CASE時代のモビリティーサービスを支える半導体サイバーセキュリティーエンジニアリング技術

Cybersecurity Engineering Technologies for Semiconductor Products Supporting Mobility Services in CASE Era

伊藤　佑一 ITO Yuichi　　早乙女　一郎 SAOTOME Ichiro　　高橋　清紀 TAKAHASHI Kiyonori

自動車業界では，CASE（Connected, Automated, Shared & Service, Electric）と呼ばれる次世代モビリティーサービスへの変革が進められている。この中で，車載E/E（Electrical/Electronic）システムのサイバーセキュリティー強化が重要視されている。

東芝デバイス＆ストレージ（株）は，“自動車-サイバーセキュリティエンジニアリング” ISO/SAE 21434（国際標準化機構規格／米国自動車技術者協会規格 21434）[1]と “自動車–ソフトウェア更新エンジニアリング” ISO 24089[2]に準拠した半導体サイバーセキュリティーエンジニアリング技術として，機能安全と両立を図る際に生じる手戻りを軽減するサイバーセキュリティーの要求決定手法，車両中の半導体レベルの脆弱（ぜいじゃく）性を分類して特定する手法，並びに運用フェーズのソフトウェア更新をセキュアに実施する手法を確立した。

Lately, innovation activities related to next-generation mobility services known as CASE (connected, automated, shared and service, electric) have been conducted in the automobile industry. This has led to greater focus on enhancing cybersecurity measures for in-vehicle electrical/electronic (E/E) systems.

With this in mind, Toshiba Electronic Devices & Storage Corporation has established the following methods to develop semiconductor products based on cybersecurity engineering technologies compliant with the International Organization for Standardization/Society of Automotive Engineers (ISO/SAE) 21434 “Road vehicles - Cybersecurity engineering” and ISO 24089 “Road vehicles - Software update engineering” standards: (1) a cybersecurity requirement determination method capable of reducing delays due to reworking to balance functional safety and cybersecurity performance, (2) a risk assessment method capable of classifying and identifying the vulnerability of semiconductors in vehicles, and (3) a method capable of securely updating the software of semiconductors currently in operation.

1. まえがき

自動車業界が目指すCASEに加え，先進国を中心にMaaS（Mobility as a Service）が推進されるなど，自動車のモビリティーサービス化と，それに伴う機能のソフトウェア化が進んでいる。その中で，車載E/Eシステムのサイバーセキュリティー対策の強化は喫緊の課題である。

この課題に対応するために，国際連合欧州経済委員会の自動車基準調和世界フォーラムは2021年に，自動車のサイバーセキュリティーの国際基準UN-R155並びにUN-R156を策定した。この法規は，自動車メーカーによる車両の型式認定の際に，CSMS（Cyber Security Management System）認証[3]，及びSUMS（Software Update Management System）認証[4]の取得を求めており，車載向け半導体メーカーにもこれらへの準拠を示すエビデンスの提供や管理説明が求められる。

CSMSとSUMSへの準拠は，ISO/SAE 21434とISO 24089に準拠することで達成できる。ISO/SAE 21434は，製品ライフサイクル全般を通じて持続的なサイバーセキュリティー管理の実現に必要な手順を定義している（**図1**）[1], [5]。

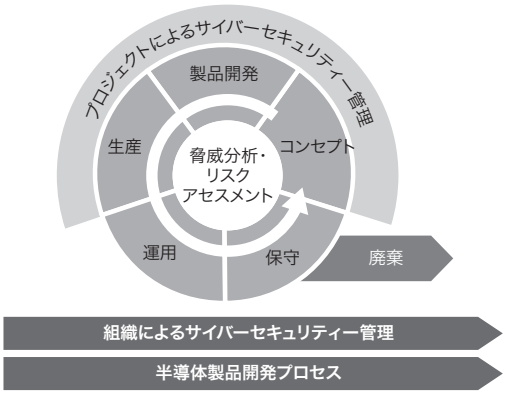


図1. 製品ライフサイクル全般のサイバーセキュリティー管理

CSMS準拠に必要なサイバーセキュリティーのリスク管理は，開発だけでなく製品ライフサイクル全般にわたって求められる。

Life-cycle cybersecurity management of semiconductor products

東芝デバイス＆ストレージ（株）は，パワートレインやボ

ディー制御用の車載E/Eシステムを開発・提供している。これらのシステムは，半導体とソフトウェアで構成されており（以下，半導体とソフトウェアを総称して半導体製品と呼ぶ），当社はISO 26262に基づく機能安全を含む実績ある既存の半導体製品開発プロセスを保有している。既存の半導体製品開発プロセスに，ISO/SAE 21434とISO 24089に準拠したエンジニアリング技術をオプションとして追加することで，車載向けの製品仕様に合わせた柔軟なサイバーセキュリティー対策を実現した。

また，継続的なセキュリティー脅威の監視やソフトウェア更新を含むインシデントへの対応は，東芝グループのPSIRT（Product Security Incident Response Team）・CSIRT（Computer Security Incident Response Team）活動と連携することで実現した。ISO 24089は，運用中の車両に対するソフトウェア更新を対象とした標準であり，更新機能開発など，半導体製品に関わる要求も含んでいる[2]。

ここでは，まず自動車製品のサプライチェーンにおける半導体の位置付けを明確にした後，当社のサイバーセキュリティーエンジニアリング技術の特徴として，製品開発時の半導体レベルでの要求決定手法，脆弱性分析手法，及び運用フェーズのセキュアなソフトウェア更新手法について述べる。

2. 自動車製品サプライチェーンにおける分散開発と半導体の位置付け

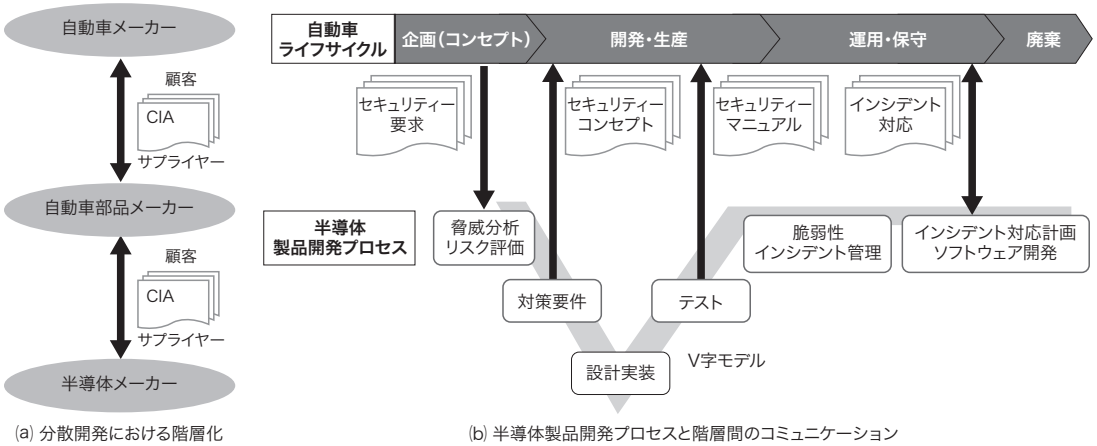
自動車メーカーは，階層的な分散開発で自動車を開発・生産している。分散開発は，自動車メーカー，自動車部品メーカー，及び半導体メーカーなど，主にそれぞれの階層間のコミュニケーションにより，責任範囲を明確にして行われる。半導体メーカーである当社は，サプライヤーとして分散開発に貢献している。サイバーセキュリティー活動は，自動車メーカーからサプライヤーに対するISO/SAE 21434とISO 24089適用要求に基づいて行われるが，汎用品を流用する場合を除き，原則としてCIA（Cybersecurity Interface Agreement）を取り交わすことで，明確に定義された役割分担に基づき開発が行われる（**図2**(a)）。

半導体製品開発プロセスは，対策要件とテストを対にしたV字モデルから成る（図2(b)）。半導体製品開発プロセスにはライフサイクルに応じて，脅威分析リスク評価，対策要件，設計実装，テストを経た半導体製品の提供，提供後のインシデント管理とその対応が含まれる。インシデント対応ではインシデント対応計画を立て，役割分担に基づいたソフトウェア開発を行う場合がある。自動車メーカーや自動車部品メーカーとのコミュニケーションは，半導体製品開発プロセスの要所において，セキュリティー要求，セキュリティーコンセプト，セキュリティーマニュアル，インシデント対応のほか，CIAで取り決めた情報の送受によって行われる。

3. 半導体製品開発プロセスのサイバーセキュリティーエンジニアリング

当社は，ISO 9001の品質管理に従って半導体製品を開発している。車載向け半導体製品は，IATF 16949（国際自動車産業特別委員会規格 16949）及びAutomotive SPICE®（ISO/IEC 15504（国際標準化機構規格／国際電気標準会議規格 15504）に沿って策定）に基づいて開発する。

加えて，安全上重要な製品には，ISO 26262に基づく



(a) 分散開発における階層化　　(b) 半導体製品開発プロセスと階層間のコミュニケーション

図2. 自動車の分散開発と半導体製品開発プロセスの関係
分散開発は責任範囲の明確化が重要であり，半導体製品開発プロセスの要所における階層間のコミュニケーションによって実現できる。
Relationship between automotive distributed development and semiconductor product development processes

機能安全が適用される。機能安全では，走行やユーザーインターフェースなどに関わる主機能の故障やバグに関して，企画段階のコンセプトフェーズ及び開発フェーズで安全分析を行い，必要な安全機構の配置や検証を実施する。安全機構を追加した場合，安全機構についても故障やバグの分析を行う。

更に，セキュリティー関連製品について，セキュリティー要求がある場合は，3.1節に述べる脅威分析を含む要求決定と3.2節の脆弱性分析を実施する。

3.1　サイバーセキュリティーエンジニアリングにおける要求決定手法

安全に関わる車載製品への要求は，主機能に加えて，機能安全とサイバーセキュリティーそれぞれの観点で，対応する国際標準の準拠が求められる。

コンセプトフェーズでの主機能への要求決定後，主機能のインターフェース並びに実現手段に対して機能安全・サイバーセキュリティーの分析を行う。ここでは，それぞれの要求の不整合防止，安全機構の脆弱性の見逃し防止，及びセキュリティーコントロール（セキュリティーリスクを低減するための機構）の故障影響の見逃し防止が課題になる（**図3**）。

このような課題に対して，コンセプトフェーズ及び開発フェーズにおいて，機能安全とサイバーセキュリティーの分析順序を定めている（**図4**）。

コンセプトフェーズでは，まず，セーフティーコンセプト(注1)として機能ブロックレベルの主機能に対して安全分析を行い，安全機構を初期配置する。次に，機能ブロックレベルの主機能と安全機構に対してサイバーセキュリティー観点で想定される脅威分析を行い，セキュリティーコントロールを配置し，セキュリティーコンセプト(注2)とする。

開発フェーズでは，セキュリティーコンセプトを出発点として，アーキテクチャー設計を行う。設計されたアーキテクチャーに基づいてソフトウェア脆弱性などを含むセキュリティー観点の脆弱性分析を行い，追加のセキュリティーコントロールを配置する。最後に，追加したセキュリティーコントロールを含めたアーキテクチャー全体の安全分析を行い，追加の安全機構を配置する。

このように，コンセプトと開発で段階的に分析を行い，分析順序を定めることで，機能安全とサイバーセキュリティー要求の不整合，安全機構の脆弱性の見逃し，及びセキュリティーコントロールの故障影響の見逃しを網羅的に防ぎ，開発の手戻りを軽減できる。

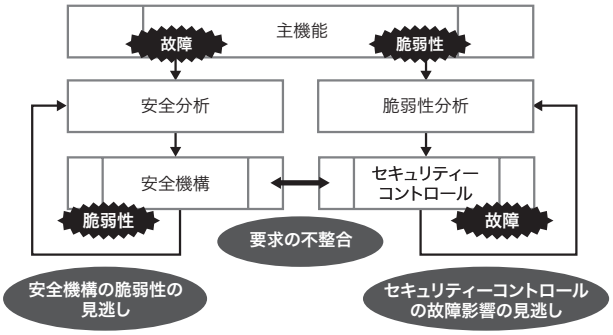


図3．機能安全との両立におけるサイバーセキュリティー分析の問題

それぞれの国際標準化機構規格では全体を通した分析手順は定義されないため，両者の整合性を十分に考慮する必要がある。

Issues faced by cybersecurity analyses ensuring compatibility with functional safety

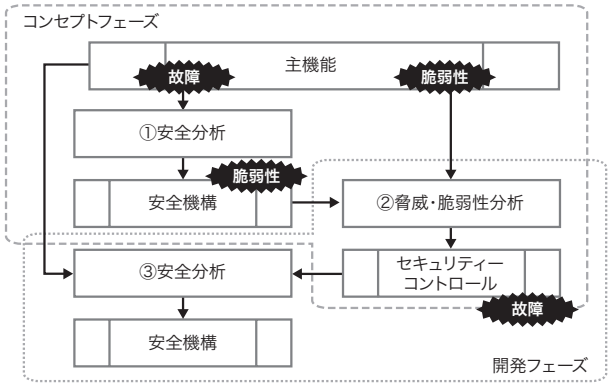


図4．製品開発フェーズにおける機能安全とサイバーセキュリティーの分析順序

製品開発の各フェーズにおいて分析順序を定めることで，機能安全とサイバーセキュリティーの整合性を確認できる。

Sequence of functional safety and cybersecurity analyses in semiconductor product concept and development phases

3.2　半導体製品レベルの脆弱性分析手法

自動車の開発における脆弱性分析の目的は，車両コンポーネントに潜在している脆弱性が外部から攻撃された結果，運転者や歩行者などの道路利用者に生じる損害リスクを評価し，リスク低減策を判断することである。CSMSでは車外のバックエンドサーバーを含めた車両システム全体で考慮が必要な脅威と脆弱性を定義しており，自動車メーカーやサプライヤーはこの定義を参照して脆弱性分析を行う[3]。

しかし，この定義での脅威と脆弱性は概念的なものであって，具体性が不足している。特に，半導体製品開発に求められる既知脆弱性の排除を達成するための，より具体的な

（注1）安全目標の達成に対する機能や，安全状態の定義，異常発生から危険事象が現れるまでの時間などを示す。
（注2）サイバーセキュリティーの達成に対する目標の適合性や，コンテキストの一貫性，リスク低減策の有効性，安全との互換性などを示す。

表1. ソフトウェアとハードウェアの代表的なCWE

Typical common weakness enumerations (CWEs) of semiconductor product software and hardware

ソフトウェア	
CWE-ID	説　明
CWE-787	境界外書き込み
CWE-79	クロスサイト スクリプティング
CWE-416	解放済み メモリー使用
CWE-78	OSコマンド インジェクション
…	…

ハードウェア	
CWE-ID	説　明
CWE-1189	SoC上の共有リソースの不適切な分離
CWE-1191	不適切なアクセス制御によるオンチップデバッグ及びテストインターフェース
CWE-1231	ロックビット変更の不適切な防止
…	…

ID：識別情報　　OS：基本ソフトウェア　　SoC：System on a Chip

基準が必要である。

そこで当社は，ソフトウェア・ハードウェアの脆弱性を体系化したCWE（Common Weakness Enumeration：共通脆弱性タイプ一覧）（**表1**）を独自に参照することで，半導体製品の既知脆弱性の分析範囲を明確化した。

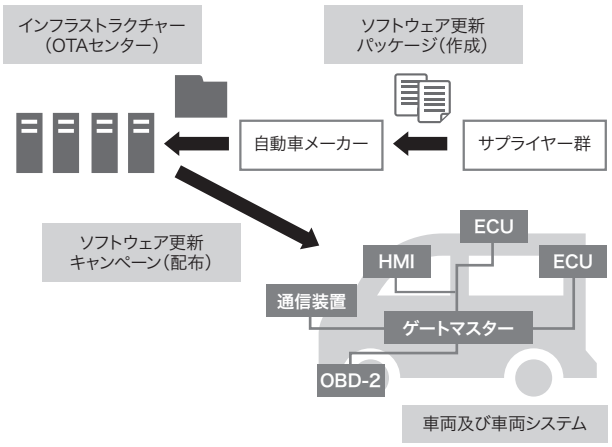
このように，CSMSで定義される車両システムレベルからのトップダウンに加え，当社独自の半導体レベルからのボトムアップによる脆弱性分析を合わせて実施することにより，半導体製品のサイバーセキュリティー対策を強化した。

4. 運用フェーズのセキュアなソフトウェア更新手法

半導体製品の運用フェーズで，東芝グループ全体のPSIRT活動と連動して，車載製品に関わる脆弱性情報の収集と分析を行っている。車載E/Eシステムは，自動車メーカーと連携した脆弱性分析の結果，半導体製品のインシデント対応が必要になるケースも想定される。インシデント対応において半導体の交換は即応性に欠けるため，多くの場合，ソフトウェア更新で対応する。サイバーインシデント以外の主機能や安全機構の更新における安全性も含めて，自動車メーカーがSUMSに準拠したソフトウェア更新を確実に実施できるように，ISO 24089の要件を満たす半導体製品開発プロセスを定義した。

当社は，ISO 24089の要件のうち“車両および車両システム”に基づいた半導体の機能開発と，“ソフトウェア更新パッケージ（作成）”に基づいたソフトウェア更新パッケージのリリースに対応している（**図5**）[5]。当社がサプライヤーとして作成したソフトウェアは，ソフトウェア更新パッケージとして自動車メーカーによりほかのサプライヤーのソフトウェアと統合され，“インフラストラクチャー（OTA（Over the Air）センター）”や“ソフトウェア更新キャンペーン（配布）”を通して，車両及び車両システムへ配布される。

ソフトウェア更新は，自動車部品メーカーにより当社のソフトウェアがECU（電子制御ユニット）用ソフトウェアに取り込まれた上で行われる。当社は，自動車部品メーカーへリリースするソフトウェアをソフトウェア更新パッケージとみなすことで，ISO 24089に準拠した機能開発及びソフトウェア更新パッケージのリリースに対応し，半導体製品のセキュアなソフトウェア更新手法を確立して，サプライチェーン全体でのセキュアなソフトウェア更新の実現に貢献している。



HMI：ヒューマンマシンインターフェース　　OBD：On-board Diagnostics

図5. ISO 24089によるソフトウェア更新プロセスの概念図

ソフトウェア更新に関わる全活動のリスク管理を実施することで，サプライチェーン全体でセキュアなソフトウェア更新を実現する。

Conceptual diagram of software update process corresponding to ISO 24089

5. あとがき

当社は，半導体サイバーセキュリティーエンジニアリング技術として，機能安全との両立にあたって生じる手戻りを軽減するサイバーセキュリティー要求決定手法，車両中の半導体レベルの脆弱性分析手法，及び運用フェーズのセキュアなソフトウェア更新手法を確立した。

この技術を用いた車載向け半導体製品を継続的に開発・提供することにより，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し，自動車業界が目指すCASEの実現に貢献していく。

文　献

(1) 日本規格協会グループ．ISO/SAE 21434:2021 自動車-サイバーセキュリティエンジニアリング．<https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=ISO%2FSAE+21434%3A2021>,（参照 2024-07-30）.

(2) 日本規格協会グループ．ISO 24089:2023 自動車-ソフトウェア更新エンジニアリング．<https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=ISO+24089%3A2023>,（参照 2024-07-30）.

(3) UN Regulation No.155 - Uniform provisions concerning the

approval of vehicles with regards to cyber security and cyber security management system.
⑷ UN Regulation No.156 - Software update and software update management system.
⑸ 東芝．サイバーセキュリティ報告書 2024．<https://www.global.toshiba/jp/cybersecurity/corporate/report.html>,（参照 2024-07-30）.

・Automotive SPICE®は，Verband der Automobilindustrie e.V.（VDA）の登録商標。

伊藤　佑一　ITO Yuichi
東芝デバイス&ストレージ(株)
半導体事業部 IC開発センター
Toshiba Electronic Devices & Storage Corp.

早乙女　一郎　SAOTOME Ichiro
東芝デバイス&ストレージ(株)
半導体事業部 半導体品質保証センター
Toshiba Electronic Devices & Storage Corp.

高橋　清紀　TAKAHASHI Kiyonori
東芝デバイス&ストレージ(株)
半導体事業部 半導体応用技術センター
Toshiba Electronic Devices & Storage Corp.