

# 「サイバー・フィジカル・セキュリティ対策 フレームワーク」策定後のWG1の進め方 (案)

平成31年4月4日

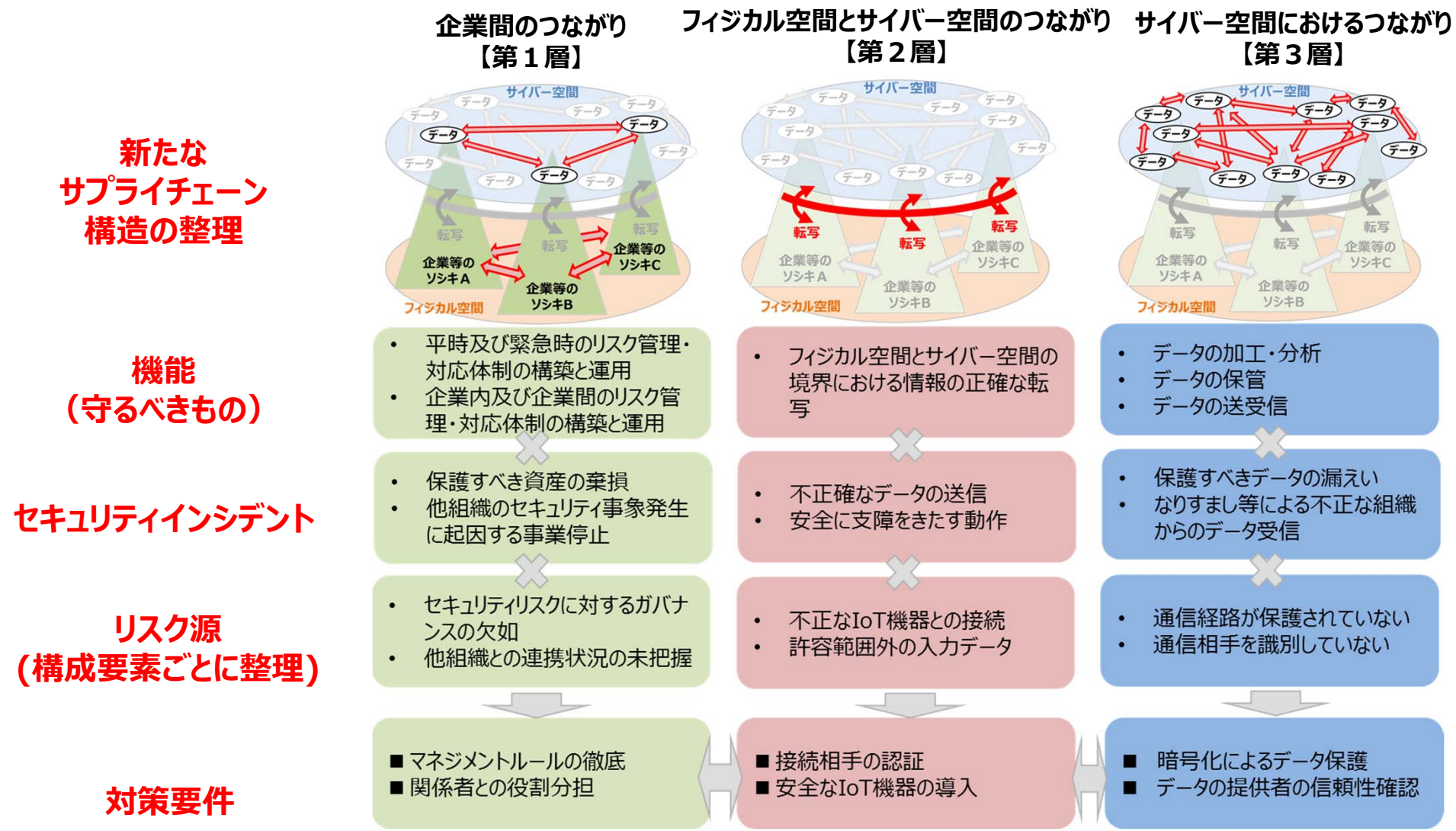
経済産業省 商務情報政策局

サイバーセキュリティ課

# 【WG 1 におけるこれまでの取組】

## 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

- サイバー・フィジカル・セキュリティ対策フレームワーク（以下「CPSF」という）は、サイバー空間とフィジカル空間が高度に融合した新たな産業社会「Society5.0」におけるセキュリティ対策の全体像を示すもの。
- 「Society5.0」における新たなサプライチェーンのリスク源を適切に捉え、検討すべきセキュリティ対策を提示するための新たなモデル（3層、6要素）を構築。



# 【WG 1 における今後の取組】CPSFの産業活動への実装の促進

- CPSFの産業活動への実装を進めるため組織間で共有する資産を扱う場合や産業特徴が共通する分野毎に、**実際の産業活動の内容に応じた対策要件と対策水準について検討を進めることが必要**ではないか。
- また、対策要件に基づいて**効率的に対策を実施するために必要となる、具体的な対策手法やルールの明確化**を行うことも必要ではないか。
- こうした検討は**国際的ハーモナイゼーションが必要**であり、国際的認知が進んだ**CPSF**をベースに進める。

## 実際の産業活動の内容のイメージ

データを介した連携を行う産業活動  
(分野間の連携 等)

### 分野別の産業活動

- ビル
- 電力
- 防衛
- 自動車
- スマートホーム 等

### 規模別の産業活動

- 中小企業向けのセキュリティ対策 等

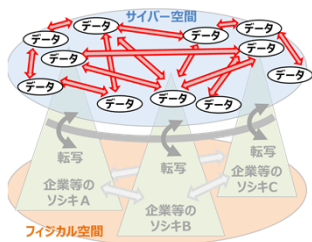
## 具体的な対策手法やルールの明確化のイメージ

データの信頼性の確認手法  
(データの完全性、真正性等の確認 等)

転写機能を持つ機器の信頼性の確認手法  
(機器・システムのセキュリティ等)

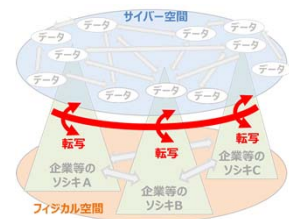
ソフトウェアの取扱いに関するルール・管理手法  
(software component transparency 等)

【第3層】



サイバー空間におけるつながり  
～信頼性の基点はデータ～

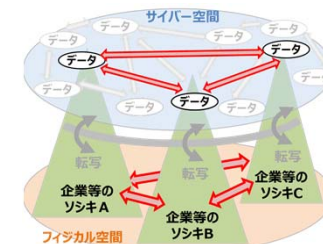
【第2層】



フィジカル空間とサイバー空間のつながり  
～信頼性の基点は転写機能～

【第1層】

企業間のつながり  
～信頼性の基点は企業（組織）のマネジメント～

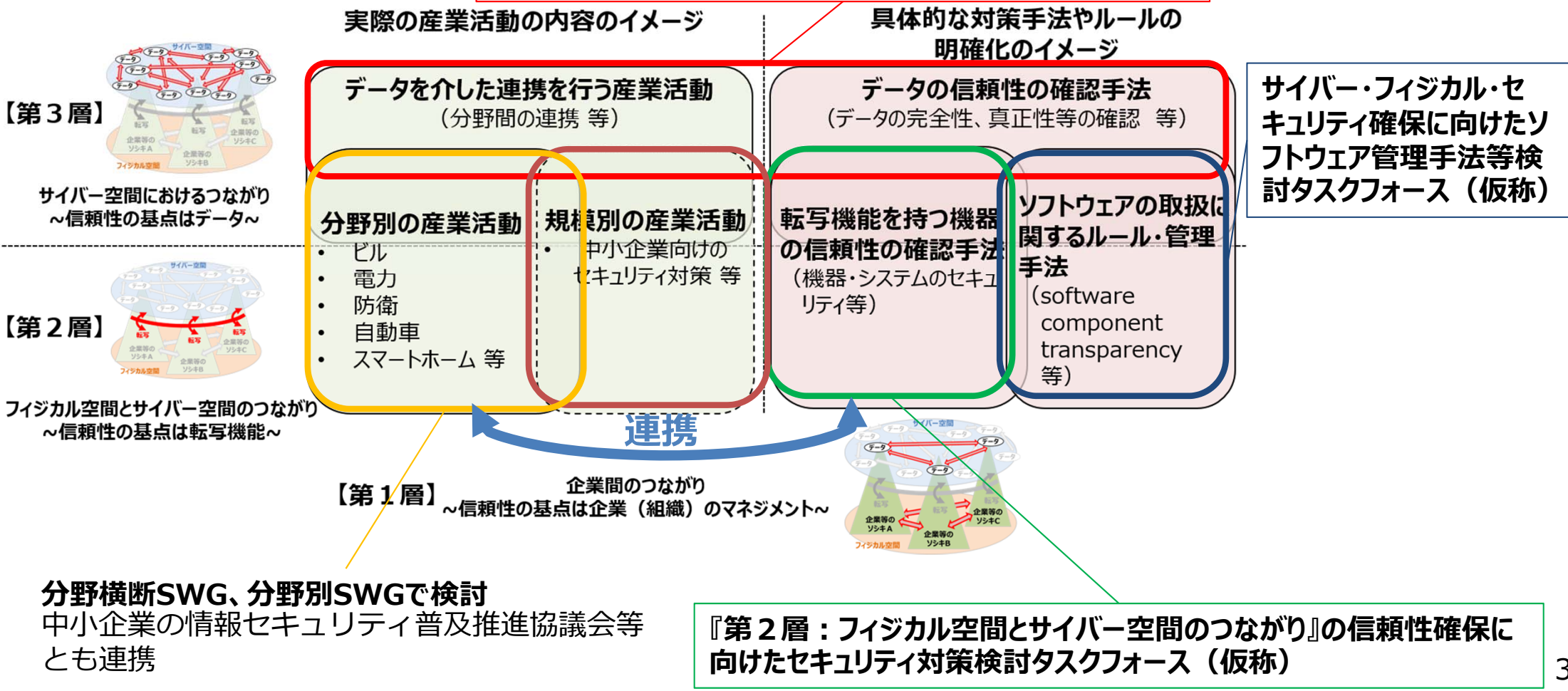


# 【WG 1 における今後の取組】

## 各検討項目に焦点を絞ったタスクフォース（TF）の設置（案）

- CPSFの実装を進めるために検討すべき項目ごとに焦点を絞ったTFを設置する。
- 各TFは、分野横断SWG、分野別SWGと連携しながら検討を進め、結果をWG1へ報告する。

『第3層：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（仮称）  
 （・特に、国際的ハーモナイゼーションを視野に入れた議論が必要  
 ・データの信頼性の確認手法は、特に、情報プロジェクト室と連携を想定）



**『第3層：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（仮称）**



# 【『第3層』タスクフォース設置の必要性】

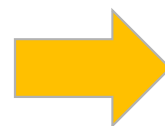
## サイバー空間におけるつながりの内容に応じたセキュリティ対策要件と対策水準の明確化

- 「Society5.0」における産業社会では、**データそのものの信頼性の確保が重要な課題**。このため、CPSFの三層構造アプローチでは、バリュークリエーションプロセスの信頼性確保のため、**データを、第3層サイバー空間のつながりにおける信頼性の基点と設定し、対策要件及び対策例を提示**。
- 実際の産業活動への実装を進めるため、**より具体的な対策要件と対策水準を定めることが必要**。
- データ・フリー・フロー・ウィズ・トラスト（DFFT）の議論が進む中、**国際的認知が進むCPSFをベースに国際的ハーモナイゼーションを視野に入れて検討**。

### <添付C> 対策要件に応じたセキュリティ対策例集

対策要件ID	対策要件	対策例	対策例を 実行する主体
CPS.GV-3	各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって <b>要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う</b> 。	...	O
CPS.SC-7	<b>自組織が関係する他組織との契約上の義務を果たしていることを証明するための情報(データ)を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする</b> 。	...	O/S
CPS.CM-4	<b>サイバー空間から受ける情報(データ)の完全性および真正性を動作前に確認する</b> 。	...	S

対策要件に、データ区分に応じた適切なデータ保護を規定。  
さらに、区分毎の具体的なセキュリティ要件を定めることも必要。



データの区分に対応した完全性確認などの  
セキュリティ対策について検討。

# 『第3層』タスクフォースにおける検討の方向性




- 本タスクフォースにおいて、取り扱うデータの区分に応じたセキュリティ対策要件と対策水準、それに対応したデータの完全性、真正性等の確認手法を検討。
- データ区分に応じたセキュリティ対策及びデータ信頼性の確認手法を確立することで、各主体が各データ区分に応じて適切なセキュリティ対策要件と水準の選択が可能となる。

## タスクフォースにおける検討内容イメージ

### サイバー空間において 流通するデータのイメージ

- 個人情報に関連するデータ
- 限定提供データ
- 輸出管理に関連する技術情報等



データ区分（案）	対策要件と対策水準（イメージ）
レベル3 	<High Advanced> を中心とした対策を選択。
レベル2 	<Advanced> を中心とした対策を選択。
レベル1 	<Basic> を中心とした対策を選択。

- ① データの管理レベルに応じた適切なセキュリティ対策の検討。
- ② その中で、必要となるデータの信頼性の確認手法を明確化。

『第2層：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（仮称）



# 【『第2層』タスクフォース設置の必要性】

## サイバー空間とフィジカル空間をつなぐ機能を持つ機器の確認方法の明確化

- Society5.0において、第2層フィジカル空間とサイバー空間をつなぐ機能の信頼性の確保は重要。このため、CPSFにおいて、サイバーとフィジカルの間での転写機能を持つ機器の対策要件として、正規品を扱うことなどを記載。
- また、CPSFでは、機能安全とサイバー・セキュリティを組み合わせることで対応することの必要性を指摘。
- こうした機能を持つ機器・システムに求められる安全も考慮に入れたセキュリティ対策とその確認方法の明確化が必要。

### <添付C> 対策要件に応じたセキュリティ対策例集

対策要件ID	対策要件	対策例	対策例を実行する主体
CPS.SC-4	外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	<Basic> <ul style="list-style-type: none"> <li>● 組織は、調達時に、<b>自組織が所有するIoT機器が正規品であるかをラベルを確認</b>する等して確かめる。</li> <li>● 組織は、IoT機器やソフトウェアに含まれるIDや秘密鍵、電子証明書等を用いて調達した機器が正規品であることを確認する。</li> </ul>	○

機器が正規品であるかの確認は、重要。



機器が正規品であるか適切に確認する仕組みの在り方について検討。

対策要件ID	対策要件	対策例	対策例を実行する主体
CPS.PT-3	ネットワークにつながることを踏まえた <b>安全性を実装するIoT機器</b> を導入する。	...	○

機器の導入はセキュリティだけではなく、安全の観点も重要。



安全も考慮に入れたセキュリティ対策について検討。

# これまでの経産省におけるアプローチ（分野別SWGにおいて検討）

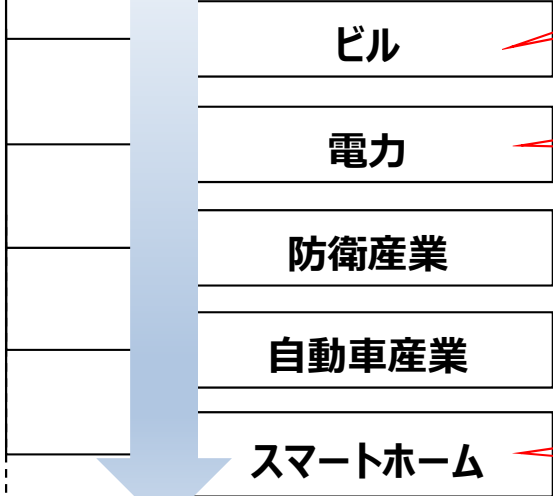
- 各分野別SWGにおいて、CPSFを参照し、その具体的適用のためのセキュリティポリシーを検討。
- **各SWG（ビル、電力、スマートホーム等）**では、各産業分野の実際の産業活動に応じたセキュリティ対策について整理し、ガイドライン等の策定を進めている。その中で、一部SWGにおいては、認証等の必要性についても議論。
- 各SWGの検討について、横ぐしを通していくことが必要となっていく。

## WG 1 制度・技術・標準化

標準モデル

### Industry by Industryで検討

(分野ごとに検討するためのSWGを設置)



※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の取組】

- ・ ビルの管理・制御システムに係る各種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を整理し、ビルに関わるステークホルダーが活用できる**ビルガイドライン**を策定中。

#### 【電力SWGの取組】

- ・ 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、官民が取り組むべき課題と方向性について、広く検討。**結果を電力制御系ガイドラインに反映していく方針**。一部機器に対する認証等の必要性（CPICへの参加等）についても議論。

#### 【スマートホームSWGの取組】

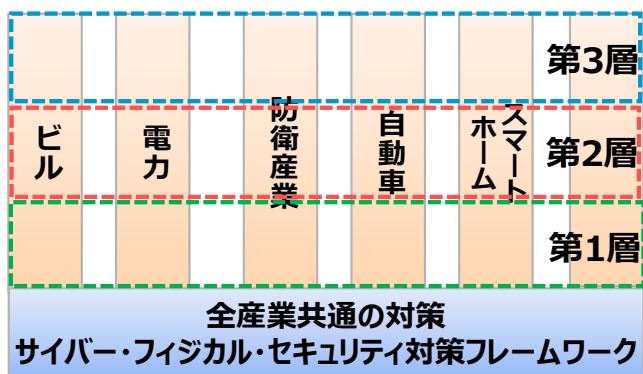
- ・ スマートホームSWGでは、各家庭におけるネットワーク構成とスマート家電等の基本形を整理し、各家庭におけるセキュリティリスクポイントを洗い出し。
- ・ 今後、**スマートホームサイバーフィジカルセキュリティ対策ガイドライン**を策定予定。

# 『第2層』タスクフォースの検討の方向性

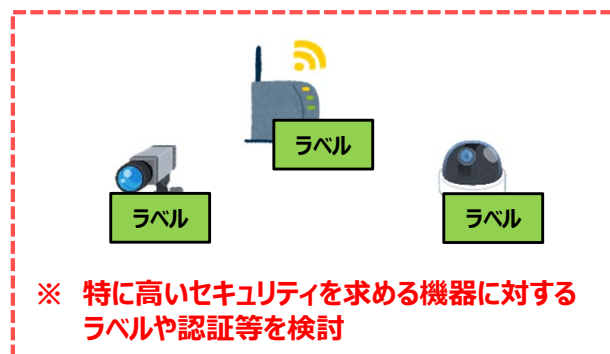
- 分野別のセキュリティ対策は、CPSFを基に、分野別SWGにおいて検討。その際、各分野の特性を踏まえて、**分野別ガイドラインにおいて第2層に求められる機能の要求を明確化**。
- 本タスクフォースは、分野別SWGの検討内容を分野横断SWGで横ぐしを通すべく、**業界の自主活動を含めたラベリングの仕組、認証制度の在り方等**を検討するとともに**機能安全・製品安全**も考慮したセキュリティ対策の在り方について検討。

## タスクフォースにおける検討内容イメージ

分野別ガイドラインにおいて機能の要求を明確化（各SWG）



① 業界の自主活動を含めたラベリングの仕組、認証制度の在り方等の検討



② 安全とサイバーリスクの一体化の進展への対応



# (参考) 米国ICT Supply Chain Risk Management Task Force の発足と重要インフラのセキュリティ対策に係る新たな政府機関設置の設置について

- 2018年10月30日、国土安全保障省（DHS）は**国家保護・プログラム局（NPPD）のサイバーサプライチェーンリスクマネジメント（C-SCRM）プログラム**の一つとして、**ICT Supply Chain Risk Management Task Force** を設置した。
- また、同年11月16日、NPPDを格上げする形で、DHS内部の独立機関として**サイバーセキュリティ・インフラストラクチャー・セキュリティ庁（CISA）** が設立された。

## ICT Supply Chain Risk Management Task Force について

- グローバルICTサプライチェーンのリスクを特定し管理するための共通の提案を検討し、展開するために形成された官民パートナーシップ。11月15日に初会合が行われた（共同議長：ITI, CTIA）。
- 民間企業からは、Verizon や AT&T のような主要ISP、Cisco、Palo Alto Networks 等のネットワーク機器会社、Samsung、Intel、FireEye、Microsoft 等が参加している。政府機関からは、DHS、国防総省（DoD）、商務省（DoC）、共通役務庁（GSA）等が参加している。

## CISAについて

- CISAの役割は米国の重要インフラに対する物理的脅威及びサイバー攻撃の脅威から守ること。

### <CISAの取組>

- 国家リスク管理センター（National Risk Management Center）による重要インフラに対するあらゆる危機に対するリスク分析を提供する。
- 緊急通信に関して、あらゆる政府レベルでの公共安全のための相互運用可能な通信の向上に取り組む。
- 自然災害、テロ、その他の人災に際して、緊急対応者及び関連する政府関係者の通信が継続できる能力の維持及び促進のために全土での連携に取り組む。

# 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（仮称）

# 【『ソフトウェア』タスクフォース設置の必要性】

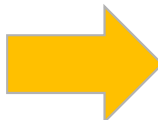
## ソフトウェア管理手法等の明確化

- 産業活動のサービス化の進展に伴い、産業における**ソフトウェアの重要性が増大**。企業においても**オープンソースソフトウェア（OSS）の活用**が進む中、安全なOSSの選定や、利活用するソフトウェアの脆弱性管理など、**ソフトウェアの利活用に起因するセキュリティリスク**が顕在化。
- 製品・サービスの安全・安心を確保するために、ソフトウェアの開発・管理・利活用にどのように取り組むかは大きな課題。

### <添付C> 対策要件に応じたセキュリティ対策例集

対策要件ID	対策要件	対策例	対策例を 実行する主体
CPS.SC-4	外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	<Basic> • … • 組織は、IoT機器やソフトウェアに含まれるIDや秘密鍵、電子証明書等を用いて調達した <b>機器が正規品であることを確認</b> する。	○
CPS.CM-7	自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が <b>必要な脆弱性の有無</b> を確認する。	• …	○

- **CPSFには、機器の正規品確認を目的としたソフトウェアの真正性の確認や、脆弱性の確認は記載されている。**
- **さらに、ソフトウェアの複雑化、OSSの利用拡大などに伴い、ソフトウェアそのもののセキュリティをどのように維持し続けるのか、それをどのように確認するかを定めることも必要。**



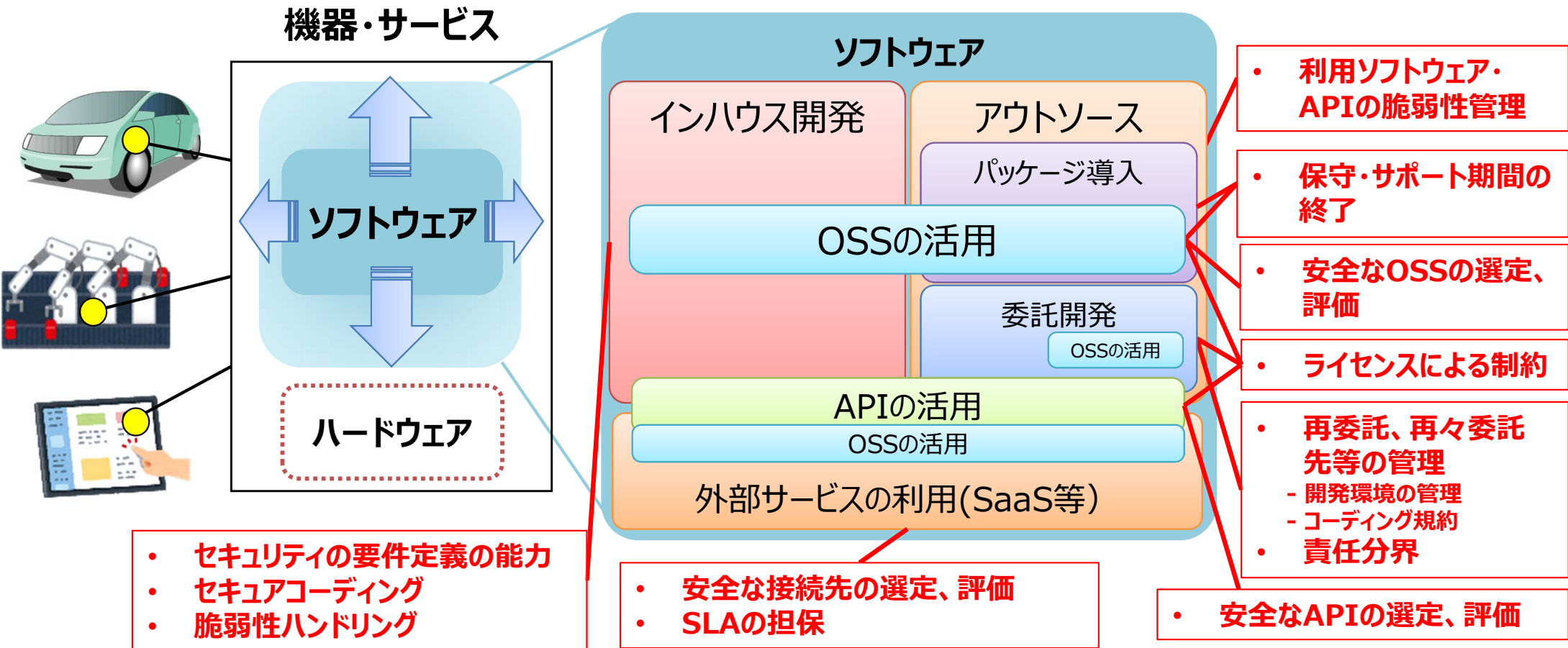
**ソフトウェアの開発・管理・利活用における具体的なセキュリティ対策について検討。**



# 『ソフトウェア』タスクフォースにおける検討の方向性

- 本タスクフォースにおいて、**米国NTIAのSoftware Component Transparencyの議論との連携を視野に入れながら、OSSを安全に活用するための手法、ソフトウェアの脆弱性管理手法等**を検討。

## ソフトウェアの利活用を巡る課題のイメージ



# (参考) 米国NTIA「Software Component Transparency」

- 2018年7月、米国NTIAにおいて、ソフトウェアの脆弱性情報の理解と処理、成長するIoTマーケットへの対処、安全なソフトウェア開発ライフサイクルの促進を議論する「Software Component Transparency」を立ち上げ。
- 中心的議題の1つが、SBOM (Software Bill of Material) である。

※ NTIA : 電気通信情報局は、米国商務省の局の一つで、情報通信にかかる助言、政策立案機能を担当。

## SBOM (Software Bill of Material)

ソフト部品構成表といえるもの。以下のイメージのように様々なソフトウェア部品の一覧とそのライセンス等で構成。

This document contains licenses and notices for open source software used in this product. With respect to the free/open source software listed in this document, if you have any questions or wish to receive a copy of any source code to which you may be entitled under the applicable free/open source license(s) (such as the GNU Lesser/General Public License), please contact us at external-opensource-requests@cisco.com.

In your requests please include the following reference number 78EE117C99-37892935

## Contents

- 1.1 #ziplib? (SharpZipLib) 0.83
  - 1.1.1 Available under license
- 1.2 ACE 5.3
  - 1.2.1 Available under license
- 1.3 ActiveMQ 5.3.1
  - 1.3.1 Available under license
- 1.4 AmazonS3 2011-01-22
  - 1.4.1 Available under license
- 1.5 ant 1.7.1
  - 1.5.1 Available under license

SBOMイメージ

## 4つのワーキンググループで活動

Understanding the Problem

SBOMの共有を含めて、「ソフトウェア透明性」の概念と課題の洗い出し。用語、課題の明確化、実装ガイドといった成果を想定。

Use Cases and State of Practice

SBOM活用に関する現在と将来のユースケース特定。現状での成功要因と課題を目指す。

Standards and Formats

ソフト開発に当たり利用される、外部のソフトウェア部品、共有ライブラリー、商用ソフトウェア、オープンソースについての現在の標準とイニシアチブの調査。

Healthcare Proof of Concept

SBOMフォーマット・プロトタイプ作成およびSBOM作成・活用ユースケース開発、利用方法確立等を、医療組織と医療デバイス製造業者で進める。

## 今後のWG 1 関連の体制

# 今後の体制（案）

## WG 1 制度・技術・標準化（サイバーセキュリティ課）

