関係各部署　御中 **To departments concerned**	表示 Confidential level	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　/

ECU 脆弱性対策評価仕様書

Test specification of vulnerability countermeasure for ECU

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
E/E Architecture Development Div.
System network & architecture development dept 4G.

No. SEC-ePF-VUL-ECU-TST-SPEC-a00-07-b

承認 Approved	調査 Checked	作成 Created	Mar. 30, 2023
平林	平井	玉樹	Omission of signature (approved electronically)

適用 **Target**	サイバーセキュリティ管理策を織り込む ECU ECUs that cybersecurity controls are incorporated.
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 E/E Architecture Development Div System network & architecture development dept Contact for security inquiries Mail:epf-sec-sp@mega.tec.toyota.co.jp

変更履歴 Δ1

記号	Version	日付	変更者	項目	変更内容
	a00-00-a	2020/06/23	46F 松井	全項目	初版発行
Δ1	a00-01-a	2021/04/01	46F 石川	4.6	目標 AP の評価要件を追加
↑	↑	↑	↑	全要件	セキュリティレベルを目標 AP に変更
↑	↑	↑	↑	4.1 4.2 4.3	エビデンス記載内容の誤記修正
↑	↑	↑	↑	3.1	本書記載要件の実施が評価機関への委託前提でない旨を明記
↑	↑	↑	↑	1.3	関連文書に ISO/IEC 18045 を追記
	a00-01-b	2021/05/20	46F 清川	全項目	英訳の追加
Δ2	a00-02-a	2021/09/02	46F 玉樹	4.6	目標 AP の評価要件明確化に伴い要件追加
↑	↑	2021/09/16	↑	4.3.4 4.3.5 4.3.6	ファジングテスト対象の明記
↑	↑	↑	↑	4.6.3	評価項目除外方法の明確化
Δ3	a00-03-a	2021/10/06	46F 石川	4.2.2	脆弱性スキャンの適用対象を変更
Δ4	a00-04-a	2021/10/14	46F 玉樹	4.3.1	Wi-Fi/Bluetooth ファジング評価要件を変更
↑	↑	↑	↑	4.6.1	「侵入テストの結果(VULETS_03001)」を削除
Δ5	a00-05-a	2021/10/25	46F 早川	1.3 1.4	適用範囲、要件の記載の章構成変更と内容明確化
↑	↑	↑	46F 石川	3.4	侵入テスト要件(VULETS_03001)の削除
↑	↑	2021/11/01	46F 安江	1.5 1.6 1.7	関連文書を追加し、SEC-ePF-TRM-GUD-PROC-***-**-*に記載されている略語、用語の削除
↑	↑	↑	46F 石川	3.3	ファジングテスト要件を明確化、 ファジングテストの対象（VULETS_02009, VULETS_02010）を追加
↑	↑	2021/11/5	46F 玉樹	3.6.2 3.6.3	（別紙 1）攻撃テストケース定義ガイドを追加
↑	↑	↑	↑	1.2	図 1 を削除
↑	↑	↑	↑	全項目	エビデンス要求を削除
↑	↑	↑	↑	3.6.1 3.6.2	攻撃耐性評価対象の明確化

Δ6	a00-06-a	2022/9/29	46F 玉樹	3.2.1 3.2.2 3.3.1 3.3.2 3.3.3 3.3.4 3.3.5 3.3.6 3.3.7 3.3.8 3.3.9 3.3.10	脆弱性の修正時期の指定を削除
Δ7	a00-07-a	2022/11/10	46F 玉樹	3.5.1	既製品に対する結合評価の要件(VULETS_04001)を削除
↑	↑	↑	↑	全項目	参考要件を削除
↑	↑	↑	↑	2.1	CIAD を CIA に変更
Δ8	a00-07-b	2023/01/31	46F 玉樹	1.5	関連文書を削除
↑	↑	2023/03/14	↑	別紙 1 4	コマンドが例示である旨を追記
↑	↑	↑	↑	別紙 1	コマンドの誤記修正(WF-002,WF-004,WF-005,BT-003,BT-004,APP-001,APP-006,APP-013)
↑	↑	↑	↑	別紙 1	デバッグ機能が無効化されている場合の手順を追記(DBG-001)
↑	↑	↑	↑	別紙 1	前提条件の明確化(BT-004)
↑	↑	↑	↑	別紙 1	評価対象 ECU が Phase5 ダイアグの N_TA を用いた拡張フォーマットを使用する場合の対応を追記(APP-006,APP-007,APP-008,APP-010)
↑	↑	↑	↑	別紙 1	前提条件・手順の修正(WF-002)
↑	↑	↑	↑	別紙 1	手順の修正(BT-004)
↑	↑	↑	↑	別紙 1	手順・判定基準の修正(BT-005)

目次

1. はじめに

1.1. 本書の目的

本書は、ISO / SAE 21434（自動車サイバーセキュリティ規格）の要求を満たし、ECU の脆弱性を適切なレベルまで低減されていることを確認するために、サプライヤが ECU に対する脆弱性テストを実施する際の要求事項を定義する。

1.2. 本書の位置づけ Δ5

本書と同様に、ECU を脆弱性なく作り込むための要求仕様書／評価仕様書と、各文書の位置づけの一覧を表 1 に示す。

表 1　脆弱性を低減するための仕様書一覧

文書名	位置づけ
ECU 脆弱性対策要求仕様書	ECU 開発における各アーキテクチャ設計工程において、 脆弱性分析／脆弱性対策を実施する際の要求事項を定義。
ECU 脆弱性対策評価仕様書 （本書）	ECU 開発における各テスト工程において、セキュリティに 関連する機能の評価（脆弱性評価を含む）の要求事項を定義
共通脆弱性対策要求仕様書	攻撃者による脆弱性の探索を困難にするため、設計／ 評価、および、実装工程で、各 ECU が共通に実施すべき 脆弱性対策を定義。

1.3. 適用範囲 Δ5

トヨタでは、車両へのハッキングを防ぐため、攻撃の経路上に位置する ECU に対してセキュリティ仕様書の引き当てを指示している。本書の対象は、いずれかのセキュリティ機能の開発が指示された ECU（以降、セキュリティ対象 ECU と記す）である。

1.4. 要件の記載 Δ5

本書の各要件では、適用条件として以下２つの項目を定義している。各要件を確認し、条件に該当する要件に対応すること。

① 機能/部品 ：特定の機能（無線通信機能など）／ 特定の部品（既製品など）を利用するか否か

② 目標 AP Δ1：各 ECU に引当たるサイバーセキュリティ要求に付与された値（※）

※目標 AP の定義は ECU 脆弱性対策要求仕様書にて記載する Δ1。なお、本書で記載する要件は、評価機関への委託実施を想定するものではない Δ1。

1.5. 関連文書

本書の関連文書を以下に示す。

表 2 関連文書一覧

仕様書番号	名称
(欠番) Δ8	
SEC-ePF-VUL-ECU-REQ-SPEC	ECU 脆弱性対策要求仕様書
SEC-ePF-VUL-CMN-REQ-SPEC	共通脆弱性対策要求仕様書
SEC-ePF-TRM-GUD-PROC Δ5	車両サイバーセキュリティ及びプライバシー用語定義集

表 3 公的関連文書一覧

文書名	名称/外部リンク
ISO/SAE 21434	ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering https://www.iso.org/standard/70918.html
ISA Secure EDSA	IEC 62443 - EDSA Certification Δ4 https://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification IEC 62443 - EDSA Certification (In Japanese) https://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification-(In-Japanese)
ISO/IEC 18045	ISO/IEC 18045:2008

(CEM : Common Methodology for Information Technology Security Evaluation) Δ1	Information technology — Security techniques — Methodology for IT security evaluation https://www.iso.org/standard/46412.html

1.6. 略語の定義

本書で用いる略語を定義する。

表 4　略語一覧 Δ5

略語	解説
DoCAN	Diagnostic communication over Controller Area Network
DoIP	Diagnostic communication over Internet Protocol
EDSA	Embedded Device Security Assurance

1.7. 用語の定義

本書で用いる用語を定義する。

表 5　用語一覧 Δ5

用語	解説
EDSA	制御機器のセキュリティ保証に関する認証制度。評価項目は以下の通り。 ・通信に関する堅牢性試験 ・セキュリティ機能の実装評価 ・ソフトウェア開発の各フェーズにおけるセキュリティ評価

2. 本書の前提条件

本書では、サプライヤが ISO/SAE 21434 に準拠したプロセス&ルールを整備していることを前提とする。その上で、トヨタが要求するサイバーセキュリティ管理策を、迂回・突破する脆弱性が残っていないことを確認するための評価要件を定義する。

2.1. トヨタとサプライヤ間での CIA の締結 Δ7

ECU の開発を開始する際に、トヨタはサプライヤに外注品設計申入書（以降、外設申と記載）を発行し、ECU に対して引き当てる仕様書（セキュリティに関連する仕様書を含む）を指示している。

ISO/SAE 21434 に準拠するため、外設申の発行までに、トヨタとサプライヤ間の役割／責任分担を明確化し、CIA（Cybersecurity Interface Agreement）Δ7 を締結している。締結した CIAΔ7 は、セキュリティに関連する仕様書と合わせて外設申に添付している。

3. 脆弱性テスト

本章では、ECU に対して実施すべき脆弱性テストを定義する。

3.1. 共通要件

本節では、本章で定める要件で共通の要件事項を定義する。

エビデンスの作成期限についての要件事項

項目		内容
ID		VULETS_05001
適用条件[Δ5]	機能/部品	-
	目標 AP[Δ1]	-
要件		（欠番）

推奨ツールの使用に関する要件事項

項目		内容
ID		VULETS_05002
適用条件[Δ5]	機能/部品	全ての ECU
	目標 AP[Δ1]	全て
要件		解析・テストツールに関しては、各要件に記載されているツールの使用を推奨する。推奨ツール以外を使用する場合、代替ツールについて本書発行部署の合意を得ること。

3.2. 脆弱性スキャン

3.2.1. ポートスキャン

項目		内容
ID		VULETS_01001
適用条件[Δ5]	機能/部品	TCP、又は UDP ポートを持つ ECU
	目標 AP[Δ1]	全て
要件		ポートスキャンを実施し、必要なポートのみが開いていることを確認すること。不要なポートが開いていた場合は修正すること。[Δ6] ポートスキャン後に設計変更が発生した場合は、ポートスキャンを再度実施すること。[Δ6] ※IPv4 / IPv6 デュアルスタックに対応している場合は、すべてのバージョンにおいてポートスキャンを実施すること
推奨ツール		Nmap https://nmap.org/
理由		不要なポートが開いていると外部からの攻撃に悪用される危険性があるため

3.2.2. 公知の脆弱性スキャン

項目		内容
ID		VULETS_01002
適用条件 Δ5	機能/部品	「ECU 脆弱性対策要求仕様書」の VULERQ_01001 で特定された既製品を含み、IP 通信 IF を備える ECUΔ3
	目標 APΔ1	全て
要件		IP 通信 IF を利用して Δ3 公知の脆弱性スキャンを実施し、脆弱性が検出されないことを確認すること。 発見された脆弱性は修正すること。やむをえず取り除けない場合には、その脆弱性をエビデンスに記載した上で、許可を得ること。Δ6 公知の脆弱性スキャン後に設計変更が発生した場合は、公知の脆弱性スキャンを再度実施すること。Δ6
推奨ツール		Nessus
理由		公知の脆弱性が残存している場合、攻撃の糸口として利用される可能性があるため。

3.3. ファジングテスト

3.3.1. Wi-Fi／Bluetooth のファジングテスト

項目		内容
ID		VULETS_02001
適用条件 Δ5	機能/部品	Wi-Fi / Bluetooth の通信 IF を備える ECU
	目標 APΔ1	14~20Δ5
要件		Wi-Fi / Bluetooth に対して、推奨ツールのデフォルト設定で全パターンのファジングテストを実施し、セキュリティの脆弱性が発見されないことを確認すること。(*1) Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙動とずれがないこと、ファズデータに対して例外処理(*2)が動いていることなどを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 ECU がテストの間その負荷に対して正常であること。 Δ4 発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール		Defensics
理由		想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、それを攻撃の糸口とされる可能性があるため。

3.3.2. イーサネット系通信プロトコルのファジングテスト

項目		内容
ID		VULETS_02002
適用条件 Δ5	機能/部品	イーサネット系通信プロトコル（イーサネット, ARP, IPv4, ICMPv4, UDP, TCP）を使用する IF を備える ECU
	目標 APΔ1	全て
要件		攻撃経路上の IF（目標 AP が割り当たる機能が配置されている IF）で用いる Δ5 イーサネット系通信プロトコル（イーサネット, ARP, IPv4, ICMPv4, UDP, TCP）に対して、以下の ISA Secure EDSA の CRT の評価仕様に示されるファジング テストを実施し、セキュリティの脆弱性が発見されないことを確認すること。(*1) Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙

項目	内容
	動とずれがないこと、ファズデータに対して例外処理(*2)が動いていることなどを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 - EDSA-310 Common Requirements for Communication Robustness Testing (CRT) - CRT Test Requirements for Protocols in EDSA Certification - EDSA-401 Ethernet robustness test specification - EDSA-402 ARP robustness test specification - EDSA-403 IPv4 robustness test specification - EDSA-404 ICMPv4 robustness test specification - EDSA-405 UDP robustness test specification - EDSA-406 TCP robustness test specification 発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール	Defensics
理由	想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、それを攻撃の糸口とされる可能性があるため。

3.3.3. ストレージデバイスのファジングテスト

項目		内容
ID		VULETS_02003
適用条件 Δ5	機能/部品	ストレージデバイス（USB, SD, CD, DVD, Blu-ray）を使用する IF を備える ECU
	目標 AP Δ1	14~20 Δ5
要件		ストレージデバイス（USB, SD, CD, DVD, Blu-ray）に対して、推奨ツールのデフォルト設定で、ファイル拡張子あたり 8 時間のファジングテストを実施し、セキュリティの脆弱性が発見されないことを確認すること。(*1) Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙動とずれがないこと、ファズデータに対して例外処理(*2)が動いていることなどを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 ECU がテストの間その負荷に対して正常であること。

	発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール	Defensics
理由	想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、それを攻撃の糸口とされる可能性があるため。

3.3.4. DoCAN のファジングテスト

項目		内容
ID		VULETS_02004
適用条件 Δ5	機能/部品	DoCAN を使用する IF を備える ECU
	目標 APΔ1	全て
要件 Δ2		攻撃経路上の IF（目標 AP が割り当たる機能が配置されている IF）で用いる Δ5DoCAN, 及び UDS に対して、推奨ツールのデフォルト設定で、全パターンのファジングテストを実施し、セキュリティの脆弱性が発見されないことを確認すること。(*1)Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙動とずれがないこと、ファズデータに対して例外処理(*2)が動いていることなどを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 ECU がテストの間その負荷に対して正常であること。 発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール		Defensics
理由		想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、それを攻撃の糸口とされる可能性があるため。

3.3.5. DoCAN のファジングテスト (CAN-FD)

項目		内容
ID		VULETS_02005
適用条件 Δ5	機能/部品	DoCAN（CAN-FD）を使用する IF を備える ECU
	目標 APΔ1	全て
要件 Δ2		攻撃経路上の IF（目標 AP が割り当たる機能が配置されている IF）で用いる

	Δ5DoCAN(CAN-FD), 及び UDS(CAN-FD)に対して、推奨ツールのデフォルト設定で、全パターンのファジングテストを実施し、セキュリティの脆弱性が発見されないことを確認すること。(*1)Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙動とずれがないこと、ファズデータに対して例外処理(*2)が動いていることなどを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 ECU がテストの間その負荷に対して正常であること。 発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール	Defensics
理由	想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、それを攻撃の糸口とされる可能性があるため。

3.3.6. DoIP のファジングテスト

項目		内容
ID		VULETS_02006
適用条件 Δ5	機能/部品	DoIP を使用する IF を備える ECU
	目標 APΔ1	全て
要件 Δ2		攻撃経路上の IF（目標 AP が割り当たる機能が配置されている IF）で用いる Δ5DoIP, 及び UDSonIP に対して、推奨ツールのデフォルト設定で、全パターンのファジングテストを実施し、セキュリティの脆弱性が発見されないことを確認すること。(*1)Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙動とずれがないこと、ファズデータに対して例外処理(*2)が動いていることなどを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 ECU がテストの間その負荷に対して正常であること。 発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール		Defensics
理由		想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、

	それを攻撃の糸口とされる可能性があるため。

3.3.7. CAN のファジングテスト

項目		内容
ID		VULETS_02007
適用条件 Δ5	機能/部品	CAN を使用する IF を備える ECU
	目標 AP Δ1	全て
要件		攻撃経路上の IF（目標 AP が割り当たる機能が配置されている IF）で用いる Δ5CAN に対して、推奨ツールのデフォルト設定（CAN Sequences, 及び OBD-II）で全パターンのファジングテストを実施し、セキュリティの脆弱性が発見されないことを確認すること。(*1) Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙動とずれがないこと、ファズデータに対して例外処理(*2)が動いていることなどを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 ECU がテストの間その負荷に対して正常であること。 発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール		Defensics
理由		想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、それを攻撃の糸口とされる可能性があるため。

3.3.8. CAN-FD のファジングテスト

項目		内容
ID		VULETS_02008
適用条件 Δ5	機能/部品	CAN-FD を使用する IF を備える ECU
	目標 AP Δ1	全て
要件		攻撃経路上の IF（目標 AP が割り当たる機能が配置されている IF）で用いる Δ5CAN-FD に対して、推奨ツールのデフォルト設定（CAN Sequences, 及び OBD-II）で、全パターンのファジングテストを実施し、セキュリティの脆弱性が発見されないことを確認すること。(*1) Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙動とずれがないこと、ファズデータに対して例外処理(*2)が動いていること

	などを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 ECU がテストの間その負荷に対して正常であること。 発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール	Defensics
理由	想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、それを攻撃の糸口とされる可能性があるため。

3.3.9. TLS のファジングテスト Δ5

項目		内容
ID		VULETS_02009
適用条件	機能/部品	TLS を使用する IF を備える ECU
	目標 AP	14~20
要件		TLS に対して、推奨ツールのデフォルト設定で、全パターンのファジングテストを実施し、セキュリティの脆弱性が発見されないことを確認すること。 ECU がテストの間その負荷に対して正常であること。(*1) Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙動とずれがないこと、ファズデータに対して例外処理(*2)が動いていることなどを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール		Defensics
理由		想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、それを攻撃の糸口とされる可能性があるため。

3.3.10. HTTP のファジングテスト Δ5

項目		内容
ID		VULETS_02010
適用条件	機能/部品	HTTP を使用する IF を備える ECU

	目標 AP	14~20
要件		HTTP に対して、推奨ツールのデフォルト設定で、全パターンのファジングテストを実施し、セキュリティの脆弱性が発見されないことを確認すること。ECU がテストの間その負荷に対して正常であること。(*1) Δ5 *1) ツールで検出されるエラーが ECU の仕様において想定される応答・挙動とずれがないこと、ファズデータに対して例外処理(*2)が動いていることなどを確認する Δ5 *2) 正常入力、異常入力以外の想定外の入力に対する処理 Δ5 発見された脆弱性は修正すること。Δ6 ファジングテスト後に設計変更が発生した場合は、ファジングテストを再度実施すること。Δ6
推奨ツール		Defensics
理由		想定外の入力により予期せぬ異常動作や異常終了、再起動が発生する場合、それを攻撃の糸口とされる可能性があるため。

3.4. （欠番）Δ5

3.4.1. （欠番）Δ5

項目		内容
ID		VULETS_03001
適用条件 Δ5	機能/部品	
	目標 AP Δ1	
要件		（欠番）Δ5
推奨ツール		
理由		

3.5. （欠番）[Δ7]

3.5.1. （欠番）[Δ7]

項目		内容
ID		VULETS_04001
適用条件[Δ5]	機能/部品	-
	目標 AP[Δ1]	-
要件		（欠番）
推奨ツール		-
理由		-

3.6. 目標 AP の評価（攻撃耐性評価）Δ1Δ2

トヨタより各 ECU に指示するサイバーセキュリティ要求(セキュリティ機能)を ECU に実装する上で生ずる恐れのある脆弱性に対し、目標 AP 未満の攻撃を想定した評価を行い、セキュリティ機能の目標 AP 達成を確認する。評価の実施者は第三者ではなく、設計者を想定しているが、第三者で実施することも可能である。

3.6.1. 脆弱性候補の収集 Δ2Δ5

項目		内容
ID		VULETS_06001
適用条件 Δ5	機能/部品	全ての ECU
	目標 AP	全て
要件		セキュリティ機能に関連する全ての脆弱性候補を収集すること。収集する対象は脆弱性候補への対策有無に関わらず、下記で識別された全ての脆弱性候補である。ただし対策の結果、脆弱性として識別されなくなった脆弱性候補は収集の対象外とする。 ・脆弱性分析(「ECU 脆弱性対策要求仕様書」 VULERQ_01002, VULERQ_01004, VULERQ_02004, VULERQ_02005, VULERQ_02006) ・脆弱性スキャン(VULETS_01001, VULETS_01002) ・ファジング(VULETS_02001～VULETS_02010)
推奨ツール		なし
理由		リスクが許容できる値に低減していることを確認するため。

3.6.2. 評価項目の定義 Δ2

項目		内容
ID		VULETS_06002
適用条件 Δ5	機能/部品	全ての ECU
	目標 AP	全て
要件		VULETS_06001 にて収集した脆弱性候補に対し、攻撃の入り口から脆弱性候補までの攻撃経路を分析し、攻撃を想定した評価項目を定義すること。 評価項目の定義にあたり、(別紙 1) 攻撃テストケース定義ガイド Δ5 を参照してもよい。
推奨ツール		なし
理由		リスクが許容できる値に低減していることを確認するため。

3.6.3. AP の算出 Δ2

項目	内容

ID		VULETS_06003
適用条件 Δ5	機能/部品	全ての ECU
	目標 AP	全て
要件		VULETS_06002 にて策定した評価項目の実施に必要と想定される AP を机上にて算出すること。AP の算出方法については(別紙 1) 攻撃テストケース定義ガイド Δ5 を参照すること。 算出した AP が目標 AP 以上の場合は、評価項目から除外する。Δ2
推奨ツール		なし
理由		リスクが許容できる値に低減していることを確認するため。

3.6.4. AP の実機評価 Δ2

項目		内容
ID		VULETS_06004
適用条件 Δ5	機能/部品	全ての ECU
	目標 AP	全て
要件		VULETS_06002 にて策定した評価項目に従って評価を実施し、目標 AP 未満の攻撃が成功しないことを確認すること。算出した AP が目標 AP 未満の場合、当該脆弱性について対策し、目標 AP 未満の攻撃が成功しないことを確認すること。
推奨ツール		なし
理由		リスクが許容できる値に低減していることを確認するため。

Change History[Δ1]

Mark	Version	Date	Revised by	Item	Description
	a00-00-a	Jun.23,2020	46F Matsui	All items	Initial release
Δ1	a00-01-a	Apr.01,2021	46F Ishikawa	4.6	Add requirement “Evaluation of Target AP”.
↑	↑	↑	↑	All requirements	Replace security level with target AP.
↑	↑	↑	↑	4.1 4.2 4.3	Correction of errors for Contents described in the evidence.
↑	↑	↑	↑	3.1	Describe that it is not assumed that tests will be outsourced to external evaluation organization
↑	↑	↑	↑	1.3	Add ISO/IEC 18045 to reference documents.
	a00-01-b	May 20,2021	46F Kiyokawa	All items	Add English translation.
Δ2	a00-02-a	Sep.02,2021	46F Tamaki	4.6	Add requirement in accordance with evaluation requirement clarification of target AP
↑	↑	Sep.16,2021	↑	4.3.4 4.3.5 4.3.6	Describe targets of fuzz testing
↑	↑	↑	↑	4.6.3	Clarify method of removing from evaluation items.
Δ3	a00-03-a	Oct.06,2021	46F Ishikawa	4.2.2	Change the target of vulnerability scanning
Δ4	a00-04-a	Oct.14,2021	46F Tamaki	4.3.1	Change the requirement for Fuzz testing for Wi-Fi／Bluetooth
↑	↑	↑	↑	4.6.1	Delete “Result of penetration testing(VULETS_03001)”
Δ5	a00-05-a	Oct. 24,2021	46F Hayakawa	1.3 1.4	Change the chapter structure and clarify the content of scope and description of requirements
↑	↑	↑	46F Ishikawa	3.4	Delete Penetration Testing requirement(VULETS_03001)

↑	↑	Nov. 1,2021	46F Yasue	1.5 1.6 1.7	Add the related document and delete abbreviations and terms which are described in SEC-ePF-TRM-GUD-PROC-***-**-*
↑	↑	↑	46F Ishikawa	3.3	Clarify fuzz testing requirements, Add the target of fuzz testing(VULETS_02009, VULETS_02010)
↑	↑	Nov. 5,2021	46F Tamaki	3.6.2 3.6.3	Add（Annex 1）Guide for Defining Cyber Attack Test Case
↑	↑	↑	↑	1.2	Delete Fig 1.
↑	↑	↑	↑	All items	Delete evidence requirements.
↑	↑	↑	↑	3.6.1 3.6.2	Clarify the target of evaluation of target AP.
Δ6	a00-06-a	Sep. 29,2022	46F Tamaki	3.2.1 3.2.2 3.3.1 3.3.2 3.3.3 3.3.4 3.3.5 3.3.6 3.3.7 3.3.8 3.3.9 3.3.10	Delete vulnerability fix timing.
Δ7	a00-07-a	Nov. 10, 2022	46F Tamaki	3.5.1	Delete the requirement “Integration evaluation for off-the-shelf component(VULETS_04001)”
↑	↑	↑	↑	All items	Delete the “Reference requirements”
↑	↑	↑	↑	2.1	Change terms from CIAD to CIA
Δ8	a00-07-b	Jan.25, 2023	46F Tamaki	1.5	Delete the Related Document
↑	↑	Mar.14, 2023	↑	Annex 1 4	Add the note that commands are examples
↑	↑	↑	↑	Annex 1	Correct errors for commands(WF-002,WF-004,WF-005,BT-003,BT-004,APP-

					001,APP-006,APP-013)
↑	↑	↑	↑	Annex 1	Add the procedure when the debugging function is disabled(DBG-001)
↑	↑	↑	↑	Annex 1	Clarify the prerequisites(BT-004)
↑	↑	↑	↑	Annex 1	Add the action when the target evaluation ECU uses the extended format using N_TA of Phase5 Diagnosis(APP-006,APP-007,APP-008,APP-010)
↑	↑	↑	↑	Annex 1	Correct the prerequisites and procedure(WF-002)
↑	↑	↑	↑	Annex 1	Correct the procedure(BT-004)
↑	↑	↑	↑	Annex 1	Correct the procedure and criteria(BT-005)

Table of Contents

1. Introduction

1.1. Purpose of this Document

This document defines the requirements on vulnerability testing for ECU done by supplier to meet the requirements of ISO / SAE21434 and confirm that the vulnerability of ECU is mitigated to the appropriate level.

1.2. Position[Δ5]

Including this document, the requirements specification / test specification to design and implement ECU without vulnerabilities and each position are shown in Table 1.

Table 1　List of Specifications to reduce vulnerability

Title	Position
Requirements specification of vulnerability countermeasure for ECU	In each architecture design process in ECU development, define requirements for vulnerability analysis and vulnerability countermeasures.
Test specification of vulnerability countermeasure for ECU（this document）	In each test process in ECU development, define requirements for evaluating security-related features (including vulnerability assessments).
Requirements Specification of Common Vulnerability Countermeasure	To make it difficult for an attacker to find a vulnerability, define vulnerability countermeasures that each ECU should take in common during the design/evaluation and implementation process.

1.3. Scope[Δ5]

To prevent vehicle hacking, Toyota instructs the ECU located on the attack path to assign the security specification. The scope of this document is an ECU that is instructed to develop one of the securityfunctions. (Hereinafter an ECU that is instructed to develop one of the security specifications will be referred to as "security target ECU")

1.4. Description of Requirements[Δ5]

The following two items are defined as the application conditions for each requirement of this document. The ECU designer shall check each requirement and implement the requirements that apply to own condition.

① Functions/Parts：Whether to use specific functions (wireless communication function, etc.) / specific parts (Off-the-shelf products, etc.).

② Target AP[Δ1]：The value given to the cybersecurity requirement that is assigned to each ECU.　（※）

※The definition of target AP is described in “Requirements specification of vulnerability countermeasure for ECU”[Δ1]. Note that it is not assumed that tests will be outsourced to external evaluation organization, regarding

requirements in this document[Δ1].

1.5. Related Document

The documents related to this document are as follows.

Table 2 List of Related Documents

Specification Number	Title
(Delete)[Δ8]	
SEC-ePF-VUL-ECU-REQ-SPEC	Requirements specification of vulnerability countermeasure for ECU
SEC-ePF-VUL-CMN-REQ-SPEC	Requirements Specification of Common Vulnerability Countermeasure
SEC-ePF-TRM-GUD-PROC[Δ5]	Terms and Definitions related to Vehicle Cybersecurity and Privacy

Table 3 List of Public Related Documents

Abbreviation in this document	Title and External links
ISO/SAE 21434	ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering https://www.iso.org/standard/70918.html
ISA Secure EDSA	IEC 62443 - EDSA Certification[Δ4] https://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification IEC 62443 - EDSA Certification (In Japanese) https://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification-(In-Japanese)
ISO/IEC 18045 (CEM：Common Methodology for Information Technology Security Evaluation) [Δ1]	ISO/IEC 18045:2008 Information technology — Security techniques — Methodology for IT security evaluation https://www.iso.org/standard/46412.html

1.6. Abbreviations and Definitions

The abbreviations to be used in this document are explained in Table 4.

Table 4 List of Abbreviations[Δ5]

Abbreviation	Explanation
DoCAN	Diagnostic communication over Controller Area Network
DoIP	Diagnostic communication over Internet Protocol
EDSA	Embedded Device Security Assurance

1.7. Terms and Definitions

The terms used in this document are explained in Table 5.

Table 5 List of terms[Δ5]

Term	Explanation
EDSA	A Certification scheme for security assurance of control devices. Evaluation items are as below. ・Testing the robustness of communication ・Evaluating the implementations of security functions ・Evaluating the Security at each phase in software developments.

2. The precondition of this document

In this document, it's prerequisite that ISO/SAE 21434 compliant processes & rules of supplier are prepared. Based on this, this document defines the evaluation requirement to confirm that there are no vulnerabilities that can bypass or penetrate the cybersecurity control required by Toyota.

2.1. Conclusion CIA between Toyota and suppliers[Δ7]

When starting the development of the ECU, Toyota issues the REQUEST FOR DESIGN & DEVELOPMENT OF PARTS (subsequently described as "RDDP") to the supplier, it directs the specifications (including security-related specifications) to be assigned to the ECU.

In order to comply with ISO/SAE 21434, by the date the RDDP is issued, the division of roles /responsibilities between Toyota and the supplier will be clarified and a CIA (Cybersecurity Interface Agreement)[Δ7] will be concluded. The CIA[Δ7] concluded is attached to the RDDP in addition to the security-related specifications.

3. Vulnerability testing

This chapter defines vulnerability testing to be implemented for ECUs.

3.1. Common Requirement

This section provides common requirements for each requirement set out in this chapter.

Requirements for evidence creation deadlines

Item		Contents
ID		VULETS_05001
Application Conditions[Δ5]	Functions/Parts	-
	Target AP[Δ1]	-
Requirements		Deleted.

Requirements for use of the recommended tool

Item		Contents
ID		VULETS_05002
Application Conditions[Δ5]	Functions/Parts	All ECUs
	Target AP[Δ1]	All
Requirements		For analysis and test tool, use of a tool described in each requirement is recommended. If a tool other than the recommended tool is to be used, agreement on use of the substitute tool shall be obtained from the department issuing this document.

3.2. Vulnerability Scanning

3.2.1. Port Scanning

Item		Contents
ID		VULETS_01001
Application Conditions[Δ5]	Functions/Parts	ECUs with TCP or UDP ports
	Target AP[Δ1]	All
Requirements		Port scanning shall be performed and it shall be confirmed that only necessary ports are open. If an unnecessary port is open, it shall be fixed.[Δ6] If design changes occur after port scanning, port scanning shall be performed again.[Δ6] ※ If the in-vehicle part is corresponding to IPv4/IPv6 dual stack, port scanning shall be performed in both IPv4 and IPv6.
Recommended Tool		Nmap https://nmap.org/
Reasons		An open unnecessary ports would otherwise be exploited by an external attack.

3.2.2. Scanning public domain vulnerability

Item		Contents
ID		VULETS_01002
Application Conditions[Δ5]	Functions/Parts	ECUs with off-the-shelf components identified according to VULERQ_01001 in ” Requirements specification of vulnerability countermeasure for ECU” and IP communication IF. [Δ3]
	Target AP[Δ1]	All
Requirements		The supplier shall scan public domain vulnerabilities for using the IP communication IF[Δ3] and check that vulnerabilities have not been detected. If a vulnerability is discovered, it shall be fixed. [Δ6] If unavoidably the vulnerability cannot be remove, ECU design department shall describe the vulnerability in an evidence and shall obtain agreement from the department issuing this document. If design changes occur after scanning public domain vulnerability, scanning public domain vulnerability shall be performed again. [Δ6]
Recommended Tool		Nessus
Reasons		If a public domain vulnerability is remained, it would otherwise be exploited for a clue to attack.

3.3. **Fuzz testing**

3.3.1. Fuzz testing for Wi-Fi／Bluetooth

Item		Contents
ID		VULETS_02001
Application Conditions[Δ5]	Functions/Parts	ECUs with IF for Wi-Fi / Bluetooth communication.
	Target AP[Δ1]	14~20[Δ5]
Requirements		For Wi-Fi / Bluetooth, a fuzz testing shall be performed for all testing patterns with default configuration of the recommended tool, and it shall be confirmed that security vulnerabilities have not been detected. (*1) [Δ5] *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. [Δ5] *2) Processing for unexpected inputs other than normal and abnormal inputs.[Δ5] The target ECU shall be kept normal against the load during the test. [Δ4]The vulnerability found by fuzz testing shall be fixed.[Δ6] If design changes occur after fuzz testing, fuzz testing shall be performed again.[Δ6]
Recommended Tool		Defensics
Reasons		If an unexpected input causes unpredictable abnormal behavior, abnormal termination, or restart, it would otherwise be exploited for a clue to attack.

3.3.2. Fuzz testing for Ethernet based communication protocol

Item		Contents
ID		VULETS_02002
Application Conditions[Δ5]	Functions/Parts	ECUs with IF using Ethernet based communication protocol(Ethernet, ARP, IPv4, ICMPv4, UDP, TCP).
	Target AP[Δ1]	All
Requirements		For Ethernet based communication protocol (Ethernet, ARP, IPv4, ICMPv4, UDP, TCP) used in IF on the attack path (IF where the functions assigned Target AP are allocated)[Δ5], a fuzz testing indicated in the CRT specification in ISA Secure EDSA below shall be performed, and it shall be confirmed that security vulnerabilities have not been detected. (*1) [Δ5] *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. [Δ5] *2) Processing for unexpected inputs other than normal and abnormal inputs.[Δ5] - EDSA-310 Common Requirements for Communication Robustness Testing (CRT) - CRT Test Requirements for Protocols in EDSA Certification - EDSA-401 Ethernet robustness test specification - EDSA-402 ARP robustness test specification - EDSA-403 IPv4 robustness test specification - EDSA-404 ICMPv4 robustness test specification - EDSA-405 UDP robustness test specification - EDSA-406 TCP robustness test specification The vulnerability found by fuzz testing shall be fixed.[Δ6] If design changes occur after fuzz testing, fuzz testing shall be performed again.[Δ6]
Recommended Tool		Defensics
Reasons		If an unexpected input causes unpredictable abnormal behavior, abnormal termination, or restart, it would otherwise be exploited for a clue to attack.

3.3.3. Fuzz testing for storage device

Item		Contents
ID		VULETS_02003
Application Conditions[Δ5]	Functions/Parts	ECUs with IF using storage device（USB, SD, CD, DVD, Blu-ray）
	Target AP[Δ1]	14~20[Δ5]

Requirements	For storage device（USB, SD, CD, DVD, Blu-ray）, a fuzz testing shall be performed for 8 hours for each file extension with default configuration of the recommended tool, and it shall be confirmed that security vulnerabilities have not been detected. (*1) Δ5 *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. Δ5 *2) Processing for unexpected inputs other than normal and abnormal inputs.Δ5 The target ECU shall be kept normal against the load during the test. The vulnerability found by fuzz testing shall be fixed.Δ6 If design changes occur after fuzz testing, fuzz testing shall be performed again.Δ6
Recommended Tool	Defensics
Reasons	If an unexpected input causes unpredictable abnormal behavior, abnormal termination, or restart, it would otherwise be exploited for a clue to attack.

3.3.4. Fuzz testing for DoCAN

Item		Contents
ID		VULETS_02004
Application Conditions Δ5	Functions/Parts	ECUs with IF using DoCAN
	Target AP Δ1	All
Requirements Δ2		For DoCAN and UDS used in IF on the attack path (IF where the functions assigned Target AP are allocated)Δ5, a fuzz testing shall be performed for all testing patterns with default configuration of the recommended tool, and it shall be confirmed that security vulnerabilities have not been detected. (*1) Δ5 *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. Δ5 *2) Processing for unexpected inputs other than normal and abnormal inputs.Δ5 The target ECU shall be kept normal against the load during the test. The vulnerability found by fuzz testing shall be fixed. Δ6 If design changes occur after fuzz testing, fuzz testing shall be performed again. Δ6
Recommended Tool		Defensics
Reasons		If an unexpected input causes unpredictable abnormal behavior, abnormal termination, or restart, it would otherwise be exploited for a clue to attack.

3.3.5. Fuzz testing for DoCAN(CAN-FD)

Item		Contents
ID		VULETS_02005
Application Conditions[Δ5]	Functions/Parts	ECUs with IF using DoCAN（CAN-FD）.
	Target AP[Δ1]	All
Requirements [Δ2]		For DoCAN (CAN-FD) and UDS(CAN-FD) used in IF on the attack path (IF where the functions assigned Target AP are allocated)[Δ5], a fuzz testing shall be performed for all testing patterns with default configuration of the recommended tool, and it shall be confirmed that security vulnerabilities have not been detected. (*1) [Δ5] *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. [Δ5] *2) Processing for unexpected inputs other than normal and abnormal inputs.[Δ5] The target ECU shall be kept normal against the load during the test. The vulnerability found by fuzz testing shall be fixed. [Δ6] If design changes occur after fuzz testing, fuzz testing shall be performed again. [Δ6]
Recommended Tool		Defensics
Reasons		If an unexpected input causes unpredictable abnormal behavior, abnormal termination, or restart, it would otherwise be exploited for a clue to attack.

3.3.6. Fuzz testing for DoIP

Item		Contents
ID		VULETS_02006
Application Conditions[Δ5]	Functions/Parts	ECUs with IF using DoIP
	Target AP[Δ1]	All
Requirements [Δ2]		For DoIP and UDSonIP used in IF on the attack path (IF where the functions assigned Target AP are allocated)[Δ5], a fuzz testing shall be performed for all testing patterns with default configuration of the recommended tool, and it shall be confirmed that security vulnerabilities have not been detected. (*1) [Δ5] *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. [Δ5]

	*2) Processing for unexpected inputs other than normal and abnormal inputs.[Δ5] The target ECU shall be kept normal against the load during the test. The vulnerability found by fuzz testing shall be fixed.[Δ6] If design changes occur after fuzz testing, fuzz testing shall be performed again.[Δ6]
Recommended Tool	Defensics
Reasons	If an unexpected input causes unpredictable abnormal behavior, abnormal termination, or restart, it would otherwise be exploited for a clue to attack.

3.3.7. Fuzz testing for CAN

Item		Contents
ID		VULETS_02007
Application Conditions[Δ5]	Functions/Parts	ECUs with IF using CAN
	Target AP[Δ1]	All
Requirements		For CAN used in IF on the attack path (IF where the functions assigned Target AP are allocated)[Δ5], a fuzz testing shall be performed for all testing patterns with default configuration (CAN Sequences and OBD-II) of the recommended tool, and it shall be confirmed that security vulnerabilities have not been detected. (*1) [Δ5] *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. [Δ5] *2) Processing for unexpected inputs other than normal and abnormal inputs.[Δ5] The target ECU shall be kept normal against the load during the test. The vulnerability found by fuzz testing shall be fixed.[Δ6] If design changes occur after fuzz testing, fuzz testing shall be performed again.[Δ6]
Recommended Tool		Defensics
Reasons		If an unexpected input causes unpredictable abnormal behavior, abnormal termination, or restart, it would otherwise be exploited for a clue to attack.

3.3.8. Fuzz testing for CAN-FD

Item		Contents
ID		VULETS_02008
Application	Functions/Parts	ECUs with IF using CAN-FD

Conditions[Δ5]	Target AP[Δ1]	All
Requirements		For CAN-FD used in IF on the attack path (IF where the functions assigned Target AP are allocated)[Δ5], a fuzz testing shall be performed for all testing patterns with default configuration (CAN Sequences and OBD-II) of the recommended tool, and it shall be confirmed that security vulnerabilities have not been detected. (*1) [Δ5] *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. [Δ5] *2) Processing for unexpected inputs other than normal and abnormal inputs.[Δ5] The target ECU shall be kept normal against the load during the test. The vulnerability found by fuzz testing shall be fixed.[Δ6] If design changes occur after fuzz testing, fuzz testing shall be performed again.[Δ6]
Recommended Tool		Defensics
Reasons		If an unexpected input causes unpredictable abnormal behavior, abnormal termination, or restart, it would otherwise be exploited for a clue to attack.

3.3.9. Fuzz testing for TLS[Δ5]

Item		Contents
ID		VULETS_02009
Application Conditions[Δ5]	Functions/Parts	ECUs with IF using TLS
	Target AP[Δ1]	14~20
Requirements		For TLS, a fuzz testing shall be performed for all testing patterns with default configuration of the recommended tool, and it shall be confirmed that security vulnerabilities have not been detected. (*1) [Δ5] *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. [Δ5] *2) Processing for unexpected inputs other than normal and abnormal inputs.[Δ5] The target ECU shall be kept normal against the load during the test. The vulnerability found by fuzz testing shall be fixed.[Δ6] If design changes occur after fuzz testing, fuzz testing shall be performed again.[Δ6]
Recommended Tool		Defensics
Reasons		If an unexpected input causes unpredictable abnormal behavior, abnormal

	termination, or restart, it would otherwise be exploited for a clue to attack.

3.3.10. Fuzz testing for HTTP[Δ5]

Item		Contents
ID		VULETS_02010
Application Conditions[Δ5]	Functions/Parts	ECUs with IF using HTTP
	Target AP[Δ1]	14~20
Requirements		For HTTP, a fuzz testing shall be performed for all testing patterns with default configuration of the recommended tool, and it shall be confirmed that security vulnerabilities have not been detected. (*1) [Δ5] *1) The tester confirm that the error detected by the tool does not deviate from the response / behavior expected in the ECU specifications, and that exception processing (*2) is working for the fuzz data, etc. [Δ5] *2) Processing for unexpected inputs other than normal and abnormal inputs.[Δ5] The target ECU shall be kept normal against the load during the test. The vulnerability found by fuzz testing shall be fixed. [Δ6] If design changes occur after fuzz testing, fuzz testing shall be performed again. [Δ6]
Recommended Tool		Defensics
Reasons		If an unexpected input causes unpredictable abnormal behavior, abnormal termination, or restart, it would otherwise be exploited for a clue to attack.

3.4. **Deleted** [Δ5]

3.4.1. Deleted [Δ5]

Item		Contents
ID		VULETS_03001
Application Conditions[Δ5]	Functions/Parts	
	Target AP[Δ1]	
Requirements		Deleted. [Δ5]
Recommended Tool		
Reasons		

3.5. **Deleted** [Δ7]

3.5.1. Deleted [Δ7]

Item		Contents
ID		VULETS_04001
Application Conditions[Δ5]	Functions/Parts	-
	Target AP[Δ1]	-
Requirements		Deleted.
Recommended Tool		-
Reasons		-

3.6. Evaluation of Target AP[Δ1Δ2]

For vulnerabilities that potentially occur in implementing cybersecurity requirements (security functions) on ECU directed to each ECU from TMC, evaluate assuming an attack below the target AP, and confirm the achievement of the target AP of the security function,

It is assumed that evaluator is ECU designer, but it is also possible to conduct the evaluation by third party.

3.6.1. Collection of vulnerability candidate [Δ2Δ5]

Item		Contents
ID		VULETS_06001
Application Conditions[Δ5]	Functions/Parts	All ECUs
	Target AP[Δ1]	All
Requirements		Evaluator shall collect all vulnerability candidates about security function on ECU. Regardless of applying countermeasures, all candidates identified in the process shown below are the target of evaluation. If the vulnerability is eliminated by the countermeasure, it is excluded from the candidates. - Vulnerability analysis (“Requirements specification of vulnerability countermeasure for ECU” VULERQ_01002, VULERQ_01004, VULERQ_02004, VULERQ_02005, VULERQ_02006) - Vulnerability scanning (VULETS_01001, VULETS_01002) - Fuzz testing (VULETS_02001～VULETS_02008)
Recommended Tool		No recommendation
Reasons		To confirm that the risks are reduce to be acceptable level.

3.6.2. Define of evaluation item[Δ2]

Item		Contents
ID		VULETS_06002
Application Conditions[Δ5]	Functions/Parts	All ECUs
	Target AP	All
Requirements		For the vulnerability candidate collected in VULETS_06001, evaluator shall analyze attack path from entry point to vulnerability candidate, and define evaluation items to expected attacks. To define evaluation item, it may refer to “Annex1: Guide for Defining Cyber Attack Test Case”.[Δ5]
Recommended Tool		No recommendation
Reasons		To confirm that the risks are reduce to acceptable level.

3.6.3. Calculation of AP[Δ2]

Item		Contents
ID		VULETS_06003
Application Conditions[Δ5]	Functions/Parts	All ECUs
	Target AP	All
Requirements		Evaluator shall calculate AP to evaluate the evaluation items defined in VULETS_06002. Evaluator shall refer to “Annex1: Guide for Defining Cyber Attack Test Case,”about AP calculation. If the calculated value of AP is greater than or equal to the target AP, the evaluation item can be removed from evaluation items.[Δ2]
Recommended Tool		No recommendation
Reasons		To confirm that the risks are reduce to acceptable level.

3.6.4. Evaluation of AP on a real device[Δ2]

Item		Contents
ID		VULETS_06004
Application Conditions[Δ5]	Functions/Parts	All ECUs
	Target AP	All
Requirements		Evaluator shall conduct the evaluation in accordance with evaluation items defined in VULETS_06002, and evaluator shall confirm that attacks whose AP are less than target AP do not succeed. If the calculated AP is less than target AP, evaluator shall take measure against the vulnerability and confirm that attacks whose AP are less do not succeed.
Recommended Tool		No recommendation
Reasons		To confirm that the risks are reduce to acceptable level.