TRIAS 99-R155-01

サイバーセキュリティ業務管理システム試験
（協定規則第 155 号（同規則の規則 7.2.に限る））

1. 総則

サイバーセキュリティ業務管理システム試験の実施にあたっては、「自動車の特定改造等の許可に関する技術上の基準に関する細目等を定める告示」（令和 2 年国土交通省告示第 787 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 7.2.に限る。）」の規定及び本規定によるものとする。

2. 試験条件

書面及び現地審査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

サイバーセキュリティ業務管理システム試験記録及び成績
CYBER SECURITY MANAGEMENT SYSTEM TEST DATE RECORD FORM
（協定規則第155号（規則7.2.サイバーセキュリティ業務管理システムに関する要件））
1958 Agreement of the United Nations Economic Commission for Europe Regulation No.155
(Restricted to paragraphs 7.2. Requirements for the Cyber Security Management System)

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.

○ 試験対象業務管理システム
Test Management System

社名	業務管理システムの名称
Manufacturer	Names of Management System

○ 試験成績
Test Results

※ 各項目について適合性を裏付ける資料のリストを添付のこと。書式は任意で構わない。
Attach a list of supporting material for each paragraph. The format does not matter.

要件 Requirements		適合性 Conformity
段落 Paragraph	内容 Contents	
7.2.1.	For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.	
7.2.2.	The Cyber Security Management System shall cover the following aspects:	
7.2.2.1.	The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases: - Development phase; - Production phase; - Post-production phase.	pass ／ fail
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:	
(a)	The processes used within the manufacturer's organization to manage cyber security;	pass ／ fail
(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.	pass ／ fail ※1
(c)	The processes used for the assessment, categorization and treatment of the risks identified;	pass ／ fail

	(d)	The processes in place to verify that the risks identified are appropriately managed;	pass ／ fail
	(e)	The processes used for testing the cyber security of a vehicle type;	pass ／ fail
	(f)	The processes used for ensuring that the risk assessment is kept current;	pass ／ fail
	(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;	pass ／ fail
	(h)	The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks;	pass ／ fail
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.	pass ／ fail
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;	pass ／ fail
	(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.	pass ／ fail
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.	pass ／ fail

※1 附則5パートAの各項目も確認すること。
Also check each item in Annex 5 Part A.

備考
Remarks

附則5
Annex5

Part A. Vulnerability or attack method related to the threats

1. High level descriptions of threats and relating vulnerability or attack method are listed in Table A1.

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*		Included in analysis
4.3.1 Threats regarding back-end servers related to vehicles in the field	1	Back-end servers used as a means to attack a vehicle or extract data	1.1	Abuse of privileges by staff (**insider attack**)	inclded / not included
			1.2	**Unauthorized internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	inclded / not included
			1.3	**Unauthorized physical access** to the server (conducted by for example USB sticks or other media connecting to the server)	inclded / not included
	2	Services from back-end server being disrupted, affecting the operation of a vehicle	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	inclded / not included
	3	Vehicle related data held on back-end servers being lost or compromised ("data breach")	3.1	Abuse of privileges by staff (**insider attack**)	inclded / not included
			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	inclded / not included
			3.3	**Unauthorized internet access to the server** (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	inclded / not included
			3.4	**Unauthorized physical access to the server** (conducted for example by USB sticks or other media connecting to the server)	inclded / not included
			3.5	**Information breach** by unintended sharing of data (e.g. admin errors)	inclded / not included

4.3.2 Threats to vehicles regarding their communication channels	4	Spoofing of messages or data received by the vehicle	4.1	**Spoofing of messages** by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)	inclded / not included
			4.2	**Sybil attack** (in order to spoof other vehicles as if there are many vehicles on the road)	inclded / not included
	5	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	5.1	Communications channels permit **code injection**, for example tampered software binary might be injected into the communication stream	inclded / not included
			5.2	Communications channels permit **manipulate** of vehicle held data/code	inclded / not included
			5.3	Communications channels permit **overwrite** of vehicle held data/code	inclded / not included
			5.4	Communications channels permit **erasure** of vehicle held data/code	inclded / not included
			5.5	Communications channels permit introduction of data/code to the vehicle (write data code)	inclded / not included
	6	Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	6.1	Accepting information from an **unreliable or untrusted source**	inclded / not included
			6.2	**Man in the middle** attack/ session hijacking	inclded / not included
			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	inclded / not included
	7	Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	7.1	**Interception of information** / interfering radiations / monitoring communications	inclded / not included
			7.2	Gaining **unauthorized access** to files or data	inclded / not included
	8	Denial of service attacks via communication channels to disrupt vehicle functions	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	inclded / not included
			8.2	**Black hole attack**, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles	inclded / not included
	9	An unprivileged user is able to gain privileged access to vehicle systems	9.1	An unprivileged user is able to **gain privileged access**, for example root access	inclded / not included
	10	Viruses embedded in communication media are able to infect vehicle systems	10.1	**Virus** embedded in communication media infects vehicle systems	inclded / not included

	11	Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	11.1	Malicious **internal** (e.g. CAN) **messages**	inclded / not included
			11.2	Malicious **V2X messages,** e.g. infrastructure to vehicle or vehicle–vehicle messages (e.g. CAM, DENM)	inclded / not included
			11.3	Malicious diagnostic messages	inclded / not included
			11.4	Malicious **proprietary messages** (e.g. those normally sent from OEM or component/system/function supplier)	inclded / not included
4.3.3. Threats to vehicles regarding their update procedures	12	Misuse or compromise of update procedures	12.1	Compromise of **over the air software update procedures.** This includes fabricating the system update program or firmware	inclded / not included
			12.2	Compromise of **local/physical software update procedures.** This includes fabricating the system update program or firmware	inclded / not included
			12.3	The **software** is **manipulated before the update process** (and is therefore corrupted), although the update process is intact	inclded / not included
			12.4	**Compromise** of cryptographic keys of the software provider **to allow invalid update**	inclded / not included
	13	It is possible to deny legitimate updates	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	inclded / not included
4.3.4 Threats to vehicles regarding unintended human actions facilitating a cyber attack	15	Legitimate actors are able to take actions that would unwittingly facilitate a cyber–attack	15.1	Innocent victim (e.g. owner, operator or maintenance engineer) being **tricked into taking an action** to unintentionally load malware or enable an attack	inclded / not included
			15.2	**Defined security procedures** are not followed	inclded / not included
4.3.5 Threats to vehicles regarding their external connectivity and connections	16	Manipulation of the connectivity of vehicle functions enables a cyber–attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications	16.1	Manipulation of **functions designed to remotely operate systems**, such as remote key, immobilizer, and charging pile	inclded / not included
			16.2	**Manipulation of vehicle telematics** (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)	inclded / not included
			16.3	Interference with **short range wireless systems** or sensors	inclded / not included
	17	Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems	17.1	**Corrupted applications**, or those with poor software security, used as a method to attack vehicle systems	inclded / not included

	18	Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	18.1	**External interfaces** such as USB or other ports used as a point of attack, for example through code injection	inclded / not included
			18.2	Media infected with a **virus** connected to a vehicle system	inclded / not included
			18.3	**Diagnostic access (e.g. dongles in OBD port)** used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	inclded / not included
4.3.6 Threats to vehicle data/code	19	Extraction of vehicle data/code	19.1	Extraction of copyright or proprietary software from vehicle systems (product **piracy**)	inclded / not included
			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.	inclded / not included
			19.3	Extraction of cryptographic keys	inclded / not included
	20	Manipulation of vehicle data/code	20.1	Illegal/unauthorized changes to **vehicle's electronic ID**	inclded / not included
			20.2	**Identity fraud.** For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend	inclded / not included
			20.3	Action to **circumvent monitoring systems** (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)	inclded / not included
			20.4	Data manipulation to **falsify vehicle's driving data** (e.g. mileage, driving speed, driving directions, etc.)	inclded / not included
			20.5	Unauthorized changes to **system diagnostic data**	inclded / not included
	21	Erasure of data/code	21.1	Unauthorized deletion/manipulation of **system event logs**	inclded / not included
	22	Introduction of malware	22.2	Introduce **malicious software** or malicious software activity	inclded / not included
	23	Introduction of new software or overwrite existing software	23.1	**Fabrication of software** of the vehicle control system or information system	inclded / not included
	24	Disruption of systems or operations	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	inclded / not included
	25	Manipulation of vehicle parameters	25.1	Unauthorized access of **falsify the configuration parameters** of vehicle's key functions, such as brake data, airbag deployed threshold, etc.	inclded / not included
			25.2	Unauthorized access of **falsify the charging parameters**, such as charging voltage, charging power, battery temperature, etc.	inclded / not included

4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	26	Cryptographic technologies can be compromised or are insufficiently applied	26.1	Combination of short **encryption keys** and long period of validity enables attacker to break encryption	inclded / not included
			26.2	Insufficient use of cryptographic algorithms to protect sensitive systems	inclded / not included
			26.3	Using already or soon to be deprecated **cryptographic algorithms**	inclded / not included
	27	Parts or supplies could be compromised to permit vehicles to be attacked	27.1	**Hardware or software, engineered to enable an attack** or fails to meet design criteria to stop an attack	inclded / not included
	28	Software or hardware development permits vulnerabilities	28.1	**Software bugs**. 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	inclded / not included
			28.2	**Using remainders** from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit access to ECUs or permit attackers to gain higher privileges	inclded / not included
	29	Network design introduces vulnerabilities	29.1	**Superfluous internet ports left open**, providing access to network systems	inclded / not included
			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	inclded / not included
	31	Unintended transfer of data can occur	31.1	Information breach. Personal data may be leaked when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)	inclded / not included
	32	Physical manipulation of systems can enable an attack	32.1	**Manipulation of electronic hardware**, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack **Replacement of authorized electronic hardware** (e.g., sensors) with unauthorized electronic hardware **Manipulation of the information** collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox)	inclded / not included

備考

Remarks