



1. OTA Update基礎

スライド作成者の許可なく、掲載内容の一部又は全てを複製、転載、配布など、第三者の利用に供することはご遠慮いただきますようお願いいたします。

本章の目的

- 自動車のソフトウェア更新で登場する基本的な用語を理解する
- 自動車のOTA Updateの背景とサイバーセキュリティの重要性を理解する
- 自動車のソフトウェア更新に対する国際基準と国際標準の概要を理解する
- 自動車のOTA UpdateにおけるUptaneの位置付けについて理解する

アジェンダ

- 1. OTA Update
OTA, OTA Update, 特徴, 歴史
- 2. 自動車のOTA Update
自動車のOTA Update, 制度, ソフトウェア要因のリコール, 必要性
- 3. UN-R156
概要, プロセス, ソフトウェアの構成管理, 対象範囲
- 4. SUMS
概要, 要件
- 5. Uptaneの位置付け
OTA Updateフレームワーク, Uptaneの位置付け

- 1. OTA Update
OTA, OTA Update, 特徴, 歴史
- 2. 自動車のOTA Update
自動車のOTA Update, 制度, ソフトウェア要因のリコール, 必要性
- 3. UN-R156
概要, プロセス, ソフトウェアの構成管理, 対象範囲
- 4. SUMS
概要, 要件
- 5. Uptaneの位置付け
OTA Updateフレームワーク, Uptaneの位置付け

用語の定義

- Over The Air (OTA)
 - 無線通信を経由してデータを送受信すること
 - ただし、無線通信を経由してデバイスのソフトウェア更新を行うことを指す場合もあるため、要注意
- OTA Update
 - 無線通信を経由してデバイスのソフトウェアやデータの更新を行うこと
 - また、他の代表的な呼び方として、以下が存在する
 - **Software Updates Over The Air (SOTA)**
 - **Firmware Updates Over The Air (FOTA)**
 - **Over-the-air programming (OTA programming)**
 - **Over-the-air provisioning (OTA provisioning)**
- ソフトウェア更新
 - 有線無線に限らず、デバイスのソフトウェアやデータの更新を行うこと

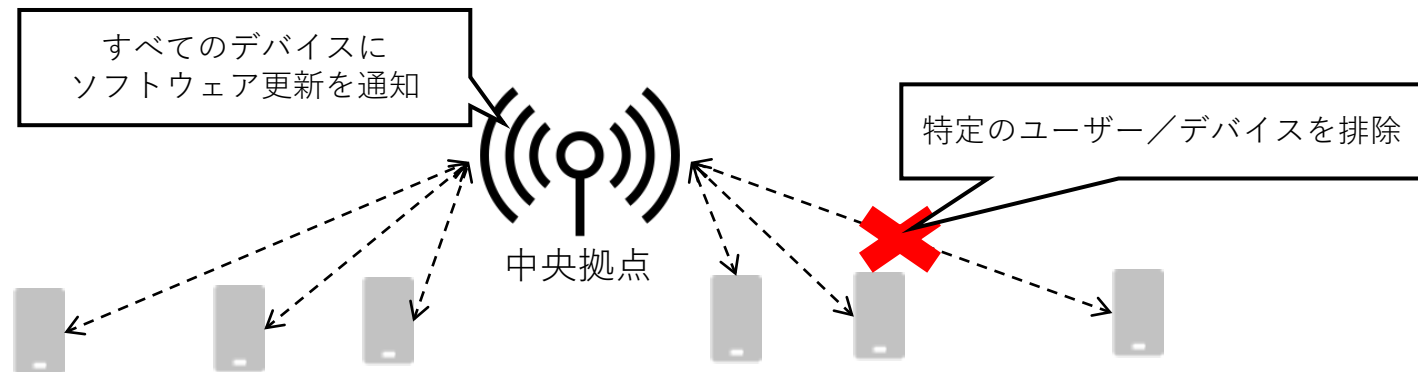
OTA Updateの歴史

- OTA Updateはモバイル機器の増加により導入されてきた
- 携帯電話／通信事業者
 - 1990年代以降，携帯電話会社や通信事業者はSIMカードのデータ更新設定，システム更新の配布，暗号鍵の更新などのため，SMSでOTA Updateを実施
- スマートフォン
 - 2000年代，サードパーティのアプリケーションをユーザが選択しインストール
 - アプリケーションがデバイスの差別化要因
- IoT(Internet of Things)デバイス
 - 2010年代に，初めてOTA Updateが免許不要の周波数帯（868 MHz，900 MHz，2400 MHz）と802.15.4やZigBeeなどのパーソナルワイヤレスLANプロトコルに採用

SMS: Short Message Service

OTA Updateの特徴

- 強制力のあるソフトウェア更新が可能
 - 中央拠点から無線通信を介して全ユーザーにソフトウェア更新を通知でき、ユーザーはそのソフトウェア更新を拒否することができず、そのチャンネルにいる全員にソフトウェア更新が直ちに適用可能
 - 一方で、もしユーザーがOTA Updateを拒否する場合には、中央拠点が自動的にチャンネルから「追い出す」ことも技術的には可能
 - 例. 特定のユーザー／デバイスを排除



OTA Updateの利点と欠点

- OTA Updateの利点

- 迅速なソフトウェア更新の適用
- 新規アプリケーションの配布が容易
- ソフトウェア更新にかかる負担（手間やコスト）の低減が可能
 - 例. 自動車会社がOTA Updateによって節約できるコストは2015年の27億ドルから2022年には350億ドルに拡大すると予測[1]

- OTA Updateの欠点

- 金銭面では通信利用料が必要
 - 例. デバイスがインターネットに接続される必要あり
- 技術/運用面ではサイバー攻撃の脅威にさらされる危険性あり

[1] <https://embeddedcomputing.com/application/automotive/ota-software-updates-now-serving-ecus-for-engine-brakes-and-steering>

OTA Updateで適用される技術

- 差分更新

- OTA Updateを実行する際、デバイス上のプログラムをすべて上書きするような更新方法をとると、更新時間が長いことが懸念
- このため、通常はデルタと呼ばれる差分更新プログラムを作成し配信することを差分更新と呼ぶ

- 差分更新のメリット

- ソフトウェア更新時間の短縮
- 通信トラフィックの削減

- デルタ作成技術

- bsdiff

- オープンソースによるバイナリ差分圧縮方式 [1]
- androidでも活用 [2]
- bsdiff の利用により、アプリの完全な APK のサイズと比べ、ソフトウェア更新のサイズを平均 47% 減 [3]

[1] <https://www.daemonology.net/bsdiff/>

[2] https://source.android.com/docs/core/ota/reduce_size?hl=ja

[3] <https://developers-jp.googleblog.com/2016/12/saving-data-reducing-the-size-of-app-updates-by-65-percent.html>

アジェンダ

- 1. OTA Update
OTA, OTA Update, 特徴, 歴史
- 2. 自動車のOTA Update
自動車のOTA Update, 制度, ソフトウェア要因のリコール, 必要性
- 3. UN-R156
概要, プロセス, ソフトウェアの構成管理, 対象範囲
- 4. SUMS
概要, 要件
- 5. Uptaneの位置付け
OTA Updateフレームワーク, Uptaneの位置付け

自動車のOTA Update

- カーナビゲーションシステム
 - 2007年，トヨタ自動車が最初に導入したのは，テレマティクスユニットを使ったカーナビゲーションシステムの地図の差分更新を実施 [1]
 - **ただし，この時点では制御ECUのソフトウェア更新は未実施**
- 制御ECUのソフトウェア更新の事例
 - 2018年，Tesla社はOTA Updateを実施し，アンチロックブレーキアルゴリズムのキャリブレーションを調整したと発表 [2]
- 自動車のOTA Updateの制度の創設
 - 自動車では保安基準に適合しているか認証する型式認証制度に影響
 - ➔ **ソフトウェア更新による不正（例．排ガス規制逃れ）が懸念**
 - ➔ **日本では道路運送車両法の一部を改正し特定改造等許可制度が創設**

[1] <https://global.toyota/jp/detail/1646667>

[2] <https://www.wired.com/story/tesla-model3-braking-software-update-consumer-reports/>

特定改造等許可制度

- 2020年11月より道路運送車両法の一部が改正され「特定改造等許可制度」が開始 [1]
- 特定改造等許可制度
 - 自動運行装置等に組み込まれたプログラム等の改変による改造を電気通信回線を使用する方法によりする行為等をしようとする者は、あらかじめ、国土交通大臣の許可を受けなければならないとする制度
- 特定改造等許可制度の許可に関する3要件
 - 能力：申請者が適切なソフトウェア更新及びサイバーセキュリティーを確保するために必要な業務管理能力を有すること
 - 体制：申請者がソフトウェア更新に起因した不具合の是正を適確に実施するために必要な体制を有すること
 - 保安基準適合性：ソフトウェア更新された自動車が保安基準に適合すること
 - 尚、「能力」は原則3年ごとの審査、「体制」と「保安基準適合性」は1件ごとの審査が必須
- 「特定改造等許可制度」による影響
 - 以前は、ソフトウェア更新で動力系の性能を変更すると日本の法規制上は「改造」に該当し「型式認証」を取り直す必要があった
 - この新制度により、「型式認証」を取り直しは不要で「申請」でソフトウェア更新が可能

自動車のセキュリティとソフトウェア更新

- black hat USA 2015でJeepの脆弱性が突かれ、140万台をリコール [1]
- 販売店やUSBを配布することでソフトウェア更新を実施
 - ➔ 自動車のサイバーセキュリティとソフトウェア更新が注目
 - ➔ 今後は脆弱性を持つ自動車はリコールしなければならない可能性あり
 - ➔ サイバーセキュリティとソフトウェア更新の国際基準の策定が進展



black hat USA 2015の発表時の様子 [1]



USBにて更新ソフトウェアが配布 [2]

[1] <https://blog.kaspersky.co.jp/blackhat-jeep-cherokee-hack-explained/8480/>

[2] <https://www.bbc.com/news/technology-34156598>

自動車基準調和世界フォーラム(WP29)

- 自動車基準調和世界フォーラム(WP29)

安全で環境性能の高い自動車を容易に普及させる観点から、自動車の安全環境基準を国際的に調和することや、政府による自動車の認証の国際的な相互承認を推進

- 制定・改正作業を行うとともに協定の管理・運営を実施

- 国際的な相互承認に関する基準

- 「国連の自動車等の型式認証相互承認協定（略称）」（1958年協定）
- 「国連の自動車等の世界技術規則協定（略称）」（1998年協定）

- 2020年6月に以下の国際基準が策定、車両型式認証の必須要件化

- サイバーセキュリティ(UN-R155)
- ソフトウェア更新(UN-R156)

国際基準が策定され、今後の自動車開発では対応が必須となった。
今後は段階的に対応自動車を増やしていくことが必要あり。

セキュリティ強化とOTA Updateの必要性(1/2)

- **国連規則の策定 … 型式認証において要求される国際基準**
 - UN-R155 (2021年3月に発行) [1]
 - Cyber security and cyber security management system
 - UN-R156(2021年3月に発行) [2]
 - Software Update Processes and Management Systems
- **国際標準の策定 … 各国際基準の参照先となる国際標準規格**
 - ISO/SAE 21434 (2021年8月に発行) [3]
 - エンジニアリングプロセスとサイバーセキュリティ要件を規定
 - サイバーセキュリティ上の脅威の排除に言及
 - ISO 24089 (2023年2月に発行) [4]
 - ソフトウェア更新に関する要件を規定

[1] <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security>

[2] <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update>

[3] <https://www.iso.org/standard/70918.html>

[4] <https://www.iso.org/standard/77796.html>

OTAを実現するにはUN-R155とUN-R156の対応が必須。

セキュリティ強化とOTA Updateの必要性(2/2)

- UN-R155およびUN-R156の適用が各国で進行中

地域	状況
欧州連合 (EU) [1]	2022年7月からすべての新型自動車にサイバーセキュリティに関する新規制が義務化 2024年7月からは生産されるすべての自動車に義務化
日本 [2]	2022年7月からOTA Updateに対応している新型自動車 2024年7月からOTA Updateに対応しているすべての自動車に義務化 2024年1月からOTA Updateに対応していない新型自動車 2026年5月からOTA Updateに対応していないすべての自動車に義務化
韓国 [3]	2020年後半にサイバーセキュリティに関する規則の条項を国家ガイドラインに導入。2022年に実施予定
カナダ [4]	Canadian Motor Vehicle Safety Standards (CMVSS)が発行するMotor Vehicle Safety RegulationsでSecurityに導入。
中国 [5]	幾つかGD/Tが策定されており、独自の基準が明確になりつつある

[1] <https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll>

[2] <https://www.mlit.go.jp/report/press/content/001379922.pdf>

[3] <https://unece.org/sustainable-development/press/three-landmark-un-vehicle-regulations-enter-force>

[4] https://tc.canada.ca/sites/default/files/migrated/tc_safety_framework_for_acv_s.pdf

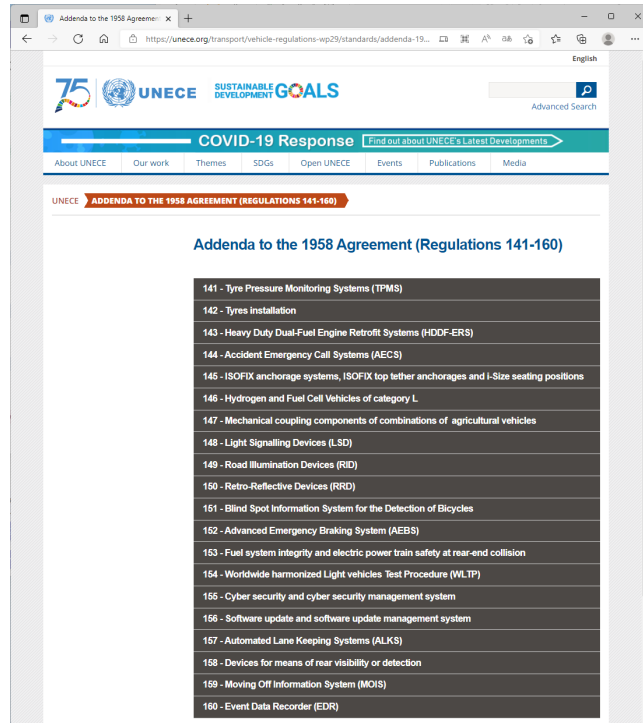
[5] <https://www.chinesestandard.net/PDF.aspx/GBT38628-2020>

アジェンダ

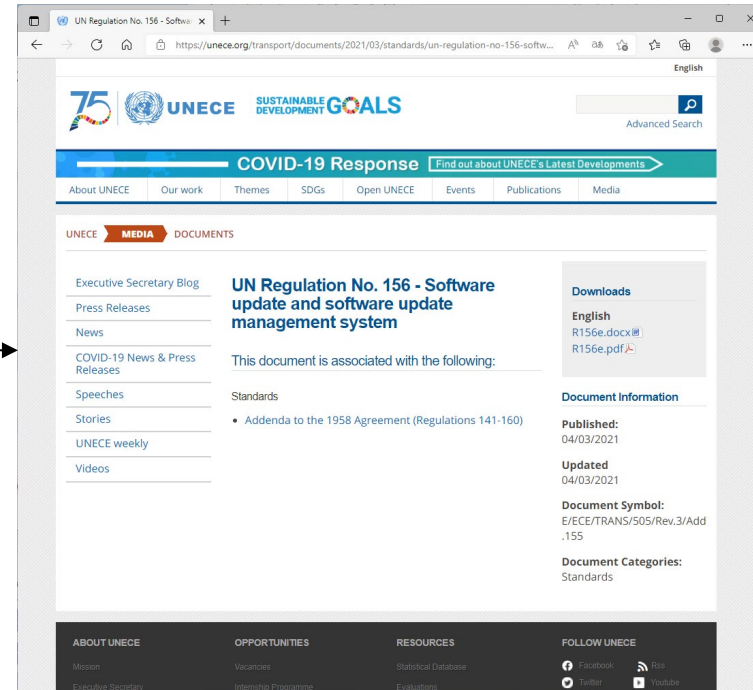
- 1. OTA Update
OTA, OTA Update, 特徴, 歴史
- 2. 自動車のOTA Update
自動車のOTA Update, 制度, ソフトウェア要因のリコール, 必要性
- 3. UN-R156
概要, プロセス, ソフトウェアの構成管理, 対象範囲
- 4. SUMS
概要, 要件
- 5. Uptaneの位置付け
OTA Updateフレームワーク, Uptaneの位置付け

UN-R156

2021年3月4日発行に“Software update and software update management system (SUMS)”というタイトルで発行



58協定 [1]



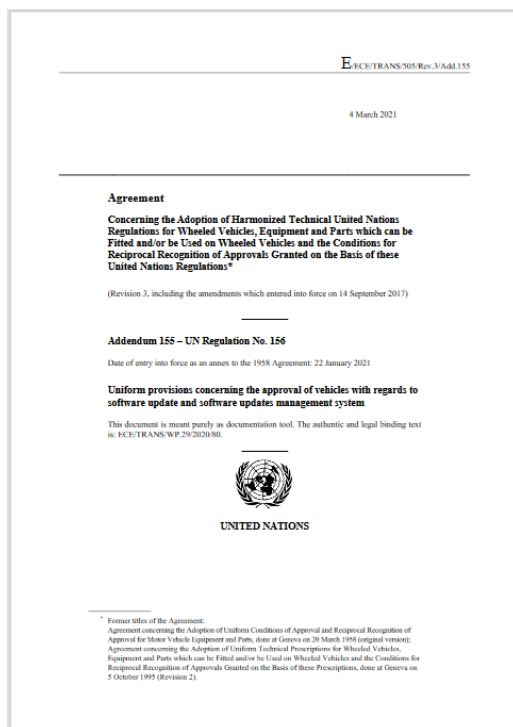
UN-R156 [2]

[1] <https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160>

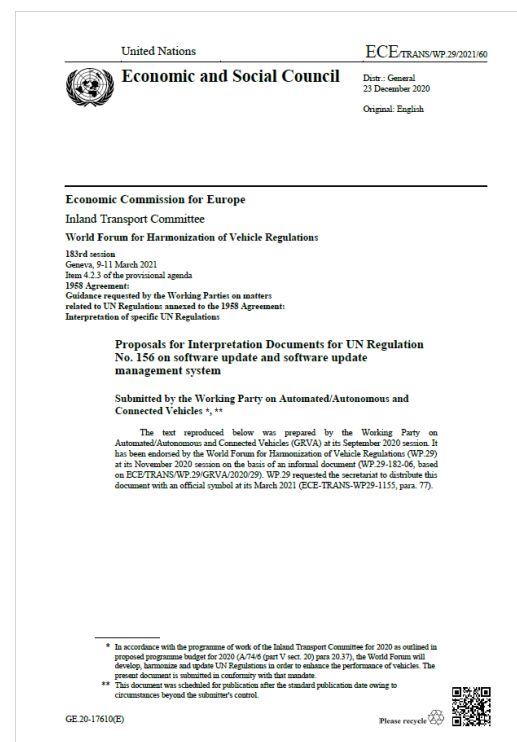
[2] <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update>

UN-R156

- UN-R156の本文 [1]
 - SUMSへの要求が書かれた文章
- UN-R156 interpretation document [2]
 - UN-R156の要求を解釈するための文書



UN-R156の本文 [1]



UN-R156 interpretation document [2]

[1] <https://unece.org/sites/default/files/2021-03/R156e.pdf>

[2] <https://unece.org/sites/default/files/2021-02/ECE-TRANS-WP29-2021-060e.pdf>

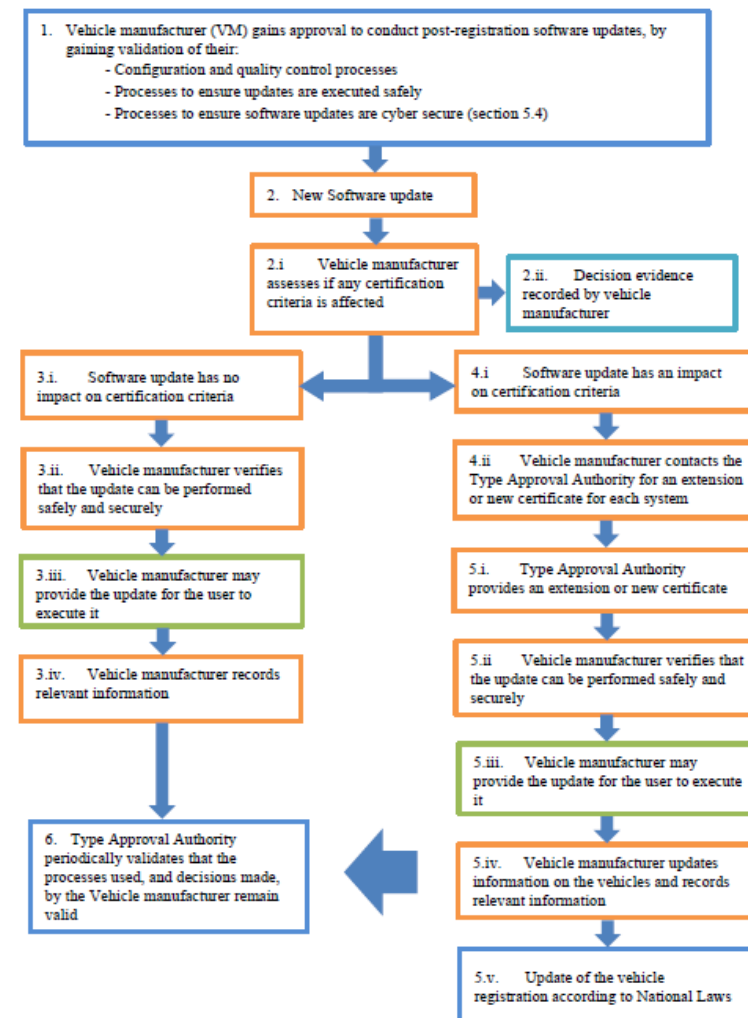
UN-R156におけるソフトウェア更新フロー[1]

ソフトウェア更新の事前条件

- 自動車会社(OEM)はSUMSを構築していること
- 自動車会社(OEM)はソフトウェア更新が自動車の型式認証されたシステムの承認の適合性に直接的又は間接的に影響を与えるかどうかを評価しその結果を文書化すること

ソフトウェア更新フロー（右図の要約）

- ソフトウェアのバグ修正など更新が型式認証システムのコンプライアンスに影響を与えない場合、自動車会社(OEM)は型式認証機関に連絡することなく更新を行ってもよいが、採用した更新プロセスが安全かつ確実であり、更新に関わる変更が文書化されていることを確認しなければならない
- 一方、更新が1つ以上の型式認証システムの適合性に影響を与える可能性がある、又は与えることになる場合、自動車製造業者(OEM)は影響を受けるシステムに対して延長又は新規認証を求めるために関連する型式認証機関に連絡しなければならない



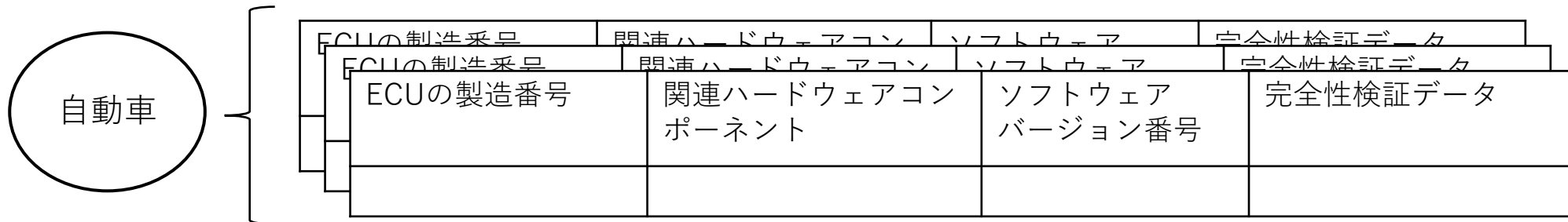
UN-R156での主要要件

- Software Update Management System(SUMS)認証
必要となるSUMSが構築されていることを立証
- ソフトウェアの構成管理とRXSWINの付与
RxSWINとは“Regulation x”に対する Software Identification Numberの略のことで、法規が要求するソフトウェアのバージョンを指す。
(例えば、UN-R156の場合、R156SWIN)
- Cyber Security Management System(CSMS)への適合
UN-R155が要求するCyber Security Management System (CSMS)に適合し、サイバーセキュリティ強化されていること

以降では、ソフトウェアの構成管理について説明する。

ソフトウェアの構成管理の要求

- **1. ソフトウェアの識別と管理プロセス**とは、型式認証されたシステムの完全性検証データを含むすべての初期及び更新されたソフトウェアバージョン、及び関連するハードウェアコンポーネントに関する情報を一意に識別することができるプロセス
- 目的は、自動車会社が使用する構成管理プロセスについて保証を提供し、これらが規則の実施を支援すること
- **2. バージョン番号**とは、ソフトウェア/ハードウェアの一意的な識別に関する規則の要求事項を満たすことが可能である限り、自動車レベルおよび/またはコンポーネントレベルで行うことができる
- **3. 完全性検証データ**とは、ソフトウェアが自動車会社が主張するバージョンであることをどのように認証するかということです。チェックサムやハッシュ値をこの目的に使用することができる
- **4. 関連ハードウェアコンポーネント**とは、型式認証されたシステム内のソフトウェアが搭載されたハードウェアを指す。これには、自動車会社(OEM)が特定するECU, CPUまたはその他のハードウェアが含まれるべきである
- **5. 一意に特定できる**とは、少なくとも、自動車会社(OEM)が型式認証された自動車システム上に存在するソフトウェアを、そのソフトウェアのバージョン番号に基づいて特定し、検証することが可能でなければならない



[1] <https://unece.org/sites/default/files/2021-02/ECE-TRANS-WP29-2021-060e.pdf>

ソフトウェアの構成管理とSBOM

- SBOM (Software Bill Of Materials)
 - ソフトウェア部品表のこと
- SBOMの必要性
 - ソフトウェアのサプライチェーンと存在する可能性のあるライセンスコンプライアンス、セキュリティ、および品質リスクに対する可視性を提供
 - **自動車でもすべてのソフトウェア更新がRxSWINに影響するとなるとリコールが必要になるため、細かくSBOMを管理することが重要**
- SBOMに対する社会的要求
 - バイデン政権が発表したサイバーセキュリティ大統領令 (Cybersecurity Executive Order and Software Supply Chain Security [1])
[1] <https://fossa.com/blog/cybersecurity-executive-order-software-supply-chain-security/>
- (大統領令で要求される)SBOMの構成要素として、以下の3要素が定義
 - Data fields: 各ソフトウェアコンポーネントの説明情報
 - Automation support: 人間及び機械が読める形式のSBOM自動生成機能
 - Practices and processes: SBOMをいつ、どのように生成し配布するか

次頁では、(大統領令で要求される)SBOMの構成要素の詳細について説明する。

(大統領令で要求される)SBOMの構成要素

- Data fields

以下のフィールドが含まれること

フィールド	内容
Supplier Name	サプライヤ名
Component Name	コンポーネント名
Version of the Component	コンポーネントのバージョン
Other Unique Identifiers	その他の固有識別子
Dependency Relationship	依存関係
Author of SBOM Data	SBOMデータの作成者
Timestamp	タイムスタンプ

- Automation support

組織を超えてSBOMを交換する際、以下のいずれかのフォーマットを使用すること

フォーマット	概要
Software Package Data Exchange (SPDX)	ISO/IEC 5962:2021として国際標準化
CycloneDX	OWASP Dependency-Track で使用するため 2017 年に設計された軽量な SBOM 仕様
Software Identification (SWID) Tags	ISO/IEC 19770-2:2015として国際標準化

(大統領令で要求される)SBOMの構成要素

- Practices and processes

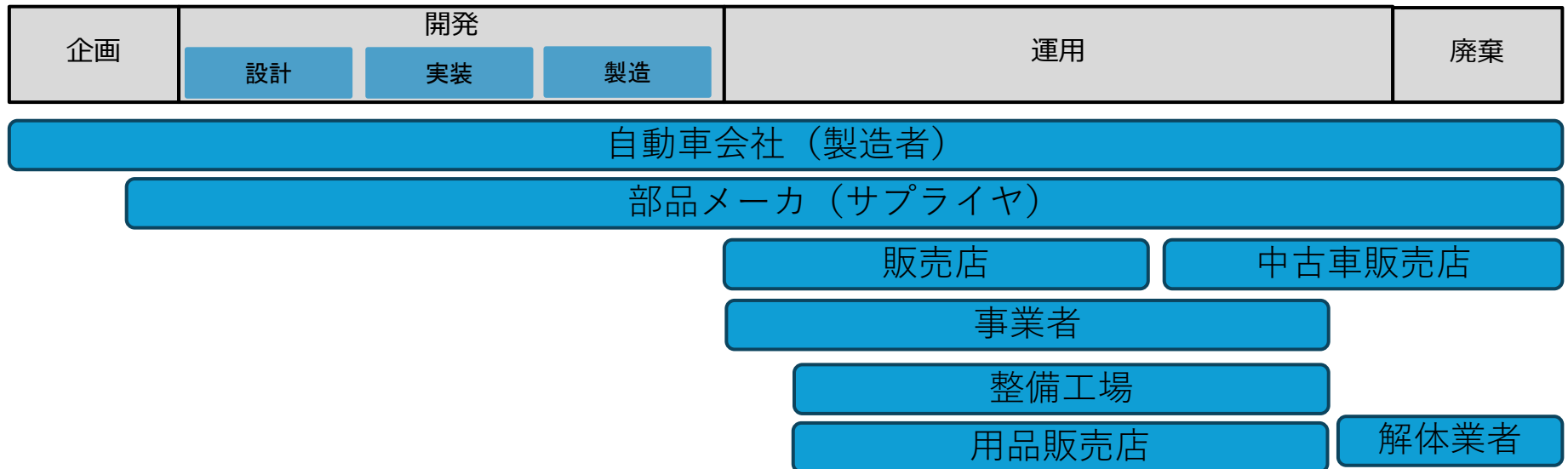
いつ、どのように更新して配信すべきかに関する以下の6つの観点が規定

観点	内容
Frequency (頻度)	新しいビルドやリリースによってソフトウェアコンポーネントが更新された場合、新しいSBOMを作成しなければならない。
Depth (深さ)	SBOM作成者は、トップレベルのコンポーネントとその推移的（間接的）な依存関係の両方を含める必要がある。
Known Unknowns (既知の未知のもの)	SBOMに完全な依存関係グラフが含まれていない場合、SBOM作成者は以下を記載すべきである。 a)そのコンポーネントにはそれ以上の依存関係がないのか b)依存関係の存在が「未知であり不完全である」
Distribution and Delivery (配布と配信)	SBOMは、適切なアクセス許可と役割が与えられた状態でタイムリーに利用可能でなければならない。
Access Control (アクセス制御)	SBOMの特定の要素を非公開にしようとする組織は、SBOMデータをユーザーのセキュリティツールに統合するための特定の許容範囲などに関するアクセス制御の条件を規定する必要がある。
Accommodation of Mistakes (誤りの許容)	SBOM作成に関する規制は新しいものであるため、SBOMの消費者は意図しないエラーや脱落に寛容であることが求められる。

ただし、自動車でどのようなSBOMで管理するかは未定義

自動車のライフサイクルとサプライチェーンへの影響

- 自動車の製品ライフサイクル (4段階)
 - 企画: 自動車の企画 → **ソフトウェア更新方式を決定**
 - 開発: 自動車の設計, 実装, 製造が含まれる → **ソフトウェアの構成管理を設計**
 - 運用: 自動車販売後の期間(平均10年程度) → **ソフトウェア更新を実行**
 - 廃棄: 自動車の廃棄時
- 自動車の製品ライフサイクルに関わるすべてのステイクホルダーに対応を要求
 - OEMが型式認証時に必要となるエビデンスの提供が必要
 - 運用にも影響があり, 開発に関連する事業者だけではない点に注意が必要



自動車のライフサイクルとソフトウェアの構成管理

従来からの変更点

- ライフサイクルの全段階でRxSWIN, SBOMの管理が必要
- 細かくソフトウェアを管理しなければ, 差分更新できずに更新時間が必要



ソフトウェア更新



VIN	RxSWIN	該当ECU	ソフトウェアバージョン
xx	012345678	ECU1	1.1
		ECU2	1.2
		ECU3	1.3
		ECU4	2.1

VIN	RxSWIN	該当ECU	ソフトウェアバージョン
xx	012345678	ECU1	1.1
		ECU2	1.3
		ECU3	1.3
		ECU4	2.1

ECU2のバージョンアップを実施

各ECUはSBOMの管理が必要

ECUの製造番号	ECUのソフトウェアバージョン	関連ハードウェアコンポーネント	ソフトウェアバージョン番号	整合性検証データ
ECU20001	1.2	HW001	1.0	Aaaaa
		HW002	1.2	Bbbbbbb
		HW003	1.0	Cccccc
		HW004	1.1	Ddddd

ECUの製造番号	ECUのソフトウェアバージョン	関連ハードウェアコンポーネント	ソフトウェアバージョン番号	整合性検証データ
ECU20001	1.3	HW001	1.0	Aaaaa
		HW002	1.3	Zzzzzz
		HW003	1.0	Cccccc
		HW004	1.1	dddddd

UN-R156の適用範囲

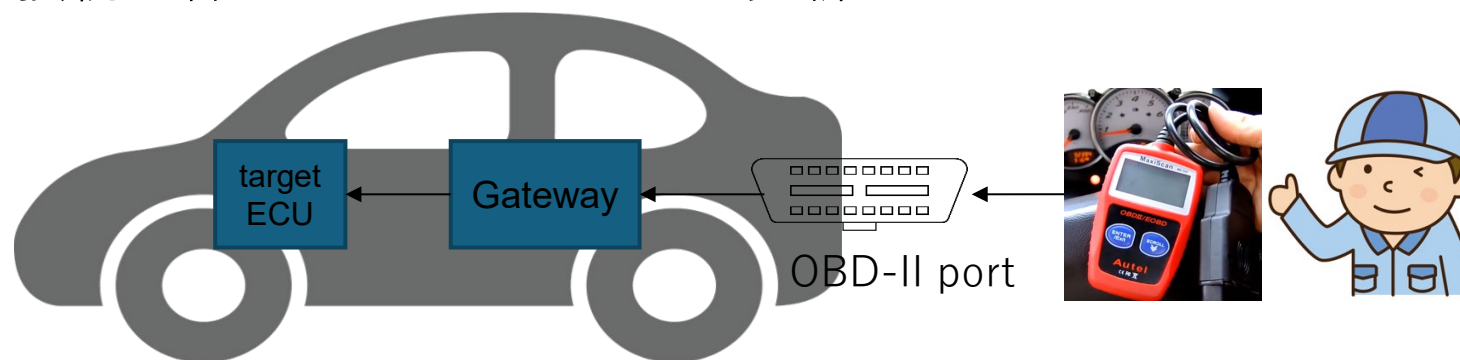
- UN-R156の適用範囲
 - **OTA Updateだけではなく、ソフトウェア更新全般に言及**
→ **既存する自動車のソフトウェア更新方法にも適用が必須**
- 自動車のソフトウェア更新方法
 - 方法1. 販売店によるソフトウェア更新
 - 方法2. 所有者によるソフトウェア更新
 - 方法3. OTA Update

UN-R156は、すべてのソフトウェア更新方法に適用される。
以降では、各方法について説明する。

自動車のソフトウェア更新方法

• 方法1. 販売店によるソフトウェア更新

- 自動車に搭載される診断通信用コネクタ(OBD-IIコネクタ)に診断機を接続し各ECUのソフトウェアを更新



• 方法2. 所有者によるソフトウェア更新

- USBメモリなどを用いて、ソフトウェアを更新
- メーカーからUSBメモリの配布, 所有者自身でUSBを作成し更新



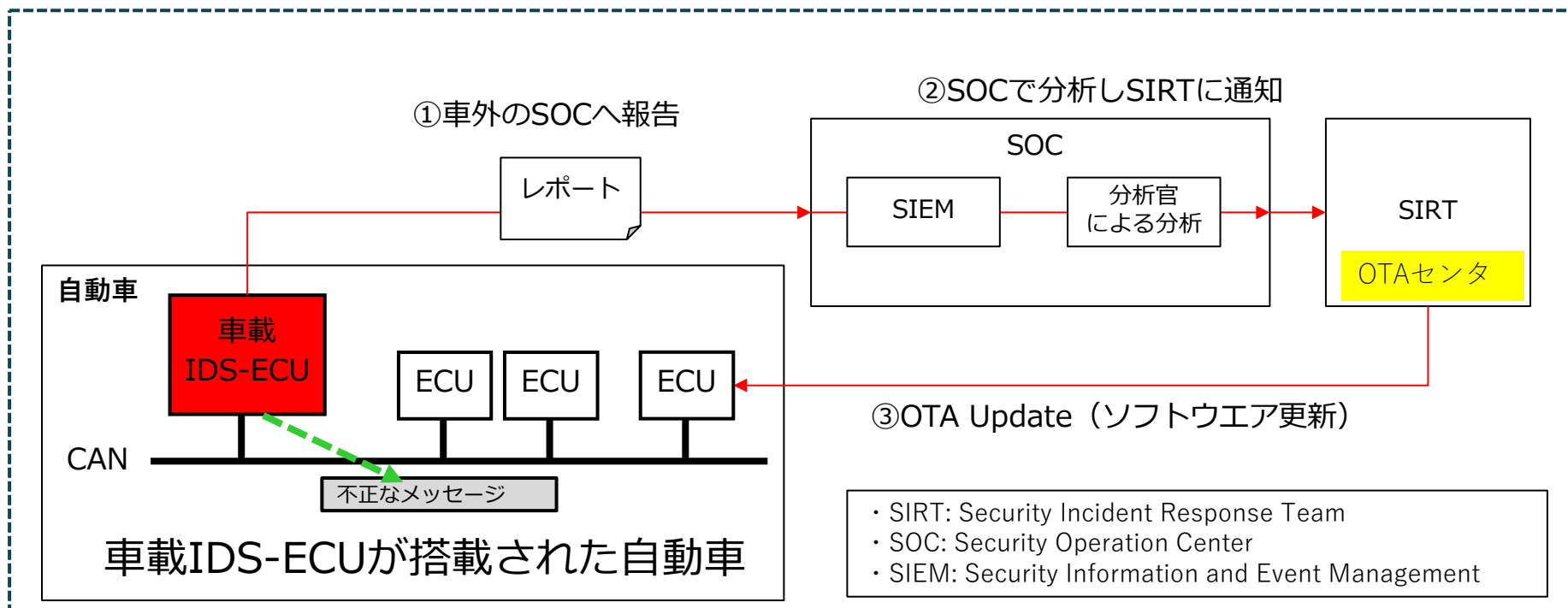
自動車のソフトウェア更新方法

• 方法3. OTA Update

- OEMが運用するSIRT(OTAセンタ)がソフトウェア更新の管理や配信を実施
- 自動車は常にソフトウェアの更新状態をSIRT(OTAセンタ)に通知

• OTA Updateにおける追加の要求

- 遠隔からの自動車の監視が必須化
- SOCで自動車内のECUの異常を判別し，OTAセンタからOTA Updateを実施



自動車のソフトウェア更新方法の比較

- OTA Updateのメリット
 - キャンペーン適用時の運用コストを低減できることが期待
- OTA Updateのデメリット
 - 自動車に無線通信インフラが必要，通信料金がかかる
 - ソフトウェア更新パッケージを配信するシステムが必要
 - ➔ Software Update Management System (SUMS) が必要
 - ➔ UN-R156ではSUMSに対する要求を定義

	方法1 販売店によるソフトウェア更新	方法2 所有者によるソフトウェア更新	方法3 OTA Update
パッチ適用にかかるコスト (キャンペーン実施コスト)	× (高い, 作業が必要)	△ (中程度, 郵送コストが必要)	○ (低い, 販売店の作業が不要)
パッチ適用の即時性	△ (時間がかかる)	△ (時間がかかる)	○ (適時配布可能)
SUMSの必要性	必須	必須	必須

UN-R156とISO 24089の関係

- UN-R156は法的拘束力があるため、適合しないと自動車や部品を他の国へ輸出したり販売することが出来なくなる懸念
- 国際標準ISO 24089はUN-R156に適合することが出来るよう、必要なエンジニアリングプロセスが規定

	国際基準	国際標準
	UN-R156	ISO 24089
策定者	政府，政府から依頼された機関	産業界，標準化団体の委員
ゴール	法的拘束力のある要件	国際基準を満たすために必要な要件
内容	<ul style="list-style-type: none">・ 自動車のソフトウェア更新の適合すべき要求・ ソフトウェア更新の管理すべき要件・ SUMSの要求	<ul style="list-style-type: none">・ ソフトウェア更新に関するエンジニアリングプロセスの定義・ SUMSのベースラインを策定

国際標準は、国際基準を満たすためのベースラインのコンセンサスを決定
国際基準を満たすためには国際標準の参照が必須。

ISO 24089

- 2022年1月11日にDIS(ドラフト)が発行後, 2023年2月に第1版が発効
- 内容としては, 4章以降で具体的な要件に言及
- ただし, 現時点ではプロセス要件が中心
- プロダクト要件は主に6章と7章が中心

4章: 組織

5章: プロジェクト

1. Scope			
2. Normative references			
3. Terms and definitions			
4. Organization level software update requirements			
5. Project level software update requirements			
6. Infrastructure design and development	7. Vehicle and vehicle systems design and development	8. Software update package development	9. Software update campaign operations

6章: インフラと7章: 自動車システム

8章: ソフトウェアパッケージ

9章: キャンペーン運用

ISO 24089の各章のキーワード

- 4章. 組織レベル
 - ガバナンス, 継続的な改善, 情報共有, 監査, サポート
- 5章. プロジェクトレベル
 - プロジェクト管理, テーラリングと理論的根拠
- 6章. インフラの設計と開発
 - リスク管理, 自動車構成情報の収集と管理, ソフトウェア更新キャンペーン情報の収集と管理, ソフトウェア更新パッケージの作成と管理と配布, ソフトウェア更新キャンペーンの障害の管理
- 7章. 自動車システムの設計と開発
 - 自動車及び/又はそのECUの安全性及びサイバーセキュリティのリスクを管理, 自動車構成情報を管理, ソフトウェア更新キャンペーンに関する情報の管理, ソフトウェア更新パッケージの検証
- 8章. ソフトウェア更新パッケージの開発
 - ソフトウェア更新パッケージの対象及び内容の特定, 組み立て, 検証・妥当性確認, リリースの承認
- 9章. キャンペーンの運用
 - ソフトウェア更新キャンペーン準備, 実施, 終了

詳細については権利の都合上解説できませんので、規格文書をご一読下さい

アジェンダ

- 1. OTA Update
OTA, OTA Update, 特徴, 歴史
- 2. 自動車のOTA Update
自動車のOTA Update, 制度, ソフトウェア要因のリコール, 必要性
- 3. UN-R156
概要, プロセス, ソフトウェアの構成管理, 対象範囲
- 4. SUMS
概要, 要件
- 5. Uptaneの位置付け
OTA Updateフレームワーク, Uptaneの位置付け

Software Update Management System(SUMS)

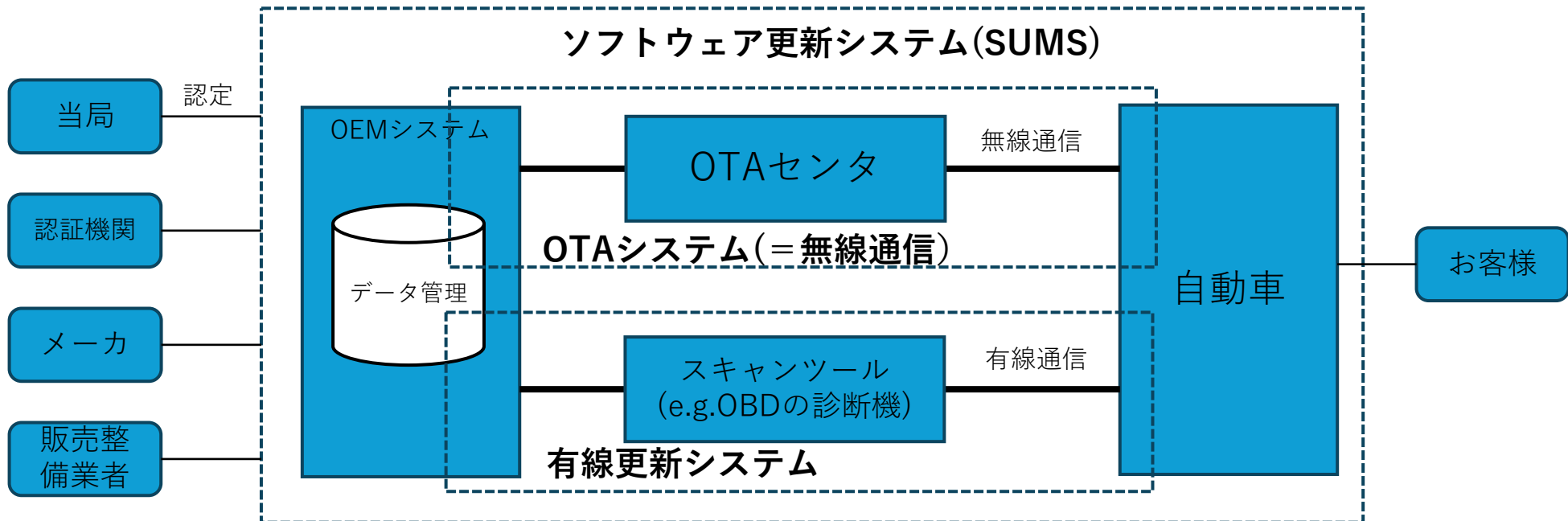
- SUMS (UN-R156の定義より参照)

本規則に基づく、ソフトウェア更新の配信に関する要求事項を遵守するための組織的なプロセスおよび手順を定義する体系的なアプローチを意味する。

"Software Update Management System (SUMS)" means a systematic approach defining organizational processes and procedures to comply with the requirements for delivery of software updates according to this Regulation.

SUMSの例

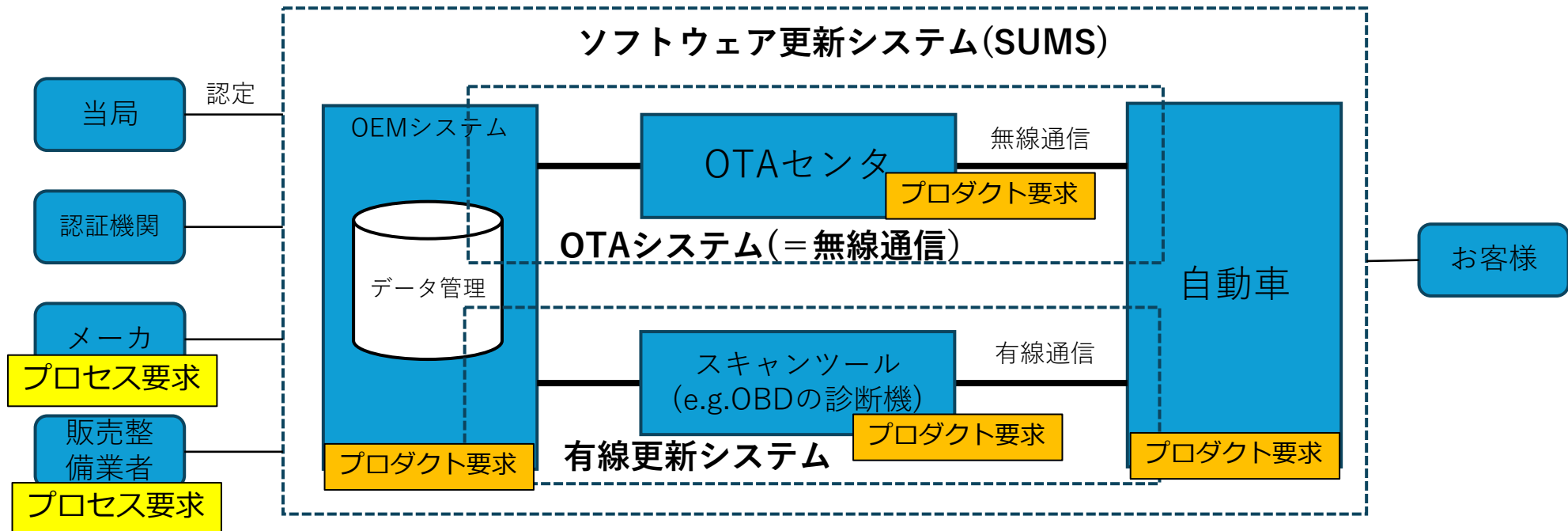
- OEMシステム
 - 設計・開発・製造などの業務で使用するメーカーのシステム、データの管理等を実施
- OTAセンタ
 - OTA技術を活用し、センタから通信区間経由にて遠隔での車載ECUのソフトウェア更新を実施
- スキャンツール
 - 販売整備業者のエンジニアが車載ECUの診断およびソフトウェア更新に使用する診断ツール
- 自動車
 - ソフトウェア更新の対象となる自動車



SUMSの要求

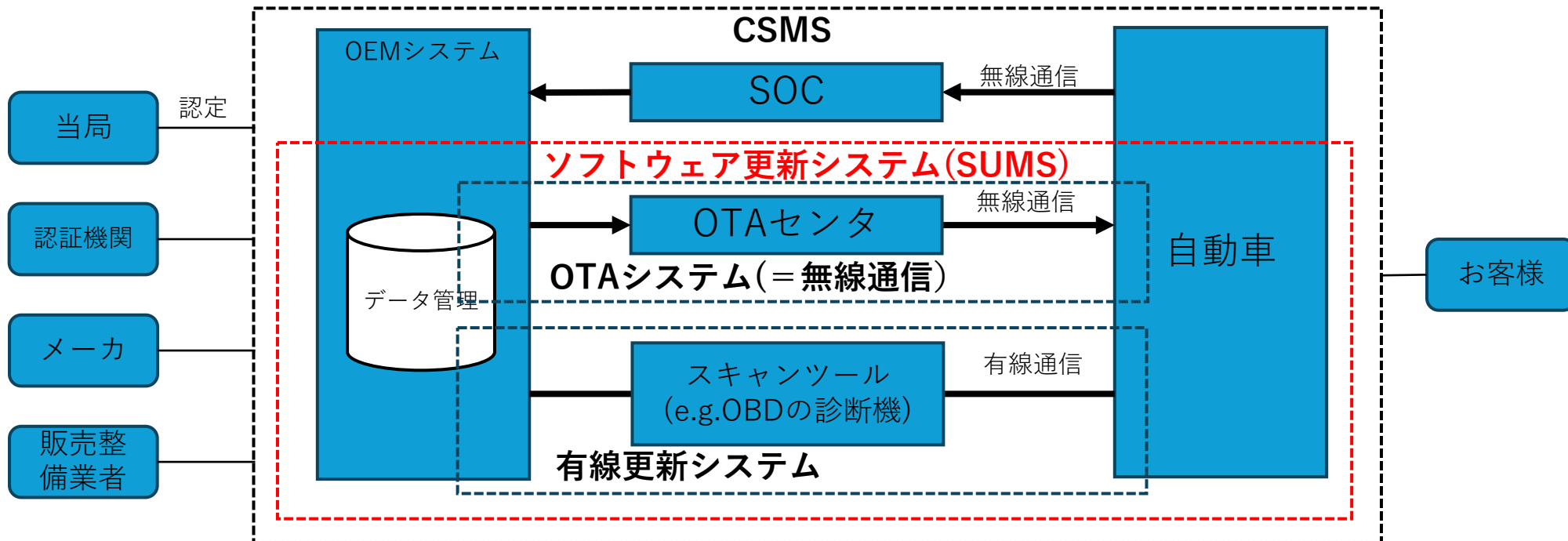
- プロセス要求 … メーカーの開発や運用体制に要求
 - ライフサイクル全体でのソフトウェアの管理
 - 更新プロセスの保護, 管理
 - ソフトウェアの検証プロセスの定義や管理 など
- プロダクト要求 … 主に自動車やその他のシステムに要求
 - セキュアなソフトウェア更新が実行できること
 - RxSWINがOBDから読み出せること など

RxSWIN (Rx Software Identification Number) : UN規則におけるRegulation No.ごとに関連するシステムのソフトウェアバージョンを管理するための識別子



おまけ：CSMSとSUMSの関係

- Cyber Security Management System (CSMS)
 - 自動車の異常を監視し必要な手当てを行うため、SUMSを包含する場合あり
- SOC(VSOCとも呼ばれる)
 - 自動車を遠隔監視しサイバー攻撃の検出や分析，対応策の助言を行う組織
 - SOCとOTAセンタが連携して必要に応じてOTA Updateを実施することが想定



アジェンダ

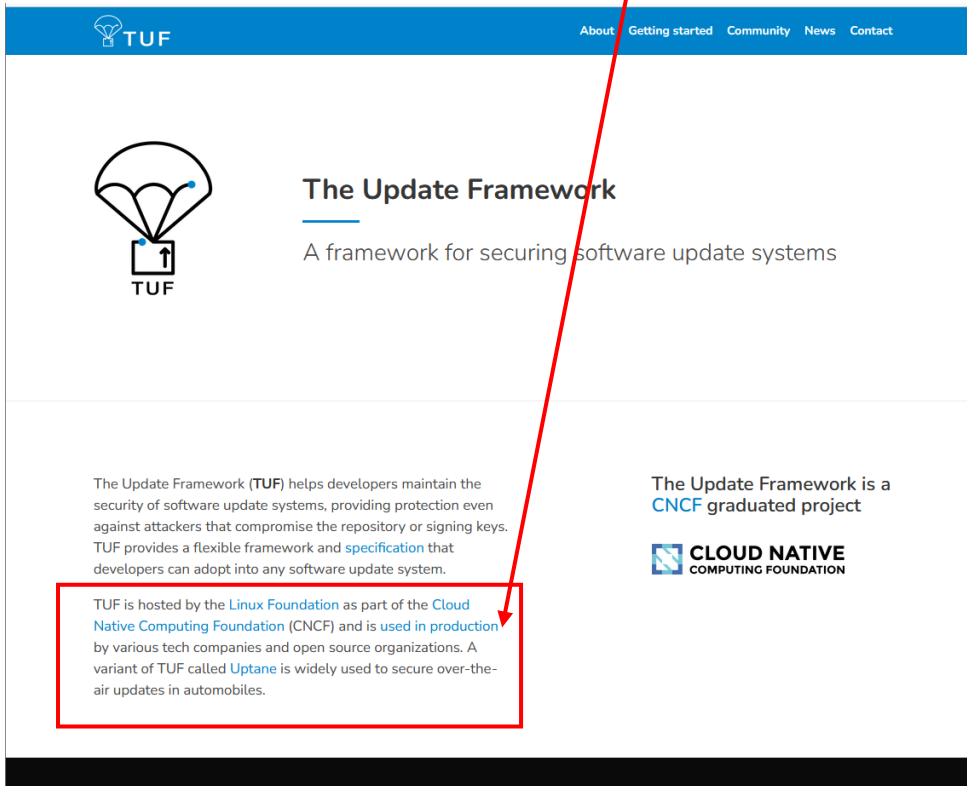
- 1. OTA Update
OTA, OTA Update, 特徴, 歴史
- 2. 自動車のOTA Update
自動車のOTA Update, 制度, ソフトウェア要因のリコール, 必要性
- 3. UN-R156
概要, プロセス, ソフトウェアの構成管理, 対象範囲
- 4. SUMS
概要, 要件
- 5. Uptaneの位置付け
OTA Updateフレームワーク, Uptaneの位置付け

OTA Updateフレームワーク

- 商用ベースとオープンなフレームワークが存在
- 現在は徐々にオープンなフレームワークが主流になりつつある
- 携帯電話
Redbendが有力企業だった（2017年にハーマンが買収）
- スマホ
Android等のソフトウェアプラットフォーム独自のOTAフレームワークを規定
- Linux
SWUpdate, mender.io, The Update Frameworkなど
- 自動車
Uptane

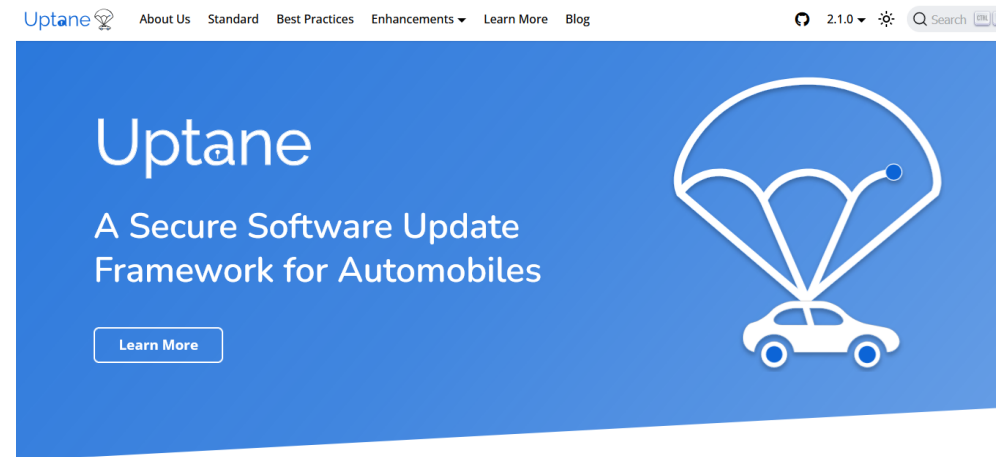
The Update Framework(TUF)

- Linux FoundationがCloud Native Computing Foundation (CNCF)の一部としてホストしており，様々な技術企業やオープンソース組織で実際に運用
- UptaneはTUFの自動車向けのバリエーションとして開発



The screenshot shows the homepage of the Update Framework (TUF). The header includes the TUF logo and navigation links: About, Getting started, Community, News, Contact. The main content area features the TUF logo (a parachute with an upward arrow) and the text "The Update Framework" followed by "A framework for securing software update systems". Below this, there are two columns of text. The left column states: "The Update Framework (TUF) helps developers maintain the security of software update systems, providing protection even against attackers that compromise the repository or signing keys. TUF provides a flexible framework and specification that developers can adopt into any software update system." The right column states: "The Update Framework is a CNCF graduated project" and includes the Cloud Native Computing Foundation logo. A red box highlights a paragraph at the bottom left: "TUF is hosted by the Linux Foundation as part of the Cloud Native Computing Foundation (CNCF) and is used in production by various tech companies and open source organizations. A variant of TUF called Uptane is widely used to secure over-the-air updates in automobiles." A red arrow points from the second bullet point in the list above to this highlighted text.

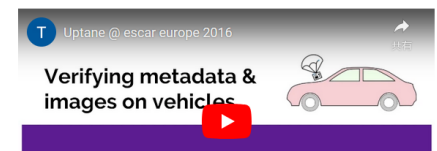
[1] <https://theupdateframework.io/>
(現在は画面が変更されている)



The screenshot shows the homepage of Uptane. The header includes the Uptane logo and navigation links: About Us, Standard, Best Practices, Enhancements, Learn More, Blog. The main content area features the Uptane logo and the text "Uptane" followed by "A Secure Software Update Framework for Automobiles". Below this is a "Learn More" button. To the right is a large illustration of a car with a parachute, symbolizing secure updates. The background is a solid blue color.

Resilient protection against all attackers

Uptane is the first software update security system for the automotive industry capable of resisting even attacks by nation-state level actors. It is designed so that the security of software updates does not degrade all at once, but follows a hierarchy in which different levels of access to vehicles or the automaker's infrastructure must be gained before irreparable damage can be inflicted. By building these levels

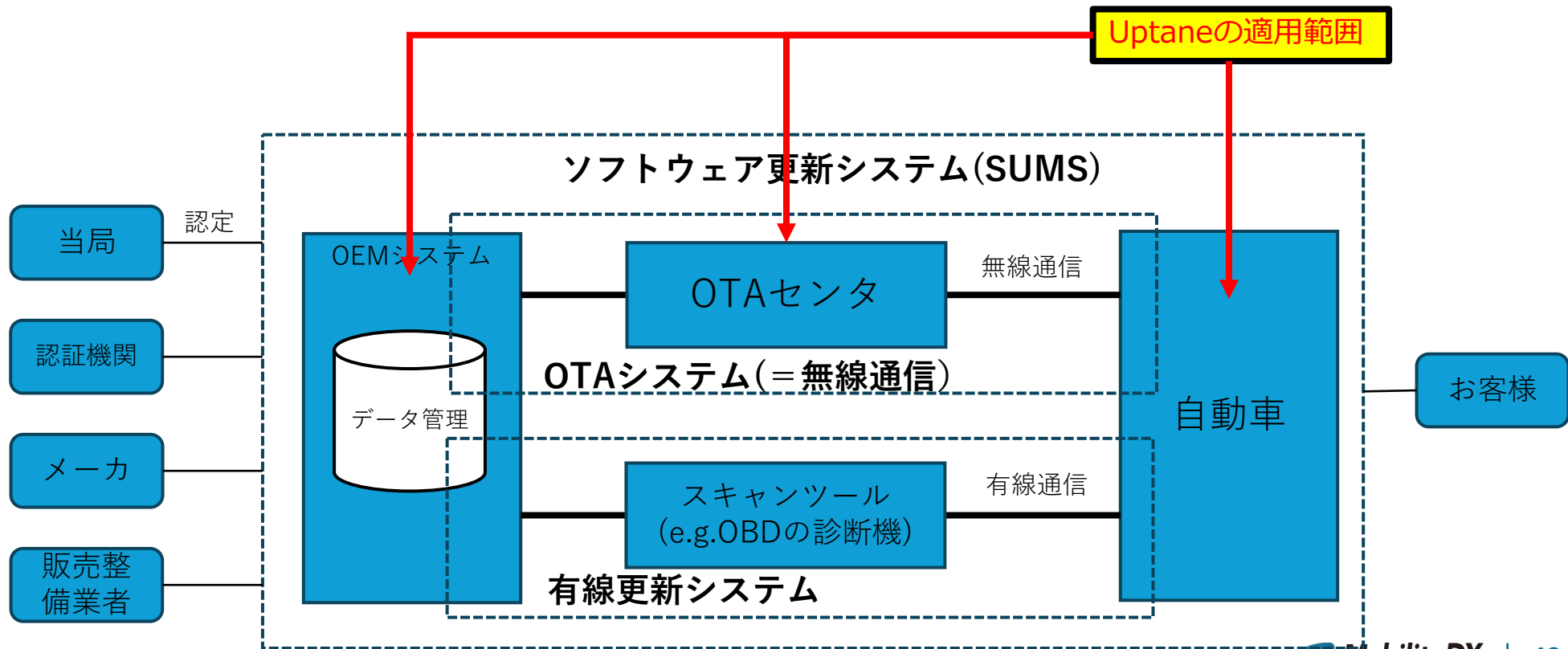


The thumbnail shows a YouTube video titled "Verifying metadata & images on vehicles" by Uptane @ escar europe 2016. It features a red play button icon and a small illustration of a car with a parachute.

[2] <https://uptane.github.io/>

Uptaneの適用範囲

- 自動車のOTA Updateに対する脅威と対策
- ソフトウェア更新パッケージに必要なデータ定義
- 自動車のソフトウェア更新のルールや責務
- 通信プロトコルは規定していないため、OTAだけでなく有線更新システムでも適用可能



まとめ

- 自動車のソフトウェア更新で登場する基本的な用語を説明した
- 自動車のOTA Updateが登場する背景とサイバーセキュリティの重要性を説明した
- 自動車のソフトウェア更新で適用される国際基準と国際標準の概要を説明した
- 自動車のOTA UpdateにおけるUptaneの位置付けについて説明した