経済産業省

資料５

サブワーキンググループ、タスクフォース等の検討状況

令和２年３月

経済産業省　商務情報政策局

サイバーセキュリティ課

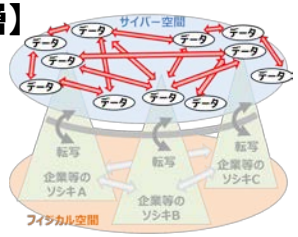
CPSFに基づく具体化・実装の推進

- 平成31年4月、**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。
- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**TFを新たに設置。**

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

【第3層】



サイバー空間におけるつながり

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)

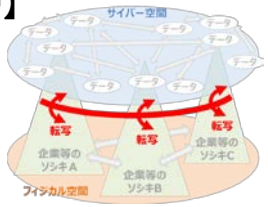
分野別の産業活動
- ビル
- 電力
- 防衛
- 自動車
- スマートホーム 等

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

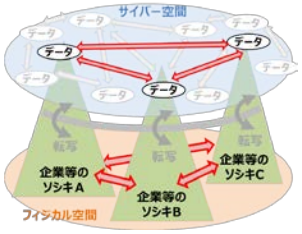
【第2層】



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



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 (⇒ 機器のラベリングの仕組、認証制度の在り方 等)

１．産業分野別SWG

２．第３層タスクフォース

３．ソフトウェアタスクフォース

４．第２層タスクフォース

産業分野別SWGの検討状況

- 各産業分野別SWG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（CPSF）を参考にしつつ、各産業分野の特性に応じたセキュリティ対策の検討が進んでいる。

WG１　制度・技術・標準化

2018/2/7　第1回会合開催
2020/3　第6回会合開催（書面）

標準モデル

Industry by Industryで検討

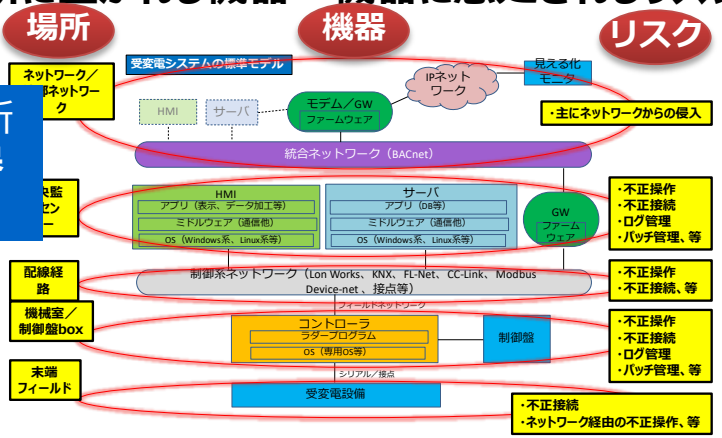
- ビル
  - 2018/2/28 第　1回会合開催
  - 2020/2/13 第10回会合開催
- 電力
  - 2018/6/12 第　1回会合開催
  - 2020/2/20 第　8回会合開催
- 防衛産業（防衛装備庁 情報セキュリティ官民検討会）
  - 2018/3/29 第　1回会合開催
  - 2019/8/26 第　4回会合開催
- 自動車産業
  - 2019/3/29 第　1回会合開催
  - 2020/3/　6 第12回会合開催
- スマートホーム
  - 2018/3/13 第　1回会合開催
  - 2020/2/25 第19回会合開催
-

ビルSWG（座長：江崎 浩 東京大学 教授）

- ビルの管理・制御を行うビル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、2019年6月17日付でガイドライン第1版を公開。
- 記述充実化と個別編(空調編)作成を実施中。関係者間の情報共有の在り方についても検討中。

- **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**

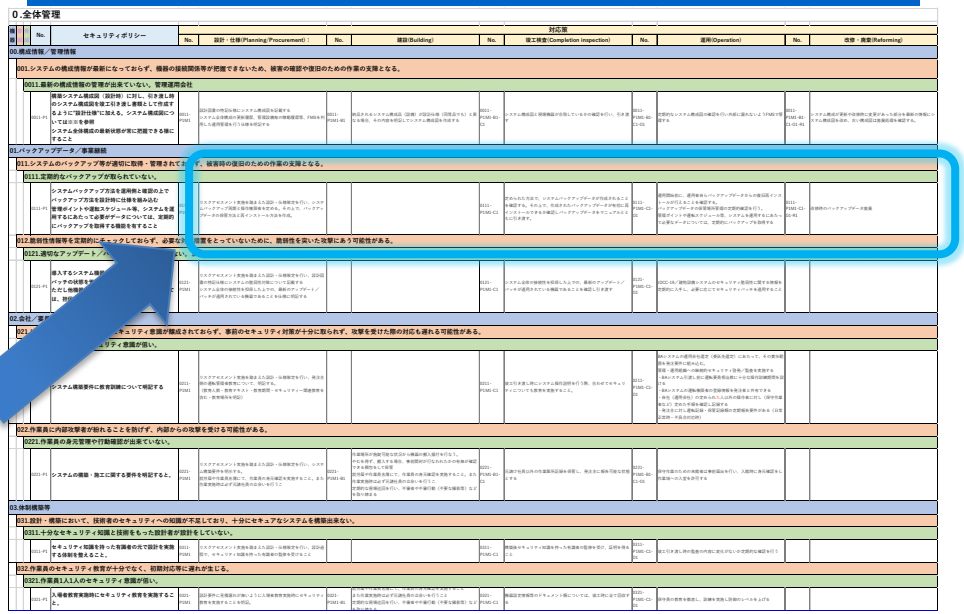
場所及びその場所に設置される**機器等**をリストアップ



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。 ・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なく、ビルシステムへの被害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を組み込む。 ・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（パッチ等）が適用されているかを週1等で確認する。 ・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、その結果を基に整理監査 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

電力SWG（座長：渡辺 研司 名古屋工業大学大学院 教授）

- 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、**短期・中長期という時間軸を加味**しつつ、広く検討。
- **CPSFも踏まえ、電力分野におけるセキュリティ向上を目指す。**

＜構成員＞

有識者（大学教授、弁護士等）、電気事業者、業界団体

＜検討項目＞

- **電力制御系システム**に関するセキュリティ向上策
  - →**「電力制御システムセキュリティガイドライン」への提言**（サプライチェーンのリスクマネジメントや緊急時対応の強化）
  - →国際的な検討枠組みへの参加及び最新動向も踏まえた**サプライチェーンリスクへの対応**策の継続検討

- **大手電気事業者**のサイバーセキュリティ対策について
  - →大手電気事業者におけるサイバーセキュリティの対策状況について、各社独自の評価に加え、**国内外のフレームワークを踏まえた共通枠組み**によるアセスメントの実施手法を検討
  - →**2020年東京オリンピック・パラリンピック**に向けた対応策を検討

- **新規プレーヤー**のサイバーセキュリティ対策について
  - →**太陽光や風力等の発電事業者**、**アグリゲーター**、**小売電気事業者**など、多様な新規プレイヤーによる参入を踏まえ、これらの事業者における**サイバーセキュリティ対策の実態調査**を実施
  - →実態把握を踏まえ、そのサイバーセキュリティリスクへの対応策について、**系統連系におけるセキュリティ要件**の在り方等を検討

防衛産業SWG（防衛装備庁 情報セキュリティ官民検討会）

● 我が国の防衛調達におけるセキュリティ強化の方策について検討

我が国の防衛調達における情報セキュリティ強化の方策について、防衛装備庁と主要な防衛関連企業（２３社４団体）との間で「**防衛調達における情報セキュリティ強化に関する官民検討会**」を開催

＜検討の背景＞

1. **我が国におけるサイバー攻撃の増大**：高度化するサイバー攻撃により、我が国のサプライチェーンが標的となる可能性。
2. **米国の情報セキュリティ強化の動き**：米国の新標準（NIST SP800-171）を満たすことが、今後の米国をはじめとする国際共同研究・開発への参加を継続する最低条件となる可能性。

＜対応方針＞

契約企業が保護すべき情報を取り扱う際に適用される情報セキュリティ基準を、**米国の新標準と同程度まで強化した新情報セキュリティ基準を策定**する。

＜開催の状況＞

	開催日	検討テーマ
第１回	平成２９年　２月２８日	米国の防衛調達における情報セキュリティ強化の動向
		我が国の防衛調達における情報セキュリティ強化の方向
第２回	平成２９年　４月　５日	情報セキュリティ強化のためのルールのあり方
第３回	平成２９年　５月１９日	
第４回	平成２９年　６月１５日	中間的論点整理
第５回	平成２９年１１月２８日	これまでの振り返り及び現在の検討状況
第６回	平成３０年　３月２９日	新基準適合に向けた取り組み
第７回	平成３０年　９月　５日	防衛調達におけるサイバーセキュリティの強化に向けて
第８回	平成３１年　２月２８日	サイバー攻撃に関する留意事項、米国企業のNIST SP800-171対応状況
第９回	令和　元年　８月２６日	新情報セキュリティ基準（案）

第６回検討会より、経済産業省産業サイバーセキュリティ研究会と連携を図るため「**産業サイバーセキュリティ研究会WG1防衛産業SWG** 」として実施。

自動車産業SWG (一般社団法人　日本自動車工業会　電子情報委員会)

- 日本の自動車業界として対象のセキュリティフレームワーク・ガイドライン・実現レベルを定め、活用を推進することで、適切なセキュリティ対策の実施を図る

  ◆対象範囲（車載に関連する部分を除く）

  - 部品やサービス/ソフトウェアのサプライチェーン
  - 個社工場における設備や設備保守
  - “クルマやお客様”と”個社を含むサービス提供者”をつなぐシステムや提供するサービス及びデータ

個社の実施レベル測定と最適化

＜メンバー構成＞
日本国内の乗用車、二輪車、商用車生産の14社

＜開催状況＞
2019年4月16日(火) 第１回　電子情報委員会／サイバーセキュリティ部会開催、以後11回の会合を経てサイバーセキュリティ業界対応を推進

＜2019年度成果＞
国内外のフレームワークやガイドライン、国際標準規定をベースに、自動車業界のリファレンスとなるサプライチェーン領域におけるガイドライン初版（自動車業界の全ての企業が実施すべき項目を規定）を部工会殿と共同で作成し、2020年4月目処で自工会H/P公開予定

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）

- スマートホームにおける安全で安心な生活の実現のため、スマートホームの提供事業者から住まい手まで、幅広いステークホルダに必要なセキュリティ対策をまとめたガイドライン原案を今年度中に策定。

◆ガイドラインの対象

- スマートホーム向けIoT機器、スマートホーム向けサービス、スマートホーム（住宅）の開発・生産・販売・供給・サポート等を行う事業者
- スマートホーム化された区分所有型集合住宅および賃貸型集合住宅の管理者
- スマートホームの住まい手

＜メンバー構成＞
企業）家電・AV関連、IT・通信関連、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、医療関係、健康関連分野、研究機関

＜開催状況＞
2018年3月より、おおよそ月1回程度の頻度で開催。これまで19回開催。

＜進め方＞
- 国内外のIoT機器に関する文献から、サイバーセキュリティ対策動向を調査。
- ユースケースやCPSFから導出される脅威や脆弱性について、ステークホルダ毎に対策要件をまとめたガイドライン原案を作成中。

１．産業分野別SWG

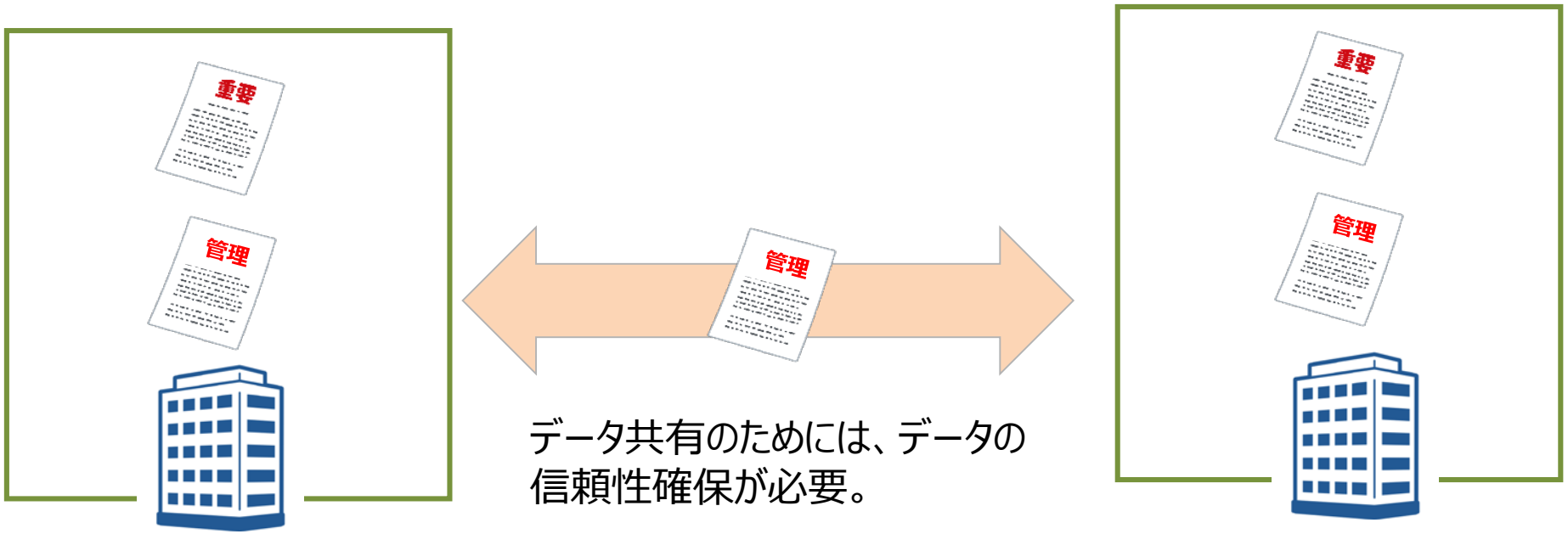
２．第３層タスクフォース

３．ソフトウェアタスクフォース

４．第２層タスクフォース

第３層タスクフォースの検討の方向性

- CPSFでは、第３層（サイバー空間のつながり）で確保すべき**信頼性の基点をデータと定義**。
- データの自由な流通を拡大していくためには、**一定のセキュリティ対策等による信頼性の確保の考え方を整理し、社会に実装していくことが必要**。
- 第３層タスクフォースでは、**データの信頼性確保に求められる要件**を検討。



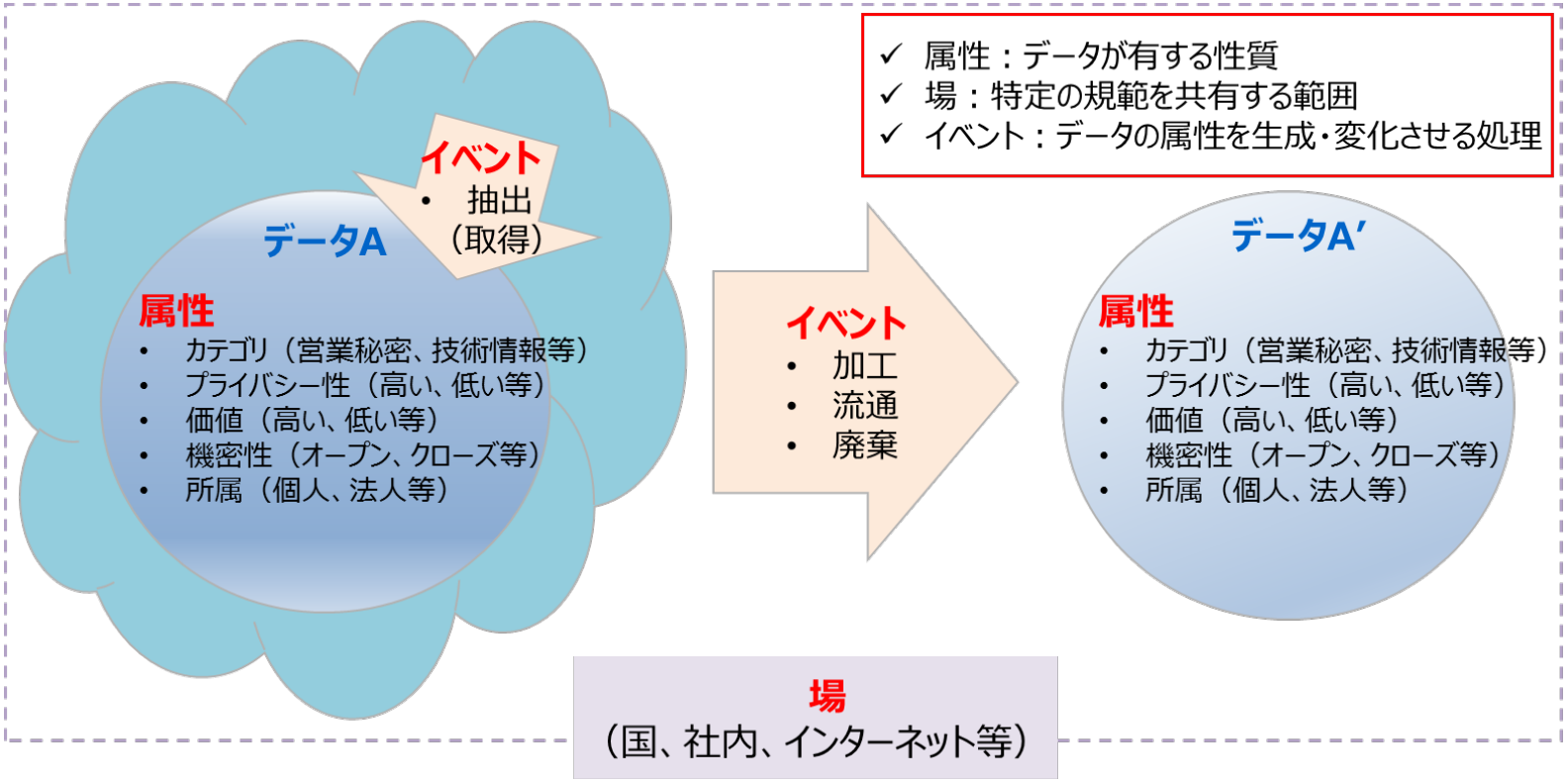
データ共有のためには、データの信頼性確保が必要。

第３層タスクフォースの検討の方向性

- データの信頼性を明確化するため、**データに関わるファクターとデータのライフサイクルを俯瞰するモデルを提案。**

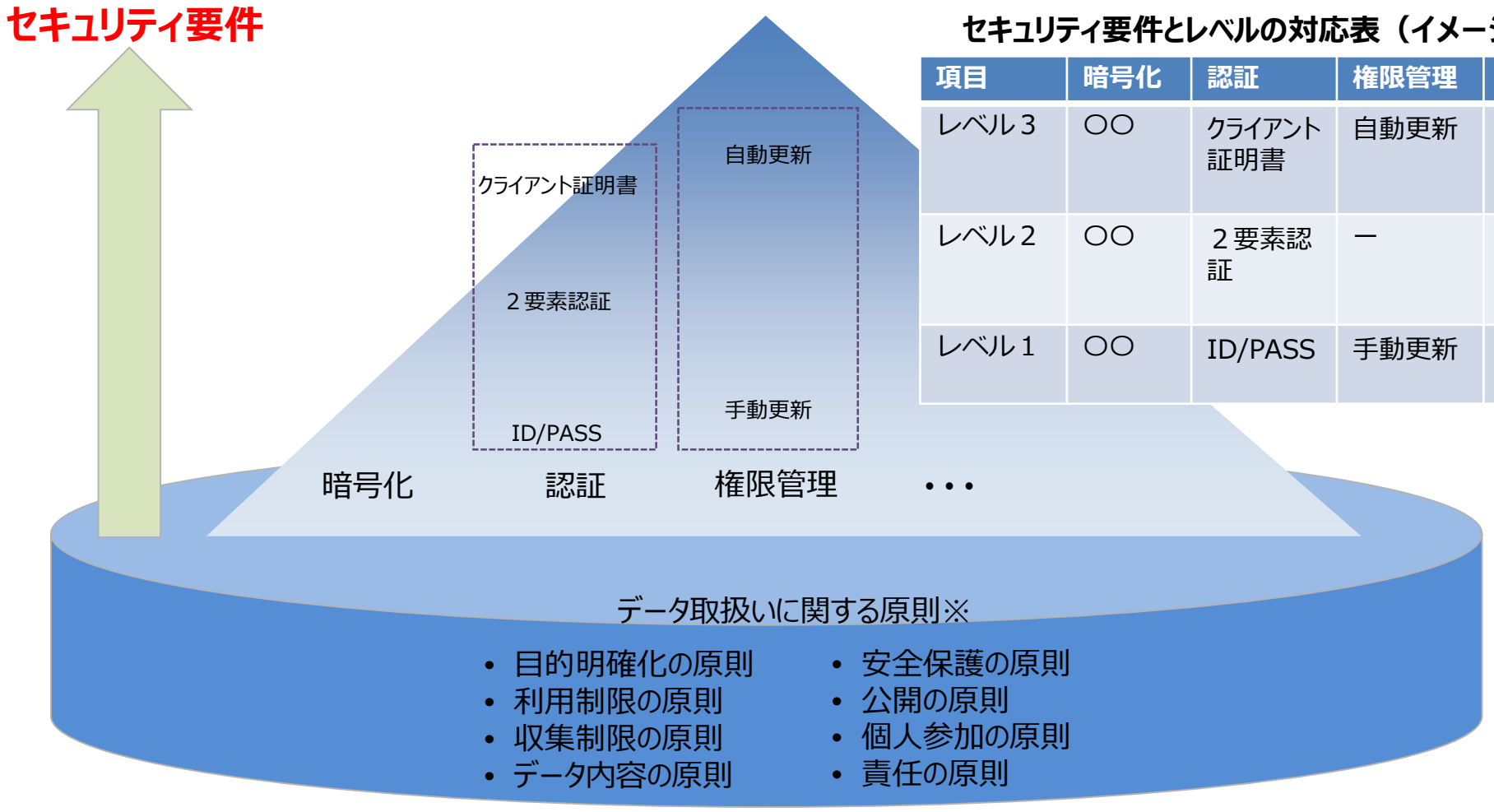
データマネジメントの新たな捉え方

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**」と提案。



第３層タスクフォースの検討の方向性

- 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）

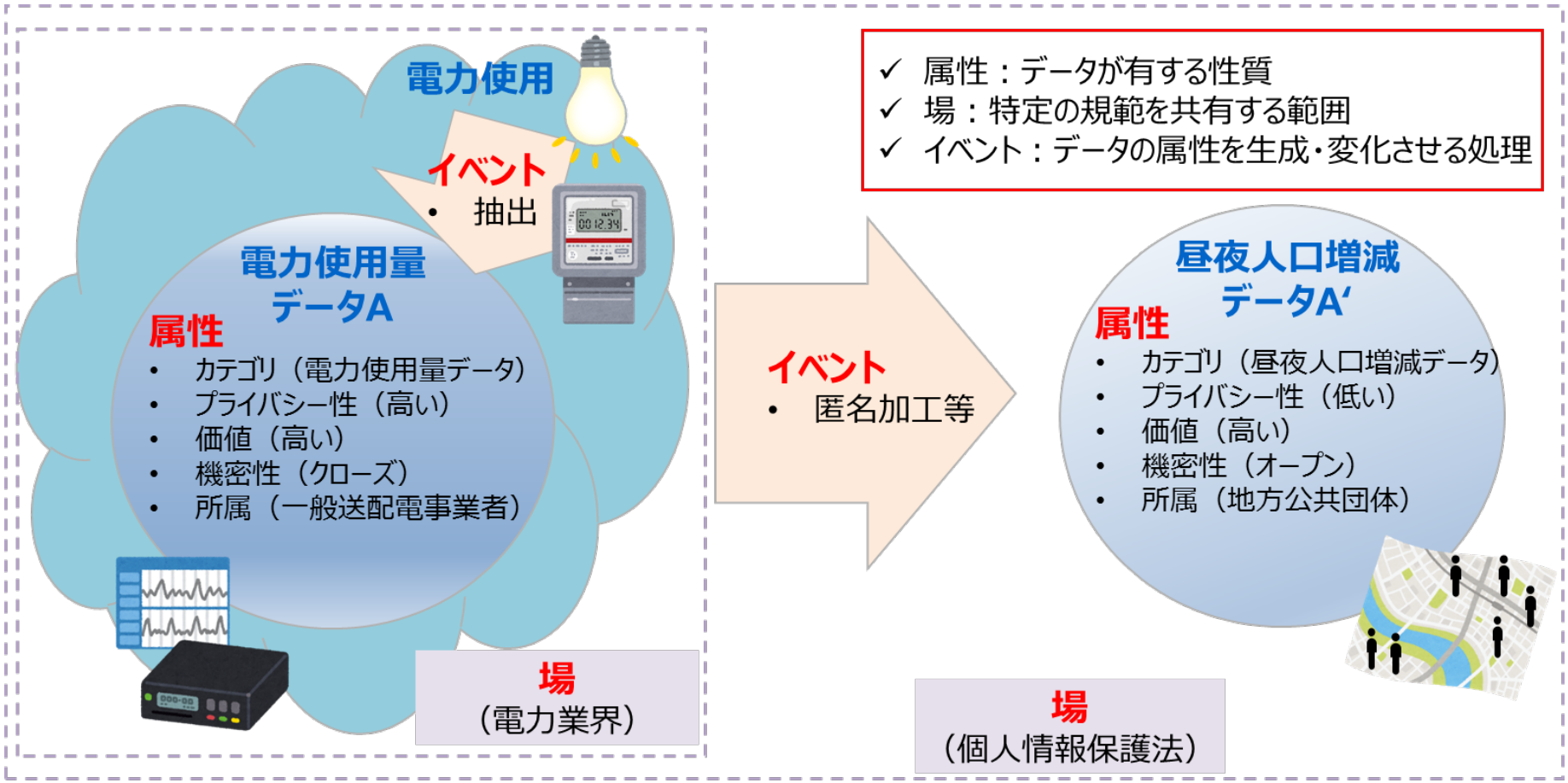
項目	暗号化	認証	権限管理	…
レベル３	○○	クライアント証明書	自動更新	
レベル２	○○	２要素認証	ー	
レベル１	○○	ID/PASS	手動更新	

※　OECDプライバシーガイドラインにおける8原則。

第３層タスクフォースの検討の方向性

- 適切なセキュリティ要件は、データAの**属性**及び対応する**場**、並びに、データA'へ処理するための**イベント**で決定できるのではないかと提案。
- 来年度も引き続き検討を継続。

電力使用量データから防災等に活用するための昼夜人口増減データへの匿名加工化の想定（イメージ）



１．産業分野別SWG

２．第３層タスクフォース

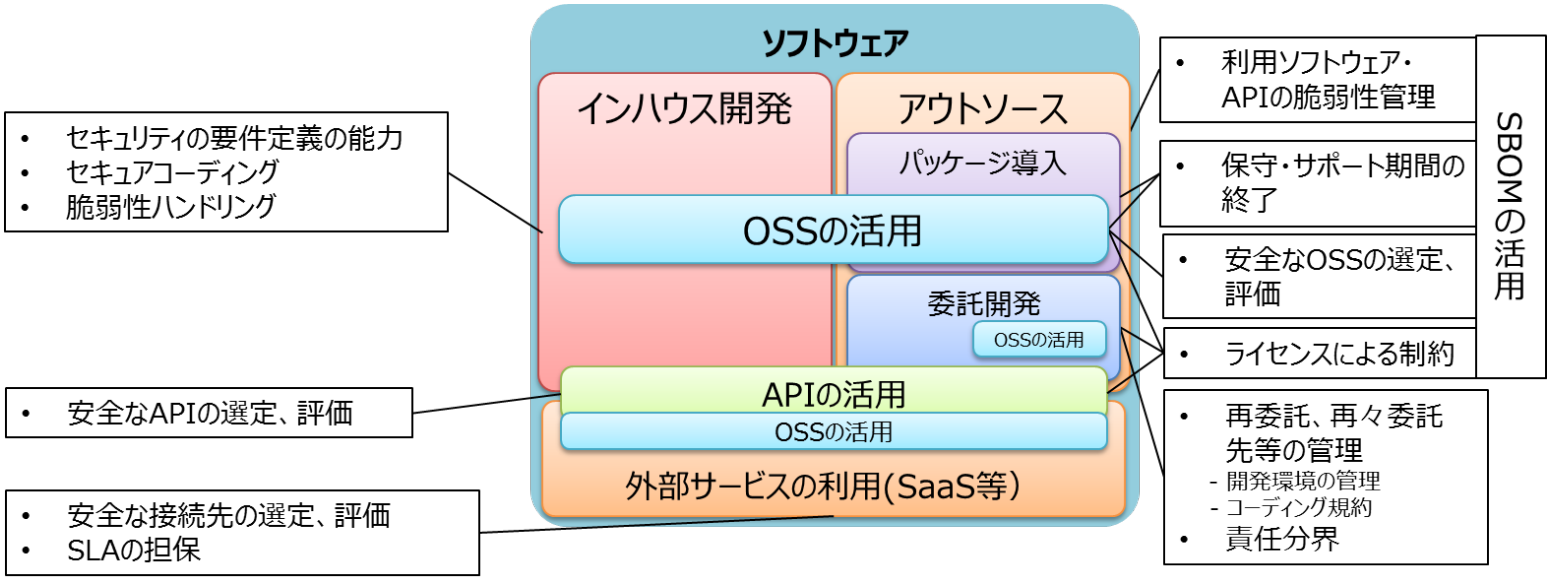
３．ソフトウェアタスクフォース

４．第２層タスクフォース

ソフトウェアタスクフォースの検討の方向性

- 仮想化技術の進展などにより、**OSSを含むソフトウェア技術への依存が高まる中**で、**ソフトウェアの管理手法、脆弱性対応やライセンス対応等の重要性が増している**。
- 2018年、**米国NTIA（電気通信情報局）は、「Software Component Transparency」を設立**し、ソフト部品構成表である**SBoM (Software Bill of Material）の活用に関する議論**を推進。
- ソフトウェアタスクフォースでは、**適切なソフトウェア（特にOSS）の管理手法、脆弱性対応やライセンス対応等を検討**。

ソフトウェアを利用する際に考慮すべき観点



ソフトウェアタスクフォースの検討の方向性

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

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

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

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1回
検討事項

第2回
検討事項

第3回
検討事項

ソフトウェアタスクフォースの検討の方向性

- 3回のタスクフォースでの議論を経て、「OSSの利活用及びセキュリティ確保に向けた管理手法」の**事例集作成に着手**。
- 今年度先行して事例のサンプルを作成し、**来年度広く事例を集めて策定予定**。
- 米国では、ヘルスケア分野においてSBOMのPoCが進展。日本においても実施できる分野が無いか検討を継続。

OSS利活用における留意事項の観点

プロセス別観点

選定評価
- ✓ 安全なOSS選定が困難
- ✓ 製品構成（部品やOSS等）や、脆弱性の把握が困難

脆弱性管理
- ✓ ソフトウェア管理の粒度のばらつき
- ✓ 費用対効果（労力、コスト）
- ✓ 脆弱性告知、適用手段、サポートが不適切
- ✓ 詳細なソフトウェア情報公開によるリスク（対ユーザー）
- ✓ レガシーな機器やシステム、IoT機器

保守・ライセンス
- ✓ 改変のライセンス違反
- ✓ サポート終了したOSSの放置
- ✓ 運用、保守計画が立てづらい
- ✓ OSSのライセンスを評価できていない
- ✓ 納品時のセキュリティの保証、保守条件（対ユーザー）
- ✓ 廃棄、終了時の対応

サプライチェーン管理
- ✓ 網羅的な調整が困難
- ✓ OSS前提ではない取引慣行
- ✓ SBOMの活用が進んでいない
- ✓ 契約による明文化の必要性
- ✓ 企業ごとの対応能力のばらつき
- ✓ 全てのサプライチェーン内のOSS管理及び脆弱性体制の確保

人・組織に関する観点

個の能力
- ✓ 経営者のリスク管理不足
- ✓ 判断基準、対応基準が未整備
- ✓ リテラシー不足
- ✓ お客様への説明の難しさ（対ユーザー）
- ✓ 人依存・コミュニティ依存の対応

組織体制
- ✓ OSS利活用をサポートする社内体制がない
- ✓ コミュニティへの関わり方が定まっていない
- ✓ 多くのベンダでPSIRTが立ち上がってない（対ユーザー）

グローバルな観点

- ✓ 国際調和の重要性認識
- ✓ 海外のOSSコミュニティにおける発言力UP

１．産業分野別SWG

２．第３層タスクフォース

３．ソフトウェアタスクフォース

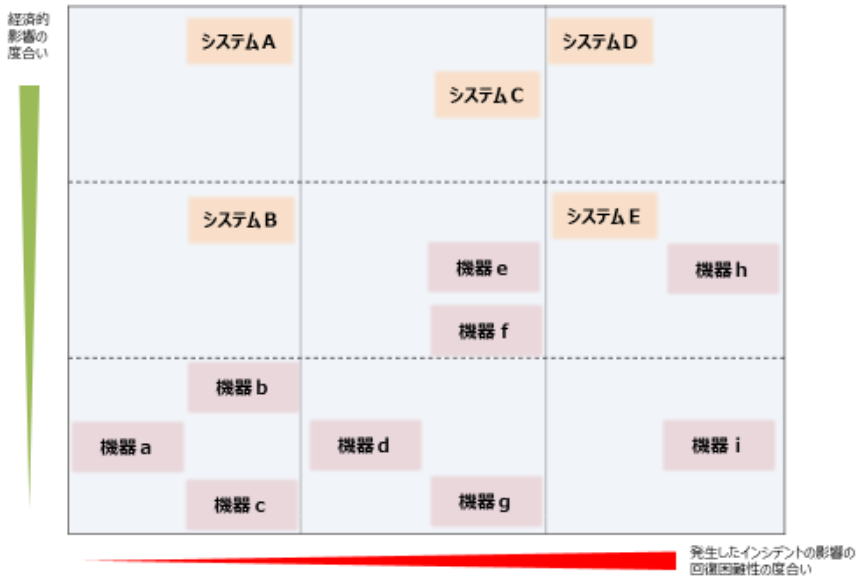
４．第２層タスクフォース

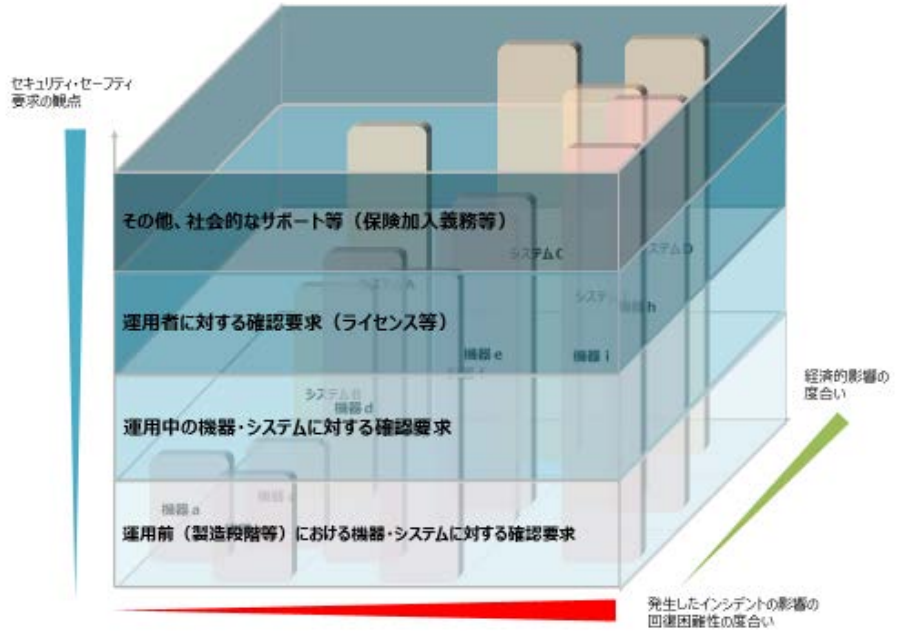
第２層タスクフォースの検討の方向性

- CPSFでは、第2層（フィジカル空間とサイバー空間のつながり）で確保すべき信頼性を、**フィジカル・サイバー間を正確に“転写“する機能**と定義。
- 第2層で想定されるセキュリティインシデントの影響は、サイバー空間に留まらず**安全面にも支障をきたす可能性**がある。
- 第2層タスクフォースでは、サイバー・フィジカル間の**転写機能を持つ機器について、人体に対する影響や社会に与える被害等を考慮した信頼性確保に求められる要件**を検討。

第２層タスクフォースの検討の方向性

- 3回のタスクフォースでの議論を経て、「**IoT機器は**使われ方や製造コスト等が**多様であるため、リスクに応じてIoT機器をカテゴライズした上で、基本的に任意でセキュリティ・セーフティ要件を課すべき**」との考えの下、**フレームワークを策定中**。
- 本フレームワークでは、カテゴライズする軸を『**発生したインシデントの影響の回復困難性の度合い**』と『**発生したインシデントの経済的影響の度合い**』の2軸で定義。また、セキュリティ・セーフティを確保するための手法を、運用前、運用中、運用者、社会的なサポートの4つの観点から整理。
- 本フレームワークは、近々パブリックコメントを行うことを想定。





フィジカル空間とサイバー空間のつながりの信頼性を確保するための フレームワークの提案について

- これまでのTFでの議論を踏まえ、フィジカル・サイバー間をつなげる機器・システムにおけるセキュリティ・セーフティ要求の強度を適切に検討するため、それらの**機器・システムのカテゴライズおよびセキュリティ・セーフティ要求の検討に資するフレームワーク**を提案する。

<目次>

1.　本フレームワークの必要性
1-1 CPSFにおける第2層（フィジカル空間とサイバー空間のつながり）
1-1-1 CPSF概論
1-1-2 第2層の位置づけ
1-2 本フレームワークの目的
2.　本フレームワークの想定読者
3.　本フレームワークの基本構成
3-1 基本構成の背景にある考え方
3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理
3-2-1 第1軸：発生したインシデントの影響の回復困難性の度合い
3-2-2 第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）
3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ
3-3 求められるセキュリティ・セーフティ要求の整理
3-3-1 第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求
3-3-2 第2の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求
3-3-3 第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求
3-3-4 第4の観点：その他、社会的なサポート等の仕組みの要求
4.　本フレームワークの活用方法

フレームワークの必要性、想定読者

- IoT等の新たな仕組み・サービスに関するセキュリティ・セーフティについて、**包括的に課題を捉える統一的な手法が欠如**しており、対応策が不整合となること等による社会として新たな仕組みを**受容・管理していくためのコストが増大する恐れ**がある。
- 新たな仕組みによってもたらされる新たなリスクに着目し、リスク形態及びそうしたリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示。サイバー空間とフィジカル空間をつなぐ、新たな仕組みを**社会として効果的に受容していくことができるようにするための基本的共通基盤を提供する**ことを目的とする。

<目次>

1. 本フレームワークの必要性

1-1 CPSFにおける第2層
（フィジカル空間とサイバー空間のつながり）

1-1-1 CPSF概論

1-1-2 第2層の位置づけ

1-2 本フレームワークの目的

2. 本フレームワークの想定読者

想定読者

- IoTを活用してサイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスを実現しようとする者
- そのような新たな仕組み・サービスで活用されるIoT機器・システムの開発を行う者
- そのような新たな仕組み・サービスを適切に管理していく制度・環境を実現していこうとする者
- IoTによる新たな仕組み・サービスを受ける者

フレームワークの基本構成（機器・システムのカテゴライズ）

- IoT機器・システムにおけるセキュリティ上の課題は多様であり、**一律のセキュリティ要求を課すのは適切ではない。**多様性に対してどうアプローチするかが重要。
- そこで、発生したインシデントによる人命/身体に対する影響を表す**「回復困難性の度合い」**と、回復の可能性・困難性という観点を除いて影響の大きさを金銭的価値に換算した**「経済的影響の度合い」**の2軸を用い、フィジカル・サイバー間をつなげる機器・システムに潜むリスクを整理。**リスクに応じて機器・システムをカテゴライズ**。
- 同じ機器であったとしても、**その用途等により、**重要性や課題、インシデントによる影響等は大きく異なるため、**マッピング先が異なり得る**ことに留意。

<目次>

3.　本フレームワークの基本構成

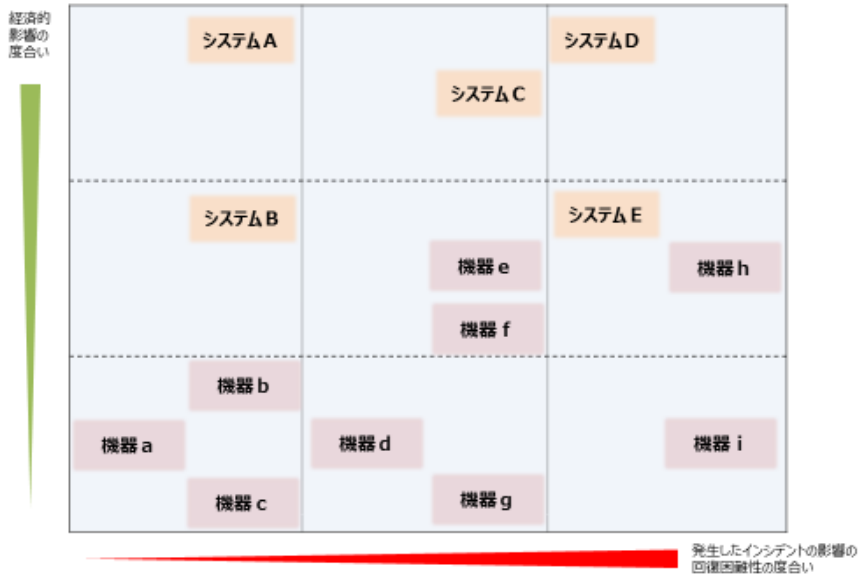
3-1 基本構成の背景にある考え方

3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理

3-2-1 第1軸：発生したインシデントの影響の回復困難性の度合い

3-2-2 第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）

3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ



フレームワークの基本構成（セキュリティ・セーフティ要求）、活用方法

- セキュリティ・セーフティを確保するための手法を、**運用前、運用中、運用者、社会的なサポートの4つの観点**から整理。
- 各観点はセキュリティ・セーフティ要求に関する内容の考え方の違いに基づいて設定されたものであって、**同じ観点であっても具体的に要求される個々のセキュリティ・セーフティ対策は一様ではない**ことに留意し、**セキュリティ・セーフティ要求の強度を適切に検討するための枠組みとして利用されることを期待**。

<目次>

3.　本フレームワークの基本構成

3-3 求められるセキュリティ・セーフティ要求の整理

3-3-1 第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求

3-3-2 第2の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求

3-3-3 第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求

3-3-4 第4の観点：その他、社会的なサポート等の仕組みの要求

4.　本フレームワークの活用方法