　https://www.cyber.gov.au/sites/default/files/2024-07/apt40-advisory-prc-mss-tradecraft-in-action.pdf〔2025/6/4 確認〕
※ 159 警察庁：ナイジェリアとの国際共同捜査について　https://www.npa.go.jp/news/release/2025/release.pdf〔2025/6/4 確認〕
※ 160 NHK：インターポールと JICA ロマンス詐欺などの捜査力向上へ支援　https://www3.nhk.or.jp/news/html/20240728/k10014527031000.html〔2025/6/4 確認〕
※ 161 警察庁：DDoS 攻撃ウェブサービスに関する国際共同捜査について　https://www.npa.go.jp/news/release/2024/20241206001.html〔2025/6/4 確認〕
※ 162 警察庁：豪州主導国際文書「OT サイバーセキュリティの原則」への共同署名について　https://www.npa.go.jp/news/release/2024/caution20240913.html〔2025/6/4 確認〕
※ 163 読売新聞オンライン：生成AI悪用しウイルス作成、警視庁が25歳の男を容疑で逮捕…設計情報を回答させたか　https://www.yomiuri.co.jp/news/national/20240528-OYT1T50015/〔2025/6/4 確認〕
※ 164 読売新聞オンライン：大手銀行のネットバンキングに不正アクセス容疑、指示役の男逮捕…警察庁サイバー特捜部など　https://www.yomiuri.co.jp/national/20240709-OYT1T50166/〔2025/8/4 確認〕
朝日新聞：ネット不正送金の指示役逮捕　詐欺グループ全体、異例の摘発　警察庁　https://www.asahi.com/articles/ASS791S95S79UTIL01VM.html〔2025/6/4 確認〕
※ 165 日本経済新聞：災害時の SNS デマ、警察が厳格姿勢　安易な拡散は要注意　https://www.nikkei.com/article/DGXZQOUE242390U4A720C2000000/〔2025/6/4 確認〕
朝日新聞：能登半島地震で SNS にうその投稿の男性、罰金 20 万円　輪島簡裁　https://www.asahi.com/articles/ASSC11GTLSC1PJLB001M.html〔2025/6/4 確認〕
※ 166 ScanNetSecurity:警察庁、総務省それぞれの最新の取り組みは?官民連携、国際連携を通してより安全なサイバー空間の実現を ～JPAAWG 6th General Meeting レポート　https://scan.netsecurity.ne.jp/article/2024/04/02/50805.html〔2025/6/4 確認〕
※ 167 https://www.kantei.go.jp/jp/singi/hanzai/kettei/240618/honbun.pdf〔2025/6/4 確認〕
※ 168 https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study〔2025/6/4 確認〕
※ 169 ISC2, Inc.：Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen　https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen〔2025/6/4 確認〕
※ 170 https://juas.or.jp/cms/media/2025/04/JUAS_IT2025.pdf〔2025/6/6 確認〕
※ 171 レバテック株式会社：「セキュリティ」が転職求人倍率 1 位に、50 倍超えの高需要　https://levtech.jp/partner/guide/research/detail/303/〔2025/6/4 確認〕
※ 172 IPA：「DX 動向 2024」進む取組、求められる成果と変革　https://www.ipa.go.jp/digital/chousa/dx-trend/dx-trend-2024.html〔2025/6/4 確認〕
※ 173 IDC Japan 株式会社：国内市場におけるエッジコンピューティングへの投資は、2024 年に 1 兆 6 千億円と予測～国内エッジインフラ市場予測を発表～　https://my.idc.com/getdoc.jsp?containerId=prJPJ51979224〔2025/6/4 確認〕
※ 174 https://www.global-nikkei.com/cit/24/〔2025/6/4 確認〕
※ 175 日本経済新聞：サイバー防御の強化　防衛相「人材育成が基盤」　https://www.nikkei.com/article/DGKKZO85061580W4A121C2EP0000/〔2025/6/4 確認〕
※ 176 日本経済新聞:企業のサイバー対策、経産相「事業活動に不可欠」　https://www.nikkei.com/article/DGKKZO85085330X21C24A1EP0000/〔2025/6/4 確認〕
※ 177 IPA：「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について　https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html〔2025/6/4 確認〕
※ 178 パロアルトネットワークス株式会社：日本国内の中小企業のサイバーセキュリティに関する実態調査 2024 年版　https://www.paloaltonetworks.jp/content/dam/pan/ja_JP/PressRelease/2024-ecosystem-sme-press-release-supplement.pdf〔2025/6/4 確認〕
※ 179 経済産業省：第 1 回産業サイバーセキュリティ研究会ワーキンググループ 2（経営・人材・国際）サイバーセキュリティ人材の育成促進に向けた検討会事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/pdf/001_04_00.pdf〔2025/6/4 確認〕
※ 180 IPA：セキュリティ・キャンプ　https://www.ipa.go.jp/jinzai/security-camp/index.html〔2025/6/4 確認〕
※ 181 経済産業省：サイバーセキュリティ人材の育成促進に向けたこれまでの議論の整理と継続的な検討事項　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/pdf/003_03_00.pdf〔2025/6/4 確認〕
※ 182 IPA：中小企業の情報セキュリティ対策ガイドライン第 3.1 版　https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf〔2025/6/4 確認〕
※ 183 経済産業省：ワーキンググループ 2（サイバーセキュリティ人材の育成促進に向けた検討会）最終取りまとめ　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/20250514_report.html〔2025/6/4 確認〕
※ 184 経済産業省：サイバーセキュリティ人材の育成促進に向けた検討会における検討状況について　https://www.meti.go.jp/shingikai/mono_info_service/society_digital/digital_skill/pdf/005_02_00.pdf〔2025/6/4 確認〕
※ 185 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。
※ 186 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 21 日及び秋期 10 月 13 日に実施した。
※ 187 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６年度試験 全試験区分版）　https://www.ipa.go.jp/shiken/reports/nq6ept000000i5c9-att/toukei_r06.pdf〔2025/6/4 確認〕
※ 188 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。
※ 189 IPA：国家資格「情報処理安全確保支援士」2025 年 4 月 1 日付新規登録者 1,173 名の内訳　https://www.ipa.go.jp/jinzai/riss/

reports/data/20250401newriss.html〔2025/6/4 確認〕
※ 190 IPA：講習の目的と概要 https://www.ipa.go.jp/jinzai/riss/forriss/koushu/overview.html〔2025/6/4 確認〕
※ 191 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〔2025/6/4 確認〕
※ 192 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〔2025/6/4 確認〕
※ 193 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〔2025/6/4 確認〕
※ 194 IPA：登録セキスペインタビュー https://www.ipa.go.jp/jinzai/riss/interview/riss.html〔2025/6/4 確認〕
※ 195 IPA：活用企業・組織のインタビュー https://www.ipa.go.jp/jinzai/riss/interview/soshiki/index.html〔2025/6/4 確認〕
※ 196 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〔2025/6/5 確認〕
※ 197 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〔2025/6/5 確認〕
※ 198 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〔2025/6/5 確認〕
※ 199 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〔2025/6/5 確認〕
※ 200 IPA：実務者向けプログラム ERAB サイバーセキュリティトレーニング 事業内容 https://www.ipa.go.jp/jinzai/ics/short-pgm/erab/index.html〔2025/6/5 確認〕
※ 201 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/007_05_04.pdf〔2025/6/5 確認〕
※ 202 IPA：セキュリティ・キャンプ 2024 全国大会 https://www.ipa.go.jp/jinzai/security-camp/2024/camp/zenkoku/index.html〔2025/6/5 確認〕
※ 203 セキュリティ・キャンプ協議会：セキュリティ・キャンプ キャンプレポート https://www.security-camp.or.jp/camp/index.html〔2025/6/5 確認〕
※ 204 IPA：セキュリティ・キャンプ 2024 ネクスト https://www.ipa.go.jp/jinzai/security-camp/2024/camp/next/index.html〔2025/6/5 確認〕
※ 205 IPA：セキュリティ・キャンプ 2024 ジュニア https://www.ipa.go.jp/jinzai/security-camp/2024/camp/junior/index.html〔2025/6/5 確認〕
※ 206 セキュリティ・キャンプ協議会：地方大会 https://www.security-camp.or.jp/minicamp/〔2025/6/5 確認〕
※ 207 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 2024 https://www.security-camp.or.jp/minicamp/tokyo2024.html〔2025/6/5 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 宮城 2024 https://www.security-camp.or.jp/minicamp/miyagi2024.html〔2025/6/5 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 2024 https://www.security-camp.or.jp/minicamp/mie2024.html〔2025/6/5 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 2024 https://www.security-camp.or.jp/minicamp/hiroshima2024.html〔2025/6/5 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 愛知 2024 https://www.security-camp.or.jp/minicamp/aichi2024.html〔2025/6/5 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 2024 https://www.security-camp.or.jp/minicamp/yamanashi2024.html〔2025/6/5 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 2024 https://www.security-camp.or.jp/minicamp/okinawa2024.html〔2025/6/5 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 岩手 2024 https://www.security-camp.or.jp/minicamp/iwate2024.html〔2025/6/5 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 2024 https://www.security-camp.or.jp/minicamp/hokkaido2024.html〔2025/6/5 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 熊本 2024 https://www.security-camp.or.jp/minicamp/kumamoto2024.html〔2025/6/5 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 2024 https://www.security-camp.or.jp/minicamp/ishikawa2024.html〔2025/6/5 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 2025 https://www.security-camp.or.jp/minicamp/osaka2025.html〔2025/6/5 確認〕
※ 208 IPA：セキュリティ・キャンプフォーラム 2025 https://www.ipa.go.jp/jinzai/security-camp/2024/forum2025.html〔2025/6/5 確認〕
※ 209 セキュリティ・キャンプ協議会：GCC 2025 Taiwan - Global Cybersecurity Camp 2025 Taiwan https://www.security-camp.or.jp/event/gcc_taiwan2025.html〔2025/6/5 確認〕
※ 210 https://cynex.nict.go.jp/〔2025/6/5 確認〕
※ 211 NICT：社会実装・外部連携等に関する NICT の取組について https://www.soumu.go.jp/main_content/000987147.pdf〔2025/6/5 確認〕
※ 212 NICT：2024 年度 実践的サイバー防御演習「CYDER」の受講申込受付を開始 https://www.nict.go.jp/press/2024/05/14-1.html〔2025/6/5 確認〕
※ 213 NICT：プレ CYDER 後半が開講しました https://cyder.nict.go.jp/news/2024/post_11.html〔2025/6/5 確認〕
※ 214 NICT：ナショナルサイバートレーニングセンター https://nct.nict.go.jp/〔2025/6/5 確認〕
※ 215 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〔2025/6/5 確認〕
※ 216 NICT：SecHack365 の目的 https://sechack365.nict.go.jp/document/〔2025/6/5 確認〕
※ 217 NICT：集合イベントレポート https://sechack365.nict.go.jp/report/〔2025/6/5 確認〕
※ 218 NICT：SecHack365 2024 年度 成果発表会 https://sechack365.nict.go.jp/presentation/〔2025/6/5 確認〕
※ 219 SECCON：セキュリティコンテスト SECCON 実行委員会とは https://www.seccon.jp/13/seccon/executivecommittee.html〔2025/6/5 確認〕
※ 220 SECCON：SECCON と は https://www.seccon.jp/13/seccon/about.html〔2025/6/5 確認〕
※ 221 SECCON：本年度より、SECCON の呼称を西暦から連番といたします。 https://www.seccon.jp/13/seccon.html
※ 222 SECCON：SECCON 13 開催スケジュール https://www.seccon.jp/13/seccon/schedule.html〔2025/6/5 確認〕
※ 223 SECCON：SECCON 13 電脳会議 https://www.seccon.jp/13/ep250301.html〔2025/6/5 確認〕
※ 224 SECCON：SECCON CTF 13 予選のお知らせ https://www.seccon.jp/13/seccon_ctf/quals.html〔2025/6/5 確認〕
※ 225 SECCON：SECCON Beginners とは https://www.seccon.jp/13/beginners/about-seccon-beginners.html〔2025/6/5 確認〕
※ 226 SECCON：CTF for GIRLS とは https://www.seccon.jp/13/girls/ctf-for-girls.html〔2025/6/5 確認〕
※ 227 SECCON：SECCONCON とは https://www.seccon.jp/13/seccon/secconcon.html〔2025/6/5 確認〕
※ 228 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〔2025/6/5 確認〕
※ 229 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〔2025/6/5 確認〕
※ 230 IPA：セキュリティ要件適合評価及びラベリング制度（JC-STAR） https://www.ipa.go.jp/security/jc-star/index.html〔2025/6/6 確認〕
※ 231 総務省：令和 6 年版 情報通信白書｜データ集 第Ⅱ部第 1 章第 5 節 41. 世界の IoT デバイス数の推移及び予測 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00246〔2025/6/6 確認〕
※ 232 NICT：NICTER 観測レポート 2024 の公開 https://www.nict.go.jp/press/2025/02/13-1.html〔2025/6/6 確認〕
※ 233 CNET：That massive internet outage, explained https://www.cnet.com/tech/computing/what-is-a-ddos-attack/〔2025/6/6 確認〕
※ 234 https://www.ipa.go.jp/security/10threats/10threats2025.html〔2025/6/6 確認〕
※ 235 https://notice.go.jp/〔2025/6/6 確認〕
※ 236 サプライチェーン・リスク：「サイバー空間を構成するシステムのサプライチェーンの複雑化やグローバル化を通じ、サプライチェーンの過程で製品に不正機能等が埋め込まれるリスクや政治経済情勢による機器・サービスの供給途絶など、サイバー空間自体の信頼性や供給安定性に係るリ

スク」とされる。
NISC：サイバーセキュリティ戦略（令和３年９月28日閣議決定） https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf〔2025/6/6 確認〕
※ 237 経済産業省：ワーキンググループ３（IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会） https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html〔2025/6/6 確認〕
※ 238 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html〔2025/6/6 確認〕
※ 239 IPA：申請手続き・報告手続き https://www.ipa.go.jp/security/jc-star/shinsei/index.html〔2025/7/11 確認〕
※ 240 https://www.ipa.go.jp/security/jc-star/list/jc-star-product-list/index.html〔2025/7/11 確認〕
※ 241 https://www.meti.go.jp/policy/netsecurity/chusyosecurityguide_r6.pdf〔2025/6/6 確認〕
※ 242 https://www.ipa.go.jp/security/jc-star/detail.html〔2025/6/6 確認〕
※ 243 IPA：欧州規格 ETSI EN 303 645 V2.1.1（2020-06）の翻訳 https://www.ipa.go.jp/security/controlsystem/etsien303645.html〔2025/6/6 確認〕
※ 244 米国国立標準技術研究所（NIST：National Institute of Standards and Technology）：NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products https://csrc.nist.gov/pubs/ir/8425/final〔2025/6/6 確認〕
※ 245 European Commission:Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act〔2025/6/6 確認〕
※ 246 https://www.ipa.go.jp/security/jc-star/begoj9000000gg60-att/JC-STARsetumeikai_1.pdf〔2025/6/6 確認〕
※ 247 https://www.soumu.go.jp/main_content/001000932.pdf〔2025/6/6 確認〕
※ 248 https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/20250522.pdf〔2025/6/6 確認〕
※ 249 https://www.nisc.go.jp/pdf/policy/infra/rmtebiki202307.pdf〔2025/6/6 確認〕
※ 250 Cyber Security Agency of Singapore：About Cybersecurity Labelling Scheme for IoT - CLS (IoT) https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/〔2025/6/6 確認〕
※ 251 GOV.UK：The UK Product Security and Telecommunications Infrastructure (Product Security) regime https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime〔2025/6/6 確認〕
※ 252 FCC：U.S. Cyber Trust Mark https://www.fcc.gov/CyberTrustMark〔2025/6/6 確認〕
※ 253 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20241106_2.pdf〔2025/6/6 確認〕
※ 254 JBMIA：BMSec は、JC-STAR と制度統合します https://bmsec.jbmia.or.jp/news/details.php?id=76〔2025/6/6 確認〕
※ 255 https://www.ipa.go.jp/security/jisec/index.html〔2025/6/6 確認〕
※ 256 https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf〔2025/6/6 確認〕
※ 257 IPA：国際承認アレンジメント（CCRA）概要 https://www.ipa.go.jp/security/jisec/about/ccra.html〔2025/6/6 確認〕
※ 258 https://www.commoncriteriaportal.org〔2025/6/6 確認〕
※ 259 IPA：評価・認証プロテクションプロファイルリスト https://www.ipa.go.jp/security/jisec/pps/certified-pps/〔2025/6/6 確認〕
※ 260 経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ https://www.meti.go.jp/press/2025/04/20250414002/20250414002-2.pdf〔2025/6/6 確認〕
※ 261 経済産業省：「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」を公表しました https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html〔2025/6/6 確認〕
NISC：「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」を公表しました https://www.nisc.go.jp/pdf/council/wg_supply_chain/20250414_press.pdf〔2025/6/6 確認〕
※ 262 IPA：情報セキュリティ 10 大脅威 2025 組織編 ２位「サプライチェーンや委託先を狙った攻撃」 https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf〔2025/6/6 確認〕
※ 263 経済産業省：ワーキンググループ１（サプライチェーン強化に向けたセキュリティ対策評価制度に関する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_supply_chain/index.html〔2025/6/6 確認〕
※ 264 英国の「Cyber Essentials」、米国の「Cybersecurity Maturity Model Certification 2.0 Program（CMMC 2.0）」、フランスのサイバースコア法、オーストラリアの「Essential Eight」等。
NCSC：Cyber Essentials https://www.ncsc.gov.uk/cyberessentials/overview〔2025/6/6 確認〕
CISA：Cybersecurity Maturity Model Certification 2.0 Program https://www.cisa.gov/resources-tools/resources/cybersecurity-maturity-model-certification-20-program〔2025/6/6 確認〕
legifrance.gouv.fr：LOI n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public (1) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045294275〔2025/6/6 確認〕
ACSC：Essential Eight https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight〔2025/6/6 確認〕
※ 265 経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（概要） https://www.meti.go.jp/press/2025/04/20250414002/20250414002-1.pdf〔2025/6/6 確認〕
一般財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〔2025/6/6 確認〕
一般財団法人日本情報経済社会推進協会：情報マネジメントシステム関連文書 ISMS 認証に関するガイド類 https://www.jipdec.or.jp/library/smpo_doc.html#11〔2025/6/6 確認〕
※ 266 IPA：SECURITY ACTION セキュリティ対策自己宣言 https://www.ipa.go.jp/security/security-action/〔2025/6/6 確認〕
※ 267 内閣官房、総務省、経済産業省：「政府情報システムのためのセキュリティ評価制度 (ISMAP)」の運用開始 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00071.html〔2025/6/6 確認〕
※ 268 https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf〔2025/6/6 確認〕
※ 269 総務省、経済産業省：クラウドサービスの安全性評価に関する検討会について https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/001_02_00.pdf〔2025/6/6 確認〕
※ 270 機密性２情報：行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害されまたは行政事務の遂行に支障を及ぼすおそれがある情報を指す。
※ 271 NISC、デジタル庁、総務省、経済産業省：ISMAP 制度改善の取組み https://www.ismap.go.jp/sys_attachment.do?sys_id=be1ce75c4713b5103f0f6befe16d4355〔2025/6/6 確認〕
※ 272 ISMAP：ISMAP 管理基準の解釈や具体的な実装例を示したガイドはありますか。 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010068〔2025/6/6 確認〕
※ 273 NISC、デジタル庁、総務省、経済産業省：ISMAP 制度の見直しについて https://www.ismap.go.jp/sys_attachment.do?sys_id=87b793a583e86a10aa68c6a8beaad3af〔2025/6/6 確認〕
※ 274 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005〔2025/6/6 確認〕
※ 275 https://www.ismap.go.jp〔2025/6/6 確認〕
※ 276 総務省：「クラウドサービスの安全性評価に関する検討会 とりまとめ」の公表 https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00096.html〔2025/6/6 確認〕
※ 277 IPA：海外のクラウドサービスのセキュリティ評価制度に関する調査 https://www.ipa.go.jp/security/reports/cloud_oversea.html〔2025/6/6 確認〕
※ 278 https://www.ismap.go.jp/sys_attachment.do?sys_id=570a04b62b606e10f0bbfd69fe91bf74〔2025/6/6 確認〕
※ 279 ISMAP：「ISMAP クラウドサービス登録規則」第９章において求められる、情報セキュリティインシデント報告を行う際の具体的な方法や基準、項目などを教えてください。 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010898&sys_kb_id=42b3851f83889210d54cba98beaad33e&spa=1〔2025/6/6 確認〕
※ 280 デジタル庁、総務省、経済産業省：電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト） https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r1.pdf〔2025/6/4 確認〕
※ 281 CRYPTREC：CRYPTREC の体制 https://www.cryptrec.go.jp/system.html〔2025/6/4 確認〕
※ 282 https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf〔2025/6/4 確認〕

※ 283 https://www.cryptrec.go.jp/report/cryptrec-gl-3005-1.0.pdf〔2025/6/4 確認〕
※ 284 NICT、IPA：CRYPTREC Report 2024 https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2024.pdf〔2025/7/31 確認〕
※ 285 https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2024.pdf〔2025/6/4 確認〕
※ 286 NIST：Module-Lattice-Based Key-Encapsulation Mechanism Standard https://csrc.nist.gov/pubs/fips/203/final〔2025/6/4 確認〕
※ 287 NIST：Module-Lattice-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/204/final〔2025/6/4 確認〕
※ 288 NIST：Stateless Hash-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/205/final〔2025/6/4 確認〕
※ 289 NIST：Post-Quantum Cryptography https://csrc.nist.gov/projects/post-quantum-cryptography〔2025/6/4 確認〕
※ 290 CRYPTREC：量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024 年度版 https://www.cryptrec.go.jp/exreport/cryptrec-ex-3401-2024.pdf〔2025/6/4 確認〕
※ 291 https://www.cryptrec.go.jp/report/cryptrec-gl-3004-1.1.pdf〔2025/6/4 確認〕
※ 292 https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf〔2025/6/4 確認〕
※ 293 https://www.cryptrec.go.jp/events/cryptrec_symposium2024_presentation.html〔2025/6/4 確認〕
※ 294 https://www.nri-secure.co.jp/download/insight2024-report〔2025/6/6 確認〕
※ 295 https://sc3.jp/〔2025/7/31 確認〕
※ 296 https://cric.jp/guide/〔2025/6/6 確認〕
※ 297 https://sc3.jp/〔2025/6/6 確認〕
※ 298 https://www.ipa.go.jp/security/sme/otasuketai-about.html〔2025/6/6 確認〕
※ 299 https://www.ipa.go.jp/security/sme/ps6vr7000001hnrl-att/otasuketai-leaflet.pdf〔2025/6/6 確認〕
※ 300 https://www.ipa.go.jp/security/sme/otasuketai/nq6ept000000faii-att/000092713.pdf〔2025/6/6 確認〕
※ 301 https://www.ipa.go.jp/security/otasuketai-pr/〔2025/6/6 確認〕
※ 302 https://www.ipa.go.jp/security/security-action/index.html〔2025/6/6 確認〕
※ 303 https://www.ipa.go.jp/security/guide/sme/5minutes.html〔2025/6/6 確認〕
※ 304 IPA：セキュリティインシデント対応机上演習教材 https://www.ipa.go.jp/security/sec-tools/ttx.html〔2025/6/6 確認〕
※ 305 IPA：制御システムのセキュリティリスク分析ガイド 第 2 版 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html〔2025/7/4 確認〕
※ 306 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〔2025/7/4 確認〕
※ 307 https://www.ipa.go.jp/security/controlsystem/ug65p900000019bkg-att/begoj9000000hpvw.pdf〔2025/7/4 確認〕
※ 308 https://www.ipa.go.jp/security/controlsystem/ug65p900000019bkg-att/begoj9000000hqxn.pdf〔2025/7/4 確認〕
※ 309 https://www.ipa.go.jp/security/controlsystem/controlsystem-smartplant.html〔2025/7/4 確認〕
※ 310 IPA：制御システムのセキュリティリスク分析ガイドセミナー https://www.ipa.go.jp/security/seminar/controlsystem/controlsystem.html〔2025/7/4 確認〕
※ 311 東スポ WEB:ミャンマー地震がフェイク画像で混乱 IT事情通は「再生回数稼ぎや募金詐欺」と指摘 https://www.tokyo-sports.co.jp/articles/-/339475〔2025/6/6 確認〕
※ 312 https://www.soumu.go.jp/use_the_internet_wisely/special/generativeai/〔2025/6/6 確認〕
※ 313 KRY 山口放送：「元本が多いほど得られる利益も多くなる」下関市の 60 代女性が SNS 型投資詐欺で 2200 万円被害 https://news.ntv.co.jp/n/kry/category/society/krb301e87a451b4b33a12831f008dd6e0c〔2025/6/6 確認〕
※ 314 https://www.npa.go.jp/bureau/safetylife/sos47/〔2025/6/6 確認〕
※ 315 警察庁：SNS 型投資詐欺 https://www.npa.go.jp/bureau/safetylife/sos47/case/sns-romance/investment/〔2025/4/9 確認〕
※ 316 金融庁：「詐欺的な投資に関する相談ダイヤル」の開設について https://www.fsa.go.jp/news/r5/sonota/20240619/toshisagi.html〔2025/6/6 確認〕
※ 317 KRY 山口放送：「私と会うためには会員カード作って」…50 代男性が 125 万円の SNS 型ロマンス詐欺被害・宇部 https://news.ntv.co.jp/n/kry/category/society/krf35d63b34e704c4bad718274a53b1efc〔2025/6/6 確認〕
※ 318 警察庁：SNS 型ロマンス詐欺 https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/sns-romance/romance/〔2025/6/6 確認〕
※ 319 岩手日日新聞社：被害防止へ連携 SNS型投資・ロマンス詐欺 岩手県警 NTT、セコムと協定 https://www.iwanichi.co.jp/2024/12/07/13985771/〔2025/6/6 確認〕
※ 320 インターネット掲示板や SNS 等で、仕事内容を明示せず高額な報酬を提示して犯罪の実行者を募集するもの。
※ 321 テレ朝 news：“闇バイト”コア 19 事件で 47 人逮捕 「トクリュウ対策元年」になった一連の強盗事件を振り返る https://news.tv-asahi.co.jp/news_society/articles/900015077.html〔2025/6/6 確認〕
※ 322 埼玉新聞：母娘が恐怖…寝ていると男 3 人が襲いかかる 深夜に自宅で テープで縛り暴行した 26 歳、カードなど強奪し逮捕 母娘は自力でテープはがす カードで現金を下ろそうとした大学生も逮捕、番号が一致せず諦めた 21 歳 https://www.saitama-np.co.jp/index.php/articles/101710/postDetail〔2025/6/6 確認〕
※ 323 朝日新聞：「闇バイト」実行役 2 人を強盗殺人容疑で再逮捕 横浜市青葉区の事件 https://www.asahi.com/articles/AST2B0GWPT2BOXIE003M.html〔2025/6/6 確認〕
※ 324 https://www.youtube.com/@mextchannel〔2025/6/6 確認〕
※ 325 https://www.youtube.com/watch?v=SkdwK9PdKfI〔2025/6/6 確認〕
※ 326 警視庁：＃BAN 闇バイト https://www.keishicho.metro.tokyo.lg.jp/kurashi/drug/yami_arbeit/ban_yamiarbeit.html〔2025/6/6 確認〕
※ 327 LINE ヤフー：LINE ヤフー、闇バイト対策として新たな取り組みを開始／闇バイトへの加担リスクを学べる中学生・高校生向け 情報モラル教材を静岡大学と共同開発／さらに「LINE」を悪用した闇バイト・詐欺行為の撲滅を目指し、啓発活動を実施 https://www.lycorp.co.jp/ja/news/release/017128/〔2025/6/6 確認〕
※ 328 福井新聞：競歩柳井、中傷被害を訴え 個人種目の辞退発表後 https://www.fukuishimbun.co.jp/articles/-/2096071〔2025/6/6 確認〕
※ 329 TEAM JAPAN：第 33 回オリンピック競技大会（2024/ パリ）TEAM JAPAN からのメッセージの掲出について https://www.joc.or.jp/news/20240801035399.html〔2025/6/6 確認〕
※ 330 株式会社セント・フォース：所属タレントに対する誹謗中傷等への対応につきまして https://www.centforce.com/topics/page/12〔2025/6/23 確認〕
※ 331 https://no-heart-no-sns.smaj.or.jp/〔2025/6/6 確認〕
※ 332 https://www.youtube.com/@MOJchannel〔2025/6/6 確認〕
※ 333 https://www.youtube.com/watch?v=onA58-GRKQQ〔2025/6/6 確認〕
※ 334 法務省：人権啓発動画「インターネットはヒトを傷つけるモノじゃない。」公開中! https://www.moj.go.jp/JINKEN/jinken04_00257.html〔2025/6/6 確認〕
※ 335 NISC：NISC サイバーセキュリティ月間 2025 https://security-portal.nisc.go.jp/cybersecuritymonth/2025/〔2025/6/6 確認〕
※ 336 NISC：インターネットの安全・安心ハンドブック https://security-portal.nisc.go.jp/guidance/handbook.html〔2025/6/6 確認〕
※ 337 内閣府大臣官房政府広報室：スマートフォンのセキュリティ対策できていますか? 4 つのポイント【字幕付】 https://www.gov-online.go.jp/prg/prg26093.html〔2025/6/6 確認〕
※ 338 総務省：つくろう!守ろう!安心できる情報社会 https://www.soumu.go.jp/dpa/#initiative〔2025/6/6 確認〕
※ 339 https://www.soumu.go.jp/use_the_internet_wisely/〔2025/6/6 確認〕
※ 340 https://www.soumu.go.jp/use_the_internet_wisely/special/lctliteracy_for_yps/〔2025/6/6 確認〕

付録

第20回 IPA「ひろげよう情報セキュリティコンクール」2024 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30,636点の応募作品の中から、IPAが授与している最優秀賞と優秀賞をご紹介いたします。

最優秀賞

〈標語部門〉

パスワード
意味ない配列
意味がある

板野 早希さん　東京都 東京都立上野高等学校

〈ポスター部門〉

多要素認証があなたを守る

岩永 陽翔さん　東京都 国際基督教大学高等学校

優秀賞

〈標語部門〉

パスワード　よりふくざつに　足すワード

佐藤 海璃さん
宮城県 南三陸町立志津川小学校

謎メール　軽いクリック　重い代償

酒井 翔琉さん
茨城県 北茨城市立中郷中学校

多要素認証　そのひと手間が　漏洩防ぐ

一ノ瀬 玲央さん
北海道 北海道旭川東高等学校

〈ポスター部門〉

タップの前に疑って!!

今岡陽菜歌さん　大阪府 大阪市立大淀小学校

覗き見に注意

井上羽南さん 茨城県 茨城県立並木中等教育学校

同じ鍵は危険です

杉本瑞季さん 愛知県 愛知県立安城南高等学校

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）
- 企業規模、業種が自組織と近い他組織と診断項目別にスコアを比較
- 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、複数人での学習

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

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	国内外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

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

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、自社で対応していない場合に生じる情報セキュリティ上のリスクと、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！」

学習 診断 対策

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

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

概要

• セキュリティベンダー、公的機関、政府等から発信される注意喚起や、資料・動画・ツール等のコンテンツを網羅的に掲載したポータルサイト
• コンテンツを「被害に遭ったら」「対策する」「教育・学習」「セキュリティチェック」「データ＆レポート」に分類。必要な情報が見つけやすい
• 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

診断

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

用途・目的	セキュリティ対策の実施状況のセルフチェック
利用対象者	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

学習

https://www.ipa.go.jp/security/sec-tools/5mins_point.html

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、情報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
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、様々な情報セキュリティ上の脅威・手口、対策を学ぶことができます。
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

F

G

I

J

L

M

N

O

P

さ

た

な

は

ま

や

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　沖田 孝裕　小山 明美　涌田 明夫　白石 歩
井上 佳春　渋谷 環

執筆者　IPA
伊藤 彰朗　伊藤 さやか　伊藤 忠彦　伊藤 吉史　井上 佳春
入来 星衣　大久保 直人　奥村 明俊　大海 健太　小川 賢一
小川 隆一　沖田 孝裕　金木 陽一　金子 成徳　加納 諒也
神谷 健司　亀山 友彦　菅野 和哉　菊池 秀一　小杉 聡志
小山 明美　小山 祐平　佐藤 栄城　渋谷 環　白石 歩
新保 淳　鷲見 拓哉　銭谷 謙吾　田島 凛　辻 宏郷
豊田 亮子　長迫 智子　西尾 秀一　野村 春佳　平本 健二
冨士 愛恵里　藤井 明宏　古居 敬大　松島 伸彰　宮本 冬美
森貞 夏樹　守屋 真人　籔口 春南　山下 恵一　吉原 正人
吉本 賢樹

三菱電機株式会社　神余 浩夫
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　中村 元洋
順天堂大学 健康データサイエンス学部　満塩 尚史
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

協力者　IPA
浅見 侑太　井上 真弓　板橋 博之　伊藤 真一　江島 将和
大澤 淳　小野塚 直人　甲斐 成樹　釜谷 誠　唐亀 侑久
神田 雅透　岸野 照明　北村 弘　桐淵 直人　黒岩 俊二
桑名 利幸　佐川 陽一　貞広 憲一　篠塚 耕一　白井 綾
瀬光 孝之　高見 穣　高柳 大輔　田口 聡　田中舘 隼
田村 智和　土屋 正　遠山 真　中島 尚樹　西原 栄太郎
西村 奏一　日向 英俊　福原 聡　松岡 光　松田 修平
宮崎 卓行　安田 進　渡邉 祥樹
サイバーレスキュー隊 J-CRAT（ジェイ・クラート）
AISI 事務局 戦略・企画チーム

一般財団法人日本情報経済社会推進協会　大熊 三恵子
NRI セキュアテクノロジーズ株式会社　北原 幸彦
一般財団法人日本情報経済社会推進協会　崎村 夏彦
一般社団法人 JPCERT コーディネーションセンター　染川 夕貴
NTT 株式会社　永井 彰
国立研究開発法人情報通信研究機構　中尾 康二
総務省 サイバーセキュリティ統括官室
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

2024年度は、仕事や日々の生活での生成AIの活用が本格化し、「日常が一変」したという方も多いのではないでしょうか。 その一方で、総合エンターテインメント企業がランサムウェア攻撃で多大な被害を受けた事例のように、1回のサイバー攻撃で、いままでの「日常が一変」することも起こっています。 良くも悪くも「一変する日常」に私達は対応していかないといけない、そしてその日常を支えるのは個々人や個々の組織だけでは難しいことから、サブタイトルを「一変する日常:支える仕組みを共に築こう」としました。
IPAでは2025年3月にIoT製品のセキュリティレベルを可視化する新たな制度「セキュリティ要件適合評価及びラベリング制度(JC-STAR)」を開始し、5月には適合ラベルの交付が開始されました。サブタイトル後半の日常を「支える仕組み」の一つとして、本制度が浸透し、安全なIoT機器が積極的に選ばれることで、DDoS攻撃等のサイバー攻撃の被害を減らす一助になればと思います。

編集子

情報セキュリティ白書 2025

一変する日常 : 支える仕組みを共に築こう

2025 年 9 月 30 日　PDF 版 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**