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	V-24MM.SEC.QC.FDE.5を追加 [DC24-6389]		TMC Kitamura
1.03	2023/07/07	V-24MM.SEC.HW.PER.4を追加[SEC24-5337] V-24MM.SEC.PLAT.CRT.4を追加[SEC24-5337] V-24MM.SEC.APP.COM.WIFI.1を追加[SEC24-5337]		TMC Kawasaki
1.03	2023/7/12	V-24MM.SEC.RI5は要件がなくなったため削除[AGLSD-6782] V-24MM.SEC.RI1の試験内容を追記[SEC24-5432] V-24MM.SEC.RI1の試験手順を修正[SEC24-5432] V-24MM.SEC.RI1の合否判定を修正[SEC24-5432] V-24MM.SEC.RI2の試験内容を追記[SEC24-5432] V-24MM.SEC.RI2の試験手順を修正[SEC24-5432] V-24MM.SEC.RI3の試験内容を追記[SEC24-5432] V-24MM.SEC.RI3の試験手順を修正[SEC24-5432] V-24MM.SEC.RI3の合否判定を修正[SEC24-5432]		TMC Kawasaki

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
–	–
–	–
–	–

4. 評価要求の詳細

4.1. ECU独自のサイバーセキュリティ評価要求

ECU独自サイバーセキュリティ要求仕様に対する評価要求を下記に示す。
サイバーセキュリティ要求仕様のは上位要求の詳細化にあたるため、上記要求の評価仕様に従うことを基準とする。本書では、特に、詳細化にあたり、不明な部分について、記載する。

表4.1-1にRIに対する評価仕様を記載する。

表4.1-1 RIに対する評価仕様

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定	備考
V-24MM.SEC.RI1	RIシステムはSecure Bootで起動した機器が動作を終了するまでの間に、機器内の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ことを確認する。本試験ではRIシステムの機能を利用するアプリケーションに対する改ざんを実施する。	-	１．MMを起動する。 ２．侵入検知システムを改ざんする。	-	２で監視モジュールより危殆化のログが出力されること。	実機評価のログは保存しておくこと。
V-24MM.SEC.RI2	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を確認する。本試験ではRIシステムを構成するコンポーネントである基点監視モジュールに対する改ざんを実施する。	-	1. 信頼の連鎖に含まれる基点監視モジュールを改ざんする。 2. MMを起動する。	-	2でMMの起動がエラー終了すること。	実機評価のログは保存しておくこと。
V-24MM.SEC.RI3	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を確認する。本試験ではRIシステムを構成するコンポーネントである監視モジュールに対する改ざんを実施する。	-	１．MMを起動する。 ２．RIシステムの信頼の連鎖に含まれる監視モジュールを改ざんする。 ３．RIシステムの定期検証時間分待機する。	-	２で基点監視モジュールより危殆化のログが出力されること。	実機評価のログは保存しておくこと。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定	備考
V-24MM.SEC.RI4	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を確認する。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。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・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。	-

表4.1-2にTMNA要求に対する評価仕様を記載する。

表4.1-2 TMNA要求に対する評価仕様

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PRJ.PGM.1	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性 分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.PGM.2	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性 分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.PGM.3	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性 分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.PGM.4	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性 分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.PGM.6	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性 分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PRJ.PGM.8	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.PGM.9	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.PGM.10	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.PGM.12	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.PGM.13	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.1	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.2	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.3	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.4	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.5	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.6	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PRJ.SW.7	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.8	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.9	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.10	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.11	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.12	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.SW.13	ISO21434に沿った開発プロセスにそって、脅威分析、脆弱性　分析していること、評価していることを確認する	-	ISO21434沿って、情報資産、および、脅威を特定し、脅威分析、脆弱性分析、評価を実施し報告する	提出した報告書を確認する	ドキュメントが一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.TST.2	デバイスの脆弱性テストを可能にするために必要なすべてのワイヤーハーネス、テストハードウェア、およびドキュメントを提供する。	-	テストに必要なハードやドキュメントが提出されていることを確認する。	提出されたハードやドキュメントの一覧を確認する	提出物が一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.TST.3	ECUのテストを実施するために、外部デバイスを模擬またはシミュレートするために必要なすべてのハードウェアおよびソフトウェアツールを提供する。	-	テストに必要なハードやソフトウェアが提出されていることを確認する。	提出されたハードやソフトウェアの一覧を確認する	提出物が一貫しているか、網羅しているかを確認する。
V-24MM.SEC.PRJ.TST.5	開発およびテスト中にサプライヤーから独立してアップデートをインストールできるように、必要な文書とツールを提供するものを確認する。	-	開発に要な文書とツールを提供できていることを確認する	テスト工程が独立して実施できていることを確認する	テスト工程が問題なく実施できたことをテスト結果を見て確認する

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PRJ.TST.6	完全な更新プログラム パッケージでは、ユニットの現在のバージョンに関係なく、ユニットを最新バージョンにアップグレードできるものを提供できていることを確認する。	-	テスト工程において、プログラムを更新できることを確認する。	テストにて、プログラムのアップデートができることを確認する	プログラムのバージョンが想定されたバージョンになっていることを確認する
V-24MM.SEC.PRJ.TST.8	トヨタに配信されるすべてのアップデートには、前回のアップデート以降にセキュリティ機能に加えられた変更を文書化し、記述した変更ログを含める。	-	アップデート時の変更管理を実施することで確認する。	アップデート時に差分の変更を記載した文書を確認する運用フローが作成されていることを確認	運用フローに、アップデート時の変更に管理について、文書化することが明示されていることを確認する。
V-24MM.SEC.PRJ.TST.11	有線・無線問わず、すべてのI/Fに対してファジングテストによって問題が修正されていることを確認する	-	ファジングテストの内容を合意し、テスト結果を入手し、問題点が修正されているエビデンスを確認する。	-	計画したテストがすべて完了していること、問題点がすべて修正されていること
V-24MM.SEC.PRJ.TST.12	コンフィグを確認する	-	コンフィグを確認する	-	コンフィグが正しいことを確認した結果を報告書として受領する
V-24MM.SEC.PRJ.TST.13	コンフィグを確認する	-	コンフィグを確認する	-	コンフィグが正しいことを確認した結果を報告書として受領する
V-24MM.SEC.PRJ.TST.14	コンフィグを確認する	-	コンフィグを確認する	-	コンフィグが正いことを確認した結果を報告書として受領する
V-24MM.SEC.PRJ.FCT.2	各社のセキュリティ対策を確認する	-	工場への入退出制限について実現されていることを確認する	-	セキュリティ対策について、人の認証が実施される運用となっているかを確認する
V-24MM.SEC.PRJ.FCT.3	各社のセキュリティ対策を確認する	-	工場への入退出制限について実現されていることを確認する	-	ツールの利用時に、人の認証が実施される運用となっているかを確認する
V-24MM.SEC.PRJ.FCT.4	各社のセキュリティ対策を確認する	-	ツールがスタンドアローンで運用されているかを確認する	-	ツールがスタンドアローンで運用されているかを確認する
V-24MM.SEC.HW.SB.1	ECU上のすべてのプロセッサがセキュアブートをサポートしていることを確認する。サポートしていないものがあった場合、トヨタのレビューを依頼する。	-	各プロセッサに対してセキュアブートのサポート状況を確認する。	-	すべてのプロセッサがセキュアブートをサポートしていることを確認した場合、合格とする。またサポートしていないプロセッサは全てトヨタのレビューが済んでいること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.HW.SB.2	全てのプロセッサがハードウェアベースのアンチロールバック機能をサポートしていることを確認する。サポートしていないものがあった場合、トヨタのレビューを依頼する。	-	各プロセッサに対してハードウェアベースのアンチロールバック機能をサポートしていることを確認する。	-	全てのプロセッサがハードウェアベースのアンチロールバック機能をサポートしていることを確認できた場合、合格とする。またサポートしていないプロセッサは全てトヨタのレビューが済んでいること。
V-24MM.SEC.HW.COM.WIFI.1	Wi-FiチップセットがWPA2とWPA3の双方をサポートしていることを確認する。	-	全てのWi-Fiチップセットが WPA2とWPA3の双方をサポートしていることを確認する。	-	全てのWi-FiチップセットがWPA2とWPA3の双方をサポートしていることを確認できた場合、合格とする。
V-24MM.SEC.HW.COM.WIFI.2	Wi-Fiチップセットが、メインSoCに対して新しいMACアドレスを設定することを許可していることを確認する。	-	メインSoCからWi-Fiチップセットに対して新しいMACアドレスが設定可能なことを確認する。	-	メインSoCからWi-Fiチップセットに対して新しいMACアドレスが設定可能なことを確認できた場合、合格とする。
V-24MM.SEC.HW.COM.BLT.1	BluetoothチップセットがBluetooth 4.2またはそれ以上のバージョンをサポートしていることを確認する。	-	Bluetoothチップセットのプロトコルバージョンを確認する。	-	BluetoothチップセットがBluetooth 4.2またはそれ以上のバージョンをサポートしていた場合、合格とする。
V-24MM.SEC.HW.PER.4	HDCPを無効化することで、上位アプリケーションが動作しないこと、もしくは上位アプリケーションの機能が制限されていることを確認する。	・HDCPを利用するアプリケーションを洗い出していること ・HDCPを利用するアプリケーションが正常に稼働していること	・HDCPを利用するアプリケーションの動作を確認する ・HDCPを無効化する ・該当するアプリケーションの動作を確認する。	-	該当するアプリケーションが稼働しない、もしくはアプリケーションの機能が制限されていること。
V-24MM.SEC.HW.MEM.2	SoC上のフラッシュストレージがRPMBをサポートしていることを確認する。	-	SoC上のフラッシュストレージがRPMBをサポートしていることを確認する。	-	SoC上のフラッシュストレージがRPMBをサポートしていることを確認できた場合、合格とする。
V-24MM.SEC.HW.MEM.3	すべてのRAMモジュールがはんだ付けされており、ソケットや簡単に除去できる方法で取り付けられていないことを確認する。	-	すべてのRAMモジュールを確認する。	-	すべてのRAMモジュールがはんだ付けされており、ソケットや簡単に除去できる方法で取り付けられていないことを確認できた場合、合格とする。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.CRYP.1	デジタル署名は、FIPS PUB 186-4を満たし、NIST SP 800-57 Part 1 Rev.5に従ってセキュリティ強度128以上のキー長を使用していることを確認する。その他のすべての署名アルゴリズムは、トヨタによって承認されていることを確認する。 例:RSA-4096;ECDSA-256;ECDSA-384;ED 25519。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・デジタル署名はFIPS PUB 186-4を満たしていること ・セキュリティ強度128以上のキー長を使用していること。 ・その他のすべての署名アルゴリズムは、トヨタによって承認されていること。
V-24MM.SEC.PLAT.CRYP.2	NIST SP 800-131A Rev. 2によって使用が承認されたメッセージ認証コード(MAC)のみを使用していることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・NIST SP 800-131A Rev. 2によって使用が承認されたメッセージ認証コード(MAC)のみを使用していること。
V-24MM.SEC.PLAT.CRYP.3	ハッシュ関数は、NIST SP 800-57 Part1 Rev 5に従ってセキュリティ強度128以上であることを確認する。使用される他のすべてのハッシュアルゴリズムは、トヨタによって承認されていることを確認する。 例:SHA-256、SHA-384。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・ハッシュ関数は、NIST SP 800-57 Part1 Rev 5に従っていること。 ・セキュリティ強度128以上であること。 ・使用される他のすべてのハッシュアルゴリズムは、トヨタによって承認されていること。
V-24MM.SEC.PLAT.CRYP.4	AES-128、AES-192およびAES-256は、使用される唯一の対称暗号化アルゴリズムであることを確認する。AESの実装では、NIST SP 800-38シリーズで承認されたモードを使用していることを確認する。ECBモードはトヨタの承認がない限り使用していないことを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・AES-128、AES-192、AES-256であること。 ・NIST SP 800-38シリーズで承認されたモードを使用すること。 ・ECBモードはトヨタの承認がない限り使用しないこと。
V-24MM.SEC.PLAT.CRYP.5	AESモードの動作に初期化ベクト(IV)が必要な場合、IVは、TRNGまたはTRNGによってシードされたPRNGを使用してランダムに生成されることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・AESモードの動作に初期化ベクト(IV)が必要な場合は、IVを無作為に生成すること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.KEY.2	事前共有および保存された暗号秘密(例:プライベート非対称キー、対称キー)は、Trusted Execution Environment (TEE)またはSecure Element (例:HSM、セキュリティプロセッサ)によって保存および管理されていることを確認する。暗号秘密を使用するすべての暗号操作は、TEEまたはセキュアエレメント内で実行されていることを確認する。暗号の秘密は、Normal Worldのソフトウェアにアクセスできないことを確認する。ここで、暗号秘密を使用する暗号操作は、Normal Worldのソフトウェアによって開始され得る。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・事前共有および保存された暗号秘密は、TEEまたはSecure Elementによって保存および管理されること。 ・暗号秘密を使用するすべての暗号操作は、TEEまたはセキュアエレメント内で実行されること。 ・暗号の秘密は、Normal Worldのソフトウェアにアクセスできないこと。
V-24MM.SEC.PLAT.KEY.4	暗号秘密(非対称秘密鍵、対称鍵など)は、TEE又はセキュアエレメントに裏打ちされたメカニズムを用いて機密性が保護されていることを確認する。このメカニズムは、TEEまたはセキュアエレメント以外のいかなるソフトウェアによっても、または外部通信バスをプローブする攻撃者によっても、暗号エレメントが読み取られないことを保証することを保証するものである。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・暗号秘密は、TEE又はセキュアエレメントに裏打ちされたメカニズムを用いて機密性が保護されていること。
V-24MM.SEC.PLAT.KEY.5	暗号マテリアルは、TEEまたはセキュアエレメントに裏打ちされたメカニズムを用いて完全性が保護されることを確認する。このメカニズムは、暗号マテリアルが意図された更新プロセスの外で変更されないことを保証するものである。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・暗号マテリアルは、TEEまたはセキュアエレメントに裏打ちされたメカニズムを用いて完全性が保護されること。
V-24MM.SEC.PLAT.KEY.6	暗号マテリアルは、TEEまたはセキュアエレメントに裏打ちされたメカニズムを使用して、ロールバック攻撃から保護されることを確認する。	-	1. 以前のバージョンにアップデートしようとする。	-	1でアップデートがエラー終了すること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.KEY.8	暗号マテリアルの更新プロセスでは、一般的な更新に使用されるキーと同じキーではなく、キーの更新にのみ使用される特殊なキーを使用してデータを暗号化および認証することを確認する。	-	1. トヨタサーバから割り当てられたキーを使用して鍵のアップデートを実施する。	-	1で鍵のアップデートに成功すること。
V-24MM.SEC.PLAT.KEY.9	暗号マテリアルの更新プロセスは、TEEまたはセキュアエレメントを使用して実行することを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・暗号マテリアルの更新プロセスは、TEEまたはセキュアエレメントを使用して実行すること。
V-24MM.SEC.PLAT.KEY.10	暗号マテリアル更新処理の後に、古い暗号マテリアルへの参照が存在しないことを確認する。	-	1. 古い暗号キーを使ってアップデートを実施する。	-	1でアップデートがエラー終了すること。
V-24MM.SEC.PLAT.SB.2	セキュアブートが、サポートされる唯一のブートモードであることを確認する。セキュアブートプロセスのどの段階でも、セキュアブートをバイパスしたり無効にしたりする仕組みはないことを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・セキュアブートが、サポートされる唯一のブートモードであること。 ・セキュアブートプロセスのどの段階でも、セキュアブートをバイパスしたり無効にしたりする仕組みはないこと。
V-24MM.SEC.PLAT.SB.3	セキュアブートには、ブートアップを停止して、セキュアブートのバイパスを防止するように設計されていない汎用コマンドラインまたはその他のモードに入ることができる機能を含んでいないことを確認する。	-	1.ECUの起動時にICEなどのテスターを接続し、デバッグモードに移行しようとする。	-	1でデバッグモードに移行せず、ECUが起動すること。
V-24MM.SEC.PLAT.SB.4	電源投入時、SoCが、SoC内に埋め込まれた不変ROMから常に最初の命令を実行することを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・電源投入時、SoCが、SoC内に埋め込まれた不変ROMから常に最初の命令を実行すること。
V-24MM.SEC.PLAT.SB.5	SoC ROMの実行を変更するいかなる機能も、変更をインストールする前に認証を必要とすることを確認する。 例:ROMパッチメカニズム。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・SoC ROMの実行を変更するいかなる機能も、変更をインストールする前に認証を必要とすること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.SB.6	インストール後に、トヨタが承認したSoC ROMの実行に対する変更を無効にするメカニズムがないことを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・トヨタが承認したSoC ROM実行に対する変更は、インストール後は変更できず無効にすることができないこと。
V-24MM.SEC.PLAT.SB.7	SoC ROMに変更を加える前に、トヨタの承認を得ていることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・SoC ROMに変更を加える前に、トヨタの承認を得ていること。
V-24MM.SEC.PLAT.SB.8	セキュアブート処理を実行する場合、SoC ROMコードは、SoC内部の揮発性メモリ、または外部メモリの暗号化された完全性保護領域のみを使用することを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・セキュアブート処理を実行する場合、SoC ROMコードは、SoC内部の揮発性メモリ、または外部メモリの暗号化された完全性保護領域のみを使用すること。
V-24MM.SEC.PLAT.SB.9	SoC ROMコードは、セキュアブート処理に使用される揮発性メモリへのアクセスをセキュアプロセッシング環境内のコードのみに制限するように、セキュアプロセッシング環境内で動作することを確認する。 例:ARM TrustZone。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・SoC ROMコードは、セキュアブート処理に使用される揮発性メモリへのアクセスをセキュアプロセッシング環境内のコードのみに制限するように、セキュアプロセッシング環境内で動作すること。
V-24MM.SEC.PLAT.SB.10	SoC ROMコードは、処理/例外レベルセグメンテーションの最も特権的なレベルで動作を開始することを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・SoC ROMコードは、処理/例外レベルセグメンテーションの最も特権的なレベルで動作を開始すること。
V-24MM.SEC.PLAT.SB.11	後のステージのブートローダは、ブートを実行しているイメージ部分の最高の特権レベルより高い特権レベルでは動作しないことを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・後のステージのブートローダは、ブートを実行しているイメージ部分の最高の特権レベルより高い特権レベルでは動作しないこと。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.SB.12	マスクROMは、ハードウェア暗号化エンジンを使用して、すべての暗号化操作を実行することを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・マスクROMは、ハードウェア暗号化エンジンを使用して、すべての暗号化操作を実行すること。
V-24MM.SEC.PLAT.SB.13	ブートプロセスの各段階は、次のブートステージに実行を移す前に、次のブートステージの信頼性を検証することを確認する。これにはSoC ROMブートステージが含まれ、ロードされたすべてのソフトウェアイメージの信頼性を検証することを確認する。	-	1. 次のブートステージのイメージに対して正しくない署名を作成する。 2. 上記イメージと署名を組み込んでセキュアブートを実施する。	-	2でセキュアブートがエラー終了すること。
V-24MM.SEC.PLAT.SB.14	ROMコード後のブートステージでは、ROMコードを使用して信頼性チェックを実行することを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・ROMコード後のブートステージでは、ROMコードを使用して信頼性チェックを実行すること。
V-24MM.SEC.PLAT.SB.15	ソフトウェアイメージの信頼性は、ソフトウェアイメージを使用するSoC（「ターゲットSoC」）によって検証されることを確認する。 ソフトウェアイメージの信憑性を検証しないプロセッサは、サプライヤによって文書化され、トヨタによってレビューおよび承認されることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・ソフトウェアイメージの信頼性は、ソフトウェアイメージを使用するSoC(「ターゲットSoC」)によって検証されること。 ・ソフトウェアイメージの信憑性を検証しないプロセッサは、サプライヤによって文書化され、トヨタによってレビューおよび承認されること。
V-24MM.SEC.PLAT.SB.16	ソフトウェアイメージの信頼性は、次の2つの手順で検証していることを確認する。 • ソフトウェアイメージの長さと暗号化ハッシュを含むセキュアブート証明書のデジタル署名を検証する。 • ソフトウェアイメージのハッシュが、セキュアブート証明書に含まれるハッシュと一致することを検証する。	-	1. 正しくない証明書を組み込んでセキュアブートを実行する。 2. ソフトウェアイメージのハッシュと異なるハッシュを含む証明書を組み込んでセキュアブートを実行する。	-	1、2でセキュアブートがエラー終了すること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.SB.17	デジタル署名を検証するために使用される鍵は、信頼されたルート鍵で終わる公開鍵証明書チェーンの一部であることが検証されていることを確認する。	-	1. 証明書のチェーンに含まれない鍵で署名を作成する。 2. 上記鍵の証明書と上記署名を組み込んでセキュアブートを実施する。	-	2でセキュアブートがエラー終了すること。
V-24MM.SEC.PLAT.SB.18	セキュアブート署名の検証に使用される信頼されたルートキーは、SoCハードウェアに不変に保存されることを確認する。 注：信頼されたルートキーは完全なキーではなくハッシュとしてSoCハードウェアに不変に格納される場合がある。ハッシュは24MM.SEC.PLAT.CRYP.3に準拠している必要がある。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・セキュアブート署名の検証に使用される信頼されたルートキーは、SoCハードウェアに不変に保存されること。
V-24MM.SEC.PLAT.SB.19	すべてのセキュアブート証明書は、X.509v3形式を実装することを確認する。代替の証明書フォーマットは、サプライヤーによって文書化され、レビューと承認のためにトヨタと共有されることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・すべてのセキュアブート証明書は、X.509v3形式を実装すること。 ・代替の証明書フォーマットは、サプライヤーによって文書化され、レビューと承認のためにトヨタと共有されること。
V-24MM.SEC.PLAT.SB.20	HMACまたはCMACを使用して真正性を検証する場合、秘密鍵はSoCハードウェアに不変に保存されることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・HMACまたはCMACを使用して真正性を検証する場合、秘密鍵はSoCハードウェアに不変に保存されること。
V-24MM.SEC.PLAT.SB.21	HMAC又はCMACが真正性を確認するために使用される場合、秘密鍵は、いかなるソフトウェアもそれを読み取ることができないような方法で保存されていることを確認する。計算を実行する暗号化エンジンのみが秘密鍵にアクセスできることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・HMAC又はCMACが真正性を確認するために使用される場合、秘密鍵は、いかなるソフトウェアもそれを読み取ることができないような方法で保存されていること。 ・計算を実行する暗号化エンジンのみが秘密鍵にアクセスできること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.SB.22	Linuxオペレーティングシステムによってロードされるすべてのカーネルモジュールは、トヨタが発行した鍵で署名されていることを確認する。	-	1.署名されていないか署名が正しくないカーネルモジュールをロードする。	-	1でカーネルモジュールのロードに失敗すること。
V-24MM.SEC.PLAT.SB.23	セキュアブートに使用されるキーの失効は、不可逆的な方法で行うことを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・セキュアブートに使用されるキーの失効は、不可逆的な方法で行うこと。
V-24MM.SEC.PLAT.SB.24	セキュアブートプロセスは、指定されたセキュリティバージョンより古いソフトウェアイメージのロードを恒久的に防止するメカニズムをサポートすることを確認する。以下、この機構を「アンチロールバック機構」と称する。	-	1. 指定されたセキュリティバージョンより古いソフトウェアイメージを組み込む。 2. セキュアブートを実施する。	-	2でセキュアブートがエラー終了すること。
V-24MM.SEC.PLAT.SB.25	アンチロールバックメカニズムは、アップデートによるセキュリティバージョンの増加をサポートすることを確認する。	-	1. ソフトウェアをアップデートする。	-	1でセキュリティバージョンが増加していること。
V-24MM.SEC.PLAT.SB.26	すべてのソフトウェアイメージに対して、アンチロールバックメカニズムを有することを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・すべてのソフトウェアイメージに対して、アンチロールバックメカニズムを有すること。
V-24MM.SEC.PLAT.SB.28	セキュアブートプロセスは、ウォッチドッグまたはSoCのセキュアに読み込まれたサブプロセッサによって監視されることを確認する。ブートプロセスが読み込まれず、すべてのセキュアブートイメージの検証が予想される時間枠内に完了しない場合、ブートプロセスが中止されることを確認する。	-	1. セキュアブートプロセスが予想される時間枠内に完了しないようにして、セキュアブートを実施する。	-	以下の設計情報に基づき試験内容が確認できること。 ・セキュアブートプロセスは、ウォッチドッグまたはSoCのセキュアに読み込まれたサブプロセッサによって監視されること。 2でセキュアブートがエラー終了すること。
V-24MM.SEC.PLAT.SB.31	ECUが起動できない場合、ECUは、サプライヤーおよびトヨタの担当者がヘッドユニットを分析および復元できるリカバリモードに入ることを確認する。	-	1. 代替側もセキュアブートが失敗する状態にして、セキュアブートを実施する。 2. 上記を3回繰り返す。	-	2で下記挙動となること。 • リカバリモードに移行すること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.UPD.1	ECU装置は、トヨタのRoot-of-Trustキーにチェーンするキーを使用して、トヨタによって発行されたものとして認証されたアップデートのみを適用することを確認する。	-	1. トヨタのRoot-of-Trustキーにチェーンするキーを使用して、トヨタによって発行されたものとして認証されたアップデートを使ってリプロを実施する。	-	1でリプロが成功すること。
V-24MM.SEC.PLAT.UPD.2	ECU装置は、トヨタのRoot-of-Trustキーにチェーンするキーを使用して、トヨタによって発行されたものとして認証されていないアップデートパッケージのコンポーネントを実行しないことを確認する。	-	1. トヨタのRoot-of-Trustキーにチェーンするキーを使用して、トヨタによって発行されたものとして認証されていないアップデートを使ってリプロを実施する。	-	1でリプロがエラー終了すること。
V-24MM.SEC.PLAT.UPD.5	更新メカニズムは、更新パッケージのローカルおよびリモート配布をサポートすることを確認する。	-	1. OTAによるリプロを実施する。 2. ローカルからのリプロを実施する。	-	1、2でリプロが成功すること。
V-24MM.SEC.PLAT.UPD.7	ECUの各プロセッサは、イメージが外部プロセッサによって検証された場合でも、更新イメージを自ら検証することを確認する。 更新イメージ検証をサポートしないプロセッサは、サプライヤによって文書化され、トヨタによってレビューおよび承認されることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・ECUの各プロセッサは、イメージが外部プロセッサによって検証された場合でも、更新イメージを自ら検証すること。 ・更新イメージ検証をサポートしないプロセッサは、サプライヤによって文書化され、トヨタによってレビューおよび承認されること。
V-24MM.SEC.PLAT.UPD.8	セキュアな更新検証コードは、電力およびクロックグリッチ攻撃によるバイパスに耐性があるように構築されていることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・セキュアな更新検証コードは、電力およびクロックグリッチ攻撃によるバイパスに耐性があるように構築されていること。
V-24MM.SEC.PLAT.UPD.10	ECUは、インストール前にソフトウェアイメージのサイズを検証するメカニズムを備えることを確認する。指定されたサイズは、認証機構によって保護される。	-	1. OTAにおいて、指定されたサイズを超えた更新パッケージをECUに送信する。	-	1でリプロがエラー終了すること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.UPD.14	ECU内のプロセッサの更新データは、ターゲットプロセッサから外部不揮発性メモリに保存されるときに暗号化されることを確認する。	-	1. 外部不揮発性メモリに保存されている更新データを確認する。	-	1で更新データが暗号化されていること。
V-24MM.SEC.PLAT.UPD.15	プロセッサの更新データは、更新パッケージの整合性を検証するメカニズムで検証されることを確認する。このメカニズムの衝突率は低くする必要があります。	-	1. ソフトウェア更新パッケージを改ざんした上でリプロを実施する。	-	以下の設計情報に基づき試験内容が確認できること。 ・プロセッサの更新データは、更新パッケージの整合性を検証するメカニズムで検証されること。 1でリプロがエラー終了すること。
V-24MM.SEC.PLAT.UPD.16	ECUは、いかなる方法(バックドアなど)でも、セキュア更新手順をバイパス、無効化、または回避することができないことを確認する。例えば、秘密性、完全性、または真正性の暗号保証を無効にするメカニズムは許可されない。これには、トヨタの発行キーによって署名されていないイメージを受け入れるか、まったく署名されていないイメージを受け入れるメカニズムが含まれる。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・ECUは、いかなる方法(バックドアなど)でも、セキュア更新手順をバイパス、無効化、または回避することができないこと。
V-24MM.SEC.PLAT.UPD.17	ECUは、更新が失敗した場合、トヨタサーバに通知することを確認する。	-	1. リプロを失敗させる。	-	1でトヨタサーバにおいてリプロが失敗したログが記録されていること。
V-24MM.SEC.PLAT.UPD.18	更新が正常に適用された後、更新ファイルまたはソフトウェアイメージがデバイスに保持されないことを確認する。これには、周辺プロセッサのファームウェアイメージに対しても同じであることを確認する。 注：起動時に周辺プロセッサにロードする必要があるファームウェアは存続する可能性がある。 注：代替のブート側イメージは保持しても問題ない。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・更新が正常に適用された後、更新ファイルまたはソフトウェアイメージがデバイスに保持されないこと。 ・これには、周辺プロセッサのファームウェアイメージに対しても同じであること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.UPD.19	デバイスにアップデートを適用するソフトウェアアプリケーションは、アップデートと一緒に提供されることを確認する。ソフトウェアアップデートアプリケーションは、デバイス上で永続化していないことを確認する。 注：これには、周辺プロセッサ用のソフトウェア更新アプリケーションが含まれる。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・デバイスにアップデートを適用するソフトウェアアプリケーションは、アップデートと一緒に提供されること。 ・ソフトウェアアップデートアプリケーションは、デバイス上で永続化していないこと。
V-24MM.SEC.PLAT.DBG.DEV.1	号口暗号鍵またはその他の秘密は、デバッグ・ユニットにインストールしたり、デバッグ・ソフトウェアに組み込んだりしていないことを確認する。	-	1. デバッグユニットから号口サーバに接続する。	-	1で号口サーバに接続できないこと。
V-24MM.SEC.PLAT.DBG.DEV.2	デバッグユニットは、デバッグユニットであることを明確に示す認証情報のみを発行することを確認する。	-	1. デバッグユニットから号口サーバに接続する。	-	1で号口サーバに接続できないこと。
V-24MM.SEC.PLAT.DBG.PROD.1	すべてのデバッグおよび診断機能とサービスは、実稼働ユニットで削除または無効化することを確認する。例外は以下の通り。 •ディーラーまたはサービス技術者に必要なデバッグまたは診断サービス。 •分析のためにログを取得します。 •安全なデバッグメカニズム。	-	1. 開発中に使用されたデバッグポートに物理的にアクセスする。 2. USB JTAGなどのアクセスポートを介してデバッグ機能にアクセスする。	-	1、2でアクセスできないこと。
V-24MM.SEC.PLAT.DBG.PROD.2	ハードウェアに関連付けられた一意の識別子に基づいて、特定の実稼働デバイスにのみデバッグ機能を追加できるようにする、排他的な安全なデバッグメカニズムを実装していることを確認する。 注：サプライヤーは、実稼働デバイスに他のデバッグメカニズムを実装してはなりません。	-	1. 特定のデバイス向けに発行したクレデンシャルを該当するデバイスで使用する。 2. 特定のデバイス向けに発行したクレデンシャルを他のデバイスで使用する。	-	1でデバッグ機能を使用できること。 2でデバッグ機能を使用できないこと。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.DBG.PROD.3	セキュアデバッグメカニズムは、ハードウェアベースの暗号化認証メカニズム(Qualcommデバッグポリシーなど)を使用して、トヨタが発行した資格情報でセキュアデバッグが有効になっていることを確認することを確認する。	-	1. トヨタが発行したものでないクレデンシャルをデバイスで使用する。	-	1でデバッグ機能を使用できないこと。
V-24MM.SEC.PLAT.DBG.PROD.5	SoC構成では、24MM.SEC.PLAT.DBG.PROD.1の許可されたデバッグ機能に必要なハードウェアデバッグインターフェイスのみを有効にする必要があります。 JTAGを含む他のすべてのハードウェアデバッグインターフェイスは、SoC構成によって無効にされることを確認する。	-	1. P21.MM.SEC.PLAT.DBG.PROD.1で許可されていないデバッグ機能を使用しようとする。	-	1でデバッグ機能を使用できないこと。
V-24MM.SEC.PLAT.DBG.PROD.6	永続的に無効にされていないハードウェアデバッグインターフェイスは、24MM.SEC.PLAT.DBG.PROD.3のメカニズムによる検証後にのみ有効になることを確認する。 注：デバッグインターフェイスを使用する前の暗号化認証が不可能な場合は、デバッグインターフェイスを永続的に無効にすることを確認する。 メカニズムの例：許可されたデバッグ機能を指定し、その署名がSoCのマスクROMによって検証されるQualcommデバッグポリシー。	-	1. デバッグポートに接続し、トヨタバックエンド接続を使用して認証を実行してクレデンシャルを作成し、該当するデバッグ機能を使用する。 2. デバッグポートに接続し、トヨタバックエンド接続を使用して認証を実行せずに、該当するデバッグ機能を使用する。	-	1でデバッグ機能を使用できること。 2でデバッグ機能を使用できないこと。 以下の設計情報に基づき試験内容が確認できること。 ・デバッグインターフェイスを使用する前の暗号化認証が不可能な場合は、デバッグインターフェイスを永続的に無効にすることを確認する。
V-24MM.SEC.PLAT.DBG.PROD.8	セキュアデバッグ検証コードは、グリッチ攻撃によるバイパスに耐性があるように構築されていることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・セキュアデバッグ検証コードは、グリッチ攻撃によるバイパスに耐性があるように構築されていること。
V-24MM.SEC.PLAT.DBG.PROD.13	ECUは、エクスポートされたログファイルおよびデバッグ情報を暗号化して、特権ユーザーのみが情報にアクセスできることを確認する。	-	1. ログファイルおよびデバッグ情報をエクスポートする。 2. 特権ユーザーがログファイルおよびデバッグ情報にアクセスする。	-	1でログファイルおよびデバッグ情報が暗号化されていること。 2で特権ユーザのみが復号されたログファイルおよびデバッグ情報にアクセスできること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.DBG.PROD.14	すべてのデバッグおよび診断認証の試みは、4.11項ロギングに従ってログに記録されることを確認する。	-	1.エクスポートされたログファイルおよびデバッグ情報に特権ユーザーがアクセスする。	-	1で復号されたログファイルおよびデバッグ情報は、4.11項ロギングに従ってログに記録されること。
V-24MM.SEC.PLAT.DBG.PROD.15	ECUは、ダイアグ通信を介して機密情報またはソフトウェアの読み取りまたは書き込みを一切許可しないことを確認する。	-	1.トヨタバックエンド接続を使用して認証を実行した後、診断コンソールを使用して拡張セッションを要求する。 2. ダイアグ通信を介して機密情報またはソフトウェアの読み取り、書き込みを試みる。	-	1で読み取り、書き込みの試みが失敗すること。
V-24MM.SEC.PLAT.DBG.PROD.16	ECUは、診断通信による揮発性または不揮発性メモリの直接の読み取りまたは書き込みをサポートしないことを確認する。	-	1.診断コンソールを使用して読み取り、書き込みサービスを実行する。	-	1で読み取り、書き込みの試みが失敗すること。
V-24MM.SEC.PLAT.DBG.PROD.17	UDSサービスは、証明書を使用した認証についてのみSID 0x29をサポートすることを確認する。SID 0x27はサポートされないことを確認する。。	-	1. USDサービスで、SID 0x29に対する応答を監視する。 2. USDサービスで、SID 0x27に対する応答を監視する。	-	1で肯定応答が返され、システムが証明書ベースの認証をサポートしていること。 2で否定応答が返され、システムが証明書ベースの認証をサポートしていないこと。
V-24MM.SEC.PLAT.DBG.PROD.19	Diagnostics over IP (DoIP)の使用は、内部イーサネットネットワークに限定されていることを確認する。Wi-Fi、Bluetooth、その他の通信インターフェイスを介したDoIPサービスへのアクセスは許可されない。	-	1. 内部イーサネットインターフェイス以外のネットワークインターフェイスを介してDoIPサービスにアクセスする。	-	1でアクセスできないこと。
V-24MM.SEC.PLAT.DBG.PROD.21	セキュアデバッグメカニズムは、新しい署名付きLinuxカーネルイメージ、initramfs、デバイスツリーバイナリ、およびカーネルブートパラメータのロードと実行をサポートすることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・セキュアデバッグメカニズムは、新しい署名付きLinuxカーネルイメージ、initramfs、デバイスツリーバイナリ、およびカーネルブートパラメータのロードと実行をサポートすること。
V-24MM.SEC.PLAT.DBG.PROD.22	セキュアデバッグメカニズムは、新規または変更された起動構成ファイルの使用をサポートすることを確認する。 例：systemdユニットファイル、MACポリシー、ロギング構成、/etc内のファイルなど。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・セキュアデバッグメカニズムは、新規または変更された起動構成ファイルの使用をサポートすること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.DBG.PROD.23	セキュアデバッグイメージは暗号化することを確認する。	-	1. セキュアデバッグイメージを確認する。	-	1でセキュアデバッグイメージが暗号化されていること。
V-24MM.SEC.PLAT.TEE.1	TEEは、可能な限り、認証操作を実行し、機密情報を管理するために使用されることを確認する。実装されるべきTEEのいくつかの用途は以下の通りである。 •セキュアストレージ。 •セキュアブートサービス。 •セキュアデバッグサービス。 •セキュア更新サービス。 •デジタル権利管理（DRM）保護。 •セキュアペリフェラルのドライバー。 •相互TLSのクライアント秘密鍵を含む暗号化シークレットの管理。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・左記のセキュリティサービスの設計文書をトヨタに提出し、レビューを受けること。 ・トヨタ、すべてのセキュリティ・サービスが高い権限レベル(SEL 3、SEL 1、SEL 0)で実行されていること。
V-24MM.SEC.PLAT.TEE.2	TEEは、TEEサービスにアクセスするNormal Worldのアプリケーションのアイデンティティを検証する認証メカニズムを実装することを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・サプライヤーは、検証のために認証メカニズムの設計をトヨタに提供すること。 ・TrustZone(Secure World)に存在するセキュリティ機能にアクセスできるのは、Normal Worldから認証されたアプリケーションだけであること。
V-24MM.SEC.PLAT.TEE.3	TrustZoneアーキテクチャ拡張をサポートするすべてのArm Cortex®-Aマイクロプロセッサに対してTrustZoneを有効にしていることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・サプライヤは、TrustZoneアーキテクチャがシステムで有効になっていることを確認するための証拠を提供すること。
V-24MM.SEC.PLAT.TEE.4	TrustZoneは、オプションのTrustZoneアーキテクチャ拡張をサポートするすべてのSoC Arm Cortex®-Mマイクロプロセッサに対して有効にしていることを確認する。	-	-	-	以下の設計情報に基づき試験内容が確認できること。 ・サプライヤは、TrustZoneアーキテクチャがシステムで有効になっていることを確認するための証拠を提供すること。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.TEE.5	全ての電源状態で作動する全てのセキュリティクリティカルな機能がTEEを介して処理されることを確認	・全ての電源状態で作動するセキュリティクリティカルな機能が全て明確であること	-	-	事前条件で明確となっている全ての電源状態で作動する全てのセキュリティクリティカルな機能がTEEを介して処理されること
V-24MM.SEC.PLAT.OS.GEN.1	システム起動パラメータがセキュアブートの一部として完全に保護されることを確認	-	-	-	文書化されたセキュアブートのブートステージ構成を確認し、システム起動パラメータが含まれること
V-24MM.SEC.PLAT.OS.GEN.2	「/proc/sys」の下のシステムデフォルト設定が最小限の設定になっていることを確認	「/proc/sys」の下の最小限の設定が明確であること	-	-	「/proc/sys」の下のシステムデフォルト設定を確認し、事前条件で明確となっている最小限の設定となっていること
V-24MM.SEC.PLAT.OS.GEN.3	ユーザーが使用できるデフォルトのLinuxリソース制限が最小限の値に設定されていることを確認	ユーザーが使用できるLinuxリソース制限の最小限の値が明確であること	1．ulimitやgetrlimitのコマンドを使用してデフォルト設定を確認	-	ユーザーが使用できるデフォルトのLinuxリソース制限が最小限の値に設定されていること
V-24MM.SEC.PLAT.OS.GEN.5	LinuxカーネルのCONFIG_AUDITオプションがオンになっていることを確認	-	1．カーネルパラメータがaudit=1に設定されていることを確認	-	LinuxカーネルのCONFIG_AUDITオプションがオンになっていること
V-24MM.SEC.PLAT.OS.GEN.6	Linux PRNGの初期および起動時にPRNGをシードすることを確認	-	-	-	Linux PRNGの初期および起動時にPRNGをシードすること
V-24MM.SEC.PLAT.OS.GEN.7	パスワードおよびPINの全てはソルト処理されたハッシュとして保存されることを確認	パスワードおよびPINのすべてが明確であること	-	-	パスワードおよびPINの全てはソルト処理されたハッシュとして保存されること
V-24MM.SEC.PLAT.OS.GEN.8	ASLRが有効であることを確認	-	1．/proc/sys/kernel/randomize_va_spaceの設定を確認	-	/proc/sys/kernel/randomize_va_spaceの設定値が2であること
V-24MM.SEC.PLAT.OS.GEN.9	KASLRが有効であることを確認	-	1．LinuxカーネルのCONFIG_RANDOMIZE_BASEの設定を確認	-	CONFIG_RANDOMIZE_BASEの設定値がYであること
V-24MM.SEC.PLAT.OS.GEN.10	KASLRに使用するPRNGは、PRNGによってシードされることを確認	-	-	-	KASLRに使用するPRNGは、PRNGによってシードされること
V-24MM.SEC.PLAT.OS.GEN.11	強制アクセス制御が有効であることを確認	-	1．許可されていないアクションを実行	-	強制アクセス制御が有効であり、許可されていないアクションがブロックされること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.OS.GEN.12	強制アクセス制御はenforcingモードで作動することを確認	-	1. 許可されていないアクションを実行	-	強制アクセス制御はenforcingモードで作動し、アクションがブロックされること
V-24MM.SEC.PLAT.OS.SFC.1	全てのデバッグおよび開発ユーティリティと未使用のコンポーネントがすべての号口ソフトウェアイメージから削除されていることを確認	使用する必要最小限のコンポーネントが明確であること	1. ファイルシステムダンプを使用して、この要件に違反するオブジェクトが残っていないことを確認	-	全てのデバッグおよび開発ユーティリティと未使用のコンポーネントがすべての号口ソフトウェアイメージから削除されていること
V-24MM.SEC.PLAT.OS.SFC.2	ライブカーネルパッチツールが無効かつ削除されていることを確認	-	1. ファイルシステムダンプを使用して、この要件に違反するオブジェクトが残っていないことを確認	-	ライブカーネルパッチツールが無効かつ削除されていること
V-24MM.SEC.PLAT.OS.SFC.3	全てのソフトウェアバイナリがストリップされていることを確認	-	1. ファイルシステムダンプを使用して、すべてのソフトウェアバイナリがこの要件を満たしていることを確認	-	全てのソフトウェアバイナリがストリップされていること
V-24MM.SEC.PLAT.OS.SFC.4	全てのソフトウェアバイナリが再配置に必要でない全てのシンボルを削除していることを確認(非パブリックシンボルは要削除)	-	1. ファイルシステムダンプを使用して、すべてのソフトウェアバイナリがこの要件を満たしていることを確認	-	全てのソフトウェアバイナリが再配置に必要でない全てのシンボルを削除していること
V-24MM.SEC.PLAT.OS.USR.1	Linuxのrootユーザーを使用するのは必要最小限とし、それ以外では通常のユーザーとして実行することを確認(adminなどの他の特権ユーザーは不可)	rootを使用するすべてのプロセスが明確であること	1. 実行中のシステム上の全てのプロセスが非rootで実行されることを確認	-	Linuxのrootユーザーを使用するのは必要最小限とし、それ以外では通常のユーザーとして実行すること
V-24MM.SEC.PLAT.OS.USR.2	使用されていないユーザーアカウントが削除されていることを確認	使用するユーザーアカウントが明確であること	1. システム構成および実行中のプロセスを調査し、全てのユーザーアカウントが使用されていることを確認	-	使用されていないユーザーアカウントが存在しないこと(削除されていること)
V-24MM.SEC.PLAT.OS.USR.3	使用されていないグループが削除されていることを確認	使用するグループが明確であること	1. システム構成および実行中のプロセスを調査し、全てのグループが使用されていることを確認	-	使用されていないグループが存在しないこと(削除されていること)
V-24MM.SEC.PLAT.OS.USR.4	全てのユーザーアカウントがロックされていることを確認	-	1. ユーザーアカウント設定ファイルを分析し、無効な(壊れた)ハッシュとなっていることを確認	-	全てのユーザーアカウントのログインが無効化されていること
V-24MM.SEC.PLAT.OS.USR.5	全てのグループがロックされていることを確認	-	1. グループアカウント設定ファイルを分析し、無効な(壊れた)ハッシュとなっていることを確認	-	全てのユーザーアカウントのログインが無効化されていること
V-24MM.SEC.PLAT.OS.USR.6	ログインシェルが無効であることを確認	-	1. ユーザーアカウント設定ファイルの分析、および各ユーザーとしてのログイン試行を行い、シェルが作成されないことを確認	-	ログインシェルが無効であること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.OS.USR.7	suidおよびsgid機能で特権昇格が組み込まれた機能が削除されていることを確認。また、最低限の権限昇格を必要とするバイナリについては、ソフトウェアサンドボックスの強制アクセス制御要件によって文書化および保護されていることを確認	特権昇格を必要とするバイナリが明確であること	1．ファイルシステムのダンプによりsuidおよびsgidが設定されたバイナリやスクリプトが文書化されたもの以外存在しないことを確認	-	・suidおよびsgid機能で特権昇格が組み込まれた機能が削除されていること ・最低限の権限昇格を必要とするバイナリについては、ソフトウェアサンドボックスの強制アクセス制御要件によって文書化および保護されていること
V-24MM.SEC.PLAT.OS.FS.1	「/dev」のマウントを除くすべてのファイルシステムで「nodev」マウント・オプションを使用していることを確認	-	1．各ファイルシステムのオプションをランタイム解析で確認	-	「/dev」のマウントを除くすべてのファイルシステムで「nodev」マウント・オプションを使用していること
V-24MM.SEC.PLAT.OS.FS.2	すべてのファイルシステムのマウントで「nosuid」マウント・オプションを使用していることを確認(suid/sgidアプリが存在してはならない場合に限る)	suid/sgidアプリが存在してはならないファイルシステムが明確であること	1．マウントされた各ファイルシステムのオプションをランタイム解析で確認	-	すべてのファイルシステムのマウントでで「nosuid」マウント・オプションを使用していること(suid/sgidアプリが存在してはならない場合に限る)
V-24MM.SEC.PLAT.OS.FS.3	すべてのファイルシステムのマウントでで「noexec」マウント・オプションを使用していることを確認(実行可能バイナリを持たない場合に限る)	実行可能バイナリを持たないファイルシステムが明確であること	1．マウントされた各ファイルシステムのオプションをランタイム解析で確認	-	すべてのファイルシステムのマウントでで「noexec」マウント・オプションを使用していること(実行可能バイナリを持たない場合に限る)
V-24MM.SEC.PLAT.OS.FS.4	デフォルトのumaskが制限的であることを確認(推奨設定は027であり、可能な限り制限的であること)	各ディレクトリ/ファイルに対するumaskの設定値が制限的であり、かつ明確であり文書化されていること	1．umaskと論拠が記載された文書と各プロセスの実行時のumaskの整合性を確認	-	デフォルトのumaskが制限的であり、文書と一致すること
V-24MM.SEC.PLAT.OS.FS.5	ファイルとディレクトリのアクセス許可が最低限であり、DACで保護されていることを確認	各ディレクトリ/ファイルに対するアクセス許可の設定値が制限的であり、かつ明確であること	1．ファイルシステムのダンプと動的ファイルシステムのランタイム分析により事前に明確化された設定と一致することを確認	-	ファイルとディレクトリのアクセス許可が最低限であり、DACで保護されていること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.OS.FS.6	業界のベストプラクティスに従って、システムパーティションがファイルシステムの論理的に分離された領域に適用されていることを確認(例：①起動に必須でないディレクトリ：/home, /usr、②動的に変化するディレクトリ：/var、③起動に必須のディレクトリ：その他(/bin, /boot, /dev, /etc, /lib, /mnt, /opt, /root, /sbin, /tmp)、②をRAMに割り当て、①・③をROMに割り当て)	システム起動に必須のファイル、必須でないファイル、動的に変化するファイルの区別が明確であり、別のパーティションに分けて格納されること	1．ファイルシステムのダンプを使用し、ファイルの格納場所が事前に明確化された設定と一致することを確認	-	業界のベストプラクティスに従って、システムパーティションがファイルシステムの論理的に分離された領域に適用されていること
V-24MM.SEC.PLAT.OS.KRN.1	Linuxカーネルが整合性モードまたは機密性モードでロックダウン機能を使用するように設定されていることを確認し、かつバイパスできないように設定されていることを確認	-	1．「/sys/kernel/security/lsm」を調べて、アクティブなLinux LSMを検証し、ロックダウンされていることを確認	-	Linuxカーネルが整合性モードまたは機密性モードでロックダウン機能を使用するように設定され、かつバイパスできないように設定されていること
V-24MM.SEC.PLAT.OS.KRN.2	Linuxカーネルは、Yama Linuxセキュリティモジュール(デフォルトモード：3)を有効にするように設定されていることを確認	-	1．「/sys/kernel/security/lsm」を調べて、アクティブなLinux LSMに「yama」が含まれていることを確認し、起動後に「/proc/sys/kernel/yama」が3に設定されていることを確認	-	Linuxカーネルは、Yama Linuxセキュリティモジュール(デフォルトモード：3)を有効にするように設定されていること
V-24MM.SEC.PLAT.OS.KRN.3	Linuxカーネルが署名付きカーネルモジュールのみをロードすることを確認	-	1．署名ありのカーネルモジュールが正常にロードされることを確認 2．署名なしのカーネルモジュールがロードを拒否されることを確認	-	Linuxカーネルが署名付きカーネルモジュールのみをロードすること
V-24MM.SEC.PLAT.STG.1	4.1「暗号アルゴリズム」および4.2「鍵管理」に従って、ストレージに渡されるデータが暗号化されていることを確認	-	1．ソフトウェア上にストレージの安全性を確保できる暗号化メカニズムがあることを確認	-	暗号鍵がTEEにのみアクセス可能でHLOSのソフトウェアへはアクセスできない仕組みになっていること
V-24MM.SEC.PLAT.STG.2	暗号化データが古いバージョンに置換されることを防ぐロールバック保護が実装されていることを確認	-	1．暗号化データを古いものと新しいものの2種類用意し(タイムスタンプのみを変えて他のパラメータは変えない)、ストレージ上に古いデータを格納後に新しいデータに置き換える	-	再書き込み不可であり、ロールバック保護が実装されていること
V-24MM.SEC.PLAT.STG.3	RPMBセクションに収まらないアイテムはハッシュ化が必須であり、直接RPMBに格納されるか、グループハッシュと一緒にRPMBに格納されることを確認	-	1．RPMBの使用方法について文書化	-	RPMBセクションに収まらないアイテムについてハッシュ化を行ったうえで、直接RPMBに格納されるか、グループハッシュと一緒にRPMBに格納されること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.STG.4	ルート鍵が装置に固有の暗号鍵に基づいて生成されていることを確認	-	1．セキュアストレージの実装と鍵生成プロセスについて文書化し、レビューを実施 2．2つの異なるデバイス上のセキュアストレージに保存された同一のシークレット値が異なる暗号文で保存されていることを確認	-	ルート鍵が装置に固有の暗号鍵に基づいて生成されていること
V-24MM.SEC.PLAT.STG.8	セキュアストレージ内の機密情報は、作成したLinuxアプリケーションのみがアクセスできることを確認	-	1．セキュアストレージの実装と通常のワールドアクセス制御メカニズムを文書化し、レビューを実施 2．別のアプリケーションのシークレット値にアクセスを試行するテストアプリを作成し、結果を確認	-	セキュアストレージ内の機密情報は、作成したLinuxアプリケーションのみがアクセスできること
V-24MM.SEC.PLAT.STG.9	セキュアストレージ実装は、APIを内部的に呼び出すアプリケーションのアイデンティティを決定することを確認	-	1．セキュアストレージの実装と通常のワールドアクセス制御メカニズムを文書化し、レビューを実施 2．別のアプリケーションのシークレット値にアクセスを試行するテストアプリを作成し、結果を確認	-	セキュアストレージ実装は、APIを内部的に呼び出すアプリケーションのアイデンティティを決定すること
V-24MM.SEC.PLAT.STG.10	HLOSセキュアストレージが、機密情報を保護するために使用できる共通アプリケーションプログラミングインターフェース (API) を公開することを確認	-	1．セキュアストレージの実装と通常のワールドアクセス制御メカニズムを文書化し、レビューを実施 2．セキュアなストレージにアイテムを格納し、APIを用いて構築したテスト・アプリケーションによる読み取りを試行し、結果を確認	-	HLOSセキュアストレージが、機密情報を保護するために使用できる共通アプリケーションプログラミングインターフェース (API) を公開すること
V-24MM.SEC.PLAT.STG.11	HLOSセキュアストレージAPIが、機密情報を保護するために使用するすべてのソフトウェアと互換性のあるプログラミング言語をサポートすることを確認	-	1．セキュアストレージの実装とAPIを文書化し、レビューを実施 2．サポートされている各言語でテストアプリケーションを構築し、セキュアなストレージに格納したアイテムの読み戻しを試行し、結果を確認	-	HLOSセキュアストレージAPIが、機密情報を保護するために使用するすべてのソフトウェアと互換性のあるプログラミング言語をサポートすること
V-24MM.SEC.PLAT.FDE.1	外部の永続ストレージに書き込まれるECU上のすべてのデータが暗号化されることを確認	-	1．外部の永続ストレージ内の未加工コンテンツをダンプし、エントロピーを分析して、コンテンツが暗号化されていることを確認	-	外部の永続ストレージに書き込まれるECU上のすべてのデータが暗号化されること
V-24MM.SEC.PLAT.FDE.2	フルディスク暗号化が、一般的なソフトウェアアプリケーションに対して明白な方法で、SoCの外部に保存されたすべてのデータを暗号化することを確認	-	1．フルディスク暗号化の実施について文書化し、レビューを実施	-	フルディスク暗号化が、一般的なソフトウェアアプリケーションに対して明白な方法で、SoCの外部に保存されたすべてのデータを暗号化すること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.FDE.3	(利用可能な場合)フルディスク暗号化を実施するためにSoCのインライン暗号化機能、またはdm-cryptのような代替実施手段が使用されることを確認	-	1．フルディスク暗号化の実施について文書化し、レビューを実施	-	(利用可能な場合)フルディスク暗号化を実施するためにSoCのインライン暗号化機能、またはdm-cryptのような代替実施手段が使用されること
V-24MM.SEC.PLAT.FDE.6	全ディスク暗号化アルゴリズムが、AES-XTRまたはAES-GCMであることを確認	-	1．フルディスク暗号化と暗号化アルゴリズムの実施ついて文書化し、レビューを実施	-	全ディスク暗号化アルゴリズムが、AES-XTRまたはAES-GCMであること
V-24MM.SEC.PLAT.FDE.7	完全なディスク暗号化鍵長が、少なくとも128ビットであり、性能目標を満たす最大長であることを確認	-	1．フルディスク暗号化と暗号化アルゴリズムの実施ついて文書化し、レビューを実施。最大暗号鍵長でない場合、パフォーマンスメトリクスを使用した正当化根拠も併せて提供すること	-	完全なディスク暗号化鍵長が、少なくとも128ビットであり、性能目標を満たす最大長であること
V-24MM.SEC.PLAT.SOC.1	SoCにより、各プロセッサーのアクセスが、メモリマップされた対象となる周辺機器のみに制限されることを確認	-	1．メモリマッピングされた周辺機器のアクセスコントロールについて文書化し、レビューを実施 2．プロセッサーが意図しない周辺機器へのアクセスを試みるテストアプリを作成し、そのアクセスが許可されないことを確認	-	SoCにより、各プロセッサーのアクセスが、メモリマップされた対象となる周辺機器のみに制限されること
V-24MM.SEC.PLAT.SOC.2	SoCにより、各プロセッサーのアクセスが、意図したメモリ範囲のみに制限されることを確認	-	1．各プロセッサーによるメモリへのアクセス制御について文書化し、レビューを実施 2．プロセッサーが意図しないメモリへのアクセスを試みるテストアプリを作成し、そのアクセスが許可されないことを確認	-	SoCにより、各プロセッサーのアクセスが、意図したメモリ範囲のみに制限されること
V-24MM.SEC.PLAT.SOC.3	SoCにより、バスマスタ機能を有する周辺機器のメモリアクセスが制限されることを確認	-	1．バスマスタ周辺機器のアクセス制御について文書化し、レビューを実施 2．アクセスを意図しないメモリの読み書きを試行するバスマスタ周辺機器を接続し、アクセスが許可されないことを確認	-	SoCにより、バスマスタ機能を有する周辺機器のメモリアクセスが制限されること
V-24MM.SEC.PLAT.SOC.4	SOCメモリ制御が、TEEまたはリッチOS以上の特権で動作するノーマルワールドソフトウェアによってのみ変更又は更新されることを確認。	-	1．SOCメモリ制御の実装と設定のメカニズムについて文書化し、レビューを実施 2．特権のないノーマルワールドのテストアプリにSoCメモリコントロールの設定変更を施行させ、許可されないこと確認	-	SOCメモリ制御が、TEEまたはリッチOS以上の特権で動作するノーマルワールドソフトウェアによってのみ変更又は更新されること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.LOG.GEN.1	ECU上のすべてのソフトウェアコンポーネントが、本文書の要件を満たすロギングサブシステムにアクセスできることを確認	-	1．ソフトウェア設計レビュー時に、各ソフトウェアコンポーネントが使用するログサブシステムについて文書化し、レビューを実施	-	ECU上のすべてのソフトウェアコンポーネントが、本文書の要件を満たすロギングサブシステムにアクセスできること
V-24MM.SEC.PLAT.LOG.GEN.2	ECUログアーキテクチャが、ECUの中核機能や安全性や車両運用などの重要な機能のパフォーマンスを低下させるほど多くの処理リソースやIOリソースを消費しないように設計されることを確認	テストのための各ログ設定セットを定義すること	1．ECU上の各ログサブシステムが、記録を生成できる速度でログ記録の連続ストリームを同時に生成するようにし、事前に定義した各ログ設定セットに対して実施	-	重要な機能またはユーザーが視認できる機能の性能が低下しないこと
V-24MM.SEC.PLAT.LOG.GEN.3	すべてのログアペンダまたはログシンクが、本番環境で使用されていない場合、無効にされるか削除されることを確認	-	1．ECUで使用されるすべてのログアペンダまたはログシンクについて文書化し、レビューを実施 2．ECUファイルシステムおよびログ構成を分析し、システム上に本番環境で使用されないログアペンダまたはログシンクが存在しないことを確認	-	すべてのログアペンダまたはログシンクが、本番環境で使用されていない場合、無効にされるか削除されること
V-24MM.SEC.PLAT.LOG.GEN.4	ECUログサブシステムがすべて、少なくとも1ミリ秒の精度の時間源を使用することを確認	-	1．ECUロギングサブシステムが、使用する時刻源から現在時刻を読み取る能力を提供し、その時刻が１ミリ秒以内に現在の時刻と一致することを確認	-	ECUログサブシステムがすべて、少なくとも1ミリ秒の精度の時間源を使用すること
V-24MM.SEC.PLAT.LOG.CFG.3	ロギング・エコシステムは、ロギング構成の変更が意図されたメカニズムによってのみ発生するように設計されていることを確認。さらに、更新可能なロギング構成が破損している場合、ロギング構成は既知のデフォルトに設定されることを確認。	サプライヤーは②の手順で利用されるルートレベルのコンソールを有効にするテストファームウェアは提供すること	1．ECUロギングアーキテクチャの設計について文書化し、レビューを実施 2．テストファームウェアによりログ設定ファイルを変更できないことを確認。また、ロギングサブシステムが非ロギングソフトウェアによる他のソフトウェアのログ設定の変更を許可しないことを確認。さらに、意図されたメカニズムで破損したロギング構成に変更時にデフォルト構成で設定されることを確認。	-	ロギング・エコシステムは、ロギング構成の変更が意図されたメカニズムによってのみ発生するように設計されていること。また、裏返しで、意図されていないメカニズムによってログ構成が変更できないこと。さらに、更新可能なロギング構成の破損時はデフォルト構成で設定されること。
V-24MM.SEC.PLAT.LOG.CFG.6	ログ設定変更によるログ機能検証 ・ロギング設定変更中の電源OFFにより、再起動後、ロギングが設定変更前の状態で処理されること ・異なるユーザにより、ログ設定の同時設定変更しても正常にログ設定がなされること	・ロギング機能が正常に動作していること	変更中の電源OFF 1．ロギング設定変更中の電源OFF 2．再度電源ON 複数ユーザによる設定変更 3．異なるユーザから同時にロギング設定変更を実施	・ロギング設定内容に一貫性があること ・ログ処理が正常に動作すること	・ロギング設定の変更中の突然の電源切断後、ログ機能が正常に動作すること ・異なるユーザーによるロギング設定への同時変更しても一貫性を保持し、ログ機能が正常に動作すること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.LOG.CI.1	ログレコードの暗号化による機密性担保 すべてのログ記録は、保管時に不正な読み取りから保護されるものとする。この保護は、ログ記録を暗号化することによって実施するものとする。	・ロギング機能が正常に動作していること ・FDEが有効の状態で端末を起動すること	1．任意のログを記録 2．ログレコードを含む領域のバイナリフラッシュイメージを取得 3．バイナリフラッシュイメージ内にログのテキストデータが含まれないことを検証	-	・バイナリフラッシュイメージ内にログのテキストデータが含まれないことを確認すること
V-24MM.SEC.PLAT.LOG.CI.2	ログレコードの完全性保護メカニズム検証 システムが意図しないログレコードの変更により、ログがバックエンドログデータベースにアップロードされないことを検証	・ロギング機能が正常に動作していること	１．規定のプロセス以外でログレコードを編集	-	・バックエンドログデータベースにアップロードされないことを確認すること
V-24MM.SEC.PLAT.LOG.CI.3	ログレコードのアクセス保護 アプリケーションまたはソフトウェアプロセスは、他のアプリケーションまたはプロセスのログを読み取ったり、変更したり、削除したりできないことを検証	・ロギング機能が正常に動作していること ・強制アクセス制御が正常に動作していること	１．テスト用の規定外のプロセスから、特定プロセスの専用ログの読み込み、変更をおこなう	-	・実行中に他のソフトウェアがログレコードにアクセスできないことを確認すること
V-24MM.SEC.PLAT.CRT.1	証明書管理 証明書マネージャは、証明書検証のために信頼のルートを確立する認証局 (CA) ストアを維持することを確認	-	・セキュリティチップのコンフィグレーションを確認する	-	190_[Body]_jpn_24CY_情報セキュリティ要求仕様書のAppendix.Aに規定されている証明書がセキュリティチップに登録されていることを確認すること
V-24MM.SEC.PLAT.CRT.2	証明書管理 証明書マネージャによって維持されるCAストアは、必要な接続を可能にするために必要な最小セットに制限されることを確認	-	・セキュリティチップのコンフィグレーションを確認する	-	190_[Body]_jpn_24CY_情報セキュリティ要求仕様書のAppendix.Aに規定されている証明書がセキュリティチップに登録されていることを確認すること
V-24MM.SEC.PLAT.CRT.4	証明書失効確認の検証 証明書失効確認が共通のモジュールで実行されていることを確認する	・トヨタサーバとの通信が可能であること ・3rdPartyサーバとの通信が可能であること	2つのユースケースで検証 ・トヨタセンターサーバと接続する ・3rdPartyサーバと接続する	-	失効された証明書を検証した結果、サーバと接続が確立しないこと
V-24MM.SEC.PLAT.COM.TLS.3	証明書チェーンの検証 TLSエンドポイントの認証は、信頼できる証明書ストア内のルート証明書に証明書がチェーンしていることを検証することによって、常に強制されることを確認	・トヨタサーバとの通信が可能であること	1．トヨタセンターサーバと接続する	-	・多段の証明書を使ったサーバ認証が行われていること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.COM.TLS.5	TLS接続で使用するクライアント証明書の検証 各ユニットは、相互TLSのために使用される固有のクライアント証明書を持つことを確認	・正常なクライアント証明書が実機に格納されていること	1. センタとの接続を実施する	-	・正常に認証が完了し、センタサーバと接続が完了すること。 ・クライアント証明書がECUごとにユニークであること
V-24MM.SEC.PLAT.COM.TLS.6	TLS接続で使用するクライアント証明書の検証 クライアント証明書は、トヨタによって発行され、トヨタ認証局で終わる証明書チェーンによって署名されることを確認	・正常なクライアント証明書が実機に格納されていること	1. センタとの接続を実施する	-	・正常に認証が完了し、センタサーバと接続が完了すること。 ・クライアント証明書がトヨタ認証局が発行したものと一致することを確認すること
V-24MM.SEC.PLAT.COM.REV.2	証明書管理 ・OSCPによる失効チェック	-	1. トヨタセンターサーバと接続する	-	OCSPレスポンダによる証明書の失効確認を行うこと。以下の仕様に準拠すること。 - RFC 5019 - RFC 6960 ・ECUは、CRLによる失効確認を行うこと。CRLダウンロード前に証明書のステータスをチェックすること。
V-24MM.SEC.PLAT.COM.REV.3	証明書管理 ECUは、OCSPステープリング (RFC 6066) をサポートするものとする。ECUは、TLSハンドシェイク中、常にstatus_request拡張を含むものとする。ECUは、OCSP応答が有効であり、かつ証明書が有効であることを検証するものとする。ECUは、OCSP応答が供給されている場合、常にステープルOCSP応答を使用するものとする。	-	1. トヨタセンターサーバと接続する	-	OCSPレスポンダによる証明書の失効確認を行うこと。以下の仕様に準拠すること。 - RFC 6066OCSPステープリング ・ ECUからのすべてのTLS接続にstatus_request拡張が存在すること ・ 有効なOCSPステープル応答が返された場合、ECUはその証明書の直接OCSPまたはCRLを続行しないこと ・ 無効なOCSPステープル応答が返された場合、ECUがTLS接続を終了すること ・ OCSPステイプル応答が返されない場合、ECUは引き続きその証明書のOCSP検証を指示すること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.COM.REV.4	証明書管理 ECUは、OCSP must staple (RFC 7633) をサポートするものとする。 ECUは、必須ステイプル証明書オプションが存在する場合はOCSP応答を提供しなければならず、存在しない場合はハードフェイルを強制するものとする。	・must-stapleオプションを含む証明書を持つテストサーバを使用すること	1. テストサーバと接続する	-	OCSPレスポンダによる証明書の失効確認を行うこと。以下の仕様に準拠すること。 - RFC 7633 OCSP must staple ・有効なOCSPステープル応答が返された場合、ECUはその証明書の直接OCSPまたはCRLを続行しないこと ・ 無効なOCSPステープル応答が返された場合、ECUがTLS接続を終了すること ・OCSPステープル応答が返されない場合は、ECUがTLS接続を終了すること
V-24MM.SEC.PLAT.COM.REV.6	証明書管理 ECUは、信頼証明書ストアに保存されたルート証明書にロールアップするために、証明書チェーン内のすべての証明書を検証するものとする。これには、サーバー証明書とすべての中間証明書が含まれます。	・must-stapleオプションを含む証明書を持つテストサーバを使用すること ・サーバ証明書および各中間証明書について、証明書を、適切な形式の署名で信頼できるルート証明書にチェーンされていないバージョンに置き換える	1. テストサーバと接続する	-	・ECUがTLS接続を終了すること
V-24MM.SEC.PLAT.COM.REV.7	証明書管理 ステープルされたOCSPが、証明書チェーン内の1つ以上の証明書についてサーバによってサポートされていない場合、ECUは、OCSPレスポンダ (「ダイレクト」OCSP) からOCSP応答のオンライン収集および検証を直接実行するものとします。	・must-stapleオプションを含む証明書を持つテストサーバを使用すること ・サーバ証明書および各中間証明書について、ステープル応答に証明書が含まないように設定	1. テストサーバと接続する	-	・ECUがTLS接続を終了すること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.COM.REV.8	証明書管理 ECUは、「ダイレクト」OCSPの実行時に複数のOCSP URLをサポートするものとする。OCSP URLへの接続が失敗した場合(例えば、タイムアウト)、ECUは、有効な応答が収集されるかリストが枯渇するまで、リスト内の次のOCSP URLを使用して再試行するものとする。	・複数のOCSP URLを指定した証明書を生成・登録すること	1. テストサーバと接続する	-	・2つ以上のOCSP URLを持つ証明書を生成し、最初のURLが接続を拒否した場合に、2番目のURLで直接OCSPが実行されること
V-24MM.SEC.PLAT.COM.REV.9	証明書管理 ECUは、すべてのアプリケーションが使用するOCSP応答をキャッシュするものとする。	・2つのヘッドユニットアプリケーションまたはサービスが同じエンドポイントにアクセスする必要があることを確認するか、または同じ中間証明書を設定	1. テストサーバと接続する	-	・両方が独立して、同じエンドポイント証明書または中間証明書に対して直接OCSPを実行すること ・1つのアプリケーションで直接OCSPを実行して、良好なOCSP応答を得てすぐに2番目のアプリケーションを起動し、直接OCSPを実行しないこと(キャッシュを使用)とTLS接続を完了すること ・1つのアプリケーションに、不良OCSP応答に対して直接OCSPを実行させる。次に、すぐに2番目のアプリケーションを起動し、TLS接続を終了すること
V-24MM.SEC.PLAT.COM.REV.10	証明書管理 ECUは、OCSP応答をキャッシュする時間を通知するCache-Control HTTPヘッダをサポートするものとする (RFC 5019) 。	-	1. テストサーバと接続する(Cache-control HTTPヘッダーをサポートするエンドポイントへの接続を実行)	-	OCSPレスポンダによる証明書の失効確認を行うこと。以下の仕様に準拠すること。 - RFC 5019 Cache-Control HTTPヘッダをサポート ・有効期限の直前にはキャッシュされたレスポンスが使用され (直接OCSPは実行されない) 、有効期限の直後には新しいレスポンスが収集される(直接OCSPが実行される) こと

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.COM.REV.11	証明書管理 ECUは、キャッシュ制御max-age指令およびOCSP応答のnextUpdateフィールドの最小値を超えない範囲でOCSP応答をキャッシュするものとする。	-	1．テストサーバと接続する(Cache-control HTTPヘッダーをサポートするエンドポイントへの接続を実行)	-	OCSPレスポンダによる証明書の失効確認を行うこと。以下の仕様に準拠すること。 - RFC 5019 Cache-Control HTTPヘッダをサポート ・有効期限の直前にはキャッシュされたレスポンスが使用され (直接OCSPは実行されない) 、有効期限の直後には新しいレスポンスが収集される (直接OCSPが実行される) こと ・キャッシュ制御max-age指令およびOCSP応答のnextUpdateフィールドの最小値を超えない範囲でOCSP応答をキャッシュすること
V-24MM.SEC.PLAT.COM.REV.12	証明書管理 ECUは、必要な場合にのみ更新されたOCSP応答をダウンロードするために、ETag HTTPヘッダーをサポートするものとします (RFC 5019) 。	-	1．テストサーバと接続する(ETag HTTPヘッダーをサポートするエンドポイントへの接続を実行)	-	OCSPレスポンダによる証明書の失効確認を行うこと。以下の仕様に準拠すること。 - RFC 5019 ETag HTTPヘッダをサポート ・ETagがOCSPが不要であることを示している場合、ECUが直接OCSPを実行する際にOCSPステータスを再ダウンロードしないこと
V-24MM.SEC.PLAT.COM.REV.13	証明書管理 OCSPがサーバによってサポートされていない場合、ECUは、すでにECUにインストールされている失効リストに対する検証をサポートするものとする。	・HU内に保持する失効リストに失効した証明書が設定されていること	１．リプログラミングにより失効リスト（失効した証明書を設定）を更新 2．テストサーバと接続する	-	・失効した証明書によるTLS接続が終了すること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.COM.REV.14	証明書管理 インストールされた失効リストが該当しない場合、ECUはCRLをダウンロードして検証するものとする。	・HU内に保持する失効リストへの失効設定がないこと	１．テストサーバと接続する	-	・OCSP非サポートのインストールされている失効リストの範囲外にある証明書を確認すること。CRLがダウンロードされ、適用されていること ・証明書がCRLで失効としてリストされているケースで、TLS接続が終了していること ・証明書がCRLで失効としてリストされてないケースで、TLS接続が続行されること
V-24MM.SEC.PLAT.COM.FWL.2	Firewall検証 ネットワークファイアウォールは、すべての組み込みチェーンに対してデフォルトのDROPポリシーを採用する必要があります。	-	1．Iptables -Lコマンドを実行し、Firewall設定を表示	-	・INPUT, OUTPUT, FORWARDチェーンに対してデフォルトのDROPポリシーが採用されていること
V-24MM.SEC.PLAT.COM.FWL.3	Firewall検証 ネットワークファイアウォールは、システム要件/ユーザーストーリーを実装するために必要なインバウンドおよびアウトバウンドトラフィックルールのみを許可するものとする。	-	1．Firewallによるホワイトリスト（iptables ACCEPT設定が対象）以外の条件でpingを実行	-	・システム要件/ユーザーストーリーを実装するために必要なインバウンドおよびアウトバウンドトラフィックルールのみを許可すること ・pingが接続タイムアウトすること
V-24MM.SEC.PLAT.COM.FWL.4	Firewall検証 ネットワークファイアウォールは、期待されるIPアドレスからのトラフィックのみを許可し、他のすべてをドロップするものとする。これは、各ネットワークサービス/ポートに対して特別に設定される。	-	1．Firewallによるホワイトリスト（送信元IPアドレス）以外の条件で有効なサービスポートに対しpingを実行	-	・ネットワークファイアウォールは、期待されるIPアドレスからのトラフィックのみを許可し、他のすべてをドロップすること ・pingが接続タイムアウトすること
V-24MM.SEC.PLAT.COM.FWL.5	Firewall検証 ネットワークファイアウォールは、ステートフルなパケット検査をサポートする。	-	1．Iptablesコマンドにより、Firewall設定を確認	-	・ネットワークファイアウォールは、ステートフルなパケット検査をサポートすること ・Firewallの設定にconnection trackingが設定されていること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.COM.FWL.6	Firewall検証 ネットワークファイアウォールは、FTPのようなマルチポートTCP/UDPプロトコルのサポートを省略する。	-	1. Iptablesコマンドにより、Firewall設定を確認	-	・FTPのようなマルチポートのTCP/UDPプロトコルのサポートを省くこと ・マルチポートのTCP/UDPプロトコルを必要とする場合、ICMPプロトコルエラーのiptables->conntrack->RELATED機能を禁止しないことを確認すること
V-24MM.SEC.PLAT.COM.FWL.7	Firewall検証 ネットワークファイアウォールは、次のものを包括的に許可しないものとする。 • アドレス範囲 • ポート範囲 • ネットワークインタフェース • プロトコル。	-	1. Iptablesコマンドにより、Firewall設定を確認	-	・アドレス範囲、ポート範囲、ネットワークインターフェイス、プロトコルが要求に応じてどんなときでもブロードキャストされないことを確認すること
V-24MM.SEC.PLAT.COM.FWL.8	Firewall検証 ネットワークファイアウォールはICMP要求を破棄する。	-	1. Iptablesコマンドにより、Firewall設定を確認	-	・ICMP要求を破棄する設定になっていること
V-24MM.SEC.PLAT.COM.WIFI.1	Wi-Fiインターフェース検証 Wi-Fiインターフェースは、WPA 2およびWPA 3モードをサポートするものとする。	-	1. Wi-Fi接続	-	・WPA 2（AES）およびWPA 3モードによりWi-Fi接続できることを確認すること
V-24MM.SEC.PLAT.COM.WIFI.2	Wi-Fiインターフェース検証 Wi-Fiインターフェースは、TKIPモードをサポートしないものとする。	-	1. Wi-Fi接続設定を確認	-	・Wi-Fiインターフェースは、TKIPモードをサポートしないこと
V-24MM.SEC.PLAT.COM.WIFI.5	Wi-Fiインターフェース検証 Wi-Fiインターフェースは、SSID、パスフレーズ、およびすべての秘密暗号物質を、セクション4.8 HLOSセキュアストレージに記述されているようにHLOSセキュアストレージに保存するものとする。	-	-	-	・Wi-Fiインターフェースは、SSID、パスフレーズ、およびすべての秘密暗号物質を、HLOSセキュアストレージに保存されていること
V-24MM.SEC.PLAT.COM.BLT.1	Bluetoothインターフェース検証	-	-	-	・BluetoothチップセットがBluetooth 4.2以上をサポートしていること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.COM.BLT.2	Bluetoothインターフェース検証	-	-	-	・Bluetoothインターフェイスは、Bluetooth LE接続のセキュリティモード1レベル4をサポートし、Bluetoothファームウェアがファームウェアのセキュリティモード1およびレベル4を使用しており、各ハードウェア(BLE v 4.2)がBluetooth LE接続でサポートされていること
V-24MM.SEC.PLAT.COM.BLT.3	Bluetoothインターフェース検証 Bluetoothインターフェースは、Just Worksペアリングモードをサポートしないものとする。ECUは、Just Worksペアリングのペアリング要求に失敗するものとする。それが不可能な場合、ECUはJust Worksのペアリング完了後、通信を受け付けずに1秒以内に強制的に接続を切断します。	検証用にBluetoothテストデバイスを用意	・Bluetoothテストデバイスをペアリングする	-	・Bluetoothインターフェースは、Just Worksペアリングモードをサポートしない・JustWorksペアリングモードが無効になっていることを確認するため、第2フェーズ (キー生成および交換フェーズ) でデバイスが交換する一時キー値がゼロ以外に設定されていることを検証すること。 ・Bluetoothテストデバイスを使用して、JustWorksペアリングの有無にかかわらず接続し、JustWorksペアリングがない場合、Bluetoothテストデバイスが正常に接続できることを確認すること ・JustWorksペアリングが使用されている場合は、ペアリングが失敗するか、切断されること

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.COM.BLT.4	Bluetoothインターフェース検証 Bluetoothインターフェースは、解決可能なプライベートBluetoothアドレスをサポートするものとし、15分以内ごとにアドレスをローテーションするものとする。	-	1. Bluetoothプロトコルアナライザを用いて装置からのBluetooth広告パケットを監視	-	・Bluetoothインターフェースは、解決可能なプライベートBluetoothアドレスをサポートしていること ・15分以内ごとにアドレスをローテーションすること ・Bluetooth MACがランダム化されていることを検証し、MACランダム化をサポートするようにBluetoothファームウェアが実装されていることを確認すること ・デバイスからのBluetooth広告パケットを監視することによって、Bluetooth MACがランダム化されることを検証すること
V-24MM.SEC.PLAT.COM.BLT.5	Bluetoothインターフェース検証 Bluetoothインタフェースは、2.5.2節に記述されるように、HLOS安全記憶装置にBluetoothリンクキーを格納する。	-	-	-	・Bluetoothリンクキーをセキュアストレージに格納すること
V-24MM.SEC.PLAT.COM.INT.1	USBインターフェース検証 USBインタフェースは、生産ユースケースに必要なデバイスのみをサポートするものとする。	-	1. USB-イーサネットアダプタを接続し、ネットワーク接続をおこなう	-	・USBインタフェースは、USB-イーサネットアダプタをサポートしないことを確認する
V-24MM.SEC.PLAT.COM.INT.2	CANインターフェース検証 CANインターフェースは、ECUの意図した機能を実行するために必要なCAN IDのみを送受信するものとする。これは、CAN IDのための送信および受信ホワイトリストによって実施される。	-	1. 不正なCAN信号をHUに送信	-	・CANインターフェースは、ECUの意図した機能を実行するために必要なCAN IDのみを送受信すること ・ECU宛であるがホワイトリストに実装されていないメッセージでCANBUSをフラッディングすることを確認する
V-24MM.SEC.PLAT.COM.INT.3	CANインターフェース検証 CANインターフェースのホワイトリスト機能は、CAN送受信パス内のすべてのSoCで実装されるものとする。	-	1. 不正なCAN信号をHUに送信	-	・CANインターフェースは、ECUの意図した機能を実行するために必要なCAN IDのみを送受信すること ・ECU宛であるがホワイトリストに実装されていないメッセージでCANBUSをフラッディングすることを確認する

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.PLAT.PER.1	シリアル・SSH コンソールの無効化	商品用ソフトウェアを使用すること	1．HUを起動し、シリアルポートに接続	-	・コンソールが認識しないこと
V-24MM.SEC.PLAT.PER.2	ECU内のプロセッサ間の周辺バス通信 ECU上のプロセッサ間の周辺バス通信は、機密情報の送信時に暗号化されるものとする。	-	1．ECU上のプロセッサ間周辺バス通信に機密情報の電気信号が流れるように操作する	-	・機密情報を含むバスレベル通信において、プロセッサー間のデータラインを利用して通信データ内容が暗号化されていることを検証すること
V-24MM.SEC.PLAT.PER.3	ECU内のプロセッサ間の周辺バス通信 機密情報を含むバスレベル通信は、メッセージ内容に完全性保護機構を実装しなければならない。	-	1．ECU上のプロセッサ間周辺バス通信に機密情報の電気信号が流れるように操作する	-	・機密情報を含むバスレベル通信は、メッセージ内容に完全性保護機構を実装され、完全性保護メカニズムを検証すること
V-24MM.SEC.PLAT.PER.8	周辺機器のバスマスタへの対策 バスマスタ機能を有する周辺機器は、必要最小限のメモリアクセスに制限されるものとする。	-	-	-	・IOMMUマッピングおよび割り当てを検証し、必要最小限のメモリアクセスに制限されていること
V-24MM.SEC.APP.CRYP.1	使用されている暗号アルゴリズムを精査し、自作された暗号アルゴリズムが使用されていないこと確認する。	-	使用されている暗号アルゴリズムを精査し、自作された暗号アルゴリズムが使用されていないことソースコードレビューで確認をする。	自作された暗号アルゴリズムが使用されていないこと確認する	自作された暗号アルゴリズムが使用されていない
V-24MM.SEC.APP.SB.1	U-Boot、Linux カーネル、ファイルシステム、およびアプリケーションのSWイメージを変更した状態でシステムをブートすると、ブートプロセスが終了することを確認する。 セキュアブートチェーンに組み込まれていない動的ライブラリを読み込み、実行した際に、システムが該当ライブラリのロードに失敗することを確認する。		U-Boot、Linux カーネル、ファイルシステム、およびアプリケーションのSWイメージを変更した状態でシステムをブートする。 ブートプロセスが終了することを確認する。 セキュアブートチェーンに組み込まれていない動的ライブラリ読み込ませ、実行した際に、システムが該当ライブラリのロードに失敗することを確認する。	ブートプロセスが終了することを確認する。 ライブラリのロードに失敗することを確認する。	ブートプロセスが終了するライブラリのロードに失敗する
V-24MM.SEC.APP.LOG.1	ソースコードのレビューにて、レビュー対象のソフトウェアによって実行されるすべてのロギングが明示的にログサブシステムを使用していることを確認する。標準出力または標準エラーに依存していないことを確認する。確認結果は、各マイルストーンでトヨタに送付する。		ソースコードのレビューにて、レビュー対象のソフトウェアによって実行されるすべてのロギングが明示的にログサブシステムを使用していることを確認する。標準出力または標準エラーに依存していないことを確認する。確認結果は、各マイルストーンでトヨタに送付する。	ログサブシステムを使用していることを確認する。 標準出力または標準エラーに依存していないことを確認する。	ログサブシステムを使用している 標準出力または標準エラーを使用していない。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.APP.LOG.2	サプライヤーは、各サイバーセキュリティ対策を違反しているテスト実施し、対応するログレコードが生成されることを確認する。 サプライヤーは、テストを再現するために必要なすべてのツールと文書をトヨタに提供する。		各サイバーセキュリティ対策を違反しているテスト実施し、対応するログレコードが生成されることを確認する。	対応するログレコードが生成されることを確認する。	下記のセキュリティ関連イベントを収集している。 • Authorization errors. Examples: o A process attempts to access memory it is not authorized for. o A process attempts to access a file it is not authorized for. o Unauthorized policy changes to Mandatory Access Control. o Violations of Mandatory Access Control policy. • Authentication errors. Examples: o A Linux user login fails. o Wi-Fi authentication failure. o PKI validation failure. • Hardware Access Control error. Example: o SoC throws an exception when normal world process accesses peripheral reserved for TrustZone. • Unexpected data: o High CPU, memory, IO, or network usage. o Low free storage. o Malformed communication packets or frames. o Unexpected return values or function parameters. • Failed updates. • Unexpected system reboot. • System crashes. • Time delta of more than 24 hours between RTC and gPTP.

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.APP.LOG.3	サプライヤーは、特にセキュリティに関連するすべてのイベントの少なくとも1つの例をテストし、対応するログレコードが生成されることを確認する サプライヤーは、トヨタの検証施設でテストを再現するために必要なすべてのツールと文書をトヨタに提供する。		セキュリティに関連するすべてのイベントの少なくとも1つの例をテストし、対応するログレコードが生成されることを確認する	対応するログレコードが生成されることを確認する。	下記のセキュリティ関連イベントを収集している。 Successful updates. Kernel modules loaded / unloaded. User logins. Debug tool accesses. Startup / shutdown
V-24MM.SEC.APP.LOG.4	サプライヤは、最も許容度の高いログ重大度レベルでECUのできるだけ多くの機能を実行しながら作成されたサンプルログファイルを生成する。生成されたログファイルにはソフトウェアコンポーネントのバージョン番号が含まれていることを確認する。 サンプルログファイルはトヨタに提供する。		生成されたログファイルにはソフトウェアコンポーネントのバージョン番号が含まれていることを確認する。	生成されたログファイルにはソフトウェアコンポーネントのバージョン番号が含まれていることを確認する。	ECUの起動時にすべてのソフトウェアコンポーネントのバージョンを記録している。
V-24MM.SEC.APP.LOG.5	サプライヤは、最も許容度の高いログ重大度レベルでECUのできるだけ多くの機能を実行しながら作成されたサンプルログファイルを生成する。ログファイルのバージョン番号がソースコードのバージョン番号と一致することを確認する。		ログファイルのバージョン番号がソースコードのバージョン番号と一致することを確認する。	ログファイルのバージョン番号がソースコードのバージョン番号と一致することを確認する。	ログファイルのバージョン番号がソースコードのバージョン番号と一致している。
V-24MM.SEC.APP.LOG.7	サプライヤは、最も許容度の高いログ重大度レベルでECUのできるだけ多くの機能を実行しながら作成されたサンプルログファイルを生成する。ログレコードに機密情報が含まれていないことを確認する。 サンプルログファイルはトヨタに提供する。		ログレコードに機密情報が含まれていないことを確認する。	ログレコードに機密情報が含まれていないことを確認する。	ログレコードが下記が含まれていない。 • Personal Information as defined in the P21MM Privacy Specification. • Raw protocol streams such as CAN frames or HTTPS payloads. • Firmware dumps. • Financial information • Cryptographic keys or state information • Bluetooth link keys • Wi-Fi passphrase • PIN codes • Passwords

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.APP.LOG.9	サプライヤは、最も許容度の高いログ重大度レベルでECUのできるだけ多くの機能を実行しながら作成されたサンプルログファイルを生成する。ログレコードに異なるソフトウェアコンポーネントを区別するラベルが含まれていることを確認する。 サンプルログファイルをトヨタに提供する。		ログレコードに異なるソフトウェアコンポーネントを区別するラベルが含まれていることを確認する。	ログレコードに異なるソフトウェアコンポーネントを区別するラベルが含まれていることを確認する。	ログレコードに異なるソフトウェアコンポーネントを区別するラベルが含まれている
V-24MM.SEC.APP.LOG.10	サプライヤは、最も許容度の高いログ重大度レベルでECUのできるだけ多くの機能を実行しながら作成されたサンプルログファイルを生成する。ログファイルのラベルがソースコードのラベルと一致することを確認する。		ログファイルのラベルがソースコードのラベルと一致することを確認する。	ログファイルのラベルがソースコードのラベルと一致することを確認する。	ログファイルのラベルがソースコードのラベルと一致する
V-24MM.SEC.APP.LOG.11	サプライヤは、最も許容度の高いログ重大度レベルでECUのできるだけ多くの機能を実行しながら作成されたサンプルログファイルを生成する。ログレコードに少なくとも1秒の精度のタイムスタンプが含まれていることを確認する。 サンプルログファイルをトヨタに提供する。		ログレコードに少なくとも1秒の精度のタイムスタンプが含まれていることを確認する。	ログレコードに少なくとも1秒の精度のタイムスタンプが含まれていることを確認する。	ログレコードに少なくとも1秒の精度のタイムスタンプが含まれている
V-24MM.SEC.APP.LOG.12	サプライヤは、最も許容度の高いログ重大度レベルでECUのできるだけ多くの機能を実行しながら作成されたサンプルログファイルを生成する。ログレコードに重大度レベルが含まれていることを確認する。 サンプルログファイルをトヨタに提供する。		ログレコードに重大度レベルが含まれていることを確認する。	ログレコードに重大度レベルが含まれていることを確認する。	ログレコードに重大度レベルが含まれている

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.APP.CRT.1	ファイルシステムをスキャンし、下記を実行する。 ・*.cer、*.pem、*.crt、*.derなどの一般的なファイル拡張子を探します。 ・PEMヘッダーで始まるファイルを探します。 ・Java 鍵ストア・ファイルを探します。 すべての証明書が単一のcentral certificate storeに属していることを確認する。		ファイルシステムをスキャンし、下記を実行する。 ・*.cer、*.pem、*.crt、*.derなどの一般的なファイル拡張子を探します。 ・PEMヘッダーで始まるファイルを探します。 ・Java 鍵ストア・ファイルを探します。 すべての証明書が単一のcentral certificate storeに属していることを確認する。	すべての証明書が単一のcentral certificate storeに属していることを確認する。	すべての証明書が単一のcentral certificate storeに属している
V-24MM.SEC.APP.CRT.2	TLS 操作を実行するすべてのアプリケーションを識別できていることを確認する。 下記の観点で確認をする 1) サプライヤから提供されたドキュメント上で確認をする。 2) アプリケーションのトラフィックに対してセクション 4.13.5 証明書失効チェックの検証チェックを実行できていることを確認する。 または 3) アプリケーションをリバースエンジニアリングすることにより、各アプリケーションが共通の証明書失効サービスを使用していることを証明する。		TLS 操作を実行するすべてのアプリケーションを識別できていることを確認する。 1) サプライヤから提供されたドキュメント上で確認をする。 2) アプリケーションのトラフィックに対してセクション 4.13.5 証明書失効チェックの検証チェックを実行できていることを確認する。 または 3) アプリケーションをリバースエンジニアリングすることにより、各アプリケーションが共通の証明書失効サービスを使用していることを証明する	TLS 操作を実行するすべてのアプリケーションを識別できていることを確認する。 アプリケーションのトラフィックに対してセクション 4.13.5 証明書失効チェックの検証チェックを実行できていることを確認する。 または、アプリケーションをリバースエンジニアリングすることにより、各アプリケーションが共通の証明書失効サービスを使用していることを証明する	TLS 操作を実行するすべてのアプリケーションを識別できている。 アプリケーションのトラフィックに対してセクション 4.13.5 証明書失効チェックの検証チェックを実行できている。または各アプリケーションが共通の証明書失効サービスを使用している
V-24MM.SEC.APP.COM.EXT.3	バックエンド接続試行のトレースまたはログから、この要件を検証できいることを確認する。 ログは、使用されている認証の種類の証明となります。		バックエンド接続試行のトレースまたはログから、この要件を検証できいることを確認する。	バックエンド接続試行のトレースまたはログから、使用されている認証の種類を確認する。	mutual-TLSで認証している。
V-24MM.SEC.APP.COM.EXT.11	サプライヤーは、受信機またはテストツールの認証コードを変更して暗号化できていることを確認する 受信したデータが正確であるか、正確でない場合通信を終了しているか確認する		受信機またはテストツールの認証コードを変更して暗号化できていることを確認する 受信したデータが正確であるか、正確でない場合通信を終了しているか確認する	テストツールの認証コードを変更し、暗号化できていることを確認する。 受信したデータが正確であるか、正確でない場合通信を終了しているか確認する	TLSトランスポート暗号化に加えてエンドツーエンドで暗号化している。 受信したデータが正確でない場合通信を終了している。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.APP.COM.WIFI.1	WPA2、WPA3の接続方式でのみ接続されることを確認する。 上記以外の接続方式は無効化されていることを確認する。	WPA2、WPA3以外の接続方式は無効化されている。	WPA2、WPA3で接続できることを確認する。	-	WPA2、WPA3で接続できること。 WPA2、WPA3以外の接続方式が無効化されていることを確認すること
V-24MM.SEC.APP.COM.BLT.1	サプライヤーは、Bluetoothのバージョンおよびその他の情報の証明を提供し、この要件を検証できていることを確認する。 コマンドを使用して取得できます: sudo hcitool -a		Bluetoothのバージョンおよびその他の情報の証明を提供し、この要件を検証できていることを確認する。	Bluetoothサービスは、NIST SP 800-121 リビジョン 2 に準拠しているか確認する。	Bluetoothサービスは、NIST SP 800-121 リビジョン 2 に準拠している
V-24MM.SEC.APP.COM.BLT.2	サプライヤーは、使用されているBluetoothバリアントの文書を提供することにより、この要件が検証できていることを確認する。 コマンドを使用して取得することができます: sudo hcitool -a		使用されているBluetoothバリアントの文書を提供することにより、この要件が検証できていることを確認する。	すべてのBluetoothサービスは、BluetoothのBR、EDR、および高速(HS)接続に対してセキュリティモード4 レベル4となっていることを確認する。	Bluetoothサービスは、BluetoothのBR、EDR、および高速(HS)接続に対してセキュリティモード4 レベル4となっている
V-24MM.SEC.APP.COM.BLT.3	サプライヤーは、使用されているBluetoothバリアントの文書を提供することにより、この要件が検証できていることを確認する。 コマンドを使用して取得することができます: sudo hcitool -a		使用されているBluetoothバリアントの文書を提供することにより、この要件が検証できていることを確認する。	すべてのBluetoothサービスは、BluetoothのLE接続のためにセキュリティモード1レベル4になっていることを確認する。	Bluetoothサービスは、BluetoothのLE接続のためにセキュリティモード1レベル4になっている
V-24MM.SEC.APP.COM.BLT.4	サプライヤーは、Bluetooth sniffer toolを使用して要件が検証されていることを確認する。 例.)nRF Sniffer for Bluetooth LE ツールから取得したデータは、コンテンツが暗号化されていることを示す証拠として残すこと。		Bluetooth sniffer tool を使用して要件が検証されていることを確認する。	Bluetoothサービスは、Bluetoothの既存のメカニズムの上にアプリケーションレベルの認証と暗号化を実装され、下記に準拠しているかを確認する。 Security Recommendation #25 Table 4-2. Bluetooth Piconet Security Checklist from NIST SP 800-121 revision 2 https://csrc.nist.gov/publications/detail/sp/800-	Security Recommendation #25 Table 4-2. Bluetooth Piconet Security Checklist from NIST SP 800-121 revision 2 に準拠している

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
				121/rev-2/final.	
V-24MM.SEC.APP.HRD.1	サプライヤーはlinker ELFファイルをレビューし、GNU-STACK項目がRWを示していることを検証、確認する。 トヨタでも、GNU-STACKの項目がRWを示していることを確認する。		linker ELFファイルをレビューし、GNU-STACK項目がRWを示していることを検証、確認する。	ARM Execute Never (XN)ビットは、コードを含むメモリ領域のみを実行できるように、ソフトウェアによって有効にして構成できているかを確認する。 (XN) ビット・タグ領域は、「実行しない」または「非実行可能コード」として指定され、この領域のコードを実行しようとすると、実行を停止するセグメンテーション違反が発生することを確認する。	ARM Execute Never (XN)ビットは、コードを含むメモリ領域のみを実行できるように、ソフトウェアによって有効にして構成できている。 (XN) ビット・タグ領域は、「実行しない」または「非実行可能コード」として指定されている。 (XN) ビット・タグ領域のコードを実行しようとすると、実行を停止するセグメンテーション違反が発生する
V-24MM.SEC.APP.SBX.1	MAC ポリシーとシステム リソース (ファイル、プロセスなど) に配置されている MAC ラベルを確認する。 アプリケーションが可能な限り制限されていることを確認する。		MAC ポリシーとシステム リソース (ファイル、プロセスなど) に配置されている MAC ラベルを確認する。 アプリケーションが可能な限り制限されていることを確認する。	強制アクセス制御ポリシーが有効になってることを確認する。	下記のリソースに対し、強制アクセス制御ポリシーが有効になっている。 ・Files ・Directories ・Inter-process communication channels ・Other processes ・Peripherals

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.APP.SBX.2	実行中のすべてのプロセスの機能が必要な特権のみを持っていることを確認する。 アプリケーションの初期化の構成、実行時に機能が正しく設定されていることを確認する。		実行中のすべてのプロセスの機能が必要な特権のみを持っていることを確認する。 アプリケーションの初期化の構成、実行時に機能が正しく設定されていることを確認する。	実行中のすべてのプロセスの機能が必要な特権のみを持っていることを確認する。 アプリケーションの初期化の構成、実行時に機能が正しく設定されていることを確認する。	実行中のすべてのプロセスの機能が必要な特権のみを持っている（最小権限）。 アプリケーションの初期化の構成、実行時に機能が正しく設定されている。
V-24MM.SEC.APP.SBX.5	名前空間のコマンド ライン ツールを使用して、各プロセスが必要なネットワーク インターフェイスにのみアクセスできることを確認する。		名前空間のコマンド ライン ツールを使用して、各プロセスが必要なネットワーク インターフェイスにのみアクセスできることを確認する。	・Network namespaceでネットワークインターフェースなどへのアクセス制限でできていることを確認する。 ・IPC namespaceで、通信意図しない IPC 通信を防止されていることを確認する ・namespaceをマウントして、不要なファイルへのアクセスを防がれていることを確認する。 ・PID namespaceで、他のプロセスの操作を防がれていること確認する。 ・cgroup namespaceで、リソース制限の変更を防がれていることを確認する。	Linux namespacesがアクセス制限するために使用されている。 ・Network namespaceでネットワークインターフェースなどへのアクセス制限でできている ・IPC namespaceで、通信意図しない IPC 通信を防止されている ・namespaceをマウントして、不要なファイルへのアクセスを防がれている。 ・PID namespaceで、他のプロセスの操作を防がれている ・cgroup namespaceで、リソース制限の変更を防がれている
V-24MM.SEC.APP.SBX.6	アプリケーションにてデータまたはコマンドをあふれさせて過剰なリソースを消費されないかを確認する。 アプリケーションが消費できるリソースが限られているため、システムの残りの部分が安定していることを確認する。 cgroup 構成を分析して、他のアプリケーションを検証し、制限が設定されていることを確認する。		アプリケーションにてデータまたはコマンドをあふれさせて過剰なリソースを消費されないかを確認する。 アプリケーションが消費できるリソースが限られているため、システムの残りの部分が安定していることを確認する。 cgroup 構成を分析して、他のアプリケーションを検証し、制限が設定されていることを確認する。	Linux cgroupを過剰なリソースを消費されないために使用されていることを確認する。 システムが安定していることを確認する。 cgroup 構成を分析して、他のアプリケーションを検証し、制限が設定されていることを確認する。	Linux cgroupを過剰なリソースを消費されないために使用している。 過剰にリソースを消費しようとしても、システムが安定している。 cgroup 構成を分析して、他のアプリケーションを検証し、制限が設定されている。

評価仕様ID	試験内容（MUST）	事前条件	試験手順	測定項目	合否判定
V-24MM.SEC.QC.FDE.1	外部フラッシュストレージがQualcomm Inline Crypto Engine (ICE)を使用したFull Disk Encryptionに対応していることを検証する。	-	外部フラッシュストレージがQualcomm Inline Crypto Engine (ICE)を使用したFull Disk Encryptionに対応しているか確認する。	-	外部フラッシュストレージがQualcomm Inline Crypto Engine (ICE)を使用したFull Disk Encryptionに対応していることを検証できた場合、合格とする。
V-24MM.SEC.QC.FDE.2	Qualcomm Inline Crypto Engine (ICE)がFull Disk Encryptionを行う際、NIST SP 800-38Eに従いAES XTSモードを利用するよう設定されていることを確認する。	-	Qualcomm Inline Crypto Engine (ICE)がFull Disk Encryptionを行う際の設定を確認する。	-	Qualcomm Inline Crypto Engine (ICE)がFull Disk Encryptionを行う際、NIST SP 800-38Eに従いAES XTSモードを利用するよう設定されていることを確認できた場合、合格とする。
V-24MM.SEC.QC.FDE.3	下記のブートイメージに対して、Qualcomm Unified Image Encryption (UIE) が実装されていることを確認する。 • XBL (including XBLSEC) • QSEE / QTEE • QHEE • All Trusted Applications	-	評価内容記載のブートイメージを確認する。	-	下記のブートイメージに対して、Qualcomm Unified Image Encryption (UIE) が実装されていることを確認できた場合、合格とする。 • XBL (including XBLSEC) • QSEE / QTEE • QHEE • All Trusted Applications"
V-24MM.SEC.QC.FDE.5	下記のブートイメージが暗号化されており、Qualcomm APPSBLで復号化されること確認する。 ・Linux kernel ・initramfs ・DTB images		1. 評価内容記載のブートイメージを確認する。 2. システムを起動する。		下記のブートイメージが暗号化されており、2でシステムが起動できることが確認できた場合、合格とする。 ・Linux kernel ・initramfs ・DTB images

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 CIAD

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 for Development) を用いて明確化する。別紙参照のこと。

Appendix F. 24MM Cybersecurity Specification_v1.3

TMNAより示された24MM Cybersecurity Specification_v1.3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_v1.3.pdfを参照のこと。