サイバーセキュリティが定義する自動車の将来

著者：赤路 陽太

法規制により照らされる道

ここ数年、IoTやAIなどのエマージングテクノロジーに導かれ、自動車産業およびその周辺産業においては、コネクテッドサービス、自動運転、モビリティサービス、EVなどに関する議論が数多く行われてきた。

自動車メーカーにおいてはもちろんのこと、自動車部品メーカーや周辺産業のプレイヤーにおいても多くのプロジェクトが立ち上がり、巨額の予算と工数が費やされてきた。

世界中の企業においてスマートデバイス経由で利用するモビリティサービスが検討され、シェアリングサービスやロボットタクシーが新車販売台数とタクシードライバーの雇用を奪うというシナリオが描かれている。

PoC（Proof of Concept）と呼ばれる実証実験も多数行われ、その結果報告書が山のように積み上げられている。

市場はまだ立ち上がってもいないにもかかわらず既にレッドオーシャンの様相を呈しており、なかなか見えない「宝探し」に企画・開発担当者が焦り、疲弊し始めている状況もある。

いつの時代においてもエマージングテクノロジーは企業に不安と期待を与え、混乱と進化をもたらしてきた。

自動車産業は今まさにその状況にある。

しかし最近、そうした状況に変化が起こりつつある。変化をもたらしているのは自動運転などに関する国際機関や国による法やガイドラインの整備の進展である。

国際機関や国が定める法やガイドラインは、企画・開発担当者たちの道を照らす明かりとなり、「どこに行けば良いか」「どこまで行けば良いか」「何は許されて何は許されないのか」などの指針を与え始めている。

その結果、これまでのコンセプチュアルな議論に道しるべが立ち、より現実的で具体的な議論が始まりつつある。

サイバーセキュリティも、そうした明かりが灯されたテーマの一つである。そしてその明かりは、今後の自動車の在り方を示唆するものとなっている。

データより大切なもの

海外におけるセキュリティイベントなどで実車へのハッキングが可能と証明されたことは記憶に新しい。大規模リコールに発展した事例もある。だが、自動車産業各社はそれらがきっかけで動き出したわけではない。各社はかなり以前からサイバーセキュリティの必要性を認識しており、その取り組みは既に長期にわたっている。自動車メーカー複数社が参画するサイバーセキュリティプロジェクトの発足や、自動車部品メーカーによるサイバーセキュリティソリューションベンダー買収などが示すように、各社は少なくとも2000年代から取り組みを開始し、国際基準・国際標準がない中で仕様を模索し続けてきた。

そうした長期にわたる研究・開発の結果、自動車のサイバーセキュリティについては、開発段階から生産・販売・使用・再販・廃棄に至るまで、そしてコンセプトからオフィス、工場、生産ライン、ディーラー、クラウド、通信、車両、通信ユニット、車載ネットワーク、ECU、ソフトウェアに至るまでをさまざまなソリューションで包括的かつ多層的に防御する必要があると認識されている。

Strategy&ではこれを「Holistic Multilayer Security」と呼称し、図表1に簡略イメージを提示する。

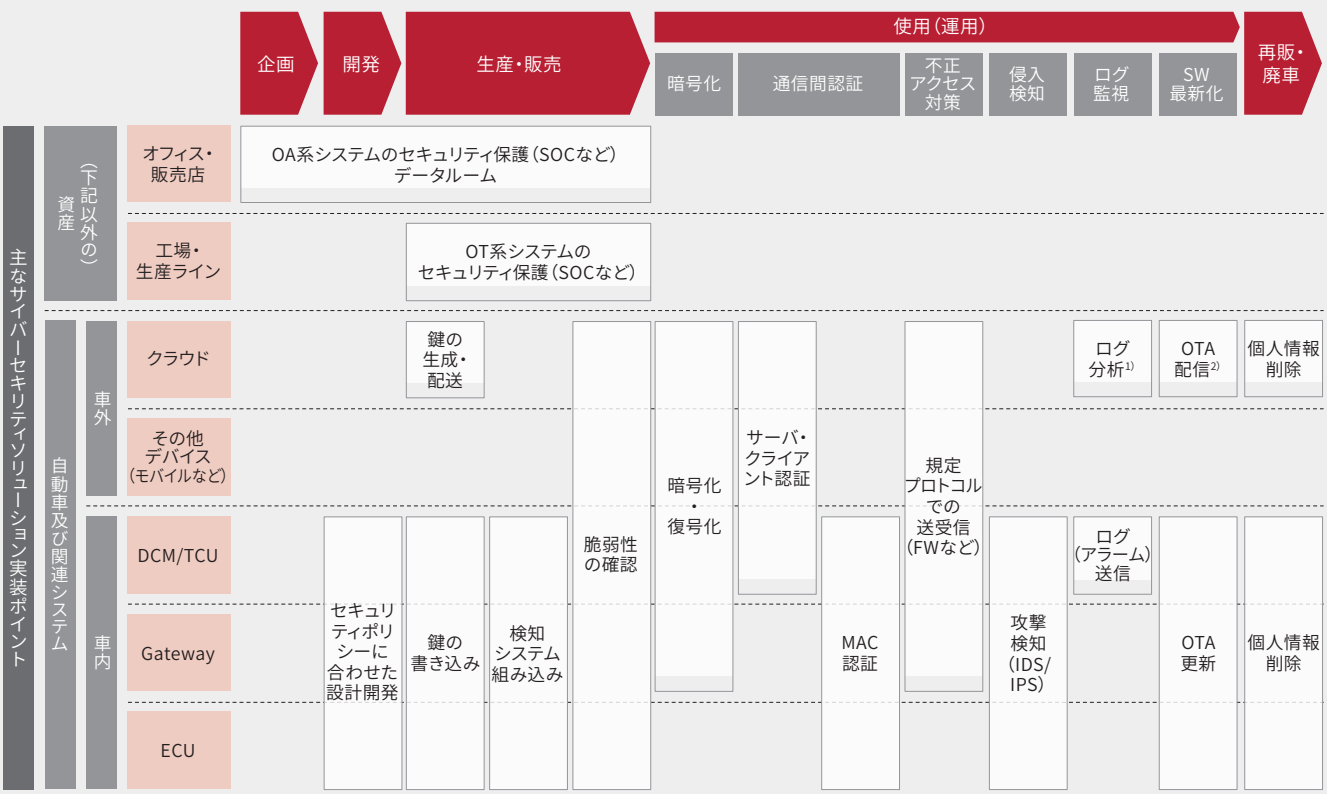
これほど多岐にわたるソリューションが必要と認識されるのは、自動車におけるサイバーセキュリティリスクが、「車両盗難」「個人情報漏洩」「技術情報漏洩」「漏洩情報悪用による二次被害」「それらがもたらす風評被害や損害賠償などの経営リ

赤路 陽太（あかじ・ようた）
yota.akaji@pwc.com

PwCコンサルティング、Strategy&のシニアマネージャー。自動車産業および情報サービス産業を中心に、イノベーション、新事業開発、成長戦略、事業変革、マーケティングなどのテーマについて豊富なコンサルティング実績を有し、次世代のモビリティに関するコンサルティングを多く手掛けている。

なお、本稿の執筆にあたっては、Strategy&のシニアアソシエイトの米本 和希、アソシエイトの長山 東哲の協力を得た。

図表1
Holistic Multilayer Security（簡略イメージ）



1）ログ分析はクラウド（SOC）上で監視しているホワイトハッカーにより実施される
2）OTA配信は、通常更新の他、SOC上での分析結果や脆弱性情報収集の結果行われる

出所：Strategy&分析

スク」はもちろんのこと、「自動車を踏み台にした企業サーバー攻撃」、そして「事故による人命毀損」「周囲の巻き込みによる甚大被害」にまで及びうるからである。

一昔前に「クルマのスマホ化」という言葉が多用された時期があったが、サイバーセキュリティの観点では、残念ながら自動車とスマートフォンが置かれている状況は大いに異なる。

スマートフォンの場合、ハッキングされたアプリケーションが使用者本人や他人に被害をもたらすことはあっても、スマートフォン自体が使用者本人や他人の生命を奪うことはほぼない（バッテリーを熱暴走させるなどはあるかもしれないが）。

一方、自動車の場合、特に制御系のECUがハッキングされると、使用者本人に加え、歩行者ら、他人の生命まで奪ってしまうリスクがある。さらにそれが保険会社も対応しきれない規模の損害になるリスクがある。そのため万が一のリスクも発生しないよう、徹底的なソリューションが必要と考えられている。

ガイドラインが示唆する未来

ところが、これほどまでに時間をかけて検討されてきたにもかかわらず、これまでのところこれらの内容はあくまでも自動車産業各社の研究の域を脱していなかった。

準拠すべきルールが存在していなかったため、結局どこまで実装しなくてはならないのか個社では判断がつかず、研究のみが延々と続けられる状況に陥っていたのである。

しかし、ここ1～2年で国際機関や国によるガイドラインなどの整備が進展し、状況が変わり始めている。

レギュレーションの整備にはもうしばらく時間を要する見込みであるが、これまで先行するICT産業の規格などを参考にしながら個別に検討を進めてきた自動車産業各社にとっては十分なよりどころが整備されつつあり、いよいよ実装に向けての判断が可能な状況が整い始めている。

同時にこれらのガイドラインなどは「今後の自動車の姿」も示している。

図表2にそうしたガイドラインなどから主なものを抜粋して例示する。これらのガイドラインなどにおけるポイントは以下の2点である。

①通信が絡む自動運転技術を搭載する車両は、徹底的なサイバーセキュリティソリューションの実装が必須になる

②サイバー攻撃は防ぎきれないことが前提となる

ポイント①は、言うまでもないことであるが、これまで曖昧で個社に対応が委ねられていたものがルール化されることにより、「必要なサイバーセキュリティソリューションを実装していなければ通信が絡む自動運転技術搭載車両を販売できない」「サイバーセキュリティソリューションの実装によるコストアップに対する解決策を見いださなくてはならない」という新たな課題が自動車メーカーにもたらされることを意味している。

前述のHolistic Multilayer Securityを実装するためには、多額のシステム開発費、ソフトウェア開発費、部品費、組み込み加工費、運用費などが必要になる。これらは従来なかった新規のコストになるため、自動車メーカーとしては回収方法を考える必要がある。単純に車両販価に上乗せしたり所有者にサブスクリプション型で請求したりすると、所有者は当然のことながら嫌がるだろう。「自動運転なんてなくて良いから安くしてほしい」と言う消費者も現れることが想定される。無理に強制しようものなら、買い替えを見送る所有者や、そもそも所有を諦める消費者が現れ、新車販売台数を押し下げるリスクが想定される。

ポイント②は、WP.29/2017/46 Guideline on cybersecurity and data protectionにおける「サイバー攻撃による不正な操作を自動運転システムが検知した時は、ドライバーに警告の上、自動車を安全にコントロールすること」という要件や、Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVAにおける「自動車での攻撃が検知された際は、システムは適切にインシデントレスポンスが行われるように設計すべき」という要件がそれに相当する。

これらの要件の存在は、「工場出荷時に実装された暗号化や相互認証などのサイバーセキュリティソリューションでは防ぎきれないサイバー攻撃の存在」を示唆している。

パソコンやスマートフォンにおいてセキュリティソフトの更新が必要であるように、自動車においてもサイバー攻撃は日々進化している。それらのサイバー攻撃はいつしか工場出荷時に実装されたサイバーセキュリティソリューションでは防げないレベルに進化し、車載ネットワークに侵入し、ドライバーの意志とは異なる挙動を引き起こすことで重大事故を生むリスクがある。

さらに最近はハッキングAIも台頭し始めており、多層防御の脆弱性を機械学習により自動的に見いだし、脆弱性が解消される前にゼロデイ攻撃を仕掛けてくるリスクがある。

そのようなリスクを回避するためには、まずもって自動車のセキュリティソフトを常に最新版にアップデートし続ける必要があり、方法としてはOTA（無線通信）によるセキュリティソフト

図表2
主なガイドラインなどの例

ガイドラインなど	概要（一部抜粋）
WP.29/2017/46 Guideline on cybersecurity and data protection (UN)	❖ **コネクテッド車両および自動運転車両は以下の要件を満たすこと** ★ コネクテッド車両または自動運転技術（ADT）装備車両が適用範囲。コネクテッド車両とは、外部の装置、車、ネットワークまたはサービスとの間で自動運転テクノロジーに関係する可能性がある無線接続または通信を行えるように設計された装置が搭載されている車両を指す ★ 一般要件 • 自動車製造者らは、コネクテッド車両および自動運転車両において、データの操作、誤用などに対して適切な保護を確実にすること • 自動車製造者らは、コネクテッド車両および自動運転車両において、世界標準の通信技術などによるデータおよび通信の暗号化を実施すること ★ データ保護にかかる要件 • コネクテッド車両および自動運転車両におけるデータの収集および処理を行う際は、以下を満たすこと - データ主体（例、運転手）に、どのようなデータが収集・処理されているのかなど、包括的な情報を提供すること - これらの説明を受けたデータ主体による、データの収集および処理に対する同意を得ること • 個人情報については、自動運転に関わる情報の収集および処理に関連するものに限定し、場合によって情報主体は同意を取り下げる権利を持つ ★ 安全性にかかる要件 • コネクテッド車両および自動運転車両は、接続および通信の安全確保のため、以下を満たすこと - 車外のネットワークから車内の制御系ネットワークが影響を受けないこと - 無線インターフェイス、故障診断ポートを介した不正アクセスを回避するよう設計されていること - システムの機能不全時の「セーフモード」を備えること • サイバー攻撃による不正な操作を自動運転システムが検知した時は、ドライバーに警告の上、自動車を安全にコントロールすること ★ セキュリティにかかる要件 • コネクテッド車両および自動運転車両は以下のものが装備されていること - 完全性保護措置（例として、セキュアなソフトウェアアップデート） - 暗号鍵を管理するための適切な措置 • コネクテッド車両および自動運転車両へのリモートアクセスに関わるオンラインサービスについては、強力な相互認証を有すること
Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA （UN、次ページに続く）	❖ **車両へのサイバー攻撃に対するリスクを軽減するために、考慮されるべきサイバーセキュリティ対策を示す。必須事項は「しなければならない（Shall）」、推奨事項は「すべき（Should）」とした** 1. インサイダー攻撃（内部者による攻撃）のリスクを最小限にするため、セキュリティコントロールをバックエンドシステムにも適用しなければならない 2. 不正アクセスを最小限にするため、セキュリティコントロールをバックエンドシステムにも適用しなければならない 3. バックエンドサーバーがサービスの提供に不可欠な場合、システム停止に備えて回復措置を設けなければならない 4. クラウドコンピューティングに関連するリスクを最小限に抑えるため、セキュリティコントロールを適用しなければならない 5. 情報漏洩を防止するため、セキュリティコントロールをバックエンドシステムにも適用しなければならない 6. 車両への攻撃の影響を最小限に抑えるため、設計によるセキュリティ（Security by Design）の原則を採用しなければならない 7. システムデータ/コードを保護するため、アクセス制御技術および設計を適用しなければならない 8. 不正な担当者が重要なデータにアクセス可能なシステム設計およびアクセス制御にすべきではない 9. 不正アクセスを防止し、検出するための措置が採用されなければならない 10. 車両は、受信したメッセージの信頼性と整合性を検証しなければならない 11. 暗号鍵を格納するためのセキュリティコントロールが実装されなければならない

ガイドラインなど	概要（一部抜粋）
Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA (UN)	12. 自動車に対し機密データが送受信される場合は保護しなければならない 13. DoS攻撃に対する検知・回復するための措置を検討すべき 14. 組み込まれたウイルス・マルウェアからシステムを保護するための措置を検討すべき 15. 悪意のある内部メッセージまたは活動を検知するための措置を検討すべき 16. セキュアなソフトウェアアップデート手順を採用しなければならない 17. 保守手順を統制するための手段を講じなければならない 18. ユーザーロールとアクセス権限は、必要最小限な形で統制するための手段を講じなければならない 19. セキュリティ手順が実行されるような組織を定義し、維持しなければならない 20. リモートアクセスを持つシステムに対し、セキュリティコントロールを適用しなければならない 21. ソフトウェアはセキュリティ観点で評価・認証され、完全性を保護しなければならない 22. セキュリティコントロールは、外部インターフェイスに対しても適用しなければならない 23. ソフトウェアとハードウェア開発におけるサイバーセキュリティのベストプラクティスを守らなければならない 24. 個人情報・機密情報を格納する際はデータ保護のベストプラクティスを守らなければならない 25. 自動車での攻撃が検知された際は、システムは適切にインシデントレスポンスが行われるように設計すべき
自動運転車の安全技術ガイドライン（国土交通省）	❖ サイバーセキュリティの要件 ★ 自動車製作者などまたは自動運転車を用いた移動サービスのシステム提供者は、サイバーセキュリティに関する国連（WP29）などの最新の要件を踏まえ、自動運転車のハッキング対策などのサイバーセキュリティを考慮した車両の設計・開発を行うこと ★ 2017年3月にWP29で成立したサイバーセキュリティガイドラインなどで示されている要件（抜粋） • 自動運転車の接続および通信の安全確保 - 車外のネットワークから車内の制御系ネットワークが影響を受けないこと - システムの機能不全時の「セーフモード」を備えること • 不正操作を検知した時は、運転者に警告の上、車両を安全にコントロールすること ❖ 自動運転システムの安全性要件 ★ レベル3の自動運転車については、次の要件を満たす自動運転システムであること • 設定されたODD（運行設計領域）の範囲外となった場合や自動運転車に障害が発生した場合など、自動運転の継続が困難であるとシステムが判断した場合において、運転者に対し介入のための警告（運転権限の委譲）を行うこと • 運転者に運転権限が委譲されるまでの間、システムの機能を維持またはシステムの機能を制限した状態でシステムの稼働を継続させるフォールバック（縮退運転）を行うことにより、安全に自動運転を継続すること • システムから運転者に運転が引き継がれたか否かを判別することができること • システムから運転者に運転が引き継がれない場合において、車両を自動で安全に停止させるミニマル・リスク・マヌーバー（MRM）を設定すること - 車両を路肩などの安全な場所に自動で移動して停止させることが望ましい - 自動運転車の MRM の設定は、周囲への警報を行いつつ、車線を維持、または車線を変更しながら自動で安全に停止させる措置が想定されるが、今後の技術開発の動向および国際的な基準の検討状況を踏まえ具体的要件を検討する

出所：Strategy&分析

のアップデートが考えられる。しかしOTAの実行は基本的に所有者の許可が必要になるため、所有者が許可しなければ永遠に古いセキュリティソフトのままになってしまう。

そのため自動車メーカーは車載ネットワーク上のイベントを常時監視し、それらを分析することによってインシデントと考えられる兆候を検知し、阻止する必要もある。また、車載検知システムでは検知しきれない新たな攻撃を特定すべく、車載ネットワークのログを車外のSOC（Security Operation Center）に送信し、SOCが保有するSIEM（Security Information and Event Management）と呼ばれるログの集約・蓄積・管理・分析を行う仕組みによる相関分析およびセキュリティ専門家による詳細分析にかけることでインシデントを特定し、阻止する必要もある。しかし車載検知ソフトウェアは100%正確に検知を行うことができない。検知精度を高くし過ぎると問題の無いイベントまでインシデントと誤検知してしまい運転に支障が出てしまうため、検知精度に幅を持たせてあるからだ。そうした状況でもインシデントの見逃しがないようにSOCでのバックアップがあるわけだが、残念ながらSOCでの相関分析およびセキュリティ専門家による詳細分析には時間を要するという問題がある。サイバー攻撃の方が早かった場合、このソリューションは効果を発揮することができない。

つまり、「防ぎきれないサイバー攻撃が存在しうる」ということである。

「セキュリティソフトのアップデートをしないのは所有者の責任ではないか」という意見もあるだろうが、そこの責任分担はこれから議論されるところであろう。少なくとも現時点においては自動車メーカーが安全な自動車をつくることが求められているし、そもそもハッキングAIにとってはセキュリティソフトのバージョンは関係ない可能性もある。

こうした状況が想定されてか、ガイドラインなどにおいては、通信が絡む自動運転技術搭載車両について「サイバー攻撃による不正な操作を自動運転システムが検知した時は、ドライバーに警告の上、自動車を安全にコントロールすること」と要件が定義されている。

もしサイバーセキュリティ技術の進化や徹底的な機能・装置追加により上述のソリューションが有効になったとしても、実装するためには相当な仕組みとコストが必要になる。

まず、検知する仕組みを車両に組み込まなければならない。これは従来なかった仕組みのため、検知ソフトウェアやデバイスの開発費、それらの組み込み加工費などが必要になる。

検知したログをSOCに送信するための通信費も必要になる。車両の自動化が進み高度ADAS（先進運転支援システム）や自動運転が搭載されると、車載ネットワークを流れるデータ量は膨大になる。某半導体企業は1台の車両で1日あたり数テラのデータが生成されると予測しているが、それらに基づくログをSOCに送信するとなると、かなりの通信費が必要になるであろう。

通信費を抑制するためにログの送信頻度や送信量を抑制するというアイデアもあるが、そうするとリアルタイムでのインシデント特定ができなくなってしまうため、本末転倒になってしまう（通信量についてはそもそも自動運転技術やストリーミング配信などの方が大きくなるからサイバーセキュリティだけ抑制しても意味がないという意見もあるであろうが、それはいったん置いておこう）。

ログ送信先のSOCも従来なかった仕組みのため、新たなコストが発生する。SIEMの開発費や、セキュリティ専門家の人件費などを含む運用費が必要になる。

インシデントを特定した場合は、所有者に通知するとともにセキュリティパッチを生成し、配信する必要がある。これにも費用が発生する。

ただしこれでも完璧ではなく、セキュリティパッチの生成に時間を要することを想定すると、攻撃を検知した瞬間に車外および車内の通信を遮断し、なんらかのバックアップシステムにより強制的に安全に路肩に停車させるなどの機能安全の仕組みも搭載している必要がある。

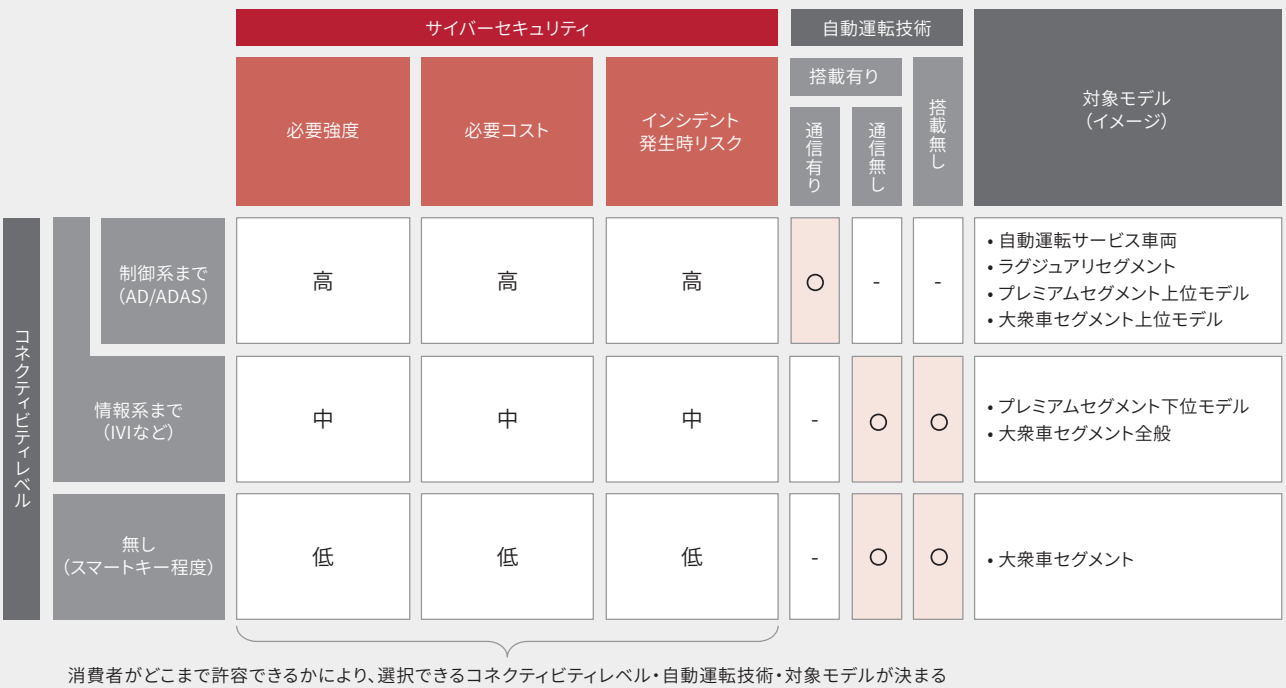
そして最終的にはこれらを自社の車両が走行する世界中の国で対応可能にする必要がある。

1台あたりに換算すると、通信費・運用費・部材費がかさみ、前述のHolistic Multilayer Securityの実装費用も含め、かなりのコストアップになることが容易に想定される。

提示されているガイドラインは、そうした未来の到来を示唆している。

図表3

サイバーセキュリティにより規定されるコネクティビティレベル・自動運転技術搭載動向・対象モデルイメージ



出所：Strategy&分析

サイバーセキュリティにより規定される車両

こうした状況を踏まえると、「これ以上、車にお金を払えない」「せっかく高いお金を払ってもリスクがあるなら、通信が絡む自動運転技術は要らない」という消費者が現れてもおかしくないだろう。

もし「セキュリティソフトのアップデート忘れによるハッキングに起因する事故は所有者責任」ということになれば、そういう消費者がますます増える可能性もある。

つまり、サイバーセキュリティが消費者の費用対効果判断の軸となり、許容できる「サイバーセキュリティコスト」や「インシデント発生時のリスク」により、選択できるコネクティビティレベルおよび自動運転技術が決まる（コスト要因により対象モデルも決まる）ようになる可能性がある。

その結果、昨今のCASE（Connected, Autonomous, Shared, Electric）ブームにより世の中の全車両がすべからく完全自動運転になるかのような見方がある中で、実際はサイバーセキュリティ起点で複数の車両バリエーションが求められる可能性が想定される。

自動車産業各社および関連産業各社は、こうしたバリエーション展開の可能性を認識し、準備を進めておく必要があるだろう。

おわりに

自動車のサイバーセキュリティもエマージングテクノロジーの一つである。よって今後も進化する可能性があり、現時点で全てを結論づけるのは難しい。もしかするとHolistic Multilayer Securityをより多層化することでハッキングを完全に防御できる状態を作り出せるかもしれないし、ゼロデイ攻撃に対するソリューションが開発されるかもしれない。

一方、「万が一のリスクがありえる」状態で販売する自動車メーカーが出てくる可能性がないとも言い切れない。しかしながら自動車は人の命がかかわる製品であることを忘れてはならず、サイバーセキュリティの特性、想定されるリスク、自動車産業が社会で果たさなくてはならない責任、消費者の安全・安心・予算などを総合的に考えれば、安易に予想された未来の実現難度がいかに高いか、遅かれ早かれ気付くであろう。

通信が絡む自動運転技術の開発が進む今、サイバーセキュリティがキーテクノロジーの一つになり、自動車開発において重要な役割を担っていくのは間違いない。

今後サイバーセキュリティは、パワートレイン構成を左右する燃費・排ガス規制のような位置づけになる可能性がある。

よって自動車産業各社および関連産業各社は早急に「サイバーセキュリティが定義する自動車の将来」を勘案し、開発予算・工数の適切な差配と競争力のある商品・サービスポートフォリオを実現していくべきであり、それが「全ての人の自由な移動」を実現することにもつながっていくであろう。