

SU能力審査マニュアル 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す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、提出文書の一例であり、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。
- ・本マニュアルに示した提出文書を審査部に提出したうえで、審査部試験として提出文書に記載されたプロセスの存在を確認するヒアリングおよび書面等を現認する。
- ・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。
- ・解釈文書においてISOに準拠した説明文書の活用可能性が記載されている場合、これが検討できるのは当該文書にて本マニュアル記載のエビデンスを説明できる場合のみとする。
- ・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。

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ない、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)

7.1.1.1.

A process whereby information regarding all initial and updated software versions, including integrity validation data, and relevant hardware components of a type approved system can be uniquely identified;”

本規則に関する情報を文書化し、車両メーカーにおいてセキュアに保持し、要請に応じて認可当局またはその技術機関に対して利用可能な状態にすることができるプロセス、

解釈 (UN解釈文書における要件の説明)

本要件は2つの部分に分かれる。

最初の部分は、車両メーカーが本規則に関連する情報を保管するために使用するプロセス／手順および当該情報を保護する方法について記載するという要件である。この目的において、「セキュアに」という語は、メーカーにおいて実施するIT（情報技術）セキュリティを指す。

車両メーカーが、すべての関連する文書／情報が保管され、当該情報を保護するために適切なセキュリティ対策が実施されているという保証を提供することができる、というのがその結果であるべきものとする。

2つめの部分は、車両メーカーが、技術機関または認可当局がかかる情報に対してアクセスする権利を有し、かつその必要がある場合に、車両メーカーが、技術機関または認可当局に対して利用可能な状態にする方法についてのプロセス／手順を詳述するという要件である。

本規則（および必要な場合は以前の版）に関連する情報を含む文書は、要請に基づいて、技術機関／認可当局に対して利用可能な状態にすべきものとする。メーカーは、それについて希望するファイル転送プラットフォームを使用してもよい。ただし、技術機関／認可当局との合意があることを条件とする。

車両メーカーと技術機関／認可当局が、記載されたプロセスによって技術機関／認可当局がソフトウェア更新およびその提供プロセス、ならびにそれを共有すべき場合の条件に関する情報にアクセスができることに合意する、というのがその結果であるべきものとする。

具体的な書面のイメージ

1) 組織図

文書管理に関連する部署について、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。

(想定は対象の業務G r までが確認できるもの)

※CSと同レベルの組織図をイメージ。

2) 業務フロー図

3) 業務手順書 (文書管理規定の類を想定)

当局が開示を要求したときに文書開示するプロセスを含むこと。

4) 保管されている書類のリスト

(概略で良い、本規則の各項に対し該当する文書の概略)

5) 書面保管システムにおけるISMS適用を確認できる資料。

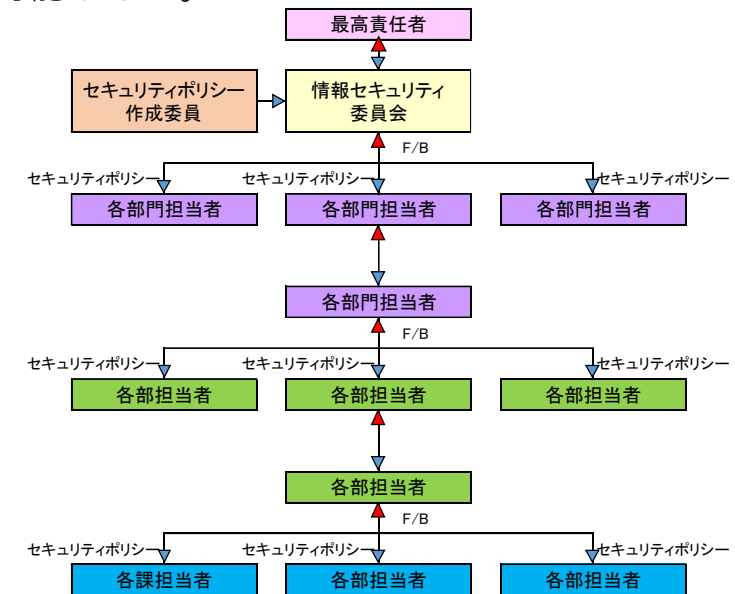
(セキュアな保管を保証するため。または、各社の情報セキュリティに関する管理レベル(保管基準)や文書管理規定や要領を確認する)

6) 保管文書のサンプル(様式)

7) 当局が開示を要求する方法(窓口)

8) 当局が開示を要求した場合に出される結果のサンプル

表紙+内容のサンプル(任意項目、中身なく様式のみでもよい)



7.1.1.1.

Explanation of the requirement

This requirement has two parts.

本要件は2つの部分に分かれる。

The first is a requirement for the vehicle manufacturer to state the processes/procedures they use to store the information relevant to this regulation and how they will secure it. For this the term 'securely' refers to the IT (information technology) security implemented at the manufacturer.

最初の部分は、車両メーカーが本規則に関連する情報を保管するために使用するプロセス／手順および当該情報を保護する方法について記載するという要件である。この目的において、「セキュアに」という語は、メーカーにおいて実施するIT（情報技術）セキュリティを指す。

The outcome should be that the vehicle manufacturer is able to provide assurance that all relevant documentation/information will be stored and that they have appropriate security controls in place to protect that information.

車両メーカーが、すべての関連する文書／情報が保管され、当該情報を保護するために適切なセキュリティ対策が実施されているという保証を提供することができる、というのがその結果であるべきものとする。

The second part is a requirement for the vehicle manufacturer to detail the processes/procedures for how they will make such information available to a Technical Service or Appropriate Authority should they have the right and need to access that information.

2つめの部分は、車両メーカーが、技術機関または認可当局がかかる情報に対してアクセスする権利を有し、かつその必要がある場合に、車両メーカーが、技術機関または認可当局に対して利用可能な状態にする方法についてのプロセス／手順を詳述するという要件である。

Documents containing information relevant to this regulation (and their previous versions, if needed) should be made available to the Technical Service/Approval Authority based on their request. The manufacturer may use their preferred file transfer platforms for the same, as long as it is in agreement with the Technical Service/ Approval Authority.

本規則（および必要な場合は以前の版）に関連する情報を含む文書は、要請に基づいて、技術機関／認可当局に対して利用可能な状態にすべきものとする。メーカーは、それについて希望するファイル転送プラットフォームを使用してもよい。ただし、技術機関／認可当局との合意があることを条件とする。

The outcome should be that the vehicle manufacturer and Technical Service/Approval Authority agree that the process described would allow the Technical Service/ Approval Authority to access information pertinent to the approval of software updates and their delivery processes and the conditions under which it should be shared.

車両メーカーと技術機関／認可当局が、記載されたプロセスによって技術機関／認可当局がソフトウェア更新およびその提供プロセス、ならびにそれを共有すべき場合の条件に関する情報にアクセスができることに合意する、というのがその結果であるべきものとする。

7.1.1.1.

Examples of documents/evidence that could be provided

For evidencing that information is securely held, International Standard Organization (ISO) 27001 or ISO 9001 (add-on) can be used.

The information provided can cover:

- (a) Access controls (both physical and personal);
- (b) Controls for securing the servers that hold the information;
- (c) Monitoring controls;
- (d) Configuration controls;
- (e) quality controls/ quality management systems employed.

The information to be included in these processes is defined within the Regulation, for example paragraph 7.1.2.

For detailing the processes by which this information may be accessed the vehicle manufacturer should include:

- (a) Contact point at the vehicle manufacturer;
- (b) Information on the file transfer platform.

情報がセキュアに保持されていることの証明について、国際標準化機構（ISO）27001またはISO 9001（アドオン）を使用することができる。

提供する情報は、以下を含むことができる：

- (a) アクセス制御（物理的および個人的の両方）、
- (b) 情報を保持するサーバを保護するための対策、
- (c) モニタリング制御、
- (d) 構成の制御、
- (e) 使用している品質管理／品質マネジメントシステム

かかるプロセスに含むべき情報は、例えば7.1.2項のように、本規則内で定められている。

本情報にアクセスすることができるプロセスを詳述するために、車両メーカーは以下を含むべきものとする：

- (a) 車両メーカーの連絡先、
- (b) ファイル転送プラットフォームに関する情報。

7.1.1.2.

A process whereby information regarding all initial and updated software versions, including integrity validation data, and relevant hardware components of a type approved system can be uniquely identified;”

初期および更新済みのすべてのソフトウェアバージョンに関する情報完全性検証データを含む）、ならびに型式認可済みシステムの関連するハードウェア構成部品を一意的に識別することができるプロセス、

解釈 (UN解釈文書における要件の説明)

本要件の目的は、メーカーで使用される構成の制御プロセスに関する保証、ならびにこれらのプロセスが規則の実施をサポートするという保証を提供することである。

具体的な書面のイメージ

1) 組織図

ソフト・ハードの情報管理に関連する部署について、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。（想定は対象の業務Grまでが確認できるもの）

2) 業務フロー図

3) 業務処理手順書

4) ソフトウェアバージョン情報データベース、ハードウェアデータベースの概要

※車体番号に対し、搭載ハード情報、ソフト情報、完全性確認結果等を一意に確認できることが必要。

※来歴を全て追えることを説明する必要がある。

5) 識別結果のサンプル

※特定の型式において、上記の情報が追えることの証明。

7.1.1.2.

Explanation of the requirement

The aim of the requirement is to provide assurance on the configuration control processes used in the manufacturer and that these will support the implementation of the regulation.

本要件の目的は、メーカーで使用される構成の制御プロセスに関する保証、ならびにこれらのプロセスが規則の実施をサポートするという保証を提供することである。

The following clarification should be noted

‘Version number’ may be done at vehicle level and/or component level as long as it is possible to fulfil the requirement of the Regulation for unique identification of software/hardware

「バージョン番号」は、車両レベルおよび／構成部品レベルで実施してもよいが、ソフトウェア／ハードウェアの固有識別に関する本規則の要件を満たすことが可能であることを条件とする

‘Integrity validation data’ refers to how the software can be authenticated as being the version claimed by the vehicle manufacturer. Check sums or hash values can be used for this purpose. The term was used to be technology neutral as other, equivalent methods, could be employed.

「完全性検証データ」とは、ソフトウェアが、車両メーカーが主張するバージョンであるとして認証することができる方法を指す。この目的には合計値またはハッシュ値の確認を用いることができる。この語は、他の同等の方法も使用することができたため、以前は技術に関係のない用語であった。

‘Relevant hardware components’ refer to hardware with software on it within the type approved system. This should include ECUs, CPUs or other hardware as identified by the vehicle manufacturer

「関連するハードウェア構成部品」とは、型式認可済みシステム内でソフトウェアを搭載したハードウェアを指す。これは、ECU、CPUまたは車両メーカーが指定したその他のハードウェアを含むべきものとする

‘Can be uniquely identified’ intends that it should be possible, at the very least, for the vehicle manufacturer to identify and verify the software present on a type approved system based on its software version numbers

「一意的に識別することができる」とは、少なくとも車両メーカーがソフトウェアのバージョン番号に基づいて、型式認可済みシステムに搭載されているソフトウェアを識別し検証することが可能であるべきである、ということを意図している

Examples of documents/evidence that could be provided

For evidencing the processes existing configuration control processes/procedures can be used and relevant standards may be referred to. This should be accompanied by an explanation of why they are relevant.

プロセスの証拠については、既存の構成制御プロセス／手順を用いることができ、関連する基準に言及してもよい。これには、なぜそれらが関連するかという理由の説明を添付すべきものとする。

7.1.1.3.

A process whereby, for a vehicle type that has an RXSWIN, information regarding the RXSWIN of the vehicle type before and after an update can be accessed and updated. This shall include the ability to update information regarding the software versions and their integrity validation data of all relevant software for each RXSWIN;”

RXSWINを有する車両型式について、更新前後の車両型式のRXSWINに関する情報にアクセスができ、更新することができるプロセス。これは、各RXSWINに関連するすべてのソフトウェアのソフトウェアバージョンおよび完全性検証データに関する情報を更新する能力を含むものとする、

解釈 (UN解釈文書における要件の説明)

RXSWINとは、任意のUN規則「X」に従って、型式認可済みシステムの固有のソフトウェアセットを定義づける固有識別子を指す。この範囲内において、型式認可の拡大または更新につながる、当該定義済みシステムのソフトウェアに変更があった場合に限り、固有識別子に変更になるべきものとする。ソフトウェア更新が当該システムの型式認可に影響を与えない場合は、本固有識別子は、変更しないままとすべきものとする。

本規則は、車両メーカーがRXSWINに関連する情報を記録するプロセスを有することを義務付けるものである（7.1.2.3参照）。これは、任意のRXSWINで定義されたソフトウェアの許容されるすべてのソフトウェアバージョン、かかる異なるソフトウェアバージョンの関連する「完全性検証データ」に関する情報を含む。

RXSWINに関する情報にアクセスし更新することができることを車両メーカーが証明できる、というのがその結果であるべきものとする。

具体的な書面のイメージ

1) 組織図

RXSWINに関する情報管理にについて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。

(想定は対象の業務Grまでが確認できるもの)

2) 業務フロー図

3) 業務手順書

※2) 3) ではアクセスだけでなくアップデート時にRxSWIN関連情報を“更新”するプロセスの概要説明を含むこと。

4) RXSWINの定義について概要説明 (どのような考え方に基づいて番号を定めているか)

5) RXSWINのサンプル

6) RXSWINデータベースの概要

※RXSWINから関連ソフトウェア、バージョン、完全性確認結果が追えることの説明。また、情報の保管場所に関する概略説明。

7) 識別結果のサンプル

※特定の型式において、上記の情報が追えることの証明。(ダミーデータでもOK)

※ここでは、RxSWINに紐付けられるべき情報とその管理プロセスに注目。アップデートによる車両の機能変更についての検証プロセスは7.1.1.8

7.1.1.3.

Explanation of the requirement

The RXSWIN refers to a unique identifier that defines a unique set of software of a type approved system in accordance with a given UN Regulation “X”. Within this the unique identifier should only change when there is a change to the software of that defined system which leads to an extension or renewal of type approval. Where a software update does not affect the type approval of the system this unique identifier should remain unchanged.

RXSWINとは、任意のUN規則「X」に従って、型式認可済みシステムの固有のソフトウェアセットを定義づける固有識別子を指す。この範囲内において、型式認可の拡大または更新につながる、当該定義済みシステムのソフトウェアに変更があった場合に限り、固有識別子が変わるべきものとする。ソフトウェア更新が当該システムの型式認可に影響を与えない場合は、本固有識別子は、変更しないままとすべきものとする。

This Regulation mandates that the vehicle manufacturer should have a process in place to record information relating to the RXSWIN (see 7.1.2.3). This includes information on all permissible software versions of the software defined under a given RXSWIN, the relevant ‘integrity validation data’ of those different software versions.

本規則は、車両メーカーがRXSWINに関連する情報を記録するプロセスを有することを義務付けるものである(7.1.2.3参照)。これは、任意のRXSWINで定義されたソフトウェアの許容されるすべてのソフトウェアバージョン、かかる異なるソフトウェアバージョンの関連する「完全性検証データ」に関する情報を含む。

The outcome should be that the vehicle manufacturer is able to demonstrate that information regarding the RXSWIN can be accessed and update

RXSWINに関する情報にアクセスし更新することができることを車両メーカーが証明できる、というのがその結果であるべきものとする。

The following clarification should be noted

This requirement only applies when an RXSWIN is implemented
The storage of the information should be at the vehicle manufacturer. The vehicle manufacturer should determine the level of information stored on the vehicle

本要件は、RXSWINが実施される場合に限り適用する情報は、車両メーカーにおいて保管すべきものとする。車両メーカーが、車両に保管する情報のレベルを決定すべきものとする

Examples of documents/evidence that could be provided

Manufacturer should detail and explain their processes to provide information regarding:
(a) How the information regarding the RXSWIN is updated, this should include reference to configuration control processes used;
(b) How all information related to the RXSWIN, held either on the vehicle or at the manufacturer, can be accessed.

メーカーは、以下に関する情報を提供するプロセスについて詳細に説明すべきものとする：
(a) RXSWINに関する情報を更新する方法。これは、使用される構成制御プロセスへの言及を含むべきものとする、
(b) 車両または車両メーカーのいずれかで保存されているRXSWINに関連するすべての情報にアクセスできる方法。

7.1.1.4.

A process whereby, for a vehicle type that has an RXSWIN, the vehicle manufacturer can verify that the software version(s) present on a component of a type approved system are consistent with those defined by the relevant RXSWIN;”

RXSWINを有する車両型式について、型式認可済みシステムの構成部品に搭載されているソフトウェアバージョンが、関連するRXSWINで定義されたバージョンと一致することを車両メーカーが検証できるプロセス、

解釈 (UN解釈文書における要件の説明)

本規則は、型式認可済みシステムに搭載されているソフトウェアが、関連するRXSWINに定義されたソフトウェアに対応することを検証することが可能であることを要求するものである。最低でも、車両メーカーが構成部品レベルまで本検証を実施することが可能でなければならない。

具体的な書面のイメージ

1) 組織図

RXSWINに関する情報管理にについて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。
(想定は対象の業務G rまでが確認できるもの)

2) 業務フロー図 (検証業務について)

3) 業務手順書 (基準書そのものでなくとも緒業務処理方法が判別できればよい)

4) 検証を電算システムで行うのであれば、そのシステムの概要。人的に行うのであればその手法の概要。

5) 識別結果のサンプル

※特定のRXSWINについて、実構成部品のソフトバージョンとの検証結果 (ダミーデータでもOK)

注： RxSWIN読み出しについてはSU型式審査マニュアルを参照のこと

7.1.1.4.

Explanation of the requirement

The regulation requires that it should be possible to verify that the software on a type approved system corresponds to that defined in the relevant RXSWIN. As a minimum it must be possible for the vehicle manufacturer to perform this verification down to a component level.

本規則は、型式認可済みシステムに搭載されているソフトウェアが、関連するRXSWINに定義されたソフトウェアに対応することを検証することが可能であることを要求するものである。最低でも、車両メーカーが構成部品レベルまで本検証を実施することが可能でなければならない。

Examples of documents/evidence that could be provided

The manufacturer should provide details of their process(es) and/or tools that will be used to verify the software on a type approved system corresponds to the list of software versions covered under a particular RXSWIN.

メーカーは、型式認可済みシステムに搭載されたソフトウェアが、特定のRXSWINの対象であるソフトウェアバージョンのリストに対応することを検証するために使用されるプロセスおよび／またはツールの詳細を提供すべきものとする。

7.1.1.5.

A process whereby any interdependencies of the updated system with other systems can be identified;”
更新したシステムとその他のシステムとの相互依存性が識別できるプロセス、

解釈 (UN解釈文書における要件の説明)

本要件は、例えばカスケード効果など、更新がその他のシステムに影響を与えるかどうかを評価するためのプロセスが1つ以上あることを保証するためのものである。プロセスがどの程度相互依存性を対象とするかについて制限があることは容認されている。

車両メーカーが、異なるシステムがどのように相互作用するかを特定し、更新がその他のシステムの想定される挙動に影響を与えるかどうかを評価することができることの保証が、その結果であるべきものとする。

具体的な書面のイメージ

1) 組織図

相互依存の検証において、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。

(想定は対象の業務G r までが確認できるもの)

2) 業務フロー図 (検証業務について)

3) 検証を電算システムで行うのであれば、そのシステムの概要。人的に行うのであればその手法の概要。

4) 業務手順書

5) 相互依存の識別結果のサンプル

※特定のシステムにおいて、相互依存を検証した結果 (ダミーデータでもOK)

7.1.1.5.

Explanation of the requirement

This requirement is to ensure that there is one or more processes to assess if an update will affect other systems, e.g. for cascading effects. It is accepted that there are limits in how far a process could cover interdependencies.

本要件は、例えばカスケード効果など、更新がその他のシステムに影響を与えるかどうかを評価するためのプロセスが1つ以上あることを保証するためのものである。プロセスがどの程度相互依存性を対象とするかについて制限があることは容認されている。

The outcome should be assurance that the vehicle manufacturer is able to identify how different systems interact and assess if an update will impact the expected behaviour of any other system.

車両メーカーが、異なるシステムがどのように相互作用するかを特定し、更新がその他のシステムの想定される挙動に影響を与えるかどうかを評価することができることの保証が、その結果であるべきものとする。

The following clarification should be noted

'Interdependencies' should be identified at both the functional and software level and should consider all systems which have an interface with the updated system

「相互依存性」は、機能レベルとソフトウェアレベルの両方において特定すべきものであり、かつ更新されたシステムとインターフェースを有するすべてのシステムを考慮すべきものとする。

'Other systems' includes systems affecting safety, cyber security, theft protection, energy efficiency and environmental behavior

「その他のシステム」は、安全、サイバーセキュリティ、窃盗保護、エネルギー効率および環境挙動に影響を及ぼすシステムを含む。

7.1.1.5.

Examples of documents/evidence that could be provided

The processes used to assess if there are any interdependencies between systems and the potential for a software update to affect other systems should follow best practice. This may include quality control processes.

Standards that might be applicable include:

- (a) ISO 10007;
- (b) ISO 9001;
- (c) International Automotive Task Force (IATF) 16949;
- (d) A Software Process Improvement and Capability Determination (SPICE) or similar.

The processes should consider the following:

- (a) Initiation, identification and documentation of the change;
- (b) Identification of interfaces and systems which communicate with the updated systems;
- (c) Identification of any systems that are affected by the updated systems and the corresponding impact;
- (d) Evaluation of the change.

システム間に相互依存性があるかどうか、およびソフトウェア更新がその他のシステムに影響を与える可能性があるかどうかを評価するために用いられるプロセスは、ベストプラクティスに従うべきものとする。これには、品質管理プロセスを含んでいる場合がある。

適用される可能性のある基準には以下が含まれる：

- (a) ISO 10007、
- (b) ISO 9001、
- (c) 国際自動車タスクフォース（IATF）16949、
- (d) ソフトウェアプロセス改善・能力評価（SPICE）またはそれに類似するもの。

プロセスは以下を考慮に入れるべきものとする：

- (a) 変更の開始、特定および文書化、
- (b) 更新されたシステムと通信をするインターフェースおよびシステムの特定、
- (c) 更新されたシステムによって影響を受けるシステムと対応する影響の特定、
- (d) 変更の評価。

7.1.1.6.

A process whereby the vehicle manufacturer is able to identify target vehicles for a software update;”
車両メーカーが、ソフトウェア更新の対象車両を特定することができるプロセス、

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) 組織図

特定車両の特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。
(想定は対象の業務G rまでが確認できるもの)

2) 業務フロー図

3) 業務手順書 (基準書そのものでなくとも業務処理方法が判別できればよい)

4) 検証を電算システムで行うのであれば、そのシステムの概要。人的に行うのであればその手法の概要。

※具体的に、どのようなデータベースからどのパラメータを使って車両をVIN単位で特定するかを説明できること。

※更新対象デバイス (ECU) によってVINの特定方式が異なる場合には全ての方式について。

5) 識別結果のサンプル

※特定のシステムにおいて、VINを特定した結果。(ダミーデータでもOK)

7.1.1.6.

The following clarification should be noted

'Target vehicle' refers to individual vehicles (for example VIN based for registered vehicles)
This requirement is on the process

「対象車両」とは、個別の車両（例えば、登録車両についてはVINに基づく）を指す
本要件はプロセスに関する

Examples of documents/evidence that could be provided

The processes should consider the following:
(a) Listing target vehicles affected by the software update;
(b) The process should consider the steps of going from target groups for an update (e.g. all diesel vehicles of a specific vehicle type) through to the individual vehicles to be updated;
(c) Measures implemented to reduce the risk of error in identification of target vehicles.

当該プロセスは以下を考慮すべきものとする：
(a) ソフトウェア更新によって影響を受ける対象車両のリスト化、
(b) プロセスは、更新の対象グループ（例えば、特定の車両型式のすべてのディーゼル車両）から更新すべき個別車両までのステップを考慮に入れるべきものとする。
(c) 対象車両の特定における間違いを低減するために実施している措置。

7.1.1.7.

A process to confirm the compatibility of a software update with the target vehicle(s) configuration before it is issued. This shall include an assessment of the last known software/hardware configuration of the target vehicle(s) for compatibility with the update before it is issued;”

ソフトウェア更新と対象車両の構成の適合性を発行される前に確認するプロセス。これは、発行される前に当該更新との適合性に関する、対象車両の最新の既知ソフトウェア／ハードウェア構成の評価を含むものとする、

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) 組織図

互換性検証プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。
(想定は対象の業務G rまでが確認できるもの)

2) 業務フロー図

3) 業務手順書

4) 検証を電算システムで行うのであれば、そのシステムの概要。人的に行うのであればその手法の概要。

※具体的に、どのようなデータベースからどのパラメータを使って互換性の検証を行うかが説明できること。

5) 確認結果のサンプル

※特定のシステムにおいて、相互依存を検証した結果 (ダミーデータでもOK)

7.1.1.7.

The following clarification should be noted

‘Issued’ refers to the software update being made available for installation 「発行される」とは、インストール用に利用可能な状態にしているソフトウェア更新を指す。

Examples of documents/evidence that could be provided

Standards that might be applicable include:

- (a) Compliance with configuration management as per ISO 10007;
- (b) ISO 9001;
- (c) IATF 16949 or similar.

適用される可能性のある基準には以下が含まれる：

- (a) ISO 10007に準拠した構成管理への適合、
- (b) ISO 9001、
- (c) IATF 16949またはそれに類似するもの。

The processes should consider the following:

- (a) Regression testing with the last known configuration of the software update;
- (b) Listing the hardware or software preconditions required for the software update;
- (c) How these preconditions will be checked before an update is downloaded;
- (d) Identifying relevant configurations of the target vehicle type;
- (e) demonstrating how testing will cover compatibility for those configurations.

プロセスは以下を考慮に入れるべきものとする：

- (a) ソフトウェア更新の最新の既知構成を用いた回帰テスト、
- (b) ソフトウェア更新に必要なハードウェアまたはソフトウェアの前提条件のリスト化、
- (c) 更新がダウンロードされる前に、かかる前提条件を確認する方法、
- (d) 対象車両型式の関連する構成の特定、
- (e) テストによってかかる構成の適合性をどのように網羅するかの証明。

7.1.1.8.

A process to assess, identify and record whether a software update will affect any type approved systems. This shall consider whether the update will impact or alter any of the parameters used to define the systems the update may affect or whether it may change any of the parameters used to type approve those system (as defined in the relevant legislation);”

ソフトウェア更新が型式認可済みシステムに影響を与えるかどうかを評価、特定および記録するプロセス。これは、更新が、当該更新が影響を与える可能性のあるシステムを定義するために使用したパラメータのいずれかに影響を与える、あるいはかかるパラメータを変えるかどうか、または更新がかかるシステムの型式認可に使用されたパラメータ（関連する法規で定められているとおり）のいずれかを変えるかどうかを考慮するものとする、

解釈 (UN解釈文書における要件の説明)

本要件は、型式認可済みシステムおよび当該型式認可に用いられた関連するテストにのみ関係している。本要件は、ソフトウェア更新が、テストが実施された条件において、当該テストの結果に影響を与える、あるいはかかる結果を変える可能性があるかどうかを評価するプロセスがあることを求めている。本要件は、型式認可に使用された関連するテストおよび、ソフトウェア更新が、テストが実施された条件において、当該テストの結果に影響を与える、あるいはかかる結果を変える可能性があるかどうかを考慮すべきものとする。

具体的な書面のイメージ

当該パラメータの定義や内容の説明書面 例：部品によりCSが型式要件になるか否かで対象が変化

1) 組織図

評価、特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。

(想定は対象の業務Grまでが確認できるもの)

2) 業務フロー図

3) 業務手順書

4) ソフトウェアの具体的な変更内容を抽出する方法 (7.1.1.2と関連させても良い) ただし、変更の具体的な変更内容を把握できること。

(制御設計レベルまでで良く、コーディングを含まない。)

5) 変更内容が関連するレギュレーションの抽出手法 (業務手順書に記載があること)

6) 変更内容が影響するレギュレーションに対するエクステンションの要否判断手法 (業務手順書に記載があること)

7) 関連するレギュレーションの再審査までの業務プロセス (再審査結果の刈り取りまで、業務手順書に記載があること)

8) 確認結果のサンプル

※特定のシステムにおいて、既存システムへの影響を確認した結果 (ダミー車両に対してでも良い)

9) 確認結果を記録として残す手段についての説明 (業務手順書に記載があること) 7.1.1.1もしくは7.1.2.5.等と関連付けて説明してもよい。

7.1.1.8.

Explanation of the requirement

This requirement relates only to type approved systems and the relevant test used for the type approval(s). It requires that there are processes to assess whether a software update might affect or change the outcome of that test under the conditions in which it was conducted. This requirement should consider the relevant test used for the type approval(s) and whether the software update might affect or change the outcome of that test under the conditions in which it was conducted.

本要件は、型式認可済みシステムおよび当該型式認可に用いられた関連するテストのみ関係している。本要件は、ソフトウェア更新が、テストが実施された条件において、当該テストの結果に影響を与える、あるいはかかる結果を変える可能性があるかどうかを評価するプロセスがあることを求めている。本要件は、型式認可に使用された関連するテストおよび、ソフトウェア更新が、テストが実施された条件において、当該テストの結果に影響を与える、あるいはかかる結果を変える可能性があるかどうかを考慮すべきものとする。

The following clarification should be noted

‘Parameters’ here does not refer to software parameters but to the parameters describing the system type approval

この「パラメータ」とは、ソフトウェアのパラメータではなくシステムの型式認可について記載するパラメータを指す

‘Affect’ refers to a change requiring an extension of a type approved system or a new type approval

「影響を与える」とは、型式認可済みシステムの延長または新規型式認可が必要な変更を指す

Examples of documents/evidence that could be provided

Standards that might be applicable include:

- (a) Compliance with configuration management as per ISO 10007, ISO 9001, IATF 16949 or similar
- (b) Standards for providing claims, arguments and evidence such as BSI 15026-2:2011

適用される可能性のある基準には以下が含まれる：

- (a) ISO 10007、ISO 9001、IATF 16949またはそれに類似するものに準拠した構成管理への適合
- (b) BSI 15026-2:2011など、主張、論拠および証拠を提供するための基準

The processes should consider the following:

- (a) Quality control procedures for the software updates may be relevant;
- (b) Evaluation of the change;
- (c) Assessment of which regulatory requirements/ parameters are impacted/ altered by the software update. This should include what evidence is required to reach a conclusion.

プロセスは以下を考慮に入れるべきものとする：

- (a) ソフトウェア更新の品質管理手順が関連する可能性がある、
- (b) 変更の評価、
- (c) ソフトウェア更新によってどの規制要件/パラメータが影響を受ける/変更になるかの評価。これは、結論を出すためにどの証拠が要求されるかを含むべきものとする。

7.1.1.9.

A process to assess, identify and record whether a software update will add, alter or enable any functions that were not present, or enabled, when the vehicle was type approved or alter or disable any other parameters or functions that are defined within legislation. The assessment shall include consideration of whether:

- (a) Entries in the information package will need to be modified;
- (b) Test results no longer cover the vehicle after modification;
- (c) Any modification to functions on the vehicle will affect the vehicle's type approval.”

ソフトウェア更新が、車両が型式認可を受けたときには存在していなかった、あるいは有効ではなかった機能を追加、変更もしくは有効にするかどうか、あるいは法規内で定義されているその他のパラメータもしくは機能を変更する、あるいは無効にするかどうかを評価、特定および記録するプロセス。当該評価は、以下の考慮を含むべきものとする：

- (a) 資料パッケージの項目を変更する必要があるかどうか、
- (b) 変更後、当該車両がテスト結果の対象ではなくなるかどうか、
- (c) 車両の機能への変更が、車両の型式認可に影響を与えるかどうか。

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

基本的な考え方は7.1.1.8に同じ

1) 組織図

評価、特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。
(想定は対象の業務G rまでが確認できるもの)

2) 業務フロー図

3) 業務手順書

4) ソフトウェアの具体的な変更内容を抽出する方法 (7.1.1.2と関連させても良い) ただし、変更の具体的な変更内容を把握できること。
(制御設計レベルまでで良く、コーディングを含まない。)

5) 変更内容が関連するレギュレーションの抽出手法 (業務処理基準書に記載があること)

6) 変更内容が影響するレギュレーションに対するエクステンションの要否判断手法 (業務手順書に記載があること)

7) 関連するレギュレーションの再審査までの業務プロセス (再審査結果の刈り取りまで、業務手順書に記載があること)

8) 確認結果のサンプル

※特定のシステムにおいて、既存システムへの影響を確認した結果 (ダミー車両に対してでも良い)

9) 確認結果を記録として残す手段についての説明 (業務手順書に記載があること) 7.1.1.1もしくは7.1.2.5等と関連付けて説明してもよい。

7.1.1.9.

The following clarification should be noted

'Alter or disable any other parameters or functions' refers to type approved systems

「その他のパラメータもしくは機能を変更する、あるいは無効にする」とは、型式認可済みシステムを指す

'Parameters' here does not refer to software parameters but to the parameters describing the system type approval

この「パラメータ」とは、ソフトウェアのパラメータではなくシステムの型式認可について記載するパラメータを指す

'Information package' refers to the affected type approval and its information document

「資料パッケージ」とは、影響を受けた型式認可およびその資料文書を指す

7.1.1.10.

A process to assess, identify and record if a software update will affect any other system required for the safe and continued operation of the vehicle or if the update will add or alter functionality of the vehicle compared to when it was registered;”

ソフトウェア更新が、車両が安全で継続的に作動するために必要なその他のシステムに影響を与えるかどうか、あるいは更新が車両登録時と比較して車両の機能性を追加または変更するかどうかを評価、特定および記録するプロセス、

解釈 (UN解釈文書における要件の説明)

本要件は、車両の安全な作動を確保するために要求される型式認可済みではないシステム、およびソフトウェア更新がかかるシステムに影響を与えるかどうかを評価するプロセスがあるということに関連している。

本要件はまた、車両登録時と比較して、更新が車両の機能性を変更するかどうかを特定するプロセスを要求している。

具体的な書面のイメージ

基本的な考え方は7.1.1.9に同じ

1) 組織図

評価、特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。
(想定は対象の業務G rまでが確認できるもの)

2) 業務フロー図

3) 業務手順書 (基準書そのものでなくとも業務処理方法が判別できればよい)

4) ソフトウェアの具体的な変更内容を抽出する方法 (これまでの項と共通化してもよい) ただし、変更の具体的な変更内容を把握できること。(制御設計レベルまでで良く、コーディングを含まない。)

5) 変更内容の安全機能への影響判断手法 (業務手順書に記載があること)

7) 登録時からの変更内容の判断手法 (業務手順書に記載があること)

8) 確認結果のサンプル

※特定のシステムにおいて、既存システムへの影響を確認した結果 (ダミー車両に対してでも良い)

9) 上記の評価結果を記録する手法 (業務手順書に記載があること)

7.1.1.10.

Explanation of the requirement

This requirement relates to non-type approved systems that are required to ensure safe operation of the vehicle and there are processes to assess if software updates will affect them.

本要件は、車両の安全な作動を確保するために要求される型式認可済みではないシステム、およびソフトウェア更新がかかるシステムに影響を与えるかどうかを評価するプロセスがあるということに関連している。

The requirement also requires processes to identify if an update will change the functionality of a vehicle compared to when it was registered.

本要件はまた、車両登録時と比較して、更新が車両の機能性を変更するかどうかを特定するプロセスを要求している。

Examples of documents/evidence that could be provided

Standards that might be applicable include:

(a) IATF 16949 contains Quality Management Systems for configuration management

適用される可能性のある基準には以下が含まれる：

(a) IATF 16949は構成管理に関する品質マネジメントシステムを含んでいる

The processes should consider the following:

- (a) Quality control and configuration management processes;
- (b) Processes for assessment of which systems are impacted by the software update;
- (c) Processes for assessment of which safety and operational conditions are impacted by a software update;
- (d) Processes for assessment of any functionality that was added/ altered after the vehicle was registered;
- (e) How these impacts are documented.

プロセスは以下を考慮に入れるべきものとする：

- (a) 品質管理および構成管理プロセス、
- (b) ソフトウェア更新によってどのシステムが影響を受けるかを評価するためのプロセス、
- (c) ソフトウェア更新によってどの安全および作動条件が影響を受けるかを評価するためのプロセス、
- (d) 車両登録後に追加／変更された機能性を評価するためのプロセス、
- (e) かかる影響を文書化する方法。

7.1.1.11.

A process whereby the vehicle user is able to be informed about updates.

車両ユーザーが更新について通知を受けることができるプロセス。

解釈 (UN解釈文書における要件の説明)

本要件の意図は、車両ユーザーが、ユーザーが責任を有する車両への変更について通知を受けられるということである。これは、車両ユーザーが更新のダウンロードおよびインストールのために何らかの行動を実行することが想定される状況に関連する情報を含むべきものとする。複数の更新のパッケージの場合、「車両ユーザー」は、当該更新パッケージについて通知を受けられるべきものとする。

ユーザーに情報を提供する手段は車載でなくてもよいが、「車両ユーザー」がアクセスしたい場合にはアクセス可能でなければならない。

本要件は、同意の必要性は含んでいない。

車両ユーザーが、車両メーカーが記載するプロセスによって、自分の車両に対する更新について通知を受けられることを技術機関／該当局が納得していることが、本要件の結果であるべきものとする。

具体的な書面のイメージ

- 1) 組織図
評価、特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。
(想定は対象の業務G r までが確認できるもの)
- 2) 業務フロー図
- 3) 業務手順書
- 4) 更新をユーザに伝えるプロセスの概要 (業務基準書に含まれていること)

今後、通知方法には以下をはじめ様々な手段が検討対象になる可能性がある。(解釈文書では車上でなくともよいと記載あり)

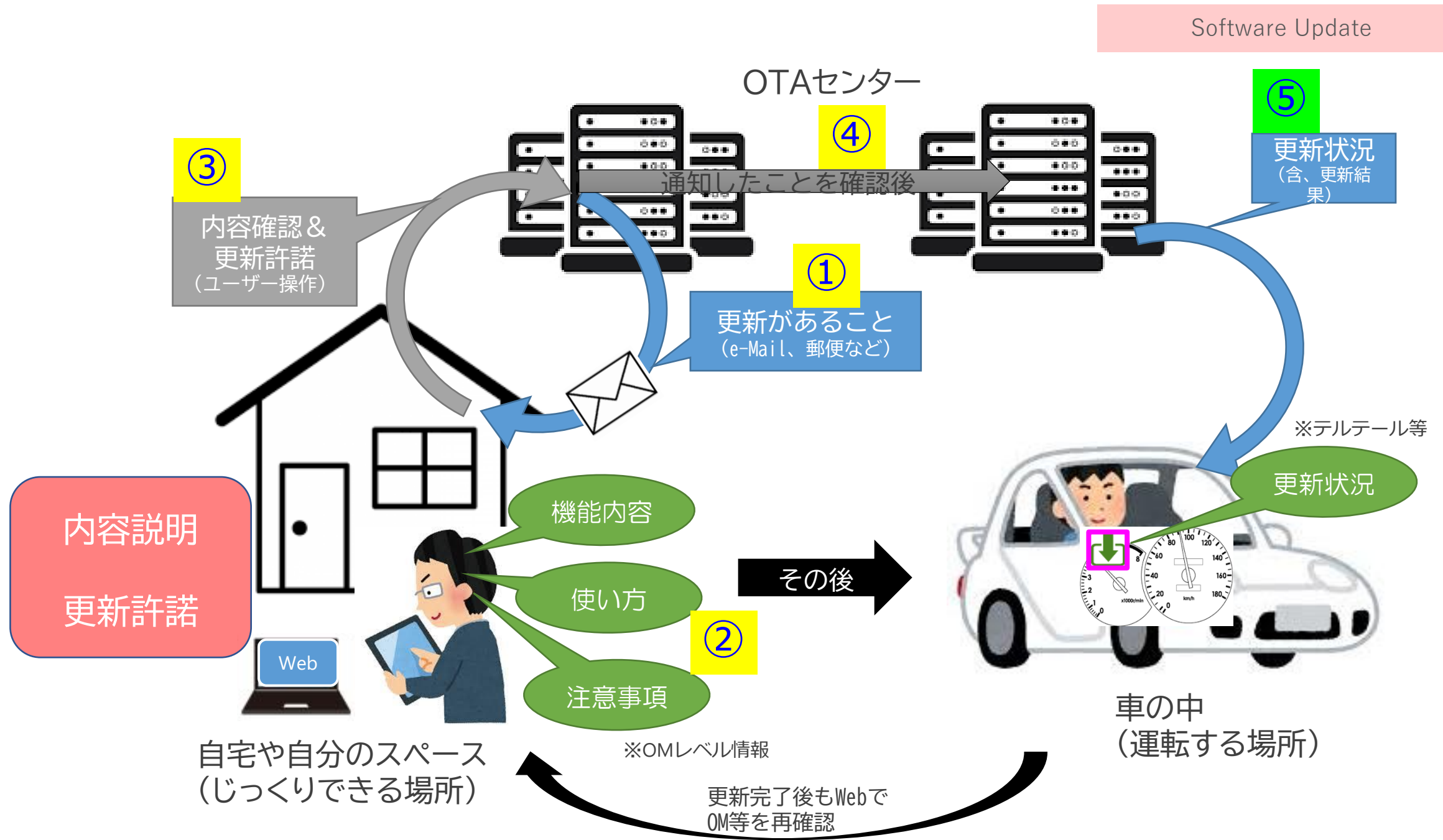
この際は、SUMSとして採用する可能性のある全ての通知手段について上記の通りプロセスを説明のこと。

車載以外のデバイスにて通知を行う場合は、ユーザに通知を確実に伝達するプロセスを含め説明のこと。(次項はそのイメージ、認証時には業務手順書等にて説明のこと。)

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。

通知手段として可能性がある例 (例でありこれに限らない、また現時点で必ずしも全てが通知手段として許容されているとは限らない)

- ・ 車両HMI
- ・ スマートフォン
- ・ PC
- ・ 手紙
- ・ 訪問
- ・ Web通知
- ・ 広報



7.1.1.11.

Explanation of the requirement

The intention of this requirement is that the vehicle user is able to be informed about changes to the vehicle they are responsible for. This should include any information relating to the situation where the vehicle user is supposed to perform some/any action for the download and installation of the updates. In case of a package of multiple updates the 'vehicle user' should be able to be informed about that package of updates.

本要件の意図は、車両ユーザーが、ユーザーが責任を有する車両への変更について通知を受けることができるということである。これは、車両ユーザーが更新のダウンロードおよびインストールのために何らかの行動を実行することが想定される状況に関連する情報を含むべきものとする。複数の更新のパッケージの場合、「車両ユーザー」は、当該更新パッケージについて通知を受けることができるべきものとする。

The means whereby information is provided to the user need not be on the vehicle but it must be accessible by 'vehicle users' if they want to access the information.

ユーザーに情報を提供する手段は車載でなくてもよいが、「車両ユーザー」がアクセスしたい場合にはアクセス可能でなければならない。

This requirement does not cover the need for consent.

本要件は、同意の必要性は含んでいない。

The outcome for this requirement should be that the Technical Service/ Appropriate Authority is satisfied that vehicle users will be able to be informed about updates to their vehicle by the process described by the vehicle manufacturer.

車両ユーザーが、車両メーカーが記載するプロセスによって、自分の車両に対する更新について通知を受けることができることを技術機関/該当局が納得していることが、本要件の結果であるべきものとする。

The following clarification should be noted

'Is able to' requires that the user should be informed by any suitable means

「することができる」とは、ユーザーがいずれかの適切な手段によって通知を受けることが求められるということである

Examples of documents/evidence that could be provided

The vehicle manufacturer should provide information on the methods of communication used to inform the vehicle user about updates. They should demonstrate the effectiveness of these methods.

車両メーカーは、更新について車両ユーザーに通知するために使用する通信手段に関する情報を提供すべきものとする。車両メーカーは、かかる手段の有効性を証明すべきものとする。

7.1.1.12.

A process whereby the vehicle manufacturer shall be able to make the information according to paragraph 7.1.2.3. and 7.1.2.4. available to responsible Authorities or the Technical Services. This may be for the purpose of type approval, conformity of production, market surveillance, recalls and Periodic Technical Inspection (PTI).”

車両メーカーが、7.1.2.3項および7.1.2.4項に従って責任を有する当局または技術機関に対して、情報を利用可能な状態にすることができるプロセス。これは、型式認可、生産の適合性、市場監視、リコールおよび定期技術検査（PTI）の目的のためである場合がある。

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) 組織図
評価、特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。
(想定は対象の業務G rまでが確認できるもの)
- 2) 業務フロー図
- 3) 業務手順書
- 4) 関係情報を当局に利用可能とする方法（問い合わせ先を含む）。およびそのシステムの説明。
(データベース、問い合わせでの応答など)
- 5) 情報開示結果のサンプル。（記載内容はダミーでもよい）

※7.1.1.1.と関連付けて表現してもよい。

7.2.2.1.3.

No guidance included in this document with regards this requirement

-

-

7.1.2.

The vehicle manufacturer shall record, and store, the following information for each update applied to a given vehicle type:”

車両メーカーは、任意の車両型式に適用される各更新について、以下の情報を記録および保管するものとする：

解釈 (UN解釈文書における要件の説明)

本要件は、車両メーカーのプロセスによって、ソフトウェア更新に関する情報（以下の下位の項に定義）を記録することができることを保証するために定められている。

本要件によって、登録当局がソフトウェア更新に関連してメーカーの監査を要請した場合に、かかる当局に対して情報が利用可能な状態になり、かつ本要件は、当該要件についてどのような情報を記録すべきものかを定めるものである。

車両システムが同じ種類の更新で定期的に更新され、更新中のシステムが型式認可を受けていない場合がある。同じ提供方法を介して同じデータフィールドおよびフォーマットを用いるマップデータが、この例である場合がある。この場合、繰り返しを削減するために、下記に詳述する情報を1回だけ記録し、当該クラスの更新（これはメーカーが定義する必要がある）については本情報が該当すると記載するように要求することができる。更新のかかる定期的なシリーズが存在することをメーカーが証明することができた場合には、メーカーの負担を低減することがこの論理である。

具体的な書面のイメージ

- 1) 組織図
評価、特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。
(想定は対象の業務G rまでが確認できるもの)
- 2) 業務フロー図
- 3) 業務処理手準書 (基準書そのものでなくとも緒業務処理方法が判別できればよい)
- 4) 7.1.2.1.~7.1.2.5.までの文書管理の方法
(保管方法の概要。以下の資料をどのようにまとめて、どのように保管するか。保管方法の信頼性に関する評価内容。)
- 5) 保管文書のサンプル

※ 7.1.2.1.~7.1.2.5.の内容の検証プロセスはこれまでの項で定められている認識。本項では結果について記録を残しておくことが目的。

7.1.2.

Explanation of the requirement

The requirement is provided to ensure that a vehicle manufacturer's processes enable information regarding software updates, as defined in the sub-clauses below, to be recorded.

This requirement enables information to be made available to the registration authority should they request an audit of a manufacturer relating to software updates and establishes what information should be recorded for that requirement.

There may be cases where a vehicle system is regularly updated with the same type of update and the system being updated is not type approved. An example of this may be map data using the same data fields and formats via the same delivery method. To reduce repetition, in this instance, one could require that the information detailed below is recorded only once and it is stated that it holds true for that class of updates (which would need to be defined by the manufacturer). The logic of this would be to reduce the burden on manufacturers if they can demonstrate that such a regular series of updates would exist.

本要件は、車両メーカーのプロセスによって、ソフトウェア更新に関する情報（以下の下位の項に定義）を記録することができることを保証するために定められている。

本要件によって、登録当局がソフトウェア更新に関連してメーカーの監査を要請した場合に、かかる当局に対して情報が利用可能な状態になり、かつ本要件は、当該要件についてどのような情報を記録すべきものを定めるものである。

車両システムが同じ種類の更新で定期的に更新され、更新中のシステムが型式認可を受けていない場合がある。同じ提供方法を介して同じデータフィールドおよびフォーマットを用いるマップデータが、この例である場合がある。この場合、繰り返しを削減するために、下記に詳述する情報を1回だけ記録し、当該クラスの更新（これはメーカーが定義する必要がある）については本情報が該当すると記載するように要求することができる。更新のかかる定期的なシリーズが存在することをメーカーが証明することができた場合には、メーカーの負担を低減することがこの論理である。

7.1.2.

The following clarification should be noted

'Each update' refers to every update (both type approved and non-type approved)

「各更新」とは、すべての更新（型式認可済み、型式認可を受けていないものの両方）を指す

'Vehicle type' is intended such that information is recorded for a given vehicle type and not for each vehicle

「車両型式」は、各車両ではなく任意の車両型式について情報を記録することを意図している

Examples of documents/evidence that could be provided

The requirement should be evidenced by the vehicle manufacturer demonstrating how they will/do record the information required below in the sub-clauses of 7.1.2. The information may be contained in (existing) configuration control management documentation.

本要件は、車両メーカーが下記7.1.2の下位の項で要求される情報をどのように記録する／しているかを車両メーカーが証明することによって証明すべきものとする。当該情報は、（既存の）構成管理マネジメント文書に含めてもよい。

7.1.2.1.

Documentation describing the processes used by the vehicle manufacturer for software updates and any relevant standards used to demonstrate their compliance;”

ソフトウェア更新について車両メーカーが使用するプロセス、およびその適合を証明するために使用する関連する基準について記載した文書、

解釈 (UN解釈文書における要件の説明)

本要件は、本規則に関連する車両メーカーのプロセスについて記載した文書を指し、車両メーカーがかかるプロセスを文書化することを要求している。

具体的な書面のイメージ

- 1) 上記書面に相当する書類のサンプル。

7.1.2.1.

Explanation of the requirement

This requirement refers to documents that describe the vehicle manufacturer's processes relevant to this Regulation and requires that the vehicle manufacturer documents them.

本要件は、本規則に関連する車両メーカーのプロセスについて記載した文書を指し、車両メーカーがかかるプロセスを文書化することを要求している。

Examples of documents/evidence that could be provided

Documentation of the processes listed in paragraph 7.1.1 and its sub-clauses and a description of how these are applied to individual vehicle types.

7.1.1項およびその下位の項に記載されているプロセスの文書、ならびにこれらのプロセスが個別の車両型式にどう適用されるかの説明。

7.1.2.2.

Documentation describing the configuration of any relevant type approved systems before and after an update, this shall include unique identification for the type approved system's hardware and software (including software versions) and any relevant vehicle or system parameters;"

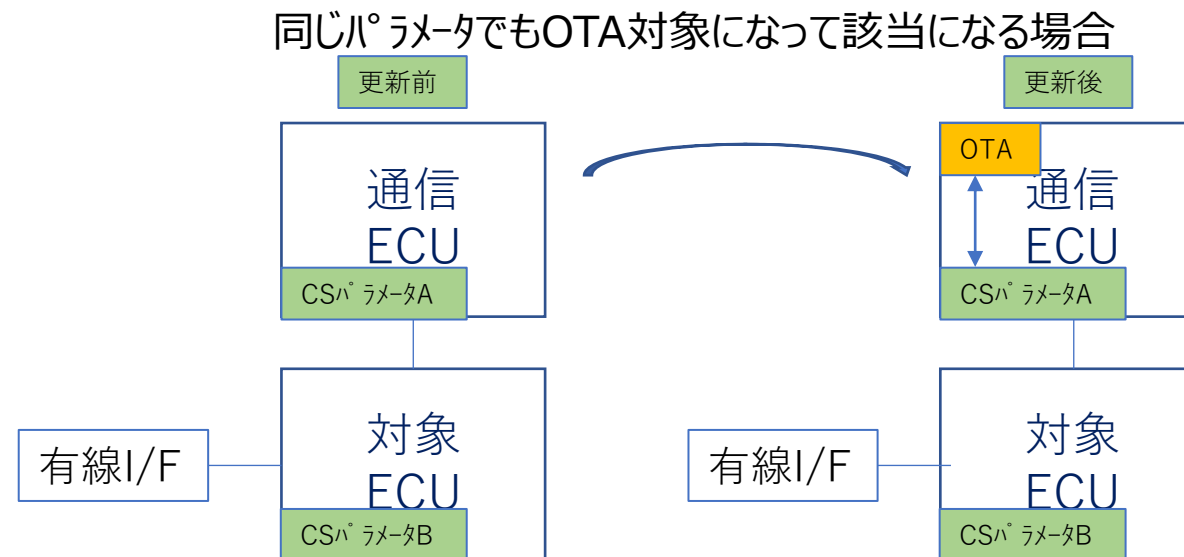
関連する型式認可済みシステムの更新前後の構成を説明する文書。これは、型式認可済みシステムのハードウェアおよびソフトウェア（ソフトウェアバージョンを含む）の固有識別、ならびに関連する車両またはシステムのパラメータを含むものとする、

解釈 (UN解釈文書における要件の説明)

本要件は、ソフトウェア更新に関連する車両システムのすべての構成を記録することができ、それが記録されるという保証を提供することができることを要求するものである。更新中の型式認可済みシステムは、ある範囲の以前の構成またはすべての以前のバージョンで構成されていてもよい。

具体的な書面のイメージ

1) 上記書面に相当する書類のサンプル。



7.1.2.2.

Explanation of the requirement

The requirement requires that all configurations of a vehicle system relating to a software update are able to be recorded and assurance can be provided that they will be recorded. The type approved systems being updated may comprise a range of previous configurations or all previous versions.

本要件は、ソフトウェア更新に関連する車両システムのすべての構成を記録することができ、それが記録されるという保証を提供することができることを要求するものである。更新中の型式認可済みシステムは、ある範囲の以前の構成またはすべての以前のバージョンで構成されていてもよい。

Examples of documents/evidence that could be provided

Configuration management processes may be used to evidence what the manufacturer will record. This should include the recording of:
(a) Any relevant vehicle or system parameters of the target update system before and after update;
(b) Hardware and software version numbers of the system being updated.

メーカーが何を記録するかを証明するために、構成管理プロセスを用いてもよい。これは、以下の記録を含むべきものとする：
(a) 更新対象システムの更新前後の関連する車両またはシステムのパラメータ、
(b) 更新中のシステムのハードウェアおよびソフトウェアバージョン番号。

7.1.2.3.

For every RXSWIN, there shall be an auditable register describing all the software relevant to the RXSWIN of the vehicle type before and after an update. This shall include information of the software versions and their integrity validation data for all relevant software for each RXSWIN.”

各RXSWINについて、更新前後の車両型式のRXSWINに関連するすべてのソフトウェアについて記載した監査可能なレジスターがあるものとする。これは、各RXSWINについて、すべての関連するソフトウェアのソフトウェアバージョンおよびその完全性検証データの情報を含むものとする。

解釈 (UN解釈文書における要件の説明)

完全性検証データは、適切な技能を有する者が、ソフトウェアが改ざんされていないことを検証することが可能であるようなものであるべきものとする。

具体的な書面のイメージ

- 1) 上記書面に相当する書類のサンプル。

7.1.2.3.

Explanation of the requirement

The integrity validation data should allow a suitably skilled person to verify that the software has not been manipulated.

完全性検証データは、適切な技能を有する者が、ソフトウェアが改ざんされていないことを検証することが可能であるようなものであるべきものとする。

The following clarification should be noted

‘Integrity validation data’ refers to the output of the method used for authentication of the software versions

「完全性検証データ」とは、ソフトウェアバージョンの認証に用いる方法のアウトプットを指す

‘Auditable register’ refers to a register that can be audited

「監査可能なレジスター」とは、監査することができるレジスターを指す

Examples of documents/evidence that could be provided

Configuration management processes may be used to evidence what the manufacturer will record. This should include evidencing the effectiveness of the processes for recording of:

メーカーが何を記録するかを証明するために、構成管理プロセスを用いてもよい。これは、以下を記録するプロセスの有効性の証明を含むべきものとする：

(a) For each RXSWIN:

(a) 各RXSWINについて：

(i) List of software relevant to the RXSWIN

(i) RXSWINに関連するソフトウェアのリスト

(j) Software version and integrity validation data of each piece of software before and after the update

(j) 更新前後の各ソフトウェアのソフトウェアバージョンおよび完全性検証データ

(b) How information regarding the RXSWIN is recorded. Information relating to an RXSWIN should include:

(b) RXSWINに関する情報の記録方法。RXSWINに関連する情報は以下を含むべきものとする：

(i) Description of the system/software functionality relevant to that RXSWIN;

(i) 当該RXSWINに関連するシステム／ソフトウェアの機能性の説明、

(ii) Regulations affected;

(ii) 影響を受ける規則、

(iii) Software relevant to the RXSWIN;

(iii) RXSWINに関連するソフトウェア、

(iv) Integrity validation data of the software relevant to the RXSWIN;

(iv) RXSWINに関連するソフトウェアの完全性検証データ、

(v) Method used for generating the integrity validation data.

(v) 完全性検証データの生成に使用した方法。

How information regarding an update that is relevant to an RXSWIN is recorded, this should include:

RXSWINに関連する更新についての情報の記録方法。これは、以下を含むべきものとする：

(i) List of RXSWINS affected by the software update

(i) ソフトウェア更新の影響を受けるRXSWINのリスト

7.1.2.4.

Documentation listing target vehicles for the update and confirmation of the compatibility of the last known configuration of those vehicles with the update.”

更新の対象車両を記載した文書、およびかかる車両の最新の既知構成と更新との適合性の確認。

解釈 (UN解釈文書における要件の説明)

対象車両の情報は、登録車両のVINレベルで利用可能であるべきものとする。
適合性が確保されているという確認は、個別車両ではなく車両のグループについて提供することができる。

具体的な書面のイメージ

- 1) 上記書面に相当する書類のサンプル。

7.1.2.4.

Explanation of the requirement

Information on target vehicles should be available on the VIN-level for registered vehicles.

対象車両の情報は、登録車両のVINレベルで利用可能であるべきものとする。

Confirmation that compatibility is ensured can be provided for a group of vehicles rather than individual vehicles.

適合性が確保されているという確認は、個別車両ではなく車両のグループについて提供することができる。

The following clarification should be noted

‘Target vehicles’ refers to the vehicles targeted for the software update

「対象車両」とは、ソフトウェア更新の対象になる車両を指す

‘Last known configuration’ refers to the fact that the vehicle manufacturer may not know the actual configuration of every vehicle of a vehicle type in the field, for example if it has been modified by its owner or a mechanic

「最新の既知構成」とは、例えば、その所有者または整備士が変更した場合など、車両メーカーが実地での車両型式の各車両の実際の構成を知らない可能性があるという事実を指す

Examples of documents/evidence that could be provided

Configuration management processes may be used to evidence what the manufacturer will record. This should include evidencing the effectiveness of the processes for:

メーカーが何を記録するかを証明するために、構成管理プロセスを用いてもよい。これは、以下のプロセスの有効性の証明を含むべきものとする：

- (a) Identification of target vehicles for the update
- (b) Checking the compatibility of the last known configuration of the target vehicles with the software update

- (a) 更新の対象車両の特定
- (b) 対象車両の最新の既知構成とソフトウェア更新との適合性の確認

7.1.2.5.

Documentation for all software updates for that vehicle type describing:

- (a) The purpose of the update;
- (b) What systems or functions of the vehicle the update may affect;
- (c) Which of these are type approved (if any);
- (d) If applicable, whether the software update affects the fulfilment of any of the relevant requirements of those type approved system;
- (e) Whether the software update affects any system type approval parameter;
- (f) Whether an approval for the update was sought from an approval body;
- (g) How the update may be executed and under what conditions;
- (h) Confirmation that the software update will be conducted safely and securely.
- (i) Confirmation that the software update has undergone and successfully passed verification and validation procedures.

当該車両型式のすべてのソフトウェア更新について、以下を記載する文書：

- (a) 更新の目的、
- (b) 更新が影響を与える可能性のある車両のシステムまたは機能、
- (c) これらのうち型式認可を受けているもの（ある場合）、
- (d) 該当する場合は、ソフトウェア更新が当該型式認可済みシステムの該当する要件への適合に影響を与えるかどうか、
- (e) ソフトウェア更新がシステムの型式認可パラメータに影響を与えるかどうか、
- (f) 更新の承認は認可機関の依頼かどうか、
- (g) 更新をどのような条件下でどのように実行すればよいか、
- (h) ソフトウェア更新が安全かつセキュアな方法で実施されるという確認。
- (i) ソフトウェア更新が実施され、検証および妥当性確認手順が問題なく終了したことの確認。

解釈 (UN解釈文書における要件の説明)

複数の目的を持つ更新または同じ目的の複数の更新（該当する場合）については、情報をまとめてもよい。車両システムが同じ種類の更新で定期的に更新され、更新中のシステムが型式認可を受けていない場合がある。同じ提供方法を介して同じデータフィールドおよびフォーマットを用いるマップデータが、この例である場合がある。この場合、繰り返しを削減するために、下記に詳述する情報を1回だけ記録し、当該クラスの更新（これはメーカーが定義する必要がある）については本情報が該当すると記載するように要求することができる。更新のかかる定期的なシリーズが存在することをメーカーが証明することができた場合には、メーカーの負担を低減することがこの論理である。

具体的な書面のイメージ

- 1) 規則で定められた1～9までの情報が記載されるべき書面サンプルの提示。
項目が多いので、これらが1ファイルになっていない場合はツリー構造的な書面を提示いただく必要がある場合がある。

CSMSを取得しない場合(SUMS単独取得の場合) セキュリティに関する説明については“(補足1) セキュリティ要件の取り扱いについて”を参照のこと。

7.1.2.5.

Explanation of the requirement

Information may be clustered for updates covering multiple purposes or multiple updates covering the same purpose (if appropriate). There may be cases where a vehicle system is regularly updated with the same type of update and the system being updated is not type approved. An example of this may be map data using the same data fields and formats via the same delivery method. To reduce repetition, in this instance, one could require that the information detailed below is recorded only once and it is stated that it holds true for that class of updates (which would need to be defined by the manufacturer). The logic of this would be to reduce the burden on manufacturers if they can demonstrate that such a regular series of updates would exist.

複数の目的を持つ更新または同じ目的の複数の更新（該当する場合）については、情報をまとめてもよい。車両システムが同じ種類の更新で定期的に更新され、更新中のシステムが型式認可を受けていない場合がある。同じ提供方法を介して同じデータフィールドおよびフォーマットを用いるマップデータが、この例である場合がある。この場合、繰り返しを削減するために、下記に詳述する情報を1回だけ記録し、当該クラスの更新（これはメーカーが定義する必要がある）については本情報が該当すると記載するように要求することができる。更新のかかる定期的なシリーズが存在することをメーカーが証明することができた場合には、メーカーの負担を低減することがこの論理である。

Examples of documents/evidence that could be provided

Evidence should be provided by demonstrating the processes used to record the information. If the processes have already been used then the output of the processes (the resultant documentation) could be shown to demonstrate them.

証拠は、情報を記録するために用いたプロセスを証明することによって提供すべきものとする。当該プロセスがすでに使用されている場合には、それを証明するために、プロセスのアウトプット（結果となる文書）を提示することができる。

(a) The purpose of the update;

(a) 更新の目的、

No guidance included in this document with regards this requirement

-

-

7.1.2.5.

(b) What systems or functions of the vehicle the update may affect;
更新が影響を与える可能性のある車両のシステムまたは機能、

Explanation of the requirement

The intent is for the vehicle manufacturer to describe the target system or function for the update, e.g. braking system, radio and any other systems or functions that may be affected by the update.

意図は、車両メーカーが、更新の対象システムまたは機能（例えば制動システム、無線および更新による影響を受ける可能性のあるその他のシステムまたは機能）について記載することである。

(c) Which of these are type approved (if any);
これらのうち型式認可を受けているもの（ある場合）、

No guidance included in this document with regards this requirement

-

-

(d) If applicable, whether the software update affects the fulfilment of any of the relevant requirements of those type approved system;
該当する場合は、ソフトウェア更新が当該型式認可済みシステムの該当する要件への適合に影響を与えるかどうか、

Explanation of the requirement

This requires the manufacturer to record the output of the processes described in paragraph 7.1.1.8 (the two requirements are linked).

本要件は、メーカーに7.1.1.8項で記載したプロセスのアウトプットを記録するよう要求するものである（2つの要件が関連している）。

The justification / reasoning for the decisions should be recorded together with the outcome (to allow verification at audit should that be required by a Technical Service or Approval Authority).

決定の根拠／理由を結果とともに記録すべきものとする（それによって、技術機関または認可当局から要求があった場合に監査において検証ができるようにする）。

7.1.2.5.

(e) Whether the software update affects any system type approval parameter;
ソフトウェアの更新がシステム型式承認パラメーターに影響するかどうか。

Explanation of the requirement

This requirement should consider the relevant test used for the affected type approval(s) and whether the software update might affect or change the outcome of that test under the conditions in which it was conducted

本要件は、影響を受けた型式認可に使用された関連するテスト、およびソフトウェア更新が、テストが実施された条件において、当該テストの結果に影響を与える、あるいはかかる結果を変える可能性があるかどうかを考慮すべきものとする。

The justification / reasoning for the decisions should be recorded together with the outcome (to allow verification at audit should that be required by a Technical Service or Approval Authority).

決定の根拠／理由を結果とともに記録すべきものとする（それによって、技術機関または認可当局から要求があった場合に監査において検証ができるようにする）。

The following clarification should be noted

‘Software update’ refers to the definition in 2.9

「ソフトウェア更新」とは、2.9の定義を指す

‘Any system type approval parameter’ refers to any parameters defined within any affected type approval regulation(s)

「システムの型式認可パラメータ」とは、影響を受ける型式認可規則内で定義されているパラメータを指す

(f) Whether an approval for the update was sought from an approval body;
更新の承認は認可機関の依頼かどうか、

No guidance included in this document with regards this requirement

-

-

7.1.2.5.

(g) How the update may be executed and under what conditions;
更新をどのような条件下でどのように実行すればよいか、

The following clarification should be noted

‘Conditions’ refers to any criteria needed to execute an update

「条件」とは、更新を実行するために必要な基準を指す

If new hardware is necessary for the update, this should be mentioned in the conditions under this requirement

更新に新規のハードウェアが必要な場合、これを本要件に基づく条件の中に記載すべきものとする

Examples of documents/evidence that could be provided

The manufacture may use the release notes for the software update to fulfil this requirement. The release note should contain the following information (but are not limited to):

- (a) Conditions that define a safe state for the update to be executed;
- (b) Actions required from the vehicle user / a competent person (if needed) before an update is installed.

メーカーは、本要件を満たすためにソフトウェア更新のリリースノートを使用してもよい。リリースノートは、以下の情報を含むべきものとする（が、これだけに限定されない）：

- (a) 更新を実行するための安全な状態を定義する条件、
- (b) 更新をインストールする前に、車両ユーザー／有資格者（必要な場合）に要求される行動。

(h) Confirmation that the software update will be conducted safely and securely.
ソフトウェア更新が安全かつセキュアな方法で実施されるという確認。

Explanation of the requirement

The information provided should contain details on why the conditions from clause g) lead to a safe and secure software update (justification) and how they will be met (verification).

提供する情報は、(g)項の条件が安全でセキュアなソフトウェア更新につながる理由（根拠）、および当該条件を満たす方法（検証）の詳細を含むべきものとする。

7.1.2.5.

(i) Confirmation that the software update has undergone and successfully passed verification and validation procedures.

ソフトウェア更新が実施され、検証および妥当性確認手順が問題なく終了したことの確認。

Explanation of the requirement

The purpose of verification and validation is to ensure that the software update works as intended. The method(s) used should be appropriate to the software update.

検証および妥当性確認の目的は、ソフトウェア更新が意図したとおりに作用することを保証することである。用いられる方法は、ソフトウェア更新に適したものであるべきものとする。

The following clarification should be noted

‘Adequate’ refers to a level where the manufacturer is able to justify that what has been performed is sufficient for the purposes of verification and validation. This should be primarily determined by the manufacturer and may be confirmed by a Technical Service/Approval Authority (upon audit for example)

「適切な」とは、実施されたことが検証および妥当性確認の目的において十分であることをメーカーが正当化することができるレベルを指す。これは主にメーカーが決定すべきものであり、（例えば監査時に）技術機関／認可当局が確認してもよい

‘Update’ refers to installation & execution

「更新」とは、インストールと実行を指す

Examples of documents/evidence that could be provided

The processes use for ensuring software updates undergo verification and validation to a level that the manufacturer is satisfied with and how this will be recorded.

ソフトウェア更新について、メーカーが満足するレベルで検証および妥当性確認が実施され、それを記録する方法を保証するために使用するプロセス。

- 7.1.3.
Security, the vehicle manufacturer shall demonstrate:
セキュリティ。車両メーカーは以下を証明するものとする：
- 7.1.3.1.
The process they will use to ensure that software updates will be protected to reasonably prevent manipulation before the update process is initiated;
更新プロセスが開始する前に、合理的に改ざんを防止する目的でソフトウェア更新が保護されることを保証するために車両メーカーが使用するプロセス、

解釈 (UN解釈文書における要件の説明)

本要件は、提供される予定のソフトウェア更新の完全性および真正性を保証するためのプロセスに対処するものである。車両メーカーが、どの更新が車両に送られるかを制御し、既知で有効な更新のみが車両に送られることを保証するプロセスがあるという根拠を技術機関／認可当局に対して示すことができる、というのがその結果であるべきものとする。これは、車両に提供するためにサプライヤーからメーカーに提供された更新を保護するプロセスを含んでいてもよい。

具体的な書面のイメージ

- ・ CSMSの参照（有効期限内のCOC適合証明書の提示）

但し、CSMS取得時において以下マニュアルの7.2.2.2.項に基いた説明がされていること。

審査マニュアル

- ・ CS能力審査マニュアル 2021年1月22日施行版
- ・ CS型式審査マニュアル 2021年1月22日施行版

7.1.3.1.

Explanation of the requirement

This requirement addresses processes for ensuring the integrity and authenticity of the software updates that are to be delivered. The outcome should be that a vehicle manufacturer can justify to a Technical Service/Approval Authority that they have processes in place for controlling what updates are sent to a vehicle and for ensuring that only known and valid updates are sent to vehicles. This may include processes for securing updates provided to them by suppliers for delivery to a vehicle.

本要件は、提供される予定のソフトウェア更新の完全性および真正性を保証するためのプロセスに対処するものである。車両メーカーが、どの更新が車両に送られるかを制御し、既知で有効な更新のみが車両に送られることを保証するプロセスがあるという根拠を技術機関／認可当局に対して示すことができる、というのがその結果であるべきものとする。これは、車両に提供するためにサプライヤーからメーカーに提供された更新を保護するプロセスを含んでいてもよい。

The following clarification should be noted

‘Manipulation’ refers to changes or interference in the software code of the update that is not authorised by the originator(s) of the update

「改ざん」とは、更新の作成者によって権限を与えられていない更新のソフトウェアコードの変更または介入を指す

The test of “reasonable” should be that the manufacturer can argue through claims, arguments and evidence that the process employed is sufficient to meet the threat

メーカーが主張、論拠および証拠を介して、使用されたプロセスが脅威に対応するのに十分であると主張することができる、というのが「合理的」のテストであるべきものとする。

Examples of documents/evidence that could be provided

Standards that might be applicable include: ISO/SAE 21434

適用される可能性のある基準には以下が含まれる：ISO/SAE 21434

The Cyber Security Management System may be used to evidence this requirement. The vehicle manufacturer should explain how it does this.

本要件を証明するために、サイバーセキュリティ管理システムを用いてもよい。車両メーカーは、当該システムがどのようにこれを実行するかを説明すべきものとする。

The cyber security regulation may be used as a reference.

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。

Demonstration of the manufacturers processes may be provided as evidence. This may include a description of any integrity checking mechanism for software updates during their download and execution stage. This should provide proof of authenticity if it demonstrates that the sourced software update is same as the one sent to the vehicle.

メーカーのプロセスの証明を証拠として提供してもよい。これは、ダウンロードと実行の段階におけるソフトウェア更新の完全性確認メカニズムの説明を含んでいてもよい。これによって、元になるソフトウェア更新が車両に送られたものと同じであることを証明すれば、真正性の証拠を提供したことになるはずである。

7.1.3.2.

The update processes used are protected to reasonably prevent them being compromised, including development of the update delivery system;

使用された更新プロセスが危殆化されることを合理的に防ぐ目的で保護されている（更新提供システムの開発を含む）、

解釈 (UN解釈文書における要件の説明)

本要件は、不正な更新を提供する目的でソフトウェア更新を危殆化することができないことを保証するために、ソフトウェア更新を提供するプロセスに対処するものである。車両メーカーが、不正な更新を提供する目的で更新メカニズムを改ざんすることができないことを保証するプロセスがあるという根拠を技術機関／認可当局に対して示すことができる、というのがその結果であるべきものとする。

具体的な書面のイメージ

- 1) CSMSの参照（有効期限内のCOC適合証明書の提示）
- 2) 申請者がCS規則の適用を受けない場合は、SUに関してCSMSと同様の審査を実施。

7.1.3.2.

Explanation of the requirement	
<p>This requirement addresses the processes for delivering software updates to ensure they cannot be compromised to deliver unauthorized updates. The outcome should be that a vehicle manufacturer can justify to a Technical Service/Approval Authority that they have processes in place for ensuring that the update mechanism cannot be manipulated to provide unauthorised updates.</p>	<p>本要件は、不正な更新を提供する目的でソフトウェア更新を危殆化することができないことを保証するために、ソフトウェア更新を提供するプロセスに対処するものである。車両メーカーが、不正な更新を提供する目的で更新メカニズムを改ざんすることができないことを保証するプロセスがあるという根拠を技術機関／認可当局に対して示すことができる、というのがその結果であるべきものとする。</p>
The following clarification should be noted	
<p>‘Development’ refers to processes employed during the creation of the update system to build in security by design</p>	<p>「開発」とは、設計によってセキュリティを埋め込むために、更新システムの作成中に使用されたプロセスを指す</p>
<p>‘Update system’ refers to the system created to deliver updates</p>	<p>「更新システム」とは、更新を提供するために作成されたシステムを指す</p>
Examples of documents/evidence that could be provided	
<p>The Cyber Security Management System may be used to evidence this requirement. The vehicle manufacturer should explain how it does this.</p>	<p>本要件を証明するために、サイバーセキュリティ管理システムを用いてもよい。車両メーカーは、当該システムがどのようにこれを実行するかを説明すべきものとする。</p>
<p>The cyber security regulation may be used as a reference.</p>	<p>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。</p>
<p>Demonstration of the security processes applied to the software update process.</p>	<p>ソフトウェア更新プロセスに提供されたセキュリティプロセスの証明。</p>

7.1.3.3.

The processes used to verify and validate software functionality and code for the software used in the vehicle are appropriate.

車両で使用されているソフトウェアについて、ソフトウェアの機能性およびコードが適切であることを検証および確認するために使用されるプロセス。

解釈 (UN解釈文書における要件の説明)

本要件の意図は、適切にテストされたソフトウェア更新だけが車両に送られるようなプロセスがあることを保証することである。要求されるプロセスは、ソフトウェア更新におけるエラーのバグ修正を最小限にすることを目指すべきものとする。

本要件は、7.1.2.5項(i)に関連している。7.1.3.3項は、プロセスの確認を要求している。7.1.2.5項は、それらがソフトウェア更新に適用されたことを示す文書を要求している。

具体的な書面のイメージ

1) 組織図

評価、特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。

(想定は対象の業務G r までが確認できるもの)

2) 業務フロー図

3) 業務処理手準書

4) ソフトウェアの機能性およびコードの検証方法。

5) 検証結果のサンプル。

7.1.3.3.

Explanation of the requirement

The intention of this requirement is to ensure there are processes in place so that only properly tested software updates are sent to the vehicle. The processes required should aim to minimise bug-fixing of errors in software update.

本要件の意図は、適切にテストされたソフトウェア更新だけが車両に送られるようなプロセスがあることを保証することである。要求されるプロセスは、ソフトウェア更新におけるエラーのバグ修正を最小限にすることを目指すべきものとする。

This requirement is linked to paragraph 7.1.2.5. part i). Paragraph 7.1.3.3. requires confirmation of the processes. Paragraph 7.1.2.5. requires documentation that they have been applied to software updates.

本要件は、7.1.2.5項(i)に関連している。7.1.3.3項は、プロセスの確認を要求している。7.1.2.5項は、それらがソフトウェア更新に適用されたことを示す文書を要求している。

The following clarification should be noted

'Appropriate' refers to the use of processes which meet a justifiable level of expectation

「適切である」とは、正当と認められるレベルの期待を満たすプロセスの使用を指す

Examples of documents/evidence that could be provided

The manufacturer should be able to provide an argument, based on claims and evidence, that the processes they employ are appropriate. These may refer to standards and best practice.

メーカーは、主張および証拠に基づいて、使用するプロセスが適切であることの論拠を提供することができるべきものとする。これらは、基準およびベストプラクティスを指してもよい。

7.1.4.

Additional Requirements for Software Updates over the air

Over the Airソフトウェア更新に関する追加要件

7.1.4.1.

The vehicle manufacturer shall demonstrate the processes and procedures they will use to assess that over the air updates will not impact safety, if conducted during driving.

車両メーカーは、Over the Air更新が運転中に実施された場合でも安全性に影響を与えないことを評価するために使用するプロセスおよび手順を証明するものとする。

解釈 (UN解釈文書における要件の説明)

車両メーカーが、プロセスが本要件を満たすという合理的な論拠を提供することができる、というのがこのプロセスの結果であるべきものとする。

これらのプロセスの結果を、7.1.2.5項に記載するとおりに記録すべきものとする

具体的な書面のイメージ

1) 組織図

評価、特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。

(想定は対象の業務G rまでが確認できるもの)

2) 業務フロー図

3) 業務手順書

4) 安全性への影響の評価結果のサンプル

※ メーカーとして運転中にOTA更新を実施しない場合は”運転中に更新される仕様がないことを再確認するプロセス”があることを確認することとしたい。

7.1.4.1.

Explanation of the requirement	
The outcome of this process should be that vehicle manufacturers are able to provide a reasoned argument that their processes fulfil this requirement.	車両メーカーが、プロセスが本要件を満たすという合理的な論拠を提供することができる、というのがこのプロセスの結果であるべきものとする。
The outcome of these processes should be recorded as described in paragraph 7.1.2.5.	これらのプロセスの結果を、7.1.2.5項に記載するとおりに記録すべきものとする
Examples of documents/evidence that could be provided	
Manufacturers should provide details of the processes and criteria used for assessing whether updates may have an impact on safety while driving.	メーカーは、更新が運転中の安全性に影響を与える可能性があるかどうかを評価するために使用されるプロセスおよび基準の詳細を提供すべきものとする。

7.1.4.2.

The vehicle manufacturer shall demonstrate the processes and procedures they will use to ensure that, when an over the air update requires a specific skilled or complex action, for example recalibrate a sensor post-programming, in order to complete the update process, the update can only proceed when a person skilled to do that action is present or is in control of the process.”

車両メーカーは、Over the Air更新の更新プロセスを完了させるために、特定の技能または複雑な行動（例えば、センサのポストプログラミングの再キャリブレーション）が要求される場合に、かかる行動をする技能を有する者がその場にいるか、あるいはプロセスを制御できる状態にある場合に限り更新を進めることができることを保証するために使用するプロセスおよび手順を証明するものとする。

解釈 (UN解釈文書における要件の説明)

本要件の意図は、ソフトウェア更新を開始または完了するために、車両の所有者が技術的なこと、あるいは複雑なことをすることは一切要求されないことを保証することである。本要件は、これを管理するプロセスをメーカーが確立するよう規定している。更新が複雑な行動を要求する可能性がある場合は、適切な技能を有するか、もしくは訓練を受けた者がその場にいるか、あるいは遠隔で実施される場合にはプロセスを制御できる状態にある場合に限り、かかる更新が実施されることを保証するプロセスが必要である。

これらのプロセスの結果を、7.1.2.5項に記載するとおりに記録すべきものとする

具体的な書面のイメージ

1) 組織図

評価、特定プロセスにおいて、業務手順書を用いて実業務を行う単位部署までの確認が可能なもの。

(想定は対象の業務G r までが確認できるもの)

2) 業務フロー図

3) 業務手順書

特殊技能者の認定方法を含むこと。

7.1.4.2.

Explanation of the requirement

The intention of this requirement is to ensure that vehicle owners are not required to do anything technical or complex for a software update to be initiated or completed. The requirement specifies that manufacturers have established processes for managing this. Where an update may require complex action there needs to be a process to ensure such updates are only carried out when a suitable skilled or trained person is present, or is in control of the process when it is conducted remotely.

The outcome of these processes should be recorded as described in paragraph 7.1.2.5.

本要件の意図は、ソフトウェア更新を開始または完了するために、車両の所有者が技術的なこと、あるいは複雑なことをすることは一切要求されないことを保証することである。本要件は、これを管理するプロセスをメーカーが確立するよう規定している。更新が複雑な行動を要求する可能性がある場合は、適切な技能を有するか、もしくは訓練を受けた者がその場にいるか、あるいは遠隔で実施される場合にはプロセスを制御できる状態にある場合に限り、かかる更新が実施されることを保証するプロセスが必要である。

これらのプロセスの結果を、7.1.2.5項に記載するとおりに記録すべきものとする

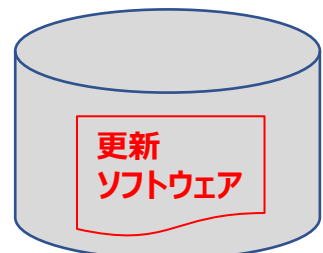
【OTA対応&有線対応時のセキュリティ対象配信経路】

更新ソフト開発~量産プロセス

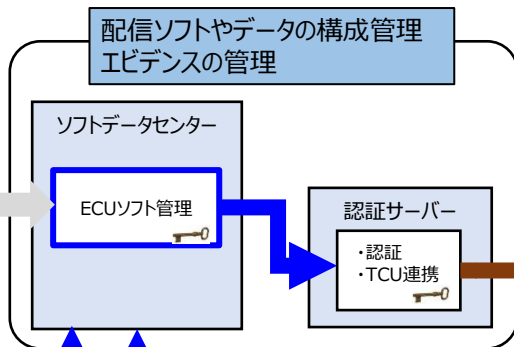
更新ソフト管理~配信プロセス

更新ソフト車両実装プロセス

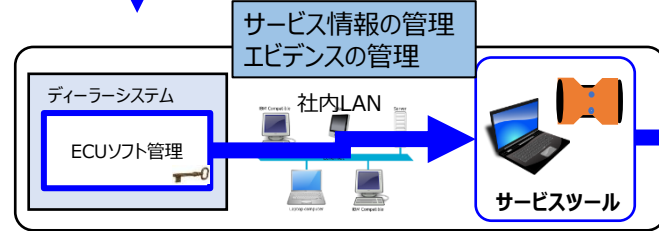
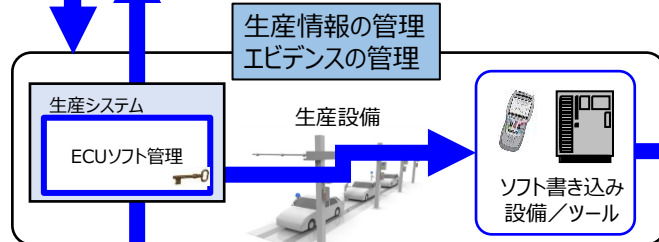
- 7.1.1.1 エビデンスをセキュアに保管
- 7.1.3.1 ソフトウェアの改ざん防止
- 7.1.3.2 更新プロセスの保護
- 7.1.3.3 ソフトウェアの機能性とコードの検証
- 7.1.2.5-8 更新が安全かつセキュアか検証



仕入れ先



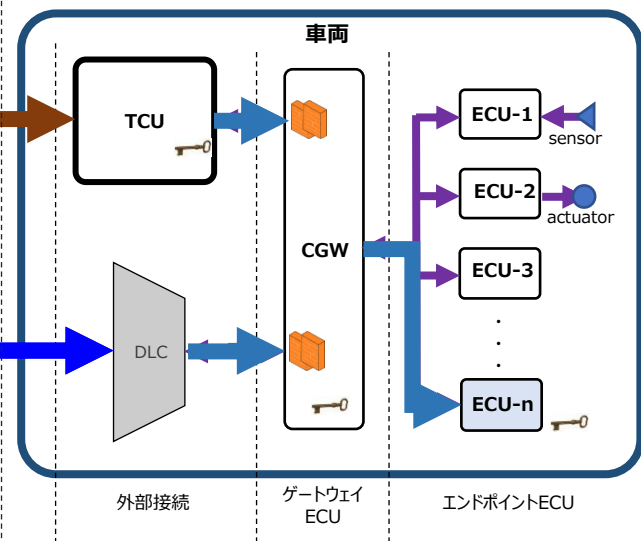
キャリア回線



一般事業者



- 7.2.1.1ソフトウェアの真正性、完全性の保護
- 7.2.1.2.3RxSWINの保護



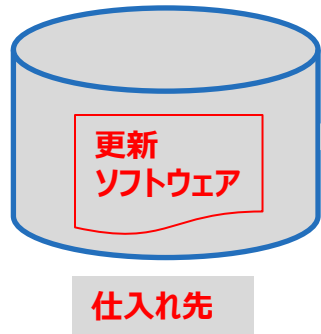
↔ : データの経路

ポイント：7.1章&7.2章いずれも、セキュリティは有線&OTAの「共通要件」にのみ定義】

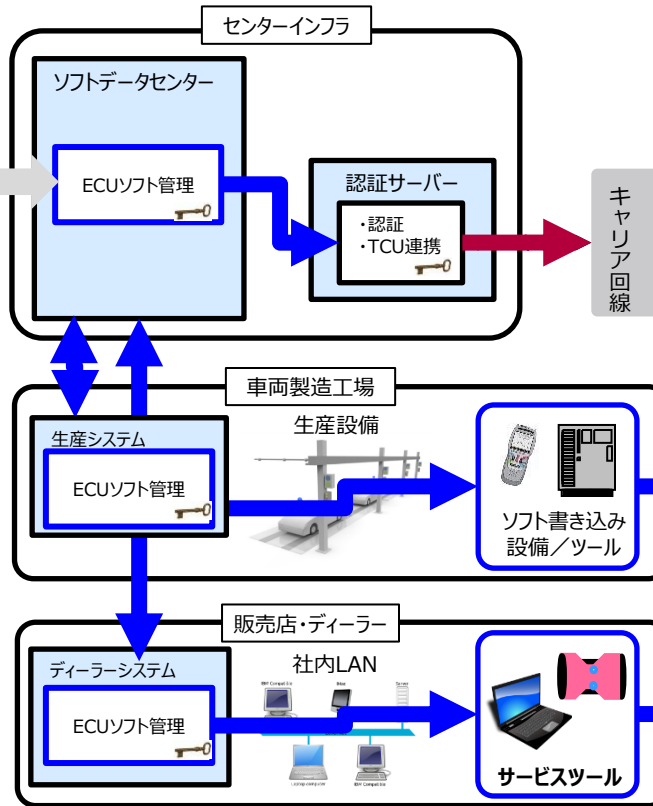
<u>SU法規</u>	<u>CS法規</u>	
<p>7.1 SUMSプロセス要件</p> <ul style="list-style-type: none">7.1.1.1 エビデンスをセキュアに保管7.1.3.1 ソフトウェアの改ざん防止7.1.3.2 更新プロセスの保護7.1.3.3 ソフトウェアの機能性とコードの検証7.1.2.5-8 更新が安全かつセキュアか検証	<p>7.2 CSMSプロセス要件</p> <ul style="list-style-type: none">7.2.2.1 Postproduction Phase7.2.2.2 CSMSによるCS性能の証明	<p>ANNEX5</p> <ul style="list-style-type: none">PartA 4.3.1PartA 4.3.3 更新手順に関わる脅威PartA 4.3.4PartA 4.3.5 外部接続及び接続部PartA 4.3.6PartA 4.3.7 潜在的脆弱性PartB 表B2 更新プロセスに関する脅威PartB 表B4 外部接続&接続部PartB 表B5 攻撃の潜在的標的PartB 表B6 潜在的脆弱性PartB 表B7 データ損失・漏洩PartB 表B8 物理的改ざんPartC 表C1 バックエンド
<p>7.2 型式要件</p> <ul style="list-style-type: none">7.2.1.1ソフトウェアの真正性、完全性の保護7.2.1.2.3RxSWINの保護	<p>7.3 型式要件</p> <ul style="list-style-type: none">7.3.3 車両型式の網羅的リスクアセス7.3.4 車両型式の保護7.3.5 車両型式上の専用環境の保護	

【OTA対応 & 有線対応時のセキュリティ対象配信経路】

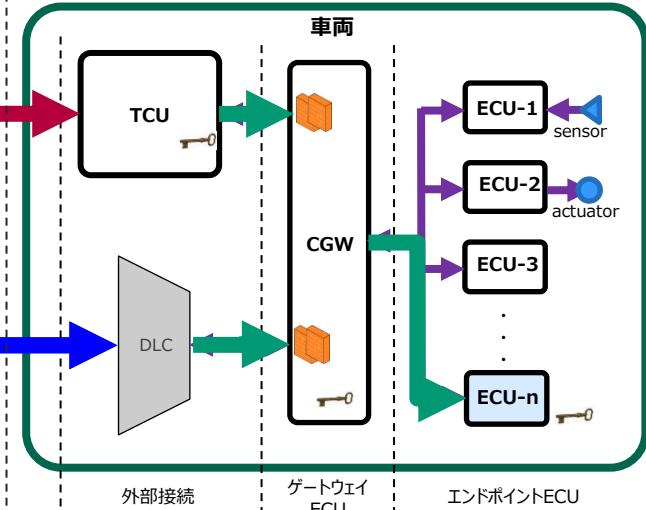
更新ソフト開発~量産プロセス



更新ソフト管理~配信プロセス



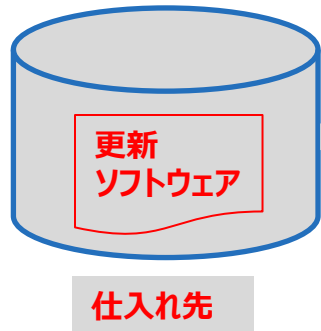
更新ソフト車両実装プロセス



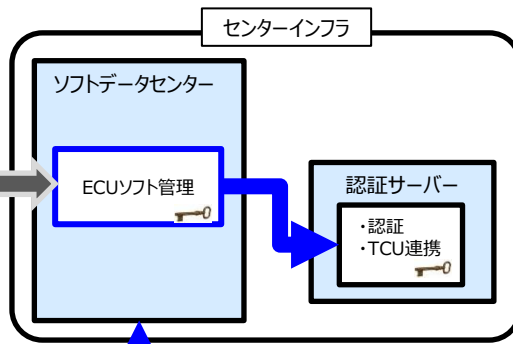
↔ : データの経路

【OTA未対応、有線のみ対応時のセキュリティ対象配信経路】

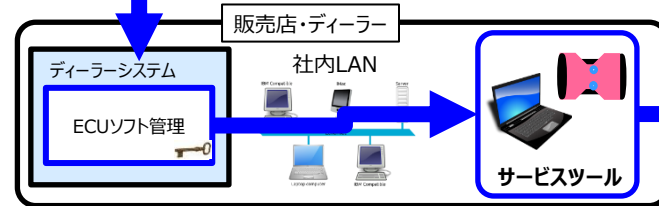
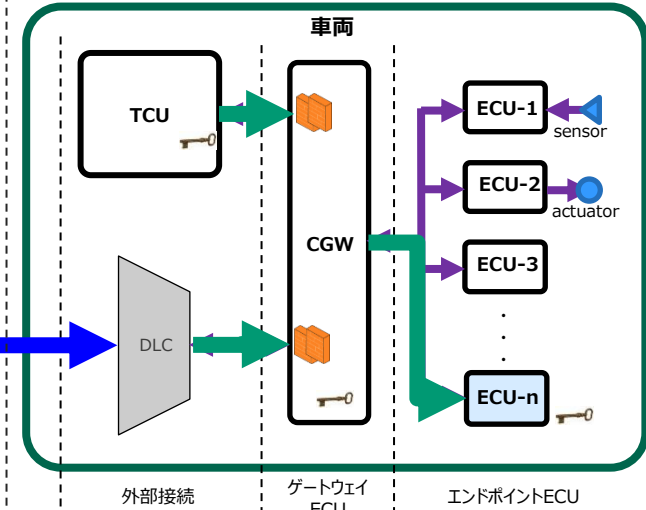
更新ソフト開発～量産プロセス



更新ソフト管理～配信プロセス



更新ソフト車両実装プロセス



↔ : データの経路