コネクティッドカー向け車両管理システム

Fleet Management System for Connected Vehicles

矢野　純史*
Junji Yano
高木　建太朗
Kentarou Takaki
村吉　諄之
Tomoyuki Murayoshi
羽賀　剛
Tsuyoshi Haga
滝本　周平
Shuhei Takimoto
田中　亮
Ryo Tanaka

世界中の多くの自動車メーカは、車両販売ビジネスからモビリティサービスビジネスへとシフトしており、当社もコネクティッドビジネス領域への参入を進めている。情報ネットワーク研究開発センターでは自動車事業本部のシステム事業部、CAS-EV開発推進部、及び㈱オートネットワーク技術研究所と共に車載機及び車載ソフトウェアや車載データの管理と分析を行うソリューションを試作開発している。当社では新たに、本技術を活用したコネクティッドカー向け車両管理システムの製品化を目指しており、その取り組みを紹介する。

Many motor vehicle manufacturers around the world are shifting from the vehicle sales business to the mobility service business. Participating in the connected business area, the Information Network R&D Center is developing a prototype solution for managing and analyzing in-vehicle devices, in-vehicle software, and in-vehicle sensor data together with Systems & Electronics Division, CAS-EV Development Promotion Division, and AutoNetworks Technologies, Ltd. This paper introduces our efforts in commercializing fleet management systems for connected vehicle in the future.

キーワード：CASE、コネクティッド、車両管理、OTA

1. 緒　　言

次世代コネクティッドカーでは、CASE時代に対応したコネクティッドサービス実現のため、車両の電気／電子アーキテクチャがセントラル化、集中制御化され[(1)]、アプリケーションを含めたソフトウェアは車外からのOTA※1により頻繁に追加、更新されることが想定される。ただし、車両のライフサイクルは長いため、全ての車両にコネクティッドデバイスが装備される本格的なコネクティッド時代になるまでの過渡期には、非コネクティッドカーである既販車をコネクティッド化することが考えられ、その一つの手段が後付け車載機の搭載である。当社においても既販車をコネクティッド化するための後付け車載機（Drive Link※2）を製品化しており、当該ビジネス分野に本格的に参入しようとしているところである。

一方で車外とのインタフェースが増えることで、車両が脅威にさらされるリスクも高まる。日々進化する多様なモビリティサービスに対応するため、車載機上でアプリケーションやサービスソフトウェアが動作することを想像することは難しくなく、通常のWebサーバやスマートフォンアプリと同様に悪意ある第三者のターゲットになる可能性は高い[(2)]。安心安全を提供するために、車両で動作するアプリケーションやソフトウェアの管理を行うことは、リスク低減のための必須項目の一つであると考えられる。

そこで我々は当該課題を解決するため、車両上で動作するアプリケーション、ソフトウェアの管理を行う「車載アプリケーション管理技術」の開発を行った。また車載アプリケーション管理技術を活用して、車両上のアプリケーション、ソフトウェアを継続的に運用保守するためのシステムである「車載アプリケーションライフサイクル管理システム」の開発を行った。

当社は当該分野の技術開発、試作、製品化を先行的に行い、当社の得意分野である物流ソリューション[(3)]や当社車両運行管理システム（Eagle Sight※3）と連携し、物流DX※4を促進させる自社車載機システムとして展開することを考えている。

以降2章で車載アプリケーション管理技術の内容、3章で車載アプリケーションライフサイクル管理システムの内容を説明し、4章に結言として、今後の進め方を述べる。

2. 車載アプリケーション管理技術

車載アプリケーション管理技術は、車載機とクラウドが連携して車両で動作するアプリケーションを管理する技術である。具体的には、「実行状況監視機能」「構成情報監視機能」「更新管理機能」「ID／アクセス管理機能」「ログ管理機能」といった機能で構成している。**図1**は車載機にアプリケーション管理技術を適用した場合のイメージである。

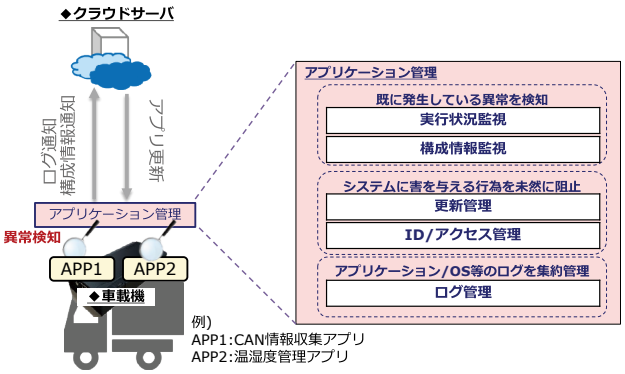

図1　車載アプリケーション管理技術

本技術により、車両上で発生している異常を素早く検知したり、システムに害を与える行為を未然に防止（堅牢化）したりすることが可能となる。

本章のまとめとして、各機能の処理を以下で説明する。

2−1　実行状況監視機能

アプリケーション異常検知のため、状態遷移異常、制御フロー異常が発生していないか監視する。

図2　認証がバイパスされたことを検知

2−2　構成情報監視機能

車両の安定稼働のため、車内の構成情報（バージョン等）を監視し、クラウドへ定期的に通知する。

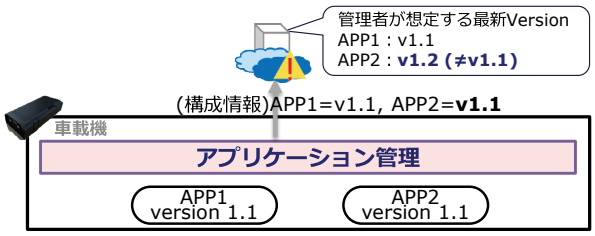

図3　定期的にアプリケーションバージョンを送付

2−3　更新管理機能

不正なアプリケーションの侵入を防ぐため、デジタル署名等を使って正規のアプリケーションであることを検証する。

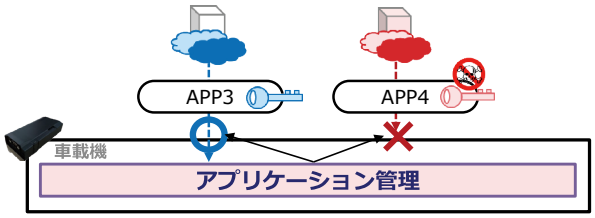

図4　信頼できない署名をブロック

2−4　ID／アクセス管理機能

不正アクセス防止のため、アプリケーションがアクセスできる保護資産を管理する。

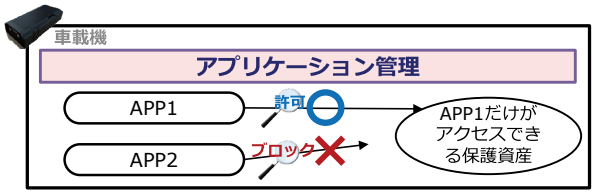

図5　権限がないAPPのアクセスをブロック

2−5　ログ管理機能

システムの稼働確認や異常発生時の分析を素早く行うため、アプリケーションやシステムのログ構成や配置場所を管理する。

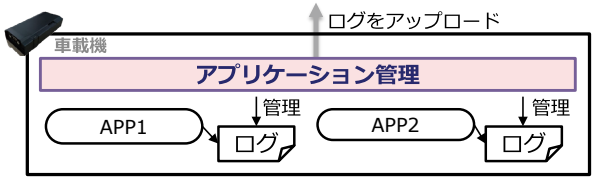

図6　APPのログの場所を把握

3.　車載アプリケーションライフサイクル管理システム

車載アプリケーションライフサイクル管理システムは、前述した車載アプリケーション管理技術をベースに、車両に搭載されているアプリケーションやソフトウェアのトレーサビリティの確保や継続的な運用・保守を実現するためのシステムである。

システムを構成する主な機能としては「OTA 機能」「構成管理機能」「データ蓄積機能」「分析機能」があり、これらは車載機クラウド連携を実現するための車載機クラウド連携プラットフォームと呼ぶことができる。**図7**は車載アプリケーション管理システムのシステム構成図である。

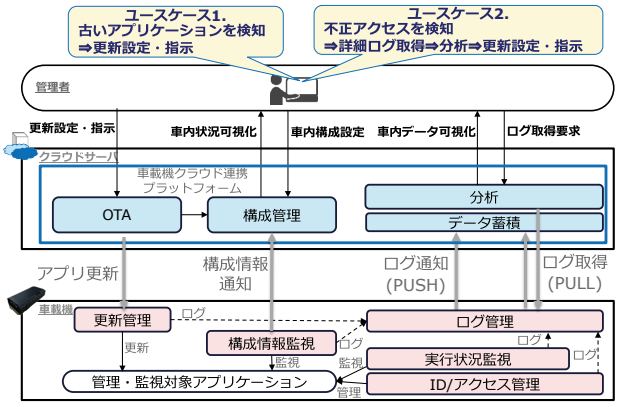

図7　車載アプリケーションライフサイクル管理システム

各機能の内容は次の通りである。

3−1　OTA 機能

車載ソフトウェアを遠隔から更新するための仕組みを提供する。具体的には更新用ソフトウェアの管理や更新スケジュールの管理、更新発生した際の車両への更新通知を行う。

3−2　構成管理機能

車載ソフトウェア・ハードウェアの動作状況（健全に動作しているか等）を把握するため、車載ソフトウェア構成（ソフトウェア名・バージョン等）やハードウェア構成（ハードウェアインタフェースに接続されているデバイス等）を管理する。

3−3　データ蓄積機能

車両の状態把握や分析のため、車両からアップロードされたセンサデータやシステムのログデータを蓄積する。

3−4　分析機能

異常発生時の原因究明や、データドリブンのサービス立案、改善のため、蓄積されたデータの可視化、分析を行う。

本章のまとめとして、システム運用時に極めて重要となる代表的なユースケース (a)、(b) を紹介する。

なお紹介する画面は実際に「車載アプリケーションライフサイクル管理デモシステム」を構築した際の可視化用 PC で取得したスナップショット画面である（※一部見やすさのため本稿用に文字を追記している）。

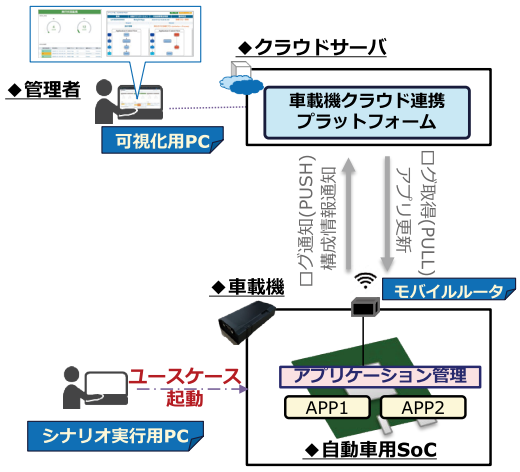

図8　車載アプリケーションライフサイクル管理デモシステム構成

(a) 古いアプリケーションを検知し更新

1) システムが特定車両で古いバージョンのアプリケーションが稼働していることを検知
2) 管理者は更新用アプリケーションを選択
3) システムは車両に更新を依頼
4) 車両は指示に従いアプリケーション更新，完了後クラウドに完了通知を発行

以下管理画面の遷移例を示す。

図9　システムはECU Xに搭載されているアプリケーションBodyCtrlSubAppのバージョンが最新バージョンでないこと検知する（図中破線部）。管理者は当該箇所をクリックして詳細を表示する。

図10　管理者は最新バージョンへ更新するのが最適と判断し（図中破線部①）、システムに当該アプリケーション更新を依頼する（図中破線部②をクリック）。

図11　システムは管理者の指示を受け、車両に当該アプリケーションの更新指示を出す（OTA）。画面上では状態が更新中となる（図中破線部）。

図12　車両はシステムからの依頼を受け、当該アプリケーションの更新を行い、完了後システムに完了通知を発行する。画面上では状態が更新完了となる（図中破線部）。

(b) 不正アクセスを検知、詳細ログ取得し分析

1) システムが不正アクセスを検知
2) 管理者は既存データから状況把握を行い、更なる状況把握のため関連する詳細ログの取得をシステムに依頼
3) システムは車両に詳細ログ取得依頼を行い、車両から受領したログを表示し、管理者は取得したログを基に分析

以下管理画面の遷移例を示す。

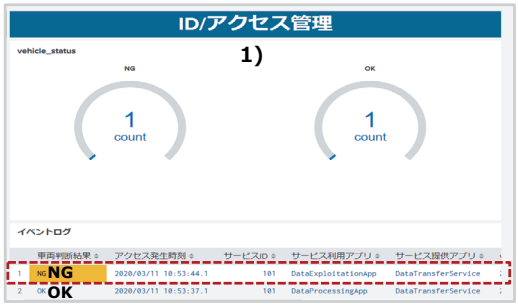

図13　システムが車両で不正アクセスが起きていることを検知する（図中破線部）。管理者は当該箇所をクリックし詳細を表示する。

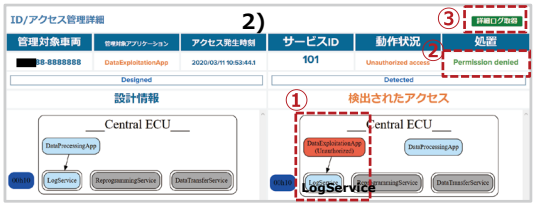

図14　管理者は管理者権限アプリケーションしかアクセスできないLogServiceに、アクセス権限のないDataExploitationAppがアクセスしようとしていること（図中破線部①）、ID／アクセス管理によりアクセス拒否されたこと（図中破線部②）を確認する。更なる状況把握のため管理者は関連アプリケーションのログ取得を車両に依頼する（図中破線部③）。

図15　システムは車両に当該アプリケーションの関連するログデータの取得指示を出し、車両からデータ受信後画面上に表示する（図中赤破線部）。
管理者は本ログをベースに分析、原因究明を行う。

4. 結　　言

本稿では、車載アプリケーションを管理する車載アプリケーション管理技術と当該技術を適用した車載アプリケーションライフサイクル管理システムについて紹介した。

当社製品であるDrive Linkに本技術やシステム、及び当社物流ソリューションのノウハウを適用することで、物流DXを加速させることができると考えている。現在、コネクティッドカー向け車両管理システムとして製品化に向けた開発を進めており、Drive Linkの後継機として展開予定である。

用語集

※1　OTA

Over-The-Air の略。無線経由でデータを送受信する技術を指す。

※2　Drive Link

住友電工システムソリューション㈱製の GPS や CAN データ等をクラウドに送信する後付け車載機。

※3　Eagle Sight

住友電気工業㈱製の車両運行管理トータルソシューションシステム。

※4　物流DX

機械化・デジタル化を通じて物流のこれまでの在り方を変革すること。

・Drive Link は住友電工システムソリューション㈱の登録商標です。
・Eagle Sight は住友電気工業㈱の登録商標です。

参考文献

(1) BOSCH、Mobility topics
https://www.bosch-mobility-solutions.com/en/mobility-topics/ee-architecture/
(2) 独立行政法人情報処理推進機構セキュリティセンター (IPA)、「IoT 開発におけるセキュリティ設計の手引き」
https://www.ipa.go.jp/files/000052459.pdf
(3) 住友電工システムソリューション㈱、物流ソリューション
https://www.seiss.co.jp/ms/logistics/index.html

執筆者

矢野　純史＊：情報ネットワーク研究開発センター　グループ長

高木建太朗　：情報ネットワーク研究開発センター

村吉　諄之　：情報ネットワーク研究開発センター

羽賀　剛　：情報ネットワーク研究開発センター　部長

滝本　周平　：㈱オートネットワーク技術研究所　室長

田中　亮　：㈱オートネットワーク技術研究所　グループ長

＊主執筆者