TRIAS 17(2)-R155-01

サイバーセキュリティシステム試験
（協定規則第 155 号（同規則の規則 7.3.（7.3.1.を除く）に限る））

1. 総則

サイバーセキュリティシステム試験の実施にあたっては、「道路運送車両の保安基準の細目を定める告示」（平成 14 年国土交通省告示第 619 号）に定める「協定規則第 155 号の技術的な要件（同規則の規則 7.3.（7.3.1.を除く。）に限る。）」の規定及び本規定によるものとする。

2. 試験条件

自動車での実車試験及び書面等の説明により試験を行うことができる。

3. 試験記録及び成績

試験記録及び成績は、付表の様式に記入する。

3.1. 当該試験時において該当しない箇所には斜線を引くこと。

3.2. 記入欄は、順序配列を変えない範囲で伸縮することができ、必要に応じて追加してもよい。

3.3. 試験記録及び成績は、日本語又は英語のみの記載でもよい。

付表
Attached Table

サイバーセキュリティシステム試験記録及び成績
CYBER SECURITY TEST DATA RECORD FORM
(協定規則第155号(規則7.3.車両型式に関する要件(規則7.3.1.を除く)))
1958 Agreement of the United Nations Economic Commission for Europe Regulation No.155
(Restricted to paragraphs 7.3. Requirements for vehicle types (Except for paragraphs 7.3.1.))

試験期日	年	月	日	試験場所	試験担当者
Test Date	Y.	M.	D.	Test Site	Tested by

○改訂
Series

改訂番号	補足改訂番号
Series No.	Supplement No.

○ 試験自動車
Test Vehicle

車名	型式	類別	車台番号
Make	Type	Variant	Chassis No.

○ 試験成績
Test Results

要件 Requirements		適合性 Conformity
段落 Paragraph	内容 Contents	
7.3.2.	The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks.	
7.3.3.	The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.	pass ／ fail
7.3.4.	The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented. In particular, for type approvals prior to 1 July 2024, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority.	pass ／ fail
7.3.5.	The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.	pass ／ fail

7.3.6.	The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.	pass ／ fail
7.3.7.	The vehicle manufacturer shall implement measures for the vehicle type to:	
(a)	detect and prevent cyber-attacks against vehicles of the vehicle type;	pass ／ fail
(b)	support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;	pass ／ fail
(c)	provide data forensic capability to enable analysis of attempted or successful cyber-attacks.	pass ／ fail
7.3.8.	Cryptographic modules used for the purpose of this Regulation shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use.	pass ／ fail

備考

Remarks