escrypt
Embedded Security by ETAS

侵入検知&防御

攻撃検出、 ポリシー適用、 リアルタイム解析

コネクテッドビークルをサイバー攻撃から確実に保護できるのは、 統合型のセキュリティソリューションだけです。こうしたソリューションでは、 車両のライフサイクル全体で起こりうるあらゆるリスクシナリオを考慮に入れる必要があります。 したがって、 運転中に車両のセキュリティ状況の概要を随時把握しておくことは不可欠です。

信頼性の高いリアルタイム検出とポリシー適用

ESCRYPT の侵入検知 & 防御ソリューションは、 路上の車両をサイバー攻撃から確実に防御します。

このターンキーソリューションの中心に組み込まれているコンポーネント「**CycurIDS**」は、 車内通信における異常の認識を、 一部は既知の攻撃パターンに基づいて、 一部は現在の通信と予想される通信動作との比較に基づいて行います。 この方法により、 CycurIDS は、 強力なリアルタイム検出を行い、 車両の安全性が重視されるシステムに悪意ある通信が認識されずに到達するのを防ぎます。

CycurGATE は、さまざまな車載ネットワーク技術（CAN、イーサネット）用のファイアウォールであり、 既存のシステムに容易に統合できます。 CycurGATE は、 通信ポリシーの適用に基づいて、 個々の ECU またはネットワーク全体にコマンドを送信しようとする試みをブロックします。このポリシー適用では、 ホワイトリスト（明示的に指定された通信フローのみを許可するリスト）をブラックリスト（既知の攻撃を防ぐためのリスト）で修正します。 侵入防止策として、 適用するファイアウォールのルールセットを新しいルールや改訂したルールで更新できます。

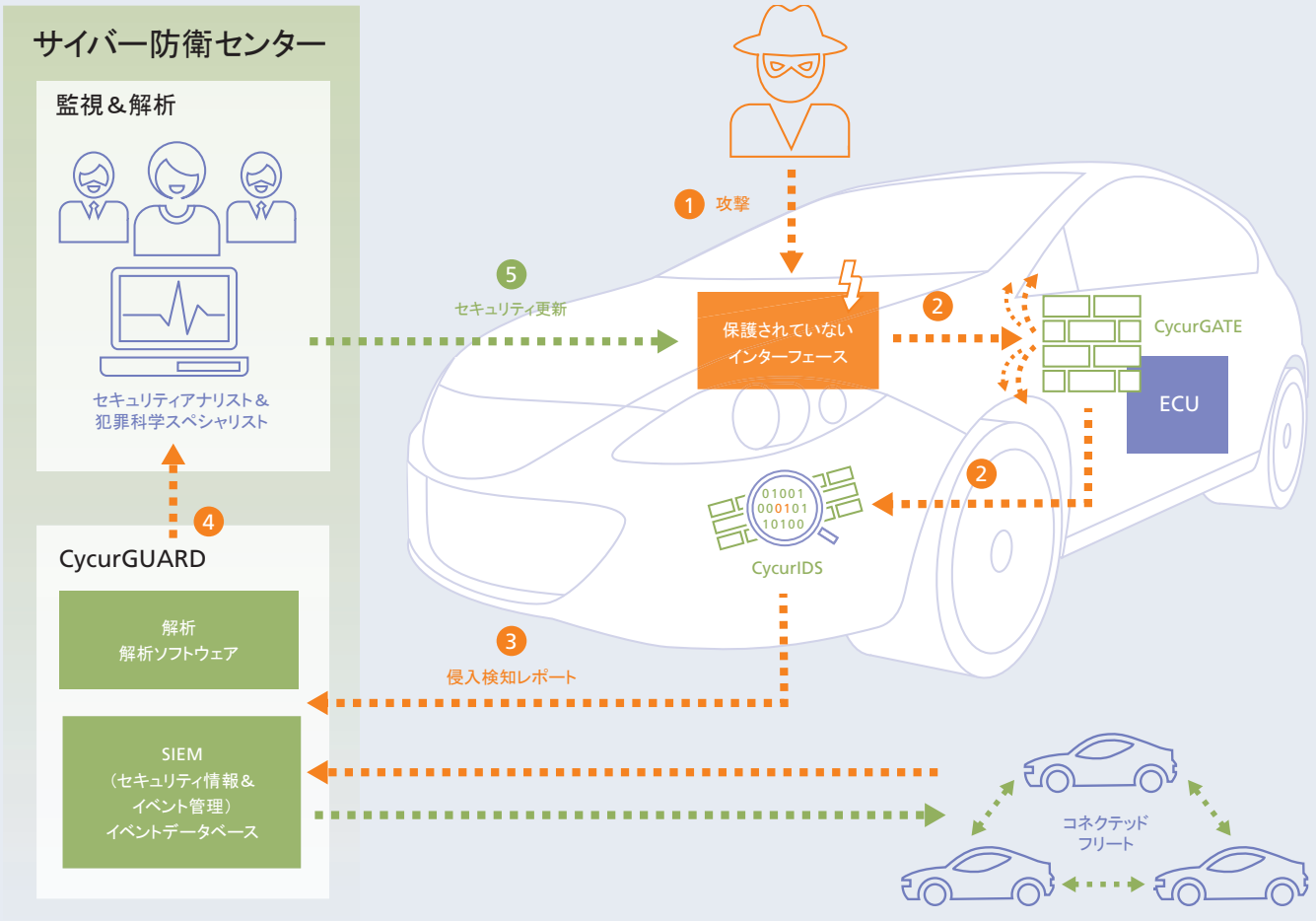
サイバー防衛バックエンド ー 車載セキュリティのビッグデータ

CycurIDS は、 個々の自動車のセキュリティイベントを監視します。 **CycurGUARD** は、 コネクテッドフリート全体からのデータを解析して新たな脅威の識別を可能にします。ESCRYPT は、ビッグデータ解析技術に基づく監視バックエンド製品を活用して、 運転中の車両の異常レポートの収集と解析を行う統合型ソリューションを提供します。既知の攻撃パターンのデータベースは拡大し続けていますが、 CycurGUARD は、 この膨大なデータベースを参照し、 重大な脅威を確実に識別します。 一時的な、 または既定のレポートを使用することで、コネクテッドフリートの安全性とセキュリティの評価、 変化の識別、 問題領域へのリソースの集中、 新しい脅威の先読みが容易になります。

ESCRYPT 2016/11

escrypt
Embedded Security by ETAS

侵入検知＆防御



お客様の利点

- 現在の E/E アーキテクチャですぐに使用できる攻撃検知ソフトウェアソリューション
- 実際の攻撃を確実かつリアルタイムに識別
- 攻撃を瞬時に防御できるため、 高コストとなるリコールを回避
- ワランティクレームを回避
- 車内のデータセキュリティに対する法定要件と規制要件に準拠
- 市場にある各車両モデルのセキュリティの概要を把握
- セキュリティ概念の開発の焦点を絞ることができるため、 さらなる開発の効率をアップ

当社の主なサービス

- ソリューションコンサルティング
- セキュリティソリューション設計
- カスタム実装（プロセス、ソフトウェア、ハードウェア）
- 管理されたセキュリティサービスと保守
- トレーニング、 サポート、 認証サービス