経済産業省

資料５－１

サイバー・フィジカル・セキュリティ対策フレームワークの概要

経済産業省　商務情報政策局

サイバーセキュリティ課

１．はじめに
～サイバーセキュリティを巡る状況の変化

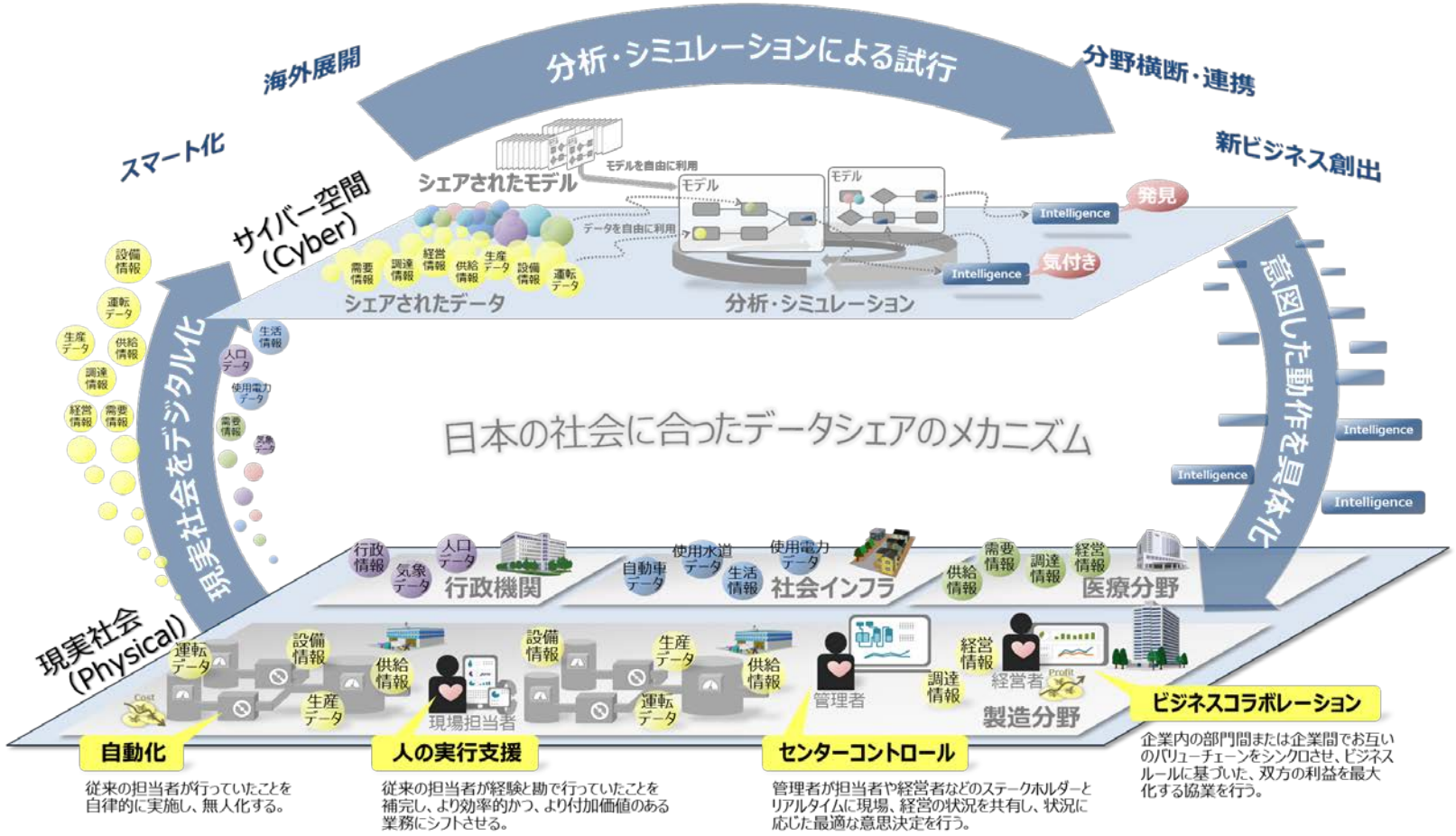
２．サイバー・フィジカル・セキュリティ対策フレームワークの考え方

３．Society5.0において必要なセキュリティ対策

４．信頼の確保に向けて

1．1．Society5.0、Connected Industries が実現する社会

- Society5.0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**する社会。
- Society5.0へ向けて、様々なつながりによる新たな付加価値を創出する**Connected Industriesの実現に向けた新たな産業構造の構築が必要**。



出典：経済産業省「平成27年度我が国経済社会の情報化・サービス化に係る基盤整備(水道事業におけるCPS(サイバーフィジカルシステム)実装のための調査研究)」報告書を基に作成

1．2．サイバー攻撃の脅威の増大

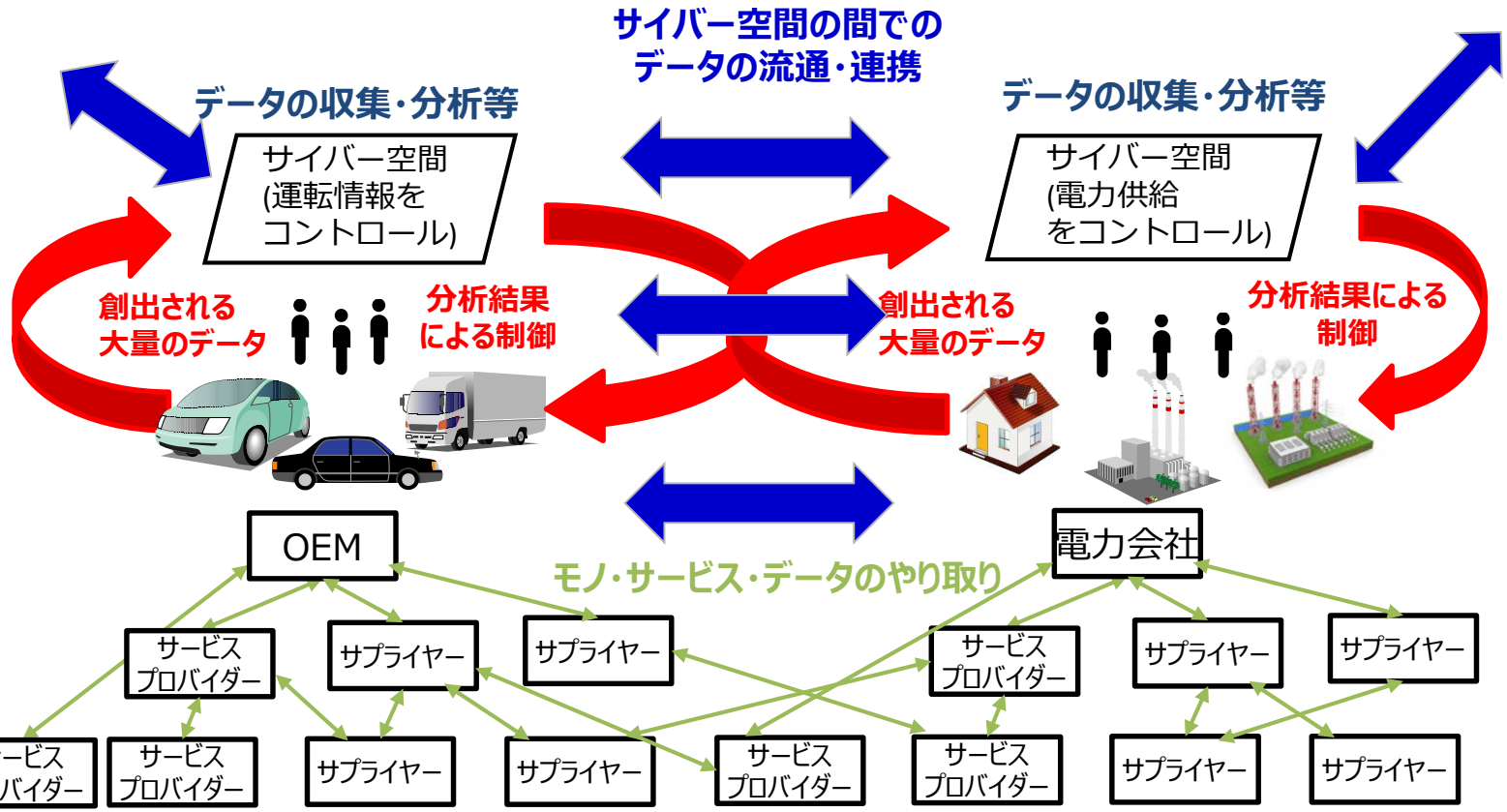
- IoTとAIによって実現されるSociety5.0の社会(人間中心の社会)では、**サイバー攻撃の起点が増大するとともに、複雑につながるサプライチェーンを通じてサイバーリスクの範囲が拡大**。
- サイバー空間とフィジカル空間が高度に融合するため、**サイバー攻撃がフィジカル空間まで到達**。
- IoTから得られる**大量のデータの流通・連携を支えるセキュリティも課題**。
- **海外においても、IoTやICS防衛のためにはサプライチェーンマネジメントでアプローチする必要が広く認識**されるようになっている。

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
⇒データプロテクションの重要性が増大

フィジカルとサイバーの融合
⇒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



１．はじめに
　～サイバーセキュリティを巡る状況の変化

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
　の考え方

３．Society5.0において必要なセキュリティ対策

４．信頼の確保に向けて

2．1．フレームワークを策定する目的

- 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、産業に求められるセキュリティ対策の全体像を整理**し、**産業界が活用できる『サイバー・フィジカル・セキュリティ対策フレームワーク』を策定**することを目指す。

1．各事業者が本フレームワークを活用することで期待される効果

- **Society5.0、Connected Industries の実現に求められるセキュリティの確保**
- **製品・サービスのセキュリティ品質を差別化要因(価値)にまで高めることで競争力を強化**

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に必要な要件

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。
- 社会として目指すべき概念だけではなく、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コストの関係を把握できる。
- サプライチェーン全体を構成する中小企業を含めた事業者が、実際に対策を行えるよう、想定されるリスクと必要な対策のコストのバランスをイメージできるようなものにする。
- セキュリティレベルを保ったままでコストを圧縮できるようにする。
- リスク・シナリオ・ベースの考え方も考慮する。

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、グローバルの動きをよく取り入れ、米欧などの主要な認証制度との相互承認を確保する。

2．2．フレームワークの構造～Society5.0型サプライチェーン“価値創造過程”への対応

- あらゆるものがつながるIoT、データがインテリジェンスを生み出すAIなどによって実現される**Society5.0（人間中心の社会）、Connected Industriesでは、製品/サービスを生み出す工程（サプライチェーン） も従来とは異なる形態をとる**ことになる。
- 本フレームワークでは、**Society5.0型サプライチェーンを**これまでのサプライチェーンと区別するため、**価値創造過程（バリュークリエイションプロセス）と定義**し、そのセキュリティへの対応指針を示す。

- 本フレームワークは、価値創造のための活動が営まれる産業社会を、下記の**三層構造**と**6つの構成要素**で捉え、包括的にセキュリティポイントを整理し、それらに対応するための指針となるもの。

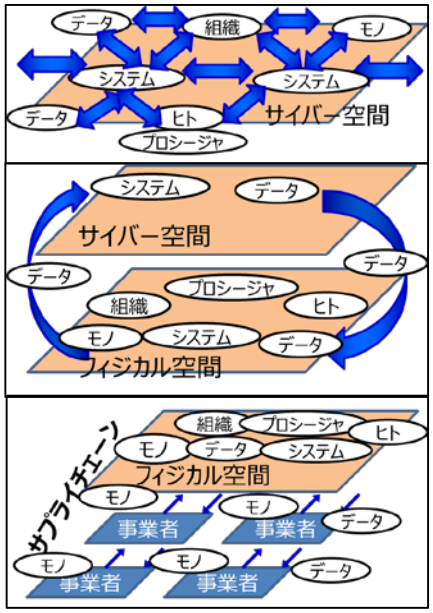
  ⇒ **詳細は次頁以降参照**

◆三層構造

－サイバー空間におけるつながり

－フィジカル空間とサイバー空間のつながり

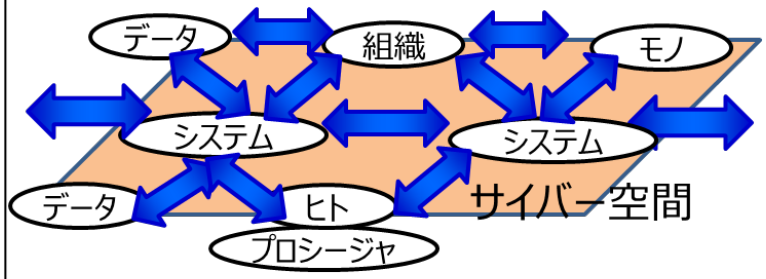
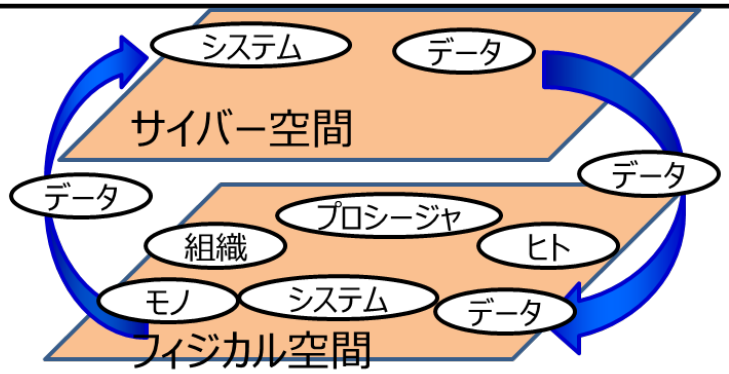
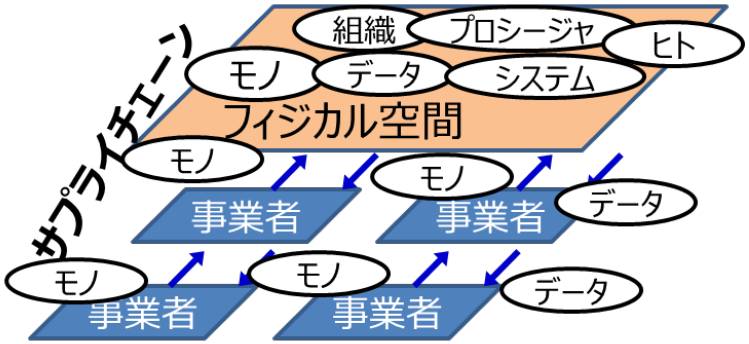
－企業間のつながり（従来型サプライチェーン）



◆６つの構成要素　－組織、ヒト、モノ、データ、プロシージャ、システム

2．2．フレームワークの構造～Society5.0型サプライチェーン“価値創造過程”への対応

（１）価値創造過程が展開する産業社会の三層構造

	概念図	想定される脅威
サイバー空間における つながり 【第３層】		データプラットフォームへの攻撃 － データ改ざん － 大規模な情報漏えい　等
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－サイバー層）		サイバー空間を通じたフィジカルへの攻撃 － センサの計測データ改ざん － IoT機器等で得られて加工されたデータの改ざん　等
企業間のつながり （従来型サプライチェーン） 【第１層】		サプライチェーンを介した攻撃 － マルウェア混入 － 機器へのバックドア － 情報漏えい(設計図面等) － 不正機器混入・接続　等

三層構造アプローチの意義

- ３つの層では、それぞれ価値が創造される。
  第１層では生産された製品等
  第２層ではセンサーで読み込まれたデータ等
  第３層ではデータ分析で得られたデータ等
- 本フレームワークでは、各層で創造される価値の持つ特徴を踏まえた対応の方針を示す。

サイバー空間におけるつながり
【第３層】

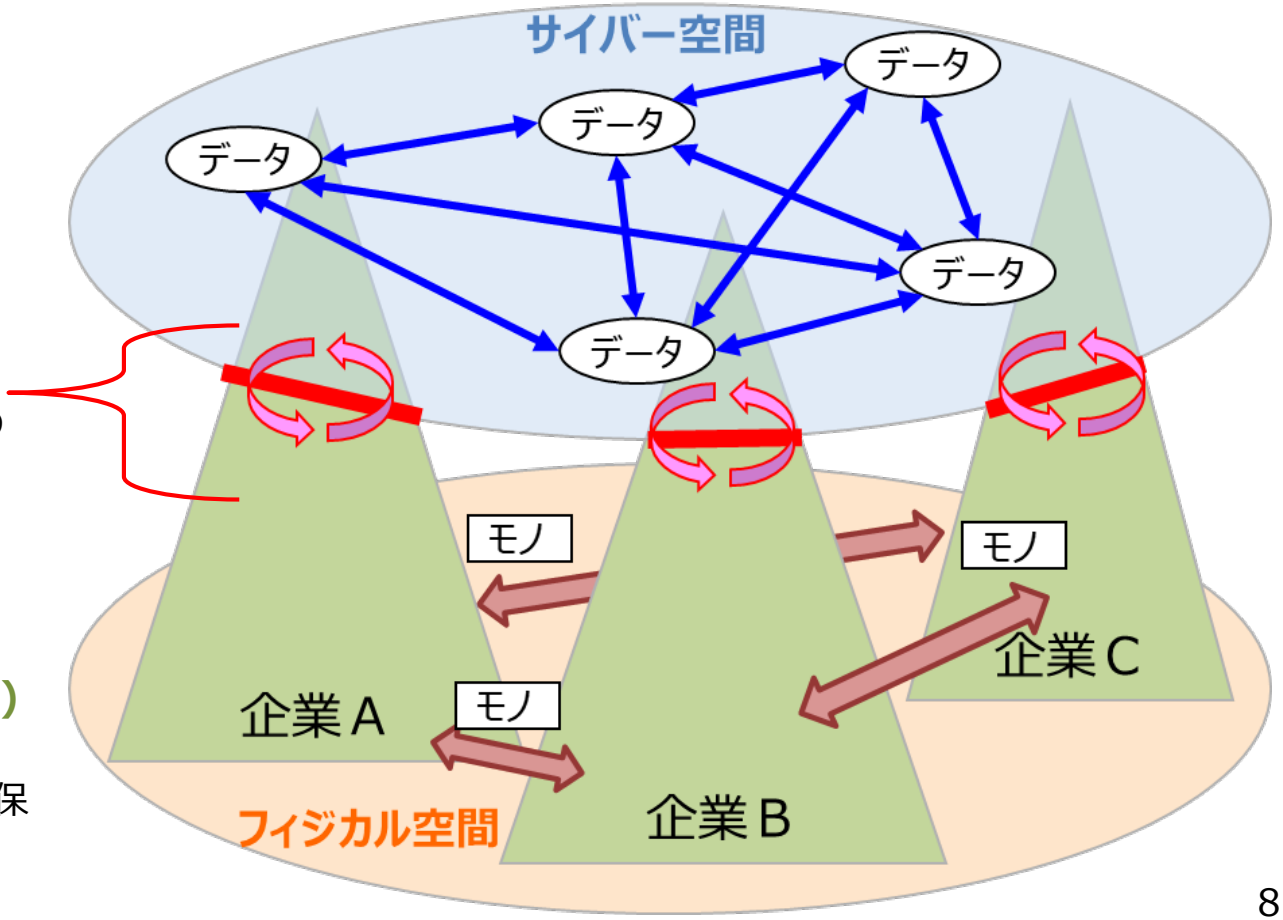
- 自由に流通し、加工・創造されるサービスを創造するためのデータの信頼を確保

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“し、機能の信頼を確保
  （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（従来型サプライチェーン）
【第１層】

- 適切なマネジメントを基盤に各主体の信頼を確保



2．2．フレームワークの構造～Society5.0型サプライチェーン“価値創造過程”への対応

（２)価値創造過程に関わる６つの要素

構成要素	ポイント
組織	[対象]・サプライチェーンを構成する法人(製品やサービスを提供、または利用する) [要件]・ユニークな識別子（ID）で識別できること ・セキュリティポリシーに従い策定したセキュリティマネジメントシステムを運用していること
ヒト	[対象]・組織に属する人（組織から役割、権限を与えられ、何らかの責任を負う） [要件]・組織のセキュリティマネジメントシステムに従って行動すること ・ユニークな識別子（ID）で識別できること ・人の正当性、真正性が担保されていること
モノ	[対象]・機器、ソフトウェア、およびそれらを構成する部品 [要件]・ユニークな識別子（ID）で識別できること ・モノの正当性、真正性が担保されていること
データ	[対象]・フィジカル空間にて収集される(符号化された)情報、およびその情報をシェアし分析・シミュレーションすることで得られる付加価値を含む情報 [要件]・データの完全性が担保されていること
プロシージャ	[対象]・定義された目的を達成するための一連の手続き [要件]・プロシージャの信頼性、安全性、可用性が担保されていること
システム	[対象]・複数のヒト、モノ、データ、プロシージャで構成され、機能やサービスを実現する仕組み・インフラ [要件]・ユニークな識別子（ID）で識別できること ・システムの信頼性、安全性、可用性が担保されていること

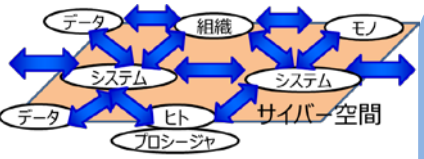
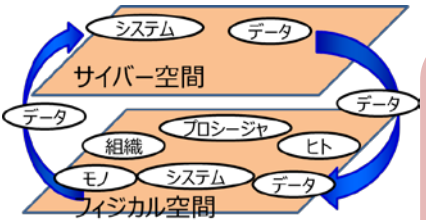
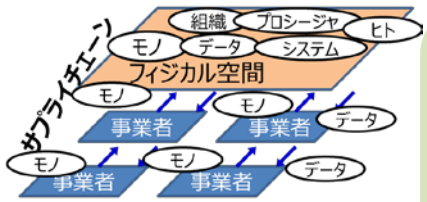
１．はじめに
　～サイバーセキュリティを巡る状況の変化

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
　の考え方

３．Society5.0において必要なセキュリティ対策

４．信頼の確保に向けて

3．1．各層において守るべき事項･リスク･対策の概要

新たなサプライチェーン構造の整理	守るべきもの	セキュリティリスクの洗い出し	具体的な対策の提示（構成要素ごとに整理）
 **サイバー空間におけるつながり【第３層】**	・セキュアなデータ流通 ・サイバー上でのサービス利用	・データの信ぴょう性 ・データプラットフォームへの攻撃 ・ネットワーク上での攻撃	**セキュアなデータ連携・活用に必要な対策の項目** ■データプラットフォームのセキュリティ ■データ品質の確認 ■データプラットフォームに参加する企業のセキュリティの確認　等
		互いに関係	
 **フィジカル空間とサイバー空間のつながり【第２層】**	・実現したい機能 ・レジリエンス ・セキュリティ ・セーフティー　等	・不正な機器の混入（設置段階） ・計測データの改ざん ・制御機能への攻撃	**セキュアなシステム構築に向けて必要な対策の項目** ■機能安全に考慮したシステムの構築、運用 ■セキュアなIoT機器等の導入　等
		互いに関係	
 **企業間のつながり（従来型サプライチェーン）【第１層】**	・仕様どおりの製品、サービス ・情報の秘密保持 ・安全な取引	・マルウェアの混入 ・不正な機器の混入（調達段階）	**セキュアなサプライチェーン構築のために取引先に確認すべき項目** ■納入されるモノのセキュリティ確保 ■取引先のセキュリティ状況の確認 ■取引先とのやり取りのセキュリティ確保

3．2．各層におけるセキュリティ対策
（1）企業間のつながり（従来型サプライチェーン）に係るセキュリティ対策(1/2)【第1層】

No.	必要な対策	リスク要因と影響	対策の概要
L1.001	セキュリティポリシーの策定、体制の整備	要因：セキュリティインシデント発生時の実施すべき内容、対応の優先度がわからず、対応着手が遅れる。組織内で統一的なセキュリティ対策がとれず、効率的な対策ができない。 影響：セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する。	・セキュリティポリシーの策定と運用 ・セキュリティ管理責任者の任命とセキュリティ対策組織立ち上げ
L1.002	セキュリティリスク管理	要因：セキュリティ対策の内容や優先順位、範囲がわからない。 影響：セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する。	・リスクアセスメント(発生しうるセキュリティリスクの特定・分析・評価)の実施 ・セキュリティルールの策定(情報公表時のルールを含む)
L1.003	セキュリティインシデントへの対応の明確化	要因：セキュリティインシデント発生時の対応の内容や優先順位、範囲がわからない。 影響：セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する。	・セキュリティ運用マニュアルの作成
L1.004	サプライヤーとの保守契約	要因：セキュリティ対策の内容や優先順位、範囲がわからない。 影響：セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する。	・サービスやシステム、IoT機器、サーバ等のサプライヤーとの保守契約手続き
L1.005	セキュリティ対策のPDCA実施	要因：新たに発生したセキュリティインシデントに対応できない。 影響：セキュリティインシデントへの対応が遅れ、被害が拡大する。 セキュリティ対策への要員確保、要員の専門知識、再発防止の準備が不十分になり、セキュリティインシデントが再発する。	・セキュリティリスクに対するPDCAの実施 ・モノ、システム等に関する脆弱性情報の継続的な収集
L1.006	定期的な教育・訓練	要因：組織内で統一的なセキュリティ対策がとれない。 影響：セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する。	・定期的なセキュリティ対策教育の実施 ・定期的なセキュリティインシデント対応訓練の実施
L1.007	モノ、システム等の資産管理	要因：サイバー空間と接続するIoT機器等の資産管理の対応不足。 影響：セキュリティ対策漏れを引き起こすIoT機器等が存在し、外部からの不正アクセス、マルウェア感染源になる。	・IoT機器等の棚卸しや資産管理 ・IoT機器等の適切な資産運用
L1.008	セキュリティインシデントの適切な分析機能、手順の実装	要因：セキュリティインシデントを正確に特定できない。 影響：セキュリティインシデントの発見の遅れにより、セキュリティ被害が拡大する。	・アラート通知後の相関の分析 ・外部の脅威情報と比較したセキュリティインシデント検知内容の分析

３．２．各層におけるセキュリティ対策
（１）企業間のつながり（従来型サプライチェーン）に係るセキュリティ対策(2/2)【第1層】

No.	必要な対策	リスク要因と影響	対策の概要
L1.009	事業継続計画又はコンティンジェンシープランへの反映	要因：セキュリティインシデント発生時における事業継続判断が適切に行えない。 影響：セキュリティインシデント発生時において、その影響と事業継続の可否について適切な判断を行うことができず、組織の社会機能や組織に対する社会的評価を喪失する。	・事業継続計画又はコンティンジェンシープランにセキュリティインシデント発生時の対応を位置づける
L1.010	各種法令への対応	要因：組織内で各種法令が守られない。 影響：組織内でコンプライアンス違反が発生する。	・法令や業界のガイドラインを考慮したセキュリティ対策の立案
L1.011	生産したモノの記録の管理	要因：サプライチェーン上で発生したと考えられる問題の発生時点の把握ができなくなる。 影響：価値(モノ)を創造するプロセスにおける問題発生時点が特定できないことから、サプライチェーンにおける問題対処の方法が決まらず、生産活動の適正化に長時間を要することになる。	・生産したモノに関し、後日、監査によって確認できるように、生産したモノの特定方法を定めるとともに、生産記録を作成し、一定期間保管する
L1.012	プライバシー保護	要因：現場のIoT機器等及びサイバー空間を通じて、ユーザーのプライバシーに関する情報(データ)が本人の同意なしに収集・活用される。 影響：収集データの取扱いにおいて、ユーザーのプライバシーに関する情報(データ)が本人の同意なしにシステムに収集され、プライバシー侵害の問題を引き起こす。	・プライバシー保護の法令に準拠したプライバシー情報の取り扱いルールの作成

3．2．各層におけるセキュリティ対策
（2）フィジカル空間とサイバー空間のつながりに係るセキュリティ対策(1/3)【第２層】

No.	必要な対策	リスク要因と影響	対策の概要
L2.001	セキュリティ対策が施されたIoT機器の導入	要因：IoT機器のアクセス制御等のセキュリティ対策が不十分で、不正アクセスされる。 影響：IoT機器が不正に操作されることで、誤動作が発生する。	・第三者機関による評価(EDSA認証等)を取得したIoT機器の選択
L2.002	セキュリティバイデザインの実践	要因：セキュリティ対策を考慮していないIoT機器を利用する。 影響：IoT機器における脆弱性に対し、対策に時間がかかり費用が増加する。	・企画・設計の段階からセキュリティリスクを考慮して実装されたIoT機器の選択
L2.003	機能安全を考慮したIoT機器の導入	要因：機能安全を実装しないIoT機器を利用する。 影響：IoT機器の動作により作業員に危害が及ぶ、又はIoT機器の破損が発生する。	・機能安全を考慮したIoT機器の導入
L2.004	正規品の導入	要因：不正なIoT機器やソフトウェアが混入する。 影響：模倣品等品質や信頼性が低いIoT機器(IoT機器に導入されているソフトウェア含む)を利用することで、不正な情報(データ)の混入、故障頻度の上昇を引き起こす。	・IoT機器のサプライヤーにより、正規であることが認証されたIoT機器の導入 ・ソフトウェアのサプライヤーにより、正規であることが認証されたソフトウェアの導入
L2.005	IoT機器への適切なセキュリティ設定	要因：IoT機器が不正に操作される。 影響：IoT機器に対する不正アクセスにより、誤動作が発生する。	・IoT機器の初期設定手順(パスワード等)を定義する ・不要なサービスの停止等、IoT機器の利用環境に適した設定値を適用する
L2.006	IoT機器へのアクセス制限	要因：IoT機器が不正に操作される。 影響：IoT機器に対する不正アクセスにより、誤動作が発生する。	・アクセス元に対する識別、認証、認可の実施 ・通信におけるセッションの開始、終了条件の明確化
L2.007	IoT機器への不正ログイン対策	要因：IoT機器が不正に操作される。 影響：不正なユーザーによるシステム等へのアクセスにより、IoT機器の設定変更や、IoT機器にある情報(データ)が抜き取られ解析されることで、誤動作が発生する。	・ログイン認証失敗等への適切な対応
L2.008	IoT機器等への物理的なセキュリティ対策	要因：IoT機器等が不正に操作される。 影響：IoT機器等に対する物理的な不正アクセスにより、マルウェア感染被害が発生し、誤動作が発生する。	・監視カメラ等による物理的なアクセスの記録・監視 ・施錠・入退室管理等による物理的なアクセスの制限

3．2．各層におけるセキュリティ対策
（2）フィジカル空間とサイバー空間のつながりに係るセキュリティ対策(2/3)【第２層】

No.	必要な対策	リスク要因と影響	対策の概要
L2.009	IoT機器等の可用性維持	要因：IoT機器等に故障や不具合が生じる。 影響：現場のIoT機器や通信機器、回線の機能が停止し、業務の運用に悪影響を及ぼす。	・サービス不能攻撃を受けた場合でも、サービス活動を停止しないよう、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 ・定期的なバックアップや品質管理、冗長化、予備を確保する
L2.010	IoT機器等の適切な廃棄	要因：不適切な手順でIoT機器等を廃棄する。 影響：廃棄されたIoT機器等を悪用され、不正IoT機器等が作成される。	・適切な手順でIoT機器等を廃棄する
L2.011	不正なソフトウェアへの対策	要因：IoT機器が不正に操作される。 影響：IoT機器の起動時に動作するマルウェア等により、誤動作が発生する。	・ソフトウェアの適切な起動順序確認機能を実装したIoT機器の導入 ・不正なソフトウェアの起動防止機能を実装したIoT機器の導入
L2.012	IoT機器へのマルウェアへの感染防止	要因：IoT機器が不正に操作される。 影響：IoT機器に対する不正アクセスにより、マルウェア感染被害が発生し、誤操作が発生する。	・IoT機器等に対するウイルスチェックの実施
L2.013	IoT機器の継続的な脆弱性対策	要因：IoT機器が不正に操作される。 影響：IoT機器の脆弱性が悪用され、マルウェア感染被害が発生し、誤動作が発生する。	・IoT機器のセキュリティパッチの定期的な更新
L2.014	IoT機器へのリモートアップデート	要因：IoT機器の脆弱性が発見された場合への対応(セキュリティパッチの適用等)に時間がかかる。 影響：セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する。	・IoT機器等に対して、迅速な脆弱性対策の実施
L2.015	IoT機器に導入するソフトウェアの管理	要因：IoT機器に、不正なソフトウェアが搭載される。 影響：IoT機器に搭載された不正なソフトウェアにより、マルウェア感染被害が発生し、誤動作が発生する。	・IoT機器の導入前に、搭載されているソフトウェアを確認する ・IoT機器の導入後に、追加するソフトウェアを制限する
L2.016	IoT機器等の機能の分離	要因：IoT機器等を管理するシステムの機能が不正に操作される。 影響：システムの管理機能に対する不正アクセスにより、設定が変更され、マルウェア感染被害が発生し、誤動作が発生する。	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する

３．２．各層におけるセキュリティ対策
（２）フィジカル空間とサイバー空間のつながりに係るセキュリティ対策(3/3)【第２層】

No.	必要な対策	リスク要因と影響	対策の概要
L2.017	ネットワークの分離	要因：IoT機器等を管理するシステムが不正に操作される。 影響：システムに対する不正アクセスにより、マルウェア感染が発生し、誤動作が発生する。	・ネットワークの物理的又は論理的な分離
L2.018	IoT機器への広域ネットワークからの不正侵入対策	要因：IoT機器が不正に操作される。 影響：IoT機器に対する不正アクセスにより、マルウェア感染が発生し、誤動作が発生する。	・ネットワーク監視によるサイバー攻撃検知 ・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 ・接続元のMACアドレス、IoT機器の設置場所、アクセス時間・頻度等の情報をもとにした不正接続の有無の確認
L2.019	不正な無線接続への対応	要因：IoT機器等が不正に操作される。 影響：IoT機器等に対する不正アクセスにより、マルウェア感染が発生し、誤動作が発生する。	・Bluetooth等による無線接続の制限 ・無線LANアクセスポイントの認証強化
L2.020	IoT機器の集中管理	要因：IoT機器の稼働状況の把握や、セキュリティインシデントの検知に時間がかかる。 影響：セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する。	・IoT機器の稼働情報等を集中管理する仕組みの導入
L2.021	IoT機器の不正動作の検知	要因：IoT機器が不正に動作する。 影響：IoT機器が故障等により不正に動作し、作業員に危害が及ぶ、又はIoT機器の破損が発生する。	・IoT機器が、指示された動作内容と実際のIoT機器の動作結果と比較して、異常の検知や動作の停止を行う

3．2．各層におけるセキュリティ対策
（3）サイバー空間におけるつながりに係るセキュリティ対策(1/3)【第３層】

No.	必要な対策	リスク要因と影響	対策の概要
L3.001	信頼できるサービスサプライヤーの選定	要因：システムの停止が頻発する、又は復旧時間の長期化が生じる。 影響：システムが停止することで、情報(データ)の収集・分析・IoT機器へのフィードバックができず、業務の運用に悪影響を及ぼす。	・第三者による評価(ITSMS等)を取得したサービスサプライヤーの選択
L3.002	耐タンパーデバイスを利用したIoT機器、サーバ等の導入	要因：IoT機器、サーバ等が盗難にあい、情報(データ)が不正閲覧される。 影響：IoT機器、サーバ等が盗難され内部に残存していた情報(データ)を解析されることで、情報(データ)が漏えいする。	・耐タンパーデバイスを利用したIoT機器、サーバ等を選定する
L3.003	サイバー空間への不正ログイン対策	要因：サイバー空間にある情報(データ)が不正アクセスされる。 影響：不正なユーザーによるシステムへのアクセスにより、情報(データ)が抜き取られ解析されることで、情報(データ)が漏えいする。	・パスワード、生体認証、電子証明書等、二つの認証機能を組み合わせた二要素認証機能の実装
L3.004	サイバー空間における接続相手の識別	要因：サイバー空間における機器への処理結果の送信において、機器が誤った接続元から通信データを受信する。 影響：本来とは異なるサイバー空間からの情報(データ)を受け取ることで、業務の運用に悪影響を及ぼす。機器の設定を誤り、本来とは異なるサイバー空間に収集データを送信することで情報(データ)が漏えいする。	・接続相手の一意の識別
L3.005	サイバー空間における接続相手の認証	要因：サイバー空間における機器への処理結果の送信において、機器が誤った接続元から通信データを受信する。 影響：本来とは異なるサイバー空間からの情報(データ)を受け取ることで、業務の運用に悪影響を及ぼす。IoT機器の設定を誤り、本来とは異なるサイバー空間に収集データを送信することで情報(データ)が漏えいする。	・相互認証による接続相手の認証
L3.006	IoT機器、サーバ等への物理的なセキュリティ対策	要因：IoT機器、サーバ等が不正に操作される。 影響：IoT機器、サーバ等に対する物理的な不正アクセスにより、情報(データ)が漏えいする。	・監視カメラ等による物理的なアクセスの記録・監視 ・施錠・入退室管理等による物理的なアクセスの制限
L3.007	サイバー空間における不正な送受信情報(データ)の検知	要因：不正な情報(データ)が送受信される。 影響：マルウェア感染やサイバー攻撃を受けることで、情報(データ)が不正に送受信される。本来とは異なるサイバー空間からの情報(データ)を受け取ることで、業務の運用に悪影響を及ぼす。	・送受信する情報(データ)に対し、許容範囲内であることを動作前に検証する

3．2．各層におけるセキュリティ対策
（3）サイバー空間におけるつながりに係るセキュリティ対策(2/3)【第３層】

No.	必要な対策	リスク要因と影響	対策の概要
L3.008	サイバー空間の可用性維持	要因：サイバー空間のサーバや通信機器、回線の機能に故障や不具合が生じる。 影響：サイバー空間のサーバや通信機器、回線の機能が停止し、業務の運用に悪影響を及ぼす。	・サービス不能攻撃を受けた場合でも、サービス活動を停止しないよう、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 ・定期的なバックアップや品質管理、冗長化、予備を確保する
L3.009	IoT機器、サーバ等の適切な廃棄	要因：不適切な手順でIoT機器、サーバ等を廃棄する。 影響：廃棄されたIoT機器、サーバ等を悪用され、内部に残存する情報(データ)が漏えいする。	・適切な手順でIoT機器、サーバ等を廃棄する
L3.010	IoT機器、サーバ等の継続的な脆弱性対策	要因：IoT機器、サーバ等が不正に操作される。 影響：IoT機器、サーバ等の脆弱性が悪用され、情報(データ)が漏えいする。	・IoT機器、サーバ等のセキュリティパッチの定期的な更新
L3.011	サイバー空間の保管データの暗号化	要因：サイバー空間にある情報(データ)が不正アクセスされる。 影響：情報(データ)が抜き取られ解析されることで、保管していた情報(データ)が漏えいする。	・保管データの秘匿化
L3.012	IoT機器、サーバ等に導入するソフトウェアの管理	要因：IoT機器、サーバ等に、不正なソフトウェアが搭載される。 影響：IoT機器、サーバ等に搭載された不正なソフトウェアにより、情報(データ)が漏えいする。	・IoT機器、サーバ等の導入前に、搭載されているソフトウェアを確認する ・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する
L3.013	サイバー空間における機能の分離	要因：IoT機器、サーバ等を管理するシステムの機能が不正に操作される。 影響：システムの管理機能に対する不正アクセスにより、情報(データ)が漏えいする。	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する
L3.014	ネットワークの分離	要因：IoT機器、サーバ等を管理するシステムが不正に操作される。 影響：システムに対する不正アクセスにより、情報(データ)が漏えいする。	・ネットワークの物理的又は論理的な分離
L3.015	サイバー空間における不正アクセスの検知	要因：サイバー空間にある情報(データ)が不正閲覧される。 影響：システムやIoT機器等への不正なアクセスにより、構成要素にある情報(データ)が抜き取られ解析されることで、保管していた情報(データ)が漏えいする。	・システムやIoT機器等へのアクセスに対する監査ログの実装

3．2．各層におけるセキュリティ対策
（3）サイバー空間におけるつながりに係るセキュリティ対策(3/3)【第３層】

No.	必要な対策	リスク要因と影響	対策の概要
L3.016	IoT機器、サーバへの広域ネットワークからの不正侵入対策	要因：IoT機器、サーバ等が不正に操作される。 影響：IoT機器、サーバ等に対する不正アクセスにより、情報(データ)が漏えいする。マルウェア感染やサイバー攻撃を受けることで、情報(データ)が漏えいする。	・ネットワーク監視によるサイバー攻撃検知 ・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 ・接続元のMACアドレス、IoT機器の設置場所、アクセス時間・頻度等の情報をもとにした不正接続の有無の確認
L3.017	IoT機器、サーバ等の間における通信の保護	要因：IoT機器、サーバ等間で送受信する情報(データ)が盗聴される。 影響：IoT機器、サーバ等間の通信経路上で情報(データ)が漏えいする。	・通信経路の暗号化を利用して情報(データ)を送信する
L3.018	サイバー空間における暗号化通信	要因：サイバー空間において送受信する情報(データ)が盗聴される。 影響：通信経路上で情報(データ)が漏えいする。	・通信経路の暗号化を利用して情報(データ)を送受信する
L3.019	サイバー空間における送受信する情報(データ)の暗号化	要因：サイバー空間において送受信する情報(データ)が盗聴される。 影響：通信経路上で情報(データ)が漏えいする。	・情報(データ)そのものを暗号化して送受信する
L3.020	サイバー空間における送受信情報(データ)の改ざん対策	要因：通信経路上で情報(データ)が改ざんされる。 影響：送受信する情報(データ)が改ざんされる。	・送受信する情報(データ)に電子署名やメッセージ認証コード(MAC)やチェックサム、タイムスタンプ等を付与し、改ざんを検知する
L3.021	不正な無線接続への対応	要因：IoT機器、サーバ等が不正に操作される。 影響：IoT機器、サーバ等に対する不正アクセスにより、情報(データ)が漏えいする。	・Bluetooth等による無線接続の制限 ・無線LANアクセスポイントの認証強化
L3.022	適切な区分を踏まえたデータの管理	要因：各種法令や取決め等によって要求されるデータの保護の水準を適切に確保できなくなる。 影響：各種法令や取決め等によっては、要求されるデータの保護の水準が異なることになるが、データを区分して管理しないことにより、要求を満たしていない不十分な保護によって漏えい等が起きた場合の賠償責任の重大化や、逆に過剰な保護による管理コストの増大等が発生する。	・各種法令や取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、区分毎に適切なデータの保護を行う。

１．はじめに
　～サイバーセキュリティを巡る状況の変化

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
　の考え方

３．Society5.0において必要なセキュリティ対策

４．信頼の確保に向けて

４．１．フレームワークにおける信頼の確保の考え方

- サイバー・フィジカル・システムのセキュリティを確保するため、それぞれの構成要素についての**セキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築することで、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**。

１．信頼の創出

・セキュリティ要件を満たす機器・サービス等の生成
・対象機器・サービス等が要件を満たした形で生成されたことを確認

２．信頼の証明

・対象機器・サービス等が正常に生成されたものであることを確認できるリスト（トラストリスト）の作成と管理
・トラストリストを参照することで対象機器・サービス等が信頼できるものであることを確認

３．信頼のチェーンの構築と維持

・信頼の創出と証明を繰り返すことで信頼のチェーンを構築（トレーサビリティの確保）
・信頼のチェーンに対する外部からの攻撃等への検知・防御
・攻撃に対するレジリエンスの強化

４．１．フレームワークにおける信頼の確保の考え方

（１）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