CS能力審査マニュアル
2021年1月22日施行版

・UN Regulation No. 155 on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security 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155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、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実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。

検討方針

１）目的

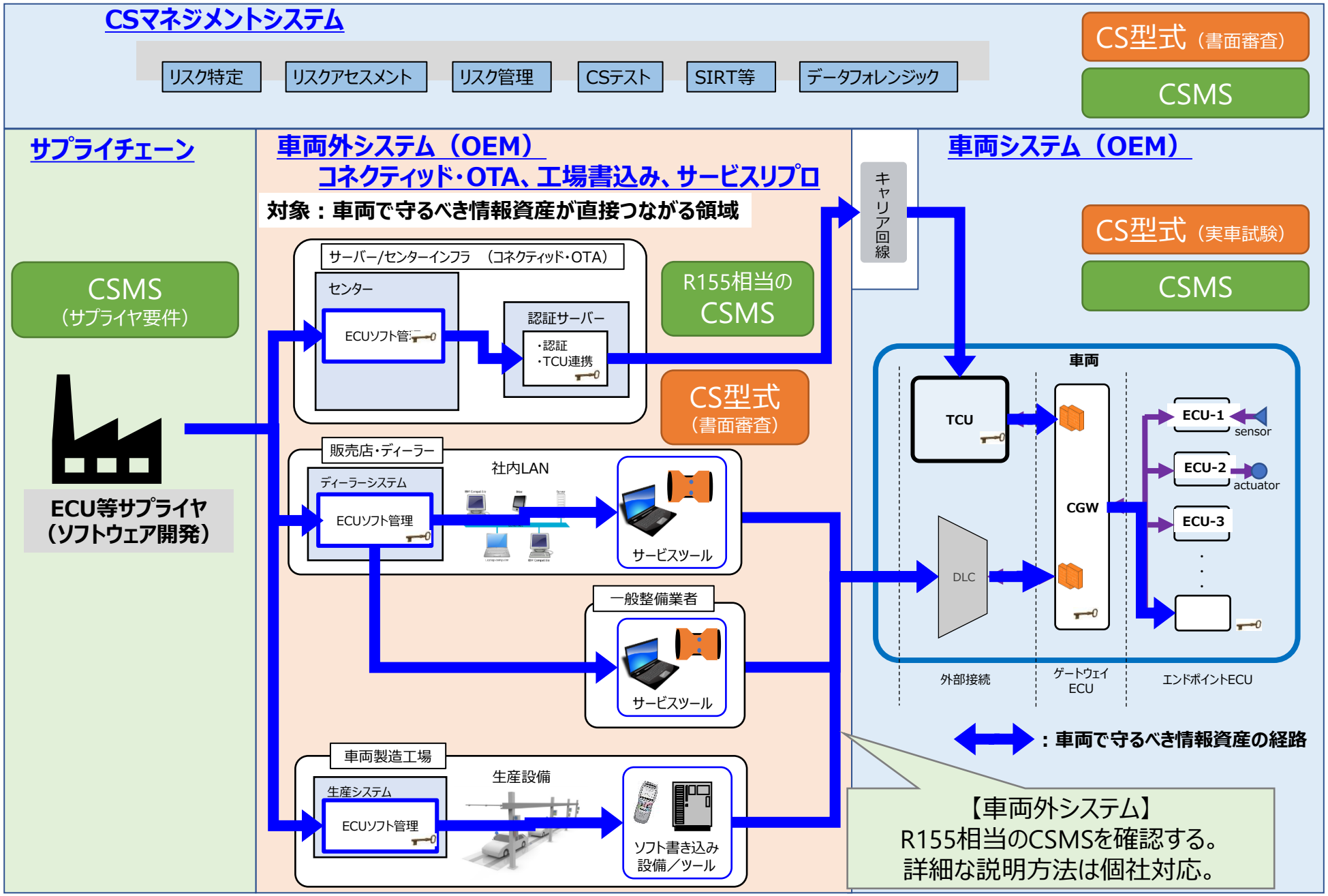
　解釈文書を参照して、審査時に確認するエビデンスおよび審査方法の明確化を目的とする。
（UNでのテストフェーズにならい、法文解釈の一義化ではなくエビデンスの明確化による審査レベルの安定化も考慮する）

２）検討根拠は以下の基準等とする。

- 協定規則第155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

（WP29-182-05e.docx）

R155におけるセキュリティ要件の説明範囲（R156におけるセキュリティ要件の説明範囲（配信経路の例）を含む）



7.2.2.2.
The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:
サイバーセキュリティ管理システム内で使用されるプロセスによってセキュリティが適切に考慮されていることを実証する。これには、以下の点が含まれるものとする

解釈

なし

提出文書

・なし
次項以降（7.2.2.2.(a)~(h)）にて説明のこと。

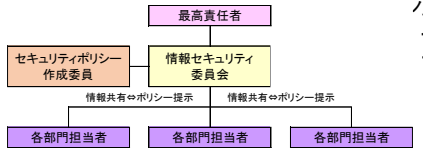
7.2.2.2.(a)
The processes used within the manufacturer's organization to manage cyber security;
サイバーセキュリティ管理のためにメーカーの組織内で使用するプロセス

解釈

「サイバーセキュリティを管理するためのプロセス」とは、2.2「車両と機能が脅威から保護されている状態」を組織として管理するためのプロセスのことである。すなわち、組織としてセキュリティへの取り組みがプロセス化している（組織規約、ルールとなっている状態）を説明する。

提出文書

社内管理体制を説明する資料（組織図）および社内規定の全体構成を説明する資料。
具体的には、
①社内管理体制（組織体制図、役割）
トップ→実務現場までセキュリティマネジメントが行き届いていること、および現場からのフィードバックを反映し社内管理体制やプロセスが定義され、そのプロセスの改善を推進および規定の遵守状況をチェックする役割を持つ部署を明示すること。（チェックに関しては監査部署を求めるものでは無く、担当部署が明確になっていればよい）



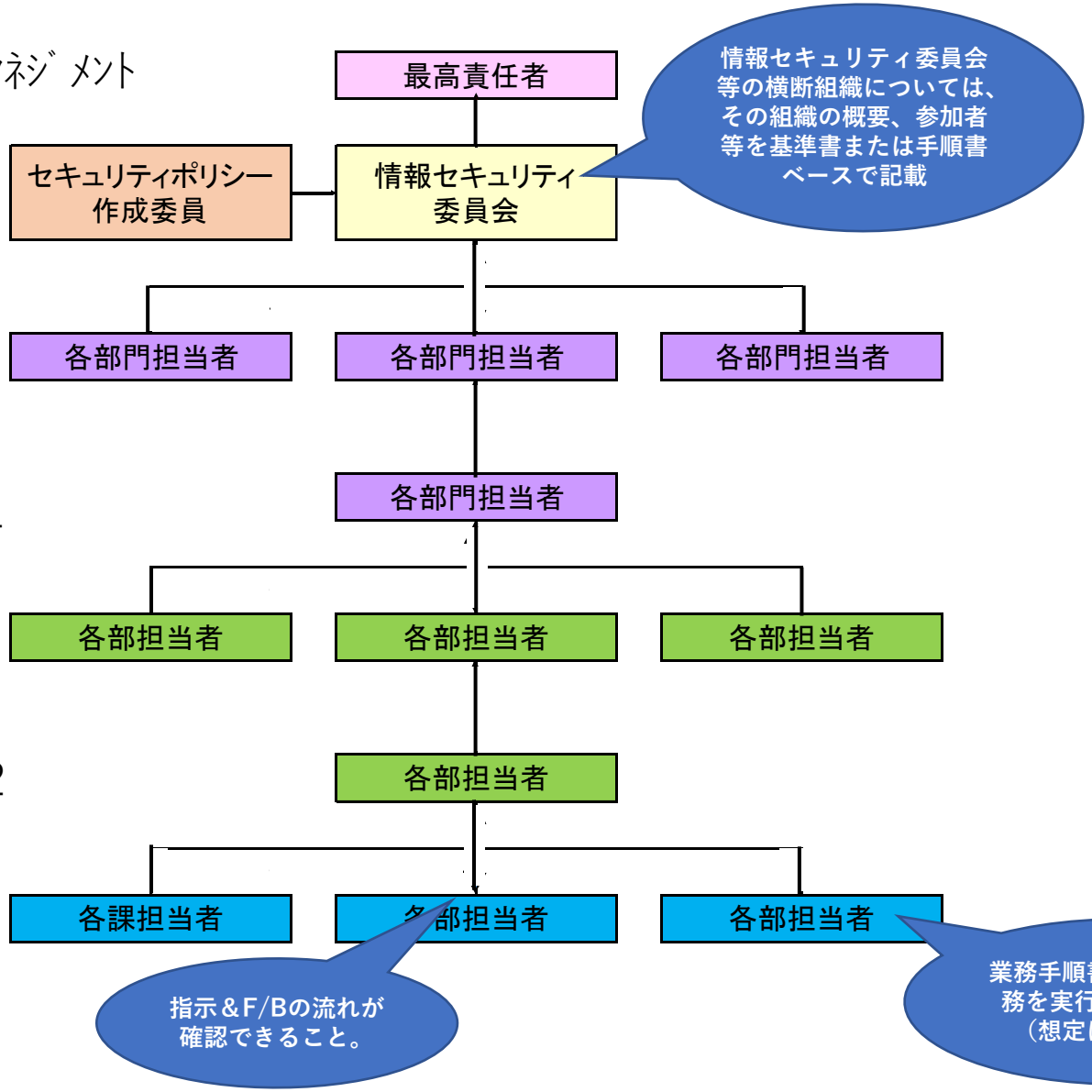
１）組織体系図（トップマネジメント）
メッシュ：トップ→部門毎までサイバーセキュリティ推進体制の概要が把握できること。
具体的にはトップマネジメントから各部門（各部）レベルまでのマネジメント経路および各部門のおおまかな役割、その責任者が把握できること。

２）組織体系図（レベル１）
メッシュ：部門長→各部毎まで上位で決定された方針を各部門内で具体的な業務に落とすまでの組織が把握できること。
具体的には、トップマネジメントで決定した部門毎ゴールに対し、関連部署がどう連携しているかを確認できること。
（組織図と業務フローを分けても良い。ただし、組織図と業務フローを実際に見てわからないところがあれば、追加で記載が必要。）

３）組織体系図（レベル２）
メッシュ：各部長→各課毎まで上位で決定された方針を各部内で具体的な業務に落とすまでの組織が把握できること。
具体的には、各部に落ちたゴールに対し、関連部署がどのように連携しているかを確認できること。

組織図のレベル感

トップマネジメント



一般的な例

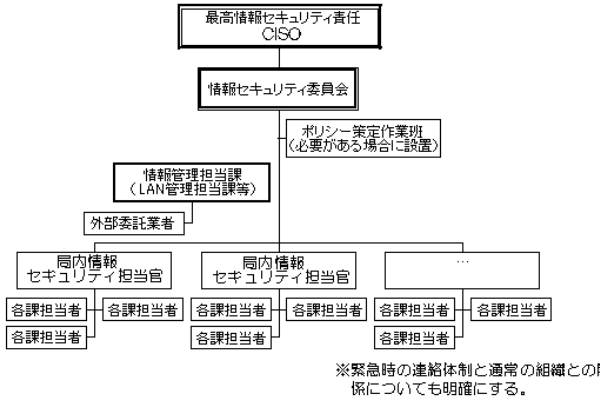
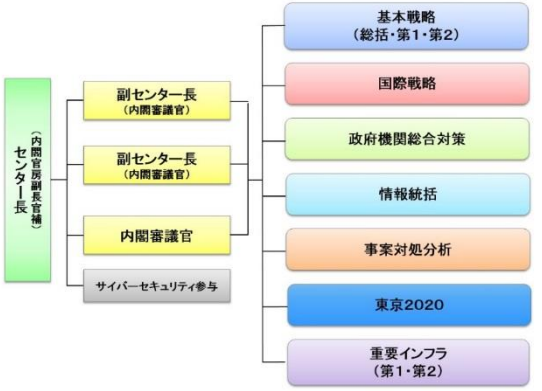
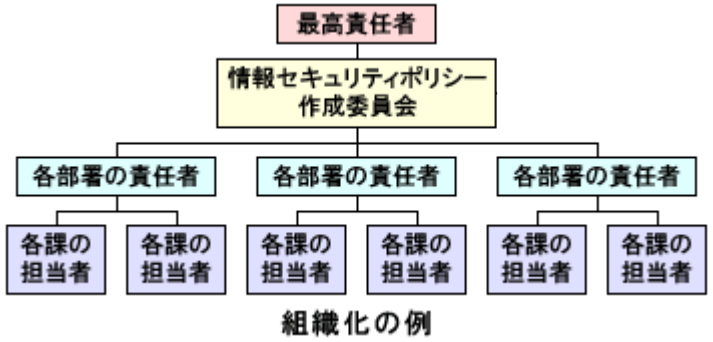


図６：組織図例

首相官邸HP



内閣サイバーセキュリティセンター



総務省HP

「矢印」「セキュリティポリシー、F/B」などは記載せず、トップマネジメントから部単位までの体制を示す。

組織図のレベル感

参考：COPに関する品質保証体系図の例

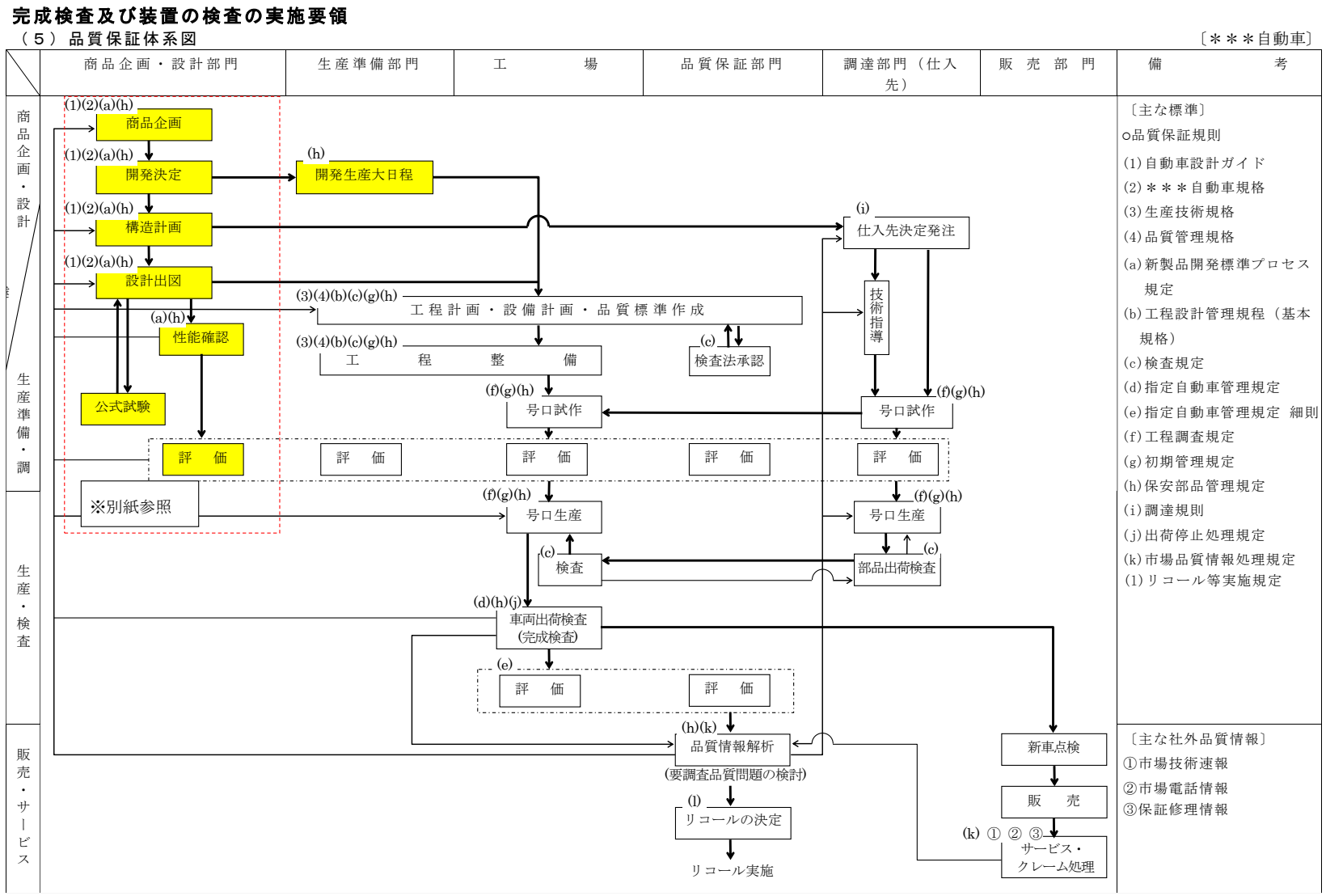
以下の理由からＣＯＣ審査の組織図としては、不適と考える。
（元来目的の違う資料であるため、流用は厳しい）

1）プロセス図であり組織図でない。

2）具体的にどの組織がどの業務を担当しているかが把握できない。
（メッシュが粗く業務手順書単位まで分解されていない？）

3）インシデントが発生した場合のＦ／Ｂ経路が把握できない。

※以降のプロセスを説明する資料の一部としては活用可能と考える。
（プロセスの概要説明として）



提出文書（つづき）

なお、組織図のレベル感としては品質保証体系図よりも細かいメッシュ感（セキュリティに関する各業務単位における
実行部署を特定できるレベル）を想定している。

<u>②社内規定全体図（セキュリティ関連規定：ポリシー、標準、プロシージャー）</u>
ポリシーを筆頭とした社内規定のヒエラルキーが確認できること。
　具体的には、基本方針→対策基準書→実施手順書の順で、それぞれの業務内容が社内基準として整備されていることが確認できれば良い。（実施手順とは実作業者の作業手順を具体的に記したものであること）

具体的な個々手順の内容は7.2.2.2. (b)以降で確認する。
ここでは規定類が設置され、管理（更新を含む）するプロセスが構築されているか？のみを確認する。

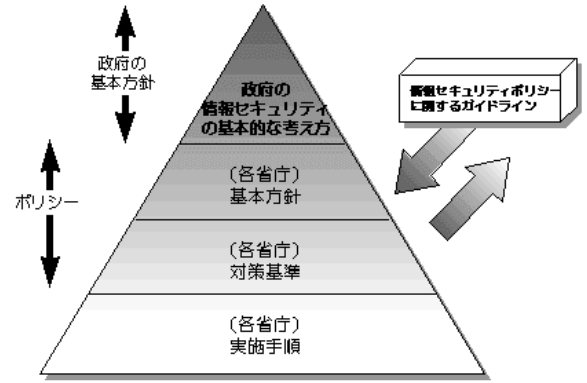


図2：ポリシーの位置づけ

関連規定のイメージ

各書面定義
①基本方針：
企業が取るべき行動を社内に展開するための文書。
基本方針の内容は、必ずしも社外に宣言するものではない（社外に宣言するのは、その中の基本理念や取組み姿勢）
②対策基準書：
「何を実施しなければならないか」を記述した文書。組織的に情報セキュリティ対策を行うためのルールで、適用範囲や対象者を明確にするもの。
③実施手順書（プロシージャー）：
作業マニュアル的な位置づけの文書、実作業者の作業手順を具体的に記したものであり、スキルに関係なく、本文書によって実務が遂行できる内容。（説明書、マニュアルなど）なお、担当部署が明記されていること。
但し、対策基準書と実施手順書が厳密に分けることは必須ではない。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (a)

Explanation of the requirement	
The aim of this requirement is to ensure that the organization has processes to manage the implementation of the CSMS. Its scope is limited to processes that are relevant for the cyber security of the vehicle types and not other aspects of the organization. For example, the scope of this requirement is not intended to cover the entire Information Security Management System of an organization. The following could be used to show the range of activities performed by the manufacturer to manage the cyber security of the development, production and post-production phases of a vehicle type: (a)Organizational structure used to address cyber security; (b)Roles and Responsibilities regarding cybersecurity management incl. accountability.	この要件の狙いは、CSMSの実施を管理するためのプロセスを当該組織が確実に有していることである。その適用範囲は、車両型式のサイバーセキュリティに関連するプロセスに限定され、当該組織のその他の側面は関係しない。例えば、この要件の適用範囲に組織の情報セキュリティ管理システム全体を含めることは意図されていない。 車両型式の開発、生産および生産後フェーズのサイバーセキュリティを管理するためにメーカーによって実施される活動の範囲を示すには、下記が使用できると考えられる： (a)サイバーセキュリティに対処するために使用する組織的構造、 (b)サイバーセキュリティ管理に関する役割および責任（説明責任を含む）。
Examples of documents/evidence that could be provided	
(c)ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-05-01], [RQ-05-02]. [RQ-05-07], [RQ-05-08]; (d)BSI PAS 1885 could be used to help evidence this requirement. National certification schemes, like the UK Cyber Essentials, could be used to evidence a manufacturer’s organizational processes.	(c)要求されている証明および評価の根拠としてISO/SAE 21434、特に[RQ-05-01]、[RQ-05-02]、[RQ-05-07]、[RQ-05-08]に基づく箇所を用いることができる。 (d)この要件の証拠に役立つものとして、BSI PAS 1885が使用できると考えられる。メーカーの組織的プロセスの証拠としては、UKサイバーエッセンシャルズのような国内認証制度が使用できると考えられる。

判断の目安（WP29解釈文書より引用）

7.2.2.2.における全ての書面が適切に提出されたことを確認したうえで、現地審査（インタビュー等）を含め総合的に基準への適合性を判断する。この際、以下の判断の目安については適合性判断の一助となるものであるが、これが判断基準の全てではない。（あくまで一例である）提出文書に不足があり内容を確認する上での適合性判断の参考として当該部分の追加提出を求める場合がある。
以降、“判断の目安”については同様に扱う。

7.2.2.2. (a)

The requirement should be considered unfulfilled if one of the following statements is true	
1.Processes are absent or incomplete. 2.Processes are not applied universally or consistently. 3.Processes are often or routinely circumvented to achieve business objectives. 4.The vehicle manufacturer’s security governance and risk management approach has no bearing on its processes. 5.System security is totally reliant on users' careful and consistent application of manual security processes. 6.Processes have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period. 7.Processes are not readily available to staff, too detailed to remember, or too hard to understand.	1.プロセスが欠如している、または不完全である。 2.プロセスの適用が普遍的でない、または一貫していない。 3.事業目標を達成するためにプロセスが頻繁にまたは定期的に回避されている。 4.車両メーカーのセキュリティガバナンスおよびリスク管理アプローチがそのプロセスに基づいていない。 5.システムセキュリティがユーザーによる注意深くかつ一貫したマニュアルセキュリティプロセスの適用に完全に依存している。 6.重大な変化（例えば、技術または規制の枠組み）に対応するものとして、または適切な期間内に、プロセスの見直しが行われていない。 7.プロセスが従業員にとって容易に使用できる状態にない、過度に詳細で覚えられない、または過度に難しくて理解できない。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (a)

The requirement may be considered fulfilled if all of the following statements are true	
1.The vehicle manufacturer fully documents its overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is integrated and embedded throughout these processes and key performance indicators are reported to its executive management. 2.The vehicle manufacturer's processes are developed to be practical, usable and appropriate for its policies and technologies. 3.Processes that rely on user behaviour are practical, appropriate and achievable. 4.The vehicle manufacturer reviews and updates processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident. 5.Any changes to the essential function or the threat it faces triggers a review of processes. 6.The vehicle manufacturer's systems are designed so that they are, and remain, secure even when user security policies and processes are not always followed. For such claim a justification should be provided.	1.車両メーカーがその包括的なセキュリティガバナンスおよびリスク管理アプローチ、技術的なセキュリティの実践および特定の規制適合性を完全に文書化している。サイバーセキュリティが統合されており、かつこれらのプロセス全体にわたり埋め込まれており、また、重要な性能指標がその経営管理者に報告されている。 2.車両メーカーのプロセスがその方針および技術に対して実用的、有用かつ適切になるように開発されている。 3.ユーザーの挙動に依存するプロセスが実用的、適切かつ達成可能である。 4.プロセスが現状に合致するものであり続けることを確保するために、車両メーカーが適切に定期的な間隔でプロセスの見直しおよび更新を行っている。これは、重大なサイバーセキュリティインシデントの後で行われる見直しに追加されるものである。 5.不可欠な機能に生じた変更またはそれが直面する脅威によってプロセスの見直しが行われる。 6.車両メーカーのシステムが、ユーザーセキュリティの方針およびプロセスが守られているとは限らない場合でも、セキュアであり、かつセキュアであり続けるよう設計されている。かかる主張については、それを正当とする理由を提供すべきものとする。

7.2.2.2.(b)
The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered;
車両型式に対するリスクの特定のために使用するプロセス

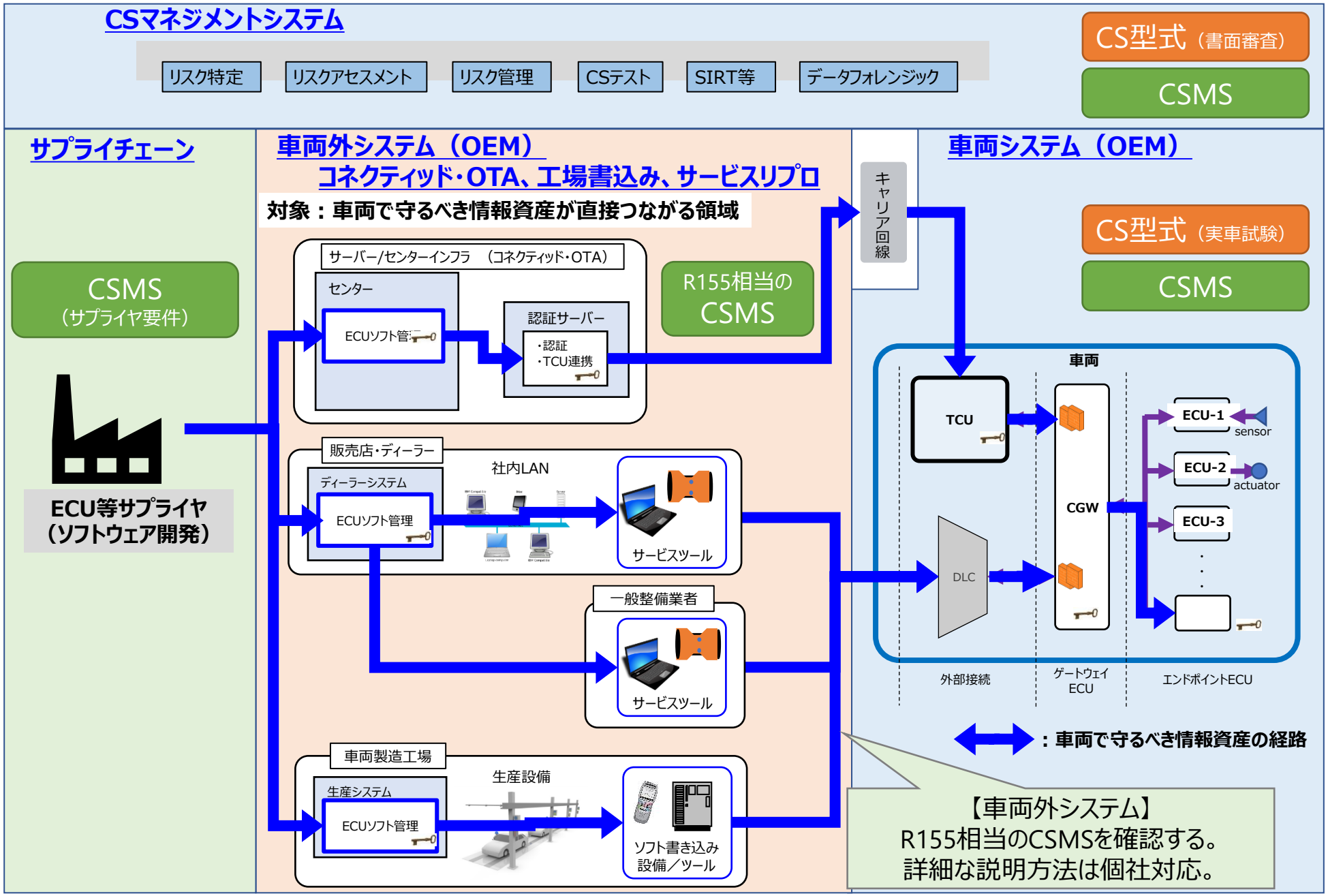
解釈

車両の脅威分析を実施するにあたり、車両としての保護資産を抽出し、リスクを特定するプロセスを定義する。

提出文書

・車両へのリスク特定のために使用されるプロセス（アイテム定義、資産分析・脅威分析）
　について具体的な作業手順を定めた書面（実施手順書など）
※役割、作業フロー、作業内容含む
具体的には以下の記載された書面。
・業務実施部署
・業務処理組織図（7.2.2.2. (a)) で求める組織図ではなく、実務を進める上で関連する部署との関係）
・業務フロー
・具体的な実務プロセス（本書面を参照することによって実作業者の作業方針を規定できるもの。）
・リスク特定結果のサンプル（評価結果を記入する帳票書式のみを提出書面とし、実際に記入された帳票については提示のみで構わない(秘匿性を考慮）立ち合い試験時に確認する。）
上記は認証用に特別に作られた書類ではなく実務で使用される書面であること。但し、必要箇所のみの抜粋でも構わない。
なお、UN規則Annex 5, Part Aに規定する脅威に関し、明らかに車両で発生しえない脅威についてはその理由（リスク特定結果資料と同様にOEM内で保管されること）を明らかにした上で考慮対象から外れるプロセスとしても構わない。
・リスク特定にあたり、当該型式に対するCSMSのマネジメント適用範囲（関係の無いサーバ等の明確化）を記載した資料
　車両リスク特定のために必要と判断した、車両外システムの対象範囲を記載した書面（添付図例）

車両外システムの対象範囲を記載した書面サンプル



判断の目安（WP29解釈文書より引用）

7.2.2.2. (b)

Explanation of the requirement	
The aim of this requirement is for a manufacturer to demonstrate the processes and procedures they use to identify risks to vehicle types. Processes implemented should consider all probable sources of risk. This shall include risks identified Annex 5 of the Cyber Security Regulation e.g. risks arising from connected services or dependencies external to the vehicle. Sources for risk identification may be stated. These may include: (a)Vulnerability/ Threats sharing platforms; (b)Lessons learned regarding risks and vulnerabilities.	この要件の狙いは、車両型式に対するリスクを特定するために使用するプロセスおよび手順をメーカーが証明することである。 実施されるプロセスは、リスクの推定原因をすべて考慮すべきものとする。これは、サイバーセキュリティ規則の附則5で特定されたリスク（例えば、車両外部の接続されているサービスまたは依存関係に起因するリスク）を含むものとする。 リスクの特定に用いた情報源を記載してもよい。これには下記を含めてもよい： (a)脆弱性／脅威を共有するプラットフォーム、 (b)リスクおよび脆弱性に関して学んだ教訓。
Examples of documents/evidence that could be provided	
The following standards may be applicable: (c)ISO/SAE 21434, especially based on [RQ-08-01], [RQ-08-02], [RQ-08-08], [RQ-08-09]. The processes may consider: (d)Identification the relevance of a system to cybersecurity; (e)Description of the overall system with respect to: (i)Definition of the system/function; (ii)Boundaries and interactions with other systems; (iii)Architecture; (iv)Environment of operation of the system (context, constraints and assumptions). (f)Identification of assets; (g)Identification of threats; (h)Identification of vulnerabilities.	下記の規格を適用してもよい： (c)ISO/SAE 21434、特に[RQ-08-01]、[RQ-08-02]、[RQ-08-08]、[RQ-08-09]に基づく箇所。 当該プロセスは下記を考慮してもよい： (d)サイバーセキュリティに対するシステムの関連性の特定。 (e)下記に関するシステム全体の説明： (i)当該システム／機能の定義。 (ii)他のシステムとの境界および相互作用。 (iii)アーキテクチャ。 (iv)システムの作動環境（状況、制約および前提）。 (f)資産の特定。 (g)脅威の特定。 (h)脆弱性の特定。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (b)

The requirement should be considered unfulfilled if one of the following statements is true	
1.Risk identification is not based on a clearly defined set of assumptions. 2.Risk identification for vehicle types are a "one-off" activity (or not done at all). 3.Vehicle types are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).	1.リスクの特定が、明確に定義された一連の前提に基づいていない。 2.車両型式に関するリスクの特定が「一度限り」の活動である（あるいは一度も行われない）。 3.他のシステムとの依存関係および相互作用（例えば、IT環境とOT環境の相互作用）が考慮されずに、車両型式が単独で評価されている。
The requirement may be considered fulfilled if all of the following statements are true	
1.The vehicle manufacturer’s organisational process ensures that security risks to vehicle types are identified, analysed, prioritised, and managed. 2.The vehicle manufacturer’s approach to risk is focused on the possibility of adverse impact to its vehicle types, leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of its networks and systems. 3.The vehicle manufacturer’s risk identification is based on a clearly understood set of assumptions, informed by an up-to-date understanding of security threats to its vehicle types and its sector. 4.The vehicle manufacturer’s risk identification is informed by an understanding of the vulnerabilities in its vehicle types. 5.The vehicle manufacturer performs detailed threat analysis and understand how this applies to your its organisation in the context of the threat to its vehicle types and its sector.	1.車両メーカーの組織的プロセスによって、確実に、車両型式に対するセキュリティリスクが特定され、分析され、優先順位が付けられ、かつ管理される。 2.リスクに対する車両メーカーのアプローチの焦点がその車両型式に対する悪影響の可能性に当てられており、これにより、生じ得る攻撃者の行動ならびにそのネットワークおよびシステムのセキュリティプロパティを原因としてかかる影響がどのように生じるかを詳細に理解することができる。 3.車両メーカーによるリスクの特定が、その車両型式およびその部門に対するセキュリティ脅威の最新情報を理解することによって形成された、明確に理解された一連の前提に基づいている。 4.車両メーカーによるリスクの特定が、その車両型式における脆弱性を理解することによって形成されている。 5.車両メーカーが、詳細な脅威分析を行い、これがその車両型式およびその部門に対する脅威との関連においてどのようにその組織に適用されるのかを理解している。

7.2.2.2.(c)
The processes used for the assessment, categorization and treatment of the risks identified;
特定されたリスクのアセスメント、カテゴリー化および処理のために使用するプロセス

解釈

リスクアセスメントからセキュリティ要求作成までのプロセスのこと。
・リスクアセスメント：リスク特定・リスク分析・リスク評価を行う一連のプロセス
・リスク分類：リスクの保有(許容)、リスクの移転(転嫁)、リスクの低減、リスクの回避に分類
・処置：セキュリティゴール、セキュリティ要求作成（リスクの保有に係わるものを除く）

提出文書

リスクアセスメントを構成する主要プロセス（以下）
に関し、具体的な作業手順を定めた書面
（実施手順書など）
・リスクアセスメントプロセス
・リスク分類プロセス
・リスク処置決定プロセス
具体的には以下の記載された書面。
・業務実施部署
・業務処理組織図
・業務フロー
・具体的な実務プロセス
本書面を参照することによって実作業者の作業方針を規定できるもの。
・リスクアセスメント、分類結果および処置のサンプル（検討開始から結果までの一連の流れを含むこと、但し、認証用に特別に作られた書面ではなく実務で使用される書式であること。但し、必要箇所のみの抜粋でも構わない。また、実在の型式についてで無くとも良く、任意の1つのコントローラに対する書面でも良い。また、エントリーポイント等も限定して良い）また、審査部試験の際には業務手順書等によりリスクアセスメントの手順を本サンプルを用いながら説明すること。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (c)

Explanation of the requirement	
The aim of this requirement is that the manufacturer demonstrates the processes and rules they use to assess, categorize and treat risks identified.	この要件の狙いは、メーカーが特定されたリスクのアセスメント、カテゴリー化および処理のために使用するプロセスおよび規則を証明することである。
Examples of documents/evidence that could be provided	
The following standards may be applicable: (a)ISO/SAE 21434, especially based on [RQ-08-11], [RQ-08-04]. [RQ-08-06], [RQ-08-10], [RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08]; (b)BSI PAS 11281:2018 may be applicable for the consideration of safety and security. The processes may consider: (c)Assessing the associated impact related to the risks identified in requirement 7.2.2.2. b); (d)Identification of potential attack paths related to risks identified in requirement 7.2.2.2. b); (e)Determination of feasibility/likelihood of attack for every attack paths identified above; (f)Calculation and categorization of risks; (g)Treatment options of those identified and categorized risks.	下記の規格を適用してもよい： (a)ISO/SAE 21434、特に[RQ-08-11]、[RQ-08-04]、[RQ-08-06]、[RQ-08-10]、[RQ-08-12]、[RQ-09-07]、[RQ-05-06]、[RQ-09-08]に基づく箇所。 (b)安全およびセキュリティの検討にはBSI PAS 11281:2018を適用してもよい。 当該プロセスは下記を考慮してもよい： (c)7.2.2.2. b)の要件で特定されたリスクに関連する関連影響のアセスメント。 (d)7.2.2.2. b)の要件で特定されたリスクに関連する潜在的攻撃経路の特定。 (e)上記で特定された各攻撃経路に関する攻撃の実現可能性／確率の決定。 (f)リスクの計算およびカテゴリー化。 (g)特定およびカテゴリー化されたリスクの処理に関する選択肢。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (c)

The requirement should be considered unfulfilled if one of the following statements is true	
1.Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner. 2.Security requirements and mitigation techniques are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of vehicle types. 3.Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT). 4.Inventories of assets relevant to vehicle types are incomplete, non-existent, or inadequately detailed. 5.Asset inventories are neglected and out of date. 6.Systems are assessed in isolation, without consideration of dependencies and interactions with other systems (e.g. interactions between IT and OT environments). 7.Risk assessments are not based on a clearly defined set of assumptions. 8.Risk assessments for vehicle types are a "one-off" activity (or not done at all).	1.リスクアセスメントの結果が、過度に複雑であるため、または過度に扱いにくいために、意思決定者が把握することができず、明確かつ適時な方法で効果的に伝達されない。 2.セキュリティ要件および軽減手法が任意のものである。または、それらが、車両型式のセキュリティにどのように寄与するのか考慮されることなく、対策カタログから適用されている。 3.資産の特定の領域または種類のみが文書化および理解されている。資産間の依存関係が理解されていない（ITとOTの依存関係など）。 4.車両型式に関連する資産のインベントリが不完全である、存在していない、または十分に詳細でない。 5.資産インベントリが放置されており、最新の状態でない。 6.他のシステムとの依存関係および相互作用（例えば、IT環境とOT環境の相互作用）が考慮されずに、システムが単独で評価されている。 7.リスクアセスメントが明確に定義された一連の前提に基づいていない。 8.車両型式に関するリスクアセスメントが「一度限り」の活動である（あるいは一度も行われない）。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (c)

The requirement may be considered fulfilled if all of the following statements are true	
1.The output from the vehicle manufacturer's risk management process is a clear set of security reuirements that will address the risks in line with its organisational approach to security. 2.All assets relevant to the secure operation of its vehicle types are identified and inventoried (at a suitable level of detail). 3.The inventory is kept up-to-date. 4.Dependencies on supporting infrastructure are recognised and recorded. 5.The vehicle manufacturer has prioritised assets according to their importance to the operation of its vehicle types. 6.The vehicle manufacturer's risk identification is based on a clearly understood set of assumptions, informed by an up-to-date understanding of security threats to its vehicle types and its sector. 7.The vehicle manufacturer's risk identification is informed by an understanding of the vulnerabilities in its vehicle types. 8. The manufacturer can demonstrate the effectiveness and repeatability of their processes for their categorisation and treatment of risk.	1.車両メーカーのリスク管理プロセスから、セキュリティに対するその組織的アプローチに沿ってリスクに対処する明確な一連のセキュリティ要件が得られる。 2.その車両型式のセキュアな運用に関連するすべての資産が特定されており、かつそのインベントリが（適切な詳細度で）作成されている。 3.当該インベントリが最新の状態に保たれている。 4.支持インフラへの依存関係が認識および記録されている。 5.車両メーカーが、その車両型式の運用に対する重要度に応じて資産に優先順位を付けている。 6.車両メーカーによるリスクの特定が、その車両型式およびその部門に対するセキュリティ脅威の最新情報を理解することによって形成された、明確に理解された一連の前提に基づいている。 7.車両メーカーによるリスクの特定が、その車両型式における脆弱性を理解することによって形成されている。 8.メーカーはリスクのカテゴリー化および処理を行うための自社のプロセスの有効性および再現性を証明することができる。

7.2.2.2.(d)
The processes in place to verify that the risks identified are appropriately managed;
特定されたリスクが適切に管理されていることを検証するために実施されているプロセス

解釈

特定されたリスクに対して確実に対策が適用されるプロセスのこと。（リスクと対策をトレース可能なプロセス）

提出文書

・リスクに対して確実に対策が適用されていることを確認するための社内レビュー等のプロセス※
に関し、具体的な作業手順を定めた書面（実施手順書など）
※社内レビュー、品質ゲートなど

具体的には以下の記載された書面。
・業務実施部署
・業務処理組織図
・業務フロー
・具体的な実務プロセス
本書面を参照することによって実作業者の作業方針を規定できるもの。
但し、認証用に特別に作られた書類ではなく実務で使用される書面であること。但し、必要箇所のみの抜粋でも構わない。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (d)

Explanation of the requirement	
The aim of this requirement is that the manufacturer demonstrates the processes and rules they use to decide how to manage the risks. This can include the decision criteria for risk treatment, e.g. the process for selecting what controls to implement and when to accept a risk. The results of the process for risks identification and assessment should feed into selecting the appropriate treatment category options to address those risks. The outcome of this process should be that the residual risk (risks remaining after treatment) is within the manufacturer's stated tolerance of risks (i.e. within stated acceptable limits). Mitigations identified in Annex 5 of the Cyber Security Regulation shall be considered in the processes.	この要件の狙いは、リスク管理方法を決定するために使用するプロセスおよび規則をメーカーが証明することである。これには、リスク処理に関する決定基準（例えば、実施すべき対策およびリスクを受け入れるべき時を選択するためのプロセス）を含めることができる。 リスクの特定およびアセスメントのためのプロセスの結果を利用して、これらのリスクに対処するための適切な処理カテゴリーの選択肢を選択すべきものとする。このプロセスの結果、残存リスク（処理後に残っているリスク）は、メーカーによって定められたリスクの許容範囲内（すなわち、定められた容認限度内）にあるべきものとする。 サイバーセキュリティ規則の附則5で特定された軽減策が当該プロセスで考慮されるものとする。
Examples of documents/evidence that could be provided	
The following standards may be applicable: (a)ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-09]; (b)ISO 31000 may be applicable if adapted for product related risks. The processes may consider: (c)Appropriate and proportional risk treatment methodologies; (d)Treatment of critical elements (with safety and environment) to ensure the risks to them are appropriately mitigated and proportionately based on the safety or environmental goal of dependent vehicle systems; (e)Ensuring the residual risk remains within acceptable limits for components or the overall vehicle type; (f)Detailing any cases where the organization would accept justification for non-adherence to their stated risk tolerance.	下記の規格を適用してもよい： (a)要求されている証明および評価の根拠としてISO/SAE 21434、特に[RQ-09-09]に基づく箇所を用いることができる。 (b)ISO 31000を製品関連リスクに適応させた上で適用してもよい。 当該プロセスは下記を考慮してもよい： (c)適切かつ比例的なリスク処理方法。 (d)（安全および環境に）必要不可欠な要素に対するリスクが適切に軽減され、かつ当該要素がそれらに依存している車両システムの安全または環境目標に比例的に基づくことを確保するために行われる当該要素の処理。 (e)残存リスクが構成部品または車両型式全体に関する容認限度内にあり続けることを確保すること。 (f)当該組織によって定められたリスク許容範囲を遵守しないことを正当化する根拠を当該組織が受け入れる場合に関する詳細説明。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (d)

The requirement should be considered unfulfilled if one of the following statements is true	
1.The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes. 2.There is no systemic process in place to ensure that identified security risks are managed effectively. 3.Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.	1.プロジェクトまたはプログラムのセキュリティ要素がリスク管理 アセスメントの完了にのみ依存しており、結果がまったく考慮されない。 2.特定されたセキュリティリスクが効果的に管理されることを確保するための系統的プロセスが確立されていない。 3.登録されたリスクが、解決のための上層部による意思決定または資源配分を待ちながら長期にわたり未解決のままの状態にある。
The requirement may be considered fulfilled if all of the following statements are true	
1.Significant conclusions reached in the course of the vehicle manufacturer’s risk management process are communicated to key security decision-makers and accountable individuals. 2.The effectiveness of the vehicle manufacturer’s risk management process is reviewed periodically, and improvements made as required.	1.車両メーカーのリスク管理プロセスの過程において達した重大な結論が主要なセキュリティ意思決定者および個々の責任者に伝達されている。 2.車両メーカーのリスク管理プロセスの有効性が定期的に再評価されており、必要に応じて改善が行われている。

7.2.2.2. (e)
The processes used for testing the cyber security of a vehicle type;
車両型式のサイバーセキュリティをテストするために使用するプロセス

解釈

車両に対するセキュリティテスト

提出文書

・7.2.2.2. (c)（リスク処置）で決定した対策結果が確実に導入されていることを確認するプロセスに関し、
具体的な実施手順を定めた書面（実施手順書など）
各社によって評価プロセスが異なるため画一的な書き方が難しいが、以下のような書面を想定。
・クルマのセキュリティテストプロセス
セキュリティ試験手順書（※役割、作業フロー、作業内容含む）を含むこと。
・確認結果に問題があった場合の対応（上流へのF/B方法）含む
・生産車両に確実に想定した対策が導入されていることを確認するプロセス。
認証時と同一のクルマが生産されていることの説明を記載すること。
・テスト結果のサンプル（結果記述は空欄もしくは参考内容で良く、実試験結果でなくともよい）

Explanation of the requirement

The aim of this requirement is to ensure the manufacturer has appropriate capabilities and processes for testing the vehicle type throughout its development and production phases. Testing processes in the production phase may be different to the ones used during the development phase.

この要件の狙いは、車両型式を開発フェーズおよび生産フェーズの全体を通してテストするための適切な能力およびプロセスをメーカーが有していることを確保することである。
生産フェーズにおけるテストプロセスは、開発フェーズ中に使用されるものとは異なっていてもよい。

Examples of documents/evidence that could be provided

The following standards may be applicable:
(a)ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-10], [RQ-10-01]. [RQ-11-01], [RQ-11-02], [RQ-12-01];
(b)BSI PAS 11281:2018 may be utilised for considering the interaction of safety and security and processes for evidencing security outcomes are met.

The processes may consider:
Development Phase:
(c)Organization specific rules for testing during development;
(d)Processes for creation and execution of test strategies;
(e)Processes for cybersecurity testing planning;
(f)Processes for cybersecurity system design testing;
(g)Processes for cybersecurity software unit testing;
(h)Processes for cybersecurity hardware testing;
(i)Processes for cybersecurity integration testing;
(j)Processes for documentation of the results of testing;
(k)Processes for handling vulnerabilities identified during testing;
(l)Justification and requirements for cybersecurity tests, like Functional (requirement-based, positive and negative) testing, Interface testing, Penetration testing, Vulnerability scanning, Fuzz testing but not limited to the same.
Production Phase:
(m)Processes for testing to ensure the produced system has the cybersecurity requirements, controls and capabilities outlined in the production plan;
(n)Processes for testing to ensure the produced item meets the cybersecurity specifications which are in accordance with the system in the development phase;
(o)Processes for testing to assure that cybersecurity controls and configuration as cybersecurity specifications are enabled in the produced item;
(p)Processes for documenting the test results and findings handling.

下記の規格を適用してもよい：
(a)要求されている証明および評価の根拠としてISO/SAE 21434、特に[RQ-09-10]、[RQ-10-01]、[RQ-11-01]、[RQ-11-02]、[RQ-12-01]に基づく箇所を用いることができる。
(b)安全およびセキュリティとセキュリティ成果が得られたことを証明するためのプロセスとの相互作用を検討する際にはBSI PAS 11281:2018を利用してもよい。

当該プロセスは下記を考慮してもよい：
開発フェーズ：
(c)開発におけるテストに関する組織固有の規則。
(d)テストストラテジーの策定および実行のプロセス。
(e)サイバーセキュリティテスト計画のプロセス。
(f)サイバーセキュリティシステム設計テストのプロセス。
(g)サイバーセキュリティソフトウェア単体テストのプロセス。
(h)サイバーセキュリティハードウェアテストのプロセス。
(i)サイバーセキュリティ統合テストのプロセス。
(j)テスト結果の文書化のプロセス。
(k)テスト中に特定された脆弱性に対処するためのプロセス。
(l)サイバーセキュリティテスト（機能（要件に基づく、成功および失敗）テスト、インターフェーステスト、侵入テスト、脆弱性スキャン、ファジングなどを指すが、これらに限定されない）に関する正当性の根拠および要件。
生産フェーズ：
(m)生産されたシステムが生産計画に記載されたサイバーセキュリティ要件、対策および能力を有していることを確保するためのテストのプロセス。
(n)生産製品が開発フェーズのシステムに沿ったサイバーセキュリティ仕様を満たしていることを確保するためのテストのプロセス。
(o)サイバーセキュリティ仕様としてのサイバーセキュリティ対策および構成が生産製品内で有効であることを保証するためのテストのプロセス。
(p)テスト結果および知見の扱いを文書化するためのプロセス。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (e)

The requirement should be considered unfulfilled if one of the following statements is true	
1.A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value. 2.Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments. 3.Assurance is assumed because there have been no known problems to date.	1.特定の製品またはサービスが「特効薬」とみなされており、ベンダーの主張がそのまま受け止められている。 2.保証方法の長所および欠点（運用環境における侵入テストのリスクなど）が認識されることなく、保証方法が適用されている。 3.現在まで既知の問題が生じていないという理由から保証があると考えられている。
The requirement may be considered fulfilled if all of the following statements are true	
1.The vehicle manufacturer validates that the security measures in place to protect systems are effective and remain effective until the end-of-life of all vehicles under the vehicle types for which they are needed. 2.The vehicle manufacturer understands the assurance methods available to it and chooses appropriate methods to gain confidence in the security of vehicle types. 3.The vehicle manufacturer’s confidence in the security as it relates to its technology, people, and processes can be justified to, and verified by, a third party. 4.Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way. 5.The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.	1.車両メーカーが、システムを保護するために実施されているセキュリティ措置が効果的であること、ならびに、それらが必要とされる車両型式に属するすべての車両が使用済みになるまでそれらが効果的であり続けることを確認している。 2.車両メーカーが、利用可能な保証方法を理解しており、車両型式のセキュリティに対する信頼を得るために適切な方法を選択している。 3.車両メーカーがその技術、人員、およびプロセスに関連して有しているセキュリティに対する信頼について、その正当性を第三者に説明することができ、かつ第三者がそれを検証することができる。 4.保証活動によって見つかったセキュリティの不備は、評価され、 優先順位が付けられ、 必要に応じて適時かつ効果的な方法で是正される。 5.使用している保証方法が目的のとおりに機能しており、かつ最も適切な使用方法であり続けることを確保するために、当該方法の見直しが行われている。

7.2.2.2. (f)
The processes used for ensuring that the risk assessment is kept current;
リスクアセスメントが最新の状態に保たれていることを確保するために使用するプロセス

解釈

市場動向を反映したリスクアセスメントの定期見直し（ハッキング技術動向、レベル調査）に関するプロセス

提出文書

・SIRT活動
（脆弱性モニタリングプロセス）の実施手順書

判断の目安（WP29解釈文書より引用）

7.2.2.2. (f)

Explanation of the requirement	
The aim of this requirement is to ensure the risk assessment is kept current. This should include processes to identify if the risks to a vehicle type have changed and how this will be considered within the risk assessment. Sources for risk identification may be stated. These may include: (a)Vulnerability/ Threats sharing platforms; (b)Lessons learned regarding risks and vulnerabilities; (c)Conferences. It is noted that requirements 7.2.2.2. parts f) to h) may have overlaps in terms of the processes used and therefore the same evidence may be applicable to demonstrating that these requirements are met.	この要件の狙いは、リスクアセスメントが最新の状態に保たれることを確保することである。これは、車両型式に対するリスクが変化したかどうか、また、リスクアセスメントにおいてこれをどのようにみなすのかを特定するためのプロセスを含むべきものとする。 リスクの特定に用いた情報源を記載してもよい。これには下記を含めてもよい： (a)脆弱性／脅威を共有するプラットフォーム、 (b)リスクおよび脆弱性に関して学んだ教訓、 (c)会議。 7.2.2.2.パートf)からh)の要件は使用プロセスの観点から重複している可能性があり、したがって、これらの要件が満たされていることの証明には同一の証拠を適用してもよいことに留意する。
Examples of documents/evidence that could be provided	
(d)ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-11-03], [RQ-06-08]. [RQ-07-05], [RQ-07-06].	(d)要求されている証明および評価の根拠としてISO/SAE 21434、特に[RQ-11-03]、[RQ-06-08]、[RQ-07-05]、[RQ-07-06]に基づく箇所を用いることができる。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (f)

The requirement should be considered unfulfilled if one of the following statements is true	
1.No processes are in place which require the risk assessment to be updated.	1.リスクアセスメントの更新を要求するプロセスが確立されていない。
The requirement may be considered fulfilled if all of the following statements are true	
1.The vehicle manufacturer conducts risk assessments when significant events potentially affect vehicle types, such as replacing a system or a change in the cyber security threat. 2.The vehicle manufacturer's risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to vehicle types, change of use and new threat information.	1.システムの交換またはサイバーセキュリティ脅威の変化などの重大イベントが車両型式に影響を及ぼす可能性があるときに車両メーカーがリスクアセスメントを実施する。 2.車両メーカーのリスクアセスメントは動的であり、関連のある変化（車両型式に行われる技術的変更、使用の変化および新しい脅威情報を含む場合がある）に対して更新される。

7.2.2.2. (g)
The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.
車両型式へのサイバー攻撃・脅威・脆弱性を監視および検知し、対応するために使用するプロセスおよび実施された対策が、特定された新たなサイバー脅威と脆弱性に対して引き続き有効かを評価するプロセス

解釈

- 車両型式へのサイバー攻撃が発覚してから対応/復旧までに関するプロセス
- フィールド監視（J-Auto-ISACの活動も参考）を実施し、自社のシステムに対する影響有無判断、その後対応に関するプロセス
- 脆弱性が発覚してから対応/復旧までに関するプロセス

提出文書

- SIRT活動（インシデント）の実施手順書
－フィールド監視（インシデント・脆弱性の情報入手）の手順
－インシデント発生時の手順
－脆弱性発生時の手順
－監視、検出によって得られた新たな脅威に対して、実装された対策が依然として有効であることを確認する手順。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (g)

Explanation of the requirement

The aim of this requirement is to ensure that the manufacturer has processes to monitor for cyber-attacks, threats or vulnerability to vehicles that the manufacturer has had type approved, i.e. are in the post-production or production phase, and that they have established processes that would permit them to respond in an appropriate and timely manner.
It is noted that requirements 7.2.2.2. parts f) to h) may have overlaps in terms of the processes used and therefore the same evidence may be applicable to demonstrating that these requirements are met.

この要件の狙いは、型式認可を受けた車両（すなわち、生産後または生産フェーズにある車両）に対するサイバー攻撃、脅威または脆弱性を監視するためのプロセスをメーカーが有していること、ならびに適切かつ適時な方法で対応することを可能とするプロセスをメーカーが確立していることを確保することである。
7.2.2.2.パートf)からh)の要件は使用プロセスの観点から重複している可能性があり、したがって、これらの要件が満たされていることの証明には同一の証拠を適用してもよいことに留意する。

Examples of documents/evidence that could be provided

The following standards may be applicable:
(a)ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-07-01], [RQ-07-02]. [RQ-07-03], [RQ-07-04], [RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03], [RQ-13-01], [RQ-13-02], [RQ-13-03].

The following could be used to evidence the processes used:
(b)Cyber security monitoring processes for post-production vehicles. This may include processes that will collect information that may or may not be pertinent to the manufacturer's vehicle/system;
(c)Cyber security information assessment processes. These will be processes for the identification of the relevance of the information collected with respect to the system/vehicle of the manufacturer;
(d)Processes for risk determination/assessment for the relevant information;
(e)Incident response procedures for both vehicles already registered and yet to be registered of the vehicle types covered by the CSMS, which may include evidence of procedures for:
  (i)Interaction with authorities;
  (ii)Identified or stated triggers that would lead to an escalation or action;
  (iii)Determining what response options might be implemented for which condition;
  (iv)Handling any dependencies and interactions with suppliers.
(f)Evidence that the response procedures would work, for example through exercising and verification that planning assumptions remain valid under test.

下記の規格を適用してもよい：
(a)要求されている証明および評価の根拠としてISO/SAE 21434、特に[RQ-07-01]、[RQ-07-02]、[RQ-07-03]、[RQ-07-04]、[RQ-07-05]、[RQ-15-04]、[RQ-15-05]、[RC-15-03]、[RQ-13-01]、[RQ-13-02]、[RQ-13-03]に基づく箇所を用いることができる。

使用プロセスの証明には下記が使用できると考えられる：
(b)生産後の車両に関するサイバーセキュリティ監視のプロセス。これには、情報（メーカーの車両／システムとの関連があってもよいし、なくてもよい）を収集するプロセスを含めてもよい。
(c)サイバーセキュリティ情報アセスメントのプロセス。これらは、メーカーのシステム／車両に対する収集情報の関連性を特定するためのプロセスである。
(d)関連情報に関するリスク判定／アセスメントのプロセス。
(e)CSMSの対象車両型式の登録済み車両と未登録車両の両方に関するインシデント対応手順。これには、下記に関する手順の証拠を含めてもよい：
  (i)当局との相互関係。
  (ii)深刻化または措置の実行を引き起こすきっかけとなるものを特定または規定すること。
  (iii)実施される可能性がある対応策の選択肢およびその条件を決定すること。
  (iv)サプライヤーとの依存関係および相互関係に対処すること。
(f)対応手順が機能するという証拠。この証拠は、例えば、訓練によって、また、計画の前提がテスト時にも有効であり続けることの検証によって得られる。

判断の目安（WP29解釈文書より引用）

7.2.2.2. (g)

The requirement should be considered unfulfilled if one of the following statements is true	
1.The vehicle manufacturer has no sources of threat intelligence. 2.The vehicle manufacturer does not apply updates in a timely way, after receiving them. 3.The vehicle manufacturer does not evaluate the usefulness of its threat intelligence or share feedback with providers, authorised aftermarket service providers or other users. 4.There are no staff who perform a monitoring function. 5.Monitoring staff do not have the correct specialist skills. 6.Monitoring staff are not capable of reporting against governance requirements. 7.Security alerts relating to vehicle types are not prioritised.	1.車両メーカーが脅威に関する情報源を有していない。 2.車両メーカーが、更新を受け取った後、適時にそれらを適用していない。 3.車両メーカーがその脅威情報活動の有用性を評価していない。または、提供者、権限が与えられたアフターマーケットサービス提供者またはその他のユーザーとフィードバックを共有していない。 4.監視役を果たす従業員がいない。 5.監視員が正しい専門家の技能を有していない。 6.監視員がガバナンス要件の違反を報告できていない。 7.車両型式に関連するセキュリティアラートに優先順位が付けられていない。
The requirement may be considered fulfilled if all of the following statements are true	
1.Data relating to the security and operation of vehicle types is collected. 2.Alerts from third parties are investigated, and action taken. 3.Some logging datasets can be easily queried with search tools to aid investigations. 4.The resolution of alerts to an asset or system is performed regularly. 5.Security alerts relating to vehicle types are prioritised. 6.The vehicle manufacturer applies updates in a timely way. 7.The vehicle manufacturer has processes to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities which are relevant to its business needs, or specific threats in its sector. 8.The vehicle manufacturer knows how effective its processes are (e.g. by tracking how they helps it identify security problems). 9.Monitoring staff have appropriate investigative skills and a basic understanding of the data they need to work with. 10.Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers). 11.The vehicle manufacturer successfully demonstrates the processes to evaluate whether the cyber security measures implemented are robust enough to conclude whether they are still effective.	1.セキュリティおよび車両型式の運用に関連するデータが収集されている。 2.第三者からのアラートが調査され、措置が講じられる。 3.いくつかのロギングデータセットは、調査を補助する検索ツールを用いて容易に検索することができる。 4.資産またはシステムに対するアラートの解決が定期的に行われている。 5.車両型式に関連するセキュリティアラートに優先順位が付けられている。 6.車両メーカーが更新を適時に適用している。 7.車両メーカーのビジネスニーズまたはその部門における特定の脅威に関連するサイバー攻撃、サイバー脅威および脆弱性を監視および検知し、それらに対応するためのプロセスを車両メーカーが有している。 8.車両メーカーがそのプロセスの効果の程度を（例えば、セキュリティ問題の特定にどのように役立っているかを追跡することによって）知っている。 9.監視員が適切な調査技能を有しており、扱う必要があるデータの基礎を理解している。 10.監視員が当該組織の他の部署（例えば、セキュリティ担当取締役、レジリエンス担当部長）の指示を仰ぐことができる。 11.車両メーカーが、実施されたサイバーセキュリティ措置が依然として効果的であるか否かを結論付けるための、当該措置が十分に強固であるか否かを評価するためのプロセスの証明に成功している。

7.2.2.2. (h)
The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.
実施されたサイバー攻撃の分析に資する関連データを提供するために使用されるプロセス

解釈

分析に必要なデータを分析担当部署（分析を社外に委託している場合には当該分析を実施する者）に対して提供するプロセスが構築されていることを証明するものとする。

提出文書

SIRT活動（インシデント）の実施手順書
－フィールド監視（インシデント・脆弱性の情報入手）の手順
－インシデント発生時の手順
　（どのような情報を、どのような手順で分析担当に渡すかの概要を含む）
　（脆弱性分析の結果に照らして、攻撃の影響があるかの分析を含む）
－脆弱性発生時の手順
　（どのような情報を、どのような手順で分析担当に渡すかの概要を含む）
－関連データを提供するために用いる帳票等（結果記述は空欄もしくは参考内容でよい）

判断の目安（WP29解釈文書より引用）

7.2.2.2. (h)

Explanation of the requirement	
The intention of this requirement is to ensure that a process has been established to provide the data required for analysis and associated responsibilities for handling the data and analysis. (a)ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-07-03].	この要件の意図は、分析に必要なデータを提供するためのプロセスが確立されていること、ならびに当該データの扱いおよび分析に関連する責任を確保することである。 (a)要求されている証明および評価の根拠としてISO/SAE 21434、特に[RQ-07-03]に基づく箇所を用いることができる。
Examples of documents/evidence that could be provided	
The following could be used to evidence the processes used: (b) Procedure for implementing Security Incident Response Team activities (incidents); (c)Field monitoring (obtaining information on incidents and vulnerabilities); (d)Procedure when an incident occurs (including an overview of what information is passed to the analyst in what steps); (e) Procedure when a vulnerability is discovered (including an overview of what information is passed to the analyst in what steps).	使用プロセスの証明には下記が使用できると考えられる： (b) セキュリティインシデント対応チームの活動（インシデント）を実施するための手順。 (c)フィールド監視（インシデントおよび脆弱性に関する情報の取得）。 (d)インシデントが発生したときの手順（分析者に送られる情報およびそのステップに関する概要を含む）。 (e)脆弱性が見つかったときの手順（分析者に送られる情報およびそのステップに関する概要を含む）。

7.2.2.3.
The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 7.2.2.2 (c) and 7.2.2.2 (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.
脅威及び脆弱性のうち対応が必要なものが合理的な期間内に軽減されることが確保されることを証明しなければならない

解釈

特定されたリスクが分類及び対応された後、当該分類結果に基づいて対応期限を決定するプロセスが構築されていることを証明するものとする。トリアージなどのプロセスによる対応期限の設定と対応期限内に実行されているかの監視プロセスの説明は必要。

提出文書

SIRT活動（インシデント）の実施手順書
－フィールド監視（インシデント・脆弱性の情報入手）の手順
－インシデント発生時の手順
－脆弱性発生時の手順
ただし、これらの手順書においてインシデント対応の期限が設定され、その期限内に確実に対応するようマネジメントするプロセスが記載されていない場合には、別文書等（ただし通常業務で用いる基準書、手順書の類に限る）で当該プロセスを記載すること。

判断の目安（WP29解釈文書より引用）

7.2.2.3.

Explanation of the requirement	
The intention of this requirement is to ensure that after the identified risks have been classified, a process has been established to determine the response time limit based on the classification results. It is necessary to set the response deadline by processes such as triage and explain the monitoring process to see if it is executed within the deadline. The timeframes provided by the manufacturers should be able to be justified and explained. There may be a set of timeframes covering different possible situations. This should include timeframes for deciding and implementing possible reactions or responses. ISO/SAE 21434 can be used as the basis for evidencing the required processes, especially based on [RQ-05-02] b).	この要件の意図は、特定されたリスクが分類された後に、分類結果に基づき応答期限を決定するためのプロセスが確立されていることを確保することである。 トリアージなどのプロセスによって応答期限を設定し、監視プロセスが期限内に実行されるかどうかを知るために監視プロセスについて説明することが必要である。 メーカーが提供する時間枠については、その正当性の根拠を示して説明することができるべきものとする。複数の異なる想定状況を対象にした一連の時間枠があってもよい。これには、想定される反応または応答を決定および実施するための時間枠を含めるべきものとする。 要求されているプロセスの証明の根拠としてISO/SAE 21434、特に[RQ-05-02] b)に基づく箇所を使用することができる。
Examples of documents/evidence that could be provided	
The following could be used to evidence the processes used: (a)Procedure for implementing cyber security incident response activities, including: (i)Field monitoring (obtaining information on incidents and vulnerabilities); (ii)Procedure for incident handling, including how the timeframe to respond is determined; (iii)Procedures for discovering vulnerabilities. (b)Demonstration of how the procedures are implemented.	使用プロセスの証明には下記が使用できると考えられる： (a)下記を含むサイバーセキュリティインシデント対応活動を実施するための手順： (i)フィールド監視（インシデントおよび脆弱性に関する情報の取得）。 (ii)インシデントに対処するための手順（応答時間枠の決定方法を含む）。 (iii)脆弱性を見つけるための手順。 (b)当該手順を実施する方法の証明。

7.2.2.4.
The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 7.2.2.2 (g) shall be continual. This shall:
(a)Include vehicles after first registration in the monitoring;
(b)Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.
監視が継続的であることを保証し証明しなければならない

解釈

7.2.2.2.(g)に従って取得した、および、その他メーカーが保管しているモニタリングに関する情報を活用し、当該データ等が分析に活用されるプロセスが構築されていることを証明するものとする。

提出文書

SIRT活動（インシデントに関すること）の実施手順書
－フィールド監視（インシデント・脆弱性の情報入手）の手順
－インシデント発生時の手順
－脆弱性発生時の手順
ただし、上記書面において7.2.2.4.(a)および7.2.2.4.(b)の記載が無い場合には別途基準書または手順書を提出すること。
7.2.2.4.(a)については、公開された脆弱性情報やインシデントなどを収集して解析する手順
7.2.2.4.(b)については、 車両のデータおよびログから脅威、脆弱性、サイバーアタック等を検出および解析する手順の記載があること。また、本取り扱いの際には個人情報その他のプライバシー保護を考慮していることの記載があること。
－検出および解析結果を記入する帳票類（結果記述は空欄もしくは参考内容でよい。）

判断の目安（WP29解釈文書より引用）

7.2.2.4.

Explanation of the requirement	
The intention of this requirement is to ensure that processes of monitoring for cyber-attacks, cyber threats and vulnerabilities on vehicle types are continual and apply to all registered vehicles of the manufacturer that fall within the scope of their Cyber Security Management System and use: a)the information on monitoring acquired in accordance with 7.3.7. in addition to other sources of information on monitoring acquired in accordance with 7.2.2.2. (g) (such as social media). It is noted that paragraph 1.3., and compliancy with data privacy laws, are particularly relevant to this requirement, ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on 7.3 “Cybersecurity Monitoring”, 7.4 “Cybersecurity event assessment”, 7.5 “Vulnerability analysis.	この要件の意図は、車両型式におけるサイバー攻撃、サイバー脅威および脆弱性の監視のプロセスが、継続するものであり、自社のサイバーセキュリティ管理システムの適用範囲内にあるメーカーのすべての登録車両に適用されており、かつ下記を使用することを確保することである： a)7.2.2.2. (g)に従って取得したその他の監視情報の情報源（ソーシャルメディアなど）に加えて、7.3.7に従って取得した監視情報。 1.3項、およびデータプライバシーに関する法律の遵守はとりわけこの要件に関連していることに留意する。 要求されている証明および評価の根拠としてISO/SAE 21434、特に7.3「サイバーセキュリティの監視」、7.4「サイバーセキュリティイベントのアセスメント」、7.5「脆弱性分析」に基づく箇所を用いることができる。
Examples of documents/evidence that could be provided	
The following could be used to evidence the processes used: (b)Procedure for implementing cyber security incident response activities, including: (i)Field monitoring (obtaining information on incidents and vulnerabilities) (ii)Procedure for incident handling (iii)Procedures for discovering vulnerabilities (c)Demonstration of how the procedures are implemented.	使用プロセスの証明には下記が使用できると考えられる： (b)下記を含むサイバーセキュリティインシデント対応活動を実施するための手順： (i)フィールド監視（インシデントおよび脆弱性に関する情報の取得）。 (ii)インシデントに対処するための手順。 (iii)脆弱性を見つけるための手順。 (c)当該手順を実施する方法の証明。

7.2.2.5.
The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.
車両メーカーは、7.2.2.2.項の要件に関して、契約したサプライヤーおよびサービス提供者、またはメーカーの下位組織との間に存在する可能性がある依存関係について、自社のサイバーセキュリティ管理システムがどのように対処するかを証明するよう要求されるものとする。

解釈

7.2.2.2.要件に対してサプライヤとOEMの責任分担を明確にした契約（例：CIA等）を締結すること

提出文書

CIAの締結などサプライヤとの契約における
責任分解点およびサプライヤー責任の管理方法に関する
社内規定。（CIA：Cybersecurity Interface Agreement）
想定としては以下の書面。
・サプライヤ選定・契約するための社内手順書（セキュリティ対象のみ）
・サプライヤCS管理規定（セキュリティ対象のみ）
また、サプライヤとの開発・生産契約が切れた後も、新たな脅威や脆弱性が検出された場合に、OEMが対策を実施するプロセスの記載があること。

判断の目安（WP29解釈文書より引用）

7.2.2.5.

Explanation of the requirement	
The intention of this requirement is to ensure that it can be shown that risks from suppliers are able to be known and can be managed within the processes described in the CSMS. The steps taken should be proportionate to the risks from what is supplied. The final implementation of the processes may be incorporated into bilateral agreement between the vehicle manufacturer and their suppliers. Within the CSMS there may be processes to: (a)identify risks associated with parts, components, systems or services provided by suppliers; (b)manage risks to the vehicle coming from service providers providing connectivity functions or services that a vehicle may rely on, this may include for example cloud providers, telecom providers, internet providers and authorised aftermarket service providers; (c)ensure contracted suppliers and/or service providers are able to evidence how they have managed risks associated with them. The processes may include consideration of validation or testing requirements that may be used to evidence that risks are appropriately managed; (d)delegate relevant requirements to relevant departments or sub-organisations of the manufacturer, in order to manage risks identified. It is noted that it is possible to put requirements on Tier1 suppliers and to require they cascade it to Tier 2 suppliers. However, it may be difficult for a manufacturer to cascade requirements further down in the supply chain (especially legally binding requirements).	この要件の意図は、サプライヤー由来のリスクを知ることができ、かつそれらはCSMSに記載されたプロセス内で管理可能であると証明できることを確保することである。講じる措置は、供給されるものに由来するリスクに比例すべきものとする。 当該プロセスの最終的な実施を車両メーカーとそれらのサプライヤーの二者間合意に組み込んでもよい。 CSMS内には下記を行うためのプロセスがあってもよい： (a)サプライヤーから提供される部品、構成部品、システムまたはサービスと関連付けられるリスクを特定する。 (b)車両が依存する可能性がある接続性の機能またはサービスを提供するサービス提供者（これは、例えば、クラウド提供者、電気通信提供者、インターネット提供者および権限が与えられたアフターマーケットサービス提供者を含む場合がある）に由来する車両に対するリスクを管理する。 (c)契約サプライヤーおよび／またはサービス提供者がそれらと関連付けられたリスクをどのように管理してきたかを証明できることを確保する。当該プロセスには、リスクが適切に管理されていることを証明するために使用してもよい妥当性確認またはテスト要件を考慮することを含めてもよい。 (d)特定されたリスクを管理するために、メーカーの関連部署または下部組織に関連要件を委託する。 ティアワンサプライヤーに要件を課して、それをティアツーサプライヤーに伝達するよう要求することが可能であることに留意する。ただし、メーカーがサプライチェーンのより下の組織へ要件を伝達することは難しい場合がある（特に法的拘束力のある要件）。

判断の目安（WP29解釈文書より引用）

7.2.2.5.

Examples of documents/evidence that could be provided	
The following standards may be applicable: (e) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-06-09], [RQ-15-03], [RC-15-02]. The following could be used to evidence the processes used: (f)Contractual agreements in place or evidence of such agreements; (g)Evidenced arguments for how their processes will ensure suppliers / service providers will be considered in the risk assessment process; (h)Procedures/Methods of sharing information on risk between suppliers and manufacturers; (i)Existing solutions / contracts like ISMS (Information Security Management System) regulation can be used for evidence. This may be evidenced by certificates based on ISO/IEC 27001 or TISAX (Trusted Information Security Assessment eXchange).	下記の規格を適用してもよい： (e)要求されている証明および評価の根拠としてISO/SAE 21434、特に[RQ-06-09]、[RQ-15-03]、[RC-15-02]に基づく箇所を用いることができる。 使用プロセスの証明には下記が使用できると考えられる： (f)実施中の契約またはかかる契約の証拠。 (g)リスクアセスメントプロセスにおいてサプライヤー／サービス提供者が考慮されることをそれらのプロセスがどのように確保するのかに関する議論の証拠。 (h)サプライヤーとメーカーの間でリスクに関する情報を共有する手順／方法。 (i)ISMS（情報セキュリティ管理システム）規則のような既存の解決策／契約を証拠として使用することができる。これは、ISO/IEC 27001またはTISAX（信頼できる情報セキュリティアセスメントの交換）に基づく認定書によって証明してもよい。

判断の目安（WP29解釈文書より引用）

7.2.2.5.

The requirement should be considered unfulfilled if one of the following statements is true	
1.Relevant contracts with suppliers and service providers do not have cyber security requirements.	1.サプライヤーおよびサービス提供者との関連契約にサイバーセキュリティ要件がない。
The requirement may be considered fulfilled if all of the following statements are true	
1.The vehicle manufacturer has a deep understanding of its supply chain, including sub-contractors and the wider risks it faces. The vehicle manufacturer considers factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs its risk assessment and procurement processes. 2.The vehicle manufacturer's approach to supply chain risk management considers the risks to its vehicle types arising from supply chain subversion by capable and well-resourced attackers. 3.The vehicle manufacturer has confidence that information shared with suppliers that is essential to the operation of your vehicle types is appropriately protected from sophisticated attacks. 4.The vehicle manufacturer can clearly express the security needs it places on suppliers in ways that are mutually understood and are laid in contracts. There is a clear and documented shared-responsibility model. 5.All network connections and data sharing with third parties is managed effectively and proportionately. 6.When appropriate, the vehicle manufacturer's incident management process and that of its suppliers provide mutual support in the resolution of incidents.	1.車両メーカーは、そのサプライチェーン（下請け業者を含む）およびそれが直面する、より広範なリスクを深く理解している。車両メーカーは、サプライヤーの共同経営者、競合業者、国籍および下請け契約を結んでいる他の組織などを要因として考慮に入れている。この情報によって、そのリスクアセスメントおよび調達プロセスが形成される。 2.サプライチェーンリスク管理に対する車両メーカーのアプローチにおいて、能力および十分な資金力のある攻撃者によるサプライチェーンの破壊から生じるその車両型式に対するリスクが考慮されている。 3.車両メーカーは、サプライヤーと共有されるその車両型式の運用に不可欠な情報が 巧妙な攻撃から適切に保護されていると確信している。 4.車両メーカーは、サプライヤーに求めるセキュリティニーズを、相互に理解され、かつ契約に記載された方法で、明確に表現することができる。文書化された明確な共有責任モデルが存在する。 5.すべてのネットワーク接続および第三者とのデータ共有が効果的かつ相応に管理されている。 6.適切な場合、インシデントの解決において車両メーカーのインシデント 管理プロセスとそのサプライヤーのインシデント管理プロセスが相互支援を提供する。

補足　Annex5

	List of threats and corresponding mitigations	脅威および対応する軽減策のリスト
1	This annex consists of three parts. Part A of this annex describes the baseline for threats, vulnerabilities and attack methods. Part B of this annex describes mitigations to the threats which are intended for vehicle types. Part C describes mitigations to the threats which are intended for areas outside of vehicles, e.g. on IT backends.	本附則は3部から成る。本附則のパートAは、脅威、脆弱性および攻撃方法のベースラインを定める。本附則のパートBは、車両型式に向けられた脅威に対する軽減策を定める。パートCは、車両外の領域（例えばITバックエンド）に向けられた脅威に対する軽減策を定める。
2	Part A, Part B, and Part C shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers.	車両メーカーが実施するリスクアセスメントおよび軽減策においては、パートA、パートBおよびパートCを考慮するものとする。
3	The high-level vulnerability and its corresponding examples have been indexed in Part A. The same indexing has been referenced in the tables in Parts B and C to link each of the attack/vulnerability with a list of corresponding mitigation measures.	高レベルの脆弱性およびそれに対応する例は、パートAにおいて索引付けされている。パートBおよびパートCの表においても、各攻撃／脆弱性とそれに対応する軽減策のリストを関連付けるために、同じ索引付けが参照されている。
4	The threat analysis shall also consider possible attack impacts. These may help ascertain the severity of a risk and identify additional risks. Possible attack impacts may include: (a) Safe operation of vehicle affected; (b) Vehicle functions stop working; (c) Software modified, performance altered; (d) Software altered but no operational effects; (e) Data integrity breach; (f) Data confidentiality breach; (g) Loss of data availability; (h) Other, including criminality.	脅威分析においては、生じ得る攻撃の影響も考慮するものとする。これらはリスク重大度の確定および追加リスクの特定に役立つ可能性がある。生じ得る攻撃の影響には、下記が含まれる可能性がある： (a) 車両の安全な操作に影響が及ぶ。 (b) 車両機能が停止する。 (c) ソフトウェアが改変され、性能が変更される。 (d) ソフトウェアは変更されるが操作への影響はない。 (e) データ完全性の侵害。 (f) データ機密性の侵害。 (g) データ可用性の損失。 (h) その他（犯罪行為を含む）。

補足　Annex5 PartA

1. High level descriptions of threats and relating vulnerability or attack method are listed in Table A1.
1. 脅威の高レベルの記述ならびに関連している脆弱性または攻撃方法のリストを表A1に示す。

Table A1 List of vulnerability or attack method related to the threats

High level and sub-level descriptions of vulnerability/ threat					Example of vulnerability or attack method		
4.3.1 Threats regarding back-end servers related to vehicles in the field	フィールドの車両に関連するバックエンドサーバーに関する脅威	1	Back-end servers used as a means to attack a vehicle or extract data	車両を攻撃する手段またはデータを抽出する手段としてバックエンドサーバーが利用される	1.1	Abuse of privileges by staff (insider attack)	スタッフによる特権の悪用（インサイダー攻撃）
					1.2	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	サーバーへの不正なインターネットアクセス（例えば、バックドア、パッチが適用されていないシステムソフトウェアの脆弱性、SQL攻撃またはその他の手段によって可能となる）
					1.3	Unauthorized physical access to the server (conducted by for example USB sticks or other media connecting to the server)	サーバーへの不正な物理的アクセス（例えば、USB、またはサーバーに接続する他の媒体によって行われる）
		2	Services from back-end server being disrupted, affecting the operation of a vehicle	バックエンドサーバーからのサービスが中断され、車両の動作に影響を与える	2.1	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on	バックエンドサーバーへの攻撃による機能停止。例えば、サーバーと車両との相互作用ならびに車両が依存しているサーバーによるサービスの提供が妨げられる。
		3	Vehicle related data held on back-end servers being lost or compromised (“data breach”)	バックエンドサーバーに保持されていた車両関連データが損失または危殆化される（データ漏洩）	3.1	Abuse of privileges by staff (insider attack)	社員・職員による特権の悪用（インサイダー攻撃）
					3.2	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers	クラウドにおける情報損失。取扱いに注意を要するデータがサードパーティクラウドサービス提供者により保管されているときに攻撃または自己によりデータが損失される可能性がある。
					3.3	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	サーバーへの不正なインターネットアクセス（例えば、バックドア、パッチが適用されていないシステムソフトウェアの脆弱性、SQL攻撃、またはその他の手段によって可能となる）
					3.4	Unauthorized physical access to the server (conducted for example by USB sticks or other media connecting to the server)	サーバーへの不正な物理的アクセス（例えば、USB、またはサーバーに接続する他の媒体によって行われる）
					3.5	Information breach by unintended sharing of data (e.g. admin errors)	意図的でないデータ共有による情報漏洩（例：管理者のエラー）

補足　Annex 5　B, C　解釈

Part B. Mitigations to the threats intended for vehicles.

パートB 車両に向けられた脅威に対する軽減策

1. Mitigations for “Vehicle communication channels”
Mitigations to the threats which are related to "Vehicle communication channels" are listed in Table B1.

1. 車両通信路に関する軽減策
車両通信路に関する脅威に対する軽減策のリストを表B1に示す

Table B1 Mitigation to the threats which are related to "Vehicle communication channels"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation なりすましによるメッセージ偽装（隊列走行中の802.11p V2X通信、GNSSメッセージなど）	M10	The vehicle shall verify the authenticity and integrity of messages it receives 車両は、受信したメッセージの真正性と完全性を検証するものとする	車両が受信したメッセージまたはデータ（隊列走行中の802.11p V2X通信、GNSSメッセージなど）がなりすまされる脅威を想定して、車両は受信したメッセージの真正性と完全性を検証するものとする。 （例：V2X,規格による真正性を確保する等、各々の通信規格/方式に従ったセキュリティ対応をすること。その上でV2X,GNSS等の通信規格/方式で守り切れないなりすましが発生した場合にリスク事象にならないことを示すこと。）
4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road) シビル攻撃（あたかも路上に多くの車両が存在しているかのように他の車両になりすますため）	M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules) 暗号鍵の保管に対してセキュリティ対策を実施するものとする（例：HSMの使用）	車両が受信したメッセージまたはデータに対するシビル攻撃（あたかも路上に多くの車両が存在しているかのように他の車両になりすます）の脅威を想定して、暗号鍵の保管に対してセキュリティ車両は受信したメッセージの真正性と完全性を検証するものとする。 （例：想定脅威の対象である路車間/車車間通信に用いる暗号鍵は、セキュリティ対策を実施するものとする（例：HSMの使用など）、車車間/路車間通信のなりすましが発生した場合にリスク事象にならないことを示すこと）
5.1	Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream 通信路が車両に保存されているデータ/コードへのコード注入を許可する。例えば、改ざんされたソフトウェアバイナリが通信ストリームに注入される可能性がある。	M10	The vehicle shall verify the authenticity and integrity of messages it receives 車両は、受信したメッセージの真正性と完全性を検証するものとする	通信路が車両に保存されているデータ/コードへのコード注入を許可（例えば、改ざんされたソフトウェアバイナリが通信ストリームに注入される可能性）の脅威を想定して、車両は、受信したメッセージの真正性と完全性を検証するものとする。 （例：SSL/TLS、ファームウェアの署名検証など）
		M6	Systems shall implement security by design to minimize risks システムはリスクを最小限にするために設計によるセキュリティを実装するものとする	通信路が車両に保存されているデータ/コードへのコード注入を許可（例えば、改ざんされたソフトウェアバイナリが通信ストリームに注入される可能性）の脅威を想定して、システムはリスクを最小限にするために、設計によるセキュリティを実装するものとする。 （例：レギュレーション7.2項に従った開発を行った結果を車両に実装すること）

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
5.2	Communication channels permit manipulation of vehicle held data/code 通信路が車両に保存されているデータ／コードの改ざんを許可する。	M7	Access control techniques and designs shall be applied to protect system data/code システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする	通信路が車両に保存されているデータ／コードの改ざんを許可する脅威を想定して、システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。 （例：OTAや有線リプロに対して、アクセス制御、ファームウェアの署名検証。Diag通信に対して、リスク事象となるリクエストを受け付けないように制限を掛ける）
5.3	Communication channels permit overwrite of vehicle held data/code 通信路が車両に保存されているデータ／コードの上書きを許可する。			通信路が車両に保存されているデータ／コードの上書きを許可する脅威を想定して、システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。 （例：OTAや有線リプロに対して、アクセス制御、ファームウェアの署名検証。Diag通信に対して、リスク事象となるリクエストを受け付けないように制限を掛ける）
5.4 21.1	Communication channels permit erasure of vehicle held data/code 通信路が車両に保存されているデータ／コードの消去を許可する。			通信路が車両に保存されているデータ／コードの消去を許可する脅威を想定して、システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。 （例：OTAや有線リプロに対して、アクセス制御、ファームウェアの署名検証。Diag通信に対して、リスク事象となるリクエストを受け付けないように制限を掛ける）
5.5	Communication channels permit introduction of data/code to vehicle systems (write data code) 通信路が車両へのデータ／コードの導入（データ／コードの書き込み）を許可する。			通信路が車両に保存されているデータ／コードの書き込みを許可する脅威を想定して、システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。 （例：OTAや有線リプロに対して、アクセス制御、ファームウェアの署名検証。Diag通信に対して、リスク事象となるリクエストを受け付けないように制限を掛ける）
6.1	Accepting information from an unreliable or untrusted source 信頼できない、または信用できないソースからの情報を受け入れる。	M10	The vehicle shall verify the authenticity and integrity of messages it receives 車両は、受信するメッセージの真正性および完全性を検証するものとする	不正なソースからの情報を受け入れる脅威を想定して、受信するメッセージの真正性および完全性を検証するものとする。 （例：SSL/TLS、MACなど、接続先との認証機能を備えること）

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
6.2	Man in the middle attack / session hijacking 中間者攻撃/セッションハイジャック	M10	The vehicle shall verify the authenticity and integrity of messages it receives 車両は、受信するメッセージの真正性および完全性を検証するものとする	中間者攻撃やセッションハイジャックの脅威を想定して、受信するメッセージの真正性および完全性を検証するものとする。 （例：SSL/TLS、MACなど、接続先との認証機能を備えること。）
6.3	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway リプレイ攻撃。例えば、通信ゲートウェイに対する攻撃により攻撃者がゲートウェイのファームウェアまたはECUソフトウェアをダウングレードすることが可能になる。			リプレイ攻撃（例えば、通信ゲートウェイに対する攻撃により、攻撃者がゲートウェイのファームウェアまたはECUソフトウェアをダウングレードする）の脅威を想定して、受信するメッセージの真正性および完全性を検証するものとする。 （例：SSL/TLS、MACなど、接続先との認証機能を備えること。）
7.1	Interception of information / interfering radiations / monitoring communications 情報の傍受/干渉放射/通信の監視	M12	Confidential data transmitted to or from the vehicle shall be protected 車両に送信されるまたは車両から送信される機密データを保護するものとする。	通信メッセージの盗聴の脅威を想定し、車両と車外の間で送受信する機密データを保護するものとする。 （例：SSL/TLSなど）
7.2	Gaining unauthorized access to files or data ファイルまたはデータへの不正アクセス	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of Security Controls can be found in Security Controls can be found in OWASP システム設計およびアクセス制御によって、権限のない者が個人データまたはシステムの重要なデータにアクセスできないようにするものとする。セキュリティコントロールの例は、OWASPを参照。	車両システムのファイルまたはデータへの不正アクセスに関する脅威を想定し、権限のない者が個人データまたはシステムの重要なデータにアクセスできないようにするものとする。 （例：個人データのような機微情報、およびシステムの重要データに対するアクセス制御など）
8.1	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner 車両情報システムが正常な方法でサービスを提供できないように、当該システムに対しゴミのようなデータを大量に送信する。	M13	Measures to detect and recover from a denial of service attack shall be employed DoS攻撃の検知と復旧のための措置を講じるものとする	DoS攻撃の脅威を想定し、通信途絶時および復帰時の車両システムのふるまいを考慮した設計をするものとする （例：通信途絶のフェールセーフ設計で対応。復旧はフェールセーフで安全状態になった後、DoSがなくなり次第（通信回復次第）、正規メッセージを受信で自動復旧）

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
8.2	Black hole attack, disruption of communication between vehicles by blocking the transfer of messages to other vehicles ブラックホール攻撃。車両間通信を妨害するために、攻撃者が車両間のメッセージをブロックする。	M13	Measures to detect and recover from a denial of service attack shall be employed DoS攻撃の検出と復旧のための措置を講じるものとする	ブラックホール攻撃を想定し、通信途絶時および復帰時の車両システムのふるまいを考慮した設計をするものとする。 （例：通信途絶のフェールセーフ設計で対応。復旧はフェールセーフで安全状態になった後、ブラックホール攻撃がなくなり次第（通信回復次第）、正規メッセージを受信で自動復旧） ブラックホール攻撃：メッセージ転送をブロックすることによる通信が届かなくなること。 具体的には、攻撃ノードがメッセージを受信して応答パケットを偽装して送信することで、正規の受信ノードがメッセージを受信できなくなる。
9.1	An unprivileged user is able to gain privileged access, for example root access 非特権ユーザーが特権アクセスを取得できる。例えば、ルート権限。	M9	Measures to prevent and detect unauthorized access shall be employed 不正アクセスを防止し検知するための措置を講じるものとする	通信路経由で、ルート権限などの特権を取得される脅威を想定し、不正アクセスを防止し検知するための措置を講じるものとする。 （例：TLS/SSL）
10.1	Virus embedded in communication media infects vehicle systems 通信媒体に組み込まれたウイルスが車両システムに感染する。	M14	Measures to protect systems against embedded viruses/malware should be considered 埋め込まれたウィルス/マルウェアからシステムを保護する措置を講じるものとする	通信媒体に組み込まれたウィルスが車両システムに感染する脅威を想定し、ウィルス/マルウェアからシステムを保護する措置を講じるものとする。 （例：ファームウェアの署名検証、セキュアブート）
11.1	Malicious internal (e.g. CAN) messages 悪意のある内部メッセージ（例：CAN）	M15	Measures to detect malicious internal messages or activity should be considered 悪意のある内部メッセージやふるまいを検出する措置を講じるものとする	悪意のある車両内通信メッセージを受信する脅威を想定し、悪意のある車両内メッセージやふるまいを検出する措置を講じるものとする。 （例：メッセージフィルタリング、MAC 補足説明（ふるまい） ・静的なフィルタリングでの悪意メッセージの検出。 ・正規のECU間でのメッセージ認証を経由したメッセージしか受信・動作しないことで悪意のあるふるまいを検出

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
11.2	Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM) 悪意のあるV2Xメッセージ 例：インフラ対車両、または車車間メッセージ（例：CAM、DENM）	M10	The vehicle shall verify the authenticity and integrity of messages it receives 車両は、受信するメッセージの真正性と完全性を検証するものとする	悪意のあるV2Xメッセージを受信する脅威を想定し、受信するメッセージの真正性と完全性を検証する措置を講じるものとする。 （例：車両メーカーが公共インフラに対して独自に対策をすることはできない。このため、各々の通信規格/方式に応じたセキュリティ対応をすること。V2Xなりすましが発生した場合にリスク事象にならないことを示すこと）
11.3	Malicious diagnostic messages 悪意のある診断メッセージ			悪意のある診断メッセージを受信する脅威を想定し、受信するメッセージの真正性と完全性を検証する措置を講じるものとする。 （例：重要なメッセージ（リプロ）に対して、 ・認証 ・フィルタ ・改ざんチェック リプロ以外でリスクのあるメッセージに対して、 ・認証 ・リスク事象に至る診断メッセージを禁止 ・不正な値についてはアプリケーションでチェック・破棄）
11.4	Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier) 悪意のある専用メッセージ（例：通常はOEMまたはコンポーネント/システム/機能サプライヤから送信されるメッセージ）			悪意のある専用メッセージを受信する脅威を想定し、受信するメッセージの真正性と完全性を検証する措置を講じるものとする。 （例：デバックポートの削除、量産時に特殊モードを削除、アクセス制御） proprietary messages：テストや開発、生産時のために使用するメッセージと解釈

2. Mitigations for "Update process"
Mitigations to the threats which are related to "Update process" are listed in Table B2.

2.更新プロセスに関する軽減策
更新プロセスに関する脅威に対する軽減策のリストを表B2に示す

Table B2 Mitigations to the threats which are related to "Update process"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
12.1	Compromise of over the air software update procedures. This includes fabricating the system update program or firmware OTAソフトウェア更新手順の危殆化。これはシステム更新プログラムまたはファームウェアの偽造を含む。	M16	Secure software update procedures shall be employed セキュアなソフトウェアアップデートプロセスを採用するものとする	OTAソフトウェア更新手順の危殆化（システム更新プログラムまたはファームウェアの偽造を含む）を想定し、セキュアなソフトウェア更新手順を採用するものとする。 （例：OTAによるソフトウェア更新手順において、相互認証や改ざん検知、重要なOTA制御プログラムの改ざん対策などのセキュリティ対策を実施する）
12.2	Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware ローカル/物理的ソフトウェア更新手順の危殆化。これはシステム更新プログラムまたはファームウェアの偽造を含む。			ローカル/物理的なソフトウェア更新手順の危殆化（システム更新プログラムまたはファームウェアの偽造を含む）を想定し、セキュアなソフトウェア更新手順を採用するものとする。 （例：重要なソフトウェアについては標準的なソフトウェア更新手順において、認証や改ざん検知、重要な制御プログラムの改ざん対策などのセキュリティ対策を実施する）
12.3	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact 更新手順は損なわれていなくても、更新手順前にソフトウェアが改ざんされている（したがって破損している）			更新手順の前にソフトウェアが改ざんされている脅威を想定し、セキュアなソフトウェア更新手順を採用するものとする。 （例：ソフトウェア/ファームウェアの署名検証）
12.4	Compromise of cryptographic keys of the software provider to allow invalid update 無効な更新を許可するためのソフトウェア提供者の暗号鍵の危殆化。	M11	Security controls shall be implemented for storing cryptographic keys 暗号鍵の保管に対して、セキュリティコントロールを講じるものとする	無効な更新を許可するための暗号化の危殆化を想定し、暗号鍵の保管に対してセキュリティ対策を講じるものとする。 （例：暗号鍵に関する運用規定の遵守）

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
13.1	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features 重要なソフトウェア更新のロールアウトおよび/または顧客固有機能のロック解除を妨げるための、更新サーバーまたはネットワークに対するDoS攻撃。	M3	Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP セキュリティコントロールをバックエンドシステムに適用するものとする。バックエンドサーバーがサービス提供に不可欠である場合、システム停止を想定した復旧手段を備えるものとする。セキュリティコントロールの例は、OWASPを参照。	バックエンドサーバーへの攻撃による機能停止に対して、 バックエンドシステムのセキュリティ対策を行う。 またシステム停止時の復旧手順を予め備えておく。 （例：OWASP Top10対策、バックアップ・リストア手順確立）

3. Mitigations for "Unintended human actions facilitating a cyber attack"
Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack" are listed in Table B3.

3. サイバー攻撃を助長する意図しない人間の行動に関する軽減策
サイバー攻撃を助長する意図しない人間の行動に対する軽減策のリストを表B3に示す

Table B3 Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack 罪のない被害者（例：所有者、操作者またはメンテナンス技術者）が騙されて、意図せずにマルウェアをロードする行動または攻撃を可能にする行動をとる。	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege 最小のアクセス権限の原則に基づいて、ユーザ役割とアクセス権限を定義および管理するための方策を実装するものとする	意図せずマルウェアをロードする行動または攻撃に関与してしまう脅威を想定して、所有者、操作者またはメンテナンス技術者に対して、アクセス権限定義や管理する方策を講じるものとする。 （例：上記関連者に対する最小のアクセス権限設定）
15.2	Defined security procedures are not followed 定められたセキュリティ手順に従っていない。	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions 組織は、セキュリティ手順が定義され、セキュリティ機能の管理に関連する行動およびアクセスのログを含んで遵守されているものとする	正規の行動主体が、定められたセキュリティ手順に従っていない脅威を想定して、管理が必要なセキュリティ手順を定義し管理するものとする。 （例：開発時の機密情報などに対する運用マニュアル定義、運用記録など）

4. Mitigations for "External connectivity and connections"

Mitigations to the threats which are related to "external connectivity and connections" are listed in Table B4.

4. 外部接続および接続部に関する軽減策

外部接続および接続部に対する軽減策のリストを表B4に示す

Table B4 Mitigation to the threats which are related to "external connectivity and connections"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
16.1	Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile リモートキー、イモビライザー、充電パイルなど、システムを遠隔操作するための機能の改ざん	M20	Security controls shall be applied to systems that have remote access リモートアクセスを持つシステムにセキュリティコントロールを適用するものとする	リモートキー、イモビライザー、充電パイルなど、システムを遠隔操作するための機能の改ざんの脅威を想定して、セキュリティ対策を適用するものとする （例：各々の通信に対応した認証）
16.2	Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors) 車両テレマティクスの改ざん（例：温度測定を改ざんし、貨物ドアを遠隔解除する）			車両テレマティクスの改ざんによる脅威を想定して、セキュリティ対策を適用するものとする （例：各々の通信に対応した認証）
16.3	Interference with short range wireless systems or sensors 短距離無線システムまたはセンサへの干渉			短距離無線システムまたはセンサへの干渉による脅威を想定して、セキュリティ対策を適用するものとする （例：各々の通信に対応した認証、センサや接続認証が無いものに関してはフェールセーフ対策やシステムの冗長化）
17.1	Corrupted applications, or those with poor software security, used as a method to attack vehicle systems 改ざんされたアプリケーションまたはソフトウェアセキュリティが不十分なアプリケーションを、車両システムを攻撃する方法に使用する	M21	Software shall be security assessed, authenticated and integrity protected. Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle ソフトウェアは、セキュリティアセスメントおよび認証され、完全性が保護されるものとする。 車両にホストされることを意図もしくは予測されるサードパーティソフトウェアからのリスクを最小化するためにセキュリティコントロールを適用するものとする	改ざんされたアプリケーションやソフトウェアが利用される脅威を想定して、ソフトウェアは、セキュリティアセスメントおよび認証されて真正性と完全性を保護されているものとする。 車両にホストされることを意図もしくは予測されるサードパーティソフトウェアからのリスクを最小化するためにセキュリティコントロールを適用するものとする。 （例：ファームウェアの署名検証、配信アプリと車両システムソフトウェアのメモリ分離、ネットワーク分離）

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
18.1	External interfaces such as USB or other ports used as a point of attack, for example through code injection USBまたはその他のポートなどの外部インターフェースが、例えばコード注入の攻撃場所として利用される	M22	Security controls shall be applied to external interfaces 外部インタフェースにセキュリティコントロールを適用するものとする する	外部インターフェース（例：USBポート、OBDポート）に接続された装置が利用されて、例えばコード注入の攻撃場所として利用される脅威を想定して、外部インタフェースにセキュリティ対策を適用するものとする。 （例：不正機器に対するアクセス制御、ネットワーク分離）
18.2	Media infected with viruses connected to the vehicle ウイルスに感染した媒体を車両に接続する			外部インターフェース（例：USBポート、OBDポート）に接続された装置が利用されて、ウィルスに感染した媒体を車両に接続される脅威を想定して、外部インタフェースにセキュリティ対策を適用するものとする。 （例：不正機器に対するアクセス制御、ネットワーク分離） ※18.1と同じ
18.3	Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly) 例えば（直接的または間接的に）車両パラメータを改ざんするなどの攻撃を容易化するために、診断アクセス（例：OBDポートのドングル）が利用される			外部インターフェース（例：USBポート、OBDポート）に接続された装置が利用されて、車両パラメータを改ざんするなどの攻撃を容易化するために、診断アクセス（例：OBDポートのドングル）が利用される脅威を想定して、外部インタフェースにセキュリティ対策を適用するものとする。 （例：リスク事象となるリクエストを受け付けないように制限を掛ける、ネットワーク分離）

5. Mitigations for "Potential targets of, or motivations for, an attack "
Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack " are listed in Table B5.

5. 攻撃の潜在的標的または動機に関する軽減策
攻撃の潜在的標的または動機に対する軽減策のリストを表5に示す

Table B5 Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
19.1	Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software) 著作権または所有権のあるソフトウェアを車両システムから抽出する（製品の著作権侵害/ソフトウェア流出）	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。セキュリティコントロールの例は、OWASPを参照	車両に保管されたデータ（著作権または所有権のあるソフトウェア）が不正アクセスされることで漏洩する脅威を想定して、システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。 （例：リスク事象となるデータ/コードに対する暗号化、ECUデバックポートのアクセス制御）
19.2	Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc. 個人ID、支払いアカウント情報、アドレス帳情報、位置情報、車両の電子IDなど、所有者のプライバシー情報へ不正にアクセスする	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP システム設計およびアクセス制御によって、権限のない者が個人データまたはシステムの重要なデータにアクセスできないようにするものとする。セキュリティコントロールの例は、OWASPを参照。	車両に保管されたデータ（所有者のプライバシーデータ）が不正アクセスされることで漏洩する脅威を想定して、システム設計およびアクセス制御によって、権限のない者がアクセスできないようにするものとする。 （例：リスク事象となるデータに対する暗号化、データへのアクセス制限）
19.3	Extraction of cryptographic keys 暗号鍵を不正に取り出す	M11	Security controls shall be implemented for storing cryptographic keys e.g. Security Modules 暗号鍵の保管に対してセキュリティ対策を実施するものとする（例：セキュリティモジュール）	車両に保管されたデータ（暗号鍵）が不正アクセスされることで漏洩する脅威を想定して、暗号鍵の保管に対してセキュリティ対策を実施するものとする。 （例：セキュリティモジュール）

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
20.1	Illegal/unauthorised changes to vehicle's electronic ID 車両の電子IDを違法/不正に変更する	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP	車両に保管されたデータ/コード（車両の電子ID）が不正アクセスされることで改ざんされる脅威を想定して、アクセス制御技術と設計を適用するものとする。 （例：リスク評価結果に応じた対策として、データへのアクセス制限）
20.2	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend ID詐称。例えば、通行料金徴収システム、製造業者のバックエンドと通信する際に、ユーザーが他のIDを表示させたい場合。		システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。セキュリティコントロールの例は、OWASPを参照	車両に保管されたデータ/コード（通行料金収受システム、ユーザーIDなど）が不正アクセスされることで改ざんされる脅威を想定して、アクセス制御技術と設計を適用するものとする。 （例：リスク評価結果に応じた対策として、データへのアクセス制限、HSM）
20.3	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs) 監視システムを回避する行動（例：ODRトラッカーデータや実行回数のようなメッセージのハッキング/改ざん/ブロッキング）	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information	車両に保管されたデータ/コード（監視システム：ODRトラッカーデータや実行回数など）が不正アクセスされることで改ざんされる脅威を想定して、アクセス制御技術と設計を適用するものとする。 （例：リスク評価結果に応じた対策として、データへのアクセス制限）
20.4	Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.) 車両の運転データを偽るためにデータを改ざんする（例：走行距離、車速、走行方向等）		システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。セキュリティコントロールの例は、OWASPを参照 センサーまたは送信データに対するデータ改ざん攻撃は、さまざまな情報ソースからのデータを相互に関連付けることにって軽減できる	車両に保管されたデータ/コード（車両の運転データ：走行距離、車速、走行方向等）が不正アクセスされることで改ざんされる脅威を想定して、アクセス制御技術と設計を適用するものとする。 （例：リスク評価結果に応じた対策として、データへのアクセス制限） EDR、オドメーターなどを想定
20.5	Unauthorised changes to system diagnostic data システム診断データを不正に変更する			車両に保管されたデータ/コード（システム診断データ）が不正アクセスされることで改ざんされる脅威を想定して、アクセス制御技術と設計を適用するものとする。 （例：リスク評価結果に応じた対策として、データへのアクセス制限） DTCクリアなどを想定

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
21.1	Unauthorized deletion/manipulation of system event logs システムイベントログの不正な削除/改ざん	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。セキュリティコントロールの例は、OWASPを参照	車両に保管されたデータ/コード（システムイベントログ）が不正アクセスされることで削除/改ざんされる脅威を想定して、アクセス制御技術と設計を適用するものとする。 （例：リスク評価に応じた対策として、データへのアクセス制限） OEMやサプライヤが解析のために保管しているイベントログ
22.2	Introduce malicious software or malicious software activity 悪意のあるソフトウェアまたは悪意のあるソフトウェアアクティビティを導入する			車両に保管されたデータ/コード（悪意のあるソフトウェアまたは悪意のあるソフトウェアアクティビティ）が導入されることでマルウェアが導入される脅威を想定して、アクセス制御技術と設計を適用するものとする。 （例：リプロ時のアクセス制御、ファームウェアの署名検証、セキュアブート）
23.1	Fabrication of software of the vehicle control system or information system 車両制御システムまたは情報システムのソフトウェアの偽造			車両に保管されたデータ/コード（車両制御システムまたは情報システムのソフトウェア偽造）が上書きされることで、新たなソフトウェアの導入、または既存のソフトウェアが上書きされる脅威を想定して、アクセス制御技術と設計を適用するものとする。 （例：リプロ時のアクセス制御、ファームウェアの署名検証、セキュアブート）
24.1	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging DoS攻撃。例えば、大量のメッセージが送りつけられた結果、CANバスのあふれ、またはECUに障害が発生することによって、引き起こされる可能性がある	M13	Measures to detect and recover from a denial of service attack shall be employed DoS攻撃の検出と復旧のための措置を講じるものとする	車載ネットワークに対して、大量のメッセージが送りつけられた結果、CANバスのあふれ、またはECUに障害が発生する脅威を想定して、通信途絶時の車両システムのふるまいを考慮した設計をするものとする （例：通信途絶のフェールセーフ設計で対応） 8.1＝M13と同じ軽減策

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
25.1	Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc. ブレーキデータやエアバッグ展開しきい値など、車両の主要機能の設定パラメータを改ざんするために不正にアクセスする	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする。セキュリティコントロールの例は、OWASPを参照	車両に保管されたデータ/コード（車両の主要機能の設定パラメータ：ブレーキデータやエアバック展開しきい値など）が不正アクセスされることで改ざんされる脅威を想定して、アクセス制御技術と設計を適用するものとする。（例：データへのアクセス制御）
25.2	Unauthorized access to falsify charging parameters, such as charging voltage, charging power, battery temperature, etc. 充電電圧、充電電力、バッテリ温度などの充電パラメータを偽装するために不正にアクセスする			車両に保管されたデータ/コード（充電パラメータ：充電電圧、充電電力、バッテリ温度など）が不正アクセスされることで改ざんされる脅威を想定して、アクセス制御技術と設計を適用するものとする。（例：データへのアクセス制御）

6. Mitigations for "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened“

6. 十分に保護または堅牢化しない場合に悪用される可能性がある潜在的脆弱性に関する軽減策

Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened" are listed in Table B6.

十分に保護または堅牢化しない場合に悪用される可能性がある潜在的脆弱性に対する軽減策のリストを表6に示す

Table B6 Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
26.1	Combination of short encryption keys and long period of validity enables attacker to break encryption 暗号鍵が短く、長期間鍵の更新を行わないという状況の組み合わせにより、攻撃者は暗号を破ることができる	M23	Cybersecurity best practices for software and hardware development shall be followed ソフトウェアおよびハードウェア開発のサイバーセキュリティベストプラクティスに従うものとする	暗号鍵が短く、長期間鍵の更新を行わないことで暗号技術が危殆化される脅威を想定して、ソフトウェアおよびハードウェア開発のベストプラクティスに従うものとする。 （例：十分な鍵長、推奨暗号方式の使用）
26.2	Insufficient use of cryptographic algorithms to protect sensitive systems 機密性の高いシステムを保護する際に不十分な暗号アルゴリズムを利用する			機密性の高いシステムに対して不十分な暗号アルゴリズムを利用することで暗号技術が危殆化される脅威を想定して、ソフトウェアおよびハードウェア開発のベストプラクティスに従うものとする。 （例：推奨暗号方式の使用）
26.3	Using deprecated cryptographic algorithms 非推奨となる暗号アルゴリズムを使用する			非推奨の暗号アルゴリズムを利用することで暗号技術が危殆化される脅威を想定して、ソフトウェアおよびハードウェア開発のベストプラクティスに従うものとする。 （例：推奨暗号方式の使用）
27.1	Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack 攻撃が可能となるように設計された、または攻撃を停止するための設計基準を満たしていないハードウェアまたはソフトウェア			十分な保護または堅牢化されていないために、部品または供給品が危殆化されて車両が攻撃される脅威を想定して、ソフトウェアおよびハードウェア開発のベストプラクティスに従うものとする。 （例：CSMSに従った設計開発の実施、リスク評価に応じた対策の実装）

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
28.1	The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present ソフトウェアバグの存在は、悪用可能な潜在的脆弱性の根拠になり得る。これはとりわけ、既知の悪いコード／バグが存在しないことを検証し、かつ未知の悪いコード／バグの存在のリスクを減らすためのテストを、ソフトウェアに対し実施していない場合に当てはまる。	M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity testing with adequate coverage ソフトウェアおよびハードウェア開発のサイバーセキュリティベストプラクティスに従うものとする 適切なカバレッジのサイバーセキュリティテスト	ソフトウェアに対する不十分なテストの結果、ソフトウェアバグによる脆弱性の脅威を想定して、ソフトウェアおよびハードウェア開発のサイバーセキュリティベストプラクティスに従うものとする。 （例： ・セキュアコーディング（CERT-C等） ・侵入テスト ・脆弱性スキャン ・ファジングテスト ・既知の脆弱性を確認）
28.2	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit an attacker to access ECUs or gain higher privileges 開発の残り（例：デバッグポート、JTAGポート、マイクロプロセッサ、開発証明書、開発者パスワード・・・）を利用すると、ECUへのアクセスが可能となる、または、攻撃者がより高い特権を取得することが可能となる。			開発時の専用環境（デバッグポート、JTAGポート、マイクロプロセッサ、開発証明書、開発者パスワードなど）を利用したECUアクセスや特権取得される脅威を想定して、ソフトウェアおよびハードウェア開発のサイバーセキュリティベストプラクティスに従うものとする。 （例：開発用機能の無効化、アクセス制限）
29.1	Superfluous internet ports left open, providing access to network systems 不要なインターネットポートが開放されており、ネットワークシステムへのアクセスが可能となる。			ネットワーク設計の不備（不要なインターネットポート開放による、ネットワークシステムへの不正アクセス）による脅威を想定して、ソフトウェアおよびハードウェア開発のサイバーセキュリティベストプラクティスに従うものとする。 （例：メーカーの意図しないネットワークポート閉鎖）
29.2	Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages ネットワーク分離を回避し、制御を奪取する。 具体例は、任意のCANバスメッセージの送信などの悪意のある行為をするため、保護を回避して他のネットワークセグメントへのアクセスを取得するために、保護されていないゲートウェイまたはアクセスポイント（トラック-トレイラーゲートウェイなど）を使用することである。			ネットワーク設計の不備（ネットワーク分離の回避）による脅威を想定して、ソフトウェアおよびハードウェア開発のサイバーセキュリティベストプラクティスに従うものとする。また、システム設計およびシステム統合におけるサイバーセキュリティベストプラクティスに従うものとする。 （例：メッセージ認証、GWフィルタリング、接続先に対するアクセス制御）

7. Mitigations for "Data loss / data breach from vehicle "
Mitigations to the threats which are related to "Data loss / data breach from vehicle" are listed in Table B7.

7. 車両からのデータ損失/データ漏洩に関する軽減策

車両からのデータ損失/データ漏洩に対する軽減策のリストを表7に示す

Table B7 Mitigations to the threats which are related to "Data loss / data breach from vehicle"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
31.1	Information breach. Personal data may be breached when the car changes user (e.g. is sold or is used as hire vehicle with new hirers) 情報漏えい。車両のユーザ変更の際にパーソナルデータが漏えいする可能性がある（例：車両が販売されたり、もしくは新たな人に使用されたときなど）	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. パーソナルデータの保管に関してデータの完全性と機密性を保護するベストプラクティスに従うものとする	車両のユーザ変更（転売や、別ユーザの使用）によってパーソナルデータが漏えいする脅威を想定して、パーソナルデータの保管に関してデータの完全性と機密性を保護するベストプラクティスに従うものとする。 （例：廃棄や車両所有者が変更された場合に、 ・プライバシーデータを消去する機能の実装 ・それを実行する手順を明示した文書を作成し、ユーザー及びディーラー等の関係者に通達すること）

8. Mitigations for "Physical manipulation of systems to enable an attack"
Mitigation to the threats which are related to "Physical manipulation of systems to enable an attack" are listed in Table B8.

8. 攻撃を可能にするシステムの物理的な改ざんに関する軽減策

攻撃を可能にするシステムの物理的な改ざんに対する軽減策のリストを表8に示す

Table B8 Mitigations to the threats which are related to "Physical manipulation of systems to enable an attack"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
32.1	Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack 電子ハードウェアの不正操作。例：中間者攻撃を可能にするために車両に不正な電子ハードウェアを追加するなど。	M9	Measures to prevent and detect unauthorized access shall be employed 不正アクセスを防止および検知するための措置を講じるものとする	システムの物理的改ざん（車両に不正な機器取付、不正なハードウェアと交換、センサーが誤操作する改ざん）による脅威を想定して、不正アクセスを防止および検知するための措置を講じるものとする。

Part C. Mitigations to the threats outside of vehicles　パートC車外の脅威に対する軽減策

1. Mitigations for "Back-end servers"
Mitigations to the threats which are related to "Back-end servers" are listed in Table C1.

1. バックエンドサーバーに関する軽減策
バックエンドサーバーに対する軽減策のリストを表C1に示す

Table C1 Mitigations to the threats which are related to "Back-end servers

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
1.1 & 3.1	Abuse of privileges by staff (insider attack) スタッフによる特権の悪用（インサイダー攻撃）	M1	Security Controls are applied to back-end systems to minimise the risk of insider attack インサイダー攻撃のリスクを最小化するために、セキュリティコントロールをバックエンドシステムに適用するものとする	スタッフによる特権の悪用に対して、 特権・ID管理（ロールベース、職務分離）、操作ログ収集管理により抑止を図る
1.2 & 3.3	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) サーバーへの不正なインターネットアクセス（例えば、バックドア、パッチが適用されていないシステムソフトウェアの脆弱性、SQL攻撃またはその他の手段によって可能となる）	M2	Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP 不正アクセスを最小化するために、セキュリティコントロールをバックエンドシステムに適用するものとする。セキュリティコントロールの例は、OWASPを参照。	サーバーへの不正なインターネットアクセスに対して、 サーバの脆弱性対策、アプリケーション対策、通信制御を行う。 （例：公開脆弱性対策、通信制御、OWASP Top10の対策）
1.3 & 3.4	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server) サーバーへの不正な物理的アクセス（例えば、USB、またはサーバーに接続する他の媒体によって行われる）	M8	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data システム設計およびアクセス制御によって、権限のない者が個人データまたはシステムの重要なデータにアクセスできないようにするものとする。	サーバーへの不正な物理的アクセスにたいして、 システム設計およびアクセス制御による、個人またはシステムの重要データへのアクセス制限を行う
2.1	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on バックエンドサーバーへの攻撃による機能停止。例えば、サーバーと車両との相互作用ならびに車両が依存しているサーバーによるサービスの提供が妨げられる。	M3	Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP セキュリティコントロールをバックエンドシステムに適用するものとする。バックエンドサーバーがサービス提供に不可欠である場合、システム停止を想定した復旧手段を備えるものとする。 セキュリティコントロールの例は、OWASPを参照。	バックエンドサーバーへの攻撃による機能停止に対して、 バックエンドシステムのセキュリティ対策を行う。 またシステム停止時の復旧手順を予め備えておく。 （例：OWASP Top10対策、バックアップ・リストア手順確立）

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
3.2	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers クラウドにおける情報損失。取扱いに注意を要するデータがサードパーティクラウドサービス提供者により保管されているときに攻撃または自己によりデータが損失される可能性がある。	M4	Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance クラウドコンピューティングに関連するリスクを最小化するために、セキュリティコントロールを適用するものとする。セキュリティコントロールの例は、OWASPおよびNCSCクラウドコンピューティングガイダンスを参照。	クラウドにおける情報損失に対して、 クラウド側で用意されているセキュリティ機能の利用および利用しているセキュリティ機能がアクティブにされているか定期的に確認する
3.5	Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages) 意図的でないデータ共有による情報漏洩（例：管理者のエラー、ガレージにあるサーバーにデータを保管）	M5	Security Controls are applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP データ漏洩を防止するために、バックエンドシステムにセキュリティコントロールを適用するものとする。セキュリティコントロールの例は、OWASPを参照。	意図的でないデータ共有による情報漏洩に対して、 データの管理者のミスを防止する仕組みによるデータの漏洩防止。 （例：システム設計での織込み、運用操作ルール）

2. Mitigations for "Unintended human actions"
Mitigations to the threats which are related to "Unintended human actions" are listed in Table C2.

2. 意図しない人間の行動に関する軽減
意図しない人間の行動に対する軽減策のリストを表C2に示す

Table C2 Mitigations to the threats which are related to "Unintended human actions"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack 罪のない被害者（例：所有者、操作者またはメンテナンス技術者）が騙されて、意図せずにマルウェアをロードする行動または攻撃を可能にする行動をとる。	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege 最小のアクセス権限の原則に基づいて、ユーザ役割とアクセス権限を定義および管理するための方策を実装するものとする	罪のない被害者（例：所有者、操作者またはメンテナンス技術者）が騙されて、意図せずにマルウェアをロードする行動または攻撃を可能にする行動に対して、 最小のアクセス権限の原則に基づいて、ユーザ役割とアクセス権限を定義および管理するための方策を実装するものとする。 （例：操作者の役割定義、アクセス権限管理）
15.2	Defined security procedures are not followed 定められたセキュリティ手順に従っていない。	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions 組織は、セキュリティ手順が定義され、セキュリティ機能の管理に関連する行動およびアクセスのログを含んで遵守されているものとする	定められたセキュリティ手順違反に対して、 組織は、セキュリティ手順が定義され、セキュリティ機能の管理に関連する行動およびアクセスのログを含んで遵守されているものとする。 （例：ログ管理）

3. Mitigations for "Physical loss of data"
Mitigations to the threats which are related to "Physical loss of data" are listed in Table C3.

3. データの物理的な損失に関する軽減策
データの物理的な損失に対する軽減策のリストを表C3に示す

Table C3 Mitigations to the threats which are related to "Physical loss of data loss"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation	脅威と軽減策の解釈
30.1	Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft 第三者によって引き起こされる損害。 交通事故や盗難の場合、物理的な損傷によって機密データが損失または危殆化される可能性がある。	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. Example Security Controls can be found in ISO/SC27/WG5 パーソナルデータの保管に関してデータの完全性と機密性を保護するベストプラクティスに従うものとする。セキュリティコントロールの例は、ISO/SC27/WG5を参照。	交通事故や盗難などの物理的な損傷によって機密データが損失または危殆化される脅威を想定して、パーソナルデータの保管に関してデータの完全性と機密性を保護するベストプラクティスに従うものとする。（例：リスク評価結果に応じた対策として、データ暗号化、アクセス制御）
30.2	Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues DRM（デジタル著作権管理）コンフリクトによる損失。DRMの問題によりユーザーデータが削除される可能性がある。			DRMが、車両の安全に影響を与える可能性がないと考えます。
30.3	The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example) ITコンポーネントの摩耗や消耗により、機密データ（の完全性）が失われ、潜在的なカスケードの問題を引き起こす可能性がある。（例えば、鍵を変更する場合）			IT機器の故障に対して、 データが失われない対策を行う。 （バックアップ、二重化）