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）の概要

平成31年4月18日

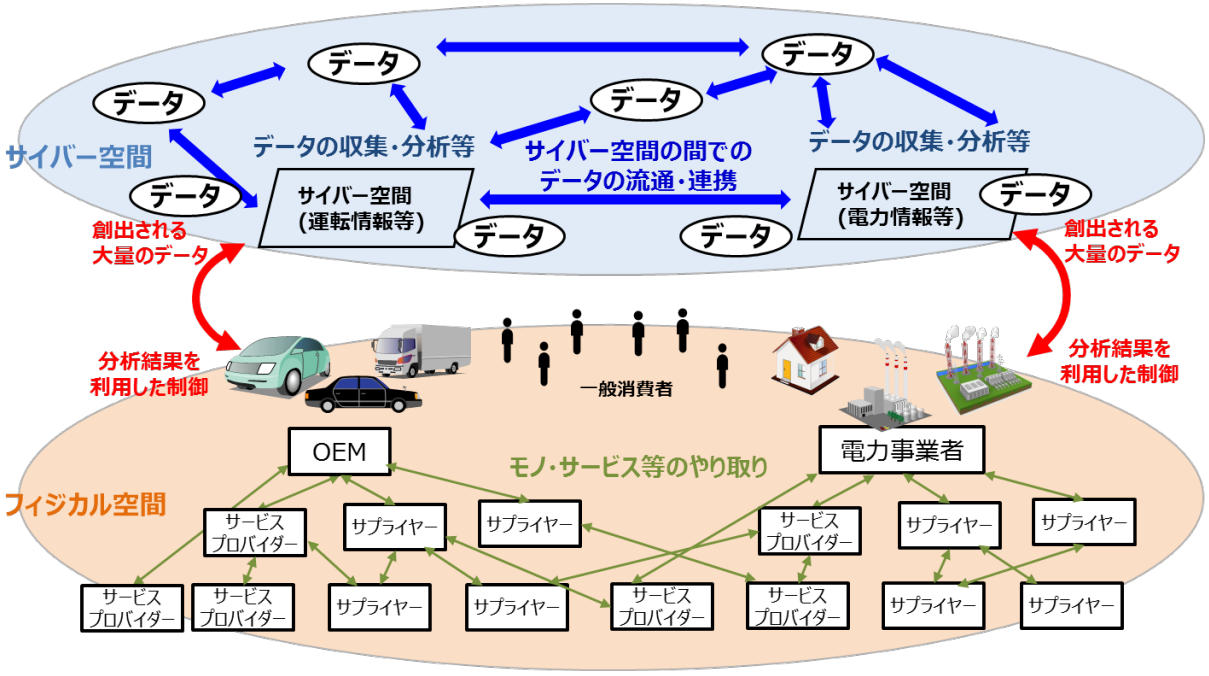
経済産業省　商務情報政策局

サイバーセキュリティ課

はじめに

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。

CPSFに含まれる対策

従来型サプライチェーンにおいても適用可能な対策	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対策

- **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

CPSFの想定読者、全体構成

- CPSFは、産業社会の全体像を捉えたものであるため、**バリュークリエイションプロセスに取り組むすべての主体が適用対象。**
- **技術等の変化に伴う見直し等も考慮し、三部構成（コンセプト、ポリシー、メソッド）を採用。**

想定読者	第Ⅰ部【コンセプト】	第Ⅱ部【ポリシー】	第Ⅲ部【メソッド】
• CISO（Chief Information Security Officer; 最高情報セキュリティ責任者）	○	○	
• サプライチェーンマネジメントに関わる戦略・企画部門の担当者	○	○	
• バリュークリエイションプロセスに関わる企業・団体等のセキュリティ担当者		○	○
• 情報関連機器、制御系機器の開発・品質保証、システム設計・構築・検証担当者		○	○
• データマネジメントの担当者		○	○
• 各産業分野におけるセキュリティ対策のガイドライン等を策定する業界団体等の担当者	○	○	○

第Ⅰ部【コンセプト】

- サイバーセキュリティの観点から、バリュークリエイションプロセスにおける**リスク源を整理するためのモデル（三層構造と６つの構成要素）**を整理。

第Ⅱ部【ポリシー】

- 第Ⅰ部で示した**モデルを活用したリスク源の整理**と、**リスク源に対応する対策要件**を提示。

第Ⅲ部【メソッド】

- 第Ⅱ部で示した対策要件を対策の種類に応じて整理。

CPSFに期待される効果・特徴、使い方

- CPSFを活用することで期待される効果。
  - セキュリティ対策の実行による**バリュークリエイションプロセスの信頼性の確保**
  - 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**
- CPSFは、「Society5.0」という新たな産業社会において、付加価値の創造に取り組む主体が、その活動に必要なセキュリティ対策を講じようとする際に参照されることを想定。
- 一方、業界や企業により、**守るべき資産、人的・資金的リソース、又は許容できるリスク等は異なる**ため、以下の内容を参考に本フレームワークを利用することを期待。

リスク源の洗い出し

第Ⅱ部、添付Ａ、添付Ｂ

- 三層構造モデルを参考にし、企業等の付加価値の創造活動におけるモデルを構築
- 企業等のリスク源の明確化

企業等におけるセキュリティポリシーの策定及び対策の実装

第Ⅲ部、添付Ｃ

- 第Ⅲ部、添付Ｃを参考に、自組織におけるセキュリティポリシーの策定及びセキュリティ対策の実装
- 国際標準等との比較

企業等、業界等における信頼のチェーンの構築への活用

- リスク源を洗い出し、セキュリティ対策を実施することで、一つ一つのバリュークリエイションプロセスの信頼性を確保
- 上記取組をつなげることで信頼のチェーンを構築。

第Ⅰ部　コンセプト：

サイバー空間とフィジカル空間が高度に融合した産業社会における産業分野のサイバーセキュリティの在り方

”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

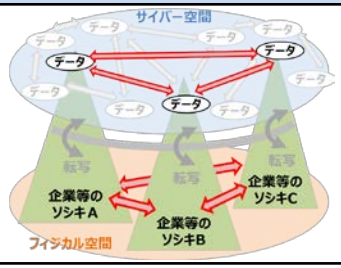
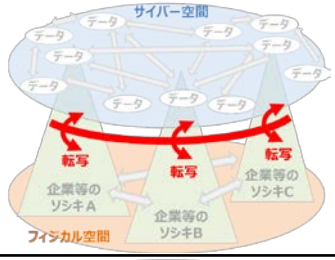
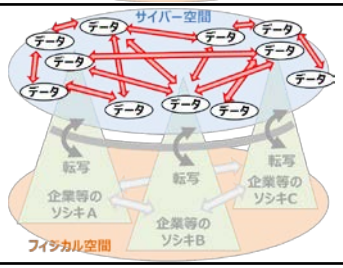
バリュークリエイションプロセスが発生する産業社会を、３つの「層」で整理。

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

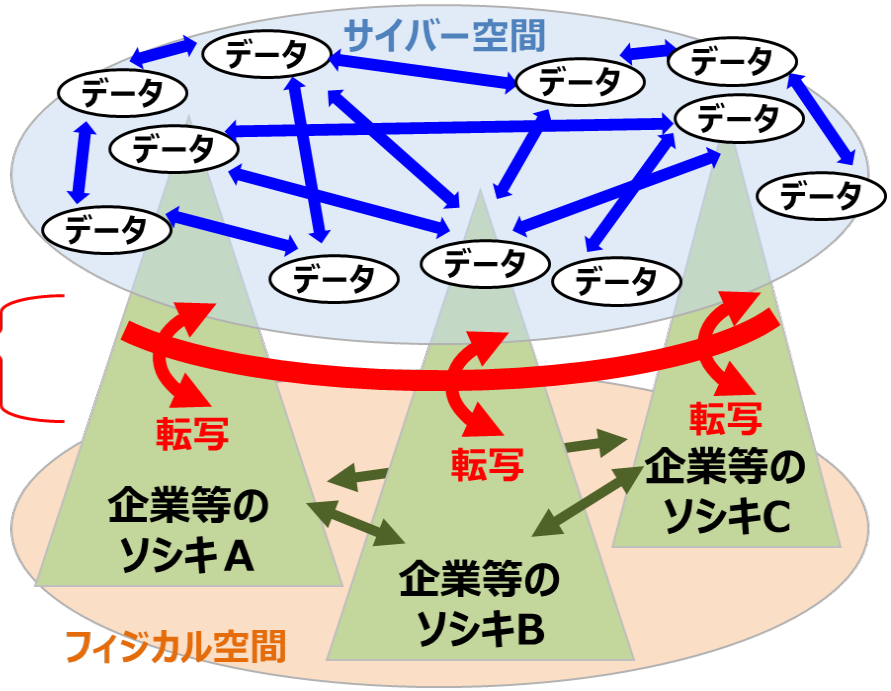
~バリュークリエイションプロセスのセキュリティを確保するための信頼性の基点の設定~

- **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

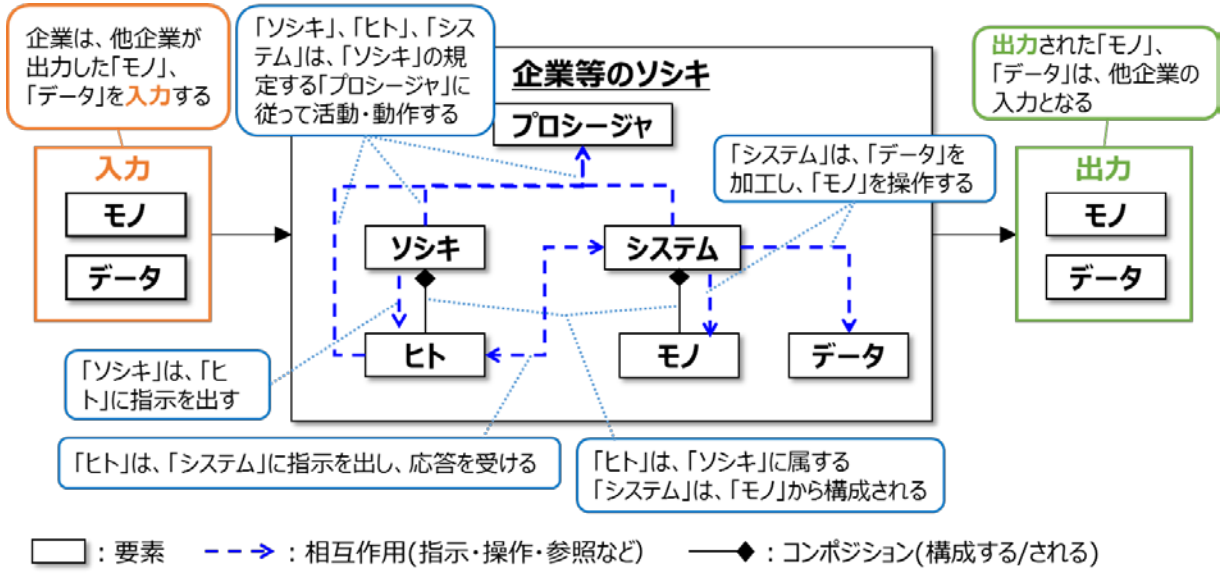


６つの構成要素

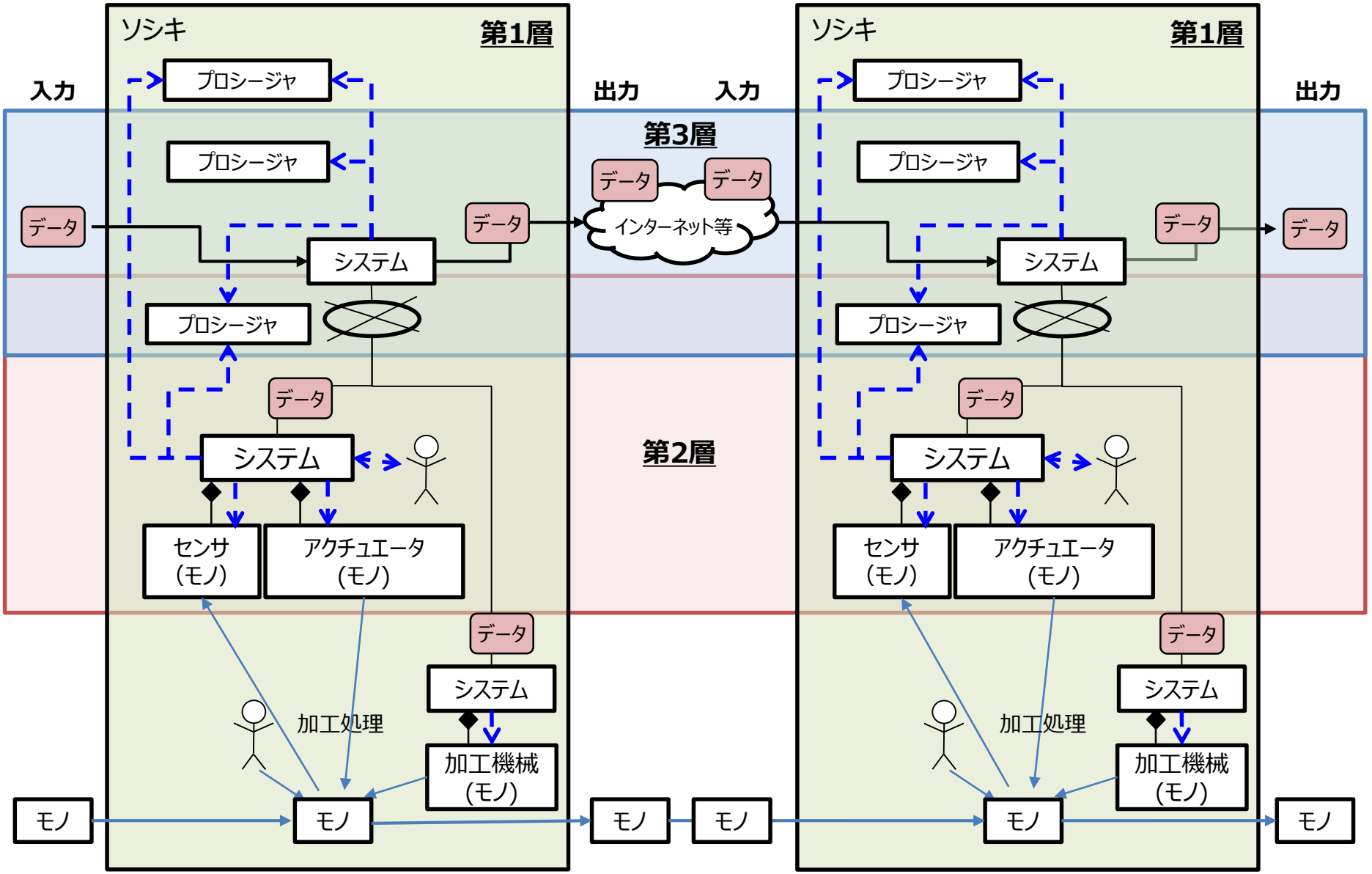
～動的で柔軟なバリュークリエイションプロセスを捉えるための構成要素～

- 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	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・ソシキ	**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
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	**プロシージャ**	• 定義された目的を達成するために一連の活動を定めたもの
モノ	• ハードウェア、ソフトウェア及びそれらの部品操作する機器を含む	**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

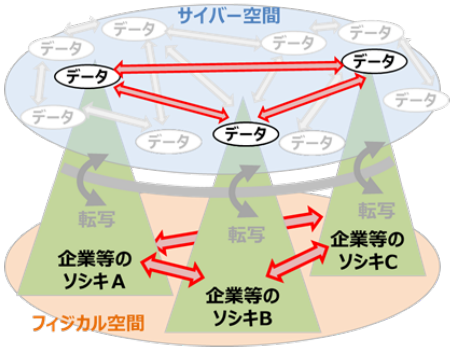
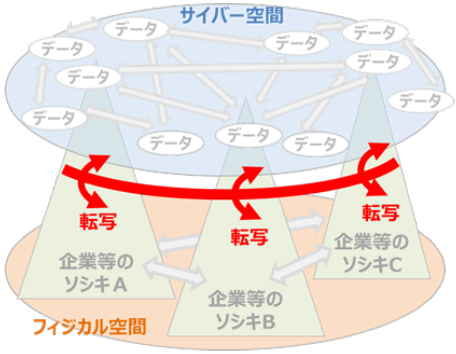
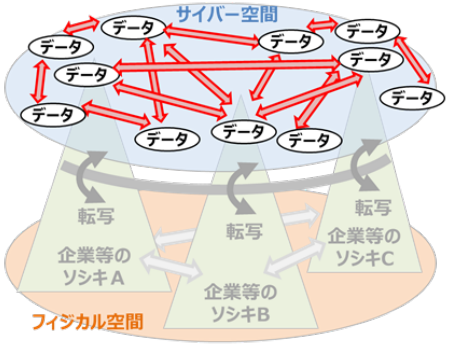


（参考）三層構造における6つの構成要素の関係



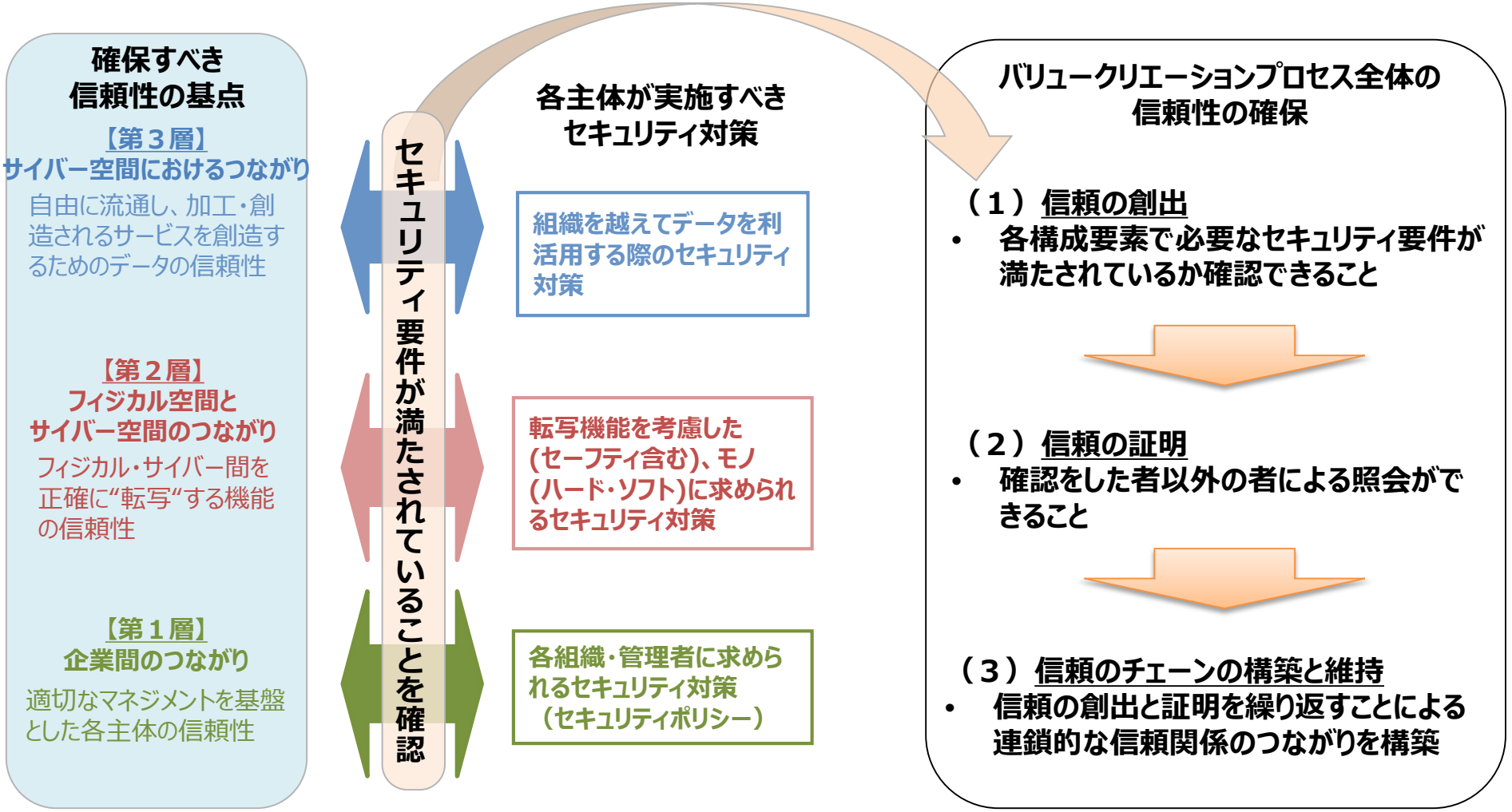
CPSFの全体概要（リスク源と対応する方針の整理）

- 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。

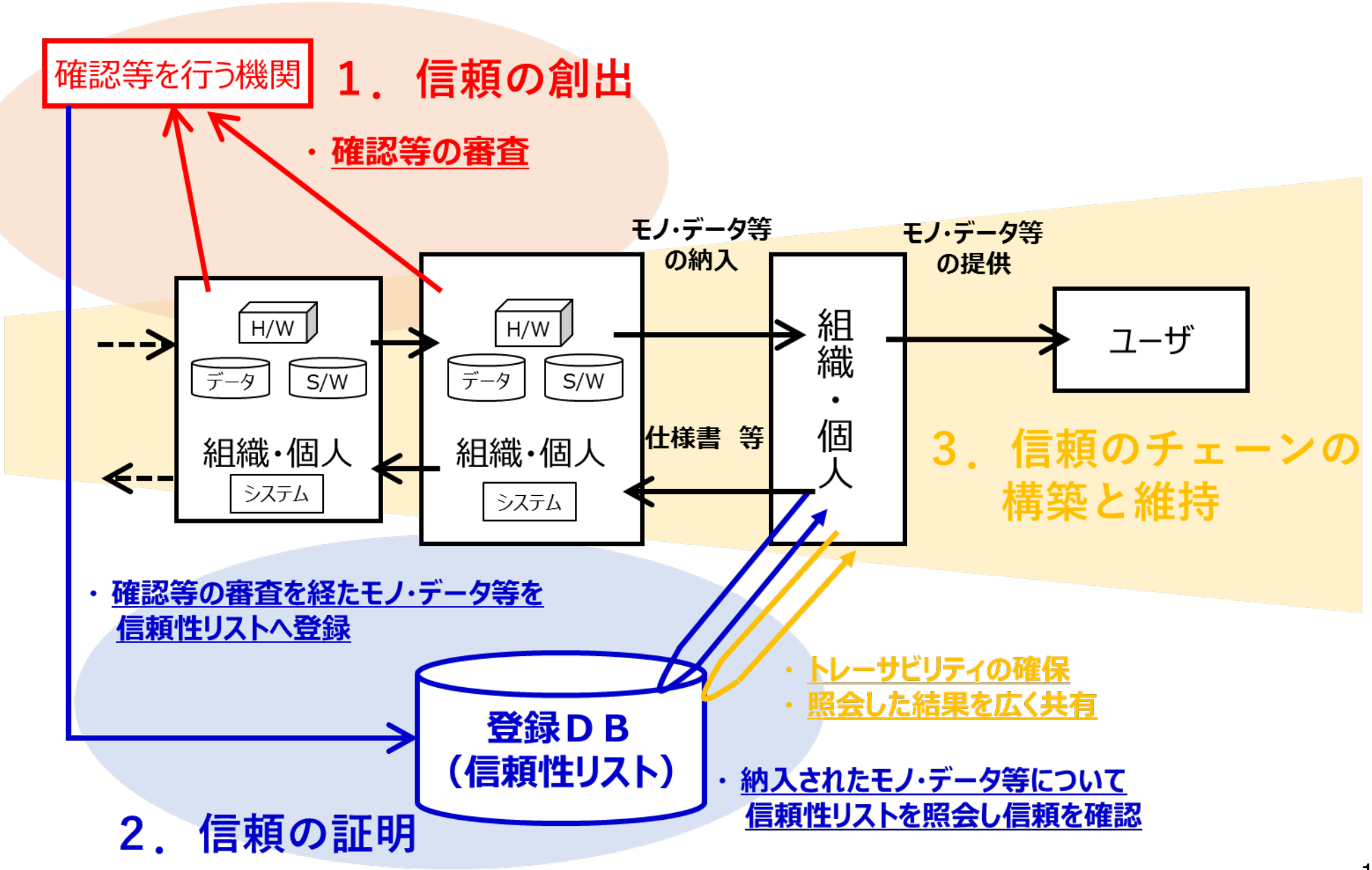
	企業間のつながり【第１層】	フィジカル空間とサイバー空間のつながり【第２層】	サイバー空間におけるつながり【第３層】
新たなサプライチェーン構造の整理			
機能（守るべきもの）	• 平時及び緊急時のリスク管理・対応体制の構築と運用 • 企業内及び企業間のリスク管理・対応体制の構築と運用	• フィジカル空間とサイバー空間の境界における情報の正確な転写	• データの加工・分析 • データの保管 • データの送受信
セキュリティインシデント	• 保護すべき資産の棄損 • 他組織のセキュリティ事象発生に起因する事業停止	• 不正確なデータの送信 • 安全に支障をきたす動作	• 保護すべきデータの漏えい • 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 • 他組織との連携状況の未把握	• 不正なIoT機器との接続 • 許容範囲外の入力データ	• 通信経路が保護されていない • 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 ■ 関係者との役割分担	■ 接続相手の認証 ■ 安全なIoT機器の導入	■ 暗号化によるデータ保護 ■ データの提供者の信頼性確認

CPSFにおける信頼性の確保の考え方

- 各構成要素について必要なセキュリティ要件が満たされていることを確認し(**信頼の創出**)、確認した主体以外の者による照会ができるようにし(**信頼の証明**)、それを繰り返し行い、広く共有して**信頼のチェーンを構築、維持**することで、**バリュークリエイションプロセス全体のセキュリティを実現**することになる



（参考）信頼の創出、信頼の証明、信頼のチェーンの構築と維持の関係のイメージ



第Ⅱ部　ポリシー：
リスク源の洗い出しと対策要件の特定

三層構造モデルと６つの構成要素を活用したリスクマネジメント

- リスクマネジメントにおける標準的なプロセス（例：JIS Q 31000:2010, JIS Q 27001:2014）も踏まえ、**CPSFに基づくセキュリティリスクマネジメントの流れを整理。**
- **三層構造モデル、6つの構成要素の考え方を活用し、バリュークリエイションプロセスの特徴をとらえたセキュリティリスクマネジメントが可能。**

セキュリティ・リスクマネジメントの流れ

1. 分析対象の明確化
2. 想定されるセキュリティインシデント及び事業被害レベルの設定
3. リスク分析の実施
4. リスク対応の実施

CPSFの考え方を踏まえたリスクマネジメントで考慮すべき観点

① バリュークリエイションプロセスに関わるステークホルダーとの関係

② IoT機器を介したサイバー空間とフィジカル空間の融合

③ 組織を跨がるデータの流通

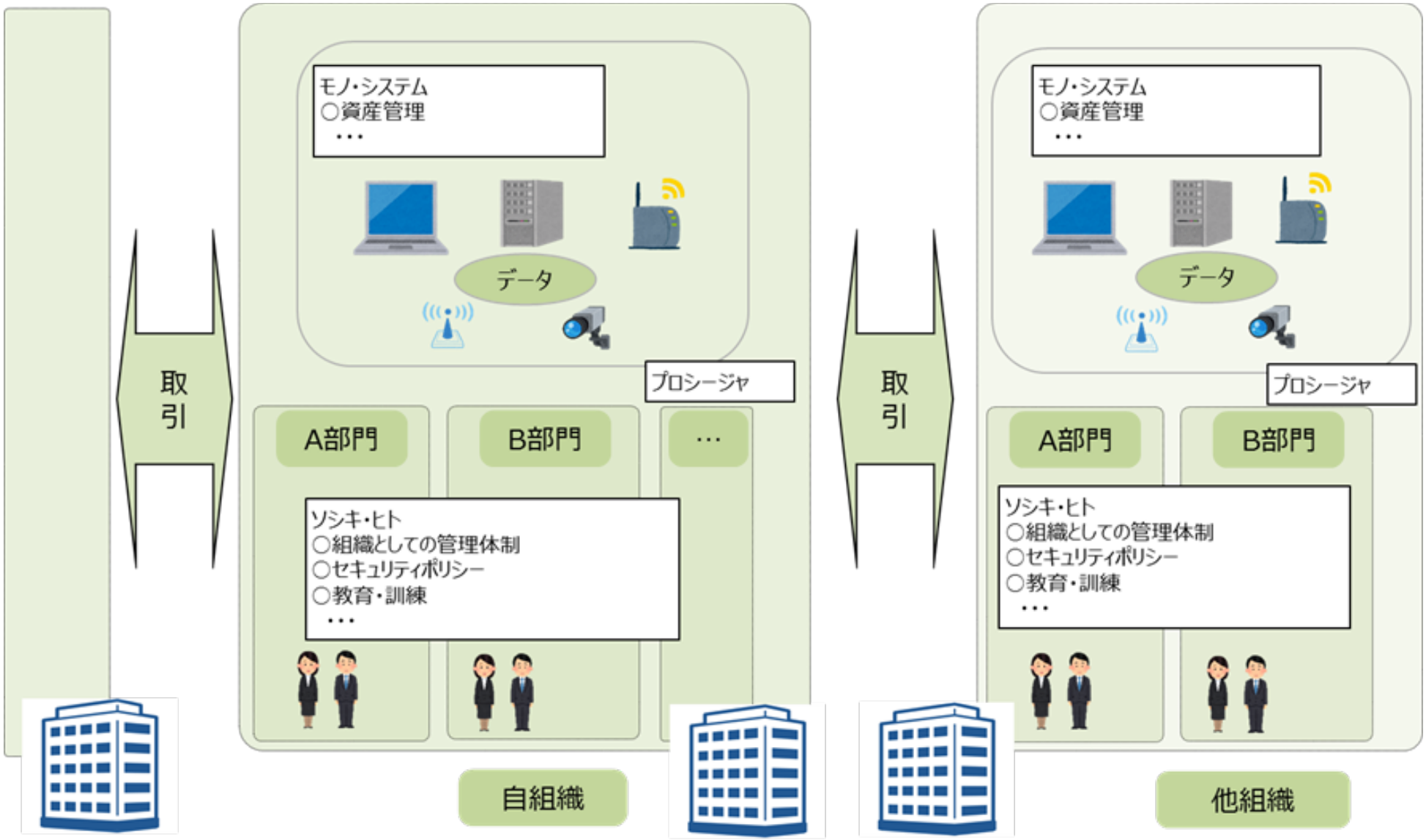
④ 各層における信頼性の基点の確保

分析対象の明確化（三層構造モデルへの落とし込み）

- 各層の特性及び機能・役割を理解した上で**分析範囲及び資産を整理**。
- 分析対象のシステムによっては第２層の機能と第３層の機能を併せ持つモノもあることに留意。

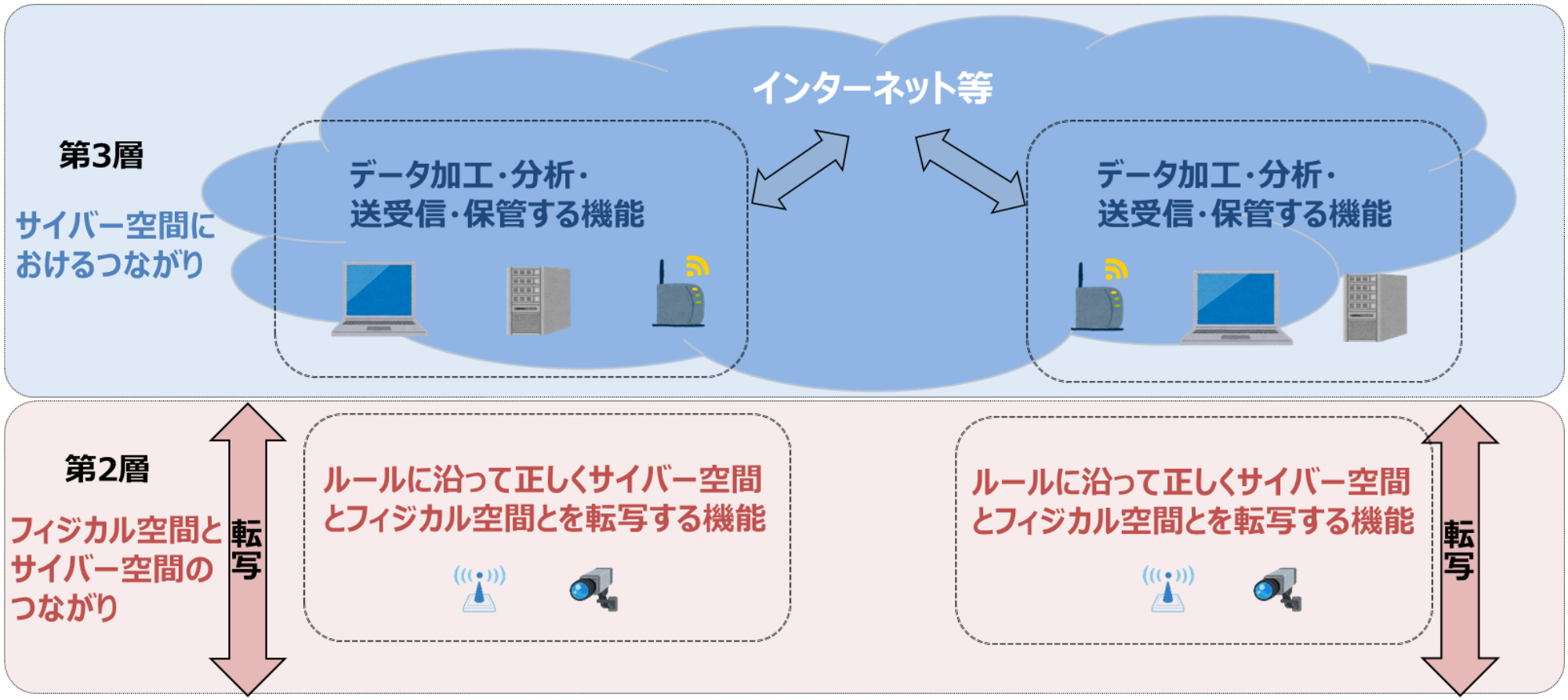
階層	特性	機能・役割	分析対象	分析対象の具体的イメージ
第1層	各組織の適切なガバナンス・マネジメント	• 各組織のセキュリティマネジメント **【信頼性の基点】**組織・マネジメント	• 組織で管理されるモノ・システム等 • 組織内で流通するデータ 等	• 社員、従業員 • 企業のIT資産 等
第2層	フィジカル空間とサイバー空間のつながり拡大	• フィジカル空間とサイバー空間との間のデータのやりとり **【信頼性の基点】**ルールに沿って正しくフィジカル空間とサイバー空間とを転写する機能	• データを転写するモノ・システム • 転写されるデータ 等	• センサ • アクチュエータ • 3Dプリンタ • 監視カメラ 等
第3層	サイバー空間で組織を超えた多様・大量のデータの流通・処理	• データの送受信、加工・分析、保管 **【信頼性の基点】**データ	• データを送受信／加工・分析／保管するモノ・システム • 組織を超えて流通するデータ等	• サーバ • ルータ • スマートメータ • オープンデータ 等

第1層の分析対象及び分析対象の具体的イメージ

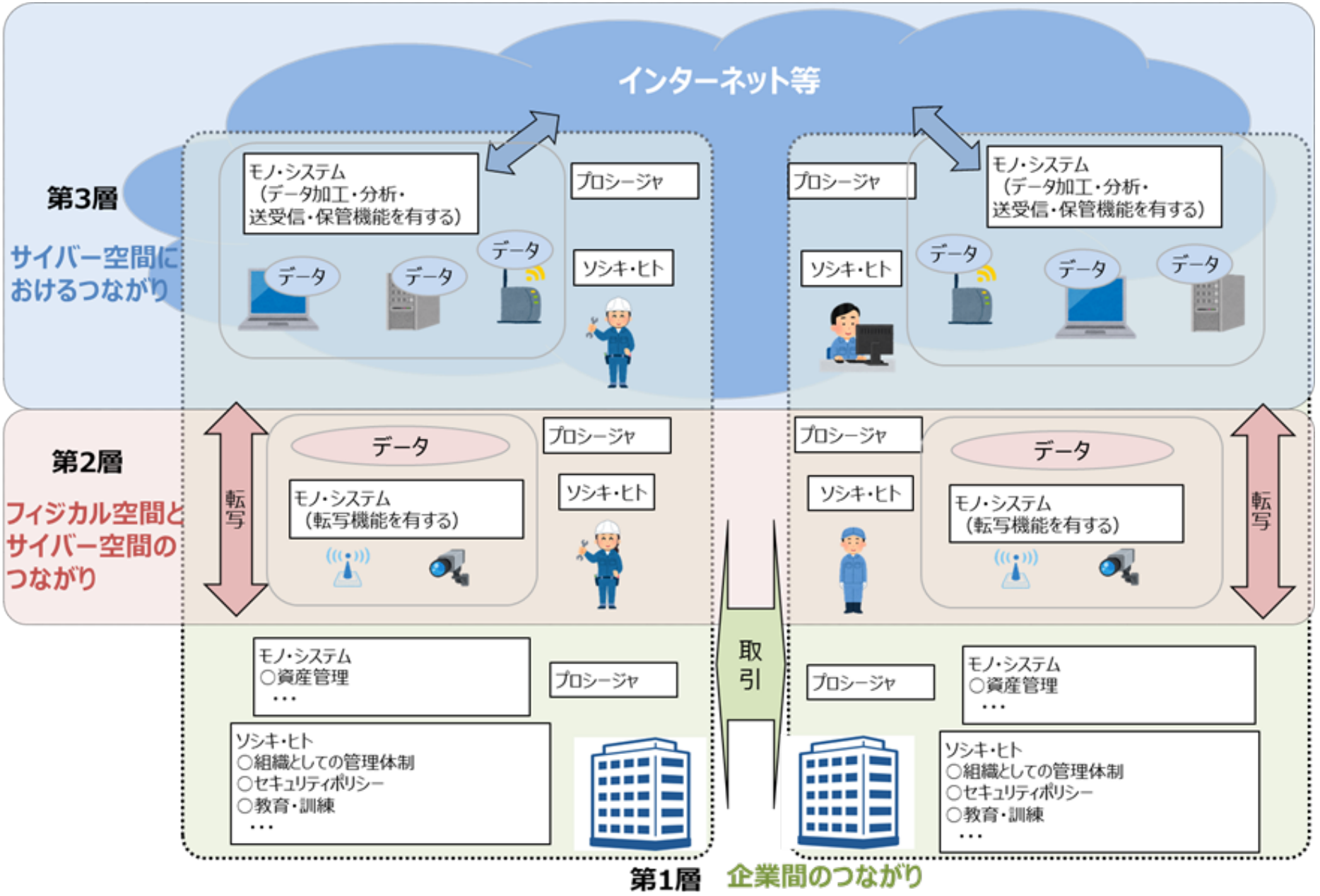


第1層 企業間のつながり

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



想定されるセキュリティインシデント及び事業被害レベルの設定①
～各層の機能に対する悪影響のイメージ～

- 三層構造モデルにおける各層の特性などを踏まえ、**各層の機能（守るべきもの）とそれに対する悪影響のイメージを整理**。

階層	各層の機能（守るべきもの）	機能（守るべきもの）に対する悪影響のイメージ
第1層	• 各組織のセキュリティマネジメント	• **セキュリティインシデントの発生**（営業秘密の漏えい） • **セキュリティインシデントによる影響の拡大**（被害拡大による事業影響）
第2層	• フィジカル空間とサイバー空間との間のデータのやりとり	• **機器の機能停止**（IoT機器の稼動停止） • **信頼性の低い稼動**（IoT機器の意図しない稼働）
第3層	• データの送受信、加工・分析、保管	• **データ保護に係る法制度等への不準拠** • **セキュアでない稼動**（データ処理側での情報資産の棄損） • **信頼性の低い稼動**（データ関連サービスの意図しない稼動）

想定されるセキュリティインシデント及び事業被害レベルの設定②
～想定されるセキュリティインシデントの設定～

- 各層の機能及び機能に対する悪影響の観点を踏まえ、**三層構造の各層で発生を回避すべき一般的なセキュリティインシデントを整理。**

階層	想定されるセキュリティインシデントの例
第1層	• セキュリティインシデントによる被害が拡大し、**適切に事業継続できない** 等
第2層	• 内部に不正アクセスされた**IoT機器が意図しない動作** • 改ざんされた**IoT機器による正確でないデータの送信等**が発生 等
第3層	• サイバー空間にて取り扱われる**保護すべきデータの漏えい** • なりすましされた機器等から**不適切なデータを受領** 等

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 • データを加工・分析する機能 • データを保管する機能 • 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]** ・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。

第Ⅲ部　メソッド：
セキュリティ対策要件と対策例集

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 L1_1_b_COM L1_1_c_COM L2_1_a_ORG L2_3_b_ORG	<H-Advanced> ・・・	O/S	○	○	―
			<Advanced> ・・・	O/S	○	○	○
			<Basic> ・・・	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) RC.RP (Recovery Planning)
伝達	CPS.CO	RS.CO (Communications) RC.CO (Communications)
分析	CPS.AN	RS.AN (Analysis)
低減	CPS.MI	RS.MI (Mitigation)
改善	CPS.IM	RS.IM (Improvements) 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, L1_1_b_COM, ・・・	<H.Advanced> ・・・	O/S	○	○	—
			<Advanced> ・・・	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	・・・

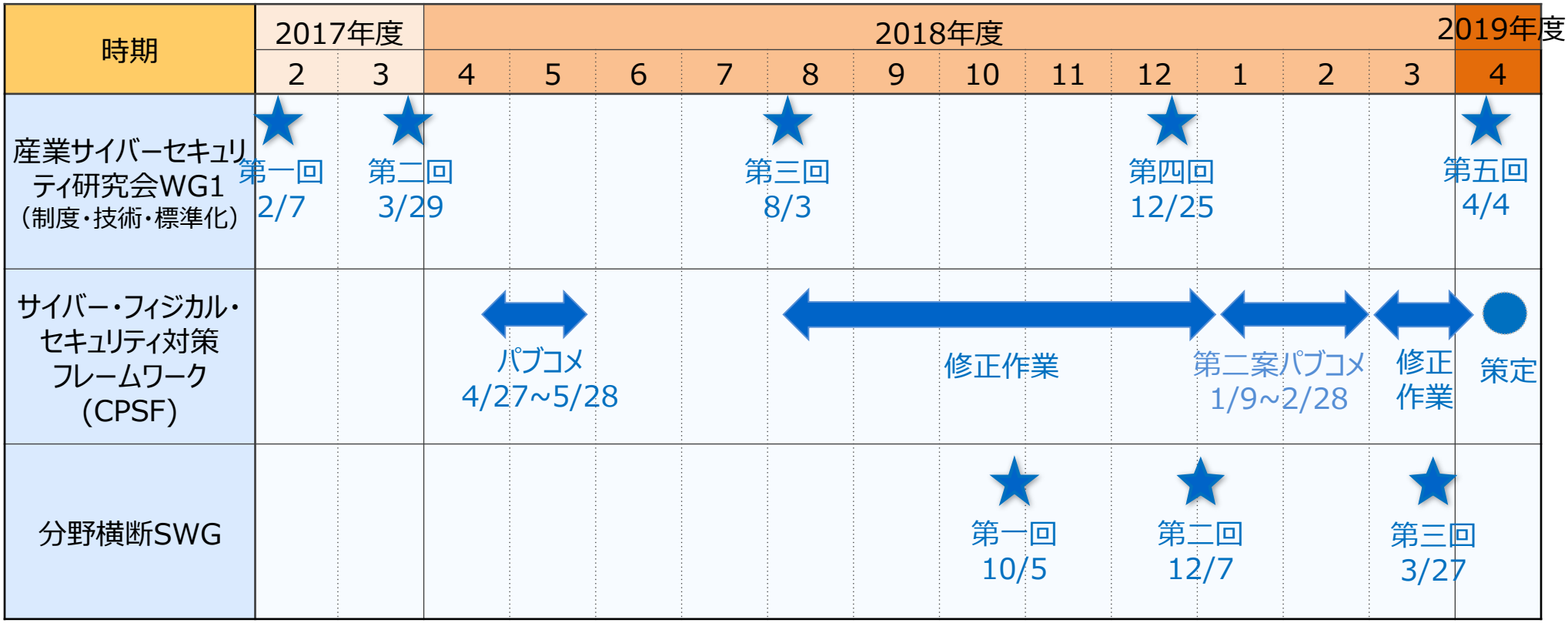
NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク		
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例
アクセス制御	3.1.1	・・・	・AC-2 アカウント管理 ・・・	CPS.AC-9	・・・	・・・

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	・・・	・・・

これまでの取組について

- **『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4月18日に策定。**
- 今後、CPSFを主要な産業分野に展開し、各産業分野で求められる具体的なセキュリティ対策の検討を推進。

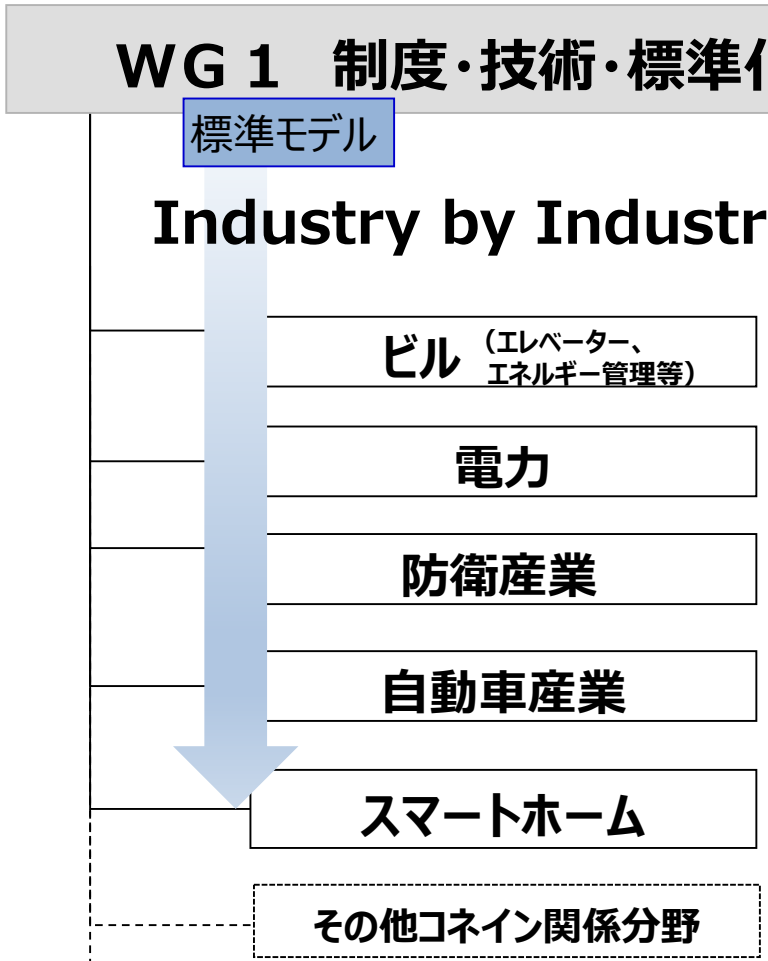
これまでの取組の経緯



関連した取組（各産業分野への展開）

産業分野ごとの検討の促進：分野別のSWGの設置

- 産業サイバーセキュリティ研究会WG1（技術・制度・標準化）で検討してきたCPSFを、**産業分野別に順次展開**し、具体的適用のためのセキュリティポリシーを検討。



［2018年2月～（５回開催）］
2019年４月　CPSFの決定・公表

［2018年２月～（８回開催）］
2018年9月　ガイドライン（β版）を公開
2019年3月　ガイドライン第1版（案）のパブコメを実施

［2018年6月～（４回開催）］

［2018年３月～（８回開催）］
（防衛装備庁 情報セキュリティ官民検討会）

2019年４月　第1回会合開催

［2018年３月～（８回開催）］
（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）