WP29への対応
自動運転車のサイバーセキュリティ(2)

UNECE WP29 GRVAサイバーセキュリティ法規基準への対応
CSMS構築におけるISO/SAE 21434の活用

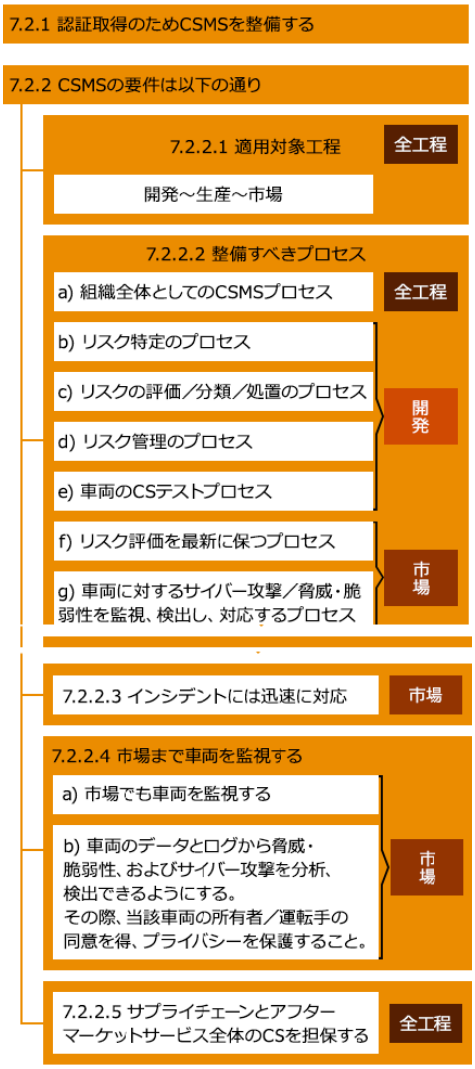
PwC コンサルティング合同会社　シニアマネージャー
奥山 謙

国連欧州経済委員会（United Nations Economic Commission for Europe）の「自動車基準調和世界フォーラム（WP29）」の分科会「自動運転（GRVA）」が策定するサイバーセキュリティ法規基準の施行に向けて、自動車業界は同法規基準に記されるサイバーセキュリティマネジメントシステム（CSMS）の整備を軸とした対応を迫られています。

今後、日本をはじめとする車両等の型式認定相互承認協定の対象国において車両の型式認可を取得するには、CSMSで求められる組織体制や製品ライフサイクルを通じたリスクベースのセキュリティプロセスを体系的に構築・運用し、当該プロセスが実際の車両に適用されていることを実証できなくてはなりません。

今回はCSMSを構築するにあたって参照可能な国際標準規格の内容と、その活用のポイントを紹介します。

図表1:UNECE WP29 GRVAサイバーセキュリティ法規基準における要求事項



[1] 7章の法規要件とISO/SAE 21434の対応関係については、CS/OTA 17th session(2020/1/21-23) のTFCS 17-15 (ISO SAE) Comparison of UN-Reg-CS with ISO SAE 21434 and coherence check,やCS/OTA Test Phase - ad hoc meeting(2019/9/18)の各種資料が参照できる。
[2] PSIRT（Product Security Incident Response Team）：製品セキュリティインシデント対応体制

国際標準規格に基づくCSMSへの対応が有用

サイバーセキュリティ法規基準の施行が差し迫る一方で、既存の組織体制やプロセスとの整合性、一貫性が要求されるCSMSの構築はOEM・サプライヤー双方にとって大きなチャレンジです。そんな中、OEM・サプライヤーが共通認識に基づいてプロセス・プロダクト両面でCSMS対応を具体化するための基準として注目されているのが、2020年2月にDIS（Draft International Standard）版が公開された車両サイバーセキュリティの国際標準規格「ISO/SAE 21434 Road vehicles — Cybersecurity engineering」です（同規格の前身は、機能安全規格ISO 26262のサイバーセキュリティ版として2016年に発行された「SAE J3061 Cyber Security Guidebook For Cyber - Physical Vehicle Systems」です）。特に車両開発のV字プロセスを通じたリスクベースの保障アプローチと各工程成果物に基づく安全性の論証といった基本的な考え方を共有している点が、既存の自動車開発の取り組みに親和性があるとされます。また、サイバーセキュリティ法規基準との対応性に関しても、WP29内でしばしば議論されている通り1、一定の十分性を有すると考えられています。

サイバーセキュリティ法規基準とISO/SAE 21434への対応を並行して進めることで、現状の国際社会で求められる車両サイバーセキュリティの実現を期待できると考えられます。

ISO/SAE 21434の概要

ISO/SAE 21434は、車両の企画・開発から生産、廃棄に至る製品ライフサイクル全体を通じた車両のセキュリティ確保における要求事項をまとめた国際標準規格です。同規格については『車両サイバーセキュリティの未来』で解説しています。現在公開されているDIS版において、約140の要求／推奨事項が規定されていますが、本コラムでは簡素化した以下の分類に基づき、あらためて概説します。

全体的なサイバーセキュリティマネジメント:

車両のサイバーセキュリティ確保を目的とした組織体制、ガバナンス、ポリシー策定、監査、教育・文化醸成、情報共有体制の整備、品質管理システムといった全社的なサイバーセキュリティ活動基盤が求められます。コーポレートガバナンス、ITシステムの情報セキュリティ、リスクマネジメント、機能安全、品質保証などの各社における既存の活動領域との責任分担や依存関係を整理し、関連部門と効果的に連携した取り組みが求められます。

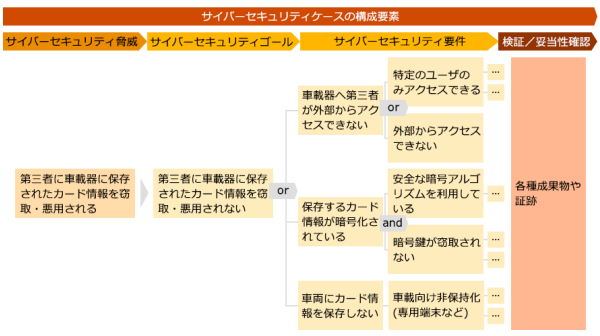
開発プロジェクト毎のサイバーセキュリティマネジメント:

「全体的なサイバーセキュリティマネジメント」で整備された組織体制やポリシーを開発プロジェクトレベルで具体化し、サイバーセキュリティ計画として実施すべきエ程と成果物を定義します。

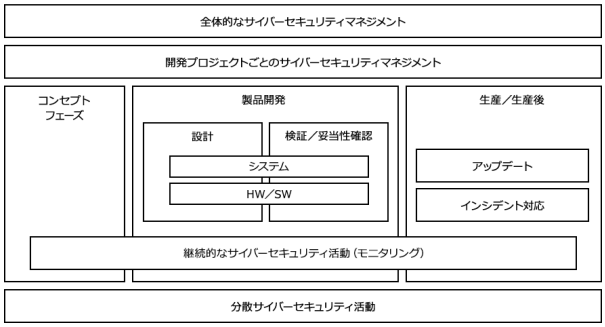
図表2：WP29サイバーセキュリティ法規基準とISO/SAE 21434の対応性（2020年4月時点）

	WP29 GRVAサイバーセキュリティ法規基準	ISO/SAE 21434
原則	リスクベース、プロセス、体制、実証	リスクベース、プロセス、体制、成果物／論証
対象工程	開発／生産／生産後（7.2.2.1）	コンセプト／製品開発／生産／運用・保守／廃棄
主な要求	組織全体としてのプロセス（7.2.2.2a） リスクアセスメント（7.2.2.2b,c） リスクマネジメント（7.2.2.2d） CSテストプロセス（7.2.2.2e） リスク評価の最新化（7.2.2.2f） 車両脆弱性の監視／検出／対応（7.2.2.2g） インシデント対応（7.2.2.3） 市場でのCS監視（7.2.2.4） サプライチェーン（7.2.2,5）	全体的サイバーセキュリティマネジメント（5章） リスクアセスメント（8章） リスクマネジメント（5,8,11章） サイバーセキュリティ検証／妥当性確認（5,8,11章） サイバーセキュリティ計画の最新化（6章） サイバーセキュリティモニタリング（7章） インシデント対応（13章） サイバーセキュリティモニタリング（7章） 分散サイバーセキュリティ活動（15章）

図表4：サイバーセキュリティケースの構成要素（イメージ）



図表3：ISO/SAE 21434の構成



コンセプトフェーズ（企画）：

コンセプトレベルでのリスクアセスメント（脅威分析）を行い、対応すべきリスクを特定し、以降の活動の起点となるサイバーセキュリティ上の目標（サイバーセキュリティゴール）を定義します。

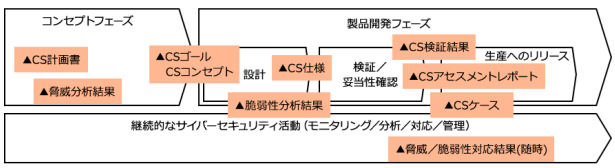
製品開発フェーズ（システム／HW／SW）：

コンセプトフェーズの成果をもとに、特定の設計／実装内容、また設計／実装を通じて顕在化する脆弱性にも考慮したリスクアセスメント（脆弱性分析）を通じて、リスクおよびセキュリティ要求を具体化します。

設計フェーズでは、ハードウェア（HW）／ソフトウェア（SW）両面でのセキュリティ確保が必要となります。ソフトウェア実装時のセキュアコーディング、ハードウェア耐タンパ性確保など、それぞれで特有のセキュリティ管理策が求められます。

検証／妥当性確認フェーズでは、各種セキュリティテストの手法によりセキュリティ要件が満たされていることを確認し、合わせてセキュリティ要件そのものが適切に設定されていることの妥当性を確認します。

図表5：コンセプトフェーズ・製品開発フェーズの工程と成果物のイメージ



生産／運用・保守／廃棄：

生産フェーズにおいては、工場全体のセキュリティ確保が求められます。特に通信の暗号化やメッセージ認証などで用いられるデータ（暗号鍵）の生成・保管、車載機器への書き込みなどにおけるセキュリティを保つための設備や運用を含む鍵管理システムを整備する必要があります。

運用／保守フェーズでは、IDS（Intrusion Detection System）／IDPS（Intrusion Detection and Prevention System）といった不正検知・防止の技術を用いたサイバーセキュリティモニタリングやソフトウェアアップデート、運用施策としてのPSIRT2、SOC（Security Operation Center）などの構築が特に重要になってきます。

廃棄フェーズでは、車載器に登録されたセキュリティや利用者に関する情報の適切な削除ができることが求められます。こうした生産／運用・保守／廃棄時に求められるセキュリティ機能や運用については、後から追加・変更することが難しいため、製品開発フェーズからセキュリティ要件として考慮される必要があります。

継続的なサイバーセキュリティ活動（モニタリング）：

車両のサイバーセキュリティに影響を与え得る情報を継続的に収集／トリアージ／分析／対応します。セキュリティコミュニティや脆弱性情報データベース、自社内の検証活動などの多用な情報源が監視対象となります。また、販売後の車両のみが対象ではなく、開発時においても収集した情報を適切に設計へフィードバックするためのプロセスが求められます。

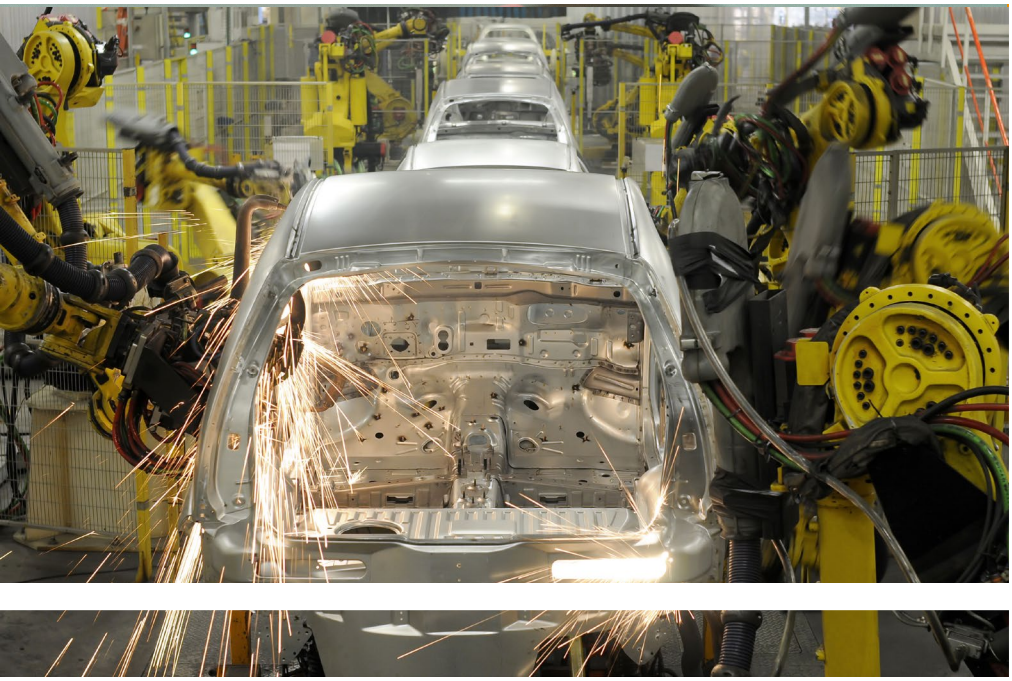
分散サイバーセキュリティ活動：

OEMがサプライヤーに部品開発を依頼して分散開発を行う場合は、責任分解点について明確に合意し、各社が責任範囲に応じたCSMSを確立する必要があります。OEM観点からはサプライヤーの能力評価や受け入れ基準の定義、選定プロセスの整備、サプライヤー観点ではOEMのセキュリティ要求を理解・整合し、自社のサイバーセキュリティ能力を実証することが求められます。分散開発やサプライチェーンを通じたセキュリティ対応については、OEM・サプライヤーそれぞれが多数の取引先と並行して調整を進める必要があり、適切な対応・コミュニケーションが求められます。このテーマについては、本連載において後日、詳細に解説します。

CSMSの導入にあたっては組織や製品に応じたテーラリングが必要

UNECE WP29 GRVA サイバーセキュリティ法規基準およびISO/SAE 21434における要求事項は多くの組織に適用できるよう抽象化されており、それゆえ一部、解釈の余地を残しています。法規基準と国際標準規格の要求への対応をどのように具体化し、自組織や自社製品に落とし込むか（テーラリング）は各組織に委ねられます。客観的かつ十分な論拠と証跡をもって、論証を成立させることが求められます。

今回はISO/SAE 21434を中心に、国際連合の法規基準で求められるCSMS対応の概要を説明しました。次回は、同法規基準で求められるソフトウェアアップデートマネジメントシステム（SUMS）への対応について解説します。自動車に組み込まれるソフトウェアのアップデートは、サイバー攻撃の予防、問題が発見された際の事後対応など、セキュリティ確保の観点からも重要な機能です。こうした自動車のソフトウェアアップデートを管理する仕組みであるSUMSの構築は、車両の形式認可とは切り離せない活動です。



お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel : 03-6250-1200（代表）　Mail : jp_cyber_inquiry@pwc.com