経済産業省

資料６

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策定に向けて

経済産業省　商務情報政策局

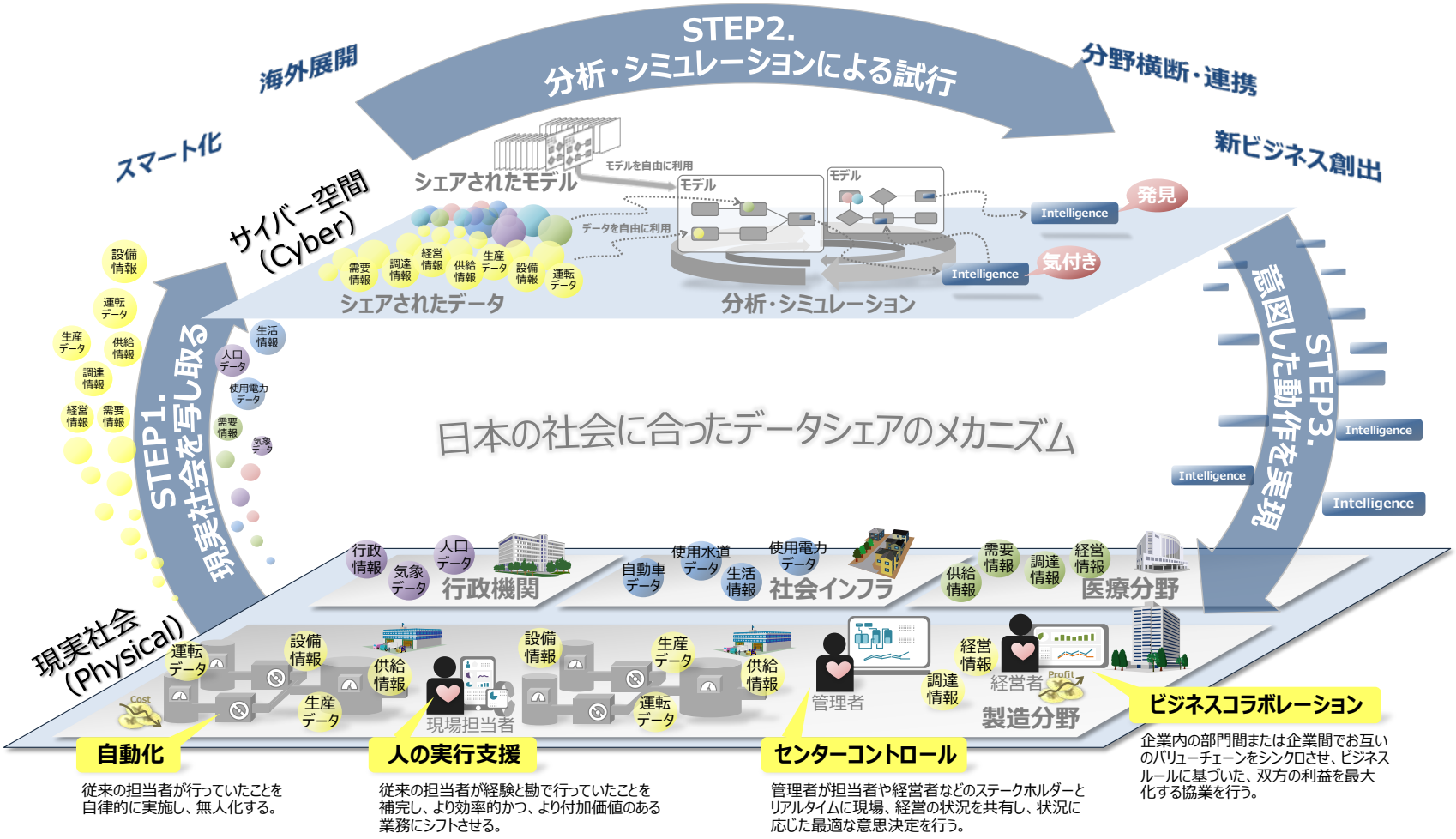
サイバーセキュリティ課

社会の変化に伴い

増大するサイバー攻撃の脅威

社会の変化： Society5.0、Connected Industries が実現する社会

- Society5.0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。
- 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

Society5.0、Connected Industries の実現へ向けた社会の変化に伴い、サイバー攻撃の脅威は増大

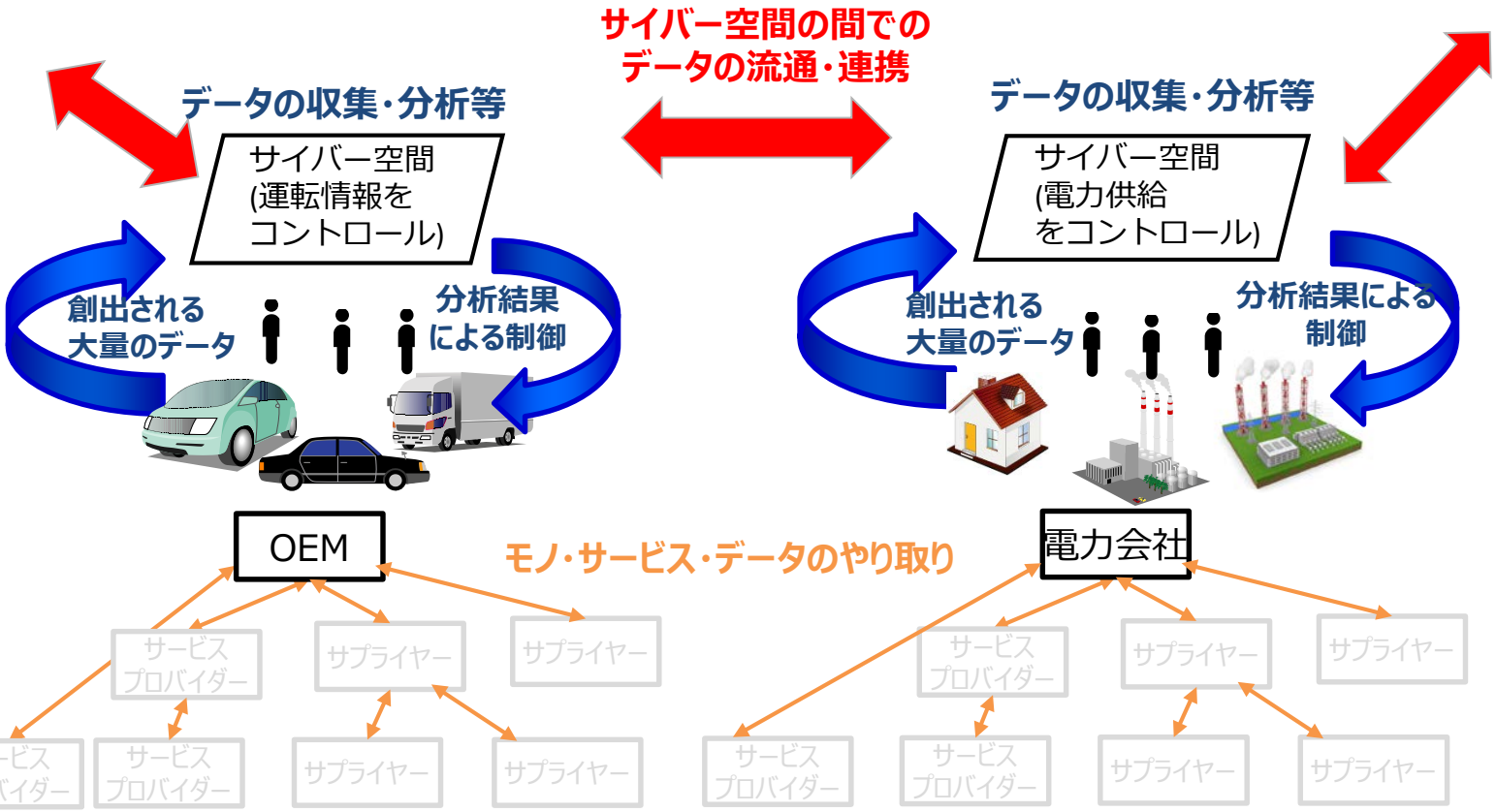
- IoTで全てのヒトとモノがつながるsociety5.0の社会では、**サイバー攻撃の起点が増大するとともに、複雑につながるサプライチェーンを通じてサイバーリスクの範囲が拡大**。
- サイバー空間とフィジカル空間が高度に融合するため、**サイバー攻撃がフィジカル空間まで到達**。
- IoTから得られる**大量のデータの流通・連携を支えるセキュリティも課題**。
- **海外においても、IoTやICS防衛のためにはサプライチェーンマネジメントでアプローチする必要が広く認識**されるようになっている。

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



複雑なサプライチェーンによる脅威の例①：
ランサムウェア”WannaCry”の猛威

参考：産業サイバーセキュリティ研究会第1回にて配布

- 平成29年５月、世界の少なくとも約150か国において、Windowsの脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。
- **感染した欧州企業から、サプライチェーン経由で国内企業も感染。**

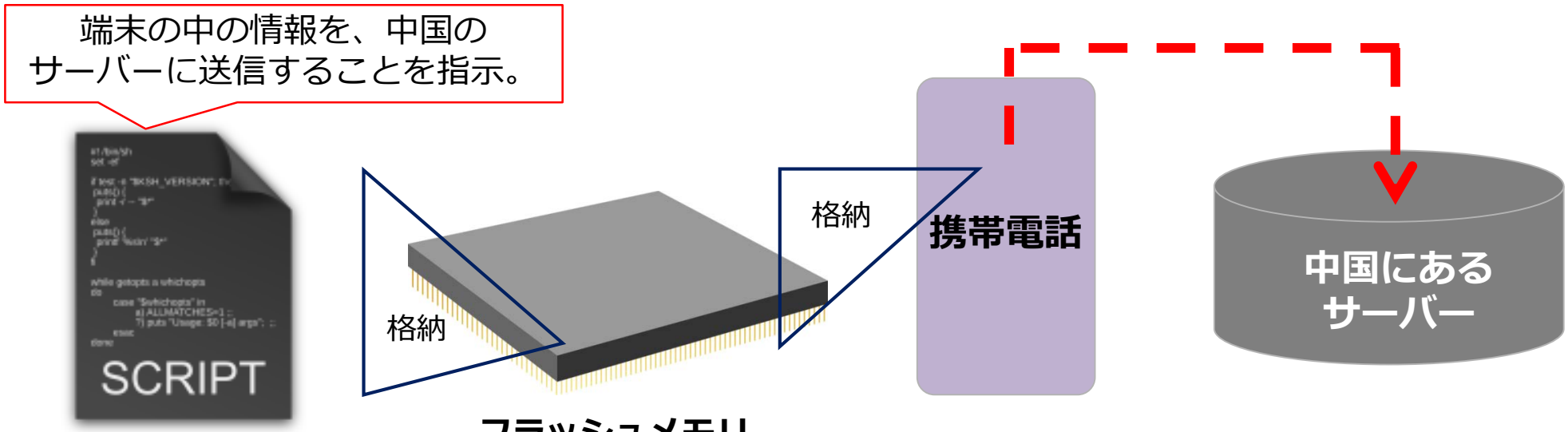
複雑なサプライチェーンによる脅威の例②：
携帯端末に不正プログラムが仕掛けられた事例

参考：産業サイバーセキュリティ研究会第1回にて配布

- メモリに不正プログラムが仕掛けられ、保存されている情報の不正送信や改ざんを受けるリスクが顕在化。
- **製造時に物理的に組み込まれた不正プログラムは検知や削除が容易ではない。**

フラッシュメモリに不正プログラムが仕掛けられた事例

- 2016年、**米国セキュリティ会社が携帯電話のフラッシュメモリのファームウェアに仕込まれている不正プログラムを発見。**
- 中国企業が開発・製造したもので、ユーザーの同意なしに、72時間おきに携帯電話内の情報が中国のサーバーに送信される。



不正プログラム（イメージ）　フラッシュメモリ

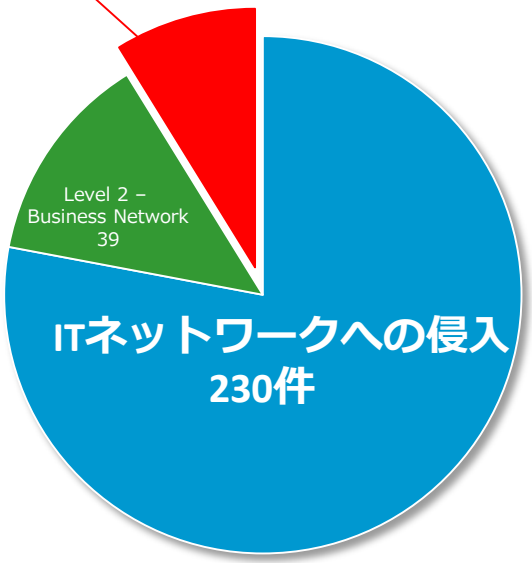
フィジカルとサイバーの融合による脅威の例：サイバー攻撃のレベルが上がり、制御系にまで影響が波及

参考：産業サイバーセキュリティ研究会第1回にて配布

- 米国ICS-CERTの報告では、**重要インフラ事業者等において、制御系にも被害が生じている**。
- ウクライナでは、2015年と2016年にサイバー攻撃による停電が発生。**2016年の攻撃(CrashOverRide)**では、**サイバー攻撃のみで、停電が起こされた**。

米国の重要インフラへのサイバー攻撃の深さ

攻撃のうち約一割は、制御系までサイバー攻撃が到達



（出典）NCCIC/ICS-CERT Year in Review FY2015 Homeland Security より経済産業省作成

2016年に発生したウクライナの停電に係る攻撃（CrashOverRide(Industryoyer)）

(出典)https://www.jiji.com/jc/v2?id=20110311earthquake_25photo
(出典)www.chuden.co.jp/hekinan-pr/guide/facilities/thermalpower.html

欧米において強化される『サプライチェーン』サイバーセキュリティへの要求

参考：産業サイバーセキュリティ研究会第1回にて配布

- **米国、欧州は、サプライチェーン全体に及ぶサイバーセキュリティ対策を模索。**

【米国】

- 2017年、**サイバーセキュリティフレームワーク**（NIST策定のガイドライン）**に、『サイバーサプライチェーンリスクマネジメント』を明記へ**
- 2017年末、**防衛調達に参加する全ての企業に対してセキュリティ対策（SP800-171の遵守）を義務化**

【欧州】

- 2016年、**エネルギー等の重要インフラ事業者に、セキュリティ対策を義務化（NIS Directive）**
- 2017年、**単一サイバーセキュリティ市場を目指し、ネットワークに繋がる機器の認証フレームの導入検討を発表**
- **EUの顧客データを扱う企業に対するデータ処理制限等の新たな義務（GDPR）を2018年から適用**
- **ドイツにおいてルーターのテクニカルガイドラインを作成中**

セキュリティ要件を満たさない事業者、製品、サービスは

グローバルサプライチェーンからはじき出されるおそれ

産業活動において必要なセキュリティ対策を示す

『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

『サイバー・フィジカル・セキュリティ対策フレームワーク』の策定へ向けて

- 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。
- 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。

『サイバー・フィジカル・セキュリティ対策フレームワーク』策定へ向けた検討
（１）フレームワークで考慮すべき構成要素を整理する

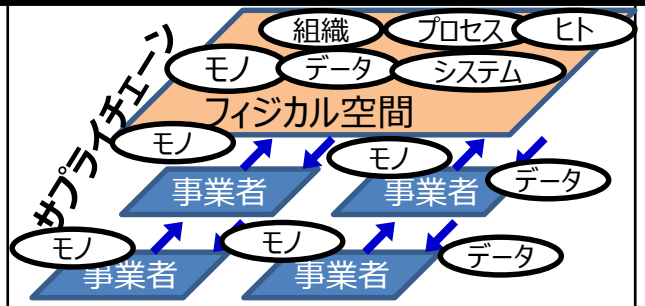
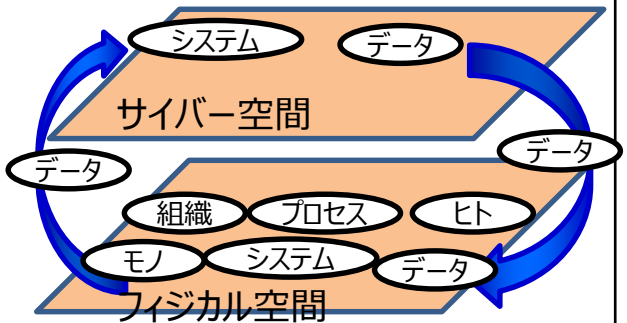
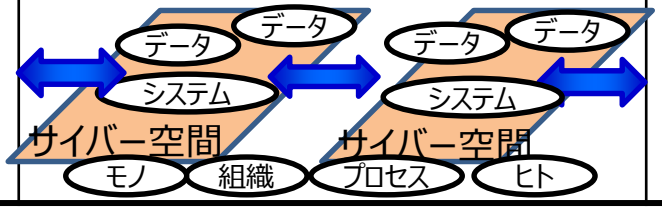
- サプライチェーン含め、CPS/IoT全体のサイバーセキュリティを担保するには、**各産業の事業活動において、セキュリティバイデザインの思想に基づき、構成要素全体のセキュリティ確保が必要**。

No.	構成要素	定義	キーワード
1	組織	[対象]・CPS/IoTおよび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	基本方針、管理、 マネジメント、 ポリシー、法令遵守
2	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	本人確認、アクセス権、 アクセス履歴
3	モノ	[対象]・CPS/IoTに接続する機器、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	識別・認証、パッチ、 機能安全、耐タンパー
4	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	機密情報、データ暗号、 データ改ざん、保管データ、 デジタルエビデンス
5	プロセス	[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]・プロセスの信頼性、安全性、可用性が担保されていること	手順、プロセスの証跡
6	システム	[対象] ・複数のヒト、モノ、データ、プロセスで構成され、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	セキュリティ機能、SOC監視、 脆弱性対策、パッチ

『サイバー・フィジカル・セキュリティ対策フレームワーク』策定へ向けた検討

（２）“繋がること”に着目して、3つの切り口で整理する

- Society5.0、Connected Industries が目指す社会にとって、“繋がること”が価値を生み出す源泉であるが、その一方でリスクも増加される。
- **“繋がること”に着目してセキュリティ対策の切り口を3つに整理して検討を進める。**

社会の変化	繋がることに着目した3つの切り口	切り口のイメージ	想定される脅威
IoT機器の拡大 ・ 複雑につながるサプライチェーン ・ フィジカルとサイバーの融合 ・ 大量のデータの流通・連携と活用	サプライチェーンを構成する企業と企業の繋がり		サプライチェーンを介した攻撃 ーマルウェア混入 ー機器へのバックドア ー情報漏えい(設計図面等) ー不正機器混入・接続　等
	フィジカル空間とサイバー空間の繋がり		サイバー空間を通じたフィジカルへの攻撃 ーセンサの計測データ改ざん ーIoT機器等で得られて加工されたデータの改ざん　等
	サイバー空間とサイバー空間の繋がり		データプラットフォームへの攻撃 ーデータ改ざん ー大規模な情報漏えい　等

『サイバー・フィジカル・セキュリティ対策フレームワーク』のイメージ

WG1において検討を進め、年度内に大枠を整理することを目指す

来年度以降SWGにおいて具体を検討

3つの切り口

脅威が守るべきものへ与える影響(リスク分析)

守るべきもの

脅威

具体的な対応策(構成要素ごとに整理)

3つの切り口	守るべきもの	脅威	具体的な対応策(構成要素ごとに整理)
企業と企業の繋がり	・仕様通りの製品、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
フィジカル空間とサイバー空間の繋がり	・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CPS構築に向けて必要な対策の項目** ■安全なIoTシステムの導入 ■CPS/IoTの構築と運用 ■組織文化の醸成　等
サイバー空間とサイバー空間の繋がり	・セキュアなデータ流通 ・サイバー上でのサービス利用	■データベースに格納される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

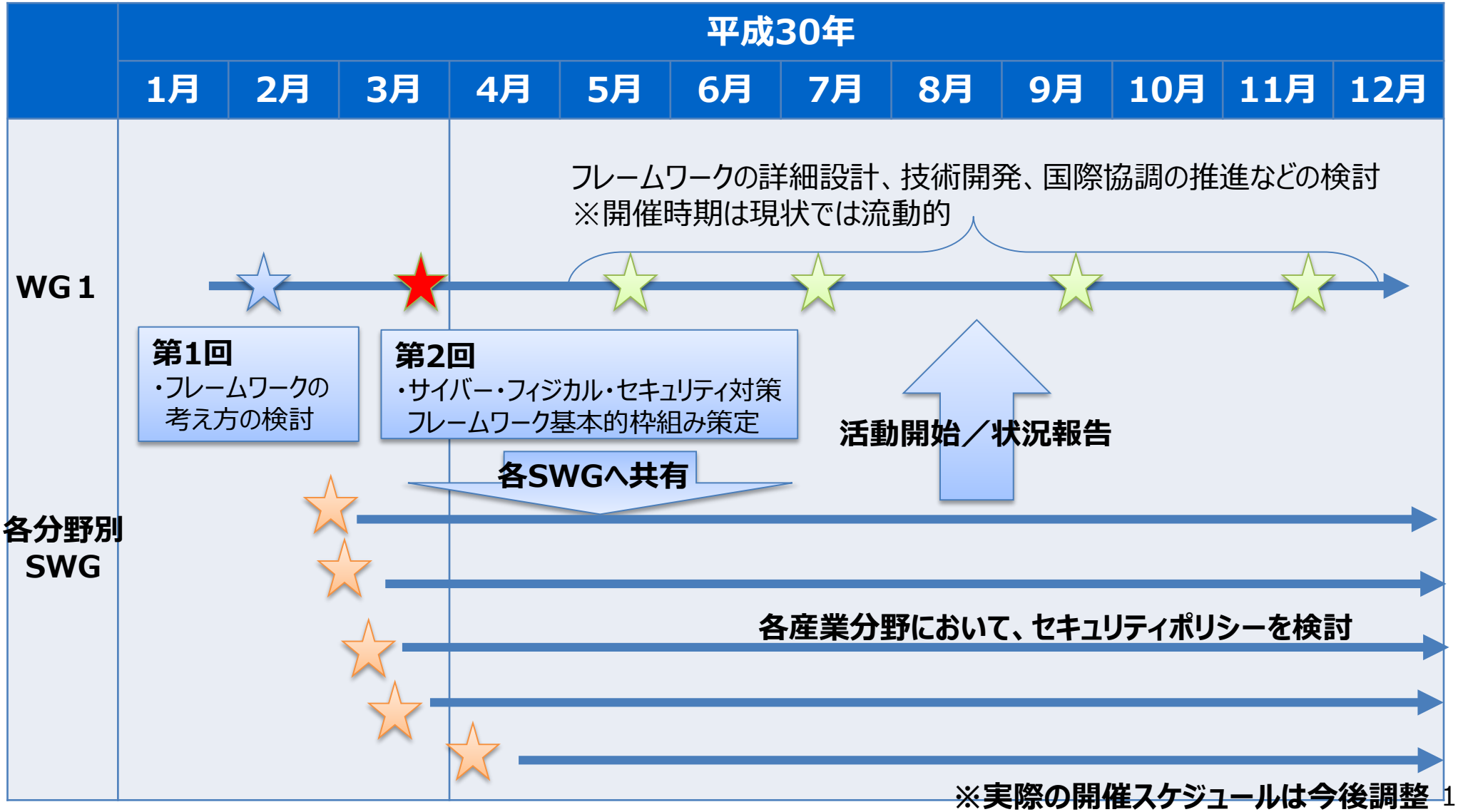
互いに関係

互いに関係

各分野のライフサイクルや求められる機能を踏まえたセキュリティ対策ガイドライン

検討のスケジュールのイメージ

- 年度内に、『サイバー・フィジカル・セキュリティ対策フレームワーク』の基本的枠組みを策定。
- 来年度は詳細設計とともに、技術開発要素の洗い出し、国際協調の推進などの検討を進める。



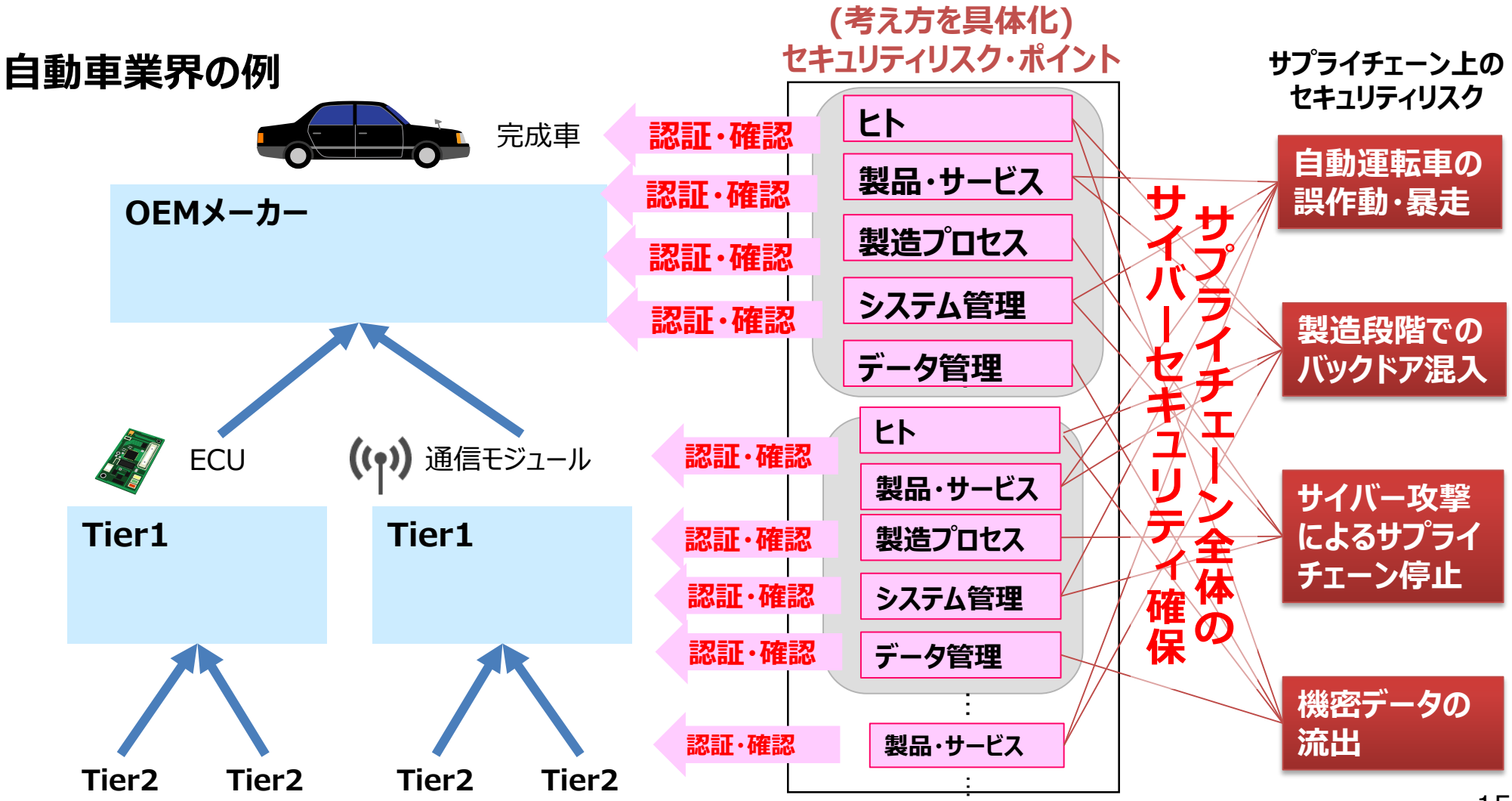
(これから検討を進めていくイメージ)

それぞれの切り口において

想定されるリスクと対策の整理

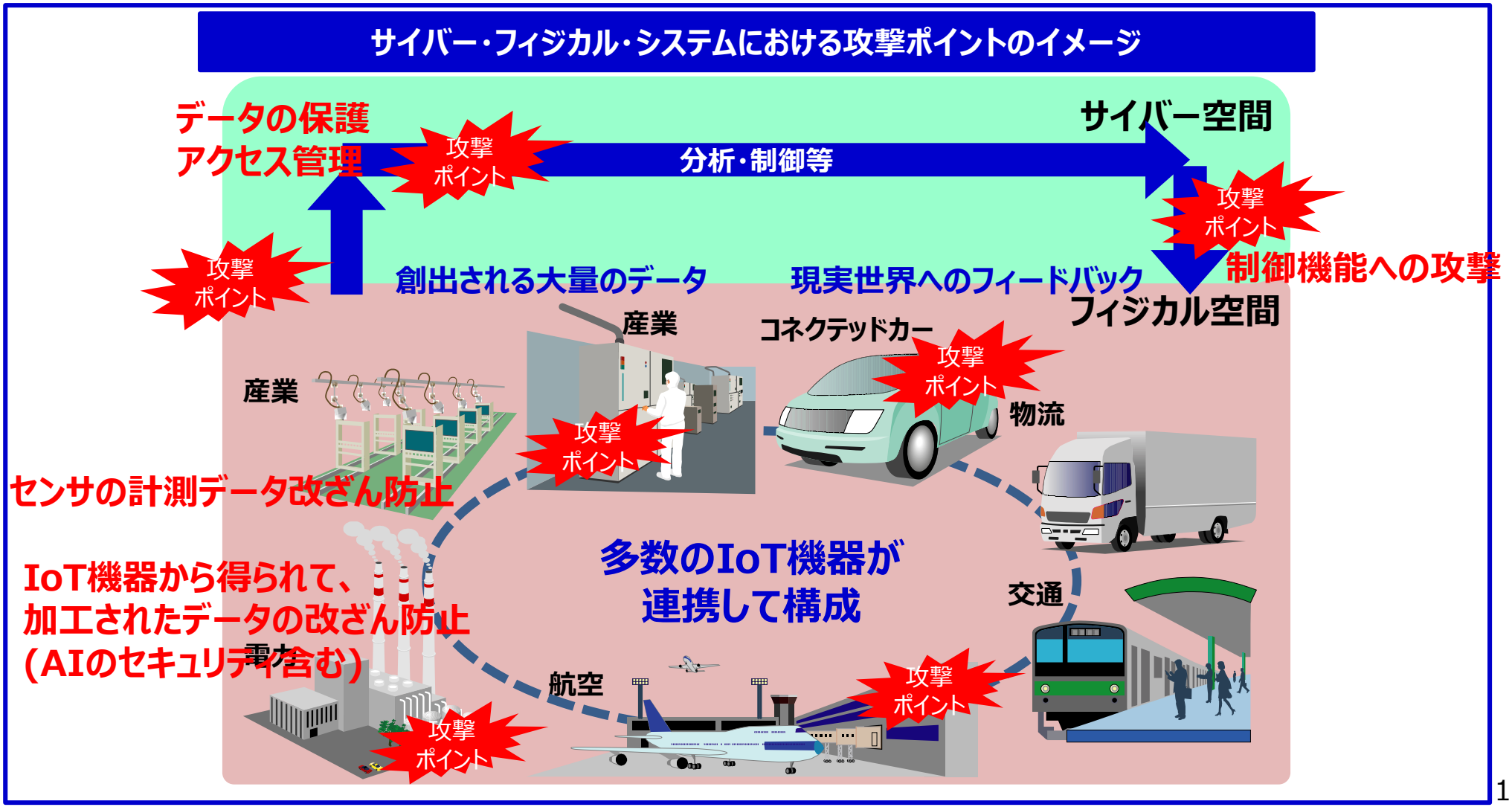
サイバー・フィジカル・セキュリティ対策フレームワークの各切り口の考え方
①サプライチェーンを構成する企業と企業の繋がり

- サプライチェーン全体のサイバーセキュリティを担保するには、**取引先やモノが信頼できることを各リスクポイントにおいて確認することが必要**。



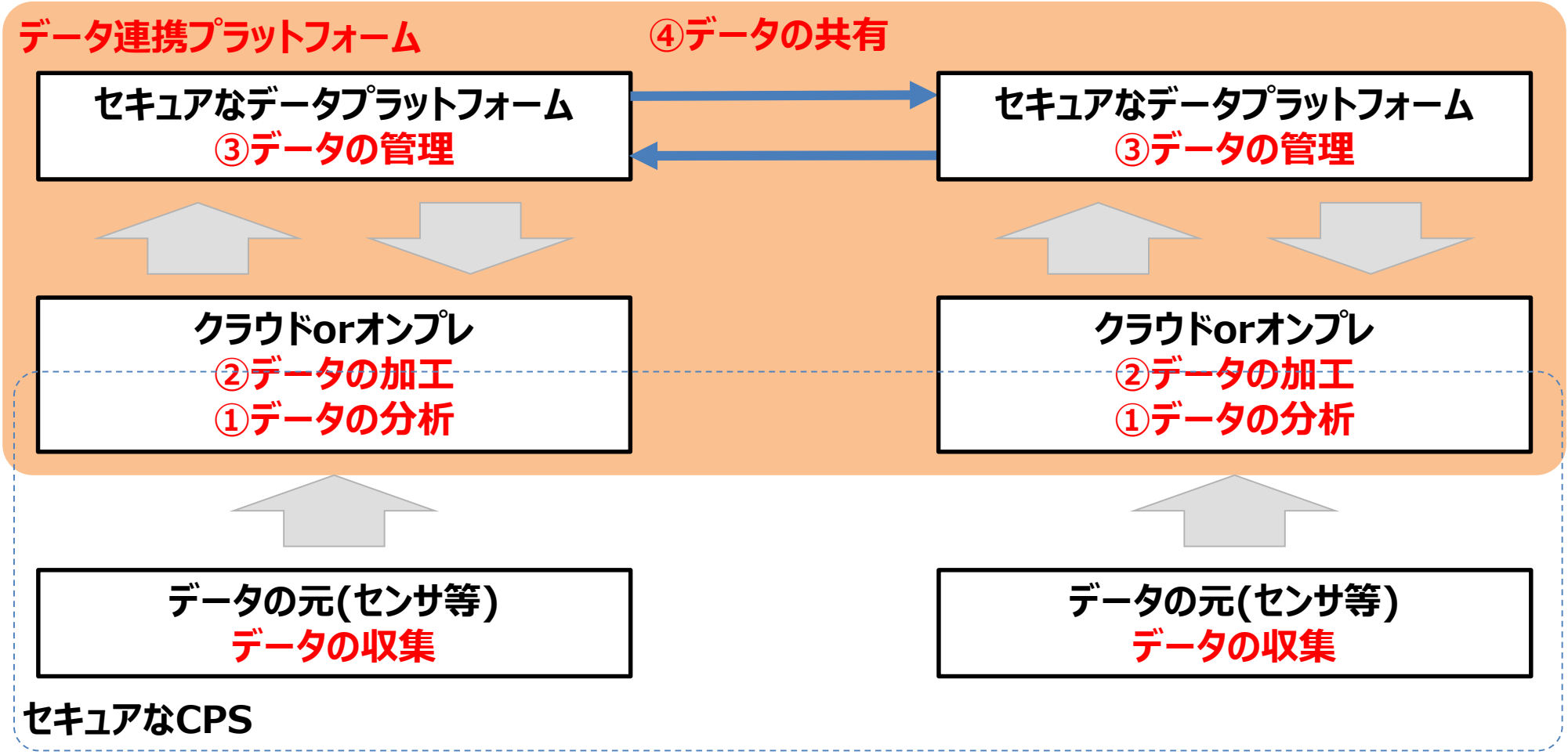
サイバー・フィジカル・セキュリティ対策フレームワークの各切り口の考え方
②フィジカル空間とサイバー空間の繋がり

- CPSにおいては、フィジカル空間からサイバー空間へデータが流れる中で、そのデータの信頼性の確保が必要。このため、センサから得られる計測データの改ざん対策や、データの管理、送信、分析等におけるセキュリティ対策が求められる。



サイバー・フィジカル・セキュリティ対策フレームワークの各切り口の考え方
③サイバー空間とサイバー空間の繋がり

- セキュアなデータプラットフォーム連携のサイバーセキュリティを担保するには、**データの加工・分析・管理・共有を行う際にそれぞれ信頼できることを確認することが必要**。



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実装へ向けて

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、サプライチェーン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認証

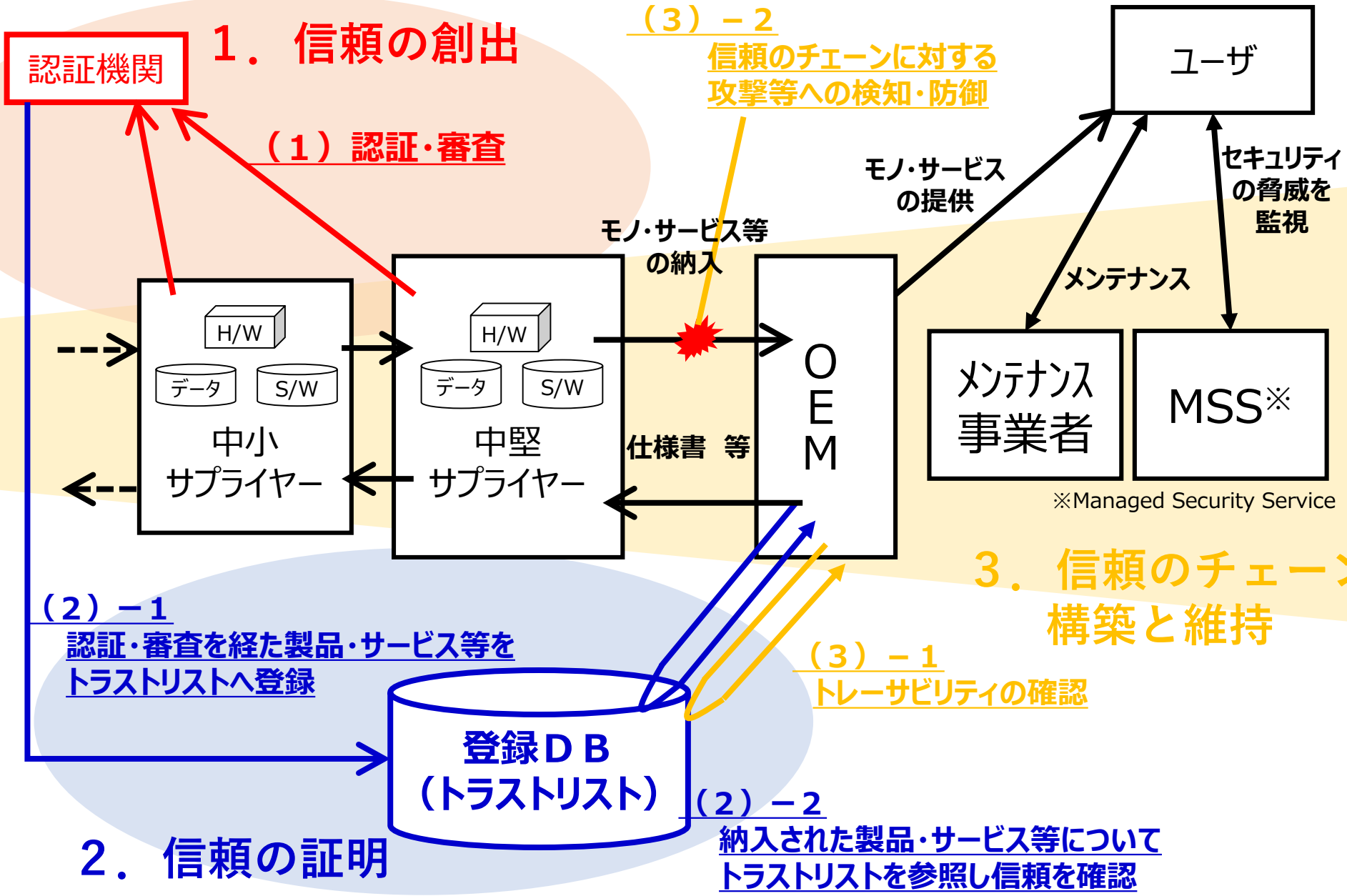
2．信頼の証明

・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

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



成果物のイメージ

サイバー・フィジカル・セキュリティ対策フレームワーク
①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のイメージ

守りたいもの	主なリスク	主な構成要素	対策例
仕様どおりの製品	製造工程における不正部品の混入	組織	• 組織としてセキュアなサプライチェーンを確保する体制を確立すること • 取引先のセキュリティ対策を監査すること
		ヒト	• 製品の製造工程に携わる人を制限していること
		モノ	• 完成製品の確認・検査を行うこと
		プロセス	• 正規であることが確認された部品等を使用していること • 製造プロセスの証跡を確認すること
情報の秘密保持（設計図面等）	委託先からの漏えい	組織	• 組織としてセキュアなサプライチェーンを確保する体制を確立すること • データ保管場所の監視を行うこと
		ヒト	• データにアクセスできる人を制限すること
		データ	• データの暗号化を行うこと • 秘密分散技術を活用して単純なデータ漏えいを防ぐこと
		プロセス	• 取引先のセキュリティ対策を監査すること
		システム	• 外部から容易にアクセスできないシステムになっていること
…			
…			

サイバー・フィジカル・セキュリティ対策フレームワーク
②セキュアなCPS構築に向けて必要な対策の項目のイメージ

守りたいもの（NIST CPS FWを参考）	主なリスク	主な構成要素	対策例
リライアビリティ	不正なIoT機器の設置	組織	• 組織としてセキュアなサイバー・フィジカル・セキュリティを確保する体制を確立すること
		ヒト	• 設置する人間が特定されていること
		プロセス	• 設置するプロセスが管理されていること
		モノ	• 正規のサプライチェーンからの調達であること【切り口１を活用】 • IDを付与して管理されていること
	計測データの改ざん	モノ	• 正規のサプライチェーンからの調達であること【切り口１を活用】 • モノそのもののセキュリティ対策を確認すること
		システム	• データの暗号化やアクセス制限を行うこと • 機器に対する不正アクセスを監視すること
		データ	• デジタル署名等によりデータの真正性を確認すること
IoTの機能(可用性、機密性、完全性)	IoT機器等で得られて加工されたデータの改ざん	モノ	• モノそのもののセキュリティ対策を確認すること
		データ	• デジタル署名等によりデータの真正性を確認すること
		システム	• データの暗号化やアクセス制限を行うこと
…			

サイバー・フィジカル・セキュリティ対策フレームワーク
③セキュアなデータ連携・活用に必要な対策の項目のイメージ

守りたいもの	主なリスク	主な構成要素	対策例
データセンターに集められたデータの管理	不正アクセス等によるデータの改ざん	組織	• 組織としてセキュアなデータプラットフォーム連携を確保する体制を確立すること
		ヒト	• データにアクセスできる人を制限していること
		モノ	• デジタル署名による連携機器の相互認証を行うこと
セキュアなデータの流通	不正アクセス等によるデータの漏えい	データ	• デジタル署名によりデータの真正性を確認すること
		システム	• データの暗号化やアクセス制限を行うこと

『サイバー・フィジカル・セキュリティ対策フレームワーク』の検討と関連する文献等

Framework for Improving Critical Infrastructure Cybersecurity Version 1.0（改訂版含む）,
Framework for Cyber-Physical Systems Release 1.0,
NIST Special Publication 800-53 (FedRAMP),
NIST Special Publication 800-161,
NIST Special Publication 800-171,
The Industrial Internet of Things Reference Architecture Version 1.8,
Industrial Internet of Things Volume G4: Security Framework,
Umsetzungsstrategie Industrie 4.0,
Security in RAMI 4.0,
Structure of the Administration Shell,
Secure cross-company communication,
Secure Identities,
IEC 62443,
ISO 27000 Series,
XML Encryption Syntax and Processing/XML Signature Syntax and Processing,
安全なIoTシステムのためのセキュリティに関する一般的枠組み,
サイバーセキュリティ経営ガイドライン Ver 2.0,
IoTセキュリティガイドライン Ver 1.0,
セキュリティ評価基準 CC バージョン3.1 リリース5,
情報セキュリティ早期警戒パートナーシップガイドライン - 2017年版 -,
つながる世界の開発指針,
ISMS適合性評価制度　等