経済産業省

# 経済産業省のサイバーセキュリティ政策

経済産業省　商務情報政策局

サイバーセキュリティ課

吉川 弘晃

# 1．サイバーセキュリティ戦略

# 2．経済産業省の政策

## 2.1．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）
～サイバーセキュリティ経営ガイドライン
～サイバーセキュリティお助け隊サービス
～高度セキュリティ人材の育成
～日米欧によるインド太平洋地域の能力構築支援

## 2.2．国際連携を意識した認証・評価制度の立ち上げ

～IoT適合性評価制度
～SBOM（Software Bill Of Materials）
～QUAD上級サイバー会合、G7等を通じた連携

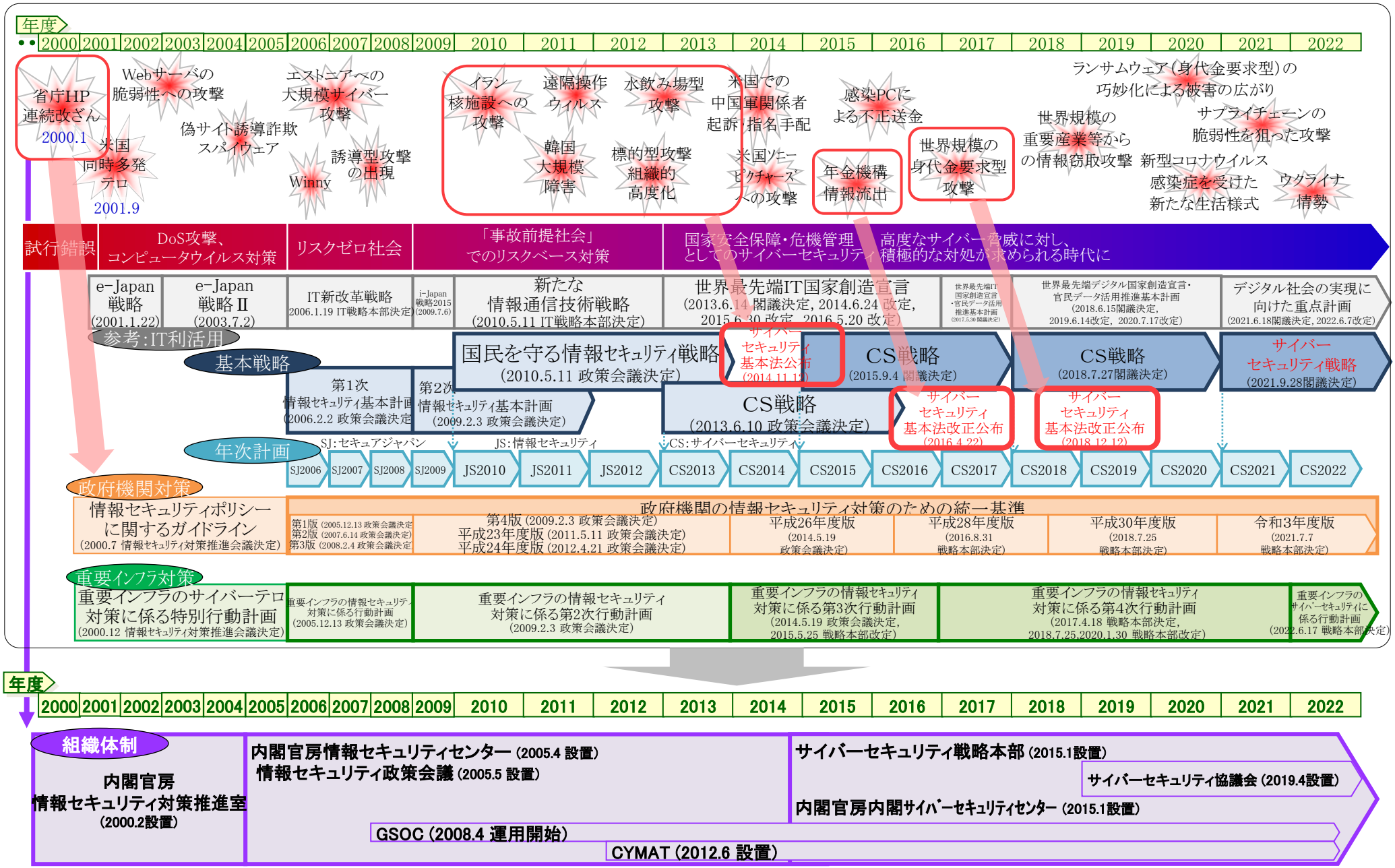
## 2.3．政府全体でのサイバーセキュリティ対応体制の強化

～国境を越えて行われるサイバー攻撃への対処能力向上
～重要インフラ事業者等での事案発生時の初動対応体制強化
～事故調査体制の構築
～サイバー攻撃被害情報の共有促進

## 2.4．新たな攻撃を防ぎ、守るための研究開発の促進

～セキュリティ産業の成長加速化

# サイバーセキュリティ政策の経緯



# サイバーセキュリティ政策の推進体制

**内 閣**　内閣総理大臣

**国家安全保障会議（NSC）**

緊密連携

## サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）※

**本部長**　内閣官房長官

**副本部長**　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣

**閣僚本部員**　国家公安委員会委員長
デジタル大臣
総務大臣
外務大臣
経済産業大臣
防衛大臣
経済安全保障担当大臣

**有識者本部員**

| | |
|---|---|
| 上沼 紫野 | 弁護士（虎ノ門南法律事務所） |
| 遠藤 信博 | 日本電気(株)特別顧問 |
| 後藤 厚宏 | 情報セキュリティ大学院大学学長 |
| 酒井 啓亘 | 京都大学大学院法学研究科教授 |
| 桜井 敬子 | 学習院大学法学部教授 |
| 田中 孝司 | KDDI(株)代表取締役会長 |
| 土屋 大洋 | 慶應義塾大学大学院教授 |
| 松原実穂子 | 日本電信電話(株)チーフ・サイバーセキュリティ・ストラテジスト |
| 村井 純 | 慶應義塾大学教授 |

① サイバーセキュリティ戦略の案の作成及び同戦略の実施推進
② 国の行政機関・独法・指定法人における対策基準の作成／監査等
③ 国の行政機関・独法・指定法人で発生した重大事象について原因究明調査等
④ サイバーセキュリティに関する事象が発生した場合の国内外の関係者との連絡調整
⑤ 重要施策の企画・調査・審議、経費見積り方針等の指針の作成、総合調整

重要インフラ専門調査会 | 研究開発戦略専門調査会 | 普及啓発・人材育成専門調査会 | サイバーセキュリティ対策推進会議（CISO等連絡会議）

緊密連携

**デジタル庁**

デジタル社会の形成に向けた司令塔としてデジタル改革を推進

連携

**サイバーセキュリティ協議会**

官民の多様な主体が相互に連携した、より早期の段階での、サイバーセキュリティの確保に資する情報の迅速な共有等

**<重要インフラ所管省庁>**
〔所管重要インフラ事業におけるサイバーセキュリティの確保〕
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス、化学、クレジット、石油）
国土交通省（鉄道、航空、物流、空港）

**<その他関係省庁>**
文部科学省（セキュリティ教育）等

協力

（事務局）

## 内閣官房 内閣サイバーセキュリティセンター（NISC）（2015.1.9 内閣官房組織令により設置）

〔各省のサイバーセキュリティ施策の統一性保持のための総合調整〕

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）

副センター長（内閣審議官）

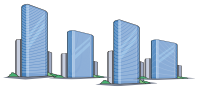
政府関係機関・情報セキュリティ横断監視・即応調整チーム（GSOC）

情報セキュリティ緊急支援チーム（CYMAT）

協力

**閣僚本部員６省庁**
〔各省の所掌に基づくサイバーセキュリティ施策の実施〕
警察庁（サイバー犯罪取締り）
デジタル庁（デジタル社会形成）
総務省（通信・ネットワーク政策）
外務省（外交・安全保障）
経済産業省（情報政策）
防衛省（国の防衛）


重要インフラ事業者等


政府機関（各府省庁）

企業


個人

# サイバーセキュリティ戦略2021

## 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

政府のサイバーセキュリティ関連予算
令和5年度予算政府案　1378.9億円

「自由、公正かつ安全なサイバー空間」の確保

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

情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

| 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**(G7,二国間,ランサムウェア対応 等)

## 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）

- 人材育成
- 普及啓発
- 研究開発の推進

※赤字は経産省が主体的に関与

# 1．サイバーセキュリティ戦略

# 2．経済産業省の政策

## 2.1．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）
～サイバーセキュリティ経営ガイドライン
～サイバーセキュリティお助け隊サービス
～高度セキュリティ人材の育成
～日米欧によるインド太平洋地域の能力構築支援

## 2.2．国際連携を意識した認証・評価制度の立ち上げ

～IoT適合性評価制度
～SBOM（Software Bill Of Materials）
～QUAD上級サイバー会合、G7等を通じた連携

## 2.3．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対処能力向上
～重要インフラ事業者等での事案発生時の初動対応体制強化
～事故調査体制の構築
～サイバー攻撃被害情報の共有促進

## 2.4．新たな攻撃を防ぎ、守るための研究開発の促進

～セキュリティ産業の成長加速化

# 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

- 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

サイバーセキュリティ お助け隊

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

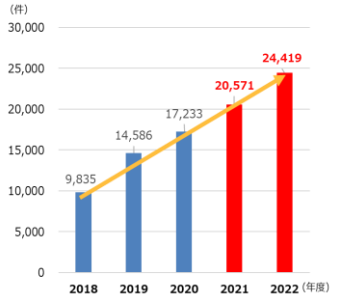
**SBOMの概念的イメージ**

| ID | サプライヤー名 | コンポーネント名 | コンポーネントのバージョン | その他の一意の識別子 | 依存関係 | SBOM作成者 | タイムスタンプ |
|---|---|---|---|---|---|---|---|
| 1 | Company A | Application | 1.1 | 234 | Primary | Company A | 05-09-2022 13:00:00 |
| 2 | Company B | Browser | 2.1 | 334 | Included in #1 | Company B | 04-18-2022 15:00:00 |
| 3 | Mr. C | Compression Engine | 3.1 | 434 | Included in #2 | Company A | 05-09-2022 13:00:00 |
| 4 | Community P | Protocol | 2.2 | 534 | Included in #1 | Company A | 05-09-2022 13:00:00 |

## 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新興）

- 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

# 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

**構成員**

- 泉澤　清次　三菱重工業株式会社取締役社長　※2022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、日本電気株式会社取締役会長等
- 大林　剛郎　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
- 櫻田　謙悟　経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役社長
- 篠原　弘道　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　一般財団法人アジア・パシフィック・イニシアティブ理事長
- 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、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

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

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

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

# 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

- **<u>7つの産業分野別サブワーキンググループ（SWG）</u>**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、**<u>3つのタスクフォース（TF）を設置</u>**

**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。

# 「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>**

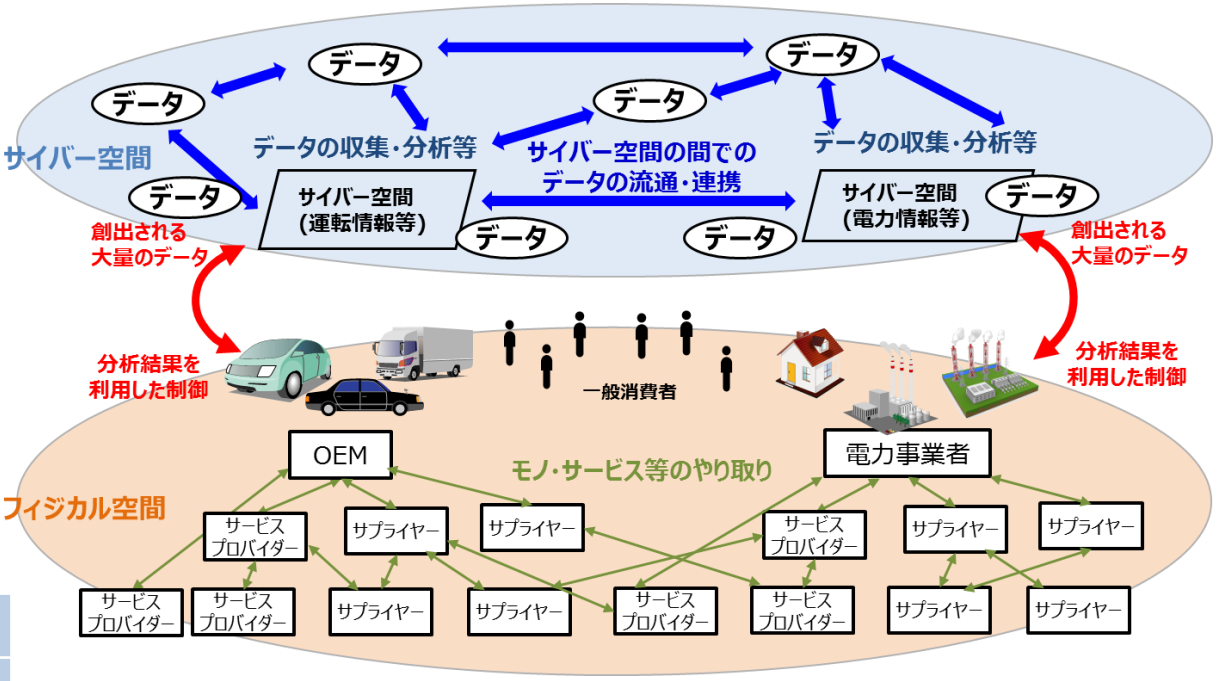
**【第３層】**
**サイバー空間におけるつながり**

**【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 |

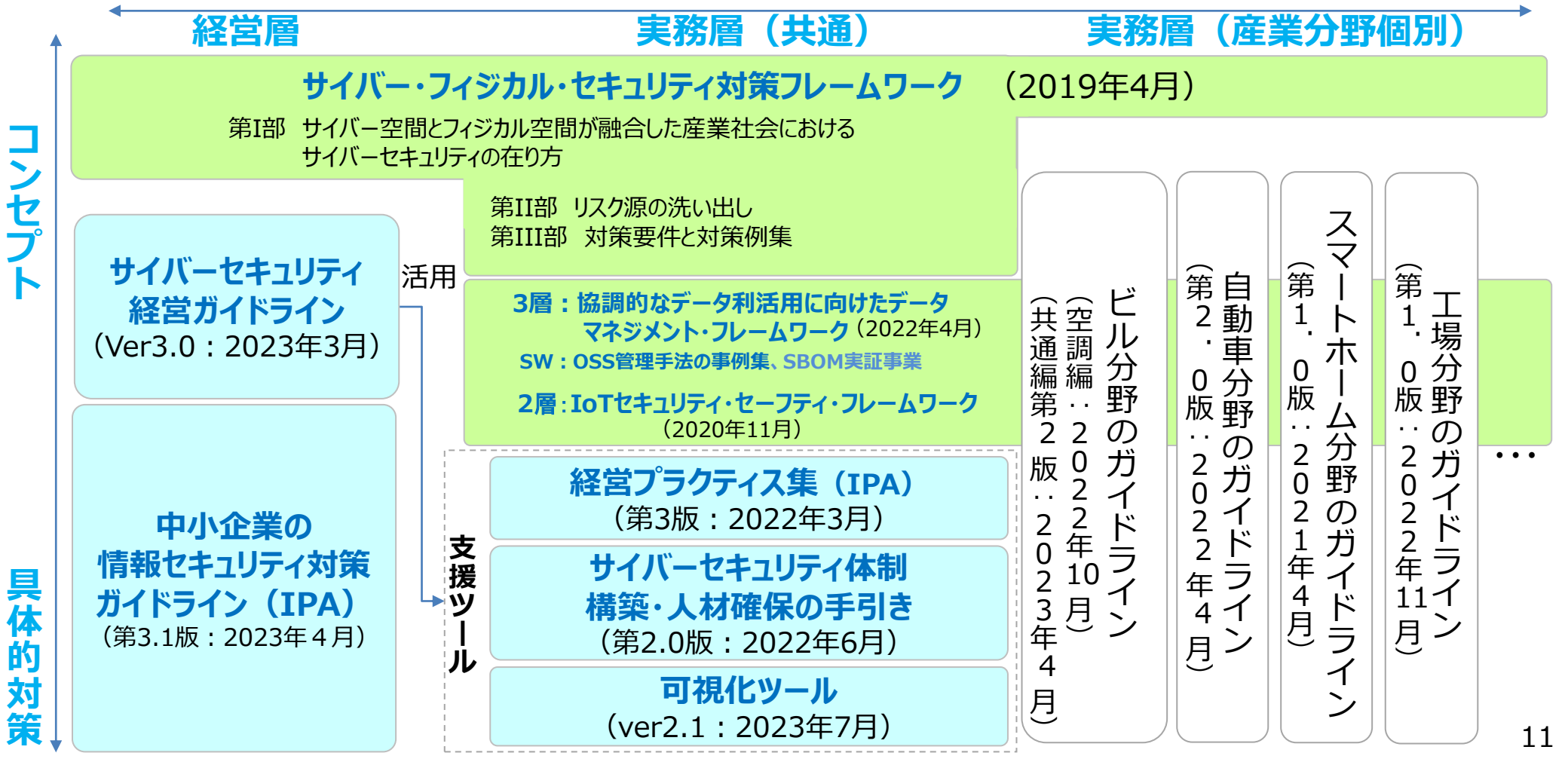



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

# 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＞



# 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

## 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**

# サイバーセキュリティ経営ガイドライン Ver3.0の改訂概要

- 経営者が指示すべき10の重要事項については、**デジタル環境の活用等の情勢の変化やサイバー・フィジカル空間の融合に対応した対策の必要性**を踏まえた改訂を実施

## ■ 経営者が指示すべき１０の重要事項

### リスク管理体制の構築

（指示１）**サイバーセキュリティリスクの認識、組織全体での対応方針の策定**
※経営リスクとして認識、組織全体の対応方針、公表

（指示２）**サイバーセキュリティリスク管理体制の構築**
※役割と責任の明確化、組織内のリスク管理体制とも整合

（指示３）**サイバーセキュリティ対策のための資源（予算、人材等）確保**
※外部ベンダーや自社のセキュリティ人材、プラス・セキュリティ

### リスクの特定と対策の実装

（指示４）**サイバーセキュリティリスクの把握とリスク対応に関する計画の策定**
※事業に用いるデジタル環境、サービス及び情報の特定、サイバー攻撃の脅威・影響度合を踏まえた対応計画

（指示５）**サイバーセキュリティリスクに効果的に対応する仕組みの構築**
※防御、監視・検知、分析、対応

（指示６）**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**
※サイバーセキュリティリスクの特徴、最新の脅威への対応

### インシデントに備えた体制構築

（指示７）**インシデント発生時の緊急対応体制の整備**
※CSIRT、PSIRT等（初動対応、再発防止）、情報開示、演習（制御系含む）

（指示８）**インシデントによる被害に備えた事業継続・復旧体制の整備**
※復旧目標、手順、体制、制御系含めたBCPとの連携、サプライチェーン含めた実践的な演習

### サプライチェーンセキュリティ

（指示９）**ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策**
※監査の実施など対策状況の把握、対策の導入支援や共同実施、緊急時の協力

### 関係者とのコミュニケーション

（指示10）**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**
※情報共有を行う関係の構築、被害の報告・公表への備え（IPA・JPCERT/CC、ISAC、CSIRT間の連携など）

# 企業経営におけるサイバーセキュリティ対策の重要性が拡大

- 「投資家と企業の対話ガイドライン」や「グループ・ガバナンス・システムに関する実務指針(グループガイドライン)」、「デジタルガバナンスコード」などにおいて、サイバーセキュリティ対策の必要性について言及。
- サイバーセキュリティリスクを組織の経営リスクの一環として認識し、サイバーセキュリティを包含するエンタープライズリスクマネージメントの実践が求められており、対策の実施を通じてサイバーセキュリティに関する残留リスクを許容水準まで低減することは経営者の責務。
- そのため、組織のリスクマネジメントの責任を担う経営者が自らの役割として実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが重要。

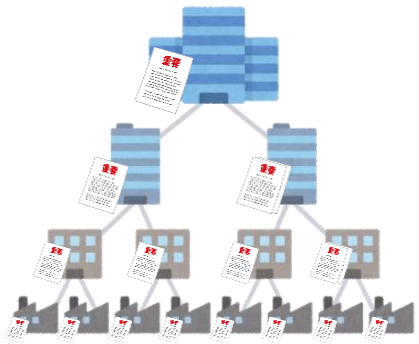
〔Ver.2.0〕
・セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必要なものと位置づけて「投資」と捉えることが重要
・セキュリティ投資は必要不可欠かつ経営者としての責務
・経営責任や法的責任が問われる可能性がある

〔Ver. 3 .0〕
・サイバーセキュリティ対策は「投資」（将来の事業活動・成長に必須な費用）と位置付けることが重要。企業活動におけるコストや損失を減らすために必要不可欠な投資
・サイバーセキュリティリスクを把握・評価した上で、対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務
・善管注意義務違反や任務懈怠（けたい）に基づく損害賠償責任を問われ得るなどの会社法・民法等の規定する法的責任やステークホルダーへの説明責任を負う

# サプライチェーン全体のサイバーセキュリティ対策が急務に

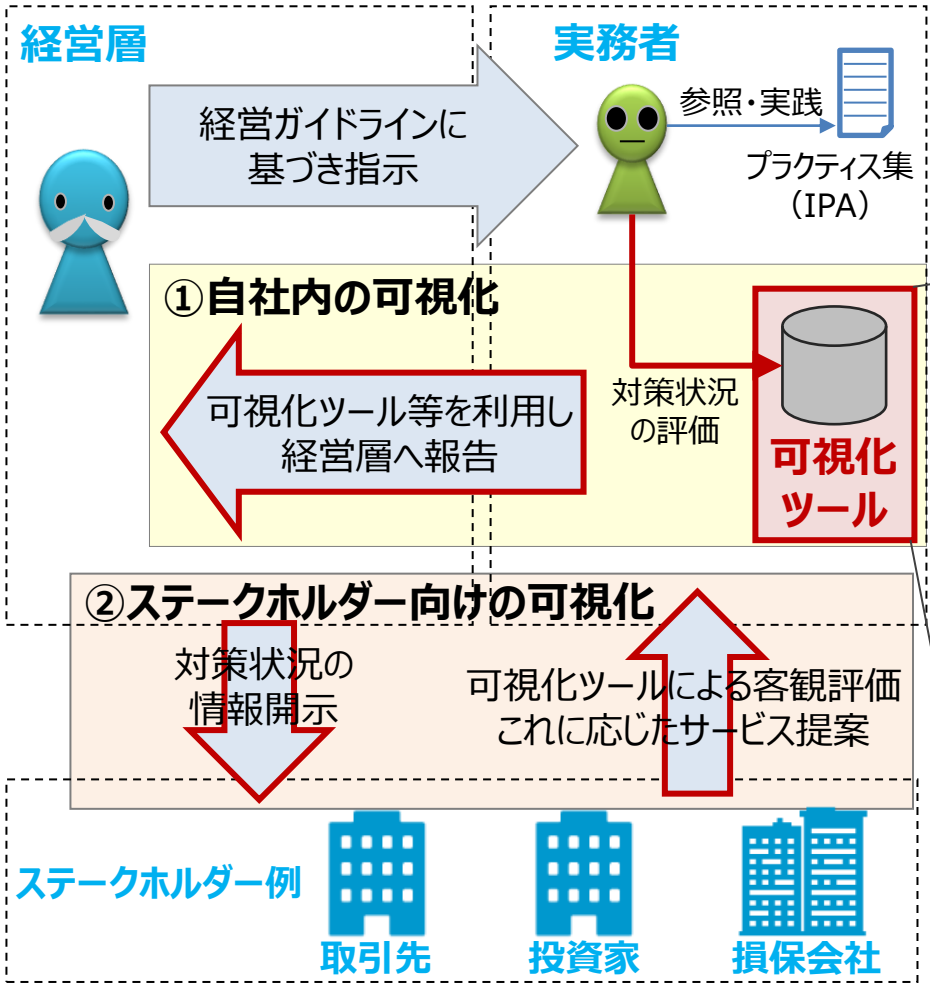
- **大企業から中小企業まで、サプライチェーンの弱点を狙ったサイバー攻撃が顕在化・高度化。**
  - 取引先への攻撃を起点として、自社のシステムが被害を受けるケース
  - サイバー攻撃による取引先の事業停止により、自社の事業が影響を受けるケース
  - ネットワーク監視等のソフトウエアのアップデートを通じてマルウエアが仕込まれ、被害を受けるケース

〔Ver. 3 .0〕
○経営者が認識すべき３原則（２）
・自社のサイバーセキュリティ確保に関する責務を全うするには、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
・サプライチェーン全体を俯瞰し、総合的なセキュリティ対策を徹底
○サイバーセキュリティ経営の重点10項目　指示９
・国内外の拠点、ビジネスパートナーや委託先等における状況等の把握をもとに、サイバーセキュリティ対策の役割、責任の明確化や対策の導入支援等、サプライチェーン全体での方策の実効性を高める適切な方策を検討



# 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（2023年7月Excel版、Ver2.1公開）。
- 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。




**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。2023年9月時点で35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。

EDR・UTMによる異常監視

緊急時の対応支援・駆け付けサービス

相談窓口

簡易サイバー保険

簡単な導入・運用

**中小企業のサイバーセキュリティ対策に不可欠な各種サービス**

**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**

**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。サプライチェーン全体の対処能力の底上げを目指す。

**IT導入補助金によるの導入支援**

※新たに「セキュリティ対策推進枠」を設置。
「お助け隊サービス」の単品での申請が可能に。

# サイバーセキュリティお助け隊サービス　登録サービスリスト

- 全国各地域の中小企業にとって選択・利用可能な「サイバーセキュリティお助け隊サービス」のリスト。現時点で35事業者がサービスを登録・提供中。

## 【サイバーセキュリティお助け隊サービス　事業者・登録サービスリスト】

| | 事業者名<br>(サービス名称) |
|---|---|
| 1 | **大阪商工会議所**<br>（商工会議所サイバーセキュリティお助け隊サービス） |
| 2 | **ＭＳ＆ＡＤインターリスク総研株式会社**<br>（防検サイバー） |
| 3 | **株式会社ＰＦＵ**<br>（PCセキュリティみまもりパック） |
| 4 | **株式会社AGEST**<br>（EDR運用監視サービス「ミハルとマモル」） |
| 5 | **ＳＯＭＰＯリスクマネジメント株式会社**<br>（SOMPO SHERIFF） |
| 6 | **株式会社アイティフォー**<br>（ランサムガード） |
| 7 | **富士ソフト株式会社**<br>（オフィスSOCおうちSOC） |
| 8 | **株式会社BCC**<br>（セキュリティ見守りサービス「＆セキュリティ＋」） |
| 9 | **中部事務機株式会社**<br>（CBM ネットワーク監視サービス） |
| 10 | **中部電力ミライズ株式会社**<br>（中部電力ミライズ　サイバー対策支援サービス） |
| 11 | **セントラル警備保障株式会社**<br>（ＣＳＰサイバーガード） |
| 12 | **沖電グローバルシステムズ株式会社**<br>（PCお助けパック　PC定期侵害調査プラン） |
| 13 | **株式会社コハマ**<br>（ネットワークセキュリティ見守り隊＆PCセキュリティ見守り隊サービス）<br>（ネットワークセキュリティ見守り隊） |
| 14 | **NTTコミュニケーションズ株式会社**<br>（マイセキュア　ビジネス） |
| 15 | **セキュアエッジ株式会社**<br>（セキュアエッジＭＤＲ９９） |
| 16 | **株式会社大塚商会**<br>（Cloud Edge運用支援EasySOC Plus　パック） |
| 17 | **株式会社アクロネット**<br>（アクロネットサイバーセキュリティサービス） |
| 18 | **コスモテレコム株式会社**<br>（ビジネスサポートサービス） |
| 19 | **京セラドキュメントソリューションズジャパン株式会社**<br>（TASKGUARD EDR WS セキュリティーサービス）<br>（TASKGUARD UTM CP セキュリティーサービス） |
| 20 | **三井物産セキュアディレクション株式会社**<br>（MBSD Global Security Platform<br>（略称：MGSP）） |
| 21 | **ラディックス株式会社**<br>（ラディックスお助け隊サービス） |
| 22 | **株式会社テクノル**<br>（MRⅡ Plus） |
| 23 | **株式会社四日市事務機センター**<br>（YONJINサイバーセキュリティ UTM）<br>（YONJINサイバーセキュリティ UTM&EDR） |
| 24 | **株式会社ハイテックシステム**<br>（TSOCエンドポイントパッケージ） |
| 25 | **株式会社アクシス**<br>（AXIS総合セキュリティパック）<br>－ネットワーク＆端末監視コース<br>－小規模ネットワーク＆端末監視コース<br>－端末監視コース |
| 26 | **富士フィルムビジネスイノベーションジャパン株式会社**<br>（beat/solo 見守りサービス） |
| 27 | **株式会社アクト**<br>（データお守り隊） |
| 28 | **株式会社ケーオウエイ**<br>（サイバーセキュリティお助け隊パック） |
| 29 | **株式会社ソフトクリエイト**<br>（SecurityFREEレスキュー隊 for PC監視） |
| 30 | **グローバルセキュリティエキスパート株式会社**<br>（サイバードラレコ） |
| 31 | **株式会社ブロードバンドセキュリティ**<br>（サイバープロテクション（CP）） |
| 32 | **ステラグループ株式会社**<br>（ステラお助け隊サービス） |
| 33 | **田中工業株式会社**<br>（ネットワークセキュリティパッケージ　パソコンセキュリティパッケージ） |
| 34 | **バリオセキュア株式会社**<br>（VCR116wPlus） |
| 35 | **タクテックス株式会社**<br>（タクテックスセキュリティサービス） |

# サイバーセキュリティ人材施策の全体像

- 昨年度は、「セキュリティ体制構築・人材確保の手引き」の改訂を行うとともに、セキュリティ人材育成の既存施策を進めつつ、特に、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」の取組を推進するため、SC3での検討や地域での具体的な取組を推進。

## 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

デジタル人材育成プラットフォームにおけるスキル標準の整理・教育コンテンツ・実践型教育

大学・高専等と産業界の連携

## 今後の方向性

- 手引きの普及による各企業での体制構築の促進と各種セキュリティ人材育成施策を引き続き実施するとともに、プラス・セキュリティの取組を普及させるため、SC3産学官連携WG、デジタル人材育成プラットフォーム、各地域における産学官連携の取組（地域SECUNITY）との連携による取組の具体化・拡大を進めていく。

# 情報処理安全確保支援士試験・情報処理技術者試験

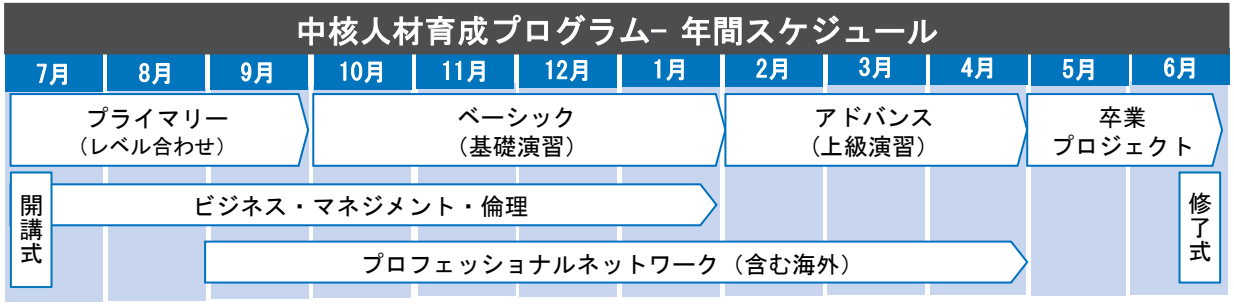
- 1969年から開始されたＩＴに関する知識・技能を客観的に評価するため「情報処理技術者試験」（国家試験）を2004年からIPAで実施。対象者別（IT利活用者・IT技術者）に試験体系を構築。
- 2017年度から、「情報処理安全確保支援士試験」を開始。

# 産業サイバーセキュリティセンター（ICSCoE）(2017年4月設置)

- 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年程度のトレーニング等を実施。
- 第7期中核人材育成プログラム（2023年7月開講）には、65名が参加。

**□　１年を通じた集中トレーニング**

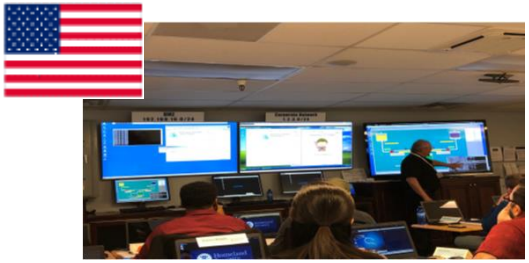
**□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣**
**（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人）**




- 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

# 中核人材育成プログラムの成果と修了者の活動

- 中核人材育成プログラム受講者は、１年間のプログラムで学んだ技術や人脈を業界の課題に当てはめていくことを主眼に、**プログラムの最後にチーム別の卒業プロジェクトに取り組む。**
- また、修了者の知見をアップデートし、また、その知見やノウハウを産業界や社会へ還元していくため、**業種横断の修了者コミュニティ「叶会」を運営。**経済産業省やＩＰＡの取組に貢献。

## 最近の卒業プロジェクトの成果物

**【第5期生　2022年6月】（一部紹介）**

- **未来のKidsサイバーセキュリティ教室～No SEC No Life～**

  子供たちがセキュリティについて積極的に学び、理解し易いように、動画やゲームといった児童向けの教育コンテンツ・教育カリキュラムを作成


- **IoT Sec for Users　5分でIoTのセキュリティリスクがわかる本**

  IoT機器に潜むセキュリティリスクを認識してもらうため、既存のガイドラインで紹介されているインシデント事例等をまとめたハンドブックを作成


https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/iot-sec.html

## 修了者コミュニティ　叶会

【目的】
- 卒業後も知見をアップデート
- 卒業年次・業種を超えた人脈形成
- 修了者の知見の社会還元


【主な活動】
- 年１回年次総会（11月）で最新動向と修了者の近況の活躍を発表。
- サイバーセキュリティ情報提供活動：
  情報共有ツール「SIGNAL」を使い、ICSCoEが入手した脆弱性情報等を修了者に提供。
- 東京以外の地域（関西・中京等）でも修了者がコミュニティを形成、各地でセミナー等を開催、またセキュリティ対応等のノウハウをシェア。
- 商工会や地銀と連携、会報や業界紙にセキュリティの啓発記事を掲載。

**●修了者の技術や知見の活用：「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」作成への貢献**

中核人材育成プログラムでビルが直面するセキュリティの課題と解決手法を学んだ受講者が、有志で経済産業省のビルSWGに参加。カリキュラムのアウトプットとして、経済産業省が2019年6月にリリースした「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」をより分かりやすく理解できる “解説書”を作成するとともに、ビル関係者向けの脆弱性情報やその解説の配信にも協力。

# インド太平洋地域向け日米EU産業制御システム（ICS）サイバーセキュリティ演習

- 経済産業省及びIPA産業サイバーセキュリティセンターは、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、エネルギー省、アイダホ国立研究所）、EU政府（通信総局）と連携し、**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（第５回）**を2022年10月に実施。

■ **日時・場所：**2022年10月24日（月）～28日（金）（ハイブリッド開催）

■ **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、台湾の電力・石油会社、National CERT、エネルギー及びサイバーセキュリティ関係政府機関から37名が参加。一部セミナー部分にはオブザーバーも含め約130名が参加。

■ **開催概要：**リモートでのハンズオン演習や、日米欧の専門家によるサイバーセキュリティ政策、サプライチェーンマネジメント及びエネルギー分野特有の課題も含むセミナーを提供するとともに、アイダホ国立研究所が提供するワークショップを提供。実機を用いたハンズオン演習など参加者に有益な能力構築機会を与えるとともに、参加者間の知見共有を行った。

## 演習の様子

経済産業省　上村審議官挨拶

ゴールドスタイン　米国DHS/CISA 長官代行挨拶


アロンソ 欧州通信総局デジタル社会・トラスト・サイバーセキュリティ局長挨拶



リモートハンズオン演習の様子

インド太平洋地域からの受講生

# サイバーセキュリティに関する米国国土安全保障省（DHS）との大臣級MOC

- **2023年1月6日、マヨルカス国土安全保障長官と西村経産大臣が会談**し、人権タスクフォースへの協力を確認するとともに、**サイバーセキュリティに関するMOCに署名**。
- 今回のMOCでは、①「国家安全保障戦略」の改定を踏まえた経済産業省と国土安全保障省との協力関係の深化、②**「開かれたインド太平洋（FOIP）」の実現に向けたインド太平洋における能力構築**、③サイバーセキュリティ制度調和の促進、の実現を目指す。

**【MOC概要】**

経済産業省と米国国土安全保障省は、高度化し増加し続けるサイバー攻撃への対応のため、関係機関からの協力も得ながら、以下のサイバーセキュリティ分野について協力を行う。

＜協力分野＞

- 運用面での協力
- 制御システムセキュリティの向上
- インド太平洋地域等の能力向上に関する協力
- サイバーセキュリティ関連規制及びスキームの調和のための対話促進

＜MOC改定のねらい＞

①「国家安全保障戦略」改定を踏まえた経済産業省とDHSとの協力深化
②「FOIP」実現に向けたインド太平洋地域での能力構築
③制度調和の促進

＜今回のMOCにおいて追加された協力分野＞

・インド太平洋地域等の能力向上
・日米間のサイバーセキュリティ関連規制・制度の調和に向けた対話
（SBOMやIoT機器ラベリング制度等の調和を想定）

# 1．サイバーセキュリティ戦略

# 2．経済産業省の政策

## 2.1．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）
～サイバーセキュリティ経営ガイドライン
～サイバーセキュリティお助け隊サービス
～高度セキュリティ人材の育成
～日米欧によるインド太平洋地域の能力構築支援

## 2.2．国際連携を意識した認証・評価制度の立ち上げ

～IoT適合性評価制度
～SBOM（Software Bill Of Materials）
～QUAD上級サイバー会合、G7等を通じた連携

## 2.3．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対処能力向上
～重要インフラ事業者等での事案発生時の初動対応体制強化
～事故調査体制の構築
～サイバー攻撃被害情報の共有促進

## 2.4．新たな攻撃を防ぎ、守るための研究開発の促進

～セキュリティ産業の成長加速化

# 経産省においてIoT適合性評価制度検討会立ち上げ

- **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。

→ **JISEC制度**

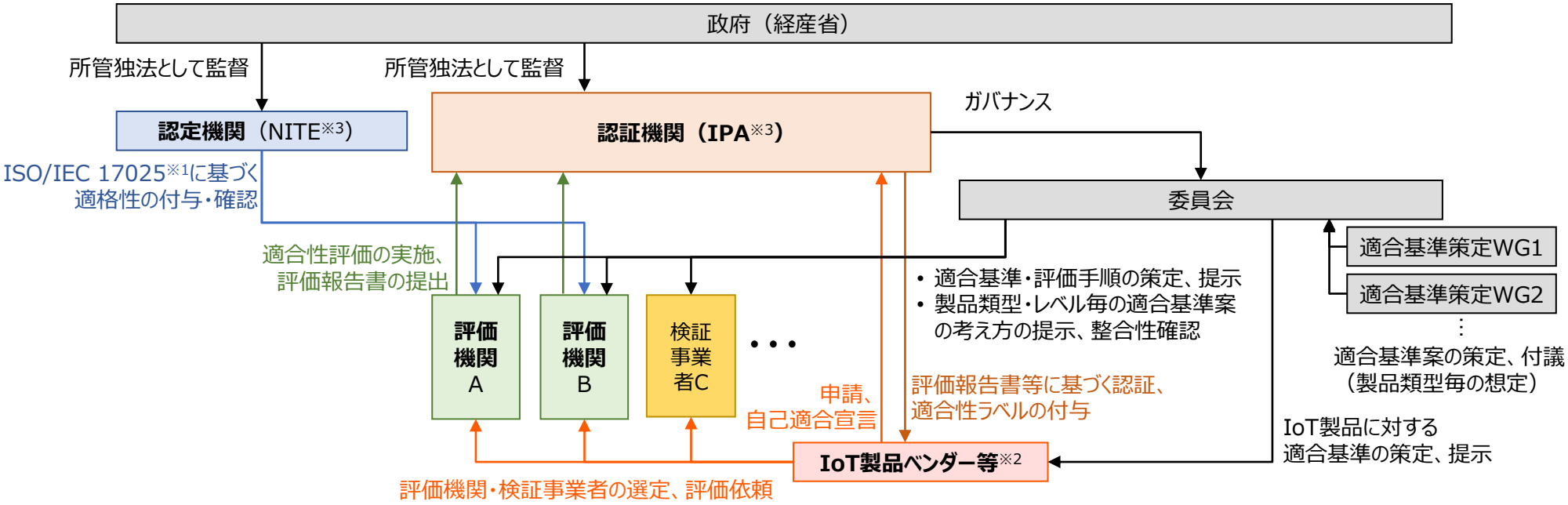
### 今後議論が必要な事項

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

# JISEC制度をベースとした適合性評価制度の全体像

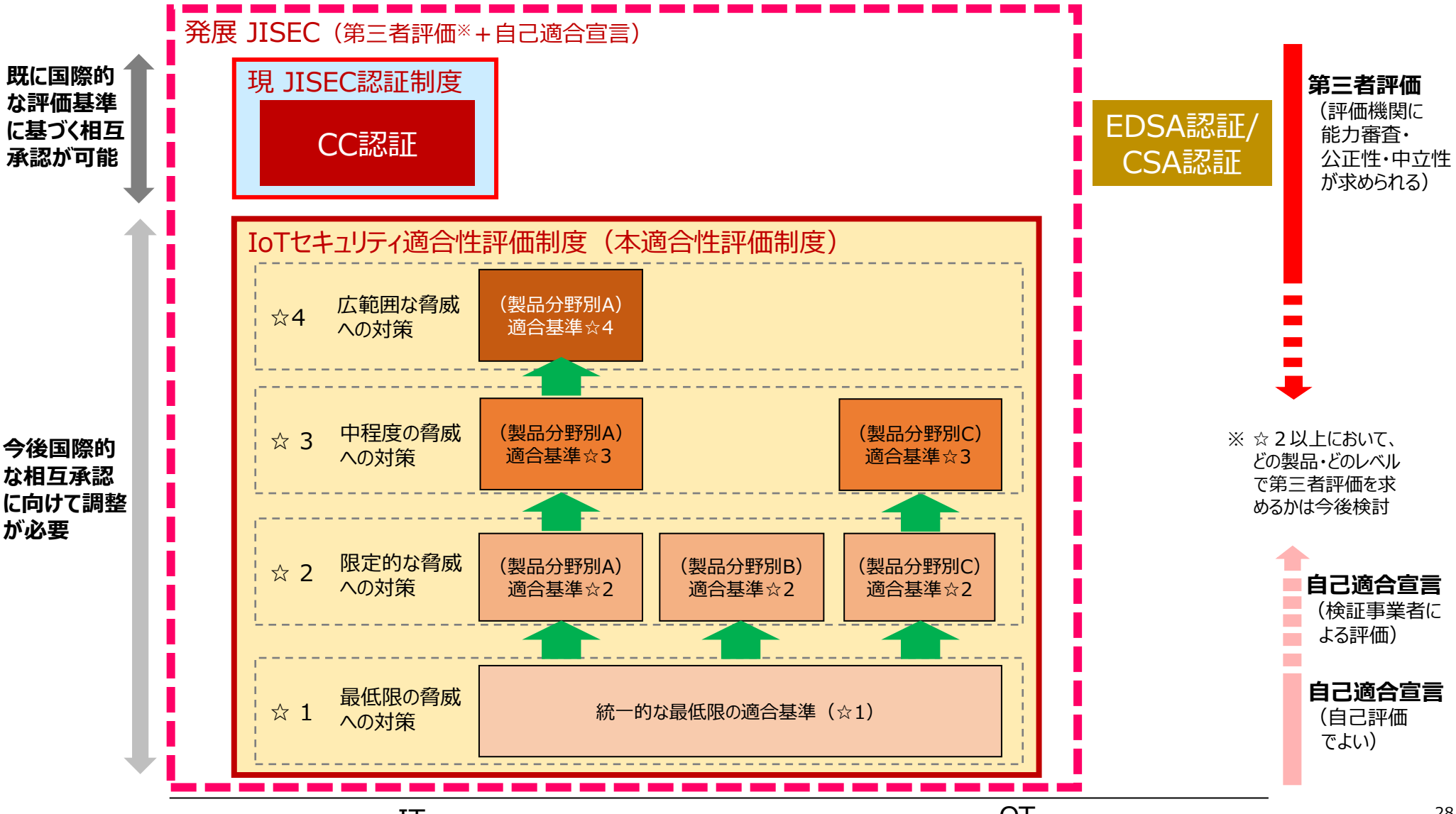
- これまでの議論を踏まえ、本制度の各主体の適格性について、政府のガバナンスが効く構造が重要。かかる観点から、**CC認証の知見があるIPAのJISEC認証制度**（ITセキュリティ評価及び認証制度）**を拡張する形の制度**を構築予定。
- **2023年度末までに要求基準・適合基準の検討**および**ルーター、スマート家電、ネットワークカメラ等を対象とした評価検証**を行う予定。




※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。
※3：組織名称は制度発足時に変更となる可能性がある。

# 既存制度との関係性と評価方法

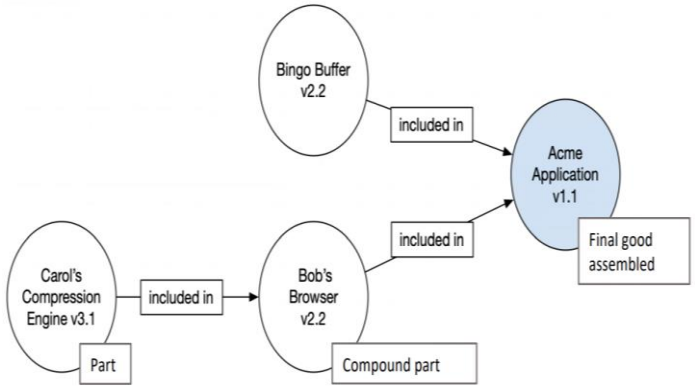
- CC認証のみを対象としている現行のJISEC認証制度を拡張し、本適合性評価制度を含む形の新たな枠組みを立ち上げる。
- 最低限の適合性評価レベル(☆1)では自己適合宣言を許容しつつ、リスクの高い分野の製品には第三者評価を求める。



# 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。

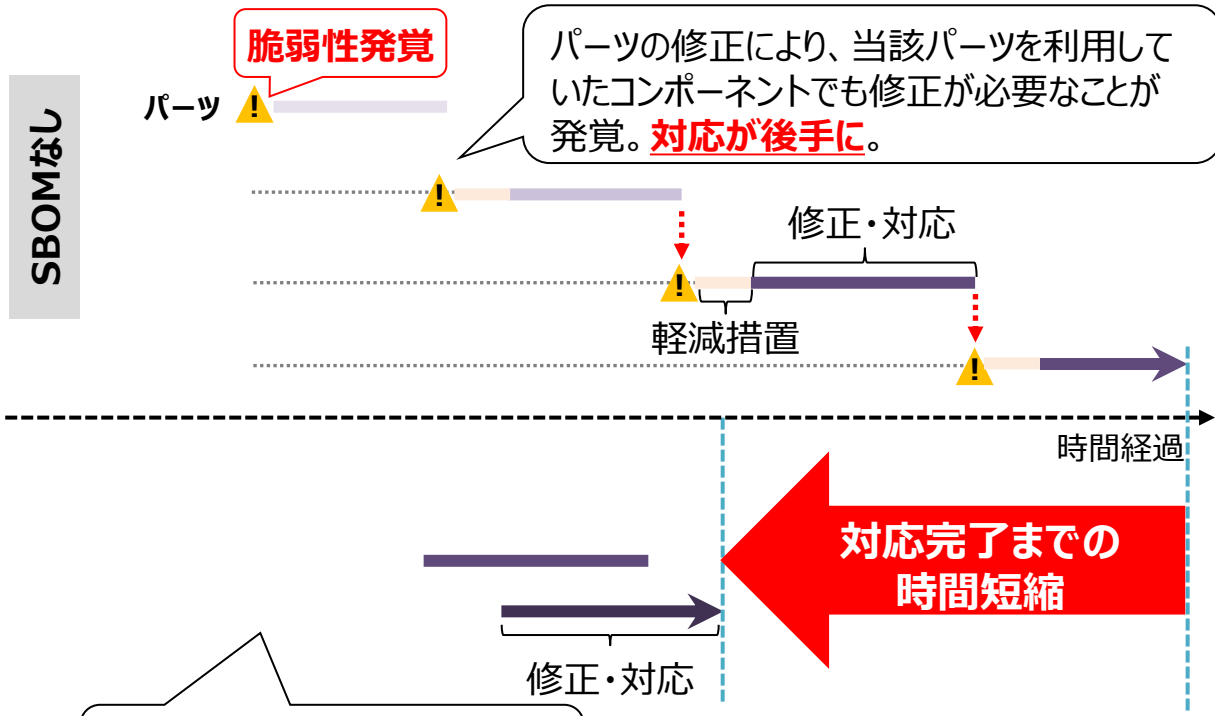
SBOMの構成イメージ




| 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**



# 2022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**。

経済産業省

事業委託先

- 実証の対象分野／組織の選定
- SBOMの効果に係る評価の観点、項目の整理
  - 調達時のリスク評価（脆弱性、ライセンス、サポート期間、ベンダー評価）
  - 運用時の脆弱性対応（脆弱性および影響の特定～対応の時間短縮、特定漏れの低減等）
  - 資産管理（システムや機器の更新判断、計画）
  - 供給者管理（契約書における責任分界点等の規定）
- SBOM活用モデルの選択肢の整理
- 参加者の知見共有の仕組み（定期的な会議開催等）の検討
- これまでの調査、検討結果や、国内外の動向等の共有

**自動車業界**
（OEM/部品サプライヤー等）

**医療機器業界**
（医療機器メーカー等）

SBOMに関する規制や推奨化が見込まれる分野

知見を共有

**ソフトウェア業界**
（ITベンダーとそのサプライチェーン等）

SBOMの効果が大きいと思われる分野

- 規制等において定められる**SBOMへの要求事項を満たしつつ、効率的にSBOMを作成、活用していくモデル**（作成者、作成／共有方法、最低限含むべき項目やフォーマット等）を検討。
- 米国NTIAにおける既存のPoCについて得られる情報を確認、活用。

- 社内システム及び顧客向け**システム／サービスを多く管理**し、**SBOMを多様なサプライヤーやユーザーと共有**し、**メリットを最大限享受できる活用モデル**の検討。
- 開発環境や構成管理ツール等との連携など、ツール環境に関する知見や課題の整理。

# ソフトウェア管理に向けたSBOMの導入に関する手引き

2023年7月28日、経済産業省は「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」を策定。

経済産業省
Ministry of Economy, Trade and Industry

申請・お問合せ | English | サイトマップ | 本文へ | 文字サイズ変更 小 中 大 | アクセシビリティ閲覧支援ツール

ニュースリリース | 会見・談話 | 審議会・研究会 | 統計 | 政策について | 経済産業省について

ホーム ▶ ニュースリリース ▶ ニュースリリースアーカイブ ▶ 2023年度7月一覧 ▶ 「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」を策定しました

印刷

「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」を策定しました

2023年7月28日

▶ 安全・安心

【2023年7月28日発表資料差し替え】「ソフトウェア管理に向けたSBOMの導入に関する手引きVer 1.0」に関して、ページ番号の記載がなかったため追記しました。

経済産業省は、ソフトウェアサプライチェーンが複雑化する中で、急激に脅威が増しているソフトウェアのセキュリティを確保するための管理手法の一つとして「SBOM」（ソフトウェア部品表）に着目し、企業による利活用を推進するための検討を進めてきました。今般、主にソフトウェアサプライヤー向けに、SBOMを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手引書を策定しましたのでお知らせします。

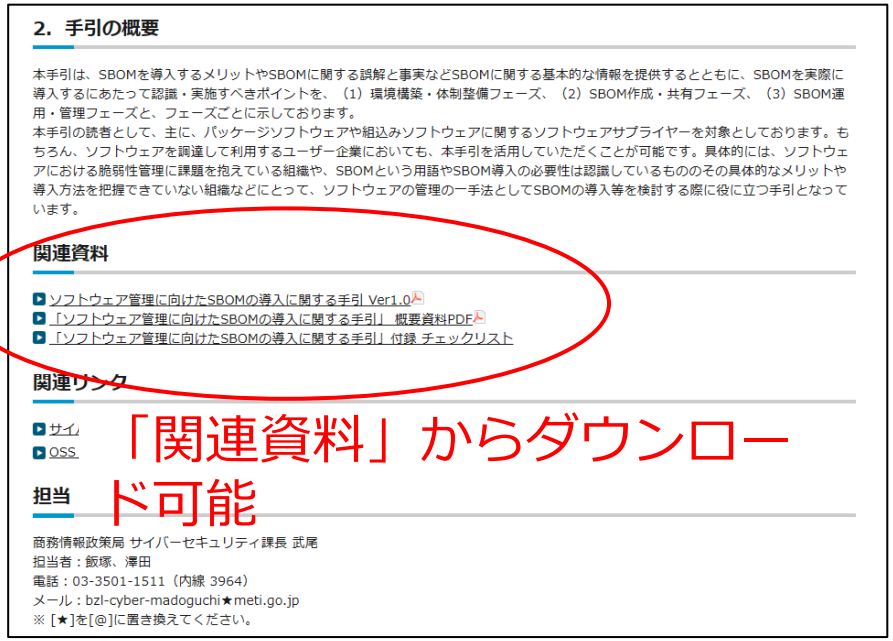
本手引の普及により企業におけるSBOMの導入が進むことで、ソフトウェアの脆弱性への対応に係る初動期間の短縮や管理コストの低減など、ソフトウェアの適切な管理が可能となり、企業における開発生産性が向上するだけでなく、産業界におけるサイバーセキュリティ能力の向上に繋がることが期待されます。

1. 背景・趣旨

近年、産業活動のサービス化に伴い、産業に占めるソフトウェアの重要性は高まっています。具体的には、産業機械や自動車等の制御にもソフトウェアの導入が進んでおり、また、IoT機器・サービスや5G技術においても、汎用的な機器でハードウェア・システムを構築した上で、ソフトウェアにより多様な機能を持たせることで、様々な付加価値を創出していくことが期待されているなど、企業においてOSSを含むソフトウェアの利用が広がっております。

このようにサイバー空間とフィジカル空間の融合が進む一方で、ソフトウェアの脆弱性が企業経営に大きな影響を及ぼすなど、ソフトウェアに対するセキュリティ脅威が増大しています。このため、自社のセキュリティを強化するためにソフトウェアを適切に管理していくことが重要になりますが、ソフトウェアサプライチェーンが複雑化し、OSSの利用が一般化する中で、自社製品において利用するソフトウェアであっても、コンポーネントとしてどのようなソフトウェアが含まれているのかを把握することが困難な状況という課題があります。

このようなソフトウェアの脆弱性管理に関し、ソフトウェアの開発組織と利用組織双方の課題を解決する一手法として、「ソフトウェア部品表」とも呼ばれるSBOM（Software Bill of Materials）を用いた管理手法が注目されています。米国では大統領令に基づき、連邦政府機関におけるSBOMを含めたソフトウェアサプライチェーンセキュリティ対策の強化に向けた動きが進展しています。QUAD（日米豪印戦略対話）では、政府調達ソフトウェアのセキュリティ確保に向け、ソフトウェアの安全な開発・調達・運用に関する方針を示した共同原則が



2. 手引の概要

本手引は、SBOMを導入するメリットやSBOMに関する誤解と事実などSBOMに関する基本的な情報を提供するとともに、SBOMを実際に導入するにあたって認識・実施すべきポイントを、（1）環境構築・体制整備フェーズ、（2）SBOM作成・共有フェーズ、（3）SBOM運用・管理フェーズと、フェーズごとに示しております。

本手引の読者として、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を対象としております。もちろん、ソフトウェアを調達して利用するユーザー企業においても、本手引を活用していただくことが可能です。具体的には、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や、SBOMという用語やSBOM導入の必要性は認識しているもののその具体的なメリットや導入方法を把握できていない組織などにとって、ソフトウェアの管理の一手法としてSBOMの導入等を検討する際に役に立つ手引となっています。

関連資料

- ソフトウェア管理に向けたSBOMの導入に関する手引 Ver1.0
- 「ソフトウェア管理に向けたSBOMの導入に関する手引」 概要資料PDF
- 「ソフトウェア管理に向けたSBOMの導入に関する手引」 付録 チェックリスト

関連リンク

- サイ
- OSS

「関連資料」からダウンロード可能

担当

商務情報政策局 サイバーセキュリティ課長 武尾
担当者：飯塚、澤田
電話：03-3501-1511（内線 3964）
メール：bzl-cyber-madoguchi★meti.go.jp
※ [★]を[@]に置き換えてください。

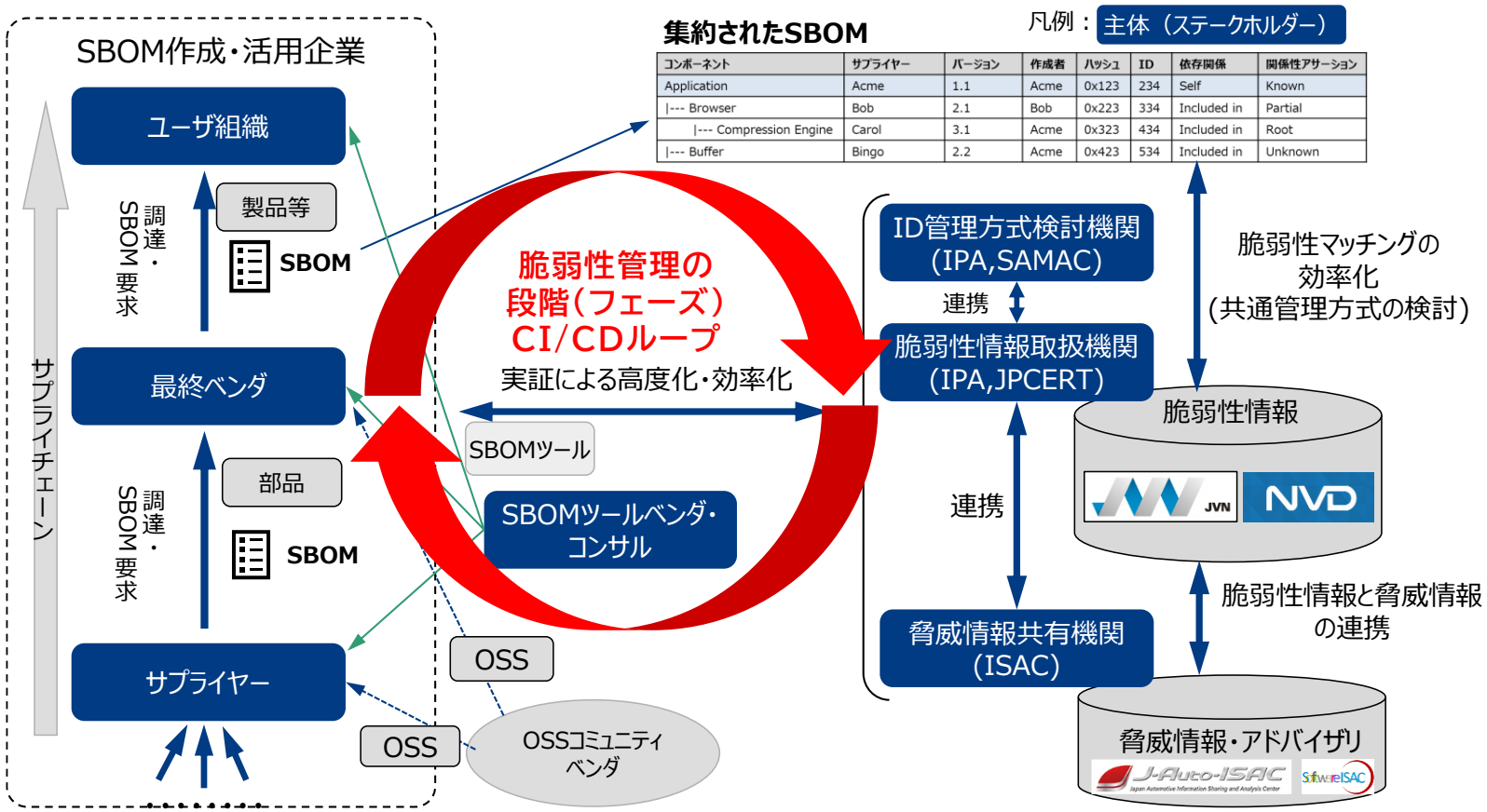
「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」
（2023年7月、経済産業省）：
https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

# 2023年度SBOM実証の全体像： SBOMを活用した脆弱性管理の効率化

実証の目的（ポイント）

- 脆弱性管理プロセスを俯瞰し、SBOMを活用した脆弱性管理の効率的な方法について検討し、その効果評価、課題の整理を行う。**脆弱性情報の提供に係る機関（IPA, ISAC等）と連携**し、脆弱性情報を効率的に取得する方法を検討する。
- SBOMを活用した脆弱性管理を広く普及させるため、**中小企業を含む多くの企業が活用**できるように、脆弱性の深刻度、脅威、アドバイザリなども活用するための方策等について整理する。

## 脆弱性管理の主なステークホルダとプロセスの全体像




| コンポーネント | サプライヤー | バージョン | 作成者 | ハッシュ | ID | 依存関係 | 関係性アサーション |
|---|---|---|---|---|---|---|---|
| Application | Acme | 1.1 | Acme | 0x123 | 234 | Self | Known |
| \|--- Browser | Bob | 2.1 | Bob | 0x223 | 334 | Included in | Partial |
| \|--- Compression Engine | Carol | 3.1 | Acme | 0x323 | 434 | Included in | Root |
| \|--- Buffer | Bingo | 2.2 | Acme | 0x423 | 534 | Included in | Unknown |

# G7群馬高崎デジタル・技術大臣会合の概要

- **4月29日(土)、30日(日)、G7群馬高崎デジタル・技術大臣会合を開催。**
- 我が国からは、**河野デジタル大臣、松本総務大臣、西村経済産業大臣**が共同議長として参加。
  また、G7各国（仏、米、英、独、伊、加）＋EU、招待国（印、インドネシア、ウクライナ）、国際機関（OECD、ITU、世銀、国連、ERIA）が参加。

## 主な成果

以下6つのテーマについて議論が行われ、成果として、**「G7デジタル・技術閣僚宣言」**を採択。

(1) 越境データ流通と信頼性のある自由なデータ流通(DFFT)の推進
(2) 安全で強靭性のあるデジタルインフラ
(3) 自由でオープンなインターネットの維持・推進
(4) 経済社会のイノベーションと新興技術の推進
(5) 責任あるAIとAIガバナンスの推進
(6) デジタル競争


## ポイント

- 社会インフラ整備にあたって必要な**基幹技術間での相互運用性の確保**に向けて協力。
- **ソフトウェアの脆弱性対策**やIoT等の**技術セキュリティ確保に向けた標準策定協力の加速化。**

会合HP：https://g7digital-tech-2023.go.jp/

# 日米豪印（Quad（クアッド））第５回首脳会合について

- **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）
- 岸田総理大臣からは、ASEANや南アジア、太平洋島嶼国といった地域の国々の声に耳を傾けながら、**「善を推進する力」として、地域に真に裨益する実践的協力を展開していく重要性**を強調。
- また会合後、**４カ国は共同声明を発出**。当省関連では、**重要・新興技術、気候、サイバーセキュリティ、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。その他、海洋安全保障、海洋状況把握、国際保健等での新たな協力が記載された。
- **来年の首脳会合は、インドで開催**することで一致した。

## サイバーセキュリティ

- 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。

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

# 1．サイバーセキュリティ戦略

# 2．経済産業省の政策

## 2.1．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）
～サイバーセキュリティ経営ガイドライン
～サイバーセキュリティお助け隊サービス
～高度セキュリティ人材の育成
～日米欧によるインド太平洋地域の能力構築支援

## 2.2．国際連携を意識した認証・評価制度の立ち上げ

～IoT適合性評価制度
～SBOM（Software Bill Of Materials）
～QUAD上級サイバー会合、G7等を通じた連携

## 2.3．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対処能力向上
～重要インフラ事業者等での事案発生時の初動対応体制強化
～事故調査体制の構築
～サイバー攻撃被害情報の共有促進

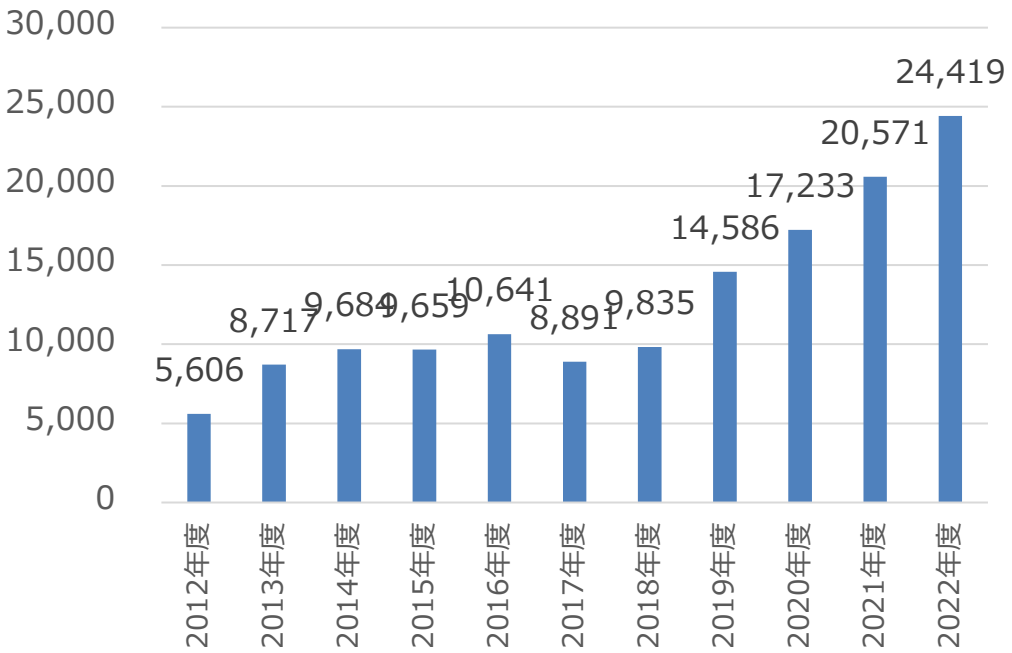
## 2.4．新たな攻撃を防ぎ、守るための研究開発の促進

～セキュリティ産業の成長加速化

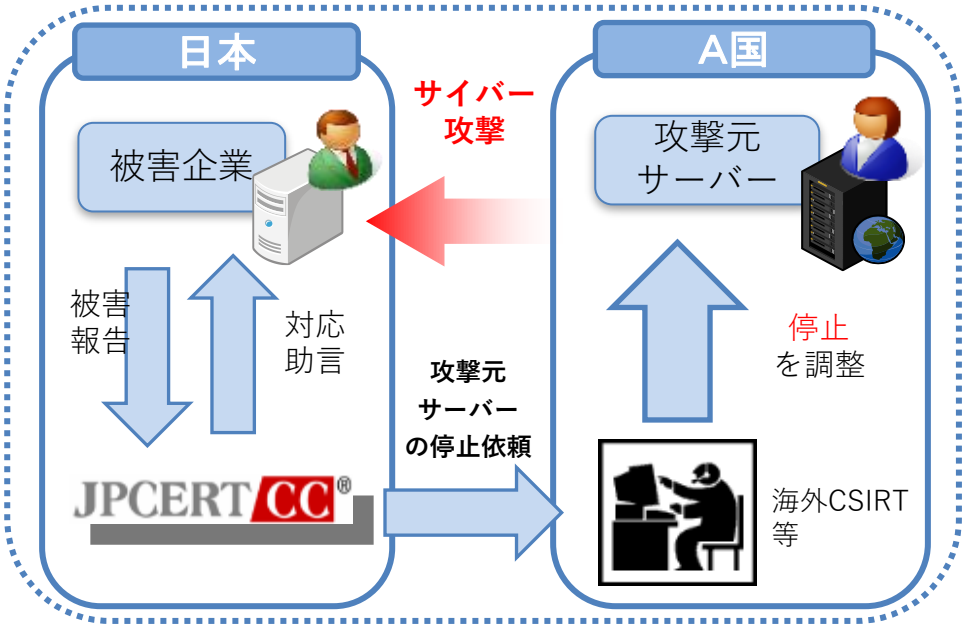
# 国際連携によるサイバー攻撃元への対応（JPCERT/CC）

- 一般社団法人JPCERT/CC（ジェイピーサートコーディネーションセンター）は、国境を越えて行われるサイバー攻撃に対処するため、サイバー攻撃連絡調整窓口の間で情報共有を行うとともに、共同対処等を実施。

## サイバー攻撃事案の調整件数（年度集計）

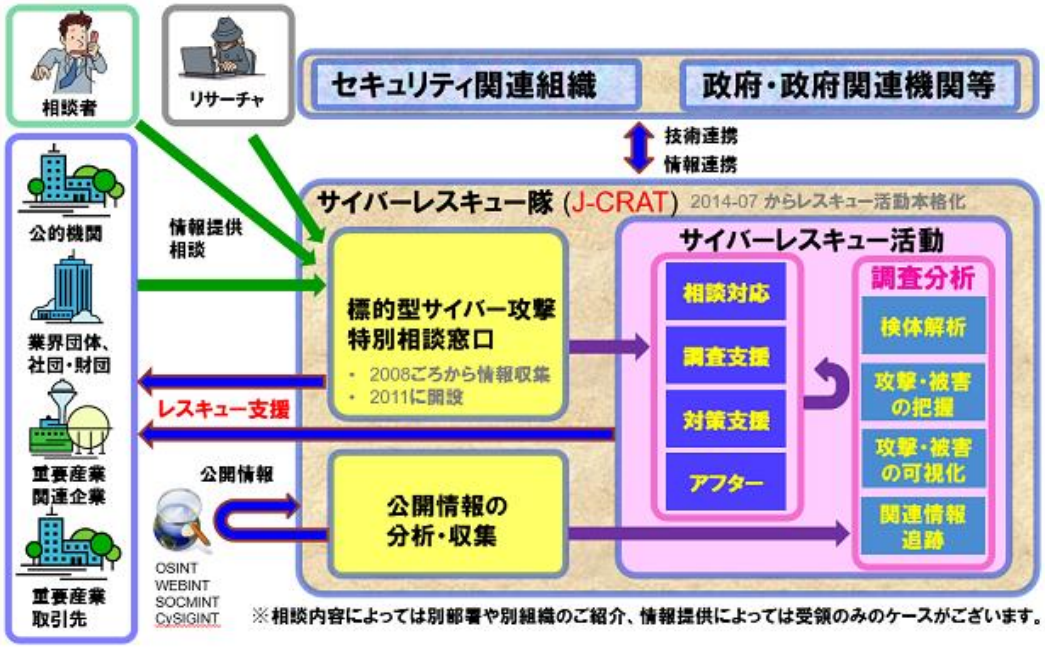



## 国際連携によるサーバの停止等の対応



# サイバーレスキュー隊＜J-CRAT＞

- 2014年７月発足。J-CRATは、「標的型サイバー攻撃特別相談窓口」にて、広く一般から相談や情報提供を受付け、提供された情報を分析して調査結果による助言を実施。
- その中で、**標的型サイバー攻撃の被害の発生が予見**され、その**対策の対応遅延が社会や産業に重大な影響を及ぼすと判断される組織**や、**標的型サイバー攻撃の連鎖の元となっていると推測される組織**などに対しては、レスキュー活動にエスカレーションして支援。



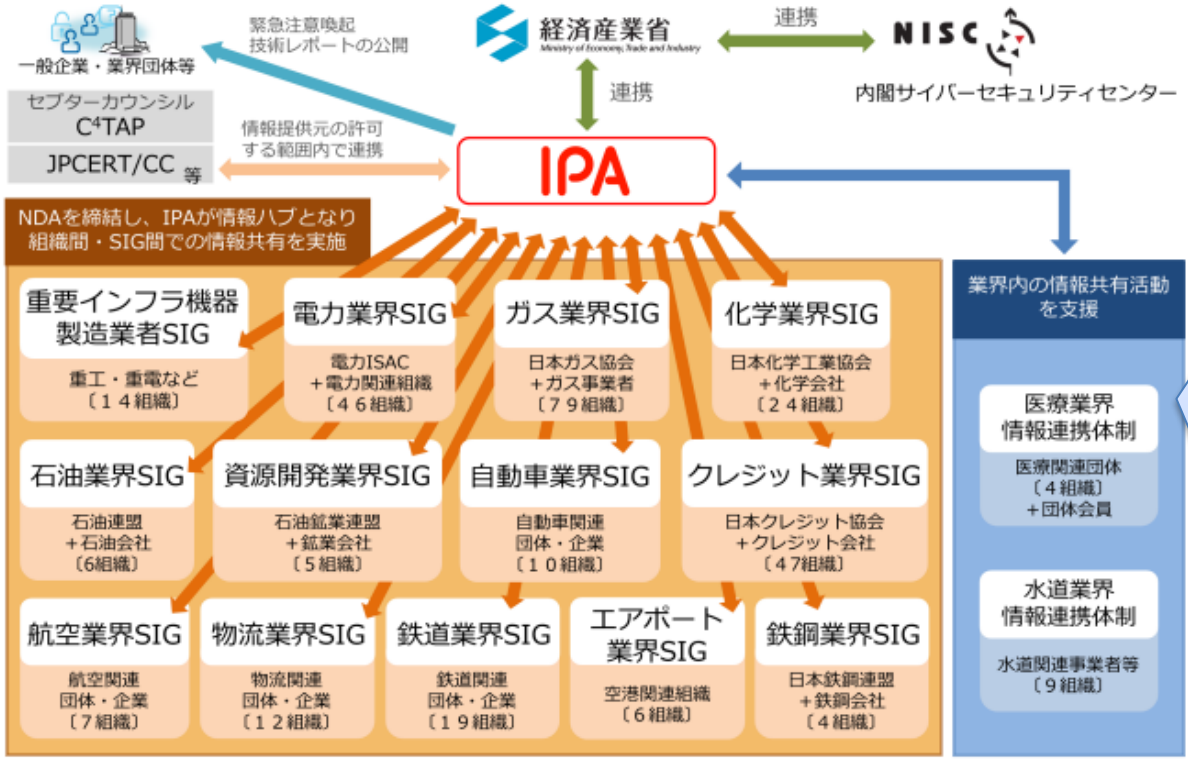

出典：IPA「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）について」
https://www.ipa.go.jp/security/j-crat/about.html

| | 2014年度 | 2015年度 | 2016年度 | 2017年度 | 2018年度 | 2019年度 | 2020年度 | 2021年度 | 2022年度 |
|---|---|---|---|---|---|---|---|---|---|
| 相談件数 | 107 | 537 | 519 | 412 | 413 | 392 | 406 | 375 | 330 |
| レスキュー支援数 | 38 | 160 | 123 | 144 | 127 | 139 | 102 | 94 | 163 |
| オンサイト | 11 | 39 | 17 | 27 | 31 | 20 | 17 | 9 | 43 |

# サイバー情報共有イニシアティブ（J-CSIP）

- 2011年10月発足。IPAは公的機関として、NDA※の締結等により、メンバー企業間の信頼できる**情報ハブ（集約点）**の役割を担う。

※ NDA: Non-Disclosure Agreement、秘密保持契約




**SIG**: Special Interest Group の略。各組織や業界団体とNDAを締結し情報共有を行う、業界ごとの情報共有グループ。

**情報連携体制**: NDA締結が難しい業界からの要望に基づき、書面の参加申込書により秘密保持等を担保しつつ、情報共有を実現する形態。

## 2012年度～2022年度の情報共有の実績

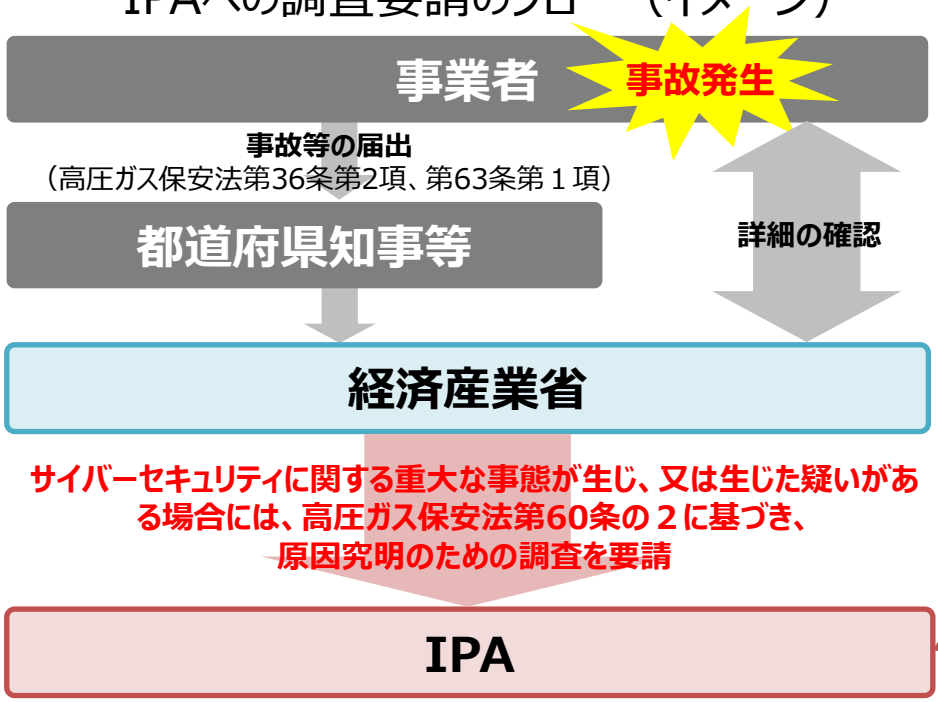
出典:IPA「サイバー情報共有イニシアティブ（J-CSIP） 運用状況 」
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy22-q4-report.pdf

| 項目 | 2012年度 | 2013年度 | 2014年度 | 2015年度 | 2016年度 | 2017年度 | 2018年度 | 2019年度 | 2020年度 | 2021年度 | 2022年度 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| IPAへの情報提供件数 | 246件 | 385件 | 626件 | 1,092件 | 2,505件 | 3,456件 | 2,020件 | 2,303件 | 6,202件 | 843件 | 241件 |
| 参加組織への情報共有実施件数 | 160件 | 180件 | 195件 | 133件 | 96件 | 242件 | 195件 | 225件 | 147件 | 118件 | 120件 |

# サイバーインシデントに係る事故調査

- 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**。
- 昨年交付された改正保安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（以下「IPA」という。）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。

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。

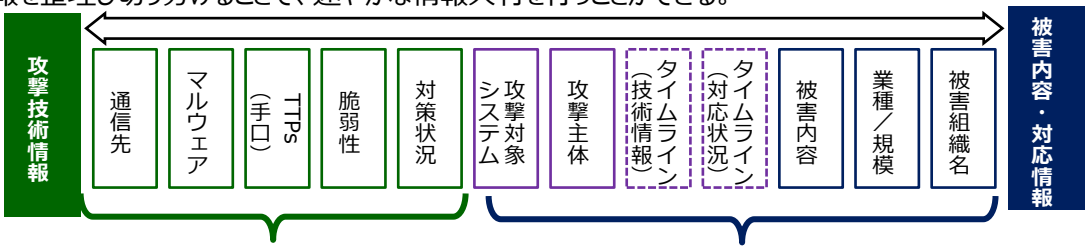
改正高圧ガス保安法
第六十条の二　経済産業大臣は（中略）**保安に係るサイバーセキュリティ（中略）に関する重大な事態が生じ、又は生じた疑いがある場合**において、必要があると認めるときは、**独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる**。

# 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）

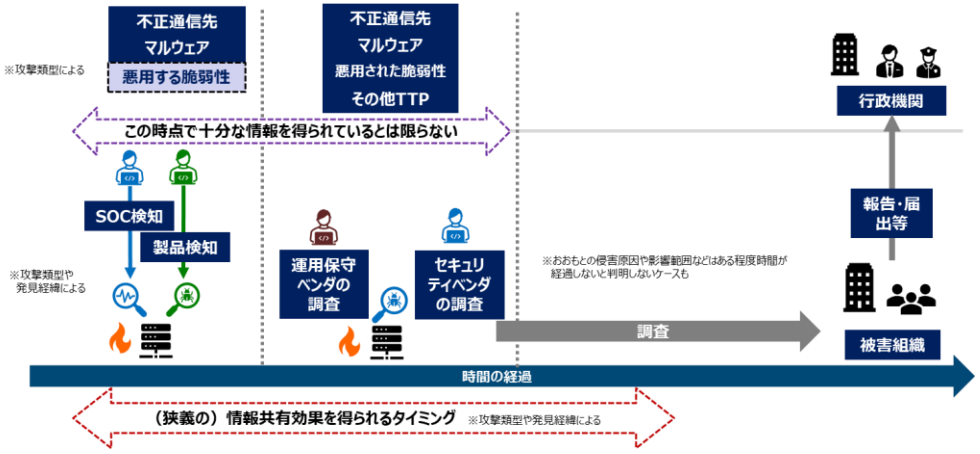

## 想定読者（被害組織等）

# サイバー攻撃による被害に関する情報共有の促進に向けた検討会

- サイバー攻撃が高度化・複雑化する中、官民が連携して、サイバー攻撃により早期に対処することで、被害拡大を防止することが必要。
- サイバー攻撃の被害組織が専門組織と連携して、効率的・効果的な攻撃技術情報を共有することで、より早期に対処を行うこと可能になることが期待。
- サイバー攻撃による被害に関する情報の種類と性質について整理を行うとともに、被害組織と専門組織の間で結ぶ秘密保持契約のあり方をはじめ、情報共有活動における制度的課題や仕組みについて検討中。

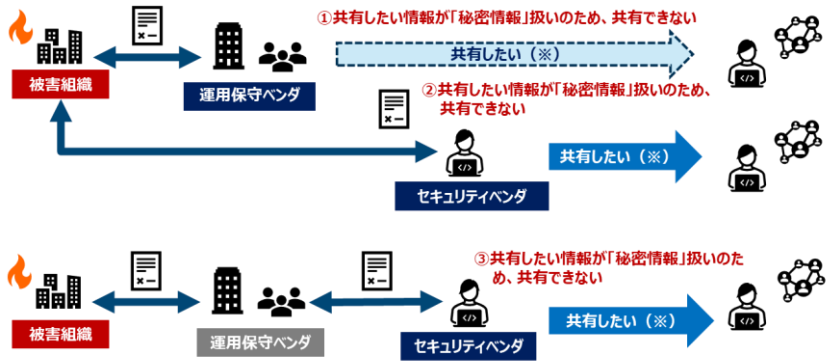
## サイバー被害の状況把握

- 被害企業のシステム監視をしている運用保守ベンダや、そこで使用されている製品の開発者が不正通信先やマルウェア等を検知
- ユーザー企業側がシステムの異変に気づいた後、運用保守ベンダやセキュリティベンダがシステム分離等の初動対応に当たった段階での調査で、悪用された脆弱性等が把握　etc・・・
- 被害企業において、原因究明・再発防止に十分な情報を得られているとは限らない。




## NDAが情報共有の制約になると考えられるケース

- 被害組織と運用保守ベンダとの契約で、運用保守ベンダが情報共有できないケース
- 被害組織とセキュリティベンダとの契約で、セキュリティベンダが情報共有できないケース
- 運用保守ベンダとセキュリティベンダとの契約で、セキュリティベンダが情報共有できないケース　etc・・・




（※）情報の種類や性質、企業の業態等にもよるが、共有したいと考えるベンダは一定数存在。

# 1．サイバーセキュリティ戦略

# 2．経済産業省の政策

## 2.1．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）
～サイバーセキュリティ経営ガイドライン
～サイバーセキュリティお助け隊サービス
～高度セキュリティ人材の育成
～日米欧によるインド太平洋地域の能力構築支援

## 2.2．国際連携を意識した認証・評価制度の立ち上げ

～IoT適合性評価制度
～SBOM（Software Bill Of Materials）
～QUAD上級サイバー会合、G7等を通じた連携

## 2.3．政府全体でのサイバーセキュリティ対応体制の強化

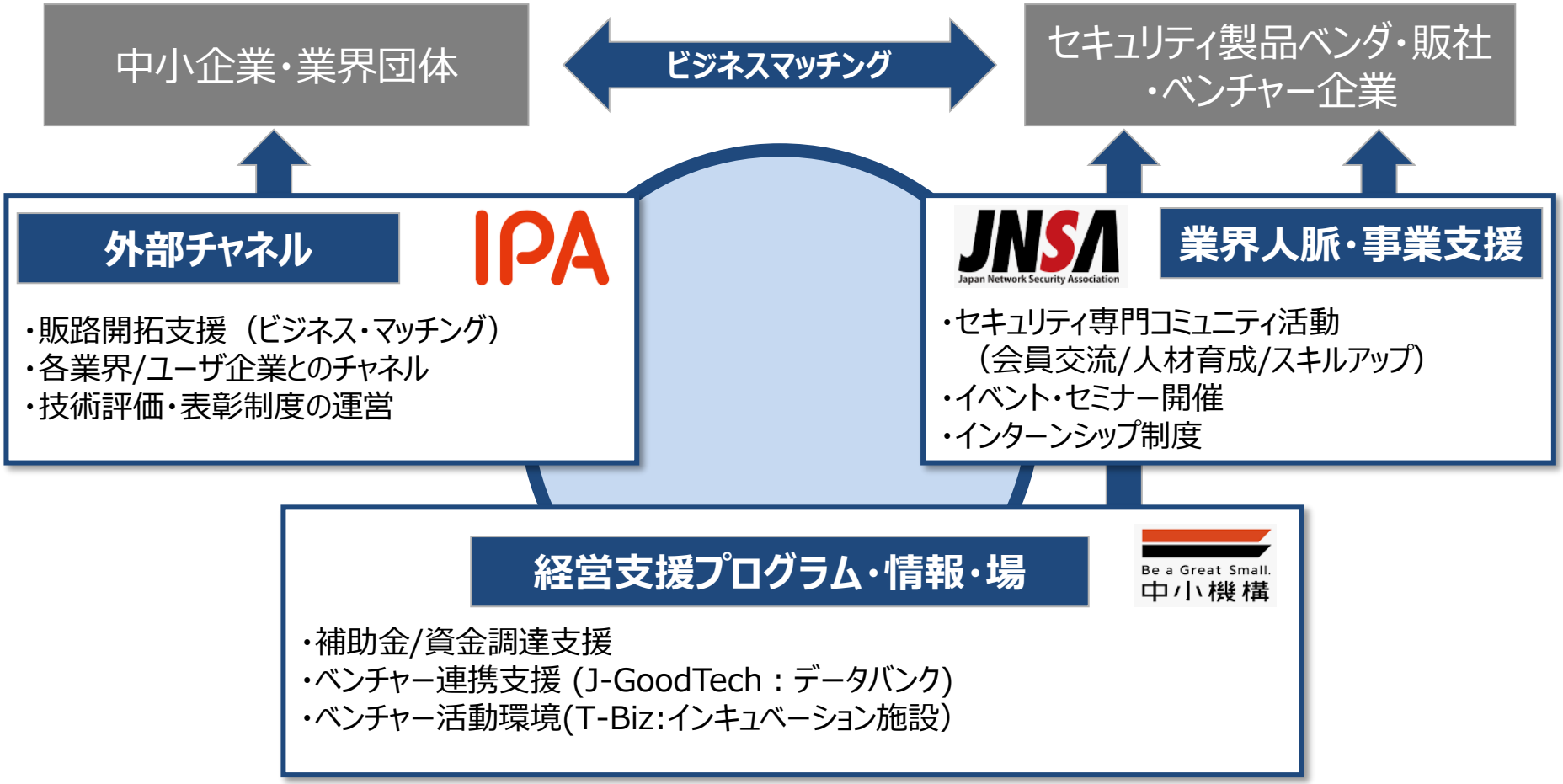
～国境を越えて行われるサイバー攻撃への対処能力向上
～重要インフラ事業者等での事案発生時の初動対応体制強化
～事故調査体制の構築
～サイバー攻撃被害情報の共有促進

## 2.4．新たな攻撃を防ぎ、守るための研究開発の促進

～セキュリティ産業の成長加速化

# 実現すべきエコシステム（イメージ）

- 関連機関のアセットや既存プログラムを活用し、セキュリティ企業がステージに応じて必要とする支援を、経営/技術/事業の３面から実施する。
- また、IPAによる顧客接点・業界チャネルを活用し、販路開拓・事業化支援を実施する。



# IoT機器等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作成・普及

- このような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**」を策定し、公開（2023年6月）。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。
- 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）

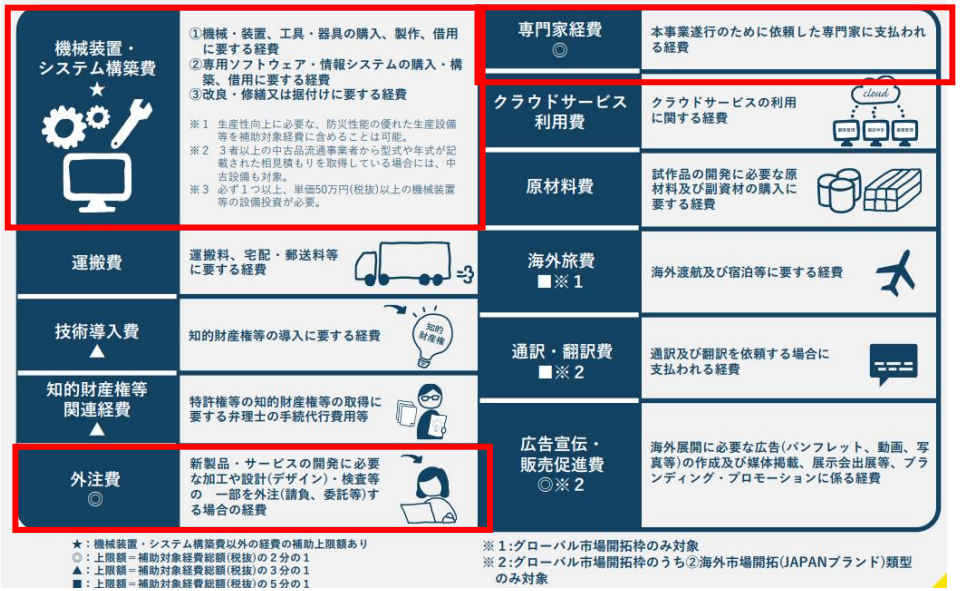
# 中小企業に対するセキュリティ・バイ・デザインの補助

- 前述のとおり、中小企業によるセキュアな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行っていくことが重要**。
- 「ものづくり補助金」では、中小企業が開発するIoT機器に関連して、
  - ✓ **設計時にセキュリティ設計が得意な専門家のアドバイスを受けることに係る経費**
  - ✓ **生産性向上やセキュリティ向上に資する機械・ソフトウェア等の設備投資**
  - ✓ **ペネトレーションテスト等の検証費用**

  等に対する補助を行うことが可能。
- このように、**IoT機器の開発から出荷に至る一連のプロセスでサポートを行う**ことで、**中小企業がセキュアなIoT機器を数多く出荷していくことを後押し**していく。

- 予算額：2,000億円（R4年度2次補正）
- 補助下限額：100万円、補助上限額：750万円～5,000万円※
  補助率：1/2~2/3※

※従業員数や公募枠により補助上限・補助率が変動
※例年の採択件数は、1公募あたり、2,000～3,000件程度
※補助を受けるには50万円以上の設備投資が必要




**設計・開発**

設計・開発段階で、どのようなセキュリティ機能を搭載すべきかについて、セキュリティの専門家のアドバイスを受けたい。

**生産**

IoT製品の機能性を上げるために生産設備を導入したい。また、生産段階でセキュリティ上不正な機能が混入しないようセンサを導入したい。

**検証**

製品に脆弱性がないかを確認するために、ペネトレーションテストや脆弱性診断を行いたい。

**もの補助で補助が可能**

**セキュアなIoT機器の出荷**

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