To departments concerned

関係各部署　御中

Confidential level			
	PROTECTED 関係者外秘	Store original until 原紙保管	M/Y :　/
		Storage of copy コピー保管	M/Y :　/

Terms and Definitions related to Vehicle Cybersecurity and Privacy

車両サイバーセキュリティ及びプライバシー用語定義書

System Network & Architecture Development Dept.,
E/E Architecture Development Div.
制御電子ﾌﾟﾗｯﾄﾌｫｰﾑ開発部 制御ﾈｯﾄﾜｰｸ・ｱｰｷ開発室

No. SEC-ePF-TRM-GUD-PROC-a00-02-a

Approved / 承認	Checked / 調査	Created / 作成	
Kawai	Hirabayashi	Ozaki	Jun. 18, 2021

Omission of signature (Electronic approval)

Scope **適用範囲**	Documents related to vehicle cybersecurity and privacy 車両分野のサイバーセキュリティ及びプライバシーに関連する文書
Changes **変更内容**	Addition of terms 用語の追加
Description **説明**	Purpose / 目的 : This document defines the terminology related to vehicle cybersecurity and privacy. Note that this does not preclude the inclusion of separate definitions in individual documents. 本書は、車両分野におけるサイバーセキュリティ及びプライバシーに係る用語を定義する。なお、各文書が個別に用語を定義することを制限するものではない。 Notes on Use / 使用上の注意 : ➢ Use the longest matching term as reference. 最も長く一致する用語を参照すること（最長一致）。 ➢ This document shall be cited in other documents. It is not necessary to give it a specification allocation. 本書は他の文書から被引用されるものとする。仕様としての引き当ては不要。 ➢ This document may be disclosed to Toyota 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. 海外事業体/ボデーメーカー/協業先 OEM/サプライヤ/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。 Contact information / 問合せ先 : Email: epf-sec-sp@mega.tec.toyota.co.jp

Revision Records

Version	Item	Date	Revised by
a00-00-a	All terms	Sep. 28, 2020	Ozaki, 46F3G
a00-01-a	Terms which “Revised version” column is a-00-01-a	May 10, 2021	Ozaki, 46F3G
a00-02-a	Terms which “Revised version” column is a-00-02-a	Jun. 18, 2021	Ozaki, 46F3G

Term	Definition	用語	解説	Revised version
cyber security, cybersecurity	The condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components.	サイバーセキュリティ	電気部品又は電子部品に対するサイバー脅威から、車両及び車両の機能が保護されている状態	a00-00-a
cyber security management system, CSMS	A systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.	サイバーセキュリティマネジメントシステム（CSMS）	車両に対するサイバー脅威に関連するリスクへ対応し、サイバー攻撃から保護するための組織プロセス、責任、ガバナンスを定義する体系的なリスクベースのアプローチ	a00-00-a
risk	The potential that a given threat will exploit vulnerabilities of a vehicle and thereby cause harm to the organization or to an individual.	リスク	特定の脅威が車両の脆弱性を悪用し、それによって組織または個人に損害を及ぼす可能性	a00-00-a
residual risk	Risk remaining after risk treatment	残存リスク、残留リスク	リスク対応後にまだ残っているリスク	a00-00-a
concept phase	Series of activities conducted by the Toyota department in charge of cybersecurity in the initial stages of vehicle system development to derive the cybersecurity goals by analyzing threats to the architecture.	コンセプトフェーズ	トヨタのサイバーセキュリティ主管部署が、車載システム開発の初期に、アーキテクチャを対象とした脅威分析をすることで、サイバーセキュリティゴールを導出する一連の活動	a00-00-a
risk assessment	The overall process of finding, recognizing and describing risks (risk identification) , to comprehend the nature of risk and to determine the level of risk (risk analysis), and of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable (risk evaluation).	リスクアセスメント	次の３つのプロセス全体 ・リスク特定：リスクの発見、認識及び記述するプロセス ・リスク分析：リスクの特質を理解し、リスクレベルを決定するプロセス ・リスク評価：リスク及び／又はその大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス	a00-00-a
item	Component or set of components that implements a function at the vehicle level NOTE: This definition is limited to use in processes related to risk management.	アイテム	車両レベルの機能を実現する部品あるいは部品の集合 注記　この定義は、リスクマネジメントに係る工程で用いるときに限る。	a00-01-a
preliminary architecture	A basic function for providing vehicle control and information communication services. In cybersecurity documents, this refers to “an element other than cybersecurity function” to be installed in an ECU.	本来機能	車両の制御および情報通信サービスを提供するための基本機能。 サイバーセキュリティ関連の文書では、ECUに搭載される「サイバーセキュリティ機能以外の要素」を指す。	a00-00-a
asset, information asset	Object that has value, or contributes to value. An asset shall be categorized as either Safety (S), Financial (F), Operational (O) or Privacy (P).	資産、情報資産	価値のあるもの、または価値に貢献するもの。 車載システムでは、安全(S)、フィナンシャル(F)、オペレーショナル(O)及びプライバシー(P)の、4つのいずれかに分類できるものとする。	a00-01-a
sub-asset	Object required to achieve the cybersecurity controls and indirectly important to protect assets. EXAMPLE: CSPs, PSPs, programs, security logs, and authorization to use privileged functions.	副次資産	サイバーセキュリティ管理策を実現するために必要となる構成要素。資産を保護するために間接的に重要なもの。 例　CSP、PSP、プログラム、セキュリティログ、特権機能の利用権限	a00-01-a
cybersecurity property, security property	Attribute that can be worth protecting. Attributes include confidentiality, integrity and/or availability.	サイバーセキュリティ特性、セキュリティ特性	保護する価値のある属性 例　機密性、完全性、可用性	a00-01-a
confidentialitiy	A cybersecurity property that make information unusable or non-disclosed to an unauthorized entity (person, system, hardware, software, etc.)	機密性	許可されていない実体（人、システム、ハードウェア、ソフトウェアなど）に対して、情報を使用不可または非公開にするサイバーセキュリティ特性	a00-01-a
integrity	A cybersecurity property that ensure correct information free from an error or omission	完全性	誤りや欠落がなく、正しい情報であることを保証するサイバーセキュリティ特性	a00-01-a
availability	A cybersecurity property that ensure access and use when an authorized entity (person, system, hardware, software, etc.) makes a request	可用性	許可された実体（人、システム、ハードウェア、ソフトウェアなど）が要求したときに、アクセスおよび使用できることを保証するサイバーセキュリティ特性	a00-01-a
personal and privacy information	Personal information and privacy information	個人・プライバシー情報	個人情報及びプライバシー情報の総称	a00-00-a
personal information	Information protected by Japanese Personal Information Protection Act or related laws in other countries.	個人情報	日本国の個人情報保護法若しくは各国の関連法令に基づいて保護される情報	a00-00-a
privacy information	Information that is not personal information by itself, but it is possible to identify an individual by combining multiple pieces of information. And attributes that are sensitive to that individual.	プライバシー情報	単独では個人情報にならないが、複数の情報が合わさることで個人の特定につながるものや、その個人にとってセンシティブな属性情報	a00-01-a
triage	Analysis to determine the relevance of cybersecurity information to an item or component.	トリアージ	サイバーセキュリティ情報が、アイテムや部品に関係するかを判断するための分析。	a00-01-a
cybersecurity event, security event	A cybersecurity information sent forward to the event assessment process following triage. It can be shortened to event in some contexts.	サイバーセキュリティイベント、セキュリティイベント	トリアージの結果、次のイベントアセスメントに進む判定がなされたサイバーセキュリティ情報。文脈によってはイベントと略すことがある。	a00-01-a
event assessment	Using the security event impact analysis and risk assessment to determine whether to initiate an incident response. It can be shortened to assessment in some contexts.	イベントアセスメント	セキュリティイベントの影響分析・リスク評価により、インシデント対応プロセスを開始するか否かを判断すること。文脈によってはアセスメントと略すことがある。	a00-00-a
cybersecurity incident	Situation in the field that can involve vulnerability exploitation.	サイバーセキュリティインシデント	市場において脆弱性が悪用される可能性のある状況	a00-01-a
damage scenario	Adverse consequence involving a vehicle or vehicle function and affecting a road user.	ダメージシナリオ	車両又は車両の機能や、利用者への悪影響	a00-01-a
impact	Estimate of magnitude of damage or physical harm from a damage scenario	影響度、インパクト	ダメージシナリオによる被害または物理的な損害の大きさ	a00-00-a
attack feasibility	Attribute of an attack path describing the ease of successfully carrying out the corresponding set of actions.	攻撃可能性、アタックフィージビリティ	攻撃経路の属性であり、攻撃経路に対応する行為がどの程度容易に成功させられるかを示す。	a00-01-a
threat	A potential cause of an unwanted incident, which may result in harm to a system or organization. e.g., deliberate threats: attacks such as data tampering, eavesdropping, spoofing, etc. accidental threats: human errors, etc.	脅威	システム又は組織に損害を与える可能性がある望ましくないインシデントの潜在的な原因 例　意図的脅威：データの改ざん、盗聴、なりすまし等の攻撃 偶発的な脅威：ヒューマンエラー等	a00-00-a
threat analysis	Activities intended to derive the cybersecurity goals defined in the ISO/SAE FDIS 21434:2021 [RQ-09-03]. Carried out by the Toyota department in charge of cybersecurity at the concept phase.	脅威分析	ISO/SAE FDIS 21434:2021の要件[RQ-09-03]に定義された、サイバーセキュリティゴールを導出するための活動のこと。トヨタのサイバーセキュリティ主管部署が、コンセプトフェーズにおいて実施する。	a00-01-a
spoofing	Executing unauthorized processing while pretending to execute appropriate processing.	なりすまし	適切な処理をしているようにみせかけて、不正な処理を実施すること	a00-00-a
vulnerability	Weakness that can be exploited as part of an attack path. Of findings detected by testing to on-vehicle compornets, weaknesses from a cybersecurity flaw due to an implementation/specification failure fall under vulnerabilities.	脆弱性	攻撃経路の一部として付け込まれる可能性のある弱点。 車載部品に対するテストによって発見された指摘事項のうち、実装や仕様上の不具合によるサイバーセキュリティの欠陥に該当するものが、脆弱性に該当する。	a00-01-a

vulnerability analysis	In the product development phase, the product developer takes primary responsibility for identifying and analyzing vulnerabilities based on detailed system and component information to avoid building vulnerabilities into the product. Defined in requirement [RQ-08-05] (Section 8.5) of ISO/SAE FDIS 21434:2021. Risk analysis can be carried out using either top-down or bottom-up approachs.	脆弱性分析	脆弱性を作りこまないため、製品開発フェーズにおいて、主に製品開発者が、システム/コンポーネントの詳細情報を用いて脆弱性を特定・分析する作業。ISO/SAE FDIS 21434:2021の要件[RQ-08-05]（即ち8.5節）に定義される。リスク分析の手法は、トップダウンでもボトムアップでもどちらでもよい。	a00-01-a
vulnerability information monitoring	Identifying sources of information inside and outside the organization, collecting the vulnerability information disclosed, updated or discovered on a daily basis, as well as applying triage to identify security events. It can be shortened to monitoring or vulnerability monitoring in some contexts.	脆弱性情報の監視	組織の内外の情報源を特定し、そこで日々更新される、あるいは発見される脆弱性情報を収集し、トリアージによってセキュリティイベントを抽出すること。文脈によっては、監視、脆弱性監視、と略すことがある。	a00-00-a
vulnerability database	Databases that collect and store information on already known vulnerabilities and measures to address them. Representative vulnerability databases publicly accessible are listed below. [1] JVN iPedia: http://jvndb.jvn.jp [2] CVE: http://cve.mitre.org/cve [3] US-CERT DB: http://www.kb.cert.org/vuls/	脆弱性データベース、脆弱性DB	これまで明らかになった脆弱性と、その対策に関する情報を収集・蓄積しているデータベース。無償で一般に公開されている脆弱性データベースとしては、以下が代表的なものである。 [1] JVN iPedia：http://jvndb.jvn.jp/ [2] CVE：http://cve.mitre.org/cve/ [3] US-CERT DB：http://www.kb.cert.org/vuls/	a00-01-a
common weakness enumeration, CWE	Database that classifies and organizes software vulnerabilities based on their type ID and assigns each type a CWE ID. It is released by MITRE, a corporation supported by the U.S. government. http://cwe.mitre.org/data/index.html	共通脆弱性タイプ一覧（CWE）	ソフトウェアにおける脆弱性を、その特徴によって分類し、それぞれのタイプにCWE識別子（CWE-ID）を付与して体系化したもの。米国政府が支援するMITRE社が公開している。 http://cwe.mitre.org/data/index.html	a00-00-a
common vulnerability scoring system, CVSS	One of methodologies for assessing the severity of a vulnerability. An impact, etc. on confidentiality, integrity, and availability, calculated with use of a common scale is expressed as a point from 0.0 to 10.0.	共通脆弱性評価システム（CVSS）	脆弱性の深刻度を評価する手法のひとつ。機密性、完全性、可用性への影響等を共通の尺度で計算し、0.0から10.0までの得点で表す。	a00-00-a
attack path	Set of deliberate actions to realize a threat scenario.	攻撃経路、アタックパス	脅威シナリオを実現するための、意図的な行為の集合。	a00-01-a
entry point	An interface at the boundary between in-vehicle system and external devices/users on an attack path identified by threat analysis. In other words, it is an entrance that can be attacked under nomal conditions in which the customer uses the vehicle. Entry points include not only 3G, LTE and other cellular phone communication line but also Wi-Fi, Bluetooth, USB, SD memory cards, CD/DVD/BD and DLC.	エントリーポイント	車載システムの有するインタフェースのうち、脅威分析により明らかになった攻撃経路上で、外部機器/利用者との境界に位置するもの。すなわち、利用者が車両を用いる通常の状態において、攻撃の可能性がある入口を指す。3G, LTE等携帯通信回線のほか、Wi-Fi、Bluetooth、USB、SDメモリーカード、CD/DVD/BDやDLCもエントリーポイントである。	a00-01-a
attack surface	Refers to all possible entrances through which an attack can be made. Attack surface in an in-vehicle system include entrances through which an attack might be made in a way which is not anticipated in an ordinary use condition by the users (e.g., test access port, etc.) as well as entry points.	攻撃の入口、アタックサーフェース	攻撃の可能性があるすべての入口のこと。 車載システムにおける攻撃の入口には、エントリーポイントに加えて、通常のユーザの使用する状態としては考えられないような攻撃の可能性がある入口（例. テストアクセスポート等）も含まれる。	a00-00-a
resource separation function	Mechanics that either physically or logically separates access to physical hardware resources.	リソース分離機能	物理ハードウェアリソースを物理的または論理的にアクセス分離する機構	a00-00-a
entry point region	Region without resource separation from the entry point region.	エントリーポイント領域	エントリーポイントからリソース分離されていない領域	a00-00-a
internal region	Region with resource separation from the entry point region.	内部領域	エントリーポイント領域からリソース分離される領域	a00-00-a
untrusted zone	Region protected at the first layer from the entry point.	Untrusted Zone	エントリーポイントから1層目防御で守られた領域	a00-00-a
trusted zone	Region with resource separation from the entry point that has two layers of protection from regions with an entry point. Even if there is a security breach in the entry point region, it is protected by the second layer. Functions involving vehicle control of risk rank 7 or higher can be placed here.	Trusted Zone	エントリーポイント領域からリソース分離され、かつエントリーポイントのある領域から2層の防御で守られた領域。エントリーポイント領域がセキュリティ侵害された際においても、2層目防御によって保護されており、車両のリスクランク７以上の制御に関わる機能を配置することができる。	a00-00-a
first layer protection	First line of protection along the attack path	1層目防御	攻撃経路上に配置される最初の防御	a00-00-a
second layer protection	Filtering or tampering function set along the attack path to prevent communication messages that can affect vehicle control of risk rank 7 or higher from reaching functions placed in the trusted zone from the untrusted zone. This protection is set in an internal region with resource separation from the entry point region.	2層目防御	攻撃経路上に配置され、車両のリスクランク７以上の制御に影響する通信メッセージがUntrusted ZoneからTrusted Zoneに配置された機能に到達しないよう、フィルタまたは改竄検知する機能。本防御はエントリーポイント領域からリソース分離された内部領域に配置される。	a00-00-a
defence-in-depth	A system with multiple levels of protection that maintains a total protection level even in the event of failure or penetration of a single protection level.	多層防御、多層防衛	ひとつの保護レベルにおける失敗または侵入が生じた場合でも総保護レベルが維持される多重保護レベルを有するシステムを指す。	a00-00-a
direct attack	An attack which is made in the form of physically contacting the in-vehicle system	直接攻撃	車載システムに物理的に接触した形式で行われる攻撃	a00-00-a
remote attack	An attack which is made via an external network in the form of not physically contacting the in-vehicle system	遠隔攻撃	車載システムには物理的に接触していない形式で、外部ネットワークを通して行われる攻撃	a00-00-a
cybersecurity assuarance level, CAL	A CAL can be used to specify and communicate a set of assurance requirements, in terms of levels of rigour to provide confidence that protection of the assets of an item or component is adequately developed. This CAL classification scheme does not specify technical requirements for cybersecurity controls, however it can be used to drive the cybersecurity engineering, providing a common language for communicating cybersecurity assurance requirements among the organizations involved.	サイバーセキュリティ保証レベル（CAL）	アイテムの資産の保護や、部品の適切な開発を確かにするために供する厳格さのレベル。保証要件を指定したり伝達したりできる。 CALによる分類スキームは、サイバーセキュリティ管理策の技術要件を指定するものではない。一方で、関係する組織間において、サイバーセキュリティの保証要件を伝えるための共通言語としてCALを用いることで、サイバーセキュリティの技術開発を推進することができる。	a00-01-a

cybersecuirty requirement	The result of selecting whether to apply measures against the applicable attack path based on the attack behavior for which risk was reduced. Assigned the same CAL as the cybersecurity goal. Remark: A single attack path usually contains multiple attack behaviors. Taking the in-vehicle system architecture and the feasibility of measures into account, designers select one or more attack behaviors and defines their reverse as cybersecurity requirements. Since cybersecurity requirements are the reverse of an attack action, they are more abstract than most items generally called requirements.	サイバーセキュリティ要求	どの攻撃行為をリスク低減することで、当該の攻撃経路を対策するのかを選択した結果。CALを付与するときは、サイバーセキュリティゴールと同じレベルとなる。 備考　一つの攻撃経路には、通常は複数の攻撃行為が含まれる。設計者は、車載システムのアーキテクチャと対策の実現可能性を考慮して、攻撃行為をひとつ以上選択し、その裏返しをサイバーセキュリティ要求とする。サイバーセキュリティ要求は、攻撃行為の裏返しなので、一般的な"要求"と呼ばれるものに比べて、抽象的な表現となる。	a00-01-a
cybersecurity control	Measure of achieving the cybersecurity requirements obtained from the threat analysis. Usually, it is instructed by the specifications. The design and implementation of cybersecurity control shall include the verification and documentation required by ISO/SAE 21434. EXAMPLE: Use tool authentication and electronic signatures in ECU XX to prevent unauthorized reprogramming.	サイバーセキュリティ管理策	脅威分析によって導出したサイバーセキュリティ要求を実現するための手段。通常は、仕様書によって具体的に指示される。サイバーセキュリティ管理策の設計・実装においては、ISO/SAE 21434が要求する検証やエビデンス作成が必要となる。 例．不正なリプログラミングを防ぐために、○○ECUでツール認証、電子署名を行う。	a00-01-a
penetration testing	Cybersecurity testing in which real-world attacks are mimicked to identify ways to compromise cybersecurity goals.	侵入テスト、ペネトレーションテスト	サイバーセキュリティゴールを侵害する方法を特定するために、実環境の攻撃を模擬するサイバーセキュリティのテスト	a00-00-a
fuzz testing	Inspection method involving sending a large amount of data liable to cause problems in the software product and detecting vulnerabilities by monitoring its response and behavior.	ファジング、ファズテスト	検査対象のソフトウェア製品に問題を引き起こしそうなデータを大量に送り込み、その応答や挙動を監視することで脆弱性を検出する検査手法。	a00-00-a
critical security parameter, CSP	Cybersecurity related information whose disclosure or modification can compromise the cybersecurity of a cryptographic module EXAMPLE: Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchours NOTE: A CSP can be plaintext or encrypted.	クリティカルセキュリティパラメタ（CSP）	サイバーセキュリティに関する情報であって、その開示又は変更が、暗号モジュールのサイバーセキュリティを危殆化し得るもの 例　秘密鍵、プライベート鍵、認証データ（例えば、パスワード、証明書） 注記　CSPは平文であることも、暗号化されていることもある。	a00-00-a
public security parameter, PSP	Cybersecurity related public information whose modification can compromise the cybersecurity of a cryptographic module EXAMPLE: Public cryptographic keys, public key certificates, self-signed certificates, trust anchors, one time passwords associated with a counter and internally held date and time NOTE: A PSP is considered protected if it cannot be modified or if its modification can be determined by the module.	公開セキュリティパラメタ（PSP）	サイバーセキュリティに関する情報であって、その変更が、暗号モジュールのサイバーセキュリティを危殆化し得るもの 例　公開鍵、公開鍵証明書、自己署名証明書 注記　PSPは、変更することができない場合、又は変更が暗号モジュールによってなされる場合、保護されているものとみなす。	a00-00-a
sensitive security parameter, SSP	Critical security parameters (CSP) and public security parameters (PSP)	センシティブセキュリティパラメタ（SSP）	クリティカルセキュリティパラメタ（CSP）及び公開セキュリティパラメタ（PSP）の総称	a00-00-a
certificate	Entity's date rendered unforgeable with the private or secret key of a certification authority NOTE: Not to be confused with a modules validation certificate issued by a validation authority	証明書	認証局のプライベート鍵又は秘密鍵で、偽造できないようにされたエンティティのデータ。 注記　認証機関によって発行された暗号モジュール証明書と混同しないように注意する。	a00-00-a
password	String of characters used to authenticate an identity or to verify access authorisation EXAMPLE: Letters, numbers, and other symbols	パスワード	識別認証又はアクセス権の検証に使用される文字列 例　英字、数字、その他の記号	a00-00-a
access control	Means to ensure that access to assets is authorized and restricted based on business and cybersecurity requirements	アクセス制御	資産へのアクセスが、事業上及びサイバーセキュリティの要求事項に基づいて認可及び制限されていることを確実にする手段	a00-00-a
challenge–response authentication	One of the means to realize access control. Validation process by sending random numbers and identifying whether the target is the intended one based on the response value.	チャレンジレスポンス認証、C&R認証	アクセス制御の実現手段のひとつ。相手に乱数を送付し、それに対するレスポンスの値により、正しい相手であることを確認する。	a00-00-a
authenticaion code	Symbol used to guarantee the integrity of the authenticated data.	認証子	認証データの完全性を保証するための符号	a00-00-a
digest	Data to be created to generate a signature. By using a hash function, fixed-length data is created from the writing program	ダイジェスト	署名を生成する為に作成するデータ。ハッシュ関数を利用して、書込みプログラムから固定長のデータを作成する。	a00-00-a
digital signature	Encrypted signature information provided to ensure the validity of a digital document or techniques and a series of procedures for giving such signature. This signature certifies the transmitter of the document and ensures that the document is not tampered.	電子署名	デジタル文書の正当性を保証するために付けられる、暗号化された署名情報。また、そのような署名を行なうための技術および一連の手順。文書の送信者を証明し、かつその文書が改竄されていないことを保証する。	a00-00-a
cryptographic algorithm	Well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output	暗号アルゴリズム	可変入力を受けて、出力を生成する、明確に定義された計算手順。可変入力は暗号鍵を含む場合がある。	a00-00-a
cryptographic key, key	Sequence of symbols that controls the operation of a cryptographic transformation EXAMPLE: A cryptographic transformation can include but not limited to encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification.	暗号鍵、鍵	暗号変換の動作を制御する記号列。 例　暗号変換は、暗号化、復号、MAC計算、署名生成、又は署名検証を含むが、これに限定されない。	a00-00-a
public key	A type of cryptographic key used in public-key cryptography	公開鍵	公開鍵暗号で使用する暗号鍵の一種。	a00-00-a
private key	A type of cryptographic key used in public-key cryptography. This is a cryptographic key that should not be disclosed.	秘密鍵	公開鍵暗号で使用する暗号鍵の一種。公開してはならない暗号鍵。	a00-00-a
symmetric-key cryptography	An encryption method which uses common key to encrypt and decrypt the message.	共通鍵暗号	暗号化と復号に共通の鍵を用いる暗号方式	a00-00-a
symmetric-key cryptography	Encryption protocol that uses a pair of public and private keys to encrypt and decrypt data. Data encrypted with the public key can only be decrypted by its paired private key.	公開鍵暗号	公開鍵と秘密鍵の対になる2つの鍵を使用してデータの暗号化、復号を行う暗号方式。公開鍵を使用して暗号化したデータはペアとなる秘密鍵でしか復号できない。	a00-00-a

session key	A disposable temporary key that is valid only during one communication session (a certain amount of time or number of times, or from the start to the end of communication) (TLS session key etc.)	セッションキー	一つの通信セッション(一定の時間や回数、あるいは通信開始から終了まで)の間だけ有効な使い捨ての暗号鍵 (TLSセッションキー 等)	a00-02-a
public-key encryption	The encryption method which performs encryption and decryption of data with a public key and a secret key. A public key and a secret key are pairs. The data encrypted with the public key can be decrypted only with the secret key of a pair.	公開鍵暗号	公開鍵と秘密鍵の対になる2つの鍵を使用してデータの暗号化、復号を行う暗号方式。公開鍵を使用して暗号化したデータはペアとなる秘密鍵でしか復号できない。	a00-00-a
plaintext	Unencrypted data and/or programs	平文	暗号化していないデータやプログラム	a00-00-a
ciphertext	Encrypted data and/or programs	暗号文	暗号化したデータやプログラム	a00-00-a
advanced encryption standard, AES	Symmetric-key encryption method standardized as a new encryption standard in the US. The key length can use 128, 192, or 256 bits.	Advanced Encryption Standard（AES）	アメリカ合衆国の新暗号規格として規格化された共通鍵暗号方式。鍵長は128bit、192bit、256bitの3つが利用可能。	a00-00-a
transport layer security, TLS	One of the protocols (communication procedures) used to encrypt and transmit data of the Internet or other TCP/IP network. Its main functions include authenticating the other party in the communication, encrypting the communication, and detecting tampering.	Transport Layer Security（TLS）	インターネットなどのTCP/IP ネットワークでデータを暗号化して送受信するプロトコル（通信手順）の一つ。主な機能として、通信相手の認証、通信内容の暗号化、改竄の検出を提供する。	a00-00-a
CRYPTREC	A project that evaluates and monitors the security of e-government-recommended cryptography, and investigates and examines appropriate implementation and operation methods for cryptography. This project publishes "CRYPTREC Ciphers List".	クリプトレック（CRYPTREC）	電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。『CRYPTREC暗号リスト』を公開している。	a00-00-a
entropy	Measure of the disorder, randomness or variability in a closed system NOTE: The entropy of a random variable X is a mathematical measure of the amount of information provided by an observation of X.	エントロピー	一つの閉鎖系における無秩序さ、無作為性又は変動性の尺度。 注記 確率変数Xのエントロピーとは、Xの観測によって提供される情報量の数学的尺度である。	a00-00-a
message authentication code, MAC	Cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data EXAMPLE: A Hash Based Message Authentication Code	メッセージ認証コード（MAC）	偶然の及び意図的なデータの変更を検出するための、対称鍵を使用した暗号チェックサム 例 ハッシュベースメッセージ認証コード	a00-00-a
reverse engineering	After analysing the structure of the product with disassembling the machine, observing the operation of the product and analysing the operation of the software etc., an action of investigating the specifications of the production method, the operationg principle and the drawing etc. and the source code etc. from the analysis result.	リバースエンジニアリング	機械を分解したり、製品の動作を観察したり、ソフトウェアの動作を解析したり等により、製品の構造を分析し、そこから製造方法や動作原理、設計図などの仕様やソースコードなどを調査すること	a00-00-a
tamper resistance	The capability to prevent the reading of confidential data through irregular means. Examples of irregular means include applying physical stress (e.g., high or low voltage, strong electromagnetic fields, or high or low temperatures) to induce actions that deviate from normal state, then impeding the normal operation of logical security functions in an attempt to gain unauthorized logical access.	耐タンパー性	非正規な手段による機密データの読み取りを防ぐ能力のこと。 非正規な手段の例として、物理的なストレス (高電圧、低電圧、強電磁界、高温、低温など) を印加して正常時と異なる動作を誘発させ、論理的セキュリティ機能の正常な動作を妨げて論理的な不正アクセスを試みる等がある。	a00-00-a
hardware security module, HSM	Hardware function that protects the confidentiality and integrity of information (e.g., key information, security function programs) inside the microcomputer.	ハードウェアセキュリティモジュール（HSM）	マイコンが内蔵する情報（鍵情報、セキュリティ機能のプログラム等）の機密性及び完全性を保護するためのハードウェア機能	a00-00-a
side-channel attack	Exploitation of the fact that the instantaneous side-channels emitted by cryptographic device depends on the data it processes and on the operation, it performs to retrieve secret parameter. The attack can be performed by power consumption analysis, electromagnetic emissions analysis, timing analysis, among others.	サイドチャネル攻撃	暗号化装置の正規の入出力とは違う副次的な放出物が、その瞬間において処理するデータや操作に依存してしまう事実を利用して、秘密のパラメータを取得する攻撃手法。 消費電力分析、電磁放射分析、タイミング分析等によって攻撃が実施できる。	a00-00-a
backdoor	A path created to intrude into the in-vehicle parts without passing through the authorized path or following the authorized procedure. If security is not applied to the functions provided for product development and inspection, a hacker may use the functions as backdoor.	バックドア	正規の経路や手続きを経ずに車載部品に侵入するために設置される経路。製品の開発用、検査用に設けられる機能のセキュリティが掛かっていない場合、ハッカーにバックドアとして利用される可能性がある。	a00-00-a
Data Link Connector, DLC	An interface that connects an in-vehicle ECU to a failure diagnostics tool, etc.	データリンクコネクタ（DLC）	車載ECUと故障診断ツールなどを接続するためのインターフェース	a00-00-a
test access port	Input/output port of microcontroller provided for debug testing E.g. JTAG	テストアクセスポート	マイコンのデバッグ・テストのために準備されたマイコンの入出力ポート。JTAG 等。	a00-00-a
privileged function	Subset of functions in the interfaces of in-vehicle components to which Toyota does not allow access by ordinary customers. If they remain, there is a risk that they will be used as attack entry points or backdoors. EXAMPLE: Programming functions, functions to support the calibration of vehicle parameters, functions to read ECU programs and data, product inspection functions.	特権機能	車載部品が有するインタフェース上の機能のうち、トヨタが一般的なお客様による使用を許容しないもの。残置すると、攻撃の入口やバックドアとして利用される恐れがある。 例：プログラムデバッグ機能、車両パラメータの適合を支援する機能、ECUのプログラム/データを読書きする機能、製品検査用機能	a00-00-a
denial-of-service attack, DoS attack	Abbreviation for denial of service attack. Attack designed to impede normal system operation by transmitting a large number of messages or other signals to overload the CPU processing capacity of the receiving ECU and block other normal messages.	DoS攻撃	Denial of Service攻撃の略。 大量のメッセージ送信等により、受信側ECUのCPU処理負荷を飽和させたり、他の正常なメッセージ送信を阻害したりすることで、システムが正常に稼働できない状態にする攻撃。	a00-00-a
bandwidth	Communication rate The volume of communication per unit time. It is expressed in bits per second (bps).	帯域	通信速度。単位時間あたりの通信量。bps [bit per sec]の単位で表される。	a00-00-a
firewall	Software, device, or other system set at the boundary between a given computer or network and an external network to relay and monitor internal and external communication and protect internal data from external attacks. It blocks communication deemed unauthorized based on certain criteria.	ファイアウォール（Firewall）	あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのこと。一定の基準に従って不正と判断した通信を遮断する。	a00-00-a

filtering	The function of a firewall, router, etc. installed on a network boundary, etc. to detect unauthorized data from data packet transmitted/received in and outside of the network and discarding it	フィルタリング	ネットワークの境界などに設置されたファイアウォールやルータなどが、内外で送受信されるデータのまとまり(パケット)の中から一定の基準に基づいて不正なものを検知し、破棄する機能	a00-00-a
network based intrusion detection system, NIDS	System that monitors network traffic and detects malicious intrusions.	ネットワーク型侵入検知システム（NIDS）	ネットワークの通信内容等を監視して、不正侵入を検知するシステム	a00-00-a
host based intrusion detection system, HIDS	System that monitors internal events in a single host (ECU) and detects malicious intrusions.	ホスト型侵入検知システム（HIDS）	単一のホスト（ECU）内部で発生するイベントを監視して、不正侵入を検知するシステム	a00-00-a
padding	Processing that adjusts the length by adding data after the input to use the block encryption protocol.	パディング	ブロック暗号方式を使用するために、入力の後ろにデータを追加して長さを合わせる処理のこと	a00-00-a
information sharing and analysis centers, ISAC	The group's purpose is to share each organization's information about Cybersecurity attacks and vulnerabilities among all the members.	アイザック（ISAC）	メンバー間での、各組織のサイバーセキュリティ攻撃および脆弱性に関する情報の共有を目的とするグループ	a00-00-a
security incident response team, SIRT	Organization conducting activities with the aims listed below. Installation is also recommended by the national government and the industry. • Minimize losses due to an attack or intrusion in the event of an incident. • Disseminate information on vulnerabilities, strengthen the in-house information security framework, and take other measures to enhance the proactive prevention of information security breaches.	サート（SIRT）	以下の目的のために活動する組織。国・業界も設置を推奨。 ・インシデント発生の際、攻撃や侵入による損失を最小限にする。 ・脆弱性情報の展開、社内の情報セキュリティ管理体制の強化等、情報セキュリティ侵害の未然防止を向上させる。	a00-00-a
request for comments, RFC	RFC is a publication of the IETF (Internet Engineering Task Force). It is the principal technical development and standards-setting bodies for the Internet.	Request for Comments（RFC）	標準化団体IETF（Internet Engineering Task Force）が発行する文書。技術の標準仕様等が記載されている。	a00-00-a
supply chain	Network of organisations that are involved, through upstream and downstream linkages, in the different processes and activities that produce value in the form of products and services in the hands of the ultimate consumer	サプライチェーン	製品開発における上流と下流のリンケージによって最終消費者が手にする商品やサービスといった形態の価値を生むプロセスおよび活動に携わる組織のネットワーク	a00-00-a
tier1 supplier	A tier 1 supplier directly supplies products or services to the OEM usually through a contractual arrangement.	Tier1 サプライヤ	通常は契約に基づいて、製品やサービスをOEMに直接供給するサプライヤ。	a00-00-a
software development vendor	Business operator that develops software and sells it directly. It can be shortened to developing vendor in some contexts.	ソフトウェア開発ベンダ	ソフトウェアを開発し直接販売する業者。文脈によっては開発ベンダと略すことがある。	a00-00-a
lifecycle of a vehicle	Vehicle life span, starting from initial stage of development and continuing through production, sales, actual use, and disposal. It is also called the life cycle.	車両ライフサイクル	開発の初期から生産・販売・実使用・廃棄に至る車両の存続期間。文脈によってはライフサイクルと略すことがある。	a00-00-a
quality assurance	Systematic activities conducted by the organization to clearly meet customer and community needs, as well as to verify and demonstrate they are met.	品質保証	顧客・社会のニーズを満たすことを確実にし、確認し、実証するために、組織が行う体系的な活動。	a00-00-a
record on behavior function, RoB	Function within the diagnostics function that logs control data as RoB information when a vehicle state triggers a determination of *unexpected vehicle behavior* .	RoB機能	ダイアグ機能において、「予期せぬ車両挙動」と判断した車両状態をトリガに、その際の制御データをRoB情報として記録する機能	a00-00-a
CAN300	Function that legitimately uploads CAN messages passing through the in-vehicle network to the data center (the uploaded CAN-IDs are fixed).	CAN300	車載ネットワークに流れるCANメッセージをデータセンタに常時アップロードする機能（アップロードするCAN-IDは固定）	a00-00-a
CAN300+	CAN message uploading function that extends CAN 300 functionality to enable varying the transmitted CAN-IDs.	CAN300+	CAN300機能を拡張し、対象CAN-IDを可変としたCANメッセージアップロード機能	a00-00-a
Cybersecurity Interface Agreement, CIA	Agreement between customer and supplier concerning distributed cybersecurity activities. NOTE: Previously CIAD was defined, but it was changed in "ISO/SAE 21434:2021" to CIA. For this reason, both are posted for now.	CIA	サイバーセキュリティ活動を分担するときの、サプライヤとの間の取り決め 注記　従来はCIADと表記されていたが、『ISO/SAE FDIS 21434:2021』ではCIAに変更になった。このため、いまのところは両者ともに掲載する。	a00-01-a
Cybersecurity Interface Agreement for Development, CIAD	Agreement between customer and supplier concerning distributed cybersecurity activities.	CIAD	サイバーセキュリティ活動を分担するときの、サプライヤとの間の取り決め	a00-01-a
On-board Security Event, SEv	A piece of data detected in a vehicle that is indicative of an attack or is suited to assess the security state of the vehicle.	On-board Security Event（SEv）	車両において検知された、車両への攻撃を示す情報、もしくは車両のセキュリティ状態を評価するのに有用な情報	a00-01-a
Qualified Security Event, QSEv	A QSEv is a SEv that has passed filters.	Qualified Security Event（QSEv）	フィルタを通過したSEv	a00-01-a

Abbreviated term	Definition	略語	解説	Revised version
AES	Advanced Encryption Standard			a00-00-a
Auto-ISAC	Automotive Information Sharing & Analysis Center			a00-00-a
CAL	Cybersecurity Assuarance Level			a00-00-a
CAN	Controller Area Network			a00-00-a
CERT/CC	Computer Emergency Response Team Coordination Center			a00-00-a
CIA	Cybersecurity Interface Agreement NOTE: Previously CIAD was defined, but it was changed in "ISO/SAE 21434:2021" to CIA.		注記　従来はCIADと表記されていたが、『ISO/SAE FDIS 21434:2021』ではCIAに変更になった。このため、いまのところは両者ともに掲載する。	a00-01-a
CIAD	Cybersecurity Interface Agreement for Development			a00-00-a
CISO	Chief Information Security Officer, Chief Information & Security Officer			a00-00-a
CMAC	Cipher based Message Authentication Code			a00-00-a
CRYPTREC	CRYPTography Research and Evaluation Committees			a00-00-a
CS	CyberSecurity			a00-00-a
CSIRT	Computer Security Incident Response Team			a00-00-a
CSMS	CyberSecurity Management System			a00-00-a
CSP	Critical Security Parameter			a00-00-a
CVD	Coordinated Vulnerability Disclosure			a00-00-a
CVSS	Common Vulnerability Scoring System			a00-00-a
CWE	Common Weakness Enumeration			a00-00-a
DB	DataBase			a00-00-a
DoS	Denial of Service			a00-00-a
DLC	Data Link Connector			a00-00-a

ECE	Economic Commission for Europe	ECE	欧州経済委員会	a00-02-a
ECU	Electronic Control Unit			a00-00-a
FIPS	Federal Information Processing Standards			a00-02-a
FV	Freshness Value			a00-00-a
GB	Chinese national mandatory standards, "*Guojia Biaozhun* "	GB	中国国家強制標準	a00-02-a
GB/T	Chinese national recommended standards, "*Guojia Biaozhun/Tuijian* "	GB/T	中国国家推奨標準	a00-02-a
HIDS	Host based Intrusion Detection System			a00-00-a
HSM	Hardware Security Module			a00-00-a
HTTP	HyperText Transfer Protocol			a00-00-a
HTTPS	HyperText Transfer Protocol Secure			a00-00-a
IATF	International Automotive Task Force			a00-00-a
IDS	Intrusion Detection System			a00-00-a
IF	InterFace			a00-00-a
IP	Internet Protocol			a00-00-a
IPA	Information-technology Promotion Agency, Japan	IPA	独立行政法人 情報処理推進機構	a00-00-a
IPS	Intrusion Prevention System			a00-00-a
ISO	International Organization for Standardization	ISO	国際標準化機構	a00-00-a
ISAC	Information Sharing and Analysis Center			a00-00-a
JASIC	Japan Automobile Standards Internationalization Center	JASIC	自動車基準認証国際化研究センター	a00-02-a
JASPAR	Japan Automotive Software Platform and Architecture	JASPAR	一般社団法人JASPAR	a00-00-a
J-Auto-ISAC	Japan Automotive Information Sharing & Analysis Center	J-Auto-ISAC	一般社団法人Japan Automotive ISAC	a00-02-a
JIS	Japanese Industrial Standards	JIS	日本産業規格	a00-00-a
JISA	Japan Information Technology Service Industry Association	JISA	一般社団法人 情報サービス産業協会	a00-00-a
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center	JPCERT/CC	一般社団法人 JPCERTコーディネーションセンター	a00-00-a
JTAG	Joint Test Action Group			a00-00-a
JVN	Japan Vulnerability Notes			a00-00-a
KATRI	Korea Automobile Testing & Research Institute	KATRI	韓国自動車安全研究院	a00-02-a
LAN	Local Area Network			a00-00-a
LIN	Local Interconnect Network			a00-00-a
MAC	Message Authentication Code			a00-00-a
MAC address	Media Access Control Address	MACアドレス	Media Access Control アドレス	a00-00-a
NALTEC	National Agency for Automobile and Land Transport Technology	NALTEC	独立行政法人自動車技術総合機構	a00-02-a
NESSIE	New European Schemes for Signature, Integrity, and Encryption			a00-02-a
NHTSA	National Highway Traffic Safety Administration	NHTSA	米国運輸省高速道路交通安全局	a00-00-a
NIDS	Network based Intrusion Detection System			a00-00-a
NIST	National Institute of Standards and Technology	NIST	米国国立標準技術研究所	a00-02-a
NTSEL	National Traffic Safety and Environment Laboratory NOTE: Internal organization of NALTEC	NTSEL	交通安全環境研究所 注記 独立行政法人自動車技術総合機構の内部機関	a00-02-a
NVD	National Vulnerability Database			a00-00-a
OEM	Original Equipment Manufacturer			a00-00-a
OS	Operating System			a00-00-a
OSS	Open-Source Software			a00-00-a
OTA	Over-the-Air			a00-01-a
PF	PlatForm			a00-00-a
POC	Point Of Contact			a00-00-a
PSIRT	Product Security Incident Response Team			a00-00-a
PSP	Public Security Parameter			a00-00-a
QSEv	Qualified Security Event			a00-01-a
R/C	Running Change			a00-00-a
RDDP	Request for Design & Development of Part	外設申	外注品設計申入書	a00-00-a
RFC	Request for Comments			a00-00-a
RoB	Record on Behavior			a00-00-a
SAE	Society of Automotive Engineers	SAE	米国自動車技術者協会	a00-00-a
SEv	On-board Security Event			a00-01-a
SHE	Secure Hardware Extension			a00-00-a
SI	System Integration			a00-00-a
SIRT	Security Incident Response Team			a00-00-a
S/N	Serial Number			a00-00-a
SSP	Sensitive Security Parameter			a00-00-a
SU	Software Update			a00-01-a
TCP	Transmission Control Protocol			a00-00-a
TCP/IP	Transmission Control Protocol / Internet Protocol			a00-00-a
TIS	Technical Instruction Sheet	TIS	技術指示書	a00-01-a
TLS	Transport Layer Security			a00-00-a
TLP	Traffic Light Protocol			a00-00-a
UDP	User Datagram Protocol			a00-00-a
UNECE	United Nations Economic Commission for Europe	UNECE	国際連合欧州経済委員会	a00-02-a
UN-R	United Nations Regulations			a00-01-a
USB	Universal Serial Bus			a00-00-a
Wi-Fi	Wireless Fidelity			a00-00-a
WP.29	UNECE World Forum for Harmonization of Vehicle Regulations	WP.29	国際連合欧州経済委員会 自動車基準調和世界フォーラム	a00-00-a
WVTA	Whole Vehicle Type Approval			a00-02-a
XML	eXtensible Markup Language			a00-00-a