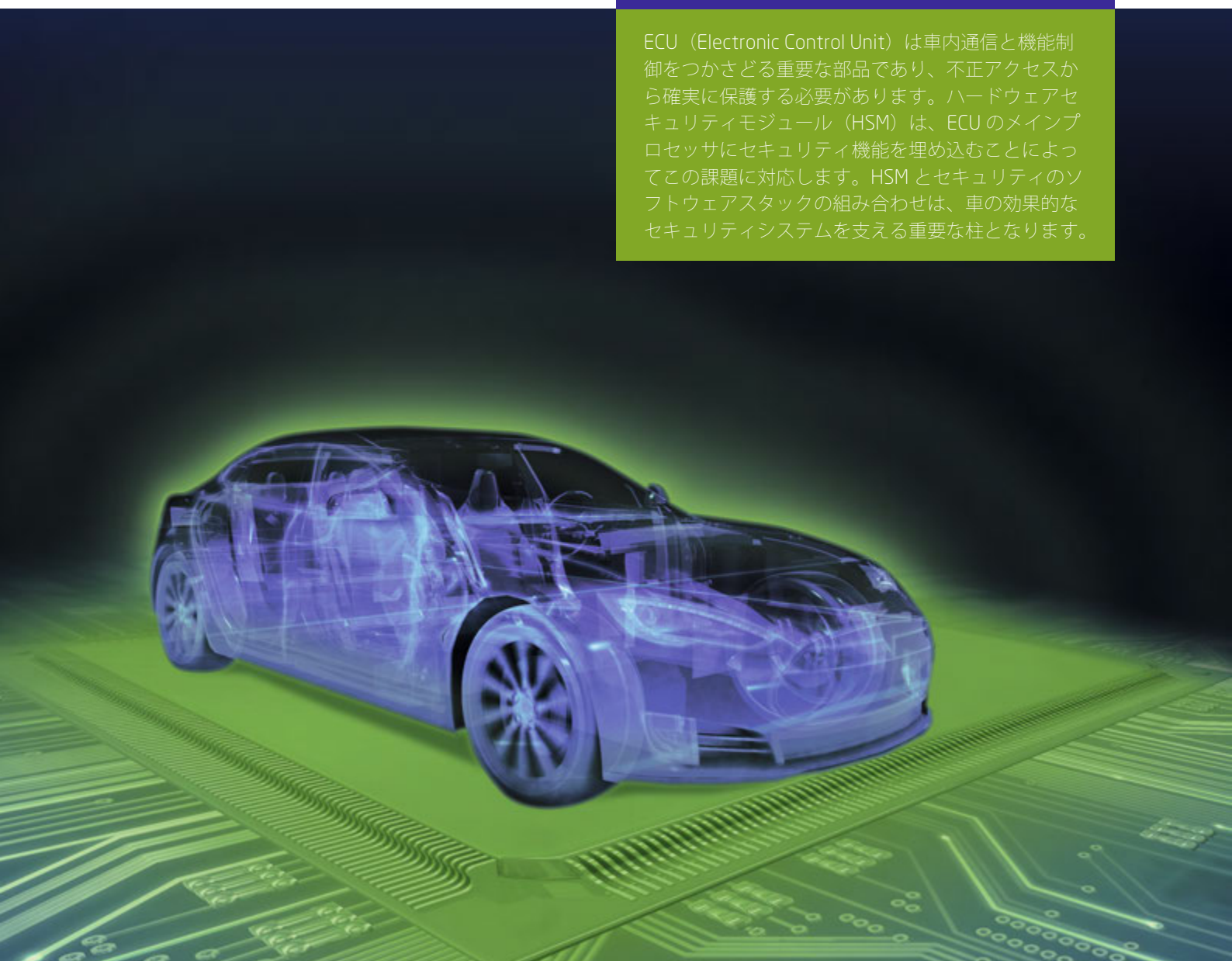
内側から守る自動車セキュリティ

ハードウェアセキュリティモジュール（HSM）が ECU メインプロセッサを内側から守る

ECU（Electronic Control Unit）は車内通信と機能制御をつかさどる重要な部品であり、不正アクセスから確実に保護する必要があります。ハードウェアセキュリティモジュール（HSM）は、ECU のメインプロセッサにセキュリティ機能を埋め込むことによってこの課題に対応します。HSM とセキュリティのソフトウェアスタックの組み合わせは、車の効果的なセキュリティシステムを支える重要な柱となります。



車両のチューニング作業においてパワートレインの ECU にアクセスしてシステムのパラメータを変更するとき、あなたの頭の中には、騒音や排ガス規制とは別のことが真っ先に思い浮かぶでしょう。何にも増して気がかりなのは、電子的に制御された車両システムに自分がアクセスできるという事実です。

悪意のあるハッカーがパワートレインやシャーシの ECU に問題を引き起こしたらなどとは、恐ろしくて考えたくもないでしょう。車両の電気系統にあるすべての ECU が標的になる可能性があります。ましてやコネクテッドビークルともなればなおさらです。ソフトウェアが不正に操作されたり、きわめて重要なキーマテリアルにアクセスされたりするのを防ぐために、最新の車両には、外部と遮断する堅牢な IT セキュリティ機構が必要です。それこそが、ECU の心臓部にセキュリティ機能を埋め込むハードウェアセキュリティモジュール（HSM）の意義なのです。

自動車専用の HSM

HSM は、セキュリティ機能を物理的にカプセル化した一種のハードウェアです。その集積チップは IT セキュリティ用途に特化して設計されており、通常、独自のプロセッサコア、各種メモリ（RAM、ROM、フラッシュなど）、ハードウェア暗号アクセラレータを備えています。加えて HSM は、車両用途における特定の基準を満たす必要があり、また、コストを低く抑えるために、きわめて効率的な集積化が不可欠となります。その主な要件として、ECU アプリケーションと HSM との間の安全なインターフェースや、動作不良を分析するためのデバッグ／テスト用インターフェースがあります。HSM は、できるだけ短い待ち時間で暗号情報を処理できること、また、自動車環境の標準的な温度に対して十分な耐性を持ち合わせていることが求められます。

車載仕様のアーキテクチャを備えたハードウェアセキュリティモジュールが、Infineon、ST Microelectronics、Renesas、NXP など、すでにいくつかの大手チップメーカーから提供されています。基本的に HSM は、自動車のユースケースで求められるすべての IT セキュリティ機能を、その独自のプロセッサコアを使用して実行します。そうした機能には、128 ビット AES ハードウェアアクセラレータ、キーマテリアルを生成するための完全乱数生成器（TRNG：True Random Number Generator）、暗号化キーを格納するハードウェアで保護されたストレージ、フラッシュ／デバッグ機能、システムメモリと分離された HSM 独自の RAM などがあります（図 1 を参照）。

目的に合わせて作られたセキュリティソフトウェアとリアルタイム通信

自動車 HSM は、セキュアなソフトウェアスタックがあって初めてその真価を発揮します。HSM が車の IT セキュリティの細胞核だとすれば、HSM セキュリティソフトウェアはその遺伝コードです。ESCRYPT では、これを CycurHSM セキュリティファームウェアの形で提供しており、ファームウェアは、さまざまなメーカーの自動車 HSM 向けに作られています。既存のハードウェアセキュリティ周辺装置は、CycurHSM によって適切な HSM およびホストコントローラアプリケーションに関連付けられます。また、対称暗号化メカニズムと非対称暗号化メカニズム、HSM ベースの追加的なセキュリティ機能など、包括的な暗号ライブラリも、このファームウェアによって HSM に導入されます。さらに、CycurHSM には、標準的な車載 ECU に HSM を統合するために必要な AUTOSAR 準拠のインターフェースと AUTOSAR 非準拠のインターフェースが含まれています。

ソフトウェアアーキテクチャの核となる要素は、リアルタイム

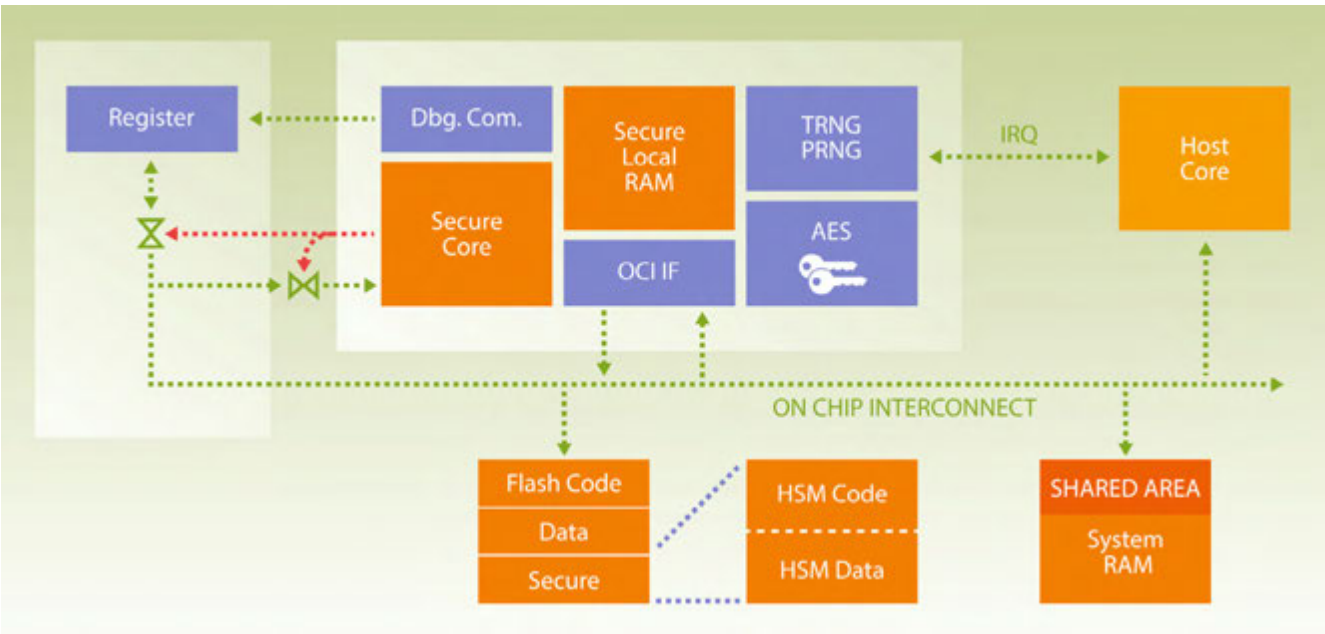


図 1：ハードウェアセキュリティモジュール（HSM）のハードウェアアーキテクチャ

オペレーティングシステムです。この ISO 26262 認定システムは、車載 ECU に特化して作られており、リアルタイム HSM 機能（車内のセキュアなリアルタイム通信など）をサポートします。このオペレーティングシステムは、ごくわずかな実行時オーバーヘッドで動作し、また MISRA-C に準拠しています。CycurHSM には、優先度ベースのタスクスケジューリングを実装するセッションマネージャが組み込まれていて、例えば、車載バス上の新しいメッセージを検証することは、タイムクリティカルではない操作よりも優先されます。また、HSM 内のキーマテリアルへのアクセスとその生成、保管、削除とを管理するキーストアマネージャを実装し、さまざまな長さの対称鍵と非対称鍵をサポートします。暗号ライブラリ（CycurLIB）は、HSM の暗号アクセラレータを使用して暗号プリミティブ（ECC、RSA）を提供します。HSM で必要に応じて SHE エミュレーションを実行することもできます。暗号ライブラリにアクセスしながら、自動車固有の高度な要件（SHE+）を満たすことが可能です。加えて、専用 HSM ドライバが、HSM とホストプロセッサとの間の通信をセキュリティで保護します。HSM とのインターフェースにある AUTOSAR 準拠の

- 高性能な暗号化が要求されるユーザー固有の用途向けにハードウェア／ソフトウェア協調設計の強力なプラットフォームを提供
- HSM とのインターフェースが標準化されているため、シンプルなカスタマーインテグレーションが可能
- 完全にプログラム可能。モジュール構造により特定のニーズを満たす構成が可能
- マルチコア対応

この機能セットによって、HSM ソフトウェアスタックは広範なセキュリティユースケースに対応できるようになります。標準化されたインターフェースを使用すれば、さまざまな IT セキュリティ機能を実装できます。IT セキュリティ機能は HSM 自体に実装できるほか、ホストプロセッサと協調して動作するように実装することもでき、どちらの場合も、その基盤として強力な暗号化技術を利用することができます。これらの機能はセキュアブートで起動します。つまり、ECU が起動するたびに、フラッシュメモリに格納されているコードがチェックされます。また、実行時改ざん検知とセキュアフラッ

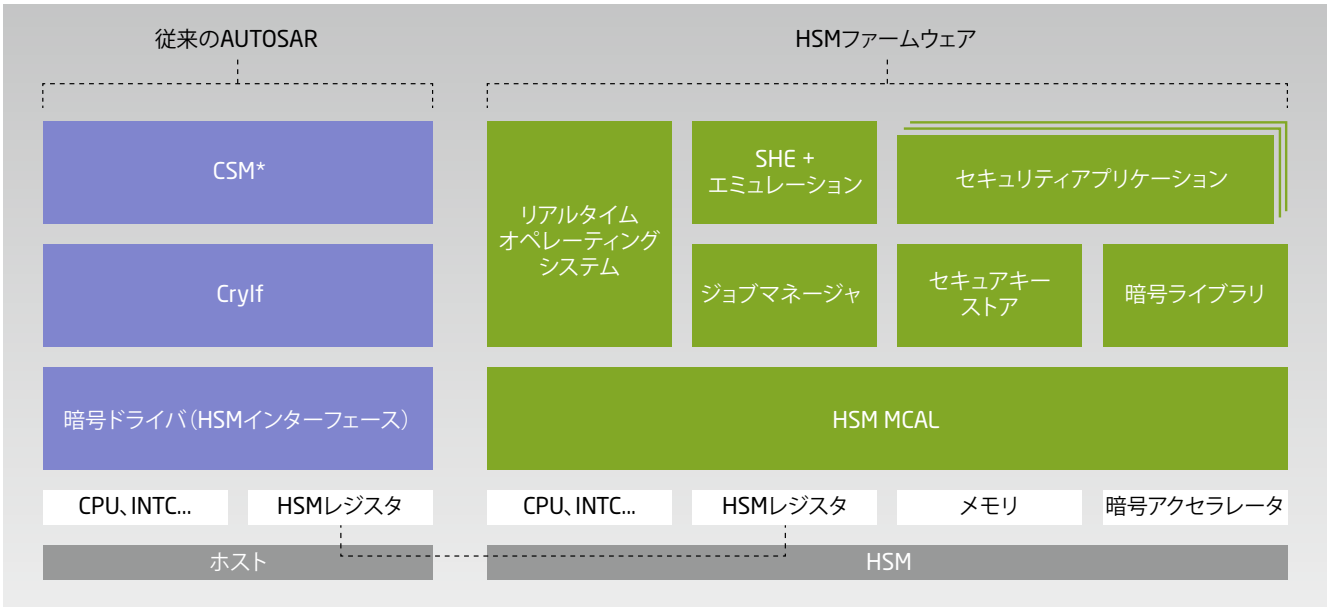


図 2：ハードウェアセキュリティモジュール（HSM）のソフトウェアアーキテクチャ

暗号サービスマネージャ（CSM：Crypto Service Manager）の働きにより、AUTOSAR アプリケーションはいつでも HSM にアクセスすることができます（図 2 を参照）。

多機能で実装が容易

ハードウェアセキュリティモジュールの機能は、純粋にソフトウェアをベースとしたソリューションよりもはるかに強力です。HSM のセキュリティ機能は物理的にカプセル化されているため、ECU ホストコントローラは、その本来のタスクに専念することができます。HSM セキュリティソフトウェアと相まって、このアプローチは、さまざまな利点を備えたターンキーソリューションを実現します。

シュ、ソフトウェアダウンロードプロバイダーの認証機能を備えているほか、セキュアログ機能を備えているため、セキュリティを脅かすイベントは確実に記録されます。そのすべての場合において基本となるのは、要求元のインスタンスと HSM との相互認証です。これは、セキュアデバッグにも当てはまります。セキュアデバッグは、デバッグポートへの不正アクセスから ECU を保護しつつ、ソフトウェアのデバッグ目的で承認されているアクセスを許可するものです。この場合も、通信と認証は HSM によって制御されます。

新世代の HSM ファームウェア

HSM のハードウェアとソフトウェアの開発が急速に進み、

自動車専用のハードウェアセキュリティモジュールを標準搭載した ECU のマイクロコントローラも増えてきています。ESCRYPT は、そうした進歩に後れを取ることなく、着実にその HSM ソフトウェアスタックである CycurHSM の改良を進めています。最新世代の CycurHSM は、従来よりもさらに使いやすくなり、また、特色あるオプションを通じて、独自仕様の IT セキュリティ機能を ECU に実装できるようになっています。新しい HSM ファームウェアは、アプレットマネージャを使用したり、さまざまな管理システムを使用して個々のセキュリティ機能をアクティブ化したりすることによって容易に設定することができます。また、ASPICE に準拠したこのソフトウェアには、柔軟なキーストアアーキテクチャが備わっています。

今後、加速的に導入が進むコネクテッドビークルと自動運転技術を保護するためには、End-to-End の保護が何よりも重要です。インターネットに接続された環境では、侵入検知システム、車載ファイアウォール、安全な無線ソフトウェアアップデート、セキュア V2X などの技術を開発者が実装することによって重要な要素をすべてセキュリティで保護しなければなりません。End-to-End の保護とは、デジタル車両の機能を構成する最も基本的なコンポーネントのレベル、つまり個々の ECU のマイクロプロセッサ内に IT セキュリティ機能を埋め込むことを意味します。それこそが、ハードウェアセキュリティモジュールの意義なのです。ハードウェアセキュリティモジュールは、今日の自動車におけるセキュリティ開発において中核をなすものと考えられ、全般にその将来は明るい見通しです（図 3 を参照）。

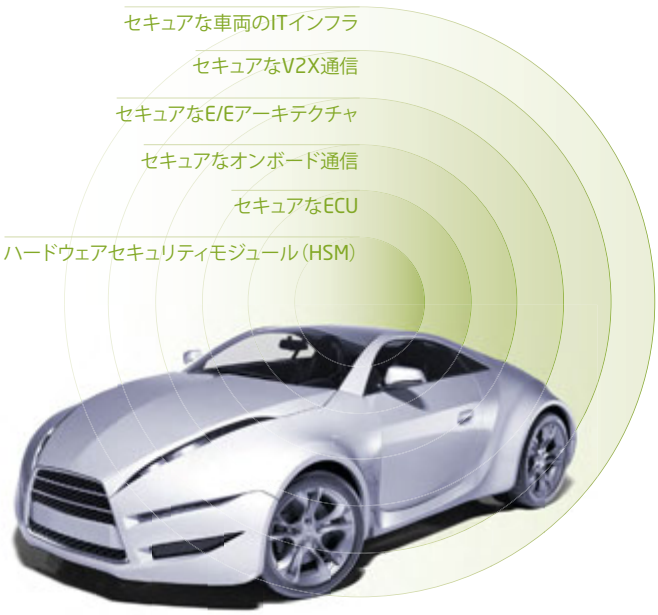


図 3：ハードウェアセキュリティモジュール（HSM）は自動車セキュリティの中核

執筆者

Dr. Frederic Stumpf、ESCRYPT
プロダクトマネジメント統括

ESCRYPT が “Innovator 2018” を受賞

ドイツの有名なビジネス出版社 **brand eins** が最近発表した、最も革新的なドイツ企業の年間ランキングにおいて、ESCRYPT が最優秀企業の一社に選ばれました。ESCRYPT は Technology and Telecommunication カテゴリで最も多くの専門家の支持を集め、**「Innovator of the year 2018」**賞を獲得しました。

25,000 人を超える専門家が、特定の選考基準に従い、3,400 社以上の企業の中からイノベーションリーダーを選びました。ESCRYPT は「製品とサービス」、「プロセスイノベーション」、「企業文化」という、あらかじめ規定された 3 部門で平均を上回る支持を集めました。統括部長である Uwe Müller 氏は、**「このような賞をいただけて光栄です。これほど励みになることはありません。今後もイノベーションを弊社の原動力として邁進していきたいと思います。」**と話しています。

brand eins Thema
2018
INNOVATOR DES JAHRES