SU型式審査マニュアル
2021年1月22日施行版

・UN Regulation No. 156 on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system

審査エビデンスおよび審査方法について

CS/OTA国内採用WG
CS/SU規則検討小WG

更新履歴

- 2021年1月22日　2021年1月22日施行版として新規作成。

CS/SU規則検討小WG参加団体

- 独立行政法人　自動車技術総合機構交通安全環境研究所自動車認証審査部情報セキュリティ審査センター
- 一般社団法人　日本自動車工業会エレクトロニクス部会、技術管理部会性能試験法分科会、届出業務分科会
- 日本自動車輸入組合
- 一般社団法人　日本自動車部品工業会自動運転基準検討部会

本マニュアルについて

本マニュアルは、 2021年1月22日より国内に直接引用されている“協定規則第156号の技術的な要件”およびその関係告示等の審査に関る提出書面および審査の手順および手法について明確化を図るものである。

なお、本マニュアル活用に関しては以下を留意のこと。
・本マニュアルに示した方法は、エビデンスの一例であり、その方法を限定するものではない。他の試験方法や詳細な方法については、国交省および審査部と協議の上、決定することができる。
・適用する試験項目及び試験手順については、審査部と十分協議の上、決定することができる。
・本マニュアルで想定しない事例が生じた場合には国交省および審査部と協議の上、試験方法等決定することができる。

検討方針

１）目的

　解釈文書を参照して、審査時に確認するエビデンスおよび審査方法の明確化を目的とする。
（UNでのテストフェーズにならい、法文解釈の一義化ではなくエビデンスの明確化による審査レベルの安定化も考慮する）

２）検討根拠は以下の基準等とする。

- 協定規則第156号の技術的な要件
- 解釈文書
  WP29 GRVA以下のインフォーマルグループ（Task Force on Cyber Security and software updates (CS/OTA)）にて作成され、WP29で承認された解釈文書

（ECE-TRANS-WP29-GRVA-2020-29e.docx）

7.2.1.
Requirements for Software updates
ソフトウェア更新に関する要件
7.2.1.1.
The authenticity and integrity of software updates shall be protected to reasonably prevent their compromise and reasonably prevent invalid updates.
ソフトウェア更新の真正性および完全性を、その危殆化を合理的に防ぎ、かつ無効な更新を合理的に防ぐ目的で保護するものとする。

解釈 (UN解釈文書における要件の説明)

本要件は、有効なソフトウェア更新だけがダウンロードされ実行されることを保証するための、任意の車両型式で実施されているメカニズムに対処するものである。これは、例えばサインすることによって、更新の真正性および完全性を車両が検証することを要求するものである。7.1.3.1項および7.1.3.2項に記載するプロセスとともに、これによって、作成から提供、実行までのソフトウェア更新のエンドツーエンドシステムがセキュアであることが保証されるはずである。

具体的な書面のイメージ

- 認証され整合性チェックが行われたソフトウェア更新のみが車両で実行されることを保証するために使用されるメカニズムの概要の説明。（認証システム全体が把握できる程度の資料でよい）
- 当該メカニズムについて開発時における試験方法の概要および試験結果の概要。
- サイバーセキュリティ（UNR-155）側で説明し、それを引用してもよい。

鍵認証され整合性チェックを行うロジックを意味する

判断の目安（WP29解釈文書より引用）

Software Update

7.2.1.1.

Explanation of the requirement	
This requirement addresses the mechanisms implemented on a given vehicle type to ensure that only valid software updates are downloaded and executed. This requires that updates authenticity and integrity are validated by the vehicle, for example by signing. Together with the processes described in paragraphs 7.1.3.1. and 7.1.3.2. this should ensure that the end to end system for software updates, from creation through delivery to execution, is secure.	本要件は、有効なソフトウェア更新だけがダウンロードされ実行されることを保証するための、任意の車両型式で実施されているメカニズムに対処するものである。これは、例えばサインすることによって、更新の真正性および完全性を車両が検証することを要求するものである。7.1.3.1項および7.1.3.2項に記載するプロセスとともに、これによって、作成から提供、実行までのソフトウェア更新のエンドツーエンドシステムがセキュアであることが保証されるはずである。
The following clarification should be noted	
‘Reasonably’ refers to the level of protection being foreseeable and based on state of the art preventions	「合理的に」とは、保護が予見可能で、かつ最先端の防止策に基づいているレベルを指す
Examples of documents/evidence that could be provided	
Vehicle manufacturers should provide details of the mechanisms used to ensure that only authenticated and integrity checked software updates are executed on a vehicle. The results of authentication testing may be used as evidence. The cyber security regulation may be used as a reference.	車両メーカーは、認証され完全性が確認されたソフトウェア更新だけが、車両で実行されることを保証するために使用されるメカニズムの詳細を提供すべきものとする。認証テストの結果を証拠として使用してもよい。 サイバーセキュリティ規則を参照として使用してもよい。

7.2.1.2.
Where a vehicle type uses RXSWIN:
車両型式がRXSWINを使用している場合:
7.2.1.2.1.
Each RXSWIN shall be uniquely identifiable. When type approval relevant software is modified by the vehicle manufacturer, the RXSWIN shall be updated if it leads to a type approval extension or to a new type approval.
各RXSWINは、一意的に識別できるものとする。車両メーカーが型式認可に関連するソフトウェアを変更した場合、それが型式認可の拡大または新規型式認可につながる場合には、RXSWINを更新するものとする。

RxWIN関係は継続議論とする。

解釈（UN解釈文書における要件の説明）

なし

2021/3月末までに記載内容を確定し改定する。

具体的な書面のイメージ

・RxSWINの仕様（桁数や各桁の意味合いなど）
・RxSWINが“一意”であることの確認結果。（プロセスと絡めての説明でも良い、重複を防ぐプロセスを用いて確認した結果等の説明）
・認可に影響があった場合に、どのように番号が変更されるかの説明。（プロセスと絡めての説明でも良い、どのプロセスを用いて番号を変更するのか等の説明）
・該当の車両型式のソフトウェアとRxSWINの関係一覧表
→申請時点のもので良く当該型式に搭載した装置のExt.等でRxSWINが更新された場合でもSUDの再申請は不要と考えるため、ワイルドカードのような記載でも可？（要検討）

※ソフトウェアとRxSWINの関係一覧表について、 RxSWINに紐づくソフトウエアを開示する粒度等も検討が必要。
・RxSWINの管理はOEM毎の解釈でよく、読み出し方を整合させればOKか？
・今後Egdeｺﾝﾋﾟｭｰﾃｨﾝｸﾞ化なども進むと予想され、車載機での厳重な管理ではなくバックエンド側での管理も視野に入れるべきか？
などを継続議論とする。

判断の目安（WP29解釈文書より引用）

Software Update

7.2.1.2.1.

RxWIN関係は継続議論とする。

Examples of documents/evidence that could be provided	
Vehicle manufacturers may provide: Demonstration of how an RXSWIN is generated for a given vehicle type and made unique Demonstration that each RXSWIN has a one on one relation with its appropriate Regulation and how the regulation can be identified	車両メーカーは、以下を提供してもよい： 任意の車両型式についてRXSWINがどのように生成され、一意的になっているかの証明 各RXSWINが該当する規則と1対1の関係を有しており、当該規則をどのようにして特定することができるかの証明

2021/3月末までに記載内容を確定し改定する。

7.2.1.2.2.
Each RXSWIN shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port).
If RXSWINs are not held on the vehicle, the manufacturer shall declare the software version(s) of the vehicle or single ECUs with the connection to the relevant type approvals to the Approval Authority. This declaration shall be updated each time the declared software version(s) is updated. In this case, the software version(s) shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port).
各RXSWINは電子通信インターフェースの使用を介して、少なくとも標準インターフェース（OBDポート）によって、標準化された方法で容易に読むことができるものとする。
RXSWINが車両に保持されていない場合、メーカーは、車両または単体ECUのソフトウェアバージョンを、関連する型式認可とのつながりと共に認可当局に申告するものとする。本申告は、申告したソフトウェアバージョンが更新される度に更新するものとする。この場合、ソフトウェアバージョンは、電子通信インターフェースの使用を介して、少なくとも標準インターフェース（OBDポート）によって、標準化された方法で容易に読むことができるものとする。

RxWIN関係は継続議論とする。
2021/3月末までに記載内容を確定し改定する。

解釈 (UN解釈文書における要件の説明)

本要件は、RXSWINを車両から読むことができるように、RXSWINが車両に保管されていること、あるいは車両に保管されていない場合には、RXSWINに関連するソフトウェアバージョンが車両に保管され、RXSWINへのリンクが申告されていることを要求するものである。

具体的な書面のイメージ

OBD以外を使用の場合は事前に審査部と協議のこと。

以下の内容を網羅した書面の提出および実車での試験による。

- 読み出せるI/Fおよびツールの仕様。（ツールおよび通信の概要、I/F規格としてOBDポートとする。
- 読み出し手順。（既存のマニュアルでも良い）
- 読み出した結果のサンプル（全てのコントローラに対する社内試験結果）
- 実車によるデモ（立会い認証試験）
- 読み出せるRxSWINもしくはソフトバージョンの仕様。（ Rxswinの場合7.2.1.2.1の説明で代えても良い）
- バージョンを使用する場合は当該車料におけるソフトウエアバージョンのリスト。
- 読み出せるバージョンはECU単位（ECU全体のソフトを包含したバージョン）でよい。

※RxSWINが車外に保管される形態も想定される。車外保管の例は、次頁参照

RxWIN関係は継続議論とする。

2021/3月末までに記載内容を確定し改定する。

今後、車両のHMI等の他の手段を定義する場合は情報共有していく

審査マニュアルへ参考として記載

Software Update

1．RxSWINの持ち方

UNR156の目的：ソフトウェアアップデート行為における法規適合性の保証(体制認可)及び、確認手法(車両認可)を定めるものであると考えている。

RxWIN関係は継続議論とする。

例１：RxSWINを車両からの情報を元にｻｰﾊﾞ経由で読み出せる方式

例2：RxSWINを車両を介して出力する方式
サーバーから出力されたRxSWINは
車両をパススルーしてOBDから出力

2021/3月末までに記載内容を確定し改定する。

判断の目安（WP29解釈文書より引用）

Software Update

7.2.1.2.2.

Explanation of the requirement	
This requirement requires that the RXSWINs shall be stored on a vehicle, in order for them to be read from it or that if it is not stored on the vehicle that the versions of software relevant to an RXSWIN should be stored on a vehicle and the link to a RXSWIN be declared.	本要件は、RXSWINを車両から読むことができるように、RXSWINが車両に保管されていること、あるいは車両に保管されていない場合には、RXSWINに関連するソフトウェアバージョンが車両に保管され、RXSWINへのリンクが申告されていることを要求するものである。
Examples of documents/evidence that could be provided	
The following standards and regulations may be relevant: (a) ISO14229/1; (b) (OBD port): ISO 14229; (c) UN Regulation No. 83.	以下の基準および規則が関連する場合がある： (a) ISO 14229/1、 (b) （OBDポート）：ISO 14229、 (c) UN規則No. 83。

7.2.1.2.3.
The vehicle manufacturer shall protect the RXSWINs and/or software version(s) on a vehicle against unauthorised modification. At the time of Type Approval, the means implemented to protect against unauthorized modification of the RXSWIN and/or software version(s) chosen by the vehicle manufacturer shall be confidentially provided.
車両メーカーは、不正な変更から車両に搭載したRXSWINおよび／またはソフトウェアバージョンを保護するものとする。型式認可時に、車両メーカーが選択した不正な変更からRXSWINおよび／またはソフトウェアバージョンを保護するために実施する手段を機密として提供するものとする。

解釈 (UN解釈文書における要件の説明)

本要件は、RXSWINのセキュリティに対処するものである。その意図は、公認された当事者だけがRXSWINを変更することができ、関連するソフトウェア更新が車両で実行された場合に限りこれが発生する、ということである。

具体的な書面のイメージ

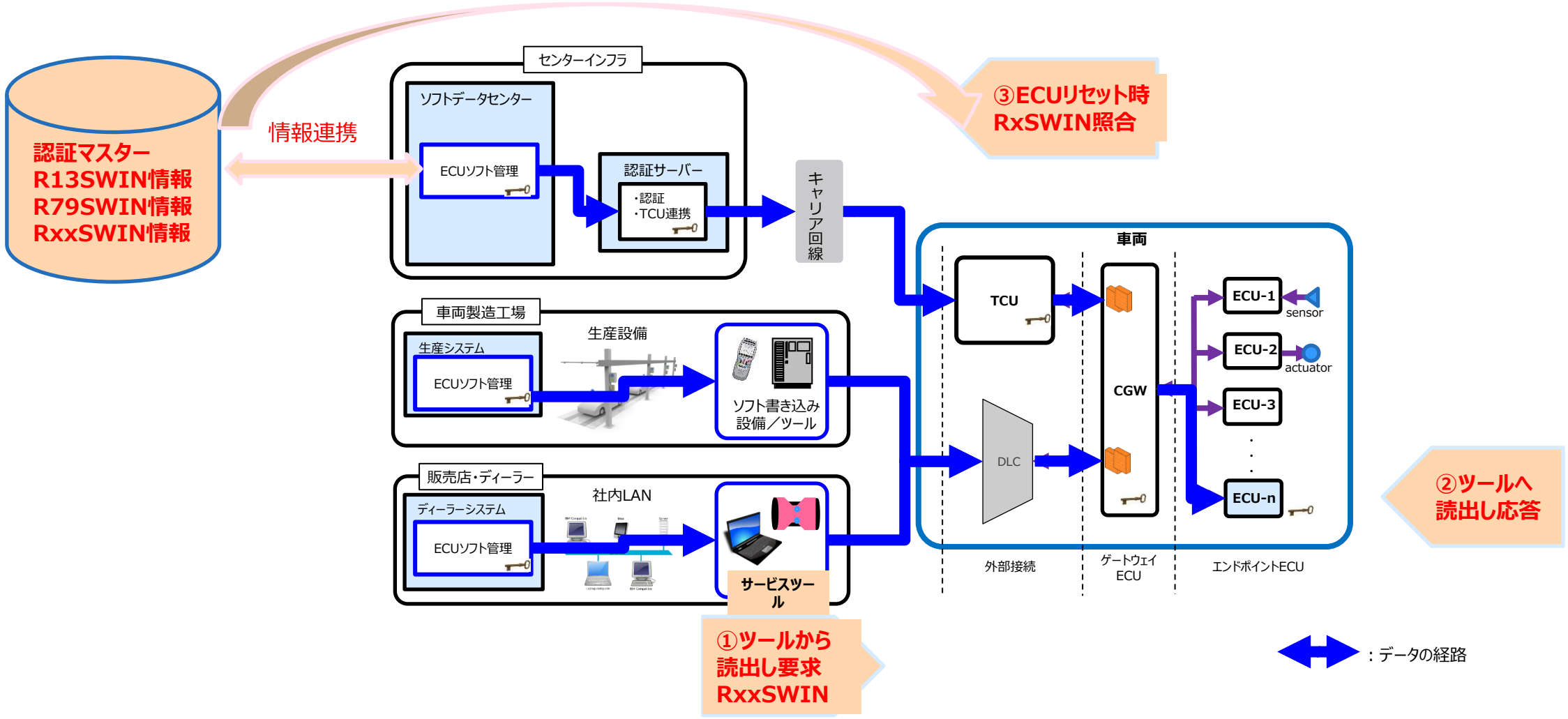
・CSの範囲として改変保護が含まれているはずなので、CSMS適合証明書およびCS側型式指定審査結果における確認を基本とする。
（当該型式において改変保護が適用されているかを確認する）
・Rxswinおよびソフトウエアバージョンの格納場所の概要説明。
・当該型式において実装された対策についての概要説明。[但し、本説明については資料提示のみで提出は要しない]

コメント
書面の提出要否については機密性に鑑み個社で相談とする

（補足）先回の検討小WGにて提出した全体構成図

ソフトアップデート　システム構成図
（In-Car, Out-Car）

2020/1/9



（センター、生産、サービスの対象範囲　⇒　車両の電子制御システムに直接つながる範囲）

判断の目安（WP29解釈文書より引用）

Software Update

7.2.1.2.3.

Explanation of the requirement	
This requirement addresses the security of the RXSWIN. Its intention is that only authorised parties may change the RXSWIN and that this only happens when a relevant software update is executed on the vehicle.	本要件は、RXSWINのセキュリティに対処するものである。その意図は、公認された当事者だけがRXSWINを変更することができ、関連するソフトウェア更新が車両で実行された場合に限りこれが発生する、ということである。
Examples of documents/evidence that could be provided	
The manufacturer may describe where/how the RXSWINs are stored and what measures have been implemented to protect them against unauthorized modification.	メーカーは、どこに／どのようにRXSWINが保管され、不正な変更から保護するためにどのような措置が実施されているかを記載してもよい。

7.2.2.
Additional Requirements for over the air updates
Over the Air更新に関する追加要件
7.2.2.1.
The vehicle shall have the following functionality with regards to software updates:
車両は、ソフトウェア更新に関連して以下の機能性を有するものとする:
7.2.2.1.1.
The vehicle manufacturer shall ensure that the vehicle is able to restore systems to their previous version in case of a failed or interrupted update or that the vehicle can be placed into a safe state after a failed or interrupted update.
車両メーカーは、更新が失敗または中断した場合に、車両がシステムをその前のバージョンまで復元することができる、あるいは更新の失敗または中断後、車両を安全な状態に置くことができることを保証するものとする。

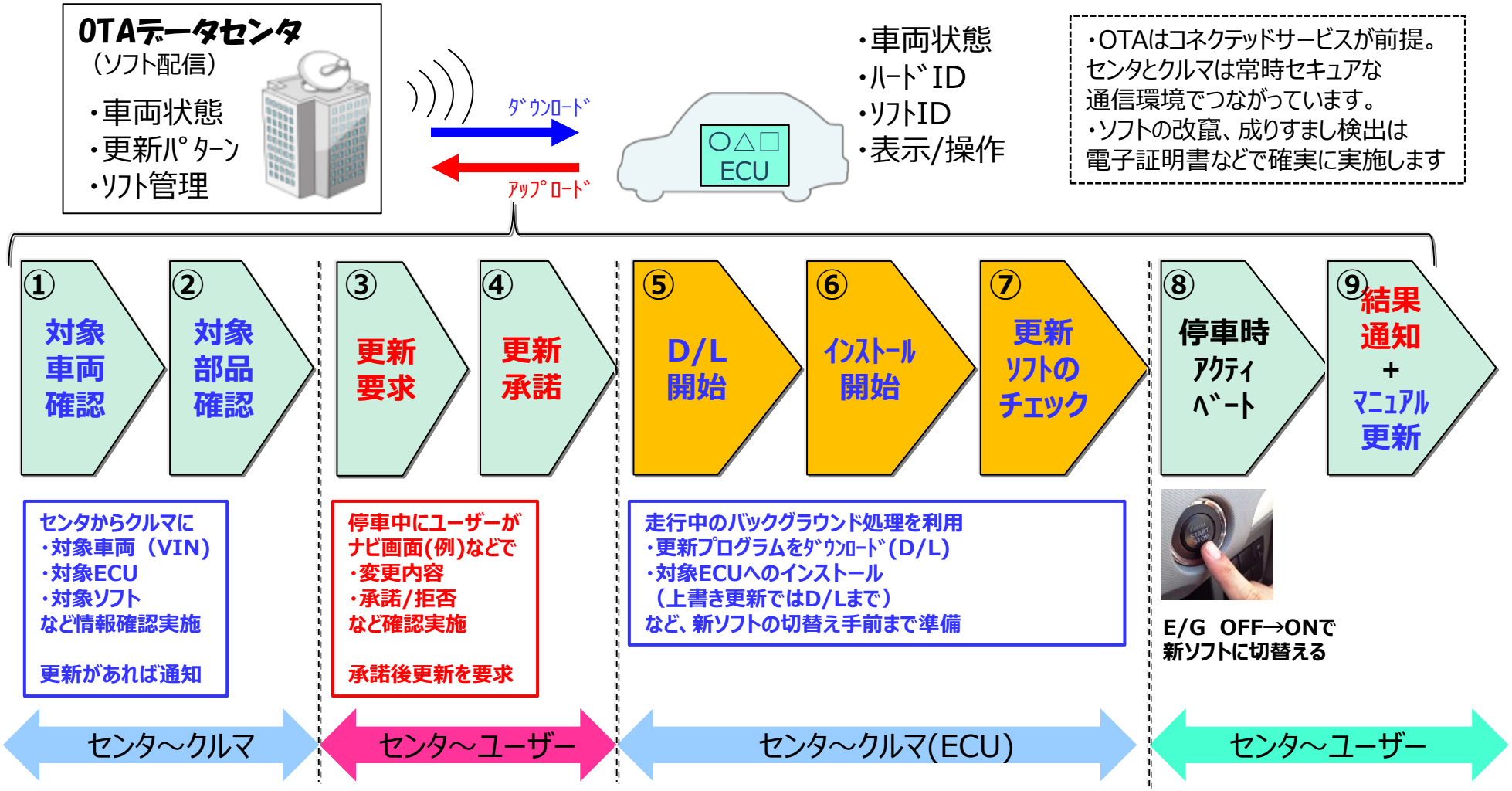
解釈（UN解釈文書における要件の説明）

本要件の意図は、車両型式が失敗した更新を管理することができることを保証することである。
以前のバージョンに戻ることが不可能である、または好ましくない場合は、安全な状態を実施すべきものとする。これは、車両の能力または機能性の低減を含む場合がある。メーカーは、安全な状態とはどういうものである可能性があるかを決めるべきものとする。

具体的な書面のイメージ

・OTA手順の概要説明
　車両側でOTAを実施する場合の手順説明であり、バックエンド等まで含む必要は無い。
・更新失敗または中断が想定されるケーススタディ
　電源断、キャリア圏外、ECU故障など設計的に想定しているケースを説明する。
・フェールリカバリ仕様の概要説明
　更新が失敗または中断した場合に、7.2.2.1.1（改変前or安全状態）の状態とするためのロジックの説明。
　ECU故障で更新が失敗または中断した場合には、安全状態とするロジックを説明すれば良い。
・実車でのデモ（原則上記で説明された中断が想定される全てのケースについて）
　ただし、実際の認証試験でどの項目を立会い試験の対象とするかは申請時の試験選定で決定する。

E⑱. 実車デモ 7.2.2.1.1更新の中断、失敗



【デモの手順】

- **⑤から⑦のプロセスで、車両の電源をOFFにする**
- **一定時間経過後、再電源ONで再開(Resume）処理が始まるかを確認**

判断の目安（WP29解釈文書より引用）

Software Update

7.2.2.1.1.

Explanation of the requirement	
The intention of this requirement is to ensure that vehicle types can manage failed updates. A safe state should be implemented when it is not possible or desirable to roll-back to a previous version. This may include reducing the capability or functionality of the vehicle. The manufacturer should determine what a safe state may be.	本要件の意図は、車両型式が失敗した更新を管理することができることを保証することである。 以前のバージョンに戻ることが不可能である、または好ましくない場合は、安全な状態を実施すべきものとする。これは、車両の能力または機能性の低減を含む場合がある。メーカーは、安全な状態とはどういうものである可能性があるかを決めるべきものとする。
The following clarification should be noted	
‘Safe state’ may be interpreted as “an operating mode in case of a failure of an item without an unreasonable level of risk” (using the definition provided in ISO 26262)	「安全な状態」は、「アイテムが失敗した場合に、不合理なリスクレベルを伴わない作動モード」（ISO 26262の定義を使用）と解釈してもよい
Examples of documents/evidence that could be provided	
The following standards and regulations may be relevant: (a) ISO 26262 may be used with regards functional safety The following may be relevant or evidenced to provide assurance that this requirement is met: (a) Requirements of the safe state; (b) Functionalities added/ disabled to achieve the safe state.	以下の基準および規則が関連する場合がある： (a) 機能的安全性に関してISO 26262を使用してもよい 以下は、本要件が満たされているという保証の提供に関連する、あるいはその証拠となる場合がある： (a) 安全な状態の要件、 (b) 安全な状態を達成するために追加した／無効にした機能性。

7.2.2.1.2.
The vehicle manufacturer shall ensure that software updates can only be executed when the vehicle has enough power to complete the update process (including that needed for a possible recovery to the previous version or for the vehicle to be placed into a safe state).
車両メーカーは、車両が更新プロセスを完了するだけ十分なパワー（前のバージョンへの想定される復元のため、または車両を安全な状態に置くために必要なパワーを含む）がある場合に限りソフトウェア更新を実行することができることを保証するものとする。

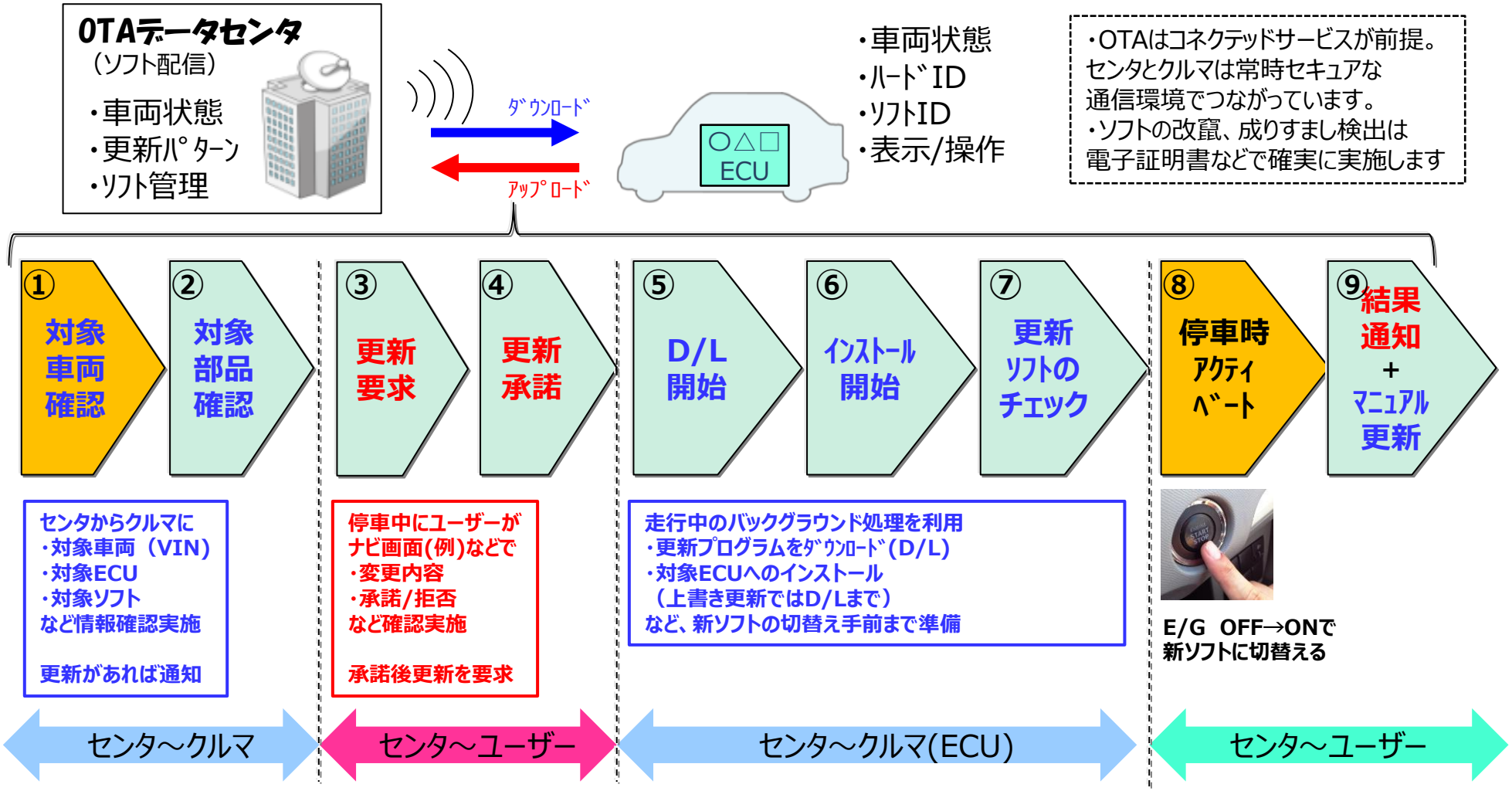
解釈 （UN解釈文書における要件の説明）

なし

具体的な書面のイメージ

・プロセスを完了するのに十分な電力があるかどうかの判断方法（ロジック）を記載した書面。
（十分な電源確保については各社が型式認証の時に説明する。リスクがあれば、リスクに対する対策を各社で説明。）
・上記または、複数ケースによるデモ。（電力が十分な場合、不十分な場合、など）

E⑱. 実車デモ 7.2.2.1.2 電源管理



【デモの手順】

- **①のプロセスで、車両の電源状態をモニタ、判定しているプロセスをデモする**
- **⑧のプロセスで保証電圧以下でアクティベートさせないガードロジックをデモする**

判断の目安（WP29解釈文書より引用）

Software Update

7.2.2.1.2.

Examples of documents/evidence that could be provided	
Examples of documents/evidence that could be provided The following may be used to provide assurance that this requirement is met: (a) Description of measures taken by the vehicle manufacturer; (b) Demonstration of requirements via documentation/presentation and/or physical test.	本要件が満たされているという保証を提供するために以下を使用してもよい： (a) 車両メーカーが講じる措置の説明、 (b) 文書／プレゼンテーションおよび／または物理テストを介した要件の証明。

7.2.2.1.3.
When the execution of an update may affect the safety of the vehicle, the vehicle manufacturer shall demonstrate how the update will be executed safely. This shall be achieved through technical means that ensures the vehicle is in a state where the update can be executed safely.
更新の実行が車両の安全性に影響を与える場合、車両メーカーは、どのように更新が安全に実行されるかを証明するものとする。これは、車両が安全に更新が実行できる状態であることを保証する技術的な手段を通して達成するものとする。

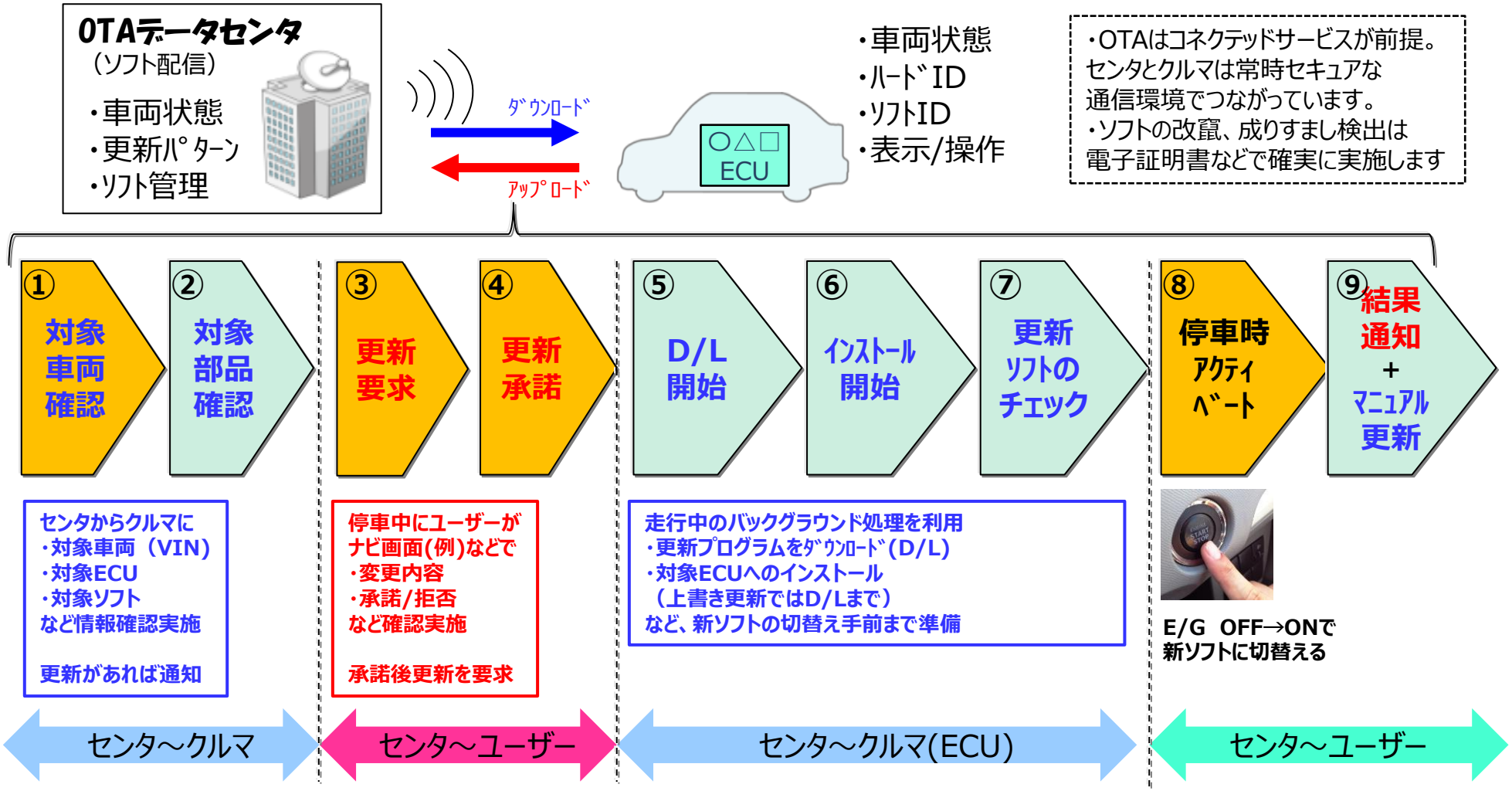
解釈 （UN解釈文書における要件の説明）

なし

具体的な書面のイメージ

1.改変の実行が車両の安全に影響を与える可能性があるかの検討書。
（可能性のある全てのOTAアップデートについて）
2.上記で安全に影響が有ると判断した場合、更新を安全に実施するためのプロセス（更新中に車両の安全状態を確保するためのロジック）
3.　2.で確認したプロセスに対する実車を使用したデモンストレーション。（立会い試験）

E⑱. 実車デモ 7.2.2.1.3 更新の安全性



【デモの手順】

- **③④更新内容が車両の安全性に影響を与える場合の留意事項をユーザーへ通知、承諾を得ているか、確認**
- **例えば⑧アクティベート時は、車両（制御や機能）がプログラム切替に影響のない状態下であるか、のデモ**

判断の目安（WP29解釈文書より引用）

Software Update

7.2.2.1.3.

No guidance included in this document with regards this requirement	
-	-

7.2.2.2.
The vehicle manufacturer shall demonstrate that the vehicle user is able to be informed about an update before the update is executed. The information made available shall contain:
(a) The purpose of the update. This could include the criticality of the update and if the update is for recall, safety and/or security purposes;
(b) Any changes implemented by the update on vehicle functions;
(c) The expected time to complete execution of the update;
(d) Any vehicle functionalities which may not be available during the execution of the update;
(e) Any instructions that may help the vehicle user safely execute the update;
In case of groups of updates with a similar content one information may cover a group.
車両メーカーは、車両ユーザーが更新実行前に更新について通知を受けることができることを証明するものとする。利用可能な状態にする情報は、以下を含むものとする：
(a) 更新の目的。これは、更新の重要性、ならびに更新がリコールに関する場合は、安全性および／またはセキュリティの目的を含むことができる、
(b) 車両の機能に関して更新で実施される変更、
(c) 更新実行を完了するために想定される時間、
(d) 更新実行中に利用できなくなる可能性のある車両の機能性、
(e) 車両ユーザーが更新を安全に実行するのを支援する可能性のある指示、
類似の内容を有する複数の更新のグループである場合は、1つの情報でグループ全体を網羅してもよい。

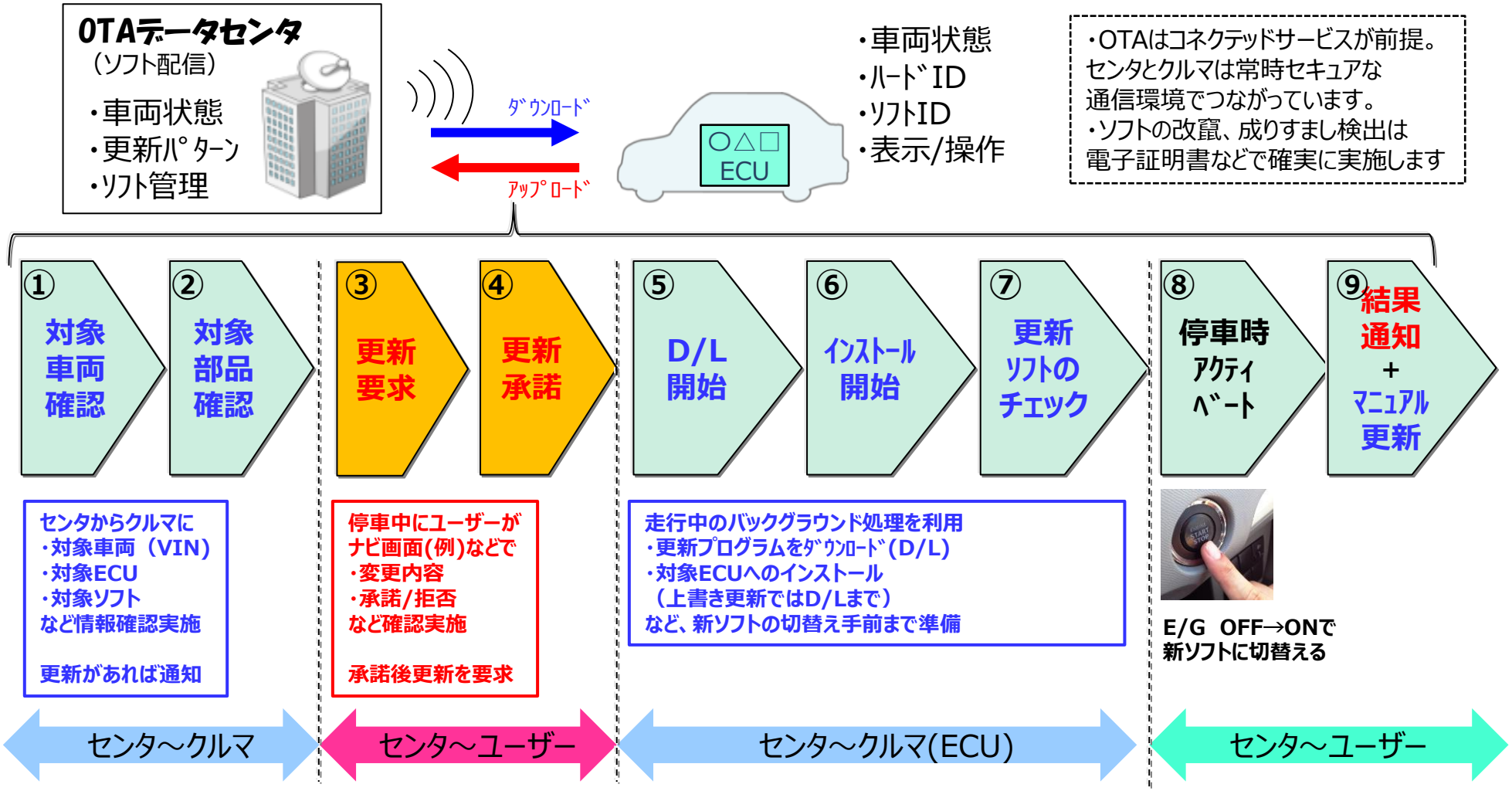
解釈（UN解釈文書における要件の説明）

本要件は、7.1.1.11項で要求されるプロセスと関連しているが、本要件は、Over the Air更新が提供される車両型式に関連している。その意図は、車両ユーザーが更新実行前に更新について通知を受け、更新を実行するかどうかを判断するために必要な情報を提供されることである（車両ユーザーはその法的権利を有し、かつ通知を受けることを希望しているという前提）。
車両ユーザーが、ソフトウェア更新について1回だけ認証を受ける選択肢が提供され、それを選択した場合に、当該ユーザーは更新の度に通知を受け取る必要はない。ただし、新規ユーザーへの車両の譲渡、または車両ユーザーの希望変更が可能であることを保証するために、これをどう管理するかを証明する必要がある場合がある。

具体的な書面のイメージ

・ユーザへの通知方法の概説。
　どの通知手法を使って、更新のどのタイミングでどのような情報が提供されるかについて説明。
　通知方法は車載HMIに限定しない。ただし、当該通知方法が確実に通知を出来るものとして型式申請時に引用するSUMSにて説明済であること。この際、当該デバイスは保安基準適合審査の対象外とする。ただし、型式審査にて通知を実証する際には当該デバイスを使用して実施のこと。
　なお、使用者の許諾（承認）が前提。結果として、許諾を得たことを記録として残すプロセスが必要。型式ごと（各社ごとや各車両ごと）に許諾を得る方法が異なるため型式要件とする。
・ユーザへの通知のサンプル
　実際に通知されるディスプレイ情報など。
・実車を使用したデモンストレーション。（立会い試験）

E⑱. 実車デモ 7.2.2.2 更新の通知



【デモの手順】

・③④ユーザーへの更新内容の通知表示をデモし、下記の要件が表示されることを確認
（更新目的、車両機能の変更点、予想される更新時間、更新時に制限される機能の有無、ユーザーに役立つ指示、等）

判断の目安（WP29解釈文書より引用）

Software Update

7.2.2.2.

Explanation of the requirement	
This requirement is linked to the processes required under paragraph 7.1.1.11 but this requirement is linked to the vehicle type where over the air updates are provided. The intention is that the vehicle user may be informed about updates before they are executed and be provided with any information they need to decide whether or not to execute the update (assuming they have the legal right to do so and wish to be informed). If a vehicle user is provided the option for a onetime authorisation for software updates, and opts for it, he need not be informed about every update. How this is managed may still need to be demonstrated to ensure it enables the transfer of a vehicle to a new user or a vehicle user to change their preference.	本要件は、7.1.1.11項で要求されるプロセスと関連しているが、本要件は、Over the Air更新が提供される車両型式に関連している。その意図は、車両ユーザーが更新実行前に更新について通知を受け、更新を実行するかどうかを判断するために必要な情報を提供されることである（車両ユーザーはその法的権利を有し、かつ通知を受けることを希望しているという前提）。 車両ユーザーが、ソフトウェア更新について1回だけ認証を受ける選択肢が提供され、それを選択した場合に、当該ユーザーは更新の度に通知を受け取る必要はない。ただし、新規ユーザーへの車両の譲渡、または車両ユーザーの希望変更が可能であることを保証するために、これをどう管理するかを証明する必要がある場合がある。
Examples of documents/evidence that could be provided	
The vehicle manufacturer could have release notes for each of the updates detailing the information from the requirement in paragraph 7.2.2.2. The vehicle manufacturer could demonstrate how this information may be made available to the user. This may include: (a) Description of how the vehicle user is able to be informed; (b) Demonstration via documentation/presentation and/or physical test.	車両メーカーは、各更新について、7.2.2.2項の要件による情報を詳述したリリースノートを有することができる。車両メーカーは、この情報をユーザーに対してどのように利用可能な状態にすることができるかを証明することができる。これは、以下を含んでいてもよい： (a) 車両ユーザーがどのように通知を受けることができるかの説明、 (b) 文書／プレゼンテーションおよび／または物理テストを介した証明。

7.2.2.3.
In the situation where the execution of an update whilst driving may not be safe, the vehicle manufacturer shall demonstrate how they will:
(a) Ensure the vehicle cannot be driven during the execution of the update;
(b) Ensure that the driver is not able to use any functionality of the vehicle that would affect the safety of the vehicle or the successful execution of the update.
運転中に更新を実行することが安全ではない可能性がある場合は、車両メーカーは、以下をどのように実行するかを証明するものとする：
(a) 更新実行中は車両を運転することができないことを保証する、
(b) 運転者が、車両の安全性または問題のない更新の実行に影響を与える車両の機能性を使用することができないことを保証する。

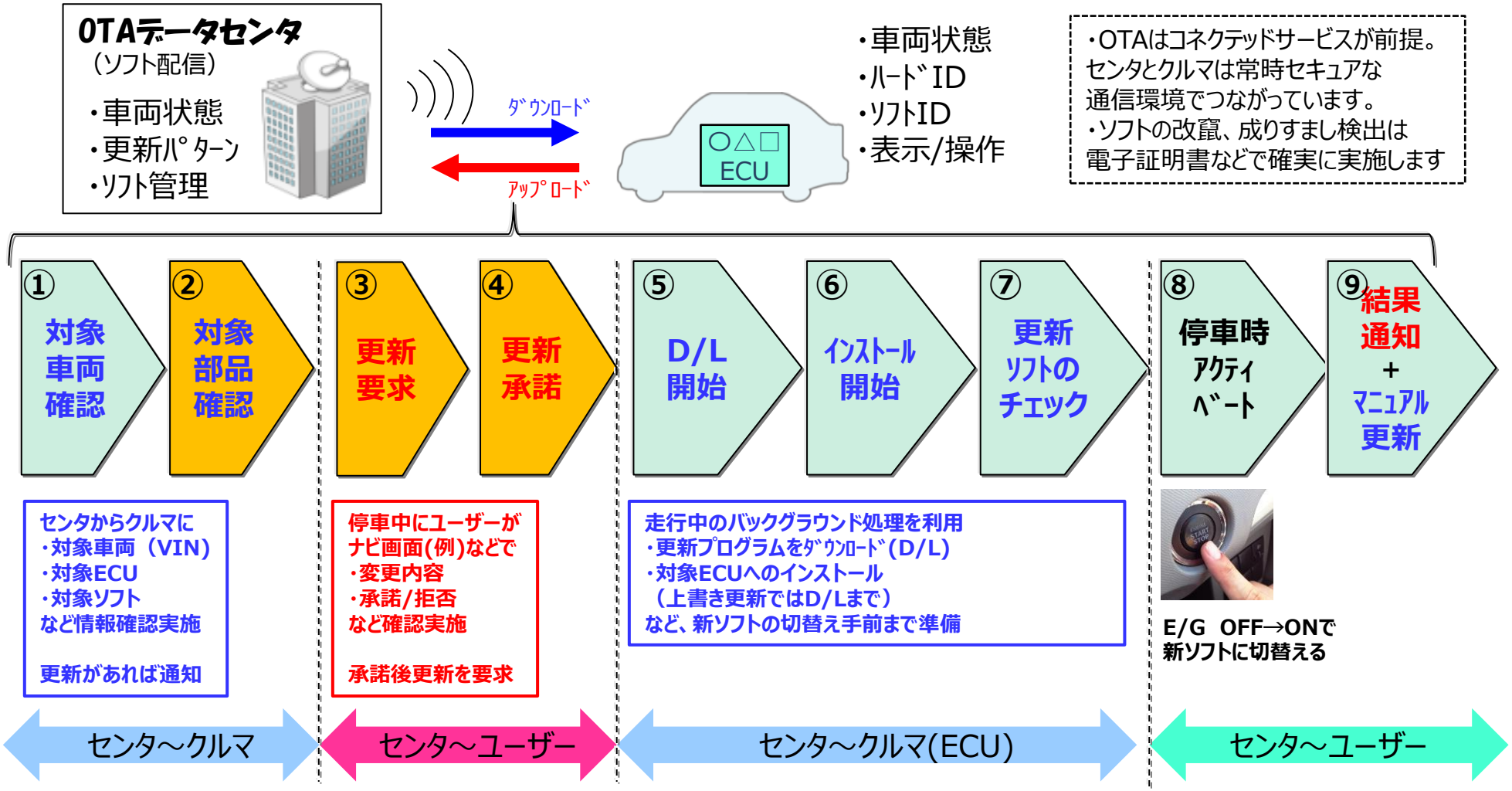
解釈 (UN解釈文書における要件の説明)

なし

具体的な書面のイメージ

1.改変の実行が車両の安全に影響を与える可能性があるかの検討書。（可能性のある全てのOTAアップデートについて）
2.上記で安全に影響が有ると判断した場合、車両を運転不可能にする手法および更新に影響を及ぼす機能を停止する手法の説明。
3.実車を使用したデモンストレーション。（立会い試験）

E⑱. 実車デモ 7.2.2.3 更新中の制約



【デモの手順】

・②③④更新対象機能と影響範囲(7.1.1.5）から、制約を受ける機能の有無の通知と承諾、対処方法、及び影響する車両状態（駐車中、走行中、アクティベート時、等）が、ユーザーへ適切に通知され、承諾を得ていることを確認。

判断の目安（WP29解釈文書より引用）

Software Update

7.2.2.3.

Examples of documents/evidence that could be provided	
The following may be used to provide assurance that this requirement is met: (a) Demonstration of requirements via documentation/presentation and/or physical test.	本要件が満たされているという保証を提供するために以下を使用してもよい： (a) 文書／プレゼンテーションおよび／または物理テストを介した要件の証明。

7.2.2.4.
After the execution of an update the vehicle manufacturer shall demonstrate how the following will be implemented:
(a) The vehicle user is able to be informed of the success (or failure) of the update;
(b) The vehicle user is able to be informed about the changes implemented and any related updates to the user manual (if applicable).
更新実行後、車両メーカーは以下をどのように実施するかを証明するものとする：
(a) 車両ユーザーが、更新の成功（または失敗）について通知を受けることができる、
(b) 車両ユーザーが、実施される変更およびユーザーマニュアルに対する関連する更新（該当する場合）について通知を受けることができる。

解釈（UN解釈文書における要件の説明）

なし

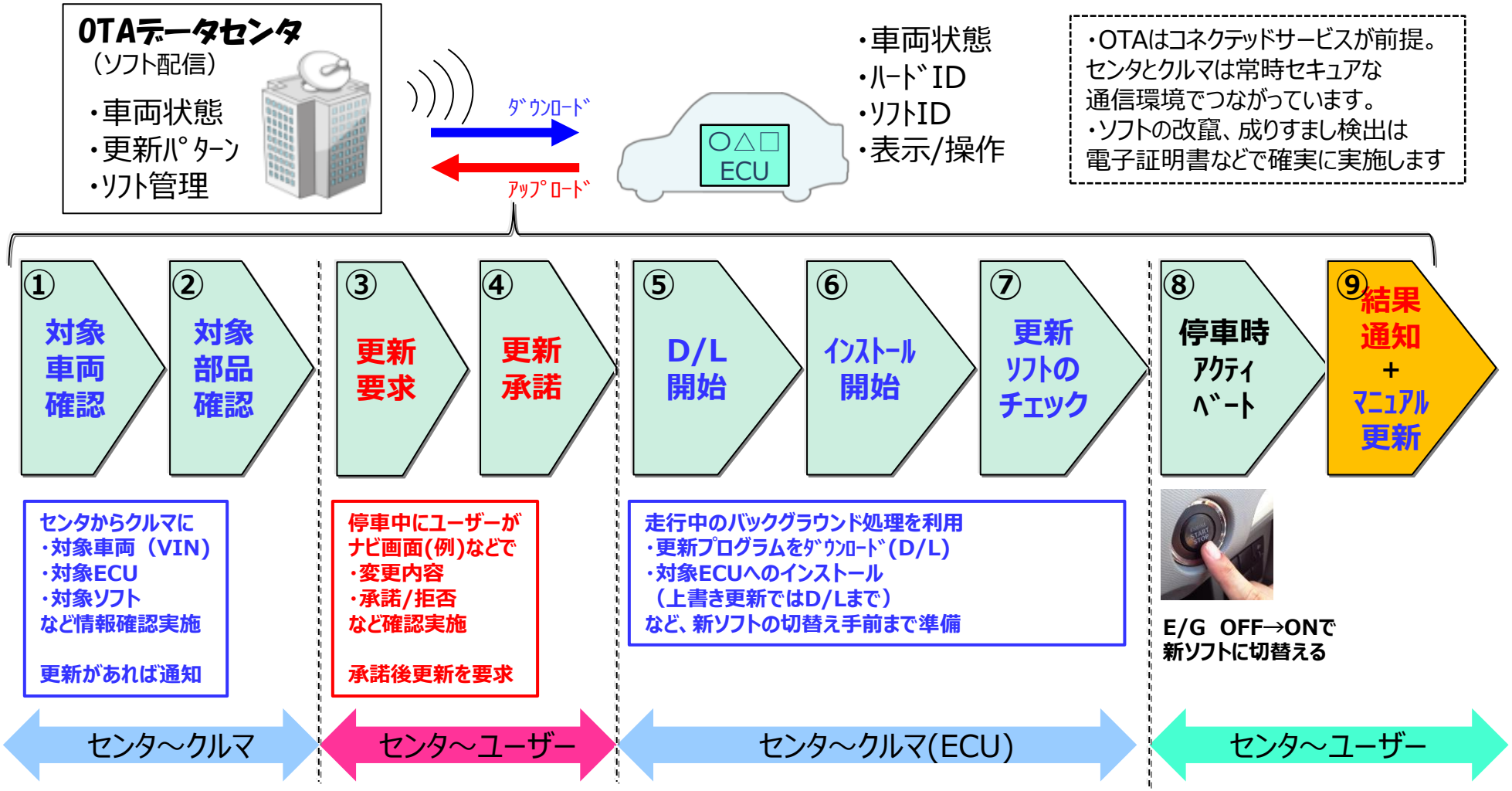
具体的な書面のイメージ

・Demonstrationの内容確認例
①コンテンツの画面表示(sample表示)
②特定ユースケースの画面遷移（ﾕｰｽｹｰｽは申請時の選定で決定）
③規定ユースケースの画面遷移（例：更新通知~更新完了まで）

1.当該型式における改変の成功又は失敗を通知する方法の概説。（通知内容のサンプル提示を含む）
通知方法は車載HMIに限定しない。ただし、当該通知方法が確実に通知を出来るものとして型式申請時に引用するSUMSにて説明済であること。この際、当該デバイスは保安基準適合審査の対象外とする。ただし、型式審査にて通知を実証する際には当該デバイスを使用して実施のこと。
2.取扱説明書の更新をユーザに伝える方法の概説。（通知内容のサンプル提示を含む）

複数の方式がある場合はその全てにおいて、1.及び2.を説明すること。
現車によるデモンストレーション（公式試験にて実施する）

E⑱. 実車デモ 7.2.2.4 更新結果の通知



【デモの手順】

・⑨更新完了時に、更新結果（成功、失敗・・）、更新による変更/追記されるユーザーマニュアルの内容、更新未完了時のユーザーへの対処方法の提示、等が表示されることを確認

判断の目安（WP29解釈文書より引用）

Software Update

7.2.2.4.

Examples of documents/evidence that could be provided	
The following may be used to provide assurance that this requirement is met: (a) Demonstration of requirements via documentation/presentation and/or physical test.	本要件が満たされているという保証を提供するために以下を使用してもよい： (a) 文書／プレゼンテーションおよび／または物理テストを介した要件の証明。

7.2.2.5.
The vehicle shall ensure that preconditions have to be met before the software update is executed.
車両は、ソフトウェア更新が実行される前に、前提条件が満たされなければならないことを保証するものとする。

解釈 (UN解釈文書における要件の説明)

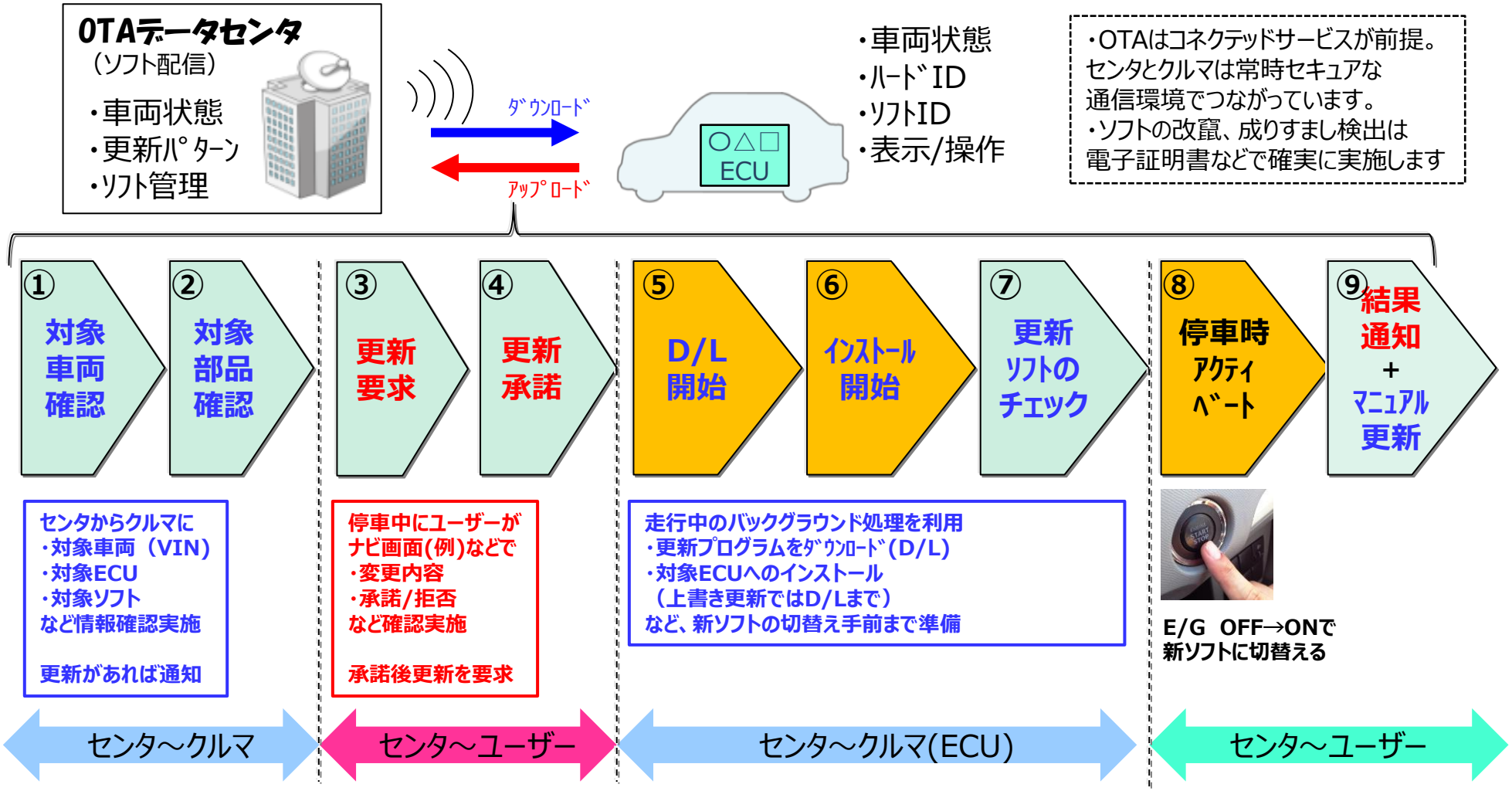
メーカーは、満たすべき前提条件を定義し、ソフトウェア更新が開始するときは常にかかる前提条件が満たされていることを確認すべきものとする。

具体的な書面のイメージ

1）アップデートを開始する前に確認する前提条件の概要説明。（少なくとも何をどのレベルで確認するか説明すること）
2）前提条件から外れた場合の対応についての概要説明。（アップデートを開始しない等）
3）2）の対応について実車での同一性確認。（説明の通りの機能となっているか）

補足
・前提条件は各OEMで定義できる。
・前提条件の説明には状態遷移図などでのSU状態遷移の説明を伴っても良い。

E⑱. 実車デモ 7.2.2.5 開始条件の確認



【デモの手順】

・更新開始条件は、状態遷移図などを用い、車両の状態と関連する条件が、開始条件として成立するフローを確認
ex.ある条件が未成立時には、既定の開始が得られないことをデモ、等

判断の目安（WP29解釈文書より引用）

Software Update

7.2.2.5.

Explanation of the requirement	
The manufacturer should define preconditions to be met and confirm that those preconditions are met whenever the software update starts.	メーカーは、満たすべき前提条件を定義し、ソフトウェア更新が開始するときは常にかかる前提条件が満たされていることを確認すべきものとする。
Examples of documents/evidence that could be provided	
The following may be used to provide assurance that this requirement is met: (a) Demonstration of requirements via documentation/presentation and/or physical test	本要件が満たされているという保証を提供するために以下を使用してもよい： (a) 文書／プレゼンテーションおよび／または物理テストを介した要件の証明。