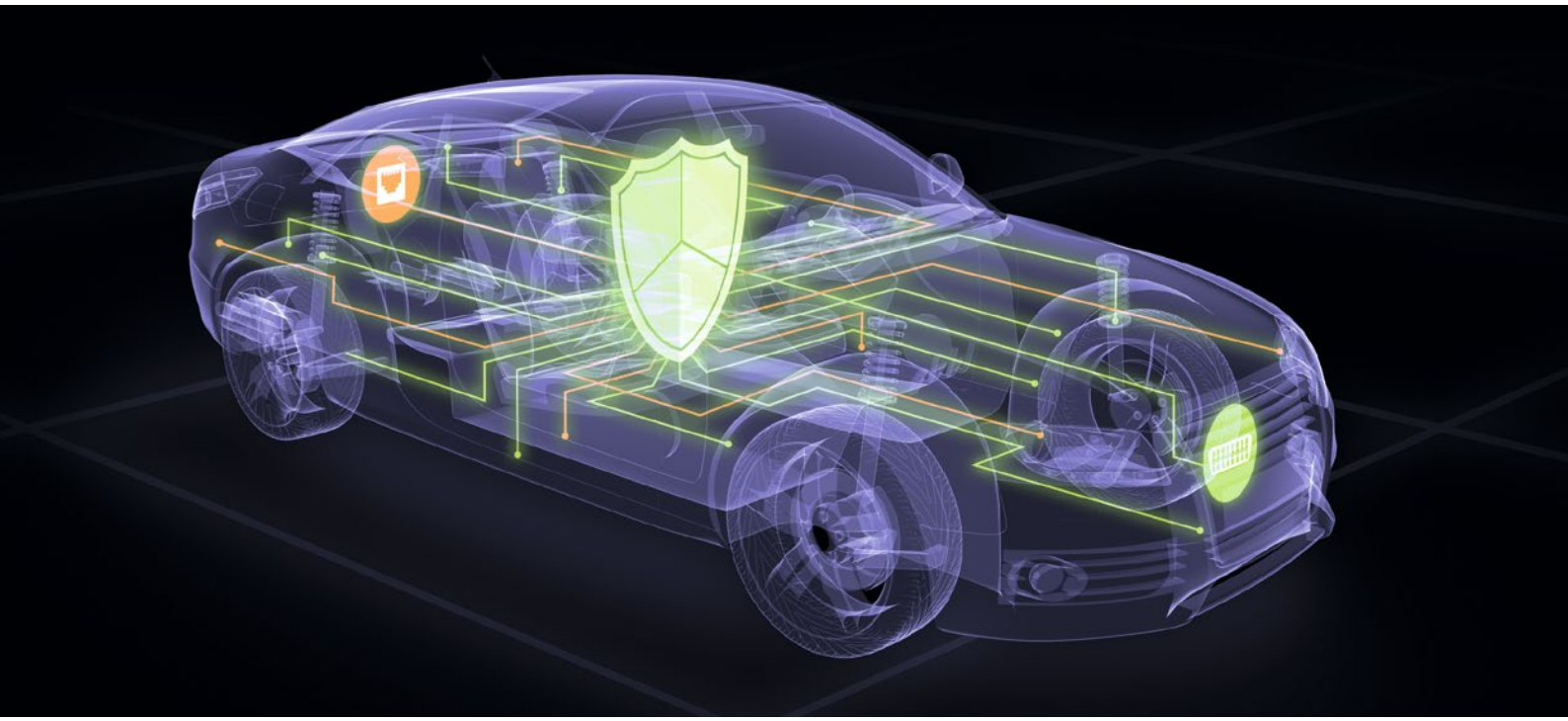
# ハイブリッド CAN-Ethernet ネットワークでの侵入検知

## 2 つの世界に最適なセキュリティ対策の構築



**今日の分散化された E/E アーキテクチャでは、ネットワーク接続を備えた自動運転車両で生じる課題に対応できなくなっています。そのため、ビークルコンピュータと車載 Ethernet を使用して、従来の ECU と CAN バスを補完することが必要になっています。そして、このような車両ネットワークは、専用設計の攻撃検知方式とデータトラフィック監視方式を用いて保護する必要があります。**

CAN、LIN、および FlexRay データバスによって接続された多くの ECU を含む今日の車両電気システムを補完するには、ビークルコンピュータ（VC）と広帯域の車載 Ethernet であるということは、現在の業界の明確な開発方針となっています。現在の車両電気システムは、高度なリアルタイム要件や周期的反復機能を実装しなければならない領域では今後も需要がありますが、それ以外の領域では、マイクロプロセッサベースの中央コンピュータを仮想マシンで分割する方式に切り替わるでしょう。その方がネットワーク接続を備えた自動運転車両で生じる課題に対しより適切に対応できるからです。

ところで、CAN-Ethernet ハイブリッドアーキテクチャとそのデータプロセスのセキュリティは、実際にはどのような形で保護するのでしょうか？基本的には、通信のシールディングとパーティショニングという 2 つの手法が用いられます。サイバー攻撃を早期の段階で検出するためには、通信をシームレスに監視することが必要です。また、攻撃を受けた場合の侵入深度を最小限に抑えるためには、ドメイン固有の仮想サブネット（VLAN）が必要です。ハイブリッド電気システムではいずれに対応できますが、CAN および Ethernet の世界では異なる系統的アプローチが必要になります。

### CAN 向けの効率的な攻撃検知

CAN バスを監視するには、侵入検知システム（IDS）をゲートウェイまたは ECU に統合します。このシステムは、OEM メーカーが指定する「正常動作」と CAN データトラフィックを比較することにより、異常を検知します。組み込みセキュリティコンポーネントは、たとえば、周期的メッセージや不正な診断要求の異常を検出し、潜在的攻撃として分類し、ログやレポートを作成します（図 1）。

CAN IDS（CycurIDS）のパフォーマンスは、その構成品質に大きく左右されます。そのため、OEM メーカーが提供する初期ルールが優れていたとしても、最新の攻撃ベクトルの分析に基づいた新しい検出メカニズムで継続的に補完し、可能な限り少ない誤警告で高い検出率を達成できるようにする必要があります。つまり、初期構成に使用するツールボックスの品質を高くし、ルールセットを継続的に開発していくことが重要です。IDS（CycurIDS）などのソフトウェアはすぐに使用できるよう設定されており、ハイブリッド電気システムにおける CAN 攻撃向けの検出システムとしていつでも利用できます。

### 車載ファイアウォールを Ethernet スイッチ内に実装

これに対して、車載 Ethernet ファイアウォール（CycurGATE）は、ハイブリッド電気システムにおいてセキュアかつスムーズな Ethernet 通信が必要な場合に使用することが推奨されます。この車載 Ethernet ファイアウォールを Ethernet スイッチに直接実装すると、ECU やホストコントローラへの干渉リスクを伴わずにパケットフロー全体を監視できるようになります。このようなファイアウォールでは、協調型の設計によりハードウェアとソフトウェアのバランスを取っており、スイッチ上でのファイアウォールによるハードウェアアクセラレーションが可能なため、大半のデータパケットをワイヤースピード（理論上の最大速度）で処理できます。これは主に、サービス妨害攻撃の防御に有効です。ただし、ネットワーク層のパーティションはすべて維持されているため、パーティションで区切られた領域間においても、ファイアウォールがデータをセキュアに交換することができます。これは、パケットフィルタが送受信データをフィルタリングし、ステートフルパケットインスペクションとディープパケットインスペクションを使用して各データをチェックすることで可能になっています。

これにより、車載 Ethernet ファイアウォール（CycurGATE）によって電気システムを不正アクセスや不正操作から保護しつつ、オンボード通信も制御できるようになります（図 2）。車載 Ethernet ファイアウォールは、Ethernet/IP だけでなく、（SOME/IP などの）一般的な車載プロトコルにも完全に対応しており、ネットワークへのアクセスと VLAN の監視を MAC レベルで行います。通信は、常時更新可能なホワイトリストとブラックリストによってフィルタリングされます。そのため、新しい攻撃パターンにも迅速かつ効果的

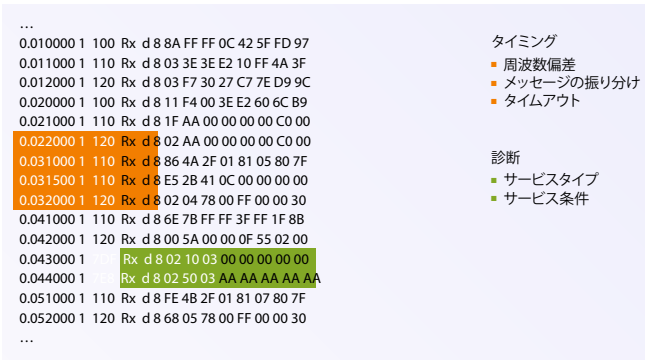



図 1：周期的メッセージの異常と診断要件の不正使用を検出する CAN IDS

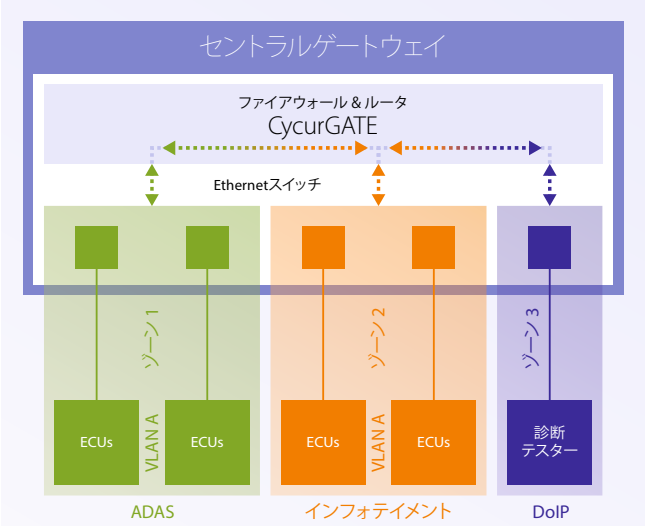



図 2：ゲートキーパーおよびルーター機能を担う車載 Ethernet ファイアウォール

に対応できます。

### インテリジェントな負荷分散

車載 Ethernet ファイアウォールを中央 Ethernet スイッチに実装することに加えて、ホストベースのファイアウォールを ECU に直接統合することも可能です。この場合は、リアルタイムでチェックを行ったり、個々のデータパケットのルーティングの有無やルーティング先を決定したりできる十分なパワーを持ったファイアウォールなど、高性能なソリューションが必要となります。ただし、この手法では、ステートフル SOME/IP 通信の周波数などの複雑な攻撃検出パターンをカバーすることはできないため、Ethernet IDS を追加して、メッセージ頻度やシーケンス、ペイロード、データ、サービスに基づいて異常パターンを検出し、これらを攻撃試行として記録およびレポートできるようにする必要があります。また、最適なパフォーマンスを達成するためには、スイッチとマイクロコントローラ間で負荷配分をインテリジェントに行うことが重要です。ファイアウォールと侵入検知の機能は、スイッチやターゲットコントローラに部分的に実装することができます。

CAN IDS、車載 Ethernet ファイアウォール、および Ethernet IDS を組み合わせると、大きな遅延を伴わずにハイブリッド E/E アーキテクチャを確実に保護することが可能です。また、これらを中心的なコンポーネントとして統合セキュリティコンセプトに組み込めば、ネットワーク接続を備えた未来の自動運転車両に伴うリスクを防止し、機能的安全を確保できるようになります。■


執筆者

**Jan Holle 博士**、ESCRYPT プロダクトマネージャ、侵入検知システム **Siddharth Shukla 修士**、ESCRYPT プロダクトマネージャ、車載ファイアウォール