



コネクテッド・カーによるソフトウェア更新



一般社団法人情報通信技術委員会
コネクテッド・カー専門委員会
TF Auto-OTA-Updating
(TFAOU) 主査
富士通株式会社

こ なたに
小 谷 誠剛



独立行政法人情報処理推進機構

つかもと たかし
塚元 卓

1. はじめに

これまでの長い期間、独立した個体として存在し、確固たる地位を築いて来た自動車は、近年、汎用ネットワークにつながるという意味でのコネクテッド・カーとして、大きな変貌を遂げつつある。1990年頃から一般化したパソコン等のネット接続から遅れる事20数年、後塵を拝している事は否めないが、人の命を預かるクルマとして、確たる意識、覚悟、かつ具体的な動機、利潤発生期待を持って、欧米日で進み始めている。

その過程で期待される多種ユースケースで共通的に必要となる機能の一つに、車載システムの遠隔ソフトウェア（広い意味で、クルマが保持する情報全般）のセキュアな更新がある。

本機能は、リプログラミングやフラッシングなどといった呼称の違い、また、処理対象の違いがみられるものの、様々な機関／組織で規格化、標準化の提案／協議が進められている。それらを迅速に収集、分析、把握、理解し、日本の施策に取り込む提案作業の一助とするために、遠隔ソフトウェア更新のうちOTA (Over The Air) 技術に係る種々の世界規模での活動を、車載システム遠隔更新技術の観点から集積、検討、分析したレポートが一般社団法人情報通信技術委員会 (TTC) から発行されている。本稿では、このレポート（以下、TR-1068）を引用しつつ、コネクテッド・カーにおけるソフトウェア（広い意味での車載情報）更新の現状と課題を紹介させていただく。

2. ソフトウェア更新の現状

近年の自動車においては走行制御（エンジン、ブレーキ、ステアリングなど）、ADAS制御（ACC、LKAなど）、マルチメディア（カーナビ、オーディオ、HUD、など）、ボディ制御（パワーウィンドウ、灯火制御、など）の各種機能を実現するために、自動車1台当たり数十個以上のECU（マイクロコンピュータ）が搭載されている。

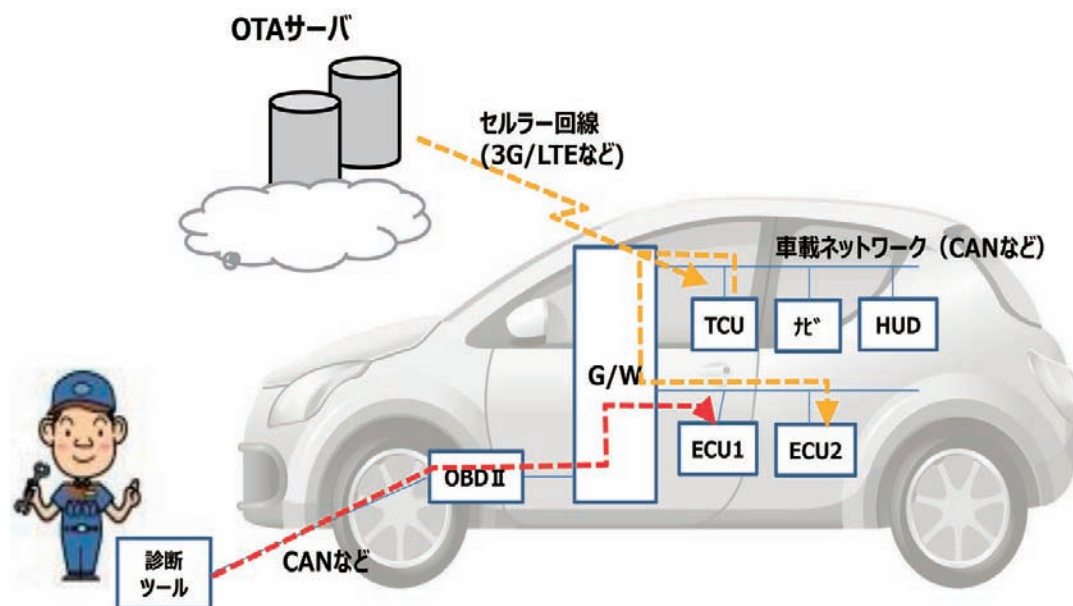
各ECU上では各々のソフトウェアが動作しており、車載ネットワークを介した協調制御を行うことによって、上記の各種機能を実現している。自動車に搭載されている各ECUのソフトウェアは、車両出荷前に各ECU内のメモリに記録されるが、車両出荷後に機能改善、新たなバグ発見／修復などのために更新される場合が往々にしてある。この車両出荷後のソフトウェア更新のことをリプログラミングと呼んでいる。なお、当然ながらパソコン、スマホ等では既に一般化している。

自動車におけるリプログラミング作業は、現時点での通例として、ディーラーや自動車整備工場（以下、ディーラー等）において、そこに運び込まれた自動車個々に対し、自動車整備士が専用の機器を用い、それを有線接続して実施される。しかし、近年はテスラなどが実用化したように、車両と車メーカーのサーバを無線接続し、遠隔から（専門作業者を介することなく）ソフトウェアを更新する技術も一般化しており、このような技術は遠隔ソフトウェア更新（OTAリプログラミング）と呼ばれている。この動きに対し、「人の命を預かるクルマ」として、なし崩し的实施がいかげんなのか、という懸念があるのも事実である。

OTAリプログラミングは、狭義にはECUのソフトウェア（OS、アプリ）が更新対象となるが、ソフトウェアのコンフィグレーションデータ、カーナビの地図データ、なども含め、広義のOTAリプログラミングと呼ぶ場合もある。ここではリプログラミング対象は特に限定せず、概要を紹介する。

図は、TR-1068に示されているリプログラミングのイメージ例である。

TR-1068では上記車載システム向け遠隔ソフトウェア更新のユースケースに着目し、国内外の政府機関、学術団体、業界団体、NPO等での、活動状況に関して調査を行った結果をまとめている。なお、TR-1068が参照した公開情報とは、特に断りがない限り2017年9月末日時点でのものである。



■図. リプログラミングの例 (赤色：従来の有線リプログラミング、黄色：OTAリプログラミング)

関連団体の活動内容、策定文書には様々な内容／段階があるため、それらを3つのレベルに分類すると分かりやすい。TR-1068ではそれぞれのレベルを、車両レベル、通信システムレベル、部品システムレベルとし、個々に以下の概要を紹介している。

各団体の章では、所定の様式として、各々の組織概要とその発行物（公開状況）に関して紹介。各発行物に関しては、概要として位置付けとその対象をまず明示し、遠隔ソフトウェア更新に関する記載内容、将来展望をまとめている。位置付け／重み付けとしては、規定、勧告、ガイダンス、仕様、技術報告、提案等に分類し、更に法的拘束力の有無について記載している。

① 車両レベル

TR-1068では標準規格の動向調査をスコープとしているが、この車両レベルの記載においてはUNECE WP29（国際連合配下の自動車基準調和世界フォーラム）などで策定が進められている車両レベルの基準・法規などに拡大して調査を行い、遠隔ソフトウェア更新（OTAリプログラミング）に係る要件に関して抽出を行っている。

検討の具体的な対象組織／団体名としては、上記UNECE WP29ITS/AD TFCSに加え、SAE、U.S.DOT/NHTSA、5GAA、ACEAなどがあげられる。

幸いな事に、WP29活動状況について、本特集に、国

交省交通安全環境研究所）新国様からの寄稿がある。このWP29に関する詳細は、そのページを参照していただくと幸甚である。

② 通信システムレベル

システムレベルとして、TR-1068ではITU-TやISOなどで策定している通信プロトコルに関する規格を調査し、OTAに係る要件に関して抽出を行っている。

ITU-TやISOなどで策定している通信プロトコルに関する規格が、ここに該当する。具体的な対象組織／団体名は、ITU-T SG16、ITU-T SG17、ISO TC22、ISO TC204、IEEE 802、Wi-Fi Alliance、W3C、Bluetooth SIG、oneM2Mなどがあげられる。

③ 部品システムレベル

システムレベルの中でもTCG (Trusted Computing Group) やEVITA (E-safety vehicle intrusion protected applications) などで策定しているチップなどの部品に関する規格を調査し、OTAに係る要件に関して抽出を行ってまとめている。即ち、同じシステムレベルの中でもTCG/EVITAなどで策定し、実際に自動車に実装されている部品に関する規格が、ここに該当する。

具体的な対象組織／団体名は、TCG、EVITA、HISなどがあげられる。



3. 課題の整理

実際の自動車内での適用／実装において、課題となる可能性が高いものの中で、例えばデータ転送時間の増大は、差分データ抽出／配信／インストール／事後検証や5G応用で解決の目的が立つ可能性が高まったと考えられる。

残る課題の主な類は、フラッシュメモリへの書き込み時間、リプログラミング前後の完全性チェック／証拠の担保、OTAリプログラミング処理中のセキュリティ攻撃等である。これらの攻撃への対策の高度化が必須であると考えられる。

少し視点を変えて見ると、自動車における遠隔更新技術の中での標準化に向けた課題整理は、TR-1068での分析どおりに関連各団体で検討されている途上である。

例えば、NHTSAは「テストはカーメカ、部品メカなどのエンティティが実施してもよいし、独立した第三者機関が実施することもできる」と述べているが、これは公開標準仕様にに基づく説明責任担保が前提と考えられる。

これらの説明は具体的な実現の面ではまだ十分整理されているとは言えない面もあると考える。即ちAccountability（第三者による説明責任性保証）が非常に重い意味を持つと考えられるが、明確な定義、推奨形態の提示が不十分なのではないかとの懸念が残っている。

Accountabilityに関して少し付言する。昨今の流れから、極めて遺憾ながら性善説ではなく、性悪説に立脚した対策を講じる必然性が高まっている。とは言え、完璧な対策構築に要する費用が膨大である事は自明の理である。取り分け、「人の命を預かるクルマ」においては、安全性の担保は必要不可欠である。

この状況において、現実解として、その意義を評価されつつあるのがAccountabilityである。即ち、その時点（過去のある時点、その後に発見されたセキュリティホール、脆弱性は対象外）で、最善を尽くした事実を、その後の、例えばトラブル発生時に、第三者によって検証／証明していただく、という事である。これによって、クレイマー等によるいたずらな訴訟、言い掛かりを排除できる可能性が増す、という事である。

これは、個々の被害者を救うに止まらず、全世界でのコスト削減に寄与する事が確実である。

さらに、自動運転にまで視野を広げると、自動運転用ダイナミック地図配信、EDR (Event Data Recorder)、TPMS (Tire Pressure Monitoring System) のセキュア化についても同等の対策が急務であると考えられる。ここに

においてもAccountabilityの重要性、意義は明白と考える。

これらの観点から、先に言及したNUECE WP29の活動、動静は非常に重大な意味付けになると考えられる。即ち、Accountability実現において、第三者による検証／証明性担保は、1つの国の範囲を超えて世界規模での検討、協議が必須であると考えられる。

4. まとめ

コネクテッド・カーとして通信機能を有し、利用する自動車において、車載システムのソフトウェアを遠隔で更新する技術の国内外の諸団体における検討状況について、TR-1068での記述に基き、課題の整理を目的に考察した。

TR-1068で述べられているように、各々の組織／機関で、車載システムの遠隔更新（ソフトウェア、それらが扱う情報も含め）に関し、多種多様の検討が活発に行われていることが把握できる。その中で遠隔更新を実現する際に要求されるセキュリティの重要性、Accountability実現の意義は非常に高く、セキュリティ攻撃への対策の強化、それ故、公開標準仕様にに基づくチップその他による説明責任担保が重要であることが示唆されている。

車載システムの遠隔更新の普及に当たっては、具体的なユースケースにおける価値（お金を生むか?）、有効性／利便性、が確実に認められる必要がある。広く知られているように、自動車業界はコスト意識が極めて高い。日米欧で近い将来の実現を目指した自動運転、車体そのものを工場に運び入れずに済ますリコール対策が検討されている現時点において、車載システムの遠隔更新、Accountability担保によるクレイマー対策強化は極めて有意義であると考えられる。

5. おわりに

クルマでのリコールは近年、数百万台／件に及び大きな課題になっている。種々の原因の内、現時点で約3割がソフトウェアによるものと言われ、この割合は将来増大する事が確実視されている。

パソコン／スマホ等と同様にクルマ自体を回収する事なく、リモートで改修する事が可能になれば、メーカーのみならずユーザも恩恵を手にと考えられる。本稿のベースとなっているTR-1068の内容に関しては、以下のURLを参照していただきたい。

http://www.ttc.or.jp/jp/document_list/pdf/j/TR/TR-1068v1.pdf