DENSO
Crafting the Core

CASEに向けたサイバーセキュリティの取り組み

2022年9月

平永敬一郎

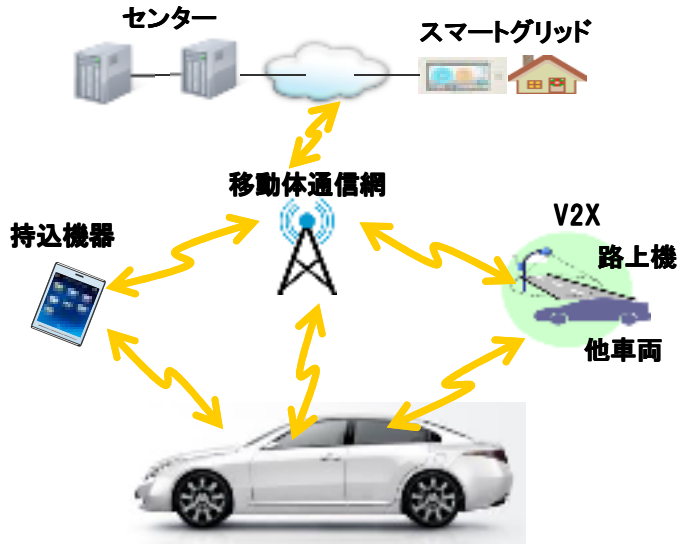
情報セキュリティ推進部
製品セキュリティ室
keiichiro.hiranaga.j2g@jp.denso.com

目 次

環境変化と自動車業界の動向

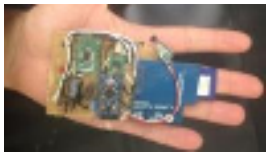
クルマとセキュリティの現状

正の面
車外環境とつながり、より安全・便利に



新しいモビリティ社会に

負の面
様々な攻撃事例報告



ドイツ自動車協会
（ADAC）

DEF CON 23!

出展：Wired.com

Recall

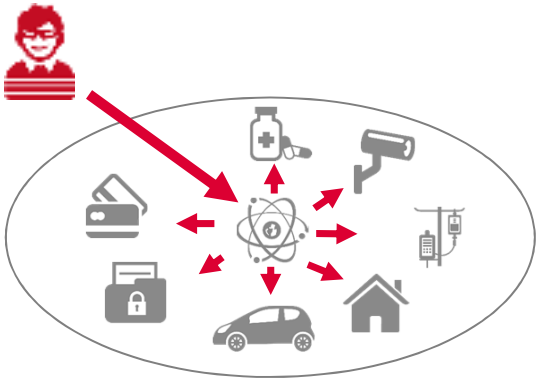
背景～サイバー攻撃のリスク～

- 攻撃対象となる金銭/安全/プライバシーに関わる**資産**がつながる時代（Connected）に
- 攻撃対象が**ネットワークに接続**されていることにより、攻撃の機会が増大
- 攻撃者は**脆弱性**を悪用し攻撃

サイバー攻撃リスクの高まり

攻撃の動機

- 金銭/安全/プライバシーに関わる資産がネットワークにつながっている



×

攻撃機会の増大

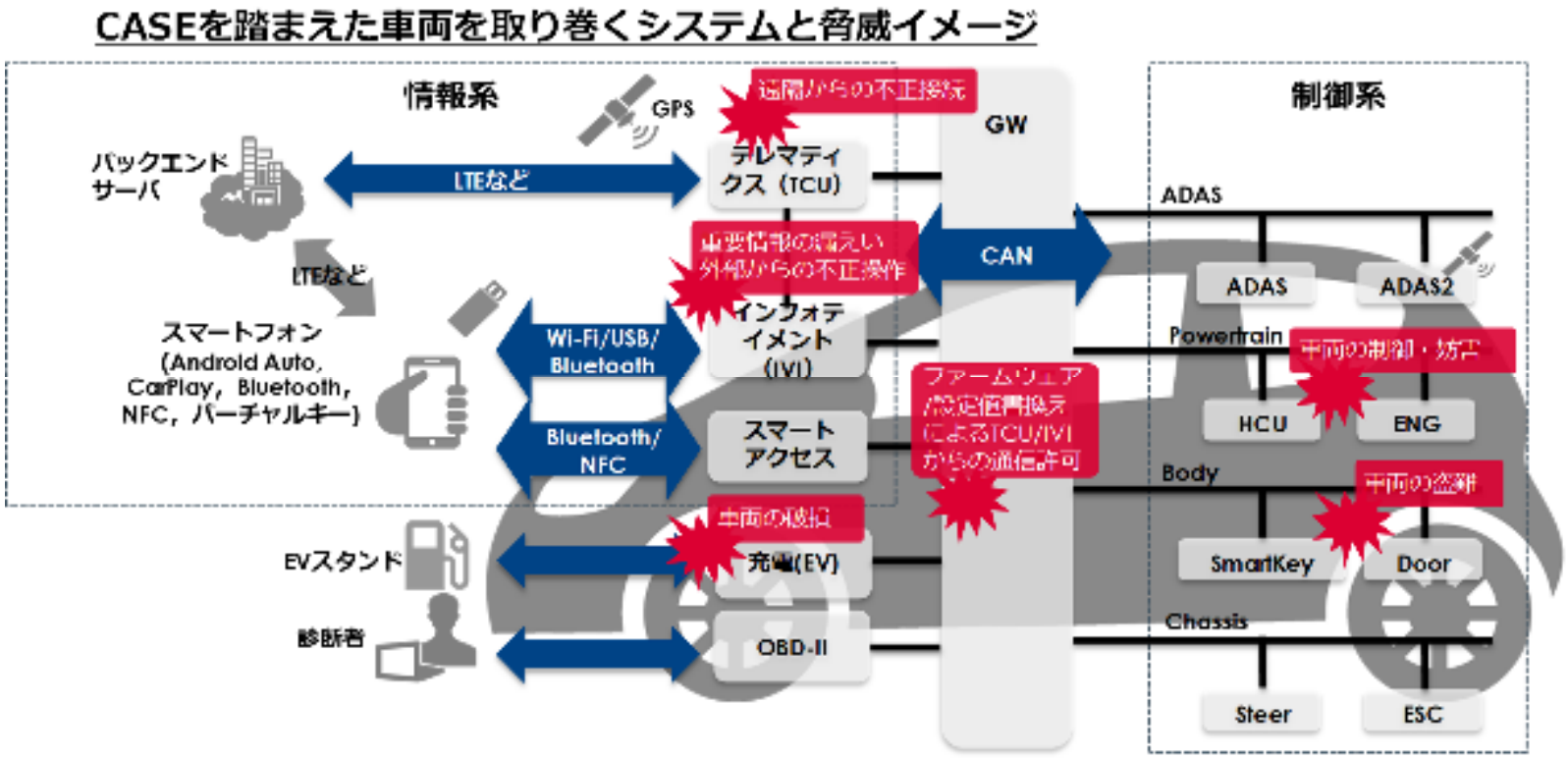
- 常時ネットワーク接続
- 無線通信の利用

攻撃技術の進歩

- ネットワーク構成の脆弱性調査
- 通信プロトコルの脆弱性調査
- コードの解析
- OSSの脆弱性調査
- 認証方式の脆弱性調査
- 鍵情報の漏洩

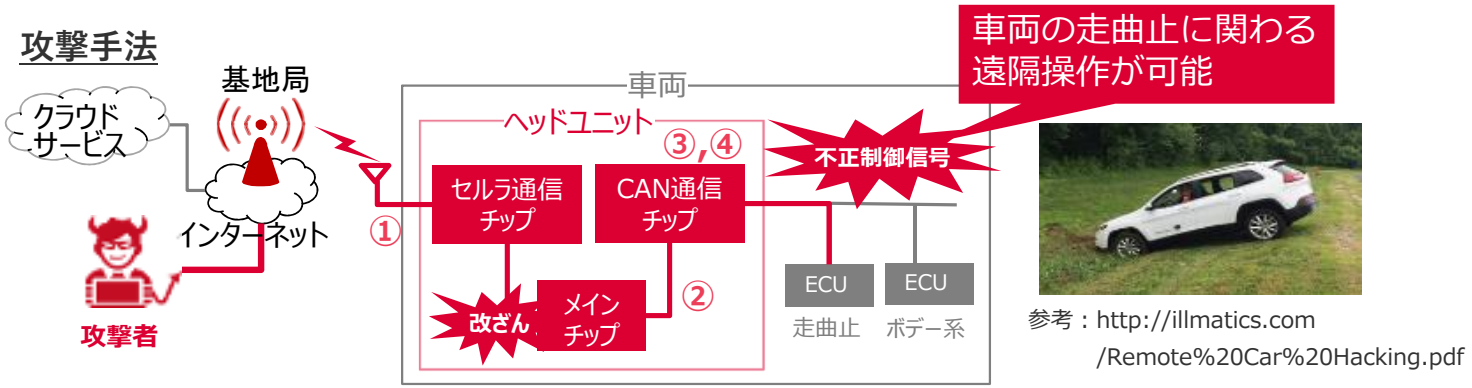
背景 ～CASEを踏まえた車両セキュリティへの脅威～

- 車両においても、スマホやパソコンと同様に対策を行う必要がある
  遠隔からの攻撃の可能性があるリスクについては特に注意が必要



遠隔からのハッキング成功事例報告

- 2015年7月、**サイバー攻撃によりクルマを遠隔操作できる**ことを米国のセキュリティ研究者が発表した
  - ✓ 不特定多数の同一車種への攻撃が可能だったと報告された
  - ✓ メーカはリコールを実施し、自動車業界にインパクトを与えた



参考：http://illmatics.com
/Remote%20Car%20Hacking.pdf

関連脆弱性	
①	セルラ回線経由でヘッドユニットにtelnet接続可能
②	ヘッドユニットが更新モードで起動した際に、CAN通信チップのファームウェアを遠隔で更新可能にできる
③	CAN通信チップのファームウェアをリバースエンジニアリングすることにより、CANメッセージを生成する機能を特定可能
④	CAN通信チップのファームウェアのセキュアブート(完全性チェック)を回避可能

車両サイバーセキュリティに関わる法規と国際規格

- 国連法規（UNR155）　21年1月 発効　(日本・欧州は22年7月新型車施行)
- 国際規格（ISO/SAE21434）　21年8月発行済み
- **国内法規**　**22年7月 OTA*有り新型車適用開始済み**

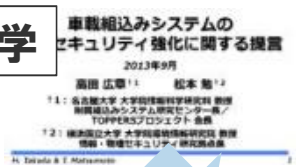
		FY2017		FY2019	FY2020	FY2021	FY2022
法規	UNR155	▼11月法規化決定			**▽6月 採択** **▽1月 発効**		**▽7月 EU新型車適用**
法規	国内法			▽5月 公布	**▽４月施行 自動運転車**		**▽7月 OTA有新型車適用**
標準	ISO/SAE 21434	▽5月WD Working Draft		2月12日▽ DIS発行		**▽8月 発行**	

*OTA：Over The Air

国内の標準化組織

- 法規・標準に対しては業界3団体で連携した活動を推進中

大学



国プロ　内閣府　SIP
総務省
経産省

JAMA 一般社団法人 日本自動車工業会

司令塔

・基本方針
・前提条件
・相場観（対策・評価）

公益社団法人 自動車技術会

標準開発プロセス

・脅威分析手法
・リスク評価手法

⇒JASO　テクニカルペーパを発行

JasPar

標準技術・評価

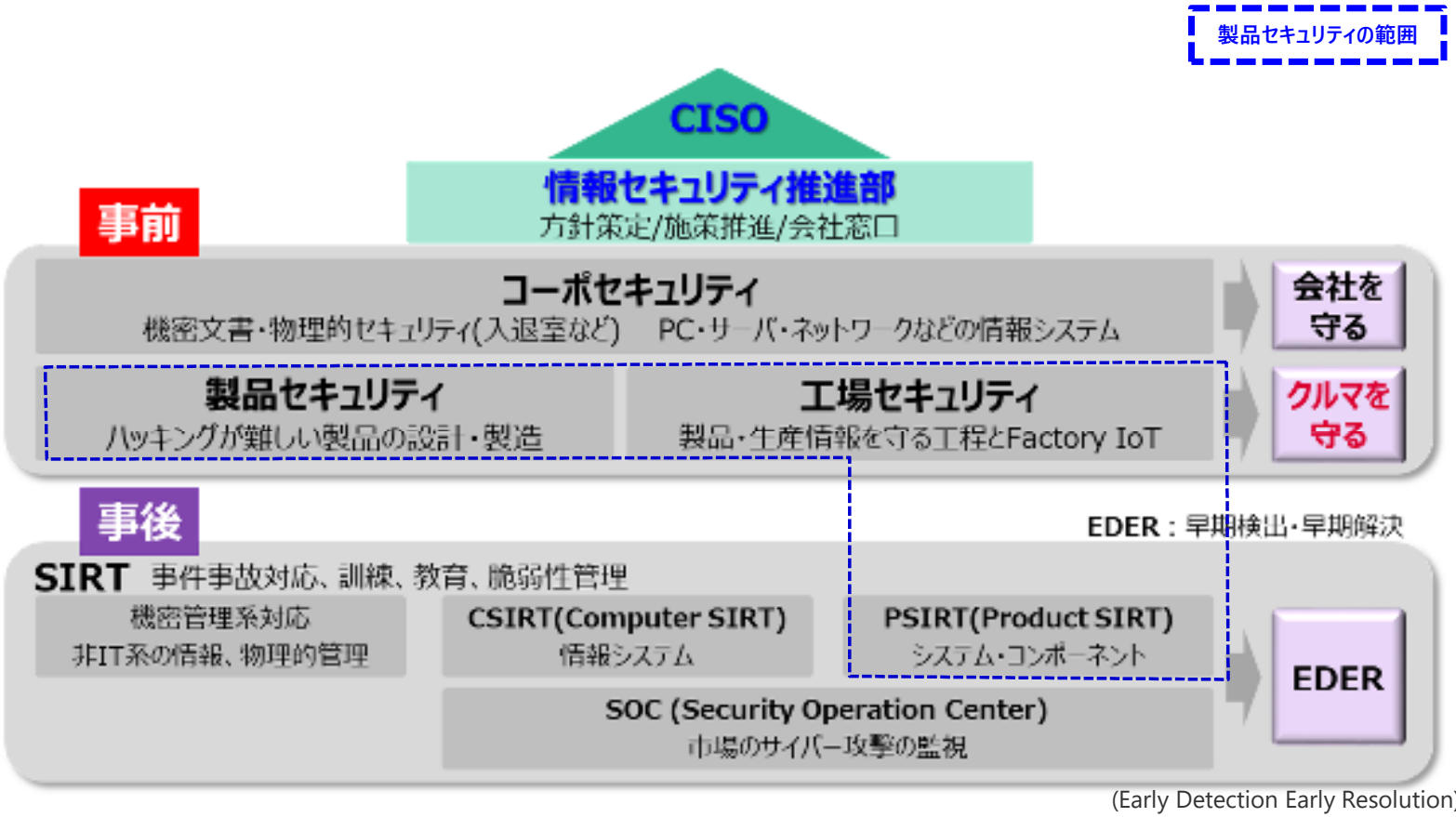
・メッセージ認証
・鍵管理
・脆弱性評価

⇒技術解説書/要件定義書の発行

II

デンソーのセキュリティ推進体制

組織：デンソーの製品セキュリティ体制

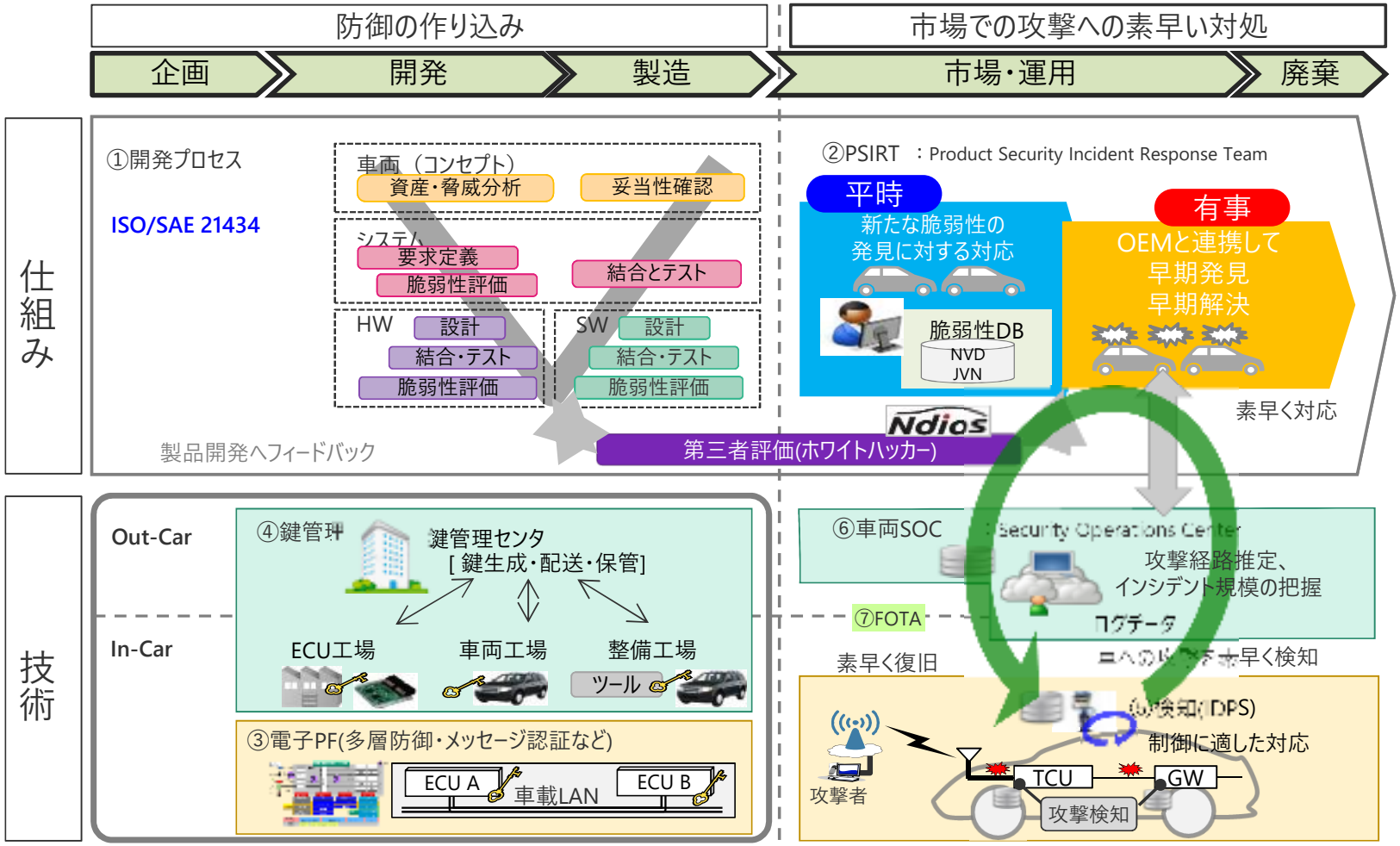


(Early Detection Early Resolution)

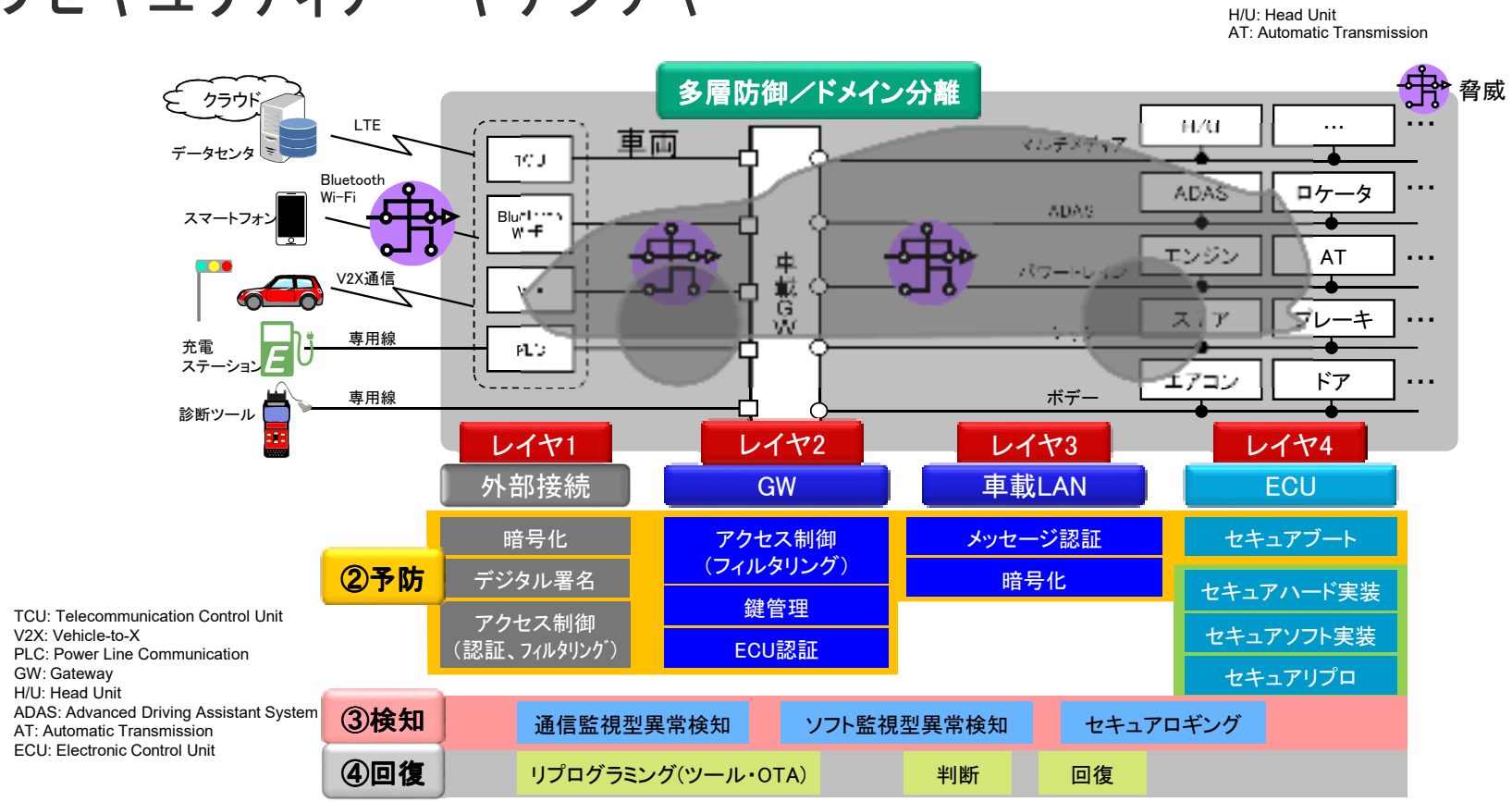
製品セキュリティはCISOの元、デンソーグループのガバナンスとして推進

クルマ＆工場サイバーセキュリティ

モビリティ社会のセキュリティ推進活動全体像



クルマのセキュリティアーキテクチャ

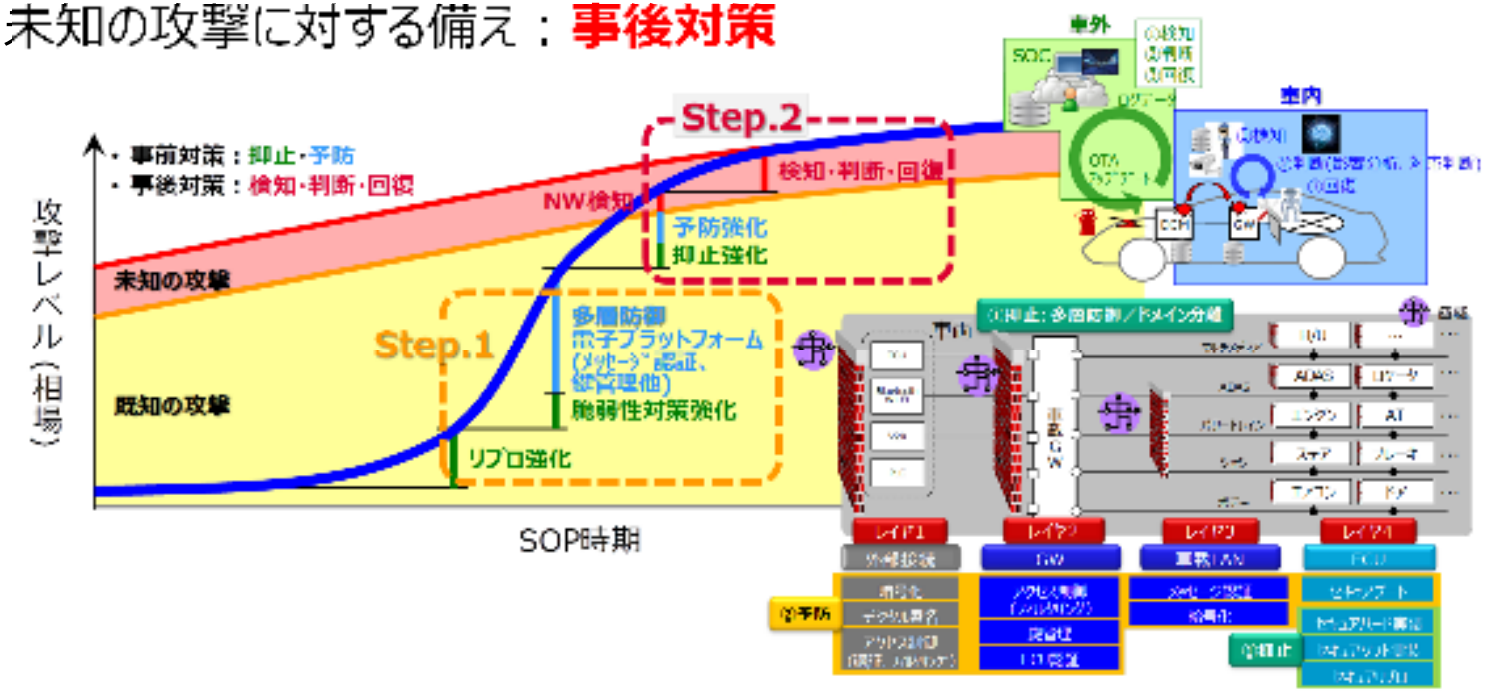


TCU: Telecommunication Control Unit
V2X: Vehicle-to-X
PLC: Power Line Communication
GW: Gateway
H/U: Head Unit
ADAS: Advanced Driving Assistant System
AT: Automatic Transmission
ECU: Electronic Control Unit

守るべき対象(保護資産)に対して適切な技術を最適配置

セキュリティ技術の対応方針

- 想定攻撃 と 対応方針
  - ✓ ステップ1　既知の攻撃に対する備え：多層防御をベースに**事前対策と未然防止**
  - ✓ ステップ2　未知の攻撃に対する備え：**事後対策**



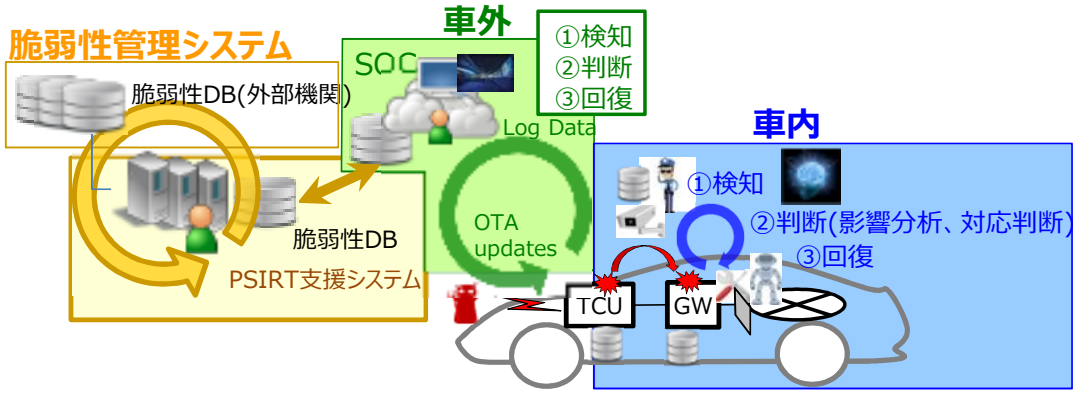
将来サービスと想定脅威を踏まえて、段階的にセキュリティレベルを向上

事後対策

- **サイバー攻撃(未知の攻撃含む)**による機能不全に備えて、
  クルマおよびモビリティ社会全体を検知・判断・回復することで**安全・安心を提供**する

【事後対策のステップ】

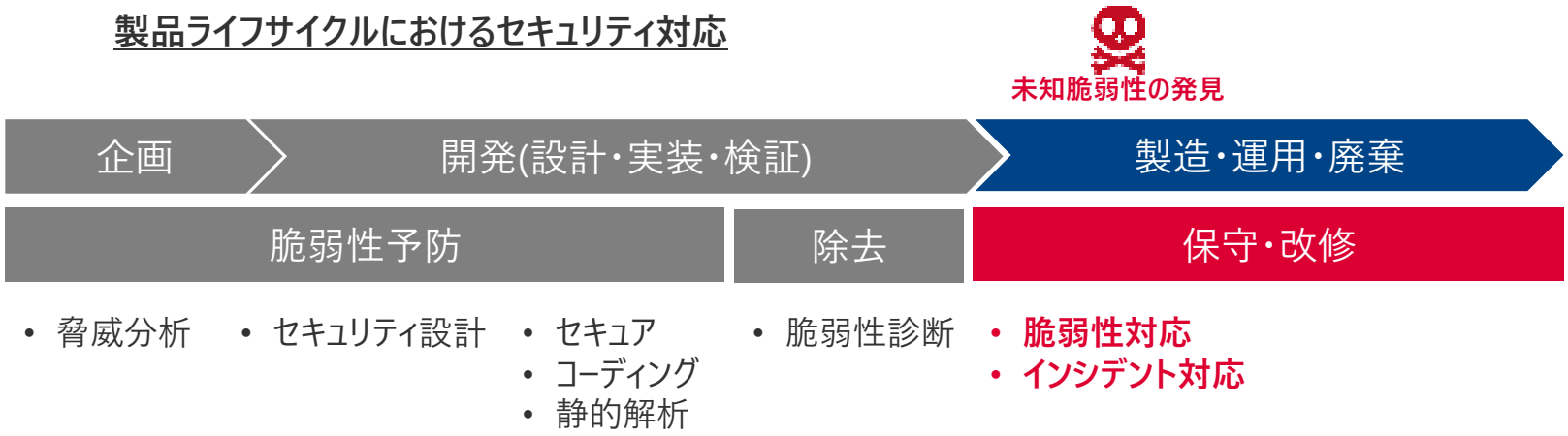
① 【検知】攻撃の予兆、攻撃、侵入などの異常を検知する
② 【判断】影響を分析し、対応を判断する
③ 【回復】攻撃の影響を軽減/排除し、機能回復する



車両の内部・外部の両面から安心の見える化と見守りをする

PSIRTの役割

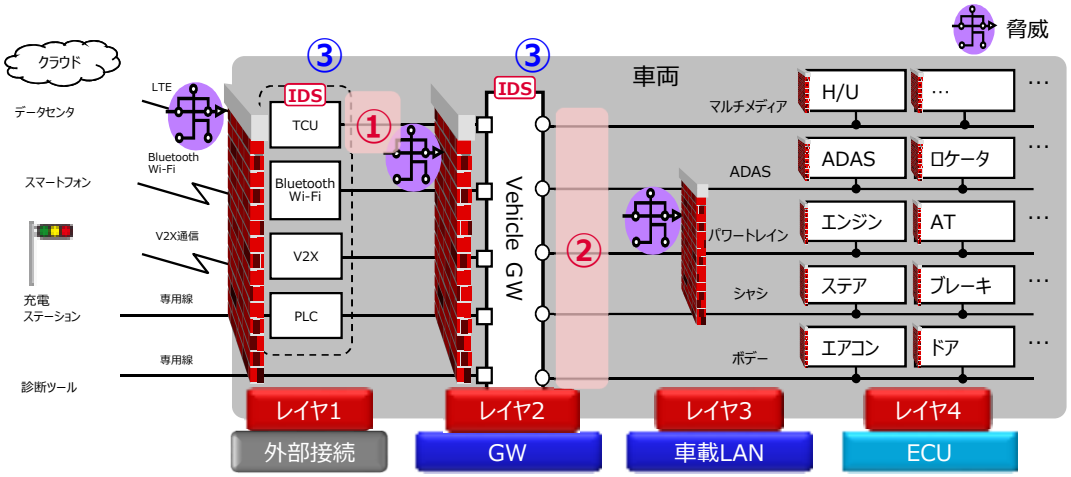
- セキュリティでは、一般品質対応と以下の点が相違
  ①監視の必要性、②未知脆弱性への対応、③対応期間の長期化
- これらを**PSIRT**（Product Security Incident Response Team）が組織横断で実施する
  - ✓ 製造～廃棄前の企画/開発(設計～検証)で脆弱性の予防/除去を行うが、
    完全に対策を施すことは困難なため、**製造開始後も継続して保守/改修が必要**



（参考）侵入検知とは

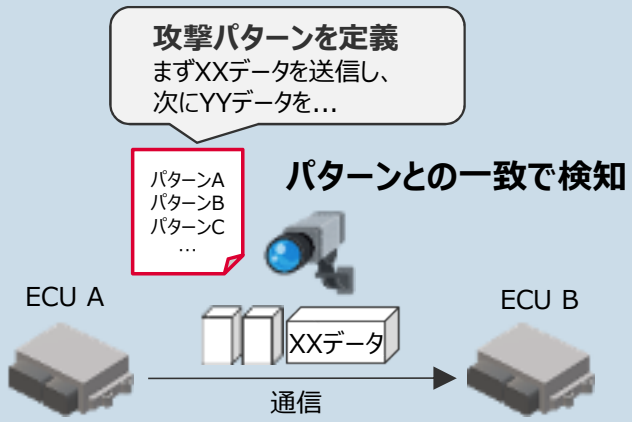
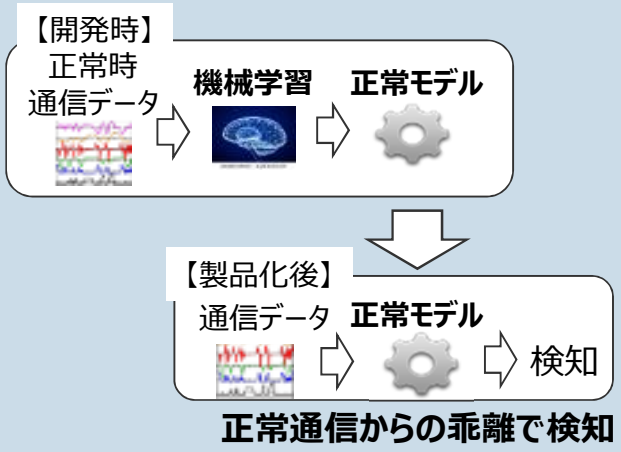
- NIDS(Network based Intrusion Detection System) ①、②
  特定のネットワークまたはネットワーク装置の**トラフィックを監視**し、
  プロトコルの活動を解析して、疑わしい活動を特定する
- HIDS(Host based Intrusion Detection System) ③
  製品**内部で発生するログなどからイベントを監視**し、疑わしい活動を特定する

監視対象と機能配置のイメージ



車両内にセキュリティセンサを配置することで侵入を検知する

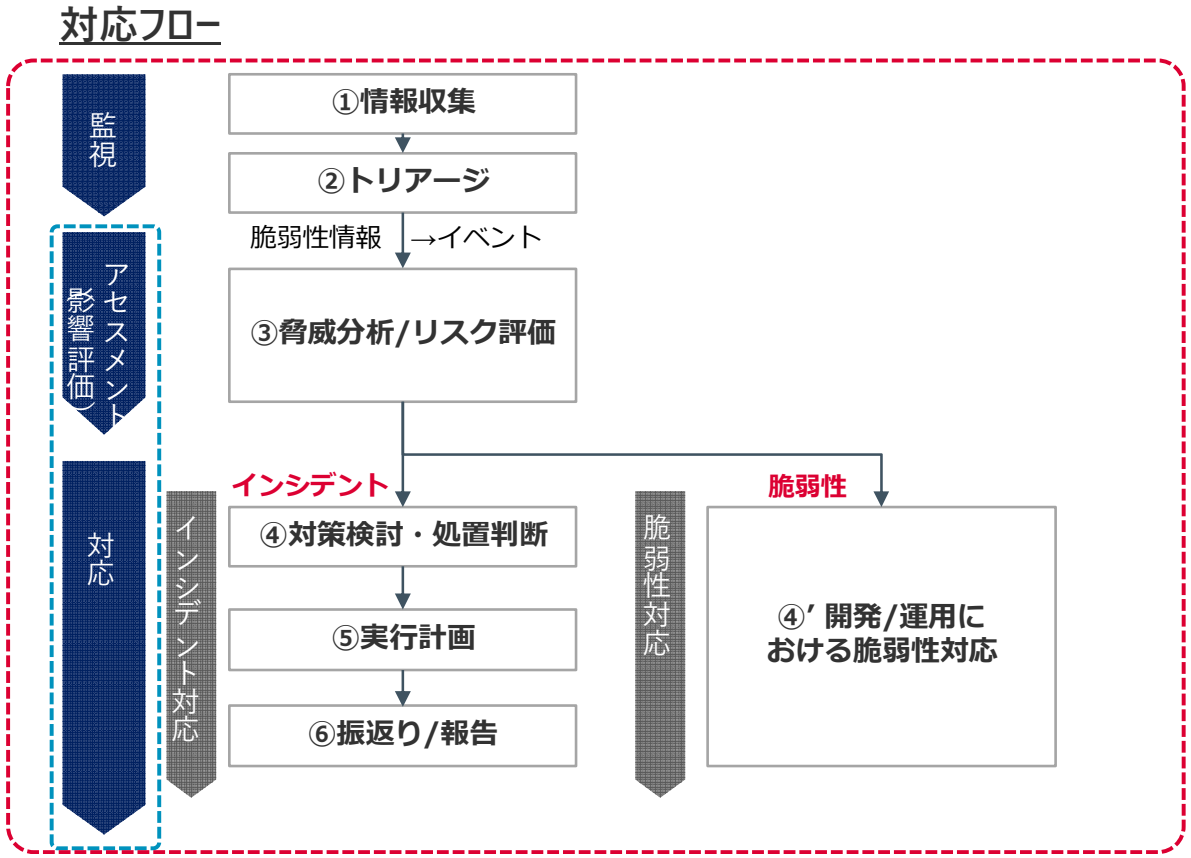
（参考）侵入検知とは －検知方法による分類－

	シグネチャ型	アノマリ型
動作概要		
検知対象	周期フレーム　（タイミングで検知：易）	イベントフレーム　（データで検知：難）
検知率 既知の攻撃	高	中　(原理的に誤検知あり)
検知率 未知の攻撃	－	低～中　（原理的に誤検知あり）

複数の検知方式によりサイバー攻撃を検知する

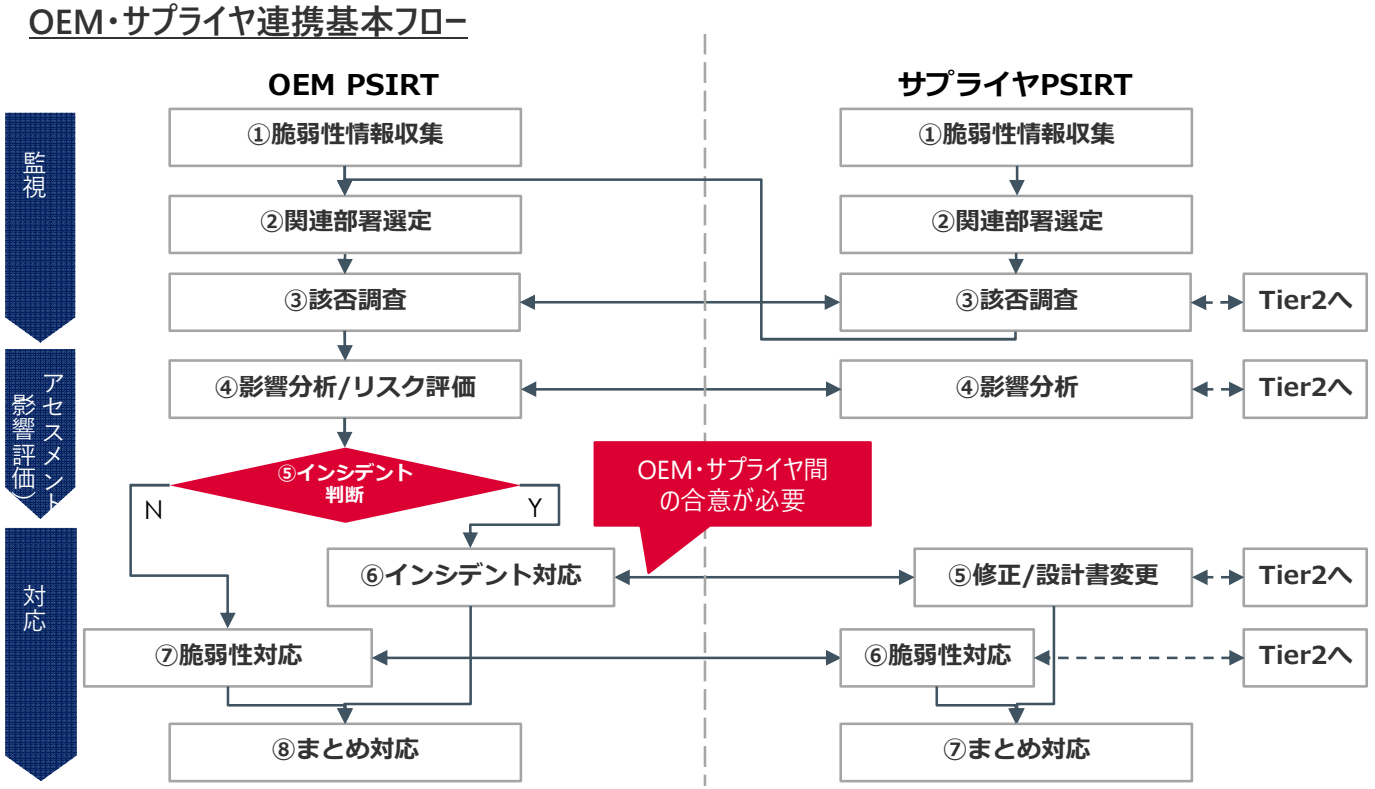
脆弱性情報への対応　～基本フロー～

- PSIRTにおける脆弱性の監視、アセスメント（影響分析）、対応の基本フローを示す



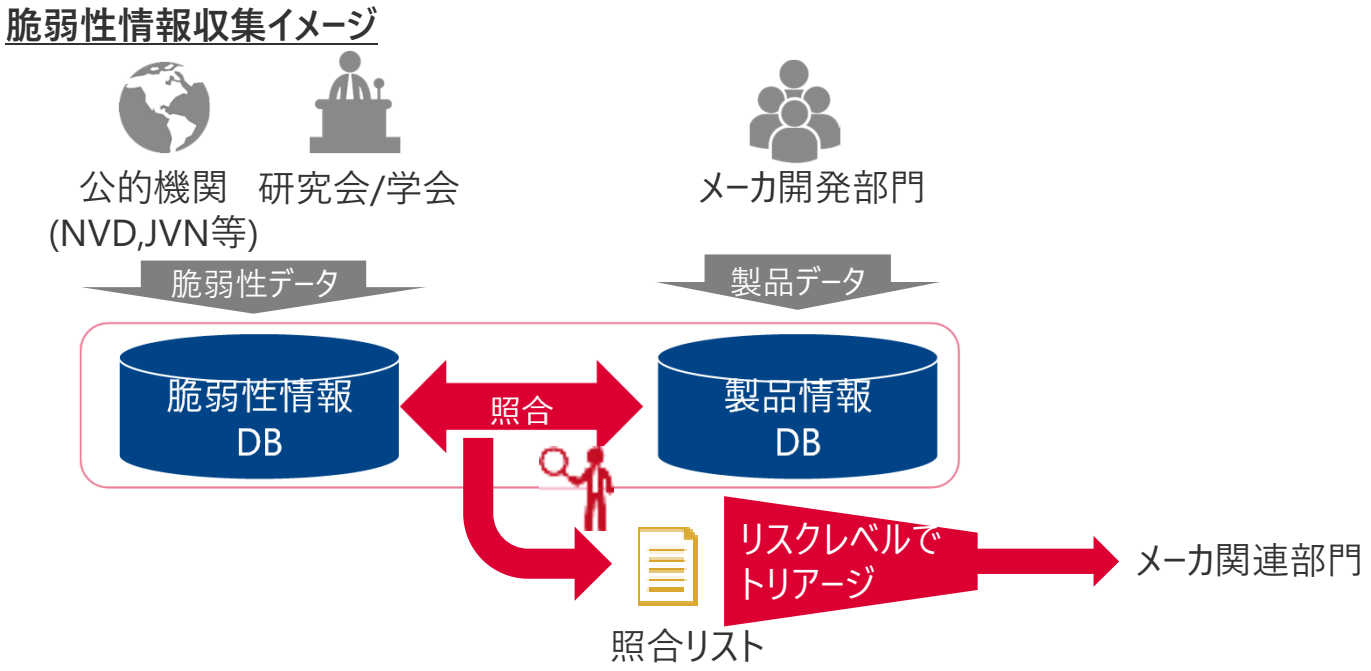
脆弱性情報への対応　～連携フロー～

- 基本フローに基づいた脆弱性情報への連携フローを示す
  - ✓ インシデント判断、及び対応はOEMと合意する必要がある



PSIRT運用の概要 ～脆弱性情報の照合～

- 脆弱性情報を**収集**し、製品の**ソフトウェア構成情報と照合**することにより
  製品に脆弱性のあるソフトウェアが含まれているか**特定**。必要に応じ詳細調査を行う
  - ✓ 照合作業は製品の設計・開発担当者が実施する
  - ✓ 近年では**専門企業や脆弱性の照合サービス**の利用が増加



業界全体での情報収集 ～J-Auto-ISAC～

- J-Auto-ISACはOEM・サプライヤ含む幅広い会員（約100社）で構成されている
- **脆弱性/脅威情報の収集/分析**および展開は**SOC**(Security Operation Center)が担う
  - ✓ 複数の**セキュリティ企業**が**SOCへ情報提供**している
  - ✓ 情報の閲覧権限は会員ランクに応じて限定されている（当社は理事会社）

J-Auto-ISACの組織構成

ISAC:　Information Sharing and Analysis Center

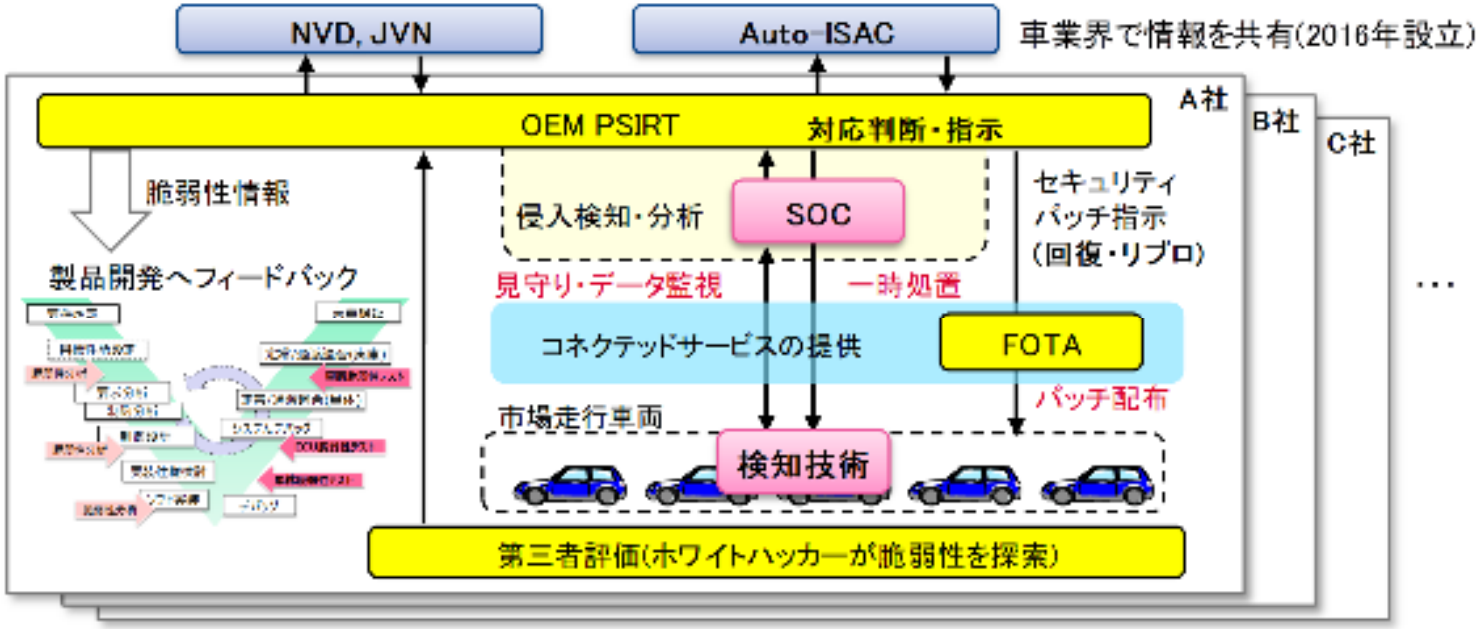
業界全体での情報収集 ～J-Auto-ISAC～

- 国内関連組織に加え国外のISACとの連携も推進している

自動車業界の目指す姿

NVD: National Vulnerability Database
JVN: Japan Vulnerability Notes
ISAC: Information Sharing and Analysis Center
PSIRT: Product Incident Response Team
SOC: Security Operation Center
FOTA: Firmware Over-The-Air

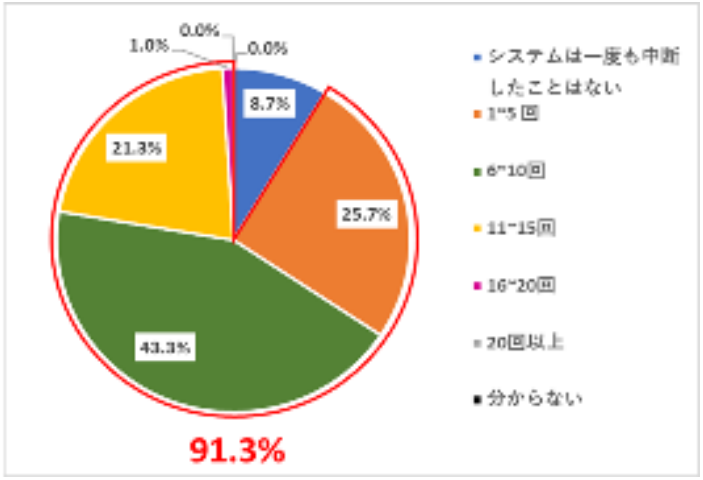
従来		コネクテッド・サービスの時代
モノの品質を監視	＋	流通する情報の品質を監視

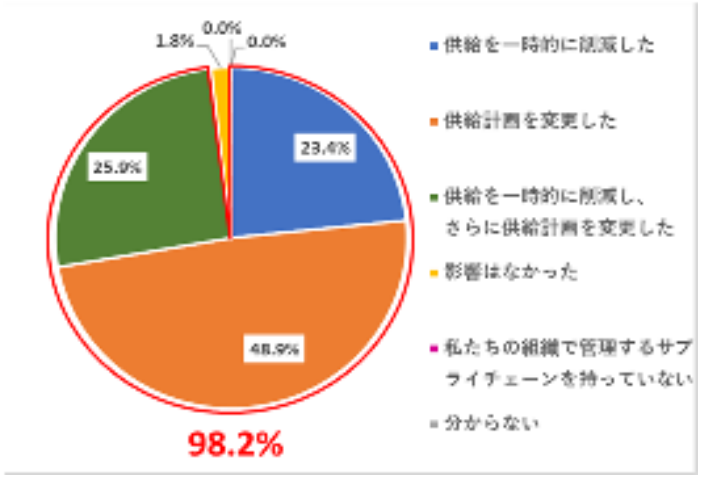


市場でのサイバー攻撃情報を業界で迅速に共有し、レジリエントな社会を実現する

工場セキュリティ

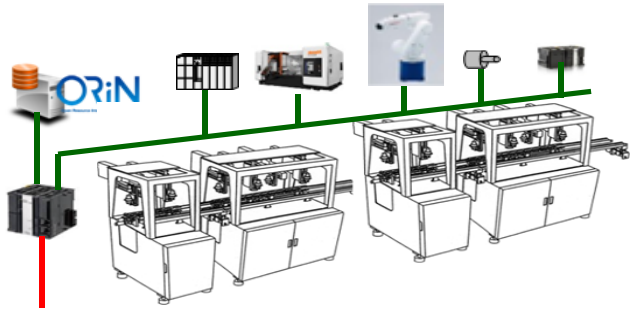
- 日本では**約9割がサイバー攻撃による産業制御システムの中断を経験**

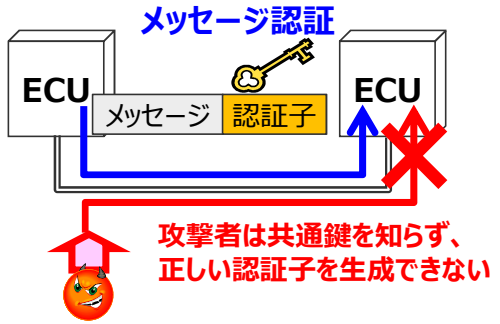




出展：
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220711-01.html

- Factory IoTによるリスク増大・**セキュリティ強化製品立上げ（工場での暗号鍵管理）**





ECU: Electronic Computing Unit

（参考）IPA 産業用制御システム（ICS）のセキュリティ10 大脅威

産業用制御システムのセキュリティ 10大脅威（2019年）		2016年
1位	リムーバルメディアや外部機器経由のマルウェア感染	2位
2位	インターネットやイントラネット経由のマルウェア感染	3位
3位	ヒューマンエラーと妨害行為	5位
4位	外部ネットワークやクラウドコンポーネントの攻撃	8位
5位	ソーシャルエンジニアリングとフィッシング	1位
6位	DoS/DDoS攻撃	9位
7位	インターネットに接続された制御機器	6位
8位	リモートアクセスからの侵入	4位
9位	技術的な不具合と不可抗力	7位
10位	スマートデバイスへの攻撃	10位

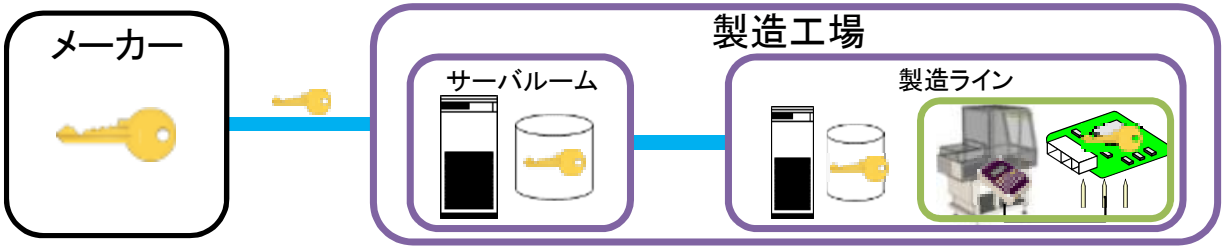
出展：[ドイツBSI] 産業用制御システム（ICS）のセキュリティ -10大脅威と対策 2019-：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/controlsystem/bsi2019.html

工場セキュリティ（暗号鍵管理）

- 工場において、マイコンに暗号鍵をセキュアに書込む

✓ カーメーカー提供の暗号鍵をECU（Electronic Computing Unit）にセキュアに書込む

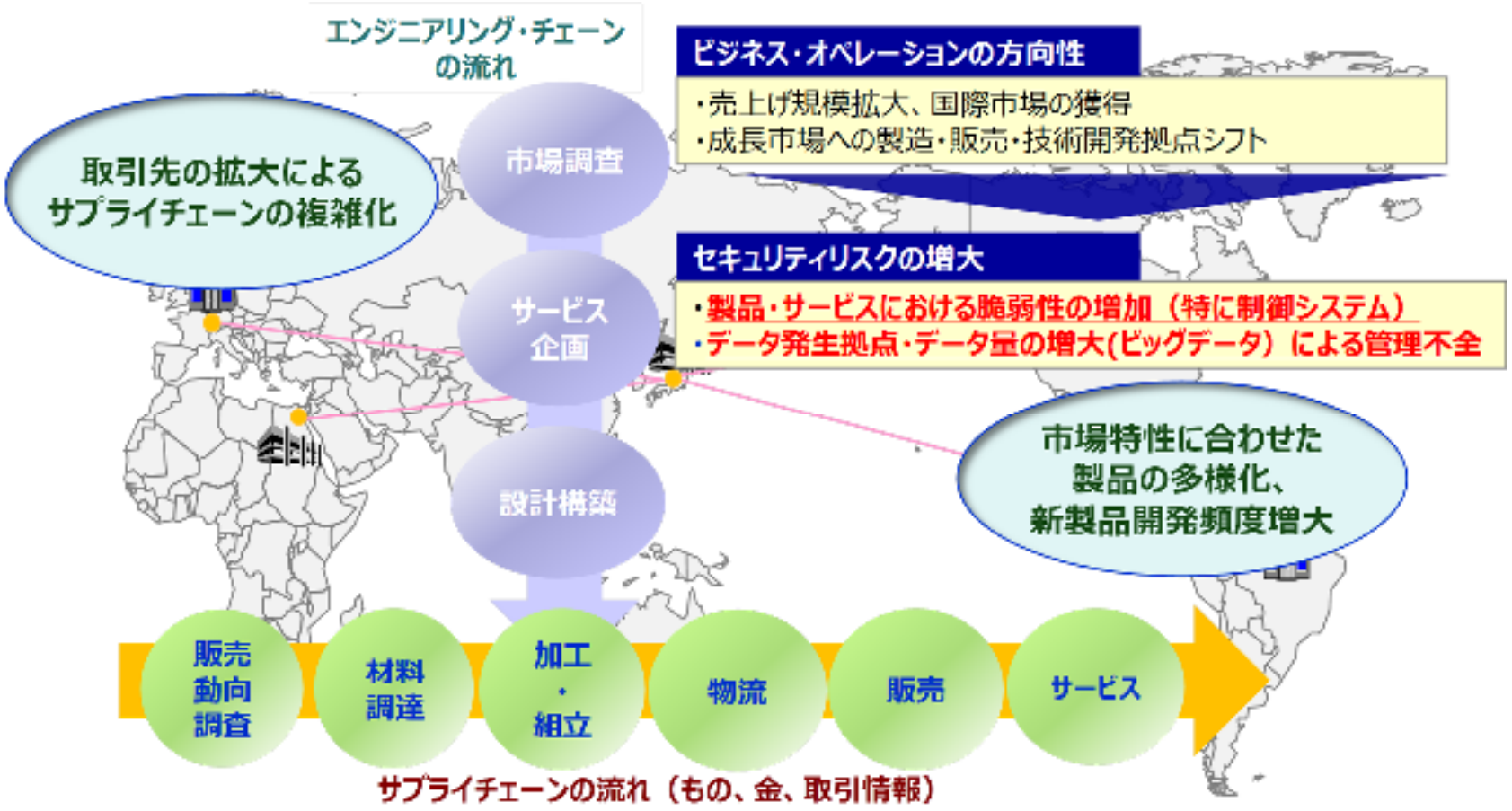
✓ 暗号鍵の配送・保管・書込みの**全工程（ライフサイクル）でセキュリティ強化が必要（鍵管理）**
cf.サプライヤ側で使用する暗号鍵はサプライヤが生成・保管（15年以上）



①ネットワークセキュリティ強化　②物理セキュリティ（入退室）強化　③製造工程と装置の変更

鍵をセキュアに書き込むための設備の他、鍵配送のための通信・サーバなども準備要

サプライチェーンのセキュリティリスク

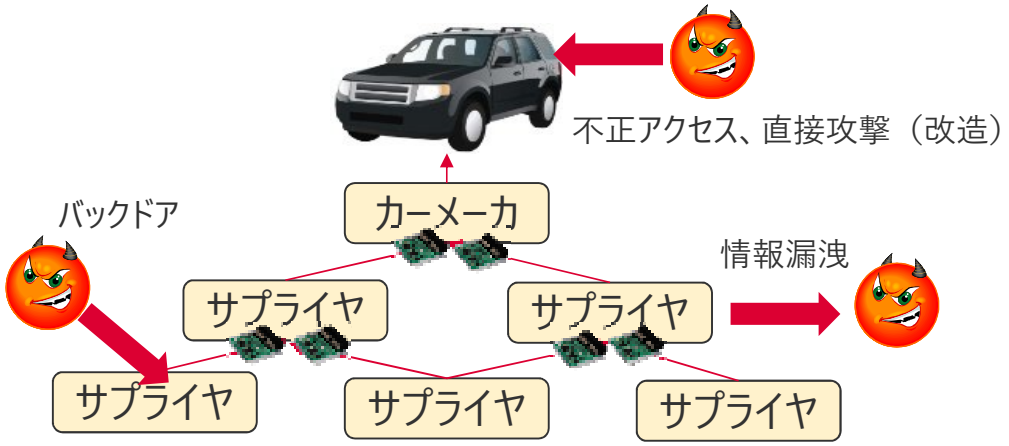


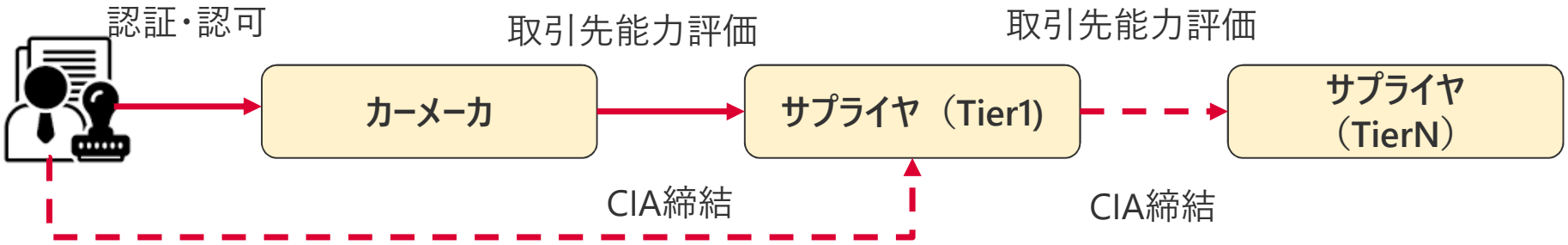
グローバル化により情報の発生量・場所が拡大（グループ会社、委託先、再委託先・・・）

自動車業界でのサプライチェーン対策

車両型式法規要件

(概略、抜粋) 車両メーカーは**サプライヤとの間に存在する可能性がある依存関係について、サイバーセキュリティ管理システムがどのように対処するかを証明する**必要がある。

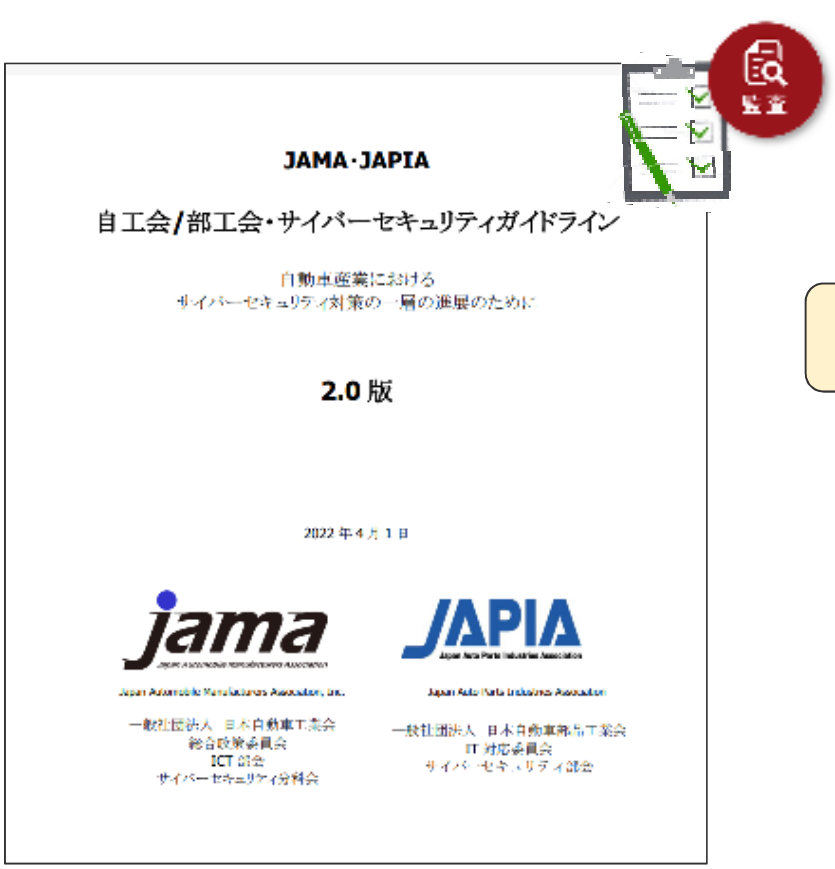


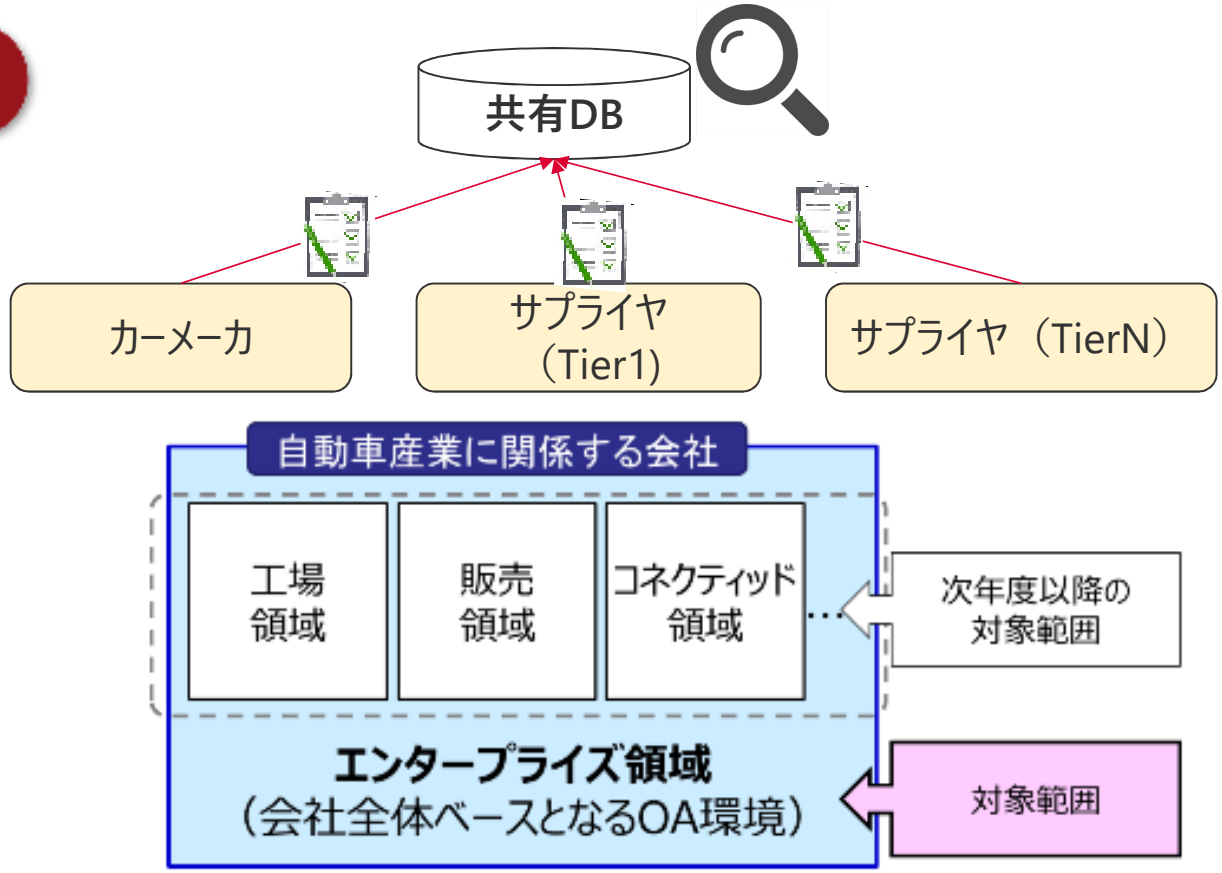


法規要件として、サプライチェーンの依存関係や取引先の能力を管理する必要がある

CIA: Cybersecurity Interface Agreement

（参考）自工会/部工会・サイバーセキュリティガイドラインV2.0（22年4月～）



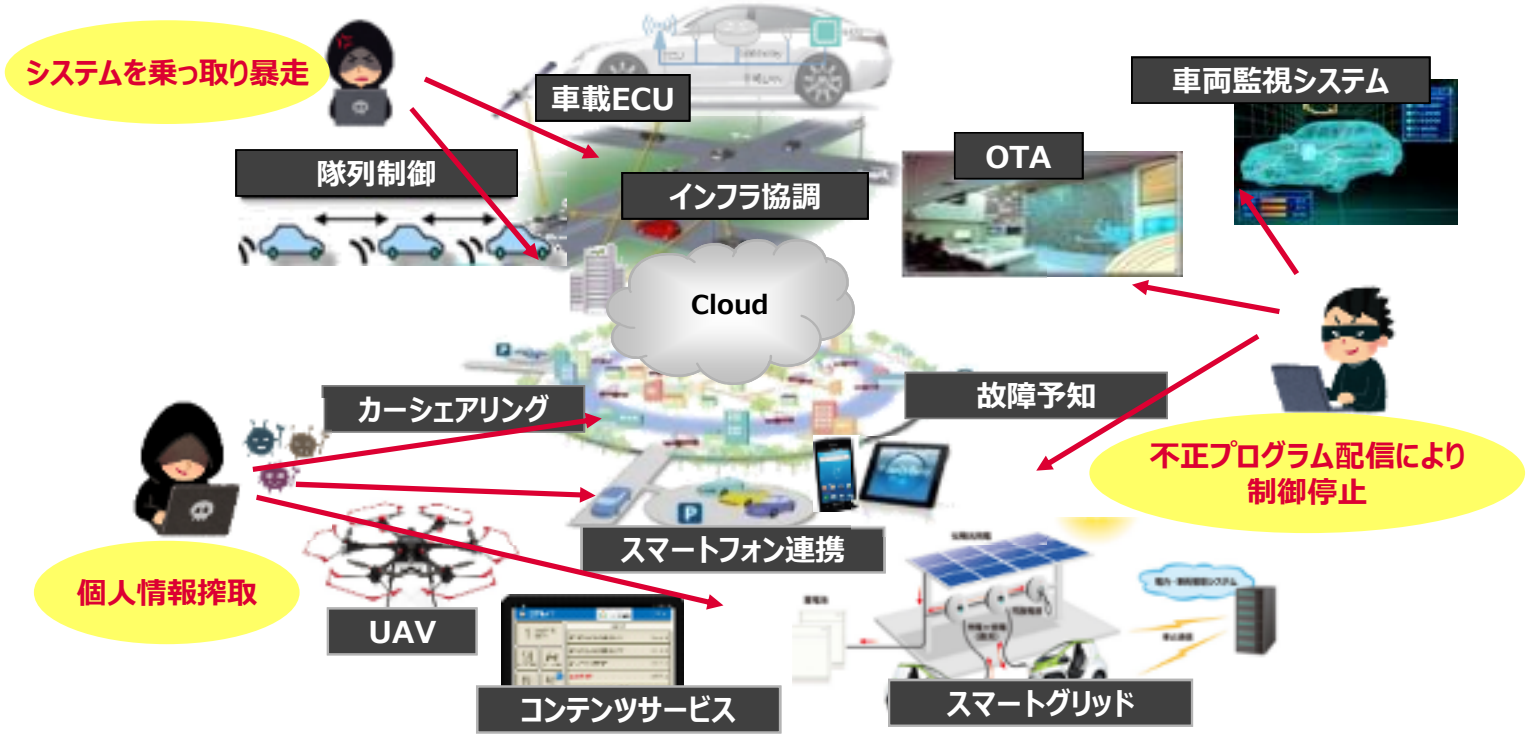


出展：自動車産業サイバーセキュリティガイドライン | JAMA - 一般社団法人日本自動車工業会
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

IV

CASEに向けたセキュリティ＆プライバシ

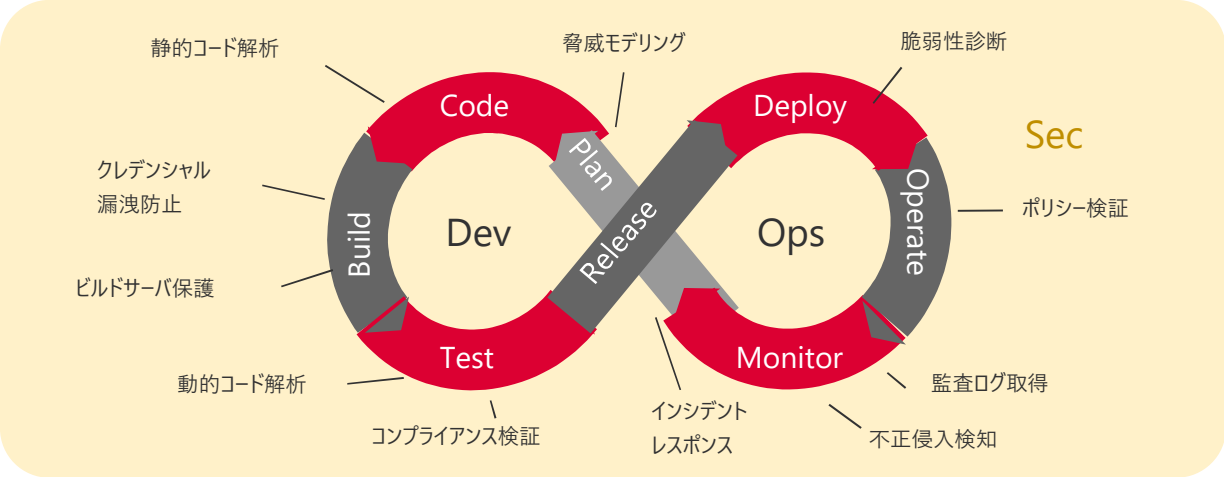
セキュリティとプライバシへの対応



製品・サービスの多様化による様々な脅威に対応する必要がある

リリースサイクルの高速化に伴う対応

- 素早くユーザニーズを検証、確認するため、製品のリリースサイクル高速化が求められている。
- 後工程で発見されたセキュリティの問題は手戻り・やり直しにかかるコストが大きいため、システム開発・運用の各工程でセキュリティ対応を組み込んでいく**DevSecOps**が注目される。
  - ✓ DevSecOpsでは各工程にコードチェック、ログ監視等のツールを用いてセキュリティチェックを自動化、開発速度を損なわず開発していく。

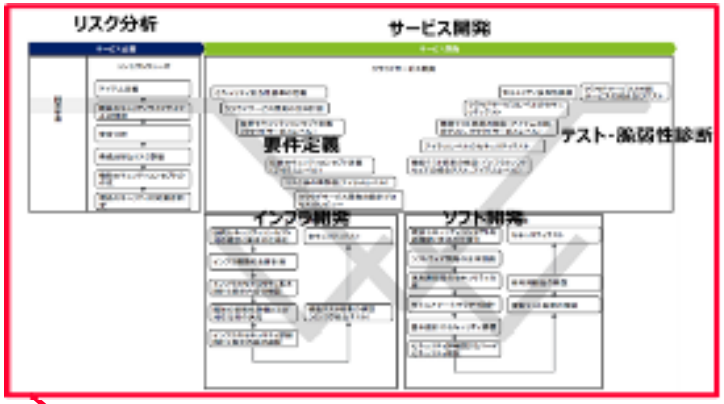


アジャイル開発でも初期のアーキテクチャ検討、脅威分析が重要

デンソーのITサービスセキュリティ＆製品プライバシ活動

- アウトカービジネスは、お客様の個人情報を持つことによる**プライバシへの対応と**
  クラウド等のITサービスに対するインカー（車載ECU)とは異なるセキュリティ対応が必要。
  （ex.短納期での開発、グローバル法規制への準拠、最新技術の追従）

■ITサービスセキュア開発プロセス



リスク分析・要件定義・設計・評価の手順に従い作成（設計者）した成果物に対して適切に実施できていることを確認（アセスメント）

■PIA （プライバシ影響評価）

各工程でプライバシの影響を確認するための成果物を作成（設計者）し、適切に実施できているかを確認（プライバシ監査）

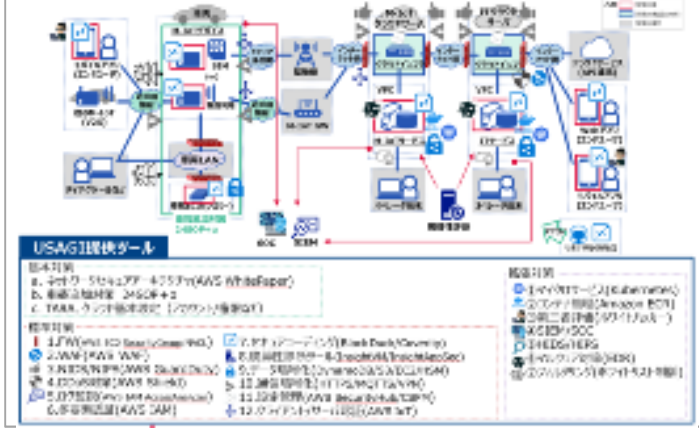
USAGI（Universal Security Architecture for Global IoT system ）

目的	製品のセキュリティ開発において、**製品共通で直面する問題に対して、あらかじめ解決策を用意**することで、**セキュリティ品質の向上・開発の効率化**を狙う。これにより、開発者が**製品固有の問題に注力**できるようにする。

■IoTセキュリティ基盤の構築

- M-IoTシステムにおいて、標準で備えるべきセキュリティ対策を明確化
- 標準セキュリティ対策を実現するためのツール群を定義(=USAGI)

USAGI全体像

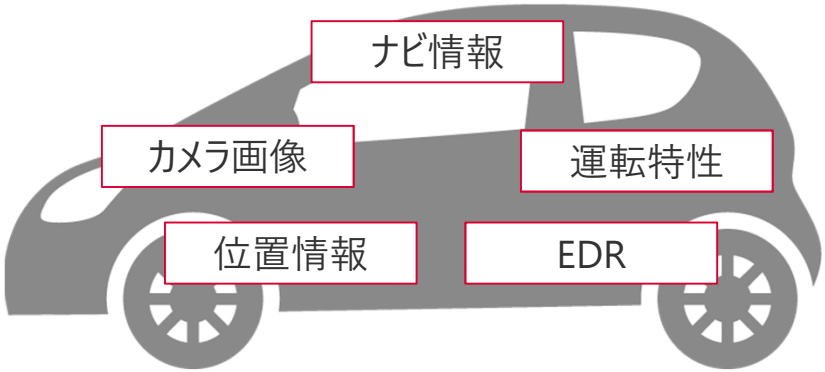


■USAGI利用者向け手引書を用意

- USAGIが提供するツールについて、利用方法を解説する文書を用意
- ツールを利用するタイミングで参照できるよう、文書はフェーズごとに分冊

クルマとプライバシの関係

- 「つながるクルマ (クラウド連携サービス)」が普及すると、より多くのパーソナルデータを車内/外で取り扱うようになり、**プライバシの侵害リスク**が高まる。
  - ✓ 例：位置情報、ナビ情報、カメラ画像、運転特性、EDR
  - ✓ 漏洩のみならず、同意がないデータ取得/提供や説明漏れ
- 近年、プライバシ意識の高まりもあり、様々な法規が制定されており、**プライバシを考慮したクルマづくりが求められている**



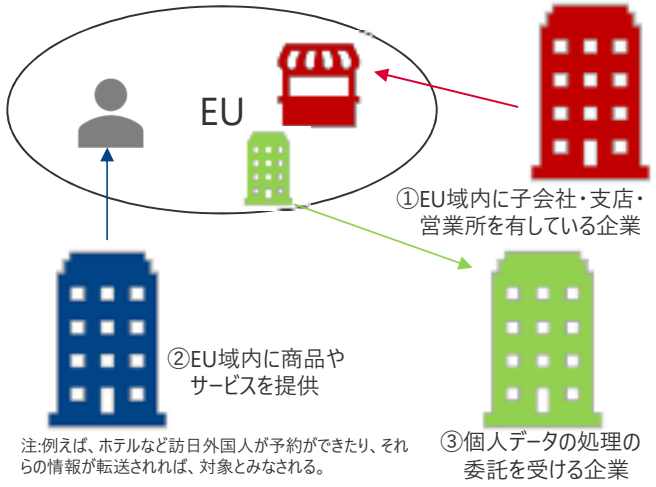
GDPR

- **GDPR**（一般データ保護規則）は、パーソナルデータ保護のために、2018年にEUで施行された。
- 世界で初めて、民間事業者に対して**プライバシ影響評価**（PIA：Privacy Impact Assessment）を義務づけし、パーソナルデータを、プライバシ保護原則に基づくリスクベースで評価・対処することを企業に求めている。
- EU域外にも適用されるとともに、パーソナルデータの越境データ移転を制限している。

ポイント	概要
個人の権利	• 「忘れられる権利」「プロファイリングを拒否する権利」「データポータビリティの権利」など個人の権利が規定され、個人データに対する本人のコントロールの権限を大幅に強化
罰則 (制裁金)	• 最大2000万ユーロか、世界年間総売上の4%いずれか高い方
プライバシバイデザイン	• GDPRで新たに導入された、サービス開始に当たって、発生する可能性があるプライバシ侵害を、事前評価してリスクを特定し、最小化する取り組み（詳細は後述）
漏洩報告の義務	• パーソナルデータの漏洩に気づいた場合、企業は72時間以内に当局に通知しなければならない。 • あわせて、本人にも速やかに通知しなければならない。

https://www.nri.com/-/media/Corporate/jp/Files/PDF/knowledge/publication/chitekishisan/2018/09/cs20180903.pdf?la=ja-JP&hash=4853261705549D05CEFCC42DFA8B2C6AFD2AD8B7

EU域外への適用パターン

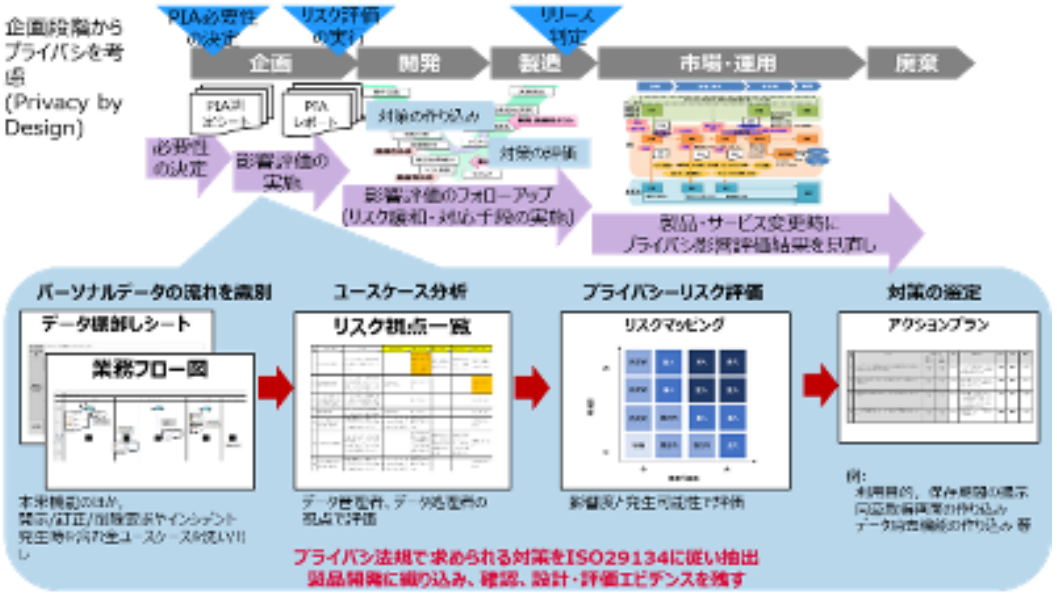


注:例えば、ホテルなど訪日外国人が予約ができたり、それらの情報が転送されれば、対象とみなされる。

https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

プライバシ影響評価

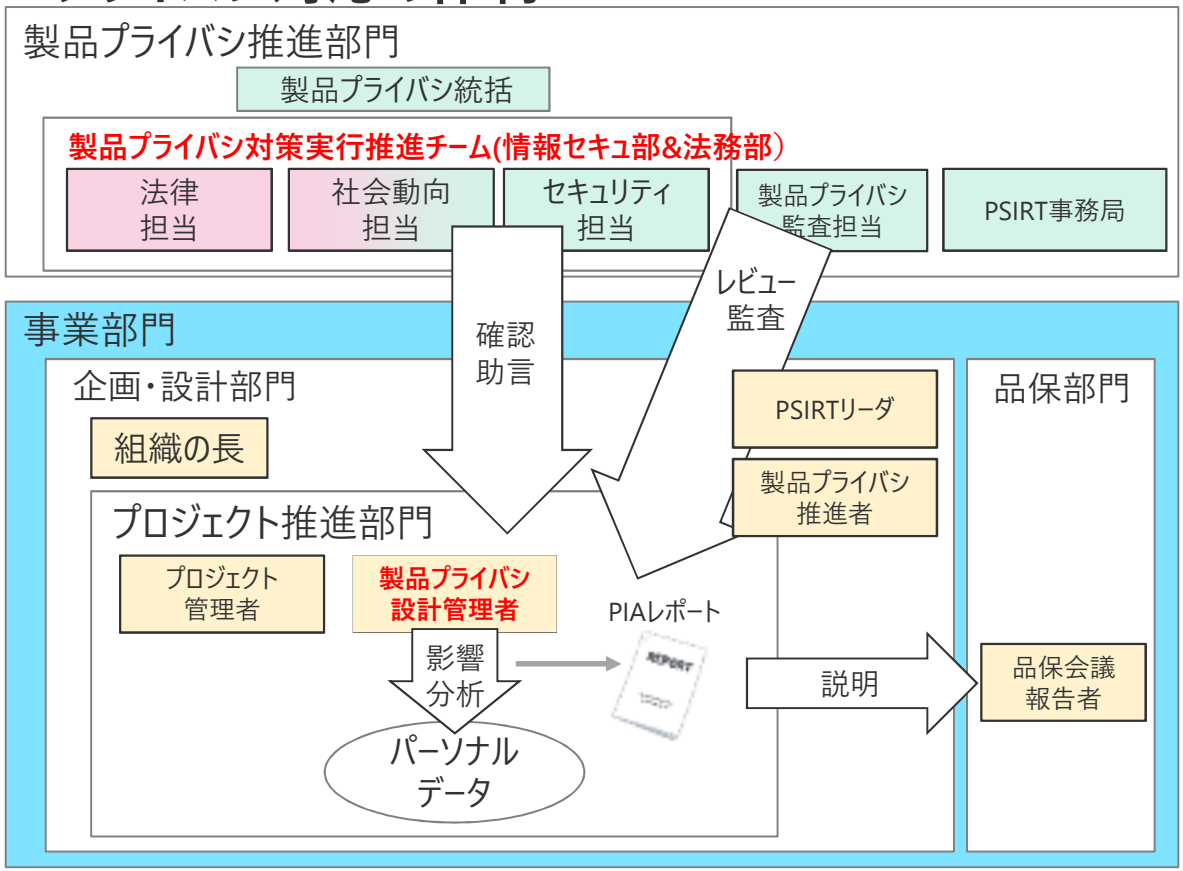
- 企画段階からプライバシを考慮する“Privacy by Design”で、プライバシ上のリスクに適切に対処した製品・サービスの提供が必要
- プライバシ影響評価（PIA）により、対策を実施した製品サービスの提供が可能



”Privacy by Design”を実現する方法を開発ルールとして規定

プライバシ監査・アセスメント体制の構築

■プライバシ対応の体制



V

まとめ

まとめ

■背景・動向
- 正の側面：クルマがIoTの一部となりつつあり、サイバーセキュリティの重要性は高まっている
- **負の側面：クルマがハッキング対象と認識**されている
- 車業界でセキュリティの標準化にむけた動き

■当社の活動
- 【仕組み】車業界のセキュリティの確立を目指し、**ライフサイクルとサプライチェーンで解決中**
- 【業界連携】業界全体での**情報収集・分析を行ってものづくりを強化（J-Auto-ISAC）**
- 【工場のセキュリティコンセプト】国際規格への準拠や多層防御による強化

■今後の課題
- グローバルかつ他業界を踏まえて、車業界の想定攻撃を定義する
- クルマのリスク評価手法を定め、各リスクレベルにおける設計・評価レベルを策定する
- CASE対応に向けた**セキュリティ＆プライバシのグローバルでの仕組み整備**

DENSO

Crafting the Core