関係各部署　御中

To departments concerned

Confidentiality classification	PROTECTED 関係者外秘	原紙保管 Storage of original	M/Y /
		コピー保管 Storage of copy	M/Y /

侵入検知 サイバーセキュリティイベントロギング要求仕様書
Requirements Specification of Cyber Security Event Logging

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 4G
System Network & Architecture Development Dept. 4G
E/E Architecture Development Div.

No. SEC-ePF-IDS-ANO-REQ-SPEC-a01-07-a

承認 Approved by	調査 Checked by	作成 Created by	
平林	松井 竹山	河野 石田	2022/12/28

適用先 Target	エントリーポイント ECU/VM、メッセージ認証機能を有する ECU/VM、2 層目メッセージフィルタリング機能を有する ECU/VM Allocated to ECU/VMs that have entry points, message authentication functions, or second-layer message filtering functions.
特記 Special note	【展開規則　Distribution rule】 必要に応じて、関係会社・関係部署（海外事業体、ボデーメーカ、ECU サプライヤ）への展開をお願いします。 Please distribute this document to affiliated companies, or departments (e.g. overseas business entities, car body manufacturers, or ECU suppliers) if necessary. 【問合せ先　Contact information】 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 セキュリティ仕様問合せ窓口 System Network & Architecture Development Dept. E/E Architecture Development Div. Contact for Security Inquiries email: epf-sec-sp@mega.tec.toyota.co.jp

変更履歴

Version	変更内容	日付	変更者
a01-00-a	新規作成	2020/06/23	46F 4G 稲垣
a01-01-a	誤記修正（ヘッダ仕様書英名） 適用範囲を「エントリーポイント ECU/VM、メッセージ認証機能を有する ECU/VM」に変更 1.1 本書の目的を詳細化、2.1 システム構成を簡略化 参照文書を追加（AUTOSAR SWS,PWS） QSEv 送信機能（IDSANR_10001 - 10013）を追加 要求一覧を追加、ハードウェア関連要件を記載	2021/04/5	46F 4G 稲垣
a01-01-b	英訳を追加 記入漏れのため、適用範囲を「エントリーポイント ECU/VM、メッセージ認証機能を有する ECU/VM、2 層目メッセージフィルタリングを有する ECU/VM」に変更 上位文書名を「車両サイバーセキュリティコンセプト定義書」に変更	2021/05/14	46F 4G 稲垣
a01-02-a	・仕様書名称変更 ・構成、項目名変更 ・ロギング要求に対応する防御仕様と項番を追記 ・ロギング要求の詳細化 ・SEv、QSEv 要件の記載を詳細化	2021/08/06	46F 4G 竹山
a01-03-a	・1.3 前提条件 修正 ・無線 LAN、BT 以外の通信のロギング要求 削除 ・3.1.2 死活監視機能　追加 ・SEv 生成機能 修正 ・QSEv 生成機能 修正 ・QSEv 送信機能 修正 ・QSEv 保管機能 修正 ・SEv、QSEv 要件の(T.B.D.)解消	2021/12/03	46F 4G 竹山

a01-04-a	・1.3 前提条件から対象外の防御要求を削除 ・1.5.2 参照文書[15], [23]を削除、[31]を追加 ・サードパーティアプリケーションのサイバーセキュリティ要件に関するロギング要求を削除 ・センター接続機器認証要求仕様に関するロギング要求を削除 ・侵入検知 対応スレーブ向け 侵入阻止 要求仕様に由来する要求を削除 ・3.1.5 QSEv 送信機能要求を修正 ・【要求事項：IDSANR_06200】誤記修正 ・3.1.6 QSEv 保管の要求の文言を修正 ・品質要求、設計値の(T.B.D.)解消 ・Annex1 ダイアグタイムスタンプ仕様参照、可変長データの設定方法補足追加、誤記訂正	2022/02/03	46F 4G 竹山
a01-05-a	・要求一覧にハードウェア関連要件の列を追加 ・IDSANR_10001 Context Data 修正 （KZK ID、通信ヘッダ） ・IDSANR_10003 削除 ・IDSANR_10005 修正 ・IDSANR_01100 適用条件修正 ・IDSANR_01200 適用条件修正 ・IDSANR_10006 QSEv 保管の要求を変更 ・IDSANR_10009 UserDefineDTC と DID の要求追加 ・IDSANR_10007 QSEv 読み出しの SID を明確化 ・IDSANR_10008 QSEv 消去の SID を明確化	2022/04/29	46F 4G 竹山
a01-05-b	・IDSANR_10006 誤記訂正 ・IDSANR_10007 ダイアグ仕様参照を追記 ・IDSANR_10008 ダイアグ仕様参照を追記 ・IDSANR_10009 UserDefMemoryDTC の値修正	2022/05/20	46F 4G 竹山
a01-05-c	・IDSANR_10006 補足の一部を要求として記載	2022/06/09	46F 4G 竹山
a01-05-d	・IDSANR_11108 誤記訂正(日本語版のみ) ・IDSANR_06200 誤記訂正(日本語版のみ) ・IDSANR_11109 誤記訂正(日本語版のみ) ・IDSANR_06300 誤記訂正(日本語版のみ) ・IDSANR_10004 誤記訂正(英語版のみ) ・IDSANR_10005 誤記訂正(英語版のみ)	2022/07/05	46F 4G 竹山

a01-06-a	・表 1-1 誤記訂正 ・表 1-3 参照文書追加 ・表 2-2 誤記訂正(IDSANR_12000 削除) ・IDSANR_11108 誤記訂正(英語版のみ) ・IDSANR_14010 仕様明確化 ・IDSANR_09101 ➢ 仕様修正 ➢ ContextData 修正(SEC-ePF-IDS-ANO-REQ-SPEC-a01-06-a_Annex1_draft.xlsx H 列 191 行目) ・IDSANR_10005 仕様修正 ・IDSANR_05300 仕様修正 ・IDSANR_14030 仕様修正 ・軽微な誤記訂正	2022/11/25	46F 4G 石田
a01-07-a	・表 1-1 誤記訂正 ・表 1-3 参照文書追加、削除 ・2.3 節及び表 2-2 適用条件に関する記述を追加 ・IDSANR_06102 ContextData 修正(SEC-ePF-IDS-ANO-REQ-SPEC-a01-07-a_Annex1.xlsx) ・IDSANR_04301 ContextData 修正(SEC-ePF-IDS-ANO-REQ-SPEC-a01-07-a_Annex1.xlsx) ・IDSANR_11108 可読性向上 ・IDSANR_06200 可読性向上 ・IDSANR_11109 可読性向上 ・IDSANR_06300 可読性向上 ・IDSANR_11115 誤記訂正（英語版のみ） ・IDSANR_06400 誤記訂正（英語版のみ） ・IDSANR_11111 誤記訂正、可読性向上 ・IDSANR_07102 誤記訂正、可読性向上 ・IDSANR_11112 可読性向上 ・表 3-19 誤記訂正 (0xC5E2, 0x85E2, 0x85E1, 0x85E3, 0x85E4 削除) ・軽微な誤記訂正（英語版のみ）	2022/12/28	46F 4G 河野 石田

目次

1. はじめに

1.1. 本書の目的

サイバーセキュリティイベントロギングシステム（以下本システム）の目的はサイバー攻撃から車両を守る防御機能の動作を記録することである。本システムによって記録される防御機能の動作は、米国国立標準研究所（NIST）が作成したサイバーセキュリティ対策に関するフレームワークにおける「検知」機能（参照文書[4]）の実現に用いられる。本システムの要求を定義することが本書の目的である。

1.2. 適用先

本書はエントリーポイント ECU/VM、メッセージ認証機能を有する ECU/VM、2 層目メッセージフィルタリングを有する ECU/VM に適用する。

1.3. 前提条件

本書にて言及される防御機能については、表 1-1 に記載の文書を参照のこと。

表 1-1：本書の対象となる防御要求

防御要求仕様書	対象機能記載箇所
無線通信セキュリティ要求仕様書	4.2 ファイアウォールに関する要求 4.3.1 センターと接続する場合の要求 4.3.2 センター以外の車外機器と接続する場合の要求
センター通信セキュリティ要求仕様書	4.1 セキュア通信確立要件
メッセージフィルタリング要求仕様書	3 フィルタリング要件 4 ダイアグフィルタリング要件 5 ロギングフィルタリング要件
2 層目メッセージフィルタリング要求仕様書	4 フィルタリング要件
メッセージ認証（フル FV 版）要求仕様書	4.4 認証子付きメッセージの検証処理
Phase6 ダイアグシステム標準通信仕様 （TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications）	10.4 SecurityAccess (27_{16}) service 10.6 Authentication (29_{16}) service 11.7 WriteDataByIdentifier($2E_{16}$) service
OTA4.0 ソフト更新マスタ ECU 要求仕様書	3.6.16 完了後処理 3.6.18 例外処理
車載鍵管理スレーブ要求仕様書	5.1 セーフキーナンバー取得応答機能 5.2 鍵更新機能（単一更新） 5.3 鍵更新機能（複数スレーブ一括更新） 5.4 鍵検証機能（複数スレーブ一括検証）
車載鍵管理マスタ要求仕様書	5.1 MAC 鍵更新情報送信機能
センター接続機器認証要求仕様書	4.2 センター接続機器認証

1.4. 要求事項の記載

【要求事項：**】と記載されているものが要求である。ここで、<補足>と記載されているものは単に補足事項であり要求ではない。

1.5. 関連文書

上位文書、参照文書を本節にて示す。なお、関連文書のバージョンは ECU の要求仕様書に従うこと。

1.5.1. 上位文書

表 1-2：上位文書

No.	文書名	Ver.
1	車両サイバーセキュリティコンセプト定義書	-

1.5.2. 参照文書

表 1-3：参照文書

No.	文書名	Ver.
1	AUTOSAR_SWS_IntrusionDetectionSystemManager	R20-11
2	AUTOSAR_PRS_IntrusionDetectionSystem	R20-11
3	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	-
4	Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11	1.1
5	無線通信セキュリティ要求仕様書	-
6	センター通信セキュリティ要求仕様書	-
7	メッセージフィルタリング要求仕様書	-
8	2 層目メッセージフィルタリング要求仕様書	-
9	メッセージ認証（フル FV 版）要求仕様書	-
10	TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	-
11	欠番	-
12	車載鍵管理スレーブ要求仕様書	-
13	車載鍵管理マスタ要求仕様書	-
14	セキュアブート要求仕様書	-

15	欠番	-
16	センター接続機器認証要求仕様書	-
17	侵入検知 検知マスタ要求仕様書	-
18	QSEv 生成要求仕様書	-
19	欠番	-
20	ISO/SAE 14229-1	-
21	Phase5 ダイアグシステム標準通信仕様	-
22	侵入検知 IdsM Instance ID・Sensor Instance ID 定義書	-
23	欠番	-
24	RFC7296	-
25	RFC4555	-
26	RFC5026	-
27	RFC6407	-
28	RFC5246	-
29	RFC8446	-
30	欠番	-
31	タイムスタンプ要求仕様書	-
32	PF LAN 仕様書	-
33	車載 Ethernet 通信機能仕様書	-
34	CAN(CAN-FD)通信フェールセーフ仕様書	-
35	車載 Ethernet 通信フェールセーフ仕様書	-
36	OTA4.0 ソフト更新マスタ ECU 要求仕様書	-

1.6. 用語定義

本書で用いる用語については、1.5.2 参照文書[3] を参照のこと。

2. 要求概要

2.1. システムコンテキスト

サイバーセキュリティイベントロギングシステム（以下、本システム）のシステムコンテキストをデータフローダイアグラムで示す（図 2-1）。円は本システムを、四角は本システムと情報やサービスのやり取りを行う主体を表す。本システムは 1.3 に示した防御機能の動作を記録し QSEv で保管もしくは検知マスタへ送信する。保管された QSEv はダイアグ通信およびリモートダイアグ通信で読み出される。

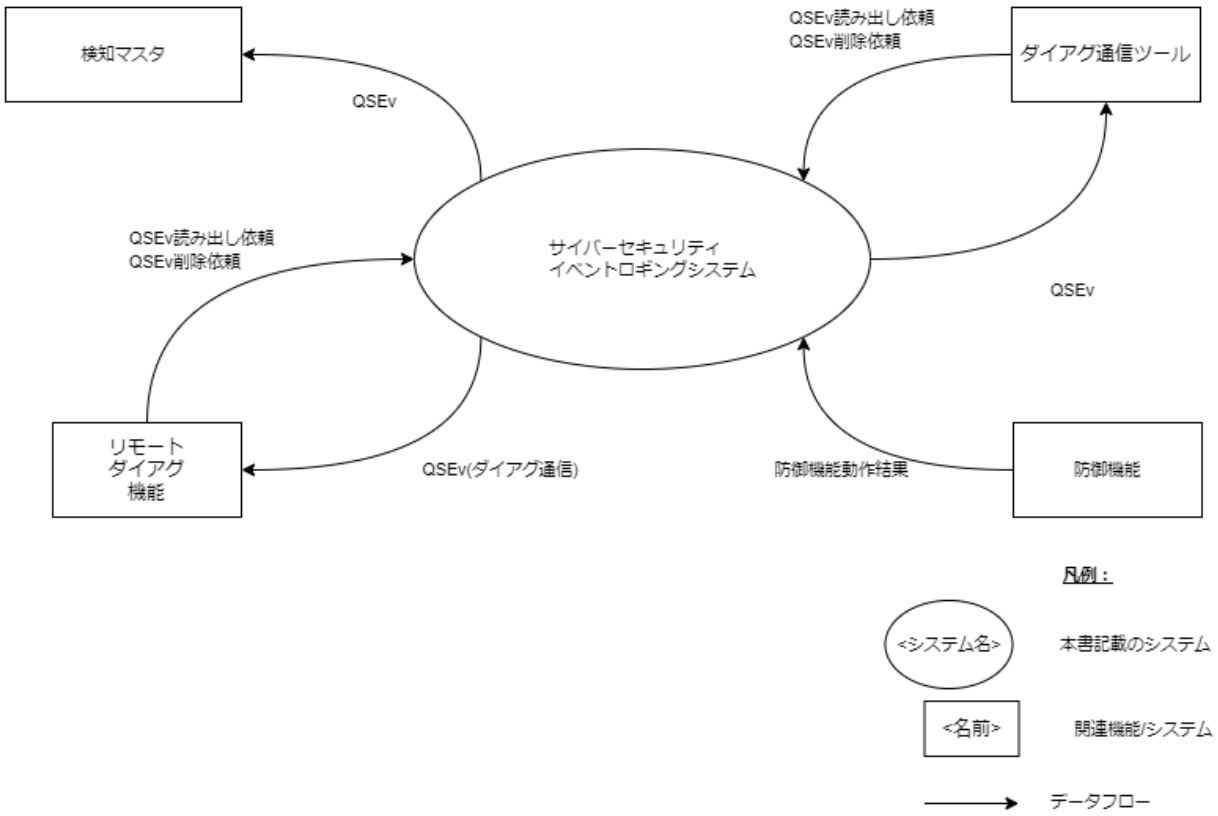

図 2-1：システムコンテキスト図

2.2. システム動作概要

本システムは表 2-1 に示す事象のいずれかが生じたとき、UML アクティビティ図（図 2-2）で示すとおりの動作をする。

表 2-1：本システムの動作始点となる事象

事象番号	本システム動作始点となる事象
①	本システム搭載先 ECU・VM の防御機能・死活監視機能の動作
②	本システムに保管されている QSEv の読み出し依頼
③	本システムに保管されている QSEv の削除依頼

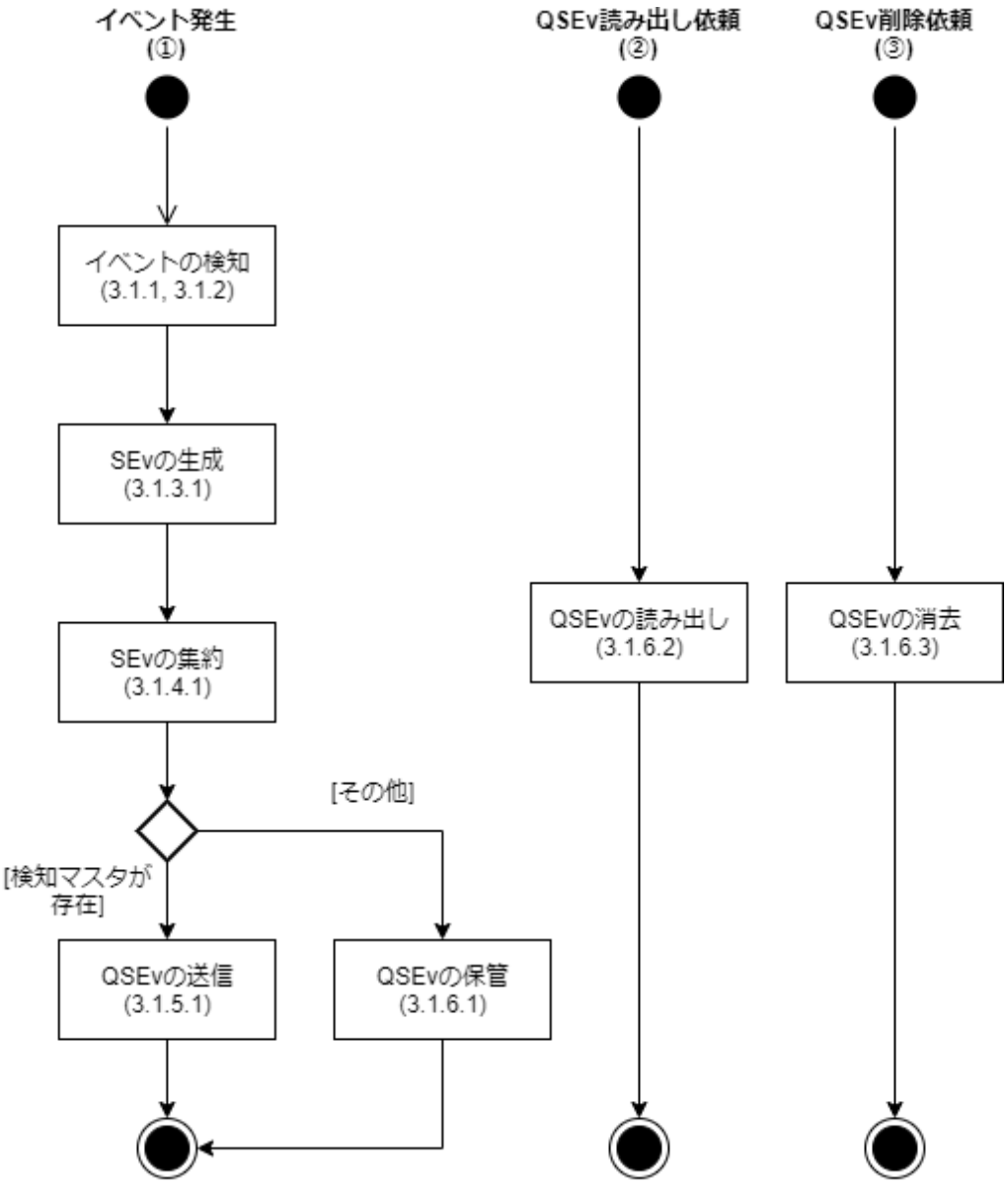

図 2-2：動作概要

2.3. 要求一覧

本書で定義する要求の一覧及び各要求の適用条件を表 2-2 に示す。また、ハードウェア選定時に参照すべき要件をハードウェア関連要求として示す。ハードウェアの採否は各要件に従うこと。

表 2-2：要求一覧

分類			要求 ID	ハードウェア関連要求	適用条件
機能要求	セキュリティイベントロギング要求	無線通信セキュリティ要求仕様に関するロギング要求	IDSANR_01100	No	無線通信セキュリティ要求仕様が引き当たる ECU/VM
			IDSANR_01200	No	
			IDSANR_11150	No	
			IDSANR_02150	No	
			IDSANR_11104	No	
			IDSANR_02200	No	
			IDSANR_11105	No	
			IDSANR_02300	No	
		センター通信セキュリティ要求仕様に関するロギング要求	IDSANR_11107	No	センター通信セキュリティ要求仕様が引き当たる ECU/VM
			IDSANR_05301	No	
			IDSANR_05302	No	
		メッセージフィルタリング要求仕様に関するロギング要求	IDSANR_06101	No	メッセージフィルタリング要求仕様が引き当たる ECU/VM
			IDSANR_06102	No	
			IDSANR_04101	No	
			IDSANR_04301	No	
		2層目メッセージフィルタリング要求仕様に関するロギング要求	IDSANR_04102	No	2 層目メッセージフィルタリング要求仕様が引き当たる ECU/VM
			IDSANR_04302	No	
		メッセージ認証（フル FV 版）要求仕様に関するロギング要求	IDSANR_05100	No	メッセージ認証（フル FV 版）要求仕様が引き当たる ECU/VM
			IDSANR_05200	No	
			IDSANR_05300	No	
		Phase6 ダイアグシステム標準通信仕様に関するロギング要求	IDSANR_11108	No	メッセージフィルタリング要求仕様が引き当たる ECU/VM
			IDSANR_06200	No	
			IDSANR_11109	No	
			IDSANR_06300	No	
			IDSANR_11115	No	VIN 情報を保管し、ダイアグ通信で VIN 情報を更新する ECU/VM
			IDSANR_06400	No	

		OTA4.0 ソフト更新マスタ ECU 要求仕様に関するロギング要求	IDSANR_11111	No	OTA4.0 ソフト更新マスタ ECU 要求仕様が引き当たる ECU/VM
			IDSANR_07102	No	
		車載鍵管理スレーブ要求仕様に関するロギング要求	IDSANR_11112	No	車載鍵管理スレーブ要求仕様が引き当たる ECU/VM
			IDSANR_09101	No	
		車載鍵管理マスタ要求仕様に関するロギング要求	IDSANR_09102	No	車載鍵管理マスタ要求仕様が引き当たる ECU/VM
	死活監視機能	死活監視	IDSANR_10002	No	本書が引き当たる全ての ECU/VM
	SEv 生成機能	SEv 生成	IDSANR_10001	No	
	QSEv 生成機能	SEv の集約	IDSANR_10004	No	
	QSEv 送信機能	QSEv の送信	IDSANR_10005	No	検知マスタがいずれかの ECU に存在する車両に搭載される ECU/VM
			IDSANR_10010	No	
	QSEv 保管機能	QSEv の保管	IDSANR_10006	No	検知マスタがいずれの ECU にも存在しない車両に搭載される ECU/VM
			IDSANR_10009	No	
		QSEv の読み出し	IDSANR_10007	No	
		QSEv の消去	IDSANR_10008	No	
品質要求			IDSANR_12000	No	本書が引き当たる全ての ECU/VM
制約			IDSANR_13000	No	
設計値			IDSANR_14000	No	
			IDSANR_14010	No	
			IDSANR_14030	No	

3. システム要求

サイバーセキュリティロギングシステム要求を定義する。

3.1. 機能要求

本節では機能要求を定義する。

3.1.1. セキュリティイベントロギング機能

本項に記載の防御機能が動作した際に、セキュリティイベントロギング機能は 3.1.3 に記載の SEv 生成機能へ動作結果を通知すること。

3.1.1.1. 無線通信セキュリティ要求仕様に関するロギング要求

3.1.1.1.1. ファイアウォール機能に関するロギング要求

【要求事項：IDSANR_01100】

本要求は、下記のいずれかに該当する ECU/VM に適用される。

(1) 車外と Cellular/Wi-Fi/Bluetooth 通信のいずれかを終端する機能を持つ

(2) (1)を経由して TLS 終端となる

上記通信を監視するファイアウォール機能が、車外からのフレームを破棄したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_01200】

本要求は、下記のいずれかに該当する ECU/VM に適用される。

(1) 車外と Cellular/Wi-Fi/Bluetooth 通信のいずれかを終端する機能を持つ

(2) (1)を経由して TLS 終端となる

上記通信を監視するファイアウォール機能が、車外へのフレームを破棄したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

3.1.1.1.2. TLS 通信機能に関するロギング要求

【要求事項：IDSANR_11150】

TLS 通信機能（RFC5246、RFC8446）がサーバ証明書の検証もしくは接続先サーバにて行われるクライアント認証、車外機が持つクライアント証明書の検証に成功したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_02150】

TLS 標準仕様（RFC5246、RFC8446）もしくは TLS 標準以外のクライアント認証を使用する場合、

TLS 通信機能が表 3-1～表 3-3 の記録対象に該当する失敗をしたとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

表 3-1：RFC5246（TLS1.2）における記録対象のエラーコード一覧

ID	エラーコード名	記録対象
0x0A	unexpected_message	○
0x14	bad_record_mac	○
0x15	decryption_failed_RESERVED	○
0x16	record_overflow	○
0x1E	decompression_failure	○
0x28	handshake_failure	○
0x29	no_certificate_RESERVED	○
0x2A	bad_certificate	○
0x2B	unsupported_certificate	○
0x2C	certificate_revoked	○
0x2D	certificate_expired	○
0x2E	certificate_unknown	○
0x2F	illegal_parameter	○
0x30	unknown_ca	○
0x31	access_denied	○
0x32	decode_error	○
0x33	decrypt_error	○
0x3C	export_restriction_RESERVED	○
0x46	protocol_version	○
0x47	insufficient_security	○
0x50	internal_error	○
0x5A	user_canceled	×
0x64	no_renegotiation	×
0x6E	unsupported_extension	○

表 3-2：RFC8446（TLS1.3）における記録対象のエラーコード一覧

ID	エラーコード名	記録対象
0x0A	unexpected_message	○
0x14	bad_record_mac	○

0x16	record_overflow	○
0x28	handshake_failure	○
0x2A	bad_certificate	○
0x2B	unsupported_certificate	○
0x2C	certificate_revoked	○
0x2D	certificate_expired	○
0x2E	certificate_unknown	○
0x2F	illegal_parameter	○
0x30	unknown_ca	○
0x31	access_denied	○
0x32	decode_error	○
0x33	decrypt_error	○
0x46	protocol_version	○
0x47	insufficient_security	○
0x50	internal_error	○
0x56	inappropriate_fallback	○
0x5A	user_canceled	×
0x6D	missing_extension	○
0x6E	unsupported_extension	○
0x70	unrecognized_name	○
0x71	bad_certificate_status_response	○
0x73	unknown_psk_identity	○
0x74	certificate_required	○
0x78	no_application_protocol	○

表 3-3：TLS 標準以外のクライアント認証における記録対象のエラーコード一覧

ID	エラーコード名	記録対象
0xFF	Client authentication failure	○

3.1.1.1.3. 無線 LAN 通信機能に関するロギング要求

【要求事項：IDSANR_11104】

無線 LAN 通信機能が WPA で接続認証に成功したとき、セキュリティイベントロギング機能は、SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_02200】
無線 LAN 通信機能が WPA で接続認証に失敗したとき、セキュリティイベントロギング機能は、SEv 生成機能に結果を通知する必要がある。

3.1.1.1.4. Bluetooth 通信機能に関するロギング要求

【要求事項：IDSANR_11105】
ペアリングによる接続認証を使用する場合、Bluetooth 通信機能がペアリングによる接続認証に成功したとき、セキュリティイベントロギング機能は、SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_02300】
ペアリングによる接続認証を使用する場合、Bluetooth 通信機能がペアリングによる接続認証に失敗したとき、セキュリティイベントロギング機能は、SEv 生成機能に結果を通知する必要がある。

3.1.1.2. センター通信セキュリティ要求仕様に関するロギング要求

【要求事項：IDSANR_ 11107】
IPsec 通信機能がセンター通信中継モジュールとの相互認証に成功したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_05301】
IPsec 通信機能がセンター通信中継モジュールとの相互認証において、IKEv2 関連仕様（RFC7296、RFC4555、RFC5026、RFC6407）の Error Types の内で記録対象（表 3-4）となっている失敗をしたとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

表 3-4：Error Types 一覧及び記録対象

ID	Error Types	記録対象	出典
0x01	UNSUPPORTED_CRITICAL_PAYLOAD	○	RFC7296
0x04	INVALID_IKE_SPI	○	RFC7296
0x05	INVALID_MAJOR_VERSION	○	RFC7296
0x07	INVALID_SYNTAX	○	RFC7296
0x09	INVALID_MESSAGE_ID	○	RFC7296
0x0B	INVALID_SPI	○	RFC7296
0x0E	NO_PROPOSAL_CHOSEN	○	RFC7296
0x11	INVALID_KE_PAYLOAD	○	RFC7296
0x18	AUTHENTICATION_FAILED	○	RFC7296
0x22	SINGLE_PAIR_REQUIRED	○	RFC7296
0x23	NO_ADDITIONAL_SAS	○	RFC7296

0x24	INTERNAL_ADDRESS_FAILURE	○	RFC7296
0x25	FAILED_CP_REQUIRED	○	RFC7296
0x26	TS_UNACCEPTABLE	○	RFC7296
0x27	INVALID_SELECTORS	○	RFC7296
0x28	UNACCEPTABLE_ADDRESSES	○	RFC4555
0x29	UNEXPECTED_NAT_DETECTED	○	RFC4555
0x2A	USE_ASSIGNED_HoA	○	RFC5026
0x2B	TEMPORARY_FAILURE	○	RFC7296
0x2C	CHILD_SA_NOT_FOUND	○	RFC7296
0x2D	INVALID_GROUP_ID	○	RFC6407(Draft)
0x2E	AUTHORIZATION_FAILED	○	RFC6407(Draft)

【要求事項：IDSANR_05302】
IPsec 通信機能が受信したパケットの完全性の検証に失敗したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

3.1.1.3. メッセージフィルタリング要求仕様に関するロギング要求

【要求事項：IDSANR_06101】
CAN 通信における SID フィルタ機能がダイアグメッセージを破棄したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_06102】
Ethernet 通信における SID フィルタ機能がダイアグメッセージを破棄したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_04101】
DLC1 層目アプリの CAN フレームフィルタ機能が CAN フレームを破棄したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_04301】
DLC1 層目アプリの Ethernet フレームフィルタ機能が Ethernet フレームを破棄したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

3.1.1.4. 2 層目メッセージフィルタリング要求仕様に関するロギング要求

【要求事項：IDSANR_04102】

2 層目防御 ECU・アプリの CAN フレームフィルタ機能が CAN フレームを破棄したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_04302】
2 層目防御 ECU・アプリの Ethernet フレームフィルタ機能が Ethernet フレームを破棄したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

3.1.1.5. メッセージ認証（フル FV 版）要求仕様に関するロギング要求

【要求事項：IDSANR_05100】
メッセージ認証機能による CAN FD フレームの検証結果が「検証 NG」(参照文書[9])のとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_05200】
メッセージ認証機能による Ethernet フレームの検証結果が「検証 NG」(参照文書[9])のとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_05300】
参照文書[34][35]で定義されたダイアグマスク条件が成立している間、セキュリティイベントロギング機能は、SEv 生成機能に異常を通知してはならない。

3.1.1.6. Phase6 ダイアグシステム標準通信仕様（TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications）に関するロギング要求

【要求事項：IDSANR_11108】

参照文書[7]（メッセージフィルタリング要求仕様書）を適用する ECU/VM に適用される。プログラミングセッション以外のセッションにおいて、ダイアグ通信機能が SecurityAccess (SID 0x27)の記録対象となっている Sub-Function（表 3-5）の実行に成功したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

表 3-5：SecurityAccess (SID 0x27) 成功時の記録対象 Sub-Function

Sub-Function	記録対象
0x01	×
0x02	○
0x03	×
0x04	○
0x05	×
0x06	○
0x07-0x7D	×
0x08-0x7E	○
0x21	×
0x22	×
0x23-0x42	×
0x5F	×
0x60	×

【要求事項：IDSANR_06200】

参照文書[7]（メッセージフィルタリング要求仕様書）を適用する ECU/VM に適用される。プログラミングセッション以外のセッションにおいて、ダイアグ通信機能が SecurityAccess (SID 0x27)での認証において記録対象となっている Sub-Function（表 3-6）の実行に失敗し、かつ、その失敗が記録対象となっている（表 3-7）とき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

表 3-6：SecurityAccess (SID 0x27) 失敗時の記録対象 Sub-Function

Sub-Function	記録対象
0x01	○
0x02	○

Sub-Function	記録対象
0x03	○
0x04	○
0x05	○
0x06	○
0x07-0x7D	○
0x08-0x7E	○
0x21	○
0x22	○
0x23-0x42	○
0x5F	○
0x60	○

表 3-7：SecurityAccess (SID 0x27)失敗時の記録対象 NRC

NRC	記録対象
0x10	×
0x11	×
0x12	○
0x13	○
0x21	×
0x22	○
0x24	○
0x31	○
0x33	×
0x35	○
0x36	○
0x37	○
0x78	×
0x7E(※1)	○
0x7F	×

※1：NRC 0x7E は、参照文書[21]を参照。

【要求事項：IDSANR_11109】

参照文書[7]（メッセージフィルタリング要求仕様書）を適用する ECU/VM に適用される。プログラミングセッション以外のセッションにおいて、ダイアグ通信機能が Authentication (SID 0x29) の記

録対象となっている Sub-Function（表 3-8）の実行に成功したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

表 3-8：Authentication (SID 0x29)成功時の記録対象 Sub-Function

Sub-Function	記録対象
0x00	×
0x01	○
0x02	○
0x03	○
0x04	×
0x05	○
0x06	○
0x07	○
0x08	×
0x09 – 0x7F	×

【要求事項：IDSANR_06300】
参照文書[7]（メッセージフィルタリング要求仕様書）を適用する ECU/VM に適用される。プログラミングセッション以外のセッションにおいて、ダイアグ通信機能が Authentication (SID 0x29) の記録対象となっている Sub-Function（表 3-9）の実行に失敗し、かつ、その失敗が記録対象となっている（表 3-10）とき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

表 3-9：Authentication (SID 0x29) 失敗時の記録対象 Sub-Function

Sub-Function	記録対象
0x00	○
0x01	○
0x02	○
0x03	○
0x04	○
0x05	○
0x06	○
0x07	○
0x08	○
0x09 – 0x7F	○

表 3-10：Authentication (SID 0x29)失敗時の記録対象 NRC

NRC	記録対象
0x10	×
0x11	×
0x12	○
0x13	○
0x21	×
0x22	○
0x24	○
0x33	×
0x78	×
0x7F	×

【要求事項：IDSANR_11115】
本要求は、VIN 情報を保管し、ダイアグ通信で VIN 情報を更新する ECU/VM に適用される。ダイアグ通信機能が WriteDataByIdentifier (SID 0x2E)での VIN の更新に成功したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_06400】
本要求は、VIN 情報を保管し、ダイアグ通信で VIN 情報を更新する ECU/VM に適用される。ダイアグ通信機能が WriteDataByIdentifier (SID 0x2E)での VIN の更新に失敗したとき、かつ、その失敗が記録対象となっている（表 3-11）とき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

表 3-11：VIN 更新（SID 0x2E、DID 0xF190)失敗時の記録対象 NRC

NRC	記録対象
0x10	×
0x11	×
0x13	○
0x21	×
0x22	○
0x31	○
0x33	×
0x72	○
0x78	×
0x7F	×

3.1.1.7. OTA4.0 ソフト更新マスタ ECU 要求仕様に関するロギング要求

【要求事項：IDSANR_11111】

本要求は、参照文書[36]（OTA4.0 ソフト更新マスタ ECU 要求仕様書）が引き当たる ECU/VM に適用される。OTA リプログラミングが成功したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_07102】

本要求は、参照文書[36]（OTA4.0 ソフト更新マスタ ECU 要求仕様書）が引き当たる ECU/VM に適用される。 OTA リプログラミングが失敗したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

3.1.1.8. 車載鍵管理スレーブ要求仕様に関するロギング要求

【要求事項：IDSANR_11112】

鍵更新機能が鍵の単一更新または一括更新に成功したとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

【要求事項：IDSANR_09101】

鍵更新機能が記録対象となっている鍵更新処理（表 3-12）に失敗し、かつ、その失敗が記録対象となっている（表 3-13）とき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

表 3-12：鍵更新処理失敗時の記録対象リクエストメッセージ

リクエストメッセージ				記録対象
SID	Sub-Function	パラメータ		
		Phase5	Phase6	
0x22	-	DID 0x010B	DID 0xA901	○
0x31	0x01/0x81	RID 0x1010	RID 0xD904	○
0x31	0x01/0x81	RID 0x100E	RID 0xD902	○
0x31	0x01/0x81	RID 0x100F	RID 0xD903	×

表 3-13：鍵更新処理失敗時の記録対象 NRC

NRC	記録対象
0x10	×

NRC	記録対象
0x11	×
0x12	○
0x13	○
0x14	○
0x21	×
0x22	○
0x24	○
0x31	○
0x33	×
0x72	○
0x78	×
0x7F	×

3.1.1.9. 車載鍵管理マスタ要求仕様に関するロギング要求

【要求事項：IDSANR_09102】

MAC 鍵更新情報送信禁止の状態で、MAC 鍵更新情報送信開始を要求されたとき、セキュリティイベントロギング機能は SEv 生成機能に結果を通知する必要がある。

3.1.2. 死活監視機能

3.1.2.1. 死活監視

【要求事項：IDSANR_10002】

死活監視機能は、設計値[HeartbeatInterval]が経過するたびに、3.1.3 に記載の SEv 生成機能へ通知する必要がある。

3.1.3. SEv 生成機能

3.1.3.1. SEv の生成

【要求事項：IDSANR_10001】

SEv 生成機能は、3.1.1 セキュリティイベントロギング機能及び 3.1.2 死活監視機能から通知されるたびに、SEv（表 3-14）を生成し QSEv 生成機能に通知する必要がある。ここで、Security Event ID と Context Data は、SEC-ePF-IDS-ANO-REQ-SPEC-a01-07-a_Annex1.xlsx に従って設定される必要がある。また、Context Data は、ビッグエンディアンにて内容が設定される必要がある。

表 3-14：生成される SEv

Field Name	Length	Description
Security Event ID	16 bit	QSEv 生成機能が QSEv に設定する Event Definition ID と Sensor Instance ID の組み合わせを一意に識別するための情報を設定する。 - Event Definition ID は、検知したイベントに基づいて設定される。 - Sensor Instance ID は、固定値 0 である。 <補足> 本フィールドは、AUTOSAR CP では IdsMInternalEventId 型の引数として実現される。
Context Data Size※	8 bit or 32 bit	Context Data のバイト長。ソフトウェアの設計者等が Event Definition ID 毎にその Context Data の長さに応じてどちらか一方を選択する。
Context Data※	Variable length	検知されたイベントについての情報を格納するバイト列であり、イベントを通知した検知機能の要求 ID に基づいて設定する。また、そのイベントが発生した時点でのダイアグタイムスタンプ等も設定する。

（※）死活監視の SEv 及び CAN 通信で検知マスタに送信される SEv は、ContextData を持たない。

3.1.4. QSEv 生成機能

3.1.4.1. SEv の集約

【要求事項：IDSANR_10004】

QSEv 生成機能は、参照文書[18]に定義される方式を用いて、通知される SEv を Security Event ID ごとに集約し QSEv を生成する必要がある。Security Event ID ごとの集約の設定は【要求事項：IDSANR_14010】で定義する。

3.1.5. QSEv 送信機能

3.1.5.1. QSEv の送信

【要求事項：IDSANR_10005】

検知マスタ(参照文書[17])がいずれかの ECU に存在する場合に、本要求事項は適用される。QSEv 生成機能が QSEv を生成する度に、QSEv 送信機能は、自 ECU から検知マスタへ送信する際に用いるプロトコルに応じて下記で定義されるフレームを生成し、検知マスタへ送信する必要がある。

・自 ECU が、CAN 通信または CAN FD 通信を用いて、フレームを送信する場合：

参照文書[32]において QSEV_DATA_[ECU ノード名(※1)]で定義される Data Label を含むフレーム。なお、QSEV_DATA_[ノード名]には図 3-1 で定義されるデータが格納される。

・自 ECU が、Ethernet 通信を用いて、フレームを送信する場合：

表 3-15 で定義される構造のフレーム。なお、表 3-15 の IDS Message には図 3-1 で定義されるデータが格納される。

Protocol Version	Protocol Header	IdsM Instance ID	Sensor Instance ID	Event Definition ID	Count	Reserved	Context Data (※2)
msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb

図 3-1：データ構造

表 3-15：フレームフォーマット（Ethernet の場合）

Layer	Protocol	Description	Note
L2	Ethernet	各フィールドの値は、参照文書[33]に従うこと なお、Destination MAC address は、検知マスタが搭載される CEN2 の MAC address を指定すること	
L3	IPv4	各フィールドの値は、参照文書[33]に従うこと なお、Destination IP address は、検知マスタが搭載される CEN2 の IP address を指定すること	
L4	TCP	各フィールドの値は、参照文書[33]に従うこと 但し、Destination Port Number、Source Port Number は、下記に示す値を指定すること ・Destination Port Number ：50004 (0xC354) ・Source Port Number ：50004 (0xC354)	
L5	IDS	各フィールドの値は、下記データをビックエンディアン方式で格納し、構成すること ・Message ID (4Byte) ：ALL 0 ・Length (4Byte) ：Message ID, Length, IDS Message のデータ長の和 ・IDS Message (Variable) ：図 3-1 で定義されるデータ	IDS プロトコルの詳細は、参照文書[2]参照

（※1）[ECU ノード名]は、自 ECU を示すノード名に置換すること。該当する Data Label が参照文書[32]中に存在しない場合は、本書の発行元部署に相談すること。
（※2）CAN FD 通信及び Ethernet 通信に適用される。CAN 通信は適用対象外。

【要求事項：IDSANR_10010】
QSEv 送信機能が、QSEv を検知マスタへ送信する場合に本要求は適用される。QSEv 送信機能による QSEv 送信がネットワークの Wakeup 要因もしくは Sleep 阻害要因となる場合、QSEv 送信機能は QSEv を送信してはならない。
<補足>
QSEv の送信が、バッテリ上がりの原因となることを避けるため。

3.1.6. QSEv 保管機能

3.1.6.1. QSEv の保管

【要求事項：IDSANR_10006】

検知マスタがいずれの ECU にも存在しない場合に、本要求事項は適用される。QSEv 保管機能は、死活監視の SEv より生成された QSEv を除いて、QSEv 生成機能が生成する最新[NumberOfQSEvs]個の QSEv を、Event Definition ID 毎に不揮発性メモリに保管する必要がある。ただし、QSEv 保管機能は、不意のリセット（バッテリ瞬断、低電圧等）時に QSEv を保管しなくてもよい。なお、QSEv 保管機能は、不揮発性メモリの書き込み回数上限を考慮し設計される必要がある。

<補足>

検知マスタがいずれかの ECU に存在する場合には、QSEv を保管するかは任意である。

不揮発性メモリの書き込み回数上限を考慮した設計の例として、IG-ON 中は RAM 領域に QSEv をバッファリングし、IG-OFF 時に不揮発性メモリに書き込む設計が挙げられる。

【要求事項： IDSANR_10009】

QSEv 保管に関する UserDefMemoryDTC および DID は表 3-16、表 3-17、表 3-18 に従う必要がある。

UserDefMemoryDTC および DID は以下の方針で定義している。

・UserDefMemoryDTC：Event Definition ID ごとに定義

・DID：QSEv 全体で一つ定義、かつ、全 Event Definition ID に対して共通で一つ定義

表 3-16：UserDefMemoryDTC 関連情報

UserDefMemoryDTC	FTB	対応 Event Definition ID	Memory Selection
U2B00	0x00	0x8501	0x14
U2B01	0x00	0x8502	0x14
U2B02	0x00	0xC503	0x14
U2B03	0x00	0x8503	0x14
U2B04	0x00	0xC504	0x14
U2B05	0x00	0x8504	0x14
U2B06	0x00	0xC505	0x14
U2B07	0x00	0x8505	0x14
U2B08	0x00	0xC506	0x14
U2B09	0x00	0x8506	0x14
U2B0A	0x00	0x8530	0x14
U2B0B	0x00	0x8550	0x14
U2B0C	0x00	0x8570	0x14
U2B0D	0x00	0x8590	0x14
U2B0E	0x00	0x8591	0x14
U2B0F	0x00	0x85A0	0x14
U2B10	0x00	0x85A1	0x14
U2B11	0x00	0x85A2	0x14
U2B12	0x00	0x85A3	0x14
U2B13	0x00	0xC5A4	0x14
U2B14	0x00	0x85A4	0x14
U2B15	0x00	0xC5A5	0x14
U2B16	0x00	0x85A5	0x14
U2B17	0x00	0xC5A6	0x14
U2B18	0x00	0x85A6	0x14
U2B19	0x00	0xC5D0	0x14

U2B1A	0x00	0x85D0	0x14
U2B1B	0x00	0x85E0	0x14

表 3-17：QSEv 保管に関する DID

DID	Data	Length [Bit]
0xA910	Protocol Version	4
	Protocol Header	4
	IdsM Instance ID	10
	Sensor Instance ID	6
	Event Definition ID	16
	Count	16
	Reserved	8
	Context Data (※1)	Variable Length

(※1) CAN FD 通信及び Ethernet 通信に適用される。CAN 通信は適用対象外。

表 3-18：QSEv 保管データ例(Event Definition ID:0x8501 の QSEv を 5 件保管)

UserDefMemoryDTC	FTB	UserDefDTC SnapshotRecordNumber	Description
U2B00	0x00	0x01	最新[NumberOfQSEvs]個の QSEv のうち、最も古い QSEv (DID: 0xA910)
		0x02	最新[NumberOfQSEvs]個の QSEv のうち、2 番目に古い QSEv (DID: 0xA910)
		0x03	最新[NumberOfQSEvs]個の QSEv のうち、3 番目に古い QSEv (DID: 0xA910)
		0x04	最新[NumberOfQSEvs]個の QSEv のうち、4 番目に古い QSEv (DID: 0xA910)
		0x05	最新[NumberOfQSEvs]個の QSEv のうち、最も新しい QSEv (DID: 0xA910)

3.1.6.2. QSEv の読み出し

【要求事項：IDSANR_10007】

QSEv が不揮発性メモリに保管される場合に、本要求事項は適用される。不揮発性メモリに保管される QSEv は、オフボードクライアントおよびオンボードクライアントからダイアグ通信 SID 0x19 (Sub Function 0x17/0x18)で読み出しできる必要がある。ただし、前述の QSEv が一時的に揮発性メモリ上に置かれている場合、揮発性メモリ上のそれら QSEv が読み出される必要がある。

ダイアグ通信の詳細は、参照文書[10]を参照。

3.1.6.3. QSEv の消去

【要求事項：IDSANR_10008】

QSEv が不揮発性メモリに保管される場合に、本要求事項は適用される。不揮発性メモリに保管される QSEv は、オフボードクライアントからダイアグ通信 SID 0x14 (QSEv 出力用 MemorySelection 0x14)で消去できる必要がある。

ダイアグ通信の詳細は、参照文書[10]を参照。

3.2. 品質要求

無し

3.3. 制約

本節では制約を定義する。

【要求事項：IDSANR_13000】

機密性または完全性に関する法規の対象となる ECU に本システムが搭載される場合に本要求事項は適用される。QSEv 保管機能は当該法規に従う必要がある。

3.4. 設計値

本節では設計値を定義する。

【要求事項：IDSANR _14000】

本節で定義する設計値は各要求で定められる条件下で設定変更可能である必要がある。

【要求事項：IDSANR _14010】

QSEv 生成・保管は表 3-19 の設計値を用いて行われる必要がある。なお、単位などの設計値に関する条件は表 3-20 と表 3-21 に従う必要がある。

表 3-19：QSEv 生成・保管の設計値

名称	Event Definition ID	Sensor Instance ID	設定値（※1）
IdsMEventAggregationTimeInterval	0x8501	0x0	0.3
	0x8502	0x0	0.3
	0xC503	0x0	0.3
	0x8503	0x0	0.3
	0xC504	0x0	0.3
	0x8504	0x0	0.3
	0xC505	0x0	0.3
	0x8505	0x0	0.3
	0xC506	0x0	0.3
	0x8506	0x0	0.3
	0x8530	0x0	0.3
	0x8550	0x0	0.3
	0x8570	0x0	0.3
	0x8590	0x0	0.3
	0x8591	0x0	0.3
	0x85A0	0x0	0.3
	0x85A1	0x0	0.3
	0x85A2	0x0	0.3
	0x85A3	0x0	0.3
	0xC5A4	0x0	0.3

	0x85A4	0x0	0.3
	0xC5A5	0x0	0.3
	0x85A5	0x0	0.3
	0xC5A6	0x0	0.3
	0x85A6	0x0	0.3
	0xC5C0	0x0	0.3
	0x85C0	0x0	0.3
	0xC5D0	0x0	0.3
	0x85D0	0x0	0.3
	0x85E0	0x0	0.3
	0xF500	0x0	0.3
IdsMContextDataSourceSelector	0x8501	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8502	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC503	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8503	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC504	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8504	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC505	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8505	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC506	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8506	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8530	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8550	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8570	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8590	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8591	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A1	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A2	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A3	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC5A4	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A4	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC5A5	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A5	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC5A6	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A6	0x0	IDSM_FILTERS_CTX_USE_FIRST

	0xC5C0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85C0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC5D0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85D0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85E0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xF500	0x0	IDSM_FILTERS_CTX_USE_FIRST
NumberOfQSEvs	0x8501	0x0	5
	0x8502	0x0	5
	0xC503	0x0	5
	0x8503	0x0	5
	0xC504	0x0	5
	0x8504	0x0	5
	0xC505	0x0	5
	0x8505	0x0	5
	0xC506	0x0	5
	0x8506	0x0	5
	0x8530	0x0	5
	0x8550	0x0	5
	0x8570	0x0	5
	0x8590	0x0	5
	0x8591	0x0	5
	0x85A0	0x0	5
	0x85A1	0x0	5
	0x85A2	0x0	5
	0x85A3	0x0	5
	0xC5A4	0x0	5
	0x85A4	0x0	5
	0xC5A5	0x0	5
	0x85A5	0x0	5
	0xC5A6	0x0	5
	0x85A6	0x0	5
	0xC5C0	0x0	5
	0x85C0	0x0	5
	0xC5D0	0x0	5
	0x85D0	0x0	5
	0x85E0	0x0	5

	0xF500	0x0	5

表 3-20：QSEv 生成設計値メタ情報

名称	単位	型	下限値	上限値
IdsMEventAggregationTimeInterval (※2)	秒	EcucFloatParamDef	0.05	10.00
IdsMContextDataSourceSelector	-	EcucEnumerationParamDef	IDSM_FILTERS_CTX_USE_FIRST	IDSM_FILTERS_CTX_USE_LAST

※1： IdsMEventAggregationTimeInterval および IdsMContextDataSourceSelector の設定値がハイフン「-」であるのは集約を行わないことを意味する。

※2：設定値列に記載の値と同じ値を設定できない場合、記載の設定値より小さく、かつ、設定可能な設計値のうち、最大の値が設定される必要がある。

表 3-21：QSEv 保管設計値メタ情報

名称	説明	単位	下限値	上限値
NumberOfQSEvs	QSEv の保管件数	-	0	10

【要求事項：IDSANR _14030】

QSEv 生成・保管以外の設計値は表 3-22 に従う必要がある。なお、単位などの設計値に関する条件は表 3-23 に従う必要がある。

表 3-22：QSEv 生成・保管以外の設計値

名称	説明	設定値
HeartbeatInterval	死活監視 SEv 生成間隔	1.0

表 3-23：QSEv 生成・保管以外の設計値メタ情報

名称	単位	下限値	上限値
HeartbeatInterval	秒	0.0	10.0

Revision history

Version	Change	Date	Reviser
a01-00-a	First version issued	2020/06/23	46F 4G Inagaki
a01-01-a	Clerical error modified (specification name in header), Target name modified to “entry-point ECUs/VMs, ECUs/VMs with a message authentication function”, “1.1 Purpose of this document” refined and “2.1 System structure” simplified, References AUTOSAR SWS and PWS added, QSEv transmission function (IDSANR_10001-10013) added, List of requirements and indicator of hardware relevance added	2021/04/05	46F 4G Inagaki
a01-01-b	English translation added, Target modified to “entry-point ECUs/VMs, EUs/VMs with a message authentication a function, ECUs/VMs with a 2nd layer message filtering function” due to omission, Name of input document modified to “Vehicle Cyber Security Concept Definition Document”	2021/05/14	46F 4G Inagaki
a01-02-a	Name of this document modified, Document structure modified, Relations between logging requirements and defense requirements, Logging requirements refined, Requirements of SEv and QSEv modified	2021/08/06	46F 4G Takeyama
a01-03-a	1.3 Prerequisite modified, Logging requirements of communication functions other than wireless LAN and Bluetooth deleted, 3.1.2 Heartbeat function deleted, 3.1.3 SEv creation function modified, Modified QSEv creation function, QSEv transmission function modified, QSEv storing function modified	2021/12/03	46F 4G Takeyama

a01-04-a	1.3 Prerequisite modified, 1.5.2 Reference [15], [23] deleted and [31] added, 3.1.1.10 Logging requirements of P19ePF Third-Party Application Cybersecurity Requirements deleted, 3.1.1.5 Requirements that comes from Requirements Specification of Response Slave of Intrusion Prevention System deleted, 3.1.1.7 Requirements related to a wired reprogramming function deleted, 3.1.5 QSEv transmission function requirement modified, [Requirement: IDSANR_06200] Table 3-8 modified. 3.1.6 QSEv storing function modified, 3.2 Quality requirements modified, 3.4 T.B.D. deleted Annex1 diagnostic timestamp specification reference added, variable-length data supplements added, clerical mistakes corrected	2022/02/03	46F 4G Takeyama
a01-05-a	- Added a column for “Hardware-Related Requirement” in List of requirements. - IDSANR_10001 Context Data modified. - (KZK ID, Communication Header) - IDSANR_10003 deleted - IDSANR_10005 modified. - IDSANR_01100 target condition modified. - IDSANR_01200 target condition modified. - IDSANR_10006 QSEv storing requirement modified - IDSANR_10009 UserDefineDTC and DID requirement added - IDSANR_10007 SID for QSEv read clarified - IDSANR_10008 SID for QSEv deletion clarified	2022/04/29	46F 4G Takeyama
a01-05-b	- IDSANR_10007 diagnostic specification reference added - IDSANR_10008 diagnostic specification reference added - IDSANR_10009 UserDefMemoryDTC value modified	2022/05/20	46F 4G Takeyama

a01-05-c	- IDSANR_10006 The part of the note moved to requirement	2022/06/09	46F 4G Takeyama
a01-05-d	- IDSANR_11108 Editorial errors corrected (Japanese version only) - IDSANR_06200 Editorial errors corrected (Japanese version only) - IDSANR_11109 Editorial errors corrected (Japanese version only) - IDSANR_06300 Editorial errors corrected (Japanese version only) - IDSANR_10004 Editorial errors corrected (English version only) - IDSANR_10005 Editorial errors corrected (English version only)	2022/07/05	46F 4G Takeyama
a01-06-a	- Table 1-1 editorial error corrected - Table 1-3 references added - Table 2-2 editorial error corrected(IDSANR_12202 deleted) - IDSANR_11108 editorial error corrected (English version only) - IDSANR_14010 Sensor Instance ID clarified - IDSANR_09101 ➢ Specification modified ➢ Context Data modified (H191 cell in SEC-ePF-IDS-ANO-REQ-SPEC-a01-06-a_Annex1_draft.xlsx) - IDSANR_10005 modified - IDSANR_05300 modified - IDSANR_14030 modified - Minor errors corrected	2022/11/25	46F 4G Ishida

a01-07-a	- Table 1-1 editorial error corrected - Table 1-3 reference added, deleted - Added a description for “Target Condition” in 2.3. and Table 2-2 - IDSANR_06102 ContextData modified (SEC-ePF-IDS-ANO-REQ-SPEC-a01-07-a_Annex1.xlsx) - IDSANR_04301 ContextData modified (SEC-ePF-IDS-ANO-REQ-SPEC-a01-07-a_Annex1.xlsx) - IDSANR_11108 readability improved - IDSANR_06200 readability improved - IDSANR_11109 readability improved - IDSANR_06300 readability improved - IDSANR_11115 editorial error corrected (English version only) - IDSANR_06400 editorial error corrected (English version only) - IDSANR_11111 editorial error corrected, readability improved - IDSANR_07102 editorial error corrected, readability improved - IDSANR_11112 readability improved - Table 3-19 editorial error corrected (0xC5E2, 0x85E2, 0x85E1, 0x85E3, 0x85E4 deleted) - Minor editorial errors corrected (English version only)	2022/12/28	46F 4G Kawano, Ishida

Table of coontents

1. Introduction

1.1. Purpose of this document

The goal of Cyber Security Event Logging (hereinafter referred to as *this system*) is to log operations of defense functions. Log recorded by this system is used to realize the *detection* function in the framework for cybersecurity (the reference [4]) defined by National Institute of Standards and Technology (hereinafter referred to as *NIST*). The purpose of this document is to define the requirements of this system.

1.2. Target

This document is allocated to entry-point ECUs/VMs, ECUs/VMs with massage authentication functions, and ECUs/VMs with 2nd layer Message Filtering functions.

1.3. Prerequisite

See documents on Table 1-1 for defense requirements referred in this document.

Table 1-1: Target defense requirements

Requirements specification	Defense function
Requirements Specification of Wireless Communication Security	4.2. Requirements related to Firewall 4.3.1. Requirements related to connection with center 4.3.2. Requirements related to Connection with Devices outside of vehicle except for Center
Requirements Specification of Center Communication Security	4.1. Requirements of Secure communication establishing
Requirements Specification of Message Filtering	3. Filtering Requirements 4. Diagnostic Filtering Requirements 5. Logging Filtering Requirements
Requirements Specification of 2nd Layer Message Filtering	4. Filtering Requirement
Requirements Specification of Message Authentication for FULL FV	4.4. Verification Processing of Message with Authentication Code
TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	10.4. SecurityAccess (27_{16}) service 10.6. Authentication (29_{16}) service 11.7. WriteDataByIdentifier($2E_{16}$) service
OTA4.0 SoftWare Update MasterECU Requirements	3.6.16. 完了後処理(only Japanese available) 3.6.18. 例外処理(only Japanese available)
Requirements Specification of In-vehicle Key Management Slave	5.1. Safe Key Number Acquisition Response Function 5.2. Key Update Function (Single Update) 5.3. Key Update Function (Batch Update for Multiple Slaves) 5.4. Key Verification Function (Multi-slave Batch Verification)
Requirements Specification of Key Management Master	5.1. MAC Key Update Information Transmission Function
Requirements Specification of Online Client Authentication	4.2. Center Connection Device Authentication

1.4. Description of requirements

We describe requirements as [Requirement: **] in this document where <Note> means just a supplementary note.

1.5. Related documents

Inputs documents, and references are shown in this section. If the specification of the ECU specifies the version of the reference, follow it.

1.5.1. Input documents

Table 1-2: Input documents

No.	Document name	Ver.
1	Vehicle Cyber Security Concept Definition Document	-

1.5.2. References

Table 1-3: References

No.	Document name	Ver.
1	AUTOSAR_SWS_IntrusionDetectionSystemManager	R20-11
2	AUTOSAR_PRS_IntrusionDetectionSystem	R20-11
3	Terms and Definitions related to Vehicle Cybersecurity and Privacy	-
4	Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, https: //www.nist.gov/publications/framework-improving -critical-infrastructure-cybersecurity-version-11	1.1
5	Requirements Specification of Wireless Communication Security	-
6	Requirements Specification of Center Communication Security	-
7	Requirements Specification of Message Filtering	-
8	Requirements Specification of 2nd Layer Message Filtering	-
9	Requirements Specification of Message Authentication for FULL FV	-
10	TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	-
11	Deleted	-
12	Requirements Specification of In-vehicle Key Management Slave	-
13	Requirements Specification of Key Management Master	-

14	Requirements Specification of Secure Boot	-
15	Deleted	-
16	Requirements Specification of Online Client Authentication	-
17	Requirements Specification of Intrusion Detection Master	-
18	QSEv creation requirements specification	-
19	Deleted	-
20	ISO/SAE 14229-1	-
21	Phase5 Standard Diagnostic Communication Framework Specifications	-
22	Instruction Document of IdsM Instance ID and Sensor Instance ID	-
23	Deleted	-
24	RFC7296	-
25	RFC4555	-
26	RFC5026	-
27	RFC6407	-
28	RFC5246	-
29	RFC8446	-
30	Deleted	-
31	Time Stamp requirement specification	-
32	PF LAN Specification	-
33	Automotive Ethernet communication function specification	-
34	CAN(CAN-FD) Communication Fail Safe specification	-
35	Automotive Ethernet Communication Fail Safe specification	-
36	OTA4.0 SoftWare Update MasterECU Requirements	-

1.6. Glossary

See the reference [3] for terms used in this document.

2. Requirements overview

2.1. System context

We show the system context with DFD (Figure 2-1). The circle means this system, and the rectangles mean subjects transmitting or receiving information or services. This system logs the operations of the defenses shown 1.3 and stores the logs in QSEv or sends them to the intrusion detection master. The QSEvs stored are read by diagnostic or remote diagnostic communication.

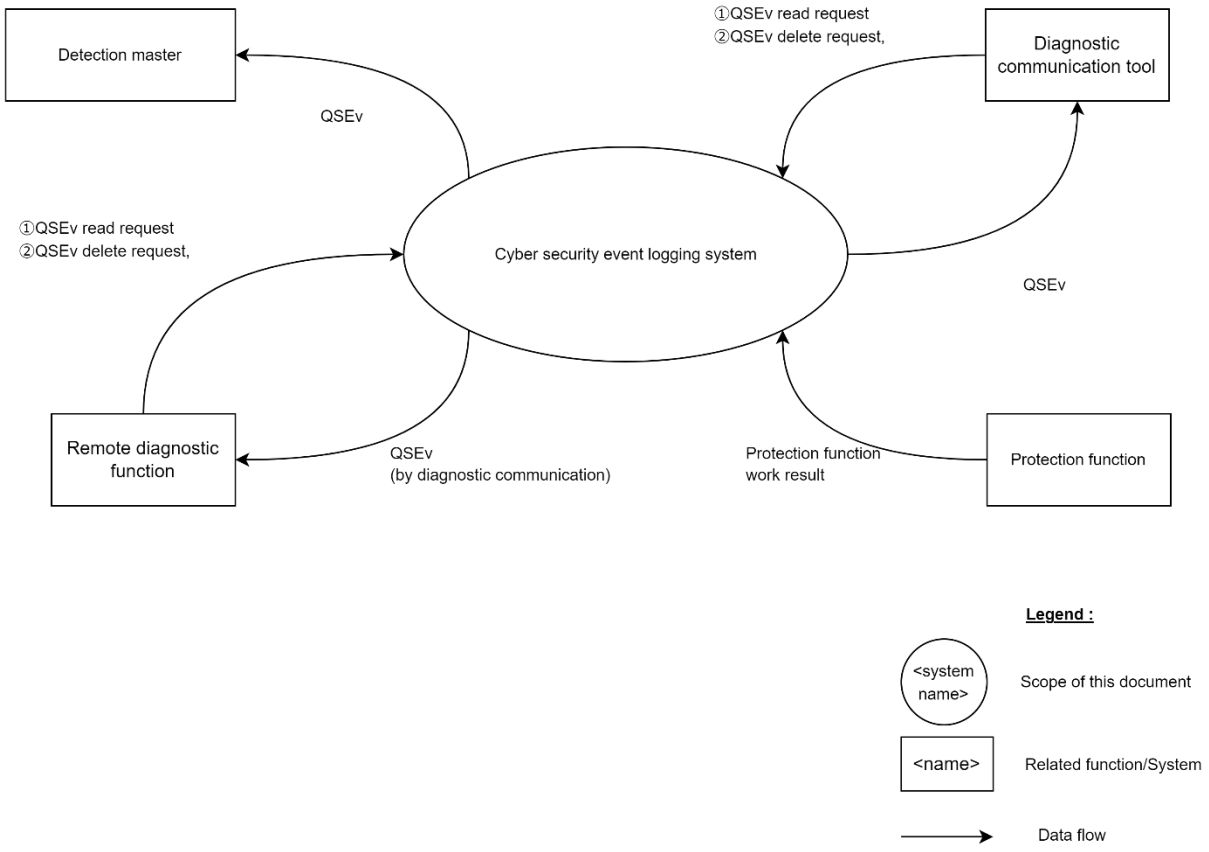

Figure 2-1: System context

2.2. System operation overview

This system operates as the UML activity diagram (Figure 2-2) when one of these events shown in (Table 2-1) happens.

Table 2-1: Events to start the operation

Event No.	Event that can be the starting point of the operation
①	Operation of defense functions on ECUs/VMs where this system is implemented
②	Request to read QSEvs stored by this system
③	Request to delete QSEvs stored by this system

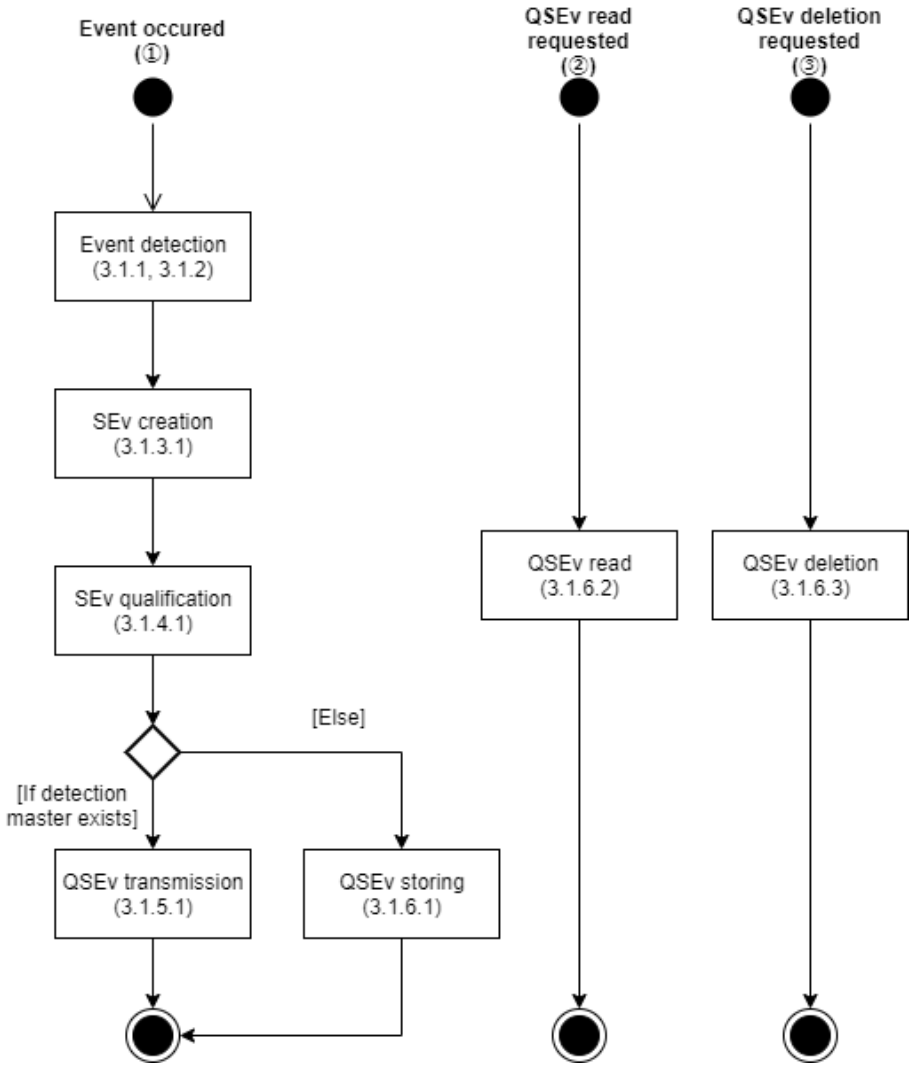

Figure 2-2: System operation

2.3. List of requirements

We show the list of all requirements defined in this document and Target Condition of each requirement (Table 2-2). In addition, we show the requirements which shall be referred in selecting hardware as hardware-related requirements.

Table 2-2: List of requirements

Category			Requirement ID	Hardware-Related Requirement	Target Condition
Functional requirements	Security event logging function	Logging requirements of Requirements Specification of Wireless Communication Security	IDSANR_01100	No	ECUs/VMs allocated to Requirements Specification of Wireless Communication Security
			IDSANR_01200	No	
			IDSANR_11150	No	
			IDSANR_02150	No	
			IDSANR_11104	No	
			IDSANR_02200	No	
			IDSANR_11105	No	
			IDSANR_02300	No	
		Logging requirements of Requirements Specification of Center Communication Security	IDSANR_11107	No	ECUs/VMs allocated to Requirements Specification of Center Communication Security
			IDSANR_05301	No	
			IDSANR_05302	No	
		Logging requirements of Requirements Specification of Message Filtering	IDSANR_06101	No	ECUs/VMs allocated to Requirements Specification of Message Filtering
			IDSANR_06102	No	
			IDSANR_04101	No	
			IDSANR_04301	No	
		Logging requirements	IDSANR_04102	No	ECUs/VMs allocated to
			IDSANR_04302	No	

		of Requirements Specification of 2nd Layer Message Filtering			Requirements Specification of 2nd Layer Message Filtering
		Logging requirements of Requirements Specification of Message Authentication for FULL FV	IDSANR_05100	No	ECUs/VMs allocated to Message Authentication for FULL FV
			IDSANR_05200	No	
			IDSANR_05300	No	
		Logging requirements of TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	IDSANR_11108	No	ECUs/VMs allocated to Requirements Specification of Message Filtering
			IDSANR_06200	No	
			IDSANR_11109	No	
			IDSANR_06300	No	
			IDSANR_11115	No	ECUs/VMs allocated to whose VINs are stored and whose VINs are updated by diagnostic communication
			IDSANR_06400	No	
		Logging requirements of OTA4.0 SoftWare Update	IDSANR_11111	No	ECUs/VMs allocated to OTA4.0 SoftWare Update
			IDSANR_07102	No	

		MasterECU Requirements			MasterECU Requirements
		Logging requirements of Requirements Specification of In-vehicle Key Management Slave	IDSANR_11112	No	ECUs/VMs allocated to Requirements Specification of In-vehicle Key Management Slave
			IDSANR_09101	No	
		Logging requirements of Requirements Specification of Key Management Master	IDSANR_09102	No	ECUs/VMs allocated to Requirements Specification of Key Management Master
	Heartbeat function	Heartbeat	IDSANR_10002	No	All ECUs/VMs allocated to this document
	SEv creation function	Anomaly notification SEv creation	IDSANR_10001	No	
	QSEv creation function	SEv qualification	IDSANR_10004	No	
	QSEv transmission	QSEv transmission	IDSANR_10005	No	ECUs/VMs equipped in a vehicle which has an intrusion detection master on any of the ECUs
			IDSANR_10010	No	
	QSEv storing function	QSEv storing	IDSANR_10006	No	ECUs/VMs equipped in a
			IDSANR_10009	No	

		QSEv read	IDSANR_10007	No	vehicle which does not have an intrusion detection master on any of the ECUs
		QSEv deletion	IDSANR_10008	No	
Quality requirements			IDSANR_12000	No	All ECUs/VMs allocated to this document
Constraints			IDSANR_13000	No	
Parameters			IDSANR_14000	No	
			IDSANR_14010	No	
			IDSANR_14030	No	

3. System requirements

We here define system requirements of this system.

3.1. Functional requirements

We define functional requirements in this section.

3.1.1. Security event logging function

When defense functions in this subsection work, a security event logging function shall notify a SEv creation function of the work result.

3.1.1.1. Logging requirements of Requirements Specification of Wireless Communication Security

3.1.1.1.1. Logging requirements of firewall function

[Requirement: IDSANR_01100]

This requirement shall be allocated to ECUs/VMs that meet any of the following items

(1) An ECU/VM that has capabilities to terminate Cellular/Wi-Fi/Bluetooth communications

(2) An ECU/VM that is an end of TLS connection through (1)

When a firewall function that monitors communications drops a frame from Out-Car, a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_01200]

This requirement shall be allocated to ECUs/VMs that meet any of the following items

(1) An ECU/VM that has capabilities to terminate Cellular/Wi-Fi/Bluetooth communications

(2) An ECU/VM that is a TLS termination through (1)

When a firewall function that monitors communications drops a frame to Out-Car, a security event logging function shall notify a SEv creation function of the work result.

3.1.1.1.2. Logging requirements of TLS communication function

[Requirement: IDSANR_11150]

When a standard TLS (RFC5246, RFC8446) function succeeds in one of the followings, a security event logging function shall notify a SEv creation of the work result.

- Verification of server certificate
- Client authentication in destination server
- Verification of client certificate of external device

[Requirement: IDSANR_02150]

When a TLS communication function fails in TLS standard client authentication (RFC5246 or RFC8446) or the other client authentication which are targeted to be recorded (Table 3-1, Table 3-2, and Table 3-3), a security event logging function shall notify a SEv creation function of the work result.

Table 3-1: List of error codes in RFC5246 (TLS1.2) to be recorded

ID	Error code	Targeted to be recorded
0x0A	unexpected_message	Yes
0x14	bad_record_mac	Yes
0x15	decryption_failed_RESERVED	Yes
0x16	record_overflow	Yes
0x1E	decompression_failure	Yes
0x28	handshake_failure	Yes
0x29	no_certificate_RESERVED	Yes
0x2A	bad_certificate	Yes
0x2B	unsupported_certificate	Yes
0x2C	certificate_revoked	Yes
0x2D	certificate_expired	Yes
0x2E	certificate_unknown	Yes
0x2F	illegal_parameter	Yes
0x30	unknown_ca	Yes
0x31	access_denied	Yes
0x32	decode_error	Yes
0x33	decrypt_error	Yes
0x3C	export_restriction_RESERVED	Yes
0x46	protocol_version	Yes
0x47	insufficient_security	Yes
0x50	internal_error	Yes
0x5A	user_canceled	No
0x64	no_renegotiation	No
0x6E	unsupported_extension	Yes

Table 3-2: List of error codes RFC8446 (TLS1.3) to be recorded

ID	Error Code	Targeted to be recorded
0x0A	unexpected_message	Yes
0x14	bad_record_mac	Yes
0x16	record_overflow	Yes
0x28	handshake_failure	Yes
0x2A	bad_certificate	Yes
0x2B	unsupported_certificate	Yes
0x2C	certificate_revoked	Yes
0x2D	certificate_expired	Yes
0x2E	certificate_unknown	Yes
0x2F	illegal_parameter	Yes
0x30	unknown_ca	Yes
0x31	access_denied	Yes
0x32	decode_error	Yes
0x33	decrypt_error	Yes
0x46	protocol_version	Yes
0x47	insufficient_security	Yes
0x50	internal_error	Yes
0x56	inappropriate_fallback	Yes
0x5A	user_canceled	No
0x6D	missing_extension	Yes
0x6E	unsupported_extension	Yes
0x70	unrecognized_name	Yes
0x71	bad_certificate_status_response	Yes
0x73	unknown_psk_identity	Yes
0x74	certificate_required	Yes
0x78	no_application_protocol	Yes

Table 3-3: List of non-standard error codes to be recorded

ID	Error Code	Targeted to be recorded
0xFF	Client authentication failure	Yes

3.1.1.1.3. Logging requirements of wireless LAN communication function

[Requirement: IDSANR_11104]

When a wireless LAN communication function succeeds in connection authentication using WPA, a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_02200]

When a wireless LAN communication function fails in connection authentication using WPA, a security event logging function shall notify a SEv creation function of the work result.

3.1.1.1.4. Logging requirements of Bluetooth communication function

[Requirement: IDSANR_11105]

When a Bluetooth communication function succeeds in connection authentication by paring, a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_02300]

When a Bluetooth communication function fails in connection authentication by paring, a security event logging function shall notify a SEv creation function of the work result.

3.1.1.2. Logging requirements of Requirements Specification of Center Communication Security

[Requirement: IDSANR_11107]

When an IPsec communication function succeeds in mutual authentication with a center communication module, a security event logging shall notify a SEv creation function of the work.

[Requirement: IDSANR_05301]

When an IPsec communication function fails in mutual authentication with a center communication module and the failure is targeted in Table 3-4, a security event logging shall notify a SEv creation function of the work.

Table 3-4: List of Error Types to be recorded

ID	Error Types	Targeted to be recorded	References
0x01	UNSUPPORTED_CRITICAL_PAYLOAD	Yes	RFC7296
0x04	INVALID_IKE_SPI	Yes	RFC7296
0x05	INVALID_MAJOR_VERSION	Yes	RFC7296
0x07	INVALID_SYNTAX	Yes	RFC7296
0x09	INVALID_MESSAGE_ID	Yes	RFC7296

0x0B	INVALID_SPI	Yes	RFC7296
0x0E	NO_PROPOSAL_CHOSEN	Yes	RFC7296
0x11	INVALID_KE_PAYLOAD	Yes	RFC7296
0x18	AUTHENTICATION_FAILED	Yes	RFC7296
0x22	SINGLE_PAIR_REQUIRED	Yes	RFC7296
0x23	NO_ADDITIONAL_SAS	Yes	RFC7296
0x24	INTERNAL_ADDRESS_FAILURE	Yes	RFC7296
0x25	FAILED_CP_REQUIRED	Yes	RFC7296
0x26	TS_UNACCEPTABLE	Yes	RFC7296
0x27	INVALID_SELECTORS	Yes	RFC7296
0x28	UNACCEPTABLE_ADDRESSES	Yes	RFC4555
0x29	UNEXPECTED_NAT_DETECTED	Yes	RFC4555
0x2A	USE_ASSIGNED_HoA	Yes	RFC5026
0x2B	TEMPORARY_FAILURE	Yes	RFC7296
0x2C	CHILD_SA_NOT_FOUND	Yes	RFC7296
0x2D	INVALID_GROUP_ID	Yes	RFC6407 (Draft)
0x2E	AUTHORIZATION_FAILED	Yes	RFC6407 (Draft)

[Requirement: IDSANR_05302]
When a IPsec communication function fails in verification of integrity of a packet, a security event logging function shall notify a SEv creation function of the work result.

3.1.1.3. Logging requirements of Requirements Specification of Message Filtering

[Requirement: IDSANR_06101]
When a SID filter function for CAN communication drops a diagnostics message, a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_06102]
When a SID filter function for Ethernet communication drops a diagnostics message, a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_04101]
When a CAN frame filter in a *DLC-first-layer* application function drops a CAN frame, a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_04301]

When an Ethernet frame filter in a *DLC-first-layer* application function drops an Ethernet frame, a security event logging function shall notify a SEv creation function of the work result.

3.1.1.4. Logging Requirements of Requirements Specification of 2nd Layer Message Filtering

[Requirement: IDSANR_04102]

When a CAN frame filter function in a *second-layer-protection* ECU/application drops a CAN frame, a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_04302]

When an Ethernet frame filter in a *second-layer-protection* ECU/application function drops an Ethernet frame, a security event logging function shall notify a SEv creation function of the work result.

3.1.1.5. Logging requirements of Requirements Specification of Message Authentication for FULL FV

[Requirement: IDSANR_05100]

When verification result of a CAN frame by a message authentication function is “Verification NG” (the reference [9]), a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_05200]

When verification result of an Ethernet frame by a message authentication function is “Verification NG” (the reference [9]), a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_05300]

While diag mask condition defined in the references [34] [35] is satisfied, the message authentication function shall not notify a SEv creation function of any event.

3.1.1.6. Logging requirements of TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications

[Requirement: IDSANR_11108]

This requirement shall be allocated to ECUs/VMs that the reference [7] (Requirements Specification of Message Filtering) is allocated to. When a diagnostic communication function succeeds in execution of a Sub-Function targeted to be recorded (Table 3-5) of SecurityAccess (SID

0x27) during a session other than programming one, a security event logging function shall notify a SEv creation function of the work result.

Table 3-5: Sub-Function to be recorded when SecurityAccess (SID 0x27) succeeds

Sub-Function	Targeted to be recorded at success
0x01	No
0x02	Yes
0x03	No
0x04	Yes
0x05	No
0x06	Yes
0x07-0x7D	No
0x08-0x7E	Yes
0x21	No
0x22	No
0x23-0x42	No
0x5F	No
0x60	No

[Requirement: IDSANR_06200]
This requirement shall be allocated to ECUs/VMs that the reference [7] (Requirements Specification of Message Filtering) is allocated to. When a diagnostic communication function fails in execution of a Sub-Function targeted to be recorded (Table 3-6) of SecurityAccess (SID 0x27), and the failure is targeted to be recorded (Table 3-7) during a session other than programming one, a security event logging function shall notify a SEv creation function of the work result.

Table 3-6: Sub-Function to be recorded when SecurityAccess (SID 0x27) fails

Sub-Function	Targeted to be recorded at failure
0x01	Yes
0x02	Yes
0x03	Yes
0x04	Yes
0x05	Yes
0x06	Yes
0x07-0x7D	Yes

Sub-Function	Targeted to be recorded at failure
0x08-0x7E	Yes
0x21	Yes
0x22	Yes
0x23-0x42	Yes
0x5F	Yes
0x60	Yes

Table 3-7: NRC to be recorded during SecurityAccess (SID 0x27)

NRC	Targeted to be recorded
0x10	No
0x11	No
0x12	Yes
0x13	Yes
0x21	No
0x22	Yes
0x24	Yes
0x31	Yes
0x33	No
0x35	Yes
0x36	Yes
0x37	Yes
0x78	No
0x7E (*1)	Yes
0x7F	No

*1: see the reference [21] for NRC 0x7E.

[Requirement: IDSANR_11109]
This requirement shall be allocated to ECUs/VMs that the reference [7] (Requirements Specification of Message Filtering) is allocated to. When a diagnostic communication function succeeds in execution of a Sub-Function targeted to be recorded (Table 3-8) of Authentication (SID 0x29) during a session other than programming one, a security event logging function shall notify a SEv creation function of the work result.

Table 3-8: Sub-Function to be recorded when Authentication(SID 0x29) succeeds

Sub-Function	Targeted to be recorded at success
0x00	No
0x01	Yes
0x02	Yes
0x03	Yes
0x04	No
0x05	Yes
0x06	Yes
0x07	Yes
0x08	No
0x09 – 0x7F	No

[Requirement: IDSANR_06300]
This requirement shall be allocated to ECUs/VMs that the reference [7] (Requirements Specification of Message Filtering) is allocated to. When a diagnostic communication function fails in execution of a Sub-Function targeted to be recorded (Table 3-9) of Authentication (SID 0x29), and the failure is targeted to be recorded (Table 3-10) during a session other than programming one, a security event logging function shall notify a SEv creation function of the work result.

Table 3-9: Sub-Function to be recorded when Authentication(SID 0x29) fails

Sub-Function	Targeted to be recorded at failure
0x00	Yes
0x01	Yes
0x02	Yes
0x03	Yes
0x04	Yes
0x05	Yes
0x06	Yes
0x07	Yes
0x08	Yes
0x09 – 0x7F	Yes

Table 3-10: NRC to be recorded during Authentication (SID 0x29)

NRC	Targeted to be recorded
0x10	No
0x11	No
0x12	Yes
0x13	Yes
0x21	No
0x22	Yes
0x24	Yes
0x33	No
0x78	No
0x7F	No

[Requirement: IDSANR_11115]
This requirement shall be allocated to ECUs/VMs whose VINs are stored and whose VINs are updated by diagnostic communication. When a diagnostic communication function succeeds in VIN update by WriteDataByIdentifier (SID 0x2E), a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_06400]
This requirement shall be allocated to ECUs/VMs whose VINs are stored and whose VINs are updated by diagnostic communication. When a diagnostic communication function fails in VIN update by WriteDataByIdentifier (SID 0x2E), and the failure is targeted to be recorded (Table 3-11), a security event logging function shall notify a SEv creation function of the work result.

Table 3-11: NRC to be recorded during VIN update (SID 0x2E, DID 0xF190)

NRC	Targeted to be recorded
0x10	No
0x11	No
0x13	Yes
0x21	No
0x22	Yes
0x31	Yes
0x33	No
0x72	Yes

NRC	Targeted to be recorded
0x78	No
0x7F	No

3.1.1.7. Logging requirements of OTA4.0 SoftWare Update MasterECU Requirements

[Requirement: IDANR_11111]
This requirement shall be allocated to ECUs/VMs that allocated the reference [36] (OTA4.0 SoftWare Update MasterECU Requirements). When an OTA reprogramming succeeds, a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDANR_07102]
This requirement shall be allocated to ECUs/VMs that allocated the reference [36] (OTA4.0 SoftWare Update MasterECU Requirements). When an OTA reprogramming fails, a security event logging function shall notify a SEv creation function of the work result.

3.1.1.8. Logging requirements of Requirements Specification of In-vehicle Key Management Slave

[Requirement: IDSANR_11112]
When a key update function succeeds in key single update or collective update, a security event logging function shall notify a SEv creation function of the work result.

[Requirement: IDSANR_09101]
When a key update function fails in a key-update procedure targeted to be recorded (Table 3-12), and the failure is to recorded (Table 3-13), a security event logging function shall notify a SEv creation function of the work result.

Table 3-12: Request messages for procedures to be recorded

Request messages for procedures				Targeted to be recorded
SID	Sub-Function	Parameter		
		Phase5	Phase6	
0x22	-	DID 0x010B	DID 0xA901	Yes
0x31	0x01/0x81	RID 0x1010	RID 0xD904	Yes
0x31	0x01/0x81	RID 0x100E	RID 0xD902	Yes
0x31	0x01/0x81	RID 0x100F	RID 0xD903	No

Table 3-13: NRC to be recorded

NRC	Targeted to be recorded
0x10	No
0x11	No
0x12	Yes
0x13	Yes
0x14	Yes
0x21	No
0x22	Yes
0x24	Yes
0x31	Yes
0x33	No
0x72	Yes
0x78	No
0x7F	No

3.1.1.9. Logging requirements of Requirements Specification of Key Management Master

[Requirement: IDSANR_09102]

When MAC key update information transmission is requested while MAC key update information transmission is prohibited, a security event logging function shall notify a SEv creation function of the work result.

3.1.2. Heartbeat notification function

3.1.2.1. Heartbeat notification

[Requirement: IDSANR_10002]

A heartbeat notification function shall notify a SEv creation function every [HeartbeatInterval].

3.1.3. SEv creation function

3.1.3.1. Anomaly notification SEv creation

[Requirement: IDSANR_10001]

When a SEv creation function is notified of an event by a detection function, it shall create an SEv (Table 3-14), and notify a QSEv creation function of the SEv. Event Definition ID, and Context Data shall be set in accordance with SEC-ePF-IDS-ANO-REQ-SPEC-a01-07-a_Annex1.xlsx. Context Data shall be set with big endian.

Table 3-14: Event notification SEv

Field Name	Length	Description
Security Event ID	16bit	This field shall be set to an identifier which identifies a pair of Event Definition ID and Sensor Instance ID which a QSEv creation function sets to a QSEv. - Event Definition ID shall be in accordance with an event detected. - Sensor Instance ID shall be fixed to 0. [Note] This field is implemented by an IdsMInternalEventId type parameter.
Context Data Size*	8 or 32 bit	This field shall be set to a byte length of Context Data. One of them shall be chosen for each Event Definition ID in software design phase up to size of Context Data
Context Data*	Variable length	This field shall be set to a sequence of bytes about an event detected, and shall be set depending on a requirement ID of a detection function that has notified an event. Diagnostic timestamp of occurrence of event shall be also set.

*The Heartbeat SEv and the SEV sent to the intrusion detection master by CAN communication do not have Context Data.

3.1.4. QSEv creation function

3.1.4.1. SEv qualification

[Requirement: IDSANR_10004]

A QSEv creation function shall qualify notified SEvs to a QSEv for each Security Event ID, in accordance with the reference [18], with parameters specified in [IDSANR_14010].

3.1.5. QSEv transmission function

3.1.5.1. QSEv transmission

[Requirement: IDSANR_10005]

If an intrusion detection master (the reference [17]) exists on any ECU, this requirement shall be allocated. When a QSEv creation function creates a QSEv, a QSEv transmission function shall create a frame defined below for each protocol used for the transmission from the own ECU to the intrusion detection master, and send it to the intrusion detection master.

- **When an ECU sends the frame with CAN communication or CAN FD communication:**
  The frame which contains data Label defined by QSEV_DATA_[ECU node name(*1)] in the reference [32]. In addition, the data defined in Figure 3-1 shall be set to the QSEV_DATA_[ECU node name].
- **When an ECU sends the frame with Ethernet communication:**
  The frame which defined by Table 3-15. In addition, the data defined in Figure 3-1 shall be set to IDS Message in Table 3-15.

Protocol Version	Protocol Header	IdsM Instance ID	Sensor Instance ID	Event Definition ID	Count	Reserved	Context Data (*2)
msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb

Figure 3-1: Data Structure

Table 3-15: Frame format (case of Ethernet)

Layer	Protocol	Description	Note
L2	Ethernet	The values of each field shall follow the reference [33].In addition, the MAC address of CEN2 which have the intrusion detection master shall be set to Destination MAC address.	-
L3	IPv4	The values of each field shall follow the reference [33]. In addition, the IP address of CEN2 which have the intrusion detection master shall be set to Destination IP address.	-

L4	TCP	The values of each field shall follow the reference [33] However, the follow values shall be set to Destination Port Number and Source Port Number. - Destination Port Number: 50004 (0xC354) - Source Port Number: 50004 (0xC354)	-
L5	IDS	The values of each field shall store and compose the follow data by big-endian method - Message ID (4Byte): ALL 0 - Length (4Byte): sum of data length of Message ID, Length, IDS Message - IDS Message (Variable): the data defined by Figure 3-1	For the details of the IDS protocol, see the reference [2].

*1: [ECU node name] shall be replaced by a node name of an own ECU that this document is allocated to. If Data Label is not defined in the reference [32], please contact us.
*2: Allocated to ECUs/VMs on CAN-FD or Ethernet network but **NOT** allocated to ECU/VMs on CAN network.

[Requirement: IDSANR_10010]
If a QSEv transmission function transmits QSEvs to an intrusion detection master, this requirement shall be allocated. If QSEv transmission by the QSEv transmission function wakes up network or prevents network from sleeping, the QSEv transmission function shall not transmit QSEvs.
<Note>
This requirement has been defined to avoid running out of battery due to transmitting QSEv.

3.1.6. QSEv storing function

3.1.6.1. QSEv storing

[Requirement: IDSANR_10006]
If any intrusion detection master does not exist on any ECU, this requirement shall be allocated. A QSEv storing function shall store the latest QSEvs created by a QSEv creation function, except QSEvs created by aggregating heartbeat notification SEvs, into non-volatile memory for each Event Definition ID where the number of QSEvs to be stored is [NumberOfQSEvs]. However, it may not store QSEvs at unexpected reset (e.g., power source instantaneous interruption, low voltage). In addition, QSEv storing function shall be designed considering the limit of number of writes to non-volatile memory.

<Note>

If an intrusion detection master exists on an ECU, it is optional to store QSEvs.
Buffering QSEvs in RAM during IG-ON, and then writing the QSEvs into non-volatile memory at IG-OFF can be an example of the implementation of storing QSEvs in non-volatile memory considering the maximum number of writes to non-volatile memory.

[Requirement: IDSANR_10009]

UserDefMemoryDTC and DID for QSEvs storing shall be in accordance with Table 3-16, Table 3-17, and Table 3-18.

UserDefMemoryDTC and DID are defined in accordance with the following policy.

・UserDefMemoryDTC: Defined for each Event Definition ID

・DID：Defined for whole QSEv, and common among all Event Definition IDs

Table 3-16: UserDefMemoryDTC Related Information

UserDefMemoryDTC	FTB	Event Definition ID corresponding to UserDefMemoryDTC	Memory Selection
U2B00	0x00	0x8501	0x14
U2B01	0x00	0x8502	0x14
U2B02	0x00	0xC503	0x14
U2B03	0x00	0x8503	0x14
U2B04	0x00	0xC504	0x14
U2B05	0x00	0x8504	0x14
U2B06	0x00	0xC505	0x14
U2B05	0x00	0x8505	0x14
U2B08	0x00	0xC506	0x14
U2B09	0x00	0x8506	0x14
U2B0A	0x00	0x8530	0x14
U2B0B	0x00	0x8550	0x14
U2B0C	0x00	0x8570	0x14
U2B0D	0x00	0x8590	0x14
U2B0E	0x00	0x8591	0x14
U2B0F	0x00	0x85A0	0x14
U2B10	0x00	0x85A1	0x14
U2B11	0x00	0x85A2	0x14
U2B12	0x00	0x85A3	0x14
U2B13	0x00	0xC5A4	0x14
U2B14	0x00	0x85A4	0x14
U2B15	0x00	0xC5A5	0x14

U2B16	0x00	0x85A5	0x14
U2B17	0x00	0xC5A6	0x14
U2B18	0x00	0x85A6	0x14
U2B19	0x00	0xC5D0	0x14
U2B1A	0x00	0x85D0	0x14
U2B1B	0x00	0x85E0	0x14

Table 3-17: DID for QSEv storing

DID	Data	Length [Bit]
0xA910	Protocol Version	4
	Protocol Header	4
	IdsM Instance ID	10
	Sensor Instance ID	6
	Event Definition ID	16
	Count	16
	Reserved	8
	Context Data (*1)	Variable Length

*1: Allocated to ECUs/VMs on CAN-FD or Ethernet network but **NOT** allocated to ECU/VMs on CAN network.

Table 3-18: Example of QSEv storage data(Store 5 QSEvs with Event Definition ID 0x8501)

UserDefMemoryDTC	FTB	UserDefDTC SnapshotRecordNumber	Description
U2B00	0x00	0x01	Oldest QSEv of the last [NumberOfQSEv] QSEvs (DID: 0xA910)
		0x02	Second oldest QSEv of the last [NumberOfQSEv] QSEvs (DID: 0xA910)
		0x03	Third oldest QSEv of the last [NumberOfQSEv] QSEvs (DID: 0xA910)
		0x04	Fourth oldest QSEv of the last [NumberOfQSEv] QSEvs (DID: 0xA910)
		0x05	Newest QSEv of the last [NumberOfQSEv] QSEvs (DID: 0xA910)

3.1.6.2. QSEv read

[Requirement: IDSANR_10007]

If QSEvs are stored in non-volatile memory, this requirement shall be allocated. QSEvs stored in non-volatile memory shall be able to be read from off-board client and on-board client by diagnostic communication with SID 0x19 (Sub Function 0x17/0x18). However, if the QSEvs are loaded on volatile memory, these QSEvs shall be read.

For the details of the diagnostics communication, see the reference [10].

3.1.6.3. QSEv deletion

[Requirement: IDSANR_10008]

If QSEvs are stored in non-volatile memory, this requirement shall be allocated. QSEvs stored in non-volatile memory shall be able to be deleted from off-board client by diagnostic communication with SID 0x14 (QSEv output MemorySelection 0x14).

For the details of the diagnostics communication, see the reference [10].

3.2. Quality requirements

None.

3.3. Constraints

We define constraints in this section.

[Requirement: IDSANR_13000]
If this system is on an ECU that is subject to legal regulations, and QSEvs are stored in non-volatile memory, this requirement shall be allocated. A QSEv storing function must meet the regulations.

3.4. Parameters

We define parameters in this section.

[Requirement: IDSANR_14000]
All parameters defined in this section shall be able to be changed under conditions defined in each requirement.

[Requirement: IDSANR _14010]
QSEvs shall be created and stored with parameters in Table 3-19 and the meta-information of the parameters shall be in accordance with Table 3-20 and Table 3-21.

Table 3-19: Parameters for QSEv creation and storing

Name	Event Definition ID	Sensor Instance ID	Value (*1)
IdsMEventAggregationTimeInterval	0x8501	0x0	0.3
	0x8502	0x0	0.3
	0xC503	0x0	0.3
	0x8503	0x0	0.3
	0xC504	0x0	0.3
	0x8504	0x0	0.3
	0xC505	0x0	0.3
	0x8505	0x0	0.3

	0xC506	0x0	0.3
	0x8506	0x0	0.3
	0x8530	0x0	0.3
	0x8550	0x0	0.3
	0x8570	0x0	0.3
	0x8590	0x0	0.3
	0x8591	0x0	0.3
	0x85A0	0x0	0.3
	0x85A1	0x0	0.3
	0x85A2	0x0	0.3
	0x85A3	0x0	0.3
	0xC5A4	0x0	0.3
	0x85A4	0x0	0.3
	0xC5A5	0x0	0.3
	0x85A5	0x0	0.3
	0xC5A6	0x0	0.3
	0x85A6	0x0	0.3
	0xC5C0	0x0	0.3
	0x85C0	0x0	0.3
	0xC5D0	0x0	0.3
	0x85D0	0x0	0.3
	0x85E0	0x0	0.3
	0xF500	0x0	0.3
IdsMContextDataSourceSelector	0x8501	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8502	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC503	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8503	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC504	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8504	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC505	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8505	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC506	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8506	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8530	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8550	0x0	IDSM_FILTERS_CTX_USE_FIRST

	0x8570	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8590	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8591	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A1	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A2	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A3	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC5A4	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A4	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC5A5	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A5	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC5A6	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85A6	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC5C0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85C0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xC5D0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85D0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x85E0	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0xF500	0x0	IDSM_FILTERS_CTX_USE_FIRST
NumberOfQSEvs	0x8501	0x0	5
	0x8502	0x0	5
	0xC503	0x0	5
	0x8503	0x0	5
	0xC504	0x0	5
	0x8504	0x0	5
	0xC505	0x0	5
	0x8505	0x0	5
	0xC506	0x0	5
	0x8506	0x0	5
	0x8530	0x0	5
	0x8550	0x0	5
	0x8570	0x0	5
	0x8590	0x0	5
	0x8591	0x0	5
	0x85A0	0x0	5

	0x85A1	0x0	5
	0x85A2	0x0	5
	0x85A3	0x0	5
	0xC5A4	0x0	5
	0x85A4	0x0	5
	0xC5A5	0x0	5
	0x85A5	0x0	5
	0xC5A6	0x0	5
	0x85A6	0x0	5
	0xC5C0	0x0	5
	0x85C0	0x0	5
	0xC5D0	0x0	5
	0x85D0	0x0	5
	0x85E0	0x0	5
	0xF500	0x0	5

Table 3-20: Meta information of parameters for QSEv creation

Name	Unit	Type	Lower limit	Upper limit
IdsMEventAggregationTimeInterval (*2)	sec	EcucFloatParamDef	0.05	10.00
IdsMContextDataSourceSelector	-	EcucEnumerationParamDef	IDSM_FILTERS_CTX_USE_FIRST	IDSM_FILTERS_CTX_USE_LAST

*1: That value of IdsMEventAggregationTimeInterval is hyphen means no aggregation.

*2: If it is not available to set the value specified in the value column, the biggest value among available values smaller than the value specified shall be adopted.

Table 3-21: Meta information of parameters for QSEv storing

Name	Description	Unit	Lower limit	Upper limit
NumberOfQSEvs	The number of QSEvs to be stored	-	0	10

[Requirement: IDSANR _14030]

Parameters for other than QSEv creation or storing shall be in accordance with Table 3-22 and the meta-information of the parameters shall be in accordance with Table 3-23.

Table 3-22: Parameters for other than QSEv creation or storing

Name	Description	Value
HeartbeatInterval	Heartbeat SEvs notification interval	1.0

Table 3-23: Meta information of parameters for other than QSEv creation or storing

Name	Unit	Lower limit	Upper limit
HeartbeatInterval	sec	0.0	10.0