変化する未来自動車の５つの要素

AMO Labs CEO / 工学博士シン・サンギュ

CONTENTS

SPACE とは?

「モノのインターネット（IoT）」や「クラウド」のような言葉が日常的な用語となり、技術系で働かない人々にも、おなじみのものとなった。近年では、さまざまな分野で「第4次産業革命」が言及され、社会全般にわたって大きな変化と革新がもたらされるはずだと期待される。

まさに、第4次産業革命を率いる技術がIoTとクラウドだ。IoTは、ソフトウェアと相互接続（インターコネクト）を基本とした端末、自動車、家電などがネットワークに接続されてデータを交換できる一連のネットワークと定義される。[1] 第4次産業革命のために必要な要素はたくさんあり、IoTデバイスの種類も多い。特に第4次産業革命の主力となるのは自動車だろう。

出典：space.com

18世紀後半、蒸気機関車が商業的な目的で開発され、19世紀末に石油を使用する内燃機関エンジンを搭載した自動車が発明されて以来、自動車の変化は着実に続いた。自動車は、より安全に、より早く、より便利な移動手段としてわれわれの生活に欠かせないものになった。

最近では、自動車の限界を超えるような変化が起きている。近いうちにわれわれは空を飛んだり海の中を走る自動車を購入できるかもしれない。2018年2月、自動車は宇宙に行った。[2]イーロン・マスク（Elon Musk）が、「スペースX（SpaceX）」

[1] https://en.wikipedia.org/wiki/Internet_of_things
[2] https://www.space.com/39633-spacex-tesla-roadster-starman-final-photo.html

の宇宙船で「テスラ（Tesla）」の自動車を宇宙に送ったのだ。

イーロン・マスクという人物があまりにも独特な人物だということもある。だが、この出来事は「従来の自動車が持っていた限界を超える」という新しい観点をわれわれに提示した。

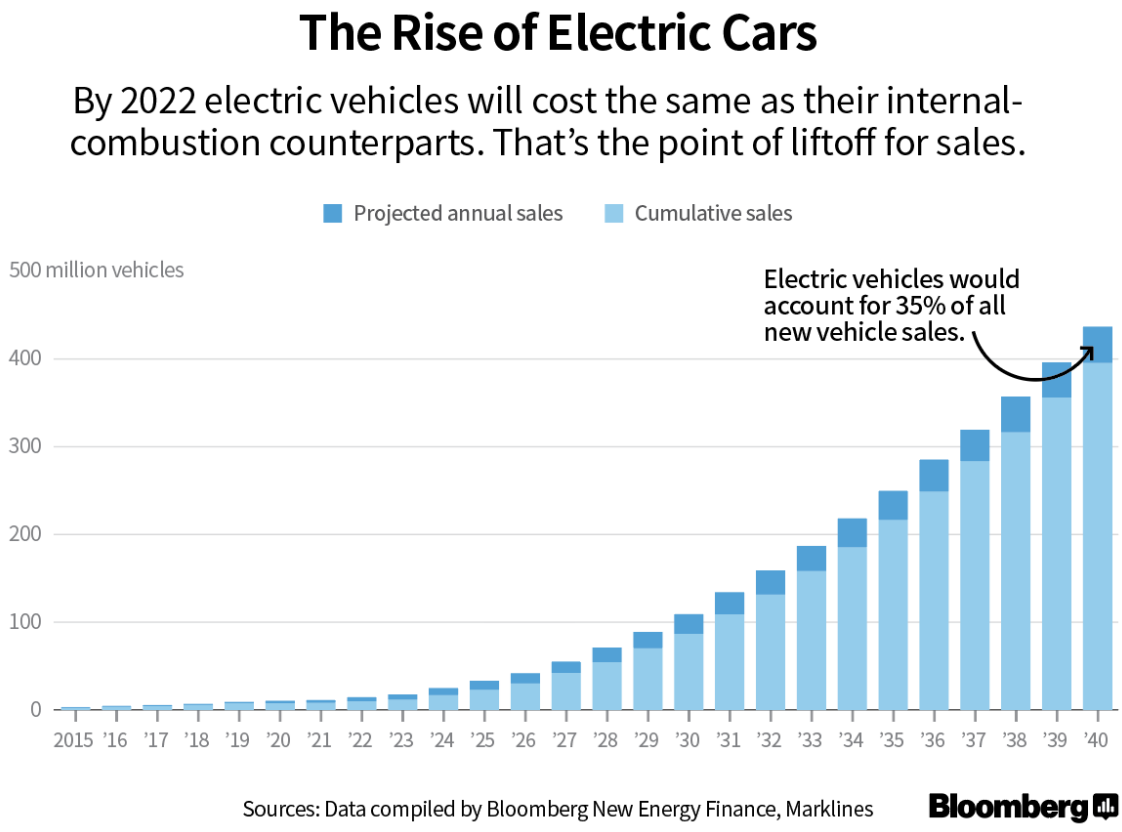
宇宙を意味する単語「SPACE」は、空間という意味も持つ。筆者には自動車と空間が別の概念とは思えない。自動車が提供する移動性が人間の生活空間を広めた。自動車の運転中の室内空間もまたわれわれの一つの生活空間となった。もはや、地球という空間（SPACE）の限界を超え、宇宙（SPACE）まで行った自動車をみることになったのだ。

ここで筆者は、宇宙または空間を意味する「SPACE」に、Security（セキュリティ）、Platform（プラットフォーム）、Autonomous（自律性）、Connectivity（連結性）、Electrification（電化）の5つの単語の組み合わせとして再定義したい。人々からよく「未来の自動車」と言われるスマートカー（Smart Car）が上記5つの技術概念を必然的に要求するからだ。

電化 Electrification

イーロン・マスクは、自動車を宇宙に送ったが、彼は電気自動車専門の自動車メーカー、テスラをリードする人でもある。私たちの周りで電気自動車を見ることは、さほど難しいことではなくなった。純粋な電気自動車（EV）だけでなく、ハイブリッドカー（HV）やプラグインハイブリッドカー（PHV）まで含めれば、もはや電気自動車はありふれたものだ。

自動車分野で起きている変化はこれだけではない。自動車の変化を見てみよう。英国とフランスは、2040年からガソリンやディーゼルなどの化石燃料を使用する内燃機関車の生産を禁じることを発表した。[3] オランダも2030年からは内燃機関車の生産を禁じることを発表し、ドイツも2030年から内燃機関車の生産を禁じる方案を検討中だ。[4] ボルボ（Volvo）は2019年以後、内燃機関車両の開発を中断すると宣言した。[5] 2040年には新車モデルの35%が電気自動車になるという見込みもある。[6]



内燃機関エンジンを使用する自動車が、エンジンの動力を車輪まで伝えるためのパワートレイン（Powertrain）を中心に

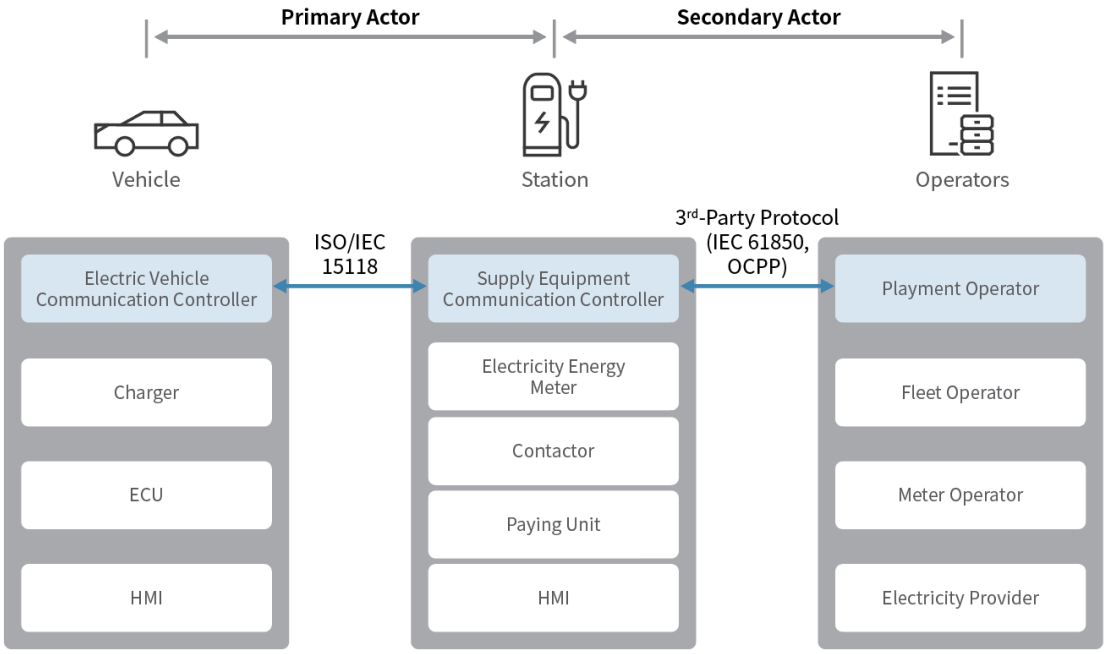
[3] http://global-autonews.com/bbs/board.php?bo_table=bd_008&wr_id=2387
[4] http://thegear.co.kr/15232
[5] http://www.autodaily.co.kr/news/articleView.html?idxno=336321
[6] https://www.bloomberg.com/features/2016-ev-oil-crisis/

動作することに比べ、電気自動車は電池とモーターを組み合わせることで単純かつ軽い構造で動作できるメリットがある。そのため、電池充電の頻度と所要時間が電気自動車の便利さや性能を示す主要指標にもなる。だが、電気自動車の充電はバッテリーに電荷を満たすだけの単純な作業と勘違いされやすい。実際のところ、電気自動車の充電ケーブルは電気を伝えるだけでなく、データの送受信も一緒に行われるように作られている。私たちが使用するスマートフォンをコンピューターに連結すれば、充電とデータ同期化が同時に行われることを連想すれば分かりやすいだろう。

電気自動車の充電ケーブルは、新たな通信チャンネルだと理解する必要がある。例えば、充電中に消費した電気料金の支払いが車両と充電器の間の通信によって自動的に行われるようになるだろう。このようなサービスは、「プラグ＆チャージ（Plug&Charge）」あるいは「プラグ＆ペイ（Plug&Pay）」と呼ばれる。停車中の有線充電ではなく、走行しながら充電できる無線充電が実用化したら、プラグ&チャージ技術は今後さらに主要な技術になるだろう。

充電にかかる時間も新しい意味を持つことになる。電気自動車の充電は数秒では終わらない。数十分あるいは数時間かかるものだ。この間、車両と充電器の間には安定的な通信チャンネルが維持されるので、車両を診断したり車両に必要なソフトウェアや情報を更新することも可能だ。

つまり、充電器が車両に電気を供給しながら車両を診断したり、車両にソフトウェアを供給する接点の役割も果たすようになるのだ。充電器と連結し、決済を含むさまざまなサービスを提供する主体を電気自動車分野では「セカンダリーアクター（Secondary Actor）」と呼ばれる。



車両と充電器（プライマリーアクター）、充電器と各種サービス（セカンダリーアクター）の間で通信が行われるようになれば、安全のためのセキュリティが重要になる。

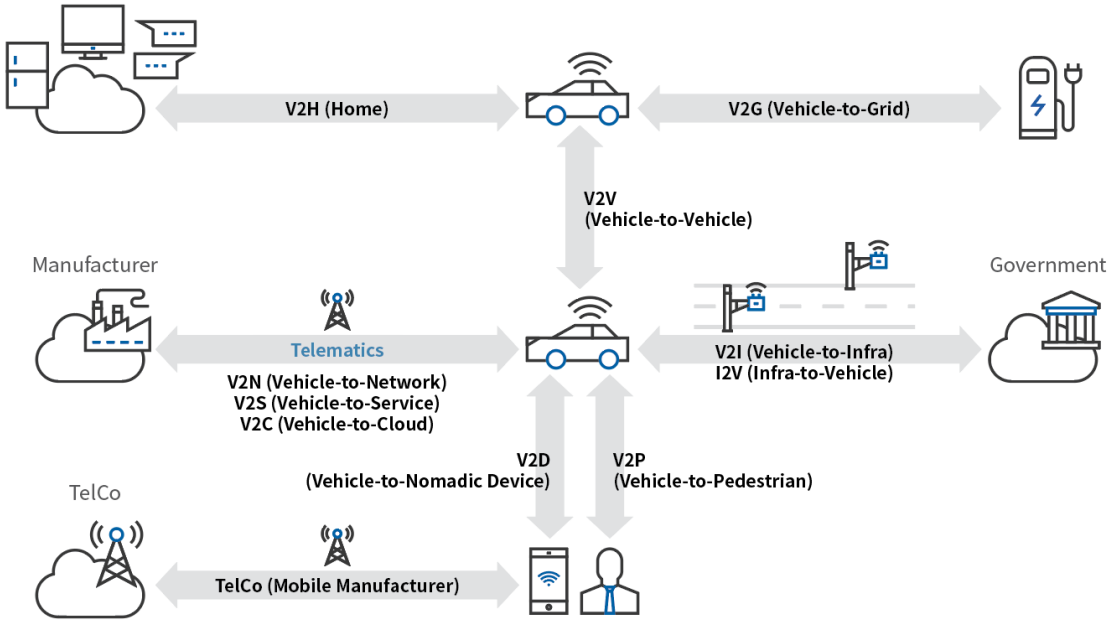
通信で連結される主体間の認証を提供し、機密性が必要なデータには暗号化を提供し、整合性と認証性が必要なデータには電子署名を提供することがセキュリティの基本的な範囲だ。決済を安全に提供してセカンダリーアクターが提供するサービスの信頼度を確保することもセキュリティが解決しなければならない宿題だ。

連結性 Connectivity

IoTに分類されるデバイスとそうではないデバイスを仕分ける核心は連結性だ。IoTという文脈の中で最も重要な位置の1つを占める自動車が、従来の自動車と区別される核心的な機能もまた連結性だ。従来の自動車にも連結性がなかったわけではない。スマートフォンをBluetoothで連結して電話したり、音楽を聴いたりするのも連結性だ。モバイルアプリで自動車のドアの鍵を開閉したり、エンジンをかけたりする機能を提供するテレマティクス（Telematics）も通信会社を通じた移動通信を使用する。

一方、コネクティッドカー（Connected Car）と呼ばれる自動車は、従来よりも幅広い連結性を追求する。自動車と自動車の間の通信である「V2V」（Vehicle-to-Vehicle）、自動車と道路などのインフラ間の通信である「V2I」（Vehicle-to-Infra）、自動車と電力網の間の通信である「V2G」（Vehicle-to-Grid）、自動車とモバイル機器間の通信である「V2D」（Vehicle-to-Nomadic Device）、自動車と家を連結する「V2H」（Vehicle-to-Home）などがこれに該当する。

自転車、二輪車などの交通手段や歩行者との通信である V2P（Vehicle-to-Pedestrian）も新しい通信モデルとして浮上する。自動車メーカーは、テレマティクスを通じた断片的なサービスよりも、さらに幅広いサービスの実現に向けてクラウドやオンラインサービスとの連結を提供できる通信モデルを準備している。この通信モデルは、「V2N」（Vehicle-to-Network）、「V2S」（Vehicle-to-Service）、「V2C」（Vehicle-to-Cloud）などの名称で呼ばれている。



V2Gモデルは、前述した「電化」で説明したように、電気自動車が充電器を通じてセカンダリーアクター（Secondary Actor）と連結されるサービスを反映したものだ。V2Hモデルで主導権を先取するため、サムスン電子などの家電メーカーはスマート冷蔵庫やスマートテレビと自動車との連結を試みている。フォルクスワーゲン（Volkswagen）は、2016年のCES展示会でLG電子の冷蔵庫と連結するシナリオに沿った展示をした。

最近は、音声認識機能を搭載したスマートスピーカーの躍進が目立つ。これをリードするのは、Amazonの「Alexa」（アレクサ）だ。2018年のCESでは自動車だけでなく、IoT機器をAlexaと連結した製品がたくさん展示された。Alexaとアマゾンのクラウドサービスを媒介に、自動車とIoT機器、家が連結されるシナリオが自然に完成された。類似の試みは、アップルの「CarPlay」（カープレー）やグーグルの「Android Auto」（アンドロイドオート）でも、それぞれのクラウドサービスを通じて行われている。

各国政府が興味を持つ分野は、V2VとV2Iモデルだ。V2V通信を通じて車両間の衝突事故を、V2I通信を通じて安全運転に必要な交通情報を提供することで交通事故を減らし、安全性を高めることを目指す。米国、欧州、日本、中国、韓国で推進される次世代交通システム「C-ITS」（Cooperative Intelligent Transportation System、協調型高度道路交通システム）事業は、V2VとV2I通信を基盤にして交通システムを革新するものだ。今後のV2Pモデルも次世代交通システムに反映されると予想される。

自動車メーカーがリードするV2CやV2S、V2Hモデルを通じて、自動車は単なる移動手段から、さまざまなオンラインサービスを活用する新たな空間として価値を高め、新しい事業の創出が期待されている。これはSPACEの中の「プラットフォーム」部分と大きな関連性を持つ。

よく自動車の未来像を「スマートカー」（ここにはコネクティッドカーも含まれている）だという。自動車がスマート機器の一つになるということだ。私たちが既に持つスマート機器が一つが「スマートフォン」だ。スマートフォンに連結性がない、特にインターネットにつながらないと仮定してみよう。恐らく「どうやって使ったらいいか」で悩むことになるだろう。新たなスマート機器であるスマートカーも同じだ。自動車がスマートカーに進化するためには連結性が必要なのだ。

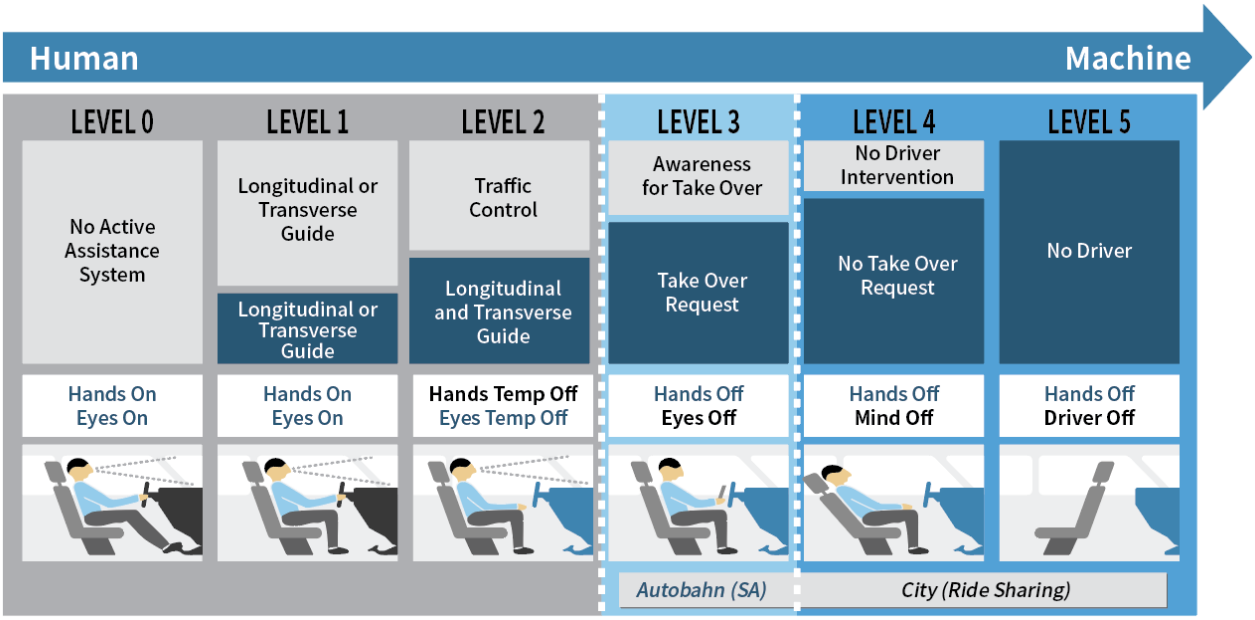
自動車の安全度を高めたり、活用度を高めるために連結性は重要な役割をするが、連結性を持つために通信チャネルが公開されることはセキュリティ上の脅威とも共存することになる。信頼できない主体が生成した誤った情報が自動車の運行を妨害したり、露出した通信チャンネルを通じてクラッカーに攻撃されたりするだろう。自動車の制御を乗っ取られるかもしれない。情報漏えいなどのセキュリティ事故は金銭的な被害で収まる。だが、自動車のセキュリティ事故は人の生命と安全に直結する。それ故にセキュリティの重要度が非常に、いや、最も高くなる。自動車を外部と安全に連結するためにはセキュリティの課題は必ず解決しなければならない。

自律走行 Autonomous Driving

自律走行は、未来を描いたドラマや映画でおなじみ技術だ。だが、自律走行は既に未来の技術ではない。船舶や飛行機では一部でオートパイロット（自動操舵）を使って運航されている。決められた航路に沿って自律走行をする船舶や飛行機と違い、自動車は急変する道路状況に対処しなければならない。そのため自律走行の適用が簡単ではなく、未完の技術として研究が重ねられている。

たくさんの企業が巨額の資金をつぎ込んで自動車向けの自律走行技術を開発している。自律走行自動車の交通事故で死亡者が発生したという記事も主要なニュースとして取り上げられている。

自律走行技術のレベルを定義した「SAE J3016」では、自動運転レベルを 0 から 5 までの 6 段階に分け、レベル 3 以上を技術を搭載した自動車を「自律走行自動車」（Autonomous Vehicle）と見る。

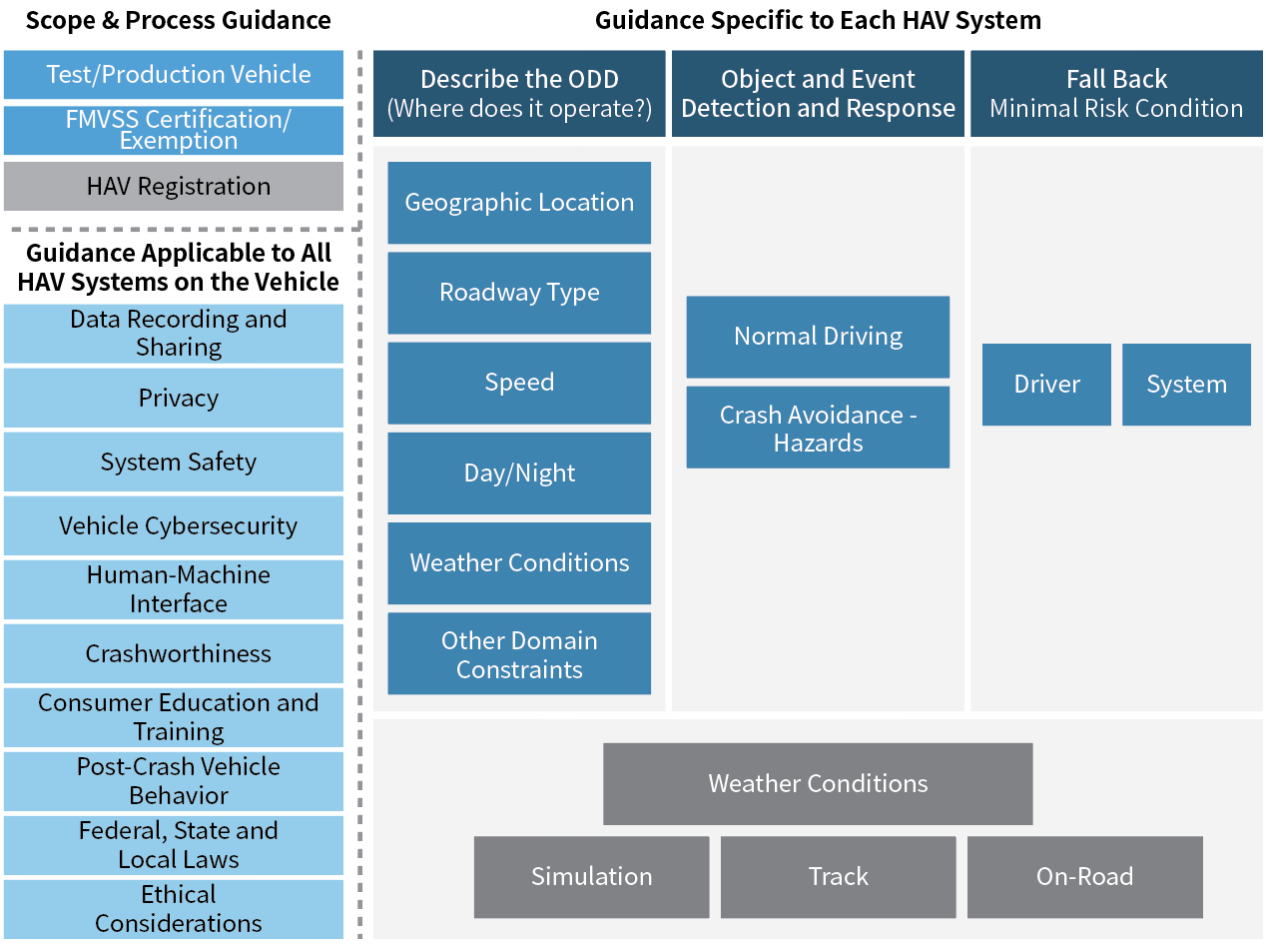


出典 ：iQ.intel.com

ある自動車メーカーはレベル3の技術を開発したといい、別のある自動車メーカーはレベル4の技術に成功したという。果たして、レベル4の技術はレベル3よりも優れたものなのだろうか。そうかもしれないし、そうではないかもしれない。

米国運輸省（DoT、Department of Transportation）傘下の道路交通安全局（NHTSA、National Highway Traffic Safety Administration）が2016年に作成した「Federal Automated Vehicles Policy」では、「ODD」

（Operational Design Domain、運行設計領域）という概念を自律走行の構成要素に含めた。



出典："Federal Automated Vehicles Policy", NHTSA, 2016

ODDは、自律走行が動作できる条件である「地理的位置」「道路類型」「走行速度範囲」「天気」などの制約を含む。ODDが同一であれば、レベル3の技術よりもレベル4の技術の方が優れた技術であることは間違いない。だがODDが異なれば、どの技術がより優れた技術なのかを判断することは容易ではない。快晴でドイツのアウトバーンを走れるレベル4の技術と、可視距離が数十メートルしかない大雨の状況でも都心の繁華街を走れるレベル3の技術を比較するのは難しい。

NHTSAの文書は、自律走行自動車が順守すべき技術の要素として「サイバーセキュリティ」（Cyber Security）を明示している。自律走行とセキュリティにはどんな関係があるのだろうか。

自律走行自動車は、自動車に搭載されたカメラ、レーダー（Radar）、ライダー（LiDAR、レーザー光による検知と測距)、赤外線センサーなどのさまざまなセンサーを通じて周辺を認識して、どのように走行するかの判断をリアルタイムでする。センサー

から収集したデータを分析し、リアルタイムで判断することがまだ未完の技術であり、悲劇的な事故の発生につながることもある。2016年に発生したテスラの交通事故は、左折する白いトレーラーの横面と空を区分できなかったせいで発生した事故だった。[7] それなら、クラッカーがセンサーの正常動作を妨害したり、信号をかく乱したりして、自動車が誤った判断を下すように誘導することも可能ではないか。

人間は真正面から強力な光を当てられると、しばらく前が見えない状態になる。同じように自動車のカメラに強力な光が照らされると、自動車はすぐ前の障害物も識別できなくなる。このような攻撃は高価な装備や高度の技術が必要なものではない。性能の良い電灯や大きな鏡だけで実行できる犯罪だ。

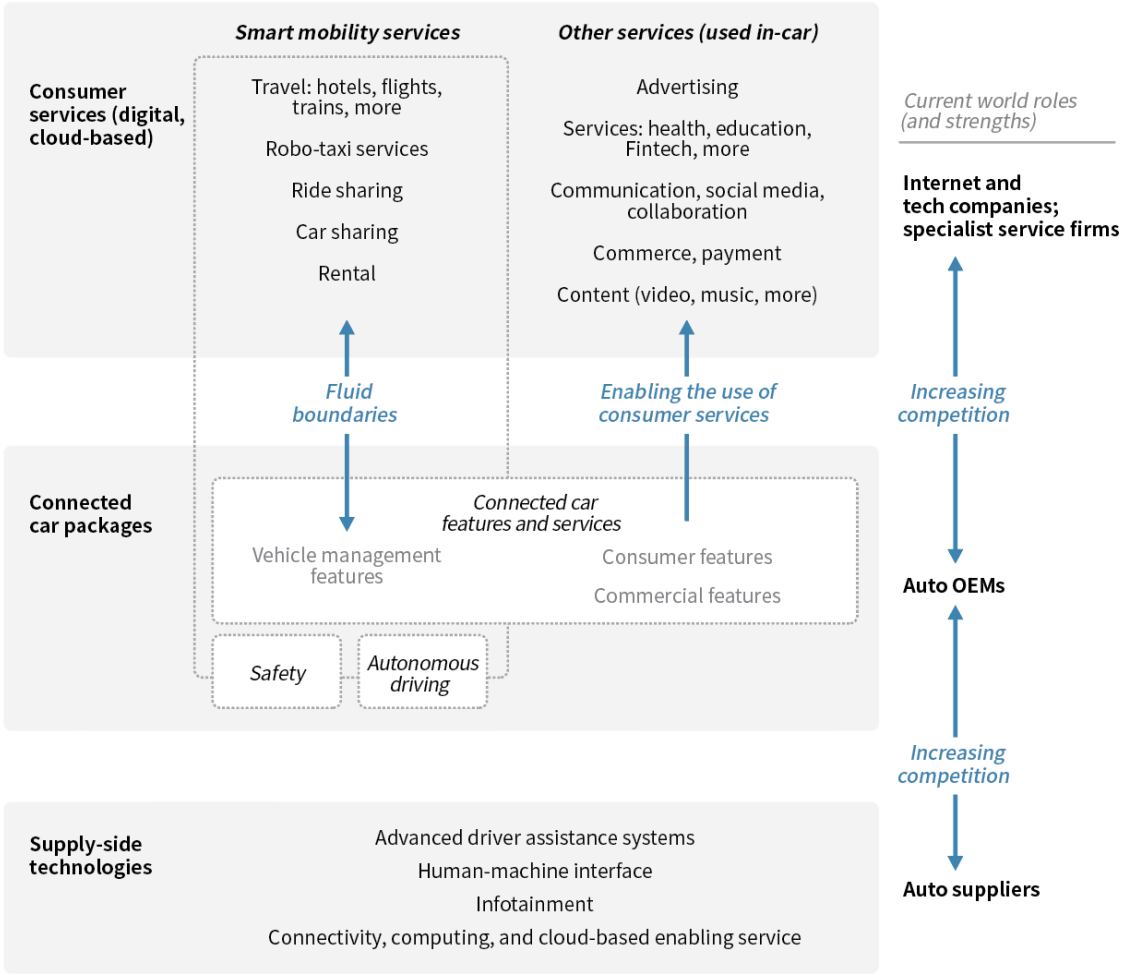
車両の内蔵センサーだけでは、周辺の状況を正しく判断することに限界がある。だからこそ、自動車が周辺の自動車や道路と情報をやりとりしながら自律走行をするのだ。このような自律走行を「自律協力走行」という。「連結性」で説明したV2VとV2Iが自律協力走行でも使用されるのだ。外部との通信を通じて周辺状況の情報を得るためには、通信相手に対する信頼を検証し、通信チャンネルの信頼可否を検証することが必要になる。

自律走行で使用される、また違う形の通信がある。自律走行タクシーを運営するタクシー会社を想像してみよう。タクシーを利用しようとする乗客がタクシー会社に要請すれば、タクシー会社は所有するタクシーの中から特定のタクシーに利用客の状況を伝えなければならない。それ以前にタクシー会社はタクシーの現状をリアルタイムで把握し、顧客の需要が多発する場所にタクシーを移動させておくことも必要だろう。この場合に V2N もしくは V2C モデルの通信を利用することになる。自律走行自動車は外部通信を活用するためのセキュリティも確保しなければならないのだ。

[7] http://www.straitstimes.com/world/united-states/tesla-car-on-autopilot-crashes-killing-driver

プラットフォーム Platform

自動車が連結性を持つことになり、ネットワークに連結されている自動車を活用する様々なサービスが新しく開発されている。従来の自動車産業は、部品サプライヤーと完成車メーカーで構成される自動車生産産業や、自動車が顧客に販売されてから形成される市場（After Market)を通して販売される部品市場、そして自動車販売と関連した金融および保険市場で構成されていた。しかし、自動車に付加された連結性は、従来の市場とは違う様々なサービスを生み出している。



出典 ：pwc.com

新しく話題になっているサービスの中で最も代表的なサービスは、自動車公有サービス（Car Sharing service)だ。ソフトウェアがオンデマンド（On Demand)方式のサービス形式で提供されるSaaS(Software-as-a-Service)にたとえ、自動車公有サービスがMaaS(Mobility-as-a-Service)に発展していると説明する専門家たちもいる。他の概念では「Pay as you dirve」と

も言えるが、自動車を利用した分だけ費用を支払う方式を意味する。このような概念を適用した保険製品も登場している。

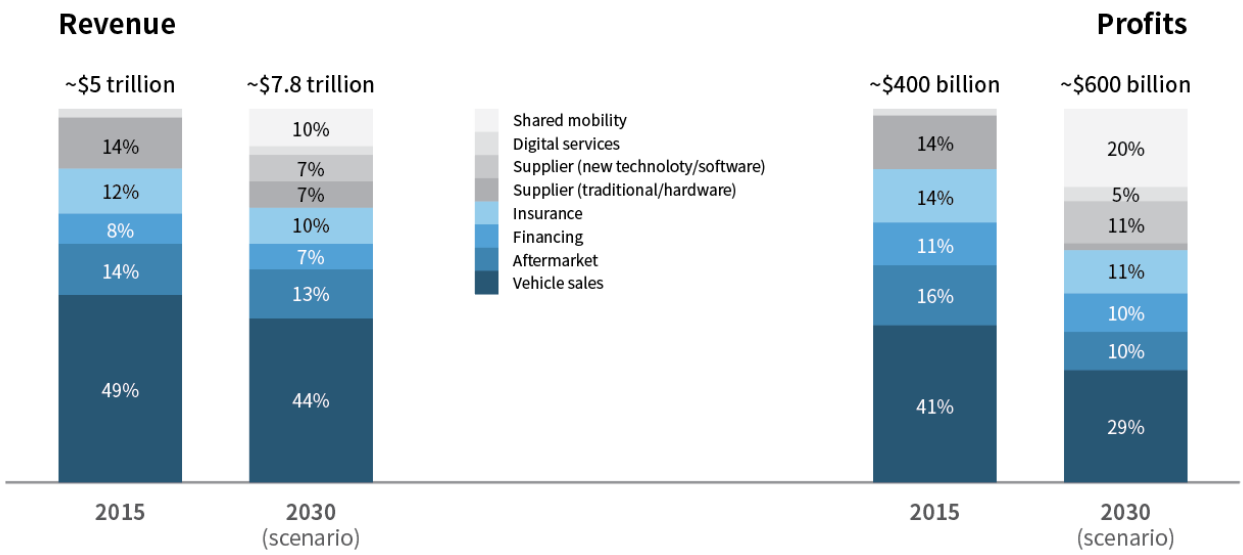
私たちが使っている携帯電話がフィーチャーフォン（Feature Phone)からスマートフォン（Smart Phone)へと進化して行った過程を見てみると、フィーチャーフォンも制限的だが、インターネットを使うことができた。しかし、スマートフォンへ進化しながら、インターネットへの連結範囲はさらに拡大され、活用方式も多様になった。例えば、フィーチャーフォンのソフトウェアは、メーカーにより一度搭載されると、消費者が任意に選択・修正することができないが、スマートフォンのソフトウェアは利用者が選択してインストールし、自分の好みに合わせて設定することができる。

コネクティッドカーがスマートカーに変わって行く過程は、フィーチャーフォンがスマートフォンに変わって行く過程と似ているはずだ。自動車のソフトウェアは自動車メーカーの選択によってインストールされるのではなく、利用者の選択によってインストールされ、インターネットへの連結範囲は幅広く多様になるはずだ。

スマートフォンの拡散になり、多様なサービス・プラットフォームと生態系(Eco system)ができた。アイフォン(iPhone)を開発したアップル(Apple)社は、アップストア(App Store)とアイチューンズ・ストア(Itunes Store)を介し、アイフォン(iPhone)利用者にソフトウェアやマルチメディア・コンテンツを提供するプラットフォームを作り、さらに、これを通じてアプリ開発社とコンテンツ提供社を結ぶ生態系を作ることにより、プラットフォームと生態系が新しい付加価値市場を作り出すという事実を証明した。アップル(Apple)社の売上は、2017年第4四半期基準で526億ドルであり、そのうち、プラットフォームによるサービスの売上が85億ドルに達する。[8]

自動車産業でもこのような変化や革新が起こると期待されている。自動車というハードウェアを販売し、自動車に搭載したり付着可能なアクセサリーを販売することにとどまらず、自動車を利用するに便利なサービスが巨大な新規市場を形成すると見込まれる。アイフォン(iPhone)、アイパット(iPad)などのハードウェア販売のみならず、プラットフォームを活用したサービスによっても売上を出しているアップル(Apple)社のビジネス仕組みと似ている。

[8] https://www.macrumors.com/2017/11/02/earnings-4q-2017/



出典 ：pwc.com

2015年と2030年展望を比較した資料[9]をみると、新しい技術やソフトウェアのサプライヤー（Supplier of New Technology and Software)が生み出す市場、サービス（Digital Service)が作り出す市場、カーシェアリング(Shared Mobility)のような新規事業が作り出す市場の規模は、2015年では売上基準で3%未満、利益基準で４％未満になると推算された。 一方、2030年では、売上基準で19%、利益基準は36%に達すると予測されるという。

EU28ヵ国の国土交通大臣は、「コネクティッドカーおよび自律走行自動車分野における協力」を目指し、2016年４月にアムステルダム議定書(Declaration of Amsterdam)[10]を採択して公表した。この議定書には大きく8つの協力項目が盛り込まれている。その中でデータ使用(Use of Data)の部分は、コネクティッドカーと自律走行自動車の利用により生成されたデータを活用し、公的もしくは私的な付加価値サービス（Public and Private Value-Added Service)を作り出せると書いてある。

これは、自動車データを収集し、加工して新しいサービスとして利用者に提供可能であることを意味する。車両がオンライン上のコンテンツとリソースにアクセスすることに対しては、ISO20077とISO20078標準の拡張車両(ExVe;Extended Vehicle)にて定義されている。これらの標準には、HTTP通信のWeb技術を基に、自動車がオンライン上のコンテンツと情報リソースにアクセスする方法を含めている。

新しいサービスによる新規市場の胎動を予測する一方で、自動車がオンライン上の情報リソースにアクセスする方法を標準

[9] https://www.strategyand.pwc.com/reports/connected-car-2016-study

[10] https://english.eu2016.nl/documents/publications/2016/04/14/declaration-of-amsterdam

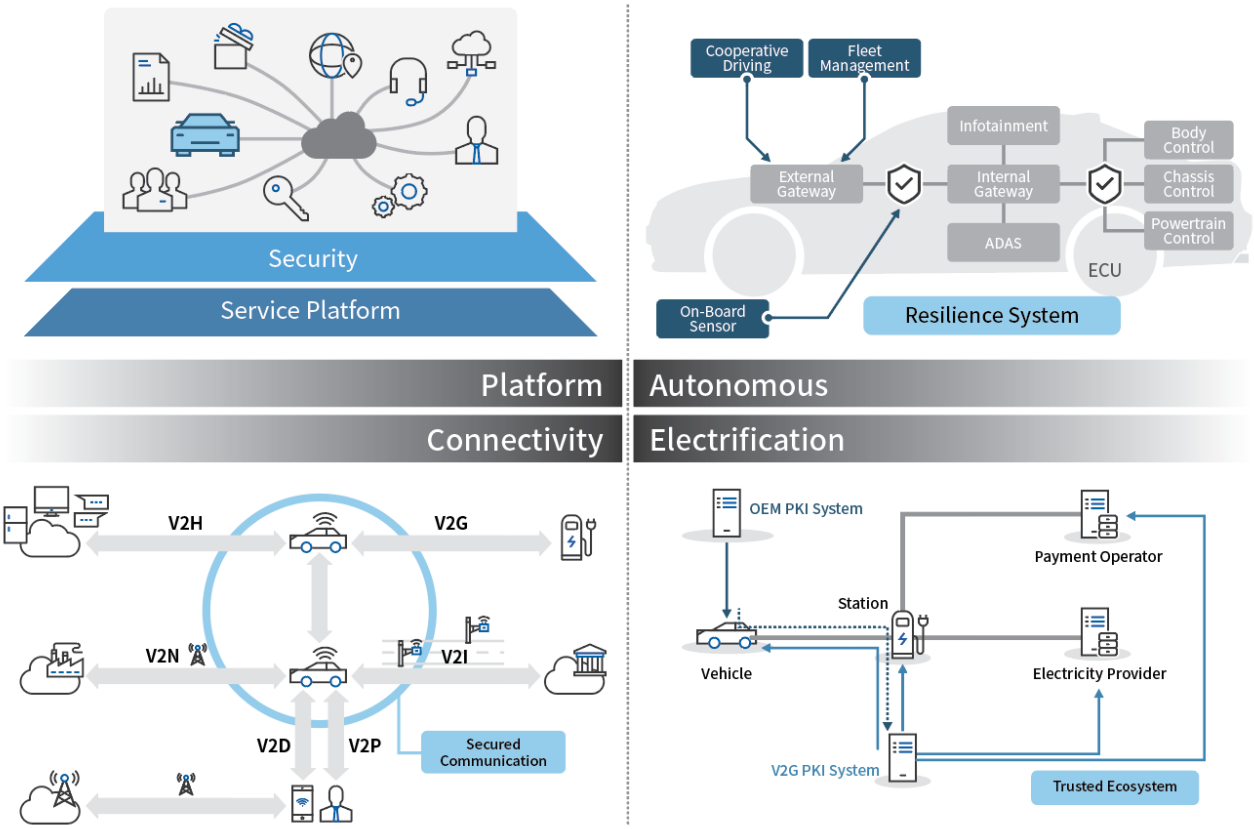
化している。スマートフォンに新規のアップリケーションをインストールすると、スマートフォン内部のデータを収集し、オンラインサーバへの提供に同意することを求められる。私たちは意識せずそれに同意し、オンラインサービスを楽しむ。これは、私たちが今後、自動車に対し取る態勢でもある。自動車からオンラインサーバへとデータが収集され、オンラインサーバから自動車へとサービスが提供されるというオンラインサービス・プラットフォームが求められる時期が来る。従来の自動車が速く移動するための交通手段に過ぎなかったら、将来の自動車のスマートカーは、オンラインサービスを活用する新しい空間になるはずだ。

自律走行技術の完成度が高くなればなるほど、ドライバーは運転することから解放され、解放された分、多様なオンライサービスを活用できようになる。地下鉄とバスの中で多くの人がスマートフォンで何かをしているではないか。

新しいサービスは、自動車があるから可能になるものではあるが、自動車がその中心にあるわけではない。スマートフォンで利用可能なオンラインサービスの中で、スマートフォンのみで利用可能なサービスは殆どない。利用者はスマートフォン以外に様々なデバイスや環境でサービスが利用でき、利用者以外に他の多くの主体が参加するケースも多い。スマートカーと連結されるサービスも同じく、サービスプラットフォームが中心になり、スマートカーは、スマートフォンなどの多様なデバイスと連結され、多くの主体が参加できるようになるだろう。アップル(Apple)社がプラットフォームを基盤に生態系を構築し、スマートフォンの利用環境をリードしていることを繰り返し考えてみると、生態系の基盤となるプラットフォームが、スマートカーの発展を牽引する肝心な要素になることに疑いはないはずだ。

セキュリティ Security

電化（Electrification)、連結性（Connectivity)、自律走行（Autonomous)、プラットフォームplatform）化による様々な変化を探ってみた。電化、自律走行、プラットフォーム化においても外部通信が基本道具で使用されるため、連結性は、これらの変化のスタート時点とも言える。



自動車が外部と連結されるV2V、V2I、V2P、V2D、V2H、V2G、V2Nなどの様々な通信モデルにおいてセキュリティは、必ず先決されなければならない課題として確認されている。セキュリティが保障されていない状態で連結のみ行うことは危険であることに疑う余地もないだろう。セキュリティ対策を立てた後に連結をするのが意味があるため「セキュリティから始まる。そして、つなぐ(Secure First、Then Connect)」の戦略が核心戦略にならなければならない。

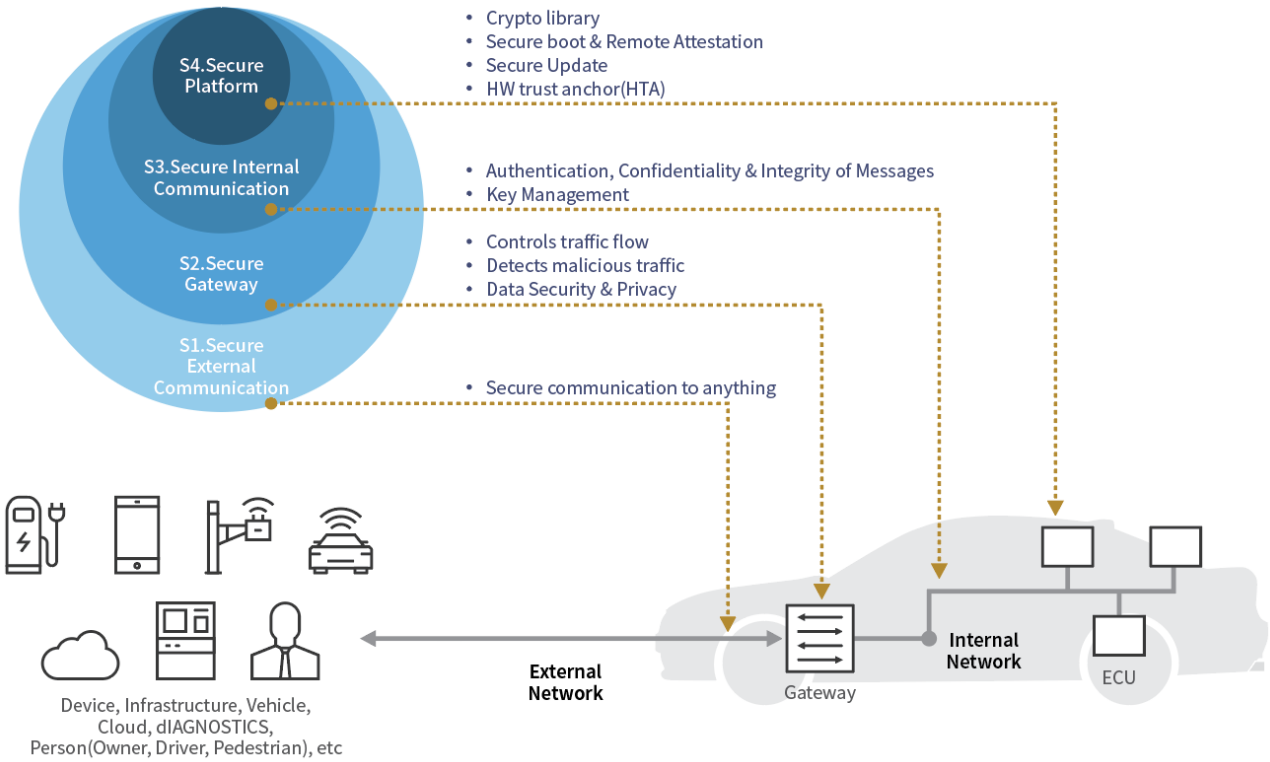
電化の分野でも電気自動車が充電器を介した決済会社を含む様々な二次アクターとの連結に、必ずセキュリティが必要

になる。連結性にて定義するV2G通信モデルがこれに当たる。

オンラインサービス・フラットフォームではサービスが中心に位置され、自動車、モノのインターネット、モバイル端末、そして様々な主体がサービスに連結されるプラットフォーム化でも、個体間の認証や暗号化などの基本的なセキュリティツールは、必須要素になる。

自律走行自動車の場合は、外部通信が自動車の運行に直接影響を及ぼすため、安全問題に直結する。

これは、外部から流入されるデータに対しては認証と暗号化が必ず必要という意味である。外部通信が使用されなくてもセキュリティは必要である。車内の認可されていないまたは誤作動を起こす制御機器の部品は、車両の正常動作を阻害する要因になる。車両の内部ネットワークに、マルウェアなど悪意のあるパケットの差し込みを試す外部通信攻撃に対しても、車両内部ネットワークの強健性維持は、最も重量な課題である。車両環境に最適化されたファイアウォールや侵入検知技術などがこれに当たる。



自動車に適用されるセキュリティ技術は、大きく4つに分けられる。

1つ目は、車両と車両外部の個体間の安全な通信確立のためのセキュリティ技術である。連結性確保のために必要なセキュリティがここに当たる。

2つ目は、車両のゲートウェイから車両に流入されるトラフィックに対し、有害性を検査する侵入検知、通信経路をコントロールするファイアウォール、車両内部のデータを外部に転送し、公有するためのデータ保護と個人情報保護の技術である。これらの技術は、車両の外部ネットワークと内部ネットワークの境界で車両の戦い場を保護する。

3つ目は、車両の内部ネットワークの通信に対するセキュリティ技術である。車両の内部には、100個を超える電子制御装置(ECU：Electronic Control Unit)が存在し、これらがお互いに連結されてプライベートネットワークが構成されると理解すれば良い。車両の内部ネットワークにおいて電子制御装置間の安全な通信確立に必要な認証や暗号化のようなセキュリティ技術がここに当たる。

4つ目は、それぞれの電子制御装置を安全に守るセキュリティ技術である。完全に起動されたかとうかが確認できるセキュアブート(Secure Boot)、第三者が電子制御装置の完全性を検証できるリモート検証(Remote Attestation)、電子制御装置のファームウェアやソフトウェアの更新のためのセキュア更新(Secure Update)などがここに当たる。これらの技術が電子制御装置内でより安全に適用されるようにするには、ハッキングや改ざんから安全だとみられるハードウェアトラストアンカー(HTA；Hardware Trust Anchor)を採用すれば良い。

自動車の外部通信のうち、V2V、 V2I、V2G などの通信モデルに適用されるセキュリティ技術は、既に標準化が進められている。しかし、それ以外の技術に対しては、標準が存在していない。自動車メーカー、部品サプライヤー、セキュリティソリューションベンダーなどが協力して安全な自動車を設計し、開発いていくしかない。

今まで自動車分野における 5 つの変化について探ってみた。これらの変化に対する理解を深めるためには、私たちが普段使っているスマートフォンを改めて注意深くみてほしい。自動車の将来はスマートカーであり、スマートカーは私たちが持つもう一つのスマート機器になるためである。

スマートカーへの進化には、相当な時間が必要になり、その過程の中で命の安全を保障しながら利便性と有用性を共に得るためには、自動車関連企業だけではなく、政府機関から一般利用者に至るまで多くの人の協力と努力が必要である。