経済産業省

資料３

第８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６年４月５日

経済産業省

商務情報政策局

目次

最近の主なサイバー攻撃事案（国内）

①機微技術情報などの窃取

- 先端技術情報を扱う中小企業の従業員や、国内の学術関係者等に対する**ソーシャルエンジニアリング**（私的なSNSアカウントに対して好待遇の求人情報をもちかける、講演や取材依頼等を装ったメールを送信する等）を観測。**マルウェア感染を通じた情報窃取**が目的とみられ、**特定の国家を背景とする**攻撃集団によるとみられるケースもある。
- ルータやVPNなどインターネット境界に設置された装置の脆弱性が狙われる「**ネットワーク貫通型攻撃**」が、**サイバー情報窃取活動における攻撃の初段として用いられる**ケースが増加。侵害されたネットワーク装置等にバックドアが設置されるケースも。

②工場等の機能停止

- 自動車部品メーカーが、ランサムウェア攻撃を受けサーバがダウン。同社と連係関係にある自動車メーカーは、**国内全工場の稼働を１日間停止**。（2022年３月）
- 公立病院がランサムウェア攻撃を受け、電子カルテシステムに障害が発生し、緊急以外の手術や外来診療が一時停止する等、**２か月以上にわたって通常診療ができない状況**に。（2022年10月）
- 港のコンテナターミナルにおいて、ランサムウエア攻撃によるシステム障害が発生し、**約3日間コンテナの搬入・搬出が停止**。（2023年７月）

③顧客情報等の漏えい

- 通信サービス企業が、委託先企業の従業員が所持するPCがマルウェアに感染したことを契機として、第三者による不正アクセスを受け、**利用者情報等約44万件の漏えい**があった旨を発表。その後の調査で**従業員等約8万件の個人情報漏えい（可能性含む）**も判明。（2023年11月、2024年2月）

④アクセス障害

- ALPS処理水放出に伴いハッカー集団が政府関係機関や原子力関係組織に対する攻撃を示唆。（2023年8月～）

最近の主なサイバー攻撃事案（海外）

①機微情報などの窃取

- SolarWinds社のネットワーク監視ソフトウェアに**正規のアップデートを通じてマルウェアが仕込まれ**、感染が拡大（サプライチェーン攻撃）。米政府機関等を含む**最大約18,000組織が影響**し、多くの組織で情報窃取等の被害が確認。（2020年12月）

②工場等の機能停止

- 米石油パイプライン大手（コロニアル・パイプライン）が**ランサムウェア攻撃を受け**、**全ての業務を一時停止**。米運輸省が燃料輸送に関する緊急措置の導入を宣言する事態に陥った。（2021年5月）
- 世界の少なくとも150か国において、Windowsの脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。**世界規模で拡大し、医療、空港、通信、鉄道等幅広い分野に影響**。英国では、多数の病院で電子カルテや病理診断システムが使用不能に。（2017年５月～）
- 米国ペンシルバニア州西部にある水道局において水圧の監視や調整を行う複数の加圧施設がサイバー攻撃を受け、**手動での操作に切り替え**て運用を継続。同様の事案が米国内で複数件発生。（2023年11月）。

③インフラの破壊

- ウクライナでは、**サイバー攻撃による大規模な停電が複数発生**。標的型メールにより認証情報が窃取され、変電所のブレーカーが遠隔操作されて大規模停電に至った例（2015年12月）や、マルウェアから制御システムに直接コマンドが送信され１時間程度の停電に至った例（2016年12月）、侵入先の正規ツールを悪用する攻撃（現地調達型の攻撃）により変電所のブレーカーが遮断され、**ミサイル攻撃と同時に停電が発生**した例（2022年10月）等。
- **特定の国家を背景**とする攻撃集団による、「**ネットワーク貫通型攻撃**」を利用した重要インフラ等を標的とする攻撃キャンペーン等の活動が報告。（2023年５月）

サイバー攻撃の現状

- 企業等の情報を暗号化して金銭をゆすり取る「**ランサムウェア攻撃**」やセキュリティ対策に弱点のある取引先等が攻撃経路として狙われ、被害が拡大する「**サプライチェーンの弱点を悪用した攻撃**」により、甚大な影響が生じている。また国家支援型の攻撃集団等が特定の企業を執拗に狙う「**標的型攻撃**」も大きな課題。
- 社会のデジタル化は進展する一方、AI等のデジタル技術の発展や地政学情勢の不安定化の影響もあり、**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**。

情報セキュリティ10大脅威 2024

順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい等の被害
4位	標的型攻撃による機密情報の窃取
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	不注意による情報漏えい等の被害
7位	脆弱性対策情報の公開に伴う悪用増加
8位	ビジネスメール詐欺による金銭被害
9位	テレワーク等のニューノーマルな働き方を狙った攻撃
10位	犯罪のビジネス化（アンダーグラウンドサービス）

<出典：(独)情報処理推進機構(IPA)、2024.1.24>

デジタル技術の発展によるサイバーリスクの増加の例

■　情報システムの利用拡大やクラウド等の活用拡大、インターネットに接続されるIoT製品の急増（2019年：231億台⇒ 2024年：399億台）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**。

■　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 ツールも登場**。

□　NICTER において2023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6,197億パケット（2018年の約３倍）。中でも、**IoT機器を狙った攻撃関連通信が多い**。

□　フィッシング対策協議会によると、2023年における**フィッシングの報告件数は100万件超**（2019年の約20倍まで増加）。

<出典：総務省「令和 5 年度版情報通信白書データ集」、(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威2024」解説書、(国研)情報通信研究機構「NICTER観測レポート2023」、フィッシング対策協議会「月次報告書」 等>

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、重要インフラ事業者等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**。
- また、**セキュア・バイ・デザイン**＊1**の概念が国際的に支持**＊2**を集める**など、企業は自社をサイバー攻撃から守ることのみならず、**自社が提供する製品のサイバーセキュリティ対策についても問われる時代に**なりつつある。

＊1 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。
＊2 日米含む13か国の政府機関等が2023年10月にセキュア・バイ・デザイン等の実践に向けた推奨事項をまとめたガイダンスに共同署名。

重要インフラ事業者等に関する制度整備

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）

- 米国の16の「重要インフラ」セクターに対し、①**重大なサイバーセキュリティインシデント**について発生を認知後**72時間以内**、②**ランサム支払い**について支払い後**24時間以内に米CISAに報告すること等を義務付け**。
- 2022年3月に成立、2024年4月に規則案のパブコメ開始。施行は2025年秋を想定。

米国証券取引委員会開示規則（SEC Form 8-K）

- 登録企業に対し、①サイバーセキュリティインシデントに重要性があると判断してから**4営業日以内に、当該インシデントの性質、影響等の開示**、②**リスク管理、戦略、ガバナンスの年次開示等を義務付け**。
- 2023年7月に採択、2023年12月18日より運用開始。

NIS 2指令
（Directive (EU) 2022/2555）

- **2016年NIS指令から対象セクターを拡大**の上、対象「主要エンティティ」、「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**重大なサイバーセキュリティインシデントについて**発生を認知後**24時間以内に早期警告、72時間以内にインシデント通知をCSIRT又は管轄省庁に報告すること等を義務付け**。
- **2023年1月発効、2024年10月18日より執行予定**、それまでに加盟国が国内法に反映予定。

セキュア・バイ・デザインの要請

PSTI法
（Product Security and Telecommunication Infrastructure Act）

- **消費者向けIoT機器の製造者に対し**、デフォルトパスワードを使用しない等の**最低セキュリティ基準への自己適合宣言を義務化**。
- 2022年12月に国王裁可し、下位法制定を経て**2024年4月29日より施行予定**。

サイバーレジリエンス法案
（Cyber Resilience Act）

- **デジタル要素を備えた全ての製品（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**について**認識後24時間以内の早期警告通知**、**72時間以内の通知をCSIRTに報告すること等を義務付け。**
- 2023年11月に暫定合意。**報告義務の運用開始は2025年秋～冬、その他は2027年夏頃運用開始を想定。**

目次

（前提）政府全体における経済産業省のこれまでの施策の位置付け

- 内閣サイバーセキュリティセンター（NISC）による総合調整機能の下、経済産業省は、我が国**産業界へのサイバー攻撃を抑制・防御**し、**事業活動への影響を最小化**するために国が行うべき政策を企画・実行。
- この観点から、経営層の意識改革や、地域・中小企業におけるサイバーセキュリティの推進、サプライチェーン管理のためのガイドライン策定、研究開発の推進、人材育成プログラムの強化等、**産業界に向けた取組を実施**。
- これらの施策の実行を通じ、また、関係省庁による他の取組（我が国の防御力の強化、政府機関における人材活用等）とも合わさって、**政府全体として目指すべき「自由、公正かつ安全なサイバー空間」の確保に貢献。**

サイバーセキュリティ戦略（2021年９月閣議決定）において示された計画期間（３年間）における目標達成のための施策

※赤字（下線箇所は特に）は経済産業省が主体的に関与

＜3つの方向性＞（１）デジタル改革を踏まえたデジタルトランスフォーメーション とサイバーセキュリティの同時推進
（２）公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
（３）安全保障の観点からの取組強化

経済社会の活力の向上及び持続的発展	国民が安全で安心して暮らせるデジタル社会の実現	国際社会の平和・安定及び我が国の安全保障への寄与
１．**経営層の意識改革**	１．**国民・社会を守るためのサイバーセキュリティ環境の提供**	１．**「自由、公正かつ安全なサイバー空間」の確保**
２．**地域・中小企業におけるDX with Cybersecurityの推進**	２．デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保	２．我が国の防御力・抑止力・状況把握力の強化
３．**新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり**	３・４・５．経済社会基盤を支える各主体における取組 ①(政府機関等) ②**(重要インフラ)** ③(大学・教育研究機関等)	３．**国際協力・連携**
４．誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	６．多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用	
	７．大規模サイバー攻撃事態等への対処態勢の強化	

横断的施策

研究開発の推進	人材の確保・育成・活躍促進	全員参加による協働・普及啓発

※内閣サイバーセキュリティセンター「サイバーセキュリティ戦略の概要（令和３年９月28日）」の一部を加工）

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2,000億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

- 経営者向け・産業分野別のガイドライン等の整備
- 中小企業対策ツール（サイバーセキュリティお助け隊、SECURITY ACTION等）の整備
- セキュリティ人材の育成

IPA 産業サイバーセキュリティセンター Industrial Cyber Security Center of Excellence（ICSCoE）

②国際連携を意識した認証・評価制度等の立上げ

- IoTセキュリティ適合性評価制度の検討、国際制度調和に向けた活動
- SBOM（Software Bill of Materials）の活用促進

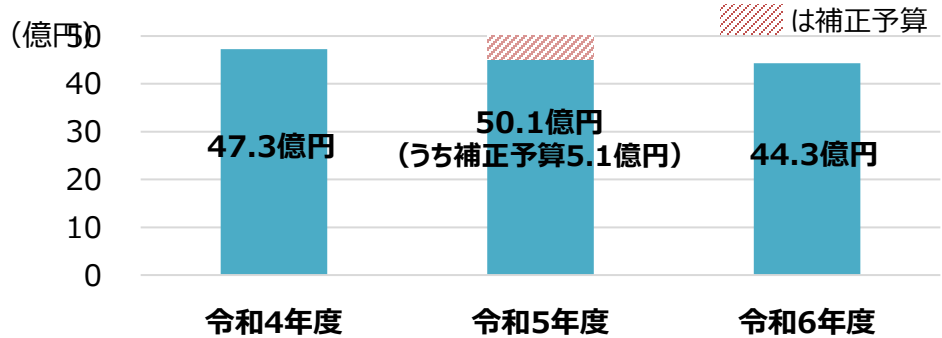
③政府全体でのサイバーセキュリティ対応体制の強化

- JPCERT/CC、J-CRAT、サイバー事故調査を通じた対処支援
- サイバー被害に係る情報共有の促進

④新たな攻撃を防ぎ、守るための研究開発の促進

- 先進的サイバー防御機能・分析能力の強化
- セキュリティ産業の成長加速化

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、**最大320億円規模のプロジェクト**を組成中

② 中小企業生産性革命推進事業

- IT導入補助金において、SECURITY ACTIONを要件化するとともにサイバーセキュリティお助け隊の導入を補助（令和５年度補正予算（**2,000億円**）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に向けたガイドライン等の整備）

- Society5.0下の産業社会におけるセキュリティ対策のフレームワークとして2019年４月に**「サイバー・フィジカル・セキュリティ対策フレームワーク」を策定**。以降、本フレームワークに基づく**各種ガイドライン等を順次整備**。
- サイバーセキュリティお助け隊サービス、ASM（Attack Surface Management）、SBOM（Software Bill of Materials：ソフトウェア部品構成表）の導入促進など、**具体的な対策ツールの普及も進めている**。

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）

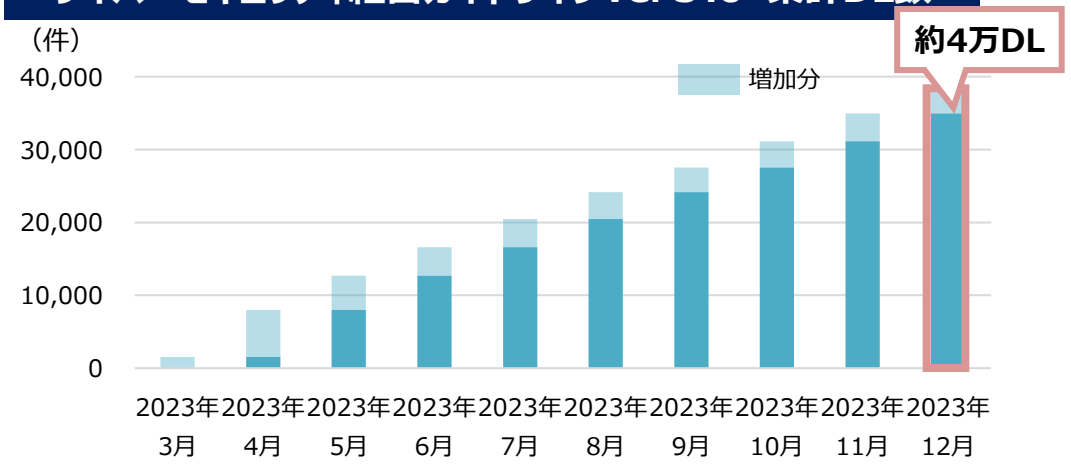
サイバー・フィジカル・セキュリティ対策フレームワーク（2019年4月）

	経営層	実務層（共通）	実務層（産業分野個別）
コンセプト	**サイバーセキュリティ経営ガイドライン**（Ver3.0：2023年3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**（2022年4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）	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２．１版：2023年９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） 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 別冊：2024年４月） 宇宙分野のガイドライン（第２．０版：2024年３月）
具体的対策	**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）	**SBOMの導入に関する手引き**（2023年7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） **お助け隊サービス**（2021年4月～）	

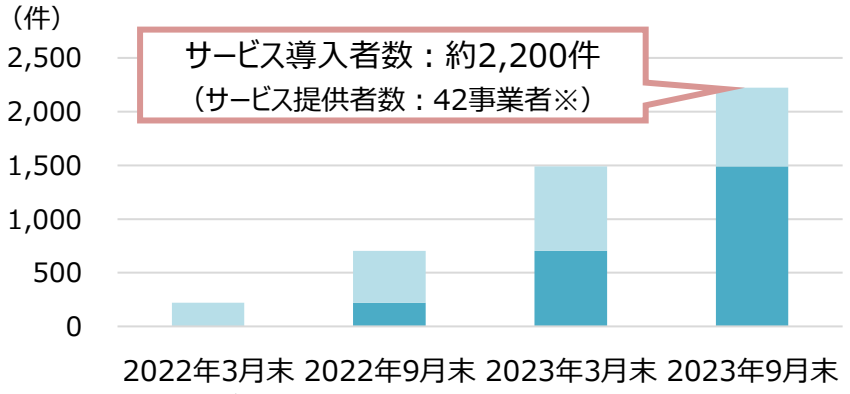
施策の進捗③（ガイドライン・各種施策の活用状況等）

- 「サイバー・フィジカル・セキュリティ対策フレームワーク」に基づくガイドラインは、2023年末時点で、**延べ30万件以上ダウンロード**。昨年3月に改訂した「経営ガイドラインVer3.0」も**毎月継続して一定数ダウンロード**。
- 中小企業等向け施策である「SECURITY ACTION宣言」や「サイバーセキュリティお助け隊」については、IT導入補助金との連携効果もあり、**宣言数・導入実績は増加傾向**。
- IPAを通じた施策などにより、**継続的にサイバーセキュリティ人材を育成**。また、地域でのワークショップ等を通じて**セキュリティ・コミュニティ（地域SECUNITY）の形成を促進**。

サイバーセキュリティ経営ガイドラインVer３.0　累計DL数

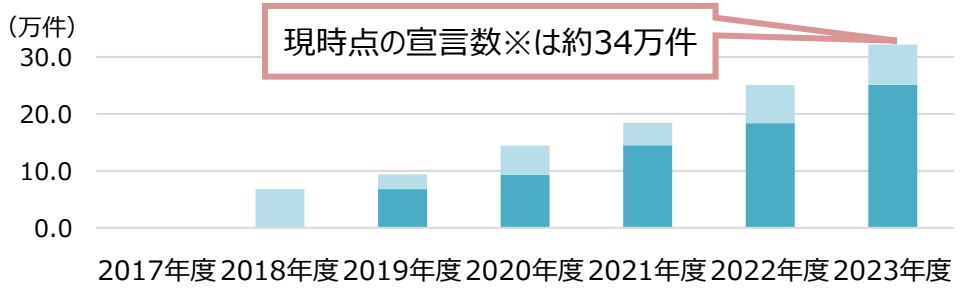


サイバーセキュリティお助け隊導入実績（累計）



※サービス提供者数は2024年3月時点

SECURITY ACTION宣言の実績（累計）



※一つ星、二つ星の いずれかまたはその両方の自己宣言の件数

人材育成及び地域ワークショップの実績

中核人材育成プログラム修了者数	370名(2017年7月～2023年6月)
セキュリティ・キャンプ参加者数	全国大会：1152名(2004年～) ネクストキャンプ：43名(2019年～) ジュニアキャンプ：５名(2023年～)
情報処理安全確保支援士	22,692名(2024年４月時点)
地域SECUNITY形成促進WG ワークショップ開催回数	全国単位で５回、地域単位で２回 (延べ12地域)

施策の進捗④（国際連携を意識した認証・評価制度等の立上げ）

- 欧米諸国を中心に、ソフトウェアの構成情報を詳細に把握することができる**SBOM**（Software Bill of Materials（ソフトウェア部品構成表））**の活用促進**や、**IoT製品に対するセキュリティ対策強化に向けた議論が加速**。
- **我が国でもSBOMの活用を促進**すべく、「SBOMの導入に関する手引き」を策定するとともに、実証による課題検証も実施（今後、実証結果を踏まえて手引きも改訂予定）。日米豪印（クアッド）の枠組みを含め、政府間での定期的な対話も実施中。
- IoT製品のセキュリティ対策強化に向けては、諸外国との制度調和も図りつつ、IoT製品のセキュリティ対策を適切に評価し、適切な対策が講じられているIoT製品が広まる仕組みの検討を実施。その結果を2024年３月15 日に公表。**IoT製品に対するセキュリティ適合性評価制度（以下、「IoTセキュリティ適合性評価制度」）を2024年度中に一部運用開始予定**。

SBOMの普及促進

- SBOMの作成効果やコスト等の課題が存在するため、主にソフトウェアサプライヤー向けに、**導入するメリットや実際に導入するにあたって認識・実施**すべきポイントをまとめた**「SBOMの導入に関する手引き」を2023年7月に公表**。
- **中小企業を含む多くの企業が活用**できるよう、**実証による検証も実施**。
- **日米豪印（クアッド）**において、**関係国でのSBOM活用を促す旨を記載した首脳級の共同原則を2023年5月に公表**。
- **政府間での定期的な対話**も実施しており、引き続き各国との国際調和を図っていく。

IoTセキュリティ適合性評価制度

- 「**IoTセキュリティ適合性評価制度**」を2024年度中に一部運用開始予定。
- 幅広いIoT製品を対象に、製品の特性に応じ、**複数レベル（☆1～☆4）の基準を設定**。

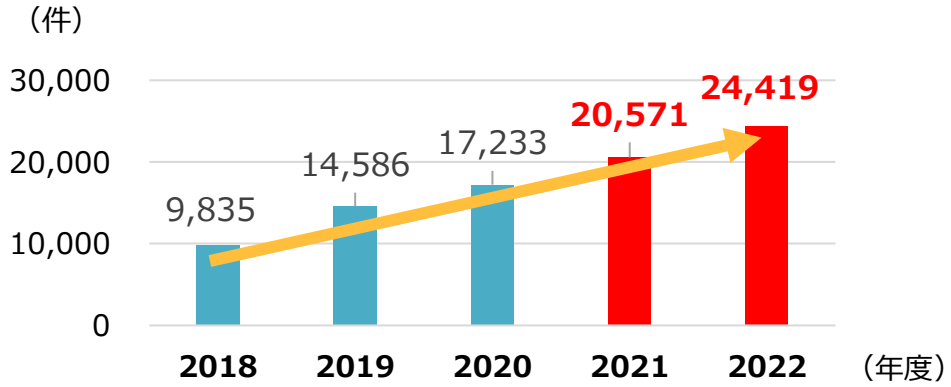
☆１：	2024年半ばに制度開始を予定。
☆2以上：	2025年度下期以降に一部のIoT製品類型に対する制度を開始すべく、検討中

- 今後は、重要インフラ事業者の調達ルールへの適用も念頭に、**政府機関等・地方自治体への**ラベル取得済みIoT製品調達の**必須化等を調整**するとともに、引き続き、**米欧等の諸外国との制度調和**を図っていく。

施策の進捗⑤（政府全体でのサイバーセキュリティ対応体制の強化）

- サイバー攻撃が高度化する中、JPCERT/CCによる**対処調整**や、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**、告示に基づく**脆弱性調整を着実に実施**。
- 攻撃の全容把握や被害拡大防止のために重要な、専門組織を通じた速やかな情報共有を促進すべく、「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（情報共有の促進に向けた検討会）」を実施し、**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等を整理**。

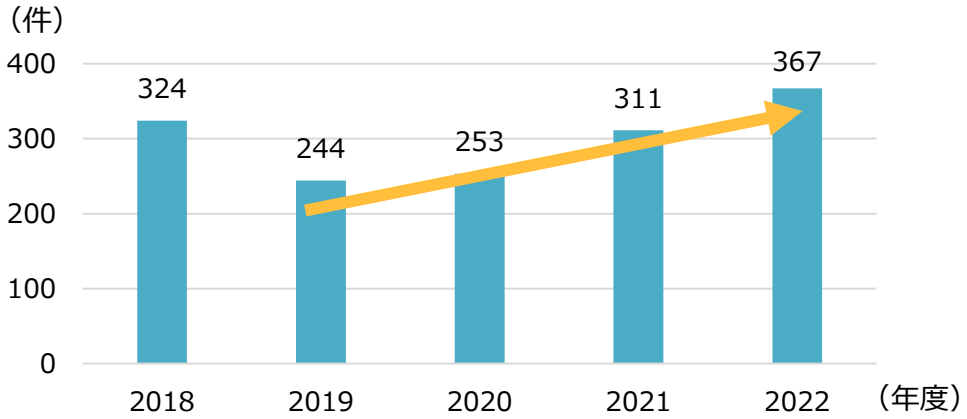
JPCERT/CCによる対処調整件数



J-CRAT活動実績

年度	2019	2020	2021	2022
相談・情報提供数	392	406	375	330
支援数	139	102	94	163
オンサイト支援数	31	20	9	43

ソフトウェア脆弱性届出件数（調整件数）



情報共有の促進に向けた検討会の概要

- 通信先情報やマルウェア情報等の**「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、速やかな情報共有の対象**となり得ると提言。
- 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」を策定**
- **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を提示**。

目次

（前提）政府全体における経済産業省の今後の政策の位置付け

- 国家安全保障戦略（令和４年12月閣議決定）の趣旨を踏まえつつ、サイバーセキュリティ戦略（令和３年９月閣議決定）で掲げた３つの方向性に基づき、**政府全体でサイバー空間における必要な取組を推進**。
- 経済産業省では、**デジタル時代の社会インフラ**（デジタルライフライン）**を守り**、国民生活や経済活動を守るとの観点から、**産業界に向けた政策を企画・実行**する。それにより、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、これらの戦略において掲げられている「**『自由、公正かつ安全なサイバー空間』の確保**」や「**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**」**目標に貢献**していく。
- **これまでの施策の一層の普及・啓発**などに取り組みながら、政府調達等への要件化を通じたサイバーセキュリティ対策の実効性強化など**新たな取組も進める**ことで、**産業界における対策水準の底上げ**につなげていく。

サイバーセキュリティ戦略（2021年９月閣議決定）（抄）

2.1.確保すべきサイバー空間

- **サイバー空間を「自由、公正かつ安全な空間」とすること**により、基本法に掲げた目的に資するべく、国は、（略）サイバーセキュリティ戦略を策定してきた。（略）その確保が危機に直面する中で、「自由、公正かつ安全なサイバー空間」を確保する必要性はこれまで以上に増しているとの認識が深められるべきである。

4. 目的達成のための施策 ～Cybersecurity for All～

- 不確実性を増す環境において「自由、公正、かつ安全なサイバー空間」を確保するため、以下の３つの方向性に基づき、施策を推進する。

(1) デジタル改革を踏まえた**デジタルトランスフォーメーションとサイバーセキュリティの同時推進**

(2) 公共空間化と相互連関・連鎖が進展する**サイバー空間全体を俯瞰した安全・安心の確保**

(3) **安全保障の観点からの取組強化**

国家安全保障戦略（令和４年12月閣議決定）（抄）

- 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**。
- 具体的には、まずは、最新のサイバー脅威に常に対応できるようにするため、政府機関のシステムを常時評価し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築する。その一環として、サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用する。そのことにより、**外交・防衛・情報の分野を始めとする政府機関等のシステムの導入から廃棄までのライフサイクルを通じた防御の強化**、**政府内外の人材の育成・活用の促進等を引き続き図る**。

貢献

経済産業省における今後の政策の方向性

サイバーセキュリティ対策の実効性強化

- ✓ 各種ガイドライン・評価制度の**政府調達等の要件化**
  - → 規模や業種等に応じて適切なセキュリティ対策レベルを評価し**可視化する仕組み**を検討
  - → 一定のセキュリティ基準を満たす**IoT製品を認証する制度**や、ソフトウェア部品構成表（**SBOM**）について、政府調達等の要件化に向けて関係省庁と議論を開始
- ✓ **中小企業向け補助的施策の一層の強化**
  - → セキュリティ人材の活用促進（マッチング実証事業）、お助け隊サービスの拡充　等

サイバーセキュリティ供給力の強化

- ✓ **産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環構築に向けた戦略の検討**
  - → スタートアップ支援策等
- ✓ **高度人材の育成・確保**

官民の状況把握力・対処能力向上

- ✓ IPAをハブとした**サイバー情勢分析能力強化**

新たなサイバーセキュリティ政策の方向性

- サプライチェーン全体での対策強化に向け、これまでソフトロー・アプローチとして、経営層の意識改革の促進、各種のフレームワーク・ガイドライン等の策定を実施。今後、関係省庁と連携し、**政府調達等への要件化を通じ、その実効性を強化**する。　※十分なリソースの確保が困難な中小企業等に対しては、支援策を一層強化。
- こうした需要側への働きかけと同時に、**国産製品の開発・普及促進や高度人材の育成・確保**といったセキュリティの供給側への働きかけを通じて、我が国におけるセキュリティ市場の拡大を図ることが重要。
- また、サイバー安全保障の実現に向けて、産業界との接点を活かしつつ、**官民のサイバー状況把握力・対処能力向上に向けた取組**を進める。

サイバーセキュリティ対策の実効性強化

＜これまでの取組：フレームワーク・ガイドライン等の整備＞

サイバー・フィジカル・セキュリティ対策フレームワーク

- 経営ガイドライン
- 工場ガイドライン
- ●●ガイド・・・etc

政府調達に関する基準／民間企業における調達要件
（政府機関等のサイバーセキュリティ対策のための統一基準群等）

＜今後目指すべき取組：調達要件化等を通じた実効性の強化＞

IPA

策定・連携

サイバー・フィジカル・セキュリティ対策フレームワーク

- 経営ガイドライン
- 工場ガイドライン
- ●●ガイド・・・etc

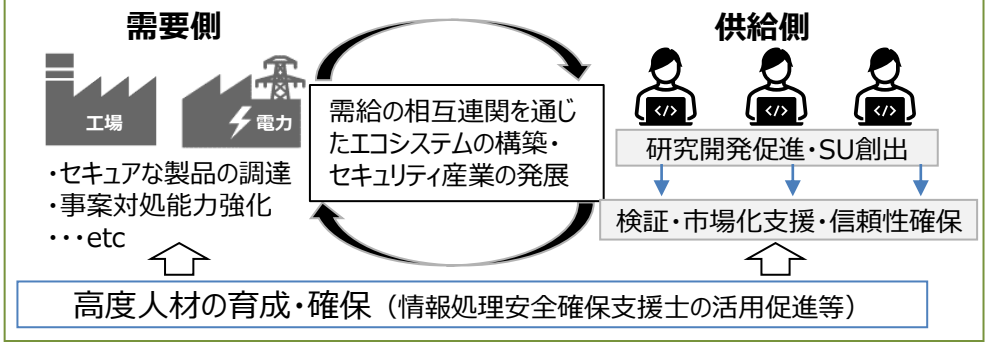
政府調達に関する基準／民間企業における調達要件
（政府機関等のサイバーセキュリティ対策のための統一基準群等）

認証製品の調達要件化等の連携（例：IoTセキュリティ適合性評価制度）

認証基準策定

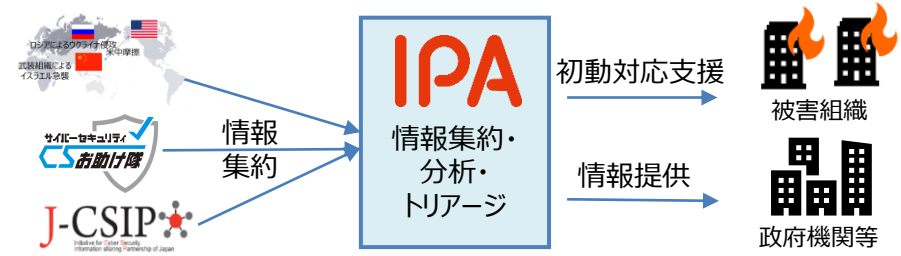
認証制度（新設）

セキュリティ市場の拡大に向けたエコシステムの構築



サイバー情勢分析能力の強化

官民の情報ハブとしてのIPAの強みを活かし、地政学等の情勢と産業界（エンドポイント）から得られるサイバー攻撃情報の集約・分析を一層推進。攻撃者の意図を把握し、攻撃の対象や手法を予見して効果的な防御策を講じる。



サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討

実効性強化

- これまで「サイバーセキュリティ経営ガイドライン」や産業分野別のガイドライン等を整備し、各企業等による積極的な取組を推進してきたところ。他方、**異なる取引先から様々な対策水準を要求される**といった課題や、**外部から各企業等の対策状況を判断することが難しい**といった課題は依然として存在。
- 今後は、諸外国で議論が進んでいる、「サイバー対策」のレーティング等も参考にしつつ、**各企業等の業種・規模などのサプライチェーンの実態を踏まえた満たすべき各企業の対策のメルクマール**や、**業界間の互換性を確保しながら**その**対策状況を可視化する仕組みを検討していく。**
- 併せて、関係省庁とも連携し**政府機関・企業による活用を促す枠組みと紐付ける**ことで、**その実効性を強化**していく。

想定される検討事項

- **既存のガイドライン等をIPAが一元的に管理・体系化し、企業のセキュリティ対策基準を明確化できないか**
- 既存ガイドライン等と整合を取りつつ、**業種横断的なセキュリティ対策レベルを評価（自己評価、第三者認証）できないか**
- 政府機関等における**調達要件**や、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**を促進し、**実効性の強化**につなげられないか

※サイバーセキュリティへの取組に関し、投資家を含むステークホルダと企業経営者との対話（開示）の在り方等についても検討が必要ではないか。

対策レベルの可視化（イメージ）

成熟度の定義	三つ星（★３）	四つ星（★４）	五つ星（★５）
レベル感の説明	サプライチェーン形成企業として最低限満たすべき基準	サプライチェーン形成企業として標準的に満たすべき基準	重要インフラ事業者、経済安全保障上、特に重要なインフラ事業者、関連サプライヤーが満たすべき基準
ガイドラインの相当性を認定	・IPA「中小企業の情報セキュリティ対策ガイドライン」	・○○業界ガイドライン ・・・・	・重要インフラ行動計画 ・・・・
ガイドライン準拠を確認する方法を定義	自己宣言型	第三者認証型	第三者認証型

政府調達・補助施策等への要件化

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

ガイドライン等の実効性の強化

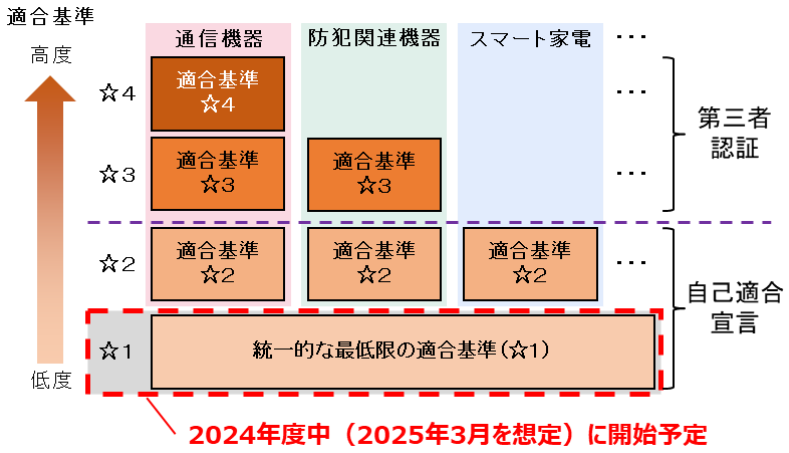
（セキュアなIoT製品及びソフトウェアの流通に向けた取組等）

実効性強化

- セキュリティ対策レベルを評価し、それを可視化する取組の**先行例として、IoTセキュリティ適合性評価制度を検討中**。**米欧等の諸外国との制度調和を図るための議論も継続中**。
- また、**SBOM（ソフトウェア部品構成表）**導入時の課題検証のための実証や企業向けの手引書を策定。
- IoTセキュリティ適合性評価制度の実効性強化やSBOMの導入促進に向けては、**産業界との連携のほか、政府調達等の要件化等に向けて関係省庁と議論も開始**。
- さらに、米国が策定し、我が国政府も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、**ソフトウェア開発者が行うべき取組整理**や**安全なソフトウェアの自己適合宣言の仕組みの検討**を行っていく。

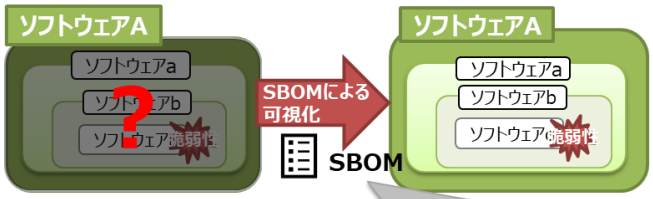
IoTセキュリティ適合性評価制度

- 幅広い**IoT製品を対象**として、一定のセキュリティ基準を満たすものを認証し、ラベルを付与する制度の整備に向けて、検討を実施。その結果を2024年３月に取りまとめ、**2024年度中に一部運用を開始**予定。



SBOMのイメージ

- **SBOM（ソフトウェア部品構成表）**がソフトウェアのセキュリティの脆弱性を管理する手法の一つとして着目。



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	……	…

セキュアバイデザイン・セキュアバイデフォルト

- **セキュア・バイ・デザイン**：IT製品（ソフトウェア等）が、設計段階から安全性を確保されていること。
- **セキュア・バイ・デフォルト**：ユーザーが、追加の手間をかけることなく、購入後すぐにIT製品（ソフトウェア等）を安全に利用できること。

（出典：国際共同ガイダンス「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」）（2023年10月28日署名）

半導体関連産業におけるセキュリティの確保に向けた検討の開始

実効性強化

- 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、**安定的な供給を確保する観点からも、サイバーセキュリティ対策を進めることが重要**。
- 経済産業省においても、**「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を整備**。当該ガイドラインの浸透を進めつつ、**半導体関連産業におけるセキュリティの確保に関して必要な政策を模索するため実態把握・調査等を進めていく**。また、**サイバーセキュリティ対策への取組、問題意識や事例、防御に資する脅威情報を相互にを共有できる場を設置**する。
- こうした議論の中で、**半導体関連産業において求められるセキュリティ対策を具体化**していくとともに、その内容を**経済産業省の投資促進関係施策の要件等とも紐付けること等**を検討し、**その実効性を強化**していく。

半導体セキュリティの直近の動向

海外の動向

- TSMCは、2018年に主力工場がランサムウェアの被害に遭い生産停止を余儀なくされ、影響額は最大190億円に及んだ。
- 2023年に半導体装置のセキュリティ規格であるSEMI E187を調達要件化。SEMI E187の要件を満たしていることを、認証機関によって証明されたサプライヤーも出現。

（出典）日本経済新聞、TSMC社プレスリリース

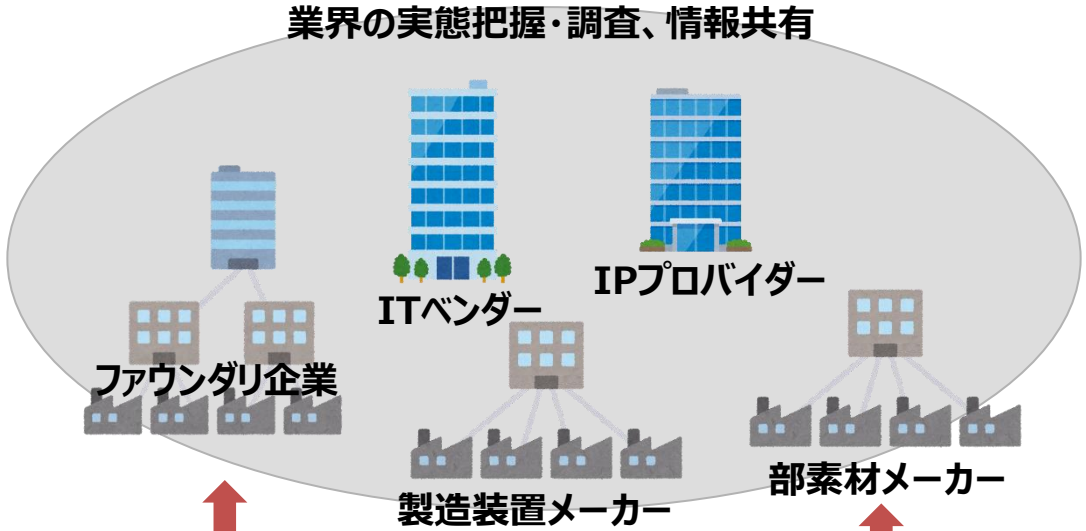
国内の動向

- 半導体向けの研磨材を扱うフジミインコーポレーテッドは、サーバへの不正アクセスがあったことから公式Webサイトを含む社内システムを全面停止し、一部製品の生産と出荷を見合わせた。
- シリコンウェハを扱うグローバルウェーハズ・ジャパンは、社内サーバーに不正アクセスを受けたことから、ネットワークから社内システムを切り離す措置を実施し、シリコンウェハの製造および出荷が不能となった。

（出典）フジミインコーポレーテッド社プレスリリース、グローバルウェーハズ・ジャパン社プレスリリース

国内の安定供給確保のためサイバーセキュリティ対策を進めていく

半導体関連産業全体でのセキュリティ水準の底上げ



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

自ら工場のセキュリティ対策を立案・実行し、工場のセキュリティ水準の底上げを図るための、参照すべき考え方やステップを示した手引き

サプライチェーン全体での対策強化（中小企業等向けの支援の一層強化）

実効性強化

- サプライチェーン全体のセキュリティ対策を更に強化するためには、中小企業の**中堅レベルにおいては事業継続に耐えうるレジリエンスを確保、小規模レベルにおいては経営層が最低限の危機管理の認識を持つ水準**のセキュリティの確保が必須。
- 一方で、セキュリティへの対策も含め、**十分なリソースの確保が困難であるとの課題**も存在するところ、こうした中小企業等に対しては、中小企業の実態も踏まえた**適切なセキュリティ対策のあり方を提示**しつつ、**支援策を一層強化**していく。

中小企業等における課題

- IPAの調査（2021年度）によれば、中小企業のうち、合計で**４割が「どこからどう始めたらよいかわからない」「コストがかかり過ぎる」と回答。**セキュリティ対策を効果的に実践できていない状況。
- また、セキュリティに支出可能な金額は**月額３万円未満と回答する企業が４割超**。セキュリティ人材についても、多くの企業において不足している状況。

出典：2021年度中小企業における情報セキュリティ対策に関する実態調査、令和３年度中小企業サイバーセキュリティ対策促進事業　（北海道におけるサイバーセキュリティコミュニティ強化に向けた調査）

- サプライチェーン単位での攻撃が増加する中、必要十分なセキュリティ対策を実施できない企業が狙われることで大きな経済的損失をもたらすおそれがある。
- こうした状況の打開に向けて、予算や人材が不足している中小企業が、**それぞれの規模や業種、事業上の事情等に照らして自らに最も効果的なセキュリティ対策の水準を把握**し、それを**実践できる環境を整備**していくことが必要。

中小企業等向け支援施策

- 中小企業等において効果的なセキュリティ対策を実践できるよう、**規模等に応じたセキュリティ対策を提示するとともに、対策の実践に当たって必要となるセキュリティ人材の確保やサービスの支援策を強化**。

規模等に応じたセキュリティ対策の提示

➢ 中小企業等のIT資産の内容等、実態調査も行い、**企業規模やIT資産の内容等に応じて、ガイドラインとも紐付けながら、費用対効果のある方法等の提示**を図る。

セキュリティ人材の活用促進

➢ **中小企業等とセキュリティ人材とのマッチングを促す場を構築する実証を実施**し、セキュリティ人材のシェアリング促進等、中小企業が行う人材探索を支援する。

「サイバーセキュリティお助け隊サービス」の拡充

➢ **新たな類型（２類）を創設し**、中規模以上の中小企業が求める高度なサービスに対応。さらに**2類サービス事業者とIPA間で重大サイバー攻撃に関する情報共有を活性化し、効果的に中小企業のサイバー攻撃被害防止を行う体制を作る。**

- このほか、中小企業等の身近な相談先である**地場ベンダの能力強化**に向けた施策や、金融機関など**DX支援機関を通じた面的支援**の促進なども展開。

これらの施策について、各地域においてワークショップやセミナー等も開催しながら、産業界や地域SECUNITYとも連携した施策の展開・普及を実施し、産業界のサプライチェーンセキュリティ全体の向上を図る。

我が国サイバーセキュリティ産業の振興に向けた強化策の検討

供給力強化

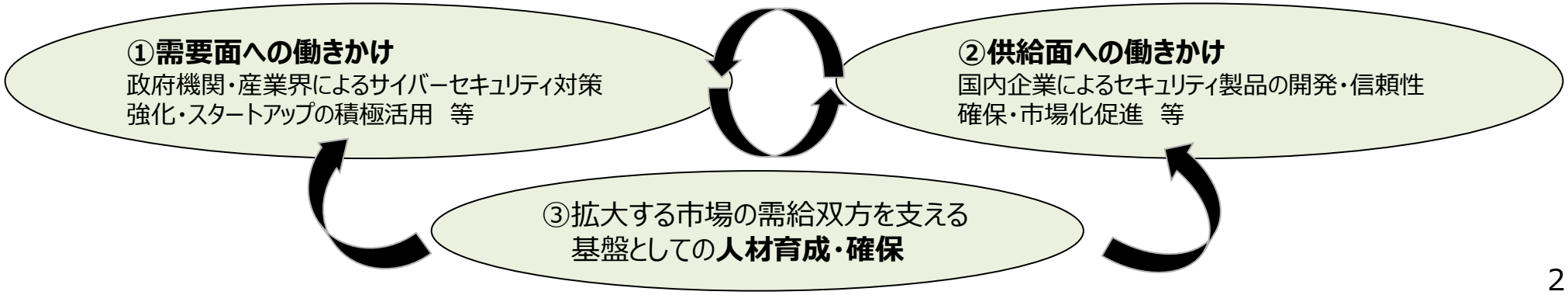
問題意識

- 我が国の**サイバーセキュリティは必要な技術や製品の多くを海外に依存をしている状況。**
- 現状のままでは、我が国ユーザー企業のデータが国内に蓄積されず、当該データを活用してより品質の高い製品・サービスを提供することが我が国セキュリティ企業において一層困難になるとの**負のスパイラルが生じる**こととなる。また、安全保障環境が厳しさを増す中、我が国ユーザー企業にとって重要なデータのセキュリティを**過度に諸外国の製品・技術に依存することにより、我が国の自立性が危ぶまれるリスク**も生じる。
- 今後重要度がますます増してくるサイバーセキュリティ関連市場において、我が国のセキュリティ企業が相対的に**強みを発揮できる領域**や、我が国のセキュリティ企業が**抑えるべき領域**を、しっかり確保していけるよう、**サプライサイドを強化**することが、①経済安全保障の観点からも、②産業政策の観点からも重要。また、そのような能力を確保することにより、同盟国・同志国との強固な連携も可能となる。

目指すべき姿

- 海外主要国では、政府や企業の需要を背景にしつつセキュリティ企業は積極的に製品開発・販路拡大を行い、スケールアップ。我が国でも、こうした構造を参考として、**需要と供給のエコシステムの構築**により、**「セキュリティエコノミー」の確立**と**主要国と同等以上のサイバーセキュリティ能力の確保**を目指す。
- もっとも、品質の高い外資製品の利用を妨げるものではなく、必要な海外連携は実施しつつも、サイバーセキュリティ市場が拡大する中で、我が国にとって重要な領域を中心に、**「高品質」な国産セキュリティ製品・サービスの供給が強化される状況**を目指す。これにより、「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」政府全体の目標にも貢献。

<「セキュリティエコノミー」好循環のイメージ>



（参考）我が国サイバーセキュリティ産業の振興に向けた強化策の検討に係る論点例

供給力強化

- 「目指すべき姿」の解像度をどのように高めるか。
  - 我が国における「サイバーセキュリティ産業」はどのように構造化されるのか。市場参加者としてどのような主体があり、それぞれの収益構造はどのように構造化されるのか。
  - その中で、経済安全保障及び産業政策の観点から、我が国セキュリティ企業が抑えるべき「領域」とはどの部分か（一気にシェアを拡大できる・すべき領域、時間をかけてシェアの拡大を狙うべき領域、現状のシェアを維持しつつ市場拡大の果実を取りに行くべき領域　等）。
  - 「目指すべき姿」の実現までの時間軸をどのように設定するのか。As isの場合、X年後の世界・我が国サイバーセキュリティ産業の姿はどのような状態になっているか。
  - 我が国セキュリティ産業の「振興」とはどのような状態をいうか。定量的な目標としてどのように表現することが可能か（例：「市場規模」は適当な指標と言えるのか）。　等
- 「目指すべき姿」をどのように実現できるか。
  - これまでのセキュリティ産業振興を目的とした政府の各種施策をどのように評価するか。
  - 米国やイスラエル等において多くのセキュリティ・スタートアップがスケールアップしている実態をどのように評価するか。我が国において同じモデルを取り入れることが可能なのか。我が国の特殊性があるとして、それを考慮した異なるモデルとしてどのような方策があり得るか。
  - 我が国においてスタートアップ製品がより活用・調達されるためには、需要面への働きかけとしてどのような仕掛けが必要か。さらに、そのためにどのような人材育成・確保施策が必要か。
  - 「需要側」は全産業を表象するところ、サイバーセキュリティ産業の振興をもたらす要素を特定するために、どのように細分化して分析するべきか。
  - グローバルなエコシステムに我が国セキュリティ企業が食い込んでいくためには、何が必要か。世界市場を目指すとの発想は、「目指すべき姿」の実現に当たって必要な要素か。　等

今後検討を深め、今年度中に、我が国サイバーセキュリティ産業の振興に向けた強化策のパッケージを提示

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

供給力強化

- 深刻化するサイバー攻撃に対して、サイバー防御機能や分析能力の強化につながる技術を確保することが重要。
- 経済安全保障重要技術育成プログラムにおいて、経済安全保障の確保・強化の観点から、「サイバー空間」を支援すべき重要技術とし、**サイバー空間の状況把握力や防御力の向上に資する技術**や、**セキュアなデータ流通を支える暗号関連技術**等の研究開発を実施予定（320億円を超えない範囲／5年）。
- 2023年10月に具体的な研究開発の構想を決定。これに基づき、同年12月に公募を開始し、外部有識者による審査等も踏まえた上で、実施事業者を採択。**本年5月頃から研究開発を開始予定**。

目　的

- サイバー空間において提供される多様なサービスが複雑化するに伴い、サイバー空間内やサイバーとフィジカルの垣根を超えた主体間の「相互連関・連鎖性」が一層深化。近年では、**人工知能（AI）**を活用した攻撃に代表される**新たなサイバー攻撃のリスク**や、**量子計算機の活用**の広がりに伴う**既存暗号の危殆化によりデータが漏洩するリスク**が顕在化。
- **サイバー空間の状況把握力や防御力の向上に資する技術**や、**セキュアなデータ流通を支える暗号関連技術**等を開発し、我が国のサイバー領域における状況把握力・防御力を飛躍的に向上させることを目的とする。

実施内容

（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

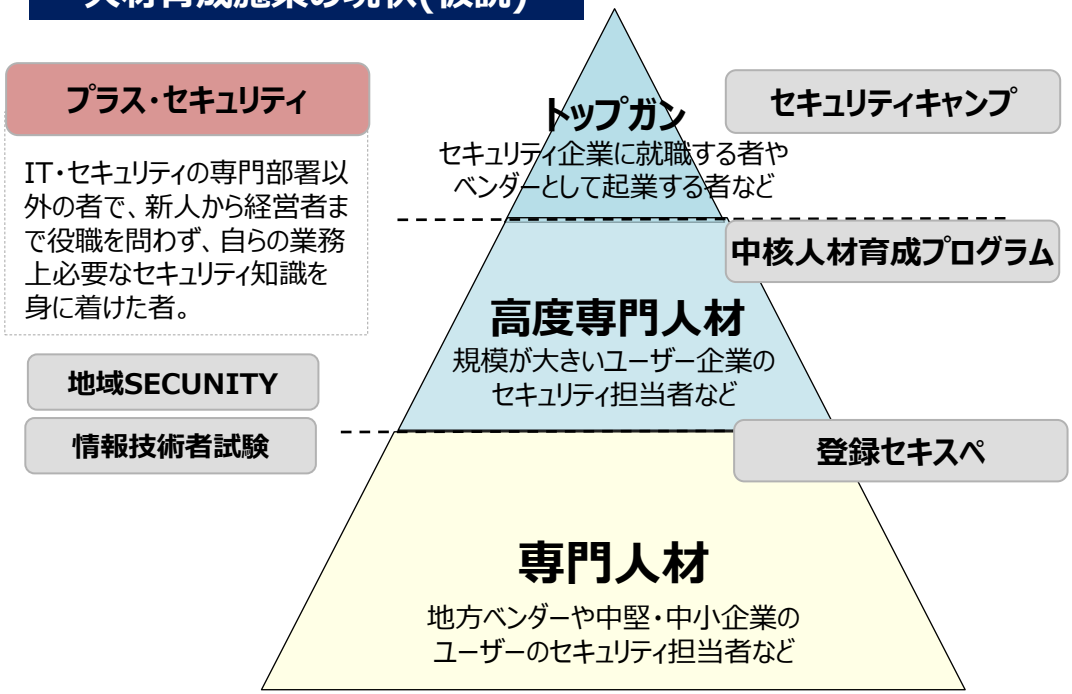
- Y-00のデジタルコヒーレントの開発／Y-00の高速光ファイバ通信の開発／Y-00の高速光ワイヤレス通信の開発

サイバーセキュリティ人材の育成・確保に向けた取組の方向性

供給力強化

- セキュリティ市場の拡大に向けたエコシステムを構築するためには、産業・技術基盤の維持・発展を支える供給側、セキュリティ対策を実装する需要側、**双方の基盤となる人材の育成・確保が重要**。
- しかし、NRIセキュアの調査（※1）によると、日本においては、従業員規模に関わらず**９割の企業でセキュリティ人材が不足していると回答**。またISC2の調査（※２）によると国内のサイバーセキュリティ人材は現在約48万人存在しているが、**11万人不足**。
- セキュリティ人材施策として、セキュリティキャンプや中核人材育成PG、情報処理安全確保支援士試験を通じた**高度専門人材の育成**、地域SECUNITY活動等を通じた**プラス・セキュリティの普及**等を進めてきているが、**需給ギャップを解消するためには、セキュリティ人材の裾野を更に拡大するための施策の検討が必要**。
- また、 NISC改組後の「新たな組織」を含む**政府機関等において十分なセキュリティ人材を確保する**ことにより、政府全体でのサイバー安全保障分野での対応能力を向上につなげることも重要。こうしたセキュリティ人材が、産業界に留まることなく、**政府と民間との間でより活発に行き来できるようにする**ことも必要ではないか。

人材育成施策の現状(仮説)



現状の課題

- これまで、トップガンや高度専門人材の育成は進めてきたものの、1年間に育成できる人数が限定的。
- 登録セキスペは、首都圏のベンダー側に偏っており、ユーザー企業での活用が進んでいない。
- これまで施策では、地方ベンダーや中堅・中小企業のユーザーのセキュリティ担当者などにアプローチできない。

今後の方向性

- トップガンの発掘・育成及び事業化促進に向けてセキュリティキャンプの拡張及び未踏事業との連携を検討。
- ユーザー企業における登録セキスペの活用を促進（中小企業等とのマッチング実証事業、DX促進施策との連動等）するとともに、制度の見直しも検討。これらを通じて、**登録人数**（2024年４月現在、約2.3万人）**を2030年までに５万人まで増加を目指す**。
- 専門人材の育成に関する課題整理を行うとともに、基礎知識・スキル習得できるような環境整備に関する検討を実施。

※1　NRI Secure Insight 2023
※2　ISC2 Cybersecurity Workforce Study 2023

IPAにおけるサイバー情勢集約・分析能力の強化

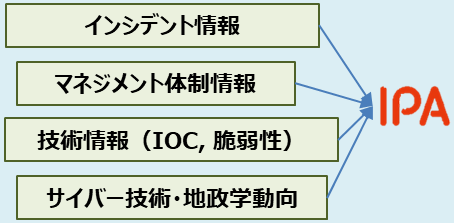
官民対処

- 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。今後は、産業界（エンドポイント）を通じて得られる**サイバー攻撃情報の集約・分析機能を強化**し、J-CRATを中心に**IPAの対応支援機能を強化**。

ＩＰＡにおけるサイバー情勢の集約・分析機能の強化

１．情報収集・検知力の向上

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。



２．統合的な分析・脅威評価機能の強化

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。

３．情報共有／ 対応支援機能の強化

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。

活動イメージ）

- 政府機関や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**
- 主要産業に対する経済産業省関連**中小企業支援策の普及展開**、IPAによるリスクアセスメント支援等を通じたセキュリティ体制構築支援
- 攻撃の背景となる地政学動向等を踏まえた**サイバー脅威評価の共有**や、主要産業に対する**重大なサイバー攻撃関連情報の共有・注意喚起**　等

今後の産業サイバーセキュリティ研究会ＷＧの位置付け

- 本研究会の下部会合であるＷＧでは、各WGに設定されたテーマの範囲で、産業界におけるサイバーセキュリティの確保に向けた政策対応の在り方について議論してきたところ。
- 今回提示した新たな政策の方向性に伴って、**テーマ設定の見直しも含め、WGを再編する**ことにより、効果的に政策検討・施策の効果検証等を進めていくための枠組みを改めて整備したい。

＜これまで＞

産業サイバーセキュリティ研究会

- 産業界におけるサイバーセキュリティの確保に向けた政策の在り方について大所高所から議論

ＷＧ１
（制度・技術・標準化）

ＷＧ２
（経営・人材・国際）

ＷＧ３
(サイバーセキュリティビジネス化)

- 各テーマに沿った政策課題に対応するための具体的施策の検討
- 個別施策の進捗確認・評価

＜今後（イメージ）＞

産業サイバーセキュリティ研究会

- 産業界におけるサイバーセキュリティの確保に向けた政策の在り方について大所高所から議論
- 政策を通じた成果の確認・評価

新ＷＧ１
・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

新ＷＧ２
・地域・中小企業等における対策支援

新ＷＧ３
・セキュリティ産業振興、研究開発
・人材育成・確保

※「官民の対処能力向上」の取扱いについては今後検討。
※現ＷＧ１下のSWGやTFは原則維持する方向で検討。

- 各テーマに沿った政策課題に対応するための具体的施策の検討
- 個別施策の進捗確認・評価

目次

産業界へのメッセージ（令和６年４月５日）（全体像）

- 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。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。また、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おり、**我が国においても一層の対策強化が求められる状況**。
- 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、**これまでの施策の一層の普及・啓発などに取り組みながら**、政府調達等への要件化を通じたサイバーセキュリティ対策の実効性強化や、サイバーセキュリティ供給力の強化、官民の状況把握力・対処能力向上に向けた**新たな取組も進める**。今後も産業界からの御意見を聴くなど、官民の協力関係を維持・発展させつつ、**不断に取組を見直していく**。
- 各企業・団体においては、こうした状況も踏まえ、**各種ガイドラインや随時の「注意喚起」に沿った対応を前提**として、組織幹部のリーダーシップの下、必要な人材の育成や確保・体制の構築を進めながら、以下の対応をお願いしたい。

  ①　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（ＤＸ、ＢＣＰ、サステナビリティ等に紐付ける。）。その上で、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**。

  ②　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）**の製品の購入を優先**するなど、**ＩＴサービス等提供事業者に対してセキュリティ慣行を求める**。併せて、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体制を整備する**。

  ※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。

  ③　**サプライチェーン全体での対策強化に向けた意識を徹底**する（ASM（Attack Surface Management）等外部サービスの活用や、サプライチェーンに参加する中小企業等への共助（取引先からの要請対応への負担配慮や脆弱性診断などの支援等））。**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」などの支援パッケージの活用**も検討する。

  ④　「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。

- ＩＴサービス等提供事業者においては、**自らの製品・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」や「セキュア・バイ・デフォルト」の考え方に沿った一層の対応**（「顧客だけにセキュリティの責任を負わせない」、「トップ主導での実施」等の基本原則の遵守、SBOMの採用、メモリに安全なプログラミング言語の採用等）をお願いしたい。
- セキュリティベンダや調査ベンダ、情報共有活動のハブ組織等のサイバー被害組織を直接支援する専門組織においては、「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」に沿って、**専門組織間で必要な情報を共有することの意義等について被害組織と共通の認識を醸成する**努力をお願いしたい。

（参考）産業界へのメッセージに対応した政府文書・窓口等

- 各企業・団体向け

①関係

- 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）
- 経済産業省「デジタル・ガバナンス・コード2.0」（令和４年９月改訂）
- 経済産業省「価値共創ガイダンス2.0」（令和４年８月改訂）

②関係

- 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「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」に署名しました」（令和５年10月）

③関係

- 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「『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）
- 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「中小企業のサイバーセキュリティ」
- IPA「サイバーセキュリティお助け隊サービス制度」

④関係

- 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「情報セキュリティ安心相談窓口」「コンピュータウイルス・不正アクセスに関する届出」「J-CRAT 標的型サイバー攻撃特別相談窓口」
- JPCERT/CC「インシデント対応依頼」

- ＩＴサービス等提供事業者向け
  - 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「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」に署名しました」（令和５年10月）
- サイバー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）

産業界へのメッセージ（１）（背景）

- サイバーリスクの高まりや米欧等の動向を背景に、**我が国においても一層の対策強化が求められる状況**。
- 経済産業省では、**これまでの施策の一層の普及・啓発**や**新たな取組**を進め、**不断にその見直し**もしていく。
- 他方で、**産業界における積極的な取組も不可欠**。そのため、次頁以降で、**各主体に向けたメッセージを提示**。

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	→	こうしたデジタル技術の取扱いに当たっては、サイバーセキュリティの確保は必須。
世界的な地政学リスクの高まり	→	特定の国や地域における地政学的な問題が、企業活動上のリスクとなりつつある。危機管理対応の中でサイバーセキュリティ上のリスクも考慮した対応が求められる。（※１）
サイバー攻撃の深刻化・巧妙化（※２）	→	サイバー攻撃による事業の停止や情報の漏えい等、企業の信用を毀損する事例が多発。企業経営を行う上でこうしたサイバー攻撃の高度化への対応は必須。
米欧等での制度整備活発化	→	グローバルに活動する企業や海外企業と取引する企業にとっても、こうした制度整備への対応が必要。

（※１）経済安全保障推進法に基づく基幹インフラの安定的な提供の確保に関する制度が令和６年５月17日より運用開始。特定重要設備の導入時等にサイバーセキュリティの観点を含む国の事前審査が特定社会基盤事業者に対し義務付け。

（※２）「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、…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。」（国家安全保障戦略（令和４年12月16日閣議決定））

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。**我が国においても一層の対策強化が求められる状況**。

経済産業省としての取組

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、**これまでの施策の一層の普及・啓発に取り組みながら**、①政府調達等への要件化を通じたサイバーセキュリティ対策の実効性強化や、②サイバーセキュリティ供給力の強化、③官民の状況把握力・対処能力向上、それぞれに向けた**新たな取組も進める**。今後も産業界からの御意見を聴くなど、官民の協力関係を維持・発展させつつ、**不断に取組を見直していく**。

産業界における積極的な取組

組織幹部によるリーダーシップの下、**必要な人材の育成や確保・体制の構築**も進めながら、当省のサイバーセキュリティ政策の方向性に沿った**積極的な取組を行っていただくことも不可欠**。

次頁以降で、**それぞれの主体**（※）**に向けたメッセージを提示**。

（※）
- 各企業・団体
- ＩＴサービス等提供事業者（機器やサービス等を提供する事業者）
- サイバー被害組織を直接支援する専門組織（セキュリティベンダや調査ベンダ、情報共有活動のハブ組織等）

産業界へのメッセージ（２）（各企業・団体向け①）

- 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（ＤＸ、ＢＣＰ、サステナビリティ等に紐付ける。）、その上で、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**ことをお願いしたい。

趣旨・背景

- 米国においてサイバーセキュリティに関するリスク管理や戦略、ガバナンスに係る年次開示等が義務付けられ、また、我が国においても企業のサステナビリティ情報開示が義務化されるなど、**企業におけるサイバーセキュリティに関する取組が、（企業価値に結び付くものとして）資本市場により評価される時代**となってきている。
- すなわち、企業においては、**サイバーセキュリティ対策を、中長期的な企業価値向上に向けた「投資」として捉え、利害関係者に対して積極的に開示すること等が、一層求められる状況**となる。
- 経済産業省が2023年３月に改訂した「サイバーセキュリティ経営ガイドライン」においても、**サイバーセキュリティ対策を「投資」**（将来の事業活動・成長に必須な費用）**と位置付けることの重要性について言及**しており、サイバーセキュリティ経営の重要項目の一つとして、「サイバーセキュリティに関する情報の収集、共有及び開示の促進」を掲げているところ。本文書で示した考え方は、各企業等にとって一つの参照点となり得る。
- 今後、経済産業省としては、**外部から各企業等の対策状況を判断することが難しい**といった課題等に対応するため、関係省庁とも連携しながら、各企業等の業種・規模などのサプライチェーンの実態を踏まえた満たすべき対策のメルクマールや、業界間の互換性を確保しながらその**対策状況を可視化する仕組みを検討していく**。

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　Ver3.0」（令和５年３月改訂）
- 経済産業省「デジタル・ガバナンス・コード2.0」（令和４年９月改訂）
- 経済産業省「価値共創ガイダンス2.0」（令和４年８月改訂）

産業界へのメッセージ（３）（各企業・団体向け②）

- 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）**の製品の購入を優先する**など、**ＩＴサービス等提供事業者に対してセキュリティ慣行を求める**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。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。

- 併せて、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体制を整備する**ことをお願いしたい。

趣旨・背景

- 「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4月に米国サイバーセキュリティー・インフラセキュリティー庁（CISA）が一部有志国と共に**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を作成**し、**ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置を講じるよう**促した。同年10月に本文書が改訂され、我が国を含む13か国が共同署名。**当該文書には、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**。

- 今後、経済産業省としても、本文書も踏まえ、**ソフトウェア開発者が行うべき取組整理など推進のための取組を検討**していく予定。その中で、**ユーザ組織（顧客）が行うべき取組も提言する**ことで、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。

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「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」に署名しました」（令和５年10月）

産業界へのメッセージ（４）（各企業・団体向け③）

- **サプライチェーン全体での対策強化に向けた意識を徹底**すること（ ASM（※）等外部サービスの活用や、サプライチェーンに参加する中小企業等への共助（取引先からの要請対応への負担配慮や脆弱性診断などの支援等））をお願いしたい。 ※ 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。
- **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」などの支援パッケージの活用**も検討することをお願いしたい。

趣旨・背景

- サイバーセキュリティ対策不足の企業がサプライチェーン上に存在することは、大きなリスク。サプライチェーン全体での対策を更に強化するためには、資金的な余力の観点等から大企業と同じような対策を講じることが難しい**地域の中小企業等における**一定水準以上の**セキュリティの確保が必須**。
- こうした観点から、経済産業省と公正取引委員会は、 2022年10月に、中小企業等におけるサイバーセキュリティ対策を支援するための施策と、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、整理を実施。**こうした整理も参照しつつ、サプライチェーンに参加する中小企業等への共助を実践することが重要**。
- また、経済産業省が2023年３月に改訂した「サイバーセキュリティ経営ガイドライン」において、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。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、こうした**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）こと も有用。
- さらに、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**、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**とされており、これを実施することも、サプライチェーン全体での対策を強化する上で効果的と考えられる。
- 今後、経済産業省としては、中小企業等に対して、実態も踏まえた**適切なセキュリティ対策のあり方を提示**しつつ、**「サイバーセキュリティお助け隊サービス」の拡充**をはじめ、**支援策を一層強化**していく。

関係する政府文書・窓口等

- 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「『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）
- 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「中小企業のサイバーセキュリティ」
- IPA「サイバーセキュリティお助け隊サービス制度」

産業界へのメッセージ（５）（各企業・団体向け④）

- 「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**等を行うことをお願いしたい。

趣旨・背景

- 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**。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**。
- 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では、サイバー攻撃を受けた**被害組織がサイバーセキュリティ関係組織とサイバー攻撃被害に係る情報を共有する際の実務上の参考となるガイダンス**を公表。
- 当該ガイダンスは、被害組織の担当部門（例：セキュリティ担当部門、法務・リスク管理部門等）を主な想定読者とし、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FAQ形式で整理したもの**。
- 今後、経済産業省として、本ガイダンスについて、**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・啓発活動を進めていく**。

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）
- 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「情報セキュリティ安心相談窓口」「コンピュータウイルス・不正アクセスに関する届出」「J-CRAT 標的型サイバー攻撃特別相談窓口」
- JPCERT/CC「インシデント対応依頼」

産業界へのメッセージ（６）（ＩＴサービス等提供事業者向け）

- **自らの製品・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）**の考え方に沿った一層の対応**（「顧客だけにセキュリティの責任を負わせない」、「トップ主導での実施」等の基本原則の遵守、SBOMの採用、メモリに安全なプログラミング言語の採用等）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。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

- 「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4月に米国サイバーセキュリティー・インフラセキュリティー庁（CISA）が一部有志国と共に**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を作成**し、**ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置を講じるよう**促した。同年10月に本文書が改訂され、我が国を含む13か国が共同署名。その中でも、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**。
- 今後、経済産業省としても、本文書も踏まえ、**ソフトウェア開発者が行うべき取組整理など推進のための取組を検討**していく予定。それにより、ITサービス等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。

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「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」に署名しました」（令和５年10月）

産業界へのメッセージ（７）（被害組織を直接支援する専門組織向け）

- 「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」に沿って、**専門組織間で必要な情報を共有することの意義等について被害組織と共通の認識を醸成する**努力をお願いしたい。

趣旨・背景

- 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。
- 今後、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の活用促進や工場の制御システムに係るセキュリティ、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コンソーシアム

- ✓ **NTT・NECをはじめとした民間企業10社**が、「**セキュリティ・トランスペアレンシー・コンソーシアム**」を立ち上げ。
- ✓ **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を高めることを目指す。
- ✓ その**活用過程での課題**（※）に対して、**民間企業としての対処策をとりまとめ**、順次公表予定。

（※）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

【事例②】工場防衛に特化したセキュリティチームの立上げ

- ✓ 住友ゴム工業や横河電機等の企業が**工場の制御システムの防衛・復旧に特化**した**サイバーセキュリティーチームを立ち上げ**。
- ✓ 具体的には、**工場の制御システムを監視・攻撃の予兆をつかむ**組織や**制御システムに実際に攻撃が起きた時に復旧を進める**組織を想定。
- ✓ **制御システムに特化した組織は珍しい事例**。今春から本格稼働の予定。

【事例③】商工会による中小企業等の脆弱性診断調査

- ✓ 大阪商工会議所・立命館大学が、**中小企業等のHPの脆弱性診断**を実施したところ、**約66%**のURLに、**改ざんや不正プログラム埋め込み等が行われる危険性**が見受けられると発表。
- ✓ この結果を踏まえ、本年2月に**セミナーを開催**し、**中小企業セキュリティに関する実態や対策ポイント**を解説。

（出典）各種公開情報・報道より作成。

参考資料

①サプライチェーン全体での対策強化
②国際連携を意識した認証・評価制度等の立上げ
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新たな攻撃を防ぎ、守るための研究開発の促進
　（サイバーセキュリティ産業振興）
⑤政府全体の動向

産業サイバーセキュリティ研究会とWGの設置による検討体制

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　開催
第２回：平成30年　5月30日　開催
　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　開催
　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　開催（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　開催
　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　開催
　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　開催
　産業界へのメッセージを発信
第８回：令和６年　　４月５日　開催
　産業界へのメッセージを発信

構成員

泉澤　清次	三菱重工業株式会社取締役社長	※2024年4月開催時点
遠藤　信博	日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社特別顧問	
大林　剛郎	日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組取締役会長 兼 取締役会議長	
寺田　航平	経済同友会副代表幹事、寺田倉庫株式会社　代表取締役社長	
澤田　純	日本電信電話株式会社取締役会長	
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（制度・技術・標準化）

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

１．サプライチェーン強化パッケージ

WG２（経営・人材・国際）

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

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３（サイバーセキュリティビジネス化）

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

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する～Proven in Japan～
３．『中小企業・地域』まで展開する

参考資料

①サプライチェーン全体での対策強化
②国際連携を意識した認証・評価制度等の立上げ
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新たな攻撃を防ぎ、守るための研究開発の促進
（サイバーセキュリティ産業振興）
⑤政府全体の動向

分野別SWGにおけるサイバー・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

- **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（制度・技術・標準化）

ビルSWG

- 事前対策が中心の第1版にインシデントレスポンスを追加した**ガイドライン第2版を公開（2023年4月）**。
- **個別編(空調システム)ガイドライン第1版を公開（2022年10月）**。

防衛産業SWG

- 米国の新標準と同程度まで強化した**新情報セキュリティ基準を策定（2022年４月１日）**。

スマートホームSWG

- シンプルな対策ガイドから、具体的な対策要件や他の標準との対比まで、セキュリティ対策を階層的に整理し、**ガイドライン1.0版を公開（2021年4月）**。

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2.0版を公開（2024年3月）。**

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）

電力SWG

- 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、官民が取り組むべき課題と方向性について広く検討。**小売電気事業者ガイドラインを策定（2021年2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2.1版を公開（2023年9月）。**
- 工場領域や販売領域セキュリティの課題対応についても検討中。

工場SWG

- 業界団体や企業が自ら対策を企画実行するに当たり参照すべき考え方やステップを手引きとして**ガイドラインVer1.0版を公開（2022年11月）。**
- 工場をスマート化する際に留意すべき点や対策のポイント等についてまとめた**ガイドライン 別冊：スマート化に向けた対策ポイントを公開（2024年4月）。**

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。
- **2023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 2.1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。

＜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。

＜2022年度進捗＞
- 2022年３月に公開した**「自工会／部工会サイバーセキュリティガイドライン2.0版」をサプライチェーンに展開**し適用状況を集約。
- **21年度(1.0版)の回答2,300社に対し、22年度(2.0版)は約4,000社に増加。**
- 集計データ最終結果、自動車業界平均比較テンプレート活用方法の公表

＜2023年度進捗＞
- 自己評価結果の提出方法のシステム化に伴う入力項目追加と誤記修正を実施した**「自工会／部工会サイバーセキュリティガイドライン2.1版」を公開**。
- 2023年度の自己評価を実施のための自工会・部工会合同の説明会開催
- データ集計中であり、最終結果は例年通り３月末に公表予定
- 部工会と連携したサプライヤー向けの相談会やインシデント実例をもとにしたセミナーも開催

https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

工場SWG （座長：江崎 浩　東京大学 教授）

- 2022年1月6日に工場SWGを設置し、これまでに計7回開催。委員、オブザーバー、ヒアリング対象など、主な関係団体・企業も広く参画し、工場セキュリティガイドラインの策定に向けて活動。
- 2022年11月16日に**「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を公表**。
  2024年4月4日に本ガイドライン**「別冊：スマート化を進める上でのポイント」を公表**。

開催実績

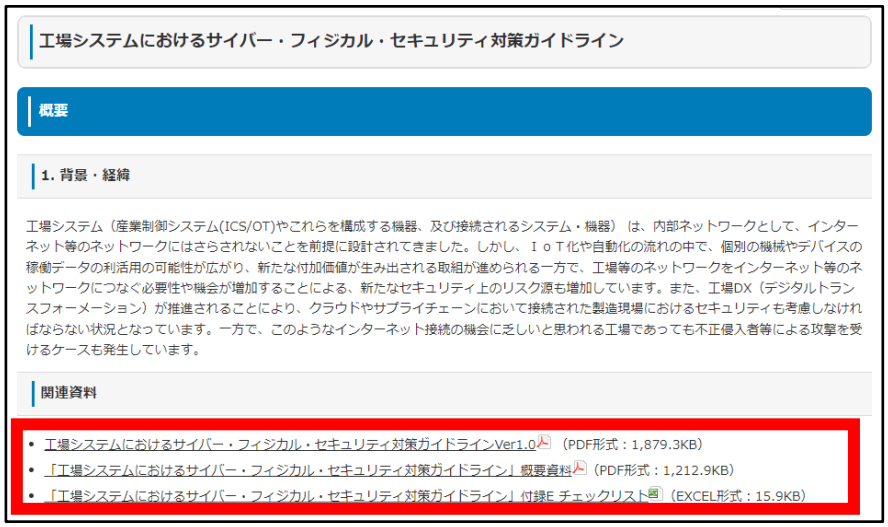
第１回　工場SWG設置について
第２回　主な産業界団体・企業からのヒアリング
第３回　パブコメに向けたガイドライン案の審議
第４回　パブコメ意見を踏まえたガイドライン案の審議
第５回　ガイドラインの普及に関する取組等について
第６回　ガイドラインの拡充版について

【拡充版 作業部会】
- 第1回：2023年10月30日
- 第2回：　〃　11月22日
- 第3回：　〃　12月6日
- 書面レビュー：〃 12月28日～翌年1月12日

第７回　ガイドライン拡充版 別冊(案) について

委員名簿

江崎 浩（座長）	東京大学 教授
岩﨑 章彦	電子情報技術産業協会
榎本 健男	日本工作機械工業会
桑田 雅彦	日本電気株式会社
斉田 浩一	ファナック株式会社
佐々木 弘志	フォーティネットジャパン株式会社
斯波 万恵	株式会社東芝
高橋 弘宰	トレンドマイクロ株式会社
中野 利彦	株式会社日立製作所
市岡 裕嗣	三菱電機株式会社
藤原 剛	ビー・ユー・ジーDMG森精機株式会社
松原 豊	名古屋大学　准教授
村瀬 一郎	技術研究組合制御ｼｽﾃﾑｾｷｭﾘﾃｨｾﾝﾀｰ
渡辺 研司	名古屋工業大学　教授


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

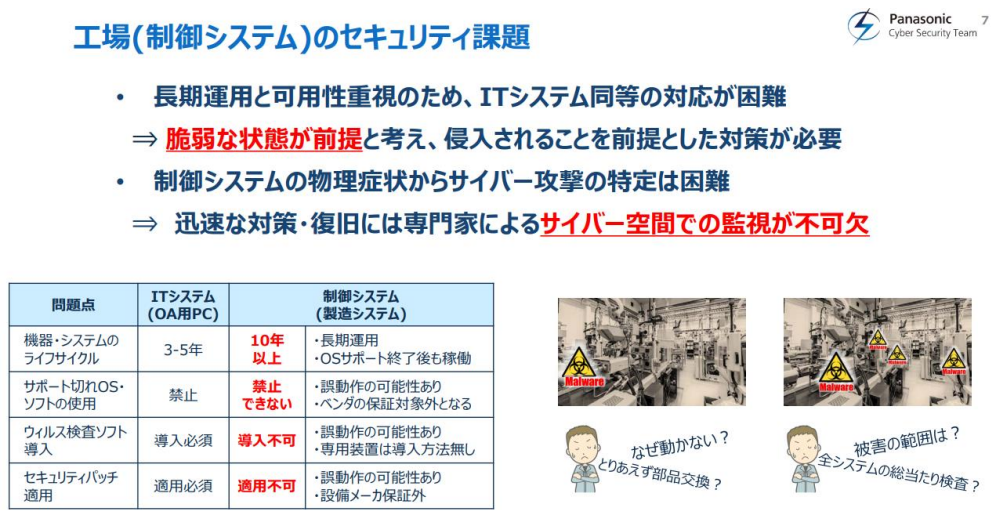
概要

1. 背景・経緯

工場システム（産業制御システム(ICS/OT)やこれらを構成する機器、及び接続されるシステム・機器） は、内部ネットワークとして、インターネット等のネットワークにはさらされないことを前提に設計されてきました。しかし、ＩｏＴ化や自動化の流れの中で、個別の機械やデバイスの稼働データの利活用の可能性が広がり、新たな付加価値が生み出される取組が進められる一方で、工場等のネットワークをインターネット等のネットワークにつなぐ必要性や機会が増加することによる、新たなセキュリティ上のリスク源も増加しています。また、工場DX（デジタルトランスフォーメーション）が推進されることにより、クラウドやサプライチェーンにおいて接続された製造現場におけるセキュリティも考慮しなければならない状況となっています。一方で、このようなインターネット接続の機会に乏しいと思われる工場であっても不正侵入者等による攻撃を受けるケースも発生しています。

関連資料

- 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Ver1.0（PDF形式：1,879.3KB）
- 「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」概要資料（PDF形式：1,212.9KB）
- 「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」付録E チェックリスト（EXCEL形式：15.9KB）



第2回 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） 工場サブワーキンググループ　資料4-2,4-4より抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/002.html

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　～全体概要～

ガイドラインの背景・目的

- 工場の**IoT化やクラウド活用によるネットワーク接続機会の増加**に伴いサイバー攻撃リスクが増加。また、ネットワークの接続が少ない工場であっても不正侵入者等による攻撃の可能性あり。
- 意図的な攻撃の場合もあれば、たまたま攻撃される場合もある。

→**いかなる工場でもサイバー攻撃のリスクあり**。

- 本ガイドは業界団体や個社が自ら対策を企画・実行するに当たり、**参照すべき考え方やステップを示した「手引き」**。

→**各業界・業種が自ら工場のセキュリティ対策を立案・実行**することで、**工場のセキュリティの底上げを図ることが目的**。

想定する読者の方

- ITシステム部門
- 生産関係部門（生産技術部門、生産管理部門、工作部門等）
- 戦略マネジメント部門（経営企画等）
- 監査部門
- **機器システム提供ベンダ、機器メーカ**
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。
※事務系の情報システム（IT）は対象外。

対策に取り組む効果

- **工場のBC／SQDC※の価値がサイバー攻撃により毀損されることを防止**。
- **経営目標(事業伸長、継続の観点等)**との連関
- セキュリティが担保されることで**IoT化や自動化が進み、多くの工場から新たな付加価値**が生み出されていくことを期待。

※ 安全確保(S：Safety)、
事業／生産継続(BC：Business Continuity)
品質確保(Q：Quality)
納期遵守・遅延防止(D：Delivery)
コスト低減(C：Cost)

セキュリティ対策企画・導入の進め方

ステップ 1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
- **ステップ1-3**　業務の重要度の設定
- **ステップ1-4**　保護対象の整理
- **ステップ1-5**　保護対象の重要度の設定
- **ステップ1-6**　**ゾーン**の整理とその業務、保護対象の結びつけ
  （生産管理・監視、制御系、自動搬送、自動倉庫、リモートメンテナンス等）
- **ステップ1-7**　ゾーンと、セキュリティ脅威の影響の整理
  （**俯瞰化、別ゾーンへの影響の抑止、被害の抑制**）

ステップ 2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **ステップ2-2**　**（高・中・最低限）**
  想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策
① ネットワークにおけるセキュリティ対策
② 機器におけるセキュリティ対策
③ 業務プログラム・利用サービスにおけるセキュリティ対策

(2)物理面での対策
① 建屋にかかわる対策
② 電源／電気設備にかかわる対策
③ 環境(空調など)にかかわる対策
④ 水道設備にかかわる対策
⑤ 機器にかかわる対策
⑥ 物理アクセス制御にかかわる対策

ステップ 3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策

(1)ライフサイクルでの対策
① 運用・管理面のセキュリティ対策
A) サイバー攻撃の早期認識と対処（OODAプロセス）
B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C) 情報共有

②維持・改善面のセキュリティ対策
・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
・組織・人材のスキル向上（教育、模擬訓練等）

(2) サプライチェーン対策
・**取引先や調達先に対するセキュリティ対策の要請、対策状況の確認**

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

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】 ～全体概要～

ガイドラインの背景・目的

- 制御システムにおけるシステムアーキテクチャの変化や、サプライチェーンによる脅威の増加により、工場がサイバー空間に密接に繋がっていく世界におけるセキュリティのあり方を検討することが必要。
  →**先進的な企業が臆することなく工場のスマート化を進め、工場の価値創造を促進することを後押しする。**
- 工場のスマート化を先進的に進める業界（例：半導体業界等）では、サプライチェーンにおいて取引先に対するセキュリティ対策が要請。海外では、機器に対するセキュリティ確保の取組が推進。
  →**近年さらに強まっているセキュリティの必要性を訴える。**

想定する読者の方

- IT関係部門（情報システム部門、セキュリティ部門等）
- 生産関係部門（生産技術部門、生産管理部門、工作部門　等）
- 戦略マネジメント部門（経営企画等）
- 監査部門
- リスク管理部門
- DX担当部門
- 機器システム提供ベンダ、機器メーカ（サプライチェーンを構成する調達先を含む）

本ドキュメントの読み方

- **スマート工場の概要を示すとともに、ガイドライン本編3章に示した各ステップの対策におけるスマート化を進めるにあたっての留意点や具体例を提示。**
- 各ステップの冒頭の青枠にスマート化を進める上でのポイントを示すとともに、緑枠にガイドライン本編の記載内容の概要を提示。

セキュリティ対策企画・導入の進め方

ステップ 1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**　セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
  - スマート化の目的に照らした業務の広がり
  - 業務の広がりに応じたシステム範囲の拡大
- **ステップ1-3**　業務の重要度の設定
- **ステップ1-4**　保護対象の整理
- **ステップ1-5**　保護対象の重要度の設定
- **ステップ1-6**　ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7**　ゾーンと、セキュリティ脅威の影響の整理
  - スマート化におけるゾーンごとのセキュリティ要件の考え方
  - スマート化により考慮すべき脅威と影響の考え方

ステップ 2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ
  (1)システム構成面での対策
  ①ネットワークにおけるセキュリティ対策
  - ネットワーク接続における対策
  - クラウド利用時の対策

  ②機器におけるセキュリティ対策
  - 汎用品のセキュリティ対策

  ③業務プログラム・利用サービスにおけるセキュリティ対策
  - データ活用・連携における対策

  (2)物理面での対策

ステップ 3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策、サプライチェーンを考慮した対策**
  (1)ライフサイクルでの対策
  ①運用・管理面のセキュリティ対策
  - スマート化におけるサイバー攻撃の早期認識と対処プロセスの実現

  ②維持・改善面のセキュリティ対策
  - スマート化におけるPDCAサイクルの実現

  (2) サプライチェーン対策
  - 汎用品利用時の留意事項
  - クラウド利用時の留意事項
  - ソフトウェア利用時の留意事項

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

ビルSWG （座長：江崎 浩　東京大学 教授）

- **2023年4月にガイドライン第2版を策定し、**当該SWG内外を問わず**ガイドラインの拡張・充実化**が進んでいるため、**業界の自主的取組への移行が期待**される。
- 現在、IPAを中心に設置が検討されている**スマートビルアソシエーション(仮称)のセキュリティWGへの合流**を検討中。

時期	内容
2018年2月	**ビルSWG設置** ：ビルオーナーを始め、建設会社、設計事務所、ビルに係わる各種設備機器のベンダ、制御システムセキュリティの有識者など、多数のステークホルダーが一堂に会し、ビルシステムに関するサイバーセキュリティ対策のガイドラインを議論。
2019年6月	**ビル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第1版の策定** ：CPSFに基づいてビルシステムに対するサイバーセキュリティ対策についてまとめた共通編ガイドラインとして策定。 ＜背景＞ 近年のサイバー攻撃技術の高度化や、様々なシステムが益々ネットワークに繋がっていく状況の中、制御システムへのサイバー攻撃リスクも高まってきている一方で、ビルシステムに関するサイバーセキュリティ対策は遅れていた。
2022年10月	**ビル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（個別編：空調システム第1版の策定）** ：共通編ガイドラインに加え、ビルの個別のサブシステムに特化した内容をまとめた個別編ガイドラインとして策定。 ＜背景＞ ガイドラインは共通編及び個別編の2階建てで作ることとしていた。共通編が出来上がったことを受け、個別編の議論に入り、当初より要望のあった空調分野でまず検討が開始された。
2023年4月	**ビル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第2版の策定** ：インシデントレスポンスに係る内容を共通編ガイドラインに組み込む形で策定。 ＜背景＞ スマートビル化の進展により、ビルシステムがサイバー攻撃を受ける可能性はより高まっている。事前対策でサイバー攻撃を受ける可能性を抑止するとともに、それでもサイバー攻撃（サイバーインシデント）を受けてしまった場合に、その損害を最小限に抑え、復旧にかかる時間とコストを削減するための取組（インシデントレスポンス）が重要。

ビル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第2版の構成

目次

1．はじめに
- 1．1．ガイドラインを策定する目的
- 1．2．ガイドラインの適用範囲と位置づけ
- 1．3．本ガイドラインの構成

2．ビルシステムを巡る状況の変化
- 2．1．ビルシステムを含む制御システム全般の特徴と脅威の増大
- 2．2．ビルシステムにおける攻撃事例
- 2．3．ビルシステムにおけるサイバー攻撃の影響

3．ビルシステムにおけるサイバーセキュリティ対策の考え方
- 3．1．一般的なサイバーセキュリティ対策のスキーム
- 3．2．ビルシステムの構成の整理
- 3．3．ビルシステムの特徴
- 3．4．ビルシステムにおけるサイバーセキュリティ対策の整理方針
- 3．5．ガイドラインの想定する使い方例

4．ビルシステムにおけるリスクと対応ポリシー
- 4．1．全体管理
- 4．2．機器ごとの管理策

5．ライフサイクルを考慮したセキュリティ対応策

6．インシデント発生時の対応策

付録A　用語集
付録B　JDCCの建物設備システムリファレンスガイドとの関係
付録C　建物設備システム リファレンスガイド　インシデント対応・セキュリティ…ション編との関係
付録D　サイバー・フィジカル・セキュリティ対策フレームワークの　考え方とビル…におけるユースケース
付録E　参考文献
付属書　ビルシステムにおけるサイバー・フィジカル・セキュリティ対策インシデント…ンス・ガイドライン

（非公開の部分）

主に教育・啓発的内容
・なぜビルのサイバー対策が必要か？
・誰が考えるべきか？

第2版で**インシデントレスポンス**のエッセンスを追加

主にガイドラインの作り／考え方
・対象システムのモデル
・対策を導き出す思考アプローチ

対象ごとの考え得る**インシデント、リスク源、対策（ポリシー）**をワンセットで記載

さらに詳細な対応を、**ビルのライフサイクルのそれぞれの場面にブレークダウン**（別表としてインデックス化）

サイバー攻撃（インシデント）の発生時に、その損害を最小限に抑え、復旧にかかる時間とコストを削減するための取組を記載

実装レベルの対策（対策の具体的解説や、実際の対策事例）は、関係者のみで共有

宇宙産業SWG（座長：坂下 哲也 JIPDEC 常務理事）

- **2023年3月にガイドライン1.1版を公開**。2023年度は改訂に向けてスコープの拡大、セキュリティ関連規程雛形の追加、具体的な対策内容の追記等について議論を行い、**2024年3月にガイドライン2.0版を公開**。
- また、宇宙事業者が抱える情報共有に関する課題・ニーズを踏まえ、国内の宇宙分野における**情報共有体制のあり方について検討。**

「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」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 1.1

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 1.1」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。

和文

- 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 Ver1.1（PDF形式：4,464KB）
- 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 1.1 概要資料（PDF形式：1,788KB）
- 【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：20KB）

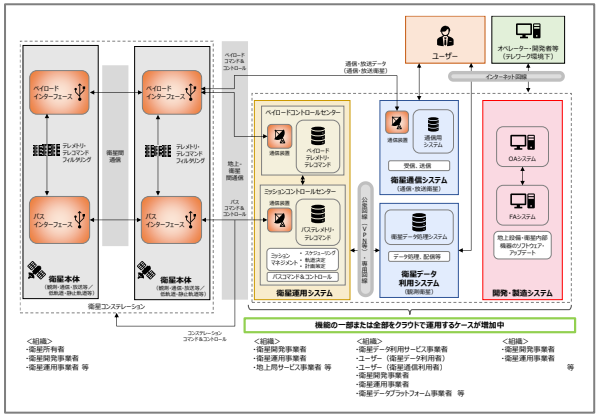
英文

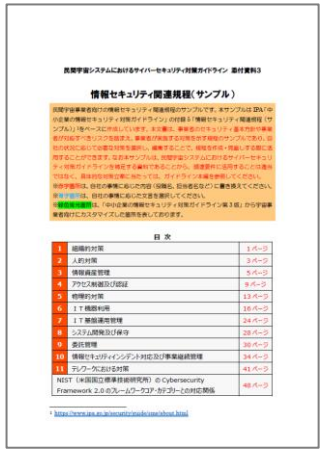
- Cybersecurity Guidelines for Commercial Space Systems Ver 1.1（PDF形式：2,846KB）
- Cybersecurity Guidelines for Commercial Space Systems Ver 1.1 (Summary)（PDF形式：665KB）
- 【Attachment 1】Checklist of Requirements and Measures（Excel形式：15KB）
- 【Attachment 2】Correlation between NIST CSF and Specific Measures for Space Systems（Excel形式：18KB）

- 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 1.0

～2022年度：
ガイドライン1.0版/1.1版に関する議論、公開

民間宇宙システムの標準的なモデル





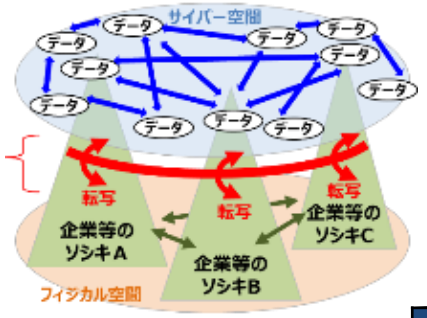
セキュリティ関連規程雛形

2023年度：
ガイドライン2.0版への改訂に向けた議論
（スコープの拡大、セキュリティ管理規程雛形の追加、具体的な対策内容の追記等）

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

- ISO/IECの国内エキスパートの協力のもと、**CPSFのモデル等を盛り込んだ国際規格（TS:技術仕様書）策定**を推進。現在、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。
- WD（作成段階）へ移行し、最終的な投票にかけるTS原案(DTS)を策定中。2024年度中にFDTS投票を行う予定で2/3以上の賛成を得た場合TSが成立し、2025年度早々の発行を目指す。

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 → WG 4

※ 下図において、「会合」とは、SC 27/WG 4で通常4月周辺、10月周辺に年2回開催される定期会合を指す。「中間会合」とは、上記に示す定期的な会合とは別に、アドホックに開催されるプロジェクト単位の会合を指す。

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

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

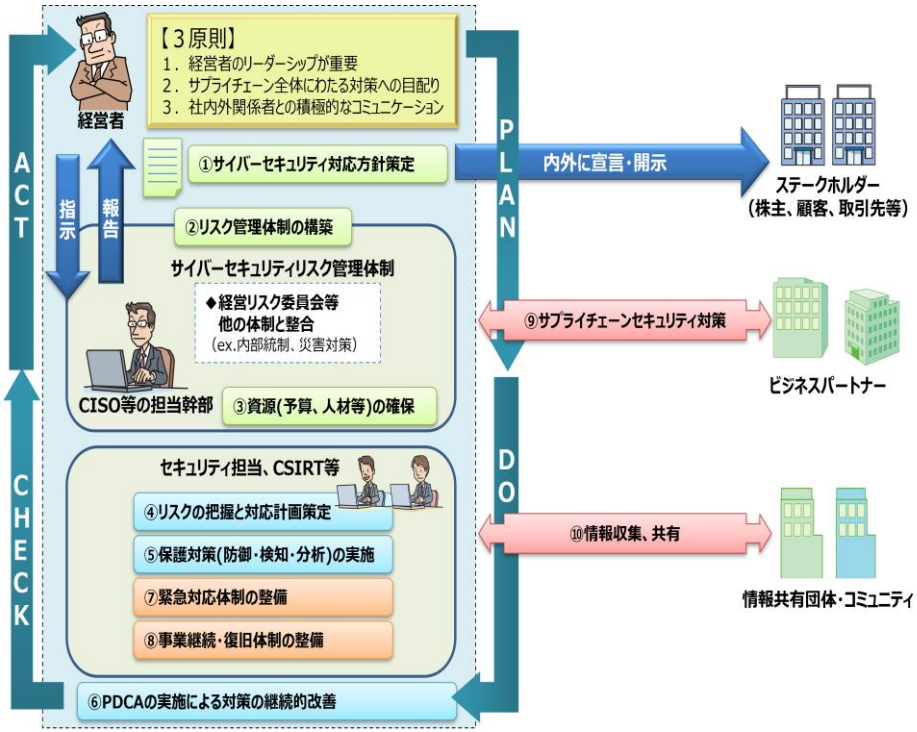
- サイバーセキュリティ対策に当たっては、経営者がリーダーシップをとってセキュリティ対策を推進していくことが重要。サイバーセキュリティ対策を推進するため、経営者を対象としたサイバーセキュリティ経営ガイドラインを策定。
- ガイドラインにおいては、経営者が認識すべき３原則及び経営者が情報セキュリティ対策を実施する上での責任者（CISO等）に指示すべき１０の重要事項をまとめている。

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

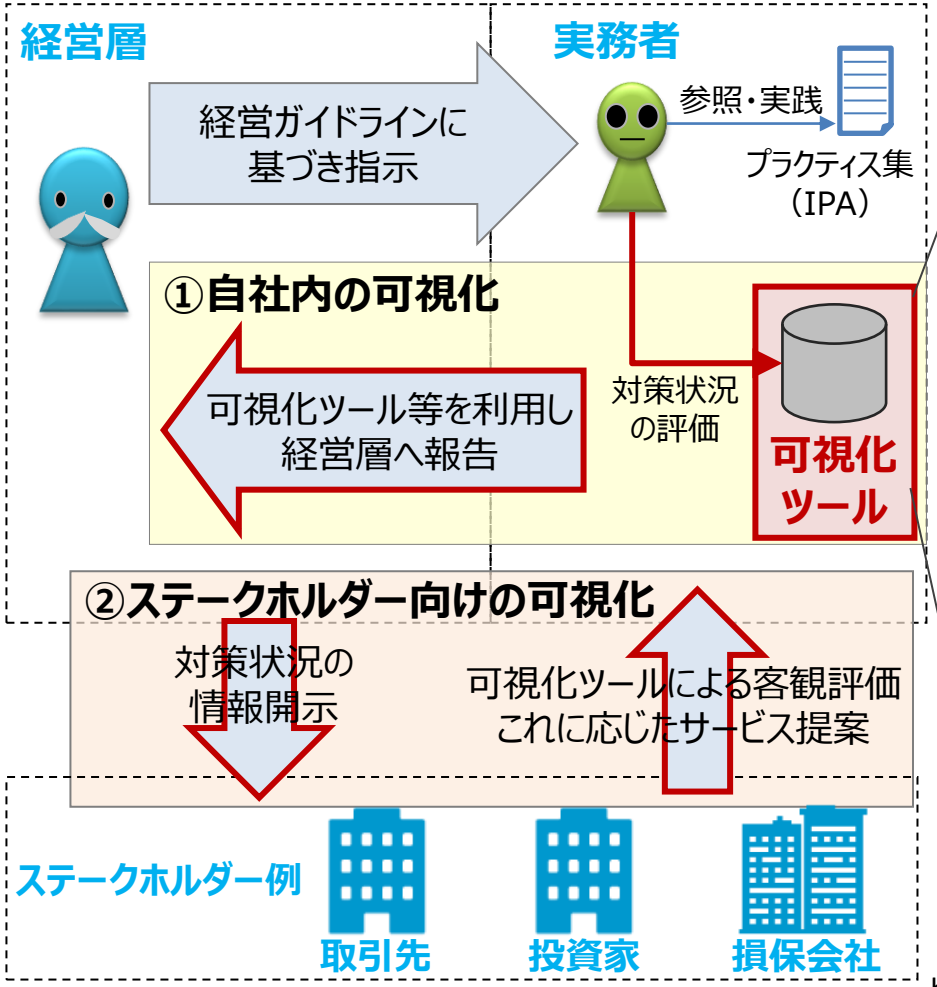
リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施による継続的改善
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 事業継続・復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の状況把握及び対策
関係者とのコミュニケーション	**指示10** 情報収集、共有及び開示の促進



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

サイバーセキュリティ経営可視化ツール

- 「サイバーセキュリティ経営ガイドライン」で定める重要10項目の実施状況を5段階の成熟モデルで可視化（レーダーチャート表示）するツール。自社のサイバーセキュリティ対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定、適切なセキュリティ投資の実行等が可能。
- **2023年7月、業界ごとの平均値を参考値として表示する機能を追加**し、更なる利便性向上を実施。



特徴

- 40の設問に回答⇒実践状況をレーダーチャート表示
- 業界ごとの平均値を参考値として表示することも可能

https://www.ipa.go.jp/security/economics/checktool/index.html

『サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集』

- サイバーセキュリティ経営ガイドラインの重要10項目を具体的に実践していくに当たり、サイバーセキュリティ経営ガイドライン実践のためのプラクティス集を公開。**実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示**。
- **2023年10月**、サイバーセキュリティ経営ガイドラインVer3.0の改訂を踏まえ、**プラクティスの拡充や企業インタビュー調査で得られた事例をミニプラクティスとして追加した第４版を公表**。

＜特徴＞

サイバー攻撃対策やインシデント対応の強化に向けた体制づくりや対策は何から始めるべきか、と考えている経営者やCISO等、セキュリティ担当者を主な読者と想定し、ガイドラインの「重要10項目」を実践する際に参考となる考え方やヒント、実施手順、実践事例を掲載。

【第４版の主な改訂内容】

- 実践例として、「リテラシーにとどまらないプラス・セキュリティ教育の実践」「DX推進を支える仕組みづくり」「サプライチェーンでの連携体制の構築」「『情報の共有・公表ガイダンス』に基づくCSIRTと社内外関係者との連携推進」などの事例を追加
- ミニプラクティスとして、クラウドサービスを利用する際のセキュリティ対策の強化や従業員向けのサイバーセキュリティ教育の効果を高めることなどに関する事例を追加

＜構成＞

はじめに
第1章　経営とサイバーセキュリティ
第2章　サイバーセキュリティ経営ガイドライン実践のプラクティス
第3章　セキュリティ担当者の悩みと取組みのプラクティス
ミニプラクティス
付録


プラクティス 4-1　経営への重要度や脅威の可能性を踏まえたサイバーセキュリティリスクの把握と対応

F社の実践のステップ

F社の実践内容

表2-4.2 F社で想定したサイバー攻撃の事例とリスク値の例

図2-4.1 F社で利用した被害発生可能性と重要度からリスク値を判定する方法の例

サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて（概要）

令和４年10月28日
経 済 産 業 省
公 正 取 引 委 員 会

【 背　景 】

■ 昨今、サイバーセキュリティ対策が不十分な**中小企業がサイバー攻撃に狙われ、サプライチェーン全体に問題が波及**する事態が発生。

■ 令和４年４月、「原油価格・物価高騰等に関する関係閣僚会議」（内閣総理大臣、内閣官房長官、関係大臣、公正取引委員会委員長が出席）において、**コロナ禍における「原油価格・物価高騰等総合緊急対策」**を決定。

「サイバーインシデントによってサプライチェーンが分断され、物資やサービスの安定供給に支障が生じることのないよう、**中小企業等におけるサイバーセキュリティ対策を支援**するとともに、**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**を行う。」

【 内　容 】

■ 発注者側となる事業者は、以下を参考に、**サプライチェーンの保護に向けて、取引先のサイバーセキュリティ対策の強化を促しつつ、サプライチェーン全体での付加価値の向上に取り組み、取引先とのパートナーシップの構築**を目指していただきたい。

①サイバーセキュリティ対策に関する支援策

■ **サイバーセキュリティお助け隊サービス**（中小企業に対するサイバー攻撃への対処として不可欠なサービスをワンパッケージで提供）の利用促進

■ **セキュリティアクション**（中小企業がセキュリティ対策に取り組むことを宣言）の推進

■ **中小企業の情報セキュリティ対策ガイドライン**（中小企業を対象に、情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき方針、対策を実践する際の手順や手法をまとめたもの）の活用

■ **パートナーシップ構築宣言**（発注側企業が取引先との間でパートナーシップを構築することを宣言）の中で、取引先にサイバーセキュリティ対策の助言・支援を行うことを取組例として記載

②サイバーセキュリティ対策の要請に係る独占禁止法・下請法の考え方

■ サイバーセキュリティ対策の必要性が高まる中、**サプライチェーン全体のセキュリティ対策強化は重要**な取組。**サイバーセキュリティ対策を要請すること自体が直ちに問題となるものではない**。

■ ただし、要請の方法や内容によっては、問題となることもあるため、そのようなケースを例示。

＜問題となるケースの例＞

① 取引上の地位が優越している事業者が、サイバーセキュリティ対策の実施によって取引の相手方に生じるコスト上昇分を考慮することなく、一方的に著しく低い対価を定める場合

② 取引上の地位が優越している事業者が、新たなセキュリティサービスを利用する必要がないにもかかわらず、自己の指定する事業者が提供するより高価なセキュリティサービスの利用を要請し、当該事業者から利用させる場合

システム監査基準及びシステム管理基準について

- サイバーセキュリティ体制の適切性等の担保のため、システム監査含む各種監査を実施していくことは重要。
- 経済産業省では、**システム監査の品質の確保及び効果的な監査の実現のため、システム監査基準とシステム管理基準を策定、公表**している。

＜管理体制を担保するための監査の重要性＞

● サイバーセキュリティ経営ガイドラインVer3.0

（対策例の抜粋）
・取締役、監査役はサイバーセキュリティリスク管理体制が適切に構築、運用されているかを監査する。
・サプライチェーンに参加する企業の合意のもと、それぞれの企業が実施すべき対策を定め、監査又は自己点検等の実施を通じてその実効性を担保する。

● 重要インフラのサイバーセキュリティに係る行動計画（2022年6月17日） 抜粋
・サイバーセキュリティ体制の適切性を担保するための監査等組織内のサイバーセキュリティ体制が適切であることを担保するための方策としては、内部監査、情報セキュリティ監査、システム監査等の各種監査、内部通報、情報開示、CSIRTの設置といった方策が考えられる。

＜システム監査制度＞

システム監査とは、専門性と客観性を備えたシステム監査人が、一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査の一類型

組織体の経営活動等の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、**組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすことにつながる。**

システム監査基準の改訂の概要

- システム監査基準については、システム監査人の行為規範及び監査手続の規則として監査人の独立性・客観性等に関する基準や監査計画・監査報告などの監査全般に関する基準を規定。
- 令和５年４月、システム監査の意義・目的を達成するに当たり、**システム監査人の倫理が監査の前提となるものであることをより明確にするため、倫理規定部分について、基準から切り離して構成に整理**し、倫理に関して監査人が守るべき原則を明示するなどの改訂を実施。

＜現行のシステム監査基準＞

前文

Ⅰ．体制整備に係る基準	1　監査人の権限と責任等の明確化 2　監査能力の保持と向上 3　ニーズの把握と品質の確保
Ⅱ．監査人の独立性・客観性等に係る基準	4　監査人としての独立性と客観性の保持 5　慎重な姿勢と倫理の保持
Ⅲ．監査計画策定に係る基準	6　監査計画策定の全般的留意事項 7　リスクの評価に基づく監査計画の策定
Ⅳ．監査実施に係る基準	8　監査証拠の入手と評価 9　監査調書の作成と保管 10　監査の結論の形成
Ⅴ．監査報告とフォローアップに係る基準	11　監査報告書の作成と提出 12　改善提案のフォローアップ

改訂

＜改訂後＞

前文
システム監査の意義と目的
監査人の倫理

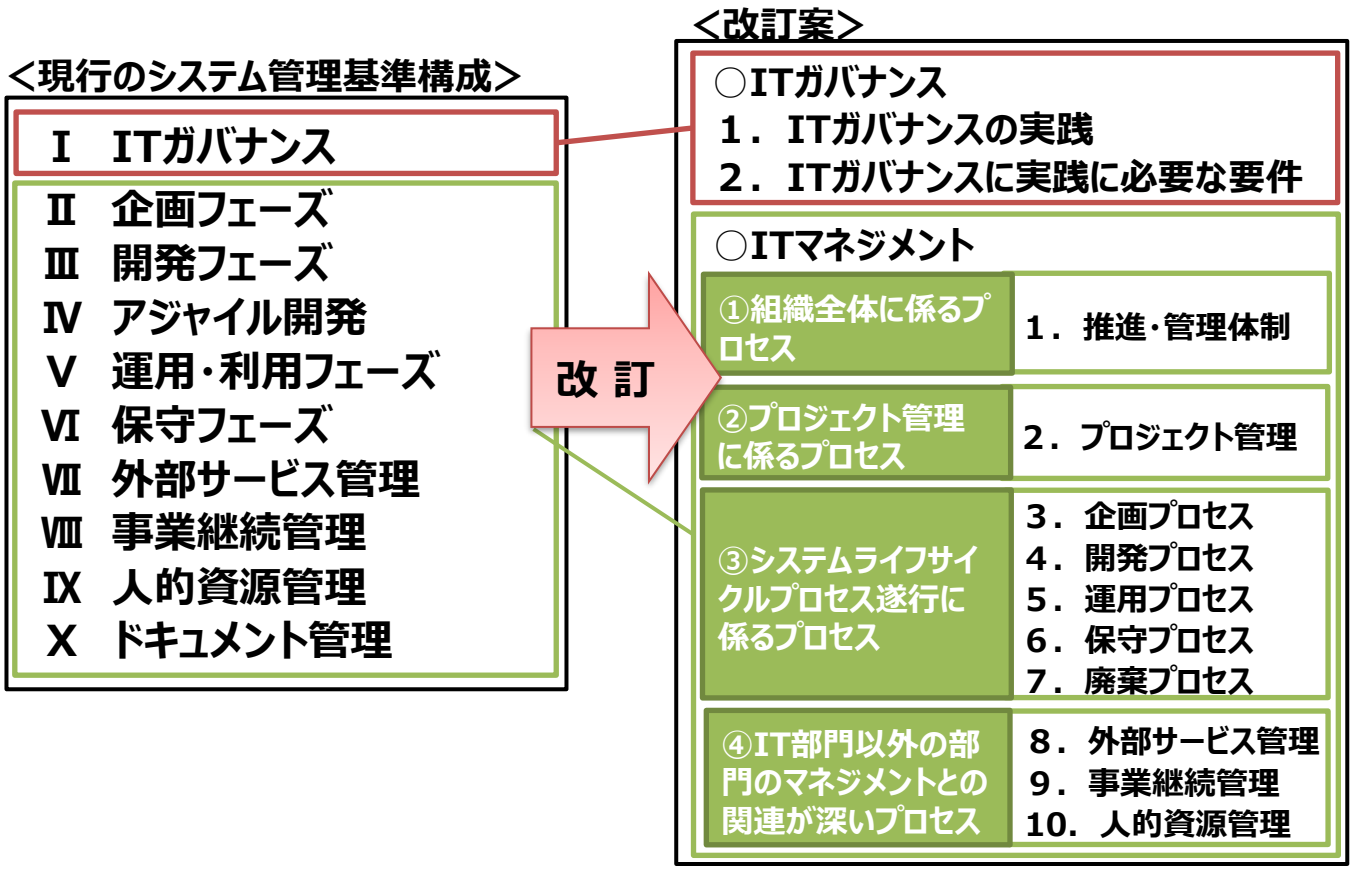
Ⅰ．監査の属性に係る基準	1　監査に係る権限と責任等の明確化 2　専門的能力の保持と向上 3　ニーズの把握と品質の確保 4　監査の独立性と客観性の保持 5　監査能力及び正当な注意と秘密の保持
２．監査の実施に係る基準	6　監査計画の策定 7　監査計画の種類 8　監査証拠の入手と評価 9　監査調書の作成と保管 10　監査の結論の形成
３．監査の報告に係る基準	11　監査報告書の作成と報告 12　改善提案のフォローアップ

【改訂概要】

- 監査人が意識すべき**倫理に関する部分については基準と切り離す構成に整理し、守るべき原則として①誠実性、②客観性、③能力及び正当な注意、④秘密の保持**を明示
- 基準に**監査人のみならず、組織としての対応の在り方、デジタル技術・システム開発手法の変化によるリスクへの留意点**や**監査を効率的・効果的に進めるための手法（リスクアプローチ）**等を追記
- **アジャイル監査などの新たな監査手法例や監査における報告書書式例などはガイドラインとして別冊化**

システム管理基準の改訂の概要

- システム管理基準については、ITシステムの利活用のあるべき姿を示すIT戦略の方針や体制等のガバナンスに関する基準とITシステムの開発・運用等のマネジメントに関する基準を規定。
- 令和５年４月、IT利活用による新たな開発技術やボーダーレスとなっているIT環境のボーダーレス化等の現状を踏まえ、**アジャイル開発やAI活用等の新たな手法・技術等にも対応できるよう、国際規格の考え方なども踏まえながら、各プロセスを細分化して再整理**するなどの改訂を実施。



【改訂概要】

- **ITガバナンス部分につき、**国際規格の考え方も踏まえ、**実践のための直接的な活動に係るプロセスと実践に当たって必要となる要件に係るプロセスに分類し再整理**
- **ITマネジメント部分につき、**国際規格のプロセス区分も参考にしつつ、**新たな手法・技術等にも対応できるよう、各プロセスを細分化し再整理**
- **アジャイル開発を含む様々なプロセスモデルや情報システムの導入形態に対応する留意点**については、**ガイドラインとして別冊化**

ASM(Attack Surface Management)とは

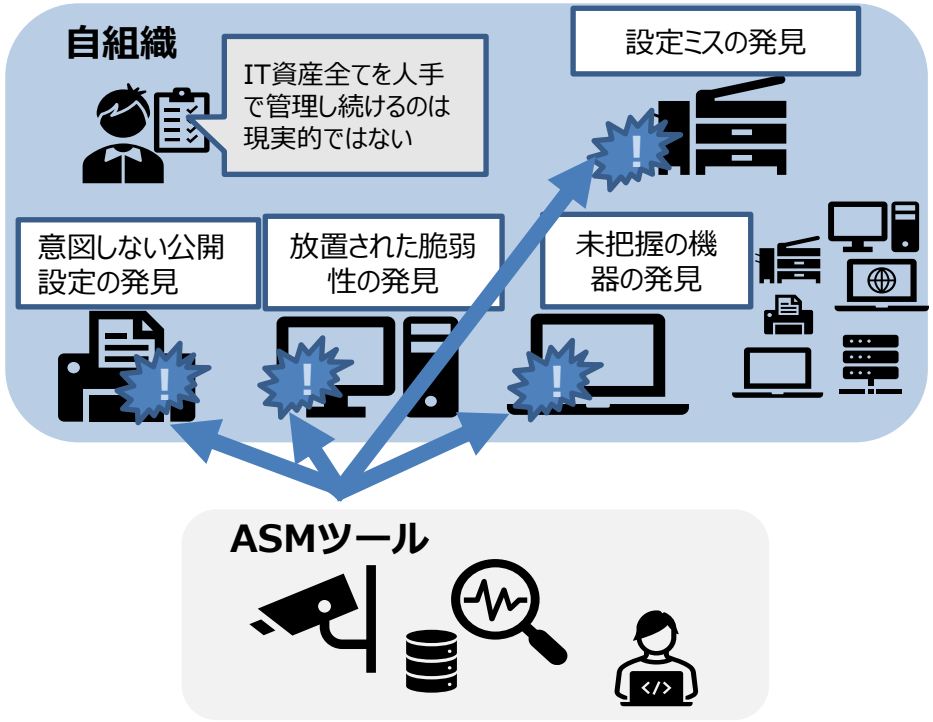
- ASMとは、**組織の外部（インターネット）からアクセス可能なIT資産（＝攻撃面）を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価**する一連のプロセスのこと。
- ASMの継続的な実施により、組織管理者の未把握の機器や意図しない設定ミスを攻撃者視点から発見でき、脆弱性管理活動において、**リスク低減の効果が期待**される。
- 経済産業省では、ASMの基本的な考え方や特徴、留意点などの基本情報とともに取組事例などを紹介した、「**ASM（Attack Surface Management）導入ガイダンス**～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」**を令和５年５月に策定・公表**。

ASMの定義

ASMプロセス

(1) 攻撃面の発見	**企業で保有、管理するIPアドレス・ホスト名の発見** (例) 公開Webサイト、WHOIS情報を利用してドメイン名を特定 など
(2) 攻撃面の情報収集	**攻撃面の情報収集** (例) OS、ソフトウェア、バージョン情報、オープンなポート番号など
(3) 攻撃面のリスク評価	**(2)の収集情報をもとにリスク評価** (例) 公開の既知の脆弱性情報と(2)の収集情報を突合し、脆弱性存在の可能性を識別
リスクへの対応	脆弱性管理と同様の対応 (例) パッチ適用（リスク低減）や対策見送り（リスク受容）など

ASMの特徴



組織の外から機器の情報を収集しデータベース化

ASM(Attack Surface Management)導入ガイダンス

背景・目的

- DXの進展、コロナ禍でのテレワーク拡大により、社会全体でリモート化が進展。サイバー攻撃の起点が増加。
- 自社のIT資産やリスクの適切な把握が求められるなか、**人手によってIT資産を管理しきるのは困難**。
- **外部公開されているサーバ機器等の情報を収集・分析し、不正侵入経路となるポイントを把握するASM**が注目を集めている。
- 本書では、**民間企業における利用実態**の明確化、**ASMツール・サービスの特徴や活用方法**を提示する。

想定読者

- 情報システム部門
- 情報セキュリティ担当部門
- CISやCISOなどの経営層

※セキュリティ向上施策、体制、ツールなどの検討、自社のセキュリティ戦略への組み込みを検討する際などに活用することを想定

ASM導入メリット

- 情報システムを管理している部門が**把握していないIT資産を発見**できる。
- 情報システムを管理している部門の想定と異なり、**公開状態となっているIT資産を発見**できる。
- 情報システムにおいて**放置された脆弱性**を発見できる。

※ただし、外部から確認できる情報を用いるため、脆弱性が存在する可能性の検知にとどまる。

ASM導入のポイント

ポイント1 実施計画の策定

他のセキュリティ施策と同様、ASMも実施計画を策定することが肝要

- **導入目的**
  - ✓ 未把握IT資産を発見する等の目的を明確化
- **調査対象範囲**
  - ✓ どの単位でどの範囲を対象とするのか、IT資産数等の規模とともに明確化
- **運用**
  - ✓ 既存の脆弱性管理施策との整合性、企業間の連絡方法等の整理
- **ツール**
  - ✓ 選定事項とツール機能を考慮し、決定

ポイント2 攻撃面の調査と評価

ASMを全て手作業で実施することは困難、ASM支援ツールを活用するのが一般的

- **事前準備**
  - ✓ 調査対象組織が管理する情報の抽出
- **ASMツール**
  - ✓ 検索エンジン型/オンアクセス型のツール活用
- **必要な知識・スキル**
  - ✓ ASMツールの取扱いに必要な要素
- **注意事項**
  - ✓ 不正確な情報の検知、対象企業への影響、脆弱性評価方法、リスク評価指標の活用方法等
- **ASMサービス**
  - ✓ 外部事業者による取組のサポート

ポイント3 継続的な対応

自社のIT資産に関する状況は時間経過によって変化するため、継続的な取組が重要

- **時間経過による変化**
  - ✓ 例えば、時間経過により、IT資産の増加や変化、IT資産における脆弱性の発見の可能性
- **ASM実施の頻度**
  - ✓ 高頻度で実施したほうがリスク低減できるが業務負荷が高くなる
  - ✓ 実施頻度は自社のセキュリティポリシーや業務負荷、サーバー攻撃の流行などの内外の要因をもとに総合的に判断

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）について

- 大企業と中小企業がともにサイバーセキュリティ対策を推進するため、**幅広い経済団体、業種別業界団体等が参加するコンソーシアム（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））が2020年に創設**（2024年3月時点で102団体含む179会員が参加）。産業界全体で取り組むべきサプライチェーンセキュリティ対策の議論等を実施。
- **令和５年度においては、国際WGを新設するとともに、各WGにおいて情報発信や試行調査、ワークショップ等を実施。**

攻撃動向分析・対策WG（2021年6月～）

- **経営層が認識すべきサイバーセキュリティ関連情報（サイバー攻撃に関する動向やインシデント対応上の留意点等）の発信**

・これまでに4回WGを開催
・令和４年度までの経営層向けサイバーセキュリティに係る情報発信の在り方の検討を踏まえ、**令和５年度は中小企業対策強化WG内で情報発信等を実施**

中小企業対策強化WG（2020年12月～）

- **中小企業対策促進**
- **サイバーセキュリティお助け隊の普及**
- **悩み・課題・解決策・プラクティス共有**

・これまでに12回WGを開催。
・令和５年度はお助け隊サービス制度の普及、業界セキュリティガイドラインの共通項の実装試行、お助け隊サービスの普及を含む中小企業向けセキュリティ普及啓発ウェビナーの開催を実施

産学官連携WG（2020年12月～）

- **産学官連携促進**
- **人材育成**
- **共同研究**

・これまでに8回WGを開催。
・令和４年度のセキュリティ人材フレームワークに関し、産・学の双方にとって参照・活用可能な共通語彙集の試作検討を踏まえ、**令和５年度は企業と大学等において試行調査を実施**

地域SEUNITY形成促進WG（2021年6月～）

- **地域SECUNITY形成促進**
- **悩み・課題共有**
- **解決策・プラクティス共有**

・これまでに７回ワークショップを開催
・令和５年度は、全国ワークショップ（２回）及び地域でのワークショップ（中部、九州、近畿）を実施。
・形成・発展に向けて地域SECUNITY間の情報共有や、共通課題の解決に向けた取組を検討・推進

国際WG（2023年11月～）

- **国際間の意思疎通**
- **問題意識、共通課題、対処法の共有**

・令和５年度に発足。これまでに2回WGを開催。
・国を跨るサプライチェーンサイバーセキュリティの強化を推進するため、国外の機関や団体と連携して実施すべき取組について検討・推進

※これらのWGのほか、業界間の課題抽出、連携の検討、中小企業に限らないサプライチェーンの課題解決を図るため、今後、新たなWGを創設する予定。

中小企業向けセキュリティ対策

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

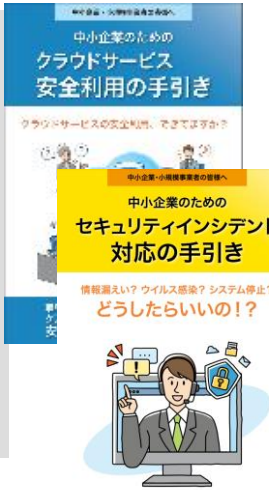
–中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、を実践する際の手順や手法をまとめたもの。付録としてクラウドサービスの安全利用やセキュリティインシデント対応に関する手引きなどがある

中小企業の情報セキュリティ対策ガイドライン

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

付録6、8:クラウドサービス安全利用の手引き、セキュリティインシデント対応手引き



【クラウドサービス導入時の考慮ポイントの例】

- ✓ 選択時のポイント（利用業務の明確化、取り扱う情報の重要度確認、クラウドサービスの安全・信頼性確認　等）
- ✓ 運用時のポイント（管理担当者、利用者範囲の決定　等）
- ✓ セキュリティ管理のポイント（利用者サポート体制の確認、利用終了時のデータ確保、適用法令や契約条件の確認　等）

【セキュリティインシデント対応時等の例】

- ✓ インシデント対応の基本ステップ（ステップ１ 検知・初動対応、ステップ２ 報告・公表、ステップ３ 復旧・再発防止）に関する具体例
- ✓ インシデント発生時の相談窓口・報告先　等

● 「SECURITY　ACTION」

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度。約34万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

● 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。
（2024年3月時点で42事業者）

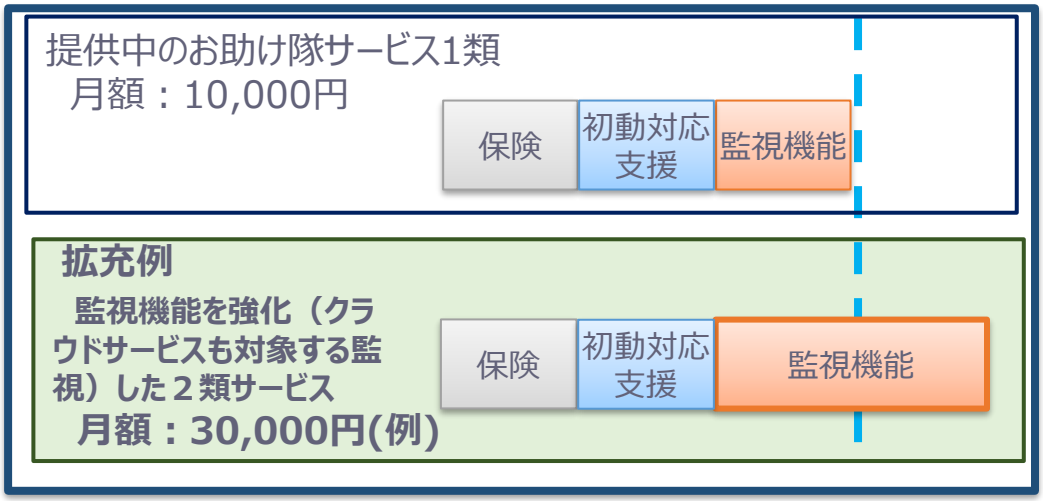
サイバーセキュリティ お助け隊

IT導入補助金に
「セキュリティ推進枠」創設

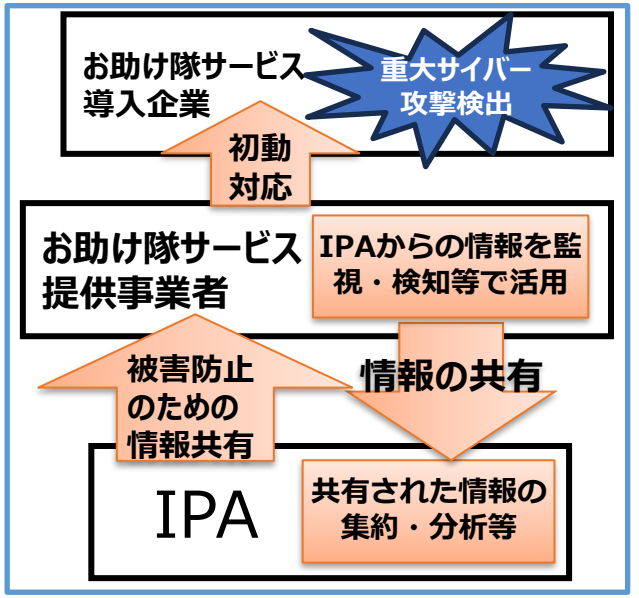
サイバーセキュリティお助け隊サービスの新たな類型（２類）について

- 経済産業省では、ＩＰＡを通じて、システムの異常監視やサイバー攻撃時の初動対応支援、復旧費用の簡易保険など**中小企業のセキュリティ対策に必要となる各種サービスをまとめて提供する民間のセキュリティサービスを登録し公表する「サイバーセキュリティお助け隊サービス」制度を運用（2021年度開始）**。
- 現行のお助け隊サービス（１類）は価格上限があるため実態上、従業員10人前後の中小企業への提供がメインであるところ、**中規模以上の中小企業のニーズにも応えるサービスとなるよう、お助け隊サービスの新たな類型（２類）の検討を実施**。
- 具体的には、現行のお助け隊サービスのコンセプトは維持しながら、**価格要件を緩和しつつ、提供中のお助け隊サービス１類をベースに監視機能の強化や定期的なコンサル実施などの拡充、IPAへの重大サイバー攻撃に関する情報の共有等を要件として、基準の改定を実施**（2024年３月15日に公開）。**お助け隊サービス提供事業者から共有された情報は、IPA内で集約・分析等し、お助け隊サービス提供事業者へ情報共有する**。
- **令和６年度以降、２類サービスの基準への適合性審査を開始し、適合した２類サービスを公表予定**。厚生労働省等の**関係機関や業界団体とも連携しながら、お助け隊サービスの更なる普及、促進を図る**。

2類のイメージ



IPAとの情報共有イメージ



サイバーセキュリティお助け隊サービスの普及の取組

- お助け隊サービスの２類については、より中小企業のニーズにも応えるサービスが想定されるところ、サプライチェーンセキュリティ全体の向上を図るため、**中小企業等へ更にお助け隊サービスを普及していくことが重要**。
- **引き続き関係機関や業界団体と連携しながら、お助け隊サービスの普及を推進**する。

２類追加による効果

・現行サービスと比較して、高スペックな監視機器や、より充実したサービスを提供することが可能となるため、**中規模以上の中小企業のニーズにも応えるサービス**として更なる普及を図る。
・２類サービスと現行サービスの比較表において提供されるサービスの比較などを確認できるようにするなど、ユーザ企業もより利用しやすくする。

業界団体との連携

・引き続き、業界団体とも連携しながら、業界全体のサイバーセキュリティを底上げし、サプライチェーンセキュリティを確保するために、お助け隊の普及を推進する。

業界セキュリティガイドラインにおけるお助け隊活用例：
①日本自動車工業会、日本自動車部品工業会「自工会/部工会・サイバーセキュリティガイドライン解説書」 2023年9月公開
　求める項目の一部について達成の一助になるサービスとしてお助け隊サービスを記載
②日本建設業連合会「協力会社における 情報セキュリティガイドライン」 2023年2月公開
　「実施する情報セキュリティ施策」の感染予防としてお助け隊サービスを記載

関係機関と連携した普及の取組

・例えば、医療機関のニーズを踏まえたお助け隊サービスとの連携について、厚生労働省等と連携しサービス事業者に働きかけていくなど、**お助け隊サービスを普及させるため、引き続き、関係機関とも連携し進めていく。**

中小企業のニーズに応えられるように基準の改定を実施。引き続き、関係機関や業界団体とも連携しながら、更なる普及、促進を図る。

（参考）サイバーセキュリティお助け隊サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。現時点で**42事業者**がサービスを提供。
- 中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開を開始。IT導入補助金による支援を拡充。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

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

中小企業でも導入・維持できる価格でワンパッケージで提供

サイバーセキュリティお助け隊サービスウェブページ
https://www.ipa.go.jp/security/otasuketai-pr/

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊マークの商標利用権を付与

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

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

お助け隊サービス利用の推奨等の中小企業の取組支援

サイバーセキュリティお助け隊

SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)

→SC3（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。

SC3地域SECUNITY形成促進WG

- 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（「地域SECUNITY」）の形成を全国において推進。
- **地域間の情報共有や、共通課題の解決に向けた取組を検討／推進**。

①各地域での活動

各地域においてSECUNITYの活動を推進

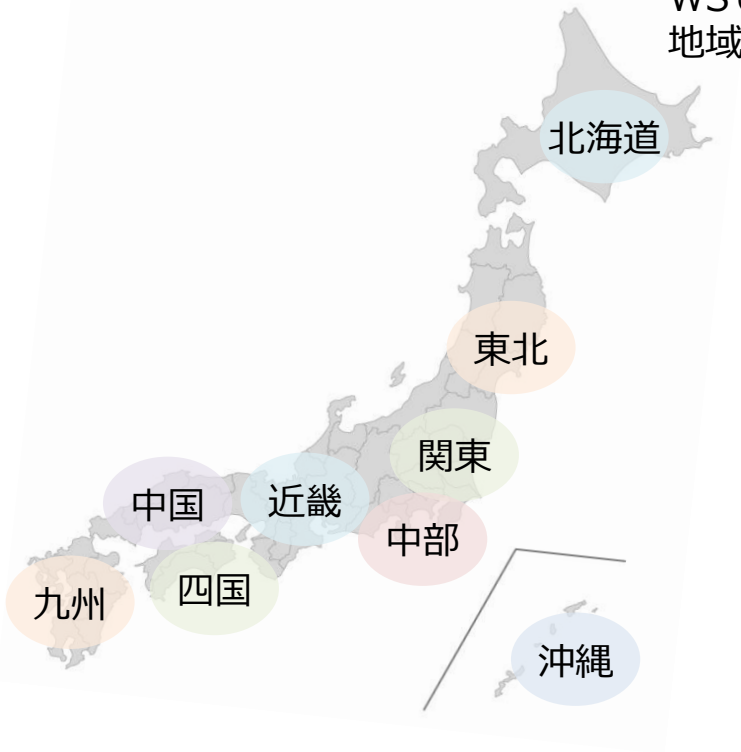
他地域への事例共有

WSで得た知見の活用
地域間の連携創出

②活動の横展開

- **SC3地域SECUNITY形成促進WG ワークショップ（WS）の開催**
- **地域SECUNITYリスト（※）の作成・情報提供**

(※)地域SECUNITY間の直接対話（各種相談、各地域の会合・セミナーの案内等）を自主的・積極的に行うことを推奨



【活動の中で出てきた課題・問題意識の例】

SECUNITYとしての地域の人材不足にどう対応するか。

活動の継続性をどう確保するか。
活動の裾野をどのように広げるか。

他のSECUNITYと連携しつつ、地域の特性にあったコミュニティの形成を目指すには

SC3地域SECUNITY形成促進WG活動実績

- 地域SECUNITYの形成を全国において推進すべく、地域SECUNITY形成促進WGにおいて継続した議論を実施。これまでに全国単位で５回、地域単位で２回（延べ12地域）開催。

① WG設立趣旨：
各地域で形成が進みつつある地域のセキュリティ・コミュニティ（SECUNITY）の取組をさらに推進するため、地域間の情報共有や、共通課題の解決に向けた取組の検討・推進を行う。

② WG設立経緯：
上記設立趣旨を踏まえ、SC3第3回運営委員会（2021年6月22日開催）にて設置。

③ WG活動実績：　https://www.ipa.go.jp/security/sc3/activities/secunityWG/
各地域SECUNITYの担当者等を対象として、各地域における活動にあたって必要となる情報の共有、ベストプラクティスの展開共通課題に対する解決策の検討などを目的としたワークショップを開催。

第1回　2021年10月27日
第2回　2022年 3月 4日
第3回　2022年10月19日
第4回　2023年 1月17日～ 2023年 2月24日（地域開催）
　　2023年度以降に各地域の状況に合わせた支援活動を行うための情報収集を目的とし、各地域の生の声を聞くために各地域（全国9か所）にて開催。
第5回　2023年 6月29日
　　第4回開催における各地域での意見等をもとに、座長・委員でパネルディスカッションを実施。
第6回　2023年11月20日～ 2024年 1月9日（地域開催）
　　地域SECUNITYが活発に活動している地域（中部・近畿・九州）にて、取組の紹介および課題解決に向けた議論を目的に開催。
第7回　2024年2月20日
　　第6回開催における各地域の取組および課題解決に向けた議論の報告。

地域SECUNITY形成のためのプラクティス集（第２版）（2022年6月13日公開）

- 2020年度、全国各地域で経済産業局や地元の協力機関等とともにセキュリティコミュニティの形成を促進。
  （北海道、東北、関東、東海、関西、中国、四国、九州、沖縄）
- 各地域におけるセキュリティコミュニティの形成を促進するため、モデルとなるようなコミュニティへのヒアリングを実施し、プラクティスとして公開。
- 合わせてコミュニティ形成に関連するセキュリティセミナー等への対応が可能な講師派遣制度のリスト、現在活動中の地域コミュニティのリスト及びコミュニティを可視化したマップを公開。

＜プラクティス集概要＞

対象コミュニティ

- 北海道地域情報セキュリティ連絡会
- 北海道中小企業サイバーセキュリティ支援ネットワーク
- サイバーセキュリティセミナー in 岩手
- 宮城県サイバーセキュリティ協議会
- みちのく情報セキュリティ推進機構　みちのく情報セキュリティ推進センター
- 地域中小企業における情報セキュリティの普及促進に関する検討会
- 名古屋中小企業IT化推進コンソーシアム
- 東海サイバーセキュリティ連絡会
- 関西サイバーセキュリティ・ネットワーク
- 総関西サイバーセキュリティLT大会
- 鳥取県サイバーセキュリティ対策ネットワーク
- セキュリティうどん
- 四国IT協同組合
- 九州地域の多様な地域団体とセキュリテベンダーとの連携による地域ニーズを踏まえた普及啓発活動の実践
- 九州経済連合会　サイバーセキュリティ推進WG
- 熊本県サイバーセキュリティ推進協議会
- 鹿児島県サイバーセキュリティ協議会

項目

1．コミュニティ設立の経緯・狙い
2．取組方針
3．協力機関・団体等との関係性
4．取組・イベント開催概要
5．実践からのプラクティス

サイバーセキュリティ人材施策の全体像

- 令和４年度、「サイバーセキュリティ経営ガイドライン」の付録として**「セキュリティ体制構築・人材確保の手引き」を改訂**。各組織における体制構築・資源確保に向けた具体的検討の流れをステップ・バイ・ステップで整理。
- サイバーセキュリティに関する**高度な知見等を有する人材の育成・確保に向けた施策**を進めるとともに、セキュリティを本務としない者が自らの業務遂行にあたってセキュリティを意識し、必要かつ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**「プラス・セキュリティ」の取組も推進**。

取組の全体像

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）

セキュリティ人材の育成

- ICSCoE中核人材育成プログラム
- 情報処理安全確保支援士
- セキュリティキャンプ

プラス・セキュリティの普及

- SC3産学官連携WGでのプラス・セキュリティ具体化
- NISCにおけるモデルカリキュラム策定
- 地域SECUNITYにおける人材育成

デジタルスキル標準の策定及び普及・
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

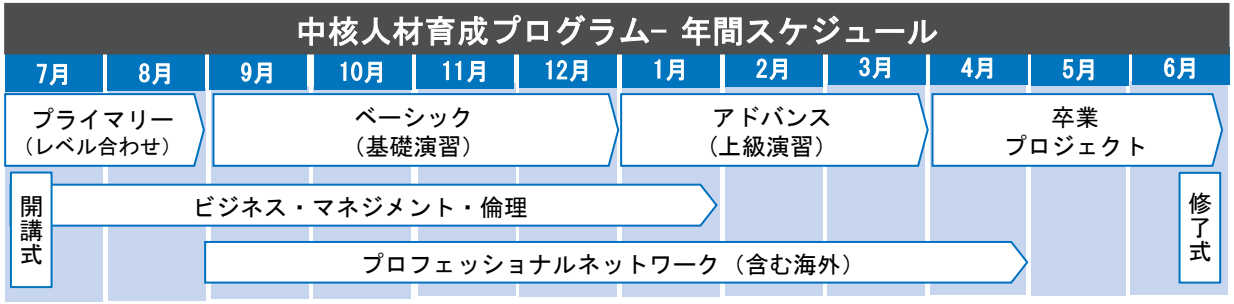
大学・高専等と産業界の連携

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

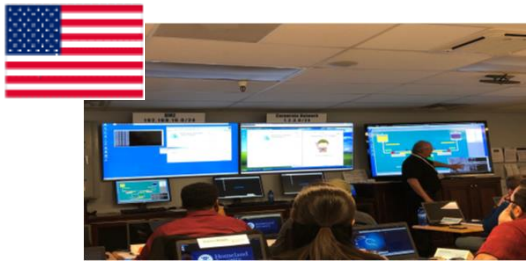
□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人）



- 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、自動車業界、スタートアップ企業の代表者等からの講義や意見交換を実施

➢ 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

など

産業サイバーセキュリティセンター（ICSCoE）2025Visionの達成に向けて

- サイバー領域の脅威がフィジカル領域に大きな影響を与える**DXが進んだ産業社会のサイバーセキュリティ対応能力の開発・普及を行う中核機関を目指す**。

事故調査の役割

幅広い分野のサイバー事故調査支援

世界に類を見ないユニークな機関

多様で実践的な研修プログラム

様々な分野の実環境の再現
外部機関の設備の活用

高い専門性・多様性

様々な分野・技術の専門家との
ネットワーク強化

最新情報の流通経路

OB会ネットワークの整備・組織化
OB人材活用

有能な人材輩出・知識のアップグレード

攻撃情報の分析・追究
カウンター能力とオープン・サイバーセキュリティ技術の開発

国際的な連携拠点

既存の国際交流活動の拡大・強化
JETRO・在外公館との連携強化

ICSCoE 2025Vision達成に向けたこれまでの取組

サイバーインシデント事故調査

- ✓ 高圧ガス保安法などの改正により、高圧ガス、ガス、電力分野において、サイバーインシデント事故調査規定を整備
- ✓ 対象事業者と協力し、事故調査フロー、調査内容等を整理
- ✓ IPA内の体制整備を実施中

最新情報の流通経路

- ✓ 修了者の活動基盤（修了者コミュニティ「叶会」）を整備するとともにコミュニティの規模を拡大
- ✓ 修了者のサイバーセキュリティ情報共有ツールを整備

世界に類を見ないユニークな機関

- ✓ １年間、アクティブラーニング形式の演習プログラムを実施
- ✓ セキュリティ啓発・インシデントレスポンス用のプラントを複数整備
- ✓ 流派の異なるユニークな講師による重層的教育及び受講者の自主研究を通じ、部門間のギャップを乗り越えるマインドセットを醸成

有能な人材輩出・知識のアップグレード

- ✓ サイバー攻撃の模擬的な実施など、試行錯誤できる環境を構築し、提供
- ✓ シン・テレワークシステムを構築
- ✓ 自治体テレワークシステム for LGWAN を開発し、7 万人の地方自治体の行政職員が利用

高い専門性・多様性

- ✓ 脆弱性を悪用したサイバー攻撃手法などを分類・整理した「MITRE ATT&CK※」へ情報を提供

※ MITRE（The MITRE Corporation）という米国連邦政府が資金提供している非営利組織が、脆弱性を悪用したサイバー攻撃を、戦術と技術または手法の観点で分類したナレッジベース。ATT&CKは、Adversarial Tactics, Techniques, and Common Knowledgeの略。

国際的な連携拠点

- ✓ フランス、英国、米国への派遣演習やイスラエルの特別講義を実施
- ✓ 日米欧演習等による対インド太平洋地域へのキャパビル支援を通じ、QUAD（日米豪印）等、国際枠組の協力に貢献

横断的な取組

- ✓ 世界最大級のセキュリティに関する国際イベント「Black Hat」やNATOサイバー防衛協力センター（CCDCOE）が主催する「Locked Shields」等、ハイレベルの会議・演習への参画
- ✓ 多様な専門性を有する人材（修了者）を輩出

ICSCoE 2025Vision達成に向けたアクションプラン

サイバーインシデント事故調査

- ✓ サイバーインシデント事故調査機能を整備
- ✓ 事故調査に備え、平時からサイバー攻撃と想定される事案に関する情報を収集し、最新の技術・ノウハウを蓄積
- ✓ 海外や国内の環境変化、サイバー事故の実態等を踏まえ、調査の在り方や対象について、継続的な検討を実施

世界に類を見ないユニークな機関

- ✓ 引き続き、“１年間”の演習プログラムを実施するとともに、2025年までに、教育グループを追加し、これまで卒業プロジェクトでカバーされていたセキュリティエンジニアリング並びにセキュリティサービス等の教育を実施
- ✓ 中核人材育成プログラムに派遣いただけていない業界等にアプローチするため、2025年までに短期コースや模擬プラントを拡充
- ✓ 教育グループを追加するために、2025年までに新規講師を育成・採用する「場」を整備

高い専門性・多様性

- ✓ トップレベルの国際的イベント等への参画、情報発信等を行うための方法論・インセンティブ制度を確立し、国際舞台で活躍する人材を拡大
- ✓ 各業界の専門人材を拡大するため、業界の特徴を理解する機会（ステークホルダーとの対話等）の拡大
- ✓ AI等、先端技術のサイバーセキュリティリスクの検証・対策の立案を実施・指導できる人材の拡大
- ✓ 各国・各言語圏に通じた修了者を把握する仕組みの整備、認知度拡大に向けた海外専門機関との関係構築

最新情報の流通経路

- ✓ 叶会を活用し、攻撃情報等をICSCoE関係者間で共有する仕組みを構築
- ✓ 叶会を通じた情報共有機能の強化を目的として、叶会の活動を対外的に発信するための基盤を整備
- ✓ 叶会から国の有識者検討会に参画する者を輩出するなど、活動の場を更に拡大
- ✓ 叶会の安定運営に向けた運営方針を決定

有能な人材輩出・知識のアップグレード

- ✓ サイバー技術研究室のような試行錯誤空間をスケールさせる
- ✓ IPA内だけでなく、関係省庁や民間企業との連携を強化し、各組織のキャパビルを強化
- ✓ コード群を含め、サイバー技術に関する基本文献集を整備
- ✓ 実験的にネットワークインフラの構築を容易とする環境やツール等を開発

国際的な連携拠点

- ✓ 海外におけるOTセキュリティの人材育成等についての調査、各地域のハブとなる海外機関等とのネットワーキング、ベストプラクティスの共有等を実施
- ✓ 海外関係機関・産業界と国内インフラ企業に所属する中核人材育成プログラム受講者をつなぐ橋渡し人材の育成に向け、修了者等による海外人脈相談対応、国際経験蓄積機会提供等を実施
- ✓ ICSCoEの発信力強化に向け、海外発信が効果的な卒プロの英訳や国際会議での発表等を支援し、その活動を国内外に発信

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最新の知識・技能を備えた専門人材の国家資格として、「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。
- 2024年４月１日時点の登録者数は22,692人。
- 2020年５月より、**登録に３年間の有効期限**を設け、**更新が行われない場合**には、**登録が失効**する**更新制を導入**。

◆ 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、さらに民間企業等が人材を活用できるよう登録簿を整備。**

◆ 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。

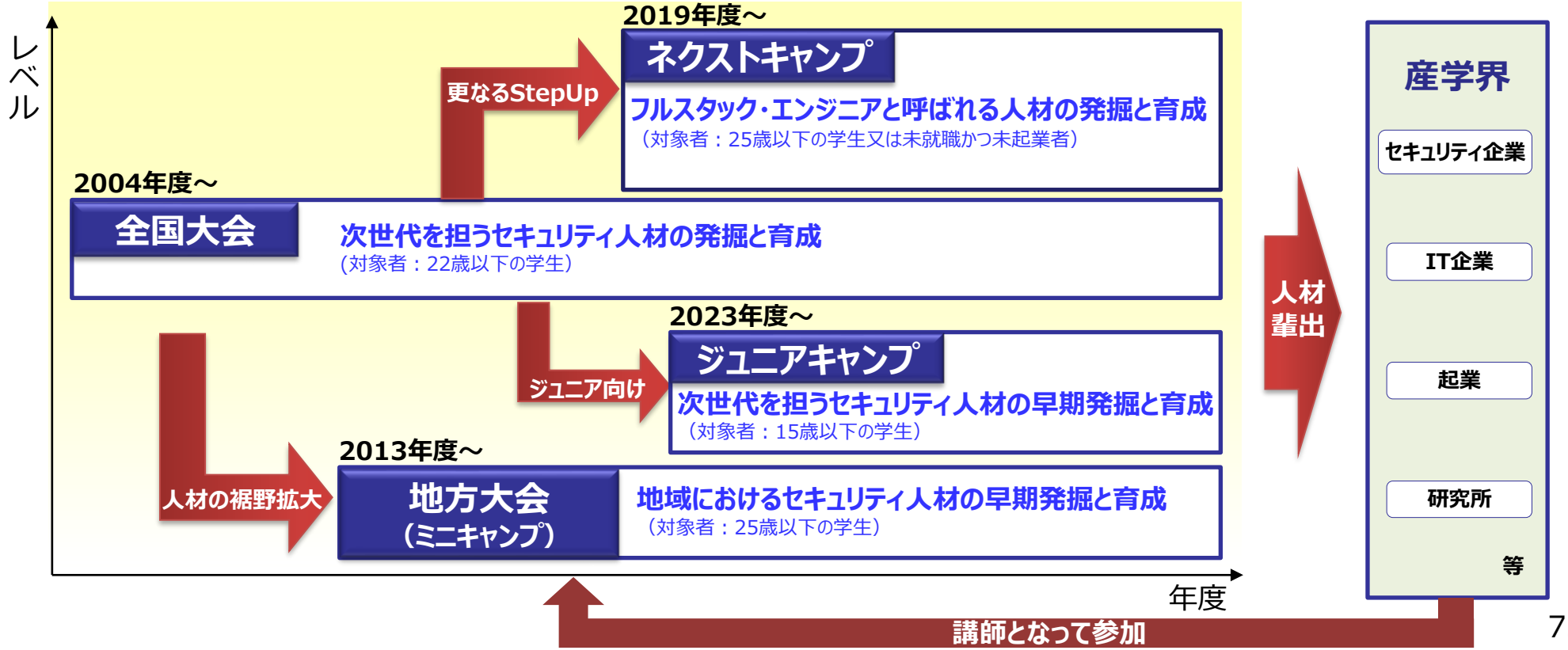
➡ **有資格者の継続的な知識・技能の向上を図るため、講習の受講を義務化。**
※登録の更新制導入により、義務講習を受講したもののみ登録を更新。

◆ 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。**

セキュリティ・キャンプ

- 複雑かつ高度化しているサイバー攻撃に適切に対応するため、**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人材を創出**することが必要。
- IPAとセキュリティ・キャンプ協議会は、選抜された22歳以下の学生・生徒を対象とした、次代を担う情報セキュリティ人材発掘・育成する「**セキュリティ・キャンプ全国大会**」を開催。**最新ノウハウも含めたセキュリティ技術を、倫理面と併せ、第一線の技術者から伝授**。2004年度の開始からこれまでに、累計で**1,152名**が修了。
- 2019年度からは、全国大会修了生の次のステップとして、選抜された25歳以下の学生・生徒等を対象とした、**情報セキュリティの多様なシーンに対応し新たな価値を生み出していけるトップオブトップの人材（フルスタック・エンジニア）を発掘・育成する「セキュリティ・ネクストキャンプ」**を開催。これまでに累計で**43名**が修了。また、2023年度からは、全国大会の一部ゼミとして開催していたジュニアゼミを、「**セキュリティ・ジュニアキャンプ**」として、15歳以下の生徒を対象に開催。



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6回開催。
- 本演習は、**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、**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**とし、 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**、及び**参加者間のネットワーキング**を行うことができるものとなっている。

2023年演習の概要

- **日時**：2023年10月9日～13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

※写真は昨年演習（2023年10月）の内容

参考資料

①サプライチェーン全体での対策強化
②国際連携を意識した認証・評価制度等の立上げ
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新たな攻撃を防ぎ、守るための研究開発の促進
（サイバーセキュリティ産業振興）
⑤政府全体の動向

2023年度の国際連携の取組　（2023年4月～2024年３月）

- 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セキュリティ適合性評価制度**：同様に検討を進めている**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。
- **SBOM（ソフトウエア部品表）**：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：11/14 日米経済版2+2閣僚会合
  - 欧：7/3日EUデジタルパートナーシップ閣僚会合、11/22日EUサイバー協議
  - シンガポール：10/16-19シンガポールサイバーセキュリティウイーク
  - 英：1/16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。2023年は10/9-13に東京で４年ぶりに対面実施。
  - その他連携：10/3日ASEAN政策会議、10/5-6日ASEAN50周年記念官民共同フォーラム　等

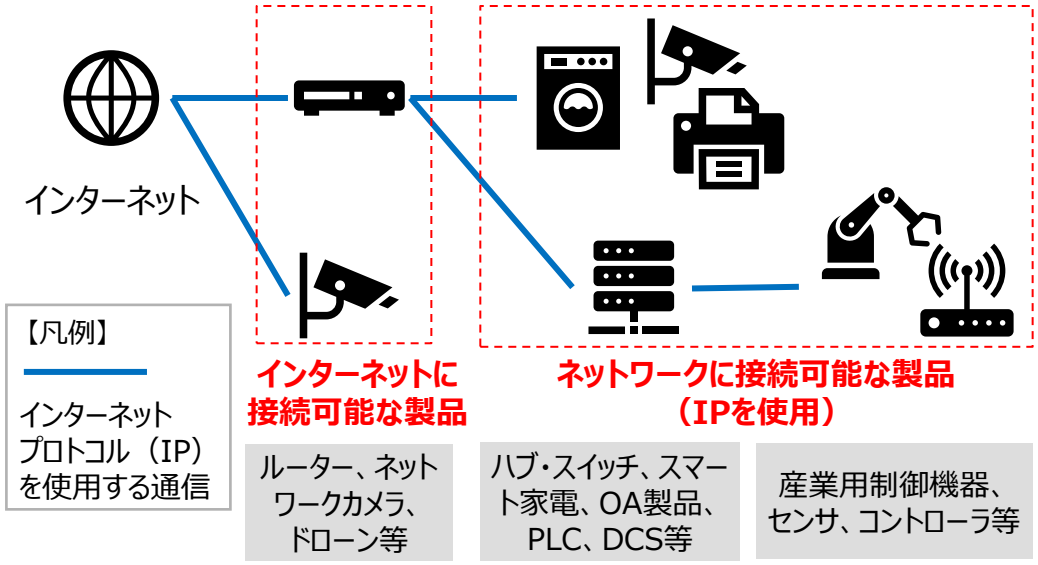
③幅広い有志国との連携

- 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（7/11中谷副大臣（当時）イスラエルサイバー総局訪問、9/4閣僚級経済イノベーション政策対話）
  - インド（9/14日印サイバー協議）
  - フランス （11/20日仏サイバー協議）
  - 豪州（12/4日豪サイバー協議）
  - 日米豪印（5/20首脳会合、11/2・12/5-12/6上級サイバーグループ会合）　　等

IoT製品に対するセキュリティ適合性評価制度の概要

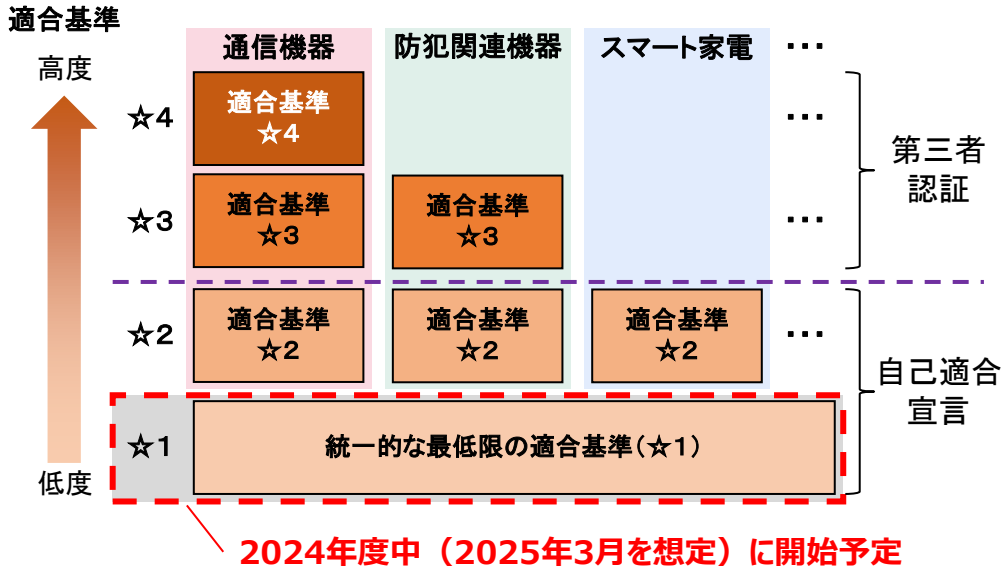
- 2022年11月より「**IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会**」を開催。**2024年3月15日に最終とりまとめを公開し、制度構築方針案のパブコメを開始。**
- **インターネットに直接接続されない製品も含め、幅広いIoT製品を対象**としつつ、製品ごとの特性に応じた基準を既存の制度を活かしながら設けられるよう、**複数のレベル（☆１～☆４）を用いた制度**を想定。
- 制度を広く普及させるため**☆１～２は自己適合宣言によるラベル付与**とし、高い信頼性が求められる**☆３以上は独立した第三者による評価を受ける第三者認証**とする。
- 検討会の最終とりまとめを踏まえ、**☆１については2024年度中の制度開始**を予定。**政府調達等の要件等とすべく関係省庁と議論中**。併せて、**米欧等の諸外国との制度調和を図るため議論中**。

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。

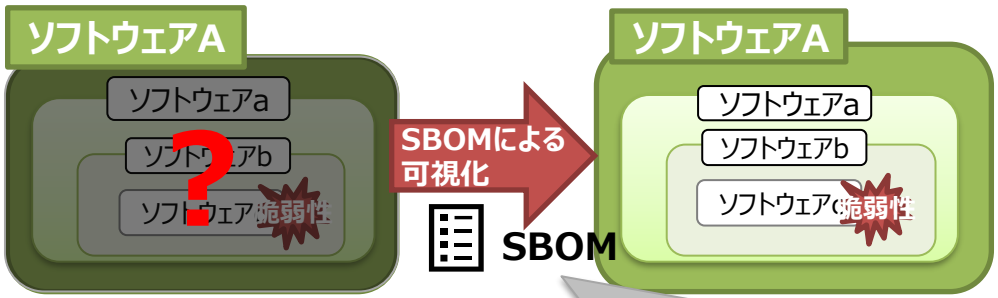
制度の概要



ソフトウェア・セキュリティ確保手段としてのSBOM

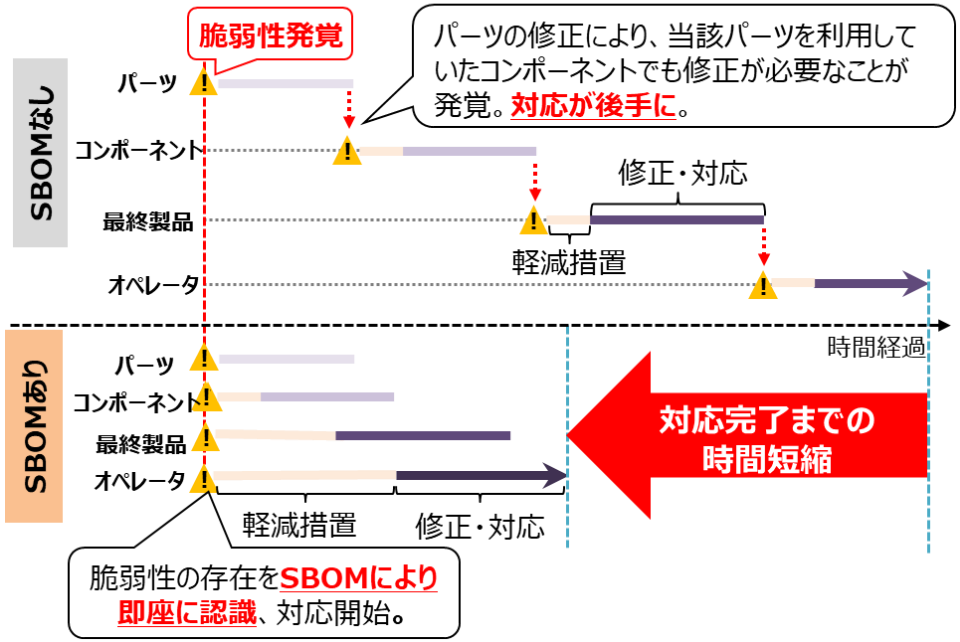
- SBOM （Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。ソフトウェアを構成する**各部品（コンポーネント）を誰が作り、何が含まれ、どのような構成となっているか**等を示す。
- SBOMによりソフトウェアの構成情報を詳細に把握することができるため、脆弱性情報の即時の特定が可能であり、**脆弱性対応などへの活用が期待**できる一方、その作成効果やコストなどの課題が存在するため、実証による検証を実施。
- 2023年7月、**「ソフトウェア管理に向けたSBOMの導入手引」きを公表**。SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示す。

＜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



ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引　～全体概要～　（2023年7月策定）

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（OSS）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を活用することで効率的なソフトウェア管理を実施できることが確認できた一方で、実際のSBOM導入に際しては様々なハードル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SBOMに関する誤解と事実を提供**するとともに、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導入にあたって認識しておくべきポイント**を示す。

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

※ このうち、以下に示すようなSBOM初級者を特に対象としている。

- ソフトウェアにおける脆弱性管理に課題を抱えている組織
- SBOMという用語は聞いたことがあるが具体的な内容やメリットは把握できていない組織
- SBOMの必要性は理解しているが、導入に向けた取組内容が認識できていない組織　など

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

フェーズ1　環境構築・体制整備フェーズ

- **1-1. SBOM適用範囲の明確化**
  - ✓ SBOMを作成する対象ソフトウェアに関する情報（言語、開発ツール、構成図、契約形態・取引慣行、規制要求事項、SBOM導入に関する組織内の制約等）を整理する。
  - ✓ 整理した情報を踏まえて、SBOM適用範囲を明確化する。
- **1-2. SBOMツールの選定**
  - ✓ SBOMツールの選定の観点を整理し、当該観点に基づきSBOMツールを評価・選定する。
    （選定観点の例：機能、性能、解析可能な情報・データ形式、コスト、対応フォーマット、解析方法、サポート体制、他ツールとの連携、ユーザーインタフェース、対応する言語、日本語対応等）
- **1-3. SBOMツールの導入・設定**
  - ✓ SBOMツールが導入可能な環境の要件を確認し、整備する。
  - ✓ 取扱説明書等を確認して、SBOMツールの導入・設定を行う。
- **1-4. SBOMツールに関する学習**
  - ✓ 取扱説明書等を確認して、SBOMツールの使い方を習得する。
  - ✓ ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する。

フェーズ2　SBOM作成・共有フェーズ

- **2-1. コンポーネントの解析**
  - ✓ SBOMツールを用いて対象ソフトウェアのスキャンを行い、コンポーネントの情報を解析するとともに、コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れが無いかを確認する。
  - ✓ SBOMツールを用いることで、手動の場合と比較して効率的にコンポーネントの解析及びSBOMの作成を行うことができる。
  - ✓ パッケージマネージャーを用いることで、SBOMツールでは特定できない粒度の細かいコンポーネントを特定できる場合がある。
- **2-2. SBOMの作成**
  - ✓ 作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定し、当該要件を満足するSBOMを作成する。
- **2-3. SBOMの共有**
  - ✓ 対象ソフトウェアの利用者及びサプライヤーに対するSBOMの共有方法を検討した上で、当該方法に基づきSBOMを共有する。

フェーズ3　SBOM運用・管理フェーズ

- **3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施**
  - ✓ 脆弱性に関するSBOMツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応を行う。
  - ✓ ライセンスに関するSBOMツールの出力結果を踏まえ、OSSのライセンス違反が発生していないかを確認する。
- **3-2. SBOM情報の管理**
  - ✓ SBOMに含まれる情報やSBOM自体を適切に管理する。
    ※ SBOMの管理は、組織内のPSIRTに相当する部門が対応することが効果的
  - ✓ 自動で脆弱性情報が更新・通知されるSBOMツールを用いることで、新たな脆弱性に関する情報を即座に把握することができる。ツールを用いた自動管理ができない場合、担当者を別途設置するなど運用面でカバーする。

日米豪印（Quad（クアッド））第５回首脳会合について

- **2023年5月20日（土）、第５回日米豪印（通称「Quad（クアッド）」）首脳会合を広島で対面開催。**
  第１回：2021年３月（オンライン）、第２回：同９月（米国）、第３回：ウクライナに関する臨時会合 2022年3月（オンライン）、第４回：同5月（日本）
- また会合後、**４カ国は共同声明を発出。**経産省関連では、**サイバーセキュリティ、重要・新興技術、気候、インフラ、宇宙等での新たな協力を進めること**が記載された。

首脳共同声明（サイバーセキュリティ部分抜粋）

- 我々は、より安全なサイバー空間と、全ての人々のためになる国際デジタル経済を促進することへのコミットメントを再確認する。**日米豪印パートナーは、サイバー事案及び脅威への地域の能力及び強靱性を高めるため、引き続き協働する。**
- 地域のサイバー人材の能力向上支援を継続、サイバーセキュリティの啓発を目的とした**「日米豪印サイバー・チャレンジ」**の実施を歓迎。
- ソフトウェアの開発、利用、政府調達に係るセキュリティ向上を奨励する**「ソフトウェア・セキュリティに関する日米豪印共同原則」**及び**「重要インフラのサイバーセキュリティに関する日米豪印共同原則」**の発表を歓迎。

ソフトウェアセキュリティに関する共同原則（抜粋）

ソフトウェアベンダーによる安全な開発の実践に関する原則

安全なソフトウェア開発手法が実践されたソフトウェアを調達するため、当該手法を実践することを政府方針に取り入れるとともに、**ソフトウェアベンダーに対して、当該手法の実践を推奨**することを目指す。

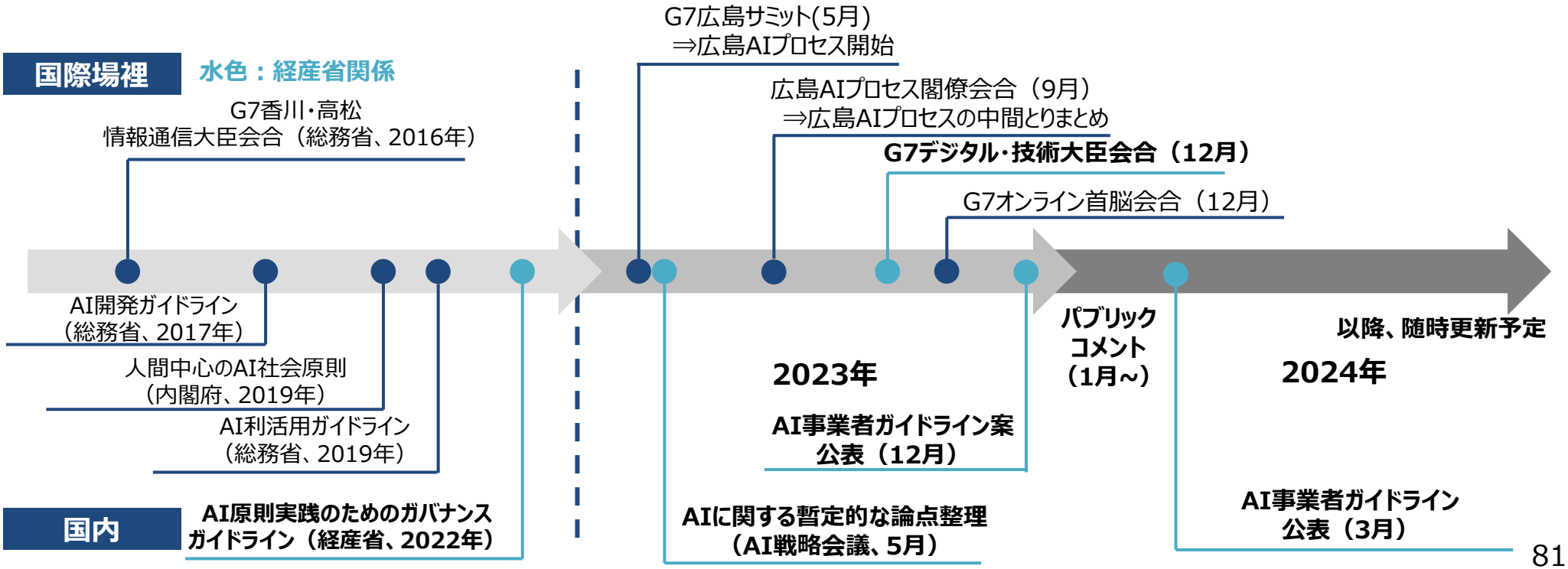
- **組織の準備**
  安全なソフトウェア開発手法を実践するため、適切な教育を受けた人材、プロセス、技術を適切に整備する。
- **ソフトウェアと開発環境の保護**
  ソフトウェアに含まれるコンポーネントを、改ざんや不正アクセスから適切に保護する。また、ソフトウェアは、リリースされたバージョンごとに管理し、バージョンごとに使用されているコンポーネントの詳細情報（**SBOM等**）やサプライチェーン情報を適切に管理する。
- **安全なソフトウェアの開発**
  脆弱性を最小限に抑え、セキュリティに関するテストを経て十分なセキュリティを備えたソフトウェアをリリースする。
- **脆弱性への対応**
  ソフトウェアに存在する脆弱性を特定し、特定した脆弱性に適切な対処を行い、同様の脆弱性が今後発生することを防止する。

外務省HP：https://www.mofa.go.jp/mofaj/fp/nsp/page1_001702.html

AIのルールメイキング（背景・経緯）

- 生成AIの出現を受けて、**AIのルールメイキングの必要性が一層高まる**
- 国際場裡では、G7広島サミット（2023年5月）において、岸田総理が「**広島AIプロセス**」の立ち上げを発表。総務省を中心に議論を進め、「**広島AIプロセス包括的政策枠組**」として閣僚級で成果をとりまとめ（2023年12月1日）、首脳級で最終合意（2023年12月6日）
- 国内では、「**AIに関する暫定的な論点整理**」（2023年5月、AI戦略会議）を踏まえ、総務省・経済産業省を事務局に、**既存のガイドラインを統合・アップデート**（注）し、**広範なAI事業者を対象にしたガイドライン案をとりまとめ（第7回AI戦略会議において発表。1月からパブコメを実施、3月に公表）**

（注）AI開発ガイドライン（2017年、総務省）、AI利活用ガイドライン（2019年、総務省）、**AI原則実践のためのガバナンスガイドライン（2022年、経済産業省）**



AIのルールメイキング（AI事業者ガイドライン）

- AIの活用に**一律に事前規制を課すのではなく、イノベーションの促進と規律のバランスを確保を重視**
  ⇒ **ガイドラインという「ソフトロー」の形式**（遵守のために適切なAIガバナンスを構築するなど、**事業者の具体的な取組を自主的に推進**することが重要）
- 「**AIに関する暫定的な論点整理**」（2023年5月、AI戦略会議）を踏まえ、総務省・経済産業省を事務局に、**既存のガイドラインを統合・アップデート**（注）し、**広範なAI事業者を対象にしたガイドライン案**をとりまとめ。
- **広島AIプロセス（2023年12月に閣僚級、首脳級で成果をとりまとめ済み）**を含む国際的な動向を取り込むとともに、**マルチステークホルダー・アプローチを重視**。総務省、経産省の検討会及びWGを活用し、**産業界、アカデミア及び市民社会の多様な意見**を聴取

（注） AI開発ガイドライン（2017年、総務省）、AI利活用ガイドライン（2019年、総務省）、**AI原則実践のためのガバナンスガイドライン（2022年、経済産業省）**

本編

紺色：広島AIプロセス成果物の国内担保箇所

総論

第１部　AIとは

第２部　AIにより目指すべき社会と各主体が取り組む事項
- A　基本理念
- B　原則
- **C　共通の指針（一般的なAIシステム）**
- **D　高度なAIシステムに関係する事業者に共通の指針**
- E　AIガバナンスの構築

第３部　AI開発者に関する事項
データ前処理・学習時、AI開発時、AI開発後、**国際行動規範の遵守**

各論

第４部　AI提供者に関する事項
AIシステム実装時、AIシステム・サービス提供後、**国際指針の遵守**

第５部　AI利用者に関する事項
AIシステム・サービス利用時、**国際指針の遵守**

別添

簡潔な本編を補完すべく、以下の内容を盛り込む
- AIシステム・サービスの例（各主体の関係性等を含む）
- AIによる便益や可能性、具体的なリスクの事例
- ガバナンス構築のための実践ポイント、具体的な実践例
- 本編の各項目に関するポイント、具体的な手法の例示、分かりやすい参考文献　等

（上記に加え）
- 「AI・データの利用に関する契約ガイドライン」を参照する際の主な留意事項
- チェックリスト
- 主体横断的な仮想事例
- 海外ガイドラインとの比較表

AI事業者ガイドライン案を検討している総務省、経済産業省の関連会議体

総務省
- AIネットワーク社会推進会議
  （議長：須藤 修
  中央大学国際情報学部教授）
- 同　AIガバナンス検討会
  （座長：平野 晋
  中央大学国際情報学部教授）

経済産業省
- AI事業者ガイドライン検討会
  （座長：渡部 俊也
  東京大学未来ビジョン研究センター教授）

AIセーフティ・インスティテュート

- 国際的にAIガバナンスの焦点は、対象となるAIを限定した**履行確保（特にAIの市場導入前の安全性評価）に収斂**（注）
- 我が国においても、**国際的な基準と整合的なAI評価手法を策定**するとともに、**国自身がAIの安全性に関する開発者の知見を獲得**する必要。
- 第7回AI戦略会議（昨年12月）において、**岸田総理からAIセーフティ・インスティテュート（AISI）を設置する旨を対外公表**（**情報処理推進機構（IPA）**に設置。**政府関係機関の協力を得て**、各国・AI開発者との連携を担う）

（注）米国では**開発者の自己評価結果を政府に対し報告する義務**を課し、英国では**AISIが対象事業者のAIを評価**する方向

AIセーフティ・インスティテュートの概要

名　称

（日本語）AIセーフティ・インスティテュート
（英　語）Japan AI Safety Institute

業　務

1．安全性評価に係る調査、基準等の作成

2．安全性評価の実施手法に関する検討

3．他国の関係機関（英米のAI Safety Institute等）との国際連携に関する業務

関係機関

内閣府（科学技術イノベーション）、国家安全保障局、内閣サイバーセキュリティセンター、デジタル庁、総務省（情報通信研究機構）、外務省、文科省（理化学研究所）、経済産業省（情報処理推進機構、産業技術総合研究所）、防衛省等

※関係機関は現時点での予定

参考資料

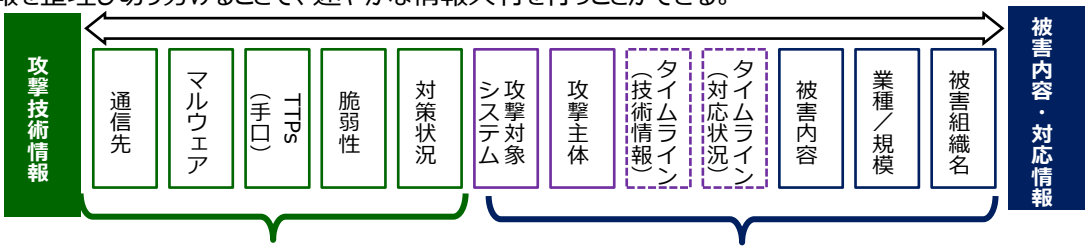
①サプライチェーン全体での対策強化
②国際連携を意識した認証・評価制度等の立上げ
③政府全体でのサイバーセキュリティ対応体制の強化
④新たな攻撃を防ぎ、守るための研究開発の促進
（サイバーセキュリティ産業振興）
⑤政府全体の動向

サイバー被害に係る情報共有ガイダンスの策定

- 攻撃手法が高度化する中で、単独組織による攻撃の全容解明はより困難になっている。他方で、被害組織はお互いに「他にどのような情報が存在するかを知ることができない」ため、情報共有がなかなか行われにくく、また、共有タイミングも遅いケースが多い。
- 第三者との関係などサイバー攻撃被害が複雑化する中で、被害組織のインシデント対応が適切になされているかどうかが外部から確認できず、また、被害組織も被害公表を通じた情報の開示に消極的なため、被害組織によるインシデント対応（結果）に不安や警戒を募らせるような状況になっている。
- ガイダンスでは、被害組織の担当部門（例：セキュリティ担当部門、法務・リスク管理部門等）を主な想定読者とし、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FAQ形式で整理。

どのような情報を？（様々な種類・性質の情報が存在）

情報を整理し切り分けることで、速やかな情報共有を行うことができる。



基本的に個別の被害組織には紐づかず、対応初期で見つかりやすく、早期に情報共有しなければ効果を得られない情報

ある程度調査期間を経なければ判明しない情報や、ステークホルダー等との調整が必要な機微な情報などが含まれるため、公表までに時間がかかる情報

どのタイミングで？（サイバー攻撃への対処の時系列を意識）

どのような主体と？（様々なサイバーセキュリティ関係組織が存在）

想定読者（被害組織等）

サイバー攻撃被害に係る情報の共有・公表ガイダンス ～情報共有・被害公表のポイント～

本ガイダンスは、被害組織で見つかった情報を「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」共有／公表するのか、ポイントを整理したものです。

1.情報共有

- **(1)目的：**被害調査に必要な情報の提供や被害の未然防止に資する【→概要8ページ】
- **(2)タイミング：**情報共有と被害公表を分離し、迅速な情報共有を図る【→概要9ページ】
- **(3)情報の整理：**攻撃に関する情報（攻撃技術情報）と被害に関する情報（被害内容・対応情報）を分離し、迅速な攻撃技術情報の共有を図る【→概要10ページ】

2.被害公表

- **(1)目的：**レピュテーションリスク低下やインシデント対応上の混乱の回避に資する【→概要11ページ】
- **(2)タイミング：**攻撃の種類や被害の状況から、効果的な公表タイミングを選ぶ【→概要12ページ】
- **(3)情報の整理：**専門組織との連携や情報共有活動の状況など対応の経緯等を含めて示すことで、ステークホルダーの不安等を解消することができる【→概要13ページ】

3.外部組織との連携

- 専門組織との連携、警察への通報・相談、所管官庁への報告等を実施することで、正確な情報共有や注意喚起、捜査を通じた犯罪抑止や広く国民に影響する事案への対処等につなげることができる【→概要14ページ】

4.機微な情報への配慮

- 被害者への保護や機微な情報への配慮が必要な情報の取扱いを知ることで、スムーズな情報共有、被害公表を行うことができる【→概要15ページ】

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**。

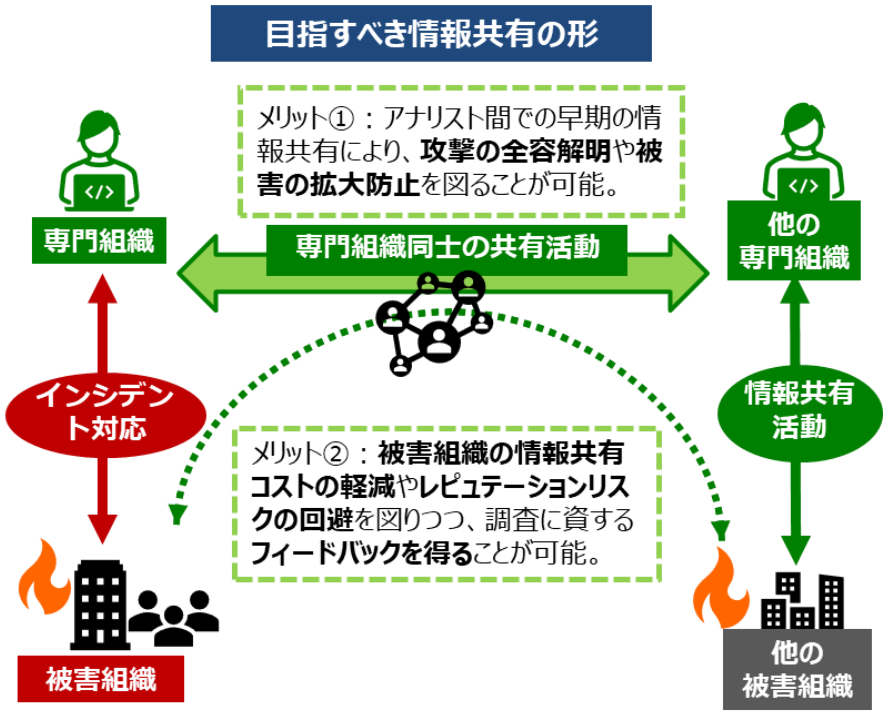
３．今後の課題

- 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。

サイバー被害情報の情報共有の更なる促進に向けた対応

- 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**。
- これまで、①**被害組織における情報共有・公表**に関する検討及び②**専門組織を通じた速やかな情報共有**について検討を実施し、それぞれの組織において**実務上参考となるガイダンスや手引き等を整備**。
- 今後、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。

＜参考＞専門組織を通じた速やかな情報共有の促進に向けた対応

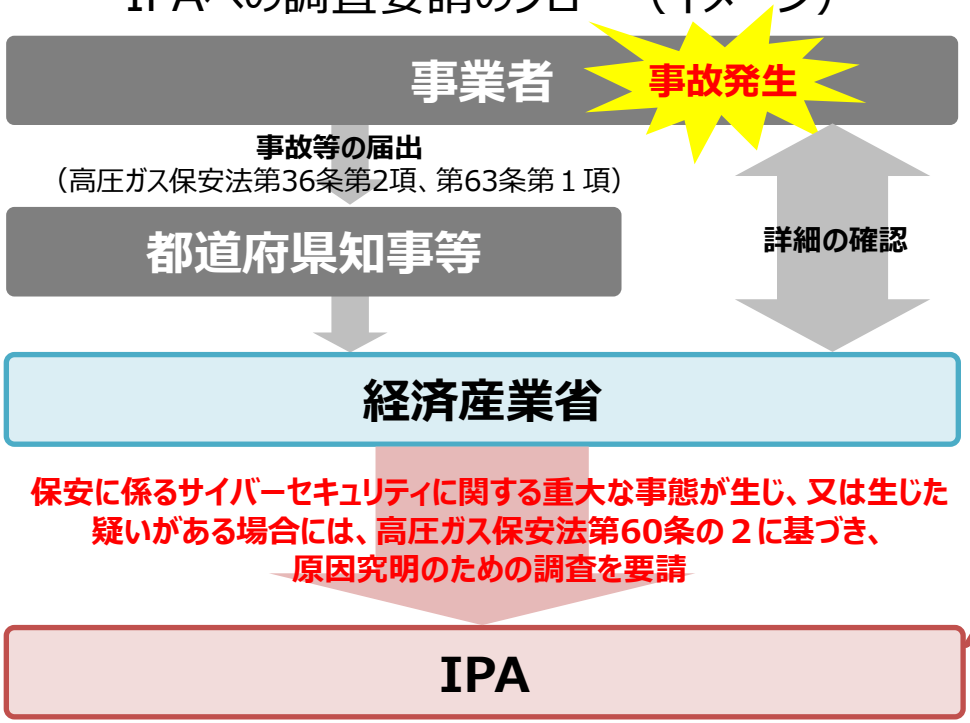


- 最終報告書において、**被害組織の同意を個別に得ることなく専門組織間で速やかに情報共有することが可能な情報として「攻撃技術情報」**※**を整理**し、そうした考え方に基づく専門組織間での円滑な情報共有を提言。
  ※通信先情報やマルウェア情報などから被害組織が推測可能な情報を非特定化したもの。
- 最終報告書の**提言を補完する２つの文書**（以下①②）**を提示**。
  ① 専門組織向けに、**効果的な共有対象となる情報や非特定化加工の方法**といった専門組織同士の情報共有における論点について、複数のユースケースも用いつつ解説した**手引き**（案）
  ② 被害組織と専門組織が共通の認識を持ち、情報共有について合意するための**秘密保持契約に盛り込むべきモデル条文案**
- さらに、最終報告書では、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、情報共有に向けた官民連携のあり方 、サプライチェーンにおけるベンダ等の役割について提言**。

保安に係るサイバーインシデントに関する事故調査の実施

- 諸外国においては、サイバー攻撃による石油パイプラインの操業停止や、電力関連施設へのサイバー攻撃による停電といった事案が発生しており、我が国においても、**産業保安関連設備に対するサイバー攻撃のリスクが懸念**。
- 令和４年に公布された改正保安3法に基づき、**サイバーセキュリティに関する重大な事態が生じ、又は生じた疑いがある場合**には、国は、**独立行政法人情報処理推進機構（IPA）に原因究明調査を要請。**
- 事故調査は、**原因究明による再発防止を目的に実施**。調査結果を踏まえ、サイバーセキュリティ水準の向上を図るための対策を講じることを想定。**令和５年12月21日の施行**に伴い、**IPAにおいて体制を整備。**

IPAへの調査要請のフロー（イメージ）



IPAによる調査のイメージ

- ✓ IPAは対象システムのログ等を確認することによって、サイバーセキュリティに関する重大な事態が生じた原因を究明するための調査を行う。
- ✓ IPAによる調査は、書面審査と現地調査の二段階で構成する。
  ※ただし、書面調査のみで十分に原因を特定できた場合には、現地調査は行わない。
- ✓ 調査日数や調査内容等は、IPAと事業者で相談の上、決定する。

改正高圧ガス保安法
第六十条の二　経済産業大臣は（中略）**保安に係るサイバーセキュリティ（中略）に関する重大な事態が生じ、又は生じた疑いがある場合**において、必要があると認めるときは、**独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる**。

参考資料

①サプライチェーン全体での対策強化
②国際連携を意識した認証・評価制度等の立上げ
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新たな攻撃を防ぎ、守るための研究開発の促進
（サイバーセキュリティ産業振興）
⑤政府全体の動向

検証基盤の構築（「Proven in Japan」）に向けたこれまでの取組

	主な内容	これまでの取組・成果
緑 セキュリティ製品の有効性検証	サイバー攻撃に対応するセキュリティ製品分野を公表し、その分野に該当する我が国発の製品について、専門家による有効性確認を実施し、その内容を発信することで、ユーザーが我が国発の製品を選定しやすい環境を構築。	・試行導入・導入実績公表の手引き（2021年4月公開）やセキュリティ製品・サービス重要分野マップ（2022年3月改訂）等を公開。
青 実環境における試行検証	実環境への試行導入・実績公表を行う企業向けの手引きを作成するとともに、試行導入に関心があるユーザーとベンダーをマッチングし、我が国発のセキュリティ製品の試行導入・実績公表を促進。	
赤 攻撃型を含めたハイレベルな検証	機器のハイレベル検証(ペネトレーションテスト)の方法や人材育成の方法を整理・公開。産業機器等を対象に検証も実施し、その方法の有効性を確認。	・サービス事業者と検証依頼者が実施すべき事項等を整理した手引きを公開（2023年6月改訂）。 ・機器検証サービスの運営開始（2023年3月から審査登録制度に追加、現状登録されているサービスは8件）
開発 セキュリティ・バイ・デザインを実現する開発段階検証	開発段階から、設計書とソースコード、実装したプロトタイプで検証を行い、脆弱性を排除した開発を実施することにより、効果的な検証の進め方を整理するとともに、開発段階からの検証の効果を可視化。これにより、設計段階からセキュリティを意識する「セキュリティ・バイ・デザイン」の考え方を採り入れ、コスト低減を図りつつ、中小企業に検証の必要性を認知してもらうことを目指す。	・検証事業者や製品ベンダが参照するための手引きを公開（2023年9月公開）。 ・ものづくり補助金において、当該補助金を活用して開発・導入した製品やサービス、システムに対するペネトレーションテスト・脆弱性診断も支援対象として追加（第15次公募（2023年4月）から開始）。

情報セキュリティサービス審査登録制度

- 情報セキュリティサービス業の普及を促進し、**国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的**として、**一定の技術・品質要件を定めた「情報セキュリティサービス基準」を経産省が2018年より策定**し、基準に適合する**サービスのリストをIPAが公開中**（2023年12月時点で、300サービスが登録中）。
- 2024年4月より、事業者からの要望を踏まえ、**「ペネトレーションテスト（侵入試験）サービス」を既存区分のオプションサービスとして追加。**

<情報セキュリティサービスにおける課題>

どの事業者のサービスを選べば良いかわからない

信頼できるサービス事業者にお願いしたい

ユーザ
（企業、政府機関等）

我が社のサービスを もっと見つけて欲しい

我が社の技術力、サービス 品質をアピールしたい

ベンダー
サービス提供事業者

審査を受けリストに掲載

選定時に活用

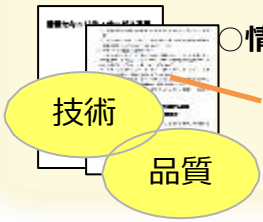
○情報セキュリティサービス基準適合サービスリスト（IPA）

審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開

基準を満たした300サービスを掲載

- 情報セキュリティ監査（68サービス）
- 脆弱性診断（135サービス）
- ペネトレーションテスト（侵入試験）（2024年9月審査開始）
- デジタルフォレンジック（38サービス）
- セキュリティ監視・運用（51サービス）
- 機器検証 （8サービス）

（2023年12月現在）



○情報セキュリティサービス基準（METI）

上記６サービスに関して技術要件・品質管理要件を定めた基準

本制度を通じて目指す社会

専門知識を持たないユーザでも、自社に最適かつ品質を備えたサービスを選択できる

技術と品質を備えた情報セキュリティサービスの普及・発展

制度の普及・浸透

参考資料

①サプライチェーン全体での対策強化
②国際連携を意識した認証・評価制度等の立上げ
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新たな攻撃を防ぎ、守るための研究開発の促進
（サイバーセキュリティ産業振興）
⑤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。

（出典）国家安全保障戦略（令和４年12月16日閣議決定）より抜粋

サイバーセキュリティ戦略2021：「Cybersecurity for All」を踏まえた対応の強化

サイバー空間の課題認識

- あらゆる主体が参画する公共空間化
- サイバー・フィジカルの相互連関・連鎖の深化
- サイバー攻撃の複雑化・巧妙化
- 安全保障上の脅威の増大

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

個人		組織	
DXに向き合う**地方、中小企業、若年層、高齢者等**	目に見えないリスクと向き合う**個人・組織**	サイバー攻撃による**重要インフラ**停止、知財の窃取、金銭被害等の増大	**国家の関与**が疑われる攻撃

DXとサイバーセキュリティの同時推進

○デジタル改革と一体で：**経営層の意識改革、地域・中小企業の取組促進**
（経営インセンティブ、安価かつ効果的な支援サービス・保険の普及）

○誰も取り残さないリテラシーの向上と定着
（高齢者向けデジタル活用支援講習会との連携、GIGAスクール構想にあわせた普及啓発、サイバー防犯ボランティア）

安全保障の観点からの取組強化

○中露北からの脅威等を踏まえた外交・安全保障上のサイバー分野の優先度向上

○防衛省・自衛隊におけるサイバー防衛能力の抜本的強化

○「妨げる能力」、外交的手段や刑事訴追等を含めた対応、日米同盟の維持・強化

○**国際協力・連携**

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

○**国民・社会を守るためのサイバーセキュリティ環境の提供**
（**産業横断的なサプライチェーン管理**、サイバー犯罪対策、クラウドサービス利用のための対策の多層的な展開、経済安全保障の視点を含むサイバー空間の信頼性確保）

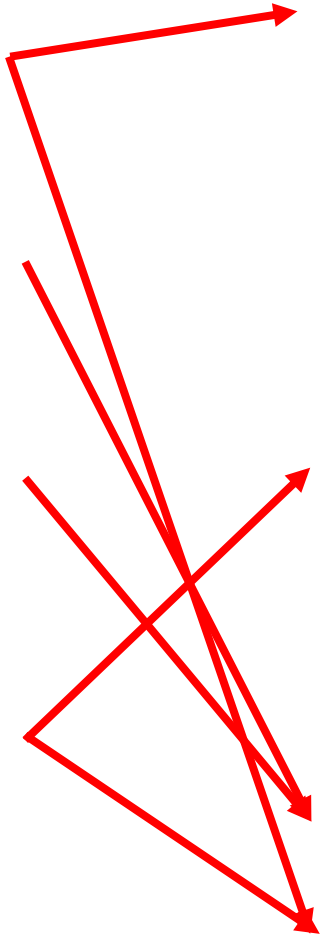
○深刻なサイバー攻撃から国民生活・経済を守る**包括的なサイバー防御等の展開**
（**情報収集から対処調整、政策措置までの一体的推進の総合調整を担うナショナルサートの機能強化**、政府機関・重要インフラ等の各主体のセキュリティ対策）

※赤字は経済産業省が主体的に関与

サイバーセキュリティ戦略と今後の産業サイバーセキュリティ政策との関係①

サイバーセキュリティ対策の実効性強化

- サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討
- ガイドライン等の実効性の強化（セキュアなIoT製品及びソフトウェアの流通に向けた取組等）
- 半導体関連産業におけるセキュリティの確保に向けた検討の開始
- サプライチェーン全体での対策強化（中小企業等向けの支援の一層強化）



サイバーセキュリティ戦略（令和３年９月）

4.1.1 経営層の意識改革

（略）これらを踏まえつつ、デジタル化と一体となったサイバーセキュリティ強化に向けた取組状況が、サステナビリティを重視する投資家等のステークホルダーに可視化され、かつそうした取組に対しインセンティブが生まれるよう取り組む。

4.1.2 地域・中小企業における DX with Cybersecurity の推進

（略）ビジネスマッチングや人材の育成・マッチング、地域発のセキュリティソリューションの開発など、リソース不足を踏まえた地域による課題解決・付加価値創出が行われる場の形成を促進する（略）中小企業が利用しやすい安価かつ効果的なセキュリティサービス・ 保険の普及など、中小企業向けセキュリティ施策の推進に取り組む。

4.1.3 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

(1) サプライチェーンの信頼性確保

（略）上記フレームワーク等に基づく産業分野別及び産業横断的なガイドライン等の策定や活用促進を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。（略）サイバーセキュリティ強化に向けた取組状況の可視化を行うことで、サプライチェーンを通じて地域・中小企業に取組を広げ、サプライチェーン全体の信頼性向上に繋がることが期待される。

サイバーセキュリティ戦略と今後の産業サイバーセキュリティ政策との関係②

サイバーセキュリティ市場の拡大

- 我が国サイバーセキュリティ産業の振興に向けた強化策の検討
- 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
- サイバーセキュリティ人材の育成・確保に向けた取組

官民の状況把握力・対処能力向上

- IPAにおけるサイバー情勢集約・分析能力の強化

4.4.2 人材の確保、育成、活躍促進

サイバー攻撃が複雑化・巧妙化する中（略）サイバーセキュリティ確保に向けた人材の育成・確保が不可欠である。（略）「質」・「量」両面での官民の取組を、一層継続・深化させていくことが必要である。

サイバーセキュリティ戦略（令和３年９月）

4.1.3 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

(3) セキュリティ製品・サービスの信頼性確保

（略）信頼性確保の基盤づくりに取り組み、ひいては先端技術・イノベーションの社会実装に係る取組と相まって、他国に過度に依存しない日本発の製品・サービスの育成に取り組む。

4.3.2 我が国の防御力・抑止力・状況把握力の強化

(3) サイバー空間の状況把握力の強化

深刻化するサイバー攻撃やサイバー空間を利用した影響工作の脅威を抑止していくためには、（略）サイバー攻撃等を検知・調査・分析する十分な能力が求められる。このため、関係機関におけるこうした能力を質的・量的に引き続き向上させ、（略）

4.4.1 研究開発の推進

サイバーセキュリティ研究分野は、脅威に関する情報やユーザ等のニーズを踏まえ、実践的な研究開発を進めることが非常に重要な分野である。一方で、（略）産学官エコシステムが築かれていることが大前提である。こうした基盤づくりに向けた中長期的観点からの取組と、それを基礎とした実践的な取組の双方の視点をあわせ持って取組を進めていく。また、研究開発の推進に当たってはデジタル技術の進展に応じた観点も重要であり、中長期的な技術トレンドを視野に入れた対応を行う。