▽R_1

目次

変更履歴

Version	Date	Changes	Target	Resp.
1.01	2022/6/30	New release		TMC Kurashige
1.02	2022/7/29	・4.1.3.1 RSA4096bitからRSA3072bitへ変更. ・5.7. TMNA要求：追記 [DC24-4594] ・5.5.1 図の修正 [DC24-5016] ・5.1.2. トヨタ管理サーバへの接続：追記 ・5.2. セキュアブート：修正 [DC24-7088] ・図5-3 サブマイコンリプロに関する記載を追加 ・5.2.1. 検証のタイミングと検証範囲：Linux起動前のセキュアブートの反映を明記[DC24-6476] ・5.6.1. 侵入検知システムの基本構成：HALでの検知対象を明記[DC24-6940]		TMC Sakurada
1.03	2022/9/30	・5.7 TMNA要求：誤記修正と”Cybersecurity Specification_v1.3”を”24MM Cybersecurity Specification_v1.5”に修正 [AGLSD-2662] ・Appendix F：” 24MM Cybersecurity Specification_v1.3”を” Cybersecurity Specification_v1.5”に修正 [AGLSD-2662] ・5.6.2.1 SELinuxポリシー違反のハンドリングについて：SELinuxポリシー違反はHAL側ではなくサービス側でハンドリングすることを記載 [AGLSD-2510] ・5.5.1. HSM Identifier：識別子を10桁から12桁に変更		TMC Kitamura
1.04	2022/11/11	・4.1.2.1. ディレクトリ暗号化などを使用する際の注意点を追加[AGLSD-2844] ・4.1.3. 標準アルゴリズムのHUが第三者サーバに接続する場合のアルゴリズム詳細に他の暗号アルゴリズムを排除しない旨の記載を追加[SEC24-1644]		

		・4.1.3.1. トヨタサーバ向けCipher SuitesのIDの誤記を修正[SEC24-1644]		
1.05	2023/3/16	5.8 ログ暗号化の章を追加[350-1][DC24-13983] 5.6.3.CFI要件について[352-1][DC24-13924]、[AGLSD-4431]、 [AGLSD-4430]		TMC Kurashige
1.0.6	2023/6/26	4.1.3. 標準アルゴリズムの参照番号が間違っている(4.2.2.1 ではなく4.1.3.1)。[AGLSD-6576] 5.1.1. 共通の対策の参照番号が間違っている(3.1.4ではなく4.1.3)。[AGLSD-6576] 5.3. ソフトウェアアップデートの図5-3を削除。「同等の内容によりセキュリティを担保できるのであれば、OTAマスタで実現してもよい」記載を追加。[AGLSD-6578]		TMC Kitamura
1.0.6	2023/7/11	5.6.2. Runtime Integrity に要件として、「RIシステムは ソフトウェアが改ざん等により危殆化したこと検知できること」を追加し、「侵入検知が出力するログファイルを改ざんされることなく、検知マスタへ提供できること」を削除。また、RIの要件番号を追加し、誤記を修正[AGLSD-6782] 5.6.4. OTAマスタ侵入検知ロギング要件を追加[AGLSD-6819]		TMC Kitamura

1. 目的

本書は、24CY情報セキュリティ要求仕様書の詳細を記載するものである。

2. 適用範囲

本書の適用範囲は、24CY情報セキュリティ要求仕様書と同様のものとする

3. 関連文書と用語集

本書に関連する文書は、24CY情報セキュリティ要求仕様書を基本とする。特に、詳細化において、関連する文書を下記に記載する。

表 3-1 関連文書一覧

ID	文書名	説明	発行者
ADC01	–	–	–

本書は、46F発行の『DC02』の要求を受け、その要求をシステムに適用する方法および結果について規定する。DC02に記載のない要求については、本書独自に規定する。

注記：

- 本書および本書から参照する関連書において記載される、「Post21CY」は「24CY」と、読み替えること。

次に、用語は、24CY情報セキュリティ要求仕様書に記載のものを基本とする。下記に、本書で特に記載すべき用語を記載する。

表 3-2 用語集

名称	説明
–	–
–	–
–	–

▽R_1

4. 要求の詳細

4.1. ▽R上位要求

46Fが各ECU向けに発行する要求仕様書のうち、マルチメディアに適用すべきものについては、24CY情報セキュリティ要求仕様書に記載している。
ただし、24CY情報セキュリティ要求仕様書にて要求される項目に対して、以下のような要求項目の詳細を記載する。理由も合わせて以下に示す。

4.1.1. 標準リプログラミングセキュリティ要求仕様書の詳細

『標準リプログラミングセキュリティ要求仕様書』に関する要求の詳細については、下記のとおりとする。

- 書き込みプログラムの暗号化
  リプログラミングを実施する際に新たに書き込むプログラムのことを、「書き込みプログラム」と呼ぶ。書き込みプログラムは以下の方式で暗号化したのち、ECUまで伝送または搬送すること。またリプログラミング実行時、ECUにて復号を行うこと。
  ［暗号アルゴリズム］　AES128
  ［鍵長］　128bit
  ［ブロック長］　128bit
  ［モード］　CBC

- 書き込みプログラムの署名
  書き込みプログラムに付与する署名については、以下の方式で生成すること。
  ［署名アルゴリズム］　ECDSA　（FIPS PUB 186-4 Curve P-256）
  ［鍵長］　256bit
  ［ハッシュ関数］　SHA-256
  より暗号強度の高いアルゴリズムを採用する目的で、24CY MMではECDSAを用いる。

4.1.2. 暗号鍵

H/Uで利用する暗号鍵の種類と、鍵の保管方法について次のように規定する。詳細はAppendix Dに定義する。

- 信頼の基点となる暗号鍵、およびトヨタサーバとの通信に最低限必要な暗号鍵と証明書は、耐タンパ性の保証されるセキュリティチップ内に保管する。
- 第三者サーバ用ルートCA証明書については、セキュアブートやアクセス制御により改ざんを防止する。
- 上記以外の暗号鍵と証明書については、セキュリティチップ内に保管することが望ましいが、記憶領域の制約上困難な場合には、セキュリティチップ外に保管してもよい。このとき、以下の点に留意する。
  - セキュリティチップ外に保管する場合は、セキュリティチップ内に保管される鍵で暗号化して保管する。

4.1.2.1. ディレクトリ暗号化などを使用する際の注意点

ディレクトリ暗号化技術などを使用する際は、以下2点を満足すること。

・暗号強度が、上記の暗号アルゴリズム以上であること（AES-128、AES-256など）。

・暗号化／復号用の鍵（または鍵のシード）を耐タンパ性のない不揮発ストレージに保存する場合は、耐タンパメモリ上の鍵で暗号化しておくこと。

4.1.3. 標準アルゴリズム

24CYのHUが利用する暗号アルゴリズム、署名検証アルゴリズム、ハッシュ関数を以下に示す。これ以外のアルゴリズムを利用する場合には、事前に本書の担当者に確認し許可を得ること。

技術分類	ユースケース例	対策技術	アルゴリズム詳細
サーバ認証	HUがトヨタサーバに接続。	TLS 1.2 TLS 1.3	4.1.3.1章参照
	HUが第三者サーバに接続。		Mandatory Cipher Suites A) TLS_RSA_WITH_AES_128_CBC_SHA B) TLS_AES_256_GCM_SHA384 C) TLS_AES_128_GCM_SHA256 D) TLS_AES_128_CCM_SHA256 なお上記の指定は、他のCipher Suitesの実装を排除するものではない。
クライアント認証	HUがトヨタサーバに接続。		ECDSA [256]
データ完全性検証	A) リプロデータ B) セキュアブート C) その他署名	デジタル署名	A) ECDSA-256 B) ECDSA-256 ※マイコン特有の形式を用いる場合は、本書の担当者と協議後、別途取り決める。 C) ECDSA-256、RSA-3072、RSA-4096
	ユーザプロファイル	メッセージ認証	HMAC [SHA-256]

4.1.3.1. トヨタサーバ向けCipher Suites

トヨタサーバ向けのTLSに必須となる、Cipher Suitesを以下に示す。

ID	Key Exchange	Auth	Encryption			MAC	
			Cipher	Len	Mode	Hash	Len
{0xc0, 0x23}	ECDHE	ECDSA	AES	128	CBC	SHA	256
{0xc0, 0x2b}	ECDHE	ECDSA	AES	128	GCM	SHA	256
{0xc0, 0x27}	ECDHE	RSA	AES	128	CBC	SHA	256

{0xc0, 0x2f}	ECDHE	RSA	AES	128	GCM	SHA	256
{0x13, 0x02}	-	-	AES	256	GCM	SHA	384
{0x13, 0x01}	-	-	AES	128	GCM	SHA	256
{0x13, 0x04}	-	-	AES	128	CCM	SHA	256

なお上記の指定は、他のCipher Suitesの実装を排除するものではない。

サーバ認証アルゴリズムについては、以下に詳細を指定する。

- ECDSA：secp256r1
- RSA：3072bit (key length)

4.2. その他の要求

4.2.1. コーディングルール

コーディングルールについては、『46F要求仕様書』で指示されるものの他に、以下の対応を行うこと。

表 4-1 コーディングルール一覧

ルール	発行元	補足
MISRA C++(2008)	MISRA	–
MISRA Compliance:2016	MISRA	–
SEI CERT C++ Coding Standard ver 134	Software Engineering Institute	–
AUTOSAR C++14	AUTOSAR	AUTOSAR C++14 Release17-10の一部

また、コーディングルールの運用については、「MISRA Compliance:2016」に従うこと。

4.2.2. 車両サイバーセキュリティECU開発プロセス

ISO21434、及びUN-R155に準拠すること（サプライチェーン含）。このプロセスにおけるトヨタとTier-1サプライヤの役割分担については、Appendix E 車両サイバーセキュリティECU開発プロセス CIAD に定めるフォーマットに則り、トヨタとサプライヤの間で別途取り決める。

5. セキュリティ機能

本章では、セキュリティ要件の実現方法について規定する。

5.1. サーバ接続セキュリティ

サーバ接続に関するセキュリティ対策は、接続先サーバがトヨタの管理するサーバか否かで異なる。以下に両者で共通の対策と、個別の対策を示す。

5.1.1. 共通の対策

- TLS Version 1.2 （RFC5246）またはTLS Version 1.3（RFC8446、RFC8448）に準拠したサーバ認証を行うこと。
- 認証に利用する鍵および証明書の保管場所については、Appendix Dに従うこと。
- TLSハンドシェイク時に、HUから送信するCipher Suitesは、4.1.3章に従うこと。

5.1.2. トヨタ管理サーバへの接続

- トヨタが発行するRootCA証明書によるサーバ認証を行うこと。
- サーバが、TLSハンドシェイク内でクライアント証明書による認証を要求してきた場合：
  - TLS version 1.2、TLS Version 1.3に準拠したクライアント認証を行うこと。
  - トヨタが準備するRootCA鍵による署名が付与されたクライアント証明書を用いて、クライアント認証を行うこと。

・ OCSPレスポンダによる証明書の失効確認に対応すること。以下の仕様に準拠すること。
  - Support for OCSP per RFC 6960
  - Support for OCSP stapling per RFC 6066
  - Support for OCSP stapling TLS1.3 per RFC 8446

● CRLに対応する場合は、車載器-センタ間通信標準仕様書1.2版 図 7-2 CRL/OCSP失効確認基本フローを基準とすること。

5.1.2.1 RootCA鍵ペアの失効を想定したサーバ認証フロー

HUで保持する証明書および鍵は危殆化に備えて更新可能であるが、更新の前提としてのサーバ接続を確保する必要がある。RootCA秘密鍵の漏洩等による失効に備えて、最低限のサーバ接続を確保するために、サーバ認証は以下のフローで行う。

・ HUは、サーバ認証の際に、Root CA証明書またはRoot CAの公開鍵を、サーバ証明書のIssuerによって選択すること。

5.1.3. トヨタ管理外サーバ（第三者サーバ）への接続

・ OCSPによるサーバ証明書の失効確認を行うこと。左記以外の方式を採用する場合、あらかじめトヨタ自動車に連絡して許可を得ること。

・

5.2. セキュアブート

5.2.1. 検証のタイミングと検証範囲

セキュアブートは原則、システム起動前に行うこと。ただし、起動時の各性能要件（各仕様書による）を満了するために、システム起動前にすべての検証が終えられない場合は、以下の考え方に則り、「起動前に検証すべきもの」と「起動後に　dm-verityで検証できるもの」の分別をつけて動作すること。

(1) 起動前に検証すべきもの
  1 ブートローダ
  2 カーネル
    ※基本的にはQualcomm様のBSPでセキュアブート対象になっているものが対象

(2) dm-verityで検証できるもの
  3 セキュアブートのバックグラウンド検証用のプログラム
  4 HSM機能利用時に実行するライブラリおよびこれに準ずるソフトウェア（HSM独自の検証の仕組みがある場合は、この限りではない）
  5 リプログラム機能

上記以外

また、以下の範囲については、検証対象外とする。

・ HUリリース後、市場で変化するデータ（設定値や受信データ等。リプロによる変化を除く。）

但し、上記のプログラムやデータの真正性検証が別途定められている場合には、これに従う。

5.2.2. 検証失敗時

セキュアブートの検証に失敗した場合は、以下の動作を行う。

- システム起動前の検証または　dm-verityの検証に関わらず、失敗時にはシステムリセットを行う。
- 検証失敗が一定回数連続発生した場合は、「システム起動失敗」と表示すること。但し、検証失敗が表示能力の起動より前の場合は、この限りではない。
- 検証失敗が連続発生する場合は、延々とシステムリセットを繰り返すことを回避すること。
- 起動電源がOFFされた場合は、検証失敗のカウントを０に戻すこと。

5.2.3. 署名生成

ブート処理において、Linux起動前までの検証については、Tier1鍵にて実施する。Linux起動後については、トヨタ鍵にて検証を行う。

5.2.4. バックグラウンド検証の性能要件　※dm-verityを使う場合は対象外

上位要件書「セキュアブート要求仕様書」の「SBTREQ_00007」に、『バックグラウンドでの完全性検証は可能な限り速やかに行うこと』とある。24CYも21CYと同様に『1分以内に使用している全ソフトウェア領域の完全性検証を完了。』を性能目標とすること。実現が困難な場合は、本仕様書担当に申し入れること。

5.3. ソフトウェアアップデート

要求については、標準リプログラミングセキュリティ要求仕様書、評価については、標準リプログラミングセキュリティ評価仕様書を基準とし、同等の内容によりセキュリティを担保できるのであれば、OTAマスタで実現してもよい。

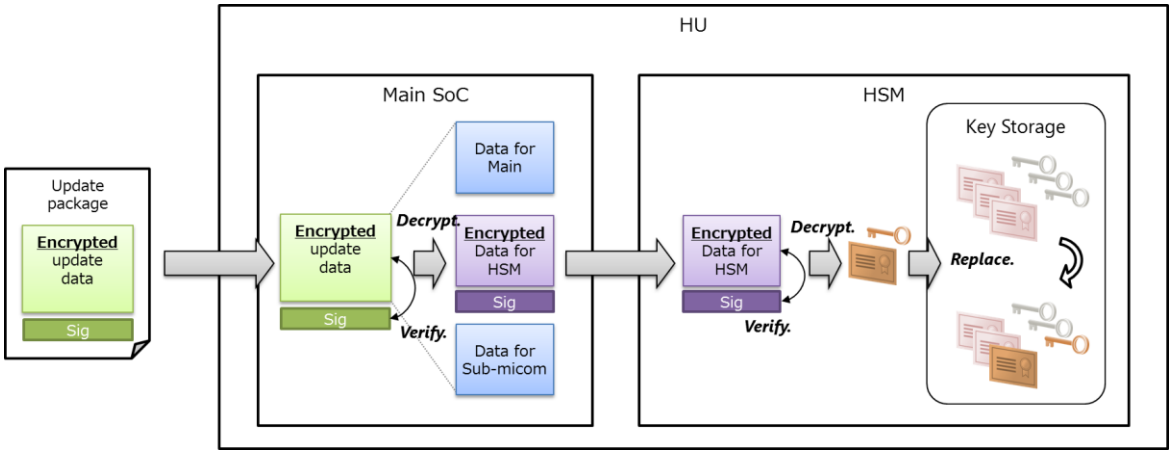
5.4. セキュリティパラメータの更新

HSMの管理下にあるセキュリティパラメータ（鍵・証明書）の更新は5.3 ソフトウェアアップデートの仕組みに則るが、それ以外のプログラム・データの更新よりも、セキュリティ性を向上させる必要がある。以下にその違いを示す。

- アップデートデータの復号および署名検証に用いる鍵は、HSM管理下にあり、かつセキュリティパラメータの更新専用とする。
- アップデートデータの復号および署名検証をHSM内で行ったあと、復号データをHSM外に出してはならない。

図5-4に、HSM管理下のセキュリティパラメータを更新する際の、Main SoCとHSMの役割を示す。本図では便宜的にHSMをMain SoCと分けて表現しているが、HSMがSoC内蔵の場合にもその役割を変えずに適用する。

図5-4 セキュリティパラメータの更新手順



5.5. Hardware Security Module

24CYでのHSMとしては、下記の要件を満たすこと。

- Advanced Crypto Engine (ACE) for Execution of All Cryptography Commands
- Fast Crypto Engine for SHA-256, HMAC and AES-CMAC Algorithms
- Sign/Verify Support: – ECDSA – P224, P256, P384 and 256-bit Brainpool elliptic curves – ECDSA – SECP256K1 (Bitcoin/Blockchain) curve – RSA 2048-bit signature generation and verification – RSA 3072-bit signature verification only
- ECDH/ECDHE/ECBD Key Agreement Support – Elliptic-Curve Diffie-Hellman (ECDH) Support for P224, P256, P384 and 256-bit Brainpool – Elliptic-Curve Burmeiseter-Desmedt (ECBD) Support for P224 Curve • Internal Symmetric and Asymmetric Key Generation and Derivation: – P224, P256, P384 and 256-Bit Brainpool – 2048-bit RSA keys – AES 16-byte keys
- AES and RSA Encryption / Decryption Support – AES ECB/GCM Encryption/Decryption Supported directly – RSA 1024-bit and 2048-bit Keys Encryption/Decryption Support
- NIST SP800-90 A/B/C Random Number Generator (RNG) • Multiple I/O Options for Security Commands Include: – 1 MHz standard I2C interface – 16 MHz SPI interface
- Package Options: – 8-lead SOIC – 24-pad 4 x 4 mm VQFN
- Voltage Supply Range: 2.7V to 5.5V
- Automotive Temperature Range: -40°C to +125°C Ambient Operating Range

参考として、下記のHSMがあげられる。

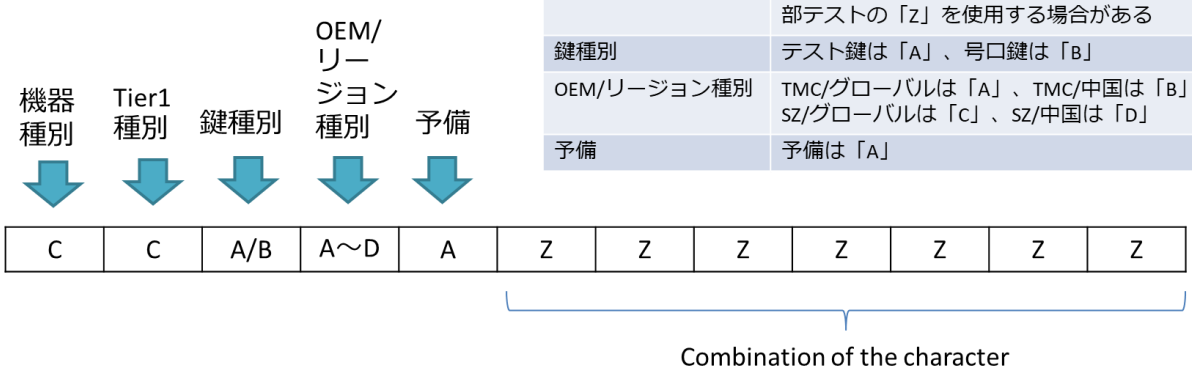
HSMベンダ	製品型情報
Microchip Technology Inc.	TA100 https://www.microchip.com/en-us/product/ta100

5.5.1. HSM Identifier

HSMは、以下の特徴を備える。

- ユニークなIDを持つ。
- IDは、12　桁の文字列であり、幅は、「A」から「Z」である。
- 上位5桁は下記参照。下位7桁はシリアル番号。

項目	内容
機器種別	HUは「C」
Tier1種別	Microchipは「C」 ※開発中はサプライヤテストの「Y」、TMC内部テストの「Z」を使用する場合がある
鍵種別	テスト鍵は「A」、号口鍵は「B」
OEM/リージョン種別	TMC/グローバルは「A」、TMC/中国は「B」、SZ/グローバルは「C」、SZ/中国は「D」
予備	予備は「A」



5.5.2. HSMで扱う鍵および証明書のフォーマット

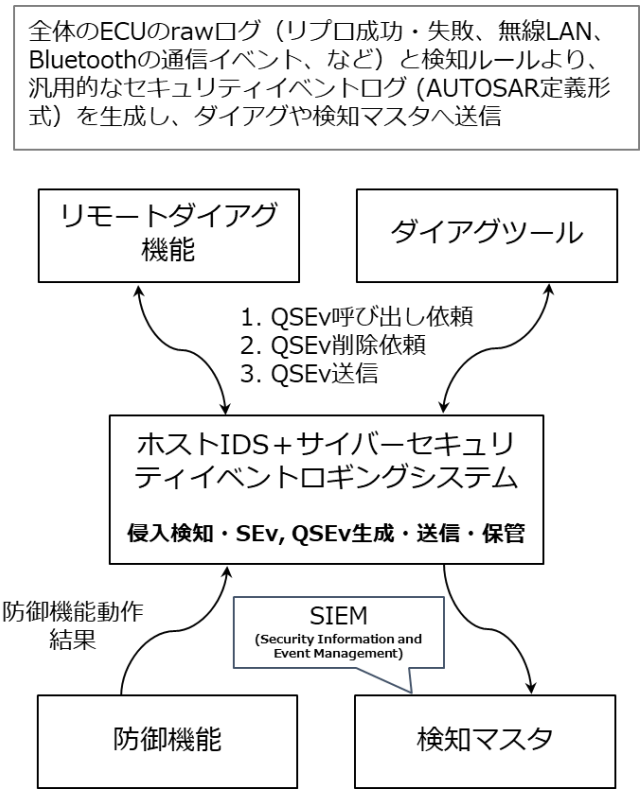
Appendix Dを参照のこと。

5.6. 侵入検知

5.6.1. 侵入検知システムの基本構成

24CYでは、下記のシステム概要を基準として、図5-6-1のとおり、侵入検知システムを採用する。

図5-6-1 セキュリティパラメータの更新手順



防御機能の内、HALで対応が必要な対象は下記である。

- セキュアブート：Linux起動前については対象外とし、Linux起動後についてはdm-verityで改ざんを検知したプログラムファイルの識別子をQSEvに登録
- セキュアストレージ：格納データの完全性チェックに失敗した場合のエラーコード(TMNAから提示)に基づきQSEvに登録

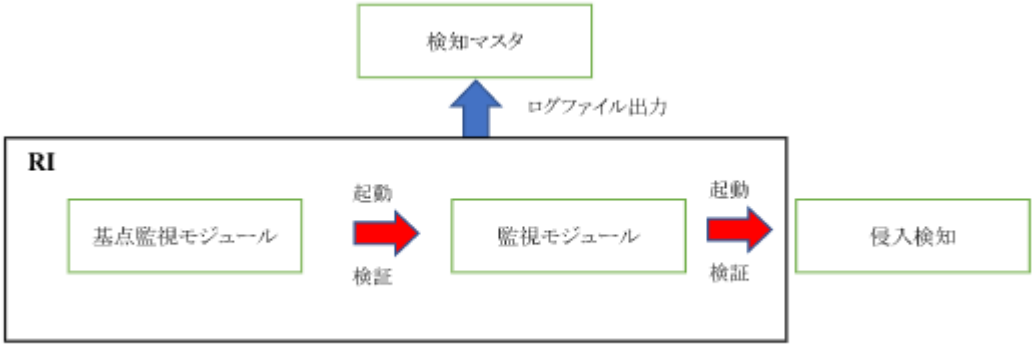
5.6.2. SELinuxポリシー違反のハンドリングについて

SELinuxのポリシー違反については、HAL側ではなくサービス側でハンドリングする。

5.6.2.1. Runtime Integrity

本要求の、要求仕様IDは、24MM.SEC.RIとする。侵入検知（上位要件にて定義）の機能が正常動作していることを保証するためにRuntime Integrity（RI）を用いる。その概要を、図5-6-2に示す。RIはSecure Bootで起動した機器が動作を終了するまでの間に、ソフトウェアが改ざん等により危殆化したこと検知する技術である。RIを用いて侵入検知機能の動作を保証するシステム（以下、RIシステム）の要件を以下に示す。

図5-6-2 RIの概要



要求ID	仕様内容
24MM.SEC.REQ.RI.1	RIシステムはソフトウェアが改ざん等により危殆化したこと検知できること。
24MM.SEC.REQ.RI.2	RIシステムはセキュアブートにて検証され、完全性が保証されること。
24MM.SEC.REQ.RI.3	RIシステムは基点監視モジュールと１つ以上の監視モジュールによって構成され、侵入検知機能に至るまで、定期的な検証を行うことで信頼の連鎖を構築すること。
24MM.SEC.REQ.RI.4	基点監視モジュール、監視モジュール、侵入検知機能に対して監視モジュールは論理的、もしくは物理的に異なる領域に配置することで十分な機能分離を行う、同様に監視モジュールに対して基点監視モジュールも十分な機能分離を行うこと。例えば、基点監視モジュールはARM Trust Zone等のハードウェアレベルで保護されたセキュアワールド上に、監視モジュールはカーネル領域上に配置する。侵入検知機能の配置領域は侵入検知の仕様に従う。

5.6.3. CFI要件について

SEC-ePF-IDS-HIE-REQ-SPEC(侵入検知エントリーポイント向けHost IDS要求仕様書)、要求事項「IDSHER_01601」はバージョン「a00-04-c」を適用する。

5.6.4. OTAマスタ侵入検知ロギング要件

OTA処理中に、車両内でサイバー攻撃と疑われる事象が発生した場合、または正常に処理を終了した場合に、OTAマスタは当該事象に合わせたログを記録し、侵入検知システムへログデータを送信する。送信するログデータ・送信のトリガーとなるイベント・データフォーマットは下記の要件に従うものとする。

- 「OTA4.0 ソフト更新マスタECU 要求仕様書」の「3.6.15バージョン 整合チェック」終了時に正常終了ログを記録すること。
- サイバー攻撃が疑われる事象が発生した場合、侵入検知ログを記録すること。この事象は、「OTA4.0ソフト更新シス テム要求仕様書」の「7.5.1.例外事象」にて定義される。
- 正常終了ログ/侵入検知ログで記録が求められるデータ項目は「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」に従うこと。但し、OTA固有部分は、「OTA4.0ソフト更新マスタ I/F仕様書」に従うこと。
- 正常終了ログ/侵入検知ログは「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」に従い、侵入検知システムに大きな遅滞なく送信されること。

5.7. TMNA要求

以下の項目を除いて、TMNAの要求に従うこと。ただし、除外した項目について、実現することは推奨する。
矛盾する項目については、24CY_情報セキュリティ要求仕様書を優先すること。
TMNAが記載した要求は、Appendix F.　24MM Cybersecurity Specification_v1.6を参照すること。

No	参照元	カテゴリ	要求事項
5	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.PGM.5
7	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.PGM.7
11	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.PGM.11
14	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.PGM.14
28	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.TST.1
31	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.TST.4
34	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.TST.7
36	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.TST.9
37	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.TST.10
42	24MM Cybersecurity Specification	Project	24MM.SEC.PRJ.FCT.1
51	24MM Cybersecurity Specification	Hardware	24MM.SEC.HW.PER.1
52	24MM Cybersecurity Specification	Hardware	24MM.SEC.HW.PER.2
53	24MM Cybersecurity Specification	Hardware	24MM.SEC.HW.PER.3
54	24MM Cybersecurity Specification	Hardware	24MM.SEC.HW.MEM.1
57	24MM Cybersecurity Specification	Hardware	24MM.SEC.HW.MEM.4
64	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.CRYP.7
65	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.KEY.1
67	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.KEY.3

No	参照元	カテゴリ	要求事項
71	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.KEY.7
75	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.SB.1
101	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.SB.27
103	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.SB.29
104	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.SB.30
106	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.SB.32
109	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.UPD.3
110	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.UPD.4
112	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.UPD.6
115	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.UPD.9
117	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.UPD.11
118	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.UPD.12
119	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.UPD.13
126	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.DBG.GEN.1
132	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.DBG.PROD.4
135	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.DBG.PROD.7
137	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.DBG.PROD.9
138	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.DBG.PROD.10
139	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.DBG.PROD.11
140	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.DBG.PROD.12
146	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.DBG.PROD.18

No	参照元	カテゴリ	要求事項
148	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.DBG.PROD.20
160	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.GEN.4
189	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.4
190	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.5
191	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.6
192	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.7
193	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.8
194	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.9
195	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.10
196	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.11
197	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.12
198	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.13
199	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.14
200	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.15
201	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.16
202	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.17
203	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.18
204	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.19
205	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.20
206	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.21
207	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.22

No	参照元	カテゴリ	要求事項
208	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.23
209	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.24
210	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.25
211	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.26
212	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.27
213	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.28
214	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.OS.KRN.29
219	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.STG.5
221	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.STG.7
226	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.STG.12
230	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.FDE.4
231	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.FDE.5
234	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.FDE.8
251	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.LOG.ACC.2
260	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.LOG.TR.3
263	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.LOG.TR.6
264	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.LOG.TR.7
265	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.LOG.TR.8
266	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.LOG.TR.9
267	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.LOG.TR.10
272	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.TLS.1

No	参照元	カテゴリ	要求事項
273	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.TLS.2
275	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.TLS.4
278	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.TLS.7
279	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.TLS.8
280	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.TLS.9
285	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.DNS.1
286	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.DNS.2
287	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.DNS.3
290	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.MQTT.1
292	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.MQTT.3
293	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.REV.1
307	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.REV.15
308	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.FWL.1
318	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.WIFI.3
319	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.COM.WIFI.4
334	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.PER.4
337	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.PER.7
339	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.AT.1
341	24MM Cybersecurity Specification	Platform	24MM.SEC.PLAT.AT.3
343	24MM Cybersecurity Specification	Application	24MM.SEC.APP.KEY.1
345	24MM Cybersecurity Specification	Application	24MM.SEC.APP.UPD.1

No	参照元	カテゴリ	要求事項
346	24MM Cybersecurity Specification	Application	24MM.SEC.APP.UPD.2
347	24MM Cybersecurity Specification	Application	24MM.SEC.APP.UPD.3
348	24MM Cybersecurity Specification	Application	24MM.SEC.APP.UPD.4
349	24MM Cybersecurity Specification	Application	24MM.SEC.APP.UPD.5
350	24MM Cybersecurity Specification	Application	24MM.SEC.APP.DBG.1
351	24MM Cybersecurity Specification	Application	24MM.SEC.APP.DBG.2
352	24MM Cybersecurity Specification	Application	24MM.SEC.APP.STG.1
358	24MM Cybersecurity Specification	Application	24MM.SEC.APP.LOG.6
360	24MM Cybersecurity Specification	Application	24MM.SEC.APP.LOG.8
367	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.EXT.1
370	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.EXT.4
371	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.EXT.5
372	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.EXT.6
373	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.EXT.7
374	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.EXT.8
375	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.EXT.9
376	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.EXT.10
378	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.EXT.12
384	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.INT.1
385	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.INT.2
386	24MM Cybersecurity Specification	Application	24MM.SEC.APP.COM.INT.3

No	参照元	カテゴリ	要求事項
388	24MM Cybersecurity Specification	Application	24MM.SEC.APP.HRD.2
389	24MM Cybersecurity Specification	Application	24MM.SEC.APP.HRD.3
390	24MM Cybersecurity Specification	Application	24MM.SEC.APP.HRD.4
391	24MM Cybersecurity Specification	Application	24MM.SEC.APP.HRD.5
392	24MM Cybersecurity Specification	Application	24MM.SEC.APP.HRD.6
393	24MM Cybersecurity Specification	Application	24MM.SEC.APP.HRD.7
396	24MM Cybersecurity Specification	Application	24MM.SEC.APP.SBX.3
397	24MM Cybersecurity Specification	Application	24MM.SEC.APP.SBX.4
400	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.1
401	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.2
402	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.3
403	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.4
404	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.5
405	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.6
406	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.7
407	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.8
408	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.9
409	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.10
410	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.SB.11
411	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.TEE.1
412	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.TEE.2

No	参照元	カテゴリ	要求事項
413	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.TEE.3
414	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.TEE.4
415	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.TEE.5
419	24MM Cybersecurity Specification	Qualcomm	24MM.SEC.QC.FDE.4

5.8. ログ暗号化

図5-8-1の番号「3」、番号「5」、番号「6」のプライバシー情報はログ内に保存をしない。番号「3」、番号「5」、番号「6」のプライバシー情報をログ内に保存をしないため、ログは暗号化の対象外とする。

図5-8-1 プライバシー情報 対象データの層別

Appendix1 対象データの層別

番号	カテゴリー	具体例	重要度	プライバシー要件	車両外の暗号化	車両内の暗号化	厳重暗号化
1	バイオメトリックデータ	指紋、録音・音声、顔認証データ、虹彩、静脈	S	基本適用（個別事情により都度例外、適切な実務を検討）	○	○	○
2	カメラ画像・動画	車内カメラ画像・動画、車外カメラ画像・動画			○	○	
3	法令上、配慮が必要とされる情報	健康情報、遺伝子データ、犯罪等に関わるデータ（スピード違反、車線走行帯の違反などを明らかにするようなデータ）、通信情報（通信記録、メールの内容など）、その他（人種、民族、宗教的又は哲学的な信条、政治的見解、労働組合への加入、性生活又は性的指向）			○	○	○
4	位置情報	位置情報			○	○	推奨
5	公的機関が発行した ID などの情報	免許証番号、住民 ID、パスポート番号			○	○	○
6	経済的損失をもたらす情報・財産情報	クレジットカード番号、銀行口座			○	○	○
7	ユーザー・お客様に関する情報（含. 属性情報）	氏名、電話番号、住所、メールアドレス、年齢、性別、職業	A		○		
8	特定の個人・ユーザーに紐づくためのキーとなる情報	車両 ID、ユーザーID、車載 ID、サービス用 ID			○		
9	車両の挙動や制御に関わるデータ（ユーザーの運転特性や好みが分かるデータ）	舵角、アクセル・ブレーキ操作量、車速、エアコン・ヘッドライト・ワイパー・エアコン設定値・ドアの開閉などの操作信号、シート位置、運転・操作履歴(位置、顔画像、音声除く)	B		○		
10	車両の挙動や制御に関わるデータ（上記以外）	エンジン回転数、エンジン水温、ブレーキ圧、ECT ギア位置、ECT の制御学習値			○		
11	クルマの故障診断に用いるデータ	ダイアグコード、フリーズフレームデータ、RoB などの故障診断用情報			○		
12	それ自体で個人の行動や特性等を明らかにするまたは意味を理解することが極めて困難な情報（ただし、VIN による個人への紐づけは可能）	「クルマの各機能やサービスを実現するための ECU・マイコン内部の各種変数・レジスタ値」、「ある車両データを意味のある情報、値として構成するための、ソフトウェアやシステムの挙動に影響を与えるような、人間が意味を理解、感知できない細かいパラメーターデータ（プログラミング言語、演算子など）」			○		

（※）暗号化にて使用する技術レベルについては、セキュリティ部署、設計部署等で協議の上、適切と判断した手段を選択するものとする。

Appendix C. 暗号鍵

別紙『190_AppendixC+D_鍵フォーマット資料』を参照のこと。

Appendix D. 鍵フォーマット

別紙『190_AppendixC+D_鍵フォーマット資料』を参照のこと。

Appendix E. 車両サイバーセキュリティECU開発プロセス CIA

車両サイバーセキュリティECU開発プロセスにおける、トヨタとTier1サプライヤの責務を、本CIAD (Cybersecurity Interface Agreement) を用いて明確化する。別紙参照のこと。

Appendix G. 24MM Cybersecurity Specification_v1.6

TMNAより示された24MM Cybersecurity Specification_v1.6　に記載した要件の一部を、本書に統合する。本要件は、全仕向けに適用する。24MM Cybersecurity Specification_v1.6　.pdfを参照のこと。