

ECU	Requirements of Information Provision for Cybersecurity Examination		1/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

関係各部 御中  
To departments concerned

Confidential level	Protected 関係者外秘	原紙保管 Storage of original	-
		コピー保管 Storage of copy	-

<b>サイバーセキュリティ審査 情報提供要件書</b> <b>Requirements of Information Provision for Cybersecurity Examination</b>		制御電子プラットフォーム開発部 制御ネットワーク・アーキ開発室 System Network & Architecture Development Dept. E/E Architecture Development Div.							
		No. SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a							
		承認 Approved 河井 Kawai	調査 Checked 平林 Hirabayashi	作成 Created 尾崎 Ozaki	May 17, 2021				
		<div style="border: 1px solid black; padding: 2px; text-align: center;">           Omission of signature (approved electronically)         </div>							
適用 / Scope	UN-R155 審査を受ける車両の電気・電子部品 Electrical or electronic components of vehicles taking the UN-R155 examination								
変更履歴 / Revision records	(1) <span style="border: 1px solid black; padding: 2px;">新規 / New</span> (2) 変更 / Revision								
	Version	Major revision contents	Date	Revised by					
	a00-00-a	初版発行 / Initial version	May 17, 2021	46F3G Ozaki					
特記 / Note	<p>➤ 本文書によって、ECU 設計部署やサプライヤーに、情報の提供を要求する。 本書は、設計や評価のための仕様書ではない。 This document requests ECU Design Departments and suppliers to provide information. This document isn't design specifications or evaluation specifications.</p> <p>➤ 本文書は iSpirit (Electronics_Spec &gt; Cybersecurity) からダウンロードする。 Please download this document from iSpirit (Electronics_Spec &gt; Cybersecurity)</p> <p>➤ 海外事業体/ボデーメーカー/協業先 OEM/サプライヤー/委託先には、目的（外設申/RFQ 等）に沿った機密保持に係る契約を締結している場合のみ展開可。 This document may be disclosed to Toyota's overseas entities, body makers, partner OEMs, suppliers and outsourcing contractors only if the confidentiality agreements suitable for purposes such as RDDP, RFQ, etc. are valid.</p> <p>➤ サイバーセキュリティ問合せ窓口 / Contact Point of Cybersecurity Mail : <a href="mailto:epf-sec-sp@mega.tec.toyota.co.jp">epf-sec-sp@mega.tec.toyota.co.jp</a></p>								

ECU	Requirements of Information Provision for Cybersecurity Examination		2/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

## 変更履歴 / Revision Records

Mark	Version	Item	Revision contents
-	a00-00-a	All items	新規作成 / Newly created

ECU	Requirements of Information Provision for Cybersecurity Examination		3/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

## 目次 / Contents

変更履歴 / Revision Records.....	2
目次 / Contents.....	3
1. はじめに / Introduction.....	4
1.1. 目的 / PURPOSE.....	4
1.2. 適用範囲 / SCOPE .....	4
1.3. 関連文書 / RELATED DOCUMENTS.....	4
1.4. 関係者の定義 / DEFINITION OF ORGANIZATIONS AND DEPARTMENTS.....	6
2. 審査のための情報提供 / Information Provision for Examination .....	7
2.1. 要求の一覧 / LIST OF REQUIREMENTS.....	7
2.2. 要求 / REQUIREMENTS.....	8
2.2.1. テスト 1 / Test 1 .....	8
2.2.2. テスト 2 / Test 2 .....	10
2.2.3. 暗号方式 / Encryption .....	12
Appendix. A. 記入用紙 / Forms.....	15
Appendix. B. 引用 / Quotation.....	16

ECU	Requirements of Information Provision for Cybersecurity Examination		4/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

## 1. はじめに / Introduction

### 1.1. 目的 / Purpose

審査機関が、CS 規制（UN-R155）のための審査マニュアルを発行している。審査機関は、審査マニュアルにおいて、文書の提出及びテストの現認を OEM に要求している。

本書では、既存の設計/評価仕様書とは別に、トヨタが審査機関による審査を受けるために、部品の開発者（通常はサプライヤー）からの提供が必要な情報を定義する。本書を部品に引き当てることで、トヨタは、開発者に情報の提供を依頼する。

Japanese authority has issued examination manuals for CS regulations (UN-R155). In the manuals, the authority requires OEMs to submit documents and demonstrate testing.

This document defines, in addition to existing design/evaluation specifications, the information that the component developers (usually the supplier) need to provide in order for Toyota to be examined by the authority. By allocating this book to components, Toyota requires developers to provide information.

### 1.2. 適用範囲 / Scope

本書は、UN-R155 の審査を受ける車両の電気・電子部品に適用する。ただし、本書の各要求が指定する提供要否の条件にいずれも該当しないときは、情報提供は不要とする。

This document is applied to the electrical or electronic components of vehicles taking the UN-R155 examination. However, if conditions specified by each requirement in this document are not met, developers do not have to provide information.

### 1.3. 関連文書 / Related Documents

Table 1. トヨタ発行関連文書一覧 / List of Related Documents Issued by TMC

ID	名称 / Document Name	発行部署 / Department
SEC-ISO-VCL-MES-PCD-PROC-***_**_*	車両サイバーセキュリティ管理要項 Vehicle Cybersecurity Management Essentials *サプライヤーへは開示不可 / Cannot be disclosed to suppliers	46F
SEC-ISO-VCL-PRD-PCD-PROC-***_**_*	車両サイバーセキュリティ ECU 開発プロセス運用手順書 Procedures of ECU Development Process for Vehicle Cybersecurity *サプライヤーへは開示不可 / Cannot be disclosed to suppliers	46F
SEC-**PF-WLS-REQ-SPEC-***_**_*	無線通信セキュリティ要求仕様書 Requirements Specification of Wireless Communication Security	46F
SEC-**PF-MAC-REQ-SPEC-***_**_*	メッセージ認証要求仕様書 Requirements Specification of Message Authentication	46F
SEC-**PF-RPR-REQ-SPEC-***_**_*	標準リプログラミングセキュリティ要求仕様書 Requirements Specification of Standard Reprogramming Security	46F

ECU	Requirements of Information Provision for Cybersecurity Examination		5/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

Table 2. 公的関連文書一覧 / List of Related Public Documents

本書における略称 / Abbreviation	名称 / Document Name	公開元組織 / Publisher organization
UN-R155	UN Regulation No. [155] on Uniform Provisions Concerning the Approval of Vehicles with regards to Cyber Security and Cyber Security Management System, Jan. 22, 2021	UNECE
審査マニュアル Examination manuals	CS 能力審査マニュアル 2021 年 1 月 22 日施行版 CS Capability Examination Manual, Enforced Jan. 22, 2021	自動車基準認証国際化研究センター CS/OTA 国内採用 WG CS/SU 規則検討小 WG CS/SU Regulations Investigative Small Working Group, CS/OTA Domestic Application Working Group, JASIC
〃	CS 型式審査マニュアル 2021 年 1 月 22 日施行版 CS Type Examination Manual, Enforced Jan. 22, 2021	〃
不正アクセス禁止法 Act No.128 of 1999	不正アクセス行為の禁止等に関する法律 Act on Prohibition of Unauthorized Computer Access	日本国政府 Government of Japan
FIPS	Federal Information Processing Standards	NIST 米国国立標準技術研究所
CRYPTREC	電子政府における調達のために参照すべき暗号のリスト (CRYPTREC 暗号リスト) e-Government Recommended Cipher List (a.k.a. CRYPTREC Cipher List)	CRYPTREC
SP800-57	NIST Special Publication 800-57 Recommendation for Key Management	NIST 米国国立標準技術研究所
SP800-140	NIST Special Publication 800-140 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759	〃
NESSIE	New European Schemes for Signature, Integrity, and Encryption	European Commission 欧州委員会

ECU	Requirements of Information Provision for Cybersecurity Examination		6/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

#### 1.4. 関係者の定義 / Definition of Organizations and Departments

本書の関係者を下表のように定義する。部署名は変わることがあるため、実際の部署名は、最新のものを確認する。

The organizations and departments involved in this document are defined as shown in the table below. Since the department name may change, check the actual department name for the latest.

Table 3. 本書の関係者の一覧 / List of Organizations and Departments

組織 / Organization	役割 / Role	実際の部署 / Actual Department
審査機関 / Authority	-	独立行政法人自動車技術総合機構 交通安全環境研究所 情報セキュリティ審査センター NALTEC/NTSEL CST
トヨタ / Toyota	CS 開発管理部署 / CS Development Management Departments	46F
〃	CS 標準設計部署 / CS Standard Design Departments	46F
〃	CS 試験部署 / CS Testing Departments	ETF, 46F
〃	ECU 設計部署 / ECU Design Departments	-
サプライヤー / Supplier	-	-

注 1 : この表における“実際の部署”は、本書の最新版の発行時点のものを記載している。

NOTE 1: The “Actual Department” in this table is as of the time of the latest version of this document.

注 2 : この表は、『車両サイバーセキュリティ管理要項』を参考に定義している。

NOTE 2: This table is defined with reference to “Vehicle Cybersecurity Management Essentials”.

ECU	Requirements of Information Provision for Cybersecurity Examination		7/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

## 2. 審査のための情報提供 / Information Provision for Examination

### 2.1. 要求の一覧 / List of Requirements

本書の要求の一覧を下表に示す。

The table below lists the requirements of this document.

Table 4. 本書の要求の一覧 / List of requirements in this document

ID	Section of UN-R155	分類 Category	要求の名称 Title of requirements
VCLEIP_00010	Section 7.3.1	能力基準適合証明書 Certificate of Compliance for CSMS	(Reserved)
VCLEIP_00020	Section 7.3.2	サプライヤー関連リスク Supplier-related risks	(Reserved)
VCLEIP_00030	Section 7.3.3	リスクアセスメント Risk assessment	(Reserved)
VCLEIP_00040	Section 7.3.4	軽減策 Mitigations	(Reserved)
VCLEIP_00050	Section 7.3.5	アフターマーケット製品・サービス Aftermarket products and services	(Reserved)
VCLEIP_00060	Section 7.3.6	テスト Test	ソフトウェア更新機能 Software update function
VCLEIP_00061	〃	〃	審査の支援 Examination support
VCLEIP_00070	Section 7.3.7	攻撃の検知・防御 Detection and defense	(Reserved)
VCLEIP_00080	Section 7.3.8	暗号方式 Encryption	暗号方式 Encryption

注 1 : (Reserved)としている要求は、現版では定義しない。19 制御電子 PF では、トヨタの CS 標準設計部署が発行する仕様書によって、審査マニュアルの要求を満たせる見込みのため。

NOTE 1: “(Reserved)” requirements are not defined in the current version. On 19 ePF, the specifications issued by Toyota CS Standard Design Departments alone will be able to meet the requirements of examination manuals.

ECU	Requirements of Information Provision for Cybersecurity Examination		8/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

## 2.2. 要求 / Requirements

情報提供の条件に該当するときは、トヨタに情報を提供する。

Information shall be provided to Toyota when components meet any conditions.

### 2.2.1. テスト 1 / Test 1

ID	VCLEIP_00060																						
要求の名称 / Title	ソフトウェア更新機能 / Software update function																						
情報提供の条件 Condition	<p><u>&lt;19 制御電子 PF の車両における条件 / Conditions on 19ePF&gt;</u></p> <p>次の 2 つの条件を両方満たすソフトウェア更新機能を有す部品 Components with software update function that meet both of following two conditions</p> <ol style="list-style-type: none"> <li>1. 車両を改造せずとも有効なソフトウェア更新の機能 Available software update function without modification of the vehicle</li> <li>2. DLC コネクタ又は DCM ECU を<u>経由しない</u>ソフトウェア更新の機能 Software update function that does <u>not</u> communicate via DLC connector or DCM ECU</li> </ol> <p>Table. 19 制御電子 PF における例/ Examples on 19ePF</p> <table> <tr> <th colspan="2">条件 / Condition</th><th rowspan="2">提供要否 / Result</th><th rowspan="2">通信媒体の例 / Examples of Communication media</th></tr> <tr> <th>No.1</th><th>No.2</th></tr> <tr> <td rowspan="3">Yes</td><td>Yes</td><td>o</td><td>USB memory, Memory card, CD/DVD/BD, Wi-Fi, Bluetooth</td></tr> <tr> <td>No (DLC Connector)</td><td>-</td><td>DoCAN, DoIP</td></tr> <tr> <td>No (DCM ECU)</td><td>-</td><td>2G, 3G, LTE</td></tr> <tr> <td>No</td><td>-</td><td>-</td><td>JTAG</td></tr> </table> <p>注 1 : 本書では、車両に乗り込むことを必要とし、かつ取扱書に記載していない行為を“改造”とする。なお、インパネを外してから行うソフトウェア更新の機能は“改造”にあたるため、条件 1 には該当しない。 Note 1: In this document, actions that require boarding the vehicle and are not described in the owner’s manual are defined as “modification”. The software update function performed after removing the instrument panel is “modification”, so it does not meet condition No.1.</p> <p><u>&lt;Post19 制御電子 PF の車両における条件 / Conditions on Post19ePF&gt;</u></p> <p>T.B.D.</p>			条件 / Condition		提供要否 / Result	通信媒体の例 / Examples of Communication media	No.1	No.2	Yes	Yes	o	USB memory, Memory card, CD/DVD/BD, Wi-Fi, Bluetooth	No (DLC Connector)	-	DoCAN, DoIP	No (DCM ECU)	-	2G, 3G, LTE	No	-	-	JTAG
条件 / Condition		提供要否 / Result	通信媒体の例 / Examples of Communication media																				
No.1	No.2																						
Yes	Yes	o	USB memory, Memory card, CD/DVD/BD, Wi-Fi, Bluetooth																				
	No (DLC Connector)	-	DoCAN, DoIP																				
	No (DCM ECU)	-	2G, 3G, LTE																				
No	-	-	JTAG																				
提供する情報 Information to be provided to Toyota	<p>(1) ソフトウェア更新機能の名称 / Name of software update function</p> <p>(2) ソフトウェア更新をするために必要なツールやアプリケーション / Tools and applications needed to update software</p>																						



ECU	Requirements of Information Provision for Cybersecurity Examination		9/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

	<p>(3) ソフトウェア更新をするときの手順書 / Manuals of updating software</p> <p>(4) 型式認証車の搭載部品において試験するための更新プログラム（リプロデータ） / Update program (reprogramming data) for testing components mounted on vehicles of type examination</p>
<p>提供する方法</p> <p>Provision method</p>	<p><u>CV 品納入までに</u>、サプライヤーは、トヨタの ECU 設計部署を介して、CS 試験部署と提供方法を調整する。調整に従って情報を提供する。ただし、トヨタが内製開発をするときは、開発部署と CS 試験部署とで直接調整する。</p> <p>By the time the CV product is delivered, the supplier shall coordinate the provision method with Toyota CS Testing Departments through ECU Design Department. Information shall be provided according to coordination. If Toyota develops in-house, the departments shall coordinate directly.</p>
<p>備考</p> <p>Remarks</p>	<p>i. 型式審査において、審査機関の立会いのもと、車両のソフトウェア更新機能のサイバーセキュリティについてテストする（例：不正な更新ができない）。 The software update functions of the vehicle shall be cybersecurity tested in the presence of the authority when the type examination. Example: Confirmation that unauthorized updates are not possible.</p> <p>ii. 情報を提供しない代わりに、トヨタの ECU 設計部署またはサプライヤーが、型式審査において、ソフトウェア更新機能を再テストしてもよい。 If not provided, Toyota ECU Design Department or supplier shall instead retest the software update function in the type examination.</p> <p>iii. 19 制御電子 PF では、標準リプロ、パワトレリプロ及びボデーリプロはいずれもこの条件に該当しない。 “Standard Reprogramming”, “Powertrain Reprogramming” and “Body Reprogramming” on 19 ePF do not meet this conditions.</p> <p>iv. 19 制御電子 PF では、DLC コネクタ経由と DCM ECU 経由のソフトウェア更新機能は、情報提供の対象外とした。なぜなら、これらの機能には、トヨタの標準サイバーセキュリティ仕様書を適用しており、CS 試験部署においてテスト可能なためである。 Software update functions via DLC connector and DCM ECU on 19 ePF are excluded from this information provision. This is because Toyota's Standard CS Specifications are applied to these functions and can be tested by Toyota CS Testing Departments.</p> <p>v. CS 試験部署は、不正な更新による影響のない部品を除外することができる。 CS Testing Departments may exclude components that are not affected by unauthorized updates.</p>

ECU	Requirements of Information Provision for Cybersecurity Examination		10/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

## 2.2.2. テスト 2 / Test 2

ID	VCLEIP_00061											
要求の名称 / Title	審査の支援 / Examination support											
情報提供の条件 Condition	<p>型式審査及びその事前試験において、トヨタの CS 試験部署がテストできない以下の部品。</p> <p>The following components that Toyota CS Testing Departments cannot test in the type examination and its pre-examination.</p> <p>Table. テストできない部品 / Components that cannot be tested</p> <table><tr><th>#</th><th>部品 / Component</th><th>理由 / Reason</th></tr><tr><td>[1]</td><td>充電インレット経由で充放電器と通信する ECU / ECU that communicates with charger/discharger via the charging inlet</td><td>サイバーセキュリティのテストを車両をするとき、感電、過充電等の恐れがある。トヨタの CS 試験部署では安全にテストできない。 There are risks such as electric shock and overcharging when testing cybersecurity in a vehicle. For this reason, Toyota CS Testing Departments cannot safely test the component.</td></tr><tr><td>[2]</td><td>- ITS ECU - ETC ECU</td><td>サイバーセキュリティに係る通信プロトコルが、開発者ではない者に開示されない。開発者ではない者によるテストが、『不正アクセス禁止法』に抵触する恐れがある。 Communication protocols related to cybersecurity are not disclosed to non-developers. Testing by non-developers may violate “Act No.128 of 1999”.</td></tr></table>			#	部品 / Component	理由 / Reason	[1]	充電インレット経由で充放電器と通信する ECU / ECU that communicates with charger/discharger via the charging inlet	サイバーセキュリティのテストを車両をするとき、感電、過充電等の恐れがある。トヨタの CS 試験部署では安全にテストできない。 There are risks such as electric shock and overcharging when testing cybersecurity in a vehicle. For this reason, Toyota CS Testing Departments cannot safely test the component.	[2]	- ITS ECU - ETC ECU	サイバーセキュリティに係る通信プロトコルが、開発者ではない者に開示されない。開発者ではない者によるテストが、『不正アクセス禁止法』に抵触する恐れがある。 Communication protocols related to cybersecurity are not disclosed to non-developers. Testing by non-developers may violate “Act No.128 of 1999”.
#	部品 / Component	理由 / Reason										
[1]	充電インレット経由で充放電器と通信する ECU / ECU that communicates with charger/discharger via the charging inlet	サイバーセキュリティのテストを車両をするとき、感電、過充電等の恐れがある。トヨタの CS 試験部署では安全にテストできない。 There are risks such as electric shock and overcharging when testing cybersecurity in a vehicle. For this reason, Toyota CS Testing Departments cannot safely test the component.										
[2]	- ITS ECU - ETC ECU	サイバーセキュリティに係る通信プロトコルが、開発者ではない者に開示されない。開発者ではない者によるテストが、『不正アクセス禁止法』に抵触する恐れがある。 Communication protocols related to cybersecurity are not disclosed to non-developers. Testing by non-developers may violate “Act No.128 of 1999”.										
提供する情報 Information to be provided to Toyota	トヨタの CS 試験部署、ECU 設計部署、サプライヤーの間で個別に調整する。 It shall be decided by coordination among Toyota CS Testing Departments, ECU Design departments, and suppliers.											
提供する方法 Provision method	同上 Same as above											
備考 Remarks	<p>i. トヨタの CS 試験部署は、ECU のサイバーセキュリティに係る設計とテストの情報を個別に聴取し、審査機関との交渉に向けた提案を検討する。 Toyota CS Testing Departments will ask ECU design and test information related to cybersecurity, and then consider proposals for negotiation with the authority.</p> <p>ii. 審査機関との交渉結果にもとづき、ECU 開発中のテストを、サプライヤーに再テスト・実演いただくことがある。</p>											

ECU	Requirements of Information Provision for Cybersecurity Examination		11/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

	Based on the results of negotiations with the authority, Toyota CS Testing Departments may request the supplier to retest and demonstrate the testing under ECU development.
--	--

ECU	Requirements of Information Provision for Cybersecurity Examination		12/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

### 2.2.3. 暗号方式 / Encryption

ID	VCLEIP_00080																
要求の名称 / Title	暗号方式 / Encryption																
情報提供の条件 Condition	<p>通信を暗号化している部品 Components that encrypt communication.</p> <p>注 1 : 下表の[1], [2]はどちらもこの条件に該当する。 Note 1: For example, both [1] and [2] in the table below meet this condition.</p> <p>Table. 通信の暗号化の例 / Examples of communication encryption</p> <table> <tr> <th>#</th><th>分類 / Category</th><th>部品の例 / Example of Component</th></tr> <tr> <td>[1]</td><td>トヨタの標準 CS 仕様書をもとに、通信を暗号化している。 Communication is encrypted based on Toyota's Standard CS Specifications.</td><td>DCM ECU (HTTPS/TLS) , 21CY AVN ECU</td></tr> <tr> <td>[2]</td><td>トヨタの標準セキュリティ仕様書ではない仕様をもとに、通信を暗号化している。 Communication is encrypted based on specifications that are not Toyota's Standard CS Specifications.</td><td>DCM ECU (2G, 3G, LTE) , ITS ECU, ETC ECU, BLE 制御 ECU / BLE control ECU, ガレージドアオープナー / Garage door opener</td></tr> </table> <p>標準 CS 仕様書の例 : 『無線通信セキュリティ要求仕様書』 Example of Toyota's Standard CS Specifications: "Requirements Specification of Wireless Communication Security"</p> <p>注 2 : 「ECU-非車両搭載機器間の通信」、「ECU 間の通信」及び「ECU 内部の通信」は、いずれもこの条件に該当する。 Note 2: All of the communications "between ECU and out-of-vehicle equipment", "between ECUs" and "inside the ECU" meet this condition.</p> <p>注 3 : 下表の[i], [ii]はどちらもこの条件に<u>該当しない</u>。 Note 3: For example, both [i] and [ii] in the table below <u>do not</u> meet this condition.</p> <p>Table. 条件に該当しない例 / Examples that do not meet this condition</p> <table> <tr> <th>#</th><th>分類 / Category</th><th>暗号化の例 / Example of Encryption</th></tr> <tr> <td>[i]</td><td>通信の暗号化ではない The target of encryption is</td><td>- 記憶媒体上に保存するデータの暗号化 Encryption of data to record on storage</td></tr> </table>		#	分類 / Category	部品の例 / Example of Component	[1]	トヨタの標準 CS 仕様書をもとに、通信を暗号化している。 Communication is encrypted based on Toyota's Standard CS Specifications.	DCM ECU (HTTPS/TLS) , 21CY AVN ECU	[2]	トヨタの標準セキュリティ仕様書ではない仕様をもとに、通信を暗号化している。 Communication is encrypted based on specifications that are not Toyota's Standard CS Specifications.	DCM ECU (2G, 3G, LTE) , ITS ECU, ETC ECU, BLE 制御 ECU / BLE control ECU, ガレージドアオープナー / Garage door opener	#	分類 / Category	暗号化の例 / Example of Encryption	[i]	通信の暗号化ではない The target of encryption is	- 記憶媒体上に保存するデータの暗号化 Encryption of data to record on storage
#	分類 / Category	部品の例 / Example of Component															
[1]	トヨタの標準 CS 仕様書をもとに、通信を暗号化している。 Communication is encrypted based on Toyota's Standard CS Specifications.	DCM ECU (HTTPS/TLS) , 21CY AVN ECU															
[2]	トヨタの標準セキュリティ仕様書ではない仕様をもとに、通信を暗号化している。 Communication is encrypted based on specifications that are not Toyota's Standard CS Specifications.	DCM ECU (2G, 3G, LTE) , ITS ECU, ETC ECU, BLE 制御 ECU / BLE control ECU, ガレージドアオープナー / Garage door opener															
#	分類 / Category	暗号化の例 / Example of Encryption															
[i]	通信の暗号化ではない The target of encryption is	- 記憶媒体上に保存するデータの暗号化 Encryption of data to record on storage															

ECU	Requirements of Information Provision for Cybersecurity Examination		13/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

		not communication.	medium - 『メッセージ認証要求仕様書』をもとに認証子を生成するための暗号化 Encryption for generation of authentication code according to the “Requirements Specification of Message Authentication”
	[ii]	ECU は復号のみする（暗号化しない）。 The ECU decrypts program but does not encrypt it.	『標準リプログラミングセキュリティ要求仕様書』をもとに書き込みプログラムを暗号化 Encryption of program according to “Requirements Specification of Standard Reprogramming Security”
提供する情報 Information to be provided to Toyota	<p>(1) 部品の名称 / Component name</p> <p>(2) (1)において暗号化している通信 / Encrypted communication on (1)</p> <p>(3) 暗号化を要求している仕様書 / Document name of the specifications requiring encryption of (2)</p> <p>(4) 暗号方式 / Encryption (Algorithms)</p> <p>(5) (4)は標準的な暗号であるか？ / Is encryption (4) standard?</p> <p>(6) (5)が Yes のときのみ、(4)はどの業界標準に含まれているか？ / Name of standards, only if (5) is yes.</p> <p>(7) (5)が No のときのみ、(4)の概要とその妥当性の説明 / Explanation of (4) and its validity, only if (5) is no.</p> <p>注 4：本書では、CRYPTREC、FIPS、SP800-57、SP800-140、NESSIE に含まれている暗号方式を、“標準的な暗号” とする。(6)の業界標準には、これらの標準のなかから、ひとつ以上を選択する。</p> <p>Note 4: In this document, the encryption (algorithms) included in CRYPTREC, FIPS, SP800-57, SP800-140, and NESSIE are defined as "standard encryption". For (6) name of standards, select one or more of these standards.</p> <p>注 5：暗号強度が不足しているとき（例：電子政府推奨暗号等と比較して明らかに暗号強度が低い。）は、(7)においてその暗号方式を用いる理由を詳細に説明する。</p> <p>Note 5: When the encryption strength is insufficient (Example: The encryption strength is clearly lower than the encryption of “CRYPTREC Cipher List”), the reason for using the encryption (algorithms) shall be explained in detail in (7).</p>		

ECU	Requirements of Information Provision for Cybersecurity Examination		14/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

<p>提供する方法</p> <p>Provision method</p>	<p><u>CV 品納入までに</u>、サプライヤーは、トヨタの ECU 設計部署を介して、CS 開発管理部署へ提供する。ただし、トヨタが内製開発をするときは、開発部署が CS 開発管理部署に直接提供する。</p> <p>By the time the CV product is delivered, the supplier shall provide the information to Toyota CS Development Management Departments through ECU Design Department. If Toyota develops in-house, the departments shall provide directly.</p> <p>(1)～(6)は、Appendix の記入用紙を用いる。 もし(7)があるときは、記入用紙とは別に文書を作成する。</p> <p>(1) to (6): Please use the form on Appendix. If (7) exist.: Please create a document separately from the form.</p>
<p>備考</p> <p>Remarks</p>	<p>i. この情報は、型式審査における文書の一部として審査機関に提出する。 This information will be submitted to the authority as part of the type examination document.</p> <p>ii. “暗号方式”と“暗号化プロトコル”とは異なる。 例えば、HTTPS/TLS/WPA は、暗号化プロトコルであって、暗号方式ではない。ここでは、HTTPS/TLS/WPA が用いる“暗号方式”を回答する。 “Encryption (Algorithms)” and “Cryptographic protocols” are different. For example, HTTPS/TLS/WPA are protocols, not algorithms. You shall tell the name of encryption algorithms used in HTTPS/TLS/WPA protocol.</p> <p>iii. 原則として、標準的な暗号を用いなければならない。 In principle, standard encryption shall be used.</p> <p>iv. <u>UN-R155 は、標準的な暗号モジュールの使用を、通信に限定せずに要求している。</u>一方、審査マニュアルが、提出文書に記載するよう要求しているのは、リスクアセスメントの結果をもとに通信を暗号化するものである。 In UN-R155, standard cryptographic modules are required to use for not just communication. But, in examination manuals, only the encrypted communication based on the result of risk assessment are required to be included in the submission.</p> <p>v. リスクが低い部分を任意で暗号化しているものは、トヨタの CS 開発管理部署の判断において、審査機関への提出文書から除外することがある。 Any encryption for low-risk communication may be excluded from the submission to the authority at the discretion of Toyota CS Development Management Departments.</p>

ECU	Requirements of Information Provision for Cybersecurity Examination		15/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

## Appendix. A. 記入用紙 / Forms

- 文書名 / Document name : (例)ECU 名 暗号方式
- 文書 ID / Document ID : (例)部署内でユニークな ID
- 発行部署 / Department/Division :
- 連絡先 / Contact address :
- 作成日 / Date :

承認 Approved	調査 Checked	作成 Created

Table. 暗号方式の記入様式 / Form of Encryption

	(1)	(2)	(3)	(4)	(5)	(6)
	部品の名称	暗号化している通信	暗号化を要求している仕様書	暗号方式	標準的な暗号方式か？	業界標準
	Component name	Encrypted communication	Document name of the specifications requiring encryption	Encryption	Is encryption (4) Standard ?	Name of standards
Ex.	ITS ECU	ITS 通信	〇〇書	AES128	Yes	CRYPTREC
1						
2						
3						
4						
5						
6						

ECU	Requirements of Information Provision for Cybersecurity Examination		16/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

## Appendix. B. 引用 / Quotation

Table. UN-R155 条項の引用 / Quotation of UN-R155

Section	原文 / Original	和訳 / Japanese translation
7.3.1	The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved. However, for type approvals prior to 1 July 2024, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned.	メーカーは、認可対象の車両型式に関する有効なサイバーセキュリティ管理システム適合認定書を有しているものとする。 ただし、2024 年 7 月 1 日より前の型式認可の場合、車両メーカーは、CSMS に適合する車両型式を開発することができなかったことを証明できる場合には、当該車両型式の開発フェーズにおいてサイバーセキュリティが十分に考慮されたことを証明するものとする。
7.3.2	The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks.	車両メーカーは、認可対象の車両型式に関して、サプライヤー関連リスクを特定および管理するものとする。
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.	車両メーカーは、車両型式の必要不可欠な要素を特定し、車両型式に関する網羅的なリスクアセスメントを実施するものとし、特定されたリスクを適切に処理／管理するものとする。リスクアセスメントでは、当該車両型式の個々の要素およびそれらの相互作用を考慮するものとする。リスクアセスメントではさらに、外部システムとの相互作用を考慮するものとする。リスクアセスメントにおいて、車両メーカーは、Annex 5、Part A で言及されたすべての脅威に関連するリスク、ならびにその他一切の関連リスク考慮するものとする。
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	車両メーカーは、車両メーカーのリスクアセスメントで特定されたリスクから車両型式を保護するものとする。車両型式を保護するために相応な軽減策を実施するものとする。実施する軽減策には、Annex 5、Part B および C で言及された軽減策のうち、特定されたリスクに関連するす



ECU	Requirements of Information Provision for Cybersecurity Examination		17/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

	<p>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.</p> <p>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.</p>	<p>すべての軽減策を含めるものとする。ただし、Annex 5、Part B および C で言及された軽減策が、特定されたリスクに関連していないまたは十分でない場合、車両メーカーは、他の適切な軽減策が実施されることを確保するものとする。</p> <p>とりわけ、2024 年 7 月 1 日より前の型式認可の場合、車両メーカーは、Annex 5、Part B または C で言及された軽減策が技術的に実現可能でない場合には他の適切な軽減策が実施されることを確保するものとする。メーカーは、各技術的実現可能性アセスメントを認可当局に提供するものとする。</p>
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.	車両メーカーは、アフターマーケットのソフトウェア、サービス、アプリケーションまたはデータの保管および実行のための車両型式上の専用環境（設けられている場合）を保護するために適切かつ相応な措置を実施するものとする。
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.	車両メーカーは、型式認可の前に、実施するセキュリティ措置の有効性を検証するために適切かつ十分なテストを行うものとする。
7.3.7	<p>The vehicle manufacturer shall implement measures for the vehicle type to:</p> <p>(a) Detect and prevent cyber-attacks against vehicles of the vehicle type;</p> <p>(b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;</p> <p>(c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.</p>	<p>車両メーカーは、車両型式に関して下記の措置を実施するものとする：</p> <p>(a) 当該車両型式の車両に対するサイバー攻撃を検知および防止するための措置。</p> <p>(b) 当該車両型式に関連している脅威、脆弱性およびサイバー攻撃の検知に関する車両メーカーの監視能力を支えるための措置。</p> <p>(c) 未遂に終わったサイバー攻撃または成功したサイバー攻撃の分析を可能にするデータフォレンジック能力を提供するための措置。</p>

ECU	Requirements of Information Provision for Cybersecurity Examination		18/18
Application: Electrical and electronic components of vehicles taking the UN-R155 examination		No.	SEC-ePF-VCL-EIP-REQ-SPEC-a00-00-a

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.	本規則の目的のために使用する暗号モジュールは、コンセンサス標準に沿うものとする。使用する暗号モジュールがコンセンサス標準に沿っていない場合には、車両メーカーは、その使用が正当であることを証明するものとする。
-------	---	---