CSMS を構築するための Automotive SPICE の活用について（山内）

7 月のメルマガではサイバーセキュリティと Automotive SPICE に関する最新動向をお伝えしましたが、今回は CSMS（サイバーセキュリティ管理システム）の構築についての考慮点をライフサイクル、プロセス構築、プロセス認証の観点で説明するとともに Automotive SPICE の活用をご紹介いたします。

まず、ライフサイクルですが、ISO/SAE DIS 21434 では開発、生産、生産後の運用・保守、廃棄までが対象となります。特にサイバーセキュリティは生産後の運用・保守の段階においてもセキュリティ資産に対する新たな脆弱性が発見された場合の対応をしなければなりません。これには、サプライヤーおよびサービスプロバイダーとの間に存在する可能性のある依存関係の考慮を含みます。この事から車両開発プロジェクト完了で終わりではなく、OEM とサプライヤーの連携による継続的な保守がサイバーセキュリティ対応として求められることが分かります。

次にプロセス構築ですが、ISO/SAE DIS 21434 では、組織、プロジェクトの管理に関する要件が記載されています。これは Automotive SPICE では、能力レベル 2 （プロジェクトレベル）だけではなく、能力レベル 3（組織レベル）でのプロセス構築が必要となることを意味しています。当然、プロセスとしては、セキュリティに関するリスクや脅威、脆弱性の特定と評価を行い、それぞれに対する軽減策を検討、実施することが求められ、組織としてセキュリティに対する説明責任を果たす必要があります。この事から、CSMS を構築する際は、組織レベルで運用可能なプロセスおよび体制を構築する必要があります。

最後にプロセス認証ですが、OEM は認証当局によってプロセス認証を受ける必要があります。その際に OEM は、サイバー攻撃から自動車を守るためにサプライヤーも含めた CSMS を構築し、セキュリティ対策が盤石であることを証明する必要があり、OEM、Tier1、Tier2 などにおける各々の作業範囲の役割と責任を明確し、発注者と受注者を管理することが重要といえます。

上記 3 つの考慮点を踏まえると CSMS を構築するためには発注者と受注者の役割と責任の明確化、その内容に対する契約がポイントとなることが言えます。Automotive SPICE では発注者が受注者を管理する上で、一般的に「ACQ.4:サプライヤー監視プロセス」が参照されることが多いのですが、ACQ.4 に関する活動の前提となる「ACQ.3 ： 契約と合意プロセス」が契約に関する内容となります。

ACQ.3 のプロセス目的は、“サプライヤーと契約／合意を交渉し、承認すること”であり、さらにプロセス成果は、“サプライヤーおよび発注者の両者の期待事項、責任、作業成果物／納入物、および責務が、明確かつあいまいさを残さずに契約書／合意文 書に明示されている”と規格には記載されています。この事から ACQ.3 は CSMS を構築する上で OEM,Tier1、Tier2 の役割責任を明確にし、その役割を合意し契約するためのプロセスを構築するためのヒントとして、大きく活用することが出来ますのでこの機会に参照していただければと思います。

弊社では、今回ご紹介した CSMS の構築に関する内容の詳細や事例紹介、サイバーセキュリティの最新動向について 11 月 25 日の【無償】自動車サイバーセキュリティセミナーを実施いたします。ご興味がある方は是非セミナーへお申し込みください。

2020/10/23 山内 誠