「自動車業界の未来を支える！最新サイバーセキュリティと機能安全、サステナビリティ」セミナー

自動車サプライチェーンに求められるサイバーセキュリティ対応とは

SGSジャパン株式会社　C&P Connectivity

2025年5月23日

自己紹介

古田 健裕
SGSジャパン株式会社
C&P Connectivity 機能安全
takehiro.furuta@sgs.com

- 電機メーカ（オートモーティブ部門）出身
  ソフトウェアプロセス改善、機能安全、サイバーセキュリティなどの推進業務に従事
- 2021年より、SGSジャパンにてAutomotive SPICE、サイバーセキュリティ、機能安全などの業務に従事
  - SGS-TÜV認定 Automotive Cyber Security Expert (CACSE)
  - SGS-TÜV認定 Assessor and Auditor for automotive cyber security
  - SGS-TÜV認定 Automotive Functional Safety Expert (AFSE)
  - intacs認定 Principal Assessor (Automotive SPICE)
  - PMI認定 PMP
  - 日本SPICEネットワーク 運営委員

CACSE by SGS-TÜV Saar

AFSE by SGS TÜV SAAR

講演内容

- 自動車サイバーセキュリティの法規（UN-R155）・標準（ISO/SAE 21434）の制定から4年が経過しました。自動車のサプライチェーンを構成する各社への要求は様々であり、取り組み状況も濃淡があります。

- 本講演では、自動車のサプライチェーンを構成するOEM、サプライヤ、部品メーカに、プロセス・技術の両面からそれぞれどのようなことが求められているかを解説し、それを支援するサービスを紹介いたします。

目次

- サイバーセキュリティ攻撃事例
  - 自動車へのセキュリティ攻撃事例
  - 工場へのセキュリティ攻撃事例
- サイバーセキュリティに関する法規・標準
  - 自動車サイバーセキュリティ、ソフトウェアアップデート
  - 工場セキュリティ
- サイバーセキュリティへの対応
  - 自動車のサプライチェーンを構成する各社に対する要求
  - サイバーセキュリティマネジメントシステムの構築
  - サイバーセキュリティに対応した開発
  - インシデントに対応するサイバーセキュリティ体制の構築

目次

- サイバーセキュリティ攻撃事例
  - 自動車へのセキュリティ攻撃事例
  - 工場へのセキュリティ攻撃事例
- サイバーセキュリティに関する法規・標準
- サイバーセキュリティへの対応

自動車へのセキュリティ攻撃事例（１）

- 車両への攻撃が可能であることを実証（2010）

  IEEE Symposium on Security and Privacy（2010/5）

  - 電子制御ユニット（ECU）に侵入できる攻撃者が、ブレーキの無効化、オンデマンドでの個々のホイールの選択的なブレーキング、エンジンの停止など、ドライバーの入力を完全に無視して、幅広い自動車機能を制御する能力を実証した。
- 車両への攻撃が遠隔操作で可能であることを実証（2015）

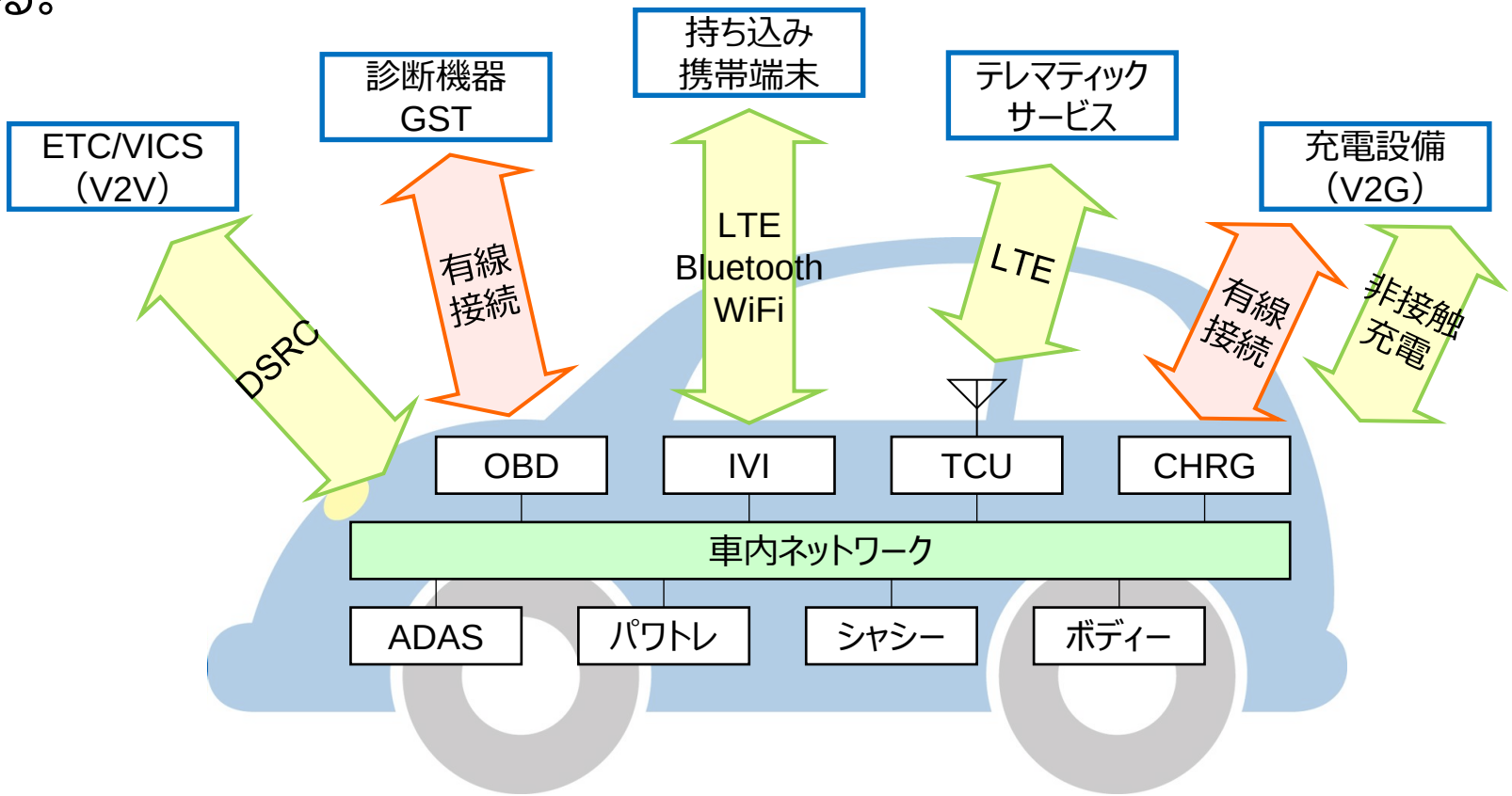
  Remote Exploitation of an unaltered Passenger Vehicle

  - 無線通信サービス（Uconnect）を介してECUを攻撃することにより、エンジン、ステアリング、ワイパーを制御できることを実証した。
  - FCA社は140万台のリコールを実施することになった。

自動車システムにおいて、サイバーセキュリティ対策が必要

自動車におけるサイバーセキュリティリスク

- 高度な自動走行については、外部からの通信が車内ネットワークにつながることによるサイバーセキュリティリスクが想定される。



参照：自動走行システムにおけるサイバーセキュリティ対策，経済産業省，2019

自動車へのセキュリティ攻撃事例（２）

- 複数のセキュリティ脆弱性をつき、車両への攻撃が遠隔操作で可能であることを実証（2016）

  Car Hacking Research: Remote Attack Tesla Motors

  - 通信機能の脆弱な仕様、車載情報端末のWebブラウザ、Linuxカーネルなどに存在した脆弱性をつき、自動車を遠隔操作（ドア開錠、ワイパー、ブレーキを制御）
  - テスラ社は、通知を受けて10日間で Model S の脆弱性を修正した。
- 第三者が脆弱性を発見・通知し、自動車メーカが公表（2020）

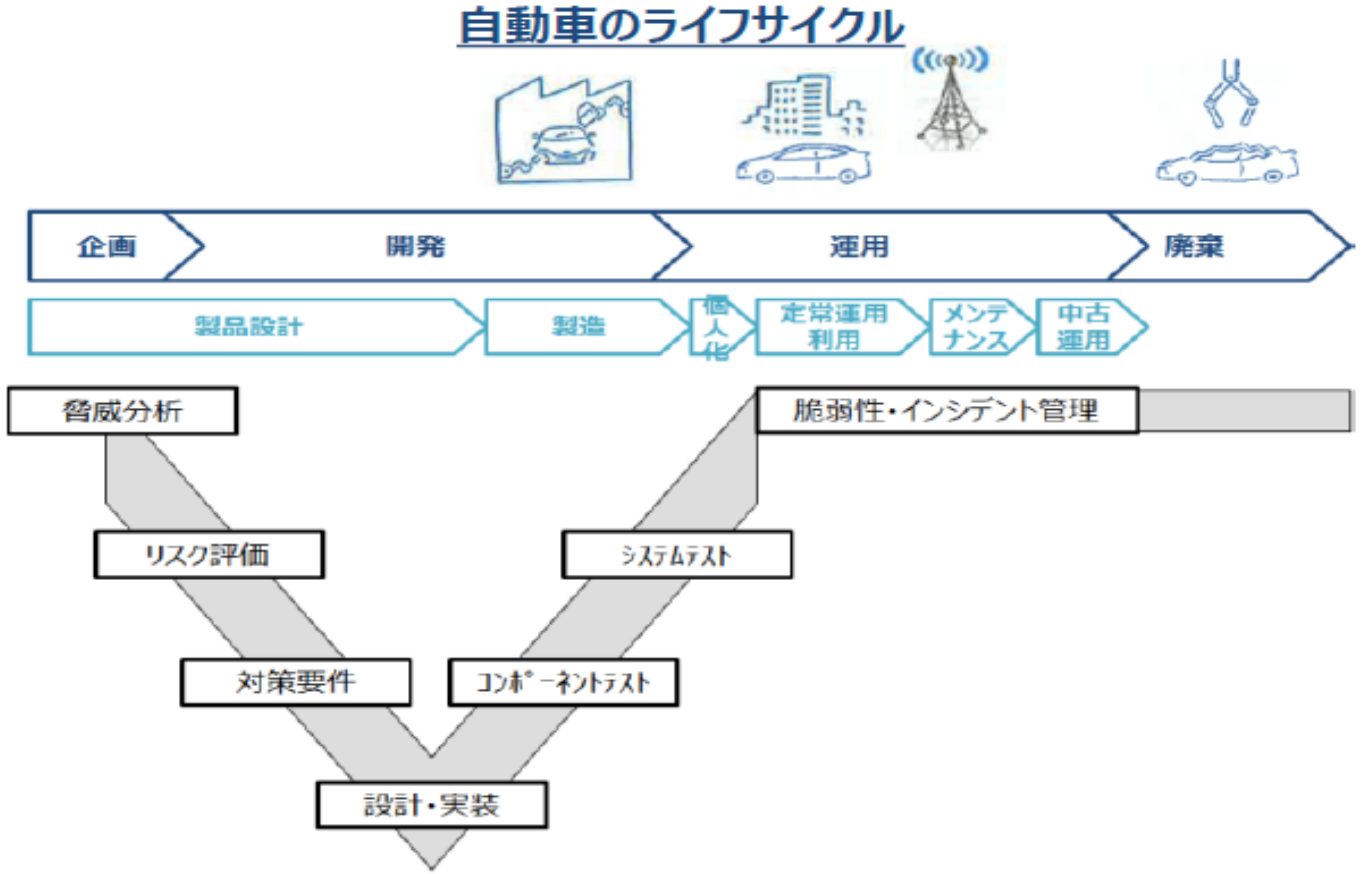
  Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars

  - 攻撃は極めて困難な内容であるが、ソフトウェアアップデートの対応を実施。
  - ニュースリリースを公開し、脆弱性発見者への謝意も示した。

PSIRT（Product Security Incident Response Team）体制の確立が必要
合理的な期間内に脆弱性を低減できるしくみ、セキュリティコミュニティとの良好なコミュニケーション、など

自動車におけるサイバーセキュリティへの対策

- 自動走行・コネクテッド化が進む中、企画～開発～運用～廃棄に至るまでライフサイクル全体を考えた検討・対策が必須である。



参照：自動走行システムにおけるサイバーセキュリティ対策，経済産業省，2019/6/26

工場へのセキュリティ攻撃事例

- 外部からのサイバー攻撃により、OEMの工場稼働が停止（2020/6）
  - 外部からのサイバー攻撃により大規模なシステム障害が発生
  - ホンダの国内外9工場の操業が停止し、オフィス系ネットワークシステムへの障害も発生

- サプライヤへのランサムウェア被害により、OEMの工場稼働が停止（2022/3）
  - サプライヤ（小島プレス工業）の子会社が独自に特定外部企業との専用通信に利用していたリモート接続機器に脆弱性があり、リモート接続機器から子会社内のネットワークに侵入し、さらにサプライヤのネットワークへ侵入して攻撃
  - サプライヤの工場稼働が停止
  - トヨタの14工場のラインが停止

参照：システム停止事案調査報告書（第1報）、小島プレス工業，2022

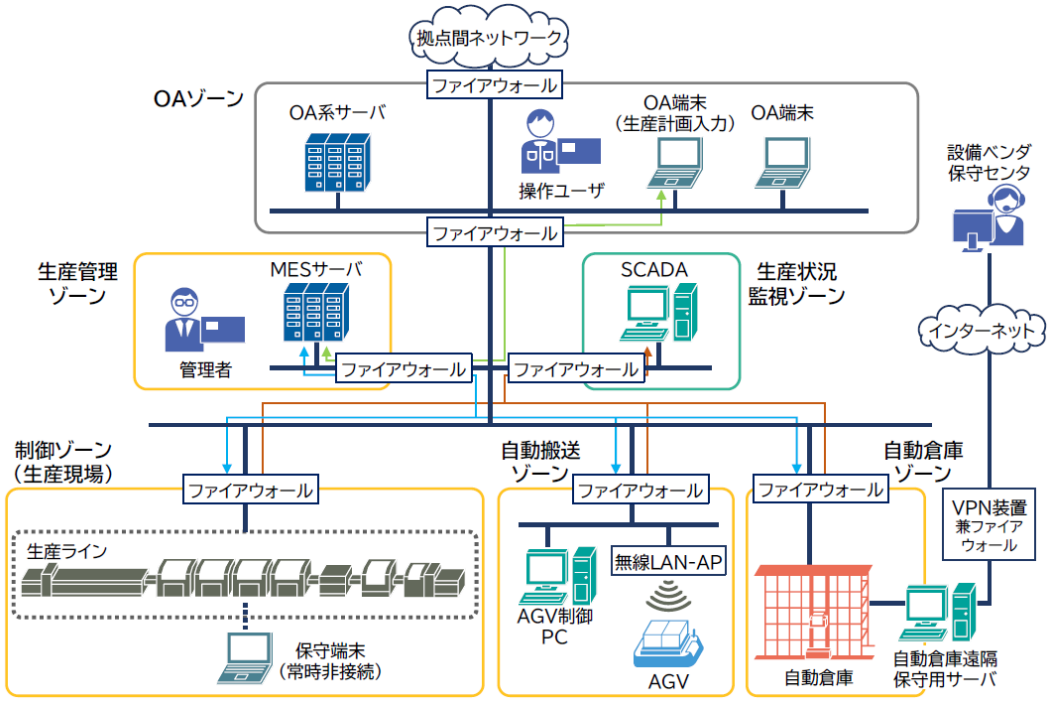
生産プロセスのサイバーセキュリティ管理システムの確立が必要

工場システムにおけるサイバーセキュリティ対策

- 背景
  - 工場のIoT化によるネットワーク接続機会の増加に伴い、サイバー攻撃リスクが増加。
  - 意図的な攻撃だけでなく、たまたま攻撃される場合もある。

⇩

  - いかなる工場でもサイバー攻撃のリスクがある。
  - 製造業／工場で重視されている安全確保、事業／生産継続、品質確保、納期遵守・遅延防止、コスト低減という価値が脅かされる恐れがある。
- 工場システムにおいて必要なサイバーセキュリティ対策
  - ネットワークにおけるセキュリティ対策
  - 機器におけるセキュリティ対策
  - 業務プログラム・利用サービスにおけるセキュリティ対策



参照：工場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，経済産業省，2022

目次

- サイバーセキュリティ攻撃事例
- **サイバーセキュリティに関する法規・標準**
  - **自動車サイバーセキュリティ、ソフトウェアアップデート**
  - 工場セキュリティ
- サイバーセキュリティへの取り組み

自動車サイバーセキュリティの法規化・標準化

	2020	2021	2022	2023	2024	2025
国連法規	2020/6 ▼ WP29において、CS/SU法規が成立	2021/3 ▼ UN-R155 (Cyber Security) UN-R156 (Software Update) 正式発行	2022/11 ▼ UN-R155 Amd.1		2024/3 ▼ UN-R155 Amd.2	2025/3 ▼ UN-R155 Amd.3 （2029/7より2輪を対象に追加）
国際標準		2021/8 ▼ ISO/SAE 21434 サイバーセキュリティエンジニアリング		2023/2 ▼ ISO 24089 ソフトウェア更新エンジニアリング		
国内法 道路交通法 道路運送車両法	2020/4 ▼ 自動運行装置（自動運転レベル3）を対象に サイバーセキュリティ確保 の要件を定義	2021/1 ▼ サイバーセキュリティ確保の要件を 全ての自動車を対象 とした 適用時期 OTAに対応している車両 新型車：2022/7、継続生産車：2024/7 OTAに対応していない車両 新型車：2024/1、継続生産車：2026/5		2023/4 ▼ 特定自動運行（自動運転レベル4）の許可制度を創設		
		2020/11 ▼ 自動車の特定改造等（OTAによるソフトウエア更新）の許可制度を創設				

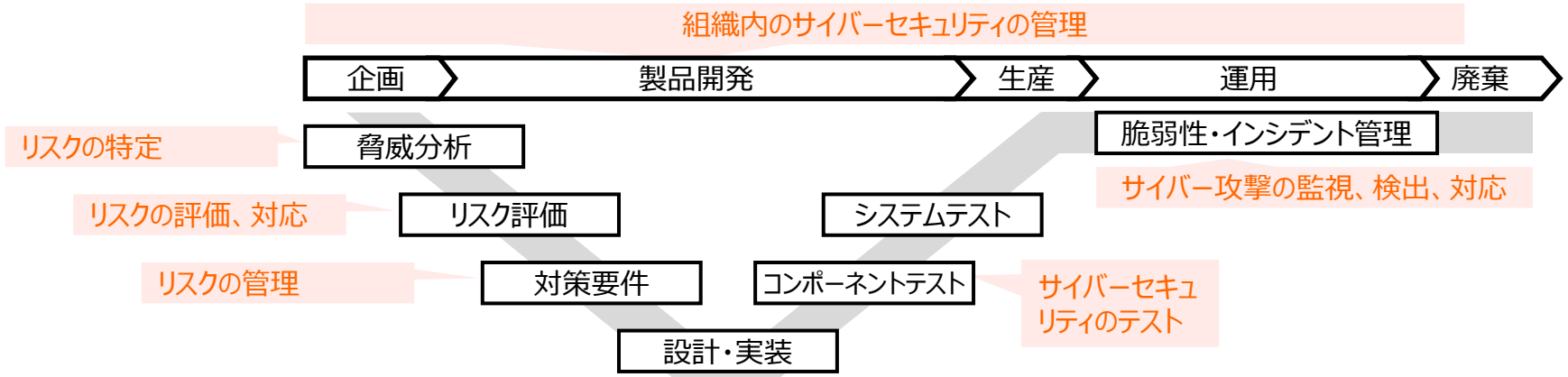
国連法規　UN-R155

- UN Regulation No.155

  Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

  サイバーセキュリティ及びサイバーセキュリティマネジメントシステムに関する車両の認可に関する統一規定

  - サイバーセキュリティマネジメントシステムの要件
    - 自動車メーカは、サイバーセキュリティマネジメントシステムの導入を認証当局又はテクニカルサービスに実証すること。
    - 自動車メーカは、サイバーセキュリティマネジメントシステムを確立し、サプライヤとの依存関係を管理すること。



  - 車両型式の要件
    - 認証される車両型式に関連するサイバーセキュリティマネジメントシステムの有効な適合証明書が必要。
    - 車両型式の重要な要素を特定し、リスクアセスメントを行い、特定されたリスクを適切に対応/管理すること。

参照：UN-R155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system，UN/ECE，2021

国連法規　UN-R155

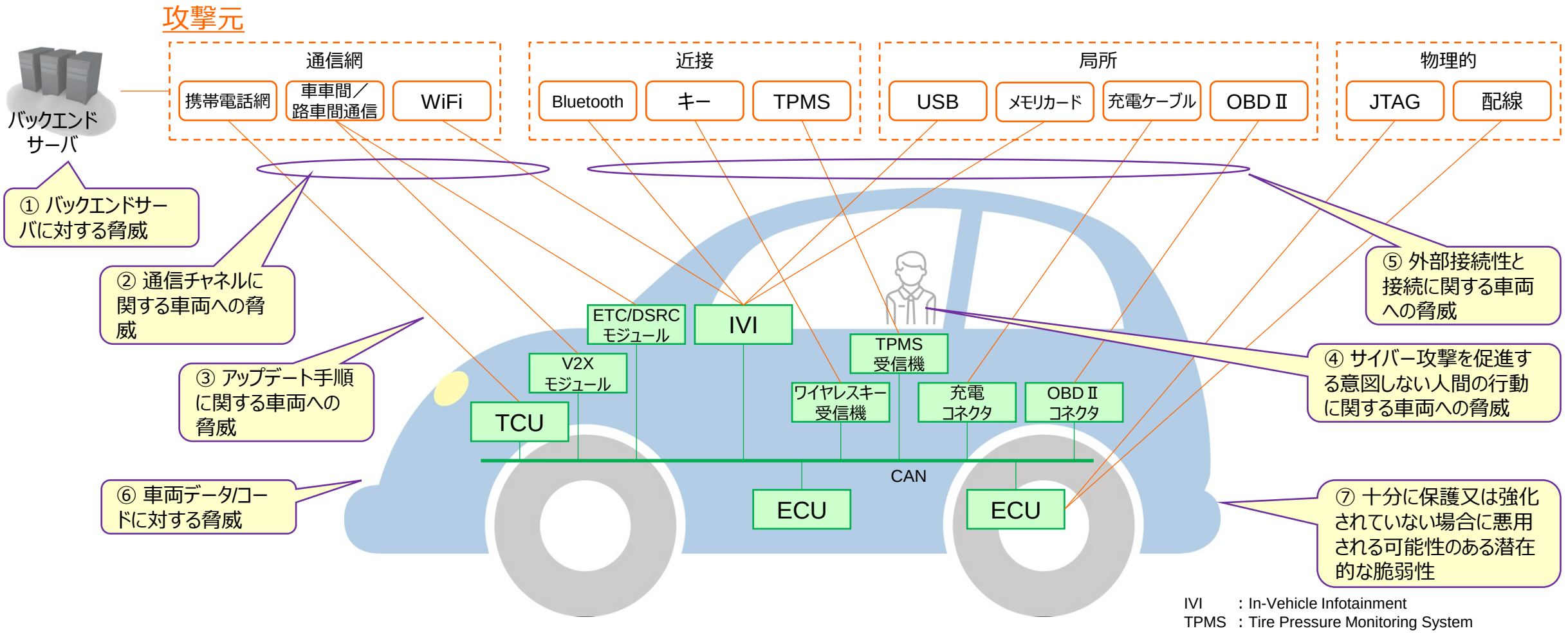
- UN Regulation No.155
  Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system
  サイバーセキュリティ及びサイバーセキュリティマネジメントシステムに関する車両の認可に関する統一規定
  - サイバーセキュリティマネジメントシステムの要件
    - 自動車メーカは、サイバーセキュリティマネジメントシステムの導入を認証当局又はテクニカルサービスに実証すること。
    - 自動車メーカは、サイバーセキュリティマネジメントシステムを確立し、サプライヤとの依存関係を管理すること。
  - 車両型式の要件
    - 認証される車両型式に関連するサイバーセキュリティマネジメントシステムの有効な適合証明書が必要。
    - 車両型式の重要な要素を特定し、リスクアセスメントを行い、特定されたリスクを適切に対応/管理すること。

OEMは、
サイバーセキュリティ対応の開発プロセスと継続的な活動（PSIRT）が必要であり、
さらにサプライヤの管理が必要である。

サプライヤは、
OEMからの要求及び ISO/SAE 21434 に対応し、
サイバーセキュリティマネジメントシステムの確立とサイバーセキュリティ対応開発が必要である。

参照：UN-R155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system，UN/ECE，2021

自動車システムにおける脅威



IVI　：In-Vehicle Infotainment
TPMS　：Tire Pressure Monitoring System

参照：UN-R155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system，UN/ECE，2021

各国法規

- 日本　道路運送車両の保安基準
  - 自動運行装置（自動運転レベル3）搭載の自動車にサイバーセキュリティ確保の要件を追加［2020/4施行］
  - 国連法規（UN-R155, 156）の成立結果を反映［2021/1施行］
- 欧州（EU）法規
  - 欧州委員会でサイバーセキュリティに関する欧州法規が決定　［2020/10/8］
    - REGULATION(EU) 2019/2144
- 米国
  - NHTSA（National Highway Traffic Safety Administration）ガイドライン
    - Cybersecurity Best Practices for the Safety Modern Vehicles
      - 初版：2016/11、Update版：2022/09
- 中国
  - 強制規格（GB）として発布
    - GB 44495　車両サイバーセキュリティの技術要件（UN-R155 相当）
      - 発布：2024/8、施行：2026/1

国際標準　ISO/SAE 21434

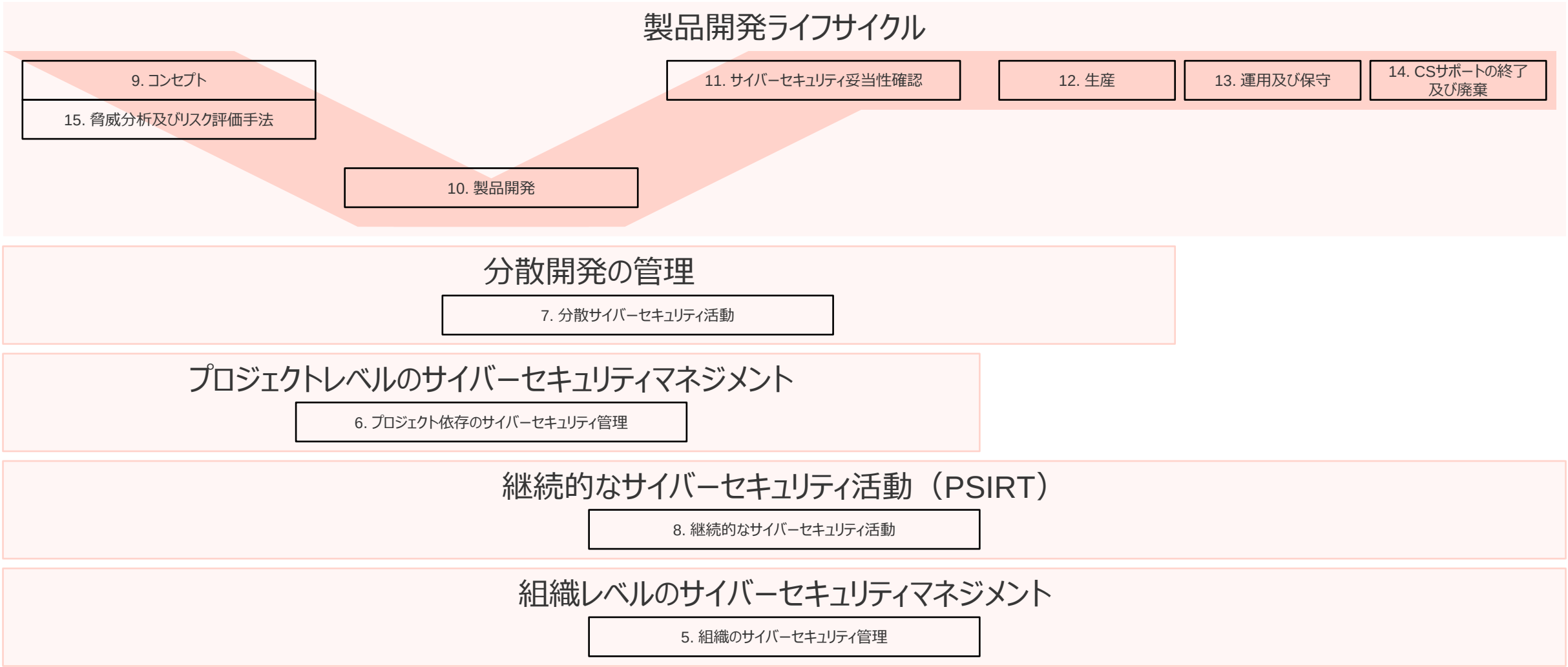
- ISO/SAE 21434:2021
  Road vehicles – Cybersecurity engineering
  自動車 – サイバーセキュリティエンジニアリング
  - 目的
    - 自動車の電気/電子（E/E）システムにおいて、サイバーセキュリティを適切に考慮することで、最先端の技術及び進化する攻撃手法に対応できるようにすること。

      サイバーセキュリティ：　資産が自動車のアイテム、それらの機能、及びそれらの電気/電子コンポーネントに対する脅威シナリオから十分に保護されている状態
    - サイバーセキュリティのリスク管理を含むサイバーセキュリティ管理システム（CSMS）を導入するために使用できる。
  - 適用範囲
    - 自動車の電気/電子システムのコンセプト、製品開発、生産、運用、保守及び廃棄に関するサイバーセキュリティ管理のエンジニアリング要求を規定
    - サイバーセキュリティプロセスの要求並びに、サイバーセキュリティリスクを伝達及び管理するための共通言語を含むフレームワークを定義

OEM/サプライヤは、
ISO/SAE 21434 に準拠したサイバーセキュリティマネジメントシステムを構築・運用する必要がある。

参照：ISO/SAE 21434:2021 Road Vehicles – Cybersecurity engineering，2021

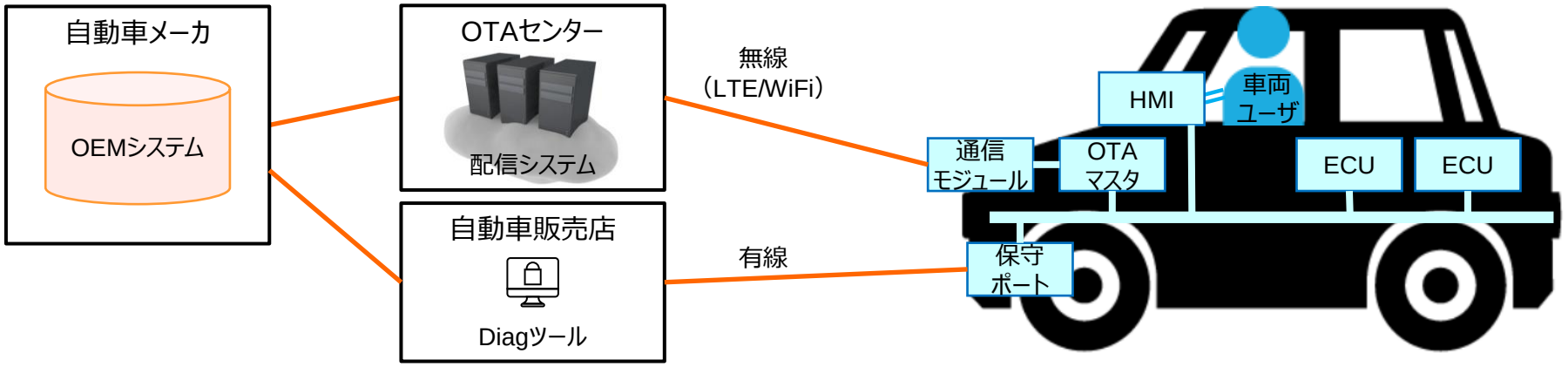
ISO/SAE 21434 の概要



参照：ISO/SAE 21434:2021 Road Vehicles – Cybersecurity engineering，2021

国連法規　UN-R156

- UN Regulation No.156
  Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system
  ソフトウェア更新及びソフトウェア更新マネジメントシステムに関わる車両の承認に関わる統一規定
  - ソフトウェア更新マネジメントシステムの要件
    - 自動車メーカは、ソフトウェア更新マネジメントシステムの導入を認証当局又はテクニカルサービスに実証すること。
    - 自動車メーカは、特定の車両型式に適用される各更新に関する情報を記録及び保存すること。
    - 自動車メーカは、ソフトウェア更新プロセスに関するセキュリティを実証すること。
  - 車両型式の要件
    - ソフトウェア更新の真正性及び完全性を保護すること。



参照：UN-R156 Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system，UN/ECE，2021

国連法規　UN-R156

- UN Regulation No.156
  Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system
  ソフトウェア更新及びソフトウェア更新マネジメントシステムに関わる車両の承認に関わる統一規定
  - ソフトウェア更新マネジメントシステムの要件
    - 自動車メーカは、ソフトウェア更新マネジメントシステムの導入を認証当局又はテクニカルサービスに実証すること。
    - 自動車メーカは、特定の車両型式に適用される各更新に関する情報を記録及び保存すること。
    - 自動車メーカは、ソフトウェア更新プロセスに関するセキュリティを実証すること。
  - 車両型式の要件
    - ソフトウェア更新の真正性及び完全性を保護すること。

OEMは、
ソフトウェア更新のためのマネジメントシステムとソフトウェア更新のセキュリティ対応が必要である。

参照：UN-R156 Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system，UN/ECE，2021

国際標準　ISO 24089

- ISO 24089:2023
  Road vehicles – Software update engineering
  自動車 – ソフトウェア更新エンジニアリング
  - 序文
    - ソフトウェアは、機能を向上させ、自動車の安全及びサイバーセキュリティを維持するために頻繁に更新される。
    - ソフトウェア更新キャンペーンの頻度が増すにつれて、個々の車両構成情報を保持することが重要になる。
  - 適用範囲
    - ソフトウェアの更新が可能な自動車
    - 車両、車両システム、ECU、インフラストラクチャ、ソフトウェア更新パッケージの作成及び展開
    - 自動車のソフトウェア更新エンジニアリングに関わる組織

OEMは、
ソフトウェア更新マネジメントシステムを構築・運用する必要がある。

サプライヤは、
OEMからの要求及び ISO 24089 に対応し、ソフトウェア更新に対応できる必要がある。

参照：ISO 24089:2023 Road Vehicles – Software update engineering，2023

目次

- サイバーセキュリティに関する動向
- **サイバーセキュリティに関する法規・標準**
  - 自動車サイバーセキュリティ、ソフトウェアアップデート
  - **工場セキュリティ**
- サイバーセキュリティへの対応

IATF 16949

- IATF 16949:2016
  自動車産業の生産部品及び関連するサービス部品の組織に対する品質マネジメントシステム要求事項
  - ランサムウェアなどのサイバー攻撃の状況をふまえ、公式解釈集（Sanctioned Interpretations）によりサイバーセキュリティへの対応が追加されている。

6.1 リスク及び機会への取組み

6.1.2.1 リスク分析

組織は、そのリスク分析において、少なくとも次を含めなければならない。

a) 製品リコール、製品検査、フィールドからの返品・修理、クレーム、スクラップ、及び再処理、から学んだ教訓

b) 情報技術システムに対するサイバー攻撃の脅威

6.1.2.3 緊急事態対応計画

組織は、次の事項を実施しなければならない。

a) 顧客要求事項が満たされることを確実にし、及び生産からのアウトプットを維持するのに不可欠なすべての製造工程及びインフラストラクチャの設備に対する内部及び外部のリスクを特定し評価する。

b) （省略）

c) 次のような事態において、供給の継続のために緊急事態対応計画を準備する。ただし、これらだけに限定されるものではない。
主要設備の故障、外部から提供される製品、プロセス、及びサービスの中断、繰り返し発生する自然災害、火事、パンデミック、電気・ガス・水道の停止、情報技術システムに対するサイバー攻撃、労働力不足、又はインフラストラクチャ障害

d) （省略）

e) 緊急事態対応計画の有効性のテストを定期的に行うこと。サイバーセキュリティに関して：テストには、サイバー攻撃のシミュレーション、特定の脅威に対する定期的監視、依存関係の特定、及び脆弱性の優先順位付けが含まれ得る。このテストは、関連する顧客操業中断リスクに見合ったものとする。

f) （以下省略）

参照：IATF 16949 Quality management system requirement for automotive production and relevant service parts organizations．2016
IATF 16949:2016 – Sanctioned Interpretations

IEC 62443-2-1

- IEC 62443-2-1:2024
  産業用オートメーション及び制御システムのセキュリティ
  – IACSアセットオーナーのためのセキュリティプログラム要求事項
    - 概要
      - 産業用オートメーション及び制御システム（Industrial Automation and Control Systems：IACS）には、COTS（汎用品）などざまざまな機器が導入され、サイバー攻撃にさらされるようになってきている。
      - サイバーセキュリティという用語は、コンピュータ又はコンピュータシステムを認可されていないアクセス又は攻撃から保護するために取られる一連のセキュリティ対策又は実践を表すために使用される。IACSでは、要求される時間枠で正しい機能を実行しない結果となる望まれないアクセス又は攻撃を含む。
    - 範囲
      - IACSのアセットオーナーのためのセキュリティプログラムのポリシー及び手順の要求事項を規定している。
      - IACSセキュリティプログラムの要素は、IACSのセキュアな運用に適用される、要求されるセキュリティ能力を定義している。

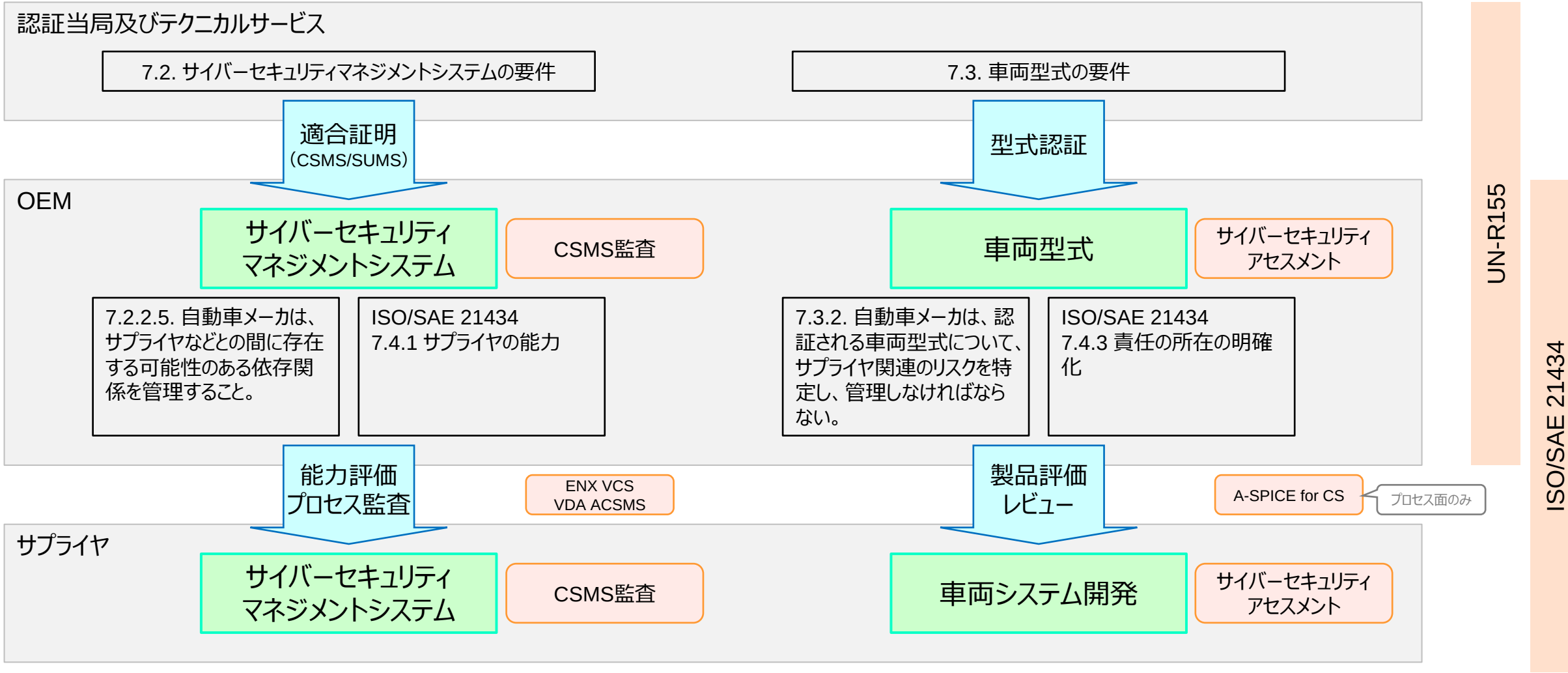
OEM/サプライヤは、
生産プロセスのサイバーセキュリティマネジメントシステムを構築・運用する必要がある。
（ISO/SAE 21434 では、IEC 62443-2-1 を例示している。）

参照：IEC 62443-2-1 Establishing an industrial automation and control system security program，2024

目次

- サイバーセキュリティに関する動向
- サイバーセキュリティに関する法規・標準
- サイバーセキュリティへの対応
  - 自動車のサプライチェーンを構成する各社に対する要求
  - サイバーセキュリティマネジメントシステムの構築
  - サイバーセキュリティに対応した開発
  - SIRT（Security Incident Response Team）

自動車のサプライチェーンを構成する各社に対する要求（OEMとサプライヤの関係）



参照：UN-R155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system，UN/ECE，2021

自動車のサプライチェーンを構成する各社に対する要求

- 自動車のサプライチェーンを構成するOEM、サプライヤ、部品メーカに対し、以下のような活動が必要となる。

	OEM	サプライヤ	部品メーカ（汎用品）
サイバーセキュリティマネジメントシステム（CSMS）の構築/監査	• CSMSの構築 • プロセス認証 （当局からの適合証明）	• CSMSの構築 • CSMS監査 （内部、顧客、第三者）	• CSMSの構築 • CSMS監査 （内部、第三者）
サイバーセキュリティに対応した開発	アイテム開発 • 脅威分析及びリスク評価 • セキュリティテスト • サイバーセキュリティアセスメント • 妥当性評価	コンポーネント開発 • 脅威分析及びリスク評価 • 脆弱性分析 • セキュリティテスト • サイバーセキュリティアセスメント	コンテキスト外コンポーネント開発 • 脅威分析及びリスク評価 • 脆弱性分析 • セキュリティテスト • サイバーセキュリティアセスメント （製品認証）
インシデントに対応する組織体制の構築	• PSIRT	• PSIRT	• PSIRT

目次

- サイバーセキュリティに関する動向
- サイバーセキュリティに関する法規・標準
- **サイバーセキュリティへの対応**
  - 自動車のサプライチェーンを構成する各社に対する要求
  - **サイバーセキュリティマネジメントシステムの構築／監査**
  - サイバーセキュリティに対応した開発
  - インシデントに対応するサイバーセキュリティ体制の構築

サイバーセキュリティマネジメントシステムの構築

プロセス構築
チーム

開発プロジェクト

サイバーセキュリティマネジメントシステム

規定・基準
- サイバーセキュリティ管理規程
- サイバーセキュリティプロジェクト管理基準

など

ガイドライン・手法
- 脅威分析ガイドライン
- 脆弱性分析ガイドライン

など

テンプレート

プロジェクト作業成果物

- サイバーセキュリティ計画書
- 再利用分析報告書
- サイバーセキュリティインタフェース合意書
- TARA報告書
- サイバーセキュリティコンセプト
- サイバーセキュリティ仕様
- 脆弱性分析報告書
- ソースコード静的検証報告書
- セキュリティテスト報告書

など

監査員

アセッサ

PSIRT

工場

サイバーセキュリティ監査報告書	サイバーセキュリティアセスメント報告書

継続的なサイバーセキュリティ活動

生産プロセスのサイバーセキュリティマネジメントシステム

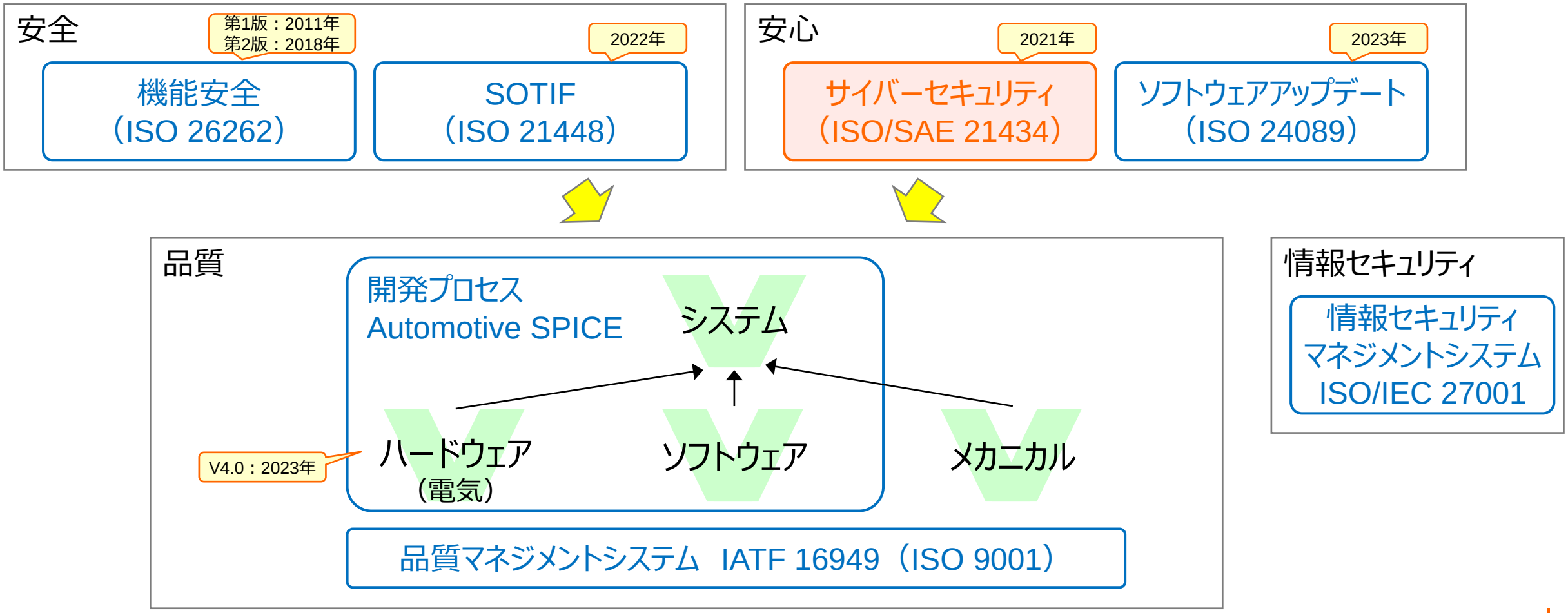
- コントロールプラン

関連/相互作用するシステム

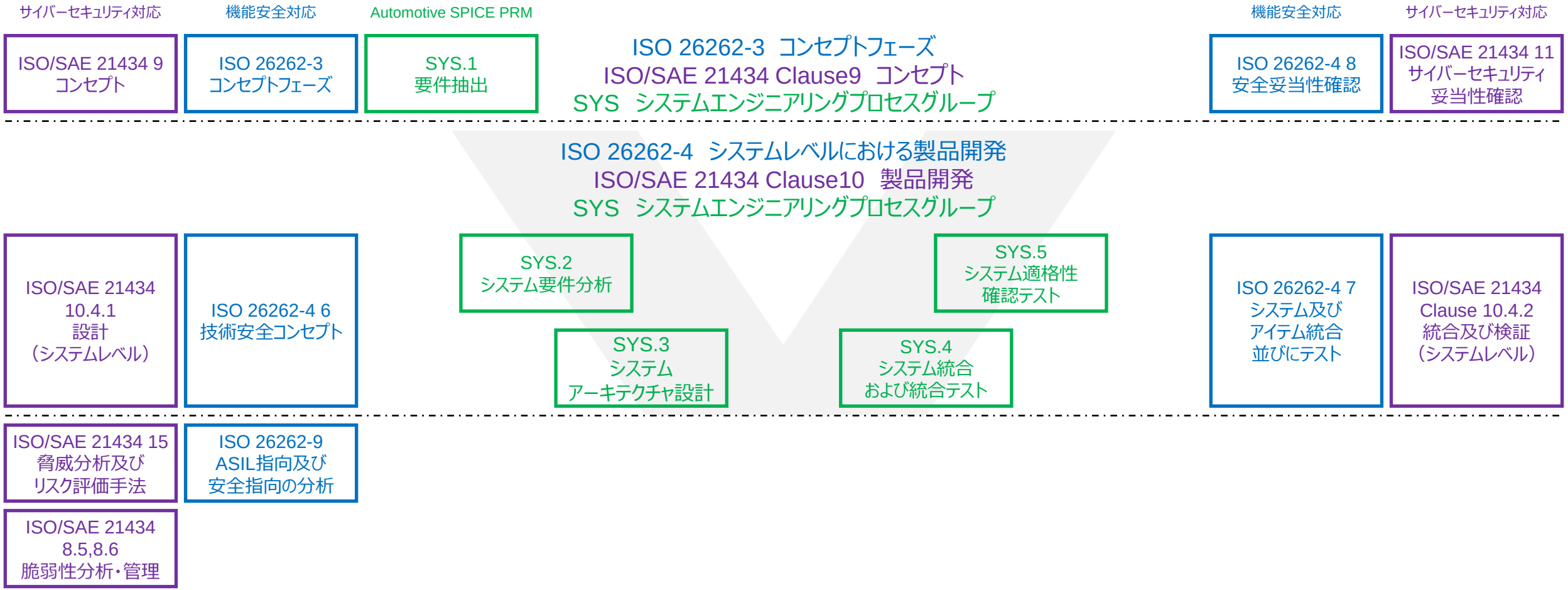
品質マネジメントシステム（QMS）	機能安全プロセス	情報セキュリティマネジメントシステム（ISMS）

サイバーセキュリティマネジメントシステムの構築　（プロセスの統合）

- 最終的な製品/システムは、さまざまな法規・標準の要求すべてを満たしたものとなる。



サイバーセキュリティマネジメントシステムの構築（コンセプト／システムレベルの開発の例）



- 車載品質を確保する開発プロセスの基盤の上に、機能安全対応、サイバーセキュリティ対応が必要となる。
- 規格・標準の個別要件に対応した基準・ガイドラインが必要となる。

サイバーセキュリティマネジメントシステムの監査

- サイバーセキュリティマネジメントシステムの監査（組織のサイバーセキュリティ監査）
  - UN-R155　　認証当局は、自動車メーカがCSMSを導入していることを確認し、評価する。
  - ISO/SAE 21434　　組織のプロセスが、ISO/SAE 21434 の目的を達成しているかどうかを独立して判断する。
    - 監査基準の例
      - ISO/PAS 5112 Road vehicles — Guidelines for auditing cybersecurity engineering

        ISO 19011（マネジメントシステム監査のための指針）の指針に加えて、サプライチェーン全体にわたる自動車のサイバーセキュリティの達成に寄与する組織に対するCSMS監査のガイドライン
      - ENX Vehicle Cyber Security Audit (ENX VCS)

        ISO/SAE 21434 に従って CSMS を実装していることを、ISO/PAS 5112 に従って実証
    - 監査主体
      - 内部監査（自社監査）

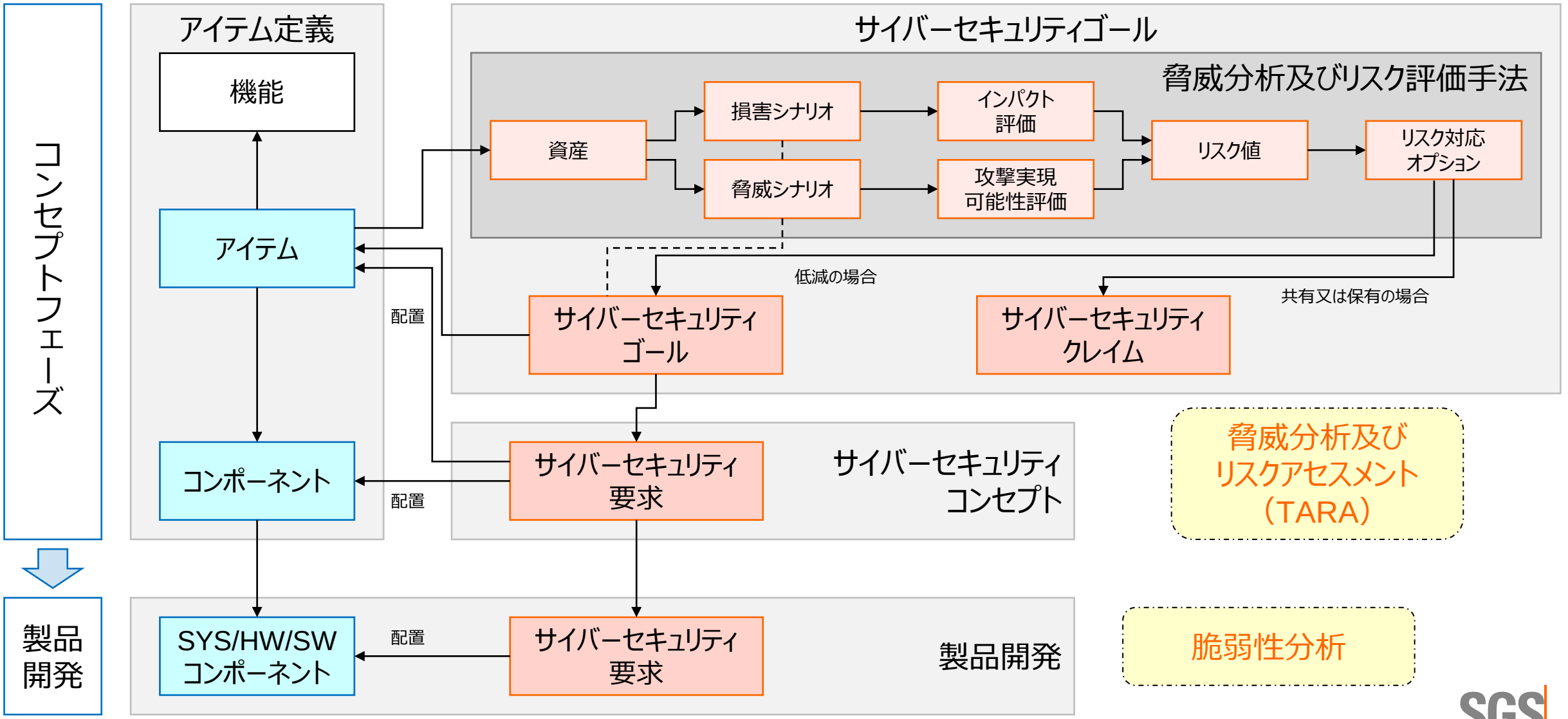
        弊社サービス：CS監査演習（トレーニング）、CS監査支援サービス
      - 顧客監査（第二者監査）
      - 第三者監査

        弊社サービス：SGS- TÜVプロセス認証、CSMS監査（適合性確認）、ENX VCS監査

目次

- サイバーセキュリティに関する動向
- サイバーセキュリティに関する法規・標準
- **サイバーセキュリティへの対応**
  - 自動車のサプライチェーンを構成する各社に対する要求
  - サイバーセキュリティマネジメントシステムの構築
  - **サイバーセキュリティに対応した開発**
  - インシデントに対応するサイバーセキュリティ体制の構築

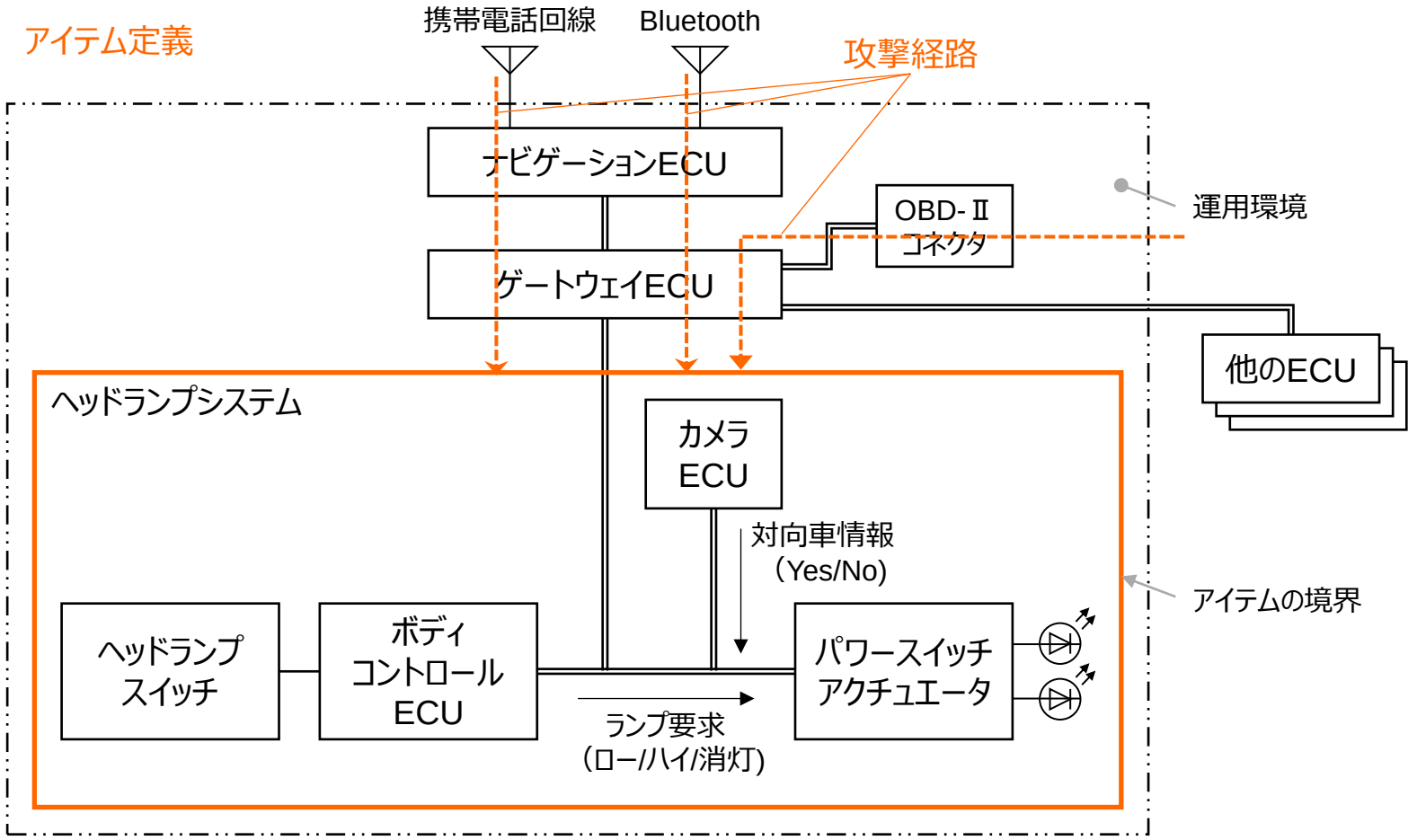
サイバーセキュリティに対応した開発



参照：ISO/SAE 21434:2021　自動車 – サイバーセキュリティエンジニアリング

サイバーセキュリティに対応した開発　（脅威分析及びリスクアセスメント）

- ヘッドランプシステムの例



損害シナリオ

中速での夜間の運転中にヘッドランプが意図せずに消灯することによって引き起こされる、小幅な静止物との前面衝突。

脅威シナリオ

信号をなりすますことによって、パワースイッチアクチュエータECUへの“ランプ要求”信号のデータ通信の完全性が損失し、ヘッドランプが意図せずに消灯する可能性がある。

リスク評価

サイバーセキュリティゴール

“ランプ要求”信号のデータ通信の完全性を、なりすましから保護すること。

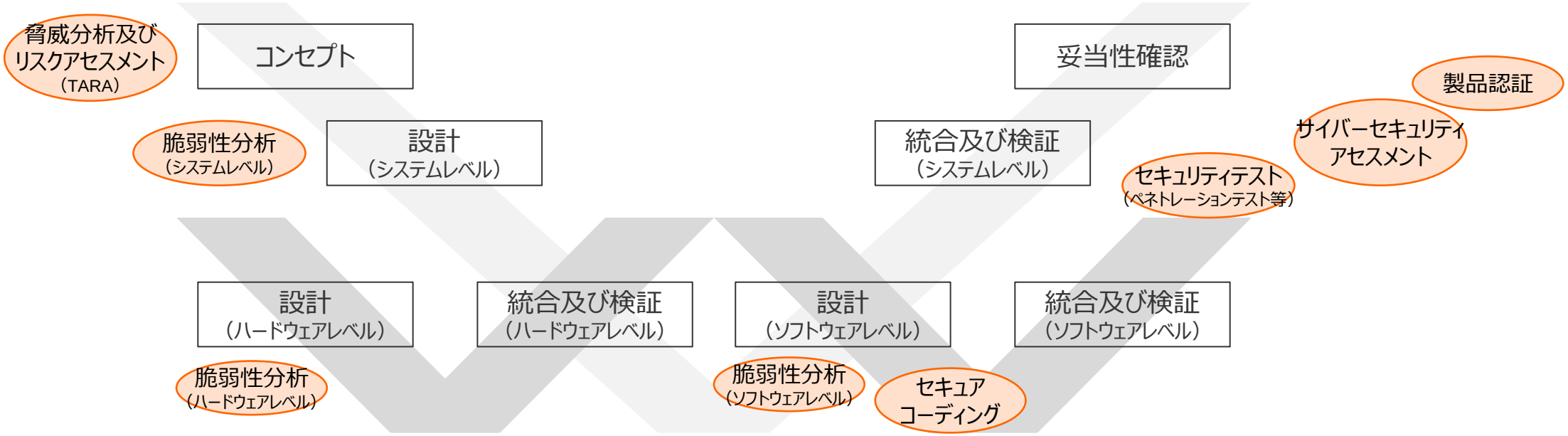
サイバーセキュリティ要求

“ランプ要求”信号にメッセージ認証を適用する。

参照：ISO/SAE 21434:2021　自動車－サイバーセキュリティエンジニアリング　附属書H

サイバーセキュリティに対応した開発

- サイバーセキュリティコントロール（技術的/運用上のセキュリティリスク対応方策）の適用



- 弊社サービス
  - TARA/脆弱性分析演習（トレーニング）、TARA支援サービス
  - CSアセスメント演習（トレーニング）、CSアセスメント支援
  - SGS- TÜV製品認証、Automotive SPICE for CSアセスメント

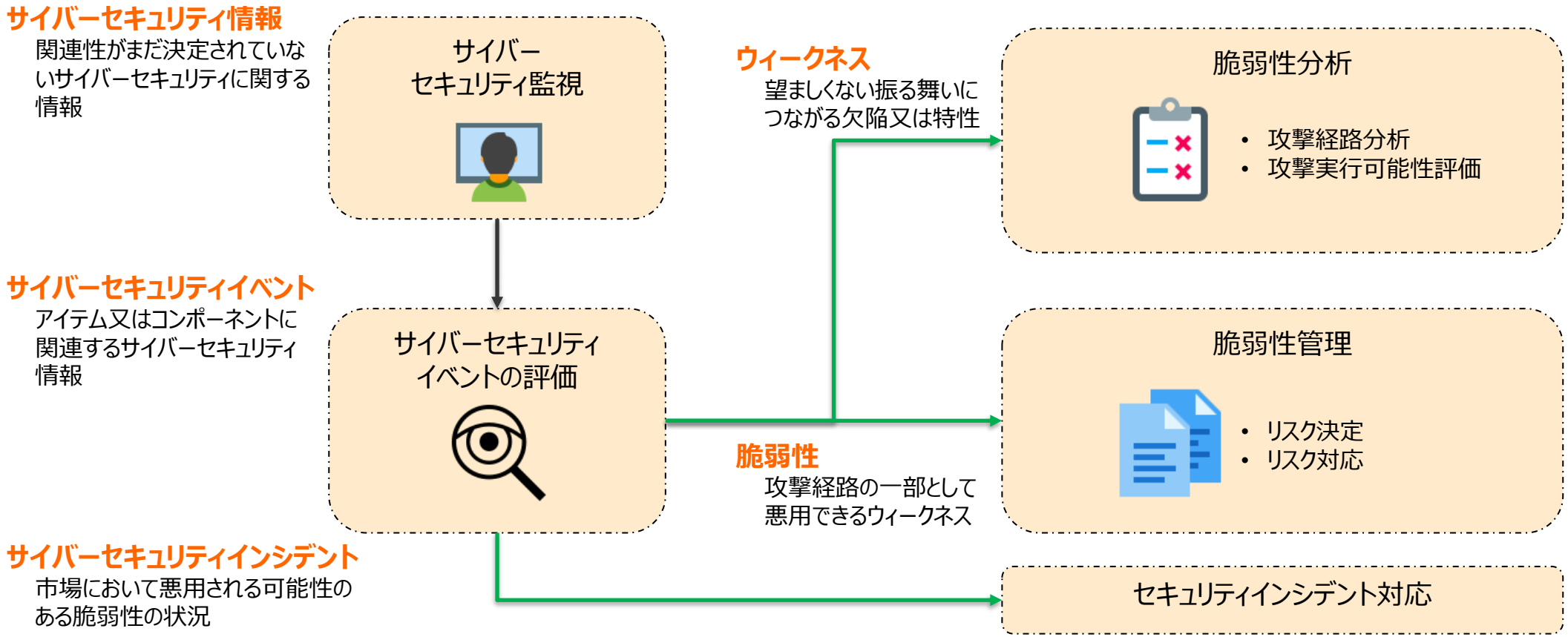
VicOne様ソリューション
- TARA
- ペネトレーションテスト
- 教育・トレーニング

目次

- サイバーセキュリティに関する動向
- サイバーセキュリティに関する法規・標準
- **サイバーセキュリティへの対応**
  - 自動車のサプライチェーンを構成する各社に対する要求
  - サイバーセキュリティマネジメントシステムの構築
  - サイバーセキュリティに対応した開発
  - **インシデントに対応するサイバーセキュリティ体制の構築**

インシデントに対応するサイバーセキュリティ体制の構築

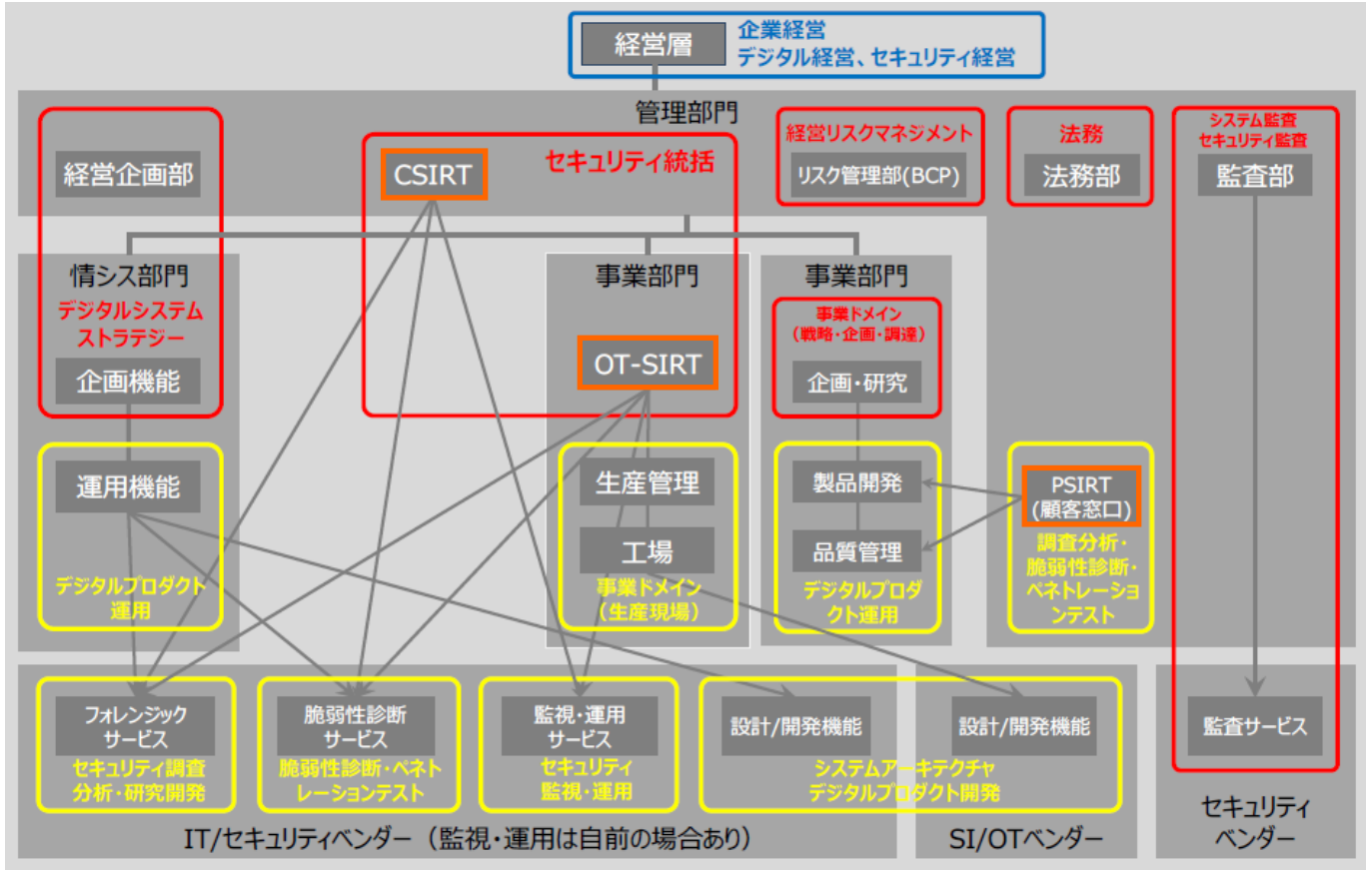
- PSIRT（Product Security Incident Response Team）を組織し、継続的にサイバーセキュリティ管理を行う必要がある。



参照：ISO/SAE 21434:2021　自動車 – サイバーセキュリティエンジニアリング

インシデントに対応するサイバーセキュリティ体制の構築

- CSIRT（Computer Security Incident Response Team）
  - 組織内で利用する情報システムやネットワークにおいて発生するインシデントに対応を行う機能
- PSIRT（Product Security Incident Response Team）
  - 顧客に販売された製品において発生が懸念されるインシデントに対応する機能
- OT-SIRT（Operational Technology - Security Incident Response Team）
  FSIRT（Factory Security Incident Response Team）
  - 制御系設備の運用において発生するインシデントに対応する機能
- SOC（Security Operation Center）
  - 監視や検知に関する機能



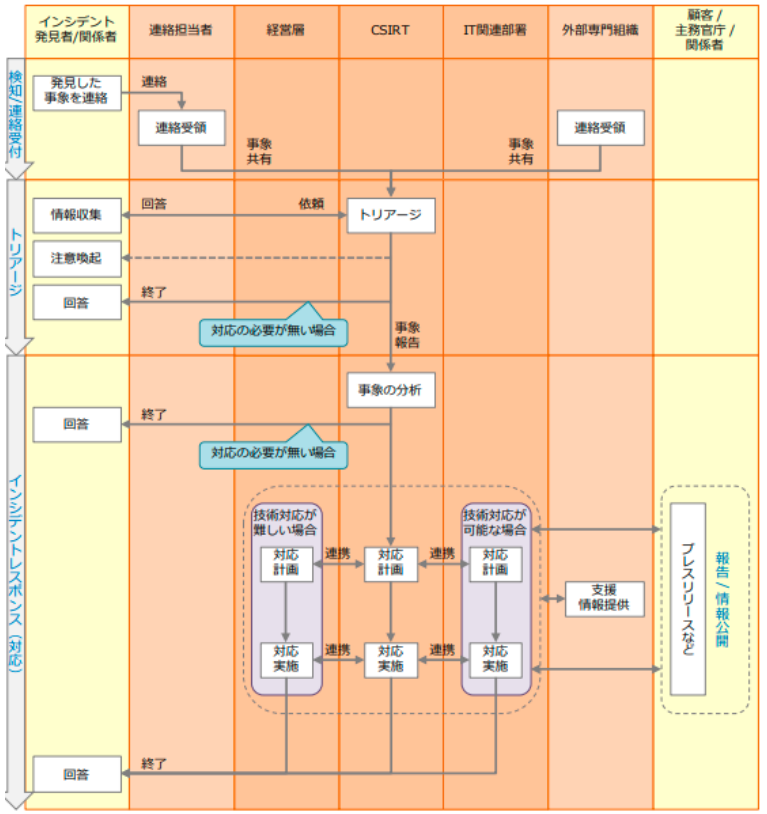
サイバーセキュリティ体制と分野のマッピング例：製造業

参照：サイバーセキュリティ体制構築・人材確保の手引き 第2版，経済産業省/IPA，2022

インシデントに対応するサイバーセキュリティ体制の構築

- 継続的なサイバーセキュリティ活動及びサイバーセキュリティインシデント対応のワークフロー
  - サプライチェーン全体としてのワークフローが必要となる。
  - 弊社サービス
    - PSIRT演習（トレーニング）

CSIRTのワークフロー例



参照：インシデントハンドリングマニュアル，JPCERT/CC，2021

VicOne様ソリューション
- SBOM生成及び脆弱性の調査・発見・分析ツール
- In CarからOut Carまで幅広いセキュリティソリューション
- 自動車に特化した脅威インテリジェンスサービス
- 車載器からクラウドプラットフォーム、モバイルまで対応可能なペネトレーションテスト

Thank you!

Do you have any questions?

jp.fsafety@sgs.com

050-1780-7876

http://safety-testing.jp/sgs/

（参考）自動車サイバーセキュリティ対応のロードマップ

フェーズ１
全体方針と実施体制の確立

（1～2カ月）

フェーズ2
プロセス構築
プロジェクトでの試行
（6～12カ月）

フェーズ３
プロセス確立（正式化）
プロジェクト適用
PSIRT運用

基礎
トレーニング

ギャップ分析

中級
トレーニング

監査
（準拠性確認）

プロセス構築

プロジェクトでの試行

プロセス改善

プロジェクト適用

トレーニングプログラム

（参考）自動車サイバーセキュリティ適用支援サービス

- 当社では様々なトレーニング及びワークショップを実施し、自動車サイバーセキュリティ適用の支援をしています。

トレーニング

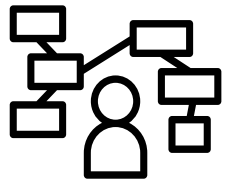
- SGS-TÜV認定コース（CACSP）
- 領域別トレーニング

現状分析

- 社内体制構築
- ギャップ分析

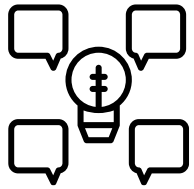
プロセス構築

- プロセス構築支援
  - 構築主体
  - レビュー主体
- プロセス改善支援



プロジェクト適用

- TARA作成支援
- 成果物レビュー
- 成果物作成支援
- ペネトレーションテスト
- PSIRT支援



技術支援ワークショップ

- Q&A対応
- 個別テーマ支援

アセスメント

- プロセス監査（準拠性確認）
- プロセス認証支援
- アセスメント支援
- 製品認証支援