WP29 サイバーセキュリティ法規 CSMS対応の実態調査

PwCコンサルティング合同会社　シニアマネージャー　山田 素久

日本において、新型車に対し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の適用が求められる2022年7月まで1年を切りました。既に対応を終えてプロセス通りに開発を進めている企業がある一方、急ピッチで準備を進めている企業もあることでしょう。PwCコンサルティング合同会社では、日本の完成車メーカー（以下、OEM）および部品メーカー（以下、サプライヤ）の各社に対しWP29 サイバーセキュリティ法規に基づくCSMS（Cyber Security Management System）への現在の対応状況について調査を実施しました。本稿では、その調査結果について解説します。

調査概要

項目	内容
目的	■ 日本におけるWP29 CSMS対応状況を明らかにする ■ 車両サイバーセキュリティ業務に携わる方へ有益な参考情報を提供する
調査方法	Webによるアンケート
調査対象	OEMおよびOEMに部品を提供しているサプライヤに所属しており、WP29 CSMS対応に関与している方々
調査期間	2021年6月
回答者	101名（OEM：40名、サプライヤ：61名）

＊本稿にはアンケート回答者による私見や経験に基づく内容が含まれており、またアンケートを通じて得られた情報をもとに本稿を執筆したPwCによる見解および考察が含まれています。

OEM回答者の80%がCSMS対応に着手するも、サプライヤ回答者は49%にとどまる

各社のCSMS対応状況を調査した結果、全体の回答者のうち20.8%が「既に完了した」、40.6%が「現在実施中」と回答し、約6割が既に着手していることがわかりました。

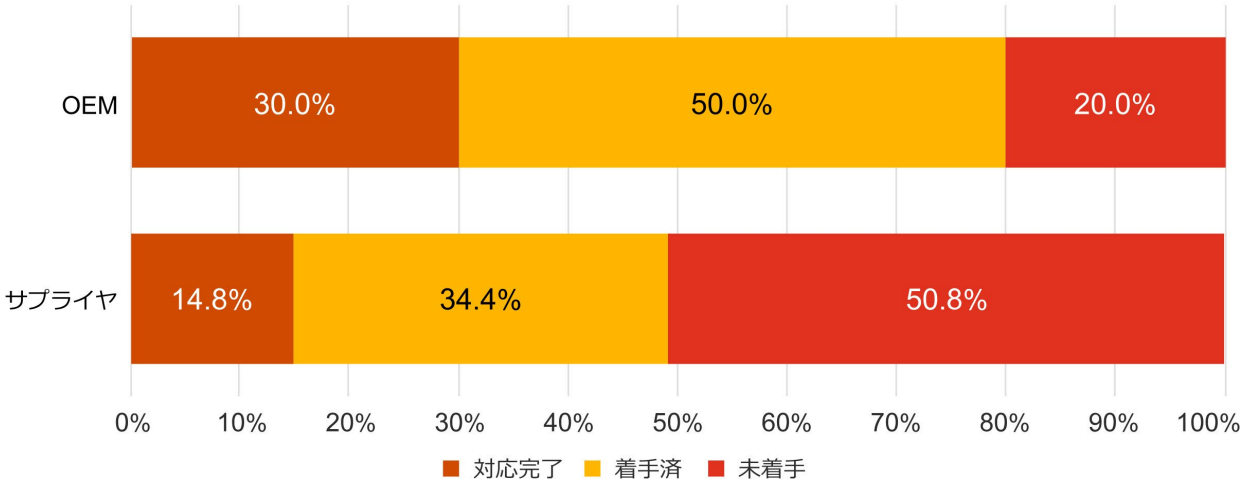
回答者をOEMとサプライヤに分けて分析すると、OEM回答者の80%は既に準備に「着手済」、または「対応完了」としている一方で、サプライヤ回答者は合わせて49%にとどまっています。今後の予定については、2022年7月までに完了させる予定との回答は全体で47.6%にとどまりましたが、全車種に対して法規が適用される2024年7月までに対応を完了する予定との回答は95%に上りました（図表1参照）。

OEMとサプライヤの回答者を比較すると、OEM回答者の60%が2022年7月までに完了させる予定であるのに対し、サプライヤ回答者では37%にとどまりました。

注目すべきは対応の遅れです。新型車へのCSMS対応が求められる2022年7月まで1年を切った現時点でも、OEM回答者のうち対応を完了していると回答したのは30%、現在対応中と回答したのは50%に留まりました。2022年7月から法規制が適用されるのは無線によるアップデート機能を持った新車だけであることから、新車の発売計画に応じて対応計画も策定しているとみることもできますが、一方で全社的なプロセス構築やサプライヤの管理に苦慮しているとも考えられます。

一方、サプライヤはさらに対応が遅れている実情が見て取れます。扱う製品によってはまだOEMから正式な対応を依頼されていないサプライヤもあり、今後型式認証を取得する必要がある新車の開発が進むにつれ、サプライヤの対応への要求も強まるでしょう。

図表１：CSMS対応状況

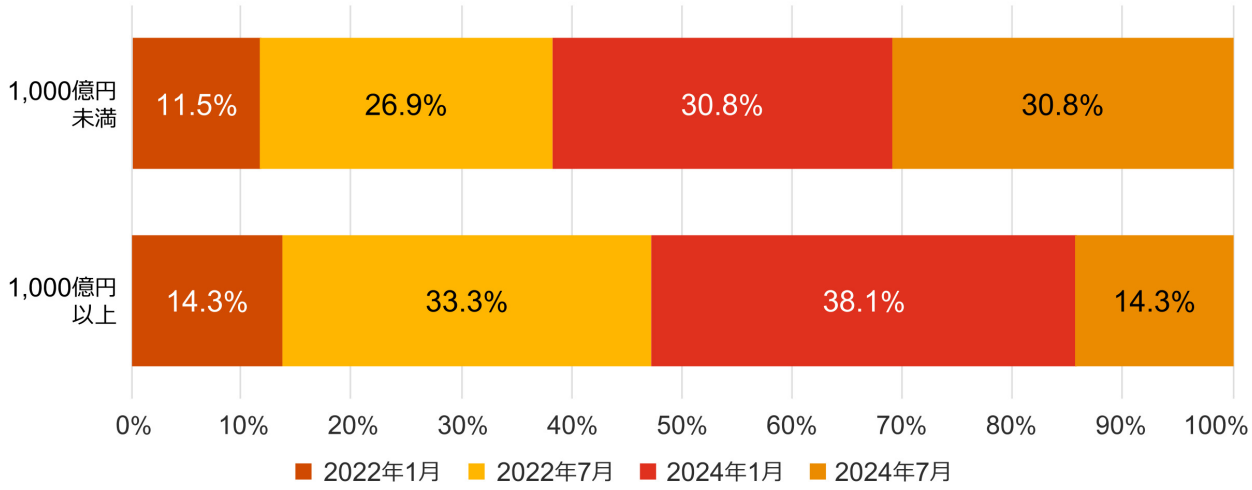


サプライヤの中でも、売上1,000億円以上の企業と1,000億円未満の企業を比較すると、1,000億円以上の企業に所属する回答者の59%が2022年7月までに対応を完了する予定であるのに対し、1,000億円未満の企業に所属する回答者では34%にとどまりました（図表2参照）。

また、サプライヤを扱う製品別に比較すると、電装系（電子電装系＜パワトレ／車体＞、カーナビ、ラジオなど）の部品を扱う企業に所属する回答者の55%が2022年7月までに対応を完了する予定である一方、他の部品（エンジン／パワトレ系部品、懸架／制動装置、車体部品など）を扱う企業に所属する回答者では31%にとどまっています。

これらのデータから、中小企業が対応に苦慮していることや、扱う製品によって対応を決めかねている実情をうかがい知ることができます。

図表２：売上規模別サプライヤCSMS対応完了予定



全社的な対応推進部門が必要不可欠、OEMはサプライヤの巻き込みに苦慮

WP29は開発や生産、運用など製品のライフサイクル全般への対応が求められるため、もれなく行うためには部門ごとの活動では限界があり、全社的な体制づくりが不可欠になります。

各企業が実際にどのような体制でWP29の対応を進めたかについての設問には、48.5%がCSMS対応を統括・推進する部門があると回答し、特に57.5%のOEMでは特定の部門が主導する形で活動を推進している実態が明らかになりました。具体的に統括・推進する部門としては、OEMでは「法務またはコンプライアンス部門」が47.8%と最も多かったのに対し、サプライヤでは「情報システム部門」が最多の43.3%でした。

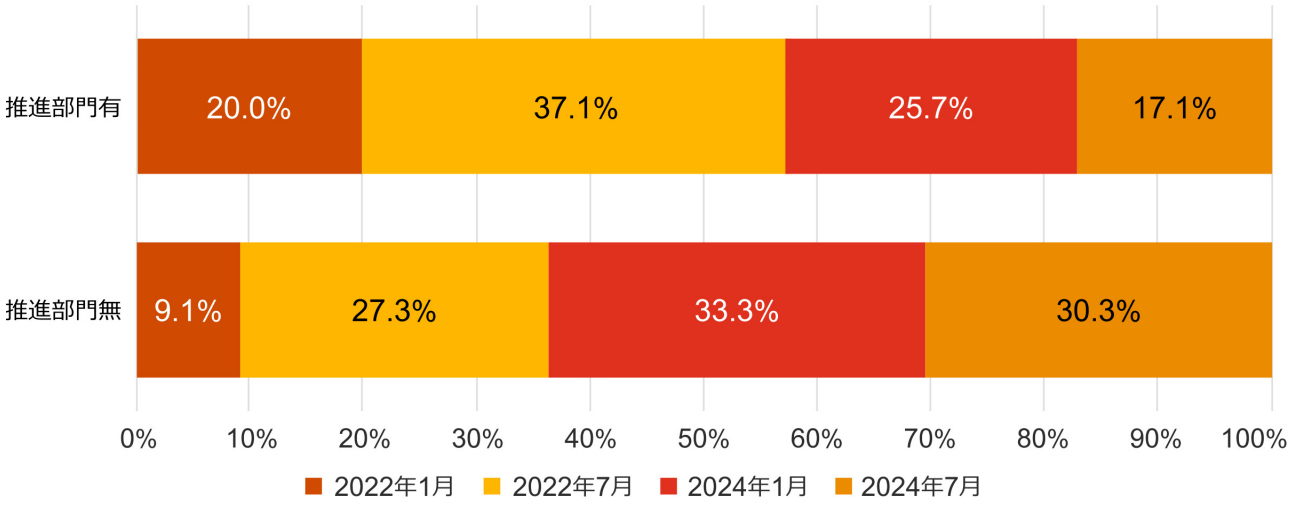
CSMS対応を推進する部門の有無と対応完了時期の関係については、推進部門がある企業のうち2022年7月までに完了予定であると回答したのは57.1%だったのに対し、推進部門が無い企業は36.4%にとどまり、全社的な推進体制の有無が完了時期に大きく影響していると推察されます（図表3参照）。

この結果は、CSMS対応の推進にあたって、全社的な体制の構築が重要であることを如実に表わしています。大企業であるOEMで全社的な体制を構築することは非常に難しく、情報セキュリティと製品セキュリティを含む、サイバーセキュリティのガバナンス体制の見直しにもつながるため、大きな課題であると考えられます。

対応推進部門については、OEMにおいては、法務・コンプライアンス部門が全社的な業務を担う組織であることから、その責任を担ったものと推察できます。一方でサプライヤでは、最もサイバーセキュリティに知見のある情報システム部門がリードして対応を進めたのではないでしょうか。

CSMS対応プロセスの構築が完了しても、その後の運用を考えると、製品の監視組織であるV-SOC（Vehicle Security Operation Center）やインシデント対応体制であるPSIRT（Product Security Incident Response Team）の構築など、部門を横断する組織体制が必要となります。OEMやTier1サプライヤにとってはサイバーセキュリティガバナンス体制の構築は不可欠と言えるでしょう。

図表３：CSMS推進部門有無別CSMS対応完了予定



スキル不足は開発プロセスより生産・運用プロセスで実感、工場のセキュリティ人材不足がその要因

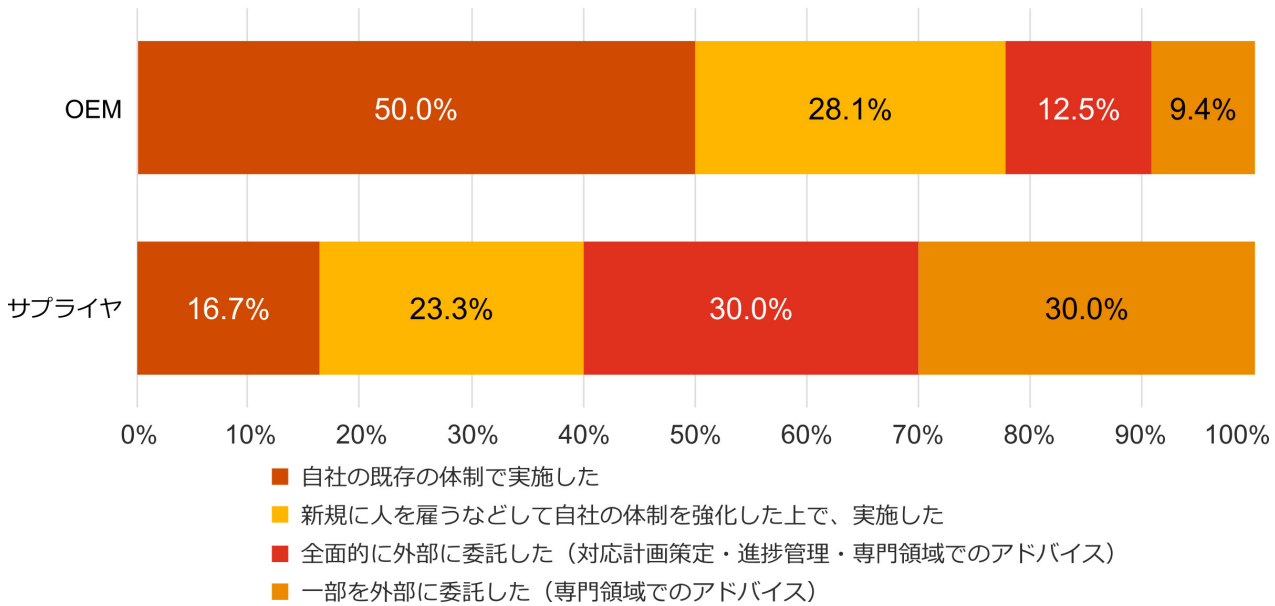
WP29対応には、サイバーセキュリティに関する知識やスキルが不可欠ですが、セキュリティに精通した人材は世界的に不足しており、各社とも必要なスキルや人材の確保に苦労していると推察できます。知識や人材の確保に関する設問では、全回答者の66.2%が人材の「新規採用」（25.8%）か「外部委託」（40.4%）で対応を進めていました。また、OEMとサプライヤを比較すると、サプライヤの60%が外部に協力を依頼していたのに対し、OEMでは21.9%にとどまり、自社内で対応を進めている状況がうかがえます（図表4参照）。

前述の通り、本調査では25.8%が人材を新規で採用することでWP29への対応を進めたと回答する一方で、多くの企業が外部委託により対応している状況が明確になりました。その傾向は特にサプライヤにおいて顕著であり、増員する余裕がないことや、現状、自社の業務に製品のセキュリティ対応を追加することが難しいことなどにより、外部に委託せざるを得ない状況であると考えられます。

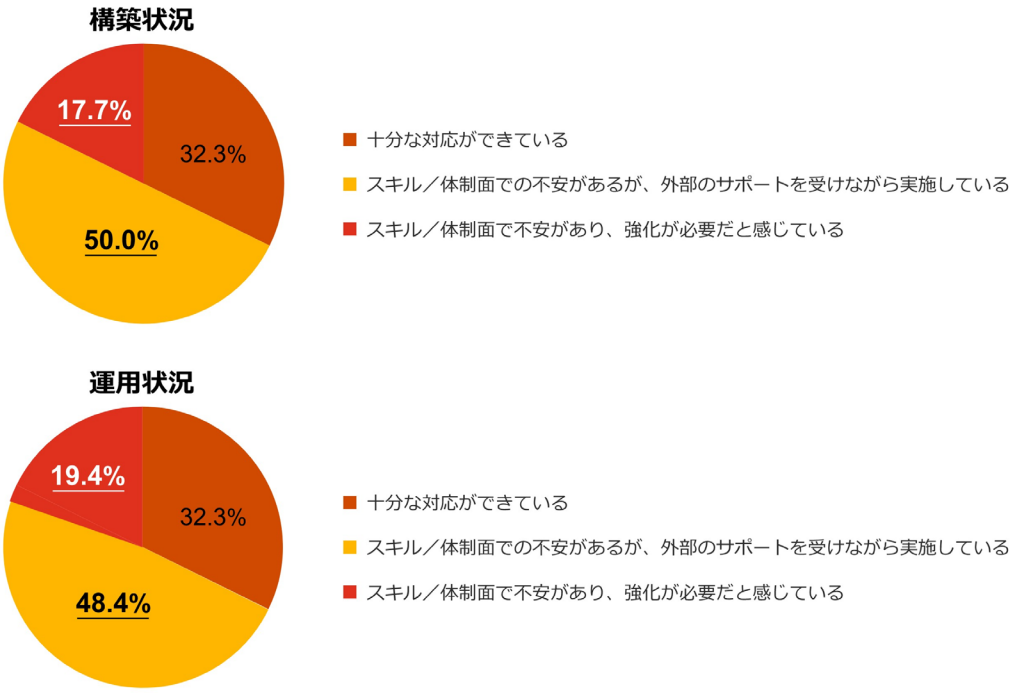
対応を進めている企業でも、「十分な対応ができている」との回答は32%にとどまり、多くの企業がスキル・体制面で不安を抱えながらプロセスの構築・運用を行っている実態が浮き彫りになりました。「十分な対応ができている」と回答した企業の60%は「自社の既存の体制で実施した」と答え、2017年以前からCSMS対応を開始しているケースも一定数あることがわかりました。十分に準備ができている企業は、対応に自信を持っているのでしょう（図表5参照）。

広範にわたるサイバーセキュリティの知識を一朝一夕に身に着けることは難しく、継続的に社内教育などにより社員のスキルを向上させていく必要があります。調査でも50.5%の企業が「CSMS対応活動の推進のため社内教育を行った」と回答しており、今後もセキュリティの専門家を育成するだけでなく、開発などの実務担当者向けの教育を行っていく必要もあります。

図表４：CSMS対応に必要な知識・人材確保方法



図表５：CSMSプロセス構築・運用状況



法規制や脅威についての幅広い情報収集・活用・選別が大きな壁

次に、各社がCSMS対応に向け、どういった方法で必要な情報を得ているかを見ていきます。調査によると97%がWP29法規制以外にも参照した情報があると回答し、77%が2つ以上の情報を参照しています。特にISO21434は74%が参照しており、実際の法規制対応に活用されていることがわかりました。ISO15504を基にした「Automotive SPICE®」や、OEMがサプライヤなどに自社の重要データを含む情報資産に関するセキュリティの確保を求める「TISAX（Trusted Information Security Assessment Exchange）」なども一定程度（15%～20%程度）参照されていました。各社ともさまざまな情報を参考にし、試行錯誤しながら対応を進めている状況が見て取れます。

一方、売上高1,000億円以上の企業に所属する回答者のうち66.1%がベンダー、業界団体、公開情報などをソースとして「情報源が2つ以上ある」と回答したのに対し、1,000億円未満の企業に所属する回答者の75%が「単一の情報源から情報を得ている」と回答しています。また、脅威情報の入手については、売上高1,000億円以上の企業に所属する回答者の73%が「業界団体から入手する」と回答したのに対し、1,000億円未満の企業に所属する回答者は54%にとどまり、業界団体から距離がある様子でした。

技術が共通化され、コモディティ化しているIT業界とは異なり、サイバーセキュリティのさまざまな規格や独自の実装が今も多い自動車業界は、幅広い情報源から自社の製品に関連する情報を収集、選別し、活用できるよう整形する必要があります。しかし、中小企業の情報源は限定されており、自社で情報を収集し、選別しようにも人的リソースが不足しているとみられます。情報を発信している業界団体からの情報入手も大企業と比べ進んでいません。安心・安全なクルマを製造し続けるには、自動車業界全体でサイバーセキュリティに対応する必要があります。今後、中小企業に対する業界横断的な支援、そして国を挙げての支援が重要になるでしょう。

CSMS対応プロセス構築後の全社推進が課題、VSOCやPSIRTなど部門を超えた体制整備

CSMS対応の実施にあたって大きな課題となるのが、必要なスキルとコストであることは明白です。具体的にプロセス上のどのような点に各社が課題を感じているのかについて考えていきます。

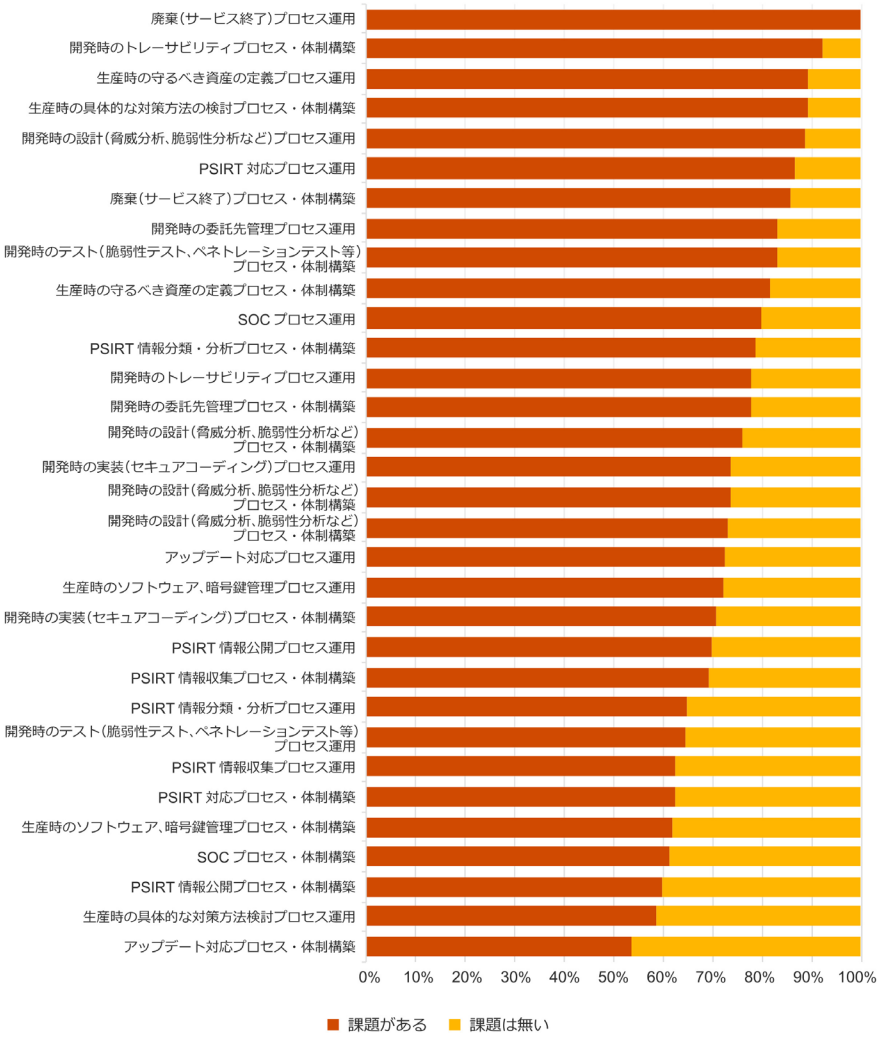
まず、「スキル面に課題がある」という回答のうち、課題がある具体的なスキルとして特に多かったものとして、「開発プロセスにおけるトレーサビリティの確保」(92.3%)、「生産プロセスにおけるセキュリティ対策」(89.5%)、「生産プロセスにおけるサプライチェーンのセキュリティ対策」(88.9%)、「運用プロセスにおけるPSIRT運用」(86.7%)が挙げられます(図表6参照)。

スキルが不足していると感じられるプロセスは、開発よりも生産・運用のプロセスに多いことが調査結果から見て取れます。これまでネットワークから隔離されていた工場では、開発部門に比べセキュリティのスペシャリストが少なく、CSIRT(Computer Security Incident Response Team)はあってもPSIRT(Product Security Incident Response Team)はない企業が多いことが理由として挙げられます。

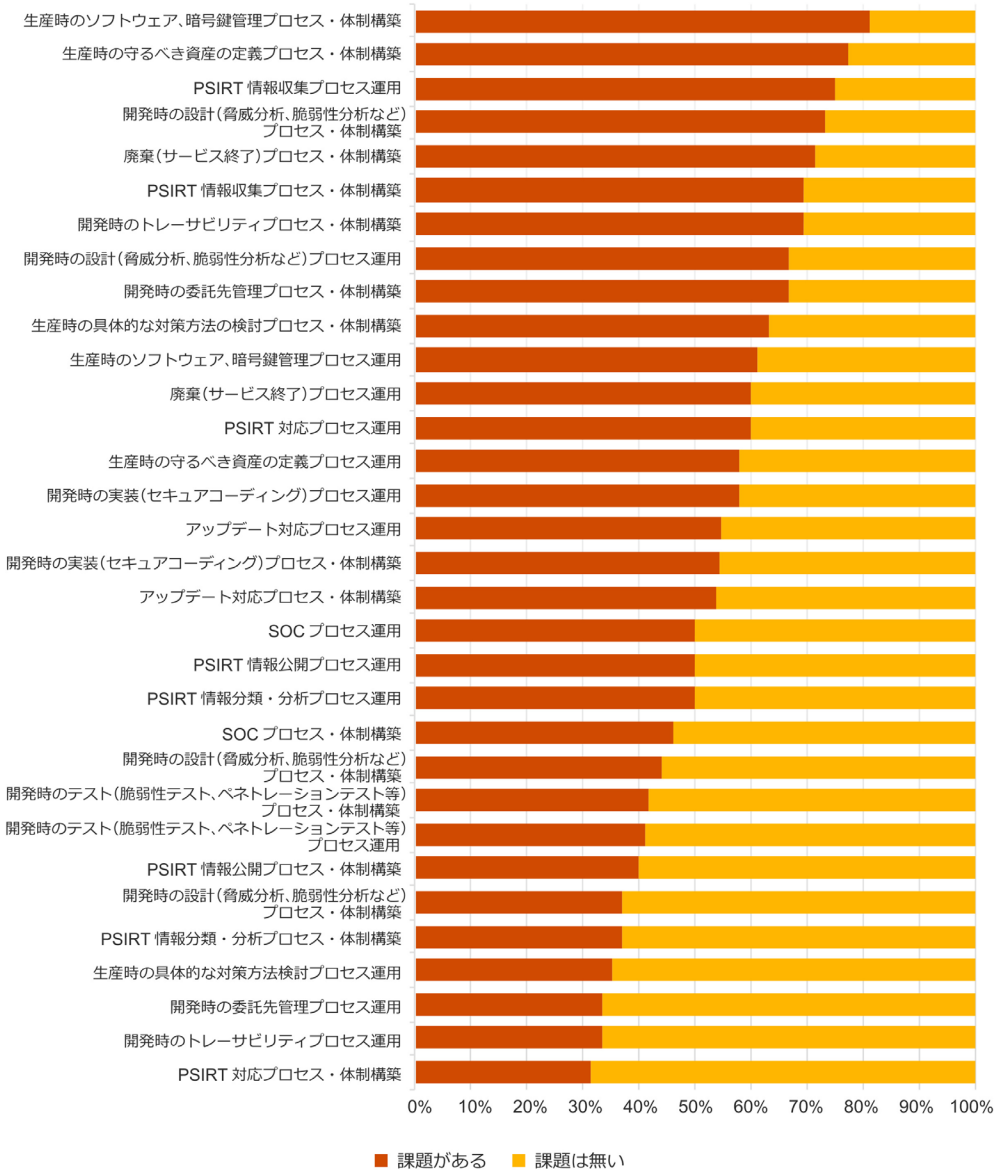
また、コスト面では「生産プロセスにおける暗号鍵管理」(81%)や、「守るべき資産の定義」(77.3%)などのほか、運用面では「サプライチェーンのセキュリティ対策」(73.3%)や「PSIRT情報収集」(75.0%)に対する課題意識が高いという結果が得られました(図表7参照)。一方で、実際にWP29対応に際しどの程度のコストを要したかの全体感については、50.5%の企業が「分からない」と回答しており、費用の正確な把握が困難であることが推察されます。

CSMS対応にはプロセス構築のための対応工数や外部への委託、分析およびトレーサビリティのためのツールの導入など、さまざまな費用がかかります。さらに実際の製品設計では、セキュリティのための追加機能の開発や、テストのためのコストも必要になります。対応プロセスを構築し、実際にそのプロセスに沿って開発を進めている企業は25%前後であることが明らかになりましたが、前述の通りCSMS対応にかかる費用は不透明で、今後の運用も踏まえ、どのように製品コストに転嫁するかをOEMやサプライヤは検討する必要があるでしょう。

図表６：CSMS対応にあたってスキル面で課題が多いプロセス



図表７：CSMS対応にあたってコスト面で課題が多いプロセス

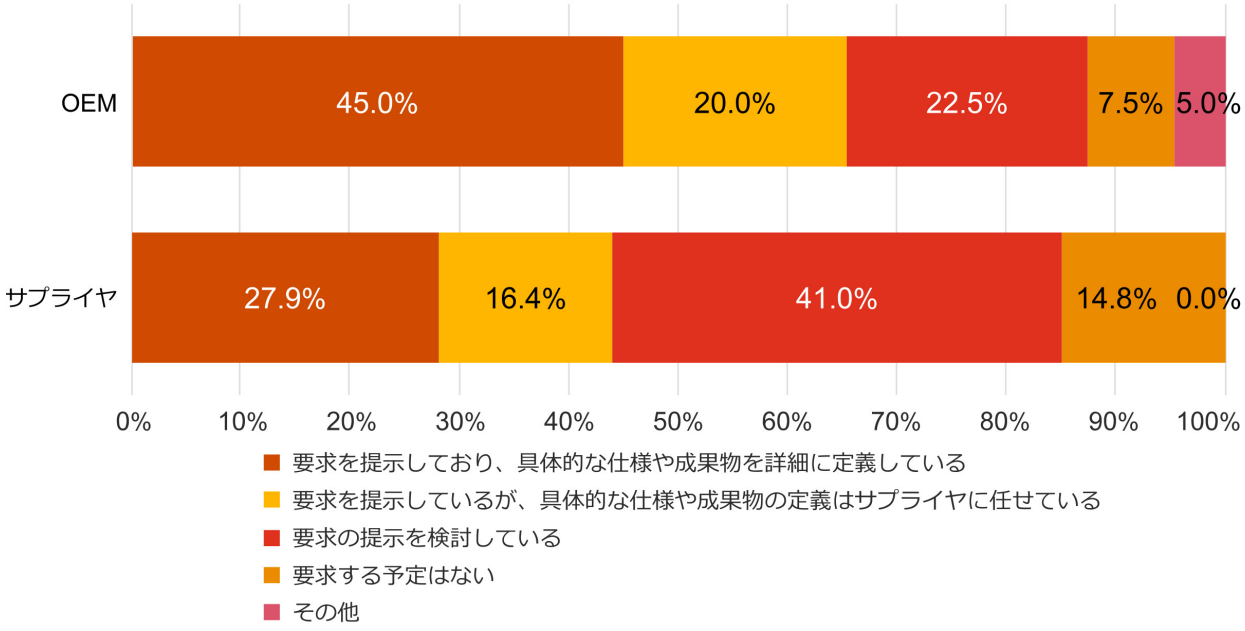


プロセス全般におけるサイバーセキュリティ対応を保証するためには、サプライヤの管理も大きなポイントの1つになってきます。実際にOEMや上流のサプライヤが、自社に製品を供給するサプライヤに対してどのように対応を要求しているのかという点を見ていきます。

まず、自社が発注先のサプライヤに対しCSMS対応要求を出しているかという点については、OEMとサプライヤで対応が明確に分かれ、65%のOEMが既に対応を要求しているのに対し、サプライヤは44.3%にとどまりました。また、OEMの62.9%が作成プロセスやエビデンスの提出を求めているのに対し、サプライヤは38%にとどまっています（図表8参照）。

裾野の広い自動車産業においては発注先サプライヤの管理は重要な課題であり、それはサイバーセキュリティに関しても同様です。OEMやTier1サプライヤが自社の製品を構成する部品を提供するサプライヤに対して、どのようにCSMS対応を要求するかについては、今後も試行錯誤が続くでしょう。DIA（Development Interface Agreement：開発協働契約書）によって役割分担を厳密に定めて開発を進めていく欧米諸国のOEMに比べ、日本のOEMとサプライヤは、すり合わせで要件を決め、ともに開発を進めていくため、責任の境界線があいまいになるというケースが散見されます。セキュリティにおいては、今後OEM／サプライヤ間で要求仕様やエビデンスについての明確化が行われていくものと考えられます。

図表8：自社のサプライヤへCSMS対応を要求しているか



調査結果を通じ、法規制に対し試行錯誤しながらも真摯に向き合い、対応を進めているOEM／サプライヤ各社の現状が明らかになりました。自動車におけるサイバーセキュリティは、人の命にかかわる可能性があることから極めて重要であり、厳密な対応が求められる分野です。一方で実際にどこまでコストと時間をかけて対応すべきなのか、判断に迷う部分もあるでしょう。その線引きに明確な答えは無いため、各社さまざまな法規やベストプラクティスを共有しながら対応しているのが実情です。

今後、サイバーセキュリティに関する情報を自社のみで収集し対応することはますます難しくなっていくと考えられます。日本の自動車業界が一丸となって情報を共有し、サイバー攻撃に立ち向かっていかなければならないのではないでしょうか。本稿がWP29の対応を推進する皆様にとって、現状を理解する一助になれば幸いです。

お問い合わせ

PwCコンサルティング合同会社
〒100-0004 東京都千代田区大手町1-2-1 Otemachi One タワー
Tel : 03-6257-0700（代表）　Email :　jp_cyber_inquiry@pwc.com

© 2021 PwC Consulting LLC. All rights reserved. PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.