

Connected Vehicle Platformにおける北米技術動向 と、 日本の大学生・若手技術者への期待

8/24/2017@SWEST19

DENSO International America, INC.
NAREC(North America Research Center)
ePF 課長 佐藤洋介

関係する北米拠点

The image features a map of North America with two callout boxes. The first callout, labeled 'DIAM DENSO', points to a blue dot in the Detroit area. The second callout, labeled 'TOYOTA connected', points to a red dot in the Dallas area. The map includes labels for various cities and states in both Japanese and English.

【赴任前のイメージ】

This section contains two images: a large burger with the text '祝45周年 みんなの車で大宴会 テキサスバーガー' and 'のワイルドな', and a silhouette of two cowboys on horseback against a sunset sky.

【現実】

This section contains two images: a city skyline with skyscrapers and a large multi-level highway interchange.

佐藤洋介の経歴

学生時代(UML, Design Pattern, Java Virtual Machine, Slackware Linux)

期間	所属	役職	担当業務	その他
2002年 ～ 2003年	電子機器事業Gr 特定開発室SSC	担当	ソフトPF先行技術調査 →UML, Product Line, Java/CORBA, AUTOSAR 【役割】ソフト先行技術調査とソフトPFへの適用検討	SWEST5より実行委員会へ参加 情報処理学会 組込みシステムWG研究員
2004年 ～ 2008年	電子PF開発部 ソフトPF開発室	担当	ソフトPF製品開発 【役割】CAN通信層ソフト部品量産開発	 ETロボコン2006優勝
2009年 ～ 2010年	電子PF開発部 先行技術開発室	担当係長	JASPAR BSW仕様開発 【役割】JASPARソフト構造仕様取りまとめ・評価リーダー 	SWEST10,11,12プログラム委員長 AUTOSAR参画 
2011年 ～ 2013年	情報通信技術4部	担当係長	欧州OEM殿向けエアコンパネルECUソフト開発 →Vector MICROSAR, Renesas MCAL 【役割】BSW開発Project Leader 	日科技連SQUBOK参画 【役割】組込み技術リーダー 
2014年 ～ 2016年	DIAM 	担当課長	北米OEM殿向けメータECUソフト開発 →Cyber-security, OTA, QNX 【役割】BSW開発Project Manager 	DHS※ SOTA標準化活動参画 ※Department of Homeland Security
2017年 ～ 現在	DIAM (TC出向) 	担当課長	Connected PFシステム開発 【役割】System Architect	

DENSO

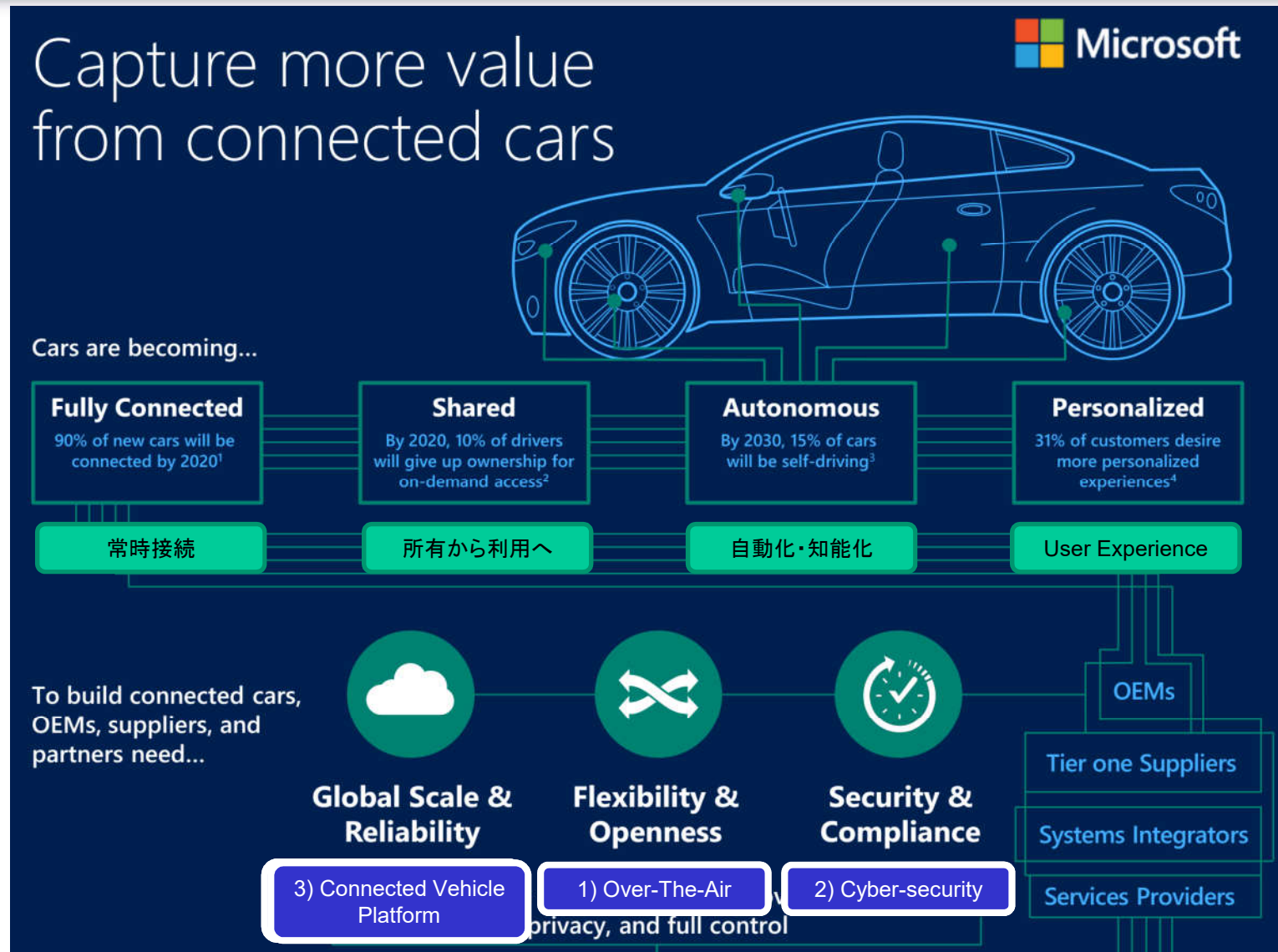
© DENSO CORPORATION All rights reserved.

This information is the exclusive property of DENSO CORPORATION. Without their consent, it may not be reproduced or given to third parties.

本日の趣旨

- 現在、自動車業界ではデジタルトランスフォーメーション(Digital transformation)の真っ只中において、IoT(Internet of Things)関連技術やビッグデータ分析基盤関連技術のブレークスルーが、車両制御や車両サービスに対して、イノベーションの波を起こしつつあります。
- 「**ビッグデータ分析基盤**を核としたクラウドからサービスの提供を受ける、ネットワークインフラに常時接続された**コネクテッド・カー**」という構図は、**ドライバ行動予測**による燃費向上や、**機械学習**による自動運転支援といった新たなサービス生み出しつつあり、我々は自動車の世界が変革する重要な変化点にいると言えます。
- 本講演では、北米でのコネクテッド・カー関連の技術、具体的には**Cyber-security, Over-The-Air, Connected Vehicle Platform**といった**今後の10年を支える自動車関連技術**を紹介し、北米から見た日本の大学生・若手技術者への期待についてお話しします。
- また、そこから私自身のSWESTとの関わりや海外赴任経験といったキャリアパスを紹介することで、講演を聴いてくださった方々にインスパイアいただけると嬉しいです。

コネクテッド・カーを取り巻く環境変化と、基盤技術

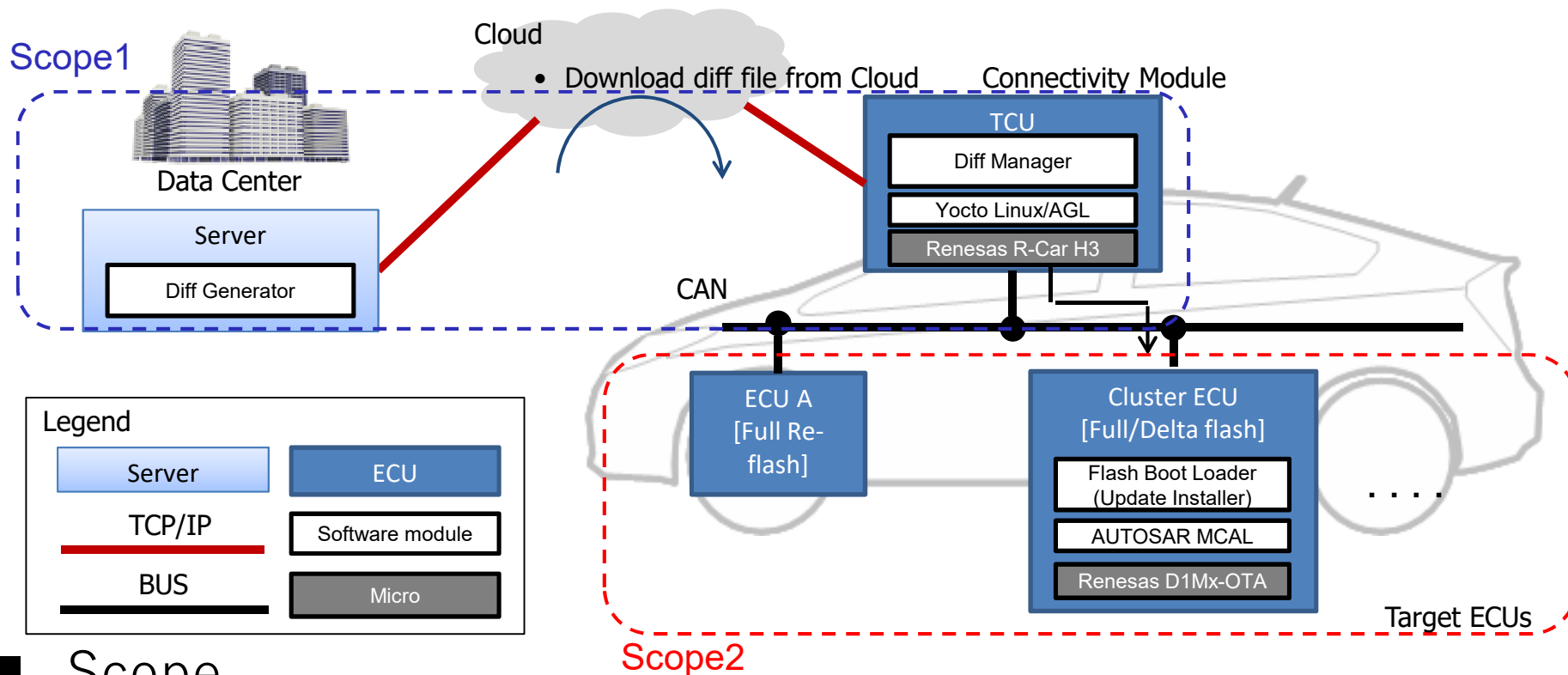


個々の技術だけの話を聞くとチグハグに聞こえるが、近未来で実現したい姿は「Connected Cars」


1) Over-the-Air

OTAシステムアーキテクチャ

System Architecture for Secure OTA



Scope

	Characteristics / Challenges	Activity
Scope1	<ul style="list-style-type: none"> Connectivity How to reduce communication costs by delta flash algorithm Security the authenticity and integrity of software updates 	DHS SOTA(Uptane)  Explain DHS SOTA
Scope2	<ul style="list-style-type: none"> Reliability/Cost-effectiveness A/B storage, enough additional space to keep a delta 	Lead by OEMs/Tire 1/Micro vendors

What's DHS SOTA(Uptane)

- Overview
 - This work is sponsored by DHS(Department of Homeland Security) Cybersecurity Division
 - 2 year project(Oct. 2015 – Sept. 2017)
 - UMTRI, SwRI are leading this work
- Basic principle
 - **Competitive** area : Delta-flash algorithm, E/E Architecture, Cloud ...
 - **Collaborative** area : Security mechanism
- Objective
 - Develop an **open standard** for secure over-the-air (SOTA) automotive software updates
 - Create a proof-of-concept **secure reference implementation**
 - Focus on **automotive platform**, usability, security, and the supply chain



Task #	Task	Task Start Date	Task Due Date	Milestones	Milestone Due Date
1	Requirements	Month 1	Month 6	Initial Requirements	Month 3
				Workshop	Month 3
				Final Requirements	Month 6
2	Design	Month 1	Month 12	Initial Design	Month 6
				Workshop	Month 9
				Final Design	Month 12
3	Implementation & Integration	Month 1	Month 18	Prototype Implementation	Month 12
				Final Vehicle-Integrated Implementation	Month 18
4	Testing and Evaluation	Month 1	Month 24	Test & Evaluation Plan	Month 6
				Workshop (combined with Task 2 workshop)	Month 9
				Refined Test & Evaluation Plan	Month 10
				Test & Evaluate Prototype Implementation	Month 18
				Test & Evaluate Final Vehicle-Integrated Implementation	Month 24

DHS SOTA(Uptane) Overview 1/2

- Use cases

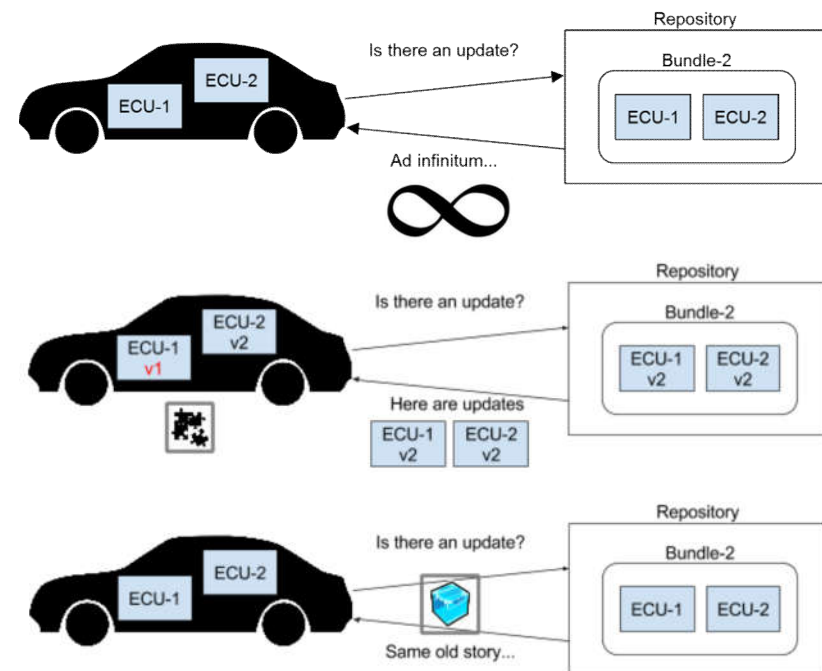
- A vehicle must be able to verify the authenticity, integrity, and timeliness of a bundle of software updates an OEM wishes to install on its ECUs.
- A vehicle should be able to install this bundle of updates on some (ideally all, if there are no failures) ECUs.

- Failure model

- An ECU may run out of power while installing a software update.
- A software update may be interrupted during download.
- An ECU may suffer permanent network loss.
- An ECU may run out of storage for update.
- ...

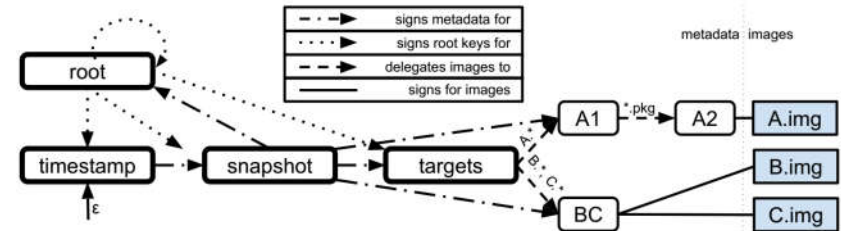
- Threat model

- Endless data attack
- Partial bundle installation attack
- Freeze attack
- ...



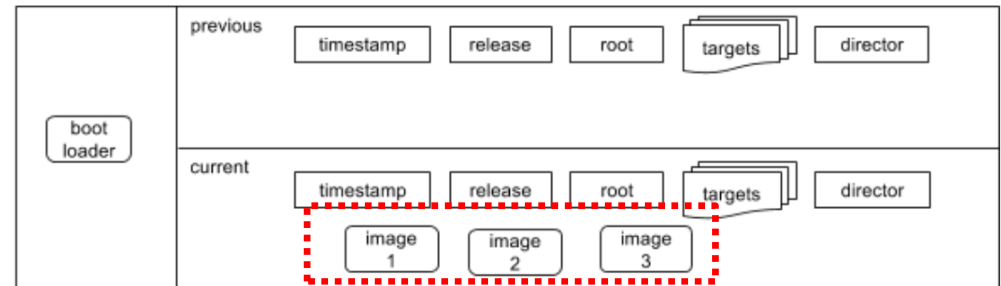
DHS SOTA(Uptane) Overview 2/3

- The Update Framework
 - Separation of duties (roles, keys, metadata).
 - Multi-trust signatures.
 - Explicit and implicit revocation of keys.



- Logical Architecture
 - Primary ECU
 - downloads, verifies, distributes metadata + images to secondaries.
 - Secondaries ECU
 - verify* metadata + image distributed by primary, and installs image.

Primary (ECU 1)



Full verification Secondary (ECU 2)



Partial verification Secondary (ECU 3)



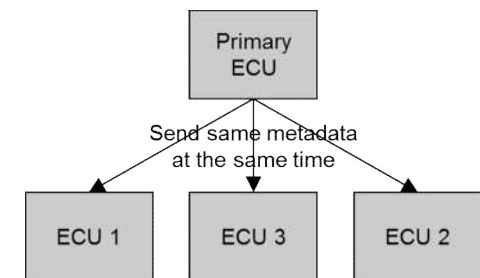
DHS SOTA(Uptane) Overview 3/3

• UPTANE design features

- Additional storage to recover from endless data attacks
 - **A/B storage** the simplest implementation.
 - Optimization: add just enough space to store delta from old to new image.

Boot-loader	Previous metadata	Latest downloaded metadata	Previous image	Latest downloaded image (possibly a delta)
-------------	-------------------	----------------------------	-----------------------	--

- Vehicle version manifest to detect partial bundle installation attacks
 - Primary must send the director the **vehicle version manifest** (what every ECU has installed) whenever it contacts for the latest updates.
 - If director detects mismatch between last updates and manifest, then OEM can be **alerted** for follow-up.
- Time server to limit freeze attacks
 - ECUs continually update time from a time server

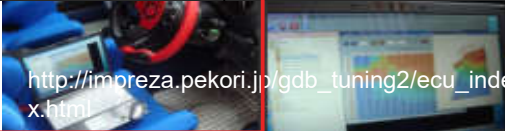



今後10年を支える技術としての考察

- ECUへのインパクト
 - ECUの役割としてFlashの対象となるSecondaryとその面倒を見るPrimaryが定義されている。CGWなどに代表されるPrimaryは、SecondaryのFlashイメージを保持する必要があることから、相当のストレージスペースが必要になるのに加え、Flashイメージヘッダの照合も全Secondary分処理するため、相当のCPUパワーが必要な見込み
 - 今後は、頭脳ECUと手足ECUの再配置がより加速すると思われる。特に頭脳系ECUの計算機アーキテクチャやOSの検討がより進む見込み。
- リファレンス情報として
 - セキュリティや想定される異常系は、各々Threat modelとFailure modelという形になっているため、我々の要件定義やテストケース構築の有用な情報ソースとなりそう。
 - Threat modelは時代の進展とともに刻々と変化する。Uptaneのようなオープンな場でアンテナを張ることは重要。

2) Cyber-security

Recent Security Trends

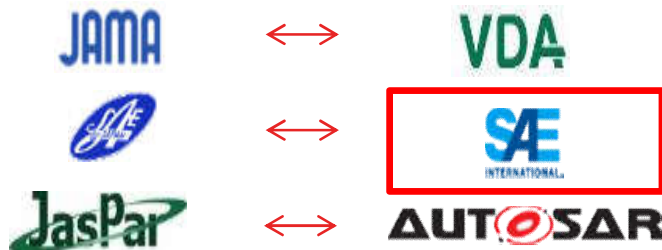
Category	2013	2015	2017	202x
Service	Connected Service ECUs(Telematic) OBD Aftermarket Device		V2X (CACC)	Automated Driving (Lv2.9) Automated Driving (Lv3-)
Attack to vehicle Terrorism, Fun Vehicle theft, Attach malicious device		Remote attack through Smartphone/Center Remote attack to Telematics	Direct & Remote attack to Telematics, IVI V2V Attack Pretend Emergency Vehicle Accident/ Block traffic	Warning to industry Attack to Local Vehicle Bus
Improve Performance			Tune-up	
Add Function	Aftermarket: Remote Starter, Cruise Control, LDW, Collision Detection		Aftermarket: Door lock with speed Aftermarket: Emergency Brake Signal	
Disable Restriction				Aftermarket Automated Driving Disable ACC restriction Alter/Disable ADAS restriction

Remote Attack
Advancement
of attacks

Motivation
of vehicle
owner

Improve ADAS
function by
vehicle owner

OBD: Onboard Diagnostics, CACC: Cooperative Adaptive Cruise Control
LDW: Lane Departure Warning



今回は北米セキュリティ標準化動向にフォーカス

Security Standardization in N.A.



400 Commonwealth Dr.
Warren, PA 15096
www.sae.org

F +1281.232.4505
E CustomerService@sae.org

Roll mouse over a committee name to view its scope.
Click on a committee name to view its fact sheet.

GLOBAL GROUND VEHICLE STANDARDS

For information about the Automotive Services Committee Meeting Schedule, click here.

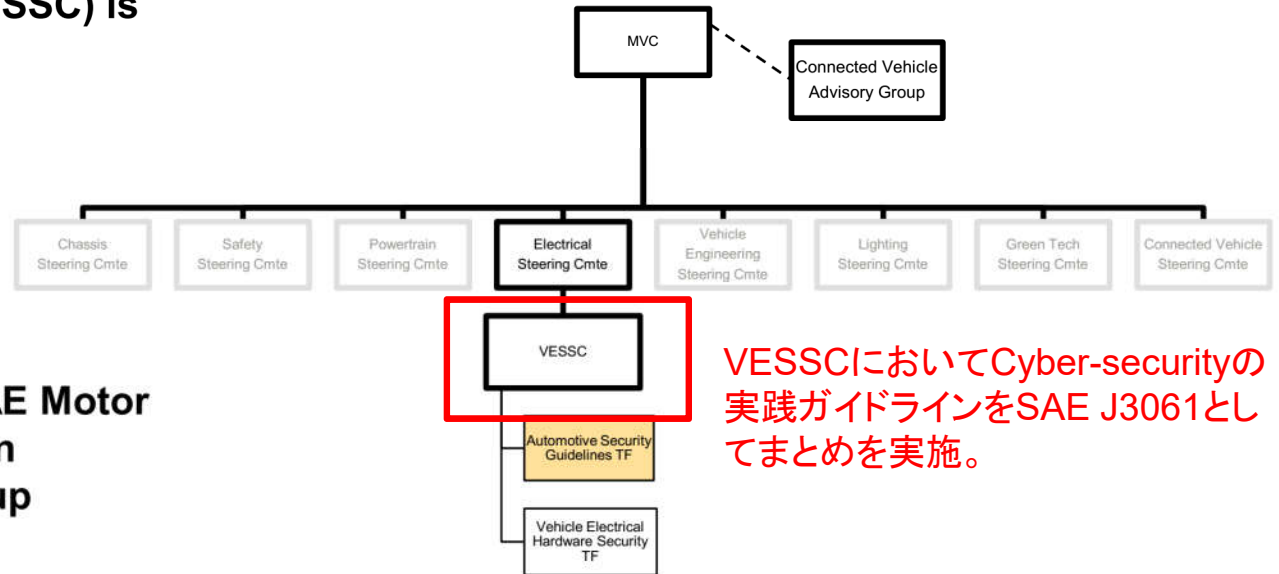
For information about the Commercial Vehicle Council Meeting Schedule, click here.

609 committees
8,865 members
2,898 companies
1,423 meetings

Committee meetings are **open** to all interested parties, but **only committee members vote**

- The Vehicle Electrical System Security Committee (VESSC) is active since May 5, 2011

- Organized under the SAE Motor Vehicle Council (MVC) in Electrical Systems Group

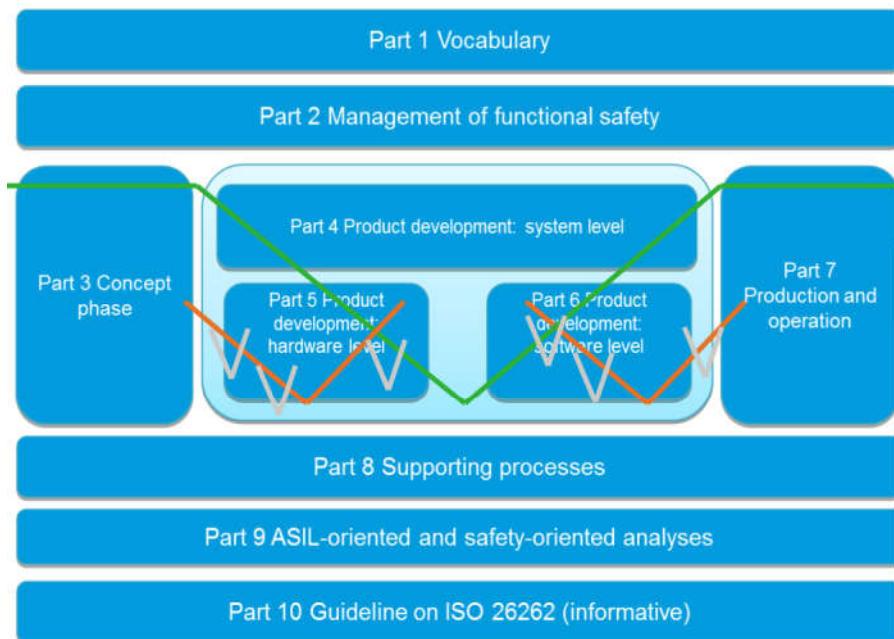


VESSCにおいてCyber-securityの実践ガイドラインをSAE J3061としてまとめを実施。

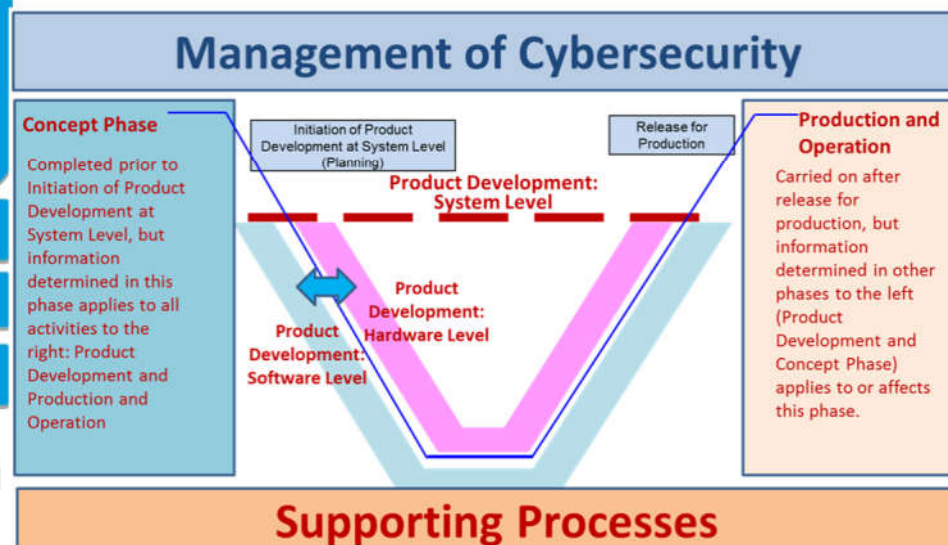
What's SAE J3061

- This recommended practice establishes **a set of high-level guiding principles for cybersecurity** as it relates to automotive cyber-physical systems to be utilized in series production.
- Motivation
 - Cybersecurity was relatively new to automotive, and most existing information **did not address unique aspects of embedded controllers**
 - Cybersecurity principles, process and terminology are needed that can be **commonly understood** between OEMs, Tier 1 suppliers & key stakeholders
 - A defined and structured process helps ensure that cybersecurity is built into the design throughout product development
 - **Based on ISO 26262** Functional Safety process framework

ISO26262 vs. SAE J3061



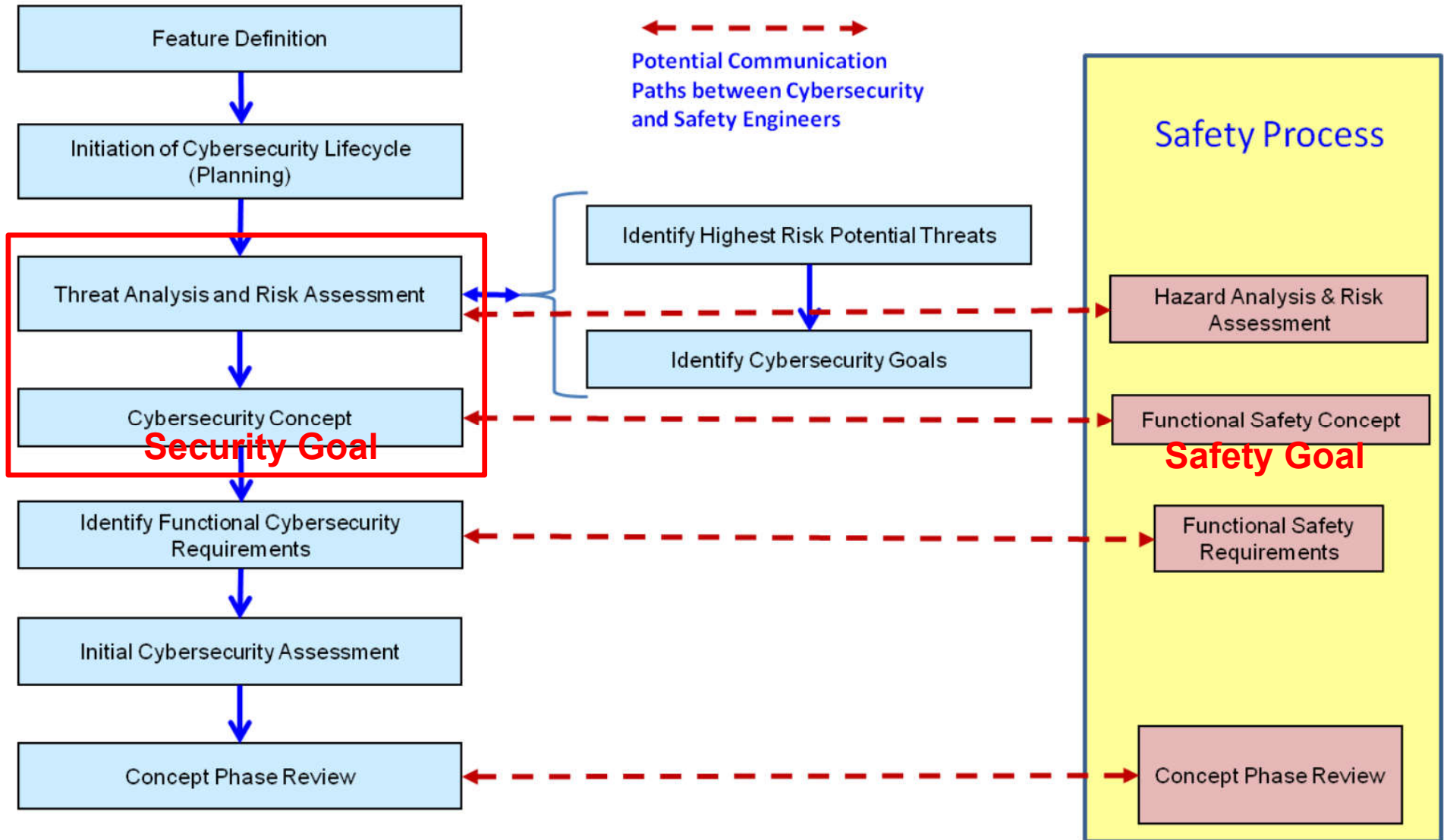
ISO 26262



Source: J3061™
Copyright SAE International

SAE J3061™

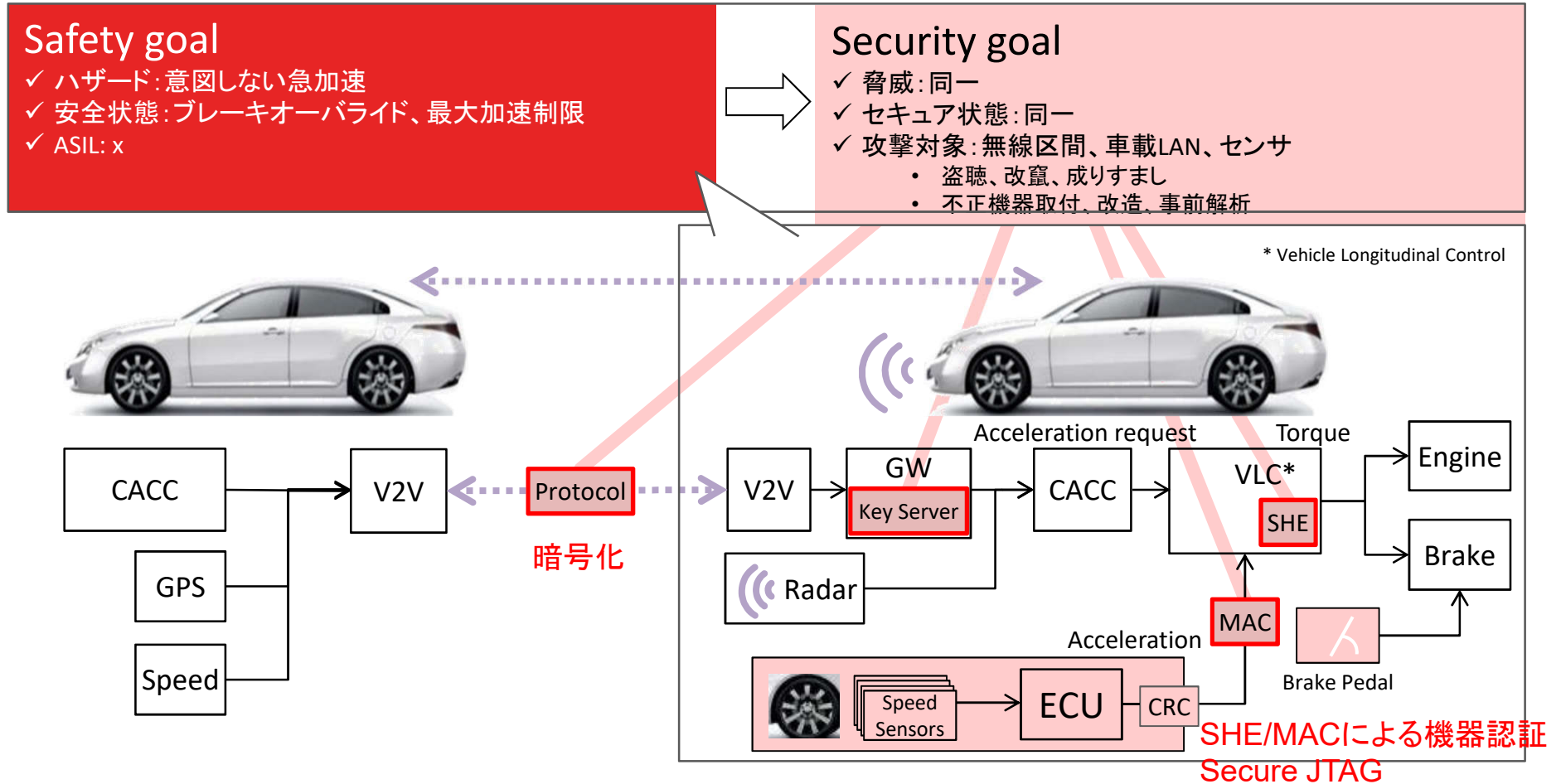
Relationship between Security and Safety Process



【事例】デンソーCACC (Cooperative Adaptive Cruise Control)

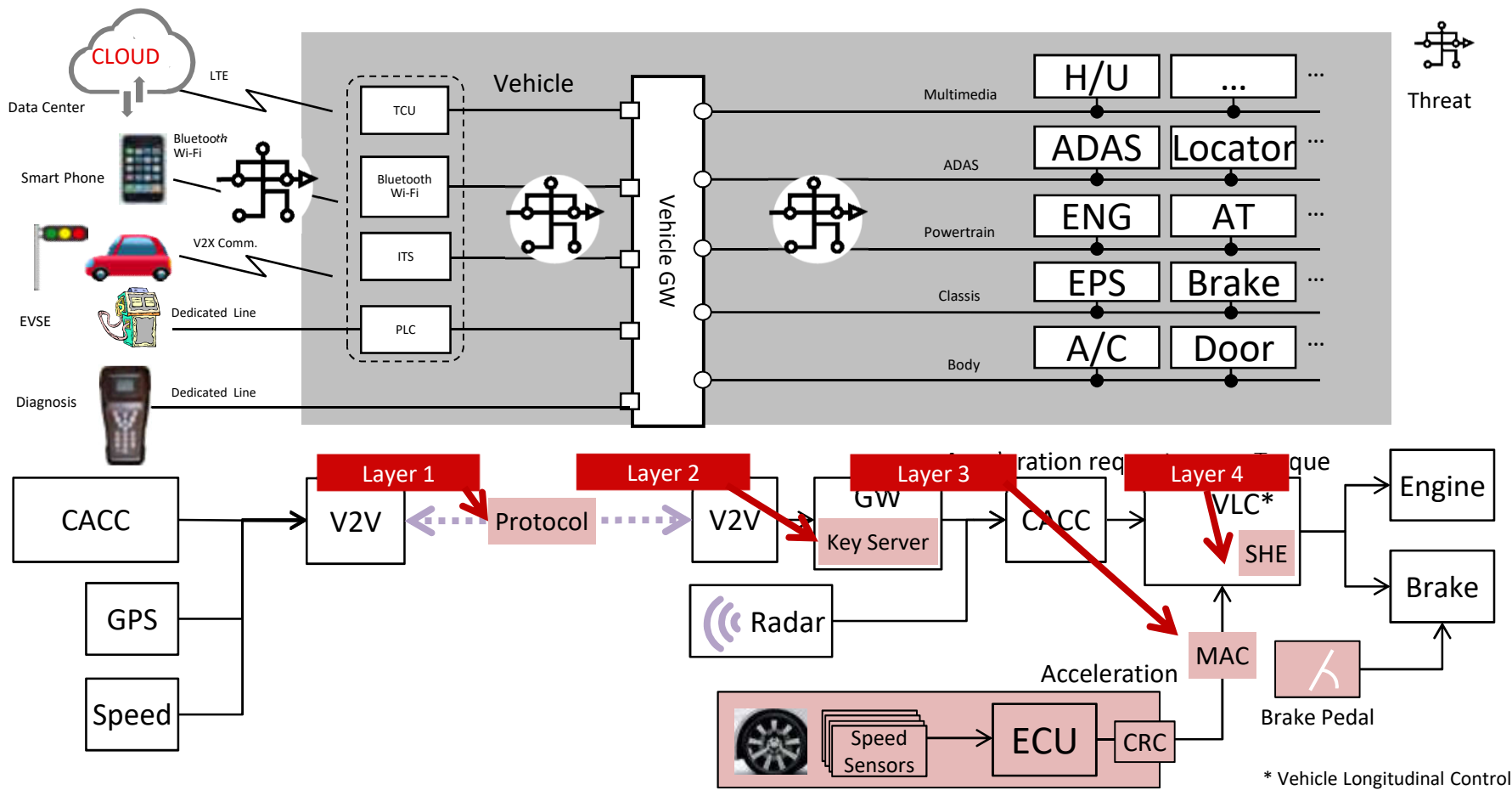
▶ Definition of security requirement from hazards

SHE: Secure Hardware Extension
MAC: Message Authentication Code



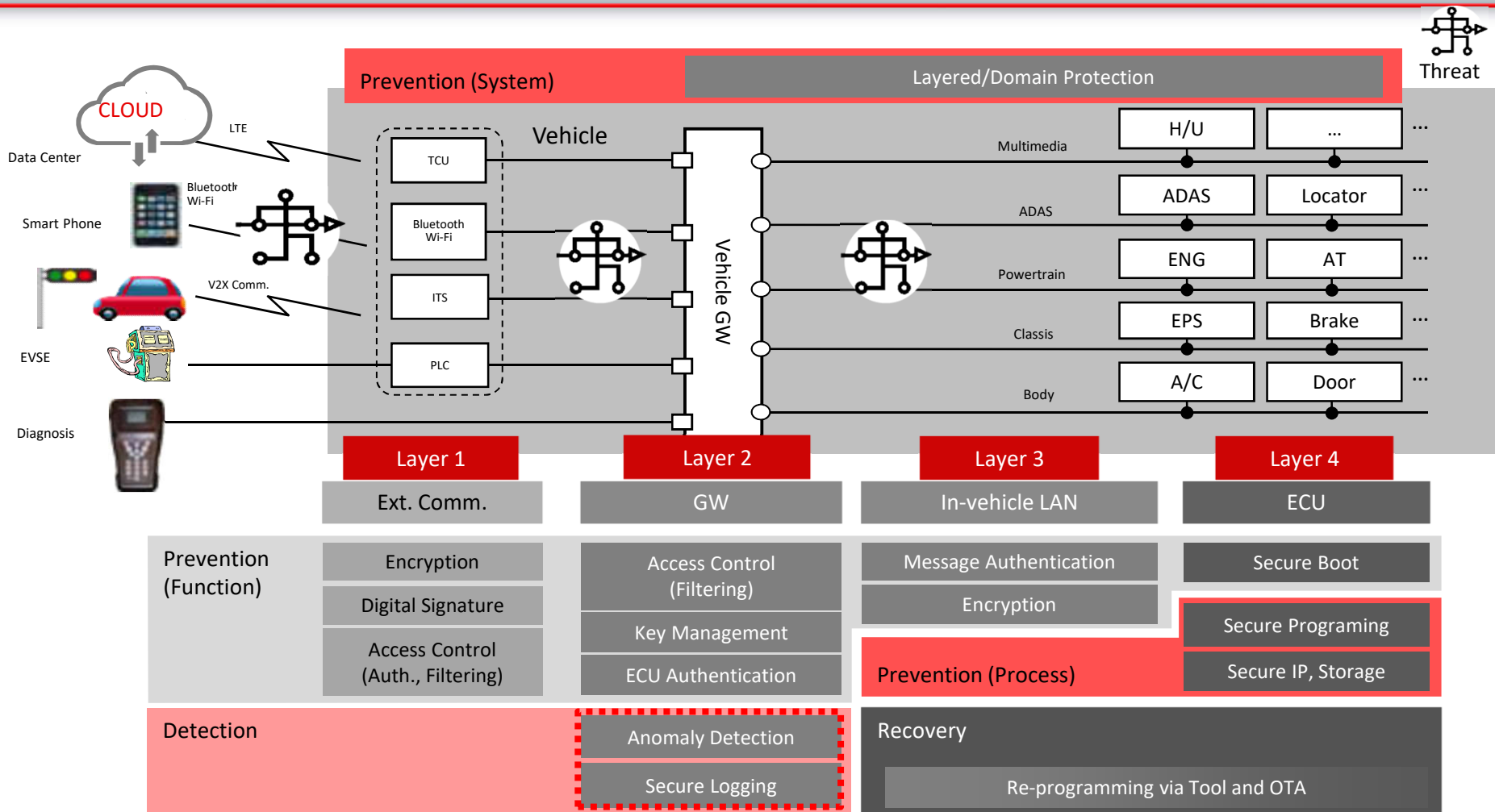
▶ Safety & Security両方の対策で車を守る

セキュリティ・アーキテクチャの考え方



▶ IT業界の一般的なセキュリティコンセプト「多層防御」を車に適用。

セキュリティ・アーキテクチャ実現のための要素技術



▶ 2020年目線の車を守るための、アーキテクチャを定義の上、必要となる対策技術を適用

Connected Vehicle PlatformのSecurity機能

考え方:膨大な車両情報を侵入検知へ活用する

- 侵入検知アルゴリズム
 - Signatureベース
 - Signatureベースは古くからある手法で、攻撃による**異常パターン**を予めプロファイルとして定義しておいて、そのパターンにマッチしたかどうかを判定。
 - 利点: 検知に計算機パワーがそれほど必要ない。
 - 欠点: パターンにマッチしない未知の攻撃には一切効果を発揮しない。
 - Anomalyベース
 - 正常パターンからの**逸脱で異常を判断する**技術で、予め学習期間を置いて通常動作の負荷状況やシグナルパターンを学習し、それを仮の正常パターンとする。正常パターンの特徴は時間とともに変化するため、継続的な学習が必要。
 - 利点: **未知の攻撃**に対しても効果を発揮する。
 - 欠点: 正常と異常の閾値定義が難しいため、**誤検出が多い**。また、誤検出の原因が特定しづらい。
 - Stateful Protocolベース
 - セッションを監視し、それと**状態モデル**を照らし合わせることにより侵入を検知する技術。ただ、そもそもこの状態モデルの定義が難しく、例えば標準仕様をベースとしていても実装製品により取りうる状態が異なったり、車種ごとに微妙に差異がある。
 - 利点: 未知の攻撃に対しても効果を発揮する上、他2つよりも効果的に侵入を検知できる。
 - 欠点: 1つ1つのセッションに対して状態を管理する必要があるため、**膨大な計算機パワー**が必要。また、状態モデル定義がそもそも難しい。

今後10年を支える技術としての考察

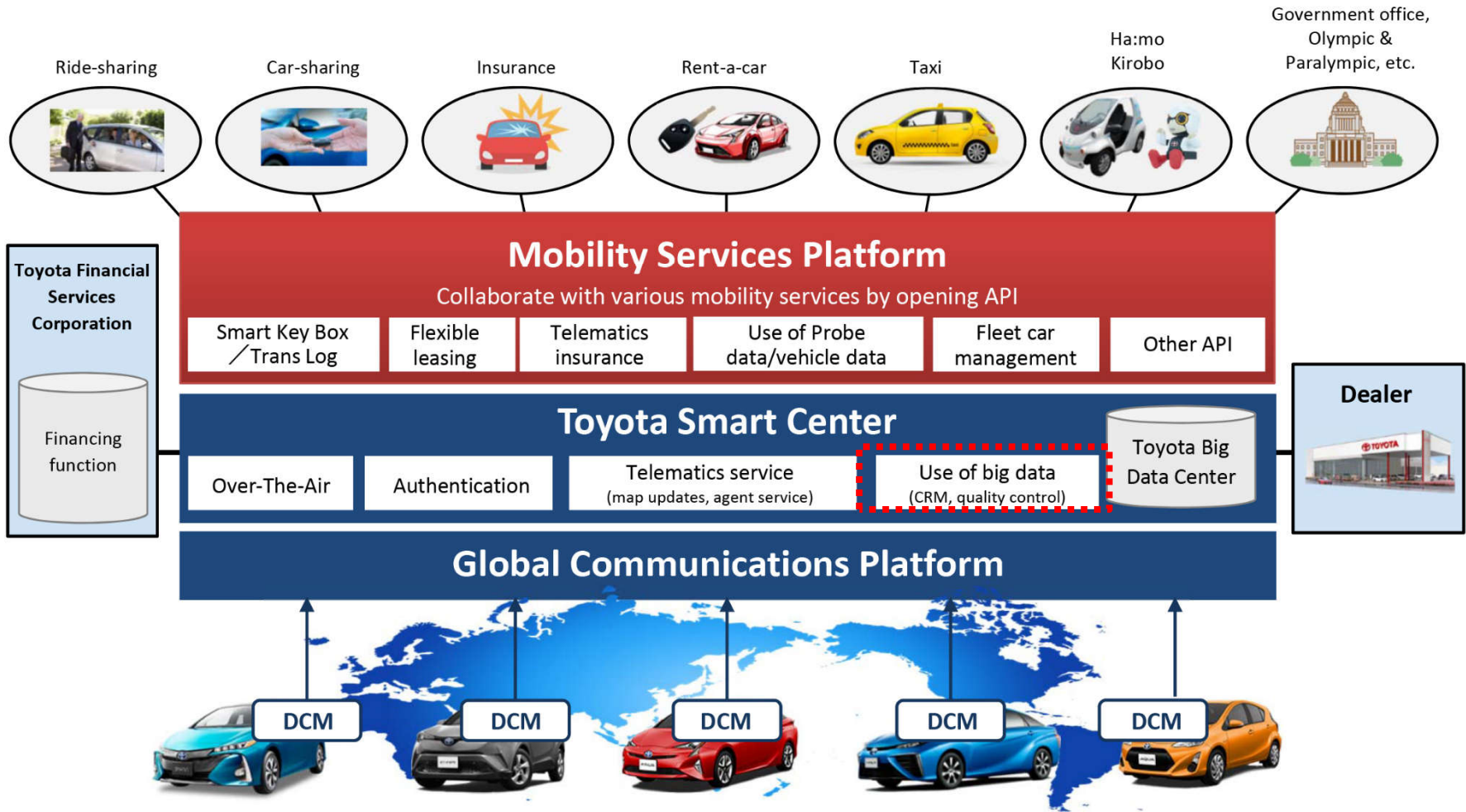
- 北米Security標準化活動
 - 標準化については、各社独自で対策を考えるのではなく、協調領域として、車両全体の開発を通じた技術、基準作りを進めている。特に北米で検討中のガイドラインSAE J3061は、人命に関わるISO26262との一貫性も考慮しており注目である
- プロセス面
 - Safety & Securityプロセスで二重苦・三重苦にならない工夫が必要
 - 車両全体は機能安全で定義されたシステムセーフティで守る。セキュリティ要因はリスクを踏まえたセーフティまたはセキュリティで対応する。
 - 車は人命、プライバシー、財産と保護対象が多岐に渡るため、脅威とSecurity Controlとの適正バランス・相場作りが課題。今後はリスクマネージメントに関するOEMを跨いだ議論が加速する見込み。
- 技術面
 - Connected Vehicle Platformから収集される膨大な車両情報を侵入検知に利用する検討が盛んになりつつある。ただし、開発した手法の良し悪しを図る評価フレームの定義が手薄。

3) Connected Vehicle Platform

BMW Series7



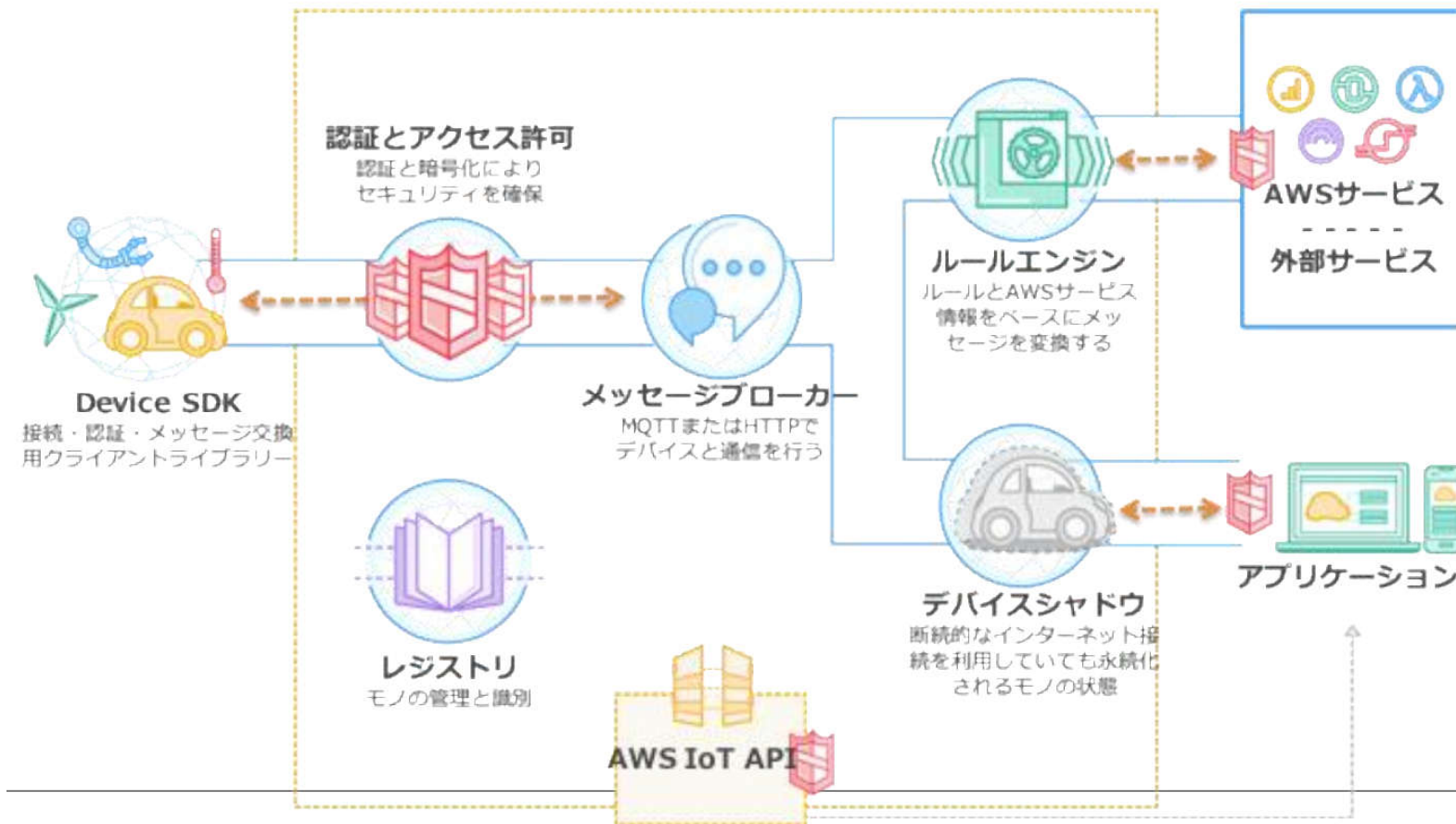
Connected Vehicle Platformを取り巻く現状



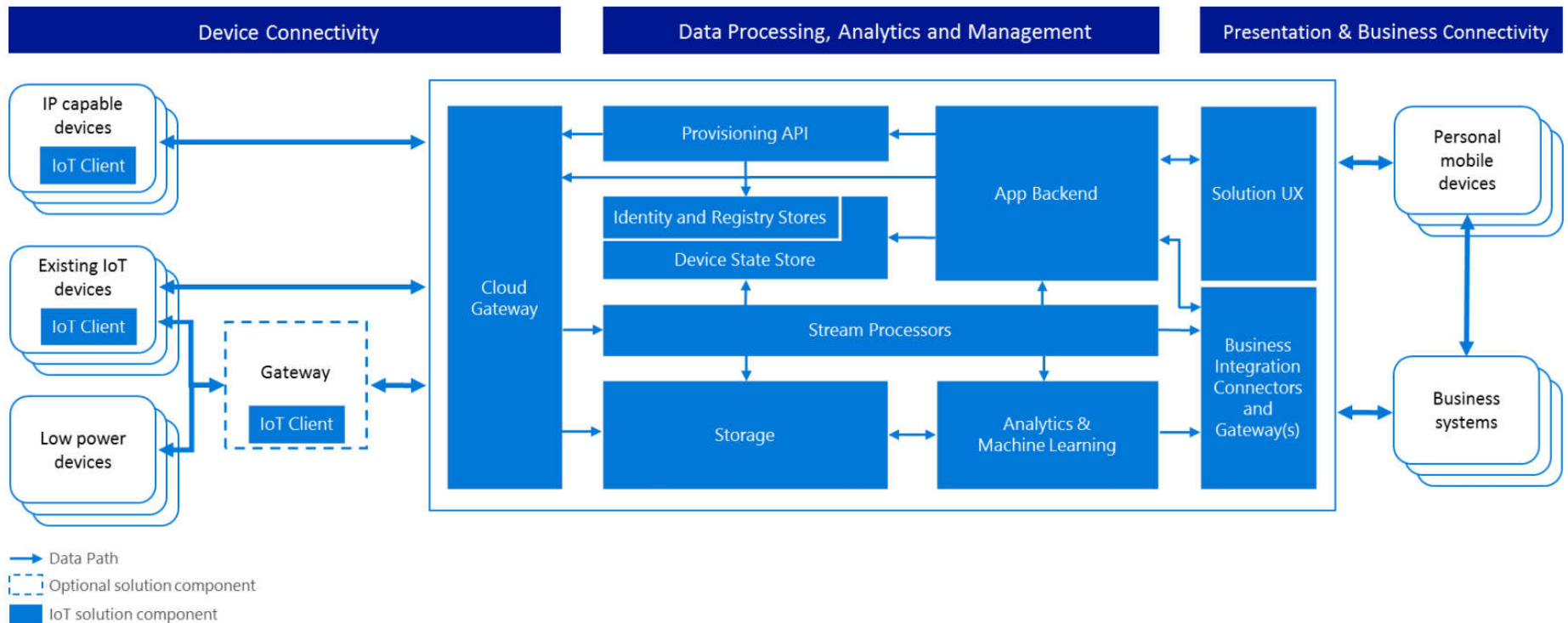
© Toyota Motor Corporation

出展: IEEE.org

AWS IoT Overview

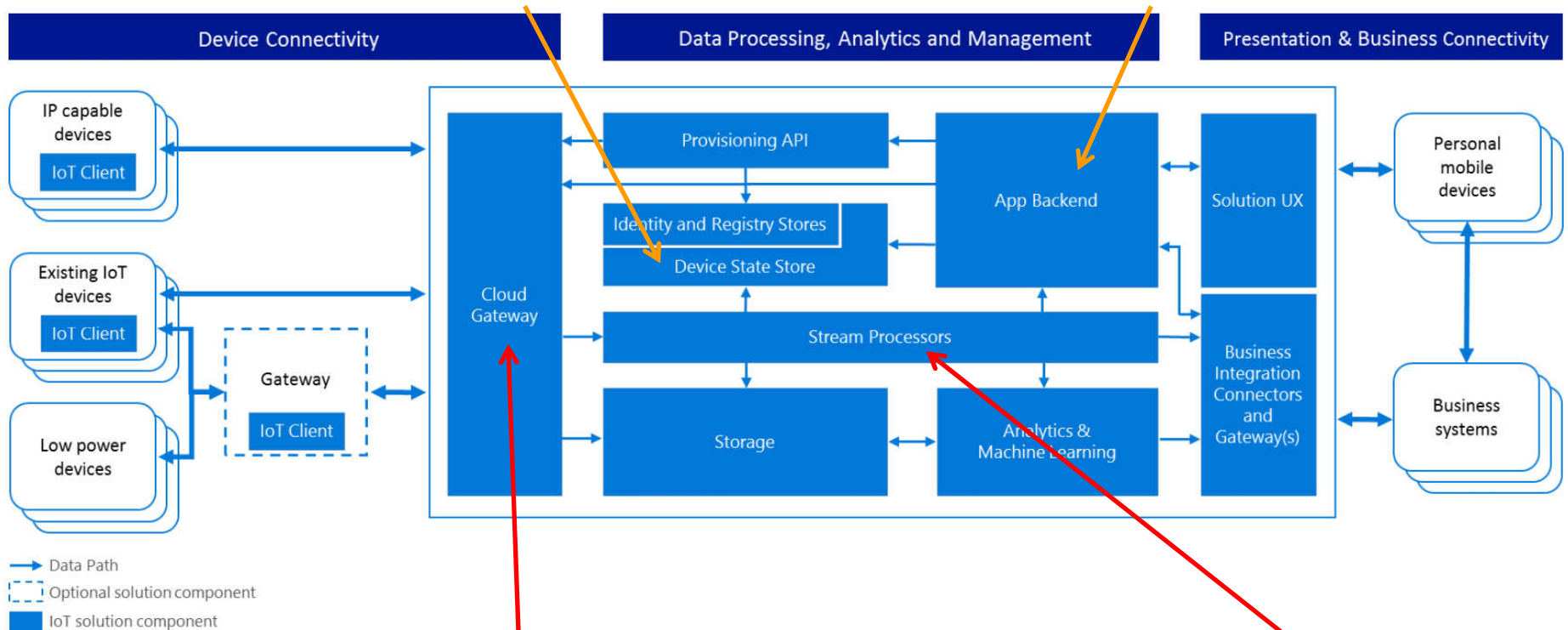


Microsoftが定義したIoT PFのリファレンスアーキテクチャ



③ 機器認証含むセキュリティ
(セキュリティに関しては説明済み)

④ 並列プログラミングモデルへの対応
(本日は対象外)

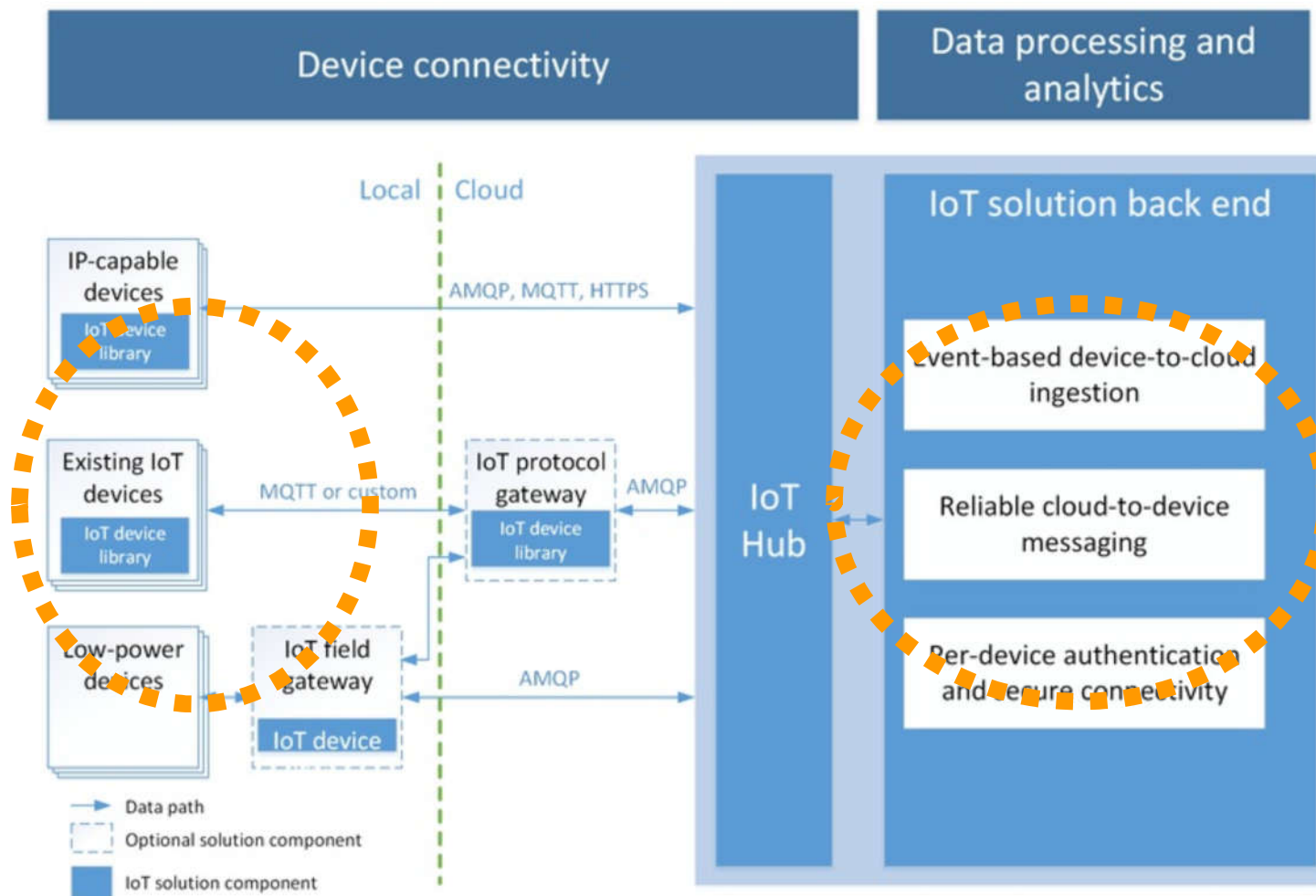


① Vehicle To Cloud通信におけるQoS制御

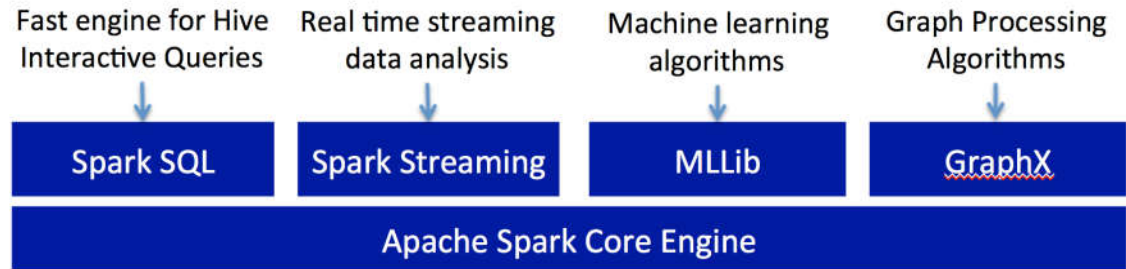
② 車両からの大量センサ情報のリアルタイム処理

① Vehicle To Cloud通信におけるQoS制御

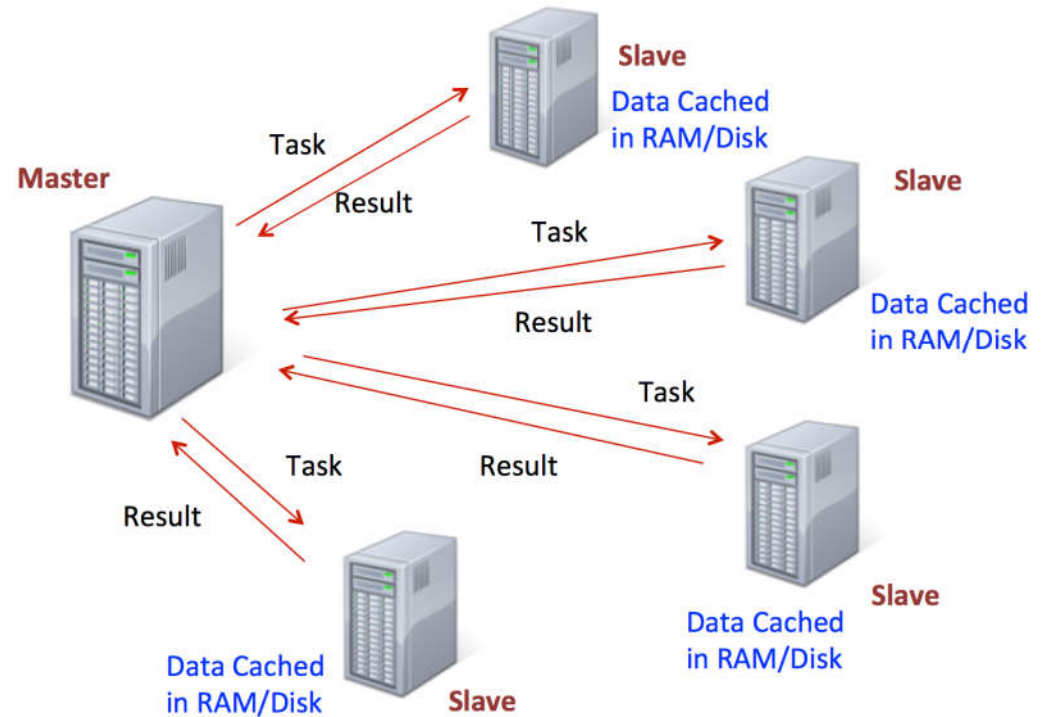
- 1) 適切なプロトコルの見極め(リアルタイム性、優先度制御、消費電力)
- 2) 通信が不安定な状態での、各制御系の自律制御



②車両からの大量センサ情報のリアルタイム処理



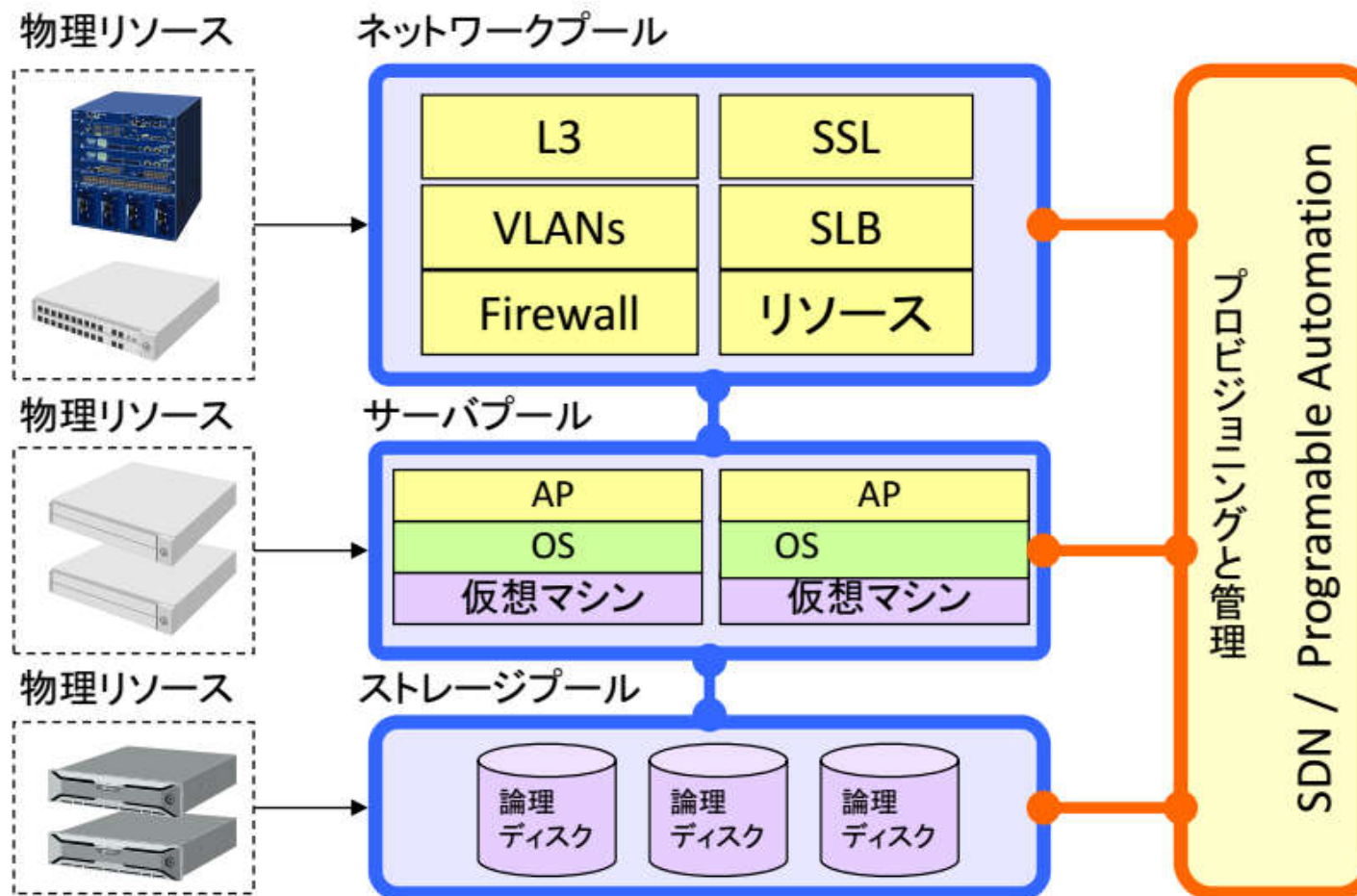
How does Spark execute a job

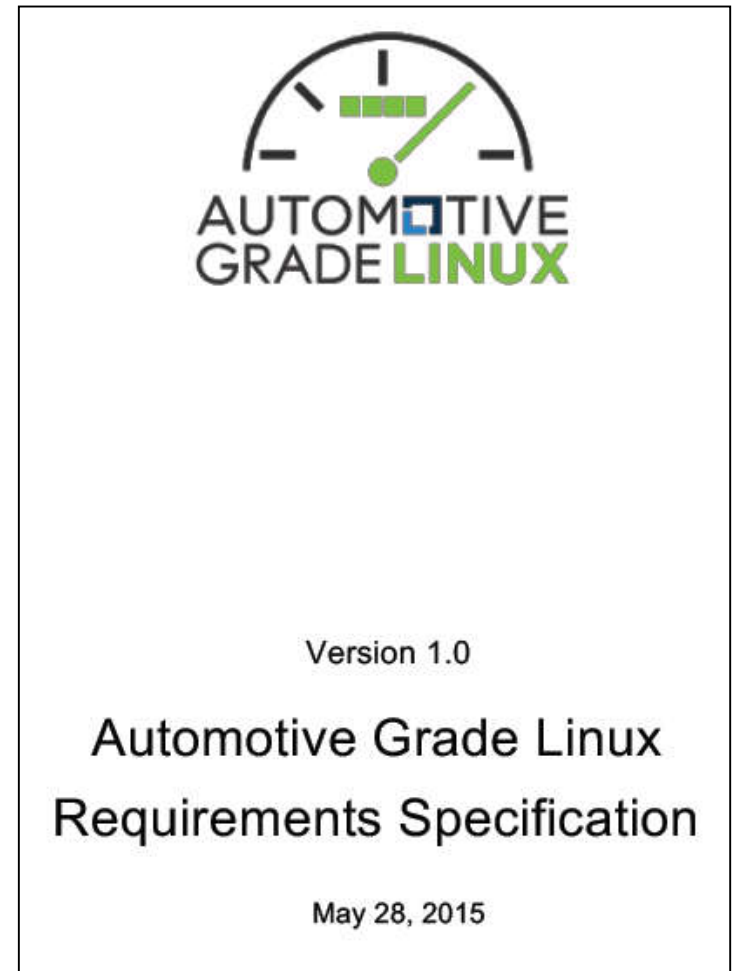
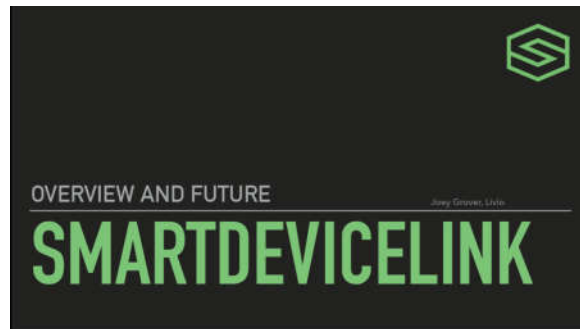


ビッグデータのリアルタイム処理には Slaveノードの規模特定がポイント

②車両からの大量センサ情報のリアルタイム処理

サーバの仮想化事例。
 サーバ規模拡張はVM単位で追加していくので、コスト試算はVM単位となる。





- IoT(Internet of Things)関連技術やビッグデータ分析基盤関連技術のブレークスルーが、車両制御や車両サービスに対して、イノベーションの波を起こしつつある
 - 「常時接続」「所有から利用へ」「自動化・知能化」「User Experience」がポイント
- 「ビッグデータ分析基盤を核としたクラウドからサービスの提供を受ける、ネットワークインフラに常時接続されたコネクテッド・カー」という構図は、ドライバ行動予測による燃費向上や、機械学習による自動運転支援といった新たなサービスを生み出しつつある
 - これら新たなサービスの受け皿としてのソフトウェアプラットフォームを総称して、Connected Vehicle Platformと呼称
- 今後10年を支えるConnected Vehicle Platformの要件
 - Flexibility & Openness
 - OTA, 各種標準化活動(SDL, AGL等)によるエコシステムの構築
 - Security & Compliance
 - Cyber-security, SAE J3061
 - Global Scale & Reliability
 - AWSやAzure等のITインフラとの融合

おわりに ～日本の大学生・若手技術者への期待～

- SWESTで鍛えられたこと
 - SWESTに参加することで、様々なバックグラウンド・年齢層を持つ技術者との議論の中において、自分の考えを表明する・立ち位置を確認する
 - SWESTセッションを企画運営することで、参加者の発言を即したり、議論の流れを整理したり、参加者の合意形成をサポートしたりといった、ファシリテーション技術
 - SWEST実行委員会に参加することで、社外人脈を構築することができた
- 今後のキャリアパスを意識して取り組んでいただきたいこと
 - 英語力向上
 - まずは単語力、次はリエゾンと多読
 - 設計力・抽象化能力向上
 - [設計力] 数多ある解決策の中かから最適解を探る
 - 技術的な最適解を選定する上で、実装力を失わない
 - ドキュメンテーション
 - [抽象化] 本質的な情報を引き出し、それ以外を捨てる判断力
 - 各種形式手法言語、LISP、Smalltalk、UMLメタモデルなど、いろいろな言語に触れるとよい