

# “調和のとれた相互連携”

## Thomas Wollinger博士がコネクテッドカーの包括的なセキュリティを語る

大変革期を迎えた自動車業界。時代の岐路に立つ自動車産業を成功に導くファクターとして、自動車セキュリティが注目を浴びています。ESCRYPT GmbHのマネージングディレクター Thomas Wollinger 博士が、人々の認識と行動がどう変わっていくか、そして変革にはなぜ指揮者が必要なのかを説明します。

**Wollinger 博士に伺います。自動車業界では、セキュリティの問題に対する意識が高まり始めていますか？**

**Thomas Wollinger 博士：**

はい、セキュリティへの意識が形になっていくのを実感しています。今後が楽しみです。この業界は、構造的な変化に直面しています。自動車販売への依存度を下げ、データ重視のサービスに重きを置いた、まったく新しいビジネスモデルもその一つです。デジタル化とコネクティビティの実現が加速するにつれ、私たちは静的制御装置を搭載した従来の車両プラットフォームの終焉と、ネット接続された分散 ECU を搭載したイーサネットベースのプラットフォームの到来を目の当たりにしています。個別の組み込みセキュリティ機能では、もはや太刀打ちできません。車の枠を超えた考え方と行動、そして包括的なアプローチが求められているのです。

**具体的にはどうということですか？**

**Thomas Wollinger 博士：**

私たちが将来について語る時、ネット接続された自動運転が話題に上ります。自動運転の実現にはデータのリアルタイム通信が不可欠ですが、このことは攻撃の標的が増大すること、そしてまったく新しい脅威が形成されることを意味します。ネットワーク内に車両が移動するコンピュータとして存在するとき、IT セキュリティは「人の安全」という重要な課題に直面することになります。

システムとしての自動車を完全に守る必要があるとともに、車車間の通信や、車両と沿道に設置された装置との通信、交通インフラ自体を守らなければなりません。さらに、自動車ライフサイクルの最初から最後までを、見届けなければなりません。公道を走る車を、未だ経験したこともないサイバー攻撃手法から 15 年以上にわたって守る必要がある

のです。それを達成することは取りも直さず、適切なプロセスと組織が最初から整備されていなければならないことを意味します。ESCRYPT が考える包括的な自動車セキュリティは、システムとインフラストラクチャ全体に対して効果的な防御を実施します。それをライフサイクル全体に適用し、それに応じた組織的支援を行うのです。

**理論は理解しました。では、それをどのようにして実行に移しているのでしょうか？**

**Thomas Wollinger 博士：**

その最たる例が侵入検知・防御ソリューションです。車載セキュリティソフトウェアがセントラル ECU とゲートウェイを監視します。電気システムの通信に異常が検出されると、異常が記録されて、バックエンドのセキュリティオペレーションセンターに転送されます。集約されたデータはそこで各種ツールによって分析され、万が一サイバー攻撃であった場合は、規定されたインシデントレスポンス措置に沿って、フリート全体に対してセキュリティアップデートが実施されます。1 台の車両が標的にされるとすぐに新たな攻撃パターンが検出されるため、フリート全体を守るための措置を直ちに講じることができるのが、その大きな利点です。IT セキュリティ機構がライフサイクル全体にわたって持続的に効果を発揮し、組織によって守られるという、ある種の免疫機能を構築します。

**つまり、自動車メーカーのフリートに対する IT セキュリティは、セキュリティ対策そのものよりも、それらをどう連携させて管理するかの方がはるかに重要になってきているのですね。**

**Thomas Wollinger 博士：**

おっしゃるとおりです。OEM にとって、車両フリートを守ることが今後、複雑かつきわめて重要な不変の課題になるでしょう。そのためには予測のコンセプトや具体的なセ

Thomas Wollinger 博士 -  
ESCRYPT GmbH  
マネージングディレクター



セキュリティ体制、適切なリソースが必要となります。そしてセントラルセキュリティ管理機能が不可欠です。セントラルセキュリティ管理機能が、あらゆるセキュリティ対策に調和のとれた相互連携を確保し、OEMのすべての関係者と外部のサービスプロバイダー、サプライヤー、ワークショップ参加者にガイダンスを提供するのです。これはまさに指揮者がオーケストラを統率して演奏を作り上げる様子を思わせます。

自動車メーカーは既に主要事業のプロセスや要件を指揮しています。それと同様に将来は、自動車のセキュリティも指揮することが必要になるでしょう。効果的なITセキュリティがなければ、スマートモビリティを実現することはできないのです。

「ネットワーク内に車両が移動するコンピュータとして存在するとき、ITセキュリティは「人の安全」という重要な課題に直面することになります」