

サイバーセキュリティ、 ソフトウェアアップデート マネジメントシステムの 更新審査への取組

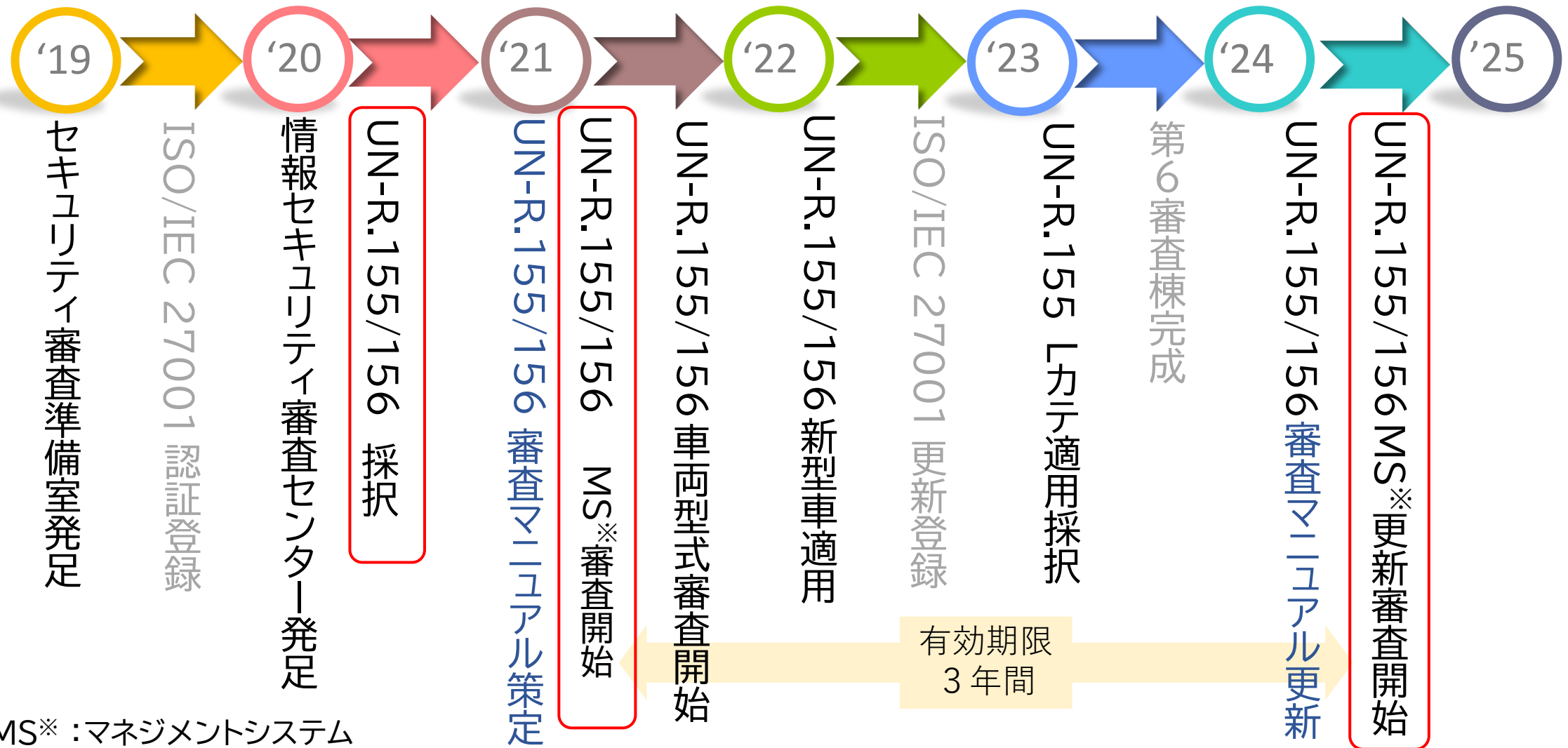
小林 一樹

自動車認証審査部 情報セキュリティ審査センター

講演内容

1. 情報セキュリティ審査センターの紹介
2. マネジメントシステムの基準と審査方法
3. 更新審査へ向けた取組
4. 更新審査結果
5. 今後へ向けて
6. CS/OTA IWGの議論内容紹介

情報セキュリティ審査センター(CSTセンター)



MS※ : マネジメントシステム

UN-R155/UN-R156 基準構成

自動車をつくる上での管理体制 【マネジメントシステムの審査】

- ・ 開発、生産、市場投入後までが範囲
 - ・ 年1回インシデント報告
 - ・ 3年ごと更新審査
- 自動車の特定改造等の許可に関する省令
 - 第4条第1項 告示で定める基準
 - 細目告示(特定改造) 第1条



個々の車両 【車両型式の審査】

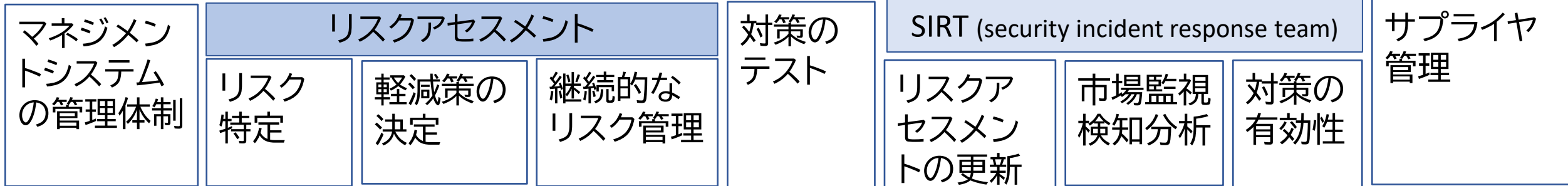
- 道路運送車両の保安基準
 - 第17条の2 電気装置
 - 細目告示(保安基準) (第1節)

自動車メーカーの
「しくみ（プロセス）」を審査

「しくみ（プロセス）」の結果
製作された車両の審査

UN-R155 サイバーセキュリティ マネジメントシステム要件

UN-R155 7.2.2



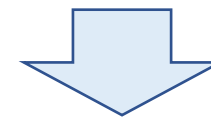
CSMSを確実に実施するための全社的な管理プロセス

車両開発において、守るべき資産の特定、想定脅威、影響度などから、リスク値を算出し、軽減策を適用するなどして、目標とするリスク値を達成するプロセス

車両に導入する軽減策が目的通り実装されていることを確認するプロセス

セキュリティインシデントの情報収集、検知、分析、軽減策が引き続き有効かどうかの調査のプロセス

サプライヤとの責任分担、セキュリティ管理のプロセス



年1回報告



【車両型式の審査】

個々の車両に実装されていることを確認

UN-R156ソフトウェアアップデート マネジメントシステム要件

UN-R156 7.1

SU文書の記録、 情報開示	SWバージョンの 管理	RXSWI Nの管理	更新対象 車両の 特定	更新ソフトウェア			更新の 通知	改ざん 防止など セキュリ ティ	OTA 更新の 安全 性
				相互依存 互換性確 認	法規 影響 確認	車両の 安全へ の影響			

ソフトウェア
更新の記録、
要求に応じ
て情報開示
するプロセス

更新するソ
フトウェア
のバージョ
ンを管理す
るプロセス

RXSWIN
の割振り
の管理

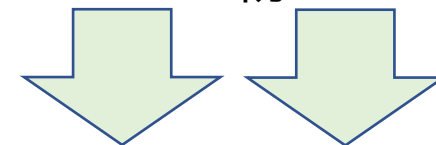
更新対象
車両の抽
出方法

更新するソフトウェアの互換性、
安全性、法規適合性を判断するプ
ロセス

更新を
ユーザに
知らせる
プロセス

更新ソフト
ウェアや
RXSWIN
の改ざん
防止

OTA更
新時の特
別な手順



個々の車両に実装され
ていることを確認

【車両型式の審査】

RXSWIN：RXはUN規則番号をさし、関連するソフト
ウェア群のバージョン情報を集約して管理できる

マネジメントシステム審査の流れ

申請者(自動車メーカー)

CS能力審査マニュアル

SU能力審査マニュアル

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
- CS/SU課題検討小WG
- R155審査マニュアル検討小WG

文書提出 QA

ヒアリング先リスト
タイムスケジュール

前相談

① 審査資料受領・リスト化

② 評価シート作成

③ QA

④ ヒアリング項目検討

⑤ 評価シートすり合わせ

⑥ ヒアリング先調整

⑦ 評価シートレビュー

⑧ ヒアリングリスト作成

⑨ 現地審査準備

⑩ 現地審査

⑪ 記録集計

⑫ 最終レビュー

2~3週

1~2週

書面審査

7.2.2.2 b) 方針 車両開発

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。これらのプロセスでは、附則5、パートAにおける脅威およびその他の関連脅威を考慮するものとする。

更新履歴
確認済項目数 0 / 20

書面審査
 リスク特定のための実施手順書がある

業務実施部署 マニュアル (1)

部門引き当てが必要な場合、提出済

業務処理組織図 マニュアル (2)

業務フロー マニュアル (3)

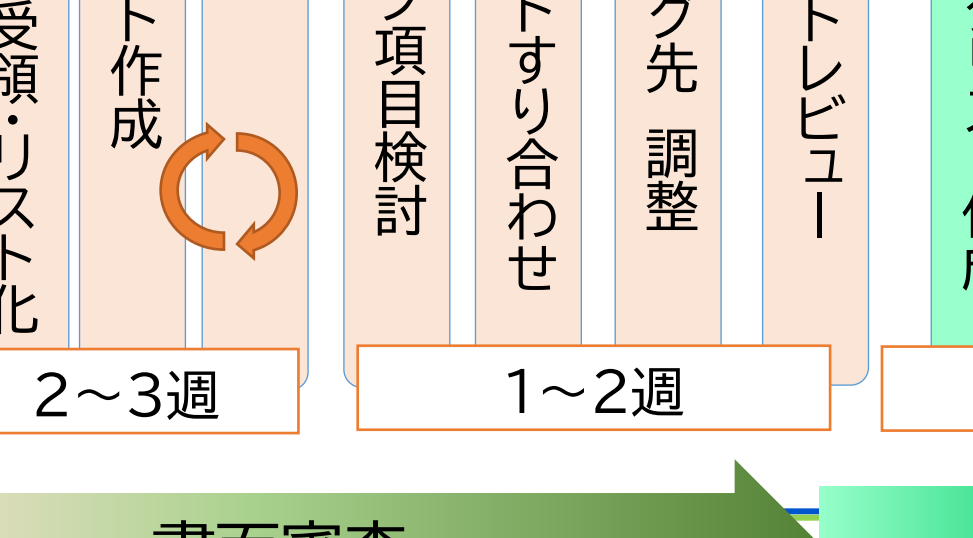
具体的な業務プロセス マニュアル (4)

車両へのリスク特定の目的に
 実作業者の作業方針を規定できるものとなっている

リスク特定に関してCSMSのマネジメント適用範囲が説明されている。 マニュアル (6)

想定脅威が明確に定義されている

車両型式ごとに想定脅威を確

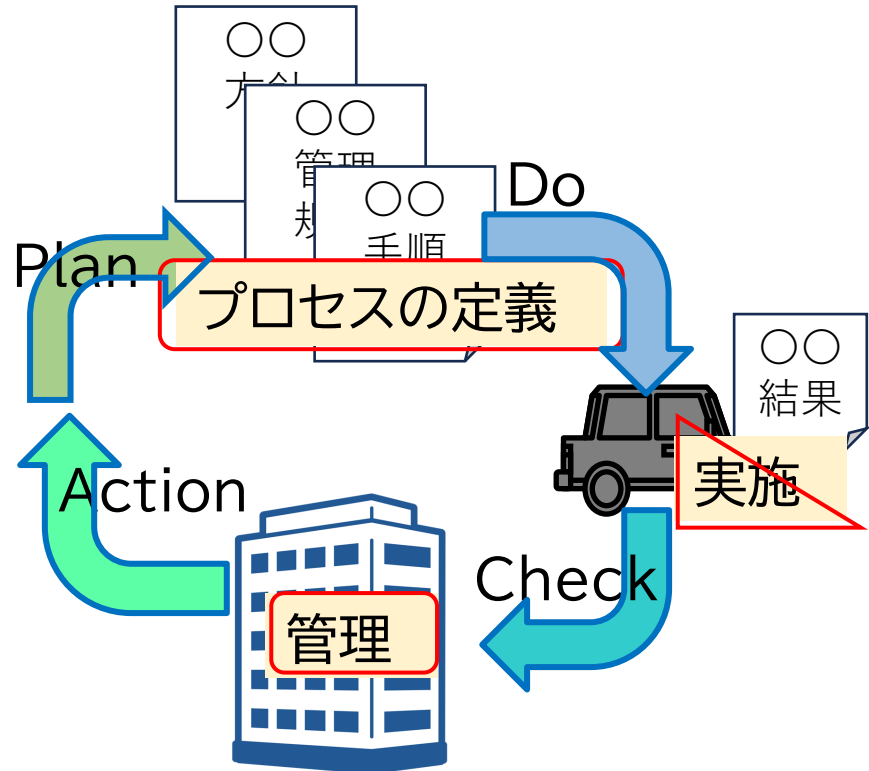


No.	ヒアリング内容	目的	文書(手順書/規定)または口頭による説明	達成/確認事項	備考	評価	備考
7.2.2.2 a)	サイバーセキュリティ管理のためにメーカーの組織内で使用するプロセス						
7.2.2.2 b)	情報セキュリティ政策の策定について、規定書を用いて説明してください。	情報セキュリティ政策の策定	情報セキュリティ政策	情報セキュリティ政策の策定	情報セキュリティ政策の策定		
7.2.2.2 c)	車両内の各分野/機能等としての役割について、規定書を用いて説明してください。	車両内の各分野/機能等としての役割	車両内の各分野/機能等としての役割	車両内の各分野/機能等としての役割	車両内の各分野/機能等としての役割		
7.2.2.2 d)	CSMSの運用と関係するシステムについて説明してください。	CSMSの運用と関係するシステム	CSMSの運用と関係するシステム	CSMSの運用と関係するシステム	CSMSの運用と関係するシステム		
7.2.2.2 e)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 f)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 g)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 h)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 i)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 j)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 k)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 l)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 m)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 n)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 o)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 p)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 q)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 r)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 s)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 t)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 u)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 v)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 w)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 x)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 y)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		
7.2.2.2 z)	特定のリスクの発生を防止するための手順書はどのように書かれ、誰が管理していますか。	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書	特定のリスクの発生を防止するための手順書		

マネジメントシステムの更新審査

R155, 156のマネジメントシステムとは

要件に適合するための組織的なプロセスおよび手順を定める体系的な (systematic) アプローチ



マネジメントシステムの審査ポイント

- 要件であるプロセスの構築
- 体系的なアプローチ
組織的なプロセス
PDCAサイクルなどによる改善

有効期限3年

初回審査の確認ポイント

更新審査の確認ポイント

マネジメントシステムの更新審査へ向けた取組

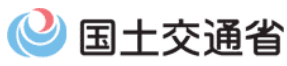
- 審査マニュアルの改訂
 - JASIC (自動車基準認証国際化研究センター)の会議体
 - 官民での法規解釈、審査手順の共有
- 評価シートチェック項目の見直し
 - 初回審査の結果を反映
 - 更新審査固有の項目を追加
- 現地審査の効率化

審査マニュアルの改訂

Cyber Security



国内採用WG



CS能力審査マニュアル

UN Regulation No. 155 on uniform provisions concerning the approval of vehicles with regards to cybersecurity management system

審

SU能力審査マニュアル

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
CS/SU残課題検討小WG
R155審査マニュアル検討小WG

1

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。これらのプロセスでは、附則5、パートAにおける脅威およびその他の関連脅威を考慮するものとする。

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・脅威分析等）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）

具体的には以下の記載された書面。

（リスク特定プロセスが複数の手順に分割されている場合、それぞれについて以下を説明のこと。）

- ・業務実施部署
- ・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者の各プロセスの入力情報と出力結果、結果を得るための具体的な作業内UN規則Annex 5, Part Aに規定する脅威を考慮することが含まれている）
- ・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（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らう、UN規則Annex 5, Part Aに規定する脅威に関し、明らかに車両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・リスク特定にあたり、CSMSのマネジメント適用範囲（関係の無いサンプルについては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

変更点

- ・表現の訂正
- ・初回審査を終え、解釈を再確認
- ・更新審査を想定した記述

15

追加

- ・マネジメントシステム審査手順
- ・マネジメントシステムの変更手続き
- ・R155の年次インシデント報告手順

評価シート

- 審査官がプロセスを確認
 - チェック形式
- 現地審査のヒアリング項目をピックアップ

Cyber Security

CS能力審査マニュアル

UN Regulation No. 155 on uniform provisions concerning the approval of vehicles with regards to cybersecurity management system

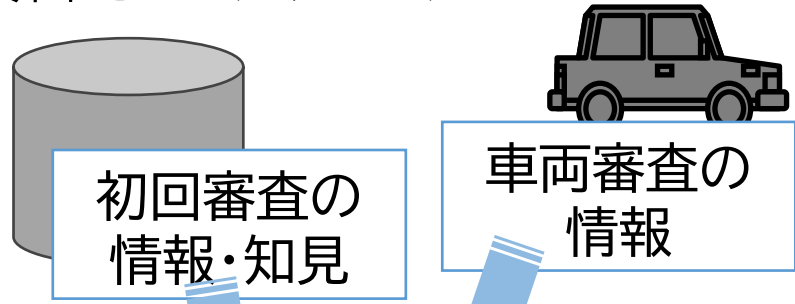
Software Update

SU能力審査マニュアル

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
- CS/SU残課題検討小WG
- R155審査マニュアル検討小WG



7.2.2.2 b) ... The processes used for the identification of risks to vehicle types. Within the relevant threats shall be considered: ...

更新履歴

確認事項

書類審査

リスク特定のための実施手順書がある

業務実施部署

部門引当が必要な場合、提出済

業務処理組織図

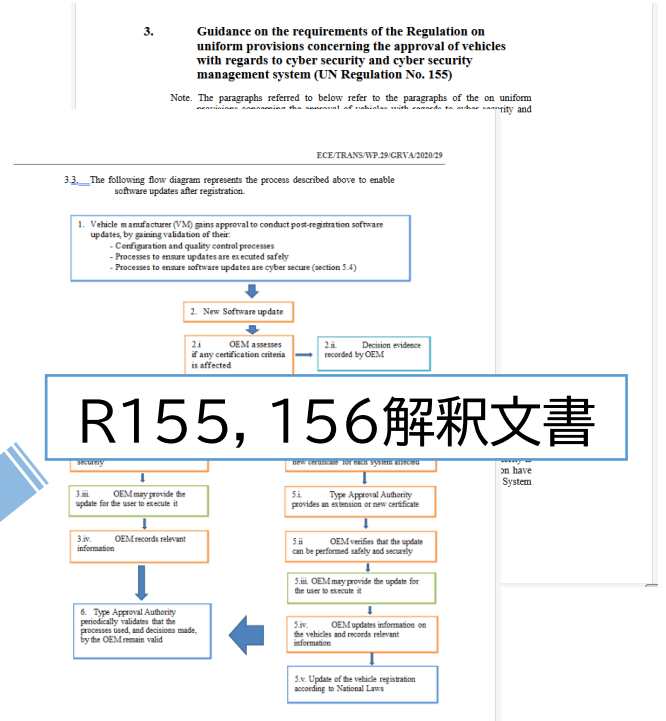
業務フロー

具体的な実務業務プロセス

実作業者の作業方針を規定できるものとなっている

リスク特定に関してCSMSのマネジメント適用範囲が説明されている。

想定脅威が明確に定義されている



専門機関等の情報

評価シートの中のチェック項目の見直し1

● 初回審査の内容を反映

- プロセスの実現方法の技術進化を反映

例) 手順をシステム化

例) プロセスの一部を外注

R156 7.1.6 ソフトウェア更新対象車両の特定

対象車両特定の手順書

実施組織

対象車両特定結果

...

R155 7.2.2.2 (g)市場監視

定期的な脅威情報取得が実施される

脅威情報取得を担当する者

(専任性、組織上の位置づけ)

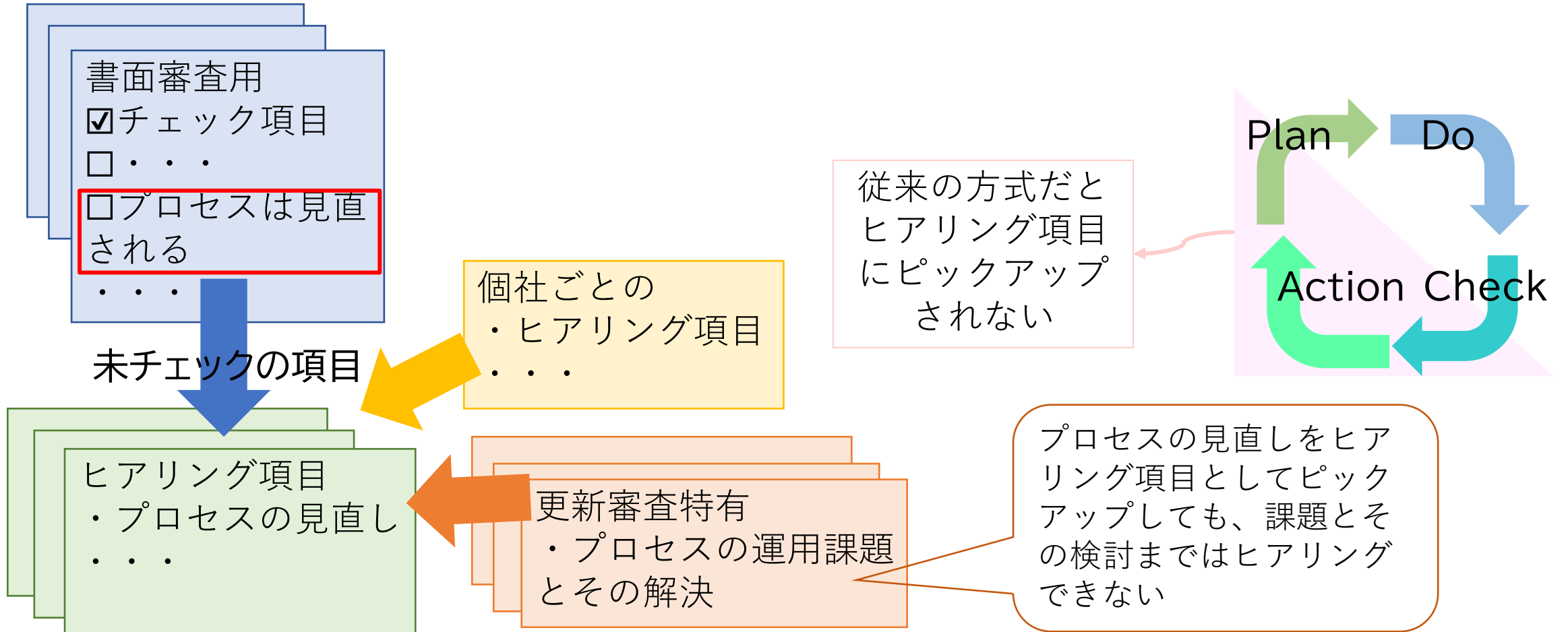
人数が不足しない

...

VSOC: Vehicle Security Operation Center 車両セキュリティ監視センター

評価シートの中のチェック項目の見直し2

●更新審査固有の項目を追加



現地審査

● ヒアリング先：プロセス実施部門

● 現地審査

- 部門ごとに実施
- 質問表に沿って質疑応答

ヒアリング対象部門(相談)

- CSMS(要件別)

Reg.項	ヒアリング概要	対象者(ご相談)
7.2.2.2(a)	・CSMSガバナンス ・CSMS関連規定文書管理	①情報セキュリティ統括部署 ②(車両)情報セキュリティ推進部署 ③(車両外各領域)情報セキュリティ推進部署 ④CSアセスメント部署(※)
7.2.2.2(b)(c)(d)(e)(f)	・リスクアセスメント ・CS試験 ・リスクアセスメントの維持(車両)	⑤CS 開発管理 / ⑥CS標準設計 / ⑦試験部署 ⑧ECU設計
7.2.2.2(b)(c)(d)(e)(f)	・リスクアセスメント ・リスクアセスメントの維持(車両外) バックエンドシステムの最新のリスクアセスメント結果をご説明ください	⑨各車両外システム構築部署
7.2.2.2(g)(h) 7.2.2.3	・SIRT活動全般	⑩SIRT統括推進部署 ⑪車両制御システム分野推進部署 ⑫車両品質主管部署(※) ⑬ECU設計部署(SIRT窓口) ⑭車両外各分野推進部署 ⑮車両外各分野品質主管部署(※) ⑯車両外各分野設計部署(SIRT窓口)
7.2.2.4	・車両ログによる攻撃検知	⑩SIRT統括推進部署
7.2.2.5	・サプライヤ管理(車両)	⑤CS 開発管理 ⑧ECU設計
7.2.2.5	・サプライヤ管理(車両外)	⑨各車両外システム構築部署

現地審査 時間割

時刻	時間(分)	項目	規程等呼称
11:40~12:50	70	昼休憩	-
12:50~13:20	30	ヒアリング	サービ部門 (SU) 7.1.1.11, 7.1.4.2
13:20~13:50	30	ヒアリング	ソフトウェア開発部門 (SU) 7.1.2, 7.1.1.6
13:50~14:05	15	休憩	-
14:05~15:35	90	ヒアリング	コネクテッドサービ部門 (CS) 7.2.2.2 (b), (c), (d)
15:35~15:50	15	休憩	-
15:50~16:50	60	ヒアリング	コネクテッドサービ部門 (SU) 7.1.1.2, 7.1.1.5, 7.1.1.7, 7.1.1.10
16:50~17:00	10	休憩	-
17:00~17:15	15	休憩	-
17:15~			
18:00~18:10	10	休憩	-
18:10~18:25	15	休憩	-
18:25~	10	送別	-
19:00~9:10	10	受入れ	-
9:00~9:10	10	送別	-
9:10~10:40	90	ヒアリング	ECU開発室 (SU) 7.1.1.2, 7.1.1.5, 7.1.1.7, 7.1.1.10, 7.1.3.3, 7.1.4.1
10:40~10:50	10	休憩	-

ヒアリング対象者を担当者へ
質問表の表現を工夫

① 情報セキュリティ推進室

ヒアリング内容が担当業務ではない場合は教えてください。

No	ヒアリング内容
7.2.2.2 a)	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
7.2.2.2 a)	1 情報セキュリティ統括の役割について、規定等を用いて説明してください。
7.2.2.2 a)	2 車両外の各分野推進部署としての役割について、規定等を用いて説明してください。
7.2.2.2 a)	3 情報を共有するための会議は定期的には実施されていますか。最近実施された会議の議事録を提示してください。
7.2.2.2 a)	4 C
7.2.2.2 a)	5 備考
7.2.2.2 b)	6 車両設計
7.2.2.2 b)	7
7.2.2.2 c)	8 UN-R155 Annex.5 PartAの脅威が想定されていますか。「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。」の脅威が想定される手順となっていることを説明してください。
7.2.2.2 c)	9 UN-R155 Annex.5 PartAの脅威以外を想定していますか。
7.2.2.2 c)	10 CSMSの適用範囲となる、システムについて説明してください。社内の情報システムを対象外となるものはありますか。
7.2.2.2 c)	11 車両外のシステムのリスク評価を実施するための手順書はどこに保管され、誰が参照できますか。
7.2.2.2 c)	特定されたリスクのアクセスメント、カテゴリ化および処理のために使用するプロセス
7.2.2.2 c)	リスク分類と処置に関する手順について、手順書に沿ってデモンストラレーションしてください。

質問表 (当日配布)



マネジメントシステムの更新審査 現地審査結果

● 複数社のマネジメントシステムの更新審査を実施

- ・ 集計は、初回12社 更新 6社

	UN-R155(CSMS)		UN-R156(SUMS)	
	初回	更新	初回	更新
1. 部門数	8.8 (1.3)	8.3 (1.9)	7.2 (1.8)	6.2 (1.1)
2. 時間 (h)	8.8 (1.7)	7.4 (1.0)	6.3 (1.6)	4.9 (1.0)
3. 設問数	84.7 (32.5)	81.3 (30.7)	45.5 (17.0)	56.7 (11.9)
4. のべ回答者数(人)	35.0 (14.6)	49.8 (29.6)	28.2 (11.1)	30.5 (9.5)

平均 (標準偏差)

「プロセスの運用課題とその解決」の回答例 (R.155)

- CSMS全体管理のプロセス (R155 7.2.2.2 (a))
 - 日々改善している。プロセスを根付かせることが重要
 - サイバー脅威は常に変更しているため、対応も常時変化させていくことが課題
 - プロセスの改善要望はなかったが、運用の工夫を行っている
 - 効率化について検討している
 - 今後の環境変化に追従していくことが課題
- リスクアセスメントのプロセス (R155 7.2.2.2 (b)(c)(d)(f))
 - 運用面、チェックシートなどの改善をしている
 - リスクアセスメントの実施タイミングを協議している
 - 伝わりやすい改善履歴の残し方など改善している
 - 効率化、軽減策のベストプラクティスの展開
- SIRTのプロセス (R155 7.2.2.2 (g)(h), 7.2.2.3, 7.2.2.4)
 - インシデント報告書様式を作成し、報告をしやすくした
 - 脆弱性リスト管理、トリアージの業務量が課題。AIの活用などを検討
 - インシデント訓練を実施
 - 手順の明確化

「プロセスの運用課題とその解決」の回答例 (R.156)

- 管理サーバーへの更新登録漏れがあったため見直し部署を新設し改善
- SU型式対象かどうかの詳細判断フローを策定
- 従来の設計資料とは別にエビデンス保管一元化を実施
- 構築したプロセスについて教育、e-learningを実施
- SU実行時のプロセスフローを法規影響の有無にかかわらず一本化した
- RXSWINの強制適用に対する社内整備
- 既存のMS体系に基づき、日常の改善を行っている。
- ソフトウェア更新の量が多いので、管理が課題
- 以前から実施していることだが、エビデンスを残していくことは良い
- 有線更新の場合などの手作業によるミスが課題
- SUMS以前よりこのプロセスは存在していたが、プロセスとして定義されたことによる意識づけが課題。
- 車両への書き間違い事例に対し原因調査と対策を行った
- システム化されているため課題はない
- 有線更新の場合などの手作業によるミスが課題

更新審査への取組と今後

● 審査マニュアルの改訂

- 実態に沿った内容への改訂
- 表現の明確化



審査・受審双方の共通理解

+ 法規対応

必要に
応じ実施

● 評価シート（チェック項目）の見直し

- これまでの審査情報の反映
- 技術など実態の反映
- 審査マニュアルの反映



的確な審査
審査官の力量向上

● 審査手順の見直し



審査の効率化

継続的に
実施

マネジメントシステムの審査

● プロセスが要件である意味

- R155サイバーセキュリティ：未来永劫有効な軽減策はない
- R156ソフトウェア更新：ソフトウェア、通信技術の進化により手段が定められない

⇒ 変化を取り込むプロセスであること

● プロセスは改善される

- プロセスに正解はない
- 技術の進化、社会や組織、ビジネスの変化

マネジメントシステムの審査への要求

- ◆ プロセスの要件適合性を的確に判断
 - プロセスの変化、技術の変化に追従できる
- ◆ マネジメントシステムの有効性の判断

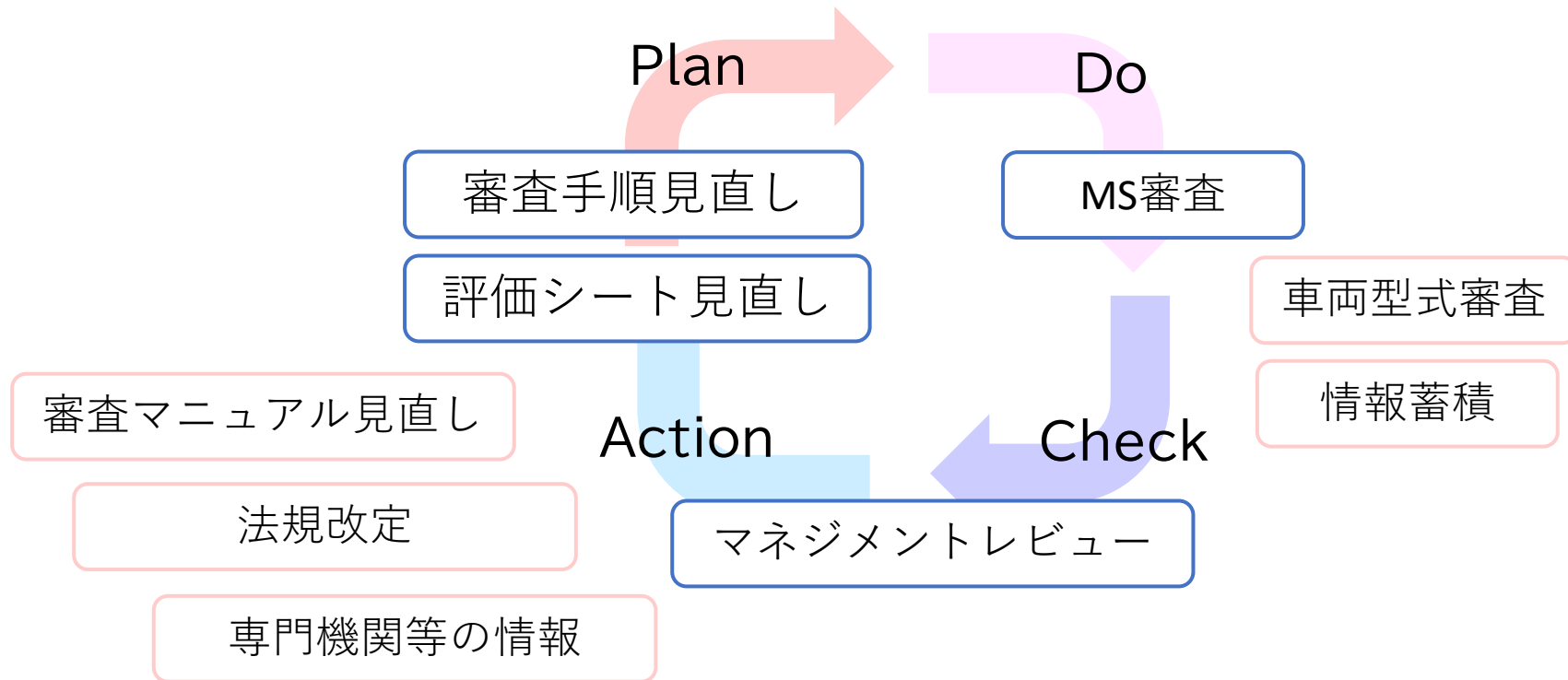


UN-R MS審査の
マネジメントシステム

情報セキュリティ審査センターのMS審査マネジメントシステム

● UN-R MS審査のマネジメントシステムを構築

- ISO/IEC 17021 マネジメントシステムの審査及び認証を行う機関に対する要求事項 に準拠



● UN-R155,156だけでなくほかの「マネジメントシステム」の審査も適用

UN-R 155 サイバーセキュリティ

● マルチステージビークル

- 架装車両のサイバーセキュリティ要件について検討
- 部品認証
 - 部品メーカーなどサプライヤがR155のマネジメントシステム認証を受ける場合の課題を検討中

● ADSへの対応

- 遠隔操作を行うオペレーションセンターから車両へ情報を伝達する際のサイバーセキュリティ要件について検討

● マネジメントシステムの認可と車両の認可当局の一致性

- マネジメントシステムの認可当局と車両の認可当局は同じであるべきではないか、について議論

UN-R 156 ソフトウェアアップデート

● RXSWINの義務化

- RXSWINによるソフトウェア管理を行わなければ、市場で法規影響のあるソフトウェア更新ができない
- 第197回 WP.29 (2025/11/11-14) で採択

● 使用過程車のソフトウェア更新の法規適合性

- 使用過程車を市場でソフトウェア更新する場合、認可された仕様とは機能が異なることがある。認可の拡大が必要ではないかという議論
- R156に限る課題ではないため、IWVTAなどで議論する必要がある