経済産業省

資料4

『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性

令和元年8月2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. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

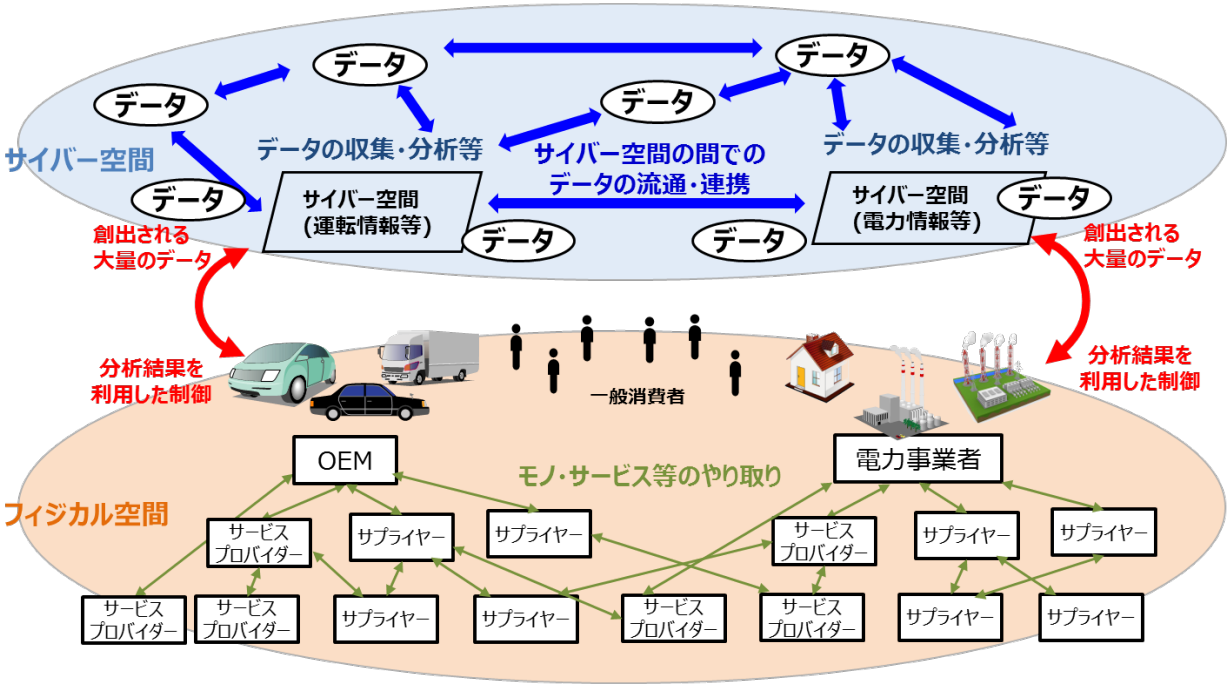
2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項

＜サプライチェーン構造の変化＞
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の策定

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要。**
- 経済産業省では、「Society5.0」における**セキュリティ対策の全体像を整理**し、産業界が自らの対策に活用できる**セキュリティ対策例をまとめた、『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）』を平成31年4月に策定。**



Society5.0の社会におけるモノ・データ等のつながりのイメージ

サイバー空間で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空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

＜三層構造と６つの構成要素＞
サイバー・フィジカル一体型社会のセキュリティのためにCPSFで提示した新たなモデル

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造と６つの構成要素**）を提示。

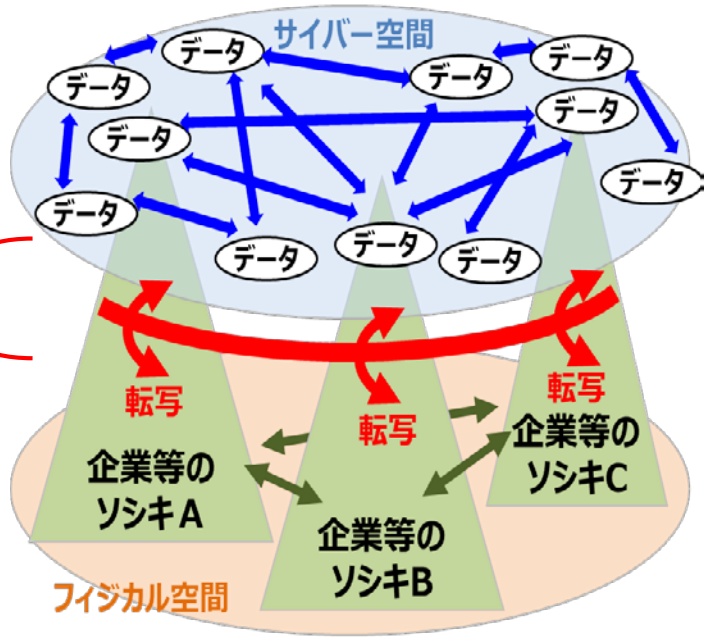
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

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



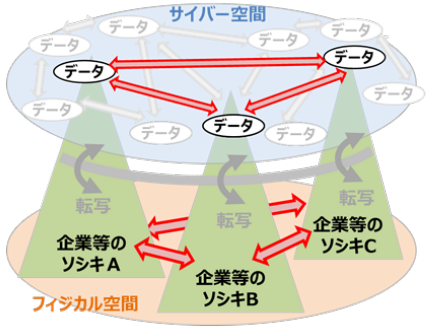
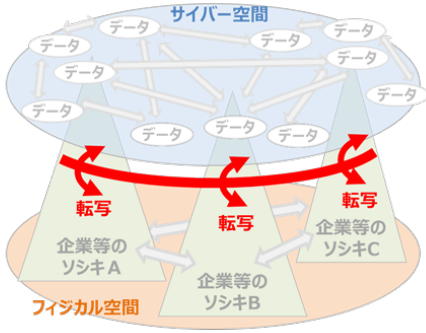
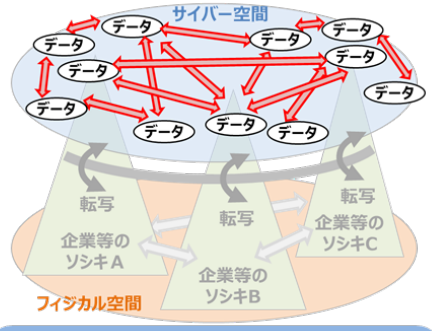
6つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を6つに整理**

構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
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
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
プロシージャ	• 定義された目的を達成するための一連の活動の手続き
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

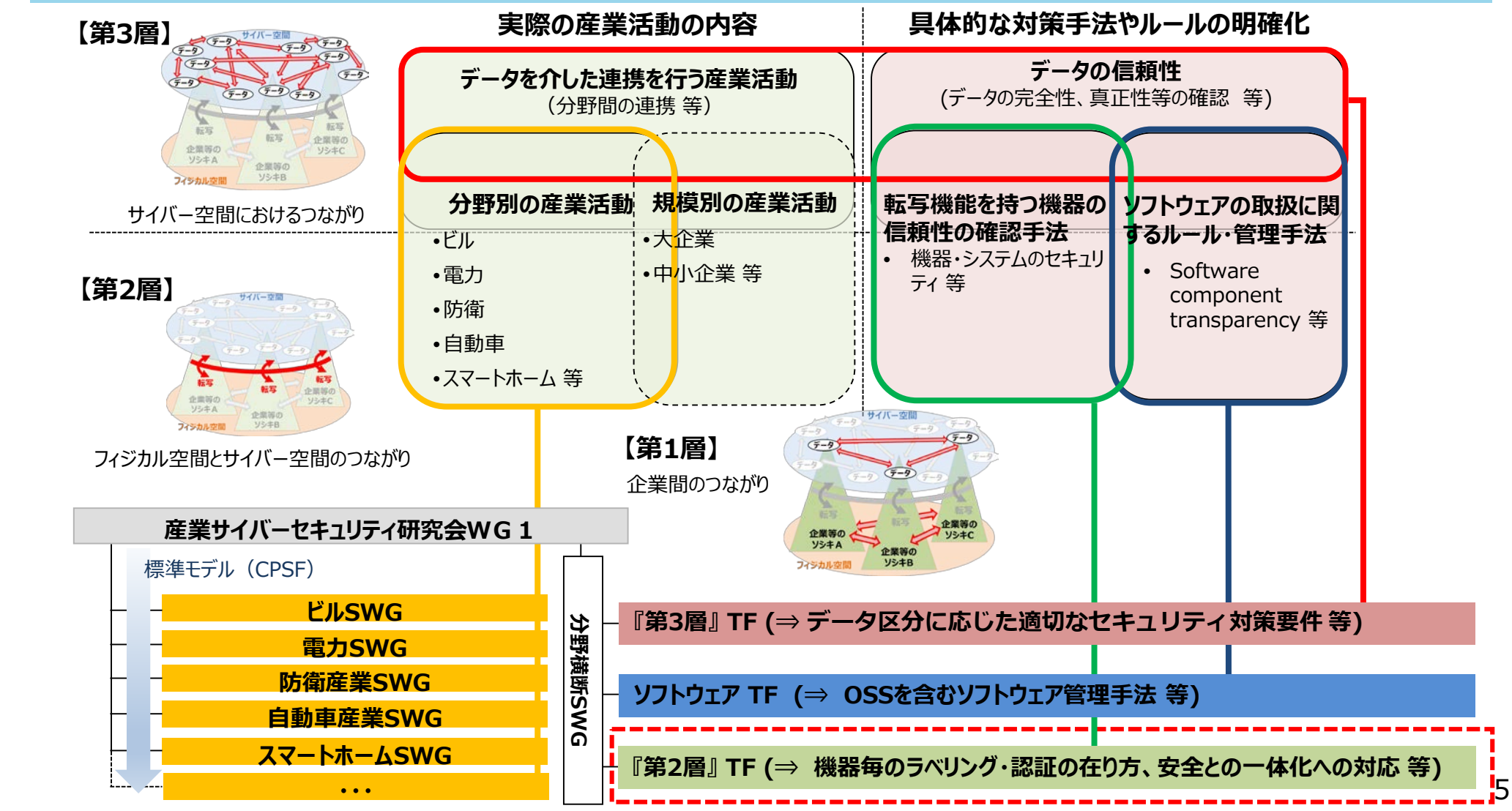
＜CPSFの全体概要＞
三層構造モデルに基づきリスク源、対応方針等を提示

- サプライチェーンの信頼性を確保する観点から、産業社会を３つの層から捉え、それぞれにおいて**守るべきもの、直面するリスク源、対応方針**等を整理。

	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及び正確な転写の証明	• データの加工・分析 • データの保管 • データの送受信
セキュリティインシデント	• 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（構成要素ごとに整理）	• 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	■ 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

CPSFに基づくセキュリティ対策の具体化・実装の推進

- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）を新たに設置。**



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（CPSF）と
その実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に
向けた諸外国の検討状況

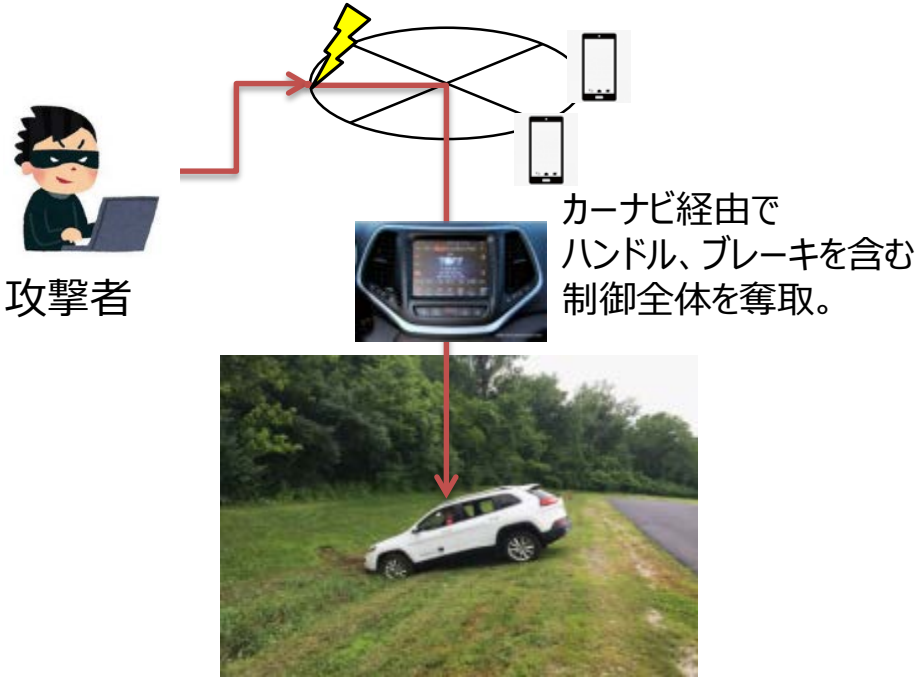
4. 本タスクフォースにおける検討事項

IoTの進展に伴う新たなセキュリティ上の脅威：新たにつながるデバイス

- これまでネットワークに接続されていなかった自動車やカメラなどの機器が、WiFiや携帯電話網などを介してインターネットに接続されることにより、新たな脅威が発生し、それに対するセキュリティ対策が必要となった。

自動車へのハッキングよる遠隔操作

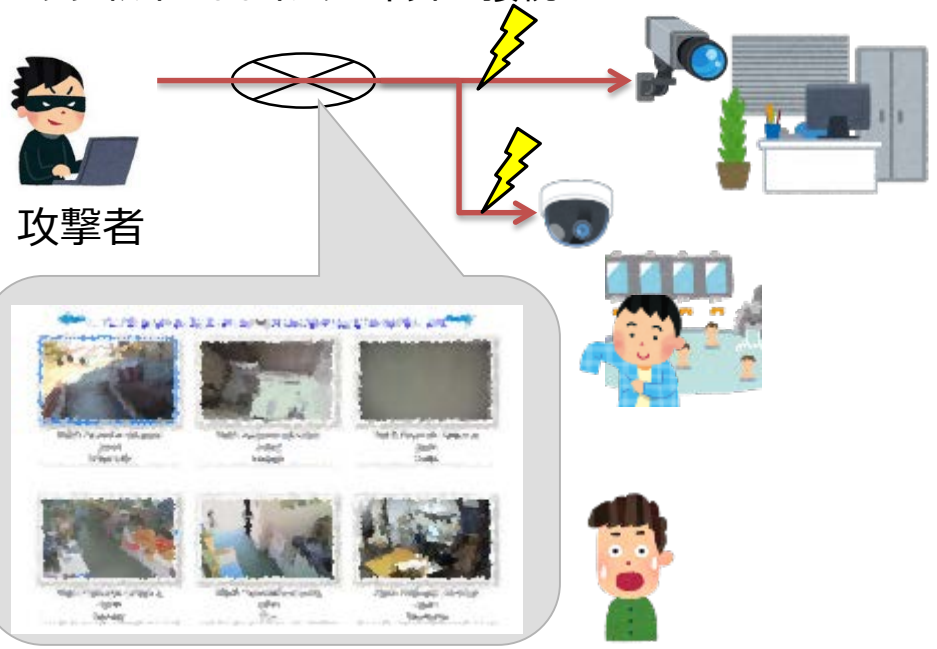
携帯電話網経由で遠隔地からハッキング



人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

監視カメラの映像がインターネット上に公開

利用者が気づかないまま、ID/パスワードを
デフォルトのままインターネットに接続



セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**。

IoTの進展に伴う新たなセキュリティ上の脅威：ドローン・航空機の脅威

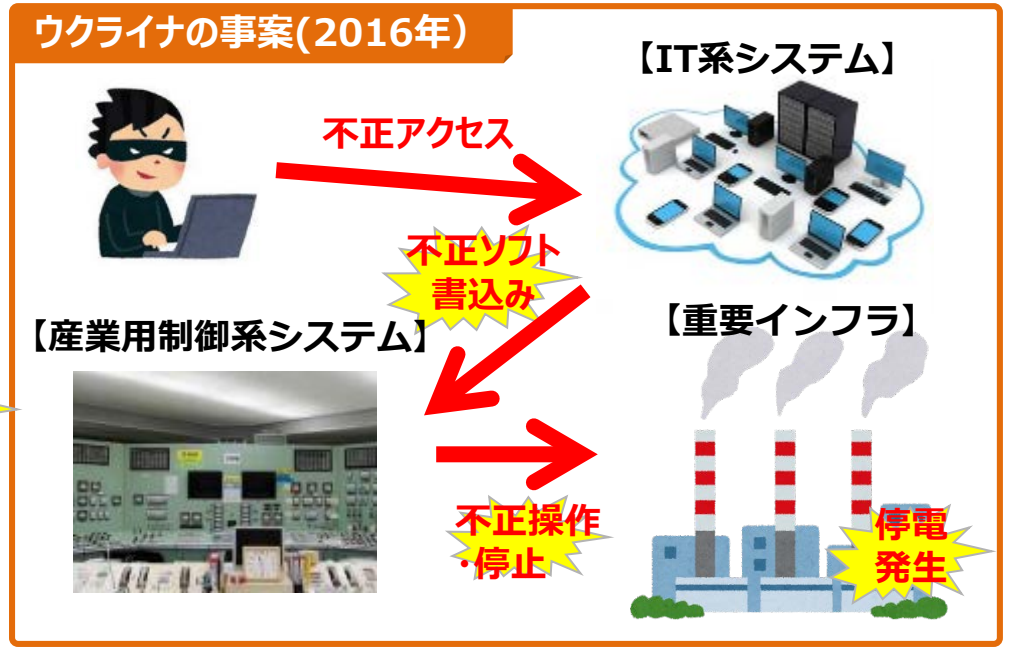
- 2012年、テキサス大学オースティン校の研究グループが**GPS信号を用いてドローンのハッキング**に成功。また、2018年に横浜国立大学の研究グループは、**超音波によりドローンの超音波距離計を攪乱**させ、制御を喪失させることを実証。
- 米国国土安全保証省（DHS）でも、2016年に民間航空機のサイバーセキュリティ脆弱性評価において、遠隔からのボーイング757のハッキングに成功し、民間航空機のサイバー攻撃に対する脆弱性を認識。

テキサス大学の実験

横浜国立大学の実験

制御系にも影響が波及：
制御系システムへのサイバー攻撃

- 米国ICS-CERTは、**米国の重要インフラへのサイバー攻撃のうち一割は、制御系まで到達**していると報告。
- ドイツ情報セキュリティ庁（BSI）は、2014年にドイツの製鉄所において、外部からの制御システムの**不正操作により溶鉱炉が制御不能**となり、生産設備に甚大な損傷が発生したと報告。
- 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。検体検査の結果から、**2016年の攻撃(CrashOverRide)** は、**サイバー攻撃のみで停電が起こされた可能性があると報告されている。**



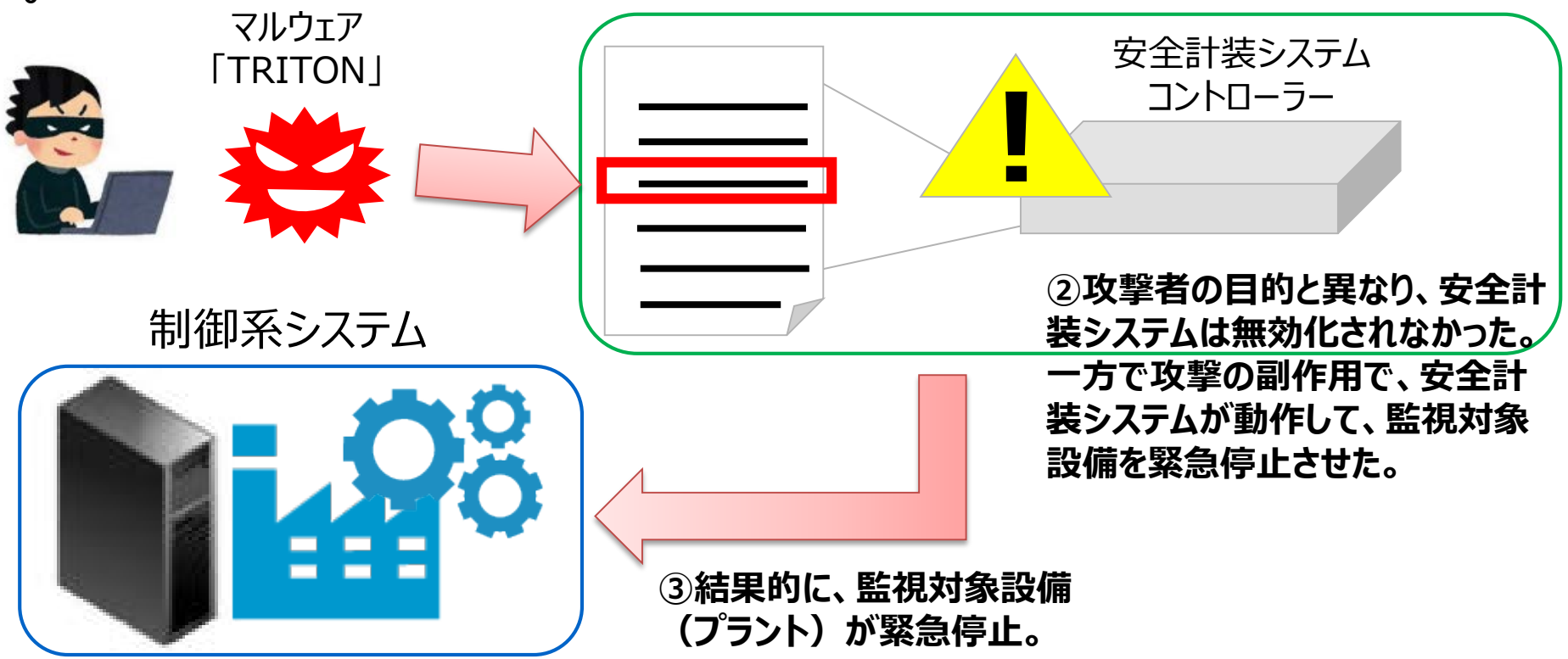
（出典）IT Security Situation in Germany 2014 （BSI）に基づき経済産業省作成
（図は参考）https://www.jiji.com/jc/v2?id=20110311earthquake_25photo，https://upload.wikimedia.org/wikipedia/commons/1/1f/Alto_horno_antiguo_Sestao.jpg

制御系にも影響が波及：
安全計装システムの不正操作による制御系システムの緊急停止

- 米国ICS-CERTの報告では、2017年8月、仏大手重電メーカーであるSchneider Electric社製の安全計装システムがマルウェア「TRITON」の攻撃を受け、**監視していた制御装置（プラント）が緊急停止。**

①設定用アプリケーションになりすまし、攻撃用スクリプトの注入（安全計装システムの無効化を目的としていたとみられる）。

安全計装システム　プロセスの状態を監視し、危険な状態になったときにプロセスの安全を確保するシステム



②攻撃者の目的と異なり、安全計装システムは無効化されなかった。一方で攻撃の副作用で、安全計装システムが動作して、監視対象設備を緊急停止させた。

③結果的に、監視対象設備（プラント）が緊急停止。

IoT機器のサプライチェーンリスク：ASUS社端末におけるアップデート機能を悪用した攻撃

- 台湾のIT機器大手ASUS社※1において、正規のアップデートサーバが攻撃を受け、当該サーバから**端末向けに配布されたアップデートファイルを介し、数十万の同社端末がマルウェアに感染**する事案が発生。

（出典：MOTHERBOARD誌にてKim Zetter氏執筆。さらにKaspersky社が本件の簡易レポート発出。）

- 正規のダウンロード経路を悪用した同様の攻撃は、2017年に「CCleaner※2」においても発生しており、**マルウェア感染経路の一つ**として警戒を要する。

※1 ASUS社：台北市に本社を置く大手PC、スマートフォン、周辺機器製造メーカー。ソニー、アップル、HP、EPSON等への部品供給も行う。
※2 CCleaner：ハードディスク内部の不要なファイルやレジストリを削除するためのツール。イギリスの Piriform Ltd. が開発。

本事案の詳細（原因・影響等）

- 本攻撃は**2018年6月から11月**にかけて発生。「Shadow Hammer」と呼ばれる。
- 「ASUS Live Update Utility（アップデートサーバ）」による**ソフトウェアアップデートを経由**し、**マルウェア（バックドアファイル）**が**数十万台のASUS端末**に感染。

※ Kaspersky社は数百万台に上る可能性も指摘

- 本攻撃の大きな特徴として、**マルウェアは標的とする端末のMACアドレスをあらかじめ保有**しており、**感染端末のMACアドレスを参照し、それが標的端末であるかを識別**していた。

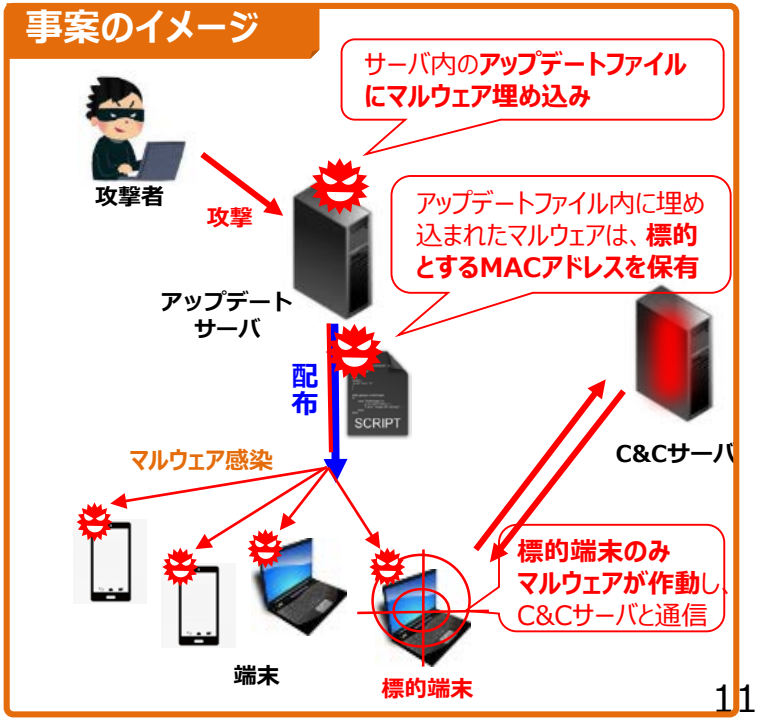
※ Kaspersky社は、200の検体サンプルから600の標的MACアドレスを確認している由

- 識別の結果、**マルウェア感染端末が標的端末であった場合、C&Cサーバと通信を開始する攻撃手法**。実際に標的端末が感染。

✓ 標的端末以外ではマルウェアを作動させないことで、事案の発覚を遅らせる狙いがあるとみられる。

✓ 攻撃者はMACアドレスにより、生産ロット等から標的とする特定の出荷先を絞り込んだものと推測される。

事案のイメージ



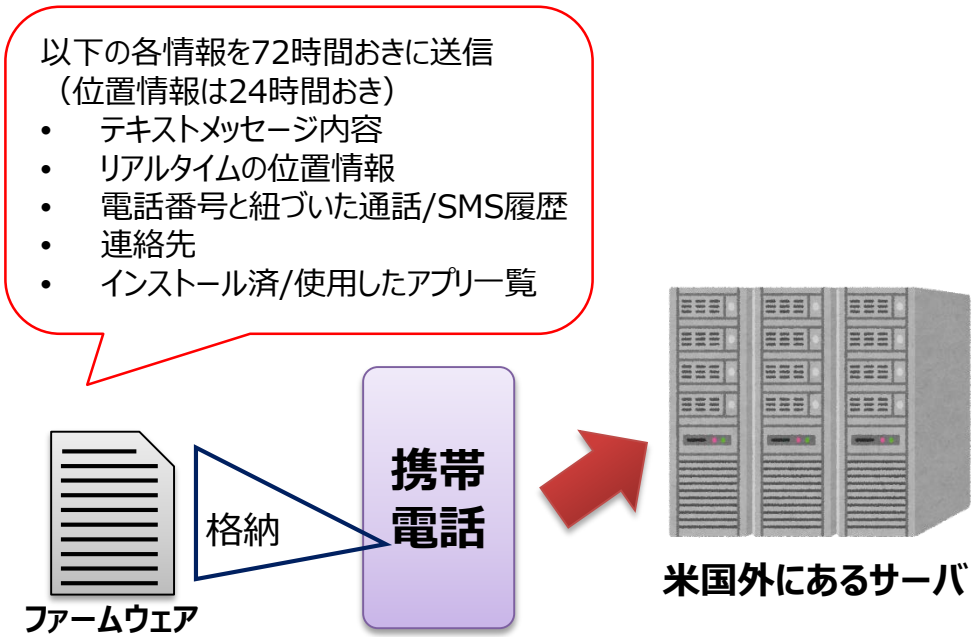
IoT機器のサプライチェーンリスク：信頼性の低い機器の販売による事業リスク

- 2016年11月、米国メーカーが販売していたスマートフォンのファームウェアが、消費者の同意を得ること無く、個人情報を海外サーバに送信していたことが判明。
- 米国連邦取引委員会（FTC）は、当該メーカーが開示する個人情報取扱方針に反する行為として提訴。当該メーカーが包括的なセキュリティプログラムを実装し、継続的な第三者評価を受けること等を条件に和解。

当該米国メーカーに対する命令

1. 個人情報のプライバシー、機密性、安全性、完全性の保護に関する誤認表示の禁止
2. 端末に関連するセキュリティリスクに対処し、個人情報を保護するための包括的なセキュリティプログラムの実装及び維持
3. 第三者による上記セキュリティプログラムの監査（2年毎に20年間）
4. 個人情報を収集し、他者に開示する際に、利用者に通知を行い、明確な同意を得る
5. コンプライアンス報告書の提出
6. 販売記録などの管理（20年間）

事案のイメージ



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（CPSF）と
   その実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

**3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に
   向けた諸外国の検討状況**

4. 本タスクフォースにおける検討事項

諸外国の検討状況（概要）

- 各国・地域において、様々な検討が行われている。

欧州サイバーセキュリティ認証フレームワーク

Cyber Security for Consumer Internet of Things

消費者向けIoT製品のセキュリティに関する行動規範

セキュアルータの技術ガイドライン

NIST
- Considerations for a Core IoT Cybersecurity Capabilities Baseline
- Security for IoT Sensor Networks
- NISTIR 8200, 8228 等

カリフォルニア州のIoTセキュリティ法

OECD 製品安全作業部会

IoT Security Policy Platform

NISTIR 8200 – Status of International Cybersecurity Standardization for the IoT

- IoTの概念を抽象化することで、IoTコンポーネント、システム、アプリケーションの共通理解を図る。
- **5つのアプリケーション（ユースケース）に対する、IoTサイバーセキュリティの目的、リスク、脅威の分析及び国際標準化状況を整理。**
- 2018年2月にドラフト版を公開後、2018年11月末に正式版が公表。

NISTIR 8200 における IoT の基礎概念

IoTは、以下の２つの基礎概念から構成：

① N対Nの関係を提供するネットワークによって、コンポーネント間が接続される

② 一部のコンポーネントは、フィジカル空間からデータを収集するセンサや、フィジカル空間に影響を及ぼすアクチュエータを備える。

IoTの5つのアプリケーション（ユースケース）

1. **コネクティッドカー（CV:Connected Vehicle）**：車両、道路、交通インフラが交通データを共有するサービス
2. **消費者向けIoT**：屋内のIoTアプリケーションと、ウェアラブル端末によるサービス
3. **ヘルスケア・メディカルデバイス**：電子化された診察記録や患者から取得されたヘルスケアデータを共有するサービス
4. **スマートビルディング**：エネルギー使用量監視システム、制御セキュリティシステム、照明制御システム等のサービス
5. **スマート製造**：データ、テクノロジー、高度な生産能力、クラウド、その他のサービスを統合するサービス

NISTIR 8228 – Consideration for Managing IoT Cybersecurity and Privacy Risks

- IoT機器の導入に伴い生じる、**サイバーセキュリティとプライバシーのリスクを軽減するための推奨事項**を整理。（2019年6月発行）
- IoT機器の機能の多様性を踏まえ、機器のセキュリティ、データのセキュリティ、個人のプライバシー情報という３つの観点からIoTデバイスにおいて生じうる懸念を列記し、NIST Cybersecurity Framework、SP 800-53 Rev.5（Draft）との対応関係を整理。

IT機器と比較して、IoT機器がサイバーセキュリティリスク、プライバシーリスクに影響を与えうる３つの懸念

物理世界とデバイスとの相互作用	IoT機器の多くは、従来のIT機器では通常行わない方法で物理世界とのやりとりを行う。
デバイスアクセス、管理、モニタリング機能	IoT機器の多くは、従来のIT機器と同じ方法でアクセス、管理、監視することができない。
サイバーセキュリティ機能、プライバシー機能の可用性、効率、有効性	IoT機器のためのサイバーセキュリティ機能、プライバイシー機能の可用性、効率、有効性は、従来のIT機器とは異なる。

IoT機器のサイバーセキュリティリスク、プライバシーリスクを軽減する対処領域

機器のセキュリティを守る	• アセットの管理、脆弱性管理、アクセス管理、機器のセキュリティインシデント検知
データのセキュリティを守る	• データ保護、データのセキュリティインシデント検知
個人のプライバシー情報を守る	• 情報フローの管理、特定個人情報の処理権限の管理、特定個人情報の提供に際する意思決定、データ管理との分離、プライバシー違反の検知

Considerations for a Core IoT Cybersecurity Capabilities Baseline

- NISTは、2019年2月にIoT機器のサイバーセキュリティ機能のコアとなる、12の任意（voluntary）のベースライン候補を公表。

12のベースライン候補

○ ほとんどのIoT機器に適用することが考えられるベースライン候補

1．論理的かつ物理的に識別できる。
2．ソフトウェア及びファームウェアは、安全で制御された、設定可能なメカニズムを用いてアップデートできる。
3．許可されたユーザーは、安全な「デフォルト」状態への復元を含めて、機器の設定を安全に変更できる。機器設定に対する許可されていない変更を防ぐことができる。
4．機器及び機器インターフェースへのローカル及びリモートのアクセスを制御できる。
5．保存及び送受信されたデータを保護するための暗号を使用できる。
6．機器通信のすべての層に、業界が承認した標準化されたプロトコルを使用できる。
7．サイバーセキュリティイベントの詳細をログに記録し、許可されたユーザー及びシステムがそれらにアクセスできる。
8．機器上の全ての保存データは、許可されたユーザーによってリセットでき、全ての内部データストレージから安全に削除される。

○全てのIoT機器に要求するには適さない可能性があるベースライン候補

9．ソフトウェア、ファームウェア、ハードウェア及びサービスの全ての取得元を確認するための情報が開示され、アクセスできる。
10．バージョンやパッチの状態を含む、現在の機器内部のソフトウェア及びファームウェアの一覧が開示され、アクセスできる。
11．機器の設計や設定を通じて、機能を最小限とする指針を実施できる。
12．物理的なアクセスを制御できるように設計される。

Security for IoT Sensor Networks

- NIST内のNCCoEは、**ビル管理システムのIoTセンサネットワーク**防御をユースケースとして、**センサネットワークに求められるセキュリティ要件、脅威等**を整理し、2019年2月にドラフト版を公表。
- センサネットワークを構成するコンポーネント毎に、セキュリティ要件、脅威、具体的なセキュリティ技術、NIST Cybersecurity Framework サブカテゴリとの対応関係を整理

【センサネットワークを構成するコンポーネント】

- **センサ（温度、湿度、動作センサ等）**
  - マイクロコントローラとセンサにより構成
  - 運用は無線だが、設定は有線の場合もある
- **ベースステーション／アグリゲータ**
  - 無線等を介してセンサから受信・集約したデータをコントローラへ送付
  - コントローラからの指示をセンサに送信
- **コントローラ**
  - センサのデータを処理し、センサに指示する
  - ソフトウェアの他に Rasberry Pi 等でも実装可能
- **通信路**
  - センサデータ、制御信号の伝送路

【コンポーネント毎の整理】

公開されるインターフェイス
想定される攻撃ベクトル
セキュリティ要件
具体的なセキュリティ技術
NIST Cybersecurity Framwork との対応関係

カリフォルニア州のIoTセキュリティ法

- インターネットに接続する機器に合理的なセキュリティ機能（例：機器固有のデフォルトパスワード設定、パスワードの初回起動時の変更 等）を備えることを製造者に求める法律にカリフォルニア州知事が署名（2020年1月1日施行予定）

接続される機器（コネクティッド・デバイス）のセキュリティ法

- インターネットに接続する機器の製造者は、当該機器に合理的なセキュリティ機能または以下のすべてを備えたものとする。
  1. デバイスの性質と機能に適し、
  2. 収集、保管、または送信できる情報に適し、
  3. 不正なアクセス、破壊、使用、変更、または開示から、機器および機器に含まれるすべての情報を保護する設計
- ローカルエリアの外で認証を実施する機器は、以下のいずれかを満たす場合に、合理的なセキュリティ機能を備えているとみなす。
  1. あらかじめプログラムされたパスワードは、製造された各機器に固有のものであること
  2. 当該機器は、初回アクセスが許可される前にユーザーが新しい認証手段を生成しなければならないセキュリティ機能を備えていること

欧州サイバーセキュリティ認証フレームワーク

- 「Cybersecurity Certification Framework」の創設を含む「Cybersecurity Act」は、2019年4月9日に欧州理事会で採択され、6月27日に発効。
- 「Cybersecurity Act」に基づき、ENISAが具体的な産業分野毎に「候補スキーム(Candidate Scheme)」を欧州委員会に提案し、順次、認証フレームワークが策定される予定。

欧州委員会、ENISAの動向

- 2017年9月、ユンカー欧州委員会委員長の施政方針演説で、EUにおけるサイバーセキュリティ政策（Cybersecurity Act）が発表され、新たなサイバーセキュリティ認証フレームワーク（Cybersecurity Certification Framework）の導入について言及。
- 2019年4月、Cybersecurity Act が欧州理事会で採択、6月27日に発効。

Cybersecurity Actの概要

- 欧州委員会は、欧州サイバーセキュリティ認証スキームの対象となるICT製品、サービス、プロセス、カテゴリのリストを含む「Union rolling work programme」を発行。最初の「Union rolling work programme」は2020年6月28日までに発行される（Article 47）。
- 本スキームでは、ICT製品等について、インシデントの可能性と影響の観点を考慮し、「basic」、「substantial」または「high」のいずれかの保証レベルを1つ以上特定する（Article 52）。
- ICT製品等の製造者または提供者は、保証レベル「basic」に対応する低リスクを示すICT製品等について、本スキームに示されている要件の充足が実証されていることを示すEU適合宣言をボランタリーに発行することができる（Article 53）。
- 本スキームには、評価に適用される国際規格、欧州規格、または国内規格への参照、および、第三国との認証制度の相互承認のための条件等が含まれる（Article 54）。
- 欧州委員会は、サイバーセキュリティ認証スキームが義務づけられることによって、ICT製品等の適切なレベルのサイバーセキュリティを確保し、国内市場の機能を改善することに効果があるか定期的にアセスメントを行う。最初のアセスメントは2023年末までに行われ、その後は少なくとも2年ごとに行われる（Article 56）

消費者向けIoT製品のセキュリティに関する行動規範（英国）

- 英国デジタル・文化・メディア・スポーツ省（DCMS）が、消費者向けIoT製品を利用するユーザのセキュリティに関する負担を軽減するために、IoT製品の開発、製造及び販売の段階で安全が確保されるよう、**製造メーカー等が実践すべき対策を13項目のガイドライン**にまとめ、2018年10月に公表。
- **一部の項目については義務化も視野に入れた、パブリックコメントを実施。**
- **ETSI（欧州電気通信標準化機構）を通じた国際標準の策定にも関与。**

ベストプラクティス一覧（13項目）

※ 下線付の項目は、義務化を視野にいれているもの

1. デフォルトパスワードを使用しない
2. 脆弱性の情報公開ポリシを策定する
3. ソフトウェアを定期的に更新する
4. 認証情報とセキュリティ上重要な情報を安全に保存する
5. 安全に通信する
6. 攻撃対象になる場所を最小限に抑える
7. ソフトウェアの整合性を確認する
8. 個人データの保護を徹底する
9. 機能停止時の復旧性を確保する
10. システムの遠隔データを監視する
11. 消費者が個人データを容易に削除できるように配慮する
12. デバイスの設置とメンテナンスを容易にできるように配慮する
13. 入力データを検証する

Cyber Security for Consumer Internet of Things (ETSI)

- 英国で策定された「消費者向けIoT製品のセキュリティに関する行動規範」に基づく欧州標準で、2019年2月に公表。**将来の欧州サイバーセキュリティ認証フレームワークの実装を助けるものであることを明示**。
- **消費者向けIoT製品のセキュリティを確保するための開発・製造者向けガイダンス**であり、セキュリティ課題の網羅的な対策ではなく、重要なセキュリティ課題を解消する技術上の対策、組織上の対策に焦点。
- 規定の13項目は英国の行動規範と実質的に同じだが、それぞれ細分化がなされており、必須要件（M）と推奨要件（R）、条件付き必須要件(MC)、条件付き推奨要件(RC)に整理。

消費者IoTのためのサイバーセキュリティ規定（13項目）

1. 単一のデフォルトパスワードを使用しない
2. 脆弱性の報告管理手段を実装する
3. ソフトウェアを定期的に更新する
4. 認証情報とセキュリティ上重要な情報を安全に保存する
5. 安全に通信する
6. 攻撃対象になる場所を最小限に抑える
7. ソフトウェアの整合性を確認する
8. 個人データの保護を徹底する
9. 機能停止時の復旧性を確保する
10. システムの遠隔データを調査する
11. 消費者が個人データを容易に削除できるように配慮する
12. デバイスの設置とメンテナンスを容易にできるように配慮する
13. 入力データを検証する

（参考）セキュアルータの技術ガイドライン（ドイツ）

- 2016年にドイツ国内で発生したマルウェア”Mirai”の事案を受けて、情報セキュリティ庁（BSI）及び経済エネルギー省（BMWi）が**エンドユーザー向けルータのセキュリティ要件を定めた技術ガイドライン**を策定し、2018年11月に公表。
- 必須の要件（MUST）と推奨の要件（SHOULD）に整理。
- 規制ではなく自己宣言するものとして活用。当該要求事項を欧州のサイバーセキュリティ認証フレームワークの議論に持ち込み、欧州レベルでのルール化を目指す可能性。

ガイドラインで求める必須要件の概要

- ルータが提供する全てのサービスについて、使用するポートを含めて開示する
- 使用しないサービスのポートを閉じる
- ゲストモードで接続する機器について、他の機器やルータ設定へのアクセスを禁止
- 工場出荷時のパスワードは、ルータのモデル名やMACアドレスに関する情報から構成してはならない
- 工場出荷時のパスワードは、複数の機器で使い回してはならない
- パスワードは8字以上、英数字・記号の組み合わせでなければならない
- ファームウェアの更新機能を備える
- ファームウェア更新前にパッケージを検証する
- 製造メーカは、重大な脆弱性に対するファームウェア更新の提供期間を情報開示し、サポート終了の際はその情報をルータ側でも確認できるようにする
- ファイアウォール機能を備える

マルチでの議論

- OECD や国際的な消費者団体においても、IoT機器のセキュリティ・セーフティは大きな関心事項となっている。
- Internet Society (ISOC)では、IoTセキュリティを議論する場として **IoT Security Policy Platform** を構築。

OECD製品安全作業部会

- IoT/AI時代の製品安全に関するOECD/EC合同の国際会議 ”Joint OECD-EC conference on IoT, AI and product safety” を開催（2018年11月）
- IoT製品の製品安全・セキュリティの両側面から各国制度の原則となることを目的としたレポート作成に向けて、各国制度調査を実施。

IoT Security Policy Platform（Internet Society）

- IoTセキュリティに関する世界的なベストプラクティスを収集、調整、及び推進して、エコシステムに対する主要な課題を検討。
- 製造業者、小売業者、政策立案者、規制当局、及び消費者の間で適切な選択を行おうとするセキュリティを促進するための世界的な取り組みの調和を目指す。

【メンバー】

AGESIC（ウルグアイ）、ARCEP（フランス）、DCMS（英国）、ISED（カナダ）、MCTPEN（セネガル）、NIST（米国）、オランダ経済・気候政策省（オランダ）、Mozilla Foundation、Internet Society　等

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（CPSF）と
   その実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に
   向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項

第2層において求められる信頼性

- CPSFでは、第2層（フィジカル空間とサイバー空間のつながり）で確保すべき信頼性を、**フィジカル・サイバー間を正確に“転写“する機能**と整理。
- 第2層で想定されるセキュリティインシデントは、安全面にも支障をきたす可能性がある。

＜現状＞CPSFにおける整理

- 第2層では、**セキュリティ上の脅威が安全上の問題につながる**可能性を認識した上で、安全上の問題につながり得る事象を引き起こし得る箇所・機器を明確にし、リスク分析・対応を進める重要性を説明。

第2層「フィジカル空間とサイバー空間のつながり」の考え方

特性	• IoT機器を介して、フィジカル空間とサイバー空間のつながりが拡大
機能（守るべきもの）	• 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、サイバー空間へ送る機能 • 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機能
リスク分析の対象となる構成要素の例	• 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 等 • これらの機器等を構成する、転写機能に関わる部品
想定されるセキュリティインシデント例	• 不正アクセスによる**IoT機器の意図しない動作（誤計測、制御・計測の停止）** • 正常動作・異常動作に関わらず、**安全に支障をきたす動作** • **IoT機器の改ざん**や**計測機能に対する物理的な妨害**による**正確でないデータの送信**等

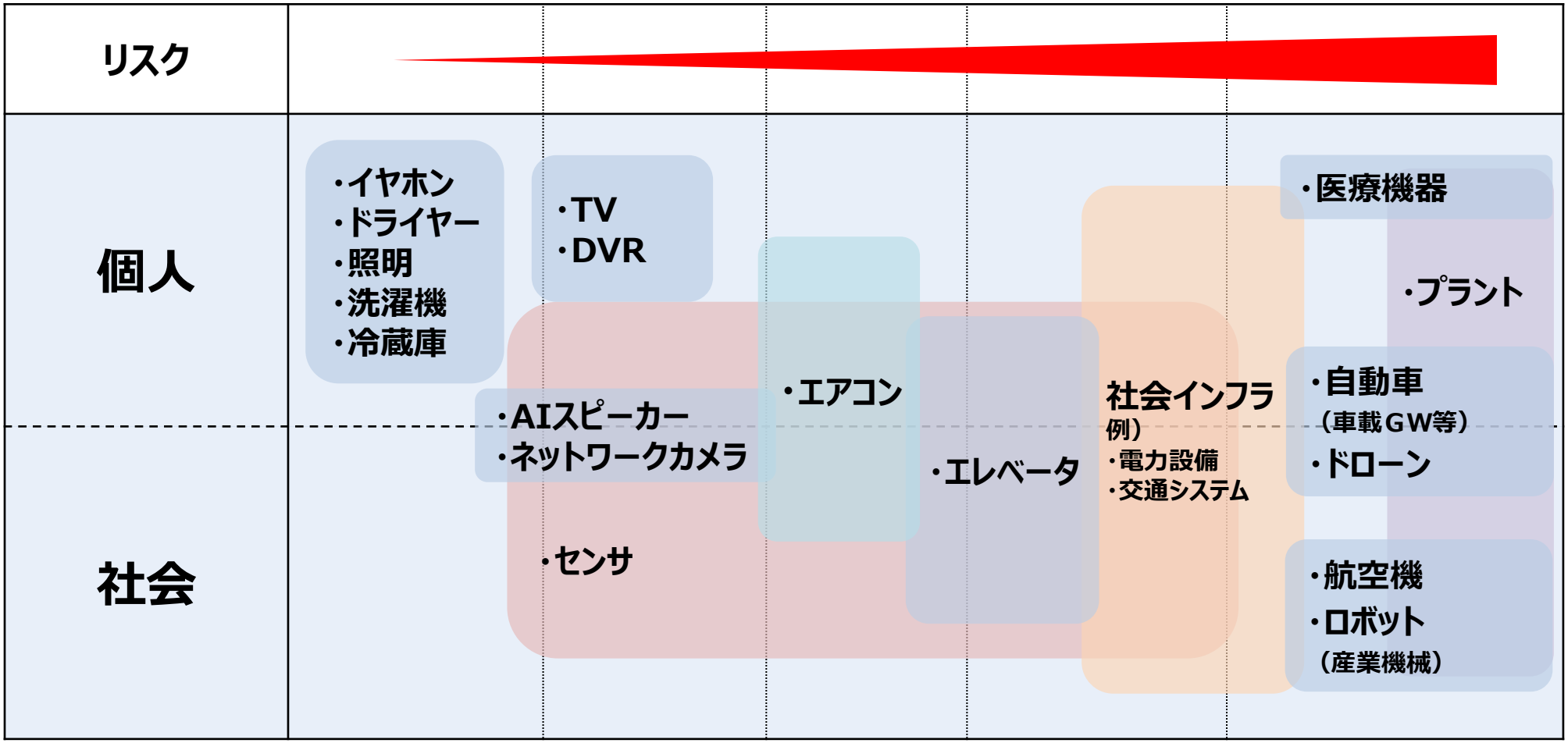
＜現状＞CPSFにおける整理

- CPSFでは、サイバーとフィジカルの間の転写機能を持つ機器のセキュリティ対策要件・対策例として、**機能安全とサイバーセキュリティを組み合わせて対応すること**などを記載。
- このような対策要件・対策例を社会実装していくためには、**転写機能を持つ機器が正規品であるかを確認するための具体的な仕組み**や、**安全等も考慮に入れたセキュリティ対策の具体化**が必要。

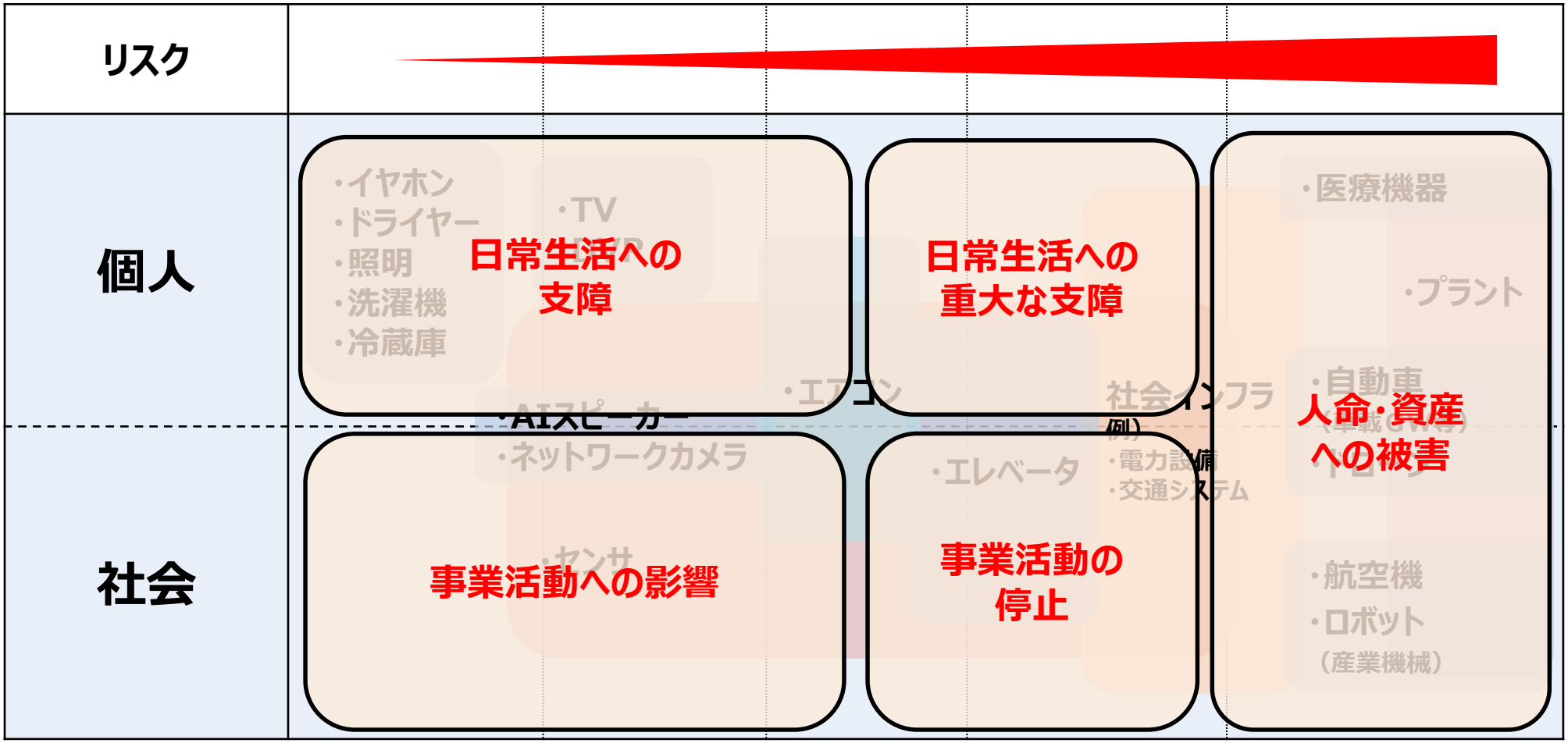
CPSF 添付C 「対策要件に応じたセキュリティ対策例集」から

対策要件ID	対策要件	対策例（抜粋）
CPS.SC-4	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	<Basic> • 組織は、調達時に、**自組織が所有するIoT機器が正規品であるかをラベルを確認**する等して確かめる。 • 組織は、IoT機器やソフトウェアに含まれるIDや秘密鍵、電子証明書等を用いて調達した機器が正規品であることを確認する。
CPS.PT-3	ネットワークにつながることを踏まえた**安全性を実装するIoT機器を導入**する。	<Advanced> • 本質安全設計を通じてハザードの縮減を図る。・・・影響度の高いハザードが残存した場合、例えば、下記のような代替的対策を講ずることが望ましい。 – 安全装置等の付加価値による安全確保 – ハザードを有する機器に要因が近づかないような空間設計

サイバー・フィジカル間をつなげる機器に潜むリスクのイメージ



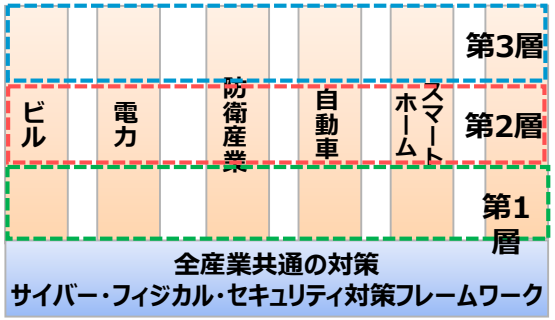
サイバー・フィジカル間をつなげる機器に潜むリスクのイメージ



『第2層』タスクフォースの検討の方向

- 本タスクフォースでは、諸外国の動向も踏まえながら、サイバー・フィジカル間の**転写機能を持つ機器について、ユーザのリスクや社会に与える被害を考慮した信頼性確保に求められる要件**を整理。
- その整理を踏まえた上で、分野別SWGの検討内容に横串を通すべく、**業界の自主活動を含めた自己適合宣言・認証等の確認の在り方等**を検討するとともに、**産業保安・製品安全も考慮したセキュリティ対策の在り方**について検討を行う。

分野別ガイドラインにおいて機能の要求を明確化（各SWG）

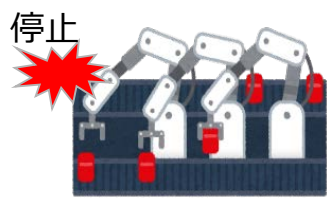


タスクフォースにおける検討内容イメージ

① 業界の自主活動を含めた自己適合宣言・認証等の確認の在り方等の検討

※ 特に高いセキュリティを求める機器に対する要件等を検討

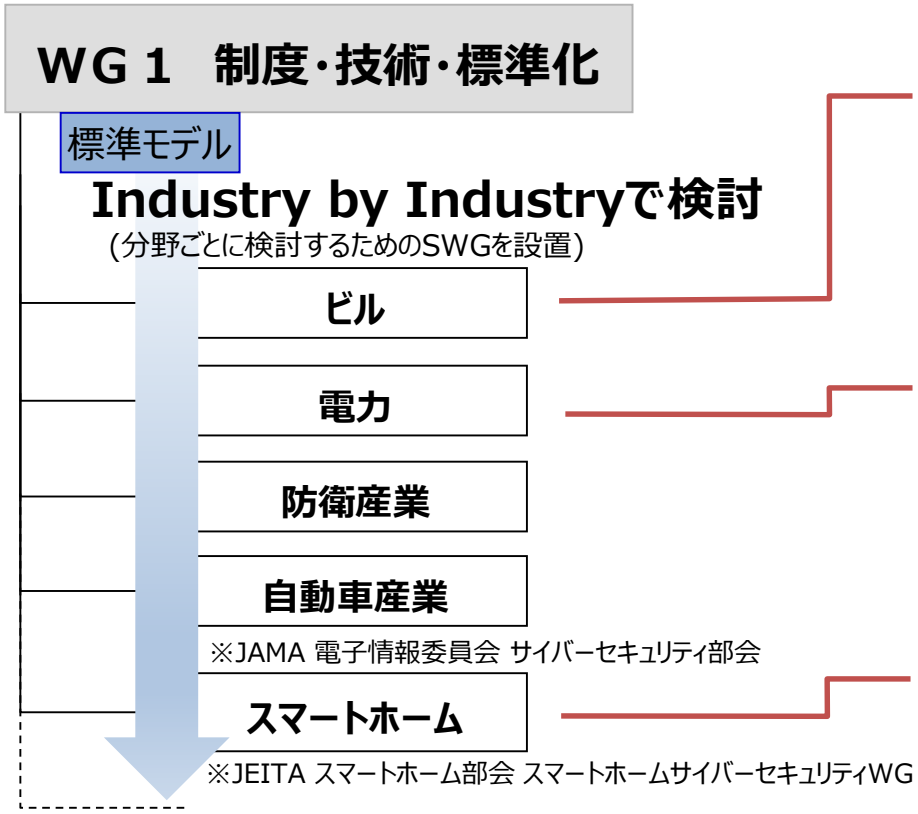
② サイバーリスクの安全への影響の増大への対応



※ 安全も考慮に入れたセキュリティ対策等について検討

（参考）産業分野別SWGの検討状況

- **各SWG（ビル、電力、スマートホーム等）**では、CPSFを参照して、各産業分野の実際の産業活動に応じたセキュリティ対策について整理し、ガイドライン等の策定を進めている。その中で、一部SWGでは認証等の必要性についても議論。
- 各SWGの検討状況も踏まえ、**産業共通で考慮すべき事項をTFの議論に反映。**



【ビルSWG】
- ビルの管理・制御システムに係る各種サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理し、ビルに関わるステークホルダーが活用できる**「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を本年6月17日に策定。**

【電力SWG】
- 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、官民が取り組むべき課題と方向性について広く検討。**結果を電力制御系ガイドラインに反映するなど対応していく方針。**一部機器に対する国際的議論にも対応（**CPIC※への参加等**）。

※CPIC: Cyber Product International Certification

【スマートホームSWG】
- 各家庭におけるネットワーク構成とスマート家電等の基本形を整理し、各家庭におけるセキュリティリスクポイントを洗い出し。
- **今後、「スマートホームサイバーフィジカルセキュリティ対策ガイドライン」を策定予定。**