車載半導体製品のサイバーセキュリティ対応

東芝デバイス&ストレージ(株)

自動車業界が目指すCASE※1に加え、先進国を中心に MaaS※2が推進されるなど、自動車のモビリティーサービスへの変革と機能のソフトウェア化が進む中、車載E/Eシステム※3のサイバーセキュリティ対策の強化は喫緊の課題です。この課題に対応するために、国連により車両向けサイバーセキュリティ法規(UN Regulation No.155(以下、UN-R155)、No.156(以下、UN-R156))が発効されました。当該法規は、自動車メーカーによる車両の型式認定取得のためにCSMS(Cyber Security Management System)およびSUMS(Software Update Management System)認証を求めており、半導体サプライヤーもまたCSMS、SUMS準拠を示すエビデンスと管理方法の説明が求められます。

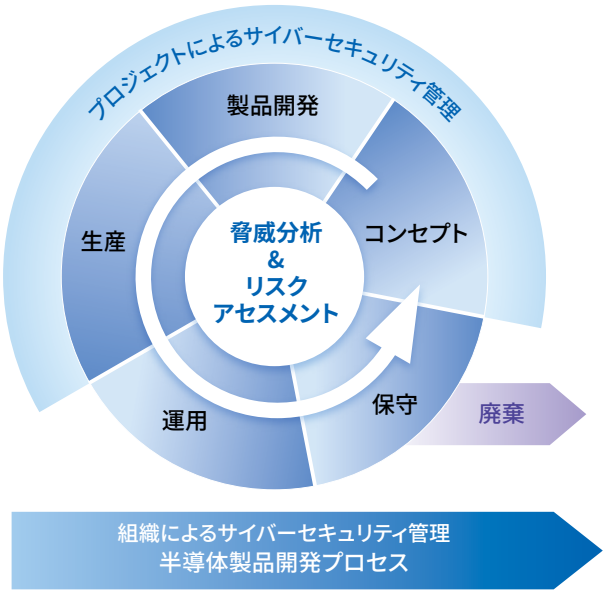
CSMS準拠は、大部分が車載サイバーセキュリティエンジニアリングの国際標準であるISO/SAE 21434に準拠することで達成できます。同標準は、下図(「ライフサイクル全体のサイバーセキュリティリスクの管理」)に示す製品ライフサイクル全般を通じて、持続的なセキュリティの実現に必要な手順を定義しています。一方でSUMS準拠もまた、大部分が車載ソフトウェアアップデートエンジニアリングの国際標準であるISO 24089に準拠することで達成できます。同標準は、下図(「ソフトウェアアップデートリスクの管理」)に示す一連のソフトウェアアップデート活動に関して、ソフトウェアアップデートにおける完全性・真正性の担保に必要な手順を定義しています。

当社は、ISO/SAE 21434並びにISO 24089に対応した社内規定および開発プロセスを整備し、当社が供給するパワートレイン、セーフティー、ボディー系等の車載E/Eシステム向け半導体に対して、製品ライフサイクル全体に対するCSMS、SUMS準拠性を担保することで、自動車の継続的なセキュリティリスクマネジメントに貢献しています。

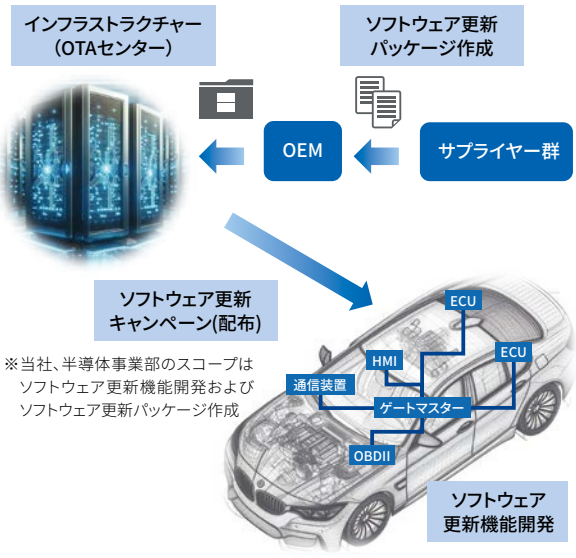
開発プロセスについては、既存の開発プロセスであるISO 9001をベースとし、IATF 16949並びにAutomotive SPICE®に基づく車載用ハードウェア・ソフトウェア品質管理プロセス、ISO 26262に基づく機能安全管理プロセス、これらにアドオンする形でISO/SAE 21434並びにISO 24089に基づくサイバーセキュリティ管理プロセス※4を実装することで、開発プロセスにおけるシームレスなサイバーセキュリティ対応を実現しました。また、継続的なセキュリティ脅威の監視やソフトウェアアップデートを含むインシデントへの対応は、東芝グループのCSIRT/PSIRT活動と連携することで実現しました。この開発プロセスは外部機関による規格準拠性評価を受け、当社は証明書を受領しています。

当社は継続的に本開発プロセスを用いた車載向け半導体製品開発を行い、自動車システムを常に最新でセキュアな状態に維持することをサポートする半導体製品を提供していきます。

※1 CASE(Connected, Autonomous, Shared, Electricの頭文字を取った造語)
自動車メーカーがモビリティーサービスプロバイダーへの変革を目指した中期戦略として使用している
※2 MaaS(Mobility as a Service)ITを活用して、従来の公共交通機関に加えライドシェア、シェアサイクルなどをシームレスに結びつける次世代の移動サービス
※3 車載E/Eシステム(Electrical/Electronicの略称、自動車の電気電子システム)
※4 ISO24089関連については、半導体事業部の範囲外のプロセス(「インフラストラクチャレベル」と「ソフトウェア更新キャンペーン」)には非対応
Automotive SPICE® は、Verband der Automobilindustrie e.V. (VDA)の登録商標である。



ライフサイクル全体のサイバーセキュリティリスクの管理



ソフトウェアアップデートリスクの管理