

自動走行システムにおける サイバーセキュリティ対策

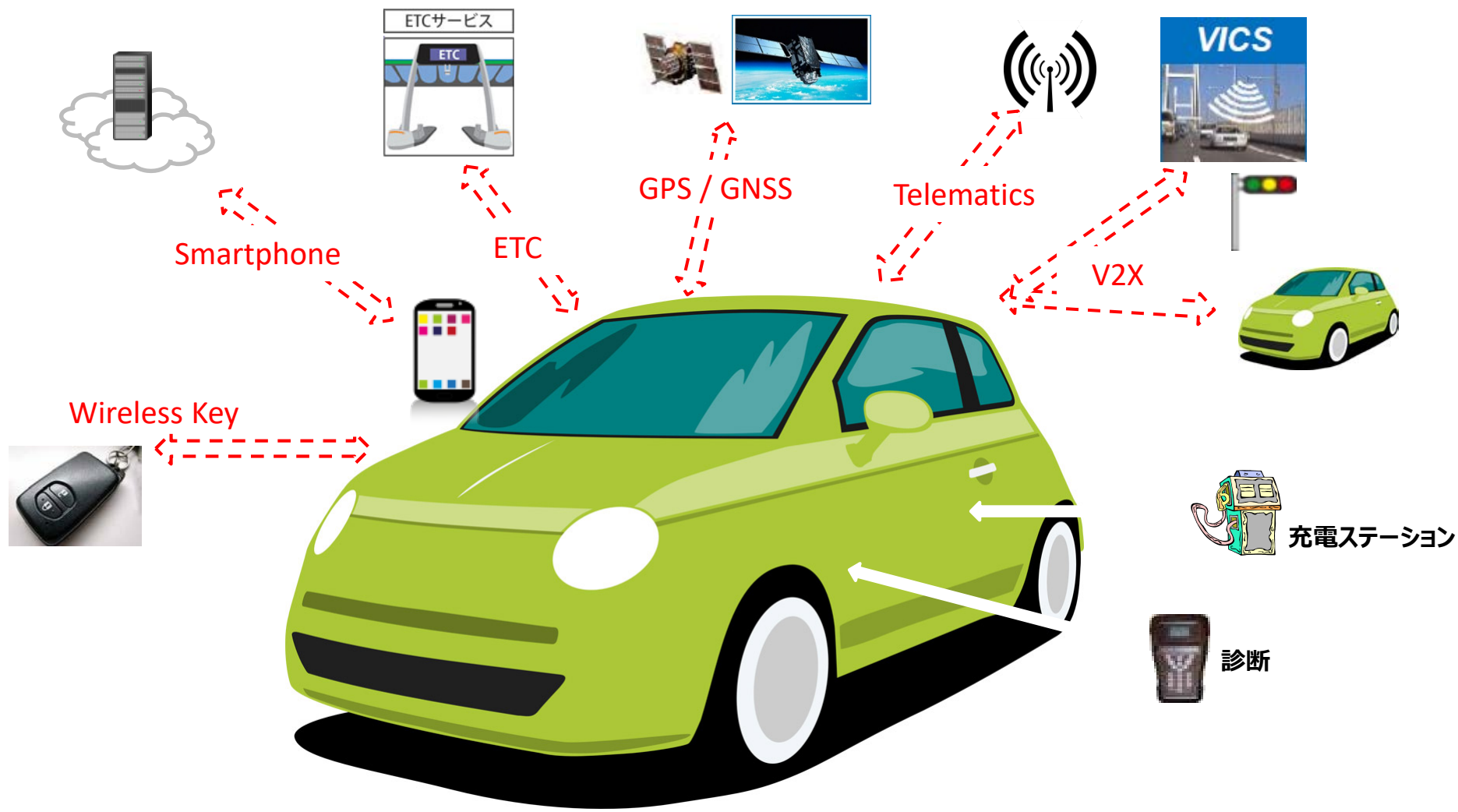
2018年3月30日
自動走行ビジネス検討会

0. 導入 (1 / 2)

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

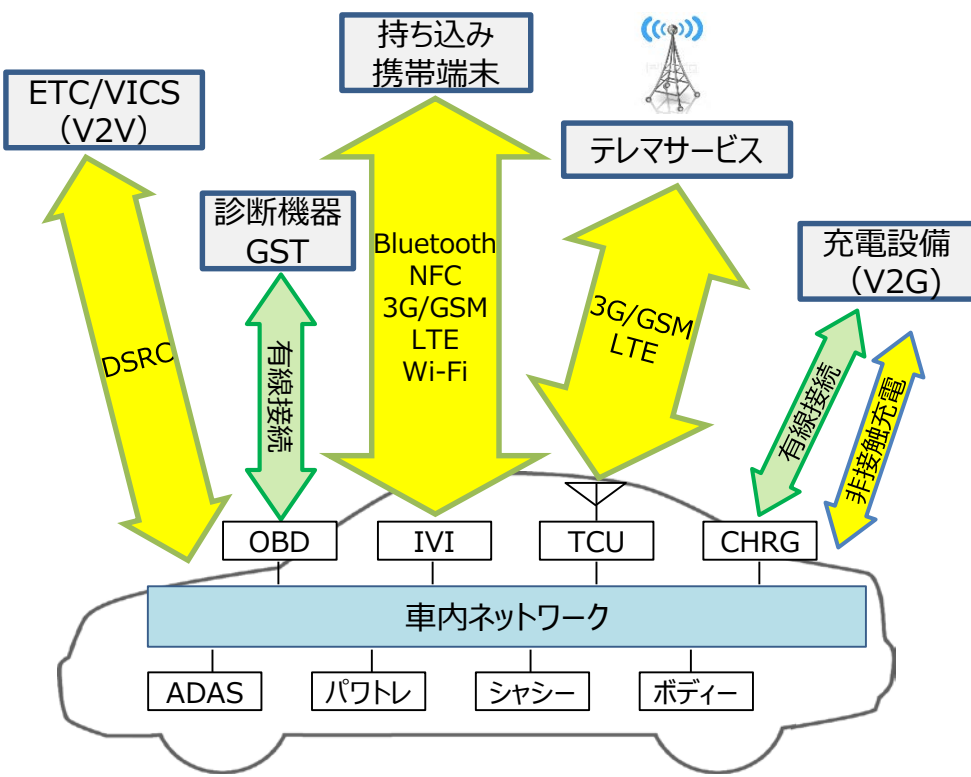


0. 導入（2／2）

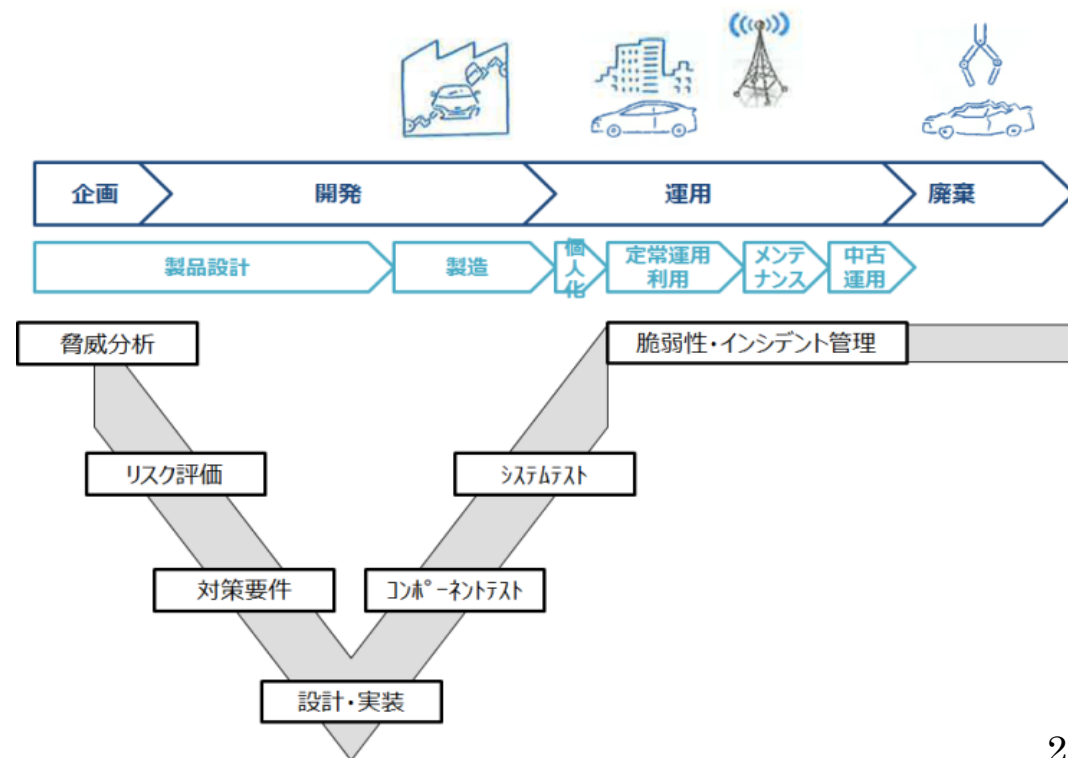
自動車におけるサイバーセキュリティ対策の方針

- 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。

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

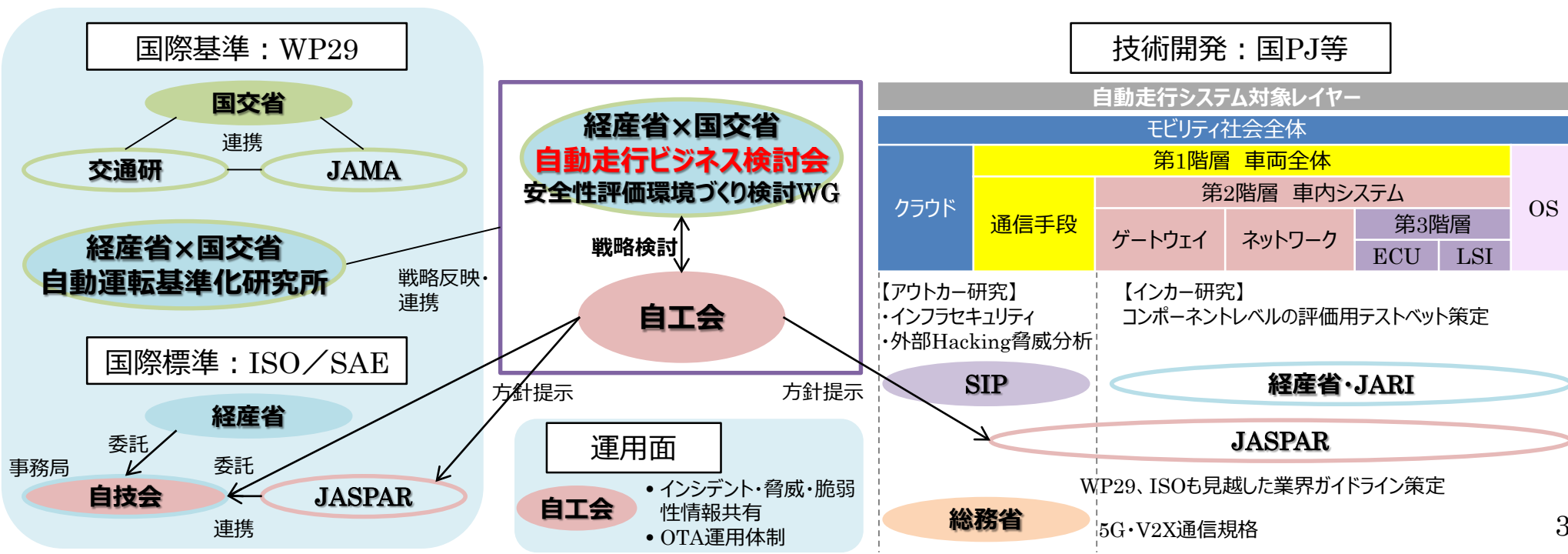


自動車のライフサイクル



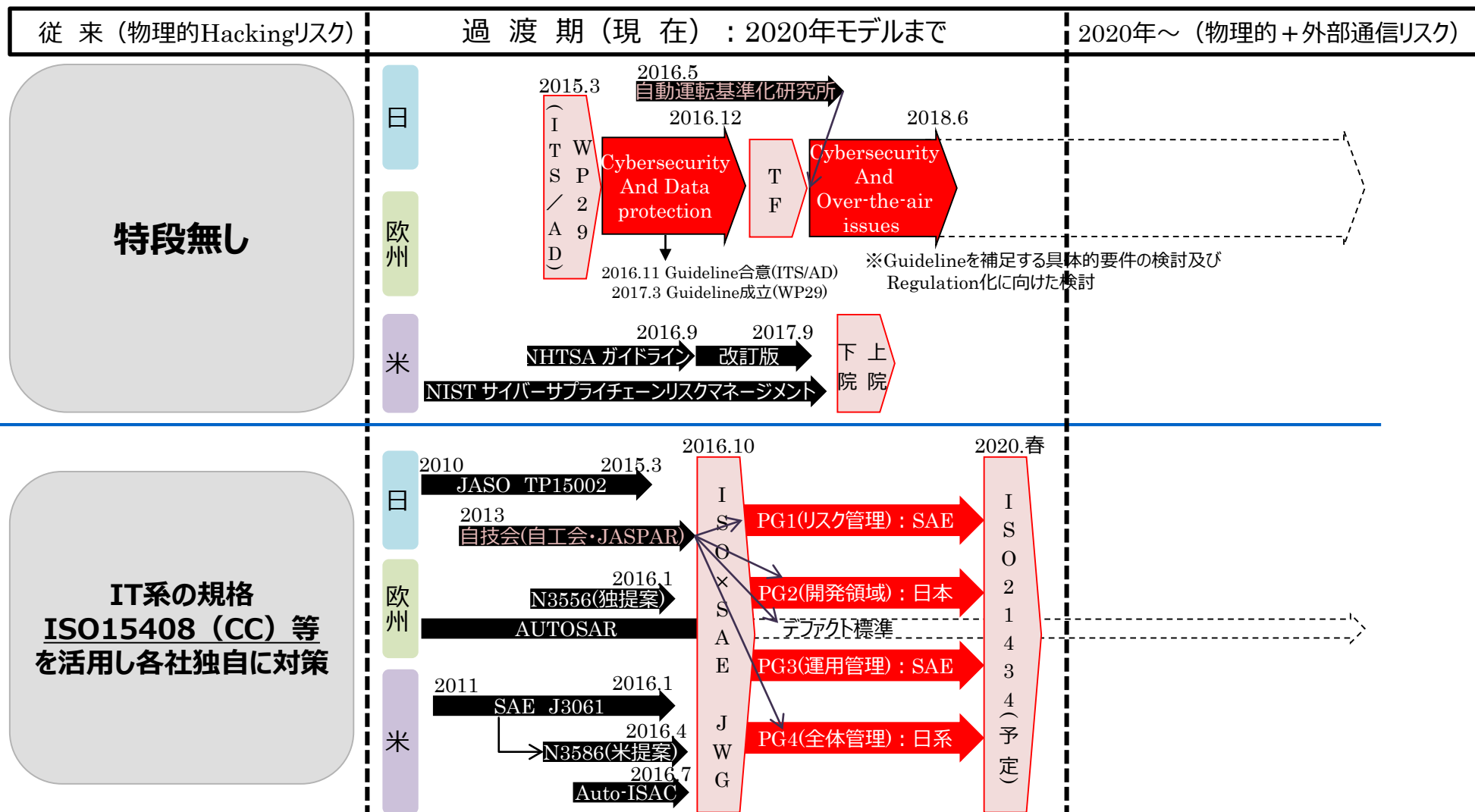
1. 現状の検討体制

- 「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）」こととしており、**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る。
- 内閣府SIP、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。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。
- SIP-adusは、大規模実証で車外通信からのWhite Hat Hackingを実施し、車両へ対する車外からの攻撃に対する評価ガイドラインを作成中。
- 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。
- なお、業界として、国際基準（WP29）は自工会、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。



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化の議論が進んでいたところ、Regulation化への動きに転じつつある。
- 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。



3. 海外動向（1／2）

米国

- 2017年9月にNHTSAガイドライン第2版が策定されたことに加え、上院、下院においても法制化の議論が進展中。
- 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）：2017年内の採択が国内で期待されている

【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）：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ティアで提出・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り入れること。
- ◆ 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ジ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（2／2）

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を求める発言有。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）

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。

4. 我が国の技術開発、情報共有、人材育成における取組（1 / 5）

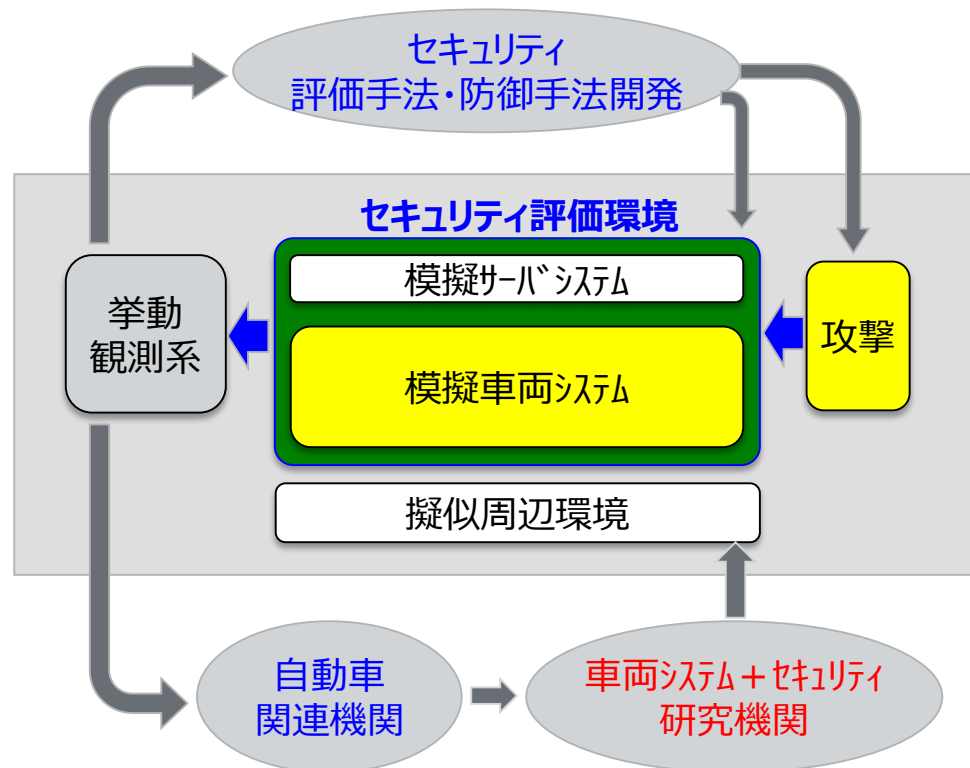
- 自動走行車両がハッキングされた場合、重大な事故を招くおそれがあり、重要インフラ分野として位置づけられている「情報通信」、「金融」、「航空」、「鉄道」、「電力」等と同様の高度な対策が必要と認識。
- システムが運転を行う、いわゆるレベル3以上の自動走行車は、商品化されておらず、また、先端的な技術を含んでいること、及び各自動車会社で電子制御システムが異なりかつ進化も早いことから、協調領域と競争領域を設定し、取組を進めている。
- 特に下記を協調領域として官民で推進中。
 - ① 中小サプライヤーや研究機関が共同で脆弱性分析を進めるための評価環境（テストベッド）整備
 - ② 安全設計のための多層防御設計、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

4. 我が国の技術開発、情報共有、人材育成における取組（2 / 5）

①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の構築を推進（「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中）。
- 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
- ◆ 意図的なセキュリティホール等の作り込み可
- ◆ ECUの設定自由度が高い

<利用形態>

- ◆ 評価環境を用いて、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

4. 我が国の技術開発、情報共有、人材育成における取組（3 / 5）

② 安全設計のための多層防御設計、開発プロセス標準化

- 外部通信からの情報は、冗長性確保のための補助的情報であり、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。
- 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。

<通常>

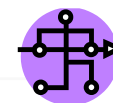
外部通信情報



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



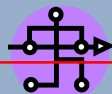
通常に走行
or
センサー情報を基に安全確保（安全に車両が停止）
※センサー情報を優先

多層防御設計

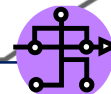
外部通信

車内システム

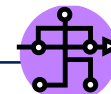
情報



通信プロトコル

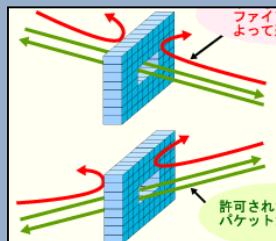


Central
Gateway



制御系

多層防御



<ファイアウォール>
不正な情報を遮断、
許可された情報のみ通す

<メッセージ認証>
メッセージに改ざんがない
ことを確認

4. 我が国の技術開発、情報共有、人材育成における取組（4／5）

③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。
- 今後は、米国で確立しているUS-Auto-ISAC、IT業界やサプライヤーとの連携を進め、迅速な情報共有・分析に向けた取組を進めていくことが必要。

サイ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

社名		US A-ISAC メンバー
トヨタ		✕
ホンダ		✕
日産		✕
マツダ		✕
SUBARU		✕
スズキ		
三菱		✕
ダイハツ		
いすゞ		
日野		
三菱ふそう		
ヤマハ		

<参考> 情報共有体制が進んでいる米国の対応

◆1998年 クリントン大統領令63
重要インフラ18分野毎に情報共有するよう指示

→ 各インフラ毎にISACを設立
（銀行、金融、電力、上下水道、交通、通信、原子炉、軍需産業・・・）

◆2003年
上記18分野を横断的に情報共有する
National Council of ISACを設立

◆2013年 オバマ大統領令13636
重要インフラのサイバーセキュリティレベル向上に向けたフレームワーク策定を指示

◆2015年8月 Auto-ISAC設立
2016年1月活動開始

4. 我が国の技術開発、情報共有、人材育成における取組（5 / 5）

④不足するサイバーセキュリティ人材の育成推進、White Hat Hackingの活用

- 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ツ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

5. 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

- 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。
- その実現に向け、最低限満たすべき水準の設定、評価環境（テストベッド）の実用化を目指す。また、インシデント対応に関する情報共有体制を構築する。

