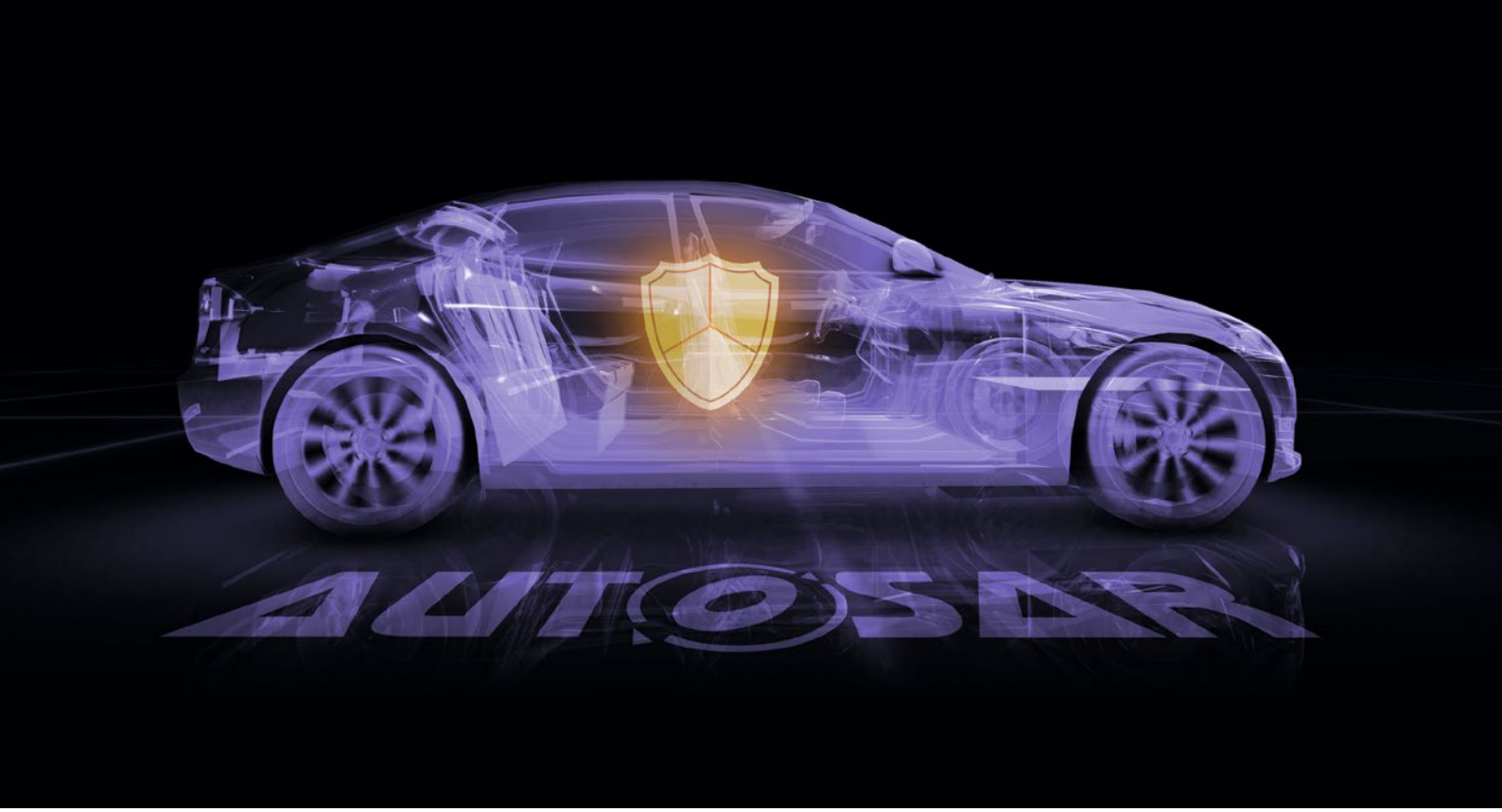

AUTOSAR セキュリティ

包括的な車両保護の実装が必要な Adaptive プラットフォーム

自動運転や接続性に関する機能が向上するにつれ、より柔軟なソフトウェアアーキテクチャと高度な IT セキュリティが必要となってきています。AUTOSAR では、このような要求に対応するため、Adaptive プラットフォームとクリティカルセキュリティコンポーネントを提供しています。

AUTOSAR Classic は、ほとんどの車両プラットフォームに対応する標準的なミドルウェアであり、一般的な要求基準を満たしています。ただし将来的には、車両はソフトウェアによって支配されるシステムとなり、ビークルコンピュータが中央アプリケーションとして E/E アーキテクチャを形成することになるというのが一般的な予想です。そのため、当社では、AUTOSAR Classic に置き代わる新たな未来志向のルールセットとして AUTOSAR Adaptive を開発しました。AUTOSAR Adaptive は、車載セキュリティプロセスにおける新たな基準となります。

AUTOSAR のセキュリティモジュール

AUTOSAR には、たとえば、車載通信のセキュリティや機密データの保護を始めとして、さまざまな IT セキュリティアプリケーションがすでに組み込まれています。しかし、AUTOSAR Classic と AUTOSAR Adaptive では現在、アーキテクチャの違いから、部分的に共通または異なるセキュリティアプリケーションを実装しています（図 1）。

- **暗号スタック：**実装される暗号化手順とキーストアを決定し、統一されたインターフェース経由でさまざまなアプリケーションに必要な鍵マテリアルを提供します。その後、アプリケーションは暗号化の実装に関係なく、提供されたインターフェースのみにアクセスし、異なる ECU にも移植できる状態を維持します。また、AUTOSAR 暗号スタックは複数の暗号化の実装にも同時に対応できます。
- **SecOC、TLS、および IPsec：**AUTOSAR Classic 固有のプロトコルである SecOC は、特に CAN 通信のセキュリティを保護します。SecOC では、メッセージの認証と新鮮度は保証しますが、機密性は保証しないため、OEM メーカーは固有のセキュリティレベルの微調整が可能です。一方、車載 Ethernet においては、TLS および IPsec の重要性はますます高まっています。この両規格は、通信の真正性と機密性をサポートします。また、TLS は外部通信にも適しています。
- **識別とアクセス管理：**AUTOSAR Identity and Access Management モジュールを使用すると、承認されたアプリケーションのみに特定のリソースへのアクセス権を付与できるようになります。

AUTOSAR では、これらのアクセス権は自由に設定でき、いつでも更新することが可能です。

- **セキュア診断：**AUTOSAR では、セキュアなメモリ内で IT セキュリティイベントを記録することができます。また、UDS サービス 0x27（SecurityAccess）と 0x29（認証）を使用することで、このデータへの認証済みのアクセスも監視します。たとえば、診断テスト装置がログに記録されているセキュリティインシデントにアクセスすることができるのは、以前にチャレンジレスポンス通信を実行したか、または証明書を使用して自身の認証を行った場合のみです。

セキュリティエンジニアリングプロセス

最も重要なことは、AUTOSAR に含まれるセキュリティモジュールを車両プラットフォームに適用し、セキュリティ要件に合わせて個別に調整することです。つまり、リスク分析、コンフィギュレーション、およびテストという 3 つの重要なステップに基づいて、AUTOSAR をセキュリティエンジニアリングプロセス全体にわたって統合する必要があるということです。SecOC を例にすると、次のようになります（図 2）。

- **リスク分析：**まず、すべてのメッセージのリスク分析を行い、SecOC で保護すべきメッセージを特定します。異なるセキュリティプロファイルが保存されている場合、メッセージは正しいプロファイルに割り当てられます。
- **コンフィギュレーション：**次に、データ交換に関連するすべての ECU について、リスク評価とセキュリティプロファイルに従って SecOC と暗号スタックが設定されます。ここでは、1 つの ECU で不適切な設定があると、保護されるメッセージが検証されず、破棄される場合があるという点に注意が必要です。
- **テスト：**ECU を量産向けにリリースする前には、セキュリティの観点から、(SecOC モジュール、暗号スタックなどの) セキュリティクリティカルなコンポーネントのコードレビュー、ECU の侵入テスト、SecOC モジュールの機能テストといった複数のテストを実施する必要があります。

統合されたセキュリティアプローチに従う必要がある AUTOSAR Adaptive

ネットワーク接続を備えた自動運転車両の実用に向けて、安全関連の車載機能の数は増え続けています。つまり、車両プラットフォームへの入念なセキュリティ対策と高度なセキュリティレベルの実装が以前にも増して重要になっています。今後、多くの OEM メーカーが高度な接続性をベースにした新たなビジネスモデルを確立していくことになるでしょうが、そこではセキュリティの保護も必要になります。つまり、セキュリティアプリケーションをこれまで以上に強固に統合できるようにするために、AUTOSAR Adaptive のさらなる開発が必要になるのです。

また、車載セキュリティの統合を目指すということが AUTOSAR Adaptive の基本理念であり、ハードウェアセキュリティモジュールなどの IT セキュリティソリューションの追加や、侵入の検知や防止向けのソリューションの実装などを考慮に入れて開発していく必要があります。■

セキュリティニーズに基づいた AUTOSAR 設定

例：認証済みの ECU 通信

- ✔ セキュリティ関連メッセージの識別
- ✔ SecOCでのメッセージの設定
- ✔ 暗号スタック内での鍵とアルゴリズムの選択
- ✔ 車両間での設定の調整
- ✔ セキュリティクリティカルなコンポーネントのコードレビュー
- ✔ ECUのポテンシャルのテスト
- ✔ SecOCモジュールの機能テスト

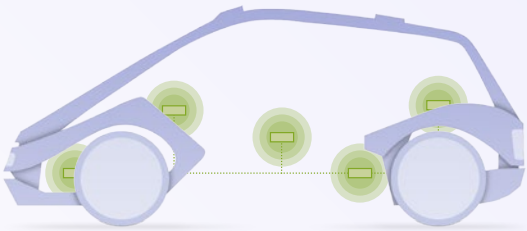

図 2：セキュリティ要件に従った AUTOSAR コンフィギュレーション（例として SecOC を使用）

執筆者

Alexandre Berthold 博士、ESCRYPT コンサルティングおよびエンジニアリングチームリーダー

Michael Peter Schneider 博士、ESCRYPT プロジェクトマネージャ、AUTOSAR セキュリティ

	暗号スタック	SecOC	TLS	IPSec	セキュア ログ / 診断	識別および アクセス管理
AUTOSAR Classic 4.4	✔	✔	✔	✖	✔	✖
AUTOSAR Adaptive R19-03	✔	✖	✔	✔	✖	✔

図 1：AUTOSAR Classic および Adaptive のセキュリティアプリケーション（2019 年 8 月現在）

ソリューションポートフォリオ

セキュリティの設計

コンサルティング、テスト、
およびトレーニング

**戦略的セキュリティ
コンサルティング**

- 戦略的セキュリティ開発、セキュリティのビジョンとロードマップ
- セキュリティの標準化、ロビーイング、戦略的協業

セキュリティトレーニング

- セキュリティの基本
- セキュリティリスク分析
- セキュアな製品設計
- セキュアなコネクテッド製品
- 車載セキュリティ

セキュリティの活用

製品およびソリューション

プロダクションキーサーバー 量産時に暗号鍵を安全に書き込む暗号化サーバー

CycurHSM 車載用の品質を備えたHSM用セキュリティスタック
CycurIDS 侵入検知
CycurV2X セキュアなV2X通信用SDK
CycurGATE 車載ファイアウォール

セキュリティの管理

オペレーション、モニタリング、
インシデントおよび対応

マネージドPKIサービス
証明書の発行／期限切れ／失効などのステータス管理をOEMメーカー内部でコントロール

セキュリティオペレーションセンター（SOC）
管制センターとして機能し、車両運用の全側面から異常やイベントを追跡

製品セキュリティ コンサルティング

- セキュリティのリスクと脅威分析、防御要件
- セキュリティのコンセプトとデザイン
- セキュリティ関連の役割とプロセス
- カスタムコンサルティング

製品セキュリティ エンジニアリング

- セキュリティの仕様
- セキュリティの実装
- セキュリティの統合
- セキュリティ製品
- セキュリティ管理

セキュリティテスト

- 機能セキュリティテスト
- 脆弱性のスキャンとファジング
- 侵入テスト
- コードセキュリティ監査
- セキュリティ認証
- セキュリティテスト管理

CycurACCESS 車両へのアクセスと鍵共有

CycurTLS 組み込みプラットフォーム用トランスポート層セキュリティ(TLS)

CycurLIB 組み込みシステム用の暗号ライブラリ

CycurKEYS 暗号鍵と証明書をセキュアに管理

CycurV2X-SCMS V2Xセキュリティ証明書管理システム

CycurGUARD 侵入の監視と解析

脅威の情報収集と犯罪科学調査

既知／新規の脅威に関するエビデンスベースのナレッジから、確かな情報に裏付けられた意志決定と対応

脆弱性管理

欠陥を発見し、OEMメーカーによる事前の脅威防御戦略の施行を可能に