経済産業省

資料３

# 第９回
# 産業サイバーセキュリティ研究会
# 事務局説明資料

令和７年５月２３日

経済産業省　商務情報政策局

# 目次

# １．サイバーセキュリティを取り巻く現状

# 最近国内外で発生した主な事案

## ①機微技術情報等の窃取

- 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）
- 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上、SNS等を通じて拡散される二次被害も発生。

## ③重要インフラの機能停止等

- 2024年2月、米国政府機関等が、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（**有事の際にサイバー攻撃を行うためにネットワークへのアクセス権限を確保するような動き**）について注意喚起。
- 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）

## 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・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を用いて**、取引管理の委託先を経由し、㈱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）
- 2025年4月、㈱インターネットイニシアティブのメールセキュリティサービスへの不正アクセス事案が発生。**メールアカウントや他社クラウドサービスの認証情報など、586の契約先において情報漏えい**が確認。（2025年4月22日時点）

# 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では高速な解読が可能とされる。
- 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（闇市場）の存在

- **ダークウェブ上の闇市場**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。

## 生成AIを通じた情報漏えい・サイバー攻撃リスク

- DeepSeek社の生成AIモデルは急速に普及。一方、**利用データが中国政府に流出するリスク**や**マルウェア作成等への悪用**が懸念され、各国で**利用の禁止・制限や注意喚起等**が行われている。

（出典）(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威 2025」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」、各種報道情報　等

# 地政学動向の変化に伴うサイバーリスクの高まり

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

## サイバー攻撃の変遷

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

**■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 Typhoon・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”

## 国家関与が疑われるサイバー動向に関する報道

- **中国における脆弱性報告義務**
  - 中国政府は2021年９月、ソフトウェア等の脆弱性発見から48時間以内の政府報告を義務付け
  - 報告件数は16件（2021年）から242件（2024年1～6月）へ急増
  - 2021年以降、中国の関与が指摘される攻撃のリポートが急増

（出典）日本経済新聞記事（2024年８月25日掲載）

- **台湾当局に対するサイバー攻撃**
  - 2024年における台湾当局に対するサイバー攻撃は１日当たり240万件と、2023年から倍増
  - 台湾当局は、その大半が中国サイバー軍による「グレーゾーン・ハラスメント」とみている

（出典）Reuters記事（2025年１月６日掲載）

## 我が国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

初選出

（出典）独立行政法人情報処理推進機構（IPA）「情報セキュリティ10大脅威2025」、
警察庁「令和6年におけるサイバー空間をめぐる脅威の情勢等について」を基に作成。

# サイバーセキュリティ政策に関する国際的な動向

- 欧米を中心に、①**セキュア・バイ・デザイン***の概念に基づく**製品のサイバーセキュリティ対策に対する要請**や、②**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。

# （参考）足下の世界情勢を踏まえた対応

- 米国トランプ政権の政策も踏まえ、サイバーセキュリティを取り巻く環境が今後大きく変化していく可能性。
- 産業界、とりわけ裾野の広いサプライチェーンを持つ企業のサイバーセキュリティ対策強化の動きが緩まらないよう、**関係諸国との連携を一層強化**するとともに、**インド太平洋地域における我が国サイバーセキュリティ施策の展開に力を入れていく**必要。
- サイバーセキュリティの脅威の変化に備え、我が国における**セキュリティ産業・技術基盤の強化**も図る必要。

## 米国トランプ政権の政策（2025年5月中旬時点）

### ①米国における国内政策の見直し

- 米サイバーセキュリティ当局（CISA）職員が40%削減される可能性
- 米サイバー・コマンドによる対露サイバー作戦一時停止
- 米国際開発庁（USAID）の本部閉鎖

### ②米国による関税措置

- 全ての国/地域を対象に10%の一律関税発動。
- 一部国/地域ごとに異なる税率（※）を上乗せで設定。

（※）一部発動は保留中

- 日本：24%
- 中国：34%
- EU：20%
- 英国：10%
- インド：26%

# ２．これまでの施策の進捗

# 施策の進捗①（経済産業省におけるサイバーセキュリティ政策全体像）

- 本研究会において提示したアクションプランを踏まえ、**以下の４つの柱の下、産業界におけるサイバーセキュリティ対策強化に向けた取組を推進（具体的な進捗は次頁以降）**。
- これらの取組を推進するためのリソースとして、**毎年度数十億円規模の予算を確保**しつつ、研究開発の実施については**約300億円の予算を確保**するとともに、中小企業等によるセキュリティ対策支援のために**総額3,400 億円の予算の一部を確保**。

## 経済産業省におけるサイバーセキュリティ政策の全体像

**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
- 経営ガイドラインの活用促進
- サイバーセキュリティお助け隊サービスの普及促進
- 日米欧によるインド太平洋地域向けの能力構築支援　等

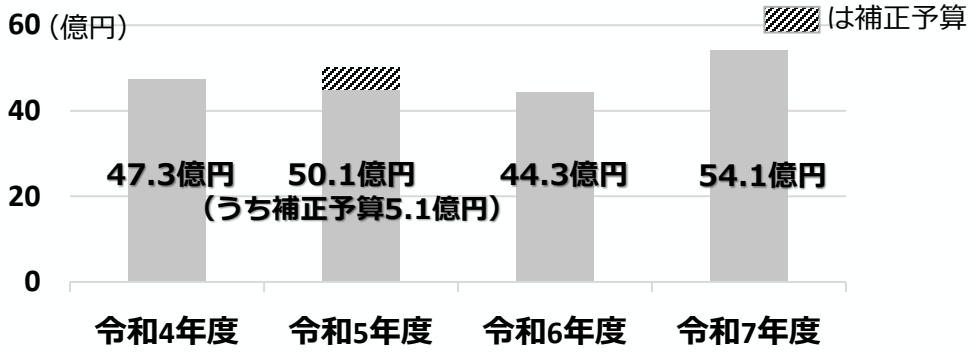
**②セキュア・バイ・デザインの実践**
- IoTセキュリティ適合性評価制度（JC-STAR）の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進
- QUAD上級サイバー会合、G7等を通じた各国間連携

**③政府全体でのサイバーセキュリテイ対応体制の強化**
- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- 改正保安３法を踏まえた事故調査体制の構築
- サイバー攻撃被害情報の共有促進に向けた検討　等


**④サイバーセキュリティ供給能力の強化**
- 先進的サイバー防御機能・分析能力の強化
- サイバーセキュリティ産業の成長加速化、製品/サービスの国内自給率向上に向けた政策検討
- 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）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)

## 経済産業省サイバーセキュリティ関連予算の推移




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

## その他関連予算事業との連携

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

②中小企業生産性革命推進事業（IT導入補助金）
- IT導入補助金において、SECURITY ACTIONを申請要件化するとともに、サイバーセキュリティお助け隊サービスの導入費用を補助

（令和６年度補正予算（**3,400億円**）の内数）

# 施策の進捗②（サプライチェーン全体での対策強化）

- 企業のセキュリティ対策の水準を可視化する**サプライチェーン対策評価制度**の検討や**新たなガイドライン**の策定を推進。
- **サイバーセキュリティお助け隊サービス**を始めとした中小企業向け施策の**広報・発信**に取り組み、同サービスの利用者数は**約7,000件まで増加**。

## 新たな制度・ガイドライン等の整備

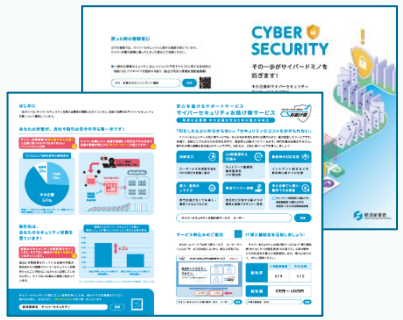
**中小企業向け**
- ○ **サプライチェーン企業の対策水準の可視化（中間整理）**
- ○ **中小企業に効果的なサイバーセキュリティの取組の整理**
- ○ **工場セキュリティガイドラインの改訂**

**半導体関連企業向け**
- ○ **半導体デバイス工場のOTガイドライン（素案）の策定**

**地場ベンダ向け**
- ○ **地域のITベンダーの能力向上に係る手引きの策定**

## 中小企業向け施策等の広報・発信実績

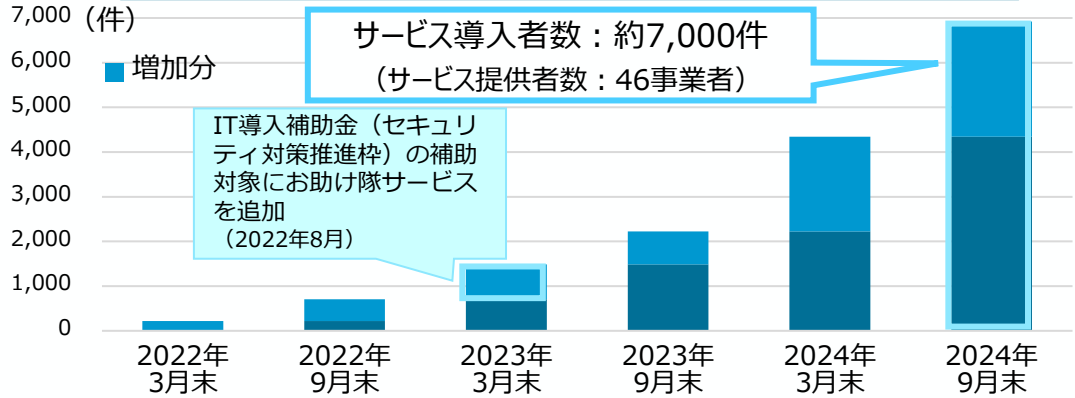

政府広報（ラジオ、雑誌、広告）を活用した普及啓発




サイバーセキュリティお助け隊リーフレットを新たに作成し、関係省庁と連携して中小企業支援団体等に展開


経済産業省ウェブサイトの大規模な改修

## 「サイバーセキュリティお助け隊」利用件数




※サービス提供者数は2025年3月末時点

## 人材育成施策・地域ワークショップの支援実績

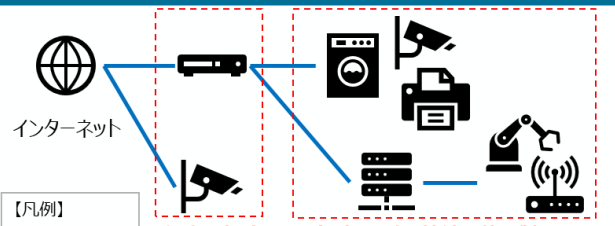
| | |
|---|---|
| **中核人材育成プログラム修了者数** | 435名(2017年～2024年) |
| **情報処理安全確保支援士** | 23,751名(2025年4月時点) |
| **セキュリティ・キャンプ参加者数** | 全国大会: 1232名(2004年～)<br>ネクストキャンプ: 53名(2019年～)<br>ジュニアキャンプ：11名(2023年～) |
| **IPA　セキュリティ講演者派遣** | 65件(2024年度) |
| **IPA　セキュリティセミナー支援** | セミナー開催支援: 26件<br>演習（経営者向けインシデント対応机上演習 等）：18件(2024年度) |

# 施策の進捗③（セキュア・バイ・デザインの実践）

- IoT製品のセキュリティ対策レベルを評価・可視化する取組として、**IoTセキュリティ適合性評価制度（通称：JC-STAR）を2025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**）。
- 我が国政府や米国等も含めた17カ国で共同署名をした**セキュア・バイ・デザインのガイダンス**も踏まえ、**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。
- これらの取組・制度について、**G7をはじめとする関係国との調和**を図るべく、議論も進展。

## JC-STAR制度（ロゴ・ラベル、対象製品の概要）

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)

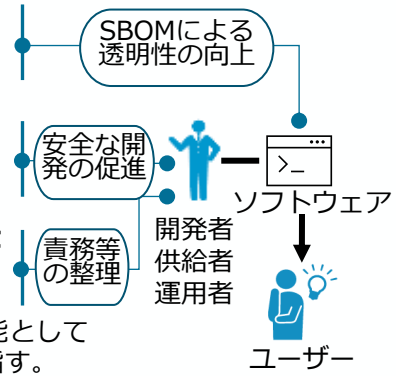



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

## セキュアなソフトウェア開発・流通に向けた取組

- **SBOM（ソフトウェア部品構成表）の導入促進に向けた手引きver2.0**（2024年8月）
- **安全なソフトウェア開発のための事業者向けガイダンスの中間整理**（2025年3月）
- **サイバーインフラ事業者**（※）**が果たすべき責務等を整理したガイドライン案**（2025年3月）

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




## IoT製品及びソフトウェアに関する関係国との制度・取組調和に向けた成果文書

### G7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…

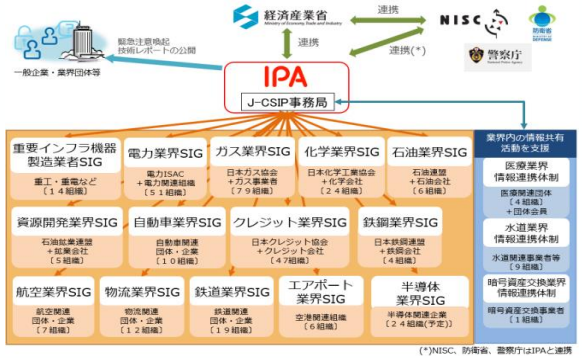
# 施策の進捗④（政府全体のサイバーセキュリティ対応体制の強化・サイバーセキュリティ供給能力の強化）

- サイバー攻撃が高度化する中、IPAの**サイバーレスキュー隊（J-CRAT）**を通じた標的型サイバー攻撃（APT）等の初動対応支援や**情報分析・共有体制等の強化**を実施。
- 2024年7月に経済安全保障重要技術育成プログラムでの**大規模な研究開発**を開始。2025年3月には「**サイバーセキュリティ産業振興戦略**」をとりまとめ。

## IPA/J-CRAT活動実績

| 年度 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|
| 相談・情報提供数 | 375 | 330 | 366 | 431 |
| 支援数 | 94 | 163 | 173 | 210 |
| オンサイト支援数 | 9 | 43 | 65 | 81 |
| アクティブレスキュー数 | ー | ー | 100 | 106 |

## 情報共有枠組みの構築




IPAがAPT攻撃等の重大なサイバー攻撃に関する情報共有を行う情報ハブ（集約点）の役割を担う**サイバー情報共有イニシアティブ（J-CSIP）**において**2025年3月に半導体業界SIG、2025年4月に暗号資産交換業界情報連携体制新たに組成**

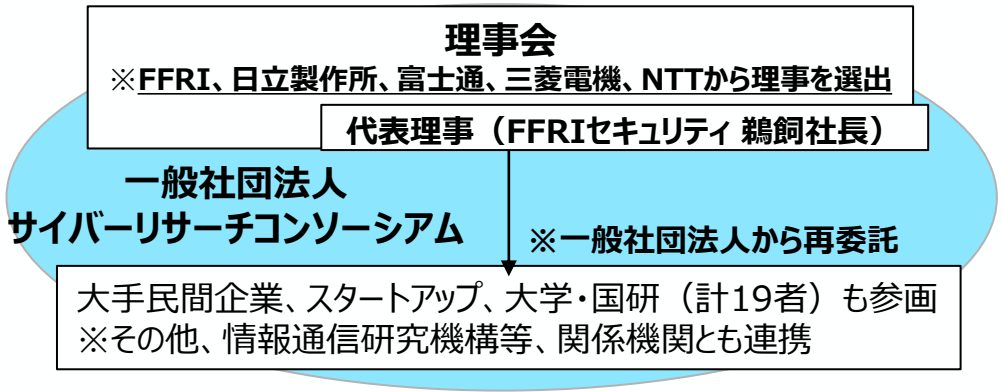
- 防衛省・経済産業省・IPAによる包括的な連携協定（令和6年12月）
  - ①自衛隊によるIPAの取組への参画等を通じた産業界向けセキュリティ支援、②**情報提供等を通じた防衛産業との連携強化**、③3者間の新たな協議体（枠組み）の設置について３者で共同して推進。

## 「サイバーセキュリティ産業振興戦略」のとりまとめ

- **背景**：
  サイバーセキュリティ対策の必要性が高まる中、需要の拡大に見合った供給力を確保するため、我が国セキュリティ産業の振興が不可欠。
- **主な政策対応**：
  ①スタートアップ等の実績作り／有望な製品・サービスの認知度向上
  ②有望な技術・競争力のある製品・サービスの創出、発掘の容易化
  ③供給力拡大を支える高度人材の確保、国際市場展開の促進
- **KPI**：10年以内に国内企業の売上高約3兆円超（足下は0.9兆円）

## 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）

### 研究開発の体制



# ３．新たなサイバーセキュリティ政策の方向性

# 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

- NISC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**

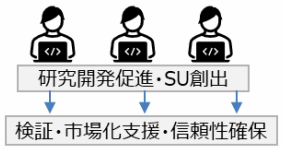
## ③政府全体でのサイバーセキュリティ対応体制の強化

- 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**

# 政府全体における経済産業省の今後の政策の位置付け

- 経済産業省では、**産業界に向けた政策を企画・実行**することにより、政府機関等の防御強化等NISCをはじめとする関係省庁による取組と両輪となって、**政府全体の取組に貢献**していく。

## 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

＜横断的課題等＞
- 政府機関や重要インフラ事業者等の対策強化
- **サイバーセキュリティ人材の育成・確保**
- **中小企業や地域における対策強化**
- **国産セキュリティ製品・サービスの供給強化**
- 被害組織の負担軽減（報告様式一元化）　等

## サイバーセキュリティ2024（特に協力に取り組む施策）

- 政府機関や重要インフラ等の対処能力の向上
- **サプライチェーン・リスクへの対応強化**
- **DXを推進・支援する取組の強化**
- **欧米主要国をはじめとする関係国との連携の一層の強化**　等

**貢献**

## 経済産業省における今後の政策の方向性

### サイバー対処能力強化法への対応
- ソフトウェア脆弱性情報の取扱い対応体制の強化　等

### サプライチェーン全体での対策強化
- 企業の対策水準の可視化、中小企業支援　等

### セキュア・バイ・デザインの実践
- 諸外国と連携したIoT・ソフトウェア制度整備　等

### 政府全体でのサイバーセキュリティ対応体制の強化
- IPAのサイバー情勢分析能力強化　等

### サイバーセキュリティ供給能力の強化
- 国産スタートアップ等の育成、技術開発　等

# 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

SC対策強化

- **異なる取引先から様々な対策水準を要求される、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**を検討。
- 2025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<br>• 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：<br>• 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：<br>• 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：<br>• 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の例

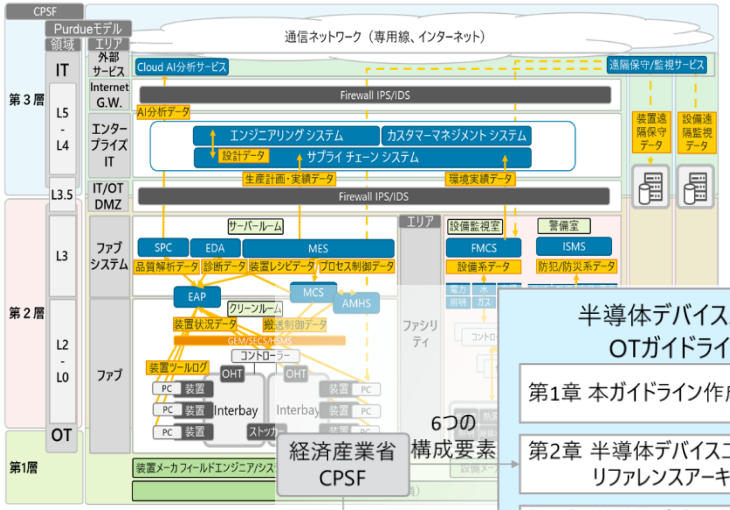
- **国内外の関連制度・評価制度との整合性確保、相互認証**
- 対策推進のための企業への支援の在り方（**専門家の活用促進、中小企業支援策との連動、評価機関の支援**）
- **下請法や価格転嫁に関する課題の整理**
- 実効性の強化に向けた取組（政府機関等における**調達要件化**、サプライチェーン上の取引先や投資家等の**ステークホルダとの対話での活用**等の促進）

# 半導体関連産業のセキュリティ対策水準の強化

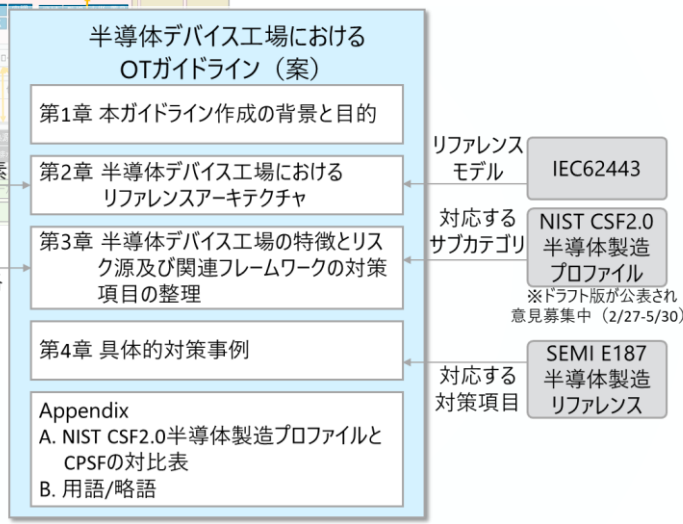
SC対策強化

- 半導体関連産業の国内投資の促進が強力に進められているところ、**継続的な半導体デバイス生産活動を確保**し、**知財・先端技術情報等を保護**する観点からも、**サイバーセキュリティ対策を進めることが重要。**
- 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。とりまとめた対策の内容を**経済産業省の投資促進関係施策の要件等に紐付けること等を検討し、その実効性を強化**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）




※半導体産業における**国際的なセキュリティ規格との整合性**も考慮しつつ作成中




経済産業省 CPSF

6つの構成要素

海外の主要規格との対応関係

リファレンスモデル → IEC62443

対応するサブカテゴリ → NIST CSF2.0 半導体製造プロファイル

※ドラフト版が公表され意見募集中（2/27-5/30）

対応する対策項目 → SEMI E187 半導体製造リファレンス

※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

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：17、SIG参加組織数：319（2025年4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）

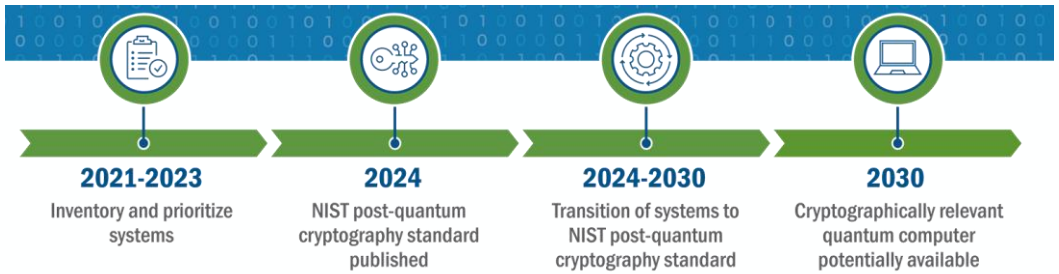
# 関係省庁と連携した耐量子計算機暗号への対応の検討

SC対策強化

- 量子コンピュータの進展による既存暗号の危殆化のリスクに備え、米国をはじめとした各国において、**耐量子計算機暗号（PQC）への移行に係る検討**が進められている。
- 我が国においても、技術的課題、安全保障、国際連携等の多様な視点から、**社会全体におけるPQCへの移行を進めるための道筋を描く**ことが必要。経済産業省としても、産業界における移行促進策の検討や関連技術の開発など、産業政策的観点から政府全体の**検討に貢献**していく。
- CRYPTRECにおいて、電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）へ順次PQCを掲載するため、2025年度中に**PQCの安全性評価・実装性能評価を開始予定**。

## 米国におけるPQCへの移行に向けた動向

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




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

## CRYPTRECにおける活動状況

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

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

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

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

**「2025 年度暗号技術評価委員会活動計画」（2025年3月）**

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

（出典）CRYPTREC 2024年度 第１回 暗号技術検討会資料

# 中小企業等向けの支援の一層の強化

SC対策強化

- サプライチェーン全体でサイバーセキュリティ対策を強化するためには、中小企業等におけるセキュリティ対策の一層の促進が不可欠。一方、**セキュリティ対策の必要性に対する認識不足**や**十分なリソースの確保の困難性**といった課題も存在。
- こうした中小企業等に対し、**必要性喚起・施策の普及広報の強化**とともに、**「サイバーセキュリティお助け隊サービス」の拡充**や**セキュリティ人材とのマッチングスキームの構築**など支援策を一層強化する。

| 中小企業等における課題 | 対応の方向性 | 今後の具体的な取組 |
|---|---|---|
| **セキュリティ対策の必要性を感じていない** | 普及広報内容・普及方法の改善 | **「自分事化」できる事例の提示：**<br>• 主要な業種における中小企業によく見られるサイバー攻撃の侵入口や、実際に攻撃された場合の想定被害額などを、必要な対策手法とセットで提示。<br>**面的な普及広報活動の実施：**<br>• 中小企業と相対する商工会議所や地方銀行等の支援機関との連携を強化し、地域SECUNITYとして各地域の文脈に沿った活動を一層推進。 |
| **コスト面・知識不足・人材不足から有効な対策ができない** | 安価で最低限のセキュリティ確保が可能なパッケージサービスの提供 | **「サイバーセキュリティお助け隊サービス」の拡充等に向けた見直し：**<br>• 普及広報に加え、「ゼロトラスト」などの技術動向に対応し、提供事業者にとって持続可能な価格設定とする観点等から、サービス基準・運用の見直しを実施。<br>• 「サプライチェーン対策評価制度」に対応したサービスの在り方について検討。 |
| | 社内人材育成・外部人材の探索コストの低減 | **内部人材育成・外部人材確保の具体的手法の提示：**<br>• 中小企業等が実施すべきセキュリティ対策の状況に応じた人材確保・育成の実践的方策「実践的方策ガイドβ版」について活用事例紹介等含め改善。<br>• IPAの人材育成プラットフォーム等を活用し、教育コンテンツを拡充。<br>**外部人材の探索コスト低減：**<br>• 中小企業に対する具体的支援ができる情報処理安全確保支援士（登録セキスペ）のリストである「アクティブリスト」を整備。支援機関等による活用も促進。 |

# サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の改訂に向けた検討

SC対策強化

- 「Society5.0」における**セキュリティ対策の基盤**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2019年4月に策定・公表**。本フレームワークに基づき各産業分野の特性に応じたセキュリティ対策等を具体化・実践してきたところ、対応する**他の国際規格等は時勢の変化に応じて改訂**が進んでいる状況。例：米国国立標準技術研究所（NIST）Cybersecurity Framework（CSF） ver1.1から2.0への改訂
- 今般、CPSFのメンテナンス主体として、**知見を有する情報処理推進機構（IPA）のデジタルアーキテクチャ・デザインセンター（DADC）を位置付け**た上で、**CPSFの改訂に向けた検討を開始**する。
- また、国際調和の観点からISO/IEC JTC1/SC27/WG4にて**CPSFのモデル等を盛り込んだ国際規格の策定**を進めているところ、 2025年3月に承認段階への移行が決定。**2025年度内の発行を目指す**。

## IPA デジタルアーキテクチャ・デザインセンター


- 「**Society5.0**」を実現するための社会や産業構造のアーキテクチャを設計。

- ３つの観点
  - ①縦の連携（サイバーとフィジカルがつながるレイヤー構造）
  - ②横の連携（サービスが相互に繋がるモジュール構造）
  - ③連携を実現するガバナンス（社会に適用できるガバナンス）

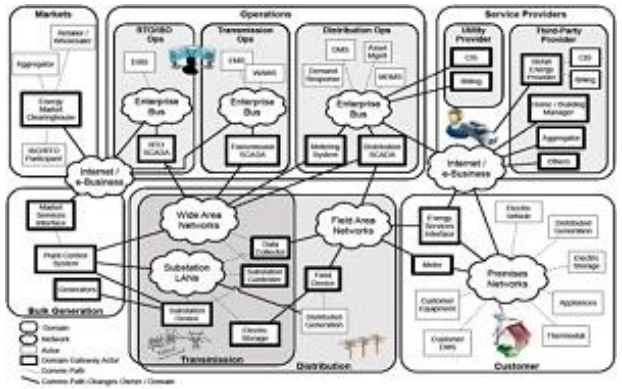
（出典）IPA デジタルアーキテクチャ・デザインセンター（DADC）
https://www.ipa.go.jp/dadc/about.html

## NIST Cybersecurity Frameworkの改訂

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

CSF2.0における6つの機能

| 統治 | 特定 | 防御 | 検知 | 対応 | 復旧 |
|---|---|---|---|---|---|



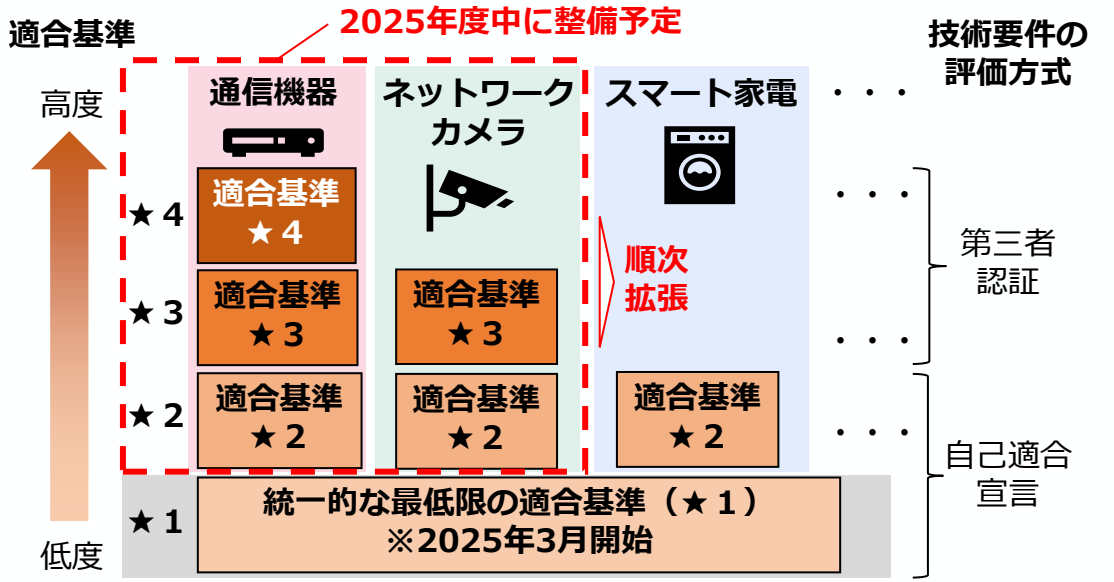
図：Cyber Physical Systems

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

# セキュア・バイ・デザインの実践向けた取組①（IoT製品のセキュリティ確保：JC-STAR）

- 特に政府調達による活用が見込まれる**通信機器とネットワークカメラについて**、2025年度中に、**より高度な基準（★2以上）を策定**するとともに、その他の製品の高度な基準の検討も順次実施。
- 最低限の基準（★１）を含め、**政府調達の要件化等**を通じた地方公共団体、重要インフラ事業者、その他民間企業等への**普及展開**を図るとともに、中小ベンダへの負担軽減策等についても検討を進めていく。
- **外国制度との相互承認**に向け、関係国との調整を加速化する。

## より高度な基準の策定（JC-STAR）




## 相互承認調整を進める外国制度の例

| 国・地域 | シンガポール | 英国 | 米国 | EU |
|---|---|---|---|---|
| 制度名 | Cybersecurity Labelling Scheme (CLS) | Product Security & Telecommunication Infrastructure Act (PSTI) | U.S. Cyber Trust Mark | Cyber Resilience Act (CRA) |
| マーク | CYBERSECURITY LABEL CSA/IOTWABCD | – | U.S. CYBER TRUST MARK | CE |
| 開始時期 | 2020年10月制度開始 | 2024年4月施行 | 2025年より基準策定開始（制度開始時期は調製中） | • 報告義務: 2026年9月<br>• その他: 2027年12月 |
| 任意/義務 | 任意 | 義務 | 任意 | 義務 |
| 対象 | 消費者向けIoT機器 | 消費者向けIoT機器 | 消費者用無線IoT製品 | デジタル要素を含む製品 |

# セキュア・バイ・デザインの実践向けた取組②（ソフトウェアのセキュリティ確保）

SBDの実践

- 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。


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

**＜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

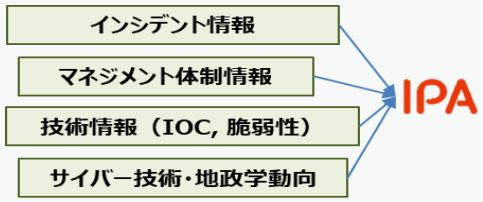

CISA “Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software”

# IPAにおけるサイバー情報集約・情勢分析能力の強化 CS体制強化

- 国家安全保障戦略に基づく対応を強化すべく、IPA第五期中期目標において、**「サイバー状況把握力」を強化し、国家の安全保障・経済安全保障の確保に貢献**する旨を明記。
- 今後、**経済インテリジェンス収集力の強化**等によりサイバー情報の集約・情勢分析機能や対処支援能力の一層の強化を図るとともに、今通常国会で成立した**サイバー対処能力強化法に基づく業務への対応**により、**政府全体のサイバー安全保障体制の強化に貢献**していく。

## サイバー情勢集約・分析機能の強化に向けて進展中の取組

- ＩＰＡが有する産業界とのネットワーク、セキュリティ対策に係る各種制度を駆使し、**産業分野のセキュリティ・リスク情報（サイバーインテリジェンス）集約のハブ**として機能を強化。
- 地政学や経済安全保障の専門家の協力も得つつ、経済活動に影響を及ぼすサイバーリスクを統合的に分析することにより、**産業分野に関する脅威評価のハブ**として機能。
- 政府機関、産業界の経営レベルと現場の双方との連携対話を強化し、**防御や抑止対応に資する情報共有／対応支援活動のハブ**として活動を推進。（ex. 重要インフラ事業者等に対するAPT攻撃に関するハントフォワード活動、主要産業に対するサイバー脅威情報の共有・注意喚起　等）





## 今後の取組の方向性

＜経済安全保障の実現に向けた取組への貢献＞

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

＜セキュリティ産業振興の観点も踏まえた産業界の防御力強化＞

- **APT検知・テレメトリ運用システムの構築**（有望スタートアップ製品等の活用等も検討）

＜サイバー対処能力強化法への貢献＞

- 法定委託事務（届出・報告情報の整理・分析、注意喚起、脆弱性情報の取扱い等）実施のための**体制強化**
- 製品開発者及び利用者における**脆弱性対策の実効性確保のための構造改善支援**（PSIRT構築等）
- 基幹インフラ事業者に対する**早期警戒システムの実証**（SBOM連携等）
- **企業組織向け相談窓口**の新規開設（2025年4月～）

# 「サイバーセキュリティ産業振興戦略」の今後の展開 CS能力強化

- 我が国へのサイバー攻撃の特異性に対応し安全保障を確保する等の観点から、**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**するなど、**包括的な政策対応を**2025年３月に**とりまとめ。**
- 「10年以内に国内企業の売上高を足下から３倍超」とのKPIの達成に向け、**具体的な取組を深化**させていく。

## 今後のロードマップ

**■STEP１（約３年以内）【裾野の拡大】**
- ✓ J-Startup選定企業をはじめスタートアップ数の拡大を図る
- ✓ プロダクトを開発する「トップガン」人材の増加を図る

**■STEP２（約５年以内）【競争力の強化】**
- ✓ 市場における我が国企業のマーケットシェア拡大を図る（とりわけ量子・AIなど先端的な技術への対応に資する技術の社会実装を進める）

**■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・企業について、市場や社会的な影響力を強める
- ✓ ユーザー企業が、自社の状況やリスクに応じて様々な製品・サービスを選択できる環境を構築する
- ✓ 我が国特有の攻撃への対応や企業の海外進出を通じて安全保障・デジタル赤字解消にも貢献する

## 「サイバーセキュリティ産業振興戦略」後の主な対応

### 政府機関等による有望なセキュリティ製品・サービスの活用機会の提供
- 足下の取組として、まずは、**IPAのセキュリティ分析・対処支援等**において、**先進のスタートアップ製品・サービスを試行的に活用**。併せて、スタートアップの製品・サービスの試行的な活用を行う**政府機関等の主体・取組を拡大**

### 製品・サービスのセキュリティや信頼性を確認する制度の構築・運用
- **JC-STARの適切な運用・制度拡張**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**」「**SSDF導入ガイダンス**」を成案化／それらへの**適合を確認する枠組み構築**を含め、**必要な制度構築・活用促進に向けた施策**を検討

### 「トップガン」等のセキュリティ供給人材の確保に向けた新たな政策検討
- **セキュリティ・キャンプの拡充**や**情報処理安全確保支援士（登録セキスペ）の活用促進**を通じた高度専門人材育成を進めつつ、新製品・サービスを開発・導入・評価できる**セキュリティ供給人材の育成に向けた政策対応の在り方**についても検討

### アジア太平洋地域への進出を見据えた我が国のセキュリティ政策の展開
- 日ASEAN政府間会合等を活用し、我が国企業が多く進出するアジア太平洋地域における**我が国のサイバーセキュリティ政策の普及・展開を推進。我が国サイバーセキュリティ製品・サービス提供事業者の海外進出を後押し**する素地を構築

**【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）】**

**【政府全体の会議体や本研究会WG等を通じ、FUを実施】**

# ４．産業界へのメッセージ

協力：

- 鴨田 浩明　　株式会社 NTT データ ソリューション事業本部セキュリティ＆ネットワーク事業部長
- 佐々木　弘志　　フォーティネットジャパン合同会社　OTビジネス開発部部長　（IPA ICSCoE 専門委員）
- 政本　憲蔵　　株式会社マクニカ　セキュリティ研究センター長

※敬称略、五十音順

# 「産業界へのメッセージ」の背景

全体向け

- 足下のサイバーセキュリティを取り巻く環境に鑑みれば、**我が国においても一層の対策強化が求められる状況**にある。
  - ① 急速に普及しつつある生成AIをはじめとする**デジタル化の進展**や世界的な**地政学リスクの高まり**、**サイバー攻撃の深刻化・巧妙化**などにより、サイバーリスクは高まっている。
  - ② このような**サイバー攻撃が、国民生活、社会経済活動及び安全保障環境に重大な影響を及ぼす可能性**も大きくなっている。
  - ③ 米欧等においても産業界におけるサイバーセキュリティ対策強化に向けた**制度整備の動きなどが活発化**している。
- こうした状況を踏まえ、まずは、「**経済産業省**」として、**デジタル時代の社会インフラを守る**との観点から、 NISC等関係省庁との連携の下、以下の取組を進めていく。
  - ① **既存施策の普及・啓発**活動の強化
  - ② 政府調達等への要件化を通じた実効性強化や、国際連携を前提とした制度構築、セキュリティ市場の拡大に向けたエコシステムの構築、官民のサイバー状況把握力・対処能力向上に向けた**新たな施策**
  - ③ 産業界からの意見聴取など、官民の協力関係の維持・発展を前提とした、取組の**不断の見直し**
- その上で、「**サイバーセキュリティを実践する各企業・団体**」 、「**ITサービス・製品提供事業者**」、「**被害組織を直接支援する専門組織**」の皆様においては、我が国全体のサイバーセキュリティ対策水準強化の観点から、 それぞれ**次ページ以降に提示する対応**をお願いしたい。

# サイバーセキュリティを実践する各企業・団体（経営層）の皆様へ

経営層向け

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

**<サイバーセキュリティ経営ガイドライン（ポイント）>**

**1．経営者が認識すべき３原則**

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

**2．経営者がCISO等に指示すべき１０の重要事項**

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

## 1．セキュア・バイ・デザインの実践

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

## 2．中小企業向け施策の積極的活用（促進）

- 中小企業においては、**「サイバーセキュリティお助け隊サービス」など中小企業向け施策の活用**も検討する。
- 大企業においては、**パートナーシップ構築の観点**からも、中小企業のビジネスパートナーに**同サービス等の活用を促す**。

## 3．価値創造経営の一環としての位置付け

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

サイバーセキュリティ経営ガイドラインと支援ツール：https://www.meti.go.jp/policy/netsecurity/mng_guide.html

# サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ①

実務層向け

- 最近の国内外の動向を踏まえ、**特に以下の取組を強化していただきたい**（詳細は次ページ以降）。
  - ※ 経済産業省が策定した実務担当者向けガイドライン（被害情報共有・公表ガイダンス等）や関係制度（JC-STAR等）概要など各種政策文書については、次ページ以降のリンクや経済産業省ウェブサイトを参照いただきたい。

## 1．セキュア・バイ・デザイン等の実践

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

## 2．サプライチェーン全体での対策強化に向けた対応

- VPNなど**自組織の**不正侵入経路となりうるポイントを把握する上で**有効な対策**とされるASM（Attack Surface Management）等の外部サービスを活用する
- 特に大企業においては、サプライチェーンに参加する中小企業等への助言・支援を行う（**「サイバーセキュリティお助け隊サービス」などの支援施策の紹介**、**対策状況調査・改善に向けた対話等**）

## 3．被害時の専門組織等への情報共有

- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照し、サイバー攻撃の被害に遭った場合等には、適時の**専門組織への相談及び所管省庁等への報告**等を行う
- 特に、国家支援型と推定される標的型サイバー攻撃の場合には、まずは警察やIPAなどの相談窓口に相談する


経済産業省「サイバーセキュリティ政策」

# サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ②

実務層向け

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

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

## 趣旨･背景･補足

- 「セキュア・バイ・デザイン」は、**セキュリティの責任は製造者等が追うべきである（「責任のリバランス」）**、という**欧米諸国を中心に提唱されている概念**。2023年10月に我が国を含む13か国が共同署名した**セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンス**の中でも、**ユーザ組織（顧客）への提言も含まれているところ、今後、当該提言を踏まえたユーザー組織における対応が全世界レベルで求められていくことが想定される**。
- 経済産業省では、本文書も踏まえ、**「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」**を2025年3月に公表したところ。この中で、ユーザー組織（顧客）に求められる責務として、リスク管理とセキュアなソフトウェアの調達・運用についても提示している。加えて、**IoTセキュリティ適合性評価制度（JC-STAR）を構築・2025年３月に制度運用開始**し、セキュアなIoT製品を容易に選択できる環境整備を進めているところ。引き続き、各企業・団体が上記メッセージをより具体的に理解し、実践しやすい環境を整備していく。
- ITサービス・製品等提供事業者に対してセキュリティ慣行を求めることに関して、外部委託契約書等に、**セキュリティインシデント発生時の連携体制**や、**契約違反時の具体的なペナルティ**（損害賠償、契約解除の条件等）を**明文化**することも考えられる。

## 関係する政府文書･窓口等

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

# サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ③

実務層向け

- VPNなど**自組織の**不正侵入経路となりうるポイントを把握する上で**有効な対策**とされるASM（Attack Surface Management※）等の外部サービスを活用する

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

## 趣旨・背景・補足

- サプライチェーン全体での対策を強化する上で、まずは自社のセキュリティ対策を確認・強化することが第一歩である。例えば、経済産業省の「サイバーセキュリティ経営ガイドライン」では、PDCA サイクルによるサイバーセキュリティ対策の継続的改善の重要性に触れており、必要に応じて、**目的に応じた脆弱性診断やペネトレーションテスト、情報セキュリティ監査等の外部サービスを利用する**といった対策例を示している。
- また、DXの進展等に伴い**サイバー攻撃の起点が増加する中**で、外部（インターネット）から把握できる情報を用いてIT資産の適切な管理を可能とする**ASMは**、VPN（Virtual Private Network）などの不正侵入経路となりうるポイントを把握する上で**有効な対策**とされている。経済産業省が公表している「ASM（Attack Surface Management）導入ガイダンス」などを参照することができる。

## 関係する政府文書・窓口等

- 経済産業省「サイバーセキュリティ経営ガイドラインと支援ツール」
- 経済産業省「『ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～』を取りまとめました」（令和５年５月）

# サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ④

実務層向け

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

## 趣旨・背景・補足

- サプライチェーン全体のセキュリティ対策水準を強化するためには、自社のサプライチェーン上にある（＝取引先である）、**中小企業等におけるセキュリティの確保も求められる**。「サイバーセキュリティ経営ガイドライン」においても、以下の対策例が掲げられている。
  - サプライチェーン上での対策の底上げの手段として、「サイバーセキュリティお助け隊」等の中小企業向け施策を活用する
    ※　「サイバーセキュリティお助け隊サービス」は、中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価（例：月額1万円以内）に提供するサービス。約7,000件の利用実績（2024年９月末時点）がある。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。
  - サプライチェーンにおけるサイバーセキュリティ対策を担保する手段として、**第三者による評価検証結果を活用する**（認証制度の活用、助言型外部監査の実施等）
- さらに、中小企業庁「パートナーシップ構築宣言取組事例集Ver1.2」においても、**サプライヤー向けの対策状況調査（アンケート調査）・フィードバック（リスクの解説や改善方法のヒント提供）**に努めている事例も掲載されており、**取引先とのパートナーシップ構築**の観点からも、こうした取組を参考とすることが有用。
- なお、取引先に対してサイバーセキュリティ対策を要請するケースも想定されるが、その際、独占禁止法等**関係法令の適用関係**が論点となる。こうした課題に対応するため、経済産業省と公正取引委員会は、2022年10月に、取引先への対策の支援・要請に係る関係法令の適用関係について整理した文書を公表したところ。現在、関係省庁と連携して、**更なる具体化（事例や解説の提示等）に向けた検討**を進めており、発注者・受注者双方が良好な関係を構築してサプライチェーンのセキュリティ対策強化に取り組むことを促していく。
- 経済産業省としては、今後も**「サイバーセキュリティお助け隊サービス」の継続的な見直し**など、中小企業向け**支援策を強化**していく。

## 関係する政府文書・窓口等

- 中小企業庁「『パートナーシップ構築宣言』ポータルサイト」
- 経済産業省「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」（令和４年10月）
- 経済産業省「中小企業のサイバーセキュリティ安心サービスのご紹介」
- 中小企業庁「中小企業の情報セキュリティ」
- IPA「ここからセキュリティ！」
- IPA「中小企業の情報セキュリティ」
- IPA「サイバーセキュリティお助け隊サービス制度」

# サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ⑤

実務層向け

- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照し、サイバー攻撃の被害に遭った場合等には、適時の**専門組織への相談及び所管省庁等への報告**等を行う
- 特に国家支援型と推定される標的型サイバー攻撃の場合には、まずは警察やIPAなどの相談窓口に相談する

## 趣旨・背景・補足

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

## 関係する政府文書・窓口等

- サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和５年３月）
- サイバーセキュリティ経営ガイドラインの付録C「サイバーセキュリティインシデントに備えるための参考情報」（令和５年３月）
- 個人情報保護委員会「漏えい等の対応とお役立ち資料」
- 警察署又は都道府県警察本部「相談窓口」
- 経済産業省サイバーセキュリティ課（代表：03-3501-1511　内線：3964）
- IPA 「コンピュータウイルス・不正アクセスに関する届出」「企業組織向けサイバーセキュリティ相談窓口」
- JPCERT/CC「インシデント対応依頼」
- 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「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」（令和６年11月）

# ＩＴサービス・製品提供事業者の皆様へ

提供事業者向け

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

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

## 趣旨･背景･補足

- 「セキュア・バイ・デザイン」は、**セキュリティの責任は製造者等が追うべきである（「責任のリバランス」）**、という**欧米諸国を中心に提唱されている概念**。2023年10月に我が国を含む13か国が共同署名した**セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンス**の中でも、組織の変革を実行できる**経営層の意思決定者による**、製品開発の重要な要素としてセキュリティを優先させるという**コミットメントの重要性**が言及されている。**今後、当該提言を踏まえた対応が全世界レベルで求められていくことが想定される**。
- 経済産業省では、本文書も踏まえ、**「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」**を2025年3月に公表したところ。この中で、ＩＴサービス・製品提供事業者に求められる責務として、セキュリティ品質を確保したソフトウェアの設計・開発・供給・運用等についても提示している。加えて、**IoTセキュリティ適合性評価制度（JC-STAR）を構築・2025年３月に制度運用開始**し、セキュアなIoT製品を容易に選択できる環境整備を進めているところ。ITサービス・製品提供事業者におかれては、積極的にこれらのガイダンスや制度を活用いただきたい。経済産業省としては、引き続き、ITサービス・製品提供事業者が上記メッセージをより具体的に理解し、実践しやすい環境を整備していく。
- また、近年、**ITサービス・製品提供事業者におけるサイバー事案**もみられるところ、自らも「サイバーセキュリティを実践する企業」であり、**ユーザー企業にも影響を及ぼし得る存在**であることを認識して、対策に取り組んでいただく必要がある。

## 関係する政府文書･窓口等

- 内閣サイバーセキュリティセンター「国際共同ガイダンス「セキュアバイデザイン・セキュアバイデフォルト原則」に署名（令和５年10月）
- 経済産業省／内閣サイバーセキュリティセンター「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」（令和７年３月）
- IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」

# 被害組織を直接支援する専門組織の皆様へ

専門組織向け

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

## 趣旨・背景・補足

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

## 関係する政府文書・窓口等

– 経済産業省「サイバー攻撃による被害に関する情報共有の促進に向けた検討会　報告書等」（令和６年３月）

# （参考）産業界へのメッセージに対応した政府文書・窓口等

- サイバーセキュリティを実践する各企業・団体向け
  ○経営層向け
  - 経済産業省「サイバーセキュリティ経営ガイドライン　Ver3.0」（令和５年３月改訂）

  ○実務層向け①
  - 経済産業省「サイバーセキュリティ政策」

  ○実務層向け②
  - 内閣サイバーセキュリティセンター「国際共同ガイダンス「セキュアバイデザイン・セキュアバイデフォルト原則」に署名（令和５年10月）
  - 経済産業省／内閣サイバーセキュリティセンター「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」（令和７年３月）
  - IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」

  ○実務層向け③
  - 経済産業省「サイバーセキュリティ経営ガイドラインと支援ツール」
  - 経済産業省「『ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～』を取りまとめました」（令和５年５月）

  ○実務層向け④
  - 中小企業庁「『パートナーシップ構築宣言』ポータルサイト」
  - 経済産業省「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」（令和４年10月）
  - 経済産業省「中小企業のサイバーセキュリティ安心サービスのご紹介」
  - 中小企業庁「中小企業の情報セキュリティ」
  - IPA「ここからセキュリティ！」
  - IPA「中小企業の情報セキュリティ」
  - IPA「サイバーセキュリティお助け隊サービス制度」

  ○実務層向け⑤
  - サイバー攻撃被害に係る情報の共有･公表ガイダンス検討会「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和５年３月）
  - 経営ガイドラインの付録C「サイバーセキュリティインシデントに備えるための参考情報」（令和５年３月）
  - 個人情報保護委員会「漏えい等の対応とお役立ち資料」
  - 警察署又は都道府県警察本部「相談窓口」
  - 経済産業省サイバーセキュリティ課（代表：03-3501-1511　内線：3964）
  - IPA「コンピュータウイルス・不正アクセスに関する届出」「企業組織向けサイバーセキュリティ相談窓口」
  - JPCERT/CC「インシデント対応依頼」
  - 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「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」（令和６年11月）

- ＩＴサービス・製品提供事業者向け
  - 内閣サイバーセキュリティセンター「国際共同ガイダンス「セキュアバイデザイン・セキュアバイデフォルト原則」に署名（令和５年10月）
  - 経済産業省／内閣サイバーセキュリティセンター「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」（令和７年３月）
  - IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」

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

# （参考）産業界における積極的な取組事例

- 産業界においても、SBOMの活用促進やセキュリティ企業等によるファンドの立ち上げ、中小企業における対策支援など、当省のサイバーセキュリティ政策の方向性に沿った**積極的な取組が進展**。
- こうした産業界における積極的な取組を慫慂しつつ、今後も引き続き**産業界全体のサイバーセキュリティ対策の強化に向けた政策を強力に推進**していく。

**【事例①】SBOM等の活用課題と対処策を検討するコンソーシアム**（※1）

- ✓ **NTT・NECをはじめとした民間企業10社**が立ち上げた「**セキュリティ・トランスペアレンシー・コンソーシアム**」の参加企業が20社まで拡大。
- ✓ **SBOM等の可視化データの活用**によって、セキュリティの透明性の向上と対策の強化を目指す。
- ✓ その**活用過程での課題**(※2) に対して、**民間企業として対処に役立つ知見**(※3) **を共創し公表**。今後も順次公表予定。

(※1)https://www.st-consortium.org
(※2)社会的認知の不足、フォーマット・データの未整備、技術・ツールの不足、活用コスト負担 等
(※3)可視化データの品質指標の提言 等

**【事例②】国内のセキュリティ企業を対象とするファンドの立上げ**

- ✓ 2024年４月、グローバルセキュリティエキスパート、兼松、兼松エレクトロニクス、ウエルインベストメントの４社で**セキュリティ企業のみに投資するファンド**（日本サイバーセキュリティファンド）**を立ち上げ**（※）。
- ✓ **幅広く国内の未上場セキュリティ企業に対して投資を行う**とともに、**サービス導入企業が使いやすいサービスと商品の開発や販売を後押し**する狙い。

（※）令和７年４月時点で25社が参画。

**【事例③】医療機関に対するサイバー攻撃を想定した演習の実施**

- ✓ 九州で地域SECUNITYとして普及・啓発活動を実施している「一般社団法人地域セキュリティ協議会」は、地域の普及啓発の一環として、2024年12月、**佐賀県警**サイバー犯罪対策課、佐賀県鹿島市の**医療機関と連携**し、**ランサムウェアを想定した演習を実施**。
- ✓ 病院でもデジタル化が進む中、演習を通じて、**サイバー攻撃への備えの重要性**や、**被害に遭った際どこに頼れば良いかについて認識を共有**した。

（出典）各種公開情報・報道より作成。

# 参考

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

# １．体制及び関連会議の実績

# 産業サイバーセキュリティ研究会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、<br>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、<br>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、<br>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＞**

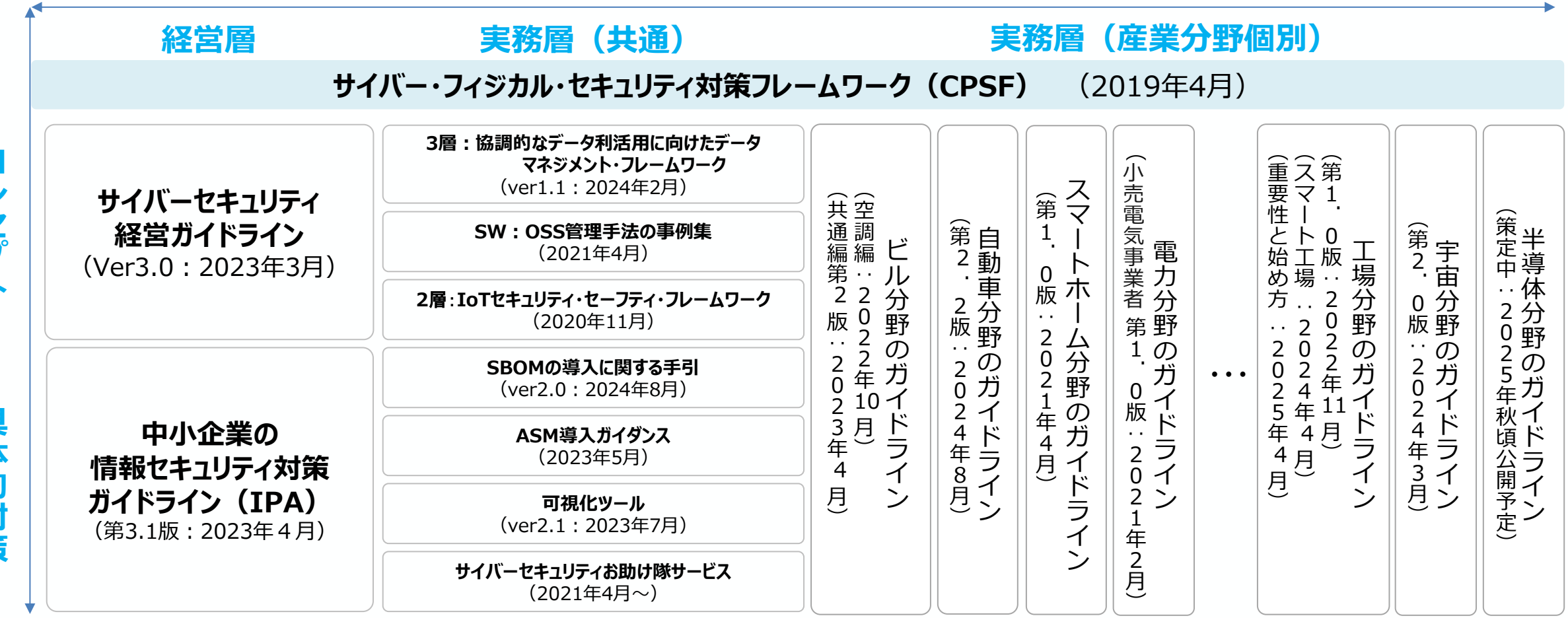
1．サプライチェーン全体での対策強化
2．セキュア・バイ・デザインの実践
3．政府全体でのサイバーセキュリティ対応体制の強化
4．サイバーセキュリティ供給能力の強化

# ２．サプライチェーン全体での対策強化

# CPSFを軸とした各種取組

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

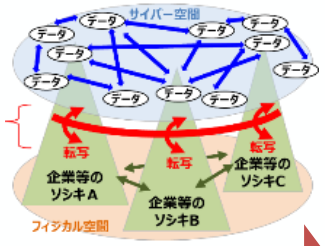
## 主なガイドラインや対策ツール



# CPSF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年度内の発行を目指す。

## 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)<br>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<br>● 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<br>● エディタがTS原案(DTS)を作成する。<br>● 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。<br>国際規格(TS等)発行 |

# 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）。

## 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**。

## 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）。

## 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を改定（2025年5月）**。

## 自動車産業SWG

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

## 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）。**

## 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）**。

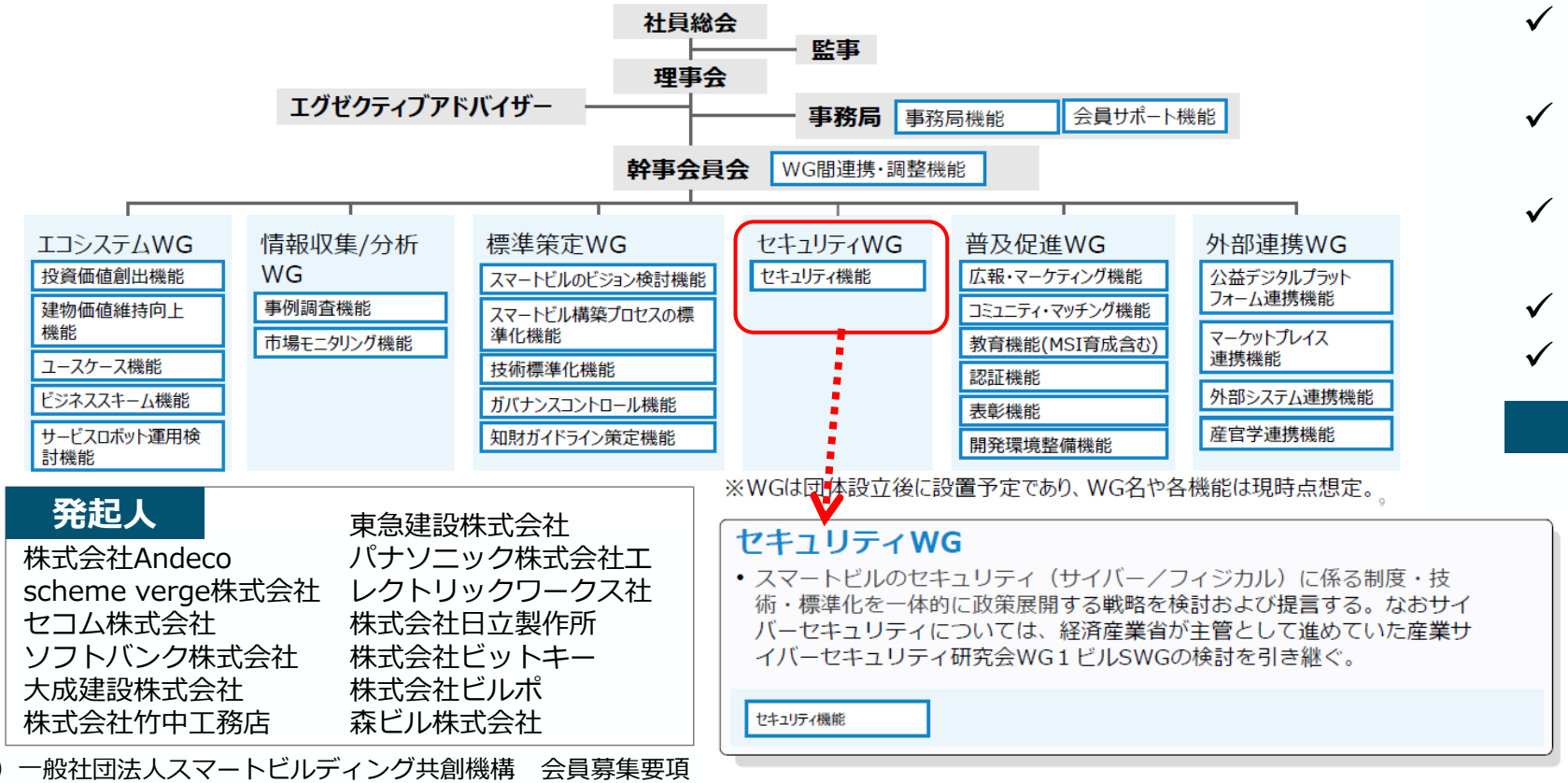
## 半導体産業SWG

- 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

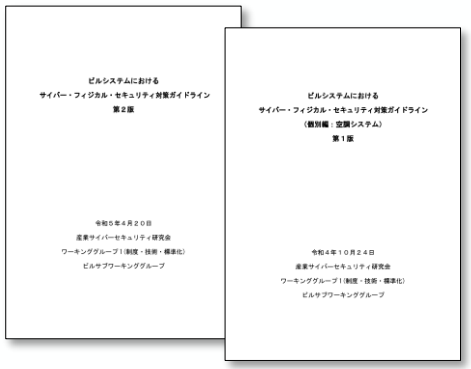
### 発起人

| | |
|---|---|
| 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

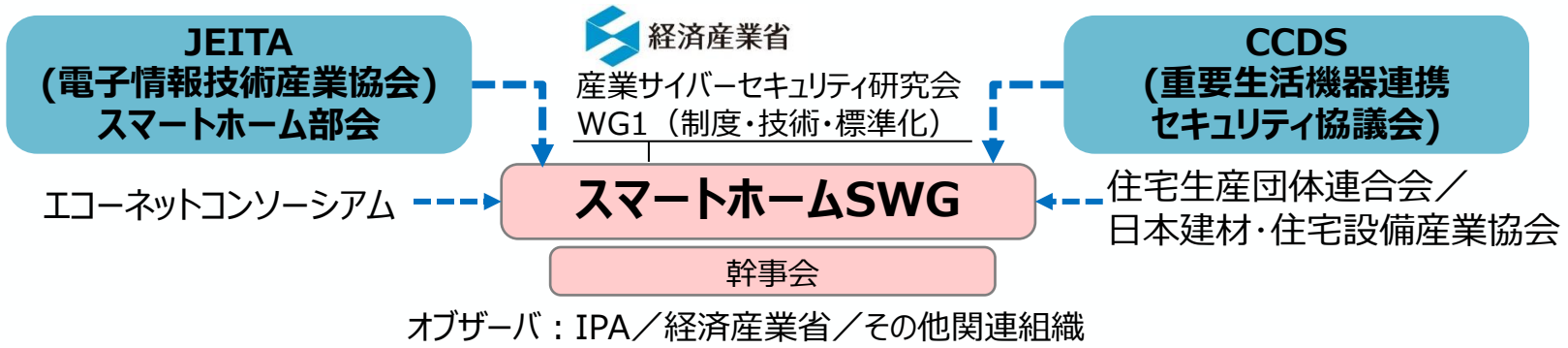
## ビルSWGが作成したガイドライン



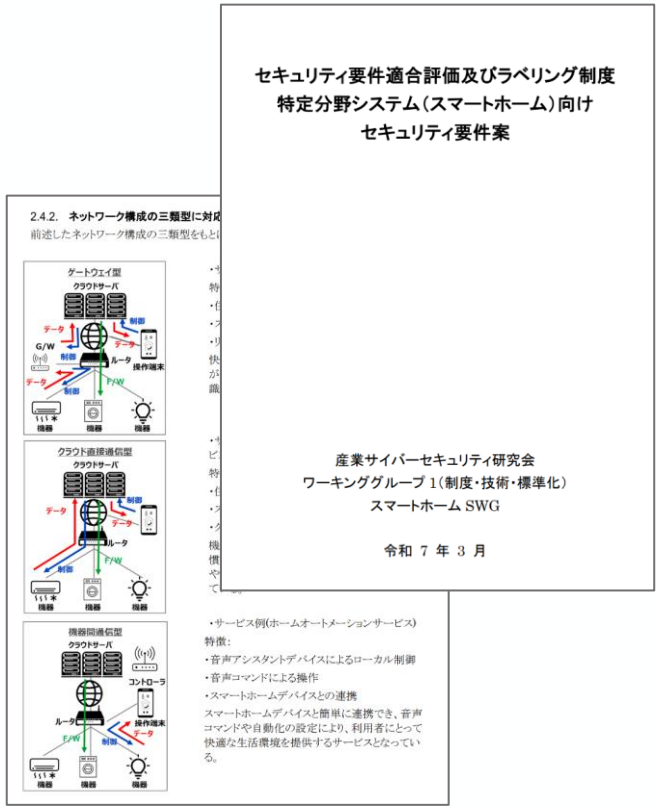
（出典）一般社団法人スマートビルディング共創機構　会員募集要項
https://www.ipa.go.jp/digital/architecture/conferences/smartbuilding-association/membership-info.html

# 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**
  - ースマートホームの定義
  - ースマートホームで実施すべきセキュリティ対策の検討
  - ー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
  - ー★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**
  - ー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
  - ー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


セキュリティ要件適合評価及びラベリング制度
特定分野システム（スマートホーム）向け
セキュリティ要件案

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）
スマートホーム SWG

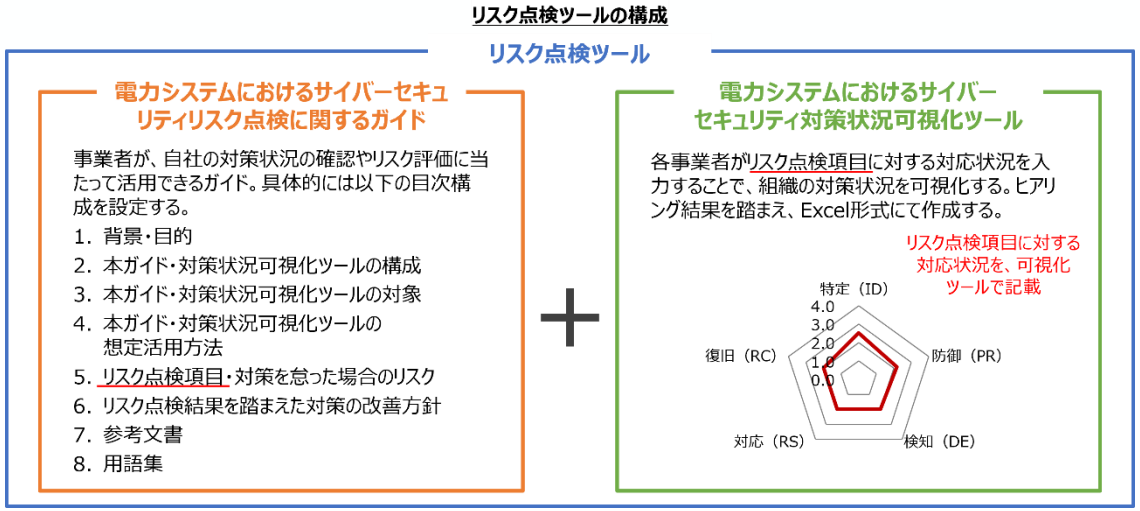
令和 ７ 年 ３ 月

（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）。

## リスク点検ガイドと対策状況可視化ツール



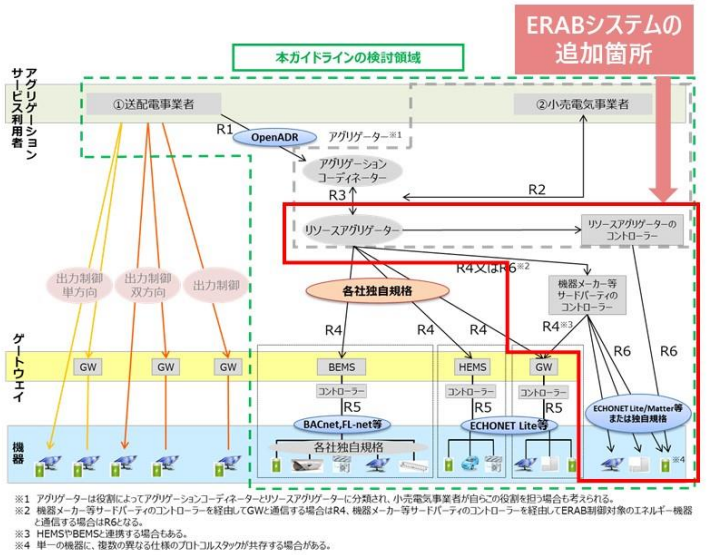

- ✓ 2024年度の電力広域的運営推進機関の会員（**電気事業者**）に対する**セキュリティ自己診断の取組に際しリスク点検ツールを活用**。ツールの使い方に関する説明会を2 回開催。
- ✓ 合計797社から診断結果の回答があり、送配電事業者、小売電気事業者、発電事業者の順番で回答率が高かった。今年度以降も継続して実施し、傾向を把握していく。

## 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

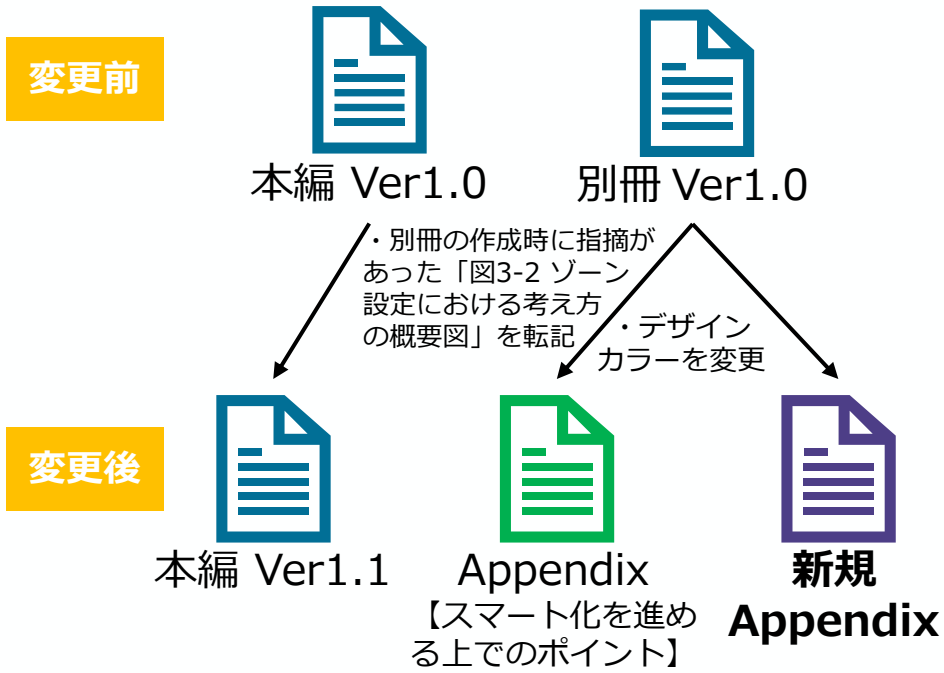
## Appendix【工場セキュリティの重要性と始め方】


※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

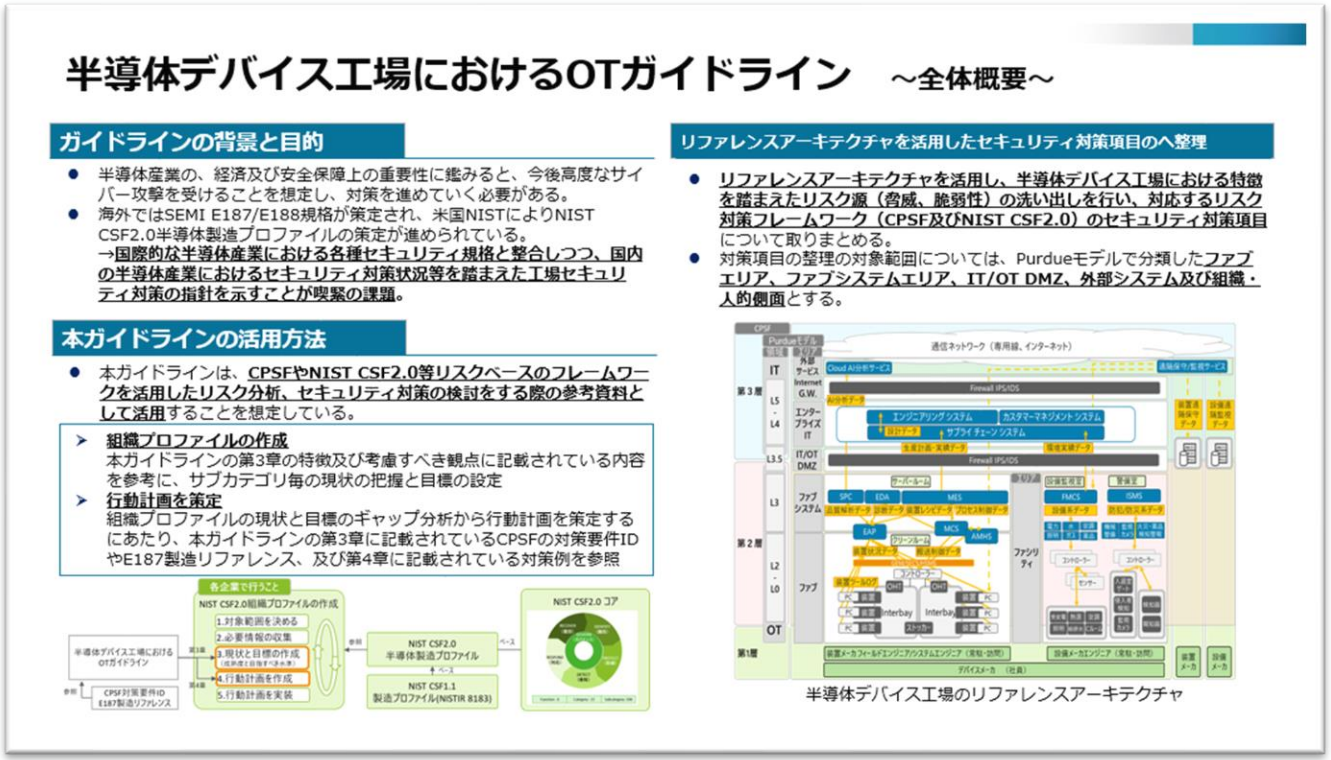
# 半導体産業SWG（座長：東京大学 江崎教授）

- 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）



# 情報セキュリティ監査基準・管理基準・ガイドラインの改定等

## 情報セキュリティ監査基準・管理基準各ガイドライン

情報セキュリティ監査基準・管理基準並びに各ガイドラインは、情報セキュリティマネジメントに関わる国際規格（ISO/IEC 27001、27002）が改正され、また情報セキュリティ監査制度を取り巻く環境に変化があったことを受け、外部有識者の意見も踏まえ、改訂作業を実施中。

＜主な改訂＞

・国際規格の改正に基づいた改訂

・条項番号*の付記方法の見直し

*情報セキュリティ管理基準に付されているJIS Q 27001/27002に基づき付記している番号。

**監査人が適正かつ円滑な監査業務を遂行出来るよう、より分かりやすい内容にするための改訂作業が進行中。**

## システム管理基準追補版（IT統制ガイダンス）

システム管理基準追補版（財務報告に係るIT統制ガイダンス）は、令和５年４月に「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（意見書）」が公表され、また、同月に「システム管理基準」及び「システム監査基準」（システム管理基準等）が改訂されたことを受けて、これらの改訂部分との差異を点検し、整合がとれたものとなるよう所要の見直しを実施。

**令和６年12月に改訂版を公表。**

➢ **今後も、これらのガイドラインが活用されるよう、普及・啓発を行っていく。**

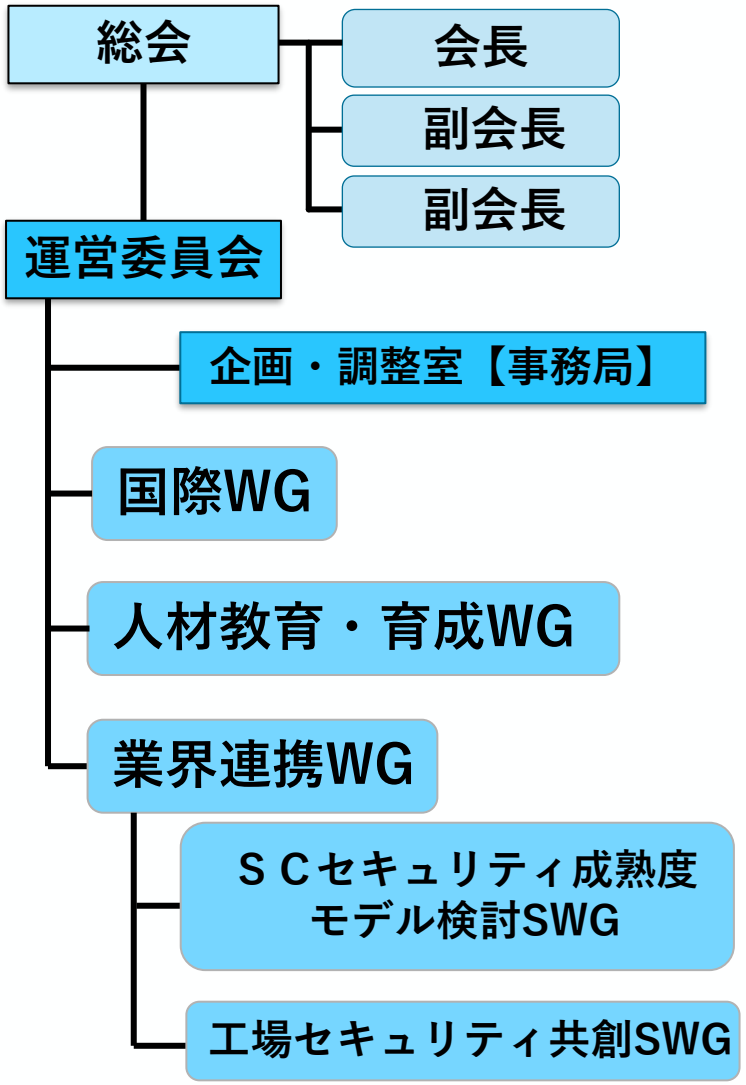
# サプライチェーンサイバーセキュリティコンソーシアム（ＳＣ３）の組織強化

　ＳＣ３は「産業界主導による業界連携のプラットフォーム」として、サプライチェーン上のステークホルダーとの対話や政策提言を主導し、施策の実効性を高めることを目指し令和２年に任意団体からスタート。
　今後サイバー攻撃が益々増化していく中、サイバー空間の安定性、安全、繁栄を推進するため、対話、協業、イノベーションを通じて、日本のサプライチェーンの強靭性を構築する取り組みを開拓し、国家全体のレジリエンス力を強化する必要がある。
　そのために、産業界横断、地域企業、中小企業の観点で幅広い会員基盤を有するSC3は法人化により体制を強化し、令和6年度、経産省・IPAの支援を経て、企画運営機能の強化、ワーキンググループの再編を進め、経済三団体からの支持、従来会員の参加の継続を維持した形で一般社団法人サイバーリスク情報センターとの一体連携の経営に移行。『民民連携・産官連携の連携プラットフォーム』として機能強化を図り、令和７年度より本格的に活動を開始する。

＜新組織＞
ＣＲＩＣ－ＳＣ３：一般社団法人サイバーリスク情報センター
　　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

・経済三団体（経団連・日商・同友会）主導で設立し、会員数は令和７年１月現在で９６業界団体と７５企業が参加。
・令和６年１０月より、企画運営機能の強化、ワーキンググループを再編し業界連携、国際連携、人材育成の課題にフォーカス。
・令和７年１月よりＣＲＩＣとの一体連携により法人化。
・HP：https://sc3.jp/　　問合せ先：info@sc3.jp

＜新組織体制＞



# SC3の活動状況と今後の方針

**従来**
- 十分なリソースを割けない中小企業での対策強化
- 情報不足により対策が進まない地域や地方にある団体／企業への情報提供
- 多重下請け構造の業界における、対応標準化やTierNへの浸透

**現在**
- 国際的なサプライチェーンでの課題検討
- 産学連携による人材育成活用環境整備
- 企業のセキュリティ対策評価制度検討
- 工場システムにおける企業の協力体制
- 企業/業種の垣根を越えた、システム/サービスの連携

**今後**
- 独禁法/下請法対応の政策提言
- 業界で異なる各種ガイドラインの見直し
- 企業間契約とインシデント時の責任分界点
- 企業のセキュリティに関わる情報公開の在り方
- 地域SECUNITYの活性化

**今後の検討テーマ**
課題の抽出と優先順位を検討

① 各種ガイドラインの在り方の検討（業界間相違、共有化／個別性のバランス）
② SBOM等の普及啓発
③ サプライチェーン先との独禁法・下請法対応の具体的なガイドの検討
④ サプライチェーン先への利益供与問題
⑤ 企業のセキュリティに関わる情報公開の在り方と情報共有におけるベンダー・ユーザ間契約
⑥ サイバー保険
⑦ 地域SECUNITYと連携した活動の展開

**活動形態**

| | 開催頻度 | 開催形式/利用システム | 概要 |
|---|---|---|---|
| **全体会議** | 年2回開催 | ハイブリッド形式 | • SC3全体活動報告<br>• 関心の高いトピックスの講演 |
| **フォーラム** | 最大年2回 | 会場開催形式 | • 1つのWG/SWGから詳細な活動報告を実施<br>• **外部専門家を招聘し、サイバーの状況を共有** |
| **勉強会** | 別途決定 | 会場開催形式/ハイブリッド形式 | • 特定トピックスについて取り上げ議論を実施<br>• 必要に応じて、SWGを設置 |
| **外部連携** | 連携組織による | 連携組織の形式 | • **IPA地域関連活動など外部組織との連携・コラボレーション** |

# 中小企業支援施策の全体像

- 中小企業等が抱える主な課題：「サイバーセキュリティ対策の必要性を感じない」「**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ながら、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。

## SECURITY ACTION

セキュリティ対策のきっかけづくり。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40万者の中小企業が宣言。

★一つ星




**情報セキュリティ５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。（2025年3月時点で46事業者）

サイバーセキュリティお助け隊

IT導入補助金に「セキュリティ対策推進枠」を創設
令和7年より支援拡充

⇒**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「情報セキュリティ関連規程」等のひな形、インシデント対応、クラウド活用に関する手引き等を収録。


**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**

# 政府広報等を活用した「サイバーセキュリティお助け隊サービス」の周知・啓発

- お助け隊の更なる普及に向けては中小企業における認知度が課題であるところ、政府広報を活用して**日経ビジネスの記事掲載**や**ラジオ番組への出演**、**新聞広告**等を実施。
- 中小企業におけるサイバーセキュリティ対策の必要性への理解とサイバーセキュリティお助け隊サービスの活用を促す**リーフレットを作成**し、全国の中小企業支援機関等に展開。※2025年２月
- 併せて、施策のターゲットを意識した**経済産業省ウェブサイトの改修**も実施。 ※2025年２月

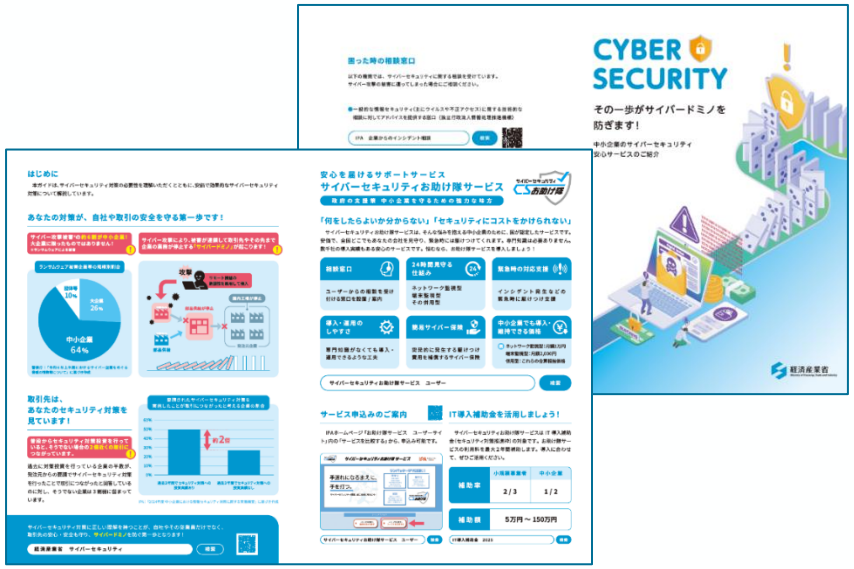
## 政府広報を通じた対外発信


<2025年2月14日発刊
「日経ビジネス」>

2025.02.16
備えて安心！中小企業のサイバーセキュリティお助け隊サービス

<2025年2月16日放送FM
TOKYO「日曜まなびより」>

## 中小企業向けリーフレットの作成

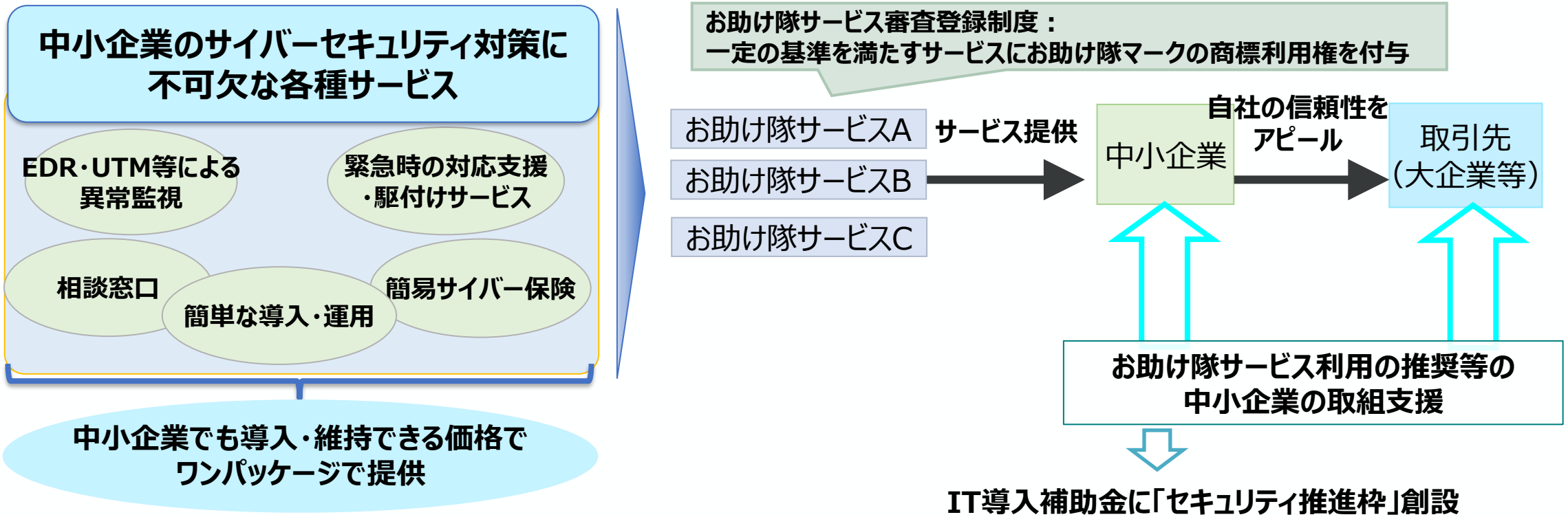



関係省庁や業界団体の御協力を得て、全国の経済産業局、総合通信局、都道府県警察、金融機関（地方銀行、信用組合等）、中小企業支援団体（商工会議所等）、士業団体（税理士会、行政書士会等）、業界団体等に広く展開。

## 経済産業省HPの改修

# 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46事業者がサービスを提供**しており、**約7,000件の利用実績**（2024年９月末時点）がある。
- 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。**




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/

# IT導入補助金セキュリティ対策推進枠の要件変更

- **サイバーセキュリティへの投資は**直接売り上げ増加につながらない（投資効果が見えにくい）ため、**中小企業にとって他のIT投資と比較しても投資へのインセンティブは極めて低いのが現状。**
- サイバーセキュリティお助け隊サービスの提供事業者10社へのヒアリングによると、**申請コストに比較して補助金によるインセンティブが低い**との実態が明らかになるとともに、**補助率の引き上げの要望が多数**寄せられた。
- そこで、IT導入補助金2025から、**補助率・補助上限を引き上げる要件変更を実施。**

## 小規模事業者の補助率引き上げ

とりわけ小規模事業者については、サイバーセキュリティ対策にコストをかけられない実態がある。
そうした者については、現在の要件（補助率及び５万円との補助下限額）では補助対象とならない場合もあることから、**小規模事業者の補助率を２／３に引き上げた。**

## 補助上限の引き上げ

お助け隊サービスの価格要件が撤廃された新たなサービス「お助け隊２類サービス」の提供が開始されたことにより、今までサービスの導入ができなかった相対的に規模の大きい中小企業についても本サービスを導入できるようになったところ、**中小企業における２類サービスの導入を促進するために、補助上限を150万円に引き上げた。**

## IT導入補助金セキュリティ対策推進枠見直しの概要

※赤字が見直し部分

| | 要件見直し前 | 要件見直し後 |
|---|---|---|
| 補助上限 | 5万円～100万円 | 5万円～**150万円** |
| 補助率 | 中小企業：１/２ | **小規模事業者：2/3**<br>中小企業：1/2 |
| その他見直し | | **事業全体における**労働生産性（※）について、以下の要件を全て満たす３年間の事業計画を策定し、実行すること。<br>一　事業計画期間において労働生産性を年平均成長率１パーセント以上向上させること。<br>二　労働生産性の向上に向けた計画が実現可能かつ合理的であること。<br>**（※）　補助により軽減された負担分を振り向けた投資による効果、サイバー攻撃リスクの低減に伴う売上損失の期待値減少効果、その他の経営努力による効果を含む。** |
| 対象経費 | 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） | |

# 地域のセキュリティ対策活性化の取組

- 地域SECUNITY活動を進めるために、セキュリティとＤＸとセットで推進することの必要性を、関連団体・地域企業との更なる連携を目的として、全国の９つの経産局を回り、関連団体に協力を要請。
- IPAにおいて、2025年2月に「地域SECUNITY連絡会」を開催し、各団体における取組を紹介することで情報の共有を図った。
- 地域SECUNITY連絡会で報告された内容は、地域SECUNITY活動促進のためのプラクティス集として2025年３月に公開した。

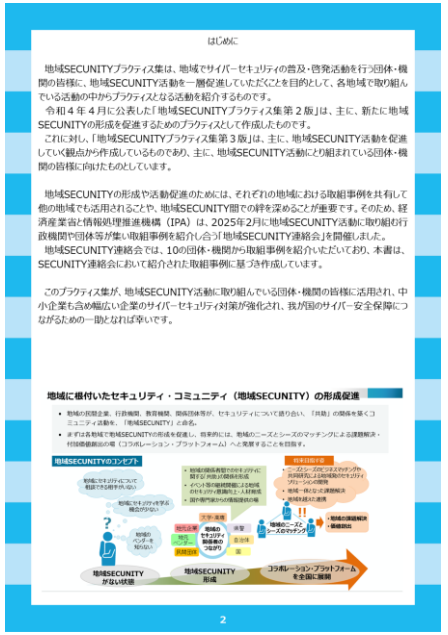
## 地域SECUNITY連絡会

各地域SECUNITYの関係者を集め、各団体の課題や問題意識の共有を行う、「地域SECUNITY連絡会」を実施。他の団体の取組みを参考とすることで、各地域SECUNITYの活動を活性化。

**開催概要**
・開催日時：2025年2月12日
・開催形態：オンライン開催
・発表団体：10団体
・参加団体：22団体
・御講演：SC3企画調整室長　武智洋様

## プラクティス集の作成

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


# 中小企業にとって効果的なサイバーセキュリティの取組（実態調査結果）

- 業種普遍的に効果的なサイバーセキュリティ対策として、**①SECURITY ACTION 二つ星に掲げる対策項目を多く実施すること（→インシデント被害の低減が期待される）**、**②第三者認証（ISMS認証、Pマーク）を取得するなどサイバーセキュリティ対策の実施状況を可視化すること（→取引先の信頼獲得・取引につながることが期待される）**が挙げられる。
- その上で、業種に応じてサイバーセキュリティ対策の目的（期待される効果）も異なることから、**それぞれの業種において多くの企業が実施している取組を参考とすることも有用**（認証の取得、機器の導入、教育の実施、保険への加入等）。
- 中小企業4,191社を対象に実施した「中小企業実態調査」の結果では、上記に係る**具体的な対策事例**や企業が実感した**具体的な効果（生声）を紹介**。「中小企業の情報セキュリティ対策ガイドライン」の実践例として参考にしていただきたい。

## 1 SECURITY ACTION 二つ星に掲げる対策項目をより多く実施することで、サイバーインシデント被害（発生率・被害額）の低減が期待される。

➡ 実態調査の結果によれば、**SECURITY ACTION 二つ星に掲げる対策項目を多く実施**している企業ほど、**サイバーインシデント被害が少なく、被害額も少ない**ことが明らかとなった。

## 2 第三者認証（ISMS認証、Pマーク）を取得することで、取引先からの信頼獲得につながり取引につながりやすくなるという効果が期待される。

➡ 実態調査の結果によれば、**第三者評価制度（ISMS認証、Pマーク）を取得している企業**は、取得していない企業よりも、取引先からのセキュリティ対策要請に応じたことが**取引につながった**大きな要因と考える割合が約2倍であった。

※セキュリティ体制の整備、リスク認識の有無についても同様の結果となった。

## 企業が実施している主な対策と具体的効果の例

| 業種 | 主な対策 | 主な効果 |
|---|---|---|
| 建設業 | セキュリティ体制の整備 | **「取引先からの信頼を得て受注が増えた」** |
| 製造業 | セキュリティ体制の整備、「お助け隊サービス」などセキュリティ機器の導入 | **「顧客からの信頼獲得による受注増や特命発注の獲得」** |
| 情報通信業 | ISMSの取得、セキュリティ体制の整備、セキュリティ教育の実施 | **「お客様からの信頼感が違うのと、業界全体では当たり前だという認識を社内で共有できた」** |
| 小売業 | セキュリティ教育の実施 | **「顧客情報の漏洩を防ぐことができるという安心感を得られた」** |
| 金融業<br>保険業 | セキュリティ体制の整備、セキュリティ教育の実施、サイバー保険への加入 | **「従業員の意識が変わり、サイバーに関しての情報を認知し事前対策を講じるようになった」** |

# 地域のITベンダーの能力向上にかかる手引きの整備

- 中小企業において、**セキュリティに関して困ったことがあった際の相談先として、「社外のIT関連業者」がもっとも多く**、特に身近なIT関連業者が重要な役割を担っている。他方、サイバー攻撃の被害にあった事案の中には、ベンダーの知識や対応不足等が起因するなど、**地元企業に対してITシステムを納入する地域のITベンダーの強化が不可欠**であり、ITベンダーの強化を図っていく必要がある。
- こうした現状を踏まえ、**地域のITベンダーのセキュリティに対する意識や知識の向上に向けて、ITベンダーとしてセキュリティに関して認識しておくべき事項をまとめた手引きの作成に向けて検討を進めている。**
- 別途検討がなされている「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」との整合性も確保しつつ本手引を作成し、**地域SECUNITYやお助け隊サービス提供事業者等を通じた広報周知を進めていく。**

## 地域ITベンダー状況調査

- **ITベンダーの約2割が、サービス導入後に顧客と運用保守契約を締結しておらず、**その後の対応を中小企業側に全て委ねるケースも見られ、中小企業のセキュリティが十分に確保されないまま放置されている状況が判明。中小企業のコスト制約や人材不足等の課題がある状況下において、**ITベンダーの利益確保に直結しにくい**という事情も明らかとなった。
- また、**ITベンダーの約７割が社内のセキュリティ技術者が１～５名**であり、**セキュリティ技術者がいないITベンダーも約１割存在**することが判明。ITベンダー自社のリソース確保についても課題が明らかとなった。
- 一方で、一部ITベンダーの中には、**セキュリティ要件の優先付け、リスク説明と責任の明確化**を行うなど、中小企業の課題に対応するための取組を進めている事例も確認された。

## 地域ITベンダー向け手引の全体構成【案】

| | 構成 | 概要 |
|---|---|---|
| 本編 | 第１部　中小企業のお客様が抱えるセキュリティ対応上の課題 | 中小企業のお客様が抱えるセキュリティ対応上の課題やそれに伴うさまざまな問題点を明らかにし、中小企業のお客様向けシステムのセキュリティ担保の重要性について説明 |
| 本編 | 第２部　地域のITベンダーが中小企業のお客様の良き相談相手となるための取組 | １．地域のITベンダーに求められる責務<br>２．責務を果たすための取組のプラクティス<br>に分け、地域ITベンダーが中小企業のお客様から信頼される良き相談相手となるための取組ヒントについて説明 |
| 付録 | 付録1　中小企業のお客様向けシステムにおけるセキュリティ対応の重要ポイントがよくわかるチェックリスト | セキュリティに不安がある中小企業のお客様向けシステムに対して、セキュリティの観点から採り得る対応がよくわかるチェックリストを提供 |
| 付録 | 付録2　中小企業のお客様のセキュリティ対応支援に役立つ情報 | 地域ITベンダーにとって、中小企業のお客様のセキュリティ対応支援に役立つ情報を紹介 |

出典：中小企業のセキュリティ対応におけるITベンダーの役割に関するアンケート・ヒアリング調査（IPA）（2024年12月～2025年2月実施）

# 登録セキスペを活用した中小企業支援

- 物価高や最低賃金引上げ等により中小企業等における資金的余力や人材確保が厳しい状況にある中、セキュリティ専任の部署（担当者）が置かれるケースは少なく、多くは兼務となっており、セキュリティ業務の外部委託も進んでいない。その要因の１つとして、**セキュリティ人材に関する需要と供給の適切なマッチングがされていない**ことが考えられる。
- 令和５年度補正予算事業において、**中小企業等と登録セキスペとのマッチング**を促す場を構築する実証事業を実施し、**登録セキスペの社外における活用**と、**中小企業等がセキュリティ人材を探索しやすくするための環境整備**を検討。
- 具体的には、**商工会議所と連携したサイバーセキュリティ相談会を実施**し、相談会参加企業105社のうち34社が登録セキスペとマッチング。**登録セキスペによる訪問指導（マネジメント指導）を実施**。

〔中小企業等と登録セキスペのマッチングフロー〕

**商工会議所と連携したサイバーセキュリティ相談会**
- 商工会議所と連携したサイバーセキュリティ相談会を開催。
- 専門家によるセキュリティ対策の必要性等を訴求する基調講演を実施。

**登録セキスペによる個別相談**
- 相談会参加者のうち希望者に対して登録セキスペによる個別相談を実施。
- 自社のセキュリティ対策の課題を特定・優先づけを実施。

**登録セキスペによるマネジメント指導**
- 個別相談参加者のうち希望者に対し、**５つのマネジメント指導テーマ**の中から選択したテーマについて伴奏支援（３回実施し、各回ごとに目標を設定）。

〔相談会・個別相談の実施結果〕

**相談会参加者アンケート・個別相談の結果**
- セキュリティに対する意識がある社の中で、**どこから始めたらよいか分からない、どこに相談したらよいか分からない社が約８割**存在した。
- **セキュリティ専門家を選定するときに重視する点**として、「**緊急時の対応力**」「**提案内容の具体性**」「セキュリティ専門家の**技術力・専門性**」「**自社の業界に対する理解度**」「**コスト**」が上位に挙がった。
- **支援を希望する内容**（個別相談の中で明らかになったものを含む）として、「従業員向け**セキュリティ教育の実施支援**」「取引先から／取引先への**要求事項への対応支援**」「情報セキュリティ**規程の作成・改訂支援**」「現在の社内の**セキュリティ対策状況の診断**」が上位に挙がった。
- **セキュリティ専門家の探索手法**として望ましいと考えるものとして、「**公的機関（IPA等）における専門家リストの利用**」のほか、「商工会議所等の**中小企業支援機関による紹介**・マッチング支援サービス」「取引のある**ITベンダーからの紹介**」が上位に挙がった。

**個別相談における具体的な相談内容**
- 各社におけるセキュリティ課題は、その**成熟度や課題領域において非常に多様**。
- 「**サンプル規程**があることは知っているが、それをどのように使用し、**自社用に作り直せばいいのかがわからない**」など**具体的なアドバイス**を求める相談が見られた。
- 「作成した規程の内容が本当に十分か、自社に合っているか」など、**自社の判断・取組の妥当性を専門家の第三者的な視点から確認したい**というニーズも存在。
- **業界別の対策水準の要求等の確保**を目的としたセキュリティ対策の相談が多く、**要求事項を自社に即した具体的な対策として落とし込む方法**について、実践的な示唆を求める声が複数確認。

# 中小企業向け人材育成・活用指針案の全体像

- 令和6年7月～令和7年5月実施のサイバーセキュリティ**人材の育成促進に向けた検討会**において、**既存施策の拡充や改善などを基本**として、**登録セキスペの活用及び制度の見直し**や、**中堅・中小企業等の内部でセキュリティ対策を推進する者の確保に向けた新たな施策**について議論。
- 令和５年度補正予算事業（セキュリティ人材活用促進実証等）や支援機関等の意見から得られた課題を踏まえ、**中小企業等がサイバーセキュリティ対策を無理なく実施できる人材面の支援策**として、 ①個社の状況に応じた個別相談・支援が可能な登録セキスペをリスト化した「**登録セキスペアクティブリスト**」 、②中小企業等の内でサイバーセキュリティ人材を育成し、又は外部の人材を活用するための実践的な方策を示したガイドブックの策定及び活用・普及策を中心に検討を実施。

| | 必要性 | 内 容 | 活用・普及策 |
|---|---|---|---|
| 登録セキスペアクティブリスト | • セキュリティ対策の「始め方が分からない」「相談先が分からない」企業が**自社の課題を特定**するために、また、ひな形や要求事項を**自社にカスタマイズ**して落とし込むために、**専門家と相談**できる機会を**探索コストをかけずに確保**する必要。 | • 相談者のニーズに応じた登録セキスペを選定できるよう、実証事業での声を踏まえ、<br>**支援実績テーマ／得意な業界／所属形態／登録セキスペ以外の保有資格など**<br>を記載メニュー化したリストを作成・公表。<br>• **定型的な支援テーマ**（規程整備・リスク分析・クラウドサービス・インシデント対応・従業員教育）について、引き続き**ニーズ把握しつつ拡充を検討**。 | • 中小企業の**直接利用（プル型）**のみならず、支援機関やITベンダー等の中小企業の**相談先を介した活用（プッシュ型）**も想定。<br>• 支援機関の**指導員への周知・研修**、支援機関の**窓口・専門家派遣事業**における利用。<br>• **専門家団体との連携**も検討。 |
| 人材確保・育成策の実践的方策ガイド | • **長尺なガイドを読むのが難しい**、人材育成のための**適切な演習が分からない**などの声や企業の**セキュリティ課題**は成熟度・課題領域が**多様**であることを踏まえ、**各所に散らばった対策の内容**や**人材確保・育成策のエッセンス**を**段階的・コンパクト**に示す必要。 | • 経営者の意識向上につながるよう、**経営者向けのメッセージ**も収録。<br>• 相談各社の**セキュリティ課題は多様**であることを踏まえ、実施すべきセキュリティ対策をSECURITY ACTION★１レベルから**段階的に提示**。<br>• 段階ごとに**提示したタスクを実施する人材の確保・育成策**を**具体的な教育コンテンツ**等とともに提示。 | • 中小企業の**経営者・セキュリティ担当者**を読者とするだけでなく、**中小企業の支援機関による活用**も想定。<br>• 支援機関、業界団体、教育コンテンツ提供者等を通じた普及のほか、**読者に応じた**チラシの作成、セミナーコンテンツ、**映像コンテンツ**等による普及も検討。 |

# 中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版

- 企業が実施するセキュリティ対策を４つのStepに分け、対策の実施に必要なタスク、人材の確保・育成策を提示。

| | | 実施するセキュリティ対策 | 人材の確保・育成の方策（外部人材の活用） | |
|---|---|---|---|---|
| （兼任でのみ確保可能） | **Step1「取組の開始」** | **基本的なセキュリティ対策を開始**<br>・情報セキュリティ5か条の実施 | **「兼務であっても、一人はセキュリティ担当者を配置」**<br>・配置転換、社内公募による人材確保 | 取組の開始前や取組中において、不明点等を**登録セキスペ等の外部のセキュリティ専門家に相談することも有効** |
| | **Step2「組織的な取組」** | **担当者の下で、組織的な取組を開始**<br>・情報セキュリティに関するルールを規定<br>・従業員へのセキュリティルールの周知、注意喚起、教育の検討 | **「兼任人材の増員」**<br>・配置転換、社内公募による兼任人材の増員<br>・既存情報、学習コンテンツ、セミナーの活用<br>・試験、資格の活用 | |
| （兼任又は専任で確保可能） | **Step3「本格的な取組」** | **セキュリティ体制を構築し、対応すべきリスクに応じたセキュリティ対策を開始**<br>・平時、有時の対応体制を構築<br>・外部専門家(セキスペ等)を活用した資産の洗い出し、リスク分析の実施<br>・必要なセキュリティ対策の検討、導入、運用を実施<br>・外部委託範囲の適切な決定、契約書・覚書などへのセキュリティ対策の明記 | **「自社のセキュリティ体制を構築」**<br>・専任人材、セキュリティ責任者の任命<br>・配置転換、社内公募による兼任人材の増員<br>・既存情報、学習コンテンツ、セミナーの活用<br>・試験、資格の活用 | 必要なセキュリティ対策を全て内部人材で実施することは困難であるが、自社で実施する業務と**外部委託が可能な業務**を判断し、適切に**委託先を管理**することが必要 |
| | **Step4「継続的な改善より強固な対策」** | **より強固なサイバーセキュリティ対策に取り組む**<br>・システム・ソフトウェアの脆弱性管理<br>・インシデントの検知 | **「自社のシステムに応じた脆弱性の管理、インシデント対応に必要な人材を確保」**<br>・セキュリティ対策関連の業務経験を有する人材の中途採用<br>・サイバーセキュリティを専門とする教育機関を修了した直後の人材の新卒採用<br>・専任の人材による兼任人材への指導<br>・教育プログラムの受講 | **自社の人材育成、リスクの洗い出し、実施すべき対策の検討等においては、登録セキスペ等の外部のセキュリティ専門家の活用が有効** |

# インド太平洋地域向け産業制御システム・サイバーセキュリティ演習

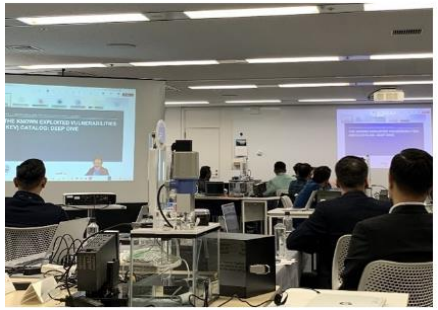
- 経済産業省とIPA産業サイバーセキュリティセンター(ICSCoE)が、**米国・EU政府等と連携し、毎年開催するインド太平洋地域向けの1週間の研修プログラム**。これまで2018年度より毎年開催。
- 本演習では、**インド太平洋地域の重要インフラ事業者、製造業者等のICSセキュリティの向上を目的**に、**産業用制御システム（ICS）のサイバーセキュリティに焦点**を当て、IPA産業サイバーセキュリティセンターの施設を使用した**ハンズオン演習**や、**日米欧専門家による講演**、**参加者間のネットワーキング**を実施。

## 2024年演習の概要

- **日時**：2024年11月12日～15日
- **場所**：IPA文京キャンパス、IPA秋葉原キャンパス、EU代表部
- **主催**：経済産業省、IPA産業サイバーセキュリティセンター、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省）及びEU政府（通信ネットワーク・コンテンツ・技術総局）
- **参加者**：ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の重要インフラ事業者、製造業者、ナショナルCSIRT、政府機関等

### ハンズオン演習

### 日米欧専門家による講演



### インド太平洋地域参加者間のネットワーキング

# ASEAN向け企業対策支援

- 経済産業省では産業界のサイバーセキュリティ向上に向け、**対象者ごとに具体的な対策を記載したガイドラインを展開している**。そのうち一部は**英語版も発行しているが、国外企業における認知度は低い。**
- サイバーセキュリティ対策は、サプライチェーン全体での対策が必要であり、 我が国とサプライチェーンの多くを共有するASEAN地域でのサイバーセキュリティ能力の向上が重要であることから、**ASEAN地域に向けて、施策の情報発信を強化。具体的には、日・ASEANサイバーセキュリティ政策会議や英語版HPにて情報発信。**

## ASEAN地域へのガイドラインの展開

◆全事業者向け

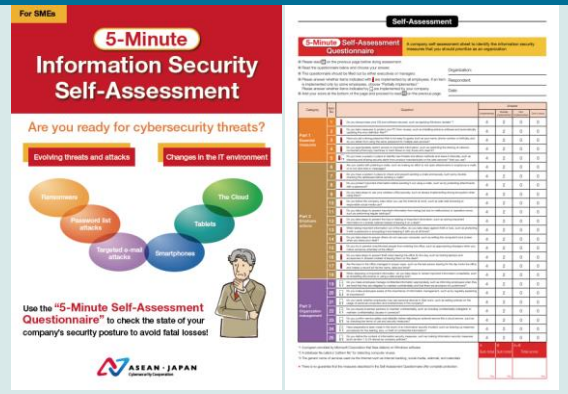
- サイバーセキュリティ経営ガイドライン
- ５分でできる！情報セキュリティ自社診断

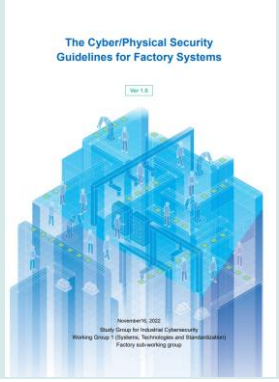
◆産業分野別

- 工場、自動車産業向けガイドライン

◆IT、ソフトウェア企業向け

- SBOMの導入に関する手引き　　等




## 英語版HPの更新

効果的に施策を発信するため、英語版HPを大幅リニューアル。必要な政策情報に簡単にアクセスできるよう、再構成。

Cybersecurity / METI Ministry of Economy, Trade and Industry

# 3．セキュア・バイ・デザインの実践

# 2024年度国際連携の取組・成果全体像

- 日本のサイバー対処能力の強化や国際競争力強化の観点から、 **①サイバー分野におけるルール作りを主導する欧米等の議論に参画し、国内制度との相互運用性を担保**する必要。
- 同時に日本企業の**②サプライチェーン上重要なインド太平洋地域のサイバー対策の能力構築を推進**し、すべての土台となる**③幅広い有志国との連携**も深めていく必要があり、この３つの柱を軸に国際連携を実施。

## ①国内外制度の相互運用性担保

- **IoTセキュリティ（JC-STAR）：**同様に制度を導入又は検討している**欧米**や**英シンガポール**を中心に、相互運用性担保に向けてバイ・マルチで議論。
- **ソフトウェアセキュリティ（SBOM、SSDF）：**同様に検討を進めている**米**を中心に、制度調和に向けて議論。

➢ 米：6/25-26 日米サイバー対話、日米経済版2+2閣僚会合
➢ 欧：11/11日EUサイバー協議、4/30日EUデジタルパートナーシップ閣僚会合
➢ シンガポール：10/14-17シンガポールサイバーセキュリティウイーク
➢ 英：9/12-13日英サイバー対話、日英デジタルパートナーシップ会合　　等

## ②インド太平洋地域向け能力構築

- **米欧政府と共に、**2018年度より**インド太平洋地域向け産業制御システム・サイバーセキュリティ演習を**毎年実施。2024年は11/12-15に東京で対面実施。

➢ その他連携：10/18日ASEAN政策会議、日ASEANサイバーセキュリティWG　等

## ③幅広い有志国との連携

- ①と②の対象国を軸に、**各種バイ協議**を実施。
- その他、①と②を含む各種アジェンダの推進に向けて**G7、日米豪印（クアッド）、IPEF等のマルチ枠組み**も活用。

➢ イスラエル（イスラエルサイバー総局、サイバーセキュリティ企業団の来訪）
➢ インド（日印デジタル・パートナーシップ）
➢ 豪州（3/6 日豪サイバー協議）
➢ 日米豪印（9/21首脳会合、サイバー大使会合、上級サイバーグループ会合）　　等

# IoTセキュリティ適合性評価制度（JC-STAR）の開始

- 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。

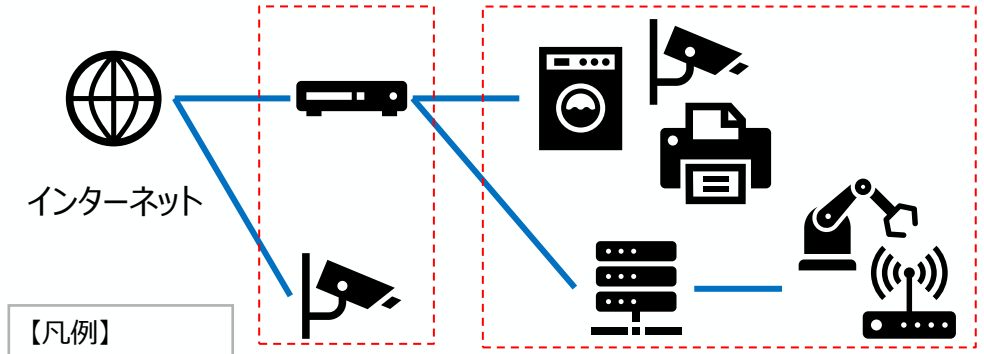
## 制度名称・ロゴ・ラベル

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

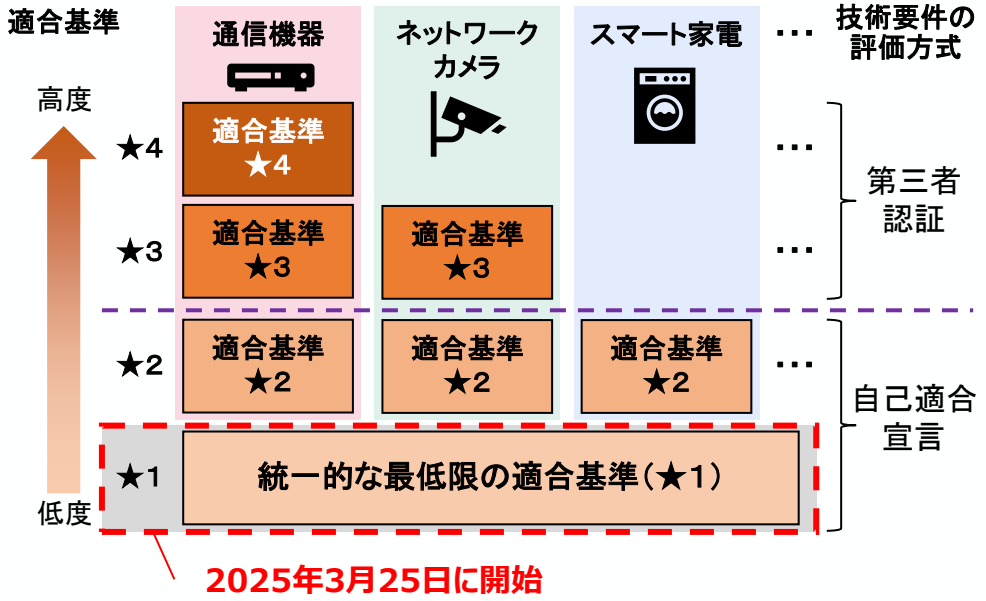
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

## 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

# 第６回日米豪印（クアッド）首脳会合：ソフトウェア・セキュリティ

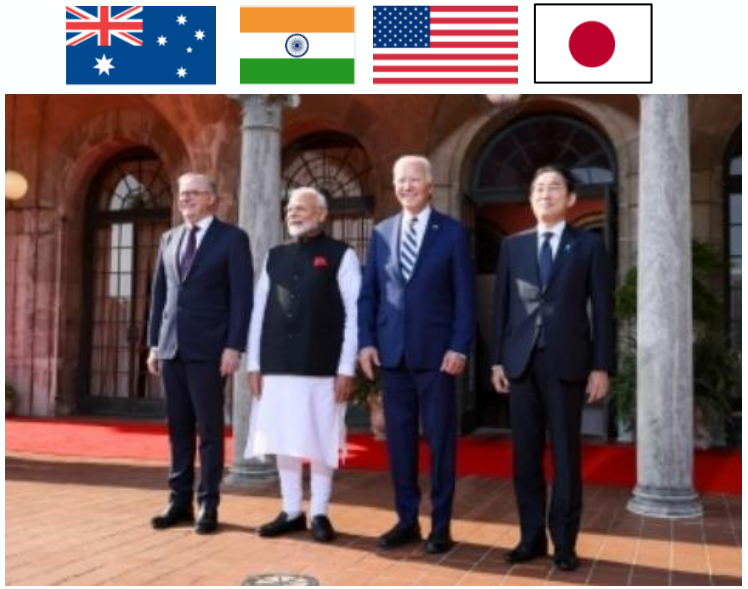
- 2024年9月21日（土）、米国デラウェア州にて**第6回日米豪印（クアッド）首脳会合**が開催された。
- 会合後に発出された**日米豪印首脳共同声明では、ソフトウェア・セキュリティに関して、**

  ①昨年首脳会合の成果物であった**「ソフトウェア・セキュリティに関する日米豪印共同原則」について産業界等にヒアリングを行う官民連携の取組、及び**

  ②今後米連邦調達においてソフトウェア開発要件への自己適合宣言が義務化される見込みであることも踏まえ、**政府調達要件における国際調和を図る**旨言及がなされた。

日米豪印諸国はまた、2023年のソフトウェア・セキュリティに関する日米豪印共同原則に基づき、**安全なソフトウェア開発要件及び認証の追求に向けた我々のコミットメントを拡大**するために、**ソフトウェア開発者、業界団体及び研究機関と連携**している。

我々は、**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**のみならず、サプライチェーン、デジタル経済及び社会のサイバー強じん性を全体として向上させる。（2024年9月21日米豪印首脳声明より抜粋）



https://www.mofa.go.jp/mofaj/fp/nsp/page1_001702_00001.html

# ソフトウェア・セキュリティの確保に係る施策の全体像

- ソフトウェアセキュリティに関する諸外国の動向、国内の現状を踏まえ、国内事業者向けのガイドライン等の策定について取組を進めている。
- 今後は、更なる実効性確保のために、ガイドライン等の指針に沿った取組を確認するための枠組みの整備、政府調達等における対応の位置づけ、国際整合化などに取り組む。

## 諸外国の動向

- 2023年10月、米国CISAがセキュア・バイ・デザイン／デフォルトに関する文書「Shifting the Balance of Cybersecurity Risk」(※1)においてソフトウェア作成業者に対する原則等を提示
- 2023年5月、日米豪印(QUAD)共同原則において、安全なソフトウェア開発の実践を政府方針に取り入れることに合意。

## 国内の現状

- 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は存在しないため、検討する必要。
- SSDF(※2)は汎用的で抽象的なフレームワークであるため、実践導入する上での具体的方法等が明確でないという課題。

※1 内閣サイバーセキュリティセンター(NISC)も共同署名
※2 米国国立標準技術研究所(NIST)が策定しているソフトウェア開発者向けの手法をまとめたフレームワーク(SSDF: Secure Software Development Framework)

諸外国の動向等を踏まえたソフトウェア施策

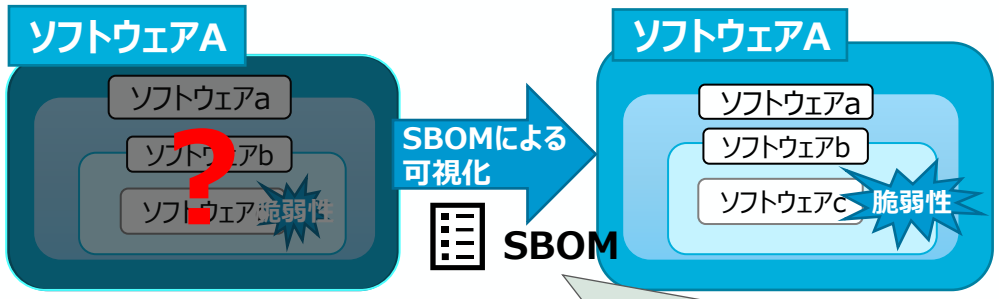
| | ガイドライン等の策定 | 今後の取組例 |
|---|---|---|
| コンセプト | **2025年3月「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）※3」を策定**<br>(※3) 一定の社会インフラの機能としてソフトウェアの開発・供給・運用を行っているサイバーインフラ事業者が顧客との関係で果たすべき責務等を指針としてまとめたもの。 | • サイバーインフラ事業者に求められる役割等に関するガイドライン（案）の成案化<br>• 当該指針に沿った取組を確認するための枠組みの整備<br>• 政府調達等における要件として、当該指針への対応の位置づけを検討 |
| 具体的対策 | **2025年3月「SSDF導入ガイダンス案（中間整理）※4」を公開**<br>(※4) 実証を通じ、国内事業者への普及に向け、実践の具体化に関してとりまとめたもの。 | • 追加の検討・実証等を通じて指針を整備し、当該指針に沿った取組を確認するための枠組みを整備。<br>• 日米豪印(QUAD)を通じて、国際的な共同指針の策定に貢献 |
| | **2024年8月「SBOM導入手引ver2.0」を策定** | • 国際整合化に関する検討 |

実効性の確保

# ソフトウェア管理に向けたSBOMの活用促進

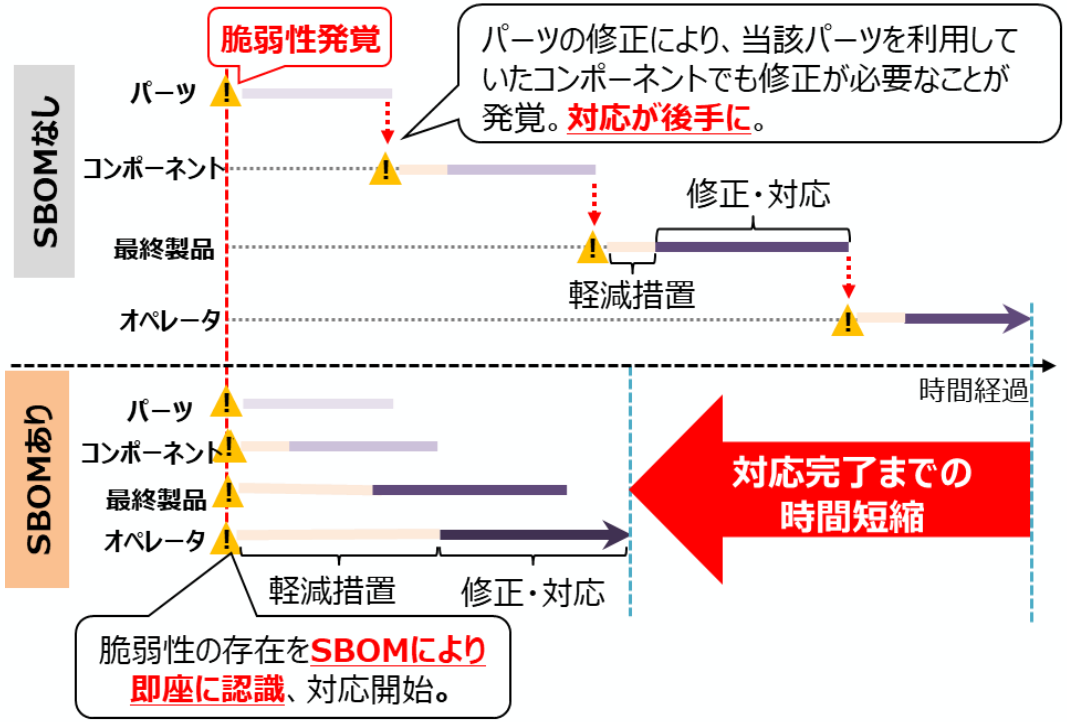
- SBOM（Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。ソフトウェアを構成する各コンポーネントを誰が作り、何が含まれ、どのような構成となっているか等を示す。SBOMによりソフトウェアの構成情報の透明性を高めることで詳細を把握することができ、ライセンス管理や脆弱性対応への活用が期待される。
- 2023年7月、SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示した**「ソフトウェア管理に向けたSBOMの導入手引」を公表。**
- **2024年８月に改訂版を公表**。主な改定ポイントは、**①脆弱性管理プロセスの具体化**、**②「SBOM対応モデル」の追加**、**③「SBOM取引モデル」の追加**。

<SBOMイメージ>




| サプライヤ名 | コンポーネント名 | バージョン | 製品URLなど | … |
|---|---|---|---|---|
| A会社 | ソフトウェアA | Ver1.0 | …… | … |
| A会社 | \|…ソフトウェアa | Ver2.1 | …… | … |
| B会社 | \|…ソフトウェアb | Ver5.3 | …… | … |
| C会社 | \|…ソフトウェアc | Ver1.2 | …… | … |

<SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮>



# （参考）ソフトウェア管理に向けたSBOM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**<br>● **1-2. SBOMツールの選定**<br>● **1-3. SBOMツールの導入・設定**<br>● **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**<br>● **2-2. SBOMの作成**<br>● **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**<br>● **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導入ガイダンス案（中間整理）概要（2025年3月公表）

## 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

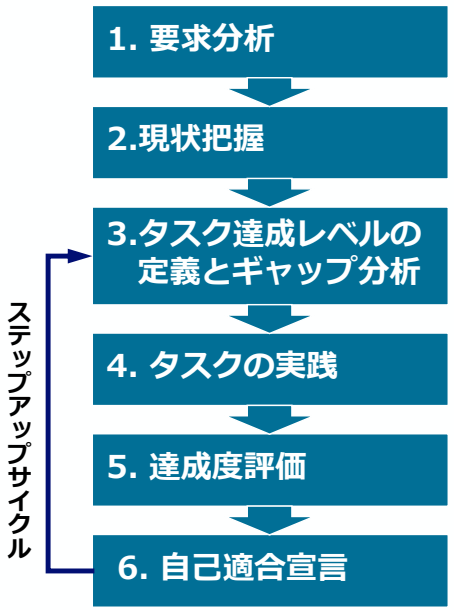
※　産業分野、開発言語、利用技術、開発プロセスに依らず幅広い領域の事業者

## 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）（2025年3月公表）の全体概要と今後の取組例

## 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<br>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<br>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）<br>＋<br>関係機関（行政機関、関連業界団体） |
| ソフトウェアサプライチェーンの管理 | ライフサイクル管理、透明性の確保※ | |
| 残存脆弱性への速やかな対処 | 残存する脆弱性の速やかな対処 | |
| ソフトウェアに関するガバナンスの整備 | 人材・プロセス・技術の整備 | |
| サイバーインフラ事業者・ステークホルダー間の情報連携・協力関係の強化 | サイバーインフラ事業者・ステークホルダー間の関係強化 | |
| 顧客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。

# ４．政府全体でのサイバーセキュリティ対応体制の強化

# サイバー被害に関する対応支援・国際調整窓口等の実施

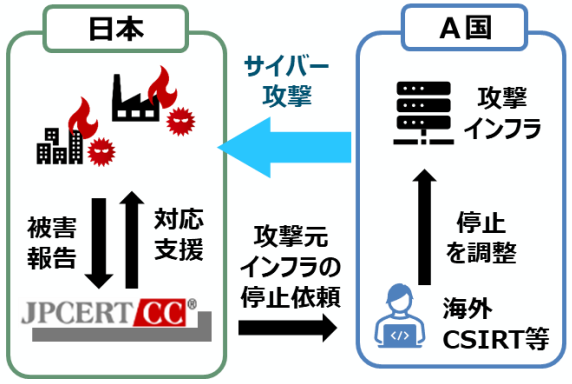
- **JPCERT/CC※は、民間の非営利団体（一般社団法人）として、1996年から活動を実施。**

※Japan Computer Emergency Response Team / Coordination Center

- **我が国の調整窓口として1998年**から機能し、これまで複数の職員が世界各国の調整機関が集まる団体（FIRST）の理事に選出されるなど、国際的な認知度・信用度も高い。

## 事案対応支援、国際連携強化・調整業務

- 幅広い事業者等において発生したあらゆるインシデントへの初動対応支援や啓発活動を実施。
- 国境を越えてくるサイバー攻撃については、信頼関係に基づき、各国窓口CSIRT間で、攻撃インフラとなっているサーバの停止について調整。

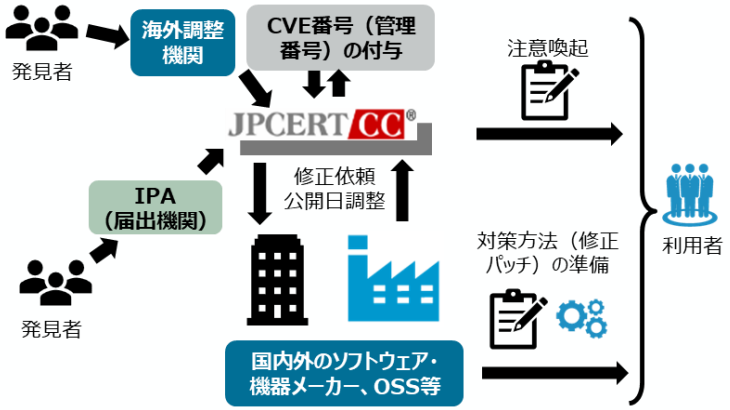



**<2024年度の取組・進捗>**

- インシデントの被害発生及び拡大防止のための調整を15,078件実施（2025年３月時点）
- APCERTの事務局及び運営委員会メンバーやFIRSTの年次会合（福岡で開催）のローカルホストを務め、アジア太平洋地域及び世界的なCSIRT連携の活動に貢献　等

## ソフトウェア等の脆弱性対応

- 脆弱性が発見された場合、対策を講じずに脆弱性の情報を公表すると、攻撃者に悪用されるおそれがあることから、メーカーや主たる利用者と調整し、対策方法を準備した後に公表。
- 事業者（特に組織内PSIRT等）への脆弱性対応枠組みの周知。




**<2024年度の取組・進捗>**

- 脆弱性対策情報を約26,000件公表（2025年３月時点）
- PSIRTとの脆弱性対処等に関する情報・意見交換会を４回実施（延べ約350人が参加）　等

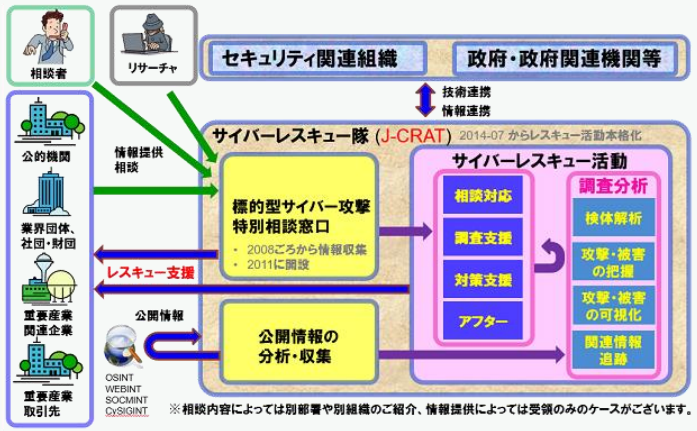
# IPA サイバーレスキュー隊（J-CRAT）／サイバー情勢分析部

## サイバーレスキュー隊（J-CRAT）※2014年７月発足

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

**＜2024年度の取組・進捗＞**

- サイバーセキュリティ分野における防衛省・経済産業省・IPAによる包括的な連携協定を締結
- サイバー攻撃グループMirrorFaceによるサイバー攻撃(警察庁・NISCが注意喚起)について情報提供で協力



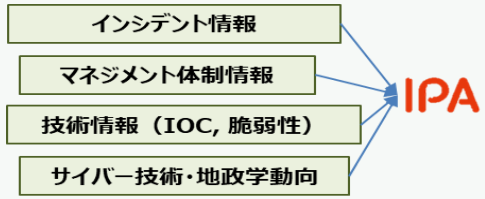

| 2024年度実績（3月末時点） | |
|---|---|
| 相談・情報提供数 | 431 |
| 支援数 | 210 |
| オンサイト支援数 | 81 |
| アクティブレスキュー数 | 106 |

## サイバー情勢分析部

- 国家安全保障戦略に基づく対応を強化すべく、IPA第五期中期目標において、**「サイバー状況把握力」を強化し、国家の安全保障・経済安全保障の確保に貢献**する旨を明記。2023年7月にサイバー情勢研究室を設置。
- 今後、**経済インテリジェンス収集力の強化**等によりサイバー情勢の集約・分析機能や対処支援能力の一層の強化を図るとともに、今通常国会で成立した**サイバー対処能力強化法に基づく業務への対応**により、**政府全体のサイバー安全保障体制の強化に貢献**していくため、2025年4月にサイバー情勢分析部に改組し、体制を強化。

**＜2024年度の取組・進捗＞**

- IPAが有する産業界とのネットワーク、セキュリティ対策に係る各種制度を駆使し、**産業分野のセキュリティ・リスク情報（サイバーインテリジェンス）集約のハブ**として機能を強化
- 地政学の専門家の協力も得つつ、経済活動に影響を及ぼすサイバーリスクを統合的分析、**産業分野に関する脅威評価のハブ**として機能
- 政府機関、産業界との連携対話を強化し、**防御や抑止対応に資する情報共有／対応支援活動のハブ**として活動を推進





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

# サイバー攻撃による被害に関する情報共有の促進に向けた検討会 最終報告書の概要

## 1．情報共有の重要性と現状の課題

- サイバー攻撃が高度化する中、単独組織による攻撃の全容解明は困難となっている。そのため、**攻撃の全容の把握や被害の拡大を防止する等の観点からサイバー攻撃に関する情報共有は極めて重要**。他方で、被害組織自らが情報共有を行うことについては、①被害組織側の調整コスト負担、②最適者が事案対応を行わない懸念、③処理コストのかかる情報共有、④被害現場依存の脱却の必要性などの課題が存在。

## 2．本検討会における提言

- **被害組織を直接支援する専門組織を通じた速やかな情報共有の促進が重要。**これにより、①全体像の解明による被害拡大の防止や②被害組織のコスト低減などが実現できる。
- 他方で、専門組織を通じた情報共有を促進するためには、**①秘密保持契約による情報共有への制約、②非秘密情報からの被害組織の特定/推測の可能性の課題に対応をする必要がある。**
- このため、本検討会では、これらの課題を乗り越え、既存の情報共有活動の枠組みも活用しながら、更に円滑な情報共有を可能とするために、被害者の同意を個別に得ることなく速やかな情報共有が可能な情報の考え方を整理。具体的には、通信先情報やマルウェア情報、脆弱性関連情報等の**「攻撃技術情報」から被害組織が推測可能な情報を非特定化加工した情報が対象となり得る**と整理。
- さらに、本報告書の提言を補完する観点から、**「攻撃技術情報の取扱い・活用手引き（案）」についてもとりまとめ**。本手引きでは、専門組織間で効果的な情報共有を行うために、どのような形で非特定化加工を行えばよいか、またどのように情報共有をおこなえばよいのかなど**専門組織として取るべき具体的な方針について整理**。
- 加えて、円滑な情報共有を促進すべく、上記考え方について**ユーザー組織と専門組織が共通の認識**を持ち、専門組織が非特定化加工済みの攻撃技術情報を共有したことに基づく**法的責任を原則として負わないことを合意するため**の**秘密保持契約に盛り込むべきモデル条文案を提示。**今後、本検討会の成果の**周知・啓発に取り組む**。

## 3．今後の課題

- 専門組織同士の情報共有促進だけでは解消されない**今後の課題**としては、**（1）情報共有に向けた官民連携のあり方**（行政機関への相談・報告のあり方や政府と民間事業者間の情報の共有など）、**（2）サプライチェーンにおけるベンダ等の役割**を挙げた。

# サイバーセキュリティ分野における防衛省との連携強化について
## （サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携）

- 防衛省・自衛隊を含む我が国のサイバー状況把握力及びサイバー事案への対処能力の強化並びにサイバー安全保障の確保に資することを目的として、経済産業省・IPAと**防衛省との間で連携を強化**すべく、協定書を締結（令和６年12月27日）。

### 連携協定の目的

第１条　本協定は、防衛省・自衛隊、重要インフラ事業者及び防衛産業事業者等企業等におけるサイバー事案（そのおそれがある事案を含む。以下同じ。）の未然防止及びサイバー事案発生時の被害の拡大防止等に関し、防衛省整備計画局（…）、経済産業省商務情報政策局（…）及び独立行政法人情報処理推進機構（…）が相互に緊密な連携を推進することにより、それぞれが保有するサイバー脅威情報等に係る技術的・専門的な知識や経験の相互利用を図り、もって防衛省・自衛隊を含む我が国のサイバー状況把握力及びサイバー事案への対処能力の強化並びにサイバー安全保障の確保に資することを目的とする。

### 連携協定の概要（想定される主な取組）

１．自衛隊によるIPAの取組への参画等を通じた産業界向けセキュリティ支援
- サイバーレスキュー隊（J-CRAT）への参加を通じた**標的型サイバー攻撃に関するハントフォワード活動への参画、協働展開**
- 制御システムの安全性・信頼性検証事業への参画（**重要インフラ事業者等へのリスクアセスメント**等）　　等

２．情報提供等を通じた防衛産業との連携強化
- サイバーディフェンス連携協議会（CDC）に対する**サイバー攻撃関連情報の共有・注意喚起**
- 防衛産業サプライチェーン向け経済産業省関連**中小企業支援策の普及展開**、IPAによる制御システムリスクアセスメントの普及促進　　等

３．３者間の新たな協議体（枠組み）の設置
- 上記１．及び２．の進捗管理その他全体の調整枠組みとして「サイバー連携フォーラム」を設置

# ５．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戦略」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。

# 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

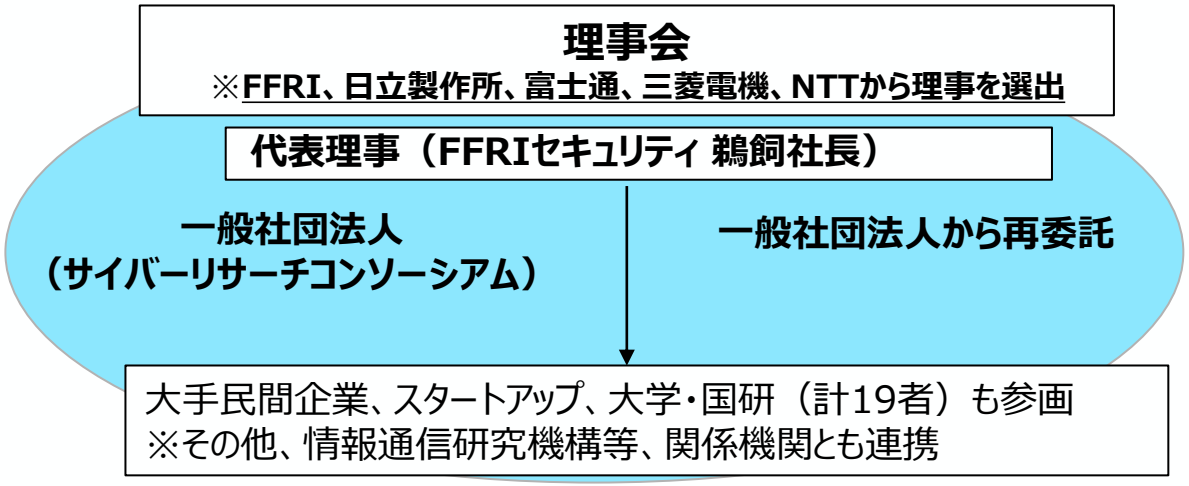
**経済安全保障重要技術育成プログラム「サイバー空間の状況把握・防御技術の向上及び共通基盤の整備」**

- 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。

## 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**




## 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**

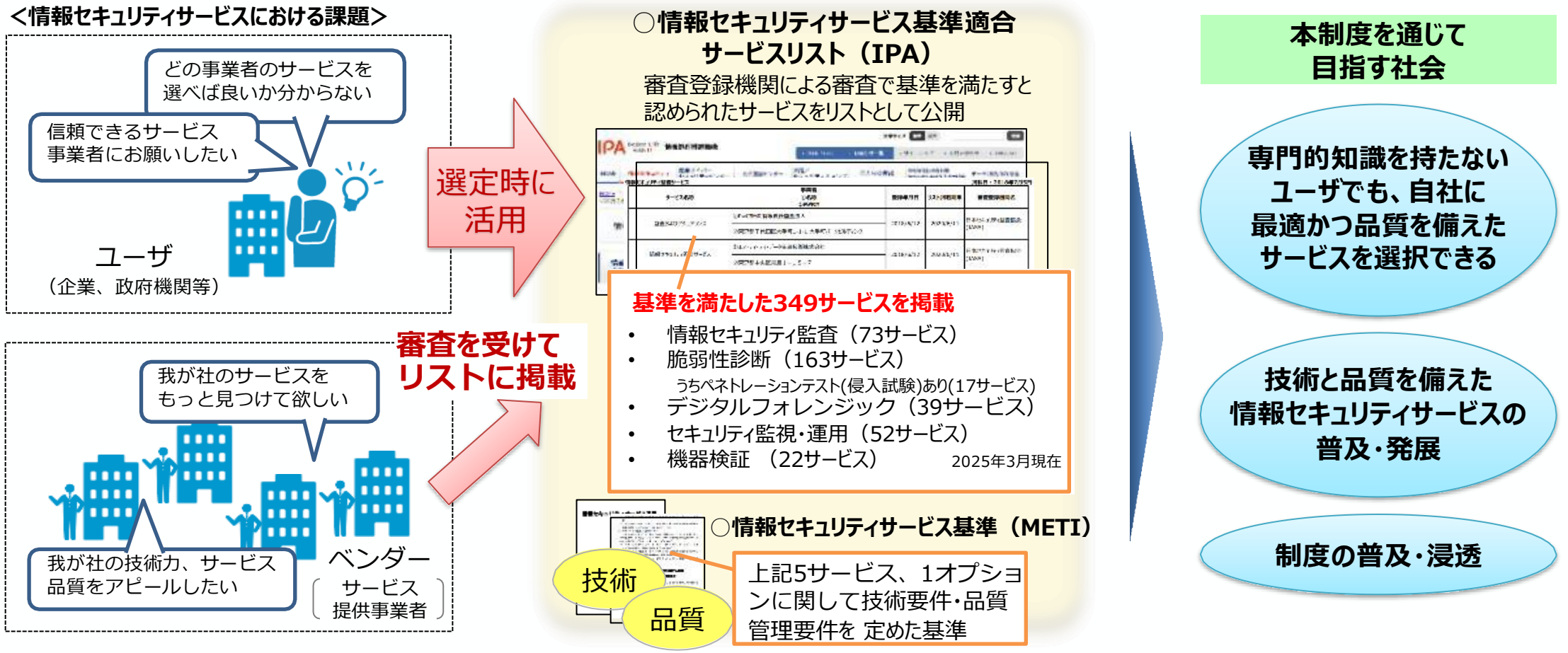
- 情報の効果的な連携に関わる技術
- 高度サイバー人材の評価・管理に関する技術

**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

# 情報セキュリティサービス基準適合サービスリスト

- **「情報セキュリティサービス基準」を策定**し、審査登録機関による**審査をクリアしたサービスのリストを公開**※。 ※IPA（独立行政法人情報処理推進機構）が公開。
- 令和６年度から、脆弱性診断のオプションとして、**ペネトレーションテスト（侵入試験）を追加。**




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

# サイバーセキュリティ人材の確保に向けた施策の全体像

## セキュリティ対策を進めるための体制・人材の考え方

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

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

**○人材確保・育成の実践的方策ガイド（β版）（中小企業の情報セキュリティ対策ガイドラインへの収録を想定）**

- 中堅・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、セキュリティ対策に関する経営者へ向けたメッセージ、外部人材の活用方策や教育・訓練機会等も提示（令和７年度中に成案化予定）

## 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

**○NISC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

**○デジタル人材育成プラットフォームにおける教育コンテンツの提示（マナビDX）**

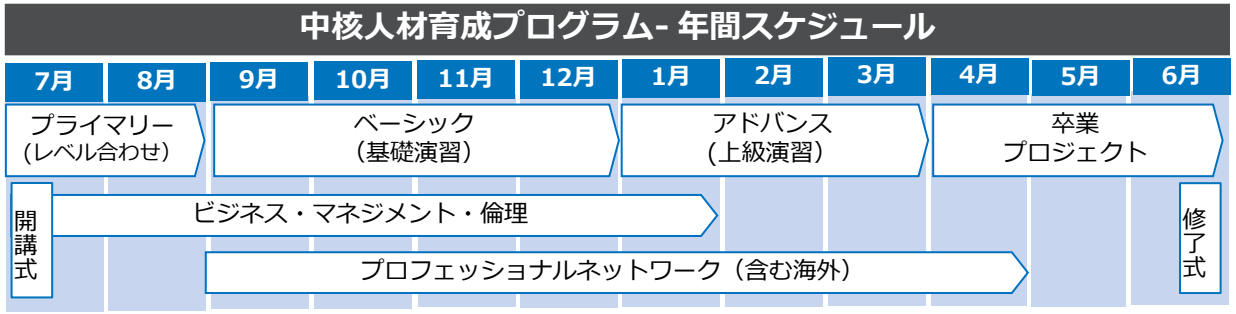
**○大学・高専等と産業界との連携**

# IPA産業サイバーセキュリティセンター（ICSCoE） ※2017年4月設置

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

**□　１年を通じた集中トレーニング「中核人材育成プログラム」**

**□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣**
**（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）**

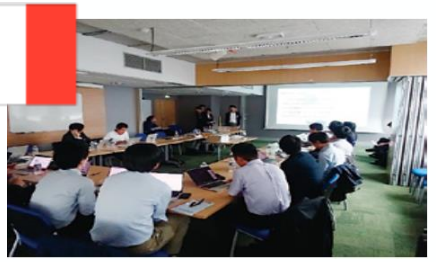



- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

**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**

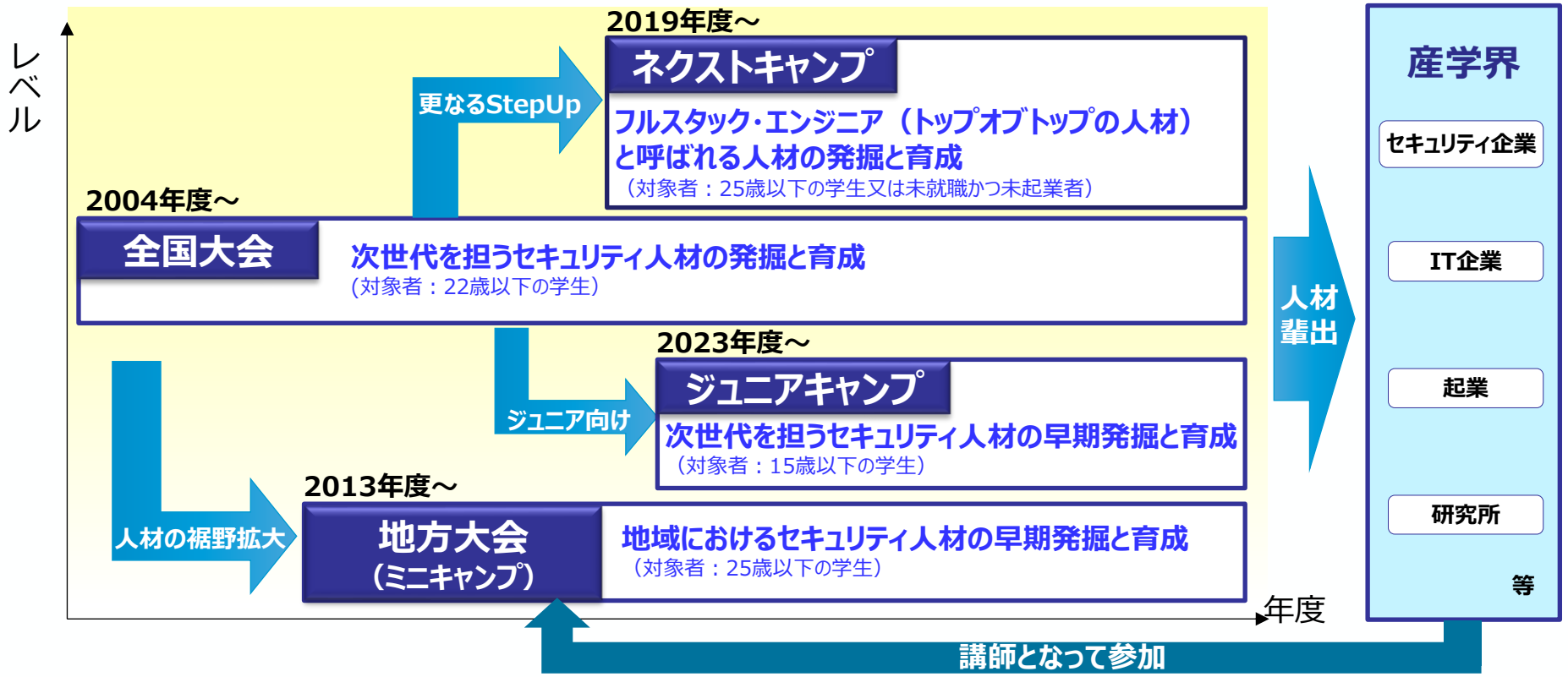
➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加



➢ 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

# 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・発掘する**ため、IPAとセキュリティ・キャンプ協議会が開催。計**約1,200名**が修了。
  ※地方大会（ミニキャンプ）を含めると計約3,000名が修了。
- 今後、裾野の拡大に向けた**新たなキャンプの実施**と、修了生の知見研鑽や活躍状況の共有等を目的とした**コミュニティを整備**していく。




## 今後の方向性（検討中）

- 単純拡大ではなく、裾野を広げる観点から、特定領域（AI等）の専門性と高度なサイバーセキュリティの知見の双方を兼ね備えた人材の育成を目的とする新たなキャンプを実施。
- 修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的としたコミュニティを整備。

# 情報処理安全確保支援士（登録セキスペ）制度

- サイバーセキュリティの確保を支援するため、**セキュリティに係る専門的な知識・技能を備えた国家資格として、「情報処理安全確保支援士」（通称：登録セキスペ）**制度を2016年に創設。2025年４月１日時点の登録者数は23,751人。

◆ 政府機関や企業等のサイバーセキュリティ対策を強化するため、専門人材を見える化し、活用できる環境を整備することが必要。

➡ **情報処理安全支援士の名称を有資格者に独占的に使用させることとし、登録簿を整備。**

◆ 技術進歩等が早いサイバーセキュリティ分野においては、知識等が陳腐化するおそれ。

➡ **有資格者の継続的な知識・技能の向上を図るため、講習の受講を義務化。**
**※登録の更新制導入により、義務講習を受講したもののみ登録を更新。**

◆ 民間企業等が安心して人材を活用できるようにするには、専門人材に厳格な秘密保持が確保されていることが必要。

➡ **業務上知り得た秘密の保持義務を措置。**

# サイバーセキュリティ人材の育成促進に向けた検討会最終取りまとめ（要点）

- 我が国においてサイバーセキュリティ人材が不足しているとの声は多く、国内で約11万人不足しているとの民間調査結果※もある。
（出典）ISC2 Cybersecurity Workforce Study 2023
- サイバーセキュリティ人材の不足に対応するためには、トップ人材や高度専門人材から、地域の中小企業等でセキュリティ対策を推進する人材まで、各層の課題に応じた施策を戦略的に進めることが重要。
- このため、これまで一定の効果を生み出している既存の施策の拡充・改善をベースとして、実際に政策ニーズを有する組織の方へのヒアリング等も通じ、令和７年５月に政策対応の方向性を取りまとめ。今後も各施策の継続的な改善を実施。

## 対応の方向性

### ①セキュリティ・キャンプ※の拡充


※世界に通用するトップクラスの人材を育成・発掘する取組

- AI等の特定領域と掛け合わせた高度セキュリティ人材の育成を目的とする新たな「キャンプ」を実施
- 修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的とした「コミュニティ」を整備

### ②登録セキスペ※の活用促進

※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（情報処理安全確保支援士）

- 個社の状況に応じた個別相談・支援等が可能な登録セキスペのリスト（アクティブリスト）を整備し、中小企業支援機関等を通じて中小企業との人材マッチングを促進
- 所定の実務経験を有する者を対象に、資格更新時の講習のみなし受講制度を導入　　等

### ③中堅・中小企業等における人材確保策の提示

- 中堅・中小企業が実施すべきセキュリティ対策に応じた人材確保・育成の実践的方策ガイドをβ版として整理
- 人材を「育成」する際に参照できる教材・資格等も提示

## 今後の取組

- 「セキュリティ・キャンプコネクト」として新たなキャンプを開催（令和８年春頃）
- 修了生向けコミュニティの活動開始（令和７年度中）

- アクティブリストの整備・運用開始（令和７年度中）
- 同リスト活用促進に向けた支援機関等との連携策具体化
- 省令改正により講習のみなし受講制度を創設（令和８年度中に制度開始想定）

- 中小企業に対するβ版の実証事業を実施等しながら成案化
※アクティブリストの活用方法も提示
- 中小企業向けセキュリティ促進施策との連携や広報資材の改善含め、普及活動を実施

## 目指す効果

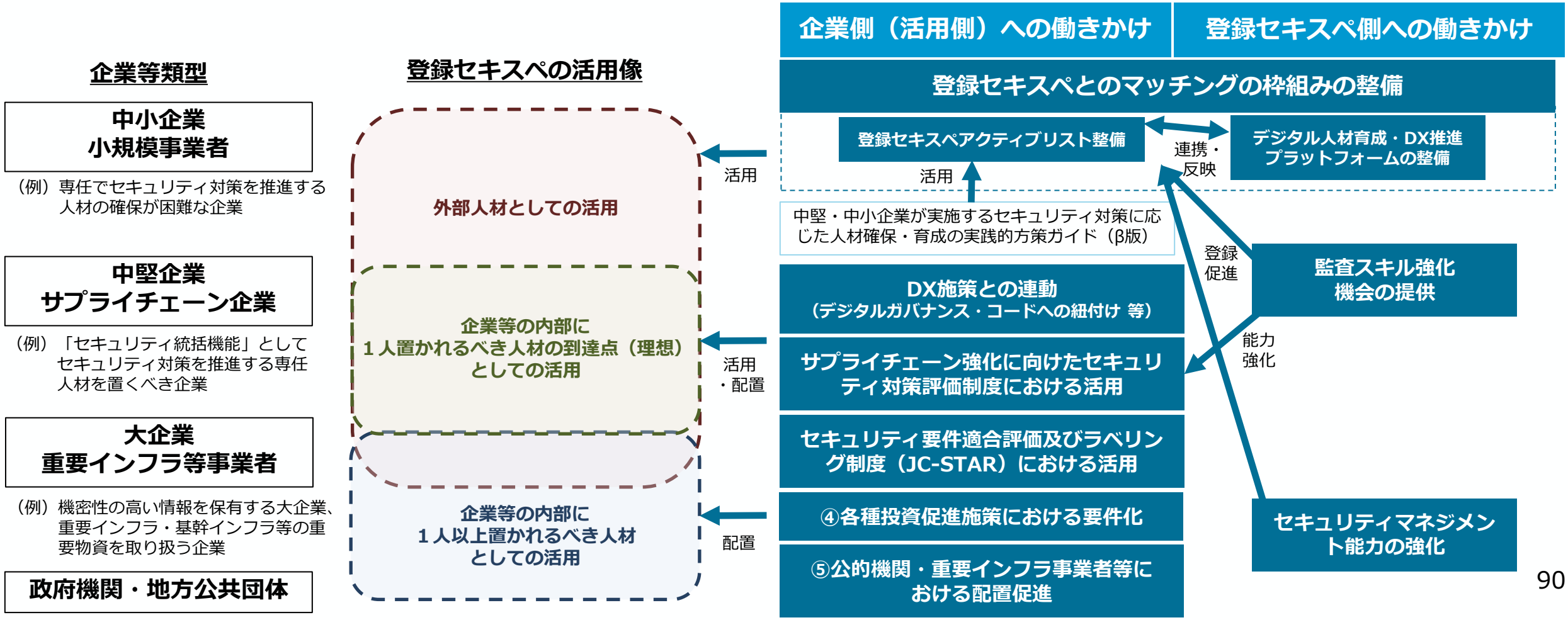
- 「トップガン」人材育成スケール拡大（現状の２倍以上）
- セキュリティ人材のキャリアの魅力化

- 登録セキスペの活躍機会（中小企業のセキュリティ確保等の実務経験機会）増加
- 登録セキスペ資格更新時の負担軽減
- 中堅・中小企業におけるセキュリティ人材探索コストの低減
- 中堅・中小企業内での内部人材育成容易化

2030年までに登録セキスペ５万人（2025年４月時点で約2.4万人）を達成

# （参考）登録セキスペの活用促進・活躍の場の拡大（施策の全体像）

- **企業等の類型によって登録セキスペに求められる役割は異なる**という点に鑑み、**中小企業等向けにはアクティブリストの整備を通じたマッチング枠組みの整備、中堅企業～大企業向けには各種対策促進制度との連動**、をそれぞれ検討。
- アクティブリストの活性化に向け、**登録セキスペに対するスキル強化・多様化につながる機会**を検討。



# ６．政府全体の動向

# 国家安全保障戦略（令和4年12月16日）に基づく政府の検討の方向性

## グローバルな安全保障環境と課題

- サイバー空間、海洋、宇宙空間、電磁波領域等において、自由なアクセスやその活用を妨げるリスクが深刻化している。特に、**相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている。サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている。**そして、武力攻撃の前から偽情報の拡散等を通じた情報戦が展開されるなど、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が、今後更に洗練された形で実施される可能性が高い。

## サイバー安全保障分野での対応能力の向上

- サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、**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。**
- **武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入**する。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

（ア）重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

（イ）**国内の通信事業者が役務提供する通信に係る情報を活用**し、**攻撃者による悪用が疑われるサーバ等を検知**するために、所要の取組を進める。

（ウ）**国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**について、**可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与**されるようにする。

- 能動的サイバー防御を含むこれらの取組を実現・促進するために、**内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組し、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を設置する。**そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。

# 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