経済産業省

# 経済産業省のSociety5.0における セキュリティ対策の取組

## ～サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）について～

令和２年２月１３日

経済産業省　商務情報政策局

サイバーセキュリティ課

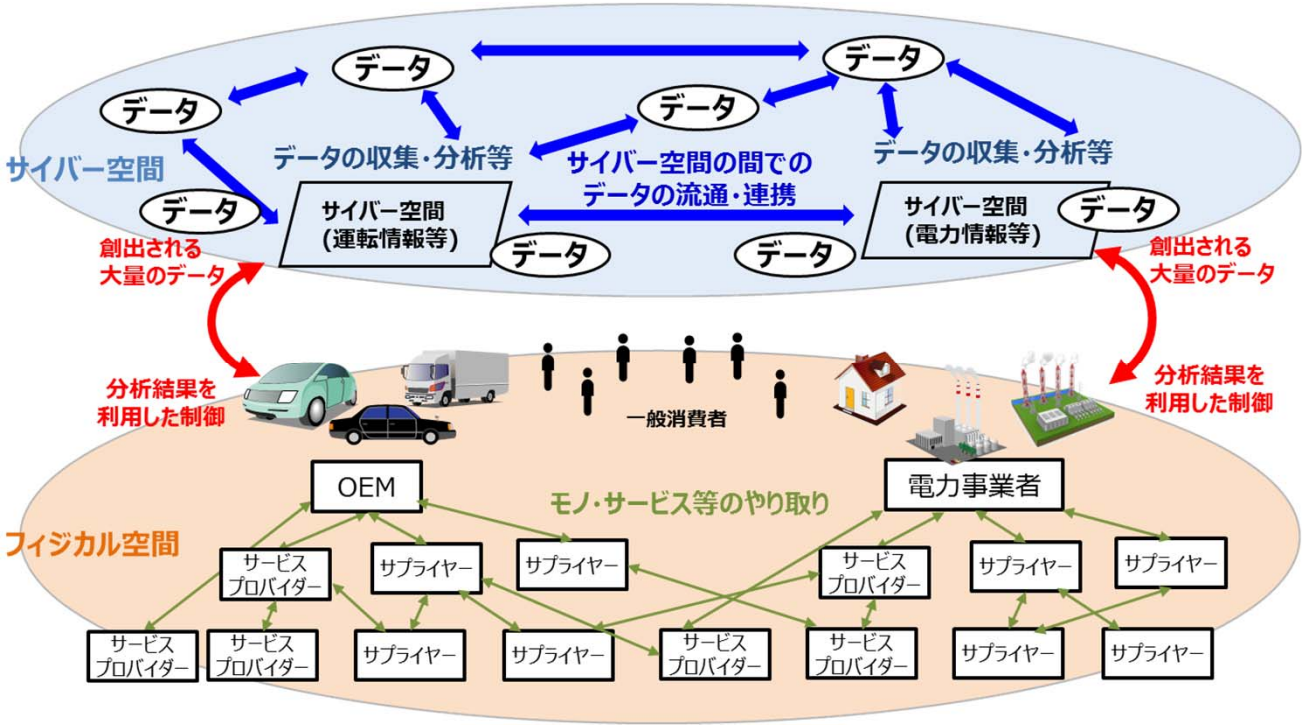
**1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）**

2. 産業分野別SWGの取組

3. 分野横断的TFの取組

# サイバー空間とフィジカル空間が高度に融合した「Society5.0」の到来

- 我が国では、**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超スマート社会**「Society5.0」**の実現を提唱。
- **「Society5.0」では、付加価値を創造するための一連の活動（サプライチェーン） の形態が、より柔軟で動的なものに変化。**この**新たな形のサプライチェーンを価値創造過程（バリュークリエイションプロセス）**と定義。
- 一方で、**サイバー空間とフィジカル空間の融合により、サイバー攻撃の脅威が増大。**




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

**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**

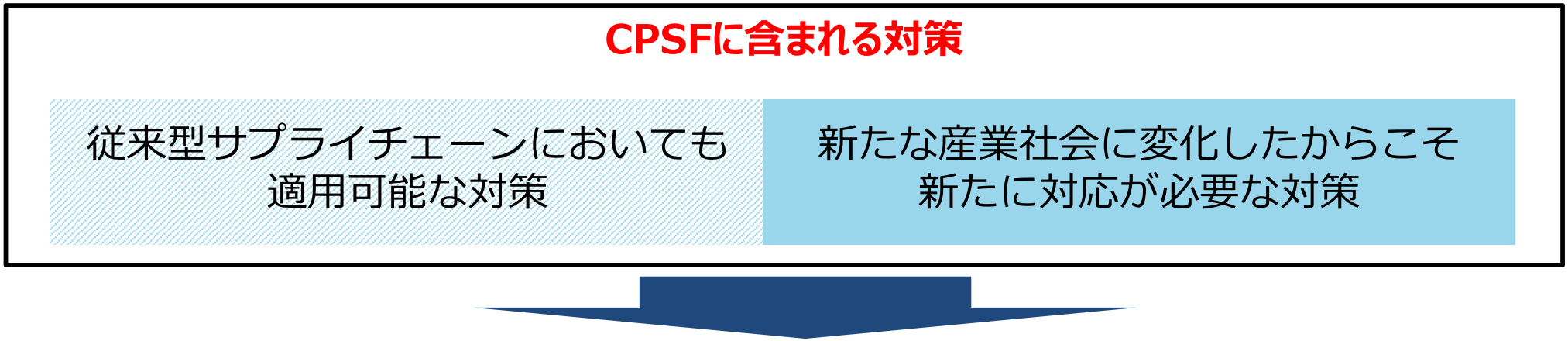
**フィジカル空間とサイバー空間の融合**
**⇒フィジカル空間までサイバー攻撃が到達**

**複雑につながるサプライチェーン**
**⇒影響範囲が拡大**

# 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）の目次

# 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）の目的と適用範囲

- 「Society5.0」の実現へ向けて、**産業構造、社会環境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、**バリュークリエイションプロセスのリスク源を適切に捉えるためのモデルを構築**し、求められる**セキュリティ対策の全体像を整理**するとともに、産業界が自らの対策に活用できる**セキュリティ対策例をまとめた、『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）』を策定する。**
- 本フレームワークは、**従来型サプライチェーンにおいても適用可能な対策に加え、新たな産業社会に変化したからこそ新たに対応が必要なものを整理**している。このため、それぞれの組織の状況に応じてセキュリティ対策を選定することが可能。




- **新たな産業社会における**バリュークリエイションプロセス全体が適用範囲
- それぞれの組織の状況に応じてセキュリティ対策を選定することが可能

# ”価値創造過程”（バリュークリエイションプロセス）への対応
## ～三層構造と６つの構成要素～

- 従来のサプライチェーンでは、セキュリティ対応をしっかりと行った主体間で行われる取引であれば、そのプロセス全体のセキュリティが確保される。
- 一方、「Society5.0」では、従来のサプライチェーンのように、**組織のマネジメントの信頼性にのみ基点を置くことでバリュークリエイションプロセスの信頼性を確保することは困難。**
- こうした、従来のサプライチェーンの活動範囲から拡張された付加価値を創造する活動のセキュリティ上のリスク源を的確に洗い出し、対処方針を示すためのモデルが必要。

**三層構造モデル**

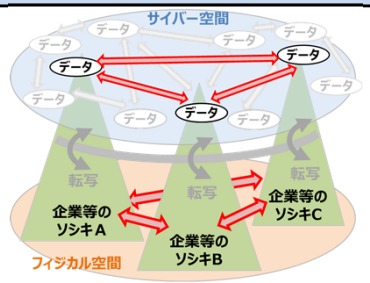
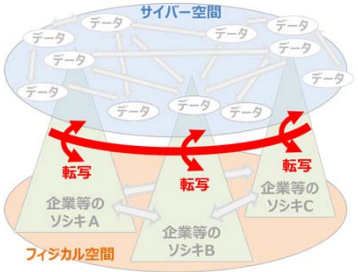
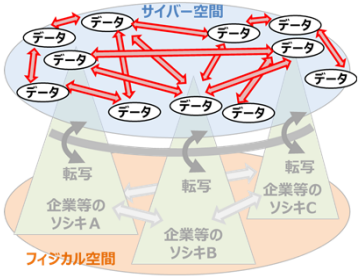
バリュークリエイションプロセスが発生する産業社会を、３つの「層」で整理。

**第1層：企業間のつながり**
**第2層：フィジカル空間とサイバー空間のつながり**
**第3層：サイバー空間におけるつながり**

**６つの構成要素**

バリュークリエイションプロセスに関与する構成要素を６つに整理。

**ソシキ、ヒト、モノ、データ、プロシージャ、システム**

| 三層構造 | 概念図 |
|---|---|
| 第1層 |  |
| 第2層 |  |
| 第3層 |  |

# 三層構造アプローチの意義

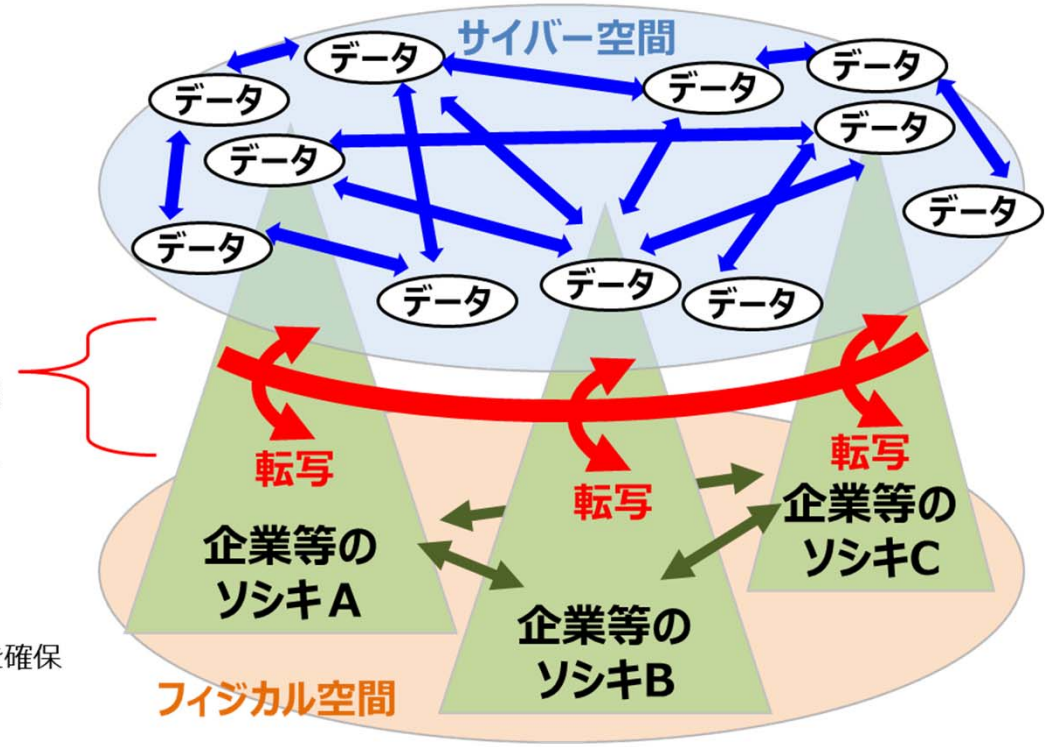
**～バリュークリエイションプロセスのセキュリティを確保するための信頼性の基点の設定～**

- **三層構造モデル**では、『Society5.0』における新たなサプライチェーン、**バリュークリエーションプロセスの信頼性の基点を的確に設定するために、産業社会を３つの「層」で整理。**
- 各層における信頼性の基点は以下のとおり。
  - **第１層**では、企業間のつながりにおける、**企業（組織）のマネジメントの信頼性**
  - **第２層**では、サイバー空間とフィジカル空間のつながりにおける、**要求される情報の正確性に応じて適切な正確さで情報が変換される“転写”機能の信頼性**
  - **第３層**では、サイバー空間のつながりにおける、**データの信頼性**

**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性を確保

**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“する機能の信頼性を確保
（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**
**【第１層】**
- 適切なマネジメントを基盤に各主体の信頼性を確保



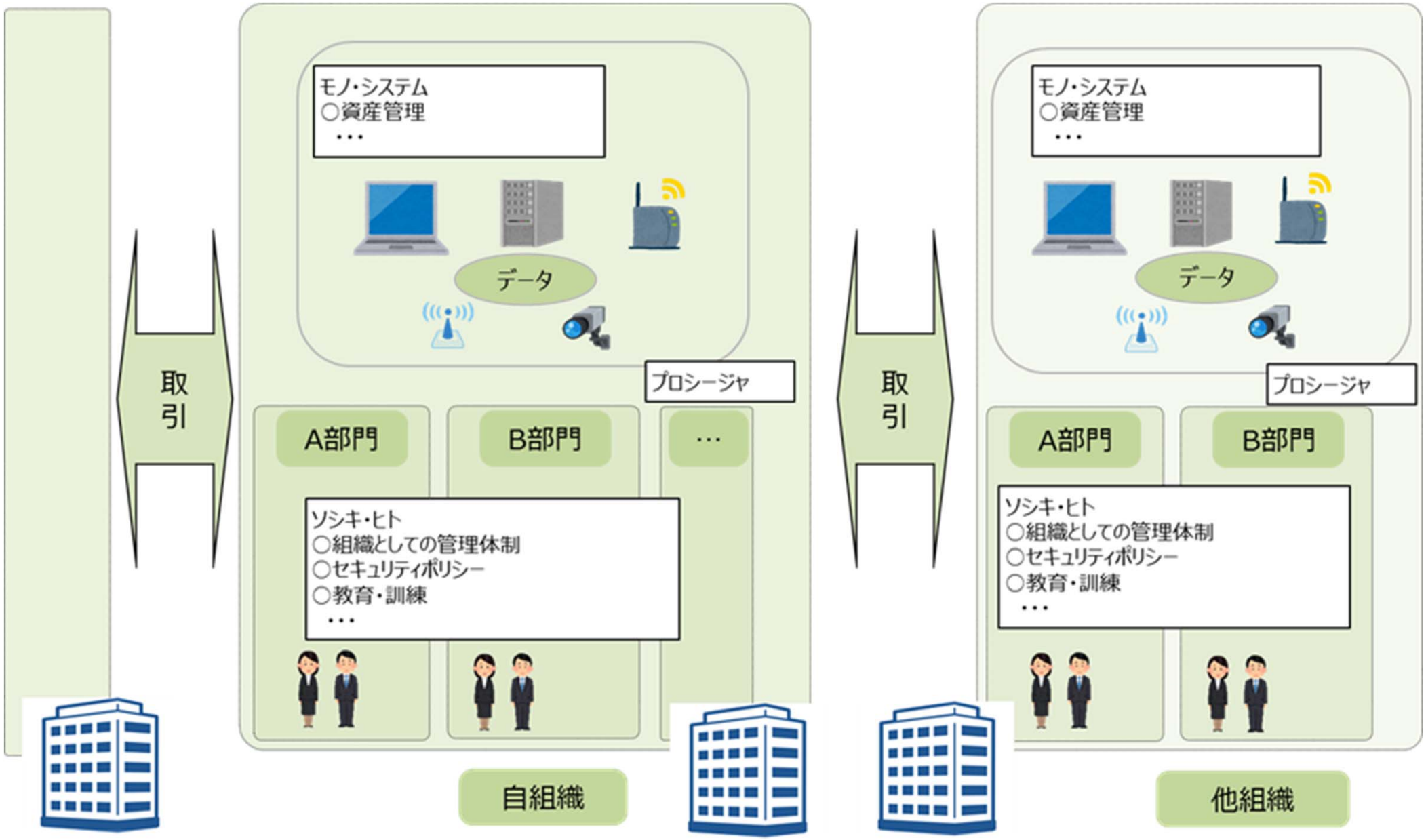
# ６つの構成要素

## ～動的で柔軟なバリュークリエイションプロセスを捉えるための構成要素～

- バリュークリエイションプロセスは、**動的に柔軟に構成されることから、資産を固定的に捉えることが難しく、構成要素について一定の抽象化を行って捉えることが必要。**
- このため、セキュリティ対策を講じる上で最適な最小単位として、**６つの構成要素で整理。**

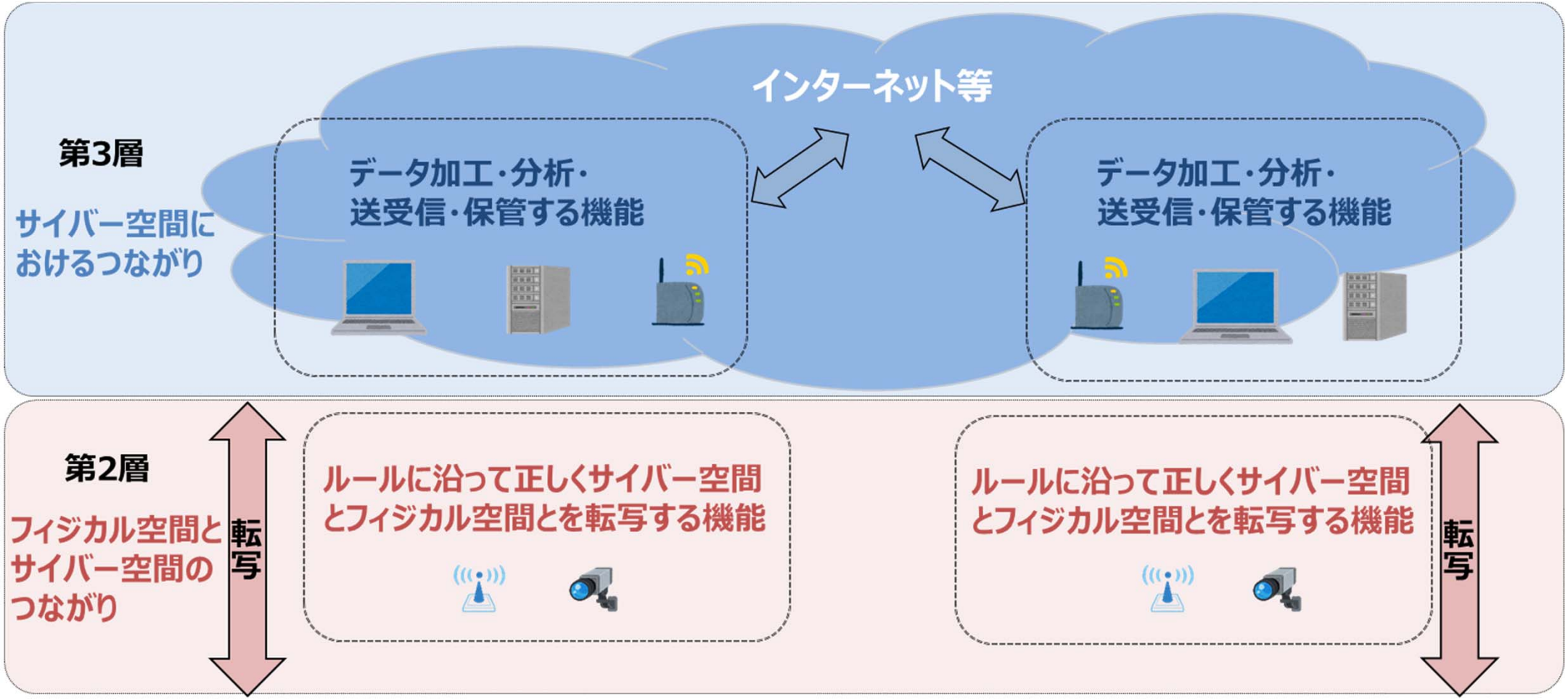
| 構成要素 | 定義 |
|---|---|
| **ソシキ** | • バリュークリエイションプロセスに参加する企業・団体・組織 |
| **ヒト** | • ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人 |
| **モノ** | • ハードウェア、ソフトウェア及びそれらの部品<br>操作する機器を含む |
| **データ** | • フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報 |
| **プロシージャ** | • 定義された目的を達成するための一連の活動の手続き |
| **システム** | • 目的を実現するためにモノで構成される仕組み・インフラ |

# 第1層の分析対象及び分析対象の具体的イメージ

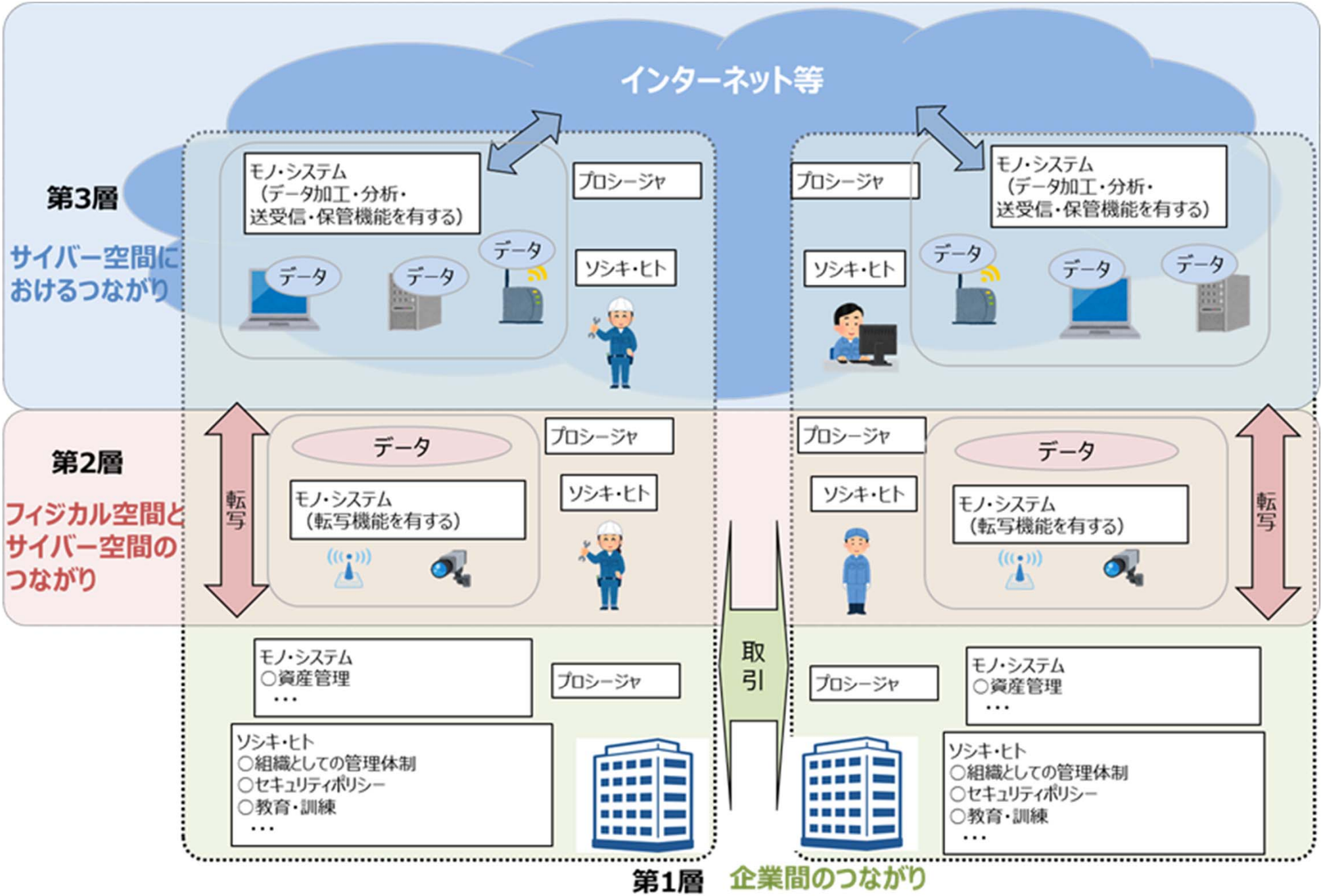



第1層 企業間のつながり

# 第2層及び第3層の機能・役割及び分析対象の具体的イメージ

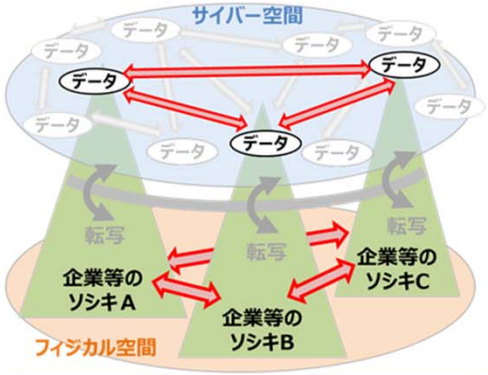
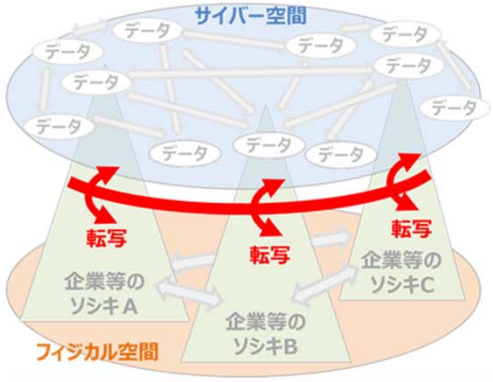
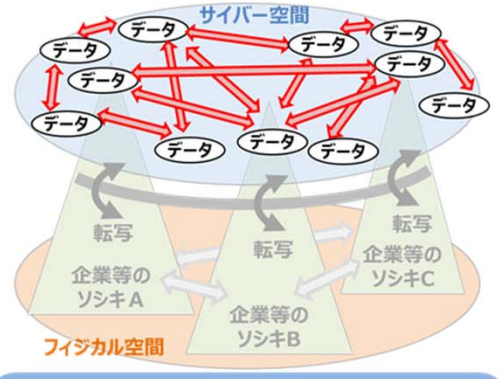


# 三層構造モデルと6つの構成要素を活用した分析対象の具体的イメージ



# CPSFの全体概要（リスク源と対応する方針の整理）

- 各層における機能、セキュリティインシデント、リスク源、対策要件を整理。

| | 企業間のつながり【第１層】 | フィジカル空間とサイバー空間のつながり【第２層】 | サイバー空間におけるつながり【第３層】 |
|---|---|---|---|
| 新たなサプライチェーン構造の整理 |  |  |  |
| 機能（守るべきもの） | • 平時及び緊急時のリスク管理・対応体制の構築と運用<br>• 企業内及び企業間のリスク管理・対応体制の構築と運用 | • フィジカル空間とサイバー空間の境界における情報の正確な転写 | • データの加工・分析<br>• データの保管<br>• データの送受信 |
| セキュリティインシデント | • 保護すべき資産の棄損<br>• 他組織のセキュリティ事象発生に起因する事業停止 | • 不正確なデータの送信<br>• 安全に支障をきたす動作 | • 保護すべきデータの漏えい<br>• なりすまし等による不正な組織からのデータ受信 |
| リスク源（構成要素ごとに整理） | • セキュリティリスクに対するガバナンスの欠如<br>• 他組織との連携状況の未把握 | • 不正なIoT機器との接続<br>• 許容範囲外の入力データ | • 通信経路が保護されていない<br>• 通信相手を識別していない |
| 対策要件 | ■ マネジメントルールの徹底<br>■ 関係者との役割分担 | ■ 接続相手の認証<br>■ 安全なIoT機器の導入 | ■ 暗号化によるデータ保護<br>■ データの提供者の信頼性確認 |

# リスク分析・リスク対応の実施（添付Ｂの活用）

- 添付Bでは、**抽出したセキュリティインシデントに対して**、当該インシデントの発生を助長、あるいは発生した**インシデントの被害を拡大させる可能性がある脅威及び典型的な脆弱性を整理。**
- 脆弱性を**6つの構成要素で捉えることで、新たなサプライチェーンにおけるリスク源の洗い出しへ対応可能。**実際のリスク分析を実施する際にも、検討するリスク源の抽出及び過不足のチェック等に活用可能。
- 添付Ｂには、さらに対応するセキュリティ対策要件も整理。**リスク対応として低減を実施する場合は、これらを参照することで対策要件の選択が可能。**

**<添付B>　リスク源と対策要件の対応関係**

| 機能 | 想定されるセキュリティインシデント | リスク源 | | | 対策要件 | 対策要件ID |
|---|---|---|---|---|---|---|
| | | 脅威 | 脆弱性ID | 脆弱性 | | |
| 下記すべてに関わる<br>• データを加工・分析する機能<br>• データを保管する機能<br>• データを送受信する機能 | サービス拒否攻撃により、関係する他組織における自組織のデータを取り扱うシステムが停止する | システムを構成するサーバ等の電算機器、通信機器等に対するDoS攻撃 | L3_3_b_ORG | **[ソシキ]**<br>・データの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない | サービスやシステムの運用において、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する | CPS.SC-2 |

**脆弱性は、６つの構成要素別に記載。**

**対策要件IDで添付Cの詳細な対策例を参照可能。**

# 対策要件及び対策例集を活用したリスク対応

- 添付Ｃでは、添付Ｂで示した対策要件を**NIST Cybersecurity Frameworkを参考にカテゴリー分けを行い整列**（次スライド参照）。更に、各対策要件について、**具体的な参考となる対策例を記載。**
- 企業等はリスクアセスメントの結果に応じて、第Ⅲ部に記載された対策要件および、**添付Cに記載されたセキュリティ対策例**を実装し、リスクマネジメントプロセスを適切に実施することで、自組織のセキュリティマネジメントを改善することが可能。

**＜添付Ｃ＞　対策要件に応じたセキュリティ対策例集**

他の国際規格等との対応関係。（説明後掲）

添付Bの脆弱性に対応。

| 対策要件ID | 対策要件 | 対応する脆弱性ID | 対策例 | 対策例を実行する主体 | NIST SP800-171 | NIST SP800-53 | ISO/IEC 27001 付属書A |
|---|---|---|---|---|---|---|---|
| CPS.AM-1 | ・・・ | L1_1_a_COM<br>L1_1_b_COM<br>L1_1_c_COM<br>L2_1_a_ORG<br>L2_3_b_ORG | <H-Advanced><br>・・・ | O/S | ○ | ○ | ― |
| | | | <Advanced><br>・・・ | O/S | ○ | ○ | ○ |
| | | | <Basic><br>・・・ | O | | | |

・添付Bの対策要件をNIST CSFを参考に整列。
・対象要件IDで添付Bの記載へ参照が可能。

対策例は３つのレベルに分けて記載。
High Advanced, Advanced, Basic

対策例を実施する主体を記載。
S:　システムに実装される対策
O:　組織に実装される対策

# （参考）対策要件のカテゴリーの考え方

- 対策要件のカテゴリーは、**NIST Cybersecurity Framework に対応**する形で整理。

| カテゴリー名称 | 略称 | NIST Cybersecurity Framework v1.1 の対応カテゴリー |
|---|---|---|
| 資産管理 | CPS.AM | ID.AM (Asset Management) |
| ビジネス環境 | CPS.BE | ID.BE (Business Environment) |
| ガバナンス | CPS.GV | ID.GV (Governance) |
| リスク評価 | CPS.RA | ID.RA (Risk Assessment) |
| リスク管理戦略 | CPS.RM | ID.RM (Risk Management Strategy) |
| サプライチェーンリスク管理 | CPS.SC | ID.SC (Supply Chain Risk Management) |
| アイデンティティ管理、認証及びアクセス制御 | CPS.AC | PR.AC (Identity Management and Access Control) |
| 意識向上およびトレーニング | CPS.AT | PR.AT (Awareness and Training) |
| データセキュリティ | CPS.DS | PR.DS (Data Security) |
| 情報を保護するためのプロセスおよび手順 | CPS.IP | PR.IP (Information Protection Processes and Procedures) |
| 保守 | CPS.MA | PR.MA (Maintenance) |
| 保護技術 | CPS.PT | PR.PT (Protective Technology) |
| 異変とイベント | CPS.AE | DE.AE (Anomalies and Events) |
| セキュリティの継続的なモニタリング | CPS.CM | DE.CM (Security Continuous Monitoring) |
| 検知プロセス | CPS.DP | DE.DP (Detection Processes) |
| 対応計画 | CPS.RP | RS.RP (Response Planning)<br>RC.RP (Recovery Planning) |
| 伝達 | CPS.CO | RS.CO (Communications)<br>RC.CO (Communications) |
| 分析 | CPS.AN | RS.AN (Analysis) |
| 低減 | CPS.MI | RS.MI (Mitigation) |
| 改善 | CPS.IM | RS.IM (Improvements)<br>RC.IM (Improvements) |

# CPSFにおける他の国際規格等との対応関係

- 第Ⅲ部、添付C及び添付Dにおいて、主要な国際規格等との対応関係を記載。
- NIST Cybersecurity Framework、NIST SP800-171、ISO/IEC 27001付属書Aについては、**各規格等から見た場合の対応関係も整理。**

**<添付C> CPSF ⇒ 他の国際規格等**

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | NIST SP800-171 | NIST SP800-53 | ISO/IEC 27001 付属書A |
|---|---|---|---|---|---|---|---|
| CPS.AM-1 | ・・・ | L1_1_a_COM,<br>L1_1_b_COM,<br>・・・ | <H.Advanced><br>・・・ | O/S | ○ | ○ | ― |
| | | | <Advanced><br>・・・ | O/S | ○ | ○ | ○ |

**<添付D> 他の国際規格等 ⇒ CPSF**

| NIST Cyberseucurity Framework v1.1 | | | サイバー・フィジカル・セキュリティ対策フレームワーク | |
|---|---|---|---|---|
| 機能 | サブカテゴリID | サブカテゴリ | 対策要件ID | 対策要件 |
| 特定(ID) | AM-1 | ・・・ | CPS.AM-1 | ・・・ |

| NIST SP 800-171 | | | NIST SP800-171 から参照される NIST SP800-53 | サイバー・フィジカル・セキュリティ対策フレームワーク | | |
|---|---|---|---|---|---|---|
| ファミリ | 管理策ID | 要求事項 | 管理策名称 | 対策要件ID | 対策要件 | 対策例 |
| アクセス制御 | 3.1.1 | ・・・ | ・AC-2 アカウント管理<br>・・・ | CPS.AC-9 | ・・・ | ・・・ |

| ISO/IEC 27001:2013 附属書A | | サイバー・フィジカル・セキュリティ対策フレームワーク | | |
|---|---|---|---|---|
| 管理策ID | 要求事項 | 対策要件ID | 対策要件 | 対策例 |
| A.5.1.1 | ・・・ | CPS.BE-2 | ・・・ | ・・・ |

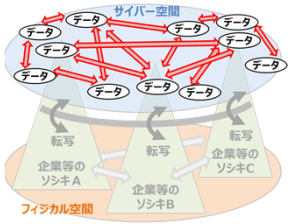
1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

**2. 産業分野別SWGの取組**

3. 分野横断的TFの取組

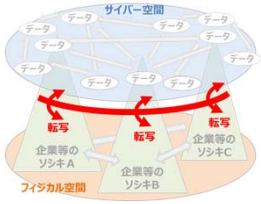
# CPSFに基づく具体化・実装の推進の全体像

【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

**実際の産業活動の内容**

**具体的な対策手法やルールの明確化**

**データを介した連携を行う産業活動**
（分野間の連携 等）

**データの信頼性**
(データの完全性、真正性等の確認　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

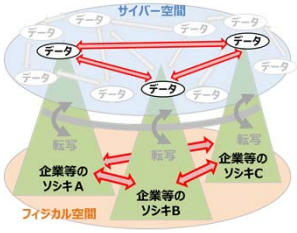
**規模別の産業活動**
- 大企業
- 中小企業 等

**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に関するルール・管理手法**
- Software component transparency 等

【第1層】

企業間のつながり




**産業サイバーセキュリティ研究会WG 1**

標準モデル（CPSF）

- ビルSWG
- 電力SWG
- 防衛産業SWG
- 自動車産業SWG
- スマートホームSWG
- ・・・

**分野横断SWG**

**『第3層』TF (⇒ データ区分に応じて適切なセキュリティ対策要件 等)**

**ソフトウェア TF （⇒ OSSを含むソフトウェア管理手法 等)**

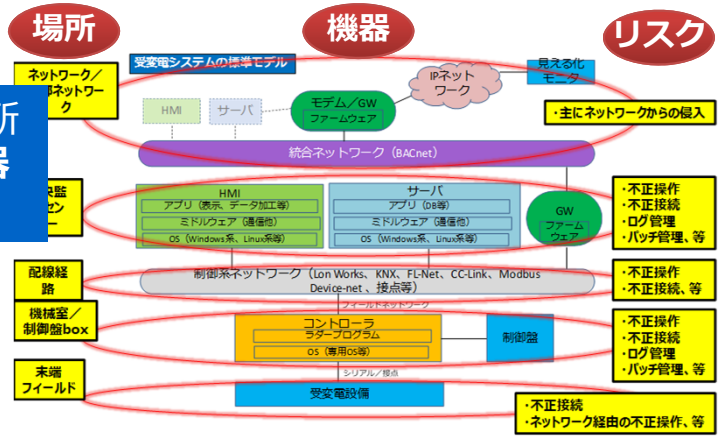
**『第2層』TF (⇒ 機器毎のラベリング・認証の在り方、安全との一体化への対応 等)**

# （参考）ビルSWG（座長：江崎 浩 東京大学 教授）

- 産業サイバーセキュリティ研究会WG1（制度・技術・標準化）の下の**ビルSWG（ビルオーナー～ベンダまで、ビル関連のステークホルダが参加）**において、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**ガイドラインを作成。2019年6月17日付で第1版を公開。**

- **場所→場所に置かれる機器→機器に想定されるリスク→対策要件→ライフサイクル別の対応策という流れで整理**

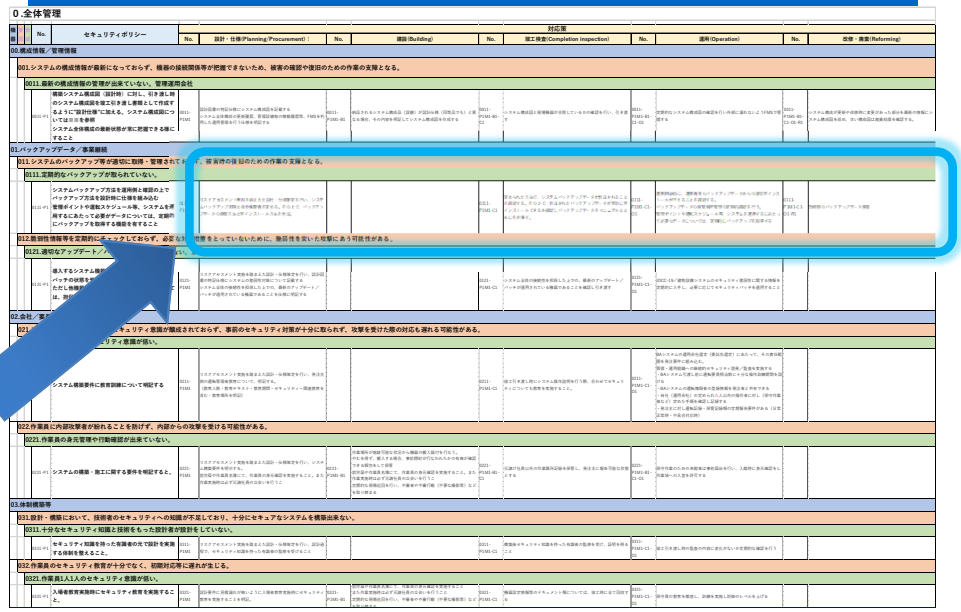
**場所**及びその場所に設置される**機器等**をリストアップ




| | | |
|---|---|---|
| 4.1 全体管理 | | |
| 2. | バックアップ データ／事業継続 | |
| 3. | 会社／要員の管理 | |
| 4. | 体制構築等 | |
| 4.2 機器 | | |
| 1. | ネットワーク(クラウド、情報系NW、BACnet) | |
| | 10 | ネットワーク |
| | 11 | クラウドサーバ/Webサーバ |
| | 12 | 情報系端末 |
| | 13 | 外部接続用ネットワーク機器（FW、ルータ） |
| | 14 | ビルシステム間相互接続 |
| 2. | 防災センター（中央監視室） | |
| | 20 | 防災センター（中央監視室） |
| | 21 | HMI/HIM |
| | 22 | 保守用持ち 込み端末 |
| | 23 | 統合NWにつながるネットワーク機器（FW、ルータ、SW） |
| | 24 | システム管理用サーバ（ビルシステム主装置） |
| 3. | 機械室／制御盤ボックス | |
| | 30 | 機械室 |
| | 31 | コントローラ（DDC、PLC等） |
| | 32 | ネットワーク機器（FW、ルータ、SW） |
| | 33 | ゲートウェイ 機器 |
| | 34 | 各種制御盤・分電盤 |
| 4. | 配線経路（MDF室、EPS、天井裏ラック） | |
| | 40 | MDF室／EPS／天井裏ラック |
| | 41 | 内部に置かれたネットワーク機器（SW類） |
| 5. | 末端装置が置かれる場所 | |
| | 50 | 末端装置 |

| | セキュリティインシデント | リスク源 | セキュリティポリシー |
|---|---|---|---|
| 1．構成情報／管理情報 | | | |
| (1) | ビルシステムへの被害発生時に、被害確認が遅れ、復旧作業の支障となる。 | ビルの構成情報が最新状態に管理できておらず、機器の最新の接続関係が把握できない。 | ・構築システム構成図（設計時）に対し、引き渡し時のシステム構成図を竣工引き渡し書類として作成するように"設計仕様"に加える。<br>・システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。 |
| 2．バックアップデータ／事業継続 | | | |
| (1) | 適切なバックアップデータが発生時に復旧作業の支障となる。 | バックアップが取られていない、またはバックアップの範囲や対象が適切ではない。 | ・システムバックアップ方法を運用側と確認の上でバックアップ方法を設計時に仕様化組み込む。<br>・管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する機能を具備する。 |
| (2) | システムの脆弱性をついた攻撃を受ける。 | 脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっている。 | ・既知の脆弱性に対して必要な対策（パッ<br>理する。<br>・ただし、他機器および他システムの正常稼動については、担保しなければならない。 |
| 3．会社／要員の管理 | | | |
| (1) | ビルシステムへの被害発生時に、迅速な対応ができず、被害が拡大する。 | ビル管理会社においてセキュリティへの意識醸成、要員教育が十分ではなく、事前 対策や対応 準備が出来ていない。 | ・システム構築要件に教 育訓練について明記する。 |
| (2) | ビルシステムが内部作業員等から攻撃を受ける。 | 作業員 等の 身元確認や行動監視が不十分で、内部攻撃者が紛れることや攻 撃を行うことを防ぐことが出来ていない。 | ・システムの構築・施工・保守にあたって、作業員等の身元確認や行動確認についての要件を明記する。 |
| 4．体制構築等 | | | |
| (1) | 攻撃等への対応 が効果的に出来ず、被害が拡大する。 | 十分なリスクアセスメントが出来ていないため、リスク対応の運用計画や体制が十 分なレベルで構築できていない。 | ・リスクアセスメントを実施し、その結果を基に監理監査 面からの「運用する管理体系」などを運用計画として 定義・整備する。 |

ビルシステムの**ライフサイクルの各フェーズ毎に対策**を展開



**場所・機器別**の想定される**インシデント**と**リスク源**を整理し、その**対策をポリシーレベル**で整理

# （参考）スマートホームSWG（JEITA スマートホームサイバーセキュリティWG）

- Society5.0の実現を目指し、IT・エレクトロニクス企業のみならず、人々の暮らしに関わる様々なメンバーが、それぞれの知見を結集して、スマートホームのセキュリティ対策の検討を実施。
- マネジメント不在といった**スマートホーム特有の脅威や、製品安全の観点も含めたスマートホーム分野のセキュリティガイドラインを整備する**とともに、運用のあり方についてまとめていく。

＜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（戸建て／マンション）・住宅設備分野、電機・通信分野、医療分野、研究機関

経済産業省

**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）**

**フレームワークと整合**

①三層構造アプローチ
②リスクベース
③国際標準との調和

＋

**スマートホーム特有の脅威を加味**

①膨大な対象
②マネジメント不在
③利用者による想定外の事象

JEITA 一般社団法人 電子情報技術産業協会

**スマートホーム実現に向けた サイバーフィジカルセキュリティ対策ガイドライン**

- 定義と説明
  - スマートホームの定義
  - スマートホームを取り巻く環境や状況の変化
  - サイバー攻撃の事例
- スマートホームの住まい手である生活者に向けて
  - 機器やサービスの導入時のリスク
  - 機器やサービスの利用時のリスク
  - 機器やサービスの解約時・機器廃棄時のリスク
  - 利用シーンごとの対策と確認内容の例
- スマートホームを構成する機器やサービスの開発者、提供者に向けて
  - 製品とサービスのライフサイクル全体におけるセキュリティレベルの維持
    - 開発時に考慮を必要とする内容
    - 利用中の製品とサービスにおけるリスクと対策
    - サービス解約や機器廃棄時のリスクとその対策
  - 製品とサービスのサポート停止以降のセキュリティレベルの維持
- ユースケース
- リスク・対策・セキュリティ要件の例
- 国際規格等の各種規格との対応

**2019年度内の策定を目指す**


- **Society5.0社会の基盤となるスマートホーム**は、社会インフラや様々な産業、サービスが結節した、住まい手中心のバリュークリエイションプロセスにより構成
- 住まい手の**セキュリティをバリュークリエイションプロセス全体で確保**

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（CPSF）

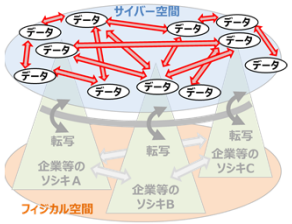
2. 産業分野別SWGの取組

**3. 分野横断的TFの取組**

# CPSFに基づく具体化・実装の推進の全体像

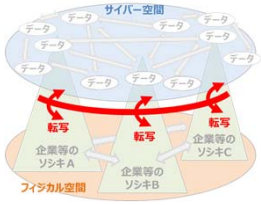
再掲

【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

**実際の産業活動の内容**

**具体的な対策手法やルールの明確化**

**データを介した連携を行う産業活動**
（分野間の連携 等）

**データの信頼性**
(データの完全性、真正性等の確認　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

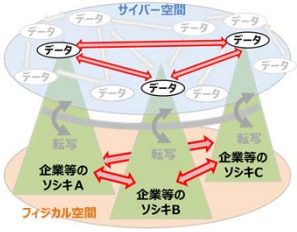
**規模別の産業活動**
- 大企業
- 中小企業 等

**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に関するルール・管理手法**
- Software component transparency 等

【第1層】

企業間のつながり




**産業サイバーセキュリティ研究会WG 1**

標準モデル（CPSF）

- ビルSWG
- 電力SWG
- 防衛産業SWG
- 自動車産業SWG
- スマートホームSWG
- ・・・

**分野横断SWG**

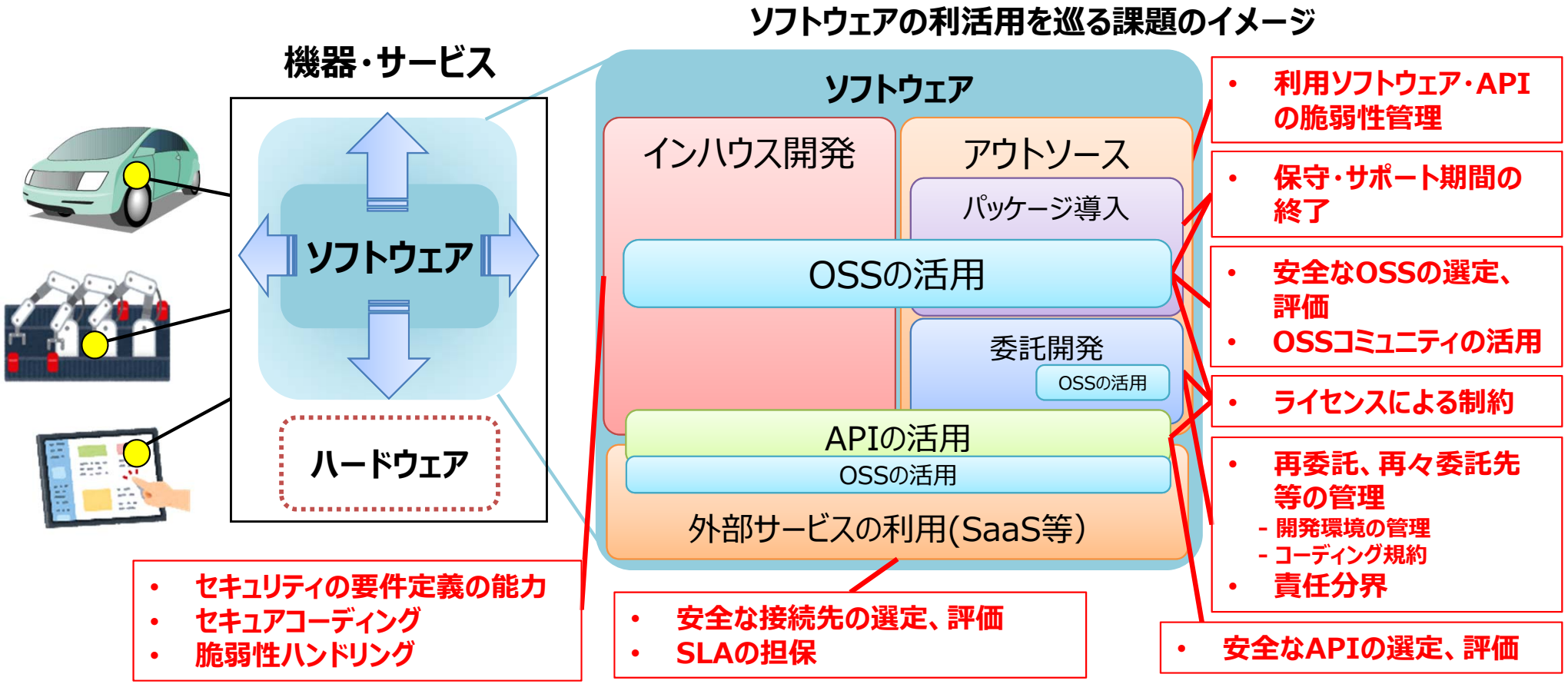
**『第3層』TF (⇒ データ区分に応じて適切なセキュリティ対策要件 等)**

**ソフトウェア TF （⇒ OSSを含むソフトウェア管理手法 等)**

**『第2層』TF (⇒ 機器毎のラベリング・認証の在り方、安全との一体化への対応 等)**

# 『ソフトウェアTF』の検討の方向性　　第１回9/5、第2回11/6、第3回12/4

- 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TF』における検討の方向性

- **ソフトウェア管理手法、脆弱性対応、OSSの利活用等**に関する検討を行う。

## ソフトウェア管理手法の検討

- ソフトウェアの開発から、運用中の脆弱性発見まで
- 構成管理・脆弱性管理に求められるソフトウェア管理手法のあり方
- SBOM等ソフトウェア管理スキームの活用に求められる技術面・制度面の課題

第1回 9/5
検討事項

## 脆弱性対応手法の検討

- 脆弱性が発見された場合のソフトウェアへの対応
- 脆弱性発覚時に必要な脆弱性への対応手法・体制のあり方
- 運用中システムへの脆弱性対応に求められる技術面・制度面の課題

第2回 11/6
検討事項

## OSSを利活用する際のビジネス的な側面の検討

・OSS利用に関連するライセンスや契約
・OSS活用のベストプラクティス／OSSコミュニティへの発信

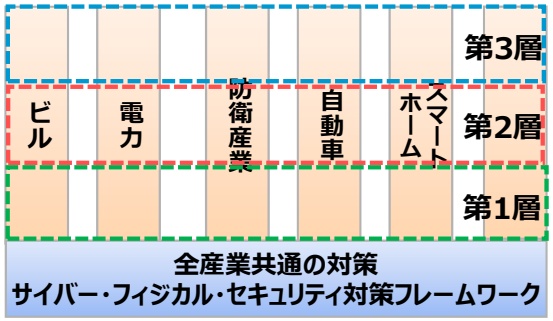
第3回 12/4
検討事項

# 『第2層TF』の検討の方向

第１回8/2 、第2回11/27

- 本タスクフォースでは、諸外国の動向も踏まえながら、サイバー・フィジカル間の**転写機能を持つ機器について、ユーザのリスクや社会に与える被害を考慮した信頼性確保に求められる要件**を整理。
- その整理を踏まえた上で、分野別SWGの検討内容に横串を通すべく、**業界の自主活動を含めた自己適合宣言・認証等の確認の在り方等**を検討するとともに、**産業保安・製品安全も考慮したセキュリティ対策の在り方**について検討を行う。

**分野別ガイドラインにおいて機能の要求を明確化（各SWG）**

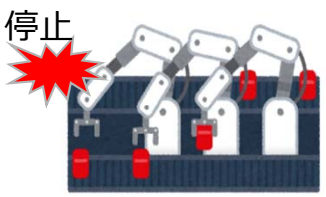



**タスクフォースにおける検討内容イメージ**

**① 業界の自主活動を含めた自己適合宣言・認証等の確認の在り方等の検討**

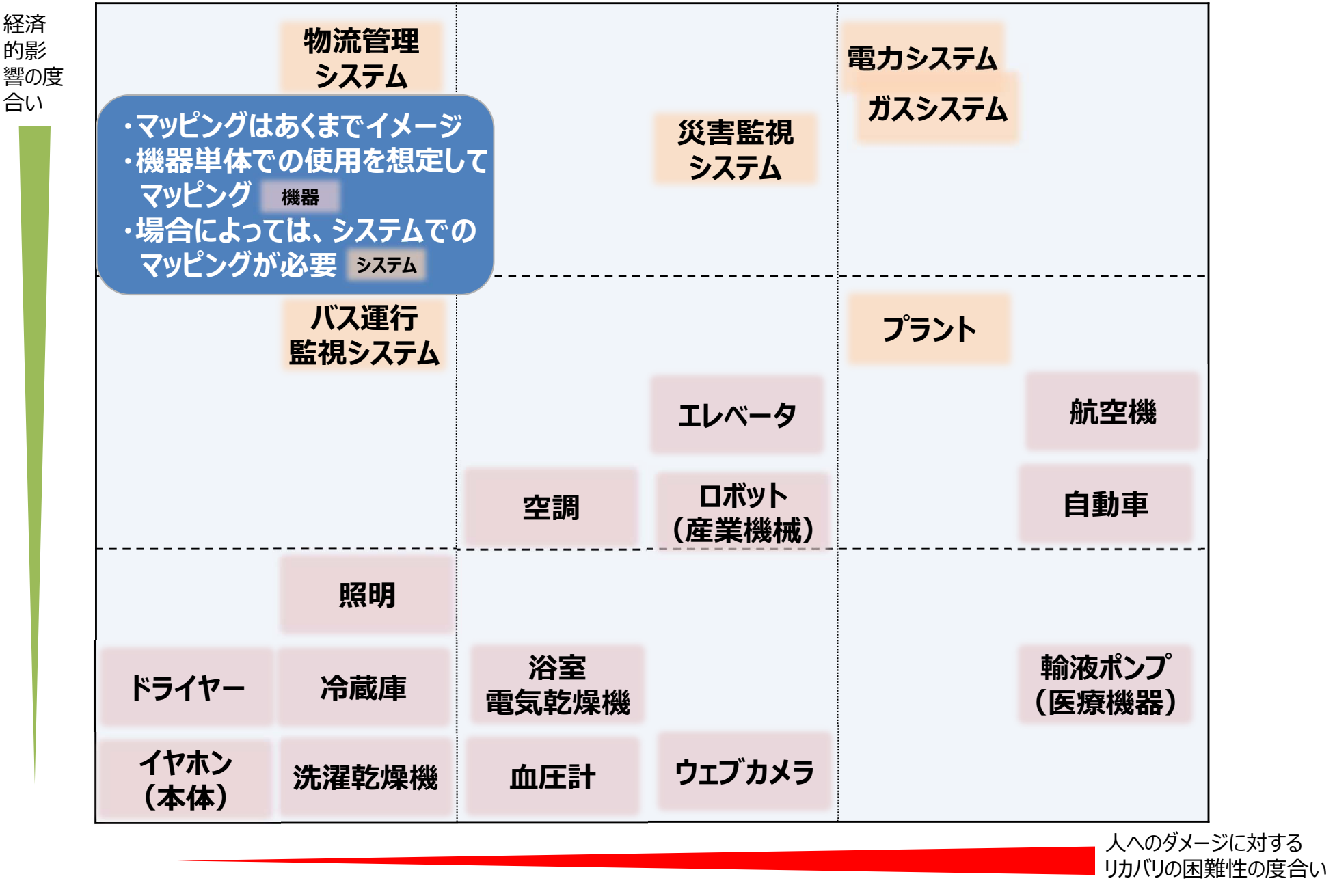
※ 特に高いセキュリティを求める機器に対する要件等を検討

**② サイバーリスクの安全への影響の増大への対応**

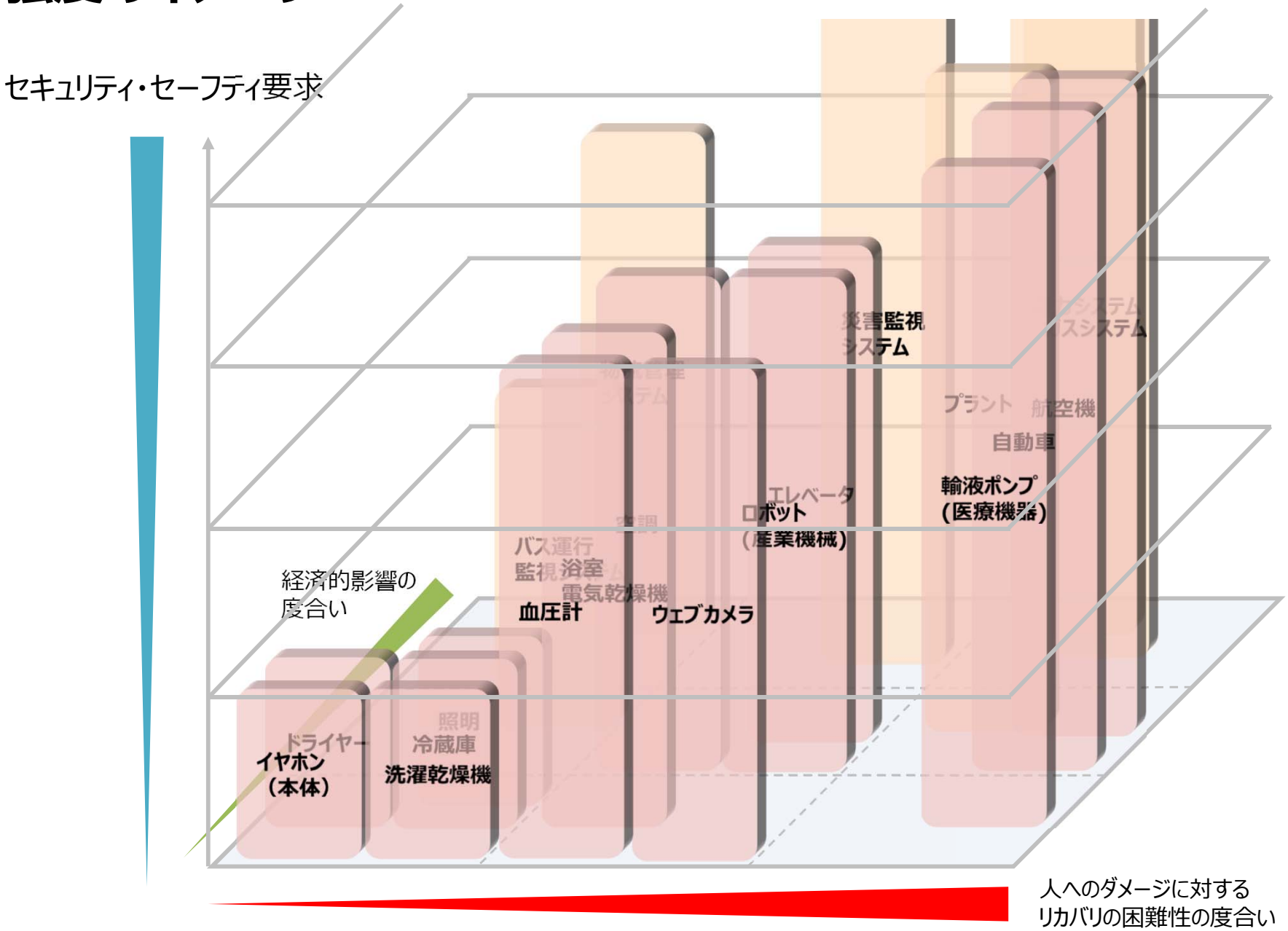



※ 安全も考慮に入れたセキュリティ対策等について検討

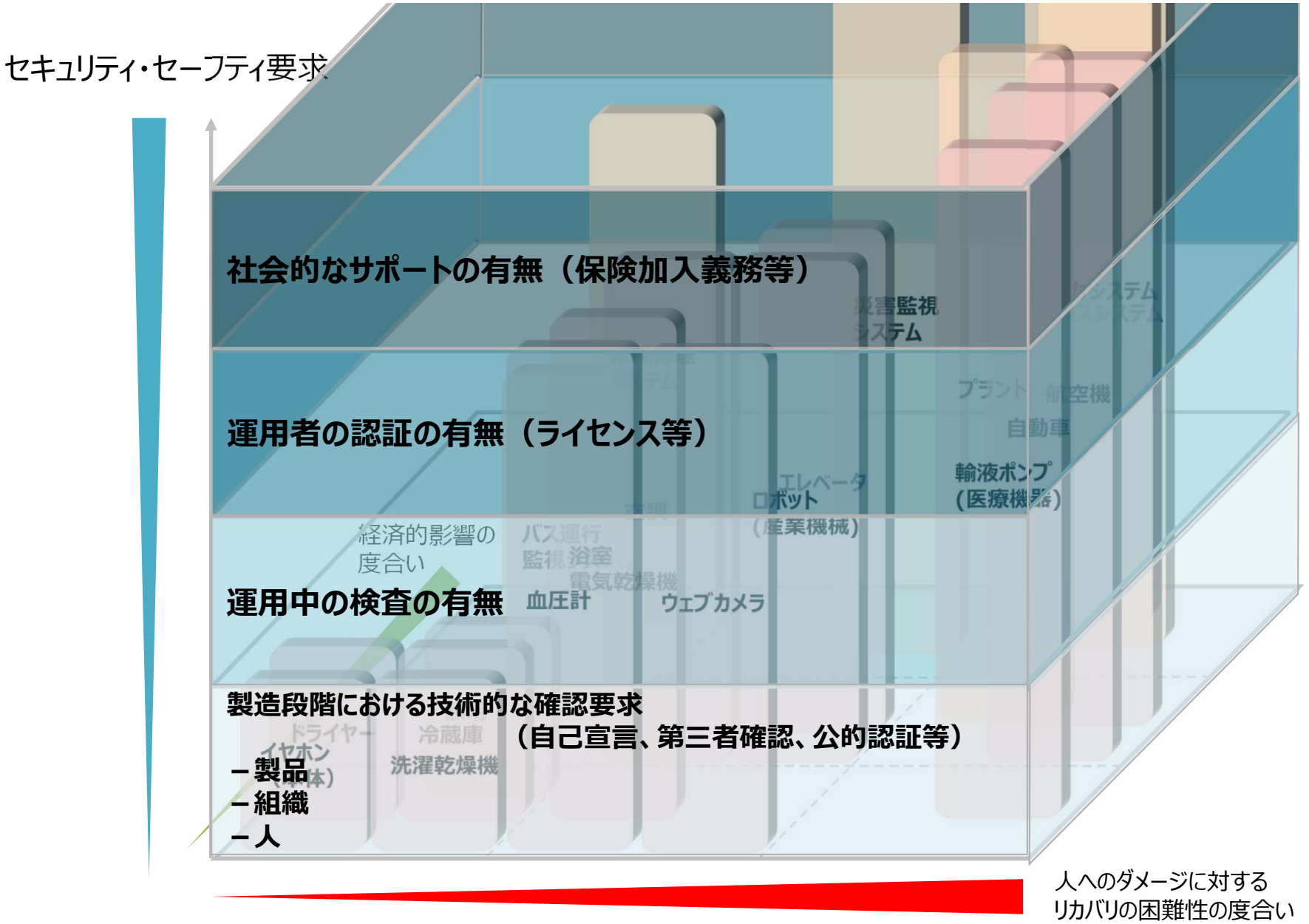
# 『第2層TF』サイバー・フィジカル間をつなげる機器・システムに潜むリスクのイメージ



# 『第2層TF』カテゴリに応じて求められるセキュリティ・セーフティ要求の強度のイメージ



# 『第2層TF』カテゴリに応じて求められるセキュリティ・セーフティ要求の強度のイメージ



# 『第3層TF』の検討の方向性

第１回7/31、第2回12/17

- 本タスクフォースにおいて、データの信頼性確保のために、「**データの区分に応じた適切なセキュリティ対策要件**」及び「**データの信頼性の確認手法**」を検討。

データの区分に応じた適切なセキュリティ対策要件の検討

**データをセキュアに管理すること**
**⇒マネジメント、プロセス、セキュリティポリシー、システム要件等のセキュリティ要件の明確化など**

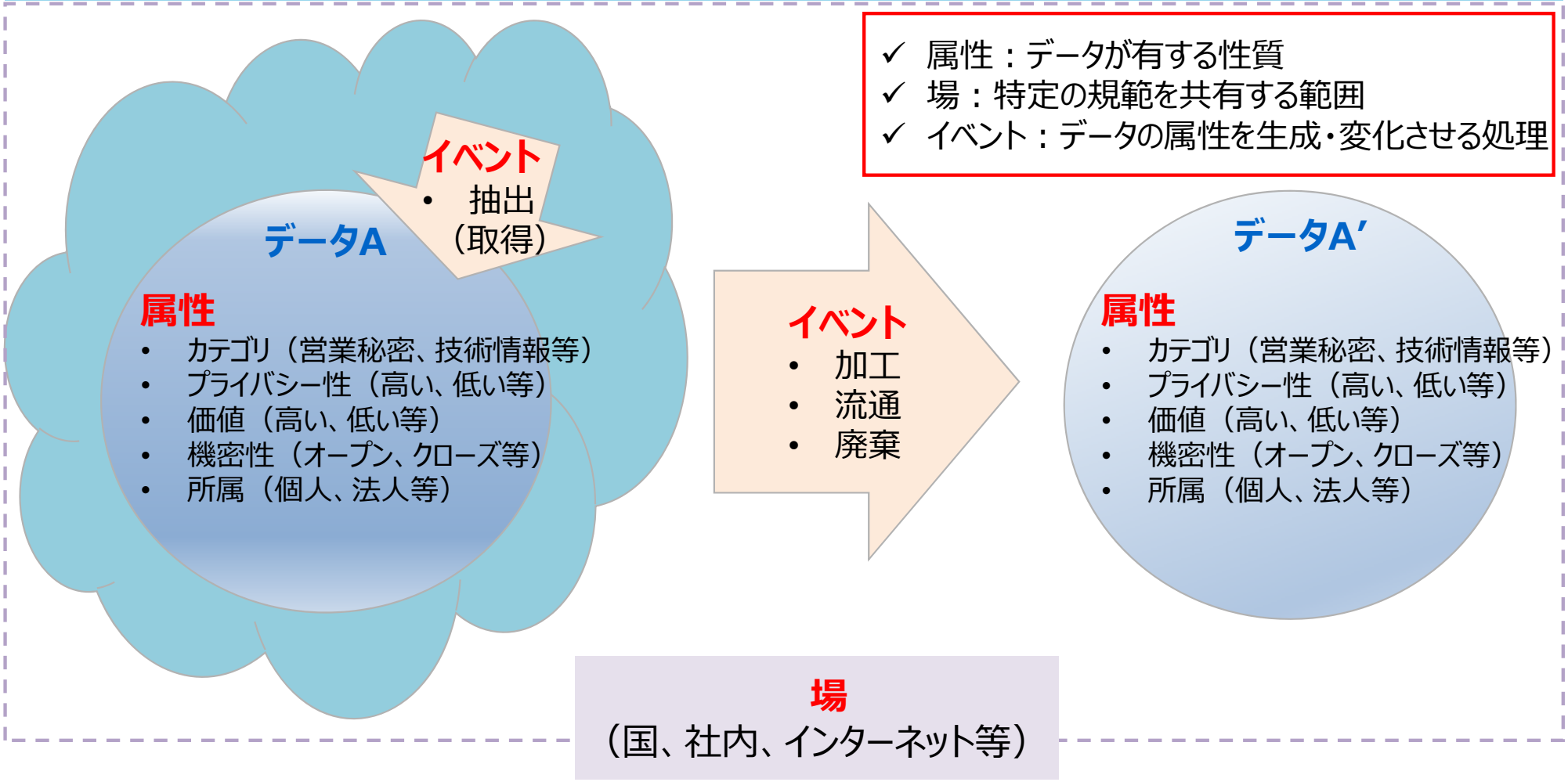
データの信頼性の確認手法の検討

**データそのものや生成者の実体の確認**
**⇒データの真正性確認、モノ等の確認など**

**データの来歴の確認**
**⇒トレーサビリティの仕組みの検討など**

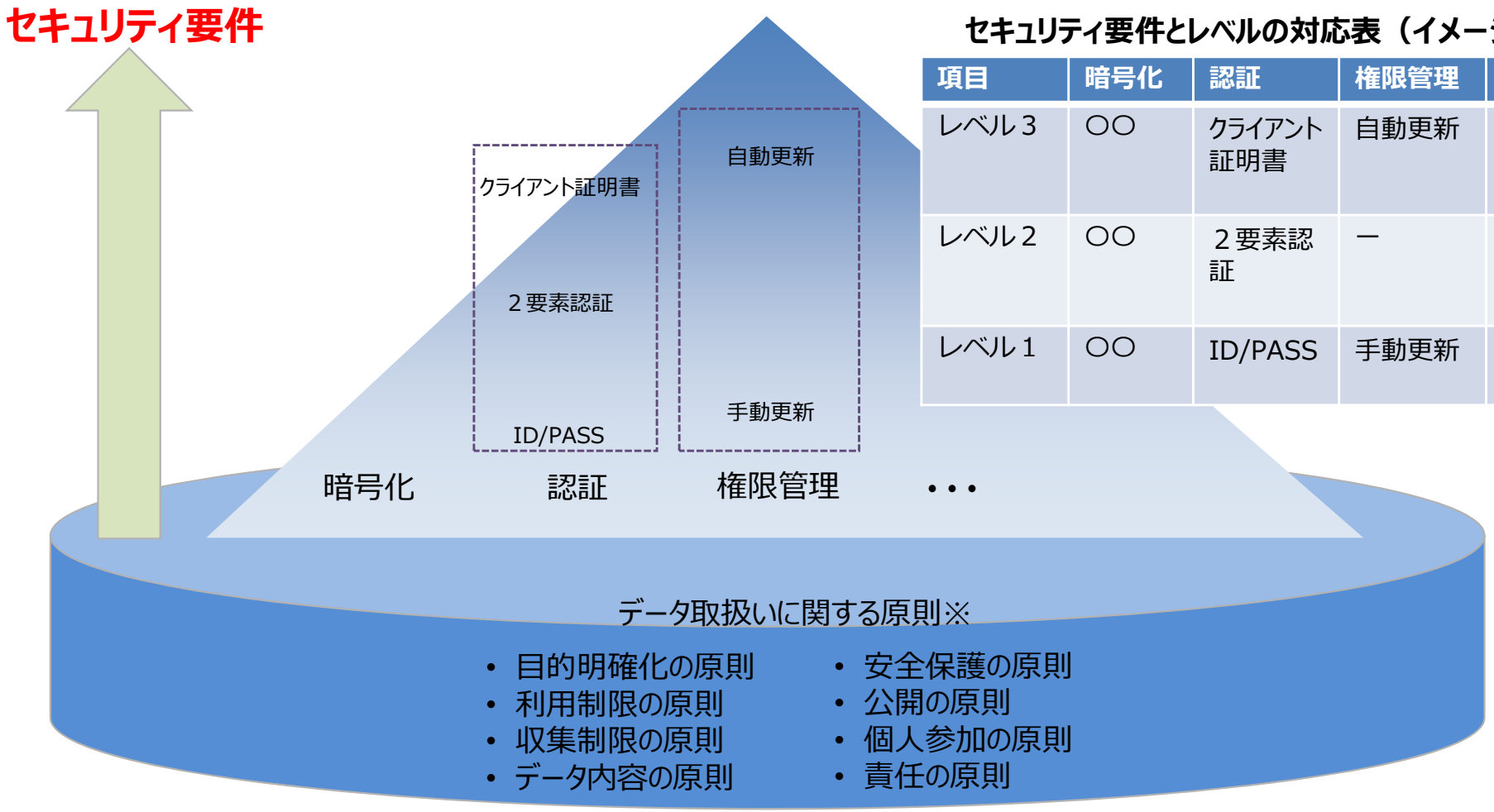
# 『第3層TF』データマネジメントの新たな捉え方

- 既存のデータマネジメント等の考え方を参考にしつつ、第1回タスクフォースの議論を踏まえ、**データマネジメント**とは、「**データの属性が場におけるイベントにより変化する過程をライフサイクルを踏まえて管理すること**」とここでは捉える。



# 『第3層TF』セキュリティ要件の考え方

- データに対する適切なセキュリティ要件を示すことができれば、データを流通させる際のセキュリティ基準が明確になり、データ有効活用の更なる拡大につながるのではないか。




**セキュリティ要件とレベルの対応表（イメージ）**

| 項目 | 暗号化 | 認証 | 権限管理 | … |
|---|---|---|---|---|
| レベル３ | ○○ | クライアント証明書 | 自動更新 | |
| レベル２ | ○○ | ２要素認証 | ー | |
| レベル１ | ○○ | ID/PASS | 手動更新 | |

※　OECDプライバシーガイドラインにおける8原則。