経済産業省

サイバー攻撃の現状と
サイバーセキュリティ政策

２０２６年８月

経済産業省 商務情報政策局
サイバーセキュリティ課

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。
- 2026年７月、㈱ニチレイにおいて、**サイバー攻撃による不正アクセスにより**個人情報の漏えい可能性を確認。**被害サーバ停止に伴い、冷蔵倉庫の入出庫業務及び冷凍食品の出荷業務を停止**し、外食・小売事業者への商品供給に影響が発生。

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

（参考）高性能AIによるソフトウェア脆弱性の早期発見

- ４月７日、米国アンソロピック社がソフトウェアの**脆弱性※の検査について高い能力**を有する汎用型次世代フロンティアAIの**Claude Mythos Preview**を発表。
- ソフトウェアの脆弱性については、これまで発見に数週間～数か月かかっていたものが、**Mythosでは数分～数時間で発見可能**、かつ、**人間では発見困難だった脆弱性も発見可能**となる。
- なお、Mythosに限らず、脆弱性の検査に係る高性能AIとしては、これまでもGoogle（BigSleep）やOpenAI（Codex Security、GPT-5.4-Cyber）等によっても開発・公表されている。

※脆弱性とは、プログラムのバグや設計上のミスが原因で発生するセキュリティ上の弱点。**サイバー攻撃の「入口」となる**ため、**脆弱性が残された状態でシステム等を利用していると、外部から攻撃を受ける等の危険性**がある。そのため、**脆弱性が発見された場合は、修正プログラム（パッチ）の適用やアップデートによる迅速な対策が必要。**
※脆弱性が公開されてから、パッチ適用等をする前に、当該脆弱性を利用して攻撃される脅威も存在。

- こうした高性能AIについては、未知の脆弱性の発見・是正の加速にも繋がり、ソフトウェアの開発者・提供者が有効に活用することで、**社会全体のサイバーセキュリティの向上につながることが期待。**
  一方、悪意ある者に用いられた場合、脆弱性に対応できていない組織への**侵入リスクが高まる懸念**も。
- 特に、重要インフラ事業者については、サイバー攻撃によって、**情報の窃取のみならず、事業活動の停止やインフラの機能停止にもつながり得る**ことから、**上述したリスクには徹底した対応が必要。**

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”

２．政府全体のセイバーセキュリティ政策

サイバー対処能力強化法及び同整備法の概要

趣　旨

- 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。
- 国家安全保障戦略に掲げら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、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（令和６年６月７日～11月29日）、「サイバー安全保障分野での対応能力の向上に向けた提言」を取りまとめ。

→　これらを踏まえ、「新法」及び「整備法」として必要な法制度を整備。

概　要

官　民　連　携　（新法）

- 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
- 情報共有・対策のための協議会の設置
- 脆弱性対応の強化

通信情報の利用　（新法）

- 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
- （同意によらない）通信情報の取得
- 自動的な方法による機械的情報の選別の実施
- 関係行政機関の分析への協力
- 取得した通信情報の厳格な取扱い
- 独立機関による事前審査・継続的検査　等

→ 分析情報・脆弱性情報の提供等 ←

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・在日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　（サイバーセキュリティ基本法改正）
- サイバーセキュリティ戦略本部の機能強化　（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。

高性能AIに関する政府の対策パッケージ（Project YATA-Shield）

* Yielding Advanced Threat Awareness with AI

- フロンティアAIモデルによるサイバーセキュリティ性能が向上する中においても、我が国のサイバーセキュリティが確保されるよう、**政府全体としての対策パッケージを取りまとめ。**

基本的な認識・考え方

重要インフラ事業者等・政府機関等が取るべき対応

- **発見された脆弱性のパッチ適用やリスク緩和措置**を速やかに実施（リスクベース）
- **基本的な対策、多層防御の実施、インシデント発生時の備え**　等

※英国・米国政府の注意喚起も参考に

脆弱性を発見するAIの進化

- **Anthropic（Project Glasswing）**：Mythosへのアクセスを、**ビッグテックや重要インフラ等**に限定。
- **OpenAI**：GPT-5.5-Cyberへのアクセスを、**一部の認証者**に限定して付与。

実施する施策

重要インフラ事業者等・政府機関等への対応

① **重要インフラ事業者等への注意喚起等**
② **金融分野での先行的な取組 及び 他分野への展開**
③ **人材育成支援**
④ **政府機関等の情報システムにおける対応**

脆弱性の発見・修正等への対応

① **外国政府機関やビッグテック等との更なる連携**
② **ソフトウェア・ベンダへの注意喚起**
③ **AISIによる技術支援等**
④ **技術開発の推進**
⑤ **高性能AIを活用したサイバー対処能力強化**

高性能AIへの対応に関する関係機関への注意喚起

- 対策パッケージ「Project YATA-Shield」の取りまとめ・公表を行い、**重要インフラ事業者等、政府機関等、ソフトウェア・ベンダへの注意喚起**を公表・実施。

重要インフラ事業者等

●経営層のリーダーシップの下での対策の実施

→ 必要な投資と捉えて、組織のリスクマネジメントとして実施

●基本的な対策の確実な実施等

英：基本的な対策
米：隔離・復旧
} が重要

→ 資産管理、脆弱性対策、インシデント対応・復旧など（重要インフラ統一基準）

→ 実施状況の機動的な確認

●高速化する脆弱性の発見・修正等への対応

→ 脆弱性のリスク評価、パッチ適用・リスク緩和措置の速やかな実施

政府機関等

●組織トップのリーダーシップの下、対応の徹底を要請

●基本的な対策の徹底

英：基本的な対策
米：隔離・復旧
} が重要

→ 資産管理、脆弱性対策、インシデント対応・復旧など（政府統一基準）

→ 実施状況の機動的な確認（各機関・NCOによる監査）

●脆弱性対策の強化

→ パッチ管理・適用の運用設計の見直し、パッチ適用・リスク緩和措置の速やかな実施

ソフトウェア・ベンダ

●高性能AIも活用しながら、**脆弱性の早期発見・対応**

① リリース前のソフトウェア

→ 脆弱性を低減させた上でリリース

② リリース後のソフトウェア

→ 脆弱性の把握、パッチの早期作成、顧客への早期提供

３．経済産業省におけるサイバーセキュリティ政策

経済産業省のサイバーセキュリティ政策の全体像

- 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
- 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等）
- サプライチェーン対策評価制度の構築（対策水準の可視化）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

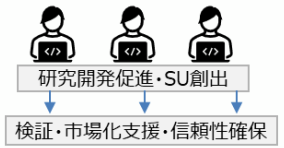
③政府全体でのサイバーセキュリティ対応体制の強化

- IPAのサイバー情勢分析能力強化
- 改正保安３法を踏まえたサイバー事故調査体制の構築
- 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

サイバー・フィジカル・セキュリティ対策フレームワーク

SC対策強化

- 2019年4月に「Society5.0」によって柔軟化・拡張するサプライチェーンに求められる**セキュリティへの対応指針**として、「サイバー・フィジカル・セキュリティ対策フレームワーク」（**CPSF**）を策定。

※「Society5.0」においては、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**。

「Society5.0」以前

個々の企業主体の定型的なつながりで価値を生み出す

<3層構造>

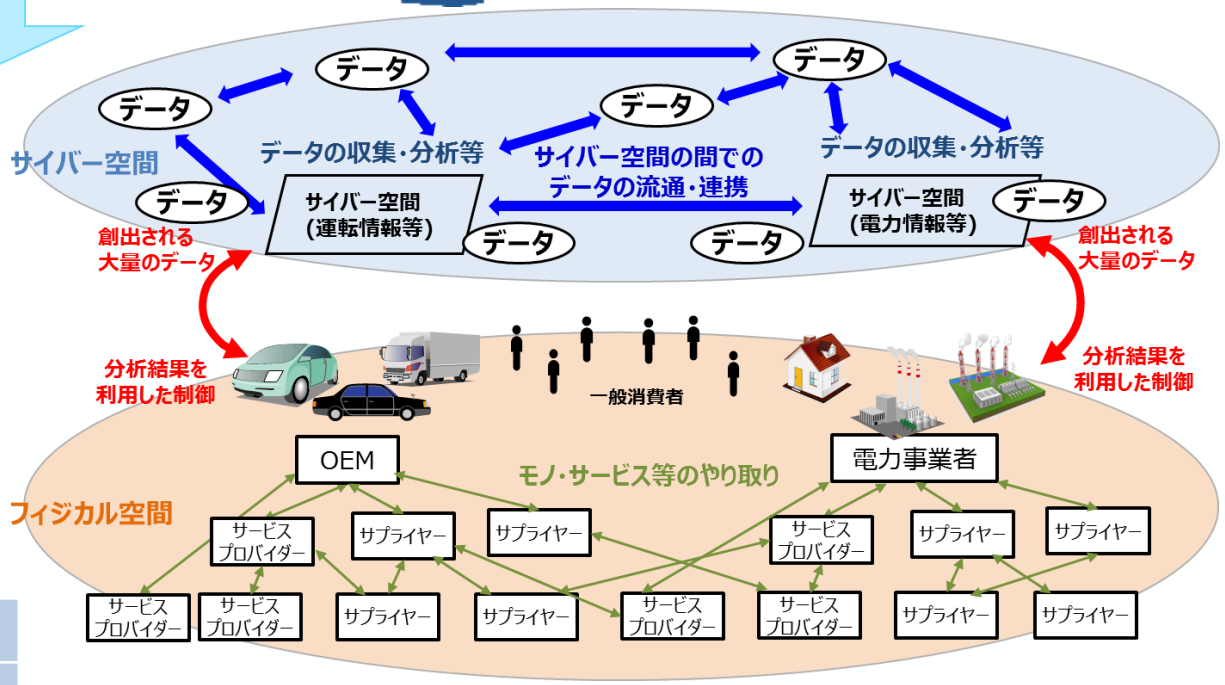
【第３層】
サイバー空間におけるつながり

【第２層】
フィジカル空間とサイバー空間のつながり

【第１層】
企業間のつながり

<6つの構成要素>

ソシキ	ヒト	モノ
データ	プロシージャ	システム



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

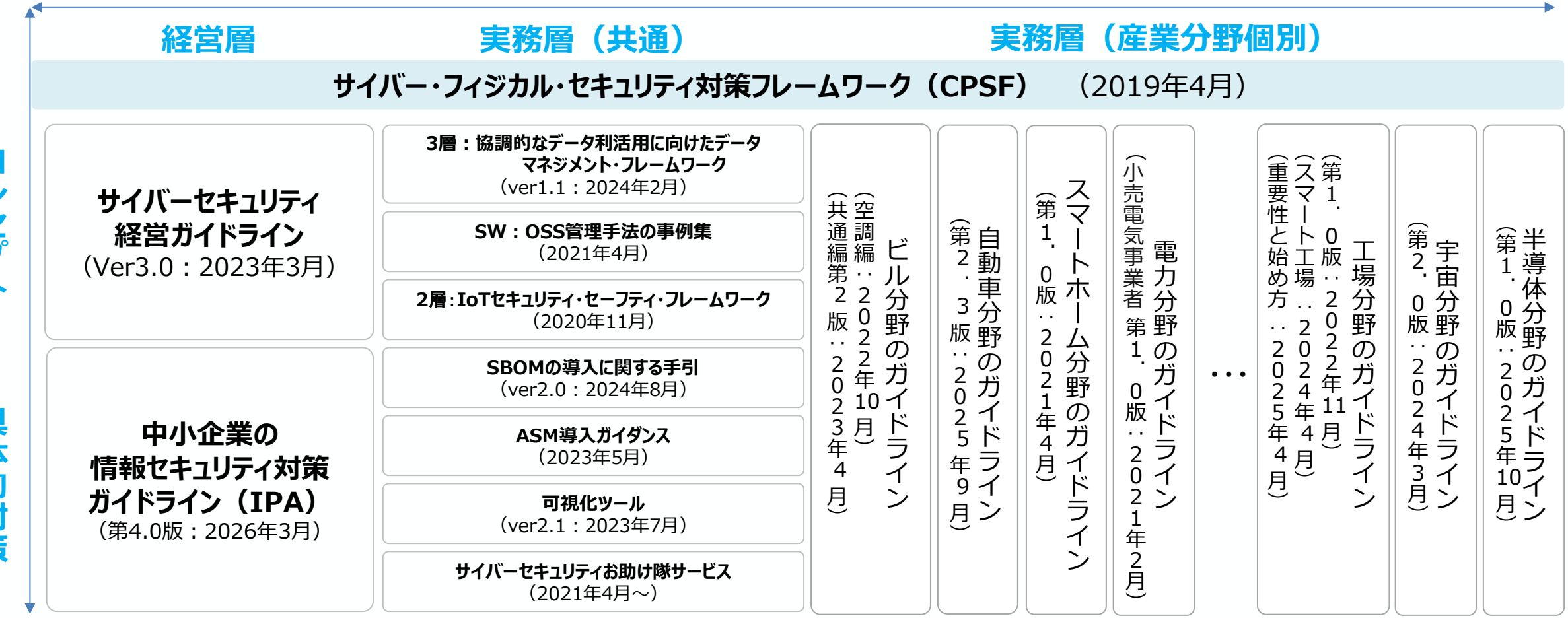
企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

CPSF関連ガイドライン

SC対策強化

- 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



中小企業支援施策の全体像

SC対策強化

- 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４７万件**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、2026年3月末時点で約**10,900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

SC対策強化

- 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、 2026年3月末時点で**約10,900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**

サービス提供 → **中小企業** → 自社の信頼性をアピール → **取引先**（大企業等）

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）

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

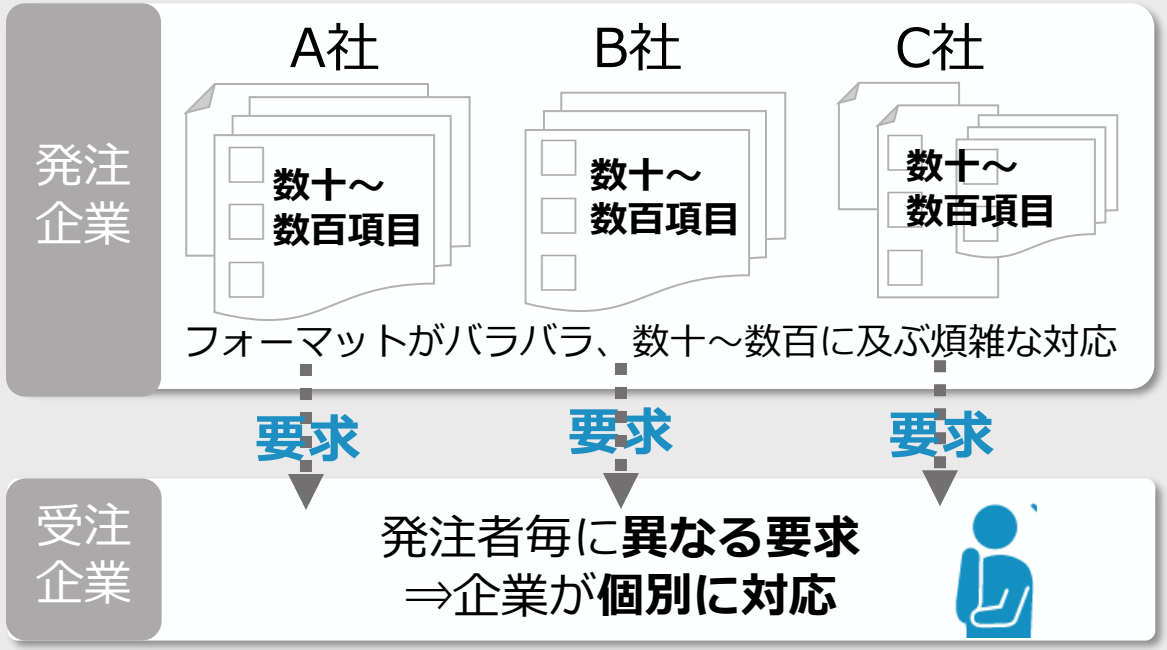
サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

（参考）中小企業がSCS評価制度の“★”を取得するメリット

SC対策強化

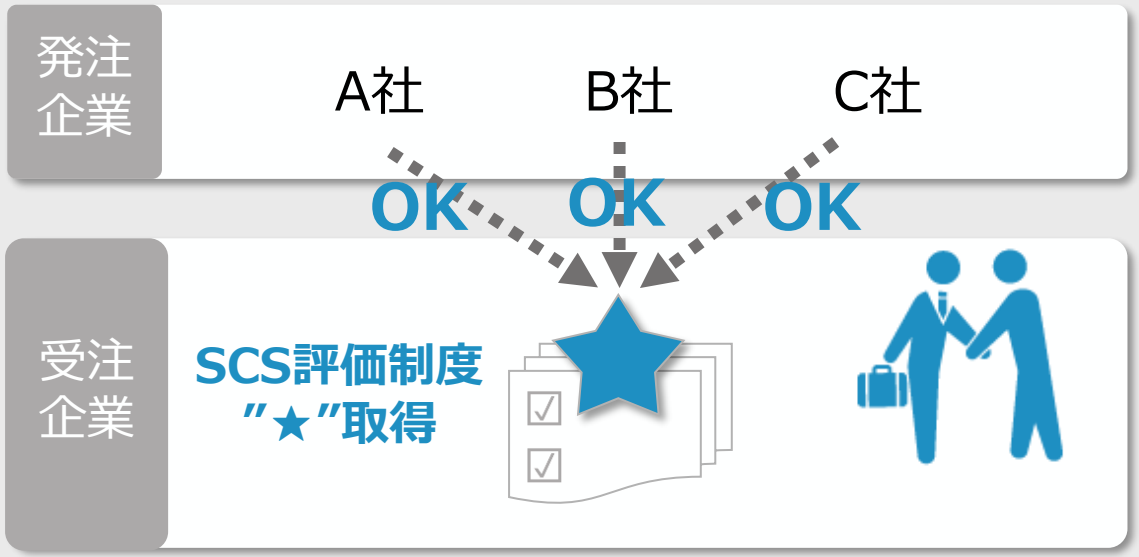
発注者ごとに異なる要求…対応が煩雑で非効率

- ✓ 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、**それぞれの企業からの要求に対応**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）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

発注者
委託先にセキュリティ対策をとってもらいたいが、
- 適切な基準が不明
- チェックリストの信憑性に不安

受注者
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

※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）

本格的 IT-BCP

★5

※令和8年度以降に検討

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

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

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

SECURITY ACTION

☆一つ星

★★二つ星

成熟度の定義	★3	★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	専門家確認付き自己評価	第三者評価

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

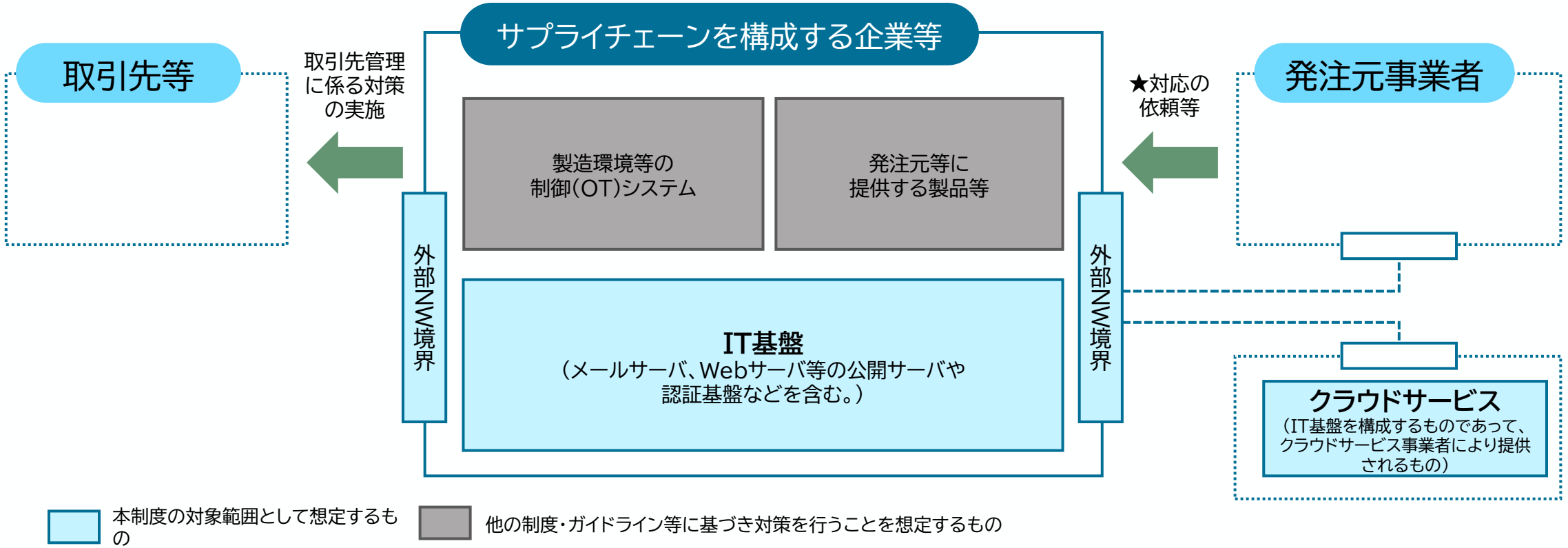
自社のセキュリティ対策
インシデント時の報告・共有

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

SCS評価制度の対象範囲

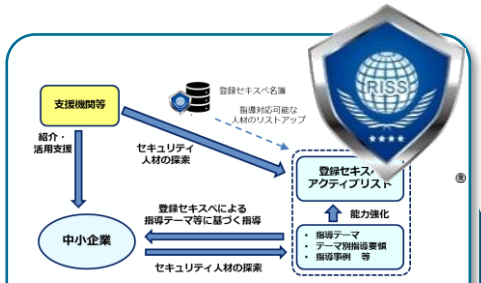
- サプライチェーンを構成する企業等の**IT基盤を対象**（クラウド環境で運用するものも含む。OTシステム、発注元等に提供する製品等は、必要な対応が基本的に異なるため、他の制度・ガイドライン等で対応）
- 評価取得の**申請主体**は、自社IT基盤を中心とした自社のセキュリティ対策の向上に責任を有する単位（**原則として法人又は個人事業主単位***）とする。 *ただし、法人にあっては、取得希望組織が設定した適用範囲についてセキュリティ専門家（★3）又は評価機関（★4）による妥当性の確認を経たうえで、**事業部単位、グループ単位などを申請主体とすることができる**。



SCS評価制度を中心とした中小企業支援策の新たな体系

SC対策強化

- **サプライチェーンに属する中小企業等が必要なサイバーセキュリティ対策**（SCS評価制度★３～４水準）**を取得するための施策を総動員**し、相互に連関/展開させる。



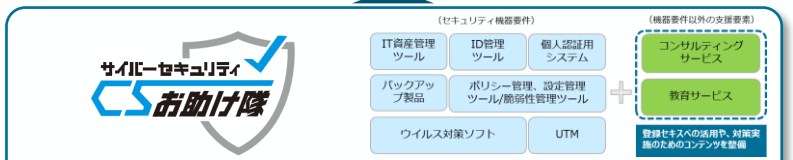
★３～４実装のための**人的支援**
（登録セキスペとのマッチング）

★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）

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）[検討中※]
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



★３～４を安価に実現する
“all-in-one”サービスの提供

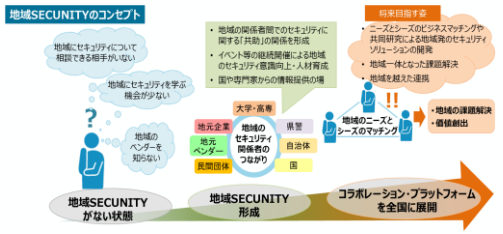
★３～４取得につながる
実践方策+規程類ひな形

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】



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

評価制度★3･★4の取得/更新時に各要件の**対応状況を診断**

課題の可視化

STEP2：必要な対策を実施

診断結果に基づき**★3･★4の取得に必要な対策を伴走支援**

※1 サイバーセキュリティお助け隊サービスは★3又は★4全ての要件を支援できるサービス
※2 評価制度の要件達成に 特定のIT ツールの導入が必須とされているものではない

支援内容の検討

※3 中小企業のニーズに沿ったサービスを提供

ポリシー整備・手順書作成･教育等

必要な対策を伴走支援（サービスの一例）

STEP3：要件達成

評価制度★3･★4の**全要件を満たし**、★取得に繋げる

要件を全て達成

“★3・★4取得”という共通ゴールに向け、提供事業者の**それぞれの強みを生かし**※3一定の価格要件の下で提供

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

SC対策強化

- 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

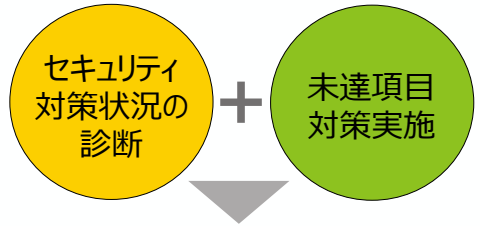
1. **組織的対策を含むセキュリティ対策を無料**で実施（実証期間中最大1年程度）
2. SCS評価制度の“★”**取得**が可能（SCS評価制度開始後の“★”取得要請への備えが可能）
3. サプライチェーン全体での対策強化に取り組む企業として、**取引先との信頼性向上**に繋がる

（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

（参考）デジタル化・AI導入補助金による「サイバーセキュリティお助け隊サービス」の導入支援

- 「通常枠」及び「インボイス対応類型」において、オプションとして「サイバーセキュリティお助け隊サービス」をメインツールと組み合わせて申請することが可能。この際、「サイバーセキュリティお助け隊サービス」を申請する事業者については、**申請採択における審査時に加点対象。**
- 2022年８月から、新たに「セキュリティ対策推進枠」を創設。**「サイバーセキュリティお助け隊サービス」のみでの補助金申請が可能。**

デジタル化・AI導入補助金概要

（旧名称：IT導入補助金）

メインツールと組み合わせて、**オプションとして「サイバーセキュリティお助け隊サービス」**を申請可能

「サイバーセキュリティお助け隊サービス」のみで申請可能。

	通常枠	インボイス枠 インボイス対応類型	セキュリティ対策推進枠
要件	業務効率化やDXの推進等に資するITツールを導入	インボイス制度に対応した会計・受発注・決済の機能を有するITツール及びそのためのハードウェアを導入	サイバーセキュリティお助け隊サービスを導入
補助上限	ITツールの業務領域が 1～３まで：5万円～150万円 4以上：150万円～450万円	ITツール： １機能：～50万円 ２機能以上：50万～350万円 PC・タブレット等：～10万円 レジ・券売機等：～20万円	5万円～**150**万円
補助率	中小企業：１/２	～50万円以下：3/4 (小規模事業者：4/5) 50万円～350万円：2/3 ハードウェア購入費：1/2	中小企業：1/2 **小規模事業者：2/3**
対象経費	ソフトウェア購入費、 クラウド利用料（最大2年分）、導入関連費	ソフトウェア購入費、 クラウド利用料（最大2年分）、導入関連費、 ハードウェア購入費	**サイバーセキュリティお助け隊サービス利用料（最大2年分）**

オプションとして**「サイバーセキュリティお助け隊サービス」を申請した場合、利用料の1年分（「サイバーセキュリティお助け隊サービス」導入は加点要素）**

赤字は令和６年度補正予算からの**拡充点**

デジタル化・AI導入補助金のインボイス枠(電子取引類型)、複数社連携デジタル化・AI導入枠においては、サイバーセキュリティお助け隊サービスは補助等の対象外である。

「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）】

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

CS能力強化

経済安全保障重要技術育成プログラム「サイバー空間の状況把握・防御技術の向上及び共通基盤の整備」

- 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。
- 2026年度以降、**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、**新たな研究開発項目を追加**し、**約400億円**に**規模を拡大**。

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　：　376億円以下（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
- 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

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
- 攻撃兆候の察知時に、リアルタイムで既に侵入済の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

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
- 国産セキュリティ特化AIモデルの構築

国産ベンチャーマッチングイベント推進

CS能力強化

- 日本ネットワークセキュリティ協会が中心となり、SIerと国産ベンチャー製品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」を開催し(経産省も共催)、**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**を予定。
- 防衛装備庁とも連携し、**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。

SIerと国産製品のマッチング

✓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SIerと国産ベンチャー製品とのマッチングを推進。2025年10月には、経産省と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3日に陸海空自衛隊等とのマッチングイベントを開催予定。

✓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備えて引き続き支援を行う。

防衛省・自衛隊

日系サイバー企業のASEAN事業拡大支援

- これまでのASEAN支援で構築した政府間の関係性を活用し、**日系サイバー企業のASEAN事業拡大を支援**。具体的には、JNSAが立ち上げた**民間主導のASEAN向け工場セキュリティ対策のための取組みを政府として後押し**する。
- まずは日系企業が多く進出するタイの日系工場向けにアセスメント及びソリューション提案の体制を、ローカルベンダーを含めて整備。その実績をもとに、ローカル製造業向けに、**現地政府及びローカルベンダーとも連携して国産ツールを含むソリューションの普及に向けた活動（展示会出展等）**を行う。将来的に、タイでの官民連携事業モデルを他のASEAN中位国他に横展開することも視野に進める。

経産省工場ガイドライン活用

- ASEAN各国への経産省工場ガイドライン・チェックリストの普及啓発、現地政府への働きかけ
- 国際標準とも整合性を確保

フレームワーク・ノウハウの提供

JNSA

OT Security WG

- OT含む工場のアセスメントのフレームワーク・ノウハウ提供
- アセスメントで把握されたリスクに対するソリューションも提供（国産ツール・サービスを含む）

現地事業者団体連盟のチャネル活用

ACCOA
ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

- JNSAが中心となり立上げた日ASEAN事業者団体連盟のチャネルを活用し、ローカル企業と連携して事業拡大

ASEANの工場セキュリティ・サプライチェーン対策強化に貢献

サイバーセキュリティ人材施策の全体像

CS能力強化

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

○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

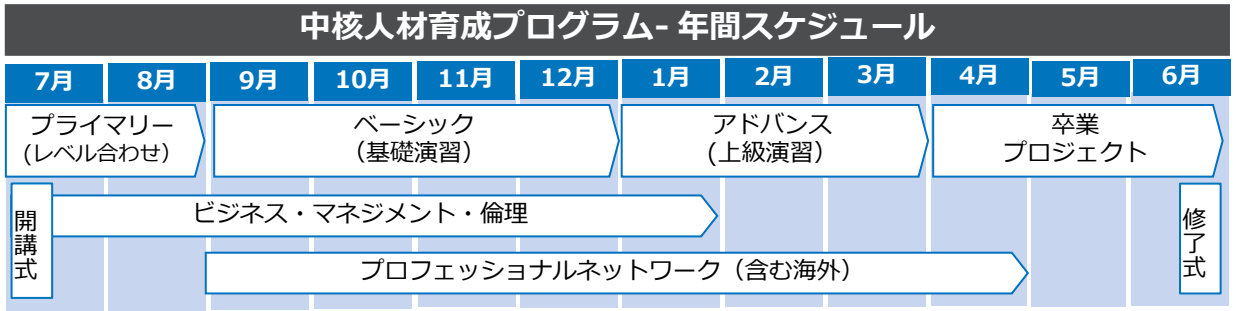
○大学・高専等と産業界との連携

IPA産業サイバーセキュリティセンター（ICSCoE※）CS能力強化

- 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、10期生まで約600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、第10期：65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

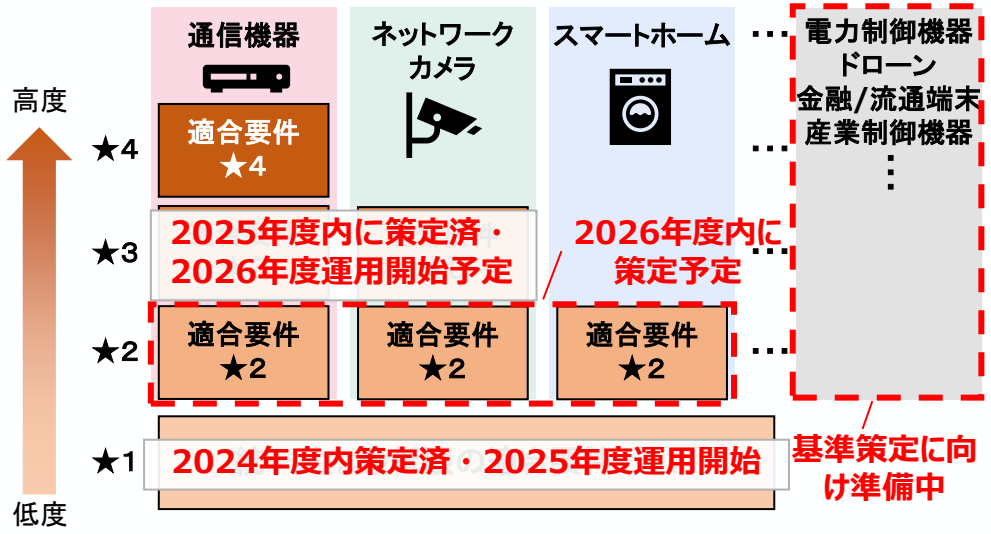
※ICSCoE : Industrial Cyber Security Center of Excellence
※CISA : Cybersecurity and Infrastructure Security Agency

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

（参考）適合ラベル取得製品の公開

- 2025年5月21日に★1適合ラベルの交付を開始。2026年2月時点、150超の申請（製品型番ベースで約1,000製品が対象）に対してラベル付与済。
- 適合ラベル取得製品リスト(※2)または製品やパッケージ等に掲示可能な適合ラベル内の二次元バーコードから、適合ラベル取得製品の情報にアクセス可能。

【JC-STARの適合ラベル取得製品リスト(※3)】


IPA 独立行政法人 情報処理推進機構

IPAについて　お問い合わせ　English

情報セキュリティ　試験情報　デジ

登録番号	ラベル取得事業者	製品名称	レベル	ステータス	ラベル取得日	有効期間
2025059900000264	株式会社アットマークテクノ	Armadillo-IoTゲートウェイ G4	★	有効	2025年5月19日	2027年5月18日
2025059900000158	株式会社バッファロー	TeraStation TS5020シリーズ, TeraStation TS3030シリーズ	★	有効	2025年5月7日	2027年5月6日
2025051600000193	株式会社Shizen Connect	Shizen Box 2	★	有効	2025年5月7日	2027年5月6日
2025051600000186	株式会社Shizen Connect	Shizen Box	★	有効	2025年5月7日	2027年5月6日
2025050900000219	NextDrive株式会社	EDGE エネルギーマネジメントコントローラー	★	有効	2025年5月7日	2027年5月6日
2025050200000244	アクシスコミュニケー	Axisネットワークカメラ、Axisネットワークイ	★	有効	2025年5月12日	2027年5月11日

【適合ラベル(★1)のイメージ】

【適合ラベル取得製品情報ページ】


適合ラベル取得製品情報ページ

(Conformance labeled products page)

English

JC-STAR 制度概要 > 製品一覧 > TeraStation TS5020シリーズ, TeraStation TS3030シリーズ

基本情報

製造事業者	株式会社バッファロー
製品名称	TeraStation TS5020シリーズ, TeraStation TS3030シリーズ
情報更新日	2025年5月7日

適合ラベル情報

適合ラベルステータス	有効
適合ラベル登録番号	2025059900000158
適合評価レベル	★ (Star 1)

(※1) 独立行政法人 情報処理推進機構（IPA）「「セキュリティラベリング制度（JC-STAR）」★1適合ラベルの交付を開始」https://www.ipa.go.jp/pressrelease/2025/press20250521.html
(※2) 独立行政法人 情報処理推進機構（IPA）「適合ラベル取得製品リスト」https://www.ipa.go.jp/security/jc-star/list/jc-star-product-list/index.html

ソフトウェア・セキュリティ施策の全体像

SBDの実践

- 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

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。**

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。

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）。

概念、枠組み (What)

具体化、事例化 (How)

運用

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

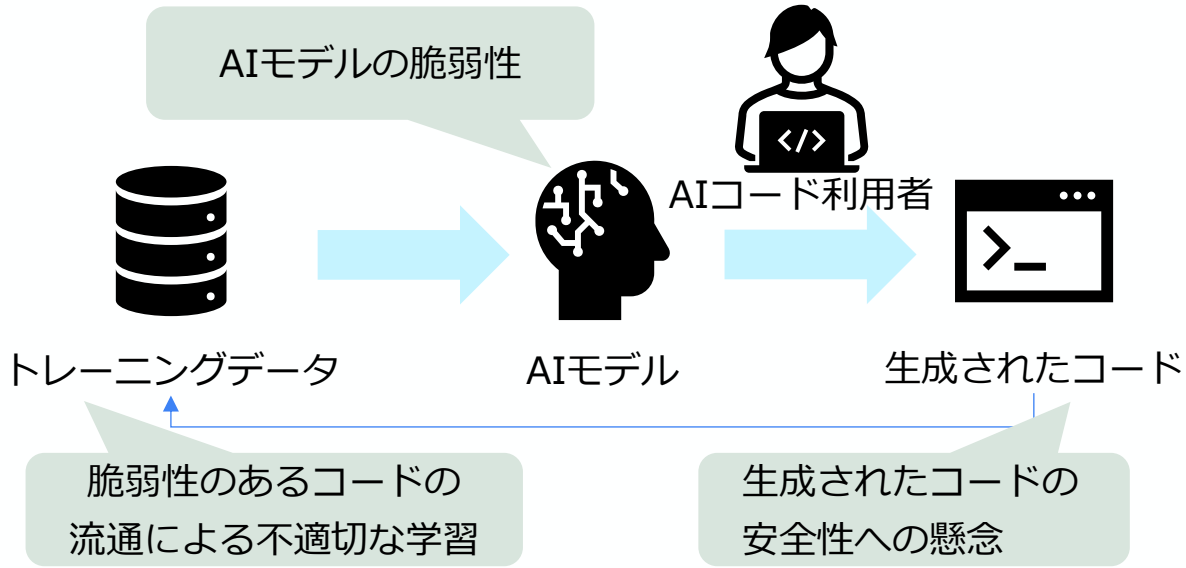
米NIST「Secure Software Development Framework（SSDF）Version 1.1（2022年２月）」

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

ソフトウェアのセキュリティの確保

- **「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。

▲ **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**

国際的な取組を含むSBOMの活用促進

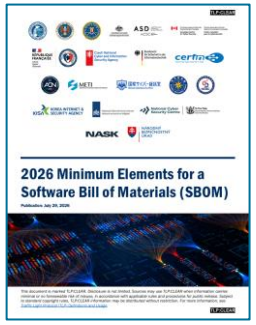
SBDの実践

- 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**。2026年7月には、SBOMの最小要素に関する**国際文書（ガイダンス）に共同署名**した。
- 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。

- SBOMにおける最小要素の定義を、SBOMツール及び技術の進展に伴い更新した国際的な文書（ガイダンス）について、積極的に議論に参加し、2026年7月、内閣官房国家サイバー統括室（NCO）を含む計14か国のサイバーセキュリティ当局等と共同署名。



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
サイバーセキュリティのためのソフトウェア部品表（SBOM）の最小要素に関する国際ガイダンスに共同署名しました（2026年7月30日） https://www.meti.go.jp/press/2026/07/20260730001.html

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html

経済産業省　サイバーセキュリティ　検索