経済産業省

資料３

第10回
産業サイバーセキュリティ研究会
事務局説明資料

令和８年４月３日

経済産業省　商務情報政策局

目次

１．サイバーセキュリティを取り巻く現状

最近国内外で発生した主な事案

① 機微技術情報等の窃取

- 2021年以降、中国を背景とするグループ「Salt Typhoon」による、**政府や軍事インフラを含む世界中のネットワークを標的に、公開された脆弱性等を利用してアクセスし、データ窃取**等を行う活動が観測されている。（2025年8月 国家サイバー統括室及び警察庁が国際アドバイザリーに共同署名）

② 事業活動の停止

- 2025年9月、英自動車大手ジャガー・ランドローバー社において、**サイバー攻撃の影響により生産・小売活動が停止**。英国非営利団体は「約3,900億円以上の経済損失が生じた、英国史上最も被害の大きいサイバー攻撃である」と報告。
- 2025年9月、アサヒグループホールディングス㈱において、**ランサムウェア攻撃の影響により**国内の酒類や飲料、食品の**受注・出荷業務が停止。主要工場での製造も一時停止**するとともに、情報漏えいも確認。
- 2025年10月、アスクル㈱において、**ランサムウェア攻撃の影響により受注・出荷業務が停止**。ネット通販の配送をアスクルのグループ会社に委託する良品計画㈱等においてもネットストアでの受注・出荷業務が停止。情報漏えいも確認。

③ 重要インフラの機能停止等

- 2025年12月、ポーランドの**風力・太陽光発電所、熱電併給プラント等を標的とした、冬季の電力高需要期を狙ったとみられる大規模なサイバー攻撃キャンペーン**が行われた。攻撃者についてはロシアが支援するAPTグループとの関連が指摘されている。

④ サプライチェーン・委託先等への攻撃を起点とした情報漏えい

- 2025年3月、日鉄ソリューションズ㈱において、**ネットワーク機器へのゼロデイ攻撃を原因とした不正アクセス**を受け、同社のサーバー内に保存されていた、過去の**業務委託元などの取引先の個人情報を含む情報の漏えい**可能性を確認。

デジタル技術の発展によるサイバー攻撃の高度化・複雑化

- AI等のデジタル技術の発展の影響もあり、**サイバー攻撃実施のハードルは下がることで、今後ますますサイバー攻撃が増加・高度化・複雑化するおそれ**がある。

デジタル技術の発展によるサイバーリスクの増加

ITシステム、クラウド等の活用拡大、OT製品の急増など**サイバー空間の利用拡大**等に伴い、サイバー攻撃を受ける**システム側の侵入口が増加**。

NICTER において2025年に観測した**サイバー攻撃関連の通信数は増加傾向**（約7,010億パケット）。
家庭用ルータや録画機器等が感染の標的になる等、**IoTボットが多様化**。

スピアフィッシングやビジネスメール詐欺等の実行を支援する**サイバー犯罪用の生成 AI ツールの登場**

2025年における**フィッシングの報告件数**は**前年比約40%増の245万件超**と**引き続き急増**。

AIを通じた情報漏えい・サイバー攻撃リスク

- ウクライナの政府機関に対し、**生成AIを利用するマルウェアによる世界初のサイバー攻撃**が発生。マルウェアには攻撃指示は記述されず、外部の生成AIサービスと通信して攻撃指示を作成する仕組み。パターンマッチングによる**検知が従来型マルウェアより難しい**とされる。
- 業務管理ソフトの**AI連携機能（MCPサーバー）の欠陥の悪用**や、営業支援システムで用いられる**AIチャットボット連携機能の侵害**により**顧客情報等流出**事案が発生。
- AI活用による更なる効率化の観点から、**AIエージェント**の活用・検討が進むが、**大きな権限が設定**されることで、**乗っ取られた際の被害が甚大**になるリスクが指摘。

サイバー攻撃のエコシステム（ダークウェブ）の存在

- **ダークウェブの闇市場**では非合法で個人や企業の機密データ、**マルウェアを容易に作成できるツールキットなどが取引**されており、**サイバー犯罪を助長**している。
- ランサムウェア攻撃に必要な一式をサービスとして提供するRansomware-as-a-Service（RaaS）の普及により、**専門知識を持たない攻撃者でも攻撃が容易に**。

（出典）(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威 2025」解説書、
(国研)情報通信研究機構「NICTER観測レポート2025」、フィッシング対策協議会「月次報告書」、各種報道情報　等

地政学動向の変化に伴うサイバーリスクの高まり

- サイバー攻撃が巧妙化・深刻化する中、地政学リスクの増大とも相まって、**安全保障にも関わるサイバー事案の脅威が高まっている**状況にある。

サイバー攻撃の変遷

■公開サーバへの攻撃
・特徴：ウェブサーバ・外向けサービスへの大量送信　等
・効果：ウェブサイト等の停止
・事例：エストニア・2007年

■機微情報の窃取の危険
・特徴：情報システムへの権限外アクセス・利用
・効果：機密情報の漏えい・悪用
・事例：Black Tech・2023年

■有事に備えた重要インフラ等への侵入（破壊準備）
・特徴：最深部・制御系システムに至る高度な侵入能力
・効果：インフラ機能の停止
・事例：Volt Typhoon・2023年　等

■世界規模の通信監視（スパイ活動）
・特徴：政府・重要インフラ等のネットワーク潜伏
・効果：通信内容・移動情報・認証情報等の窃取
・事例：Salt Typhoon他・2021-2025年

国家関与が疑われるサイバー動向に関する報道

- **国家関与が疑われるサイバー攻撃事案への対抗**
  - 米国司法省は、米国やアジアの政府機関等に対するサイバー攻撃等に関与したとして、**中国公安部職員２人を含む中国人12人を起訴**したと発表。（2025年３月）
  - 米国政府は中国系APT「Volt Typhoon」及び「Salt Typhoon」による米国重要インフラへの長期潜伏と侵入を深刻視し、**「米国は報復的サイバー攻撃も辞さない」と明確に警告**。CISAは、中国政府支援の攻撃者がITネットワークからOT（制御系）への横展開を可能にする長期的侵入を進めていると指摘。（2025年5月）

- **台湾当局・重要インフラ等に対するサイバー攻撃**
  - 中国による**台湾当局へのサイバー攻撃が1日平均280万件**発生（前年比約17%増）。台湾当局が、中国の「オンライン・トロール（迷惑行為）部隊」による**台湾社会の分断を狙ったSNSでの偽情報の投稿**を警告。
  - **エネルギー施設への攻撃は前年比約11倍**であり、医療関連施設への攻撃も54%増加。半導体や軍需関連企業も標的となった。

（出典）各種報道発表・報道情報等を基に作成。

NSA、CISA、NCO、NPA他 “Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System”

（参考）IPA「情報セキュリティ10大脅威」

情報セキュリティ10大脅威 2026	
順　位	組織向け脅威
1位	ランサム攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃
3位	AIの利用をめぐるサイバーリスク
4位	システムの脆弱性を悪用した攻撃
5位	機密情報を狙った標的型攻撃
6位	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7位	内部不正による情報漏えい等
8位	リモートワーク等の環境や仕組みを狙った攻撃
9位	DDoS攻撃（分散型サービス妨害攻撃）
10位	ビジネスメール詐欺

初選出

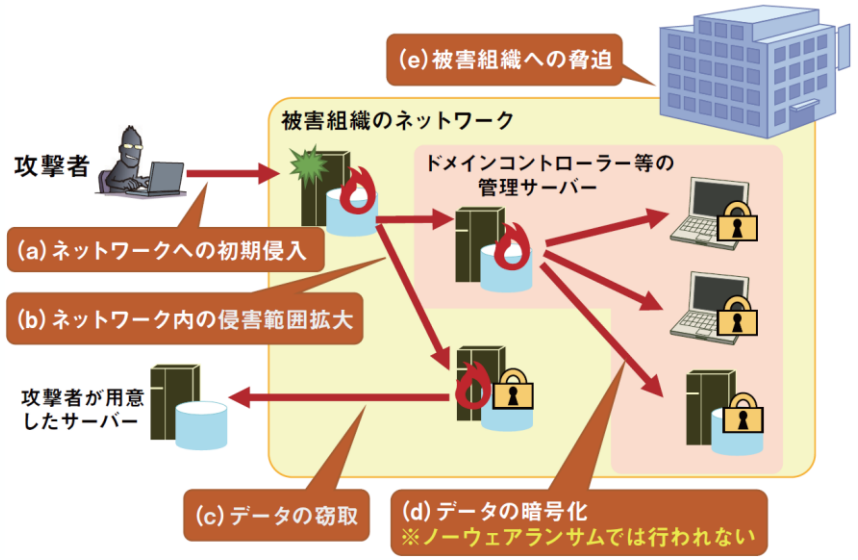
中小企業の被害が全体の約6割を占める

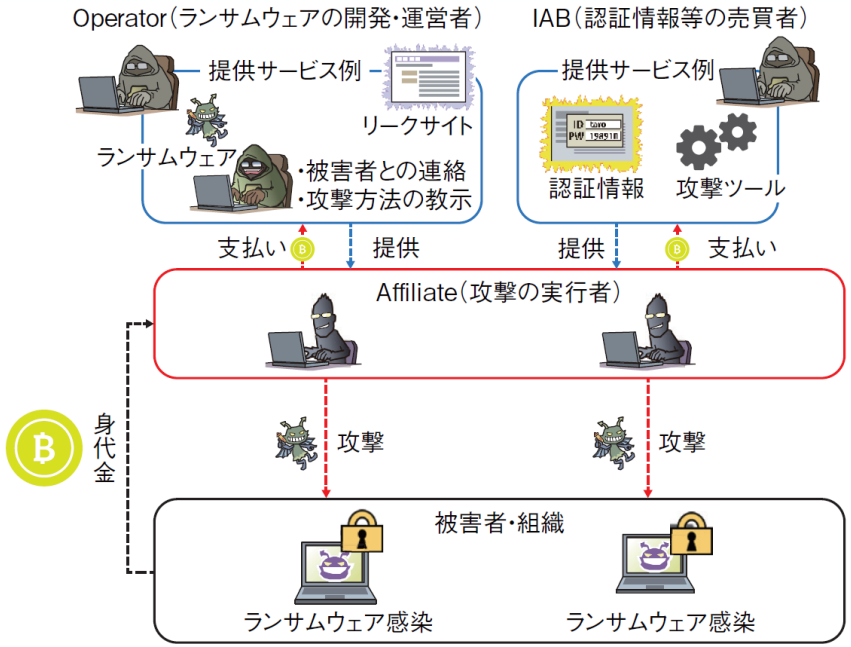
相対的にセキュリティ対策の弱い中小企業を起点に、大企業含むサプライチェーンを共有する企業を攻撃

（出典）独立行政法人情報処理推進機構（IPA）「情報セキュリティ10大脅威2026」、
警察庁「令和7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（令和８年３月）」を基に作成。

（参考）最近のランサムウェア攻撃の特徴及び主な対策例

- ネットワークへ密かに侵入して侵害範囲を拡大した後、大量のデータを暗号化することで事業継続に大きな影響を与える**「侵入型」**かつ、身代金を支払わない場合はデータを暴露する**「二重脅迫型」**が主流。
- ランサムウェアや認証情報等をサービスとして提供する攻撃者のビジネスモデル（**RaaS**）が確立。**攻撃者の組織化・分業化が進展**し、**実行者は技術的専門知識を有さずとも容易に攻撃可能**に。





主な対策例

① **ネットワーク侵入対策** ･･･攻撃対象領域の最小化、特にVPN機器の脆弱性対策や認証強化・アクセス制御 等
② **侵害範囲の拡大防止対策** ･･･EDR等の利用による不審な挙動の検知、ネットワーク接続点における不正通信の監視 等
③ **暗号化・システム停止対策** ･･･バックアップの適切な取得（複数バックアップ方式の採用）・復旧可能なことの確認 等
④ **インシデント対応力の強化** ･･･連絡体制・遮断手段を含むランサムウェア攻撃等を想定したBCPの策定・定期見直し 等

出典：独立行政法人情報処理推進機構（IPA）「情報セキュリティ白書2025（令和７年９月）」等を基に作成。

サイバーセキュリティ政策に関する国際的な動向

- 欧米を中心に、①セキュア・バイ・デザイン*の概念に基づく**製品のサイバーセキュリティ対策に対する要請**や、②**企業のサイバーセキュリティ対策**水準の整備・可視化、③国内のサプライチェーン全体をカバーする**中小企業向けサイバー対策促進支援**の取組が進展。

＊ IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていることを指す。

①IoT・ソフトウェア製品に対するセキュリティ要件

EU サイバーレジリエンス法

- デジタル要素を備えた製品（ソフトウエア含む）の製造者に対し、**①セキュリティ特性要件に従った上市前の設計製造、②上市後に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**。
- 報告義務の運用開始は2026年9月、その他は2027年12月開始予定。

PSTI法

- 英国内で主に消費者向けIoT機器の製造や流通、販売を行う事業者に対し、**3つのセキュリティ要件※を含むセキュリティ対策の遵守を義務付け**。
- 2024年4月に適用開始。

※共通パスワード設定の禁止、脆弱性情報の提供、セキュリティサポート期間の明示。

②企業のサイバーセキュリティ対策水準の整備・可視化

サイバー・エッセンシャルズ

- 英国NCSCが全ての**企業を対象に**一般的なサイバー攻撃への防御策を提供することを目的として設計した、自己適合、第三者診断の**二段階で構成される認証制度**。
- 一部政府及び公的機関の調達において必須要件として課される場合がある。

※豪州においても、すべての組織を対象とする４段階の基準（エッセンシャル・エイト）が存在。
※米国においても、国防総省がその請負業者等と共有する機密性の高い情報の保護を目的に設計したサイバーセキュリティ成熟度モデル認証（CMMC。2025年9月に国防総省が契約要件化の方針を公表。）が存在。

③中小企業向けサイバーセキュリティ対策促進支援

サイバー・アクション・ツールキット

- 英国NCSCが**個人事業主・小規模組織向けにサイバーセキュリティ対策支援ツールを無料で提供**。（2025年10月公表）

サイバー・エッセンシャルズ取得支援

- 英国NCSCがサイバー・エッセンシャルズの**認証取得を支援するツール**（準備計画策定支援、自己評価質問票等）を提供。

小規模事業者サイバーセキュリティパイロットプログラム

- 米国中小企業庁が州政府を通じて、サイバーセキュリティ対策が困難な**中小企業向けにサイバーセキュリティ対策の研修やコンサルティングを提供**。

足下の世界情勢を踏まえた対応

- 安全保障にも関わるサイバー事案の発生を背景に、サイバーセキュリティ分野において、**有志国による政策協調の傾向が強まり、サプライチェーン管理による高リスクベンダーへの対処の動きがみられた。**
- 米国の予算縮小や政府の断続的閉鎖による影響をはじめ、米国ハイパースケーラーへの依存への懸念も背景に、**欧州がサイバーセキュリティ分野で米国依存から脱却を目指す動きが加速。**

高リスクベンダーへの対処

1. IoT製品セキュリティの非技術要件

- G7閣僚は、IoT製品のセキュリティ対策について、技術的な要件に加え、ベンダーが第三国から影響を受ける全般的なリスク等の非技術的な要件を考慮すべき、として、**高リスクベンダー対処の重要性を確認。**

2. EUによる高リスクベンダー管理

- 2026年１月、 欧州委員会は、**EUが高リスクベンダー対処を統合的に管理する**内容を盛り込んだ、欧州サイバーセキュリティ法（NIS２を規定する法律）改正案を欧州議会に提案。

米国依存脱却の動き

米国
予算縮小や断続的な政府閉鎖の影響

1. MITRE社のCVE契約更新問題：

- 2025年４月、**世界的な脆弱性採番システムであるCVEを運営する連邦契約が終了する内部書簡が流出。**契約終了前日まで11か月の期限付きで契約延長が承認。

2. 米国サイバー・トラスト・マーク：

- IoT製品セキュリティ評価制度。当初、2025年内制度運用開始予定であったが、**政府閉鎖の影響や制度管理者の撤退に伴い、制度開始時期が遅延。**その後、制度管理者の再公募やサイバーセキュリティラベル管理者の公募が行われた。

欧州
独自の制度やツールの利用

1. GCVE：EU独自の脆弱性識別・追跡システム。GCVE Numbering Authorities（GNA） と呼ばれる複数組織が脆弱性IDを発行。管理運用はルクセンブルクのCIRCLが担う。

2. フランス政府職員による米国企業のオンライン会議ツールの使用禁止：フランスが政府職員に対してGoogle Meet、Zoom、Teamsの利用を禁止し、Visio（フランス製のビデオカンファレンスソフトウェア）への移行を要求。

２．これまでの施策の進捗

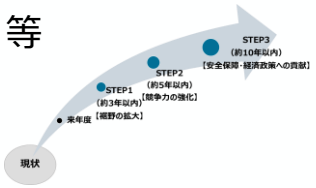
施策の進捗①（経済産業省のサイバーセキュリティ政策全体像）

- 以下の４つの柱の下、産業界におけるサイバーセキュリティ対策強化に向けた取組を推進。
- これらの取組を推進するためのリソースとして、**毎年度数十億円規模の予算を確保（令和７年度補正予算57億円）**。このほか、研究開発や懸賞金、中小企業等のセキュリティ対策支援のための予算も確保。

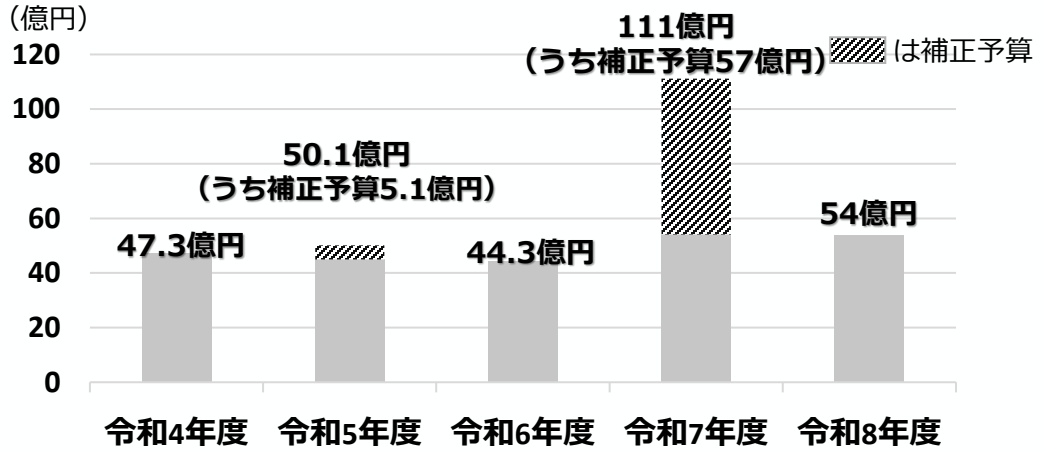
経済産業省のサイバーセキュリティ政策 主要な進捗

1. サプライチェーン全体での対策強化
   - ➢ SCS評価制度構築方針・関係法令想定事例の公表　等
2. セキュア・バイ・デザインの実践
   - ➢ JC-STAR上位基準整備・英国制度との相互承認　等

3. 政府全体でのサイバーセキュリテイ対応体制の強化
   - ➢ 新法施行に向けた脆弱性関連情報の取扱い検討　等
4. サイバーセキュリティ供給能力の強化
   - ➢ IPAによる積極調達、マッチング企画実施　等



経済産業省サイバーセキュリティ関連予算の推移



令和６年度については、「独法等の監視に係る次期システム構築事業」（57億円）を除く。

その他関連予算事業との連携

①経済安全保障重要技術育成プログラム
- 先進的サイバー防御機能・分析能力強化を推進すべく、「経済安全保障推進法に基づく指定基金」を活用した**約300億円**のプロジェクトを開始（2024年7月）

②フロンティア育成・懸賞金事業
- 技術課題や社会課題の解決に資するシーズ・解決策をコンテスト形式による懸賞金型の研究開発方式について、新たなサイバーセキュリティ技術について事業募集
（令和８年度当初予算（**約66億円**）の内数）

③中小企業生産性革命推進事業（デジタル化・AI導入補助金）
- デジタル化・AI導入補助金において、SECURITY ACTIONを申請要件化するとともに、サイバーセキュリティお助け隊サービスの導入費用を補助
（令和７年度補正予算（**3,400億円**）の内数）

施策の進捗②（サプライチェーン全体での対策強化）

- 企業のセキュリティ対策の水準を可視化する**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（SCS評価制度）の構築方針の策定**や**同制度の活用を促すための支援策の整備**を進展。
- **サイバーセキュリティお助け隊サービス**を始めとした現行の中小企業向け施策の**普及**に取り組み、同サービスの利用者数は**約9,200件を突破**。SECURITY ACTION自己宣言数も**46万件を突破**。

新たな制度等の整備

○ **SCS評価制度の構築方針（2026年3月）**

- 中間取りまとめの公表（2025年4月）以降、実証事業の結果を踏まえ、制度の運用体制、制度で用いるセキュリティ要求事項・評価基準、制度における評価スキームなどを盛り込んだ「制度構築方針」を取りまとめ。

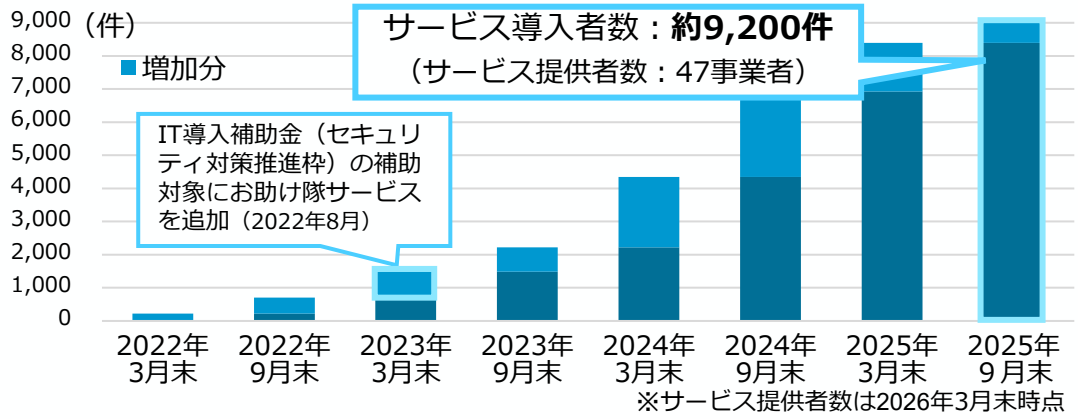
○ **サイバーセキュリティお助け隊サービス（新類型）の創設**

- SCS評価制度の★3又は★4の要求事項のうち未達成の項目を達成させるための伴走支援を目的としたサービスを創設し、SCS評価制度の制度開始に合わせてサービスインを予定。また、2026年度からサービス要件検討のための実証事業を開始。

○ **セキュリティ対策要請に当たっての関係法令整理のための想定事例・解説文書（2025年12月）**

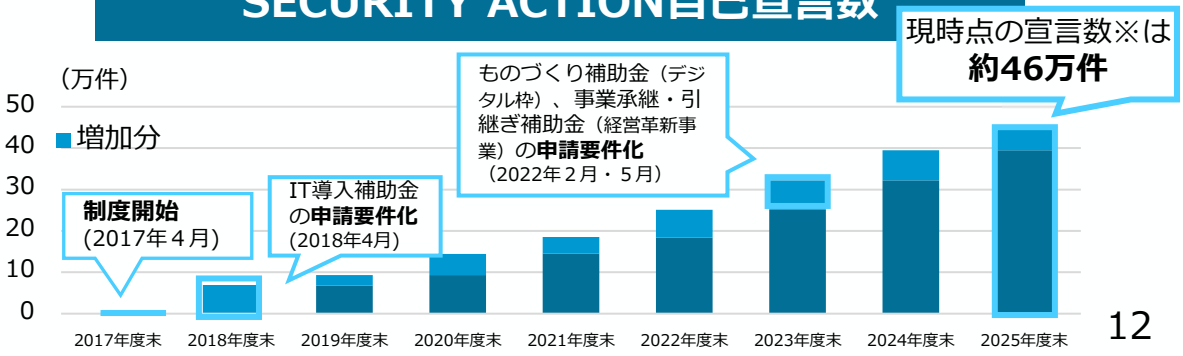
- 「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて（令和4年10月）」を補足するものとして、独占禁止法や取適法との関係で「問題とならない」ケースを想定した想定事例及びその解説文書を作成。

「サイバーセキュリティお助け隊」利用件数



※サービス提供者数は2026年3月末時点

SECURITY ACTION自己宣言数



※一つ星、二つ星の いずれかまたはその両方の自己宣言の件数

施策の進捗③（セキュア・バイ・デザインの実践）

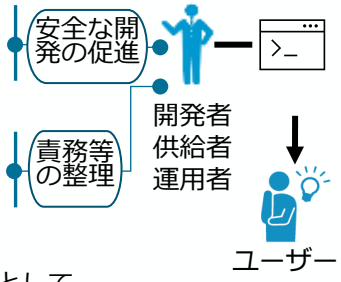
- IoT製品のセキュリティ対策レベルを評価・可視化するJC-STARについて、**製品型番ベースで1,500製品以上のIoT製品がラベル発行済み**。ネットワークカメラ等の一部類型について、**高度なセキュリティ基準（★３）も公開**。
- **セキュアなソフトウェアの開発・流通に向けた取組の具体化**や**サイバーインフラ事業者が果たすべき責務等の整理**についても成果物をとりまとめ。
- これらの取組・制度について、**G7をはじめとする関係国との調和**を図るべく、議論も進展。

JC-STAR（ロゴ・ラベル、ラベル発行製品の例）

JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

セキュアなソフトウェア開発・流通に向けた取組

- **安全なソフトウェア開発のための事業者向けガイダンス案（中間整理）を拡充**（2026年1月）
- **サイバーインフラ事業者（※）が果たすべき責務等を整理したガイドライン策定**（2026年3月）



（※）サイバーインフラ事業者とは、一定の社会インフラの機能としてソフトウェアの開発・供給・運用を行っている事業者を指す。

IoT製品及びソフトウェアに関する関係国との制度・取組調和に向けた成果文書

G7サイバーセキュリティWG

（WG議長声明、2025年6月） ※IoT

G7加盟国（政府）・**産業界**（IoTベンダ・エンドユーザー）に向けて、**IoTセキュリティの確保のために技術的及び非技術的なサイバー脅威の考慮の必要性**について**提案**。

JC-STARとPSTI法の相互承認

（2025年11月：署名、2026年1月：運用開始）※IoT

英国の科学・イノベーション・技術省（DSIT）との間で、**英国PSTI法*が要求する技術基準（3要件）**と**JC-STAR★1**のラベル取得に必要な**技術基準の3要件**が**同等**であるとみなすことに**合意**し、**相互承認を開始**。

＊Product Security and Telecommunications Infrastructure Act

サイバーセキュリティのためのSBOMの共有ビジョンに関する国際ガイダンス（2025年9月） ※ソフトウェア

米国サイバーセキュリティ・インフラ安全庁（CISA）とともに**SBOMの活用の重要性を広く国際的に発信**するとともに、**SBOM運用上の国際共同ガイダンスを整備**することを目的として作成。

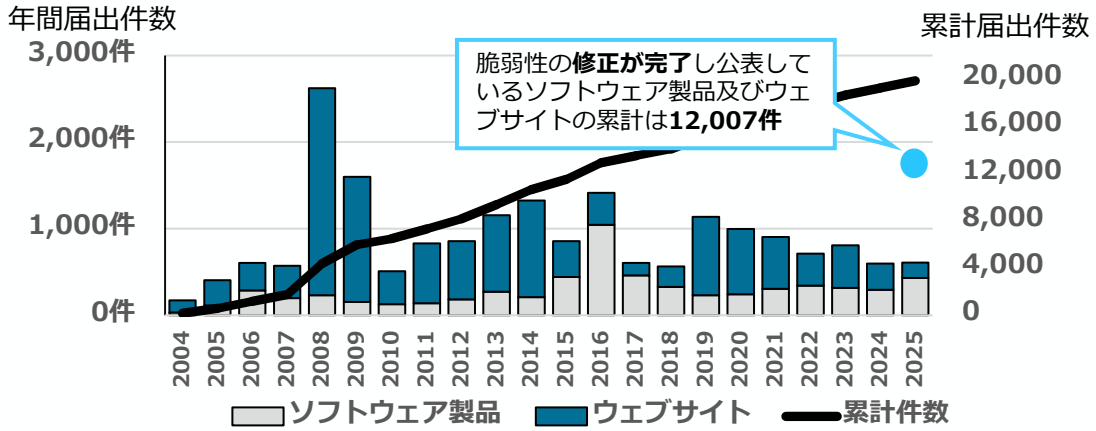
施策の進捗④（政府全体のサイバーセキュリティ対応体制の強化・サイバーセキュリティ供給能力の強化）

- サイバー攻撃が高度化する中、IPAの**サイバーレスキュー隊（J-CRAT）**を通じた標的型サイバー攻撃（APT）等の初動対応支援を実施。IPAに届出があった脆弱性関連情報の修正についても**JPCERT/CC**を通じてベンダ等に働きかけを実施。
- 2025年3月にとりまとめた「**サイバーセキュリティ産業振興戦略**」に基づき、セキュリティ・スタートアップとSI事業者とのマッチングイベントの開催や、「コンテスト形式」による懸賞金事業等を実施。

IPA/J-CRAT活動実績

年度	2022	2023	2024	2025
相談・情報提供数	330	366	431	387
支援数	163	173	210	166
オンサイト支援数	43	65	81	56
アクティブレスキュー数	ー	100	106	124

脆弱性関連情報の届出推移



サイバーセキュリティ産業振興に向けた取組

- **「国産セキュリティ推進フォーラム」の開催**
  - 国内商流を担うSI事業者とベンダとのマッチングを目的として、経済産業省とJNSA*が共同で開催し、46社・68名が参加。活発な議論、ネットワーキングが行われた。
- **フロンティア育成・懸賞金事業**
  - 募集対象の技術として、以下３つのテーマを設定。2026年中に公募開始。
    ① AI技術を活用した革新的なサイバーセキュリティ製品・サービスの開発・製品化
    ② SBOMの効率的な実運用に資するための技術開発・製品化
    ③ SSDFを現場に無理なく導入・定着させるための技術開発・製品化

＊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

人材育成施策の実績

中核人材育成プログラム修了者数	492名(2017年～2025年)
情報処理安全確保支援士	26,453名(2026年4月時点)
セキュリティ・キャンプ参加者数	全国大会: 1,317名(2004年～) ネクストキャンプ: 62名(2019年～) ジュニアキャンプ：18名(2023年～)
インド太平洋地域向け産業制御システム・サイバーセキュリティ演習	来日65名＋ライブ配信約130名（2025年） ※2024年以前は毎年約40名。

３．今後のサイバーセキュリティ政策の方向性

経済産業省におけるサイバーセキュリティ政策の全体像と方向性

- NCOをはじめ関係省庁との連携の下、サイバーセキュリティ市場における**需要拡大と供給力強化に向けた取組**や、**国際的な制度調和と国内での調達要件化促進**、**サイバー情勢分析能力強化**を図っていく。

①サプライチェーン全体での対策強化

- 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）の具体化・実装
- 我が国の半導体関連産業におけるセキュリティ対策水準の向上を通じた競争力確保
- SCS評価制度の構築（対策水準の可視化）
- 地域における中小企業支援の拡大（サイバーセキュリティお助け隊サービスの普及促進・新たな類型の創設等）　等

⇒政府調達・補助金の要件化等を通じた実効性強化

②セキュア・バイ・デザインの実践

- IoT製品におけるJC-STARの普及、国際制度調和の調整
- SBOM（Software Bill of Materials）の活用促進、安全なソフトウェアの開発に向けた指針の整備
- サイバーインフラ事業者の責務の明確化

⇒国際連携を前提とした制度構築と政府調達等要件化を通じた制度の普及

③政府全体でのサイバーセキュリティ対応体制の強化

- IPAのサイバー情勢分析能力強化
- サイバー対処能力強化法の成立を踏まえた脆弱性関連情報の取扱い強化
- サイバー攻撃技術情報の共有促進　等

⇒官民のサイバー状況把握力・対処能力向上と関係省庁との連携

④サイバーセキュリティ供給能力の強化

- サイバーセキュリティ産業振興のための政策パッケージの推進
- 先進的サイバー防御機能・分析能力の強化
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）、若手人材発掘機会（セキュリティ・キャンプ）の拡大　等

IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

⇒セキュリティ市場の拡大に向けたエコシステムの構築

（参考）政府全体における経済産業省の今後の政策の位置付け

- 経済産業省では、国家サイバー統括室をはじめとする関係省庁と連携して**産業界に向けた政策を企画・実行**することにより、サイバー空間上の脅威に対応するための**政府全体の取組に貢献**していく。

サイバーセキュリティ戦略（2025年12月23日閣議決定）

- 深刻化するサイバー脅威に対する防御・抑止
  - 国が要となる防御・抑止
  - 国際連携の推進・強化　等
- 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上
  - 重要インフラ事業者の対策強化
  - ベンダー、中小企業等を含めたサプライチェーン全体のサイバーセキュリティ及びレジリエンスの確保　等
- 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成
  - 効率的・効果的なサイバー人材の確保・育成
  - 新たな技術・サービスを生み出すためのエコシステムの形成
  - 先端技術に対する対応・取組

貢献

経済産業省における今後の政策の方向性

サイバー対処能力強化法への対応

- ソフトウェア脆弱性情報の取扱い対応体制の強化　等

サプライチェーン全体での対策強化

- 企業の対策水準の可視化、中小企業支援　等

セキュア・バイ・デザインの実践

- 諸外国と連携したIoT・ソフトウェア制度整備　等

政府全体でのサイバーセキュリティ対応体制の強化

- IPAのサイバー情勢分析能力強化　等

サイバーセキュリティ供給能力の強化

- 事業化支援、技術開発、セキュリティ人材育成　等

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（SCS評価制度）の実現

SC対策強化

- 「対策状況は**外部から判断が難しい**」「**複数の取引先から様々な対策を要求**される」等の課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策※1を提示しつつ、その状況を可視化する仕組み※2を構築（2026年３月27日に「制度構築方針」を公表）。
- 3段階の水準のうち、**★3・★４について、2026年度末頃の制度開始を目指し**、スキームオーナーであるIPAとともに、制度運営基盤の整備や利用促進等を進めていく。2026年度以降に**★５の設計も進める。**
- **制度開始５年後（2031年）までに２万件、10年後（2036年）までに５万件の★取得を目指す。**

※1　本制度では、サプライチェーンを構成する企業等のIT基盤が対象。
※2 発注時等に、必要なセキュリティ対応状況の可視化を目的としたもので、いわゆる「格付け」制度ではない。

構築する評価制度

成熟度の定義	★ 3	★ 4	★ 5 [検討中※3]
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全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： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等がさらに目指すべき高度な対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
評価スキーム	**専門家確認付き自己評価**	**第三者評価**	第三者評価

※3　ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

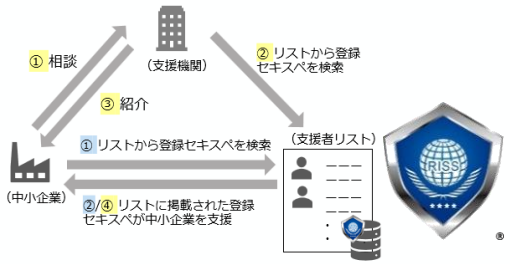
サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

SCS評価制度活用促進のための環境整備

SC対策強化

- リソースに限りのある**中小企業等によるSCS評価制度の活用**や**企業間取引における「共通のものさし」としての同評価制度の活用**を後押しするため、外部専門人材とのマッチング支援や、同制度の”★”取得を支援する民間サービス認定制度の創設、関係法令の適用関係を明確化した想定事例の周知等を進める。

登録セキスペ（外部人材）とのマッチング促進



- SCS評価制度の“★“取得支援等が可能な登録セキスペを育成。
- 育成した登録セキスペをリスト化し、支援機関と連携して周知・活用促進。

サイバーセキュリティお助け隊サービス（新類型）の創設

- SCS評価制度の“★”の取得支援を目的としたサイバーセキュリティお助け隊サービス（新類型）を創設。
- 認定されたサービス提供事業者がセキュリティ対策状況を診断し、“★“取得に向けた伴走支援を行う。

中小企業の情報セキュリティ対策ガイドラインの改訂・周知

- SCS評価制度の“★”取得を意識し、本編において規程策定などの組織的対策や技術的な防御策に取り組むための考え方を提示。
- SCS評価制度の要求事項に即した規程類のサンプル・ひな型を整備。

ステークホルダーへの情報開示における活用促進

- サイバーセキュリティリスクへの対応が中長期的な企業価値向上のために必要である旨をコーポレートガバナンス・コードに追記することを目指す。
- その上で、ステークホルダーへの情報開示における「共通のものさし」としてのSCS評価制度の活用促進を図る。

取引先へのセキュリティ対策要請等に係るパートナーシップの構築促進

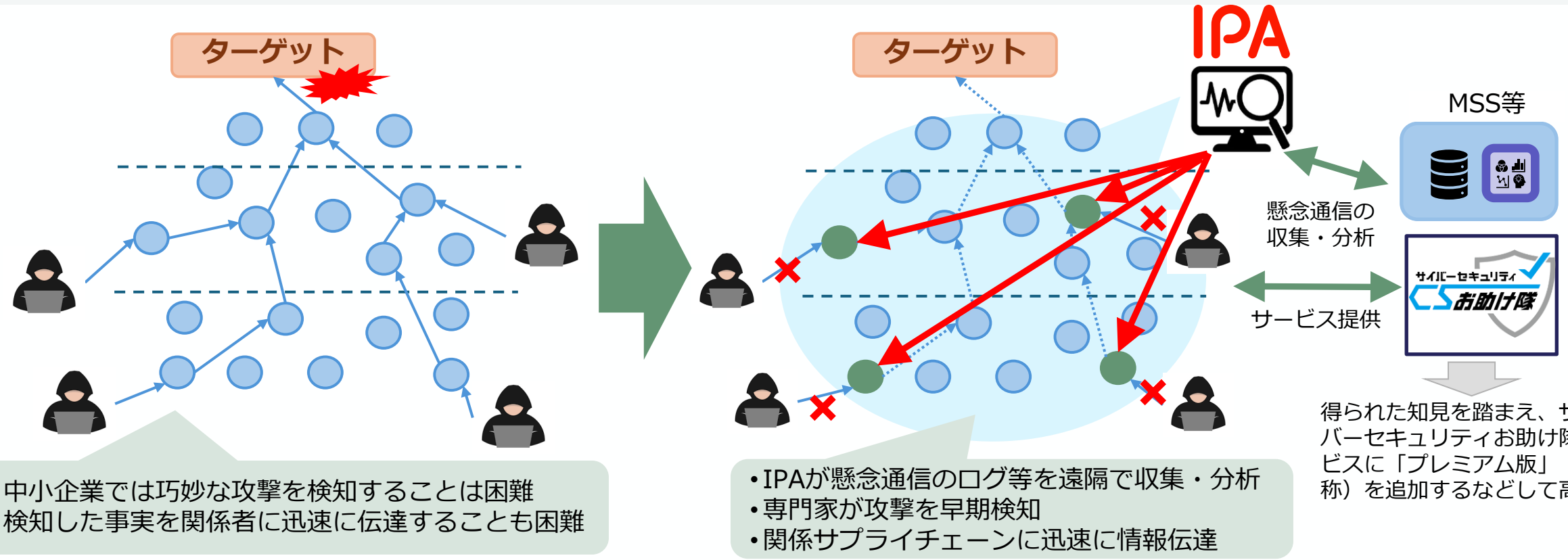
パートナーシップ構築宣言

- 企業間でパートナーシップが構築されセキュリティ対策の要請・取組（SCS評価制度の”★”取得）が円滑に進むよう、独禁法・取適法上の考え方を整理した想定事例の周知を進める。

集団的防御プラットフォームの構築

SC対策強化

- 基幹インフラ事業者を狙うサイバー攻撃は、**サプライチェーン内で脆弱な中小企業等から侵入**することが多いが、**中小企業等**にとって**その兆候の検知は困難**である。
- そこで、高度なサイバー情勢分析機能を有する**IPAが**、**中小企業等で検知された懸念通信を収集・分析**し、**攻撃の早期検知や関係先への注意喚起等を図る**実証事業を令和7年度補正予算で実施予定。
- 実証事業を通じて、**本プラットフォームの有用性等を検証**するとともに、社会実装後の普及促進を見すえ、**サイバーセキュリティお助け隊サービスに面的防御の観点を取り入れ**、その高度化を図っていく。



- 中小企業では巧妙な攻撃を検知することは困難
- 検知した事実を関係者に迅速に伝達することも困難

- IPAが懸念通信のログ等を遠隔で収集・分析
- 専門家が攻撃を早期検知
- 関係サプライチェーンに迅速に情報伝達

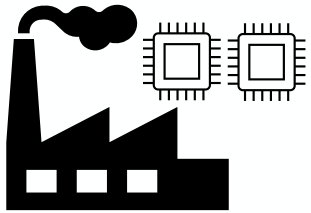
得られた知見を踏まえ、サイバーセキュリティお助け隊サービスに「プレミアム版」（仮称）を追加するなどして高度化

半導体関連産業におけるセキュリティ対策水準向上を通じた競争力確保 SC対策強化

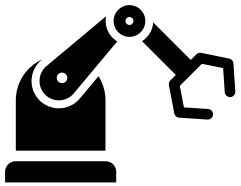
- 半導体関連産業の国内投資の促進が強力に進められているところ、継続的な半導体デバイス生産活動を確保し、知財・先端技術情報等を保護する観点からも、**サイバーセキュリティ対策を進めることが重要。**
- 国際的な枠組みとの整合も考慮し策定した「半導体デバイス工場におけるOTセキュリティガイドライン」も踏まえ、**「半導体デバイスメーカーに対するセキュリティ要求事項」を策定**（2026年１月）。
- 今後、経済安保基金（半導体）※など**経済産業省の投資促進関係施策の要件等との紐付けを順次進めていく。**また、**「半導体装置メーカーに対するセキュリティ要求事項」の策定**に向けた検討も実施する。

※「半導体に係る安定供給確保を図るための取組方針」

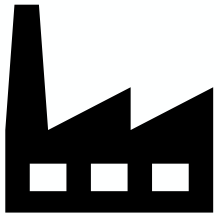
半導体関連産業におけるセキュリティ要求事項



半導体**デバイスメーカー**



半導体**装置メーカー**



半導体**部素材メーカー**

半導体デバイスメーカー	半導体装置メーカー	半導体部素材メーカー
2025年度に策定。 投資促進関係施策との紐付けを順次実施	**2026年度内の策定に向けて検討**	今後検討

セキュリティ要求事項の現状

半導体デバイスメーカーに対するセキュリティ要求事項の概要

- IT項目（43項目）
  - **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★4項目**
- OT項目（6項目）
  - **ガバナンスの整備**：１項目
    - 担当者の責任・権限の割り当て等
  - **リスクの特定**：２項目
    - OT領域の資産の可視化等
  - **攻撃等の防御**：２項目
    - 機密情報の扱いの明確化等
  - **インシデントへの対応**：１項目
    - インシデントへの対応手順の明確化等

中小企業支援策の強化と地域SECUNITY活性化

SC対策強化

- 中小企業のセキュリティ対策の促進に当たっては、**セキュリティ対策の必要性に対する認識不足**や、**十分なリソースの確保の困難性**といった課題への対応が不可欠。
- かかる観点から、既存施策の普及・広報に加え、**地域SECUNITYの活性化**や、**「サイバーセキュリティお助け隊サービス」の充実化**、**外部専門人材の活用促進**など、支援策の強化に取り組む。

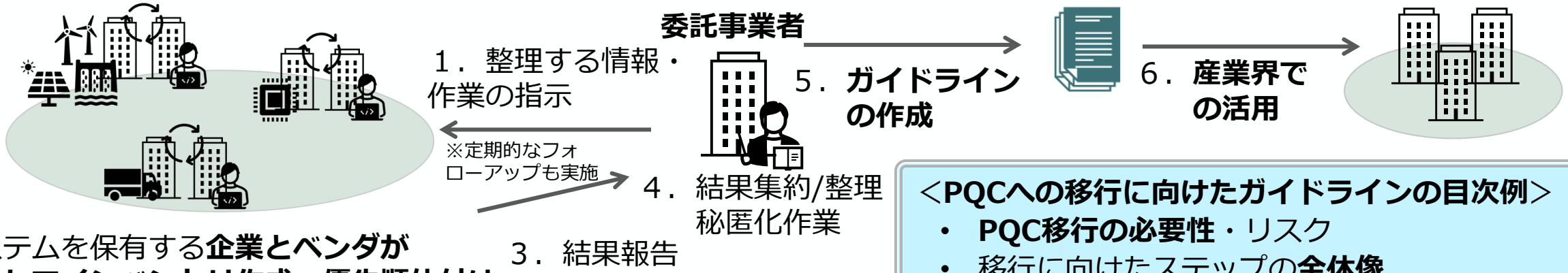
課題	対策の方向性	今後の具体的な取組
セキュリティ対策の必要性を感じていない	地域SECUNITYを通じた普及啓発活動の強化	**【中小企業が身近に感じるコンテンツの作成・展開】** • 中小企業にとって身近なインシデント事例に基づいて机上演習コンテンツを作成し、既存の事例集などとも合わせて、地域SECUNITYでの活用を促す。効果的な取組の他地域への横展開も図る。 **【活動量が相対的に少ない地域における担い手発掘・自走化後押し】** • 東北地方において産学官が連携してサイバーセキュリティセミナー・机上演習・展示会などの複合イベントを開催し、同地域における地域SECUNITY活動の活性化に向けた呼び水とする。
コスト面・知識不足・人材不足から有効な対策ができない	安価で最低限のセキュリティ確保が可能なパッケージサービスの充実化	**【「サイバーセキュリティお助け隊サービス」の新類型創設・既存類型見直し等】** • SCS評価制度“★”取得を支援するサイバーセキュリティお助け隊サービス（新類型）を創設する。 • サイバーセキュリティお助け隊サービスの既存類型（１類・２類）について、時勢に沿ったサービス（ゼロトラスト・クラウド化への対応等）が提供されるようサービス要件を見直す。 • 集団的防御プラットフォームと連携したサービスの開発に向けた検討を進める。 • 中小製造業等の制御系システム（OT）のセキュリティ確保に必要な対策・支援策を検討する。
	外部専門人材の活用促進	**【中小企業等と情報処理安全確保支援士（登録セキスペ）とのマッチング促進】** • 中小企業を支援可能な登録セキスペのリスト（支援者リスト）を整備。登録セキスペの活用事例を蓄積し、商工会議所等の支援機関を通じた両者のマッチングを促進する。 • 今後ニーズの高まるSCS評価制度の“★”取得支援・専門家確認や、機微情報を扱う業界に特化した支援が可能な登録セキスペを育成し、登録セキスペが一層活躍しやすい環境を整備する。

耐量子計算機暗号（PQC）への対応に向けた検討

SC対策強化

- 量子コンピュータの進展による既存暗号の危殆化のリスクに備え、各国において、**耐量子計算機暗号（PQC）への移行に係る検討**が進められている。我が国でも、**政府機関等におけるPQC移行を原則として2035年までに行う**ことを目指し、2026年度に工程表を策定する旨を公表。
- 経済産業省でも、**産業界によるPQCへの円滑な移行を後押し**すべく、移行に向けた第一歩となるクリプトインベントリ※の実施に係る実証事業を開始。その成果物として、**移行に向けたステップの全体像**や**PQCに対応した製品情報**を含む、**PQCへの移行に向けたガイドラインを公表**（2027年春頃）予定。
  ※自社が保有する情報・システムに適用される暗号の棚卸し
- さらに、当該成果物の発信等を通じ、PQCへの対応を巡る**国際的な議論への貢献**も目指す。

クリプトインベントリの実施に係る実証事業のイメージ



＜PQCへの移行に向けたガイドラインの目次例＞

- **PQC移行の必要性**・リスク
- 移行に向けたステップの**全体像**
- クリプトインベントリ**作成の手順**
- **実証事業の結果**（具体的な事例など）
- 関連情報（**PQC対応製品情報**）など

AIエージェント利活用に伴うリスクへの対応

SC対策強化

- 企業におけるAIエージェントの導入が加速しており、2030年までに**国内市場約3兆円規模へ拡大見込み**。
- 一方で、AIエージェントはその自律性に伴い、**意図しない不正なシステム操作**や**データ漏えいを引き起こす可能性**があり、サイバー攻撃等による**侵害時の影響は甚大**。
- こうした状況を踏まえ、**AIエージェントの導入企業が実施すべきセキュリティ対策（ガバナンス・データ保護・アイデンティティ管理等）**について、**民間企業が参照可能なガイドラインを策定**する。

AIに関連する既存のガイドライン等の整備状況（イメージ）

統一的な指針として：AI事業者ガイドライン(総務省/経済産業省 2026年3月改訂版公開)

AI開発者 / AI提供者 / AI利用者

AIセーフティに関する評価観点ガイド
(AISI 2025年3月改訂版公開)
AIセーフティ評価の観点、想定され得るリスク・評価項目例、評価の実施者等に関する考え方、評価に関する手法の概要を提示。
※他、AIセーフティに関するレッドチーミング手法ガイドも別途存在。

AIのセキュリティ確保のための技術的対策に係るガイドライン
(総務省 2026年3月初版公開)
「AIセーフティにおける重要要素」及び「AIセーフティ評価の観点」を踏まえ、AIの「セキュリティ確保」を取り扱う。脅威への技術的対策例を整理。

AI利用者である**民間企業が参照可能な実務的なガイドラインは存在せず。**

ガイドラインの方向性（イメージ）

1. AIエージェント導入パターン分類
2. AI導入時のリスクアセスメント、及びパターンごとの主要リスク整理
3. リスクに応じた対策の実装例

対策の実装例は、AIエージェント単体において実装される対策に限らず、下記に例示されるような、AIエージェント導入時にそのリスクに応じて求められる、**組織的対策及び企業のIT環境全体において実装すべき技術的対策等を想定**

- ガバナンス
- データ保護
- アイデンティティ管理

（出典）日本経済新聞記事「エージェントもAIで守る」（2025年10月1日） https://www.nikkei.com/article/DGKKZO91645480Q5A930C2TB3000/

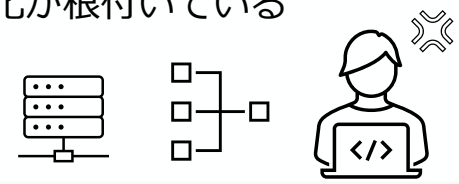
制御系（OT）システムのセキュリティ確保に向けた新たな検討

SC対策強化

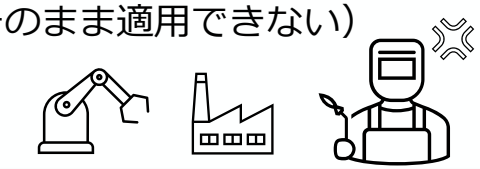
- ITだけでなく、工場の制御系（OT）システムについてもDX化が進む中、IT基盤を経由した攻撃や、オンラインに接続された機器経由での、**OTシステムに影響が及ぶ攻撃等のリスクが高まっている。**
- サイバー事案が発生した際に対応の中核を担うCSIRT（Computer Security Incident Response Team）の整備だけでなく、工場の制御系を中心とした**FSIRT**（Factory Security Incident Response Team）**の整備**や、**両者の一体的な連携、OT固有のセキュリティ対策**についても重要性が増している。
- 上記の状況を踏まえ、「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」を更新し、 **OTシステムのセキュリティ確保に必要な新たな視点を盛り込む。**

現状の課題（As is）

ITシステム
※CSIRTなどのセキュリティ対応方針と文化が根付いている



工場などのOTシステム
※OT固有の要件・セキュリティ対策（ITシステムのセキュリティの考え方がそのまま適用できない）

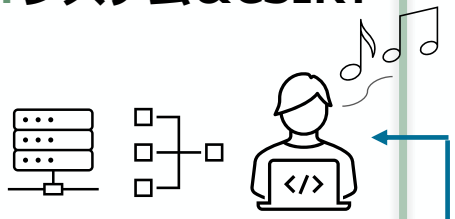


- **IT・OT間の連携が不十分**（連携体制の欠如、OT固有のセキュリティ対策・ベンダ管理等への関与不足等）。

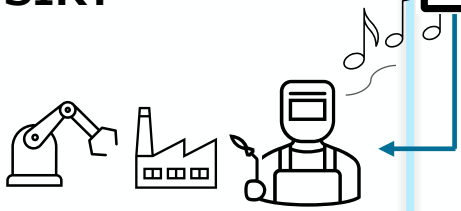
ITシステムがサイバー攻撃を受けると、**OTシステムにも波及**する（工場の稼働停止を余儀なくされる等）。

目指すべき姿（To be）

ITシステム＆CSIRT



工場OTシステム＆FSIRT



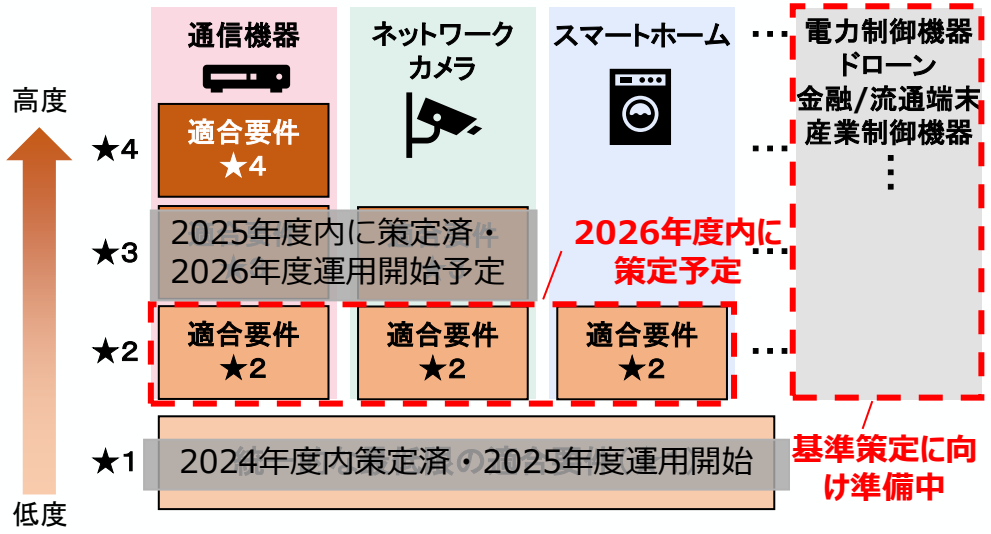
- **IT・OT間が連携**（包括的な監視・CSIRTとFSIRTとの連携体制の構築等）し、一体的かつ有機的に全社のセキュリティを支える。
- IT部門含め全社的に工場OTシステムで用いられる**資産を把握**し、関係する**ベンダとの組織的な連携が**図られている。
- ITシステムがサイバー攻撃を受けても**OTシステムが独立的に動作を継続**する。

IoT製品セキュリティの確保：JC-STAR

SBDの実践

- 2026年2月に**通信機器・NWカメラ★3の適合要件を公開**。今後、スマートホームやその他製品領域（電力、ドローン、産業制御機器等）においても**上位基準の策定に向けた動きを進展**させていく。
- 引き続き、**政府機関・重要インフラ事業者向け**をはじめとする**各種制度等への要件化等**を通じ、JC-STARの活用促進に向けた取組を継続していく。
- 国際的な制度調和に関しては、2026年１月に**JC-STARと英国のPSTI法との相互承認が開始**。同年３月に**シンガポールのCLSとも相互承認**。引き続き**主要国等の海外関連制度との相互承認を追求**していく。

上位基準の策定（★２～★４）



★1の運用開始に引き続き、**2026年2月より通信機器・ネットワークカメラの★3の適合要件を公開**。また、**2026年1月よりスマートホームの★2の適合要件について、IPA内のWGでの議論を開始**。
電力・ドローン・産業制御機器等の上位基準の策定に向け準備中。

制度活用事例（要件化等）

基準・ガイドライン等	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
	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
補助金制度等	再生可能エネルギー導入拡大・系統用蓄電池等電力貯蔵システム導入支援事業費補助金
	長期脱炭素電源オークション
	系統連系技術要件（グリッドコード）

順次拡大予定

海外の関連制度との連携状況

＜英国・シンガポールとの相互承認（概要）＞

JC-STAR→英国PSTI法	**英国PSTI法→JC-STAR**
JC-STAR★１の**ラベルがPSTI法適合証明書に代替。**	JC-STAR★１の求める**３つのセキュリティ要件に関する適合確認を免除。**
JC-STAR→星国CLS※	**星国CLS→JC-STAR**
JC-STAR★１の**ラベルによりCLSレベル１の同等要件に関する適合確認を免除。**	CLSの**ラベルによりJC-STAR★１の同等要件に関する適合確認を免除。**

※CLS: Cybersecurity Labelling Scheme

＜相互承認を目指す他国の制度（例）＞

国・地域	米国	EU
制度名	U.S. Cyber Trust Mark	Cyber Resilience Act（CRA）
任意/義務	任意	義務
対象	消費者用無線IoT製品	デジタル要素を含む製品

ソフトウェアのセキュリティの確保

SBDの実践

- **「ソフトウェアに関するQUAD共通原則」の履行**を目標に、NISTの「**セキュア・ソフトウェア開発フレームワーク**」（**SSDF**）を効果的に**導入・実践するための具体的な方法や手順等をまとめた国内事業者向け文書を成案化**予定（2026年度を予定）。
- 今後、AIコーディングをはじめとする**「AI駆動開発」の台頭に伴うリスクへの対応の在り方**の検討や、**中小ベンダによるSSDF導入・実践の促進**（費用対効果の高いツールの整理等）を進めていく。
- また、国際動向に応じた連携や、**我が国の成果の海外展開**等も引き続き進めていく。

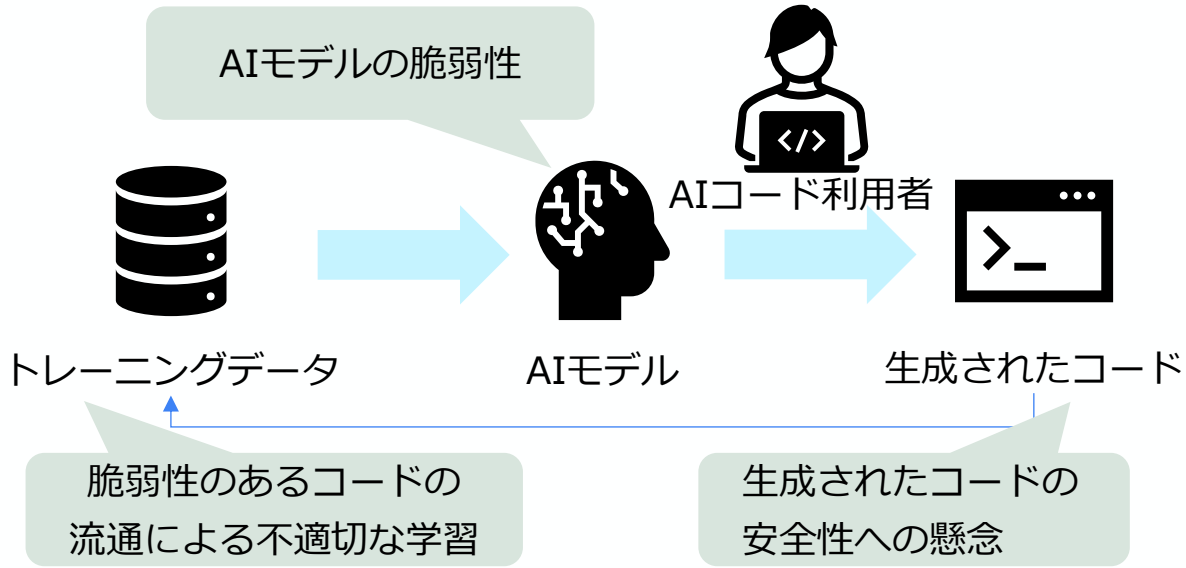

セキュア・ソフトウェア開発フレームワーク
導入ガイダンス案

経済産業省 商務情報政策局
サイバーセキュリティ課

令和８年３月31日

Practice Group	Task ID	Task名称	レベル1	レベル2	レベル3	達成レベル	参考スコア
組織の準備 (PO: Prepare the Organization)	PO.1.1	開発基盤とプロセスのセキュリティ要件定義	○	○	○	Lv2	61%
	PO.1.2	ソフトウェアのセキュリティ要件定義	○	○	○	Lv1	40%
	PO.1.3	サードパーティに求めるセキュリティ要件定義	○	○	○	Lv3	100%
	PO.2.1	役割と責任の定義	○	○	○	Lv2	71%
	PO.2.2	責任を持つ要員への役割ベースのトレーニング	○	○	○	Lv1	28%
	PO.2.3	上層部または権限者のコミットメントの取得	○	○	○	Lv1	40%
	PO.3.1	ツールチェーンに含めるツールの決定	○	○	○	Lv3	100%
	PO.3.2	ツールおよびツールチェーンの導入・運用・保守	○	○	○	Lv1	87%
	PO.3.3	ツールの設定の実施	○	○	○	Lv2	71%
	PO.4.1	ソフトウェアのセキュリティチェック基準の定義	○	○	○	Lv2	79%
	PO.4.2	基準へ準拠するためのプロセスまたは仕組みの実装	○	○	○	Lv1	35%
	PO.5.1	開発基盤の分離および保護	○	○	○	Lv1	40%
	PO.5.2	リスクベースアプローチによる開発エンドポイントの保護	○	○	○	Lv1	8%
ソフトウェアの保護 (PS: Protect Software)	PS.1.1	最小権限の原則に基づく形式コードの保管とアクセス管理	○	○	○	Lv3	100%
	PS.2.1	ソフトウェアの完全性検証に必要な情報の提供	○	○	○	Lv3	100%
	PS.3.1	ソフトウェアリリースとともにデータの安全な保管	○	○	○	Lv1	8%
	PS.3.2	ソフトウェアリリースの全コンポーネントデータの収集	○	○	○	Lv2	70%
安全なソフトウェア開発(PW: Produce Well-Secured Software)	PW.1.1	リスクモデル手法によるソフトウェアリスクアセスメント	○	○	○	Lv2	75%
	PW.1.2	ソフトウェアの要件、リスク、決定事項のトレース・管理	○	○	○	Lv1	37%
	PW.1.3	標準化されたセキュリティ機能およびサービスの利用	○	○	○	Lv3	100%
	PW.2.1	ソフトウェア設計のレビュー	○	○	○	Lv2	72%
	PW.4.1	安全性の高い既存ライブラリ・再利用コンポーネントの取得	○	○	○	Lv1	37%
	PW.4.2	安全性の高い自社製コンポーネントの作成	○	○	○	Lv1	36%
	PW.4.4	サードパーティ製コンポーネントの検証	○	○	○	Lv3	100%
	PW.5.1	選んだセキュアコーディングプラクティスへの準拠	○	○	○	Lv2	80%
	PW.6.1	実行ファイルのセキュリティが向上するツールの利用	○	○	○	Lv1	58%
	PW.6.2	コンパイラ・ビルドツール等の設定の決定および実施	○	○	○	Lv3	100%
	PW.7.1	静的テスト（コードレビュー）方法の決定および実施	○	○	○	Lv1	33%
	PW7.2	組織のセキュアコーディング基準に従ったコードレビューとコード解析の実施	○	○	○	Lv1	58%
	PW.8.1	動的テスト方法の決定	○	○	○	Lv2	80%
	PW.8.2	動的テストの設計および実施	○	○	○	Lv3	100%
	PW.9.1	ソフトウェアのセキュリティに影響を及ぼす設定の決定	○	○	○	Lv1	58%
	PW.9.2	デフォルト設定の偏差と利用者向けの設計上の工夫化	○	○	○	Lv2	80%
脆弱性対応 (RV: Respond to Vulnerabilities)	RV.1.1	ソフトウェアおよびサードパーティコンポーネントの既知脆弱性の調査	○	○	○	Lv2	73%
	RV.1.2	リリース後の継続的なコードレビュー、テスト等による脆弱性の特定または確認	○	○	○	Lv1	37%
	RV.1.3	脆弱性開示と修正ポリシーの策定および実施	○	○	○	Lv2	80%
	RV.2.1	脆弱性情報の収集と分析の実施	○	○	○	Lv3	100%
	RV.2.2	脆弱性に対するリスク低減の決定と対応計画および実施	○	○	○	Lv1	40%
	RV.3.1	検出された脆弱性を分析することによる根本原因の特定	○	○	○	Lv1	8%
	RV.3.2	根本原因を長期的に分析することによるパターンの特定	○	○	○	Lv1	8%
	RV.3.3	類似の脆弱性の積極的な検出	○	○	○	Lv2	70%
	RV.3.4	SDLCプロセスの見直し	○	○	○	Lv3	100%

▲ **SSDFガイドとチェックリスト（案）**



▲ **AI駆動開発（AIコーディング）におけるリスクのイメージ**

IPAにおけるサイバー情報集約・情勢分析能力の強化 CS体制強化

- 国家安全保障戦略に基づく対応強化のため、IPA 第五期中期目標において、**「サイバー状況把握力」を強化**し、**国家の安全保障・経済安全保障の確保に貢献**する旨を明記。
- 今後、**サイバーセキュリティ産業振興の観点**も踏まえながら、**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、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。

サイバー情勢集約・分析機能の強化に向けて進展中の取組

- IPAの有する産業界とのネットワーク、セキュリティ対策に係る各種制度を駆使し、**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**機能を強化。
- 地政学や経済安全保障の専門家の協力も得つつ、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り、**産業分野に関する脅威評価のハブ**として機能。
- 政府機関、産業界の経営レベルと現場の双方との対話を強化し、**防御や抑止対応に資する情報共有／対応支援活動のハブ**として活動を推進。（例：重要インフラ事業者等に対するAPT攻撃に関するハントフォワード活動、主要産業に対するサイバー脅威情報の共有・注意喚起　等）

今後の取組の方向性

＜国の安全保障、経済安全保障の実現に向けた取組への貢献＞

- サイバーインフラ分野における**経済インテリジェンス収集力**の強化
- 経済的威圧に関する**サイバー版机上演習**（TTX）の実施
- 対処機関との**人的交流・共同対処支援の促進**
- サイバー情勢の情報提供を目的とした**産業界との対話の枠組作り**

＜セキュリティ産業振興の観点も踏まえた産業界の防御力強化＞

- **中小企業等向け集団的防御プラットフォーム**（サイバーセキュリティお助け隊サービスを通じたテレメトリ集約分析体制）**の構築**
- **セキュアバイデザイン推進型の中小ソフトウェア開発プラットフォームの構築**

＜サイバー対処能力強化法への貢献＞

- **法定委託事務**（総合的な情報の整理分析報告、資産届出・インシデント報告に関する相談対応、脆弱性情報のトリアージ・エスカレーション等）**実施のための体制強化**
- **企業組織向け相談窓口**の相談受付

サイバー対処能力強化法の成立を踏まえた脆弱性関連情報の取扱い CS体制強化

- サイバー対処能力強化法（令和７年５月成立、公布）の施行に向け、脆弱性のうち、**重要電子計算機に対するサイバー攻撃による被害防止等の観点から必要と認められるもの**については、**政府が必要な対応を行う**ことができるよう、IPAの「情報システム等の脆弱性情報の取扱いに関する研究会」での議論も踏まえ、**脆弱性情報の取扱いに関する告示・ガイドラインの見直し**を実施する。

主な規定事項

① **受付機関（IPA）**は、**調整機関（JPCERT/CC）と必要な連絡・協力**を行いつつ、脆弱性のうち、重要電子計算機の被害防止の観点から必要と認められるものについて、**内閣府に速やかに通知**。

② **内閣府**は、**総合的な判断の下で対応**。その際必要に応じて、
・IPA及びJPCERT/CCに対して指示を行い、強化法の規定に基づき、製品開発者への脆弱性情報の提供・調整や脆弱性への対応方法等の周知等を委託できる。
・**関係する製品開発者の所管省庁（主に経済産業省）**に情報提供を行い、同省庁は、強化法の規定に基づき、**製品開発者に対して**被害防止のために**必要な措置を講ずるよう要請**できる。
・他の行政機関や特定の基幹インフラ事業者などに対し、強化法上の守秘義務等の下で情報提供を行う。

③ **JPCERT/CC**は、発見者から脆弱性情報を入手した場合、**IPAに速やかに通知**。
また、IPAが内閣府への通知が必要と認められるものを峻別するにあたっての必要な協力を行う。

④ **NICT**は、脆弱性を発見した場合、IPAに届け出るとともにJPCERT/CCに連絡し、**連携を取りつつ製品開発者への技術的助言**を行う。（製品開発者による対応方法の作成後、NOTICEプロジェクトを通じた注意喚起を行う。）

「サイバーセキュリティ産業振興戦略」実現に向けた展開 CS能力強化

- 2025年３月にとりまとめた「サイバーセキュリティ産業振興戦略」は、**各種閣議決定文書等に反映**。
- 日本成長戦略会議デジタル・サイバーセキュリティWGの議論等も通じ、政府機関等による有望なセキュリティ製品等の積極的な調達を通じた「実績作り」をはじめ、我が国の**サイバーセキュリティ供給力を強化するための施策を順次実行・深化**させていく。

供給力強化・官民投資促進に向けた今後の主な新たな取組

政府機関等による有望なセキュリティ製品等の活用・評価検証

- 2026年３月より、**IPA**において、**先進セキュリティ製品・サービスを優先調達**し、**検証する取組**を開始。今後、同様の調達の取組を行う**政府機関等の拡大**を図る。

AI等を用いた先進セキュリティ製品等の開発支援

- 2026年度中に、サイバーセキュリティ関連技術に関する懸賞金事業を開始する。
- AI等を用いた先進セキュリティ製品等の開発のために必要な**データ**（政府機関等が収集する脅威情報等）や**計算環境の整備**、**プロジェクトへの支援を各省庁連携で実施**するための枠組みの構築を目指す。

高度セキュリティ供給人材の発掘・育成

- 先進的なセキュリティ製品・サービスを**開発・導入・評価できる人材の発掘・育成**に資する新規プログラムの実施や、**セキュリティ人材のキャリアの魅力発信・活躍機会提供**を通じた母集団拡大を進める。

我が国セキュリティ企業によるアジア太平洋地域への進出後押し

- 我が国企業が多く進出するアジア太平洋地域を中心に、**我が国のサイバーセキュリティ政策の普及・展開を推進**しつつ、当該政策に沿った取組を実装・支援できる**我が国セキュリティ企業の現地進出も後押し**。

今後のロードマップ

■STEP１（約３年以内）【裾野の拡大】
- ✓ スタートアップ数の拡大（J-Startup選定企業等）
- ✓ 「トップガン」人材の増加

■STEP２（約５年以内）【競争力の強化】
- ✓ 我が国企業の市場シェア拡大（量子・AI等先端的な技術の社会実装）

■STEP３（約10年以内）【安全保障・経済政策への貢献】
- ✓ 優れた製品・サービス・企業の影響力拡大
- ✓ ユーザー企業が自社の状況に応じた製品・サービスを選択できる環境構築
- ✓ 我が国特有の攻撃への対応や安全保障・デジタル赤字解消への貢献

【KPI：国内企業の売上高を足下から3倍超（約0.9兆円⇒3兆円超）】

大規模研究開発プロジェクトの拡充

CS能力強化

- 経済安全保障重要技術育成プログラム（先進的サイバー防御機能・分析能力強化）を通じ、我が国のサイバー領域における状況把握力・防御力を向上させるための**約300億円／５年の研究開発プロジェクトを2024年７月から実施**（実施主体：一般社団法人サイバーリサーチコンソーシアム）。
- 今後、**サイバー安全保障に資する技術**や**AIを用いたセキュリティ技術**に対するニーズの増加が見込まれることから、現行のプロジェクトに**新たな研究開発項目を追加**し、**規模を拡大（約400億円）**させる。

現行プロジェクトの主な研究開発内容

1）サイバー空間の情報を収集・調査する状況把握力の向上

- アーティファクト分析技術／攻撃者からより多くの情報を獲得するための技術／高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

2）サイバー攻撃から機器やシステムを守る防御力の向上

- AIを活用した脆弱性探査技術／AI等を活用した防御能力の評価・向上技術／AIを活用したOTペネトレーションフレームワーク技術
- 耐量子計算機暗号技術／耐タンパー性向上技術

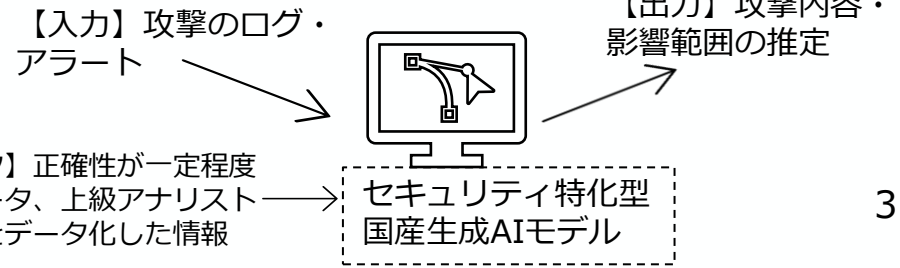
3）共通基盤の整備

- 情報の効果的な連携に関わる技術
- 高度サイバー人材の評価・管理に関する技術

新たな研究開発項目

- 攻撃前の兆候を察知し攻撃者を特定（リアルタイム防御）するための情報収集技術　等
- 攻撃兆候の察知時に、リアルタイムで既に侵入しているマルウェアを機能停止させる（偽情報を与え周辺環境を誤認させる）技術　等
- 国産セキュリティ特化AIモデルの構築　等

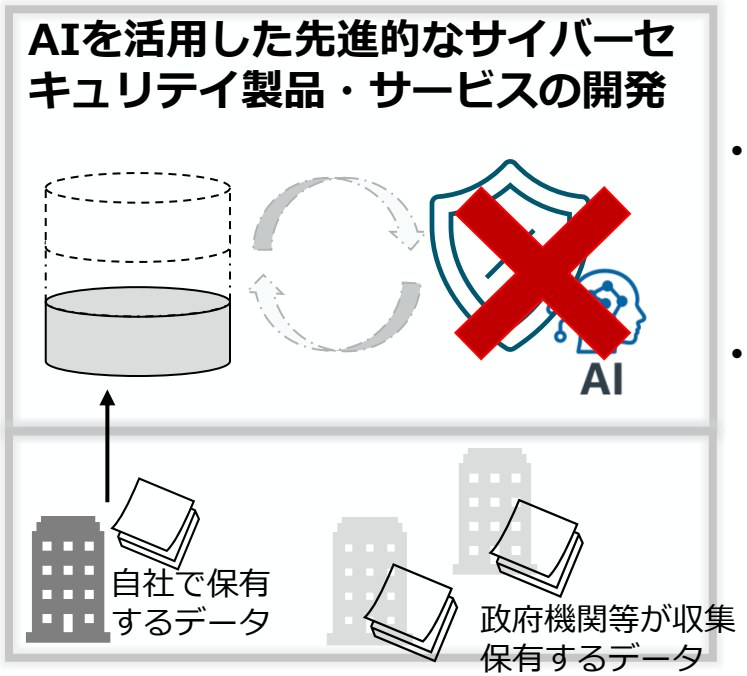
＜国産セキュリティ特化AIモデルのイメージ＞



AIを活用した先進的なセキュリティ製品等の開発・提供支援 CS能力強化

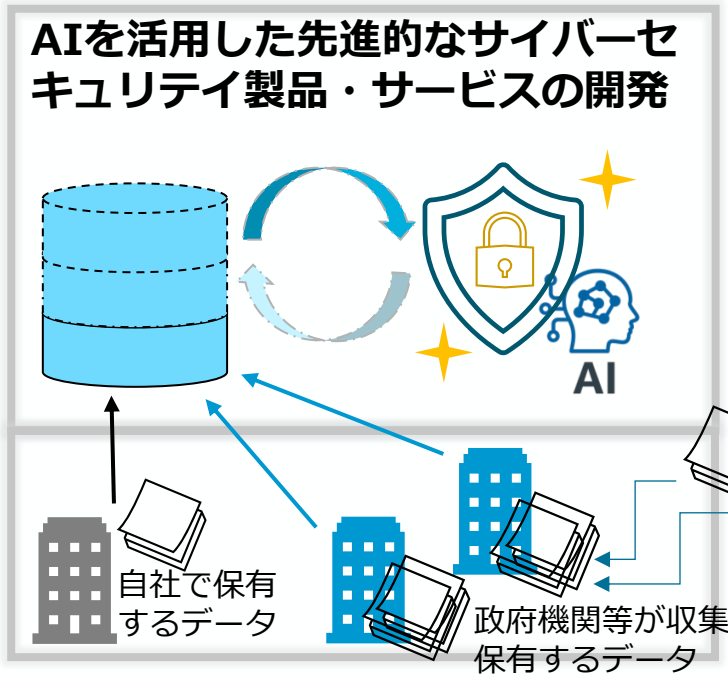
- 今後、AIを活用した先進的なセキュリティ製品・サービスの開発が期待される。他方、AIモデルの開発には必要な**計算環境の整備、データセットの収集・蓄積などが課題**となる。
- こうした課題を解決し、AI等を用いた先進セキュリティ製品等の開発を促進するため、**必要な計算環境の整備、データセットの収集を含めたプロジェクトへの支援**に向けた検討を行う。併せて、**関係省庁との連携**の下、企業側のニーズに応じて、政府機関等で集約した情報等を適切な情報保全等の下で**国内セキュリティ事業者等に対して開放**することも検討する。

現状の課題（As is）



- AIを開発するために必要な**学習データ**（脅威情報等）**の入手が困難**
- **計算資源の確保が困難**

目指すべき姿（To be）



- **脅威情報等必要なデータセットを収集・蓄積**（必要に応じて政府機関等が開放）
- **必要な計算環境を整備**

サイバーセキュリティ・サービス提供事業者の信頼性確認

CS能力強化

- サイバーセキュリティ・サービス（とりわけ、顧客の機微情報やシステムへのアクセスを許容する形態のもの）に対するニーズの増加が今後見込まれる中、**サイバーセキュリティ・サービス提供事業者の体制・措置等に起因する事案等**が生じており、**サービス提供事業者の「信頼性」の一層の強化（厳格な社内体制の整備等）が求められる状況**。
- また、政府機関や安全保障に関係する事業者等においては、**高度な「信頼性」を有するサイバーセキュリティ・サービス事業者を選定・活用するニーズ**が想定される。
- こうしたことを踏まえ、既に技術・品質の基準に基づき登録を行っている現行の「**情報セキュリティサービス審査登録制度」に登録しているサイバーセキュリティ・サービス提供事業者**を対象に、**「事業者の信頼性」を確認**する認定制度を創設するべく、検討を進めていく（2026年５月頃に制度の方向性を提示し、制度の詳細設計を進め、**2027年度中の運用開始を目指す**。）。

情報セキュリティサービス審査登録制度のサービス区分

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

認定制度のイメージ

情報セキュリティサービス審査登録制度のリストに掲載された企業から申請を受け、信頼性を確認、認定。

新たな基準を新設

サービス事業者の高い信頼性を確保するため、事業者における情報の取扱いの適正性等を確認
⇒政府や重要な情報等を扱う民間企業での活用を想定

現行制度（審査登録制度）

幅広い事業者が登録できるよう、技術や品質確保の基本的な基準を提示しているものであるが、あくまで任意制度

４．産業界へのメッセージ

協力：

- 新井　悠　　株式会社NTTデータグループ　エグゼクティブ・セキュリティ・アナリスト（2026年３月時点）
- 鴨田　浩明　　CISO, NTT DATA, Inc. Global
- 川口　洋　　株式会社川口設計　代表取締役
- 佐々木　弘志　　フォーティネットジャパン合同会社　OTビジネス開発部部長　（IPA ICSCoE 専門委員）
- 政本　憲蔵　　株式会社マクニカ　セキュリティ研究センター長

※敬称略、五十音順

「産業界へのメッセージ」の背景

全体向け

- 足下のサイバーセキュリティを取り巻く環境に鑑みれば、**我が国においても一層の対策強化が求められる状況**にある。
  - ① 急速に普及しつつある生成AIをはじめとする**デジタル化の進展**や世界的な**地政学リスクの高まり**、**サイバー攻撃の深刻化・巧妙化**などにより、サイバーリスクは顕在化している。
  - ② このような**サイバー攻撃が、国民生活、社会経済活動及び安全保障環境に重大な影響を及ぼす事案**も既に**複数発生している**。
  - ③ 米欧等においても産業界におけるサイバーセキュリティ対策強化に向けた**制度整備の動きなどが活発化**している。
- こうした状況を踏まえ、**「経済産業省」**としては、**デジタル時代の社会インフラを守る**との観点から、 国家サイバー統括室等関係省庁との連携の下、以下の取組を進めていく。
  - ① **既存施策の普及・啓発**活動の強化
  - ② サプライチェーン全体での対策強化、セキュア・バイ・デザインの実践、政府全体でのサイバーセキュリティ対応体制の強化、サイバーセキュリティ供給力の強化に向けた**新たな施策**
  - ③ 産業界からの意見聴取など、官民の協力関係の維持・発展を前提とした、取組の**不断の見直し**
- 産業界で活動する「**サイバーセキュリティを実践する各企業・団体**」 、「**ITサービス・製品提供事業者**」、「**被害組織を直接支援する専門組織**」、「**中小企業等を支援する機関**」の皆様には、政府の取組も活用・参考いただきつつ、それぞれ**次ページ以降に提示する対応**をお願いしたい。

サイバーセキュリティを実践する各企業・団体（経営層）の皆様へ

経営層向け

- リーダーシップを取ってサイバーセキュリティ対策を推進していただくため、**「サイバーセキュリティ経営ガイドライン」に沿った対応をお願いしたい。**その中でも、最近の国内外の動向を踏まえ、**特に以下の取組を強化していただきたい。**

<サイバーセキュリティ経営ガイドライン（ポイント）>

1．経営者が認識すべき３原則

（1）経営者が、**リーダーシップを取って対策**を進めることが必要
（2）自社のみならず、**サプライチェーン全体にわたる対策**への目配り
（3）平時及び緊急時のいずれにおいても、**社内外関係者との積極的なコミュニケーション**が必要

2．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施による継続的改善
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 事業継続・復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の状況把握及び対策
関係者とのコミュニケーション	**指示10** 情報収集、共有及び開示の促進

1．セキュア・バイ・デザインの実践

- **ITサービス・製品等提供事業者に対してセキュリティ慣行を求める**（JC-STARラベル取得済み製品の優先購入等）。

2．中小企業向け施策の積極的活用（促進）

- 大企業においては、**SCS評価制度**※を**中小企業等との契約時に活用**し、当該取引先に対し★取得に向けた準備や「**サイバーセキュリティお助け隊サービス**」**等の施策活用を促す。**

※「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」。2026年度末頃運用開始予定。

- 中小企業等においては、**中小企業向け施策の活用も検討**する。

3．価値創造経営の一環としての位置付け

- サイバーセキュリティに対する投資を、**中長期的な企業価値向上に向けた取組**の一環として位置付ける。その関連性について、投資家を含む**利害関係者から理解を得るための活動（対話・情報開示等）を積極的に行う。**

サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ（サマリ）

実務層向け

- 最近の国内外の動向を踏まえ、**特に以下の取組を強化していただきたい**（詳細は次ページ以降）。

※ 経済産業省が策定した実務担当者向けガイドラインや関係制度概要など各種政策文書（SCS評価制度構築方針、JC-STAR等）については、参考１のリンクや経済産業省ウェブサイトを参照いただきたい。

１．セキュア・バイ・デザイン等の実践

- 自組織のシステム運用に係るリスク管理について**ITサービス等提供事業者との役割分担を明確化**するとともに、「**セキュア・バイ・デザイン**」や「**セキュア・バイ・デフォルト**」**の製品の購入**（例えば、**JC-STARのラベル取得製品**）**を優先する**など、**ITサービス・製品等提供事業者に対してセキュリティ慣行を求める**
- ITサービス等を外部委託する際には、委託元として**自組織で判断や調整を行わなければならない事項を把握する**とともに、ITサービス等提供事業者に**委託した業務の結果の品質を自社で評価できるよう必要な人材を確保する**

２．サプライチェーン全体での対策強化に向けた対応

- VPN機器等の**脆弱性関連情報を収集し対応**するとともに、ASM（Attack Surface Management）等の外部サービスを活用して**自社のIT基盤やIT資産の現状を把握**する
- 特に大企業においては、サプライチェーンに参加する中小企業等への助言・支援を行う（**「サイバーセキュリティお助け隊サービス」などの支援施策の紹介**、**対策状況調査・改善に向けた対話等**）

３．被害時の専門組織等への相談・報告等

- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照し、サイバー攻撃の被害に遭った場合等には、適時の**専門組織・所管省庁等への相談・報告**等を行う（一定の要件に該当する個人データの漏えい等の場合には個人情報保護委員会に報告する）
- 特に国家支援型と推定される標的型サイバー攻撃の場合は、まず警察やIPA等に相談する

経済産業省「サイバーセキュリティ政策」

サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ（１．詳細）

実務層向け

- 自組織のシステム運用に係るリスク管理について**ITサービス等提供事業者との役割分担を明確化**するとともに、**「セキュア・バイ・デザイン」**※1や**「セキュア・バイ・デフォルト」**※2**の製品の購入（例えば、JC-STARのラベル取得製品）を優先する**など、**ITサービス・製品等提供事業者に対してセキュリティ慣行を求める**
- ITサービス等を外部委託する際には、委託元として**自組織で判断や調整を行わなければならない事項を把握する**とともに、ITサービス等提供事業者に**委託した業務の結果の品質を自社で評価できるよう必要な人材を確保する**

※１　「セキュア・バイ・デザイン」：IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること。前提となるサイバー脅威の特定、リスク評価が不可欠。
※２　「セキュア・バイ・デフォルト」：ユーザー（顧客）が、追加コストや手間をかけることなく、購入後すぐに IT 製品（特にソフトウェア）を安全に利用できること。

背景・補足

- 「セキュア・バイ・デザイン」は、**セキュリティの責任は製造者等が負うべきである（「責任のリバランス」）**という**概念**。2023年10月に我が国を含む13か国が共同署名した**セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンス**にはユーザ組織（顧客）への提言も含まれ、今後、**ユーザー組織における対応が全世界レベルで求められていくことが想定される**。
- 経済産業省では、本文書も踏まえ、**「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」**を2026年3月に公表したところ。この中で、ユーザー組織（顧客）に求められる責務として、リスク管理とセキュアなソフトウェアの調達・運用についても提示している。加えて、セキュアなIoT製品を容易に選択できるよう、**IoTに対するセキュリティ要件適合評価・ラベリング制度（JC-STAR）を2025年３月に運用開始**したところ。積極的にこれらのガイダンスや制度を活用いただきたい。
- 足下で**生成AIやエージェントAI**の利活用が進んでいるが、意図しない不正なシステム操作やデータ漏えいの**リスクが伴う点には注意が必要**。経済産業省では、今後、エージェントAIの「導入時」から組織全体で実施すべきセキュリティ対策を整理する予定。
- ITサービス・製品等提供事業者に対してセキュリティ慣行を求めることに関して、外部委託契約書等に、**セキュリティインシデント発生時の連携体制**や、**契約違反時の具体的なペナルティ**（損害賠償、契約解除の条件等）を**明文化**することも考えられる。

サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ（２．詳細①）

実務層向け

- VPN機器等の**脆弱性関連情報を収集し対応**するとともに、ASM（Attack Surface Management※）等の外部サービスを活用して**自社のIT基盤やIT資産の現状を把握**する

※ASM（Attack Surface Management）：組織の外部（インターネット）からアクセス可能なIT資産（=攻撃面）を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスをいう。

背景・補足

- サプライチェーン全体での対策を強化する上で、まずは自社のセキュリティ対策を確認・強化することが第一歩である。例えば、経済産業省の「サイバーセキュリティ経営ガイドライン」では、PDCA サイクルによるサイバーセキュリティ対策の継続的改善の重要性に触れており、必要に応じて、目的に応じた脆弱性診断やペネトレーションテスト、情報セキュリティ監査等の外部サービスを利用するといった対策例を示している。

- 2026年度末頃に制度運用開始を予定している「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」では、**脆弱性など最新状況の把握と反映を★４取得の要求事項の一つとして、自社のIT基盤やIT資産の現状把握を★３取得の要求事項の一つとして、それぞれ位置づけ**ている。 DXの進展等に伴いサイバー攻撃の起点が増加する中、このようなリスクを特定する取組は今後一層求められる状況にある。

- 足下では、外部（インターネット）との境界に配置される機器（**VPNやゲートウェイ等**）について**重大な脆弱性が報告**されている。IPAやJPCERT/CC等による注意喚起情報や、セキュリティ関連製品・サービスの事業者等とのコミュニケーションを通じて積極的に**脆弱性関連情報を収集**することや、脆弱性が発見された場合には、**リスク評価に基づき優先度を設定**した上で、**重大度に応じた合理的な期限を定めて**対応すること、そうした機器の導入・継続利用の要否について**定期的に見直す**ことも必要。

  ※　（補足）昨今生じた事案に鑑みると、不正侵入経路の確認だけでなく、ネットワーク接続やデータ転送を監視し、不正アクセスを検知・遮断できる体制の構築・機器等の導入も重要である。

- この点、例えば、外部（インターネット）から把握できる情報を用いてIT資産の適切な管理を可能とする**ASMは**、VPN（Virtual Private Network）などの不正侵入経路となりうるポイントを把握する上で**有効な対策**とされている。経済産業省が公表している「ASM（Attack Surface Management）導入ガイダンス」などを参照することができる。

サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ（２．詳細②）

実務層向け

- 特に大企業においては、サプライチェーンに参加する中小企業等への助言・支援を行う（**「サイバーセキュリティお助け隊サービス」などの支援施策の紹介、対策状況調査・改善に向けた対話等**）

背景・補足

- サプライチェーン全体のセキュリティ対策水準を強化するためには、自社のサプライチェーン上にある（＝取引先である）、**中小企業等におけるセキュリティの確保も求められる**。「サイバーセキュリティ経営ガイドライン」においても、以下の対策例が掲げられている。
  - サプライチェーン上での対策の底上げの手段として、「サイバーセキュリティお助け隊サービス」等の中小企業向け施策を活用する
    - ※　「サイバーセキュリティお助け隊サービス」は、中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価（例：月額1万円以内）に提供するサービス。約9,200件の利用実績（2025年９月末時点）がある。デジタル化・AI導入補助金「セキュリティ対策推進枠」を活用することで、最大150万円まで、導入費用の1/2（小規模事業者は2/3）の補助を受けられる。
  - サプライチェーンにおけるサイバーセキュリティ対策を担保する手段として、**第三者による評価検証結果を活用する**

- なお、取引先に対してサイバーセキュリティ対策を要請するケースも想定されるが、その際、独占禁止法等**関係法令の適用関係**が論点となる。こうした課題に対応するため、経済産業省と公正取引委員会は、取引先への対策の支援・要請に係る関係法令の適用関係について整理した文書や、独占禁止法や取適法との関係で「問題とならない」ケースを想定した事例等を公表している。中小企業庁「パートナーシップ構築宣言取組事例集Ver1.2」においても、**サプライヤー向けの対策状況調査（アンケート調査）・フィードバック（リスクの解説や改善方法のヒント提供）**に努めている事例も掲載されている。**取引先とのパートナーシップ構築**の観点からも、こうした文書や取組事例を参考とすることが有用である。

- その上で、サプライチェーン全体でのセキュリティ対策を強化する観点から、自社だけでなく**取引先に対して**、**「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」**（2026年度末頃に制度運用開始予定）**の”★”取得に向け準備**を進めるよう、お願いしていただきたい。
  - ※　同制度の”★”取得の要請だけでなく、同制度の評価基準を活用することも、同制度の活用の在り方として、考えられる。

サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ（3．詳細）

実務層向け

- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照し、サイバー攻撃の被害に遭った場合等には、適時の**専門組織・所管省庁等への相談・報告**等を行う（一定の要件に該当する個人データの漏えい等の場合には個人情報保護委員会に報告する）
- 特に国家支援型と推定される標的型サイバー攻撃の場合※に、まず警察やIPA等に相談する

※標的型攻撃メールを受け取った場合やネットワーク貫通型攻撃などの標的型攻撃に曝された場合等

背景・補足

- サイバー攻撃が深刻化・巧妙化するなど、サイバーリスクが高まる中、**どのような企業・団体においても**、自組織がサイバー攻撃の被害に遭った場合に**適切なハンドリング（インシデント対応）を行うことが、一層重要な状況**。
- インシデント対応の一環として、被害組織がサイバーセキュリティ関係組織（被害組織を直接支援する専門組織等）と**サイバー攻撃被害に係る情報を共有することは、攻撃の全容を解明する観点から重要**。政府機関や専門組織からは、報告したことによる不利益が生じないような配慮を前提として、**関連する情報の提供や対応に関して助言を受けることなども期待**できる。また、自組織が受けたサイバー攻撃被害の状況や対応内容について、**適切なタイミングで対外的に公表することは**、利害関係者からの信頼を確保し**当該企業・団体のレピュテーションを保護する観点からも重要**。ただし、国家支援型と推定される標的型サイバー攻撃を受けた場合には、サイバー対処能力強化法の趣旨も踏まえ、対応についてまずは政府機関に相談することが、被害組織・政府機関の双方にとって、状況把握の観点から望ましい。
- こうした背景の下、2023年３月に経済産業省及び関係省庁等にて実務者向けのガイダンスを公表したところ。当該ガイダンスでは、被害組織を保護しながら、**いかに速やかな情報共有や目的に沿ったスムーズな被害公表が行えるのか、実務上の参考となるポイントをFAQ形式で整理しており、サイバー攻撃の被害時における情報共有・公表の在り方として参考**となる。
- また、サイバーセキュリティ経営ガイドラインの**付録C「サイバーセキュリティインシデントに備えるための参考情報」**でも、インシデントにおいて経営者が行うべき事項や組織内で整理しておくべき事項を提示しており、一つの参照点となり得る。
- 経済産業省では、これら文書の周知・啓発活動に加え、**IPAやJPCERT/CCを通じた被害組織への情報提供・初動対応支援**を行っている。政府全体としても、被害組織の負担軽減と政府の対応迅速化を図るため、インシデント**報告様式の一元化**等にも取り組んでいる。

ＩＴサービス・製品提供事業者の皆様へ

提供事業者向け

- **提供する製品・サービスのセキュリティ対策に責任を持ち、「セキュア・バイ・デザイン」**※1**や「セキュア・バイ・デフォルト」**※2**の考え方に沿った対応（「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」への準拠**や、**JC-STARのラベル取得**等）をお願いしたい。
- また、自組織も「サイバーセキュリティを実践する企業」であり、かつ、ユーザー企業にも影響を及ぼし得る存在であることを認識して、**サイバーセキュリティ対策に取り組む**ことをお願いしたい。

※1　「セキュア・バイ・デザイン」：IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること
※2　「セキュア・バイ・デフォルト」：ユーザー（顧客）が、追加コストや手間をかけることなく、購入後すぐに IT 製品（特にソフトウェア）を安全に利用できること。

背景・補足

- 「セキュア・バイ・デザイン」は、**セキュリティの責任は製造者等が負うべきである（「責任のリバランス」）**、という**欧米諸国を中心に提唱されている概念**。2023年10月に我が国を含む13か国が共同署名した**セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンス**の中でも、組織の変革を実行できる**経営層の意思決定者による**、製品開発の重要な要素としてセキュリティを優先させるという**コミットメントの重要性**が言及されている。**今後、当該提言を踏まえた対応が全世界レベルで求められていくことが想定される**。

- 経済産業省では、本文書も踏まえ、**「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」**を2026年3月に公表したところ。この中で、ＩＴサービス・製品提供事業者に求められる責務として、セキュリティ品質を確保したソフトウェアの設計・開発・供給・運用等についても提示している。加えて、 **IoTに対するセキュリティ要件適合評価・ラベリング制度（JC-STAR）を2025年３月に運用開始**し、セキュアなIoT製品を容易に選択できる環境整備を進めているところ。積極的にこれらのガイダンスや制度を活用いただきたい。さらに足下では、生成AIの台頭等を受けて、AIコーディングなどのAI駆動開発を通じたサービス提供に係るセキュリティリスクが懸念される状況にある。経済産業省としても、こうした新たな課題に対する対応を進めていく。

- また、近年、**ITサービス・製品提供事業者におけるサイバー事案**もみられるところ、自らも「サイバーセキュリティを実践する企業」であり、**ユーザー企業にも影響を及ぼし得る存在**であることを認識して、対策に取り組んでいただく必要がある。 2026年度末頃に制度運用開始を予定している**「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”★”取得に向け準備**を進めていただきたい。

被害組織を直接支援する専門組織の皆様へ

専門組織向け

- サイバー攻撃の被害組織に対するより効果的・効率的な支援を可能とする観点から、「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」の成果物である**「攻撃技術情報の取扱い・活用手引き」**を活用して**専門組織間で必要な情報を積極的に共有することをお願いしたい。**
- その前提として、情報共有活動のメリットにも触れつつ、**「秘密保持契約に盛り込むべきモデル条文案」**を活用して、攻撃技術情報の共有について**被害組織と合意する努力**をお願いしたい。

背景・補足

- サイバー攻撃が高度化する中、攻撃の全容の把握や被害の拡大を防止する等の観点から、**被害組織を直接支援する専門組織を通じたサイバー被害に係る情報の速やかな共有が重要。**
- 経済産業省では、既存の情報共有活動の枠組みも活用しながら、更に円滑な情報共有を可能とするために、**被害組織の同意を個別に得ることなく速やかな情報共有が可能な情報の考え方を整理**し、検討会の最終報告書として2023年11月に公表。具体的には、通信先情報やマルウェア情報、脆弱性関連情報等の「攻撃技術情報」から被害組織が推測可能な情報を非特定化加工した情報が対象となり得ると整理。
- その補完文書として、①専門組織間で効果的な情報共有を行うために、どのような形で非特定化加工を行えば良いかなど**専門組織として取るべき具体的な方針について整理した「攻撃技術情報の取扱い・活用手引き」**と、②上記考え方についてユーザー組織と専門組織が共通の認識を持ち、専門組織が非特定化加工済みの攻撃技術情報を共有したことに基づく法的責任を原則として負わないことを合意するための**秘密保持契約に盛り込むべきモデル条文案**を提示。
- 経済産業省として、これらの成果物について、**専門組織やユーザー企業の経営層への意識啓発も含めた周知・啓発活動を行う。**

中小企業を支援する機関の皆様へ

支援機関向け

- **中小企業等の「主治医」**としてデジタル化やDX化等を伴走的に支援する役割が期待される支援機関（商工会議所、商工会、地域金融機関、ITベンダー、士業等）の皆様には、**以下の取組をお願いしたい。**

1．中小企業向け施策・コンテンツの活用促進

- 中小企業等に対するデジタル化・DX化や経営支援、それらに関連するセミナーの開催等に当たっては、**「サイバーセキュリティ」の観点も考慮**（セミナーにおいて一枠設ける等）いただきたい。その際、**IPAのセミナー開催支援制度**や、中小企業にとって身近なサイバー事案を基にした机上演習コンテンツ等も活用いただくことが可能。
- その上で、**SECURITY ACTION宣言（SA宣言）の実践**や**SCS評価制度の”★”取得に向けた準備**、最低限必要なセキュリティ対策（監視・駆付け・保険）を安価でワンパッケージにまとめた「**サイバーセキュリティお助け隊サービス**（１類・２類）」**の導入**※、**中小企業の情報セキュリティ対策ガイドライン**の**参照**を中小企業等に**促していただきたい。**

※SCS評価制度の”★”取得を伴走支援するサイバーセキュリティお助け隊サービス（新類型）の創設に向けた実証事業への参加呼びかけもお願いしたい。

2．登録セキスペ（セキュリティ専門家）の活用

- 中小企業に対する**外部専門家の派遣や紹介・相談会の開催**を検討する場合、サイバーセキュリティに課題を抱える中小企業を外部から支援することが可能な情報処理安全確保支援士（登録セキスペ）のリストを積極的に活用いただきたい。
- 支援機関の相談窓口にも同リストの人材を配置する等、支援機関自身でも同リストを活用いただきたい。

3．地域SECUNITY（セキュリティ・コミュニティ）活動への参加

- 地域の中小企業経営者向け演習やセキュリティ担当者向けセミナー、情報発信、人材育成等、地域でサイバーセキュリティの普及・啓発活動を実施している**地域SECUNITYの活動に参加し**、身近な**中小企業等にも周知いただきたい。**

（参考１）産業界へのメッセージに対応した政府文書・窓口等

- **サイバーセキュリティを実践する各企業・団体向け**

○経営層向け

- 経済産業省「サイバーセキュリティ経営ガイドライン　Ver3.0」（令和５年３月改訂）
- 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（SCS評価制度）」（令和８年３月制度構築方針公表）
- IPA「サイバーセキュリティお助け隊サービス制度」

○実務層向け

- 経済産業省「サイバーセキュリティ政策」

（１．詳細）

- 国家サイバー統括室「国際共同ガイダンス「セキュアバイデザイン・セキュアバイデフォルト原則」に署名（令和５年10月）
- 経済産業省／国家サイバー統括室「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」（令和８年３月）
- IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」

（２．詳細）

- 経済産業省「サイバーセキュリティ経営ガイドラインと支援ツール」
- 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（SCS評価制度）」（令和８年３月制度構築方針公表）
- IPA「重要なセキュリティ情報」
- 経済産業省「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」（令和５年５月）
- IPA「サイバーセキュリティお助け隊サービス制度」
- 中小企業庁「『パートナーシップ構築宣言』ポータルサイト」
- 経済産業省「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」
- 中小企業庁「中小企業の情報セキュリティ」
- IPA「ここからセキュリティ！」「中小企業の情報セキュリティ」

（３．詳細）

- サイバー攻撃被害に係る情報の共有･公表ガイダンス検討会「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和５年３月）
- 経営ガイドラインの付録C「サイバーセキュリティインシデントに備えるための参考情報」（令和５年３月）
- 個人情報保護委員会「漏えい等の対応とお役立ち資料」
- 警察署又は都道府県警察本部「相談窓口」
- IPA「コンピュータウイルス・不正アクセスに関する届出」「企業組織向けサイバーセキュリティ相談窓口」
- JPCERT/CC「インシデント対応依頼」

- **ＩＴサービス・製品提供事業者向け**
  - 国家サイバー統括室「国際共同ガイダンス「セキュアバイデザイン・セキュアバイデフォルト原則」に署名（令和５年10月）
  - 経済産業省／国家サイバー統括室「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」（令和８年３月）
  - IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」
  - 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（SCS評価制度）」（令和８年３月制度構築方針公表）

- **被害組織を直接支援する専門組織向け**
  - 経済産業省「サイバー攻撃による被害に関する情報共有の促進に向けた検討会　報告書等」（令和６年３月）

- **中小企業を支援する機関向け**
  - IPA 「地域団体等との連携による中小企業のサイバーセキュリティ対策普及促進のためのセミナー開催支援」
  - IPA「中小企業の情報セキュリティ対策ガイドライン」
  - IPA「中小企業向けサイバーセキュリティ対策支援者リスト」
  - 経済産業省「地域SECUNITY（セキュリティ・コミュニティ）」

（参考２）産業界における積極的な取組例①

- 産業界においても、一部業界でのSBOMの活用促進や国内サイバーセキュリティ供給力強化に向けた事業者コミュニティの立ち上げ、中小企業等向けサイバーセキュリティ対策啓発活動、セキュリティ投資判断に資する情報提供など、当省のサイバーセキュリティ政策の方向性に沿った**積極的な取組が進展**。
- こうした産業界における積極的な取組を慫慂しつつ、今後も引き続き**産業界全体のサイバーセキュリティ対策の強化に向けた政策を強力に推進**していく。

【事例①】自動車業界におけるSBOM活用・理解促進

- ✓ J-Auto-ISACが「**クルマのサイバーセキュリティにおけるSBOM活用（初版）**」を2025年12月に発行。
- ✓ OSSの脆弱性管理を中心に、SBOMの導入・共有・運用・廃棄に係る実務を体系化したもの。
- ✓ 経済産業省**「ソフトウェア管理に向けたSBOMの導入に関する手引Ver.2」を引用・参照**。
- ✓ 自動車業界の各社が抱えるSBOM活用の課題を整理し、業界全体での解決方針の共通化を目指したもの。

【事例②】日本サイバーセキュリティ産業振興コミュニティの設立

- ✓ 我が国のサイバーセキュリティ産業を強化・育成するための新たな枠組みとして、2025年12月に**日本サイバーセキュリティ産業振興コミュニティが設立**。
- ✓ **セキュリティ製品・サービスの開発・提供を行う事業者**や**事業化を進めるスタートアップ**等、34社が一般会員として参画（設立時点）。
- ✓ 今後、我が国**セキュリティ・サービスのマッピング・スコアリング**や**海外展開に向けた活動**等を実施。

【事例③】横須賀でのSECURITY ACTION自己宣言への伴走支援

- ✓ 「YOKOSUKA情報セキュリティプロジェクト」では、**中小企業のSECURITY ACTION自己宣言（SA宣言）の支援策として、「二つ星宣言手順書」**を作成し、中小企業のSA宣言を後押し。
- ✓ 支援策の成果により、2024年度から2025年度の2年間で、**横須賀市内における200件以上のSA宣言を後押し**。
- ✓ セミナーなどの啓発活動を通じて、中小企業へのセキュリティ対策の意識付けを実施。

（出典）各種公開情報・報道より作成。

（参考２）産業界における積極的な取組例②

- 産業界においても、一部業界でのSBOMの活用促進や国内サイバーセキュリティ供給力強化に向けた事業者コミュニティの立ち上げ、中小企業等向けサイバーセキュリティ対策啓発活動、セキュリティ投資判断に資する情報提供など、当省のサイバーセキュリティ政策の方向性に沿った**積極的な取組が進展**。
- こうした産業界における積極的な取組を慫慂しつつ、今後も引き続き**産業界全体のサイバーセキュリティ対策の強化に向けた政策を強力に推進**していく。

【事例④】企業規模・業種別に見るセキュリティ投資・人員数の目安値の公表

- ✓ 一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）は、2026年2月13日、国内企業を対象にした「**企業規模・業種別に見るセキュリティ投資・人員数の目安値**」レポートを発表。
- ✓ 多くの企業でセキュリティ投資や人員などのリソース確保が進まない原因は、その**妥当性を判断できる指標が存在しない**ことにあると考えに基づき、**企業が経営判断に活用できる実務的な指標を提示**することを目指すもの。
- ✓ 今回、我が国で初めて**企業規模・業種別**の「セキュリティ投資額および人員数の目安値」を提示。併せて、CISO・部門長クラスへのインタビューを通じて、数値の裏付けとなる実態、経営層への説明の工夫、人材・組織の課題など、**現場の知見も提示**。

＜セキュリティリソースの目安値概要及びセキュリティ責任者向け・経営層向け提言（レポートより抜粋）＞

#	企業の類型		セキュリティ投資額/売上高の目安値	セキュリティ人員数/全従業員数の目安値
	企業規模	業種	売上高の	全従業員の
1	大企業（売上高1000億円~）	金融	0.6%	0.8%
2		IT･情報通信	0.5%	0.6%
3		社会インフラ	0.3%	0.3%
4		製造	0.2%	0.2%
5		小売･サービス･その他	0.1%	0.2%
6	中堅企業（売上高100億円~1000億円）		0.3%	0.2%

【セキュリティ責任者向け提言】

- **提言１：目安値を使って、現在地を経営層に示せ**
- **提言２：目安値を使って、目的地を経営層に示し必要なセキュリティリソースを確保せよ**

【経営層向け提言】

- **提言１：目安値を使って、現在地を把握せよ**
- **提言２：目安値を使って、目的地達成のためのセキュリティリソース確保にコミットせよ**

（出典）一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）「企業規模・業種別に見るセキュリティ投資・人員数の目安値　～DX with Security を実現するために必要なリソース水準とは～」

参考

1. 体制及び関連会議の実績
2. サプライチェーン全体での対策強化
3. セキュア・バイ・デザインの実践
4. 政府全体でのサイバーセキュリティ対応体制の強化
5. サイバーセキュリティ供給能力の強化
6. 政府全体の動向

１．体制及び関連会議の実績

産業サイバーセキュリティ研究会とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日
第２回：平成30年　5月30日
第３回：平成31年　4月19日
第４回：令和　2年　4月17日※
第５回：令和　2年　6月30日
第６回：令和　3年　4月　2日
第７回：令和　4年　4月11日
第８回：令和　6年　4月　5日
第９回：令和　7年　5月23日
第10回：令和 8年　4月　3日

※電話開催

＜構成員＞　※2026年4月開催時点

伊藤　栄作　三菱重工業株式会社　取締役社長

遠藤　信博　日本経済団体連合会　副会長・サイバーセキュリティ委員長、日本電気株式会社　特別顧問

片野坂真哉　一般社団法人日本情報システム・ユーザー協会　会長、ANAホールディングス株式会社　取締役会長

寺田　航平　経済同友会　副代表幹事、寺田倉庫株式会社　代表取締役社長

東原　敏昭　株式会社日立製作所　取締役会長　代表執行役

船橋　洋一　公益財団法人国際文化会館 グローバル・カウンシル チェアマン

星野　理彰　NTT株式会社　代表取締役副社長　副社長執行役員 CTO

村井　純(座長)慶應義塾大学　特別特区特任教授／名誉教授

渡辺　佳英　日本商工会議所　特別顧問、大崎電気工業株式会社　取締役会長

＜オブザーバー＞
国家サイバー統括室、警察庁、金融庁、デジタル庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省、防衛装備庁

WG１（実効性強化・国際連携）

- ガイドライン等の実効性強化
- 国際的な制度調和に向けた連携

第１回：平成30年　2月　7日
第２回：平成30年　3月29日
第３回：平成30年　8月　3日
第４回：平成30年12月25日
第５回：平成31年　4月　4日
第６回：令和　2年　3月（書面開催）
第７回：令和　2年10月（書面開催）
第８回：令和　3年　3月15日
第９回：令和　4年　4月　4日
第10回：令和 6年　3月14日
第11回：令和 7年　4月14日
第12回：令和 8年　3月10日

WG２（地域・中小企業支援）

- 地域・中小企業等における対策支援

第１回：平成30年　3月16日
第２回：平成30年　5月22日
第３回：平成30年11月　9日
第４回：平成31年　3月29日
第５回：令和　2年　1月15日
第６回：令和　2年　8月25日
第７回：令和 3年2月18日
第８回：令和 4年3月23日
第９回：令和 5年3月27日
第10回：令和6年3月25日
第11回：令和7年4月15日
第12回：令和8年3月　3日

WG３（産業振興・人材育成）

- セキュリティ産業振興、研究開発
- 人材育成・確保

第１回：平成30年4月　4日
第２回：平成30年8月　9日
第３回：平成31年1月28日
第４回：令和 元年8月　2日
第５回：令和　2年3月（書面開催）
第６回：令和 3年3月10日
第７回：令和 4年4月　6日
第８回：令和 6年4月　3日
第９回：令和 7年4月17日
第10回：令和8年3月12日

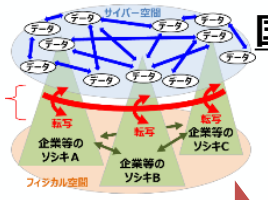
２．サプライチェーン全体での対策強化

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）が盛り込まれた国際規格の策定・CPSF改訂に向けた検討

- ISO/IECの国内エキスパートの協力のもと、CPSFのモデル等を盛り込んだ国際規格（TS:技術仕様書）策定を推進（ISO/IEC JTC1/SC27にてTS 5689としてプロジェクトが進行中）。2025年3月の国際会合にて承認段階（DTS）への移行が決定。**2026年夏頃までの発行を目指す**。
- また、2019年のCPSF ver1.0策定から６年が経過し、サイバー・フィジカル・セキュリティをめぐる国際情勢は大きく変化している。他国で改訂が進んでいる**サイバーセキュリティ関連の国際規格**（NIST CSF2.0等）の更新等の変化を踏まえ、 IPAデジタルアーキテクチャ・デザインセンター（DADC） において、引き続き**CPSFの改訂**作業も進める。

CPSF国際規格(TS 5689)

CPSFのモデル



CPSFのモデル
・「3層構造」
・「6つの構成要素」
を盛り込んだドラフト

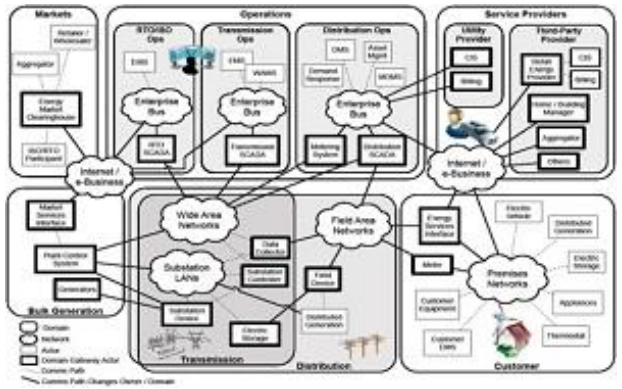
国際標準化団体へ提案

ISO　IEC
JTC 1
SC 27
WG4

WG4の動き	
2023	10月 提案NP投票実施
2024	原案作成
2025	7月 承認段階(Draft Technical Specification)へ移行
2026	夏頃に国際規格(Technical Specification)発行予定

NIST Cybersecurity Frameworkの改訂

- 米国では**標準技術機関**のNISTおいて、**専門性を活かして**CSFを策定
- **CSF 2.0（2024年２月に公表）では、**対象者を重要インフラ事業者から**中小企業を含む様々な企業へ拡大**
- Ver1.0の5つ機能に、GV（統治）が追加され計6機能に



図：Cyber Physical Systems

CSF2.0における6つの機能

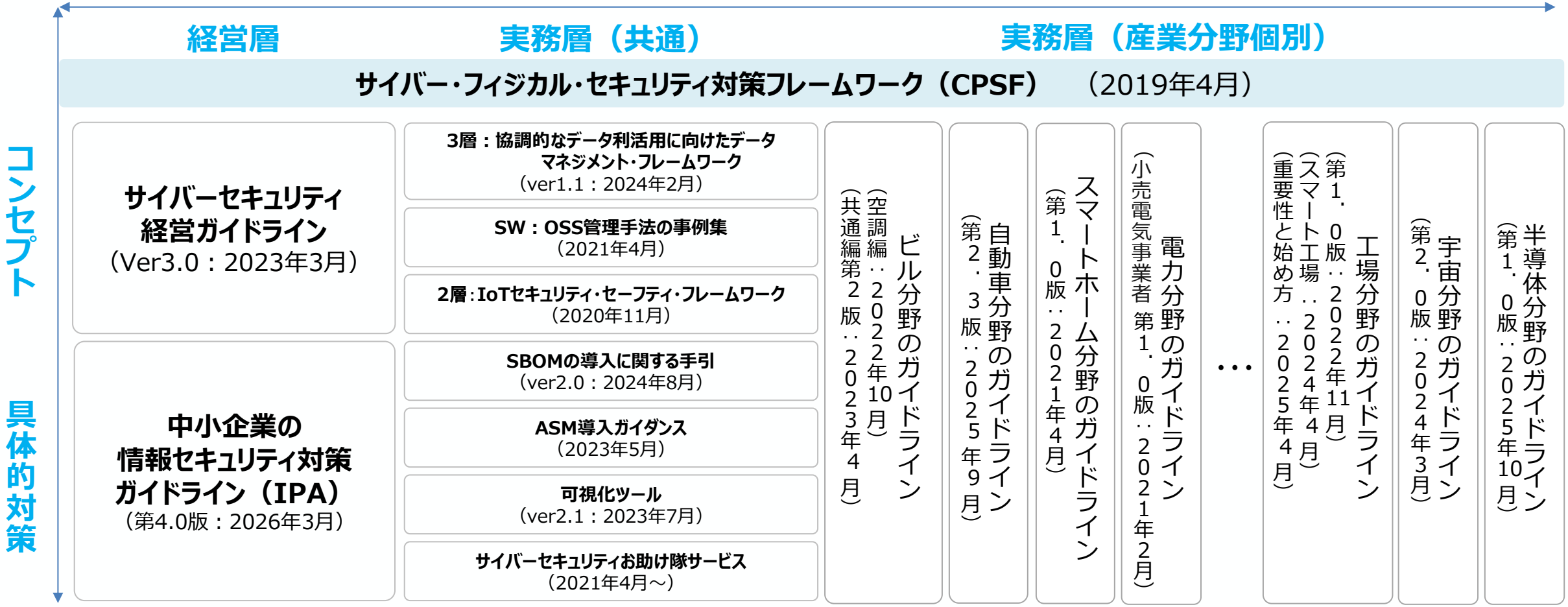
統治　特定　防御　検知　対応　復旧

（出典）NIST https://www.nist.gov/itl/ssd/cyber-physical-systems

CPSF関連ガイドライン

- CPSFに沿って、**対象者や具体的な対策を整理**し、実践的なガイドラインを整備。

主なガイドラインや対策ツール



CPSF個別分野別動向

- **産業分野別サブワーキンググループ**を設置。CPSFに基づくセキュリティ対策の具体化を推進。
- 今後は、政府と産業界の協業を進めつつ、国際的なルール形成の推進に向けた取組や、**サプライチェーン全体のセキュリティ向上に向けた取組の実装**を進める。

産業サイバーセキュリティ研究会WG１（実効性強化・国際連携）

標準モデル（CPSF） Industry by Industryで検討
（分野ごとに検討するためのSWGを設置）

ビルSWG

- 事前対策が中心の第1版にインシデントレスポンスを追加したガイドライン第2版を公開（2023年4月）。個別編(空調システム)ガイドライン第1版を公開（2022年10月）。

防衛産業SWG

- 米国の新標準と同程度まで強化した新情報セキュリティ基準を策定（2022年4月1日）。

スマートホームSWG

- ガイドライン1.0版（2021年4月）に従い、**JC-STAR★2整備・活用**に向けた**スマートホーム関連IoT機器のセキュリティ要件案（2025年3月）を策定。2026年1月に改定**。

宇宙産業SWG

- 宇宙分野における民間事業者の役割拡大や、米国等における官民の取組を踏まえ、2021年１月に立ち上げ。
- **2024年3月に公開したガイドライン Ver 2.0を英訳**。

電力SWG

- 電力分野のサプライチェーン・セキュリティ向上策を提言（2024年3月）。
- 「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ガイド」と「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」を公表（2024年3月）。
- **「電力制御システムのサプライチェーン・セキュリティ対策の手引き」を公開（2025年6月）**。

自動車産業SWG

- エンタープライズ領域（会社全体のベースとなるOA環境）対象とした「自工会／部工会サイバーセキュリティガイドライン1.0版」を策定（2020年12月）し、サプライチェーンへの展開を実施。**「自工会／部工会サイバーセキュリティガイドライン2.3版」を公開（2025年9月1日）**。

工場SWG

- 主に中小規模の工場を有する製造事業者の経営層や工場セキュリティ担当者に向けたAppendix【工場セキュリティの重要性と始め方】を公開（2025年4月）。

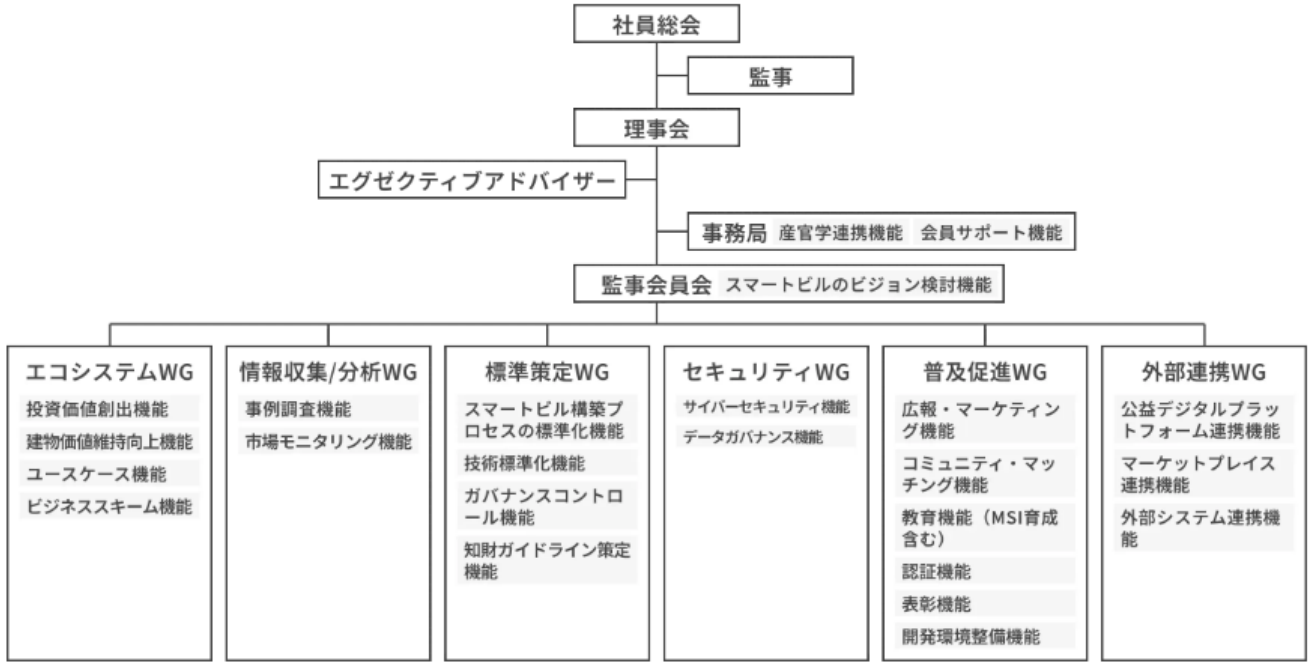
半導体産業SWG

- **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を、英訳版も含めて公表（2025年10月）**。
- 投資促進関係施策の要件等とも紐づけることを念頭にした**「半導体デバイスメーカーに対するセキュリティ要求事項」を策定（2026年1月）**。

ビルSWG（座長：東京大学 江崎教授）

- 本SWGを2025年4月2日に発足した**「一般社団法人 スマートビルディング共創機構」に移行**。
- 2025年8月にセキュリティWGのキックオフを実施し、スマートビルのセキュリティ（サイバー／フィジカル）に係る制度・技術・標準化を**一体的に政策展開する戦略を検討**。

スマートビルディング共創機構の組織体制



セキュリティWG（サイバーセキュリティ機能）
経済産業省が主管として進めていた産業サイバーセキュリティ研究会WG1ビルSWGでの検討の引き継ぎ

サイバーセキュリティSWG キックオフ参加 32社

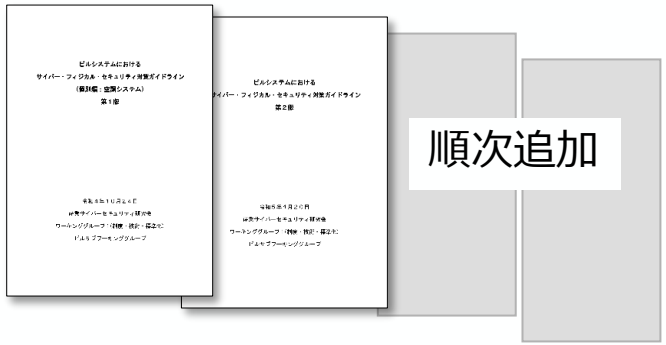
（出典）一般社団法人スマートビルディング共創機構
https://www.sbco.or.jp/

サイバーセキュリティSWGの検討事項 ※予定含む

ガイドラインをベースに具体的に展開するうえで必要な事項を順次議論
(順次ガイドラインのappendixとして追加)

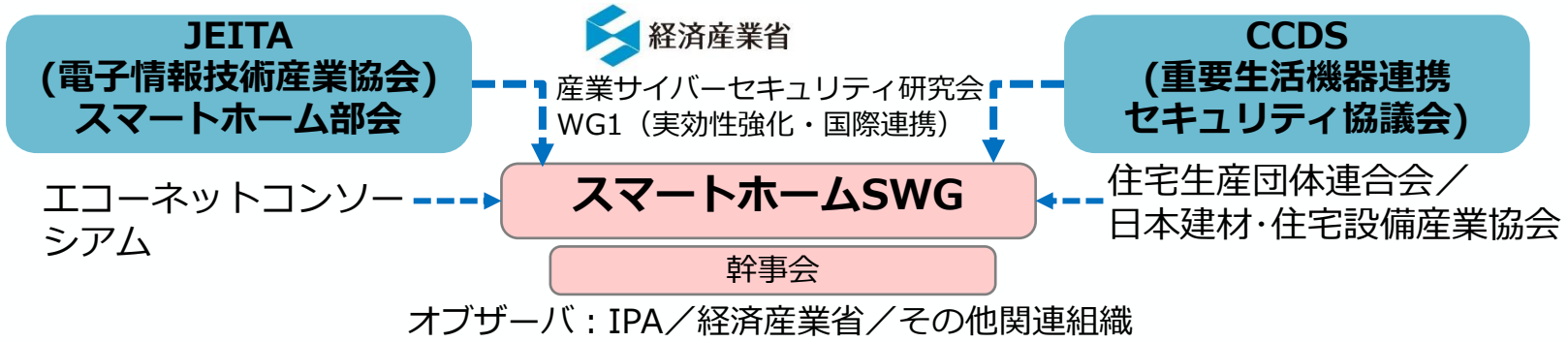
- ✓ サプライチェーン及びラベリング製品を見据え、発注仕様書への記載項目について整理
  （オーナー、設計事務所・ゼネコン、ベンダーの視点）
- ✓ 統合監視へのSOCの役割に関する議論
- ✓ ラベリング制度内容の検討

ビルSWGが作成したガイドライン

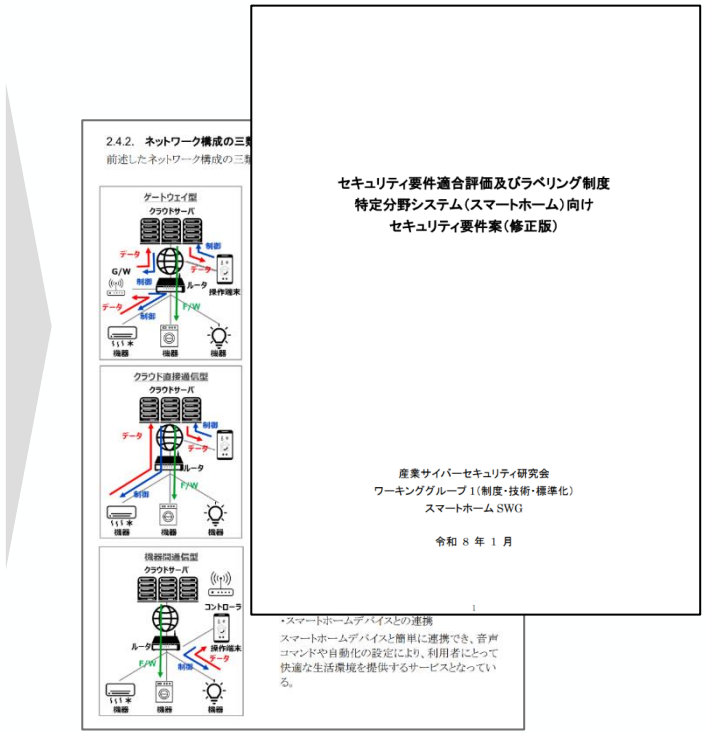


スマートホームSWG （一般社団法人 電子情報技術産業協会）

- 2025年度は、前年度策定したセキュリティ要件案について、**スマートホーム提供事業者が満たすべき要件の追加等、修正**を進めるとともに、CEATECへの出展や店頭イベント等**JC-STARの各種普及促進策について検討を実施**。2025年10月に開催されたCEATECへ出展、2026年1月に要件案の修正完了、店頭イベントについては2026年2月に開催。
- CCDS等の関係団体の参加・協力を得て、2025年7月～2026年1月に合計4回のSWGを開催。



主査：JEITA/CCDSから選出、共同主査形式
委員：JEITA/CCDSの両会員企業から、IoT製品メーカ、ユーザを中心に委員を招聘
主な活動内容：
- **JC-STARセキュリティ要件案（スマートホーム向け）の修正検討**
  - ーBtoBtoCモデルにおけるスマートホーム提供事業者に対する追加要件の検討
- **普及促進検討**
  - ー家電流通協会と連携したJC-STARラベル付き製品販売促進策の検討
  - ーCEATECへの出典、店頭イベント等各種普及促進策の検討

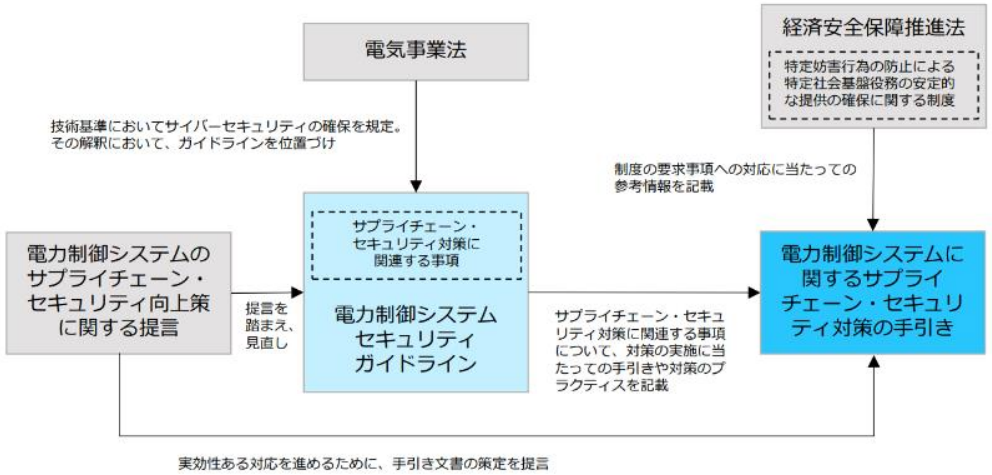


（出典）2025年度第1回~第4回スマートホームSWG資料に基づき経済産業省作成

電力SWG（座長：名古屋工業大学 渡辺教授）

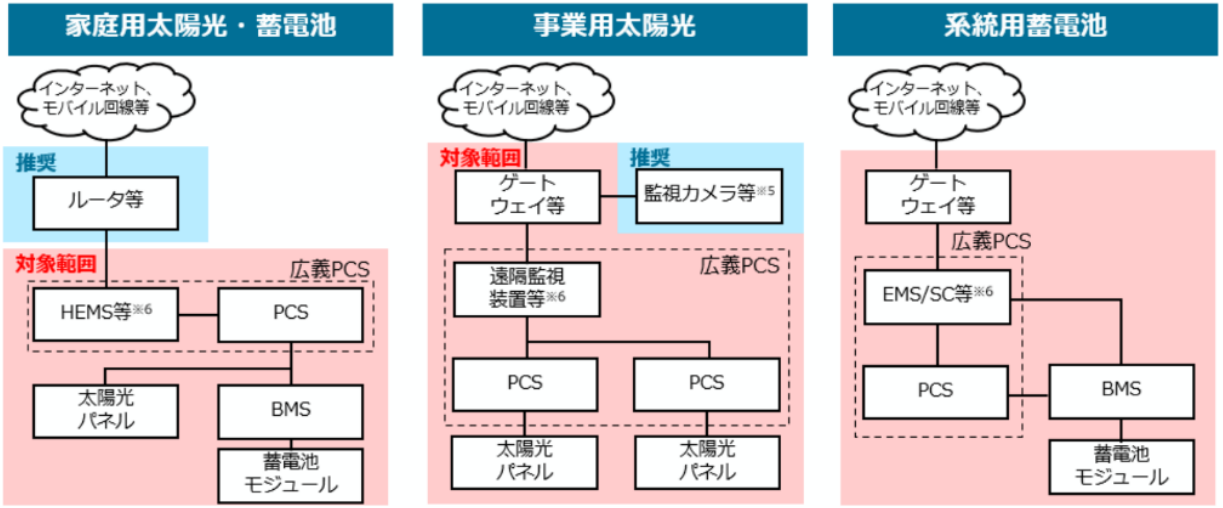
- **電気事業者に求められるサプライチェーン・セキュリティ対策の取組を支援**するため、**「電力制御システムのサプライチェーン・セキュリティ対策の手引き」**（2025年6月公開）や「リスク点検ツール」（2024年3月公開）の活用を促している。
- **分散型電源のサイバーセキュリティ対策におけるJC-STAR制度の活用**について議論。**太陽光発電・蓄電池におけるJC-STAR★1を取得した機器の使用の要件化**が決定。

サプライチェーン・リスクへの対応とリスク点検ツールの活用



- ✓ 事業者のサプライチェーン・セキュリティ対策にあたって参考となる情報をまとめた**「電力制御システムのサプライチェーン・セキュリティ対策の手引き」**を公開。
- ✓ **点検ツール（「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ガイド」及び「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」）**も併せて活用しながら、各電気事業者を中心に対策が進められている。

分散型電源におけるサイバーセキュリティ対策



- ✓ **2027年4月以降に新規に系統に接続される太陽光発電及び蓄電池**については、**系統連系技術要件においてJC-STAR★1を取得した通信機能を有する制御システムの利用を要件化**することが決定。
- ✓ **風力や燃料電池等の要件化の適用範囲・適用開始時期**や、**電力分野固有の脅威や特性を考慮したJC-STAR★2以上の基準の整備や導入**についても官民で調整していく。

（出典）第19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
電力サブワーキンググループ　資料５より抜粋

自動車産業SWG（一般社団法人 日本自動車工業会）

- 日本の自動車業界として対象のセキュリティフレームワーク・ガイドライン・実現レベルを定め、活用を推進することで、適切なセキュリティ対策の実施を図る。
- **2025年度は「自工会／部工会サイバーセキュリティガイドライン 2.3版」をサプライチェーンへ展開し自己評価の依頼**等を実施。その際、サプライヤーの経営層（予算やリソースの割り当てが決定できる方）を対象とした説明会を行い、セキュリティの重要性を訴求。

＜開催状況＞

- 2019年4月16日 第1回 電子情報委員会／サイバーセキュリティ部会を開催。
- 2020年12月4日 第1回 総合政策委員会／ICT部会／サイバーセキュリティ分科会を開催。
  （自工会の組織体制変更に伴い名称変更）
- 2021年度以降　**月1回の会合を継続して開催**し、自動車業界のサイバーセキュリティ対応を推進。

＜2025年度進捗＞

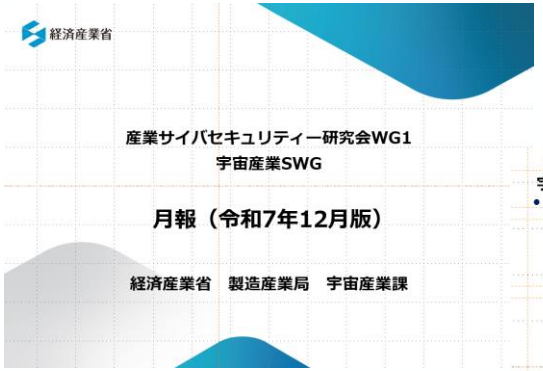
- 付録のチェックシート側の小改訂に伴い**「自工会／部工会サイバーセキュリティガイドライン2.3版」を公開。**
- 2025年度の自己評価の依頼のため、自工会・部工会合同でサプライヤーの経営層＋担当者向け説明会を開催。被害事例、経営への影響等も説明し、4回合計で3,300社、延べ5,600人が参加。
- 自己評価は過去最多となる4,032社が提出。集計結果は例年通り３月末に公表予定。
- 上記ガイドラインの要求事項や自己評価を行う上での問い合わせに対応すべく自工会HPにて生成AIを活用したチャットボットを試験的に導入。9月～12月の運用期間で利用者数1,100人、総チャット数3,700件となり、サプライヤーのサポートを推進した。

（出典）一般社団法人日本自動車工業会「自動車産業サイバーセキュリティガイドライン」を基に経済産業省作成
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

宇宙産業SWG（座長：JIPDEC 坂下 哲也 常務理事）

- **SWG体制の再編・官民の情報共有強化**：従来の作業部会（実務者会合）を宇宙産業SWGに統合。あわせて**より実務的な議論ができるよう構成員を宇宙関連事業者中心に再編。国内外の最新政策動向・脅威動向について官民の情報共有を促進**。動向調査の結果については、情報鮮度確保のため、関係者含むメーリングリストで月報として月次で共有。
- **国際連携を見据えた相互運用性の向上**：米国等との連携進展に向けて、海外で求められる対策との相互運用性・情報連携を強化するため、**2024年3月公開の民間宇宙システムにおける対策ガイドライン Ver2.0を英訳**。

SWG委員、関係省庁との情報連携の促進



- SWG会合を通じた民間宇宙事業者の経営層・実務者、関係団体、政府関係機関による官民情報共有を促進
- 国内外の宇宙分野におけるサイバーセキュリティに関する最新動向（例：政策動向、脅威情報）について情報共有

ガイドラインに関する取組

産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化）宇宙産業サブワーキンググループ 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0

経済産業省では、産業サイバーセキュリティ研究会ワーキンググループ1（制度・技術・標準化）宇宙産業SWGの下で、「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0」を策定しましたので、公表します。

本ガイドラインは、民間宇宙事業者のビジネス振興及びサイバー攻撃による倒産等の経営リスク軽減の観点から、
- 宇宙システムに係るセキュリティ上のリスク
- 宇宙システムに関わる各ステークホルダーが検討すべき基本的セキュリティ対策
- 対策の検討に当たり参考になる参考文献、活用可能な既存施策 等

について分かりやすく整理して示し、民間事業者における自主的な対策を促すことを目的としています。

- 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver2.0（PDF形式：3,805KB）
- 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0 概要資料（PDF形式：1,231KB）
- 【添付資料1】対策要求事項チェックリスト（Excel形式：16KB）
- 【添付資料2】NIST CSFと宇宙システム特有の対策との対応関係（Excel形式：27KB）
- 【添付資料3】情報セキュリティ関連規程（サンプル）（Word形式：183KB）

- 諸外国との連携を目的とし、2024年3月公開のVer2.0を英訳

半導体産業SWG（座長：東京大学 江崎教授）

- 国際的な半導体産業における各種セキュリティ規格とも整合した、半導体デバイス工場向けの工場セキュリティ対策の指針である**「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」**を作成（2025年10月24日公表）。
- 投資促進関係施策の要件等とも紐づけることを念頭にした**「半導体デバイスメーカーに対するセキュリティ要求事項」**を策定。**「半導体装置メーカーに対するセキュリティ要求事項」**についても検討中。

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

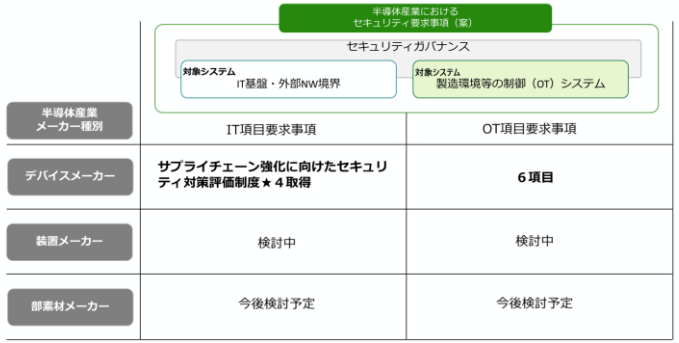
目次

セキュリティ要求事項

半導体デバイスメーカーに対するセキュリティ要求事項

- IT項目（43項目）
  - 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★4
- OT項目（6項目）
  - ガバナンスの整備：１項目
  - リスクの特定：２項目
  - 攻撃等の防御：２項目
  - インシデントへの対応：１項目

半導体産業におけるセキュリティ要求事項の対象範囲（案）



半導体産業 メーカー種別	IT項目要求事項	OT項目要求事項
デバイスメーカー	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★４取得	６項目
装置メーカー	検討中	検討中
部素材メーカー	今後検討予定	今後検討予定

(出典)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
https://www.meti.go.jp/policy/netsecurity/wg1/semiconductor_systems_guideline.html

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（SCS評価制度※1）の概要

[※1] SCS（supply chain security）評価制度

- 「対策状況は**外部から判断が難しい**」「**複数の取引先から様々な対策を要求**される」等の課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策を提示しつつ、その状況を可視化する仕組みを構築。※2
- **２社間の取引契約等において、発注企業が、受注側に適切な段階の”★”を提示**し、示された対策を促すとともに実施状況を確認することを想定。 本制度の活用促進を通じ、サプライチェーン全体でのセキュリティ対策水準の向上を図る。※3
- ３段階の水準のうち、★３・★４について、**令和８年**(2026年)**度末頃の制度開始**を予定。

[※2] 企業等のIT基盤が対象。また、評価は取得又は更新の時点において定められた水準を満たしているかを示すものであり、完全なセキュリティの確保等を保証するものではない。
[※3] 発注時等に、必要なセキュリティ対応状況の可視化を目的としたもので、いわゆる「格付け」制度ではない。

構築する評価制度

	★３	★４	★５ [検討中※5]
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全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： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等がさらに目指すべき高度な対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
要求事項 / 有効期間	26件 / １年	43件 / ３年（毎年自己評価を実施し結果を評価機関へ提出）	（今後検討）
評価スキーム	**専門家確認付き自己評価** ※4	**第三者評価**	第三者評価

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

[※4] 専門家： 登録セキスペ、CISSP等の資格を有し、かつ制度が定める研修を受講したセキュリティ専門家 [※5] ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

普及施策の例

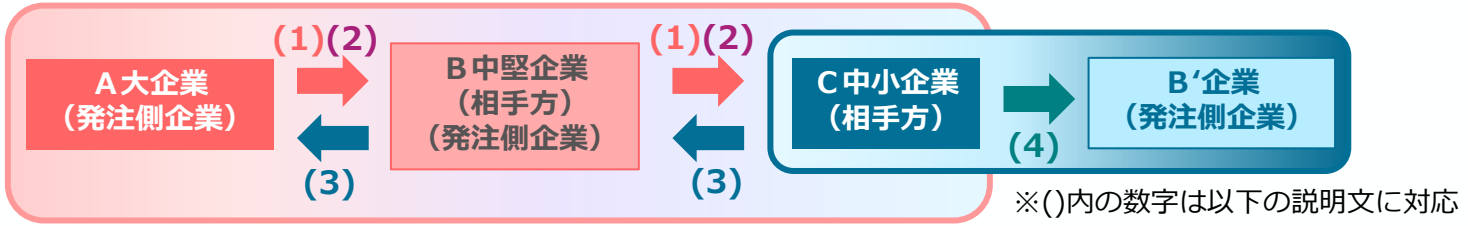
想定される課題	中小企業等における★取得の負担	中小企業等におけるセキュリティ専門家の確保	サプライヤー企業への★取得要請時の関係法令の適用
施策の概要	**サイバーセキュリティお助け隊サービス（新類型）の創設** ★３・★４取得を目的とした、サイバーセキュリティお助け隊サービス（新類型）を創設し、安価な”★”取得を実現	**中小企業ガイドライン整備** 中小企業の情報セキュリティ対策ガイドライン及び付録サンプル規程の整備により、”★”の取得を容易化	**専門家の活用促進** 「中小企業向けサイバーセキュリティ対策支援者リスト」の整備により、中小企業と専門家とのマッチングを促進	**取引先への要請等に係る考え方の整理** 取引先とのパートナーシップ構築促進に向けた想定事例及び解説案により、費用に係る円満な価格交渉を促進

サイバーセキュリティ対策要請時の関係法令適用関係明確化

- 経済産業省及び公正取引委員会では、「サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて」を補足するため、発注者・相手方双方を対象とした、独占禁止法・取適法上「問題とならない」想定事例及びその解説文書を作成。
- 想定事例は、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基づく対策要請を円滑に行い、発注者側・相手方がパートナーシップを構築してセキュリティ対策と価格交渉を実施し、円満に合意するものとしている。

【想定事例】

【サプライチェーンのイメージと想定事例の各場面】



※()内の数字は以下の説明文に対応

(1) セキュリティ対策実施の要請

A（大企業）は、相手方であるB（中堅企業）に対し、①組織ガバナンス・取引先管理、システム防御・検知、事案対応等の対策の実施(＊)、②Bの相手方であるC（中小企業）に対し①と同様の対策を講ずることを要請

(＊)**「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（SCS評価制度）」中の「★４」に相当**

(2) 要請に当たってのパートナーシップの構築

Aは、自社の対応方針を定め、B・Cに対する説明会を定期的に開催（講ずべきセキュリティ対策の内容や国の支援策等を説明）。また、AからB、BからCに対し、費用負担の考え方、セキュリティ対策が価格交渉の対象になる旨、価格交渉に積極的に対応する旨を周知。

(3) 要請への対応と価格交渉の実施

B・Cは、それぞれ発注者側から受けた説明により対策の必要性を理解し、国の支援策を活用することで要請された対策を安価に実現。対策に要したコストに関し、発注者側による説明に基づき価格交渉を実施し、円満に合意。結果を双方が書面に記録して保存。

(4) 要請を行っていない発注者側企業への対応

Cは、要請を受けていないB'（中堅企業）とも価格交渉を行うため、取引かけこみ寺などの支援機関へ相談。得られた助言に基づき、Bとの交渉で用いた費用負担の考え方等を整理した上でB'に対し価格交渉を申し入れ、対策の必要性や同社との取引割合などを勘案した費用負担の考え方等を説明。交渉は円満に合意に達し、結果を双方が書面に記録して保存。

【想定事例解説】

想定事例を補足するため、以下の点について解説を作成。

① SCS評価制度に基づいたセキュリティ対策要請が合理的範囲を超えた負担を課すものではないこと。
② 発注者・相手方双方でパートナーシップを構築することの必要性や重要性。
③ セキュリティの経費が物件費や人件費などの間接経費として計上されること。
④ 価格交渉の考え方や、要請をしていない発注者側企業に対する価格交渉に当たって支援機関を活用すること。
⑤ 取引かけこみ寺や公正取引委員会の事前相談制度・一般相談・事例集の紹介。

【今後の取組】

本文書について、経済団体や中小企業支援機関等に協力いただきつつ、大企業・中小企業等の双方に対して、普及展開を進めていく。

サプライチェーン全体での対策強化に向けたSC3の主な活動

- 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）は、**サイバーセキュリティに関する情報の共有と協力体制の強化**を目的として、**2025年7月にIPAとの間で相互協力を締結。**
- **IPAと連携**しながら、産業界におけるサプライチェーン・セキュリティ対策強化に向けた**取組を実施。**

サプライチェーン・セキュリティ・フォーラム

- ✓ サプライチェーンのレジリエンス向上を目指し、**SC3会員及び各ステークホルダーが連携するための場**として、IPAとの共催により開催。
- ✓ SC3会員に対し、**IPAからのインテリジェンスの報告や、SC3が検討している課題や技術動向などの情報共有**などを実施。

SCS評価制度推進SWG・持続可能なSC対策検討SWG

- ✓ **サプライチェーン企業のセキュリティレベルを実質的かつ持続的に向上させる**ため、**IPAと連携して以下の論点を検討。**
  - SCS評価制度の基本構想や、SCS評価制度基準案の詳細検討を実施。
  - SCS評価制度の具体的運用や普及策について検討を実施。
  - 産業界の立場から、SCS評価制度の実装可能性・コスト妥当性・持続性・定量性の観点で意見を集約。また、SCS評価制度に対する意見発信等を実施。

工場セキュリティセミナー

- ✓ 半導体産業のある九州地域において**「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」の普及に向けた講演**を実施。
- ✓ 工場のスマート化が製造業発展のカギであることを踏まえ、**製造業全体の対処能力底上げと普及促進を目的**として実施。

登録セキスペ向け指導要領

- ✓ 中小企業に対してSCS評価制度の支援ができる**登録セキスペ育成のための指導要領作成の支援**を実施。
- ✓ 本指導要領は、中小企業がSCS評価制度の★を取得する際、セキュリティ専門家として登録セキスペがその適合可否を確認・助言することを念頭とした内容。

中小企業支援施策の全体像

- 中小企業等が抱える主な課題：①「サイバーセキュリティ対策の**必要性を感じない**」、②「**何をすれば良いか分からない**」「**十分にコストをかけられない**」
- 経済産業省では、地域の支援機関等とも連携し、 ①については**サイバー攻撃が他人事でない旨を周知**し、②については**中小企業等それぞれの課題・ステップに沿った施策を推進**している（以下は主要施策）。

SECURITY ACTION

中小企業自らが、セキュリティ対策に取り組むことを**自己宣言**する制度。これまでに**約４６万件**の宣言が行われている。

★一つ星

情報セキュリティ６か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

⇒**セキュリティ対策のきっかけづくり**

サイバーセキュリティお助け隊サービス

相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など各種サービス内容を要件としてまとめた基準を満たす**ワンパッケージサービス**。（現在、**47事業者**が提供し、2025年9月末時点で約**9,200件**の利用実績。）

サイバーセキュリティお助け隊

デジタル化・AI導入補助金（旧：IT導入補助金）「セキュリティ対策推進枠」により補助

⇒**必要最低限の対策を実行（監視、駆付け、保険）**

中小企業の情報セキュリティ対策ガイドライン

経営者編と実践編から構成されており、個人事業主や小規模事業者を含む中小企業等による活用を想定し、具体的な**セキュリティ対策を示したガイドライン**。

すぐに使える「情報セキュリティ基本方針」やSCS評価制度の要求事項にも対応した**規程類のサンプル・ひな形**等も収録。

経営者向けの解説

経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説

企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

⇒**自社の状況に即したより実効的な取組の検討・実行**

サイバーセキュリティお助け隊サービス

- サイバーセキュリティお助け隊サービスは、**中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価（例：月額1万円以内）に提供するサービス。**
- **全国47事業者がサービスを提供**しており、 2025年9月末時点で**約9,200件の利用実績**がある。
- デジタル化・AI導入補助金（旧：IT導入補助金）「セキュリティ対策推進枠」を活用することで、**最大150万円まで、導入費用の1/2（小規模事業者は2/3）の補助**を受けられる。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

- ✓ **EDR・UTM等による異常監視**
- ✓ **緊急時の対応支援・駆付けサービス**
- ✓ **簡易サイバー保険**
- ✓ **相談窓口**
- ✓ **簡単な導入・運用**

➡中小企業でも導入・維持できる価格でワンパッケージで提供

サイバーセキュリティお助け隊サービスの利用はこちらから
⇒ https://www.ipa.go.jp/security/otasuketai-pr/

サイバーセキュリティ CSお助け隊

お助け隊マーク

- お助け隊サービスA
- お助け隊サービスB
- お助け隊サービスC

サイバーセキュリティお助け隊サービス審査登録制度：
一定の基準を満たすサービスに**お助け隊マークの商標利用権を付与**

お助け隊サービス利用の推奨等の中小企業の取組支援

デジタル化・AI導入補助金（旧：IT導入補助金）に「セキュリティ推進枠」創設
（補助率：中小企業1/2、小規模事業者2/3
補助上限：150万円）

SECURITY ACTION★１★２自己宣言要件の見直し

- 中小企業の実態や最新の脅威動向を踏まえSECURITY ACTIONの対策項目の見直しを実施。
- **バックアップをSA一つ星の対策項目に追加**したほか、**実施状況が低い項目について具体的対策例の見直し**などを実施。中小企業の情報セキュリティ対策ガイドラインの改訂に合わせて公表。

情報セキュリティ5か条の見直し

情報セキュリティ5か条（一つ星）に二つ星の項目であった**「バックアップを取ろう！」を新たに位置づけ、6か条**として整理。

上記追加の背景：

- ✓ **IPA「10大脅威」においてランサムウェア攻撃が上位に位置づけ**られ、その対策として重要
- ✓ 中小企業が初めに手掛ける対策としてわかりやすい

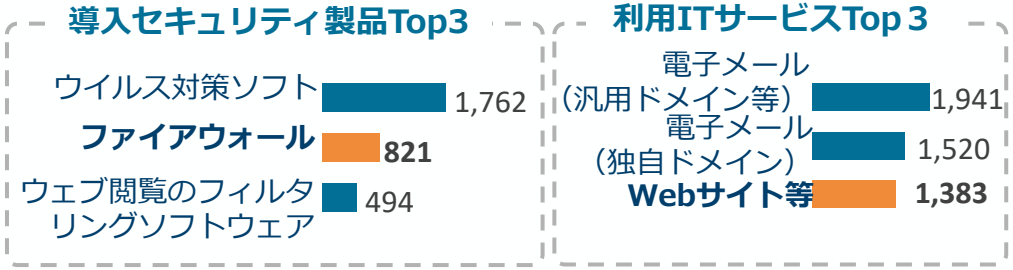
【情報セキュリティ６か条】

- □OSやソフトウェアは常に最新の状態にしよう！
- □ウイルス対策ソフトを導入しよう！
- □パスワードを強化しよう！
- □共有設定を見直そう！
- □脅威や攻撃の手口を知ろう！
- **□バックアップを取ろう！**
  ※SA一つ星の項目として位置づけ

診断25項目の見直し

【追加】

「中小企業実態調査」において、**ファイアウォール及びWebサイトの導入率が比較的高い**ことが確認された。



- ✓ **「ファイアウォール」については、定着を図る観点から項目として整理**
- ✓ 導入実態があるにもかかわらず、これまで対策項目として整理されていなかった**「Webサイト」について、新たに対策項目として位置付け**

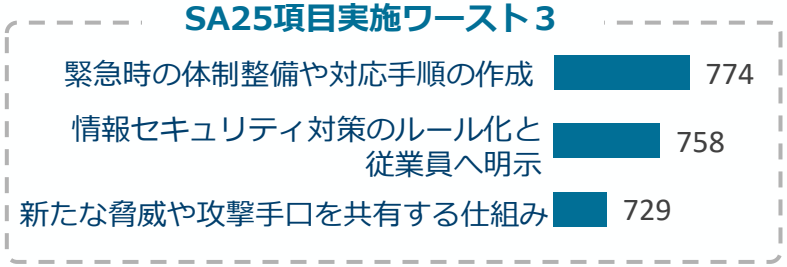
【統合】

中小企業が読んだ際の重複感を避ける観点から、**関連がある項目を、内容の趣旨は維持したまま整理**

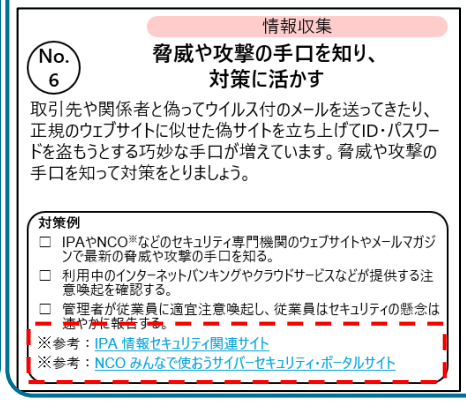
- ✓ 物理的なアクセス管理に関する項目を統合
- ✓ 従業員の情報セキュリティ意識に関する項目を統合

実施率の低い項目の見直し

実施率が低い項目について、**具体的な参照先を追加して対策を実施する際の導線を強化。**



（例）項目：6「脅威や攻撃の手口を知り、対策に活かす」


情報収集
No. 6
脅威や攻撃の手口を知り、対策に活かす
取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。
対策例
□ IPAやNCO※などのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る。
□ 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する。
□ 管理者が従業員に適宜注意喚起し、従業員はセキュリティの懸念は速やかに報告する。
※参考：IPA 情報セキュリティ関連サイト
※参考：NCO みんなで使おうサイバーセキュリティ・ポータルサイト

⇒情報収集先としてIPAやNCOなどが運営しているWebサイトを参考として明記

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」（n=中小企業4,191社、複数選択可）を基に経済産業省作成

地域におけるセキュリティ関連活動（地域WSの開催状況）

- 東海サイバーセキュリティ連絡会では、過去の中小企業に対するヒアリング等から**中小企業にセキュリティポリシー策定に対するニーズがある**こと踏まえ、令和７年11月「情報セキュリティポリシー策定ワークショップ（WS）+登録セキスペによる個別相談会」を開催。
- 参加者からは、**大変有意義なWSであった**と高い評価が得られ、また登録セキスペによる相談会についても**「有意義であり、専門家に直接自社の課題について相談することができてよかった。」**などの高評価をいただいた。

セキュリティポリシー策定に対する中小企業の意見

- 東海サイバーセキュリティ連絡会では過去の企業ヒアリングから、
  - ○ 標準的なひな形を自社向けにカスタマイズしたい
  - ○ 取組中の対策の妥当性を確認したい
  - ○ 自社だけでポリシーを策定することが難しい

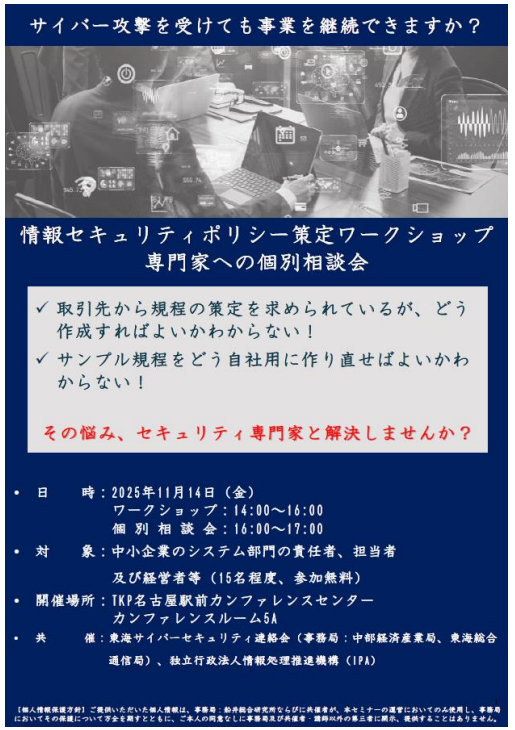
  といった課題を把握し、

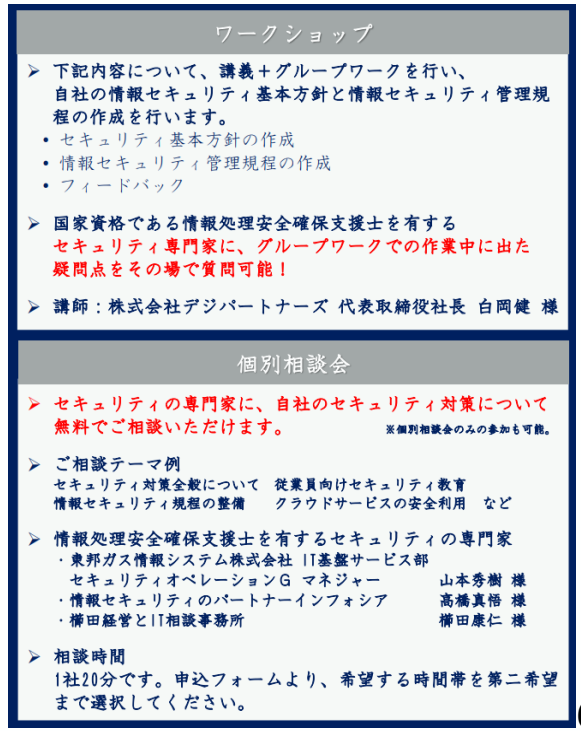
これを踏まえ、令和７年11月、ワークショップ+個別相談会を開催。

情報セキュリティポリシー策定WS+個別相談会参加者の声

- ワークショップ+個別相談会参加者からの主な意見
  - ○ 有意義であった、理解ができた。
  - ○ **専門家（登録セキスペ）の方に、直接自社の課題について相談することができてよかった。**
  - ○ **セキュリティ対策についてシステムベンダしか相談先を知らなかったので、相談先が増えてよかった。**
  - ○ 是非次回もやってほしい。

情報セキュリティポリシー策定WS+個別相談会の概要





出典：サイバー攻撃等初動対策手順書策定ワークショップ（主催：東海サイバーセキュリティ連絡会）

中小企業のための実例で学ぶサイバーセキュリティリスク事例集

- 中小企業の多くが「セキュリティ対策の必要性を十分に理解していない」実態。
- そこで、中小企業一般にありがちなサイバーセキュリティ・リスクや、攻撃された場合に想定される被害額とそれを防ぐための主な対策を（約30事例）示し、中小企業にセキュリティ対策の必要性を理解いただくための「事例集」をIPAにて2026年3月末に公表。今後、地域SECUNITY等での講演資料や社内での教材としての活用を想定。

事例集の読者層・使い方

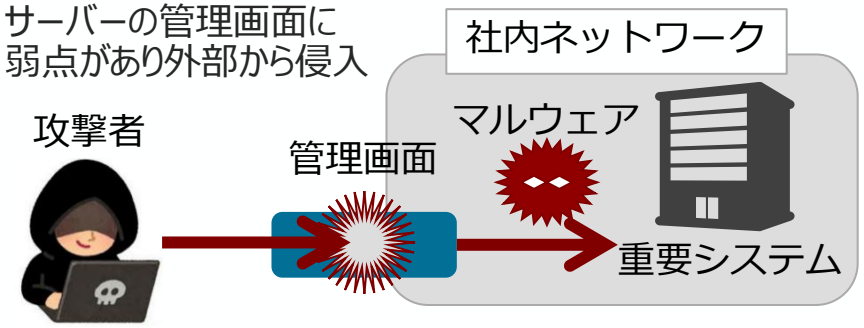
中小企業の経営者・情報システム担当者、中小企業の支援に携わる関係機関の皆様を対象とし、次のような活用を想定

- ✓ **中小企業でも被害がある**ことを示す資料や、専任の情報システム担当がいない企業の**工夫事例紹介**として
- ✓ **自社に合った対策を見つけるきっかけ**や、**社長への相談・予算交渉の材料**として
- ✓ 社内研修や勉強会、地域SECUNITY等での**講演資料や教材**として

事例集事例

①中小企業で**実際に見つかった弱点**を紹介
②中小企業のサイバー被害事例と**被害額**を紹介
③自社にあった**レベルの対策**が見つかる

1 サーバーの管理画面に弱点があり外部から侵入



2 **想定被害額** **3,900万円**

初期対応費用、復旧費用、報告公表費用、弁護士訴訟費用、再発防止費用等

業務停止し**完全復旧まで2か月**要した

3

すぐにできる対策

- ✓機器のIDとパスワードが**初期設定のまま**になっていないかチェック

より強固にする対策

- ✓トラブルが起きた時にどう対応するかの**手順書を整備**する

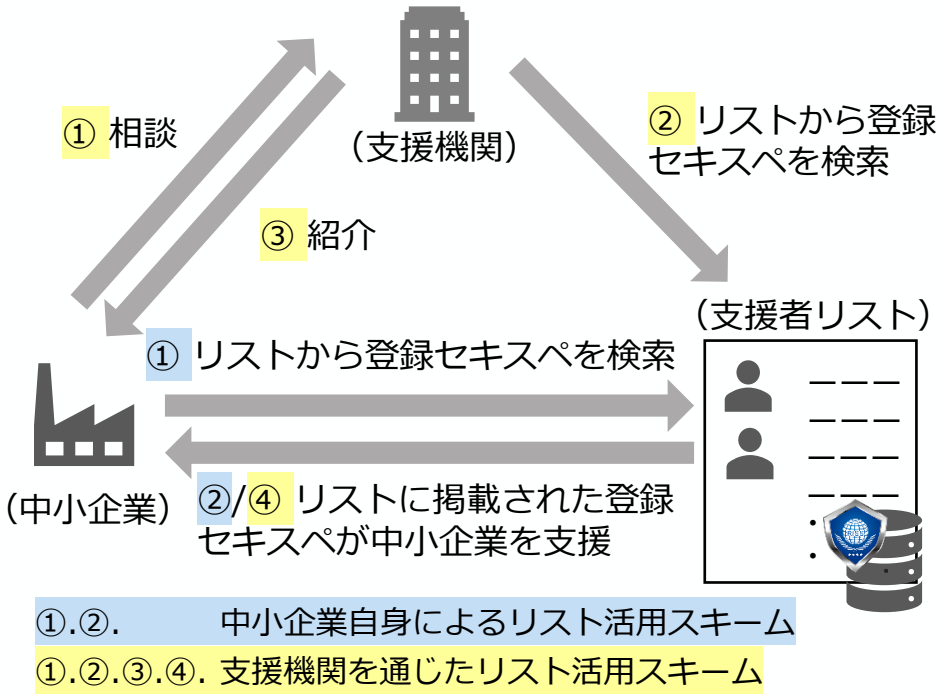
令和6年度の実態調査で中小企業のセキュリティ意識の不足を確認し、令和7年度に複数業界・規模の中小企業126社を対象にASM診断※を実施。アンケートとヒアリングで被害事例や好取組事例を収集し、リスクと対策を整理した「事例集」を作成

※ASM診断は、インターネットから見える自社のIT資産（サーバ、ネットワーク機器、IoT機器など）を把握し、攻撃されやすいポイントを特定する仕組み

中小企業向けサイバーセキュリティ対策支援者リスト

- 社内のセキュリティ人材育成に課題を抱える中小企業にとって、セキュリティ対策における**外部のセキュリティ専門家の活用**が効果的であることを踏まえ、**情報処理安全確保支援士（登録セキスペ）を効率的に探索するためのツール（支援者リスト）を整備。**
- **SCS評価制度の★３取得のために同リストを活用**できるよう、**”★”取得の適合可否を確認可能な登録セキスペの増加**を促進。

（今後の支援者リスト活用スキーム）



①.②.　中小企業自身によるリスト活用スキーム
①.②.③.④. 支援機関を通じたリスト活用スキーム

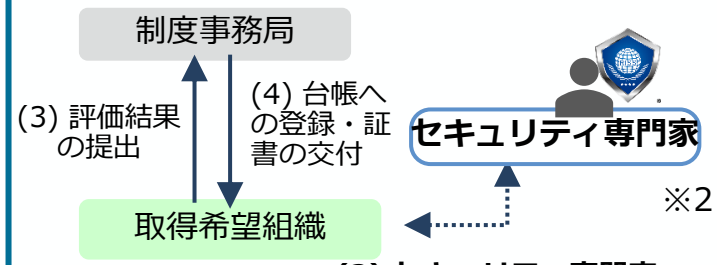
支援者リストの整備（利便性向上・掲載者の増加）

- ✓ **利便性を向上し「中小企業向けサイバーセキュリティ対策支援者リスト」**としてIPAのHP上に公開。
- ✓ 全登録セキスペに向けた**セミナー**（※1）**を開催**し、**リスト掲載者は340人に増加。**
  一方、支援ハードルの高さ等、掲載者数の更なる増加に向けた課題も明らかになった。

※1：中小企業支援の方法解説、実際に支援を行った登録セキスペによる体験談の共有を実施。

SCS評価制度★３取得の適合可否を確認できる登録セキスペの拡充

（SCS評価制度★３の評価スキーム）



- ✓ 中小企業が**SCS評価制度の★3を取得する際、**セキュリティ専門家として**登録セキスペが適合可否の確認**及び助言ができるよう、指導テーマ（※2）に「セキュリティアセスメント」を追加し、指導の実践に向けた施策（※3）を実施。

※2：支援者リストに掲載された登録セキスペは、指導テーマ（情報セキュリティ規程の整備等）から中小企業が指定するものに基づき支援を実施。

※3：指導要領の作成や、スキル習得のためのケース演習を実施。

今後の方向性について

商工会議所等の支援機関や中小企業による支援者リストの活用に向け、**活用事例の蓄積**を図るとともに、リスト掲載者数の更なる増加に向けた取組を検討。

国内における政策普及に向けた取組

- 2025年12月に公表した「SCS評価制度構築方針（案）」や「サイバーセキュリティお助け隊サービス（新類型）」創設に向けた実証事業に関して、全国各地域での周知活動を実施。
- セキュアなIoT製品を認証する「JC-STAR」の活用を促進する観点から、消費者向けの周知啓発資料の作成や展示会への出展、消費者向け普及イベントの出演等を通じた周知活動を実施。

中小企業等向けの支援策等の周知・広報

＜実証事業に関するチラシ・HP上の特設サイト＞

経産省　セキュ活　検索

https://www.meti.go.jp/policy/netsecurity/otasuketai_jissho.html

- 全国の経済産業局と連携し、総合通信局、都道府県警察をはじめ、中小企業支援団体（商工会議所、情報産業協会、経済連合会等）、ITベンダー、業界団体等へ広く展開。

JC-STARについての消費者向けの周知・広報

- 2025年3月に運用開始したJC-STARについて、製品利用者側の認知度向上を図るため、消費者向けポスターを作成。
- 家電量販店等にて配布し、JC-STARラベルが貼付された製品の活用を後押し。
- このほか、CEATECにおけるIPAとの共同ブース出展、警察庁広報資料への掲載、テレビ番組での紹介、JEITA主催の消費者向け普及イベントへの出演等、多様な普及展開活動を実施。

※写真は普及イベントの様子

インド太平洋地域向け産業制御システム・サイバーセキュリティ演習

- 経済産業省とIPA産業サイバーセキュリティセンター（ICSCoE）が、**米国・EU政府等と連携し、毎年開催するインド太平洋地域向けの1週間の研修プログラム**。これまで2018年度より8回開催。
- 本演習は、**インド太平洋地域の重要インフラ事業者、製造業者等の産業用制御システム（ICS）セキュリティの向上を目的に、ICSのサイバーセキュリティに焦点**を当て、**ハンズオン演習**や、**日米欧専門家による講演**、**参加者間のネットワーキング**等を実施。
- 2025年は**インド太平洋地域から65名が来日して参加**（加えて一部ライブ配信）。これまで以上に**サプライチェーンレジリエンスの強化、日米欧のプレセンスを維持・PR**。

2025年度 演習の概要

- **日時**：2025年11月18日～21日
- **場所**：EU代表部、IPA秋葉原キャンパス等
- **主催**：経済産業省、IPA産業サイバーセキュリティセンター、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省）及びEU政府（通信ネットワーク・コンテンツ・技術総局、欧州連合サイバーセキュリティ機関、欧州対外行動局）
- **参加者：来日65名＋ライブ配信**　ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の重要インフラ事業者、製造業者、ナショナルCSIRT、政府機関等

ハンズオン演習

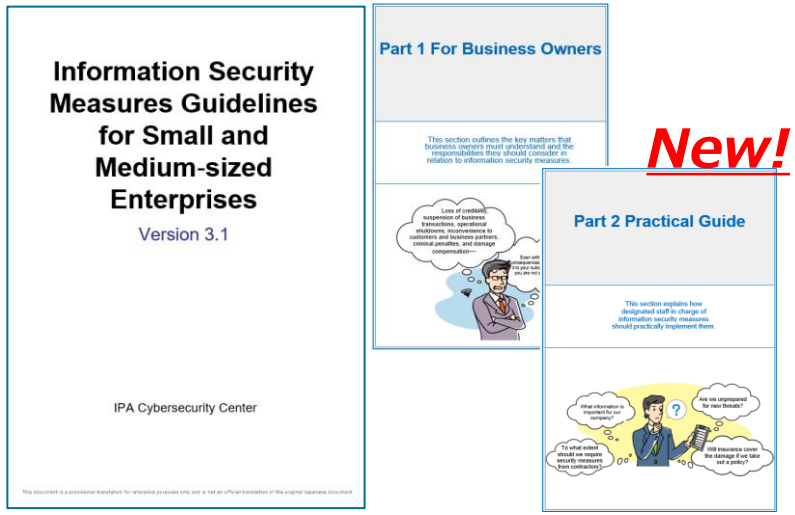
日米欧専門家による講演・ワークショップ

インド太平洋地域参加者間のネットワーキング

※写真は2025年度演習の様子

我が国のサイバーセキュリティ施策の海外発信

- これまで、産業界のサイバーセキュリティ対策水準の底上げに向け、**対象者ごとに具体的な対策を記載したガイドラインを展開**してきたところだが、一部について**英語版が未発行**であり、また、発行されている**英語版についても外国政府や企業における認知度は低い**現状。
- サイバーセキュリティ対策は、サプライチェーン全体での対策が必要であり、 我が国企業とサプライチェーンの多くを共有するASEAN地域でのサイバーセキュリティ能力の向上が重要であることから、**ASEAN地域に向けた施策の情報発信を強化。我が国のセキュリティ企業の現地進出も見据える。**
- 2025年には、IPA及び国家サイバー統括室と連携し、**中小企業の情報セキュリティ対策ガイドライン本編の英語版を発行し**、日・ASEANサイバーセキュリティ政策会議にて当該ガイドラインの**活用事例を我が国企業から発信**。経済産業省の英語版ウェブサイトにおいても情報発信を強化。



新規に英語化した中小企業向けガイドライン

日・ASEANサイバーセキュリティ政策会議の様子

3．セキュア・バイ・デザインの実践

2025年度国際連携の取組・成果全体像

- 我が国のサイバー対処能力の強化や国際競争力強化の観点から、 **①サイバー分野におけるルール作りを主導する欧米等の議論に参画**し、**国内制度との相互運用性を担保**する必要。併せて、我が国企業にとって**②サプライチェーン上重要なインド太平洋地域のサイバー対策の能力構築**を推進することも必要。
- これらの土台として**③幅広い有志国との連携**も深めていく。これら３つの柱を軸に国際連携を実施。

①国内外制度の相互運用性担保

- **IoTセキュリティ（JC-STAR）**：同様に制度を導入又は検討している**EU、米国**や**シンガポール等**を中心に、相互運用性担保に向けてバイ・マルチの枠組みで議論。とりわけG7においては、 **IoTセキュリティの確保のために技術的及び非技術的なサイバー脅威の考慮の必要性**について**共同で提案。英国とは2025年11月にPSTI法との相互承認に関する協力覚書に署名**し、**シンガポールとも2026年３月にCLSとの相互承認に関する協力覚書に署名。**
- **ソフトウェアセキュリティ（SBOM、SSDF）：米国やマルチの枠組み**を中心に、制度調和に向けて議論。
  - 米：6/17-18 日米サイバー対話、SBOM国際会議
  - 欧：7/23 首脳会合、5/12 日EUデジタルパートナーシップ閣僚会合、 1/28 日EUサイバー対話、INSTARサイバーセキュリティ会合
  - 英：1/31 首脳会合、2/27 日英サイバー対話
  - シンガポール：10/20-23シンガポールサイバーセキュリティウイーク
  - マルチ：G７（サイバーセキュリティワーキンググループ、内務・安全担当大臣会合、産業デジタル科学技術大臣会合）、GCLI（Global Cybersecurity Labeling Initiative） 等

②インド太平洋地域向け能力構築

- **米欧政府と共に、**2018年度より**インド太平洋地域向け産業制御システム・サイバーセキュリティ演習を**毎年実施。2025年は11/18-21に東京で対面実施。
  - その他連携：10/8日ASEAN政策会議、日ASEANサイバーセキュリティWG 等

③幅広い有志国との連携

- ①と②の対象国を軸に、**各種バイ協議**を実施。その他、①と②を含む各種アジェンダの推進に向けて**G7、GCLI等のマルチ枠組み**も活用。
  - 豪州（日豪経済閣僚対話）
  - タイ（NCSA長官来訪） 等

IoT製品に係るサイバーセキュリティ評価制度の国際協調

- 2025年11月、経済産業省と英国科学技術・イノベーション省（DSIT）との間で、**我が国のJC-STARと英国のPSTI法に関し、相互承認**する旨の覚書へ署名。2026年1月に、両制度間で相互承認制度が開始。
  - ※ 本制度は、JC-STARを取得した製品（★１）が英国PSTI法が要求する全てのセキュリティ要件（３要件）に適合すると認め、他方でPSTI法のセキュリティ要件に適合する製品は、JC-STARが要求する全１６要件のうち、3つの要件への適合を認めることにより、両制度間の適合証明要件を全てもしくは一部免除するもの。
  - ※ 2026年３月には、**シンガポール**サイバーセキュリティ庁との間でも、**JC-STARと同国のCLSとの相互承認**に係る覚書を署名。
- 2025年では、G7サイバーセキュリティワーキンググループでIoT製品セキュリティ対策での**有志国連携の重要性が確認**されたほか、ISO 27404でのIoTラベリング制度の規格化やGCLI（IoTセキュリティ評価制度に関心を有する政府の会合）の発足等、IoT製品に係るセキュリティ評価制度への国際的な関心が高まった。
- 今後、**類似の制度を有する米国、EU、ドイツ等を中心に制度間の協調を引き続き追求して**いく。

日英 IoTセキュリティ製品評価制度比較

国・地域	日本	英国
制度名	JC-STAR （Japan Cyber STAR）	Product Security & Telecommunication Infrastructure Act (PSTI)
開始時期	• ★1：2025年3月25日開始 • ★2以上：2026年度第1四半期以降順次開始予定	2024年4月施行
任意/義務	任意	義務
対象	IoT製品	消費者向けIoT機器
適合基準	★1：ETSI EN 303 645及びCLSの記載内容を中心に検討（ただし、総務省技適の要件、CCDSの要件も参照のほか、事務局にて記載内容を検討）	ETSI EN 303 645の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）
評価方法	• ★1、★2：自己適合宣言 • ★3以上：第三者認証	自己適合宣言

相互承認の概要（英国の場合）

＜適合要件＞

JC-STAR（星１）	PSTI法（2023年施行令）
• 適合基準S1.1-02：出荷時のデフォルトパスワードパスワード設定の禁止 • 適合基準 S1.1-05：脆弱性開示ポリシーの公開 • 適合基準 S1.1-16：製品情報の提供	• 出荷時の共通パスワード設定の禁止 • 脆弱性情報の報告方法の提供 • 製品のセキュリティサポート期間の明示

＜相互承認の手続＞

JC-STAR→PSTI法	PSTI法→JC-STAR
JC-STAR星１のラベルがPSTI法適合証明書に代替。	JC-STARの求める３つのセキュリティ要件に関する適合確認を免除。

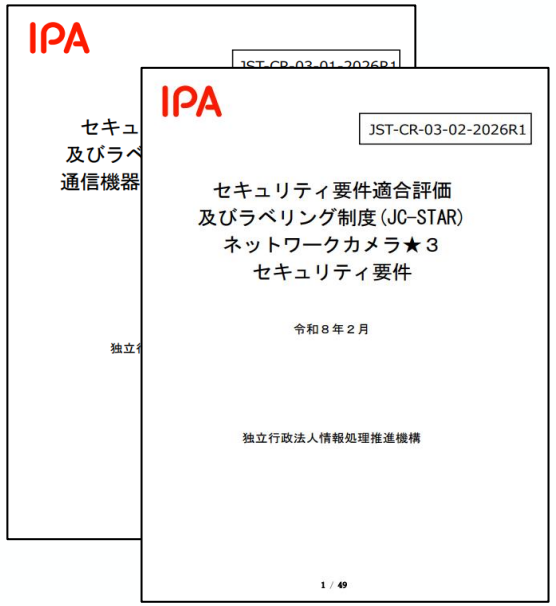
主な諸外国の類似制度

国・地域	米国	EU	ドイツ
制度名	U.S. Cyber Trust Mark	Cyber Resilience Act（CRA）	IT Security Label
マーク	U.S. CYBER TRUST MARK	CE	IT Security Label Federal Office for Information Security (BSI) The manufacturer assures: This product complies with BSI requirements. The BSI informs: Latest product news bsi.bund.de/it-sik/en/xxxxx
開始時期	2025年より基準策定開始（制度開始時期は調整中）	• 報告義務: 2026年9月 • その他: 2027年12月	2021年12月制度（申請受付）開始
任意/義務	任意	義務	任意
対象	消費者用無線IoT製品	デジタル要素を含む製品	消費者向けデジタル製品

JC-STAR制度の運用状況について

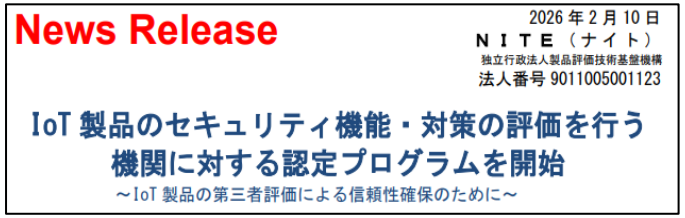
- **IoT製品が一定のセキュリティ基準に適合していることを可視化**する制度。将来的に**４段階での適合性評価**を目指すこととしており、**１段階目（★１）について、2025年３月から申請の受付を開始。**
- 2026年２月に**通信機器とネットワークカメラに関する★３の適合要件を公開。**合わせて、NITEにおいて「JC-STAR制度」に基づく評価を行う**評価機関に対する認定プログラムを立ち上げ。**
- １段階目（★１）について、2025年３月から申請の受付を開始し、2026年3月時点で**約200の申請（製品型番ベースで1,500製品以上）でラベル発行済み。**通信機器やネットワークカメラの製品類型では、国内メーカーを中心に**国内シェアの高い主要メーカーは概ねラベル取得済み。**

★3適合要件策定



通信機器・ネットワークカメラ
★3セキュリティ要件

評価機関制度立ち上げ



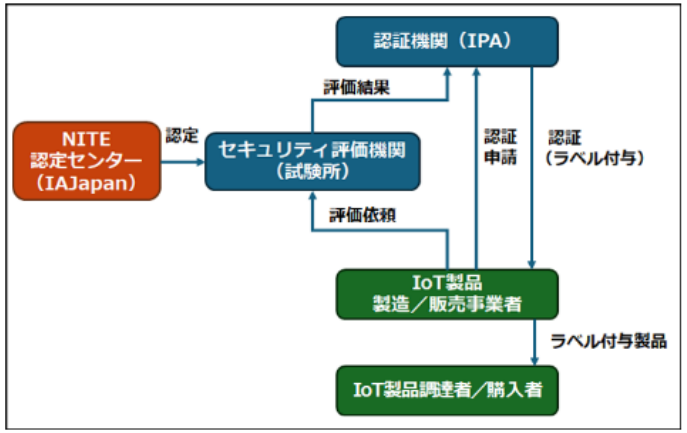


図1：JC-STAR制度のしくみ(セキュリティの第三者評価が必要な場合)

主な★1ラベル取得済み製品

通信機器

ネットワークカメラ

上記以外にも、スマートホーム関連機器（家電・HEMS等）やエネルギー関連機器（蓄電池システム・PCS等）、複合機（OA機器等）をはじめ、**幅広いカテゴリーの製品において★1のラベル取得が浸透**

ソフトウェア・セキュリティ施策の全体像

- 2025年度内に**関連するガイドライン等の策定**に向けた対応を進めつつ、国内事業者が当該ガイドライン等に**準拠した取組を自己評価するための付属文書**を充実させ、それらの活用を促していく。
- 同時に、それら成果物を海外に発信し、**我が国が主導**する形で**国際ルールの整備**につなげていく。

ソフトウェアのセキュリティ確保に関連するガイドライン等の位置付け及び今後の対応

開発

概念、枠組み（What）

具体化、事例化（How）

運用

サイバーインフラ事業者に求められる役割等の整理

- **「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」を策定。**
- ガイドラインの活用促進に向け、評価基準を作成・公表。

SSDF（安全な開発）の促進

- **「SSDF導入ガイダンス案」を拡充。**
- ガイダンスの活用促進に向け、評価基準を作成。

米NIST「Secure Software Development Framework（SSDF）Version 1.1（2022年２月）」

SBOMの国際ルール整備

- SBOMの重要性を発信し、運用上の国際ルールを整備するため、**国際文書（ガイダンス）の策定を実現**（米国CISAと作成を主導）。

米CISA「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software（2023年10月）」

米CISA「A Shared Vision of Software Bill of Materials（SBOM） for Cybersecurity（2025年９月）」

国際的な取組を含むSBOMの活用促進

- SBOM（ソフトウェア部品表）の重要性を発信し、各国における取組の融和を狙った運用上の国際ルールを整備するため、関係国とも連携し、2025年９月に**国際文書（ガイダンス）の策定を実現**。
- また、国内でのSBOMの活用の更なる促進のため、特に中小企業のSBOM導入支援に取り組む。

SBOMの国際ルール整備

- SBOMの活用の重要性を示す国際的な文書（ガイダンス）について、2024年より、米国CISAと共に作成を主導。2025年9月、内閣官房国家サイバー統括室（NCO）を含む計15か国のサイバーセキュリティ当局等と共同署名。より技術的な内容を具体化したガイダンスの策定に向けて、引き続き国際議論を進めていく。

<同文書の内容>
（1）SBOMとは何か
（2）SBOM導入のメリット
（3）SBOMにおけるステークホルダーとその影響
（4）セキュア・バイ・デザインにおけるSBOMの重要性

国内におけるSBOMの普及施策

- 特にリソースの限られる中小企業にとってのSBOM導入面の課題解決に向けた取組として、SBOMの導入を効率的かつ効果的に実現するための実証事業を行い、その成果物として、ノウハウを集約した実践ガイドを2026年度に作成予定。
- また、SBOM運用面の課題解決に向けた取組として、脆弱性マッチング精度を高める技術等、SBOMの効率的な実運用に資する技術開発・製品化をテーマとしたNEDO懸賞金活用型プログラムを2026年度～2027年度にかけて実施予定。

NEDO Challenge

サイバーセキュリティのためのソフトウェア部品表（SBOM）の共有ビジョンに関する国際ガイダンスに共同署名しました（2025年9月4日） https://www.meti.go.jp/press/2025/09/20250904001/20250904001.html

安全なソフトウェア開発に向けた指針（案）の策定

- ソフトウェアの開発運用におけるサプライチェーンセキュリティ確保のための対策事項を体系化したフレームワーク（NIST SP800-218、**SSDF**）を**組織に導入するための考え方や流れ等の導入プロセスを、ガイダンスにまとめたもの**。
- サプライチェーンにおけるソフトウェアを含む**製品・部品の調達者と供給者が必要な対策事項を選別し、合意するための手段と共通言語**として利用することができる。
- 2024年度に中間整理版を公開、2025年度は**分野別の実証とツール活用による自動化をふまえた拡充**を行い、リスクベースでの対応も可能なチェックリストを整備した。2026年度にSP800-218の改訂を踏まえ、指針を策定予定。

SSDF導入プロセス

フェーズ1 要求分析

- 提供する製品・サービス群の用途・利用環境を想定し、事業領域におけるソフトウェアに対する要求と基本方針を明確化する。

フェーズ2 現状把握

- 現在導入済のガイドライン等を特定し、SSDF×国内ガイドラインマッピング表をもとにSSDFタスク項目への対応状況を把握する。

フェーズ3 タスク達成Lvの定義とGAP分析

- タスクの達成レベルとプラクティス案を参考に、対象製品・サービスについて目指すタスクレベルを設定、現状との比較からタスク実施能力のギャップを分析する。
- アカウンタビリティアプローチを提示する。

フェーズ4 タスクの実践

- 設定したタスク達成レベルに対し不足するタスクについて、プラクティス案や、関連の国内ガイドライン、付録の参考資料等を参考に管理策を実践する。

フェーズ5 達成度評価

- タスク達成レベルとプラクティス案に基づき、タスクの実践結果を比較し、達成レベルを評価判定する。目標と乖離がある場合、妥当性を評価する。

フェーズ6 自己適合宣言

- 必要に応じ、フェーズ５までの実施内容に基づき、CISA等の自己適合宣誓フォームに基づき宣誓書を作成する。

ガイダンス案の目次

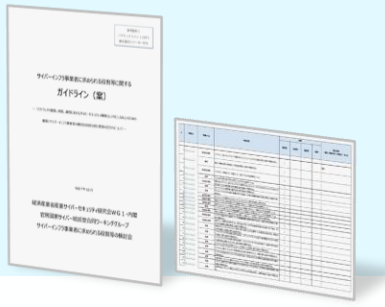
サイバーインフラ事業者に求められる役割等に関するガイドライン

- ソフトウェアサプライチェーンのレジリエンス向上を図るため、ソフトウェアの開発・供給・運用に関わる**サイバーインフラ事業者と顧客に求められる責務**、及び**責務を果たすための要求事項**（役割別の具体的な取組の在り方）をまとめた**「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）」を2024年度に公表。**
- 2025年度は、パブリックコメント、実証、およびサイバーインフラ事業者へのヒアリングを通じて、**ガイドライン**（確定版）**を策定**するとともに、ガイドラインの活用促進に向けた付属文書として**責務向上のための評価基準を作成**し、**2026年３月31日に公表**した。

指針の概要

6つの責務（事業者と顧客の基本理念）	６つの要求事項（共通して取組むべき対策）	対象組織
セキュリティ品質を確保したソフトウェアの開発・供給・運用	セキュアな開発・供給・運用	サイバーインフラ事業者（SW開発ベンダ/販売会社/運用ベンダ　等）＋関係機関（行政機関/関連業界団体）
ソフトウェアサプライチェーンの管理	ライフサイクル管理、透明性の確保	
残存脆弱性への速やかな対処	残存する脆弱性の速やかな対処	
ソフトウェアに関するガバナンスの整備	人材・プロセス・技術の整備	
サイバーインフラ事業者・ステークホルダー間の情報連携・協力関係の強化	サイバーインフラ事業者・ステークホルダー間の関係強化	
顧客経営者のリーダーシップによるリスク管理とソフトウェア調達・運用	顧客経営層によるリスク管理とセキュアなソフトウェアの調達・運用	顧客

目次



「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」を実行するための中小企業向け支援

- 「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」で求められる取組には、**PSIRTの設置**（S(3)-1.1 脆弱性対応体制の設置）や**SBOMの導入**（S(2)-1.3 ソフトウェアコンポーネントのリスク評価）など、特にリソースの限られる**中小企業にとって実施のハードルが一定程度高い**ものも存在。
- 取組支援策として、令和７年度補正予算事業等により**実証及びガイド作成**等を実施予定。

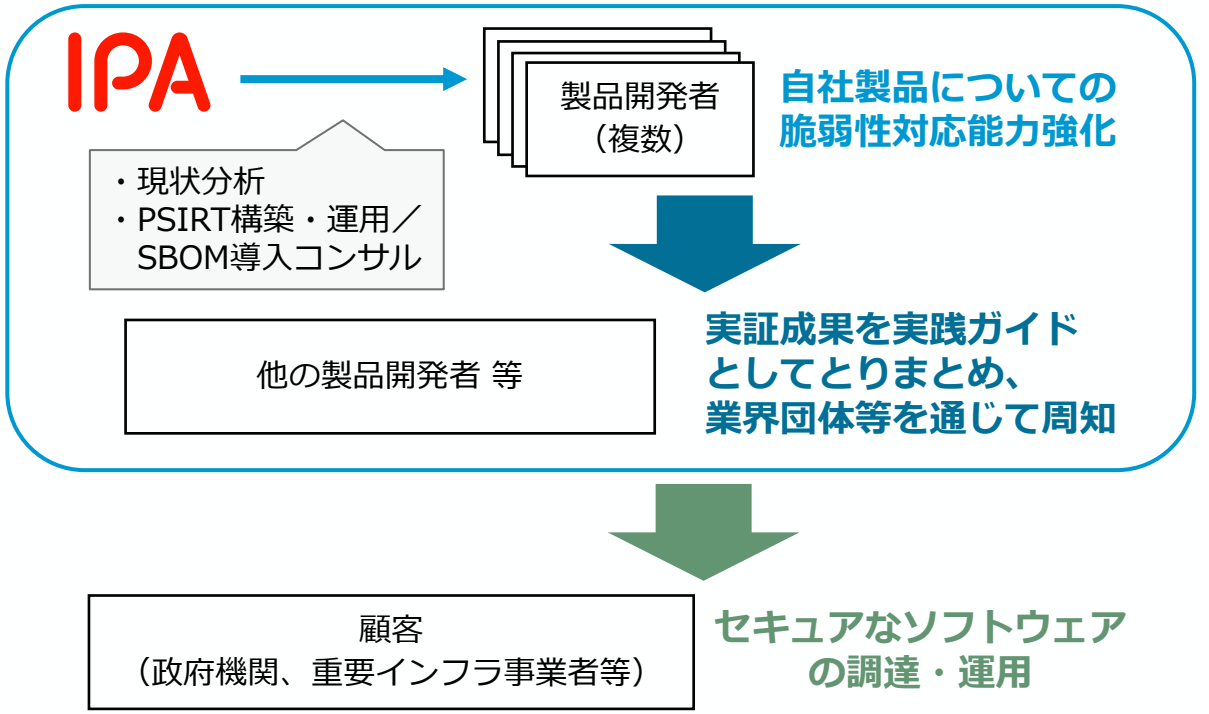
PSIRTの構築・運用及びSBOMの導入支援

- 人的・予算的制約がある中でもPSIRTの構築・運用及びSBOMの導入を効率的かつ効果的に実現するための実証事業を行い、その成果物として、上記ノウハウを集約した実践ガイドを作成予定。

地域ITベンダー向け手引きの作成

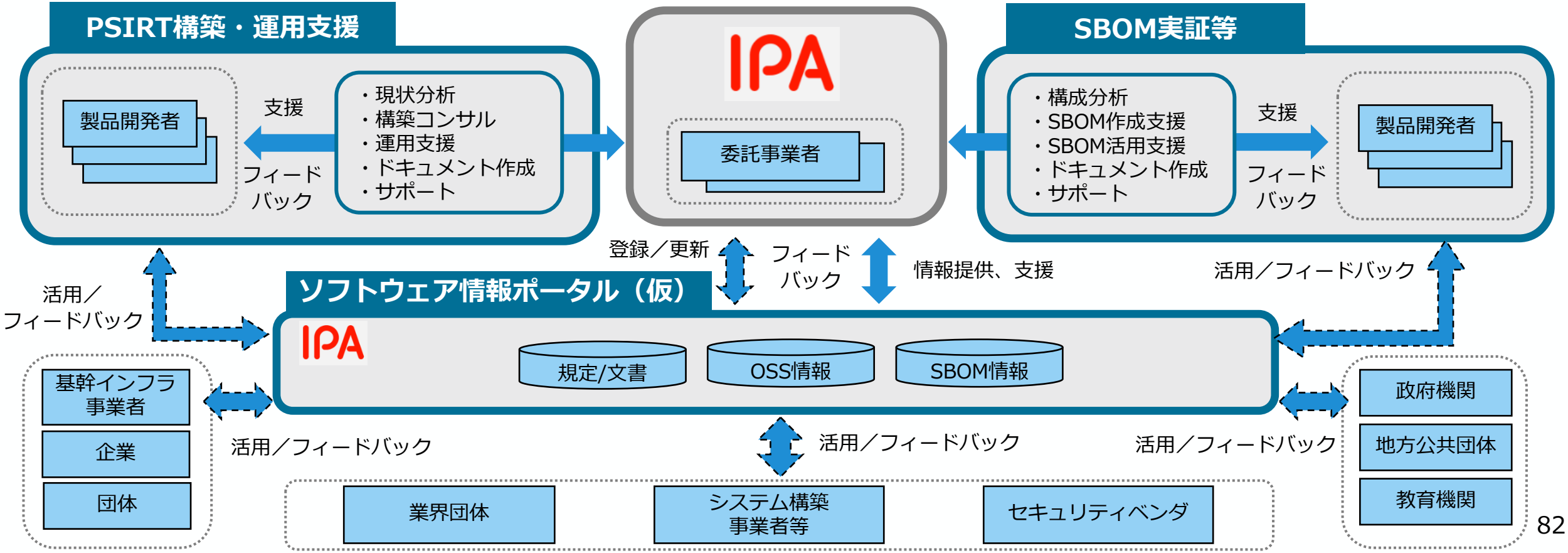
- 中小企業にとってサイバーセキュリティ対策を実施する際の主たる相談相手となる地域のIT関連企業が、その重要な役割を果たすために活用可能な、人材育成・活用策を含めた手引きについて、「サイバーインフラ事業者に求められる役割等に関するガイドライン」との整合性も確保しつつ、IPAにて別途作成中。

<PSIRT構築・運用等支援事業のイメージ>



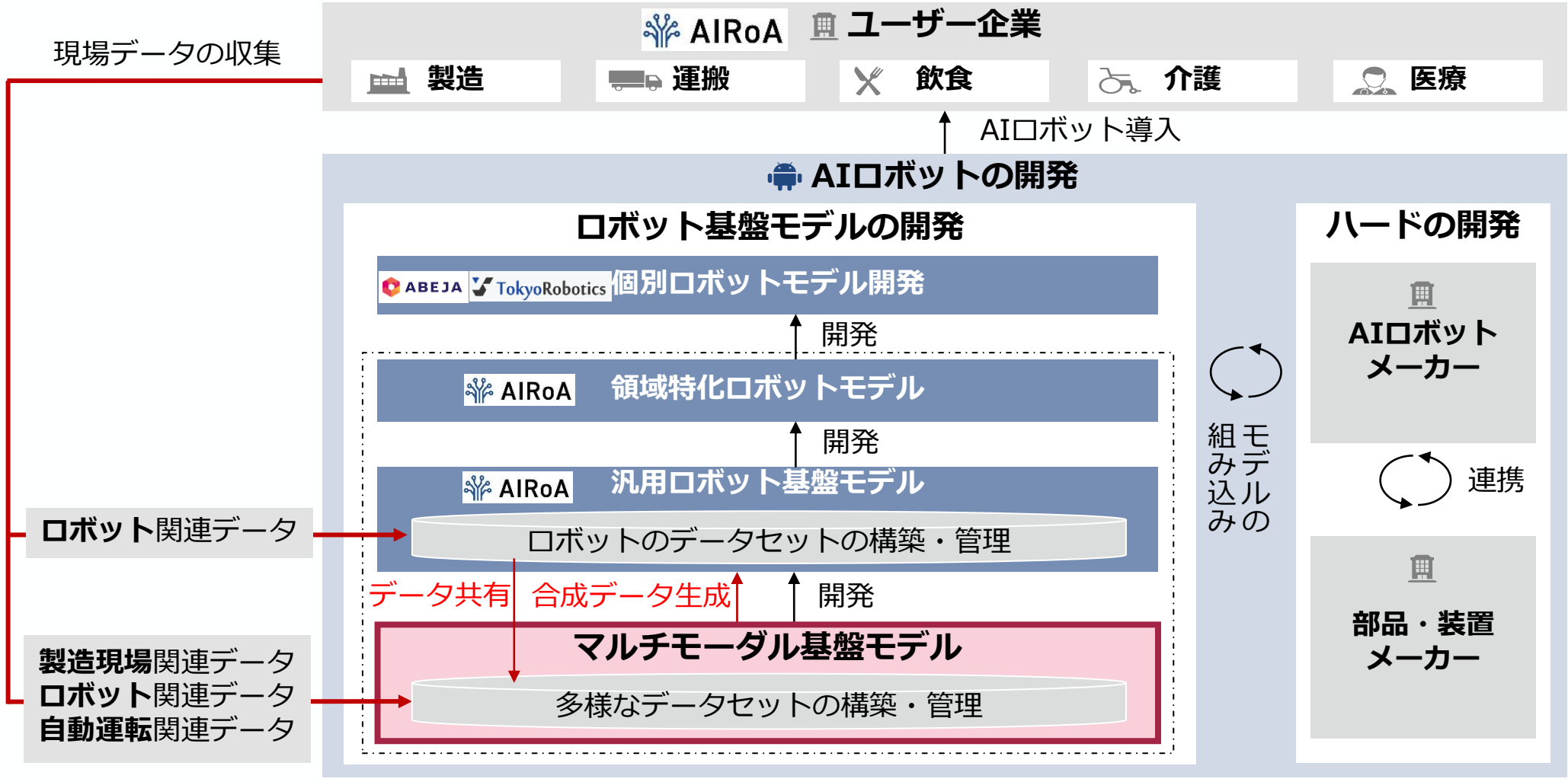
PSIRTの構築・運用及びSBOMの導入支援（中小ソフトウェア開発支援プラットフォームの構築）

- 「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」では、 PSIRTの設置やSBOMの導入など、リソースの限られる中小企業にとって実施のハードルが高い取組も求められる。
- 取組支援策として、①製品開発者に対するPSIRT構築・運用の支援、②製品開発者に対するSBOM作成・SBOM利活用の支援、③これら結果をとりまとめ、他の組織へ広く展開するためにソフトウェア情報ポータルを構築し、ソフトウェアに関する情報等の利活用を促進していく。



フィジカルAI時代のロボット基盤モデルの重要性

- AIRoAが開発する汎用ロボット基盤モデルは、**海外のオープンモデルを基盤として利用中**。ただし、現在は性能が十分ではなく、海外のオープンモデルは、①**最新のクローズドモデルに比べて物体認識や環境理解など性能に大きな差**があること、②**内部構造や学習過程がブラックボックス化**されており、**実用化に向けた継続的な改良や安全性評価に課題**を有することから、現在のものはプロトタイプに留まり、今後、今回開発する**国産の基盤モデルをベース**として、**実用・汎用的なロボット基盤モデルの開発をしていくこととなる。**
- 国産のAI基盤モデルをフィジカルAIに対応させていくために、**日本の虎の子の製造業・ロボット関連データを学習させていく**ことになる。

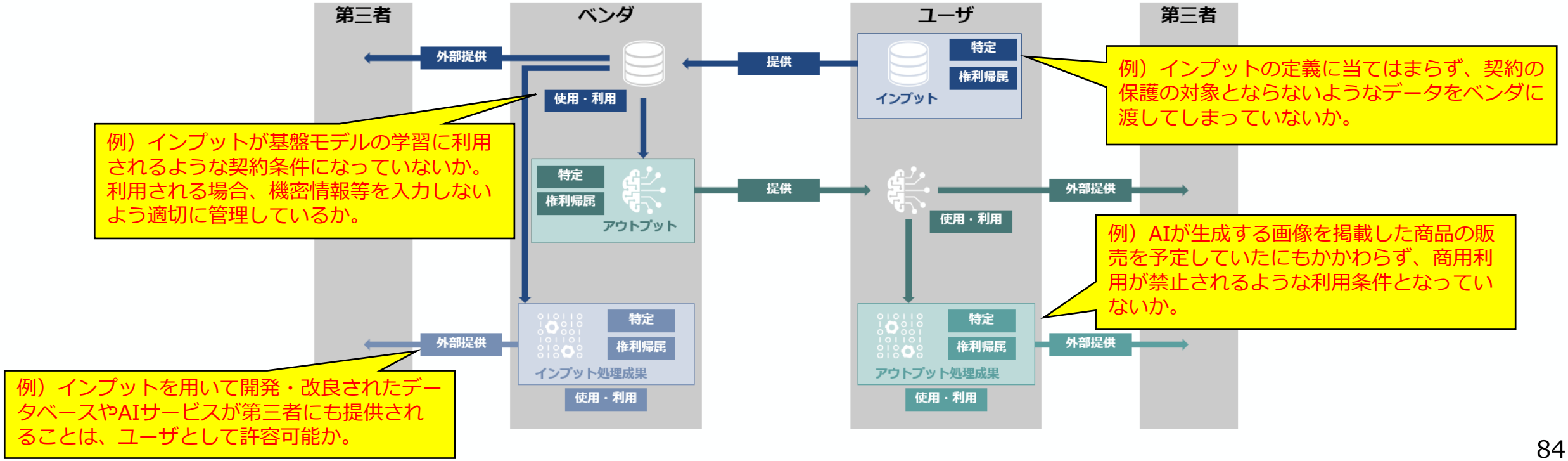


防御的な対応：契約の精査（AI契約チェックリストの活用）

- グローバルAI企業との協業において営業秘密等のデータを適切に保持し、強みを維持できるか懸念あり。**データの適切な保護が図られ、無断で利用されることが無いかなど契約を精査することが重要。**

⇒**「AI利活用に伴う契約時の留意事項検討会」を2024年10月から開催**し、**AIユーザ企業**における社内法務部・顧問弁護士とビジネス部門担当者が連携して、 **効果的なAI利活用・データ管理に資する契約書を検討できるように、チェックリストを策定。**

（参考）AI契約チェックリストの構造と活用事例



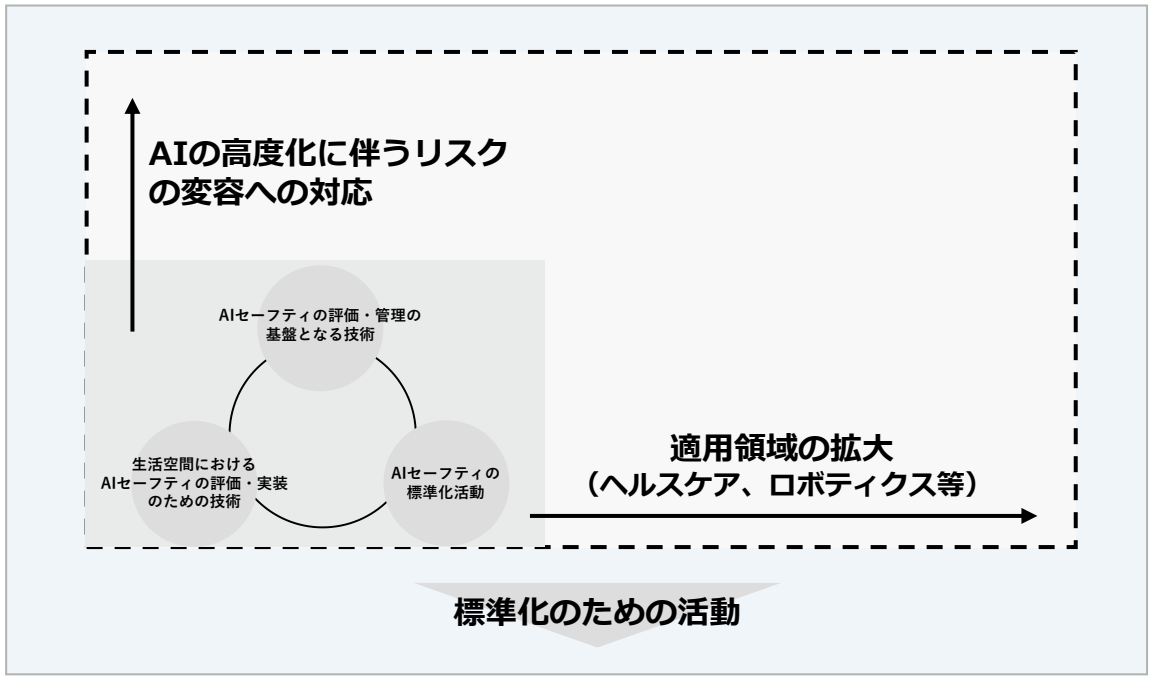
AIセーフティの取組強化 ～AISIを中核とした標準化活動～

- 国内外のAI安全性の知見のハブとして、**国内外の関係機関とのネットワーキング**を進めるとともに、**安全性評価能力を確立**しながら、**安全性評価のためのガイダンスの作成**等を目指す機関として、2024年2月、IPAに、**AIセーフティ・インスティテュート**（AISI）を設置。
- AISIは、これまでの取組を発展させ、ドキュメントの策定や国際連携に加え、**汎用／分野別のAIセーフティ評価環境の構築**等を目指す。
- その際、経済産業省としては、国研等のアセットも活用しながら、**主に技術面からAISIを支援**する。

AISIの取組方針

- 最新の動向を反映した「評価観点ガイド」「レッドチーミング手法ガイド」の改訂
- 汎用的なAIセーフティ評価環境（自動レッドチーミングツール、ベンチマーク、データセットなど）の構築
- 分野別（ヘルスケア、ロボティクス、データ品質、適合性評価等）の取組（分野別AIセーフティ評価に関するドキュメント、評価シナリオ、データセット等の策定）
- AIセキュリティに対する取組（AIシステムに対する特有の攻撃手法の調査、AIセキュリティインシデントの分類体系の検討）
- 国際連携の強化　等

国研等を活用した取組

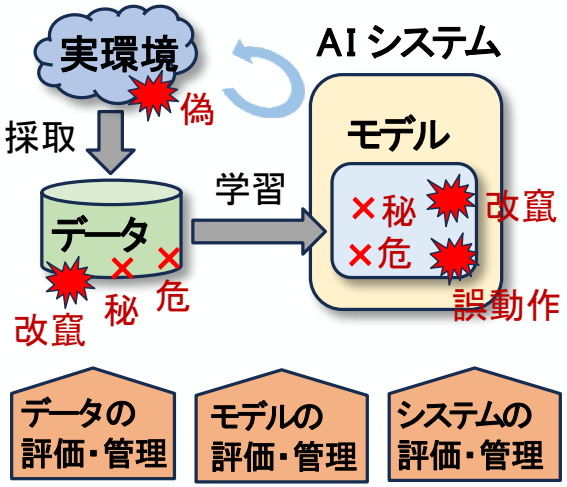


産総研におけるAIセーフティの研究開発

- AISIを中心とした取組の中で、産総研においても、日本が強みを持つフィジカル分野の知見も活かしたAIセーフティの研究開発を加速し、その成果を元に基準を策定するとともに、国際標準の形成も主導していく。

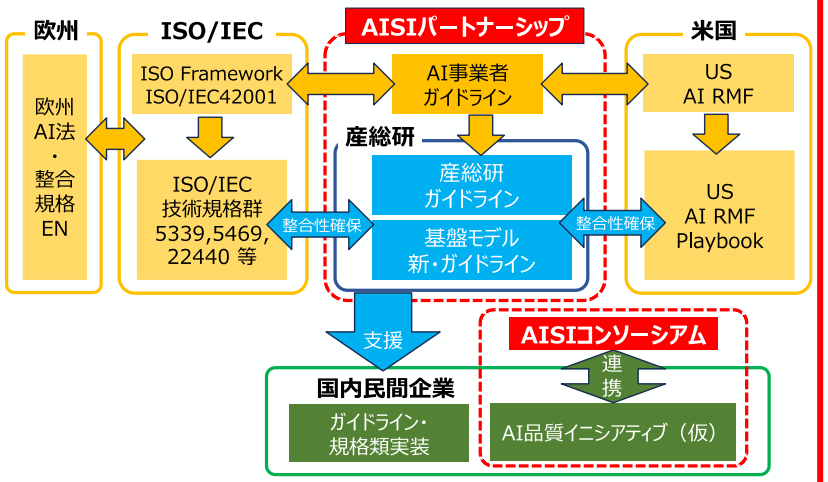
①AIセーフティ評価・管理基盤技術開発

- **AIに対する個別の攻撃や防御手法の研究は盛んだが、安全性の評価・管理技術が体系的に確立していない。**
- **このため、データ、モデル、システムそれぞれのレイヤーにおいて、それぞれの課題を踏まえ、リスクベースアプローチの基になる安全性を評価するためのソフトウェアツールやベンチマークデータを開発する。**



③AIセーフティ基準・ガイダンス作成と標準化活動

- **①や②の成果を基に、AIセーフティ基準・ガイダンスを作成する。**
- **関係する事業者を巻き込みながら、AIセーフティ基準・ガイダンスの社会実装・普及を促進する。**
- **あわせて、ISO/IECにおける標準化活動と国際連携も行う。**



②応用領域別AIセーフティ評価・実装技術開発

- **サイバー空間とフィジカル空間をつなぐ応用領域(暮らし支援、協働ロボット、スマートシティ)に特有のリスクに対応するためのAIセーフティ評価・実装技術を開発する。**

暮らし支援

プライバシー情報を適切に扱うAIを開発するため、介護見守りAIをモデルケースとして、デジタルツインを用いて生活事故環境を再現する技術を開発する。

協働ロボット

AIロボットが予想外な動き等により人をケガさせないよう、模擬的な環境下で、複数のAIロボットが相互に連携して人と協調した作業を安全にできる技術を開発する。

スマートシティ

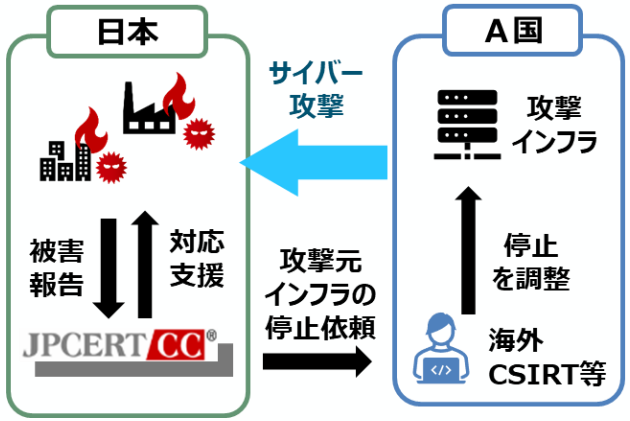
通信断で人による遠隔操作・制御不可になっても、安全・安心に動作する自律性の高いAIロボットの開発のため、屋内外のシームレスなデジタルツインを実現する技術を用いたロボットの統合運用管制システムを開発する。

４．政府全体でのサイバーセキュリティ対応体制の強化

サイバー被害に関する対応支援・国際調整窓口等の実施

- **JPCERT/CC** ※ は、民間の非営利団体（一般社団法人）として、**1996年から活動を実施**。
  ※ Japan Computer Emergency Response Team / Coordination Center
- **我が国の調整窓口として1998年から機能**し、これまで複数の職員が世界各国の調整機関が集まる団体（FIRST）の理事に選出されるなど、国際的な認知度・信用度も高い。

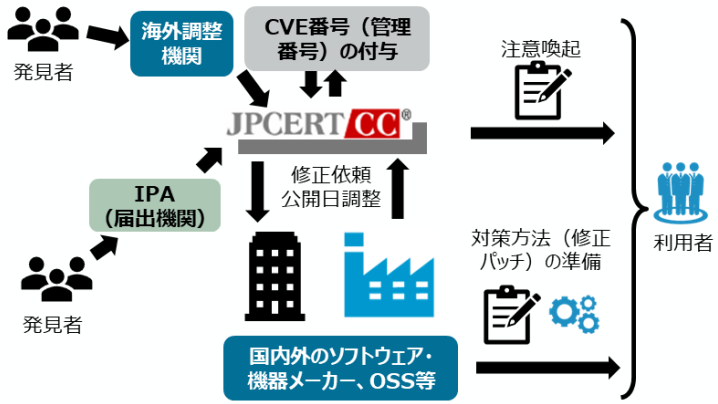
事案対応支援、国際連携強化・調整業務



<2025年度の取組・進捗>

- インシデントの被害発生及び拡大防止のための調整を11,610件実施（2026年2月末時点）
- APCERTの事務局及び運営委員会メンバーや国内企業等のCSIRTのFIRST加盟スポンサーを務め、アジア太平洋地域及び世界的なCSIRT連携の活動に貢献 等

ソフトウェア等の脆弱性対応



<2025年度の取組・進捗>

- 脆弱性に関する製品開発者との調整を約20,651件実施（2026年2月末時点）
- PSIRTとの脆弱性対処等に関する情報・意見交換会を２回実施（延べ約190人が参加） 等

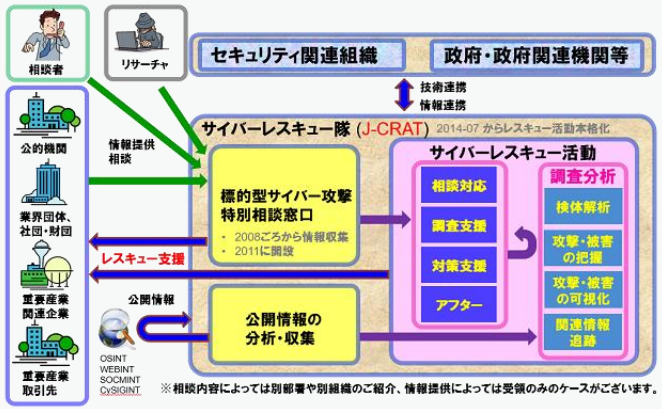
IPA サイバーレスキュー隊（J-CRAT）／サイバー情勢分析部

サイバーレスキュー隊（J-CRAT）

- 広く一般から相談や情報提供を受付け、提供された情報を分析して調査結果による助言を実施。
- **標的型サイバー攻撃の被害の発生が予見**され、その**対策の対応遅延が社会や産業に重大な影響を及ぼすと判断される組織**や、**標的型サイバー攻撃の連鎖の元となっていると推測される組織**などに対し、レスキュー活動にエスカレーションして支援。

<2025年度の取組・進捗>

- 国内組織を標的とした国家支援型の標的型サイバー攻撃に係るレスキュー活動を実施（実績は下表のとおり）。



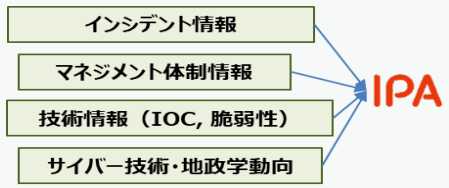
2025年度実績	
相談・情報提供数	387
支援数	166
オンサイト支援数	56
アクティブレスキュー数	124

サイバー情勢分析部

- 国家安全保障戦略に基づく対応強化のため、IPA 第五期中期目標において、**「サイバー状況把握力」を強化**し、**国家の安全保障・経済安全保障の確保**に貢献する旨を明記。2023年7月にサイバー情勢研究室を設置。
- 今後、**サイバーセキュリティ産業振興の観点**も踏まえながら、**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、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。2025年4月にサイバー情勢分析部に改組し、体制を強化。

<2025年度の取組・進捗>

- 地政学的な観点から**サイバー脅威情報を産官学へ発信**（ブリーフィングや外部講演、執筆等 合計48件）。
- NCOなどへのブリーフィングを通じて**組織間の連携強化**を図った。



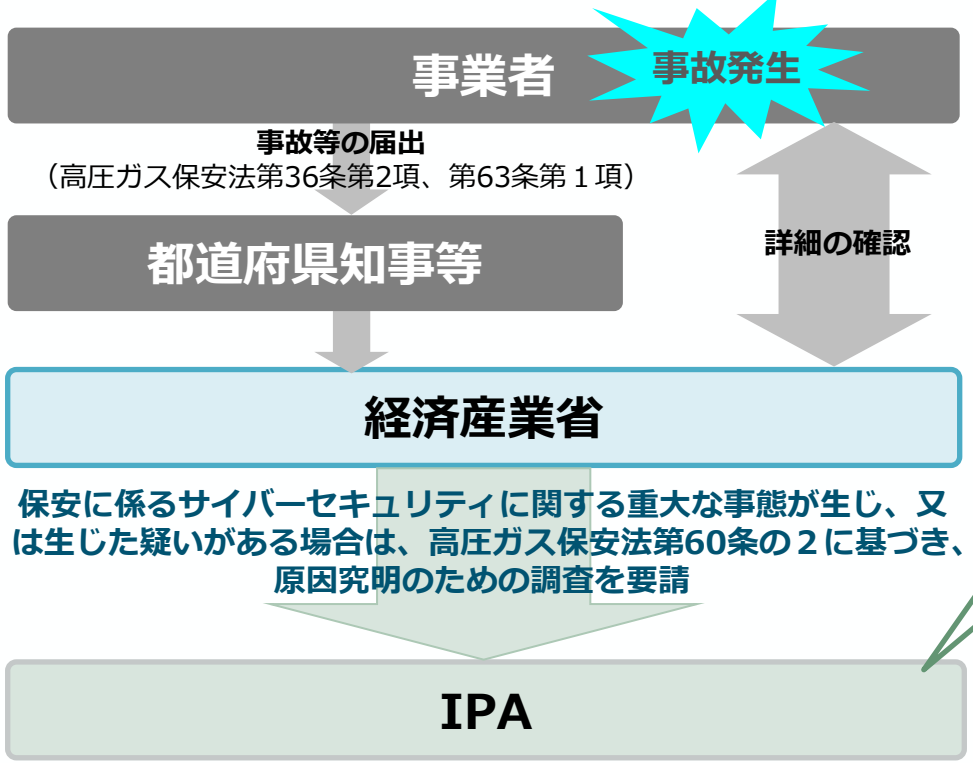
（出典）IPA「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）について」 https://www.ipa.go.jp/security/j-crat/about.html

IPAによるサイバー事故調査

- 2022年に公布（2023年に施行）された高圧ガス保安法等の一部を改正する法律に基づき、IPA（産業サイバーセキュリティセンター）内に産業保安分野におけるサイバーインシデントに係る調査体制を整備。
- 調査官には、関連する産業分野に所属する中核人材育成プログラムの修了者も加わる※ことで、体制を拡充し、フォレンジック調査、可搬プラントによる演習等に係るトレーニングなども継続的に実施。

※企業に所属しつつ、トレーニングや定例のミーティングに参加。修了者の二次的な学びの場としても機能。修了者は10名が参画（2026年4月現在）。

IPAへの調査要請のフロー（イメージ）



IPAによる調査のイメージ

- ✓ IPAによる調査は、書面審査と現地調査の二段階で構成する。
  ※ただし、書面調査のみで十分に原因を特定できた場合には、現地調査は行わない。
- ✓ 現地調査においてIPAは対象システムのログ等を確認することによって、サイバーセキュリティに関する重大な事態が生じた原因を究明するための調査を行う。
- ✓ 調査日数や調査内容等は、IPAと事業者で相談の上、決定する。

高圧ガス保安法等の一部を改正する法律（抄）
第六十条の二　経済産業大臣は（中略）**保安に係るサイバーセキュリティ（中略）に関する重大な事態が生じ、又は生じた疑いがある場合**において、必要があると認めるときは、**独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる。**

５．サイバーセキュリティ供給能力の強化

先進的サイバー防御機能・分析能力強化のための研究開発

- 高度かつ未知の攻撃にも対処可能な**攻撃の早期発見技術**や、AIを活用したシステムの脆弱性の検知・評価技術など**防御力向上に資する技術**の開発・社会実装に向け、**約300億円／５年の研究開発プロジェクト**を立ち上げ、2024年７月からプロジェクト開始。

実施体制

一般社団法人サイバーリサーチコンソーシアム

研究開発の体制

理事会
※**FFRI、日立製作所、富士通、三菱電機、NTT、NECから理事を選出**

代表理事（FFRIセキュリティ 鵜飼社長）

一般社団法人（サイバーリサーチコンソーシアム） → **一般社団法人から再委託**

大手民間企業、スタートアップ、大学・国研（計19者）も参画
※その他、情報通信研究機構等、関係機関とも連携

事業規模など

- 事業規模　：　290億円以下（2024年7月～2029年3月）
- 契約形態　：　委託事業

主な研究開発内容

1）サイバー空間の情報を収集・調査する状況把握力の向上
- アーティファクト分析技術／攻撃者からより多くの情報を獲得するための技術／高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

2）サイバー攻撃から機器やシステムを守る防御力の向上
- AIを活用した脆弱性探査技術／AI等を活用した防御能力の評価・向上技術／AIを活用したOTペネトレーションフレームワーク技術
- 耐量子計算機暗号技術／耐タンパー性向上技術

3）共通基盤の整備
- 情報の効果的な連携に関わる技術
- 高度サイバー人材の評価・管理に関する技術

4）セキュアな量子情報通信技術の開発
- Y-00のデジタルコヒーレントの開発／Y-00の高速光ファイバ通信の開発／Y-00の高速光ワイヤレス通信の開発

フロンティア育成・懸賞金事業（サイバーセキュリティ関連技術の募集）

- セキュリティ対応力強化が求められる中、現場に無理なく導入できる技術・製品の開発を促しながら、**スタートアップ企業等に実績の機会を提供**するため、**サイバーセキュリティ関連技術を募集する懸賞金事業**を2026年度～2027年度にかけて実施する予定。

懸賞金事業の目的

- ✓ **国内企業のセキュリティ対応力強化**を目的に、懸賞金事業により**先進的なサイバーセキュリティ技術**を募集。
- ✓ 高度化する脅威**迅速・実効的に対応し、現場に無理なく導入・定着できる技術開発・製品化**を重視。
- ✓ 革新的な製品・サービスの創出と発掘を促し、我が国の**DX推進と経済成長**に寄与することを目指す。

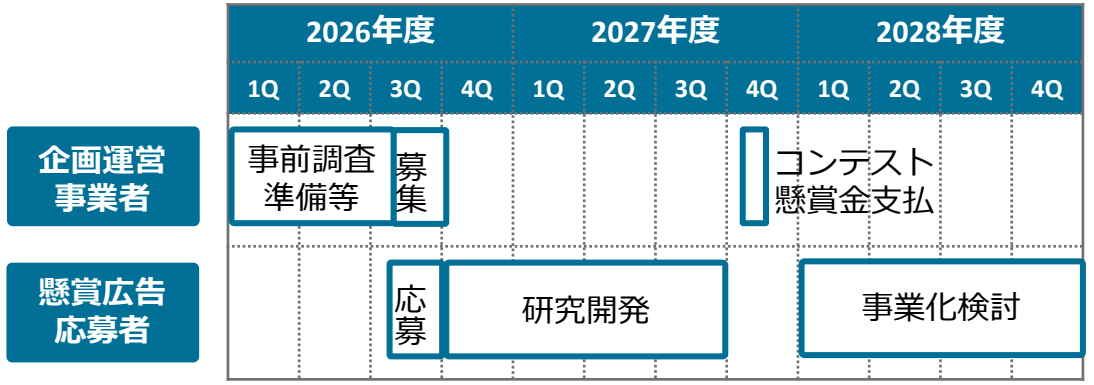
懸賞金テーマ：サイバーセキュリティの技術

以下のテーマ(案)において、効果的・効率的に革新的な**セキュリティ対策技術**の応募を期待。

- ✓ **AI技術を活用した**革新的なサイバーセキュリティ製品・サービスの開発・製品化
- ✓ **SBOM**（Software Bill of Materials：ソフトウェア部品構成表）の効率的な実運用に資するための技術開発・製品化
- ✓ **SSDF**（Secure Software Development Framework：米国NISTが策定したセキュア・ソフトウェア開発フレームワーク）

懸賞金事業スケジュール

以下のスケジュールを想定。2026年末に懸賞広告を公表し、**約1年間の研究開発期間**を設け、**2027年度末**にコンテストを実施予定。



業界団体等と連携したマッチングイベントの実施

- 日本ネットワークセキュリティ協会（JNSA）が中心となり、国内セキュリティスタートアップとSI事業者とのマッチングを推進。2025年10月に「国産セキュリティ推進フォーラム」を経済産業省・JNSA共催で開催し、**約80名が参加して国産技術振興の課題を議論。今後はテーマを絞った小規模なマッチングイベントを開催予定。**
- 防衛装備庁とも連携し、2026年２月に**自衛隊とのマッチングイベントを実施。**引き続きニーズに応じた情報収集と支援を行う。

国内スタートアップとSI事業者とのマッチング

✓日本ネットワークセキュリティ協会（JNSA）が中心となり、我が国商流の中心となっているSI事業者と国内セキュリティスタートアップとのマッチングを推進。2025年10月には、経済産業省とJNSAが共同で「国産セキュリティ推進フォーラム」を初開催。

✓本フォーラムでは、製品・サービスを開発する事業者やスタートアップ、それらを取扱うSI事業者や販売代理店、国内サイバーセキュリティ企業への投資に特化したファンド運営者、ベンチャーキャピタリストなど約80名が参加し、国産振興に係わる課題やその解決策を議論。

✓今後は、テーマを絞ってより小人数でのマッチング精度を高めたイベントを開催（2026年４月予定）。事前事後のアンケート調査により、マッチング精度を可能な限り高めつつ、進める。

JNSA

防衛装備庁と国産技術のマッチング

✓防衛装備庁と協力し、2026年２月に陸海空自衛隊等とのマッチングイベントを開催。

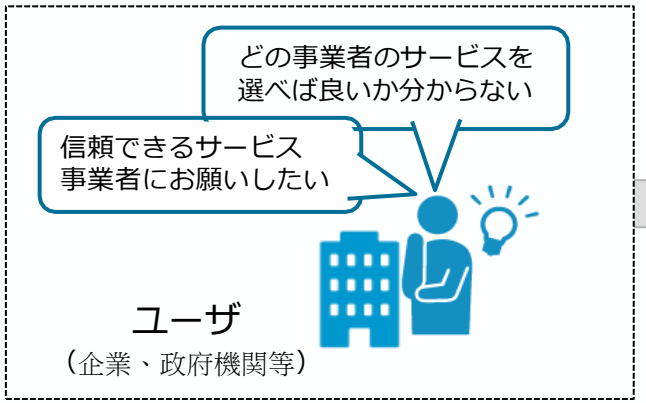
✓防衛装備庁のニーズ等を踏まえ、次回のマッチング機会に向け、引き続き支援を行う。

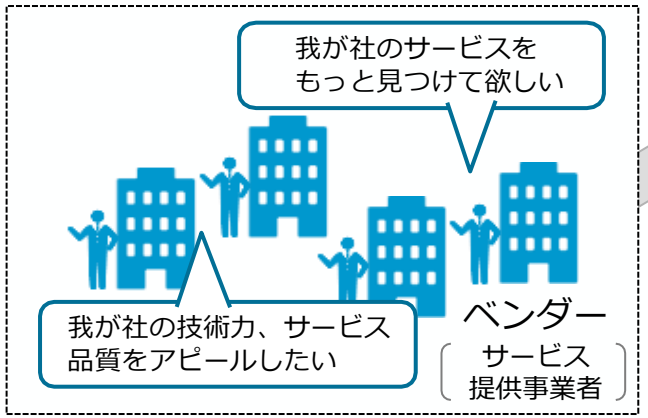
防衛省・自衛隊

情報セキュリティサービス審査登録制度

- 経済産業省の作成した「情報セキュリティサービス基準」に基づき、審査登録機関による審査をクリアしたサービスのリストをIPA（独立行政法人情報処理推進機構）が公開。
- 登録件数は398件（2026年3月時点）。　※2025年3月時点から49件増加

○情報セキュリティサービスにおける課題





選定時に活用

審査を受けてリストに掲載

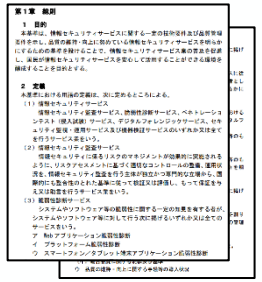
情報セキュリティサービス基準適合サービスリスト（IPA）

審査登録機関による審査で基準を満たすと 認められたサービスをリストにして公開

基準を満たした398サービスを掲載（2026年3月現在）

- 情報セキュリティ監査（84サービス）
- 脆弱性診断（188サービス）
  - うちペネトレーションテスト(51サービス)
- デジタルフォレンジック（43サービス）
- セキュリティ監視・運用（51サービス）
- 機器検証 （32サービス）

情報セキュリティサービス基準（経済産業省）



対象のサービス(5サービス、1オプション)に関して技術要件・品質管理要件を定めた基準を公開

○本制度を通じて目指す社会

専門的知識を持たない ユーザでも、自社に最適かつ品質を備えたサービスを選択できる

技術と品質を備えた情報セキュリティサービスの普及・発展

制度の普及・浸透

（出典）情報セキュリティサービス基準適合サービスリスト　https://www.ipa.go.jp/security/service_list.html

サイバーセキュリティ人材施策の全体像

セキュリティ対策を進めるための体制・人材の考え方

○セキュリティ体制構築・人材の確保の手引き（「サイバーセキュリティ経営ガイドライン」付録F）

- 企業経営者等向けに、自社でセキュリティ人材を確保し体制を整備するための実践的な指針を提示

○セキュリティ人材確保・育成の実践ガイドブック（「中小企業の情報セキュリティ対策ガイドライン」付録）

- 中小企業が実施すべきセキュリティ対策と必要な人材の確保策などを段階的に提示するとともに、各社が実践の参考とできるよう、中小企業等へのヒアリングに基づく具体的な取組事例を掲載（2026年３月に公表）

セキュリティ人材の育成

○セキュリティ・キャンプ

- 若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラスの人材を育成・発掘

○中核人材育成プログラム（IPA/ICSCoE）

IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

- OT(制御技術）とIT（情報技術）の知見を結集させた世界レベルのサイバーセキュリティ対策の中核拠点における、１年を通じた集中トレーニング

○情報処理安全確保支援士（登録セキスペ）

- サイバーセキュリティの確保を支援するための、セキュリティに係る専門的な知識・技能を備えた国家資格

プラス・セキュリティ（※）の普及

※セキュリティを本務としない者が業務遂行にあたってセキュリティを意識し、必要十分なセキュリティ対策を実現できる能力を身につけること、あるいは身に着けている状態のこと

○地域SECUNITYにおける人材育成

- セミナーの開催を通じた人材育成支援など、各地域でのセキュリティの「共助」に向けた取組を促進

○NCOにおけるモデルカリキュラム策定

- プラス・セキュリティ知識を補充できるプログラムの普及に向けて、教育事業者や社内研修の参考となるカリキュラムを公開

○サイバーセキュリティ人材フレームワーク2026（NCO）※2026年４月策定予定

○デジタル人材育成プラットフォームによる個人のデジタルスキル情報の蓄積・可視化

○大学・高専等と産業界との連携

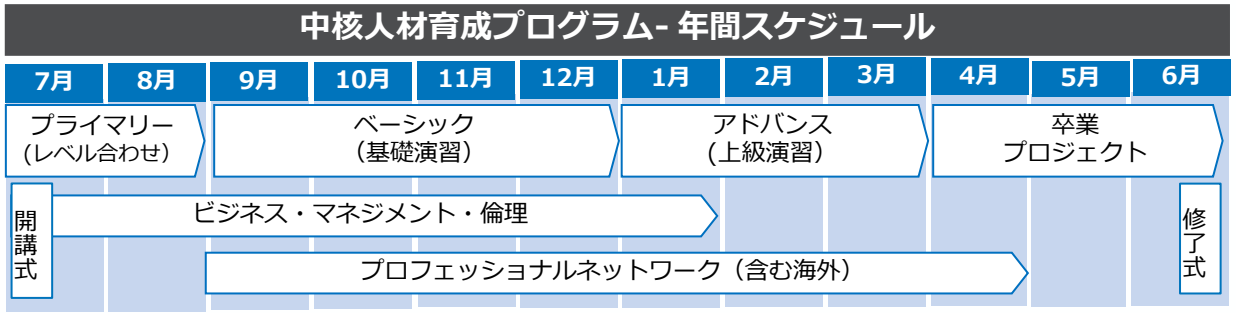
IPA産業サイバーセキュリティセンター（ICSCoE※）

2017年4月設置

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ１年の集中トレーニング等を実施。

□　１年を通じた集中トレーニング「中核人材育成プログラム」

□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣、9期生まで約550名が受講
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人、第８期：57人、第９期：55人）

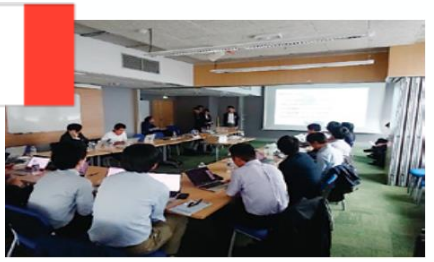


- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

現場を指揮・指導するリーダーを育成

□　米・英・仏等の海外とも協調したトレーニングを実施

➢ CISA※が開催する高度なサイバーセキュリティトレーニングである301演習への参加



➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

※ICSCoE : Industrial Cyber Security Center of Excellence
※CISA : Cybersecurity and Infrastructure Security Agency

ICSCoE修了者の活躍状況（大阪・関西万博）

- IPA ICSCoEは、大阪・関西万博における設備制御システムのセキュリティを確保するため、開催前から開催中に亘り、以下の支援を実施。
- そのうち、開催中に実施したセキュリティインシデント対応に関する業務では、**中核人材育成プログラム修了者**ほか、計12社18名で対応体制を構築し、**国際的な大規模イベントのセキュリティ確保に寄与**。

開催前（2023年10月～2025年4月）

- 博覧会協会が会場（夢洲）に設置予定の設備制御システムについて、リスク分析を実施。
- 特に対策の優先度が高い施設・重要システムを選定し、それらの実装状況の確認及びセキュリティ検証を実施。

開催後（2025年4月～2025年10月）

- **<u>セキュリティインシデント対応に関する業務</u>**
  - 継続的に会場の見回りを行い、サイバー攻撃等による脅威の兆候を把握・分析し、定期的に博覧会協会へ報告。また、見回りにおいて発見したリスク要因について対策の提案等を実施。
  - 博覧会協会からの要請に基づき、緊急的なインシデント対応として会場への駆け付けを行い、発生事象の分析、対策の提案等を実施。
  - 修了者所属企業（五十音順）
    アズビル㈱、㈱オプテージ、㈱きんでん、ダイキン工業㈱、ダイキン情報システム㈱、
    大和ハウス工業㈱、中部電力㈱、西日本旅客鉄道㈱

セキュリティ検証
（パケットキャプチャ）

ICSCoE　Mission/Vision/Values①

※2025Visionを見直しMVVとして整理

Mission（6つの柱）

組織の存在意義

リスク分析・事故調査の支援

産業保安分野のサイバー事故調査
設備制御システムのリスク分析・
セキュリティ検証

世界に類を見ないユニークな機関

多様で実践的な研修プログラム

様々な分野の実環境の再現
外部機関の設備の活用

高い専門性・多様性

様々な分野・技術の専門家との
ネットワーク強化
DXの進展による新興リスクへの対応

強力な修了者ネットワーク

修了者同士や政府機関等との連携
修了者ネットワークでの最新情報の流通

有能な人材輩出・知識のアップグレード

攻撃情報の分析・追究
オープン・サイバーセキュリティ技術の開発
自前技術を作れるタレントプールの創出

国際的な連携拠点

海外関係機関との連携強化・拡大
海外のOTセキュリティ人材の育成
に貢献

Vision

目指す組織の理想像

サイバー領域の脅威がフィジカル領域に大きな影響を与えるDXが進んだ産業社会のサイバーセキュリティ対応能力の開発・普及を行う国際的にも通用する中核機関を目指す。

ICSCoE　Mission/Vision/Values②

※2025Visionを見直しMVVとして整理

Values
大事にする価値観

高水準の人材育成	✓ 産業サイバーセキュリティ分野における**高水準の人材を継続的に育成**する。 ✓ そのために、**最高レベルの講師陣を維持・確保**する。
修了者を通じた社会への価値提供	✓ 修了者が重要インフラ等の**所属組織内で活躍**するとともに、叶会を基盤として政府や各業界との連携などを通して**社会に貢献できるよう支援**する。
モノづくり産業発展への貢献	✓ **中核人材**を内在・活用させることこそが、我が国の強みである**モノづくり産業の長期的・持続的な競争力強化に資する**との視点を持つ。
海外キープレーヤーとの連携	✓ 我が国企業が進出する主要国において、産業サイバーセキュリティに関する**最新動向を把握**し、**関係者を動かせる中心人物・機関との関係を構築・維持**する。

ICSCoE　MVV達成に向けたこれまでの取組

※６つの柱は2025Visionのもの

サイバーインシデント事故調査

- ✓ 高圧ガス保安法などの改正により、高圧ガス、ガス、電力分野において、サイバーインシデント事故調査規定を整備
- ✓ 対象事業者と協力し、事故調査フロー、調査内容等を整理
- ✓ サイバーインシデント事故調査室を設置し、対応環境を整備
- ✓ 法律に関する周知徹底のため、各地保安監督部と連携して普及啓発活動を実施
- ✓ 大阪万博におけるOTセキュリティ対策に修了者とともに協力

最新情報の流通経路

- ✓ 修了者の活動基盤（修了者コミュニティ「叶会」）を整備するとともにコミュニティの規模を拡大
- ✓ IPA主催イベント等での共催など、叶会の活動を対外的に発信
- ✓ サイバーセキュリティ情報共有ツールを用いて、脆弱性情報や攻撃情報等をICSCoE関係者間で共有する仕組みを構築

世界に類を見ないユニークな機関

- ✓ １年間、アクティブラーニング形式の演習プログラムを実施し、約500名が修了。また、ビジネスマネジメント講義を重要インフラ企業向けにリニューアル
- ✓ 流派の異なるユニークな講師による重層的教育及び受講者の自主研究を通じ、部門間のギャップを乗り越えるマインドセットを醸成
- ✓ 企画立案スキルを習得するための短期プログラム（CyberSPEX）を新設
- ✓ 中核人材育成プログラムに派遣いただけていない地域や業界等にアプローチするため、短期プログラムの地方開催を実施。さらに、可搬型模擬プラントを用いた演習を開始
- ✓ 中核人材育成プログラム修了者が短期プログラム等におけるファシリテータや講義を担当

有能な人材輩出・知識のアップグレード

- ✓ サイバー攻撃の模擬的な実施など、技術形成・人材育成・産業形成などのため試行錯誤できる環境を構築し、提供
- ✓ シン・テレワークシステムを構築。また、自治体テレワークシステム for LGWAN を開発し、企業や千を超える行政機関で数十万ユーザが重要な日常業務に利用

高い専門性・多様性

- ✓ 脆弱性を悪用したサイバー攻撃手法などを分類・整理した「MITRE ATT&CK※」へ情報を提供

※ MITRE（The MITRE Corporation）という米国連邦政府が資金提供している非営利組織が、脆弱性を悪用したサイバー攻撃を、戦術と技術または手法の観点で分類したナレッジベース。ATT&CKは、Adversarial Tactics, Techniques, and Common Knowledgeの略

- ✓ 修了者向けにリカレント教育の場を提供し、知識・スキルのアップデートを実施

国際的な連携拠点

- ✓ 仏国、英国、米国への派遣演習や米国・EUによる特別講義を実施
- ✓ 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やAJCCBCとの連携事業を通じて、米国、EU、インド太平洋地域の各機関へ中核人材育成プログラムをPR
- ✓ APANを活用したASEAN各国との演習強化に向けてネットワーク関連機器を設置
- ✓ HPや「ICSCoE Report」を英語版でも作成し、中核人材育成プログラム受講者及び修了者の国際イベント等での活躍を国内外に継続的に発信

横断的な取組

- ✓ 世界最大級のセキュリティに関する国際イベント「Black Hat」やNATOサイバー防衛協力センター（CCDCOE）が主催する「Locked Shields」等、ハイレベルの会議・演習への参画
- ✓ 多様な専門性を有する人材（修了者）を輩出

ICSCoE　MVV達成に向けた2030アクションプラン

リスク分析・事故調査の支援

- ✓ サイバーインシデント事故調査に備え、平時からサイバー攻撃と想定される事案に関する情報を収集し、最新の技術・ノウハウを蓄積
- ✓ 海外や国内の環境変化、サイバー事故の実態等を踏まえ、調査の在り方や対象について、継続的な検討を実施
- ✓ 国際イベント等での設備制御システムのリスク分析・セキュリティ検証や現場への駆け付け支援の実施

世界に類を見ないユニークな機関

- ✓ 引き続き、IT×OTのセキュリティを学ぶ“１年間”の演習プログラムを実施するとともに、中核人材育成プログラムに派遣いただけていない業界等にアプローチするため、短・中期コースや模擬プラントを拡充
- ✓ 教育の質や幅を拡充するため、新規講師の育成・採用を推進
- ✓ 中小企業等を含むサプライチェーン全体を意識した教育コンテンツを新たに整備

高い専門性・多様性

- ✓ トップレベルの国際的イベント等への参画、情報発信等を行うなど、国際舞台で活躍する人材を拡大
- ✓ 各業界の専門人材を拡大するため、業界の特徴を理解する機会（ステークホルダーとの対話等）の拡大
- ✓ AIエージェント・フィジカルAIや量子コンピュータなど、DXが進む産業社会において活用される先端技術に係るサイバーセキュリティリスクの検証・対策の立案を実施・指導できる人材の拡大
- ✓ 各国・各言語圏に通じた修了者の協力も得ながら、ICSCoE並びに中核人材育成プログラムの認知度向上に向けて海外専門機関との関係構築・拡大を図る

強力な修了者ネットワーク

- ✓ 叶会を活用し、脆弱性情報や攻撃情報等をICSCoE関係者間で共有する仕組みを強化
- ✓ 叶会やICSCoEの認知度向上を目的として、叶会の活動や修了者の活躍の対外的な発信を強化
- ✓ 叶会から国の有識者検討会に参画する者を輩出するなど、活動の場を更に拡大
- ✓ 行政機関等との人材交流や施策検討・実施における連携

有能な人材輩出・知識のアップグレード

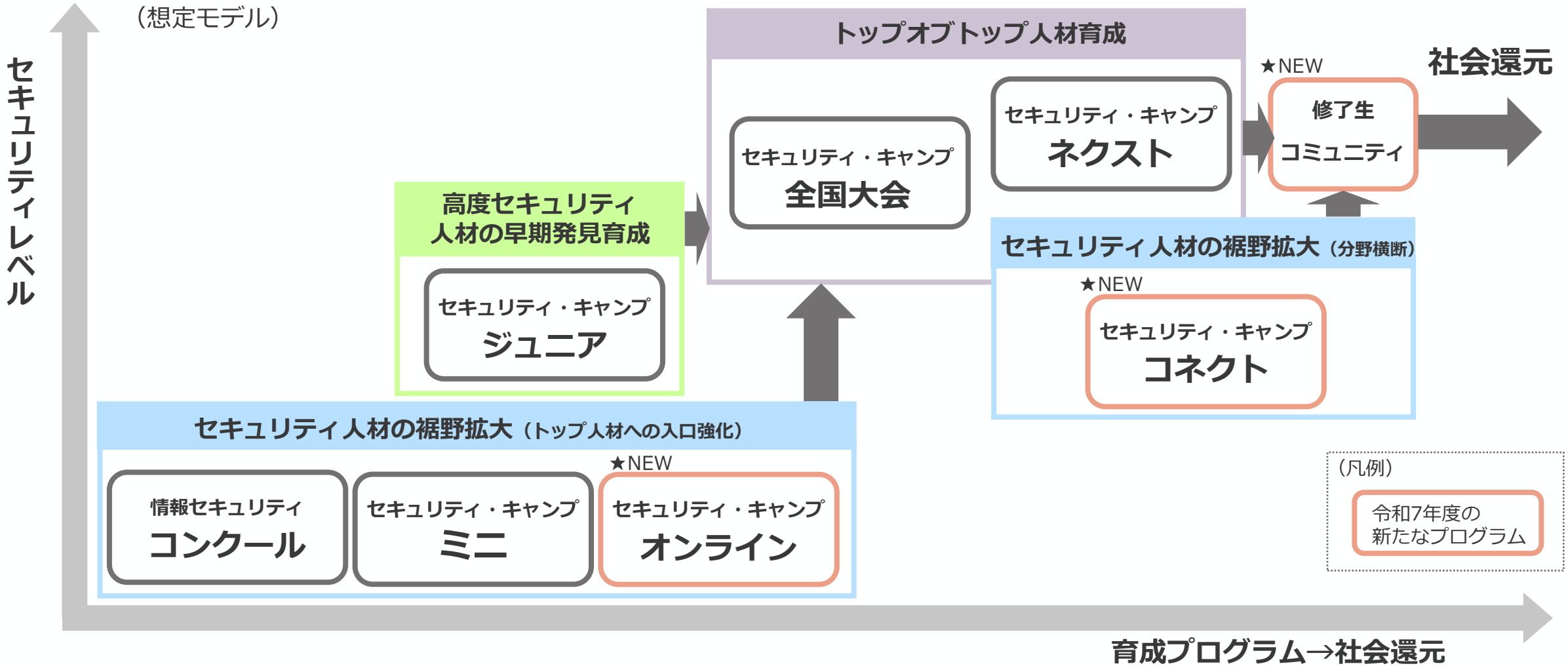
- ✓ サイバー技術形成・人材育成・プラットフォーマー等の産業形成・国際競争力回復などのため試行錯誤できる環境・空間を構築し、全国の産学官組織等にスケールさせる取組の強化
- ✓ 独立国家としてのデジタル主権の確保につながるセキュアなデジタル基盤技術やアプリケーション等の内製開発・運用の再現可能性の確立
- ✓ 国産プラットフォーマー等への発展可能性がある若手サイバー技術経営者と産学官組織とを結びつける場の創出

国際的な連携拠点

- ✓ ASEANをはじめとした海外におけるOTセキュリティの人材育成・能力向上に貢献すべく、各地域のハブとなる海外機関やキーパーソンとのネットワーキングを強化
- ✓ 海外関係機関・産業界と国内インフラ企業に所属する中核人材育成プログラム受講者をつなぐ橋渡し人材の育成に向け、修了者等による海外人脈相談対応、国際経験蓄積機会提供等を実施
- ✓ 米国をはじめとした各国の関係機関と教育カリキュラム等について積極的に意見交換を行い、教育の質・コンテンツに係る不断の向上、ICSCoEのプレゼンス強化を図る
- ✓ 国際ネットワークを活用したアジア太平洋地域向け演習の提供等を通じた国際連携の強化

セキュリティ・キャンプ

- 産業界にも資する高度なセキュリティ人材の育成を目的としてセキュリティ・キャンプを継続的に実施。
- 近年のサイバーセキュリティ脅威の拡大に対応すべく、人材の裾野拡大に向け、令和7年度は、新たなプログラムを導入するとともに、修了生支援の検討を実施。

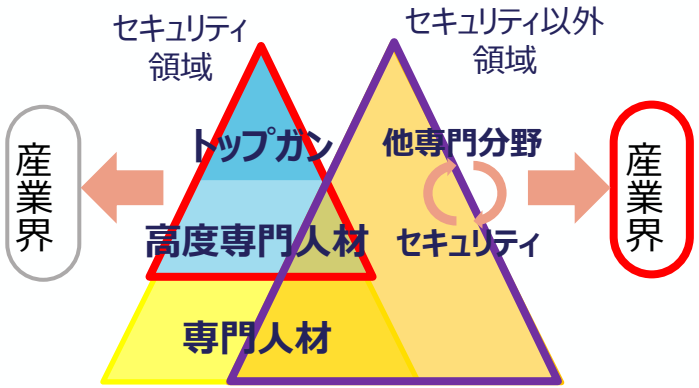


セキュリティ・キャンプ　コネクト実施状況

- サイバーセキュリティの脅威の拡大により、**あらゆる領域**の人材においてもセキュリティを学ぶ必要性が高まっている。また、全国大会では応募者増に対し講師不足から参加枠が横ばいとなっており、受入れ拡大が難しい状況。
- そこで、2025年度より、**セキュリティと他分野の専門性を併せ持つ人材を育成する新プログラム「セキュリティ・キャンプ コネクト」**を実施。2025年度はプレ開催、本開催を実施し、合計52名が参加。

セキュリティ・キャンプ コネクトの目的

✓ セキュリティと他分野を掛け合わせ、**多面的な視点からセキュリティを検討できる人材を育成し、社会で活躍できる人材を輩出する。**



参考：AI×セキュリティ

✓ AIに触れる学生を対象に、**AI技術に内在するセキュリティ課題を体系的に学ぶ**カリキュラム

参考：法律×セキュリティ

✓ 法律を専攻している学生を対象に、**サイバーセキュリティに強い法律家を目指す学生向け**カリキュラム

本開催

✓ 2026年3月26日～ 29日に実施。
✓ テーマは以下の6つ
　法律：サイバー関連の法律課題
　AI：AI技術に内在するセキュリティ課題
　脅威：攻撃者視点での脅威情報収集
　デバイス/OS/IoT：各製品開発におけるセキュリティ課題

✓ 本開催より、クラス横断型のカリキュラム「**コネクトワーク**」を導入。多種多様な分野の受講生同士の交流を通じて、新たな視点からセキュリティ課題を検討。

2026年度以降の取組

✓ 受講生からのフィードバックや時流・産業界のニーズに応じて、**カリキュラムは毎年検討を行う**ことを想定。
✓ 本年度は応募が高倍率となり受入れ可能数を超過したため、受講生の**支援対象の拡大に向けた運用改善**等も検討予定。

セキュリティ・キャンプ　修了生コミュニティ

- **セキュリティ・キャンプ修了生の更なる成長やキャリア形成、習得した知見の社会還元及びセキュリティ人材のキャリアの魅力発信を支援**するため、**修了生や講師等のネットワークを形成・維持**し、お互いを高め合える場として、修了生のコミュニティを整備。

修了生の交流活動

✓ 修了生や講師等との年度を超えた交流の場の提供と、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の提供を目的として、**「キャンプフォーラム」**を継続的に実施。
（直近では2026年２月に実施）

（過年度の開催状況）

修了生コミュニティ立上げに向けて

✓ 交流の入り口となる基盤整備として、**公式SNSプラットフォームの運用をスタート**（2026年３月に開始）。

✓ 運用開始後の支援策について、以下３つのコンセプトを基に、修了生に対するアンケートも踏まえ、具体化に向けた検討を実施。

知見の蓄積・深化	修了生の継続的な学び、最新技術や研究成果の共有等の機会を提供し専門性を高める
活動状況の共有	修了生同士が相互に知見、修了後の活動状況等を共有・公開し、セキュリティ人材としての価値を高める
知見の社会還元	講師等としてのキャンプへの参画や政府機関・組織等の活動への協力等を通じた知見・技能の社会還元

令和８年度以降の取組

■ 公式SNSプラットフォームの運用開始を契機として、**コミュニティに参加しやすい環境を整備**

➢ オンラインのLT大会・キャリア相談会、イベント紹介並びに公式SNSによる宣伝など

■ **修了生のキャリア支援と可視化並びに技術支援の強化、キャリアの魅力発信、交流の深化**などによる活性化

➢ ワークショップの実施、インターン・社会見学（未踏発企業など）の情報提供、修了生のキャリアの把握並びに外部イベントへの出展による地方在住の修了生の取り込みなど

■ **持続可能な体制の確立、社会貢献**を見据えた**コミュニティの推進・拡張**

➢ 企業・省庁・大学等とのコラボイベント実施や、修了生が自ら企画し運営できるよう、修了生を運営メンバーに組み入れの検討など

情報処理安全確保支援士（登録セキスペ）制度

- サイバーセキュリティの確保を支援するため、**セキュリティに係る専門的な知識・技能を備えた国家資格**として、**「情報処理安全確保支援士」（通称：登録セキスペ）制度**を平成28年に創設（根拠法：情報処理の促進に関する法律）。
- 国家試験に合格後（※）、IPAに登録することにより資格を取得。 **登録資格は3年ごとに更新**（定期的な講習受講が義務付け）が必要。**登録者数は26,453人**（令和８年４月１日時点）。
- 登録セキスペには、①経営課題への対応（リスク評価、セキュリティ対策、監査）、②システム等の設計・開発（設計段階からのセキュリティ対策）、③運用・保守、④緊急対応等の幅広い業務での活躍が期待されている。

※試験合格者に加えて、国が指定するポストやプログラムに従事した者も登録セキスペとなる資格を有する。

登録セキスペのメリット

＜取得者のメリット＞

①情報セキュリティに関する高度な知識・技能を保有する証

②継続的・効果的な自己研鑽が可能

③就業機会・業務範囲の拡大（※１）

※1 PCI DSS監査人の資格要件、情報セキュリティ監査人資格の取得の優遇、中小企業支援とのマッチング機会等

＜組織･企業へのメリット＞

①提供する機能やサービスへの信頼の向上

②社会的評価・信頼の向上（※２）

③ビジネスチャンスの拡大（※３）

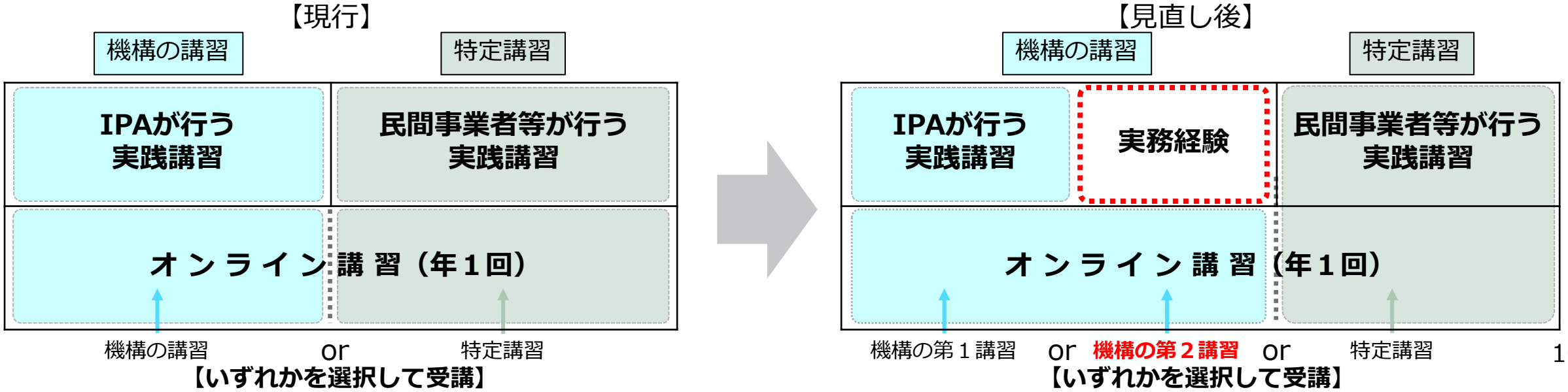
※2 知識・技能の証明に加えて、資格保有者は信用失墜行為の禁止や秘密保持の義務有する

※3 各種補助金、「デジタルガバナンスコード」（DX銘柄やDX認定基準）、サプライチェーン評価制度での活用等を推進

登録セキスペ　実務経験者向け実践講習制度の導入

- **情報処理安全確保支援士（登録セキスペ）には、サイバーセキュリティの専門家としてその知識や技能を最新の状態としておくために、講習受講が課せられている。**
- 一方、情報処理安全確保支援士の中には、**実践講習で得られる知識・技能と同等以上の知識・技能を、企業のサイバーセキュリティ対策の支援等の実務を通じて得られるケース**がある。
- また、更新制度が実施されている中で、**実務から遠のいている情報処理安全確保支援士を実務に向かわせるインセンティブを設定**することが、情報処理安全確保支援士の一層の活用促進、ひいては事業者のサイバーセキュリティ対策向上に資する。

このような講習制度や情報処理安全確保支援士の実務の実態を踏まえ、**実務経験から、講習から習得できる知識・技能と同等以上の知識・技能を得ている情報処理安全確保支援士に対して、受講すべき講習をオンライン講習のみとする、新たな講習制度を創設。（当該講習制度の申請受付は、令和８年４月１日から開始。）**



登録セキスペの活用を促進するための施策

- セキュリティ専門人材の増加を図るため、登録セキスペ制度のプレゼンス向上と登録セキスペの活躍機会拡大に向け、**セキュリティ対策促進制度等との連動を推進**する。

DX施策との連動

- 企業のDX推進に関連する各種文書に登録セキスペの活用・配置の紐づけを推進。
- 取組例として、「デジタルガバナンス・コード」（DX銘柄やDX認定の基準）や「中堅・中小企業等向けDX推進の手引き」に登録セキスペの活用を明記（令和7年3月）。

各種投資促進施策における要件化

- 経済産業省の各種補助施策において登録セキスペの配置要件化を進め、投資を通じた事業の毀損リスクを低減するために必要なサイバーセキュリティ対策を推進する人材として、登録セキスペの活用を促進。
- 取組例として、「令和６年度補正予算グローバルサウス未来志向型共創等事業費補助金」や「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律による補助」において、登録セキスペの配置を要件化。

公的機関・重要インフラ事業者等における配置促進

- 政府機関、地方自治体などの公的機関、重要インフラ事業者の内部における配置のみならず、それらの組織の委託先における配置まで含めた、登録セキスペの活用を推進。
- 取組例として、総務省において新たに作成された「（自治体DX全体手順書・別冊）デジタル人材の育成ガイドブック（令和６年12月策定）」において、デジタル人材が取得することが想定されるIT関連資格として、登録セキスペを明記。また、令和７年11月頃にNCO主催の全分野一斉演習の参加企業等に対して、登録セキスペ制度の紹介及び活用策について周知。

６．政府全体の動向

サイバー対処能力強化法及び同整備法の全体像

- 国家安全保障戦略（令和4年12月16日閣議決定）では、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、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISC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。
- これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和6年6月7日から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を開催し、同年11月29日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に**「サイバー対処能力強化法案」及び「同整備法案」**を閣議決定。国会での審議・修正を経て、**同年5月16日に成立、同月23日に公布**。

概　要

総　則
- 目的規定、基本方針等（第１章）

官民連携（強化法）
- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告

  （第２章）
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用（強化法）
- 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（第３章）
- （同意によらない）通信情報の取得（第４章、第６章）
- 自動的な方法による機械的情報の選別の実施（第22条、第35条）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の取扱制限（第５章）
- 独立機関による事前審査・継続的検査 等（第10章）

→ 分析情報・脆弱性情報の提供等（第８章）←

アクセス・無害化措置（整備法）
- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等（警察官職務執行法改正）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

組織・体制整備等（整備法）
- サイバーセキュリティ戦略本部の改組、機能強化（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設（内閣法改正）　等

施行期日　公布の日（令和7年5月23日）から起算して1年6月を超えない範囲内において政令で定める日　等

サイバーセキュリティ戦略（2025年12月23日閣議決定）

○ **「国家安全保障戦略」**及び**サイバー対処能力強化法等**に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、**今後５年の期間を念頭に、**実施すべき諸施策の目標や実施方針を内外に示す。

基本的な考え方

○ サイバー空間は、経済社会の持続的な発展、自由主義、民主主義、文化発展を支える基盤。

○ 法の支配、基本的人権の尊重といった普遍的価値に基づく国際秩序が深刻な危機にさらされ、サイバー脅威による国民生活・経済活動、ひいては国家安全保障上の懸念が高まっている。

「５つの原則」※を、引き続き「基本原則」として堅持した上で、国がこれまで以上に積極的な役割を果たすことで、厳しさを増すサイバー空間情勢に対応すべく施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することを明確化

（※施策の立案・実施原則となる「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」）

情勢認識

- 厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大
- 社会全体のデジタル化の進展とサイバー脅威の増大
- AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

施策の方向性

1 深刻化するサイバー脅威に対する防御・抑止

- 厳しいサイバー安全保障環境に対応するため、官民連携・国際連携の下、事案対処等の従来の施策に能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、脅威を防御・抑止
- 政府から民間への積極的な情報提供

国が要となる防御・抑止

官民連携エコシステムの形成

国際連携の推進・強化

2 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

- 様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施（政府機関等が範となり対策）
- デジタル化とセキュリティ確保の同時推進

政府機関等の対策強化

重要ｲﾝﾌﾗ事業者・地方公共団体等の対策強化

サプライチェーン全体のﾚｼﾞﾘｴﾝｽ確保（中小企業・ベンダー等）

全員参加によるサイバーセキュリティ向上

ｻｲﾊﾞｰ犯罪対策を通じた安全・安心の確保

3 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

・産学官を通じたサイバー人材の確保・育成
・国産を核とした、新技術・サービスの創出

効率的・効果的な人材の育成・確保

新たな技術・サービスのエコシステム形成

先端技術(AI、量子技術等)への対応・取組

官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靭さを持つ国家を目指す。

日本成長戦略会議 デジタル・サイバーセキュリティWG

- 日本成長戦略本部において戦略分野の一つとして指定された「デジタル・サイバーセキュリティ」分野の現状と課題等について議論するための場として、**デジタル・サイバーセキュリティWG**を開催。
- 2026年４月頃に「**官民投資ロードマップ**」（官民投資の促進策）の案を**取りまとめる**予定。

設置趣旨

- リスクや社会課題に対し、先手を打った**官民連携の戦略的投資を促進**し、世界共通の課題解決に資する製品、サービス及びインフラを提供することにより、**更なる我が国経済の成長を実現**する必要。
- 日本成長戦略会議の各WGのうち、**情報化・情報産業に関するWGの1つ**として、「デジタル・サイバーセキュリティWG」を設置。
- 本会議を含む各WGで策定された**官民投資のロードマップを取りまとめ、「日本成長戦略」を策定**する。

スケジュール

2026年

- **２月　デジタル・サイバーセキュリティWGの設置**
  第１回開催
  - 足元のデジタル・サイバーセキュリティ政策の現状の整理
  - 戦略投資の促進に向けた供給力強化/需要創出・拡大に向けた政策の多角的な検討
- **４月　第２回開催**
  - 戦略・ロードマップ案の取りまとめ

検討体制（敬称略）

【WG長】　デジタル大臣、経済産業大臣
【構成員】

井口　譲二	（ニッセイアセットマネジメント株式会社執行役員）
石原　直子	（株式会社エクサウィザーズ はたらくAI＆DX研究所 所長）
岩﨑　尚子	（早稲田大学電子政府・自治体研究所研究院教授）
日下部　進	（GVE株式会社共同創業者兼アドバイザー）
志濟　聡子	（合同会社アイシスコンサルティング代表）
中谷　昇	（日本電気株式会社　執行役　Chief Security Officer）
中室　牧子	（慶応義塾大学総合政策学部教授）
東原　敏昭	（株式会社日立製作所　取締役会長 代表執行役）
村上　明子	（ＳＯＭＰＯホールディングス株式会社執行役員常務グループChief Data Officer、日本経済団体連合会デジタルエコノミー推進委員会　企画部会長）
横山　直人	（株式会社フライウィール共同創業者代表取締役CEO）
和田　隆志	（金沢大学長）

【事務局】　デジタル庁（戦略・組織G）、経済産業省（商務情報政策局）
【関係省庁】
内閣官房（デジタル行財政改革会議事務局、国家サイバー統括室）、総務省、経済産業省（製造産業局）、文部科学省、厚生労働省、警察庁、国土交通省

（参考）デジタル・サイバーセキュリティの全体像

第１回デジタル・サイバーセキュリティWG事務局資料を一部加工