経済産業省

# 産業分野におけるサイバーセキュリティ政策

## ～「Society5.0」において必要なセキュリティ対策～

経済産業省　商務情報政策局

サイバーセキュリティ課長

奥家 敏和

## １．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

## ２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

## ３．「Society5.0」において必要なセキュリティ対策
～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
～海外のサプライチェーンの強化

# ASUS社端末におけるアップデート機能を悪用した攻撃
## （サプライチェーンを通じた攻撃（水平的脅威））

- 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：MOTHERBOAR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。

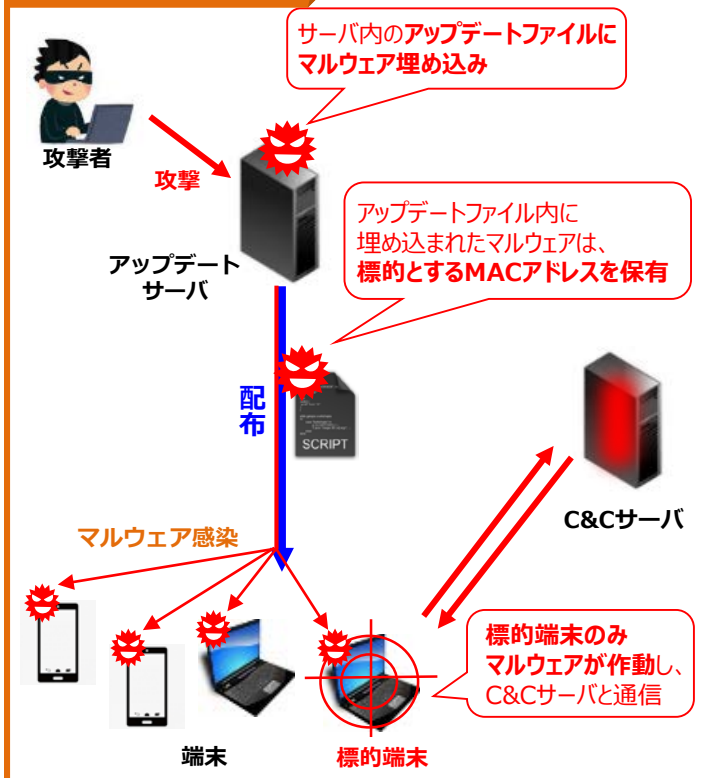
### 本事案の詳細（原因・影響）

- 本攻撃は**2018年6月から11月**にかけて発生。「ShadowHammer」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**数十万のASUS端末**に感染。　※Kaspersky社は数百万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



# 身近なサイバー攻撃の脅威：クラウドサービスにおけるサイバー攻撃の発生（サプライチェーンを通じた攻撃（水平的脅威））

- 世界のクラウドサービス市場規模は931億ドル※1。クラウドサービスを利用している国内企業の割合も56.9%と、前年の46.9%から大幅に上昇※2。
- その一方で、**クラウドサービスへのサイバー攻撃**（主に不正アクセスによる情報漏えい）**事案は絶えず発生**している状況。

※1　2015年。出典：Cisco VNI: Forecast and Methodology, 2014-2019.
※2　2017年。出典：平成30年度版　情報通信白書

## 利用者の多いクラウドサービスにおけるサイバー攻撃の特徴

**「Office365」への不正アクセス**

- 攻撃者は、**2要素認証が導入されていなかったり**、**単純なパスワードが設定**されているようなアカウントを標的としている。
- 特に**システムアカウント**については、事業者内で共有する必要があることから**単純なパスワードが設定されがち**であり、**使用頻度の低いものが放置されていることも多い**ため攻撃に気づきにくいという傾向がある。

**Amazon Web Service（AWS）のクラウドストレージ「Amazon S3」への不正アクセス**

- **ディレクトリの設定を「公開状態」**にしていたり、**パスワードが設定されていない**といった、**利用者側のAWS設定ミスが**多くの原因。

→ **基本的なセキュリティ設定の確認が重要**

## クラウドサービスにおける主なサイバー攻撃事例

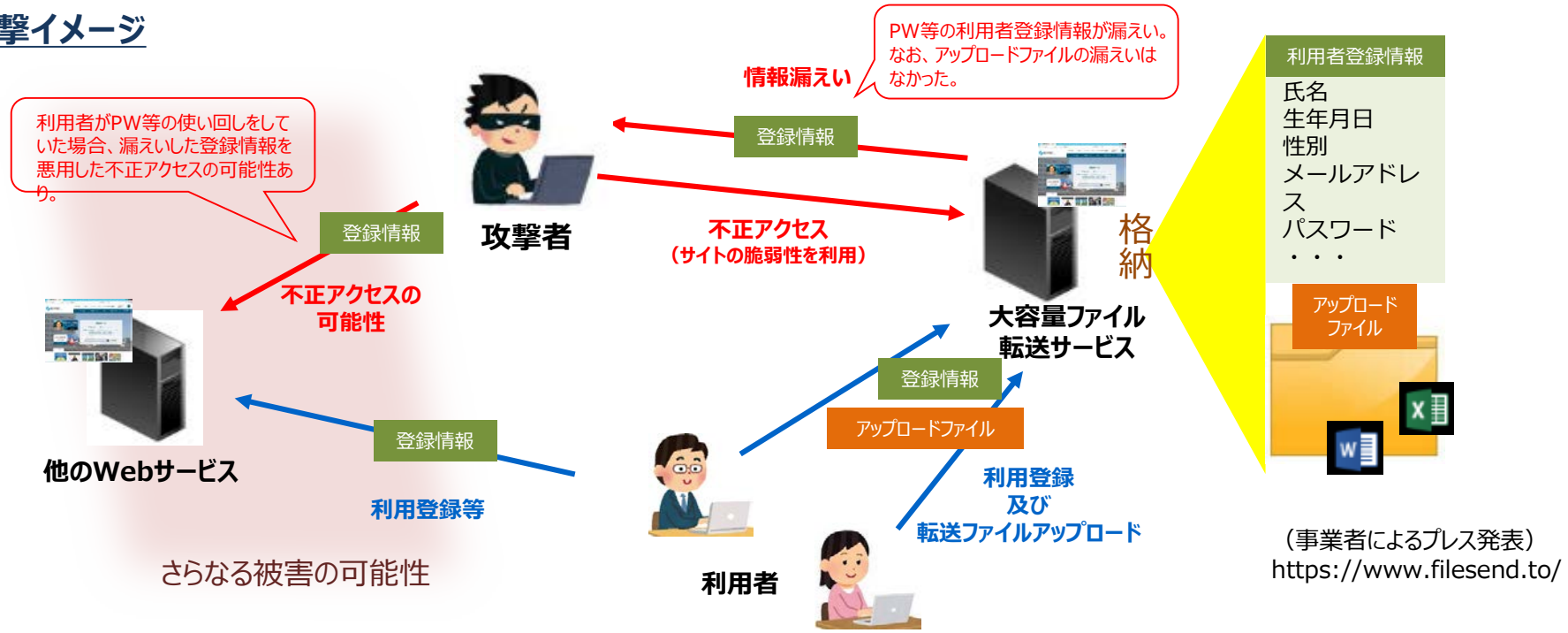
- 米国配車サービス大手のウーバー・テクノロジーズにおいて、2017年11月、顧客とドライバー合わせて**5,700万人の個人情報が流出**したことが判明。**原因はAWSへの不正アクセス**。
- A社のインド子会社において、2018年5月、**5万人以上の顧客情報が流出**したことを発表。**原因はAWSの公開設定ミス**。

# 大容量ファイル転送サービスにおける不正アクセス（情報漏えい）事案

- 2019年1月22日、大手クラウドサービス事業者による大容量ファイル転送サービスにおいて、一部サーバに対する**不正アクセス**が発生。**481万5,399件の顧客情報※の漏えい**を確認。
- 翌1月23日より、被害状況調査及びさらなる被害防止のため、サービスを停止。**本サービスは当面休止**することとしている。

※　漏えいした顧客情報は、「ログイン用メールアドレス」、「ログインパスワード」、「生年月日」、「性別」、「職業・業種・職種」、「居住地の都道府県名」、「メールアドレス」等、本サービスを利用するにあたっての利用者登録情報。
なお、本サービスで送受信されたファイルについては、漏洩がなかったことを確認。

## 攻撃イメージ




（事業者によるプレス発表）
https://www.filesend.to/

# サイバー攻撃の脅威レベルの増大（制御系にまで影響が波及）
# （情報システムを越えて制御システムに達する攻撃（垂直的脅威））

- 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

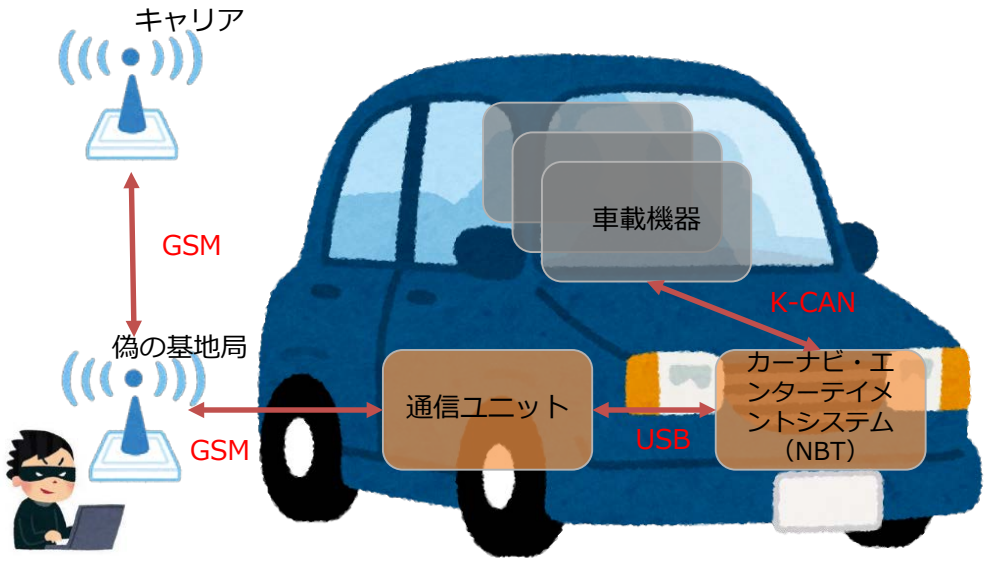
# 自動車の脆弱性に関するBlack Hat USA 2019での報告

- 2018年2月、中国Tencent社のKeen Security labは、大手自動車メーカーの自動車の脆弱性を検証してメーカーに通知。これを受け、メーカーは緩和策を実施。また、Keen labは、責任ある開示（Responsible Disclosure)方針に従い、2019年8月のBlack Hatにおいて、分析結果、検証内容及び対応策の詳細をメーカーと**共同発表**した。
- 報告では、カーナビやエンターテイメントシステムを提供する車載機器の脆弱性を用いて、偽の携帯電話ネットワークからSMSを送付する等の操作により、ドアの開錠や任意コード実行等の操作が行えたとしている。

**＜開示プロセス＞**

| | |
|---|---|
| 2017年2月～2018年2月 | Keen labが自動車の脆弱性及び攻撃チェーンを検証し、メーカーに通知 |
| 2018年3月 | メーカーは通知された脆弱性を確認し、緩和策を計画 |
| 2018年4月 | 脆弱性に関するCVE番号が予約 |
| 2018年5月 | Keen labが概要レポートを一般公開 |
| 2018年夏 | メーカーが必要な対策と緩和策を実施 |
| 2019年8月 | Black Hatにおいて共同発表、詳細レポートを公開 |

**＜偽GSM基地局を用いた遠隔攻撃イメージ＞**




https://www.blackhat.com/us-19/briefings/schedule/#-days--mitigations-roadways-to-exploit-and-secure-connected-bmw-cars-15313

１．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．「Society5.0」において必要なセキュリティ対策
～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
～海外のサプライチェーンの強化

# サイバーセキュリティ政策の方向性

**1．産業政策と連動した政策展開**

**① 重要インフラの対策強化**
－情報共有体制強化　等

**② IoTの進展を踏まえたサプライチェーン毎の対策強化(Industry by industry)**
－防衛関係、自動車、電力、スマートホーム等の分野別検討と技術開発・実証の推進

**③ 中小企業のサイバーセキュリティ対策強化**

**2．国際ハーモナイゼーション**

**① 日米欧間での相互承認の仕組みの構築**

**② 民間主体の産業活動をゆがめる独自ルールの広がり阻止**

**3．サイバーセキュリティビジネスの創出支援**

**① 産業サイバーセキュリティシステムを海外に展開**

**② サービス認定創設、政府調達などの活用**

**4．基盤の整備**

**① 経営者の意識喚起**

**② 多様なサイバーセキュリティ人材の育成（ICSCoE等）**

**③ サイバーセキュリティへの過少投資解決策の検討**

# 産業サイバーセキュリティ研究会とWGの設置による検討体制

## 産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
アクションプランを加速化する３つの指針を提示

**構成員**

※2019年4月開催時点

- **石原　邦夫**　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、東京海上日動火災保険株式会社相談役
- **泉澤　清次**　三菱重工業株式会社取締役社長
- **遠藤　信博**　日本経済団体連合会情報通信委員長、日本電気株式会社会長、サイバーセキュリティ戦略本部員
- **小林　喜光**　経済同友会代表幹事、株式会社三菱ケミカルホールディングス取締役会長
- **篠原　弘道**　日本電信電話株式会社取締役会長
- **中西　宏明**　株式会社日立製作所会長
- **船橋　洋一**　アジア・パシフィック・イニシアティブ理事長
- **村井　純(座長)**慶應義塾大学教授、サイバーセキュリティ戦略本部員
- **渡辺　佳英**　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

**オブザーバー**

NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

## WG１（制度･技術･標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日

１．サプライチェーン強化パッケージ

## WG２（経営･人材･国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日
第５回　令和　2年1月15日

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

## WG３（サイバーセキュリティビジネス化）

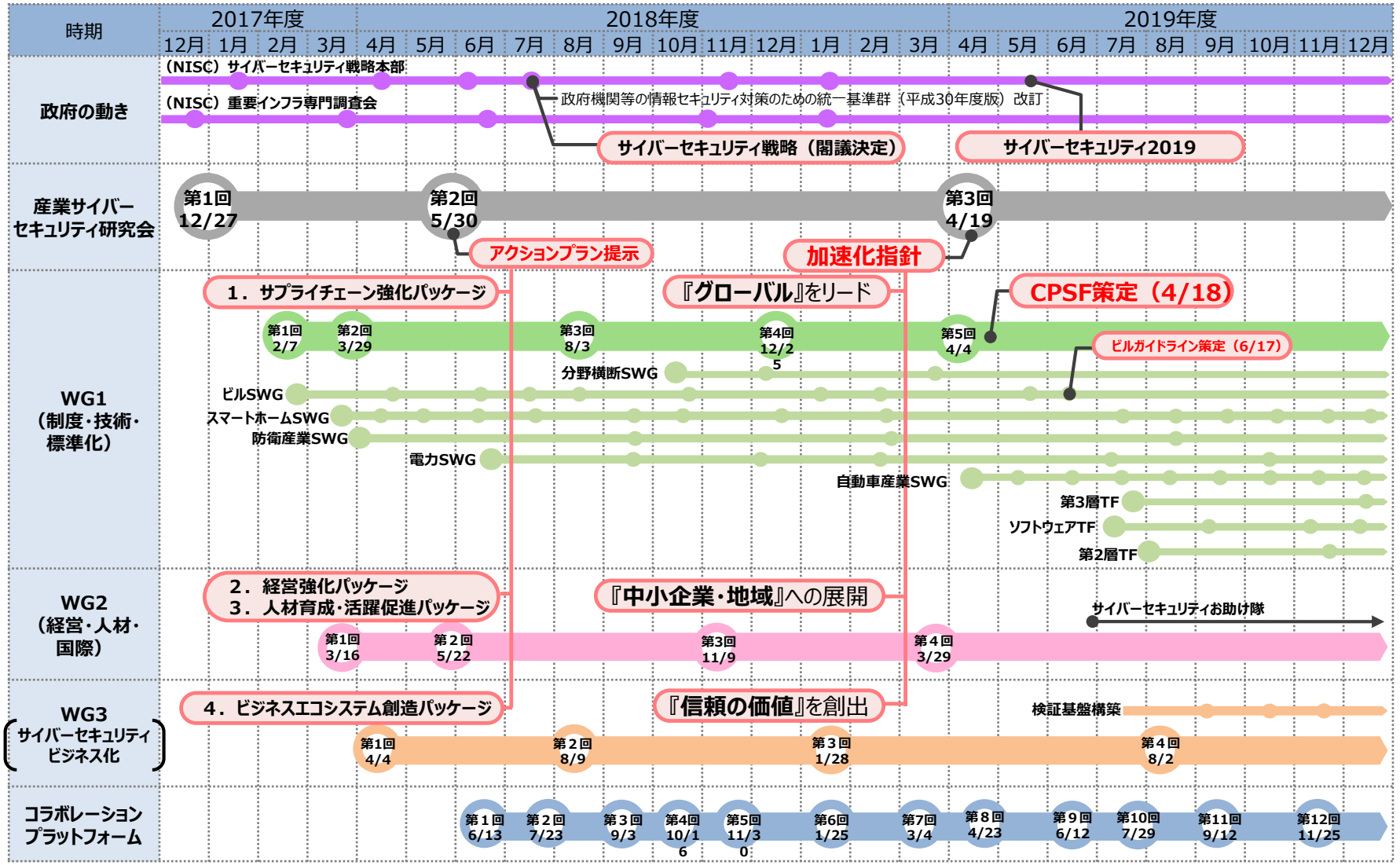
第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日

４．ビジネスエコシステム創造パッケージ

## 産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

# 産業サイバーセキュリティ研究会関連の動き



１．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

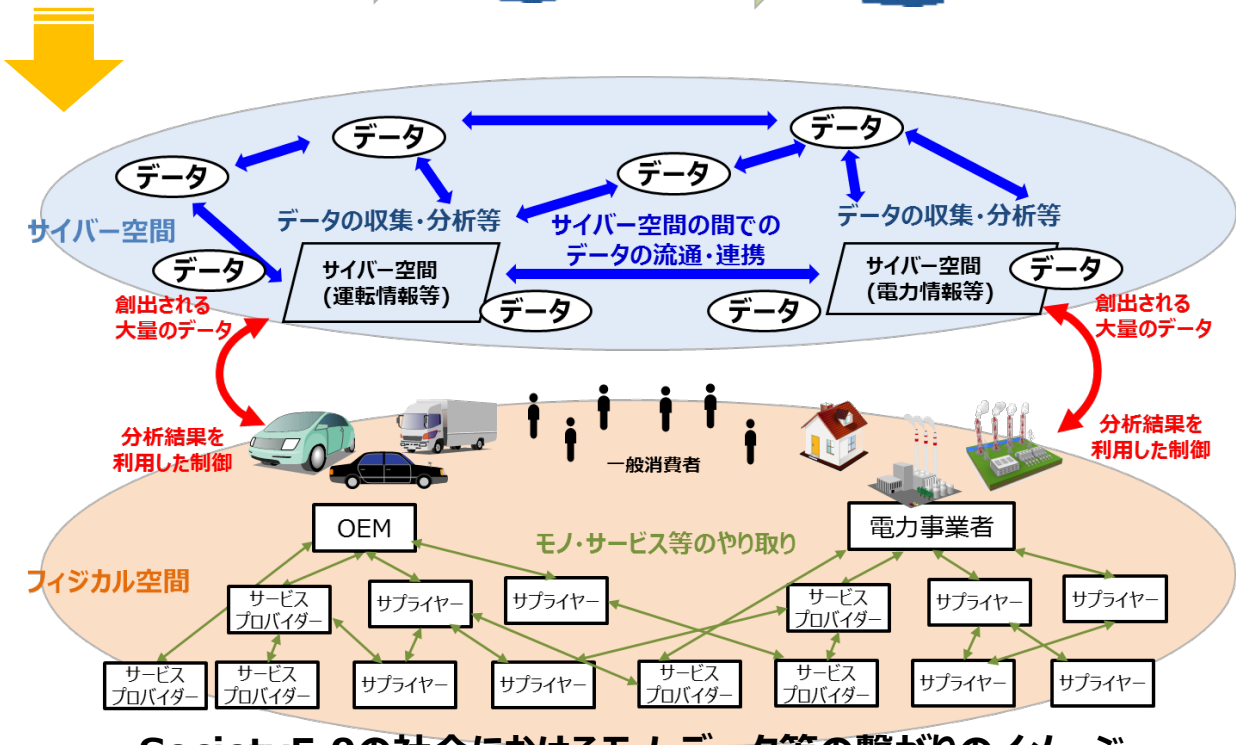
３．「Society5.0」において必要なセキュリティ対策
～サイバー・フィジカル・セキュリティ対策フレームワークの策定
～海外のサプライチェーンの強化

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

- 「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となる。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**となる。

**「Society5.0」以前**

**個々の企業主体の定型的なつながりで価値を生み出す**




**Society5.0の社会におけるモノ・データ等の繋がりのイメージ**

**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。

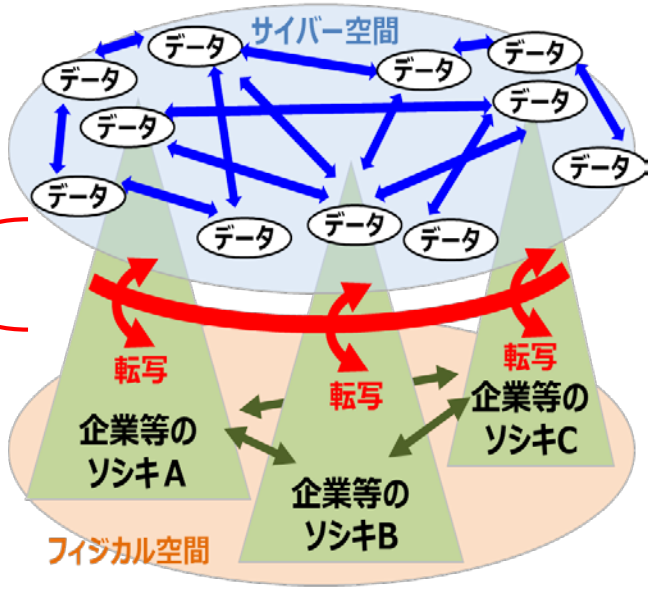
## 三層構造

「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



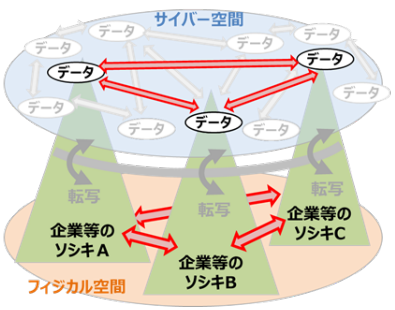
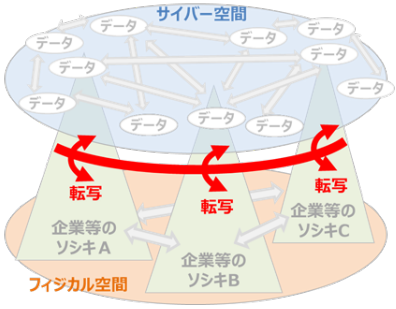
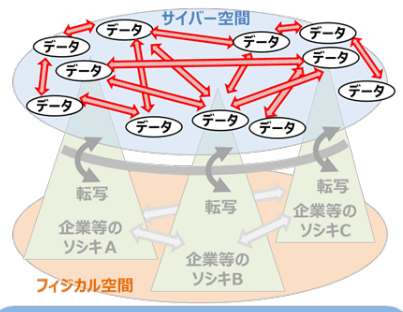

## ６つの構成要素

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<br>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<br>• 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<br>• データの保管<br>• 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<br>• 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<br>• 安全に支障をきたす動作 | • 保護すべきデータの漏えい<br>• 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<br>• 他組織との連携状況の未把握 | • 不正なIoT機器との接続<br>• 許容範囲外の入力データ | • 通信経路が保護されていない<br>• 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<br>■ 関係者との役割分担 | ■ 接続相手の認証<br>■ 安全なIoT機器の導入 | ■ 暗号化によるデータ保護<br>■ データの提供者の信頼性確認 |

# 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パブリックコメント

- ２度のパブリックコメントについて、いずれも**英語版のフレームワーク原案も同時公開**して実施し、積極的に意見を取り込んで**国際ハーモナイゼーションを推進**。

**第１回 パブリックコメント**

- **2018年4月27日～5月28日**
- **国内24, 海外9（米国7, 欧州2）の組織・個人より約300件の意見提出**

**【代表的な意見】**

- Society5.0 における信頼の確保へ向けた取組として趣旨に賛同
- 三層構造の説明や、６つの構成要素で整理した理由を明確に説明して欲しい
- セキュリティ対策の実施主体の明確化を希望
- 中小企業にとって利用しやすいフレームワークとなることを期待
- 国際標準や海外規格に留意して進めて欲しい

**第２回 パブリックコメント**

- **2019年1月9日～2月28日**
- **国内27, 海外13（米国7, 欧州6）の組織・個人より約500件の意見提出**

**【代表的な意見】**

- 三層構造は、産業システムにおける関係者・関係性を理解するための有用な考え方を提供している
- フレームワークで採用しているリスクベースのアプローチ、マルチステークホルダーを考慮したアプローチに賛同
- 本フレームワークを企業の活動に実装するために、各産業分野への落とし込みが重要。
- 海外主要規格 との対応関係が明確になり有用性が向上した。

# CPSFにおける他の国際規格等との対応関係

- 第Ⅲ部、添付C及び添付Dにおいて、主要な国際規格等との対応関係を記載。
- NIST Cybersecurity Framework、NIST SP800-171、ISO/IEC 27001付属書Aについては、**各規格等から見た場合の対応関係も整理。**

**<添付C> CPSF ⇒ 他の国際規格等**

| 対策要件ID | 対策要件 | 対応する脆弱性ID | 対策例 | 対策例を実行する主体 | NIST SP800-171 | NIST SP800-53 | ISO/IEC 27001 付属書A | IEC 62443 |
|---|---|---|---|---|---|---|---|---|
| CPS.AM-1 | ・・・ | L1_1_a_COM,<br>L1_1_b_COM, | <High-Advanced><br>・・・ | O/S | ○ | ○ | ○ | ― |
| | | | <Advanced><br>・・・ | O/S | ○ | ○ | ○ | ○ |

**<添付D> 他の国際規格等 ⇒ CPSF**

| NIST Cyberseucurity Framework Ver1.1 | | | サイバー・フィジカル・セキュリティ対策フレームワーク | |
|---|---|---|---|---|
| 機能 | サブカテゴリID | サブカテゴリ | 対策要件ID | 対策要件 |
| 特定(ID) | AM-1 | ・・・ | CPS.AM-1 | ・・・ |

| NIST SP 800-171 | | | NIST SP800-171 から参照される NIST SP800-53 | サイバー・フィジカル・セキュリティ対策フレームワーク | | |
|---|---|---|---|---|---|---|
| ファミリ | 管理策ID | 要求事項 | 管理策名称 | 対策要件ID | 対策要件 | 対策例 |
| アクセス制御 | 3.1.1 | ・・・ | ・AC-2 アカウント管理<br>・・・ | CPS.AC-9 | ・・・ | ・・・ |

| ISO/IEC 27001:2013 附属書A | | サイバー・フィジカル・セキュリティ対策フレームワーク | | |
|---|---|---|---|---|
| 管理策ID | 要求事項 | 対策要件ID | 対策要件 | 対策例 |
| A.5.1.1 | ・・・ | CPS.BE-2 | ・・・ | ・・・ |

# マルチ・バイを通じた国際協調への取組

- 「サイバー・フィジカル・セキュリティ対策フレームワーク」を軸に、**各国のステークホルダーと議論、マルチの会議で紹介**し、共通の認識を醸成。

## 【US】

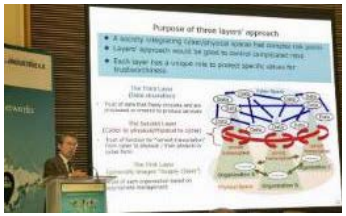
- TecGlobal （米国商工会議所主催）（2018年４月@ワシントンDC）
- Industrial Control Systems Joint Working Group (ICSJWG)（2018年４月@アルバカーキ）
- 2nd Global Cyber Dialogue（米国商工会議所主催）（2018年10月@ワシントンDC）
- CES 2019（2019年1月@ラスベガス）

## 【APEC/ASEAN】

- 第2回日・ASEANサイバーセキュリティWG（2018年５月@インドネシア・バリ）
- APEC TEL58（第58回電気通信・情報作業部会）（2018年10月@台湾・台北）

## 【EU】

- Securing Global Industrial Value Networks（2018年5月@ベルリン）
- VDE Tec Summit 2018（2018年11月@ベルリン）
- 第8回日EU・ICT戦略WS（2018年12月@ウィーン）
- Consumers International Summit（2019年5月@エストリル）

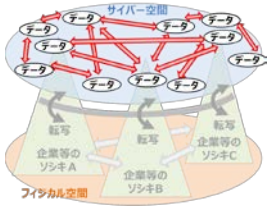


## 【OECD】

- OECD／CDEP（デジタル経済政策委員会）会合（2018年5月@パリ）
- 第1回 繁栄のためのデジタルセキュリティに関するOECDグローバルフォーラム（2018年12月@パリ）

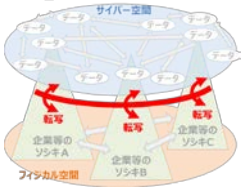
# CPSFに基づく具体化・実装の推進の全体像

【第3層】




サイバー空間におけるつながり

【第2層】




フィジカル空間とサイバー空間のつながり

**実際の産業活動の内容**

**具体的な対策手法やルールの明確化**

**データを介した連携を行う産業活動**
（分野間の連携 等）

**データの信頼性**
（データの完全性、真正性等の確認　等）

**分野別の産業活動**
- ビル
- 電力
- 防衛
- 自動車
- スマートホーム 等

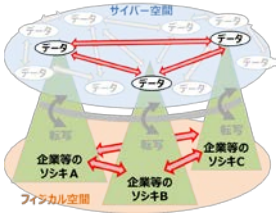
**規模別の産業活動**
- 大企業
- 中小企業 等

**転写機能を持つ機器の信頼性の確認手法**
- 機器・システムのセキュリティ 等

**ソフトウェアの取扱に関するルール・管理手法**
- Software component transparency 等

【第1層】

企業間のつながり




**産業サイバーセキュリティ研究会WG 1**

標準モデル（CPSF）

- ビルSWG
- 電力SWG
- 防衛産業SWG
- 自動車産業SWG
- スマートホームSWG
- ・・・

**分野横断SWG**

**『第3層』TF (⇒ データ区分に応じて適切なセキュリティ対策要件 等)**

**ソフトウェア TF　(⇒　OSSを含むソフトウェア管理手法 等)**

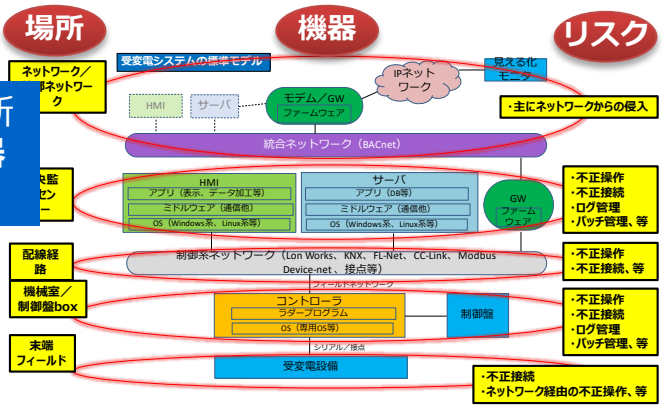
**『第2層』TF (⇒　機器毎のラベリング・認証の在り方、安全との一体化への対応 等)**

# （参考）ビルSWG（座長：江崎 浩 東京大学 教授）

- 産業サイバーセキュリティ研究会WG1（制度・技術・標準化）の下の**ビルSWG（ビルオーナー～ベンダまで、ビル関連のステークホルダが参加）**において、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**ガイドラインを作成。2019年6月17日付で第1版を公開。**

- **場所→場所に置かれる機器→機器に想定されるリスク→対策要件→ライフサイクル別の対応策という流れで整理**

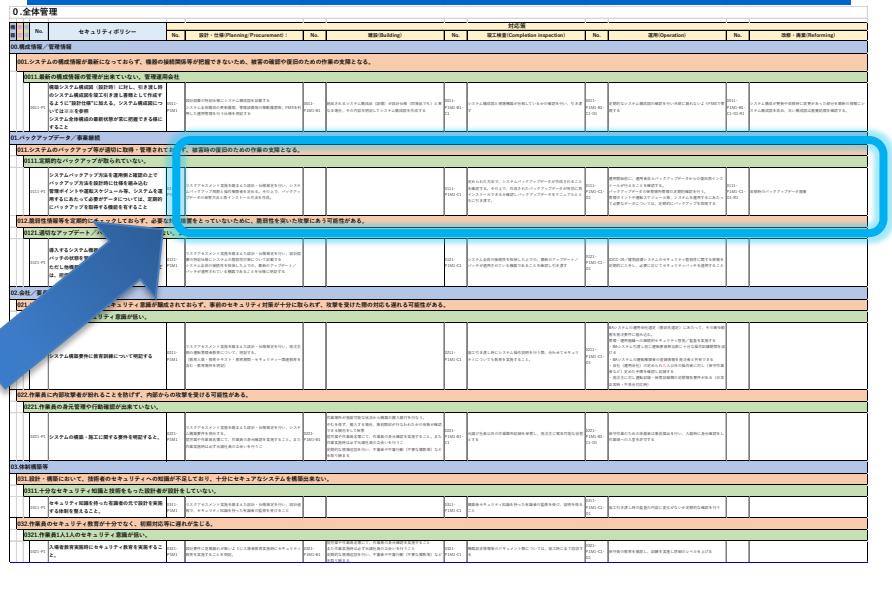
**場所**及びその場所に設置される**機器等**をリストアップ




| | | |
|---|---|---|
| 4.1 | 全体管理 | |
| 2. | バックアップデータ／事業継続 | |
| 3. | 会社／要員の管理 | |
| 4. | 体制構築等 | |
| 4.2 | 詳細 | |
| 1. | ネットワーク(クラウド、情報系NW、BACnet) | |
| | 10 | ネットワーク |
| | 11 | クラウドサーバ・Webサーバ |
| | 12 | 情報系端末 |
| | 13 | 外部接続用ネットワーク機器（FW、ルータ） |
| | 14 | ビルシステム間相互接続 |
| 2. | 防災センター（中央監視室） | |
| | 20 | 防災センター（中央監視室） |
| | 21 | HMI/HIM |
| | 22 | 保守用持ち込み端末 |
| | 23 | 統合NWにつながるネットワーク機器（FW、ルータ、SW） |
| | 24 | システム管理用サーバ（ビルシステム主装置） |
| 3. | 機械室／制御盤ボックス | |
| | 30 | 機械室 |
| | 31 | コントローラ（DDC、PLC等） |
| | 32 | ネットワーク機器（FW、ルータ、SW） |
| | 33 | ゲートウェイ機器 |
| | 34 | 各種制御盤・分電盤 |
| 4. | 配線経路（MDF室、EPS、天井裏ラック） | |
| | 40 | MDF室／EPS／天井裏ラック |
| | 41 | 内部に置かれたネットワーク機器（SW類） |
| 5. | 末端装置が置かれる場所 | |
| | 50 | 末端装置 |

| | セキュリティインシデント | リスク源 | セキュリティポリシー |
|---|---|---|---|
| 1. | 構成情報／管理情報 | | |
| (1) | ビルシステムへの被害発生時に、被害確認が遅れ、復旧作業の支障となる。 | ビルの構成情報が最新状態に管理できておらず、機器の最新の接続関係が把握できない。 | ・構築システム構成図（設計時）に対し、引き渡し時のシステム構成図を竣工引き渡し書類として作成するように"設計仕様"に加える。<br>・システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。 |
| 2. | バックアップデータ／事業継続 | | |
| (1) | 適切なバックアップデータがなく、ビルシステムへの被害発生時に復旧作業の支障となる。 | バックアップが取れていないまたはバックアップの範囲や対象が適切でない。 | ・システムバックアップ方法を運用側と確認の上でバックアップ方法を設計時に仕様を組み込む。<br>・管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する機能を具備する。 |
| (2) | システムの脆弱性をついた攻撃を受ける。 | 脆弱性についての認識が不十分で脆弱性が残ったままの状態になっている。 | ・既知の脆弱性に対して必要な対策（パッ[illegible]現する。<br>・ただし、他機器および他システムの正常稼動については、担保しなければならない。 |
| 3. | 会社／要員の管理 | | |
| (1) | ビルシステムへの被害発生時に、迅速な対応ができず、被害が拡大する。 | ビル管理会社においてセキュリティへの意識醸成、要員教育が十分ではなく、事前対策や対応準備が出来ていない。 | ・システム構築要件に教育訓練について明記する。 |
| (2) | ビルシステムが内部作業員等から攻撃を受ける。 | 作業員等の身元確認や行動監視が不十分で、内部攻撃者が紛れることや攻撃を行うことを防ぐことが出来ていない。 | ・システムの構築・施工・保守にあたって、作業員等の身元確認や行動確認についての要件を明記する。 |
| 4. | 体制構築等 | | |
| (1) | 攻撃等への対応が効果的に出来ず、被害が拡大する。 | 十分なリスクアセスメントが出来ていないため、リスク対応の運用計画や体制が十分なレベルで構築できていない。 | ・リスクアセスメントを実施し、その結果を基に監理監査 面からの「運用する管理体系」などを運用計画として 定義・整備する。 |

ビルシステムの**ライフサイクルの各フェーズ毎に対策**を展開



**場所・機器別**の想定される**インシデント**と**リスク源**を整理し、その**対策をポリシーレベル**で整理

# 『第3層TF』の検討の方向性

- 本タスクフォースにおいて、データの信頼性確保のために、「**データの区分に応じた適切なセキュリティ対策要件**」及び「**データの信頼性の確認手法**」を検討。

データの区分に応じた適切なセキュリティ対策要件の検討

**データをセキュアに管理すること**
**⇒マネジメント、プロセス、セキュリティポリシー、システム要件等のセキュリティ要件の明確化など**

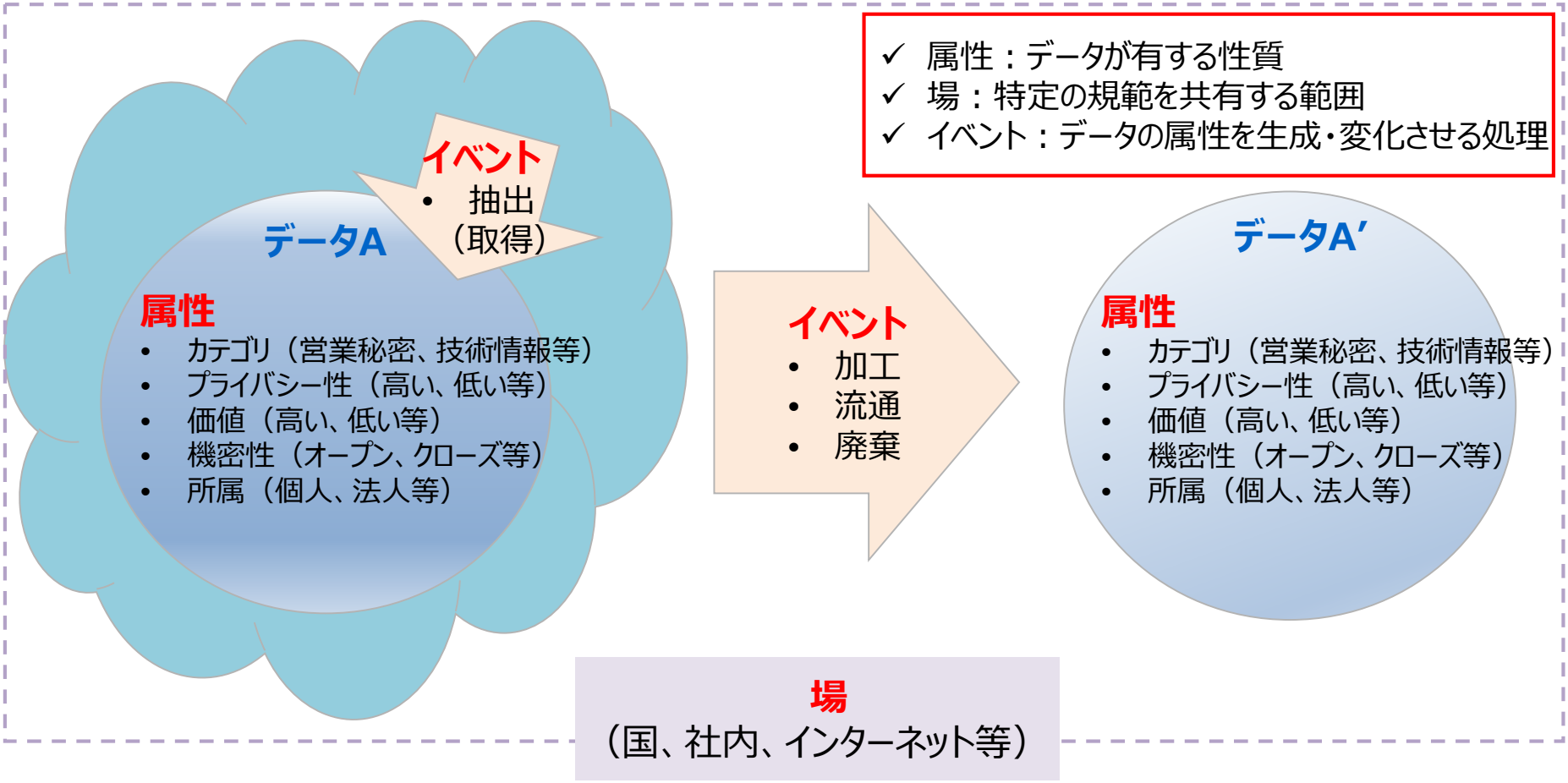
データの信頼性の確認手法の検討

**データそのものや生成者の実体の確認**
**⇒データの真正性確認、モノ等の確認など**

**データの来歴の確認**
**⇒トレーサビリティの仕組みの検討など**

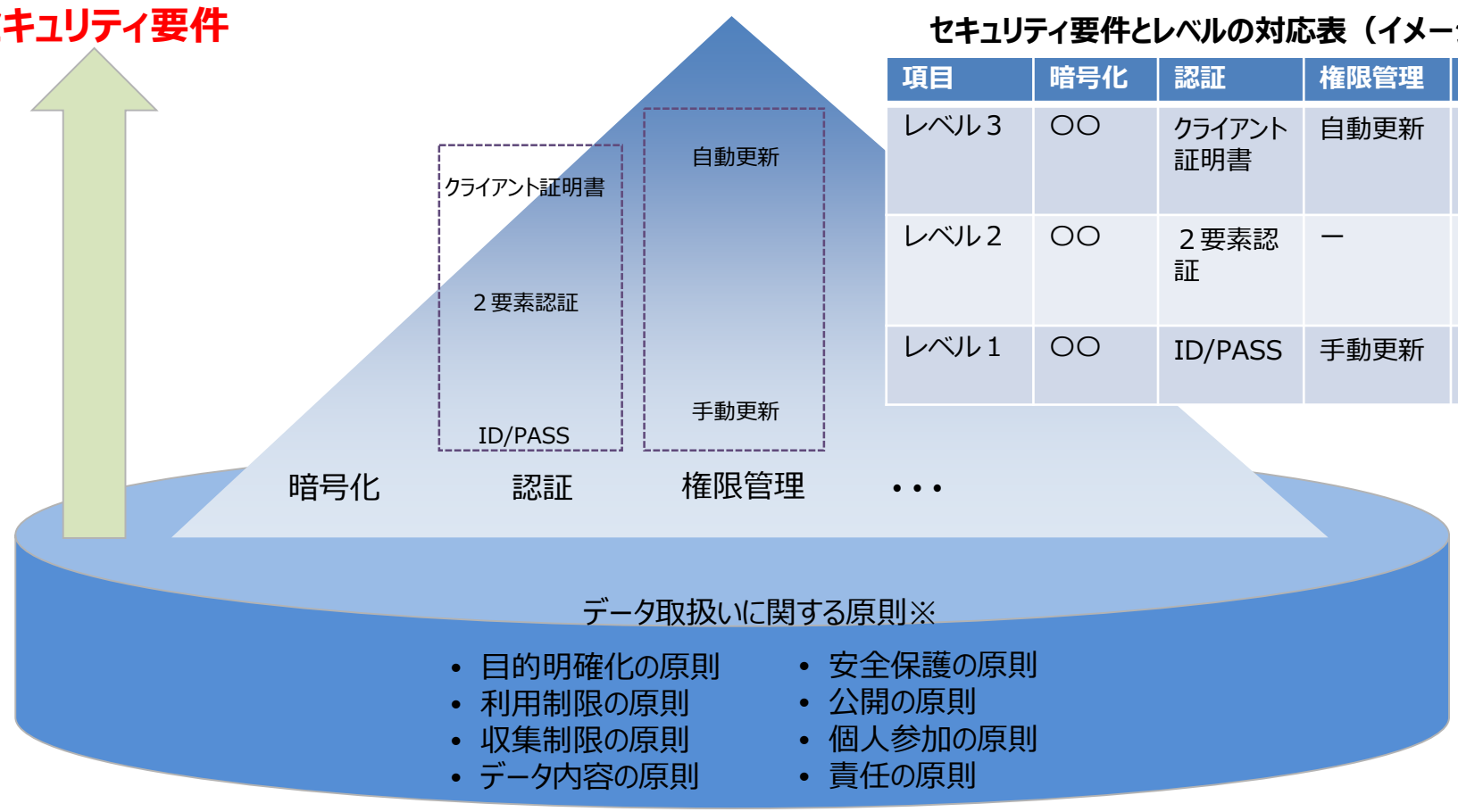
# 『第3層TF』データマネジメントの新たな捉え方

- 既存のデータマネジメント等の考え方を参考にしつつ、第1回タスクフォースの議論を踏まえ、**データマネジメント**とは、「**データの属性が場におけるイベントにより変化する過程をライフサイクルを踏まえて管理すること**」とここでは捉える。



# 『第3層TF』セキュリティ要件の考え方

- データに対する適切なセキュリティ要件を示すことができれば、データを流通させる際のセキュリティ基準が明確になり、データ有効活用の更なる拡大につながるのではないか。



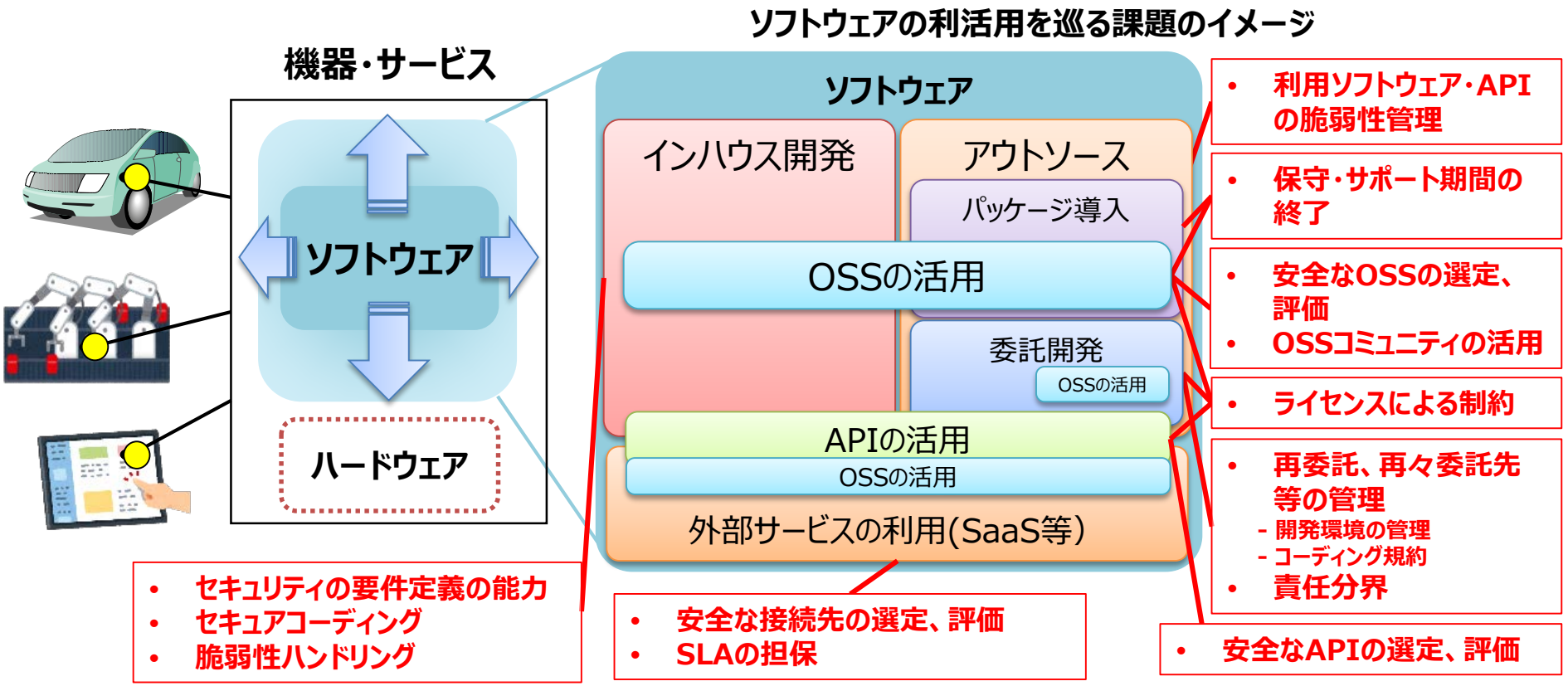

セキュリティ要件とレベルの対応表（イメージ）

| 項目 | 暗号化 | 認証 | 権限管理 | … |
|---|---|---|---|---|
| レベル３ | ○○ | クライアント証明書 | 自動更新 | |
| レベル２ | ○○ | ２要素認証 | ー | |
| レベル１ | ○○ | ID/PASS | 手動更新 | |

※　OECDプライバシーガイドラインにおける8原則。

# 『ソフトウェア』タスクフォースの検討の方向性

- 本タスクフォースにおいて、**米国NTIAのSoftware Component Transparencyの議論との連携を視野に**入れながら、**OSSを安全に活用するための手法、ソフトウェアの脆弱性管理手法等**を検討。



# 『ソフトウェアTF』における検討の方向性

- **ソフトウェア管理手法、脆弱性対応、OSSの利活用等**に関する検討を行う。

## ソフトウェア管理手法の検討

- ソフトウェアの開発から、運用中の脆弱性発見まで
- 構成管理・脆弱性管理に求められるソフトウェア管理手法のあり方
- SBOM等ソフトウェア管理スキームの活用に求められる技術面・制度面の課題

第1回
検討事項

## 脆弱性対応手法の検討

- 脆弱性が発見された場合のソフトウェアへの対応
- 脆弱性発覚時に必要な脆弱性への対応手法・体制のあり方
- 運用中システムへの脆弱性対応に求められる技術面・制度面の課題

第2回
検討事項

## OSSを利活用する際のビジネス的な側面の検討

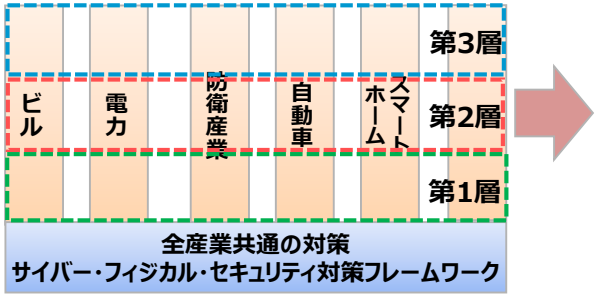
・OSS利用に関連するライセンスや契約
・OSS活用のベストプラクティス／OSSコミュニティへの発信

第3回
検討事項

# 『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）**

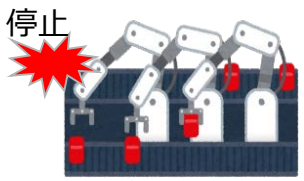



**タスクフォースにおける検討内容イメージ**

**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**

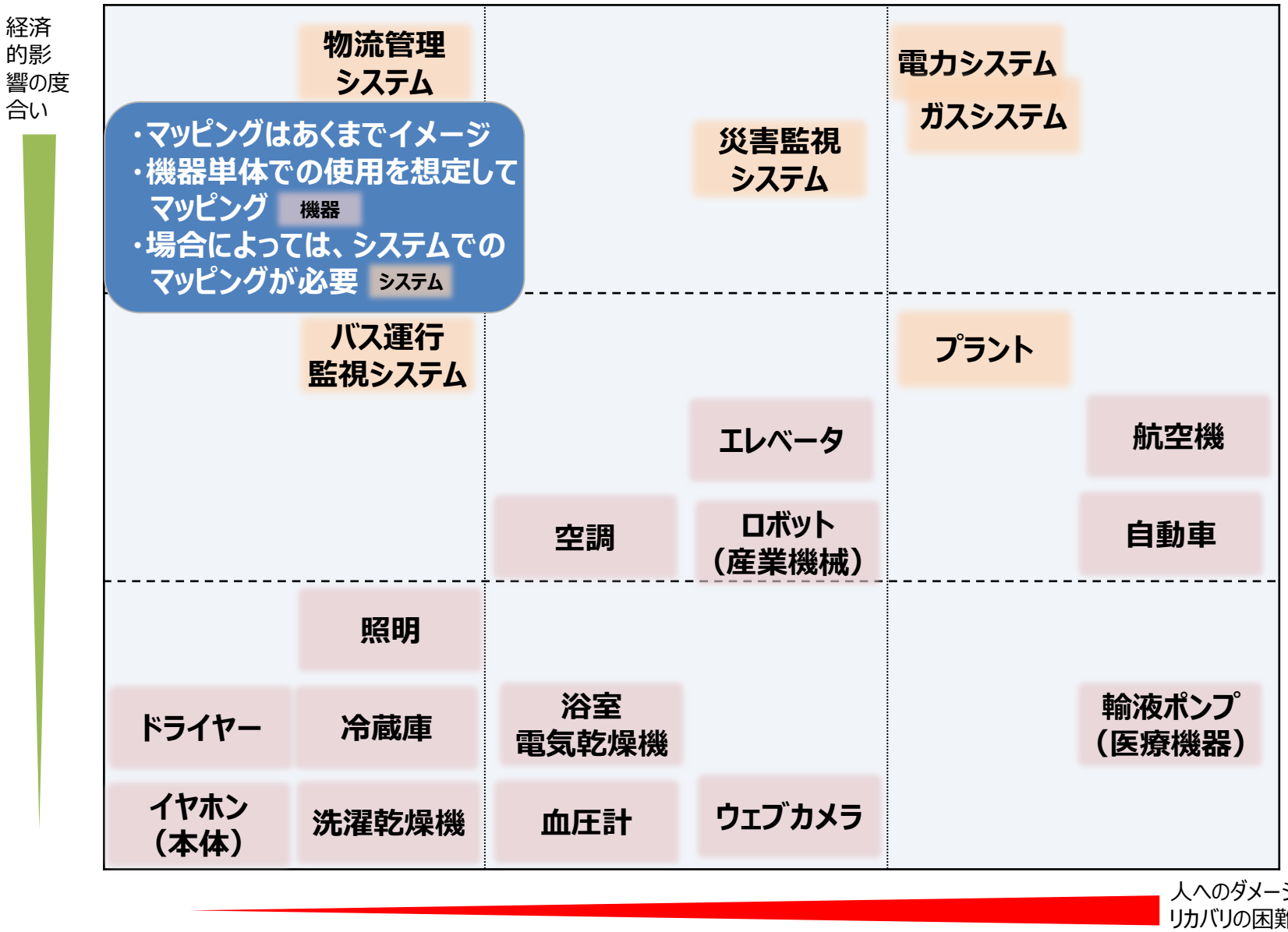
※ 特に高いセキュリティを求める機器に対する要件等を検討

**② サイバーリスクの安全への影響の増大への対応**

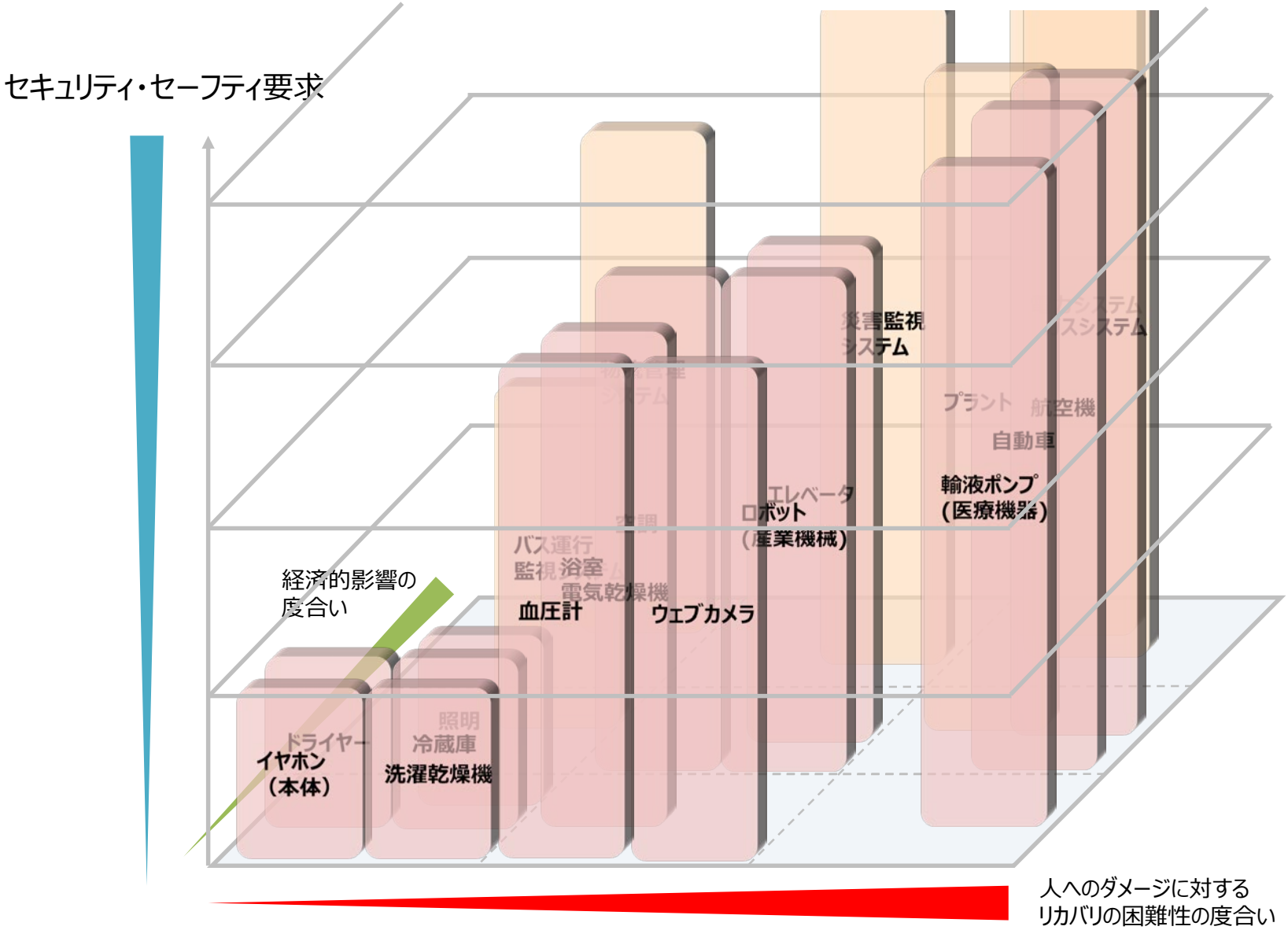



※ 安全も考慮に入れたセキュリティ対策等について検討

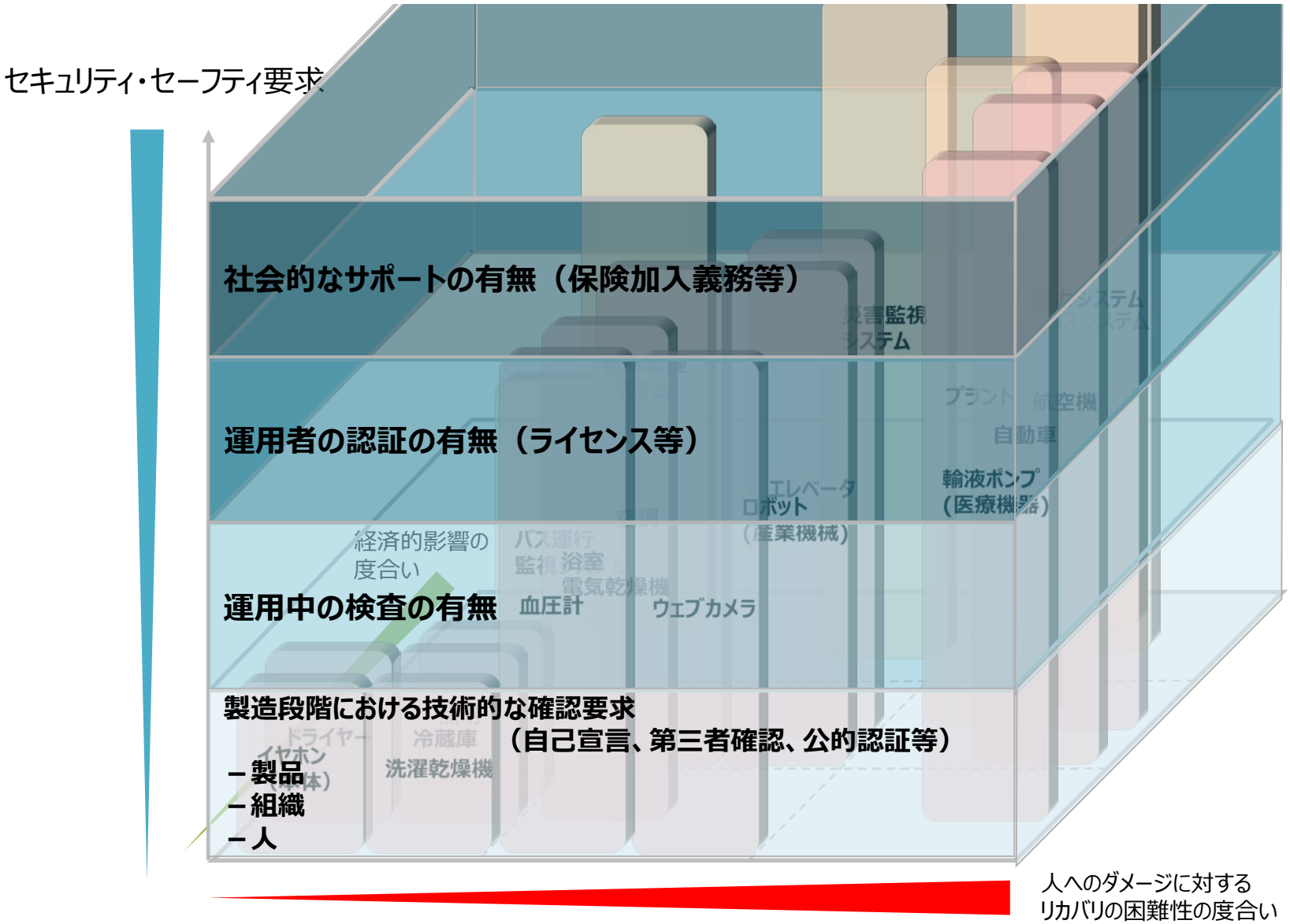
# サイバー・フィジカル間をつなげる機器・システムに潜むリスクのイメージ



# カテゴリに応じて求められるセキュリティ・セーフティ要求の強度のイメージ



# カテゴリに応じて求められるセキュリティ・セーフティ要求の強度のイメージ



# インド太平洋地域向け日米サイバー演習

- 経済産業省及びIPA産業サイバーセキュリティセンター（ICSCoE）が、日米の専門家による制御システムのサイバーセキュリティに関する演習をインド太平洋地域（14の国・地域）向けに実施。

■**日時・場所：**2019年9月9日（月）～12日（木）@東京（今年で２回目、以後毎年開催。）

■**参加者：**ASEAN９カ国、スリランカ、バングラデシュ、インド、NZ、台湾　35名

ICSCoE中核人材育成プログラム研修生　69名

■**来賓挨拶／講師：**

（米国）在日米国大使館首席公使代理、国務省東アジア・太平洋局首席次官補代理、エネルギー省、NIST、INL、ISA、米国企業

（日本）関芳弘経済産業副大臣、ICSCoE講師、日本企業

米国国務省挨拶


米国の専門家による講義


日本の専門家による講義

参加国・地域


ハンヅオントレーニング


ワークショップ


サイバー攻撃のデモ