Empowering Tomorrow's Automotive Software
www.etas.com

# 車両の侵入検知 ESCRYPT CycurIDS

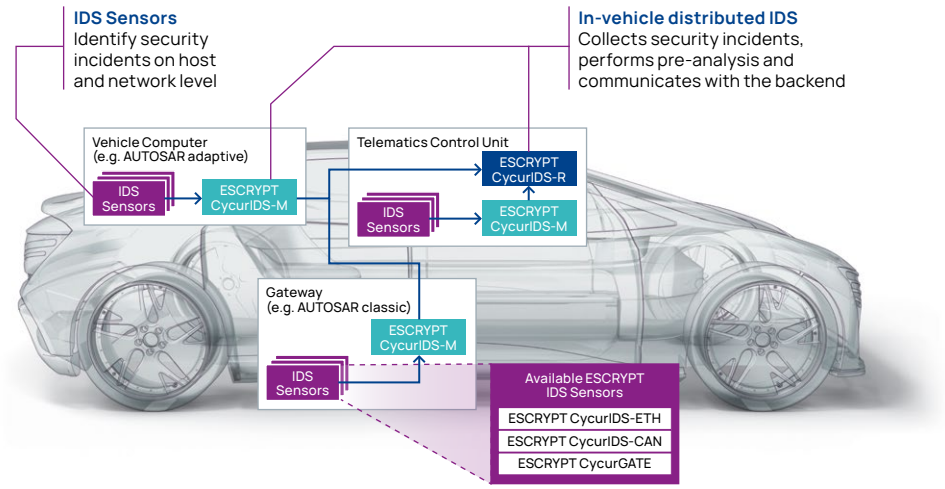
## ESCRYPT の侵入検知ソリューションによる継続的なセキュリティ監視

コネクティビティが拡大するにつれて、サイバー攻撃の手口が次々と生まれ、新たな抜け穴が出現しています。相互に接続された車両フリートに対するセキュリティの脅威は、車両そのものだけではなく、車両を管理するバックエンドサービスにまで及びます。

近年の UN-R155 の導入以来、自動車業界ではサイバーセキュリティの監視が最優先事項となっています。自動車メーカーや車両管理者は、自社の車両のライフサイクル全体を通して効果的なセキュリティリスクマネジメントを実施することが求められています。

これを達成するための要素の一つが、車両の侵入検知システム（IDS）を介した攻撃検知です。異なるシステムと通信プロトコルが存在する分散型 E/E アーキテクチャの要件、高い性能要求、リソースやストレージの制限といった課題がある中、車両にとって有効な IDS ソリューションとはどのようなものなのでしょうか。

ETAS ではネットワークベース IDS である CAN/CAN-FD 用の ESCRYPT CycurIDS-CAN と イ ー サ ネ ッ ト 用 の ESCRYPT CycurIDS-ETH、および個々の ECU に最適化されたホストベース IDS を提供することで、さまざまな世代の車両に合わせてカスタマイズ可能なソリューションを提供しています。さらに IDS マネージャ（ESCRYPT CycurIDS-M）と IDS レポータ（ESCRYPT CycurIDS-R）が車両の分散型侵入検知システムを実現します。




**車両の分散型 IDS アーキテクチャ**

- ESCRYPT CycurIDS-CAN、ESCRYPT CycurIDS-ETH、ESCRYPT CycurGATE はスマートセンサの役割を果たし、潜在的なセキュリティイベント（SEV）を収集し、事前に選択することで迅速に正確な分析を実施
- ホストベースの IDS が ECU のリスクを監視
- ESCRYPT CycurIDS-M はセキュリティイベントを収集、分析、集約、保存し ESCRYPT CycurIDS-R に通知
- ESCRYPT CycurIDS-R は車両からのセキュリティイベントを車両セキュリティオペレーションセンター（VSOC）に通知

# 車両侵入検知ソリューションのコンポーネント

ETAS の車両侵入検知ソリューションは、複数のコンポーネントで構成されています。IDS センサには ESCRYPT CycurIDS-CAN と ESCRYPT CycurIDS-ETH があります。IDS センサの特徴は以下のとおりです。
- IDS マネージャと完全に相互運用性があり、CAN やイーサネット上の侵入を検知する「スマートセンサ」として機能
- GUI ベースのコンフィグツールを使った自動ルール生成やシミュレーションの構築が可能
- 異常の報告とロギングを車両上にも、セキュリティオペレーションセンター（VSOC）向けにも実施

## ESCRYPT CycurIDS-CAN

- 転送された CAN トラフィックのモニタリング、潜在的な攻撃（異常）の検知
- ECU 上でヒューリスティック、シグネチャベースの検知

### 検出機能の例

- メッセージの頻度を観察して「メッセージインジェクション」を検出
- バス上のすべてのメッセージをホワイトリストと比較し、未指定のメッセージを検出
- 特定の ECU をシャットダウンしようとする試みなど、悪意のある診断要求を走行中に検出

## ESCRYPT CycurIDS-M

- 車載 ECU 用セキュリティイベント管理
- 2 種類のバリアント：
  - 組み込み ECU 用
  - 高性能 ECU 用
- お客様のあらゆる集約、保持、レポート戦略に対応するため柔軟に拡張できるよう設計された AUTOSAR 準拠のソリューション
- TAS4:
  セキュリティイベントを迅速かつ効率的に選択することで保存コストと処理コストを低減することが可能
- TAS4：
  生成されたセキュリティイベントに従って、車両全体のコンフィグレーションが簡単に生成できる

## ESCRYPT CycurIDS-ETH

- イーサネットトラフィックのモニタリング、潜在的な攻撃（異常）の検知
- さまざまな世代のイーサネットベース E/E アーキテクチャ向けに、車載侵入検知を実現
- μ C/ μ P に加え、イーサネットスイッチ上でも動作

### 検出機能の例

- 仕様、異常、シグネチャベースの侵入を検知
- SOME/IP、DoIP といったアプリケーションレイヤプロトコルへの悪意のある攻撃を検知
- メッセージの頻度、シーケンス、車両の状態などを観察して異常のパターンを検知可能

## ESCRYPT CycurIDS-R

- 車両のセキュリティイベントをレポート
- カスタマイズ化されたソリューションにより、車両セキュリティオペレーションセンター（VSOC）に接続
- IDS 通信機能のプロビジョニングをカプセル化
- セキュリティ要件を満たす隔離実装が可能
- ESCRYPT CycurIDS とシームレスに統合

## ESCRYPT CycurIDS のアドバンテージ

- 走行中の攻撃をタイムリーに検知
- 実車で実証済みのすぐに使えるソリューション
- IDS センサとセキュリティイベント管理やレポートを包含する、車両侵入検知のための包括的なソリューション
- ESCRYPT の侵入検知 / 防止ソリューション（IDPS）とセキュリティオペレーションセンター（VSOC）と連携
- AUTOSAR 準拠のコンポーネントが現行の車両品質要件を満たすとともに、制限のある ECU のリソースを最適化
- ホワイトボックス、かつトランスペアレントなセキュリティアプローチにより、自社のサイバーセキュリティポリシーを管理可能
- UN-R155 などの規制にも準拠

ETAS の製品とソリューションに関するお問い合わせ：
**info@etas.com**

製品の詳細情報：
**www.etas.com/CycurIDS**

ETAS/COM-JP/03-2023