経済産業省

自動走行システムにおける サイバーセキュリティ対策

2019年6月26日
自動走行ビジネス検討会

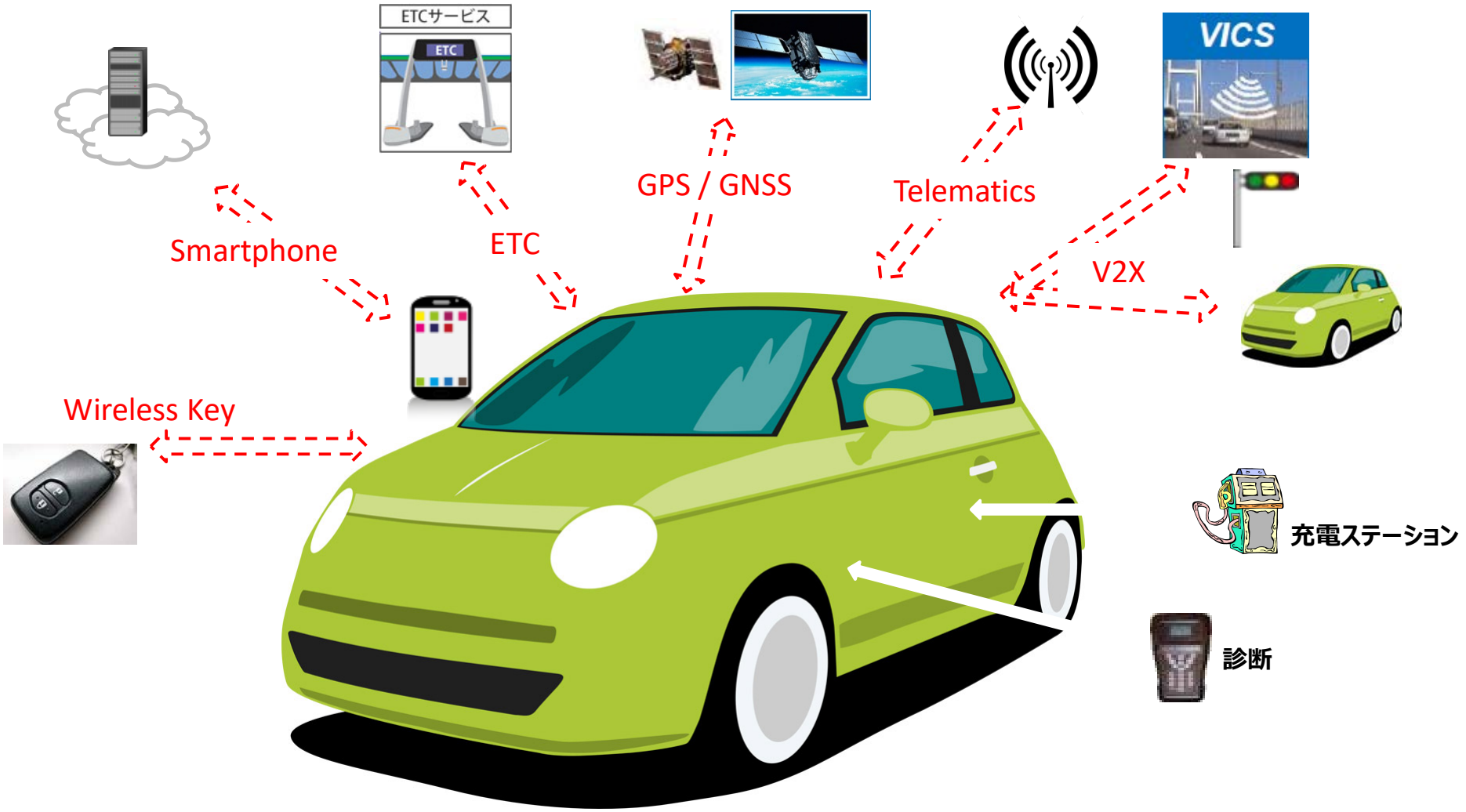
経済産業省

０．導入
１．現状の検討体制
２．ルール戦略
３．海外動向
４．技術開発・ガイドライン策定
５．運用面の取組
６．人材育成の取組

0．自動走行システムにおける外部通信リスク

- 2020年代前半に市場化が想定されている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。

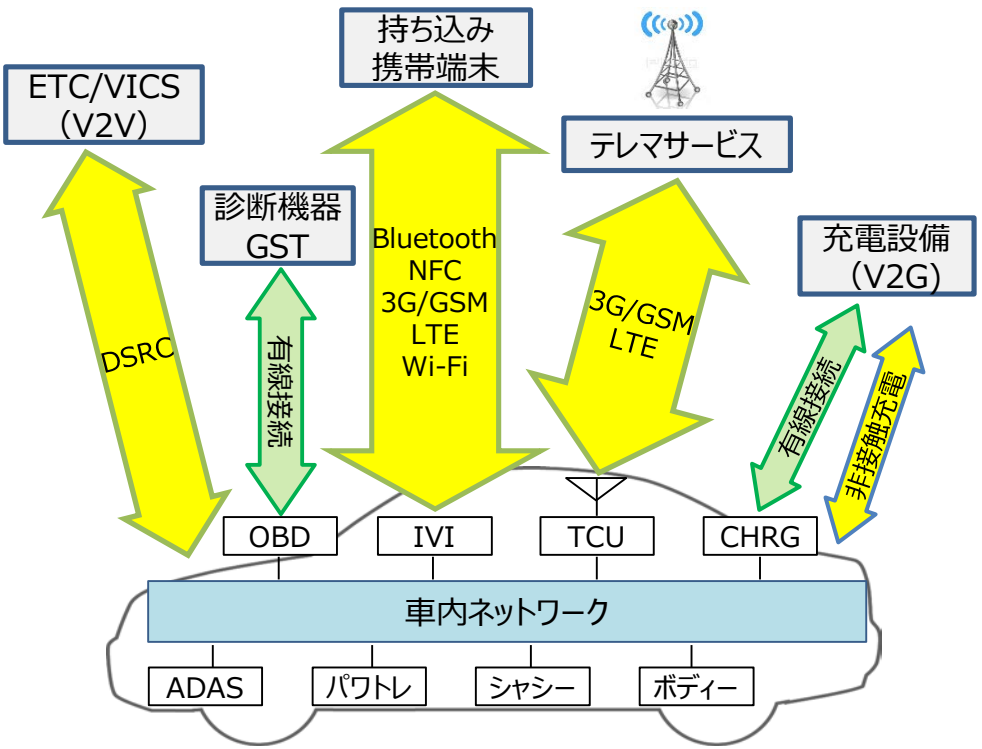
自動車は、多くの通信（無線：破線・有線：実線）で外部と繋がっていく



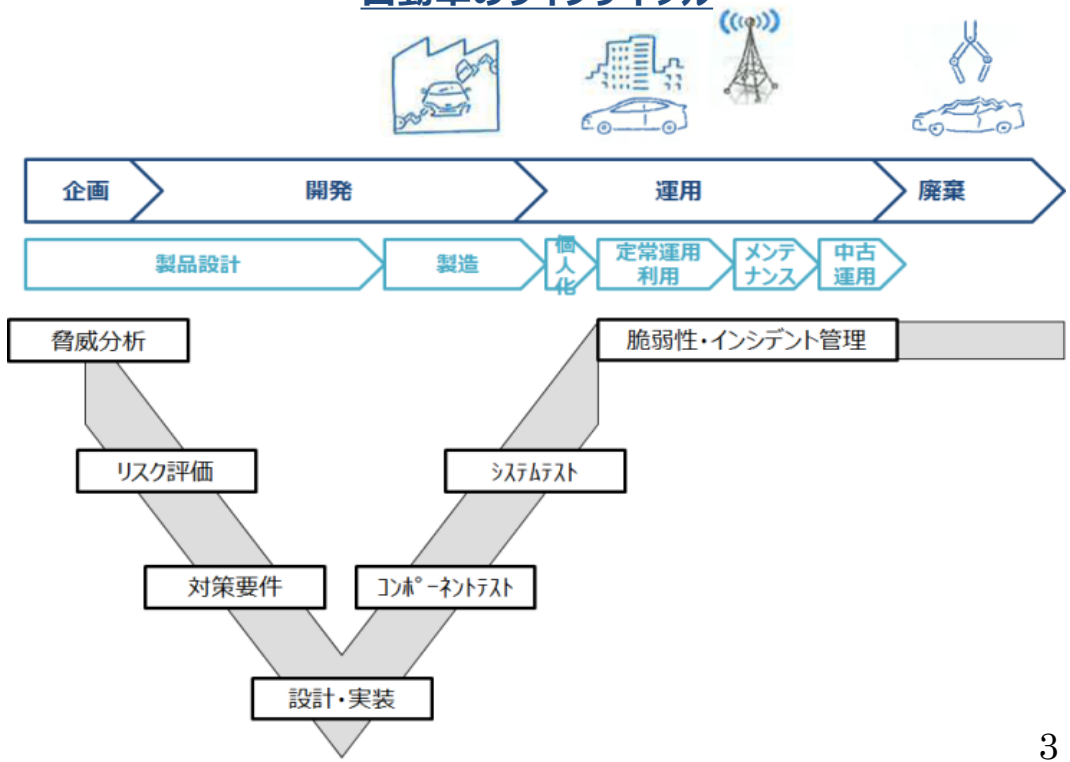
0．自動車におけるサイバーセキュリティ対策の方針

- 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**。
- 単なるセキュリティレベルの向上は**コスト増**になるため、**販売価格とのバランスを考慮した製造**が求められる一方、指標が未整備。
- そのため、各研究開発を通して、セキュリティ要件を整理した上で、ルール（基準・標準）化によりグローバルな商品化を図りつつ、**業界としてガイドラインの策定が必要**となり、①**設計・開発・運用時の安全に係る妥当性を担保**し、②**個社毎の対策レベルのバラツキを防止**することによる業界全体としての対策レベルの向上や信頼の確保を図る。
- 「車両外部からのサイバー攻撃への対応等、自動走行の安全性を確保する車載セキュリティについて、国際的に共通な開発プロセス、安全性評価の仕組み作りを進めるための工程表を本年度中に取りまとめ、人材育成を含め官民連携した取組を加速する。（未来投資戦略2017）」を踏まえ、**自動走行ビジネス検討会**において、取組方針をとりまとめている。

自動運転・コネクテッドにより生じる通信セキュリティリスク

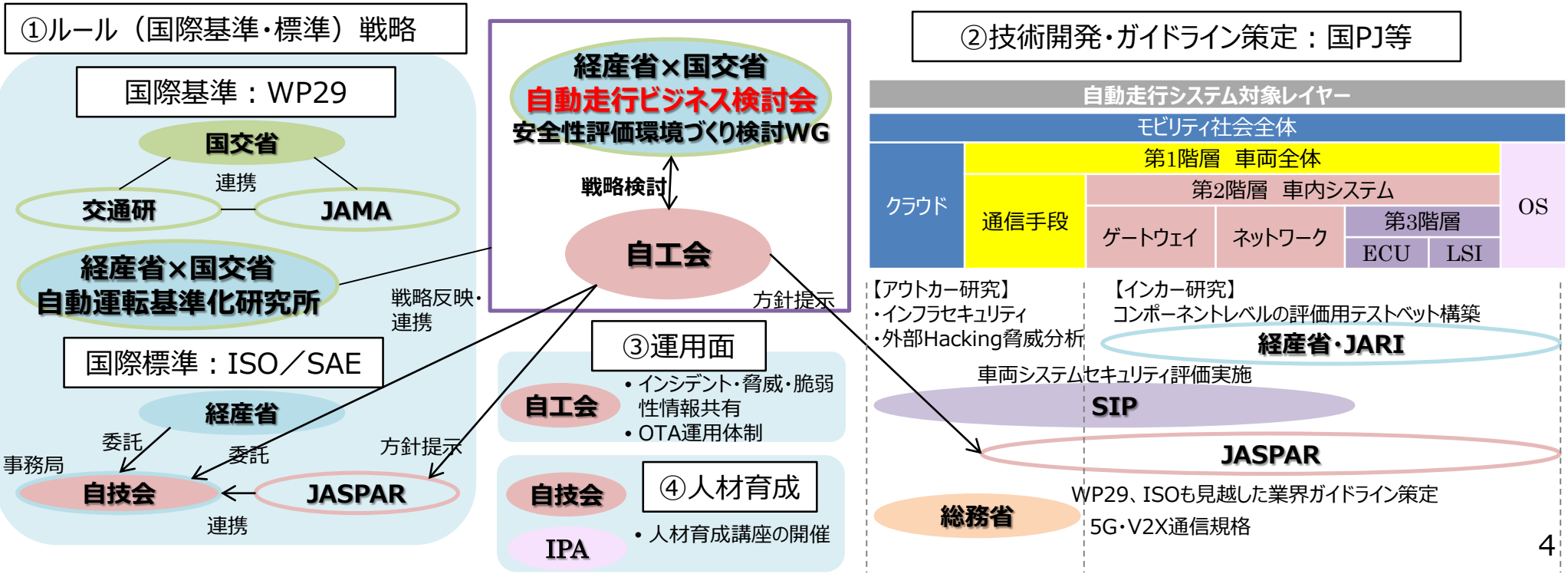


自動車のライフサイクル



1．現状の検討体制

- 自動車サイバーセキュリティについては、①**ルール（国際基準・標準）戦略**、②自動走行システムのレーヤーを網羅した形での脅威分析、セキュリティ要件、対策、評価等に関する②**技術開発・ガイドライン策定**、③**運用面での体制構築**、④**人材育成**を柱に実施。
- ①業界として、**国際基準（WP29）は日本自動車工業会（JAMA）、国際標準（ISO／SAE21434）は自技会が主体となって提案**しているとともに、他国提案に対しても意見を出し自国産業が不利とならないよう議論を進めている。また、**自動運転基準化研究所において　ルール（基準・標準）戦略を議論**。
- ②**内閣府SIP-adus、経産省、国交省、総務省と多岐に渡る省庁で研究開発**が行われている。SIP-adusは、大規模実証で車外通信からのWhite Hat Hackingを実施し、車両への車外からの攻撃に対する評価ガイドラインを作成。日本自動車研究所（JARI）は、JasParユースケースをもとに車内システムにおける脅威分析（脅威体型化・制御への影響・対策技術）、要件を整理。これら取組を踏まえ、**JasParにおいて、OEM、サプライヤーが実施する評価ガイドラインを業界協調で策定する方針**。
- ③サイバーセキュリティに関するインシデント情報を共有するため**JAMAにおいてJ-Auto-ISAC WGを設置**。
- ④産学官が連携した人材育成講座や人材育成プログラムを実施。



１．検討体制（協調領域の特定）

- 自動走行車両がハッキングされた場合、重大な事故を招くおそれがあり、重要インフラ分野として位置づけられている「情報通信」、「金融」、「航空」、「鉄道」、「電力」等と同様の高度な対策が必要と認識。

- レベル3以上の自動走行車は、商品化されておらず、また、先端的な技術を含んでいること、及び各自動車会社で電子制御システムが異なりかつ進化も早いことから、協調領域と競争領域を設定し、取組を進めている。

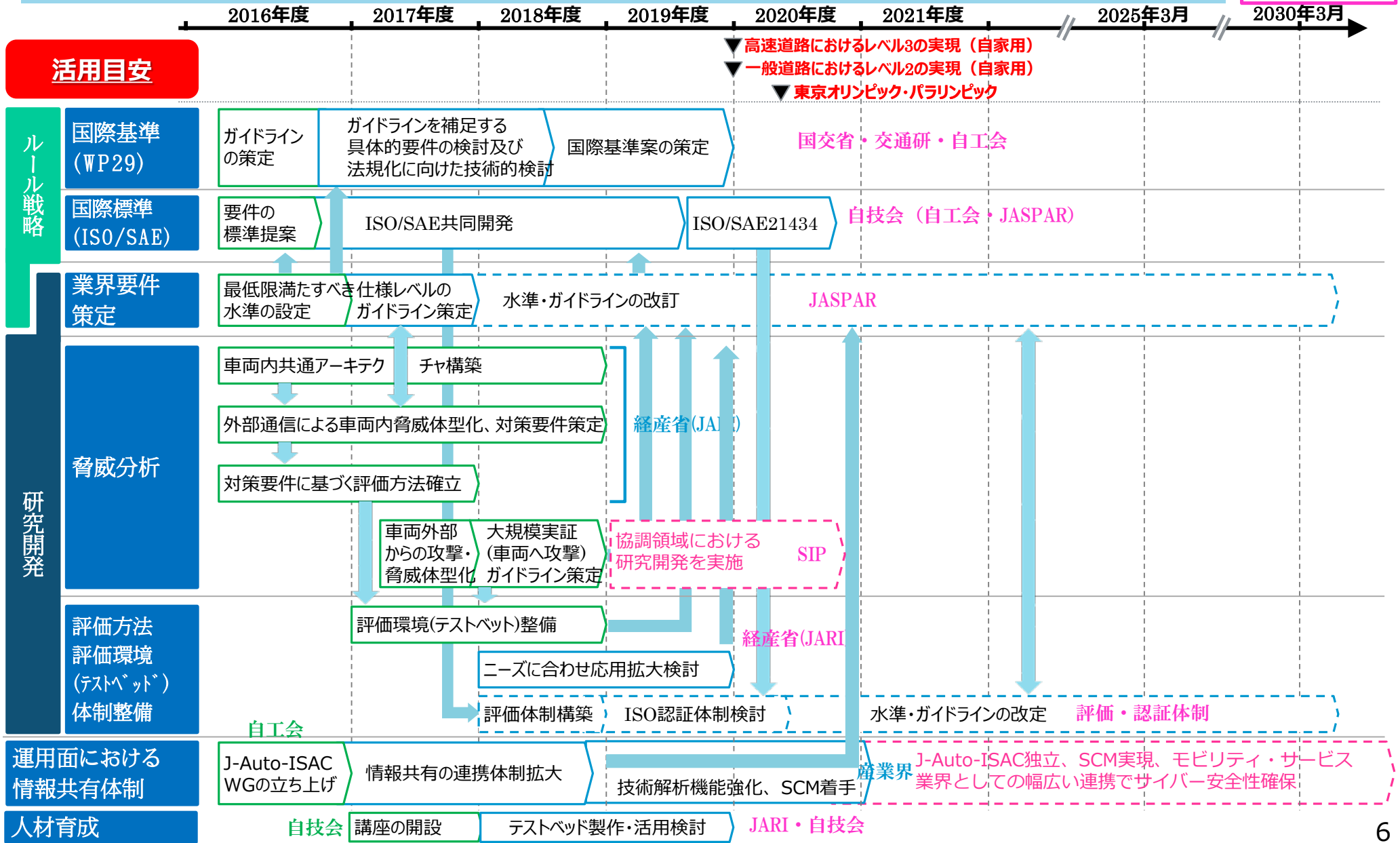
- 特に下記を協調領域として官民で推進中。
  ① 中小サプライヤーや研究機関が共同で脆弱性分析を進めるための評価環境（テストベッド）整備
  ② 安全設計のための多層防御設計、開発プロセス標準化
  ③ 運用面における情報共有体制の構築
  ④ 不足するサイバーセキュリティ人材の育成推進

- 競争領域として自動車各社は、以下の取組を推進中。
  ① 各社の電子制御システムに基づく脆弱性分析を進めるための評価環境（テストベッド）整備
  ② 標準化された設計・開発プロセスを踏まえた独自の安全設計

1．検討体制（工程表）

完了
取組中・取組方針
取組中・取組方針（新規）

実現したい姿・取組方針
- 安全確保のための開発効率を向上させるため、開発・評価方法の共通化を目指す。2018年度に評価環境（テストベッド）を構築し、2019年度中に活用方策を検討。今後、情報共有体制の強化やサイバーセキュリティフレームワークの検討を進める。



1．＜参考＞産官学の役割分担のイメージ

- 課題として最低限確保すべきセキュリティ水準がなく自動車業界でどこまで対応すればよいか不明確。自動運転、コネクテッドカーの安全を確保した上で市場投入することが求められる。
- 確保すべきセキュリティ目標を決定した上で①評価水準、②最新の脆弱性の研究、③担う人材育成の体制を構築し各社どこまでリソース投入してよいか相場観を形成することが必要。

自動車セキュリティにおける産官学の役割分担のイメージ

①業界内での最低限確保すべき水準の設定

- 目標値（評価基準）を設定した主体に発生する責任問題。
- 認証・評価を行う目的の明確化

→ 最低限守るべき水準を決めて必要な技術・人員のリソースを明確化。

- 決定した水準以上の対策は各社競争

②最新の脆弱性の研究

- 脅威が進化するなか、既存または新規評価ツールですべてカバーできない問題。

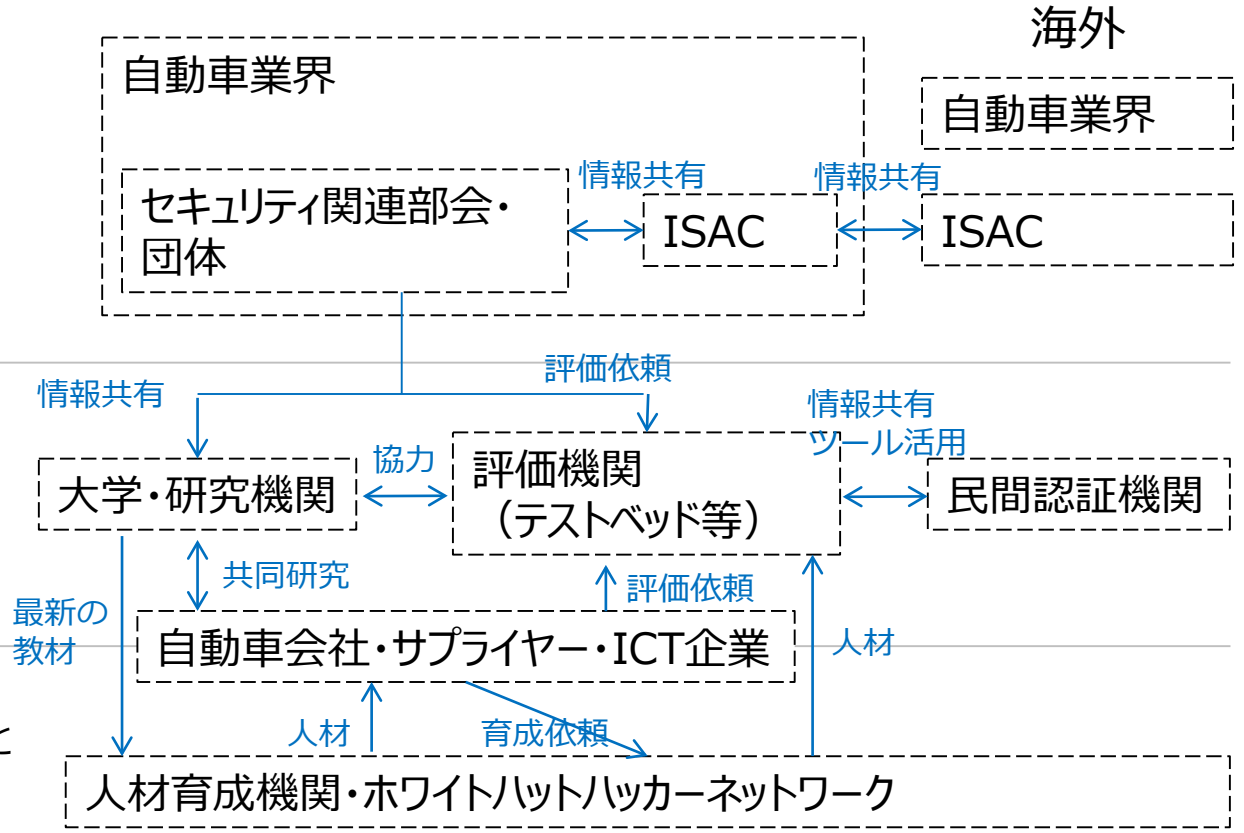
→ 最新の脆弱性に関する継続的な研究

→ 効率的な情報共有体制

③人材育成

- 各社製品開発・評価担当のレベルアップとホワイトハットハッカーとのネットワーク形成

→ 公共財的にセキュリティ対策に貢献する人材に



＊各レイヤでレベル合わせ必要

１．サイバーセキュリティ部会(一般社団法人　日本自動車工業会　電子情報委員会)

- 日本の自動車業界として対象のセキュリティフレームワーク、ガイドライン、実現レベルを定め、活用を推進することで、適切なセキュリティ対策の実施を図る

  ◆対象範囲（車載に関連する部分を除く）

  - 部品やサービス/ソフトウェアのサプライチェーン
  - 個社工場における設備や設備保守
  - “クルマやお客様”と”個社を含むサービス提供者”をつなぐシステムや提供するサービス及びデータ

個社の実施レベル測定と最適化

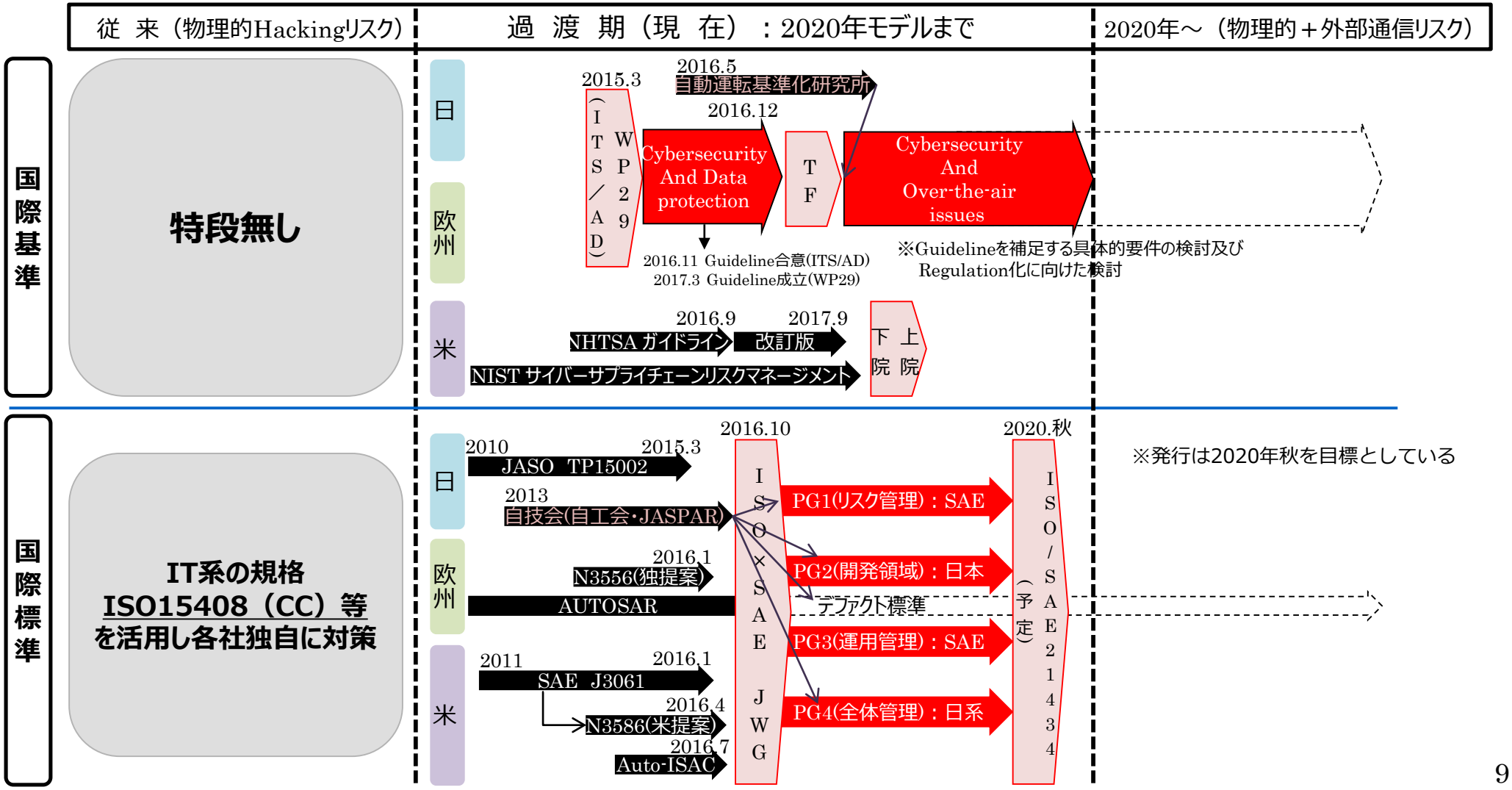
＜メンバー構成＞
日本国内の乗用車、二輪車、商用車生産の14社

＜開催状況＞
サイバーセキュリティ部会　4月16日(火)、5月10日（金）開催　今後月に一度程度、開催予定

＜進め方＞
　国内外のフレームワークやガイドライン、国際標準規定をベースに、自動車業界のリファレンスとなるガイドラインの策定を行う

2．ルール（国際基準・国際標準）戦略

- これまで、セキュリティに係るルールはなく、2020年頃に発売するモデルについては、IT系の規格を参考に個社で対応してきた。
- 国際基準については、Recommendation案及びRegulation案の議論が進められている。
- 最近、各国で自動車も含めたセキュリティのガイドラインが多数示され始めており、必要な要件を自工会・自技会・JASPARで精査を進めるとともに、設計要件を含む開発プロセスに関する国際標準について、ISO／SAE　JWGにおいて、各国と議論を進めている。

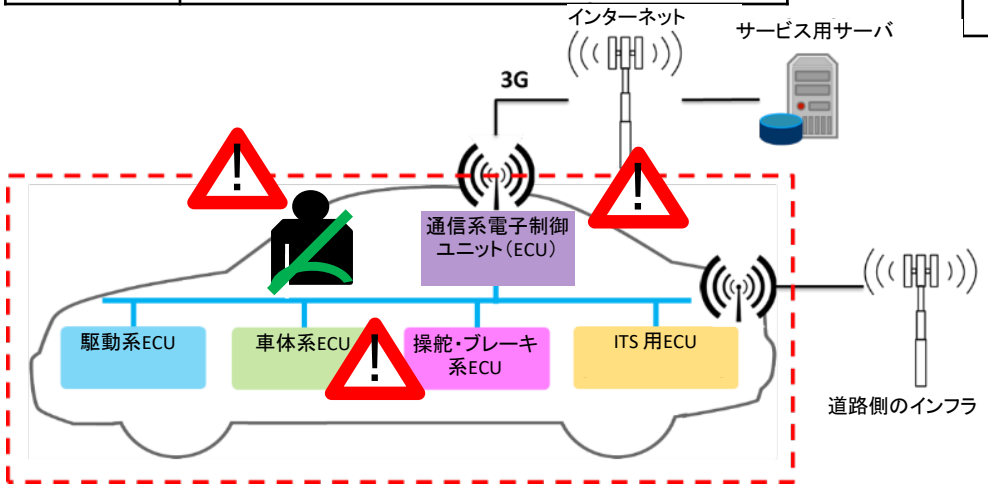


2．国際基準の動向について

- 国連WP29サイバーセキュリティタスクフォース（議長：日本及び英国）においては、自動運転車を含めた通信機能を有する自動車の開発・実用化状況を踏まえ、これらの自動車について、**サイバーセキュリティを確保するための要件**等を定めた**国際基準案を審議中。**
- 早ければ、**2019年度後半にも国際基準を策定予定**。

脅威の例	・意図せず不正なソフトウェアを導入しよう　とするユーザ
	・簡易な暗号鍵を長期間使用するような不適切なシステム設計
	・なりすましによるメッセージの不正（V2X、GPS通信等）

対応策の例	・車両システムへのアクセスを制御する
	・ソフトウェア及び構成について、セキュリティを評価・認証し、完全性を保護する
	・受信するメッセージの認証を行う



- ✓ **車両の重要機能（走る・曲がる・止まる）に対するリスクを低減**
- ✓ **万が一、リスクが顕在化した場合においても、車両を安全に停止させる等制御が可能**

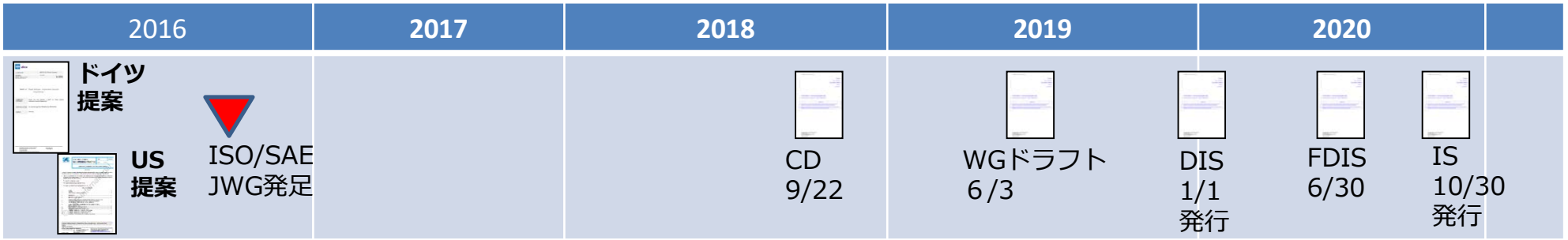
2．国際標準（ISO21434）について

- 車のライフサイクル全般にわたるサイバーセキュリティ要件を定めたエンジニアリング規格。 ISO／SAEのジョイントWGにより、国際標準化を推進。WP29のサイバーセキュリティ基準から引用される規格となる見込み。
- 我が国の自動車業界は、協調して安全設計に取り組むとともに、経済産業省及び国土交通省と連携しながら、設計要件を含む開発プロセスの国際標準について、ISO／SAE　JWGの場で開発プロセスのPGの議長ポストを確保し、議論を主導。

規格の構成

・リスク管理手法（PG1）
　リスクの管理を行うために必要な手法の定義。資産分析、脅威分析、リスク評価を実施する際の要件を定義
・開発プロセス（PG2）
　車の企画段階から開発完了までに必要なサイバーセキュリティ活動の要件を定義。コンセプト、システム、ハードウェア、ソフトウェアの車特有の水平分業に適応
・生産、運用、廃棄（PG3）
　開発完了から廃棄までに必要なサイバーセキュリティ活動の要件を定義。脆弱性情報の収集、インシデント対応、インシデント対策、廃棄時の要件が含まれる。
・サイバーセキュリティ管理（PG4）
　車のライフサイクルに関連するサイバーセキュリティ管理要件、組織のサイバーセキュリティ戦略を確立するための、組織固有のルール、プロセスの要件を定義

規格のタイムライン



CD：Committee Draft　委員会原案
DIS：Draft International Standard　国際規格案
FDIS：Final Draft International Standard　最終国際規格案
IS：International Standard

（参考）安全設計のための多層防御設計

- 外部通信による冗長性確保のための補助的情報について、情報が得られない場合、又は情報がなりすまされた場合であっても安全を確保する多層防御、フェールセーフ設計が進められている。

＜通常＞

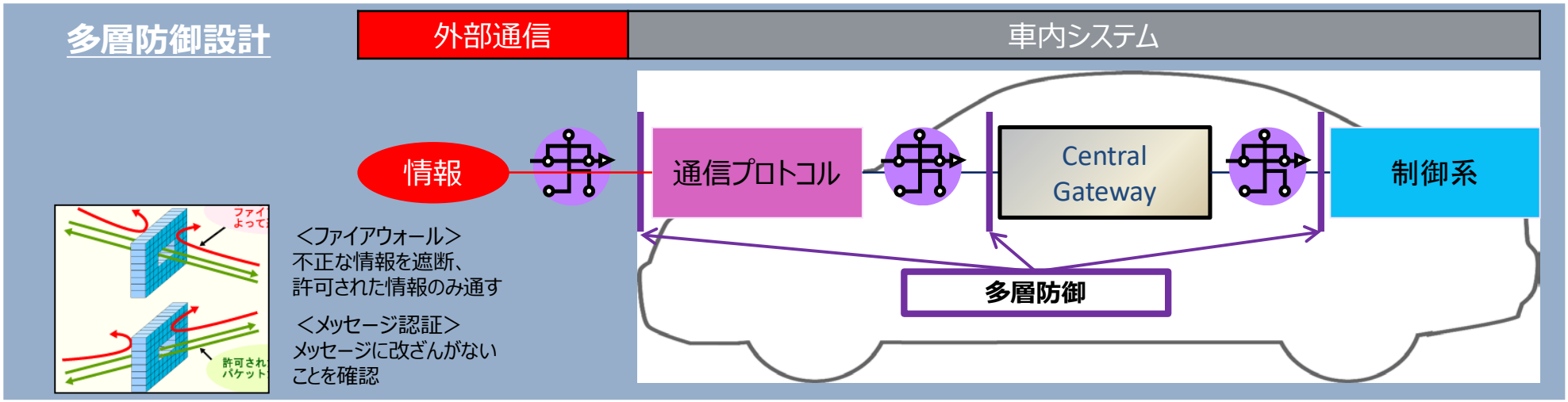
外部通信情報 ○ **通常に走行**

＜外部通信がなりすまされた場合＞

外部通信情報 → **車両システムがすぐに異常を検知し、センサー情報を基に安全確保（安全に車両が停止）**
※センサー情報を優先

＜外部通信からの情報が得られない場合＞

外部通信情報 × **通常に走行**
or
センサー情報を基に安全確保（安全に車両が停止）
※センサー情報を優先



3．海外動向（1／3）

米国

- 2018年11月にNHTSAガイドライン第3版が策定された。法案は、下院では採択されたが上院は不成立。
- SAEと国際標準化は進めているものの、米国内政府の判断により、独自に規制化される可能性がある。

下院規制（Self Driving Act）：2017年9月に採択済

【レベル3以上に関するFMVSS（米国車両基準）の更新】

◆ レベル3以上の開発者は、安全評価書をNHTSAガイドラインに基づく提出義務。

◆ NHTSAは今後5年間のレベル3等の安全基準策定及びリサーチに関する重点計画を作成し、議会に提出・公表。

【サイバーセキュリティ及びプライバシー】

◆ レベル2以上の製造者は、サイバーセキュリティプラン及びプライバシープランを作成（政府当局への提出義務無し）。

上院規制（AV Start Act）：委員会採択にとどまり、上院本会議では不成立

【サイバーセキュリティ】

◆ レベル3以上のメーカーはサイバーセキュリティ計画を策定（当局への提出義務無いが検査権限有）。メーカーは公開可能な概要の作成義務。

◆ 連邦政府機関はレベル3以上のサイバーセキュリティについて協力。運輸長官は消費者向けにサイバーセキュリティに関し情報提供。メーカーはオーナーズマニュアル等で当該情報源を紹介。

【プライバシー】

◆ 運輸省にレベル3以上のデータアクセス委員会を設置し、所有・管理・アクセス等について審議・勧告を議会に提出。会計検査院は、レベル3以上のレンタカー等のレンタル終了の際の個人情報の消去に関する調査を行い、提言を議会に報告。

◆ NHTSAにプライバシーデータベースを設置し、プライバシー情報の扱いを検索できるようにする。

連邦政府（NHTSA）：PREPARING FOR THE FUTURE OF TRANSPORTATION（2018年11月）

連邦政府（NHTSA）：自動運転政策ガイドライン（Federal Automated Vehicles Policy）改訂版発表（2017年9月）

【概要】

◆ メーカー等には12項目の安全性評価書をボランタリーで提出・公表を求める

【車両サイバーセキュリティ】

◆ 脅威や脆弱性リスクを最小限に抑えるために、システム・エンジニアリング手法に基づく堅牢な製品開発プロセスを実施すること。体型的かつ継続的な安全リスク評価を盛り込むこと。

◆ 米国国立標準技術研究所（NIST21）、NHTSA、SAE、米国自動車工業会（AAM）など、参考的ガイダンス・ベストプラクティス設計原則を検討し取入ること。

◆ NHTSAが追跡できるよう、あらゆる行動・変更・設計選択・分析・関連試験含め、ADSに組み込んだ内容を文書化し、更に堅固な文書バーション管理環境を確保すること。

◆ 内部試験・消費者の届出・外部のセキュリティ調査等で判明したあらゆる出来事・悪用・脅威・脆弱性をできる限り早く、Auto-ISACへの加入不加入に関わらず報告すること。更に、堅牢なサイバーインシデント対応計画を立て、設計手順におけるサイバーセキュリティを考慮したシステム・エンジニアリング手法を用いること。脆弱性に関する組織的な報告／開示方針を検討すべき。

【データ記録】

◆ 衝突時の原因究明及び衝突シナリオ防止の研究開発のため、（システムとドライバーのどちらが制御していたか含め）状況を再現できるよう、個人情報を保護しながら、入手可能なデータを全て記録し、検索できるようにすること。NHTSAはSAEと協力し、データ（フォーマット）の統一化を開始する。

連邦政府（NHTSA）：Cybersecurity Best Practices for Modern Vehicles（2016年10月）

3．海外動向（2／3）

独

- WP29、ISO21434における検討をメインにルール戦略を進めている。
- 個人情報やプライバシーについては、日本よりも厳しく、改正道路交通法ではデータ処理について規制。

改正道路交通法（2017年6月施行）：セキュリティ関連の新設規定抜粋

第VIa章　自動車内におけるデータ処理

第63a条　高度に自動化又は完全に自動化された運転機能を有する自動車におけるデータ処理

（１）第1a条（高度に自動化又は完全に自動化された運転機能を持つ自動車を定義）に基づく自動車は、運転車とシステムとの間で車両操縦の交代（TOR、故障・性能限界等トラブル含む）があった場合、衛星測位システムによって算出された位置・時刻情報を保存する。

（２）第1項に基づいて保存されたデータは、州法に基づき交通違反の処罰を担当する官庁からの要請に応じ送付されなければならない。送付されたデータは、当該官庁によって保存・利用することが許される。送付されるデータの範囲は、当該官庁が行う調査過程において第1項の確認を行うために不可欠な程度に限られる。個人情報の処理に関する一般規則はこれに影響を受けない。

（中略）

（４）第1項に基づき保存されたデータは、6ヶ月経過後に消去されるものとするが、当該車両が第7条1項で規定された事件に関与していた場合は別であり、この場合、当該データは3年経過後に消去されるものとする。

（５）第7条1項で規定された出来事との関連において、第1項に基づき保存されたデータは、匿名化した形態で事故調査のために第三者に送付することができる。

英国

- WP29において、Regulationを推進。国内にOEMは無いが、認証機関のVCAが民間試験機関（MIRA）と連携。

The Key Principles of Cyber Security for Connected and Automated Vehicles（2017年8月リリース）

BSI PAS 1885:2018 The fundamental principles of automotive cyber security. Specification（2018年12月発行 Principleに関連した事項を記述）

中国

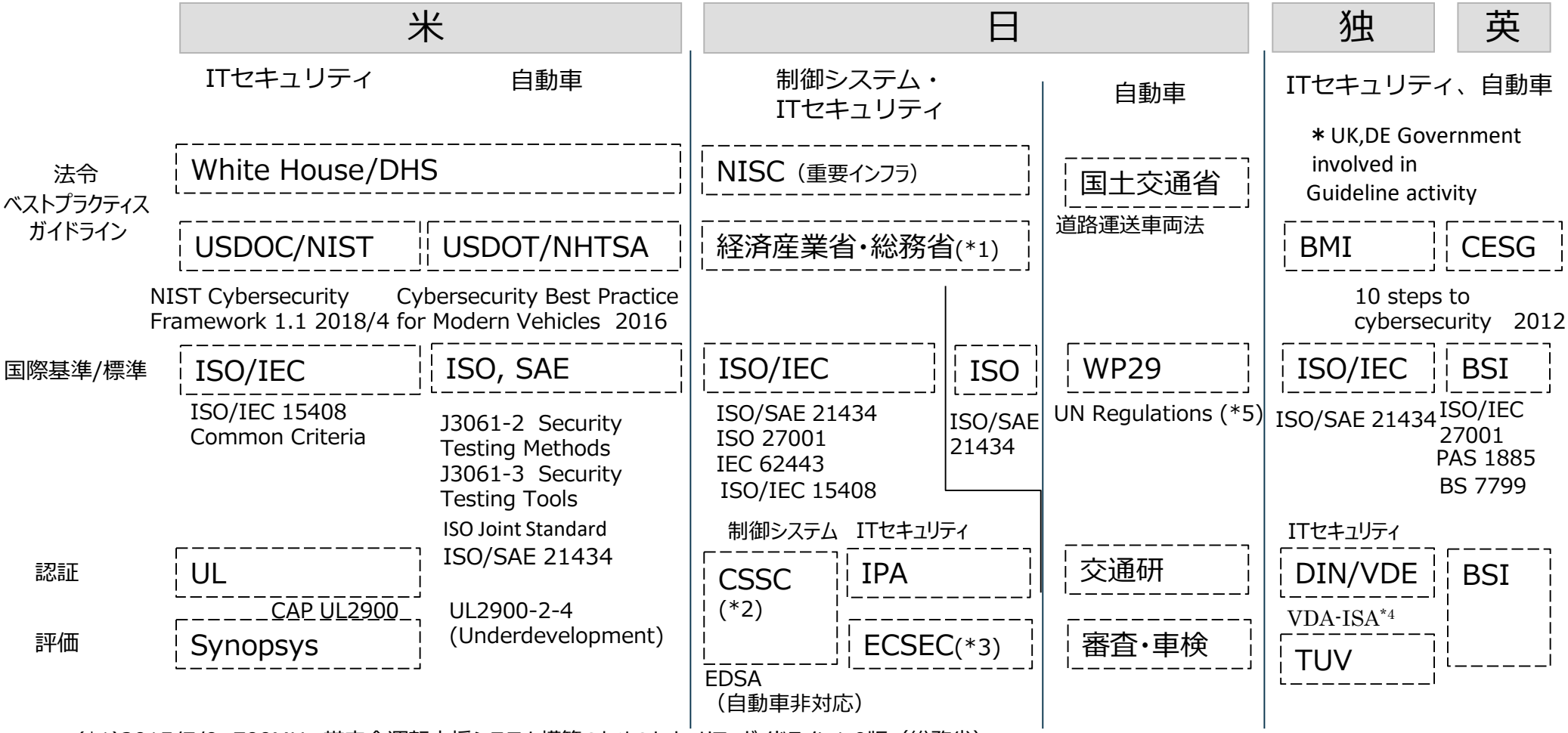
- 工業情報化部　国家標準化管理委員会が、「国家ICV産業標準体系建設指南」政策において、情報安全の国内規格化（14項目（＊））を図る方針。
- 具体的には、①2018年末までに、基礎的技術研究を完了、標準体系を確立、車両の緊急救助・通信セキュリティなどの重点標準体系の建設を制定・整備し、標準に対して試験検証を展開する。また、②2020年までに、5Gサポートのコネクテッドカー産業シリーズ標準の制定を完了し、情報通信セキュリティおよびデータセキュリティなどの標準を更に整備する。

＊情報安全汎用テストと評価方法、ECU・ゲートウェイ・OBDインターフェイスの技術要件、遠隔情報サービス通信安全　など

3．海外動向（3／3）

● 国・政府が方針を打ち出し、各業界で水準を決定し、民間ベースで認証・評価を行う形が主流。

セキュリティの国際標準と評価・認証体制について（関係整理）

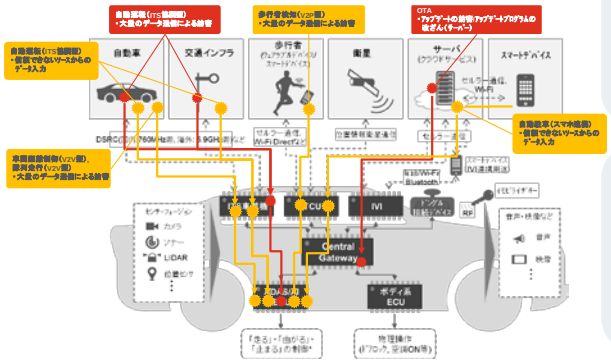


(*1)2015/7/9 700MHz 帯安全運転支援システム構築のためのセキュリティガイドライン1.0版（総務省）
(*2)技術研究組合法 経済産業大臣認可法人
(*3)鉱工業技術研究 組合法 経済産業大臣認可法人 ITセキュリティ評価及び認証制度(JISEC)
(*4)ISO/IEC 27001をベースに、業界の要件を加えた評価基準（Information Security Assessment)
(*5) GRVA（Groupe de Rapporteurs pour les Véhicules Autonomes）で議論が行われている。

4．SIP-adusにおける取組

- 自動走行システムにおける共通モデルを定義し、セキュリティ脅威の全体像を調査・分析。その上で、車両のサイバーセキュリティ防御性能を評価する手法をセキュリティ評価ガイドラインとして策定。OEMが参加する大規模実証実験を通じて、評価手法の妥当性を確認。

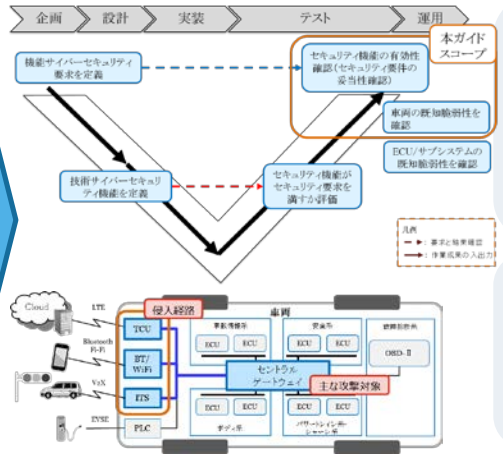
①自動走行システムの脅威分析



【自動走行システム共通 モデル導出】
- 自動運転・コネクテッドカーを調査
- 類型化による自動走行システム共通モデル導出

【脅威の全体像調査】
- 自動走行システム共通モデルに係る車外からの攻撃を含む脅威を抽出
- 脅威影響度を評価し、重大脅威を分析

②セキュリティ評価のガイドライン策定



【セキュリティ評価ガイドライン】
- OEM各社、JasPar等のステークホルダとの議論及び脅威分析の結果を踏まえ、車両開発のV字モデルにおける総合評価などで活用できるガイドラインを策定

【セキュリティ評価の特徴】
- 実際のハッカー（攻撃者）視点での車両外部から侵入テストを実施し、HW/SWのセキュリティ耐性を評価する手法を採用

③国内OEMとの実証実験によるガイドランイン検証

実験参加社募集

OEMに参加依頼
OEM4社より参加応募
OEM4社と契約/機材調整

【実証実験参加社募集】
- 国内OEM4社が参加
- 応募4社と契約/機材等の調整を実施

実証実験成果／評価ガイドライン最終化

【実証実験成果内容】
- 実証実験を通じた評価プロセス整理等の改善を経て、セキュリティ評価ガイドラインを改善・最終化
  ※参加社個社に係る機密情報は匿名化(統計化)

セキュリティ評価（ペネトレーションテスト）の評価プロセス

ガイドライン業界標準化・更新体制

SIP-adus ⟷ JasPar

SIP-adusセキュリティ評価ガイドライン

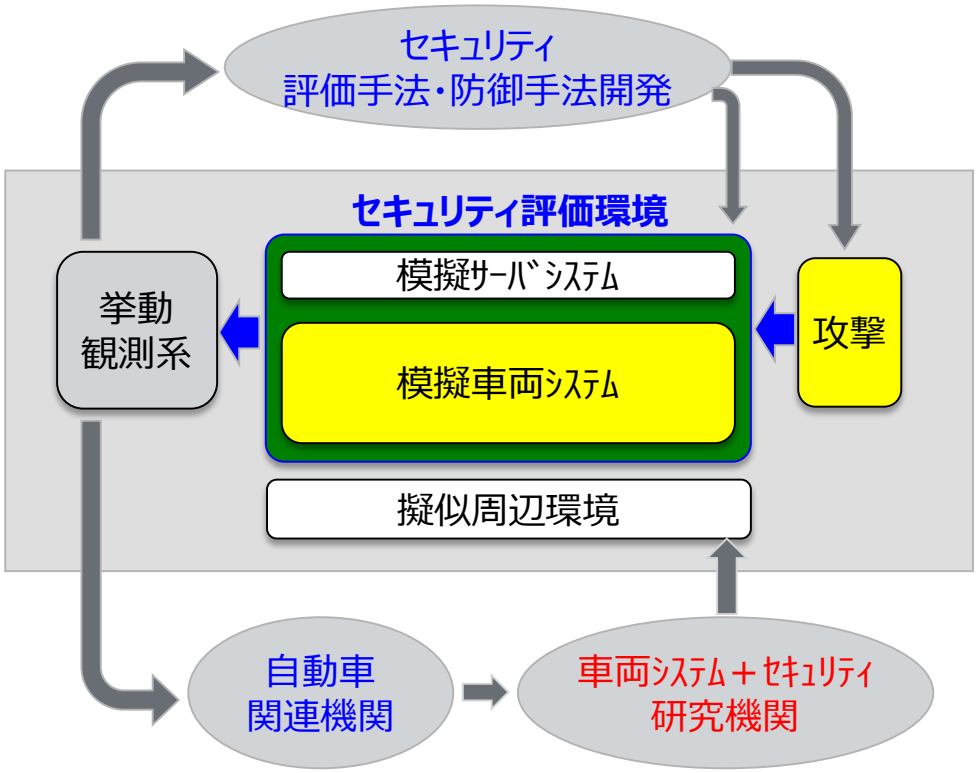
【保守体制/今後の取り組み】
- JasParと、SIP-adusセキュリティ評価ガイドラインの管理・業界活用に関する検討を実施中

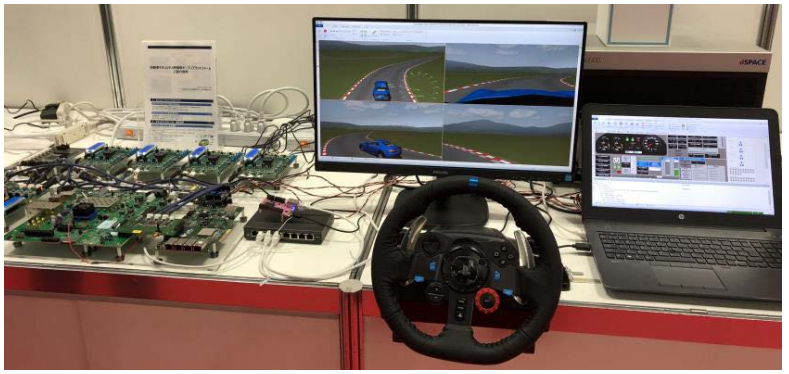
【活動主体】PwCコンサルティング

４．脆弱性分析を進めるための評価環境（テストベッド）整備

- 経済産業省、国土交通省共同プロジェクトにおいて、主として、中小サプライヤー、セキュリティベンダー及び研究機関等が脆弱性評価などを行うことを目的に、車内のコンピューターネットワークを模擬したテストベッドを構築。
  （「高度な自動走行システムの社会実装に向けた研究開発・実証事業」として日本自動車研究所において構築）
- このテストベッドにより、中小サプライヤーなどが自社製品を含む自動走行システムがハッキングを受けた場合の影響を検証する脆弱性評価を実施できるとともに、研究機関等による脆弱性分析や人材育成への活用も期待できる。
- 今後は、利用者が有効にテストベッドを利用できるよう、利用条件の設計等を進めていく必要がある。

テストベッドの活用・利用形態と特長





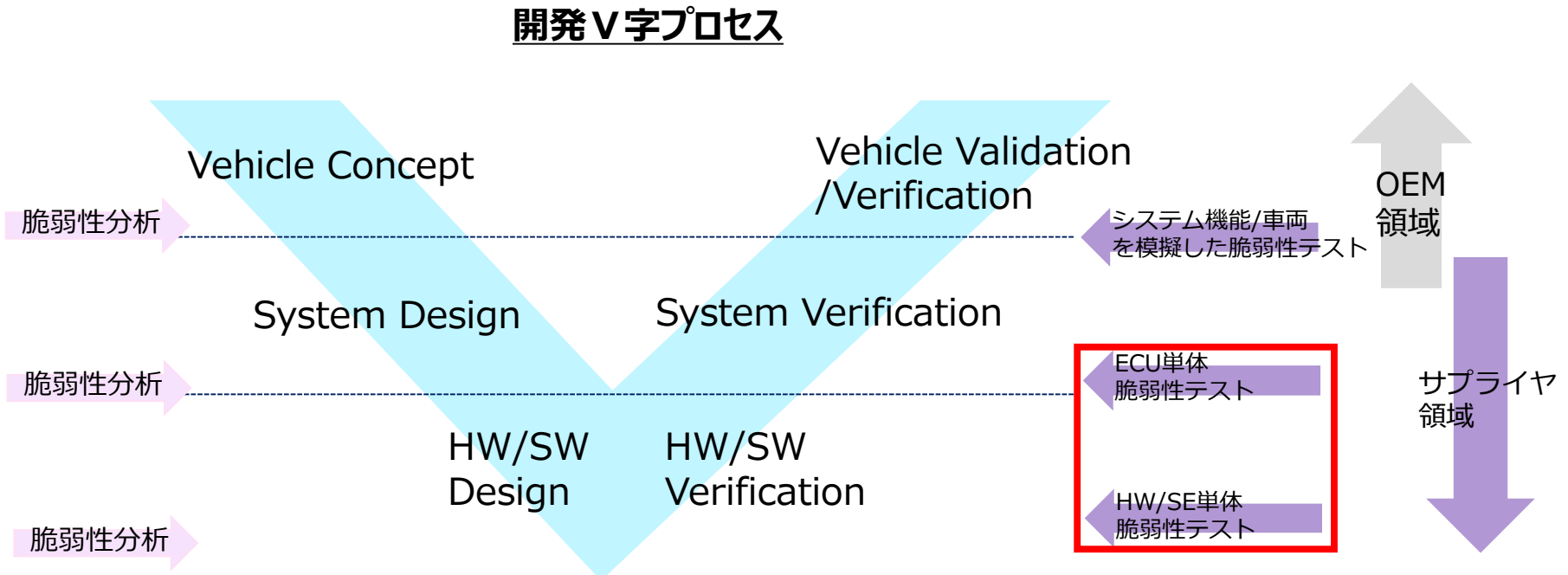
＜特長＞
◆オープンプラットホーム（仕様等の情報開示）
◆ハードウェア・ソフトウェアの改造が容易
◆意図的なセキュリティホール等の作り込み可

＜利用形態＞
◆セキュリティ評価手法、防御手法（対策技術）の開発
◆得られた成果を関連機関と共有

＜利用条件（案）＞
◆利用希望者から、実験計画等の提案を受け
評価環境を貸出し、利用者から実験結果を報告

4．技術開発・ガイドライン策定（InCar）

- JasParでは、国際標準の状況を踏まえつつ、セキュリティの想定脅威に対し、開発プロセスにおいて業界で満たすべき要件等について、業界標準化を進めている。
- 特に、 ECU、ハードウェア/ソフトウェアの脆弱性に対し、最低限実施すべき評価ガイドを策定。

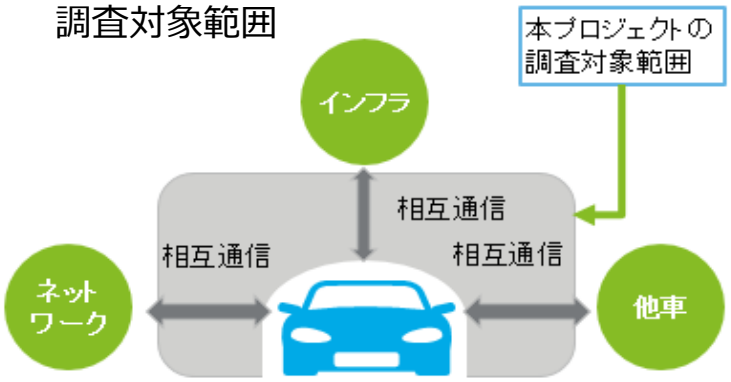


（出所）JasParより

4．無線システムのセキュリティ技術導入検討（総務省）

- V2X通信（具体的には、車両と他の車両との通信（V2V）、車両とインフラとの通信（V2I）、車両と外部ネットワークとの通信（V2N）が対象）におけるセキュリティ対策技術について、無線通信への適合性などの観点から検討を行っている。

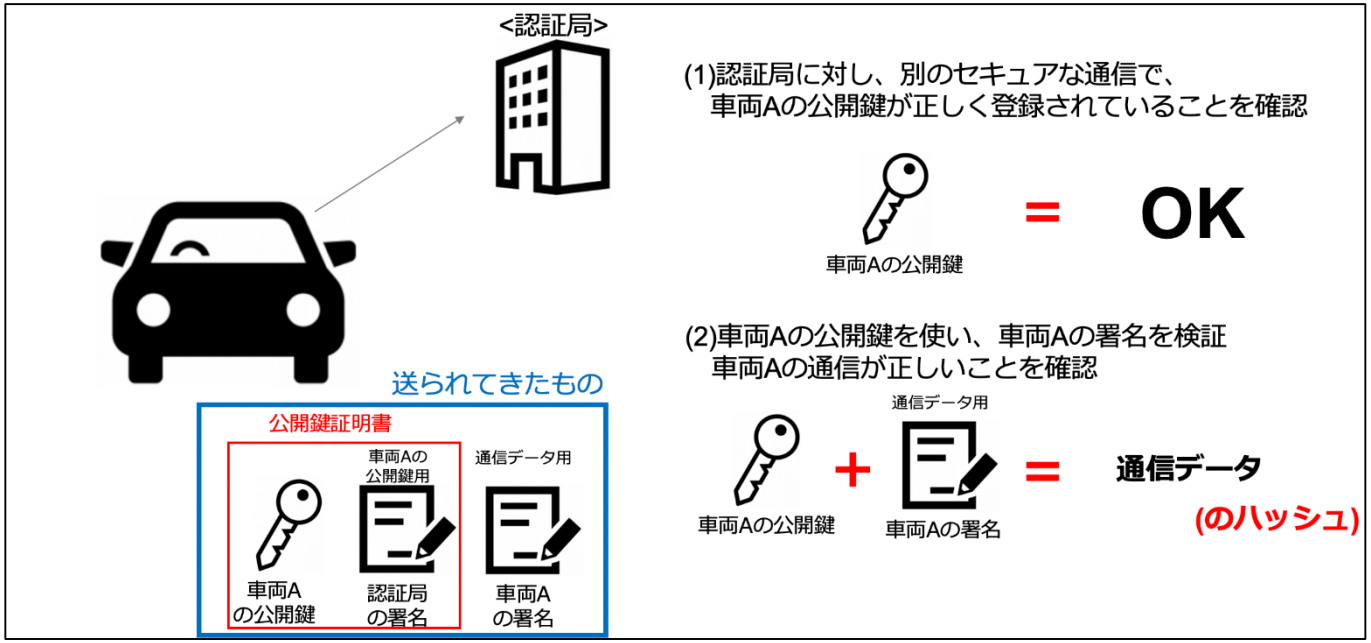
調査対象範囲



検討しているセキュリティ方式

	方式①	方式②	方式③
認証方式	AES-CCM	署名・証明書	署名・証明書
鍵	共通鍵	公開鍵	公開鍵
使用する通信経路	対象の通信のみ	対象の通信のみ	対象の通信と認証用の通信
事前準備	共通鍵とナンスの共有	認証局からの証明書と公開鍵・秘密鍵の発行	認証局からの証明書と公開鍵・秘密鍵の発行
備考	ETSI推奨モデル -秘匿通信	ETSI推奨モデル -ブロードキャスト	

セキュリティ方式検証の一例（方式③）



5．運用面における情報共有体制の構築

- 市場導入後の運用面において、未知のインシデント・脅威・脆弱性が発生し得るため、その情報を直ちに共有し業界全体として、被害拡散防止、対策レベル向上を図ることが必要。
- 経産省のサイバーセキュリティ経営ガイドラインも踏まえ、サイバーセキュリティに関するインシデント情報を共有するため日本自動車工業会においてJ-Auto-ISAC WGを設置　また、日本自動車部品工業会の主要サプライヤと連携した情報共有・解析体制を構築。
- 米国Auto-ISAC、設立検討中の欧州Auto-ISACとのグローバル連携と、国内のICT・金融・電力・交通ISACなど他業界との連携も進め、迅速かつ幅広い情報共有・分析に向けた取組を推進中。

サーバーセキュリティ経営ガイドライン

＜重要10項目＞

1. リスクの認識、組織全体での対策方針の策定
2. リスク管理体制の構築
3. 対策のための資源（予算、人材等）確保
4. リスクの把握とリスク対応計画の策定
5. リスクに対応する仕組みの構築
6. 対策におけるPDCAサイクル実施
7. インシデント発生時の緊急対応体制の整備
8. インシデント被害に備えた復旧体制の整備
9. サプライチェーン全体の対策および状況把握（含、ビジネスパートナー・委託先）
10. **情報共有活動への参加による攻撃情報の入手と有効活用**

J-Auto-ISACメンバー

J-Auto-ISAC 事務局：デロイトトーマツ リスクサービス		US Auto ISAC 加盟
いすゞ自動車	ISUZU	
川崎重工業	Kawasaki	
スズキ	SUZUKI	
SUBARU	SUBARU	✓
ダイハツ工業	DAIHATSU	
トヨタ自動車	TOYOTA	✓
日産自動車	NISSAN	✓
日野自動車	HINO	
本田技研工業	HONDA	✓
マツダ	mazda	✓
三菱自動車工業	MITSUBISHI MOTORS	✓
三菱ふそうトラック・バス	FUSO	
ヤマハ発動機	YAMAHA	
UDトラックス	UD TRUCKS	

連携

国　内

- 政府・政府系機関（METI、IPA、JPCERT/CC）
- 日本自動車部品工業会
- JASPAR
- 他業界ISAC（ICT-ISAC、金融ISACほか）

海　外

- 米国 Auto-ISAC
- 欧州 Auto-ISAC（設立検討中）

6．不足するサイバーセキュリティ人材の育成推進

- 圧倒的に不足している、サイバーセキュリティ人材については、最新かつ顕在化していない情報の収集能力、保護対象となるシステムの理解、現実的な対策方法の立案等、非常に高度な専門性が求められる。
- そのため、産学官が連携した人材育成講座や人材育成プログラムを実施している。
- 今後は、より実務的なサイバーセキュリティ人材の育成システムの構築が課題となっており、各自動車会社の評価環境を使用することが難しいことから、経産省・国交省が整備しているテストベットを活用していくことが期待される。
- 加えて、海外人材の発掘・中途採用を含めた積極的な取組が必要。その際、人材を確保するために雇用体系の検討はもちろんのこと、業界が協調して、製造現場におけるサイバーセキュリティ人材の必要性や職の魅力を発信することが不可欠。
- 更には、業界として安全性を高める観点から、SIPが策定を進めている、車両へ対する車外からの攻撃に関する評価ガイドラインを活用し、将来的には外部の優秀なハッカーと手を組み、White Hat Hackingの実施等を議論することが必要。

IPA：産業サイバーセキュリティセンター人材育成事業

◆ 2日間の短期プログラム（セキュリティ対策統括責任者向け）
◆ 1年間の長期プログラム（若手向け）

短期プログラム

- CEO、CIO・CISO、部門長等、責任者クラスの方向けに2日間のトレーニングを年6回実施（うち、業界共通トレーニングを3回、業界別トレーニングを3回）

長期プログラム「中核人材育成プログラム」

- 将来、企業などの経営層と現場担当者を繋ぐ、“中核人材”を担う方を対象としたプログラム
- テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ1年程度のトレーニングを実施

自動車技術会：人材育成事業

✓ 自動車工学基礎講座
✓ モーターサイクル工学基礎講座、
✓ 各種講習会
✓ 女性技術者交流会
✓ （支部）技術交流会、講演会、見学会
✓ **自動車サイバーセキュリティ講座**

・自動車工学ハンドブック
・自動車工学基礎
・シンポジウムテキスト　等