

TR-1068

自動車の遠隔更新技術の標準化動向
と実用化課題

Current standardization movement and issues
before practical use for Over The Air updating
in vehicle

第 1 版

2017 年 12 月 11 日制定

一般社団法人

情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

本書は、（一社）情報通信技術委員会が著作権を保有しています。

内容の一部又は全部を（一社）情報通信技術委員会の承諾を得ることなく複製、転載、改変、転用及びネットワーク上での送信、配布を行うことを禁止します。

目次

<参考>	1
<略語>	2
1. はじめに	5
2. 国内外の遠隔ソフトウェア更新関連技術の標準化動向	5
3. 関連団体調査：車両レベル	7
3.1. SAE	7
3.1.1. 組織紹介	7
3.1.2. 規格・発行物紹介	7
3.1.2.1. Firmware Update Over The Air (FOTA) for Automotive Industry	8
3.1.2.1.1. 概要	8
3.1.2.1.2. 遠隔ソフトウェア更新に関連する項目	8
3.1.2.1.3. 将来展望	9
3.1.2.2. The New ECU Update Process	9
3.1.2.2.1. 概要	9
3.1.2.2.2. 遠隔ソフトウェア更新に関連する項目	9
3.1.2.2.3. 将来展望	9
3.1.2.3. Over the Air Software Update Realization within Generic Modules with Microcontrollers Using External Serial FLASH	9
3.1.2.3.1. 概要	9
3.1.2.3.2. 遠隔ソフトウェア更新に関連する項目	9
3.1.2.3.3. 将来展望	10
3.1.2.4. Analysis of Software Update in Connected Vehicles	10
3.1.2.4.1. 概要	10
3.1.2.4.2. 遠隔ソフトウェア更新に関連する項目	10
3.1.2.4.3. 将来展望	10
3.1.2.5. OTA reflashing: the challenges and solutions	10
3.1.2.5.1. 概要	10
3.1.2.5.2. 遠隔ソフトウェア更新に関連する項目	10
3.1.2.5.3. 将来展望	11
3.1.2.6. Feasibility Study for a Secure and Seamless Integration of Over the Air Software Update Capability in an Advanced Board Net Architecture	11
3.1.2.6.1. 概要	11
3.1.2.6.2. 遠隔ソフトウェア更新に関連する項目	11
3.1.2.6.3. 将来展望	11
3.1.2.7. Safe and Secure Software Updates Over The Air for Electronic Brake Control Systems	11
3.1.2.7.1. 概要	11
3.1.2.7.2. 遠隔ソフトウェア更新に関連する項目	11
3.1.2.7.3. 将来展望	12
3.1.2.8. OTA updating bring benefits, challenges	12
3.1.2.8.1. 概要	12

3.1.2.8.2.	遠隔ソフトウェア更新に関連する項目	12
3.1.2.8.3.	将来展望	12
3.2.	UNECE WP29 ITS/AD TFCS	12
3.2.1.	組織紹介	12
3.2.2.	規格・発行物紹介	13
3.2.2.1.	遠隔ソフトウェア更新に関連する項目	13
3.2.2.2.	将来展望	13
3.3.	U.S.DOT/NHTSA	13
3.3.1.	組織紹介	13
3.3.2.	規格・発行物紹介	13
3.3.2.1.	Automated Driving Systems 2.0	14
3.3.2.1.1.	概要	14
3.3.2.1.2.	遠隔ソフトウェア更新に関連する項目	15
3.3.2.1.3.	将来展望	16
3.3.2.2.	Cybersecurity Best Practices for Modern Vehicles	16
3.3.2.2.1.	概要	16
3.3.2.2.2.	遠隔ソフトウェア更新に関連する項目	17
3.3.2.2.3.	将来展望	17
3.3.2.3.	Federal Motor Vehicle Safety Standards; V2V Communications NPRM	17
3.3.2.3.1.	概要	17
3.3.2.3.2.	遠隔ソフトウェア更新に関連する項目	18
3.3.2.3.3.	将来展望	18
3.4.	5GAA	19
3.4.1.	組織紹介	19
3.4.1.1.	規格・発行物紹介	19
3.4.1.2.	The Case for Cellular V2X for Safety and Cooperative Driving	19
3.4.1.2.1.	概要	19
3.4.1.2.2.	遠隔ソフトウェア更新に関連する項目	19
3.4.1.2.3.	将来展望	19
3.5.	ACEA	20
3.5.1.	組織紹介	20
3.5.2.	規格・発行物紹介	20
3.5.2.1.	ACEA Principles of Automobile Cybersecurity	20
3.5.2.1.1.	概要	20
3.5.2.1.2.	遠隔ソフトウェア更新に関連する項目	20
3.5.2.1.3.	将来展望	21
4.	関連団体調査：システムレベル（通信）	22
4.1.	ITU-T SG16	22
4.1.1.	組織紹介	22
4.1.2.	規格・発行物紹介	22
4.1.2.1.	F.749.2: Service requirements for vehicle gateway platforms	22
4.1.2.1.1.	概要	22
4.1.2.1.2.	遠隔ソフトウェア更新に関連する項目	22

4.1.2.1.3.	将来展望	23
4.2.	ITU-T SG17	23
4.2.1.	組織紹介	23
4.2.2.	規格・発行物紹介	23
4.2.2.1.	X.1373: Secure software update capability for intelligent transportation system communication devices	23
4.2.2.1.1.	概要	23
4.2.2.1.2.	遠隔ソフトウェア更新に関連する項目	23
4.2.2.1.3.	将来展望	24
4.3.	ISO TC22	24
4.3.1.	組織紹介	24
4.3.2.	規格・発行物紹介	25
4.3.2.1.	ISO 13400 (DoIP)	25
4.3.2.1.1.	概要	25
4.3.2.1.2.	遠隔ソフトウェア更新に関連する項目	25
4.3.2.1.3.	将来展望	25
4.3.2.2.	ISO 14229 (UDS)	25
4.3.2.2.1.	概要	25
4.3.2.2.2.	遠隔ソフトウェア更新に関連する項目	26
4.3.2.2.3.	将来展望	26
4.3.2.3.	ISO 22901 (ODX)	26
4.3.2.3.1.	概要	26
4.3.2.3.2.	遠隔ソフトウェア更新に関する項目	26
4.3.2.3.3.	将来展望	26
4.4.	ISO TC204	26
4.4.1.	組織紹介	26
4.4.2.	規格・発行物紹介	27
4.5.	IEEE 802 (車関係)	27
4.5.1.	組織紹介	27
4.5.2.	規格・発行物紹介	27
4.6.	Wi-Fi Alliance	27
4.6.1.	組織紹介	27
4.6.2.	規格・発行物紹介	28
4.7.	W3C	28
4.7.1.	組織紹介	28
4.7.2.	規格・発行物紹介	28
4.7.2.1.	Vehicle Information Access API	29
4.7.2.1.1.	概要	29
4.7.2.1.2.	遠隔ソフトウェア更新に関連する項目	29
4.7.2.1.3.	将来展望	29
4.7.2.2.	Vehicle Signal Server Specification	29
4.7.2.2.1.	概要	29
4.7.2.2.2.	遠隔ソフトウェア更新に関連する項目	29

4.7.2.2.3.	将来展望.....	29
4.7.2.3.	Cyber-Security in the Connected Car Age.....	29
4.7.2.3.1.	概要.....	29
4.7.2.3.2.	遠隔ソフトウェア更新に関連する項目.....	29
4.7.2.3.3.	将来展望.....	30
4.8.	Bluetooth SIG.....	30
4.8.1.	組織紹介.....	30
4.8.2.	規格・発行物紹介.....	30
4.9.	oneM2M.....	30
4.9.1.	組織紹介.....	30
4.9.2.	規格・発行物紹介.....	30
4.9.2.1.	Vehicle Information Access API.....	31
4.9.2.1.1.	概要.....	31
4.9.2.1.2.	遠隔ソフトウェア更新に関連する項目.....	31
4.9.2.1.3.	将来展望.....	31
5.	関連団体調査：システムレベル（部品）.....	32
5.1.	TCG.....	32
5.1.1.	組織紹介.....	32
5.1.2.	規格・発行物紹介.....	32
5.1.2.1.	Automotive Thin Spec.....	33
5.1.2.1.1.	概要.....	33
5.1.2.1.2.	遠隔ソフトウェア更新に関連する項目.....	33
5.1.2.1.3.	将来展望.....	34
5.1.2.2.	Guidance for Securing IoT Using TCG Technology.....	35
5.1.2.2.1.	概要.....	35
5.1.2.2.2.	遠隔ソフトウェア更新に関連する項目.....	35
5.1.2.2.3.	将来展望.....	35
5.2.	EVITA.....	35
5.2.1.	組織紹介.....	35
5.2.2.	規格・発行物紹介.....	35
5.2.2.1.	Deliverable D2.1: Specification and evaluation of e-security relevant use cases.....	36
5.2.2.1.1.	概要.....	36
5.2.2.1.2.	遠隔ソフトウェア更新に関連する項目.....	36
5.2.2.1.3.	将来展望.....	37
5.2.2.2.	Deliverable D2.3 Security requirements for automotive on-board networks based on dark-side scenarios.....	37
5.2.2.2.1.	概要.....	37
5.2.2.2.2.	遠隔ソフトウェア更新に関連する項目.....	37
5.2.2.2.3.	将来展望.....	39
5.2.2.3.	Deliverable D3.2 Secure on-board architecture specification.....	39
5.2.2.3.1.	概要.....	39
5.2.2.3.2.	遠隔ソフトウェア更新に関連する項目.....	39
5.2.2.3.3.	将来展望.....	40

5.2.2.4.	Deliverable D3.3 Secure on-board protocols specification.....	40
5.2.2.4.1.	概要.....	40
5.2.2.4.2.	遠隔ソフトウェア更新に関連する項目.....	40
5.2.2.4.3.	将来展望.....	43
5.3.	HIS	43
5.3.1.	組織紹介.....	43
5.3.2.	規格・発行物紹介.....	43
5.3.2.1.	SHE - Secure Hardware Extension - Functional Specification Version 1.1.....	44
5.3.2.1.1.	概要.....	44
5.3.2.1.2.	遠隔ソフトウェア更新に関連する項目.....	44
5.3.2.1.3.	将来展望.....	44
6.	今回の調査を踏まえての、標準化及び実用化に向けた課題整理.....	45
6.1.	3章から5章の記述/説明のまとめ.....	45
6.2.	前章までの記述に基づく課題整理.....	46
7.	まとめ.....	47
	<参考文献一覧>.....	48

<参考>

1. 改版の履歴

版数	制定日	改版内容
第1版	2017年12月11日	制定

2. 参照文章

主に、本文中に記載された文書、及び<参考文献一覧>に記載した文書を参照した。

3. 技術報告作成部門

TTC コネクテッド・カー専門委員会

自動車遠隔更新検討作業部会 / Task Force Auto-OTA-Updating (TFAOU)

<略語>

本書では以下の略語を使用する。一部は公益社団法人自動車技術会・基準キーワード¹を参照している。

略語一覧表

略語	名称
5GAA	5G Automotive Association
ACC	Adaptive Cruise Control
ACEA	Association des Constructeurs Europeens d'Automobiles
ADAS	Advanced Driver Assistance System
ADS	Automated Driving Systems
AES	Advanced Encryption Standard
API	Application Programming Interface
ARIB	Association of Radio Industries and Business
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Automatic Teller Machine
BSM	Basic Safety Message
CAD	Connected and Automated Driving
CAN	Controller Area Network
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CCSA	China Communications Standards Association
CEN	Comite Europeen de Normalisation
CENELEC	Comite Europeen de Normalisation Electrotechnique
CESG	Communications Electronics Security Group
CIS	Center for Internet Security
CMAC	Cipher-based MAC
CRL	Certification Revocation List
CU	Communication Unit
DoIP	Diagnostic communication Over Internet Protocol
DSRC	Dedicated Short Range Communication
DT	Diagnostic Tool
EATA	European Automotive Telecom Alliance
EBC	Electronic Brake Control
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECU	Electronic Control Unit
EPS	Electric Power Steering
ETSI	European Telecommunications Standards Institute
EVITA	E-safety vehicle intrusion protected applications
FIPS	Federal Information Processing Standards
FMVSS	Federal Motor Vehicle Safety Standard
G/W	Gate Way
GCM	Galois/Counter Mode
GF(p)	Galois Field (prime)
HAV	Highly Automated Vehicle
HIS	The Herstellerinitiative Software
HSM	Hardware Security Module
HUD	Head Up Display
ID	Identification

¹ 公益社団法人自動車技術会基準キーワード
<https://tech.jsae.or.jp/rireki/keyword.pdf>

略語	名称
IETF	Internet Engineering Task Force
IOT	Internet of Thing
IS	International Standard
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
ITU-R	ITU Radiocommunication Sector
ITU-D	ITU Telecommunication Development Sector
IVI	In-Vehicle Infotainment
LAN	Local Area Network
LKA	Lane Keeping Assist
LTE	Long Term Evolution
MAC	Message Authentication Code
MOU	Memorandum of Understanding
MSIP	Ministry of Science, ICT and Future Planning
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NPO	Nonprofit organization
NRPM	Notice of Proposed Rulemaking
OBD	On Board Diagnostics
OBD-II	On Board Diagnosis-II ²
ODD	Operational Design Domain
ODX	Open Diagnostic eXchange
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OSI	Open Systems Interconnection
OTA	Over the Air
PC	Personal Computer
PKI	Public Key Infrastructure
POS	Point of Sales
PRNG	Pseudo Random Number Generator
PTC	Power Train Controller
RAM	Random Access Memory
ROM	Read Only Memory
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SHE	Secure Hardware Extension
TC	Technical Committee
TCG	Trusted Computing Group
TCU	Transmission Control Unit
TIA	Telecommunications Industry Association
TOE	Target Of Evaluation
TPM	Trusted Platform Module
TR	Technical Report
TRNG	True Random Number Generator
TS	Technical Specification

² 国土交通省「安全 OBD」

http://www.mlit.go.jp/kisha/kisha07/09/090914_2_.html

略語	名称
TSAG	Telecommunication Standardization Advisory Group
TSDSI	Telecommunications Standards Development Society, India
TTA	Telecommunications Technology Association
TTC	The Telecommunication Technology Committee
UDX	Unified Diagnostic Services
UID	User ID
URL	Uniform Resource Locator
USB	Universal Serial Bus
USDOT	United States Department of Transportation
UTC	Universal Time, Coordinated
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to X(anything)
VGP	Vehicle Gateway Platform
W3C	World Wide Web Consortium
WG	Working Group
XML	Extensible Markup Language

1. はじめに

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、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／組織で標準化の提案／協議が進められている。本技術レポートの3章から5章で詳述しているチップを含むセキュリティモジュール、ユースケース、セキュリティ要件、通信規格、API及びこれらの運用に基づく検討／公開／提案もその中の重要な一つである。それらを迅速に把握、理解し、日本の施策に取り込む提案の一助とするために、コネクテッド・カー専門委員会自動車遠隔更新検討作業部会で活動を行った。具体的には、遠隔ソフトウェア更新のうちOTA(Over The Air)技術に係る種々の活動を公開情報から入手し、車載システム遠隔更新技術の観点から検討、分析し、レポートを作成した。

2. 国内外の遠隔ソフトウェア更新関連技術の標準化動向

自動車には走行制御(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(パワーウインドウ、灯火制御、など)の各種機能を実現するために、数十個以上のECUが搭載されている。各ECU上では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、これらの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のメモリに記録されるが、車両出荷後に機能改善などのために更新される場合がある。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。リプログラミング作業は、通常はディーラーや自動車整備工場(以下、ディーラー等という。)において、自動車整備士が診断ツールを有線接続して実施する。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)ソフトウェア更新する技術も実用化しており、本技術を遠隔ソフトウェア更新(OTAリプログラミング)と呼んでいる。

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。本報告ではリプログラミング対象は特に限定していない。

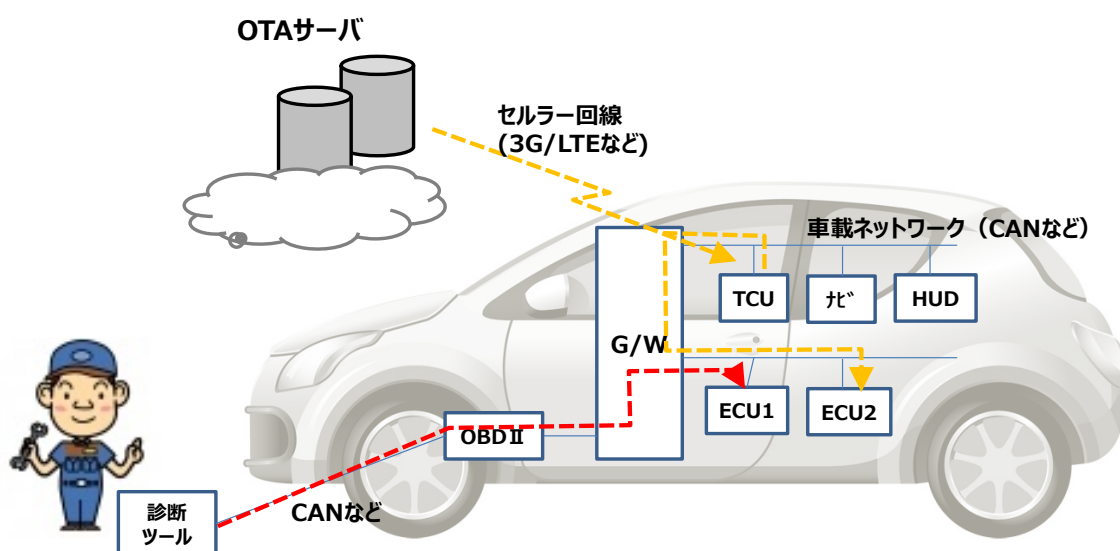


図 2-1 リプログラミングの例

(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)

本報告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。本作業部会メンバーが知見を有する当該団体の公開情報より、「OTA リプログラミング」をキーワードに関連するコンテンツをピックアップし、共通テンプレートにまとめる作業を行い、3～5章に作業結果を示した。その結果、各団体で進展している遠隔ソフトウェア更新実現に向けた活動状況を明らかにすることができた。

なお、本報告書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。

関連団体の活動内容、策定文書には様々な内容があるため、調査結果を三つのレベルに分類し、それぞれ、3章に車両レベル、4章にシステムレベル（通信）、5章にシステムレベル（部品）としてまとめた。各団体の章では、組織概要とその発行物（公開状況）に関して紹介する。各発行物に関しては、概要として位置づ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、将来展望をまとめた。位置づけとしては、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を行った。その対象としては、通信技術（車内 LAN、車外無線通信など）、更新手順、セキュリティ要件、ハードウェア、ユースケース（自動運転など）、ライフサイクル（運用、ダイアグなど）、更新対象（アプリケーション、マップデータなど）の分類で記載を行った。

3. 関連団体調査：車両レベル

本報告は標準規格の動向調査をスコープとしているが、本章では UNECE など策定し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た。

3.1. SAE

3.1.1. 組織紹介

SAE International³ は、航空機、乗用車、商用車等業界の関連技術者及び専門家を会員とする非営利団体である。

主な活動として、技術委員会で標準規格の策定を行っている。また、この団体では A World In Motion や Collegiate Design Series などの教育プログラムを支援している。

約 128,000 人以上の構成メンバーを有している世界規模の団体であり、その Board of Director は、様々な分野の出身者から構成されている。

3.1.2. 規格・発行物紹介

ここでは OTA に関する SAE の活動内容を紹介する。

- Firmware Update Over The Air (FOTA⁴) for Automotive Industry (2007/8)

◇ <http://papers.sae.org/2007-01-3523/>

リコールによるソフトウェア更新のためには費用だけでなく、車両をディーラー等に持ち込むことによって当該車両を使えなくなる時間も課題であると述べている。

- The New ECU Update Process (2013/6)

◇ <http://articles.sae.org/12250/>

ダウンロードとインストールなどといったソフトウェア更新の処理時間を短くするために、携帯電話などで利用されている方法を利用するアイデアが紹介されている。ソフトウェア更新によって当該車両を使えなくなる時間を短くするのが目的である。その方法とは、新旧バージョン間の差分を識別しデルタファイルを生成するものであり、ファイル全体をダウンロードする必要のないことが利点としてあげられている。

- Over the Air Software Update Realization within Generic Modules with Microcontrollers Using External Serial FLASH (2017/3)

◇ <http://papers.sae.org/2017-01-1613/>

ソフトウェア更新の処理時間を短縮するもう一つの方法として、外部シリアルフラッシュメモリを各 ECU に付加する実装が紹介されている。この方法では、外部シリアルフラッシュメモリへのダウンロードの間、各 ECU はローカルメモリで動作できるため当該車両は使い続けられる。

- Analysis of Software Update in Connected Vehicles (2014/4)

◇ <http://papers.sae.org/2014-01-0256/>

テレコム業界で実績のある 3G/4G モデム、Wi-Fi、スマートフォン（Bluetooth か USB テザリング）による OTA を例示している。同時にこのペーパーでは、北米におけるアンケート調査を行っている。ユースケースごとに要件に対する有利、不利な点を示し、各 OEM における OTA 対応の状況を示している。

³ <http://www.sae.org/>

⁴ OTA は FOTA と呼ばれる場合もあるが、基本的には同じ意味で利用されている。

- OTA reflashing: the challenges and solutions (2016/1)
 ◇ <http://articles.sae.org/14573/>
 テスラの成功を受け課題の整理が行われている。遠隔ソフトウェア更新の処理時間、ソフトウェア更新後のインテグレーションチェックの必要性、ロールバックに必要なメモリなどが課題としてあげられている。
- Feasibility Study for a Secure and Seamless Integration of Over the Air Software Update Capability in an Advanced Board Net Architecture (2016/4)
 ◇ <http://papers.sae.org/2016-01-0056/>
 テレコム業界と異なり、自動車業界での遠隔ソフトウェア更新は安全でシームレスな実装が要件となる。この要件に対するソフトウェア更新の実現可能性が調査、報告されている。
- Safe and Secure Software Updates Over The Air for Electronic Brake Control Systems (2016/9)
 ◇ <http://papers.sae.org/2016-01-1948/>
 遠隔ソフトウェア更新の対象が EBC (Electronic Brake Control) システムの場合は、安全対策の拡張が必要であると述べている。その事例として SHE と EVITA の HSM 及び TCG の TPM によるセキュリティアーキテクチャが紹介されている。
- OTA updating bring benefits, challenges (2016/8)
 ◇ <http://articles.sae.org/14946/>
 遠隔ソフトウェア更新はソフトウェアパッチの提供だけでなく、機能追加にも使われ得ることが紹介されている。

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

3.1.2.1. Firmware Update Over The Air (FOTA) for Automotive Industry

3.1.2.1.1. 概要

発行	2007/8/5
位置づけ	<技術報告> (法的拘束力なし)
対象	<通信技術、更新手順、ユースケース> メンテナンス、修理及びサービスの操作

3.1.2.1.2. 遠隔ソフトウェア更新に関連する項目

この時点でテレコム業界では、遠隔ソフトウェア更新に既に OTA 技術を使っていた。この方法を自動車業界に適用することを前提に、いくつかのユースケースを分析し、利点と課題を述べている。ただし、ベースにしている内容は、2001 年～2005 年の事例である。

- 保障費用
 OEM 各社が支払っている保障費用は、製品の売り上げに対して一定の割合を占めているが、その原因の一つとしてソフトウェア起因のリコールがあげられる。この解決策として OTA 技術を使って遠隔ソフトウェア更新することは、単に保障費用を抑えるだけでなく、リコールのたびに車両をディーラー等に持ち込まなくて済むといった顧客メリットもあることを述べている。
- ソフトウェア更新のユースケース
 あげられているソフトウェア更新のユースケースは、リコール、定期検査及びクレームの 3 件。ソフトウェア更新の方法としてあげているのは、ケーブルベース (有線) でのアップデートと OTA 技術を使ったアップデートである。

3.1.2.1.3. 将来展望

特になし。

3.1.2.2. The New ECU Update Process

3.1.2.2.1. 概要

発行	2013/6/22
位置づけ	<記事> (法的拘束力なし)
対象	<ライフサイクル> メンテナンスとアフターマーケット

3.1.2.2.2. 遠隔ソフトウェア更新に関連する項目

携帯電話で使われている差分アップデートの方法を、自動車の ECU のソフトウェアアップデートの方法として紹介している。紹介している方法とは、新旧の差異を認識し生成したデルタファイルを車両に転送してプログラムを更新する方法であり、通信データ量の削減、アップデートの処理時間短縮が可能であるとしている。また、OTA アップデートはディーラー等に車両を持ち込む必要がないため、いつでも更新データを配信できる利点があると述べている。このため特に更新が頻繁なインフォテインメントシステムに対する OTA アップデートは、一般的になる可能性があると述べている。

3.1.2.2.3. 将来展望

特になし。

3.1.2.3. Over the Air Software Update Realization within Generic Modules with Microcontrollers Using External Serial FLASH

3.1.2.3.1. 概要

発行	2017/3/28
位置づけ	<技術報告> (法的拘束力なし)
対象	<更新手順> プロセス設計

3.1.2.3.2. 遠隔ソフトウェア更新に関連する項目

ディーラー等での OBD インターフェースを介したソフトウェア更新の利点は、ソフトウェア更新の処理時間がユーザに見えないことにある。これは工場内で行われる他の様々なサービスの合計時間だけが見えるからである。ただし、ユーザはその間、車両を使うことができない。

同じように外部シリアルフラッシュメモリに更新データをダウンロードする方法であれば、その時間はユーザには明示されない。その間、ユーザの車両は稼働可能だからである。このペーパーでは、その実装例を紹介している。

- これまでの方法でのボトルネック

セントラルストレージにダウンロードした更新データを各 ECU に配信するが、すべての ECU に同時に配信できるわけでない。配信は OBD ポートから CAN バス経由で行われるが、転送レートは速くない。この間、車両は稼働できないので、これが課題になる。

- A/B swap

各 ECU に必要なメモリを A と B の 2 ページ用意し、メモリ B に更新データを転送する。この間、当該 ECU はメモリ A で実行しているため、車両は稼働できる。更新の完了が確認されると、メモリ A

からメモリ B に swap の後に ECU はリスタートする。

- ・ シリアルフラッシュメモリ

各 ECU に安価で容易に入手できるシリアルフラッシュメモリを付加する。当該 ECU はローカルメモリで実行しているため、これと並行してシリアルフラッシュメモリに更新データを転送可能になる。さらに、複数の ECU を同時にアップデート可能といった利点がある。本ペーパーでは、この実装例を具体的に紹介している。この実装例では、更新失敗時のロールバックのためのメモリ実装についても言及している。

3.1.2.3.3. 将来展望

特になし。

3.1.2.4. Analysis of Software Update in Connected Vehicles

3.1.2.4.1. 概要

発行	2014/4/1
位置づけ	<技術報告> (法的拘束力なし)
対象	<通信技術、ユースケース、更新手順> 組み込みソフトウェア、電子制御

3.1.2.4.2. 遠隔ソフトウェア更新に関連する項目

OTA アップデートにおける通信手段 (3G/4G、Wi-Fi、Bluetooth、USB テザリング) ごとにユースケースを分類して、要件に対する利点と不利な点を示している。これら OTA アップデートは、テレコム業界の実績ある方法であることが示されている。

ここで示している要件とは、セキュア通信、高速通信、通信費、付加装置の有無、ワイヤレス通信のエリア制約、ロールバック用メモリ、強制アップデートの可否である。これを示した上で、現在の各 OEM (Tesla, Chevy Volt, Mercedes, Chrysler, Audi, トヨタ) が北米において OTA アップデートで使用している通信手段を紹介している。

後半は、北米の各年齢層のユーザに対する車載ソフトウェア更新に関する関心度、期待度などのヒアリング内容とその結果を示している。

3.1.2.4.3. 将来展望

特になし。

3.1.2.5. OTA reflashing: the challenges and solutions

3.1.2.5.1. 概要

発行	2016/1/21
位置づけ	<記事> (法的拘束力なし)
対象	<ユースケース> ヒューマンファクター、安全性

3.1.2.5.2. 遠隔ソフトウェア更新に関連する項目

フラッシュメモリの OTA によるリプログラミング (ここでは reflashing と表現している) における課題と解決策について述べている。

- ・ リプログラミングの処理時間

テスラでも 45 分、ディーラー等の内でのリプログラミングでは 1 日以上との見積もりをしている。この原因はデータ転送の帯域幅にあり、Wi-Fi やセルラーネットワークの利用が解決する可能性があるとして述べている。

・モジュール間インテグレーション

遠隔ソフトウェア更新の後に、車内 CAN に接続されたモジュール間のインテグレーションチェックが必要であると述べている。どのモジュールが更新されたのか、その更新によってどんな影響があるかなどの確認を行い、かつインストールが失敗したときのためにロールバック機能が必要であるとしている。

3.1.2.5.3. 将来展望

特になし。

3.1.2.6. Feasibility Study for a Secure and Seamless Integration of Over the Air Software Update Capability in an Advanced Board Net Architecture

3.1.2.6.1. 概要

発行	2016/4/5
位置づけ	<技術報告> (法的拘束力なし)
対象	<更新手順、ハードウェア、セキュリティ> アーキテクチャ、電子制御ユニット、サイバーセキュリティ

3.1.2.6.2. 遠隔ソフトウェア更新に関連する項目

セルラー業界と比較して自動車業界における OTA には、安全性の確保をはじめとする固有の課題がある。運転者の観点から以下の 3 点を要件としてあげている。

- ・OTA は悪意のある攻撃に耐えなければならない
- ・OTA は短い時間で済ませ、車両の可用性を阻害してはならない
- ・運転中の車両の安全性は確保されなければならない

これらの要件に対する実現可能性を調査し、アップデートフロー、セキュリティアーキテクチャなど具体的な事例で説明している。

3.1.2.6.3. 将来展望

特になし。

3.1.2.7. Safe and Secure Software Updates Over The Air for Electronic Brake Control Systems

3.1.2.7.1. 概要

発行	2016/9/18
位置づけ	<技術報告> (法的拘束力なし)
対象	<ユースケース> 電子ブレーキ制御

3.1.2.7.2. 遠隔ソフトウェア更新に関連する項目

EBC システムにおいて OTA を適用する際は、

- ・車両の Safety と Security を確保すること
- ・車両の可用性を確保すること

の2点を考慮する必要があるとして事例を示して説明している。

前者の Security は、車両を悪意のある攻撃から守ることを意味する。このためには Firewall を実装し、暗号鍵及び鍵を格納しているメモリを守る必要がある。具体的な実装例として TPM と HSM を使ったシステムをあげている。

アップデートの間、安全のために車両は止まっている必要がある。この間、EBC システムはダウンしているからである。これが後者の可用性に影響する。安全対策を拡張しつつ、このダウンタイムを短くする実装例を次の3ステップで示している。

- ・車内ネットワーク構成とデータフローの解析
- ・車内ネットワークへのセキュリティ機能の実装例
- ・EBC システムのダウンタイムを短くする実装オプション

3.1.2.7.3. 将来展望

特になし。

3.1.2.8. OTA updating bring benefits, challenges

3.1.2.8.1. 概要

発行	2016/8/14
位置づけ	<記事> (法的拘束力なし)
対象	<更新対象、更新手順> 部品及びコンポーネント

3.1.2.8.2. 遠隔ソフトウェア更新に関連する項目

通信コスト低減のための Wi-Fi 利用が選択肢かもしれないこと、インテグレーションチェックが必要なことを示している点は、2016/1/21 の記事(OTA reflashing) と同じである。当該記事と異なる点は、対象をフラッシュメモリに限定しないで OTA の利点と課題を広く述べていることにある。

- ・リプログラミングはパッチだけでなく機能追加にも使える可能性を持っていること
- ・ロールバックのために余分なメモリが必要なこと
- ・OEM は車両の構成要素に関するデータを収集する必要があること

などに言及している。

3.1.2.8.3. 将来展望

特になし。

3.2. UNECE WP29 ITS/AD TFCS

3.2.1. 組織紹介

国際連合配下の活動の一つである自動車基準調和世界フォーラム (WP29) は、協定に基づく規則の制定・改正作業及び協定の管理・運営を行っている⁵。協定には 1958 年協定 (国連の車両等の型式認定相互承認協定)、1998 年協定 (国連の車両等の世界技術規則協定) がある。

欧州各国、日本、米国、カナダ、オーストラリア、南アフリカ、中国、韓国等が参加しており、非政府機関として OICA (国際自動車工業会)、IMMA (国際二輪自動車工業会)、ISO (国際規格協会)、CLEPA (欧州自動車部品工業会)、SAE (自動車技術会) 等も参加している。日本は 1977 年から加入している。

⁵ <https://www.mlit.go.jp/common/000036077.pdf>

日本からは国土交通省のメンバーが参加し、安全で環境性能の高い自動車の普及を促進する観点から、自動車に関する基準の国際調和及び認証の相互承認を推進している。

WP29 傘下に設置された自動運転分科会 (ITS/AD) にて、2016 年年末に自動運転車のサイバーセキュリティと OTA に関して検討を行うタスクフォース (TFCS) が発足し、日本とイギリスが共同議長となり活動を進めている。

3.2.2. 規格・発行物紹介

TFCS は、現在も活動を進めているが、正式発行された文書は現状ない。TFCS の会合は頻繁に開催されており、今回は、OTA に関連する会議資料を基に調査を行った。その結果を、以下に示す。

3.2.2.1. 遠隔ソフトウェア更新に関連する項目

2017 年 9 月末時点では、“Recommendation of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD on Software Updates”のドラフト (草案) が準備されており、下記内容に関して言及されている。

- ・リファレンスモデル
- ・ソフトウェアアップデートに関する型式認定プロセス
- ・ソフトウェアアップデートに関する追加要件 (アップデートプロセスの安全性確保を含む)
- ・ソフトウェア ID 番号とその用途

3.2.2.2. 将来展望

TFCS の活動は 1 年間で予定しており、2017 年末～2018 年には成果物の取りまとめが行われる予定である。成果物の内容は、各国における車両の基準策定に反映されていく見込みである。

3.3. U.S.DOT/NHTSA

3.3.1. 組織紹介

U.S.DOT、NHTSA はそれぞれアメリカ合衆国の政府機関である。

- ・U.S.DOT: U.S. Department of Transportation アメリカ合衆国運輸省
- ・NHTSA: National Highway Traffic Safety Administration 国家道路交通安全局

NHTSA は U.S.DOT の傘下であり、安全(Safety)に係る車の装備、性能に関する法規制やガイドラインの発行、リコールの通知・進捗管理を行う。Safety の観点から、V2X や自動運転を推進するとともに、法規制を見据えたガイドラインやポリシーの発行、意見募集を行っている。

また、U.S.DOT は米国内数箇所、V2X の実証実験を行っている。

3.3.2. 規格・発行物紹介

NHTSA の発行している遠隔ソフトウェア更新に関連すると考えられる主な発行物を下記にあげる。

- ・Automated Driving Systems 2.0 (2017/09)
◇ https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf
2016 年 9 月発行の Federal Automated Vehicles Policy を更新・差し替えたもの
- ・Cybersecurity Best Practices for Modern Vehicles (2016/10)
◇ https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf
- ・Federal Motor Vehicle Safety Standards; V2V Communications NPRM (2016/12)
◇ http://www.safercar.gov/v2v/pdf/V2V%20NPRM_Web_Version.pdf

◇ <https://www.gpo.gov/fdsys/pkg/FR-2017-01-12/pdf/2016-31059.pdf>

本 NPRM は、V2V 通信及びメッセージフォーマットに関するものであり、遠隔ソフトウェア更新を直接の対象としたものではないが、ソフトウェア更新手段として遠隔ソフトウェア更新に関する記載があるため紹介している。

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

3.3.2.1. Automated Driving Systems 2.0

3.3.2.1.1. 概要

発行	2017/09
位置づけ	<仕様> ガイダンス 本文書自体は Voluntary Guidance であり強制力は持たない。 公開時点では public comment が募集 ⁶ されている (2017 年 11 月 14 日まで)。技術の進化に対応するため、定期的なアップデートが予定されている。
対象	<ユースケース (自動運転) > ADS SAE の定義で Level 3 から Level 5 に相当する自動運転車で用いられる自動運転システム



米国では衝突事故の 94%が人的要因であることから、自動運転システム(以下、ADS と表記) の導入による事故数減少の期待が高まっている。また、安全目的以外にも障害者、高齢者、金銭的に車を所有できない人々が車を利用する機会の増加、輸送効率の向上による省エネ化や環境汚染の削減も期待されている。

本書は大きく分けて

(1) Voluntary Guidance

(2) Technical Assistance to States

の 2 部構成となっており、(2)は州政府による政策及び規制に関する内容である。以下では(1)に関するサマライズのみを行う。

Voluntary Guidance では、ADS の安全要素(Safety Elements)として 12 の項目を挙げている。

(1) System Safety

各種規格(ISO など)に適合した開発プロセスに従い、安全性の高い製品開発を行うこと。開発プロセスについては、特にソフトウェア開発についての留意事項が記載されている。

(2) Operational Design Domain

各 ADS に対して、想定する動作条件 (ODD)を定義し、その ODD 下において ADS が適切に動作するように設計すること。

ODD には、ADS が使用される条件(運転速度、日中/夜間の運転有無など)が含まれ、各 ADS は想定条件下で適切に動作するか検査する必要がある。

(3) Object and Event Detection and Response(OEDR)

定義された ODD 下において、ADS の OEDR 機能は他車、歩行者、動物など ADS の安全動作に影響しうる対象物を検知し、適切な動作を選択する必要がある。

⁶ <https://www.federalregister.gov/documents/2017/09/15/2017-19637/automated-driving-systems-a-vision-for-safety#>

(4) Fall Back (Minimal Risk Condition)

想定 ODD 以外での動作環境となった場合、システム不具合となった場合等で ADS が正常に動作しない場合には、そのときの状況に応じて適切な措置(停止など)をとること。

(5) Validation Methods

シミュレーション、テスト用トラックや公道での検証を踏まえて、ADS が想定どおりの動作をするか確認すべきことを示している。テストはカーメーカ、部品メー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ある。

(6) Human Machine Interface

自動運転の状況、緊急時に自動運転を解除するなどのメッセージを的確に伝えること。

(7) Vehicle Cybersecurity

サイバーセキュリティも考慮した、ロバスト設計を行うこと。

NIST、NHTSA、SAE、Auto-ISAC などが発行するガイダンスやベストプラクティスなどを検討、取り入れることが奨励されている。

(8) Crashworthiness

自動運転レベルに関わらず、無人車も含めて ADS は NHTSA の耐衝撃性基準を満たすこと。

(9) Post-Crash ADS Behavior

衝突事故に巻き込まれた後、自動運転を再開する場合には、そのプロセスを記録として残すこと。なお、安全に関する重要部品が故障した場合には、運転を再開してはならない。

(10) Data Recording

不具合などの原因究明&対策検討のため、様々なイベントを記録し共有すること。

(11) Consumer Education and Training

従業員、ディーラー、顧客含めて、ADS に関する教育を徹底すること

(12) Federal, State and Local Laws

各州の法律に適合していることを証明できるように、適切なログを残すこと。

なお、安全確保が必要な状況下では、人間は一時的に州法に違反することがあるが、ADS も予測可能なイベントを安全に処理できることが求められる。また、州法は将来的に変更されることがあるため、それに応じて ADS もアップデートさせる必要がある。

なお、本書の第 1 版の位置付けである 2016/9 発行の Federal Automated Vehicles Policy と比べると、下記項目が省略されている。ただし、考慮の必要がなくなったわけではなく、引き続き議論が必要であるとされている⁷。

- ・ Privacy
- ・ Ethical Considerations
- ・ Registration and sharing

3.3.2.1.2. 遠隔ソフトウェア更新に関連する項目

2016/9 発行の Federal Automated Vehicles Policy では、遠隔ソフトウェア更新が行われることを想定し、アップデートによって自動運転機能や縮退モード動作内容に変更が行われる場合、事前に Safety Assessment を提出すべきであるとされていた。

一方で本バージョンでは、遠隔ソフトウェア更新についての言及は行われていない。

⁷ <https://www.nhtsa.gov/manufacturers/automated-vehicles-manufacturers>

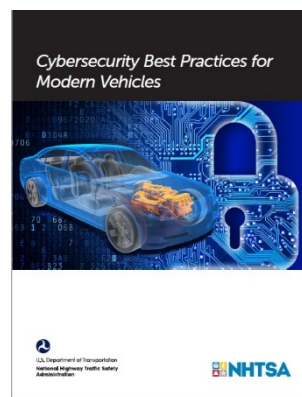
3.3.2.1.3. 将来展望

技術の進化や環境の変化を反映するため、定期的に更新されることが述べられている。

3.3.2.2. Cybersecurity Best Practices for Modern Vehicles

3.3.2.2.1. 概要

発行	2016/10
位置づけ	<ガイダンス>(法的拘束力なし) 自動車の Cybersecurity を検討するに当たり参照されることが期待されている。 本文書自体に拘束力や規制はないが、Purpose において、National Traffic and Motor Vehicle Safety Act(amended)でサイバーセキュリティの脆弱性によって生じるリスクも考慮した設計を行うことが求められているとの記載がある。
対象	<ライフサイクル> すべての自動車 車のライフサイクル全般を対象とし、車、車載システム、ソフトウェアなど自動車本体及び装備に関する個人・組織に向けた文書



特に前半は、NIST の Cyber Security Framework⁸ を広く参照し、“特定、防御、検知、対応、復旧”の5要素に基づいた設計アプローチを推奨している。また、Auto-ISAC を利用した情報共有を推奨している。

現時点では、Federal Motor Vehicle Safety Standard ではセキュリティ対策はカバーされていないが、改正版の National Traffic and Motor Vehicle Safety Act では潜在的なセキュリティ脆弱性による不当な安全リスクを回避するよう記載されており、セキュリティに対する取り組み強化を求めている。

U.S.DOT の最優先事項は、安全や個人情報の漏洩を防止するためのサイバーセキュリティ対策であり、NHTSA は積極的に車のサイバーセキュリティ調査を行い、関係者を巻き込みながら幅広くサイバーセキュリティ強化を検討している。

最近、NHTSA が行った活動としては、約 150 万台リコール実施 (Recall Campaign Number 15V461000)、連邦議会に対してセキュリティ対策含めた安全対策に関する検討報告の提出(2016/1)、セキュリティに関する有識者会議(2016/1)、セキュリティ対策含めた次世代安全方針に関する契約を自動車メーカ 18 社と締結、「NHTSA Federal Automated Vehicles Policy」の発行(2016/9)などがあげられる。

また、自動車関連メーカと他産業パートナーは、自動車セキュリティに関して、SAE による自動車のサイバーセキュリティ対策についてのガイドブックである J3061 “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems” の作成と発行(2016/1)、Auto-ISAC の確立(2015 年後半)、二つの事業者団体 (Alliance of Automobile Manufacturers と Global Automakers) によって設立されたセキュリティに関するベストプラクティスを検討するフレームワーク (Alliance of Automobile Manufacturers) の設立、といった活動を行っている。

NHTSA は上記活動をサポートしており、既に自発的に導入されているセキュリティ規格、方針、ベストプラクティス、教訓などを補足するとともに、将来の業界活動に役立つリソースとして本書を発行している。

自動車産業は、階層化セキュリティ対策を実現するための包括的、かつ体系的アプローチとして、Identify, Protect, Detect, Respond, Recover の五つの主要機能から構成される Cybersecurity Framework(NIST 発行)を遵守するべきと指摘している。

また、NHTSA は ISO/IEC 27000 のような IT セキュリティ標準規格、CIS (Center for Internet Security) のベ

⁸ <https://www.nist.gov/cyberframework>

ストブラクティス (CIS CSC) を考慮することも推奨している。これは、車両開発、ディーラー及びサービス環境並びにサプライチェーン上におけるセキュリティリスクの低減につながるためである。

3.3.2.2.2. 遠隔ソフトウェア更新に関連する項目

遠隔ソフトウェア更新とは限定されていないが、インシデント発生時に素早く回復させる手段・方法を設計しておくことが求められている (5.1 Layered Approach)。

また、ソフトウェア更新に関連して、デバッグモード・開発モードへのアクセス制限、鍵管理、ダイアグアクセス制限について言及している。ただし、詳細に関する言及はない。

多くの場合、ファームウェアの漏洩は脆弱性検出又は End-to-End のセキュリティ攻撃を構築する突破口となるため、ファームウェア・ソフトウェアの開発者はセキュアコーディングの採用や開発プロセス中のセキュリティ対策をサポートするツールを使用すべきであるとされている。

また、多くのシステムでは外部フラッシュメモリをすべて暗号化することで、不正なデータの復元とファームウェアの解析を防止することができる。ファームウェアは、アップデート時にも取得される可能性があるため、第三者が非暗号のファームウェアを取得できないような対策をすべきであるとされる (6.7.4 Control Access to Firmware)。

また、ファームウェアの修正機能を制限することで、マルウェア感染リスクを下げるができる。例えば、デジタル署名の採用によって、車載 ECU における不正なファームウェアのブート防止及び不正プログラムのインストール防止を実現できる可能性がある (6.7.5 Limit Ability to Modify Firmware)。

サーバと車の接続については、多くの分野で使用されている暗号手法を適用すべきとある。これによって、有効な証明書が確認されない通信を排除することができる (6.7.10 Control Communication to Back-End Servers)。

3.3.2.2.3. 将来展望

具体的な将来展開についての記述はない。Best practices は、適宜維持・更新されていくリスクベースアプローチの重要なプロセスを、開発するための強固な基礎 (solid foundation) を提供しているとある (1. Purpose of This Document)。

3.3.2.3. Federal Motor Vehicle Safety Standards; V2V Communications NPRM

3.3.2.3.1. 概要

発行	2016/12
位置づけ	<仕様> NPRM 法制化のための事前通知 (素案) 公開時には comment が募集されており (現在は終了)、OEM, Tier1/Tier2, 業界団体、個人等から 400 を越えるコメントが寄せられている。
対象	<通信技術 (車外) > V2V 通信に使用する通信及びメッセージフォーマット (OTA を対象としたものではないが、内部で言及されているため紹介する)

DSRC を用いた V2V 通信によって、BSM の送受信を行うための法律案とその前提となった調査分析報告である。V2V 通信における相互互換性 (interoperability) の確保が V2V 通信システムの成功のためには不可欠であり、そのために政府の行動が必要とされている。

事故防止による投資効果の見直し説明から、通信技術、BSM のフォーマット、サイバーセキュリティまで多岐に渡っている。

BSM は、車速、方向、ブレーキ状況、他車情報などを含み、この情報を適宜送受信することで、衝突事故

の可能性があると判断された場合にドライバに警告が行われることを想定している。従来の車載センサーやカメラでは捉えられない死角にある車の情報や操作・挙動情報、遠距離（300m 超）での情報把握によって、従来の車載システムでは回避できない事故の回避が可能となると考えられている。

Cyber Security の章では、V2V 通信に限らず、車載アーキテクチャ全体でのアクセスポイントの保護や、ライフサイクルを通じた NIST Cyber Security Framework に準じたセキュリティ設計、Auto-ISAC を通じた情報共有など Cyber Security Best Practices for modern vehicle に対応した内容について言及されている。

セキュリティ基盤としては、PKI を用いた SCMS を採用している。

3.3.2.3.2. 遠隔ソフトウェア更新に関連する項目

III.E.6 で Software and Security Certificate updates として言及している。また、III.E.7 Cybersecurity の中でも言及がある。

- ・ 必要性

機能面、セキュリティ面、プライバシー問題に対応するため、周期的なアップデートが必要になると考えられている。

- ・ 方法

OTA リプログラミング。最終案が法制化されるまでに OTA リプログラミングが普通の手段になっていると想定されている。また、スマートフォンを用いて車載機器に新たなアプリケーションを導入することも考えられる。

- ・ 条件

アップデートは対象によらずユーザの承認が必要とされている。数回にわたって強調されており、通知・承認メカニズムが必要とされている。

- ・ 対象

- セキュリティ証明書(certificates)とプロトコル
- 異常動作(Misbehavior)検出アルゴリズム、ポリシー
- CRL コンテンツ、ポリシー
- デバイスファームウェア

SCMS で証明書とセキュリティプロトコルのアップデートは実施できるが、セキュリティ管理を実施するソフトウェアそのものはサプライヤー依存であり、各サプライヤーはセキュリティアップデートに対応できるようにしなければならない。

ただし、ソフトウェア更新については課題認識があるのか、コメントが強く求められている。また、脆弱性が発見されてから、対策パッチが適用されるまでの期間の対応についてもコメントが募集されている（なお、コメント募集期間は現時点では終了している）。

関連して、V2V 通信装置は、セキュリティクレデンシャルを狙った侵入に耐えられるようにハード化されたものである（FIPS-140 Level 3 相当）ことが提案されており、Certificates や security policies は FIPS-140 Level 3 ストレージに保存されるべきと信じているとある。なお、FIPS-140 Level 3 はストレージのみではなく、HSM にも必要とする提案が行われている（IV.D.5.(a).5）。

3.3.2.3.3. 将来展望

V2V 通信については、2019 年の法制化を見込んでおり、2021 年から適用開始予定。2023 年で新車 100% 適用を見込むとある。OTA については法制化時点では一般的な手段になっていることが想定されている。

3.4. 5GAA

3.4.1. 組織紹介

5GAA (5G Automotive Association⁹) は、自動車メーカー、半導体メーカー等から構成される国際団体である。主な活動として、コネクテッド・モビリティと安全に対する社会ニーズに対応することを目指し、通信ソリューションや自動運転に対応するための標準化などに取り組んでいる。2017年3月には EATA とコネクテッド・自動運転ソリューションの分野で協力する覚書に調印した¹⁰。

創設メンバーは、Ericsson、Intel、Huawei、Nokia、Qualcomm、Audi、BMW Group、Daimler AG であり、2017年9月の時点で約60社がメンバーとして5GAAのページに掲載されている。

3.4.1.1. 規格・発行物紹介

コネクテッド・カーに対しては5Gの広帯域を利用した用途が期待されているが、現時点ではOTAへの言及はない。

- The Case for Cellular V2X for Safety and Cooperative Driving (2016/11)

◇ <http://5gaa.org/pdfs/5GAA-whitepaper-23-Nov-2016.pdf>

4G LTE から5G までシームレスな展開が可能な Cellular V2X を提案するにとどまっている。

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

3.4.1.2. The Case for Cellular V2X for Safety and Cooperative Driving

3.4.1.2.1. 概要

発行	2016/11/23
位置づけ	<技術報告> (法的拘束力なし) ホワイトペーパー
対象	<ユースケース、通信技術> ADAS と CAD(Connected and Automated Driving)

3.4.1.2.2. 遠隔ソフトウェア更新に関連する項目

遠隔ソフトウェア更新に関連した直接的な記述はない。ここでは、当面は4G LTE を利用した Cellular V2X を推進していく方針であることが述べられている。

しかしながら、将来において、より安全な自動運転車(ADAS や CAD) を実現するためには5G への移行が必要である。センサーやレーダーなどだけでなく周囲のあらゆるものと接続するため、5G が提供する短いレイテンシと広帯域が必要だからである。ここで3GPP 規格ファミリーの一部である Cellular V2X は、4G LTE から5G への展開パスを確保していることが、5GAA は Cellular V2X を推進する理由であると述べている。

3.4.1.2.3. 将来展望

特になし。

⁹ <http://5gaa.org/>

¹⁰ <http://www.prnewswire.com/news-releases/5g-automotive-association-and-european-automotive-telecom-alliance-sign-a-partnership-mou-615215444.html>

3.5. ACEA

3.5.1. 組織紹介

ACEA（欧州自動車工業会）は、ベルギーのブリュッセルに本部を置く、欧州自動車メーカーの業界団体である。現在の加入企業は以下のとおり。

BMW グループ、DAF, Daimler, FCA, Ford ヨーロッパ、Hyundai ヨーロッパ、Iveco, Jaguar & Land Rover, PSA グループ、Renault グループ、トヨタ自動車ヨーロッパ、VW グループ、Volvo グループ

3.5.2. 規格・発行物紹介

3.5.2.1. ACEA Principles of Automobile Cybersecurity ¹¹

3.5.2.1.1. 概要

発行	2017年9月
位置づけ	本発行物自体は法的拘束力を持たない。
対象	自動車のサイバーセキュリティ

コネクテッド・カーの増加に伴い、自動車がサイバー攻撃を受けるリスクが高まっているため、本文書では、以下の六つの鍵となる Principle に関して記載されている。

1. Cultivating a cybersecurity culture
2. Adopting a cybersecurity life cycle for vehicle development
3. Assessing security functions through testing phases: self-auditing & testing
4. Managing a security update policy
5. Providing incident response and recovery
6. Improving information sharing amongst industry actors

3.5.2.1.2. 遠隔ソフトウェア更新に関連する項目

ソフトウェア更新に関連する項目としては、以下の記述がある。

<2. Adopting a cybersecurity life cycle for vehicle development>

本章では Secure ECUs, Secure network communication, Secure E/E architecture, Secure extended vehicle に関して言及されており、Secure extended vehicle のアイテムとして、下記3点に言及されている。

- ✓ Secure internet and back-end communication
- ✓ Secure remote fleet management systems (FMS) and remote diagnostics
- ✓ Secure over-the-air software updates

また、本章では Security functions として Security logs, Communication protection, Control keys and access, User data protection, Identification/authentication/authorization に関して言及されており、Security logs と Controls keys and access に関して以下のように説明されている。

Security logs: Security events should be logged when required. Access to the security logs are documented and protected from disclosure to unauthorised users. Furthermore, when required, security logs should be sent off-board, through a secure channel, for safe storage.

Control keys and access: Keys are managed securely, and the use of a trusted infrastructure (Public Key Infrastructure) is encouraged.

¹¹ http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf

< 4. Managing a security update policy >

本章では、サイバー脅威に向けて必要に応じセキュリティアップデート機能を準備することについて言及されており、OTA に関しては下記記述がある。

In any case, while secure over-the-air updates seem theoretically possible for many components, the need for physical updates might still be present in the years to come in a number of cases.

3.5.2.1.3. 将来展望

本発行物自体は法的拘束力を持たないが、ACEA が ENISA, UNECE/WP29, Auto-ISAC などへの勧告に利用されることが記載されている。また、ACEA 会員企業が ISO/SAE21434 における議論を進める上でのリファレンスとすることも言及されている。

4. 関連団体調査：システムレベル（通信）

本章では、システムレベルの中でも ITU-T や ISO など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た。

4.1. ITU-T SG16

4.1.1. 組織紹介

ITU (International Telecommunication Union) は国際連合の専門機関の一つであり、ITU-T (ITU Telecommunication Standardization Sector)、ITU-R (ITU Radiocommunication Sector)、ITU-D (ITU Telecommunication Development Sector) から構成される。ITU-T は電気通信標準化部門、ITU-R は無線通信部門、ITU-D は電気通信開発部門となっている。ITU は 193 カ国¹²、700 以上¹³のセクターメンバー／アソシエイトメンバーが参加している(2017 年 9 月現在)。

ITU-T SG 16 はマルチメディア分野の標準化を進める研究委員会であり、SG16 会合は 9 ヶ月に 1 回の頻度で開催され、SG16 配下の Question では、上記 SG16 会合とは別に個別の専門家会合が開催されている。

ITU-T SG16 配下には 12 の Question があり、この内、Question 27 (Vehicle gateway platform for telecommunication/ITS services and applications)において車載ゲートウェイに関する標準化が検討されている。なお、ITU-T で標準化された規格は勧告(Recommendation)として発行される。

4.1.2. 規格・発行物紹介

ここでは、ITU-T SG16 が公開している規格／発行物の中で、自動車の遠隔 (OTA; Over The Air)ソフトウェア更新に関連すると考えられる主な発行物(発行年月)/出典 URL を列挙する。

- F.749.2: Service requirements for vehicle gateway platforms (2017/3)

◇ <http://www.itu.int/rec/T-REC-F.749.2/en>

VGP のサービス要件やユースケースについて記載された勧告であり、OTA に関する要件についても記載されている。

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

4.1.2.1. F.749.2: Service requirements for vehicle gateway platforms

4.1.2.1.1. 概要

発行	2017/3
位置づけ	<勧告> (法的拘束力なし) ITU-T 勧告
対象	<ユースケース、通信技術、セキュリティ> 車載ゲートウェイ

4.1.2.1.2. 遠隔ソフトウェア更新に関連する項目

F.749.2 では、「I.5.2 Vehicle-to-cloud telematics scenario」に VGP 上のサービス、アプリケーションの遠隔ソフトウェア更新に関するユースケースが記載されている。なお、ここで定義されている VGP は、車両内のデバイスと車両内外のデバイスの通信機能を提供する車載ゲートウェイであり、上位レイヤではドライバとやり取りする機能も述べられている。また、自動車の走行に関する機能はスコープ外としている。遠隔ソフトウェア更新の目的としてはバグフィックスや機能追加のためのアップデートがあげられ、ソフトウェア更

¹² <https://www.itu.int/online/mm/scripts/gensel8>

¹³ <https://www.itu.int/online/mm/scripts/gensel11>

新プロセス全体をサイバー攻撃から守る必要があると記載されている。

また、ソフトウェア管理の要件は「8.6 Software management requirements」に記載されており、次のような要件があげられている。

- ・安全、セキュア、フレキシブルな方法で管理すること
- ・VGP内のソフトウェア管理を安全な方法でサポートすること
- ・車載バスを介してVGPと接続するデバイスのソフトウェア管理を安全な方法でサポートすること
- ・ソフトウェアバージョンの確認
- ・ログの信頼性と検証可能性のため、更新記録の署名、暗号化

4.1.2.1.3. 将来展望

関連する勧告として「F.749.1: Functional requirements for vehicle gateways (2015/11)」が発行済み。「G.V2A: Communications interface between external applications and a Vehicle Gateway Platform」、「H.VGP-ARCH: Architecture and functional entities of Vehicle Gateway Platform」の2件が策定中。

4.2. ITU-T SG17

4.2.1. 組織紹介

ITU-T SG17はセキュリティ分野の標準化を進めるITU-Tの研究委員会である。SG17配下には14のQuestionがあり、この内、Question 13 (Security aspects for Intelligent Transport System)においてITSにおけるセキュリティに関する標準化が進められている。なお、Question 13は2017年5月のTSAG会合で承認されたQuestionであり、Question 13の発足以前はQuestion 6 (Security aspects of telecommunication services, networks and Internet of Things)にて検討が進められていた。

4.2.2. 規格・発行物紹介

ここでは、ITU-T SG17が公開している規格／発行物の中で、自動車の遠隔ソフトウェア更新に関連すると考えられる主な発行物(発行年月)／出典URLを列挙する。

- X.1373: Secure software update capability for intelligent transportation system communication devices (2017/3)
◇ <http://www.itu.int/rec/T-REC-X.1373/en>
セキュアなソフトウェア更新について記載された勧告であり、ソフトウェア更新のシーケンスから各メッセージ内容について記載されている。

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

4.2.2.1. X.1373: Secure software update capability for intelligent transportation system communication devices

4.2.2.1.1. 概要

発行	2017/3
位置づけ	<勧告> (法的拘束力なし) ITU-T 勧告
対象	<通信技術 (車外)、更新手順、ハードウェア> 車載ゲートウェイ

4.2.2.1.2. 遠隔ソフトウェア更新に関連する項目

X.1373ではV2I通信における車載通信デバイスへの適用を目的としたソフトウェア更新手順について記

載している。なお、車両内の通信については勧告のスコープ外としている。また、データフォーマットと XML によるメッセージのサンプルを記載している。

勧告で記載されている OTA による遠隔ソフトウェア更新のシーケンスを次に示す。なお、本勧告では車内通信はスコープ外としているため、ステップ 2)、3)、10)、11)、12)、13) は一例としている。

- 1) 更新モジュールがサプライヤーから提供される。なお、このステップは以降のステップとは非同期に処理される。
- 2) VMG (Vehicle Mobile Gateway)が ECU に対し、ソフトウェアリストを要求する。
- 3) ECU はソフトウェアの状態を確認し、ソフトウェアモジュールリストを作成して VMG に報告する。
- 4) VMG は収集したリストを更新サーバに送信し、更新の有無を確認する。
- 5) 更新サーバは受信したリストの受領確認を VMG に送信する。
- 6) 更新サーバはリストに従い、車にインストール済みのソフトウェア状態を調査し、必要なソフトウェア更新を決定する。
- 7) 6)の処理に時間がかかる可能性があるため、VMG は定期的に更新の要否を更新サーバに問い合わせる。
- 8) 更新が存在する場合、更新サーバは更新のための URL を VMG に送信し、存在しない場合は、確認応答のみ送信する。
- 9) 更新が存在する場合、VMG は更新サーバに接続して更新モジュールをダウンロードする。
- 10) ECU への更新適用前、VMG はドライバに対し更新適用について確認する。
- 11) ドライバは更新適用を確認し許可する。
- 12) VMG は該当する ECU に更新ファイルを配信し、更新の適用を要求する。
- 13) 各 ECU は更新を適用し、適用結果を VMG にレポートする。
- 14) VMG は適用結果を更新サーバにレポートする。
- 15) 更新サーバは更新情報の受領確認を VMG に送る。更新適用が失敗したり、未適用の更新が見つかったりした場合、適用が成功するまで更新サーバはステップ 0~0 を繰り返す。

「7.1 General message format with security functions」では、メッセージ送信者の認証方法とメッセージの完全性検証について記載がある。ここでは、HSM による非対称暗号を用いた X.509 をベースとしたデジタル署名、共通鍵を利用した MAC のうち、一つは使用するべきとされている。

4.2.2.1.3. 将来展望

特になし。

4.3. ISO TC22

4.3.1. 組織紹介

国際標準化機構（こくさいひょうじゅんかきこう、英: International Organization for Standardization）、略称 ISO は、国際的な標準である国際規格を策定するための非政府組織。スイスのジュネーブに本部を置き、スイス民法による非営利法人である。公用語は英語・フランス語・ロシア語。各国 1 機関だけが参加できる。国際標準化機構が出版した国際規格 (IS) も ISO と呼ぶ。

ISO は、加盟国メンバーが 162 の標準化団体から成る、独立した非政府組織である。ISO は、国際標準の世界最大のボランティアな開発組織であり、国家間に共通な標準を提供することによって、世界の貿易を促進する。ほぼ 2 万ある規格は、工業製品や技術から、食品安全、農業、医療までのすべての分野をカバーし

ている。

ISOは主要な産業分野の標準化を、技術委員会 (Technical Committee) の下で行う。ISOには多くのTCが存在しており、TC22にて自動車関連の規格策定が行われている。

4.3.2. 規格・発行物紹介

ISOが発行する文書としては、IS, TS, TR などがある。

自動車の遠隔ソフトウェア更新に関するISO規格は現在存在しないが、ダイアグ通信・リプログラミングに関するISO規格として、TC22傘下のSC31 (Data Communication) において、下記などが策定されている。

- ISO 13400-1:2011
Road vehicles -- Diagnostic communication over Internet Protocol (DoIP) -- Part 1: General information and use case definition
◇ <https://www.iso.org/standard/53765.html>
- ISO 14229-1:2013
Road vehicles -- Unified diagnostic services (UDS) -- Part 1: Specification and requirements
◇ <https://www.iso.org/standard/55283.html>
- ISO 22901-1:2008
Road vehicles -- Open diagnostic data exchange (ODX) -- Part 1: Data model specification
◇ <https://www.iso.org/standard/41207.html>

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

4.3.2.1. ISO 13400 (DoIP)

4.3.2.1.1. 概要

ISO 13400では、インターネット・プロトコル・ベースの診断サービス向け通信標準 (DoIP) を規定している。ISO 13400では、DoIPでカバーされる一般的なユースケース事例、ISO 14229によって標準化されたサービスインターフェース向けインターネット通信プロトコル、DoIP向け物理層規格、などを規定している。

発行	2011年
位置づけ	<規格> (法的拘束力なし) IS規格
対象	<通信技術> 自動車のダイアグ通信分野

4.3.2.1.2. 遠隔ソフトウェア更新に関連する項目

遠隔ソフトウェア更新は有線通信によるソフトウェア更新との関係を考慮する必要があるため、本規格の内容にも留意しておく必要がある。

4.3.2.1.3. 将来展望

特になし。

4.3.2.2. ISO 14229 (UDS)

4.3.2.2.1. 概要

ISO 14229 (UDS) は、診断ツールと車内 ECU との間のサービスレベルのダイアグ通信仕様を規定する。

発行	2013 年
位置づけ	<規格> (法的拘束力なし) IS 規格
対象	<通信技術> 自動車のダイアグ通信分野

4.3.2.2.2. 遠隔ソフトウェア更新に関連する項目

遠隔ソフトウェア更新は有線通信（診断ツール）によるソフトウェア更新との関係を考慮する必要があるため、本規格の内容にも留意しておく必要がある。

4.3.2.2.3. 将来展望

特になし。

4.3.2.3. ISO 22901 (ODX)

4.3.2.3.1. 概要

ISO 22901 は診断データをやり取りする形式として、ODX を規定している。ODX は XML ベースの標準規格で、診断に関係する ECU データの記述に使用される。車両、ECU、テスターのメーカは、自動車メーカに依存しない同一の ODX 形式で、ECU 診断データを記述してやり取りすることができる。ODX は、オープンな交換フォーマットとして設計されているため、自動車メーカ間の共同プロジェクトでの使用に適している。

発行	2008 年
位置づけ	<規格> (法的拘束力なし) IS 規格
対象	<通信技術> 自動車のダイアグ通信分野

4.3.2.3.2. 遠隔ソフトウェア更新に関する項目

本規格は有線（診断ツール）によるダイアグ・リプログラミングに向けた規格であり、遠隔ソフトウェア更新そのものを対象とした規格ではないが、遠隔ソフトウェア更新を検討する上では本規格に留意しておく必要がある。

4.3.2.3.3. 将来展望

特になし。

4.4. ISO TC204

4.4.1. 組織紹介

ISO/TC204 は、ITS の標準化を専門に行っている委員会である。スコープに関する記述は以下のようになっており¹⁴、車内交通情報及びコントロールシステムはスコープ外（ISO/TC22 の管轄）となっている。

インターモーダル及びマルチモーダル要素を含む都市部及び農村部における路上交通に関する、情報、コミュニケーション及びコントロールシステムの標準化。そこには、ITS（高度道路交通システム）の分野における旅行情報、交通管理、公共交通、商用輸送、緊急時対応といったサービスを含む。

¹⁴ http://www.jsae.or.jp/01info/its/2016_bro_j.pdf

ISO/TC204 では、2017 年現在、下記 12 の WG が活動を進めており、

- (1) 概念設計（システムアーキテクチャ）、
- (2) インターフェース（メッセージセットなど）、
- (3) フレームワーク（データ辞書、メッセージテンプレート）、
- (4) システムの性能要件、
- (5) テスト方法、

などの観点で標準化案が検討されている。

- WG1: Architecture (USA) ※括弧内はコンビナー
- WG3: ITS database technology (Japan)
- WG4: Automatic vehicle and equipment identification (Norway)
- WG5: Fee and toll collection (Sweden)
- WG7: General fleet management and commercial/freight (Norway)
- WG8: Public transport/emergency (USA)
- WG9: Integrated transport information, management and control (Australia)
- WG10: Traveler information systems (UK)
- WG14: Vehicle/roadway warning and control systems (Japan)
- WG16: Communications (USA)
- WG17: Nomadic Devices in ITS Systems (Korea)
- WG18: Cooperative systems (Germany)

4.4.2. 規格・発行物紹介

調査の結果、OTA に関する規格・発行物は確認できなかった。

4.5. IEEE 802（車関係）

4.5.1. 組織紹介

IEEE (The Institute of Electrical and Electronics Engineers, Inc.)は電気・電子技術の学会であり米国に本部がある。40 万人以上の会員を有し、標準規格の策定、国際学会の開催、論文の発表等を行っている。IEEE 802 委員会では LAN に関する規格化が検討されており、データリンク層と物理層におけるサービス及びプロトコルが規格化されている。

4.5.2. 規格・発行物紹介

調査の結果、OTA に関する規格・発行物は確認できなかった。

4.6. Wi-Fi Alliance

4.6.1. 組織紹介

Wi-Fi Alliance は無線 LAN 製品の普及促進を目的とした標準化団体であり、約 500 社の企業が参画している。Wi-Fi Alliance ではメンバー企業間のコラボレーション促進、Wi-Fi テクノロジーの普及促進、周波数帯割り当てのルール作りの提言等を行っている。現在の作業分野の一つに Automotive があり、Wi-Fi 技術の自動車セグメントでのニーズやユースケースについて検討されている。

4.6.2. 規格・発行物紹介

調査の結果、OTA に関する規格・発行物は確認できなかった。

4.7. W3C

4.7.1. 組織紹介

W3C (World Wide Web Consortium ¹⁵) は、World Wide Web で使用される各種技術の標準化を推進するために 1994 年に設立された標準化団体、非営利団体。活動の一環としてコネクテッド・カーに関する検討を行っており、GENIVI Alliance ¹⁶ と自動車関連(IVI)の標準化を協力して行うため、MoU を締結している。ここでの報告は、この MoU に基づく GENIVI との一体として扱った上でのものとする。

4.7.2. 規格・発行物紹介

ここでは、W3C が公開しているサイト／発行物の中で、自動車の遠隔 ソフトウェア更新に関連すると考えられる主な発行物(発行年月)／出典 URL を列挙する。

- Automotive and Web at W3C

- ◇ <http://www.w3.org/auto/>

コネクテッド・カーに関するカバーページ

- Automotive Working Group

- ◇ <http://www.w3.org/auto/wg/>

HTML5 や JavaScript などのアプリケーション開発者向けに、次世代車載情報通信システム(IVI)や車両データにアクセスするためのプロトコルを通して Web 接続できるようにするための仕様を策定中のグループ。議長は Jaguar Land Rover、三菱電機。

この WG で策定中の主な仕様:

- Vehicle Information Access API

- ◇ <https://www.w3.org/TR/2017/WD-vehicle-information-api-20170605/>

車両信号(vehicle signals)やデータ属性にアクセスするための高レベル API の定義、エディタは ACCESS と IBM

- Vehicle Signal Server Specification

- ◇ <https://www.w3.org/TR/2016/WD-vehicle-information-service-20161020/>

クライアントアプリケーションが車両信号やデータ属性を GET/SET/SUBSCRIBE/ UNSUBSCRIBE するための WebSocket ベースの API、エディタは Jaguar Land Rover

- Automotive and Web Platform Business Group

- ◇ <http://www.w3.org/community/autowebplatform/>

W3C メンバー以外も参加できるコミュニティ

- Cyber-Security in the Connected Car Age GENIVI Conference - Seoul, October 21, 2015

- ◇ https://lists.w3.org/Archives/Public/public-auto-privacy-security/2015Oct/att-0005/Cyber-security_Connected_Car_Age-GENIVI.pdf

講演において、OTA リプログラミングを“Remote software update emerging for quicker fix of security flaws”として紹介している。

¹⁵ <http://www.w3.org/>

¹⁶ <http://www.genivi.org/>

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

4.7.2.1. Vehicle Information Access API

4.7.2.1.1. 概要

発行	2017/5 (ドラフト)
位置づけ	<仕様> (法的拘束力はない) 車両信号(vehicle signals)やデータ属性にアクセスするための高レベル API の定義。OTA リプログラミング実行時に必要と考えられる機能の一つ。
対象	<ユースケース> ユースケースの一つとして OTA リプログラミングを想定

4.7.2.1.2. 遠隔ソフトウェア更新に関連する項目

Over the Air でのアップデート時の初期段階で使用される機能。

4.7.2.1.3. 将来展望

不明

4.7.2.2. Vehicle Signal Server Specification

4.7.2.2.1. 概要

発行	2016/10 (ドラフト)
位置づけ	<仕様> クライアントアプリケーションが車両信号やデータ属性を GET/ SET/ SUBSCRIBE/ UNSUBSCRIBE するための WebSocket ベースの API。OTA リプログラミング実行時に使用されると考えられる機能の一つ。
対象	<更新手順> OTA リプログラミング

4.7.2.2.2. 遠隔ソフトウェア更新に関連する項目

Over the Air でのアップデート時の初期段階で必要となる機能。

4.7.2.2.3. 将来展望

未定

4.7.2.3. Cyber-Security in the Connected Car Age

4.7.2.3.1. 概要

発行	2015/10
位置づけ	<講演提案 ¹⁷ > (法的拘束力なし)。
対象	<ユースケース> OTA リプログラミング

4.7.2.3.2. 遠隔ソフトウェア更新に関連する項目

Over the Air でのアップデートに関する利点、懸念点を明確に記述。

¹⁷ https://lists.w3.org/Archives/Public/public-auto-privacy-security/2015Oct/att-0005/Cyber-security_Connected_Car_Age-GENIVI.pdf

4.7.2.3.3. 将来展望

具体的展望は不明である。ただし、W3Cは GENIVI Alliance と提携し、車載ソフトウェアプラットフォームへの Web 技術の導入を推進しようとしている。

4.8. Bluetooth SIG

4.8.1. 組織紹介

Bluetooth SIG (Special Interest Group)は Bluetooth の規格策定や認証を行う標準化団体である。メンバーシップは Promoter、Associate、Adopter があり、Promoter は 7 社、Associate は約 600 社、Adopter は約 3 万社となる。

4.8.2. 規格・発行物紹介

調査の結果、OTA に関する規格・発行物は確認できなかった。

4.9. oneM2M

4.9.1. 組織紹介

(1) 2012 年 7 月に、欧米アジアで七つの地域標準化機関が共同で設立し、運営している標準化団体（2015 年から TSDSI (インド) が加入)。

(2) 主なミッション：M2M/IoT サービス層規格の標準化 (Deliverables : TS (Technical Specification (normative)) 及び TR (Technical Report (informative)) の発行、プロダクト認証のためのテスト仕様書含む)

(3) 構成メンバー：

• Partner Type 1 (運営機関)：

ARIB (日本)、ATIS (北米)、CCSA (中国)、ETSI (欧州)、TIA (北米)、TSDSI (インド)、TTA (韓国)、TTC (日本)

• メンバー：

Partner Type 1 に加盟している Individual member (約 200 社)

• Partner Type 2 (外部参加団体)：

OMA、Broadband Forum、Global Platform、CEN、CENELEC

• Associate Member：

CESG (英国)、Ministry of Science, ICT and Future Planning (MSIP/韓国)、

National Institute of Standards and Technology (NIST/米国)、

Pacific Northwest National Laboratory (米国)、

State Secretariat of Telecommunications and for the Information Society (スペイン)、

United States Department of Transportation (米国)

4.9.2. 規格・発行物紹介

• TR-0026-Vehicular Domain Enablement

◇ <http://www.onem2m.org/technical/latest-drafts>

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

4.9.2.1. Vehicle Information Access API

4.9.2.1.1. 概要

発行	2017/09
位置づけ	<技術報告> (現時点で法的拘束力なし) 現在、技術報告書 (TR : Technical Report) として、Informative な文書として制定されているが、ここから、技術仕様書 (TS-0001 (Functional Architecture)、TS-0003 (Security Solutions) 等) に盛り込まれる内容があり、それらは Normative な規格となり、いわゆる拘束力のある技術仕様となる。
対象	<通信技術、更新手順、ユースケース> Vehicular Domain における oneM2M 技術のユースケース (リモートメンテナンス、車両データ収集サービス/データワイプサービス、ECU ファームウェアの OTA 更新)

4.9.2.1.2. 遠隔ソフトウェア更新に関連する項目

(1) 関連 Use Case として、以下の4件が6章に掲載されている。

6.2 Remote Maintenance Service

6.7 Vehicle Data Service

6.9 Vehicle Data Wipe Service

6.11 Secure Over-The-Air Firmware Update for Automotive ECUs

(2) Potential Requirements

(1) から導出される Potential Requirements が7章に記載されている。

(3) High Level Architecture

(1) 及び (2) を実現するための、Vehicle のハイレベルはアーキテクチャが8章に記述されている。

(4) Security

上記から導かれる Security に関する Key Issue は9.4章、Solution は10.5章、10.6章に記載されている。

4.9.2.1.3. 将来展望

TR-0026 Vehicular Domain Enablement は、oneM2M の TP#31 会合 (9/18-22) で承認され、リリース3として、2018年1月に他のTSやTRとともに発行される予定である。しかし、上記4.9.2.1.2に掲載されている4件のユースケースに関しては、既にRelease2のTR-0001 Use Caseに、全く同一のケースが含まれ、すでに承認されてオープンとなっており、それらをTR-0026に移動させたものとなっているものであるため、これらはオープンで参照可能なものとして取り扱うことができる。

また、現在、ITU-T と oneM2M が協力して、ITU 勧告化を進めており、現在、リリース2Aとして、TS-0001や他のTRがITU-T勧告として承認されている。今後、リリース3に関してもITU-Tの勧告として制定されることになるため、oneM2MのTSやTRが開発途上国においても、ITU-Tの技術仕様/技術報告書として参照されることが期待される。

5. 関連団体調査：システムレベル（部品）

本章では、システムレベルの中でも TCG や EVITA など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た。

5.1. TCG

5.1.1. 組織紹介

TCG (Trusted Computing Group¹⁸) は、信頼できるプラットフォーム／インフラ構築のため、必要になる種々ハードウェア、ソフトウェアの業界標準、統合的公開仕様の開発、普及を目的とする 2003 年発足の非営利団体である。組織は世界各地の約 90 社の会員企業、約 30 の国家機関／大学／業界団体のリエゾンで構成されている。

主な活動として、プラットフォーム／インフラを構成する種々のハードウェア、ソフトウェアについて、各々を専門とする作業部会 (Working Group) で仕様を策定し、上部組織である技術委員会が技術的側面から他の規格／標準との関係を調整し、理事会では上記リエゾン関係にある各国政府機関の動静／意見を踏まえ評価、確定、公開している。さらに、それらの仕様を、標準化団体として実績ある ISO, IETF 等に提案し、その結果、国際公開標準として認定されている。

TCG は世界各地域での活動活性化のため、各々の地域での支部設立に尽力している。日本支部は 2008 年に設立された。TCG の意義について、TCG 日本支部のサイトで次のように説明されている¹⁹。

TCG の組織は、個々の技術分野の専門家がそのグループで共同で仕様が可能となるよう、複数のワーキンググループから構成されています。これらのワーキンググループでは、競合と協業の立場にあるそれぞれのメンバーが、相互運用性が担保され、技術的に中立な、仕様の策定が行われます。

2004 年、世界中の多くのノート／デスクトップ PC に、TCG が仕様策定／公開したチップ (TPM; Trusted Platform Module, ISO/IEC 11889 認定) が搭載され、販売が開始された。その後、適用範囲を、携帯電話／スマートフォン、ATM、POS 端末、ルータ等ネットワーク機器、自動車を含む IoT 等に拡大している。

現常任理事企業は 13 社 (AMD, Cisco, Dell, Fujitsu, HP, HPE, Huawei, IBM, Infineon, Intel, Juniper, Lenovo, Microsoft) である。

5.1.2. 規格・発行物紹介

ここでは、TCG が公開している規格／発行物の中で、自動車の遠隔ソフトウェア更新に関連すると考えられる主な発行物(発行年月)／出典 URL を列挙する。

- TCG TPM 2.0 Library Profile for Automotive Thin Specification, Version 1.0 (2015/3)

◇ https://trustedcomputinggroup.org/wp-content/uploads/TCG-TPM-2.0-Automotive-Thin-Profile_v1.0.pdf

TCG 内の組み込み作業部会で、自動車サービス検討サブグループの活動の一環として、TPM を、自動車一台当たり数十から百個搭載されていると言われている車載マイクロコンピュータ (ECU) 個々に付随させるとの想定に基づいて、TPM 全体仕様からの必要最小限化を目指したものの、個々の ECU の OTA ソフトウェア更新をセキュアに実行することを目指している。

- Guidance for Securing IoT Using TCG Technology (2015/9)

◇ https://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf

TCG 内の組み込み作業部会で、IoT 検討向け検討サブグループの活動の一環として、米国国家標準化

¹⁸ <https://trustedcomputinggroup.org/>

¹⁹ <https://trustedcomputinggroup.org/work-groups/regional-forums/japan>

機関である NIST が公開した公式文書(SP800-147 : BIOS Protection Guidelines ²⁰)、その他を引用しながら、自動車を含む IoT 全般に対する "secure software/firmware update mechanism" 等を論じている。

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

5.1.2.1. Automotive Thin Spec

5.1.2.1.1. 概要

発行	2015/3/16
位置づけ	<p><仕様> (法的拘束力なし)</p> <p>本 Automotive Thin 仕様は、ISO/IEC 11889 として国際標準仕様認定を受けた TPM2.0 仕様書 ²¹ を基としている。車載 ECU の OTA ソフトウェア更新をユースケースとして想定し、その想定の下で必要なコマンドのみを必須とし、他を推奨、オプションと峻別した仕様書である。</p> <p>近い将来、例えばリコール時 OTA 対応が立法化/ガイドライン化される際、本仕様に基づく車載 ECU の OTA ソフトウェア更新が、推奨される技術的解決策の一つとして提示される可能性を想定している。(立法化/ガイドライン化は、具体的かつ公開されている仕様に基づく解決策の見通しがあってこそ可能であることについては、一般的理解が得られると考えられる。TCG はそれを狙っていると考えられる。)</p>
対象	<p><セキュリティ、ハードウェア、ユースケース (ECU ソフトウェア更新) ></p> <p>車載 ECU の OTA ソフトウェア更新を一つのユースケースとする、車載セキュリティチップ、その仕様及び運用フロー。</p>

5.1.2.1.2. 遠隔ソフトウェア更新に関連する項目

本仕様書内で、車載 ECU の OTA ソフトウェア更新において、以下のフローで処理することを提示している。

- 1) 本仕様に基づくチップ (Automotive Thin) が、担当する部分 (ECU) の、その時点でのソフトのハッシュを取得、自らが保持する秘密鍵で電子署名生成、車載ヘッドユニットに送信する。
- 2) ヘッドユニット経由で情報を受けたセンターが証明書 (公開鍵) を用いて、情報の真贋判定を行った後、現状を分析、最適なパッチを選択、ヘッドユニット経由で車載 ECU に届ける。
- 3) ソフトウェア更新後、再び Automotive Thin が、更新後のソフトのハッシュを取得、自らが保持する秘密鍵で電子署名生成、車載ヘッドユニットに送信する。
- 4) ヘッドユニット経由で情報を受けたセンターが、証明書 (公開鍵) を用いて、情報の真贋判定を行った後、OTA ソフトウェア更新完遂を確認、将来における検証可能性を担保した形でログを保管する (各々のノードにおけるエラー分岐も記述されている (ここでは割愛))。

ここで「OTA ソフトウェア更新完遂を確認、将来における検証可能性を担保した形でログを保管する」と、即ち、説明責任担保 (Accountability) は非常に大きな意味を持つと考えられるが、この仕様書ではこれ以上の説明はされていない。他の公式文書、例えば、米国国家標準化機関である NIST の公式文書(SP800-19 : Mobile Agent Security ²²) では、章を設けて 3.3 Accountability (11, 19/52) に説明している。

TCG は、この説明責任を公開標準仕様である TPM をベースにした技術で達成すると訴求している。

これらを実現するため、Automotive-Thin は、以下のビルディングブロックを持っている。

- At least one of RSA 2048 or ECC P256.

²⁰ <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf>

²¹ <https://trustedcomputinggroup.org/tpm-library-specification/>

²² <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-19.pdf>

- At least one symmetric algorithm. AES 128 is recommended, others are allowed.
- SHA-256. Other hash algorithms are allowed.

なお、上記に関し、以下の日本政府関連プロジェクトでの公開文書で言及されているので、参考に紹介させていただきます。

「平成27年度戦略的イノベーション創造プログラム（自動走行システム）：V2X等車外情報の活用にかかるセキュリティ技術の研究・開発プロジェクト」²³

各車載 ECU にセキュリティのモジュールを追加するアーキテクチャが提案されている。これは、すでに一般のコンピュータなどに対して普及している、Trusted Platform Module (TPM) を各 ECU で利用するものである。ただし、以下の図 5-1 で示す通り、全ての ECU に一様に同じモジュールを利用するのではなく、外部との通信の入り口となる Head Unit や車載 GW 部分にはより高機能なもの (Auto-Rich TPM) を、それ以外の各 ECU にはより簡易なもの (Auto-Thin TPM) を利用することを提案している (ただし、すべての ECU で Auto-Thin TPM を利用することも想定されている)。

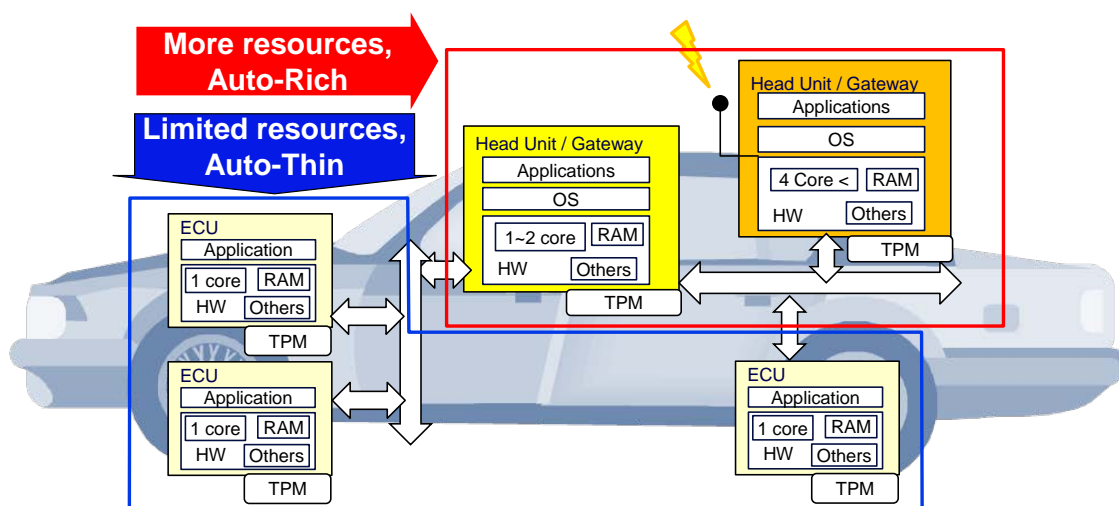


図 5-1 TPM Auto-Rich および Auto-Thin を利用した例

Auto-Rich と Auto-Thin を併用し、Head Unit/車載 GW が自動車内の ECU の署名を検証することにより、通信の相手先では Head Unit/車載 GW の署名のみを検証すればよくなる。また、自動車内の ECU に不正なものがある場合は、Head Unit/車載 GW の Auto-Rich TPM で検出し、Remote Center などへ報告される。この方式を利用することで、通信相手先の負荷は減るが、Head Unit/車載 GW の Auto-Rich TPM にリソースが必要となる。

5.1.2.1.3. 将来展望

リコール時 OTA 対応が立法化/ガイドライン化される時期は不明であるが、ソフトのみに起因するリコールの割合が増加 (2013 年時点で約 30%との報道あり²⁴) する傾向にあることは容易に理解できることであるので、そう遠くない将来と考えられる。

リコール時対応のみならず、自動運転時に必須となる、ダイナミックマップのセキュアな配信においても、OTA、リプログラミングという概念上、この仕様は有効であると TCG は主張している。すなわち、その時点での車載マップを正確に把握し、最適な更新情報を配信して、自動運転を支援する。その意味からも、この

²³ http://www.meti.go.jp/meti_lib/report/2016fy/000459.pdf

²⁴ <http://techon.nikkeibp.co.jp/article/STORE/20131216/322880/?rt=ocnt>

仕様の将来は有望であると TCG は考えている。

5.1.2.2. Guidance for Securing IoT Using TCG Technology

5.1.2.2.1. 概要

発行	2015/9/14
位置づけ	<ガイダンス> (法的拘束力なし) NIST が公開したガイドライン類を引用しながら、TCG 技術による IoT 全般における遠隔ソフトウェア更新等の方式を説明するガイダンスである。TCG 仕様が公開標準仕様であることを根拠に、Accountability を含む NIST の規定を満たすと訴求している。
対象	<セキュリティ、ハードウェア、ユースケース (ソフトウェア更新) > TCG 仕様に基づくセキュリティチップ、通信仕様その他を用いた、遠隔ソフトウェア更新運用フロー。

5.1.2.2.2. 遠隔ソフトウェア更新に関連する項目

このガイドラインにおいて、TCG 仕様は公開標準であることを強調し、その公開標準に基づいた遠隔ソフトウェア更新の意義を訴求している。

3. Use Cases の中で、機器の正常状態を保つために、セキュアに機器のソフトウェア状態(版数)を確認する機構と、セキュアにソフトウェア更新ができる機構が必要であると強調している。

また、この中の "Maintaining Audit Logs" の部分において、セキュアなログ管理/保存が、説明責任担保 "maintaining accountability" 及び分析可能性担保 "enabling forensic analysis" の本質であると明確に述べている。これは、5.1.2.1.2. で引用した NIST 文書(SP800-19)を TCG が強く意識していることを示している。即ち、SP800-19 で重要性を強調されている accountability を、公開標準仕様である TCG 技術によって実現可能であると TCG は訴求していると読むことができる。

4.4.1 Availability の章においては、NIST 文書(SP800-147)を引用する際、以下のように表現している。

The NIST document [800-147] describes requirements for PC-platform firmware-updates that are also applicable to IoT-devices.

5.1.2.2.3. 将来展望

本文書は、自動車を含む多くの機器がつながる世界において、NIST 文書の具体的展開を、公開標準 TCG 技術を用いたガイドラインとして示したものであり、多方面で用いられる可能性がある。また、この領域は動きが速いため、改訂作業も頻繁に行われる可能性がある。

5.2. EVITA

5.2.1. 組織紹介

EVITA は、欧州連合の第 7 次欧州研究開発フレームワーク計画の中のプロジェクトである。本プロジェクトの目的は、自動車の車載ネットワークにおけるセキュリティ関連コンポーネントの改ざん・改変やセンシティブなデータの危殆化を防ぐために、車載ネットワークのアーキテクチャを設計、検証、試作することである。2008 年から 2011 年の間に活動がなされた。

5.2.2. 規格・発行物紹介

ここでは、EVITA が公開している規格/発行物の中で、自動車の遠隔ソフトウェア更新に関連すると考えられる主な発行物(発行年月)/出典 URL を列挙する。

- Deliverable D2.1: Specification and evaluation of e-security relevant use cases (Dec. 2009)

◇ <https://www.evita-project.org/Deliverables/EVITAD2.1.pdf>

本報告では、セキュリティ対策が必要とされるであろう車載ネットワークのユースケースを記載している。18 のユースケースが記載されており、安全対策のアクティブブレーキ、車外エンティティからの交通情報、エンジン ECU の換装、リモート診断、リモートフラッシング（遠隔ソフトウェア更新）などを含む。各ユースケースに対して、必要となる機能、関与する通信エンティティと通信方法、通信される情報や必要なデータ、性能要件などを記載している。D2.1 に続く報告において、これらのユースケースを用いたセキュリティ要件の抽出が行われている。

- Deliverable D2.3 Security requirements for automotive on-board networks based on dark-side scenarios (Dec. 2009)

◇ <https://www.evita-project.org/Deliverables/EVITAD2.3.pdf>

本報告では、D2.1 のユースケースを対象にセキュリティ上の脅威を抽出し、リスクを算定、そして、セキュリティ要件を抽出している。本報告のセキュリティ要件を用いて、続く報告においてセキュリティアーキテクチャの設計がなされている。

- Deliverable D3.2 Secure on-board architecture specification (Aug. 2011)

◇ <https://www.evita-project.org/Deliverables/EVITAD3.2.pdf>

本報告では、EVITA のセキュリティアーキテクチャが記載されている。アーキテクチャはハードウェアモジュールとソフトウェアフレームワークからなる。ハードウェアモジュールは EVITA ハードウェアセキュリティモジュール (HSM) と呼ばれ、機能と性能のレベルが異なる三つの種類がある。ソフトウェアフレームワークは、通信制御、暗号サービス、相互認証、ポリシー決定、プラットフォーム統合、セキュアストレージ、セキュリティ監視のモジュールからなり、HSM と合わせて、EVITA セキュリティフレームワークを構成する。

- Deliverable D3.3 Secure on-board protocols specification (Jul. 2011)

◇ <https://www.evita-project.org/Deliverables/EVITAD3.3.pdf>

本報告は、車載ネットワークのユースケースをセキュアに実現するプロトコル仕様を記載している。D2.1 のユースケースを実現するのに必要となるセキュア車載プロトコルを抽出・分類し、D3.2 のセキュリティアーキテクチャのプラグインとしてプロトコルを設計している。プロトコルには、鍵配布プロトコル、セッション鍵確立プロトコル、遠隔アテストーションプロトコル、アクセス制御プロトコル、時刻同期プロトコル、遠隔ファームウェア更新プロトコル、などが含まれている。

以下、それぞれの概要及び遠隔更新に関連する部分の解説を行う。

5.2.2.1. Deliverable D2.1: Specification and evaluation of e-security relevant use cases

5.2.2.1.1. 概要

発行	2009/12
位置づけ	< 報告 > （現時点で法的強制力なし）
対象	< 通信技術（車内） > 自動車車載ネットワーク

5.2.2.1.2. 遠隔ソフトウェア更新に関連する項目

ユースケース 17 に Remote Flashing として遠隔ソフトウェア更新が記載されている。エンティティは、車外はサービスステーション、診断ツール(DT)、車内は通信ユニット(CU)、パワートレイン領域の ECU、パワートレインコントローラ(PTC) が関与する。表 5-1 のシーケンスによって、パワートレインコントローラ(PTC) のソフトウェア更新を行う例を記載している。

表 5-1 PTC のソフトウェア更新シーケンス

No.	アクター	受信者	データ/動作
1	サービスステーション	CU	接続要求
2	CU	ECU	接続要求
3	ECU	-	要求処理/完全性チェック、認証
4	ECU	CU	接続応答
5	CU	サービスステーション	接続応答
6	サービスステーション	CU	ECU 情報要求
7	CU	ECU	ECU 情報要求
8	ECU	-	認証/完全性チェック、フレッシュネス チェック
9	ECU	CU	ECU 情報応答
10	CU	サービスステーション	ECU 情報応答
11	サービスステーション	CU	暗号化済みファームウェア更新データ
12	CU	ECU	暗号化済みファームウェア更新データ
13	ECU	-	認証/完全性チェック、フレッシュネス チェック
14	PTC	-	更新データ復号、更新実行

関連するセキュリティ要素として、(機器)認証、データ認証、データフレッシュネス、否認防止、秘匿性、匿名性をあげている。

5.2.2.1.3. 将来展望

EVITA プロジェクトは 2011 年に終了しており、2017 年 9 月時点では、本発行物が改訂される予定はないと思われる。

5.2.2.2. Deliverable D2.3 Security requirements for automotive on-board networks based on dark-side scenarios

5.2.2.2.1. 概要

発行	2009/12
位置づけ	<報告> (現時点で法的強制力なし)
対象	<通信技術(車内)> 自動車車載ネットワーク

5.2.2.2.2. 遠隔ソフトウェア更新に関連する項目

本文書では、Remote Flashing 遠隔ソフトウェア更新のユースケース(Remote Flashing) から、セキュリティ要件が抽出されている。表 5-2 に、本文書から引用した遠隔ソフトウェア更新のセキュリティ要件を示す。

表 5-2 抽出されたセキュリティ要件

No.	セキュリティ要件	説明
1	Authenticity_29	ファームウェアが車両にインストールされる際には、製造者によって認証されプログラムされること。
2	Authenticity_101	コマンドが内部 ECU から別の内部 ECU に送信される際には、機能のパスに沿ってデータ認証をすること。
3	Authenticity_102	リプログラミングのためにコマンドが ECU に送信される際には、コードの生成元の認証をすること。
4	Authenticity_103	車外から車両にメッセージが到着したときに、データの生成元の認証をすること。
5		ロードサイドユニットにデータが送信される際には、機能のパスに沿ってデータの生成元の認証を行うこと。
6	Integrity_101	車外から車両にメッセージが到着したときに、メッセージの完全性を確実に保つこと。
7		ロードサイドユニットにデータが送信される際には、機能のパスに沿ってメッセージの完全性を確実に保つこと。
8	Integrity_102	リプログラミングのためにコマンドが ECU に送信される際には、そのコマンドの完全性を確実に保つこと。
9	Integrity_103	リプログラミングコマンドが ECU に送信されたときには、ファームウェアの完全性を確実に保つこと。
10	Integrity_104	コマンドが内部 ECU から別の内部 ECU に送信される際には、機能のパスに沿って情報の完全性を確実に保つこと。
11	Access_101	リプログラミングのためにコマンドが ECU に送信される際には、リプログラミング機能へのアクセス制御を確実に行うこと。
12	Access_102	リプログラミングのためにコマンドが ECU に送信される際には、フラッシュメモリへの読み込みのアクセス制御を確実に行うこと。
13	Freshness_101	車外から車両にメッセージが到着したときに、メッセージのフレッシュネスを確実に保つこと。
14		ロードサイドユニットにデータが送信される際には、機能のパスに沿ってメッセージのフレッシュネスを確実に保つこと。
15	Freshness_102	コマンドとなるメッセージが内部 ECU から別の内部 ECU に送信される際には、機能のパスに沿って情報のフレッシュネスを確実に保つこと。
16	Freshness_103	リプログラミングのためにコマンドが ECU に送信される際には、そのコマンドのフレッシュネスを確実に保つこと。
17	Confidentiality_1	無線通信の際も含めて、車両の ID は秘匿されること。
18	Privacy_101	TOE (Target Of Evaluation) やカーメーカの外部のエンティティで、サービスを提供するエンティティに車両からメッセージを送信する際には、e-サービスメッセージデータへのアクセス制御を行うこと。
19	Confidentiality_101	リプログラミングのためにコマンドが ECU に送信される際には、ファームウェアデータの秘匿性を確実に守ること。
20	Confidentiality_102	リプログラミングのためにコマンドが ECU に送信される際には、ファームウェア更新イベントの秘匿性を確実に守ること。
21	Availability_101	ECU や CU、ヘッドユニット、センサー、そのほかの車載ユニットの間で情報が交換される際には、バスの可用性が確実に保たれること。
22	Availability_102	ECU や CU、ヘッドユニット、センサー、そのほかの車載ユニットの間で情報が交換される際には、CPU の可用性が確実に保たれること。
23	Availability_103	ECU や CU、ヘッドユニット、センサー、そのほかの車載ユニットの間で情報が交換される際には、RAM の可用性が確実に保たれること。

24	Availability_104	車両から近隣の車両やロードサイドユニット、そのほかのエンティティに情報が送信される際には、CUの可用性が確実に保たれること。
25		近隣の車両やロードサイドユニット、そのほかの認可されたエンティティから車両が情報を受信する際には、CUの可用性が確実に保たれること。
26	Availability_105	車両から近隣の車両やロードサイドユニット、そのほかのエンティティに情報が送信される際には、無線媒体の可用性が確実に保たれること。
27		近隣の車両やロードサイドユニット、そのほかの認可されたエンティティから車両が情報を受信する際には、無線媒体の可用性が確実に保たれること。
28	Availability_106	車両から近隣の車両やロードサイドユニット、そのほかのエンティティに情報が送信される際には、最高レベルの優先度を持つ機能に対して要求されるデバイスの、最高レベルの可用性が確実に保たれること。
29		近隣の車両やロードサイドユニット、そのほかの認可されたエンティティから車両が情報を受信する際には、最高レベルの優先度を持つ機能に対して要求されるデバイスの、最高レベルの可用性が確実に保たれること。

5.2.2.2.3. 将来展望

EVITA プロジェクトは 2011 年に終了しており、2017 年 9 月時点では、本発行物が改訂される予定はないと思われる。

5.2.2.3. Deliverable D3.2 Secure on-board architecture specification

5.2.2.3.1. 概要

発行	2011/8
位置づけ	<報告> (現時点で法的強制力なし) 自動車業界・半導体業界での実装例あり
対象	<通信技術(車内)> 自動車車載ネットワーク

5.2.2.3.2. 遠隔ソフトウェア更新に関する項目

アーキテクチャを設計する際の想定ユースケースに遠隔ソフトウェア更新が含まれる。

なお、本報告は EVITA full、medium、light の 3 種類のハードウェアセキュリティモジュールを設計している。各モジュールの概要は、以下のとおりである。

EVITA full EVITA full は V2X 向けに設計されたセキュリティモジュールで、3 種類のうち最も高機能、高性能なモジュールである。ビルディングブロックを表 5-3 にまとめる。

表 5-3 EVITA full のビルディングブロック

No.	ビルディングブロック	説明
1	ECC-256-GF(p)	NIST 推奨曲線 P-256 上の 256 ビット楕円曲線暗号エンジン
2	WHIRLPOOL	AES ベースのハッシュ関数エンジン。ハッシュ値の長さは 512 ビット。
3	AES-128	NIST 標準ブロック暗号の鍵長 128 ビットの AES エンジン。利用モードとして、ECB、CBC、GCM、CCM をサポート。
4	AES-PRNG	BSI-AIS20-E.4 に準拠した、AES ベースの疑似乱数生成器のエンジン。内部の真正乱数生成器(TRNG)からのシード提供を受ける。

5	COUNTER	少なくとも 16 個の 64 ビットの単調増加カウンター。
6	時刻カウンター	外部と同期する UTC 時刻を刻むカウンター
7	内部 CPU	HSM 内部の CPU。ARM Cortex M3 又は類似の CPU を提案。
8	内部 RAM	HSM 内部の RAM。少なくとも 64k バイト以上。
9	内部不揮発メモリ	HSM 内部のフラッシュメモリ。少なくとも 32k バイト以上。(加えて 10k バイト以上の ROM。)
10	ハードウェア API	メイン CPU とアプリケーションから HSM 機能にアクセスするために規定された API。

EVITA medium

EVITA medium は ECU 向けに設計されたセキュリティモジュールで、3 種類のうち中間の機能、性能を持つモジュールである。EVITA full から、ECC-256-GF(p)エンジンと WHIRLPOOL エンジン在省いたもの。また、EVITA full に比べて、内部 CPU の性能が低くてよいとしている。(例えば、EVITA full は、Coretex²⁵ -M3 100MHz に対して、EVITA medium は Coretex-M3 50MHz など。)

EVITA light

EVITA light はセンサーやアクチュエータ向けに設計されたセキュリティモジュールで、3 種類のうち最も低機能、低性能を持つモジュールである。上位モジュールが持つビルディングブロックのうち、AES-128 エンジン、AES-PRNG、時刻カウンター、ハードウェア API のみを持つ。このうち、上位モジュールとは異なり、AES-PRNG は外部 TRNG からシード提供を受ける。なお、オプションとして、内部 RAM と内部不揮発メモリ、内部 TRNG を含む仕様を設定している。

5.2.2.3.3. 将来展望

EVITA プロジェクトは 2011 年に終了しており、2017 年 9 月時点では、本発行物が改訂される予定はないと思われる。なお、複数のチップベンダから、EVITA HSM に準拠したチップ²⁶が提供されている。

5.2.2.4. Deliverable D3.3 Secure on-board protocols specification

5.2.2.4.1. 概要

発行	2011/7
位置づけ	<報告> (現時点で法的強制力なし) 自動車業界・半導体業界での実装例あり
対象	<通信技術 (車内)、更新手順、ファームウェア> 自動車車載ネットワーク

5.2.2.4.2. 遠隔ソフトウェア更新に関連する項目

本報告では、遠隔ソフトウェア更新のプロトコル仕様が記載されている。遠隔ソフトウェア更新に関与する主なエンティティは、車外のエンティティとしてサービスステーションと診断ツール(DT)、車内のエンティティとしてセントラル通信ユニット(CCU)と ECU である。なお、CCU は車内の鍵マスター(KM)の役割を果たすため、以下では CCU-KM とともに記す。また、HSM_DT、HSM_CCU、HSM_ecu、HSM_oem は、それぞれ DT、CCU、ECU、OEM サーバに備えられた HSM を指す。

²⁵ ARM 社の CPU アーキテクチャ。

<https://developer.arm.com/products/processors/cortex-m/cortex-m3> を参照。

²⁶ 例えば、Infineon 社や Renesas 社、NXP 社などから、チップが提供されている。

<https://www.infineon.com/cms/jp/about-infineon/press/market-news/2016/INFATV201610-005.html>

<https://www.renesas.com/ja-jp/about/web-magazine/edge/solution/25-high-end-automotive-safety-mcu.html>

http://www.nxp.com/docs/en/supporting-information/E_SecurityMCU_JA.pdf

遠隔ソフトウェア更新プロトコルは、遠隔診断、ECU リプログラミングモード、ファームウェア暗号化鍵交換、ファームウェアダウンロード、ファームウェアインストール・検証の 5 ステップからなる。各ステップは次のとおりである。

遠隔診断

本ステップは、ECU タイプ、ファームウェアバージョン、最終更新日といった必要な情報を ECU から収集するステップである。プロトコルのアルゴリズムは次のとおりである。

- 1) DT が HSM_DT 内で共通鍵 Mk を生成する。
- 2) DT が HSM_DT から Mk をエクスポートする。なお、エクスポートする際には、HSM_DT 内で Mk を CCU の公開鍵 Pk_ccu で暗号化する。エクスポートデータを Exported-DT_Mk と記載する。
- 3) DT は、Exported-DT_Mk とタイムスタンプを結合したデータに DT の秘密鍵 Sk_dt で署名し、Exported-DT_Mk とタイムスタンプ、署名を CCU-KM に送信する。
- 4) CCU-KM は受信したタイムスタンプのフレッシュネスをチェック、署名を検証し、DT を認証する。
- 5) CCU-KM は、4 のチェック、検証が正しければ、Exported-DT_Mk を HSM_CCU にインポートする。なお、インポートの際には、HSM_CCU 内で Exported-DT_Mk が CCU の秘密鍵 Sk_ccu で復号される。
- 6) CCU-KM が HSM_CCU から Mk をエクスポートする。なお、エクスポートする際には、HSM_CCU 内で Mk を、ECU のタイプに応じて、ECU の公開鍵 Pk_ecu 又は共通鍵 Psk で暗号化する。エクスポートデータを Exported-CCU_Mk と記載する。
- 7) CCU-KM は、Exported-CCU_Mk とタイムスタンプを結合したデータに CCU-KM の秘密鍵 Sk_ccu で署名し、Exported-CCU_Mk とタイムスタンプ、署名を ECU に送信する。
- 8) データを受け取った ECU は、ポリシーに基づき CCU/DT の認可を確認、タイムスタンプのフレッシュネスをチェック、署名を検証する。
- 9) ECU は、8 が正しく通れば、Exported-CCU_Mk を HSM_ecu にインポートする。なお、インポートの際には、HSM_ecu 内で Exported-CCU_Mk が ECU の秘密鍵 Sk_ecu 又は共通鍵 Psk で復号される。
- 10) ECU は、Ack とタイムスタンプを結合したデータに、署名又は MAC を付加して、CCU-KM に送信する。
- 11) CCU-KM は、受け取ったデータの署名/MAC とタイムスタンプをチェックする。
- 12) CCU-KM は、11 のチェックが正しければ、Ack とタイムスタンプを結合したデータに、署名を付加して、DT に送信する。
- 13) DT は、受け取ったデータの署名とタイムスタンプをチェックする。
- 14) DT は、13 のチェックが正しければ、サービスステーションの従業員が選択したオプションに応じて、ECU から状態やログ情報などの診断情報を読み出す要求を送信し、情報を読み出す。

ECU リプログラミングモード

本ステップは、ECU のタイプが期待されるものであった場合、DT が ECU をアプリケーションモードからリプログラミングモードへと移行させるステップである。

- 1) DT がシード要求命令とタイムスタンプを結合したデータに、Mk で生成した MAC を付加し、ECU に送信する。
- 2) ECU は、データの完全性とフレッシュネスをチェックする。
- 3) ECU は、2 のチェックが正しければ、HSM_ecu 内でシード Na を生成し、Na を Mk で暗号化したデータ $\epsilon(\text{Na})\text{Mk}$ を取り出す。

- 4) ECU は、 $\epsilon(\text{Na})\text{Mk}$ とタイプスタンプを結合したデータに、Mk で生成した MAC を付加し、DT に送信する。また、ECU は、HSM_ecu で Na からリプログラミングモード移行用の鍵 Smk を生成する。
- 5) DT は、受け取ったデータの完全性とフレッシュネスをチェックする。
- 6) DT は、5 のチェックが正しければ、HSM_DT で Na を復号し、Na から Smk を生成する。
- 7) DT は、HSM_DT から Smk をエクスポートする。この際、Smk は Mk で暗号化された状態でエクスポートする。エクスポートデータは、Exported_Smk と記載する。
- 8) DT は、Exported_Smk とタイムスタンプを結合したデータに、Mk で生成した MAC を付加し、ECU に送信する。
- 9) ECU は、受け取ったデータの完全性とフレッシュネスをチェックする。
- 10) ECU は、10 が正しければ、HSM_ecu 内で Exported_Smk から Smk を取り出し、4 で HSM_ecu 自身が計算した Smk と比較する。
- 11) ECU は、10 の比較が一致した場合、リプログラミングモードに移行する。
- 12) ECU は、リプログラミングモードに移行したことを伝える Ack とタイムスタンプを結合したデータに、Mk で生成した MAC を付加し、DT に送信する。
- 13) DT は、受け取ったデータの完全性とフレッシュネスをチェックし、ECU のモード移行を確認する。

ファームウェア暗号化鍵交換

本ステップでは、ファームウェア暗号化鍵の交換を行う。

- 1) DT は、ファームウェア暗号化鍵要求とタイムスタンプに、Sk_dt で生成した署名を付加し、OEM サーバに送信する。なお、要求には ECU タイプや ECU 識別番号、ファームウェアバージョンなどの ECU についての情報が含まれる。
- 2) OEM サーバは、受け取ったデータの認証、完全性チェックを行う。
- 3) OEM サーバは、2 のチェックが正しければ、HSM_oem からファームウェア暗号化鍵 SSK をエクスポートする。この際、SSK を、ECU のタイプに応じて、ECU の公開鍵 Pk_ecu 又は共通鍵 Psk を用いて、暗号化した状態でエクスポートする。エクスポートするデータは、Exported-OEM_SSK と記載する。
- 4) OEM サーバは、Exported-OEM_SSK とタイムスタンプを結合したデータに、OEM サーバの公開鍵 Sk_oem で生成した署名を付加し、DT に送信する。
- 5) DT は、受け取ったデータを認証する。
- 6) DT は、5 が正しければ、Exported_SSK とタイムスタンプを結合したデータに、Mk で生成した MAC を付加し、ECU に送信する。
- 7) ECU は、受け取ったデータを認証する。
- 8) ECU は、7 が正しければ、Exported_SSK を HSM_ecu にインポートする。
- 9) ECU は、SSK がインポートされたことを伝える Ack とタイムスタンプとを結合したデータに、Mk で生成した MAC を付加し、DT に送付する。

ファームウェアダウンロード

本ステップは、DT が OEM サーバから受け取った暗号化かつ署名付加されたファームウェアを ECU にダウンロードするステップである。

- 1) DT が、SSK で暗号化され、かつ、署名付加されたファームウェアデータ、ECU コンフィギュレーションレジスタ(ECR)リファレンスとタイムスタンプを ECU に送信する。
- 2) ECU は、HSM_ecu で受け取ったデータの復号と検証を行い、ファームウェアを RAM に展開する。

なお、1のダウンロードと2のチェックは、ブロックごとに繰り返し行われる。

- 3) DTは、すべてのファームウェアデータがECUによってダウンロードされたら、transfer_exitメッセージとタイムスタンプを結合したデータに、Mkで生成したMACを付加し、ECUに送信する。
- 4) ECUは、3の認証を行う。
- 5) ECUは、3が正しければ、ダウンロードが完了したことを伝えるAckとタイムスタンプを結合したデータに、Mkで生成したMACを付加し、DTに送信する。

ファームウェアインストール・検証

本ステップは、ダウンロードしたファームウェアをECUにインストールするステップである。

- 1) ECUは、リプログラミングする前に、ファームウェアデータの署名を事前インストールされているOEMの製造者検証鍵(MVK)で検証する。
- 2) ECUは、1が正しければ、ファームウェアをインストールする。インストールは、ECR信頼チェーンを計算しながら実施される。
- 3) ECUは、ファームウェアのインストール後、ECUサプライヤーによって提供されるコールバックルーチンを用いて、ソフトウェアコンシステンシーチェックを実施する。
- 4) ECUは、ファームウェアの現在のECRとリファレンスECR値を比較する。
- 5) ECUは、4の比較が一致した場合、セキュアブート用にHSM_ecuのECR値をプリセットする。
- 6) ECUは、HSM_ecuのカウンター値をインクリメントする。
- 7) ECUは、ハードウェアリセットを行い、リプログラミング用のルーチンをフラッシュメモリから消去する。
- 8) ECUは、アプリケーションを開始する。

5.2.2.4.3. 将来展望

EVITAプロジェクトは2011年に終了しており、2017年9月時点では、本発行物が改訂される予定はないと思われる。

5.3. HIS

5.3.1. 組織紹介

HIS(The Herstellerinitiative Software)は、Audi, BMW, Daimler, Porsche, Volkswagen等で構成される委員会で、自動車製造業者がECUのソフトウェアや品質保証の原理と手法を習得することを助けることを目的としている。HISによって、2009年にセキュアハードウェアモジュールであるSHEの仕様が規格化されている。

5.3.2. 規格・発行物紹介

ここでは、HISが発行している規格/発行物の中で、自動車の遠隔ソフトウェア更新に関連すると考えられる主な発行物(発行年月)を列挙する。

- SHE - Secure Hardware Extension - Functional Specification Version 1.1. (Apr. 2009)

本文書は、車載マイコンにおけるハードウェアセキュリティモジュールのSHE規格の仕様を記載している。本文書は公開されていないため、本報告書には内容の詳細は記載しない。

次節では、公開されている文書から抽出したSHEの仕様概要について、記載する。

5.3.2.1. SHE - Secure Hardware Extension - Functional Specification Version 1.1.

5.3.2.1.1. 概要

発行	2009/4
位置づけ	<規格仕様(非公開)>、(現時点で法的強制力なし) 自動車業界・半導体業界での実装例あり
対象	<ハードウェア> 自動車車載 ECU

5.3.2.1.2. 遠隔ソフトウェア更新に関連する項目

SHE は、共通鍵ブロック暗号の AES エンジン、鍵や ID 等を格納するセキュアフラッシュメモリ等を持つ HSM である。以下、暗号エンジンとセキュアフラッシュメモリの仕様概要について説明する。

まず、AES の暗号エンジンに関しては、利用モードとして、ECB、CBC、CMAC をサポートする。また、AES をフィードバックモードで利用した PRNG も提供される。

セキュアフラッシュメモリについては、15 個の鍵スロットと 1 個の ID スロットからなる。鍵スロットは、1 個の ROM スロット、13 個のフラッシュメモリスロット、1 個の RAM スロットからなる。ROM スロットには、乱数生成用の鍵が設定される。フラッシュメモリスロットには、1 個のマスター鍵、1 個のセキュアブート用 MAC 鍵、1 個のセキュアブート用 MAC 値、10 個のアプリケーション用鍵のスロットがある。RAM スロットは、アプリケーション用鍵の格納に使われる。ID スロットは ROM スロットであり、HSM のユニーク ID である UID が格納される。これらの鍵の長さは 128 ビット、UID の長さは 120 ビットである。

フラッシュメモリの鍵スロットには、それぞれ 28 ビットのカウンター値と 6 ビットのフラグを持つ。カウンター値は、鍵更新の際にインクリメントされ、リプレイ攻撃を防ぐために利用される。フラグは、鍵の利用用途や鍵へのアクセス制御を定める。

SHE 上のセキュアフラッシュメモリの更新は、仕様書が規定するメモリ更新プロトコルによって実施される。セキュアに遠隔ソフトウェア更新をする場合、セキュアフラッシュメモリ上のセキュアブート用 MAC 値を更新する必要がある、プロトコルに従いメモリ更新をする必要がある。

5.3.2.1.3. 将来展望

複数のチップベンダから、HIS SHE に準拠したチップ²⁷ が提供されている。

²⁷ 例えば、Infineon 社や NXP 社から SHE を搭載したチップが提供されている。

<https://www.infineon.com/cms/en/about-infineon/press/market-news/2011/INFATV201111-012.html>

http://www.nxp.com/docs/en/supporting-information/E_SecurityMCU_JA.pdf

6. 今回の調査を踏まえての、標準化及び実用化に向けた課題整理

この章では、前章までの概要をまとめ、それに基づいて課題を整理する。

6.1. 3章から5章の記述／説明のまとめ

今回作業部会に参加頂いた各委員各々の知見／コネクションに基づいて調査／分析活動が行われた。ここに概要をまとめる。

3章では、SAEの技術報告やNHTSAのガイドラインに関して記述を行った。SAEの技術報告では、OTAを実装する場合にセキュリティや可用性を確保することが記載されている。また、NHTSAのCybersecurity best practiceでは、リプログラミング（有線／OTA）を車両に実装する際に留意すべき点（デバッグモード・開発モードへのアクセス制限、鍵管理、ダイアグアクセス制限、など）について言及している。いずれもOTAリプログラミングの実装を強制内容ではなく、リプログラミング機能を実装する際の上位レベルの要件記載となっている。ACEAが発行した文書”Principles of Automobile Cybersecurity”についての調査結果も報告した。OTAリプログラミングについての記述も含まれており、世界の大手自動車ベンダーが参加する団体の意向として注目される。

4章では、ITU-T勧告やISOのIS規格に関して記述した。OTAリプログラミングを直接の対象とするものとしては、ITU-T SG17においてソフトウェア更新手順、データフォーマット等に関する勧告、W3Cにおいてソフトウェア更新に必要と考えられる車両信号やデータ属性にアクセスするAPIに関するドラフト、oneM2Mにおいてユースケース、Potential Requirements、High Level Architecture等に関する技術報告が発行されている。なお、ITU-T SG17の勧告では、車両内の通信については勧告のスコープ外としている。また、ISOではOTAリプログラミングを直接の対象とはしていないものの、TC22においてダイアグ通信に関するIS規格が策定されており、OTAリプログラミングを検討する上では留意しておく必要があると考える。なお、いずれもOTAリプログラミングの実装を強制する内容ではない。

5章においては、OTAリプログラミングを実施するにあたって必要となるシステムレベル、部品の機能／仕様についての検討／策定状況をまとめた。具体的には、TCG、EVITA、HISの三つの組織での動きについて、それぞれが公開している情報を分析した。その結果、それらの活動に導かれて実際の複数の自動車ベンダーが具体的な検討段階に進みつつある状況であることが判明した。TCGに関する記述の中で、「標準化及び実用化に向けた課題整理」という観点から注目すべき動きの一つとして、5.1.2.1.2で記述した「OTAソフトウェア更新完遂を確認、将来における検証可能性を担保した形でログを保管する」、5.1.2.2.2で記述した「セキュアなログ管理／保存が、説明責任担保“maintaining accountability”及び分析可能性担保“enabling forensic analysis”の本質」が確固たるものとして想定され、これによって、セキュリティ攻撃への対策の高度化、それに加えて説明責任担保が重要であるとの認識が高まりつつあると考えられる。EVITAに関する記述の中で、将来展望の項に「EVITAプロジェクトは2011年に終了しており、2017年9月時点では、本発行物が改訂される予定はないと思われる」の記述がある。本報告書としては、近年の著しい動きを把握し、将来動向を検討する課題提供として報告することが主眼である。その趣旨において、この記述を吟味する必要があると付言する。HISでは、その将来展望の項に「複数のチップベンダから、HIS SHEに準拠したチップが提供されている」とまとめている。したがって、実用段階に達していると認識することが重要である。

これらによって、本報告書が主眼とするOTAリプログラミングの処理フローを含む技術開発及びその標準化に向けた活動は、2017年9月末時点での公開情報に基づく判断として、本書で取り上げた種々の機関／組織内で議論が進められていることが確認できた。議論の進捗状況、結論に至ったか／途中段階か、課題を

解決できたか／残されたままか等は、組織によって違いがあることも確認できた²⁸。これら調査結果が、今後の、自動車の遠隔更新技術を検討し、実現に近づけていく上で、重要な役割を果たすと考えられる。

6.2. 前章までの記述に基づく課題整理

実際の適用／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²⁹／配信／インストール／事後検証や5Gの応用³⁰で解決の目途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³¹、リプログラミング前後の完全性チェック³²、OTA リプログラミング処理中のセキュリティ攻撃³³等であると3章から5章の記述が示唆している。これら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、これまでの議論を総括すると、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が、描き切れていないのではないかと考えられる面がある。例えば、本報告の3.3.2.1.1(5)で述べた「テストはカーメーカ、部品メー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ある」は、公開標準仕様に基づく説明責任担保が前提と考えられるが、整理されているとは言えない面がある。

以上の各課題は、今後議論されるべき項目群であると考えられる。

²⁸ 5.1.2.1.2 章、3.1.2.6.2 章、5.2.2.1.2 章

²⁹ 3.1.2.2.2 章

³⁰ 3.4.2.1.2 章

³¹ 3.1.2.3.2 章、3.1.2.5.2 章

³² 5.2.2.1.2 章

³³ 3.1.2.6.2 章、3.1.2.7.2 章、5.3.2.1.2 章、4.1.2.1.2 章、3.3.2.2.2 章

7. まとめ

本レポートは、コネクテッド・カーとして通信機能を有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を把握することを目的作成した。今回の調査を通じ、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を把握した。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は非常に高く、セキュリティ攻撃への対策の強化、それに加えて公開標準仕様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を示した。

車載システムの遠隔更新の普及に当たっては、具体的ユースケースにおける価値、有効性／利便性が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は有意義であると考えられる。

今回の調査／検討に拠って、世界の各種組織での動きを迅速正確に把握し、日本における実用化活動を加速することの重要性を明確にした。本分野の検討は今後も継続されるため、日本から今回の調査対象を含む種々の動きについて継続して関与、貢献、寄与することが国際競争／協調上で極めて重要であるとする。

本レポートが、関連業界の皆様の検討にお役に立てれば幸いである。

<参考文献一覧>

SAE の 3.1 節で参照した文献

- [3-1-1] *Firmware Update Over The Air (FOTA) for Automotive Industry* (2007/8)
<http://papers.sae.org/2007-01-3523/>
- [3-1-2] *The New ECU Update Process* (2013/6)
<http://articles.sae.org/12250/http://articles.sae.org/12250/>
- [3-1-3] <http://papers.sae.org/2017-01-1613/>
- [3-1-4] *Analysis of Software Update in Connected Vehicles* (2014/4)
<http://papers.sae.org/2014-01-0256/>
- [3-1-5] *OTA reflashing: the challenges and solutions* (2016/1)
<http://articles.sae.org/14573/>
- [3-1-6] *Feasibility Study for a Secure and Seamless Integration of Over the Air Software Update Capability in an Advanced Board Net Architecture* (2016/4)
<http://articles.sae.org/14573/> <http://papers.sae.org/2016-01-0056/>
- [3-1-7] *Safe and Secure Software Updates Over The Air for Electronic Brake Control Systems* (2016/9)
<http://papers.sae.org/2016-01-1948/>
- [3-1-8] *OTA updating bring benefits, challenges*
<http://articles.sae.org/14946/>

U.S.DOT/NHTSA の 3.3 節で参照した文献

- [3-3-1] *Automated Driving Systems 2.0* (2017/09)
https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf
- [3-3-2] *Cybersecurity Best Practices for Modern Vehicles* (2016/10)
https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf
- [3-3-3] *Federal Motor Vehicle Safety Standards; V2V Communications NPRM* (2016/12)
http://www.safercar.gov/v2v/pdf/V2V%20NPRM_Web_Version.pdf
<https://www.gpo.gov/fdsys/pkg/FR-2017-01-12/pdf/2016-31059.pdf>
- [3-3-4] *NIST Cyber Security Framework*
<https://www.nist.gov/cyberframework>
- [3-3-5] *SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* (2016/1)
- [3-3-6] *ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*
- [3-3-7] *NIST FIPS PUB 140-2: Security Requirements for Cryptographic Modules* (2007/07)

5GAA の 3.4 節で参照した文献

- [3-4-1] *The Case for Cellular V2X for Safety and Cooperative Driving* (2016/11)
<http://5gaa.org/pdfs/5GAA-whitepaper-23-Nov-2016.pdf>

ACEA の 3.5 節で参照した文献

- [3-5-1] *ACEA Principles of Automobile Cybersecurity*
http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf
- [3-5-2] *ISO/SAE AWI 21434 Road Vehicles -- Cybersecurity engineering* (In Development)
<https://www.iso.org/standard/70918.html>

ITU-T SG16 の 4.1 節で参照した文献

- [4-1-1] *F.749.2: Service requirements for vehicle gateway platforms* (2017/3)
<http://www.itu.int/rec/T-REC-F.749.2/en>
- [4-1-2] *F.749.1: Functional requirements for vehicle gateways* (2015/11)
- [4-1-3] *G.V2A: Communications interface between external applications and a Vehicle Gateway Platform* (In Development)
- [4-1-4] *H.VGP-ARCH: Architecture and functional entities of Vehicle Gateway Platform* (In Development)

ITU-T SG17 の 4.2 節で参照した文献

- [4-2-1] X.1373: *Secure software update capability for intelligent transportation system communication devices* (2017/3)
<http://www.itu.int/rec/T-REC-X.1373/en>

ISO TC22 の 4.3 節で参照した文献

- [4-3-1] ISO 13400-1:2011 *Road vehicles -- Diagnostic communication over Internet Protocol (DoIP) - Part 1: General information and use case definition*
<https://www.iso.org/standard/53765.html>
- [4-3-2] ISO 14229-1:2013
Road vehicles -- Unified diagnostic services (UDS) -- Part 1: Specification and requirements
<https://www.iso.org/standard/55283.html>
- [4-3-3] ISO 22901-1:2008 *Road vehicles -- Open diagnostic data exchange (ODX) -- Part 1: Data model specification*
<https://www.iso.org/standard/41207.html>

W3C の 4.7 節で参照した文献

- [4-7-1] *Automotive and Web at W3C*
<http://www.w3.org/auto/>
- [4-7-2] *Automotive Working Group*
<http://www.w3.org/auto/wg/>
- [4-7-3] *Vehicle Information Access API*
<https://www.w3.org/TR/2017/WD-vehicle-information-api-20170605/>
- [4-7-4] *Vehicle Signal Server Specification*
<https://www.w3.org/TR/2016/WD-vehicle-information-service-20161020/>
- [4-7-5] *Automotive and Web Platform Business Group*
<http://www.w3.org/community/autowebplatform/>
- [4-7-6] *Cyber-Security in the Connected Car Age GENIVI Conference - Seoul, October 21, 2015*
https://lists.w3.org/Archives/Public/public-auto-privacy-security/2015Oct/att-0005/Cyber-security_Connected_Car_Age-GENIVI.pdf

oneM2M の 4.9 節で参照した文献

- [4-9-1] TR-0026-*Vehicular Domain Enablement*
<http://www.onem2m.org/technical/latest-drafts>

TCG の 5.1 節で参照した文献

- [5-1-1] CG (Trusted Computing Group)
<https://trustedcomputinggroup.org/>
- [5-1-2] TCG TPM 2.0 *Library Profile for Automotive Thin Specification, Version 1.0* (2015/3)
https://trustedcomputinggroup.org/wp-content/uploads/TCG-TPM-2.0-Automotive-Thin-Profile_v1.0.pdf
- [5-1-3] *Guidance for Securing IoT Using TCG Technology* (2015/9)
https://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf
- [5-1-4] NIST SP800-147:*BIOS Protection Guidelines*
https://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf
- [5-1-5] NIST SP800-19:*Mobile Agent Security*
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-19.pdf>
- [5-1-6] 平成 27 年度戦略的イノベーション創造プログラム（自動走行システム）：V 2 X 等車外情報の活用にかかるセキュリティ技術の研究・開発プロジェクト
http://www.meti.go.jp/eti_lib/report/2016fy/000459.pdf

EVITA の 5.2 節で参照した文献

- [5-2-1] Deliverable D2.1: *Specification and evaluation of e-security relevant use cases* (Dec. 2009)
<https://www.evita-project.org/Deliverables/EVITAD2.1.pdf>
- [5-2-2] Deliverable D2.3 *Security requirements for automotive on-board networks based on dark-side scenarios* (Dec. 2009)
<https://www.evita-project.org/Deliverables/EVITAD2.3.pdf>

[5-2-3] Deliverable D3.2 *Secure on-board architecture specification* (Aug. 2011)
<https://www.evita-project.org/Deliverables/EVITAD3.2.pdf>

[5-2-4] Deliverable D3.3 *Secure on-board protocols specification* (Jul. 2011)
<https://www.evita-project.org/Deliverables/EVITAD3.3.pdf>

[5-2-5] Arm Ltd, *Cortex-M3*
<https://developer.arm.com/products/processors/cortex-m/cortex-m3>

HIS の 5.3 節で参照した文献

[5-3-1] SHE - *Secure Hardware Extension - Functional Specification* Version 1.1. (Apr. 2009)

[5-3-2] Infineon *AUDO MAX SHE Enhances In-Vehicle Security and Tamper-Proofs Electronic Control Units*
<https://www.infineon.com/cms/en/about-infineon/press/market-news/2011/INFATV201111-012.html>

[5-3-3] ボディ・ゲートウェイ向け オンチップ・セキュリティ機能搭載 32 ビット・マイコン
http://www.nxp.com/docs/en/supporting-information/E_SecurityMCU_JA.pdf