資料5

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』の見直し方針

平成30年10月5日

経済産業省　商務情報政策局

サイバーセキュリティ課

# サイバー・フィジカル・セキュリティ対策フレームワークの見直し方針

- 国内外からのパブリックコメントの意見を踏まえ「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）の記載・構成を以下の観点から見直す。

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

今回のアジェンダ

### 1．フレームワークが提示するモデル

- 価値創造過程
- 3層構造
- 信頼の確保　等

### 2．フレームワークの再構成

- フレームワークの構成
- リスク源と6つの構成要素の関係
- セキュリティ対策例　等

### 3．国際規格等との対応関係の整理

次回のアジェンダ予定

# フレームワーク原案に対するパブリックコメントの主な御意見

- 本年4月、「Society5.0」におけるセキュリティ対策を、サイバー空間とフィジカル空間の関係により社会を3層に分けてモデル化したうえで、『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）』として提示し、パブリックコメントを実施。
- パブリックコメントでは、価値創造過程や3層構造等に関して賛同していただきつつも、より良いものとなるように、フレームワークの構成の見直しや国際規格等との比較を求める御意見をいただいた。

## パブリックコメントでのより分かりやすい記載を求める御意見

### 1．フレームワークが提示するモデルの明確化

- 価値創造過程を3層構造で捉え、セキュリティ上のリスクを的確に洗い出すアプローチに賛同。
- ３層構造で整理する理由、根拠、メリット等をよりわかりやすく説明すべき。
- 信頼の確保が本フレームワークの最終目的であると理解するので、総論の中に明確に位置付けるべき。
- マルチステークホルダーアプローチが、セキュリティの確立と経済活動を促進する最も効率的な手段。

### 2．フレームワークの構成の見直し

- セキュリティ対策の実施者、想定読者をわかりやすいように構成を見直すべき。
- 本フレームワークは、産業界が参照する文書になると考える。セキュリティ対策の十分性を示してほしい。

### 3．国際規格等との対応関係の整理

- 国際規格等との対応付けは、本フレームワークの特徴を示し、世界への説明にも必要。
- 本フレームワークが日本独自のものとならないよう、国際規格等との比較は重要。

# １．フレームワークが提示するモデル

# Society5.0を3層構造の社会モデルで捉えた背景①
# ～従来型のサプライチェーンからSociety5.0型のサプライチェーンへの変化

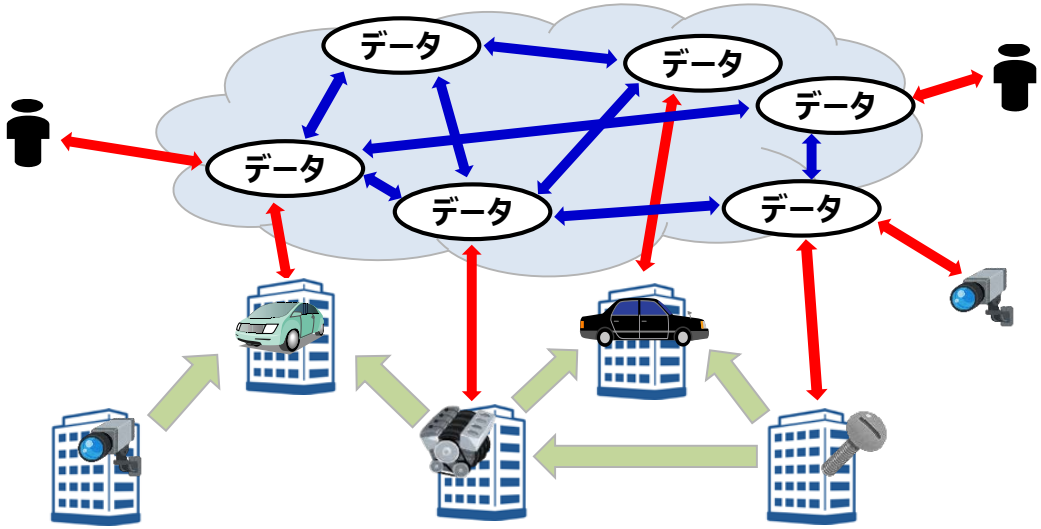
- 「Society5.0」では、企業間・産業間のネットワークが急拡大し、これまで取引を行うことがなかった**主体を新たに巻き込んだ、より柔軟で動的なサプライチェーン**の構成が可能。
- 本フレームワークでは、「Society5.0」におけるサイバー空間とフィジカル空間の相互作用で新たな付加価値を生み出す新たな形のサプライチェーンを**価値創造過程（バリュークリエイションプロセス）**と定義。

**「Society5.0」以前（従来のサプライチェーン）**

部品メーカ　　組立メーカ　　完成メーカ

**個々の企業主体の定型的なつながり（従来のサプライチェーン）で価値を生み出す**

**「Society5.0」（価値創造過程（バリュークリエーションプロセス））**

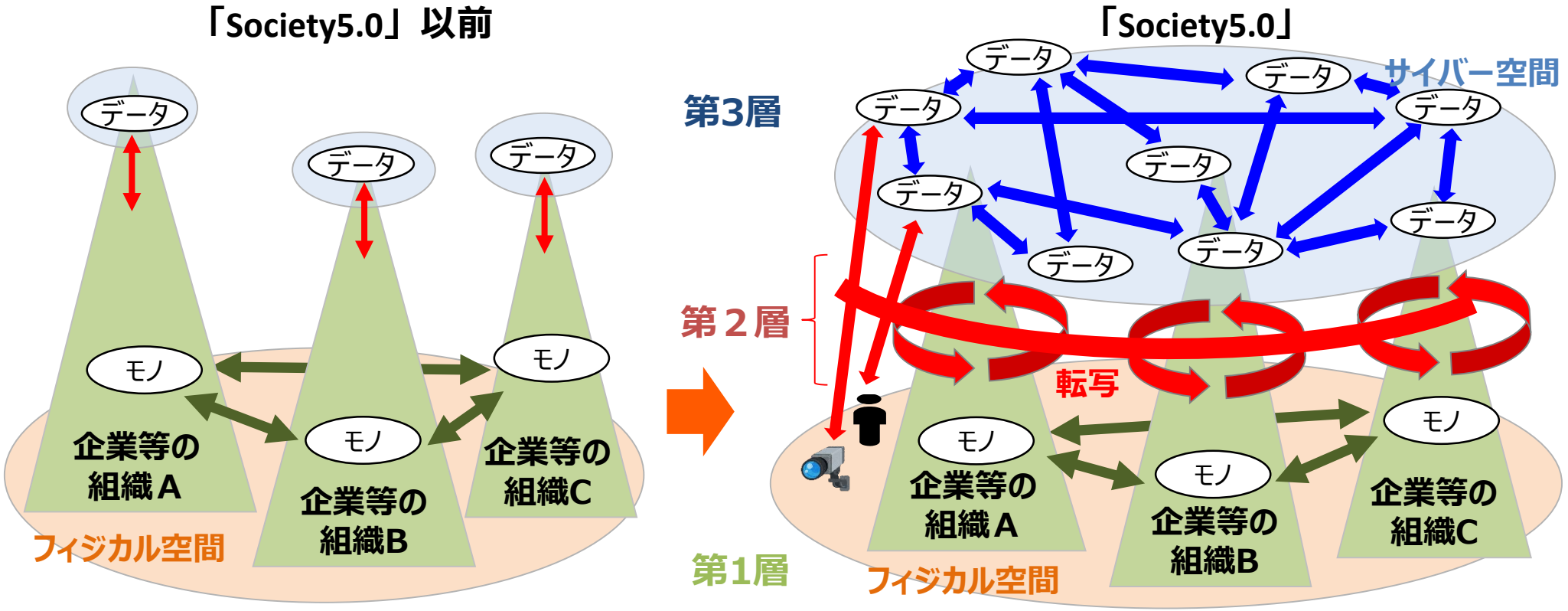



**様々な企業や個人等のより柔軟で動的なつながり（バリュークリエーションプロセス）が価値を生み出す**

**バリュークリエーションプロセスのリスク源を適切に捉えるために、今までと違う新たなモデルが必要**

# Society5.0を3層構造の社会モデルで捉えた背景②
## ～信頼を確認する対象の多様化

- 「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、組織のセキュリティ確保だけでは社会全体の信頼が確保できない。
- このため、信頼を確認する対象の機能で3層構造に分けて社会モデルを構築。



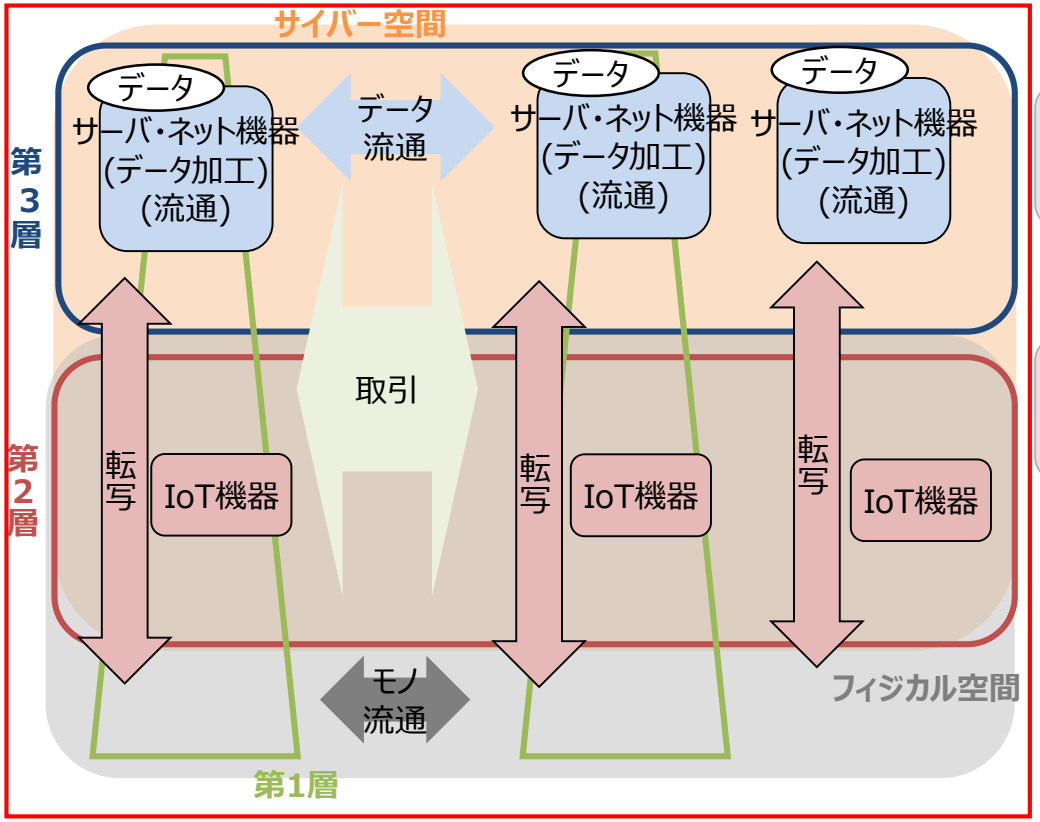

- 信頼できる組織間のモノ・データの交換が中心であり、モノ・データ等の責任をとる組織が明確
- 信頼が確認できないヒト・モノとのデータの交換が行われる等、モノ・データ等の責任をとる組織・ヒトが不明確

# Society 5.0 における各層の特性

| 階層 | 各層の特性 | |
|---|---|---|
| 第3層<br>サイバー空間におけるつながり | 【3】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 | 【3-1】組織や業界をまたいで様々なエンドポイントからデータが収集される<br>【3-2】ストリーミングデータや機密データ等を含む、様々な種類のデータが収集される<br>【3-3】複数のデータソースから取得したデータが統合的な分析のために加工される<br>【3-4】公開データおよび機密データ等を含む自社の蓄積データが、組織や業界をまたいで様々なエンドポイントからアクセスされる可能性がある<br>【3-5】データの加工・分析において、AI等を活用して高度かつ高速なデータ処理がなされる<br>【3-6】サイバー空間におけるデータのサプライチェーンの構成は、動的に変化する |
| 第2層<br>フィジカル空間とサイバー空間のつながり | 【2】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 | 【2-1】ネットワークにつながるライフサイクルの長い機器が増加する<br>【2-2】(遠隔地等にあり)管理が行き届きにくいネットワークにつながる機器が増加する<br>【2-3】ネットワークにつながる機器が様々な場所(重要インフラから家庭まで)に分散する<br>【2-4】サイバー空間からのインプットに基づいて、フィジカル空間において作業を実行する機器が増加する |
| 第1層<br>企業間のつながり（従来型サプライチェーン） | 【1】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 | |

# Society5.0における信頼確保を目指したセキュリティ対策
## ～各機能に着目したマルチステークホルダーによる対策

- 各層や各主体が相互に密接に関係する**「Society5.0」のセキュリティを確保するため**には、従来の個々の組織主体のセキュリティ対策だけでは不十分であり、各層において、**マルチステークホルダーによる対応も含めたセキュリティ対策**が必要。

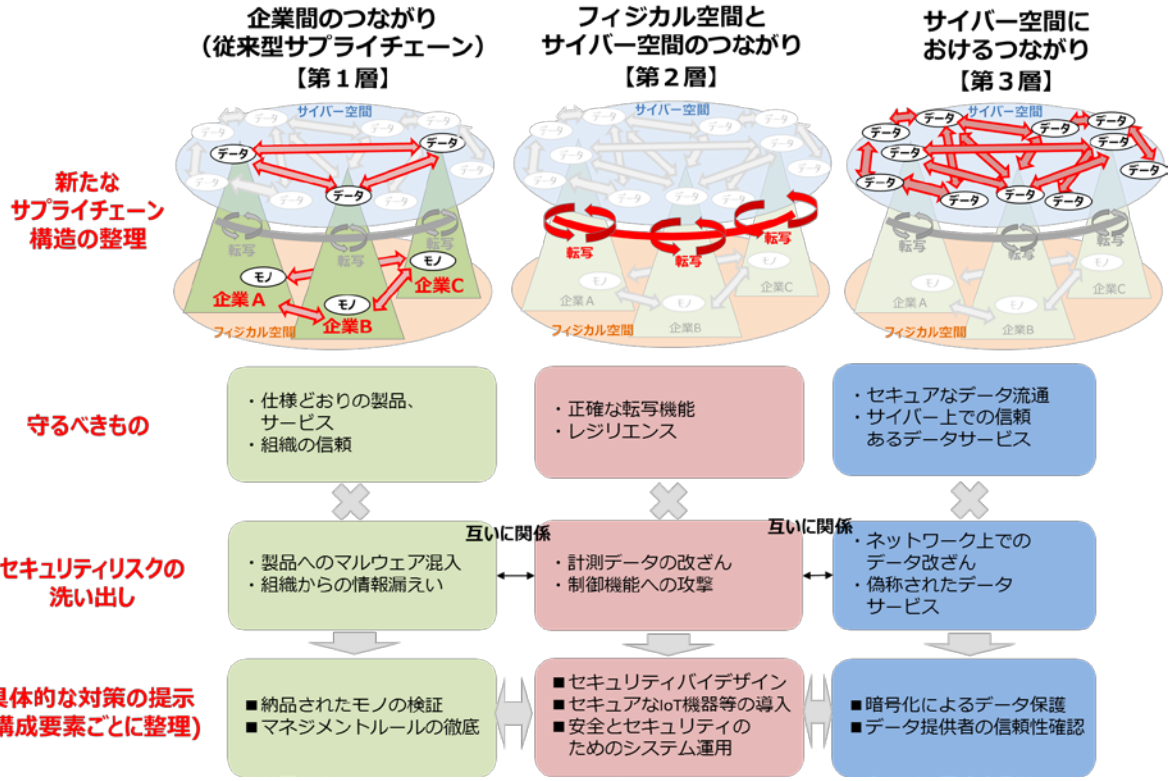



| 信頼を確保すべき対象 | 各主体が実施すべきセキュリティ対策 | 相手の信頼の確認 |
|---|---|---|
| 自由に流通し、加工・創造されるサービスを創造するためのデータの信頼 | データ加工・流通時のセキュリティ対策 | データの信頼の確保 |
| フィジカル・サイバー間を正確に“転写“する機能の信頼 | 転写機能を考慮した(セーフティ含む)、モノ(ハード・ソフト)に求められるセキュリティ対策 | 転写機能の信頼の確保 |
| 適切なマネジメントを基盤に各主体の信頼 | 組織・管理者に求められるセキュリティ対策(マネジメント規格) | 主体の信頼の確保 |

# ２．フレームワークの再構成

# 現在（パブリックコメント版）のフレームワークの構成

- 現在（パブリックコメント版）のフレームワークの構成は、各層を守るべきもので分類し、一つの項目ごとにセキュリティリスクとそれに対するセキュリティ対策を列挙。




**守るべきもので分類**

L1.001セキュリティポリシーの策定、体制の整備

■リスク要因
…
■リスク影響

**リスク**

■対策の概要
…
■対策ポイント
…
■構成要素毎の対策例
〇組織
・自組織の事業におけるミッション、目標、活動に関して優先順位を定め、関係者(サプライヤー、第三者プロバイダ等を含む)に共有する。
〇ヒト
…

**セキュリティ対策**

パブコメの御意見

- セキュリティ対策の実施者、想定読者をわかりやすいように構成を見直すべき。
- 本フレームワークは、産業界が参照する文書になると考える。セキュリティ対策の十分性を示してほしい。

- フレームワークを3部構成にしたうえで、コンセプトの明確化、対策要件やセキュリティ対策例等の特定・整理を行い、より使いやすくなるように修正を実施。

# フレームワークの全体構成の見直し

- 『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**リスク評価に活用するためには、脅威と脆弱性（リスク源）の明確化**が必要。
- また、**企業等が実施する対策の十分性・コストを検討するためには、対策例のレベル分け**が必要。
- こうした観点から、フレームワークの構成を以下のとおり**3部構成に再構成**する。

**【第１部】コンセプト**

**3層構造モデル**

**特性**

- Society5.0社会を3層構造でモデル化
- 各層の特性を示す

**【第２部】ポリシー**

**守るべきもの/セキュリティ事象**

**リスク源（脅威×脆弱性）**

**対策要件**

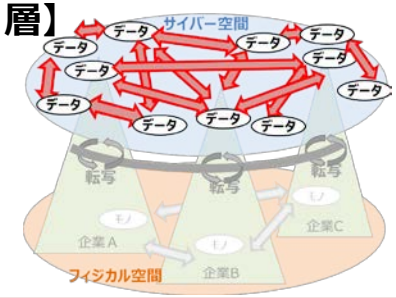
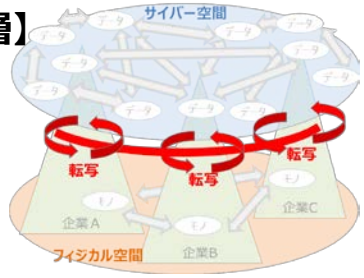
- 脅威、脆弱性を6つの構成要素を用いて特定・整理
- 他の国際規格等と比較しつつ、リスク源や対策要件の十分性に留意

**【第３部】メソッド**

**セキュリティ対策例**

- セキュリティ対策例のレベル分けを実施
- 他の国際規格等と比較しつつ、セキュリティ対策例の十分性に留意

# （第1部）フレームワークの構成
# ~フレームワークが提示する3層構造モデルと特性

| 3層構造モデル | 特性 | 守るべきもの/セキュリティ事象 |
|---|---|---|
| **サイバー空間におけるつながり**<br>【第３層】<br>  <br>**信頼を確保すべき対象**<br>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 | 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 | **【守るべきもの】**<br>• ライフサイクル全体に渡る、データの適切な保護<br>**【セキュリティ事象（例）】**<br>• サイバー空間にて保管された保護すべきデータが漏洩する |
| **フィジカル空間とサイバー空間のつながり**<br>【第2層】<br>  <br>**信頼を確保すべき対象**<br>フィジカル・サイバー間を正確に“転写“する機能の信頼 | 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 | **【守るべきもの】**<br>• サイバー空間/フィジカル空間の間における転写機能<br>• 転写機能を支えるモノ、システムの信頼性<br>**【セキュリティ事象（例）】**<br>• IoT機器の意図しない動作による機器の破損、従業員への物理的危害、業務への悪影響 |
| **企業間のつながり（従来型サプライチェーン）**<br>【第1層】<br>  <br>**信頼を確保すべき対象**<br>適切なマネジメントを基盤に各主体の信頼 | 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が維持 | **【守るべきもの】**<br>• 組織の信頼<br>• 組織間における取引の信頼性<br>**【セキュリティ事象（例）】**<br>• セキュリティインシデントによる被害が拡大し、自組織および関係する他組織が適切に事業継続できない |

# （第2部）フレームワークの構成
# ~リスク源（脅威×脆弱性）と対策要件

**守るべきもの/セキュリティ事象** → **リスク源（脅威×脆弱性）** → **対策要件**

| 階層 | 守るべきもの/セキュリティ事象 | リスク源 | | 対策要件 |
|---|---|---|---|---|
| | | 脅威 | 脆弱性 | |
| 第3層 | **【守るべきもの】**<br>• ライフサイクル全体に渡る、データの適切な保護<br>**【セキュリティ事象（例）】**<br>• サイバー空間にて保管された保護すべきデータが漏洩する | サイバー空間におけるデータの安全な利活用に対する脅威 | サイバー空間における資産または管理策の弱点 | （例）<br>適切なデータの機密区分および区分に応じた管理策を実施する |
| 第2層 | **【守るべきもの】**<br>• サイバー空間/フィジカル空間の間における転写機能<br>• 転写機能を支えるモノ、システムの信頼性<br>**【セキュリティ事象（例）】**<br>• IoT機器の意図しない動作による機器の破損、従業員への物理的危害、業務への悪影響 | フィジカル空間とサイバー空間の間の転写機能に対する脅威 | 転写機能を実現するための資産または管理策の弱点 | （例）<br>受容できない既知のセキュリティリスクの有無を企画・設計の段階から確認し、適宜対策を講じる |
| 第1層 | **【守るべきもの】**<br>• 組織の信頼<br>• 組織間における取引の信頼性<br>**【セキュリティ事象（例）】**<br>• セキュリティインシデントによる被害が拡大し、自組織および関係する他組織が適切に事業継続できない | サプライチェーン全体での事業継続に対するセキュリティに係る脅威 | フィジカル空間における資産または管理策の弱点 | （例）<br>関係する外部組織に対して、契約内容遵守状況を定期的に評価する |

# （第2部）リスク源・脅威・脆弱性等の用語について

- 国際標準(ISO/IEC 27000, ISO 31000)の定義にあわせた表現を採用しつつ、一部表現の変更を行う。

結果

保護対象が「情報セキュリティ」に限定されないことを表現するため、表記を一部変更した。

**セキュリティ事象(security event)**

セキュリティポリシーへの違反若しくは管理策の不具合の可能性，又はセキュリティに関係し得る未知の状況を示す，システム，サービス又はネットワークの状態に関連する事象

**※【元の用語】情報セキュリティ事象(information security event)**

情報セキュリティ方針への違反若しくは管理策の不具合の可能性，又はセキュリティに関係し得る未知の状況を示す，システム，サービス又はネットワークの状態に関連する事象 [ISO/IEC 27000参照]

**リスク源(risk source)**

それ自体又はほかとの組み合わせによって、リスクを生じさせる力を本来潜在的にもっている要素

[ISO31000を参照]

**脅威(threat)**

システムまたは組織に損害を与える可能性がある，望ましくないインシデントの潜在的な原因

[ISO/IEC 27000参照]

**脆弱性(vulnerability)**

一つ以上の脅威によって付け込まれる可能性のある，資産又は管理策の弱点

[ISO/IEC 27000参照]

原因

註①：赤字下線部分は、本フレームワークにおいて新たに定義したい用語

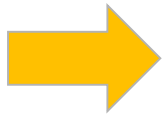
註②：「リスク源」の内容として、一般的には「脅威」および「脆弱性」を指すことが多いが、ISO/IEC 27000内で規定されているわけではない

# （第2部）3層構造における６つの構成要素
## ～脅威・脆弱性・セキュリティ対策例等の特定・整理に利用

- 3層構造に基づく社会モデルにおける構成要素を6つに分類・一般化。

**「Society5.0」以前**

**組織が中心となってモノ・データを管理してサプライチェーンを構成**



**「Society5.0」**

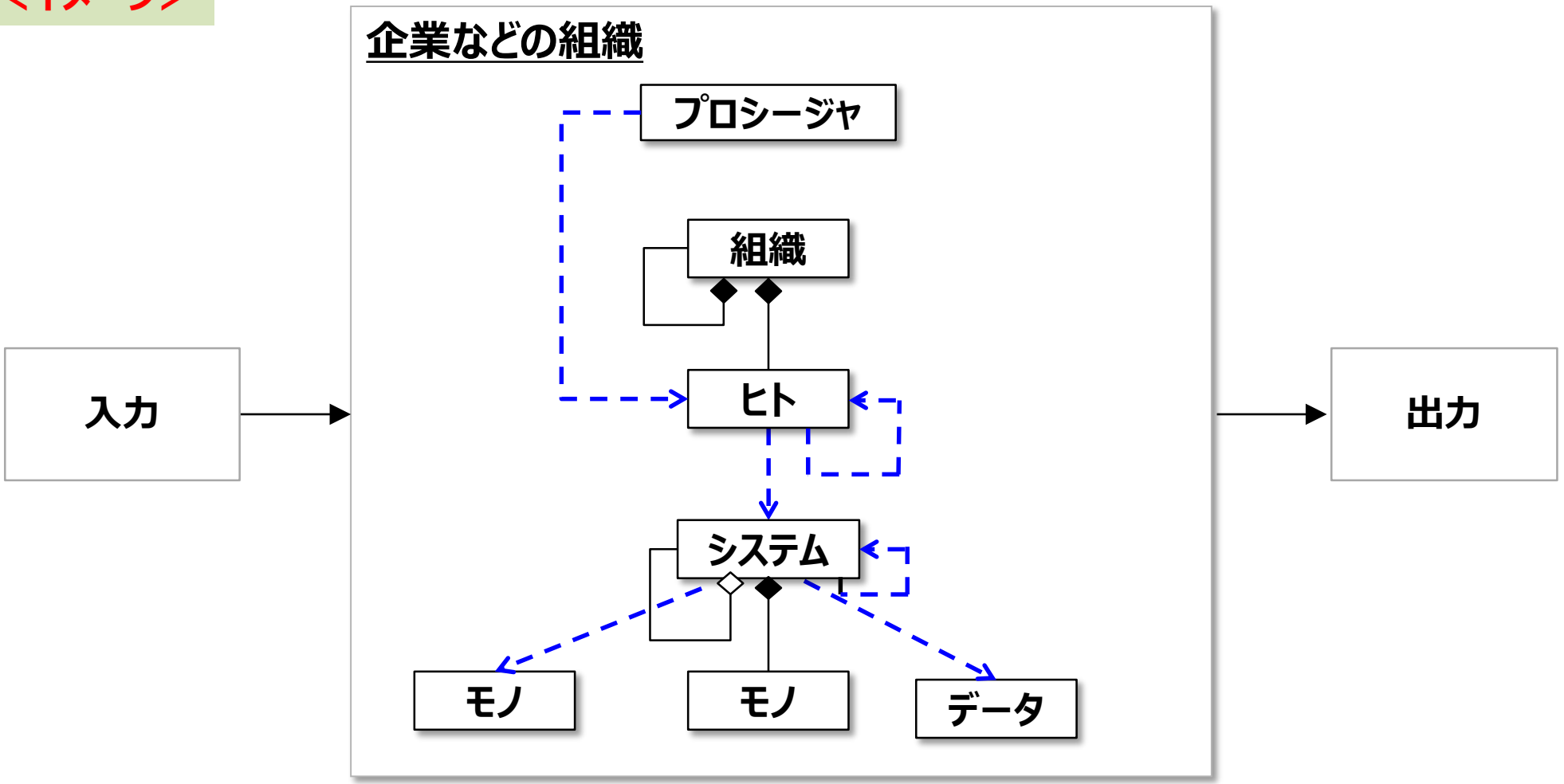
**組織に所属していないヒト・モノ・データ等も価値創造過程に直接参加可能**

| 構成要素 | 定義 | 具体例 |
|---|---|---|
| 組織 | 価値創造過程（特に、従来型サプライチェーン）に参加する企業・団体 | 企業、企業の事業部/本部/部、政府機関、学校 |
| 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 | 従業員、職員、パートタイマー、個人事業主、個人 |
| 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 | PC、サーバ機器、IoT機器、通信機器、スイッチングハブ、ルータ、ネットワークケーブル、CPUとメモリ付きの基板、CPU、メモリ、<br>ソフトウェア、モータ、アクチュエータ、発電機 |
| 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 | 文字データ、数値データ、静止画像データ、動画像データ、<br>システム設定値 |
| 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 | マニュアル、ルール、規則、ポリシー |
| システム | サービスを実現するためにモノで構成される仕組み・インフラ<br><br>【参考】 情報システム：アプリケーション，サービス，IT 資産，及び情報を取り扱う他の構成要素。JIS 27000:2014 | |

※赤字はパブコメ版から追記した個所

# （第2部）3層構造における６つの構成要素の関係

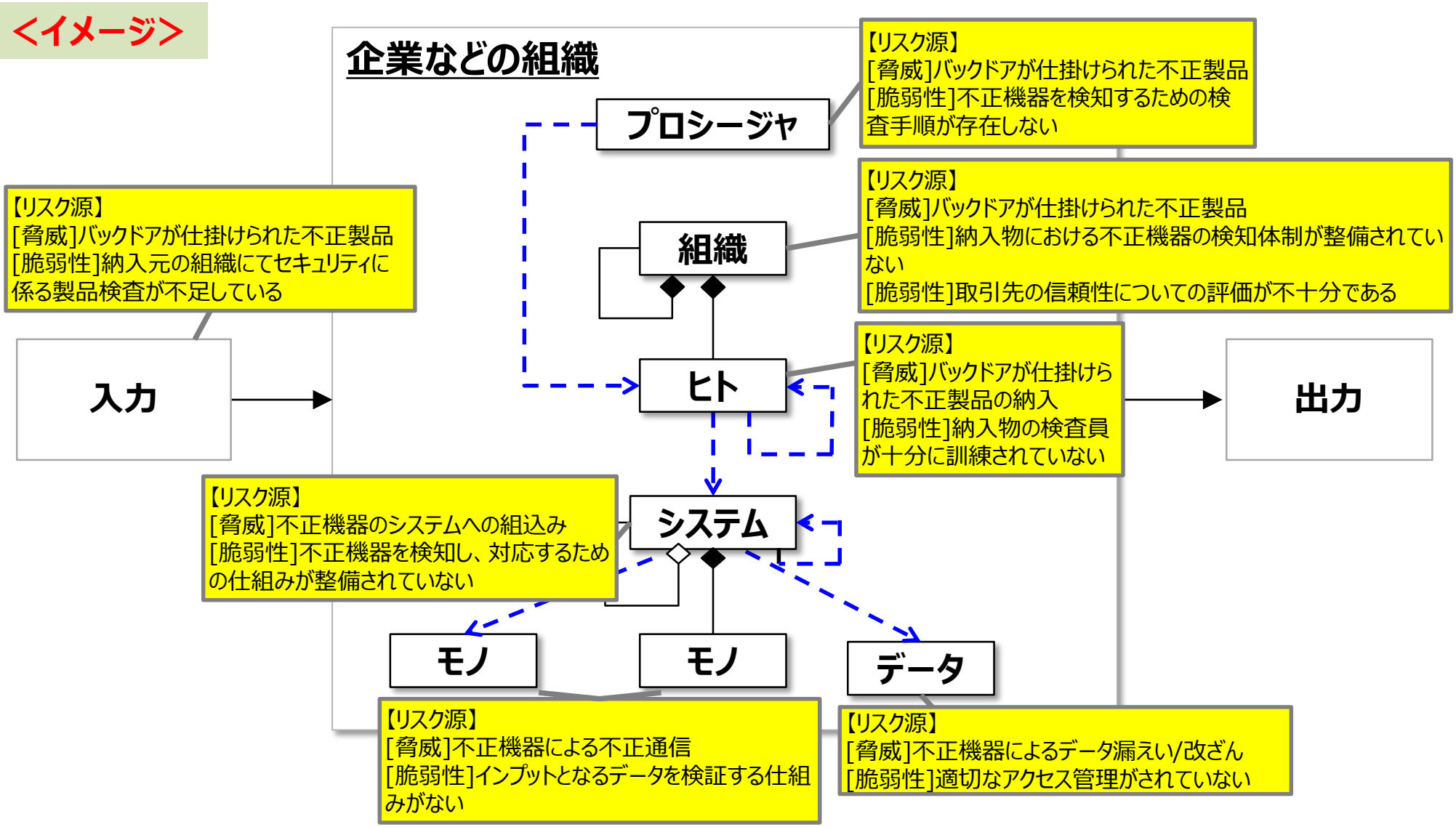
＜イメージ＞




：要素　　：相互作用(指示・操作・処理など)

# （第2部）リスク源の特定
## ～3層構造における６つの構成要素を利用

<イメージ>




：要素　　：相互作用(指示・操作・処理など)

# （第2部）リスク源の整理
## ～3層構造における６つの構成要素を利用

- 3層構造における6つの構成要素により、特定したリスク源を整理。

＜イメージ＞

| # | 特性 | セキュリティ事象 | リスク源 | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | 脅威 | 脆弱性 | | | | | |
| | | | | 組織 | ヒト | モノ | システム | プロシージャ | データ |
| 2-1 | ネットワークにつながるライフサイクルの長い機器が増加する | ・IoT機器の脆弱性等を利用した攻撃を受ける | ・不正操作/悪用<br>・盗聴/傍受/ハイジャック<br>・サービス停止<br>・損壊/損失<br>・障害/誤作動<br>・天災<br>・物理攻撃 | ・自組織のIoT機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない | | ・ネットワーク接続しているIoT機器において、危殆化したセキュリティ対策が実装されている | ・IoT機器側で十分なセキュリティ対策を実装できないことを前提とした対策を実装していない | | |
| 2-2 | (遠隔地等にあり)管理が行き届きにくいネットワークにつながる機器が増加する | ・機器の盗難<br>・機器の改ざん | | ・遠隔地にある機器等の状態を把握できていない | | ・利用している機器に耐タンパー性がない | ・IoT機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない | | |
| 2-3 | ネットワークにつながる機器が様々な場所(重要インフラから家庭まで)に分散する | ・情報の盗聴<br>・マルウェア感染による誤動作 | | ・遠隔地等にある機器の状態を把握できていない | | ・機器の利用環境に適した設定値が適用されていない<br>・機器にアンチウイルス製品が導入されていない | ・IoT機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない | | |

＜作成中＞

# （第2部）対策要件の作成
## ～3層構造における６つの構成要素を利用

- 整理したリスク源に基づき、対策要件を作成。

**リスク源（脅威×脆弱性）** → **対策要件**

**＜イメージ＞**

| # | 特性 | セキュリティ事象 | リスク源 | | | | | | 対策要件 |
|---|---|---|---|---|---|---|---|---|---|
| | | | 組織 | ヒト | モノ | システム | プロシージャ | データ | |
| | | | | | | | | | ・・・ |
| 2-1 | ネットワークにつながるライフサイクルの長い機器が増加する | ・IoT機器の脆弱性等を利用した攻撃を受ける | ・自組織のIoT機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない | | ・ネットワーク接続しているIoT機器において、危殆化したセキュリティ対策が放置されている | ・IoT機器側で十分なセキュリティ対策を実装できないことを前提とした対策を実装していない | | | • 暗号化機能、アンチウイルス機能等をIoT機器側で実装することが難しい場合、システム側で”転写機能”を守るためのセキュリティ対策を実装する必要がある。 |
| | | | | | | | | | ・・・ |
| | | | | | | | | | • IoT機器、サーバ等のソフトウェア構成情報、パッチ適用状況等を把握し、適宜対応する必要がある。 |
| | | | | | | | | | ・・・ |

**＜作成中＞**

# （第3部）セキュリティ対策例の作成

- 対策要件に基づき、セキュリティ対策例を作成。

**対策要件** → **セキュリティ対策例**

**＜イメージ＞**

| 対策要件 |
| --- |
| ・・・ |
| • 暗号化機能、アンチウイルス機能等をIoT機器側で実装することが難しい場合、システム側で”転写機能”を守るためのセキュリティ対策を実装する必要がある。 |
| ・・・ |
| • IoT機器、サーバ等のソフトウェア構成情報、パッチ適用状況等を把握し、適宜対応する必要がある。 |
| ・・・ |

| セキュリティ対策例 |
| --- |
| 【対策例】<br>・・・ |
| (L2.017)（L3.014)<br>IoT機器で構成する組織内のネットワークを、他のネットワークと物理的又は論理的な手法で分離する。 |
| (L2.018)<br>ネットワーク監視によるサイバー攻撃検知 |
| (L2.018)<br>ファイアウォール、IDS(不正侵入検知システム)、IPS(不正侵入防止システム)の導入 |
| (L2.015)<br>セキュリティルールに従って、ソフトウェアの追加/削除/更新を監視し、その作業履歴や監査ログを残し、定期的にレビューする |
| (L2.020)<br>IoT機器の稼働状況、監査ログ、IoT機器の設定、ソフトウェアの構成等を遠隔地から集中管理する。これにより、稼働状況の把握やセキュリティインシデントの検知を迅速に実施する。 |

**＜作成中＞**

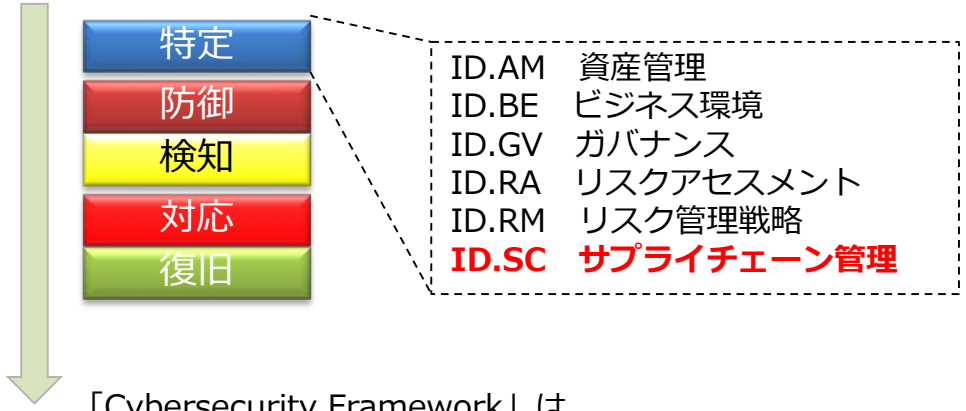
**並び順は、国際規格等を参照しつつ検討**

# ３．国際規格等との対応関係の整理

# 既存の国際規格等におけるセキュリティ対策の整理の仕方

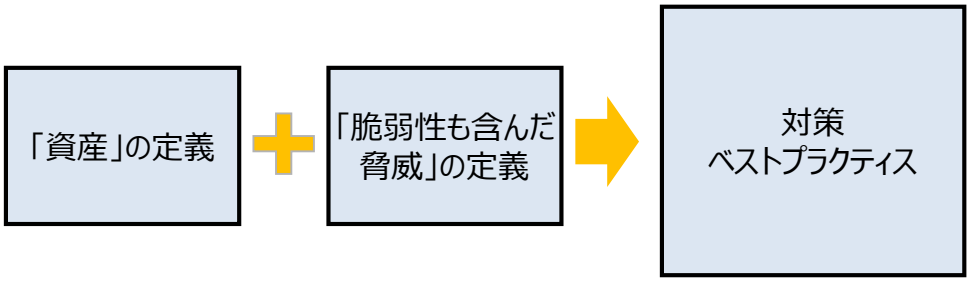
- 『サイバー・フィジカル・セキュリティ対策フレームワーク』が国際的に整合が取れるよう、既存の国際規格等との比較が必要。
- 様々な国際規格等におけるセキュリティ対策の整理の仕方（記載順）は、異なる。
  - 例１）Cyber Security Framework：インシデント対応の順番を基にセキュリティ対策を記載
  - 例２）Baseline Security Recommendations for IoT：リスクを整理したうえで、セキュリティ対策を記載

**「Cybersecurity Framework」における分類**



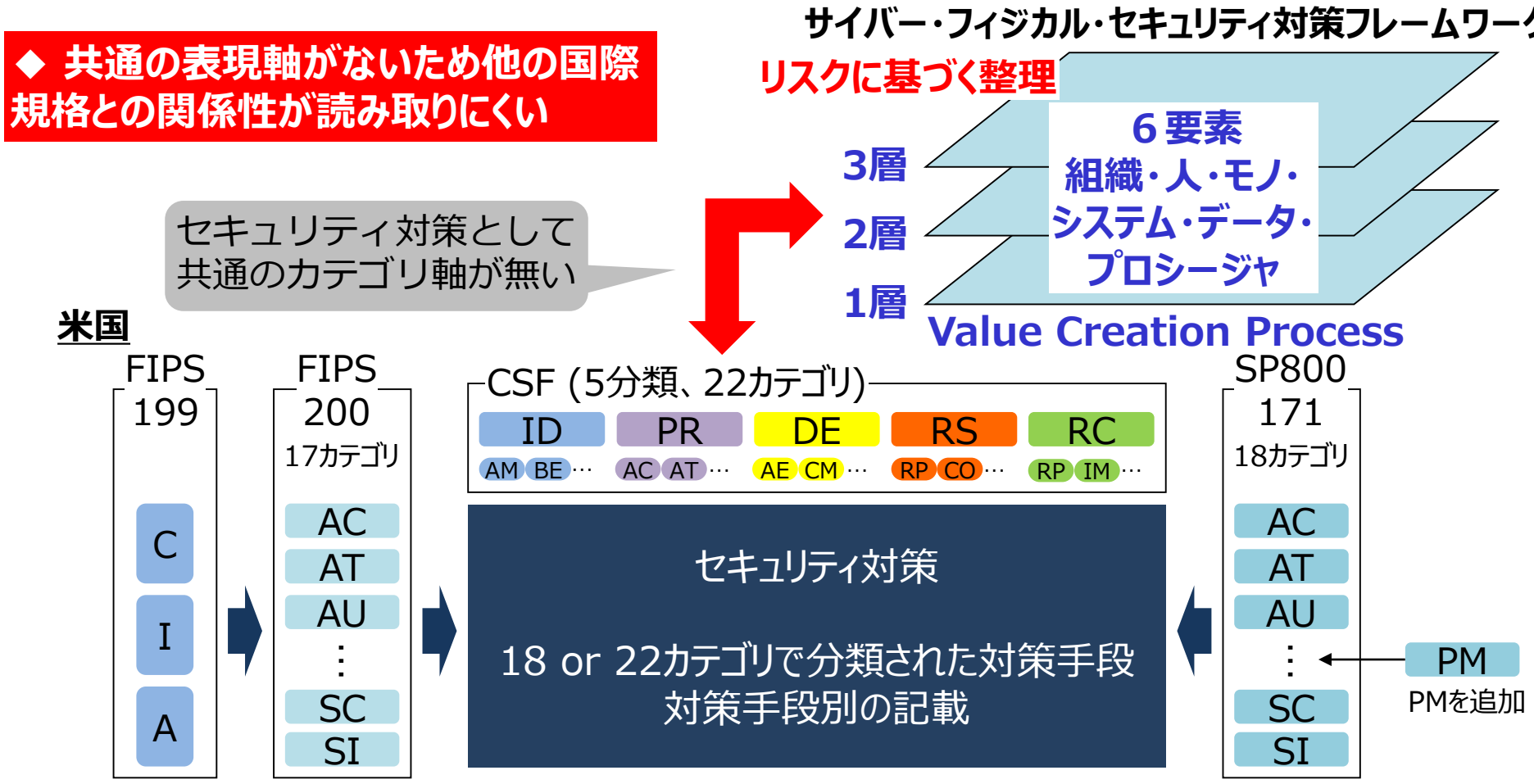

「Cybersecurity Framework」は、
インシデント対応の順番に対策を整理

**「Baseline Security Recommendations for IoT」における分類**



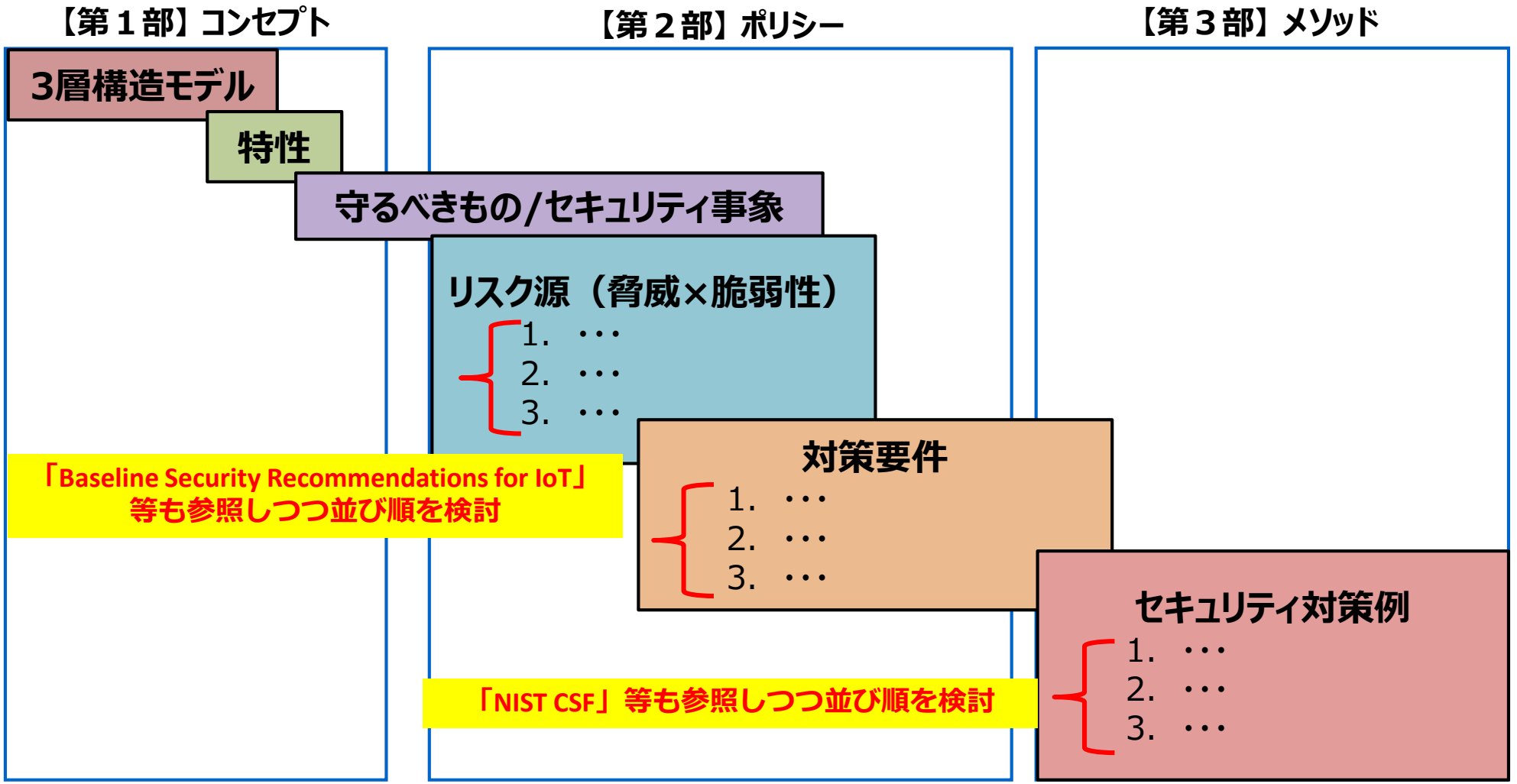
# フレームワークと国際規格等との関係・比較

- 各国際規格等で項目を整理するカテゴリの構成は様々。
- 本フレームワークは、リスクに基づく対策要件の整理をしたうえで、他の国際規格との関係性が読み取れるような分類に基づきセキュリティ対策例を記載。



# フレームワークと国際規格等との関係・比較

- リスク源、対策要件、セキュリティ対策例の並び順は、既存の国際規格等も参照しつつ検討。



セキュリティ対策例のレベル分け【次回議論予定】

# セキュリティ対策例のレベル分け

- 「各事業者がオペレーションレベルで活用できる」「セキュリティ対策の必要性とコストの関係を把握できるようにする」ことを目標として、**対策による効果やコスト等を考慮しながら、具体的な対策例を示す。**
- なお、産業分野ごとに守るべきものやリスクは異なる場合があるため、詳細な検討については各SWGにおいて検討する。

## 対策例の記載イメージ

### 現状の記載例

…

**■構成要素毎の対策例**

**〇組織**

- IoT機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。
- IoT機器やソフトウェアのサプライヤーを特定し、そのサプライヤーから正規品を導入する。

**〇ヒト**

…

**各対策例に、効果やコスト等による重み付けがなされていない**

**対策例のレベル分け**

### 分類後のイメージ（案）

…

**■構成要素毎の対策例**

**〇組織**

【レベル３】

- 製造システムの仕様、設計、開発、実装及び変更にセキュリティエンジニアリングの原則を適用する。開発過程におけるバグや脆弱性の修正課程が追跡可能な状態を維持する。

【レベル１】

- システム開発時にセキュリティの考慮事項を明確に含むライフサイクルが考慮されており、外部コンポーネントの導入時にはセキュリティ要

…

**〇ヒト**

…

**【レベル分けの例】**

**レベル３：高いセキュリティ水準、国際規格等（ISO/IEC27002, SP800-171等）への対応**

**レベル２　　ｓ**

**レベル１：セキュリティ対策として最低減求めたい事項**

# 参考

# 【参考】①他規格との関係性について(米国)

- FIPS 199：連邦政府の情報および情報システムに対するセキュリティ分類規格

表 1 に、各セキュリティ目的（機密性、完全性、および可用性）に対する潜在的影響の定義を要約する。

表 1： セキュリティ目的に対する潜在的影響の定義

| | 潜在的影響 | | |
|---|---|---|---|
| セキュリティ目的 | 低位 | 中位 | 高位 |
| *機密性*<br>しかるべき承認を受けて情報へのアクセスと開示に対して制限を設けること。これには、個人のプライバシーと機密情報の保護手段が含まれる。<br>[44 U.S.C., SEC. 3542] | 情報の不当な開示が、組織活動、組織資産、または個人に**限定的な**悪影響を及ぼすことが予想されうる。 | 情報の不当な開示が、組織活動、組織資産、または個人に**重大な**悪影響を及ぼすことが予想されうる。 | 情報の不当な開示が、組織活動、組織資産、または個人に**致命的または壊滅的な**悪影響を及ぼすことが予想されうる。 |
| *完全性*<br>不適切な情報改変または破壊から情報を保護すること。これには情報の否認防止および真正性の保証が含まれる。<br>[44 U.S.C., SEC. 3542] | 情報の不当な改変または破壊が、組織活動、組織資産、または個人に**限定的な**悪影響を及ぼすことが予想されうる。 | 情報の不当な改変または破壊が、組織活動、組織資産、または個人に**重大な**悪影響を及ぼすことが予想されうる。 | 情報の不当な改変または破壊が、組織活動、組織資産、または個人に**致命的または壊滅的な**悪影響を及ぼすことが予想されうる。 |
| *可用性*<br>タイムリーかつ信頼性の高い方法で情報にアクセスでき、利用できることを保証すること。[44 U.S.C., SEC. 3542] | 情報または情報システムへのアクセスまたは利用の妨害が、組織活動、組織資産、または個人に**限定的な**悪影響を及ぼすことが予想されうる。 | 情報または情報システムへのアクセスまたは利用の妨害が、組織活動、組織資産、または個人に**重大な**悪影響を及ぼすことが予想されうる。 | 情報または情報システムへのアクセスまたは利用の妨害が、組織活動、組織資産、または個人に**致命的または壊滅的な**悪影響を及ぼすことが予想されうる。 |

# 【参考】②他規格との関係性について(米国)

- FIPS 200：連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項
- SP800-53：連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策

| | 分類 | 日本語 | FIPS200 | SP800-53 |
|---|---|---|---|---|
| AC | Access Control | アクセス制御 | ● | ● |
| AT | Awareness and Training | 意識向上およびトレーニング | ● | ● |
| AU | Audit and Accountability | 監査および責任追跡性 | ● | ● |
| CA | Certification, Accreditation and Security Assessments | 承認、認可およびセキュリティ評価 | ● | ● |
| CA | Security Assessment and Authorization | セキュリティ評価及び運用認可 | | |
| CM | Configuration Management | 構成管理 | ● | ● |
| CP | Contingency Planning | 緊急時対応計画 | ● | ● |
| IA | Identification and Authentication | 識別および認証 | ● | ● |
| IR | Incident Response | インシデント対応 | ● | ● |
| MA | Maintenance | 保守 | ● | ● |
| MP | Media Protection | 記録媒体の保護 | ● | ● |
| PE | Physical and Environmental Protection | 物理的および環境的保護 | ● | ● |
| PL | Planning | 計画 | ● | ● |
| PS | Personnel Security | 人的セキュリティ | ● | ● |
| RA | Risk Assessment | リスクアセスメント | ● | ● |
| SA | System and Services Acquisition | システム及びサービスの調達 | ● | ● |
| SC | System and Communications Protection | システムおよび通信の保護 | ● | ● |
| SI | System and Information Integrity | システム及び情報の完全性 | ● | ● |
| PM | Program Management | プログラム管理 | | ● |

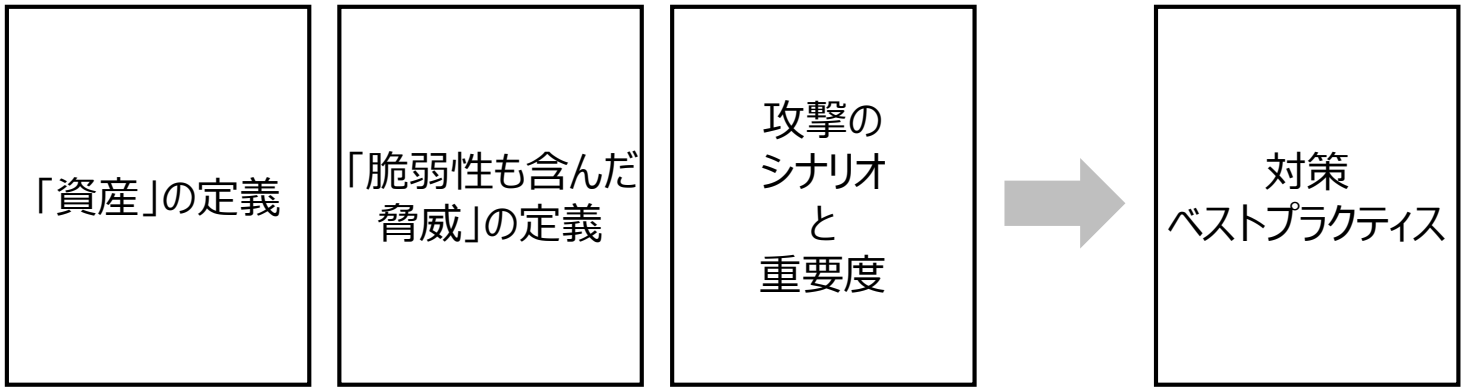
# 【参考】③他規格との関係性について(米国)

- **Cyber Security Framework ver. 1.1**

| | 分類 | 日本語 | 備考 |
|---|---|---|---|
| Identify | ID.AM Asset Management | 資産管理 | |
| | ID.BE Business Environment | ビジネス環境 | |
| | ID.GV Governance | ガバナンス | |
| | ID.RA Risk Assessment | リスクアセスメント | |
| | ID.RM Risk Management Strategy | リスク管理戦略 | |
| | ID.SC Supply Chain Risk Management | サプライチェーンリスク管理 | |
| Protect | PR.AC Identity Management and Access Control | アクセス制御 | |
| | PR.AT Awareness and Training | 意識向上およびトレーニング | |
| | PR.DS Data Security | データセキュリティ | |
| | PR.IP Information Protection Processes and Procedures | 情報を保護するためのプロセス及び手続き | |
| | PR.MA Maintenance | 保守 | |
| | PR.PT Protective Technology | 保護技術 | |
| detect | DE.AE Anomalies and Events | 異常とイベント | |
| | DE.CM Security Continuous Monitoring | セキュリティの継続的なモニタリング | |
| | DE.DP Detection Processes | 検知プロセス | |
| Response | RS.RP Response Planning | 対応計画の作成 | |
| | RS.CO Communications | 伝達 | |
| | RS.AN Analysis | 分析 | |
| | RS.MI Mitigation | 低減 | |
| | RS.IM Improvements | 改善 | |
| Recovery | RC.RP Recovery Planning | 復旧計画の作成 | |
| | RC.IM Improvements | 改善 | |
| | RC.CO Communications | 伝達 | |

# 【参考】①他規格との関係性について(欧州)

- **ENISA** Baseline Security Recommendations for IoTは、リスクベースのガイドライン




章の構成

- スコープ【1.2】
- 対象読者【1.4】
- セキュリティ上の課題【2.2】
- アーキテクチャ【2.4】
- IoT 資産の分類【2.5】
- IoT に対する脅威とリスクの分類【3.2】
- 攻撃シナリオ【3.3】
- セキュリティ対策／ベストプラクティス【4.1、4.2、4.3】
- ギャップ分析【5】
- 提言【6】

# 【参考】②他規格との関係性について(欧州)

- ENISA “Baseline Security Recommendations for IoT” における「資産」

| # | 資産グループ | 資産 | 概要 |
|---|---|---|---|
| 1 | IoT機器 | ハードウェア | IoT 機器を構成する、センサー、アクチュエータ以外の物理的コンポーネント。マイクロコントローラ、マイクロプロセッサ、物理ポート等を含む。 |
| | | ソフトウェア | IoT 機器のOS、ファームウェア、プログラム、アプリケーション。 |
| | | センサー | 温度、運動等のイベントを検知／測定して他機器に送信するサブシステム。 |
| | | アクチュエータ | 処理データに基づき決まった動作を実行するIoT 機器の出力ユニット。 |
| 2 | IoTエコシステムを為すその他の機器 | モノとのIFとなる機器 | IoT機器間のインターフェース（IF）またはアグリゲーター（収集・集約）の役割を果たす機器。人とIoT 機器とのIF となる機器。 |
| | | モノを管理する機器 | IoT 機器やネットワークを管理する機器。 |
| | | 組込システム | 自らデータ処理を行う処理ユニットを持つシステム。組込センサー、組込アクチュエータ、直接クラウドに接続するネットワーク機能等を含む。 |
| 3 | 通信 | ネットワーク | IoT エコシステム内の異なるノード間のデータおよび情報のやり取りを可能にするデータリンク。 |
| | | プロトコル | 複数のIoT 機器があるチャンネルで通信を行う際に従うべき一連の規則。 |
| 4 | インフラ | ルータ | IoT エコシステム内の異なるネットワーク間でデータパケットを転送するネットワーク機器。 |
| | | ゲートウェイ | 異なるプロトコルを使用しているネットワーク間のインターフェースとなるネットワーク機器。 |
| | | 電源 | IoT 機器および内部コンポーネントに電力を提供する機器。 |
| | | セキュリティ機器 | IoT 機器、ネットワーク、情報のセキュリティのための機器。ファイアウォール、WAF、CASB、IDS/IPS 等を含む。 |

# 【参考】③他規格との関係性について(欧州)

- ENISA “Baseline Security Recommendations for IoT” における「資産」

| # | 資産グループ | 資産 | 概要 |
|---|---|---|---|
| 5 | プラットフォーム | ウェブベースのサービス | ウェブインターフェースを持つサービス。 |
| | | クラウドインフラ、サービス | 分散した機器からのデータ収集・処理に利用。また、演算機能、データの保存場所、アプリケーション、サーバ等も提供。 |
| 6 | 意思決定 | データマイニング | 収集したデータを処理し、別の目的で利用するため特定の構造に加工するアルゴリズムおよびサービス。膨大なデータからパターンを見つけ出すためにビックデータ技術を利用。 |
| | | データ処理・演算 | 収集したデータから意味のある情報を抽出するため処理するサービス。機械学習技術も利用。 |
| 7 | アプリケーション & サービス | デー分析・可視化 | 新たなパターンの発見や効率化のため、データ収集・処理した情報を分析・可視化。 |
| | | 機器・ネットワーク管理 | IoT エコシステム内の機器のOS、ファームウェア、アプリケーションのアップデートや、ログ収集等による機器やネットワークの監視。 |
| | | 機器使用情報 | IoT エコシステム内の機器やネットワークのステータス、使用パターン、パフォーマンス等の把握。 |
| 8 | 情報 | 保存状態 | クラウド上のデータベースや機器に保存された情報。 |
| | | 転送状態 | IoT ネットワーク上を流れている情報。 |
| | | 使用状態 | アプリケーション、サービス、IoT 資産が使用中の情報。 |

# 【参考】④他規格との関係性について(欧州)

- ENISA “Baseline Security Recommendations for IoT” における「IoT に対する脅威とリスクの分類」の記載

| 分類 | 脅威 | 概要 |
|---|---|---|
| 不正操作/悪用 | マルウェア | ユーザの同意なく、望まぬ行為や不正な行為を行うプログラム。 |
| | 攻撃ツール | 脆弱性を悪用して不正アクセスを図るコード。 |
| | 標的型攻撃 | 特定の攻撃対象に対し、長期間を掛けて段階的に行われる攻撃。気づかれずにできるだけ多くの重要な情報／権限を入手することを主な目的とする。 |
| | DDoS | 複数システムから攻撃対象に集中攻撃を行い、シャットダウンさせる攻撃。 |
| | 不正機器 | 機器のなりすまし。バックドアがあり、攻撃の実行に使われることも多い。 |
| | プライバシー侵害 | ユーザのプライバシーを侵害する。または、ネットワーク上の機器を第三者に晒す。 |
| | 情報改ざん | 機器の損壊でなく、情報の改ざんによる混乱の引き起こし、または金銭の取得を目的とする。 |
| 盗聴/傍受/ハイジャック | 中間者攻撃 | メッセージを能動的に窃取し、送受信者にメッセージの中間窃取があったことを気づかれないよう、メッセージを中継する。 |
| | IoT通信プロトコルのハイジャック | 既存の通信セッションを乗っ取り、パスワード等の重要情報を入手する。 |
| | 情報傍受 | 電話やメール等の私的通信の盗聴（時には改ざんも）。 |
| | ネットワーク情報収集 | 接続機器、使用プロトコル、空いているポートやサービス等のネットワーク情報の受動的窃取。 |
| | セッションハイジャック | 正規ホストになりすまし、コネクションを乗っ取る。 |
| | 情報収集 | 接続機器、使用プロトコル、空いているポートやサービス等の内部ネットワーク情報の受動的窃取。 |
| | リプレイ攻撃 | 正規のデータ送信を再送信し、不正操作またはシステムダウンさせる攻撃。 |

# 【参考】⑤他規格との関係性について(欧州)

- ENISA “Baseline Security Recommendations for IoT” における「IoT に対する脅威とリスクの分類」の記載

| 分類 | 脅威 | 概要 |
|---|---|---|
| サービス停止 | ネットワーク障害 | 故意または過失によるネットワークの妨害・遮断。 |
| | 機器障害 | ハードウェアの誤作動・障害。 |
| | システム障害 | ソフトウェアサービスまたはアプリケーションの障害。 |
| | サポートサービスの停止 | 情報システムの正しい運用に必要なサポートサービスの利用不可。 |
| 損壊/損失 | データ/機微な情報の漏洩 | 故意または過失による機微な情報の漏洩。 |
| 障害/誤作動 | ソフトウェア脆弱性 | 弱いパスワード・デフォルトパスワード、ソフトウェアのバグ、設定ミス等。 |
| | 第三者要因 | 稼働中のIoT 資産に直接的な影響を持つ別のIoT 資産の設定ミス。 |
| 災害 | 天災 | 洪水、強風、豪雪、土砂崩れ等による機器の物理的な損壊。 |
| | 環境 | 機器が設置された場所の環境的要因による機器の動作不能。 |
| 物理攻撃 | 機器障害 | 機器の改ざん。 |
| | 機器破壊 | 機器の窃取、爆破、破壊等。 |