経済産業省

資料３

# IoT機器への対策を含む
# サプライチェーンサイバーセキュリティの強化

平成30年6月

経済産業省　商務情報政策局

サイバーセキュリティ課

## １．IoTの進展等によるSociety5.0の実現に伴うサイバー攻撃の脅威レベルの向上と海外の動向

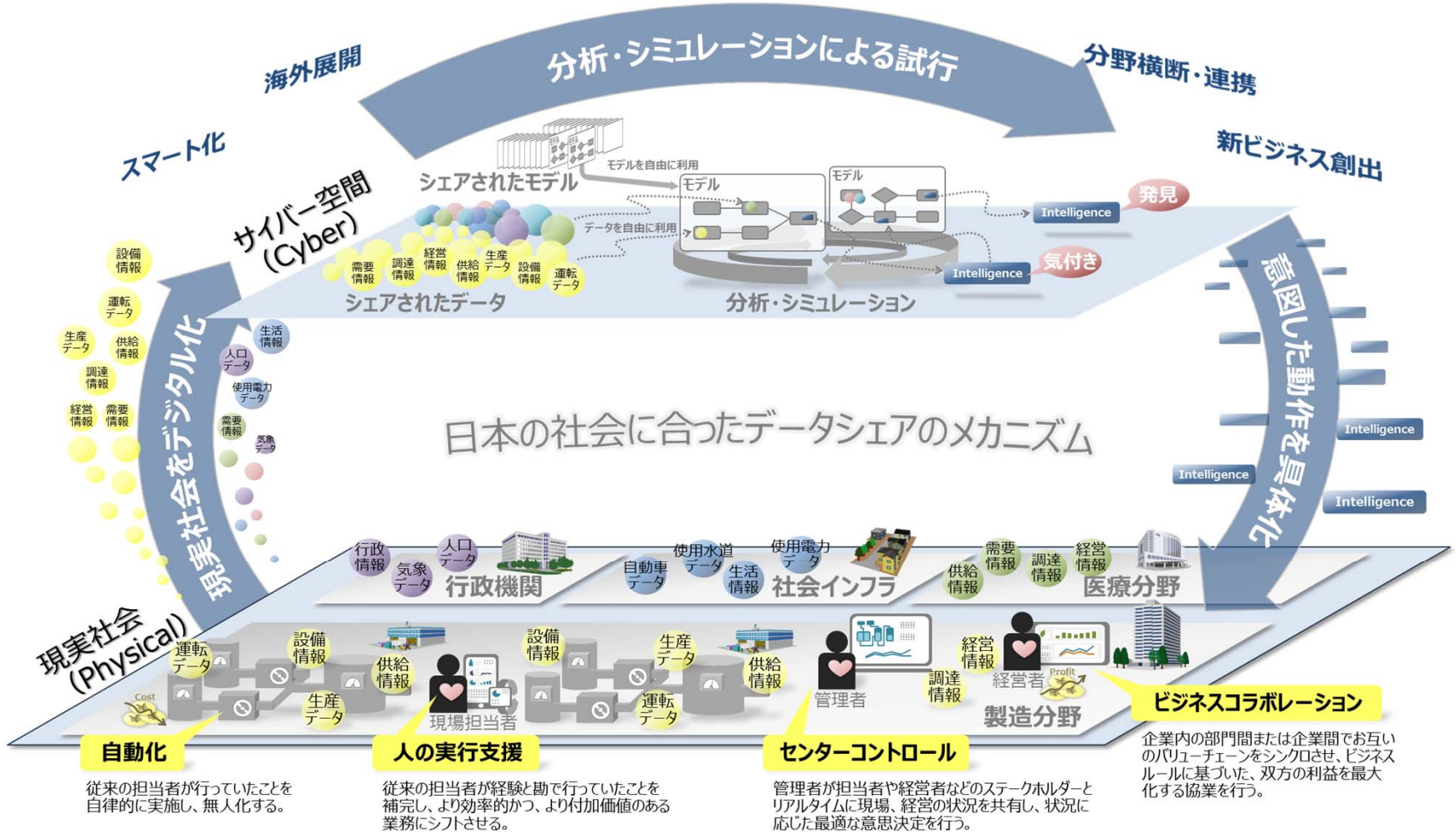
## ２．サプライチェーンサイバーセキュリティ強化へ向けた検討体制の構築

## ３．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策定

## ４．フレームワークを活用したサプライチェーンサイバーセキュリティ強化
## ～産業分野別のガイドライン策定と必要な技術開発の促進

# Society5.0、Connected Industries が実現する社会

- Society5.0は、**サイバー空間とフィジカル空間を高度に融合**させることにより、**多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立**する社会。
- Society5.0へ向けて、様々なつながりによる新たな付加価値を創出する**Connected Industriesの実現に向けた新たな産業構造の構築が必要**。




出典：経済産業省「平成27年度我が国経済社会の情報化・サービス化に係る基盤整備(水道事業におけるCPS(サイバーフィジカルシステム)実装のための調査研究)」報告書を基に作成

# サイバー攻撃の脅威の増大

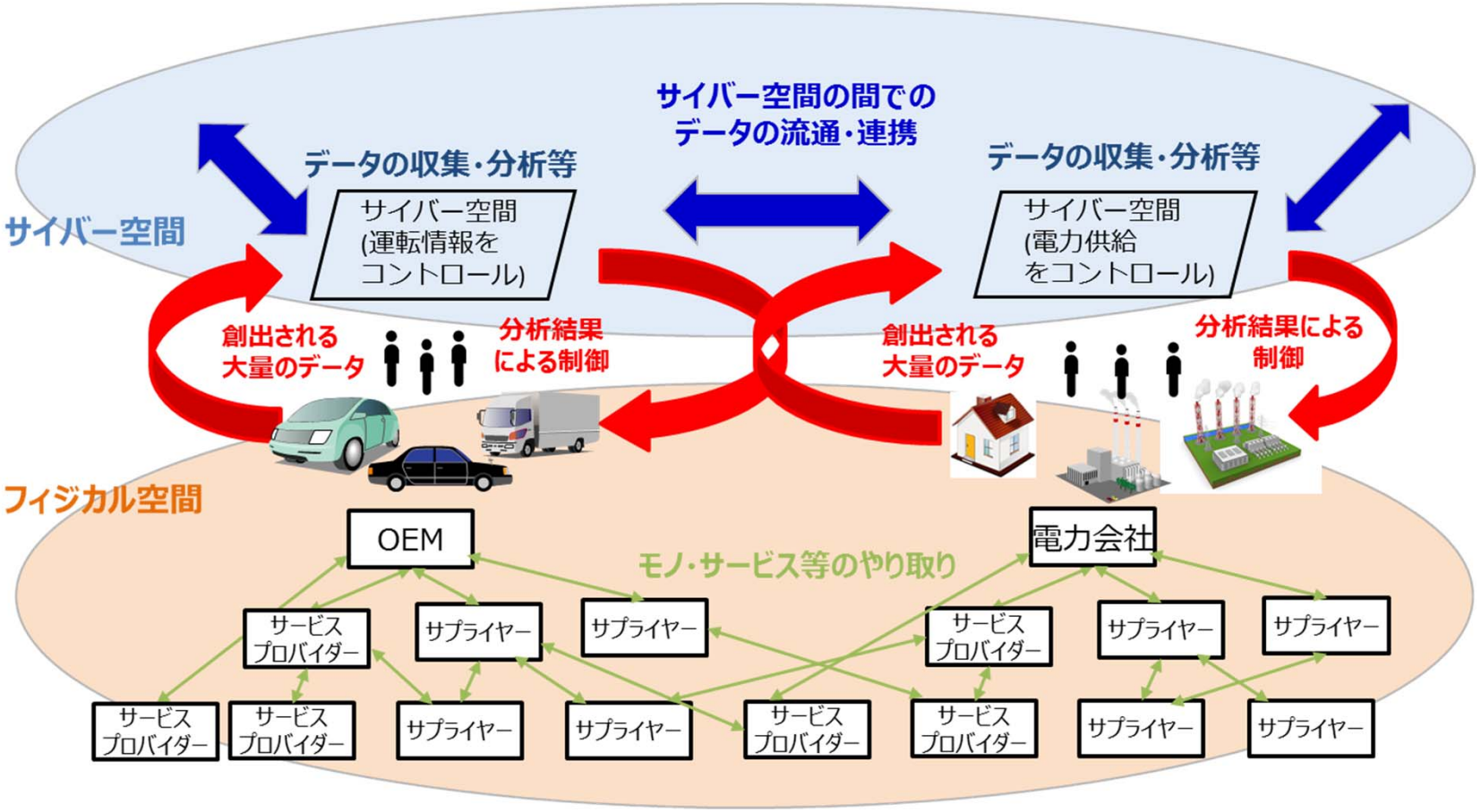
- IoTとAIによって実現されるSociety5.0の社会(人間中心の社会)では、**サイバー攻撃の起点が増大するとともに、複雑につながるサプライチェーンを通じてサイバーリスクの範囲が拡大**。
- サイバー空間とフィジカル空間が高度に融合するため、**サイバー攻撃がフィジカル空間まで到達**。
- IoTから得られる**大量のデータの流通・連携を支えるセキュリティも課題**。
- **海外においても、IoTやICS防衛のためにはサプライチェーンマネジメントでアプローチする必要が広く認識**されるようになっている。

**大量のデータの流通・連携 ⇒データ管理の重要性が増大**

**フィジカルとサイバーの融合 ⇒フィジカル空間までサイバー攻撃が到達**

**複雑につながるサプライチェーン ⇒影響範囲が拡大**

## 「Society5.0」社会におけるモノ・データ等のつながりのイメージ



# 米国における最近の動き①：
# サイバーセキュリティフレームワークの改訂

- **2度の意見募集を踏まえた修正を行った上で、2018年4月、NIST（米国国立標準技術研究所）が「Cybersecurity Framework Version1.1」を決定。**
- **国際標準化に向けた活動も開始している状況。**

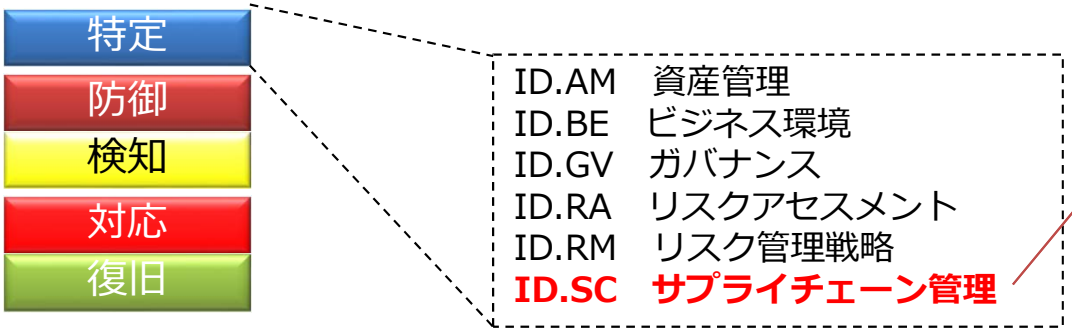
## NIST「Cybersecurity Framework」の経緯

- 2014年2月、サイバーセキュリティ対策の全体像を示し、「特定」、「防御」、「検知」、「対応」、「復旧」に分類して対策を記載した「Cybersecurity Framework Vesion1.0」を策定。
- 2017年1月、「Cybersecurity Framework Version1.1 draft1」を公表。
- 2017年12月、「Cybersecurity Framework Version1.1 draft2」を公表。
- 2018年4月、「Cybersecurity Framework Version1.1」を決定。

## NIST「Cybersecurity Framework Version1.1」の特徴

- Version1.1は、Version1.0より特に以下の点が追記され、その重要性が説かれている。
  - サプライチェーンのリスク管理（Supply Chain Risk Management）
  - サイバーセキュリティリスクの自己評価（Self-Assessing Cybersecurity Risk）

**Cybersecurity Frameworkにおける5つの分類**




Version1.1でID.SCが新規に追加され、**サプライチェーン全体で対策を実施する**ことや、必要に応じて監査を行うことを要求

# 米国における最近の動き②：
# 2017年5月大統領令に基づく各種報告書の公表

- **2017年5月、トランプ大統領が「サイバーセキュリティ強化のための大統領令」に署名。関係省庁に対して複数の報告書の策定を命令。**
- **2018年５月29-31日、関係省庁は国内での議論を喚起するため、可能な範囲で各種報告書を公表。**

**1．連邦政府のサイバーセキュリティリスクに関する報告書 (5/29 DHS・行政管理予算局):**
- 96の政府機関のサイバーセキュリティ管理能力のアセスメント結果と改善策を報告。

**2．ボットネット対策等に関する報告書 (5/30 DHS・商務省):**
- ボットネット対策等のために官民が取るべき対策を報告。120日以内にロードマップを策定予定。

**3．電力網への攻撃に対するインシデント・レスポンスに関する報告書 (5/31 エネルギー省):**
- 電力事業者がインシデントに対応するための７つの能力ギャップと提言について報告。

**4．人材育成に関する報告書 (5/31 DHS・商務省):**
- 299,000人分のオンライン上のセキュリティ関連空きポストに対応するための取組について報告。

**5．米国のサイバー利益保護のための国際活動に関する報告書（5/31 国務省）:**
- 開放的で相互運用可能で安全で信頼の高いサイバー空間のために必要な外交活動等について報告。

**6．敵対勢力に対する抑止等に関する報告書 (5/31 国務省):**
- 武力等により抑止を行うべき悪意あるサイバー活動の基準・閾値等について報告。

**7．重要インフラ防御に関する報告書 (5/31 DHS):**
- 各政府機関が各重要インフラ事業者に対して有する権限や能力について特定し、改善策を報告。

**8．市場の透明性に関する報告書 (5/31 DHS):**
- 事業者のセキュリティリスクの透明化のために必要な調査・政策検討について報告。

# 欧州における最近の動き

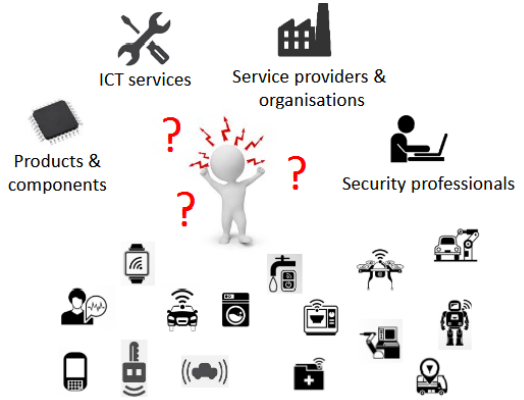
- **欧州では、「Cybersecurity Certification Framework」の導入に向けた議論を継続。**
- **なお、EU一般データ保護規則（GDPR）が2018年5月25日から施行。**

## 「Cybersecurity Certification Framework」の経緯

- 2017年9月、ユンカー欧州委員会委員長の施政方針演説で、EUにおけるサイバーセキュリティ政策（Cybersecurity Act）が発表され、そこには新たにサイバーセキュリティ認証フレームワーク（Cybersecurity Certification Framework）の導入について言及。
- 2018年2月、EU標準化団体とENISAにより、「Cybersecurity Act」に関する会議開催。
- 2018年3月、欧州委員会とENISAにより、「Cybersecurity Certification Framework」に関する会議開催。
- 2019年5月、Cybersecurity Actの施行予定。

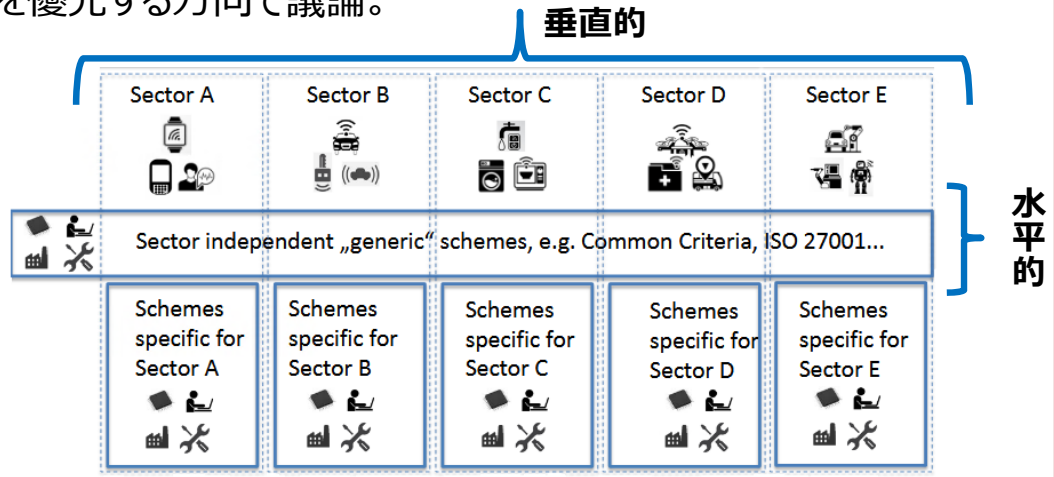
## 「Cybersecurity Certification Framework」の特徴

- 既に多数のスキームが存在していることから、一からFrameworkを作成するわけではなく、「Meta-Scheme Approach」を用いたスキームを指向。Voluntaryなものとして、枠組み作りを優先する方向で議論。




全ての要求を満たすスキームは存在せず、
現時点で多くのスキームが存在。

Meta-Scheme Approach




メタ言語を介し異なるスキームを横断して組み立て。

１．IoTの進展等によるSociety5.0の実現に伴う
サイバー攻撃の脅威レベルの向上

２．サプライチェーンサイバーセキュリティ強化へ向けた
検討体制の構築

３．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策定

４．フレームワークを活用したサプライチェーンサイバーセキュリ
ティ強化
～産業分野別のガイドライン策定と必要な技術開発の促進

# サイバーセキュリティ政策の方向性

## 1．産業政策と連動した政策展開

① 重要インフラの対策強化
－情報共有体制強化　等

② IoTの進展を踏まえたサプライチェーン毎の対策強化 (Industry by industry)
－防衛関係、自動車、電力、スマートホーム等の分野別検討と技術開発・実証の推進

③ 中小企業のサイバーセキュリティ対策強化

## 2．国際ハーモナイゼーション

① 日米欧間での相互承認の仕組みの構築

② 民間主体の産業活動をゆがめる独自ルールの広がり阻止

## 3．サイバーセキュリティビジネスの創出支援

① 産業サイバーセキュリティシステムを海外に展開

② サービス認定創設、政府調達などの活用

## 4．基盤の整備

① 経営者の意識喚起

② 多様なサイバーセキュリティ人材の育成（ICSCoE等）

③ サイバーセキュリティへの過少投資解決策の検討

# (参考)産業サイバーセキュリティ研究会

- サイバーセキュリティに関し、大所高所の観点から議論し、メッセージを強く発信。
- 政府の政策や、研究会の下に設置するWGの具体的アクションについて方向を提示。

＜構成員＞

※肩書等は平成30年5月30日時点

石原　邦夫　日本情報ｼｽﾃﾑ・ﾕｰｻﾞｰ協会会長、東京海上日動火災保険株式会社相談役

鵜浦　博夫　日本電信電話株式会社代表取締役社長

遠藤　信博　日本経済団体連合会情報通信委員長、日本電気株式会社会長、サイバーセキュリティ戦略本部員

小林　喜光　経済同友会代表幹事、株式会社三菱ケミカルホールディングス取締役会長

中西　宏明　日本経済団体連合会副会長・情報通信委員長、株式会社日立製作所会長

船橋　洋一　アジア・パシフィック・イニシアティブ理事長

宮永　俊一　三菱重工業株式会社社長

座長　村井　純　慶應義塾大学教授、サイバーセキュリティ戦略本部員

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

# サイバーセキュリティ政策の課題とWG等における対応状況

**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

- 重要インフラ分野における情報共有体制の構築

サイバーセキュリティ基本法改正（NISC）にて対応

3/9
閣議決定

- 「Society5.0」におけるサプライチェーン全体のセキュリティ確保

WG１
（制度・技術・標準化）

第１回　2/7
第２回　3/29

- 経営者のサイバーセキュリティに関する意識喚起
- セキュリティ人材の育成
- 日米欧三極の連携強化

WG２
（経営・人材・国際）

第１回　3/16
第２回　5/22

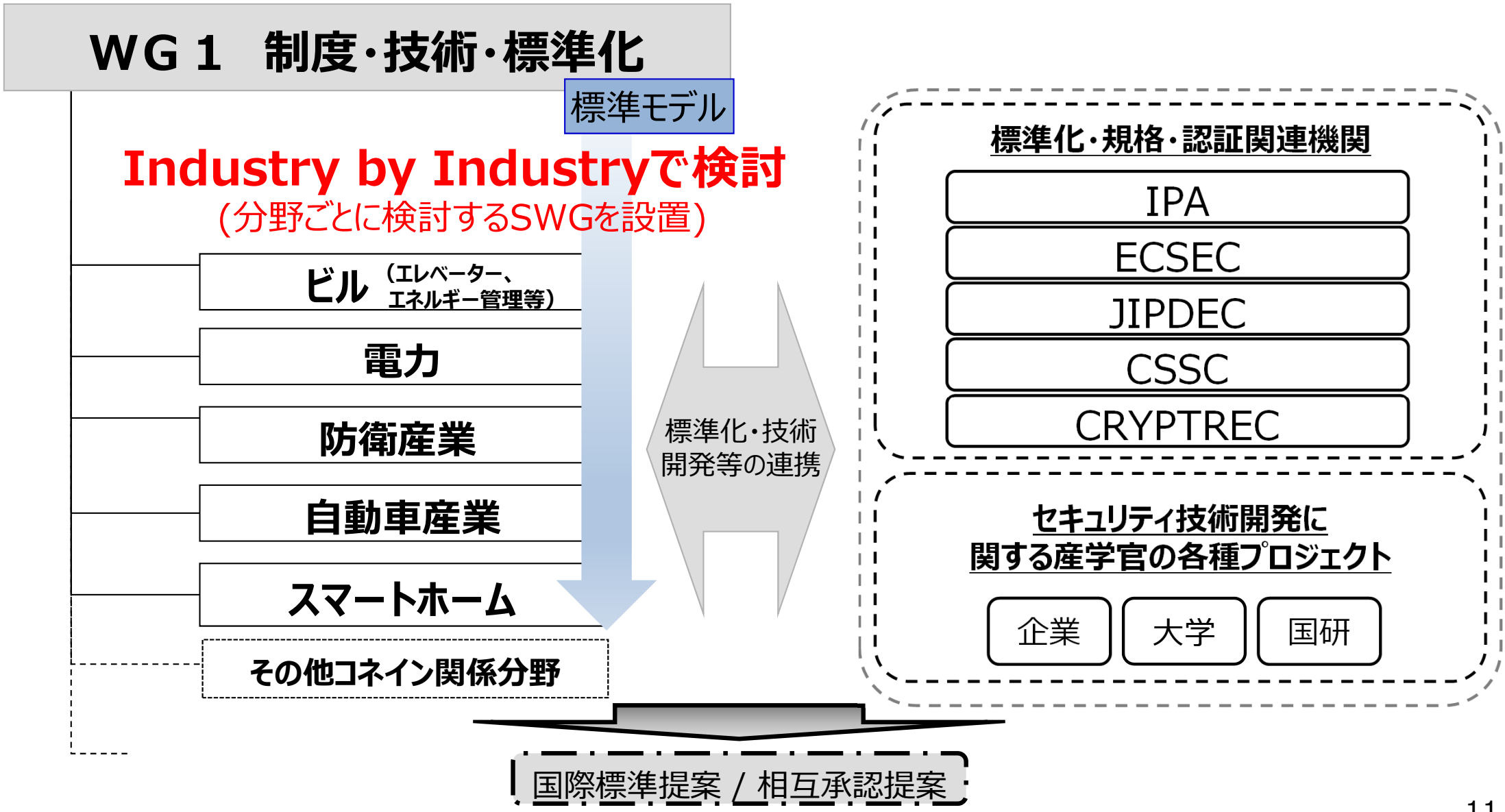
- サイバーセキュリティのビジネス化

WG３
(サイバーセキュリティビジネス化)

第１回　4/4

# WG1の検討体制

- サイバー・フィジカル・セキュリティ対策フレームワーク（後述）の標準モデルを検討し、業界毎に順次展開して、具体的適用のためのセキュリティポリシーを検討。



１．IoTの進展等によるSociety5.0の実現に伴う
サイバー攻撃の脅威レベルの向上と海外の動向

２．サプライチェーンサイバーセキュリティ強化へ向けた
検討体制の構築

**３．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策定**

４．フレームワークを活用したサプライチェーンサイバーセキュリティ強化
～産業分野別のガイドライン策定と必要な技術開発の促進

# サイバー・フィジカル・セキュリティ対策フレームワークを策定する目的

- 「Society5.0」、「Connected Industries」の実現へ向けて、**産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応することが必要**。
- **このため、産業に求められるセキュリティ対策の全体像を整理**し、**産業界が活用できる『サイバー・フィジカル・セキュリティ対策フレームワーク』の策定**を進めている。

## １．各事業者がフレームワークを活用することで期待される効果

- **「Society5.0」、「Connected Industries」の実現に求められるセキュリティの確保**
- **製品・サービスのセキュリティ品質を差別化要因（価値）にまで高めることによる競争力の強化**

## ２．フレームワークの特徴

### ①　各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる

- 社会として目指すべき概念だけではなく、各事業者が実際にセキュリティ対策を実施するうえで活用できる内容にする。

### ②　セキュリティ対策の必要性とコストの関係を把握できる

- サプライチェーン全体を構成する中小企業を含めた事業者が、実際に対策を行えるよう、想定されるリスクと必要な対策のコストのバランスをイメージできるような内容にする。
- セキュリティレベルを保ったままでコストを圧縮できるような内容にする。
- リスクシナリオベースの考え方も考慮した内容にする。

### ③　グローバルハーモナイゼーションを実現する。

- グローバルサプライチェーンの中で、日本における製品・サービスのセキュリティ対策が海外からも認められるよう、諸外国の動きをよく取り入れ、ISMSやNIST Cybersecurity Frameworkなど米欧などの主要な認証制度との整合性を確保し、相互承認を進めていくことができる内容にする。

# フレームワークの構造～「Society5.0」型サプライチェーン“価値創造過程”への対応

- あらゆるものがつながるIoT、データがインテリジェンスを生み出すAIなどによって実現される**「Society5.0」（人間中心の社会）、「Connected Industries」では、製品/サービスを生み出す工程（サプライチェーン） も従来の定型的・直線的なものとは異なる、多様なつながりによる非定型の形態を取る**ことになる。
- 本フレームワークでは、このような**「Society5.0」型サプライチェーンを**これまでのサプライチェーンとは区別して認識するため、**価値創造過程（バリュークリエイションプロセス）と定義**し、「Society5.0」、「Connected Industries」によって拡張したサプライチェーンの概念に求められるセキュリティへの対応指針を示す。

- 本フレームワークは、価値創造のための活動が営まれる産業社会を、下記の**三層構造**と**6つの構成要素**で捉え、包括的にセキュリティポイントを整理し、それらに対応するための指針となるものである。　⇒　**詳細は次頁以降参照**

**◆三層構造**

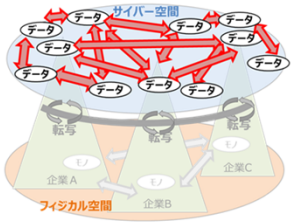
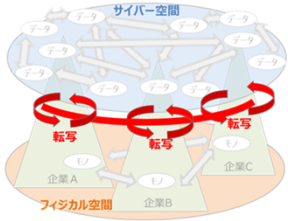
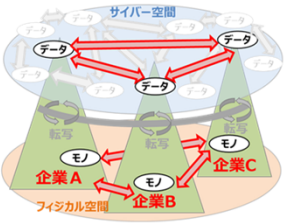
**第3層－　サイバー空間におけるつながり**

**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（従来型サプライチェーン）**

**◆６つの構成要素**

**－組織、ヒト、モノ、データ、プロシージャ、システム**

| 三層構造 | 概念図 |
|---|---|
| サイバー空間におけるつながり【第３層】 |  |
| フィジカル空間とサイバー空間のつながり【第２層】 |  |
| 企業間のつながり（従来型サプライチェーン）【第１層】 |  |

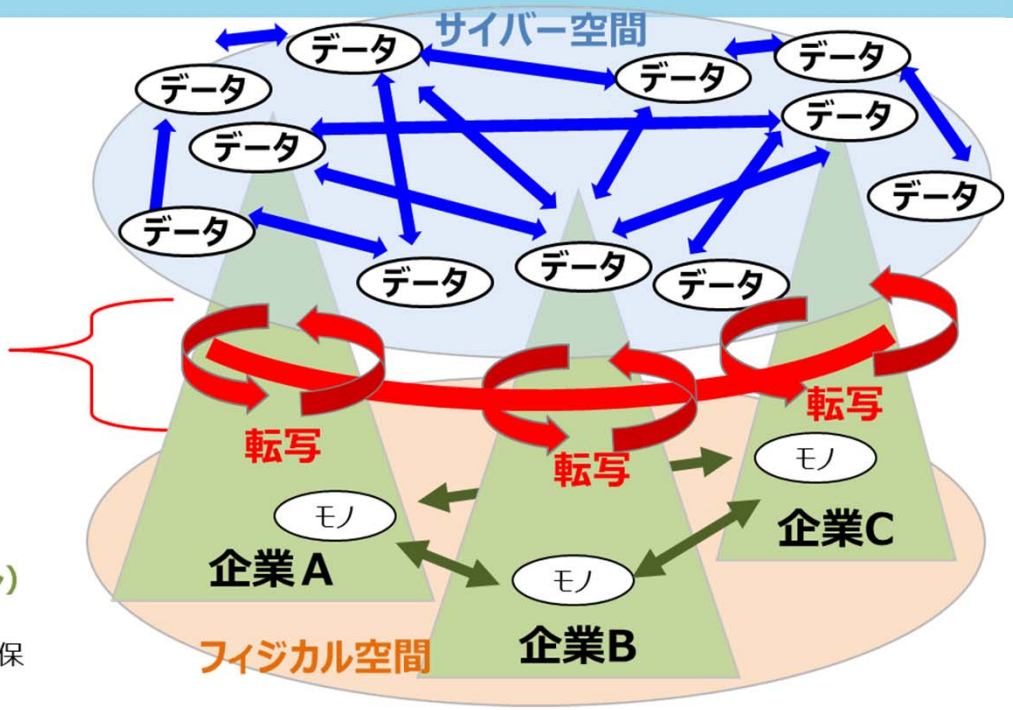
# 三層構造アプローチの意義

- 3つの層には、価値創造過程において確保されなければならない機能・役割が存在する。
- 例えば、各層において以下で示すようなことが確保されていなければ、価値創造過程は成立をしないことになる。
  - 第１層では生産された製品等－信頼できる企業が信頼できる生産活動によって仕様どおりの製品やサービスを供給しているか否か
  - 第２層ではセンサーで読み込まれたデータ等－フィジカル空間における情報を、センサーなどのIoT機器が正確にデジタル化し、サイバー空間に“転写”しているか否か
  - 第３層ではデータ分析で得られたデータ等－収集する過程で改ざんされていないデータを適切な方法で加工した、信頼できるデータを活用できるか否か
- 本フレームワークでは、各層で創造される価値の持つ特徴を踏まえた対応の方針を示す。

**サイバー空間におけるつながり**
**【第３層】**
- 自由に流通し、加工・創造されるサービスを創造するためのデータの信頼を確保

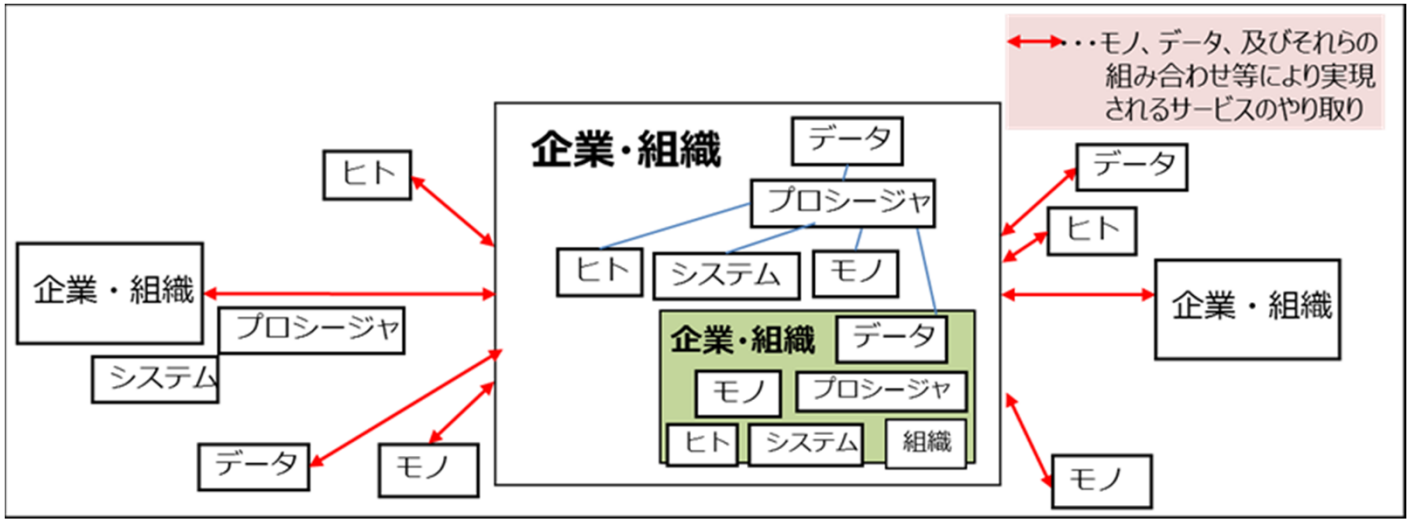
**フィジカル空間とサイバー空間のつながり**
**【第２層】**
- フィジカル・サイバー間を正確に“転写“する機能の信頼を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

**企業間のつながり（従来型サプライチェーン）**
**【第１層】**
- 適切なマネジメントを基盤に各主体の信頼を確保

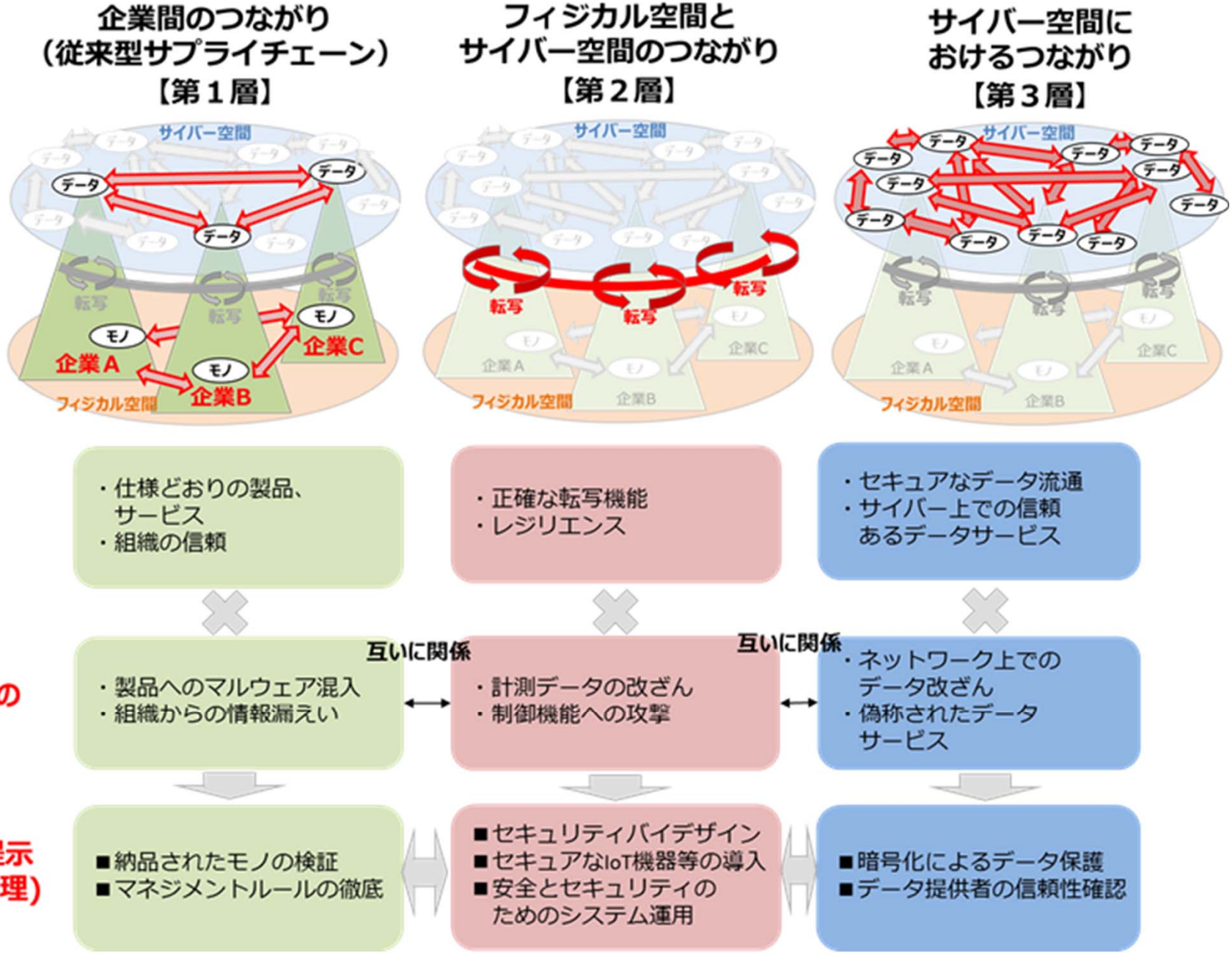


# 価値創造過程に関わる６つの要素と構成要素の関係

| 構成要素 | 定義 |
|---|---|
| **組織** | • 価値創造過程（特に、従来型サプライチェーン）に参加する企業・団体 |
| **ヒト** | • 組織に属する人、及び価値創造過程に直接参加する人 |
| **モノ** | • ハードウェア、ソフトウェア、及びそれらの部品 |
| **データ** | • フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報 |
| **プロシージャ** | • 定義された目的を達成するために要求される定型化された一連の活動 |
| **システム** | • サービスを実現するためにモノで構成される仕組み・インフラ |



# 各層におけるセキュリティ対策の概要



# フレームワークにおける信頼の確保の考え方

- サイバーフィジカルシステムのセキュリティを確保するため、それぞれの構成要素についての**セキュリティの確保(信頼の創出)とその確認(信頼の証明)を繰り返し行い、信頼のチェーンを構築、維持することで、価値創造過程全体のセキュリティを実現**。

**1．信頼の創出**

・セキュリティ要件を満たすモノ・データ等の生成
・対象のモノ・データ等が要件を満たした形で生成されたことの確認

**2．信頼の証明**

・対象のモノ・データ等が正常に生成されたものであることを確認できるリスト(トラストリスト)の作成と管理
・トラストリストを参照することで対象のモノ・データ等が信頼できるものであることの確認

**3．信頼のチェーンの構築と維持**

・信頼の創出と証明を繰り返すことで信頼のチェーンの構築(トレーサビリティの確保)
・信頼のチェーンに対する外部からの攻撃等の検知・防御
・攻撃に対するレジリエンスの強化

# サイバー・フィジカル・セキュリティ対策フレームワークへのパブコメ

- **<u>実施期間・状況</u>**
  - 平成30年4月27日～5月28日でパブリックコメントを実施。
  - 海外からの関心が高く、**英語版パブコメも実施**。
  - **国内23、海外10の組織・個人より、300以上の意見**提出あり。**肯定的な意見が9割弱**。

- **<u>国内からの主な意見</u>**
  - Society5.0における信頼の確保へ向けた取組として、**フレームワークの趣旨に賛同**。
  - **既存の国際規格等があるので、対応関係を明確化**してほしい。
  - NIST SP800-171と比較して、**対策の強度は低いが準拠するためのコストが掛かる**ことを懸念。

- **<u>海外からの主な意見</u>**
  - **フレームワーク案を広く支持**。サイバーセキュリティと経済活動を両立する上で効率的な、マルチステークホルダーアプローチやリスクベースアプローチに合致する多数の概念や対策が含まれている。
  - **国際規格であるIEC 62443 への言及が少ないように見える。**
  - **中小企業にとっても活用しやすいガイドラインを期待**。

# (参考)国際標準等との整合性について

- 国際標準等との整合性を取るため、**国内外の30以上の規格等を参照して作成。**
- 特に、**3つの重要な規格等(下記赤字のもの)**については、**対応表を作成し、整合性を確認した上で、公表済み。**

**(参照した主な規格等)**

- **国際標準**
  - ① IEC 62443 (IEC)
  - ② **ISO/IEC 27001:2013 (ISO/IEC)**
  - ③ ISO/IEC 27002:2013 (ISO/IEC)

- **欧州 Industrie 4.0 関連文書**
  - ① インダストリー4.0実現戦略 (Umsetzungsstrategie Industrie 4.0)
  - ② Security in RAM4.0
  - ③ Secure cross-company communication

- **米国NIST関連文書**
  - ① Framework for Cyber-Physical Systems
  - ② **Framework for Improving Crititcal Infrastructure Cybersecurity (NIST サイバーセキュリティフレームワーク)**
  - ③ Draft NISTIR 8200
  - ④ NIST SP800-53
  - ⑤ NIST SP800-161
  - ⑥ **NIST SP800-171**

１．IoTの進展等によるSociety5.0の実現に伴う
　サイバー攻撃の脅威レベルの向上と海外の動向

２．サプライチェーンサイバーセキュリティ強化へ向けた
　検討体制の構築

３．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策定

**４．フレームワークを活用したサプライチェーンサイバーセキュリティ強化**
**　～産業分野別のガイドライン策定と必要な技術開発の促進**

# サイバー・フィジカル・セキュリティ対策フレームワークの実装の方向性

- 『サイバー・フィジカル・セキュリティ対策フレームワーク』は、**対策の枠組み(チェックポイント)を示したものであり、セキュリティ水準(対策の強度)を示すものではない。**
- 産業分野ごとに守るべきものやリスクに違いも存在するため、**産業分野ごとにセキュリティ水準の検討を進めていく。**
- 必要に応じて、**求められるセキュリティ水準を満たしていることについて、認証を含めた確認方法についても検討を進める。**

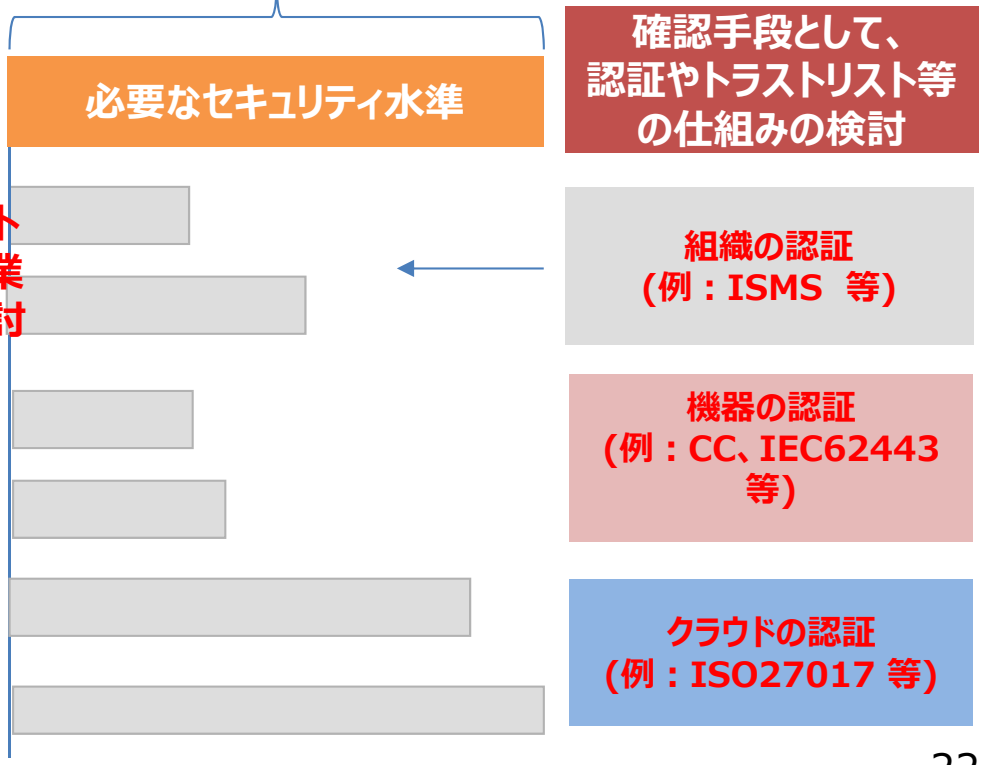
## 『サイバー・フィジカル・セキュリティ対策フレームワーク』と分野別におけるセキュリティ対策のイメージ

**サイバー・フィジカル・セキュリティ対策フレームワーク**

| 三層別アプローチ | 必要な対策のポイント |
|---|---|
| 1. 企業間のつながり (主体の信頼) | セキュリティポリシーの策定、体制の整備 |
| | 事業継続計画又はコンティンジェンシープランへの反映 |
| | ‥ |
| 2. フィジカル空間とサイバー空間のつながり (機能の信頼) | セキュリティ対策が施されたIoT機器の導入 |
| | セキュリティバイデザインの実践 |
| | ‥ |
| 3. サイバー空間におけるつながり (データの信頼) | 信頼できるサービスサプライヤーの選定 |
| | サイバー空間における接続相手の認証 |
| | ‥ |

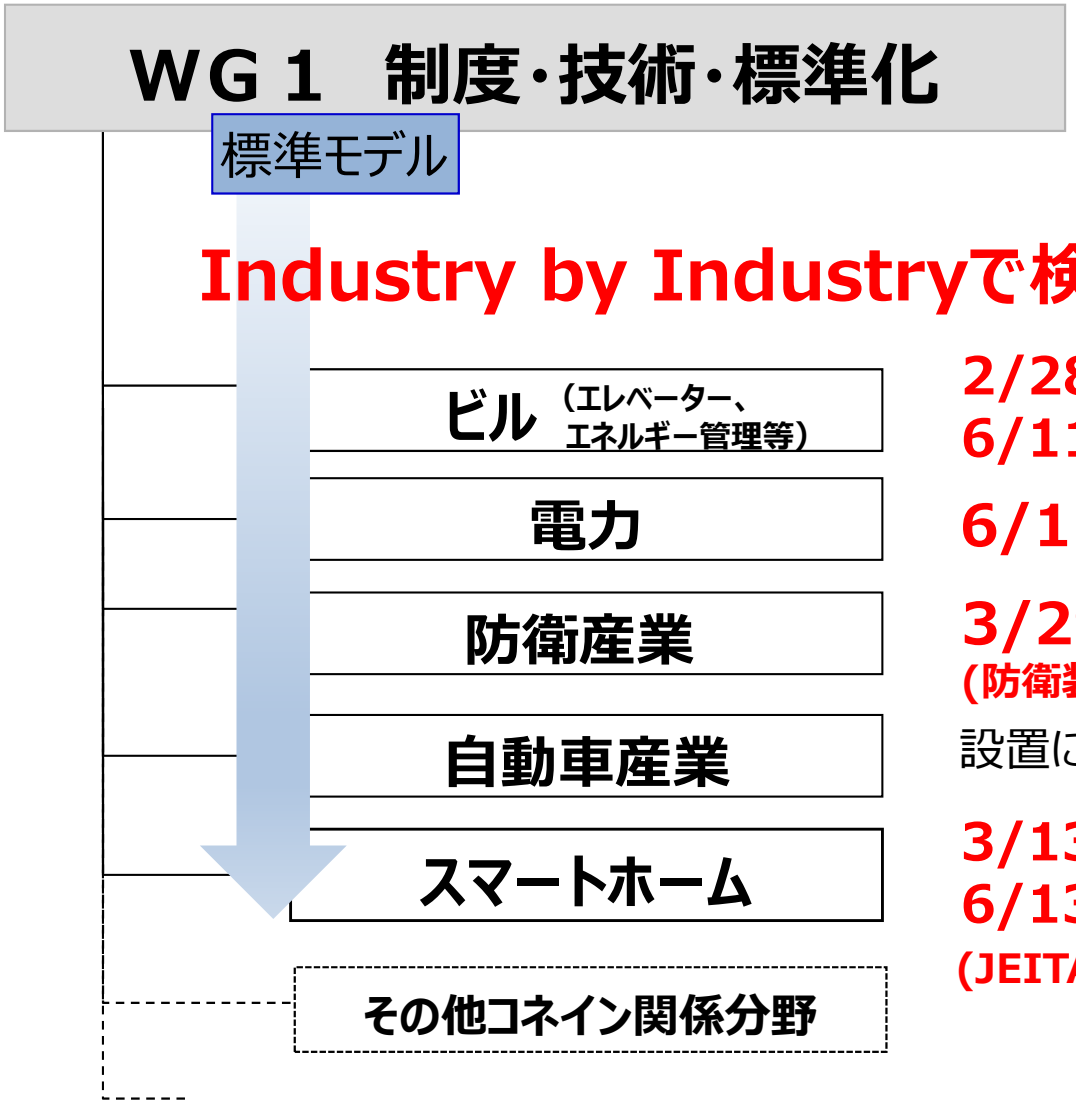
対策のポイントを踏まえて産業分野ごとに検討

**分野別セキュリティガイドライン**



# 産業分野ごとの検討の促進：分野別のSWGの設置

- WG1で検討する『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、分野別に順次展開し、具体的適用のためのセキュリティポリシーを検討。




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

**2/28 第1回会合, 4/16 第2回会合,**
**6/11 第3回会合開催**

**6/12 第1回会合開催**

**3/29 第1回会合開催**
**(防衛装備庁 第6回情報セキュリティ官民検討会)**

設置に向けた検討中

**3/13 第1回会合, 4/5 第2回会合,**
**6/13 第3回会合開催**
**(JEITA スマートホーム部会 スマートホームサイバーセキュリティWG)**

# ビルSWG（座長：江崎 浩 東京大学 教授）

- ビルの情報系・制御系システムに係るサイバー攻撃のリスクと、それに対するサイバーセキュリティ対策について、海外における取組状況を含めて知見を共有
- 共有した知見を踏まえ、ビルに求められるサイバーセキュリティ対策を整理し、ビルに関わるステークホルダーが活用できるガイドライン等をとりまとめる
- オリパラに向けて、各事業者において実施できる分野から実装を目指す

＜構成員＞

有識者、ビルオーナー、ゼネコン、サブコン、設計事務所
個別システム事業者（ビル管理、空調、エレベーター、ビデオ監視、電力・熱供給 等）
自治体、関係省庁 等

＜ガイドラインのとりまとめイメージ＞

- ビルシステム全体に共通する最低限の要求をまとめたもの＋より詳細な方策を示したものの二階建て構成
- ガイドラインでは、多くの事業者の取組の参考となるよう優先順位を示した選択肢を提供

**内容項目例**

・ビルに係わるサイバーセキュリティ上の脅威の現状
・ビルシステムに対して起こりえる攻撃とその影響の予測
・サイバーセキュリティ確保のための対策の概要
・対策の具体的内容
・対策実施に向けたチェックリスト

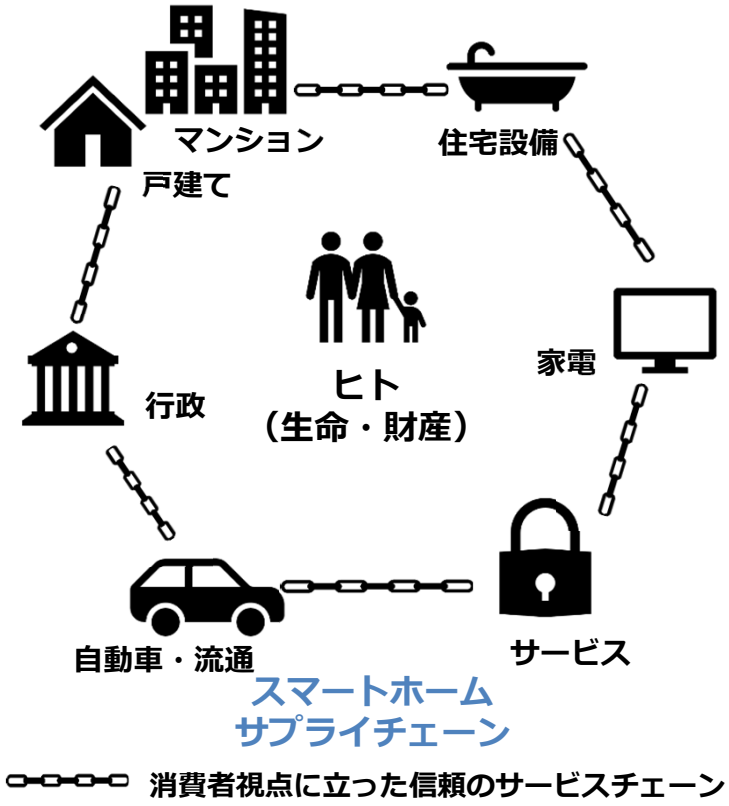
| フェーズ | 主な要求概要 | 関係するステークホルダー |
|---|---|---|
| 設計 | 機器、ネットワーク、物理セキュリティへの要求 | 設計事務所、オーナー、ゼネコン、サブコン、ベンダー |
| 施工／建築 | 機器単位、システム単位の施工プロセスへの要求 | ゼネコン、サブコン、ベンダー |
| 竣工検査 | 全体管理体制、管理結果、受入検査への要求 | ベンダー、ゼネコン、サブコン、オーナー、設計事務所 |
| 運用・保守 | 管理体制への要求 | オーナー、サブコン、ベンダー |

# スマートホームSWG（座長：小松崎 常夫 セコム株式会社 顧問）

- JEITA スマートホーム部会内にスマートホームサイバーセキュリティWGを新たに設置
- ハウスメーカ、システム・インテグレータ、機器メーカ等の住まいに関わる企業、業界団体が参加

＜構成員＞

企業）家電・AV関連、IT・通信関連、車載関連、住宅設備・サービス関連
団体・機関）住宅・住宅設備分野、電機・通信分野、医療分野、研究機関
スマートホーム部会長の丹 康雄教授（北陸先端大）も委員として参画




＜検討項目＞

Step1　“スマートホーム産業”に求められるセキュリティ対策像を整理し、**住宅・住設・家電・サービス等のスマートホームサプライチェーンで活用できる「サイバー・フィジカル・セキュリティ対策フレームワーク」**を策定する。

Step2　「サイバー・フィジカル・セキュリティ対策フレームワーク」を概念としてだけではなく、各事業者が実際のセキュリティ対策オペレーションレベルで活用できるよう、実効的な施策について検討を行い、必要に応じて、政府への政策提言を行う。

Step3　実運用に向けて、消費者へのリスク周知や免責事項、モニタリングの在り方、事業者間の信頼の創出方法等について検討。さらには、スマートホームからスマートライフ分野（街・社会インフラ）に対応したセキュリティ対策についても検討を進めていく。

# サプライチェーンサイバーセキュリティに係る研究開発の推進

- 総合科学技術・イノベーション会議の**研究開発プログラム（SIP）に「IoT社会に対応したサイバー・フィジカル・セキュリティ」プログラムを設置など**(※) 研究開発事業を拡充。
- 更に、**拠点化による中核的な研究開発体制の整備**や、研究成果の実装のための**認定・認証体制の強化**を推進。

## SIP第2期 「IoT社会に対応したサイバー・フィジカル・セキュリティ」

**平成30年3月30日：**
総合科学技術・イノベーション会議にて**課題決定**

**平成30年4月12日：**
**プログラムディレクター(PD)決定**
**後藤 厚宏 情報セキュリティ大学院大学 学長**

**平成30年度下半期：**
**研究開発開始を予定**

### 研究開発の内容

**■サプライチェーンのセキュリティ確保**

（例）
- IoT等の**エッジデバイスのセキュリティ確保**技術
- **取引先のセキュリティの確保状況を確認**するための基盤技術
- **AIを活用したサイバー攻撃の検知・解析**技術

※ AIチップ・次世代コンピューティングの技術開発においてもセキュリティ技術の研究開発を推進

# （参考）
# サイバーセキュリティの枠組みを巡る各国との議論の状況

# マルチ・バイを通じた国際協調への取り組み①

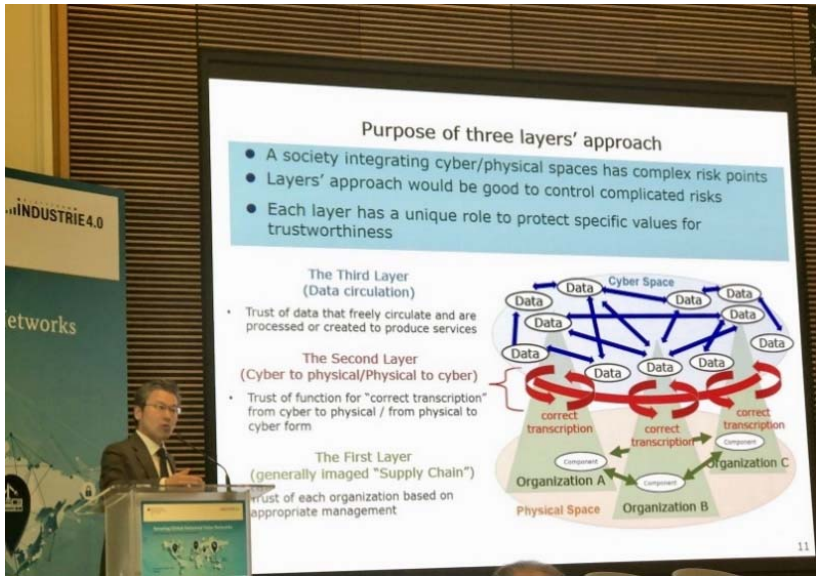
- **「サイバー・フィジカル・セキュリティ対策フレームワーク」**を軸に、各国のステークホルダーと議論、マルチの会議で紹介し、サイバー・フィジカル・セキュリティに関する共通の認識を醸成。
- **安全なサプライチェーンの実現**には関係する者の信頼性の確保について、各国と意見交換。

**【ドイツ】**

- **Securing Global Industrial Value Networks （2018年5月@ベルリン）**

➢ ドイツを中心とした各国の官民の関係者にむけて、Society5.0時代のサイバーセキュリティについてフレームワークや標準化活動等、日本の取組を説明。

➢ 日独連携の取組の成果として、2017年に引き続き2018年5月に産業サイバーセキュリティに関する共同ポジションペーパーを発出。カンファレンスの講演内で日独双方から披露・解説。

# マルチ・バイを通じた国際協調への取り組み②

**【EU・OECD】**

- **<u>日EUデータエコノミー対話 政府間会合（2018年4月@東京）</u>**

➢ EUでサイバーセキュリティを所掌する通信総局（DG CONNECT）へフレームワークを紹介。
日欧は協調してセキュリティに関する国際的なルール構築に当たっていくとの認識を共有。

- **<u>OECD／CDEP（デジタル経済政策委員会）会合（2018年5月@パリ）</u>**

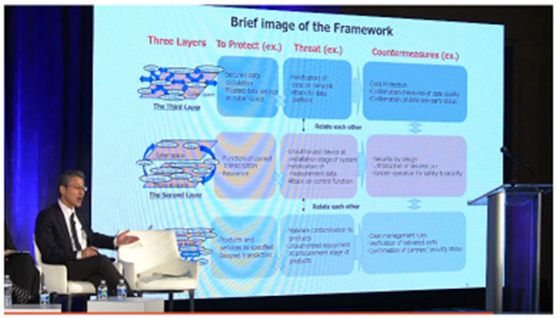
➢ セキュリティ・プライバシーに関する作業部会（SPDE）にてフレームワークを紹介。


# マルチ・バイを通じた国際協調への取り組み③

【アメリカ】

- **TecGlobal （米国商工会議所主催）（2018年４月@ワシントン）**

➢ 国土安全保障省、アメリカ民間企業等に、現在日本で検討を進めているフレームワークについて、基本的な考え方や検討状況を共有し、お互いのサイバーセキュリティの取組を協調しながら進めていく環境を整備。




米国商工会議所のHPより引用

- **Industrial Control Systems Joint Working Group (ICSJWG)**

**（2018年４月@アルバカーキ）**

➢ 米国国土安全保障省(DHS）傘下の国家サイバーセキュリティ通信総合センター（NCCIC）が、重要インフラ防護に向けて官民関係者の連携を深めるべく、関係者で情報共有を図る会議において「サイバー・フィジカル・セキュリティ対策フレームワーク」を初めとする経産省のサイバーセキュリティ政策について紹介。

# マルチ・バイを通じた国際協調への取り組み④

**【ASEAN】**

- **<u>第2回日・ASEANサイバーセキュリティWG（2018年５月@インドネシア・バリ）</u>**

➢ 情報セキュリティ分野において、我が国とASEAN諸国との国際的な連携・取組を強化することを目指す会議において、日本のサプライチェーンセキュリティの取組、フレームワークについて紹介。域内の情報セキュリティ水準向上のための意識啓発を実施。

➢ 日米共同演習への参加を呼びかけ。

# マルチ・バイを通じた国際協調への取り組み⑤

【APEC】

- **APEC TEL57（第57回電気通信・情報作業部会）（2018年6月@パプアニューギニア・ポートモレスビー）**

➢ Security and Prosperity Steering Group (SPSG)において中国のサイバーセキュリティ関連組織であるCNCERT/CCが主催した「IoT Security Workshop」で、「サイバー・フィジカル・セキュリティ対策フレームワーク」について紹介。

➢ 華為技術（Huawei）、カスペルスキー研究所、UL等の民間企業やIntermet Society(ISOC)、Asia-Pacific Network Information Centre （APNIC ）等の国際団体も参加。


# （参考）
# 海外の動向の詳細等

# 連邦政府のサイバーセキュリティリスクに関する報告書

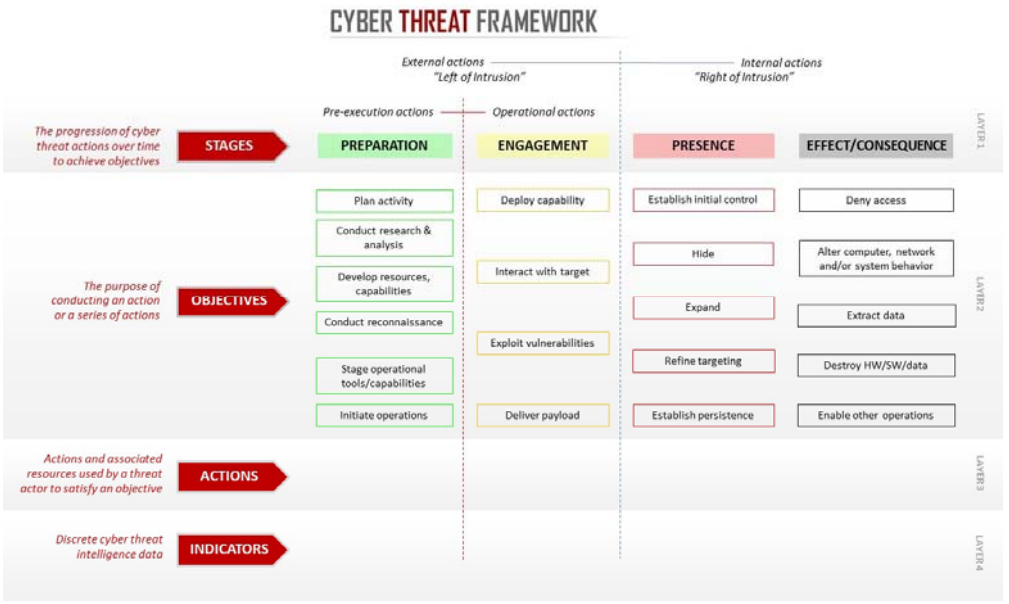
- **OMBとDHSが政府機関のサイバーセキュリティ管理能力のアセスメントを行い、96機関中71機関（74%）の機関が高リスク又はリスクがあると報告。**

## 改善に必要とされる４つのコア活動

（１）**サイバー脅威フレームワーク**の活用により、リスクの優先順位をつけて対策に取組む。
（２）ＩＴとサイバーセキュリティに係るコスト管理と資産マネジメント能力の標準化。
（３）ＳＯＣの統合により検知・対応能力を向上。
（４）プロセス改善や繰り返しのリスクアセスメントにより、説明責任能力を向上。

◆ <u>サイバー脅威フレームワーク （右図）</u>

- 国家情報長官官房(ODNI)が開発。
- サイバー攻撃における一連の活動を、４つの段階（Preparation → Engagement → Presence → Effect/Consequence）に分けて整理。
- サイバー攻撃に関する共通的な語彙と枠組みを提供し、脅威の傾向や必要な対策等を検討する際に使用されることを目指している。




出典：米国国家情報長官官房(ODNI)

# ボットネット対策等に関する報告書

- 2017年5月、トランプ大統領が「サイバーセキュリティ強化のための大統領令」に署名。
- 2018年１月、大統領令を踏まえた報告書案を公表（セキュリティ確保のためのエコシステムの形成を強調）。
- 2018年2月28日~3月1日、NIST、NTIA、DHSによるワークショップ開催。
- 2018年５月、本報告書を大統領に報告。
  同月22日、NTIAが最終報告書を公表。

**2017年5月大統領令**

**Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**（連邦ネットワーク及び重要なインフラストラクチャに対するサイバーセキュリティの強化に関する大統領令）　2017年5月11日
①連邦政府のネットワーク　②重要インフラ　③国家／国民のためのサイバーセキュリティ(ボットネット対策含む)に関して各連邦政府機関の長に対し、期限以内に大統領に報告書を提出するよう指示

**2018年5月最終報告書**

**A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats**（ボットネットおよびその他の自動化・分散化した脅威に対するインターネット・通信のエコシステムの強靭性の強化に関する報告書）　2018年5月22日
本報告書の公表をもって取組が終わる訳ではないとした上で、連邦政府が取り組むべき事項に力点を置き、関係者による様々な取組の調整・協働をサポートするための道筋を提示

# NIST SP800-171

- **NIST SP800-171は、CUIの保護を目的に14個のカテゴリと109の項目から構成。**
- **SP800-171の遵守状況に関する政府機関による第三者認証制度はなく、自己宣言という形で準拠したか否かについて判断する自己認証を採用。**

| | | |
|---|---|---|
| 2015.06 | **NIST SP800-171策定** | 非政府機関の情報システム等におけるCUI(*1)の保護を目的としたサイバーセキュリティ対策の要件を規定 |
| 2016.10 | **DFARS Clause252.204-7012発行** | CDI(*2)を保護対象とし、米国防衛省と契約する者に対し、2017年12月31日までにSP800-171相当のサイバーセキュリティの対応を要求。 |

(*1) Controlled Unclassified Information；管理対象となるが秘密指定されていない情報
(*2) Covered Defense Information

**NIST SP800-171における14個のカテゴリ**

1. アクセス制御：システムへのアクセスが出来る人／機能を制限すること
2. 意識向上と訓練：セキュリティポリシーを遵守すること
3. 監査と責任追跡性：システムの監査を行うとともに責任の追及が出来ること
4. 構成管理：システムを構成する機器に求められるセキュリティ構成設定を確立すること
5. 識別と認証：システム利用者、デバイスを識別すること(例えば、生体認証を必須化)
6. インシデント対応：インシデントの追跡、報告が出来ること
7. メンテナンス：組織のシステムのメンテナンスを行うこと
8. 記録媒体保護：CUIをセキュアに格納するとともにアクセスできる者を制限すること
9. 人的セキュリティ：システムへのアクセスを行う個人を審査すること
10. 物理的保護：組織のシステム、装置等への物理的アクセスを制限すること
11. リスクアセスメント：情報資産のリスクを適切に評価すること
12. セキュリティアセスメント：セキュリティ管理策を定期的に評価すること
13. システムと通信の保護：システムの鍵となる通信を監視し、制御し、保護すること
14. システムと情報の完全性：タイムリーに情報及びシステムフローを識別すること

# NIST SP800-171

- **NISTは、SP800-171の定期的なメンテナンスを実施。**
- **2018/06/07にも、アップデート版を公表。**

**2018/06/07アップデート版では、「APPENDIX F : DISCUSSION」が追加。**

APPENDIX F

## DISCUSSION

IMPLEMENTING AND ASSESSING CUI SECURITY REQUIREMENTS

Tables F-1 through F-14 provide discussion intended to facilitate implementing and assessing the CUI security requirements in NIST Special Publication 800-171. This information is derived primarily from the security controls and discussion in NIST Special Publication 800-53. It is provided to give assessors a better understanding of the mechanisms and procedures used to implement the safeguards employed to protect CUI. The discussion is *not* intended to extend the security requirements or the scope of the assessments of those requirements. NIST publications identified in the following tables are available at https://csrc.nist.gov/publications.

TABLE F-1: DISCUSSION ON ACCESS CONTROL REQUIREMENTS

| | |
|---|---|
| 3.1.1 | SECURITY REQUIREMENT<br>Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). |
| | DISCUSSION<br>Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for both systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2. |
| 3.1.2 | SECURITY REQUIREMENT<br>Limit system access to the types of transactions and functions that authorized users are permitted to execute. |
| | DISCUSSION |

**これは、CUIセキュリティ要件の実装と評価を容易にするための「DISCUSSION」を提供するものである。**

例

| | |
|---|---|
| **3.1.13** | **SECURITY REQUIREMENT**<br>リモートアクセスセッションの機密性を保護するために暗号メカニズムを採用する。 |
| | **DISCUSSION**<br>一般に適用される暗号標準には、FIPSで検証された暗号とNSAで承認された暗号が含まれる。 |