資料３

経済産業省

経済産業省説明資料①

（サイバーセキュリティ産業振興に向けた取組等について）

令和８年３月１９日

経済産業省　商務情報政策局

技術・研究開発/社会実装/産業育成に関する取組

（一部、ＡＩ×サイバーセキュリティに関する取組を含む。）

「サイバーセキュリティ産業振興戦略」（2025年３月）の概要

- サイバーセキュリティ対策の必要性が高まる中で、①**企業が適切なセキュリティ製品を選択できるようにする**、②**我が国へのサイバー攻撃の特異性にも対応し安全保障を確保する**、③**拡大するデジタル赤字解消に貢献する**との観点から、我が国セキュリティ産業振興が不可欠。
- 現状、**国内で活用される製品の多くを海外製が占めており**、ユーザーは、**これまでの利用実績や価格を重視**。結果として我が国セキュリティ産業は、**「買い手がつかないので儲からない」「儲からないので事業開発や投資が十分なされず競争力が低下」という悪循環**に陥っている。
- こうした現状を打破するため、**製品開発の出口をまず確保**した上で、**シーズの発掘・事業拡大を後押し**する、**包括的な政策対応**を提示。

今後の成長に向けた課題（As-Is）

導入実績が重視される商慣習

- 新規製品が販売されても、実績が重視されるため、調達先が存在せず、事業として成り立たないため、企業が育たない

十分な開発投資が行われにくい事業環境

- 安定的な収益基盤が見通しづらいため、製品開発・研究開発への投資が限られる
- セキュリティ製品の販売はSIerが商流を担っており、製品ベンダーで対応できる余地は限られている

セキュリティ産業全体を支える基盤の不足

- 人材育成や国際市場の開拓等、産業全体を支える基盤は重要であるものの、個社での対応が難しい

目指すべき方向性（To-Be）と実現のための主な政策対応

スタートアップ等が実績を作りやすくなる／有望な製品・サービスが認知される

- 「スタートアップ技術提案評価方式」等の枠組みを活用し、**政府機関等が有望なスタートアップ等の製品・サービスを試行的に活用**（中長期的には主体・取組を拡大）
- **有望な製品・サービス・企業の情報を集約・リスト化**し、政府機関等へ情報展開する／業界団体とも連携して審査・表彰を実施

有望な技術力・競争力を有する製品・サービスが創出され、発掘されやすくなる

- セキュリティ関連の技術・社会課題解決に貢献する技術・事業を発掘するための「コンテスト形式」による**懸賞金事業**等を実施（中長期的には安定供給確保策も検討）
- **約300億円の研究開発プロジェクト**を推進し社会実装を後押し
- 我が国商流の中心である**SIerと国産製品・サービスベンダーとのマッチング**の場を創出

供給力の拡大を支える高度人材が充足する／国際市場展開が当たり前になる

- 高度専門人材の育成プログラムを拡充／セキュリティ人材のキャリア魅力を向上・発信
- 海外展開を支援／標準化戦略を促進／関係国との企業・人材交流を促進

今後のロードマップ

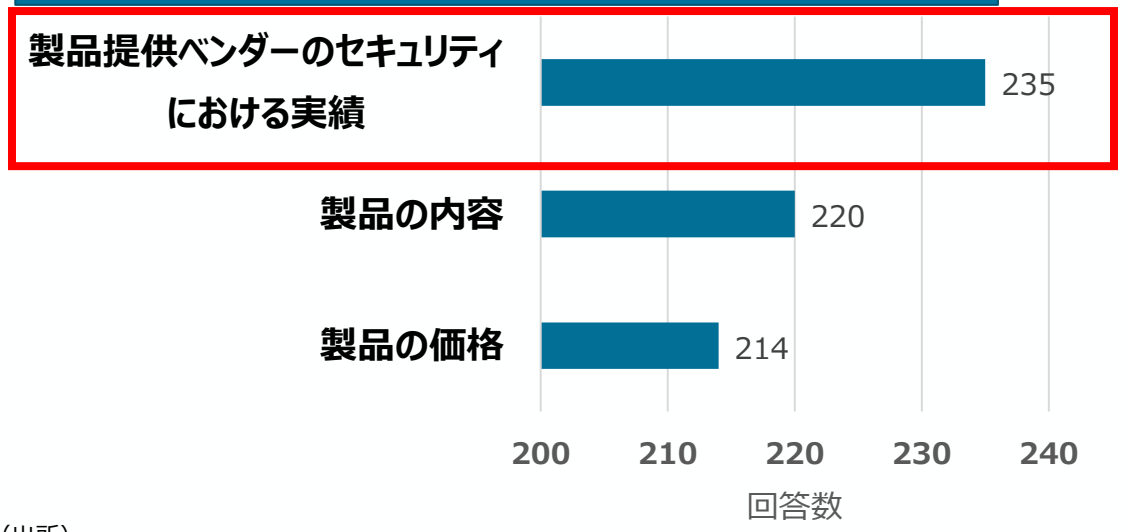
①３年以内：「企業・人材数の増加」　②５年以内：「我が国企業のマーケットシェアの拡大」「重要技術の社会実装」
③10年以内：「安全保障の確保やデジタル赤字の解消への貢献を実現」**【KPI：国内企業の売上高を足下から3倍超（約0.9兆円⇒3兆円超）】**

※前提として、サイバーセキュリティ市場の「需要」の拡大につながるような各種の取組も同時に推進。

IPAによる有望セキュリティ・スタートアップ製品・サービス等の積極的な調達

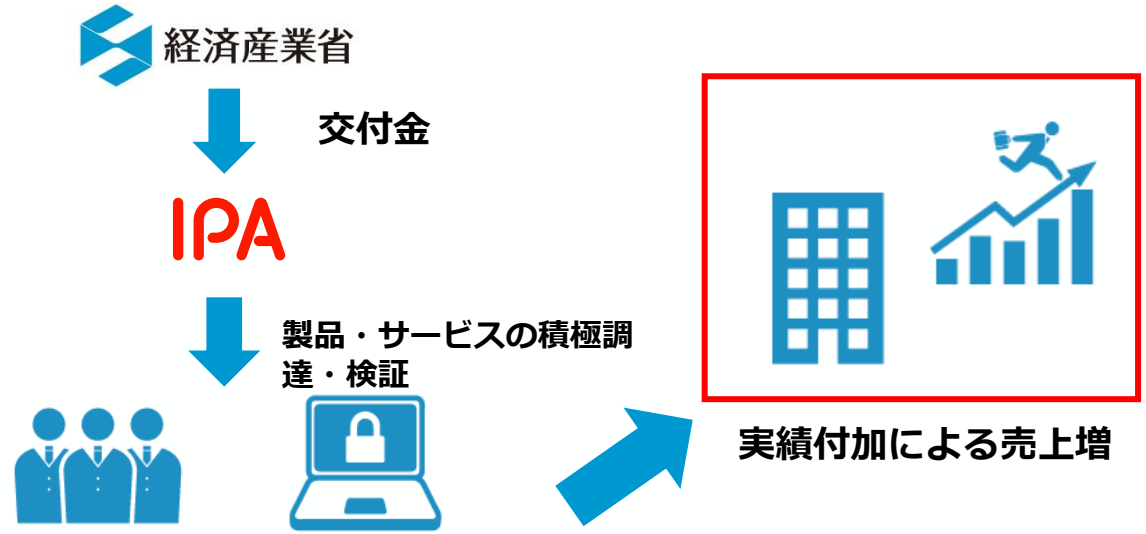
- 現状、**国内で活用される製品の多くを海外製が占めており**、ユーザーは、**これまでの利用実績や価格を重視**。我が国**セキュリティ産業が更なる成長を遂げるには、導入実績が重視**される等という商慣習を踏まえた上で、新規参入のハードルとなっている点を打破する政策が必要。
- このため、国内スタートアップ企業の実績をつくり新規参入におけるハードルを低減するために、**セキュリティに知見を持つIPAが有望なスタートアップ等の製品・サービスを積極的に調達**する取組を実施予定。
- 令和７年度補正予算を通じ、2026年春頃からIPAにて順次調達を開始。今後、**製品・サービスの有効性検証を行うための環境整備の構築**を行い、**調達した製品の評価**も実施予定。

製品を選定する際に最重要視する項目
（上位３項目、国内ユーザー企業からのアンケート）



（出所）
富士キメラ総研「2023 ネットワークセキュリティビジネス調査総覧〈市場編〉」を基に作成。
https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
https://www.jnsa.org/result/surv_mrk/2025/2024_securitymarket.pdf

製品･サービスの調達スキーム



フロンティア育成・懸賞金事業（サイバーセキュリティ関連技術の募集）

AI関連

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

懸賞金事業の目的

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

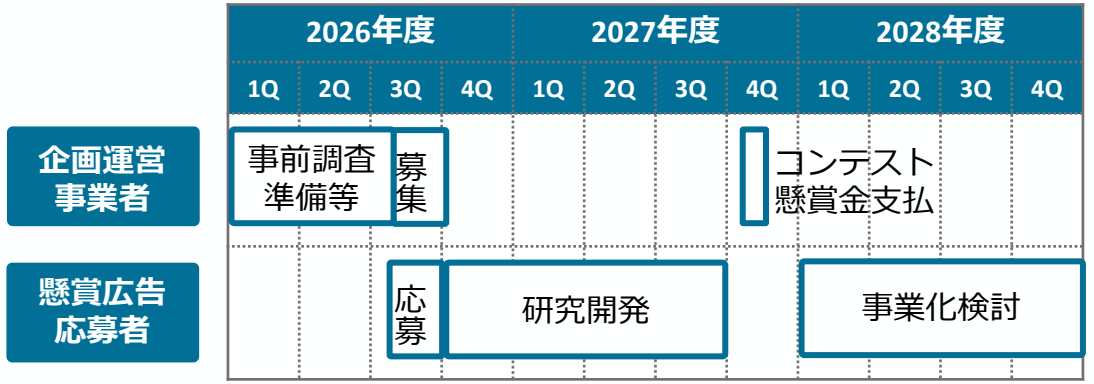
懸賞金テーマ：サイバーセキュリティの技術

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

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

懸賞金事業スケジュール

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



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

AI関連

- 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。今後、テーマを追加し、**プロジェクトを拡張予定**。

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から理事を選出**

代表理事（FFRIセキュリティ 鵜飼社長）

一般社団法人（サイバーリサーチコンソーシアム）

一般社団法人から再委託

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

事業規模など

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

主な研究開発内容

１）サイバー空間の情報を収集・調査する状況把握力の向上

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

２）サイバー攻撃から機器やシステムを守る防御力の向上

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

３）共通基盤の整備

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

４）セキュアな量子情報通信技術の開発

- Y-00のデジタルコヒーレントの開発／Y-00の高速光ファイバ通信の開発／Y-00の高速光ワイヤレス通信の開発

業界団体等と連携したマッチングイベントの実施

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

国内スタートアップとSI事業者とのマッチング

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

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

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

JNSA

防衛装備庁と国産技術のマッチング

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

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

防衛省・自衛隊

サイバーセキュリティ・サービス提供事業者の信頼性確認

- サイバーセキュリティ・サービス（とりわけ、顧客の機微情報やシステムへのアクセスを許容する形態のもの）に対するニーズの増加が今後見込まれる中、**サイバーセキュリティ・サービス提供事業者の体制・措置等に起因する事案等**が生じており、**サービス提供事業者の「信頼性」の一層の強化（厳格な社内体制の整備等）が求められる状況**。
- また、政府機関や安全保障に関係する事業者等においては、**高度な「信頼性」を有するサイバーセキュリティ・サービス事業者を選定・活用するニーズ**が想定される。
- こうしたことを踏まえ、既に技術・品質の基準に基づき登録を行っている現行の「**情報セキュリティサービス審査登録制度」に登録しているサイバーセキュリティ・サービス提供事業者**を対象に、**「事業者の信頼性」を確認**する認定制度を創設するべく、検討を進めていく（2026年4月頃に制度の方向性を提示し、制度の詳細設計を進め、**2027年度中の運用開始を目指す**。）。

情報セキュリティサービス審査登録制度のサービス区分

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

認定制度のイメージ

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

新たな基準を新設

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

現行制度（審査登録制度）

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

産業全体を支えるセキュリティ人材の育成

- 我が国サイバーセキュリティ産業のエコシステム構築にあたっては、**産業の基盤となる人材の育成も重要**であり、とりわけ製品・サービスの提供側におけるトップ人材の育成を強化することが必要。

産業を支える人材の育成に向けた主なポイント

産業全体を支える人材の育成

トップ人材の育成
- 起業や新たな技術の開発などを通じて産業界をリードする、トップオブトップ人材の育成強化が重要

製品・サービス提供者のセキュリティスキル向上
- 優れた国産製品・サービス創出を担う、サプライサイドで活躍できるセキュリティ人材の育成強化が重要

セキュリティ領域の拡大に対応する人材
- AI等の先端技術の活用が急速に進む中、セキュリティ対策が求められる領域は拡大しており、各領域でセキュリティ対策を担える人材の育成が重要

キャリアの魅力発信
- セキュリティ人材の「量」・「質」を高めるためには、人材のパイプラインの「入口」となる候補者の分母を増やすための取組が重要

基盤整備
- 産学官で連携し、人材育成を効果的に推進するためには、スキル定義やキャリアパスの可視化など、人材育成の環境整備が重要

主な人材育成施策

① セキュリティ・キャンプ

- 若年層の**トップ人材**の育成・発掘を目指す事業
  - **AI、デバイス開発**及び法律などの**他領域と、セキュリティの知見を兼ね備えた人材**の育成プログラム（セキュリティ・キャンプ コネクト）を新たに実施予定
  - 継続的なネットワーク形成を通じた**修了生の成長支援**や**キャリアの魅力発信**等を目的として、修了生コミュニティを整備

② IPA産業サイバーセキュリティセンター(ICSCoE)

- セキュリティ対策の中核拠点として、OT(制御技術）や模擬プラントの活用を特徴とするハンズオン演習等を実施
  - 半導体をはじめとする**多様な製造事業者向け**の模擬プラントを拡充予定
  - **OT領域におけるAI活用の進展**を想定し、新規プログラムを提供予定

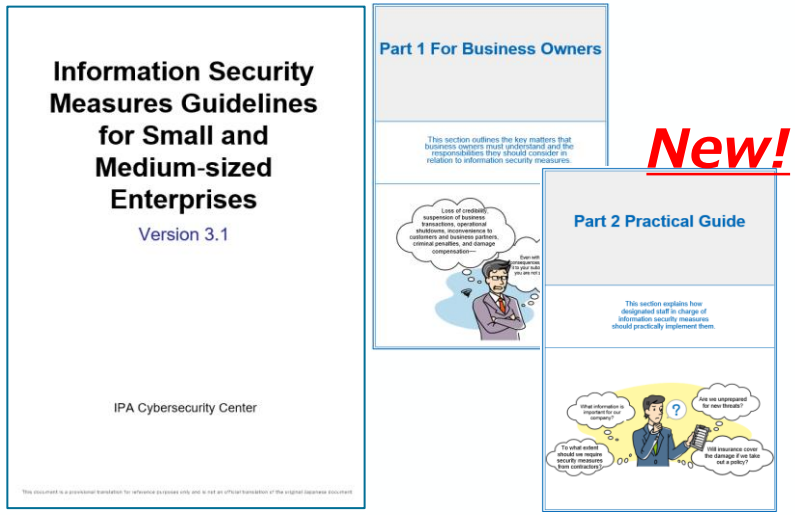
③ 情報処理安全確保支援士（登録セキスペ）

- **セキュアなシステム開発**からセキュリティマネジメントなどのセキュリティに係る**幅広い専門的な知識・技能**を備えた国家資格
  - **資格登録者数の増加**など、**制度の更なる活用**に向け、講習制度を見直し

※**基盤整備**の取組として、NCOによる人材フレームワークの検討や、**高度専門人材育成の強化**に向け、経済安全保障重要技術育成プログラムでも検討中。

我が国のサイバーセキュリティ施策の海外発信

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



新規に英語化した中小企業向けガイドライン

日・ASEANサイバーセキュリティ政策会議の様子

我が国サイバーセキュリティ事業者による海外展開支援

- 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、ローカルベンダー含めて整備する。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）**を行うことを想定。将来的に、タイでの官民連携事業モデルを他のASEAN諸国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)

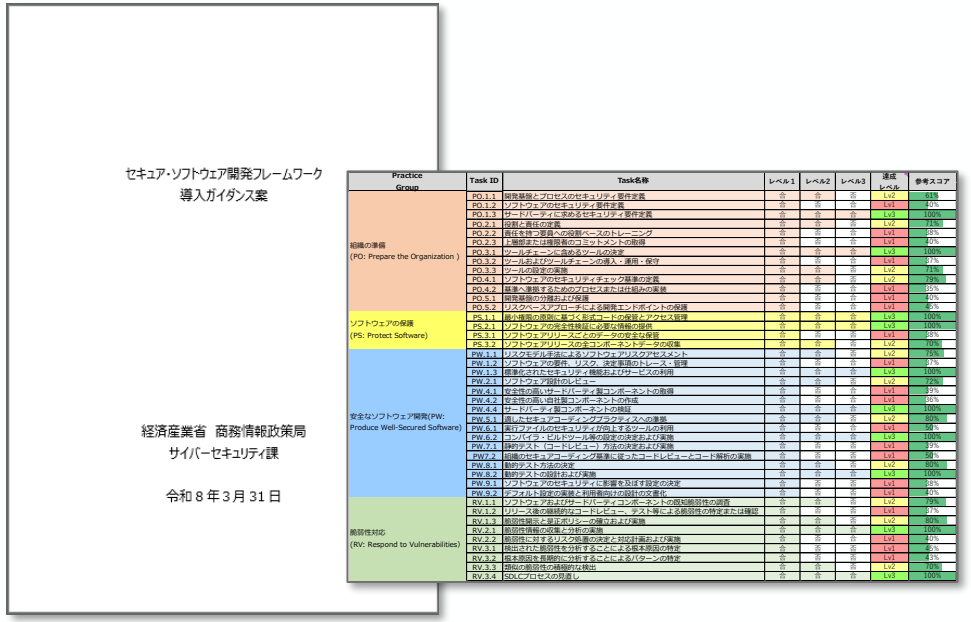
- JNSAが中心となり立上げた日ASEAN事業者団体連盟のチャネルを活用し、ローカル企業と連携して事業拡大

工場セキュリティ・サプライチェーン対策強化に貢献

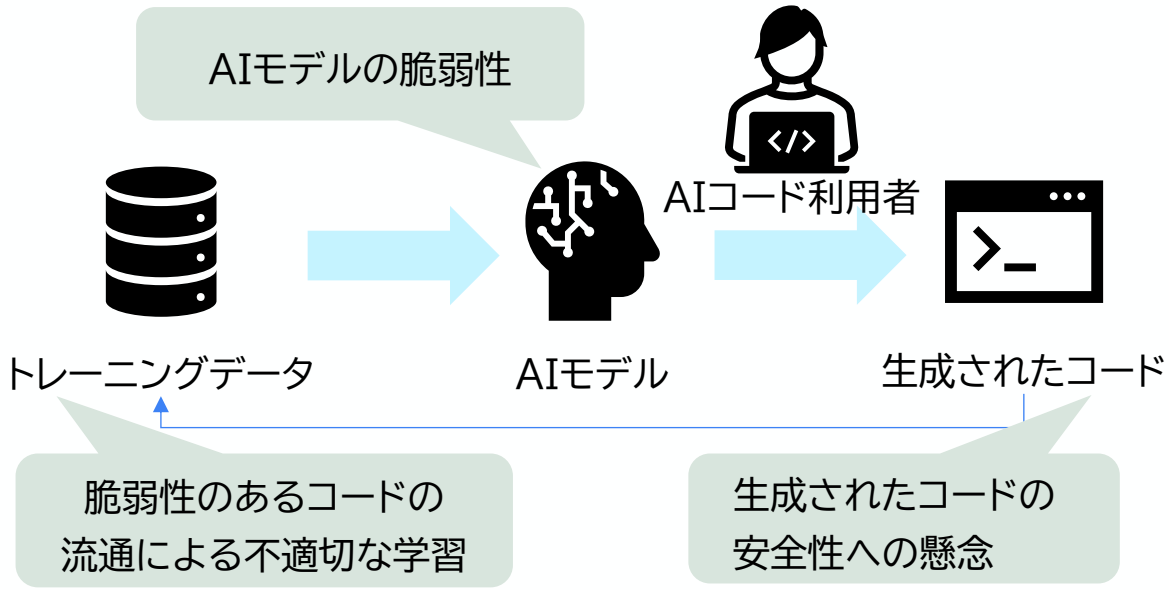
その他のＡＩ×サイバーセキュリティに関する取組

AI駆動ソフトウェア開発に伴うリスクへの対応

- **「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**）を産業分野ごとの実態に即して効果的に**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策定・成案化**（2026年度前半を予定）。
- 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

AIエージェント利活用に伴うリスクへの対応

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

AIに関連する既存のガイドライン等の整備状況（イメージ）

統一的な指針として：AI事業者ガイドライン(総務省/経済産業省 2025年3月改訂版公開)

AI開発者	AI提供者	AI利用者
AIセーフティに関する評価観点ガイド (AISI 2025年3月改訂版公開) AIセーフティ評価の観点、想定され得るリスク・評価項目例、評価の実施者等に関する考え方、評価に関する手法の概要を提示。 ※他、AIセーフティに関するレッドチーミング手法ガイドも別途存在。		AI利用者である**民間企業が参照可能な実務的なガイドラインは存在せず。**
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 2025年度末初版公開予定) 「AIセーフティにおける重要要素」及び「AIセーフティ評価の観点」を踏まえ、AIの「セキュリティ確保」を取り扱う。脅威への技術的対策例を整理。		

ガイドラインの方向性（イメージ）

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

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

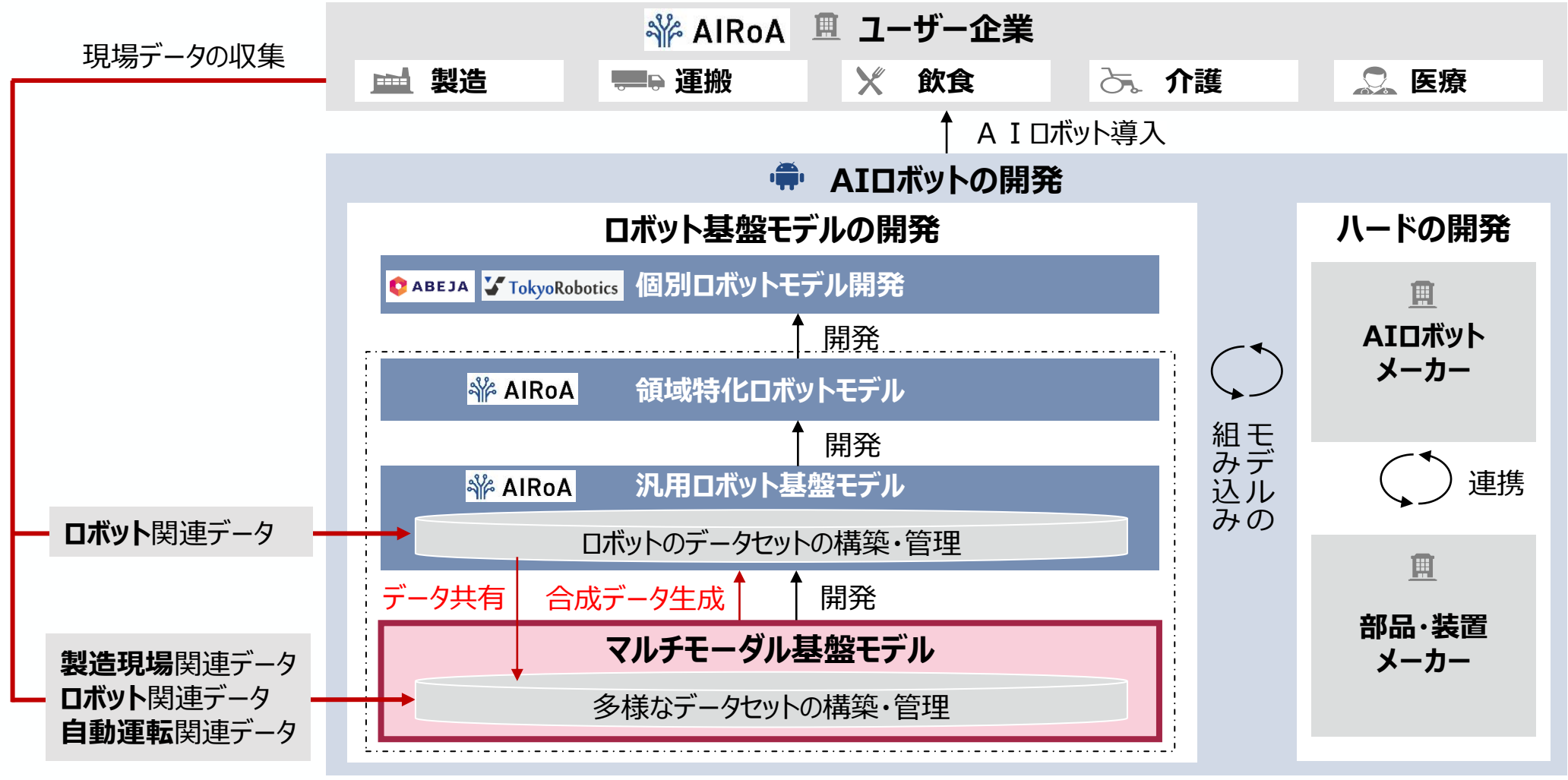
- ガバナンス
- データ保護
- アイデンティティ管理

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

フィジカルAI時代のロボット基盤モデルの重要性

AI関連

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

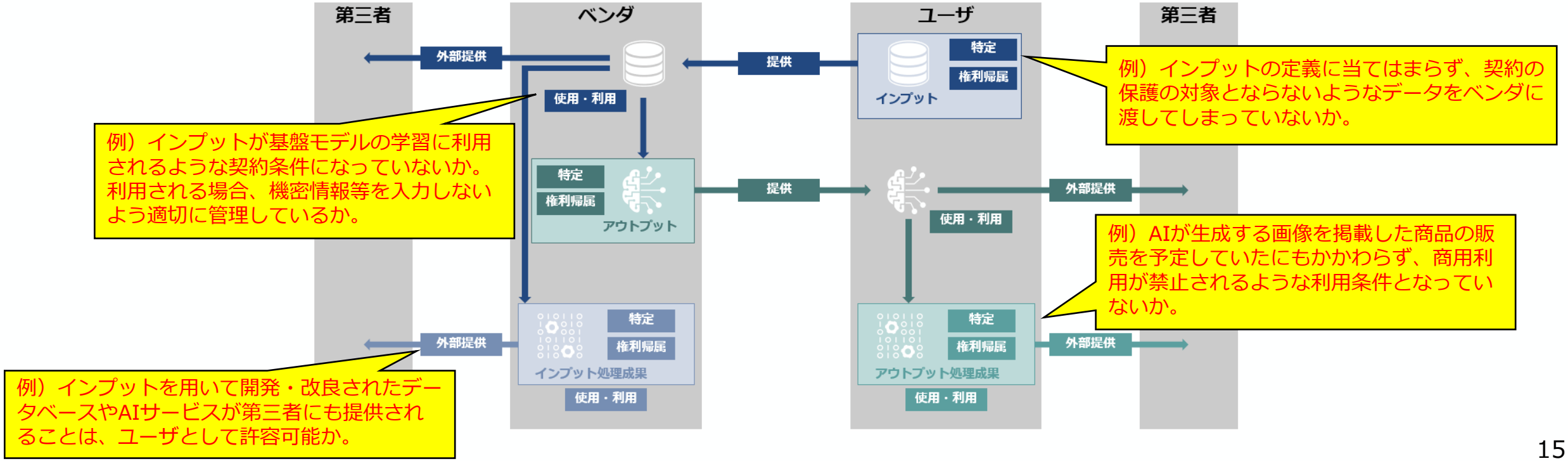


防御的な対応：契約の精査（AI契約チェックリストの活用）

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

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

（参考）AI契約チェックリストの構造と活用事例

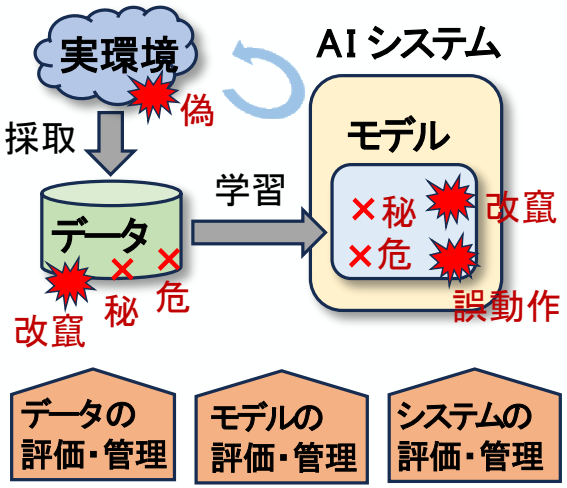


産総研におけるAIセーフティの研究開発

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

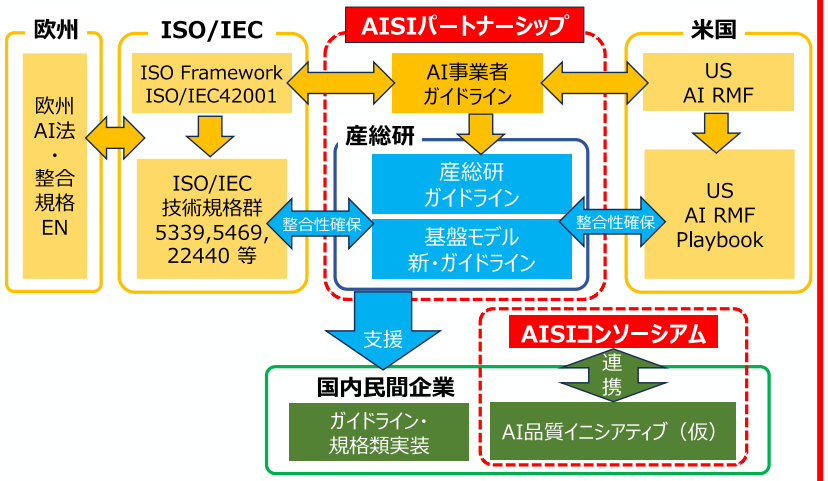
①AIセーフティ評価・管理基盤技術開発

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



③AIセーフティ基準・ガイダンス作成と標準化活動

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



②応用領域別AIセーフティ評価・実装技術開発

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

暮らし支援

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

協働ロボット

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

スマートシティ

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

経済産業省

経済産業省説明資料②

（より一層対策が必要な分野への対応について）

令和８年３月１９日

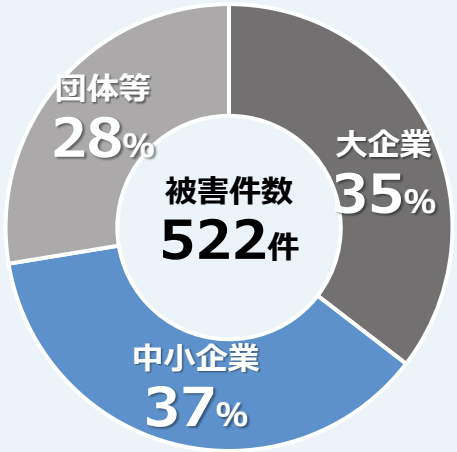
経済産業省　商務情報政策局

中小企業を含むサプライチェーン全体での対策強化に向けた取組

中小企業のサイバー被害状況とサプライチェーンへの影響

- 大企業に限らず**中小企業も相当数のサイバー攻撃の被害を受けており**、その影響として**取引先・サプライチェーンにも影響を及ぼしている場合が多い。**

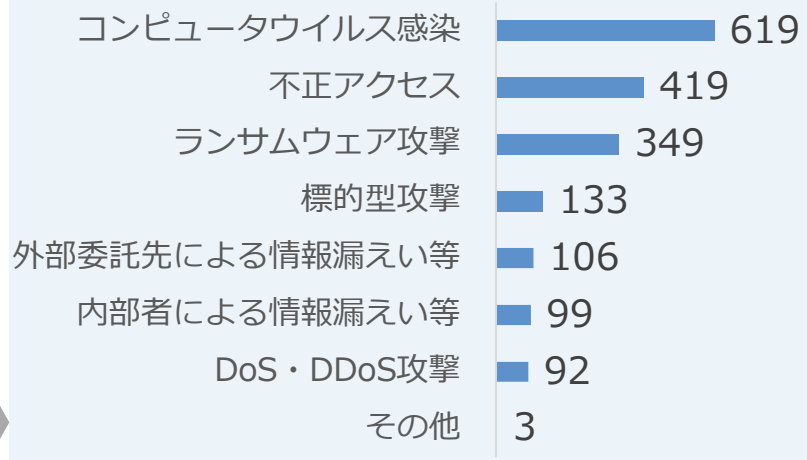
サイバー攻撃の被害組織の規模別割合（2022年７月～2024年6月）



直近２年間のサイバー攻撃による被害の**約４割**を中小企業が占めているという結果から、大企業に限らず、多くの中小企業においてもサイバー攻撃の被害が現実に発生している状況

出典：JNSA「インシデント損害額調査レポート別紙 2025年版」を基に経済産業省作成

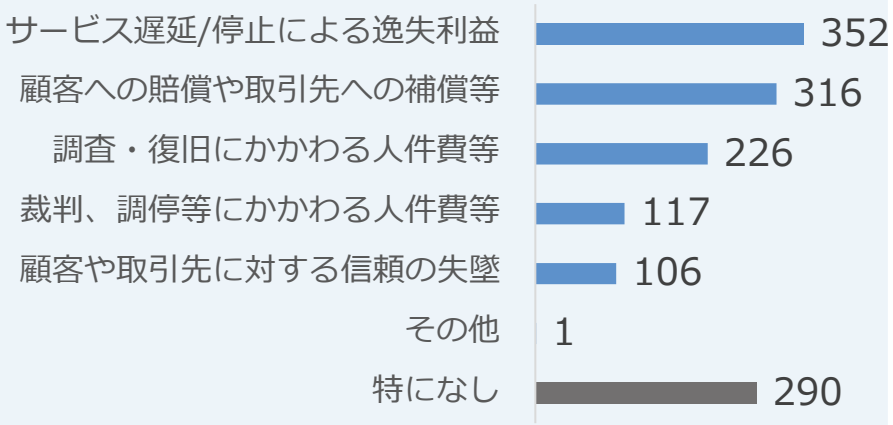
中小企業が実際に受けたサイバーインシデント（複数選択可、回答企業975社）



約1/4の中小企業が1年間（2023年4月～2024年3月）にサイバーインシデントの被害を受けたと回答
その内訳は、コンピュータウイルス感染や不正アクセス、ランサムウェア攻撃など**形態は様々**

出典：IPA「2024年度中小企業における情報セキュリティ対策に関する実態調査」を基に経済産業省作成

サイバーインシデントによるサプライチェーンへの影響（複数選択可、回答企業975社）



サイバーインシデントの被害を受けたと回答した975社のうち、**685社**がサイバーインシデントにより取引先（サプライチェーン）に影響があったと回答
その割合は**70.3%**

出典：IPA「2024年度中小企業における情報セキュリティ対策に関する実態調査」を基に経済産業省作成

中小企業のセキュリティ対策強化に向けた取組の方向性

- 経済産業省では、地域の支援機関等とも連携し、周知啓発に加え、**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。今後は、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）**を実施するための施策を総動員**する。

課題

サプライチェーンに及ぼすリスクが増す中、組織的対策を含めたサイバーセキュリティ対策が不十分

地域・企業によって、サイバーセキュリティ対策の取組状況にバラツキがある

対策の方向性

サプライチェーン全体での対策強化
中小企業等が最低限実施すべき取組の可視化と実装支援

地域SECUNITY活動の促進
コンテンツの充実化と支援機関による活動支援

現状の対策・今後の方向性

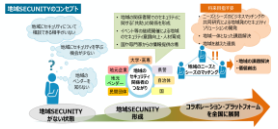
サプライチェーン強化に向けたセキュリティ対策評価制度

中小企業等が**最低限実施すべき取組を可視化した制度**（SCS評価制度）。**令和８年度末頃の制度開始**を目指す。セキュリティ対策の「**共通のものさし**」として活用されるよう、関係主体への周知等の取組を進める。

★５
★４
★３

地域SECUNITY（地域のセキュリティ・コミュニティ）

地域の支援機関等と連携した**面的な普及活動**を促進。**コンテンツの充実化**や**支援機関による活動支援**を進める。



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。

※**約45万者**の中小企業が宣言。

サイバーセキュリティお助け隊サービス

異常監視、緊急時の対応支援、サイバー保険などを**ワンパッケージで提供するサービス**。

※約**9,200件**の利用実績（2025/9時点）

SCS評価制度に対応した新類型の創設を検討。

中小企業の情報セキュリティ対策ガイドライン

中小企業等向けに具体的な**セキュリティ対策を示したガイドライン**。

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**等も収録する方向で改訂予定。

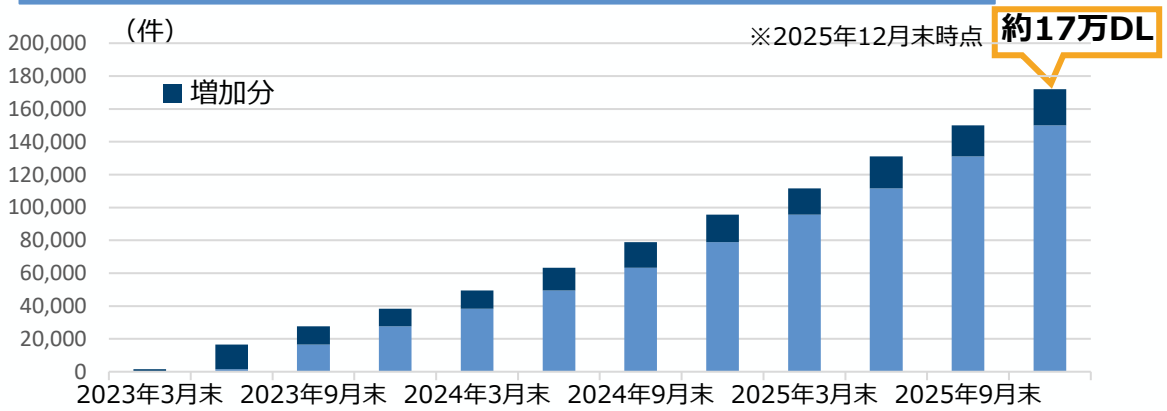
サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

IPAと連携しながら、**産業界におけるサプライチェーン・セキュリティ対策強化**に向けた取組を実施。

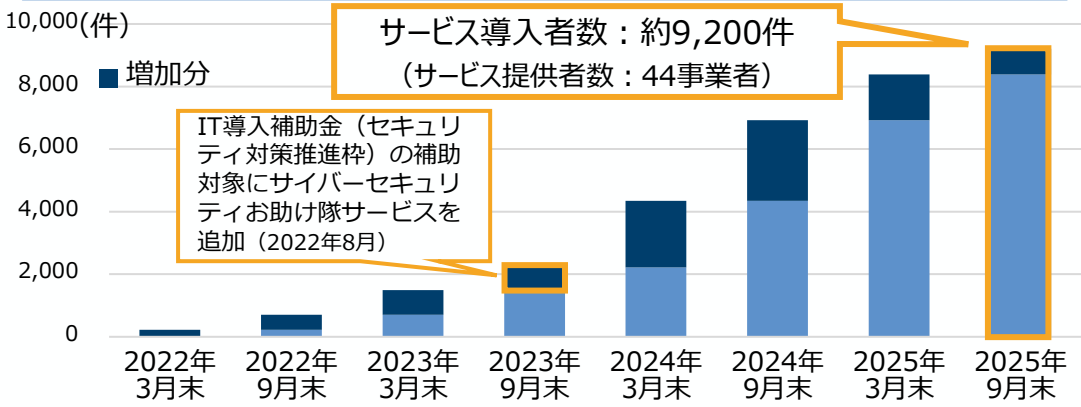
（参考）ガイドライン・各種施策の普及状況

- 「サイバーセキュリティ経営ガイドラインVer3.0」（2023年３月改訂）のダウンロード数が**約17万件**まで到達。
- 補助金の申請要件化を通じてSECURITY ACTION自己宣言者数が拡大。宣言数は**約45万件**まで到達。
- サイバーセキュリティお助け隊サービス導入件数は**約9,200件**まで到達。
- IPAを通じた施策等により、**継続的にサイバーセキュリティ人材を育成**。地域での経営者向け演習、地域団体への講師派遣、セキュリティ担当者向けセミナー等を通じて**セキュリティ・コミュニティ（地域SECUNITY）の形成・活動を促進**。

サイバーセキュリティ経営ガイドラインVer３.0　累計DL数

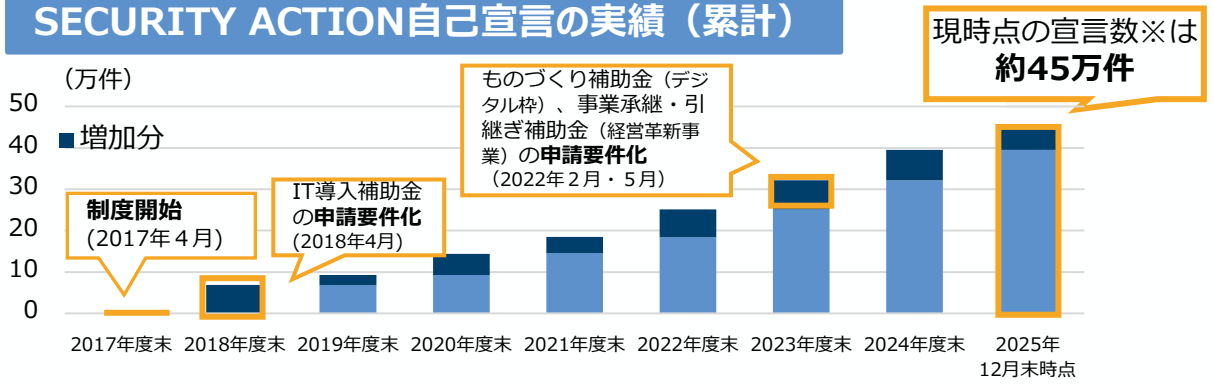


サイバーセキュリティお助け隊サービス導入実績（累計）



※サービス提供者数は2025年12月末時点

SECURITY ACTION自己宣言の実績（累計）



※一つ星、二つ星の いずれかまたはその両方の自己宣言の件数

人材育成及び地域ワークショップの実績

中核人材育成プログラム修了者数	492名(2017年～2025年)
情報処理安全確保支援士	24,937名(2025年10月時点)
セキュリティ・キャンプ参加者数	全国大会：1,311名(2004年～) ネクストキャンプ：62名(2019年～) ジュニアキャンプ：18名(2023年～)
IPA　セキュリティ講演者派遣	108件(2026年2月時点)
IPA　セキュリティセミナー支援	セミナー開催支援：21件 経営者向けインシデント机上演習WS：19件(2026年2月時点)

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

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）

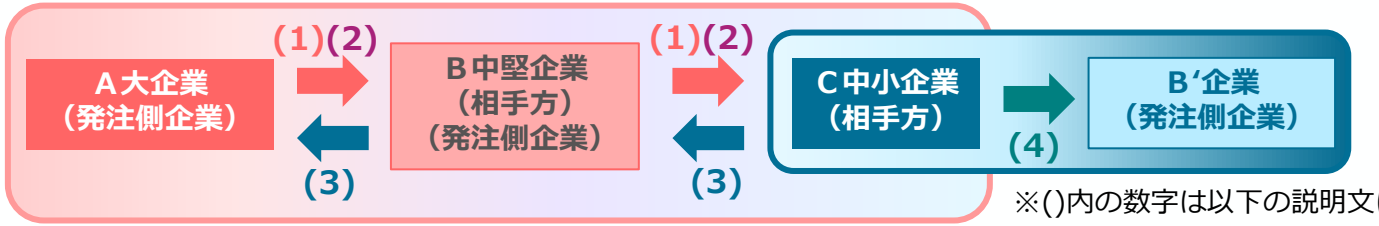
２０２５年１２月２６日
経済産業省・公正取引委員会

○　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（SCS評価制度）に基づく対策要請を円滑に行い、発注者側・相手方がパートナーシップを構築してセキュリティ対策と価格交渉を実施し、円満に合意するものとしている。

【想定事例】

【サプライチェーンのイメージと想定事例の各場面】



※()内の数字は以下の説明文に対応

(1) セキュリティ対策実施の要請

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

(＊)**「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）」中の「★４」に相当**

(2) 要請に当たってのパートナーシップの構築

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

(3) 要請への対応と価格交渉の実施

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

(4) 要請を行っていない発注者側企業への対応

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

【想定事例解説】

想定事例を補足するため、以下の点について解説を作成。

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

【今後の取組】

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

サイバーセキュリティお助け隊サービス（新類型）の創設に向けた検討

- 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

- 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44事業者がサービスを提供**しており、 2025年9月末時点で**約9,200件の利用実績**がある。
- デジタル化・AI導入補助金（旧：IT導入補助金）「セキュリティ対策推進枠」を活用することで、**最大150万円まで、導入費用の1/2（小規模事業者は2/3）の補助**を受けられる。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

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

➡中小企業でも導入・維持できる価格でワンパッケージで提供

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

サイバーセキュリティ 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：
サービス基準の要件を満たすサービスに対し、**お助け隊ロゴマークの使用を許諾**

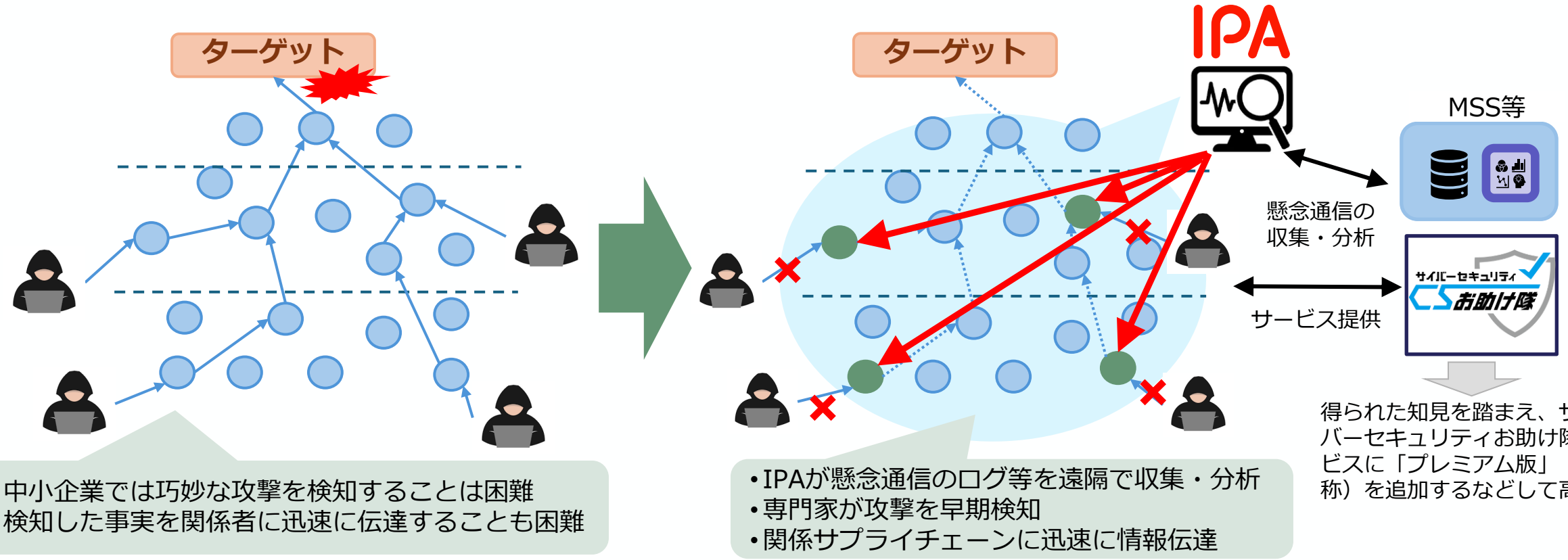
サービス提供 → **中小企業** → 自社の信頼性をアピール → **取引先**（大企業等）

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）

集団的防御プラットフォームの構築

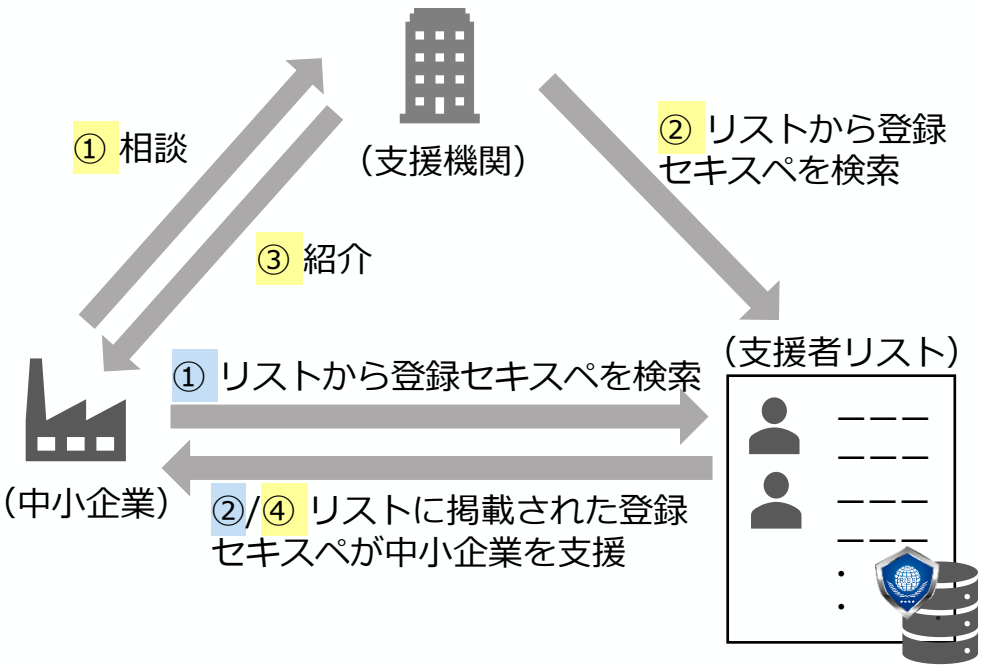
- 基幹インフラ事業者を狙うサイバー攻撃は、**サプライチェーン内で脆弱な中小企業等から侵入**することが多いが、**中小企業等**にとって**その兆候の検知は困難**である。
- そこで、高度なサイバー情勢分析機能を有する**IPAが、中小企業等で検知された懸念通信を収集・分析**し、**攻撃の早期検知や関係先への注意喚起等を図る**実証事業を令和7年度補正予算で実施予定。
- 実証事業を通じて、**本プラットフォームの有用性等を検証**するとともに、社会実装後の普及促進を見すえ、**サイバーセキュリティお助け隊サービスに面的防御の観点を取り入れ**、その高度化を図っていく。



情報処理安全確保支援士（登録セキスペ）を活用した中小企業支援

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

（今後の支援者リスト活用スキーム）



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

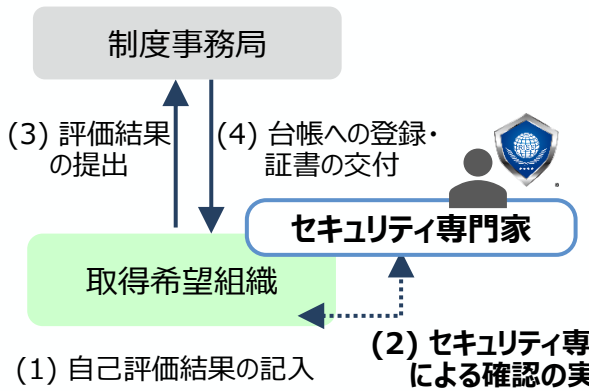
支援者リストの整備（利便性向上・掲載者の増加）

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

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

SCS評価制度★３取得の適合可否を確認できる登録セキスペの拡充

（SCS評価制度★３の評価スキーム）



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

※2：支援者リストに掲載された登録セキスペは、指導テーマ（情報セキュリティ規程の整備等）から中小企業が指定するものに基づき支援を実施。
※3：指導要領の作成や、スキル習得のためのケース演習を実施。

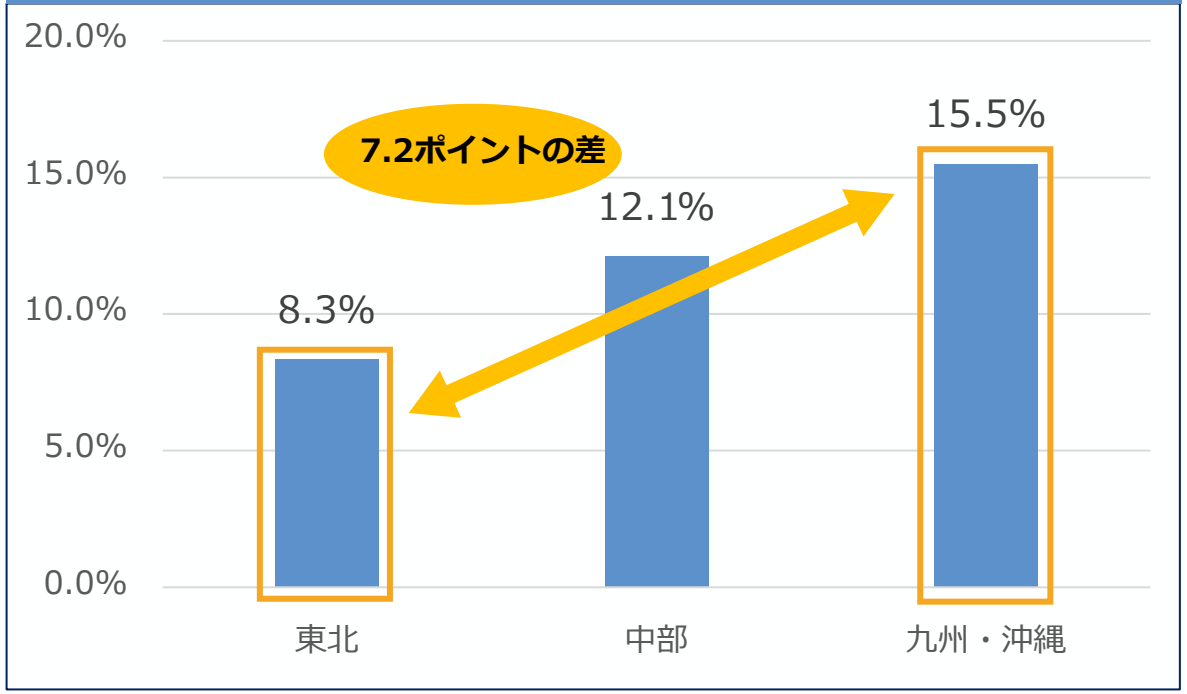
今後の方向性について

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

地域におけるサイバーセキュリティ対策状況のバラツキ

- 地域により、**中小企業のサイバーセキュリティ対策の状況**や、**セキュリティ人材の人数**に**差がみられる。**
- 特に活動が活発でない地域を中心に、中小企業支援機関と連携した**サイバーセキュリティ対策の普及・啓発を後押し**することで、サイバーセキュリティの地域差を生じさせないための取組が必要。

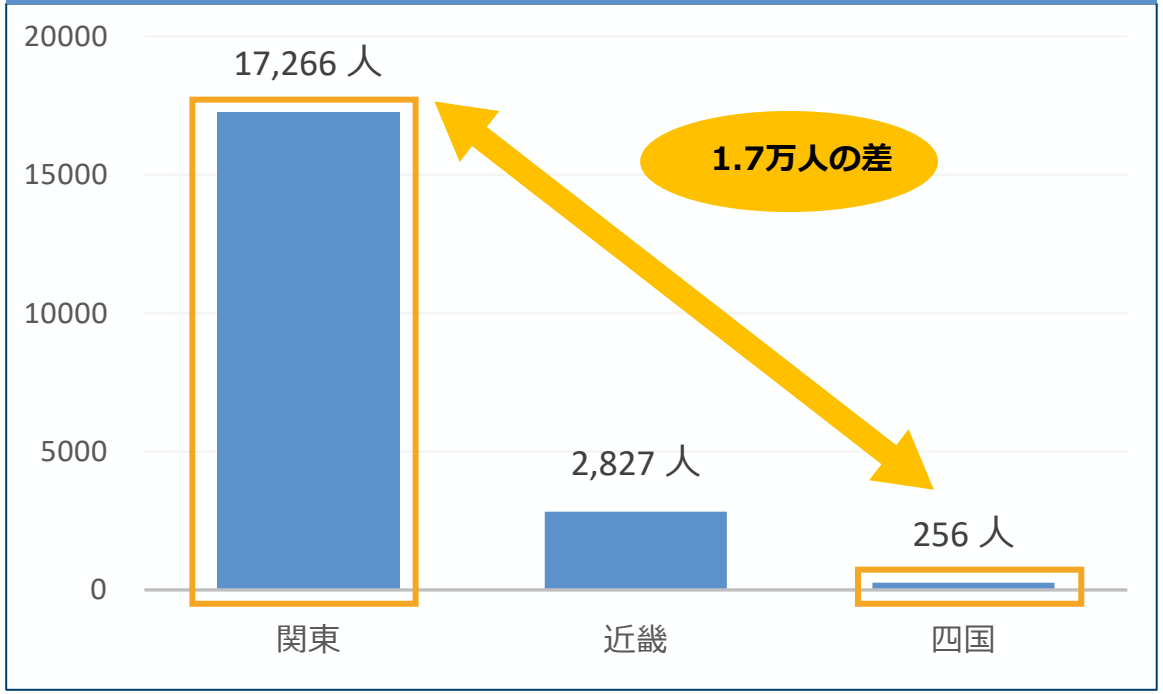
SA自己宣言者数の割合（令和7年12月時点）



➡**SA自己宣言者数の割合は、地域によって様々**であり、**東北地域の自己宣言者数割合は8.3%**に留まる。

出典：IPA提供データ（令和7年12月末時点）及び中小企業庁「令和3年経済センサス-活動調査」を基に経済産業省作成

情報処理安全確保支援士登録者数（令和8年10月時点）



➡**登情報処理安全確保支援士（登録セキスペ）登録者数は、地域毎に大きな差**があり、最も多い地域と少ない地域の間には**約1.7万人の差**が見られる。

出典：情報処理安全確保支援士登録者について（2025年10月1日時点）を基に経済産業省作成

地域SECUNITYの活動内容の横展開促進

- 地域SECUNITY団体の活動促進が普及・啓発にとって必要不可欠。そこで、**地域SECUNITY間の「横のつながり」を作るとともに、各地域の取組事例を共有し、地域SECUNITYの活動活性化を図るため、**令和８年３月、経済産業省及びIPAにおいて「地域SECUNITY連絡会」を開催予定。
- 地域SECUNITY連絡会で各団体から発表いただいた内容に基づき、**今後、経済産業省において地域SECUNITYプラクティス集として情報発信していく**予定。

地域SECUNITY連絡会

地域SECUNITY連絡会は、地域で普及・啓発活動に取り組む団体から、取組内容や工夫したことなどを発表いただくもの。
取組事例を地域SECUNITY間で共有することで、地域SECUNITY活動の活動促進につなげる。

【地域SECUNITY連絡会での発表予定団体】
- ○ 四国総合通信局
- ○ 新潟県警本部
- ○ 一般財団法人関西情報センター（KIIS）
- ○ 一般社団法人鹿児島県情報セキュリティ協議会（KPSEC）
- ○ 一般社団法人LOCAL
- ○ 宮崎県サイバーセキュリティ協議会
- ○ YOKOSUKA情報セキュリティプロジェクト

（参考）令和７年２月開催の地域SECUNITY連絡会での主な発表内容

農業をテーマとした普及･啓発活動

・農業のような一次産業はITが進んでいない一方で、個人としてはスマートフォンの利用が進んでいることや、若手就農者がECサイトを利用している実態があることから、農業分野においてもサイバーセキュリティ対策が必要と判断し、農業をテーマとした普及･啓発活動を実施。

⇒農業分野において多くの集客が実現

地域SECUNITYのノウハウを活用

・八戸地域の方々からの依頼を受け、一般社団法人地域セキュリティ協議会（ASC）のノウハウを共有、九州地域と東北地域と連携してサイバーセキュリティセミナーを企画･開催。

⇒地域SECUNITY活動のノウハウを他の地域でも活用することによって、セミナー開催の向上が図られる

具体的メッセージをキャッチフレーズとする

・千葉県地域SECUNITY連絡会では、「かっこつけない、お金をかけないセキュリティ対策」をキャッチフレーズに参加を呼びかけ。キャッチフレーズの効果もあって、105名の中小企業に参加いただいた。

⇒中小企業に向けた具体的メッセージをキャッチフレーズとすることで、より高い集客につながる

出典：経済産業省「地域セキュリティコミュニティ 【地域ＳＥＣＵＮＩＴＹ】 活動促進のためのプラクティス集　第3版」抜粋

サプライチェーン全体での対策強化に向けたSC3の主な活動

- SC3（サプライチェーン・サイバーセキュリティ・コンソーシアム）は、**サイバーセキュリティに関する情報の共有と協力体制の強化**を目的として、**2025年7月にIPAとの間で相互協力を締結。**
- **IPAと連携**しながら、産業界におけるサプライチェーン・セキュリティ対策強化に向けた**取組を実施。**

サプライチェーン・セキュリティ・フォーラム

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

SCS評価制度推進SWG・持続可能なSC対策検討SWG

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

工場セキュリティセミナー

- ✓ 半導体産業のある九州地域において**「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の普及に向けた講演**を実施。
- ✓ 工場のスマート化が製造業発展のカギであることを踏まえ、**製造業全体の対処能力底上げと普及促進を目的**として実施。

登録セキスペ向け指導要領

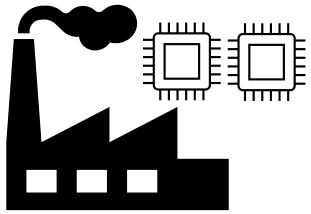
- ✓ 中小企業に対してSCS評価制度の支援ができる**登録セキスペ育成のための指導要領作成の支援**を実施。
- ✓ 本指導要領は、中小企業がSCS評価制度の★を取得する際、セキュリティ専門家として登録セキスペがその適合可否を確認・助言することを念頭とした内容。

個別の領域に関する取組

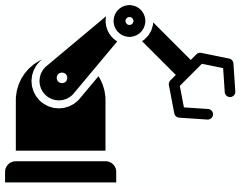
半導体関連産業におけるセキュリティ対策水準向上を通じた競争力確保

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

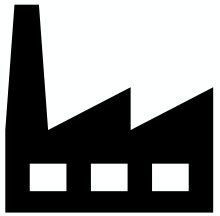
半導体関連産業におけるセキュリティ要求事項



半導体**デバイスメーカー**



半導体**装置メーカー**



半導体**部素材メーカー**

2025年度に策定。
投資促進関係施策との紐付けを順次実施

2026年度内の策定に向けて検討

今後検討

セキュリティ要求事項の現状

半導体デバイスメーカーに対するセキュリティ要求事項の概要

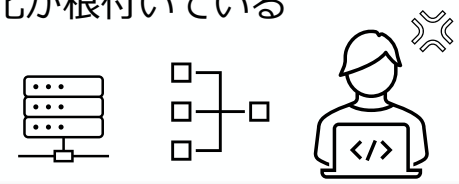
- IT項目（44項目）
  - **サプライチェーン強化に向けたセキュリティ対策評価制度の★4項目**
- OT項目（6項目）
  - **ガバナンスの整備**：１項目
    - 担当者の責任・権限の割り当て等
  - **リスクの特定**：２項目
    - OT領域の資産の可視化等
  - **攻撃等の防御**：２項目
    - 機密情報の扱いの明確化等
  - **インシデントへの対応**：１項目
    - インシデントへの対応手順の明確化等

制御系（OT）システムのセキュリティ確保に向けた新たな検討

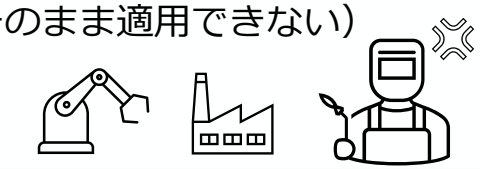
- ITだけでなく、工場の制御系（OT）システムについてもDX化が進む中、IT基盤を経由した攻撃や、オンラインに接続された機器経由での、**OTシステムに影響が及ぶ攻撃等のリスクが高まっている。**
- サイバー事案が発生した際に対応の中核を担うCSIRT（Computer Security Incident Response Team）の整備だけでなく、工場の制御系を中心とした**FSIRT**（Factory Security Incident Response Team）**の整備**や、**両者の一体的な連携、OT固有のセキュリティ対策**についても重要性が増している。
- 上記の状況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

現状の課題（As is）

ITシステム
※CSIRTなどのセキュリティ対応方針と文化が根付いている



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

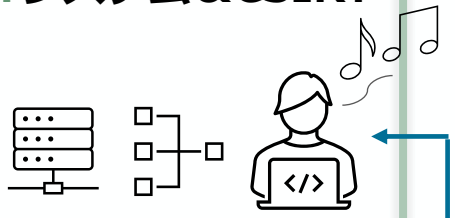


- **IT・OT間の連携が不十分**（連携体制の欠如、OT固有のセキュリティ対策・ベンダ管理等への関与不足等）。

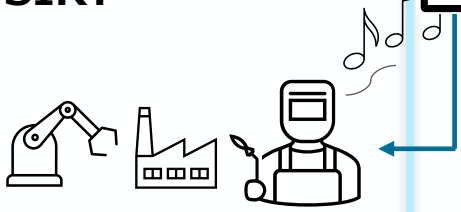
ITシステムがサイバー攻撃を受けると、**OTシステムにも波及**する（工場の稼働停止を余儀なくされる等）。

目指すべき姿（To be）

ITシステム＆CSIRT



工場OTシステム＆FSIRT

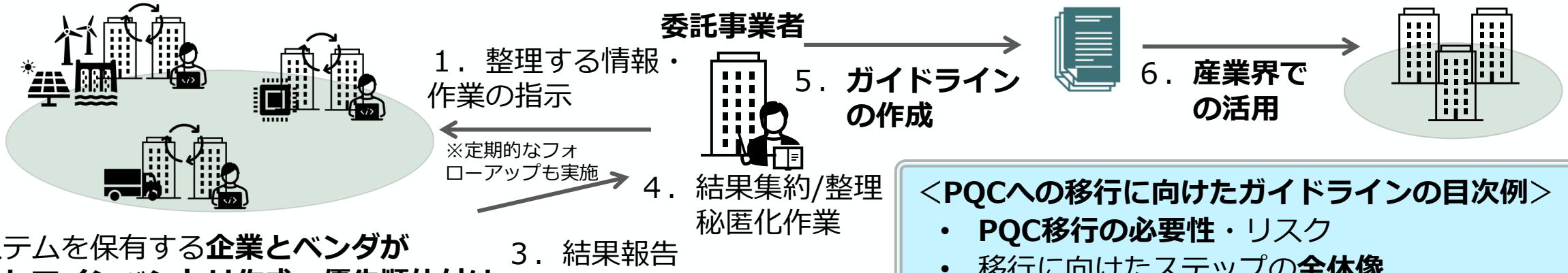


- **IT・OT間が連携**（包括的な監視・CSIRTとFSIRTとの連携体制の構築等）し、一体的かつ有機的に全社のセキュリティを支える。
- IT部門含め全社的に工場OTシステムで用いられる**資産を把握**し、関係する**ベンダとの組織的な連携が**図られている。
- ITシステムがサイバー攻撃を受けても**OTシステムが独立的に動作を継続**する。

耐量子計算機暗号（PQC）への対応に向けた検討

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

クリプトインベントリの実施に係る実証事業のイメージ



＜PQCへの移行に向けたガイドラインの目次例＞

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