経済産業省

資料４

事務局説明資料
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・WG１分野横断SWG 合同会議

令和７年４月１４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の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

第１回：平成29年12月27日	
第２回：平成30年　5月30日	アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日	アクションプランを加速化する３つの指針を提示
第４回：令和　2年　4月17日	（電話開催）産業界へのメッセージを発信
第５回：令和　2年　6月30日	サイバーセキュリティ強化運動の展開
第６回：令和　3年　4月　2日	アクションプランの持続的発展と、新たな課題へのチャレンジへ
第７回：令和　4年　4月11日	産業界へのメッセージを発信
第８回：令和　6年　4月　5日	新たなサイバーセキュリティ政策の方向性を提示
第９回：令和　7年　5月23日	具体化した新政策を提示

＜構成員＞

※2025年5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

澤田　純　日本電信電話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

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＞

NISC、サイバー安全保障体制制度準備室、警察庁、金融庁、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、デジタル庁

WG１（実効性強化・国際連携）

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

- 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

WG２（地域・中小企業支援）

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

- 地域・中小企業等における対策支援

WG３（産業振興・人材育成）

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

- セキュリティ産業振興、研究開発
- 人材育成・確保

＜新たなサイバーセキュリティ政策の全体像及び今後の方向性＞

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

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

- 2019年以降、中国の関与が疑われるグループ「MirrorFace」による、**日本の安全保障や先端技術に係る情報窃取を目的とした攻撃キャンペーン**が実行されている。（2025年1月 警察庁及びNISCが注意喚起を発出）
- 2024年後半、中国背景と指摘されるグループ「Salt Typhoon」による、米国の通信事業者のネットワークに侵入して**政府関係者等の通話記録等、安全保障に関する情報等の窃取**を狙うような活動が報告されている。

②金銭等資産の窃取

- 2024年5月、北朝鮮を背景とする攻撃グループ「TraderTraitor」が、**ソーシャルエンジニアリング等の手法を用いて**、㈱DMM Bitcoinから**約482億円相当の暗号資産を窃取**。（2024年12月 警察庁、NISC及び金融庁が注意喚起を発出）

③事業活動の停止

- 2024年6月、㈱KADOKAWAが**ランサムウェアを含む大規模サイバー攻撃を受け、Webサービス等が停止**。大量の個人情報や企業情報が漏えいしたうえ、SNS等を通じて拡散される二次被害も発生。

④重要インフラの機能停止等

- 2024年12月～2025年１月の年末年始にかけて、航空事業者、金融機関、通信事業者等が**相次いでDDoS攻撃を受け、サービスの一時停止**等の被害が発生。（2025年2月 NISCが注意喚起を発出）
- 2024年2月、米国政府機関（CISA、NSA、FBI等）が、ファイブアイズ諸国の関係機関と合同で、中国を背景とするグループ「Volt Typhoon」による米国の重要インフラを標的とした活動について注意喚起。同グループは、**有事の際に重要インフラに対するサイバー攻撃を行うため、事前に重要インフラ事業者等のネットワークへのアクセス権限を確保してOT機器に対する侵害を可能としている**旨が指摘されている。

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、**サイバー攻撃は今後ますます増加するとともに高度化・複雑化していくおそれ**がある。

デジタル技術の発展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2024年に観測した**サイバー攻撃関連通信数は増加傾向**であり、約6,862億パケット（2018年の約３倍）。

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**

2024年における**フィッシングの報告件数**は**前年比約50%増の170万件超に急増**

量子コンピュータによる暗号アルゴリズムの危殆化

- 各国が開発を加速させている**量子コンピュータが実用化**すると現在広く使用されている**公開鍵暗号（RSA暗号）アルゴリズムの危殆化される恐れ**が指摘されている。
- 現在のアルゴリズムの安全性は、古典計算機では現実的時間内では解くことが困難とされている数学的問題（素因数分解問題や離散対数問題）に依拠しているが、大規模な量子コンピューターでは高速に解読することが可能であるため。
- このため、量子コンピュータ時代にも安全に利用できる暗号技術が求められており、米国NIST等が**耐量子計算機暗号（PQC）に係る国際標準化**作業を進めている。

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。

（出典）(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威 2024」解説書、(国研)情報通信研究機構「NICTER観測レポート2024」、フィッシング対策協議会「月次報告書」　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

■IT系システムの侵害
・特徴：情報システム内部への侵入・暗号化
・効果：暗号化・システム障害、身代金要求
・事例：Wannacry・2017年　等

■有事に備えた重要インフラ等への侵入
・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 Thyphoon・2023年　等

■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

（出典）各種報道発表・報道情報等を基に作成。

CISA “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure”

ウクライナに対する主なサイバー攻撃

- 侵略開始以前：
  - ロシアは侵略開始の１年以上前からウクライナの政府機関や重要インフラ等の情報システム・ネットワークに侵入し、**破壊的サイバー攻撃を準備**。
  - 侵略開始の１か月程度前から、破壊的なサイバー攻撃等を開始。
- 2022年２月：通信衛星に対する攻撃
  - 米Viasat社が提供する**通信衛星サービス**（KA-SAT network）**が利用不能**となった。
- 2022年10月：変電所に対する攻撃
  - ウクライナの変電所が攻撃を受け、**停電が発生**。

政府機関等へのサイバー攻撃事案

- **NISCに対する不正通信事案**（2023年８月）
  - NISCの電子メール関連システムに対する不正通信があり、メールデータの一部が外部に漏えいした可能性がある旨を公表。
- **JAXAへの不正アクセス事案**（2024年７月）
  - 外部からJAXA内の業務用イントラネットの管理用サーバーに不正アクセスが行われた可能性があった旨を公表。

（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 2025	
順　位	組織向け脅威
1位	ランサムウェア攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃
3位	システムの脆弱性を突いた攻撃
4位	内部不正による情報漏えい等
5位	機密情報等を狙った標的型攻撃
6位	リモートワーク等の環境や仕組みを狙った攻撃
7位	地政学的リスクに起因するサイバー攻撃
8位	分散型サービス妨害攻撃（DDoS攻撃）
9位	ビジネスメール詐欺
10位	不注意による情報漏えい等

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「情報セキュリティ10大脅威2025」

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**重要インフラ事業者等に対するインシデント報告等の義務化**、③**企業のサイバーセキュリティ対策水準を整備・可視化等**する動きが加速。

* 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

サイバーレジリエンス法（Cyber Resilience Act）

- **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。**
- 2024年12月に発効。**報告義務の運用開始は2026年9月、その他は2027年12月開始。**

サイバー・トラスト・マーク（U.S. Cyber Trust Mark）

- **消費者向け無線IoT製品が対象の任意ラベリング制度。**ルータ、スマートメーター等**一部製品については、個別のセキュリティ要件が定義される見込み。**2024年7月に最終規則公表。**2025年中に制度運用開始**を目指す。

米国ソフトウェアサプライチェーンの確保に関する覚書（OMB M-22-18, M-23-16）

- **連邦政府機関が調達するソフトウェアのベンダー**に対し、**セキュアなソフトウェア開発に関する自己適合を義務付け。**
- 2024年3月に自己適合証明するための共通フォームを正式承認。

※英国においても、消費者向けIoT機器の製造者に対するセキュリティ基準への自己適合宣言を義務付けるPSTI法（2024年４月施行）が存在。

②重要インフラ事業者等に対するインシデント報告等の義務

重要インフラに係るサイバーインシデント報告法（Cyber Incident Reporting for Critical Infrastructure Act of 2022）

- 「重要インフラ」に対し、①**重大なサイバーインシデント**の認知後**72時間以内**、②**ランサム支払**後**24時間以内に米CISAへの報告等を義務付け。**
- 2022年3月成立、2024年4月規則案公表。2025年秋最終規則公表を想定。

NIS 2指令（Directive (EU) 2022/2555）

- **2016年NIS指令から対象セクターを拡大。**対象の主要／重要エンティティに対し、①**サイバーセキュリティ・リスクマネジメントの強化**、②**重大なサイバーインシデント**の認知後**24時間以内に早期警告、72時間以内にCSIRT又は管轄省庁に報告等を義務付け。2023年1月発効、2024年10月18日より執行。**

※豪州においても、特定の事業者に対しランサム支払い後72時間以内の報告を義務付けるサイバーセキュリティ法（下位法の制定を経て2025年5月30日より適用予定）が存在。

③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（UK Cyber Essentials）

- 英NCSCが**全ての企業に対し、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。

目次

前回ＷＧからの主な進捗

①セキュア・バイ・デザインの実践

⇒ソフトウェアセキュリティ確保に向けた一連の取組（SBOM、SSDF 等）の具体化

⇒IoTセキュリティ適合性評価制度（JC-STAR）の制度開始

②サプライチェーン全体のセキュリティ対策強化

⇒サプライチェーン対策評価制度の検討加速（「中間取りまとめ」の提示）

③その他

⇒CPSFの国際規格化推進

⇒半導体セキュリティSWGの立上げ（OTガイドラインの検討、情報共有枠組み等）

目次

前回のWG1・分野横断SWG合同会議における主なご指摘

【SBOMについて】

- SBOM には、製品の差別化やコスト削減につながる情報が含まれており、二者間で企業秘密の保護に関する規定があれば利用が促進されると思われる。また、SBOM 提供が義務化される可能性がある中、すべての要素を提供しなければならないか、ネットワークに面して攻撃される可能性が高い部分に限定するかなど、提供する範囲をいかに限定するかというスコープに係る議論がなされることを期待する。
- 供給側と利用側の双方から経済的な動機付けが必要と言われる。調査研究等を通じて、SBOM の活用等によるコスト削減効果などを明示いただけるとありがたい。
- SBOM の普及が課題になる中で、単なるリストの管理にならないよう注意が必要と考える。脆弱性管理につなげていくことが重要であり、サイバーハイジーンやポスチャー・マネジメントといった高いレベルを目指していただきたい。
- SBOM 情報の共有について、受け手側の情報管理だけでなく、脆弱性管理等での活用についても責任関係の明確化が必要と考える。
- ビジネスに SBOM を要求として入れ込んでいくことが必要である。政府調達から入れ込んでいくことも有用ではないか。第三者認証を求めることでコストが増大する場合、適切な支援策と組み合わせて事業者をサポートできないか。
- SBOM のガイドについて、利用する立場がユーザー、開発者、インテグレータといる中で、立場によって活用方法等が異なるように思われるため、ガイドにも反映されたい。規模や業種により具体的な活用方法は変わるように思われるため、共通部分とカスタマイズできる部分に分かれているとよいと思う。
- 小規模な実証事業からいきなり社会実装に向かうには大きなハードルがあると思われる。SBOM はインフラを支える技術であるため、段階を踏んで検討を進めていただけるとよい。

セキュア・バイ・デザインの実践（セキュアなIoT製品及びソフトウェアの流通に向けた取組全体像）

- ITシステム・機器への社会全体の依存が高まる中、これらへのサイバー攻撃のリスクを低下する観点からセキュアバイデザインのコンセプトの下、製品の設計・開発段階からセキュリティを考慮する重要性が増している。当省においては、**IoT製品やソフトウェアでのセキュアバイデザインの実践を推進する観点から以下の取組を推進中。**

- IoT製品について、セキュリティ対策レベルを評価・可視化する取組として、「**IoTセキュリティ適合性評価制度（通称：JC-STAR）」を本年3月に開始**（まずは**IoT製品共通の最低限の基準（★1）を開始**）。**政府機関や地方公共団体、重要インフラ事業者での活用を促しつつ**、広く民間企業や一般消費者における普及を目指す。

- また、**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**も実施。「**SBOM（ソフトウェア部品構成表）の導入促進に向けた手引き**」（2024年8月に手引ver2.0を策定）を作成。更に、「**セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）**」（2025年3月）や「**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）**」（2025年3月）**を提示**した。

- これらの取組・制度については、国内外の制度を調和する観点から国際連携が重要となっており、マルチやバイの場を通じて、**関係国と連携強化の議論**を進めている。

ソフトウェア管理に向けたSBOM (Software Bill of Materials) の導入に関する手引 ～全体概要～

手引の背景・目的

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェアの利用が一般化する中で、ソフトウェアにおける脆弱性管理やライセンス管理の重要性が高まっている。ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- 複数の産業分野における実証を通じ、SBOM活用の効果が確認できた。一方、SBOM導入・活用に際しては様々な課題(例：脆弱性管理の効率化、分野や用途に応じたSBOMの適切な範囲、ソフトウェアの調達者と供給者の立場間の取り決め）が存在することが明らかとなった。
- 本手引では、**SBOMに関する「基本的な情報」や「誤解と事実」を提供し、**企業のSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及び認識しておくべきポイント**を示す。(ver1.0)
- 加えて、ソフトウェアの脆弱性を管理する一連プロセスにおいて**SBOMを効果的に活用するための具体的な手順と考え方**、SBOM導入の効果及びコストを勘案して**SBOMを導入することが妥当な範囲を検討するためのフレームワーク**、ソフトウェアの受発注において、**調達者と供給者の間でSBOMに関して契約に規定すべき事項（要求事項、責任、コスト負担、権利等）について参考例**を示す。(ver2.0)

対象読者

- 主にパッケージソフトウェアや組込みソフトウェアに関する **ソフトウェアサプライヤー**
  - ✓ ソフトウェア開発・設計部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 経営層
  - ✓ 法務・知財部門

SBOM導入の主なメリット

- **脆弱性管理のメリット**
  - ✓ 脆弱性残留リスクの低減
  - ✓ 脆弱性対応期間の低減
  - ✓ 脆弱性管理にかかるコストの低減
- **ライセンス管理のメリット**
  - ✓ ライセンス違反リスクの低減
  - ✓ ライセンス管理にかかるコストの低減
- **開発生産性向上のメリット**
  - ✓ 開発遅延の防止
  - ✓ 開発にかかるコストの低減
  - ✓ 開発期間の短縮

SBOM導入に向けたプロセス(ver1.0)

フェーズ1	環境構築・体制整備	● 1-1. SBOM適用範囲の明確化 ● 1-2. SBOMツールの選定 ● 1-3. SBOMツールの導入・設定 ● 1-4. SBOMツールに関する学習
フェーズ2	SBOM作成・共有	● 2-1. コンポーネントの解析 ● 2-2. SBOMの作成 ● 2-3. SBOMの共有
フェーズ3	SBOM運用・管理	● 3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施 ● 3-2. SBOM情報の管理

脆弱性管理プロセスの具体化(ver2.0)

- SBOMを活用することで、ソフトウェアの脆弱性管理を通じた脆弱性リスクの低減が効果として見込まれていることから、**SBOMを活用するプロセスの中でも、脆弱性管理に関するフェーズが特に重要**。
- 脆弱性管理の一連プロセスにおいてSBOMを効果的に活用するための**具体的手順と考え方をまとめることで、SBOM活用による効果を高めるための参考情報**を提供。

SBOMを活用した脆弱性管理プロセス

フェーズ1 脆弱性特定
- マッチング手法区分選択
- 利用可能なSBOMデータ特定
- 脆弱性DBの選択
- マッチング手法の選択・作成

フェーズ2 脆弱性対応優先度付
- 予備フィルタリング
- 優先度付情報の選択・取得
- 判断ツリーに基づくカテゴリ判定
- 優先度スコア評価

フェーズ3 情報共有
- 共有情報と共有相手の特定
- 共有方法の特定と実施

フェーズ4 脆弱性対応
- 脆弱性の暫定対応
- 脆弱性の根本対応

SBOM対応モデル(ver2.0)

- SBOM導入の効果及びコストを勘案してSBOMを導入することが**妥当な範囲を検討するためのフレームワーク(5W1Hを網羅するよう体系化)**。
- 実証を通じて、**医療機器、自動車、ソフトウェア製品等の分野**において、コスト・効果を考慮して妥当な対応範囲の参考例を提示。
- 当該フレームワークを用いることで、高度な管理を行えるソフトウェア、すなわちセキュアなソフトウェアが市場に適切に評価され、その流通が促進されることが期待できる。

SBOM取引モデル(ver2.0)

- ソフトウェア部品の受発注において、調達者と供給者の間でSBOMに関して**契約に規定すべき事項（要求事項、責任、コスト負担、権利等）**について参考となる例を示す。
- 既存のソフトウェアに関するモデル契約書と組合せることで、**SBOMに対応した契約書を作成する際の項目案を提示**するもの。

SSDF導入ガイダンス（中間整理） ～全体概要～

背景・目的

- セキュリティ実現の中核となるソフトウェア・セキュリティについて、経験知を集約した体系的、包括的な取組みが重要。
- QUAD共同原則において、政府調達方針としてセキュア・ソフトウェア開発プラクティスの導入に合意。
- NIST　SSDFは、汎用的で、抽象度が高いため、組織に実践導入する上で具体策が明確ではないなど課題が大きい。
- SSDFを企業現場に導入するための手順、方法を示す。

対象読者

- ソフトウェア（パッケージ、サービス、機器組込みなど）を開発提供するベンダー
- ソフトウェアを調達する事業者

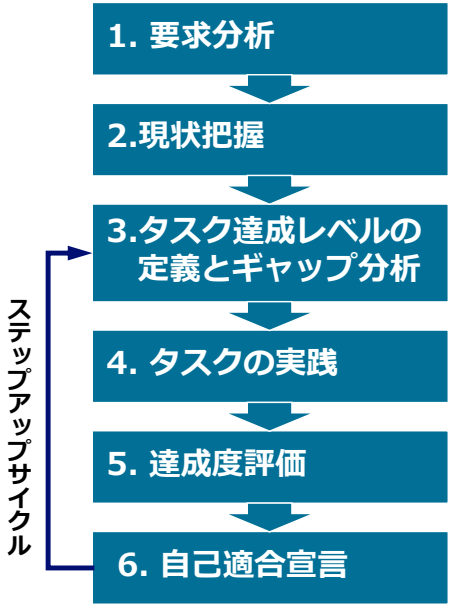
※　産業分野、開発言語、利用技術、開発プロセスに依らず幅広い領域の事業者

SSDF導入の意義・メリット

- **体系的な対策による脆弱性の解消**
  経験知を集約した体系的なフレームワークによる網羅的な対策による弱点の解消する。
- **可視化を通じた説明責任の向上（アシュアランスの向上）**
  調達者、供給者の双方にとって、開発手法を可視化・把握できるようにし、説明責任の向上（不確実なリスクの低減）を図る。
- **共通言語によるステークホルダー間の理解促進**
  産業分野、開発言語、開発プロセスに依存しない共通言語を提供し、ステークホルダー間の理解・コミュニケーションを促進する。
- **プロセスの効率化**
  組織・ツール環境の整備によるセキュリティ・プロセスの効率化を実現する。

SSDF導入プロセス

プロセスの全体像



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済/未済の状況を把握する。

フェーズ 3 タスク達成レベルの定義とギャップ分析

- タスクの達成レベルとプラクティス案を参考に、要求分析に基づき対象製品・サービスについて目指すタスクレベルを設定し、現状との比較からタスク実施能力の不足について明らかにするためギャップ分析を行う。
- アカウンタビリティアプローチの提示。

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て実施能力が不足するタスクについては、タスクの達成レベルとプラクティス案や、関連する国内ガイドライン、付録のSSDF導入実証などを参考に設定したタスクの管理策を実践する。

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することにより、タスク達成レベルを評価判定し、タスク達成レベルの目標設定と乖離がある場合、妥当性の評価を行う。

フェーズ 6 自己適合宣言

- 必要に応じて、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。

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）　～全体概要～①

- **ソフトウェア・サプライチェーンのサイバーセキュリティ対策強化**のため、令和６年９月から重要インフラ専門調査会及び、経済産業省 産業サイバーセキュリティ研究会の下に共同開催として、産学の有識者からなるワーキンググループを立ち上げ、ソフトウェアを利用する顧客等の保護を目的とした**サイバーインフラ事業者に求められる役割等**について検討。
- 令和６年度中に、ガイドライン（案）としてとりまとめ、令和7年度、自己適合宣言の仕組み化、政府機関や重要インフラの調達等での参照といった普及策等を検討予定。

背景・課題

・ソフトウェアの脆弱性を悪用するサイバー攻撃の脅威が増加

⇒ ソフトウェアの開発・供給・運用を行う「サイバーインフラ事業者」のそれぞれがより一層の責任をもって対応する必要性

⇒ セキュア・バイ・デザイン／デフォルトに関する国際文書にNISCも共同署名

・他方、サイバーインフラ事業者に求められる役割等を整理した国内のガイドラインなし

検討中のガイドライン（案）のイメージ

・サイバーインフラ事業者と顧客に求められる責務、責務を果たすための要求事項（具体的取組）を整理※

サイバーインフラ事業者	○ソフトウェア（クラウド上のものを含む）の ・開発者 ・供給者 ・運用者
顧客	○顧客（政府機関、重要インフラ 等）

(1) 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

(2) ソフトウェアサプライチェーンの管理

(3) 残存脆弱性への速やかな対処

(4) ソフトウェアに関するガバナンスの整備

(5) 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

(6) 顧客の経営層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

※諸外国の関連ガイドライン等を参照

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）　～全体概要～②

ソフトウェアサプライチェーンのサイバーセキュリティに関するレジリエンス向上のため、サイバーインフラ事業者と顧客に求められる責務(基本理念に類する事項)、及び責務を果たすための要求事項を6つに整理。今後は活用促進に向けた自己適合宣言等の制度検討等の取組を実施予定。

ガイドライン（案）の背景

- ソフトウェアとそのサプライチェーンに潜む脆弱性を悪用するサイバー攻撃が増加
- NISC等も共同署名したセキュア・バイ・デザイン／デフォルトなどデジタル製品・サービスにおけるサイバーセキュリティ対策の強化に関する制度整備が加速

ガイドライン（案）の趣旨

- 諸外国の取組と整合した、ソフトウェアを利用してサイバーインフラを提供する「サイバーインフラ事業者」の対応を整理することが求められているところ、事業者及び関係者がサイバーセキュリティ対策の実効性を確保するために参考となる考え方を示すもの

今後の取組例

- 活用促進に向けた自己適合宣言等の制度検討、ツール類の整備、広報活動などを検討

ガイドライン（案）の概要

6つの責務 サイバーセキュリティに関するレジリエンス向上のため、認識すべき基本理念	６つの要求事項 サイバーセキュリティに関するレジリエンス向上のため、共通して取組むべきサイバーセキュリティ対策	対象組織
セキュリティ品質を確保したソフトウェアの設計・開発・供給・運用	セキュアな設計・開発・供給・運用	サイバーインフラ事業者（ソフトウェア開発ベンダー、ソフトウェア販売会社、ソフトウェア運用ベンダー　等）
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	
顧客の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

※「ライフサイクル管理、透明性の確保」のうちSBOM関連の内容については、経済産業省の「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver2.0」を参考とすることができる。

IoTセキュリティラベリング制度（JC-STAR）の概要

- IoT製品の脆弱性を狙ったサイバー脅威が高まっていることを踏まえ、経済産業省にて検討会(※1)を開催し、2024年8月に**IPAを運用主体とする制度**(※2)の構築方針を公表。
- 対象製品共通の**最低限の基準（★1）の申請を2025年3月25日に開始。政府調達等での要件化について政府内で協議中。**またG7各国を中心に**諸外国との制度調和**を図るため議論中。

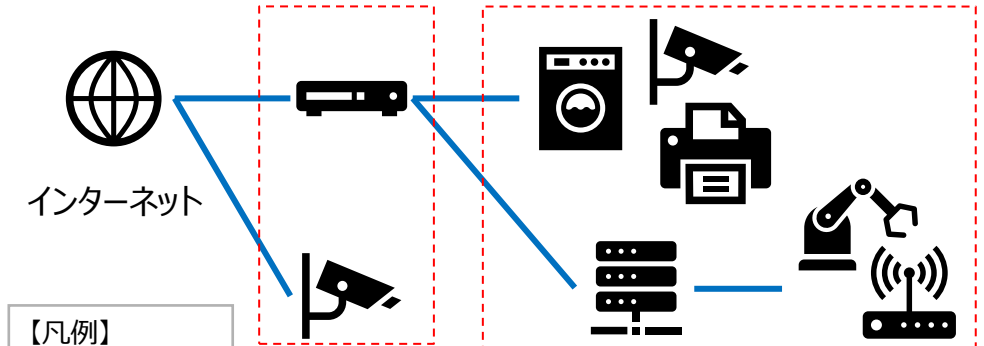
制度名称・ロゴ・ラベル

セキュリティ要件適合評価
及びラベリング制度
JC-STAR
(Labeling Scheme based on
Japan Cyber-Security Technical
Assessment Requirements)

JC-STAR

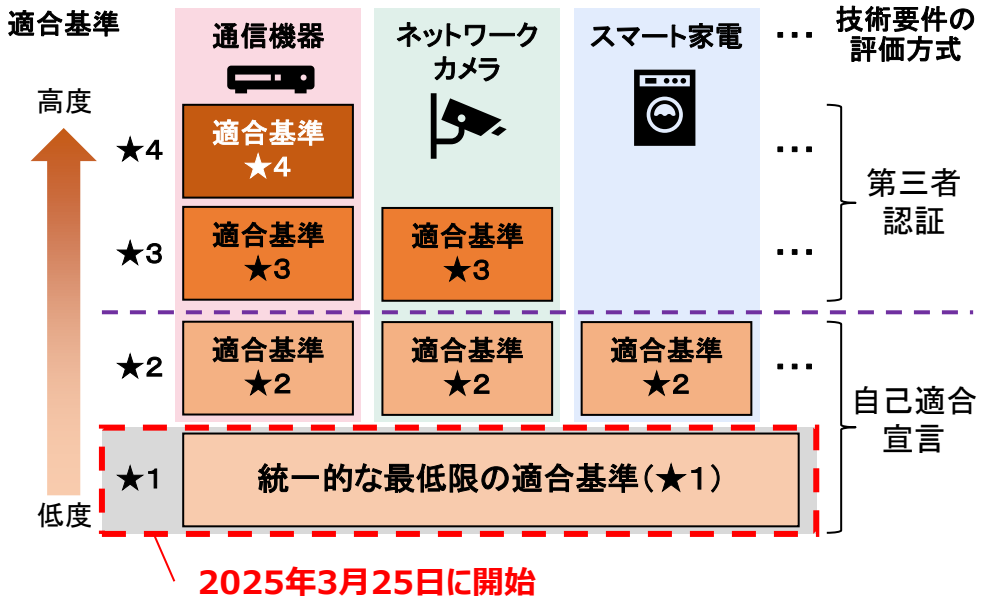
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

対象製品の概要



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

制度の概要（イメージ）



(※1) 経済産業省「ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会）」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html
(※2) 独立行政法人 情報処理推進機構（IPA）「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」https://www.ipa.go.jp/security/jc-star/index.html

関係国との制度・取組調和に向けた動き

- **IoTセキュリティ**については、**日米（首脳級）、日EU（閣僚級）、G7（首脳級）**等にて、**各国制度の相互承認に向けて取組む**旨合意。その他、シンガポール等の制度保有国とも交渉を実施。
- **ソフトウェアセキュリティ**については、**日米豪印（首脳級）でソフトウェア開発要件の国際ルール整備に向けて取組む**旨合意。その他、**SBOMの国際ルール整備**に向けて関係国と共に**国際文書（ガイドライン）の策定**を目指す。

バイ

日米首脳

（首脳ファクトシート、2024年4月）※IoT

日米両国は、**IoTのサイバーセキュリティ・ラベリング制度の相互承認を達成するため**の行動計画を策定するため、関連する専門家による作業部会を設置する予定である。

日EU閣僚

（デジタルパートナーシップ閣僚声明、2024年4月） ※IoT

それぞれの**製品セキュリティのフレームワーク…の互換性を促進するための取組を継続することで一致**した。双方は…**標準策定活動における専門家間の協力強化**や、志を同じくする他のパートナーとの調整を含め、協力することで一致した。

マルチ

G7首脳

（首脳コミュニケ、2024年6月） ※IoT・ソフトウェア

信頼性のあるサイバーセキュリティ上安全な製品の相互認証制度の確立に向けた方策を迅速に模索する。… 製造者に対し…**セキュアバイデザイン及びセキュアバイデフォルトとすることを強く促す。**

日米豪印首脳

（首脳声明、2024年9月） ※ソフトウェア

安全なソフトウェア開発要件及び認証の追求に向け…これらの**要件の国際調和を図る**ことで、政府ネットワーク用のソフトウェアの開発、調達及び利用の安全性確保…

目次

前回のWG1・分野横断SWG合同会議における主なご指摘

【サプライチェーン全体のセキュリティ対策強化について】

- 普及のインセンティブとどのように結び付けていくかを引き続き議論できればと思う。
- サプライチェーンについて数社ヒアリングしたが、2 社間で取引をする際に取引条件が生じるようである。ビジネスの上に立脚できるセキュリティを構想いただき、国際の場でも議論していただければと思う。
- 自動車業界では「自工会/部工会・サイバーセキュリティガイドライン」を既に運用する中、IPA の「中小企業の情報セキュリティ対策ガイドライン」との連携も図っているが、他の業界でも同様の必要性が生じる可能性がある。また、星の数による成熟度表示は業界によらず中小企業の良い指針になると思う。様々な既存のガイドラインに横串を刺す活動を一層強化して欲しい。
- 既存の認証制度の活用も含めてご検討されたい。
- セキュリティアーキテクチャについて、全体的な動きには賛成するが、IoT 製品の認証等も進められる中、事業者側の負荷が極端に上がらないよう配慮いただきたい。
- 全ての産業はつながっているため、ぜひ全ての業界が取り組める対策レベルの可視化を推進いただきたい。どのガイドラインにこだわるかということもなくなり、全体として進めやすくなるのではないか。中小企業を念頭に置くと、より簡便な取組みやすい施策について、サポートも含めて考えていくべきかと思われる。
- 第三者認証を含めた可視化について、横串を刺すものから業界特化のものまで基準ができるとありがたい。また、初期的なものはわかりやすいところからスタートし、レベルアップできる内容となっているとありがたい。

【産業分野別セキュリティ対策について】

- 半導体関連産業のセキュリティ確保について、ここでは、サイバー攻撃を外部から受けて製造やロジスティクスが停止する事例が扱われているが、単にオペレーションが停止するというだけでなく、中を流れる製品の品質にも課題があるようにも思われる。

サプライチェーン企業のセキュリティ対策評価制度の構築

- **サプライチェーンに起因するインシデントを背景**に、**企業の取引においてもセキュリティ対策の担保が求められる中**、受注企業が**異なる取引先から様々な対策水準を要求される**、発注企業は**外部から各企業等の対策状況を判断することが難しい**といった課題が存在。
- こうした課題に対応するため、サプライチェーンにおける重要性を踏まえた上で**満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組みの検討**を進めており、本年４月に**制度の概要を整理した中間とりまとめを公表**。今後、実証事業等を通じた**評価スキームの具体化**や制度の**利用促進のための施策の検討**等を進め、**2026年度中の制度開始**を目指す。

構築する評価制度（現時点案）

成熟度の定義	三つ星（★３）	四つ星（★４）	五つ星（★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プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施
評価スキーム	自己評価	第三者評価	第三者評価

※ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

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・複雑な自動車、半導体、主要製造業等において、優先的に本制度の利用を促進。

制度実現に向けた検討課題（例）

- **国内外の関連制度・評価制度との整合性確保、相互認証**
- 対策推進のための企業への支援の在り方（**専門家の活用促進**、**中小企業支援策との連動**、**評価機関の支援**）
- 下請法や価格転嫁に関する課題の整理
- 実効性の強化に向けた取組（政府機関や重要インフラ事業者等における活用推進、サプライチェーン上の取引先や投資家等の**ステークホルダとの対話での活用**等の促進）

（参考）サプライチェーン企業のセキュリティ対策評価制度について①

【制度において設ける段階の考え方】

- 先行する海外制度等の分析を通じて、★３については、一般的なサイバー脅威に対処しうる水準を目指すものとして規定。
  ★４は、初期侵入の防御に留まらず、内外への被害拡大防止・目的遂行のリスク低減によって取引先のデータやシステム保護に寄与する点や、サプライチェーンにおける自社の役割に適合した事業継続を推進している点を改めて明確化。
- ★５については、より高度なサイバー攻撃への対応として、自組織のリスクを適切に把握・マネジメントした上で、システムに対する具体的な対策としては既存のガイドライン等も踏まえた上で現時点でのベストプラクティスに基づく対策を実行する形を想定（★3・4の精査も踏まえ、今後さらに具体化）。
- 上位の段階はそれ以下の段階で求められる事項を包括するため、例えば、★3を事前に取得していなければ★4を取得できないという関係とはならない。

	★3	★4	★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**として、**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**として、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**として、**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プロセスを整備した**上で、**システムに対しては現時点でのベストプラクティスに基づく対策**を実施
脅威に対する達成水準（イメージ）	• **組織内の役割と責任が定義**されている。 • 一般的なサイバー脅威への対処を念頭に、自社**IT基盤**への初期侵入、侵害拡大等への対策が講じられている。 • インシデント発生時に、**取引先を含む社内外関係各所への報告・共有に必要な最低限の手順が定義、実施**されている。	• セキュリティ対策が**組織的な仕組みに基づいて実施され、継続的に改善**している。 • **取引先のシステムやデータを含む内外**への被害拡大や攻撃者による目的遂行のリスクを低減する対策が講じられている。 • **事業継続に向けた取組や取引先の対策状況の把握**など、自社の位置づけに適合した**サプライチェーン強靭化策が講じられている**。	• 組織において**国際規格等に基づくマネジメントシステム**が確立されている。 • **リスクを適宜適切に把握**した上で、インシデントに対して迅速に検知・対応するなど、**ベストプラクティスに基づくサイバーレジリエンス確保策**が講じられている。 • 取引先等への指導や共同での訓練の実施など、**自社サプライチェーン全体のセキュリティ水準向上に資する対策**が講じられている。
評価スキーム	**自己評価** （※）社内等の専門家による評価を想定	**第三者評価** ※第三者評価を原則とするが、評価コストの負担を抑える観点から詳細は今後検討	**第三者評価**
ベンチマーク （対象企業やリスクが同様であり、対策項目を検討する上で参考）	• 自工会・部工会ガイドLv1 • Cyber Essentials ⇒★3で対処する脅威等に照らして精査し、対策事項（案）を抽出	• 自工会・部工会ガイドLv2～3 • 分野別ガイドライン 等 ⇒★4で対処する脅威等に照らして精査し、対策事項（案）を抽出	• ISO/IEC27001 • 自工会・部工会ガイドLv3 等 （※）ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

（参考）サプライチェーン企業のセキュリティ対策評価制度について②

- レベルごと達成すべき「経営の責任」、「サプライチェーンの防御」、「IT基盤の防御」に資する対策を提案。

※1 以下は必ずしも全要求を網羅しているわけではない点に留意されたい。

※2 資料2の大分類のうち、ガバナンスの整備、リスクの特定、インシデントへの対応、インシデントからの復旧は「経営の責任」に、取引先管理は「サプライチェーンの防御」に、攻撃等の防御、攻撃等の検知は「IT基盤の防御」に該当

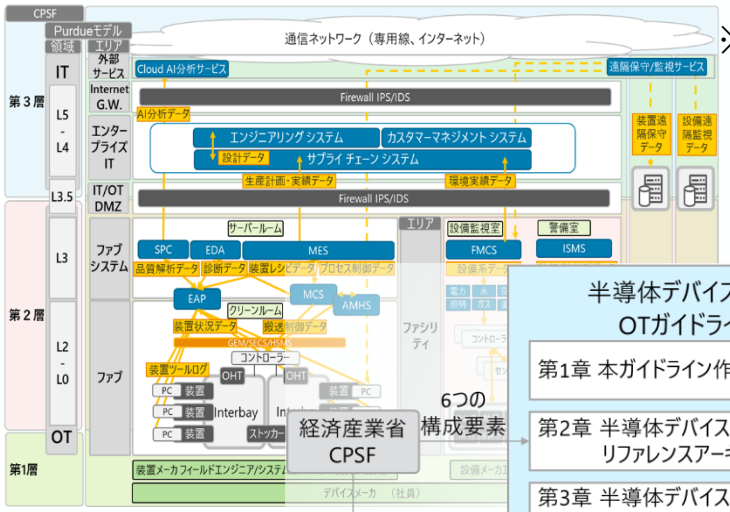
	★3（Basic）	★4（Standard）
経営の責任	**企業として最低限のリスク管理体制構築** • 自社のセキュリティ担当の明確化 [No.1] • セキュリティ対応方針の策定 [No.3] **インシデント発生に備えた対応手順の整備** • インシデント対応手順の作成 [No.25] **自社IT基盤や資産の現状把握** • 情報資産やネットワークの一覧化 [No.7,8] • 取引先等とのネットワーク接続の管理 [No.9]	**継続的改善に資するリスク管理体制の構築** • 定期的な見直しの実施 [No.6] • 定期的な経営層への報告、不備の是正等 [No.7] **インシデン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.44] **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.17] • 定期的な見直しの実施「No.6」（再掲）
サプライチェーンの防御	**取引先等に課す最低限のルールの明確化** • 接続している外部情報システムの一覧化 [No.5] • 他社との機密情報の取扱い明確化 [No.6]	**サプライチェーンにおける対策状況の把握** • 機密情報共有先の一覧化 [No.8] • 重要な取引先等の対策状況把握 [No.10] **取引先等との役割と責任の明確化** • インシデント発生時の他社との役割等の明確化 [No.11]
IT基盤の防御	**不正アクセスに対する基礎的な防御** • 基礎的なID管理手続き、アクセス権限の設定 [No.11,12,17] • パスワードの安全な設定及び管理 [No.15,16] • 内外ネットワーク境界の分離・保護 [No.23] **端末やサーバーの基礎的な保護** • ソフトウェアの適時のアップデート適用、不要なソフトウェアの削除 [No.20,21] • 端末等へのマルウェア対策 [No.22]	**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.29] • 社内システムにおける適切なネットワーク分離 [No.38] • 社外への不正通信の遮断(出口対策) [No.39] • 情報機器等の状態や挙動の監視・対応 [No.41] **迅速な異常の検知** • ログの収集・定期的な分析の実施 [No.35] • ネットワーク接続やデータ転送の監視 [No.40] • 情報機器等の状態や挙動の監視・対応 [No.41]（再掲） • 監視活動で検知された事象の分析 [No.42]

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**。
- 2024年11月に、国際的な枠組みとの整合も念頭に置きつつ、**半導体関連産業において求められるセキュリティ対策の具体化**に向けた検討を開始。**2025年度秋頃に公表**を目指し、とりまとめた対策基準を**経済産業省の投資促進関係施策の要件に紐付け**、**実効性を強化**していく。

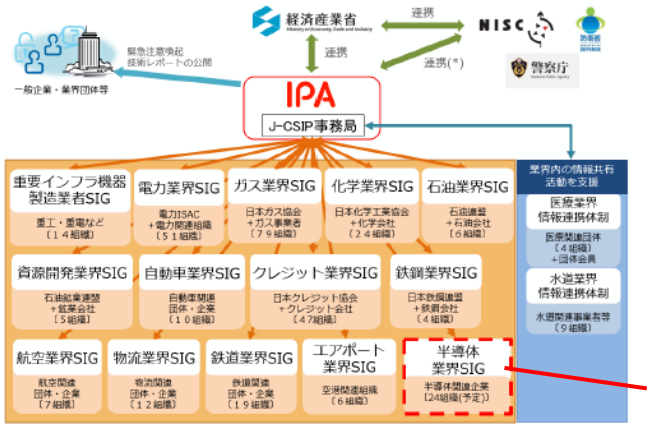
半導体デバイス工場におけるOTガイドライン（作成中）



※サプライチェーン企業のセキュリティ対策評価制度を活用しつつ、**OT分野における対策基準**を検討

※英訳版も作成し60日間のパブリックコメントを経て2025年秋頃公表予定

J-CSIP（サイバー情報共有イニシアティブ）半導体SIGの組成



J-CSIP
Initiative for Cyber Security Information sharing Partnership of Japan

高度な標的型サイバー攻撃に関する**情報共有の取組**。業界ごとにサブグループとしてSIG*を組成。IPAは、情報集約と共有のコーディネーションを担当。

*Special Interest Group

参加業界数：13、SIG参加組織数：284（2025年２月現在）

半導体業界SIGを2025年３月に発足

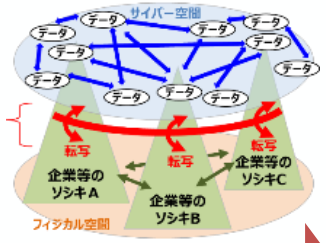
IPA ICSCoE 中核人材育成プログラムへの参加呼びかけ

- 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、１年を通じた集中トレーニング**
- **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**（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名）

サイバー・フィジカル・セキュリティ対策フレームワークが盛り込まれた国際規格の策定

- 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。
- 2023年10月にNP投票（提案段階）が行われ、賛成27票（内、積極参加8カ国）、反対1票、棄権27票となり、棄権除く2/3以上賛成および積極参加5カ国以上を満たして可決。
- **本件は2025年3月の国際会合にて承認段階（DTS）への移行が決定。**TS原案（DTS）合意後に投票を行い、2/3以上の賛成を得た場合TSが成立し、**2025年内の発行を目指す。**

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を提案

国際標準化団体へ提案

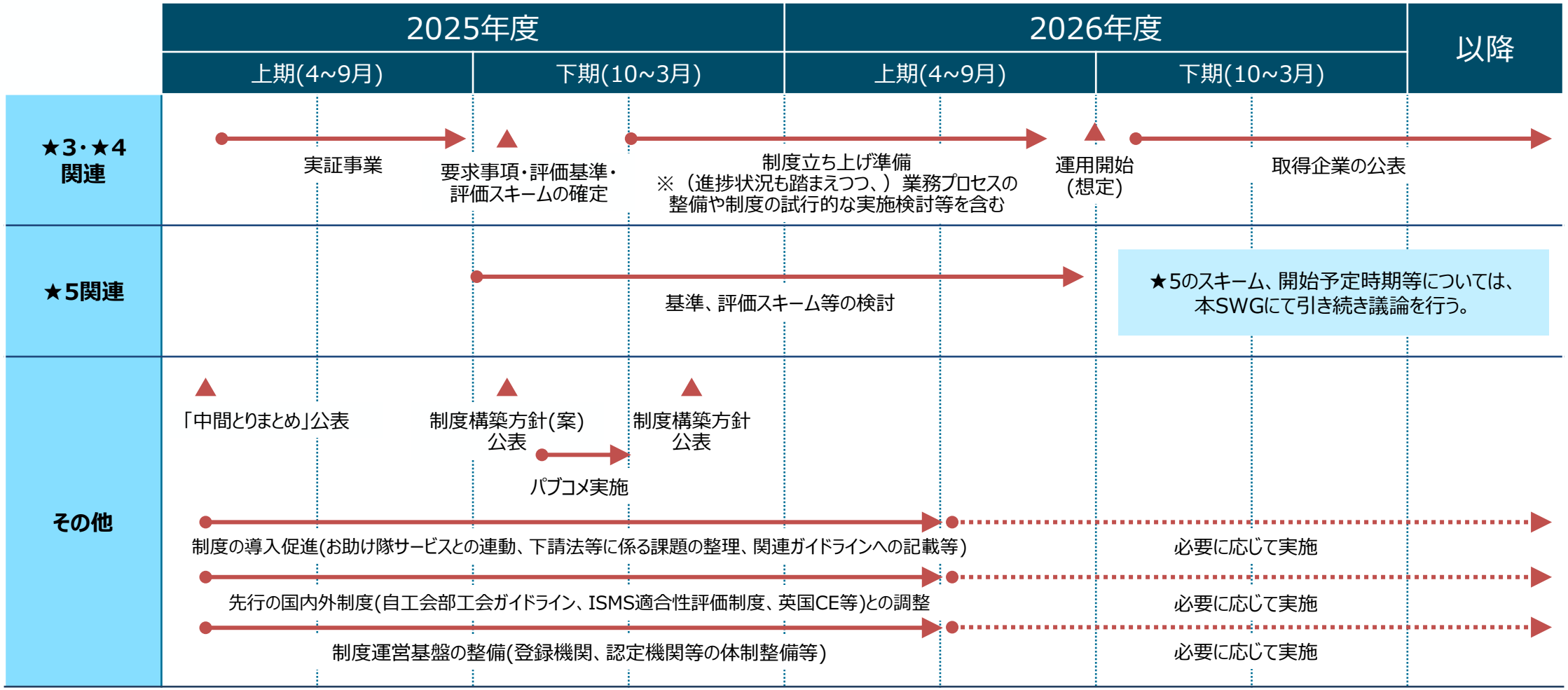
ISO / IEC
JTC 1
SC 27
WG4

区分	2023年度		2024年度			2025年度
国際標準化提案先イベント	2023/4 定期会合 ★	2023/10 定期会合 ★	2024/7 中間会合 ★	2024/10 定期会合 ★	2025/3 定期会合 ★	2025/7 中間会合 ★
CPSFをベースとした国際標準化ステップ	NP(再) PWI(再)で検討した内容をベースに再度投票を実施		作成段階 ● 担当する委員会の指名するエキスパートが作業原案(WD)を作成する。			承認段階 ● エディタがTS原案(DTS)を作成する。 ● 委員会メンバーの2/3以上の賛成を得ることで、原案を技術仕様書として発行するよう要請できる。 国際規格(TS等)発行

目次

サプライチェーン対策評価制度の一層の具体化

- 来年度においては、**実証事業等を通じて★3・★4の要求事項・評価基準や評価スキームを具体化**するとともに、**制度運営基盤の整備や利用促進のための施策の具体化**等を進め、 **2026年度の制度開始を目指す**。



セキュア・バイ・デザインの実行性担保に向けた今後の方向性

- セキュア・バイ・デザインの具体化に向けて、これまでIoT製品に関する制度（JC-STAR）／ソフトウェアセキュリティ確保のための取組の具体化（SBOM／SSDF／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）を進めてきたが、今後これらの実行性を担保すべく以下の取組を進めていく。

① **制度のさらなる具体化**（JC-STAR制度における高度な基準（★2以上） の整備）

② **海外との相互連携の推進**（JC-STAR制度及びSBOMの国際ルール整備における関係国との連携）

③ **ガイドライン等活用における自己適合宣言の枠組み構築**（SSDFやサイバーインフラ事業者に求められる役割）

JC-STAR制度

- 特定分野のシステムにおいて、**政府調達での活用を見込むより高度な基準（★2以上） の整備**を進めており（※）、**★2については2025年度下期での策定を目指す**。
- ★取得企業数の拡大に向けて、特に**中小IoTベンダーにおける申請負担軽減**を図るべく、**必要な支援策を検討**する。
- まずは政府機関等が★取得製品を積極的に活用し、セキュリティ強化を図るとともにそうした製品の需給のエコシステムを構築すべく、**政府機関等へのラベル取得済みIoT製品調達の必須化／重要インフラ事業者・地方公共団体の調達ルールでの制度活用**を、**関係機関とも調整しながら積極的に働きかける**。
- 国内IoT製品ベンダーの負担を抑えるため、類似制度を有する**諸外国（米国、欧州、シンガポール等）との相互承認に向けた調整を加速化**する等、連携を一層強化していく。

（※）現在、ネットワークカメラ・ルーターといった製品やスマートホーム・電力・金融・流通関連端末のような特定領域において★2の基準検討・議論を進めているところ。

ソフトウェア・セキュリティ

<SBOM>

- **SBOMの重要性の発信／運用する上での国際ルールを整備**し各国での取組の融和を狙った**国際文書（ガイドライン）の策定**を、関係国とも連携しつつつ目指す。

<SSDF>

- 我が国での産業実態との調和を図り、事業者から活用されうる成果物を策定すべく、**社会的影響の大きな分野（例：電力・金融 等）を対象にした実証事業**／SSDFと国内ガイドラインのマッピングを踏まえた**国内ガイドラインの不足事項への対応検討**も行った上で、**SSDF導入ガイダンスを策定**する。
- 政府調達等での活用も見据えて、国内事業者によるガイダンスへの適合がわかりやすく示されるよう、**自己適合宣言の枠組みを構築**する。

<サイバーインフラ事業者に求められる役割>

- **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した上で、**政府調達等での活用も見据えて、国内事業者によるガイダンスへの適合がわかりやすく示されるよう、**自己適合宣言の枠組みを構築**するとともに、将来的には分野別の普及を進める。

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**。

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。
- **ガイドライン Ver 2.0を公開（2024年３月）。**

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）**。
- ERABサイバーセキュリティガイドラインの改定に向けて作業中。

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。ガイドライン2.2版を公開（2024年8月）**。
- 工場領域や販売領域セキュリティの課題対応についても検討中。

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）**。

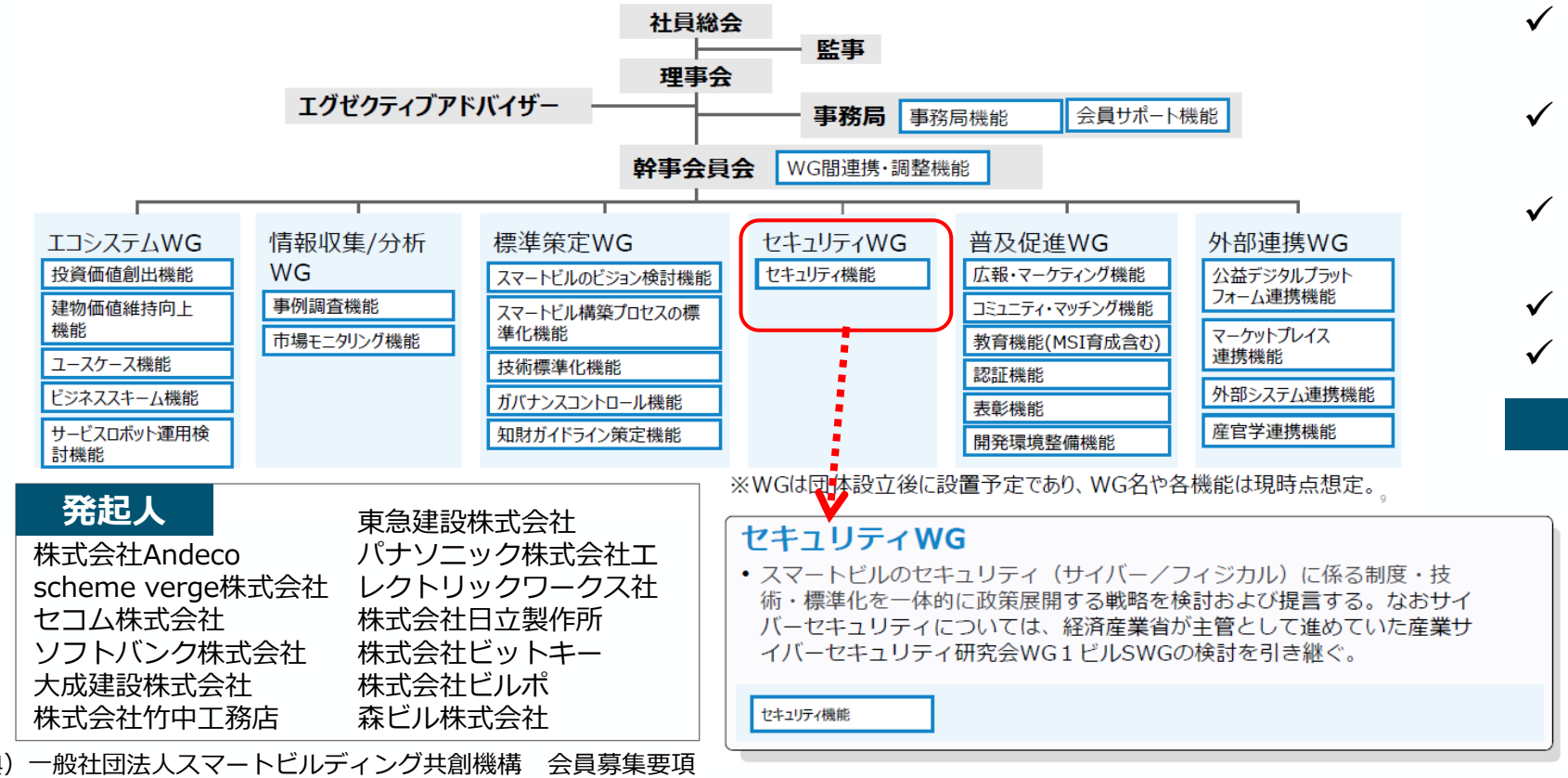
半導体産業SWG

- 半導体デバイスメーカーや製造装置メーカーを含めた半導体関連の企業・団体等が議論や情報交換を行う場として**新設（2024年11月）**。
- 現在、**半導体デバイス工場におけるOTガイドラインを作成中**。英訳版も作成し、パブリックコメントも実施して2025年秋頃公表予定。

ビルSWG（座長：東京大学 江崎教授）

- 2023年11月に開催した第16回会合において、設立が予定されるスマートビルに関する**コンソーシアムへ本SWGを合流**することが諮られ、**多数の賛成意見**が得られた。
- 2025年4月2日に**「一般社団法人 スマートビルディング共創機構」が発足**したところ、現在、同機構への本SWGの合流を前提として、**合流後の体制や検討事項についての調整を実施**中。

スマートビルディング共創機構の体制（会員募集時点での想定）



※WGは団体設立後に設置予定であり、WG名や各機能は現時点想定。

セキュリティWG

- 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および提言する。なおサイバーセキュリティについては、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の検討を引き継ぐ。

セキュリティ機能

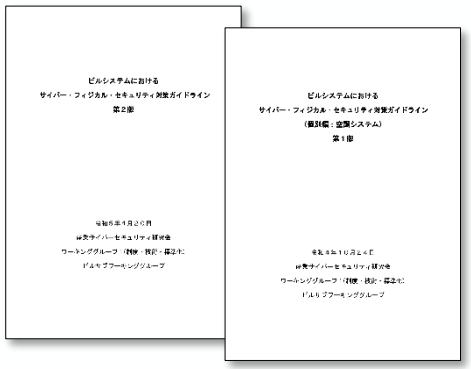
発起人

株式会社Andeco	東急建設株式会社
scheme verge株式会社	パナソニック株式会社エレクトリックワークス社
セコム株式会社	株式会社日立製作所
ソフトバンク株式会社	株式会社ビットキー
大成建設株式会社	株式会社ビルポ
株式会社竹中工務店	森ビル株式会社

本SWG合流後の検討事項（案）

- ✓ ビルSWGが作成したガイドラインのメンテナンス
- ✓ 新たなガイドラインの作成（例：スマートビル編）
- ✓ JC-STAR制度における★２以上のセキュリティ要件に係る検討
- ✓ ビルSOCやビルISACに関する議論
- ✓ レガシービルに関する検討

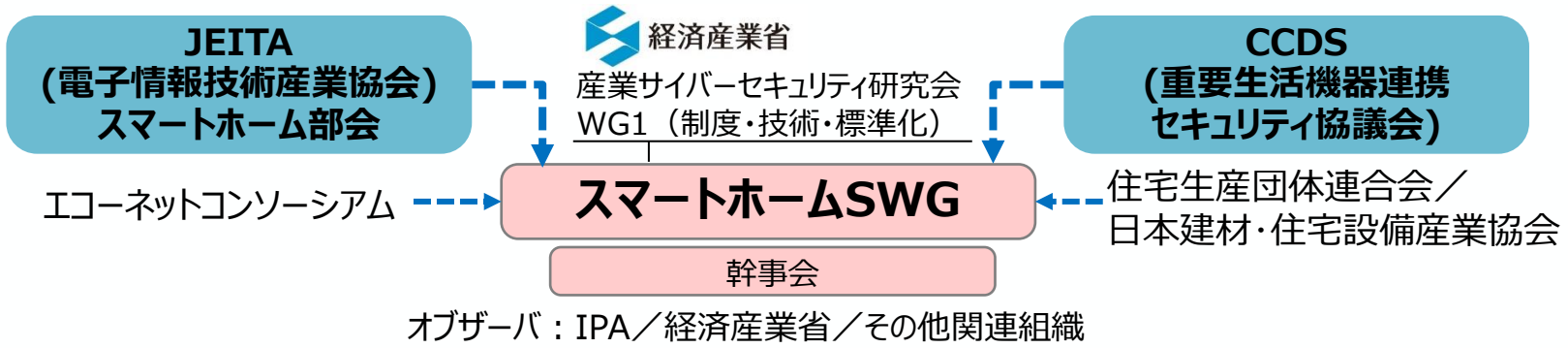
ビルSWGが作成したガイドライン



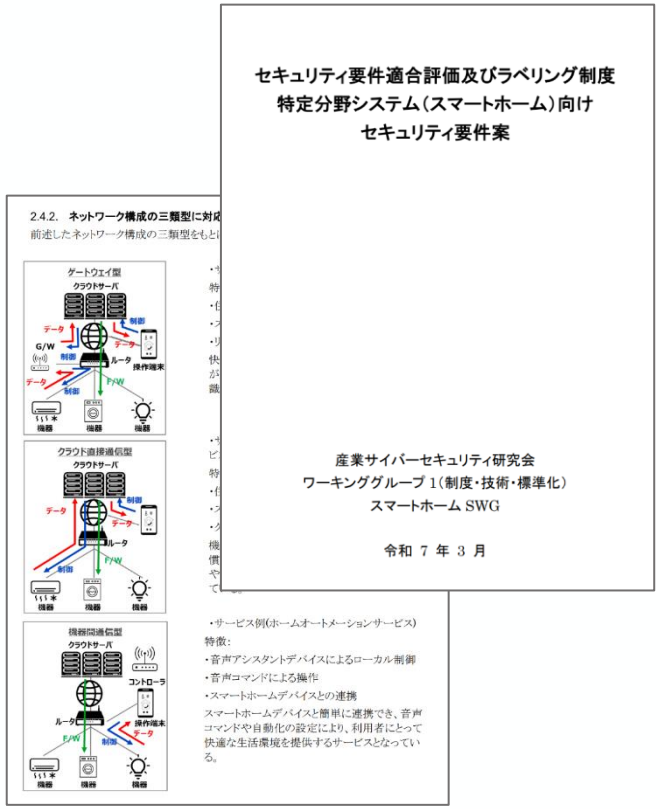
（出典）一般社団法人スマートビルディング共創機構　会員募集要項
https://www.ipa.go.jp/digital/architecture/conferences/smartbuilding-association/membership-info.html

スマートホームSWG （一般社団法人 電子情報技術産業協会）

- 2024年度は、スマートホームで使用されるIoT製品のセキュリティについて、JC-STAR制度の★2の整備・活用を視野に入れたセキュリティ要件の検討を実施。
- CCDS等の関係団体の参加・協力を得て、2024年7月～2025年1月に合計4回のSWGを開催。2025年3月にセキュリティ要件案を取りまとめた報告書を提出。



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：
- **評価基準検討**
  - スマートホームの定義
  - スマートホームで実施すべきセキュリティ対策の検討
  - スマートホーム関連の各IoT製品類型におけるIoTセキュリティラベル★１の活用及び★２以上の整備要否の検討
  - ★２以上の整備について、JC-STAR制度（IPA+経済産業省）への依頼
- **普及促進検討**
  - スマートホームの普及・セキュリティ対策状況の現状確認、セキュリティを考慮した普及促進策の検討
  - IoT製品の販売・購入の促進施策の検討、IoT製品類型の活用に関する製品ベンダー、調達関係者との合意

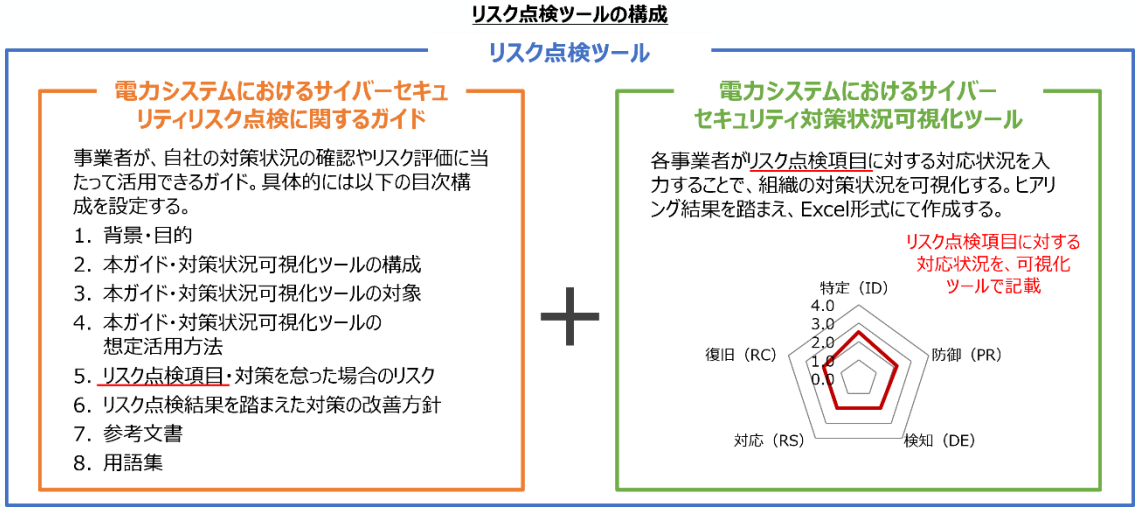


（出典）2024年度第1回スマートホームSWG資料に基づき経済産業省作成

電力SWG（座長：名古屋工業大学 渡辺教授）

- **電力分野におけるサプライチェーン・セキュリティ向上策に関する提言を公表**し、改定が進められている「**電力制御システムセキュリティガイドライン**」に反映すべく調整。また、**「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）し、**電気事業者の活用を推進**。
- **ERABサイバーセキュリティガイドライン**を改定（Ver2.0⇒3.0）。2025年5月に公表予定。

リスク点検ガイドと対策状況可視化ツール



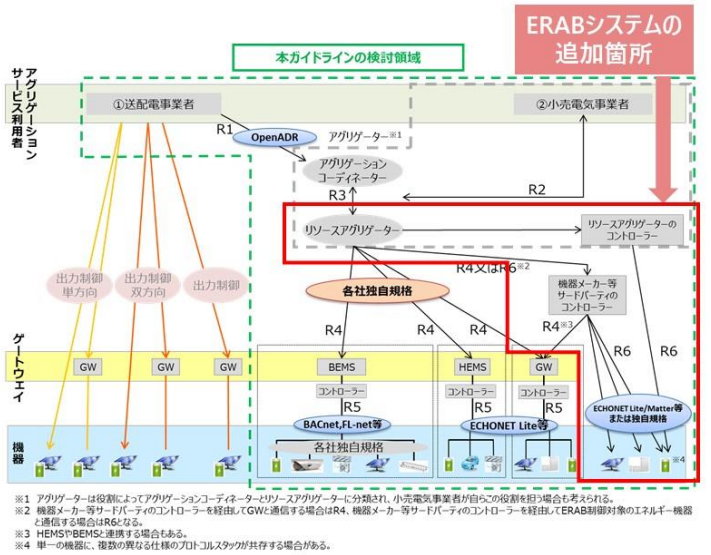
- ✓ 2024年度の電力広域的運営推進機関の会員（**電気事業者**）に対する**セキュリティ自己診断の取組に際しリスク点検ツールを活用**。ツールの使い方に関する説明会を2 回開催。
- ✓ 合計797社から診断結果の回答があり、送配電事業者、小売電気事業者、発電事業者の順番で回答率が高かった。今年度以降も継続して実施し、傾向を把握していく。

ERABサイバーセキュリティガイドラインの改定について

(参考)
ERABサイバーセキュリティガイドラインの改定点について

（出所）第18回電力SWG 資料6-3を一部修正

- 単一の機器に複数の異なる仕様のプロトコルスタックを共存させる方法を用いて、複数の異なる事業者(リソースアグリゲーター、機器メーカー等サードパーティ)が、同一のERAB制御対象のエネルギー機器との通信・制御を実施するユースケースを追加。
- 機器メーカー等サードパーティのコントローラーを経由して、直接または需要家側のルータ経由でのERAB制御対象のエネルギー機器との通信・制御を実施するユースケースを追加。



① 物理的なGWを介さないDRサービス
これまでのガイドラインでは、機器を制御する際に物理的なGWを介することを主に想定していた。このGWがクラウド上にある場合もしくは物理的なGWを介さない場合の対応を記載。

② 末端のIoT機器等の脆弱性に起因する脅威
インターネットに接続されるIoT製品の数が急速に増加したことに伴い、IoT製品の脆弱性を狙ったサイバー脅威も増加傾向にある。そこで、「IoT製品に対するセキュリティ適合性評価制度」を参考に記載。

③ アグリゲーターが機器から取得する情報に起因するリスク
機器の利用状況から、利用者の在・不在が推測できる情報等、制御対象機器に関連する情報が多様化したことによるセキュリティリスクが懸念されている。
本リスクを踏まえた対応を記載。

（出典）第87回 総合資源エネルギー調査会 電力・ガス事業分科会 電力・ガス基本政策小委員会 資料7

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。
- **2024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 2.2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。

＜2024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2.2版」を公開。**
- 2024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向け説明会を開催（4回合計で4,000社、6,000人が参加）
- 自己評価集計結果（3,100社が提出）は例年通り３月末に公表予定
- 部工会と連携したセキュリティに関するサプライヤー向けの相談会（11回延べ140名参加）やインシデント実例をもとにしたセミナー（3回延べ160名参加）も開催

（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）

- **2024年3月にガイドライン Ver 2.0を公開**。2024年度は、民間事業者におけるガイドラインの活用状況や課題等の調査を行うとともに、官民連携拡大に向けた取組を実施。
- また、情報共有の枠組みに関して、民間事業者中心の取組である「スペースセキュリティ勉強会」を母体として、宇宙分野におけるサイバーセキュリティに関する情報共有を行う**「一般社団法人Japan Space ISAC」が、2024年11月に設立**。

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

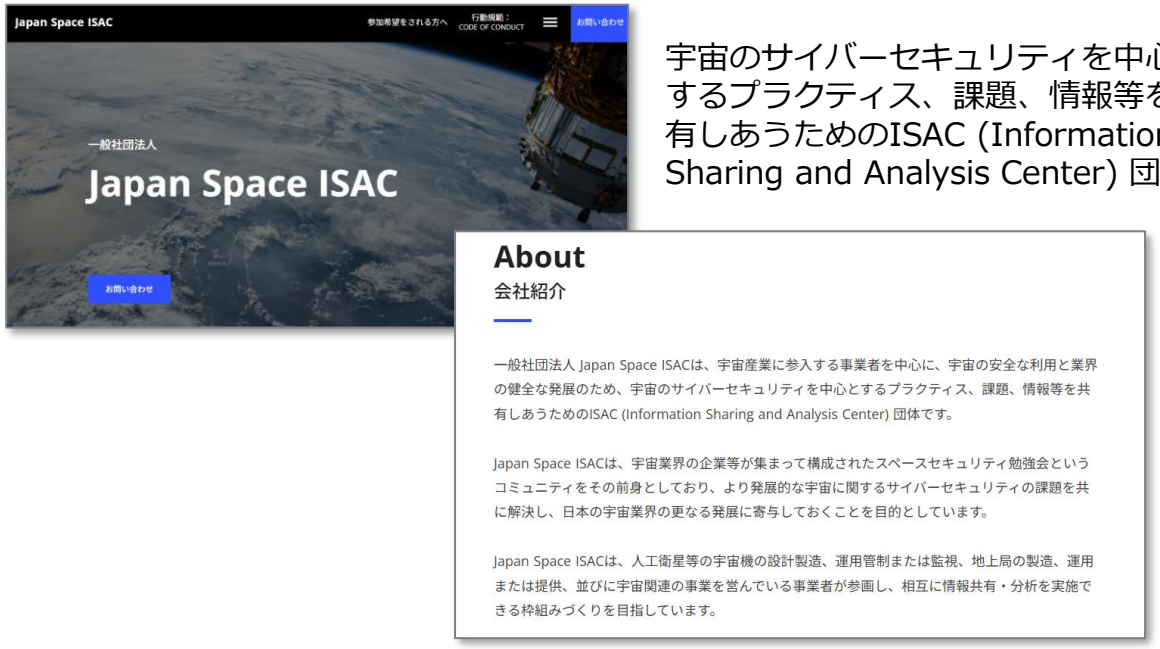
について分かりやすく整理して示し、民間事業者における自主的な対策を促すことを目的としています。

- 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）

ガイドラインVer 2.0では、ガイドラインの対象とする宇宙システムを拡大し、想定されるリスクや対策の見直しを実施。

また、民間事業者が活用できる情報セキュリティ関連規定の雛形を添付資料に追加。

一般社団法人Japan Space ISACの設立



宇宙のサイバーセキュリティを中心とするプラクティス、課題、情報等を共有しあうためのISAC (Information Sharing and Analysis Center) 団体

（出典）Japan Space ISAC https://japan-space-isac.jp/

工場SWG（座長：東京大学 江崎教授）

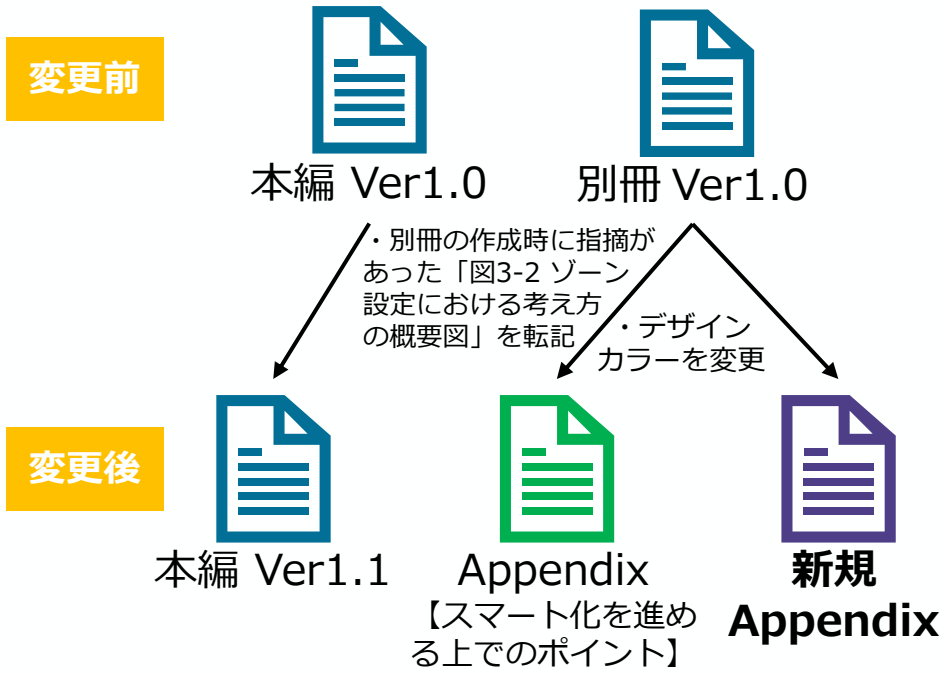
- 主に中小規模の工場を有する製造事業者の経営層や工場のセキュリティ担当者として選任された方を対象に、ガイドライン本編※1の内容をより分かりやすく解説し、具体的な事例・手順を示した解説書として**新規Appendix【工場セキュリティの重要性と始め方】※1を作成**（2025年4月11日公表）
- **工場ガイドライン※2,3の構成変更**を実施。別冊をAppendixにデザインカラーも変更してVer1.1へ改版

Appendix【工場セキュリティの重要性と始め方】

※経営層向けのチラシも作成

目次

ガイドラインの構成変更



※１：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 Appendix 【工場セキュリティの重要性と始め方】
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_appendix02.pdf
※２：工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.0.pdf
※３：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【別冊：スマート化を進める上でのポイント】
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_appendix.pdf

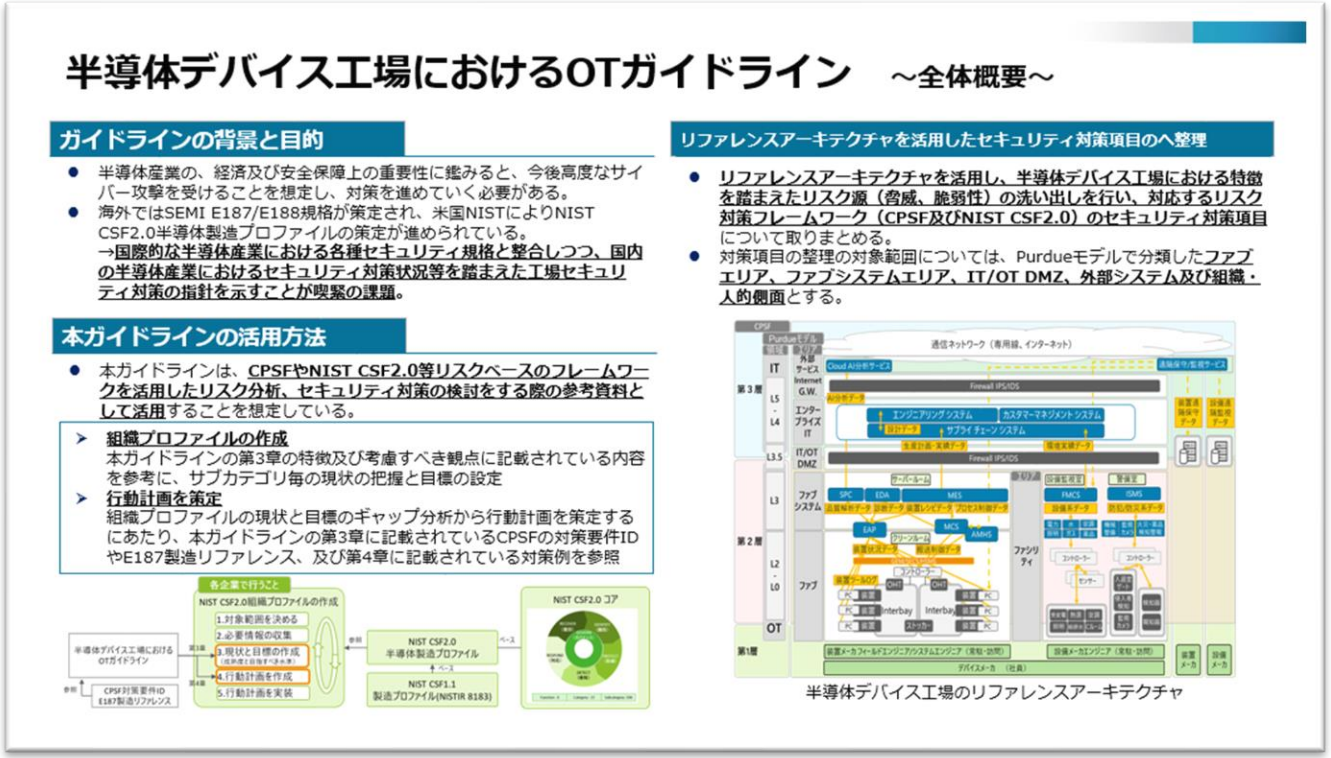
半導体SWG（座長：東京大学 江崎教授）

- 産業サイバーセキュリティ研究会WG1の下、第１回半導体産業SWGを開催（2024年11月）。
- デバイスメーカーや製造装置メーカーを含めた様々な企業・団体等が参加し、**我が国の半導体産業におけるサイバーセキュリティのあり方や守るべき対象技術などを議論する**とともに、**サイバーセキュリティ対策への取組、問題意識や事例等、相互に情報共有を行う**。

委員名簿

	秋山 裕明	マイクロンメモリジャパン株式会社
	飯嶋 織行	東京エレクトロン株式会社
（座長）	江崎 浩	東京大学
	高橋 清文	株式会社ニコン
	高原 正裕	株式会社ダイフク
	中川 昭一	（一社）電子情報技術産業協会 半導体部会
	長野 茂樹	株式会社SCREENホールディングス
	浜島 雅彦	SEMIジャパン
	東 健介	株式会社アドバンテスト
	藤井 俊郎	Rapidus株式会社
	三井 豊興	（一社）電子情報技術産業協会 半導体部会
	渡部 潔	（一社）日本半導体製造装置協会

半導体デバイス工場におけるOTガイドライン（作成中）



セキュア・バイ・デザインの実践向けた取組（ソフトウェアのセキュリティ確保）

- 2025年度内に**関連するガイドラインの成案化**を進めつつ、**自己適合宣言の枠組み構築・政府調達の要件化等**を通じて、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

＜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成案化**する。
- 政府調達等での活用も見据え、国内事業者によるガイダンスへの適合を分かりやすく示す**自己適合宣言の枠組みを構築**する。分野別の普及を進める。

＜SSDF（安全な開発）の促進＞

- **SSDF導入ガイダンスを策定**する。
- 政府調達等での活用も見据え、国内事業者によるガイダンスへの適合を分かりやすく示す**自己適合宣言の枠組みを構築**する。

＜SBOMの活用促進＞

- **SBOM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、関係国と連携しつつ**国際文書（ガイダンス）の策定**を目指す。

概念、枠組み (What)

具体化、事例化 (How)

運用

CISA “Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software”

NIST “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities”