経済産業省

サイバー攻撃の現状と
サイバーセキュリティ政策について

２０２５年８月

経済産業省 商務情報政策局
サイバーセキュリティ課

目次

１．サイバーセキュリティを取り巻く現状
２．サイバー安全保障の議論
３．経済産業省におけるサイバーセキュリティ政策の進捗と今後の方向性
４．産業界へのメッセージ

１．サイバーセキュリティを取り巻く現状

サイバー攻撃を行う主体について

①国家の支援を受けたグループ（APT（Advanced Persistent Threat）攻撃グループ）

- 執拗に高度で継続的な攻撃を行うことが特徴（つまり、ミッション達成優先でコスト度外視の攻撃集団）。インテリジェンス企業によれば、攻撃グループのバックについている国として中国、ロシア、北朝鮮、イランが挙げられている。

②サイバー犯罪組織（クライム（Crime）系）

- 情報等を盗んで現金化するグループ。2018年の被害総額は60兆円に達したという調査結果もあるようで、既に一大市場となっており、攻撃用ツール制作・販売、攻撃起点の時間貸しなど、様々な犯罪サービスの分業化が進展。

③ハクティビスト

- 「アクティビスト（社会活動家）」と「ハッカー」を掛け合わせた言葉で、サイバー攻撃を通じて社会的・政治的メッセージを発信していくことを主眼とした活動を行うグループ。アノニマスもハクティビストと捉えられることが多い・

④悪意のある個人（愉快犯、腕試し等）

- 趣味や研究の延長として個人が行う攻撃で、子供が行っているケースも少なくない。ただし、②の攻撃用ツールを使ったりしているうちに犯罪グループの活動に取り込まれているようなことも。

⑤産業スパイ

- 知的財産の窃取を目的とした攻撃グループ。

※実態は、上記のようにきれいに分類することは困難。例えば、普段はクライム系として活動しているグループが、要請に応じて“傭兵”となってAPT攻撃グループとして働いている可能性が指摘されている。

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（ダークウェブ）の存在

- **ダークウェブの闇市場**では非合法で個人や企業の機密データ、**マルウェアを容易に作成できるツールキットなどが取引**されており、**サイバー犯罪を助長**している。

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。

２．サイバー安全保障の議論

サイバー対処能力強化法及び同整備法の全体像

- 国家安全保障戦略（令和4年12月16日閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISCの発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置** 等の実現に向け検討を進めるとされた。
- これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和6年6月7日からサイバー安全保障分野での対応能力の向上に向けた有識者会議を開催し、同年11月29日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に「サイバー対処能力強化法案」及び「同整備法案」を閣議決定。国会での審議・修正を経て、同年5月16日に成立、同月23日に公布。

概　要

総　則
- 目的規定、基本方針等（第１章）

官民連携（強化法）
- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告

  （第２章）
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用（強化法）
- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
- （同意によらない）通信情報の取得（第４章、第６章）
- 自動的な方法による機械的情報の選別の実施（第22条、第35条）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の取扱制限（第５章）
- 独立機関による事前審査・継続的検査 等（第10章）

→ 分析情報・脆弱性情報の提供等（第８章）

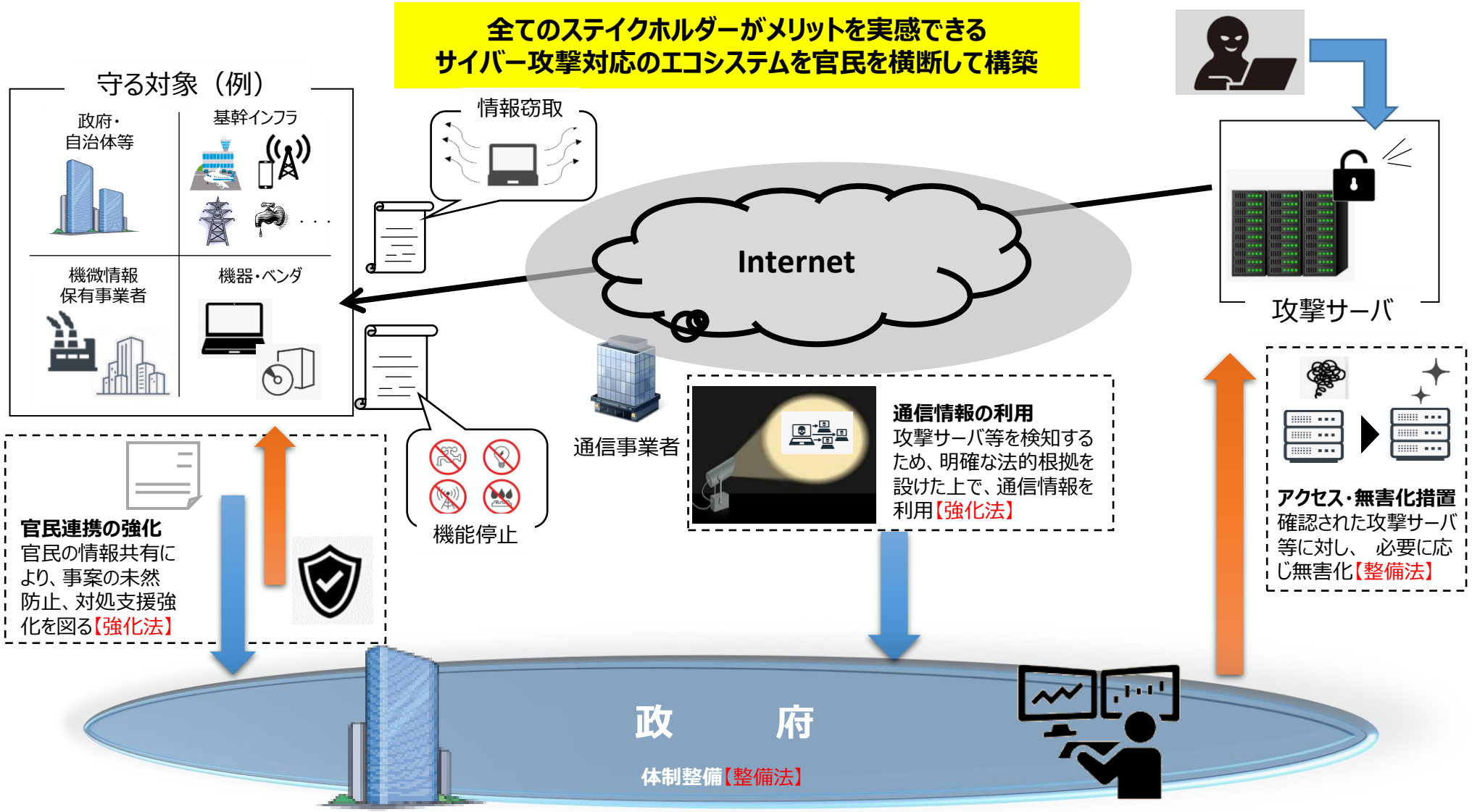
アクセス・無害化措置（整備法）
- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等（警察官職務執行法改正）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

組織・体制整備等（整備法）
- サイバーセキュリティ戦略本部の改組、機能強化（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設（内閣法改正）　等

施行期日
公布の日（令和7年5月23日）から起算して1年6月を超えない範囲内において政令で定める日　等

全体イメージ

「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。



３．サイバーセキュリティ政策の進捗と今後の方向性

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

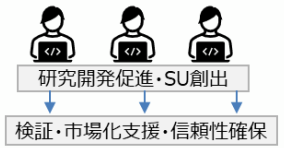
③政府全体でのサイバーセキュリティ対応体制の強化

- 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

サイバー・フィジカル・セキュリティ対策フレームワーク

SC対策強化

- 2019年4月に「Society5.0」によって柔軟化・拡張するサプライチェーンに求められる**セキュリティへの対応指針**として、「サイバー・フィジカル・セキュリティ対策フレームワーク」（**CPSF**）を策定。
- 国際規格化については、2025年3月の国際会合にて承認段階（DTS）への移行が決定。TS原案（DTS）合意後に投票を行い、2/3以上の賛成を得た場合TSが成立し、2025年度内の発行を目指す。

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

「Society5.0」以前

個々の企業主体の定型的なつながりで価値を生み出す

<3層構造>

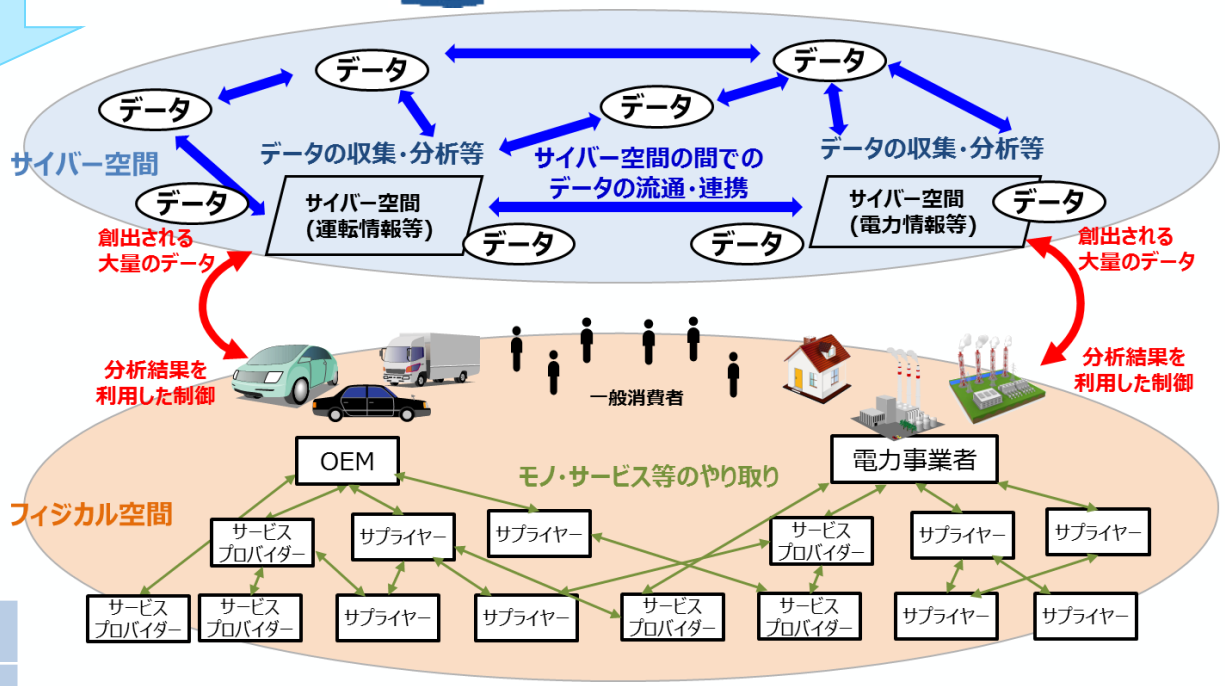
【第３層】
サイバー空間におけるつながり

【第２層】
フィジカル空間とサイバー空間のつながり

【第１層】
企業間のつながり

<6つの構成要素>

ソシキ	ヒト	モノ
データ	プロシージャ	システム



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

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

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

CPSFを軸とした各種ガイドライン等の整備

SC対策強化

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

主なガイドラインや対策ツール

経営層　実務層（共通）　実務層（産業分野個別）

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）　（2019年4月）

コンセプト

具体的対策

サイバーセキュリティ経営ガイドライン
（Ver3.0：2023年3月）

中小企業の情報セキュリティ対策ガイドライン（IPA）
（第3.1版：2023年４月）

3層：協調的なデータ利活用に向けたデータマネジメント・フレームワーク
（ver1.1：2024年2月）

SW：OSS管理手法の事例集
（2021年4月）

2層：IoTセキュリティ・セーフティ・フレームワーク
（2020年11月）

SBOMの導入に関する手引
（ver2.0：2024年8月）

ASM導入ガイダンス
（2023年5月）

可視化ツール
（ver2.1：2023年7月）

サイバーセキュリティお助け隊サービス
（2021年4月～）

ビル分野のガイドライン（空調編：2022年10月）（共通編第２版：2023年４月）

自動車分野のガイドライン（第２．２版：2024年8月）

スマートホーム分野のガイドライン（第１．０版：2021年４月）

電力分野のガイドライン（小売電気事業者 第１．０版：2021年2月）

・・・

工場分野のガイドライン（第１．０版：2022年11月）（スマート工場：2024年４月）（重要性と始め方：2025年４月）

宇宙分野のガイドライン（第２．０版：2024年3月）

半導体分野のガイドライン（策定中：2025年秋頃公開予定）

サイバーセキュリティ経営ガイドライン

平成27年12月28日策定
令和5年3月24日第3版公表

SC対策強化

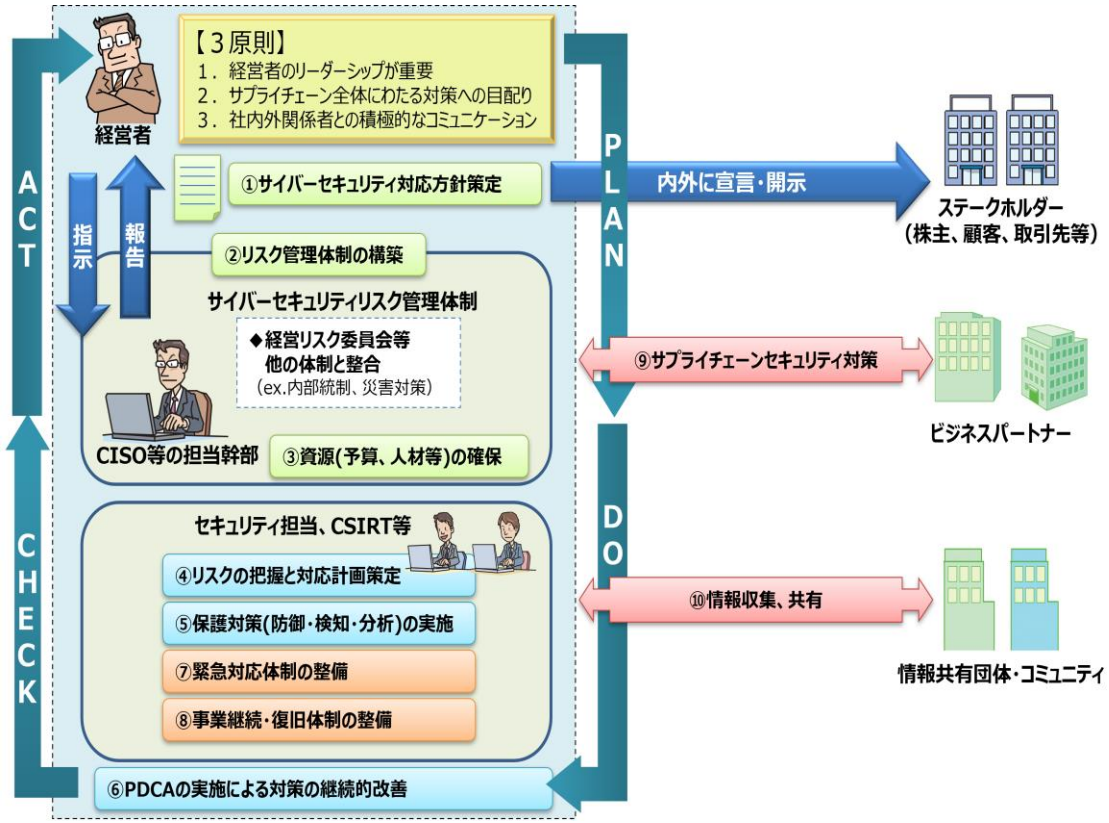
- 経営者がリーダーシップをとってセキュリティ対策を推進することが重要。このため、**経営者を対象としたガイドライン**を策定。可視化ツールや実践事例集なども整備。

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 **指示２** 管理体制の構築 **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 **指示５** リスクに対応するための仕組みの構築 **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 **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



https://www.meti.go.jp/policy/netsecurity/mng_guide.html

半導体関連産業のセキュリティ対策水準の強化

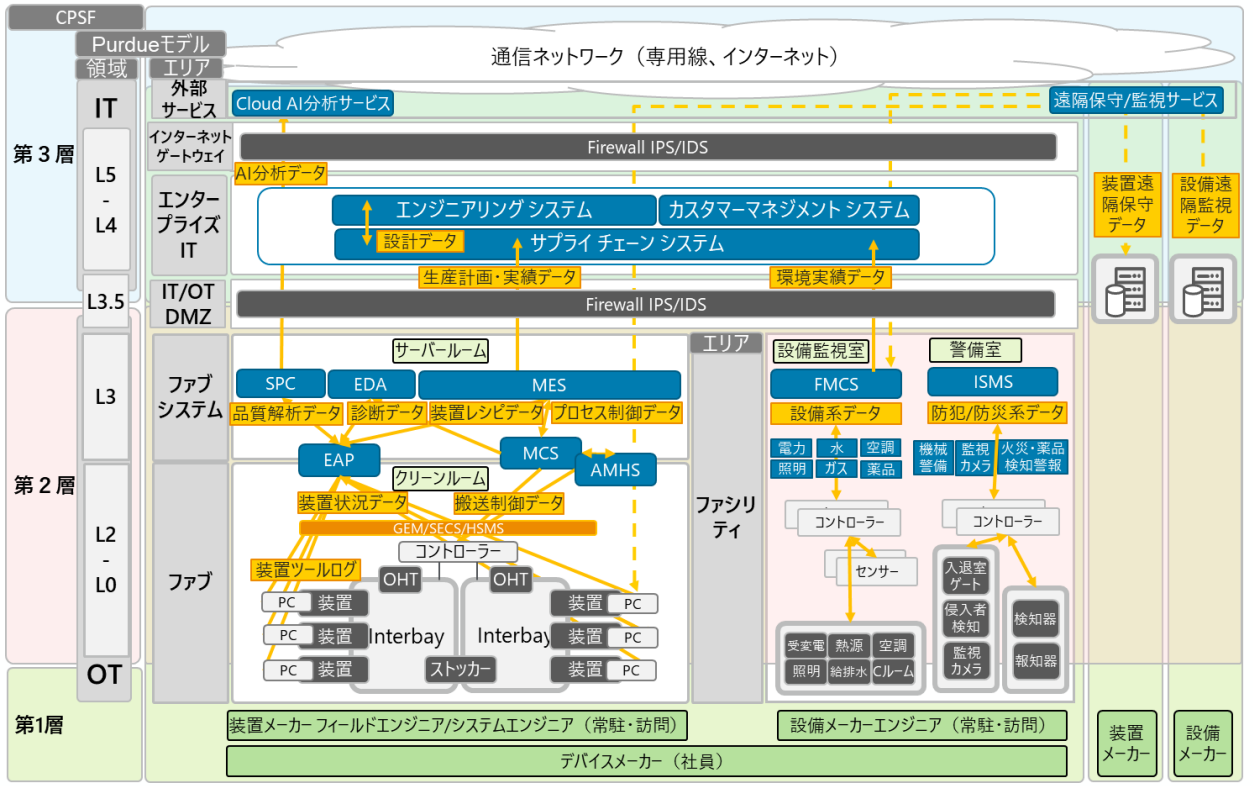
SC対策強化

- 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。**
- 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**に向けた検討し、本年6月**「半導体デバイス工場におけるOTセキュリティガイドライン」を公表。**現在パブコメ中で、本年秋頃成案化予定。
- 本対策の内容を**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。**

半導体デバイス工場におけるOTガイドライン

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

半導体デバイス工場のリファレンスアーキテクチャ



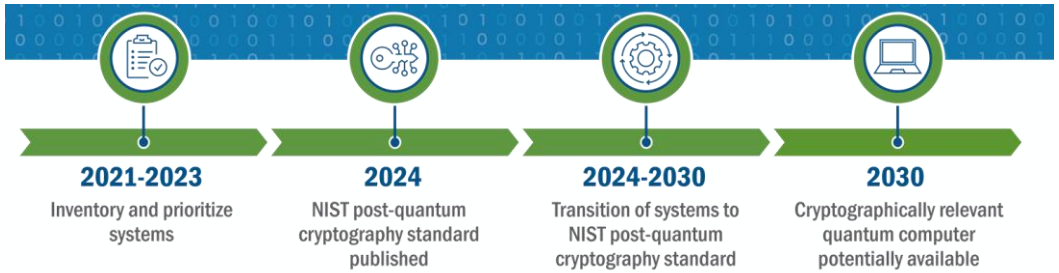
関係省庁と連携した耐量子計算機暗号への対応の検討

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、政府機関等におけるPQC利用に関して、技術的課題、安全保障、国際連携等の多岐にわたる課題に対し必要な施策を検討・推進するため、**本年６月に関係府省庁による連絡会議（局長級）を立ち上げ**。
- 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

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 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が標準的に目指すべきセキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施
評価スキーム	自己評価	第三者評価	第三者評価

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

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

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

制度実現に向けた検討課題の例

- **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）

中小企業支援施策の全体像

SC対策強化

- 中小企業等が抱える主な課題：「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

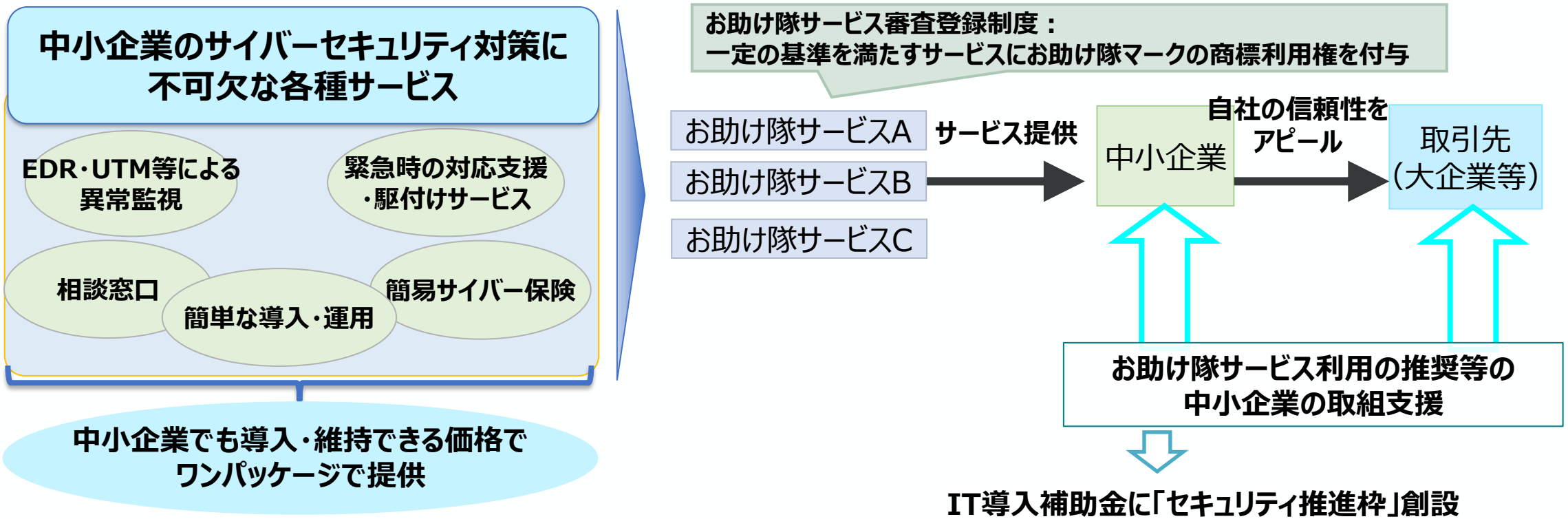
企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

⇒自社の状況に即したより実効的な取組の検討・実行

サイバーセキュリティお助け隊サービス

SC対策強化

- サイバーセキュリティお助け隊サービスは、**中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価（例：月額1万円以内）に提供するサービス。全国46事業者がサービスを提供**しており、**約8500件の利用実績**（2025年3月末時点）。
- IT導入補助金「セキュリティ対策推進枠」の活用で、**導入費用の1/2（小規模事業者は2/3）の補助が可能。**
- 更なる普及候補に加えて、サプライチェーン評価制度に対応したサービスのあり方等も検討予定。



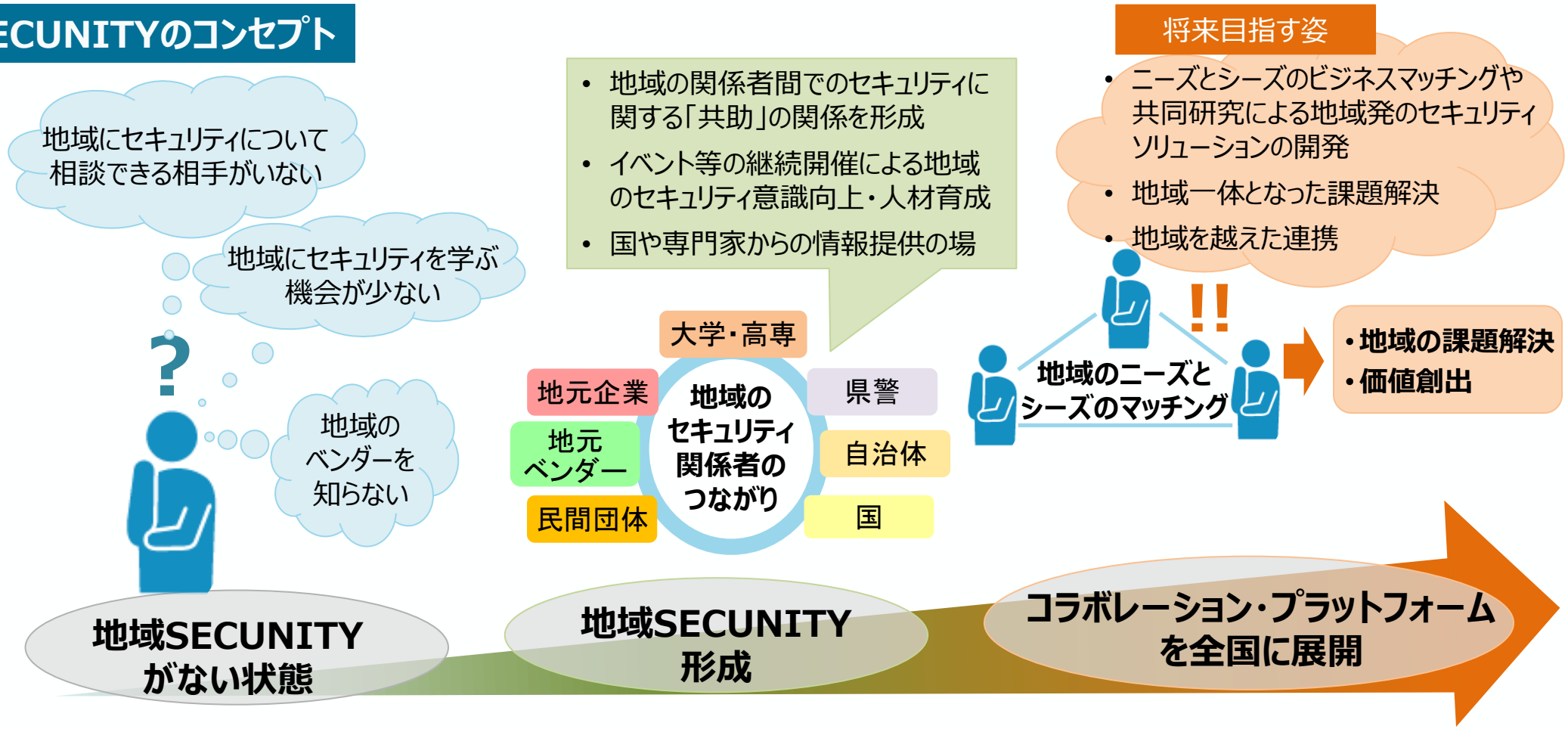
サイバーセキュリティお助け隊サービスの利用はこちらから
⇒ https://www.ipa.go.jp/security/otasuketai-pr/

地域SECUNITY（地域に根付いたセキュリティ・コミュニティ）

SC対策強化

- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動を、「地域SECUNITY」と命名。
- まずは各地域で地域SECUNITYの形成を促進し、将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指す。

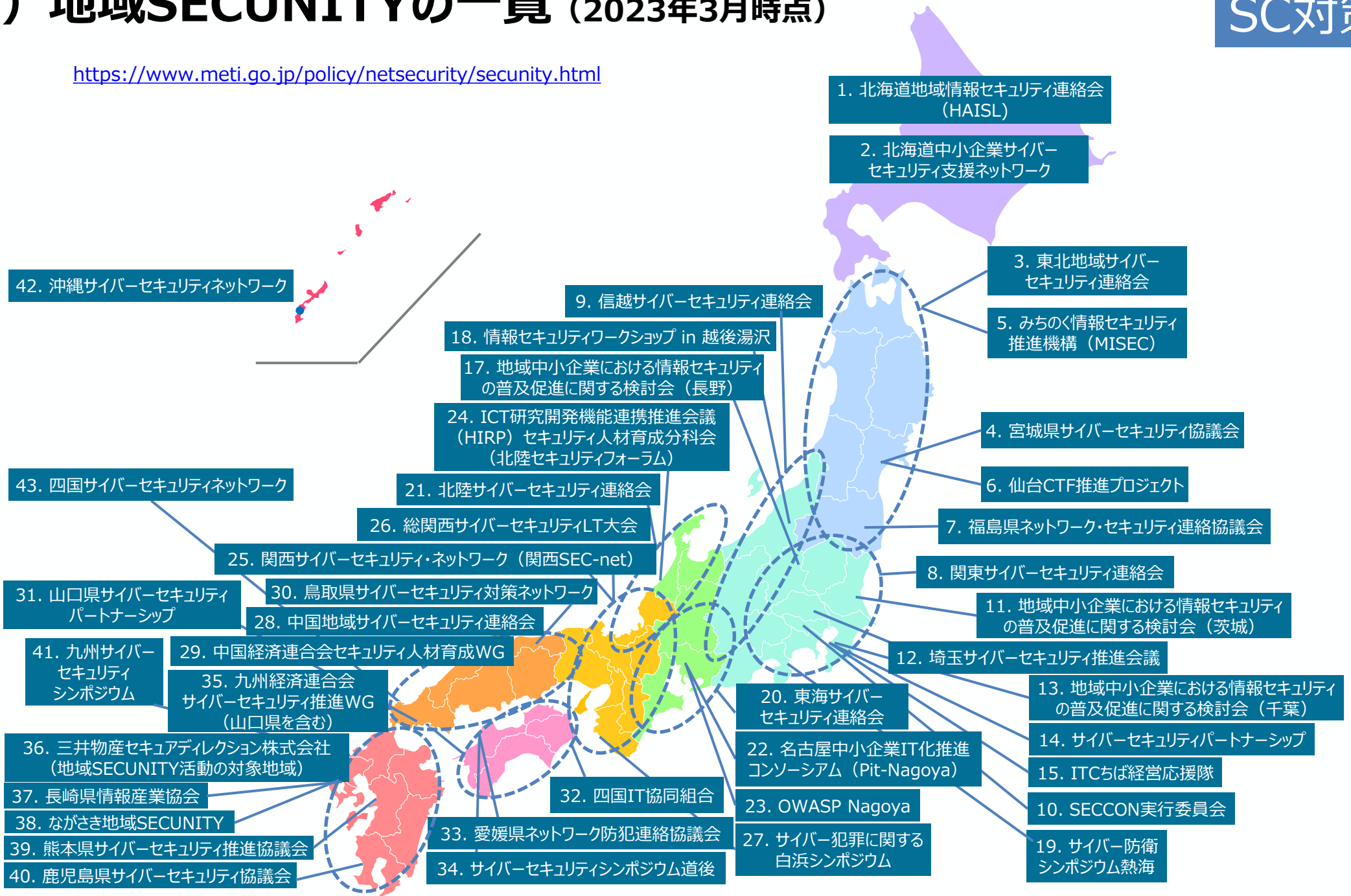
地域SECUNITYのコンセプト



（参考）地域SECUNITYの一覧（2023年3月時点）

SC対策強化

https://www.meti.go.jp/policy/netsecurity/secunity.html



IoTセキュリティ適合性評価制度（JC-STAR）

SBD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25日より運用開始（まずは最低限の基準（★１）を開始）。**現在、約500製品がラベル取得済み。
- 今後、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。
- **政府調達の要件化**等を通じて、中央政府、地方公共団体、重要インフラ事業者、その他民間事業者等へ普及展開を図る。併せて、**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。

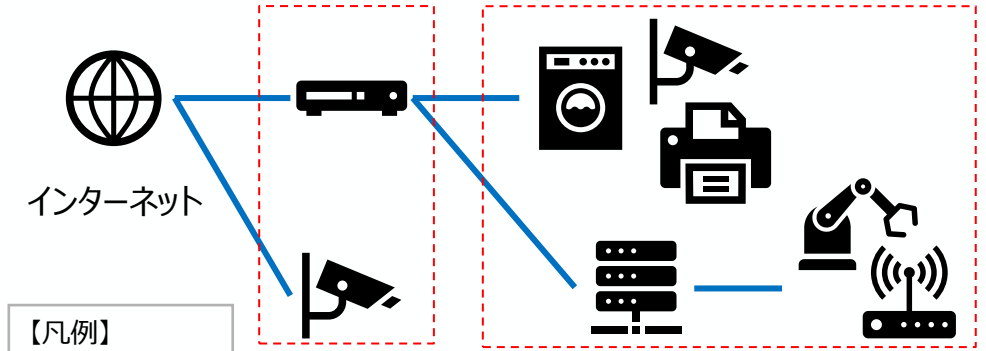
制度名称・ロゴ・ラベル

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

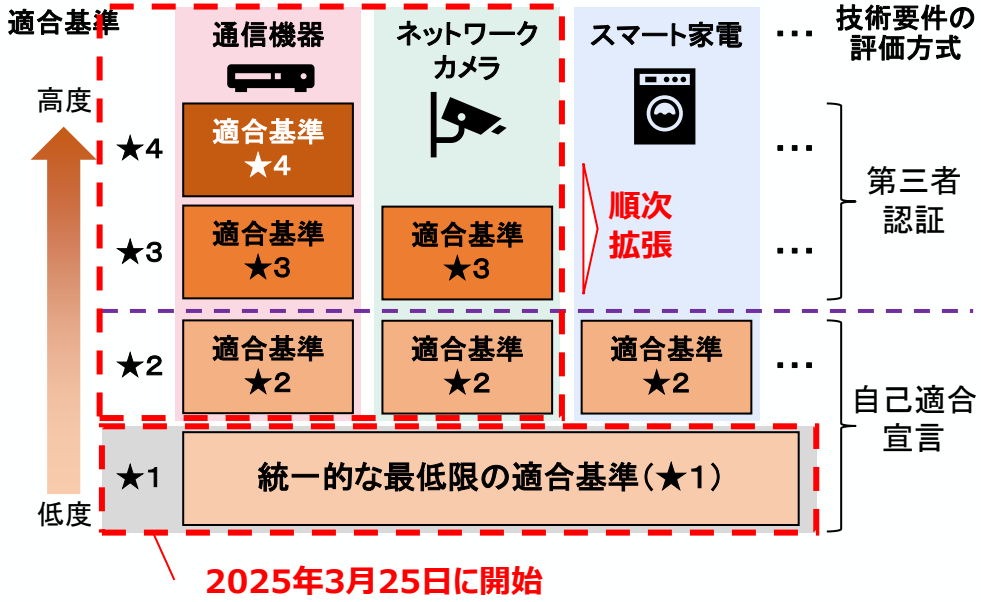
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

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

セキュア・バイ・デザインの実践向けた取組（ソフトウェアのセキュリティ確保）

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

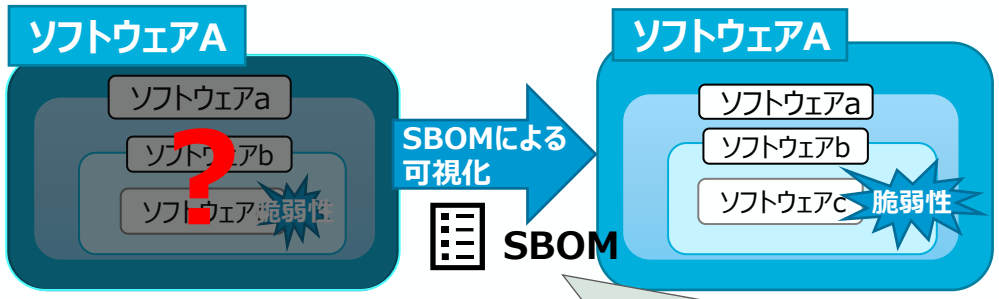
CISA “Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software”

ソフトウェア管理に向けたSBOMの活用促進

SBDの実践

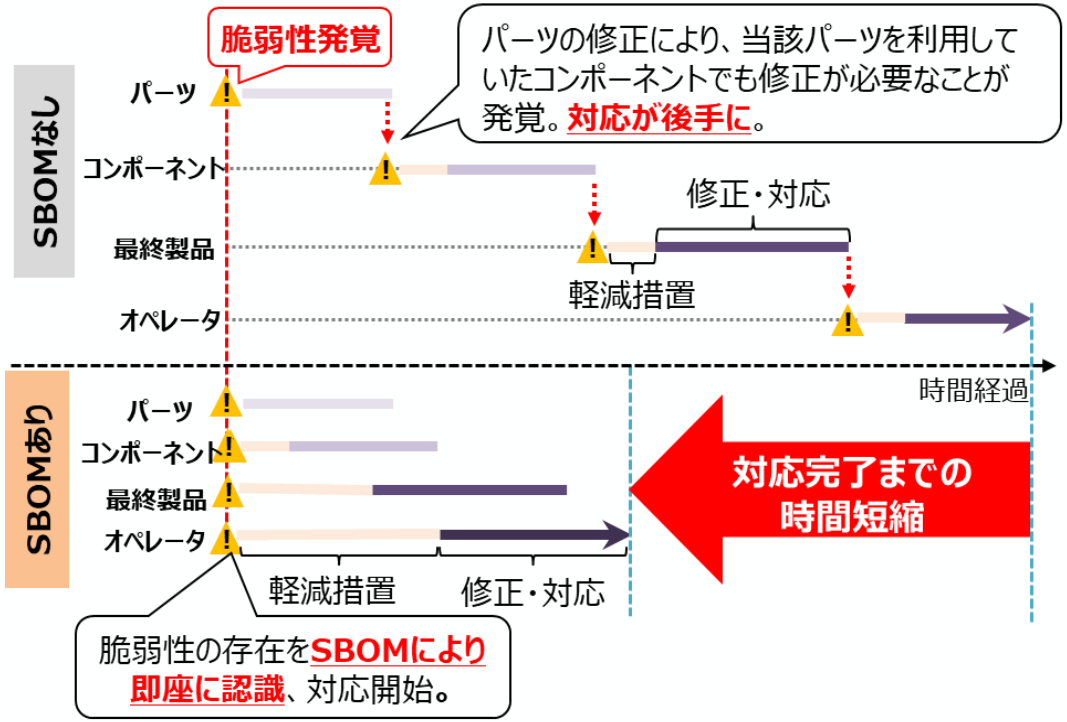
- SBOM（Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。ソフトウェアを構成する各コンポーネントを誰が作り、何が含まれ、どのような構成となっているか等を示す。SBOMによりソフトウェアの構成情報の透明性を高めることで詳細を把握することができ、ライセンス管理や脆弱性対応への活用が期待される。
- 2023年7月、SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示した**「ソフトウェア管理に向けたSBOMの導入手引」を公表。**
- **2024年８月に改訂版を公表**。主な改定ポイントは、**①脆弱性管理プロセスの具体化**、**②「SBOM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



SBDの実践

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

SSDF導入ガイダンス案（中間整理）概要（2025年3月公表）

SBDの実践

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

ステップアップサイクル

1. 要求分析
2. 現状把握
3. タスク達成レベルの定義とギャップ分析
4. タスクの実践
5. 達成度評価
6. 自己適合宣言

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。

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。

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

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
- 対処機関との**人的交流・共同対処支援の促進**

＜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**
- **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」の概要

CS能力強化

- 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

CS能力強化

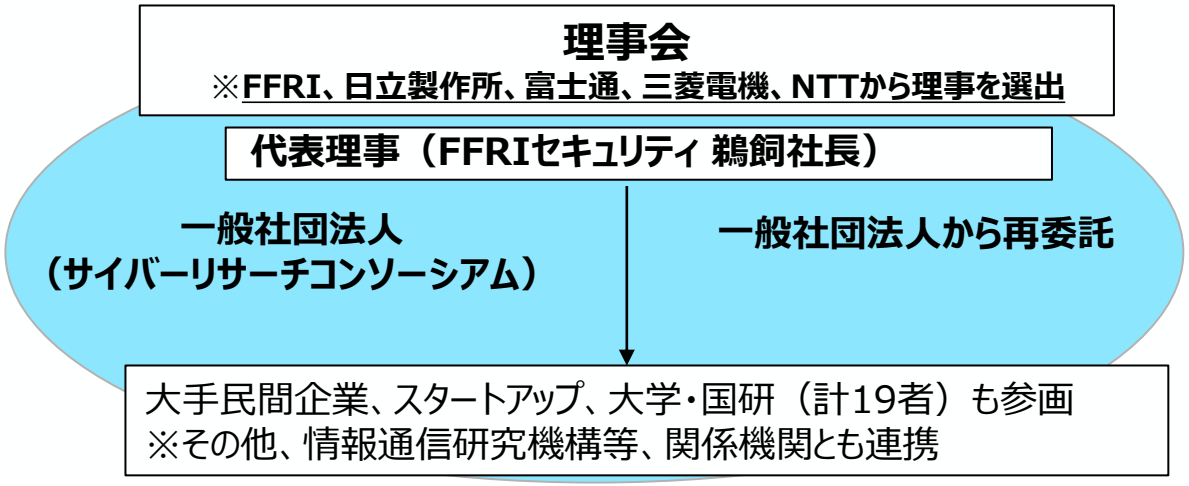
経済安全保障重要技術育成プログラム「サイバー空間の状況把握・防御技術の向上及び共通基盤の整備」

- 高度かつ未知の攻撃にも対処可能な**攻撃の早期発見技術**や、AIを活用したシステムの脆弱性の検知・評価技術など**防御力向上に資する技術**の開発・社会実装に向け、**約300億円／５年の研究開発プロジェクト**を立ち上げ、2024年７月からプロジェクト開始。

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

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

CS能力強化

セキュリティ対策を進めるための体制・人材の考え方

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

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

○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・実践型教育（マナビDX）

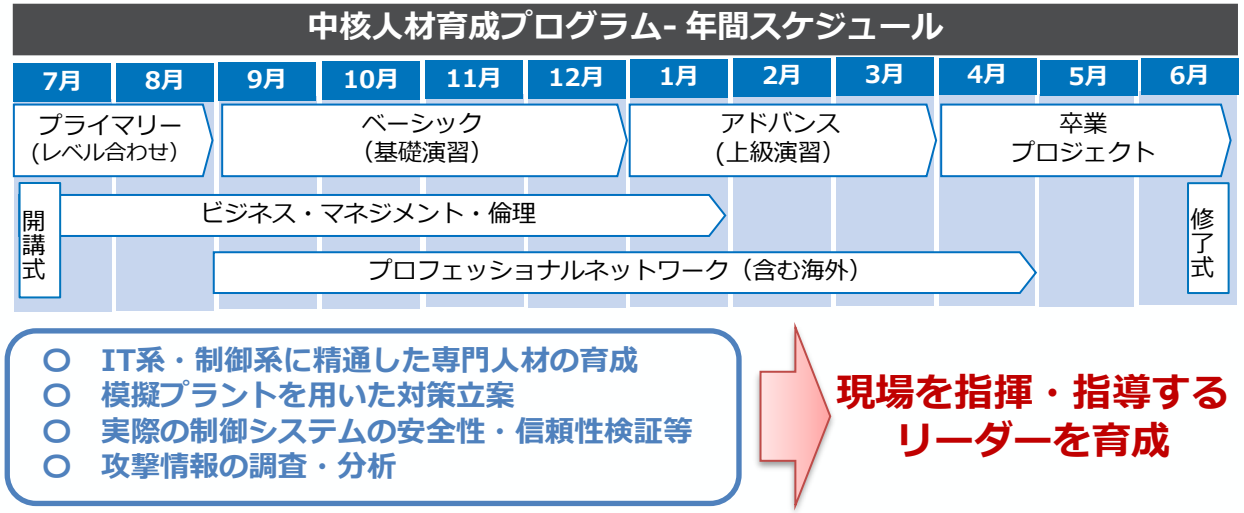
○大学・高専等と産業界との連携

IPA産業サイバーセキュリティセンター（ICSCoE）CS能力強化

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

□　１年を通じた集中トレーニング「中核人材育成プログラム」

□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人、第８期：57人、第９期：55人）



- 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

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 CS能力強化

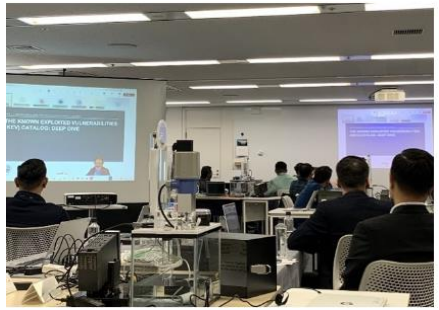
- 経済産業省とIPA産業サイバーセキュリティセンター(ICSCoE)が、**米国・EU政府等と連携し、毎年開催するインド太平洋地域向けの1週間の研修プログラム**。これまで2018年度より毎年開催。
- 本演習では、**インド太平洋地域の重要インフラ事業者、製造業者等のICSセキュリティの向上を目的**に、**産業用制御システム（ICS）のサイバーセキュリティに焦点**を当て、IPA産業サイバーセキュリティセンターの施設を使用した**ハンズオン演習**や、**日米欧専門家による講演**、**参加者間のネットワーキング**を実施。

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

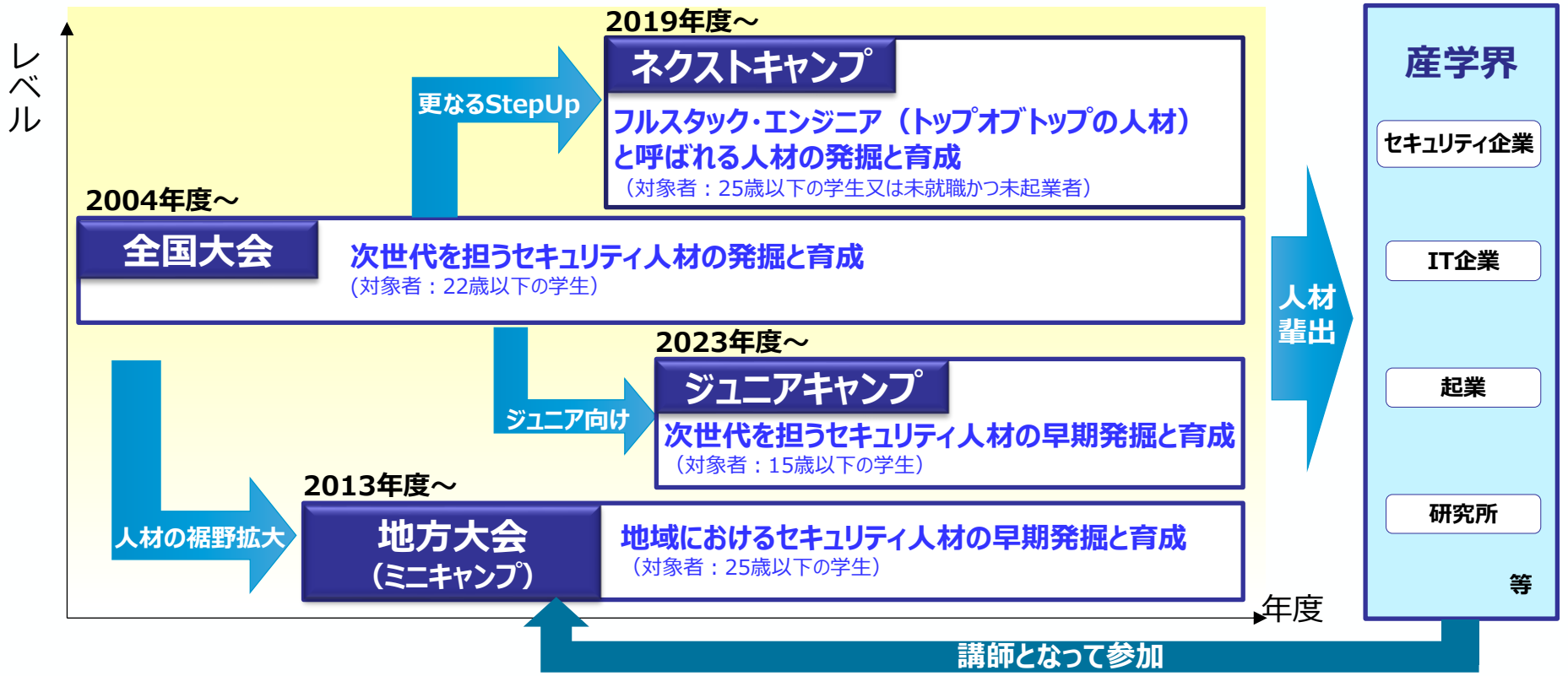


インド太平洋地域参加者間のネットワーキング

セキュリティ・キャンプ

CS能力強化

- **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1,300名**が修了。
  ※地方大会（ミニキャンプ）を含めると計約3,100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

- 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

CS能力強化

- 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（根拠法：情報処理の促進に関する法律）。
- 国家試験に合格後（※）、IPAに登録することにより資格を取得。 **登録資格は3年ごとに更新**（定期的な講習受講が義務付け）が必要。 **登録者数は23,751人**（2025年４月１日時点）。
  ※試験合格者に加えて、国が指定するポストやプログラムに従事した者も登録セキスペとなる資格を有する
- 登録セキスペには、①経営課題への対応（リスク評価、セキュリティ対策、監査）、②システム等の設計・開発（設計段階からのセキュリティ対策）、③運用・保守、④緊急対応等の幅広い業務での活躍が期待されている。

登録セキスペのメリット

＜取得者のメリット＞

①情報セキュリティに関する高度な知識・技能を保有する証

②継続的・効果的な自己研鑽が可能

③就業機会・業務範囲の拡大（※１）

※1 PCI DSS監査人の資格要件、情報セキュリティ監査人資格の取得の優遇、中小企業支援とのマッチング機会等

＜組織･企業へのメリット＞

①提供する機能やサービスへの信頼の向上

②社会的評価・信頼の向上（※２）

③ビジネスチャンスの拡大（※３）

※2 知識・技能の証明に加えて、資格保有者は信用失墜行為の禁止や秘密保持の義務有する

※3 各種補助金、「デジタルガバナンスコード」（DX銘柄やDX認定基準）、サプライチェーン評価制度での活用等を推進

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）

CS能力強化

- 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。
- 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。

（出典）ISC2 Cybersecurity Workforce Study 2023

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

目標

- 「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

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

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

- 経営者の皆様におかれては、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 指示２ 管理体制の構築 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 指示５ リスクに対応するための仕組みの構築 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 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）
- 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）」

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**の**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」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）
- 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）」

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**被害組織の合意を得る努力**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）
  - 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）」

  ○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）
  - 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）」

- 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）

METI
Ministry of Economy, Trade and Industry

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

経済産業省　サイバーセキュリティ　検索