経済産業省

資料3

『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11月27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

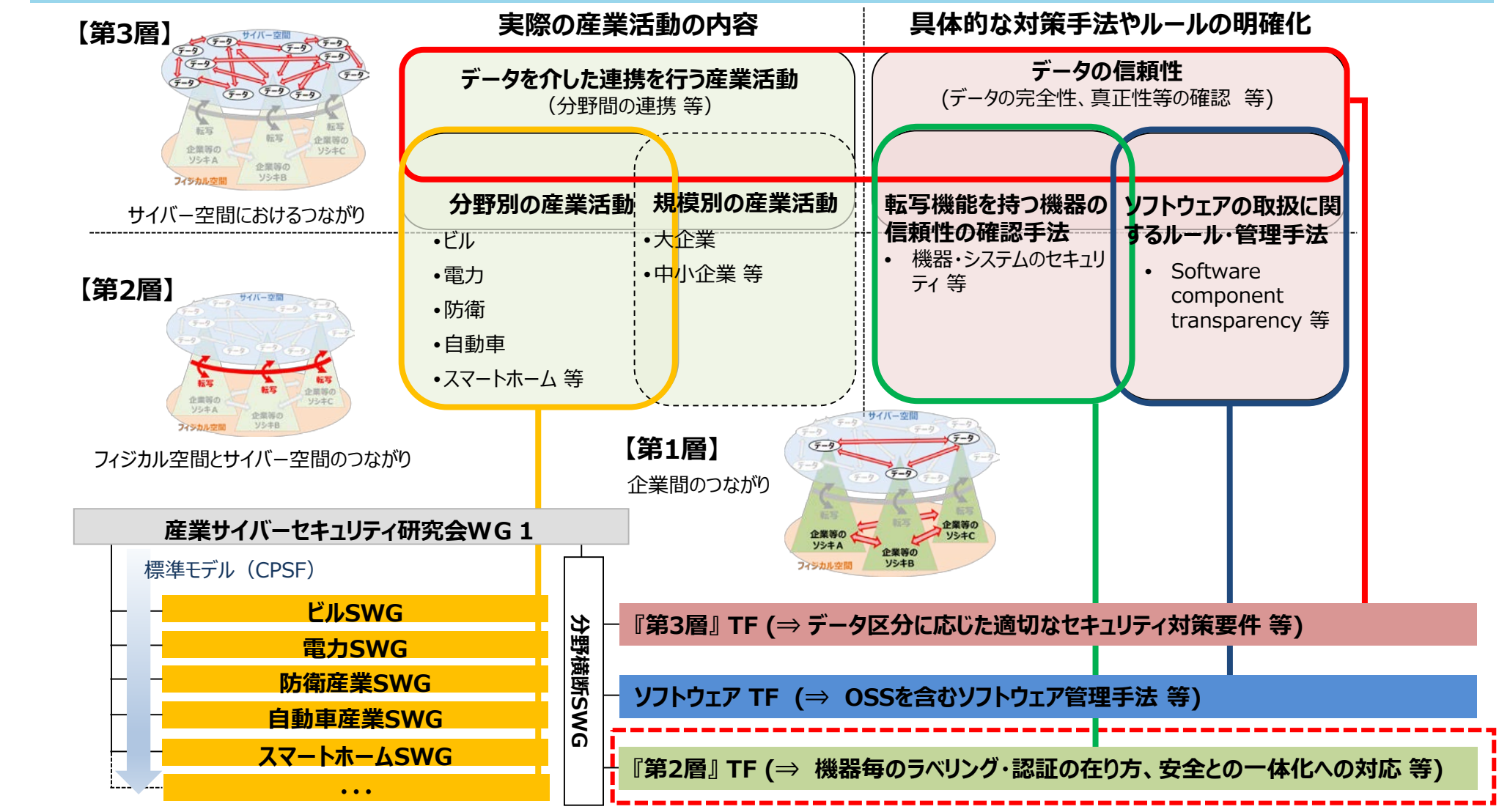
2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

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

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。**



テーマ別TFの検討状況

- 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。**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
（分野ごとに検討するためのSWGを設置）

- 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する。
7/31の第１回TFでは、プライバシーを含むデータの属性やデータに対する処理、データを扱う場等によって要求されるセキュリティが異なり得ること等を議論。

ソフトウェア TF

ソフトウェア管理手法、脆弱性対応、OSSの利活用等について検討する。
9/5の第1回TFでは、SBOM等を用いたソフトウェア管理手法について、11/6の第2回TFでは脆弱性対応について、それぞれ論点の洗い出しを行った。第3回TFでは、OSSの利活用等に関する論点の洗い出しを行う。

『第2層』TF

サイバー・フィジカル間の転写機能を持つ機器等について、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する。
8/2の第1回TFでは、安全とセキュリティを併せて考えることの重要性や求められるセキュリティに応じて機器をカテゴライズする必要性等について議論。

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

航空機の脆弱性に関するBlack Hat USA 2019での報告

- 2018年9月、大手航空機メーカーのサーバにおいて、航空機の**システム構成に関する情報がインターネット上に公開**されていることが発覚。IOActive社(I社)は、特定の脆弱性を用い、機内エンターテイメントシステム等から、**機器の操作に関わるネットワークに到達できることを発見**し、メーカーに報告。メーカーはI社に対して、報告されたのは**悪用可能な脆弱性ではなく、緩和策も実施済と回答するも、詳細は不開示**。
- これに失望したI社は2019年8月の**Black Hatで脆弱性の詳細を公開**。
- これを受けメーカーは、I社は航空機ネットワークの一部を評価しただけで、I社のシナリオでは**重要な航空機システムに影響を与えることはできず、発表は無責任だと失望を表明**。

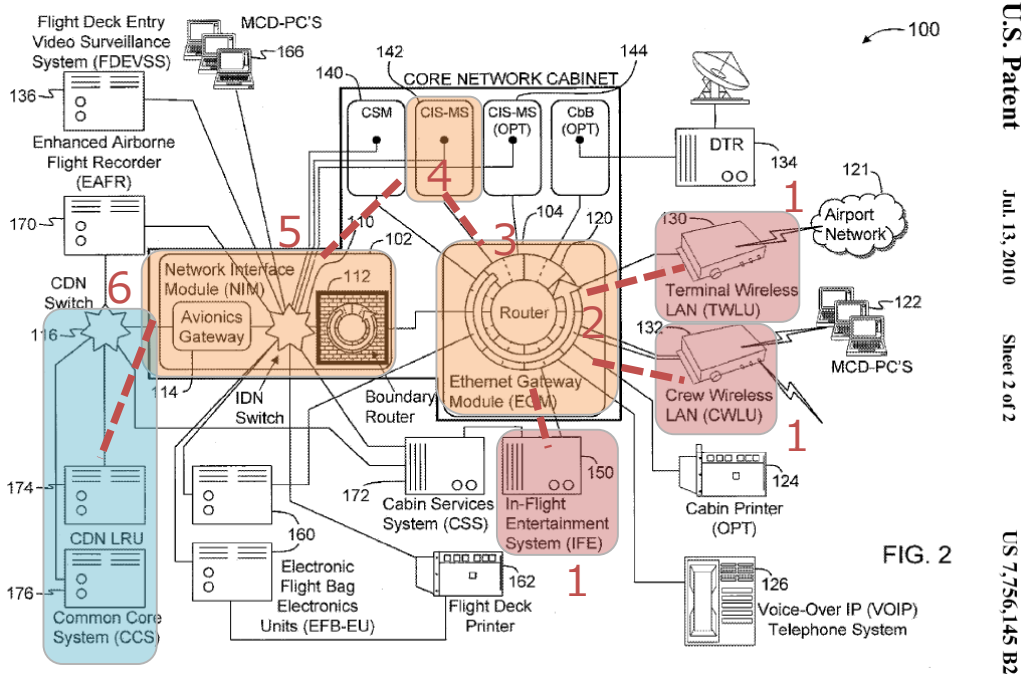


FIG. 2

U.S. Patent Jul. 13, 2010 Sheet 2 of 2 US 7,756,145 B2

●基本的な攻撃対象の解説図

1の機内エンターテイメントシステムや外部ネットワークから、6の機体の操作やナビゲーションに関連するとされるネットワークに到達できると解説されている。

https://ioactive.com/arm-ida-and-cross-check-reversing-the-787s-core-network/
https://www.wired.com/story/boeing-787-code-leak-security-flaws/

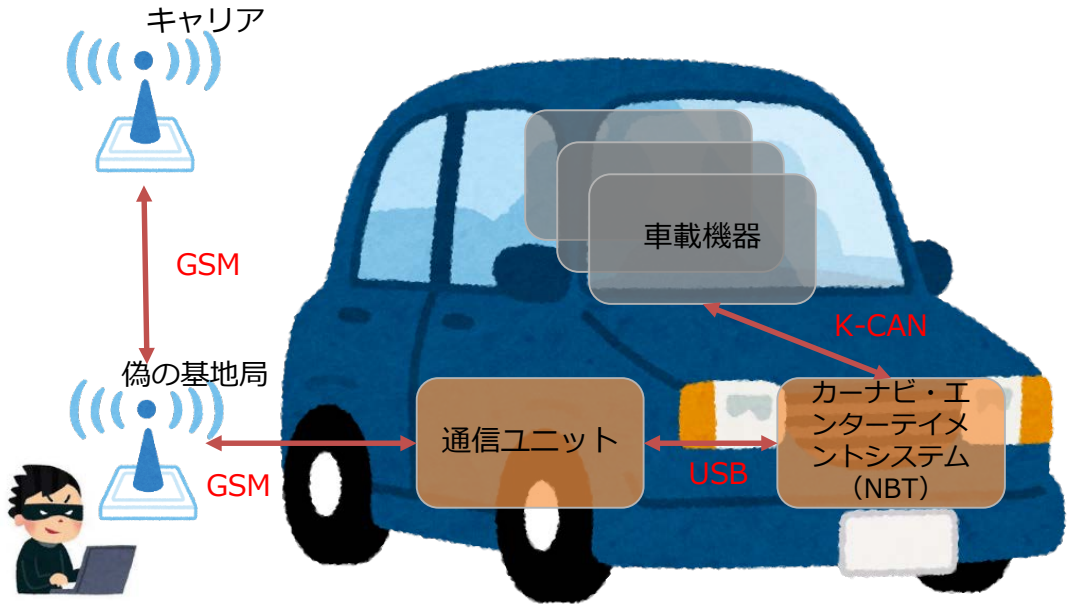
自動車の脆弱性に関するBlack Hat USA 2019での報告

- 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＞

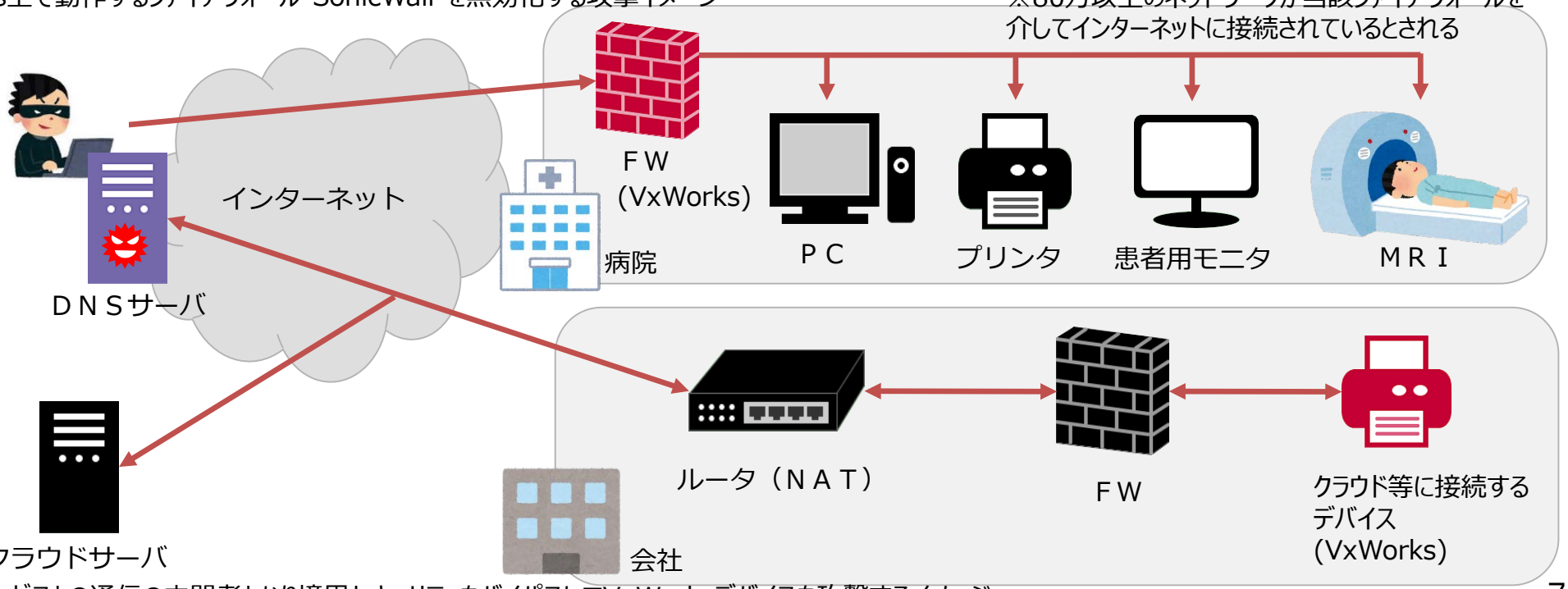


https://www.blackhat.com/us-19/briefings/schedule/#-days--mitigations-roadways-to-exploit-and-secure-connected-bmw-cars-15313

リアルタイムOS　VxWorks等における脆弱性（URGENT/11）

- 2019年7月、Armis Labは、**医療、自動車、航空機、防衛など幅広い産業において20億個以上のデバイスで採用されるWindRiver社のVxWorksに11個の脆弱性**があることを発表。本脆弱性はVxWorksが採用するTCP/IPスタックに存在し、これを利用することでファイアウォール等の境界セキュリティを制御したりバイパスすることが可能となり、ネットワーク内外でマルウェアを伝搬させることができるようになるとされる。
- 同10月、VxWorksと同じ旧Interpeak社製のTCP/IPスタックをサポートしていた**別のリアルタイムOSにも同様の脆弱性**があることが発覚。影響の拡大が懸念される。

VxWorks上で動作するファイアウォール“SonicWall”を無効化する攻撃イメージ



クラウドサービスとの通信の中間者となり境界セキュリティをバイパスしてVxWorksデバイスを攻撃するイメージ

https://www.armis.com/urgent11/

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

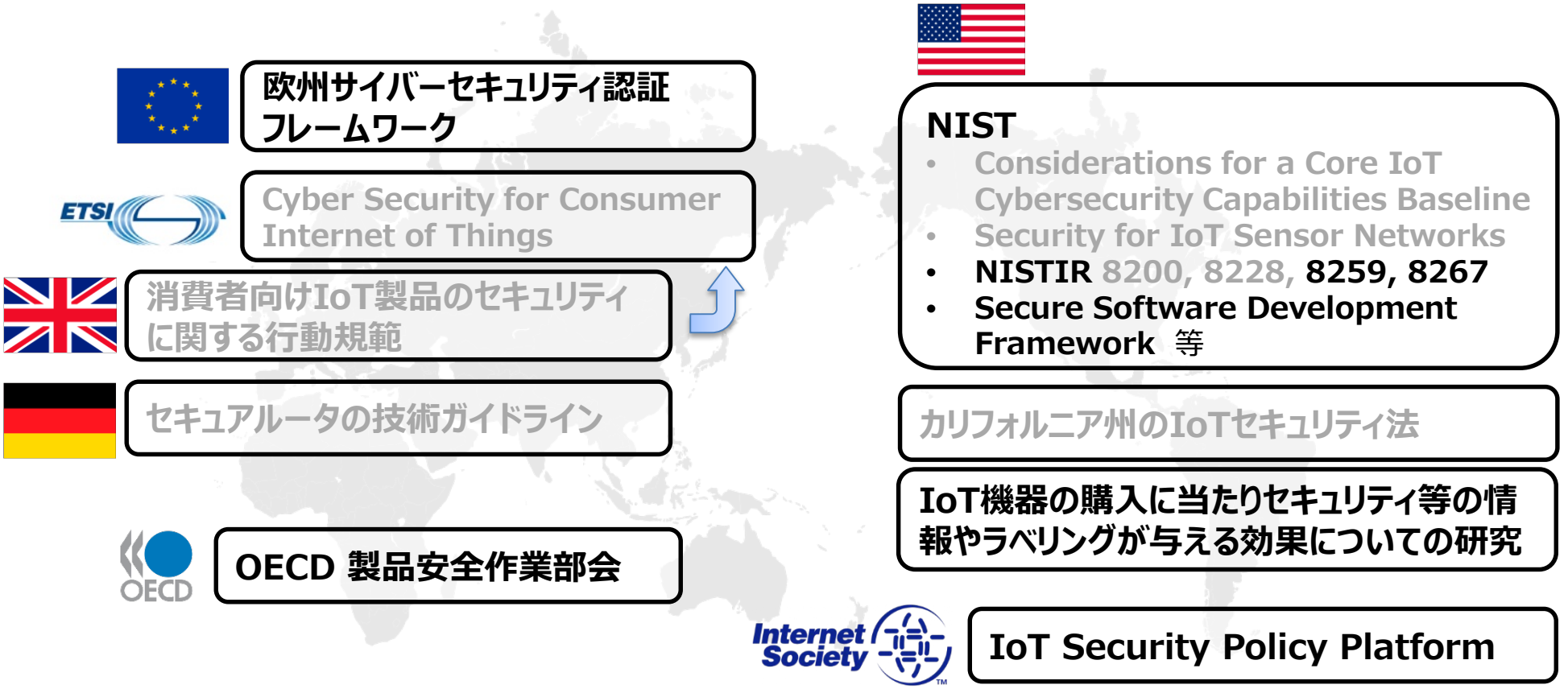
2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

**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。



※　黒字が前回TFから、新たに公開された、又は更新された文献

NISTIR 8259 draft - Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufactures

- IoT機器を管理する組織向けの推奨事項をまとめたNISTIR 8228に対し、**IoT機器の製造者がIoT機器のデザイン工程で考慮すべき事項**を整理（2019年7月ドラフト版公開）。製造者が自主的に採用することのできる**6つのコアサイバーセキュリティ機能をベースラインと定義**し、当該機能を達成するために実装すべき重要要素や、既存のIoTセキュリティガイダンス文章への参照がまとめられている。
- 一方で、コアベースラインの**全ての機能が全ての状況で必要であるわけではない**ことにも言及。

6つのコアサイバーセキュリティ機能

（１）機器の識別：IoT機器を論理的・物理的に一意に識別できる。	（４）インターフェイスへの論理アクセス：IoT機器のインターフェースへの論理アクセスを認可エンティティのみに制限可。
（２）デバイスの構成：IoT機器のソフトウェア・ファームウェアの構成変更が可能。変更は、認可エンティティのみが行うことができる。	（５）ソフトウェア等の更新：IoT機器のソフトウェア・ファームウェア更新は、認可エンティティによって安全かつ構成可能なメカニズムを用いてのみ実行できる。
（３）データ保護：IoT機器が保存・送信するデータを不正なアクセス及び変更から保護することができる。	（６）サイバーセキュリティイベントログ：IoT機器はイベントをログに記録し、認可エンティティのみにアクセスを許可。

サイバーセキュリティ機能を実装する際の留意事項

（１）デバイス仕様：サイバーセキュリティ機能を提供するのに十分なハードウェア、ファームウェア、ソフトウェアの必要性（機器のライフサイクルにおいて十分なリソースを有するか、不必要なセキュリティ機能を有していないか、等）
（２）サイバーセキュリティ機能の継承：特定の局面において、特定のサイバーセキュリティ機能が省略され得ることを提起（強固なフィジカルセキュリティ環境下にある機器の物理インターフェースのアクセス制限の省略、配下IoT機器からIoTゲートウェイへのネットワーク論理アクセス保護機能等の移行、等）

NIST - Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

- NISTは、セキュリティに配慮したソフトウェア開発手法を既存の標準やガイドライン等を参照する形でSecure Software Development Framework (SSDF)として整理（2019年6月にドラフト版を公表）。
- SSDFでは、各手法を「組織構築」「ソフトウェア保護」「セキュアなソフトウェア」「脆弱性レポート対応」の4つに分類の上、何をすべきか（Practice-Taskの2階層）、事例、参照文書について体系化。

【 SSDFにおける各手法の分類】

分類	分類（英語名）	概要	手法例	備考
組織構築	Prepare the Organization（PO）	人材、処理能力、技術等のソフトウェア開発リソース確保	• ソフトウェア開発におけるセキュリティ要件を定義 • 各役割と責任の実装	• PSの中でSBOMの作成と維持について言及あり • 参照文書（Reference）は、ISO、BSA、NIST CSF 等
ソフトウェア保護	Protect the Software（PS）	ソフトウェアの全てのコンポーネントを改ざんや不正アクセスから保護	• 全ての形式のコードを改ざんや不正アクセスから保護	
セキュアなソフトウェア	Produce Well-Secured Software（PW）	ソフトウェアリリース時のセキュリティに関する脆弱性を最小化	• ソフトウェアデザインにおいてリスク情報・セキュリティ要件を考慮	
脆弱性レポート対応	Respond to Vulnerability Reports （RV）	ソフトウェアセキュリティの脆弱性の認識、適切な対応、将来にわたる予防策	• 継続的な脆弱性の特定・確認 • 改善策の評価・優先付け	

NISTIR 8267 draft - Security Review of Consumer Home Internet of Things (IoT) Products

- NISTIR 8267では、スマートホームで用いられる7カテゴリ※1の家庭用IoTデバイスについて、サンプル調査※2を通じてセキュリティ機能をレビューした上で、NISTIR 8259 draftも参照しつつ、家庭用IoTデバイスのメーカーが開発時に考慮すべき事項をまとめている（2019年10月ドラフト版公開）。

※１　スマート電球・照明・カメラ・ドアベル・プラグ・サーモスタット・TV
※２　公開情報調査やネットワークキャプチャ等の実機調査を実施。分解等を含むより詳細な調査は行っていない。

家庭用IoTデバイスメーカーが考慮すべき事項

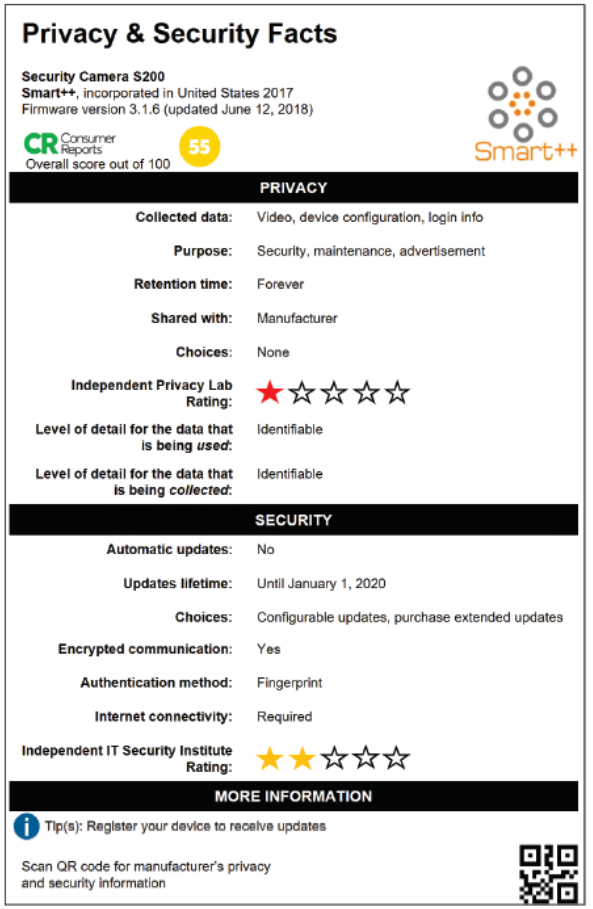
- ユーザーによるデバイスの初期設定時に、NIST SP 800-63が示したベストプラクティスと同等な強度のパスワードを設定するよう要求すること
- 中間者攻撃を防ぐため、認証書や公開鍵をホスト名と関連付ける”Certificate Pinning”を用いること
- デバイスのソフトウェア/ファームウェアの更新やデバイスを通じてやりとりされる機密データを保護するために、 NIST SP 800-52 Rev-2で推奨されるTLS暗号化スイートを使用すること
- USBを含む使用されない物理的又は論理的アクセスポートを閉じるか、アクセスを防ぐこと
- 家の外に設置されるセキュリティに関連するIoTデバイスに物理的リセットボタンを実装しないこと
- デバイスのソフトウェア/ファームウェアの更新ができ、かつ、そのことがタイムリーにユーザーへ通知されるようなプロセスを、ベストプラクティスに沿って開発・実装すること
- UPnP通信はデフォルトでは認証を利用しないため、UPnP通信を保護するために追加の端末保護機能を実装すること
- サイバーセキュリティ機能は、技術に詳しくないユーザーにも分かりやすいものにするなど、適用可能性や実行性の高いものにすること

IoT機器の購入に当たりセキュリティ等の情報やラベリングが与える効果についての研究

- Lorrie Faith Cranor教授（米カーネギーメロン大学）らの研究論文（2019年5月公開）。プライバシーとセキュリティに関する情報や、当該情報を付与したラベルが、IoT機器の購入の意思決定に及ぼす影響についてインタビュー調査等を実施。

概要

- IoTデバイスの購入を決定する際に、プライバシーとセキュリティを**自発的に検討したのは一部の参加者**だけだったが、一度促されると、**ほとんどの人が懸念を表明**した。
- **ほとんど全ての参加者は**、デバイスにおけるプライバシーやセキュリティに関する情報の重要性を認識しており、購入時に情報を利用できるなら**プレミアムを支払う意思がある**と述べた。
- 多くの参加者は、セキュリティとプライバシーに関する情報は、スマートカメラなど特に**センシティブな情報を収集していると考えるデバイスの購入決定に影響を与える**要因であると述べた。
- IoTデバイスの購入時における比較において、**ラベルに記載された独立した機関が提供するプライバシーやセキュリティに関するわかりやすいレーティング**（★等）は、ほとんど全ての参加者の**注目を集めた**。



出典：”Exploring How Privacy and Security Factor into IoT Device Purchase Behavior”
https://www.cs.cmu.edu/~pemamina/publication/CHI'19/CHI19.pdf

セキュリティ及びプライバシー対策が不十分なスマートカメラにおけるプロトタイプラベルの一例

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

- 2019年4月、Cybersecurity Act が欧州理事会で採択、6月27日に発効。
- **2019年9月、ENISAがサイバーセキュリティ認証スキームの候補を準備するためのアドホックワーキンググループの設立を呼びかけ。候補スキームとしてCommon Criteria(ISO/IEC 15408)も考えられるとの記載もある。**

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製品等の製造者又は提供者は、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、欧州規格又は国内規格への参照及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）

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

- IoTセキュリティは、セーフティとセキュリティの関係が強いことから、製品安全に関する課題を扱う製品安全作業部会と、情報システムやネットワークのセキュリティ等を扱うデジタル経済セキュリティ・プライバシー作業部会が、2020年11月から共同して検討する場を設けることとなった。

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組の調和を目指す。
- 2019年11月、各国におけるIoTセキュリティフレームワークにおいて共通する原則をまとめたステートメントを公表。

【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）、METI（日本）、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

サイバー・フィジカル間をつなげる機器・システムをカテゴライズする際の軸の設定について

- 機器のカテゴライズについて、前回TFでの議論を踏まえ、以下のように再整理し、仮のフレームワークを提案したい。
- 転写機能を持つ機器・システムに求められる安全を考慮に入れるという第2層TFの趣旨に鑑み、**危害が発生した際にリカバリできるダメージかどうか**を最重要視し、第1軸を『**人へのダメージに対するリカバリの困難性の度合い**』と再定義。
- 他方、TFで指摘があった観点全てを軸に落とし込むと複雑になってしまうことから、それらの観点の多くは、便宜上、「リカバリ可能性が高く、金銭的価値に換算可能なもの」であると考え、第2軸を『**経済的影響の度合い**』と定義し、第2軸に各観点を写像することを考える。

＜第1回TFでの指摘＞

○安全といっても、人命や資産という物理的な影響以外にも、経済性の混乱や生活の不便性等、様々ある。

○プライバシーの問題が発生したときに、プライバシー侵害は、事案によっては極めて大きな損害につながるケースがある。最近の精神的損害や刑事責任との関係の位置づけ、さらに、法的な責任とは別に事故が起きた場合のレピュテーションリスクをどこに置くべきなのか等、気になっている。

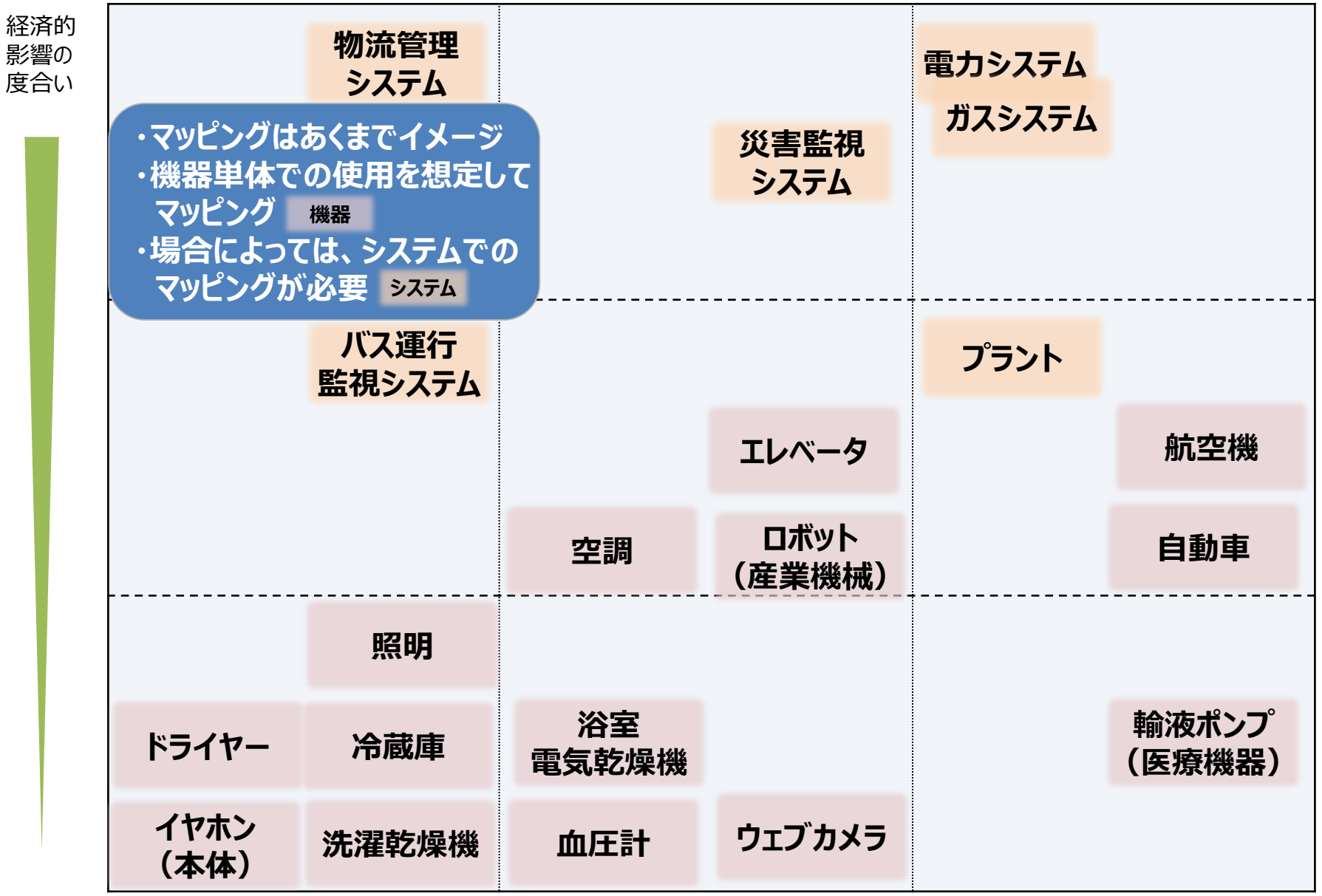
＜ISO/IEC GUIDE 51:2014（JIS Z 8051:2015)＞

3.14
安全（safety）
許容不可能なリスク（3.9）がないこと。

3.9
リスク（risk）
危害（3.1）の発生確率及びその危害の度合いの組合せ。

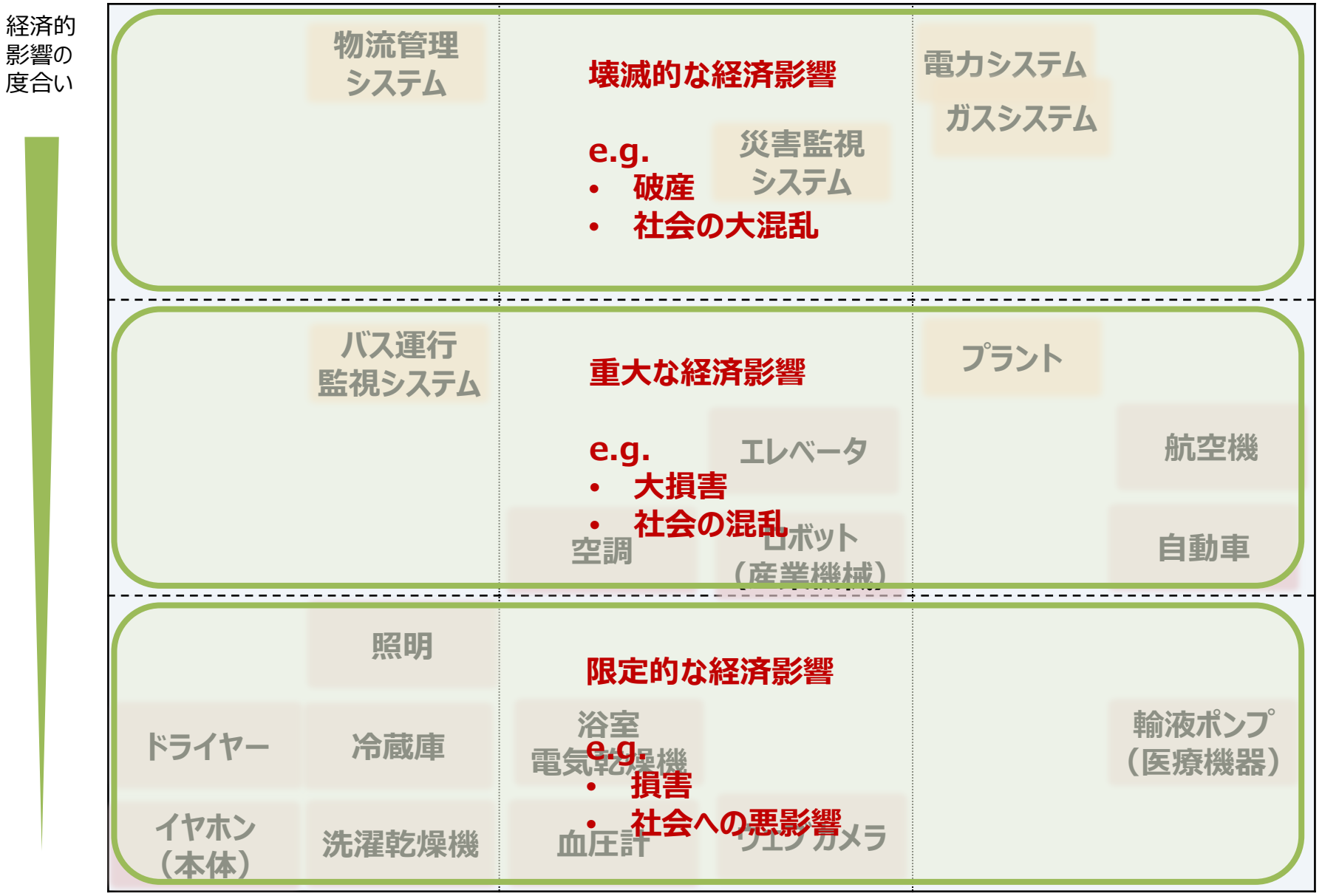
3.1
危害（harm）
人への傷害若しくは健康障害、又は財産及び環境への損害。

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



サイバー・フィジカル間をつなげる機器・システムのカテゴライズのイメージ

サイバー・フィジカル間をつなげる機器・システムのカテゴライズのイメージ

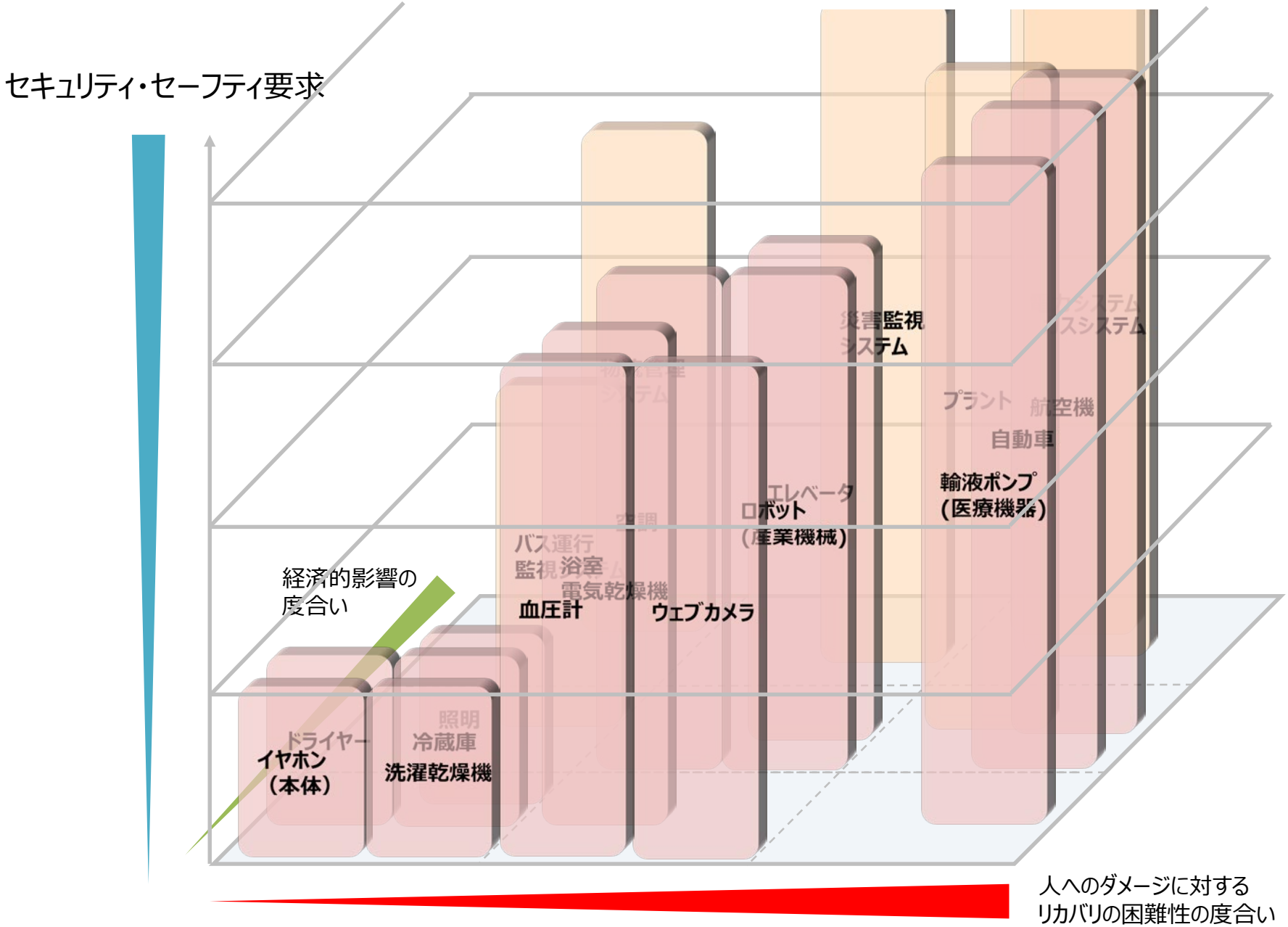


サイバー・フィジカル間をつなげる機器・システムのカテゴライズ基準の例

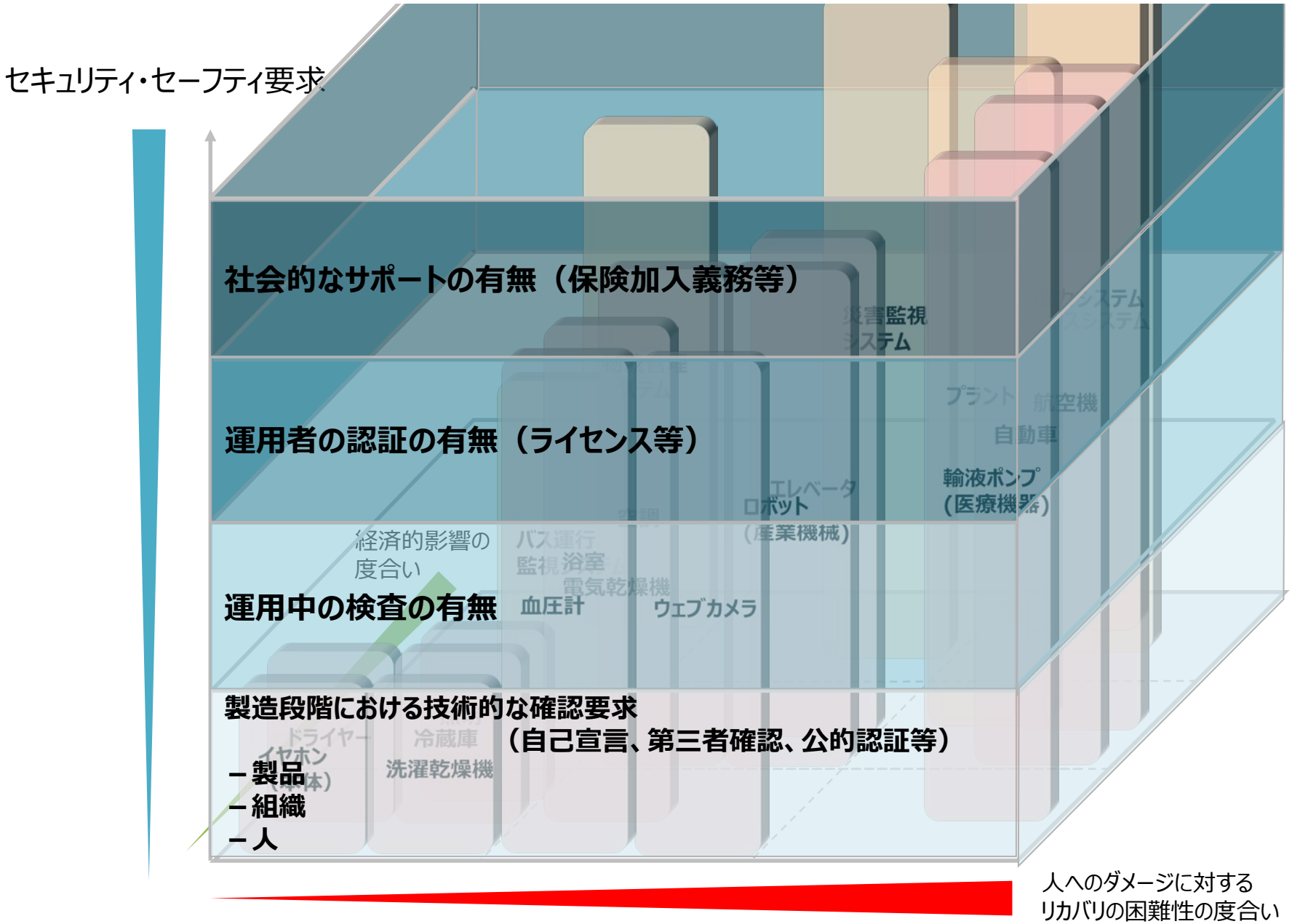
- 指摘のあった観点それぞれについて影響の度合いを整理。他に考慮すべき観点はないか、あるいは、各観点における影響の度合い（レベル）の表現は適切か、検討が必要
- CPSFを適用してリスクアセスメントを実施する際に、これらの観点が利用可能ではないか。

基準		それぞれの観点におけるカテゴライズ基準の例					
		ダメージに対するリカバリの困難性の度合い	経済的影響の度合い				
		人命/安全	プライバシー	資産	生活影響	社会影響	レピュテーション
Lv. 1	限定的な影響	軽傷	漏えい、悪用	損害	不便	悪影響	信用低下
Lv. 2	重大な影響	重傷	名誉毀損	大損害	支障	混乱	業績悪化
Lv. 3	致命的・壊滅的な影響	人命への影響	人命への影響	破産	困難	大混乱	倒産

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

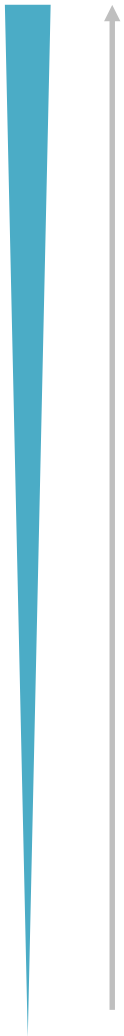


カテゴリに応じて求められるセキュリティ・セーフティ要求の強度のイメージ



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

セキュリティ・セーフティ要求



社会的なサポートの有無（保険加入義務等）
→ 自賠責保険　等

運用者の認証の有無（ライセンス等）
→ 運転免許　等

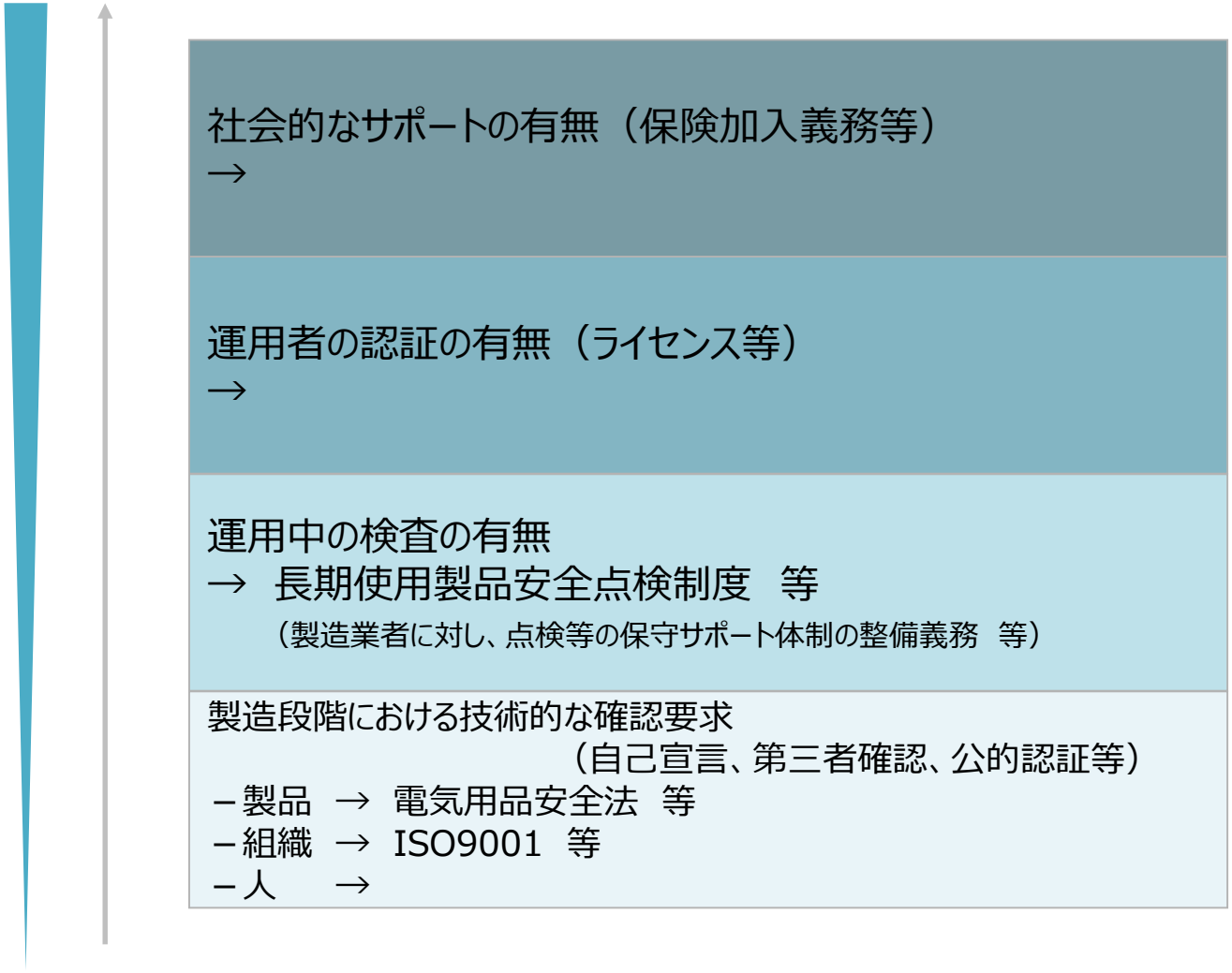
運用中の検査の有無
→ 自動車検査登録制度　等
（ユーザに対し、定期点検整備の義務　等）

製造段階における技術的な確認要求
（自己宣言、第三者確認、公的認証等）
－製品　→　型式認証　等
－組織　→　ISO26262　等
－人　　→　完成検査員（自動車型式指定規則）　等

自動車

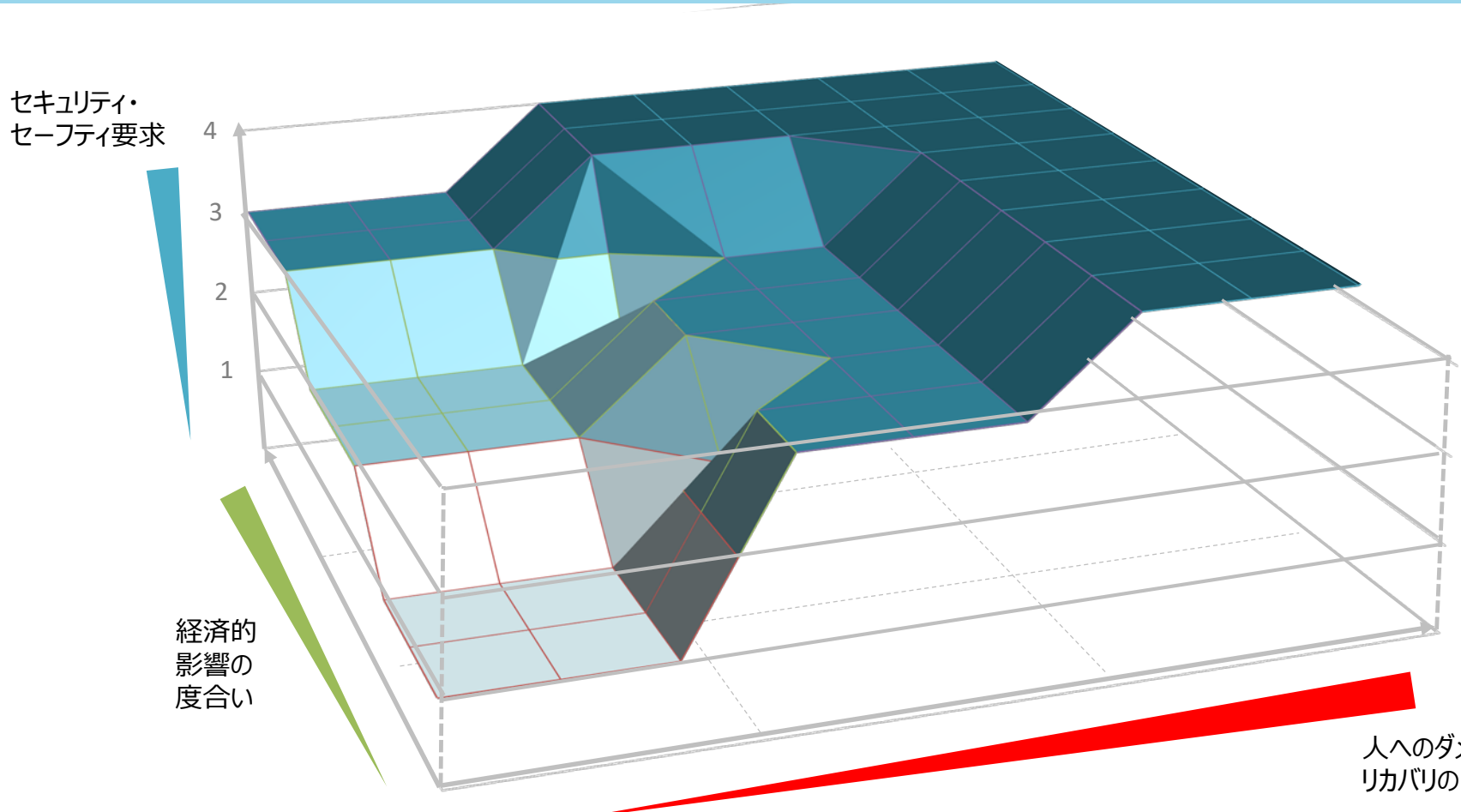
カテゴリに応じて求められるセキュリティ・セーフティ要求の強度のイメージ

セキュリティ・セーフティ要求



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について

- サイバー・フィジカル間をつなげる機器・システムに求められるセキュリティ・セーフティ要求の強度は、カテゴリ毎に異なり、リカバリが困難なものや経済的な影響が大きいものほど、より強固な要件を要するのではないか。
- カテゴリ毎に、セキュリティ・セーフティ要件の基準を見いだすことができるのではないか。



第2回TFでご議論いただきたい内容

- サイバー・フィジカル間をつなげる機器・システムのカテゴライズについて

軸の設定

危害が発生した際にリカバリできるダメージかどうかを最重要視し、第1軸を『**人へのダメージに対するリカバリの困難性の度合い**』と定義するとともに、第2軸にその他の観点を写像し、これを『**経済的影響の度合い**』と定義することは適切か。

観点

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観点として、『**人命/安全**』、『**プライバシー**』、『**資産**』、『**生活影響**』、『**社会影響**』、『**レピュテーション**』の６つを想定したが、それらの観点で十分か。また、それぞれについて、カテゴライズの基準は適切か。

セキュリティ・セーフティ強度

セキュリティ・セーフティ要件をレイヤ的に捉え、サイバー・フィジカル間をつなげる機器・システムのカテゴリ毎に、セキュリティ・セーフティ要件の基準（強度）を見いだす手法は適切か。また、それぞれのレイヤに必要なセキュリティ要素にはどのようなものがあるか。