経済産業省

資料３－２

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

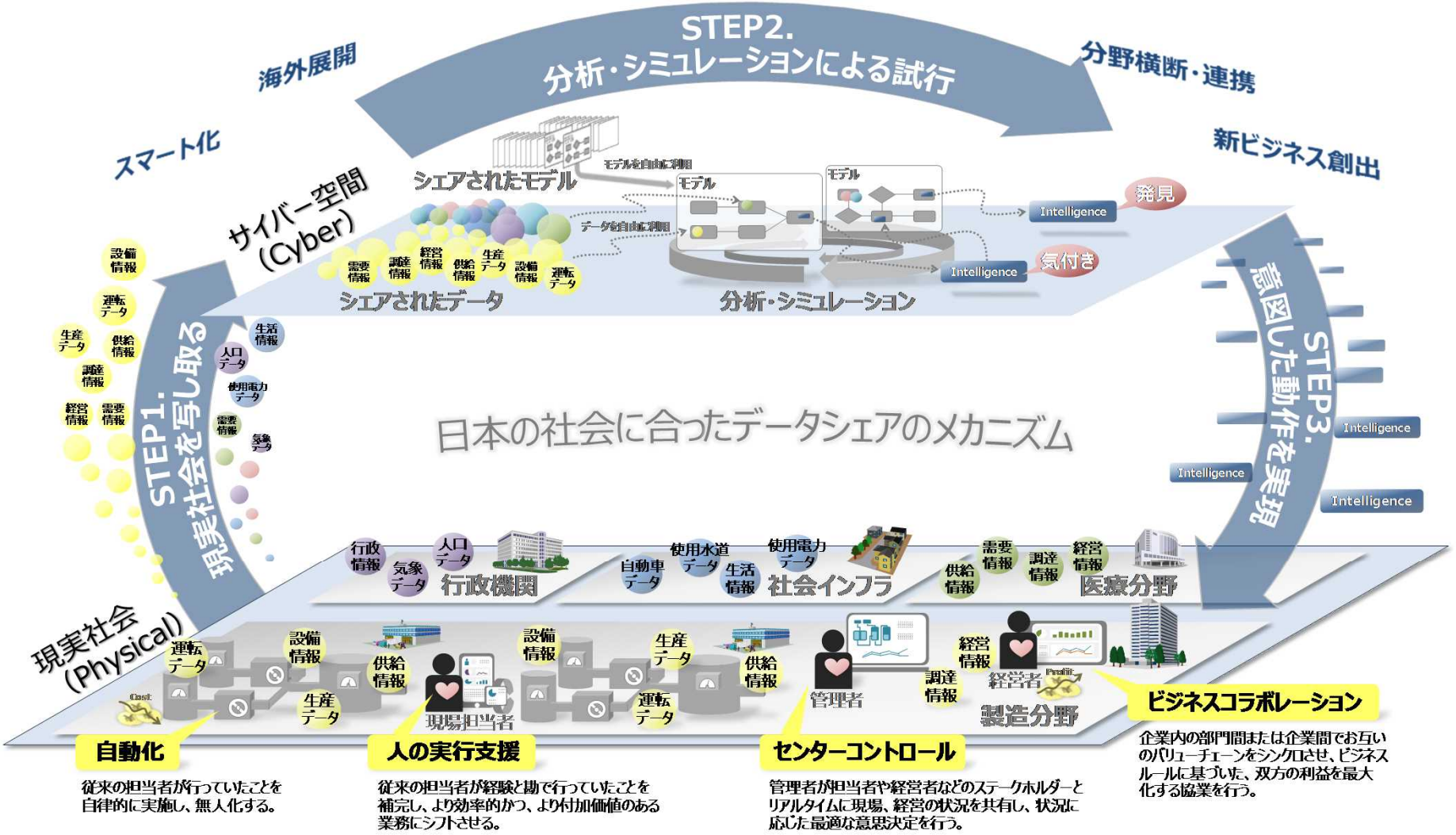
サイバーセキュリティ課

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

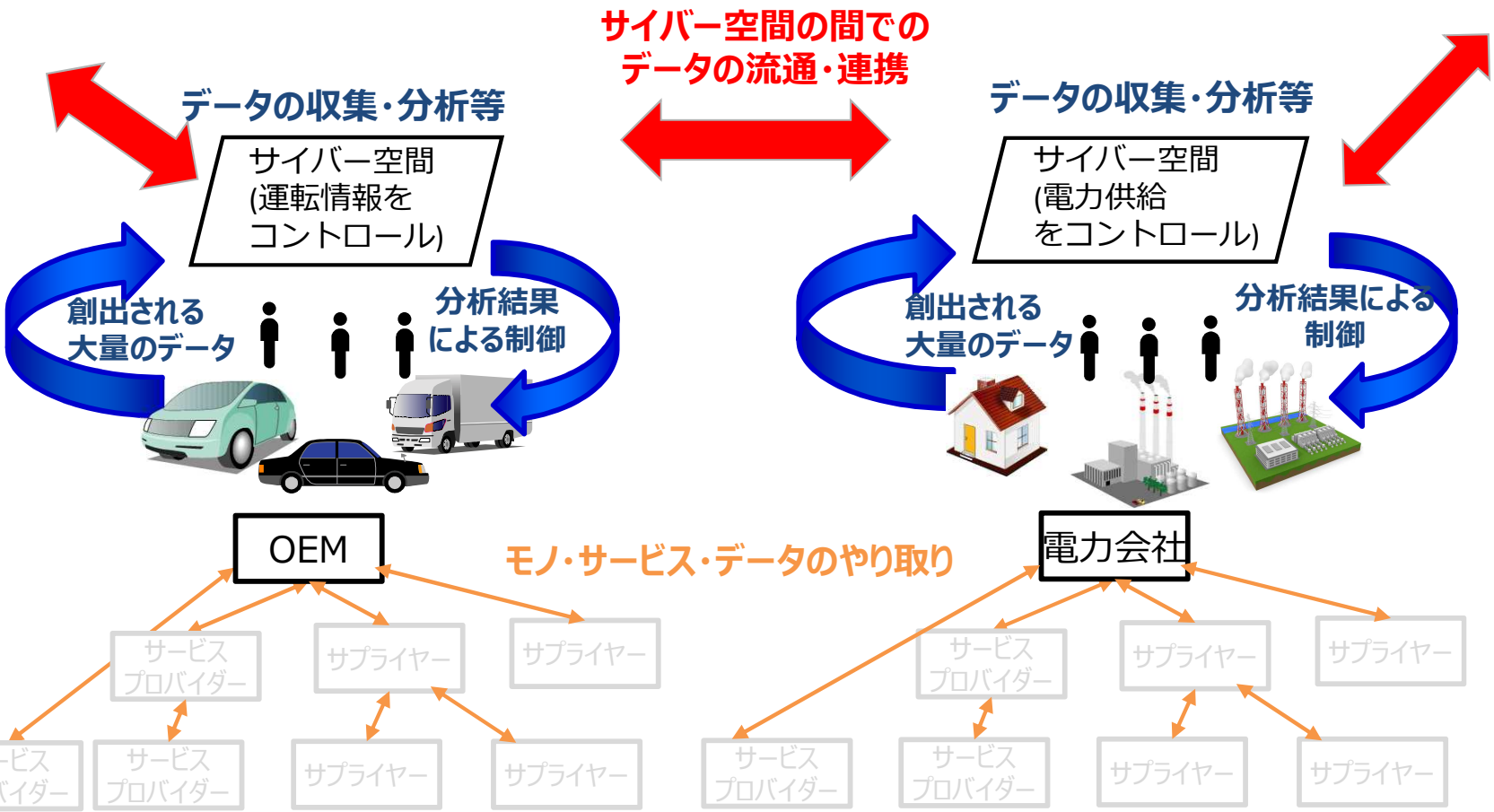
- IoTで全てのヒトとモノがつながるsociety5.0の社会では、**サイバー攻撃の起点が増大するとともに、複雑につながるサプライチェーンを通じてサイバーリスクの範囲が拡大**。
- サイバー空間とフィジカル空間が高度に融合するため、**サイバー攻撃がフィジカル空間まで到達**。
- IoTから得られる**大量のデータの流通・連携を支えるセキュリティも課題**。
- **海外においても、IoTやICS防衛のためにはサプライチェーンマネジメントでアプローチする必要が広く認識**されるようになっている。

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。**

金銭要求メッセージで画面ロック

社内へ感染拡大

悪意のあるコード

工場の制御PCがロックされ製造停止という事態も

インターネットから侵入

海外工場のPCが乗っ取られWAN経由で侵入

インターネットやWANから侵入

社外へも感染拡大

一旦社内に侵入、感染すると、Windowsの脆弱性を突いて、社内外に級数的に感染を拡大

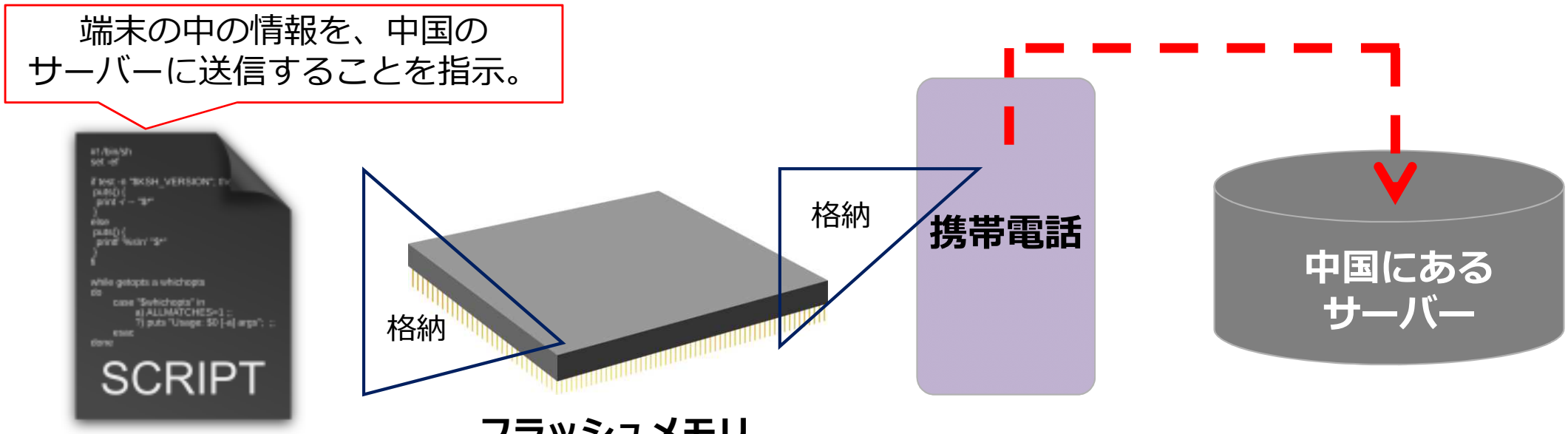
複雑なサプライチェーンによる脅威の例②：携帯端末に不正プログラムが仕掛けられた事例

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

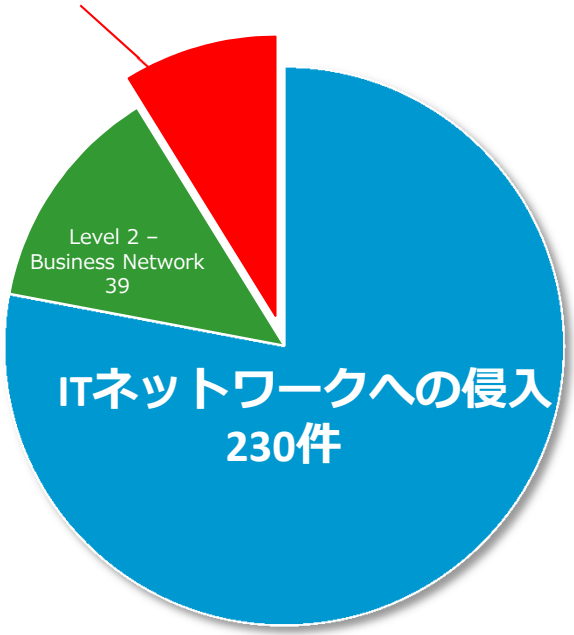
フィジカルとサイバーの融合による脅威の例：サイバー攻撃のレベルが上がり、制御系にまで影響が波及

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**。

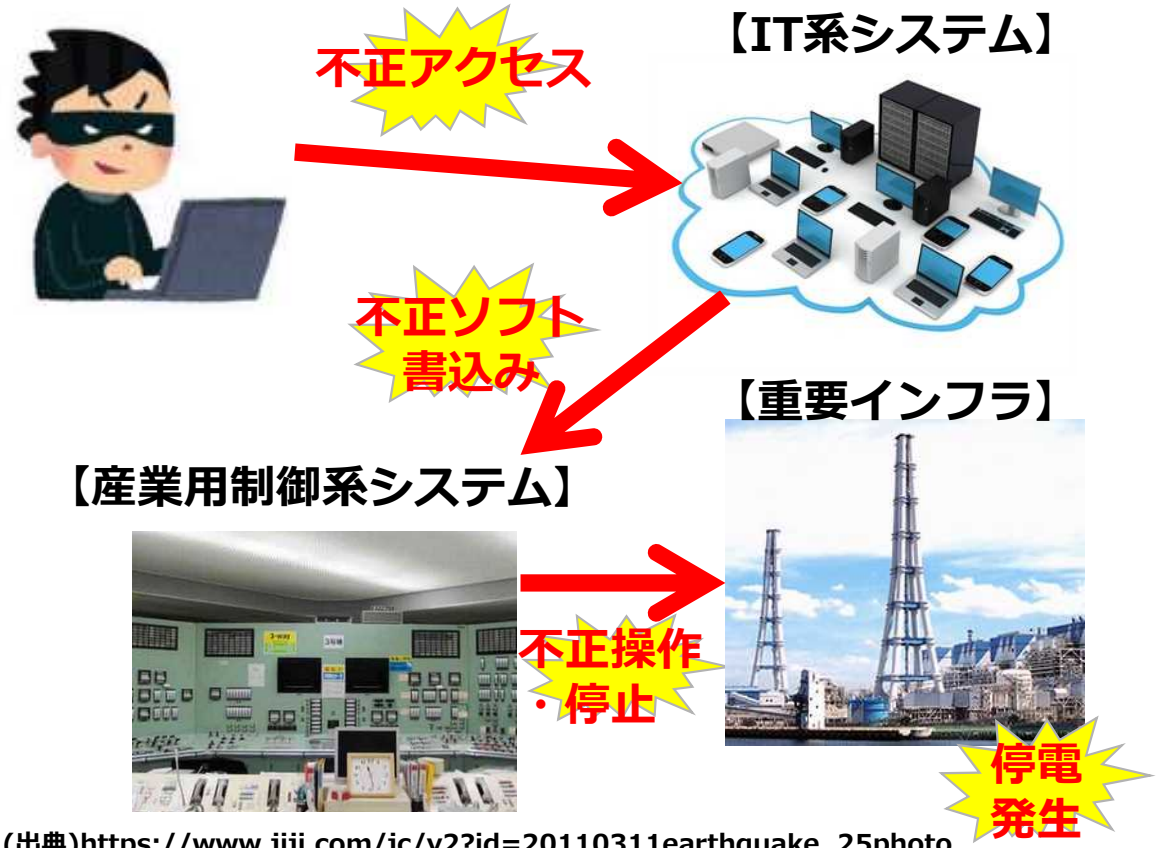
米国の重要インフラへのサイバー攻撃の深さ

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。

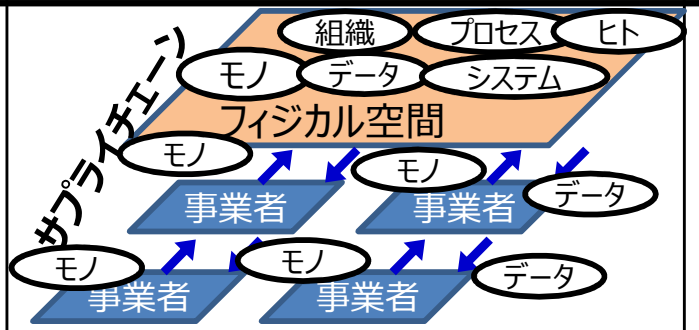
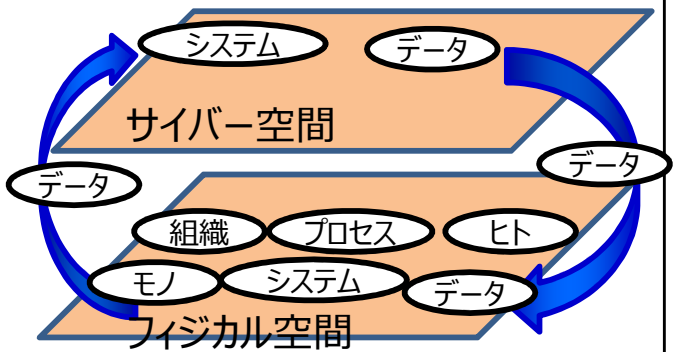
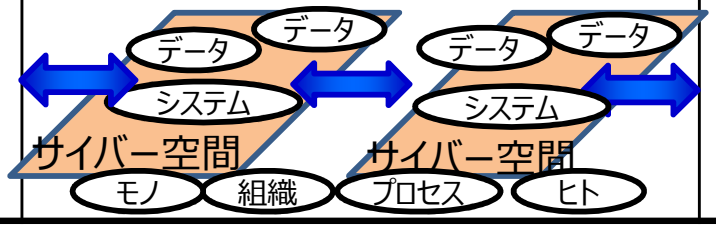
『サイバー・フィジカル・セキュリティ対策フレームワーク』策定へ向けた検討
（１）フレームワークで考慮すべき構成要素を整理する

- 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

来年度以降SWGにおいて具体を検討

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

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)
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

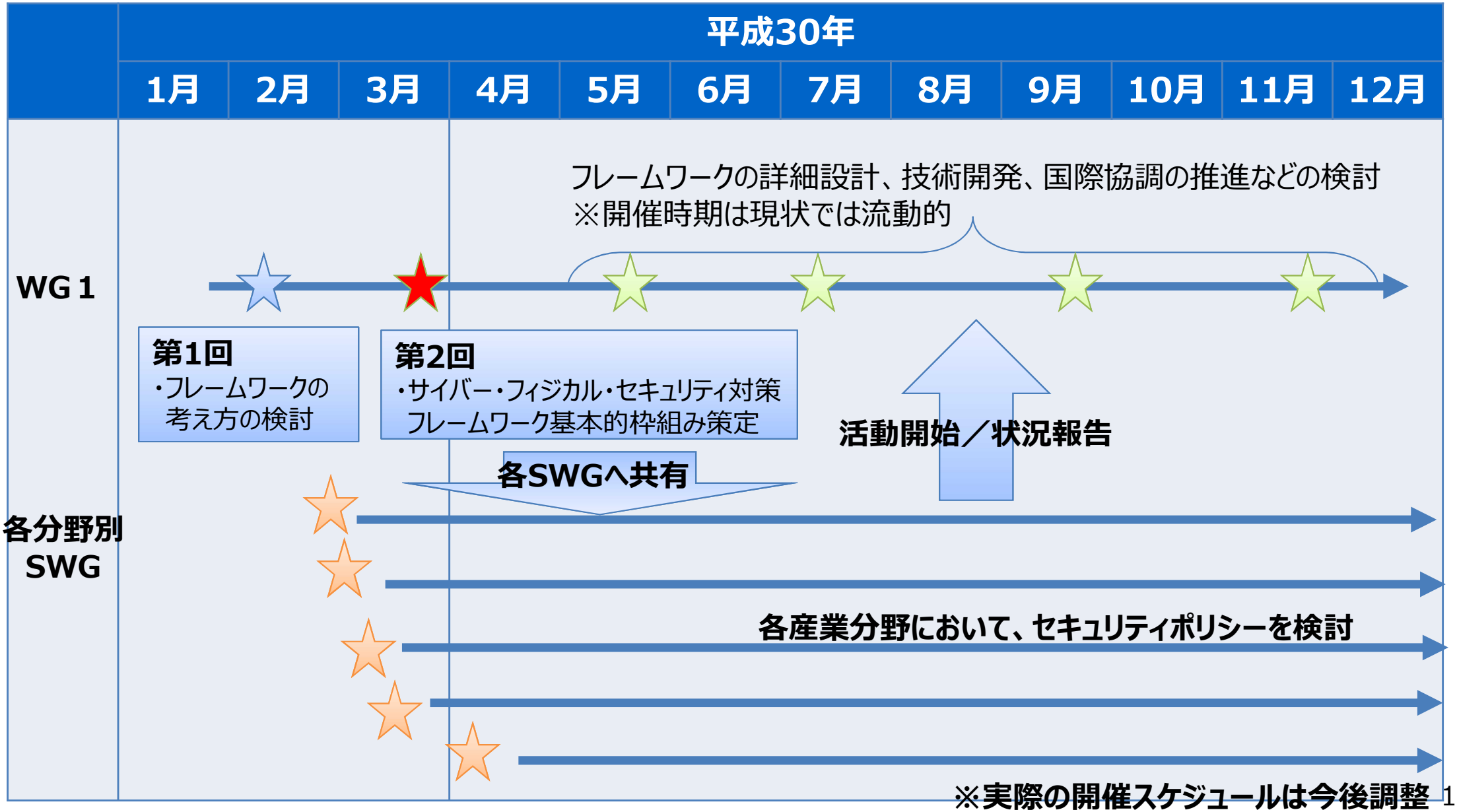
互いに関係

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。



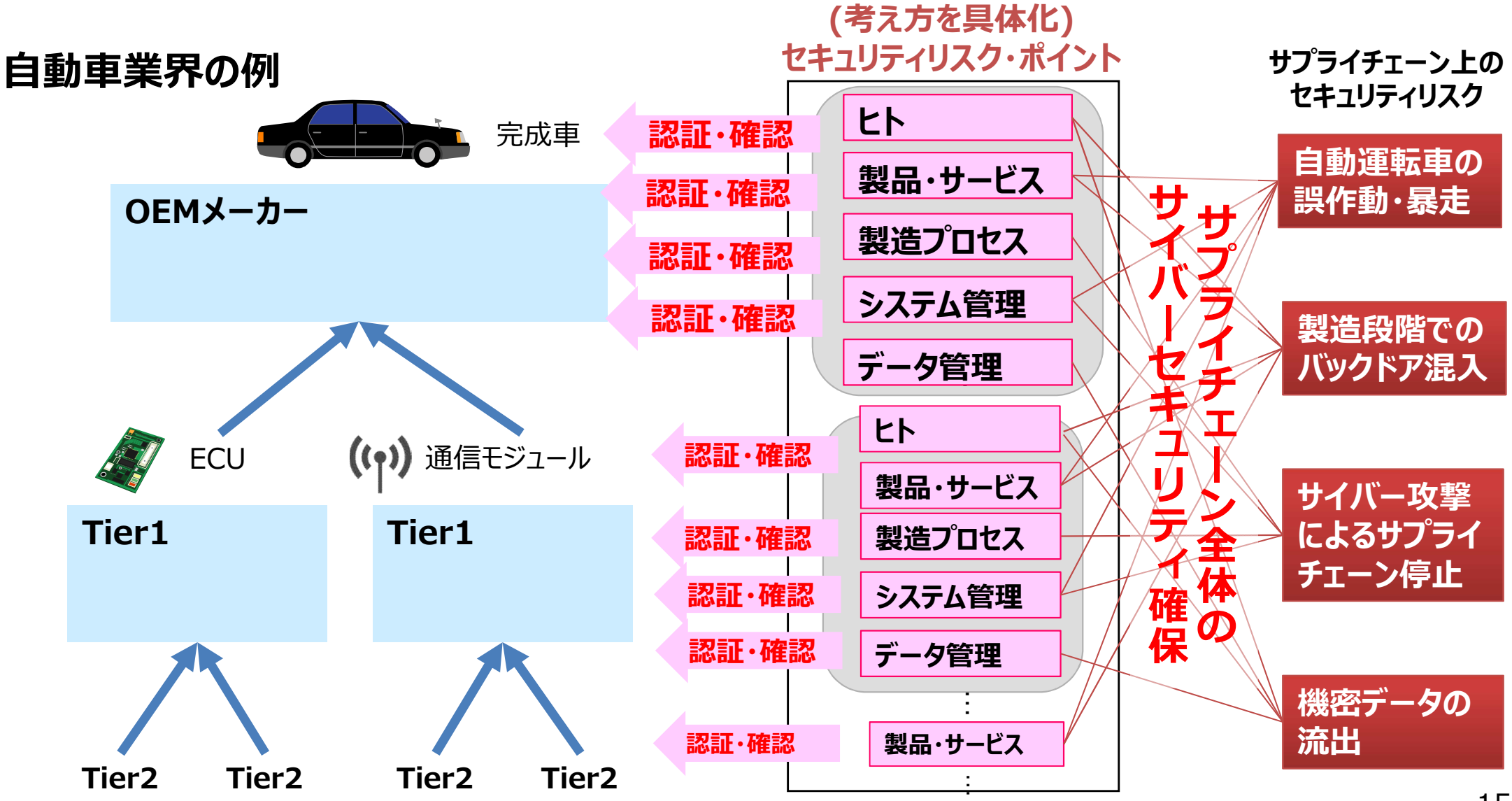
(これから検討を進めていくイメージ)

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

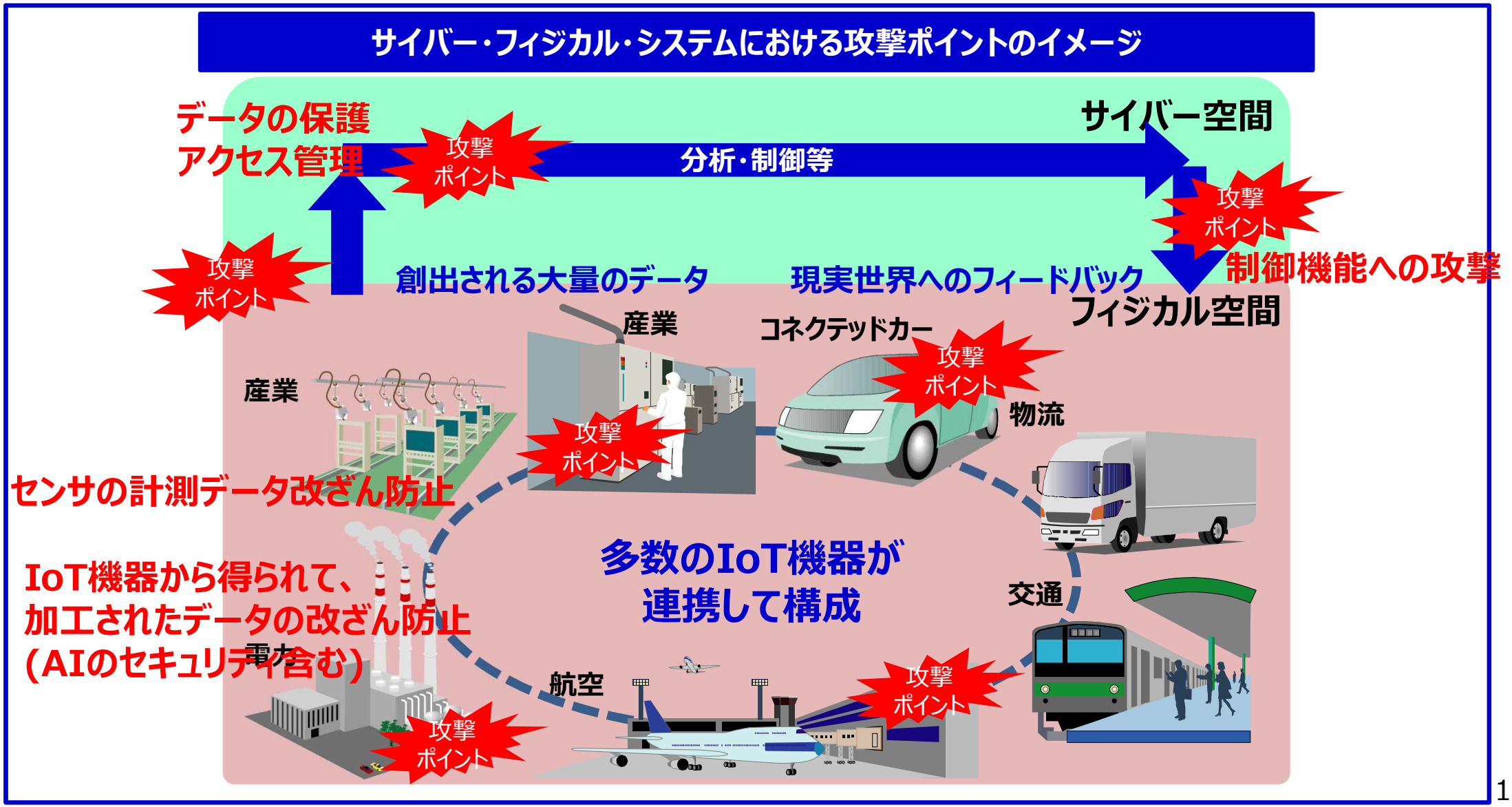
サイバー・フィジカル・セキュリティ対策フレームワークの各切り口の考え方
①サプライチェーンを構成する企業と企業の繋がり

- 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**。



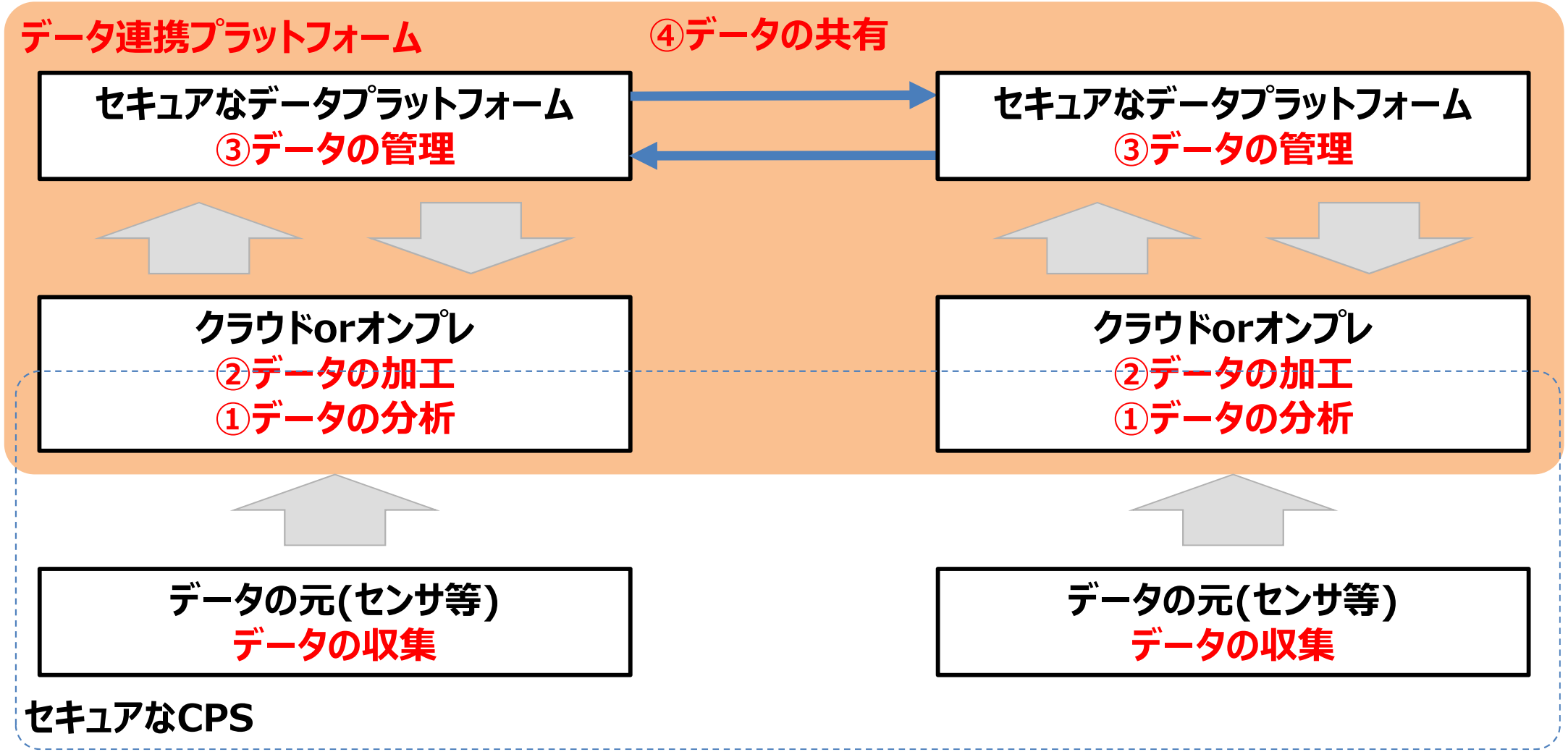
サイバー・フィジカル・セキュリティ対策フレームワークの各切り口の考え方
②フィジカル空間とサイバー空間の繋がり

- 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

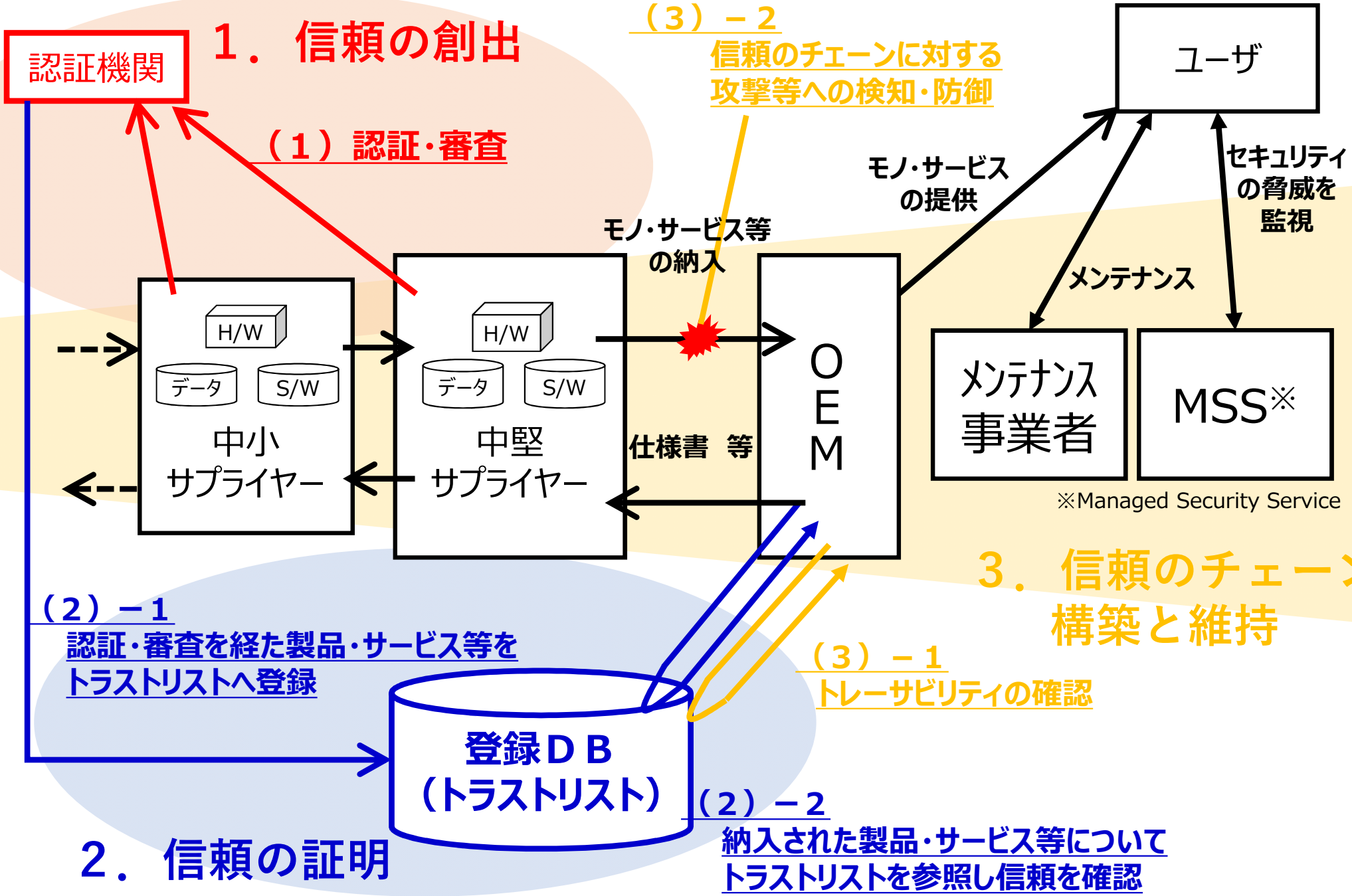
２．信頼の証明

・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

経済産業省

参考資料

サプライチェーンサイバーセキュリティ等に関する海外の動き

経済産業省　商務情報政策局

サイバーセキュリティ課

１．米国における近年の動き

- NIST SP800-171
- NIST Cybersecurity Framework
- ボットネット及びその他の自動化・分散化した脅威に対する対策

２．欧州における近年の動き

（Cybersecurity Certification Framework等）

３．ASEANにおける状況

１．米国における近年の動き

- **NIST SP800-171**
- **NIST Cybersecurity Framework**
- **ボットネット及びその他の自動化・分散化した脅威に対する対策**

米国における近年の動き

- **サイバーセキュリティの視野は、『特定機能の防御（重要インフラ中心）』から『サプライチェーンリスク管理』へ拡大。**

2010.11	米国大統領令(E.O.13556)発出	米国政府全体として、CUI(*1)のセキュリティ強化の取組を開始
2014.02	**Cybersecurity Framework vesion1.0**公表	サイバーセキュリティ対策の全体像を示し、「特定」、「防御」、「検知」、「対応」、「復旧」に分類して対策を記載
2015.06	**NIST SP800-171**策定	非政府機関の情報システム等におけるCUIの保護を目的としたサイバーセキュリティ対策の要件を規定
2016.10	**DFARS Clause252.204-7012** 発行	CDI(*2)を保護対象とし、米国防衛省と契約する者に対し、2017年12月31日までにSP800-171相当のサイバーセキュリティの対応を要求
2017.01	**Cybersecurity Framework version1.1 draft1**公表	**サプライチェーンのリスク管理（Supply Chain Risk Management）**などを追記
2017.05	米国大統領令(E.O.13800)発出	連邦ネットワーク及び重要なインフラストラクチャに対するサイバーセキュリティの強化を指示
2017.12	**Cybersecurity Framework version1.1 draft2**公表	draft1公表後のパブリックコメントを踏まえ**サプライチェーンのリスク管理の重要性の強調**や**サイバーセキュリティリスクの自己評価（Self-Assessing Cybersecurity Risk)**を追記 関係業界は肯定的に受け止め
2018.01	E.O.13800を受けた中間報告を公表	**ボットネット及びその他の自動化・分散化した脅威**に対応するためのエコシステムの強靭性の強化に関する報告書

(*1) Controlled Unclassified Information ; 管理対象となるが秘密指定されていない情報
(*2) Covered Defense Information

NIST SP800-171

- **NIST SP800-171は、CUIの保護を目的に14個のカテゴリと109の項目から構成。**
- **SP800-171の遵守状況に関する政府機関による第三者認証制度はなく、自己宣言という形で準拠したか否かについて判断する自己認証を採用。**

2010.11	米国大統領令(E.O.13556)発出	米国政府全体として、CUIのセキュリティ強化の取組を開始
2015.06	**NIST SP800-171**策定	非政府機関の情報システム等におけるCUIの保護を目的としたサイバーセキュリティ対策の要件を規定
2016.10	**DFARS Clause252.204-7012**発行	CDIを保護対象とし、米国防衛省と契約する者に対し、2017年12月31日までにSP800-171相当のサイバーセキュリティの対応を要求。

NIST SP800-171における14個のカテゴリ

(1) アクセス制御：システムへのアクセスが出来る人／機能を制限すること
(2) 意識向上と訓練：セキュリティポリシーを遵守すること
(3) 監査と責任追跡性：システムの監査を行うとともに責任の追及が出来ること
(4) 構成管理：システムを構成する機器に求められるセキュリティ構成設定を確立すること
(5) 識別と認証：システム利用者、デバイスを識別すること
(6) インシデント対応：インシデントの追跡、報告が出来ること
(7) メンテナンス：組織のシステムのメンテナンスを行うこと
(8) 記録媒体保護：CUIをセキュアに格納するとともにアクセスできる者を制限すること
(9) 人的セキュリティ：システムへのアクセスを行う個人を審査すること
(10) 物理的保護：組織のシステム、装置等への物理的アクセスを制限すること
(11) リスクアセスメント：情報資産のリスクを適切に評価すること
(12) セキュリティアセスメント：セキュリティ管理策を定期的に評価すること
(13) システムと通信の保護：システムの鍵となる通信を監視し、制御し、保護すること
(14) システムと情報の完全性：タイムリーに情報及びシステムフローを識別すること

NIST SP800-171

- **2016年10月、DFARS Clause252.204-7012が発行され、CDIを保護対象とし、米国防衛省と契約する者に対し、2017年12月31日までにSP800-171相当のサイバーセキュリティの対応を要求。**

DFARS Clause252.204-7012における要求事項

（1）主なセキュリティ要求事項

- **NIST SP800-171のセキュリティ要求事項を満たすこと。**
- **外部のクラウドサービスプロバイダ**を利用して、保護対象防衛情報を保存・処理・送信しようとする場合には、米国のクラウドの基準Fed RAMP（NIST SP800-53を満たした事業者が提供するクラウドサービス）の要求事項と**同等の基準**を満たしており、そのサービスプロバイダが、サイバー事案報告等の要求事項を満たしていることを要請。

（2）サイバー事案報告の要求

- 契約業者が、保護対象防衛情報に影響を及ぼす等のサイバー事案を発見した場合には、国防省にサイバー事案を**速やかに報告**。
- 保護対象防衛情報の漏えいの証拠を調査。
- 国防省が実施するフォレンジック分析に必要な追加情報又は機器へのアクセスを受け入れること。

（3）下請け契約の扱い

- 契約業者は、**下請け業者の業務に必要な情報が、保護対象防衛情報であるか否かを判断し、該当する場合には、DFARS Clause 252.204-7012に基づく保護を要求**する。

NIST Cybersecurity Framework

- **2017年、NIST（アメリカ国立標準技術研究所）のCybersecurity Frameworkの改訂ドラフト版が公表され、『サプライチェーンリスク管理』を追記。**

2014.02	**Cybersecurity Framework vesion1.0**公表	サイバーセキュリティ対策の全体像を示し、「特定」、「防御」、「検知」、「対応」、「復旧」に分類して対策を記載
2017.01	**Cybersecurity Framework version1.1 draft1**公表	**サプライチェーンのリスク管理（Supply Chain Risk Management）**などを追記
2017.12	**Cybersecurity Framework version1.1 draft2**公表	draft1公表後のパブリックコメントを踏まえ**サプライチェーンのリスク管理の重要性の強調**や**サイバーセキュリティリスクの自己評価（Self-Assessing Cybersecurity Risk)**を追記 関係業界は肯定的に受け止め

Cybersecurity Frameworkにおける5つの分類

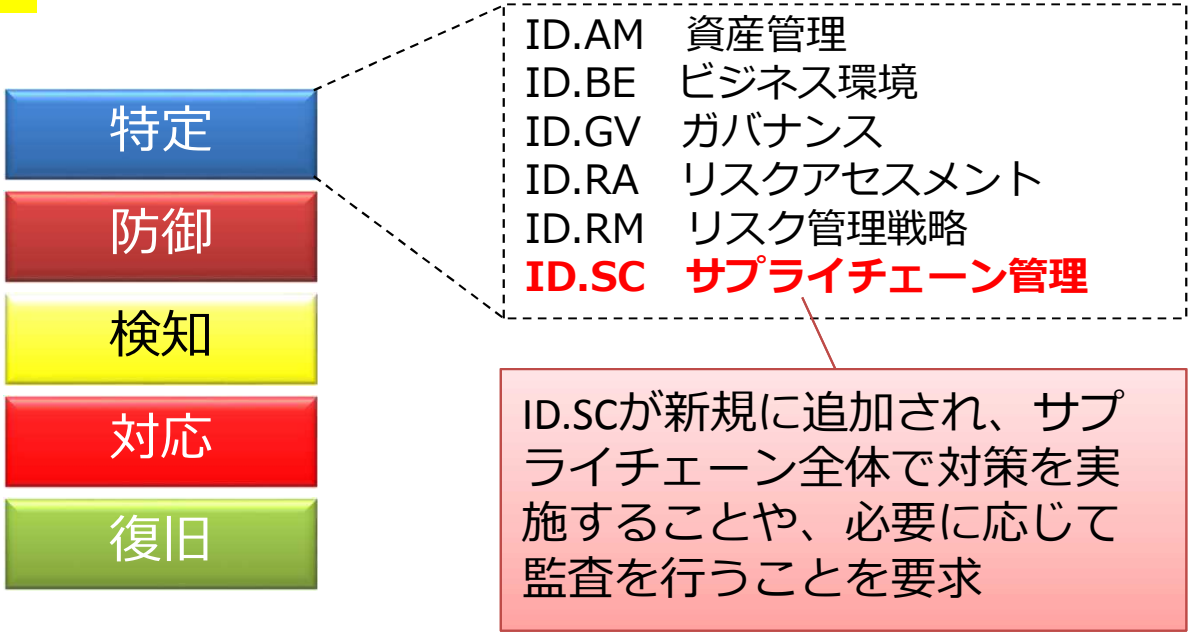
特定：最初に、組織としてサイバーセキュリティに関する方針を決定する”、“どのようなリスクがあるかを特定する”等

防御：リスクの多寡に応じて適切な予防策を講じる

検知：防御策を監視することで突破されそうになった（あるいはされた）ことをいち早く察知する

対応：異常が検知され必要な暫定処置を講じる

復旧：恒久措置を施し元通りの状態に回復させる



NIST Cybersecurity Framework

- **特に、Cybersecurity Framework version1.1 draft2では、**
  - **『サプライチェーンリスク管理（Supply Chain Risk Management）』**
  - **『サイバーセキュリティリスクの自己評価（Self-Assessing Cybersecurity Risk)』**

  の重要性がより強調された。

『サプライチェーンリスク管理』に関して、draft2でSection3.3の本文を改訂。

Supply chains are a complex, globally distributed, …. Given these complex and interconnected relationships, **supply chain risk management (SCRM) is a critical organizational function.**…. **A primary objective of cyber SCRM is to identify, assess, and mitigate "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable** due to poor manufacturing and development practices within the cyber supply chain. "

サプライチェーンは、複雑で、グローバルに広がっており、…。これらの複雑な相互作用の関係のもと、**サプライチェーンリスクマネジメント(SCRM)は、重要な組織としての役目である。**…。**サイバーSCRMの主目的は、**「サイバーサプライチェーンにおける不十分な製造や開発の実施により、**潜在的に悪意のある機能、偽物もしくは脆弱性がある製品やサービス」を特定、評価、軽減することである。**

『サイバーセキュリティリスクの自己評価』に関して、draft2でSection4.0のタイトル及び本文を改訂。

4.0 **Self-Assessing Cybersecurity Risk** with the Framework
…. Self-assessment and measuring should improve decision making about investment priorities.

4.0 フレームワークを用いた**サイバーセキュリティリスクの自己評価**
…。自己評価と測定により投資の優先順位の決定を改善すべきである。

ボットネット及びその他の自動化・分散化した脅威に対する対策

- **2017年5月、トランプ大統領が「サイバーセキュリティ強化のための大統領令」に署名。**
- **2018年１月、大統領令を踏まえた報告書案を公表（セキュリティ確保のためのエコシステムの形成を強調）。**
- **2018年５月、本報告書を大統領に報告予定。**

大統領令

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure（連邦ネットワーク及び重要なインフラストラクチャに対するサイバーセキュリティの強化に関する大統領令）　2017年5月11日
①連邦政府のネットワーク　②重要インフラ　③国家／国民のためのサイバーセキュリティ(ボットネット対策含む)に関して各連邦政府機関の長に対し、期限以内に大統領に報告書を提出するよう指示

報告書案

A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats（ボットネットおよびその他の自動化・分散化した脅威に対するインターネット・通信のエコシステムの強靭性の強化に関する報告書）　2018年1月5日

報告書の概要：自動化・分散化した脅威（ボットネット）に対処する**５つの目標**を設定

1. 適応可能、持続可能かつ安全な技術市場環境の実現に向けた明確な道筋の明確化
2. 進化する脅威に動的に対応するためのインフラのイノベーションの促進（エコシステムのすべてのドメインでの対応）
3. ネットワークのエッジにおけるイノベーションの促進による、悪意ある行為の防止、検出、影響の緩和
4. 国内外のセキュリティ、インフラ、運用技術の各コミュニティ間の連携の構築
5. エコシステム全体にわたる啓発・教育の強化

２．欧州における近年の動き

（Cybersecurity Certification Framework等）

欧州における近年の動き

- 欧州では、**重要インフラは最新のサイバーセキュリティ対応を実装することが求められ**（NIS Directive）、**ネットワークに接続する機器のセキュリティに関して認証・確認のための自主的フレームワーク（Cybersecurity Certification Framework）を整備**することを掲げている

【欧州】

- **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を検討**

  ⇒方向性：規制ではなく、自主的な仕組み　産業界：国際標準に基づく自己適合宣言を主張している。
- 2016年、ＥＵ各国の重要インフラ事業者（エネルギー、交通、銀行、金融等）に対して、**セキュリティ対策を義務化。その際セキュリティ関連国際標準を考慮することを指示。（NIS 指令）**
- 2018年から、EUの顧客データを扱う企業に対して、データ処理制限、流出などの際の通知義務などをEU域外においても義務化。（EU一般データ保護規則：GDPR）

【ドイツ】

- ＮＩＳ指令に先立ち、2015年にＩＴセキュリティ法を制定し、重要インフラ事業者（エネルギー、交通、ICTs、交通、金融・保険、健康、水、食糧）に対して以下を要求。

  ①サイバーセキュリティに係る**最低限の基準を満たしていることについて情報セキュリティ庁の証明を得ること**
  ②**２年ごとにセキュリティ監査等を受けること**
  ③**サイバー攻撃と思われる事象が発生した場合に情報セキュリティ庁へ報告すること**
- 現在、small office and homes のルーターのテクニカルガイドラインを作成中（任意制度）

欧州における近年の動き

・2017年9月13日、ユンカー欧州委員会委員長の施政方針演説でサイバーセキュリティに関する言及があり、これを受けたデジタル単一市場の施策の一環として、新たにサイバーセキュリティ認証フレームワークの導入を検討していく旨公表。併せて、サイバーセキュリティに関するENISA規則※の修正提案を承認。

・同年11月20日には、ENISAが、「IoTのベースラインセキュリティの推奨事項」を発表。

※Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

1．欧州委員会がENISAの評価の中間報告をもとに複数のオプションを提案（2017年7月7日）
①ENISAの今後の組織と戦略の方向性
②欧州デジタル単一市場におけるサイバーセキュリティ認証フレームワーク（Cybersecurity Act）

2．パブリックコメント（2017年7月7日 - 2017年8月4日）

3．インパクトアセスメント発表（2017年9月8日）
欧州委員会がENISAの過去の実績を評価するとともに、提案内容について、パブリックコメント、有識者の意見、関係者へのアンケート等を元に各オプションを採用した場合の影響を評価

4．ユンカー欧州委員会委員長による施政方針演説の中で、サイバーセキュリティについて言及
欧州委員会がインパクトアセスメントを元にしたENISAの修正提案を承認（2017年9月13日発表）
※提案（**Cybersecurity Package**）の承認であって、提案内容をそのまま採択したわけではない

①ENISAを恒久的な機関として機能を強化
・当初噂されていたEUのセキュリティ庁ではない
・EUにおけるセキュリティの標準化や認証に関する業務が含まれることになった

②セキュリティについて各国、セクター別の支援を行い、認証及び表示の枠組みについて既存の認証メカニズムに基づいて構築することを提案
・直接的な運用認証制度は導入しない
・新たな技術標準の開発は行わない

⇒次頁　詳細

5．ENISAが「IoTのベースラインセキュリティの推奨事項」を発表（2017年11月20日）
一般的な課題を抽出し、関係者が解決するために有用となる考え方やツール（既存の規格、ガイドライン、研究資料等）やベストプラクティスを紹介するレポート。

欧州のCybersecurity Certification Frameworkのポイントと欧州委員会にて承認された提案

欧州のCybersecurity Certification Frameworkのポイント	○ICT機器とサービスについて、**サイバーセキュリティ認証フレームワーク(Cybersecurity Certification Framework)を構築し、欧州内におけるサイバーセキュリティ認証制度を確立する**ことで、欧州におけるデジタル単一市場の信頼性、セキュリティを確保する。 ○欧州サイバーセキュリティ認証フレームワークは、**法の定めがない限り自主的なもの(voluntary)であり、直ちに事業者に規制を課すようなものではない**。
欧州委員会にて承認された提案	ICT機器及びサービスのための欧州Cybersecurity Certification Frameworkを確立し、サイバーセキュリティ認証の分野におけるENISAの本質的な機能及び任務を規定する。 現在の提案は、欧州のサイバーセキュリティ認証制度を支配する規則の全体的な枠組みを定めている。 この提案では、**直接的な運用認証制度を導入するのではなく、特定のICT機器/サービスのためのサイバーセキュリティ認証制度をENISAが作成**する。 この認証制度では、**製品が遵守する必要のある技術要件及び評価手順に関して既存の基準を使用し、技術標準自体を開発しない。**（例えば、現在、**SOG-IS MRA**スキームで国際CC規格に照らしてテストされているスマートカードなどの機器に関するEU全体の認定は、このスキームをEU全体で有効にすることを意味する。） 欧州のサイバーセキュリティ認証制度が採用されると、ICT機器の製造業者またはICTサービスの提供者は、自らの選択した適合性評価機関に自社の機器またはサービスの認証申請書を提出することができる。適合性評価機関は、指定された特定の要件を満たしていればその証明書を発行する。 **監視、監督、執行の任務は加盟国に委ねられている。**加盟国は、1つの認証監督当局を提供しなければならない。この権限は、適合性評価機関のコンプライアンスと、自国の地域に設置された適合性評価機関が発行した証明書と、この規則及び関連する欧州のサイバーセキュリティ認証制度の要件とを監督することを任される。

EU Cybersecurity Packageへの反応概要

2017年9月13日に発表された「Cybersecurity Package」に対して、意見募集が12月6日まで行われ、欧米の32の事業者・団体から意見が提出された。

サイト：「https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en」

ENISAの機能拡大

概ね賛同されたが、各国の規制機関との関係性、サイバーセキュリティ認証フレームワーク策定における機能について、詳細が明確でないと懸念する意見がある

サイバーセキュリティ認証フレームワーク

デジタル単一市場の形成に資するという面では概ね賛同されたが、認証の範囲、策定方法と策定に関わる関係者の選択、既存の規制との関係性、グローバルとの断絶の懸念、事業者（特に中小企業）の負担増大への懸念等について、詳細が不明であることから多数の意見が寄せられている。

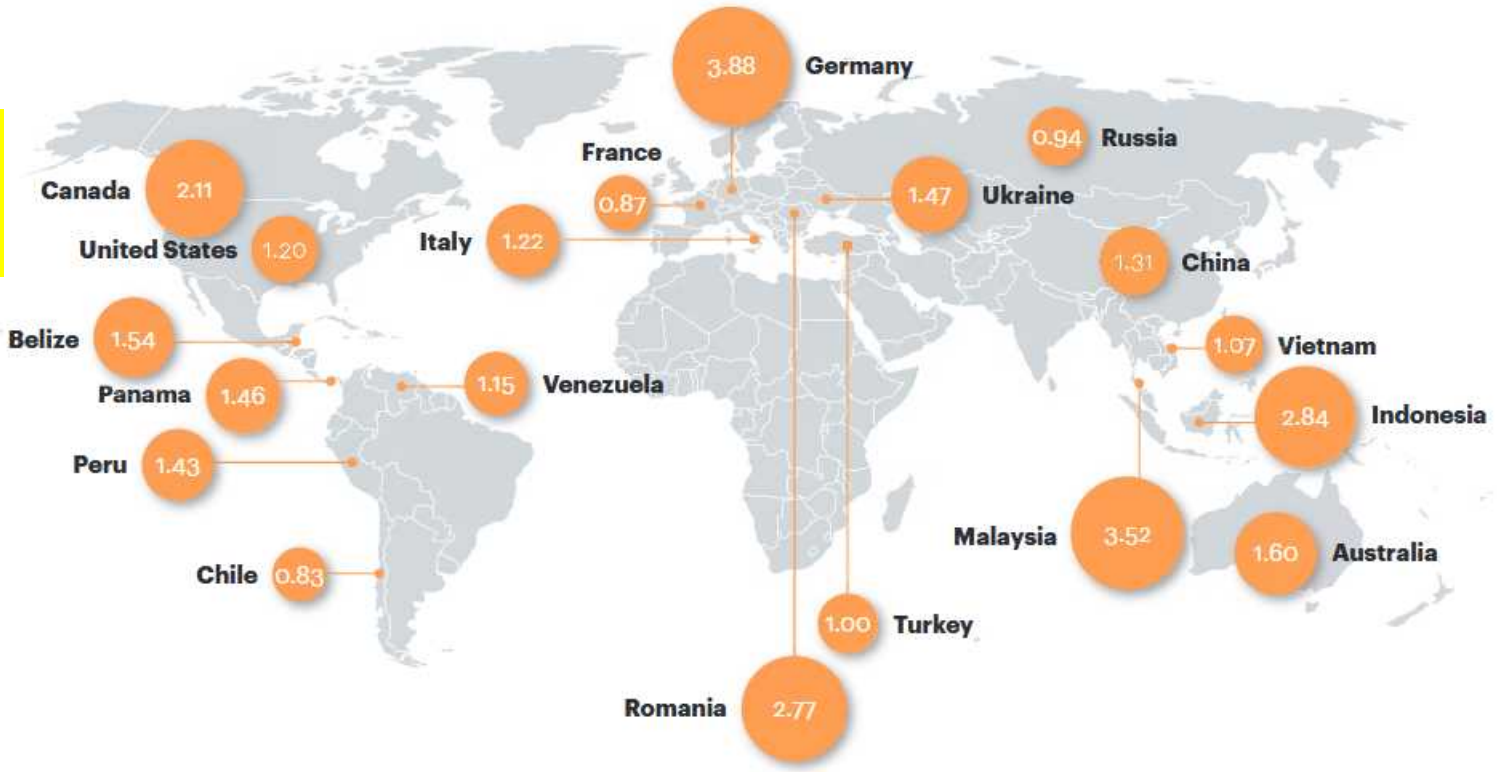
- **認証制度の範囲を明確化：BtoCとBtoB、IoTとIIoT、水平か垂直か、セクター等の分野的なものと、製品やサービスなのかプロセスやシステムなのか等の対象についての明確化**
- **国際標準へ準拠：ISO27000シリーズ、IEC62443シリーズ、CCが論点の中心だが、意見は分かれている**
- 策定の方法：WTO TBT協定、NLF等の手続きに則していることといった意見が複数
- 既存の規制の尊重：十分に機能している国家単位やセクター単位の既存の規制を尊重
- **策定に向けた議論のあり方：意見を表明している事業者・団体の多くは、ステークホルダーとして議論に加わることを強く希望しており、業界団体はセクターごとの自主的な仕様の策定を主張**
- **認証の方法：自己宣言をベースとして、重要インフラ等においてはリスクの大きさに合わせて外部（第三者）認証を追加すべきとする意見が多い**
- 認証のレベル：範囲や方法とも関連して、リスクベースで認証のレベルを設けるべきという意見と堅牢性を重視意見とに分かれている。ただし後者は主にセキュリティ認証を行っている企業や団体の意見であるため利益誘導の面があると思われる
- 啓発と教育：認証制度やその意味が利用者と事業者双方に認知されなければ意味が無いため、啓発と教育についての意見が多数見られた。

3. ASEANにおける状況

ASEANにおける状況

- **ASEAN諸国は、サイバー攻撃の活動拠点となっている。**
  - マレーシア、インドネシア、ベトナムは、遮断された不正なWEB活動の起点となっている比率が高く、マルウェアの攻撃に悪用されている。
  - ベトナムは、2015年12月から2016年11月までの間に、168万個のIPアドレスの遮断を記録した。さらに、2016年に発生したIoT機器に対する攻撃の起点に悪用された数が世界で5番目に多かった。

Blocked suspicious Web activity, by country of origin (expected ratio = 1.0)

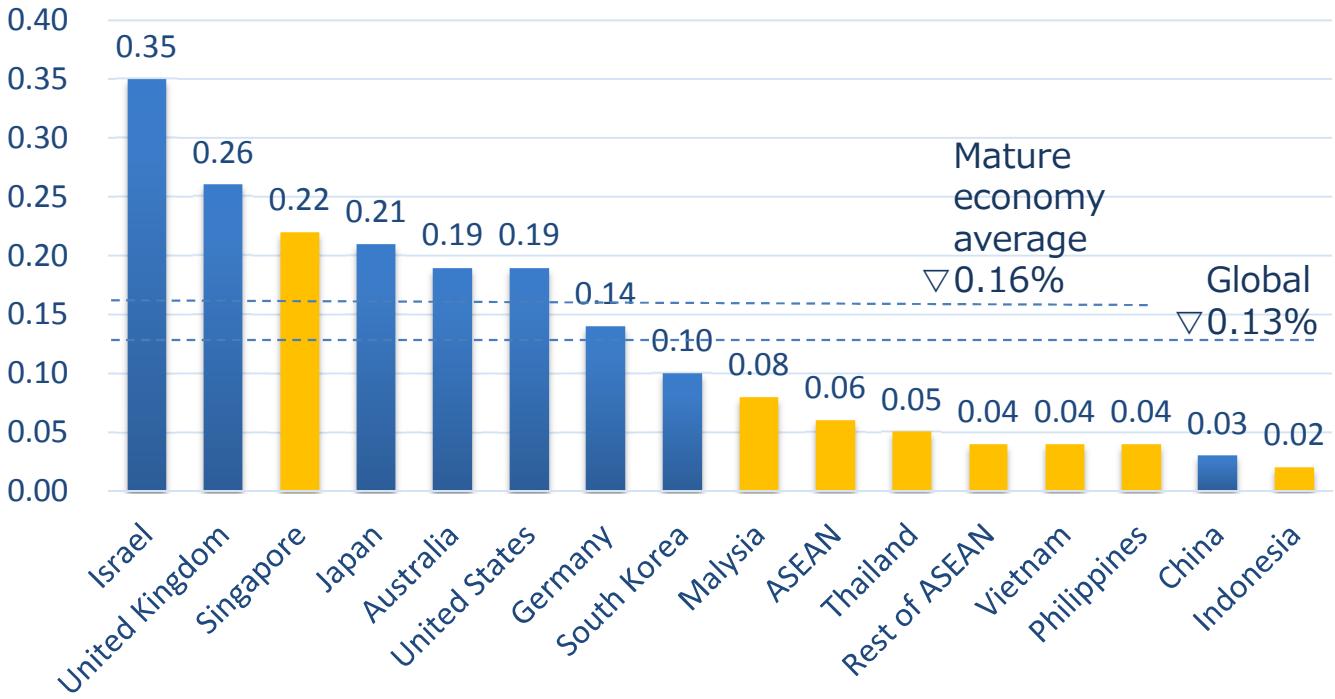


出典：「A.T. Kearney, “Cybersecurity in ASEAN—An Urgent Call to Action”」より引用

ASEANにおける状況

- **サイバーセキュリティに対するポリシーが不十分。**
  - ASEAN地域におけるサイバーレジリエンスは、一般的に低いという評価 （特に、ポリシー、ガバナンス、サイバーセキュリティ能力）。
  - 産業界もリスクを過少評価しており、結果として、サイバーセキュリティに対する投資が不足しているという指摘あり。

Cybersecurity spending (% of GDP for 2017)



出典：「A.T. Kearney, “Cybersecurity in ASEAN—An Urgent Call to Action”」より引用