経済産業省

サイバーセキュリティ政策の概要と
IoTデバイスのセキュリティリスクについて

2024年3月6日

商務情報政策局　サイバーセキュリティ課

サイバーセキュリティ戦略専門官　山田　剛人

1. サイバー攻撃の現状

2. 経済産業省のサイバーセキュリティ政策の概要

3. IoTデバイスに対するセキュリティ政策

サイバー攻撃の現状

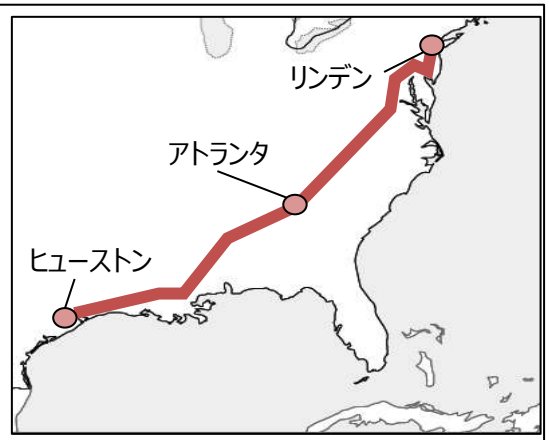
- **昨今のサイバー攻撃は、**企業等の情報を暗号化して金銭をゆすり取る「ランサムウェア攻撃」や、国家支援型の攻撃集団等が特定の企業を執拗に狙う「標的型攻撃」など、**多種多様**。
- 加えて、**サイバー攻撃が高度化・巧妙化**するとともに、あらゆるものがネットワークにつながり、**攻撃の起点が増加**したことで、**サイバー攻撃が社会や産業に「広く」、「深く」影響を及ぼすように**なっている。

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）

事例（海外）

- 米国の専門機関によれば、米国における重要インフラ事業者等への攻撃のうち、**約1割は制御系システムまで影響を及ぼした**。
- 一例として、2021年5月には、米石油パイプライン大手がランサムウェア攻撃を受け、**全てのパイプラインを一時停止**。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。



事例（国内）

- 2021年10月末、**国内の公立病院がランサムウェア攻撃を受け、電子カルテが暗号化され閲覧不可**になったほか、**診療報酬計算や電子カルテ閲覧に使用する基幹システムが使用不能**になったため、**新規患者の受け入れを停止**。
- 病院は、**身代金要求には応じず**、同年12月29日にサーバーを復旧させ、2022年1月４日から通常診療を再開。

<出典：(独)情報処理推進機構(IPA)、2024.1.24>
※「ゼロデイ攻撃」とは、あるソフトウェアに脆弱性が存在することが判明し、修正プログラムがベンダーから提供されるより前に、その脆弱性を悪用して行われる攻撃のこと。

情報セキュリティ10大脅威の変遷

- 2024年の組織向け脅威には、**「ランサムウェアによる被害」が4年連続で１位にランクイン。**
- サプライチェーンの弱点を悪用した攻撃、内部不正による情報漏えいがランクアップし上位に。

	脅威の種類	順位の変遷								
		2024	2023	2022	2021	2020	2019	2018	2017	2016
1	ランサムウェアによる被害	1	1	1	1	5	3	2	2	7
2	サプライチェーンの弱点を悪用した攻撃	2	2	3	4	4	4	-	-	-
3	内部不正による情報漏えい等の被害	3	4	2	2	1	1	1	1	1
4	標的型攻撃による機密情報の窃取	4	3	5	6	2	5	8	5	2
5	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	5	6	4	3	-	-	-	-	-
6	不注意による情報漏えい等の被害	6	9	7	-	-	-	-	-	-
7	脆弱性対策情報の公開に伴う悪用増加	7	8	8	5	3	2	3	-	-
8	ビジネスメール詐欺による金銭被害	8	7	6	10	-	9	4	-	-
9	テレワーク等のニューノーマルな働き方を狙った攻撃	9	5	10	9	7	10	-	-	-
10	犯罪のビジネス化（アンダーグラウンドサービス）	10	10	-	-	-	-	-	-	-

＜事例＞サイバー攻撃による米国石油パイプラインの操業停止について

- 2021年5月7日、米石油パイプライン最大手のコロニアル・パイプラインがランサムウェアによるサイバー攻撃を受け、全ての業務を停止したと発表。直接の影響を受けたのはITシステムだが、脅威を封じ込めるためにOTシステムをオフラインにし、全てのパイプラインの運用を停止した。パイプラインは５月12日に業務再開。
- 米運輸省は9日、燃料の輸送に関して緊急措置の発動を宣言。また、CISAのサイバーセキュリティ部門トップも声明を公表。
- FBIはロシア系攻撃集団「ダークサイド」の関与を断定。コロニアル・パイプラインは身代金として4.4百万ドルを支払ったが、その後米当局が同グループの運営インフラを差し押さえたことにより、ダークサイドは活動停止、身代金の一部が押収された。

コロニアル・パイプライン

メキシコ湾岸の製油所と米東部・南部を結ぶ全長8,850kmのパイプライン。
東海岸の需要の約半分にあたる１日約１億ガロンを輸送。

米運輸省による緊急措置の内容

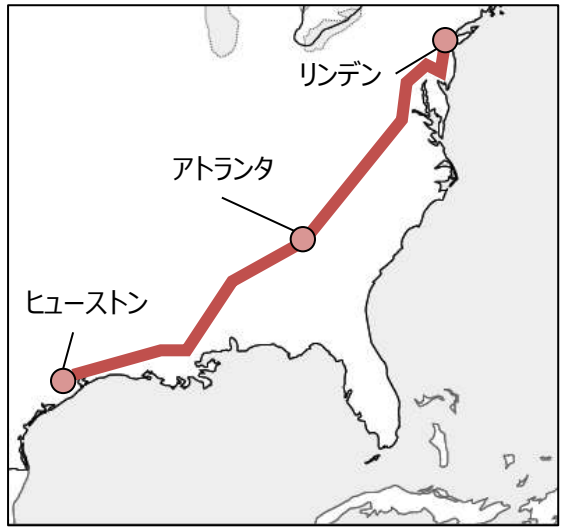
影響を受ける１７州と首都ワシントン向けに
燃料を輸送する運転手の労働時間規制を一時的に緩和。

米CISAによる声明のポイント

CISAは、サイバーセキュリティ部門トップのGoldstein氏名で声明を公表。

・被害企業と関係官庁とともに本事案に対処中。
・ランサムウェアは**組織の規模、セクターに関係なく直面**する脅威。
・この種の脅威に晒されるリスクを減らすためサイバーセキュリティ体制を強化する措置を講じることを各組織に推奨。

出典：https://piyolog.hatenadiary.jp/entry/2021/05/12/051650



コロニアル・パイプラインの
主要パイプライン（イメージ）

＜事例＞ IoTの進展に伴う新たな脅威：新たにつながるデバイスの不正操作

- これまでネットワークに接続されていなかった自動車やカメラなどの機器が、WiFiや携帯電話網などを介してインターネットに接続されることによってサイバー攻撃の新たな対象に。
- **不正操作による誤作動、不適正作動**などのリスクが顕在化。

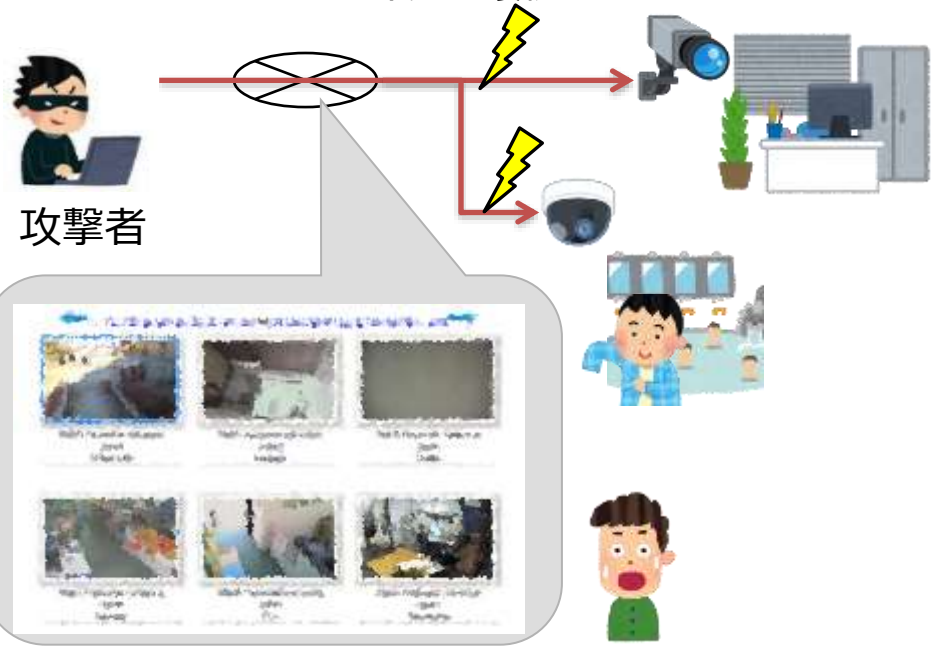
自動車へのハッキングよる遠隔操作

携帯電話網経由で遠隔地からハッキング

人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施

監視カメラの映像がインターネット上に公開

利用者が気づかないまま、ID/パスワードを
デフォルトのままインターネットに接続



セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**

1. サイバー攻撃の現状

2. 経済産業省のサイバーセキュリティ政策の全体像

3. IoTデバイスに対するセキュリティ政策

経済産業省におけるサイバーセキュリティ政策のミッション・全体像

- サイバー攻撃の高度化・多様化が生じている現状を認識しつつ、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。そのために国が行うべき政策を企画・実行する。
- その上で、サイバーセキュリティの確保に向けた各種の取組を、**我が国産業競争力の強化**につなげる。

①サプライチェーン全体での対策強化

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装
- 経営ガイドラインの活用促進
- サイバーセキュリティお助け隊サービスの普及促進
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

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

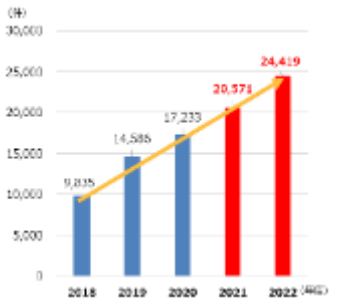
- IoT適合性評価制度の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進
- QUAD上級サイバー会合、G7等を通じた各国間連携

SBOMの概念的イメージ

③政府全体でのサイバーセキュリティ対応体制の強化

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

サイバー攻撃事案の調整件数（年度集計）



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）

- 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、製品/サービスの国内自給率向上に向けた政策検討

「Society5.0」の社会を見据えた対策の検討

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**となる。
- **サイバー・フィジカル・セキュリティ対策フレームワークを策定**し、必要な対策を検討。

https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html

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

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

CPSFのモデル

<3層構造>

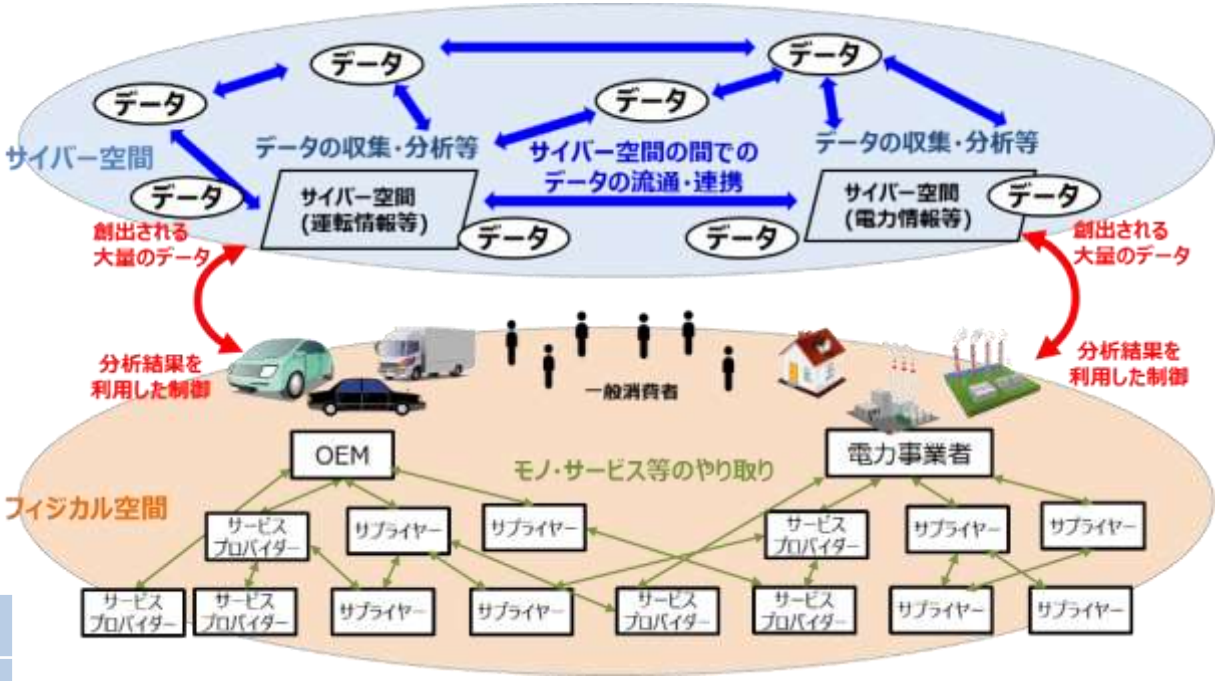
【第３層】
サイバー空間におけるつながり

【第２層】
フィジカル空間とサイバー空間のつながり

【第１層】
企業間のつながり

<6つの構成要素>

ソシキ	ヒト	モノ
データ	プロシージャ	システム



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

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 と テーマ別TFにおける検討

- **7つの産業分野別サブワーキンググループ（SWG）**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、**3つのタスクフォース（TF）を設置**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

ビルSWG
- ガイドライン第2版の策定(2023.4)

電力SWG
- 小売電気事業者ガイドライン策定(2021.2)

防衛産業SWG
- 防衛産業サイバーセキュリティ基準の改訂を公表(2022.4)

自動車産業SWG
- ガイドライン2.0版を公表(2022.4)

スマートホームSWG
- ガイドライン1.0版を公表(2021.4)

宇宙産業SWG
- 2023年３月にガイドラインVer1.1版を公表

工場SWG
- ガイドラインVer1.0を公表（2022.11）

・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
「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」を公開。

ソフトウェアTF：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

検討事項：
OSSの管理手法に関するプラクティス集を策定、SBOM活用促進に向けた実証事業（PoC）を実施。

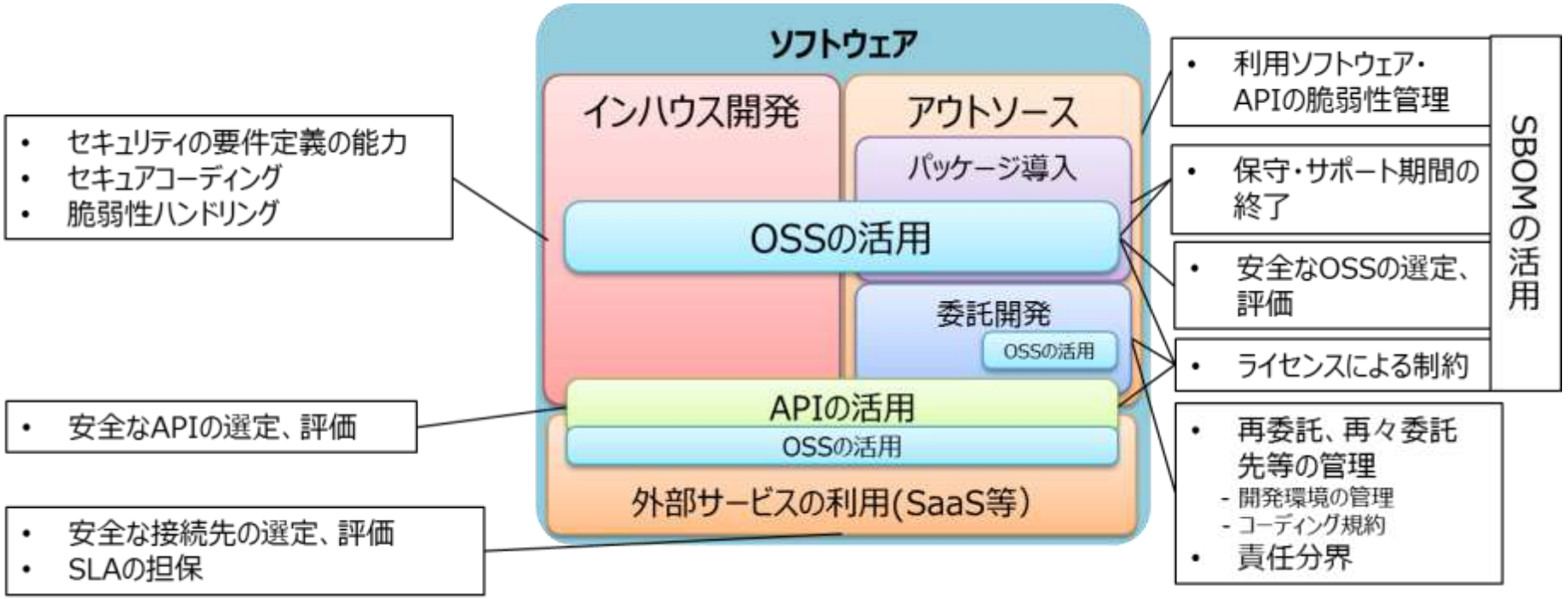
『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。このIoT-SSFをわかりやすく理解するためのユースケースを新たに公開。

経済産業省におけるソフトウェアセキュリティの検討

- 仮想化技術の進展など、**OSSを含むソフトウェア技術への依存度の高まり**。**ソフトウェアの管理手法、脆弱性対応、ライセンス対応の重要性**が増大。
- 2018年、**米国NTIA（電気通信情報局）はSoftware Component Transparencyを提唱**。ソフト部品構成表である**SBOM (Software Bill of Materials）活用の議論**を推進。
- 2019年から有識者による検討会（産業サイバーセキュリティ研究会ソフトウエアTF）を立ち上げ、**ソフトウェア（特にOSS）の適切な管理手法や脆弱性対応、ライセンス対応**を検討。

ソフトウェアを利用する際に考慮すべき観点

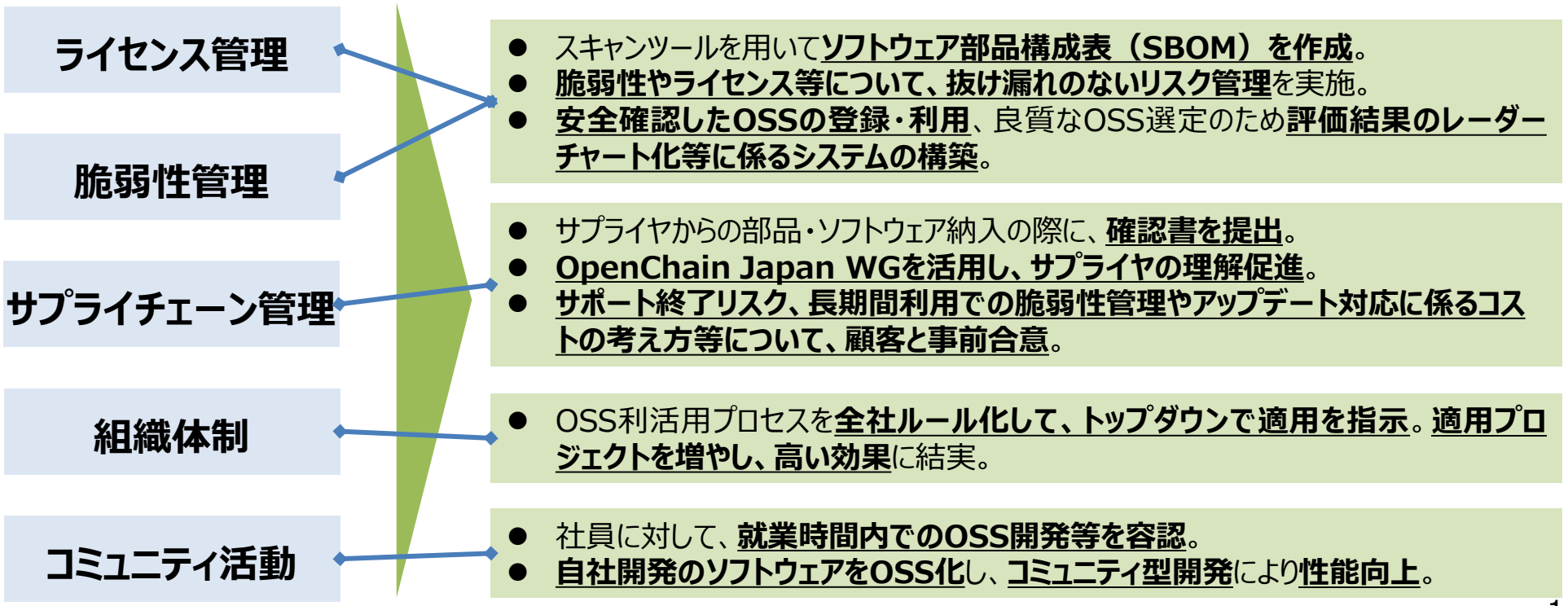


OSS管理手法に関する事例集の策定

https://www.meti.go.jp/policy/netsecurity/wg1/ossjirei_20220801.pdf

- OSSの**留意点を考慮した適切なOSS利用の促進**
  - ✓ 企業がOSSを利活用するに当たって留意すべきポイントを整理。
  - ✓ そのポイントごとに**参考となる事例を、具体的な個別企業ヒアリング等により取りまとめ**公開。
  - ✓ 企業のOSS利用の障壁を取り除くことで、一層のOSS利活用を促進。
  - ✓ 産業界において**OSSのメリットを享受することで競争力を向上**

OSSに関する課題例



OSS事例集で紹介する取組例

- スキャンツールを用いて**ソフトウェア部品構成表（SBOM）を作成**。
- **脆弱性やライセンス等について、抜け漏れのないリスク管理**を実施。
- **安全確認したOSSの登録・利用**、良質なOSS選定のため**評価結果のレーダーチャート化等に係るシステムの構築**。

- サプライヤからの部品・ソフトウェア納入の際に、**確認書を提出**。
- **OpenChain Japan WGを活用し、サプライヤの理解促進**。
- **サポート終了リスク、長期間利用での脆弱性管理やアップデート対応に係るコストの考え方等について、顧客と事前合意**。

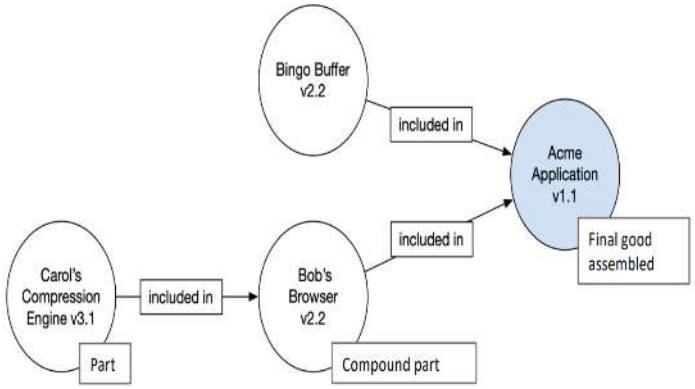
- OSS利活用プロセスを**全社ルール化して、トップダウンで適用を指示**。**適用プロジェクトを増やし、高い効果**に結実。

- 社員に対して、**就業時間内でのOSS開発等を容認**。
- **自社開発のソフトウェアをOSS化**し、**コミュニティ型開発**により**性能向上**。

ソフトウェアタスクフォースの検討の方向性（SBOMについて）

- 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。
- 2021年5月に発令された米・大統領令においてもSBOM提供について言及されており、今後、政府調達要件として整備が進むものと想定。

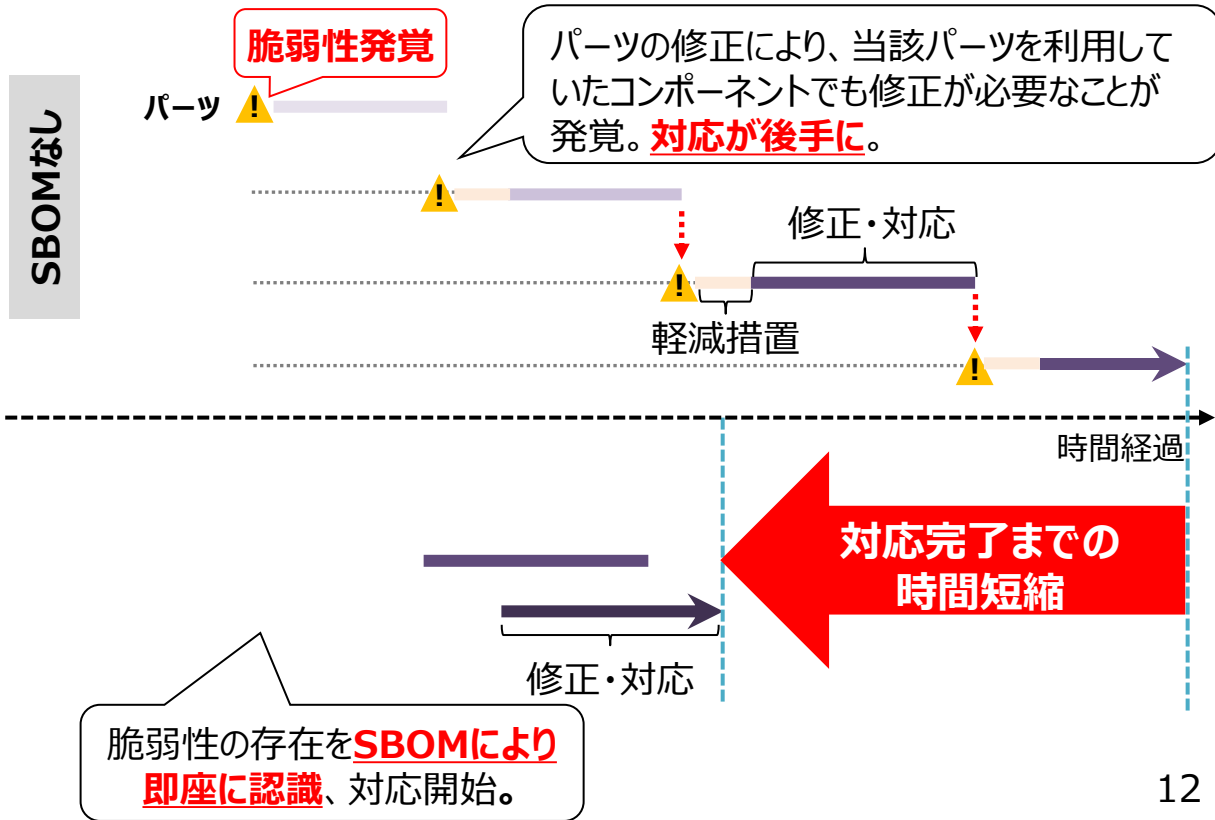
SBOMの構成イメージ



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
├─ Browser	Bob	2.1	Bob	0x223	334	Included in
├─ Compression Engine	Carol	3.1	Acme	0x323	434	Included in
├─ Buffer	Bingo	2.2	Acme	0x423	534	Included in

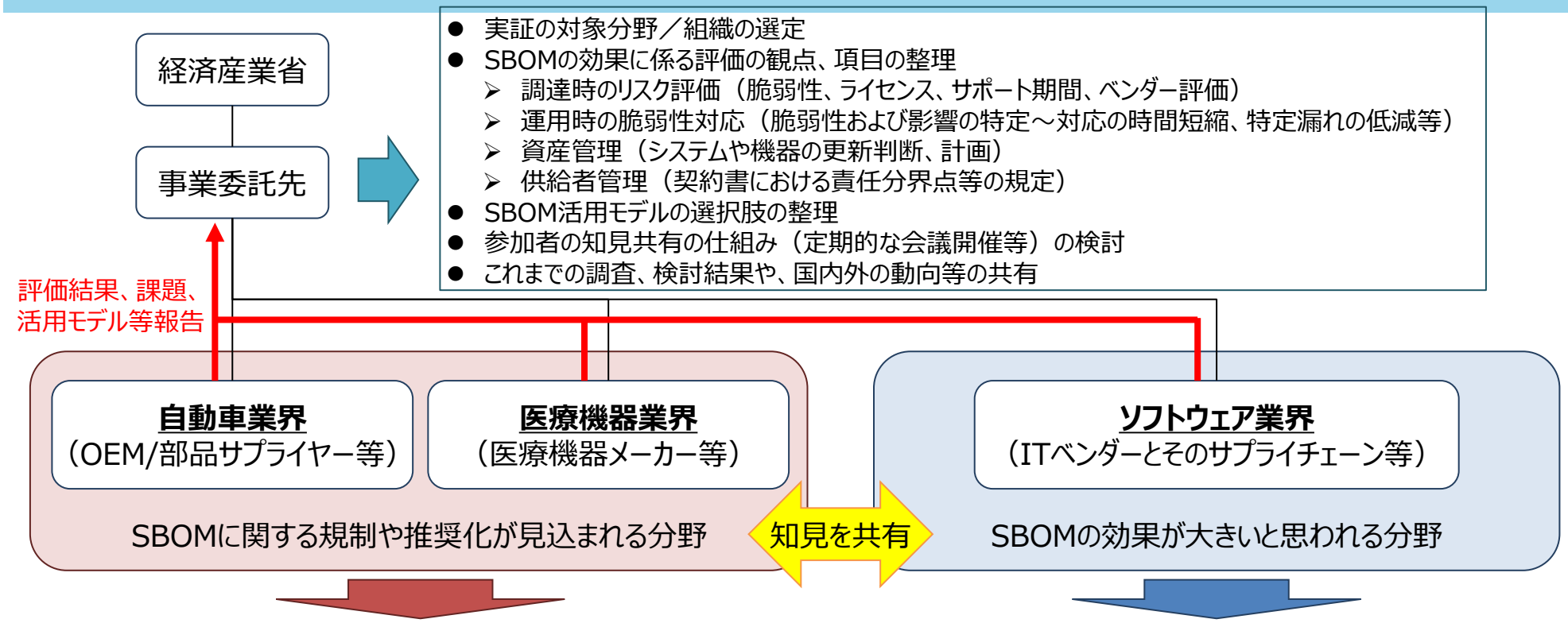
https://www.ntia.doc.gov/SoftwareTransparency

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



令和4年度の実証内容・体制

- SBOMに関して**「規制や推奨化が見込まれる分野」**や**「効果が大きいと思われる分野」を候補**に、実証参加企業の選定、実証内容を設計。
- **実証結果や民間で進められているSBOM活用の取組について、知見等を共有し、実際の活用方法を検討**。



実証結果を踏まえて下記①から③を整理し、ドキュメントを作成。
① SBOMの導入工数低減のため、SBOMの基本情報やSBOM導入に関しての実施事項等を整理。
② SBOMの効果的な活用を図るため、分野における規制の内容やリスク等を踏まえたSBOMの効果的なモデルを整理
③ SBOM活用のための環境整備を図るため、SBOMに関する責任、費用負担等、取引契約における論点を整理

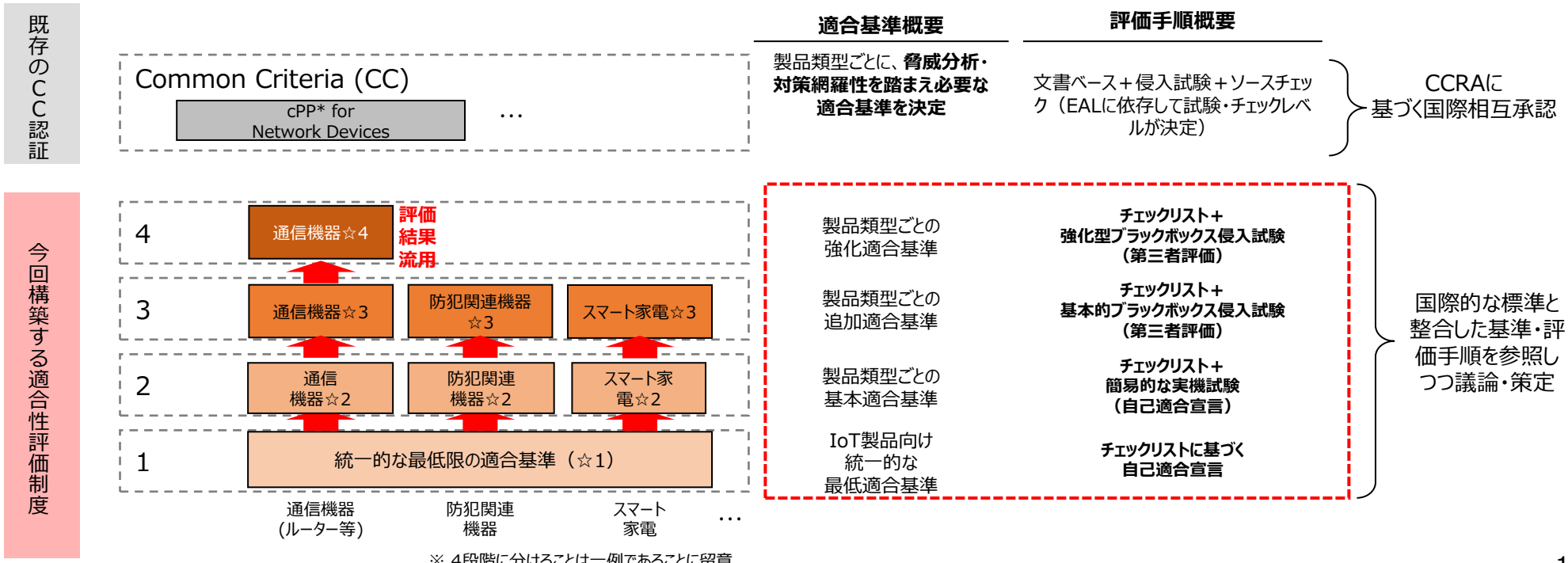
実証で抽出された主な課題と解決策（抜粋）

実証で抽出された課題に基づき、解決ノウハウの検討や今後の取組施策の整理を行った。

区分	実証から抽出した課題	解決ノウハウ （導入ガイダンスに反映予定）	今後の課題 （国、民間）	医療機器	自動車	ソフト
技術	検出した脆弱性の対応要否、優先度の判断が困難	医療機器分野の脆弱性対応フローなどを参考にアドバイザリ、脅威情報を活用し、対応の要否、優先度を判断。	脆弱性管理の高度化、脅威情報の普及促進	●		
	SBOMツールの使い分け・変更による負担増大	機能ニーズを洗い出し、ツール比較情報をもとに選択	—	●	●	●
	CI/CDなど継続的なアップデートへの対応負担	ツールによる自動化可能な範囲で管理	CI/CDに対応した自動管理			●
	SBOM初期導入、ツール等のコスト負担が大きい	ツールの効率的な導入方法、OSSツールの選択活用	OSSベースのツール整備	●	●	●
管理	SBOMに要求される精査のレベルが不明確	SBOM対応モデルの選択肢やSBOMツールの機能に応じて精査の要否を判断する。	—	●	●	
	SBOM生成の対象範囲が不明確	OS,MWを含めて対象全体の上位構成を事前に明確化	—	●	●	●
	ツールの環境構築、SBOM共有のコストが大きい	SaaS型SBOMツールで初期導入と共有の工数を低減	サプライチェーンを通じた脆弱性管理	●	●	●
	ユーザ組織によるSBOMの活用・管理が困難	SBOMツール導入、ベンダ支援の活用	—	●	●	●
	部品の脆弱性残存期間に応じたリスク評価	SBOMの履歴管理により脆弱性残存期間を特定	脆弱性の履歴評価			●
	開発部署、PSIRTなど部署ごとの脆弱性管理が非効率	社内でSBOMを一元管理することで、脆弱性管理を効率化	SBOMによる脆弱性の社内一元管理		●	●
	サプライヤごとの部品粒度のバラつき	取得したすべての粒度をツールで自動管理	脆弱性マッチングの高度化		●	
	サプライヤのサポート切れなどのリスク対応	部品のEOL等に基づくサポート計画・管理を実施	—	●		
取引	サードパーティからのSBOM取得が困難、バイナリ納品物の脆弱性の監視・修正が負担	ソースコード取得とSBOMツールの適用、（バイナリ納品の場合）SBOM提供と脆弱性修正を契約で要件化	—	●	●	●
	サプライヤ部品の精査コストが大きい	SBOMの提供と信頼性に関する責任を契約で規定	—	●	●	

制度概要

- 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（☆）を用いた制度を想定。**
- **☆1は、幅広いIoT製品を対象に、統一的な最低限の適合基準**を想定。**評価方法は**、チェックリストに基づく**自己適合宣言**を想定。
- **☆2以上は、製品類型ごとに適合基準を策定**することを想定。評価方法は、チェックリストに基づく**自己適合宣言及び実機試験・侵入試験等の第三者評価**を想定。なお、どの程度の第三者評価をどのレベルで求めるかは今後製品類型ごとに要検討。

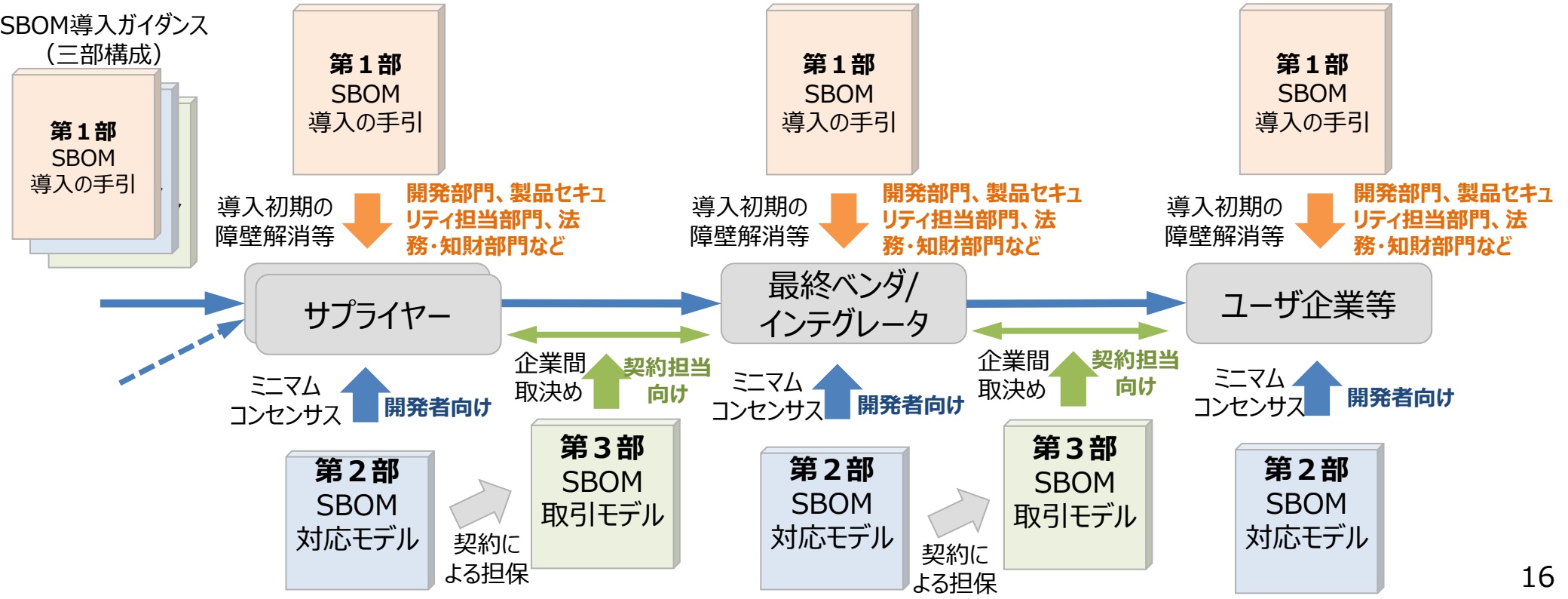


※ 4段階に分けることは一例であることに留意。

実証結果等を踏まえた検討について

- 本実証結果等を踏まえ、導入の手引、対応モデル、取引モデルから構成されるSBOMに関するガイダンス（SBOM導入ガイダンス）を作成。
- SBOM導入の手引→ 対応モデル → 取引モデル を順次活用し、サプライチェーンにおける信頼を確かなものとする。

SBOM導入ガイダンスは、以下の３部から構成する。
第１部　SBOM導入の手引：導入初期の課題、阻害要因を解消するための開発者向けのヒント・TIPS等。
　　効率的な適用方法。（実証の成果やNTIA SBOM Playbook等の関連する内容を盛り込む）
第２部　対応モデル：業界として期待される開発者向けのSBOM対応レベル（ミニマム・コンセンサス）。
第３部　取引モデル：対応モデルを契約でどのように担保するか契約担当向けの例示。要件・責任関係の明確化
※　Ver1.0として第１部を盛り込みつつ、第２部、第３部は整理・検討後、Ver2.0に盛り込む予定。



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～

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。

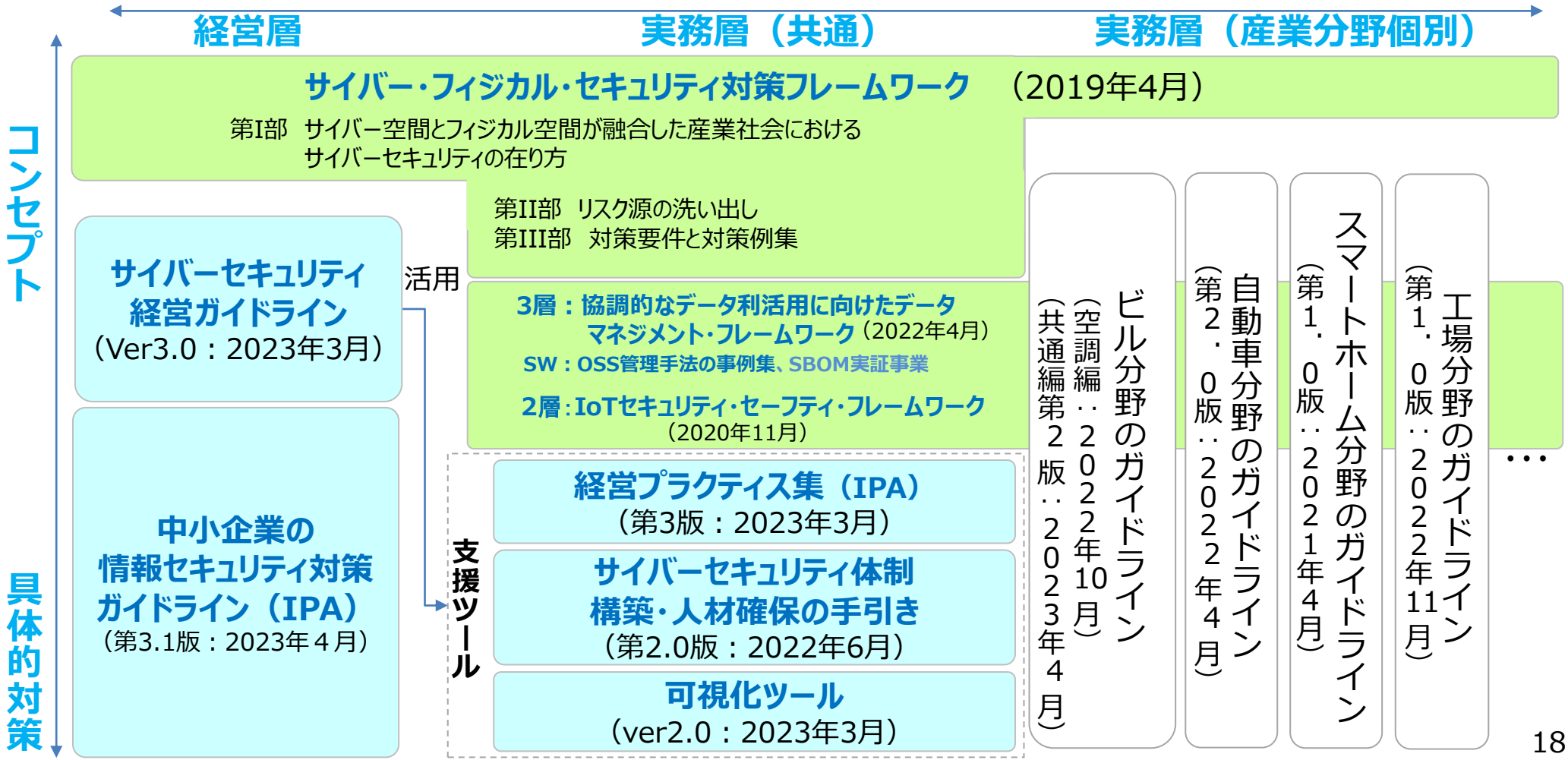
フェーズ3　SBOM運用・管理フェーズ

- **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。

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軸とした各種取組

- Society5.0における産業社会での**セキュリティ対策の全体枠組み**を提示。
- 全体の枠組みに沿って、**対象者や具体的な対策を整理**し、『**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**などの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞



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取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。

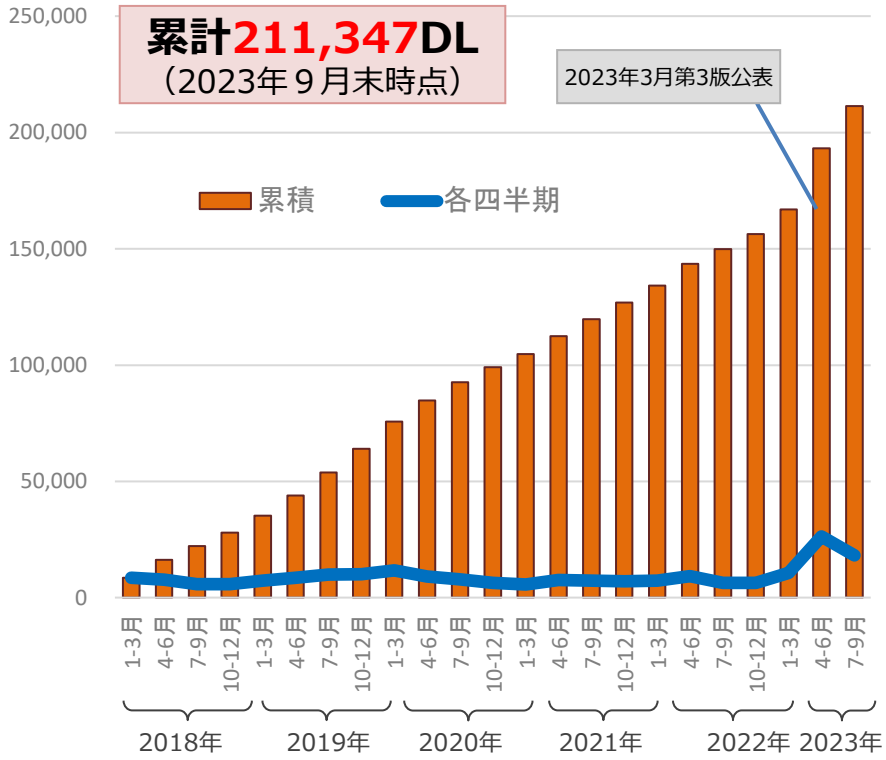
１．経営者が認識すべき３原則

（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

サイバーセキュリティ経営ガイドラインV2.0/V3.0のダウンロード数推移



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

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

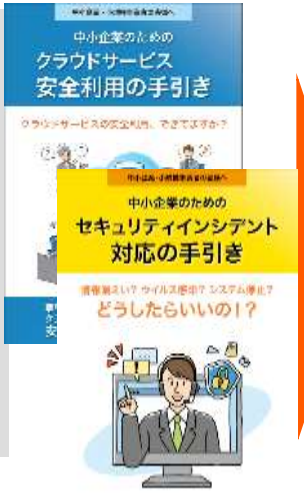
経営者向けの解説

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。25万者を超える中小企業が宣言。

★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。
（2023年7月時点で35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

中小企業向けIoTセキュリティ対策ガイドの作成・普及

- 優れた中小企業を増やすことが、我が国全体のIoT製品のセキュリティ向上には重要。しかし、IoTセキュリティに関するガイドラインは多数あるものの、内容が専門的であるなど中小企業にとってわかりやすいガイドにはなっておらず、「**何を参照していいかわからない**」「**どのような対策をすればいいかわからない**」という状況。
- そこで、中小企業がIoT製品の開発を行う際にセキュリティ面で考慮してほしいポイントをわかりやすく記載した「**IoT機器を開発する中小企業向け製品セキュリティ対策ガイド**」を策定※。本ガイドでは、**セキュアなIoT機器が数多く出荷**されていくためには、**出荷前の検証のみならず設計・開発といった初期段階からセキュリティ対策を実施することが重要**である旨を記載。また、既存ガイドの重要ポイントや優良企業の事例も記載。

  ※https://www.meti.go.jp/policy/netsecurity/chusyosecurityguide.pdf
- 今後、**中小企業関連政策や中小企業関連団体と連携**を行い、**IoT機器の設計・開発段階でのセキュリティ対策や検証の必要性をより多くの中小企業が認識するよう普及活動**を行っていく。

「IoT機器を開発する中小企業向け製品セキュリティ対策ガイド」の策定

関連ガイドラインから最初に実施すべき対策を抽出

ガイド目次

- 経営者の皆様へ
- 本ガイドの概要
- 各フェーズで求められる対策
- 設計・開発フェーズで検討すべき主な技術的対策
- IoT機器を開発する中小企業の対策事例集
- 付録

各フェーズで求められる対策

節	項目
方針・体制構築フェーズで求められる対策	【対策1】製品に関するセキュリティポリシーを策定・周知する
	【対策2】セキュリティポリシーを適切に運用するための体制を整備する
設計・開発フェーズで求められる対策	【対策3】IoT機器等において守るべきものを特定し、それに対するリスクを想定する
	【対策4】守るべきもの及びリスクを考慮した設計・開発を行う
検証フェーズで求められる対策	【対策5】セキュリティに関する要件が満たされているかを検証する
運用・保守フェーズで求められる対策	【対策6】出荷後もリスクに関する情報の収集や関係者とのコミュニケーションを行い、適切なサポートを行う

中小企業関連団体等を通じた周知

HP・メールマガジン等を通じた案内、セミナー等における案内、各都道府県を通じた地域の中小企業への周知

日本商工会議所 The Japan Chamber of Commerce and Industry　Be a Great Small. 中小機構　全国中小企業団体中央会

SC3を通じた中小企業関係者、業界団体等への周知・案内

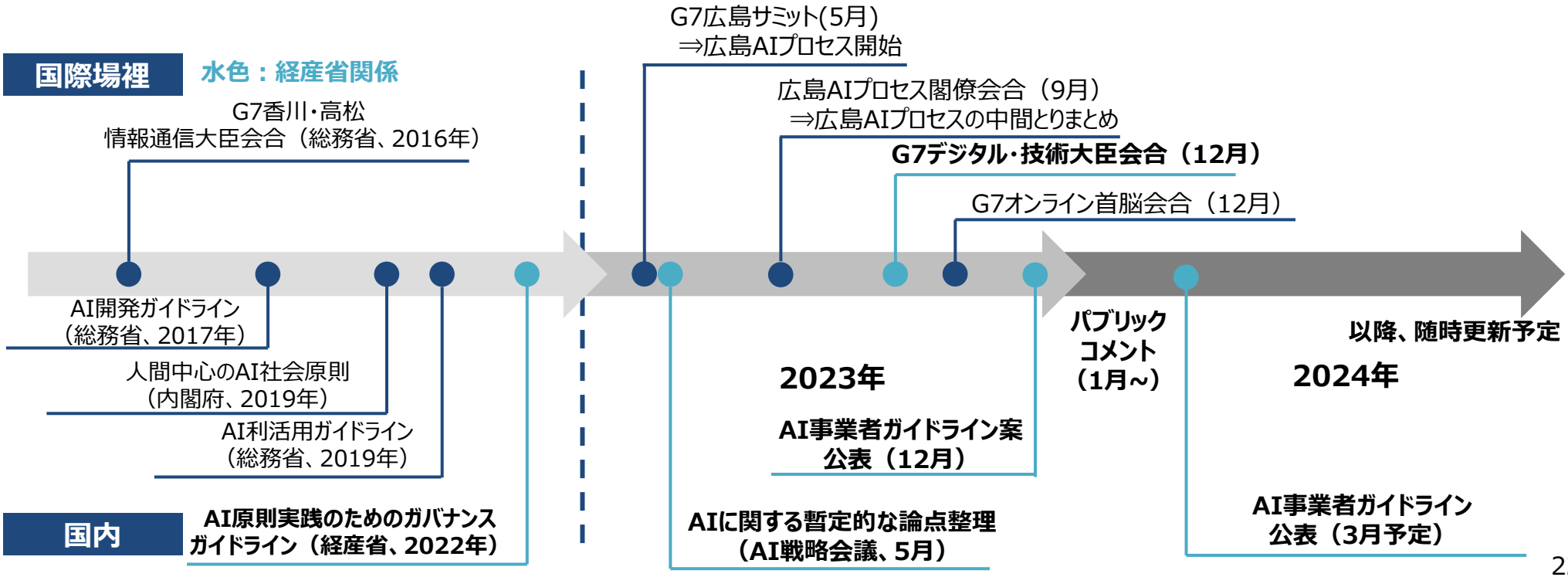
SC3 サプライチェーン・サイバーセキュリティ・コンソーシアム

設立：2020年11月1日
概要：産業界が一体となって、中小企業を含むサプライチェーン全体のサイバーセキュリティ対策を推進するコンソーシアム
会長：遠藤　信博（一般社団法人日本経済団体連合会副会長・サイバーセキュリティ委員長）

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月に公表予定**）

（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（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

各論

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**

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

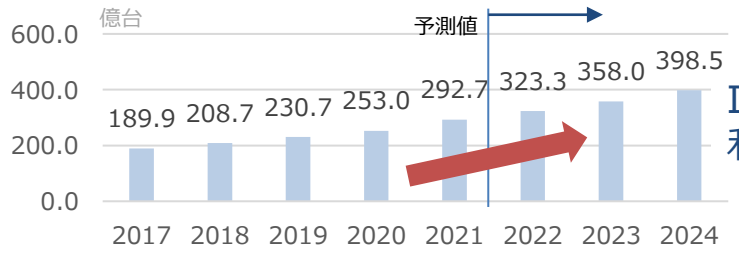
1. サイバー攻撃の現状

2. 経済産業省のサイバーセキュリティ政策の全体像

3. IoTデバイスに対するセキュリティ政策

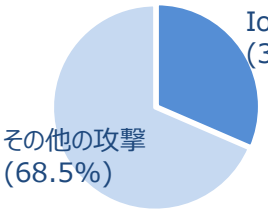
IoT機器の利用拡大に伴い増加するリスク･経営への影響

ネットワークに接続される機器(IoT機器)は増加傾向、IoT機器を狙った攻撃は多い



IoT機器の
利用数は増加

世界のIoT機器数の推移及び予測(※1)



ダークネットにおける年間観測パケット数の割合(※2)

不審な通信のうち
約1/3はIoT機器を狙った攻撃

[※1] 出所:総務省「情報通信白書令和4年版 データ集」(3章関連データ)
[※2] 出所:NICT「NICTER観測レポート2022」調査を除く攻撃パケットのうち、23/TCP、22/TCP、5555/TCP、81/TCPへのパケットを集計。

IoTにおけるセキュリティインシデントが経営に大きな影響を及ぼす可能性が高まっている

操業停止や逸失利益の発生を含む事業への直接的な影響

半導体製造工場の制御装置に対する攻撃によって、**3日間の操業停止、営業機会損失が発生(売上高(四半期)の3%損失)**[台湾:2018]

石油化学工場の安全計装システムを対象とした攻撃による**操業停止。プラント爆発のおそれ**[サウジアラビア:2017]

脆弱性対応や損害賠償を含む追加費用の発生

脆弱性発見による自動車140万台のリコールの発生。脆弱性等の対応で、**2億9900万ユーロ(約394億円)の赤字を計上**(四半期の最終損益) [米国:2015]

評判の低下等より生じる競合優位性の低下

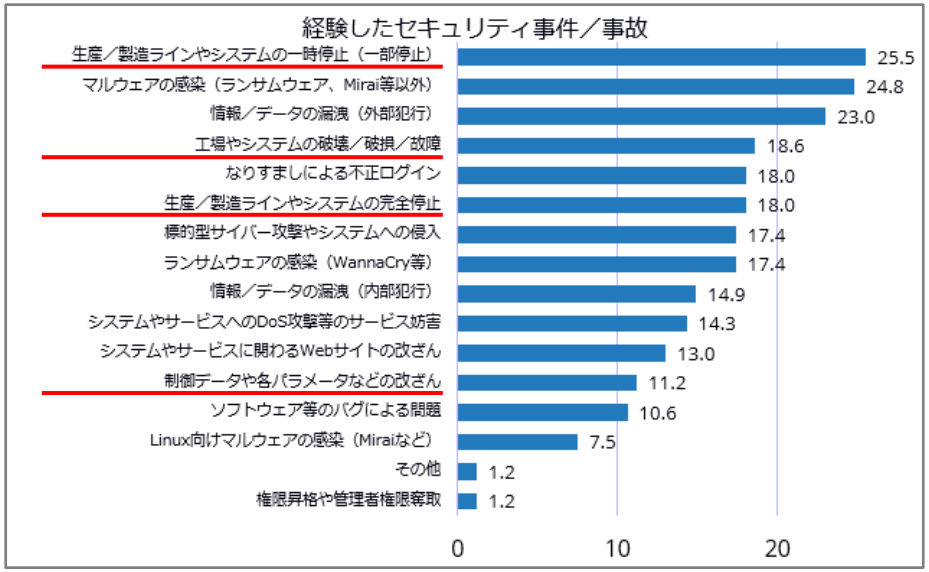
高級ホテルで客室のカードキー発行システムがランサムウェアに感染し、一切のシステム操作が不可能となった。客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生。**サービスの品質が著しく低下** [オーストリア: 2017]

[参考] 各公開情報を基に作成

IoT機器に対するセキュリティ対策の必要性

- DXの進展により、インターネットとIoT機器が繋がり始めたところであるものの、**セキュリティ事件/事故によるIoT機器やOTシステムの一時停止を約25%の企業が経験**。**こうした機器やシステムでセキュリティ対策を多くの者が導入しているとは言い難い**状況。
- 機器に対する十分なセキュリティ対策が実施されず、脆弱性が残存した場合、悪意ある攻撃者によって不正操作や誤作動が実行され、**機器の利用者へ影響を及ぼす恐れ**。
- また、**開発企業は脆弱性の対応に追われる**こととなる。過去には、**脆弱性によりリコールや利用者による訴訟に発展した事例**もあり、最悪の場合、**開発企業の経営に対して影響を与える可能性**もある。
- 今後さらなる脅威の増加・高度化が想定されるところ、**機器に対するセキュリティ対策の具備が不可欠**。

2021年 国内企業のIoT/OTセキュリティ対策実態調査結果



セキュリティ対策の不備により開発企業に影響を及ぼした事例

自動車における脆弱性の検出による140万台のリコール

販売中の自動車に対して外部から不正アクセス可能な脆弱性が公開。**顧客からの問い合わせが殺到し、開発企業は140万台のリコール**。**リコールの対応には1,000万ドル以上の費用**を要した。

心臓ペースメーカーにおける脆弱性の検出による46.5万台のリコール

販売中の心臓ペースメーカーに対して心拍リズムを外部から制御可能な脆弱性が公。**開発企業は市場に流通している46.5万台を対象にリコール**。

脆弱な家庭用ネットワークカメラのメーカに対する訴訟

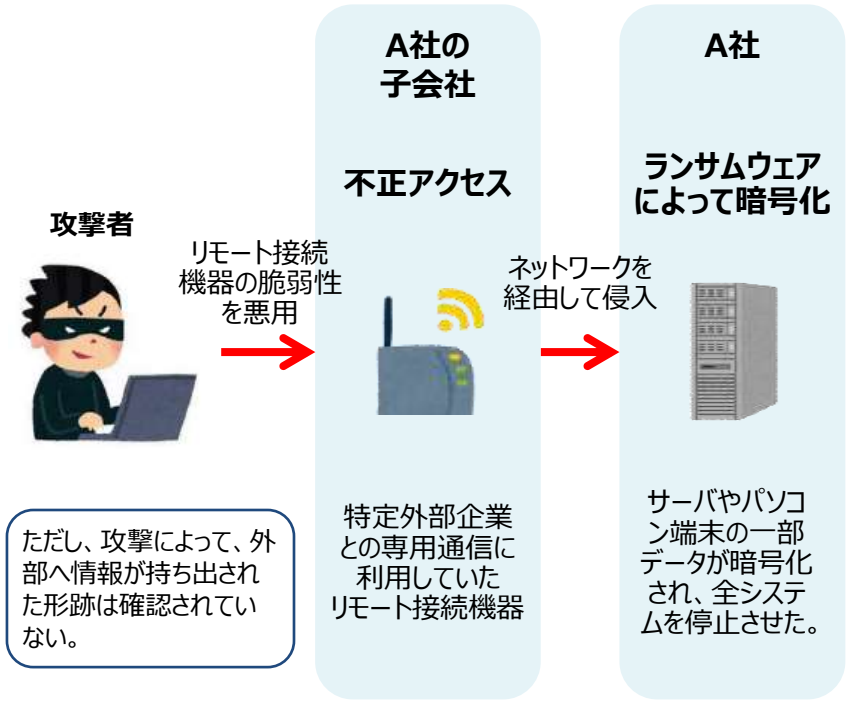
家庭用ネットワークカメラにおいて、認証不備に関する脆弱性が内在し、脆弱性を悪用した不正アクセスが行われた。不正アクセスの被害を受けた複数の利用者により、**開発企業に対して500万ドルを求める集団訴訟**が提起。

IDC「2021年 国内企業のIoT/OTセキュリティ対策実態調査」https://www.idc.com/getdoc.jsp?containerId=prJPJ47631521
※ 調査実施：2021年2月、調査対象：国内企業443社

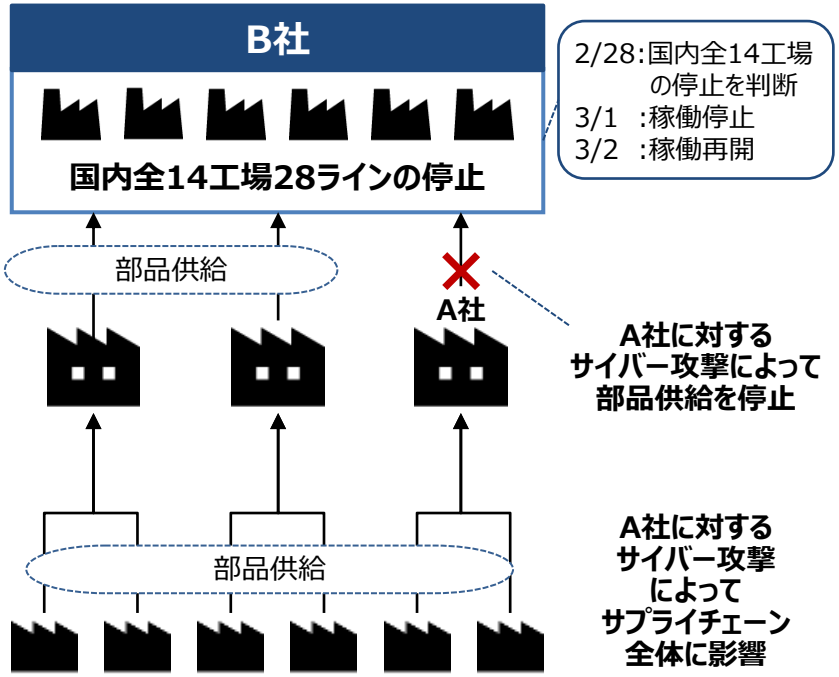
自動車部品メーカーに対するランサムウェア攻撃事案

- 2022年2月、B社に自動車部品を納入しているA社は、子会社のネットワークを経由して不正アクセスを受けたことで、サーバやパソコン端末の一部データがランサムウェアによって暗号化され、被害拡大防止のために全システムを停止させた。
- A社へのサイバー攻撃によって、 2022年3月にB社は国内全14工場28ラインの停止を判断。

子会社を通じた不正アクセスの概要



サプライチェーン全体への波及



[参考] 各公開情報を基に作成

ネットワークカメラに対する攻撃事例

- 中国のメーカー・Hikvisionが製造するネットワークカメラにおいて発見されたコマンドインジェクションの脆弱性(CVE-2021-36260)を悪用して、機器の認証情報(例:ID、パスワード)が漏えいした。
- 2022年7月、セキュリティ企業CYFIRMAは漏えいした認証情報がロシアのフォーラムで公表されていることを報告した。既に修正パッチは公開(2021年9月)されている一方で、修正パッチを未適用であり攻撃を受ける可能性があるカメラは全世界で8万台以上とされた。

ネットワークカメラへの攻撃イメージ

- 複数のネットワークカメラに対して、攻撃者はコマンドインジェクションの脆弱性を悪用し、**ネットワークカメラの認証情報(例:ID、パスワード)を不正に取得した**。

- **窃取されたHikvision製カメラの認証情報(例:ID、パスワード)がロシアのフォーラムで確認された。**
- 100カ国にわたる2300の組織で使用されている8万台以上のカメラがいまだに修正パッチを適用しておらず、脆弱性を突かれる可能性があることが明らかとなった。

[参考] 各公開情報を基に作成

IoT製品適合性評価に関する各国動向

法規制

米国

【カリフォルニア州】**SB-327 Information privacy: connected devices**
【オレゴン州】**HB-2395 (2019) Oregon Cybersecurity Bill**

- 他の法令やガイダンスに基づくセキュリティ要件の対象となっている製品を除く**インターネットに接続される機器**が対象
- **IoT機器を販売するメーカーに対し**、パスワードの管理等を含む**合理的なセキュリティ機能を具備することを要求**
- 【オレゴン州のみ】セキュリティ対策違反を起こした場合、調査措置や差止命令が行われる可能性があるほか、故意に違反していると判断された場合には、最高25,000ドルの罰金の支払いが命じられる可能性がある

日本

端末設備等規則（総務省令）

- **電気通信事業者のネットワーク（インターネット等）に直接接続するIoT製品**。
- **間接的にネットワークに接続するIoT機器**（ホームネットワークのみに繋がるスマートホーム機器、等）**は対象外。**

EU

Cyber Resilience Act（CRA）（草案提出中）

- 一部例外を除き**デジタル要素を備えた全ての製品に対して、EU全域に水平的なサイバーセキュリティ要件**を課す内容（罰則あり）
- **製造業者への①上市前の設計製造に関する義務、②上市後の報告等義務**等。

Radio Equipment Directive（RED）（2025年8月1日から）

- **直接又は間接にインターネットに接続する無線製品**が対象
- ①ネットワーク・機能の損害/ネットワーク・リソース悪用/許容できないサービス低下の防止、②個人データ・プライバシー保護、③不正行為からの保護サポートを要求予定

英国

Product Security and Telecommunications Infrastructure (PSTI) Act 2022（2024年4月開始予定）

- **インターネットもしくはネットワークにつながる製品**に対して、セキュリティ対策を義務化する内容（罰則あり）
- 今後、下位法令にて具体的な内容が規定される。

任意制度（認証、ラベリング）

米国

U.S. Cyber Trust Mark Program（検討中）

- **消費者向けIoT機器**に対する任意の認証制度を2024年内に開始予定。
- 中でも消費者向けルーターは個別に要件策定がなされている。

EU

EU Cybersecurity Certification (EUCC)（検討中）

- ICT製品を対象とするCommon Criteria（ISO/IEC 15408）及び関連する共通評価方法（ISO/IEC 18045）に基づく認証スキーム

ドイツ

IT-Sicherheitskennzeichen (IT Security Label)（導入済）

- **ブロードバンドルーター、電子メールサービス、スマートテレビ、スマートスピーカー等の消費者向けIoT製品**を対象
- 2022年8月22日時点（制度開始後8ヶ月）で34製品・サービスがラベルを取得

相互運用を実施

シンガポール

Cybersecurity Labelling Scheme (CLS)（導入済）

- **すべての消費者向けIoT製品を対象とする任意の認証制度。**4段階の認証。
- 2022年8月22日時点（制度開始後22ヶ月）で206製品がラベルを取得

オーストラリア

Labelling for Smart Devices（検討中）

- インターネットやホームネットワークに接続される前提で開発された**すべての消費者向けのスマートデバイスを対象**として検討中

フィンランド

Finnish Cybersecurity Label（導入済）

- **インターネットに接続され、デジタル形式でデータを処理・伝送する製品・サービスを対象**
- 2022年8月22日時点（制度開始後33ヶ月）で14製品がラベルを取得

相互運用を実施

【欧州】サイバーレジリエンス法案　（審議中）

- **2022年9月**に欧州委員会が欧州議会・理事会に**草案提出**。**EU全域に水平的なサイバーセキュリティ要件**を課し、製品ライフサイクル全体を通じたセキュリティ向上を目指すもの。
- 一部例外を除き、**デジタル要素を備えた全ての製品**が対象。高リスクの「重要なデジタル製品」、低リスクの「重要なデジタル製品」、「その他」に**製品を３分類し、それぞれの分類に応じた適合性評価**を求める。
- 草案は**主として、製造業者への①上市前の設計製造等に関する義務、②上市後の報告等義務**に代別される。
- **罰則あり**。（最高1,500万ユーロ又は当該企業の全世界売上高の2.5%以内）
- **現在委員会・議会・理事会間で最終調整中**。

欧州委員会草案の主な義務

- **製造業者**

上市前の設計製造等に関する義務

- 付属書Iの1に記載の「セキュリティ特性要件」に従って、製品を設計/開発/製造する。
- 技術文書を作成する。
- 適合性評価手続きを行い、付属書Iとの適合性が実証された場合はCEマーキングを貼付する。

上市後の報告等に関する義務

- 積極的に悪用された脆弱性を発見した場合やインシデントを認識した場合、24時間以内にENISAに報告する。また、インシデントについては直ちにユーザーに報告し、必要に応じてその影響を緩和するための是正措置に関する情報を提供する。
- 上市後5年間または製品寿命のうち短い期間の間、付属書Iに記載の「セキュリティ特性要件」が満たされない場合は必要な是正措置を講じる、または製品の撤回・リコールを行う等適切に対処する。
- 上市後10年間、技術文書と（該当する場合）EU適合性証明書を保管する。

- **輸入者**

- 製造業者が、CE マーキング添付を含めた技術要求を満たしていることを確認する。

- **流通業者**

- 製造業者及び輸入者が、CE マーキング添付を含めた適切な手段を講じているかを確認する。

（参考）「重要なデジタル製品」

以下の各クラスに規定された要素を主に有するデジタル製品

クラスI(低リスク)第三者認証(EUCC,EN規格以外)

1. ID管理システム、アクセス管理ソフト
2. スタンドアロン型/組込み型ブラウザ
3. パスワードマネジャー
4. マルウェア検知・削除・隔離ソフトウエア
5. VPN機能を持つ製品
6. ネットワーク管理システム
7. ネットワーク・コンフィグレーション管理ツール
8. ネットワーク・モニタリングシステム
9. ネットワーク・リソース管理
10. SEIM（セキュリティ情報イベント管理）
11. ブートマネジャーを含む更新・パッチ管理
12. アプリケーション構成管理システム
13. リモートアクセス/共有ソフトウェア
14. モバイル機器管理ソフトウェア
15. 物理ネットワークインターフェイス
16. OS（クラスII製品以外）
17. ファイアウォール、侵入検知・防止システム（産業用以外）
18. ルータ、モデム、スイッチ（産業用以外）
19. マイクロプロセッサ（クラスII製品以外）
20. マイクロコントローラ
21. NIS 2 指令の別添Iに示される目的でのASIC、FPGA
22. PLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）（クラスII製品以外）
23. 産業用IoT（クラスII製品以外）

クラスII(高リスク) 第三者認証

1. OSであってサーバ、デスクトップ、モバイル機器用のもの
2. OSや同様の環境の仮想化を実施するためのハイパバイザー及びコンテナー・ランタイム・システム
3. 公開鍵インフラ及びデジタル証明書発行
4. 産業用のファイアウォール、侵入検知・防止システム
5. 汎用マイクロプロセッサ
6. PLCやセキュアエレメントへの統合を目的としたマイクロプロセッサ
7. 産業用のルータ、モデム、スイッチ
8. セキュアエレメント
9. ハードウェア・セキュリティ・モジュール（HSMs）
10. セキュア暗号プロセッサ
11. スマートカード、スマートカードリーダー、トークン
12. 産業用のPLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）
13. NIS 2 指令の別添Iに記載された重要エンティティが使用する産業用IoT機器
14. ロボットセンシング/アクチュエーターコンポーネント及びロボットコントローラー
15. スマートメーター

【米国】U.S. Cyber Trust Mark（検討中）

- **FCC（米連邦通信委員会）**が2023年8月にNPRM（立法案公告）を公表した、**任意のラベリング制度**。米時間10月6日までパブコメを実施。
- **想定対象は「消費者用IoT機器」**（詳細は下記）。ラベリングを得た機器とその機器に関する情報を全国登録簿に掲載し、ラベルに付随するQRコードを通じて全国登録簿が参照できるような仕組みを想定。
- 今まで**NIST(米国立標準技術研究所）が公表してきた基準に基づく見込み**。なお、**消費者向けルーター、スマートメーターについては、別途セキュリティ要件を定義する**予定。
- **2024後半の運用開始を目指す。**

米FCC　NPRM（立法案公告）の主な内容

● **対象について**

以下２つを満たすものを提案。

(1) 物理的世界と直接相互作用するための、1つ以上のトランスデューサー（センサーまたはアクチュエーター）を備え、意図的にラジオ周波数を放出することができる（※intentional radiatorに限定）インターネット接続デバイス

(2) デジタル世界と相互作用するための、1つ以上のネットワークインターフェース（Wi-Fi、Bluetoothなど）

※ただし、FCCのCovered listや、米商務省のEntity List、米国防総省のList of Chinese Military Companiesの機器、またはその企業が生産する機器は対象外とする。

➢ 対象をIoT「機器」とするべきか、NIST定義に基づくIoT「製品」とするべきか（IoT機器＋バックエンド、ゲートウエイ等必要な追加部品）

➢ 「消費者」IoTに限定するべきか、「商業用」目的のものも含むべきか、対象は「使用方法」で判断するべきか。

● **スキーム・体制について**

第三者機関としてCyber LABs（Cybersecurity Labeling Authorization Bodies）を設置することを提案。

● **基準策定について**

➢ NIST基準をどのように活用できるか。その他考慮するべき基準はあるか。

➢ よりリスクが高いIoT機器・機器の分類には、別途基準を策定するべきか。

経済産業省においてIoTセキュリティ適合性評価制度の検討会を立ち上げ

- **IoT機器の急増に伴い、IoT機器の脆弱性を狙ったサイバー脅威が高まってきた**ことから、**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構築が必要**。また、我が国のIoT製品がグローバルマーケットから弾き出されないよう、諸外国の取組を考慮することが必要。
- こうした観点で制度の検討を行うため、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３回開催し、2023年5月に**中間報告をとりまとめた**。委員は、学術界、法曹界、業界団体、企業、消費者団体から構成。オブザーバとして、関係省庁、研究機関、認証機関が参画。 2023年度中の最終報告に向け議論を継続中。
- 国内での議論と並行して、米EU等の諸外国との制度調和を図るための国際的な対話も実施中。

中間報告（概要）

検討会において議論した事項

● **課題**

ベンダ、利用者、国民の三者において、以下の課題が存在。

✓ **ベンダ**： **対策が評価されず製品価値に繋がらない**。諸外国の制度対応負担が増加。
✓ **利用者**： **適切な対策の製品が可視化されていないため、適切な製品を選べない**。
✓ **国民**： 適切でない製品が多く流通した場合、IoTがボット化するなどして、**国内のシステムや国民生活に悪影響を及ぼす**。

● **構築すべき適合性評価制度**

✓ ベンダによる能動的なセキュリティ向上を促す観点や、特に中小企業の負担の観点から、**まずは任意制度として制度を運用することが適当**。**ただし、制度の浸透具合や、諸外国の動向によっては、法令に基づく義務化の検討も必要になり得る**。

✓ 対象製品範囲については、「**間接的又は直接的にインターネットに接続する製品**」とすることが適当。その上で、具体的な対象製品については今後要検討。

✓ 適合性評価基準については、国際的な標準を参照の上、**国際的な標準と整合的な形で構築していくことが適当**。その上で、具体的にいかなる製品にどのような基準を適用するかは今後要検討。

✓ 運用については、**既存の評価スキームを活用**した制度とすることが適当。その上で、具体的にどのようなスキームを活用すべきかは今後要検討。

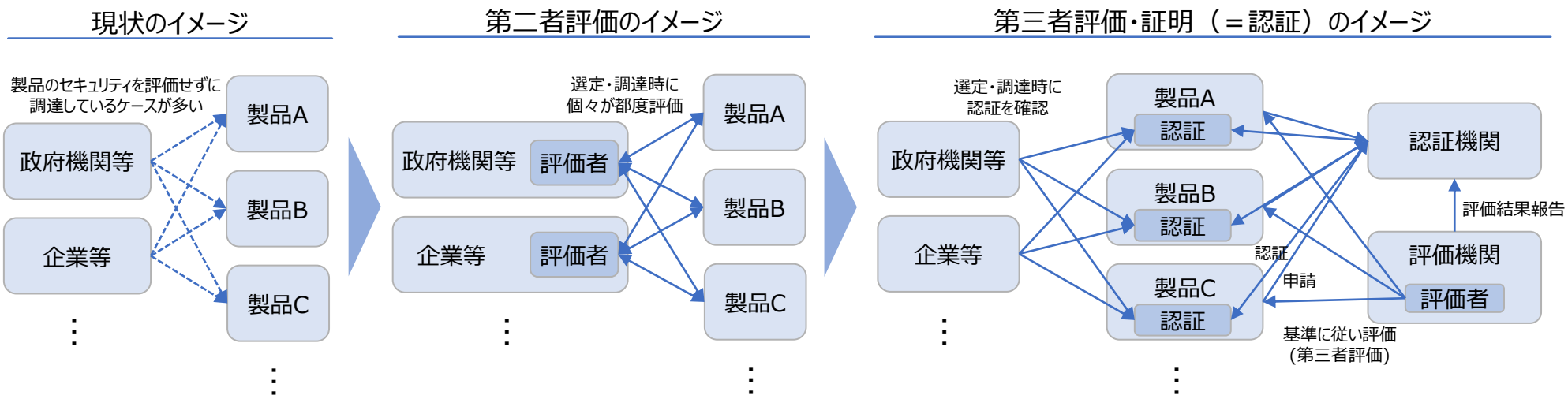
今後議論が必要な事項

上記に加え、政府の関与や検討体制のあり方、IoT製品ベンダーの能動的な制度活用を促す仕掛け、適合性評価済製品におけるセキュリティ事案への対応。

【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】会議資料
ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会） （METI/経済産業省）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html

【目的①】政府機関等・企業等のIoT製品調達ニーズへの対応

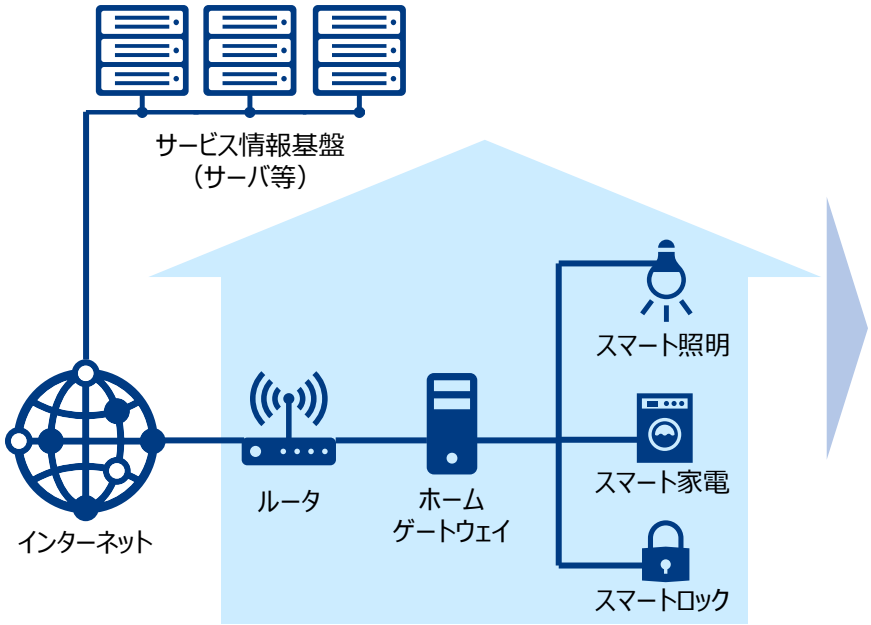
- 政府機関等・企業等のセキュリティ対策において、**調達する製品や製品ベンダーのセキュリティも含めた広義なサプライチェーンリスク管理の取り組みが広がっている**。
- その際、IoT製品のセキュリティに関して、選定時や調達時に、その**セキュリティ機能や対策状況を自組織で確認すること（第二者評価）が本来必要であるが、そのための確認プロセスを整備できている政府機関等・企業等は少ないのが現状**である。一方、仮に政府機関等・企業等がそのプロセスを整備する場合、調達を行う各組織においてその**確認のための知識と工数が必要**となり、またIoT製品ベンダーは各者から**異なる要件に対して繰り返し回答・対応が求められ**、双方対応しきれなくなる。
- そこで、第二者評価を代替する仕組みとして、**共通的な物差しでIoT製品のセキュリティを第三者が評価し、その結果に対して認証を付与する制度**を整備する。政府機関等・企業等は**認証取得の確認をベースとして活用**しながら、必要な場合に追加的な確認を実施することで、各組織の求めるセキュリティ水準のIoT製品を選定・調達することが可能となる。
- **政府機関等の第二者評価の代替として公平・中立な認証を行うためには公的機関（IPA）が認証機関**となり、制度を維持・運営していくことが望ましい。



【目的②】特定分野で使用されるIoT機器の最低限のセキュリティ確保

- IoT製品は、単体で比較・検討されて調達されるだけではなく、**特定分野のシステムに組み込まれて調達され、利用される**ケースもある。そのようなケースでは、最終調達者（ユーザー）がセキュリティを考慮したIoT製品を直接選定するのではなく、システムに組み込まれる段階で選定・調達される。（例）**スマートホーム、工場システム、ビルシステム**など
- **特定分野のシステムそれぞれの想定するユースケース、守るべき資産、脅威、リスクを定義**し、実施すべき対策のひとつとして、**組み込まれるIoT製品に求めるセキュリティ要件を定める**必要がある。当該要件で、IoT製品類型共通の☆1以上が必要となる場合に、**☆2以上の整備を本制度で検討**する。
- 各業界団体等では、特定分野のシステムのセキュリティに対して、**それぞれの用途や機能を考慮し、組み込むIoT製品のセキュリティ要件として必要な認証・ラベルを指定**する。その他のセキュリティ要件も含めたセキュリティガイドラインの作成や、システム全体としての認証制度等の整備を行い、**その準拠を業界標準とする**ことで、**当該特定分野のシステムにおいて、最低限のセキュリティが確保されたIoT機器のみが採用される**ことを目指す。

【特定分野のシステムのイメージ（スマートホームの例）】



【各IoT製品に求める認証・ラベル指定のイメージ】

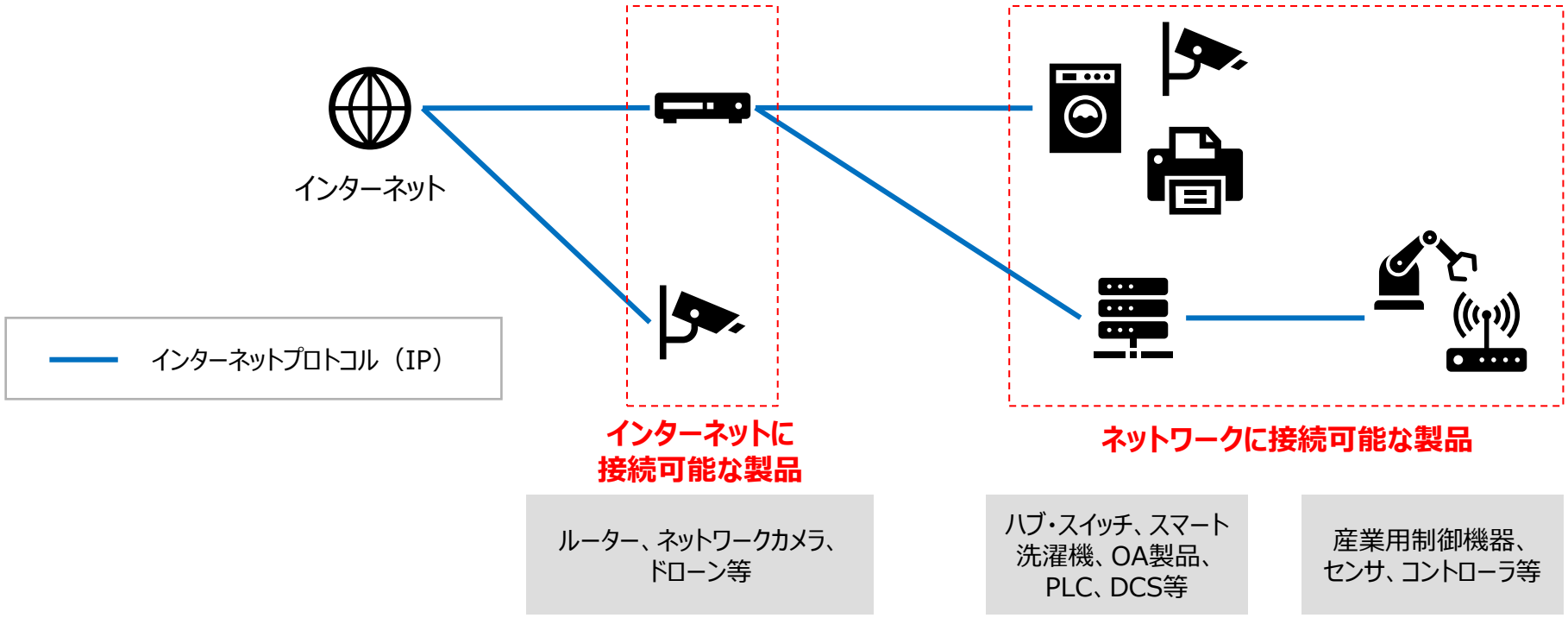
IoT製品	認証・ラベル	指定理由（例）
ルータ	☆2以上	• 外部からの侵入ルートになる可能性があるため
ホームゲートウェイ	☆2以上	• 外部からの侵入ルートになる可能性があるため
スマート照明	☆1以上	• 機器単体が侵害を受けても被害は限定的であるため
スマート家電	☆1以上	• 機器単体が侵害を受けても被害は限定的であるため
スマートロック	☆2以上	• 侵害が受けた場合、人的資産や物理的資産の損害に繋がる恐れがあるため

※ システムの重要度・規模やIoT製品の用途で指定する認証・ラベルを分けることもある。

本制度における対象製品の定義

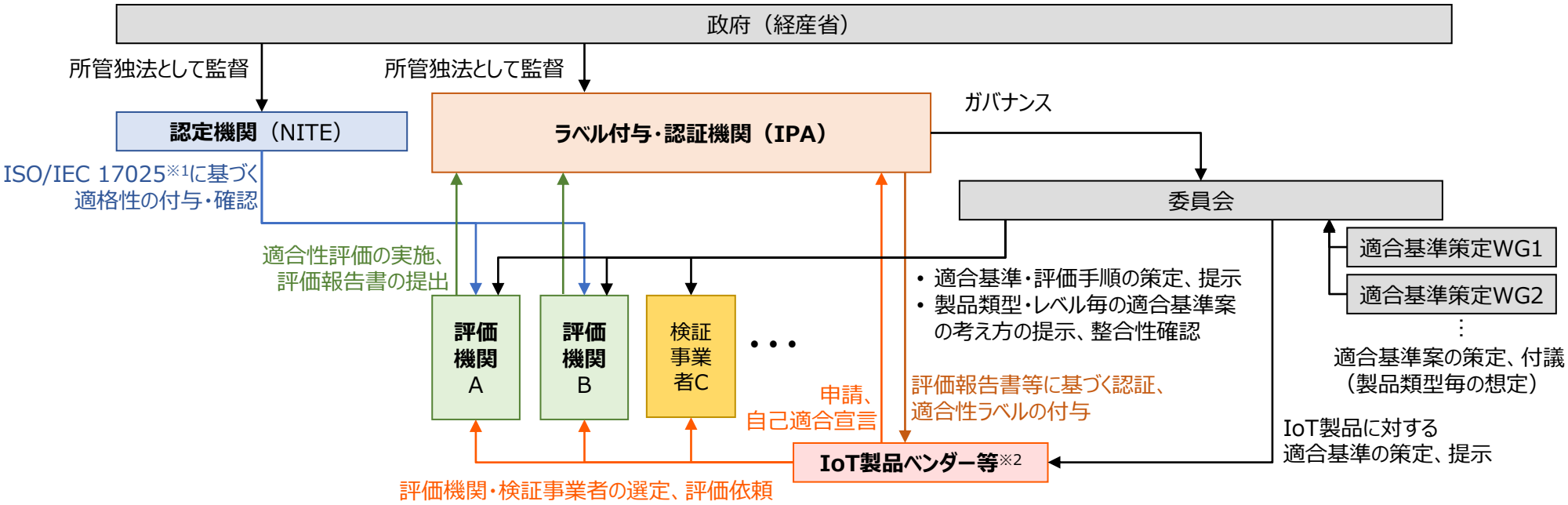
- 本制度では、**インターネットプロトコル（IP）を使用してデータを送受信する機能を持つ以下のIoT製品**(※1)を対象とする。
  - **インターネットに接続可能な製品**：IPを使用してインターネット上でデータを送受信する機能を持つ製品
  - **ネットワークに接続可能な製品**：IPを使用して、他の「インターネットに接続可能な製品」又は「ネットワークに接続可能な製品」に接続し、データを送受信する機能を持つ製品
- ただし、広くITシステムで利用されており、利用者が任意のソフトウェアにより随時かつ容易にセキュリティ機能を変更することができる汎用的なIT製品（PC、タブレット端末等）は対象外(※2)とする。

※1：ETSI EN 303 645の定義を参照し、「IoT製品（IoT product）」には、IoT機器（IoT device）とその関連サービスを含む。
※2：英国PSTI法、総務省端末設備等規則等の国内外制度も同様の理由で対象外としている。



適合性評価制度の想定スキーム

- これまでの議論を踏まえ、本制度の各主体の適格性について、政府のガバナンスが効く構造が重要。係る観点から**CC認証の知見があるIPAのJISEC認証制度**（ITセキュリティ評価及び認証制度）**を拡張する形の制度**を構築予定。
- プレ委員会を設置し、**2023年度末までに製品類型共通で最低限必要となる☆1の要求基準・適合基準の検討**および**ルーター、スマート家電等を対象とした評価検証**を実施中。

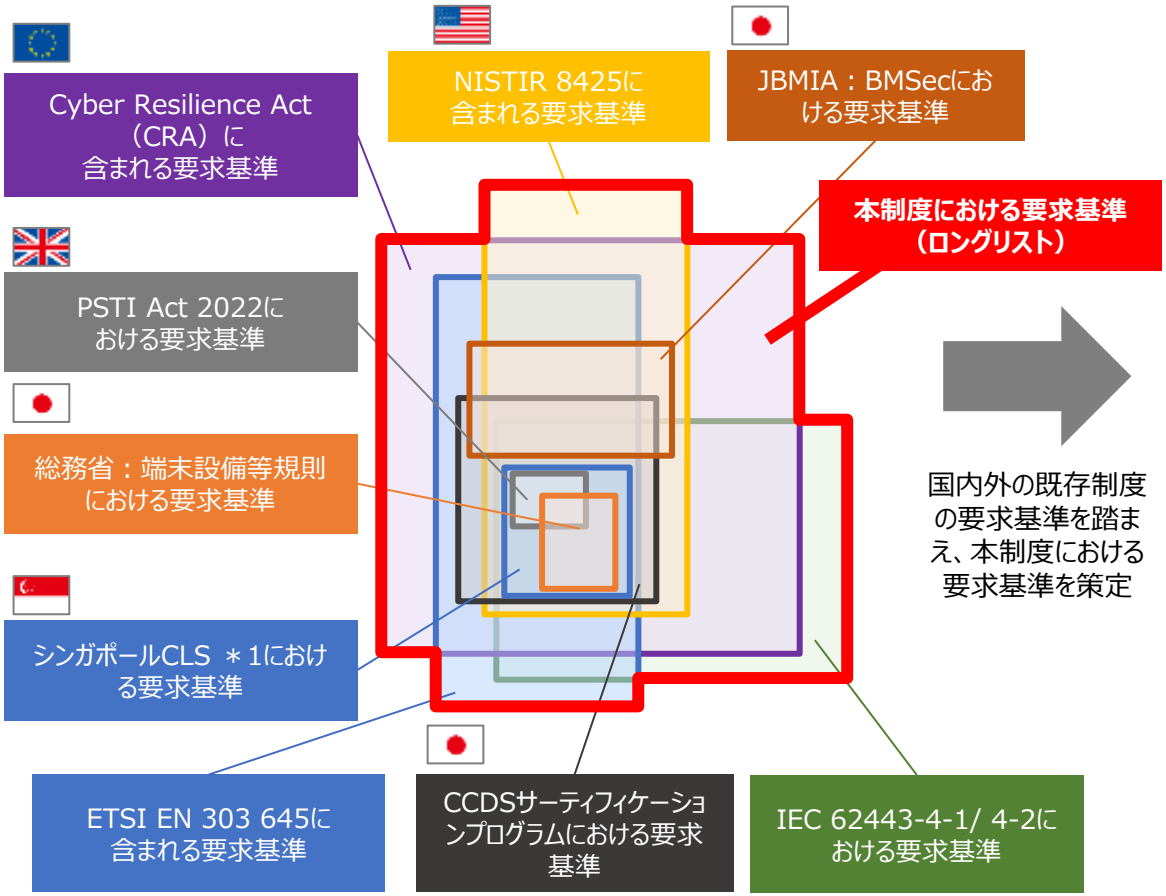


※1：ISO/IEC 17025（JIS Q 17025）は、試験所及び校正機関の試験・校正能力に関する一般要求事項を規定した国際標準であり、JISEC認証制度に基づくIT製品及びシステムのセキュリティ評価を行う試験事業者に求められる。なお、ISO/IEC 17065（JIS Q 17065）は、製品認証機関の認証能力に関する一般要求事項を規定した国際標準である。
※2：IoT製品を製造するベンダーだけでなく、海外からIoT製品を輸入・販売する輸入業者も含まれる。

国際基準を踏まえた要求基準案

- 要求基準は、本制度で対象となるIoT製品において求められうるセキュリティの要求の全体（ロングリスト）であるため、ETSI EN 303 645、NISTIR 8425、EU-CRA等の国内外の要求基準の集合関係を踏まえ、**重ね合わせの関係（∪（カップ））にある要求事項のロングリストを整理**。

諸外国制度において求められる要求基準の関係性イメージ



本制度における要求基準（ロングリスト）のイメージ

要求基準案	
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、製品ごとに固有であるか、又は利用者によって定義されるものでなければならない。
	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。
	1-3. 製品に対して利用者を認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる暗号技術を使用していなければならない。
	・・・
2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない： • 問題を報告するための連絡先情報； • 以下のタイムラインに関する情報： 1) 最初の受領確認； 2) 報告された問題が解決されるまでの状況の更新。
	・・・
・・・	・・・

諸外国の適合性評価制度との国際連携に向けて

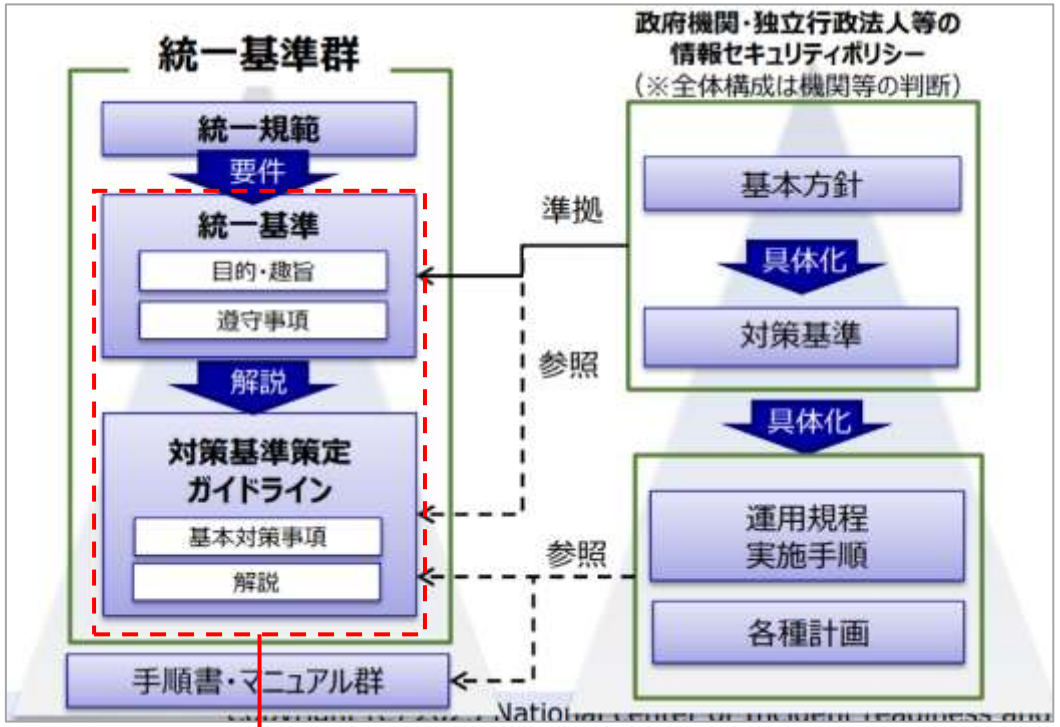
- **<u>☆１開始時に導入されている、シンガポールCLS（の＊１）と英PSTI法を内包</u>**するべく基準を設計する。
- ☆１開始時に制度設計途中の見込みである**<u>欧CRA及び米Cyber Trust Markについては、差分を確認し、国内基準（☆１更新時又は来年度以降に検討をする☆２以上）で包含又は追加対応を要する差分の公表等で対応</u>**する。
- 国内制度設計と並行して、☆１相互承認に向けて諸外国と調整を行う。
- 同時に、国際標準化に向けてISO/IEC 27404等の動きと連携をする。

国・地域					
制度名	発展JISEC制度	Cybersecurity Labelling Scheme（CLS）	Product Security and Telecommunication Infrastructure Act（PSTI法）	U.S. Cyber Trust Mark（仮）	Cyber Resilience Act（CRA）
開始時期	☆1：2024年度下期開始予定 ☆2以上：2025年度以降開始予定	2020年10月制度開始	2024年4月施行	2024年中に開始予定	未定（2027年開始想定）
任意/義務	任意	任意	義務	任意	義務
対象	IoT製品	消費者向けIoT機器	消費者向けIoT製品	消費者向けIoT機器（想定）	デジタル製品
適合基準	☆1：ETSI EN 303 645及びCLSの記載内容を中心に検討中（ただし、一部の記載については、総務省技適の要件、CCDSの要件の参照のほか、事務局にて記載内容を検討）	• ＊：ETSI EN 303 645の基準の一部※1 • ＊＊：＊の基準に加え、ETSI EN 303 645の基準の一部※2 • ＊＊＊及び＊＊＊＊：＊＊の基準に加え、IMDA「IoT Cyber Security Guide」の9つのライフサイクル基準	ETSI EN 303 645の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	NISTIR 8425をベースとした基準となる見込み	• 基本的な対策基準のほか、SBOM等に基づく脆弱性管理、脆弱性報告等、広範な基準が求められる予定 • 法案の内容について（欧州委員会・議会・理事会間で）政治合意がなされた後、法案に伴う基準がETSI EN 303 645等を参照して設定される予定
評価方法	☆1：自己適合宣言 ☆2：自己適合宣言（ただし、一定のスキル要件を満たした評価者による評価を求める） ☆3以上：第三者認証を求める方針	• ＊及び＊＊：自己適合宣言 • ＊＊＊及び＊＊＊＊：自己適合宣言及び評価機関による試験	自己適合宣言	検討中	• 「重要なデジタル製品」以外の製品：自己適合宣言 • 「重要なデジタル製品」のクラスⅠ（リスクが低い製品）でEUCCやEN規格の対象外の製品及びクラスⅡ（リスクが高い製品）の製品：第三者認証

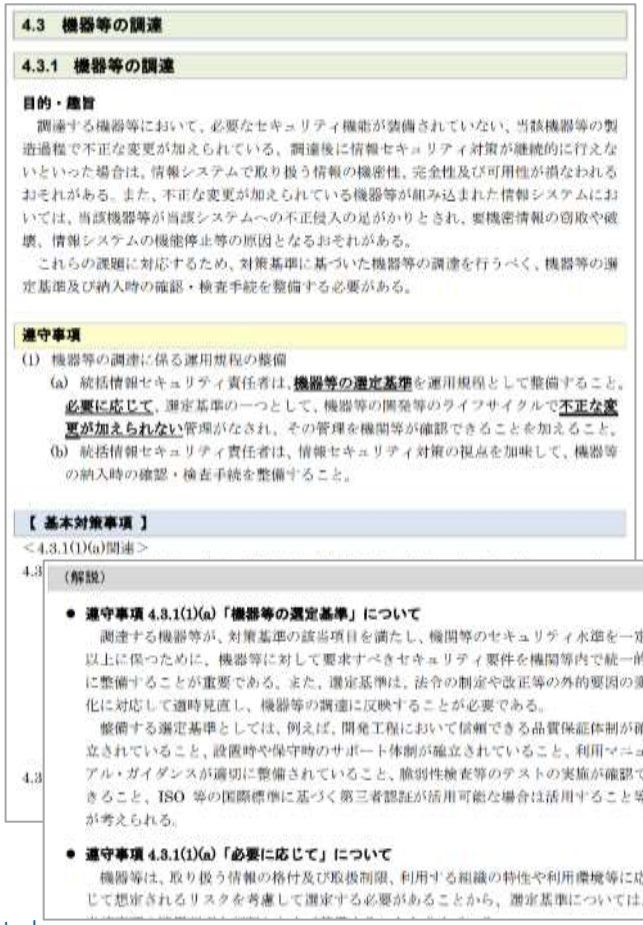
政府機関等の調達における本制度活用の検討

- 政府機関等が遵守すべき事項を定めた「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」およびそのガイドラインに、情報システムの重要度に応じ、**「重要度：低」は☆1以上**、**「重要度：高～中」は少なくとも☆3以上のIoT製品を各機関等の選定基準に含める**ことの追加をNISCと検討している。
- ラベル取得済み製品が普及する時期をめどに、政府機関等では**ラベル取得済みIoT製品の調達を必須化する方針**。

統一基準群（令和５年度版）文書体系



対策基準策定ガイドラインの「4.3.1 機器等の調達」の記載



4.3 機器等の調達

4.3.1 機器等の調達

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。また、不正な変更が加えられている機器等が組み込まれた情報システムにおいては、当該機器等が当該システムへの不正侵入の足がかりとされ、要機密情報の窃取や破壊、情報システムの機能停止等の原因となるおそれがある。

これらの課題に対応するため、対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

(1) 機器等の調達に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、**機器等の選定基準**を運用規程として整備すること。**必要に応じて**、選定基準の一つとして、機器等の開発等のライフサイクルで**不正な変更が加えられない**管理がなされ、その管理を機関等が確認できることを加えること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

【 基本対策事項 】

＜4.3.1(1)(a)関連＞

（解説）

- **遵守事項 4.3.1(1)(a)「機器等の選定基準」について**

調達する機器等が、対策基準の該当項目を満たし、機関等のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要件を機関等内で統一的に整備することが重要である。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の調達に反映することが必要である。

整備する選定基準としては、例えば、開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること等が考えられる。

- **遵守事項 4.3.1(1)(a)「必要に応じて」について**

機器等は、取り扱う情報の格付及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮して選定する必要があることから、選定基準については、

統一基準の記載内容

上記遵守事項に対する基本対策事項と解説をガイドラインに記載

出所）NISC「統一基準群改定のポイント（令和５年度版）」https://www.nisc.go.jp/policy/group/general/kijun.html
NISC「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

【参考】IoT製品の類型・既存の文書、認証制度等

【凡例】
- 製品個別のセキュリティ対策に関するガイドライン
- 製品個別のセキュリティ対策基準を定めた文書等（下線は義務）
- 製品個別のセキュリティ対策要件を含む認証制度
- システム全体のセキュリティ対策に関する文書等

赤字：Sマークによる認証が行われている製品

注）各製品類型に対するセキュリティ対策要件を定めたガイドラインや認証制度のうち、代表的なガイドライン、制度等をマッピングしている。ただし、CC（ISO/IEC 15408）に基づく認証制度については、グローバルで認証付与されている代表的な製品類型又はcPP(Collaborative Protection Profile)が用意されている製品類型に対してマッピングをしている。また、IEC 62443-4に基づく認証について、IEC 62443-4の対象である通信機能を有する産業用自動制御システムのコンポーネントに対してマッピングしている。

		製品類型	製品個別の対策に関するガイドライン、基準を定めた文書、認証制度等	高いレベルの基準に基づく認証制度	システム全体の対策に関する文書等
直接的又は間接的にインターネットに接続する製品	直接的にインターネットに接続する可能性がある製品	消費者向け	通信機器（ブロードバンドルーター、Wi-Fiルーターなど）	総務省：技術基準適合認定及び設計についての認証	CCDS：分野別ガイドライン（IoT-GW編） CCDS：CCDSサーティフィケーションプログラム（現状で取得実績は無いが、対象製品範囲に含まれる）		経産省：スマートホームセキュリティガイド CCDS：分野別ガイドライン（スマートホーム編）
			防犯関連機器（ネットワークカメラなど）		日本防犯設備協会：RBSS（監視カメラ、デジタルレコーダー）		
			自律型ロボット（ドローンなど）		NEDO：無人航空機分野 サイバーセキュリティガイドライン		
		産業向け	通信機器（ルーター、アクセスポイント、ファイアウォール、UTMなど）			CC認証 IEC 62443-4に基づく認証	
			防犯関連機器（ネットワークカメラなど）		日本防犯設備協会：RBSS CCDSサーティフィケーションプログラム（カメラで実績あり） IPA：情報セキュリティ対策要件チェックリスト（ネットワークカメラ）		
			産業用自律型ロボット（産業用ドローン、AGVなど）		NEDO：無人航空機分野 サイバーセキュリティガイドライン 国交省：機体認証制度		
	間接的にインターネットに接続する製品	消費者向け	通信機器（ハブ・スイッチなど）		CCDS：CCDSサーティフィケーションプログラム（現状で取得実績は無いが、対象製品範囲に含まれる）		経産省：スマートホームセキュリティガイド CCDS：分野別ガイドライン（スマートホーム編）
			生活家電（掃除機、洗濯機、冷蔵庫、レンジ、エアコンなど）				
			AV機器（スマートTV、レコーダー、スマートスピーカーなど）				
			防犯関連機器（警報装置、電気錠システムなど）		日本防犯設備協会：RBSS CCDS：CCDSサーティフィケーションプログラム（電気錠操作盤、電子シャッターで取得実績あり）		
			エネルギー関連機器（エネファーム、PCS、ガス給湯器など）		JET：系統連系保護装置等認証制度（PCSのみ） CCDSサーティフィケーションプログラム（ガス給湯器リモコンで実績あり） 各一般送配電事業者：系統連系技術要件		
			ヘルスケア機器（ウェアラブル端末、電動トレーニングマシンなど）				
			娯楽機器（ゲーム機、スマート玩具など）				
		産業向け	通信機器（ハブ・スイッチなど）			CC認証 IEC 62443-4に基づく認証	※
			産業用コントローラー（PLC、DCSコントローラーなど）				※
			産業用センサー（温度センサー、圧力センサー、変位センサーなど）				※
			OA機器（複合機など）		JBMIA：BMsec	CC認証	
			金融関係機器（決済端末、POS端末など）		CCDS：分野別ガイドライン（ATM編、オープンPOS編）→ CCDS：CCDSサーティフィケーションプログラム（ATM、決済端末で取得実績あり）		FISC：安全対策基準
			施設管理機器（入退室機器、受変電設備、照明、昇降機など）		IPA：情報セキュリティ対策要件チェックリスト（入退室管理）	CC認証 IEC 62443-4に基づく認証	経産省：ビルガイドライン
			医療機器（人工呼吸器、人工心臓弁、輸液ポンプなど）		厚労省：医療機器のサイバーセキュリティの確保及び徹底に係る手引書 → 厚労省：医療機器の薬事承認等		厚労省：医療情報ガイドライン
			自動車関連機器（ECU、IVI、TCUなど）		国交省：道路運送車両の保安基準 CCDS：分野別ガイドライン（車載器編）	CC認証	
			電気事業関連機器（スマートメーター、発電設備、PCSなど）		JESC：スマートメーターシステムセキュリティガイドライン		JESC：電制ガイドライン
			製造業・流通業関連機器（生産設備、自動倉庫など）				経産省：工場ガイド 国交省：物流ガイド
			鉄道事業関連機器（CTC装置、PRC装置など）				国交省：鉄道ガイドライン
			航空事業関連機器（IMS、iDMUなど）				国交省：航空ガイドライン

※ 各産業分野に設置される機器については、各ガイドラインにおいて、システム全体に求められるセキュリティ対策が示されている。

METI
Ministry of Economy, Trade and Industry

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