経済産業省

資料５

サイバー・フィジカル・セキュリティ対策フレームワーク（第二案）について

平成30年12月25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. 前回WG１以降のサイバー・フィジカル・セキュリティ対策フレームワーク（案）の修正のポイント

2. サイバー・フィジカル・セキュリティ対策フレームワーク（第二案）の概要

3. 今後のスケジュール

サイバー・フィジカル・セキュリティ対策フレームワーク（案）の修正のポイント

8月3日第3回WG1でお示しした見直し方針

フレームワークの考え方の明確化

- 目的、適用範囲、対象、想定する読者等を冒頭で明示
- 価値創造過程の定義や信頼の確保の考え方についてコンセプトの説明を行う部分に記載
- 6つの構成要素で整理する根拠、目的を追記
- マルチステークホルダーの考え方を明記

国際規格等との対応関係の整理

セキュリティ対策例のレベル分け

見直した結果

０．全体構成の見直し

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あり方
第Ⅱ部　ポリシー　：リスク源の洗い出しと対策要件の特定
第Ⅲ部　メソッド　：セキュリティ対策要件と対策例集

１．フレームワークの考え方の明確化

（１）冒頭にフレームワークの使い方等に関する考え方を整理
（２）コンセプトの説明の充実
（３）三層構造アプローチと6つの構成要素を利用したリスク源の洗い出し方法の提示

＜リスク源の洗い出しのポイント＞
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の整理
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により発生する新たなリスクの把握
③ 組織を跨るデータの流通の仕方の把握
④ 各層における信頼性の基点の確保

（４）ユースケースの作成

２．国際規格等との比較

（１）NIST CSF、NIST SP800-171、ISO/IEC 27001の各管理策等と本フレームワークの対策要件の関係の整理
（２）その他、NIST SP800-161等の主な国際規格の内容も参照

３．コストも考慮したレベル別の対策例の作成

（１）High Advanced、Advanced、Basic で対策例を提示

1. 前回WG１以降のサイバー・フィジカル・セキュリティ対策フレームワーク（案）の修正のポイント

2. サイバー・フィジカル・セキュリティ対策フレームワーク（第二案）の概要

3. 今後のスケジュール

サイバー・フィジカル・セキュリティ対策フレームワーク（案）の目次

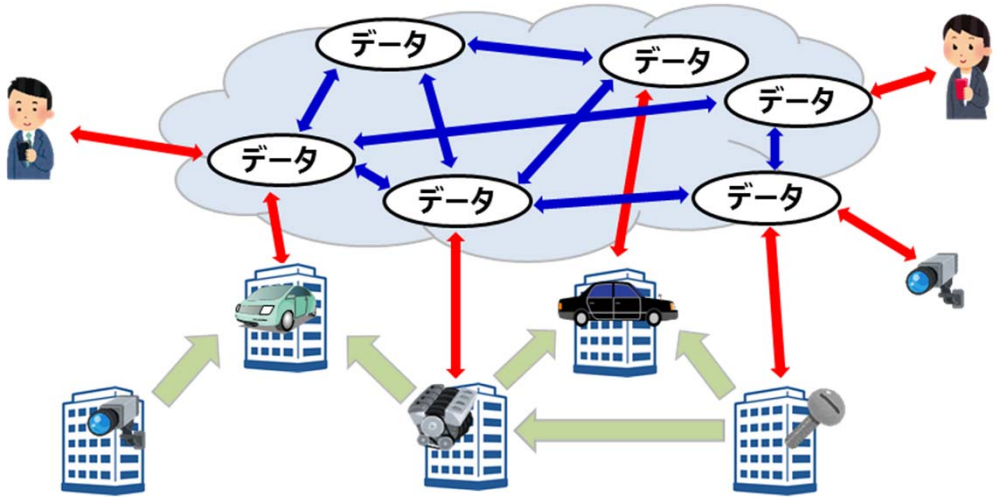
背景：「Society5.0」におけるサプライチェーンの構造変化

- あらゆるものがつながるIoT、データが新たなインテリジェンスを生み出すAIなどにより実現される**「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。**
- 本フレームワークでは、「Society5.0」におけるサイバーとフィジカルの相互作用で新たな付加価値を生み出す**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。

「Society5.0」以前のサプライチェーン

- **個々の企業主体の定型的なつながりが付加価値を生み出す**

「Society5.0」における価値創造過程（バリュークリエイションプロセス）



- **サイバー空間とフィジカル空間の両空間を跨いでモノやデータがつながる**
- **様々な企業や個人等のより柔軟で動的なつながりが付加価値を生み出す**

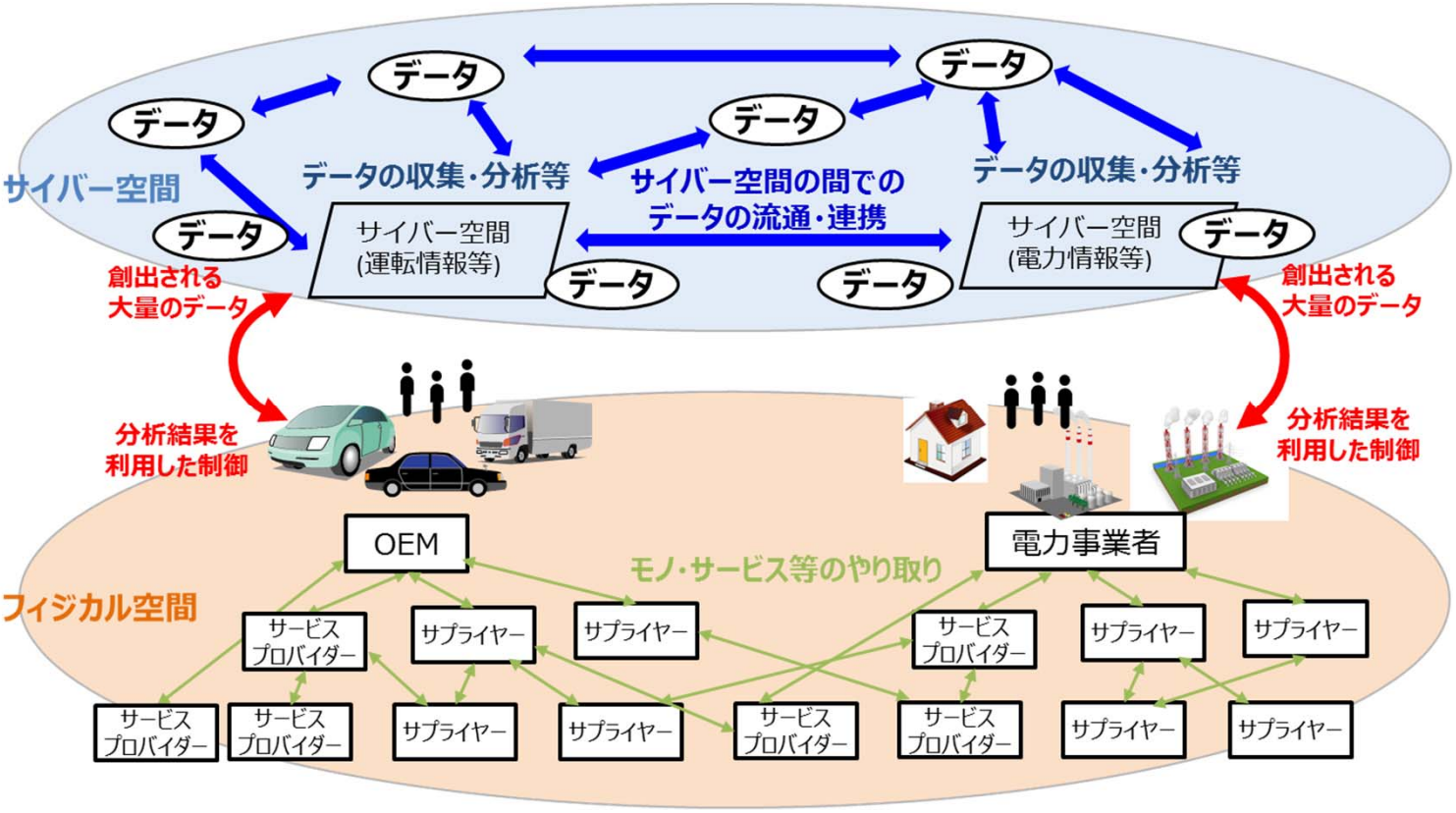
<バリュークリエイションプロセスのセキュリティの前提>

・**「ネットワーク化されず、インターネットにも接続されない」システムと認識していても、**IT機器の小型化・高機能化に伴い、電子機器を含む全てのシステム等が重要性を増し、**フィジカルを通じたサイバー攻撃を受けるなどの懸念も増大しており**、所有する電気機器及びシステムが**本フレームワークの適用範囲に含まれ得る**という認識に立ち、必要なセキュリティ対策を講じる必要がある。

背景：サイバー攻撃の脅威の拡大

- 「Society5.0」における産業社会では、**サイバー攻撃の起点が拡大**するとともに、**複雑につながる新たなサプライチェーン、バリュークリエイションプロセスで影響を受ける範囲が拡大。**
- サイバー空間とフィジカル空間が高度に融合するために、**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**データの転換処理の信頼性確保、大量のデータの正確性・流通・連携を支えるセキュリティ対策**も課題。

Society5.0の社会におけるモノ・データ等の繋がりのイメージ



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

フレームワークの目的と適用範囲

- 「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、**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**し、**産業界が自らのセキュリティ対策に活用できる対策例を『サイバー・フィジカル・セキュリティ対策フレームワーク』**として取りまとめる。
- 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。

サイバー・フィジカル・セキュリティ対策に含まれる対策

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<u>バリュークリエイションプロセス全体が適用範囲</u>**
・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

フレームワークの全体構成、想定読者

- コンセプト、ポリシー、メソッドの三部構成。
- 本フレームワークは、産業社会の全体像を捉えたものであるため、**付加価値を創造する活動に取り組むすべての主体が適用対象。**

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（三層構造アプローチと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。

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	○	○	
• サプライチェーンのマネジメントに関わる戦略・企画部門の担当者 • データマネジメントの担当者	○	○	
• 企業（組織）のセキュリティ担当者		○	○
• 情報関連機器、制御機器の開発・品質保証、システム設計・構築・検証担当者		○	○

フレームワークに期待される効果と特徴

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

- セキュリティ対策の実行による**価値創造過程（バリュークリエイションプロセス）の信頼性確保**
- 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

- 産業社会として目指すべき対策の概念の整理だけではなく、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適切な水準の対策例を示すことでコストの関係を把握できるようにする

- バリュークリエイションプロセス全体を構成する中小企業を含めた事業者が実際にセキュリティ対策を実施できる、リスク源と必要な対策の関係を明らかにし、できるだけコストがイメージできるような内容にする。
- リスクベースの考え方を踏まえ、事業者が適切なセキュリティ対策を選択することで、セキュリティレベルを保ったままでコストを圧縮する工夫ができるようにする。

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把握し、米欧などの主要な規格との整合性を確保し、こうした規格を踏まえた各国の認証制度との相互承認を進めていくことができる内容にする。
- 本フレームワークでは、国外の規格との関係を整理した対比表も用意しており、日本国内におけるサイバーセキュリティの取組が、そのまま国外においても一定水準を満たしていることを示すことができるとともに、国外における取組が、日本国内においても一定水準を満たしていることを示すことができるようになっている。

フレームワークの使い方

- 「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。
- **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産業分野や企業により異なる**ため、実際のセキュリティ対策では、産業分野の持つ特徴を踏まえる必要がある。

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とし、各組織で取り組んでいる付加価値創造活動におけるセキュリティモデルを構築
- 各組織のリスク源の明確化

各組織におけるセキュリティポリシーの策定、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
- 国際規格等との比較

各組織、業界等における信頼のチェーンの構築

- 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、一つ一つの付加価値の創造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

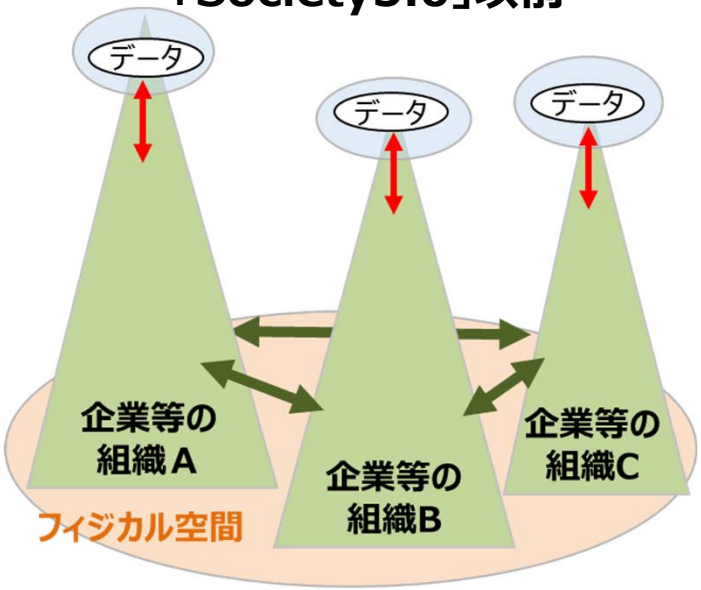
サイバー空間とフィジカル空間が高度に融合した産業社会における産業分野のサイバーセキュリティの在り方

「Society5.0」型サプライチェーン
”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

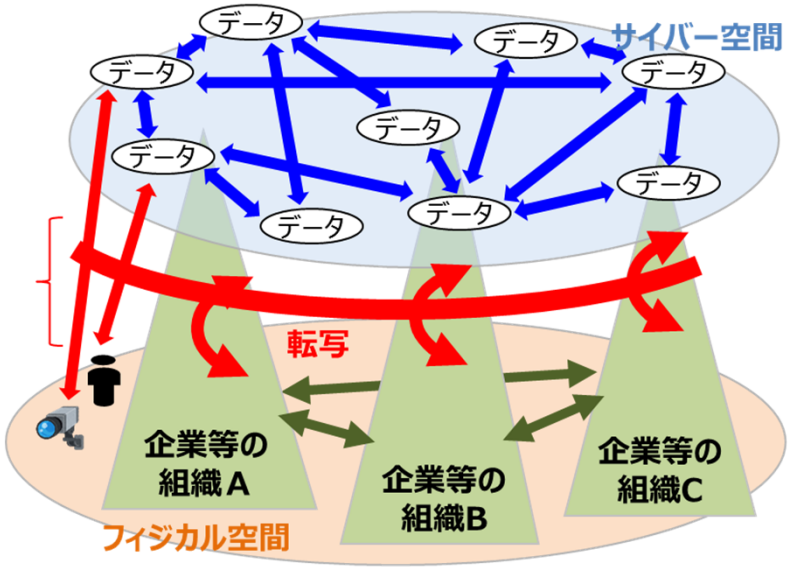
- 従来のサプライチェーンでは、セキュリティを確保した組織間の取引であれば、プロセス全体のセキュリティも確保される。
- 「Society5.0」という**サイバー空間とフィジカル空間が一体化した産業社会においては、自組織のセキュリティ確保だけではバリュークリエイションプロセスのセキュリティを確保することは困難。**
- バリュークリエイションプロセス全体のセキュリティ確保に必要な、**信頼性の基点を明確にするに新たなモデルが必要。**

サプライチェーン構造の変化のイメージ

「Society5.0」以前



「Society5.0」



- **信頼できる組織間のモノ・データの交換が中心であり、モノ・データ等の責任をとる組織が明確**
- **信頼が確認できないヒト・モノとのデータの交換が行われる等、モノ・データ等の責任をとる組織・ヒトが不明確**

三層構造アプローチ

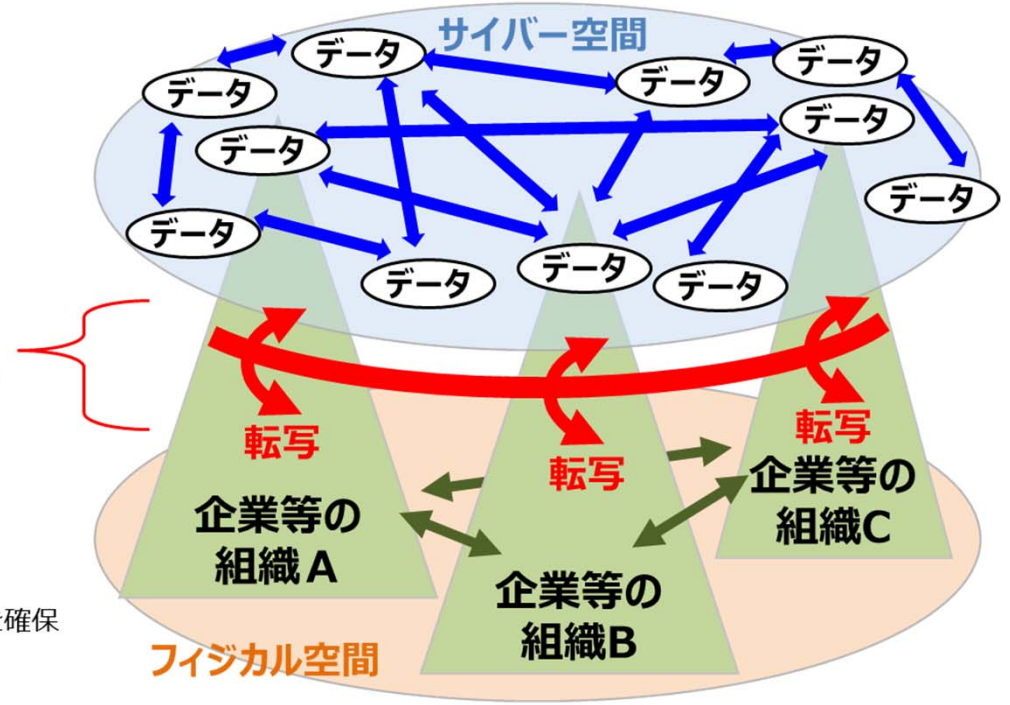
～バリュークリエイションプロセスのセキュリティを確保するための信頼性の基点を設定するためのモデル～

- **本フレームワークでは、バリュークリエイションプロセスが営まれる産業社会を、３つの層に整理**して捉え、**信頼性の基点を明確にする。**
- それぞれの層には、バリュークリエイションプロセスにおいて、信頼性が確保されなければならない機能・役割が存在する。
  - **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、**要求される正確性に応じて適切に情報が変換される“転写”機能**
  - **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

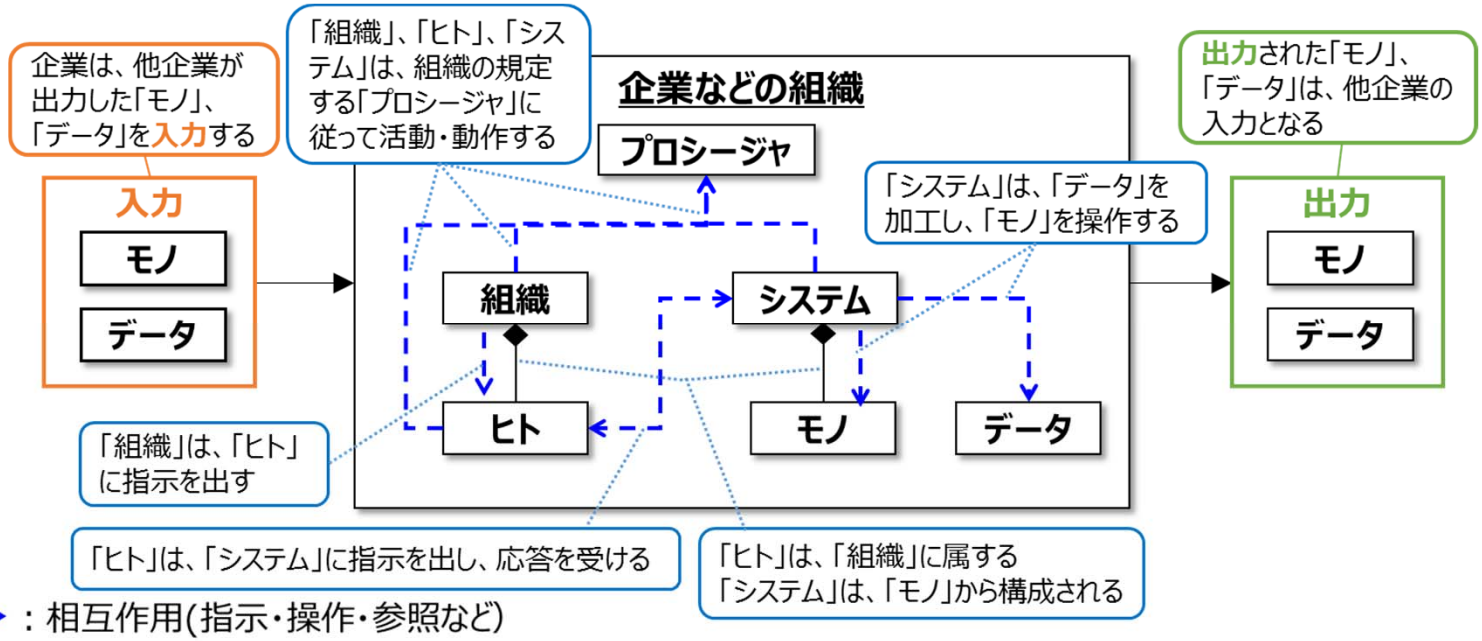


６つの構成要素

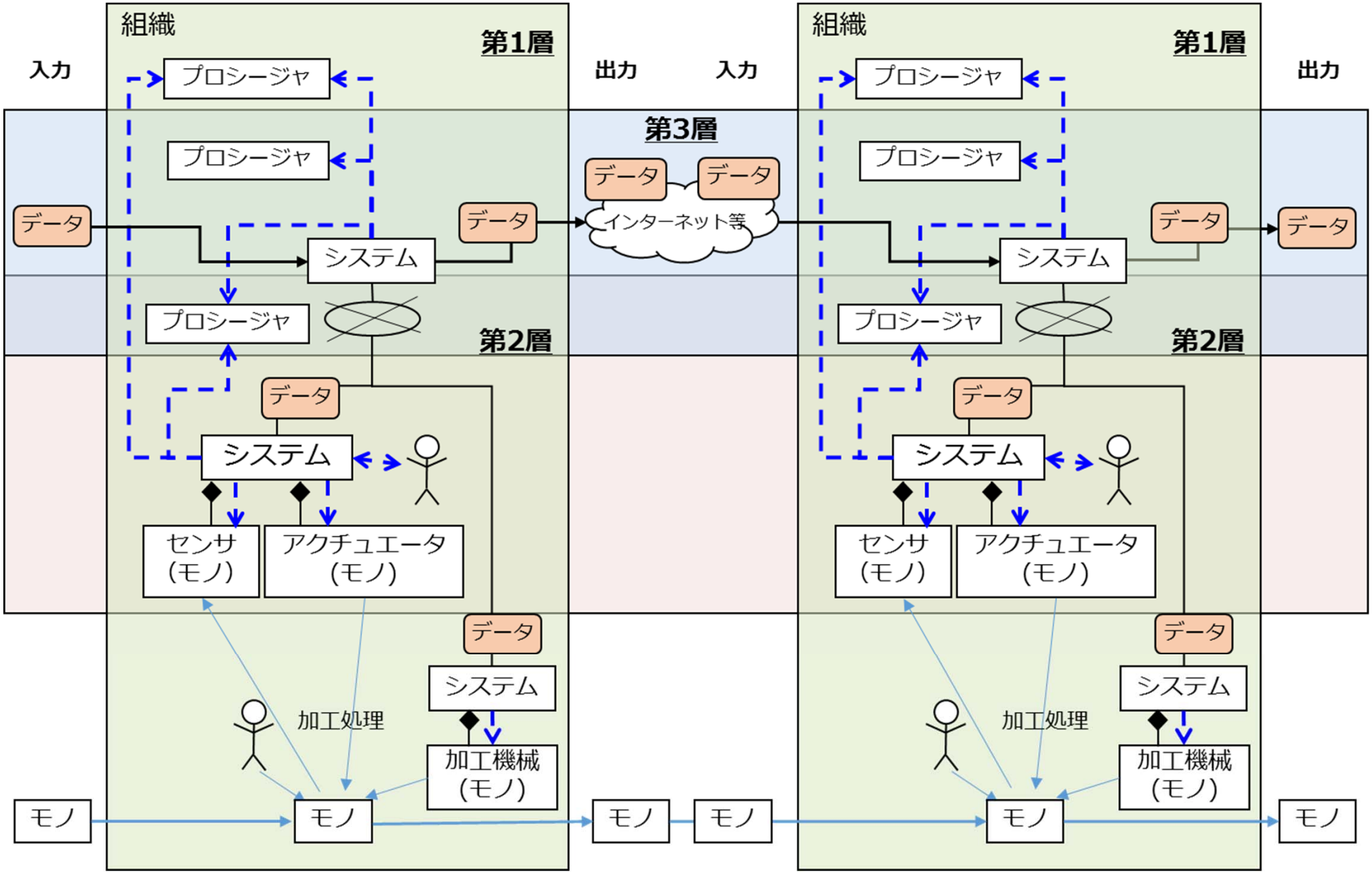
～動的で柔軟なバリュークリエイションプロセスの構成要素を抽象化して捉える～

- 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
組織	• 価値創造過程に参加する企業・団体	**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	• 組織に属する人、及び価値創造過程に直接参加する人	**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

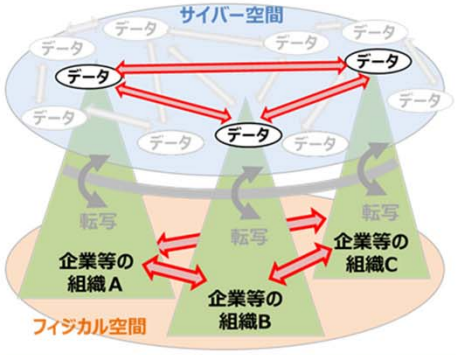
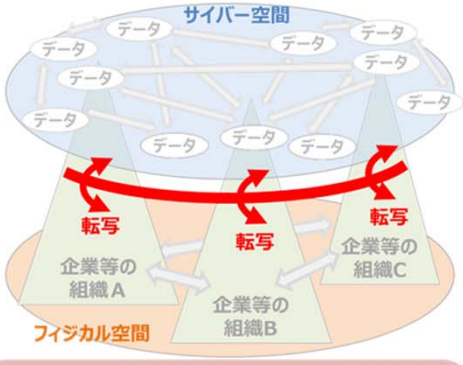
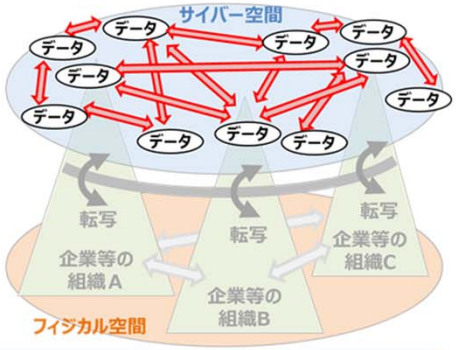


（参考）三層構造における6つの構成要素の関係



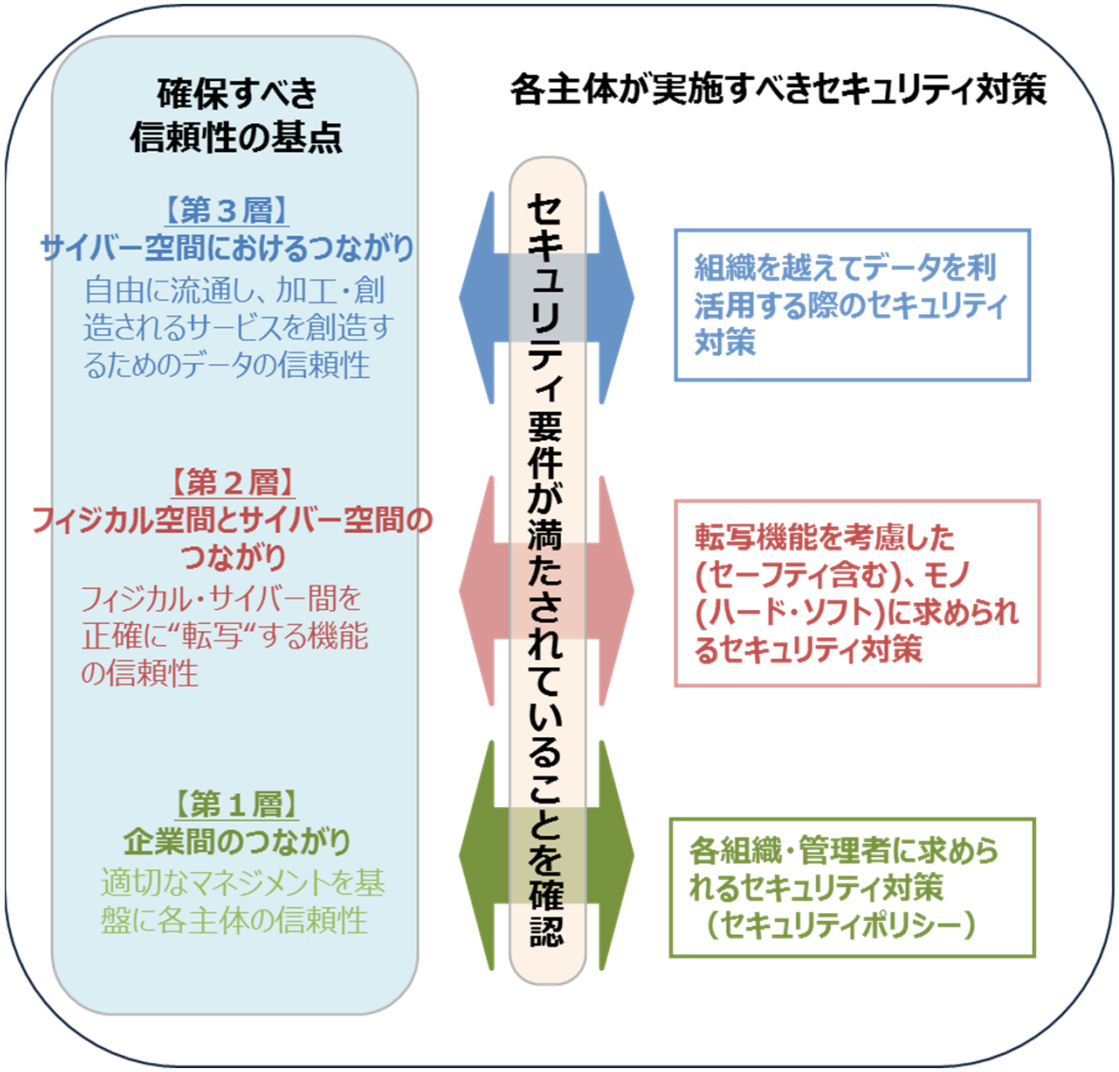
バリュークリエイションプロセスにおけるリスク源と対応する方針の整理

- 各層ごとに守るべきもの、セキュリティ事象、リスク源を整理し、どのような対策を講じるかを整理。

	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
セキュリティ事象	• 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	• 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（構成要素ごとに整理）	■ 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

フレームワーク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。



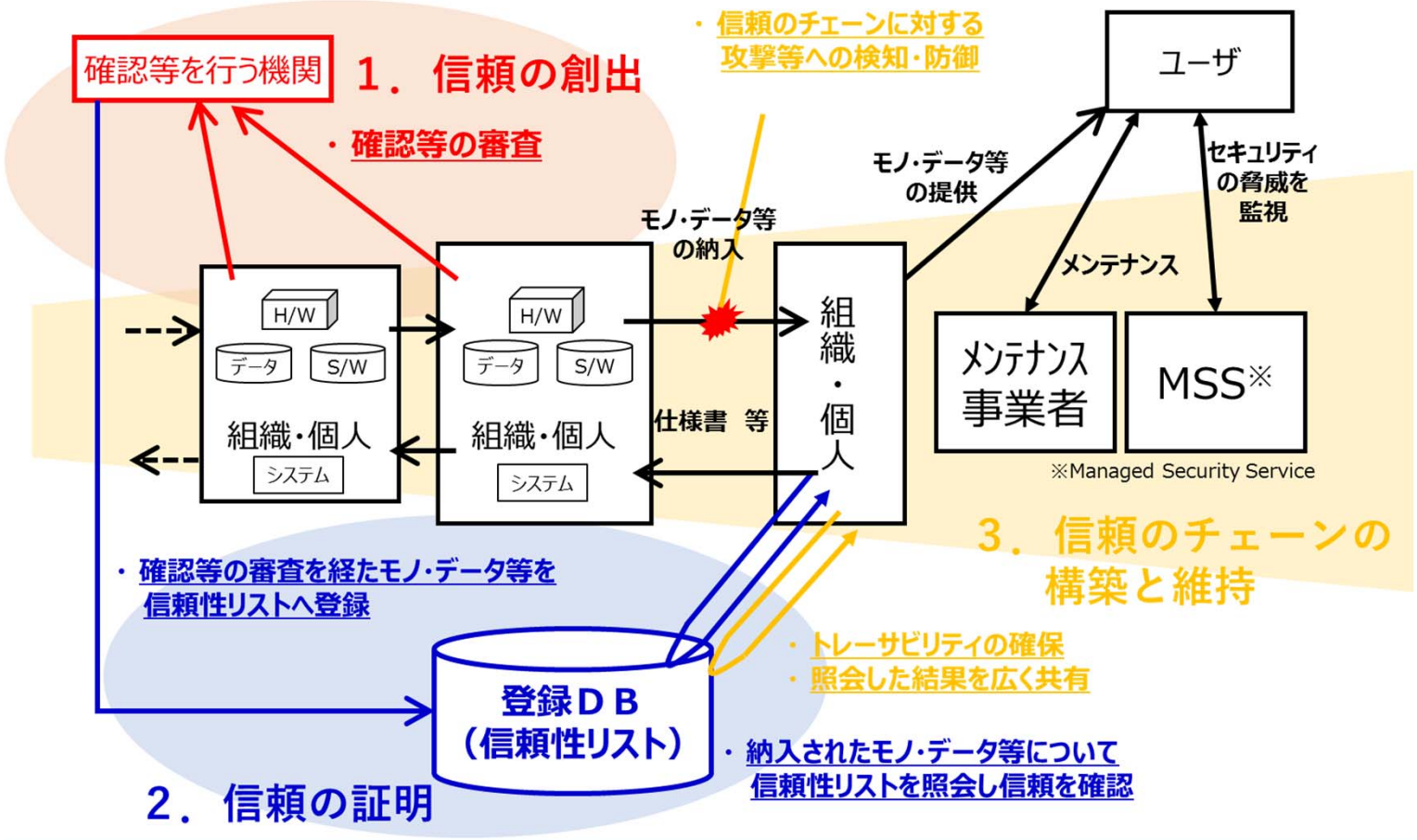
バリュークリエーションプロセス全体の信頼性の確保

（１）信頼の創出
- 確認できること

（２）信頼の証明
- 確認をした主体以外が照会できること

（３）信頼のチェーンの構築と維持
- 照会した結果が広く共有されていること

（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



1．信頼の創出（例）

- セキュリティ対策要件を満たすモノ・データ等の生成、その生成物の記録の保存
- 対象のモノ・データ等がセキュリティ要件を満たした形で生成されたことの自己確認／第三者による認証　等

2．信頼の証明（例）

- 対象のモノ・データ等がセキュリティ要件を満たした形で生成されたものであることを、生成主体以外の者も照会できるリスト（信頼性リスト）の作成と管理
- 信頼性リストを照会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（例）

- 信頼の創出と証明を繰り返すことによる信頼のチェーンの構築（信頼性リスト間でお互いの信頼性が確認され、それによってトレーサビリティを確保すること　等）
- 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

第Ⅱ部　ポリシー
リスク源の洗い出しと対策要件の特定

三層構造アプローチを活用したセキュリティ・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）の中も踏まえた、**本フレームワーク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。**
- **三層構造アプローチ、6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。**

■ 分析対象の明確化
- 分析範囲の決定と資産の明確化
- システム構成の明確化
- データフローの明確化

■ 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
- 事業被害レベルの定義
- 想定されるセキュリティインシデントの具体化及び事業被害レベルの割り当て

■ リスク分析の実施
- 自組織に対する攻撃シナリオの検討
- 事業被害レベルの評価
- 脅威の特定及び評価
- 対策／脆弱性の特定及び評価　等

■ リスク対応の実施
- 改善箇所の抽出、選定
- リスクの低減
- リスク低減効果の把握　等

本フレームワークの考え方を踏まえたリスクマネジメントで考慮すべき点

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**

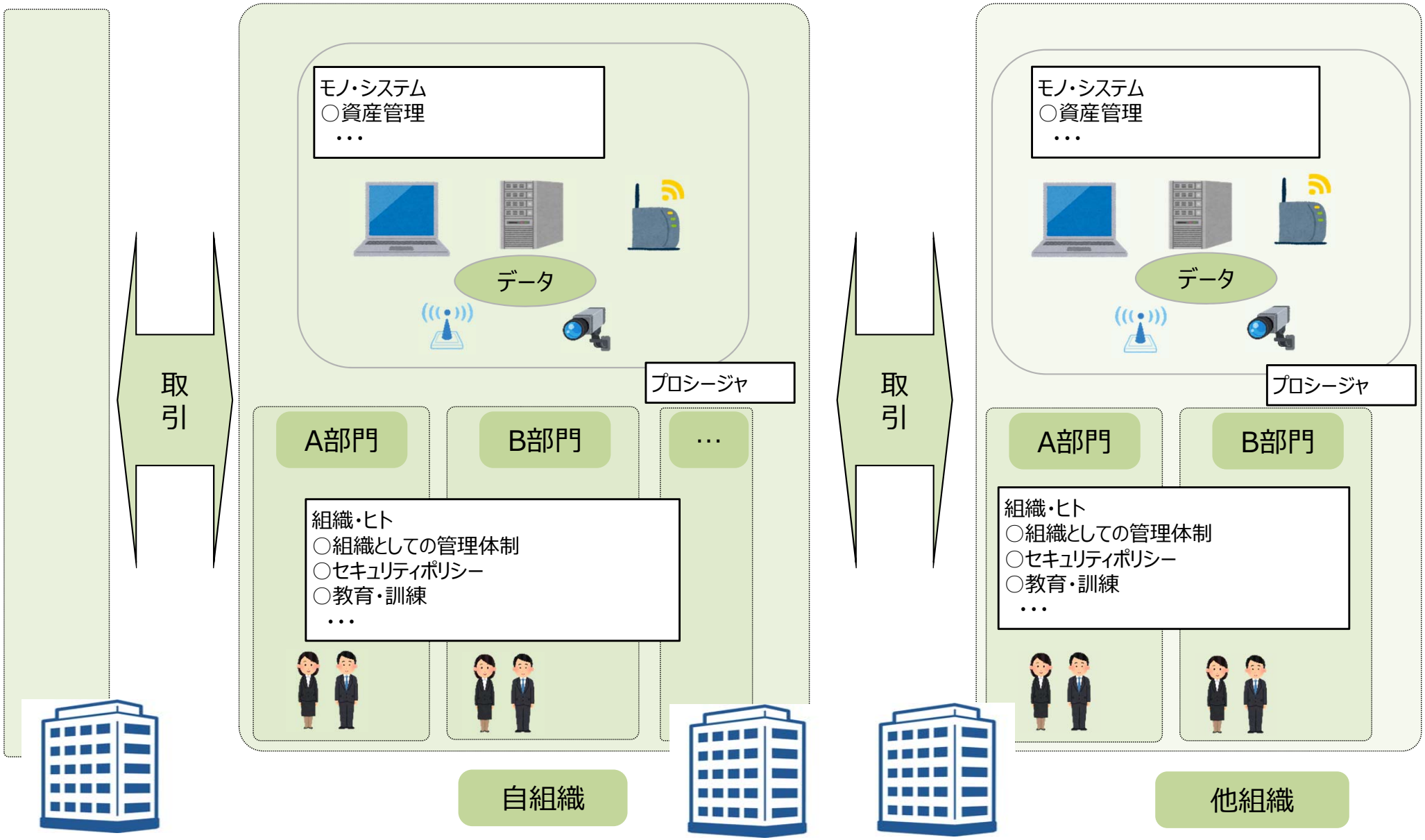
④ **各層における信頼性の基点の確保**

分析対象の明確化：三層の特性と含まれる分析対象のイメージ

- 分析対象の明確化にあたり、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。

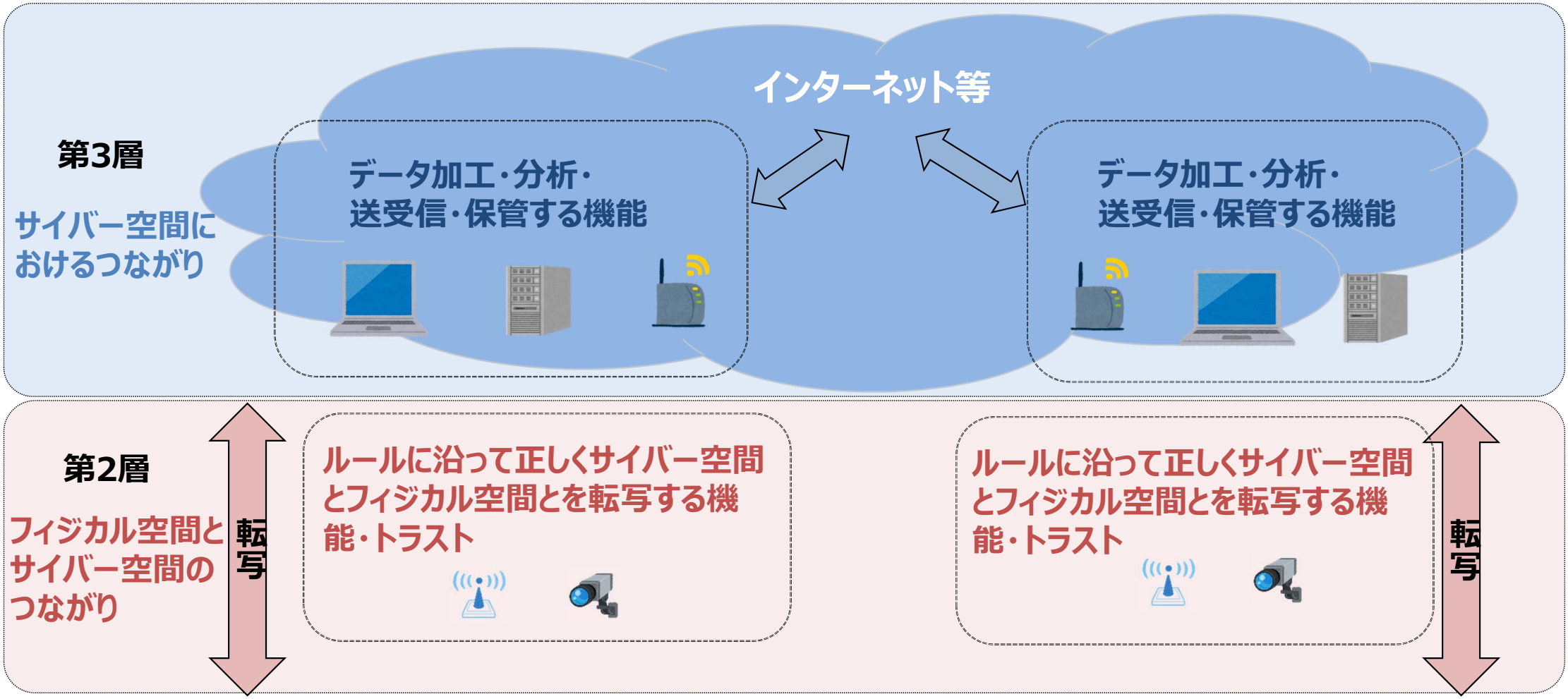
階層	各層の特性	各層の機能・役割	分析対象	分析対象の具体的イメージ
第1層	個々の組織の適切なガバナンス・マネジメントによって信頼を維持	• 組織として平時のリスク管理体制を構築し、適切に運用すること • 組織としてセキュリティインシデント発生時においても適切に自組織の事業を継続すること • フィジカル空間での製品・サービスが、望まれる品質を備えて入荷又は出荷されること **【セキュリティ要件】** 組織単位のセキュリティポリシーを定めて維持 **【信頼性の基点】** 組織・マネジメント	• 組織等で管理されるヒト・モノ・データ・プロシージャ・システム • 上記の要素が管理される場所 • 組織内でのデータの流通	• 社員、従業員 • 企業のＩＴ資産 • 企業のセキュリティポリシー • 企業間の契約　等
第2層	IoT機器を介して、フィジカル空間とサイバー空間とのつながりが増大	• フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、第三層へ送る機能 • サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりするように表示したりする機能 **【セキュリティ要件】** サイバー空間とフィジカル空間との間の転写におけるセキュリティの確保 **【信頼性の基点】** ルールに沿って正しくサイバー空間とフィジカル空間とを転写する機能・トラスト	• 転写する機能に関わる組織・ヒト • ルールに沿って正しくサイバー空間とフィジカル空間を転写する機能を備えるモノ・システム • 転写に関するデータ • 転写するプロシージャ	• アクチュエータ、センサ、コントローラ、医療機器、ECU、３Dプリンタ、監視カメラ、パソコン（入力機器として）、スマートメータ（検針機器として）　等
第3層	サイバー空間にて自組織のデータだけでなく、組織を超えて多様かつ大量なデータを収集・蓄積・加工・分析	・データを送受信する機能 ・データを加工・分析する機能 ・データを保管する機能 **【セキュリティ要件】** サイバー空間におけるデータの送受信等におけるセキュリティを確保すること **【信頼性の基点】**データ	• 組織を越えてやりとりするデータを扱う組織・ヒト • データを送受信、加工、分析、保管するモノ・システム • 組織を越えて流通するデータ • 組織を越えてデータを扱う際の共通のルール・プロシージャ	• サーバ、ルータ、スマートメータ（検針データの送信機器として） • オープンデータ／限定提供データ　等

分析対象の明確化①：第１層の抽象化モデルの構築

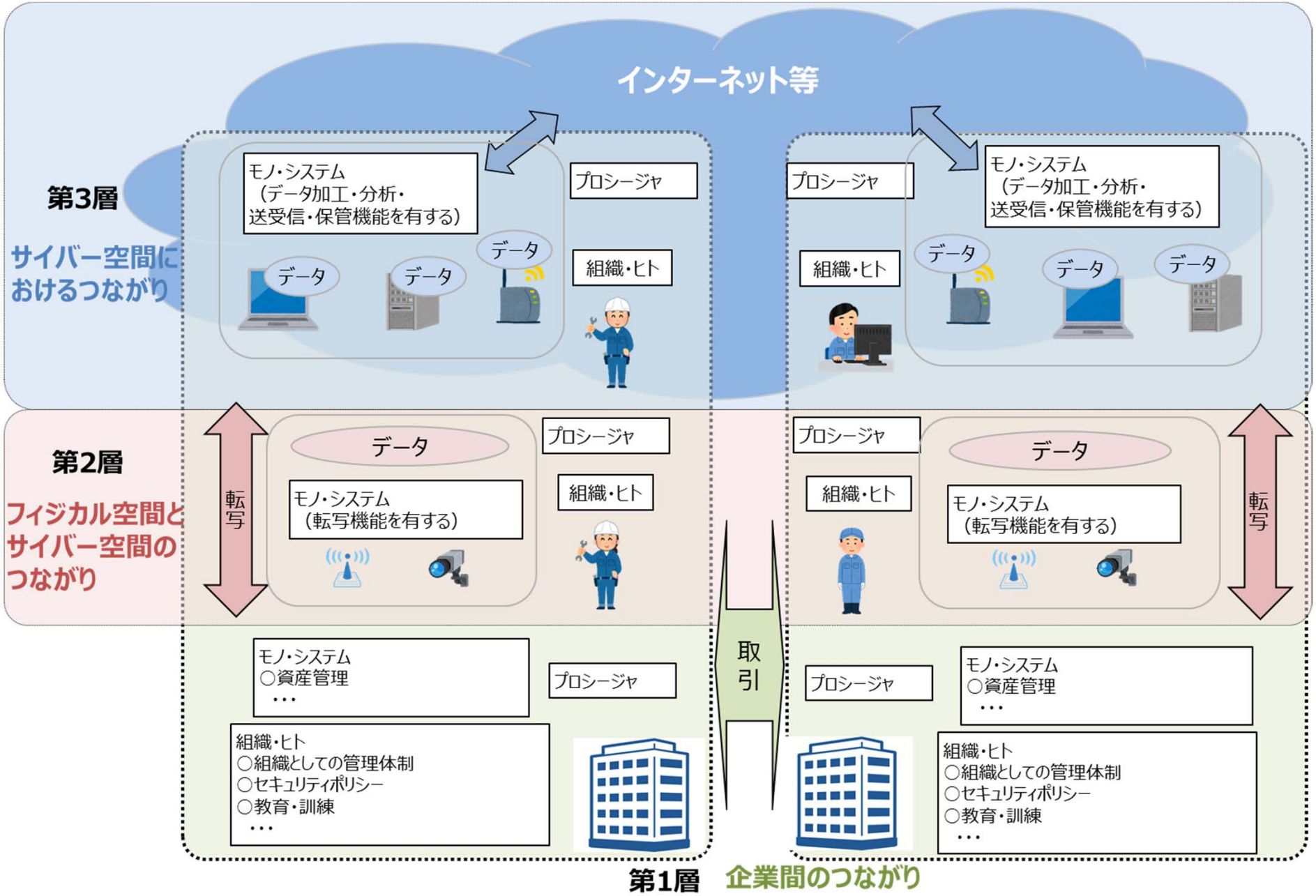


第1層 企業間のつながり

分析対象の明確化②：第２層、第３層の機能を確認



分析対象の明確化③：
第１層のモデルに、第２層、第3層の機能との関連付けを実施することで、三層構造モデルの分析対象の構築



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（守るべきもの）とそれに対する悪影響のイメージ

- 三層構造アプローチ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	• 組織として平時のリスク管理体制を構築し、適切に運用すること • 組織としてセキュリティインシデント発生時においても適切に自組織の事業を継続すること • フィジカル空間での製品・サービスが、望まれる品質を備えて入荷又は出荷されること	• **法制度等への不準拠** • **セキュリティインシデントの発生**：情報資産の棄損(漏洩/改ざん/破壊/利用停止) • **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(稼動停止、誤ったアウトプット等)
第2層	• フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、第３層へ送る機能 • サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりするように表示したりする機能	• **機器の機能停止**：IoT機器の稼動が停止すること • **信頼性の低い稼動**：IoT機器が意図した稼動をしないこと ✓ 安全面に問題のある稼動 ✓ 誤計測
第3層	• データをセキュアに加工・分析する機能 • データをセキュアに保管する機能 • データをセキュアに送受信する機能	• **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**：データ処理側でのセキュリティインシデントによる情報資産の棄損(漏洩/改ざん/破壊/利用停止) • **信頼性の低い稼動**：データ関連サービスが意図した稼動をしないこと(誤動作、停止等)

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

- 守るべきものとそれに対する悪影響の考え方を踏まえ、**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	1. 平時のリスクマネジメントプロセスに支障があり、セキュリティインシデント（情報資産の漏えい／改ざん／破壊／利用停止）が発生する 2. セキュリティに係る法制度等の規定内容を遵守できない 3. セキュリティ事象による被害が拡大し、自組織及び関係する他組織が適切に事業継続できない
第2層	1. セキュリティに係る攻撃を受けたIoT機器の意図しない動作 2. IoT機器の動作（正常動作・異常動作を問わない）による安全面に問題のある事象の発生（機器の破損、従業員への物理的危害、業務への悪影響等） 3. IoT機器によるサイバー空間へのフィジカル空間の状況の適切でない転写（誤計測）
第3層	1. サイバー空間にて取り扱われる保護すべきデータが漏えいする 2. サイバー空間にて取り扱われる保護すべきデータが改ざんされる 3. サイバー空間にて取り扱われる保護すべきデータ及びデータを収集／加工／蓄積／分析するシステムが意図しない動作（停止等）をする 4. サイバー空間上のデータの取り扱いに係る法規制や一部の関係者のみで共有するデータについて求められるセキュリティ水準を満たせない

リスク分析・リスク対応の実施（添付Ｂの活用）

- 添付Ｂに**想定されるセキュリティインシデントと、当該インシデントの発生を助長・被害拡大の可能性がある脅威・典型的な脆弱性との対応関係**を整理。**リスク分析**の際に、検討するリスク源の抽出や過不足のチェックに活用可能。
- 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することが可能。**

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#
		脅威	脆弱性#	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、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_SYS	【システム】 ・IoT機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	サービス不能攻撃等のサイバー攻撃を受けた場合でも、サービス活動を停止しないよう、モノ、システムに十分なリソース(処理能力、通信帯域、ストレージ容量)を確保する	CPS.DS-4

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に対策要件に対応した、セキュリティ対策例集、他の主要国際規格等との関係性を整理。
- 添付Dに主要国際規格から見た場合の対応関係を整理。
- リスクアセスメントの結果とこれらの対策例を活用することで、グローバルハーモナイゼーションを意識しつつ、セキュリティ対策の必要性を踏まえた適切な水準の対策の実装を進めることができる。

主要国際規格との対応関係

対策要件ID	対策要件	対策例	NIST SP800-171	NIST SP800-53	ISO/IEC 27001 付属書A
CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	<High Advanced> • 組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。	○	○	○
		<Advanced> • 組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。	○	○	
		<Basic> • 組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。	○	○	

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	概要	NIST CSF ver.1.1 対応カテゴリー
資産管理	CPS.AM	組織が事業目的を達成することを可能にするデータ、ヒト、モノ、システム、施設等を特定し、自組織のリスク戦略との相対的重要性に応じた管理をする。	ID.AM (Asset Management)
ビジネス環境	CPS.BE	自組織のミッション、目標、利害関係者、活動を理解し、優先順位付けを行う。この情報はサイバーセキュリティ上の役割、責任、リスク管理上の意思決定を伝達するために使用される。	ID.BE (Business Environment)
ガバナンス	CPS.GV	自組織に対する規制、法律、リスクと、自組織の環境、運用上の要求事項を管理しモニタリングするためのポリシー、手順、プロセスを理解し、サイバーセキュリティリスクの管理者に伝達する。	ID.GV (Governance)
リスク評価	CPS.RA	組織は自組織の業務（ミッション、機能、イメージ、評判を含む）、資産、個人に対するサイバーセキュリティリスクを把握する。	ID.RA (Risk Assessment)
リスク管理戦略	CPS.RM	自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用する。	ID.RM (Risk Management Strategy)
サプライチェーンリスク管理	CPS.SC	組織の優先順位、制約、リスク許容値、および想定が、サプライチェーンリスク管理に関連するリスクの決定を支援するために確立され、利用される。組織は、サプライチェーンのリスクを特定、評価、管理するプロセスを確立し、実施する。	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	資産および関連施設への論理的・物理的アクセスを、承認された組織、ヒト、モノ、プロシージャに限定し、承認された活動およびトランザクションに対する不正アクセスのリスクの大きさに合うよう管理する。	PR.AC (Identity Management and Access Control)
意識向上およびトレーニング	CPS.AT	自組織の職員およびパートナーに対して、関連するポリシー、手順、契約に基づいた、サイバーセキュリティに関連する義務と責任を果たすために、サイバーセキュリティ意識向上教育と、訓練を実施する。	PR.AT (Awareness and Training)
データセキュリティ	CPS.DS	データと記録をデータの機密性、完全性、可用性を保護するために定められた自組織のリスク戦略に従って管理する。	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	（目的、範囲、役割、責任、経営コミットメント、組織間の調整を扱う）セキュリティポリシー、プロセス、手順を維持しシステムと資産の保護の管理に使用する。	PR.IP (Information Protection Processes and Procedures)
保守	CPS.MA	産業用制御システムと情報システムの構成要素の保守と修理をポリシーと手順に従って実施する。	PR.MA (Maintenance)
保護技術	CPS.PT	関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティとレジリエンス、セーフティを確保するための、技術的なソリューションを管理する。	PR.PT (Protective Technology)
異常とイベント	CPS.AE	異常な活動を検知し、事象がもたらす可能性のある影響を把握する。	DE.AE (Anomalies and Events)
セキュリティの継続的なモニタリング	CPS.CM	セキュリティ事象を検知し、保護対策の有効性を検証するために、システムと資産をモニタリングする。	DE.CM (Security Continuous Monitoring)
検知プロセス	CPS.DP	異常なセキュリティ事象を正確に検知するための検知プロセスおよび手順を維持し、テストする。	DE.DP (Detection Processes)
対応計画	CPS.RP	検知したセキュリティインシデントに対応し、適切に自組織の事業を継続しつつ、影響を受ける資産やシステムを復元できるよう、対応・復旧のプロセスおよび手順を実施し、維持する。	RS.RP (Response Planning) RC.RP (Recovery Planning)
伝達	CPS.CO	例えば法執行機関のような組織からの支援を得られるよう、内外の利害関係者(例えば、取引先、JPCERT/CC、他組織のCSIRT、ベンダー)との間で対応・復旧活動を調整する。	RS.CO (Communications) RC.CO (Communications)
分析	CPS.AN	効率的な対応を確実にし、復旧活動を支援するために、分析を実施する。	RS.AN (Analysis)
低減	CPS.MI	セキュリティ事象の拡大を防ぎ、その影響を緩和し、セキュリティインシデントを解消するための活動を実施する。	RS.MI (Mitigation)
改善	CPS.IM	現在と過去の意思決定／対応活動から学んだ教訓を取り入れることで、自組織の対応・復旧活動を改善する。	RS.IM (Improvements) RC.IM (Improvements)

1. 前回WG1以降のサイバー・フィジカル・セキュリティ対策フレームワーク（案）の修正のポイント

2. サイバー・フィジカル・セキュリティ対策フレームワーク（第二案）の概要

3. 今後のスケジュール

これまでの取組と今後のスケジュール（案）

- **『サイバー・フィジカル・セキュリティ対策フレームワーク』（第二案）**について日本語・英語にてパブリック・コメントを実施し、国内外から広く意見を募る。

今後のスケジュールのイメージ