経済産業省

資料３

事務局説明資料
産業サイバーセキュリティ研究会
WG１　第12回

令和８年3月10日

経済産業省　商務情報政策局

サイバーセキュリティ課

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　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

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

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

村井　純(座長)慶應義塾大学教授

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

前回いただいた主な御意見と本検討会について

- 本日、今年度の進捗を報告するとともに、今後の政策の方向性を示す。全体的に御意見いただきたい。

①セキュア・バイ・デザインの実践

- SSDFのように具体化されていることは産業界におけるセキュリティ担保の観点で喜ばしいことである。具体的に産業界へ適用する際には、既存の制度(例:JC-STAR)や規制等とのすり合わせが必要。
- SSDFについて。今後の基準策定や認証制度構築の参考となるため、実証において各組織にヒアリングを行い、SSDF導入に係る効果測定、有効性測定をしていただきたい。
- SSDFは、抽象的な粒度で要求事項を課すものと理解。解釈で揺らぎが出るおそれもあるため、SSDFについて解説するガイドラインがあるとよい。
- SBOMについて。日本の製造業では、ソフトウェアの品質管理に対する解像度が低く、SBOM導入に係る手間と効果を把握しきれていない可能性。米国では、ソフトウェアに関して、SBOMや、”BACK TO THE BUILDING BLOCKS”と題された文書で示されるものなど、解像度の高い対策が出てきている。日本はどう対処するか、掘り下げていかないといけない。そのための制度設計やインセンティブ付与が課題。
- ソフトウェアサプライチェーンについて。ソフトウェアにおいて意図しない機能やソフトウェアが混入している場合がある。把握できていない機能やソフトの混入について確認できる仕組みを構築していくべき。
- JC-STARについて。スマートホーム分野では、IoT製品の構成はダイナミックに変わるため、ガイドラインもその変化に合わせてほしい。

②サプライチェーン全体のセキュリティ対策強化

- SCS評価制度について、自動車業界としても企業としても積極的に貢献していきたい。
- 技術的なところで客観的な評価がなされ、またコストとの兼ね合いで検討されるとよい。
- 実効性を担保するために、第三者が確認する仕組みを構築されたい。
- SCS評価制度と海外制度との整合性の検討を進めていただきたい。
- 継続的に普及の取組を行うことが重要。また、ガイドラインの継続的な見直しをお願いしたい。
- サイバーインフラ事業者を経由してサプライチェーンを対象とした攻撃が増えている。SCS評価制度を強力に推進いただきたい。ただし、実効性を保つために、適切な価格転嫁を発注元が受け入れるための仕組み作りや税制優遇等を検討されたい。
- サプライチェーン対策は、同時にやらないと意味がない。普及啓発によって、同時性を追求いただきたい。

③その他

- CPSFについて。ISO/IEC TS 5689発行については2025年度内を目指していきたい。
- AIの進展に伴い、サイバーセキュリティ分野での活用が増えている。今後サイバーセキュリティ分野にAIを活用できるような施策等を検討いただきたい。また、今後全てのデバイスにAIエージェント利用が進んでいくことが考えられる。Secure by Designから進んで、Secure AI by Designを提唱する。
- AI自体のセキュリティ対策とAIを使ったセキュリティ対策の二つを切り分けて議論する必要があるため、整理していただきたい。

目次

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、情報漏えいの可能性も確認。
- 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6割以上を占める

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年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和７年９月）」を基に作成。

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の全体像

- 令和７年12月23日に閣議決定された「サイバーセキュリティ戦略」には、**中小企業を含めたサプライチェーン全体のレジリエンス確保が重要な方向性の一つ**として位置づけられている。
- 経済産業省では、本戦略に基づき、**SCS評価制度や、JC-STAR制度、ソフトウェア開発に資する施策**の構築・実行をしていく。

「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

情勢	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	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	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

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

ｻﾌﾟﾗｲﾁｪｰﾝ全体のﾚｼﾞﾘｴﾝｽ確保

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、世界最高水準の強靱さを持つ国家を目指す

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、米国防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。2023年12月に2.0版が発効。）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**。

目次

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※2を提示しつつ、その状況を可視化する仕組み※3を構築。
- 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　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。
※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（案）

成熟度の定義	★３	★４	★５［検討中※4］
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到達点として目指すべき対策： • 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

※4　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。

制度の普及施策（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
普及施策	**サイバーセキュリティお助け隊サービス（新類型）の創設**	**中小企業ガイドライン整備**	**専門家の活用促進**	**取引先への要請等に係る考え方の整理**
	★3・★4に対応した、サイバーセキュリティお助け隊サービスの新たな類型創設により、安価な”★”取得を実現	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	「中小企業向けサイバーセキュリティ専門家リスト」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の策定により、費用に係る価格交渉を推進

（参考）制度で用いるセキュリティ要求事項・評価基準の概要

- NIST Cyber Security Framework(CSF)の機能に対応した６つの分類に、取引先管理に重点を置いた分類を加えた７つの分類において、それぞれレベルごと達成すべき対策を提案。詳細は別添を参照。要求事項・評価基準は、サイバーセキュリティの動向等を踏まえ今後定期的な見直しを想定。

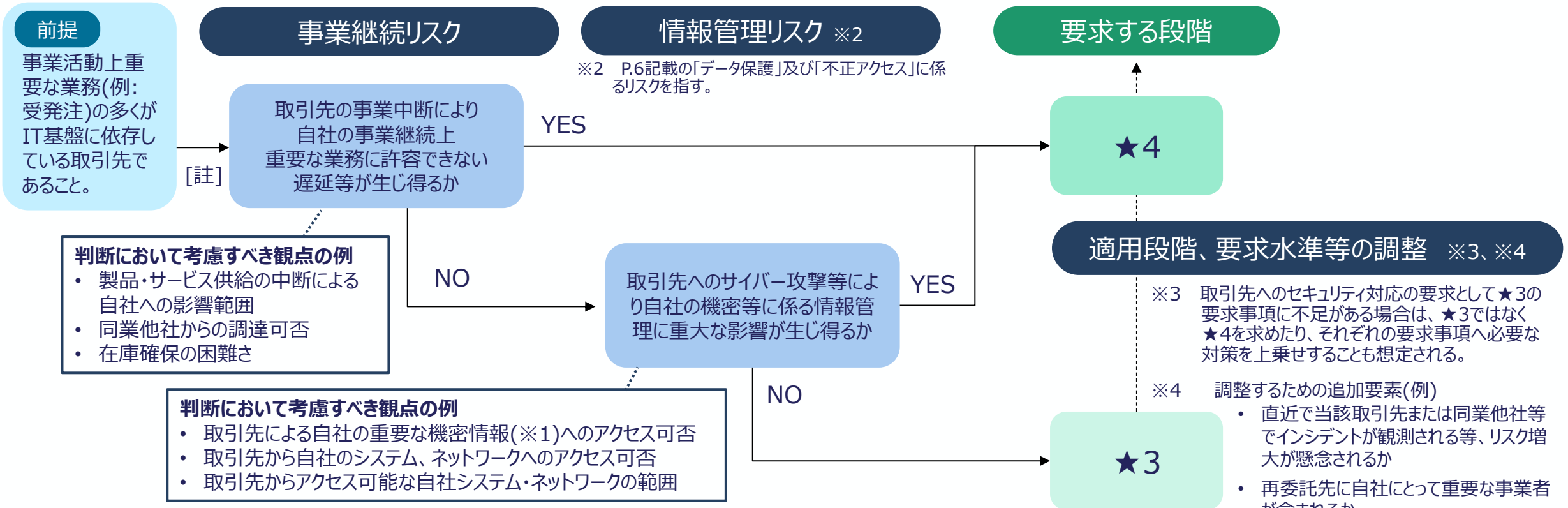
[註] 以下は必ずしも全要求事項を網羅しているわけではない点に留意されたい。　[註] []内は要求事項No.を指す

大分類	★3	★4	NIST CSFにおける機能
ガバナンスの整備	**企業として最低限のリスク管理体制の構築** • 自社のセキュリティ担当の明確化 [No.1-2-1] • セキュリティ対応方針の策定 [No.1-3-1]	**継続的改善に資するリスク管理体制の構築** • 定期的な経営層への報告、不備の是正等 [No.1-4-1]	統治(GV)
取引先管理	**取引先に課す最低限のルール明確化** • 他社との機密情報の取扱い明確化 [No.2-1-2] • 接続している外部情報サービスの把握 [No.3-1-3]	**取引先の管理・把握及び取引先との役割・責任の明確化** • 機密情報共有先の把握 [No.2-1-1] • 重要な取引先等の対策状況把握 [No.2-1-3] • インシデント発生時の他社との役割等の明確化 [No.2-1-4]	
リスクの特定	**自社IT基盤や資産の現状把握** • 情報資産やネットワークの把握 [No.3-1-1,3-1-2] • 外部情報サービスの管理 [No.3-1-3]	**脆弱性など最新状況の把握と反映** • 脆弱性管理体制、管理プロセスの明確化 [No.3-2-1]	識別(ID)
攻撃等の防御	**不正アクセスに対する基礎的な防御** • ID管理手続、アクセス権限の設定[No.4-1-1,4-1-2] • パスワードの安全な設定及び管理 [No.4-1-4,4-1-5] • 内外ネットワーク境界の分離・保護 [No.4-5-1] **端末やサーバーの基礎的な保護** • 適時のアップデート適用、不要ソフトウェアの削除[No.4-4-1,4-4-4] • 端末等へのマルウェア対策 [No.4-4-1,4-4-4]	**多層防御による侵入リスクの低減** • 重要な保管データの暗号化 [No.4-3-1,4-3-2] • ログの収集・定期的な分析の実施 [No.4-4-3] • 社内システムにおける適切なネットワーク分離 [No.4-5-1] • 社外への不正通信の遮断(出口対策) [No.4-5-2]	防御(PR)
攻撃等の検知	**ネットワーク上の基礎的な監視等** • ネットワーク接続・データの監視[No.5-1-1]	**迅速な異常の検知** • 情報機器等の状態、挙動の監視・対応や分析[No.5-1-1,5-1-2]	検知(DE)
インシデントへの対応	**インシデント発生に備えた対応手順の整備** • インシデント対応手順の作成 [No.6-1-1]	*大分類「インシデントへの対応」において、★４での追加項目はなし	対応(RS)
インシデントからの復旧	**インシデント発生から復旧するための対策の整備** • インシデント発生から復旧するための対策の整備[No.7-1-1]	**インシデントからの復旧手順等の整備** • 復旧ポイント、復旧時間を満たす手順等の整備[No.7-1-1]	復旧(RC)

（参考）制度において設ける段階　★3・★4適用の考え方(例)

- 取引先への適用に当たっては、例えば以下のように、取引先を★４又は★３の段階に割り当てたり、必要に応じて適用段階、要求水準等を調整することが考えられる。

■　★3・★4適用の考え方(例)

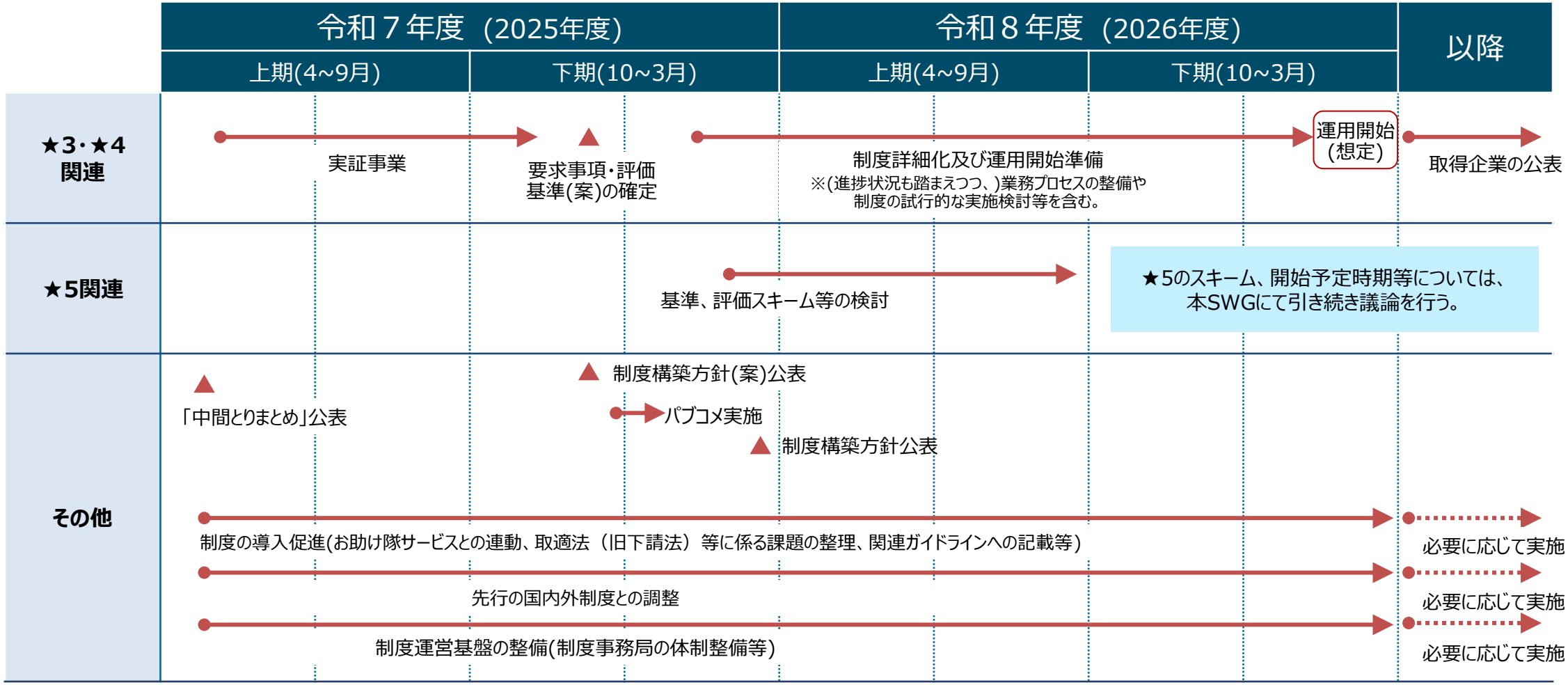


※１　当該情報を漏洩した場合における、社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響が大きいもの

[註]　単発・一過性の調達や、市販品など市場で容易に代替可能な製品・サービスの調達等のうち、重要度が相対的に高いとは言えないものについては、本フローの対象から外すことも考えられる。

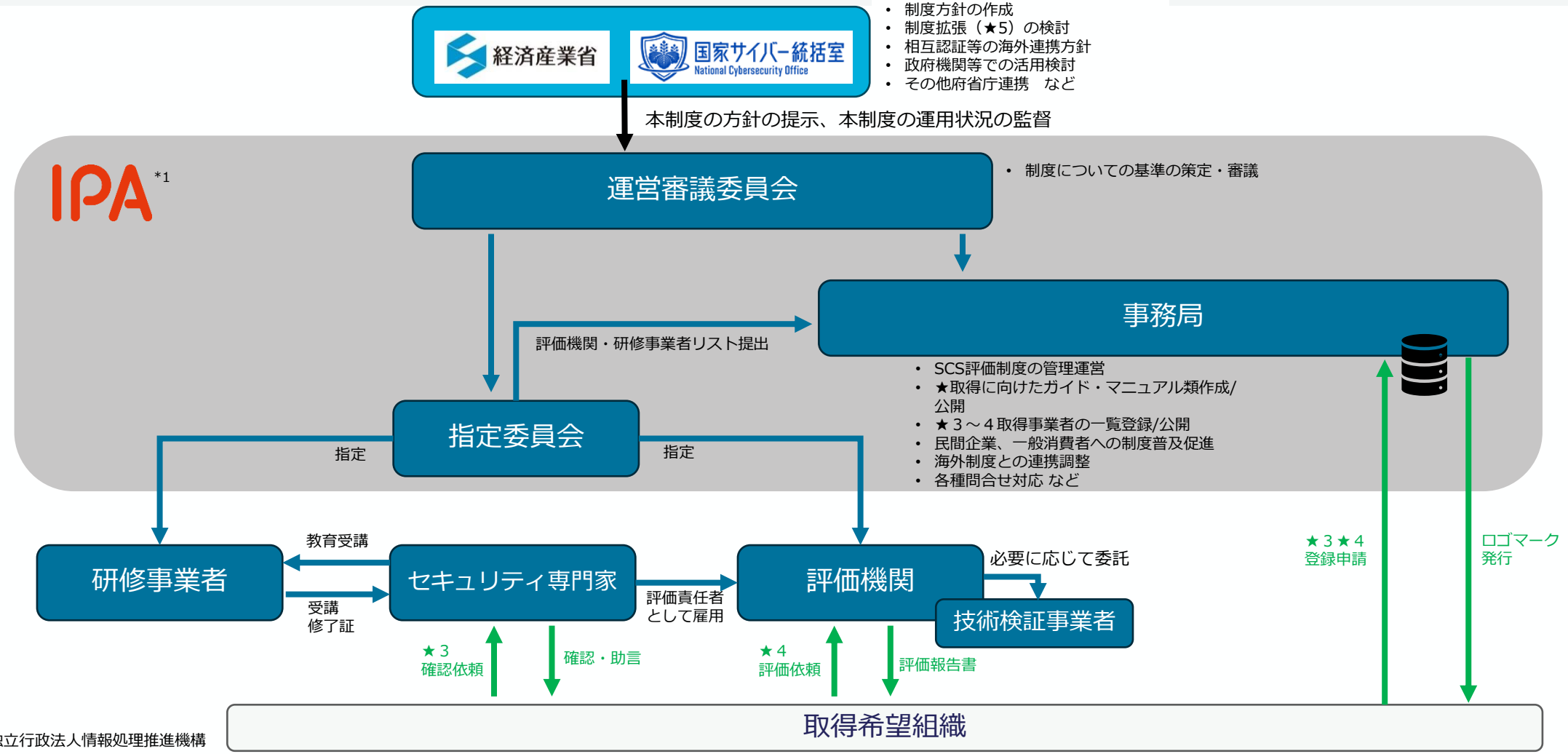
SCS評価制度に係る今後のスケジュール

- **令和８年度末頃の制度開始を目指し**、制度運営基盤の整備や利用促進等を進めていく。
- **制度開始５年後（R.13）までに２万件、10年後（R.18）までに５万件の★取得者を目指す。**



制度の運用体制案

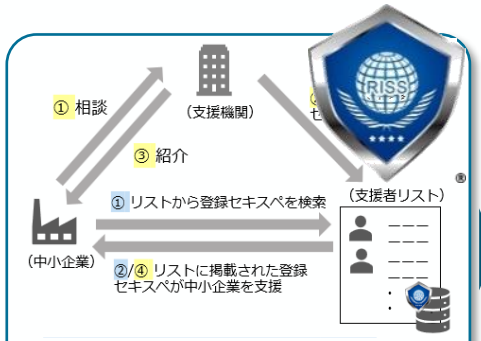
- 基本的な規則を維持管理するスキームオーナーには、社会全体への制度浸透や諸外国の制度との連携を今後調整していくことから、政府のガバナンスが効くことが重要となる。また、任意制度を新しく立上げ普及させるには高いハードルがある。こうした点を踏まえ、経済産業省の示す本方針に従い制度を構築し、同省の監督のもと制度を運営するスキームオーナーは、同省が所管官庁である独立行政法人情報処理推進機構（IPA）とする。



*1　IPA：独立行政法人情報処理推進機構

（参考）SCS評価制度を中心とした中小企業支援策の新たな体系

- 中小企業に対し、**SCS評価制度★３・★４水準のセキュリティ対策実施を後押しする**ため、各種施策を展開していく。



★3～4実装のための
人的支援
（登録セキスペとのマッチング）

★3～4取得にむけた
きっかけ作り
（補助施策と連動）

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）

成熟度の定義	★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到達点として目指すべき対策： • 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

★3～4を安価に
実現する
“all-in-one”
サービスの提供

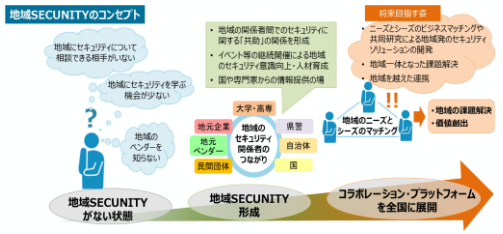
★3～4取得に
つながる
実践方策＋
規程類ひな形

パートナーシップ構築宣言

サイバー対策要請時の、
関係法令の適用関係明確化

支援機関等と連携した
面的な普及展開活動

【地域SECUNITY】



（参考）サイバーセキュリティお助け隊サービス（新類型）について

- 中小企業向けの支援策として、**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（SCS評価制度）の★3・★4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）**を創設する。具体的には、★3・★4の要件項目のうち未達成の項目について、サイバーセキュリティお助け隊サービス（新類型）の導入により要件項目を達成させるものとする。
- 今後、**実証事業を通じて、**令和８年(2026年)度末頃のSCS評価制度開始にあわせて、サイバーセキュリティお助け隊サービス（新類型）の**基準案を公表し、先行版としてサービスイン**する予定。

サイバーセキュリティお助け隊サービス（新類型）のイメージ

STEP1：課題の可視化

SCS評価制度
★3・★4の
取得及び更新時
に各要件項目の
対応状況を診断

STEP２：対象サービスの選定と対応実施

診断結果に基づき、以下の支援を実施

✓ITツールによる支援
★３・★４取得に推奨されるITツールを導入

✓ITツール以外の支援
セキュリティポリシーやインシデント手順書の整備、セキュリティ教育など、中小企業が自助努力で達成しづらい項目を支援

【サービス例】

SCS★４＋	★４要件に駆付け支援がプラスされたサービス
SCS★４	★４要件を最低限満たすサービス
SCS★３＋	★３要件に駆付け支援がプラスされたサービス
SCS★３	★３要件を最低限満たすサービス

STEP1・STEP2の支援サービスを一定の価格要件の下で提供

STEP3：★取得

SCS評価制度
の★3・★4の
項目要件をすべて充足することで“★”を取得

（参考）サイバーセキュリティお助け隊サービス（新類型）実証事業

- 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、**全国十数社程度のITベンダーに実証事業に参加いただき、顧客である中小企業にサービスを提供しながら、技術要件・価格要件を検証**する実証事業を実施する（令和８年８月頃から令和９年９月頃までの１年間を予定。）。
- 実証の結果を踏まえ、令和９年３月頃までに、**価格要件を含むサービス基準の制度化**につなげる。

実証で検証すること（ITベンダー向け）

中小企業へのサービス提供を通じて以下の項目を検証

1. セキュリティ要求に対応できる**技術要件（サービスの内容・品質等）**を検証
2. サービス導入が継続的に可能な**価格要件**を検証

実証を通して、**ITベンダー・中小企業の双方にとってメリットのあるサービス**を創設する

中小企業の実証参加メリット

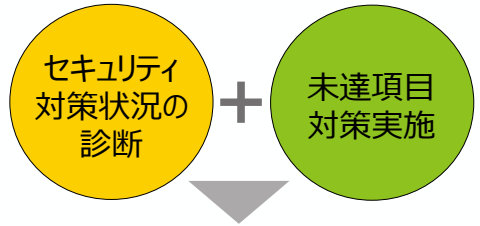
1. **組織的対策を含むセキュリティ対策を無料**で実施（実証期間中最大1年程度）
2. SCS評価制度の“★”**取得**が可能（SCS評価制度開始後の“★”取得要請への備えが可能）
3. サプライチェーン全体での対策強化に取り組む企業として、**取引先との信頼性向上**に繋がる

（参考）サイバーセキュリティお助け隊サービス　既存類型と新類型のサービス内容

既存類型 セキュリティ対策に不安のある中小企業に向けて、**最低限必要なセキュリティ対策**を安価に提供（令和7年9月末時点で9,200件の導入実績有り）

ワンパッケージで安価に提供

新類型 **SCS評価制度の★３・４取得を目指す中小企業**に向けて、セキュリティ対策状況を**診断**し、未達成項目が全て達成されるまで**伴走支援**するサービス



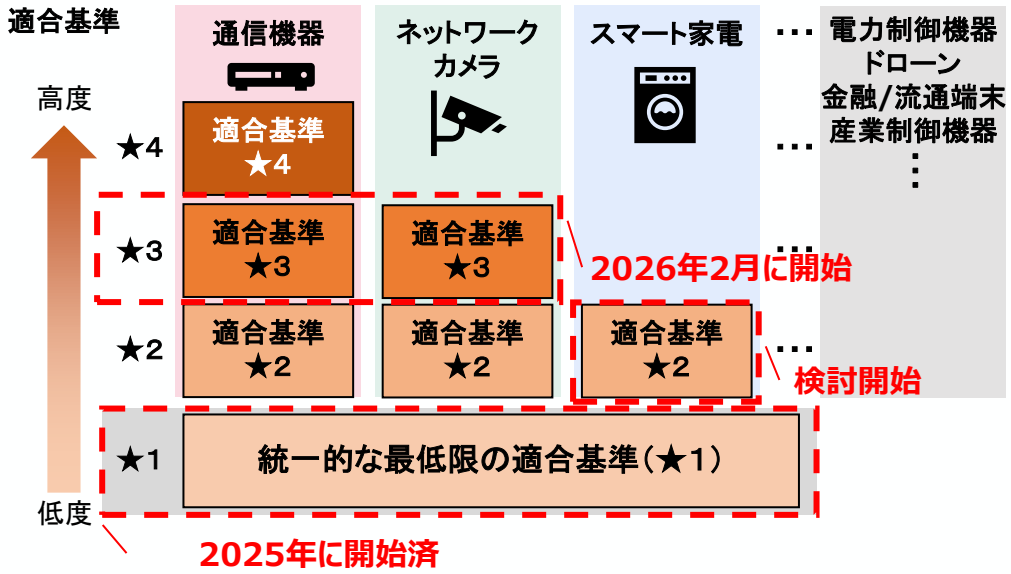
SCS評価制度の“★“取得

目次

IoTセキュリティラベリング制度（JC-STAR）の制度構築・普及状況

- １段階目（★１）について、2025年３月から申請の受付を開始し、５月より★１ラベルの「適合ラベル取得製品リスト」を公開。**2026年2月より通信機器・ネットワークカメラの★３の適合基準を公開**し申請の受付を開始予定。また、**2026年1月よりスマートホームの★２の適合基準について、IPA内のWGでの議論を開始。**
  - ★３の開始に合わせ、製品評価技術基盤機構認定制度(ASNITE)内に設置した**JC-STAR評価期間認定制度についても運用開始**
  - 上述した類型以外に、**電力制御機器・ドローン・金融/流通端末・産業制御機器等の類型についても順次基準策定予定**
- 2026年1月時点で**約150の申請（製品型番ベースで1,000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**。

制度構築状況



主なラベル取得済み製品

IoTセキュリティラベリング制度（JC-STAR）の活用状況

- 2025年3月に**「地方公共団体向けセキュリティガイドライン」へJC-STAR制度の活用に関する記載が反映**された。また、 2025年9月に**「政府機関等の対策基準策定のためのガイドライン」が改正**され、**IoT機器等の調達においてJC-STARの取得を選定基準に含める旨追記**された。
  - 民間が主管するガイドライン等を含む、下記以外の基準・ガイドライン等における必須化・活用促進等についても引き続き追求
- **系統用蓄電池補助金、長期脱炭素電源オークション、系統連系技術要件等、他制度におけるJC-STAR制度の要件化も拡大**。ラベル取得のインセンティブを拡大すべく引き続き活用を推奨。引き続き、政府調達における将来的な必須化や、政府機関等や重要インフラ事業者における**当制度活用の要件化等に向けて、関係機関等と議論を継続**する予定。

他制度におけるJC-STARの活用状況

	JC-STARを活用している制度等	当該制度等における主な対象製品
基準・ガイドライン等における制度活用促進	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	通信機器・ネットワークカメラ・ドローン等
	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	通信機器・ネットワークカメラ・ドローン等
補助金制度等におけるラベル取得の要件化	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	系統用蓄電池において利用される電力制御機器（BMS、PCS、EMS 等）
	長期脱炭素電源オークション	系統用蓄電池において利用される電力制御機器（BMS、PCS、EMS 等）
	系統連系技術要件（グリッドコード）	分散型電源が採用する通信機能を有する制御システム（PCS、EMS等）
	DR家庭用・業務産業用蓄電池補助金	家庭用蓄電池において利用される電力制御機器（BMS、PCS、EMS 等）

IoT機器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）は、IoT製品ベンダーの負担を軽減するため、IoT機器を対象とするサイバーセキュリティ評価制度の制度調和を通じた取組として、日本のJC-STARと英国のPSTI法に関し、相互承認する旨の覚書へ署名し、2026年1月、両制度間で**相互承認制度**が開始。

- 本制度では、**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、**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。**

- 2025年、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製品セキュリティ評価制度への国際的な関心が高まった。**類似の制度を有するシンガポール、米国、EU、ドイツ等を中心に制度間の協調を引き続き追求予定。**

日英 IoTセキュリティ評価制度比較

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：2025年度第4四半期以降開始予定	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

免除される適合要件及び手続

＜適合要件＞

JC-STAR（星１）	PSTI法（2023年施工令）
• 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。

英国以外の主な諸外国の類似制度

国・地域	シンガポール	米国	EU
制度名	Cybersecurity Labelling Scheme (CLS)	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA)
マーク	CYBERSECURITY LABEL CSA/IOTWABCD	U.S. CYBER TRUST MARK	CE
開始時期	2020年10月制度開始	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
任意/義務	任意	任意	義務
対象	消費者向けIoT機器	消費者用無線IoT製品	デジタル要素を含む製品

SSDFの活用促進に向けた取組について

- 近年、ソフトウェアの脆弱性が企業経営に大きな影響を及ぼす等、ソフトウェアに対するセキュリティ脅威が増大していることを背景に、2023年に**ソフトウェアに関するQUAD共通原則が発表。当該原則の履行（SWの開発・利用・政府調達に関するセキュリティのガイドラインを各国が定めること）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（SP800-218）」を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策定**するとともに、**実効性を強化することが重要**。
- 2025年度は、産業分野毎の実態に即した効果的なSSDF導入・実践等を目的に調査・実証を行い、**ガイダンス案の拡充・成案化などSSDF導入促進に向けた取組を実施**。成果物は、SP800-218の改訂をふまえ2026年中に公開予定。
- 2026年度は、**AIコーディング等における脆弱性の混入や、開発環境に起因した機微情報の漏洩リスクを含む、ゼロトラストを前提とした組織内の開発環境防御のために必要な取組（AI駆動開発に係るセキュリティを含む）を検討**する。

2024年度の取組（成果物）

- **SSDF導入ガイダンス案（中間整理）**
  - ✓ SSDFの概要と導入意義/メリット/考え方/プロセスを整理
  - ✓ SSDFタスク達成Lv.と具体的な実践策、既存の国内ガイドラインのマップしたタスクシートも併せて作成　等

2025年度の取組

調査・実証を踏まえたガイダンスの拡充を実施

① ツール等を活用した効率的な導入・実践策
② 分野特性に応じた活用策
③ 達成プラクティスレベルの段階数の見直し検討
④ タスクを実施しないことのリスクの明確化
⑤ 国内ガイドラインの不足事項への対応策の作成
⑥ 自己チェックリストの検討・案の作成

2026年度の取組（案）

ゼロトラスト・セキュア開発環境に係る検討（AI駆動開発に係るセキュリティを含む）

- **課題：**開発環境そのものが標的となり、サプライチェーンへ波及するリスクが顕在化。また、AIコーディングなどAI駆動開発において脆弱性の混入、機微情報の漏洩リスクを指摘する声が増加。
- **取組案：ゼロトラストを前提とした組織内の開発環境防御のために必要な取組（AI駆動開発に係るセキュリティを含む）**

（参考）SSDF導入ガイダンス（案）について

- 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の改訂をふまえ、成案化予定。

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

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

<共同署名の参加国>
日本、アメリカ、ドイツ、フランス、イタリア、オランダ、カナダ、オーストラリア、ニュージーランド、インド、シンガポール、韓国、ポーランド、チェコ及びスロバキア

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

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来年度作成予定。（詳細はP.30）
- 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来年度実施予定。

NEDO Challenge

<応募技術の例>
・SBOM情報を常に最新に保つ技術
・全てのコンポーネントを網羅的かつ正確に記述できる技術
・参照脆弱性データベースが異なっても脆弱性が検知できる技術

サイバーインフラ事業者と顧客に求められる責務について

- 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**、および**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、**ガイドラインを成案化**すると共に、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の整備**を行った。（パブリックコメントを踏まえて修正したガイドラインは３月に公表予定。）

指針（案）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

（参考）サイバーインフラ事業者のセキュリティ対応強化に向けた支援策について

- 「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」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。

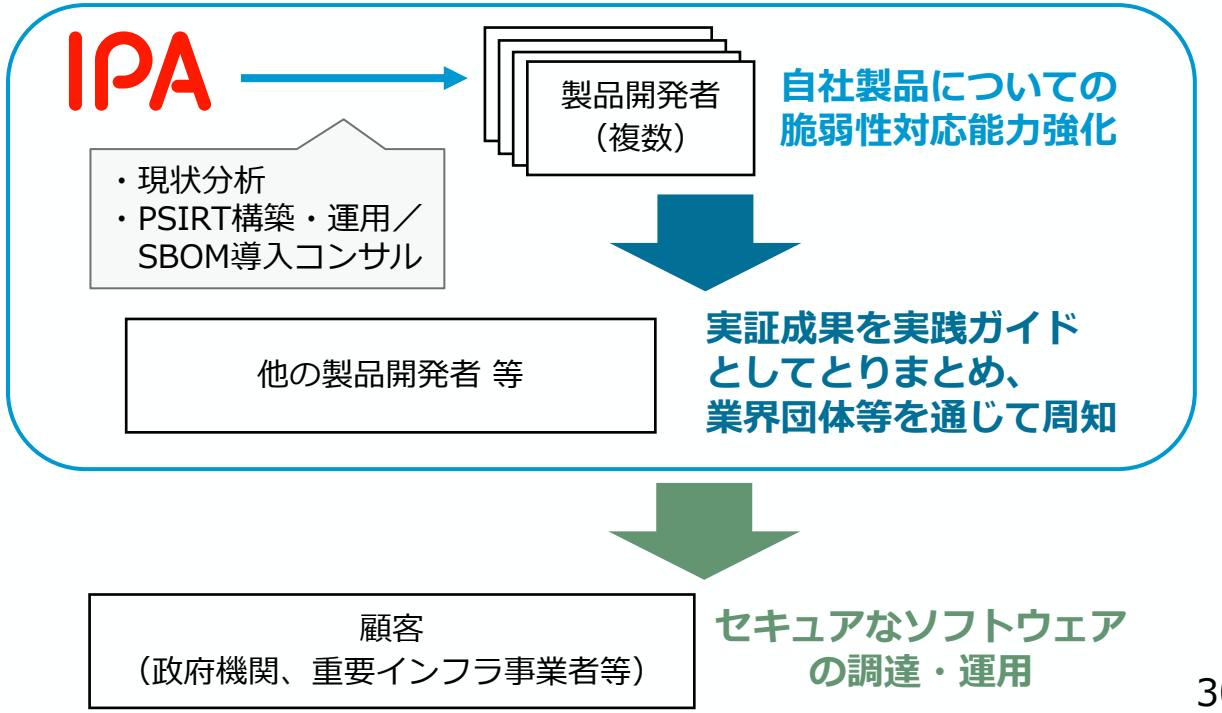
PSIRTの構築・運用及びSBOMの導入支援

- 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>



目次

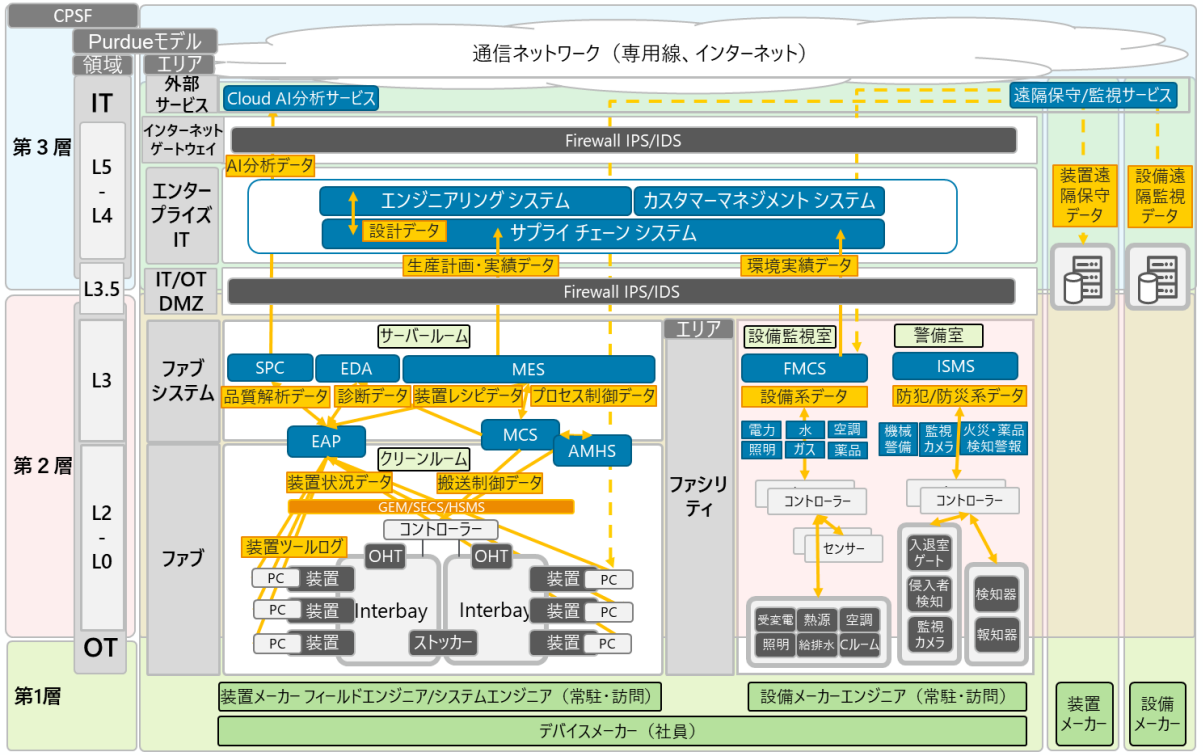
半導体関連産業のセキュリティ対策水準の強化

- 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念頭に置きつつ、**半導体工場において求められるセキュリティ対策**に向けた検討を実施し、2025年10月**「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」を公表**。
- 2026年1月**「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。**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行っていく予定。2026年度は、**「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**に向けて検討を進めていく。

半導体デバイス工場におけるOTガイドライン

- 海外では、半導体業界団体であるSEMIにより、半導体製造装置に係るE187/E188規格が策定され、米国立標準技術研究所（NIST）においてもCybersecurity Framework 2.0の半導体製造プロファイルの策定が進展。
- 本ガイドラインはこうした国際的な規格とも整合しつつ、生産目標の維持・機密情報保護・半導体品質の維持のための工場セキュリティ対策の指針として策定。
- 半導体デバイス工場のリファレンスアーキテクチャに基づき、リスク対策フレームワーク（CPSF及びNIST CSF2.0）を活用し、半導体デバイス工場の特徴を踏まえたリスク源（脅威、脆弱性）の洗い出しを行うとともに、対応するセキュリティ対策項目について取りまとめ。

半導体デバイス工場のリファレンスアーキテクチャ

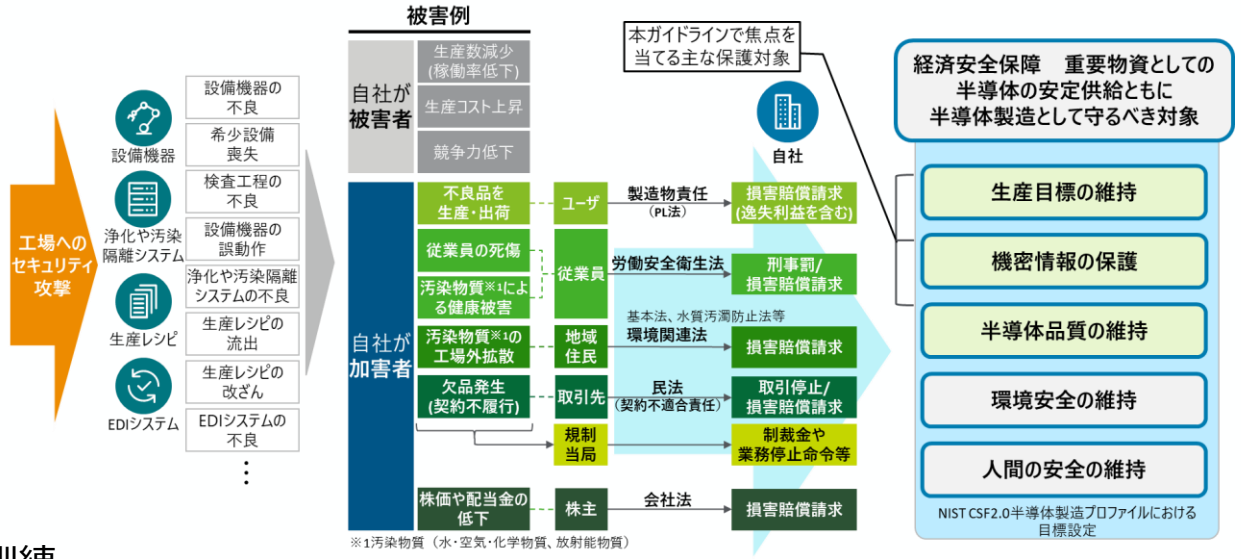


「半導体デバイス工場におけるOTセキュリティガイドライン」の改版

- 半導体デバイス工場におけるファシリティエリアへのサイバー攻撃は、**工場稼働停止を引き起こす可能性があり**、クリーンルームの再セットアップや設備の再稼働に多大な時間とコストが必要となることから、**影響は大きい。**化学薬品やガスなどの危険物を扱うため、リスクも高い。
- さらに、ファシリティエリアは**サイバー攻撃に対する対策が十分に施されていない**場合が多い。
- これらの背景を踏まえ、2026年度は「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」において、**ファシリティエリアへのセキュリティ対策の追記**に向けて、検討を進めていく。

ファシリティエリアに関する想定論点

- **管理とガバナンス**
  - 資産・構成把握と責任主体の明確化
  - 事業影響評価と経営課題としての認識
  - サプライチェーンにおける責任分界点の定義
- **技術的対策**
  - レガシーシステムに対する現実的な防御策の検討
  - 物理的な侵入経路に対する技術的制御の導入
  - 侵入・異常検知の仕組みと運用体制の構築
- **運用とインシデント対応**
  - サイバー攻撃を想定した事業継続計画（BCP）の策定と訓練
  - インシデント対応における連携体制の強化
  - 現場に即した実践的なセキュリティ教育・訓練の推進



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）の国際標準化と改訂

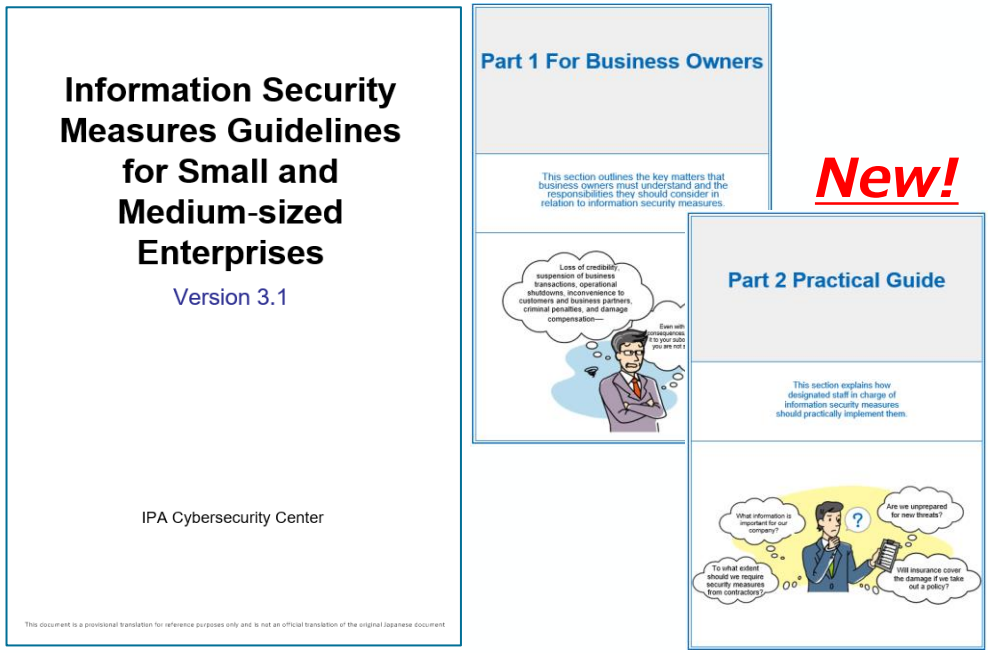
- ISO/IECにてCPSFモデルを盛り込んだ国際規格の策定を推進中。（ISO/IEC JTC1/SC27 TS 5689プロジェクト※）。2025年3月の国際会合にて承認段階となる。**2026年夏頃までに発行を目指す。**
- 2019年のCPSF ver1.0策定から6年が経過し、国内外のセキュリティ情勢は大きく変化している。他国の**サイバーセキュリティ国際規格（NIST CSF2.0等） の更新等の変化を踏まえ、CPSFの改訂作業を引き続き実施**する。

※ ： https://www.iso.org/standard/87375.html

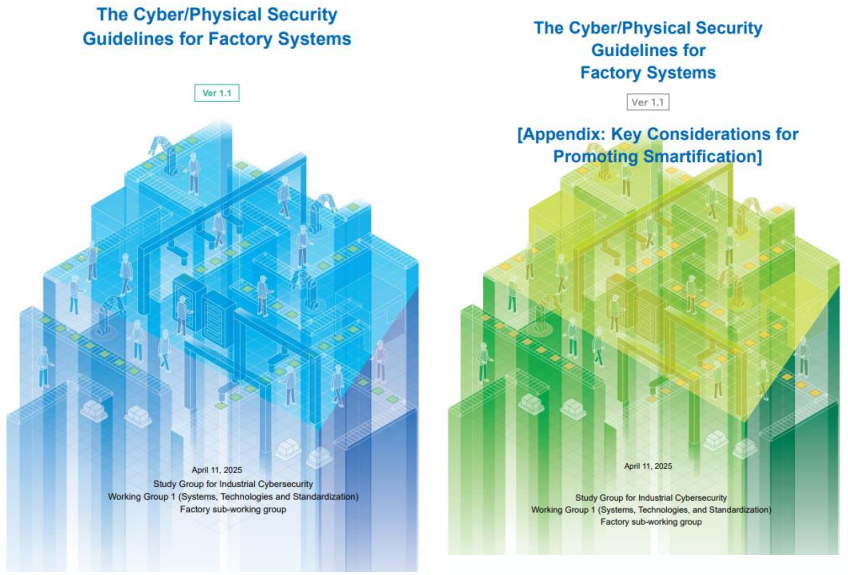
テーマ	直近の実績	2026年度予定
国際標準化	2025年3月 承認段階へ移行 2025年7月 TS原案(DTS)最終版をISO/IEC提出 2026年1月現在 ISO/IEC内でTS原案(DTS)レビュー中	ISO/IECレビューに係わるタスクの推進 ISO/IECレビュー完了後の発行プロセス実施
CPSF改訂		改訂作業開始 国際標準化の検討

ガイドラインの提供によるASEAN向け企業対策支援

- 経済産業省では産業界のサイバーセキュリティ向上に向け、**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いる**。他方、一部は**英語版が未発行**であり、発行されている**英語版も国外企業における認知度は低い**。
- 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なため、**ASEAN地域に向けて、施策の情報発信を強化。**
- 具体的には、IPA及びNCOと協力し、**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。**
  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英語版と併せて、**日・ASEANサイバーセキュリティ政策会議にて活用事例等を日本企業から発信。**あわせて英語版HPにて情報発信。



新規に英語化した中小企業向けガイドライン



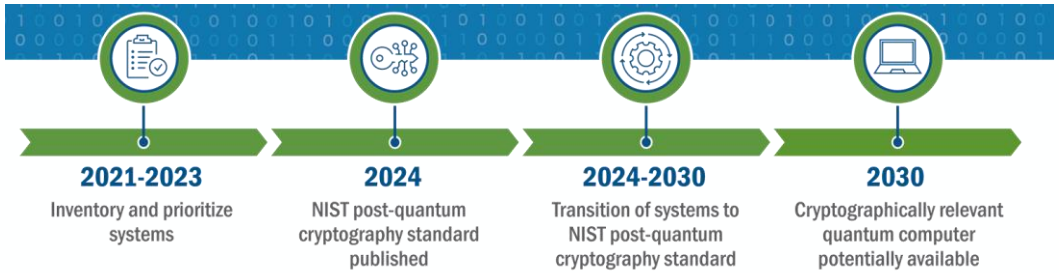
工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインの英語版

関係省庁と連携した耐量子計算機暗号（PQC）への対応の検討

- 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、米国をはじめとした各国において、**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。
- 我が国においても、政府機関等におけるPQC利用に関して、技術的課題、安全保障、国際連携等の多岐にわたる課題に対し必要な施策を検討・推進するため、**2025年６月に関係府省庁による連絡会議（局長級）を立ち上げ。25年11月、政府機関等におけるPQC移行を原則、2035年までに行うことを目指し、26年度に工程表を策定することを公表。**
- CRYPTRECにおいて、電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）へ順次PQCを掲載するため、**PQCの安全性評価・実装性能評価を実施中。**

米国におけるPQCへの移行に向けた動向

- 米国大統領令（2022年5月4日署名）を通じ、連邦政府の暗号システムをPQCへ移行し、**2035年までに量子リスクを最大限解消する方針及びタイムラインを提示。**
- 米国の国立標準技術研究所（NIST）において、**PQCの標準化作業**が進められており、2024年8月に3つの方式が連邦情報処理標準のFIPS 203, 204, 205として最終承認され、FIPS206についても引き続き標準化が進められている。



（出典）米国国土安全保障省 “Preparing for Post-Quantum Cryptography: Infographic”

CRYPTRECにおける活動状況

「耐量子計算機暗号の研究動向調査報告書」「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」（2022年３月）

- PQCとして署名・守秘・鍵共有を扱い、格子、符号、多変数、同種写像、ハッシュベースについて調査

「耐量子計算機暗号の研究動向調査報告書」「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024年度版」（2025年３月）

- PQCの範囲を明確化し、PQC導入のアプローチとして、プライオリティ設定、クリプトグラフィックアジリティ、ハイブリッド構成を整理し、FIPS 203, 204, 205についての記述を追記する等のアップデートを実施

「2025 年度暗号技術評価委員会活動計画」（2025年3月）

- 安全性等が確認されたPQCを推奨候補リストに順次掲載できるよう、諸外国において多くの専門家による検証を経て決定された方式（例：FIPS 203, 204, 205）について、安全性評価・実装性能評価等の検討を開始

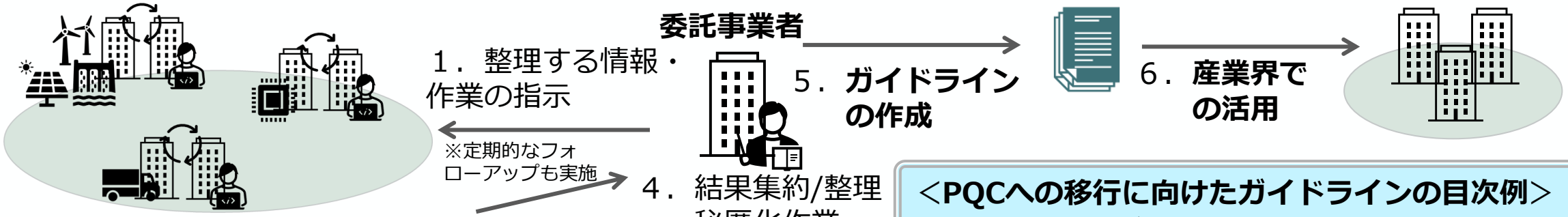
（出典）CRYPTREC 2024年度 第１回 暗号技術検討会資料

耐量子計算機暗号（PQC）への対応に向けた検討

- 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4月頃）予定。
- 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。

※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

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

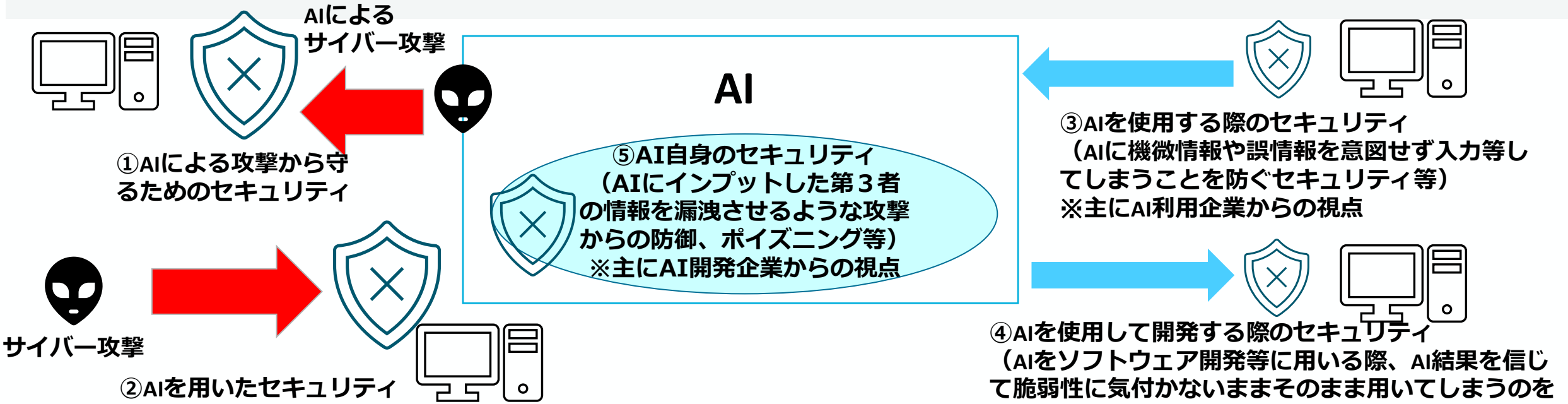


＜PQCへの移行に向けたガイドラインの目次例＞

- **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×サイバーセキュリティについての考え方

- 近年、AIの普及拡大に伴い、**AIそのものについてやAIを活用したセキュリティ対策の必要性等が指摘**されている。
- AI×サイバーセキュリティに関し、ここでは便宜上、①AIによる攻撃から守るためのセキュリティ（**Attack using AI**）、②AIを用いたセキュリティ（**AI for security**）、 ③AIを使用する際のセキュリティ（**Security for AI**） 、④AIを使用して開発する際のセキュリティ（**AI Coding Assistant Security**） 、⑤AI自身のセキュリティ（**Security for AI**）、の５領域に分類。
- 既存の政府によるガイドライン（AI事業者ガイドライン等）でカバーされているのは、③～⑤の領域が中心であるものの、AI開発者やAI提供者を中心に着目がされていることが多く、**企業がAIエージェント等を利用する際に必要な対策等は今後検討が必要**。①や②の分野は、既存の技術等で対応できるものの、AI等の技術発展により、新たなインシデント例や対策が随時生み出される注目すべき領域でもあるため、懸賞金事業等を通じて課題解決のための新たな技術の開発等を促すことが考えられる。



AI×セキュリティに関するガイドライン等の関係イメージ

AI事業者ガイド（総務省・経産省）

AIの開発・提供・利用に関わる事業者向けにAIガバナンスの統一的な指針を示すガイドライン。指針の一つにセキュリティ確保が位置付けられており、別添で手法の概要が提示。

AI開発者
＝AIシステムを開発する事業者

AI提供者
＝AI システムをアプリケーション等に組み込んだサービスとして提供する事業者

AI利用者
＝事業活動において、AIシステム又はAIサービスを利用する事業者

AIセーフティに関する評価観点ガイド（AISI）

①AIセーフティ評価の観点、想定され得るリスクの例、評価項目例、②評価の実施者や評価実施時期に関する考え方、③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）

「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。「不正操作による機密情報の漏洩、AIシステムの意図せぬ変更や停止が生じないような状態」に対する脅威への対策を主な対象とし、脅威への技術的対策例を整理

企業が利用する際に気を付けるべきガバナンスや技術的なガイドラインが必要か？

AIエージェント導入に伴うセキュリティリスクへの対応

- 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。**
- AIエージェントと言ってもその機能や役割は様々であり、その**内実に応じてAIの導入が企業にもたらすセキュリティリスクは異なる。**
  ※セキュリテイリスクの一例として、兼務によるID管理の複雑さに伴い、意図せぬ情報流出や権限逸脱行為をAIエージェントが実施する可能性あり。
- そのため、本来は**導入時のセキュリティリスクを適切にアセスメントした上で、必要なセキュリティ対策を整備する必要**があるが、現状多くの企業においては部分的な技術的ソリューションの導入にとどまっており、リスクアセスメントを含むAIセキュリティガバナンスが整備されていない。
- 以上を踏まえ、AIエージェントを導入済みもしくはこれから導入を計画している企業を想定読者とし、**AIエージェントの導入時のリスクアセスメントからそれに応じた必要なセキュリティ対策の実装例までを一気通貫で整理したガイドラインを、26年度以降整備する。**

※AISIでは、25年度から「AIエージェントシステムに関する状況及び評価方法の調査研究」を実施中。AIエージェントに関する課題やリスク、対策等を整理し、AIエージェントに関する評価項目及び評価手法の詳細化の検討を行っている。AISIや関係省庁等とも連携しながら進めたい。

今後議論するガイドラインの論点

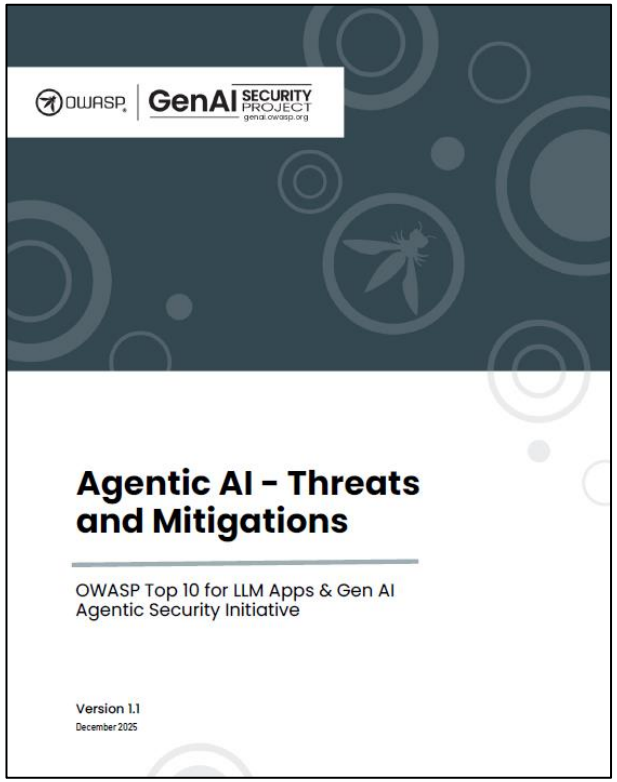
1	AIエージェント導入パターン分類	…主要なAIの導入事例をリストアップしつつ、パターン化
2	AI導入時のリスクアセスメント、及びパターンごとの主要リスク整理	…リスク評価の判定軸を整理しつつ、1のパターンごとの実例
3	リスクに応じた対策の実装例	…2の実例をベースにリスクパターンごとの対策例（IT環境全体）を整理

対策の実装例は、下記の通り、AIシステム単体の論点に限らず、IT環境全体において施すべき対策を想定
- 権限管理
- データ保護
- （AIのみならずIT環境全体を踏まえた）システム構成・設計等（監視設計等）

（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/

（参考）OWASPのガイドラインについて

- OWASPが公表した**AIエージェントに関する新たな脅威とその緩和策を体系的に整理**したガイド。
- 従来の生成AIに帯する脅威に加え、**マルチエージェントを含むAIエージェント利用環境特有の脅威**（Tool Misuse, Inter-Agent Protocol Abuse, Cascading Hallucinations, etc.）を整理の上、対応するセキュリティ上の緩和策を例示
- AIエージェントは**従来の生成AIに対する脅威を拡張し、自律性・ツール統合・マルチエージェント構造が新たな攻撃面を生む**ことが示唆されている、



ガイドライン概要

AIエージェントを用いたシステム全体のアーキテクチャ（シングルエージェント・マルチエージェント双方）を例示し、そのアーキテクチャ例に対する脅威モデリングを行った上で、**AIエージェント利用環境特有の脅威とそれに対応する緩和策を体系的に整理。**

参考

分野別SWGにおけるCPSFの具体化

- **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月に改訂。**

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）。**

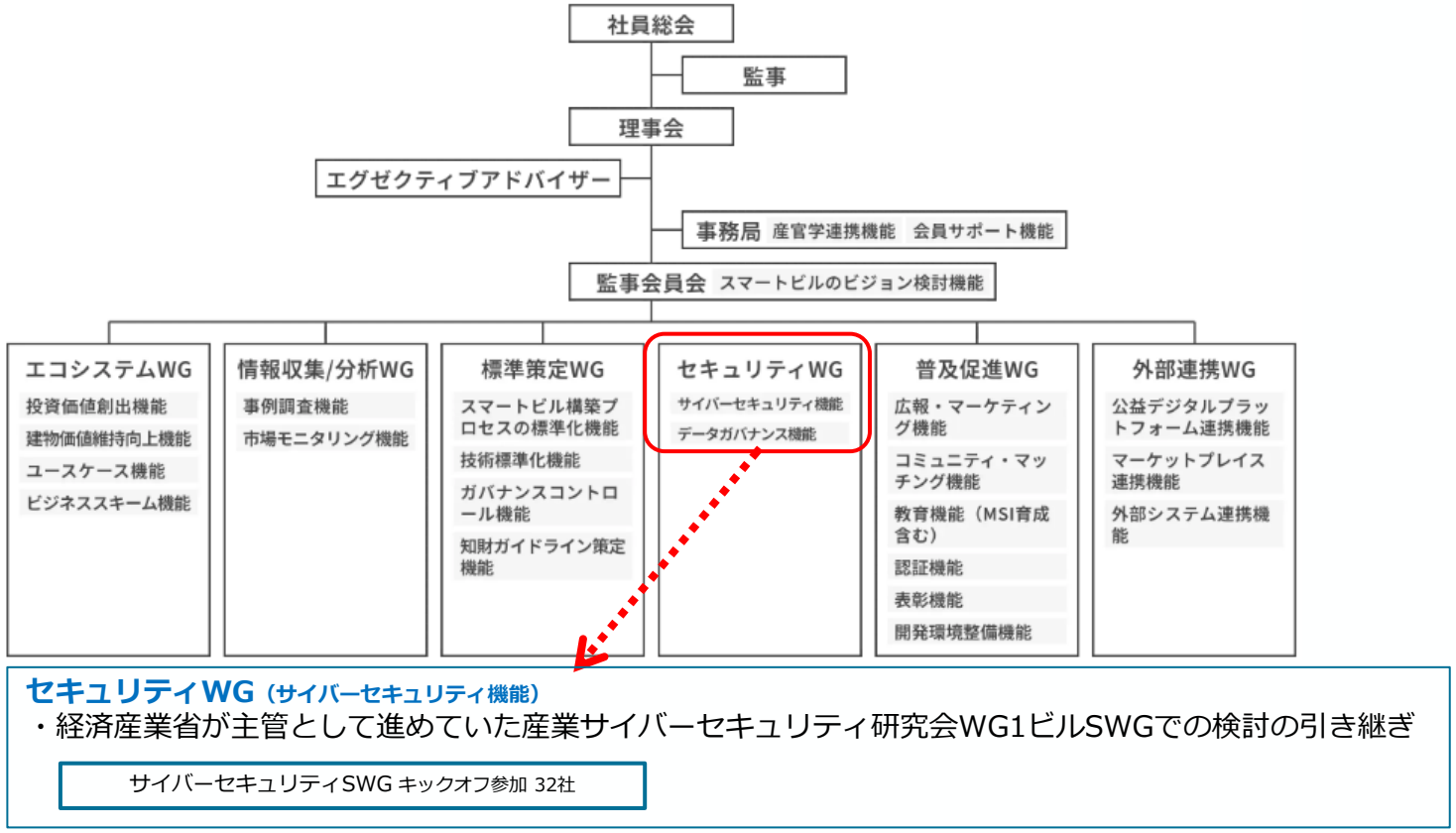
半導体産業SWG

- **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

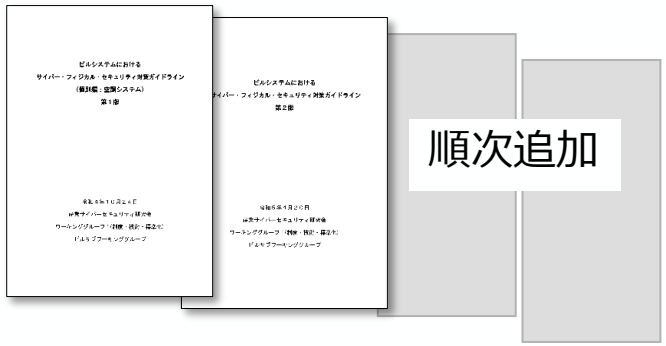
（出典）一般社団法人スマートビルディング共創機構
https://www.sbco.or.jp/

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)

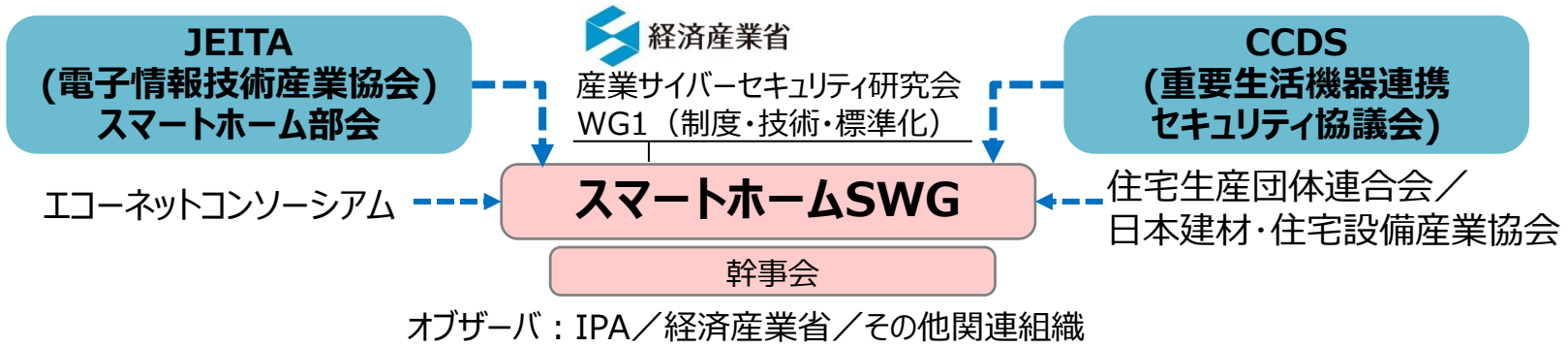
- ✓ サプライチェーンおよびラベリング製品を見据え、発注仕様書への記載項目について整理
  （オーナー、設計事務所・ゼネコン、ベンダーの視点）
- ✓ 統合監視へのSOCの役割に関する議論
- ✓ ラベリング制度内容の検討

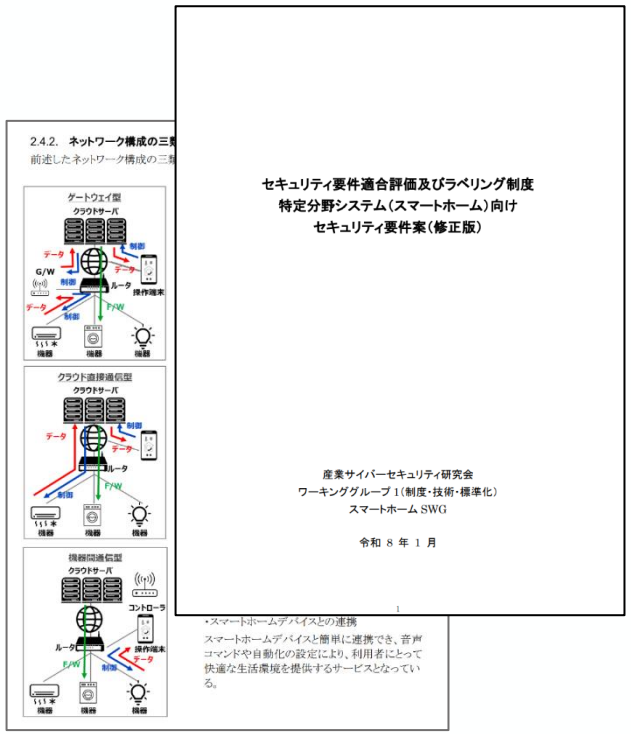
ビルSWGが作成したガイドライン



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月の開催を予定。
- 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。





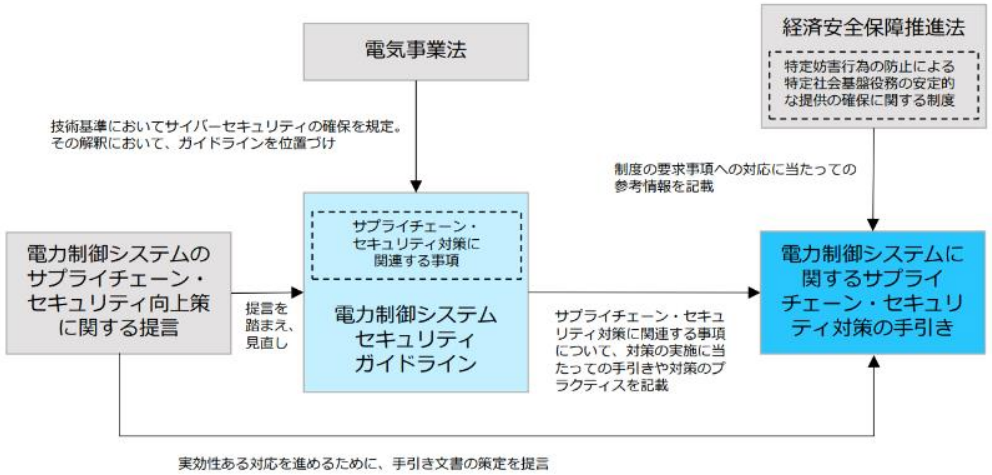
主査：JEITA/CCDSから選出、共同主査形式
委員：JEITA/CCDSの両会員企業から、IoT製品メーカ、ユーザを中心に委員を招聘
主な活動内容：
- **JC-STARセキュリティ要件案（スマートホーム向け）の修正検討**
  - －BtoBtoCモデルにおけるスマートホーム提供事業者に対する追加要件の検討
- **普及促進検討**
  - －家電流通協会と連携したJC-STARラベル付き製品販売促進策の検討
  - －CEATECへの出典、店頭イベント等各種普及促進策の検討

（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）

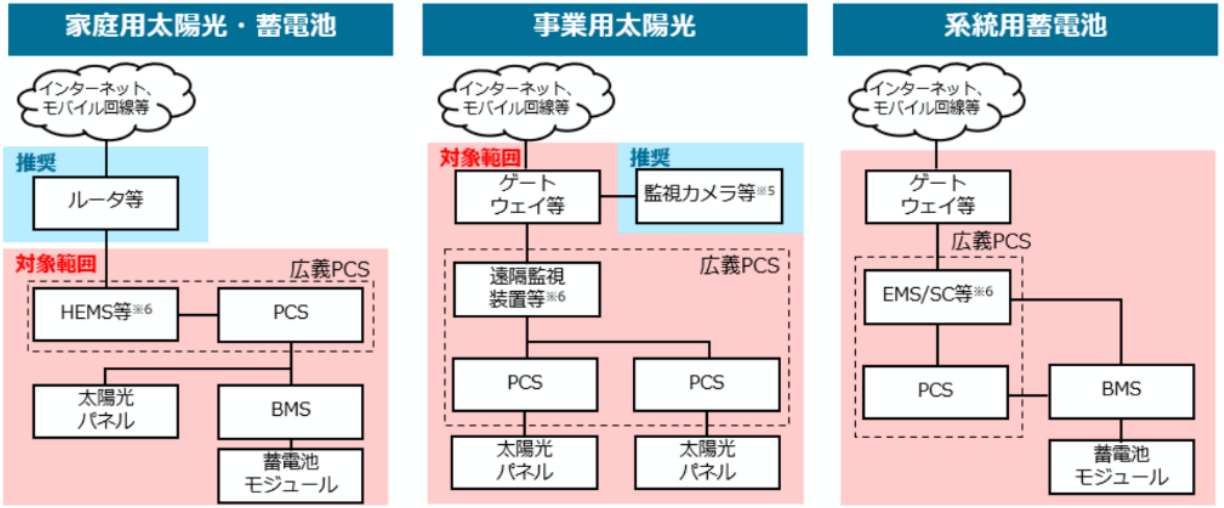
- **電気事業者に求められるサプライチェーン・セキュリティ対策の取組を支援**するため、**「電力制御システムのサプライチェーン・セキュリティ対策の手引き」**（2025年6月公開）や「リスク点検ツール」（2024年3月公開）の活用を促している。
- **分散型電源のサイバーセキュリティ対策におけるJC-STAR制度の活用**について議論。**太陽光発電・蓄電池におけるJC-STAR★1を取得した機器の使用の要件化**が決定。

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 電力SWG資料より抜粋

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。

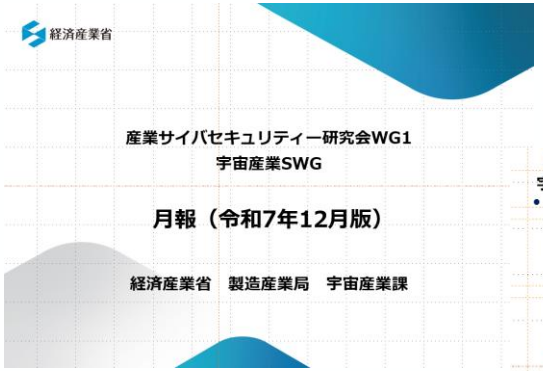
＜2025年度進捗＞
- 付録のチェックシート側の小改訂に伴い、**「自工会／部工会サイバーセキュリティガイドライン2.3版」を公開**。
- 2025年度の自己評価の依頼のため、自工会・部工会合同でサプライヤーの経営層＋担当者向け説明会を開催。被害事例、経営への影響等も説明し、4回合計で3,300社、延べ5,600人が参加。
- 自己評価は過去最多となる4,032社が提出。集計結果は例年通り３月末に公表予定。
- 上記ガイドラインの要求事項や自己評価を行う上での問い合わせに対応すべく自工会HPにて生成AIを活用したチャットボットを試験的に導入。9月～12月の運用期間で利用者数1,100人、総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

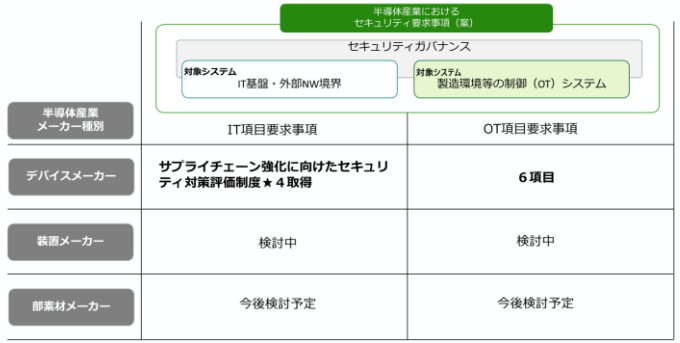
目次

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（44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）



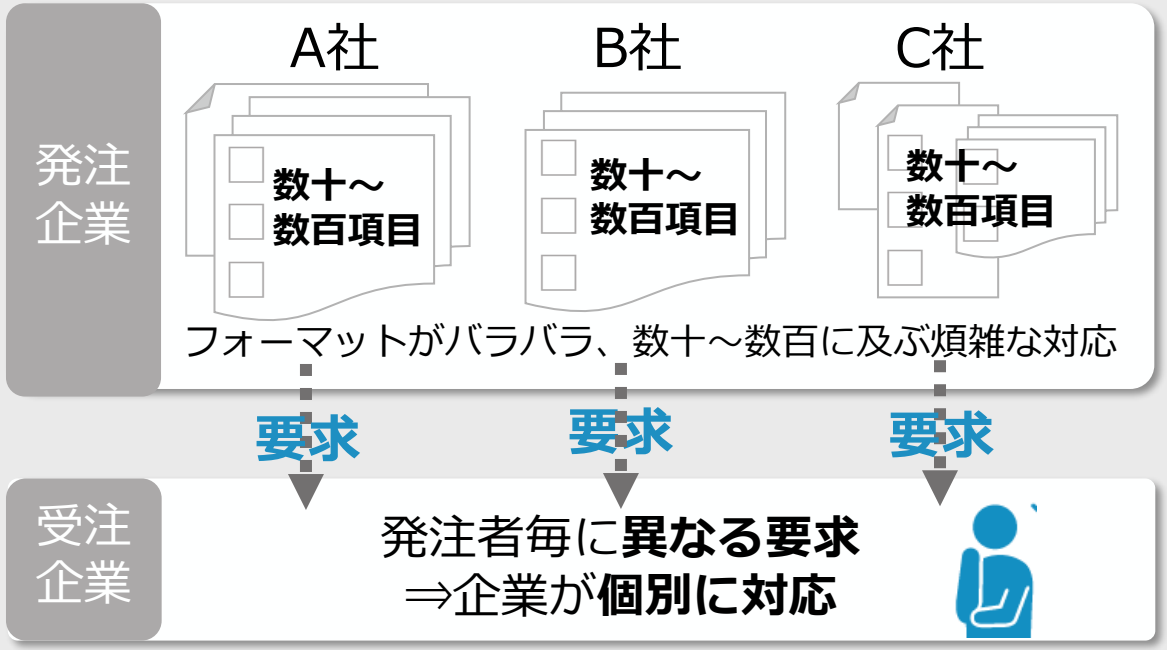
半導体産業メーカー種別	IT項目要求事項	OT項目要求事項
デバイスメーカー	サプライチェーン強化に向けたセキュリティ対策評価制度★４取得	６項目
装置メーカー	検討中	検討中
部素材メーカー	今後検討予定	今後検討予定

(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

（参考）中小企業がSCS評価制度の“★”を取得するメリット

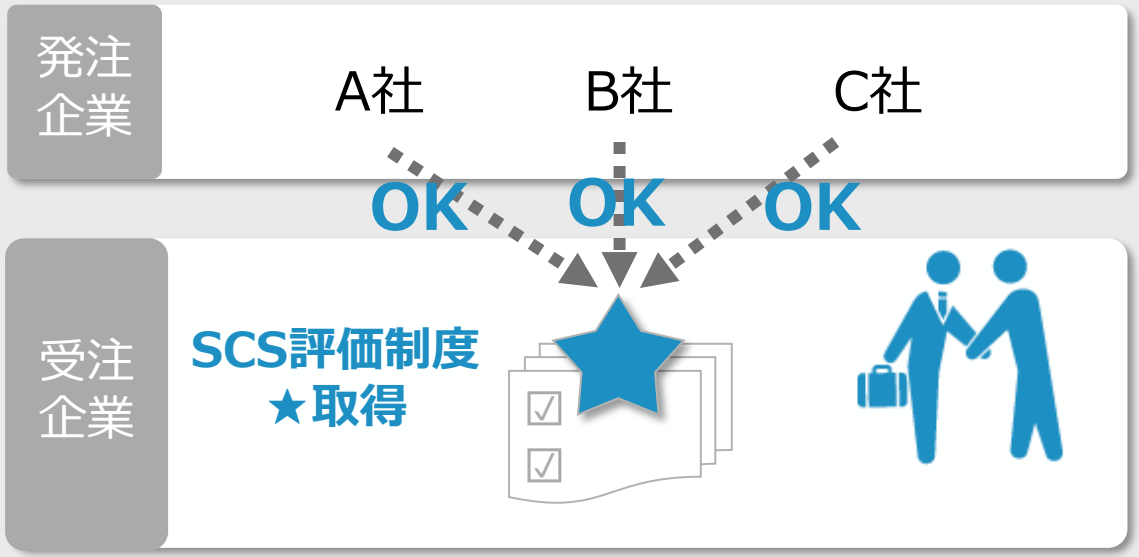
発注者ごとに異なる要求…対応が煩雑で非効率

- ✓ 発注者側からの**様々な要求に一つずつ対応**する必要がある
- ✓ 複数社と取引する場合、**それぞれの会社からの要求に対応**するのが困難
- ✓ 各企業の要求リストは似ていてもフォーマットがバラバラで、内容を理解していないと対応できず、**数百項目に及ぶ煩雑な対応が発生**



“★”取得で、発注者対応が一括クリア！

- ✓ SCS評価制度の“★”取得が、発注企業・受注企業双方にとっての**「共通のものさし」**となる
- ✓ 結果、各社からの要求に説明できるようになり、**対応工数削減や業務の標準化・効率化に繋がる**
- ✓ ★取得済み企業は、発注者がどのレベルまで対応できているかが一目でわかりスムーズな取引が可能となり、**発注者との信頼構築に繋がる**



（参考）SCS評価制度とSECURITY ACTIONとの接続

セキュリティ対策の範囲・内容

現時点でのベストプラクティス

包括的・標準的なセキュリティ対策

基礎的な組織的対策とシステム防御策

経営者・従業員への意識付け

調達側

強制はできないが、サプライヤーには
一定の対策（リスク低減策）をとってもらいたい

サプライヤー

一定の対策は必要と思うものの、
- 現実的な対策レベル感がわからない
- 各社から異なる基準を要請される

SECURITY ACTION

一つ星・二つ星

SCS評価制度

★3

サプライチェーン企業が最低限実装すべき対策

SCS評価制度

★4

サプライチェーン企業が標準的に目指すべき対策

成熟度の定義	三つ星（★3）	四つ星（★4）
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
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
評価スキーム	自己評価	第三者評価

※具体化の際に、既存認証制度との連携等スキームを検討

自工会・部工会ガイドライン LV3 等

ISO27000シリーズ（ISMS）

★5

※令和7年度以降に検討予定

組織におけるマネジメントシステムの確立
＋
システムへの具体的な対策実装

サプライチェーン強靭化への寄与

（寄与なし）経営者によるセキュリティ意識の宣言

自社のセキュリティ対策インシデント時の報告・共有

取引先を含めたセキュリティ対策

サプライチェーン全体に寄与するセキュリティ対策

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構築促進に向けた想定事例及び解説（概要）

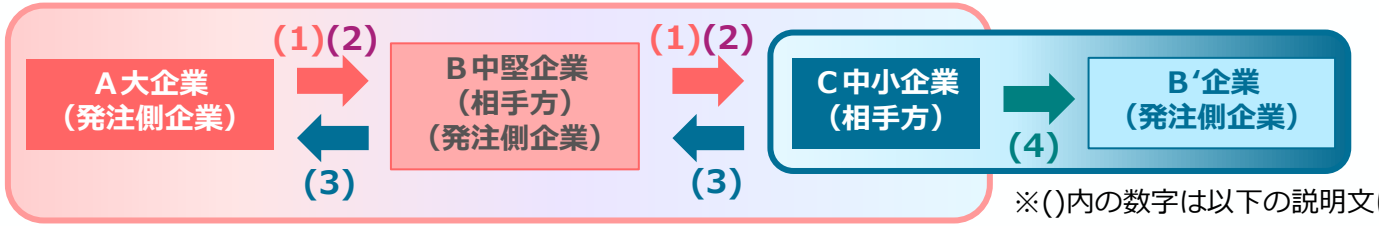
２０２５年１２月２６日
経済産業省・公正取引委員会

○　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。