SDV時代のサイバーセキュリティ

車載API、自動運転サービス、サプライチェーンリスクにどう対応していくか

2026年3月19日

株式会社 NDIAS

自動車セキュリティ事業部
GM 上松 亮介

01 NDIASの紹介

02 データで見る自動車セキュリティの変遷

03 SDV（Software Defined Vehicle）による変化

04 車載APIにおけるサイバーセキュリティ

05 自動運転サービスにおけるサイバーセキュリティ

06 モビリティサービスにおけるサプライチェーンリスク

NDIAS（NRI DENSO Industrial & Automotive Security）

NRIセキュアテクノロジーズ株式会社

IT、IoT分野における
セキュリティの知識と経験

株式会社 デンソー

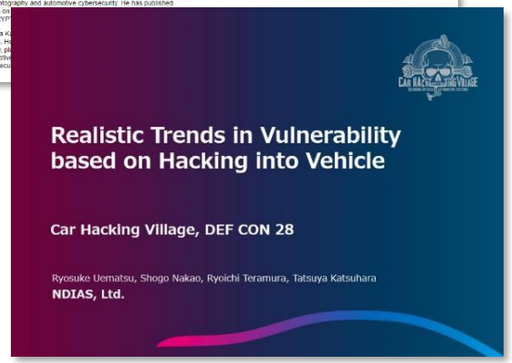
自動車の深い知識と
車両部品開発の豊富な経験

Ndias

自動車のサイバーセキュリティの専門家集団

世界トップレベルの技術力を武器とするセキュリティ専門家集団

技術研究・カンファレンス発表



https://www.youtube.com/watch?v=5ZgfhEb4E50

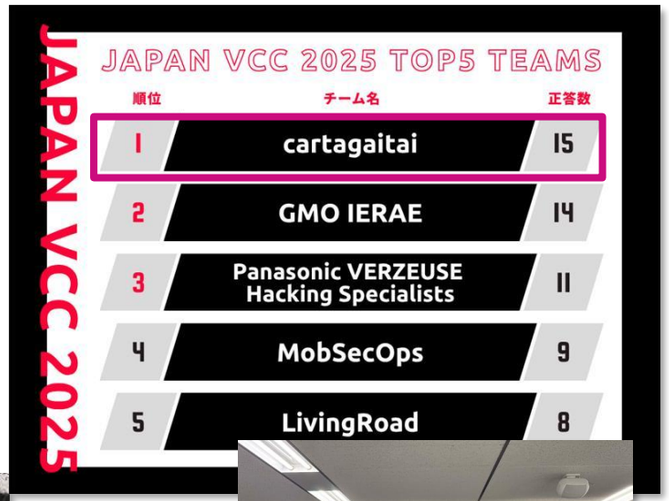
https://www.linkedin.com/posts/car-hacking-village_wed-like-to-give-a-special-thank-you-to-activity-7360361092239249408-gbfl?utm_source=share&utm_medium=member_desktop&rcm=ACoAAB3889sBlQf4vHkR4nKmHznUR1cb1uT7iV8

自動車ハッキングコンテスト 世界5位・日本1位

DEFCON33 CHV CTF 世界5位

Place	チーム
1	OBD2_Obl1terat0rs
2	VDL
3	AUTOCRYPT
4	ACQR
5	cartagaitai
6	Pla
7	De
8	zz
9	gft

JAPAN VCC2025優勝



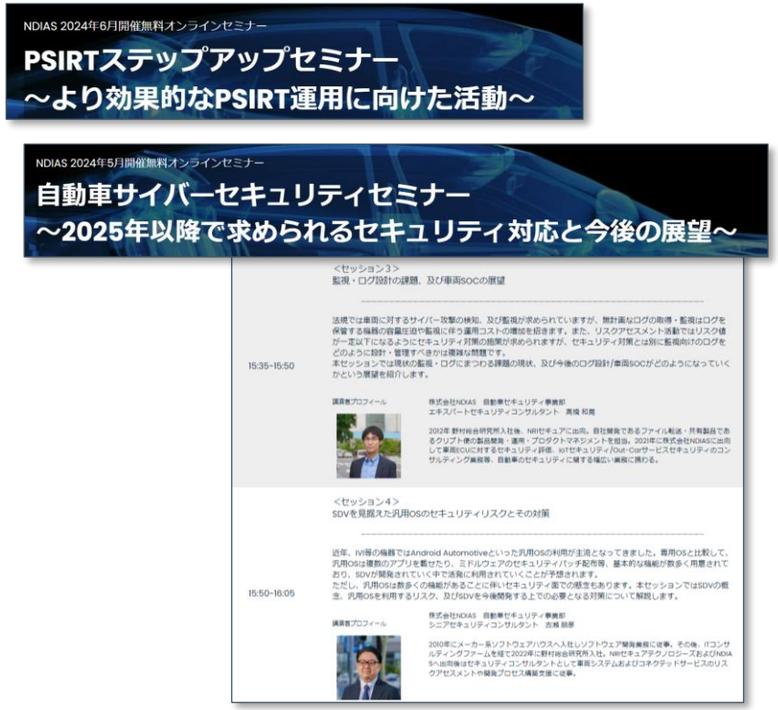
積極的な自動車業界向けのセキュリティ情報発信

NDIASでは様々な形態・媒体を通して、自動車セキュリティの最新情報や独自の分析を発信して、自動車業界の発展に貢献

公開記事による情報発信

参考: https://ndias.jp/blog.html

自動車セキュリティセミナー主催



自動車に特化した脅威分析レポートの発行

ショートペーパーは下記よりダウンロードいただけます。
https://ndias.jp/automotive-cybersecurity-report

車両に関連する領域のコンサルティング、評価、教育、PSIRTを軸としたセキュリティサービスを提供しています。

セキュリティコンサルティング

自動車セキュリティコンサルティング
- セキュリティ開発プロセス構築支援、テスト手順書作成
- 製品設計開発支援（リスクアセスメント など）
- 技術・動向調査、車載器向けセキュリティ技術要件集　　など

セキュリティ評価（診断）

車載ECUセキュリティ評価
- 脆弱性評価、ペネトレーションテスト、ファジング

コネクティッドサービスセキュリティ評価
- Webアプリケーション、プラットフォーム診断、モバイルアプリケーション診断

セキュリティ教育

セキュリティ技術教育･研修
- ハードウェア、各種通信プロトコルのハンズオン研修
- 攻撃･防御技術研修（スタックバッファオーバーフロー、ソフトウェアファジング、Kernel Exploit）

PSIRT

PSIRT運用支援
- 脅威・脆弱性情報配信（ダイジェスト配信、詳細レポート配信）

J-Auto-ISAC様へ
脅威・脆弱性情報も提供

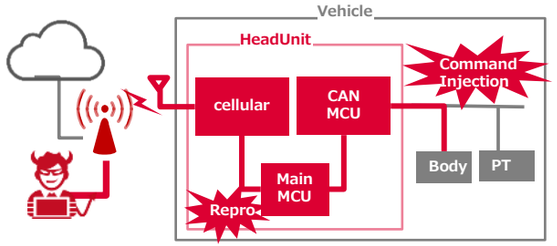
PSIRT教育・訓練
- PSIRT教育とインシデント対応訓練

PSIRT構築支援
- PSIRTプロセス評価、手順評価

02 データで見る自動車セキュリティの変遷

自動車セキュリティこの10年の変遷

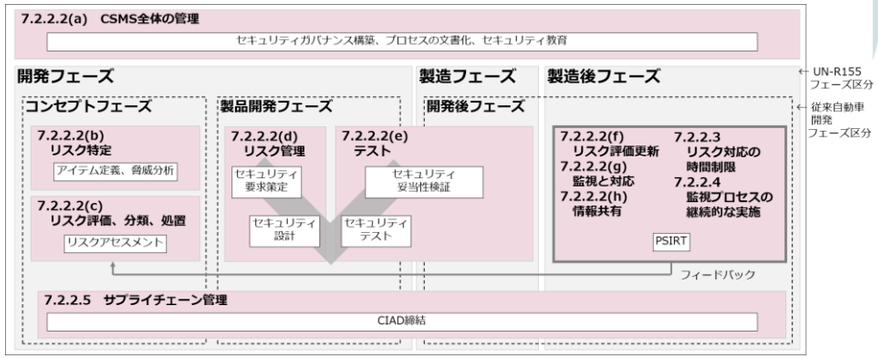
2015年
遠隔攻撃実証でリコール



法整備

2021年
UN-R155施行開始

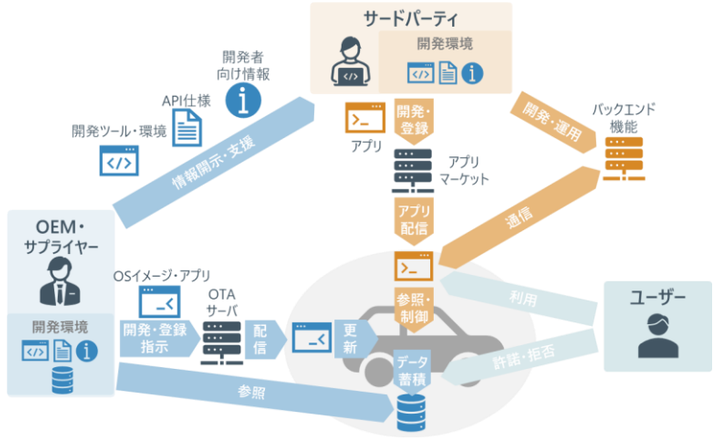
CSMS(Cyber Security Management System)と車両型式認証により**サイバーセキュリティ対応が定着**



高度化

現在
SDV化進行

SDVの発展に伴い新たな脅威への対応が求めれらる

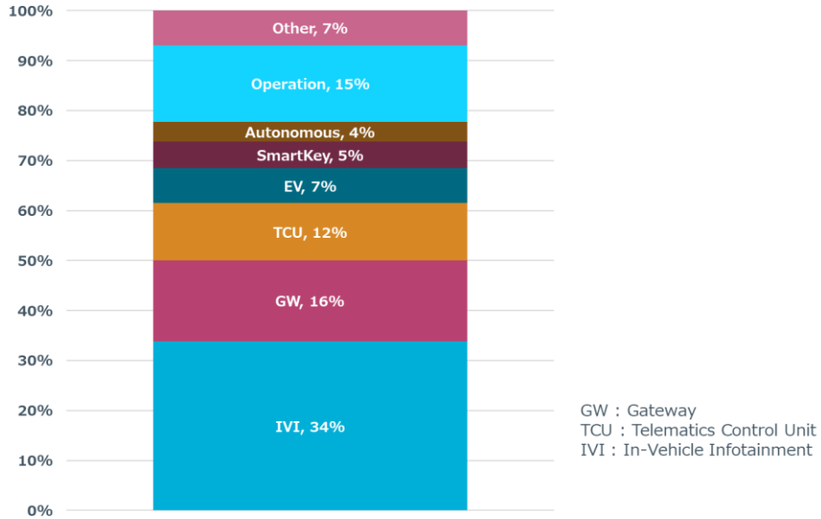


UN-R155におけるサイバーセキュリティ対応

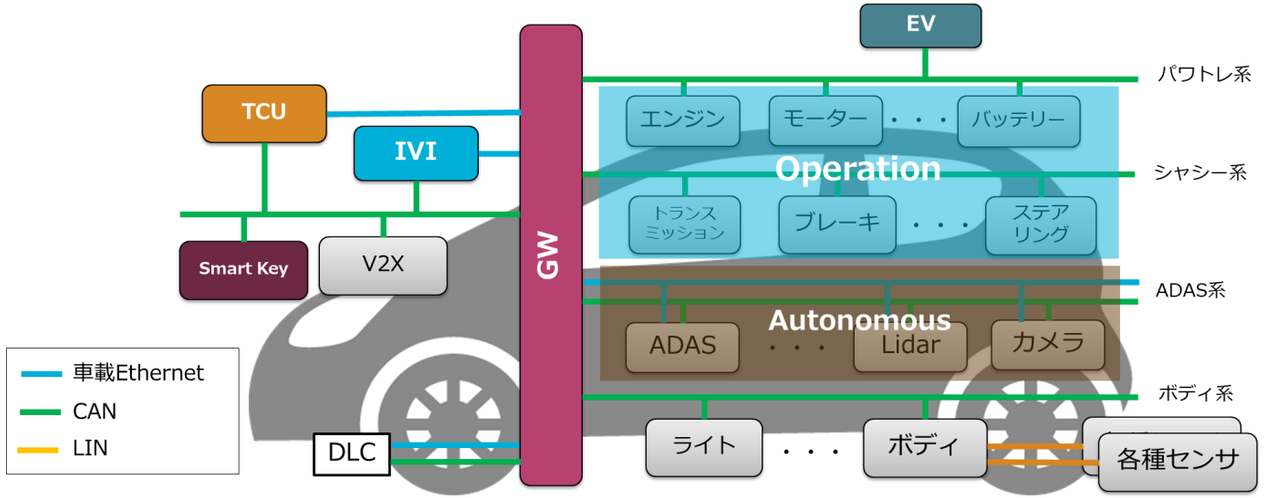
①CSMS	②車両型式	
サイバーセキュリティ管理のプロセス	CSMS認証の提示	
脅威とリスクを特定するプロセス	脅威とリスクを特定	リスクアセスメント
リスクアセスメントするプロセス リスクアセスメントを常に最新に管理するプロセス	リスクアセスメントを実施	
	リスクを適切に処置・管理 アフターマーケット品装着時にも、車両が保護される措置を実施	
テストするプロセス	テストを実施	セキュリティテスト
合理的な期間に対応を実施するプロセス	サイバー攻撃を検知・監視・防御する措置を実施 攻撃分析のため、フォレンジックデータを取得する措置を実施 暗号モジュールはコンセンサスのとれたものを使用	PSIRT
継続的に監視するプロセス		
サプライヤを管理するプロセス		

ペネトレーションテストの対象ECUのデータ

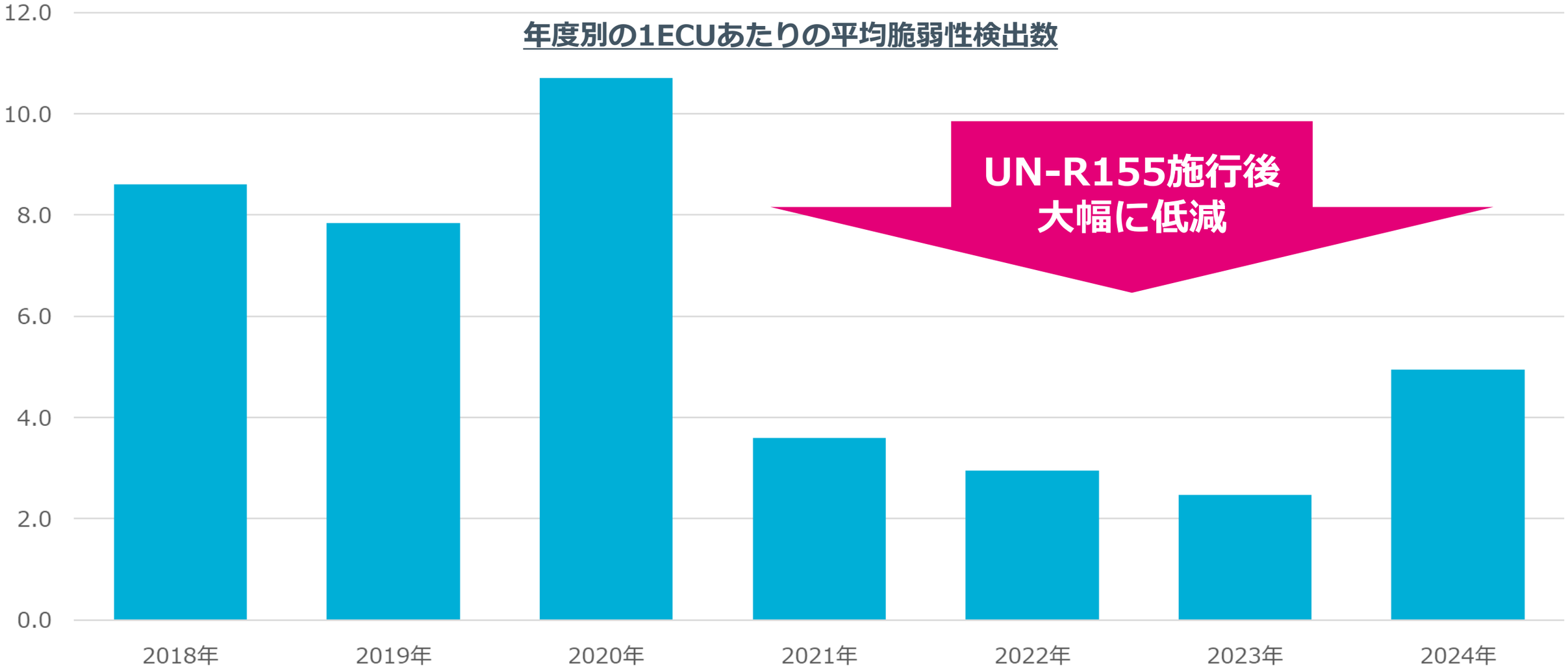
- **車両OEM約15社**の車両に搭載されるECUを対象
  - 自動車(四輪)が主ですが、二輪、トラック、建機、船舶についても含まれます。
- **国内外サプライヤ約25社**の車載ECU
  - 国内サプライヤ71%、国外サプライヤ29%
- **130ECU以上を**評価
  - 主にIVI(In-Vehicle Infotainment)、GW(Gateway)、TCU(Telematics Control Unit)など外部とつながるEUCで約60%。
  - EV(充電関連)、Smart Key、自動運転系(Autonomous)などのECUも増えてきている。



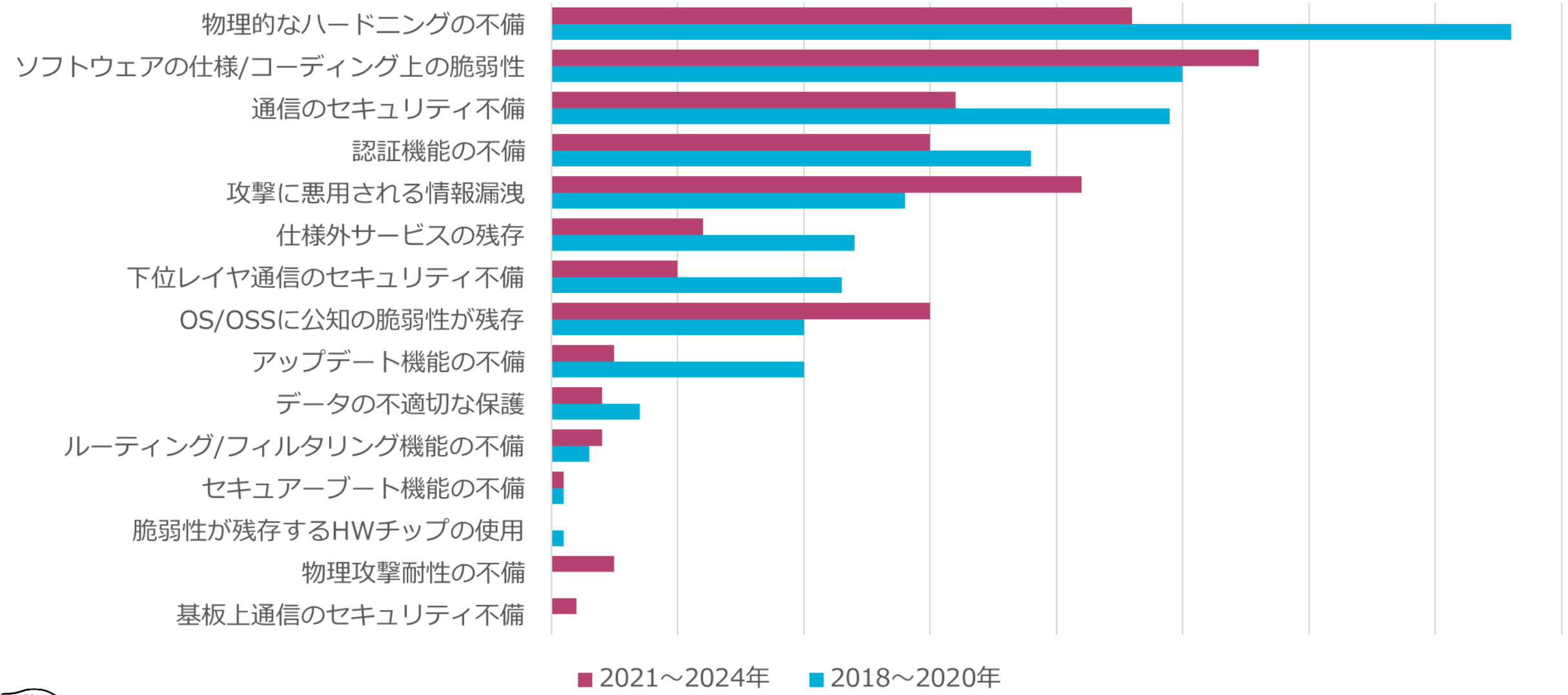
GW：Gateway
TCU：Telematics Control Unit
IVI：In-Vehicle Infotainment



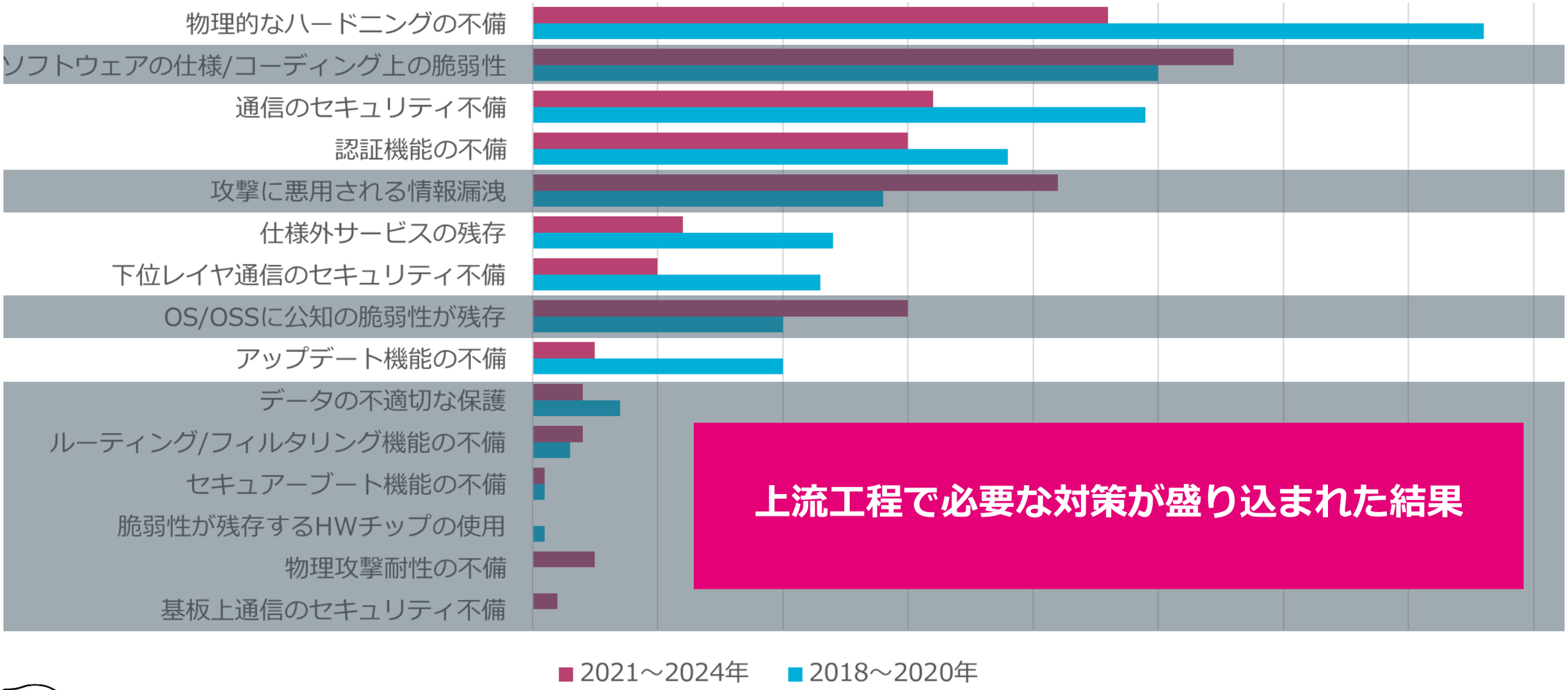
2021年以降脆弱性の検出数は大幅に減少
サイバーセキュリティ対応の定着がペンテストの結果からも見える



2020年までと2021年以降では検出される脆弱性の傾向に違いがある
基本的なセキュリティ対策の浸透した結果が出ている

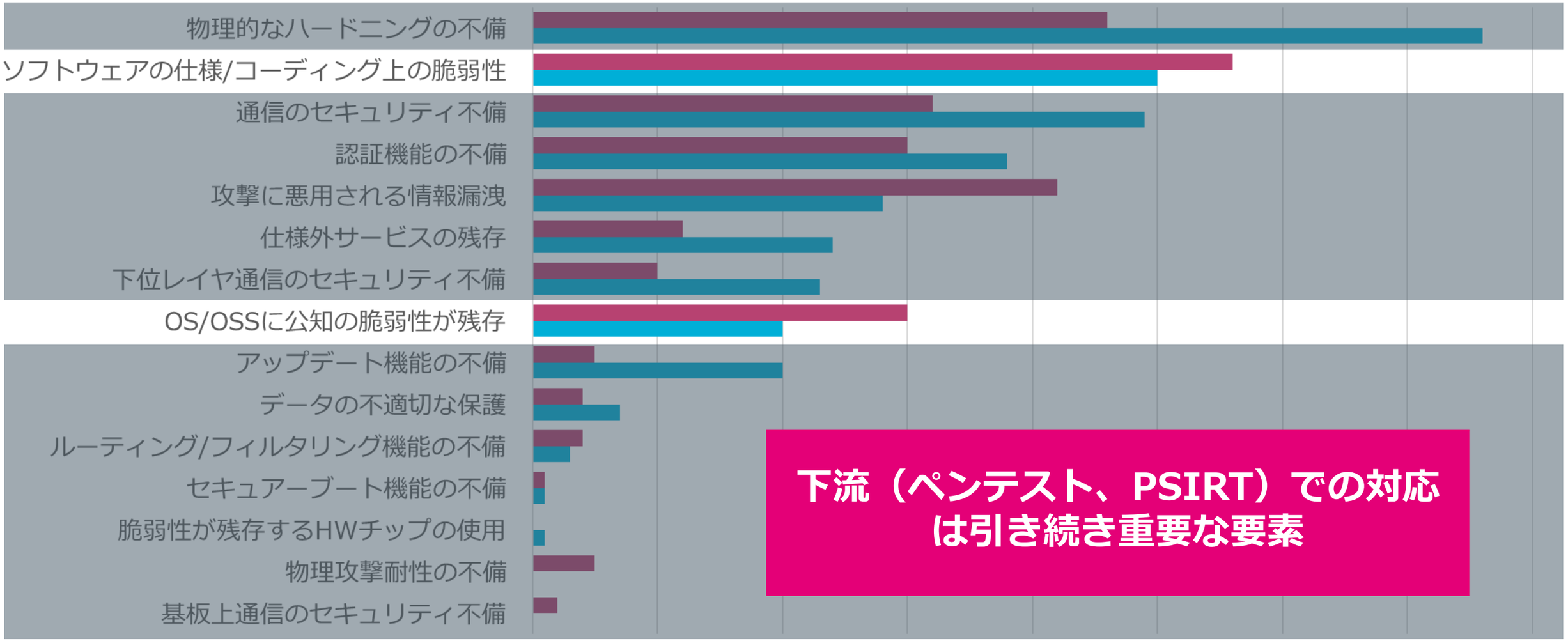


物理的なハードニングや通信のセキュリティなど基本的なセキュリティ対策が進んでおり、脆弱性の検出数が減少している



上流工程で必要な対策が盛り込まれた結果

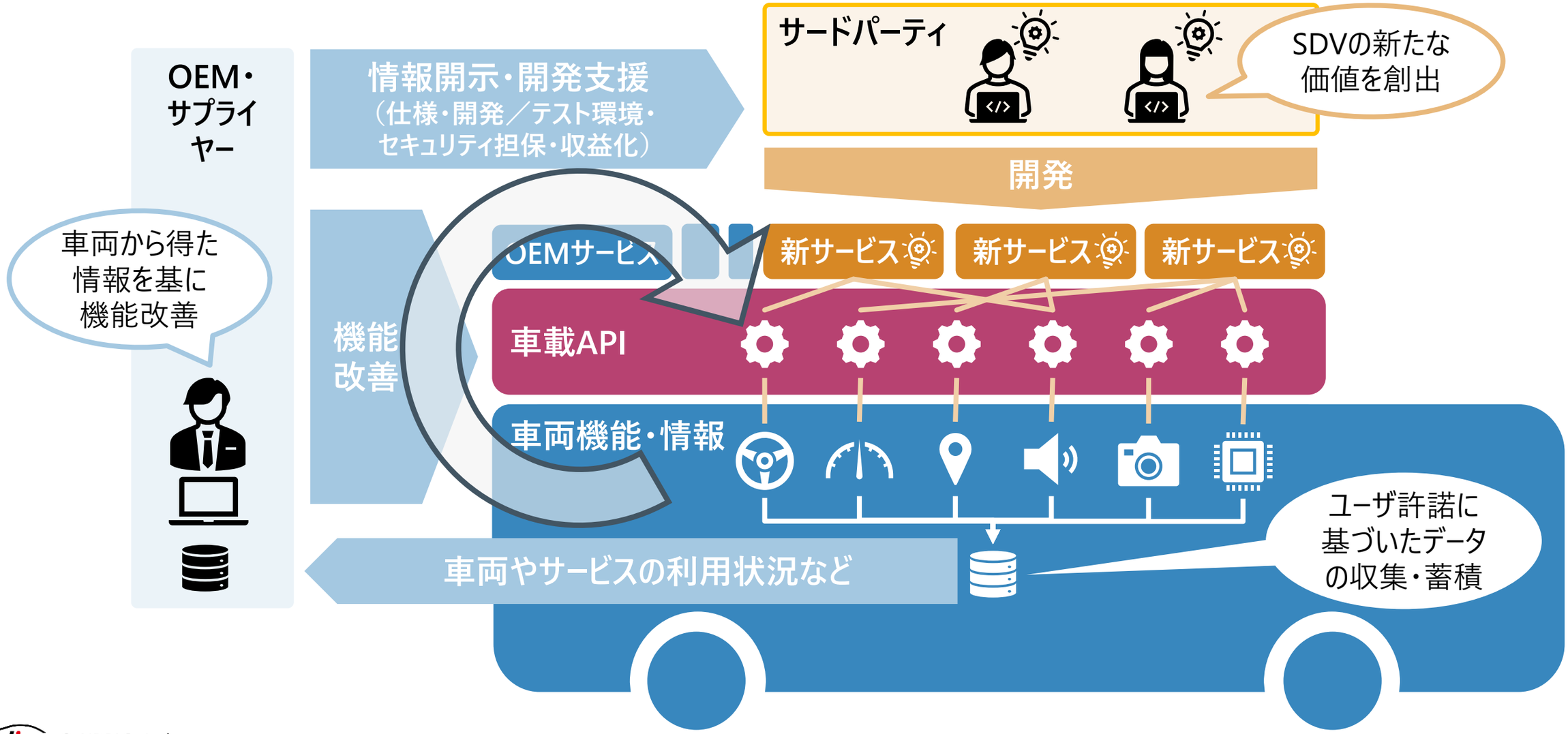
一方で、ソフトウェアのコーディング上の脆弱性やOSSなどの公知脆弱性が残存する問題は減少していない



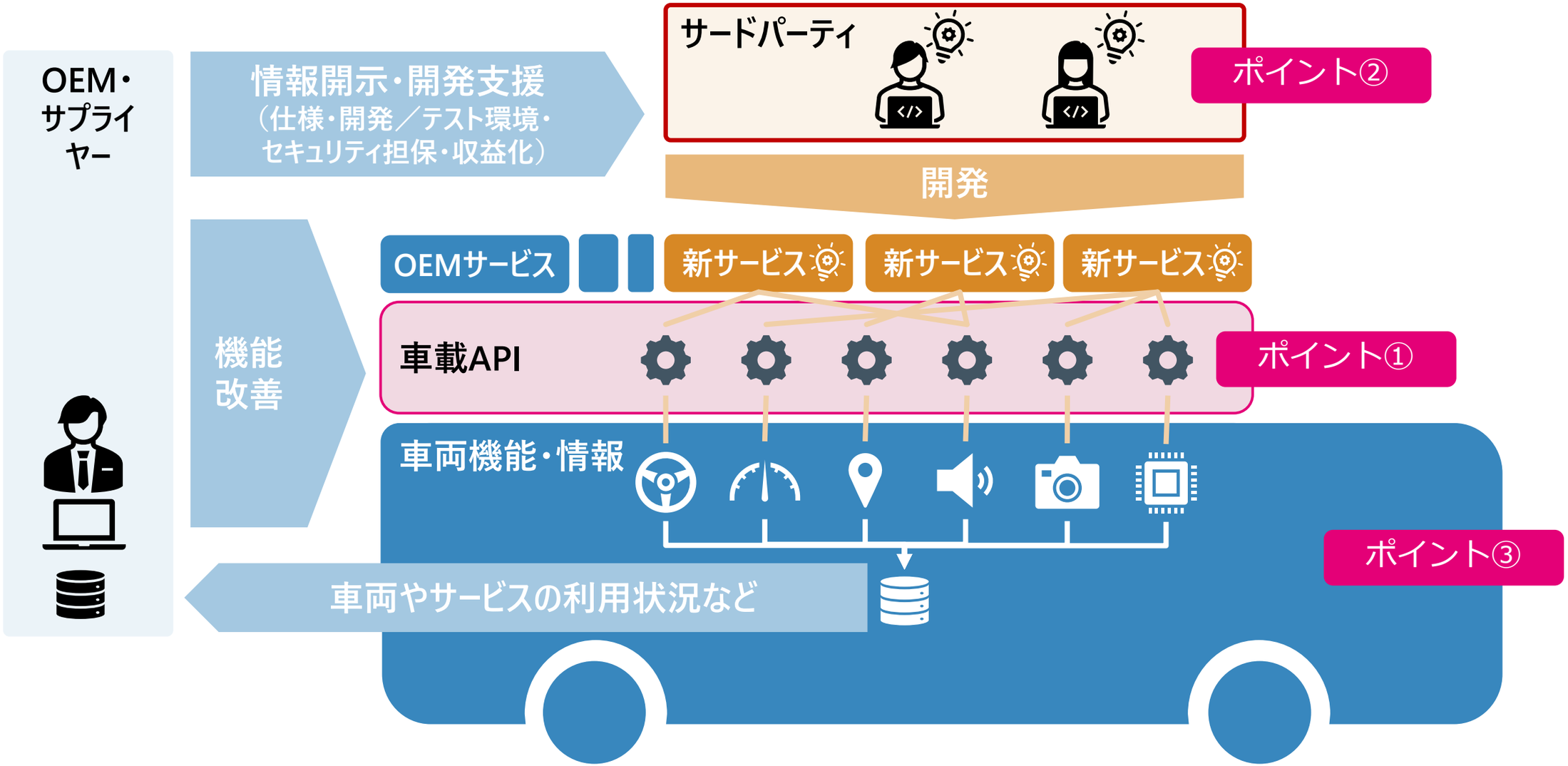
下流（ペンテスト、PSIRT）での対応は引き続き重要な要素

03 SDV（Software Defined Vehicle）による変化

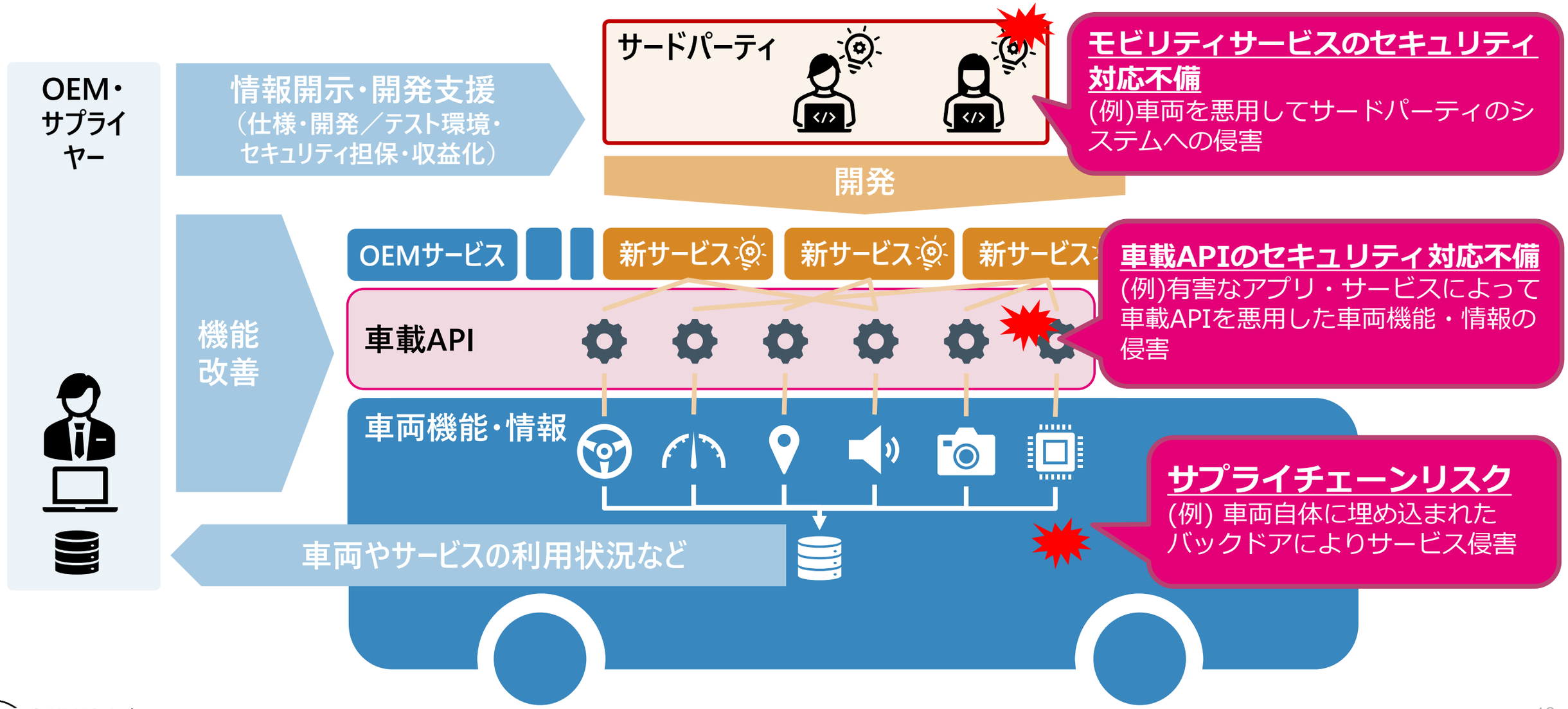
SDVによってクルマに求められる価値や市場の変化に柔軟に対応していくことが可能になる



SDVではサードパーティの参入を促し、新たなモビリティサービスを創出
車載APIの整備、様々な車両とサービスの組み合わせが柔軟に行える環境の登場



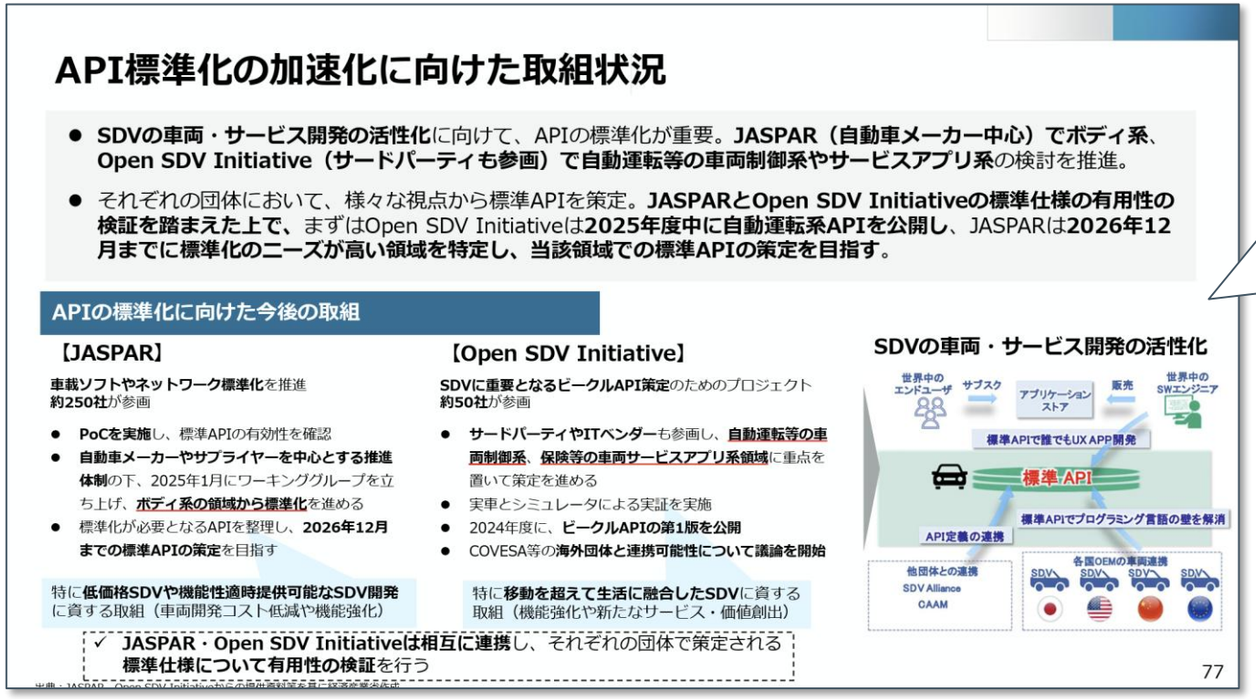
SDVによる変化によって新たな脅威への考慮が必要になる
特に従来のサイバーセキュリティ対応ではカバーできない領域が重要



04 車載APIにおけるサイバーセキュリティ

SDVのキーテーマにAPI標準化が掲げられている

標準化団体による車載APIの標準化が進行中



API標準化の加速化に向けた取組状況

- **SDVの車両・サービス開発の活性化**に向けて、APIの標準化が重要。**JASPAR（自動車メーカー中心）でボディ系、Open SDV Initiative（サードパーティも参画）で自動運転等の車両制御系やサービスアプリ系**の検討を推進。
- それぞれの団体において、様々な視点から標準APIを策定。**JASPARとOpen SDV Initiativeの標準仕様の有用性の検証を踏まえた上で、**まずはOpen SDV Initiativeは**2025年度中に自動運転系APIを公開し**、JASPARは**2026年12月までに標準化のニーズが高い領域を特定し、当該領域での標準APIの策定を目指す。**

APIの標準化に向けた今後の取組

【JASPAR】

車載ソフトやネットワーク標準化を推進
約250社が参画

- **PoCを実施**し、標準APIの有効性を確認
- **自動車メーカーやサプライヤーを中心とする推進体制**の下、2025年1月にワーキンググループを立ち上げ、**ボディ系の領域から標準化**を進める
- 標準化が必要となるAPIを整理し、**2026年12月までの標準APIの策定**を目指す

特に**低価格SDVや機能性適時提供可能なSDV開発**に資する取組（車両開発コスト低減や機能強化）

【Open SDV Initiative】

SDVに重要となるピークルAPI策定のためのプロジェクト
約50社が参画

- **サードパーティやITベンダー**も参画し、**自動運転等の車両制御系、保険等の車両サービスアプリ系領域**に重点を置いて策定を進める
- 実車とシミュレータによる実証を実施
- 2024年度に、**ピークルAPIの第1版を公開**
- COVESA等の**海外団体と連携可能性について議論を開始**

特に**移動を超えて生活に融合したSDV**に資する取組（機能強化や新たなサービス・価値創出）

✓ **JASPAR・Open SDV Initiativeは相互に連携**し、それぞれの団体で策定される**標準仕様について有用性の検証**を行う

SDVの車両・サービス開発の活性化

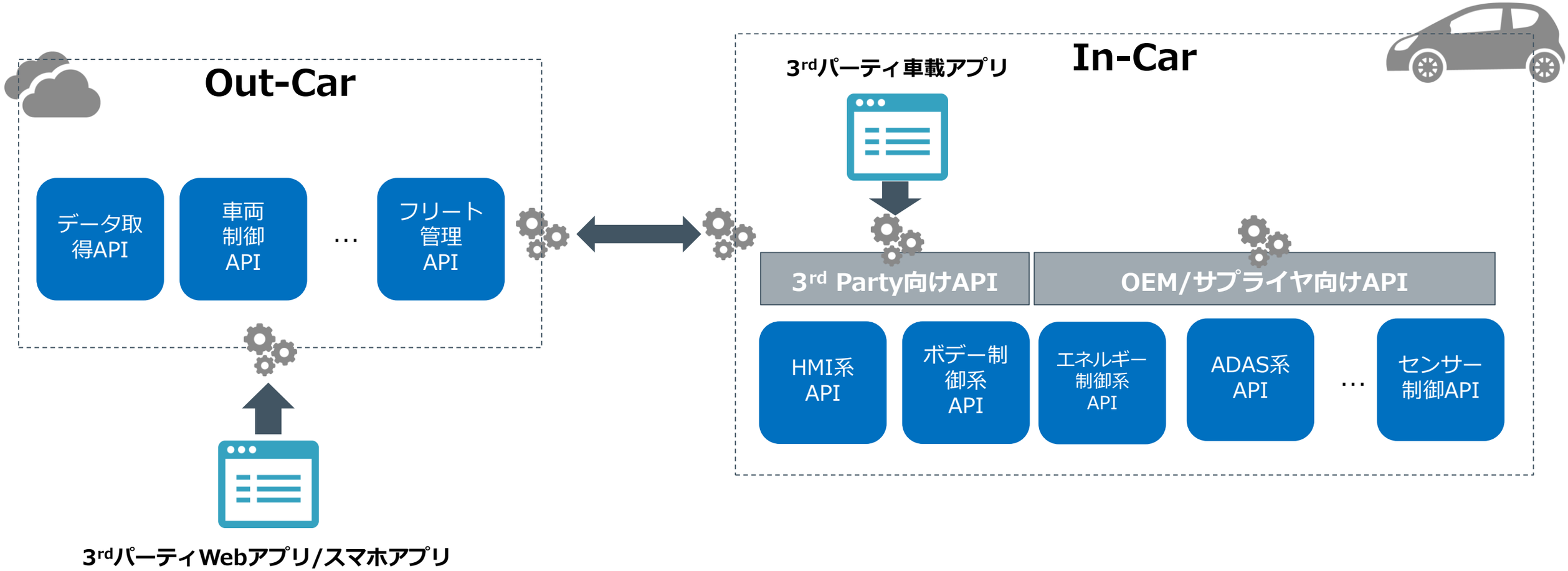
77

「グローバルのSDV日系シェア3割」の目標の実現に向けた取組を強化していく中で、SDVによる**モビリティサービス開発の活性化**を目的として車載APIの標準化が進められている

(引用) 経済産業省 製造産業局 自動車課 モビリティDX室/国土交通省 物流・自動車局 技術・環境政策課
『「モビリティDX戦略」2025年のアップデート』2025年6月9日
https://www.meti.go.jp/policy/mono_info_service/mono/automobile/jido_soko/pdf/mobilitydxsenryaku2025.pdf

車載APIの標準化は広範囲に渡り策定が進められている

将来的には3rd Partyアプリ向けのAPIも公開され新たなモビリティサービスの登場が期待される



車載APIを標準化・公開することでどのような脅威・リスクが想定されるか？

3rd Partyへの公開は様々な脅威・リスクを想定した準備が必要になる

リバースエンジニアリングによる情報漏洩
・開発ツールに機微情報を含めない
・専用の開発環境の提供

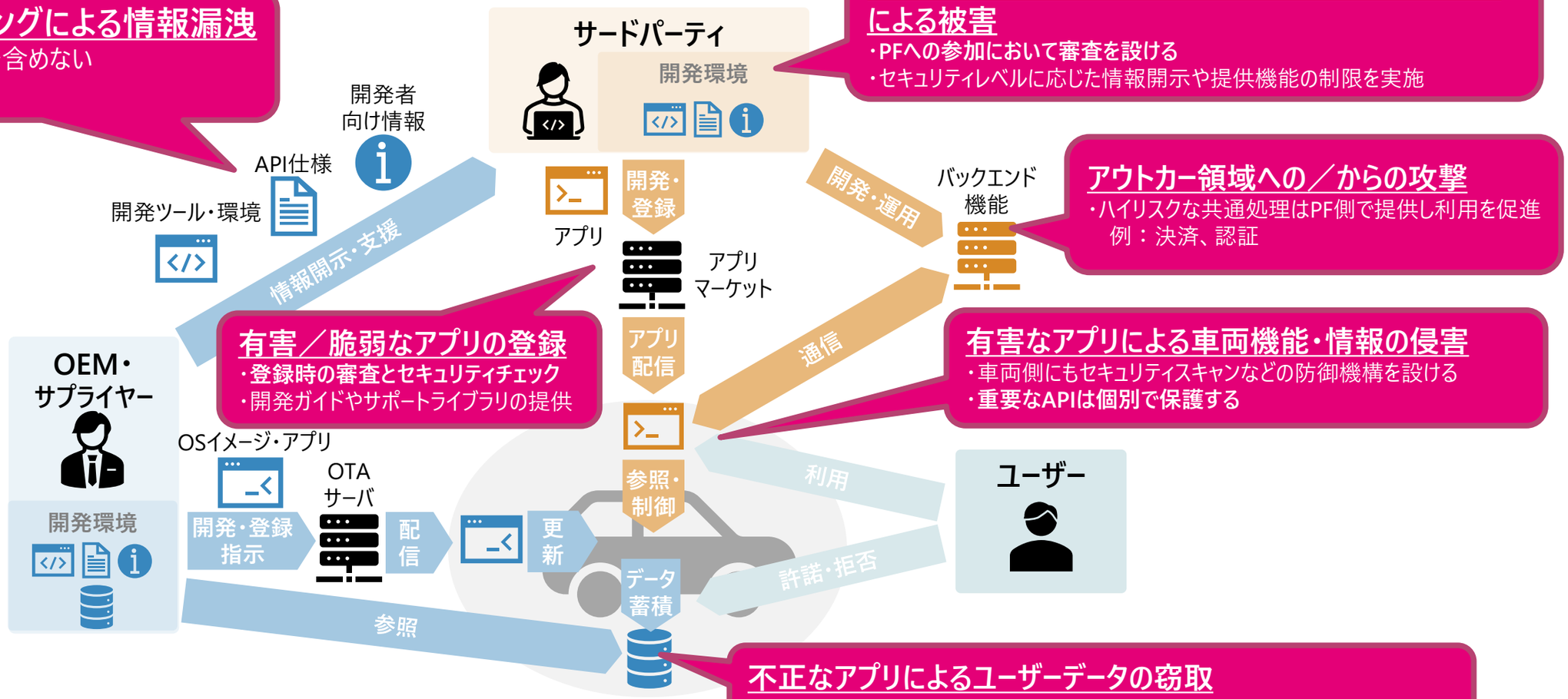
サイバーセキュリティ対策不十分なサードパーティの参入による被害
・PFへの参加において審査を設ける
・セキュリティレベルに応じた情報開示や提供機能の制限を実施

アウトカー領域への／からの攻撃
・ハイリスクな共通処理はPF側で提供し利用を促進
例：決済、認証

有害／脆弱なアプリの登録
・登録時の審査とセキュリティチェック
・開発ガイドやサポートライブラリの提供

有害なアプリによる車両機能・情報の侵害
・車両側にもセキュリティスキャンなどの防御機構を設ける
・重要なAPIは個別で保護する

不正なアプリによるユーザーデータの窃取
・プラットフォームで暗号化する機能を提供しセキュア領域に格納する機能を提供

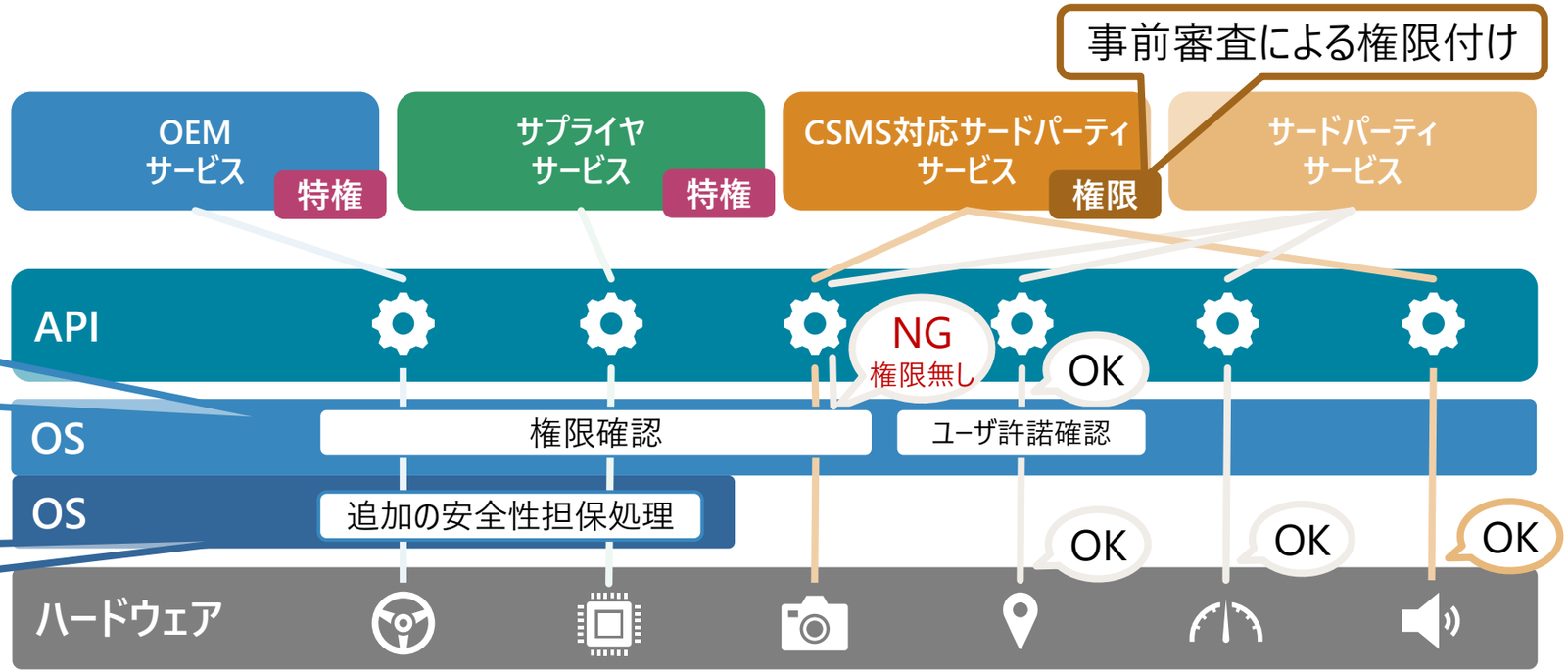


SDVプラットフォームにおいて車載APIを保護する必要がある

アプリケーション署名、ユーザ許諾、事前審査などAPIの種別に応じて保護機構を決定する

APIが提供する機能の重要度に合わせて処理を追加し不正利用を制限

必要に応じて安全対策を別のレイヤーで追加



悪用・誤用時の影響

	API機能	ハンドル制御	自動運転制御	リアカメラ参照	現在地参照	車速参照	スピーカー再生
車両影響	安全	重大	重大	ー	ー	ー	軽微
	経済	重大	重大	軽微	ー	ー	ー
	運用	重大	重大	重大	ー	ー	ー
	プライバシー	ー	ー	中程度	重大	ー	ー
APIカテゴリ		要特権	要特権	要CSMS認証	要ユーザ許諾	無条件	無条件

3rdパーティ製アプリを公開するためにはマルウェアのような有害なアプリではないのか審査や公開後も継続的な処置が必要

アプリ審査

アプリストア

アプリ

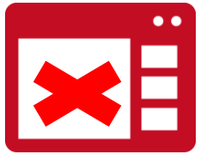
プライバシー侵害
ランサムウェア
バックドア
不正請求
…

アプリ公開後の処置

アプリストア

アプリ公開後に有害なアプリと判明したら…

公開停止・削除



有害アプリ

除名措置

違反アプリサプライヤ

05 自動運転サービスにおけるセキュリティ

2030年度には1万台の自動運転サービス車両の普及が指針となった
ドライバー不足などの社会課題の解決が急務

(引用)国土交通省 物流・自動車局 技術・環境政策課「自動運転の普及・拡大に関する取組」令和8年1月29日
https://www.mlit.go.jp/jutakukentiku/house/content/001979064.pdf

主な自動運転サービス

タクシー

ロボットタクシーとして北米、中国などでは既にサービス展開。国内でもサービス開始に向けて実証実験中。

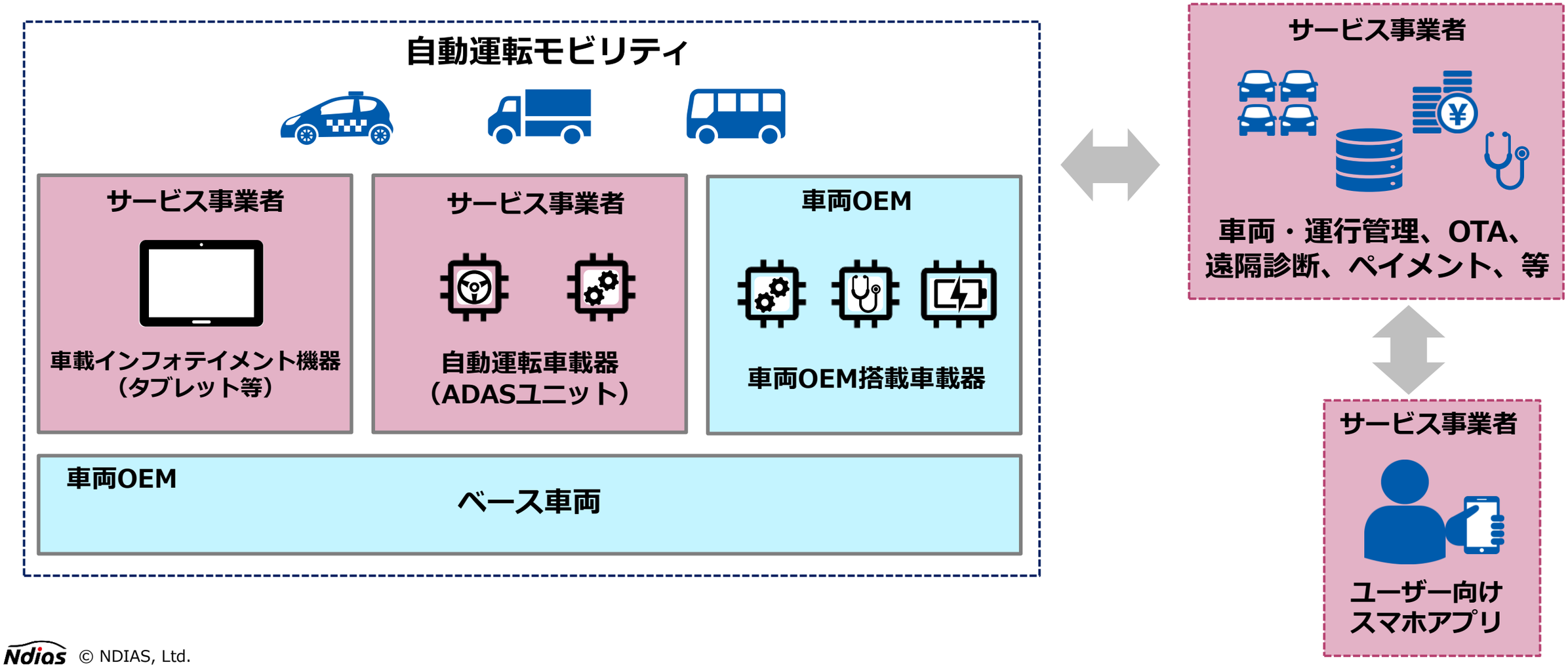
路線バス

各地方自治体にて自動運転バスの実証実験が活発に行われている。

配送トラック

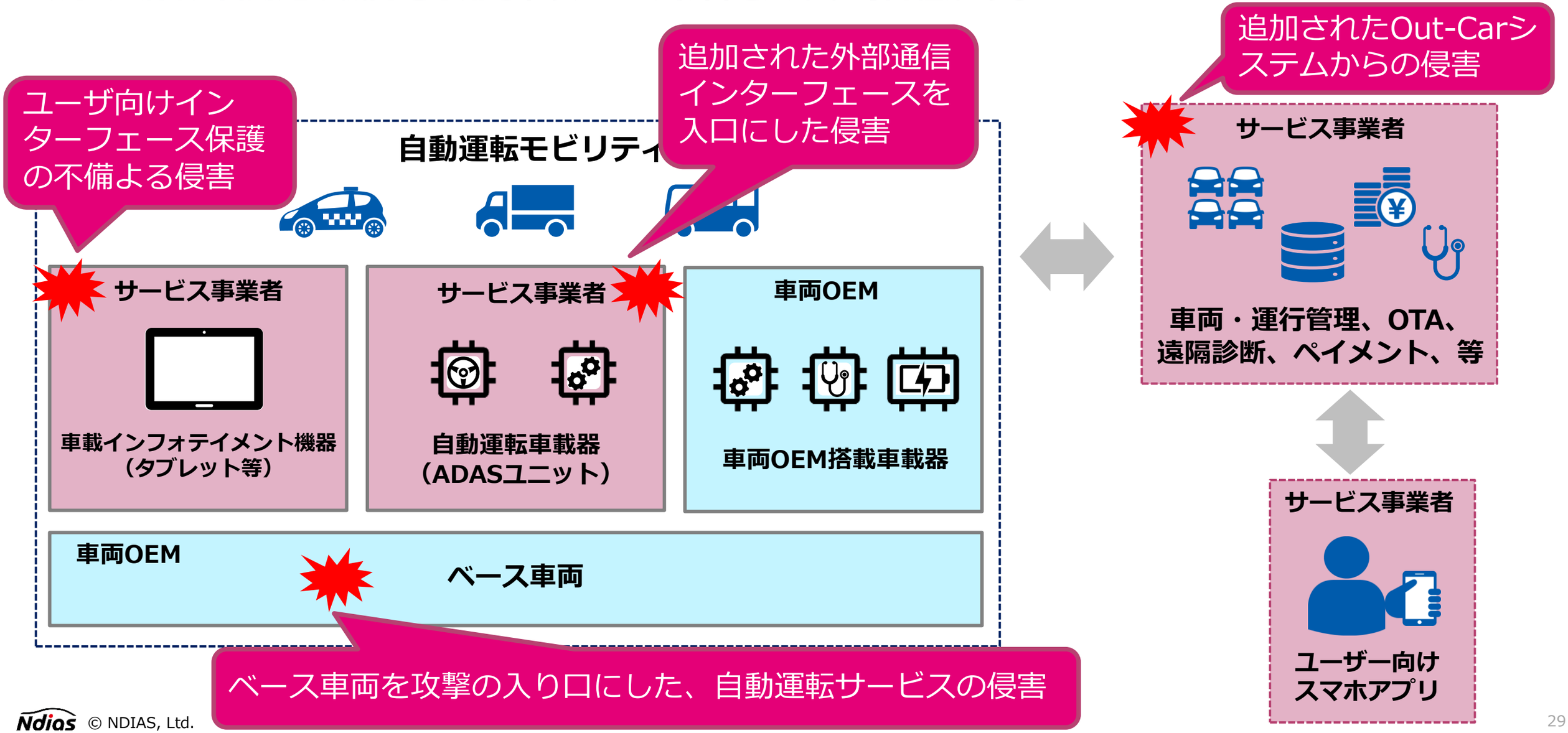
高速道路や専用道路の区間を**自動運転トラックによる幹線輸送サービス**の準備が進んでいる。

サービス事業者が主体となる場合、自動運転サービスは独自機能をベース車両に追加で搭載する構成

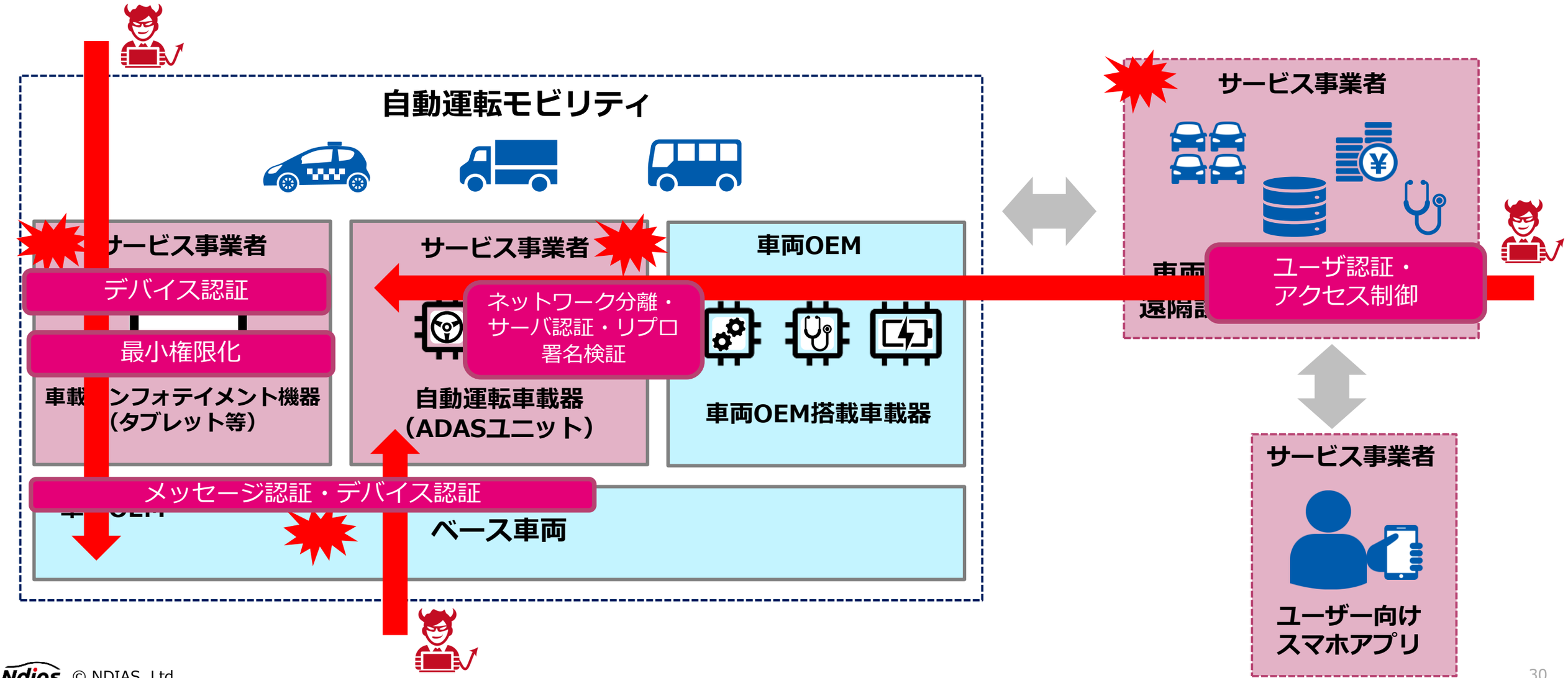


サービス事業者は独自に用意したシステムを中心にサービス全体のセキュリティ対応が必要

最悪の場合、自動運転機能を悪用され安全への影響を及ぼす可能性がある



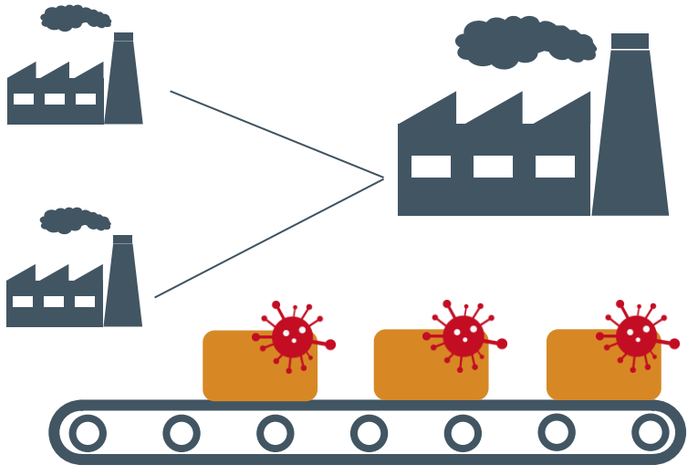
ベース車両に依存するのではなく提供サービス視点を軸としたリスクアセスメント、セキュリティ対策の導入が重要



06 モビリティサービスにおけるサプライチェーンリスク

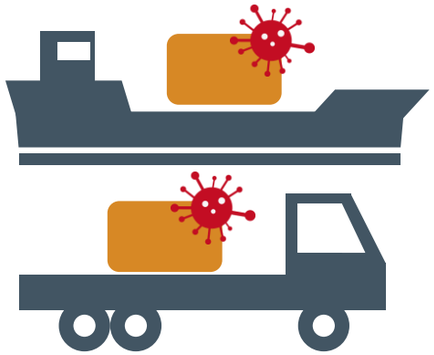
IoT機器調達におけるサプライチェーンリスクとは？

①IoT機器の開発・製造



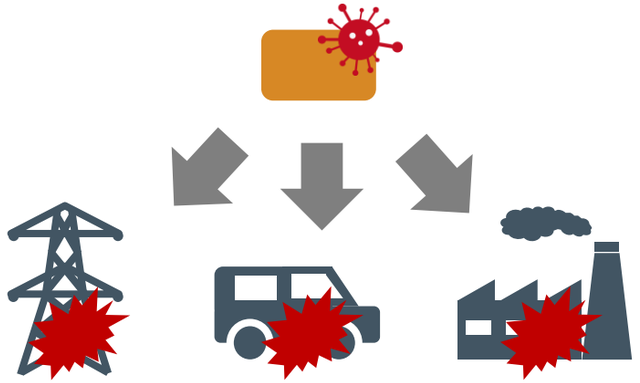
IoT機器の開発・製造過程でバックドアや悪用可能な脆弱性が混入

②出荷・輸送



脆弱な機器が出荷、輸送される

③調達側による使用・運用



調達側が自社設備等に組み込んだ後、攻撃者によってバックドアや脆弱性が悪用される

モビリティサービスにおいてもサプライチェーンリスクが顕在化しています

社会のデジタル化によりIoT機器がインフラを含む社会基盤に浸透し、サイバー攻撃の入り口（外部との接点）が増大

ノルウェーの公共交通機関運営会社が自社で採用するYutong製EVバスが遠隔制御されるリスクがあることを公表しています。

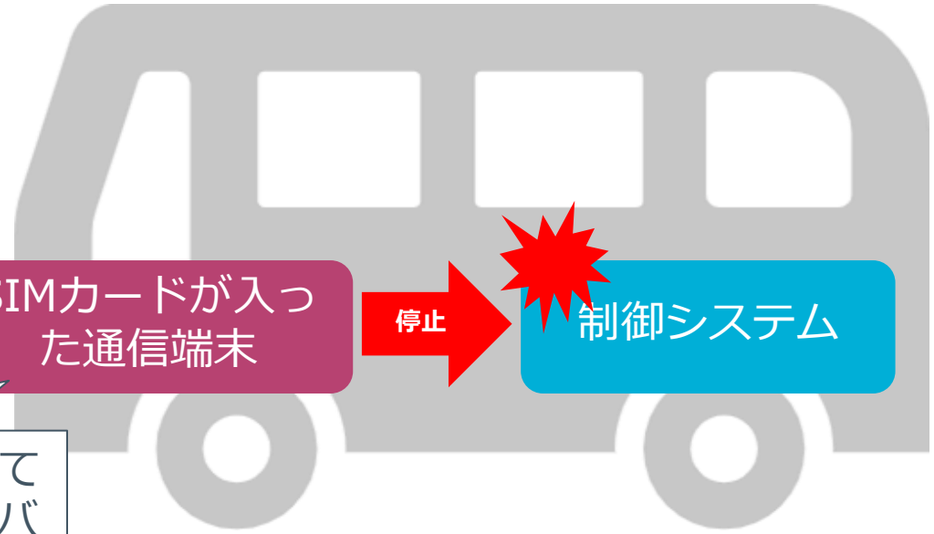
We have conducted a comprehensive safety test of electric buses

We have conducted a test of two electric buses in an isolated environment inside a mountain. The purpose was to uncover risks associated with electric buses.

（引用）https://ruter.no/en/ruter-with-extensive-security-testing-of-electric-buses

遠隔制御

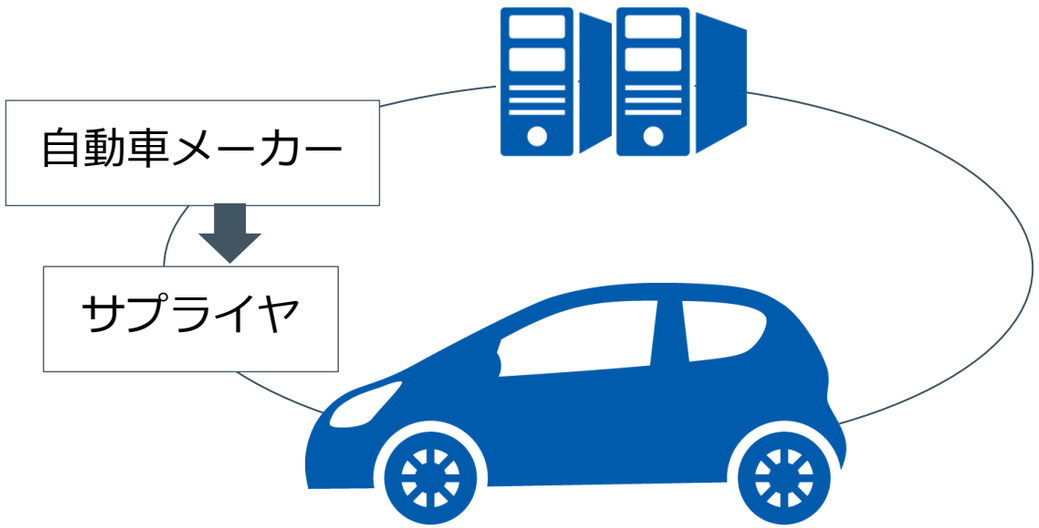
Yutong製EVバスにおいて特定されたリスク



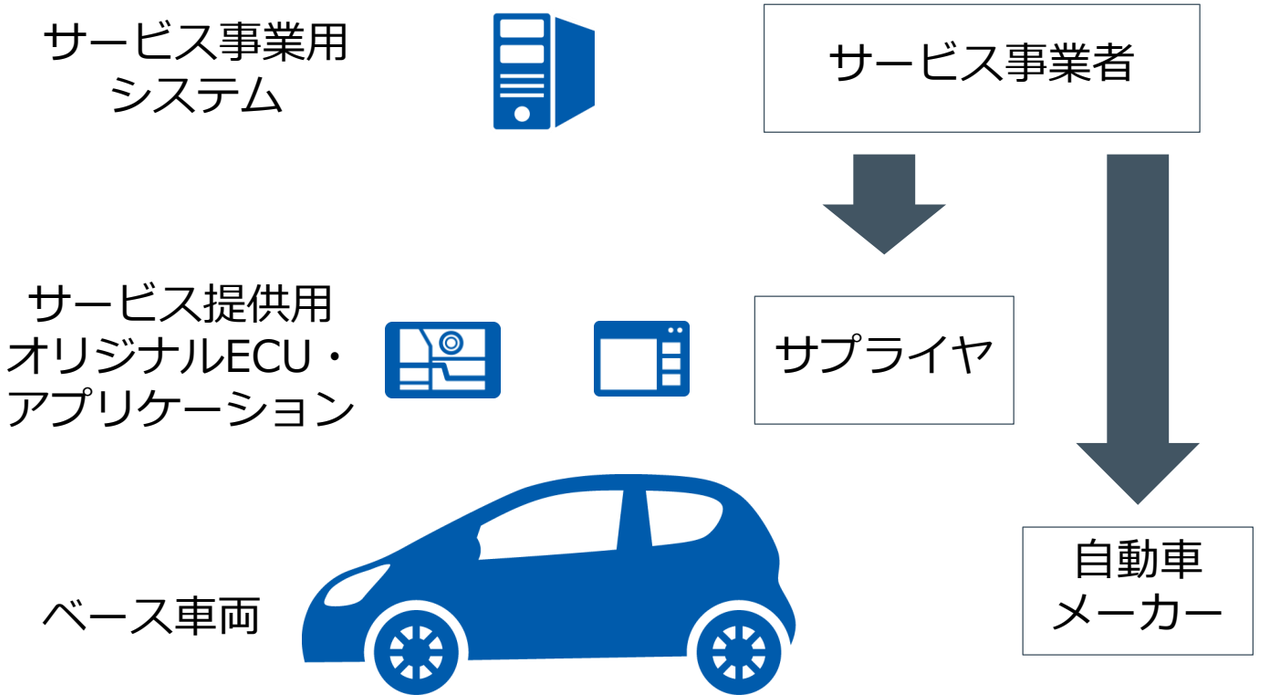
公共交通機関運営会社は認識していないSIMカードで通信するデバイスが搭載されていた

モビリティサービス提供における構造変化による影響

従来

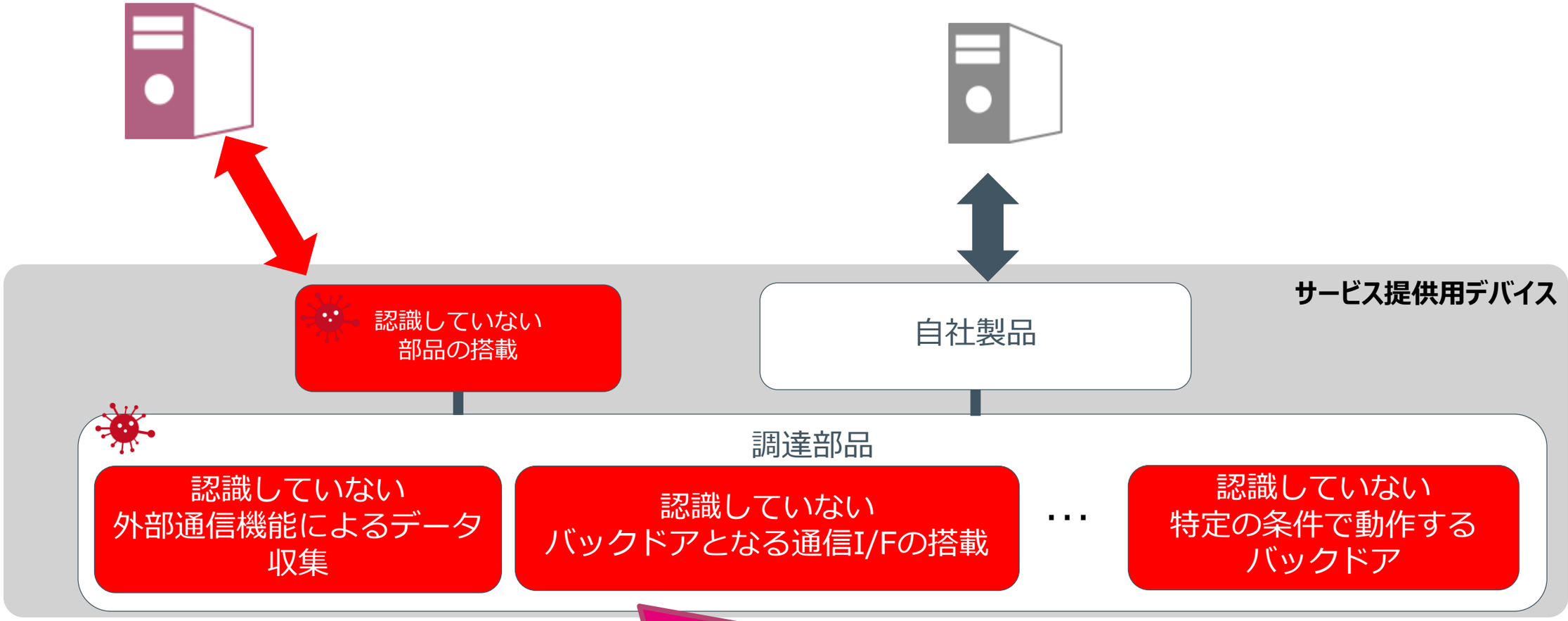


新たな形態



自動車（デバイス）に詳しくないサービス事業者が機器調達する中にサプライチェーンリスクの可能性

調達側が認識していない、意図していない機能・動作が存在し、悪用される可能性がないか確認することが必要

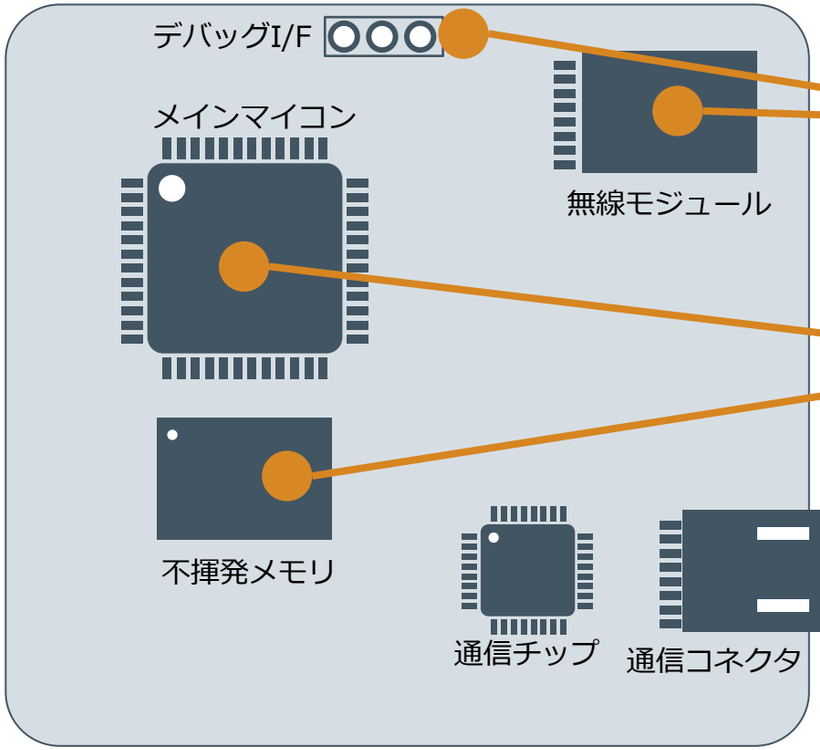


いずれも表層的な受入検査だけでは検出することは困難

実効性のある受け入れ検査としてセキュリティ視点での検査も必要

調達契約時にリバースエンジニアリングを含むセキュリティ検証する権利を確保することも重要

各デバイスの内部構造イメージ



評価観点	評価内容の例
ハードウェア	基板調査により、デバッグ用のI/Fが残存していないか、不審な通信モジュールが無いか等
ソフトウェア	ファームウェアのリバースエンジニアリングによって、仕様上は存在しない未公開機能が無いか、特定の条件で発動するバックドアが無いか等
通信	通信キャプチャの解析により仕様にない宛先への通信が発生していないか等

まとめ

SDV時代に重要なセキュリティ対応

車載APIにおける サイバーセキュリティ	API保護機構の導入、アプリ審査と運用後の継続的な対応、セキュリティ機能API
自動運転サービスにおける サイバーセキュリティ	ベース車両に依存しない、サービス軸でのセキュリティ対応
サプライチェーンリスクへの対応	調達側が認識していない、意図していない機能・動作が無いか確認することが重要


Ndias