車載ソフトウェアのセキュリティ

SECURITY OF IN-VEHICLE SOFTWARE

はじめに
INTRODUCTION

現代の自動車はハードウェアとソフトウェアの複合体であり、もはや機械工学の領域のみにとどまるものではありません。特に安全に関わる機能をソフトウェアで制御する傾向はますます高まっており、車一台に搭載されるプログラムコードは数百万行にも及ぶと言われています。

今日の車両には、数多くの有線/無線インターフェースが搭載されており、それらを介して外部アプリケーションやデバイス、ネットワークに接続することで、快適で安全な走行環境の提供を実現しています。しかしそれは同時に、長距離/近距離無線インターフェースを利用した、車載システムへの不正アクセスを可能にするなど、車両が外部からの影響や、ソフトウェアの脆弱性を狙った悪意ある攻略の対象になり得ることを意味しています。ソフトウェアへの依存が進み、今まで以上に外部露出の機会が増えることで、車両に対するサイバー攻撃の脅威は格段に高まりつつあるのです。

自動車産業におけるサイバーセキュリティのリスクは、いわば乗車している人々の安全を脅かすリスクに他ならず、そのため自動車や交通の安全に関わる全ての人々が取り組むべき新たな課題と言えます。しかし、車載ソフトウェアのセキュリティを今後どのように担保していくのか、そのために業界や規制当局はどのような役割を果たすべきなのか。これらの疑問に対する最終的な回答はいまだ出ていません。

セキュリティ問題とは

PROBLEM DEFINITION

自動車セクターにおけるサイバーセキュリティの状況

自動車産業における セキュリティ関連動向

この10年間、自動車業界は情報化時代への過渡期にあると言われてきました。コンピューター化が進み、多くの価値ある機能が追加され、車の性能が上がるとともに、ドライバーの安全性、利便性も向上しました。最近では車の接続性、自動化、データ分析といった分野への応用も進んでおり、こうしたITの活用は今後もさらに拡大していくと考えられます。特に車車間通信、自動運転、自動交通管理システム、遠隔制御機能は、開発が盛んに進められている技術の一例です。

しかし、この傾向はメリットと同時に、車に対して想像以上の複雑性をもたらします。今日、車両に搭載されている電子制御装置（ECU）は20から100種にのぼり、プログラムコードも数百万行に達すると言われています。さらに、キーレスエントリー、タイヤ空気圧モニタリングシステム（TPMS）、インフォテイメント＆テレマティクスシステム、インターネット接続型モバイル機器とのペアリングや統合、第三者OBD-IIアダプタといった無線通信機能を備えた部品の数も増加しています。

セキュリティが示唆するもの

セキュリティに関する最近の傾向として、攻撃対象範囲の拡大、プライバシー侵害リスクの増大、そしてソフトウェアの脆弱性/弱点を悪用する攻略リスクの増加が挙げられます。

このような状況の中、自動車業界はセキュリティ分野の専門家らから厳しい視線を向けられており、結果として自動車関連企業や政府、そして市民のサイバーセキュリティに対する関心を高める原動力となっています。例えば、2015年に、ある研究者グループが無線通信の脆弱性を利用してジープ車をハッキングし、安全上重要な機能を遠隔操作する様子が大きく報道され話題を呼びました。* この研究により、攻撃者は車両に接近しなければ車の制御を奪うことはできない、という自動車業界におけるかつての前提が覆される結果となりました。

上に挙げた「Jeep Hack」は最も有名な事例ですが、この他にも様々な有線/無線インターフェースをターゲットとした攻撃成功例が報告されており、自動車をとりまくサイバーセキュリティの現状と妥当性に疑問が生じています。兼ねてより、機能安全については自動車の開発に不可欠な要素であるとして、多くのメーカーが独自の基準を設け対応してきました。一方で通信技術の発達により新たに生じた「セキュリティ、安全性、プライバシー」問題については、万全な対応が行われているとは言いがたい状況です。セキュリティ開発ライフサイクルの導入や、多層防御、さらにはOTA（Over-the-air）ソフトウェアアップデートといったセキュリティ上重要な機能を組み込む「ベストプラクティス」の採用についても、近年では増加傾向にあるものの、いまだ一般的とは言えません。サイバーセキュリティについて、自動車業界は各メーカーによる対応強化を進める一方で、規格開発機関やセキュリティ専門家、規制当局と協力し、指針の策定への取り組みを始めるなど業界全体としての対策を進めています。

解決すべき問題とは

セキュリティ問題に対する認識が急速に高まったことで、自動車業界においても数々の対策が取られるようになってきました。しかし、セキュリティが確保された未来への道のりは長く、業界が一丸となったセキュリティ対策への取り組みが求められています。IoTなど他の業界に倣い、「ベストプラクティス」に対応し取り入れることで、以下のような自動車業界におけるセキュリティへの課題を解決していく必要があります。

人材の確保：他のIoT分野と同様、自動車の分野においてもサイバーセキュリティ対策に必要な能力や知識、スキルを有する人材が不足しています。セキュリティと自動車の両方の知識を備えた人材を育てるために、セキュリティの専門家と自動車の技術者に対しトレーニングを実施する必要があります。自動車メーカーは、この両分野の知識を備えたセキュリティチームを社内に組織し、チームの決定事項を共有することで開発サイクルにセキュリティ対策を組み入れていく体制を築く必要があります。

長期的な開発サイクルを見据えたセキュリティ対策：自動車の開発サイクルは長期間に及ぶため、車載システムの中には最新の脅威に対応できないものもあります。増加するハッキング攻撃に対応する為、自動車メーカーは、未来を見据えた設計を行うと同時に、セキュリティが担保された遠隔での更新を可能にするなど、自動車のライフサイクル全体を通じて強固なセキュリティを保証し続ける必要があります。

サプライチェーンを含む包括的なセキュリティ対策：自動車のサプライチェーンは膨大で、それゆえに管理プロセスが複雑になってしまう可能性があります。車両全体を管理するためには、セキュリティに関する要件を統合し、サプライチェーンを含めた包括的な保証を提供していく必要があります。

セキュリティ領域における規制の在り方：サイバーセキュリティの領域は変化が激しく、そのため規制を策定するのが困難です。また、規制が参照するセキュリティ基準に対する批判も多く存在します。例えば、セキュリティの考え方として、100パーセント完璧なセキュリティはありえないという「リスクベース・セキュリティ」の考え方が採用されにくく、誤ったセキュリティ対策の原因となりうる「チェックリスト方式」に偏りがちになるというのもそのひとつです。自動車産業における規制のあり方、その対象範囲をどのように考えるべきか、いまだ課題が残ります。

セキュリティの向上で交通安全を目指す

SECURE VEHICLE FOR SAFER ROADS

自動車のサイバーセキュリティの将来像

自動車セキュリティは比較的新しい分野であり、最近になりようやく車載システムのセキュリティ確保の困難さや検討すべきリスクなど、山積する課題が関係者に認識されるようになってきました。こうした課題の解決法を探る取り組みはまだ始まったばかりですが、不確実な状況にあっても、今後セキュリティが全ての分野において主要検討事項になるのは明らかと言えます。自動車の機能安全に関するリスクが政府機関や自動車メーカー、そして一般市民に広く認識されているように、今後はセキュリティの面においても広く意識されるようになるでしょう。
自動車のセキュリティが確保された未来を築くために、次のことが重要であると考えられます。

セキュリティに対する機能安全と同等レベルの取り組み

自動車は輸送システムの一画を担う重要なインフラです。その為、車上荒らしから国家レベルの攻撃まで、さまざまな種類の攻撃を受ける可能性が考えられます。セキュリティに対する認知度の高まりに合わせ、取り組みも強化していくべきでしょう。例えば、善意のハッカーであるセキュリティ専門家が自動車を対象に研究を行い、その成果が注目されたことで、セキュリティ関係者や自動車業界、一般市民の自動車のセキュリティに対する認識が劇的に向上した事例があるように、自動車業界はこうした善意のハッカーの専門知識や研究の成果を活用することで、セキュリティに対する意識を向上させていくことができます。

また将来的には、悪意ある攻撃の実例やセキュリティ調査報告の公表など、セキュリティに関する報道やニュースに触れる機会がさらに増えることが予想されます。セキュリティの問題が起こることで、システムの安全性、データやプライバシーの保護、ブランドや企業イメージが影響を受ける可能性が高まり、そうした状況の中で機能安全と同じくセキュリティもまた最優先事項として取り扱われるようになるでしょう。

セキュリティと機能安全への総合的な対処

車載システムの機能安全に対して、自動車産業はすでに十分な対応をとってきました。しかし安全とセキュリティについては完全に別々に運用され、両者への対応を意図した規格もほとんど整備されていないのが現状です。

セキュリティと機能安全は、製品設計に安全・セキュリティを構築するというゴールを掲げている点で共通しています。その為、既存インフラや人材を活用して、車載ソフトウェアのセキュリティレベルを上げることは不可能ではありません。同様に自動車のセキュリティ対策は新しい分野ですが、業界に深く根付いている安全の文化とシステム技術の考え方を取り入れることが可能で、効率性や一貫性・完全性の面から考えても、セキュリティと安全に対し総合的に対処することが望まれます。

法的枠組みと型式承認の要求事項の採用

特定の市場において、法的枠組みと自動車の型式承認の要求事項が、安全対策の進展に大きく貢献しました。先端技術を搭載したコネクテッドカーに対しても、同様の法的枠組みや型式承認を適用することで、道路を使用する人と自動車に乗る人、両方を守ることが可能になります。またセキュリティを車両の安全性を考える際の必須項目とするケースも増えており、セキュリティが確保されない限り、その自動車が安全であると責任を持って断定できなくなることは明らかです。

自動車サイバーセキュリティに特化した業界規格の採用

現在の安全基準（例：ISO 26262）はセキュリティの脅威に対応していないため、業界ごとに枠組み・規格を開発する必要があります。現在ISO（国際標準化機構）と自動車業界により、試験可能なセキュリティ基準を開発する取り組みが進められています。新たなセキュリティの事象が現れると、それに対応するため、車両のライフサイクル全体にわたって脅威を予測、防御、阻止、対処する仕組みとプロセスを作り出さなければなりません。こうした現状を踏まえ、自動車業界に特化した規格が求められているのです。

業界規格の開発において考慮すべき点は、以下のとおりです。

- **ワイヤレスアクセスポイントとデータ処理機能を有する車両は、ハッキング行為とセキュリティ侵害から確実に保護されていること**
- **脆弱性分析の侵入テストを用いてセキュリティシステムを検証すること**
- **リアルタイムでハッキング行為に対応する方策が含まれていること**
- **ドライバーがデータの収集、送信、使用を明確に認識できること**
- **データの収集、および、ドライバー情報の車外保存媒体への送信を中止できる選択肢がドライバーに与えられていること**

結論
CONCLUSION

ここ最近の調査によりサイバーセキュリティの重要性が明らかになりつつあります。接続性並びに安全上重要な機能などを制御するソフトウェアへの依存度はますます高まり、同時に自動車の脆弱性の数も増え続けています。こうした傾向は今後も続くと予測されています。自動車へのハッキングは時間と専門技術を要するため、現在のところ善意のハッカー集団による攻撃しか報告されていませんが、悪意あるハッキングの脅威が高まっていることは間違いありません。近い将来、セキュリティは車両の安全性を考える際の必須条件となるでしょう。
よりセキュアな自動車の未来を築くためのポイントを以下にまとめます。

・セキュリティに対する機能安全と同等レベルの取り組み
・セキュリティと機能安全への総合的な対処
・法的枠組みと型式承認の要求事項の採用
・自動車サイバーセキュリティに特化した業界規格の採用

自動車業界では、セキュリティの成熟度を上げる取り組みがあらゆるレベルで行われており、様々なプロジェクトや研究が進行中です。この動きを加速させていくために、優先度を上げて体制構築に注力していく必要があると言えるでしょう。

*出典: Valsek, Chris and Miller, Charlie. IOActive. 2015.
http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf.

株式会社 UL Japan 事業所案内

ul.com/jp

本社 〒516-0021　三重県伊勢市朝熊町4383-326
T: 0596-24-6717　F: 0596-24-8020

東京本社 〒100-0005　東京都千代田区丸の内1-8-3
丸の内トラストタワー本館6階
T: 03-5293-6000　F: 03-5293-6001

問い合わせ先
コンシューマーテクノロジー事業部
E-mail: ConsumerTechnology.JP@ul.com

本社安全試験所 〒516-0021　三重県伊勢市朝熊町3600-18
T: 0596-24-8008　F: 0596-24-8002

本社EMC試験所 〒516-0021　三重県伊勢市朝熊町4383-326
T: 0596-24-8999　F: 0596-24-8124

グローバルマーケットアクセス T: 0596-24-8116　F: 0596-24-8095

湘南EMC試験所 〒259-1220　神奈川県平塚市めぐみが丘1-22-3
T: 0463-50-6400　F: 0463-50-6401

横輪EMC試験所 〒516-1106　三重県伊勢市横輪町108
T: 0596-24-8750　F: 0596-39-0232

鹿島EMC試験所 〒289-0341　千葉県香取市虫幡1614
T: 0478-88-6500　F: 0478-82-3373

オートモーティブ テクノロジー センター (ATC) 〒470-0217　愛知県みよし市根浦町1-3-19
T: 0561-36-6120　F: 0561-36-6820

1801NS500_V1.0