自動車車両を安全に保つOTAソフトウェア更新のセキュリティ技術

Security Technology for OTA Software Updates to Maintain Safety of Motor Vehicles

阿部　保彦　　小谷　誠剛　　窪田　英一郎

あらまし

近年の自動車車両（以下，車両）は，安全に関わる基本的な機能である走る，曲がる，止まるを実現するための装置をはじめとして，多くの装置が電子化されソフトウェアで制御されている。更に，Connected Carの増加や，自動運転の実用化などにより，重大な事故を引き起こすサイバー攻撃のリスクが高まっている。セキュリティ対策ソフトウェアの更新は，販売後の車両に対して短期間でかつ安価に更新することが求められる。富士通は，無線通信を使って安全かつ少ない通信量でソフトウェアを更新するOTA（Over The Air）ソフトウェア更新システムを開発した。本システムによってセキュリティ対策を進化させ，サイバー攻撃に対抗する。本システムの特徴は，正規契約された車両に正当なソフトウェアを配布するための認証・デジタル署名技術を採用し，更に遠隔で更新を行うために正しく更新されたことを保証するAccountability技術の搭載である。また，差分更新技術を適用することで，通信量の削減も可能にしている。

本稿では，高度化するサイバー攻撃に対抗し進化するセキュリティ対策を支えるOTAソフトウェア更新システムを紹介する。

Abstract

In recent years, much of the equipment in motor vehicles (hereinafter, “vehicles”), including those that control the basic safety-related functions of driving, turning, and stopping, have become computerized and controlled by software. In addition, due to the increase in connected cars and the practical application of self-driving, the risk of cyberattacks causing major accidents is increasing. Low-cost security software updates that can be applied in a short amount of time to vehicles after sales are required. Fujitsu has developed an over-the-air (OTA) software update system that uses wireless communication to update software with safety and low communication traffic. This system evolves security measures to counter cyberattacks. It features authentication and digital signature technology adopted for distributing legitimate software to vehicles with a formal contract, as well as accountability technology incorporated to ensure correct updates are executed, which is required because updating takes place remotely. Reduced communication traffic is also achieved by applying an incremental update technology. This paper presents the OTA software update system that counters increasingly sophisticated cyberattacks to support evolving security measures.

1. まえがき

従来，自動車車両（以下，車両）は装置の故障を想定したISO 26262に従って設計（機能安全設計）され，かつ機械的なメカニズムによって制御されてきた。

一方，近年の車両は，先進的なドライバーアシスト機能を実現するために，走る，曲がる，止まるに関わる装置の電子化が進んだ。更に，利便性向上を目的に車外ネットワークにつながるConnected Carの増加や，自動運転の実用化が起きている。このため，ネットワーク経由でソフトウェアの脆弱性・不具合を狙い重大な事故を引き起こすサイバー攻撃のリスクが高まっている。

自動車業界は，無線通信によるOTA（Over The Air）ソフトウェア更新で対策することを検討している。無線通信を使って自動で更新するため，ディーラの作業が削減でき安価に更新できる。しかし，遠隔でソフトウェア更新を行うため，サイバー攻撃による不正なソフトウェア更新や情報流出などが起きる可能性がある。また，ソフトウェア容量の増加によって更新時間，通信時間が延びる問題もある。更に，整備記録を厳密に管理できない問題もある。

OTAソフトウェア更新システムはこれらの課題を解決するために，セキュリティ技術（認証，デジタル署名），更新時間短縮技術（差分更新），更新の保証技術（Accountability）を導入した。

富士通はサイバー攻撃を考慮したセキュリティ対策やプラットフォームを提供している。

本稿では，OTAソフトウェア更新システムで導入したセキュリティ技術とソフトウェアの更新時間短縮技術，更新の保証技術（Accountability技術）について述べる。

2. OTAソフトウェア更新の概要と課題

本章では，OTAソフトウェア更新の仕組みを述べるとともに，車両適用の課題を整理する。

2.1 ソフトウェア更新の概要

OTAソフトウェア更新は，装置メーカーが作成したソフトウェアを車両に配信し，受け取った装置が更新する。具体的には，車両への配信と更新を管理するOTA管理センターと車両側でソフトウェアを受信する通信装置，ソフトウェアを格納し車両装置の更新を管理するOTAマスタ，更新を行う装置で構成される。

ソフトウェア更新は，ソフトウェア開発元の装置メーカー，車両への配信を管理する車両メーカー，更新を許諾するユーザー（ドライバー），実行結果を確認するディーラが協力して行う。

図-1に示すようにOTA管理センターに更新ソフ

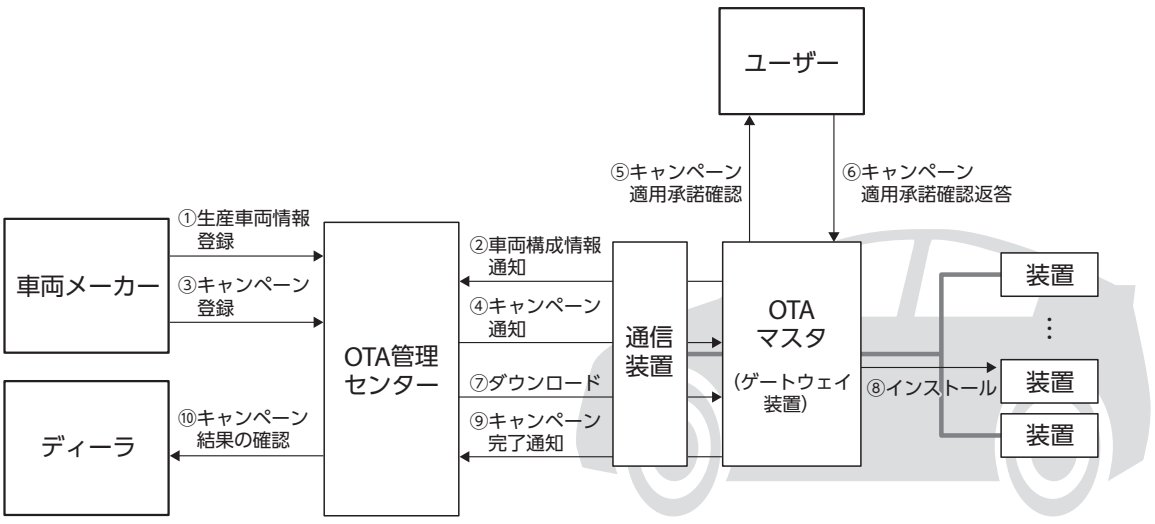

図-1　OTAソフトウェア更新の概要

トウェアの情報，車両の構成情報を集め，キャンペーン登録（更新指示）に基づきユーザーに許諾をとり，実施状況をディーラに提供する。OTA管理センターは，ソフトウェア更新全体を制御する役割を担う。

2.2 ソフトウェア更新の課題

車両のソフトウェア更新には，以下に挙げる課題がある。

(1) 車両の特定

OTAソフトウェア更新では，車両メーカーやディーラが立ち会わずにソフトウェアを更新する。正しいソフトウェアで更新しないと車両に故障が生じるため，人の代わりにOTA管理センターが車両を特定する必要がある。

また，ソフトウェアが攻撃者に渡った場合，ソフトウェアIP（Intellectual Property）が流出したり，ソフトウェアが解析されサイバー攻撃に利用されたりする可能性がある。これらを防止するため，配信先の特定が重要になる。

(2) 更新ソフトウェアの認証

正しくないソフトウェアで更新が可能であると，装置の故障や，サイバー攻撃が容易に成功することが考えられる。これを防ぐため，委託先の装置メーカーが開発したソフトウェアであること，改ざんされていないことを確認する必要がある。

(3) 通信量の削減

装置のソフトウェア容量が肥大化した結果，ソフトウェアの更新時にOTA管理センターからの通信量が増加しており，これを削減する必要がある。

(4) 更新実施の保証

OTAソフトウェア更新は車両メーカーやディーラが立ち会わずに行われる。そのため，該当の車両で更新が正しく行われたことを証明する必要がある。また，車両は正しい整備記録を保持し車検などを受けなければならない。したがって，OTAソフトウェア更新も重要な位置付けを担う。

3. システム導入技術

OTAソフトウェア更新システムでは，2.2節に記載した課題に対して以下の技術を導入し対策を行った。

3.1 車両の特定対策

本システムでは，証明書を用いた認証技術で車両を特定する。認証はOTA管理センターと車両の双方で行う。ただし，更新対象装置とOTA管理センターで認証するのではなく，車両を代表する装置とOTA管理センターで認証を行う。

車両メーカーと装置メーカーは，業界で統一したオープンな認証技術を採用する。このため，一般社団法人JASPAR（Japan Automotive Software Platform and Architecture）では，車両で用いる規格を検討[(1)]しており，X.509証明書，あるいはCVC（Card Verifiable Certificates）証明書をベースに案を作成している。

3.2 更新ソフトウェアの認証

正しい装置メーカーによって作られ，改ざんをされていないことを認証するために，更新ソフトウェアにデジタル署名を使用する。これもJASPARで規格化が検討されている技術[(2)]を採用する。

デジタル署名の概要を図-2に示す。デジタル署名は，異なるプログラムから異なるハッシュ値が生成される。また，秘密鍵がなければ署名できないことと，秘密鍵は装置に保存されておらず，流出するリスクが低いことから有効な手段である。

デジタル署名では，ハッシュ計算と公開鍵暗号の暗号強度が署名の信頼性に影響する。暗号強度が弱ければ不正プログラムを正当化できるため，検証したデータを信頼できない。本システムは，電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクトCRYPTRECが発行した「電子政府推奨暗号リスト」[(3)]に記載の方式をメーカーの要望に合わせて提供する。

3.3 通信量の削減

更新の通信量を削減するために，更新前と更新後の差分を作成し配信する。富士通独自技術である差分更新技術を採用した。この技術は4章に詳細を記述する。

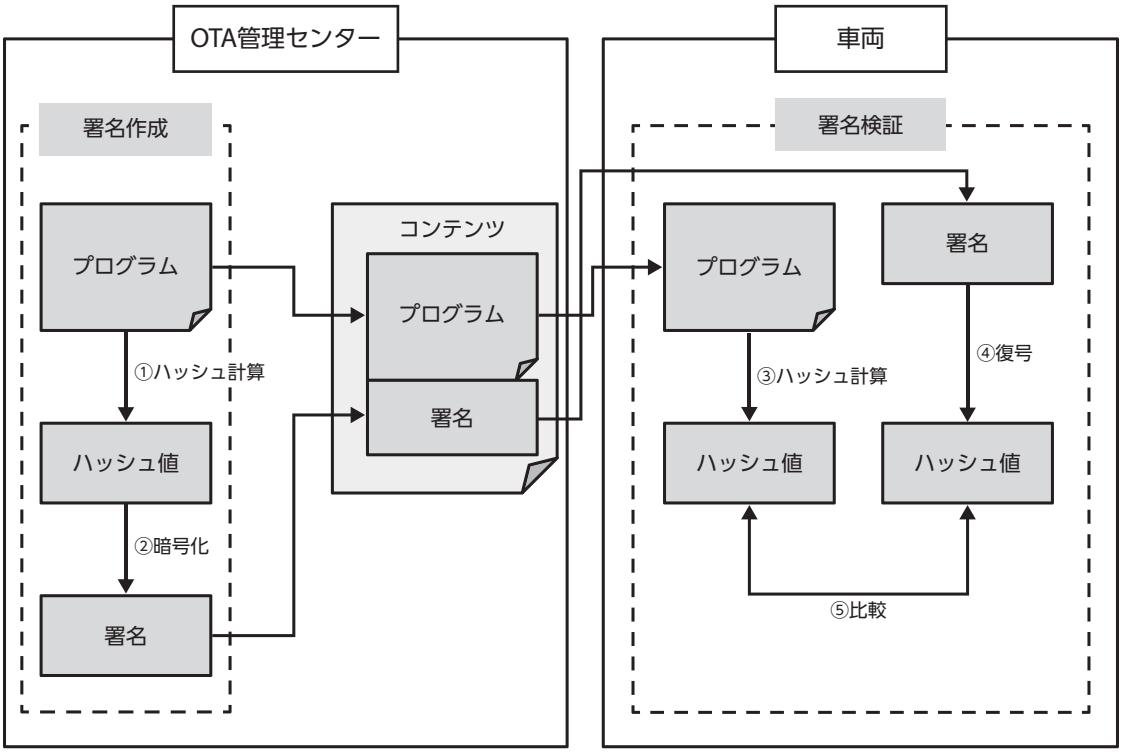

図-2　デジタル署名の概要

3.4 更新実施の保証

ディーラなどにおけるソフトウェア更新は，現場作業確認，更新履歴管理，書類への署名・日付記入，捺印などによって証拠とする。OTAソフトウェア更新においても同様の証拠が必要となるが，こうした書類が存在しない。このため，書類を使用しない証拠性の担保が重要である。即ちAccountabilityを実現する必要がある。そこで，OTAソフトウェア更新時の実施ログに適切な署名を行い，証拠性を担保する。該当の車両で署名が行われたことを担保するために，国際業界標準規格策定のための組織であるTCG（Trusted Computing Group）規格に対応した自動車セキュリティチップ（Automotive-Thin）を用いて署名することとした。

実施の証拠性担保が重要であることと，TCG規格の位置付けについて，参考までに米国の状況を紹介する。

1999年公開された米国NIST（National Institute of Standards and Technology）の文書に，明確な記述がある。NISTは，Accountabilityを法に従って，第三者への説明義務，第三者に拠る独立した検証実現性担保，と明確に定義しその必要性を訴求した。これを受けて，NHTSA｛米国運輸省（DoT）配下の組織，National Highway Traffic Safety Administration｝は2017年，Automated Driving SystemsにおけるAccountabilityの考え方や意見を募集した。それに対してTCGは意見書を提出し，NHTSAのサイトで公開されている。

4. 差分更新技術

OTAソフトウェア更新は，OTA管理センターから更新ソフトウェアを無線通信で配信する。近年の装置ソフトウェアは肥大化しており，ソフトウェア全体を配信するのは効率的ではないため，更新の差分だけを配信することが一般的である。

富士通の差分更新技術は，2002年から携帯電話の有線ソフトウェア更新に適用し，2004年からは無線ソフトウェア更新（OTAソフトウェア更新）にも適用された。この技術を車両向けOTAソフトウェア更新にも適用する。

差分更新の概要を図-3に示す。更新は，更新前の

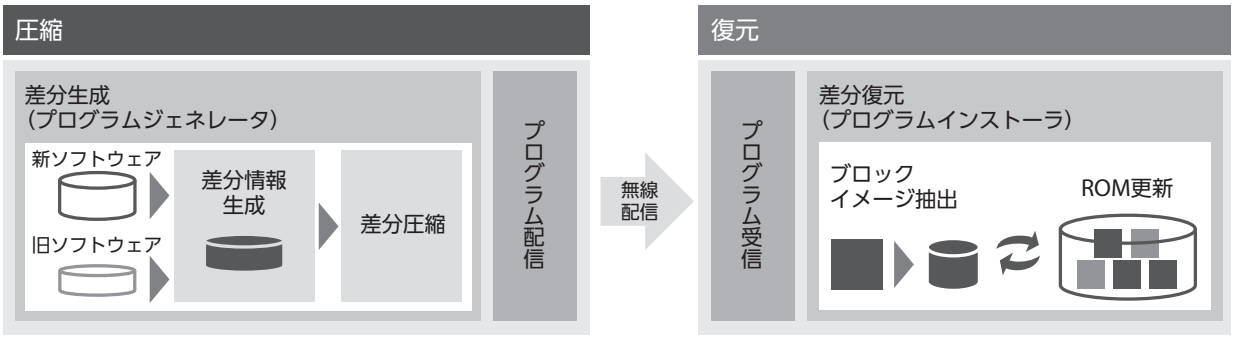

図-3　差分更新の概要

旧ソフトウェアと更新後の新ソフトウェアをブロック単位で比較し，差分があるブロックについて差分情報を生成する。この差分情報を更新先に送り，更新先でブロック単位にROM更新を行う。以下に差分更新技術の特長を述べる。

(1) 圧縮アルゴリズム

車両装置に搭載されるRISC（Reduced Instruction Set Computer）プロセッサーに特化した圧縮，符号化を実施する。RISCアーキテクチャーの特長（同じ命令の繰返し，レジスタ変更の規則性など）を利用することがポイントとなる。

(2) 限られたメモリリソースで復元が可能

更新に必要となる元のデータをブロック化して効率良く保持・参照することで，少ないメモリリソースで復元ができる。

(3) 差分復元段階での中断に対応

差分更新のタイミングをコントロールすることで，装置の電源断にも対応できる。更に，差分情報をRISCアーキテクチャーの特徴であるMOVE命令などの多用やレジスタ使用の規則性を利用し符号化する。これによって，更なる差分情報を圧縮し，更新情報の削減が可能である。

また，この処理は富士通独自のアルゴリズムであり，実行ハードウェア（メモリや処理能力）に合わせてカスタマイズが可能である。車両には複数の装置があり，個々の装置のハードウェア条件は異なっているが，それらの装置に合わせカスタマイズして提供可能である。

5. むすび

本稿では，富士通のOTAソフトウェア更新システムが備える機能について紹介した。

OTAソフトウェア更新システムは，車両の特定，更新ソフトウェアの認証，通信量の削減，更新実施の保証が可能であり，車両ソフトウェア更新に最適なシステムである。サイバー攻撃は日々進化しており，より高度なセキュリティ技術の適用が求められている。富士通ではこれらの技術を取り入れるだけでなく，サイバー攻撃に追随し進化するOTAソフトウェア更新システムを提供していく。

参考文献

(1) JasPar：JASPAR情報セキュリティ ソフトウェア更新システム デジタル署名要求仕様書．2018.
(2) JasPar：JASPAR 情報セキュリティ ソフトウェア更新システム 機器認証要求仕様書．2018.
(3) CRYPTREC：電子政府推奨暗号リスト．
https://www.cryptrec.go.jp/list.html

著者紹介

阿部　保彦（あべ　やすひこ）
富士通（株）
Mobilityシステム事業本部
Mobility関連システムの開発に従事。

小谷　誠剛（こたに　せいごう）
富士通（株）
FJQW本部
Mobility関連システムの開発に従事。

窪田　英一郎（くぼた　えいいちろう）
富士通（株）
FJQW本部
Mobility関連システムの開発に従事。