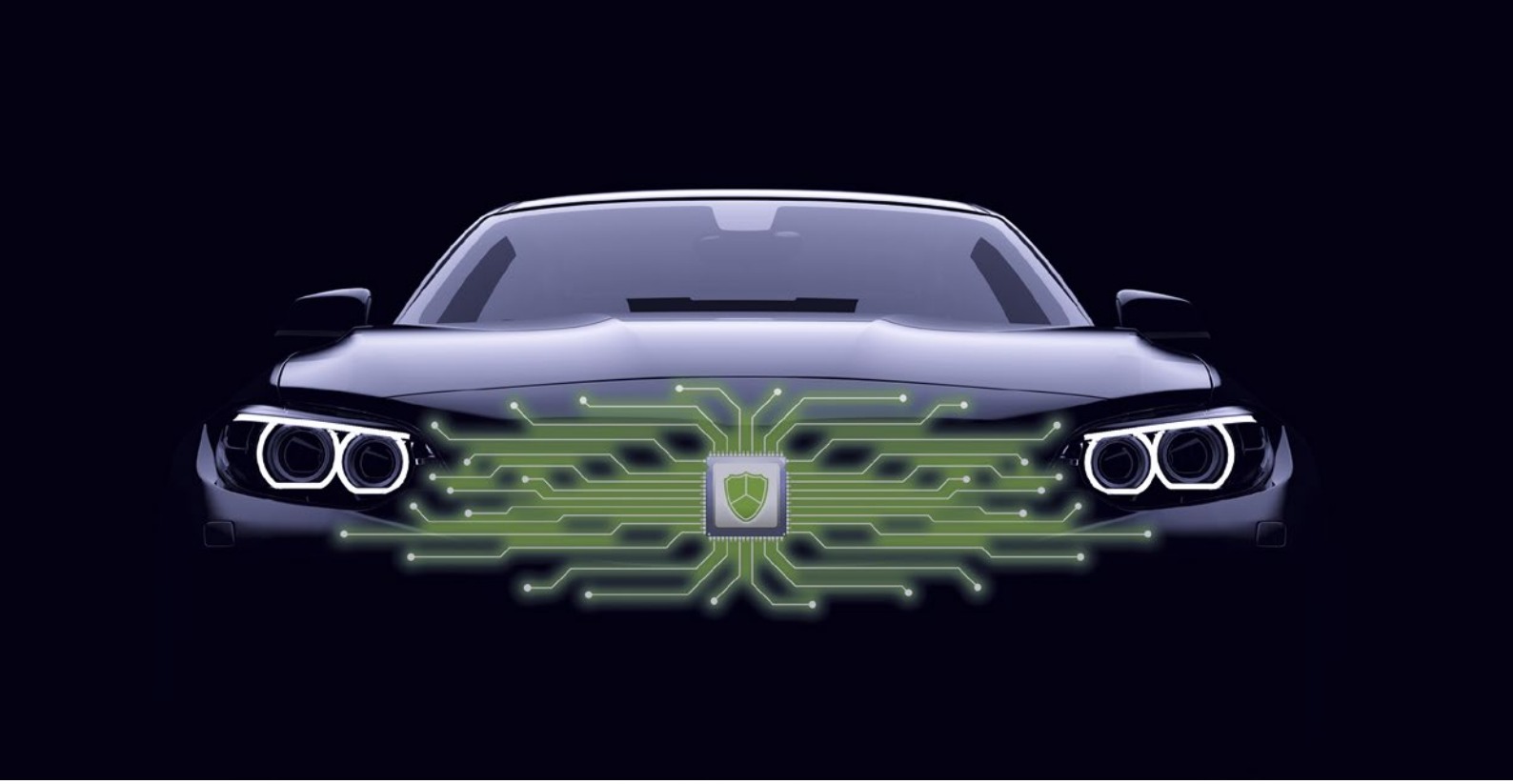

ハードウェアセキュリティモジュールの性能向上

新しいサービス指向の HSM ソフトウェアにより、未来の電気システムアーキテクチャを保護

未来の車両アーキテクチャでは、多くのソフトウェアがドメインコントローラに一元化され、車載 Ethernet が広帯域のオンボード通信を提供するようになると予想されています。これを実現するためには、IT セキュリティへの新たなアプローチが必要です。次世代型のハードウェアセキュリティモジュール（HSM）は、マルチアプリ機能とリアルタイム通信を統合するための中心的なコンポーネントとして機能しつつあります。

また、ビークルコンピュータ（VC）は、車両ドメインとソフトウェア制御機能との融合を図るためのアプローチです。つまり、周辺装置の ECU は入出力デバイスとしての役割をますます担うようになり、実際のアプリケーションの実行は VC 上で行われるようになります。これにより、IP が中央コンピュータへと移行したり、E/E アーキテクチャの複雑性が減少してエンジニアリングの作業負荷が軽減されるなど、OEM メーカーにとってさまざまな利点が提供されます。OEM メーカーは、車両世代ごとに特定の ECU とソフトウェアを購入するのではなく、ビークルコンピュータにソフトウェアアプリケーションの開発工程や相互作用を蓄積することで、時間と費用を節約することができます。

しかし、このような集中化が発生すると、オンボード通信の増加に拍車がかかります。そのため、ドメインコントローラは複数の ECU に処理を分散するのではなく、データを収集して処理し、車両に配信しなければならなくなります。多くの場合、これらはリアルタイムで処理する必要があります。そのため、データトラフィックは車載 Ethernet 経由で転送されることになります。一方で、サブネットワークでの信号の送受信はいまだに CAN バス経由で実行されています。そのため、IT セキュリティはこのようなハイブリッド（混合）アーキテクチャに対応する必要が生じます。

セキュアな製品設計

求められる接続性の増加を見据えた場合、セキュリティの確保とそのアップデートをハイブリッド車載ネットワークの設計時点で確実に組み込んでおく必要があります。特に、ハードウェアとソフトウェアの分離や多くのソフトウェアアプリケーションの再配置によって新たな可能性が示される場合があることも考慮しなければなりません。IT セキュリティ機能は、中央集中型の車載ネットワークで一元的に管理することも可能ですが、同時に周辺装置に搭載された ECU の保護も重要となります。

ハードウェアセキュリティモジュール（HSM）は、オンボード通信（SecOC）を完全にセキュアに実行するうえで不可欠な要素であり、

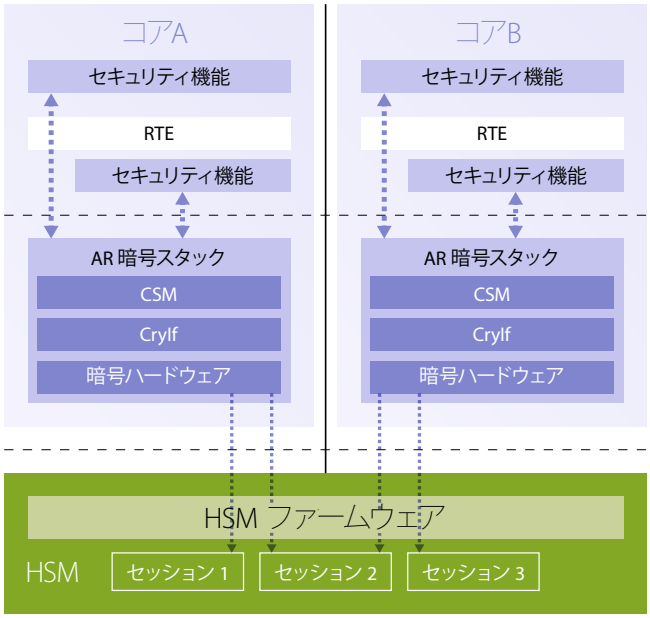

図 1：複数のホストコアからの要求は並行セッションとして HSM ファームウェアによって処理されます。

収束されるすべてのデータの真正性を保証する機能を提供します。また、セキュリティ関連の ECU インターフェースをバイパスすることにより、サイバー攻撃者による中央プロセッサまたは車載ネットワークへの侵入を阻止します。しかし、中央集中型の車載ネットワークの課題はそれだけではありません。多数の仮想マシンに分割されることが多い中央のビークルコンピュータにソフトウェアアプリケーションや複数の ECU の機能を担わせると、セキュリティコンポーネントへの要求も増加します。これに対応するため、次世代型のハードウェアセキュリティモジュールが既に開発されています。

ジョブプリフェランスとリアルタイム OS

HSM の IT セキュリティ機能は、個々のプロセッサのマイクロコントローラ上にある HSM コアに物理的にカプセル化されています。そこでは、HSM ソフトウェアスタックを介して IT セキュリティ機能が起動および動作します。これにより、ビークルコンピュータのホストコントローラが実際のタスクに専念できるようになると共に、HSM コアがセキュアなオンボード通信や実行時の改ざん検知、セキュアブート、フラッシュ、ログ、デバッグなどのセキュリティ要件を処理できるようになります。そのため、HSM は純粋にソフトウェアベースの IT セキュリティよりもはるかに強力なソリューションとなります。

ソフトウェアアプリケーションと ECU 機能をビークルコンピュータ上に統合すると、多数のアプリケーションが HSM のセキュリティ機能に同時にアクセスして競合が発生しやすくなることが予想されます。こうなると、HSM は必要な IT セキュリティ機能を提供しながら、複数のアプリケーションのデータストリームをリアルタイムで管理しなければならなくなります。標準的な HSM でこれを実行するには限界があります。まして、純粋なソフトウェアベースのセキュリティソリューションではなおさらです。しかし、リアルタイム OS を搭載し、インテリジェントかつ柔軟なセッションコンセプトを採用した次世代型のハードウェアセキュリティモジュールであれば、このようなタスクにも十分に対応できます。

マルチコア／マルチアプリケーションのサポート

将来のアーキテクチャでは、セッション数を設定できる最新の HSM ソフトウェアスタックを搭載した新しい HSM ファームウェアにより、複数のコアで同時に要求が行われた場合に HSM コアが最大 16 セッションを並列処理できるようになります。このマルチコア／マルチアプリケーションをサポートするうえで鍵となるのは、特別なアーキテクチャを持つ HSM ファームウェアドライバです。このドライバにより、仮想化されたさまざまなアプリケーションごとに個別にドライバを統合できるようになるため、さまざまなソフトウェアパーツの個別での開発が可能になります。また、統合時に「リンカ」ステップを使用すると、ドライバのさまざまなインスタンスがハードウェアの共有 RAM で共通の構造を使用できるようになります。ここでは、各インスタンスが固有の構造（セッション）を作成するため、厳密にカプセル化された並列アプリケーションから出される複数のリクエストをドライバが常に管理できるようになります（図 1）。

このセットアップの中央セキュリティコンポーネントとなるのは、ホスト -HSM ブリッジです。このブリッジからは、ハードウェアセキュリティをホストから分離するための要素として、HSM モジュールに「インフロー制御」が引き継がれます。ブリッジレジスタでは、限られたリソースである HSM を最大限に活用しながらも、ホストコアから送られたリクエストキューが要求されたセキュリティ機能を可能な限り迅速に実行できるようなセットアップが施されています。次世代型の HSM ソフトウェアを活用すれば、HSM のマルチアプリケーション／マルチコア機能の実用化が可能になります。OEM メーカーは、完全にテスト済みの量産可能な形式として、これらを使用できます（図 2）。

Bulk MAC インターフェースにより、リアルタイムパフォーマンスを提供

もう 1 つの課題は、大幅に増加する通信量を保護するための手法です。集中型電気システムにおける CAN バスと車載 Ethernet の混在を解決し、すべての通信プロトコルで車両間のデータ交換をセキュアに保護するためには多くの課題があります。革新的なソリューションである HSM は、このような対策も提供していますが、もちろ

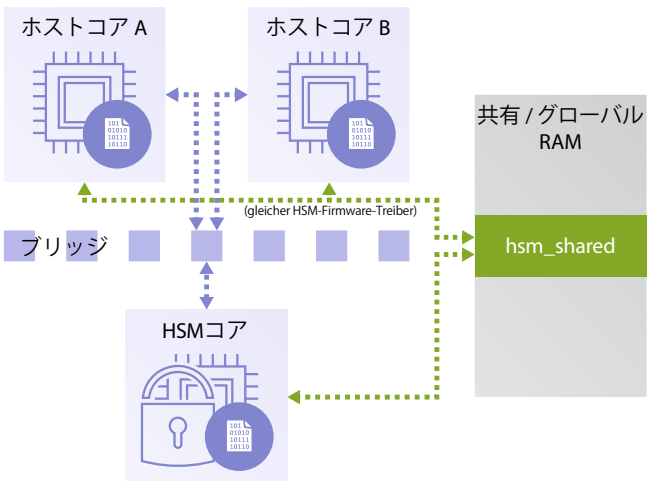

図 2：マルチコア／マルチアプリケーションのサポート – ジョブリクエストはブリッジレジスタと共有 RAM を介して処理されます。

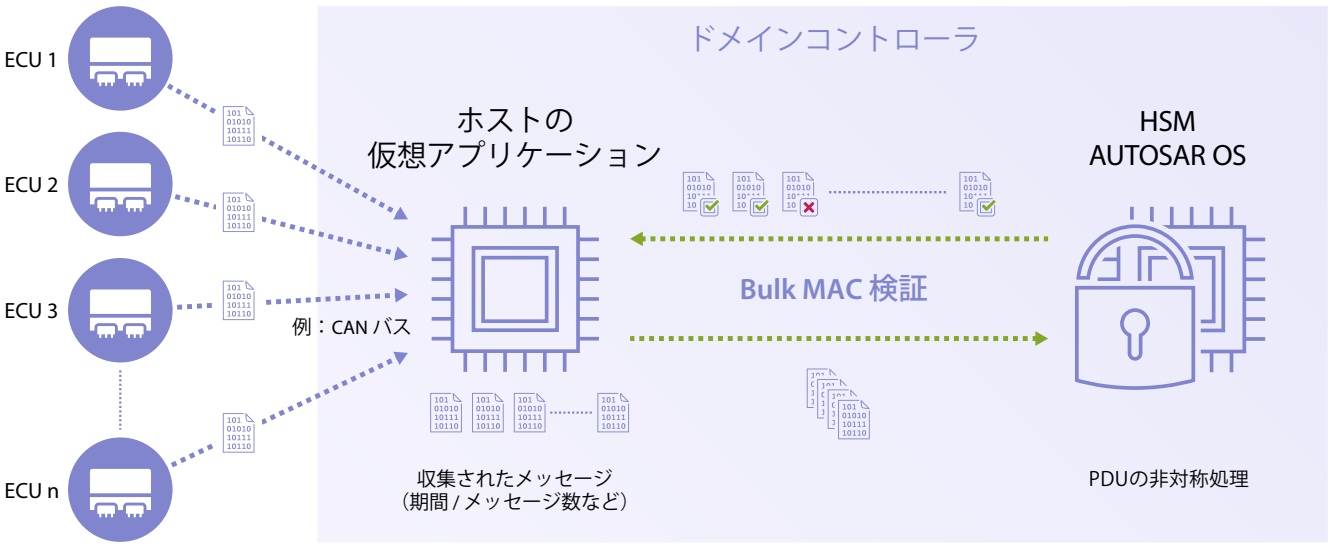

図 3：bulk MAC インターフェースによるセキュアなリアルタイム通信の提供

ん性能上の限界はあります。その限界は HSM のハードウェア暗号エンジンというより、むしろブリッジレジスタに起因します。なぜなら、ブリッジレジスタでは、量や速度を問わず、データ交換を行わないからです。ここでの解決策の 1 つとなるのは、bulk MAC インターフェースという手法です。この手法では、ホストがあらかじめ決められた期間にすべてのメッセージを収集したうえで、これらのメッセージをブリッジレジスタ経由で一括して HSM にポスティングします。この場合、データ転送はたった一度だけで済みます。HSM ファームウェアは HSM ハードウェアユニットで収集されたすべてのメッセージを一度に処理し、その結果をホストに送信します（図 3）。

これにより、性能の大幅な向上が可能になります。ホストと HSM 間での各データ転送の時間が 10 µs であっても、100 個のメッセージを処理すると遅延時間は合計 1 ms にもなります。これは、リアルタイムシステムでは無視できない問題です。しかし、bulk MAC インターフェースを使用すると、100 個のメッセージの処理時間を 100 分の 1 にすることができます。そのため、中央コンピュータとドメインコントローラをセットアップし、プロセスに多くの PDU を定義している OEM メーカーが bulk MAC インターフェースを使用すれば、明らかな優位性を得ることができます。膨大な量の多様なメッセージを十分に高速に認証できるこのインターフェースを使用することで、車両ネットワークにおけるセキュアなリアルタイム通信が実現します。次世代型の HSM ソフトウェアには、この bulk MAC セットアップがすでに統合されており、量産準備が進められています。

将来にわたって使用できるハードウェアセキュリティファームウェア

車載ネットワークが集中型プラットフォームへと移行するにつれ、ハードウェアとソフトウェアの分離が進んでいますが、ハードウェアセキュリティモジュール（HSM）は、これらのプラットフォームの IT セキュリティを保証するうえでの中心的な役割を果たしています。HSM では、（今後も引き続き CAN バスで処理される）周辺装置から中央コントローラへのデータストリームにおける不正なアクセスや改ざんを（SecOC で）防止するだけでなく、最上位のネットワークレベルでのセキュリティ要件をカバーしたり、高いデータ負荷でリアルタイムに処理する必要があるソフトウェアアプリケーションをセキュアに実行したりすることができます。マルチコア／マルチアプリケーションタスク用に設計された次世代型の HSM は、bulk MAC インターフェースを使用することにより、異種

次世代型のハードウェアセキュリティファームウェアは、OEM メーカー独自の製品バリアントにマッピングすることができます。

フォーマットが含まれている場合でも高データ負荷のリアルタイム通信を確実に処理することができます。

各 OEM メーカーでは、接続性の増大と自動運転への移行を考慮して、E/E アーキテクチャ向けの自社固有のセキュリティ基準を段階的に見直しています。次世代型のハードウェアセキュリティファームウェアは、OEM メーカー独自の製品バリアントにマッピングすることも、中央集中型のセキュリティコンセプトに柔軟に統合することも可能です。また、このファームウェアは最新のマイクロコントローラ上で動作し、ホストドライバをソースコードとして提供するため、OEM メーカーや Tier 1 サプライヤは容易に再利用やカスタマイズを行うことができます。この優れた柔軟性と性能により、最新のファームウェアを搭載したハードウェアセキュリティモジュールは、未来の中央集中型ハイブリッド車載ネットワークのセキュリティを保護するための中心的なコンポーネントとなっています。■

執筆者

Tobias Klein、ESCRYPT リードプロダクトオーナー、HSM
Frederic Stumpf 博士、ESCRYPT プロダクトマネジメント統括、サイバーセキュリティソリューション