www.pwc.com/jp

今こそアクセルを踏み込むとき –
自動車サイバーセキュリティへの
道のりを駆けていくために

PwC『2022年グローバル自動車サイバーセキュリティ
マネジメントシステム（CSMS）調査』

pwc

日本語版発行にあたって

自動車基準調和世界フォーラム（WP29）で成立した国連規則155号について、ソフトウェアアップデート機能を有する新型車に対する適用が、2022年7月より開始されました。対象車両を販売するOEMでは、同法規が求めるサイバーセキュリティマネジメントシステム（CSMS）構築が必須となっており、多くのOEMにてCSMS構築の準備が進められてきました。

PwCコンサルティング合同会社では、2021年8月に上記CSMS構築の準備状況を明らかにする目的で、「WP29 サイバーセキュリティ法規―CSMS対応の実態調査」を公開しました。この実態調査では、2021年時点の日本国内のOEMとサプライヤーにおけるCSMSの準備状況および計画の状況を調査しており、2021年の時点で主要なOEMにおいて、法規適用に先立ってCSMS構築が着手されていることなどを明らかにしていました。また、OEMに比してサプライヤーの着手が遅れている傾向にあることや、自動車業界全体の課題や今後必要となる取り組みなども明らかにしてきました。

上記2021年の実態調査から時がたち、国連規則155号の一部適用開始をうけ、最新のCSMS構築の状況を明らかにすることを目的に、本レポートでは、日本にとどまらず、海外を含めたOEM・サプライヤーにおけるCSMS構築の状況をヒアリング調査し、世界の自動車業界が置かれているサイバーセキュリティ環境を分析しました。海外展開も踏まえたCSMS施策を計画、推進する国内企業の皆様にとって、本レポートが、国内外を含む最新の車両サイバーセキュリティの状況を理解するための一助となれば幸いです。

目次

エグゼクティブサマリー

100%

の回答者が、自動車や自動車エコシステム全体に対するサイバー攻撃は激増すると予想。

91%

の回答者が、OEMとサプライヤーのセキュリティ体制について一層の連携強化が必要、と回答。

89%

のOEMが、今後の自動車販売においてサイバーセキュリティの成熟度向上が明確な競争上の優位性となることに同意。

PwC『2022年グローバル自動車サイバーセキュリティマネジメントシステム（CSMS）調査』にようこそ。本レポートでは、自動車部門における主なトレンドの詳細、最新のベンチマーク、脅威、このトピックに関する技術的ソリューションを紹介する。

2022年3月から4月にかけて、PwCは自動車業界の代表者に広くインタビューを行った。これには、市場専門家に加え、完成車メーカー（Original Equipment Manufacturer、以下OEM）やサプライヤーの代表者も含まれる。回答者の拠点は11カ国に及び、その担当部門も製品セキュリティから研究開発・品質管理、情報セキュリティ、生産・ITまで多岐にわたる。また、全員が積極的に車両サイバーセキュリティマネジメントに携わっている。回答者から、業界への規制や期待事項によって、自動車部門におけるサイバーセキュリティリスク対策の構築がどの程度進んでいるか、実務に基づく知見を提供いただいた。また、過去の歩みから現在の課題、そして将来への思いなども語っていただいた。

技術の進化やコネクテッドカー・自動運転の普及は、これまでにない方法で人や車両、企業に脆弱性をもたらしている。こういったセキュリティ上の懸念を取り払うために、新たな規則も設けられた。

しかし、地域によってそうした規則の内容は異なり、サイバー脅威対策を具体的にどう実施すればよいのか詳細がわからない場合が多い。したがって、より広範囲をカバーするガイドラインおよびそのガイドラインの上位枠組みとしての包括的ビジネス戦略が不可欠である。他社に先んじて、うまく適応できた企業は、大きな優位性を得られるだろう。

今回の調査結果から、自動車バリューチェーンにおける各ステージの企業がCSMS導入に向けた活動を開始していることが判明した。しかし、その多くは設計段階であり成熟度は低い。また、これらの活動は時間面や資金面で企業の大きな負担となっている。この業界では、プレイヤー間の情報共有が欠けており、アプローチもそれぞれ異なる。

今回の調査では、コネクテッドカーと自動運転技術により、新規プレイヤーが市場に参入するとともに、既存プレイヤーは迅速な対応を迫られ、市場シェアにも大幅な変化が生じる、という点で大方の意見が一致した。また、自動車エコシステムがサイバーリスクの脅威に晒されていることも浮き彫りになった。CSMSは、対象範囲や複雑性、関係組織という点で拡大を続ける車両エコシステムを保護するものであり、以下の3つの視点から、ビジネスの命運を左右する要素となっている。

第一に、CSMSが守るのは人々の命だけではない。新たな生活・仕事の場となりつつある自動車を中心に拡大するデータ主導・サービス主導型ビジネスモデルや、今後の大きな収益基盤も守るのである。

第二に、継続的なサイバーセキュリティ運用は、車両コストに大きな影響をもたらす。今後、ライフサイクル全体にわたり自動車エコシステムをいかにコスト効率良く運用できるか、そのカギとなるのは、モジュール型のスケーラブルなソフトウェアアーキテクチャを組み合わせたスマートCSMSである。

第三に、CSMSは世界の多くの市場で登録・生産される自動車の基本的要件であり、今後もそれは変わらない。コンプライアンス要件違反は、車両生産ライセンスの取り消しや、罰金、大規模な法的紛争につながる可能性がある。

ただし、これら全てを踏まえたうえで、CSMSはデジタルトランスフォーメーション（DX）の成功に向けた道のりの一里塚に過ぎない。OEMとサプライヤーは、消費者からの信頼を重視しつつ、自社のサイバープログラムをより相互連携性の高いものへと進化させていく必要があるだろう。

経営陣にとっての最優先事項は、サイバーセキュリティをビジネスの中核に据えてサイバーリスクマネジメントを企業リスクマネジメントに統合する企業文化を実現することである。

規制要件を総合的に考え、純粋なビジネスモチベーションと組み合わせた企業だけが、DXを巡る競争に勝利できる。

コースはすでに目の前に広がっている。この市場で成功を収めようとする企業は、自動車の変革ペースに後れをとってはならない。

大局的に見れば、セキュアかつ効率的な自動車エコシステムの実現は長く曲がりくねった道のりである。ゴールにたどり着くためには、チームワーク、スピード、そしてナビゲーションスキルが必要となるだろう。

このPwC『2022年グローバル自動車サイバーセキュリティマネジメントシステム（CSMS）調査』では、自動車業界の企業がサイバーセキュリティ分野をどのように捉えているか、そしてどのように対応しているかを詳しく調査した。今、それぞれの企業が何を行っているのか、将来に向けてどのように備えているのか、ぜひご一読いただきたい。

A はじめに

自動車業界は急速な進化を遂げている。コネクテッドカーはすでに消費者の間で受け入れられているが、関連技術の発展とともに、新たな要求も生じている。また、コネクテッドカーに関する規制も見られ始めているが、そのペースは地域、市場、国によって異なる。こうした移行によって、全く新たな指針が生まれ、自動車部門の再構築につながっている。

OEMやサプライヤーは、こうした未曾有の混乱に直面しつつ、モビリティの未来に向けて新たな、巨大な機会を掴もうとしている。成功を収めるためには、製品開発、サプライチェーン・バリューチェーンマネジメント、車両ライフサイクル全体にわたる保守・整備方法など、既存のモデルを迅速かつ広範囲に変えていく必要がある。企業はまた、生産プロセスやデジタル技術、人材の変革に向けた一歩を踏み出す必要もあるだろう。このように、車両エコシステムは拡大の一途にあり、新たな機会を創出すると同時に、複雑さやリスクに晒されるケースも増加している。

人、車両、企業は、これまでにないかたちで脆弱化している。すでに、ハッカーによる自動車のドアロック、ブレーキ、アクセルなどの遠隔操作事例も発生している。自動車へのDoS（サービス拒否）攻撃事例もあり、車間距離制御システム（車間距離が危険なレベルに達すると自動ブレーキがかかる装置）をはじめとする主要部品や機能が狙われている。

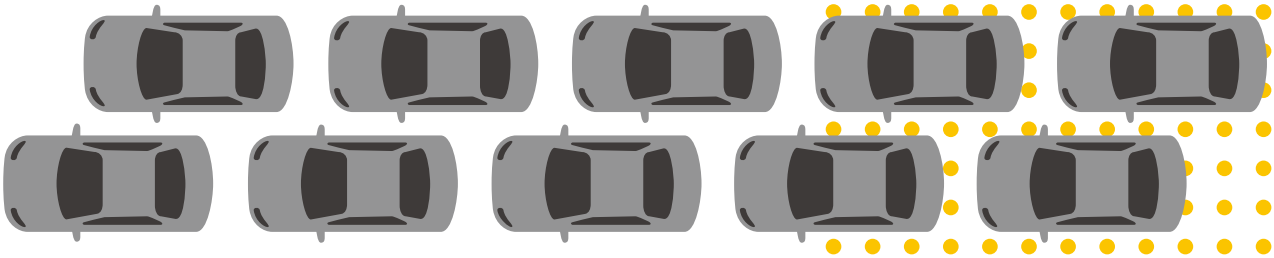
しかし、仮にサイバー犯罪者がある都市の警察車両の制御を奪い、警官が対応できない間に罪を犯す、といった事件が発生したらどうなるだろうか。あるいは、居眠り防止装置用の車載カメラがハッキングされ、ドライバーの月曜朝の憂鬱顔がネットに投稿されたとしたら。あるいは、自動車線維持補助装置の欠陥アップデートが、何千台もの車両にインストールされてしまったとしたら。

新たな規則は、このようなセキュリティ上の懸念を払拭することを目的としている。一部の市場では、自動車のサイバーセキュリティマネジメントシステムに焦点を当てた規則がすでに存在しているが、対象範囲、詳細度、施行時期はそれぞれ異なる。国連欧州経済委員会（UNECE）はこのほど、「サイバーセキュリティシステムに係る協定規則（第155号）」（CSMS：サイバーセキュリティマネジメントシステム）を導入するとともに、56カ国で拘束力を有する予定の「プログラム等改変システムに係る協定規則（第156号）」（SUMS：ソフトウェアアップデートマネジメントシステム）を発表した。

多くの生産者は、道路車両のサイバーセキュリティをカバーする国際標準規格ISO/SAE21434（道路車両：サイバーセキュリティエンジニアリング）要件を採用している。その他、ISO/DIS 24089（道路車両：ソフトウェアアップデートエンジニアリング）のような規格も策定中である。

しかし、多くの市場において、法制化は草案段階にさえ達していない。同様に、多くのOEMやサプライヤーは、CSMS技術や関連法規制の順守という点で、他の市場プレイヤーと比べて自分たちがどのような位置にいるのか認識していない。

規則の主な対象はOEMである。しかし、ソフトウェアやサービス、車両部品などのパートナーやサプライヤーとの契約義務上、OEMに対するこれらの法的要件はバリューチェーンやサプライチェーンにまで適用される。こうした関係は、グローバル規模のバリューチェーンに属する各ステークホルダーが異なる地域や市場特有の状況に左右されることもあり、さらなる一貫性の欠如を招く可能性がある。



こうした不透明性はあるものの、明々白々なポイントがひとつある―コネクテッドカーと自動運転にはセキュリティと安全性が必須、という点である。よって、市場プレイヤーはそれぞれの自動車エコシステム内でサイバーセキュリティへの投資を進めている。各国政府は今後も規則の導入・強化を図り、それに伴い、企業はCSMS要件の詳細化を進めていくだろう。

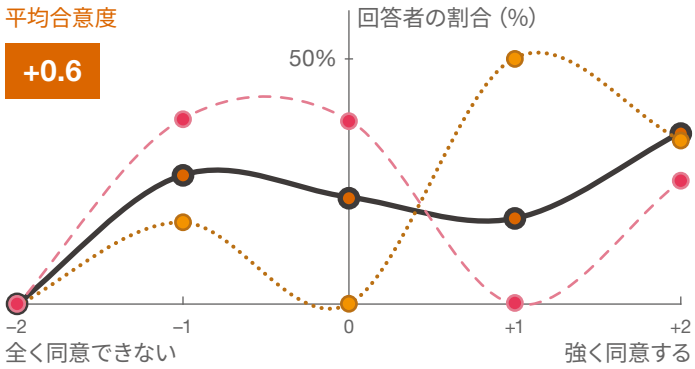
自動車エコシステムのあらゆる部分に、また自動車ライフサイクルのあらゆるステージに脅威が存在するようになる。この業界の企業は、技術的・組織的対策を講じる必要があるだろう。それは、顧客の命や自社の評判を守るためだけではない。自らの車両エコシステムを守ることで、新たな商機の創出にもつながるのである。

自動車CSMSに関する意見

詳細なインタビューを通じて、CSMSに関連する主要なトピックやトレンドについて回答者に意見を求めた。各ステートメントについて、-2（全く同意できない）～+2（強く同意する）の尺度で評価していただいた。そして、全体的な回答を示す図表を作成した。黒い太線は全体の平均、色付きの線はサプライヤー、OEM、市場専門家の各平均を示す。

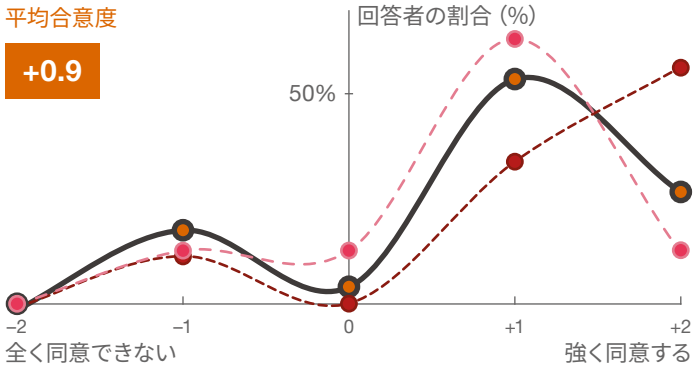
仮説 1

長期的に見て、安全な車両のみが競争を勝ち抜くことができる。したがって、OEMはたとえ規制がなかったとしてもCSMS要件を満たすために多額のコストを費やしただろう。



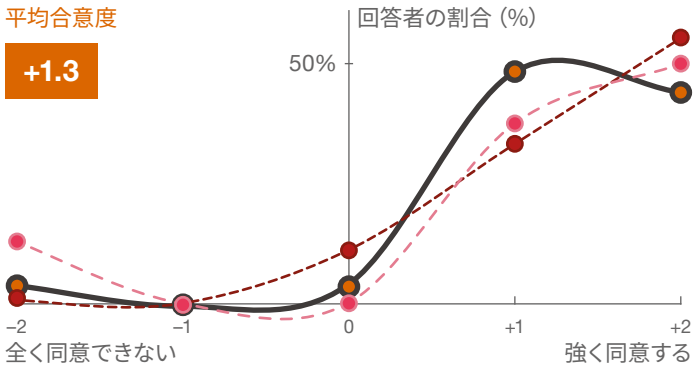
仮説 2

サイバーセキュリティの成熟度の高さは、今後、車両を販売するうえでの明確な競争上の優位性となるだろう。



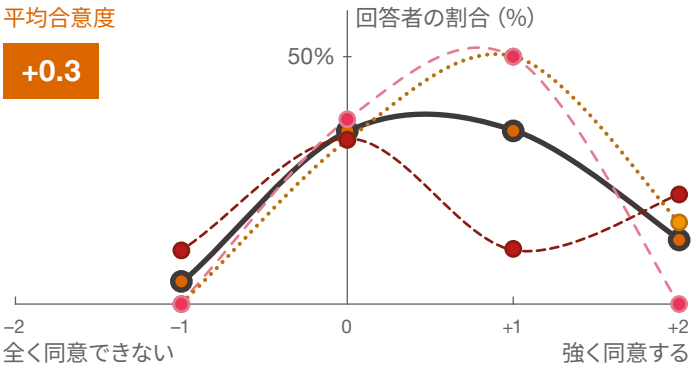
仮説 3

サプライヤーとOEMのセキュリティマネジメントシステムは、規制要件に対応するために、一層の連携強化が必要である。



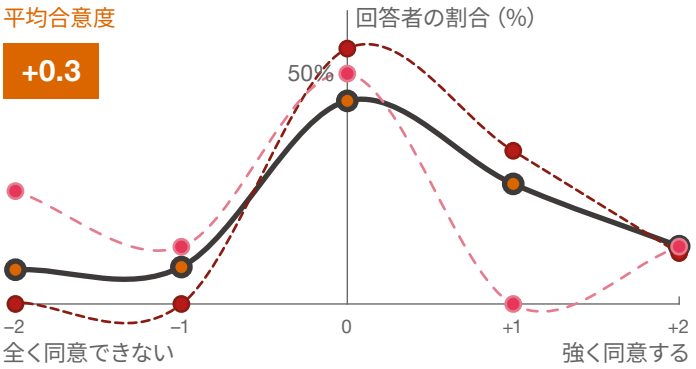
仮説 4

認証を取得しやすくするために、またリスクを細分化するために、OEMは自社のCSMSを必要最低限に絞り、他のマネジメントシステムと大規模な統合を図ることはない。



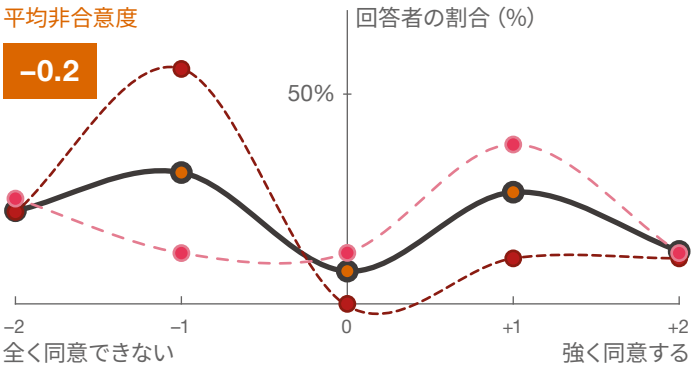
仮説 5

OEMは、今後自社によるサービス提供を増やし、自動車バリューチェーンのより多くの部分を内製化していくだろう。



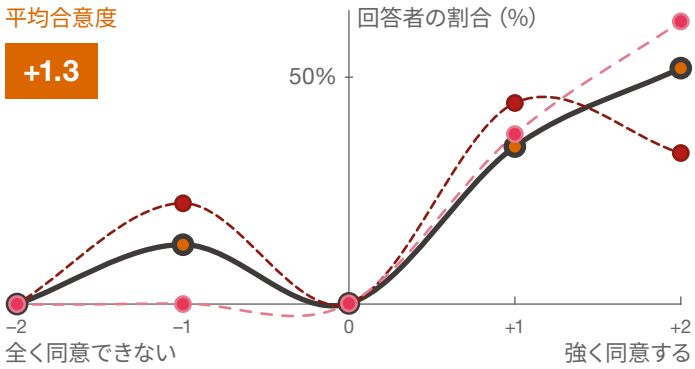
仮説 6

新型車種の承認取得を遅らせることなくCSMS要件を満たし、監査用の証拠書類を作成することは不可能である。



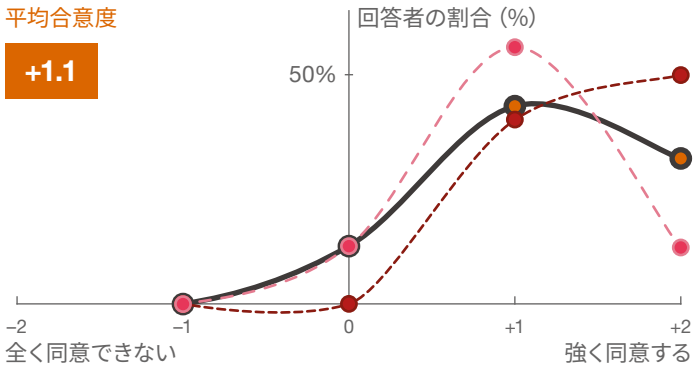
仮説 7

コネクテッドカーや自動運転の進展は、国のインフラ機能や政治的／経済的安定性に大きく左右される。



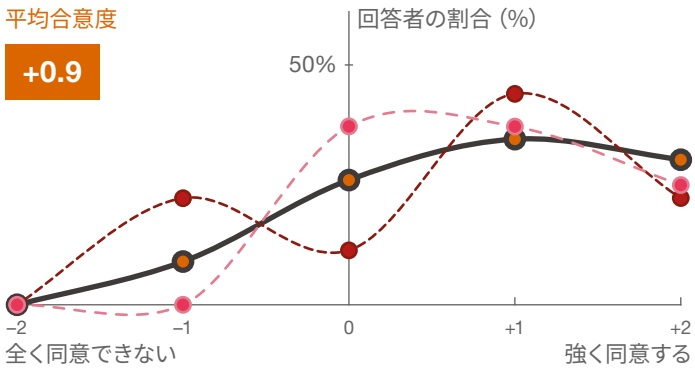
仮説 8

国連規則155号 (CSMS) は、車両の安全性向上につながるものであり、必須である。



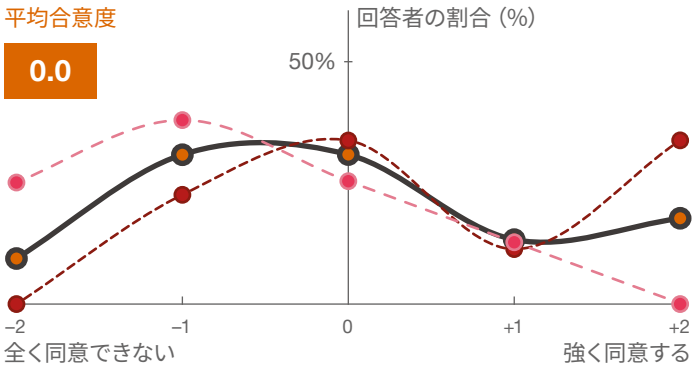
仮説 9

コネクテッドカーと自動運転の発展によって従来の市場シェアは今後大きく変わる。



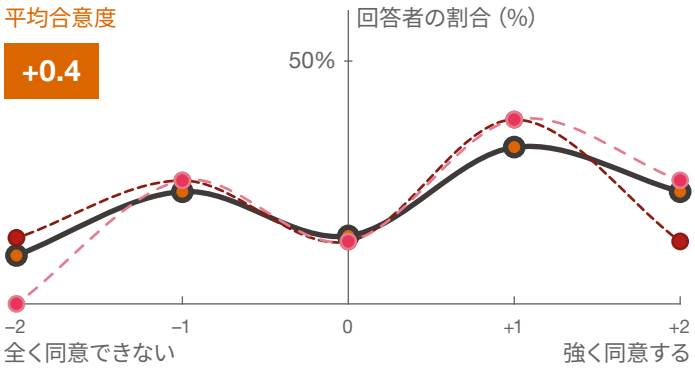
仮説 10

OEMは、自社のサプライヤーがCSMS要件との契約に準拠するために包括的なサポート (ベストプラクティスやツールなど) を提供する。



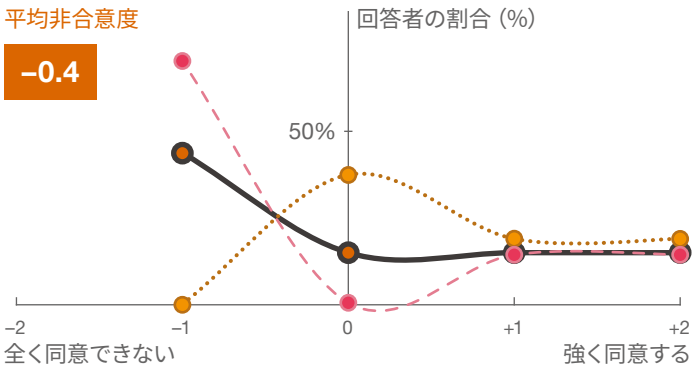
仮説 11

セキュリティ重視のサプライヤーは、OEMのバリューチェーンに対する自社の貢献度と重要性を明確に自覚している。



仮説 12

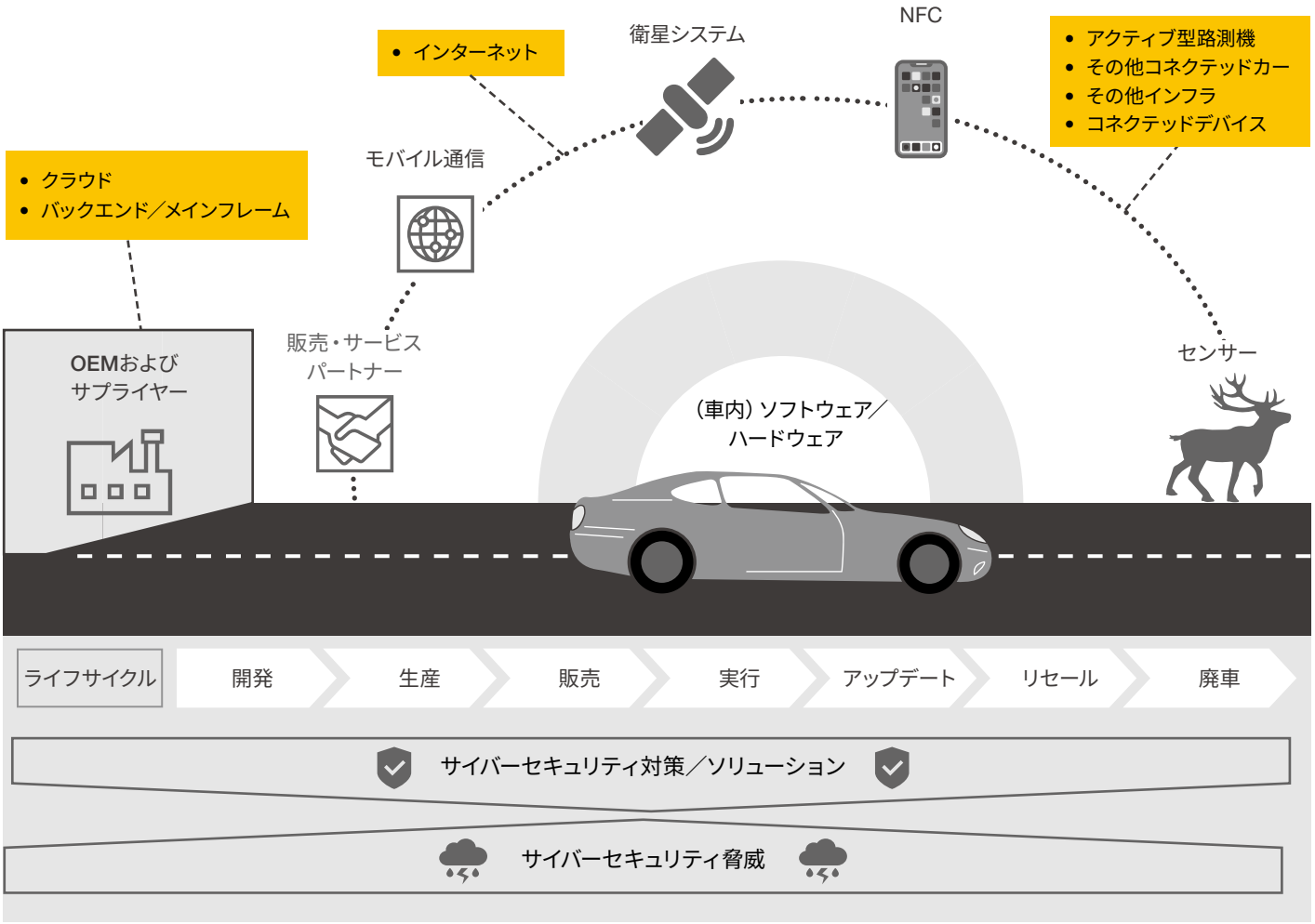
結局のところ、車両のセキュリティはエンドユーザーの行動に大きく左右される。



自動車エコシステム

この調査は、自動車エコシステムに関するPwCの理解に基づき実施したものである。言うまでもなく、このエコシステムの中心に位置するのは車両であり、ハードウェアとソフトウェアで構成され、周囲の環境と密接に結びついている。OEMはサプライヤーから部品を調達して車両を製造し、その車両を直接または販売パートナー経由でユーザーに販売する。これには、OEMやその販売・サービスパートナーによるアップデート時の車両への有線接続が含まれる。車両は、モバイルインターネット経由でOEMやサプライヤー、ユーザーとつながっており、情報のやり取りやサービスの利用が可能となっている。ユーザーや他の交通参加者は、近距離無線通信（NFC）を用いて、車両やその関連サービスに接続することも可能である。車両は、非接続・間接的な交通参加者からも情報を収集する。

図表1　自動車エコシステムに対するPwCの理解



B 重要ポイント

PwCは、自動車業界においてサイバーセキュリティマネジメントに携わるさまざまな専門家にインタビューを行った。その回答から浮かび上がってきたことは何か。以下は、専門家の回答から得られた極めて明確な知見である。

1.

自動車エコシステムに対するサイバーセキュリティ脅威は高まっており、セキュリティの高度化が急務である。

この調査ではまず、自動車エコシステムのサイバーセキュリティ課題に対する認識について質問した。その結果、OEMとサプライヤーで意見の相違が見られた。こうした相違は、サイバーセキュリティマネジメントに関して、自動車部門内でさまざまな意見があることを示している。同部門においてこのトピックは比較的新しい課題であり、明確性や透明性の水準も他業界に比べてまだ低い状態にある。しかし、両者間で広く意見が合致した点がひとつある。すなわち、車両および自動車エコシステム全体に対するサイバー攻撃は今後激増する、というものである（仮説13参照）。

車両エコシステムに対するサイバーセキュリティの脅威について評価を求められた際、サプライヤーは概して批判的だった。OEMが直面している脅威に対して、OEM自身よりもサプライヤーの方が批判的に評価していた。同様に、サプライヤーが直面する脅威については、サプライヤーよりもOEMの方がより批判的に評価していた（図表2参照）。これは、サイバーセキュリティの脅威に関してOEMとサプライヤー間でコミュニケーションと透明性が不足していることを明確に示すものである。

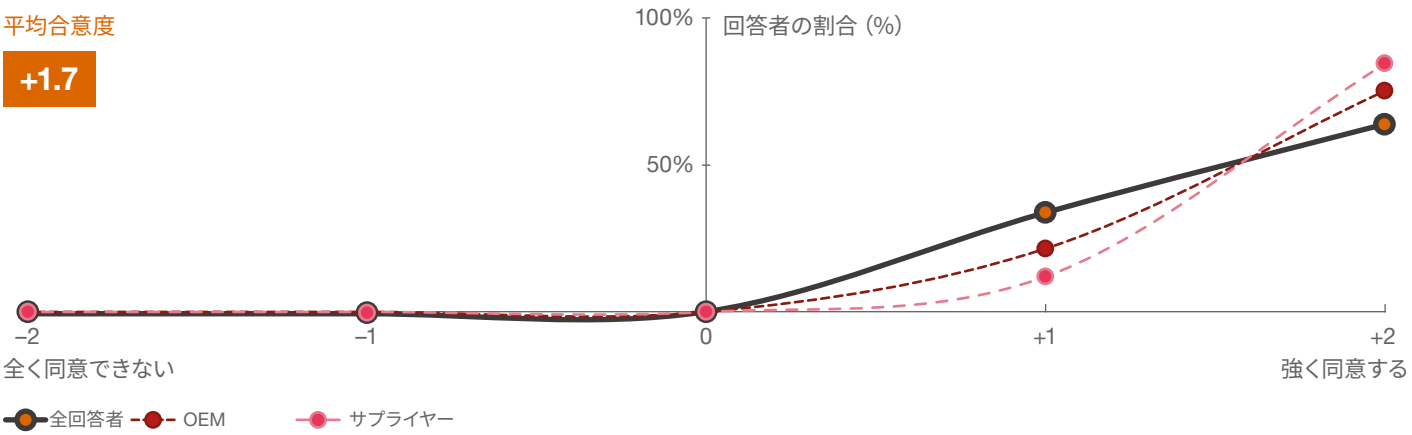
また、大部分の回答者が、OEMとサプライヤーが運営するセキュリティマネジメントシステムは、規則に準拠すべく、より連携を強化していく必要がある、という意見に同意した（仮説3参照）。OEMとサプライヤーは、バリューチェーン内全体で連携を図る重要性についてほぼ見解が一致していたが、OEMがCSMSをサポートするうえで果たすべき重要な役割をまだ認識していないサプライヤーも一部見られた（仮説11参照）。

ライフサイクルのうち、どのフェーズが最大の脅威に直面しているかについても、OEMとサプライヤーの間で広く意見の一致が見られた（図表2参照）―アップデートフェーズを含む実行フェーズにおいて、脆弱性が最も高いと考えられている。これはライフサイクルにおいて一番長いフェーズであり、管理も最も難しいことを考えれば当然と言える。また、実際に車両を購入してサイバー攻撃を試すことができるため、攻撃者が車に最もアクセスしやすいフェーズでもある。

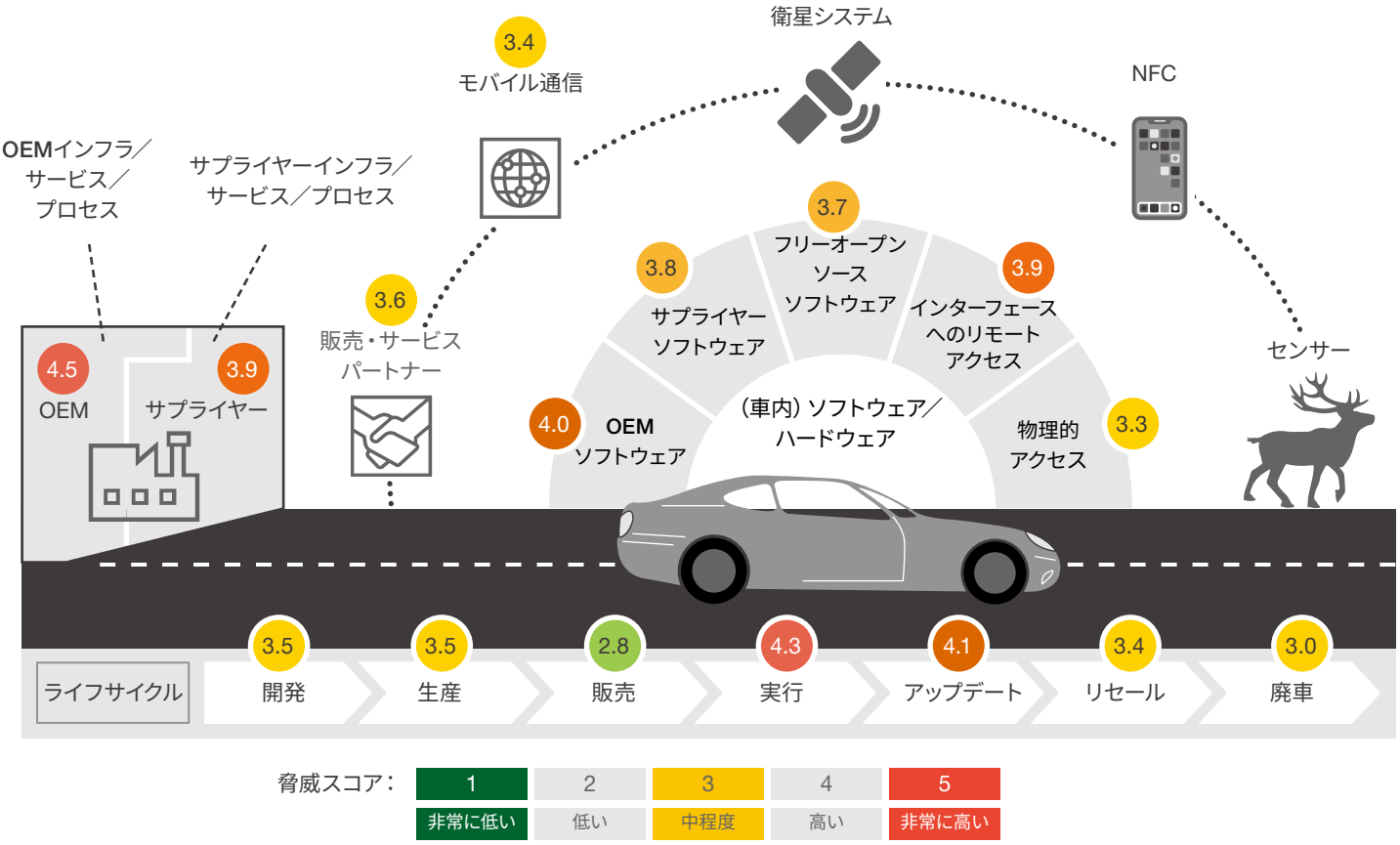
さらに、マルウェアなどによって最も侵害されやすい（脆弱性が高い）のはアップデートフェーズである、という点でも見解の一致が見られた。これは、侵害されたアップデートが、マルウェアが車両に侵入する経路になり得る、と考えられていることを示すものである。ここで重要なのは、全てのアップデートが同じとは限らない、という点である。リモートアップデートは、全ての車両に影響を及ぼすが、ローカルソフトウェアアップデートまたは物理的設定ミスは、特定の車両が対象となる。ただし、どちらも一般ユーザーにとって極めて危険になり得ることに違いはなく、またOEMの評判が著しく低下する恐れもある。

仮説 **13**

車両および自動車エコシステム全体に対するサイバー攻撃は今後激増する

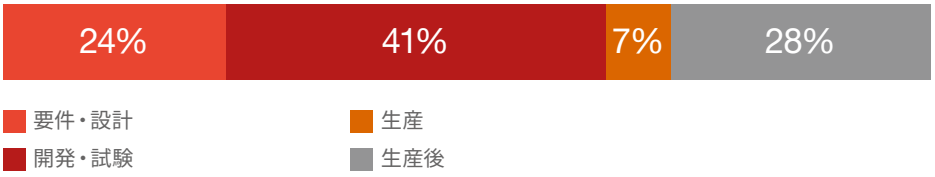


図表 **2**　貴社の車両エコシステムに対するサイバーセキュリティ脅威について、どのように評価していますか。



車両製造プロセスのうち、セキュリティ脆弱性が最も多く特定されたのはどのフェーズか、という質問に対して、全ての回答者が、開発・試験フェーズが弱点を特定する際に重要、と回答した（図表3参照）。驚くべきは、インタビュー対象者が、脆弱性の約3分の1は生産後に特定される、と推定している点である。つまり、回答者は、OEMとして試験に莫大な費用と労力を費やしているにもかかわらず、製造前試験の段階では脆弱性の3分の1が特定されない、と予想しているのである。これらの脅威は、エンドカスタマーによる運転中および使用中の自動車をターゲットとするものであり、最も重大である。生産後のフェーズは最大20年間継続する可能性があることを忘れてはならない。この期間にどのような新しい脆弱性が発生するか予測することは困難である。しかし、自動車部門のステークホルダーは、販売後もコネクテッドカーをセキュアに保つという課題を過小評価しているきらいがある。特にこのフェーズでは、ディーラーから他のコネクテッドデバイスや外部サービスに至るまで、新たな方向からの攻撃の可能性が生じる。

図表**3**　車両開発において、セキュリティ脆弱性が最も多く特定されると思われるのはどのフェーズですか。



2.

テクノロジーは急速に進化しており、ビジネスの命運を左右するにも関わらず、規制が追いついていない。

コネクテッドカーや自動運転の技術進化や、社会におけるこれらのトピックの重要性を考えると、規制当局による一貫したセキュリティ要件の設定は待ったなしの状況である。これを裏付けるかのように、インタビュー対象者のほぼ全員が国連規則155号（CSMS）は、車両の安全性向上につながるものであり必須である、と回答している（仮説8参照）。

同時に、OEMは、多くの市場において、新型車種の登録承認を受けるにはCSMSが必須となる可能性に直面している。2022年7月以降、国連規則155号によって、OEMは新型車種を世界56カ国の国家当局に登録するために、監査済みCSMS証明の提出義務を課されることになる。2024年7月以降は、CSMSを設けていない限り新車の生産が不可能になる。また、UNECE非加盟国でも同様の規則が設けられると予想される。

CSMSがビジネスの命運を左右する重要課題であることは、すでに回答からもうかがえる：インタビュー回答者の5分の2以上が、CSMS要件対応が新型車種の認証取得の遅延につながるだろう、としている（仮説6参照）。

3.

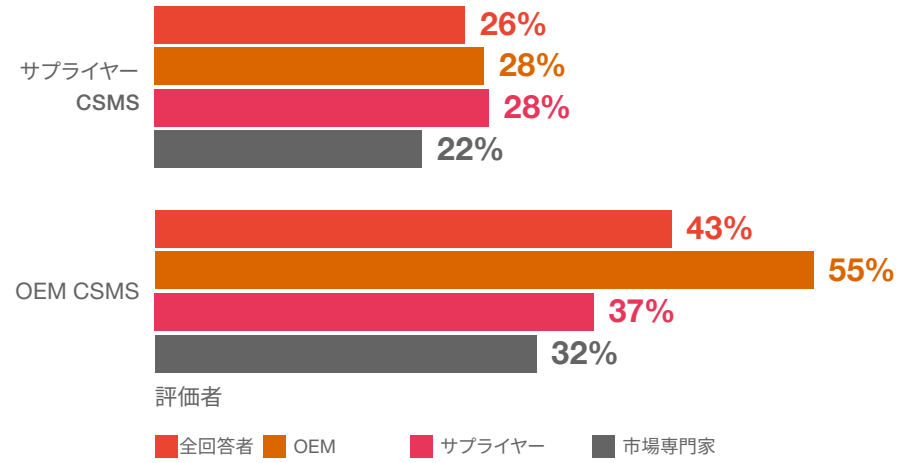
OEMやサプライヤーはすでにCSMSに着手しているものの、多くは設計段階にとどまっており、成熟度は低いため、さらに上を目指す必要がある。

今回の調査を行ったOEMはいずれも、CSMSを導入済みと回答した。ただしこの回答の大部分は、CSMSを設計しているということであって、回答者のほとんどは、CSMSの大部分はまだ運用に至っていない、と答えている。調査に参加したOEMの約3分の2が、すでに外部監査機関によるCSMS設計監査を受けている（図表9参照）。これらOEMに対して、グローバルな競合他社との比較で、自社の監査済みCSMSの普及度を尋ねたところ、低調との評価だった。OEMの5分の2、サプライヤーの4分の1のみが、自社のCSMSを評価したと推算される（図表4参照）。

「はじめに」で説明したように、OEMは、仕様と義務を契約事項に含めることにより、規制要件をサプライヤーにも適用している。技術的な実装の多くをサプライヤーに外注しているOEMにとってセキュリティ管理には限界があることを考えると、このアプローチは理解できる。したがって、サプライヤーは、さまざまなOEMまたはさまざまな車両モデルに提供するコンポーネントについて、安全性を確保する責任を負う。

こうした状況において極めて重要なポイントは、OEMは、サプライヤーが全ての関連規制・基準に準拠していることを確認する義務を負う、という点である。こうした仕組みが、ソフトウェアとハードウェアコンポーネント、ひいては車両全体のエンドツーエンドのサイバーセキュリティ基盤を形成するのである。しかし、個別のリスク評価を除けば、自動車業界に車両サイバーセキュリティの共通指標はまだ存在しない。

図表 4　これまでの経験から、OEMとサプライヤー、どのくらいの割合が自社のCSMS評価に成功していると思いますか。

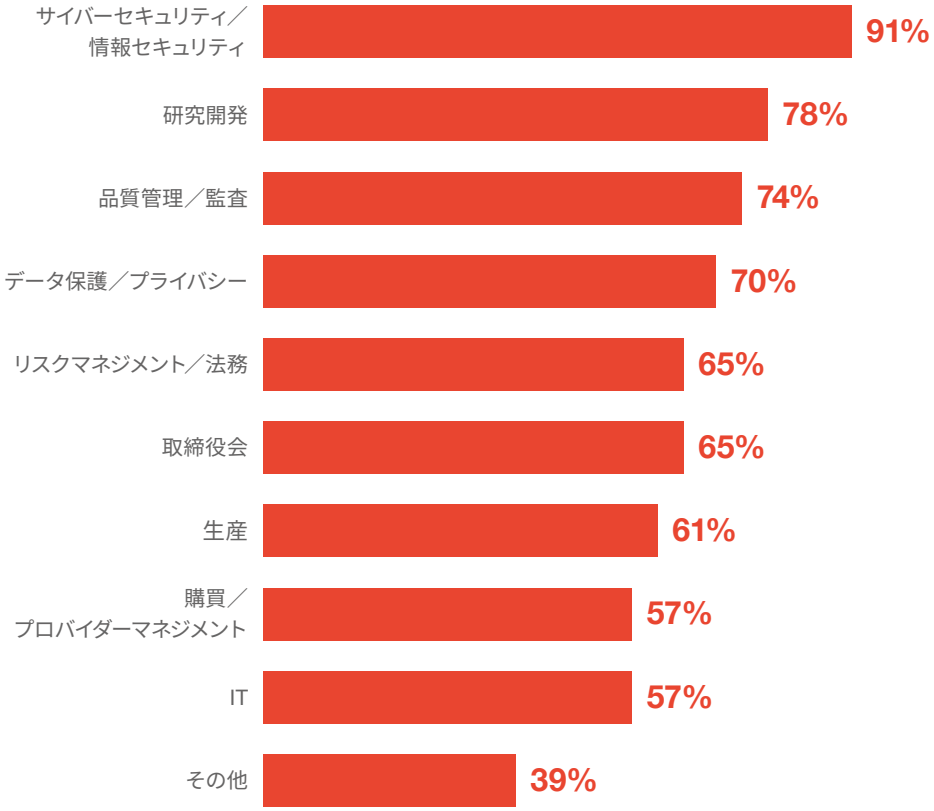


インタビューしたOEM代表者のうち75%が、サプライヤーにCSMSに関する契約要件を課していると回答しており、同じく75%のサプライヤーが、OEMからCSMSに関する契約要件を満たすよう求められている、と答えた。残りの25%は、類似の要件がすでに設けられているものの、CSMSを具体的に検討するように要件が更新されていないものと思われる。

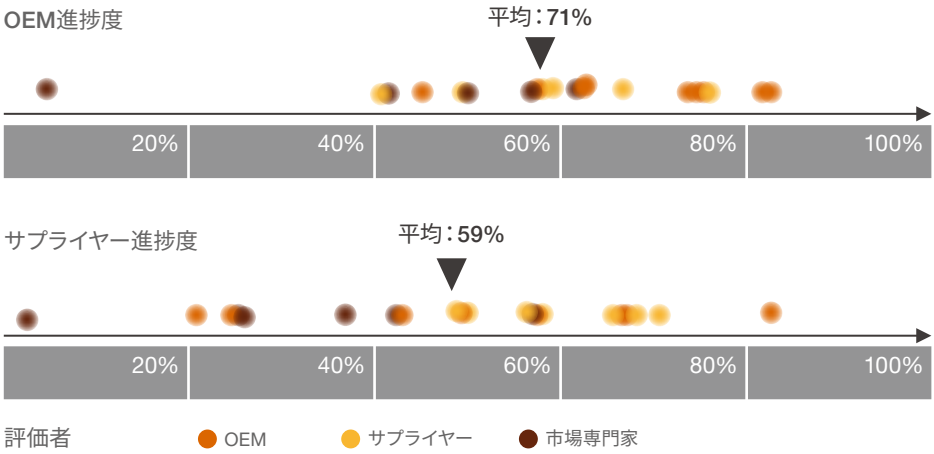
調査では、CSMS対応にどの社員／部門が積極的に関与しているか尋ねた。その結果、これらの企業の全ての領域で、サプライヤーよりもOEMの関与度が高いことが示された（図表5参照）。これは、サプライヤーが依然としてCSMSを一部にのみ関係するものとして捉えている傾向がある、つまり、OEMに提供する一部のサービスまたは製品についてのみ考慮していることを示している。一方、OEMにとって、CSMSは社内ガバナンス体制のより大きな部分を占めるようになっている。あらゆる大規模プロジェクトの成功のカギを握るのは上級管理職の関与度であることを考えると、取締役会がどれだけCSMSに関与しているか、という点は興味深いポイントである。

これらのCSMSプロジェクトが実装のどのフェーズに達しているか、という問いについては、回答者によって反応が異なる。進捗状況についての回答はOEM、サプライヤー、市場専門家で異なっており、完了度は5%～100%と大きな幅が見られた。これらの結果は、自動車業界においてこのトピックに関する情報共有が完全に欠如していることを示している。回答者はいずれも、エコシステム内のさまざまなプレイヤーがどのような立場にあるか、評価に悩んでいる（図表6参照）。

図表 5　貴社でCSMSに関与している／CSMS要件対応に関与している部門はどこですか。



図表6　CSMS実装要件に関する貴社および貴社サプライヤーのプロジェクトは、どの程度進展していますか。（完了度（%））

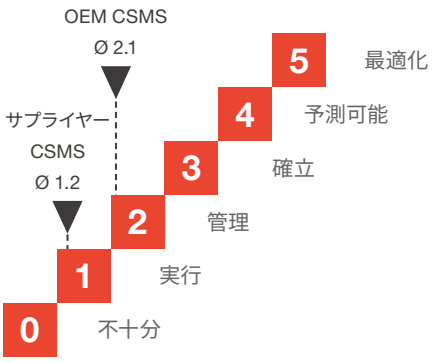


この質問への回答は、市場専門家とOEM・サプライヤーの間で、要求事項が異なっていることを示唆するものでもある。OEMとサプライヤーがCSMSの最小要件を満たすことのみを目指しているのに対して、専門家はさらに多くを求めている可能性がある。

しかし、OEMの成熟度に関する評価は、回答者間でほぼ同様であった。これは、サプライヤーはOEMに課せられた要件にのみ注力していることを示すものかもしれない。OEMが、サプライヤーの進捗状況についてサプライヤーの自己評価よりも低く評価している、という事実は、OEMがサプライヤーから提供されるソリューションに満足していないことを意味する可能性がある。

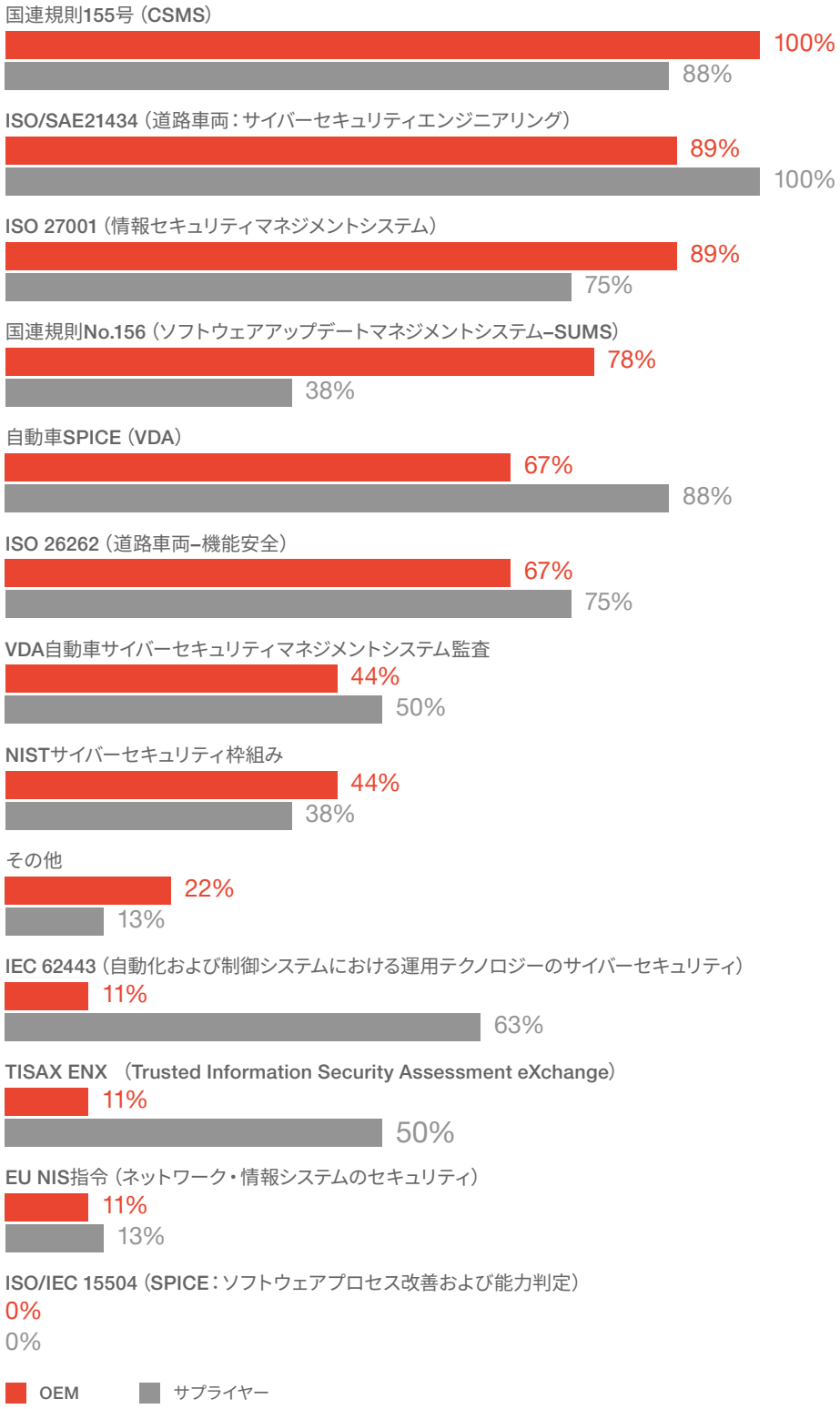
CSMSへのアプローチも、サプライヤーよりもOEM内部の方が進んでいると思われる。しかし回答者が、CSMSの実装はまだ初期段階であり（図表7参照）、コネクテッドカーを望ましいレベルの効率性とセキュリティで運用できるようになるまでにクリアすべき課題は非常に多い、という認識を共有していることは明らかである。

図表7　貴社のこれまでの経験から、OEMのCSMSの平均成熟度をどのように評価しますか。



[1] VDA ISA 5.1成熟度レベル

図表 8　（貴社の）CSMSに関連する標準／枠組みはどれですか。

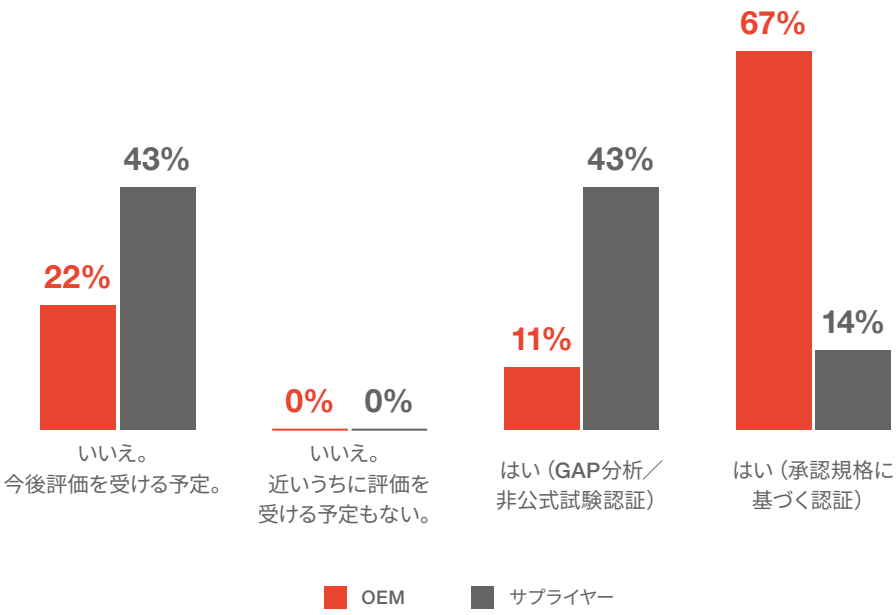


CSMSの成熟度に関して言えば、サプライヤーはOEMに後れをとっている。しかし、同じサプライヤーでも状況は大きく異なる。平均を上回る成果を上げているサプライヤーもあれば（特にティア1）、そうでないところもある。特にサプライヤーにとってCSMSは大きな競争上の優位性となる。自社がセキュリティ要件に準拠していることをOEMに証明するツールとなるためである。CSMS基準の厳格化が進む中、こうした競争上の優位性は、OEMとの取引を望むサプライヤーにとって今後必須となる可能性がある。

回答者が自社のCSMSに関連すると考えている基準や枠組みは、それぞれ異なっている。グローバル市場において、OEMとサプライヤーは各自、CSMSに取り組むうえでどのセキュリティ基準を土台としていくか（リージョンレベル／グローバルレベル）選択する必要がある。このため、今回の調査では、どの基準や枠組みが最も重視されつつあるかについても明らかにした。

このような状況において、認証制度は潜在的な問題を可視化するひとつの方法であり、OEM は市場アクセスを獲得するために認証が必要となる。今回の調査において全ての回答者が、CSMS 評価を受けることの重要性を認識している、と回答している（図表 9 参照）。大部分の OEM は、すでに国連規則 155 号に準拠した認証を獲得している。一方、サプライヤーは GAP 分析や非公式の試験認証に頼るケースがほとんどだが、将来的には外部認証の取得に向けた明確な計画を設けている。

図表9　貴社のCSMSは、外部監査機関の評価を受けたことがありますか。



4.

サイバーセキュリティ向上の道のりを阻む障壁

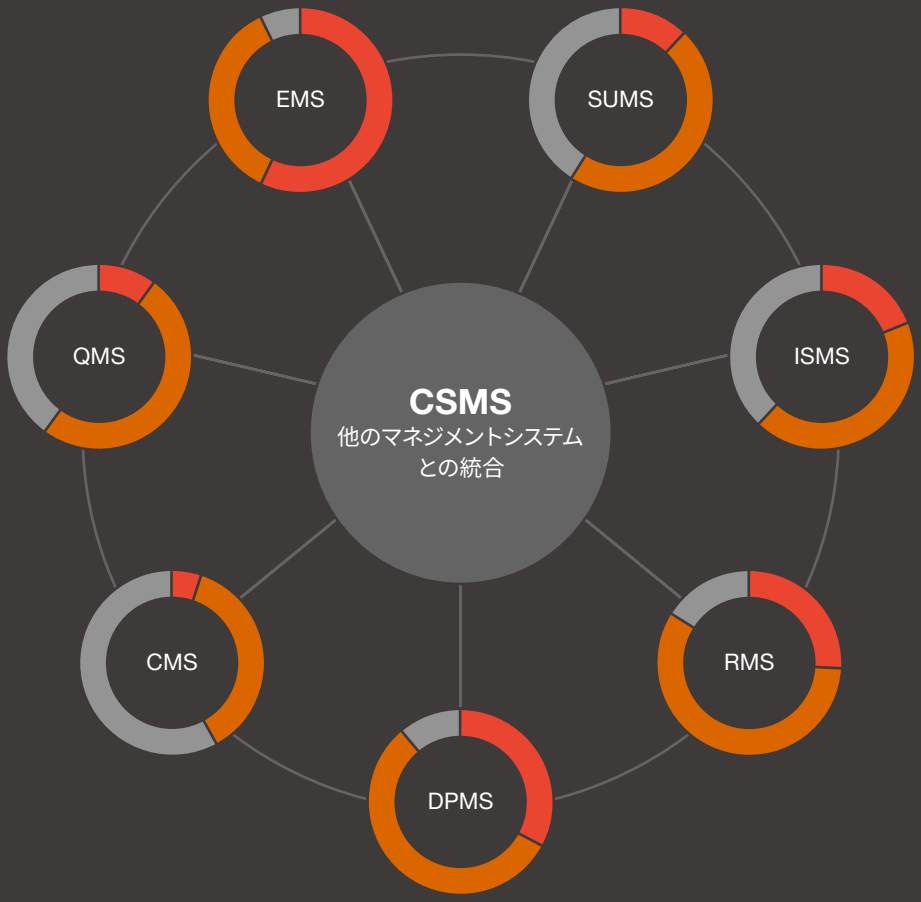
OEMが直面しているサイバーセキュリティの脅威の規模と深刻さについて意見が一致しているのであれば、なぜこれらの企業に大きな進展が見られないのか。この点について理解するために、「自動車の安全性を高めるうえで最大の障壁となるもの」を挙げてもらった。これも意見の一致が見られた数少ないポイントであった。「熟練者の不足」と「時間的制約」、次いで「要求仕様の不十分さ」が挙げられた（図表10参照）。

図表10　自動車の安全性を高めるうえで、目下最大の障壁となっていることは何ですか。

1	熟練者不足／ノウハウやトレーニングの不足
2	社内外の納期による時間的制約
3	要件に対する解釈・仕様の不足
4	サプライチェーンの複雑性
5	マネジメントの認識不足
6	予算不足
7	バックエンドインフラ不足
8	車両用ハードウェア部品の入手困難

また、社内でサイバーセキュリティをどのように管理するかという問題についても、対応が必要である。今のところ、OEMの経営陣は、完全に統合されたマネジメントシステムの必要性については、あまりピンときていないようである。全ての回答者が、ある程度CSMSを実装していると回答しているが、まだ統合マネジメント手法に組み込まれた状態になっていない（図表11参照）。むしろ、CSMSと他のシステムとの連携はまだ始まったばかり、という企業が大半である。品質マネジメントシステム（QMS）や製品コンプライアンスシステムとの統合から始めるケースが最も多い。一般的に、OEMはサプライヤーに比べてやや高いレベルの統合を達成している。

図表 **11**　貴社の**CSMS**は、その他のマネジメントシステムとどの程度連携していますか。



SUMS=ソフトウェアアップデートマネジメントシステム、ISMS=情報セキュリティマネジメントシステム、RMS=リスクマネジメントシステム、DPMS=データ保護マネジメントシステム、CMS=製品コンプライアンスマネジメントシステム、QMS=品質マネジメントシステム、EMS=環境マネジメントシステム

統合されていない　一部統合済み　完全に統合済み

この調査では、今後OEMが、認証を取得しやすくするために、またリスクを細分化するために、自社のCSMSを必要最低限に絞って他のマネジメントシステムとの統合をほとんど行わないのではないか、という懸念についても質問している。これに対して、3分の1が同意、3分の1が反対、残り3分の1がどちらとも言えない、という結果であった（仮説4参照）。CSMSがより密に連携する必要性については幅広く意見の一致が見られるのに対して、この質問については見解が分かれた。OEMが意図的にこれらのシステムの対象範囲を限定する可能性がある、という回答者もいた。では、マネジメントシステムを首尾よく統合するためにはどうすればよいのか。

現段階において、本当の意味での統合は目標ではないのかもしれない。インタビューによると、多くの企業はマネジメントシステムの完全な統合を目指すよりも、システム間の連結（interlink）を目指していることが示唆されている。これは、CSMSのアプローチの柔軟性と監査適合性のサポートにつながるだろう。同時に、コンプライアンスのみに的を絞ったアプローチは危険であって、あくまで明確な事業戦略を土台としてそうしたDXを進めていく必要がある。

サプライチェーンを見ると、CSMS要件に取り組むサプライヤーをOEMが包括的にサポートしているかどうかも曖昧である（仮説10参照）。大部分の回答者は、OEMがバリューチェーンの一部の部品を再び内製化する一方で、他の部品の外注化は一層増加すると考えている（仮説5参照）。しかし、自動車サプライチェーンが密に連携していることに変わりはなく、強力な協力体制が重要であることに変わりはないだろう。

5.

実装―細部に潜む落とし穴

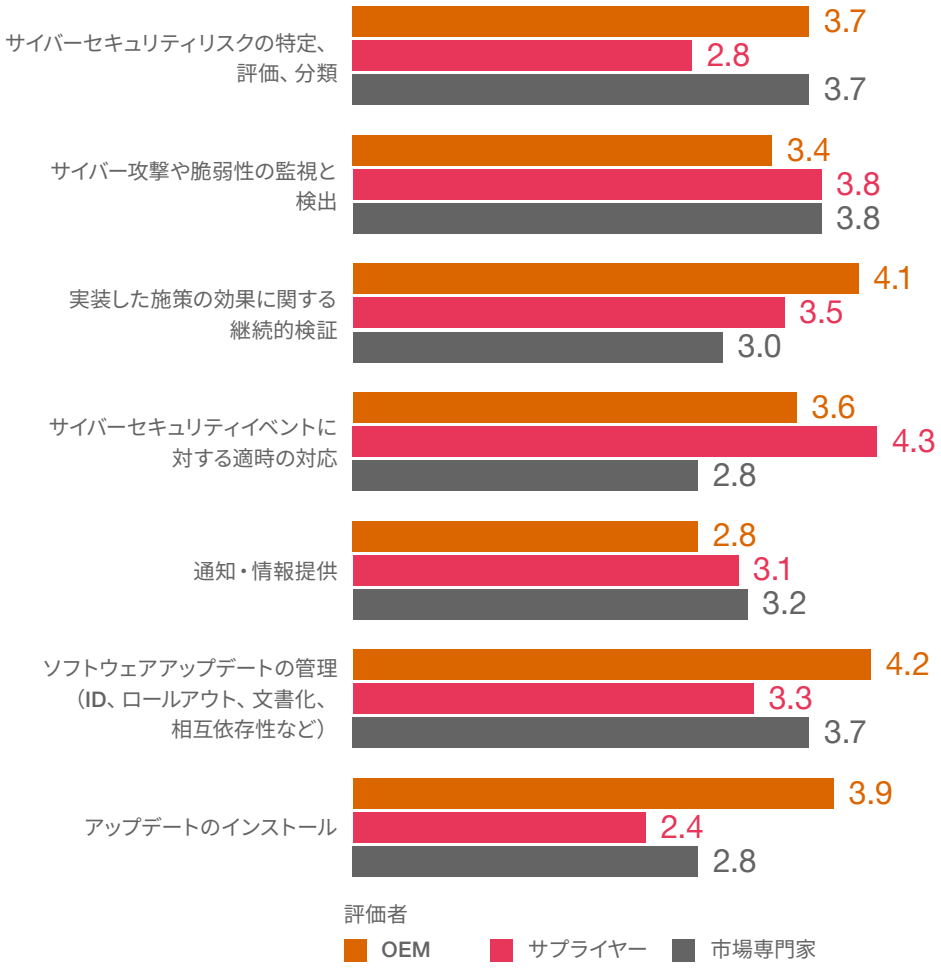
多くの回答者がすでにCSMSを実装していると思われるが、いくつかのCSMSコアプロセスについては、まだ実装のハードルは高いと考えられている。調査の結果、CSMSの実装に関する課題認識が、回答者によって明確に異なることがわかった（図表12参照）。CSMS要件の中で最も対応が難しいのは何か、という質問に対して、サプライヤーの回答で最も多かったのは「サイバーセキュリティイベントに対する適時の対応」であった。一方、OEMの場合、「ソフトウェアアップデートの管理（ID、ロールアウト、文書化、相互依存性など）」という回答が最も多かった。

これらの回答から、OEMとサプライヤーとでは、CSMSに対する観点が大きく異なることがわかる。通常、OEMがアップデート対応の責任を負う。サプライヤーは、電子制御ユニット（ECU）をアップデートするためのソフトウェアを提供するのみで、そのアップデートを車両に適用する責任を有していないため、この問題ははるかに小さい。これは、OEMがこの義務をまだ契約によってサプライヤーに託していないことを示唆している。その結果、OEMとサプライヤーは、効果的なCSMSを実装する際の課題について認識が一致していないのである。

CSMSの設計の効率性は運用段階で明らかになる。そのため、既存のビジネスに対するサイバーセキュリティコストにも重大な影響をもたらすことになる。現在実装を進めているCSMSの設計が計画どおりに運用できない場合、そのシステムは次なるコンプライアンスリスク―自社の組織要件に対するコンプライアンス違反―となる。

図表 **12**　最も対応が難しいCSMS要件は何ですか。

1=非常に簡単、2=簡単、3=中程度、4=難しい、5=非常に難しい



人間の行動もまた、不確実性の高い領域である。設計段階でのセキュリティ強化に注力すべきという意見がある一方で、例えば、安全でない機器に接続する、サードパーティー製のアフターパーツを使用する、ソフトウェアアップデートを怠るなど、ユーザーが自らの責任を果たさないケース（仮説12参照）について、業界としてできることは少ない、との意見もあった。

6.

CSMSを支える技術ソリューションのトレンドが明確に

では、業界として具体的にどのような取り組みを行うべきか。回答者に、自動車部門でCSMS推進に向けて取り組むべき技術開発を挙げてもらった（図表13参照）。

カギを握るのはソフトウェアアーキテクチャということで、実にインタビュー回答者の96%が挙げている。ユーザビリティ、セキュリティ、安全性、メンテナンスなどは全て、ソフトウェアに左右される。車両のソフトウェアおよびコンピューティング能力のモジュール化、スケーラビリティが極めて重要であり、これらは長期的にコスト効率の良い生産と運用に不可欠である。インタビュー回答者の約4分の3が、車両モニタリングと車両セキュリティオペレーションセンター（SOC）向け技術開発が必要であると述べている。

図表 13　CSMS要件に適切に対応するために、技術開発が最も必要とされるのはどの分野ですか。

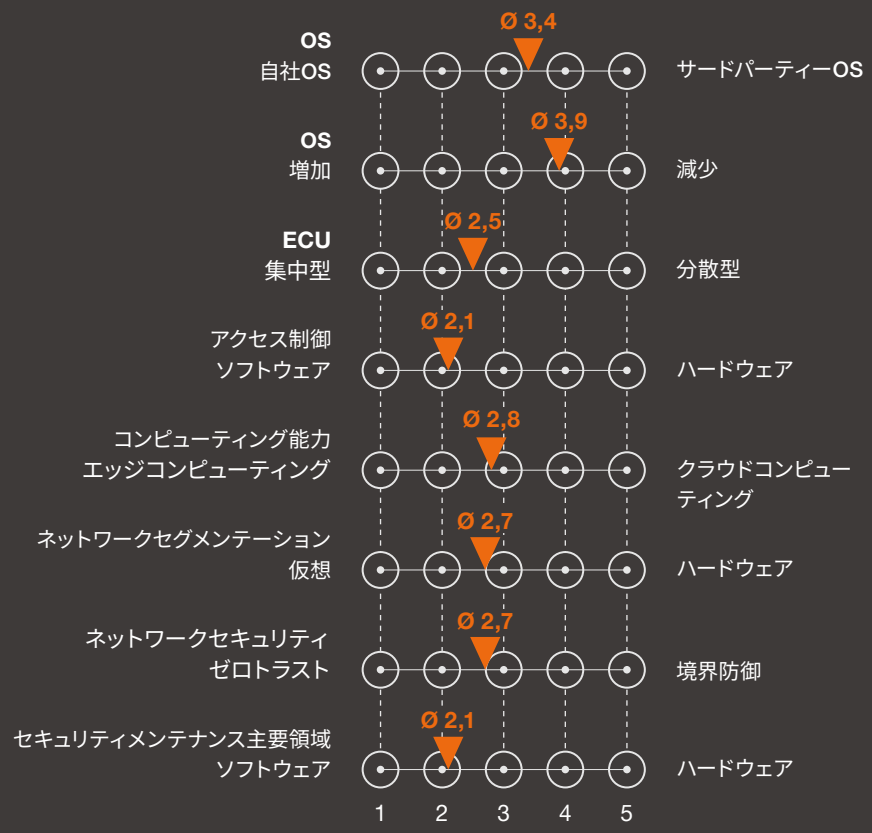
上位5分野

1. 車両ソフトウェアアーキテクチャ
2. 車両モニタリング／SOC
3. OEMとサプライヤーのバックエンド
4. 車両技術アーキテクチャ
5. モバイル通信インフラ

次に、現在のサイバーセキュリティの進化が、今後車両アーキテクチャにどのような変化をもたらすかを尋ねた。ほとんどの回答が、5段階のうち低〜中の範囲に収まっていることから（図表14参照）、将来の展望や企業が選択する長期的な戦略について、まだ意見が分かれていることが示唆される。OEMとサプライヤーの最大の相違点はECU関連であった。サプライヤーは、車載ECUの数は、OEMが予想するよりも早く減少すると考えている。ECUの数は減少傾向にある一方で、車両制御システムの複雑さは増している。これにより、ソフトウェア機能に対する要件が高くなる。そのため、ソフトウェアがサイバー攻撃ターゲットとなる可能性も一層増している。

また、国のインフラ機能や政治的・経済的環境が安定していることの重要性についても意見を求めた（仮説7参照）。自動運転とコネクテッドカーには、自動車業界外部の強力な体制が必要である、という点で回答者の意見は一致していた。これは、セキュリティがOEMやサプライヤーだけの問題ではないことを示している。また、政府は将来的に安全な運転を実現するための適正な条件を整備する必要がある。

図表 **14**　現在のサイバーセキュリティの進化は、どのような車両アーキテクチャ規則につながっていくと思われますか。



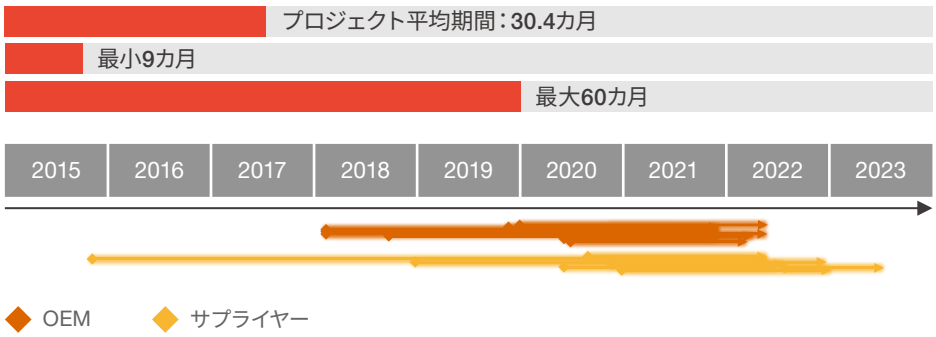
7.

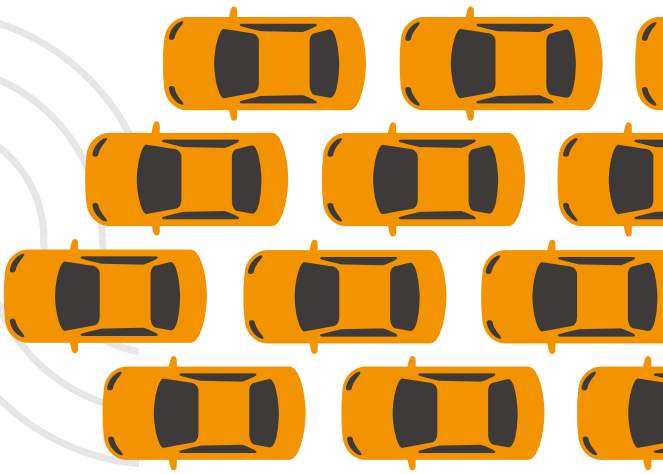
CSMS実装は困難で多くのリソースが必要

回答者のCSMSプロジェクトについては、初期実装のタイミングに大きな差が見られた。この点について、一般にはOEMがサプライヤーに先行し、より早期に終了すると予想される。これは、OEMが規制の直接的対象となっていることを考えれば納得である。ただし、サプライヤーもその後を追って実装を進めている。これは、OEMが新しいCSMS要件を自らのサプライチェーンにうまく統合していることを示唆している。最も興味深いのは、回答者が示したプロジェクトの平均期間が30カ月であることだろう。これは、CSMSプロジェクトが難しいこと、そしてほぼ間違いなく労働集約的な性質を有することを示している（図表15参照）。これは担当部門リストからも一目瞭然である（図表5参照）。

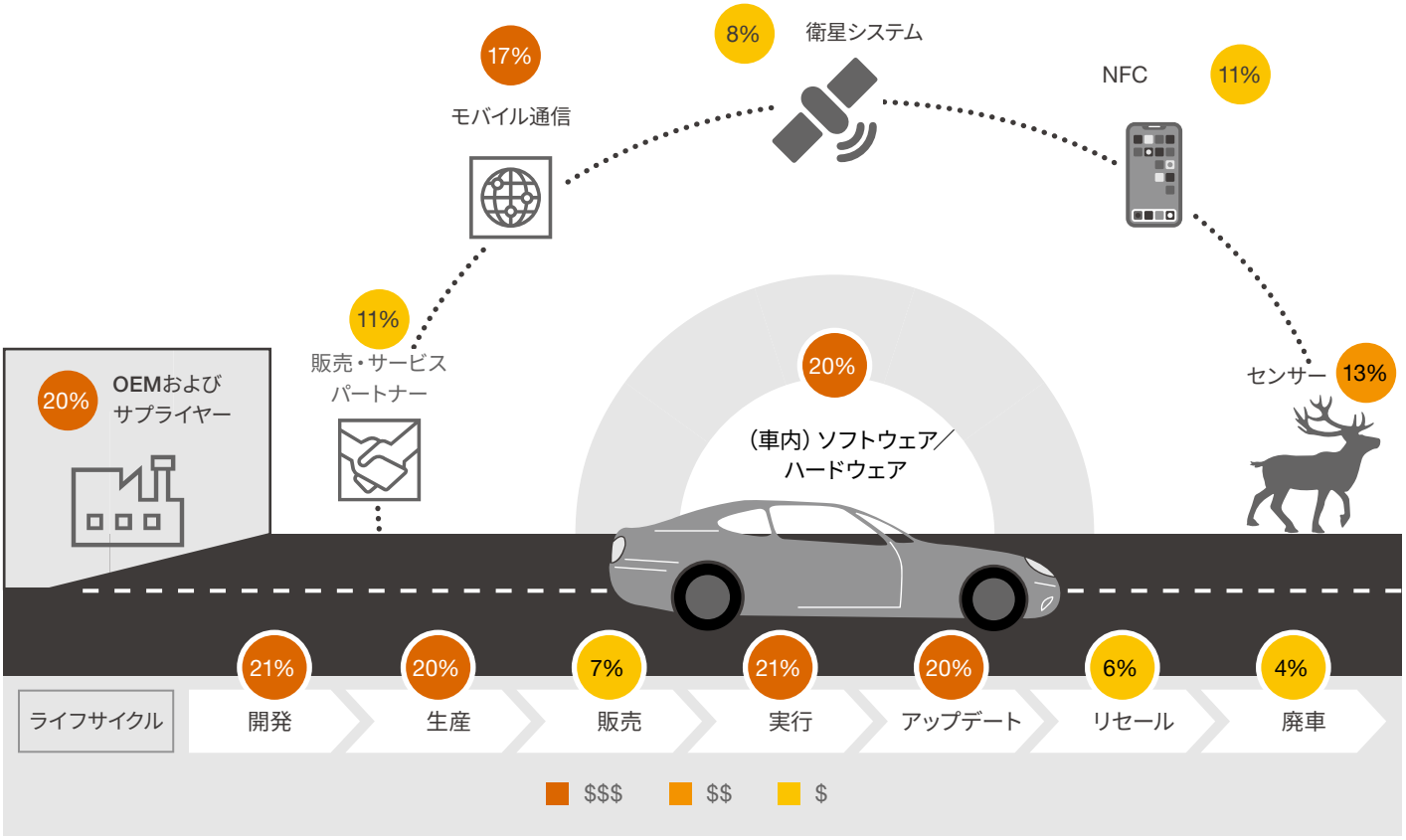
OEMによるCSMS実装への投資額が、自動車エコシステムと車両ライフサイクルにおいてどう配分されるかについては、開発・実行フェーズにそれぞれ21%、さらに生産・アップデートフェーズにそれぞれ20%という結果であった（図表16参照）。アップデートフェーズは実行フェーズの一部であることから、CSMS投資額の40%以上が運用に向けられることになる。現在、標準化されたプロセスや、自動化、適切なツールサポートに多額の投資を行っているOEMは、今後実行フェーズでコスト削減に成功し、結果的に競争上の優位性を獲得するだろう。自動車の寿命は最大で20年間に及ぶ可能性があるため、この点については長期的な視点での検討が特に重要である。

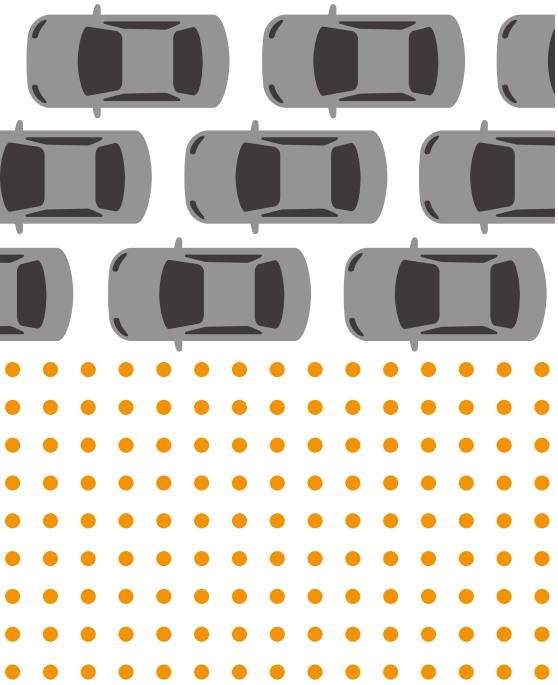
図表 **15**　初期CSMSプロジェクトの開始・終了・期間





図表 **16**　OEMによるCSMS実装に向けた投資は、自動車エコシステム内でどのように配分されていますか。





CSMSプロジェクトは、膨大なリソースを必要とするものの、コネクテッドな現代において自動車を販売するOEMにとって不可欠なものでもある。市場専門家は、規制による強制がなかったとしても、OEMはCSMS要件を満たすために莫大なコストを負担していただろう、と考えている。なぜなら、長期的に見て、安全な自動車だけが市場で成功を収めることができるためである。この意見に対するサプライヤーの見解は大きく分かれた（仮説1参照）。

図表16の数字は、自動車産業がエコシステムのほぼ全ての部分に投資する必要があることを示している。また、CSMSは車両ライフサイクルの全段階と統合する必要があり、非常に複雑で長期的なプロジェクトとなることも示唆されている。CSMSへの歩みを開始していない企業は、遅れを取り戻すべく多大な労力を費やすことになるだろう。

8.

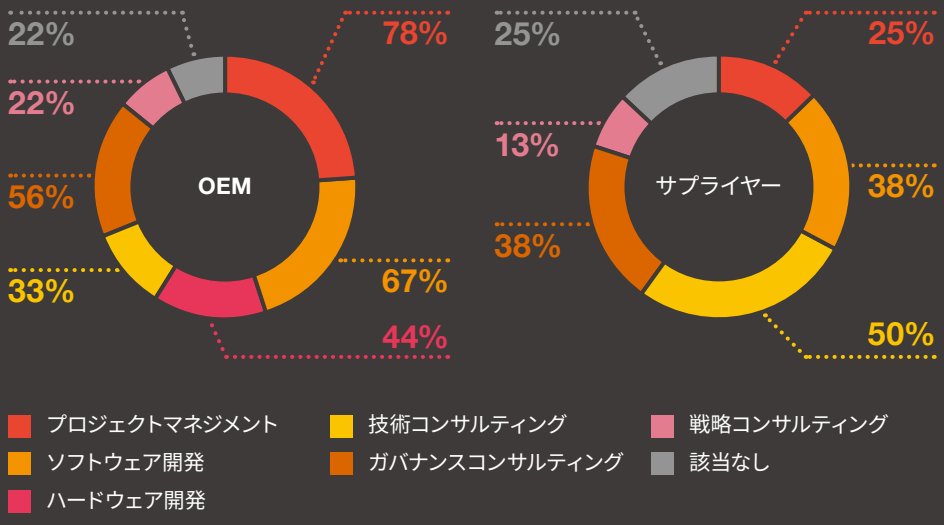
効果的なCSMSが競争上の大きな優位性をもたらす可能性

自動車産業の未来は、新技術を取り入れ、規制を見越した対応を図り、迅速に適応する企業に大きな機会をもたらすだろう。調査に回答した大部分の組織が、CSMSの歩みを加速させるために外部組織と協力している、と回答しているが、ここでもOEMとサプライヤーの間に違いが見られた。OEMのほぼ5分の4がサードパーティーによるプロジェクトマネジメントオフィス（PMO）の支援を活用しているのに対して、サプライヤーの同割合は4分の1にとどまっている。ソフトウェア開発におけるサードパーティーの利用も、サプライヤー（38%）よりOEM（67%）の方が多い。

効果的なCSMSの価値については、全ての回答者が概ね同意している。UNECE要件の影響を受けるOEMがCSMSを効率的に設計・運用できれば、他社に対する競争上の優位性を得ることができる。OEMの場合、89%が「サイバーセキュリティの成熟度の高さは、今後、車両を販売するうえでの明確な競争上の優位性となる」と回答し（仮説2参照）、3分の2が「コネクテッドカーと自動運転の発展によって従来の市場シェアは今後大きく変わる」と考えていることがわかった（仮説9参照）。

既存のサイバーセキュリティ能力は、特に現在の開発段階において重要な強み（Unique Selling Proposition、以下USP）である。特にサプライヤーは、まだ規制の直接的影響を受けていないため、こうした傾向が強い。しかし、CSMSのグローバルな基準が成熟し、標準化されれば、こうしたUSPは自動車サプライヤーとしてビジネスを行ううえでの基本要件となっていくだろう。

図表 17　ICSMS/CSMS要件の導入にあたり、サードパーティーによるサポートを最も多く利用しているのはどの分野ですか。



C 展望と結論

イノベーションは避けて通れない道

自動車部門の技術進化は日進月歩である。これによって、業界とその顧客はこれまでにない困難な脅威に直面している。企業が莫大なコストを背負う可能性、あるいは自動車の走行中に人命が失われる可能性すらある。

車両とその実行環境は、5G（および次世代以降の通信技術）、センサー精度の向上、光学画像処理、量子コンピューティングなどの開発により、大きな影響を受けることになるだろう。ここでカギとなるのはソフトウェアである。モジュール式かつスケーラブルなソフトウェアおよびコンピューティング能力を車載することにより、企業は長期的に見てコスト効率に優れた自動車の生産と運用を行うことができる。

対応には後押しが必要

政府や機関は、こうした技術イノベーションに対応すべく、より厳格な新規制や基準を打ち出す構えである。しかしこれまでのところ、これらの取り組みは非常に曖昧で、実際に規制の作成側が望むような保護を提供するには至っていない。ビジネス戦略に基づくスマートなサイバーセキュリティマネジメントによって、それを具体化し、競争上の優位性を獲得するのは、OEMの取り組み次第という状態である。

今回の調査では、OEMがすでにCSMSの設計を行い、初期対策に乗り出していることがわかった。幸先のいいスタートではあるが、これら対策の成熟度と対象範囲を改善していく必要がある。CSMSの歩みに関して、これまでサプライヤーはOEMに後れをとってきた。しかし双方ともに、CSMSを経営、コンプライアンス、ガバナンスシステムと統合する取り組みを進める必要があるだろう。

長く曲がりくねった道のり

CSMSプロジェクトは多くの新たな課題を伴うものであることは間違いなく、相当な時間と資金が必要である。ビジネスリーダーや上級マネージャーは、CSMSの重要性、そしてCSMSの先駆けとなる企業にはすばらしい競争上の優位性がもたらされる可能性があることを理解することが重要である。興味深いのは、回答者の間で、国連規則155号によって投資は必要となるが、より安全な車両につながる、という点で意見が合致していたことである。何はともあれ、この議論において「安全性とセキュリティ」が最重要であることは間違いない。

全体的に、自動車業界はコネクテッドカーに関連するサイバーセキュリティの脅威への対応について一貫性と透明性が欠如している。この業界では、技術の進展、規制、競争、顧客の期待事項などさまざまな影響をまとめる効果的アプローチを確立するには至っていない。新たな市場プレイヤーは、より合理的なバックエンドと技術体制を有しているかもしれないが、一方で、既存プレイヤーは、新しい規則への準拠という点で豊富な経験を有しているということもある。さらに、この調査のインタビューでは、販売組織の安全確保に注力している回答者が皆無であることが明らかになった。これはバリューチェーン全体をカバーできてはいないことの証左のひとつと言える。CSMSの統一基準や共通要件を設けることは、この分野の発展を促進するうえで非常に重要である。

CSMSに関する数値比較	OEM	サプライヤー
初期CSMSプロジェクトの進捗度	71%	59%
CSMSの推定成熟度レベル（0〜5）	Ø 2.1	Ø 1.2
CSMS評価を受けているグローバル競合他社の推定	43%	26%

提言

■ 規制を見越した対応
CSMSのプロジェクト期間は平均30カ月である。したがって、まだ対応に多くの期間を費やしていない企業は、あらゆる関連市場における今後の規制や契約上の要件を迅速に確認すべきである。OEMは結果重視のアプローチをとり、各国の認証当局が設けた評価仕様に常に準拠していくべきである。

■ 事業戦略の策定
大規模かつ複雑なプロジェクトは、たとえ規制上の観点から必要であったとしても、常に事業変革戦略に沿って進めていくべきである。

■ シナジーの追求
強いコスト的・時間的制約を踏まえて、シナジーを発揮するために既存のマネジメントシステムの仕組みを活用してCSMSを設計・実装していくべきである。これには、共通の解釈や市場の基準が確立されるまで、標準的なプロセスやツールを使用することで、複雑さやカスタマイズの必要性を回避することが含まれる。

■ 成熟度の向上
CSMSの成熟度を上げる必要がある。これには、社内での成熟度の測定と報告だけでなく、バリューチェーンのビジネスパートナーの成熟度の測定と報告も含まれる。リスクの特定は多くの参加者にとって有効であるが、経営的な観点からも、そうしたリスクを抑制可能なものにすることが重要である。

■ 実用性試験
CSMS設計後、企業はトライアルを実施し、CSMSが効果的に機能するか、運用においてリソースの削減につながるか、検証すべきである。

■ ソフトウェアを最優先
カギとなるのはソフトウェアである。ソフトウェアアーキテクチャの明確な要件を定め、自社のバリューチェーンに適用することにより、OEMの安全な統合とサプライヤーソフトウェアを確保すべきである。

CSMSに向けて今こそアクセルを踏み込むべき

OEMは、自社のポジショニングと製品ポートフォリオについて戦略的決定を下していく必要がある。国連規則155号および156号がその足がかりとなるだろう。しかし、それでも十分ではない。全ての市場をカバーし、全ての法律分野を考慮に入れた、より具体的なガイドラインが必要である。現在、主要な自動車市場にはさまざまな規制が存在し、要件が一部異なるものもある。したがって、OEMは開発段階において、製品やエコシステムの対象地域・市場を決定しなければならない。そのため、汎用製品の開発に頭を悩ませる企業もあるだろう。しかし、効果的な意思決定により、十分なスケーラビリティを維持できれば大きな競争上の優位性を得ることができる。

今後、道路車両のエコシステムが大幅に拡大することは間違いない。顧客の期待も高まっていくだろう。また、TVストリーミングからリモートワークまで、他企業のサービス提供スペースとして車両を位置付け、そこから生まれる可能性を積極的に探っている企業も存在し、そうした企業にとって、より魅力的な事業機会が生まれている。この価値あるエコシステムを守るのは効果的なCSMSであり、したがって、複数の観点から見て、CSMSはビジネスの命運を左右する課題である。

CSMSは世界の多くの市場で登録・生産される自動車の基本的要件であり、今後もそれは変わらない。コンプライアンス要件違反は、車両生産ライセンスの取り消しや、罰金の恐れ、大規模な法的紛争につながる可能性がある。

さらに、継続的なサイバーセキュリティ運用は、車両コストに大きな影響をもたらす。今後、ライフサイクル全体にわたり自動車エコシステムをいかにコスト効率良く運用できるか、そのカギとなるのは、モジュール型のスケーラブルなソフトウェアアーキテクチャを組み合わせたスマートCSMSである。

最後に、CSMSが守るのは人々の命だけではない。新たな生活・仕事の場となりつつある自動車を中心に拡大するデータ主導・サービス主導型ビジネスモデルや、今後の大きな収益基盤をも守るものである。

コースはすでに目の前に広がっている。この市場で成功を収めようとする企業は、自動車の変革ペースに後れをとってはならない。

大局的に見れば、セキュアかつ効率的な自動車エコシステムの実現は、長く曲がりくねった道のりである。ゴールにたどり着くためには、チームワーク、スピード、そしてナビゲーションスキルが必要となるだろう。

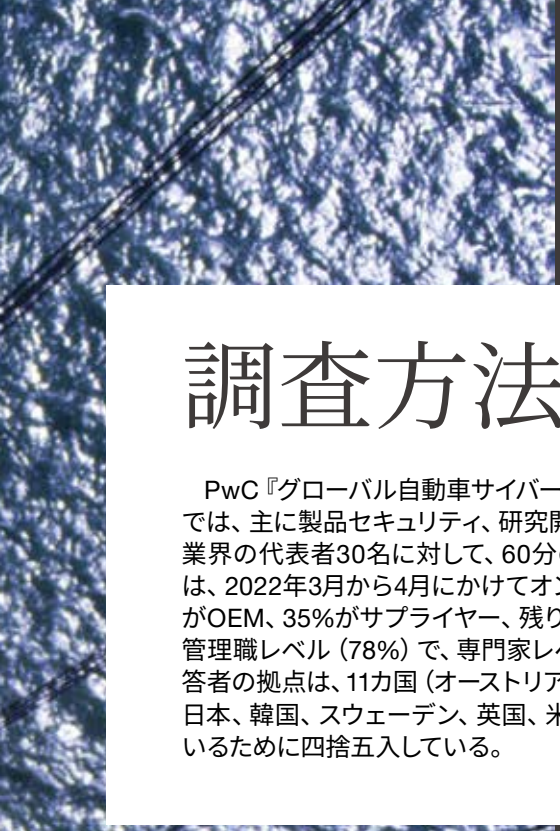
おわりに

車両のコネクテッド化や自動運転の実現など、車両の未来は社会が求める新しい価値です。このような新しい価値をもたらす自動車の登場は、人々や社会をより豊かにするでしょう。一方で、これら車両の実現には、従来の車両開発で利用していたテクノロジーだけでなく、IT業界で活用されているような最新技術の利用も必要であり、結果として、サイバーセキュリティリスクをもたらす要因ともなっています。

本レポートが明らかにしたように、CSMS構築を中心とした自動車サイバーセキュリティは、国連法規の適用などを背景に、各社の対応が加速しているものの、未だ課題も多く、継続的な推進が必要な状況にあります。課題の背景の1つには、自動車におけるソフトウェア適用の拡大があります。販売後のインシデント対応や脆弱性管理など、従来ITソフトウェア会社が得意としてきた領域の施策についても、自動車関連会社に新たに求められる要因となっています。また、OEMとサプライヤーにおける施策準備の差は、2021年の実態調査時点と同様に存在しており、引き続きサプライチェーン全体でのセキュリティ施策の実施および成熟度向上が求められています。

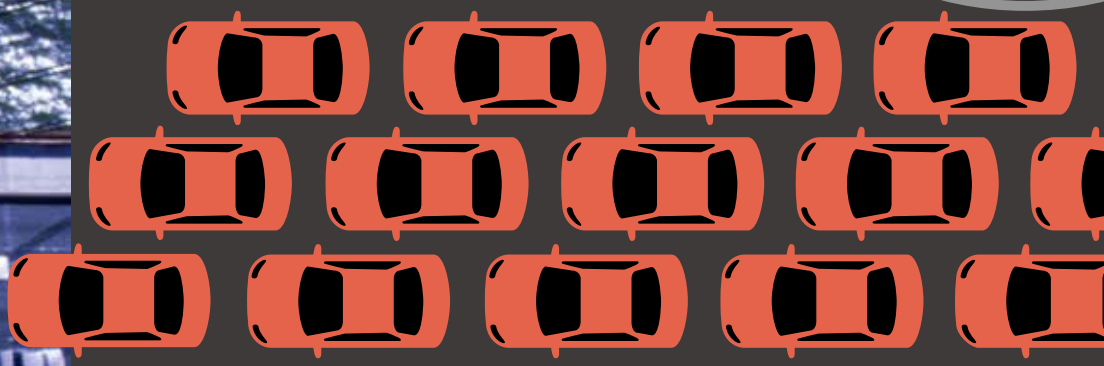
これらの課題の解決には、ある1つの企業での施策実施だけでは達成しえない状況にあるといえます。多数のソフトウェアが、サプライチェーン全体で利用されているのであれば、利用する各社が協調しあってセキュリティ対策をしなければ最終製品の品質は確保できないためです。同様に、自動車のサイバーセキュリティ対策の最新情報を1社独力で収集し対応することは、サプライチェーン全体のセキュリティ品質向上には、効果的でも効率的でもありません。

このような状況においては、日本の自動車業界全体が一丸となって最新のサイバーセキュリティ情報を共有し、今後必須となる最先端の活動を協調して進めていくことが必要になります。本レポートの内容が、これから自動車業界全体で必要となる施策実行の参考となり、業界でのセキュリティ施策実行の一助となれば幸いです。



調査方法

PwC『グローバル自動車サイバーセキュリティマネジメントシステム（CSMS）調査』では、主に製品セキュリティ、研究開発、品質保証、情報セキュリティを担当する自動車業界の代表者30名に対して、60分の半構造化インタビューを実施した。インタビューは、2022年3月から4月にかけてオンラインアンケート形式で実施した。回答者の39%がOEM、35%がサプライヤー、残りの26%が市場専門家であった。回答者の大部分が管理職レベル（78%）で、専門家レベルが13%、一般スタッフレベルが9%であった。回答者の拠点は、11カ国（オーストリア、チェコ、フィンランド、フランス、ドイツ、イタリア、日本、韓国、スウェーデン、英国、米国）に及んだ。なお、データは匿名化し、図表で用いるために四捨五入している。



お問い合わせ

PwCは、自動車業界の企業にとって信頼できるパートナーです。クライアントと大きなトレンドに関する知識を共有するとともに、今後直面するであろう課題への備えを支援しています。PwCの部門横断チームは、重要な課題に対して革新的かつ持続可能なソリューションを迅速に特定し、実行に移します。また、グローバルな視点とローカルの法的知識を組み合わせることで、刻々と進化する顧客の要求にクライアントが応えていくための道筋を示します。

PwCはクライアントと手を携え、この道の先にどのような未来が待ち受けていようとも、クライアントのビジネスが確実に立ち向かえるよう支援します。

Harald Wimmer
Global Automotive Leader
Partner, PwC Germany
Tel: +49 221 2084-240
harald.wimmer@pwc.com

Joachim Mohs
Global Industrial Manufacturing and Automotive, Cybersecurity and Privacy Leader
Partner, PwC Germany
Tel: +49 040 6378-1838
joachim.mohs@pwc.com

以下のサイトにアクセスしてより詳細な情報を入手するとともに、皆さんにとって重要なポイントをご相談ください。

Global Automotive:
www.pwc.com/gx/en/industries/automotive.html

Global Cybersecurity:
https://www.pwc.com/gx/cybersecurity

日本のお問い合わせ先

PwC Japanグループ
www.pwc.com/jp/ja/contact.html

PwCコンサルティング合同会社

林 和洋
上席執行役員 パートナー
サイバーセキュリティ&プライバシー
リーダー

奥山 謙
サイバーセキュリティ&プライバシー
ディレクター

村上 純一
サイバーセキュリティ&プライバシー
ディレクター

亀井 啓
サイバーセキュリティ&プライバシー
マネージャー

私たちについて

私たちのクライアントは、さまざまな課題に直面し、新しいアイデアの実現に努め、専門的アドバイスを必要としています。そして、PwCに対して、最大の価値を提供する包括的サポートと実践的ソリューションを求めています。PwCは、グローバル企業、ファミリービジネス、公共機関などあらゆる組織に対して、私たちが誇るあらゆる資産―豊かな経験、業界知識、高い品質基準、イノベーションへのコミットメント、156カ国に及ぶ専門家ネットワークのリソースなど―を活用します。特に重要なのは、クライアントとの信頼・協力関係の構築です。クライアントのニーズをより深く学び、理解するほど、より効果的にクライアントをサポートすることが可能になります。

PwC Germany: 21の拠点に12,000人以上の正規社員を擁しています。売上高は24億ユーロ。ドイツを代表する監査・コンサルティングファームです。

www.pwc.de/auto-csms-survey

www.pwc.com/jp

本報告書は、PwCメンバーファームが2022年5月に発行した『Pedal to the Metal – How to Navigate the Way to Automotive Cybersecurity』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
オリジナル（英語版）はこちらからダウンロードできます。https://www.pwc.de/en/cyber-security/global-automotive-cyber-security-management-system-survey.html
日本語版発刊年月：2022年11月 管理番号：I202207-02